MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2023 R3

システム管理者マニュアル

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+

milestone

目次

著作権、商標、および免責条項

商標

XProtectはMilestone Systems A/Sの登録商標です。

MicrosoftおよびWindowsは、Microsoft Corporationの登録商標です。App StoreはApple Inc.のサービスマークです。AndroidはGoogle Inc.の商標です。

本文書に記載されているその他の商標はすべて、該当する各所有者の商標です。

免責条項

本マニュアルは一般的な情報を提供するためのものであり、その作成には細心の注意が払われています。

この情報を使用することにより発生するリスクはすべて、使用者が負うものとします。また、ここに記載されている内容はいずれも、いかなる事柄も保証するものではありません。

Milestone Systems A/Sは、事前の通知なしに変更を加える権利を有するものとします。

本書の例で使用されている人物および組織の名前はすべて架空のものです。実在する組織や人物に対する類似性は、それが現存しているかどうかにかかわらず、まったく偶然であり、意図的なものではありません。

この製品では、特定の規約が適用される可能性があるサードパーティー製ソフトウェアを使用することがあります。その場合、詳細はMilestoneシステムインストールフォルダーにあるファイル`3rd_party_software_terms_and_conditions.txt`を参照してください。

概要

新機能

Management Client 2023 R3

XProtect Management Client

Azure Active Directoryを認証に使用できるようになりました。インストール時に、統合セキュリティとして**Windows認証**と**Azure Active Directory統合**のいずれかを選択できます。

Azure統合セキュリティを使用してXProtectをインストールする方法の詳細については、147ページのシステムのインストール - カスタムオプションを参照してください。

XProtect Management Client

(サーバー証明書を信頼しない)オプションが、Windows認証とAzure Active Directory統合で利用可能になりました。Azure Active Directory Integratedの場合、このオプションは必須です。(サーバー証明書を信頼しない)オプションは、インストール前にサーバー証明書が検証・確認されるようにします。

XProtect Management Client:

システム管理者がアラーム定義、アラームステータス、アラームカテゴリ、アラーム音、アラーム保持、およびイベント保持を編集できる、アラームの新しい**アラーム設定編集**ユーザー権限が導入されました。アラーム定義の対応する編集権限は、既存の**管理**ユーザー権限から削除され、システム管理者はアラーム設定を管理するために両方のユーザー権限(**アラーム設定編集**と**管理**)が必要になります。

新しい**アラーム設定編集**ユーザー権限は、既存のユーザーには適用されず、インストールまたはアップグレード後、アラームを設定するために管理者レベルのアクセスが必要なユーザーには、手動で割り当てる必要があります。

カスタムインストールについて詳しくは、477ページの役割(セキュリティノード)を参照してください

Management Client 2023 R2 の新機能

XProtect Management Client:

アダプティブストリーミングを再生モードで使用するように設定できるようになりました。この方法はアダプティブ再生と呼ばれます。詳細については、220ページのアダプティブ再生(説明付き)を参照してください。

XProtect Management Client:

XProtectコンポーネントのインストール時に、カスタムインストールの一部として、作成済みデータベースを使用するように選択できるようになりました。カスタムインストールについて詳しくは、147ページのシステムのインストール - カスタムオプションを参照してください

XProtect Management Client:

ビデオ制限のための新しいユーザー権限が導入され、システム管理者は作成、閲覧、編集、削除の権限を設定し、ユーザーに割り当てることができるようになりました。詳細については、477ページの役割(セキュリティノード)を参照してください。

Management Client 2023 R1 の新機能

XProtect Incident Manager:

- GDPRまたは個人データに関するその他の適用法を遵守するために、XProtect Management Clientのシステム管理者はインシデントプロジェクトの保存期間を定義できます。

Management Client 2022 R3

XProtect Incident Manager:

- 現在、XProtect Incident Manager拡張機能は、XProtect Expert、XProtect Professional+、およびXProtect Express+のバージョン2022 R3以降とも互換性があります。
- XProtect Incident Managerは10,000件以上のインシデントプロジェクトを表示できるようになりました。

Management Client 2022 R2

XProtect Incident Manager:

- この拡張機能の最初のリリース
- XProtect Incident Manager拡張機能は、XProtect Corporateのバージョン2022 R2以降、およびXProtect Smart Clientのバージョン2022 R2以降と互換性があります。

XProtect LPR:

- 国モジュールの一部であるナンバープレートスタイルが、1か所にリストされるようになりました。を参照
- ナンバープレートスタイルの管理を容易にするために、ナンバープレート認識のニーズに応じてエイリアスにグループ化できるようになりました。を参照
- ナンバープレート一致リストでエイリアスがサポートされるようになりました。を参照

Management Client 2022 R1

イベントサーバーの暗号化

- イベントサーバーと通信するコンポーネント(LPR Serverなど) とイベントサーバー間の双方向接続を暗号化できるようになりました。

  詳細については、「288ページのイベントサーバーの暗号化を有効に設定」を参照してください。

外部IDP経由でのログイン

- 外部IDPを使用してMilestone XProtect VMSにログインできるようになりました。外部IDP経由でのログインは、Active Directoryユーザーまたは基本ユーザーとしてログインする別の方法です。外部IDPログインでは、基本ユーザーの設定要件をスキップできますが、XProtectでコンポーネントとデバイスにアクセスすることが許可されます。

  詳細については、外部IDP(説明付き) を参照してください。

ハードウェアデータの更新

- Management Clientでシステムによって検出されるハードウェアデバイスの現在のファームウェアバージョンを確認できるようになりました。

  詳細については、330ページのハードウェアデータを更新してくださいを参照してください。

XProtect Management Server Failover

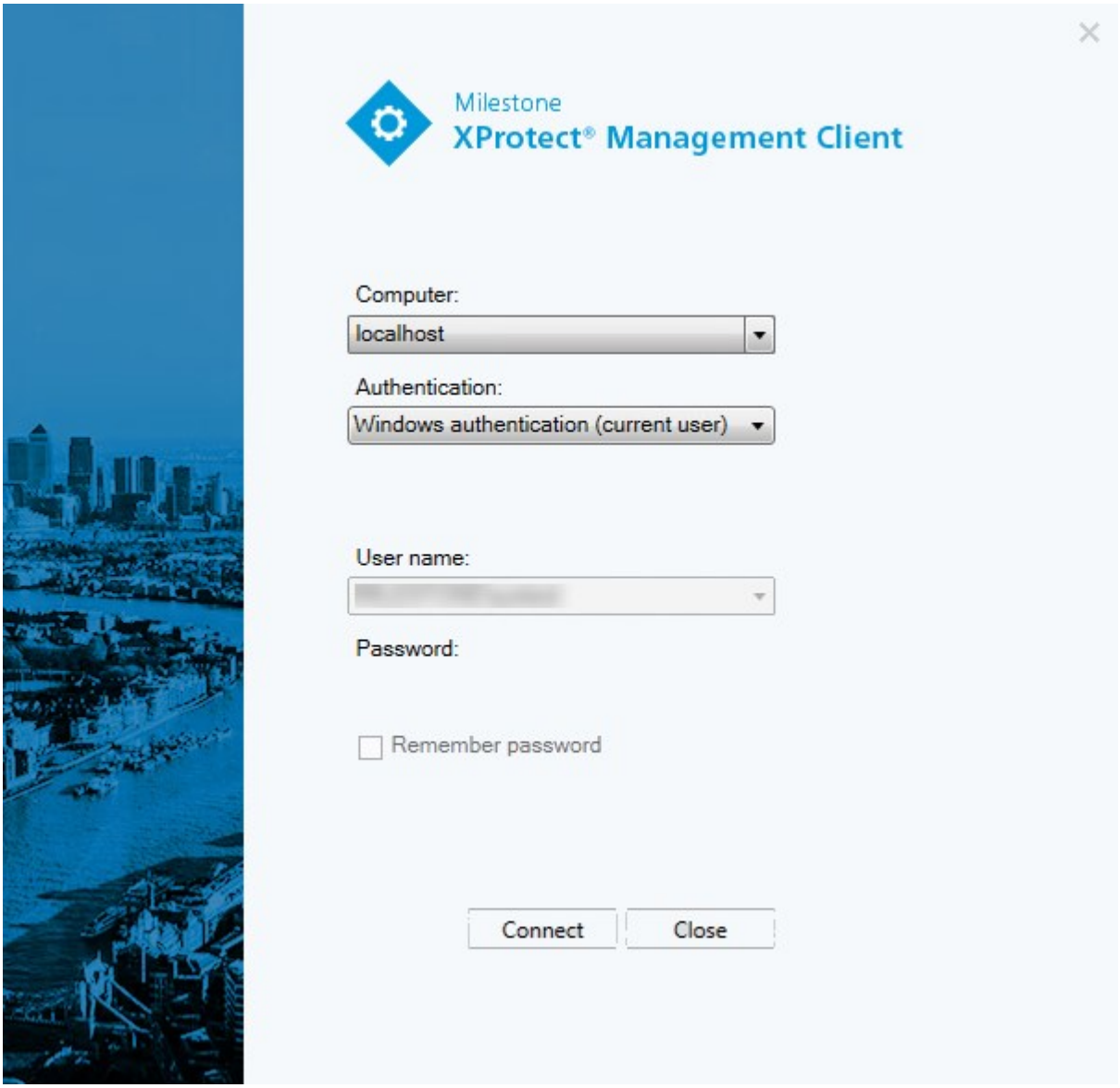
- 2台の冗長コンピュータ間でフェールオーバーマネジメントサーバーを設定することで、システムの可用性を向上できるようになりました。マネジメントサーバーを実行しているコンピュータが故障すると、2台目のサーバーによって引き継がれます。リアルタイムのデータ複製により、両方のコンピュータで同じマネジメントサーバー、ログサーバー、イベントサーバーが使用されることが保証されます。

  詳細については、36ページのXProtect Management Server Failover を参照してください。

ログイン(説明付き)

Management Clientを起動するときには、まずログイン情報を入力し、システムに接続する必要があります。

XProtect Corporate 2016 またはXProtect Expert 2016 以降がインストールされていれば、パッチをインストールした後に、古いバージョンの製品が実行されているシステムにログインできます。XProtect Corporate 2013 およびXProtect Expert 2013 以降のバージョンがサポートされています。



ログイン認証(説明付き)

十分な権限を持つ2番目のユーザーがログインを許可した場合のみユーザーがシステムにログインできるようにするため、システムでは管理者によるユーザーの設定が許可されています。この場合、XProtect Smart ClientまたはManagement Clientでは、ログイン中に2番目の認証を要求されます。

定義済みの**システム管理者**の役割に関連付けられたユーザーは常に認証する権限があるため、2番目のログインが必要な別の役割に関連付けられていないかぎり、2番目のログインは要求されません。

外部IDP経由でログインするユーザーは、2人目のユーザーによる承認要件で設定することはできません。

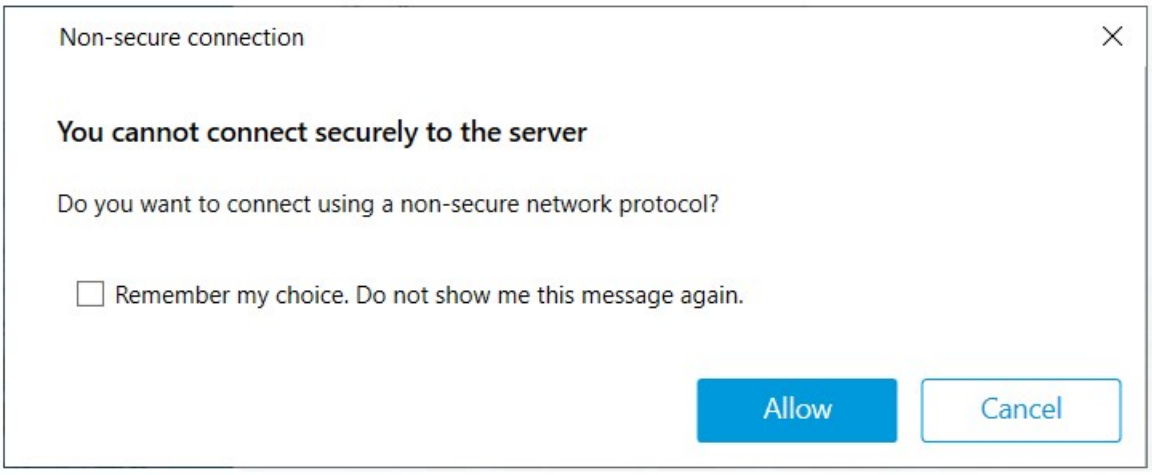
ログイン認証を役割に関連付けるには:

- **[役割]**の**[情報]**タブで、選択した役割の**[ログイン認証が必要]**を設定し(「役割の設定」を参照)、ユーザーがログイン中に追加の認証を要求されるようにします。
- **[役割]**の**[セキュリティ全般]**タブで、選択した役割の**[ユーザーを認証]**を設定し(「役割の設定」を参照)、ユーザーが他のユーザーのログインを認証できるようにします。

同じユーザーで両方のオプションを選択できます。つまり、ユーザーはログイン中に追加の認証を要求されますが、自分のログインを除き、他のユーザーのログインを認証することもできます。

安全でない接続を使用してログインする

管理クライアントにログインすると、安全でないネットワークプロトコルを使用してログインするかどうかを尋ねられる場合があります。



- 通知を無視してログインするには、**許可**をクリックします。今後この通知が届かないようにするには、**選択内容を記憶するを選択しますこのメッセージを再度表示しないか、ツール > オプション**をクリックして、**サーバーへの安全でない接続を許可するを選択します(管理クライアントの再起動が必要です)**。

安全な通信に関する詳細については、136ページの安全な通信(説明付き)を参照してください。

基本ユーザーのパスワード変更

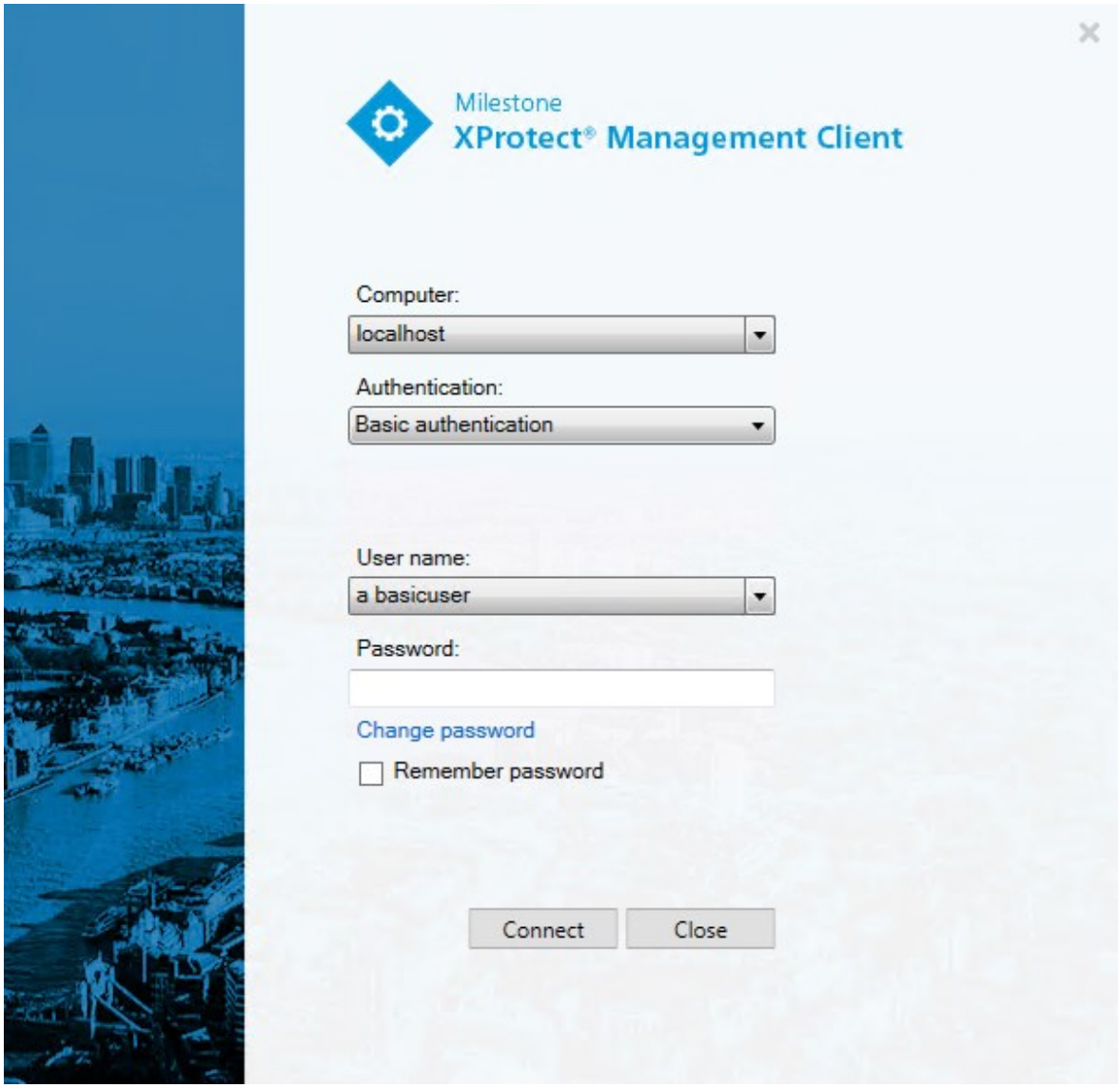
基本ユーザーとしてログインすると、自分のパスワードを変更できます。異なる認証方法を選択すると、システム管理者しかパスワードを変更できなくなります。パスワードを頻繁に変更すると、XProtect VMSシステムのセキュリティが高くなります。

要件

XProtect VMSシステムのバージョンは2021 R1以降でなくてはなりません。

手順:

1. Management Clientを起動します。ログインウィンドウが開きます。
2. ログイン情報を指定します。**認証**リストで、**基本認証**を選択します。**「パスワード変更」**と書かれたリンクが表示されます。



3. リンクをクリックします。ブラウザウィンドウが開きます。
4. 指示に従い、変更を保存します。
5. これで新しいパスワードを使い、Management Clientにログインできます。

製品概要

XProtect VMS製品は多種多様なインストール用に設計された監視カメラ管理ソフトウェアです。お店を破壊行為から守りたい場合も複数の施設を管理したい場合も、XProtectがあれば可能です。このソリューションはすべてのデバイス、サーバー、およびユーザーを集中管理し、スケジュールとイベントによる非常に柔軟なルールシステムを提供します。

このシステムは、以下の主要な要素で構成されています。

- **Management Server**は、インストールの中心で、複数のサーバーで構成されています。
- 1つまたは複数の**Recording Server**
- **XProtect Management Client**の、1つ以上のインストール
- **XProtect Download Manager**
- **XProtect® Smart Client**の、1つ以上のインストール
- **XProtect Web Client**の1つ以上の使用および/または必要に応じて**XProtect Mobile**クライアントのインストール

また、このシステムには、監視システムの任意のカメラからMatrixをインストールした任意のコンピュータにビデオを配信表示することができる、統合的なXProtect Smart Client機能があります。

システムは仮想サーバーまたは複数の物理的なサーバーに分散型設定でインストールできます。「83ページの分散型システム設定」も参照してください。

さらに、このシステムには、XProtect® Smart Client - Playerからエビデンスビデオをエクスポートする際に、スタンドアロンのXProtect Smart Client を含めることも可能です。XProtect Smart Client - Playerを使うと、エビデンスビデオの受信者(警察官、内部/外部捜査官など)は、ソフトウェアをコンピュータにインストールしなくてもエクスポートされた録画を閲覧および再生することができます。

最も豊富な機能が備わった製品をインストールすれば(「105ページの製品比較」を参照)、お使いのシステムでカメラ、サーバー、ユーザーを数に制限なく、そして必要に応じて複数のサイトにわたって使用できます。IPv4に加えて、IPv6も処理できます。

システムコンポーネント

マネジメントサーバー(説明付き)

マネジメントサーバーは監視カメラ管理ソフトウェアシステムの中心となるコンポーネントです。SQL Serverデータベース内の監視システムの設定は、SQL Serverマネジメントサーバーコンピュータ本体、またはネットワーク上の別のSQL Serverに保存されます。また、ユーザー認証、ユーザー権限、ルールシステムなども処理します。システムパフォーマンスを改善するために、複数のマネジメントサーバーを1つのMilestone Federated Architecture™として実行することができます。マネジメントサーバーはサービスと実行されるものであり、通常は専用サーバーにインストールされます。

ユーザーは初期認証のためにマネジメントサーバーに接続し、それからたとえばビデオ録画のためにレコーディングサーバーへと透過的に接続できます。

SQL Server インストールとデータベース(説明付き)

マネジメントサーバー、イベントサーバー、ログサーバーには、単一または複数のSQL Serverインストールの SQL Serverデータベースに存在するシステム構成、アラーム、イベント/ログメッセージなどが保存されます。マネジメントサーバーとイベントサーバーは同じSQL Serverデータベースを共有しますが、ログサーバー、XProtect Incident Manager、およびIdentity Providerには、それぞれ独自のSQL Serverデータベースがあります。Identity Providerに関する詳細は61ページのIdentity Provider(説明付き)を参照してください。XProtect Incident Managerデータベースとログインに関する詳細は、別途、XProtect Incident Managerのシステム管理者マニュアルを参照してください。

システムインストーラには、Microsoft SQL Server Express(SQL Serverの無料版)が含まれています。

Milestoneは、大規模なシステムまたはSQL Serverデータベースを往来するトランザクションが多いシステムについては、ネットワーク上の専用コンピュータと、他の目的で使用されていない専用ハードディスクドライブでのMicrosoft® SQL Server® StandardまたはSQL ServerのMicrosoft® SQL Server® Enterpriseエディションを使用するよう推奨しています。専用ドライブにSQL Serverをインストールすることで、全体的なシステムパフォーマンスが向上します。

レコーディングサーバー(説明付き)

レコーディングサーバーは、ネットワークカメラやビデオエンコーダーと通信して、取得された音声および動画を記録した上で、ライブおよび記録された音声および動画へのアクセスをクライアントに提供します。また、レコーディングサーバーは、Milestoneテクノロジーを使って他のMilestone Interconnect製品との通信も行います。

デバイスドライバー

- ネットワークカメラとビデオエンコーダーとの通信は、各デバイス専用に開発されたデバイスドライバー、または同じメーカーからの類似した複数のデバイス用のデバイスドライバーを通して行われます
- 2018 R1のリリースから、デバイスドライバーは2つのDevice Packに分けられます:より新しいドライバーを持つレギュラーDevice Packと、古いバージョンのドライバーを持つレガシーDevice Packです
- レギュラーDevice Packは、レコーディングサーバーをインストールする時に自動的にインストールされます。その後、新しいバージョンのDevice Packをダウンロード、およびインストールすることで、ドライバーを更新できます
- レガシーDevice Packは、システムがレギュラーDevice Packをインストール済みの場合のみ、インストールすることが可能です。前のバージョンがすでにシステムにインストールされている場合は、レガシーDevice Packからのドライバーは、自動的にインストールされます。これは、ソフトウェアダウンロードページ(https://www.milestonesys.com/downloads/)から手動でダウンロードしてインストールできます

メディアデータベース

- 取得された音声および動画データは、レコーディングサーバーに保存されます。このカスタムメードの高パフォーマンスデータベースは、音声および動画データの録画と保管用に最適化されています。
- メディアデータベースは、多段階アーカイブ、ビデオグルーミング、暗号化、および録画への電子署名の追加など、さまざまな独自の機能をサポートしています

システムは、ビデオフィードの録画、およびカメラと他デバイス間の通信のためにレコーディングサーバーを使用します。一般的に、監視システムは複数のレコーディングサーバーで構成されています。

レコーディングサーバーはRecording Serverソフトウェアをインストールし、マネジメントサーバーと通信するよう設定されたコンピュータです。**サーバー**フォルダーを展開し、**レコーディングサーバー**を選択すると、**概要**ペインにレコーディングサーバーが表示されます。

このバージョンのマネジメントサーバーよりも前のレコーディングサーバーのバージョンとの後方互換性は制限されています。旧バージョンのレコーディングサーバーの録画にアクセスすることはできますが、それらの設定を変更するには、このバージョンのマネジメントサーバーに対応していることを確認してください。Milestoneは、システム内のすべてのレコーディングサーバーを、マネジメントサーバーと同じバージョンにアップグレードすることを推奨しています。

レコーディングサーバーは、クライアントとサービスにストリーミングされるデータの暗号化に対応しています。

- 289ページのクライアントとサーバーに対して暗号化を有効にする
- 275ページのクライアントの暗号化ステータスを表示する

レコーディングサーバーもマネジメントサーバーとの接続の暗号化に対応しています。

- 285ページのマネジメントサーバーとの間で暗号化を有効にする

レコーディングサーバーの管理については、次のような複数のオプションがあります。

- 203ページのハードウェアの追加
- 323ページのハードウェアの移動
- 342ページのレコーディングサーバーでのすべてのハードウェアの削除
- 341ページのレコーディングサーバーの削除

> **!** Recording Serverサービスの実行中は、Windows Explorerや他のプログラムが、お使いのシステム設定に関連付けられたメディアデータベースファイルやフォルダーにアクセスしていないことが非常に重要です。アクセスしている場合は、レコーディングサーバーの名前を変更したり、関連するメディアファイルを移動できません。このためにレコーディングサーバーが停止することがあります。停止したレコーディングサーバーを再開するには、Recording Serverサービスを停止し、関連するメディアファイルやフォルダーにアクセスしているプログラムを閉じ、Recording Serverサービスを再起動してください。

モバイルサーバー(説明付き)

モバイルサーバーはXProtect Mobileクライアントおよび XProtect Web Clientユーザーがシステムにアクセスできるようにします。

これら2種のクライアントのシステムゲートウェイとして機能するほか、オリジナルカメラのビデオストリームでは多くの場合、クライアントユーザーの帯域幅には大きすぎるため、モバイルサーバーはビデオのトランスコード(再エンコード)も行うことができます。

分散または**カスタム**インストールを実行している場合、Milestoneは、モバイルサーバーを専用サーバーにインストールすることを推奨します。

イベントサーバー(説明付き)

イベントサーバーは、イベント、アラーム、マップ、そして場合によってはMIP SDKを介したサードパーティ統合に関連した各種タスクを処理する役割を担います。

イベント

- すべてのシステムイベントがイベントサーバーに統合されるため、システムイベントを活用して統合を実行するパートナーは、場所とインターフェースを一元化できます
- また、イベントサーバーは、ジェネリックイベントまたはアナリティクスイベントインターフェースを通してシステムにイベントを送信するためのサードパーティアクセスを提供します

アラーム

- イベントサーバーは、アラーム機能、アラームロジック、アラーム状態をホストし、アラームデータベースを処理します。アラームデータベースは、マネジメントサーバーが使用するものと同じSQL Serverデータベースに保存されます

メッセージ

- メッセージ通信はイベントサーバーによって処理され、プラグインはXProtect Smart Client、Management Client、イベントサーバーやスタンドアロンサービスなどの環境間でリアルタイムにメッセージを送信できます。

マップ

- イベントサーバーは、XProtect Smart Clientで設定および使用されているマップもホストします

MIP SDK

- 最後に、システムイベントへのアクセスに使用する、サードパーティ製のプラグインをイベントサーバーにインストールすることができます

ログサーバー(説明付き)

ログサーバーには、SQL Serverデータベース内でシステム全体に対して発せられたすべてのログメッセージが保存されます。このログメッセージSQLデータベースは、マネジメントサーバーのシステム設定SQLデータベースと同じSQL Serverまたは別のSQL Serverに実装することができます。ログサーバーは通常、マネジメントサーバーと同じサーバーにインストールされますが、マネジメント/ログサーバーのパフォーマンス向上のため別のサーバーにインストールにインストールすることも可能です。

API Gateway(説明付き)

MIP VMS APIは、OpenAPIなどの業界標準プロトコルに基づく統合「RESTful API」を提供し、XProtect VMS機能にアクセスして統合プロジェクトを簡素化し、クラウド接続通信の基盤として機能します。

XProtect VMS API GatewayはこれらのMilestone Integration Platform VMS API(MIP VMS API)を介してサポートします。

API Gatewayはオンプレミスにインストールされ、現在のすべてのVMSサーバーコンポーネント(マネジメントサーバー、イベントサーバー、レコーディングサーバー、ログサーバーなど) で「RESTful API」サービスおよび「WebSocket Messaging API」サービスのフロントエンドおよび共通のエントリポイントとして機能します。API Gatewayサービスは、マネジメントサーバーと同じホストにインストールすることも、個別にインストールすることもできます。また、複数のサービスを(それぞれの各ホストに) インストールすることもできます。

「RESTful API」は、特定のVMSサーバーコンポーネントごとに部分的に実装されており、API Gatewayはこれらのリクエストと応答を単純にパススルーできますが、他のリクエストの場合は、API Gatewayが必要に応じてリクエストと応答を変換します。

現在、マネジメントサーバーによってホストされる構成APIは、「RESTful API」として使用できます。イベントサーバーがホストするRESTful Events API、Websocket messaging API、RESTful Alarms APIも利用可能です。

詳細はAPI Gatewayシステム管理者マニュアル およびMilestone Integration Platform VMS APIリファレンスドキュメントを参照してください。

フェールオーバー

XProtect Management Server Failover

Management Serverサービスまたは SQL Serverを実行しているスタンドアロンのコンピューターにハードウェア障害が発生した場合でも、録音/録画やレコーディングサーバーに影響はありません。しかし、これらのハードウェア障害により、クライアントにログインしていないオペレータおよびシステム管理者でダウンタイムが発生する可能性があります。

XProtect Management Server Failoverは、マネジメントサーバーに高可用性と障害復旧を提供します。マネジメントサーバーが1台のコンピュータで使用できなくなった場合、もう一方のコンピュータがシステムコンポーネントの実行を引き継ぎます。

SQL Serverデータベースのセキュアなリアルタイム複製機能を利用することで、ハードウェア障害が発生した場合でもデータの損失を防ぐことができます。

XProtect Management Server Failoverはシステムのダウンタイムを軽減できます。次の場合に、フェールオーバークラスタのメリットを得られます。

- サーバーに障害が発生した場合 - 問題を解決している間に、別のコンピュータからManagement Serverサービスと SQL Serverを実行できます。
- システムのアップデートとセキュリティパッチが必要な場合 -スタンドアロンのマネジメントサーバーにセキュリティパッチを行うと時間がかかり、ダウンタイムが長引く可能性があります。フェールオーバー クラスタがあれば、最小限のダウンタイムでシステムのアップデートとセキュリティパッチを行えます。
- シームレスな接続が必要な場合 - ユーザーは、いつでも中断されることなくライブビデオと再生ビデオ、およびシステム設定にアクセスできます。

2台のコンピュータ間でXProtect Management Server Failoverを設定します。フェールオーバーを機能させるために、各コンピュータにをインストールします。

- XProtect Management Server
- XProtectEvent Server サービス
- XProtectLog Server サービス

- Microsoft SQL Server(推奨)

フェールオーバーマネジメントサーバー(説明付き)

マネジメントサーバーのフェールオーバーサポートは、MicrosoftWindowsClusterにマネジメントサーバーをインストールすることで実現できます。クラスタでは、最初のサーバーで障害が起こった場合、マネジメントサーバー機能を他のサーバーが引き継ぎます。

フェールオーバーレコーディングサーバー(説明付き)

> 使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

フェールオーバーレコーディングサーバーは、予備のレコーディングサーバーで、通常のレコーディングサーバーが使用できなくなったときに使用されます。フェールオーバーレコーディングサーバーは、**コールドスタンバイサーバー**として、または**ホットスタンバイサーバー**として、2つの方法で構成できます。

フェールオーバーレコーディングサーバーは、通常のレコーディングサーバーと同様にインストールされます(158ページのDownload Managerを介したフェールオーバーレコーディングサーバーのインストールを参照)。フェールオーバーレコーディングサーバーがインストールされると、Management Clientで表示されるようになります。Milestoneはすべてのフェールオーバーレコーディングサーバーを個別のコンピュータにインストールすることを推奨しています。フェールオーバーレコーディングサーバーが、マネジメントサーバーの正しいIPアドレス/ホスト名を用いて構成されていることを確認します。フェールオーバーサーバーサービスを実行するユーザーアカウントのユーザー権限は、インストールプロセス中に付与されます。すなわち:

- フェールオーバーレコーディングサーバーを開始または停止するための開始/停止許可
- RecorderConfig.xmlファイルを読み取る/書き込むための読み取りおよび書き込みアクセス許可

暗号化に対して証明書が選択されている場合、管理者は選択した証明書プライベートキーにおいて、フェールオーバーユーザーに読み取りアクセス許可を付与する必要があります。

> Milestoneでは、フェールオーバーレコーディングサーバーが暗号化を使用しているレコーディングサーバーを引き継ぐ際、フェールオーバーレコーディングサーバーも暗号化を使用するよう準備する必要があります。詳細については136ページの安全な通信(説明付き)と「158ページのDownload Managerを介したフェールオーバーレコーディングサーバーのインストール」を参照してください。

デバイスレベルで必要なフェールオーバーサポートのタイプを指定できます。レコーディングサーバー上の各デバイスで、フル、ライブのみ、フェールオーバーサポートなしを選択できます。これにより、フェールオーバーリソースに優先順位を付けることができます。例えば、ビデオのフェールオーバーのみを設定し、音声には設定しないことも可能です。また、重要性の低いカメラにはフェールオーバーせず、重要なカメラのみをフェールオーバーの対象にできます。

システムがフェールオーバーモードの間は、ハードウェアの置き換えや削除、レコーディングサーバーの更新、ストレージ設定やビデオストリーム設定のようなデバイスの設定を行うことはできません。

コールドスタンバイフェールオーバーレコーディングサーバー

コールドスタンバイフェールオーバーレコーディングサーバーの設定では、1つのフェールオーバーグループに複数のフェールオーバーレコーディングサーバーを集めます。複数の事前に選択されたレコーディングサーバーのいずれかが使用できなくなった場合に、フェールオーバーグループ全体が代わりに対応します。必要な数だけグループを作成することができます(200ページのコールドスタンバイ用にフェールオーバーレコーディングサーバーをグループ化を参照)。

グループ化には明確なメリットがあります。レコーディングサーバーに取って代わるフェールオーバーレコーディングサーバーを後から指定する場合は、フェールオーバーレコーディングサーバーのグループを選択します。選択したグループに複数のフェールオーバーレコーディングサーバーがある場合、レコーディングサーバーを使用できなくなっても引き継ぎの準備ができているフェールオーバーレコーディングサーバーが1台以上あるため、安全です。プライマリグループのすべてのレコーディングサーバーが応答しない場合は、プライマリグループにとって代わるフェールオーバーサーバーのセカンダリグループを特定できます。1つのフェールオーバーレコーディングサーバーは、一度に1つのグループにのみ属することができます。

フェールオーバーグループのフェールオーバーレコーディングサーバーには順序があります。この順序に従い、フェールオーバーレコーディングサーバーが、レコーディングサーバーに取って代わる順序が決定されます。デフォルトでは、フェールオーバーグループでフェールオーバーレコーディングサーバーを統合した順序が反映されます。必要に応じて、この順序は変更できます。

ホットスタンバイフェールオーバーレコーディングサーバー

このため、システムはこのフェールオーバーレコーディングサーバーを「スタンバイ」モードのままにできます。つまり、レコーディングサーバーの現在の正しい構成を使用してすでに起動されており、専用であるため、コールドスタンバイフェールオーバーレコーディングサーバーよりも迅速に切り替えられます。前述の通り、ホットスタンバイサーバーは1つのレコーディングサーバーにのみ割り当てられ、グループ化できません。すでにフェールオーバーグループに含まれているフェールオーバーサーバーは、ホットスタンバイレコーディングサーバーとして割り当てできません。

フェールオーバーレコーディングサーバーの検証

フェールオーバーサーバーからレコーディングサーバーへのビデオデータの統合を検証するには、レコーディングサーバーのサービスを停止するか、レコーディングサーバーのコンピュータをシャットダウンしてレコーディングサーバーを利用できない状態にする必要があります。

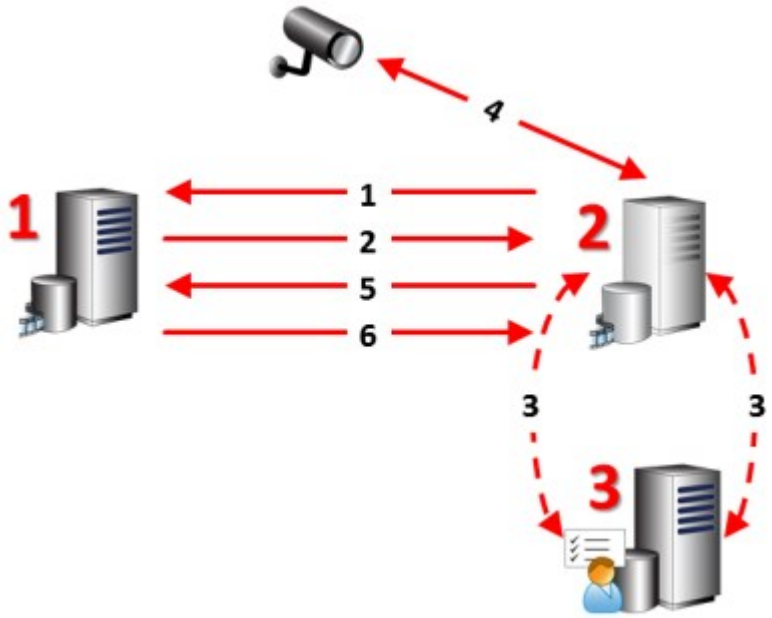
ネットワークケーブルを抜くか、テストツールを使ってネットワークをブロックするような手動によるネットワークの中断は有効な方法ではありません。

フェールオーバーレコーディングサーバー機能(説明付き)

- フェールオーバーレコーディングサーバーは、毎0.5秒ごとに関連するレコーディングサーバーの状態を確認します。2秒以内にレコーディングサーバーが応答しない場合、レコーディングサーバーは利用できないと見なされ、フェールオーバーレコーディングサーバーが取って代わります。コールドスタンバイフェールオーバーレコーディングサーバーは、使用できないレコーディングサーバーを引き継ぎます。
- この処理にかかる時間は、フェールオーバーレコーディングサーバーのRecording Serverサービスが起動する時間と、カメラに接続する時間に、5秒間を加えた時間です。これとは対照的に、ホットスタンバイのフェールオーバーレコーディングサーバーでは、Recording Serverサービスがすでに正しい設定で実行中であり、フィードを配信するためにカメラに接続するだけでよいため、より迅速に切り替えられます。起動中は、該当するカメラからの録画の保存も、ライブビデオの表示もできません。
- レコーディングサーバーがもう一度使用可能になると、フェールオーバーレコーディングサーバーから自動的に引き継がれます。フェールオーバーレコーディングサーバーによって保存された録画は、自動的に標準レコーディングサーバーのデータベースに統合されます。統合にかかる時間は、録画の分量やネットワークの能力などに応じて異なります。統合プロセスの実施中、フェールオーバーレコーディングサーバーが代替していた時間中の録画を参照することはできません。
- コールドスタンバイフェールオーバーレコーディングサーバーの設定の統合処理中に、フェールオーバーレコーディングサーバーが別のレコーディングサーバーから引き継ぐ必要が生じた場合は、レコーディングサーバーAとの統合処理が延期され、レコーディングサーバーBから引き継ぎます。
- レコーディングサーバーBが再び使用可能になると、フェールオーバーレコーディングサーバーが統合処理を再開し、レコーディングサーバーAとレコーディングサーバーBの両方を同時にレコーディングに統合します。ホットスタンバイ設定では、ホットスタンバイサーバーは1台のレコーディングサーバーに対してのみホットスタンバイできるため、他のレコーディングサーバーから引き継ぐことはできません。ただし、レコーディングサーバーで再度障害が発生した場合、ホットスタンバイは再度処理を引き継ぎ、前の期間からの録画も保持します。プライマリレコーダーに統合されるか、フェールオーバーレコーディングサーバーのディスク領域がなくなるまで、録画はレコーディングサーバーに保持されます。
- フェールオーバーソリューションでは、完全な冗長性が提供されません。これは、ダウンタイムを最小化するための信頼できる方法としてのみ利用できます。レコーディングサーバーがもう一度使用可能になると、FailoverServerサービスは、レコーディングサーバーで録画を保存する準備ができていることを確認します。その場合にのみ、録画を保存する責務が標準のレコーディングサーバーに戻されます。したがって、この段階で録画が失われることはほとんどありません。
- クライアントユーザーは、フェールオーバーレコーディングサーバーへの切り替えが発生したことにほとんど気付かないはずです。フェールオーバーレコーディングサーバーが引き継ぐと、短い停止(通常は数秒)が発生します。この切断中は、該当するレコーディングサーバーからビデオにアクセスできません。クライアントユーザーは、フェールオーバーレコーディングサーバーが切り替えられるとすぐに、ライブビデオ表示を再開できます。最近の録画はフェールオーバーレコーディングサーバーに保存されるため、フェールオーバーレコーディングサーバーが引き継いだ後からも録画を再生できます。クライアントは、レコーディングサーバーが動作を再開して、フェールオーバーレコーディングサーバーから切り替えられるまで、対象のレコーディングサーバー上にのみ保存されている古い録画を再生することができません。アーカイブ済みの録画にはアクセスできません。レコーディングサーバーが動作を再開すると、フェールオーバー録画が、レコーディングサーバーのデータベースへと再統合される統合プロセスが実行されます。このプロセスの実施中、フェールオーバーレコーディングサーバーが代替していた時間中の録画を再生することはできません。

- コールドスタンバイ設定では、別のフェールオーバーレコーディングサーバーのバックアップとして、もう1つのフェールオーバーレコーディングサーバーを設定する必要はありません。特定のレコーディングサーバーを引き継ぐためにフェールオーバーグループを割り当て、特定のフェールオーバーレコーディングサーバーを割り当てないためです。フェールオーバーグループには、最低1つのフェールオーバーレコーディングサーバーを含む必要があり、いくつでもフェールオーバーレコーディングサーバーを追加できます。フェールオーバーグループに2つ以上のフェールオーバーレコーディングサーバーが含まれている場合、2つ以上のフェールオーバーレコーディングサーバーで引き継ぎが可能になります。
- ホットスタンバイ設定では、ホットスタンバイサーバーとして、フェールオーバーレコーディングサーバーまたはホットスタンバイサーバーを設定できません。

フェールオーバーの手順(説明付き)



説明
関連するサーバー(赤字は台数): 1. Recording Server 2. Failover Recording Server 3. Management Server
コールドスタンバイ設定のフェールオーバー手順: 1. 実行しているかどうかを確認するために、フェールオーバーレコーディングサーバーには、レコーディングサーバーへの継続的なTCP接続があります。

説明
2. この接続は中断されます。 3. フェールオーバーレコーディングサーバーが、マネジメントサーバーから現在のレコーディングサーバーの設定を要求します。マネジメントサーバーが要求された設定を送ると、フェールオーバーレコーディングサーバーはレコーディングサーバーに代わって構成を受信して起動し、記録を開始します。 4. フェールオーバーレコーディングサーバーと関連するカメラはビデオデータを交換します。 5. フェールオーバーレコーディングサーバーは継続的にレコーディングサーバーへの接続を再確立します。 6. レコーディングサーバーへの接続が再確立されると、フェールオーバーレコーディングサーバーがシャットダウンし、レコーディングサーバーによってダウンタイム中に(存在する場合)録画されたビデオデータが取得されます。また、ビデオデータはレコーディングサーバーデータベースに再度統合されます。
ホットスタンバイ設定のフェールオーバー手順: 1. 実行しているかどうかを確認するために、ホットスタンバイサーバーには、割り当てられたレコーディングサーバーへの継続的なTCP接続があります。 2. この接続は中断されます。 3. ホットスタンバイサーバーは割り当てられたレコーディングサーバーの現在の構成をマネジメントサーバーからすでに把握しており、独自に録画を開始します。 4. ホットスタンバイサーバーと関連するカメラはビデオデータを交換します。 5. ホットスタンバイサーバーは継続的にレコーディングサーバーへの接続を再確立します。 6. レコーディングサーバーへの接続が再確立され、ホットスタンバイサーバーがホットスタンバイモードに戻ると、フェールオーバーレコーディングサーバーはシャットダウンし、レコーディングサーバーはダウンタイム中に(存在する場合)録画されたビデオデータを取得します。また、ビデオデータはレコーディングサーバーデータベースに再度統合されます。

フェールオーバーレコーディングサーバーのサービス(説明付き)

フェールオーバーレコーディングサーバーには、次の2つのサービスがインストールされます。

- Failover Serverサービスは、レコーディングサーバーが使用できなくなった場合に処理を引き継ぎます。このサービスは絶えず関連するレコーディングサーバーの状態をチェックしているため、常に実行されています。
- Failover Recording Serverサービスは、レコーディングサーバーの役割を果たすようフェールオーバーレコーディングサーバーを有効にします。

  コールドスタンバイ設定では、このサービスは、レコーディングサーバーからコールドスタンバイフェールオーバーレコーディングサーバーに切り替える際など、必要なときにのみ開始されます。このサービスの開始には通常数秒かかりますが、ローカルのセキュリティ設定などに応じてそれよりも長くかかる場合もあります。
  ホットスタンバイ設定では、このサービスは常に実行されるため、ホットスタンバイサーバーは通常のフェールオーバーレコーディングサーバーがよりも迅速に切り替えることができます。

クライアント

Management Client(説明付き)

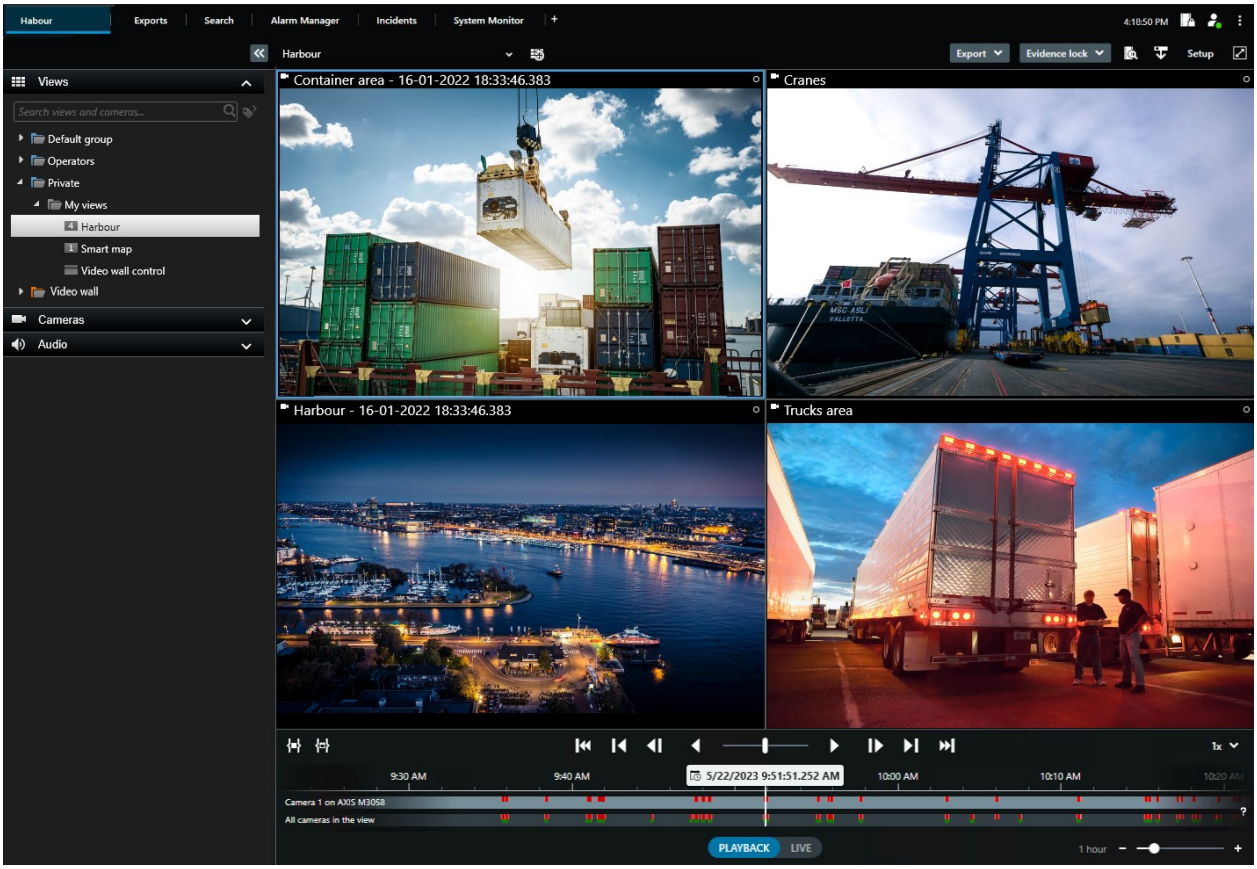
Management Clientは、システムの設定や日常的な管理を円滑にこなすための、豊富な機能を備えたマネジメントクライアントです。複数の言語で用意されています。

通常は、監視システムの管理者のワークステーションか同等の場所にインストールされます。

XProtect Smart Client(説明付き)

XProtect Smart Clientは、IP監視カメラの管理に役立つよう設計されたデスクトップアプリケーションです。ライブおよび録画ビデオへのアクセス、カメラおよび接続済みセキュリティデバイスの制御、録画とメタデータの詳細検索能力をユーザーに与えることにより、セキュリティシステムに対する直感的なコントロールを提供します。

複数の言語で使用でき、XProtect Smart Clientは柔軟性の高いユーザーインターフェースを、各オペレータの作業に応じて最適化が可能で、かつ、特定のスキルや権限レベルに応じて調整が可能です。



ライトとダークの2つのテーマを選択することで、特定の任務環境のためにビューをカスタマイズすることをインターフェイスが許可します。作業に最適化されたタブや、監視作業がしやすいメインタイムラインも搭載しています。

MIP SDKを使用することにより、ユーザーはさまざまなタイプのセキュリティシステム、ビジネスシステム、映像解析アプリケーションを統合し、XProtect Smart Clientを介して管理できます。

XProtectSmartClientはオペレータのコンピュータにインストールする必要があります。監視システム管理者はManagement Clientを通じて、監視システムを管理します。クライアントが表示する録画データは、XProtectシステムImageServerのサービスによって配信されます。サービスは、監視システムサーバーのバックグランドで実行されます。別個のハードウェアは不要です。

XProtect Mobileクライアント(説明付き)

XProtect Mobileクライアントは、モバイル監視ソリューションで、XProtectシステムの他の部分と密接に統合されます。AndroidタブレットまたはスマートフォンあるいはApple®タブレット、スマートフォン、もしくはポータブル音楽プレーヤーで実行され、カメラへのアクセス権限を与え、管理 クライアントに設定された他の機能を表示します。

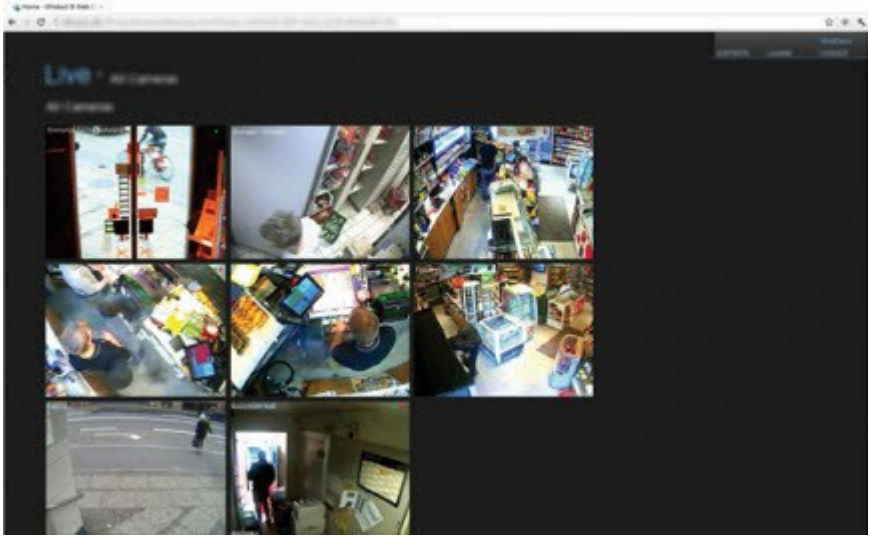
XProtect Mobileクライアントを使用して、複数のカメラのライブビューの確認および録画されたビデオの再生を行ったり、パン/チルト/ズーム(PTZ)カメラの制御や、出力やイベントを実行することができます。また、ビデオ配信機能を使用して、使用しているモバイルデバイスのビデオをXProtectシステムに送信します。

システムでXProtect Mobileクライアントを使用したい場合は、XProtect Mobileサーバーを追加して、XProtect Mobileクライアントと使用しているシステムの間での接続を確立する必要があります。XProtect Mobileサーバーが設定されたら、Google PlayまたはApp Storeから無料のXProtect Mobileをダウンロードし、XProtect Mobileの使用を開始します。

ビデオをXProtectシステムにプッシュ配信するデバイスごとに、デバイスライセンスが1つ必要となります。

XProtect Web Client(説明付き)

XProtect Web ClientはWebベースのクライアントアプリケーションで、ビデオを表示、再生、共有できます。ライブビデオの表示、録画ビデオの再生、エビデンスの印刷やエクスポートなど、最も頻繁に使用される監視機能に瞬時にアクセスできます。機能へのアクセス権は、Management Clientで設定した個別のユーザー権限によって異なります。



XProtect Web Clientへのアクセスを有効にするには、XProtect Mobileサーバーをインストールして、XProtect Web Client と、使用しているシステムの間での接続を確立する必要があります。XProtect Web Client自体はインストールを必要とせず、大半のインターネットブラウザで動作します。XProtect Mobileサーバーを設定すると、場所を問わずインターネットに接続されているコンピュータやタブレットからお使いのXProtectシステムを監視できます(ただし、正確な外部/インターネットアドレス、ユーザー名、パスワードがわかっていることが条件となります) 。

XProtectの拡張機能

XProtect Access(説明付き)

Milestoneはさまざまな拡張機能を開発してきました。拡張機能とは、XProtectVMS製品の機能を拡張し、さらに特殊な機能を追加した製品のことです。XProtectのライセンスファイルは、拡張機能へのアクセスをコントロールします。

XProtectAccessを使用する場合、XProtectシステムでこの機能の使用を許可する基本ライセンスを購入しておく必要があります。また、制御する各ドア用のアクセスコントロールドアライセンスも必要です。

XProtect Accessに対するベンダー固有のプラグインが存在するベンダーの入退室管理システムで、XProtect Accessを使用することができます。

入退室管理統合機能には、XProtectとお客様の入退室管理システムを簡単に統合できる新機能が含まれています。特長:

- XProtect Smart Client内の複数の入退室管理システムを操作できる共通のユーザーインターフェイス。
- 入退室管理システムをより素早く強力に統合
- オペレータ向けに追加された機能(以下を参照) 。

XProtect Smart Clientでは、オペレータは以下の機能を使用できます。

- アクセスポイントでのイベントのライブ監視
- オペレータによるアクセスリクエストの受理
- マップの統合
- 入退室管理イベントのアラーム定義
- アクセスポイントでのイベントの調査
- ドアの状態の一元化された概要とコントロール
- カードホルダー情報と管理

監査ログは、XProtect Smart Clientからの入退室管理システムで各ユーザーが実行するコマンドを記録します。

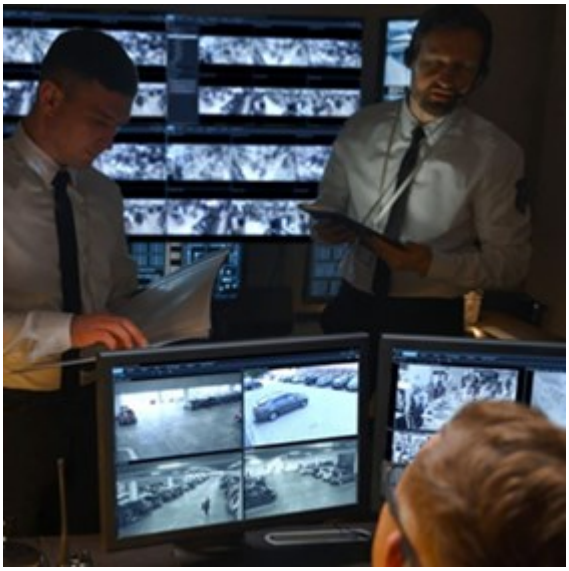
統合を開始するには、XProtect Access基本ライセンス以外にも、ベンダー特有の統合プラグインがイベントサーバーにインストールされている必要があります。

XProtect Incident Manager

Milestoneはさまざまな拡張機能を開発してきました。拡張機能とは、XProtectVMS製品の機能を拡張し、さらに特殊な機能を追加した製品のことです。XProtectのライセンスファイルは、拡張機能へのアクセスをコントロールします。

> 使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

XProtect Incident Managerは、組織がインシデントを文書化したり、XProtectVMSからのシーケンスエビデンス(ビデオ、音声でも可)と組み合わたりすることを可能にする拡張機能です。



XProtectIncidentManagerのユーザーはインシデントプロジェクトのすべてのインシデント情報を保存することが可能です。インシデントプロジェクトから、各インシデントのステータスとアクティビティを追跡することができます。このようにして、ユーザーはインシデントを効果的に管理し、内部的には同僚と、外部的には当局と強力なインシデントのエビデンスを簡単に共有できます。

XProtect Incident Managerは、調査対象の場所で起きているインシデントを概観および理解するのに役立ちます。この知識により、組織は同様のインシデントが今後発生する可能性を最小限に抑えるための手順を実装できます。

XProtect Management Clientでは、組織のXProtect VMSのシステム管理者は、XProtect Incident Managerにおいて使用可能なインシデントプロパティを組織のニーズに合わせて定義することができます。XProtect Smart Clientのオペレータはインシデントプロジェクトを開始、保存、管理し、インシデントプロジェクトにさまざまな情報を追加することができます。これには、フリーテキスト、システム管理者が定義したインシデントプロパティ、およびXProtectVMSからのシーケンスが含まれます。完全なトレーサビリティを実現するために、XProtectVMSは、システム管理者がインシデントプロパティを定義および編集するとき、およびオペレータがインシデントプロジェクトを作成および更新するときにログを記録します。

XProtect LPR(説明付き)

Milestoneはさまざまな拡張機能を開発してきました。拡張機能とは、XProtectVMS製品の機能を拡張し、さらに特殊な機能を追加した製品のことです。XProtectのライセンスファイルは、拡張機能へのアクセスをコントロールします。

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

XProtect LPRは、ビデオベースのコンテンツ分析(VCA)および、監視システムやXProtect Smart Clientでインタラクティブに利用できる車両のナンバープレート認識を提供します。

プレートの文字を読み取るために、XProtect LPRは、特殊なカメラ設定による画像の光学的文字認識を使用します。

ナンバープレート認識(LPR)を、録画やイベントベースの出力の起動などの他の監視機能と組み合わせることもできます。

XProtect LPRでのイベントの例:

- 特定の品質での監視システムによる録画の起動
- アラームの有効化
- ポジティブ/ネガティブなナンバープレート一致リストとの照合
- ゲートを開く
- ライトを点灯
- インシデントのビデオを、特定のセキュリティスタッフメンバーのコンピュータ画面へプッシュ
- 携帯電話へのテキストメッセージ送信

イベントで、XProtect Smart Clientのアラームを有効にできます。

XProtect Smart Wall(説明付き)

XProtect Smart Wallマニュアル。

Milestoneはさまざまな拡張機能を開発してきました。拡張機能とは、XProtectVMS製品の機能を拡張し、さらに特殊な機能を追加した製品のことです。XProtectのライセンスファイルは、拡張機能へのアクセスをコントロールします。

XProtect Smart Wallは、組織特有のセキュリティ要件を満たすビデオウォールを作成することを可能にする、高度な拡張機能です。XProtect Smart Wallは、XProtect VMS[1]システム上のビデオデータすべての概要を提供し、台数や組み合わせを問わず、すべてのモニターをサポートします。

XProtect Smart Wallにより、オペレータは、カメラとモニターのレイアウトの固定セットを使用してシステム管理者によって設定された静的動画を確認できます。ただし、ビデオウォールは、オペレータが表示されるコンテンツをコントロールできるある意味オペレータ主導のウォールです。これには以下が含まれます:

- カメラやその他のタイプのコンテンツ(画像、テキスト、アラーム、スマートマップなど)をビデオウォールにプッシュ中
- ビュー全体をモニターに送信する
- 特定のイベントの過程で、代替プリセット[2]を適用中

まず、ディスプレイの変更は、特定のイベントまたはタイムスケジュールに応じてプリセットを自動変更するルールでコントロールできます。

---

[1]「ビデオマネジメントソフトウェア」の短縮形

[2]XProtect Smart Clientで1台以上のSmart Wallに対して事前に設定したレイアウトプリセットにより、ビデオウォールの各モニターに表示されるカメラとコンテンツのレイアウト(表示構成)が設定されます。

XProtect Transact(説明付き)

Milestoneはさまざまな拡張機能を開発してきました。拡張機能とは、XProtectVMS製品の機能を拡張し、さらに特殊な機能を追加した製品のことです。XProtectのライセンスファイルは、拡張機能へのアクセスをコントロールします。

> 使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

XProtect Transactは、MilestoneのIPビデオ監視ソリューションの拡張機能です。

XProtect Transactは実行中のトランザクションを監視し、過去のトランザクションを調査するためのツールです。トランザクションは、詐欺を証明したり、犯人のエビデンスを提示したりするといった場合、トランザクションを監視するデジタル監視ビデオにリンクされます。トランザクションラインとビデオ画像の間には1対1の関係があります。

トランザクションデータは、さまざまなタイプのトランザクションソースから発生します。一般的には、POSシステムやATMなどです。

Milestone Open Network Bridge(説明付き)

Milestoneはさまざまな拡張機能を開発してきました。拡張機能とは、XProtectVMS製品の機能を拡張し、さらに特殊な機能を追加した製品のことです。XProtectのライセンスファイルは、拡張機能へのアクセスをコントロールします。

Milestone Open Network Bridge は、XProtect VMSシステムから他のIPベースのセキュリティシステムへの標準化されたビデオ共有のためのONVIF規格に準拠したオープンインターフェースです。これにより、警察、監視センター、または類似の組織(以下「ONVIFクライアント」) はXProtect VMSシステムから中央管理されているモニタリングソリューションへのライブビデオと録画ビデオのストリーミングにアクセスできます。ビデオストリームはRTSPストリームとしてインターネット経由で送信されます。

主なメリット:

- 大規模なマルチベンダーのセキュリティの展開と非公開ビデオと公開ビデオのシームレスな統合を実現するため、本格的な相互運用と選択の自由を可能にします
- XProtect VMSシステムで、H.264とH.265のビデオストリーム(ライブビデオと再生の両方) への外部アクセスを提供します
- XProtect VMSソリューションをアラームセンターとモニタリングステーションに統合する簡単かつ問題が生じない方法を提供する標準化されたインターフェースを提供します

このドキュメントは次の内容です。

- ONVIF基準と参考マテリアルへのリンクに関する情報
- XProtect VMS製品におけるMilestone Open Network Bridgeのインストールと構成方法
- 様々なタイプのONVIFクライアントがXProtect VMS製品からライブまた録画ビデオをストリームする方法の例

XProtect DLNA Server(説明付き)

この製品はMilestoneではもうサポートされていません。

Milestoneはさまざまな拡張機能を開発してきました。拡張機能とは、XProtectVMS製品の機能を拡張し、さらに特殊な機能を追加した製品のことです。XProtectのライセンスファイルは、拡張機能へのアクセスをコントロールします。

DLNA (Digital Living Network Alliance) は接続するマルチメディアデバイスの標準です。電子デバイスの製造者はさまざまなベンダーやデバイスの間で相互運用ができるように、そしてビデオのコンテンツを配信できるように、自社製品のDLNA認定を受けます。

一般表示やテレビの内容はDLNA認定を受けており、ネットワークに接続されています。メディアコンテンツのネットワークをスキャンしたり、デバイスに接続したり、メディアストリームが組み込みメディアプレーヤーにリスエストしたりできます。XProtect DLNA Serverは特定のDLNA認定デバイスで検出でき、選択されたカメラからメディアプレーヤー付きDLNA認定デバイスにライブでビデオストリームを配信できます。

DLNAデバイスには、1 ~ 10秒のライブビデオ遅延があります。これはデバイスのバッファサイズが異なることによって引き起こされます。

XProtect DLNA ServerはXProtectシステムと同じネットワークに接続されている必要があり、DLNAデバイスはXProtect DLNA Serverと同じネットワークに接続されている必要があります。

デバイス

ハードウェア(説明付き)

ハードウェアは次のいずれかを表します。

- IP経由で監視システムのレコーディングサーバーに直接接続する物理ユニット(カメラ、ビデオエンコーダー、I/Oモジュールなど) 。
- Milestone Interconnect設定のリモートサイトのレコーディングサーバー。

システム内の各レコーディングサーバーに対して、ハードウェアを追加するための方法は、複数あります。

ハードウェアがNAT対応ルーターまたはファイアウォールの背後にある場合、別のポート番号を指定し、ルーター/ファイアウォールを構成して、ハードウェアのポートとIPアドレスにマッピングされるようにしなければならない場合があります。

ハードウェアを追加ウィザードを使用して、ネットワーク上でカメラおよびビデオエンコーダーなどのハードウェアを検知し、システムのレコーディングサーバーに追加します。ウィザードでは、Milestone Interconnect設定のリモートレコーディングサーバーも追加できます。ハードウェアは、一度に**1つのレコーディングサーバー**にのみ追加してください。

ハードウェアの事前設定 (説明付き)

特定のメーカーは、ハードウェアを初めてVMSシステムに追加する前に新しいハードウェアで資格情報を設定するよう義務付けています。これはハードウェアの事前構成とも呼ばれ、**[ハードウェアデバイスの事前構成]**ウィザードを介して実行されます。このウィザードは、このようなハードウェアが203ページのハードウェアの追加ウィザードで検出された場合に表示されます。

[ハードウェア デバイスの事前設定]ウィザード:

- VMSシステムに追加される前に最初の資格情報が必要なハードウェアは、典型的なデフォルトの資格情報を使用しても追加できません。ウィザードで設定するか、ハードウェアに直接接続して設定する必要があります。
- 資格情報 (ユーザー名またはパスワード) は、**未設定**というマークの付いたフィールドにのみ適用できます
- ハードウェアの**ステータス**が**設定済み**に設定されると、資格情報(ユーザー名またはパスワード)を変更できなくなります。
- 事前設定は新しいハードウェアに適用され、一度だけ実行できます。事前設定後、ハードウェアは、以下の他のハードウェアと同様に管理できます:Management Client
- **[ハードウェアデバイスの事前構成]**ウィザードを閉じると、事前構成されたハードウェアが203ページのハードウェアの追加ウィザードに表示され、システムに追加できるようになります。

> **[ハードウェアデバイスの事前構成]**ウィザードを閉じてから203ページのハードウェアの追加ウィザードを完了させることで、事前構成されたハードウェアにシステムを追加するよう強くお勧めします。Management Clientは、ハードウェアがシステムに追加されなければ、事前設定された資格情報を保持しません。

デバイス(説明付き)

ハードウェアには、以下のように、個別に管理できるデバイスが複数あります。

- 物理カメラには、カメラ部品(レンズ)を表すデバイスおよび、接続型または内蔵型のマイク、スピーカー、メタデータ、入力および出力などのデバイスが付いています
- ビデオエンコーダーには、複数のアナログカメラが接続されており、デバイスのリスト1枚に表示されます。これには、カメラ部品(レンズ)を表すデバイスおよび、接続型または内蔵型のマイク、スピーカー、メタデータ、入力および出力などのデバイスが含まれています
- I/Oモジュールには、ライトなど、入出力チャネルを表すデバイスが付いています
- 音声専用モジュールには、マイクやスピーカーの入出力を表すデバイスが付いています
- Milestone Interconnect設定では、リモートシステムは、リモートシステムからのすべてのデバイスが1つのリストとして表されたハードウェアとして表示されます

ハードウェアを追加すると、ハードウェアのデバイスが自動的に追加されます。

対応ハードウェアについては、MilestoneのWebサイト (https://www.milestonesys.com/support/tools-and-references/supported-devices/) の対応ハードウェアページを参照してください。

以下のセクションでは、追加可能なデバイスタイプについてそれぞれ説明します。

カメラ

カメラデバイスは、ビデオストリームをシステムに送信し、クライアントユーザーはライブビデオビューを使用することができます。あるいは、ビデオストリームをシステムが録画して、クライアントユーザーは後日に再生できます。役割により、ビデオを表示するユーザー権限が決定されます。

マイク

多くのデバイスには、外部マイクを接続できます。マイクが内蔵されているデバイスもあります。

マイクデバイスは、音声ストリームをシステムに送信し、クライアントユーザーはライブ音声として聞くことができます。あるいは、音声ストリームをシステムが録音して、クライアントユーザーは後日に再生できます。関連アクションのトリガー要因となる、マイク特有のイベントを受信するようシステムを設定できます。

役割により、マイクを聞くユーザー権限が決定されます。Management Clientからマイクからの音声を聞くことはできません。

スピーカー

多くのデバイスには、外部スピーカーを接続できます。スピーカーが内蔵されているデバイスもあります。

ユーザーがXProtect Smart Clientの会話ボタンを押すと、システムはスピーカーに音声ストリームを送信します。この機能は、XProtect® MobileとXProtect Web Clientからでも使用できます。スピーカーの音声は、ユーザーがスピーカーに向かって話したときのみ録音されます。役割により、スピーカーを通して話すユーザー権限が決定されます。Management Clientからスピーカーを通して話すことはできません。

2人のユーザーが同時に話す場合は、スピーカーを通して話すユーザー権限は役割によって決定されます。役割の定義の一部として、スピーカーの優先度を「非常に高い」から「非常に低い」まで指定することができます。2人のユーザーが同時に話そうとする場合、優先度が一番高い役割を持つユーザーが話す機能を得ます。同じ役割の2人のユーザーが同時に話そうとする場合、「早く来たものから処理される」原則が適用されます。

メタデータ

メタデータデバイスは、クライアントユーザーがデータに関して参照できるデータストリームをシステムに配信します。たとえば、動画映像を説明するデータ、映像内のコンテンツまたはオブジェクト、または録画された映像の場所を説明することができます。メタデータは、カメラ、マイク、またはスピーカーに添付できます。

メタデータは以下の方法で生成できます。

- 自らデータを配信しているデバイス(ビデオを配信しているカメラなど)
- サードパーティシステムまたは統合で、汎用メタデータドライバーを経由した配信

デバイスで生成されたメタデータは、同じハードウェア上の1つまたは複数のデバイスに自動的にリンクされます。

役割により、ユーザーのメタデータを表示する権限が決定されます。

入力

多くのデバイスには、デバイスの入力ポートに外部ユニットを取り付けることができます。入力ユニットは、通常は外部センサーです。たとえば、ドア、窓、あるいはゲートが開いた場合に、こうした外部センサーを使用して検知することができます。こうした外部入力ユニットからの入力は、システムではイベントとして処理されます。

これらのイベントは、ルールで使用できます。たとえば、入力が有効になるとカメラが録画を開始し、入力が無効になってから30秒経過すると録画を停止するように指定するルールを作成することができます。

出力

多くのデバイスには、デバイスの出力ポートに外部ユニットを取り付けることができます。これによって、システムを通してライト、サイレンなどを有効/無効にすることができます。

出力は、ルールを作成する際に使用できます。出力を自動的に有効または無効にするルール、出力の状態が変化した時にアクションを起動するルールなどを作成できます。

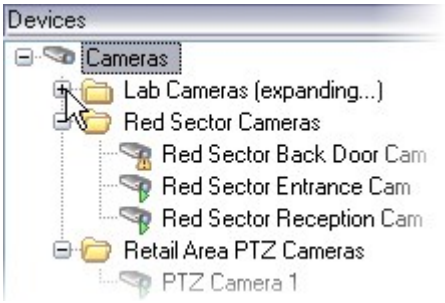
デバイスグループ(説明付き)

デバイスをデバイスグループに分類することは、**ハードウェアの追加**ウィザードの一部ですが、必要に応じていつでもグループを変更し、より多くのグループを追加できます。

システムにある異なる種類のデバイス(カメラ、マイク、スピーカー、メタデータ、入力、および出力)をグループ化すると便利です。

- デバイスグループによって、使用しているシステムのデバイスの概要を直観的に管理できます。
- デバイスは複数のグループに割り振ることができます。
- サブグループを作成したり、サブグループの中にサブグループを作成できます。
- デバイスグループのデバイスには、共通のプロパティを一度に指定することができます。
- グループに設定されたグループプロパティはグループには保存されませんが、個別のデバイスに保存されます。
- 役割を取り扱う場合、デバイスグループのすべてのデバイスに、共通のセキュリティ設定を一度に指定することができます
- 役割を取り扱う場合、デバイスグループのすべてのデバイスに、ルールを一度に適用することができます

必要な数のデバイスグループを追加できますが、異なる種類のデバイスを1つのデバイスグループで混ぜることはできません(例えばカメラとスピーカー)。



すべてのプロパティを表示し、編集できるように、400デバイス**未満**のデバイスグループを作成してください。

デバイスグループを削除すると、デバイスグループ自体のみが削除されます。例えばカメラなどのデバイスをシステムから削除する場合は、レコーディングサーバーレベルで行います。

以下の例では、カメラがデバイスグループに加えられていますが、この原則はあらゆるデバイスに適用されます。

デバイスグループの追加

デバイスグループに含めるデバイスの指定

デバイスグループのすべてのデバイスに対する共通プロパティの指定

メディアストレージ

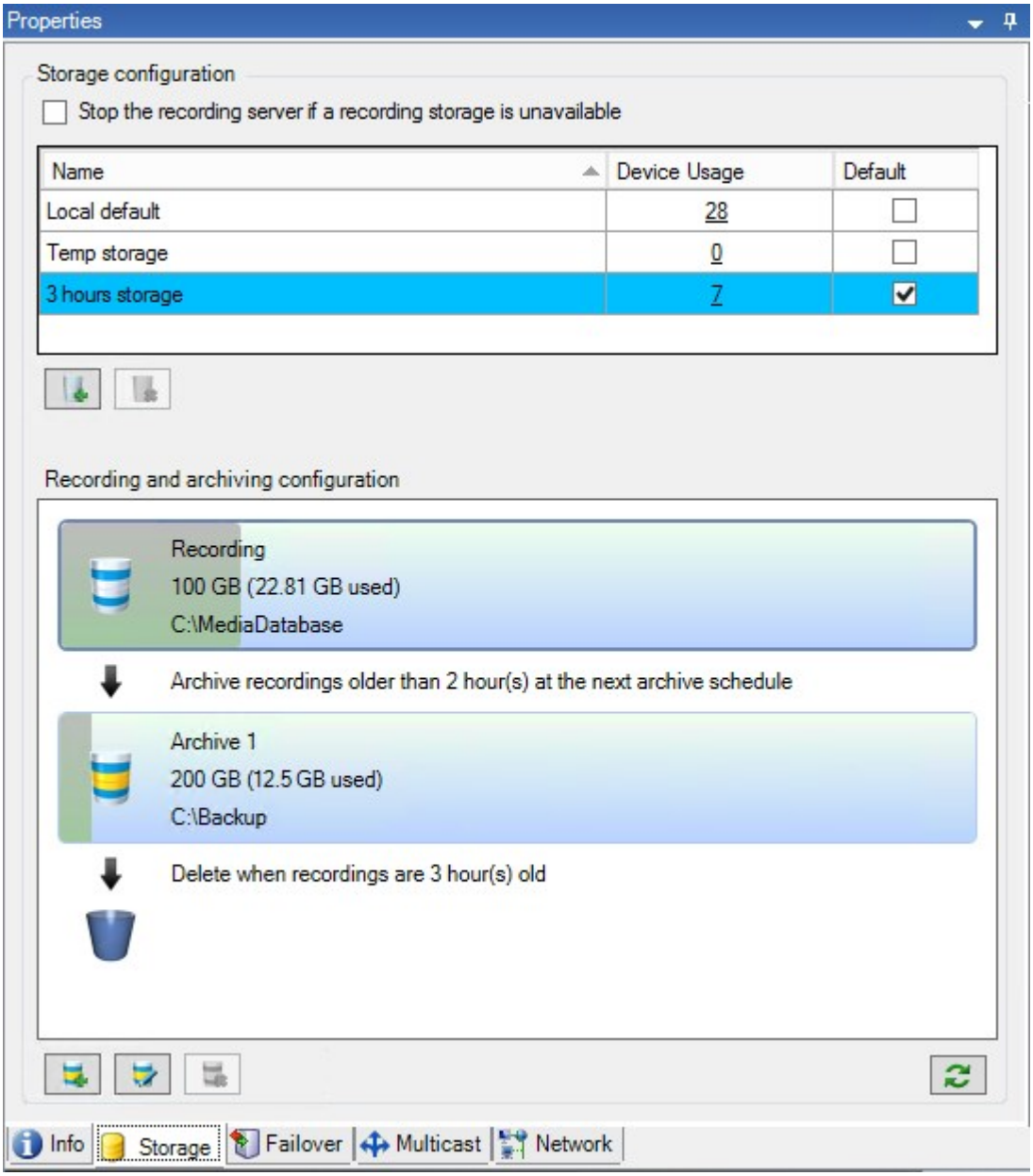
ストレージとアーカイブ(説明)

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

ストレージタブで、選択したレコーディングサーバーのストレージを設定、管理および表示することができます。

録画ストレージとアーカイブでは、横棒は現在の空き容量を示しています。録画ストレージが使用できない場合のレコーディングサーバーの動作を設定することができます。これはほとんどの場合、ご利用のシステムにフェールオーバーサーバーがあるときに関係する設定です。

エビデンスロックを使用している場合、エビデンスロックされた映像に使用される容量を示す縦の赤線があります。



カメラやデバイスがビデオおよび/または音声を録画した場合、すべての指定された録画はデフォルトでそのデバイスに対して定義されているストレージに保存されます。各ストレージは、レコーディングデータベース**レコーディング**内に録画を保存しているレコーティングストレージからなります。ストレージにはデフォルトのアーカイブはありませんが、作成できます。ストレージにはデフォルトのアーカイブはありませんが、作成できます。

レコーディングデータベースがいっぱいになるのを避けるため、追加ストレージを作成できます(「187ページの新しいストレージの追加」を参照)。各ストレージ内でアーカイブを作成し(「188ページのストレージでのアーカイブの作成」を参照)、アーカイブプロセスを開始してデータを保存することも可能です。

アーカイブとは、カメラのレコーディングデータベースから別の場所などへの、録画の自動的な転送です。これにより、保存できる録画データ量は、録画データベースのサイズによって制限を受けません。アーカイブでは、録画を別のメディアにバックアップできます。

ストレージとアーカイブは、レコーディングサーバーごとに設定します。

アーカイブされた録画をローカルまたはアクセス可能なネットワークドライブに保存する限り、XProtect Smart Clientを使用して表示できます。

ディスクドライブが破損してレコーディングストレージが使用できなくなった場合、水平バーが赤に変わります。その場合でもXProtectSmartClientでライブビデオを見ることはできますが、ディスクドライブを復旧するまで録画やアーカイブはできません。システムがフェールオーバーレコーディングサーバーで構成されている場合は、レコーディングサーバーの稼働を停止させてフェイルオーバーサーバーに引き継がせるよう設定できます(「186ページの録画ストレージが利用できない場合の動作を指定」を参照)。

次の点は、一般的にカメラとビデオに該当しますが、スピーカー、マイク、音声、およびサウンドにも適用されます。

Milestoneレコーディングストレージとアーカイブには専用のハードディスクドライブを使用し、ディスクのパフォーマンス低下を防止することをお勧めします。ハードディスクをフォーマットする際は、**アロケーションユニットサイズ**の設定を4 KBから64 KBに変更することが重要です。この変更によって、ハードディスクの録画パフォーマンスが大幅に改善できます。単位サイズの割り当てとヘルプについては、Microsoft社のWebサイト(https://support.microsoft.com/en-us/topic/default-cluster-size-for-ntfs-fat-and-exfat-9772e6f1-e31a-00d7-e18f-73169155af95) を参照してください。

空き容量が5GB未満になった場合、データベースで最も古いデータは必ず自動アーカイブされます(または、次のアーカイブが定義されていない場合は削除されます) 。空き容量が1GB未満になった場合は、データは削除されます。データベースには、必ず250MBの空き容量が必要です。データが十分な速度で削除されないためにこの制限に達すると、データベースへの書き込みが失敗する可能性があり、その場合、十分なスペースを解放するまでデータベースにデータが書き込まれなくなります。このため、データベースの実際の最大サイズは、指定したギガバイト数より5GB少なくなります。

FIPS非準拠暗号で暗号化されている2017 R1よりも前のXProtect VMSのバージョンからのエクスポートとアーカイブ済みメディアデータベースを持つFIPS 140-2準拠システムでは、FIPSを有効にした後でもアクセスできる場所でデータをアーカイブする必要があります。FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、ハードニングガイドのFIPS 140-2準拠セクションを参照してください。

デバイスをストレージに接続する

レコーディングサーバーに対してストレージおよびアーカイブを設定すると、個別のカメラまたはカメラのグループに対してストレージおよびアーカイブを有効にできます。この操作は、個々のデバイス、またはデバイスグループから行えます。188ページの個別のデバイスまたはデバイスのグループをストレージに接続するを参照してください。

効果的なアーカイブ

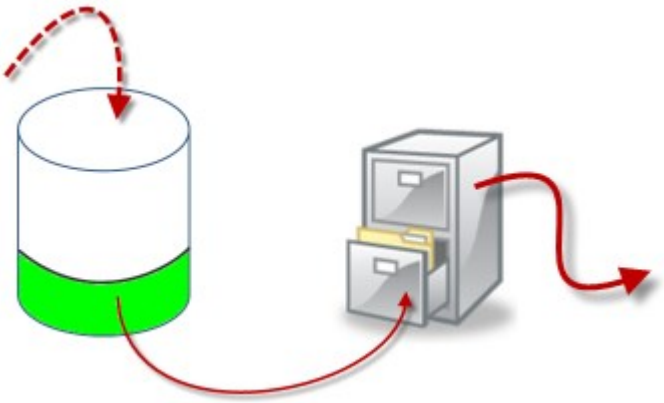
カメラまたはカメラのグループに対してアーカイブが有効であれば、レコーディングストレージの内容は定義した間隔で、自動的に最初のアーカイブへ移動します。

要件によって、それぞれのストレージに対して1つまたは複数のアーカイブを設定することができます。アーカイブは、レコーディングサーバーのコンピュータ、あるいはネットワークドライブなどのシステムが接続できる別の場所に配置することができます。

アーカイブを効果的に設定することで、ストレージのニーズを最適化できます。アーカイブされた録画によって使用される容量をできるだけ少なく抑えることが望ましいことがほとんどです。特に、長期的に考えれば、画像品質を少し下げるだけでも容量の節約に効果があります。レコーディングサーバーの**ストレージ**タブで、次のような相互依存している設定を調整することで効果的にアーカイブを調整することが可能になります。

- レコーディングストレージの保存期間
- レコーディングストレージのサイズ
- アーカイブの保存期間
- アーカイブのサイズ
- アーカイブのスケジュール
- 暗号化
- 秒当たりのフレーム数(FPS)

サイズフィールドは、シリンダー単位での、レコーディングデータベースおよびそのアーカイブのそれぞれのサイズを定義します。



シリンダーにおける空きエリアによって例証される、録画ストレージデータベースの保存期間とサイズの設定で、古い録画をアーカイブするまでの期間を定義します。例の図では、アーカイブするのに充分な期間が経過すると、録画がアーカイブされます。

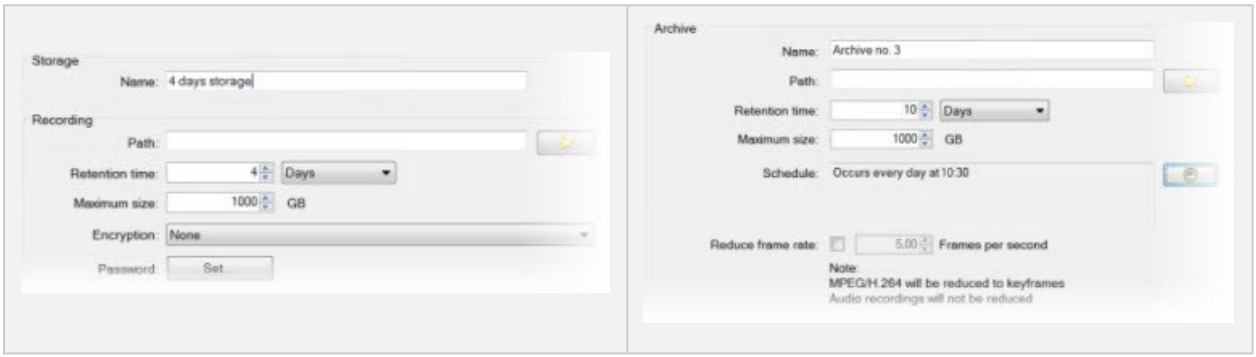
アーカイブの保存期間とサイズ設定は、録画がアーカイブにある期間を定義します。指定した期間、またはアーカイブが指定したサイズ上限に達するまで、録画がアーカイブに保存されます。これらの設定に該当すると、システムはアーカイブにある古い録画を上書きし始めます。

アーカイブのスケジュールによって、アーカイブが行われる頻度や開始時刻が定義されます。

FPSによって、データベースにおけるデータのサイズが決まります。

録画をアーカイブするには、こうしたパラメータをすべて、お互いに調和させながら設定する必要があります。これは、次段のアーカイブの保存時間は、現在のアーカイブまたは録画データベースの保存時間より長くなければならないことを意味しています。アーカイブに対して指定される保存日数には、プロセスで以前に指定されたすべての保存期間が含まれるためです。アーカイブは必ず保存期間より頻繁に行われなければなりません。そうしないとデータを失う恐れがあります。保存時間を24時間と設定した場合、24時間を経過したデータはすべて削除されます。保存時間を24時間と設定した場合、24時間を経過したデータはすべて削除されます。従って、データを確実に次のアーカイブへ移動させるには、24時間毎より頻繁にアーカイブを行う必要があります。

例:以下のストレージ(左の画像)の保存時間は4日であり、以下のアーカイブ(右の画像)の保存時間は10日です。アーカイブは毎日午前10時30分に行われるように設定されているため、必ず保存時間より頻繁にアーカイブが行われます。



ルールとイベントを使用してアーカイブをコントロールすることもできます。

アーカイブ構造(説明付き)

録画をアーカイブすると、アーカイブ内の特定のサブディレクトリ構造に保存されます。

> 全システムの標準的な使用中に、録画がアーカイブされているかどうかにかかわらず、XProtect Smart Clientを使ってすべての録画を参照しているシステムユーザーにとって、サブディレクトリ構造はまったく認識されません。したがって、アーカイブされている録画をバックアップする場合には、サブディレクトリ構造を知ることは非常に重要です。

レコーディングサーバーのそれぞれのアーカイブディレクトリに、個別のサブディレクトリが自動的に作成されます。これらのサブディレクトリには、デバイス名とアーカイブデータベースに基づく名前が付きます。

別のカメラからの録画を同じアーカイブに保存することができ、それぞれのカメラのアーカイブは一定の間隔で実行されるので、サブディレクトリはさらに自動的に追加されます。

これらのサブディレクトリは、それぞれがほぼ1時間の録画を表します。1時間毎に分割することで、アーカイブの最大許容サイズに達した場合でも、アーカイブのデータの比較的小さい部分だけを削除することが可能になります。

サブディレクトリの名前は、録画がエッジストレージかSMTPのいずれによる録画であるかを示すデバイスの名前に続いて、サブディレクトリに含まれている最新のデータベースレコードの日付と時間を**加えた**名前になります。

名前の構造

```
...[Storage Path]\[Storage name]\[device-name] - plus date and time of most
recent recording]\
```

エッジストレージからの場合：

```
...[Storage Path]\[Storage name]\[device-name] (Edge) - plus date and time of
most recent recording]\
```

SMTPからの場合：

```
...[Storage Path]\[Storage name]\[device-name] (SMTP) - plus date and time of
most recent recording]\
```

現実の例

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

サブディレクトリ

さらにサブディレクトリがあれば、自動的に追加されます。これらのサブディレクトリの量と特性は、実際の録画の特性により異なります。たとえば、複数の異なるサブディレクトリは、録画が技術的にシーケンスに分割される場合に追加されます。これは多くの場合、録画を起動するためにモーション検知を使用する場合に当てはまります。

- **メディア**：このフォルダーには、ビデオまたは音声(両方ではない)の実際のメディアが含まれます。
- **MotionLevel**：このフォルダーには、当社のモーション検知アルゴリズムを使用して、ビデオデータから生成したモーションレベルのグリッドが含まれています。このデータで、XProtect Smart Clientのスマートサーチ機能が高速で検索を行うことができます。
- **モーション**：このフォルダーに、システムはモーションのシーケンスを保存します。モーションのシーケンスは、ビデオデータ中でモーションが検知されたタイムスライスです。たとえば、この情報はXProtectSmartClientのタイムラインで使用されます。
- **レコーディング**：このフォルダーに、システムはレコーディングのシーケンスを保存します。レコーディングのシーケンスは、メディアデータで一貫しているレコーディングのタイムスライスです。たとえば、この情報はXProtect Smart Clientでタイムラインを描画するために使用されます。
- **署名**：このフォルダーには、メディアデータ用に生成された署名が含まれています(メディアフォルダーに)。この情報を使用すると、録画された後にメディアデータが改ざんされていないことを確認できます。

アーカイブをバックアップする場合、サブディレクトリ構造の基本を知ることで、正確にバックアップすることが可能になります。

バックアップの例

アーカイブ全体の内容をバックアップする場合、必要なアーカイブディレクトリとその内容のすべてをバックアップします。たとえば、次の下にあるすべてをバックアップします。

```
...F:\OurArchive\
```

特定の期間における特定のカメラからの録画をバックアップする場合は、関連するサブディレクトリの内容だけをバックアップします。たとえば、次の下にあるすべてをバックアップします。

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

録画のプレバッファリングとストレージ(説明付き)

プリバッファは、実際のイベント起動が発生する前に音声およびビデオを記録する機能です。これは、例えばドアが開くなど、記録を起動するイベントにつながる音声またはビデオを記録したい時に便利です。

システムが接続済みのデバイスから継続的に音声およびビデオストリームを受信し、指定済みのプレバッファ期間一時的に保管するので、プレバッファが可能になります。

- 録画ルールが起動されると、ルールとして設定済みプリレコーディング時間に対応する一時レコーディングが恒久的になります
- 録画ルールが起動されないと、プレバッファにある一時レコーディングは、定義されたプレバッファ期間後、自動的に削除されます

一時プレバッファ録画のストレージ

一時プレバッファ録画の保存場所は次のいずれかを選択できます。

- メモリ内。プレバッファ期間は15秒までに制限されます。
- ディスク上(メディアデータベース内)。すべての値を選択できます。

ディスクではなくメモリに保存するとシステムパフォーマンスが向上しますが、プレバッファ期間が短くなります。

録画がメモリに保存され、一時レコーディングの一部を恒久的にすると、その他の一時レコーディングは削除され、復元することはできません。残りの録画を保存できるようにする必要がある場合は、録画をディスク上に保存します。

認証

Active Directory(説明付き)

Active Directoryは、Windowsドメインのネットワーク向けにMicrosoftが実装した分散型ディレクトリサービスです。これは、ほとんどのWindows Serverオペレーティングシステムに搭載されています。このサービスは、ユーザーやアプリケーションがアクセスできるネットワーク上のリソースを識別します。

Active Directoryがインストールされている場合は、Active DirectoryからWindowsユーザーを追加できますが、Active Directoryを使用せずに基本ユーザーを追加することもできます。基本ユーザーについては、特定のシステム制限があります。

ユーザー(説明付き)

ユーザーという用語は、主にクライアントを通じて監視システムに接続するユーザーを意味します。こうしたユーザーは、次の2種類の方法で設定できます。

- **基本ユーザー**として、ユーザー名/パスワードの組み合わせで認証
- **Windowsユーザー**として、Windowsログインに基づく認証。

Windowsユーザー

Active Directoryを使用して、Windowsユーザーを追加します。Active Directory(AD)は、Windowsドメインのネットワーク向けにMicrosoftが実装したディレクトリサービスです。これは、ほとんどのWindows Serverオペレーティングシステムに搭載されています。このサービスは、ユーザーやアプリケーションがアクセスできるネットワーク上のリソースを識別します。Active Directoryは、ユーザーおよびグループの概念を使用します。

ユーザーはActive Directoryのオブジェクトで、ユーザーアカウントを持つ個人を指します。例:

グループは、複数のユーザーを持つActive Directoryオブジェクトです。この例では、管理グループに3人のユーザーがいます:

グループにはユーザーを何人でも含めることができます。グループをシステムに追加すると、1回でメンバー全員を追加できます。グループをシステムに追加した後で、Active Directoryのグループに行った変更は(新規メンバーの追加や旧メンバーの削除など)、すぐにシステムに反映されます。ユーザーは一度に複数のグループに所属できます。

Active Directoryを使用して既存のユーザーとグループの情報をシステムに追加することには以下のようなメリットがあります。

- ユーザーおよびグループはActive Directoryで一元的に指定できるため、システムで最初からユーザーアカウントを作成する必要がなくなります
- Active Directoryで認証を処理しているシステムでは、ユーザーの認証を設定する必要はありません

Active Directoryサービスでユーザーやグループを追加する前に、ネットワーク上でActive Directoryをインストールしたサーバーが必要です。

基本ユーザー

システムからActive Directoryにアクセスできない場合は、基本ユーザーを作成します。基本ユーザーを設定する方法については、「273ページの基本ユーザーの作成」を参照してください。

Identity Provider(説明付き)

Identity Provider app pool (IDP)は、基本ユーザーのID情報を作成、維持、管理するシステムエンティティです。

Identity Providerこの場合、依存するアプリケーションまたはサービスに認証および登録サービスも提供します。記録サーバー、管理サーバー、データコレクター、レポートサーバー。

基本ユーザーとしてXProtectクライアントとサービスにログインすると、リクエストはIdentity Providerに送信されます。認証されると、ユーザーは管理サーバーを呼び出すことができます。

Identity Providerは、別のデータベースを持つ同じSQL Serverを使用するマネジメントサーバーの一部としてIISで実行され、サービスが通信時に使用するOAuth通信トークン(Surveillance_IDP)の作成と処理を行います。

Identity Providerログは次の場所にあります:`\\ProgramData\Milestone\IDP\Logs`

外部IDP(説明済み)

IDPはIdentity Providerの頭字語です。外部IDPは、ユーザーID情報を保存および管理し、他のシステムにユーザー認証サービスを提供できる外部アプリケーションおよびサービスです。外部IDPはXProtectVMSに関連付けることができます。

XProtect VMS は OpenID コネクト(OIDC)に対応した外部IDPをサポートしています。

クレーム(説明付き)

外部IDPとXProtect VMS間をリンクさせるクレーム。

クレームは、ユーザーやアプリケーションが自らのことについて表現する記述です。XProtectのVMSでは、ユーザーのXProtect権限を決定する役割とクレームを関連付けることができます。

クレームは、クレーム名とクレームの値で構成される重要な値です。例えば、クレーム名はクレームの値の内容を説明する標準的な名前である可能性があります。また、クレームの値はグループ名である可能性があります。詳細については、外部IDPからのクレームの例を参照してください。外部IDPからのクレームの例。

外部IDPからXProtect VMSにログインすることを許可する

- 外部IDPから、ユーザーを作成します。また、XProtectVMS、およびXProtectと外部IDP間の相互作用を特定する必要があります。最後に、XProtectVMSでユーザーを外部IDPのユーザーとして識別するためのクレームを作成します。
- XProtect VMSから、Identity Providerが外部IDPにコンタクトするための設定を作成します。外部IDP用の設定を作成する方法の詳細については、外部IDPを追加して設定するを参照してください。

- XProtectのVMSで、外部IDPからのユーザー苦情をXProtectの役割にマッピングして、ユーザーの認証を確立します。苦情を役割にマッピングする方法の詳細については、XProtectで外部IDPからの苦情を役割にマッピングするを参照してください。

リダイレクトURI

リダイレクトURIは、認証に成功した後にユーザーに送るページを指定します。外部IDPで、マネジメントサーバーのアドレスの後に、XProtect Management Clientで定義した**コールバックパス**を追加する必要があります。例えば、https://management-server-computer.company.com/idp/signin-oidc

外部IDPユーザーの固有のユーザー名

外部IDP経由でMilestone XProtectにログインするユーザーに対してユーザー名は自動的に作成されます。

外部IDPは、XProtectのユーザーに対して名前を自動作成するためのクレーム一式を提供します。また、XProtectでは、外部IDPからVMSデータベース上で固有の名前を選択するため、アルゴリズムが使用されます。

外部IDPからのクレームの例

クレーム名とクレームの値で構成されるクレーム。例：

クレーム名	クレームの値
名前	Raz Van
メールアドレス	123@domain.com
amr	パスワード
idp	00o2ghkgazGgi9BIE5d7
preferred_username	321@domain.com
vmsRole	オペレータ
ロケール	en-US
given_name	Raz
family_name	Lindberg
zoneinfo	アメリカ/Los_Angeles
email_verified	真

対象の場所でユーザー名を作成するためクレームのシーケンス番号を使用 - 対象の場所:XProtect

XProtectでは、下の表に示されているクレームのシーケンス番号によって、XProtectのVMS上でユーザーを作成する際の検索優先度が管理されます。XProtectのVMS上では、最初に利用できるクレーム名が使用されます:

クレーム名	シーケンス番号	説明
UserNameClaimType	1	ユーザー名を設定するため1件のクレームを使って設定されたマッピング。クレームは、**ツール > オプション**の**外部IDP**タブにある**ユーザー名の作成に使用するクレーム**フィールドで設定されます。
preferred_username	2	外部IDPから発信できるクレーム。Oidc(OpenID接続)で通常使用される標準的なクレーム。
名前	3	
given_name family_name	4	名と姓の組み合わせ(例えばBob Johnson) 。
メールアドレス	5	
最初に利用できるクレーム + 番号(最初に利用できる番号)	6	例えば、ボブ#1

対象の場所でユーザー名を作成するための特定のクレームを設定中 - 対象の場所:XProtect

XProtectのシステム管理者は、XProtect VMS上でユーザー名の作成に使用すべき外部IDPからの特定のクレームを設定できます。システム管理者がXProtect VMS上でユーザー名の作成に使用するクレームを設定すると、クレーム名が外部IDPからのクレーム名とまったく同じ名前となります。

- ユーザー名に使用するクレームは、**ツール > オプション**の**外部IDP**タブにある**ユーザー名の作成に使用するクレーム**フィールドで設定できます。

外部 IDP ユーザーを削除する

XProtectで外部IDPのログインによって作成されたユーザーは、基本ユーザーと同じ方法で削除できます。作成後であればいつでも削除できます。

XProtectでユーザーが削除され、削除されたユーザーが外部IDPから再びログインすると、XProtectで新規ユーザーが作成されます。ただし、プライベートビューや役割などXProtectでユーザーに関連付けられたデータは失われ、失われた情報はXProtectでユーザーに対して再び作成する必要があります。

Management Clientで外部IDPを削除すると、外部IDPを介してVMSに接続しているすべてのユーザーも削除されます。

セキュリティ

役割と役割の権限(説明付き)

Milestone XProtect VMS のすべてのユーザーは1つの役割に属します。

役割は、ユーザーがアクセスできるデバイスを含むユーザー権限を定義します。また、役割は監視カメラ管理システム内のセキュリティと権限も定義します。

このシステムには、すべてのシステム機能にフルアクセスできるデフォルトの **システム管理者** の役割が付属していますが、ほとんどの場合、ユーザーと必要なアクセス権を区別するために、システムには複数の役割が必要です。必要とする数だけ役割を追加できます。272ページのユーザーおよびグループの役割からの削除、役割への割り当てを参照してください。

たとえば、XProtect Smart Clientのユーザーにアクセスさせたいデバイスに応じて異なるタイプの役割を設定したり、ユーザー間の区別を必要とする同様のタイプの制限を設定したりする必要があるかもしれません。

ユーザー間の差別化を図るために、以下が必要です。

- 組織のビジネスニーズに合わせて必要な役割を作成・設定
- 属するべき役割に割り当てるユーザーとユーザーグループを追加
- Smart Client とManagement Client のユーザーインターフェイスでユーザーが見ることができるものを定義するために、XProtect Smart Client プロファイルとManagement Client プロファイルを作成します。

  役割はアクセス権限を制御するだけで、XProtect Smart Client や Management Clientのユーザーインターフェイスでユーザーが何を見られるかは制御できません。Management Clientを使うことがないユーザーに特定のManagement Client プロファイルを作成する必要はありません。

XProtect Smart Client ユーザーまたは Management Client 機能へのアクセスが制限されているManagement Client ユーザーのユーザーエクスペリエンスを最大限に高めるには、役割によって提供されるアクセス権限と、Smart Client または Management Client プロファイルによって提供されるユーザーインターフェイス要素との間に一貫性を確保するべきです。

> **!** Management Serverにアクセスするために重要なのは、すべての役割が **接続** セキュリティ権限を有効にしていることです。この権限があるのは、**役割設定** > **Management Server** > 479ページのセキュリティ全般タブ(役割) です。

システムで役割を設定するには、**セキュリティ> 役割** を展開します。

役割の権限

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

システムで役割を作成する場合、その役割を関連する役割がアクセスおよび使用できるシステムコンポーネント、または機能への複数権限に割り当てることが可能です。

例えば、XProtect Smart Client または他の Milestone の閲覧クライアントの機能へのアクセス権限のみを持つ役割を作成し、特定のカメラのみを表示する権限を持たせたい場合があります。この種の役割を作成する場合、この種の役割には Management Clientにアクセスする権限や使用する権限を付与するべきではありませんが、XProtect Smart Client または他のクライアントの機能の一部または全部へのアクセス権のみ付与する必要があります。

この差別化ニーズに対応するために、次に、カメラ、サーバー、および同様の機能を追加および削除するための権限など、典型的なシステム管理者権限の一部または大部分を持つ役割を設定します。システム管理者のいくつかの権限またはほぼすべての権限を持つ役割を作成できます。たとえば、これは組織でシステムのサブセットを管理する人と、システム全体を管理する人を分けたい場合などに関連するものです。

役割は、さまざまなシステム機能にアクセス、編集、または変更するための差別化されたシステム管理者権限を提供します。例えば、システムのサーバーまたはカメラの設定を編集する権限です。これらの権限は **セキュリティ全般** タブで指定します (479ページのセキュリティ全般タブ(役割) を参照)。差別化されたシステム管理者がManagement Clientを起動できるようにするには、その役割のためにマネジメントサーバー上の読み取り権限を付与する必要があります。

> Management Serverにアクセスするために重要なのは、すべての役割が **接続** セキュリティ権限を有効にしていることです。この権限があるのは、**役割設定 > Management Server >** 479ページのセキュリティ全般タブ(役割) です。

また、役割とユーザーインターフェースから対応するシステム機能を取り除いたManagement Clientプロファイルを対応させることで、同じ制限をそれぞれの役割に対するManagement Clientのユーザーインターフェースに反映させることもできます。詳細については、「68ページのManagement Clientプロファイル(説明付き) 」を参照してください。

この種の異なる管理者権限を付与する場合、デフォルトのすべての管理者の役割を持つユーザーは、**[セキュリティ] > [役割] > [情報 タブ] > [新規追加]**で役割を設定する必要があります。新しい役割を設定する場合、システムで他の役割を設定したり、システムのデフォルトのプロファイルを使用したりするのと同じように、役割に関連付けられるのは独自のプロファイルだけです。詳細については、「271ページの役割の追加および管理 」を参照してください。

役割を関連付けるプロファイルを指定したら、**セキュリティ全般** タブに移動し、役割の権限を指定します。

> 役割に対して設定できる権限が、製品間で異なります。XProtect Corporateの役割にのみ利用できすすべての権限を付与できます。

プライバシーマスク(説明付き)

プライバシーマスク(説明付き)

プライバシーマスクでは、クライアントで表示する際に、カメラのビデオにおけるどの領域をプライバシーマスクでカバーしたいかを定義することができます。例えば、監視カメラで通りを録画する場合、住民のプライバシーを保護するために、プライバシーマスクを使用して特定の建物(窓やドアなど) の領域を非表示にすることができます。いくつかの国では、これは法的要件になっています。

プライバシーマスクは、不透明またはぼかしを選ぶことができます。マスクは、ライブ、録画、そしてエクスポートされたビデオをカバーします。

プライバシーマスクは、カメラ画像のエリアに適用および固定されます。そのため、カバーされた領域はパン/チルト/ズーム動作を追わず、常にカメライメージと同じ領域をカバーします。いくつかのPTZカメラにおいては、カメラ自体において、位置ベースのプライバシーマスを有効にすることができます。

2種類のプライバシーマスクがあります。

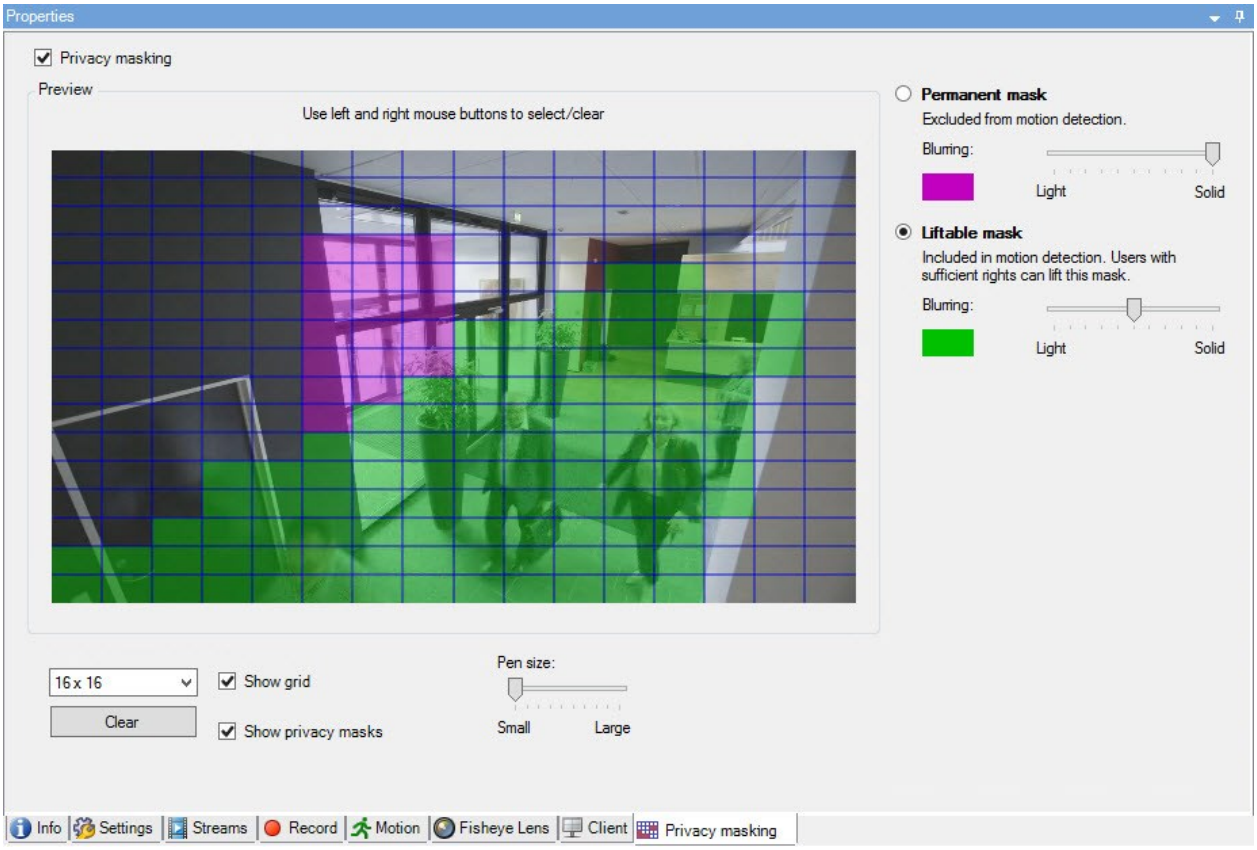
- **常設のプライバシーマスク**: このタイプのマスクがかかった領域は、常にクライアントにおいてカバーされます。公共の場所や、監視カメラが許可されていない場所といった、監視が必ずしも必要とされないビデオの領域をカバーのに使われます。モーション検知は常設のプライバシーマスク領域から除外されます。
- **除去可能なプライバシーマスク**: このタイプのマスクを持つ領域は、プライバシーマスク除去の権限をもつユーザーにより、一時的にXProtect Smart Clientにおけるカバーを外すことができます。ログインしているXProtect Smart Clientユーザーにプライバシーマスクを除去する権限がない場合、システムは権限を持つユーザーに除去の承認を依頼します。プライバシーマスクはタイムアウトまたはユーザーが再適用するまで除去されます。ユーザーがアクセス権を持つすべてのカメラのビデオで、プライバシーマスクが除去されますのでご注意ください。

もしプライバシーマスクが適応された2017 R3システム、あるいはそれより古いバージョンから更新した場合には、マスクは、除去可能なマスクとして移行されます。

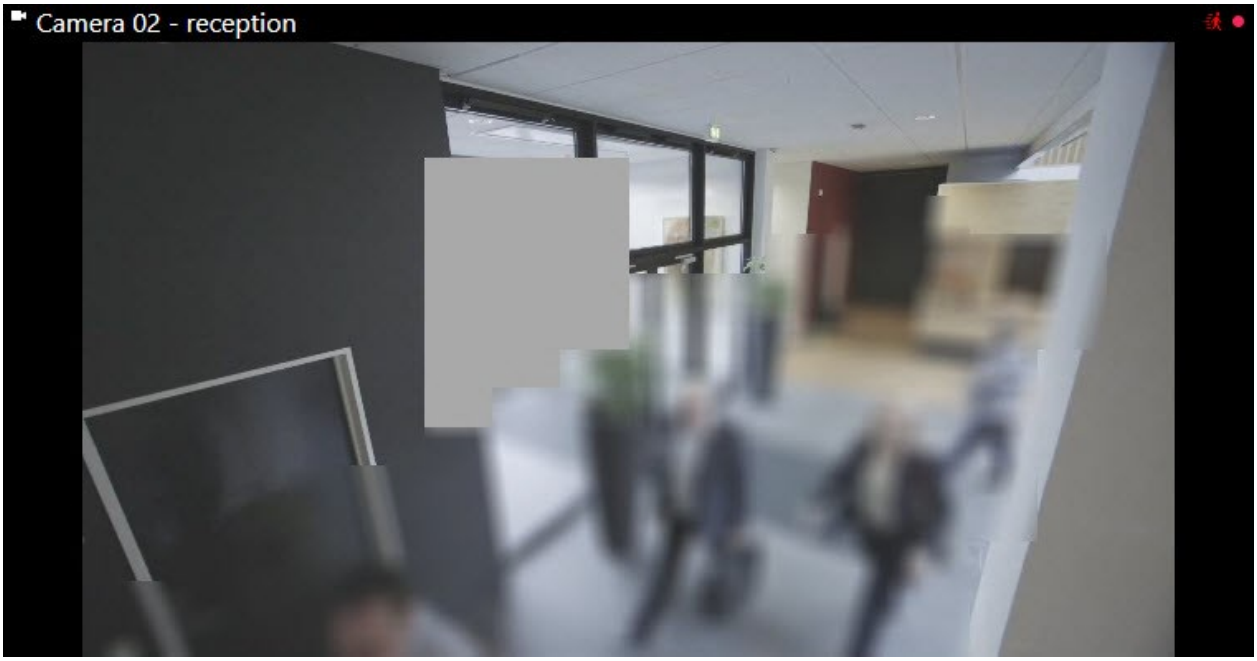
もしユーザーが、録画されたビデオをクライアントからエクスポート、あるいは再生した場合には、ビデオは録画時に設定されていたプライバシーマスクを含みます。それは、録画時より後にプライバシーマスクを変更、あるいは除去しても変わりません。もしプライバシープロテクションがエクスポート時に除去された場合には、エクスポートされたビデオは除去可能なプライバシーマスクを含み**ません**。

もしプライバシーマスク設定を、週に1回といった高い頻度で変更する場合、システムはオーバーロードされる可能性があります。

プライバシーマスク設定を持つ**プライバシーマスク**タブの例:



クライアントには、以下のように表示されます:



クライアントのユーザーに、常設のおよび除去可能なプライバシーマスクについて、通知することができます。

Management Clientプロファイル(説明付き)

Management Clientプロファイルを使用すると、システム管理者は他のユーザーのManagement Clientのユーザーインターフェースを変更できます。Management Clientプロファイルを役割と関連付け、それぞれの管理者役割で使用できる機能が表示されるように、ユーザーインターフェースを制限します。

Management Clientプロファイルは、実際のアクセスではなく、システム機能の視覚的な表示のみに対応します。システム機能への全体的なアクセスは、各ユーザーが関連付けられている役割によって付与されます。特定の役割に関するシステム機能の全体的なアクセスの管理方法については、Management Clientプロファイルの機能表示の管理を参照してください。

すべてのManagement Client要素の表示について、設定を変更できます。デフォルトでは、Management Clientプロファイルはすべての機能をManagement Clientで表示できます。

Smart Client プロファイル(説明付き)

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

Milestone XProtect VMSのすべてのユーザーは、Smart Client プロファイルが接続されている1つの役割に属します。

役割はユーザーの権限を定義し、Smart Client プロファイルはXProtect Smart Client ユーザーインターフェイスで何を見られるかを定義します。

すべてのMilestone XProtect VMSインストールには、組織のシステムで利用可能なほとんどの設定を表示するデフォルト設定のデフォルトSmart Clientプロファイル が含まれます。デフォルトで常に無効になっている設定もあります。

組織内に複数の異なる役割がある場合は、XProtect Smart Client で特定の役割にアクセスできない/アクセスすべきでない機能を無効にすることができます。

例えば、日常業務でビデオの再生を実行する必要がない役割がある場合があります。この目的のために、**再生** モードを無効にする役割のための新しい Smart Client プロファイルを作成することができます。Smart Client プロファイルでこの設定を無効にする場合、Smart Client プロファイルを使う役割があるXProtect Smart Clientユーザーは、XProtect Smart Client ユーザーインターフェイスで **再生** モードを見ることができません。

注意が必要なのは、Smart Client プロファイルが制御するのは主にユーザーが XProtect Smart Client ユーザーインターフェイスで見られるもので、役割の実際のアクセス権限は制御しないということです。読み取り、変更、削除へのアクセスなど、これらのアクセス権限は、役割設定によって制御します。なので、XProtect Smart Client ユーザーは、ユーザーインターフェイスで見られない自分の役割を経由した機能の権限を持つことができます。これは Smart Client プロファイルで無効になっているためです。

XProtect Smart Client ユーザーのユーザーエクスペリエンスを最大限に高めるには、役割によって提供される権限と、Smart Client プロファイルによって提供されるユーザーインターフェイス要素との間に一貫性を確保するべきです。

Smart Client プロファイルを作成または編集するには、**クライアント**を展開し、**Smart Client プロファイル**を選択します。

また、Smart Clientプロファイル、役割、時間プロファイル、およびこれらを同時に使用する方法についての関係を説明しています(249ページのSmart Clientプロファイル、役割、時間プロファイルの作成と設定を参照) 。

エビデンスロック(説明付き)

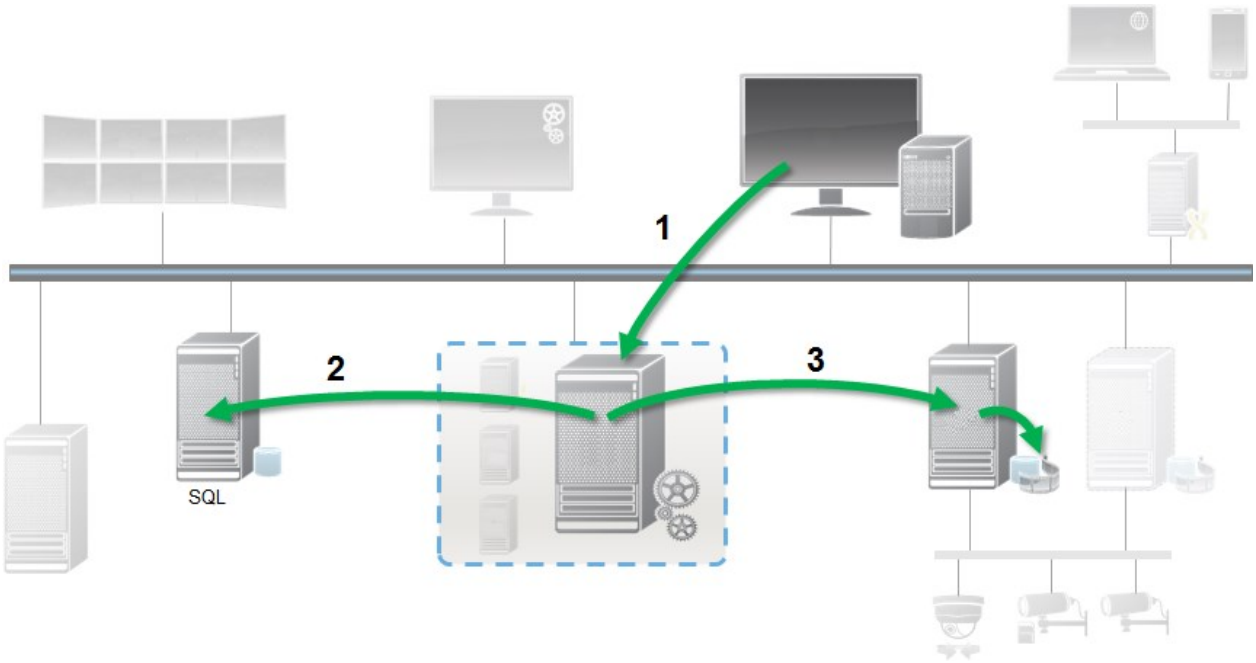
使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

XProtect VMSバージョン2020 R2の時点において、マネジメントサーバーを以前のバージョンからアップグレードしても、バージョン2020 R1またはそれ以前のレコーディングサーバーでのエビデンスロックの作成または修正は、これらのレコーディングサーバーをアップグレードしない限り行うことはできません。これは、ハードウェアが(2020 R1またはそれ以前の) レコーディングサーバーから別のレコーディングサーバーへと移され、以前のサーバーに録画が残っている場合も、エビデンスロックを作成または修正できないことを意味します。

エビデンスロック機能を使用して、クライアントオペレータは、例えば捜査や裁判が行われている間、必要に応じて、音声や他のデータを含むビデオシーケンスが削除されないように保護できます。詳細については、XProtect Smart Clientユーザーマニュアルを参照してください。

保護されている場合、システムのデフォルト保存時間を過ぎた場合の自動削除や、クライアントユーザーによる手動削除によっても、データは削除できなくなります。十分なユーザー権限を持つユーザーによってエビデンスをロックが解除されない限り、システムまたはユーザーはデータを削除できません。

エビデンスロックのフロー図：



1. XProtect Smart Clientのユーザーがエビデンスロックを作成します。情報がマネジメントサーバーに送信されます。
2. Management Serverには、SQL Serverデータベース内のエビデンスロックに関する情報が保存されます。
3. マネジメントサーバーはレコーディングサーバーに対して、データベースの保護された録画を保存して保護するように指示します。

オペレータがエビデンスロックを作成するときには、保護されたデータは録画されたレコーディングストレージにあり、保護されていないデータとともにアーカイブディスクに移動されます。一方、保護されたデータは次のように処理されます。

- エビデンスロックに設定された保持時間。これは無期限になる可能性があります。
- 保護されていないデータにグルーミングが設定されている場合でも、録画の元の品質が維持されます。

オペレータがロックを作成すると、シーケンスの最小サイズは、データベースが録画されたファイルを分割する期間です。デフォルトでは、1時間のシーケンスです。この値は変更できますが、レコーディングサーバーのRecorderConfig.xmlファイルをカスタマイズする必要があります。小さいシーケンスが2つの1時間の期間にまたがる場合は、両方の期間で録画がロックされます。

Management Clientの監査ログでは、ユーザーがエビデンスロックを作成、編集、または削除した日時を確認できます。

ディスクの領域が不足した場合、保護されたデータには影響しません。この場合、最も古い無保護データが削除されます。削除する保護されていないデータがない場合は、システムは録画を停止します。ディスクが満杯のイベントによって起動されるルールとアラームを作成し、自動的に通知を発行することができます。

大量のデータが長期にわたり保存され、ディスク領域に影響する可能性がある場合を除き、このようなエビデンスロック機能はシステムのパフォーマンスに影響しません。

ハードウェアを別のレコーディングサーバーに移動した場合(「323ページのハードウェアの移動」を参照):

- エビデンスロックで保護されている録画は、エビデンスロックの作成時に指定した保存期間にわたって、古いレコーディングサーバーに残されます。
- XProtect Smart Clientのユーザーは引き続き、(別のレコーディングサーバーへと移動される前の) カメラで作成された録画のエビデンスロックを使用してデータを保護できます。カメラを複数回移動する場合でも、録画は複数のレコーディングサーバーに保存されます。

デフォルトでは、オペレータ全員にデフォルトのエビデンスロックプロファイルが割り当てられていますが、この機能に対するユーザーアクセス権限は割り当てられていません。役割のエビデンスロックのアクセス権限を指定するには、「デバイスタブ(役割)」で役割設定について参照してください。役割のエビデンスロックプロファイルを指定する方法については、役割設定の[情報]タブ(役割)を参照してください。

Management Clientでは、デフォルトのエビデンスロックプロファイルのプロパティを編集したり、追加のエビデンスロックプロファイルを作成して、これらを役割に割り当てたりすることができます。

ルールとイベント

ルール(説明付き)

ルールは特定の条件下でどのようなアクションをするかを指定します。例:モーションが検知されたら(条件)、カメラが録画(アクション)を開始。

以下はルールでできることの**例**です。

- 録画を開始および停止する
- デフォルト以外のライブフレームレートを設定する
- デフォルト以外のレコーディングフレームレートを設定する
- PTZパトロールを開始および停止する
- PTZパトロールを一時停止および再開する
- PTZカメラを特定の位置に移動する
- 出力を有効/無効状態に設定する
- Eメールで通知を送信する
- ログエントリを生成する
- イベントを生成する
- 新しいデバイス設定を適用する(例:カメラの解像度の変更)
- ビデオがMatrix受信者に見えるようにする
- プラグインを開始および停止する
- デバイスからのフィードを開始および停止する

デバイスを停止することは、ビデオがデバイスからシステムに転送されなくなり、ライブビデオの視聴もビデオ録画もできなくなることを意味します。一方、フィードを停止したデバイスは、レコーディングサーバーとの通信が維持されます。また、Management Clientでデバイスを手動で無効にしたときとは異なり、デバイスからのフィードはルールにより自動的に開始することが可能です。

> ルールの中には、特定の機能が関連するデバイスで有効であることが要件となるものもあります。例えば、カメラによる録画を指定するルールは、関連するカメラで録画が有効になっていないと機能しません。Milestoneは、ルールを作成する前に、関連するデバイスが正しく動作するか確認しておくことを推奨しています。

ルールの複雑さ

正確なオプションの数は、作成するルールのタイプ、およびシステムで使用できるデバイスの数により異なります。ルールによって高度な柔軟性が実現します。イベントと時間条件を組み合わせることはもちろん、複数の操作を1つのルールに指定することや、システム上の一部またはすべてのデバイスを対象とするルールを作成することもできます。

必要に応じて、単純または複雑なルールを作成することができます。例えば、非常に単純な時間ベースのルールを作成できます。

例	説明
非常に単純な時間ベースのルール	月曜日08:30から11:30(時間条件)に、カメラ1とカメラ2が録画を開始(アクション)し、期間が終了したら録画を停止(アクション停止)する。
非常に単純なイベントベースのルール	カメラ1でモーションが検出されたら(イベント条件)、カメラ1が直ちに録画を開始し(アクション)、10秒後に録画を停止する(アクション停止)。 イベントベースのルールは、1個のデバイスの1つのイベントで実行されますが、2つ以上のデバイスでアクションが実行されるように指定することもできます。
複数のデバイスを使用するルール	カメラ1でモーションが検知されたら(イベント条件)、カメラ2が直ちに録画を開始し(アクション)、出力3に接続されたサイレンが直ちに鳴る(アクション)。その60秒後に、カメラ2が録画を停止し(アクション停止)、出力3に接続されたサイレンが鳴り止む(アクション停止)。
時間、イベント、デバイスを組み合わせたルール	カメラ1でモーションが検知されたら(イベント条件)、曜日が土曜日または日曜日の場合(時間条件)、カメラ1とカメラ2が直ちに録画を開始し(アクション)、セキュリティマネージャーに通知が送信される(アクション)。カメラ1またはカメラ2でモーションが検知されなくなってから5秒後に、2台のカメラは録画を停止する(アクション停止)。

組織の要件に応じて異なりますが、複雑なルールを作成するよりも、単純なルールを複数作成することをお奨めします。もしこれにより、システムにより多くのルールが存在することになっても、ルールで実行されることの概要を簡単に保存することができます。ルールを単純に保つことで、個別のルール要素を無効/有効にするときに、柔軟性を得ることができます。単純なルールであれば、必要に応じてルール全体を無効/有効にできます。

ルールとイベント(説明付き)

ルールは、システムの中心的な要素です。ルールは、非常に重要な設定を決定します。例えばカメラの録画開始、PTZカメラのパトロール開始、通知送信を開始するタイミングなどです。

例:モーションを検知したときに特定のカメラで録画を開始するよう指定したルール

イベントは**ルールの管理**ウィザードを使用する時の中心的な要素です。ウィザードでは、イベントはアクションをトリガーするために主に使用されます。例えば、モーションを検知した場合(**イベント**)に、監視システムが特定のカメラからのビデオの録画を開始するという**アクション**を取ることを指定するルールを作成することができます。

ルールは以下の2種類の条件によってトリガーされます。

名前	説明
イベント	イベントが監視システムで発生した場合(例えば、モーションを検知した時、あるいはシステムが外部センサーから入力を受信した時)。
タイムインターバル	特定の時間を入力した場合(例えば、 `Thursday 16th August 2007 from 07.00 to 07.59` または`every Saturday and Sunday`)
フェールオーバータイムインターバル	フェールオーバーが有効または無効な時間。
繰り返し時間	詳細な定期スケジュールでは、アクションをどの時点で実行するかを設定できます。 例: • 毎週火曜日の15:00 ~ 15:30の間に1時間おきに実行 • 3か月ごとにその月の15日の11:45に実行

名前	説明
	• 毎日15:00 ~ 19:00の間に1時間おきに実行 時刻は、Management Clientがインストールされているサーバーのローカル時刻設定に基づいています。

ルールとイベントで以下を使用できます。

- **ルール**: ルールは、システムの中心的な要素です。監視システムの動作の大半が、ルールにより決定されます。ルールを作成する際には、すべてのタイプのイベントを使用できます
- **時間プロファイル**: 時間プロファイルは、Management Clientで定義する期間です。これは、Management Clientでルールを作成する際に使用することができます。例えば、特定のアクションが特定の時間プロファイル内で発生するよう指定するルールを作成するために使用できます
- **通知プロファイル**: 通知プロファイルを使用して、定義済みのEメールによる通知を設定することができます。通知は、例えば特定のイベントが発生した時など、ルールによって自動的にトリガーされます。
- **ユーザー定義イベント**: ユーザー定義イベントは、カスタムメイドのイベントであり、ユーザーがシステムで手動でイベントをトリガーしたり、システムからの入力に応答することが可能になります
- **アナリティクスイベント**: アナリティクスイベントは、外部のサードパーティーのビデオコンテンツ分析(VCA)プロバイダーから受信するデータです。アナリティクスイベントはアラームの条件として使用できます
- **ジェネリックイベント**: ジェネリックイベントでは、単純な文字列をIPネットワーク経由でシステムに送信し、XProtectイベントサーバーのアクションをトリガーできます

時間プロファイル(説明付き)

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

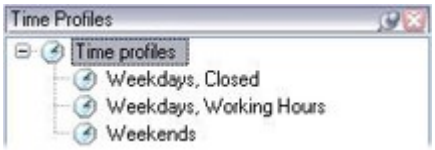
時間プロファイルは、管理者が定義する期間です。時間プロファイルは、ルール作成時に使用できます。例えば、特定のアクションが特定の期間内に発生することを指定するルールを作成するときなどです。

時間プロファイルは、SmartClientプロファイルだけでなく、役割にも割り当てられます。デフォルトでは、すべての役割はデフォルトの時間プロファイルである**常時**に割り当てられます。つまり、このデフォルトの時間プロファイルが設定された役割のメンバーには、システムにおいてユーザー権限に時間ベースの制限がありません。別の時間プロファイルを役割に割り当てることも可能です。

時間プロファイルは非常に柔軟です: 1つまたは複数の単一期間、1つまたは複数の繰り返し期間、あるいはそれらの組み合わせにより構成することができます。多くのユーザーは、Microsoft® Outlookのようなカレンダーアプリケーションでの単発や繰り返し期間のコンセプトに慣れています。

時間プロファイルは常に現地時間で適用されます。つまり、システムが異なるタイムゾーンにレコーディングサーバーを有している場合、時間プロファイルに関連するアクション(カメラの録画等) は、各レコーディングサーバーの現地時間に基づき実行されます。例 : 08:30 ~ 09:30の時間帯をカバーする時間プロファイルを使用する場合、ニューヨークにあるレコーディングサーバーのアクションは、現地時間08:30 ~ 09:30に実行され、ロサンゼルスにあるサーバーは、ロサンゼルスの現地時間が08:30 ~ 09:30になったときに遅れて実行されます。

ルールとイベント > **時間プロファイル**を展開することで、時間プロファイルを作成して管理できます。**時間プロファイル**リストが開きます。例 :



時間プロファイルに代わるものとして、日中時間プロファイル(説明付き) を参照してください。

日中時間プロファイル(説明付き)

カメラを屋外に設置した場合、カメラの解像度を頻繁に下げたり、黒/白を有効にしたり、暗くなったり明るくなったりした場合に他の設定を変更する必要があります。カメラの位置が赤道から離れるほど、日の出と日没の時間が1年間のうちで大きく変化します。このため、通常の固定の時間プロファイルを使用して、明るさに応じたカメラ設定の調整はできなくなります。

このような状況では、日中時間プロファイルを作成して、特定の地理的地域での日の出と日没を定義することができます。地理的座標を使用することで日の出と日没の時刻が算出されるほか、該当する場合は日々のサマータイムの調整も組み込まれます。その結果、時間プロファイルが選択した場所の日の出/日没の年間の変化を自動的に追跡し、必要な時だけプロファイルが有効になるようにします。日時はすべてマネジメントサーバーの日時設定に基づきます。また、開始時刻(日の出) と終了時刻(日没) のプラスまたはマイナスオフセット(分単位) を設定することも可能です。開始と終了のオフセットは、同じまたは別にすることができます。

日中時間プロファイルは、ルールと役割の両方を作成するときに使用できます。

通知プロファイル(説明付き)

通知プロファイルで、定義済みのEメールによる通知を設定することができます。通知は、ルールによって(例えば特定のイベントが発生したとき) 自動的にトリガーされます。

通知プロファイルの作成時には、メッセージテキストを指定するほか、静止画像とAVIビデオクリップをメール通知に含めたいかどうかを指定します。

> また、Eメールスキャナがある場合、Eメールによる通知を送信するアプリケーションを妨害する可能性があるため、これを無効にする必要があります。

通知プロファイル作成の要件

通知プロファイルを作成する前に、Eメールによる通知のメールサーバー設定を指定する必要があります。

メールサーバーに必要なセキュリティ証明書がインストールされていれば、メールサーバーと安全に通信できます。

Eメールによる通知にAVIムービークリップを含めるには、まず圧縮設定を指定する必要があります。

1. **ツール > オプション**に移動します。これにより、**オプション**ウィンドウが開きます。
2. メールサーバーを**メールサーバー**タブ(「368ページのメールサーバータブ(オプション)」を参照)で設定し、圧縮設定を**AVI生成**タブ(「369ページのAVI生成タブ(オプション)」を参照)で行います。

ユーザー定義のイベント(説明付き)

目的のイベントが**イベント概要**リストにない場合は、ユーザー定義イベントを作成できます。このようなユーザー定義のイベントを使用して、他のシステムを監視システムに統合します。

ユーザー定義イベントを使用すると、サードパーティー製のアクセスコントロールシステムから受信したデータをシステム内でイベントとして使用できます。イベントは後でアクションを起動できます。例えば、誰かが建物に入ったときに、該当するカメラからビデオ記録を開始できます。

また、ユーザー定義イベントを使用すると、XProtect Smart Clientのライブビデオを表示しているときに手動でイベントを起動したり、ルールで使用されている場合は自動的にイベントを起動できます。例えば、ユーザー定義イベント37が発生すると、PTZカメラ224がパトロールを停止して、プリセット位置18に移動します。

役割を通して、どのユーザーがユーザー定義イベントを起動できるかを定義できます。ユーザー定義イベントを2つの方法で使用し、必要な場合は同時に使用できます。

イベント	説明
XProtect Smart Clientで手動でイベントを起動できるようにする方法	この場合、エンドユーザーが手動でイベントを起動しながら、のライブビデオを閲覧することができますXProtect Smart Client。XProtect Smart Clientのユーザーにより手動で起動されたためにユーザー定義イベントが発生すると、ルールによりシステムで行うべき1つまたは複数のアクションが起動されます。
APIを通してイベントを起動できるようにする方法	この場合、監視システムの外のユーザー定義イベントを起動できます。この方法でユーザー定義イベントを使用するには、ユーザー定義イベントを起動する際に、個別のAPI(アプリケーションプログラムインターフェース。ソフトウェアアプリケーションの作成またはカスタマイズに必要な構築ブロックのセット)が必要です。この方法でユーザー定義イベントを使用するには、Active Directoryからの認証が必要です。これにより、ユーザー定義イベントが監視システムの外側から起動可能にも関わらず、認証されたユーザーのみが実行可能となります。 また、ユーザー定義イベントは、APIよりメタデータに関連付けし、特定のデバイスまたはデバイスグループを定義することができます。これは、ユーザー定義のイベントを使用してルールを起動する際に非常に便利です。それぞれのデバイスに対するルールを持つことを避けるのと、基

イベント	説明
	本的に同じことを行います。例：ある企業には出入り口が35箇所あり、アクセスコントロールを使用しており、それぞれにアクセスコントロールデバイスがあります。アクセスコントロールデバイスを有効にすると、システムでユーザー定義イベントが起動されます。このユーザー定義イベントをルールで使用して、有効なアクセスコントロールデバイスに関連するカメラで録画を開始することができます。どのカメラがどのルールに関連付けられるかは、メタデータで定義されます。この方法により、企業は35個のユーザー定義イベントと35個のユーザー定義イベントで起動されたルールを作成する必要がなくなります。単一のユーザー定義イベントと、単一のルールで十分な管理が可能になります。 ユーザー定義イベントをこの方法で使用する場合、XProtect Smart Clientの手動起動で常に使用できるようにしておきたくない場合もあるでしょう。役割を使用して、どのユーザー定義イベントがXProtect Smart Clientに表示されるか決定することができます。

アナリティクスイベント(説明付き)

典型的なアナリティクスイベントは、外部のサードパーティーのビデオコンテンツ分析(VCA)プロバイダーから受け取るデータです。

基本的に、アナリティクスイベントに基づいてアラームを使用する場合には、3段階のプロセスがあります。

- 1. アナリティクスイベント機能を有効にし、セキュリティを設定します。許可されたアドレスのリストを使用して、イベントデータをシステムに送信できるユーザーおよびサーバーがリスンするポートをコントロールできます。
- 2. イベントの説明などを使用してアナリティクスイベントを作成し、テストします。
- 3. アラーム定義のソースとしてアナリティクスイベントを使用します。

サイトナビゲーションペインの**ルールとイベント**リストでアナリティクスイベントを設定します。

VCAベースのイベントを使用するには、データをシステムに配信するために、サードパーティー製のVCAツールが必要です。ユーザーの選択した任意のVCAツールを使用できます。ただし、ツールが配信するデータは、指定されたフォーマットに準拠していなければなりません。このフォーマットについては、アナリティクスイベントに関するMIP SDKマニュアルで説明されています。

詳細はシステムプロバイダーにお問い合わせください。サードパーティー製のVCAツールは、Milestoneオープンプラットフォームに基づいてソリューションを提供する独立系パートナーによって開発されています。これらのソリューションは、システムのパフォーマンスに影響する場合があります。

ジェネリックイベント(説明付き)

ジェネリックイベントでは、単純な文字列をIPネットワーク経由でシステムに送信し、XProtectイベントサーバーのアクションをトリガーできます。

TCPまたはUDPを使用して文字列を送信できるハードウェアまたはソフトウェアを使用して、ジェネリックイベントをトリガーできます。システムは、受信したTCPまたはUDPデータパッケージを分析して、特定の基準が満たされたときに、ジェネリックイベントを自動的にトリガーします。この方法で、システムと、例えば入退室管理システムやアラームシステム等の外部ソースを統合することができます。目的は、可能な限り多くの外部ソースがシステムと相互作用できるようにすることです。

データソースのコンセプトにより、サードパーティー製ツールでシステムの基準を満たす必要がなくなります。データソースを使用して、指定したIPポートで特定のハードウェアまたはソフトウェアと通信し、そのポートに達するバイトの解釈方法を微調整することが可能になります。各ジェネリックイベントタイプは、データソースとペアになり、特定のハードウェアまたはソフトウェアとの通信に使用される言語を構成します。

データソースを使用する場合、IPネットワークの一般的知識およびインターフェイスを使用する個別のハードウェアまたはソフトウェアの知識が必要となります。使用できるパラメータは多数あり、実行方法はあらかじめ決められていません。基本的に、システムはツールを提供しますが、ソリューションは提供しません。ユーザー定義イベントとは異なり、ジェネリックイベントには認証がありません。これによって簡単に起動ができますが、安全性を損なわないように、ローカルホストからのイベントのみが許可されます。**オプション**メニューの**ジェネリックイベント**タブから、その他のクライアントIPアドレスも許可できます。

Webhook(説明付き)

Webhookは、Webアプリケーションが相互に通信を有効にするHTTPリクエストであり、例えば、ユーザーがシステムにログオンしたときやカメラがエラーを報告したときに、事前に定義されたWebhookエンドポイントにイベントデータを送信するなど、あらかじめ定義されたイベントが発生した際に、あるアプリケーションから別のアプリケーションにリアルタイムでデータを送信することを容易にします。

Webhookのエンドポイント(Webhook URL)は、イベントデータの送信先となる事前に定義されたアドレスで、ワンウェイ方式の電話番号とよく似ています。

Webhookを使用して、選択したイベントを定期受信する統合機能を構築できますXProtect。あるイベントがトリガーになり、イベントに定義しているWebhookエンドポイントにHTTP POSTが送信されます。HTTP POST本文には、JSON(JavaScript Object Notation[JavaScriptのオブジェクト表記法])形式のイベントデータが含まれます。

Webhookはデータやトリガーされたイベントについてシステムをポーリングしませんが、その代わりに、イベントが発生した際は、システムがイベントデータをWebhookエンドポイントにプッシュするため、ポーリングソリューションと比較してWebhookのリソース要求が少なく、設定がより高速になります。

Webhookは、コードスクリプトを使用してもしなくても、設定して統合が可能です。

> ⚠ 送信元のイベントデータが、自国の既存データおよび個人情報保護法にXProtect準拠していることを確認してください。

Webhook機能は、XProtect 2023R1以降にデフォルトでインストールされており、すぐに利用できます。Management Clientの**ルール**タブに**Webhook**アクションが表示されます。

アラーム

アラーム(説明付き)

この機能は、XProtect Event Serverがインストールされている場合のみ機能します。

この記事では、イベントによって起動されるアラームがシステムに表示されるよう設定する方法について説明します。

イベントサーバーで処理される機能に基づくアラーム機能により、組織全体の任意のインストール数(他のXProtectシステムも含む)で、一元的なアラームの確認、コントロール、およびアラームの拡張性が得られます。以下のいずれかに基づきアラームが生成されるように設定できます。

- **内部システム関連のイベント**

  例:モーション、サーバーの応答/非応答、アーカイブの問題、ディスク空き容量不足など。

- **外部統合イベント**

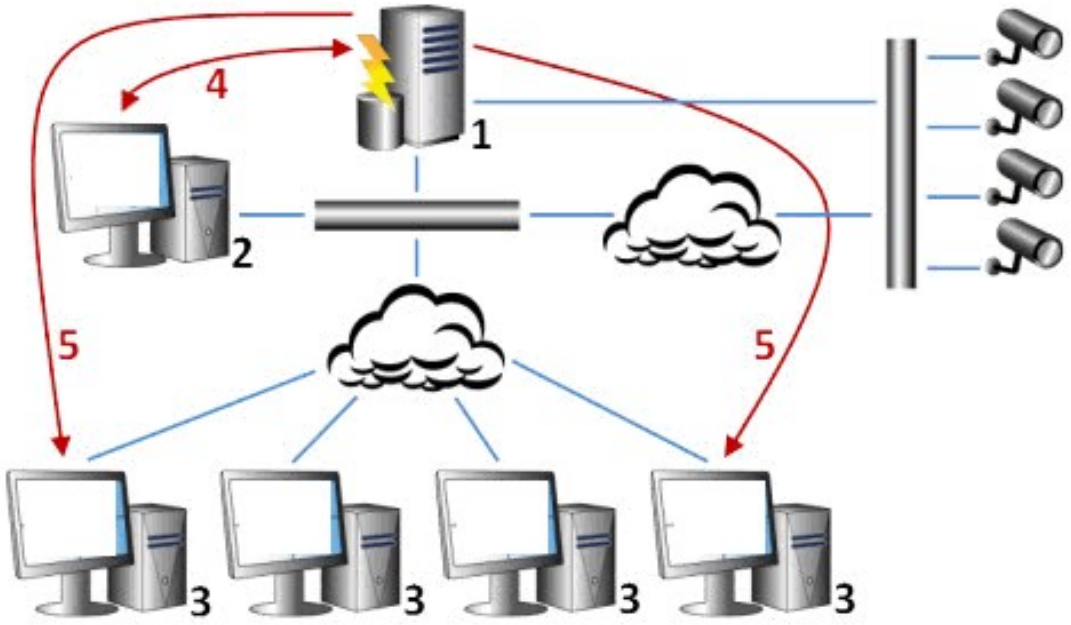
  このグループは、複数のタイプの外部イベントで構成されています。

  - **アナリティクスイベント**

    典型的には、外部のサードパーティーのビデオコンテンツ分析(VCA)プロバイダから受け取ったデータ。

  - **MIPプラグインイベント**

    MIP SDKによって、サードパーティーのベンダーは、システムのカスタムプラグイン(例:外部アクセスコントロールシステムまたは同様の機能などとの統合)を開発できます。



凡例:

1. 監視システム
2. Management Client
3. XProtect Smart Client
4. アラーム設定
5. アラームデータのフロー

アラームを処理し、XProtect Smart Clientにあるアラームリストに割り当てます。アラームはXProtect Smart Clientのスマートマップおよびマップ機能とも統合できます。

アラーム設定

アラーム設定には以下が含まれます。

- アラーム処理の動的役割ベース設定
- すべてのコンポーネントの一元的技術概要：サーバー、カメラ、および外部ユニット
- すべての受信アラームとシステム情報の一元的ログ設定
- プラグインの処理、外部アクセスコントロールまたはVCAベースシステムなどの他のシステムとのカスタム統合が可能です。

一般的に、アラームを発生させるオブジェクトの視認性によりアラームが制御されます。これは、制御/管理するユーザーと、制御/管理の度合いについて、アラームの4つの側面が役割を担っていることを意味します。

名前	説明
ソース/デバイス視認性。	アラームを発生させるデバイスが、ユーザーの役割で視認できるように設定されていない場合、ユーザーはXProtect Smart Clientのアラームリストのアラームを確認することはできません。
ユーザー定義イベントをトリガーする権限	この権限は、ユーザーの役割がXProtect Smart Clientで選択したユーザー定義システムをトリガーできるかどうかを決定します。
外部プラグイン	システムで外部プラグインが設定されている場合、それがアラームを処理するユーザー権限を制御する可能性があります。
一般的役割権限	ユーザーがアラームを表示できるだけか、あるいはアラームを管理できるかを決定します。 **アラーム**のユーザーがアラームについてできる操作は、ユーザーの役割とその役割の設定により異なります。

オプションの**アラームとイベント**タブで、アラーム、イベント、ログの設定を指定できます。

スマートマップ

スマートマップ(説明付き)

XProtect® Smart ClientとXProtect Mobileでは、スマートマップの機能を使用すると、地理的に正確な方法で世界各地の複数の場所にあるデバイスを表示したり、アクセスできます。ロケーションごとに異なるマップを使用する代わりに、スマートマップではひとつのビューで全体像を把握することができます。

スマートマップ機能の以下の設定はManagement Clientで行われます。

- スマートマップで選択可能な地理的背景を設定します。これには、スマートマップと以下のサービスのいずれかとの統合が含まれます。
    - Bing Maps
    - Google Maps
    - Milestone Map Service
    - OpenStreetMap
- XProtect Management ClientまたはXProtect Smart ClientでBing MapsまたはGoogle Mapsを有効にする
- XProtect Smart Clientでスマートマップの編集を有効にする(デバイスを含む)
- XProtect Management Clientでデバイスを配置する
- Milestone Federated Architectureでスマートマップを設定する

スマートマップとGoogle Mapsの統合(説明付き)

お使いのスマートマップにGoogle Mapsを埋め込むには、GoogleからMaps Static APIキーを取得する必要があります。APIキーを取得するには、最初にGoogle Cloud請求先アカウントを作成する必要があります。これにより、毎月読み込んだマップの量に応じて請求が行われます。

APIキーを入手した後、これをXProtect Management Clientに入力してください。「305ページのManagement ClientでBing MapsまたはGoogle Mapsを有効化」も参照してください。

制限されたファイアウォールがある場合は、中古ドメインへのアクセスを許可することが重要です。Smart Clientを実行している各マシンでmaps.googleapis.comを使用したGoogle Mapsの発信トラフィックを許可する必要がある場合があります。

詳細については以下を参照してください:

- Google Maps Platform - はじめに: https://cloud.google.com/maps-platform/
- Google Mapsプラットフォーム請求ガイド: https://developers.google.com/maps/billing/gmp-billing
- Maps Static API開発者ガイド: https://developers.google.com/maps/documentation/maps-static/dev-guide

デジタル署名をMaps Static APキーに追加

XProtect Smart Clientオペレータが1日に25,000以上のマップをリクエストすると予想される場合は、Maps Static APIキーにデジタル署名が必要になります。デジタル署名を使うと、Googleサーバーは、あなたのAPIキーを使用してリクエストを行っているサイトにその許可があることを確認できます。ただし、使用要件に関わらず、Googleは追加セキュリティレイヤーとしてデジタル署名を使用するよう推奨しています。デジタル署名を入手するには、URL署名シークレットを取得する必要があります。詳細については、「https://developers.google.com/maps/documentation/maps-static/get-api-key#dig-sig-manual」を参照してください。

スマートマップとBing Mapsの統合(説明付き)

Bing Mapsをお使いのスマートマップに埋め込むには、ベーシックキーまたはエンタープライズキーが必要です。これらの相違点として、ベーシックキーは無料ですが、トランザクションの数に制限が設けられています。この制限を超えると、トランザクションに対して請求が行われるか、マップサービスが拒否されるようになります。エンタープライズキーは有料ですが、トランザクションを無制限に実行できます。

Bing Mapsの詳細については、https://www.microsoft.com/en-us/maps/licensing/を参照してください。

APIキーを入手した後、これをXProtect Management Clientに入力してください。305ページのManagement ClientでBing MapsまたはGoogle Mapsを有効化を参照してください。

制限されたファイアウォールがある場合は、中古ドメインへのアクセスを許可することが重要です。Smart Clientを実行している各マシンで、*.virtualearth.netを使用したBingマップの発信トラフィックを許可する必要がある場合があります。

キャッシュスマートマップファイル(説明付き)

地理的背景としてGoogle Mapsを使用している場合、ファイルはキャッシュされません。

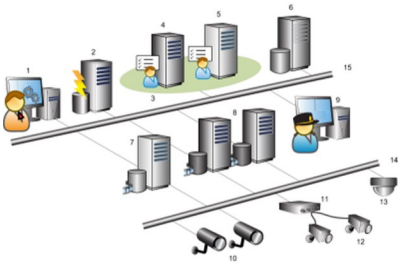
地理的背景で使用するファイルはタイルサーバーから取得します。ファイルがキャッシュフォルダーにどれだけの期間保存されるかは、XProtect Smart Clientの**設定**ダイアログの**削除されたキャッシュ済みスマートマップファイル**リストでどの値を選択するかに応じて変化します。ファイルは次のどちらかで保存されます。

- 無期限(**絶対になし**)
- ファイルが使用されていない場合は30日間(**30日間使用されていない場合**)
- オペレータがXProtect Smart Clientに存在する場合(**終了時**)

タイルサーバーのアドレスを変更すると、新規キャッシュフォルダーが自動的に作成されます。前のマップファイルは、ローカルコンピュータにある関連のキャッシュフォルダーに保持されています。

アーキテクチャ

分散型システム設定



分散型システム設定の例。カメラおよびレコーディングサーバーの数と、接続できるクライアントの数は、必要なだけ増やすことができます。

分散型のコンピュータはすべて、ドメインまたはワークグループに配置する必要があります。

凡例:

1. Management Client(s)
2. イベントサーバー
3. Microsoft Cluster
4. マネジメントサーバー
5. フェールオーバーマネジメントサーバー
6. SQL Serverを備えたサーバー
7. フェールオーバーレコーディングサーバー
8. レコーディングサーバー
9. XProtect Smart Client(s)
10. IPビデオカメラ
11. ビデオエンコーダ
12. アナログカメラ

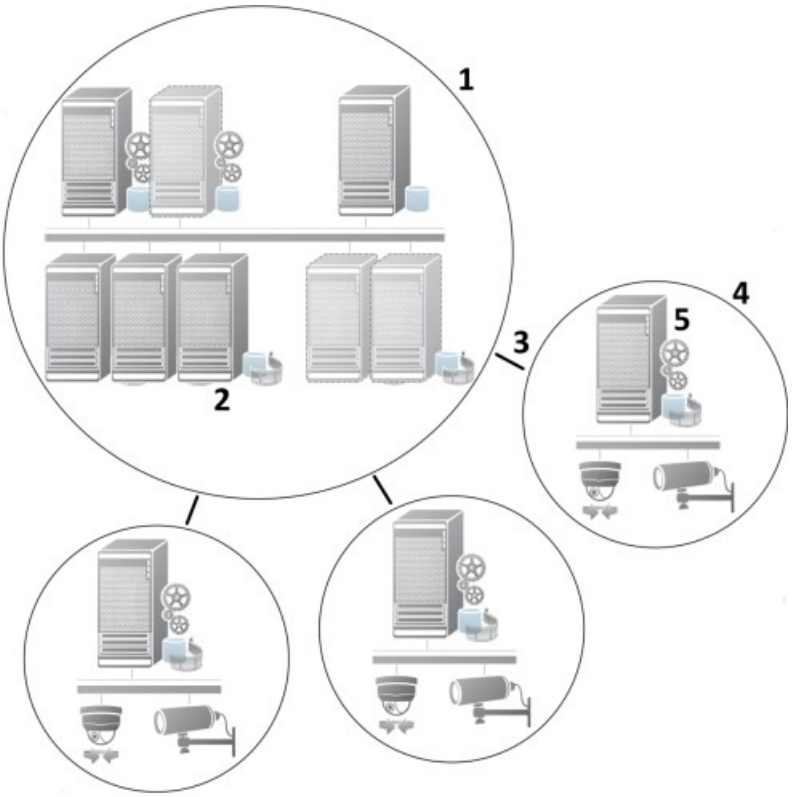
13. PTZ IPカメラ
14. カメラのネットワーク
15. サーバーのネットワーク

Milestone Interconnect(説明付き)

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

Milestone Interconnect™では、物理的に断片化された、より少ない数を統合し、1つのXProtect中央サイトでXProtect Corporateをリモートインストールできます。リモートサイトと呼ばれるこれらの小さいサイトは船舶、バス、電車などのモバイルユニットにインストールできます。つまり、このようなサイトは恒久的にネットワークに接続する必要がありません。

次の図は、システムに設定する方法Milestone Interconnectを示します。



1. Milestone Interconnect中央XProtect Corporateサイト
2. MilestoneInterconnectドライバー(中央サイトのレコーディングサーバーとリモートサイト間の接続を処理します。**ハードウェアの追加**ウィザードを使ってリモートシステムを追加する場合は、ドライバーのリストから選択する必要があります。)
3. Milestone Interconnectの接続
4. Milestone Interconnectリモートサイト(システムのインストールによる完全なリモートサイト、ユーザー、カメラなど)
5. Milestone Interconnectリモートシステム(リモートサイトでの実際の技術的なインストール)

中央サイトから**ハードウェアの追加**ウィザードを使用して、リモートサイトを中央サイトに追加します(298ページのリモートサイトを中央Milestone Interconnectサイトに追加を参照)。

各リモートサイトは独立して実行され、通常の監視タスクを実行することが可能です。ネットワーク接続および適切なユーザー権限(「299ページのユーザー権限を割り当て」を参照)によって、Milestone Interconnectは中央サイトにリモートサイトのカメラのライブビューが直接提供し、中央サイトでリモートサイトの録画を再生します。

中央サイトは、指定されたユーザー・アカウント(リモートサイトを追加したとき)がアクセス権を持つデバイスを表示し、アクセスすることのみ可能です。これにより、ローカルシステム管理者は、中央サイトとそのユーザーが使用できるデバイスを制御できます。

中央サイトではInterconnectで接続されたカメラ用システムのステータスを表示できますが、リモートサイトのステータスを直接表示することはできません。その代わり、リモートサイトをモニターするため、中央サイトでアラームまたは他の通知を起動するリモートサイトのイベントを使用できます(301ページのリモートサイトからのイベントに応答するように中央サイトを構成するを参照)。

XProtect Smart Clientユーザーによるイベント、ルール/スケジュール、または手動の要求のいずれかに基づいて、リモートサイトの録画を中央サイトに転送することが可能です。

XProtect Corporateシステムだけが、中央サイトとして動作できます。XProtect Corporateを含む他のすべての製品は、リモートサイトとして動作できます。中央サイトがリモートサイトで発生したデバイスやイベントを処理できるかどうかや、処理できる場合には、その方法、どのバージョン、何台のカメラを処理できるかは設定によって異なります。特定のXProtect製品をMilestone Interconnect設定で連携する方法の詳細については、Milestone InterconnectのWebサイト(https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/interconnect/)を参照してください。

Milestone InterconnectまたはMilestone Federated Architectureの選択(説明付き)

中央サイトのユーザーがリモートサイトのビデオにアクセスする必要がある、物理的に分散化されたシステムでは、Milestone Interconnect™またはMilestone Federated Architecture™を選択することができます。

Milestoneでは、以下の場合にMilestone Federated Architectureを推奨しています。

- 中央サイトとフェデレーテッドサイトの間でのネットワーク接続が安定している。
- ネットワークが同一ドメインを使用している。
- 大きなサイトが少数ある。
- 帯域は、必要要件に対して十分である。

Milestoneでは、以下の場合にMilestone Interconnectを推奨しています。

- 中央サイトとリモートサイトのネットワーク接続が不安定。
- 自分または組織が、リモートサイトで別のXProtect製品を使用することを希望している。
- ネットワークが異なるドメインまたはワークグループを使用している。
- 小さいサイトが多数ある。

Milestone Interconnectおよびラインセンス

Milestone Interconnectを実行するには、中央サイトに、リモートサイトのハードウェアデバイスから動画を表示するためのMilestone Interconnectカメラライセンスが必要です。必要なMilestone Interconnectカメラライセンスの数は、データを受信したいリモートサイトのハードウェアデバイスの数によって異なります。XProtect Corporateのみが中央サイトとして動作できます。

Milestone Interconnectカメラライセンスのステータスは、中央サイトの**ライセンス情報**ページに一覧表示されます。

Milestone Interconnectの設定(説明付き)

Milestone Interconnectを実行する方法は3つあります。設定の実行方法は、ネットワーク接続、録画の再生方法、リモート録画を取得するかどうか、またどの程度取得するかによって異なります。

以下では、最も一般的な3つの設定ついて説明しています。

リモートサイトから直接再生(安定したネットワーク接続)

最も単純な設定です。中央サイトは常にオンラインでリモートサイトに接続し、中央サイトのユーザーはリモートサイトから直接録画を再生します。このためには**リモートシステムから録画を再生**オプションを使用する必要があります(300ページのリモートサイトのカメラからの直接再生を可能にするを参照)。

ルールまたはXProtect Smart Clientに基づく、リモートサイトからの選択したリモート録画シーケンスの取得(一時的に制限されたネットワーク接続)

選択した録画シーケンス(リモートサイトから開始)を、リモートサイトからの独立を保証するために中央に保存する必要があるときに使用します。ネットワーク障害やネットワークが制限された場合に、独立性は非常に重要になります。リモート録画の取得設定は、**リモート取得**タブで構成します(408ページのリモート取得タブを参照)。

必要に応じて、またはルールを設定できる場合にXProtect Smart Clientからリモート録画の取得を開始できます。シナリオによっては、リモートサイトをオンラインにしておいたり、あるいはほとんどの時間オフラインにすることができます。これは多くの場合、業界によって異なります。中央サイトがリモートサイトと恒久的に接続されていることが一般的な業界もあります(小売業の本社(中央サイト)と多数の店舗(リモートサイト)など)。また、運輸業など、リモートサイトがモバイル(バス、電車、船舶など)であり、断続的にしかネットワークに接続できない業界もあります。リモート録画取得中にネットワーク接続で障害が発生した場合、ジョブは次の機会に続行されます。

自動取得またはXProtect Smart Clientからの取得リクエストを**リモート取得**タブで指定されている時間間隔外に検出した場合、リクエストは受け付けられますが、選択された時間間隔に達するまでは開始されません。新しい録画取得ジョブはキューに入れられ、許容される時間間隔に達したときに開始されます。保留中のリモート録画取得ジョブは、**システムダッシュボード>現在のタスク**から確認できます。

接続エラーの後、取得できなかったリモート録画はデフォルトでリモートサイトから取得されます。

レコーティングサーバーなどのリモートサイトは、カメラのエッジストレージを使用します。通常、リモートサイトは中央サイトとオンラインで接続されており、中央サイトにより録画されるようライブストリームをフィードしています。何らかの原因でネットワークが切断されると、中央サイトは録画シーケンスを失います。ただし、ネットワークが復旧すると、中央サイトは、ダウン期間中のリモート録画を自動的に取得します。ここでは、カメラの**レコード**タブの**接続が復旧したときに自動的にリモート録画を取得する**オプション(300ページのリモートサイトのカメラからリモート録画を取得するを参照)を使用する必要があります。

お客様の組織のニーズに合わせて上記の方法を組み合わせることができます。

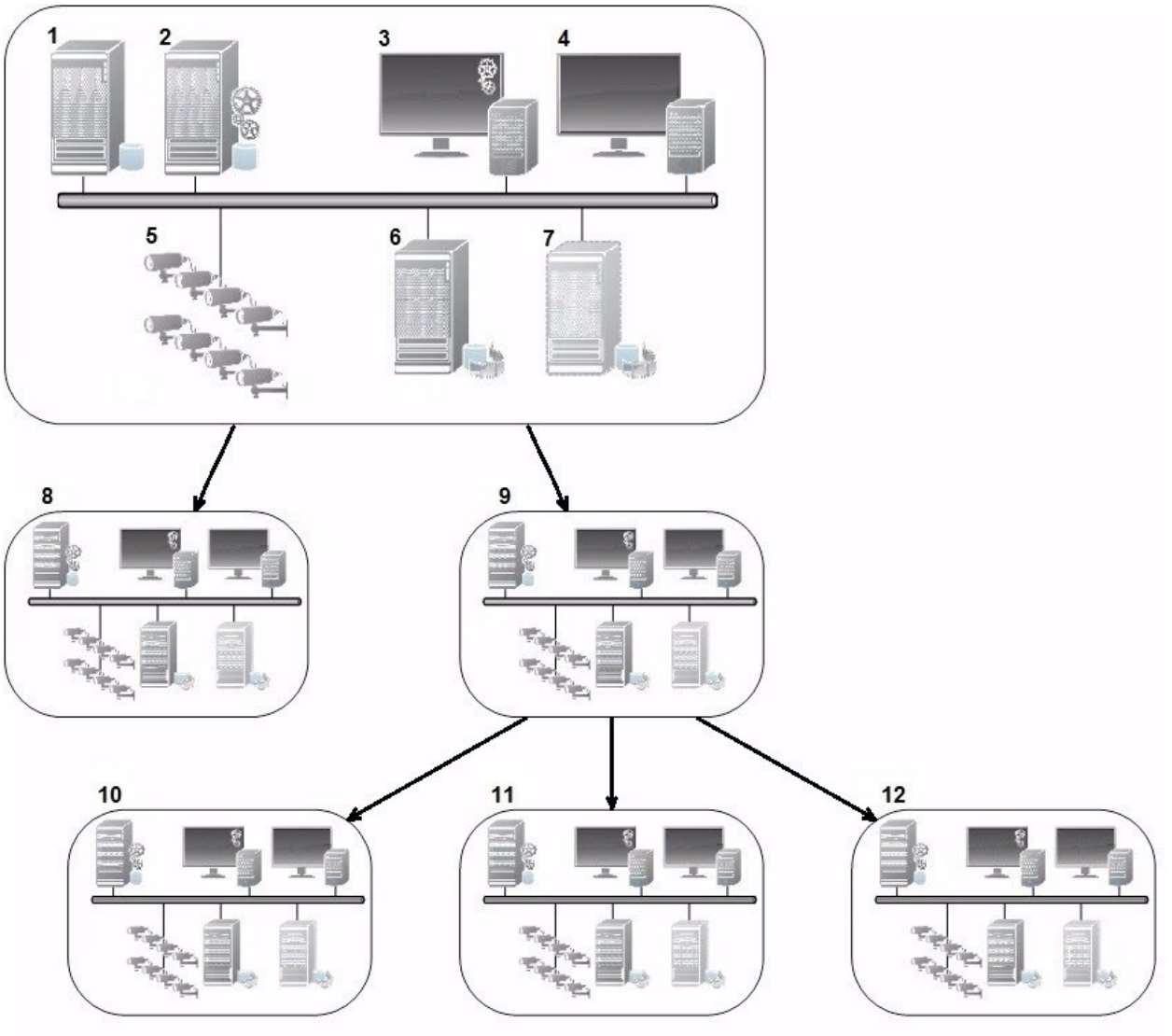
Milestone Federated Architectureの設定

XProtect Expertは子サイトとしてのみフェデレートできます。

Milestone Federated Architectureは、複数の別個の標準システムを親/子サイトのフェデレーテッドサイト階層にリンクします。十分な権限を持つクライアントユーザーは、個別のサイト全体で、ビデオ、音声およびその他のリソースにシームレスにアクセスできます。バージョン2018 R1以降管理者は、フェデレートされた階層内で個別のサイトの管理者権限に基づき、すべてのサイトを中央管理できます。

基本ユーザーはMilestone Federated Architectureシステムでサポートされていないので、Active Directoryサービスを介してWindowsユーザーとしてユーザーを追加する必要があります。

Milestone Federated Architectureは1つの中央サイト(最上位サイト)と任意の数のフェデレートされたサイトで設定されます(293ページのフェデレーテッドサイトを実行するためのシステムの設定を参照)。サイトにログインすると、すべての子サイトと子サイトの子サイトの情報にアクセスできます。親サイトからリンクを要求すると、2つのサイト間のリンクが確立されます(295ページのサイトを階層に追加を参照)。子サイトは1つの親サイトとのみリンクできます。フェデレートされたサイト階層に追加する際、子サイトの管理者でない場合は、子サイトの管理者によってリクエストが許可されなくてはなりません。



Milestone Federated Architectureセットアップのコンポーネント:

1. SQL Serverを備えたサーバー
2. マネジメントサーバー
3. Management Client
4. XProtect Smart Client
5. カメラ
6. レコーディングサーバー
7. フェールオーバーレコーディングサーバー
8. ~ 12。フェデレーテッドサイト

階層の同期化

親サイトには、現在接続されている子サイト、子サイトの子サイトなど、全てに関する更新されたリストがあります。フェデレーテッドサイト階層には、サイト間でスケジュールされている同期化のほか、サイトが追加または削除されるたびに管理により起動される同期化が含まれています。システムが階層を同期化する場合、レベルごとに実施し、情報を要求しているサーバーに到達するまで各レベルが通信を転送し、応答します。システムは、毎回1MB未満を送信します。レベルの数によって、階層への変更がManagement Clientで表示されるまでに時間がかかることがあります。独自の同期化をスケジュールすることはできません。

データトラフィック

ユーザーや管理者がライブビデオまたは録画ビデオを表示したり、サイトを設定したりすると、システムは通信または設定データを送信します。データの量は、何がどの程度表示または設定されたかによって異なります。

Milestone Federated Architectureと他の製品およびシステムの要件

- 最新版を含め3つの主要なリリースでは、Management ClientをMilestone Federated Architectureで開くことができます。それ以外のMilestone Federated Architectureセットアップでは、サーバーバージョンに一致する別個のManagement Clientが必要です。
- 中央サイトがXProtect Smart Wallを使用している場合、フェデレーテッドサイト階層のXProtect Smart Wall機能も使用できます。
- 中央サイトでXProtect Accessが使用されている状態で、XProtect Smart Clientユーザーがフェデレーテッドサイト階層にログインする場合、XProtect Smart Clientにはフェデレーテッドサイトからのアクセスリクエスト通知も表示されます。
- XProtect Expert 2013システムまたはそれ以降を、親サイトとしてではなく、子サイトとしてフェデレーテッドサイト階層に追加できます。
- Milestone Federated Architectureは追加ライセンスを必要としません。
- ユースケースと利点の詳細については、Milestone Federated Architectureに関する白書を参照してください。

フェデレーテッドサイト階層の確立

Management Clientは、Milestoneで階層を作成する前に、サイトを相互にリンクする方法を計画することをお勧めします。

各サイトをインストールし、フェデレーテッド階層で、標準のシステムコンポーネント、設定、ルール、スケジュール、管理者、ユーザー、およびユーザー権限を使用して、各サイトを通常のスタンドアロンシステムとして設定します。すでにサイトがインストールおよび構成されており、必要な作業はフェデレーテッドサイト階層で結合することだけである場合は、システムを設定できます。

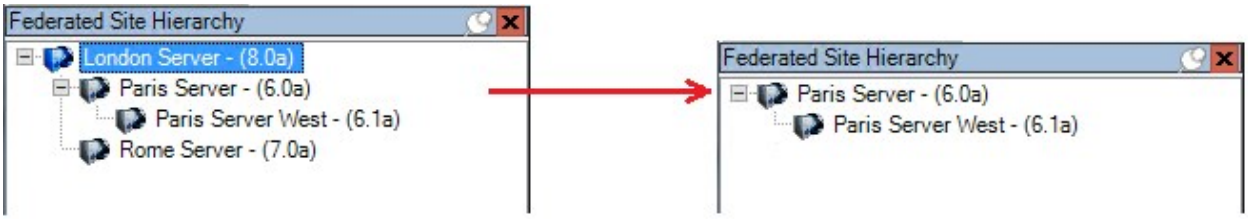
個別のサイトがインストールされた時点で、フェデレーテッドサイトとして実行するようにサイトを設定する必要があります(293ページのフェデレーテッドサイトを実行するためのシステムの設定を参照)。

階層を開始するには、中央サイトとして機能するサイトにログインし、最初のフェデレーテッドサイトを追加(295ページのサイトを階層に追加)することができます。**フェデレーション・サイト階層**にリンクが確立されると、2つ階層を展開するための複数のサイトを追加できるManagement Clientウィンドウでフェデレーション・サイト階層を自動的に作成します。

フェデレーテッドサイト階層が作成された後、ユーザーと管理者はサイトにログインし、そのサイトと関連付けられた任意のフェデレーテッドサイトにアクセスできます。フェデレーテッドサイトへのアクセスは、ユーザーの権限によって異なります。

フェデレーテッド階層に追加できるサイトの数は無制限です。また、古い製品バージョンのサイトを新しいバージョンのサイトにリンクできます。逆も可能です。バージョン番号は自動的に表示され、削除できません。ログインしたサイトは常に**フェデレーテッドサイト階層**ペインの最上部に表示され、ホームサイトと呼ばれます。

以下が、Management Clientのフェデレーテッドサイトの例です。左では、ユーザーがトップサイトにログインしています。右では、ユーザーが子サイトの一つ、Paris Server、つまりホームサイトにログインしています。



Milestone Federated Architectureのステータスアイコン

アイコンはサイトの状態を表します。

説明	アイコン
階層全体での最上位サイトが動作中。	
階層全体での最上位サイトはまだ動作中ですが、1つまたは複数の問題に注意が必要です。最上位サイトのアイコン上に表示されます。	
サイトが動作中。	
サイトは、階層での許可待ち中です。	
サイトは接続していますが、まだ動作していません。	

このシステムで使用するポート

これらが必要とするXProtectコンポーネントとポートのすべてを以下に記します。ファイアウォールが不必要なトラフィックのみをブロックするなど、システムが使用するポートを指定する必要があります。これらのポートのみを有効にします。リストにはローカルプロセスで使用するポートも含んでいます。

次の2つのグループに調整されています。

- **サーバーコンポーネント**(サービス) は特定ポートのサービスを提供しますので、これらポートについてのクライアントの要求を聞く必要があります。よって、これらのポートは着信 / 送信接続のためWindowsファイアウォールで開いておく必要があります。
- **クライアントコンポーネント**(クライアント) はサーバーコンポーネントの特定ポートに接続を開始します。よって、これらのポートは発信接続のために開く必要があります。発信接続は一般的に、デフォルトでWindowsファイアウォールで開かれています。

何も言及されていない場合は、サーバーコンポーネントのポートは着信接続のために開き、クライアントコンポーネントのポートは発信接続のために開く必要があります。

サーバーのコンポーネントは他のサーバー コンポーネントに対してクライアントのように機能する点に留意してください。この文書では明示的に記載されていません。

ポート番号はデフォルト番号ですが、変更できます。Milestoneで構成できないポートを変更する必要がある場合は、Management Clientサポートまでお問い合わせください。

サーバーコンポーネント(着信接続)

次の各セクションでは特定サービスで開く必要あるポートを記載しています。特定コンピュータで開けておく必要があるポートを見つけるためには、このコンピュータで実行しているすべてのサービスを考慮する必要があります。

Management Serverサービスと関連プロセス

ポート番号	プロトコル	プロセス	接続元	目的
80	HTTP	IIS	すべてのサーバーおよびXProtect Smart Client、Management Client	80番ポートと443番ポートの目的は同じです。ただし、VMSがどのポートを使用するかは、通信の安全性を確保するために証明書を使用したかどうかによって異なります。 • 証明書による通信のセキュリティが確保されていない場合、VMSは80番ポートを使用します。 • 証明書で通信を保護した場合、VMSはイベントサーバーからマネジメントサーバーへの通信を除き、443番ポートを使用します。イベントサーバーからマネジメントサーバーへの通信は、WindowsのSecured Framework (WCF) を使用し、80番ポートでWindows認証を行います。
443	HTTPS	IIS		
6473	TCP	Management Serverサービス	Management Server Managerトレイアイコン、	状況の表示とサービスの管理。

ポート番号	プロトコル	プロセス	接続元	目的
			ローカル接続のみ。	
8080	TCP	マネジメントサーバー	ローカル接続のみ。	サーバー上の内部プロセス間の通信。
9000	HTTP	マネジメントサーバー	Recording Serverサービス	サーバー間の内部コミュニケーション用Webサービスです。
12345	TCP	Management Serverサービス	XProtect Smart Client	システムとMatrix受信者の間の通信。 Management Clientのポート番号は変更できます。
12974	TCP	Management Serverサービス	Windows SNMPサービス	SNMP拡張エージェントとの通信。 システムがSNMPを適用しない場合でも、他の目的でこのポートを使用しないでください。 XProtect 2014 システム以前のポート番号は6475でした。 XProtect 2019 R2システム以前のポート番号は7475でした。

SQL Serverサービス

ポート番号	プロトコル	プロセス	接続元	目的
1433	TCP	SQL Server	Management Serverサービス	Identity Provider経由で構成を保存 & 取得中。
1433	TCP	SQL Server	Event Serverサービス	Identity Provider経由でイベントを保存 & 取得中。
1433	TCP	SQL Server	Log Serverサービス	Identity Provider経由でログエントリを保存 & 取得中。

Data Collectorサービス

ポート番号	プロトコル	プロセス	接続元	目的
7609	HTTP	IIS	マネジメントサーバーコンピュータ上：他の全サーバー上のData Collectorサービス。 その他のコンピュータ上：マネジメントサーバー上のData Collectorサービス。	システムモニター。

Event Serverサービス

ポート番号	プロトコル	プロセス	接続元	目的
1234	TCP/UDP	Event Server サービス	XProtectシステムにジェネリックイベントを送信するサーバーすべて。	外部システムまたはデバイスからのジェネリックイベントをリスンします。 関連のデータソースが有効な場合のみ。
1235	TCP	Event Server サービス	XProtectシステムにジェネリックイベントを送信するサーバーすべて。	外部システムまたはデバイスからのジェネリックイベントをリスンします。 関連のデータソースが有効な場合のみ。
9090	TCP	Event Server サービス	XProtectシステムにアナリティクスイベントを送信するすべてのシステムまたはデバイス。	外部システムまたはデバイスからのアナリティクスイベントをリスンします。 アナリティクスイベント機能が有効な場合のみ関連。
22331	TCP	Event Server サービス	XProtect Smart ClientおよびManagement Client	構成、イベント、アラーム、およびマップデータ。
22332	WS/WSS HTTP/HTTPS*	Event Server サービス	API GatewayおよびManagement Client	イベント/ ステータス購読、イベントREST API、Websockets Messaging API、アラームREST API。
22333	TCP	Event Server サービス	MIPプラグインおよびアプリケーション。	MIP メッセージング。

* HTTPS専用エンドポイントにアクセスするためにHTTPにアクセスすると、403エラーが返されます。

Recording Serverサービス

ポート番号	プロトコル	プロセス	接続元	目的
25	SMTP	Recording Serverサービス	カメラ、エンコーダー、およびI/Oデバイス。	デバイスからのイベントメッセージをリスンします。 このポートはデフォルトでは無効になっています。 (非推奨) これを有効にすると暗号化されていない接続用にポートが開かれるため、この操作は推奨されません。
5210	TCP	Recording Serverサービス	フェールオーバーレコーディングサーバー。	フェールオーバーレコーディングサーバーが実行された後のデータベースの統合。
5432	TCP	Recording Serverサービス	カメラ、エンコーダー、およびI/Oデバイス。	デバイスからのイベントメッセージをリスンします。 このポートはデフォルトでは無効になっています。
7563	TCP	Recording Serverサービス	XProtect Smart Client, Management Client	ビデオおよび音声ストリーム、PTZコマンドの取得。
8966	TCP	Recording Serverサービス	Recording Server Managerトレイアイコン、ローカル接続のみ。	状況の表示とサービスの管理。
9001	HTTP	Recording Serverサービス	マネジメントサーバー	サーバー間の内部コミュニケーション用Webサービスです。 複数のレコーディングサーバーインスタンスが使用されている場合は、それぞれのインスタンスに独自のポートが必要です。追加ポートは9002、9003、などとなります。

ポート番号	プロトコル	プロセス	接続元	目的
11000	TCP	Recording Serverサービス	フェールオーバーレコーディングサーバー	レコーディングサーバーのステータスのポーリング。
12975	TCP	Recording Serverサービス	Windows SNMPサービス	SNMP拡張エージェントとの通信。 システムがSNMPを適用しない場合でも、他の目的でこのポートを使用しないでください。 XProtect 2014システム以前のポート番号は6474でした。 XProtect 2019 R2システム以前のポート番号は7474でした。
65101	UDP	Recording Serverサービス	ローカル接続のみ	ドライバーからのイベント通知をリスンします。

Recording Serverサービスによって上記のRecording Serverサービスへの着信接続に加え、以下への発信接続も確立されます。

- カメラ
- NVR
- リモート相互接続サイト(Milestone相互接続ICP)

Failover ServerサービスとFailover Recording Serverサービス

ポート番号	プロトコル	プロセス	接続元	目的
25	SMTP	Failover Recording Serverサービス	カメラ、エンコーダー、およびI/Oデバイス。	デバイスからのイベントメッセージをリスンします。 このポートはデフォルトでは無効になっています。

ポート番号	プロトコル	プロセス	接続元	目的
				(非推奨) これを有効にすると暗号化されていない接続用にポートが開かれるため、この操作は推奨されません。
5210	TCP	Failover Recording Serverサービス	フェールオーバーレコーディングサーバー	フェールオーバーレコーディングサーバーが実行された後のデータベースの統合。
5432	TCP	Failover Recording Serverサービス	カメラ、エンコーダー、およびI/Oデバイス。	デバイスからのイベントメッセージをリスンします。 このポートはデフォルトでは無効になっています。
7474	TCP	Failover Recording Serverサービス	Windows SNMPサービス	SNMP拡張エージェントとの通信。 システムがSNMPを適用しない場合でも、他の目的でこのポートを使用しないでください。
7563	TCP	Failover Recording Serverサービス	XProtect Smart Client	ビデオおよび音声ストリーム、PTZコマンドの取得。
8844	UDP	Failover Recording Serverサービス	Failover Recording Serverサービス間の通信	2つのサーバーの間の通信。
8966	TCP	Failover Recording Serverサービス	Failover Recording Server Managerトレイアイコン、ローカル接続のみ。	状況の表示とサービスの管理。
8967	TCP	Failover Serverサービス	Failover Server Managerトレイアイコン、ローカル接続のみ。	状況の表示とサービスの管理。
8990	HTTP	Failover Serverサービ	Management Serverサービス	Failover Serverサービスのステータスをモニター。

ポート番号	プロトコル	プロセス	接続元	目的
		ス		
9001	HTTP	Failover Serverサービス	マネジメントサーバー	サーバー間の内部コミュニケーション用Webサービスです。

上記のフェールオーバー サーバー/ Failover Recording Serverサービスへの受信接続に加えて、フェールオーバー サーバー/ Failover Recording Server サービスは、通常のレコーダー、カメラ、ビデオプッシュ向けに送信接続を確立します。

Log Serverサービス

ポート番号	プロトコル	プロセス	接続元	目的
22337	HTTP	Log Server サービス	XProtectおよびレコーディングサーバーを除く、すべてのManagement Clientコンポーネント。	ログサーバーの書き込み、読み取り、構成を行います。

Mobile Serverサービス

ポート番号	プロトコル	プロセス	接続元	目的
8000	TCP	Mobile Serverサービス	Mobile Server Managerトレイアイコン、ローカル接続のみ。	SysTrayアプリケーション。
8081	HTTP	Mobile Serverサービス	Mobileクライアント、Webクライアント、およびManagement Client。	ビデオや音声などデータストリームの送信。
8082	HTTPS	Mobile	Mobileクライアントおよびwebクライアン	ビデオや音声などデータストリー

ポート番号	プロトコル	プロセス	接続元	目的
		Serverサービス	ト。	ムの送信。
40001 - 40099	HTTP	Mobile Serverサービス	レコーディング サーバー サービス	Mobile Server ビデオプッシュ。 このポート範囲はデフォルトでは無効になっています。

LPR Serverサービス

ポート番号	プロトコル	プロセス	接続元	目的
22334	TCP	LPR Server サービス	イベントサーバー	認証されたナンバープレートとサーバー状況の取得。 接続するためには、イベントサーバーにはLPRプラグインがインストールされている必要があります。
22334	TCP	LPR Server サービス	LPR Server Managerトレイアイコン、ローカル接続のみ。	SysTrayアプリケーション

Milestone Open Network Bridgeサービス

ポート番号	プロトコル	プロセス	接続元	目的
580	TCP	Milestone Open Network Bridgeサービス	ONVIFクライアント	ビデオストリーム構成の認証と要求
554	RTSP	RTSPサービス	ONVIFクライアント	ONVIFクライアントへの要求ビデオのストリーミング。

XProtect DLNA Serverサービス

ポート番号	プロトコル	プロセス	接続元	目的
9100	HTTP	DLNA Server サービス	DLNAデバイス	デバイス検出およびDLNAチャネル構成の提供。ビデオストリームの要求。
9200	HTTP	DLNA Server サービス	DLNAデバイス	DLNAデバイスへの要求 ビデオのストリーミング。

XProtect Screen Recorderサービス

ポート番号	プロトコル	プロセス	接続元	目的
52111	TCP	XProtect Screen Recorder	Recording Serverサービス	モニターからビデオの提供。録画サーバー上にカメラと同じように表示され、機能します。 Management Clientのポート番号は変更できます。

XProtect Incident Managerサービス

ポート番号	プロトコル	プロセス	接続元	目的
80	HTTP	IIS	XProtect Smart Clientおよび Management Client	80番ポートと443番ポートの目的は同じです。ただし、VMSがどのポートを使用するかは、通信の安全性を確保するために証明書を使用したかどうかによって異なります。 • 証明書による通信のセキュリティが確保されていない場合、VMSは80番ポートを使用します。 • 証明書で通信を保護した場合、VMSは443番ポートを使用します。
443	HTTPS	IIS		

サーバーコンポーネント(送信接続)

Management Serverサービス

ポート番号	プロトコル	接続先	目的
443	HTTPS	ライセンス管理サービスをホストするライセンスサーバー。コミュニケーションは https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx を通じて行われます。	ライセンスのアクティベーション

Recording Serverサービス

ポート番号	プロトコル	接続先	目的
80	HTTP	カメラ、NVR、エンコーダ 接続されているサイト	認証、構成、データストリーム、ビデオ、音声。 ログイン
443	HTTPS	カメラ、NVR、エンコーダ	認証、構成、データストリーム、ビデオ、音声。
554	RTSP	カメラ、NVR、エンコーダ	データストリーム、ビデオ、音声。
7563	TCP	接続されているサイト	データストリームとイベント。
11000	TCP	フェールオーバーレコーディングサーバー	レコーディングサーバーのステータスのポーリング。
40001 - 40099	HTTP	モバイル サーバー サービス	モバイル サーバー ビデオ プッシュ。 このポート範囲はデフォルトでは無効になっています。

Failover ServerサービスとFailover Recording Serverサービス

ポート番号	プロトコル	接続先	目的
11000	TCP	フェールオーバーレコーディングサーバー	レコーディングサーバーのステータスのポーリング。

Event Serverサービス

ポート番号	プロトコル	接続先	目的
80	HTTP	API GatewayおよびManagement Server	API Gatewayから構成APIにアクセス
443	HTTPS	API GatewayおよびManagement Server	API Gatewayから構成APIにアクセス
443	HTTPS	Milestone Customer Dashboard経由 https://service.milestonesys.com/	XProtectシステムからMilestone Customer Dashboardへステータス、イベント、エラーメッセージを送信。

Log Serverサービス

ポート番号	プロトコル	接続先	目的
443	HTTP	ログサーバー	メッセージをログサーバーに転送します。

API Gateway

ポート番号	プロトコル	接続先	目的
443	HTTPS	Management Server	RESTful API
22332	WS/WSS HTTP/HTTPS*	Management Client	イベント/ステータサブスクリプション、Events REST API、Websockets Messaging API、Alarms REST API。

カメラ、エンコーダー、I/Oデバイス(着信接続)

ポート番号	プロトコル	接続元	目的
80	TCP	レコーディング サーバーとフェールオーバー レコーディング サーバー	ビデオと音声の認証、構成、およびデータストリーム。

ポート番号	プロトコル	接続元	目的
443	HTTPS	レコーディング サーバーとフェールオーバー レコーディング サーバー	ビデオと音声の認証、構成、およびデータストリーム。
554	RTSP	レコーディング サーバーとフェールオーバー レコーディング サーバー	ビデオと音声のデータストリーム。

カメラ、エンコーダー、I/Oデバイス(送信接続)

ポート番号	プロトコル	接続先	目的
25	SMTP	レコーディング サーバーとフェールオーバー レコーディング サーバー	イベント通知の送信(使用されていません)
5432	TCP	レコーディング サーバーとフェールオーバー レコーディング サーバー	イベント通知の送信。 このポートはデフォルトでは無効になっています。
22337	HTTP	ログサーバー	メッセージをログサーバーに転送します。

発信接続が確立できるカメラは数種のモデルのみです。

クライアントコンポーネント(発信接続)

XProtect Smart Client、XProtect Management Client、XProtect Mobileサーバー

ポート番号	プロトコル	接続先	目的
80	HTTP	API GatewayおよびManagement Serverサービス	認証およびAPI Gatewayのその他のAPI

ポート番号	プロトコル	接続先	目的
443	HTTPS	API Gatewayおよび Management Serverサービス	暗号化が有効な場合の基本ユーザーの認証およびAPI Gatewayでのその他のAPI。
443	HTTPS	Milestone Systems A/S (doc.milestonesys.com、52.178.114.226)	Management ClientとSmart Clientにより、ヘルプURLにアクセスしてオンラインヘルプが利用できるかどうかがときどきチェックされます。
7563	TCP	Recording Serverサービス	ビデオおよび音声ストリーム、PTZ コマンドの取得。
22331	TCP	Event Serverサービス	アラーム。

XProtect Web Client、XProtect Mobileクライアント

ポート番号	プロトコル	接続先	目的
8081	HTTP	XProtect Mobileサーバー	ビデオおよび音声ストリームの取得。
8082	HTTPS	XProtect Mobileサーバー	ビデオおよび音声ストリームの取得。

API Gateway

ポート番号	プロトコル	接続先	目的
80	HTTP	Management Server	RESTful API
443	HTTPS	Management Server	RESTful API

アプリケーションプール

VMSには、.NET v4.5、.NET v4.5 Classic、DefaultAppPool.などの標準アプリケーションプールが含まれています。システムで使用可能なアプリケーションプールは、インターネット情報サービス (IIS) マネジャーに表示されます。VideoOSでは、上記の標準アプリケーションプールの他、一連のMilestone XProtect VMSアプリケーションプールが提供されます。

Milestone XProtectのアプリケーションプール

次の表では、Milestone XProtectで提供されるVideoOSアプリケーションプールの概要を確認できます。

名前	ID	目的
.NET v4.5	ApplicationPoolId	標準IIS機能
.NET v4.5 Classic	ApplicationPoolId	標準IIS機能
DefaultAppPool	ApplicationPoolId	標準IIS機能
VideoOS ApiGateway	NetworkService	将来のパブリックXProtectAPIであるAPIゲートウェイと、VMSへのゲートウェイをホストします。
VideoOS Classic	NetworkService	ローカルヘルプなどのレガシーコンポーネントをホストし、主に下位互換性に準拠します。
VideoOS IDP	NetworkService	Identity Provider APIをホストします。Identity Providerは、基本ユーザーのID情報を作成、維持、管理し、依存するアプリケーションまたはサービスに認証および登録サービスを提供します。
VideoOS IM	NetworkService	XProtect Incident Manager APIをホストします。XProtect Incident Managerインシデントを文書化し、XProtectVMSからのシーケンスエビデンス(ビデオおよび潜在的に音声)と組み合わせます。
VideoOS Management Server	NetworkService	Configuration API、サーバーコンポーネントAPI、その他のManagement Serverサービスをホストし、ユーザー認証を管理します。
VideoOS ReportServer	NetworkService	アラームやイベントのレポートを収集・作成するウェブアプリケーションをホストします。
VideoOS ShareService	NetworkService	XProtect Mobileクライアントのユーザー間のブックマークやライブビデオの共有を容易にするサービスをホストします。

アプリケーションプールを操作する

インターネット情報サービス() ウィンドウの**IISアプリケーションプール**ページから、アプリケーションプールを追加したり、アプリケーションプールのデフォルトを設定したり、各アプリケーションプールでホストされているアプリケーションを表示したりできます。

アプリケーションプールページを開く

1. Windows**スタート**メニューから、**インターネット情報サービス(IIS) マネジャー**を開きます。
2. **接続**ペインで環境の名前をクリックし、**アプリケーションプール**をクリックします。
3. **アクション**の下で、**アプリケーションプールを追加する**または **アプリケーションプールのデフォルトを設定する** をクリックし、これらのタスクを実行します。
4. **アプリケーションプール**ページでアプリケーションプールを選択すると、各アプリケーションプールの**アクション**の下に、さらにオプションが表示されます。

製品比較

XProtect VMSには以下の製品が含まれます:

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+
- XProtect Essential+

すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト
((https://www.milestonesys.com/products/software/product-index/) の製品概要ページで提供されています。

ライセンス

ライセンス(説明付き)

無料のXProtect Essential+

XProtect Essential+をインストールしている場合は、システムと8つのデバイスライセンスを無料で実行できます。自動ライセンスアクティベーションが有効なため、ハードウェアはシステムに追加するだけでアクティベートされます。

より上位のXProtect製品にアップグレードし、SLC(ソフトウェアライセンスコード)を変更する必要がある場合にのみ(115ページのソフトウェアライセンスコードの変更を参照)、このトピックの残りの部分と他のライセンス関連のトピックをお読みください。

XProtect VMS製品用のライセンス(XProtect Essential+を除く)

ソフトウェアライセンスおよびSLC

ソフトウェアとライセンスを購入すると、次のものを受け取ります。

- 注文確認書とSLC(ソフトウェアライセンスコード)に基づく名前が付けられ、.lic拡張子の付いたソフトウェアライセンスファイルが電子メールで受信されます。
- Milestone Careの監視範囲

SLCは注文確認書にも記載され、次のようにハイフンで区切られた数字と文字から構成されています。

- 製品バージョン2014以前:xxx-xxxx-xxxx
- 製品バージョン2016以降:xxx-xxx-xxx-xx-xxxxxx

購入したVMS製品、XProtect拡張機能、ライセンスについてのすべての情報は、ソフトウェアライセンスファイルに含まれています。Milestoneは、今後使用する場合に備え、SLCに関する情報とソフトウェアライセンスファイルのコピーを安全な場所に保管するよう推奨しています。SLCはのライセンス情報Management Clientウィンドウでも確認できます。**[ライセンス情報]**ウィンドウは、**[サイトナビゲーション]**ペイン**->[基本]**ノード**->[ライセンス情報]**の順に選択することで開くことができます。My Milestoneユーザーアカウントを作成したり、サポートのためリセラーに問い合わせたりする際、またはシステムに変更を加えなくてはならない場合などには、ソフトウェアライセンスファイルまたはSLCが必要となることがあります。

インストールとライセンス付与の全プロセス

開始するには、ソフトウェアを弊社ウェブサイト(https://www.milestonesys.com/downloads/)からダウンロードします。ソフトウェアのインストール中(137ページの新しいXProtectシステムのインストールを参照)、ソフトウェアライセンスファイルの提供が求められます。ソフトウェアライセンスファイルがない場合、インストールを完了できません。

インストールが完了した後、カメラを追加する際にライセンスをアクティベートする必要があります(108ページのライセンスアクティベーション(説明付き)を参照)。ライセンスのアクティベーションはのライセンス情報Management Clientウィンドウで行います。ここでは、同一のSLCでインストールされたすべての製品のライセンスの概要が確認できます。**[ライセンス情報]**ウィンドウは、**[サイトナビゲーション]**ペイン**->[基本]**ノード**->[ライセンス情報]**の順に選択することで開くことができます。

ライセンスタイプ

XProtectライセンスシステムでは、複数のライセンスタイプが用意されています。

基本ライセンス

最低でも、いずれかのXProtectVMS製品に対して1つの基本ライセンスを保有することになります。また、XProtect拡張機能用に1つ以上の基本ライセンスを持つこともできます。

デバイスライセンス

最低でも、複数のデバイスライセンスを保有することになります。通常は、システムに追加したいカメラ搭載ハードウェアデバイスごとに、1つのデバイスライセンスが必要となります。ただし、これはハードウェアデバイスによって異なる場合があり、Milestoneに対応したハードウェアデバイスであるかどうかに応じても変化します。詳細については、107ページの対応ハードウェアデバイスおよび107ページの非対応ハードウェアデバイスを参照してください。

XProtect Mobileでビデオプッシュ機能を使用したい場合は、システムにビデオをプッシュするためのモバイルデバイスまたはタブレットごとに、デバイスライセンスが1つ必要となります。

カメラに搭載されているスピーカー、マイク、入出力デバイスにはデバイスライセンスは必要ありません。

対応ハードウェアデバイス

通常は、システムに追加したいカメラ搭載ハードウェアデバイスごとに、1つのデバイスライセンスが必要となります。ただし少数ながら、複数のデバイスライセンスが必要となる対応ハードウェアデバイスも存在します。ハードウェアデバイスにいくつのデバイスライセンスが必要となるかは、Milestoneウェブサイト(https://www.milestonesys.com/support/tools-and-references/supported-devices/) の対応ハードウェアのリストで確認できます。

最大16チャネルを有するビデオエンコーダーについては、ビデオエンコーダーのIPアドレスごとに1つのデバイスライセンスしか必要ありません。ビデオエンコーダーには1つ以上のIPアドレスがある場合があります。

ただし、ビデオエンコーダーのチャネル数が16を超える場合、ビデオエンコーダー上でアクティベートされたカメラごとに(ならびにアクティベートされた最初の16台分のカメラごとに) 1つのデバイスライセンスが必要となります。

非対応ハードウェアデバイス

非対応ハードウェアデバイスについては、ビデオチャネルを使用しているアクティベート済みカメラごとにデバイスライセンスが1つ必要となります。

非対応ハードウェアデバイスは、Milestone Webサイト(https://www.milestonesys.com/support/tools-and-references/supported-devices/) の対応ハードウェアのリストには記載されていません。

Milestone Interconnect™用のカメラライセンス

Milestone Interconnectを実行するには、中央サイトに、リモートサイトのハードウェアデバイスから動画を表示するためのMilestone Interconnectカメラライセンスが必要です。必要なMilestone Interconnectカメラライセンスの数は、データを受信したいリモートサイトのハードウェアデバイスの数によって異なります。XProtect Corporateのみが中央サイトとして動作できます。

XProtect拡張機能用のライセンス

ほとんどのXProtect拡張機能には追加ライセンスが必要です。ソフトウェアライセンスファイルには、拡張機能ライセンスに関する情報も含まれています。一部の拡張機能には、個別のソフトウェアライセンスファイルがあります。

ライセンスアクティベーション(説明付き)

インストールする前に、SLCを登録する必要があります(135ページのソフトウェアライセンスコードを登録するを参照)。インストール済みのXProtectVMSとXProtect拡張機能が機能し、個々のハードウェアデバイスからシステムにデータが送信されるようにするには、SLCに紐付けされた各ライセンスをアクティベートする必要があります。XProtectの全ライセンスタイプの概要については、107ページのライセンスタイプを参照してください。

ライセンスをアクティベートする方法は数種類あります。いずれの方法も**[ライセンス情報]**ウィンドウで行うことができます。どのアクティベーション方法が最適であるかは、組織でどのようなポリシーが掲げられているか、そしてマネジメントサーバーからインターネットにアクセスできるかどうかに応じて異なります。ライセンスをアクティベートする方法については、112ページのライセンスのアクティベートを参照してください。

XProtectライセンスシステムは柔軟な構造をしているため、XProtectVMSの初回ライセンスアクティベート以降、カメラを搭載したハードウェアデバイスを追加するたびにデバイスライセンスをアクティベートする必要はありません。この柔軟性について詳しくは、109ページのライセンスアクティベーションの猶予期間(説明付き)および109ページのアクティベーションなしのデバイスの変更(説明付き)を参照してください。

自動ライセンスアクティベーション(説明付き)

Milestoneでは、メンテナンスを容易にしつつ柔軟性を維持するためにも、組織のポリシーで許容されている場合は自動ライセンスアクティベーションを有効にするよう推奨しています。自動ライセンスアクティベーションを使用するには、マネジメントサーバーがオンラインになっている必要があります。自動ライセンスアクティベーションを有効にする方法については、112ページの自動ライセンスアクティベーションを有効にするを参照してください。

自動ライセンスアクティベーションを有効にすることで得られる利点

- ハードウェアデバイスを追加、削除、または交換してから、またはライセンスの使用に影響を及ぼすような変更を加えてから数分後に、システムによってハードウェアデバイスがアクティベートされます。そのため、ライセンスアクティベーションを手動で行うことはめったにありません。まれな例外については、108ページの手動ライセンスアクティベーションが引き続き必要な状況を参照してください。
- 「アクティベーションなしのデバイスの変更」の使用済み回数は常にゼロとなります。
- ハードウェアデバイスが猶予期間に入ったり、期限切れのリスクが生じたりすることがありません。
- 基本ライセンスのいずれかが14日以内に期限切れになる場合は、XProtectシステムは、追加の対策として、毎夜自動的にライセンスのアクティベーションを試みます。

手動ライセンスアクティベーションが引き続き必要な状況

システムに対して以下の変更を加える場合は、手動ライセンスアクティベーションが必要となります。

- 追加のライセンスを購入する(115ページの追加ライセンスの取得を参照)
- より新しいバージョン、またはより上位のVMSシステムにアップグレードする(354ページのアップグレード要件を参照)
- Milestone Careサブスクリプションを購入または更新する
- 「アクティベーションなしのデバイスの変更」の回数を増やす(109ページのアクティベーションなしのデバイスの変更(説明付き) を参照)

ライセンスアクティベーションの猶予期間(説明付き)

VMSをインストールしてデバイス(ハードウェアデバイス、Milestone Interconnectカメラ、ドアのライセンス) を追加する際には、自動ライセンスアクティベーションを有効にしていない限り、これらのデバイスは30日間の猶予期間のもとで稼働します。30日間の猶予期間が終了するにあたり、「アクティベーションなしのデバイスの変更」の回数がゼロになった場合は、ライセンスをアクティベートする必要があります。これを行わないと、デバイスから監視システムにビデオが送信されなくなります。

アクティベーションなしのデバイスの変更(説明付き)

XProtectライセンスシステムの構造は、「アクティベーションなしのデバイスの変更」機能によって柔軟なものとなっています。そのため、たとえライセンスを手動でアクティベートする場合でも、ハードウェアデバイスを追加または削除するたびに必ずしもライセンスをアクティベートする必要はありません。

アクティベーションなしのデバイスの変更数はインストールによって異なり、複数の変数に基づいて計算されます。詳細については、「109ページの「アクティベーションなしのデバイスの変更」の回数の算出(説明付き) 」を参照してください。

ライセンスを最後にアクティベートしてから1年が経過すると、「アクティベーションなしのデバイスの変更」の使用済み回数が自動的にゼロにリセットされます。リセットが発生したら、ライセンスをアクティベートせずに、ハードウェアデバイスを追加および交換し続けることができます。

長期航行中の船舶状の監視システムやインターネットにアクセスできない遠隔地の監視システムなど、監視システムが長期間オフラインの場合は、Milestoneリセラーに連絡し、アクティベーションなしのデバイスの変更数を増やすように依頼できます。

アクティベーションなしのデバイスの変更数を増やす資格があると考える理由を説明する必要があります。Milestoneは各リクエストを個別に決定します。アクティベーションなしのデバイスの変更数が増えた場合は、ライセンスを認証して、XProtectシステムで登録するライセンス数を増やす必要があります。

「アクティベーションなしのデバイスの変更」の回数の算出(説明付き)

「アクティベーションなしのデバイスの変更」の回数は、3つの変数から算出されます。Milestoneソフトウェアの複数のインストールがある場合は、変数はそれぞれに個別に適用されます。変数は以下のとおりです。

- アクティベーション済みライセンスの合計数の固定割合を示す**C%**。
- アクティベーションなしのデバイスの変更数の固定最小値を示す**Cmin**。
- アクティベーションなしのデバイスの変更数の固定最大値を示す**Cmax**。

アクティベーションなしのデバイスの変更数は、**Cmin**値より低くしたり、**Cmax**値より高くすることはできません。**C%**変数に基づいて計算された値は、システムの各インストールにあるライセンスアクティベーション済みデバイス数に応じて変化します。アクティベーションなしのデバイスの変更によって追加されたデバイスは、**C%**変数によるアクティベーションとしてカウントされません。

Milestoneは3つのすべての変数の値を定義します。値は予告なく変更される場合があります。変数の値は製品によって異なります。

C% = 15%、Cmin = 10、Cmax =100に基づく例

あなたはデバイスライセンスを100購入しました。続いて、100台のカメラをシステムに追加しました。自動ライセンスアクティベーションを有効にしない限り、「アクティベーションなしのデバイスの変更」の回数はゼロのままです。次に、ライセンスをアクティベートしたことで、「アクティベーションなしのデバイスの変更」の回数は15となりました。

あなたはデバイスライセンスを100購入しました。続いて100台のカメラをシステムに追加し、ライセンスをアクティベートしました。「アクティベーションなしのデバイスの変更」の回数は現在15です。次に、システムから1台のハードウェアデバイスを削除することにしました。現在99台のデバイスがアクティベートされており、「アクティベーションなしのデバイスの変更」の回数は14に減少しました。

あなたはデバイスライセンスを1000購入しました。続いて1000台のカメラをシステムに追加し、ライセンスをアクティベートしました。これで、「アクティベーションなしのデバイスの変更」の回数は100となります。**C%**変数によれば、「アクティベーションなしのデバイスの変更」の回数は150になるはずですが、**Cmax**変数に基づき、「アクティベーションなしのデバイスの変更」の回数は100に制限されています。

あなたはデバイスライセンスを10購入しました。続いて10台のカメラをシステムに追加し、ライセンスをアクティベートしました。**Cmin**変数により、「アクティベーションなしのデバイスの変更」の回数は現在10となります。**C%**変数のみに基づいて回数を算出した場合、結果は1となります(10の15% = 1.5、少数切り捨て) 。

あなたはデバイスライセンスを115購入しました。続いて100台のカメラをシステムに追加し、ライセンスをアクティベートしました。これで、「アクティベーションなしのデバイスの変更」の回数は15となります。次に、「アクティベーションなしのデバイスの変更」の回数15回分のうち15を使用して、さらに15台のカメラをアクティベーションなしで追加しました。この状態でシステムから50台のカメラを削除すると、「アクティベーションなしのデバイスの変更」は7に減少します。これは、15回分の「アクティベーションなしのデバイスの変更」として追加したカメラのうち、8台のカメラが猶予期間に入ったことを意味します。続いて、新しいカメラを50台追加しました。前回ライセンスをアクティベートした際に100台のカメラをアクティベートしたため、「アクティベーションなしのデバイスの変更」の回数は15回に戻り、猶予期間に入っていた8台のカメラも、「アクティベーションなしのデバイスの変更」の回数に再び含まれるようになります。50台の新しいカメラは猶予期間に入ります。

Milestone Care™(説明付き)

Milestone Careは、XProtect製品用の完全サービスおよびサポートプログラムの名称です。

これらはその存続期間にわたって提供されます。Milestone Careを使うと、サポートWebサイト(https://www.milestonesys.com/support/) にあるKnowledge Base記事、ガイド、チュートリアルなど、様々なタイプのセルフヘルプ資料にアクセスできます。

より高度なMilestone Careサブスクリプションを購入すると、さらに多くのメリットが得られます。

Milestone Care Plus

さらに、Milestone Care Plusサブスクリプションがある場合は、現在のXProtectVMS製品への無料アップデートにアクセスできるとともに、より高度なXProtectVMS製品にお得な価格でアップグレードできます。Milestone Care Plusには、次の追加機能もあります。

- カスタマーダッシュボードサービス
- スマートコネクト機能
- 完全なプッシュ型通知機能

Milestone Care Premium

Milestone Care Premiumサブスクリプションがある場合は、直接Milestoneサポートに連絡することもできます。Milestone Careサポートにお問い合わせの際には、Milestone IDに関する情報も併せてお伝えください。

高レベルのMilestone Careサブスクリプションの期間満了、更新、および購入

より上位のMilestone Care PlusおよびMilestone Care Premiumサブスクリプションタイプの有効期限は、**[インストールされている製品]**一覧の**[ライセンス情報]**ウィンドウに表示されます。117ページのインストール済みの製品を参照してください。

システムのインストール後にMilestone Careサブスクリプションを購入または更新した場合は、ライセンスを手動でアクティベートしない限り、Milestone Care情報が正しく表示されません。「113ページのライセンスをオンラインでアクティベーション」または「114ページのライセンスをオフラインでアクティベート」を参照してください。

ライセンスとハードウェアの交換(説明付き)

システム内のカメラに障害が発生したため、または他の理由のためにカメラを新しいものと交換するにあたり、実行すべきベストプラクティスがいくつか存在します。

カメラをレコーディングサーバーから削除すればデバイスライセンスを開放することができますが、旧カメラのすべてのデータベース(カメラ、マイク、入出力)と設定へのアクセスが完全に失われてしまいます。旧カメラのデータベースへのアクセスを維持し、新しいカメラと交換した際にこれらの設定を再利用できるようにするには、以下の該当するオプションを使用します。

カメラを類似品と交換する

カメラを類似品(同じメーカー、ブランド、モデルなど)と交換し、かつ新しいカメラに旧カメラと同じIPアドレスを割り当てれば、旧カメラのすべてのデータベースへの完全なアクセスを維持できます。新しいカメラは、旧カメラと同じデータベースおよび設定を引き続き使用します。この場合、Management Clientで設定を一切変更せずに、旧カメラのネットワークケーブルを新しいカメラに移します。

カメラを非類似品に交換する

カメラを非類似品(異なるメーカー、ブランド、モデルなど)と交換する場合は、**[ハードウェアの交換]**ウィザード(327ページのハードウェアの交換を参照)を使用して、旧カメラのすべての関連データベースを新しいカメラにマップし、旧カメラの設定を再利用する必要があります。

ハードウェア交換後のライセンスアクティベーション

自動ライセンスアクティベーションを有効にしている場合(「112ページの自動ライセンスアクティベーションを有効にする」を参照)、新しいカメラは自動的にアクティベートされます。

自動ライセンスアクティベーションが無効にされており、かつ「アクティベーションなしのデバイスの変更」の許容回数がすべてゼロになっている場合(「109ページのアクティベーションなしのデバイスの変更(説明付き)」を参照)、ライセンスを手動でアクティベートする必要があります。ライセンスの手動アクティベーションについて詳しくは、「113ページのライセンスをオンラインでアクティベーション」または「114ページのライセンスをオフラインでアクティベート」を参照してください。

ライセンスの概要を確認

保有中のSLCと購入したライセンスの数、そしてそのステータスについて大まかに確認したいという状況は多々あります。一例を以下に示します。

- 1つまたは複数のハードウェアデバイスを追加したいけれども、未使用のデバイスライセンスが残っているのか、あるいはライセンスを新たに購入すべきなのか確認したい
- 一部のハードウェアデバイスの猶予期間がまもなく終了するのかどうか知りたい。じきに終了するのであれば、VMSにデータが送信されなくなる前にデバイスをアクティベートしたい
- これまでのやり取りから、サポートを受けるためには自分のSLCとMilestone CareIDを提示しなくてはならないことは把握しているが、どれを提示する必要があるかを知りたい
- XProtectを多数インストールしており、すべてのインストールに対して同一のSLCを使用しているが、ライセンスがどこで使用されているか、またはその状態について把握したい

このような情報(または追加の情報)は、**[ライセンス情報]**ウィンドウで確認できます。

[ライセンス情報]ウィンドウは、**[サイトナビゲーション]**ペイン -> **[基本]**ノード -> **[ライセンス情報]**の順に選択することで開くことができます。

[ライセンス情報]ウィンドウで利用できる各種情報や機能については、「116ページのライセンス情報ウィンドウ」を参照してください。

ライセンスのアクティベート

ライセンスをアクティベートする方法は数種類あります。いずれの方法も**[ライセンス情報]**ウィンドウで行うことができます。どのアクティベーション方法が最適であるかは、組織でどのようなポリシーが掲げられているか、そしてマネジメントサーバーからインターネットにアクセスできるかどうかに応じて異なります。

[ライセンス情報]ウィンドウは、**[サイトナビゲーション]**ペイン -> **[基本]**ノード -> **[ライセンス情報]**の順に選択することで開くことができます。

[ライセンス情報]ウィンドウで利用できる各種情報や機能については、「116ページのライセンス情報ウィンドウ」を参照してください。

自動ライセンスアクティベーションを有効にする

Milestoneでは、メンテナンスを容易にしつつ柔軟性を維持するためにも、組織のポリシーで許容されている場合は自動ライセンスアクティベーションを有効にするよう推奨しています。自動ライセンスアクティベーションを使用するには、マネジメントサーバーがオンラインになっている必要があります。

自動ライセンスアクティベーションを有効にすることで得られる利点についてすべて把握したい場合は、「108ページの自動ライセンスアクティベーション(説明付き)」を参照してください。

1. **[サイトナビゲーション]**ペイン-> **[基本]**ノード-> **[ライセンス情報]**で、**[自動ライセンスアクティベーションを有効にする]**を選択します。
2. 自動ライセンスアクティベーションで使用するユーザー名とパスワードを入力します。
   - 既存ユーザーの場合は、ユーザー名とパスワードを入力して、「Software Registration System(ソフトウェア登録システム)」にログインします。
   - 新しいユーザーの場合は、**[新しいユーザーの作成]**リンクをクリックして新しいユーザーアカウントを設定し、登録手順を実行します。ソフトウェアライセンスコード(SLC)をまだ登録していない場合は、登録してください。

   資格情報はマネジメントサーバーのファイルに保存されます。
3. **OK**をクリックします。

自動ライセンスアクティベーション用のユーザー名またはパスワードを後から変更する場合は、**[アクティベーション資格情報の編集]**リンクをクリックします。

自動ライセンスアクティベーションを無効にする

組織において自動ライセンスアクティベーションの使用が許可されていない場合、または単に気が変わった場合は、自動ライセンスアクティベーションを無効にできます。

どのような形で無効にするかは、今後自動ライセンスアクティベーションを再び使用する予定があるかどうかに応じて異なります。

無効にするが、今後の使用に備えてパスワードを維持する場合:

1. **[サイトナビゲーション]**ペイン-> **[基本]**ノード-> **[ライセンス情報]**で、**[自動ライセンスアクティベーションを有効にする]**を選択解除します。パスワードとユーザー名はマネジメントサーバーにそのまま保存されます。

無効にしてパスワードも削除する場合:

1. **[サイトナビゲーション]**パネル->**[基本]**ノード->**[ライセンス情報]**で、**[アクティベーション資格情報の編集]**をクリックします。
2. **[パスワードの削除]**をクリックします。
3. パスワードとユーザー名をマネジメントサーバーから削除することを確認します。

ライセンスをオンラインでアクティベーション

たとえマネジメントサーバーからインターネットにアクセスできる場合でも、アクティベーションプロセスを手動で開始するのが最も簡単なアクティベーションの方法となります。

1. **[サイトナビゲーション]**ペイン **-> [基本]** ノード **-> [[ライセンス情報]**で、**[ライセンスを手動でアクティベート]**を選択し、**[オンライン]**を選択します。
2. **[オンライン認証]**ダイアログボックスが開きます。
   - 既存のユーザーの場合は、ユーザー名とパスワードを入力します。
   - 新規ユーザーの場合は、**[Create new user(新しいユーザーを作成)]** リンクをクリックして、新しいユーザーアカウントを設定します。ソフトウェアライセンスコード(SLC) をまだ登録していない場合は、登録してください。
3. **OK**をクリックします。

オンラインアクティベーション中にエラーメッセージが発生した場合は、画面の手順に従って問題を解決するか、Milestoneサポートにお問い合わせください。

ライセンスをオフラインでアクティベート

組織においてマネジメントサーバーからのインターネットアクセスが許可されてない場合は、ライセンスを手動かつオフラインでアクティベートする必要があります。

1. **[サイトナビゲーション]**ペイン **-> [基本]** ノード **-> [ライセンス情報]**で、**[ライセンスを手動でアクティベート] > [オフライン] > [ライセンスをアクティベーション用にエクスポート]**を選択して、(ライセンスが必要な追加ハードウェアデバイスと他の要素に関する情報が含まれる) ライセンスリクエストファイル(.lrq)をエクスポートします。
2. ライセンスリクエストファイル(.lrq)には、お使いのSLCと同じ名前が自動的に付けられます。複数のサイトをお持ちの場合は、ファイルがどのサイトに属しているかを容易に特定できるよう、必ずファイルの名前を変更してください。
3. ライセンスリクエストファイルを、インターネットアクセスが可能なコンピュータにコピーし、弊社のWebサイト(https://online.milestonesys.com/) にログインしてアクティベート済みのソフトウェアライセンスファイル(.lic)を取得します。
4. 取得した.licファイルを、Management Clientがインストールされたコンピュータにコピーします。このファイルには、ライセンスリクエストファイルと同じ名前が付けられています。
5. **[サイトナビゲーション]**ペイン **-> [基本]** ノード **-> [ライセンス情報]**で、**[ライセンスをオフラインでアクティベート] > [アクティベート済みライセンスのインポート]**を選択し、続いてアクティベート済みソフトウェアライセンスファイルを選択してこれをインポートしてから、ライセンスをアクティベートします。
6. **終了**をクリックして、アクティベーションプロセスを終了します。

猶予期間が切れた後にライセンスをアクティベートする

ライセンスを手動でアクティベートすることを決定したにもかかわらず、猶予期間中に(ハードウェアデバイス、Milestone Interconnectカメラ、ドアのライセンスなどを) アクティベートすることを忘れてしまった場合、そのライセンスを使用しているデバイスが利用不可となり、これらのデバイスから監視システムにデータが送信されなくなります。

たとえライセンスの猶予期間が切れても、デバイスの構成と設定は保存されるため、次回ライセンスをアクティベートした際に再利用できます。

利用不可となったデバイスを再度有効にするには、ご希望の方法でライセンスを手動でアクティベートしてください。詳細については、「114ページのライセンスをオフラインでアクティベート」または「113ページのライセンスをオンラインでアクティベーション」を参照してください。

追加ライセンスの取得

ハードウェアデバイス、Milestone Interconnectシステム、ドアなどの要素を、現在ライセンスで許容されている数よりも多く追加したい場合、またはすでに許容数を超えて追加している場合に、これらのデバイスからシステムにデータが送信されるようにするには、追加のライセンスを購入する必要があります:

- 使用しているシステムの追加ライセンスを入手するには、XProtect製品の代理店にお問い合わせください。

既存の監視システムのバージョンに対して新しいライセンスを購入した場合:

- ライセンスを手動でアクティベートし、新しいライセンスを入手します。詳細については、「113ページのライセンスをオンラインでアクティベーション」または114ページのライセンスをオフラインでアクティベート「」を参照してください。

新しいライセンスと、アップグレード済みの監視システムのバージョンを購入した場合:

- 更新されたソフトウェアライセンスファイル(.lic)、新しいライセンス、新しいバージョンを受け取ります。新しいバージョンのインストール中には、新しいソフトウェアライセンスファイルを使用する必要があります。詳細については、「354ページのアップグレード要件」を参照してください。

ソフトウェアライセンスコードの変更

一時ソフトウェアライセンスコード(SLC)を実行している場合や、より上位のXProtect製品にアップグレードした場合は、SLCを恒久版または上位版のSLCに変更できます。新しいソフトウェアライセンスファイルを入手した場合、アンインストールや再インストールを行うことなく、SLCを変更できます。

この操作はマネージメントサーバー上でローカルで、もしくはManagement Clientから実行できます。

マネジメントサーバーのトレイアイコンから

1. マネジメントサーバーで、タスクバーの通知エリアへ移動します。

2. **マネジメントサーバー**アイコンを右クリックし、**ライセンスの変更**を選択します。
3. **ライセンスのインポート**をクリックします。
4. 次に、この目的で保存したソフトウェアライセンスファイルを選択します。完了すると、ライセンスの**[ライセンスのインポート]**ボタンのすぐ下に、選択したソフトウェアライセンスファイルの場所が追加されます。
5. **[OK]**をクリックすれば、SLCの登録準備が整います。「135ページのソフトウェアライセンスコードを登録する」を参照してください。

変更前：Management Client

1. 受領した.licファイルをManagement Clientがインストールされたコンピューターにコピーします。
2. **[サイトナビゲーション]** ペイン -> **[基本]** ノード -> **[ライセンス情報]**で、**[ライセンスをオフラインでアクティベート]** > **[アクティベート済みライセンスのインポート]** を選択し、インポートするソフトウェアライセンスファイルを選択します。
3. 開いたら、ソフトウェアライセンスファイルが現在使用中のライセンスファイルとは異なることに同意します。
4. これでSLCへの登録準備が整いました。「135ページのソフトウェアライセンスコードを登録する」を参照してください。

ソフトウェアライセンスファイルは、インポートされ変更されますが、アクティベートされません。忘れずにライセンスをアクティベートしてください。詳細については、「112ページのライセンスのアクティベート」を参照してください。

XProtect Essential+を実行中は、マネジメントサーバーのトレイアイコンからのみライセンスを変更できます。Management Clientからライセンスを変更することはできません。

ライセンス情報ウィンドウ

[ライセンス情報]ウィンドウでは、このサイトまたは他の全サイトの両方で同一のソフトウェアライセンスファイルを共有している全ライセンスに加え、現在のMilestone Careサブスクリプションを追跡できるほか、ライセンスをどのようにアクティベートするかを指定できます。

[ライセンス情報]ウィンドウは、**[サイトナビゲーション]**ペイン -> **[基本]** ノード -> **[ライセンス情報]**の順に選択することで開くことができます。

XProtectライセンスシステムがどのように機能するかについての概要は、106ページのライセンス(説明付き)で説明されています。

ライセンス付与先

ライセンス情報ウィンドウのこのエリアには、ソフトウェア登録中に入力されたライセンス所有者の連絡先情報が一覧表示されます。

[ライセンス付与先]領域が表示されない場合は、ウィンドウ右下の**[更新]**ボタンをクリックしてください。

[詳細の編集]をクリックして、ライセンス所有者情報を編集します。**[エンドユーザーライセンス契約]**をクリックして、インストール前に同意したエンドユーザーライセンス契約に目を通します。

Milestone Care

ここでは、現在のMilestone Care™サブスクリプションの情報を確認できます。現在のサブスクリプションの有効期限は、その下の**インストール済みの製品**一覧に表示されます。

Milestone Careの詳細については、リンクを使用するか、110ページのMilestone Care™(説明付き)を参照してください。

インストール済みの製品

XProtect VMS向けにすべてのインストールされた基本ライセンスと、同じソフトウェアライセンスファイルを共有するXProtect拡張機能に関する次の情報が一覧表示されます。

- 製品とバージョン
- 製品のソフトウェアライセンスコード(SLC)
- SLCの有効期限(通常は無期限)
- Milestone Care Plusサブスクリプションの有効期限
- Milestone Care Premiumサブスクリプションの有効期限。

Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 20 R	M01-C01-211-01-	Unlimited	16-11-20	16-11-20
Milestone XProtect Smart Wall	M01-P03-100-01-	Unlimited	Unlimited	
Milestone XProtect Access	M01-P01-011-01-	Unlimited	Unlimited	
Milestone XProtect Transact	M01-P08-100-01-	Unlimited	Unlimited	

ライセンス概要 - すべてのサイト

アクティベート済みのデバイスライセンスと、ソフトウェアライセンスファイルに含まれる他のライセンスの数、ならびにシステムで利用可能なライセンスの総数が表示されます。追加ライセンスを購入せずにシステムを拡張できるかどうかを簡単に確認できます。

他のサイトでアクティベーションされたライセンスのステータスの詳細概要については、**ライセンス詳細 - すべてのサイト**リンクをクリックします。どのような情報が表示されるかは、下記の「**ライセンス詳細 - 現在のサイト**」セクションを参照してください。

License Overview - All sites License Details - All Sites...

License Type	Activated
Device Licenses	51 out of 100
Milestone Interconnect Camera	0 out of 100
Access control door	9 out of 2002
Transaction source	1 out of 101

XProtect拡張機能用のライセンスをお持ちの場合は、**サイトナビゲーション**ペインで、これらのXProtect拡張機能に特有のノードのもとで追加の詳細を確認できます。

ライセンス詳細 - 現在のサイト

アクティベート済み列には、アクティベート済みのデバイスライセンスの数、またはこのサイトの他のライセンスの数が表示されます。

アクティベーションなしの変更列では、「アクティベーションなしのデバイスの変更」の使用済み回数(109ページのアクティベーションなしのデバイスの変更(説明付き)を参照)や、1年あたりの「アクティベーションなしのデバイスの変更」の許容回数を確認することもできます。

アクティベートしていないため猶予期間で実行されているライセンスがある場合は、**猶予期間**列に一覧表示されます。期限切れの最初のライセンスの有効期限は、表の下に赤で表示されます。

猶予期間が終了する前にライセンスをアクティベートし忘れた場合は、ビデオがシステムに送信されなくなります。これらのライセンスは**終了した猶予期間**列に表示されます。詳細については、「114ページの猶予期間が切れた後にライセンスをアクティベートする」を参照してください。

使用可能なライセンス数よりも使用済みライセンス数の方が多い場合は、**ライセンスなし**列に一覧表示され、システムで使用できません。詳細については、「115ページの追加ライセンスの取得」を参照してください。

猶予期間が切れた状態またはライセンスが存在しない状態で、お持ちのライセンスが猶予期間に入っている場合、Management Clientにログインするたびに、その旨をリマインドするメッセージが表示されます。

License Details - Current Site: [redacted]

License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Device Licenses	32	0 out of 10	0	0	0
Milestone Interconnect Camera	11	N/A	0	0	0
Access control door	9	N/A	0	0	0
Transaction source	1	N/A	0	0	0

複数のライセンスを使用しているハードウェアデバイスが存在する場合、**ライセンス詳細 - 現在のサイト**一覧の下に**ここをクリックしてデバイスライセンスの詳細レポートを開く**リンクが表示されます。リンクをクリックすれば、デバイスライセンスをいくつ所有しているか、そしてこれらのデバイスがそれぞれいくつのライセンスを必要としているかを確認できます。

Management Clientでは、ライセンスのないハードウェアデバイスは感嘆符「！」表示で識別されます。感嘆符「！」は他の目的でも使用されます。感嘆符の上にマウスを置くと、目的が表示されます。

ライセンスアクティベーションの機能

3つの表の下には、次のアイテムがあります。

- 自動ライセンスアクティベーションを有効にするチェックボックスと、自動アクティベーションのユーザー認証情報を編集するためのリンク。詳細については、108ページの自動ライセンスアクティベーション(説明付き)および112ページの自動ライセンスアクティベーションを有効にするを参照してください。
  自動アクティベーションに失敗した場合、失敗メッセージが赤で表示されます。詳細を表示するには、**詳細**リンクをクリックします。
  一部のライセンス(XProtect Essential+やなど)は自動ライセンスアクティベーションが有効になった状態でインストールされるため、これを無効にすることはできません。
- ライセンスをオンラインまたはオフラインで手動アクティベートするためのドロップダウンリスト。詳細については、113ページのライセンスをオンラインでアクティベーションおよび114ページのライセンスをオフラインでアクティベートを参照してください。
- ウィンドウの右下部分では、ライセンスが最後に(自動または手動で)アクティベートされたのはいつであったか、またはウィンドウがいつリフレッシュされたかについて確認できます。日付スタンプは、ローカルコンピュータではなく、サーバーから取得されます。


Enable automatic license activation
Edit activation credentials...
Activate License Manually...
Online
Offline
Last activated: 17. november 20 15:02:00
Information refreshed: 28. januar 20 11:39:11

要件と検討事項

サマータイム(説明付き)

夏時間 (DST) は、夕方の日照時間を長く、朝の日照時間を短くするために、時計を進める制度です。DSTの使用は、国/地域によって異なります。

監視システムでの作業では、本質的に時間が重要であるため、システムがどのようにDSTに対応するかを知っておくことが重要です。

> DST期間中、またはDST期間の録画がある場合は、DST設定を変更しないでください。

春:標準時間からDSTへ切り替える

標準時間からDSTへの変更は、時計を1時間進めるのであまり問題ではありません。

例:

時計は02:00(標準時間)から03:00(DST)へと進められるので、その日は23時間となります。その場合、その朝の02:00から03:00の間にデータはありません。その日にはその時間は存在しなかったためです。

秋:DSTから標準時間へ切り替える

秋にDSTから標準時間へ切り替えるとき、時計を1時間戻します。

例:

時計は02:00(DST)から01:00(標準時間)に戻されるので、その日は25時間となります。この場合、01:59:59になると、その後すぐに01:00:00に戻ります。システムが応答しなかった場合、基本的にはその時間を再録画します。たとえば、最初の01:30は、2回目の01:30によって上書きされます。

この問題が発生しないようにするために、システム時刻が5分以上変更された場合、現在のビデオがアーカイブされます。クライアントでは01:00時間の最初の発生を直接表示できませんが、データは録画され、安全です。XProtect Smart Clientでこのビデオを参照するには、アーカイブされたデータベースを直接開きます。

タイムサーバ(説明付き)

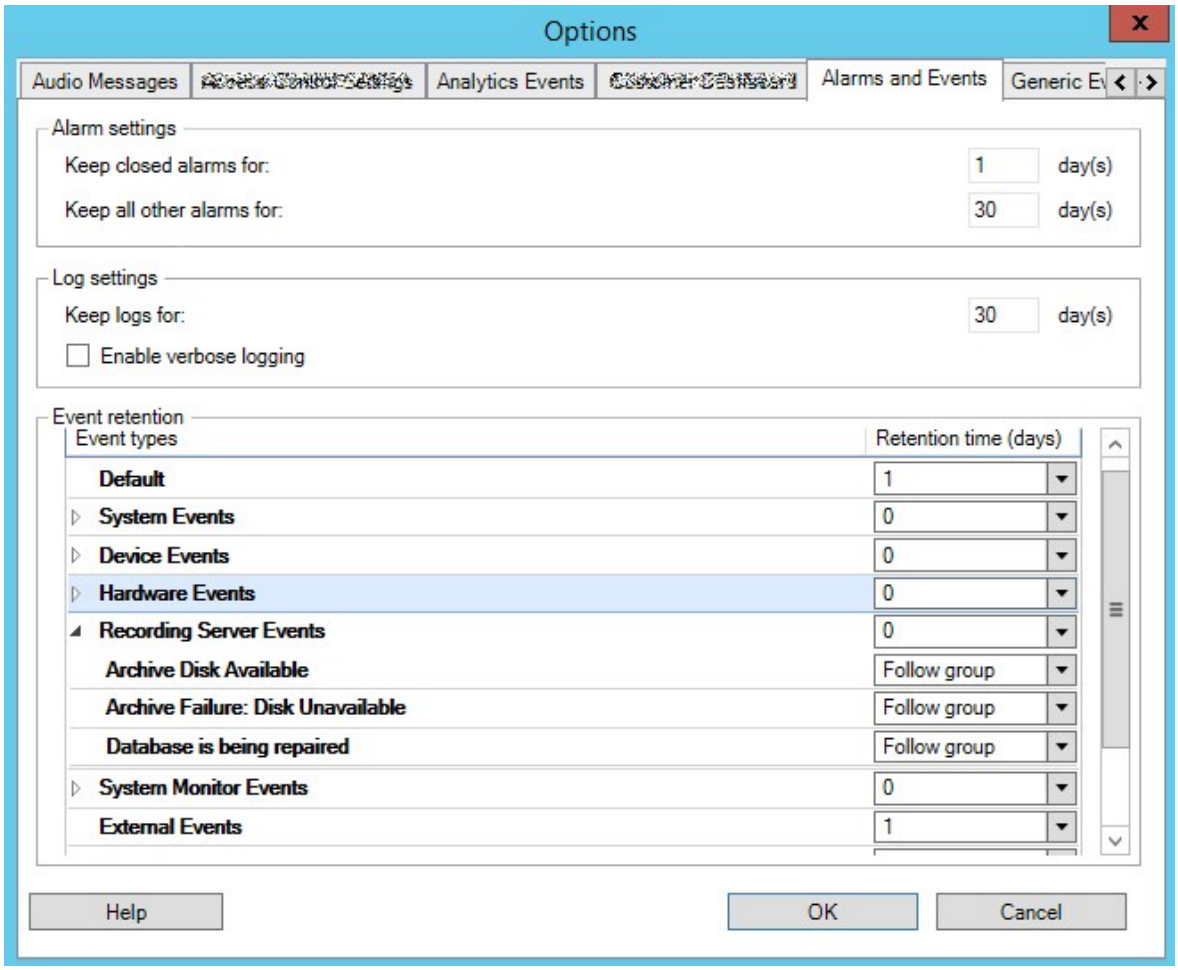
システムが画像を受信すると、ただちにタイムスタンプが付けられます。カメラは別個のユニットであり、別個のタイミングデバイスを持っているので、カメラの時刻と使用しているシステムの時刻が完全に一致していないことがあります。これが混乱の原因になる場合があります。カメラがタイムスタンプをサポートしている場合、Milestoneでは、一貫性のある同期を行うために、タイムサーバーによってカメラとシステムの時刻を自動同期することを推奨しています。

タイムサーバーを構成する方法については、Microsoft Webサイト(https://www.microsoft.com/)で「**タイムサーバー**」や「**タイムサービス**」などについて検索してください。

データベースのサイズを制限

SQLServerデータベース(「33ページのSQLServerインストールとデータベース(説明付き)」を参照)のサイズが、システムのパフォーマンスに影響が及ぶほど増大するのを防ぐため、各種イベントとアラームを何日間データベースに保存するかを指定できます。

1. **ツール**メニューを開きます。
2. **オプション>アラームとイベント**タブをクリックします。



3. 必要な設定を行います。詳細については、「377ページの[アラームおよびイベント]タブ(オプション)」を参照してください。

Ipv6およびIpv4(説明付き)

システムでは、IPv6とIPv4がサポートされています。XProtect Smart Clientでも同様。

IPv6はインターネットプロトコル(IP)の最新バージョンです。インターネットプロトコルは、形式とIPアドレスの使用を決定します。IPv6は、依然としてより広く使用されているIPバージョンIPv4と共存しています。IPv6は、IPv4のアドレス枯渇を解決するために開発されました。IPv4アドレスは32ビット長であるのに対し、IPv6アドレスは128ビットの長さです。

つまりインターネットのアドレス帳の一意アドレスの数が43億から340澗(10の34乗)へ増えたという意味です。増大係数は79000 (10の27乗)。? (10の27乗)。増大係数は79000? (10の27乗)大係数は79000? (10の27乗)。

ますます多くの組織が、ネットワークにIPv6を実装しています。たとえば、すべての米国連邦機関のインフラストラクチャは、IPv6準拠である必要があります。このマニュアルに記載されている例および図は、現在も最も一般的に使用されているIPバージョンである、IPv4の使用を反映しています。IPv6も同様に問題なく動作します。

IPv6 でのシステムの使用 (説明付き)

システムでIPv6を使用する場合は、次の条件が適用されます。

サーバー

サーバーでは、IPv4に加えて、IPv6もよく使用されます。ただし、システム内の1つのサーバーのみ(例 : マネジメントサーバー、レコーディングサーバー) で特定のIPバージョンが必要とされる場合、システム内のすべての他のサーバーが、同じIPバージョンを使用して通信しなければなりません。

例 : システム内のすべてのサーバー(1つを除く) は、IPv4とIPv6の両方を使用できます。例外は、IPv6のみ使用できるサーバーです。これは、すべてのサーバーがIPv6を使用して相互に通信する必要があることを意味します。

デバイス

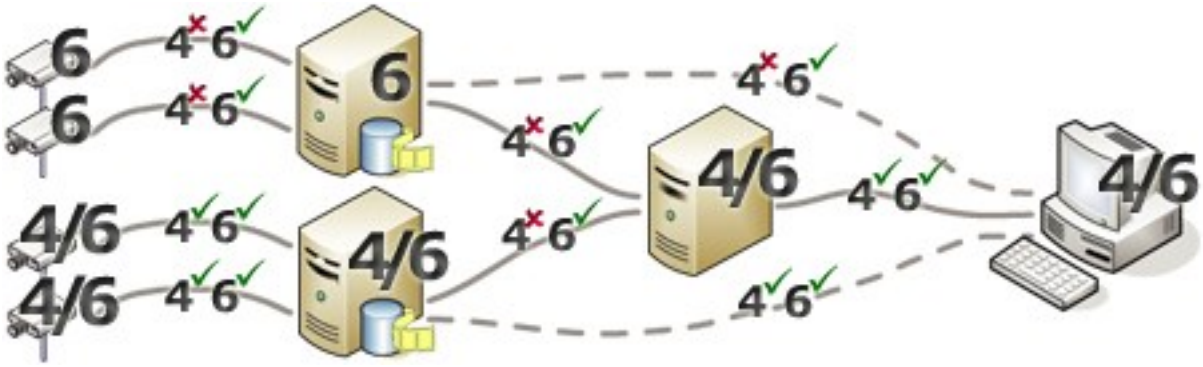
ネットワーク設備と対象のレコーディングサーバーでもデバイスのIPバージョンがサポートされていれば、サーバー通信で使用されているIPバージョンとは異なるIPバージョンのデバイス(カメラ、入力、出力、マイク、スピーカー) を使用できます。下記の図もあわせて参照してください。

クライアント

お使いのシステムがIPv6を使用している場合、ユーザーはXProtect Smart Clientを使用して接続する必要があります。XProtect Smart Clientは、IPv4だけではなくIPv6もサポートします。

システム内の1つ以上のサーバーがIPv6**だけしか**使用できない場合は、XProtect Smart Clientユーザーは、他のサーバーとの通信にIPv6を**使用しなければなりません**。このようなケースでは、XProtect Smart Clientのインストールは厳密には最初の認証のためにマネジメントサーバーに接続し、その後録画にアクセスするために必要なレコーディングサーバーに接続することに注意してください。

ただし、ネットワーク設備で異なるIPバージョン間の通信がサポートされており、コンピュータ上にIPv6プロトコルがインストールされている場合、XProtectSmartClientユーザーはIPv6ネットワーク上にある必要はありません。図もあわせて参照してください。
クライアントコンピュータにIPv6をインストールするには、コマンドプロンプトを開き、***ipv6install***と入力して**[ENTER]**を押します。
図例



例：システム内の1つのサーバーが、IPv6のみを使用しているため、そのサーバーとのすべての通信で、IPv6を使用する必要があります。ただし、そのサーバーはシステム内のすべての他のサーバー間の通信に使用されるIPバージョンも決定します。

IPv6アドレスの書き方(説明付き)

IPv6のアドレスは通常、4つの16進数から成るブロック8つで記述され、各ブロックがコロンで分離されています。

例：*2001:0B80:0000:0000:0000:0F80:3FA8:18AB*

アドレスは、ブロック内の先頭のゼロを削除することで、短縮できます。4桁のブロックの一部は、ゼロのみで構成されている場合もあることに注意してください。0000ブロックなどの番号が連続している場合、そのアドレスは、0000ブロックを2つのコロンに置き換えることによって短縮できます(アドレス内にそのような2つのコロンが1つだけである場合)。

例：
例：*2001:0B80:0000:0000:0000:0F80:3FA8:18AB*は、次のように短縮できます。

2001:B80:0000:0000:0000:F80:3FA8:18AB 先頭のゼロを削除した場合、または

*2001:0B80::0F80:3FA8:18AB*0000ブロックを削除した場合、または

*2001:B80::F80:3FA8:18AB*先頭のゼロと0000ブロックを削除した場合。

URLでのIPv6アドレスの使用

IPv6アドレスにはコロンが含まれます。ただし、コロンはまた、他の種類のネットワークアドレス指定構文でも使用されます。たとえば、IPv4は、IPアドレスとポート番号の両方がURLで使用された場合、コロンを使用して分離します。IPv6は、この原理を継承しました。したがって、混乱を避けるために、IPv6アドレスがURL内で使用される場合にIPv6アドレスを角括弧で囲みます。

IPv6アドレスを持つURLの**例**：
http:///[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]、*つまり、これは次のように短縮できます。*

例：*http:///[2001:B80::F80:3FA8:18AB]*IPv6アドレスとポート番号を持つURLの**例**：
http:///[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]:1234、*つまり、これは次のように短縮できます。例：http://[2001:B80::F80:3FA8:18AB]:1234*

IPv6の詳細については、IANA Webサイト(https://www.iana.org/numbers/)などを参照してください。IANA(Internet Assigned Numbers Authority、インターネットで利用されるアドレス資源の管理機関)は、IPアドレス指定の世界的な調整を行う組織です。

仮想サーバー

システム コンポーネント バーチャルWindows® サーバー上で VMware® や Microsoft® Hyper-V®.

仮想化は、多くの場合ハードウェアリソースの利用を向上させるために使用されています。通常、ハードウェアのホストサーバーで実行される仮想サーバーでは、同時に仮想サーバーに大きな負荷を与えることはありません。ただし、レコーディングサーバーは、すべてのカメラやビデオストリーミングを録画します。これにより、CPU、メモリ、ネットワーク、およびストレージシステムに高い負荷がかかります。そのため、仮想サーバーで実行した場合も、多くの場合は利用できるリソースをすべて使用してしまうので、仮想化の通常のメリットの大部分は活かされなくなってしまいます。

仮想環境で実行する場合、デフォルト設定を変更した上で、仮想サーバーに割り当てられるのと同じ量のメモリをハードウェアホストが持ち、レコーディングサーバーを実行している仮想サーバーが十分なCPUと記憶を割り当てられていることが重要です。設定によって異なりますが、通常、レコーディングサーバーには2 ~ 4 GBのメモリが必要です。もうひとつの問題は、ネットワークアダプタの割り当てとハードディスクのパフォーマンスです。レコーディングサーバーを実行している仮想サーバーのホストサーバーに、物理的ネットワークアダプタを割り当てるとします。これによって、ネットワークアダプタが他の仮想サーバーへのトラフィックで過負荷にならないようにすることが簡単に実現できます。ネットワークアダプタを複数の仮想サーバーで使用すると、設定された量の画像を取得および録画していないレコーディングサーバーに、ネットワークトラフィックが流入してしまいます。

複数のマネジメントサーバー(クラスタリング) (説明付き)

マネジメントサーバーは、サーバークラスタ内の複数のサーバーにインストールできます。これにより、システムのダウンタイムがほとんどなくなります。クラスタ内のサーバーで障害が発生すると、クラスターにある別のサーバーが、マネジメントサーバーを実行している障害のあるサーバーのジョブを自動的に引き継ぎます。

監視の設定毎に有効なマネジメントサーバーは1つしか持てませんが、障害の場合に他のマネジメントサーバーが代わりに使われるように設定できます。

> デフォルトで、Management Serverサービスはフェールオーバー発生回数を6時間で2回に制限しています。この制限を超えると、Management Serverサービスはクラスタリングサービスによって自動的に開始されません。この制限はニーズに合わせて変更できます。

クラスタリングの要件

- Microsoft Windows Server 2016以降がインストールされている2台のマシン。以下を確認してください。
  - クラスタノードとして追加したいすべてのサーバーが、同じWindows Serverバージョンを実行している
  - クラスタノードとして追加したいすべてのサーバーが、同じドメインに加えられている
  - ローカル管理者としてWindowsアカウントにログインするアクセス権限を持っている

  Microsoft Windowsサーバーのクラスタについては、フェールオーバークラスタ(https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster) を参照してください。

- Microsoft SQL Serverのインストール

  外部SQL Server、ならびにサーバークラスタ**外部**にインストールされたデータベース、**または**サーバークラスタ内の**内部**SQL Serverサービス(クラスタ化)のいずれか(内部SQL Serverサービスの作成には、クラスタSQL Serverとして機能することのできるMicrosoft® SQL Server® StandardまたはMicrosoft® SQL Server® Enterpriseエディションが必要)。

  > マネジメントサーバーをデータベースに接続する際は、システムの設定に応じて、現在のシステム設定のパスワードを提供するよう求められることがあります。315ページのシステム設定パスワード(説明付き)を参照してください。

> フェールオーバークラスターを使用している場合は、Server Configuratorで作業を始める前にクラスターを一時停止するようお勧めします。変更の適用中にServer Configuratorでサービスを停止する必要があり、フェールオーバークラスター環境がこの操作を妨害する可能性があるためです。

記録データベースを破損から守る

カメラデータベースが破損する可能性があります。このような問題を解決するために、いくつかのデータベース修理オプションが存在します。しかしMilestoneは、カメラデータベースが破損していないことを確認する手順を実行することをお勧めします。

ハードディスク障害:ドライブの保護

ハードディスクドライブは機械装置であり、外的な要因に対して脆弱です。以下は、ハードディスクドライブを傷つけ、カメラデータベースの破損を引き起こす可能性がある外部要因の例です。

- 振動(監視システムサーバーとその周囲が安定していることを確認してください)
- 高温(サーバーが適切に換気されていることを確認してください)
- 強力な磁場(避けてください)
- 停電(必ず無停止電源装置(UPS)を使用してください)
- 静電気(ハードディスクドライブを取り扱う場合には、必ずご自身を接地してください)
- 火災、水など(回避)

Windowsタスクマネージャー:プロセスを終了する際は注意してください

Windowsタスクマネージャで作業するときには、監視システムに影響を与えるプロセスを終了させないように注意してください。Windowsタスクマネージャで**[プロセスの終了]**をクリックして、アプリケーションまたはシステムサービスを終了すると、プロセスには、終了される前にその状態またはデータを保存する機会が与えられません。その結果として、カメラデータベースが破損する可能性があります。

Windowsタスクマネージャは通常、プロセスを終了しようとすると警告を表示します。プロセスを終了しても監視システムに影響がないことに確信が持てない場合は、警告メッセージでプロセスを終了するか尋ねられた場合に**いいえ**をクリックします。

停電:UPSを使用

データベースが破損する最大の原因として、ファイルが保存されず、オペレーティングシステムが適切に終了されずに、レコーディングサーバーが突然にシャットダウンすることが挙げられます。これは、停電、または誰かが誤ってサーバーの電源コードを抜いてしまった場合などに発生することがあります。

レコーディングサーバーが突然シャットダウンしないように保護するための最善の方法は、各レコーディングサーバーにUPS(無停電電源装置)を備え付けることです。

UPSは、電池駆動の第2電源として動作して、電源異常が発生した場合に、開いているファイルを保存して安全にシステムの電源を切るために必要な電源を提供します。UPSの仕様はさまざまですが、多数のUPSには、開いているファイルの自動保存、システム管理者へのアラート発行などを行うソフトウェアが含まれています。

組織の環境に適切な種類のUPSを選択することは、個別のプロセスです。ニーズを評価する際には、停電時にUPSが提供する必要のある実行時間を考慮に入れてください。開いているファイルを保存し、オペレーティングシステムを正しくシャットダウンするには、数分かかる場合があります。

SQL Serverデータベーストランザクションログ(説明付き)

変更がSQL Serverデータベースに書き込まれるたびに、SQL Serverデータベースによってその変更がトランザクションログに記録されます。

トランザクションログを使用すれば、Microsoft® SQL Server Management Studioを介してSQL Serverデータベースに加えられた変更をロールバックし、元に戻すことができます。デフォルトでは、SQL Serverデータベースには自身のデータベースログが無期限に保管されます。つまり、トランザクションログのエントリ数は時間とともに増えていきます。トランザクションログはデフォルトでシステムドライブに配置されており、そのサイズが増え続けることでWindowsが正常に実行されなくなるおそれがあります。

このような状況を避けるため、トランザクションログを定期的にフラッシュするようお勧めします。フラッシュを行ってもトランザクションログファイルが小さくなることはありませんが、その内容がクリーンアップされることから、制御不能な事態にまで拡大することを防ぐことができます。VMSシステムがトランザクションログをフラッシュすることはありません。SQL Serverでは、トランザクションログを複数の方法でフラッシュできますMicrosoftサポートページ(https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017)にアクセスして、*トランザクションログの切り捨て*について検索してください。

最低限のシステム要件

さまざまなVMSアプリケーションおよびシステムコンポーネントのシステム要件についての情報は、Milestoneウェブサイト(https://www.milestonesys.com/systemrequirements/)をご覧ください。

インストールを開始する前に

Milestoneは、実際のインストールを開始する前に、次のセクションに記載の要件を確認するように推奨しています。

サーバーとネットワークの準備

オペレーティングシステム

すべてのサーバーにMicrosoft Windowsオペレーティングシステムのクリーンインストールがあり、すべてのサーバーにすべての最新のWindows更新がインストールされていることを確認します。

さまざまなVMSアプリケーションおよびシステムコンポーネントのシステム要件についての情報は、Milestoneウェブサイト(https://www.milestonesys.com/systemrequirements/)をご覧ください。

Microsoft® .NET Framework

すべてのサーバーにMicrosoft .NET Framework 4.8またはそれ以上のバージョンがインストールされていることを確認します。

ネットワーク

すべてのシステムコンポーネントに固定IPアドレスを割り当てるか、カメラにDHCP予約を作成します。十分な帯域幅がネットワークで使用可能であることを保証するために、システムにより帯域幅が消費される方法とタイミングを理解する必要があります。ネットワークに対する主要な負荷には次の3つの要素があります。

- カメラビデオストリーム
- ビデオを表示するクライアント
- 録画されたビデオのアーカイブ

レコーディングサーバーはカメラからビデオストリームを取得し、これがネットワークに対する固定的な負荷になります。ビデオを表示するクライアントはネットワーク帯域幅を消費します。クライアントビューのコンテンツに変更がない場合は、負荷は一定です。ビューコンテンツ、ビデオ検索、または再生の変更により、負荷が動的になります。

録画したビデオのアーカイブはオプションの機能で、コンピュータの内部ストレージシステムに十分なスペースがない場合に、システムがネットワークストレジに録画を移動します。これは定義する必要があるスケジュールされたジョブです。一般的には、ネットワークドライブにアーカイブし、ネットワークに対するスケジュールされた動的な負荷にします。

ネットワークには、このようなトラフィックのピークに対応するための帯域幅ヘッドルームが必要です。これにより、システムの応答性と一般的なユーザー経験が改善されます。

Active Directoryの準備

Active Directoryサービスによってユーザーをシステムに追加する場合は、Active Directoryがインストールされており、ドメインコントローラーとして機能するサーバーをネットワークで使用できなくてはなりません。

ユーザーとグループ管理を簡単に行うには、Milestoneシステムをインストールする前に、Microsoftアクティブディレクトリ®をインストールし、設定することを[1]お勧めしますXProtect。システムをインストールしてから、マネジメントサーバーをActive Directoryに追加すると、マネジメントサーバーを再インストールして、Active Directoryで定義した新しいWindowsユーザーにユーザーを置き換えなければならなくなります。

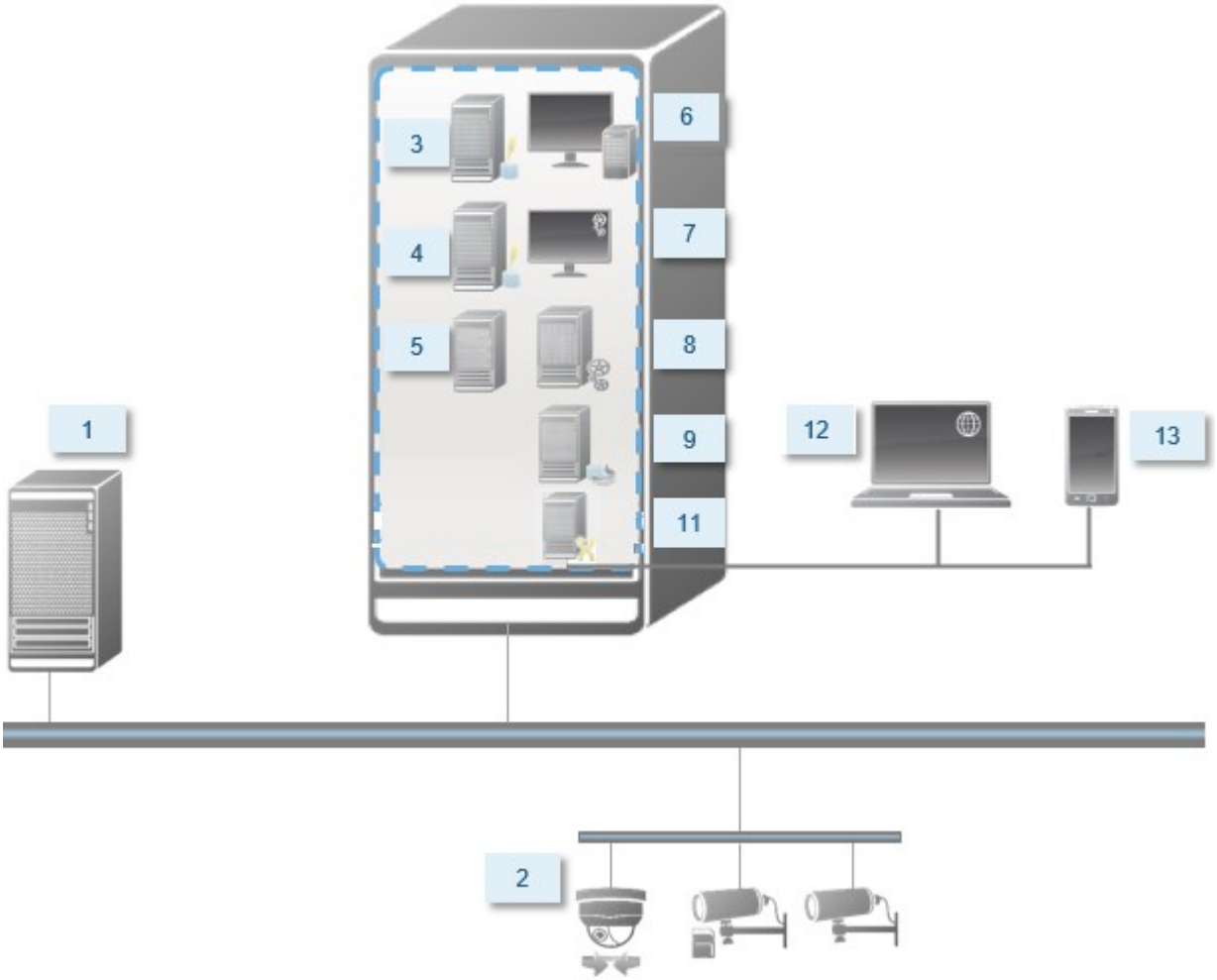
基本ユーザーはMilestone Federated Architectureシステムでサポートされていないため、Milestone Federated Architectureを使用することを計画している場合は、Active Directoryサービス経由でWindowsユーザーを追加する必要があります。Active Directoryをインストールしない場合は、インストール時に「168ページのワークグループのインストール」の手順に従ってください。

インストール方法

インストールウィザードでは、使用するインストール方法を決定する必要があります。組織のニーズに基づいて選択してください。ただし、通常は、システムを購入した時点でインストール方法はすでに決定されています。

オプション	説明
1つのコンピュータ	現在のコンピュータに、すべてのサーバー/クライアントコンポーネントと、SQL Serverがインストールされます。 インストールが完了すれば、ウィザードを介してシステムを設定できる場合があります。続行することに同意した後、レコーディングサーバーによってハードウェアのネットワークがスキャンされ、どのハードウェアをシステムに追加するかを選択できるようになります。設定ウィザードに追加できるハードウェアデバイスの最大数は、お持ちの基本ライセンスに応じて異なります。また、カメラがビュー内であらかじめ構成され、デフォルトのオペレータの役割が作成されます。インストールが終了するとXProtect Smart Clientが開き、システムを使用する準備が整います。
カスタム:	マネジメントサーバーは常にシステムコンポーネントリストで選択され、常にインストールされますが、現在のコンピュータに何をインストールするか(他のサーバーコンポーネントやクライアントコンポーネントなど)は自由に選択できます。 デフォルトでは、レコーディングサーバーはコンポーネントリスト内で選択されていませんが、これは変更可能です。未選択のコンポーネントを後から他のコンピュータにインストールすることもできます。

シングルコンピュータのインストール

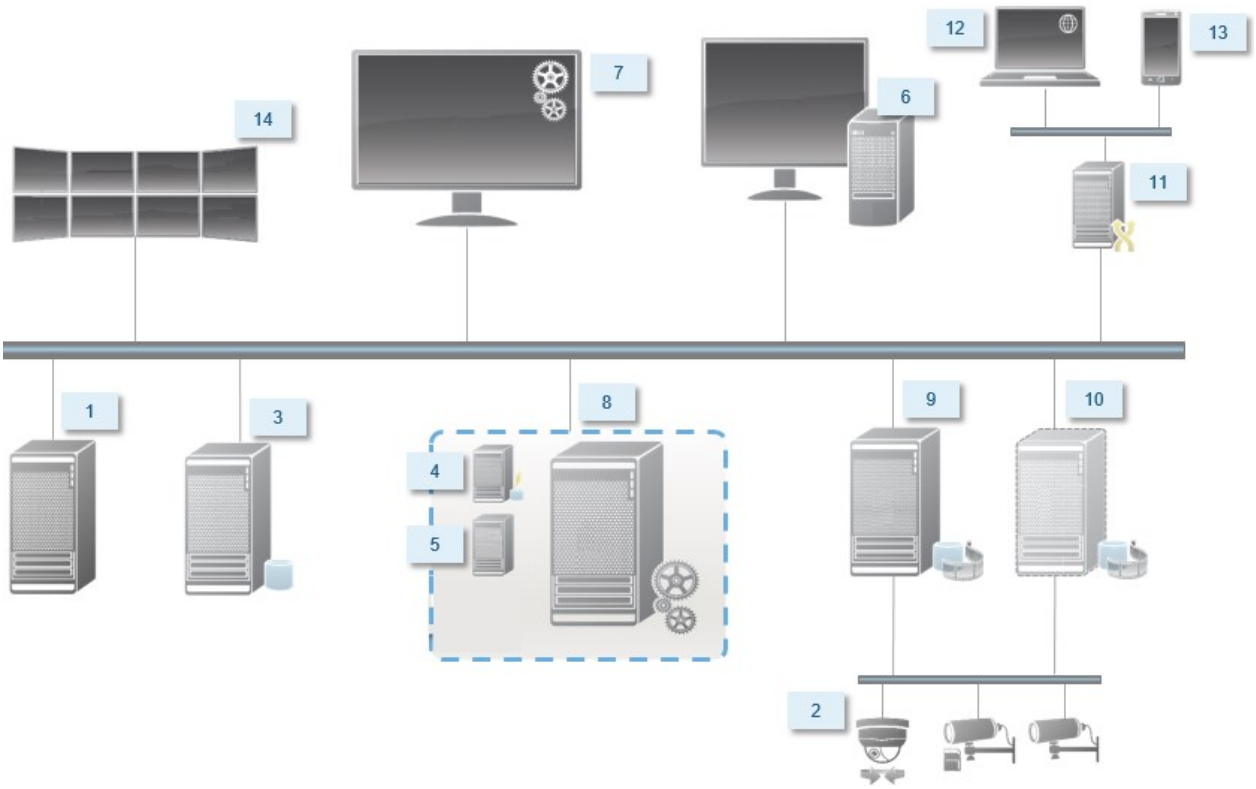


標準システムコンポーネント:

1. **Active Directory**
2. **デバイス**
3. **SQL Serverを備えたサーバー**
4. **イベントサーバー**
5. **ログサーバー**
6. **XProtect Smart Client**
7. **Management Client**
8. **マネジメントサーバー**
9. **レコーディングサーバー**

10. フェールオーバーレコーディングサーバー
11. XProtect Mobileサーバー
12. XProtect Web Client
13. XProtect Mobileクライアント
14. XProtect Smart Client とXProtect Smart Wall

カスタムインストール - 分散型システムコンポーネントの例



SQL Serverエディションの決定

Microsoft® SQL Server® ExpressはSQL Serverの無料版であり、インストールと使用に向けた準備が他のSQL Serverエディションよりも簡単です。**単一のコンピュータ**へのインストール中には、Microsoft SQL Server Expressがすでにコンピュータにインストールされていない限り、SQL Serverがインストールされます。

XProtect VMSインストールにMicrosoft SQL Server Expressバージョン2019が含まれています。一部のWindowsオペレーティングシステムは、このSQL Serverエディションに対応してません。XProtect VMSをインストールする前に、お使いのオペレーティングシステムがSQL Server 2019に対応していることを確認してください。オペレーティングシステムがこのSQL Serverエディションに対応していない場合は、SQL Serverインストールを開始する前に、対応しているXProtect VMSのエディションをインストールします。SQL Serverの対応エディションについては、https://www.milestonesys.com/systemrequirements/を参照してください。

Milestoneは、大規模なシステムまたはSQL Serverデータベースを往来するトランザクションが多いシステムについては、ネットワーク上の専用コンピュータと、他の目的で使用されていない専用ハードディスクドライブでのMicrosoft® SQL Server® StandardまたはSQL ServerのMicrosoft® SQL Server® Enterpriseエディションを使用するよう推奨しています。専用ドライブにSQL Serverをインストールすることで、全体的なシステムパフォーマンスが向上します。

サービスアカウントを選択してください

インストールの一部として、このコンピュータでMilestoneサービスを実行するためのアカウントを指定する必要があります。ログインユーザーには関係なく、サービスは常にこのアカウントで実行されます。アカウントに必要なユーザー権限すべて(例えばタスクを実行するための適切な権限、適切なネットワークおよびファイルアクセス権、ネットワーク共有フォルダーへのアクセス権など)があることを確認してください。

定義済みのアカウントまたはユーザーアカウントのいずれかを選択できます。システムをインストールする環境に応じて、判断してください。

ドメイン環境

ドメイン環境:

- Milestoneは、ビルトインのNetwork Serviceアカウントを使用することをお勧めします。

  システムを複数のコンピュータに拡張する必要がある場合でも、使いやすいアカウントです。

- ドメインユーザーアカウントも使用できますが、構成が多少困難になる可能性があります。

ワークグループ環境

Milestoneは、ワークグループ環境では、必要な権限すべてを持つローカルアカウントを使用することを推奨しています。通常は、これは管理者アカウントです。

> ⚠ 複数のコンピュータにシステムコンポーネントをインストールしている場合は、インストールしたすべてのコンピュータで、同じユーザー名、パスワード、アクセス権限を使用して選択したユーザーアカウントを設定する必要があります。

Kerberos認証(説明付き)

Kerberosはチケットベースのネットワーク認証プロトコルです。クライアント/サーバまたはサーバ/サーバ・アプリケーションのための強固な認証を提供するように設計されています。

古いMicrosoft NT LAN(NTLM)認証プロトコルの代替としてKerberos認証を使用します。

Kerberos認証は相互認証、つまりクライアントがサービスを、サービスがクライアントを認証する必要があります。この方法では、パスワードを公開せずに、クライアントXProtectからXProtectサーバーへ、より確実に認証できます。

Active Directory内にサービス・プリンシパル名(SPN)を登録することで、XProtect VMSで相互認証が可能になります。SPNは、XProtect Serverサービスのようなエンティティを一意に識別するエイリアスです。相互認証を使用するすべてのサービスでは、クライアントがネットワーク上のサービスを識別できるように、SPNを登録する必要があります。正しく登録されたSPNがなければ、相互認証を行えません。

以下の表で、Milestoneサービスおよび対応登録する必要がある対応ポート番号を一覧表示します:

サービス	ポート番号
Management Server - IIS	80 - 構成可能
Management Server - 内部	8080
Recording Server - Data Collector	7609
Failover Server	8990
Event Server	22331
LPR Server	22334

アクティブディレクトリに登録する必要があるサービスの数は、現在のインストール状況に依存します。Data Collectorは、Management Server、Recording Server、Event ServerまたはFailover Serverサービスのインストール時に自動的にインストールされます。

サービスを走らせるユーザーのために、2つのSPNsを登録する必要があります。:1つはホスト名で、もう1つは全権限を与えられたドメイン名で。

ネットワーク・ユーザー・サービス・アカウントの下でサービスを実行している場合は、このサービスを実行しているコンピュータごとに2つのSPNを登録する必要があります。

これはMilestoneSPN命名スキーム:

```
VideoOS/[DNS Host Name]:[Port]
VideoOS/[Fully qualified domain name]:[Port]
```

以下は、次の詳細で、コンピュータ上で実行されるRecording ServerサービスのSPNの例です。

```
Hostname: Record-Server1
Domain: Surveillance.com
```

登録するSPN:

```
VideoOS/Record-Server1:7609
VideoOS/Record-Server1.Surveillance.com:7609
```

ウィルススキャンの排除(説明付き)

他のデータベースソフトウェアの場合と同様に、XProtectソフトウェアを実行しているコンピュータにアンチウイルスプログラムがインストールされている場合は、特定のファイルのタイプやフォルダ、ならびに特定のネットワーク通信を除外することが重要になります。このような例外を設定しておかないと、ウイルススキャンで大量のシステムリソースが消費されてしまいます。さらに、スキャンプロセスによってファイルが一時的にロックされ、その結果として録画プロセスが破損したり、データベースが破損する可能性もあります。

ウイルススキャンを実行する必要がある場合、録画データベースを含んでいるレコーディングサーバーのフォルダー(デフォルトではC:\mediadatabase\、ならびにすべてのサブフォルダー)はスキャンしないでください。また、アーカイブ保存ディレクトリでもウイルススキャンは実行しないでください。

以下を除外に追加してください。

- ファイルのタイプ:.blk、.idx、.pic
- フォルダーおよびサブフォルダー:
  - C:\Program Files\Milestone または C:\Program Files (x86)\Milestone
  - C:\ProgramData\Milestone\IDP\Logs
  - C:\ProgramData\Milestone\KeyManagement\Logs
  - C:\ProgramData\Milestone\MIPSDK
  - C:\ProgramData\Milestone\XProtect Data Collector Server\Logs
  - C:\ProgramData\Milestone\XProtect Event Server\Logs
  - C:\ProgramData\Milestone\XProtect Log Server
  - C:\ProgramData\Milestone\XProtect Management Server\Logs
  - C:\ProgramData\Milestone\XProtect Mobile Server\Logs
  - C:\ProgramData\Milestone\XProtect Recording Server\Logs
  - C:\ProgramData\Milestone\XProtect Report Web Server\Logs
  - C:\ProgramData\Milestone\XProtect Recording Server\Secure\TablesDb

- 以下のTCPポートでのネットワークスキャンを除外：

製品	TCPポート
XProtect VMS	80、8080、7563、25、21、9000
XProtect Mobile	8081

または

- 以下のプロセスのネットワークスキャンを除外：

製品	プロセス
XProtect VMS	VideoOS.Recorder.Service.exe、VideoOS.Server.Service.exe、VideoOS.Administration.exe
XProtect Mobile	VideoOS.MobileServer.Service.exe

組織によってはウイルススキャンに関する厳密な方針があるかもしれませんが、上記の場所やファイルをウイルススキャンから除外することが重要です。

FIPS 140-2準拠モードで実行するようにXProtect VMSを設定するにはどうすればよいですか?

FIPS 140-2の操作モードでXProtect VMSを実行するには、以下を行う必要があります。

- FIPS 140-2承認の操作モードでWindowsオペレーティングシステムを実行します。FIPS有効化の詳細については、Microsoftサイトを参照してください。
- FIPSが有効になったWindowsオペレーティングシステムで、スタンドアロンのサードパーティー統合を実行できることを確認
- FIPS 140-2準拠の操作モードを確実にする方法でデバイスに接続
- メディアデータベースのデータがFIPS 140-2準拠暗号で暗号化されていることを確認

  これを行うには、メディアデータベースアップグレードツールを実行します。FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、ハードニングガイドのFIPS 140-2準拠セクションを参照してください。

FIPSが有効なシステムでXProtect VMSをインストールする前に

新しいXProtect VMSのインストールは、FIPSが有効になっているコンピュータで実行できますが、Windowsオペレーティング システムでFIPSが有効な場合はXProtect VMSをアップグレードできません。

アップグレードする場合は、インストールする前に、VMSの構成要素となっているすべてのコンピュータ(SQL Serverをホストするコンピュータも含む) でWindows FIPSセキュリティポリシーを無効にします。

XProtect VMSインストーラーはFIPSセキュリティポリシーを確認し、FIPSが有効であれば、インストールの開始を防ぎます。

ただし、XProtect VMSバージョン2020 R3以降にアップグレードしている場合は、FIPSを無効にする必要はありません。

XProtect VMSのコンポーネントをすべてのコンピュータにインストールして、FIPS向けにシステムを準備した後、VMSのすべてのコンピュータのWindowsでFIPSセキュリティポリシーを有効にできます。

FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、ハードニングガイドのFIPS 140-2準拠セクションを参照してください。

ソフトウェアライセンスコードを登録する

インストールする前に、Milestoneから受け取ったソフトウェアライセンスファイルの名前と場所を把握しておく必要があります。

XProtect Essential+の無料版をインストールできます。無料版はXProtect VMSの機能やカメラの数に制限があります。インストールするには、インターネットに接続してくださいXProtect Essential+。

ソフトウェアライセンスコード(SLC)は注文確認書に記載されています。ソフトウェアライセンスファイル名はSLCに基づいています。

Milestoneでは、インストールする前にお使いのSLCを弊社Webサイト(https://online.milestonesys.com/) に登録するよう推奨しています。代理店により登録済みの場合もあります。

デバイスドライバー(説明付き)

システムでは、ビデオデバイスドライバーを使用して、レコーディングサーバーに接続したカメラデバイスを制御し、通信しています。システムの各レコーディングサーバーに、デバイスドライバーをインストールする必要があります。

2018 R1のリリースから、デバイスドライバーは2つのDevice Packに分けられます: より新しいドライバーを持つレギュラーDevice Packと、古いバージョンのドライバーを持つレガシーDevice Packです。

レギュラーDevice Packは、レコーディングサーバーをインストールする時に自動的にインストールされます。その後、デバイスパックの新しいバージョンをダウンロードしてインストールすることで、ドライバーをアップデートすることができます。Milestoneはデバイスドライバーの新しいバージョンを定期的にリリースし、デバイスパックとしてウェブサイトのダウンロードページ(https://www.milestonesys.com/downloads/) から入手できるようにしています。Device Packを更新するときには、インストール済みのバージョンに最新バージョンを上書きインストールできます。

レガシーDevice Packは、システムがレギュラーDevice Packをインストール済みの場合のみ、インストールすることが可能です。前のバージョンがすでにシステムにインストールされている場合は、レガシーDevice Packからのドライバーは、自動的にインストールされます。これは、ソフトウェアダウンロードページ(https://www.milestonesys.com/downloads/) から手動でダウンロードしてインストールできます。

インストールする前にRecording Serverサービスを停止します。停止しなければ、コンピュータを再起動する必要があります。

最高のパフォーマンスを維持するために、常に最新バージョンのデバイスドライバーをご使用ください。

オフラインインストールの要件

オフラインであるサーバーにシステムをインストールする場合、以下が必要となります。

- `Milestone XProtect VMS Products 2023 R3 System Installer.exe`ファイル
- XProtectシステムのソフトウェアライセンスファイル(SLC)
- 必須の.NETバージョン(https://www.milestonesys.com/systemrequirements/)を含むOSインストールメディア

安全な通信(説明付き)

ハイパーテキストトランスファープロトコルセキュア(HTTPS)は、ハイパーテキストトランスファープロトコル(HTTP)をコンピュータネットワークで安全に通信するために強化したものです。HTTPSでは、通信プロトコルはトランスポートレイヤーセキュリティ(TLS)、または、それ以前の手段であるセキュアソケットレイヤー(SSL)を使用して暗号化されています。

XProtect VMSでは、非対称暗号化(RSA)によるTLS/SSLを使用して、安全な通信が確立されます。

TLS/SSLは、プライベートキー1つとパブリックキー1つのペアを使用して、安全な接続を認証、保護、管理します。

認証局(CA)は、ルート証明書を発行できるすべての機関です。これには、ルート証明書を発行するインターネットサービスや、証明書を手動で生成し配布するあらゆる機関が含まれます。CAは、ウェブサービス、すなわちHTTPS通信を使用するあらゆるソフトウェアに対して証明書を発行できます。この証明書には、プライベートキーとパブリックキーの2種類のキーが含まれています。パブリックキーは、パブリック証明書をインストールすることにより、ウェブサービスのクライアント(サービスクライアント)にインストールされます。プライベートキーはサーバー証明書の署名に使用するもので、サーバーにインストールする必要があります。サービスクライアントがウェブサービスを呼び出すと、ウェブサービスがパブリックキーを含むサーバー証明書をクライアントに送信します。サービスクライアントは、すでにインストールされたパブリックCA証明書を使用し、サーバー証明書を検証します。これで、プライベートサーバー証明書を使用して、クライアントサーバーとプライベートキーを交換し、安全なTLS/SSL接続を確立できます。

証明書が手動で配布される場合、クライアントが検証できるよう、証明書を事前にインストールしておく必要があります。

TLSについては、トランスポートレイヤーセキュリティを参照してください。

> ⚠ 証明書には期限があります。XProtect VMSは、証明書の期限が近づいても警告しません。証明書の有効期限が切れた場合
> • クライアントは、証明書の有効期限が切れたレコーディングサーバーを信頼せず、通信しません
> • レコーディングサーバーは、証明書の有効期限が切れたマネジメントサーバーを信頼せず、通信しません
> • モバイルデバイスは、証明書の有効期限が切れたモバイルサーバーを信頼せず、通信しません
>
> 証明書の更新は、本ガイドの手順に従い、証明書を作成したときと同様の要領で行います。

詳細については、XProtect VMSの保護方法に関する証明書ガイドを参照してください。

インストール

新しいXProtectシステムのインストール

XProtect Essential+をインストールする

XProtect Essential+の無料版をインストールできます。無料版はXProtect VMSの機能やカメラの数に制限があります。インストールするには、インターネットに接続してくださいXProtect Essential+。

このバージョンは、**シングルコンピュータ**インストールオプションを使用して1台のコンピュータにインストールされます。**シングルコンピュータ**オプションは、現在のコンピュータにすべてのサーバーコンポーネントとクライアントコンポーネントをインストールします。

Milestoneは、インストールの前に次のセクションをよく読むことを推奨しています: 126ページのインストールを開始する前に。

FIPSインストールでは、WindowsオペレーティングシステムでFIPSが有効になっている場合、XProtect VMSをアップグレードできません。インストールする前に、VMSの構成要素となっているすべてのコンピュータ(SQL Serverをホストするコンピュータも含む) でWindows FIPSセキュリティポリシーを無効にします。ただし、XProtect VMSバージョン2020 R3以降にアップグレードしている場合は、FIPSを無効にする必要はありません。FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、ハードニングガイドのFIPS 140-2準拠セクションを参照してください。

初期インストールの後、引き続き、設定ウィザードの操作ができます。ハードウェアと構成に応じて、レコーディングサーバーがネットワーク上のハードウェアをスキャンします。その後、どのハードウェアデバイスをシステムに追加するか選択できます。カメラはビューで事前設定されており、マイクやスピーカーといったその他デバイスは、オプションで有効にできます。また、ユーザーにオペレータの役割、あるいはシステム管理者の役割を持たせてシステムに追加することも可能です。インストール後、XProtect Smart Clientが開き、システムを使用する準備が整います。

インストールウィザードを閉じると、XProtect Management Clientが開き、ハードウェアデバイスやユーザーのシステムへの追加といった手動設定が可能になります。

以前のバージョンの製品からアップグレードすると、システムはハードウェアのスキャン、または新しいビューとユーザープロファイルの作成を行いません。

1. ソフトウェアをインターネット(https://www.milestonesys.com/downloads/) からダウンロードし、`Milestone XProtect VMS Products 2023 R3 System Installer.exe` ファイルを実行します。
2. インストールファイルが展開されます。セキュリティ設定によって、1つまたは複数のWindows® セキュリティ警告が表示されます。同意すると、展開が続行されます。
3. 完了すると、**Milestone XProtect VMS**インストール ウィザードが開きます。

1. インストール時に使用する**言語**を選択します(インストール後にシステムによって使用される言語ではなく、それは後で選択します) 。**続行**をクリックします。
2. *Milestoneエンドユーザー使用許諾契約*を読みます。**使用許諾契約の条項に同意します**チェックボックスを選択して、**続行**をクリックします。
3. **プライバシー設定**ページで、使用データを共有するかどうかを選択し、**続行**をクリックします。

   > システムを欧州GDPRに準拠するインストールにしたい場合は、データ収集を有効にしないでください。データ保護と使用状況データの収集の詳細については、GDPR プライバシーガイドを参照してください。

   > プライバシー設定は後でいつでも変更できます。システム設定(オプションダイアログボックス) も参照してください。

4. **XProtect Essential+**リンクをクリックして、無料のライセンスファイルをダウンロードします。

   無料のライセンスファイルがダウンロードされ、**ライセンスファイルの場所を入力または参照**フィールドに表示されます。**続行**をクリックします。

4. **シングルコンピュータ**を選択します。

   インストールするコンポーネントのリストが表示されます(このリストは編集できません) 。**続行**をクリックします。

5. **システム設定パスワードの割り当て**ページで、システム設定を保護するパスワードを入力します。システム回復時、またはシステムを拡張する際(クラスターの追加など) 、このパスワードが必要になります。

   > このパスワードを保存して安全に維持しておく必要があります。このパスワードをなくした場合は、システム設定を回復する能力に支障が出る可能性があります。

   システム設定をパスワードで保護したくない場合は、**システム設定パスワードを保護しないことを選択し、システム設定が暗号化されないことを承知する**を選択します。

   続行をクリックします。

6. **モバイルサーバーのデータ保護パスワードを割り当て**ページで、パスワードを入力して調査を暗号化します。システムを復元する場合や、追加のモバイルサーバーを使用してシステムを拡張する場合、モバイルサーバーのデータにアクセスするため、システム管理者はこのパスワードを入力する必要があります。

   > このパスワードを保存し、安全に保管してください。この指示に従わない場合、モバイルサーバーのデータを復元する機能が損なわれる可能性があります。

   調査をパスワードで保護したくない場合は、**モバイルサーバーのデータ保護パスワードを使用しないことを選択し、調査が暗号化されないことを理解しました**を選択します。

   続行をクリックします。

7. **レコーディングサーバーの設定**ページで、さまざまなレコーディングサーバーの設定を行います。

   1. **レコーディングサーバー名**フィールドに、レコーディングサーバー名を入力します。デフォルトでコンピュータ名になっています。
   2. **マネジメントサーバーのアドレス**フィールドにマネジメントサーバーのアドレスとポート番号が表示されます: localhost:80
   3. **メディアデータベースの場所の選択**フィールドで、ビデオ録画を保存する場所を選択します。ビデオ録画は、プログラムをインストールする場所とは別の、システムドライブ以外の場所に保存することをMilestoneは推奨します。デフォルトの場所は、空き容量が最も多いドライブです。
   4. **ビデオ録画の保存期間**フィールドで、録画を保存する期間を設定します。1日から365,000日の間の日数を入力できます。デフォルトの保存期間は7日間です。
   5. **続行**をクリックします。

8. **暗号化を選択**ページでは、以下の通信フローを保護できます。

   - レコーディングサーバー、データコレクター、マネジメントサーバー間

     内部通信フローで暗号化を有効にするには、**サーバー証明書**セクションで証明書を選択します。

     > レコーディングサーバーからマネジメントサーバーへの通信を暗号化する場合、システムは、マネジメントサーバーからレコーディングサーバーへの通信も暗号化するよう求めます。

   - レコーディングサーバーとクライアント間

     レコーディングサーバーと、レコーディングサーバーからデータストリームを受け取るクライアントコンポーネント間の暗号化を有効にするには、**ストリーミングメディア証明書**セクションで証明書を選択します。

   - モバイルサーバーとクライアント間

     モバイルサーバーからデータストリームを取得するクライアントコンポーネント間の暗号化を有効にするには、**モバイルストリーミングメディア証明書**セクションで証明書を選択します。

   - イベントサーバーと通信するコンポーネントとイベントサーバー間

     イベントサーバーと通信するコンポーネント(LPR Serverなど) とイベントサーバー間の暗号化を有効にするには、**イベントサーバー& 拡張機能**セクションで証明書を選択します。

   すべてのシステムコンポーネントに対して同じ証明書を使用することも、システムコンポーネントごとに異なる証明書を使用することもできます。

   安全なコミュニケーションのためのシステムの準備についての詳細は、以下を参照してください:

   - 136ページの安全な通信(説明付き)
   - 証明書に関するMilestoneガイド

   インストール後、通知エリアのManagement Server Managerトレイアイコンの Server Configuratorから暗号化を有効にすることもできます。

9. **ファイルの場所と製品言語を選択**ページで以下を行います。

   1. **ファイルの場所**フィールドで、プログラムをインストールする場所を選択します。

      すでにMilestone XProtect VMSがコンピュータにインストールされている場合、このフィールドは無効になっています。このフィールドには、コンポーネントがインストールされる場所が表示されます。

   2. **製品の言語**で、どの言語でXProtect製品をインストールするのか選択します。
   3. **インストール**をクリックします。

   ソフトウェアがインストールされます。まだコンピュータにインストールされていない場合は、インストール中にMicrosoft® SQL Server® ExpressとMicrosoft IISが自動的にインストールされます。

10. コンピュータを再起動するよう指示される場合があります。コンピュータの再起動後、セキュリティ設定によって1つまたは複数のWindowsセキュリティ警告が表示される場合があります。許可すると、インストールが完了します。
11. インストールが完了すると、コンピュータにインストールされているコンポーネントのリストが表示されます。

    続行をクリックして、システムにハードウェアとユーザーを追加してください。

    ここで**閉じる**をクリックすると設定ウィザードがスキップされ、XProtect Management Clientが開きます。Management Clientでは、システムを設定できます(ハードウェアやユーザーのシステムへの追加など)。

12. **ハードウェアのユーザー名とパスワードを入力**ページでは、(メーカーのデフォルト値から変更した)ハードウェアのユーザー名とパスワードを入力します。

    インストーラにより、このハードウェアのネットワークと、メーカーのデフォルトの認証情報が割り当てられたハードウェアのネットワークがスキャンされます。

    続行をクリックして、ハードウェアのスキャンが完了するまで待ちます。

13. **システムに追加するハードウェアを選択**ページで、システムに追加したいハードウェアを選択します。**続行**をクリックして、ハードウェアが追加されるまで待ちます。
14. **デバイスの設定**ページでは、ハードウェア名の横にある編集アイコンをクリックすると、ハードウェアにわかりやすい名前を付けることができます。この名前は、ハードウェアデバイスの名前の先頭に付きます。

    ハードウェアノードを展開して、カメラ、スピーカー、マイクなどのハードウェアデバイスを有効または無効にします。

    デフォルトで、カメラは有効化、スピーカーとマイクは無効化されています。

    続行をクリックして、ハードウェアが設定されるまで待ちます。

15. **ユーザーを追加**ページでは、ユーザーをWindowsユーザーまたは基本ユーザーとしてシステムに追加できます。これらのユーザーには、管理者またはオペレータの役割を割り当てることができます。

    ユーザーを定義し、**追加**をクリックします。

    ユーザーの追加が終わったら、**続行**をクリックします。

16. インストールと初期設定が完了すると、**設定が完了しました**ページが開きます。ここには以下が表示されます。
    - システムに追加されたハードウェアデバイスのリスト
    - システムに追加されたユーザーのリスト
    - ユーザーと共有できるXProtect Web ClientとXProtect Mobileクライアントのアドレス

    閉じるをクリックするとXProtect Smart Clientが開き、使用可能になります。

システムのインストール - シングルコンピュータオプション

シングルコンピュータオプションは、現在のコンピュータにすべてのサーバーコンポーネントとクライアントコンポーネントをインストールします。

Milestoneは、インストールの前に次のセクションをよく読むことを推奨しています: 126ページのインストールを開始する前に。

FIPSインストールでは、Windowsオペレーティングシステムで FIPSが有効になっている場合、XProtect VMSをアップグレードできません。インストールする前に、VMSの構成要素となっているすべてのコンピュータ(SQL Serverをホストするコンピュータも含む) でWindows FIPSセキュリティポリシーを無効にします。ただし、XProtect VMSバージョン2020 R3以降にアップグレードしている場合は、FIPSを無効にする必要はありません。FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、ハードニングガイドのFIPS 140-2準拠セクションを参照してください。

初期インストールの後、引き続き、設定ウィザードの操作ができます。ハードウエアと構成に応じて、レコーディングサーバーがネットワーク上のハードウェアをスキャンします。その後、どのハードウェアデバイスをシステムに追加するか選択できます。カメラはビューで事前設定されており、マイクやスピーカーといったその他デバイスは、オプションで有効にできます。また、ユーザーにオペレータの役割、あるいはシステム管理者の役割を持たせてシステムに追加することも可能です。インストール後、XProtect Smart Clientが開き、システムを使用する準備が整います。

インストールウィザードを閉じると、XProtect Management Clientが開き、ハードウェアデバイスやユーザーのシステムへの追加といった手動設定が可能になります。

以前のバージョンの製品からアップグレードすると、システムはハードウェアのスキャン、または新しいビューとユーザープロファイルの作成を行いません。

1. ソフトウェアをインターネット(https://www.milestonesys.com/downloads/) からダウンロードし、`Milestone XProtect VMS Products 2023 R3 System Installer.exe` ファイルを実行します。
2. インストールファイルが展開されます。セキュリティ設定によって、1つまたは複数のWindows® セキュリティ警告が表示されます。同意すると、展開が続行されます。
3. 完了すると、**Milestone XProtect VMS**インストール ウィザードが開きます。
    1. インストール時に使用する**言語**を選択します(インストール後にシステムによって使用される言語ではなく、それは後で選択します) 。**続行**をクリックします。
    2. *Milestoneエンドユーザー使用許諾契約*を読みます。**使用許諾契約の条項に同意します**チェックボックスを選択して、**続行**をクリックします。
    3. **プライバシー設定**ページで、使用データを共有するかどうかを選択し、**続行**をクリックします。

        > システムを欧州GDPRに準拠するインストールにしたい場合は、データ収集を有効にしないでください。データ保護と使用状況データの収集の詳細については、GDPR プライバシーガイドを参照してください。

        > プライバシー設定は後でいつでも変更できます。システム設定(オプションダイアログボックス) も参照してください。

    4. **ライセンスファイルの場所を入力または参照**で、XProtectプロバイダーから入手したライセンスファイルを入力します。または、ファイルの場所を参照するか、**XProtect Essential+**リンクをクリックして無料ライセンスファイルをダウンロードします。XProtect Essential+製品の無料版の制限については、105ページの製品比較を参照してください。続行する前に、システムがライセンスファイルを検証します。**続行**をクリックします。
4. **シングルコンピュータ**を選択します。

    インストールするコンポーネントのリストが表示されます(このリストは編集できません) 。**続行**をクリックします。
5. **システム設定パスワードの割り当て**ページで、システム設定を保護するパスワードを入力します。システム回復時、またはシステムを拡張する際(クラスターの追加など) 、このパスワードが必要になります。

    > このパスワードを保存して安全に維持しておく必要があります。このパスワードをなくした場合は、システム設定を回復する能力に支障が出る可能性があります。

    システム設定をパスワードで保護したくない場合は、**システム設定パスワードを保護しないことを選択し、システム設定が暗号化されないことを承知する**を選択します。

    続行をクリックします。

6. **モバイルサーバーのデータ保護パスワードを割り当て**ページで、パスワードを入力して調査を暗号化します。システムを復元する場合や、追加のモバイルサーバーを使用してシステムを拡張する場合、モバイルサーバーのデータにアクセスするため、システム管理者はこのパスワードを入力する必要があります。

   > このパスワードを保存し、安全に保管してください。この指示に従わない場合、モバイルサーバーのデータを復元する機能が損なわれる可能性があります。

   調査をパスワードで保護したくない場合は、**モバイルサーバーのデータ保護パスワードを使用しないことを選択し、調査が暗号化されないことを理解しました**を選択します。

   続行をクリックします。

7. **レコーディングサーバーの設定**ページで、さまざまなレコーディングサーバーの設定を行います。

   1. **レコーディングサーバー名**フィールドに、レコーディングサーバー名を入力します。デフォルトでコンピュータ名になっています。
   2. **マネジメントサーバーのアドレス**フィールドにマネジメントサーバーのアドレスとポート番号が表示されます：localhost:80
   3. **メディアデータベースの場所の選択**フィールドで、ビデオ録画を保存する場所を選択します。ビデオ録画は、プログラムをインストールする場所とは別の、システムドライブ以外の場所に保存することをMilestoneは推奨します。デフォルトの場所は、空き容量が最も多いドライブです。
   4. **ビデオ録画の保存期間**フィールドで、録画を保存する期間を設定します。1日から365,000日の間の日数を入力できます。デフォルトの保存期間は7日間です。
   5. **続行**をクリックします。

8. **暗号化を選択**ページでは、以下の通信フローを保護できます。

   - レコーディングサーバー、データコレクター、マネジメントサーバー間

     内部通信フローで暗号化を有効にするには、**サーバー証明書**セクションで証明書を選択します。

     > レコーディングサーバーからマネジメントサーバーへの通信を暗号化する場合、システムは、マネジメントサーバーからレコーディングサーバーへの通信も暗号化するよう求めます。

   - レコーディングサーバーとクライアント間

     レコーディングサーバーと、レコーディングサーバーからデータストリームを受け取るクライアントコンポーネント間の暗号化を有効にするには、**ストリーミングメディア証明書**セクションで証明書を選択します。

   - モバイルサーバーとクライアント間

     モバイルサーバーからデータストリームを取得するクライアントコンポーネント間の暗号化を有効にするには、**モバイルストリーミングメディア証明書**セクションで証明書を選択します。

   - イベントサーバーと通信するコンポーネントとイベントサーバー間

     イベントサーバーと通信するコンポーネント(LPR Serverなど) とイベントサーバー間の暗号化を有効にするには、**イベントサーバー& 拡張機能**セクションで証明書を選択します。

   すべてのシステムコンポーネントに対して同じ証明書を使用することも、システムコンポーネントごとに異なる証明書を使用することもできます。

   安全なコミュニケーションのためのシステムの準備についての詳細は、以下を参照してください:

   - 136ページの安全な通信(説明付き)
   - 証明書に関するMilestoneガイド

   インストール後、通知エリアのManagement Server Managerトレイアイコンの**Server Configurator**から暗号化を有効にすることもできます。

9. **ファイルの場所と製品言語を選択**ページで以下を行います。

   1. **ファイルの場所**フィールドで、プログラムをインストールする場所を選択します。

      すでにMilestone XProtect VMSがコンピュータにインストールされている場合、このフィールドは無効になっています。このフィールドには、コンポーネントがインストールされる場所が表示されます。

   2. **製品の言語**で、どの言語でXProtect製品をインストールするのか選択します。
   3. **インストール**をクリックします。

   ソフトウェアがインストールされます。まだコンピュータにインストールされていない場合は、インストール中にMicrosoft® SQL Server® ExpressとMicrosoft IISが自動的にインストールされます。

10. コンピュータを再起動するよう指示される場合があります。コンピュータの再起動後、セキュリティ設定によって1つまたは複数のWindowsセキュリティ警告が表示される場合があります。許可すると、インストールが完了します。
11. インストールが完了すると、コンピュータにインストールされているコンポーネントのリストが表示されます。

    続行をクリックして、システムにハードウェアとユーザーを追加してください。

    ここで**閉じる**をクリックすると設定ウィザードがスキップされ、XProtect Management Clientが開きます。Management Clientでは、システムを設定できます(ハードウェアやユーザーのシステムへの追加など)。

12. **ハードウェアのユーザー名とパスワードを入力**ページでは、(メーカーのデフォルト値から変更した)ハードウェアのユーザー名とパスワードを入力します。

    インストーラにより、このハードウェアのネットワークと、メーカーのデフォルトの認証情報が割り当てられたハードウェアのネットワークがスキャンされます。

    続行をクリックして、ハードウェアのスキャンが完了するまで待ちます。

13. **システムに追加するハードウェアを選択**ページで、システムに追加したいハードウェアを選択します。**続行**をクリックして、ハードウェアが追加されるまで待ちます。
14. **デバイスの設定**ページでは、ハードウェア名の横にある編集アイコンをクリックすると、ハードウェアにわかりやすい名前を付けることができます。この名前は、ハードウェアデバイスの名前の先頭に付きます。

    ハードウェアノードを展開して、カメラ、スピーカー、マイクなどのハードウェアデバイスを有効または無効にします。

    デフォルトで、カメラは有効化、スピーカーとマイクは無効化されています。

    続行をクリックして、ハードウェアが設定されるまで待ちます。

15. **ユーザーを追加**ページでは、ユーザーをWindowsユーザーまたは基本ユーザーとしてシステムに追加できます。これらのユーザーには、管理者またはオペレータの役割を割り当てることができます。

    ユーザーを定義し、**追加**をクリックします。

    ユーザーの追加が終わったら、**続行**をクリックします。

16. インストールと初期設定が完了すると、**設定が完了しました**ページが開きます。ここには以下が表示されます。
    - システムに追加されたハードウェアデバイスのリスト
    - システムに追加されたユーザーのリスト
    - ユーザーと共有できるXProtect Web ClientとXProtect Mobileクライアントのアドレス

    閉じるをクリックするとXProtect Smart Clientが開き、使用可能になります。

システムのインストール - カスタムオプション

カスタムオプションではマネジメントサーバーがインストールされますが、現在のコンピュータに他のどのサーバー/クライアントコンポーネントをインストールするか選択することもできます。デフォルトでは、レコーディングサーバーはコンポーネントリスト内で選択されていません。選択によっては、未選択のシステムコンポーネントを後から他のコンピュータにインストールすることもできます。それぞれのシステムコンポーネントとその役割について詳しくは、32ページの製品概要を参照してください。他のコンピュータへのインストールは、マネジメントサーバーのダウンロードウェブページ(DownloadManager) を介して行われます。DownloadManagerを介したインストールの詳細については、173ページのDownloadManager/ダウンロードWebページを参照してください。

Milestoneは、インストールの前に次のセクションをよく読むことを推奨しています: 126ページのインストールを開始する前に。

FIPSインストールでは、Windowsオペレーティングシステムで FIPSが有効になっている場合、XProtect VMSをアップグレードできません。インストールする前に、VMSの構成要素となっているすべてのコンピュータ(SQL Serverをホストするコンピュータも含む) でWindows FIPSセキュリティポリシーを無効にします。ただし、XProtect VMSバージョン2020 R3以降にアップグレードしている場合は、FIPSを無効にする必要はありません。FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、ハードニングガイドのFIPS 140-2準拠セクションを参照してください。

1. ソフトウェアをインターネット(https://www.milestonesys.com/downloads/) からダウンロードし、`Milestone XProtect VMS Products 2023 R3 System Installer.exe`ファイルを実行します。
2. インストールファイルが展開されます。セキュリティ設定によって、1つまたは複数のWindows® セキュリティ警告が表示されます。同意すると、展開が続行されます。
3. 完了すると、**Milestone XProtect VMS**インストール ウィザードが開きます。

1. インストール時に使用する**言語**を選択します(インストール後にシステムによって使用される言語ではなく、それは後で選択します) 。**続行**をクリックします。
2. *Milestoneエンドユーザー使用許諾契約*を読みます。**使用許諾契約の条項に同意します**チェックボックスを選択して、**続行**をクリックします。
3. **プライバシー設定**ページで、使用データを共有するかどうかを選択し、**続行**をクリックします。

   システムを欧州GDPRに準拠するインストールにしたい場合は、データ収集を有効にしないでください。データ保護と使用状況データの収集の詳細については、GDPR プライバシーガイドを参照してください。

   プライバシー設定は後でいつでも変更できます。システム設定(オプションダイアログボックス) も参照してください。

4. **ライセンスファイルの場所を入力または参照**で、XProtectプロバイダーから入手したライセンスファイルを入力します。または、ファイルの場所を参照するか、**XProtect Essential+**リンクをクリックして無料ライセンスファイルをダウンロードします。XProtect Essential+製品の無料版の制限については、105ページの製品比較を参照してください。続行する前に、システムがライセンスファイルを検証します。**続行**をクリックします。

4. **カスタム**を選択します。インストールするコンポーネントのリストが表示されます。マネジメントサーバーを除き、リストのすべてのコンポーネントはオプションです。レコーディングサーバーとモバイルサーバーはデフォルトでは選択されていません。インストールするシステムコンポーネントを選択し、**続行**をクリックします。

   システムを正しく機能させるには、XProtect API Gatewayのインスタンスを少なくとも1つインストールする必要があります。

   下記のステップにおいて、すべてのシステムコンポーネントがインストールされます。さらに分散型のシステムの場合、1台のコンピュータに少数のシステムコンポーネントをインストールし、別のコンピュータに残りのシステムコンポーネントをインストールします。インストールのステップを認識できない場合、理由としてこのページに記されているシステムコンポーネントをインストールするよう選択していないことが考えられます。その場合は、次のステップに進みます。153ページのDownload Managerを介したインストール(説明付き) 、155ページのDownload Managerを介したレコーディングサーバーのインストール、160ページのコマンドラインシェルを介したサイレントインストール(説明付き) も参照してください。

5. **XProtectシステムに使用するIISのウェブサイトを選択**ページは、コンピュータで複数のIISウェブサイトを利用できる場合にしか表示されません。XProtectシステムにどのウェブサイトを使用するかを選択する必要があります。HTTPSバインディングのあるサイトを選択します。**続行**をクリックします。

Microsoft® IISがコンピュータにインストールされていない場合、ここでインストールされます。

6. **Microsoft SQL Serverを選択**ページで、使用するSQL Serverを選択します。153ページのカスタムインストール中のSQL Serverオプションも参照してください。**続行**をクリックします。

> ローカルコンピュータにSQL Serverが存在しない場合はMicrosoft SQL Server Expressをインストールできますが、大規模な分散システムにおいては通常、ネットワーク上で専用のSQL Serverが使用されます。

7. **データベースを選択**ページ(既存のSQL Serverを選択した場合にのみ表示)で、システム設定を保存するためのSQL Serverデータベースを選択または作成します。既存のSQL Serverデータベースを選択した場合、既存のデータを**維持**または**上書き**するかを決定します。アップグレードを行う場合は、システム設定が失われないよう既存のデータを維持するよう選択します。153ページのカスタムインストール中のSQL Serverオプションも参照してください。**続行**をクリックします。

8. **データベース設定**ページで、**インストーラがデータベースを作成または再作成**または**作成済みデータベースを使用**のどちらかを選択します。

9. 自動的にデータベースに作成または再作成するには、**インストーラがデータベースを作成または再作成**を選択し、**続行**をクリックします。

10. 目的に合わせて設定したデータベース、または作成済みデータベースを使用するには、**作成済みデータベースを使用**を選択します。その後、**高度なデータベース設定**ページが表示されます。

11. **高度なデータベース設定**ページで、XProtectコンポーネントのサーバーとデータベース名を入力します。

12. **「Windows認証、サーバー証明書を信頼しない(推奨)」**または**「Windows認証、サーバー証明書を信頼する」**を選択するか、**「Azure Active Directory統合、サーバー証明書を信頼しない(推奨)」**を選択します。

> インストールに使用するアカウントは、使用する認証タイプに応じて、Azure ADまたはWindows ADに作成する必要があります。多要素認証(MFA)はこのアカウントではサポートされていません。

> **(サーバー証明書を信頼しない)**オプションは、Windows認証では推奨され、Azure Active Directory統合では必須です。これは、インストール前にサーバー証明書が検証、確認されるようにするためです。無効なサーバー証明書に関する詳細は、インストールログファイルに記載されています。**Windows認証、サーバー証明書を信頼する**オプションを使用すると、サーバー証明書の検証をスキップできます。

13. アイコンをクリックして接続を検証します。アイコンをクリックすると、サーバー証明書の検証も行われます。

14. **続行**をクリックします。

15. **システム設定パスワードの割り当て**ページで、システム設定を保護するパスワードを入力します。システム回復時、またはシステムを拡張する際(クラスターの追加など) 、このパスワードが必要になります。

> このパスワードを保存して安全に維持しておく必要があります。このパスワードをなくした場合は、システム設定を回復する能力に支障が出る可能性があります。

システム設定をパスワードで保護したくない場合は、**システム設定パスワードを保護しないことを選択し、システム設定が暗号化されないことを承知する**を選択します。

続行をクリックします。

16. **モバイルサーバーのデータ保護パスワードを割り当て**ページで、パスワードを入力して調査を暗号化します。システムを復元する場合や、追加のモバイルサーバーを使用してシステムを拡張する場合、モバイルサーバーのデータにアクセスするため、システム管理者はこのパスワードを入力する必要があります。

> このパスワードを保存し、安全に保管してください。この指示に従わない場合、モバイルサーバーのデータを復元する機能が損なわれる可能性があります。

調査をパスワードで保護したくない場合は、**モバイルサーバーのデータ保護パスワードを使用しないことを選択し、調査が暗号化されないことを理解しました**を選択します。

続行をクリックします。

17. **レコーディングサーバーのサービスアカウントを選択**で、レコーディングサーバーのサービスアカウントとして**この定義済みアカウント**または**このアカウント**のいずれかを選択します。

必要に応じてパスワードを入力します。

> アカウントのユーザー名は、1単語にしてください。スペースは使用できません。

続行をクリックします。

18. **レコーディングサーバーの設定**ページで、さまざまなレコーディングサーバーの設定を行います。

    1. **レコーディングサーバー名**フィールドに、レコーディングサーバー名を入力します。デフォルトでコンピュータ名になっています。
    2. **マネジメントサーバーのアドレス**フィールドにマネジメントサーバーのアドレスとポート番号が表示されます: localhost:80
    3. **メディアデータベースの場所の選択**フィールドで、ビデオ録画を保存する場所を選択します。ビデオ録画は、プログラムをインストールする場所とは別の、システムドライブ以外の場所に保存することをMilestoneは推奨します。デフォルトの場所は、空き容量が最も多いドライブです。
    4. **ビデオ録画の保存期間**フィールドで、録画を保存する期間を設定します。1日から365,000日の間の日数を入力できます。デフォルトの保存期間は7日間です。
    5. **続行**をクリックします。

19. **暗号化を選択**ページでは、以下の通信フローを保護できます。

    - レコーディングサーバー、データコレクター、マネジメントサーバー間

      内部通信フローで暗号化を有効にするには、**サーバー証明書**セクションで証明書を選択します。

      > レコーディングサーバーからマネジメントサーバーへの通信を暗号化する場合、システムは、マネジメントサーバーからレコーディングサーバーへの通信も暗号化するよう求めます。

    - レコーディングサーバーとクライアント間

      レコーディングサーバーと、レコーディングサーバーからデータストリームを受け取るクライアントコンポーネント間の暗号化を有効にするには、**ストリーミングメディア証明書**セクションで証明書を選択します。

    - モバイルサーバーとクライアント間

      モバイルサーバーからデータストリームを取得するクライアントコンポーネント間の暗号化を有効にするには、**モバイルストリーミングメディア証明書**セクションで証明書を選択します。

    - イベントサーバーと通信するコンポーネントとイベントサーバー間

      イベントサーバーと通信するコンポーネント(LPR Serverなど) とイベントサーバー間の暗号化を有効にするには、**イベントサーバー& 拡張機能**セクションで証明書を選択します。

    すべてのシステムコンポーネントに対して同じ証明書を使用することも、システムコンポーネントごとに異なる証明書を使用することもできます。

    安全なコミュニケーションのためのシステムの準備についての詳細は、以下を参照してください:

    - 136ページの安全な通信(説明付き)
    - 証明書に関するMilestoneガイド

    インストール後、通知エリアのManagement Server Managerトレイアイコンの Server Configuratorから暗号化を有効にすることもできます。

20. **ファイルの場所と製品の言語を選択**ページで、プログラムファイルの**ファイルの場所**を選択します。

    > すでにMilestone XProtect VMSがコンピュータにインストールされている場合、このフィールドは無効になっています。このフィールドには、コンポーネントがインストールされる場所が表示されます。

21. **製品の言語**フィールドで、どの言語でXProtect製品をインストールするのか選択します。**インストール**をクリックします。

    ソフトウェアがインストールされます。インストールが完了すると、正常にインストールされたシステムコンポーネントのリストが表示されます。**閉じる**をクリックします。

22. コンピュータを再起動するよう指示される場合があります。コンピュータの再起動後、セキュリティ設定によって1つまたは複数のWindowsセキュリティ警告が表示される場合があります。許可すると、インストールが完了します。
23. Management Clientでシステムを設定します。181ページの初期構成タスクリストを参照してください。
24. 選択内容によっては、Download Managerを介して他のコンピュータに残りのシステムコンポーネントをインストールします。153ページのDownload Managerを介したインストール(説明付き)を参照してください。

カスタムインストール中のSQL Serverオプション

どのSQL Serverとデータベースを以下のオプションと併用するかを決定します。

SQL Serverオプション

- **Microsoft® SQL Server® Expressをこのコンピュータにインストールする**: このオプションは、SQL Serverがコンピュータにインストールされていない場合にのみ表示されます。
- **SQL Serverをこのコンピュータで使用する**: このオプションは、SQL Serverがすでにコンピュータにインストールされている場合にのみ表示されます。
- **検索によりネットワーク上でSQL Serverを選択する**: ネットワークサブネット上で検索可能なすべてのSQL Serverインストールを検索できるようになります。
- **ネットワーク上でSQL Serverを選択する**: 検索で見つけることができない可能性がある、SQL Serverのアドレス(ホスト名とIPアドレス)を入力できるようになります。

SQL Serverデータベースオプション

- **新しいデータベースを作成する**: 主に新規インストール向け
- **既存のデータベースを使用する**: 主に既存のインストールのアップグレード向け。Milestoneは、システム設定が失われないよう既存のSQL Serverデータベースを再利用し、その中の既存のデータを維持するよう推奨しています。SQL Serverデータベース内のデータを上書きするよう選択することも可能です。

新しいXProtectコンポーネントのインストール

Download Managerを介したインストール(説明付き)

マネジメントサーバーがインストールされているコンピュータ以外にシステムコンポーネントをインストールしたい場合は、Management Serverのダウンロードウェブサイトから Download Managerを介してシステムコンポーネントをインストールする必要があります。

1. Management Serverがインストールされているコンピュータから、Management Serverのダウンロードウェブページに移動します。Windowsの**スタート**メニューで**Milestone > 管理インストールページ**の順に選択し、将来、他のコンピュータにシステムコンポーネントをインストールする際に使用できるよう、インターネットアドレスを書き留めるかコピーします。アドレスは通常、*http://[management server address]/installation/Admin/default-en-US.htm*です。
2. それぞれのコンピュータにログインし、他のシステムコンポーネントを1つまたは複数インストールします。

- Recording Server (詳細については、155ページのDownload Managerを介したレコーディングサーバーのインストールまたは162ページのレコーディングサーバーのサイレントインストールを参照してください)
- Management Client(詳細については、154ページのDownload Manager経由でManagement Clientをインストールを参照してください)
- Smart Client
- Event Serverインストール後、API ゲートウェイを必ず再起動してください。後日コンピュータの名前を変更するには、API ゲートウェイも再起動する必要があります。

> FIPS準拠環境でEvent Serverをインストールしている場合は、インストール前にWindows FIPS 140-2モードを無効にする必要があります。

- Log Server(詳細については、164ページのログサーバーをサイレントインストールするを参照してください)
- Mobile Server (詳細については、XProtect Mobileサーバーのマニュアルを参照してください)

3. インターネットブラウザを開き、Management Serverのダウンロードウェブページのアドレスをアドレスフィールドに入力して、関連するインストーラをダウンロードします。
4. インストーラを実行します。

インストールの各手順において何を選択または設定すべきか不明な場合は、147ページのシステムのインストール - カスタムオプションを参照してください。

Download Manager経由でManagement Clientをインストール

XProtectシステム管理者が複数いる場合や、複数のコンピュータからXProtectシステムを管理する場合は、以下の手順に従ってManagement Clientをインストールできます。

> Management Clientは常にマネジメントサーバーにインストールされます。

1. Management Serverがインストールされているコンピュータから、Management Serverのダウンロードウェブページに移動します。Windowsの**スタート**メニューで**Milestone > 管理インストールページ**の順に選択し、将来、他のコンピュータにシステムコンポーネントをインストールする際に使用できるよう、インターネットアドレスを書き留めるかコピーします。アドレスは通常、*http://[management server address]/installation/Admin/default-en-US.htm*です。
2. システムコンポーネントをインストールするコンピュータにログインします。
1. インターネットブラウザを開き、Management Serverのダウンロードウェブページのアドレスをアドレスフィールドに入力して、Enterキーを押します。
3. Management Clientインストーラで**すべての言語**をクリックします。ダウンロードしたファイルを実行します。
4. すべての警告で**はい**をクリックします。展開が開始されます。
5. インストーラの言語を選択します。**続行**をクリックします。

6. 使用許諾契約を読み、同意します。**続行**をクリックします。
7. ファイルの場所および製品の言語を選択します。**インストール**をクリックします。
8. インストールが完了しました。正常にインストールされたコンポーネントの一覧が表示されます。**閉じる**をクリックします。
9. デスクトップのアイコンをクリックし、Management Clientを開きます。
10. Management Clientのログインダイアログが表示されます。
11. **コンピュータ**フィールドでマネジメントサーバーのホスト名またはIPアドレスを指定します。
12. 認証を選択して、ユーザー名とパスワードを入力します。**接続**をクリックします。Management Clientが起動します。

    ManagementClientの機能の詳細とシステムで実行できる処理を表示するには、ツールメニューの**ヘルプ**をクリックします。

Download Managerを介したレコーディングサーバーのインストール

システムコンポーネントが別々のコンピュータに分散されている場合は、次の手順に従ってレコーディングサーバーをインストールできます。

> レコーディングサーバーは、**シングルコンピュータ**インストールではすでにインストールされていますが、より多くの容量が必要な場合は、同じ手順でレコーディングサーバーを追加することができます。

> フェールオーバーレコーディングサーバーをインストールする必要がある場合は、158ページのDownloadManagerを介したフェールオーバーレコーディングサーバーのインストールを参照してください。

1. Management Serverがインストールされているコンピュータから、Management Serverのダウンロードウェブページに移動します。Windowsの**スタート**メニューで**Milestone > 管理インストールページ**の順に選択し、将来、他のコンピュータにシステムコンポーネントをインストールする際に使用できるよう、インターネットアドレスを書き留めるかコピーします。アドレスは通常、*http://[management server address]/installation/Admin/default-en-US.htm*です。
2. システムコンポーネントをインストールするコンピュータにログインします。
3. インターネットブラウザを開き、Management Serverのダウンロードウェブページのアドレスをアドレスフィールドに入力して、Enterキーを押します。
4. **レコーディング サーバーインストーラ**の下にある**すべての言語**を選択して、レコーディングサーバーのインストーラをダウンロードします。インストーラを保存するか、ウェブページから直接実行します。
5. インストール中に使用する**言語**を選択します。**続行**をクリックします。

6. **インストールのタイプを選択**ページで以下を選択します。

   標準：デフォルト値を使用してレコーディングサーバーをインストールします。

   カスタム：カスタム値を使用してレコーディング サーバーをインストールします。

7. **レコーディングサーバーの設定**ページで、さまざまなレコーディングサーバーの設定を行います。

   1. **レコーディングサーバー名**フィールドに、レコーディングサーバー名を入力します。デフォルトでコンピュータ名になっています。

   2. **マネジメントサーバーのアドレス**フィールドにマネジメントサーバーのアドレスとポート番号が表示されます：localhost:80

   3. **メディアデータベースの場所の選択**フィールドで、ビデオ録画を保存する場所を選択します。ビデオ録画は、プログラムをインストールする場所とは別の、システムドライブ以外の場所に保存することをMilestoneは推奨します。デフォルトの場所は、空き容量が最も多いドライブです。

   4. **ビデオ録画の保存期間**フィールドで、録画を保存する期間を設定します。1日から365,000日の間の日数を入力できます。デフォルトの保存期間は7日間です。

   5. **続行**をクリックします。

8. **レコーディングサーバーのIPアドレス**ページは、**カスタム**を選択した場合にのみ表示されます。このコンピュータにインストールするレコーティングサーバーの数を指定します。**続行**をクリックします。

9. **レコーディングサーバーのサービスアカウントを選択**で、レコーディングサーバーのサービスアカウントとして**この定義済みアカウント**または**このアカウント**のいずれかを選択します。

   必要に応じてパスワードを入力します。

   > アカウントのユーザー名は、1単語にしてください。スペースは使用できません。

   続行をクリックします。

10. **暗号化を選択**ページでは、以下の通信フローを保護できます。

    - レコーディングサーバー、データコレクター、マネジメントサーバー間

      内部通信フローで暗号化を有効にするには、**サーバー証明書**セクションで証明書を選択します。

      > レコーディングサーバーからマネジメントサーバーへの通信を暗号化する場合、システムは、マネジメントサーバーからレコーディングサーバーへの通信も暗号化するよう求めます。

    - レコーディングサーバーとクライアント間

      レコーディングサーバーと、レコーディングサーバーからデータストリームを受け取るクライアントコンポーネント間の暗号化を有効にするには、**ストリーミングメディア証明書**セクションで証明書を選択します。

    - モバイルサーバーとクライアント間

      モバイルサーバーからデータストリームを取得するクライアントコンポーネント間の暗号化を有効にするには、**モバイルストリーミングメディア証明書**セクションで証明書を選択します。

    - イベントサーバーと通信するコンポーネントとイベントサーバー間

      イベントサーバーと通信するコンポーネント(LPR Serverなど) とイベントサーバー間の暗号化を有効にするには、**イベントサーバー& 拡張機能**セクションで証明書を選択します。

    すべてのシステムコンポーネントに対して同じ証明書を使用することも、システムコンポーネントごとに異なる証明書を使用することもできます。

    安全なコミュニケーションのためのシステムの準備についての詳細は、以下を参照してください:

    - 136ページの安全な通信(説明付き)
    - 証明書に関するMilestoneガイド

    インストール後、通知エリアのManagement Server Managerトレイアイコンの Server Configuratorから暗号化を有効にすることもできます。

11. **ファイルの場所と製品の言語を選択**ページで、プログラムファイルの**ファイルの場所**を選択します。

    > すでにMilestone XProtect VMSがコンピュータにインストールされている場合、このフィールドは無効になっています。このフィールドには、コンポーネントがインストールされる場所が表示されます。

12. **製品の言語**フィールドで、どの言語でXProtect製品をインストールするのか選択します。**インストール**をクリックします。

    ソフトウェアがインストールされます。インストールが完了すると、正常にインストールされたシステムコンポーネントのリストが表示されます。**閉じる**をクリックします。

13. フェールオーバーレコーディングサーバーがインストールされたら、Recording Server Managerトレイアイコンでその状態を確認し、Management Client内でその設定を行うことができます。詳細については、181ページの初期構成タスクリストを参照してください。

Download Managerを介したフェールオーバーレコーディングサーバーのインストール

> ワークグループを実行する場合は、フェールオーバーレコーディングサーバーを別の方法でインストールする必要があります(168ページのワークグループのインストールを参照) 。

1. Management Serverがインストールされているコンピュータから、Management Serverのダウンロードウェブページに移動します。Windowsの**スタート**メニューで**Milestone > 管理インストールページ**の順に選択し、将来、他のコンピュータにシステムコンポーネントをインストールする際に使用できるよう、インターネットアドレスを書き留めるかコピーします。アドレスは通常、*http://[management server address]/installation/Admin/default-en-US.htm*です。

   システムコンポーネントをインストールするコンピュータにログインします。

2. インターネットブラウザを開き、Management Serverのダウンロードウェブページのアドレスをアドレスフィールドに入力して、Enterキーを押します。

3. **レコーディングサーバーインストーラ**の下にある**すべての言語**を選択して、レコーディングサーバーのインストーラをダウンロードします。インストーラを保存するか、ウェブページから直接実行します。

4. インストール中に使用する**言語**を選択します。**続行**をクリックします。

5. **インストールのタイプを選択**ページで**フェールオーバー**を選択し、レコーディングサーバーをフェールオーバーレコーディングサーバーとしてインストールします。

6. **レコーディングサーバーの設定**ページで、さまざまなレコーディングサーバーの設定を行います。フェールオーバーレコーディングサーバーの名前、マネジメントサーバーのアドレス、メディアデータベースへのパス。**続行**をクリックします。

7. フェイルオーバーレコーディングサーバーをインストールする際には、**レコーディングサーバーのサービスアカウントを選択**ページで**このアカウント**と名付けられた特定のユーザーアカウントを使用する必要があります。これにより、フェールオーバーユーザーアカウントが作成されます。必要に応じて、パスワードを入力して確認します。**続行**をクリックします。

8. **暗号化を選択**ページでは、以下の通信フローを保護できます。

   - レコーディングサーバー、データコレクター、マネジメントサーバー間

     内部通信フローで暗号化を有効にするには、**サーバー証明書**セクションで証明書を選択します。

     > レコーディングサーバーからマネジメントサーバーへの通信を暗号化する場合、システムは、マネジメントサーバーからレコーディングサーバーへの通信も暗号化するよう求めます。

   - レコーディングサーバーとクライアント間

     レコーディングサーバーと、レコーディングサーバーからデータストリームを受け取るクライアントコンポーネント間の暗号化を有効にするには、**ストリーミングメディア証明書**セクションで証明書を選択します。

   - モバイルサーバーとクライアント間

     モバイルサーバーからデータストリームを取得するクライアントコンポーネント間の暗号化を有効にするには、**モバイルストリーミングメディア証明書**セクションで証明書を選択します。

   - イベントサーバーと通信するコンポーネントとイベントサーバー間

     イベントサーバーと通信するコンポーネント(LPR Serverなど) とイベントサーバー間の暗号化を有効にするには、**イベントサーバー& 拡張機能**セクションで証明書を選択します。

   すべてのシステムコンポーネントに対して同じ証明書を使用することも、システムコンポーネントごとに異なる証明書を使用することもできます。

   安全なコミュニケーションのためのシステムの準備についての詳細は、以下を参照してください:

   - 136ページの安全な通信(説明付き)
   - 証明書に関するMilestoneガイド

   インストール後、通知エリアのManagement Server Managerトレイアイコンから暗号化を有効にすることもできます。

9. **ファイルの場所と製品の言語を選択**ページで、プログラムファイルの**ファイルの場所**を選択します。

   > すでにMilestone XProtect VMSがコンピュータにインストールされている場合、このフィールドは無効になっています。このフィールドには、コンポーネントがインストールされる場所が表示されます。

10. **製品の言語**フィールドで、どの言語でXProtect製品をインストールするのか選択します。**インストール**をクリックします。

    ソフトウェアがインストールされます。インストールが完了すると、正常にインストールされたシステムコンポーネントのリストが表示されます。**閉じる**をクリックします。

11. フェールオーバーレコーディングサーバーがインストールされると、Failover Serverサービストイアイコンでその状態を確認し、Management Client内でその設定を行うことができます。詳細については、181ページの初期構成タスクリストを参照してください。

デフォルト以外のポートを用いたXProtect VMSのインストール

XProtect VMSのインストールには、特定のポートが必要です。特に、IISでManagement ServerとAPI Gatewayが実行されており、特定のポートが空いていることが条件となります。このトピックでは、XProtect VMSをインストールし、IISでデフォルト以外のポートを使用する方法について説明します。API Gatewayのみをインストールする場合も同様です。

VMSが使用するすべてのポートの概要は、XProtectVMSシステム管理者マニュアル(https://doc.milestonesys.com/2023r3/ja-JP/portal/htm/chapter-page-mc-administrator-manual.htm)を参照してください。

IISがまだシステムにインストールされていない場合、XProtect VMSのインストーラはIISをインストールし、デフォルトのポートでデフォルトのウェブサイトを使用します。

XProtect VMSのデフォルトを使用しないようにするには、IISを先にインストールしてください。オプションで新しいウェブサイトを追加するか、デフォルトのウェブサイトを使用して続行します。

HTTPSのバインディングがまだ存在しない場合は追加し、コンピュータ上で有効な証明書を選択します(XProtect VMSのインストール時に選択する必要があります)。HTTPとHTTPSのバインディングのポート番号を、お好みの利用可能なポートに編集してください。

XProtect VMSインストーラを実行し、**カスタム**インストールを選択します。

インストール時に、利用可能なウェブサイトが複数ある場合は、**XProtectシステムで使用するIISのウェブサイトを選択**ページが表示されます。XProtectシステムにどのウェブサイトを使用するかを選択する必要があります。インストーラは、変更されたポート番号を使用します。

コマンドラインシェルを介したサイレントインストール(説明付き)

システム管理者はサイレントインストールを実行することで、ユーザーの介入なく、エンドユーザーへの影響を最小限に抑える形で、大規模なネットワークにわたってXProtect VMSとSmart Clientソフトウェアをインストールおよびアップグレードできます。

XProtect VMSとSmart Clientインストーラー(.exeファイル)のコマンドライン引数は異なります。それぞれが特有のコマンドラインパラメータセットを有しており、これらはコマンドラインシェルまたは引数ファイルを介して直接呼び出すことができます。コマンドラインシェルでは、インストーラのコマンドラインオプションも使用できます。

Microsoft System Center Configuration Manager(SCCMまたはConfigMgrとも呼ばれます)のように、XProtectインストーラ、そのコマンドラインパラメータ、コマンドラインオプションを、サイレント配布およびソフトウェアインストール用のツールと組み合わせることができます。このようなツールの詳細については、メーカーのウェブサイトを参照してください。またMilestone Software ManagerをXProtect VMS、デバイスパック、Smart Clientのリモートインストールおよび更新に使用することもできます。詳細については、Milestone Software Managerの管理者マニュアルを参照してください。

コマンドラインパラメータと引数ファイル

サイレントインストール中は、さまざまなVNSシステムコンポーネントと密接にリンクしている設定に加え、コマンドラインパラメータと引数ファイルを用いてその内部通信を指定することができます。コマンドラインパラメータと引数ファイルは、新規インストールにおいてのみ使用してください。これは、コマンドラインパラメータによって表される設定はアップグレード中には変更できないためです。

これは、コマンドラインパラメータによって表される設定はアップグレード中には変更できないためです。利用可能なコマンドラインパラメータを表示し、インストーラ用の引数ファイルを生成するには、コマンドラインシェルでインストーラが配置されているディレクトリに移動し、以下のコマンドを入力します。

```
[NameOfExeFile].exe --generateargsfile=[path]
```

例：

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=c:\temp
```

保存された引数ファイル(Arguments.xml) 内では、コマンドラインパラメータごとにその目的についての記述が添えられます。コマンドラインパラメータの値がインストールのニーズに適合するよう、引数ファイルを修正したうえで保存することができます。

インストーラで引数ファイルを使用したい場合は、以下のコマンドを入力することで`--arguments`コマンドラインオプションを使用します。

```
[NameOfExeFile].exe --quiet --arguments=[path]\[filename]
```

例：

```
Milestone XProtect VMS Products 2023 R3 System Installer.exe --quiet
--arguments=C:\temp\arguments.xml
```

コマンドラインオプション

コマンドラインシェルでは、インストーラをコマンドラインオプションと組み合わせることもできます。コマンドラインオプションは通常、コマンドの動作を修正する目的で使用します。

コマンドラインオプションの全リストを表示するには、コマンドラインシェルでインストーラが配置されているディレクトリに移動し、`[NameOfExeFile].exe --help`と入力します。インストールを成功させるためには、値を必要とするコマンドラインオプションに対して値を指定する必要があります。

コマンドラインパラメータとコマンドラインオプションは、両方とも同一のコマンド内で使用できます。その際、`--parameters`コマンドラインオプションを使用し、それぞれのコマンドラインパラメータをコロン(:) で区切ります。以下の例では、`--quiet`、`--showconsole`、`--parameters`はコマンドラインオプションである一方、`ISFAILOVER`と`RECORDERNAME`はコマンドラインパラメータとなっています。

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --showconsole
--parameters=ISFAILOVER:true:RECORDERNAME:Failover1
```

レコーディングサーバーのサイレントインストール

サイレントインストール時には、インストールが完了しても通知が送られません。通知を受け取るには、コマンドに`--showconsole`コマンドラインオプションを加えます。インストールが完了すると、Milestone XProtect Recording Serverトレイアイコンが表示されます。

以下のコマンドラインの例では、角括弧(**[]**)内のテキストと角括弧そのものを実数値に置き換える必要があります。例:[path]の代わりに、`d:\program files\`、`d:\record\`、`\\network-storage-02\surveillance`などと入力します。`--help`コマンドラインオプションを使用すれば、各コマンドラインオプション値の正規形式について確認できます。

1. Recording Serverコンポーネントをインストールするコンピュータにログインします。
2. インターネットブラウザを開き、管理者を対象としたManagement Serverのダウンロード用ウェブページのアドレスをアドレスフィールドに入力し、Enterを押します。

   アドレスは通常、`http://[マネジメントサーバーのアドレス]:[ポート]/installation/Admin/default-en-US.htm`となっています。
3. **レコーディングサーバーインストーラ**の下にある**すべての言語**を選択して、レコーディングサーバーインストーラをダウンロードします。
4. 希望のコマンドラインシェルを開きます。Windowsコマンドプロンプトを開くには、Windowsのスタートメニューを開いて**cmd**と入力します。
5. ダウンロードしたインストーラが保存されているディレクトリに移動します。
6. 以下の2通りのシナリオのいずれであるかに応じて、インストールを続行します。

シナリオ1:既存のインストールをアップグレードするか、Management Serverコンポーネントと併せてデフォルトの値でサーバーにインストールする

- 以下のコマンドを入力してインストールを開始します。

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
```

シナリオ2:分散システムにインストールする

1. 以下のコマンドを入力して、コマンドラインパラメータが記された引数ファイルを生成します。

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=
[path]
```

2. 指定したパスから引数ファイル(Arguments.xml) を開き、必要に応じてコマンドラインパラメータの値を修正します。

> SERVERHOSTNAMEとSERVERPORTのコマンドラインパラメータに有効な値が指定されていることを確認します。そうでない場合、インストールは完了しません。

4. 引数ファイルを保存します。
5. コマンドラインシェルに戻り、以下のコマンドを入力することで、引数ファイルで指定したコマンドラインパラメータ値でインストールを実行します。

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
--arguments=[path]\[filename]
```

XProtect Smart Clientサイレントインストール

サイレントインストール時には、インストールが完了しても通知が送られません。通知を受け取るには、コマンドに`--showconsole`コマンドラインオプションを加えます。インストールが完了するとXProtect Smart Clientへのショートカットがデスクトップに表示されます。

以下のコマンドラインの例では、角括弧([ ]) 内のテキストと角括弧そのものを実数値に置き換える必要があります。例：[path]の代わりに、`d:\program files\`、`d:\record\`、`\\network-storage-02\surveillance`などと入力します。`--help`コマンドラインオプションを使用すれば、各コマンドラインオプション値の正規形式について確認できます。

1. インターネットブラウザを開き、エンドユーザーを対象としたManagement Serverのダウンロード用ウェブページのアドレスをアドレスフィールドに入力し、Enterを押します。

   アドレスは通常、`http://[マネジメントサーバーのアドレス]:[ポート]/installation/default-en-US.htm`となっています。

2. **XProtect Smart Clientインストーラ**の下にある**すべての言語**を選択して、XProtect Smart Clientインストーラをダウンロードします。
3. 希望のコマンドラインシェルを開きます。Windowsコマンドプロンプトを開くには、Windowsのスタートメニューを開いて**cmd**と入力します。
4. ダウンロードしたインストーラが保存されているディレクトリに移動します。
5. 以下の2通りのシナリオのいずれであるかに応じて、インストールを続行します。

シナリオ1：既存のインストールをアップグレードするか、デフォルトのコマンドラインパラメータ値でインストールする

- 以下のコマンドを入力してインストールを開始します。

```
"XProtect Smart Client 2023 R3 Installer.exe" --quiet
```

シナリオ2: xml引数をインプットとして使用して、コマンドラインパラメータのカスタム値でインストールする

1. 以下のコマンドを入力して、コマンドラインパラメータが記された引数xmlファイルを生成します。

```
"XProtect Smart Client 2023 R3 Installer.exe" --generateargsfile=
[path]
```

2. 指定したパスから引数ファイル(Arguments.xml) を開き、必要に応じてコマンドラインパラメータの値を修正します。
3. 引数ファイルを保存します。
4. コマンドラインシェルに戻り、以下のコマンドを入力することで、引数ファイルで指定したコマンドラインパラメータ値でインストールを実行します。

```
"XProtect Smart Client 2023 R3 Installer.exe" --quiet --arguments=
[path]\[filename]
```

ログサーバーをサイレントインストールする

サイレントインストール時には、インストールが完了しても通知が送られません。通知を受け取るには、コマンドに`--showconsole`コマンドラインオプションを加えます。

以下のコマンドラインの例では、角括弧([ ]) 内のテキストと角括弧そのものを実数値に置き換える必要があります。例: [path]の代わりに、`d:\program files\`、`d:\record\`、`\\network-storage-02\surveillance`などと入力します。`--help`コマンドラインオプションを使用すれば、各コマンドラインオプション値の正規形式について確認できます。

1. Log Serverコンポーネントをインストールするコンピュータにログインします。
2. インターネットブラウザを開き、管理者を対象としたManagement Serverのダウンロード用ウェブページのアドレスをアドレスフィールドに入力し、Enterを押します。

   アドレスは通常、`http://[`マネジメントサーバーのアドレス`]:[`ポート`]/installation/Admin/default-en-US.htm`となっています。
3. **ログサーバーインストーラ**の下の**すべての言語**を選択して、ログサーバーインストーラをダウンロードします。
4. 希望のコマンドラインシェルを開きます。Windowsコマンドプロンプトを開くには、Windowsのスタートメニューを開いて**cmd**と入力します。
5. ダウンロードしたインストーラが保存されているディレクトリに移動します。
6. 以下の2通りのシナリオのいずれであるかに応じて、インストールを続行します。

シナリオ1: 既存のインストールをアップグレードするか、デフォルトのコマンドラインパラメータ値でインストールする

- 以下のコマンドを入力してインストールを開始します。

```
"XProtect Log Server 2023 R3 Installer x64.exe" --quiet --showconsole
```

シナリオ2：XML引数をインプットとして使用して、コマンドラインパラメータのカスタム値でインストールする

1. 以下のコマンドを入力して、コマンドラインパラメータが記された引数xmlファイルを生成します。

```
"XProtect Log Server 2023 R3 Installer x64.exe" --generateargsfile=
[path]
```

2. 指定したパスから引数ファイル(Arguments.xml) を開き、必要に応じてコマンドラインパラメータの値を修正します。
3. 引数ファイルを保存します。
4. コマンドラインシェルに戻り、以下のコマンドを入力することで、引数ファイルで指定したコマンドラインパラメータ値でインストールを実行します。

```
"XProtect Log Server 2023 R3 Installer x64.exe" --quiet --arguments=
[path]\[filename] --showconsole
```

専用のサービスアカウントを使用してサイレントインストール

自動でXProtect VMSのインストールを行うには、以下の表の引数を指定してインストーラを起動する必要があります。引数は、インストール前に作成する引数XMLファイルに作成、保存する必要があります。

引数	説明
`--quiet`	サイレントインストールを強制的に実行します。
`--arguments`	完全な設定を含む引数XMLファイルへのパス。パスは次の通りです：`C:\Arguments.xml`
`--license`	ライセンスファイルへのパス。

専用のサービスアカウントを使用する

この説明は、統合セキュリティのための専用サービスアカウントを使用することを前提としています。どのユーザーがログインしていても、サービスは常に専用アカウントで実行されるため、そのアカウントが、例えばタスクの実行や、ネットワーク、ファイル、共有フォルダーへのアクセスに必要なすべての権限を有していることを確認する必要があります。

サービスアカウントは、引数XMLファイルで以下のキーを用いて指定する必要があります。

`SERVICEACCOUNT`
`SERVICEACCOUNT_NONLOC`

サービスアカウントのパスワードは、以下のキーの値にプレーンテキストで指定する必要があります。

```
ENCRYPTEDPASSWORD
```

例：サイレントモードでインストールを開始するコマンドライン

```
"Milestone XProtect VMS Products 2023 R2 System Installer.exe" --quiet --
arguments=C:\Arguments.xml --license=C:\M01-C01-231-01-ABCDEF.lic
```

例：専用サービスアカウントの使用に基づく引数ファイル

```
<?xml version="1.0" encoding="utf-8"?>
<CommandLineArguments xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="urn:milestone-systems">
  <InstallEnvironment>
    <Parameters>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>USERACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT_NONLOC</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>sampleaccountpasswordplaintext</Value>
        <Key>ENCRYPTEDPASSWORD</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>%PROGRAMFILES%\Milestone</Value>
        <Key>TARGETDIR</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsXPCO</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsDPInstaller</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>false</Value>
        <Key>LEGACY</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>yes</Value>
        <Key>SQL-KEEP-DATA</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>no</Value>
        <Key>SQL-CREATE-DATABASE</Key>
      </KeyValueParametersOfStringString>
```

```
      <KeyValueParametersOfStringString>
        <Value>True</Value>
        <Key>IS_EXTERNALLY_MANAGED</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_MS</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IDP;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IDP</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IM;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IM</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_ES</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_
LogServerV2;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated;Application
Name=Surveillance_LogServerV2</Value>
        <Key>SQL_CONNECTION_STRING_LOG</Key>
      </KeyValueParametersOfStringString>
    </Parameters>
  </InstallEnvironment>
</CommandLineArguments>
```

インストールを実行する前に完了しておくべき前提条件

- インストールに使用するアカウントと同様に、サービスアカウントも作成する必要があります。
- サービスアカウントは、インストールを実行するコンピュータ上でサービスとしてのログインが許可されている必要があります。ログオン・アズ・ア・サービスをご参照ください。
- XProtectが使用するデータベースを作成し、引数のXMLファイル内でデータベースに名前を付ける必要があります。以下に例を示します。

データベース名
Surveillance
Surveillance_IDP
Surveillance_IM
Surveillance_LogServerV2

- データベースは以下のリストに従って設定する必要があります。

データベースの設定
デフォルトの照合順序は「SQL_Latin1_General_CP1_CI_AS」に設定する必要があります。
ALLOW_SNAPSHOT_ISOLATIONをONにします
READ_COMMITTED_SNAPSHOTをONにします

- SQLサーバーのログインは、サービスアカウントと、各データベースでインストールを実行するために使用するアカウント用に作成する必要があります。各データベースにデータベースユーザーを作成し、そのユーザーは各データベースのdb_owner役割のメンバーでなければなりません。

ワークグループのインストール

Active Directoryサーバーを伴うドメインセットアップは使用しないけれども、ワークグループセットアップを使用する場合は、インストール時に以下を実行してください。

> 分散型のコンピュータはすべて、ドメインまたはワークグループに配置する必要があります。

1. 共通管理者アカウントを使用して、Windowsへログインします。

   > システムのすべてのコンピュータで同じアカウントを使用していることを確認します。

2. 必要に応じて、マネジメントサーバーまたはレコーディングサーバーのインストールを開始し、**カスタム**をクリックします。
3. 手順2の選択に応じて、共通のシステム管理者アカウントを使用して、Management ServerまたはRecording Serverのインストールを選択します。
4. インストールを終了します。
5. 手順1～4を繰り返し、接続する他のすべてのシステムをインストールします。これらはすべて、共通管理者アカウントを使用してインストールしなければなりません。

クラスタへのインストール

クラスタをインストールする前に、124ページの複数のマネジメントサーバー(クラスタリング)(説明付き)および124ページのクラスタリングの要件を参照してください。

> ここでの説明と図は、実際に画面上に表示されるものとは異なる場合があります。

マネジメントサーバーのインストール

1. マネジメントサーバーと、そのすべてのサブコンポーネントをクラスタ内の最初のサーバーにインストールします。

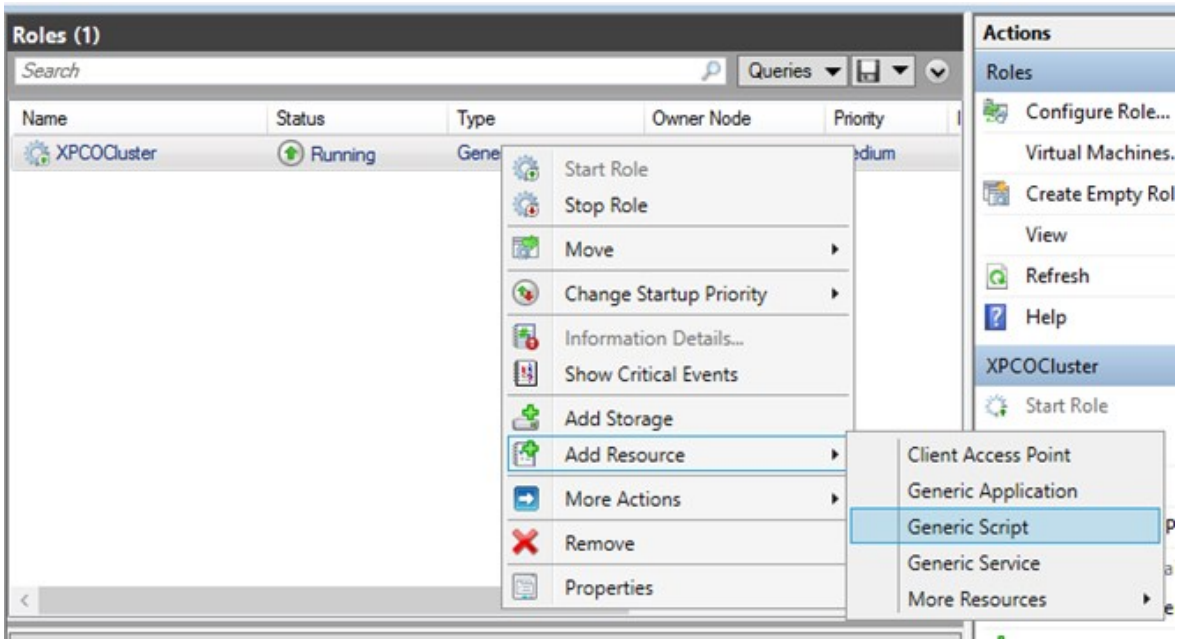
> 特定のユーザーには、ネットワークサービスとしてではなく、マネジメントサーバーをインストールする必要があります。これには、**カスタム**インストールオプションを使用する必要があります。また、特定のユーザーには共有ネットワークドライブへのアクセスと、可能であれば無期限のパスワードを割り当てる必要があります。

Management Serverサービスを、フェールオーバークラスタ内の汎用サービスとして設定します。

1. マネジメントサーバーをインストールした最後のサーバーで**スタート> 管理ツール**に移動し、Windowsの**フェールオーバークラスタ管理**を開きます。**フェールオーバークラスタマネージャ**ウィンドウでクラスタを展開し、**役割**を右クリックしてから、**役割を設定**を選択します。

2. **高可用性ウィザード> 開始前に**ページで、**次へ**をクリックします。
3. **役割を選択**ページで**汎用サービス**を選択し、**次へ**をクリックします。
4. **サービスを選択**ページで**Milestone XProtect Management Server**サービスを選択し、**次へ**をクリックします。
5. **クライアントのアクセスポイント**ページで、クライアントがサービスにアクセスする時に使用する名前(クラスタのホスト名)を指定します。ホスト名は、クラスタ名と異なるものでなければなりません。**次へ**をクリックします。
6. **ストレージを選択**ページでは、このサービスにストレージは必要ないため、**次へ**をクリックします。
7. **レジストリ設定を複製**ページでは、レジストリ設定を複製する必要はないため、**次へ**をクリックします。
8. **確認**ページでは、クラスタサービスが要件に従って設定されていることを確認したら**次へ**をクリックします。
9. **高可用性を設定**ページで、**次へ**をクリックします。
10. **サマリー**ページで、**終了**をクリックして、フェールオーバークラスタの汎用サービスとしてマネジメントサーバーの設定を完了します。

11. 作成した役割を右クリックし、**リソースを追加 > 汎用スクリプト**をクリックします。Milestone XProtect Event Serverを選択して、**Milestone XProtect Event Server**サービスをリソースとして**Milestone XProtect Management Server Cluster**サービスに追加します。



12. ステップ11を繰り返して、Log Serverなど、クラスタに必要なすべてのサービスを追加します。Milestone XProtect Event ServerとData Collector serverの両方をサービスとして追加して、最適な展開を実現する必要があります。さらに、マネジメントサーバーが停止すると必ずイベントサーバーも停止するよう、マネジメントサーバーに依存するサービスとしてMilestone XProtect Event Serverを設定する必要があります。

13. 追加されたすべてのサービスは、ウィンドウの下部ペインに表示されます。

クラスタURLのアップデート

構成を変更する場合は、Microsoftフェールオーバークラスターマネージャーで、サービスのコントロールとモニタリングを一時停止し、Server Configuratorが変更を行ってManagement Serverサービスを起動 / 停止できるようにします。フェールオーバークラスターサービスのセットアップタイプを手動に変更しても、Server Configuratorとは矛盾しないはずです。

Management Serverコンピュータで以下を実行します。

1. マネジメントサーバーがインストールされている各コンピュータでServer Configuratorを起動します。
2. **[登録]**ページに移動します。
3. 鉛筆( ) の記号をクリックして、マネジメントサーバーのアドレスを編集可能にします。
4. マネジメントサーバーアドレスをクラスターのURLに変更します(例 : `http://MyCluster`) 。
5. **[登録]**をクリックします。

Management Server(Recording Server、Mobile Server、Event Server、API Gatewayなど) を使用するコンポーネントを備えたコンピューターの場合 :

1. 各コンピュータでServer Configuratorを起動します。
2. **[登録]**ページに移動します。
3. マネジメントサーバーアドレスをクラスターのURLに変更します(例 : `http://MyCluster`) 。
4. **[登録]**をクリックします。

クラスタ環境で外部IDPに証明書を使用する

単一サーバー環境にXProtectをインストールすると、外部IDPの設定データがデータ保護API(DPAPI) で保護されます。クラスタでマネジメントサーバーを設定する場合、スムーズなノードのフェールオーバーを徹底するため、証明書で外部IDPの設定データを保護する必要があります。

証明書を生成する詳細な方法については、証明書に関するMilestoneガイドを参照してください。

証明書を個人の証明書ストアにインポートし、コンピュータで証明書を信頼済みに設定する必要があります。

データ保護を設定するには、Identity Providerの設定に証明書のサムプリントを追加する必要があります。

1. 証明書を個人の証明書ストアにインポートし、以下を確認します。
   - 証明書が有効になっている
   - Identity Provider app pool (IDP)アカウントに、証明書のプライベートキーへのアクセス権限がある

   アカウントに証明書のプライベートキーへのアクセス権限があるかどうかを確認する詳細な方法については、「証明書に関するMilestoneガイド」を参照してください。
2. Identity Providerのインストールパス(`[Install path]\Milestone\XProtect Management Server\IIS\Identity Provider`)で`appsettings.json`ファイルを見つけます。
3. 対象セクションで証明書のサムプリントを設定します。

```
"DataProtectionSettings": {
 "ProtectKeysWithCertificate": {
  "Thumbprint": ""
 }

},
```

4. マネジメントサーバーのすべてのノードでステップ3を繰り返します。
5. ノードでフェールオーバーを強制実行して、証明書の設定が正しいことを確認します。
6. Management Clientを使用して再度ログインし、外部プロバイダ設定を適用します。設定を適用済みの場合は、管理クライアントの外部IDPからクライアントシークレットを再入力する必要があります。

外部IDPの設定が証明書で保護されている場合のエラーのトラブルシューティング

無効な証明書/期限切れの証明書

サムプリントを設定した証明書が信頼できない場合や期限が切れている場合、Identity Providerは開始されません。証明書が無効の場合、Identity Providerのログ(`C:\ProgramData\Milestone\Identity Provider\Logs\Idp.log`) で明確に示されます。

解決策:

証明書が有効かつコンピュータで信頼済みであることを確認します。

証明書のプライベートキーへのアクセス権限がない場合

プライベートキーへのアクセス権限がない場合、Identity Providerはデータを保護できません。Identity Providerに権限がない場合、次のエラーメッセージがIdentity Provider(`C:\ProgramData\Milestone\Identity Provider\Logs\Idp.log`) のログファイルに書き込まれます。

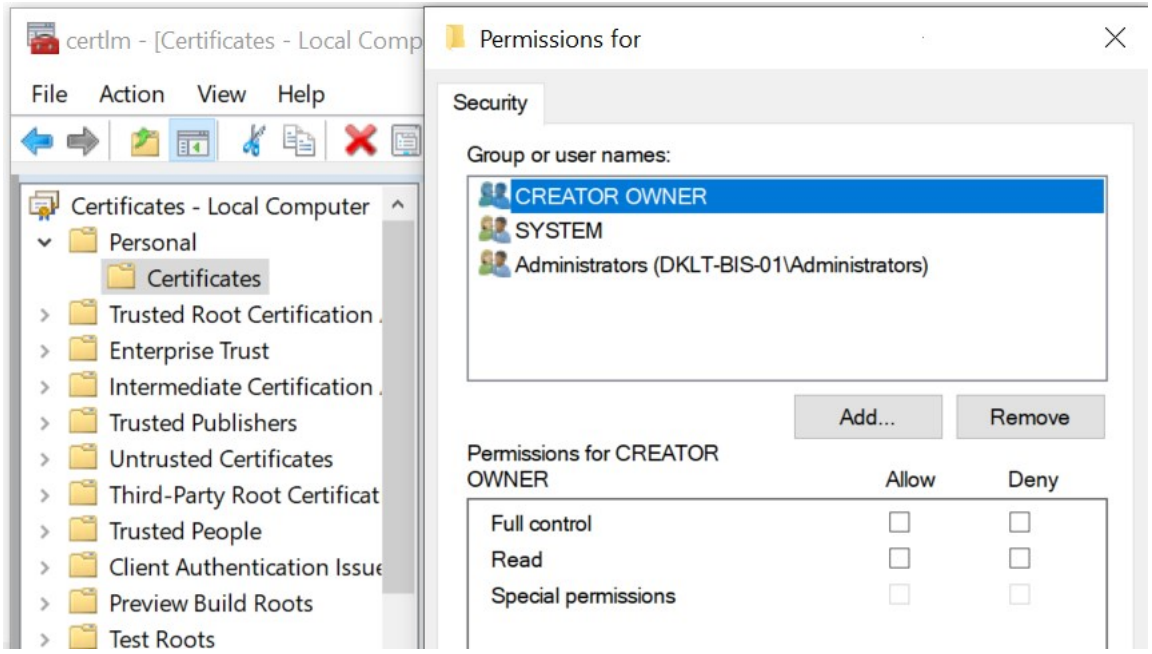
```
ERROR- An exception occurred while processing the key element '<key id="
[installation specific]" version="1" />'.
Internal.Cryptography.CryptoThrowHelper+WindowsCryptographicException:
Keyset does not exist
```

解決策:

Identity Provider app pool (IDP)アカウントに証明書のプライベートキーへのアクセス権限があることを確認します。

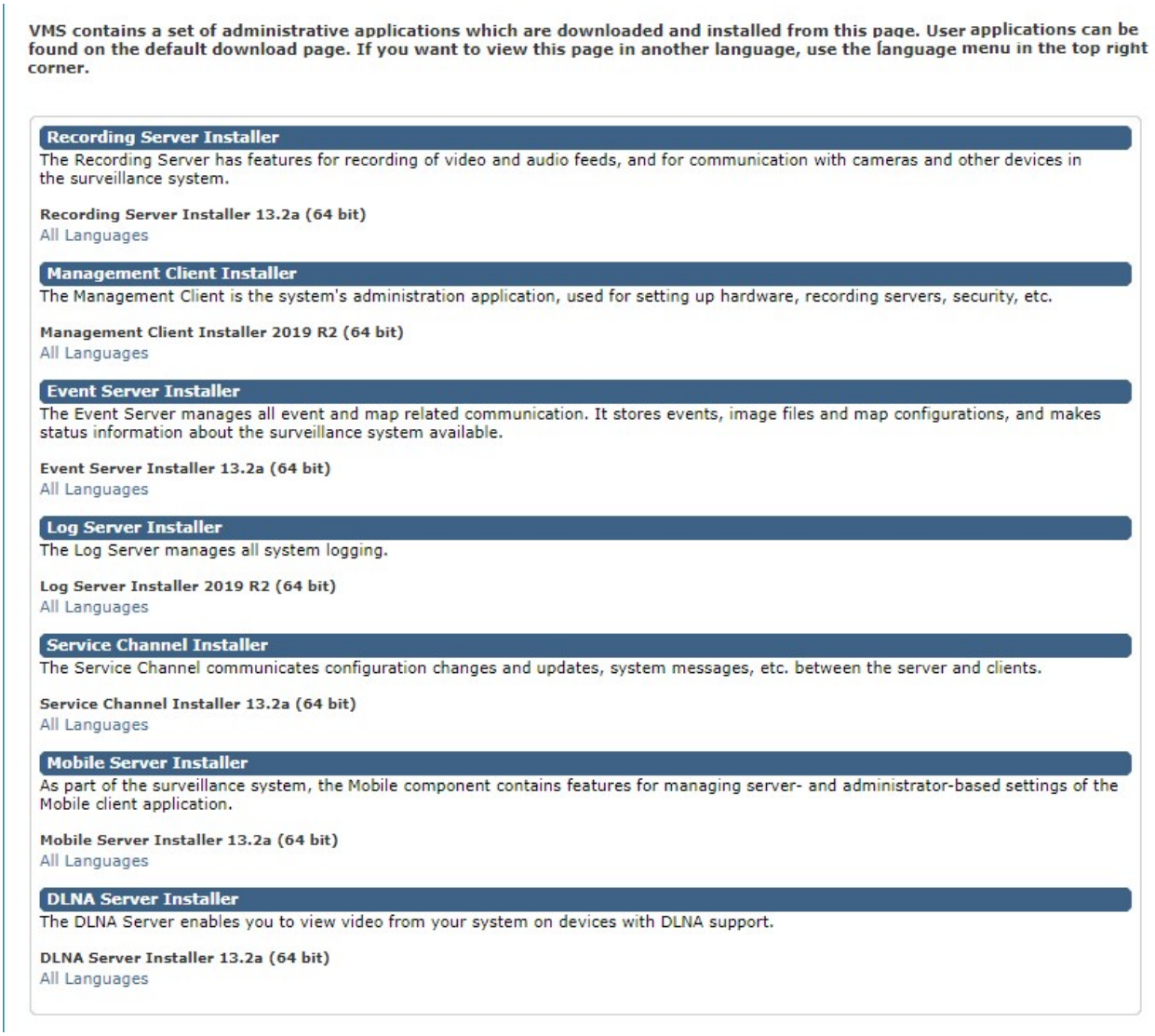
証明書のプライベートキーへのアクセス権限を確認する方法

1. Windowsのタスクバーで、**スタート**を選択し、コンピュータの証明書管理ツール(certlm.msc) を開きます。
2. 個人の証明書ストアにアクセスし、暗号化に使用する証明書を探します。
3. 証明書を右クリックし、**すべてのタスク > プライベートキーを管理**を選択します。
4. **権限設定**でIdentity Provider app pool (IDP)のアカウントに読み取り権限があることを確認します。



Download Manager/ダウンロードWebページ

ManagementServerには、組み込みWebページがあります。このWebページを使うと、管理者やエンドユーザーはXProtectシステムの必要なコンポーネントを、任意の場所から(ローカルまたはリモートで) ダウンロードしてインストールすることができます。



このWebページは、デフォルトで、システムインストールの言語と一致する言語バージョンで、次の2種類のコンテンツを表示できます。

- **管理者**向けのWebページでは、主要なシステムコンポーネントをダウンロードしてインストールできます。通常、Webページはマネジメントサーバーのインストール終了後に自動的に読み込まれ、デフォルトのコンテンツが表示されます。マネジメントサーバーで、Windowsの**[スタート]**メニューから**[プログラム]>Milestone>[管理インストールページ]**の順に選択すると、Webページにアクセスできます。それ以外の場合は、以下のURLを入力してください。

  http://[マネジメントサーバーのアドレス]:[ポート]/installation/admin/

  [マネジメントサーバーのアドレス]はマネジメントサーバーのIPアドレスまたはホスト名であり、[ポート]はマネジメントサーバーでIISが使用するように設定されたポート番号です。

- エンド**ユーザー**向けのWebページでは、デフォルト設定を使用してクライアントアプリケーションにアクセスできます。マネジメントサーバーで、Windowsの**[スタート]**メニューから**[プログラム]>Milestone>[公開インストールページ]**の順に選択すると、Webページにアクセスできます。それ以外の場合は、以下のURLを入力してください。

  http://[マネジメントサーバーのアドレス]:[ポート]/installation/

  [マネジメントサーバーのアドレス]はマネジメントサーバーのIPアドレスまたはホスト名であり、[ポート]はマネジメントサーバーでIISが使用するように設定されたポート番号です。

2つのWebページにはデフォルトのコンテンツがあるため、インストール後すぐに使用できます。なお、システム管理者としてDownload Managerを使用すると、Webページの表示内容をカスタマイズできます。また、Webページの2つのバージョン間で、コンポーネントを移動することもできます。コンポーネントを移動するには、コンポーネントをクリックし、コンポーネントを移動するWebページのバージョンをクリックします。

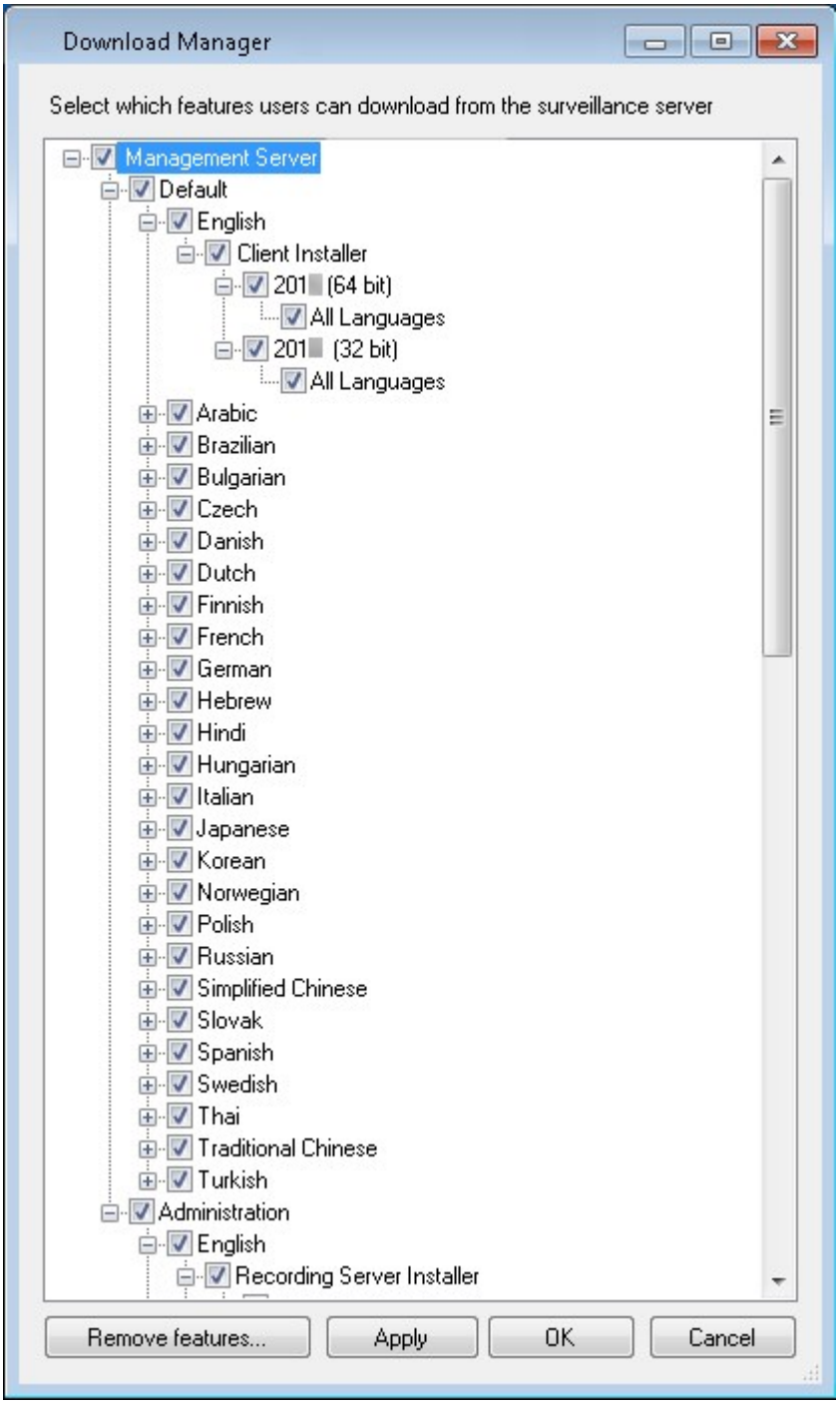
DownloadManagerではユーザーがダウンロードし、インストールできるコンポーネントを制御することはできますが、ユーザー権限の管理ツールとして使用することはできません。この種の権限は、ManagementClientで定義された役割によって決定されます。

マネジメントサーバーで、Windowsの**[スタート]**メニューから**[プログラム]>XProtect Download Manager>Milestone**の順に選択しすれば、XProtect Download Managerにアクセスできます。

Download Managerのデフォルト設定

Download Managerには、デフォルトの設定があります。これにより、組織のユーザーは最初から標準のコンポーネントにアクセスできます。

デフォルト設定では、追加またはオプションのコンポーネントをデフォルト設定によってダウンロードできます。通常は、マネジメントサーバーコンピュータからWebページにアクセスしますが、他のコンピュータからWebページにアクセスすることもできます。



- 1番目のレベル:XProtect製品を参照します。
- 2番目のレベル:Webページの2つの対象バージョンを示しています。**デフォルト**は、エンドユーザーに表示されるWebページのバージョンを示しています。**[システム管理]**は、システム管理者に表示されるWebページのバージョンを示しています。
- 3番目のレベル:Webページで使用できる言語を示しています。

- 4番目のレベル: ユーザーが使用できるか、使用可能にできるコンポーネントを示しています。
- 5番目のレベル: ユーザーが使用できるか、使用可能にできる各コンポーネントの特定のバージョンを示しています。
- 6番目のレベル: ユーザーが使用できるか、使用可能にできるコンポーネントの言語バージョンを示しています。

初期状態では標準のコンポーネントだけが使用可能であり、システムと同じ言語バージョンだけが使用可能になっていることで、インストールの時間を短縮し、サーバーのディスク容量を節約するのに役立ちます。誰も使用しないコンポーネントや言語バージョンがサーバーに存在する必要はないためです。

必要に応じてその他のコンポーネントや言語を使用可能にできます。また、不要なコンポーネントや言語を非表示にしたり削除したりできます。

Download Managerの標準インストーラ(ユーザー)

デフォルトでは、次のコンポーネントは、ユーザー向けのマネジメントサーバーのダウンロードWebページから個別にインストールできます(Download Managerで制御)。

- フェールオーバーレコーディングサーバーを含むレコーディングサーバー。フェールオーバーレコーディングサーバーは、最初にレコーディングサーバーとしてダウンロードおよびインストールされます。インストール処理中に、フェールオーバーレコーディングサーバーにすることを指定します。
- Management Client
- XProtect Smart Client
- イベントサーバー、マップ機能と組み合わせて使用されます。
- Logサーバーはシステム情報のロギングに必要な機能を提供するために使用されます。
- XProtect Mobileサーバー
- 組織によって、より豊富なオプションを利用できます。

デバイスパックのインストールについては、「179ページのDevice Packのインストーラ- ダウンロードする必要があります」を参照してください。

Download Managerインストーラコンポーネントの追加/公開

次の2つの手順を実行し、標準以外のコンポーネントおよび新しいバージョンをマネジメントサーバーのダウンロードページで使用可能にする必要があります。

最初に、新規/非標準コンポーネントをDownload Managerに追加します。次に、これを使用して、さまざまな言語バージョンのWebページで、どのコンポーネントを使用可能にするかを微調整します。

Download Managerが開いている場合は、閉じてから、新しいコンポーネントをインストールします。

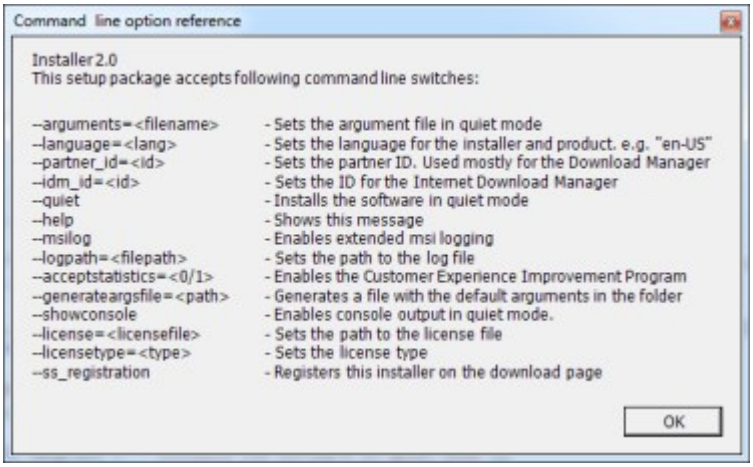
新規/非標準ファイルをDownload Managerに追加:

1. コンポーネントをダウンロードしたコンピュータで、Windowsの**[スタート]**に移動し、*コマンドプロンプト*に入ります。
2. *コマンドプロンプト*で、ファイル名(*.exe*)に[space]*--ss_registration*を付けて実行します。

   例:*MilestoneXProtectRecordingServerInstaller_x64.exe --ss_registration*

   これでファイルはDownloadManagerに追加されましたが、現在お使いのコンピュータにはまだインストールされていません。

インストーラコマンドの概要を取得するには、*コマンドプロンプト*で[スペース]*--help*と入力することで、以下のウィンドウを開きます:



新しいコンポーネントをインストールすると、Download Managerでデフォルトで選択され、Webページからすぐに使用可能になります。Download Managerのツリー構造でチェックボックスを選択または選択解除することで、Webページでいつでも機能を表示または非表示にすることができます。

Webページで、コンポーネントが表示される順番を変更できます。Download Managerのツリー構造で、コンポーネントアイテムをドラッグして必要な場所でドロップすると、順番を変更できます。

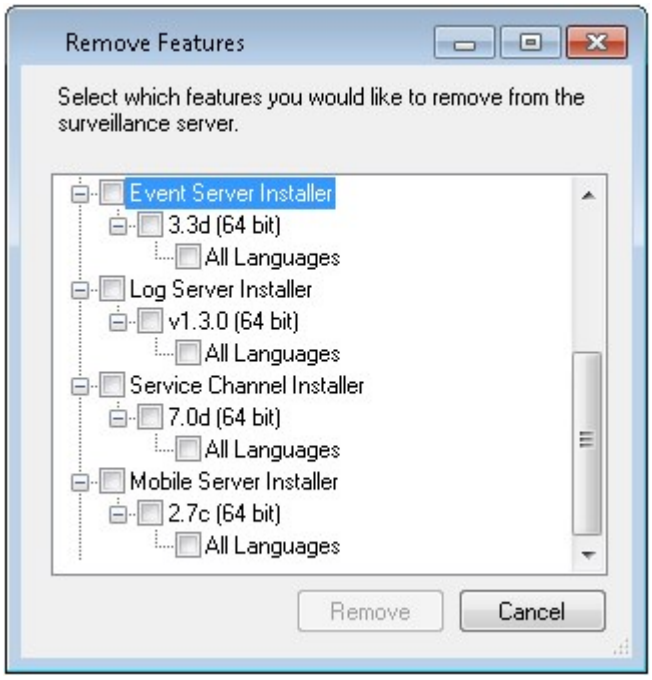
Download Managerインストーラコンポーネントを非表示化/削除

次の3つのオプションがあります:

- **のツリー構造のチェックボックスをクリアして、Webページからの**コンポーネントを非表示にするDownload Managerことができます。コンポーネントはマネジメントサーバーにインストールされたままであり、Download Managerのツリー構造のチェックボックスを選択することで、迅速にコンポーネントを再び利用可能にできます。

- マネジメントサーバーにあるコンポーネントのインストールを削除します。コンポーネントはDownload Managerに表示されなくなりますが、コンポーネントのインストールファイルは`C:\Program Files (x86)\Milestone\XProtect Download Manager`に保存されるため、必要であれば、この後再インストールすることができます。

  1. Download Managerで、**機能の削除**をクリックします。
  2. **機能の削除**ウィンドウで、削除する機能を選択します。



  3. **OK**と**はい**をクリックします。

- **不要な機能のインストールファイル**は、マネジメントサーバーから削除できます。組織では使用しない機能が分かっている場合、これによって、サーバーのディスク容量を削減するのに役立ちます。

Device Packのインストーラ- ダウンロードする必要があります

元のインストールに含まれていたDevice Pack(デバイスドライバーを含む)は、Download Managerには含まれていません。このため、Device Packを再インストールするか、またはDevice Packインストーラを使用可能にするためには、Download Managerに最新のDevice Packインストーラを追加/公開する必要があります。

1. 最新の正規デバイスパックは、Milestone Webサイトのダウンロードページ(https://www.milestonesys.com/downloads/)から入手できます。
2. 同じページにて、レガシードライバーでDevice Packをダウンロードできます。お使いのカメラが、Legacy Device Packのドライバーを使用しているかは、このWebサイト(https://www.milestonesys.com/community/business-partner-tools/device-packs/)で確認できます。
3. *--ss_registration*コマンドを使用して呼び出し、Download Managerに追加/発行します。

ネットワークに接続していない場合は、Download Managerからレコーディングサーバー全体を再インストールできます。レコーディングサーバーのインストールファイルは、コンピュータにローカル保存されます。これにより、デバイスパックが自動的に再インストールされます。

インストールログファイルとトラブルシューティング

インストール、アップグレード、アンインストール中は、以下をはじめとするさまざまなインストールログファイルにログエントリが書き込まれます: メインインストールログファイルである`installer.log`と、インストールしている各種システムコンポーネントに属しているログファイル。いずれのログエントリにもタイムスタンプが刻まれ、最新のログエントリがログファイルの末尾に配置されます。

Milestoneインストールログファイルはいずれも`C:\ProgramData\Installer\`フォルダーに配置されます。*I.logまたは*I[整数].logという名前を付けられたログファイルは新規インストールまたはアップグレードに関するログファイルです。一方、*U.logまたは*U[整数].logと名付けられたログファイルはアンインストールに関するものです。XProtectパートナーを介して、Milestoneシステムがインストール済みのサーバーを購入した場合は、インストールログファイルがない可能性があります。

ログファイルには、インストール、アップグレード、アンインストール中に使用される、コマンドラインパラメータとコマンドラインオプション、そしてその値に関する情報が記されます。使用したコマンドラインパラメータをログファイルで探すには、ログファイルの種類に応じて、**Command Line:**または**Parameter '**を検索します。

トラブルシューティングの際、最初に確認するのはメインインストールログファイル「installer.log」となります。インストール中に例外、エラー、警告が発生した場合、これらが記録されます。**exception**、**error**、**warning**がないか検索してみてください。「Exit code: 0」はインストールに成功したことを、「Exit code: 1」はその逆を表します。ログファイルの結果は、Milestoneナレッジベースで解決策を見つける役に立つ可能性があります。それができない場合は、Milestoneパートナーにお問い合わせのうえ、該当するインストールログファイルを提供してください。

設定

初期構成タスクリスト

以下のチェックリストは、システムを構成するための初期タスクを示しています。インストール中にすでに完了している場合もあります。

チェックリストが完了しても、それだけでシステムが完全に組織の要件に一致することを保証しているわけではありません。システムを組織の必要性に一致させるために、Milestoneは、システムの起動後も、システムを継続的にモニターし、調整することをお勧めします。

たとえば、システムを起動した後、異なる物理的条件(昼/夜、強風/穏やかな天候など)で個々のカメラのモーション検知感度の設定をテストして調整することをお勧めします。

ルールの設定は、システムが実行するアクション(ビデオを録画する場合など)の大半を決定するものであり、組織のニーズに合わせて変更できる設定のもう一つの例です。

手順:	説明
☑	システムの初期インストールが完了しました。 137ページの新しいXProtectシステムのインストールを参照してください。
☑	試用版SLCを恒久版SLCに変更します(必要な場合)。 115ページのソフトウェアライセンスコードの変更を参照してください。
☑	Management Clientへログインします。 29ページのログイン(説明付き)を参照してください。
☐	それぞれのレコーディングサーバーのストレージの設定が要件を満たしていることを確認します。 53ページのストレージとアーカイブ(説明)を参照してください。
☐	それぞれのレコーディングサーバーのアーカイブ設定が要件を満たしていることを確認します。 394ページのストレージおよび録画設定プロパティを参照してください。
☐	それぞれのレコーディングサーバーに追加する必要があるハードウェア(例、カメラおよびビデオエンコーダー)を検出します。 203ページのハードウェアの追加を参照してください。
☐	レコーディングサーバーごとに各カメラを設定する。 410ページのカメラ(デバイスノード)を参照してください。

手順:	説明
☐	個別のカメラまたはカメラのグループのストレージとアーカイブを有効にします。この操作は、カメラごと、またはデバイスグループに対して行えます。 188ページの個別のデバイスまたはデバイスのグループをストレージに接続するを参照してください。
☐	デバイスを有効にして設定します。 409ページのデバイス(デバイスノード)を参照してください。
☐	ルールはシステムの動作を大きく決定します。カメラが録画するとき、パン/チルト/ズーム(PTZ)カメラがパトロールするとき、通知が送信されるときなどのルールを作成します。 ルールを作成する。 73ページのルールとイベント(説明付き)を参照してください。
☐	役割をシステムに追加します。 64ページの役割と役割の権限(説明付き)を参照してください。
☐	ユーザーまたはユーザーのグループを各役割に追加します。 272ページのユーザーおよびグループの役割からの削除、役割への割り当てを参照してください。
☐	ライセンスをアクティベートする。 「113ページのライセンスをオンラインでアクティベーション」または114ページのライセンスをオフラインでアクティベート「」を参照してください。

[サイトナビゲーション]ペインでシステムを構成する方法については、「363ページのサイトナビゲーションペイン」を参照してください。

レコーディングサーバー

レコーディングサーバーの基本的な設定を変更または確認する

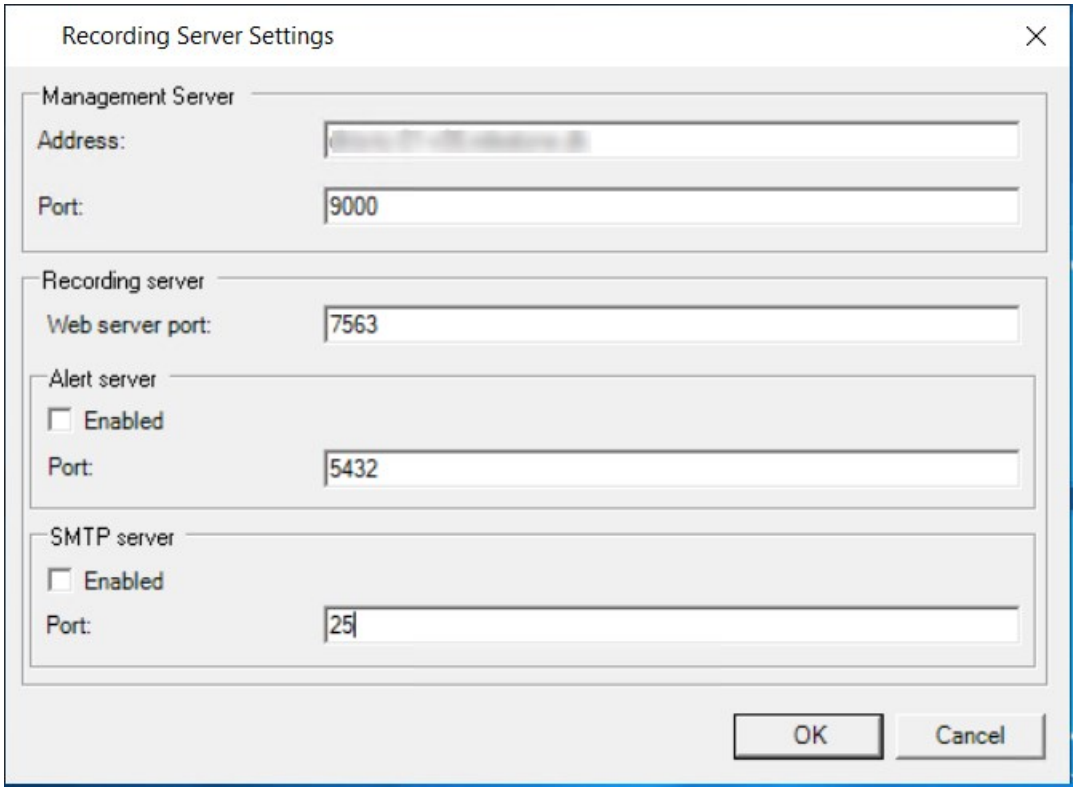
Management Clientで、インストールしたすべてのレコーディングサーバーが表示されない場合、通常は、インストール中に設定パラメータを正しく設定しなかったことが原因です(マネジメントサーバーのIPアドレスやホスト名など)。

マネジメントサーバーのパラメータを指定するには、レコーディングサーバーを再インストールする必要はありません。次の方法で基本設定を変更/確認できます。

1. レコーディングサーバーを実行しているコンピュータで、通知エリアにある**レコーディングサーバー**アイコンを右クリックします。
2. **Recording Serverサービスの停止**を選択。

3. **レコーディングサーバー**アイコンを再び右クリックし、**設定の変更**を選択します。

   レコーディングサーバーの設定ウィンドウが表示されます。



4. たとえば、以下の設定を確認するか変更します:

   - **マネジメントサーバー:アドレス**: レコーディング サーバーを接続する必要のあるマネジメントサーバーのIPアドレスまたはホスト名を指定します。
   - **マネジメントサーバー:ポート**: マネジメントサーバーと通信する際に使用するポート番号を指定します。これは必要に応じて変更できますが、ポート番号は常にマネジメントサーバーで設定されているポート番号に一致しなくてはなりません。90ページのこのシステムで使用するポートを参照してください。
   - **レコーディング サーバー:Webサーバー ポート**: レコーディング サーバーのWebサーバーと通信する際に使用するポート番号を指定します。90ページのこのシステムで使用するポートを参照してください。
   - **レコーディング サーバー:アラートサーバーポート**: レコーディング サーバーのアラート サーバーと通信する際に使用するポート番号を有効にして指定します。ここでデバイスからのイベント メッセージを受領します。90ページのこのシステムで使用するポートを参照してください。
   - **SMTPサーバー:ポート**: レコーディング サーバーのSMTPサービスと通信する際に使用されるポート番号を有効にして指定します。90ページのこのシステムで使用するポートを参照してください。

5. **OK**をクリックします。

6. Recording Serverサービスを再開するには、**[レコーディングサーバー]**アイコンを右クリックして**[Recording Serverサービスの開始]**を選択します。

Recording Serverサービスを停止すると、レコーディングサーバーの基本設定を確認/変更している間は、ビデオ録画やビデオのライブ再生ができません。

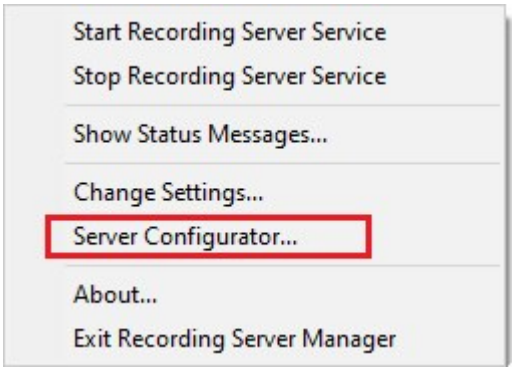
レコーディングサーバーを登録する

レコーディングサーバーをインストールすると、大抵の場合、自動的に登録されます。ただし、次のような場合は手動で登録する必要があります。

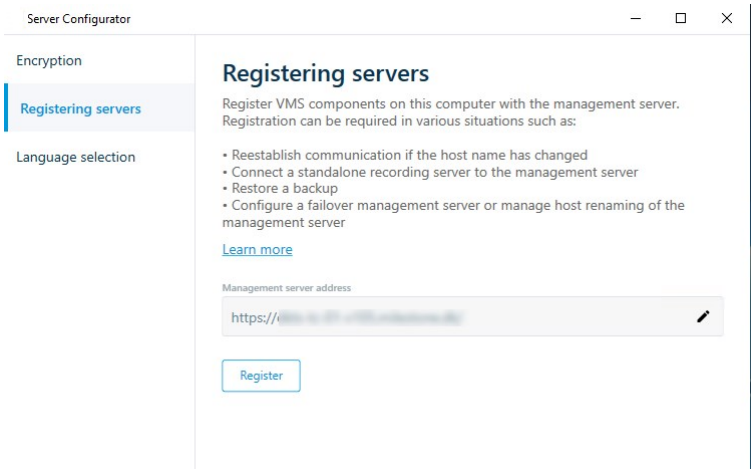
- レコーディングサーバーを交換した。
- レコーディングサーバーがオフラインでインストールされており、その後でマネジメントサーバーに追加された。
- マネジメントサーバーがデフォルトのポートを使用していない。ポート番号は暗号化の設定によって異なります。詳細については、「90ページのこのシステムで使用するポート」を参照してください。
- 自動登録が、マネジメントサーバーのアドレスを変更した後や、レコーディングサーバーのあるコンピュータの名前を変更した後、またはサーバーの通信暗号化設定を有効または無効にした後などで失敗した。マネジメントサーバーのアドレス変更の詳細については、マネジメントサーバーコンピュータのホスト名を変更を参照してください。

レコーディングサーバーを登録する際に、マネジメントサーバーに接続するように設定できます。Authorization Serverサービスは、マネジメントサーバーの一部として、登録を処理する役割を担います。

1. WindowsのスタートメニューまたはレコーディングサーバーのトレイアイコンのいずれかからServerConfiguratorを開きます。



2. Server Configuratorで**サーバーの登録**を選択します。



3. マネジメントサーバーのアドレスと、コンピュータ上のサーバーを接続するスキーム(httpまたはhttps) を確認し、**登録**をクリックします。

マネジメントサーバーの登録が成功したことを示す確認メッセージが表示されます。

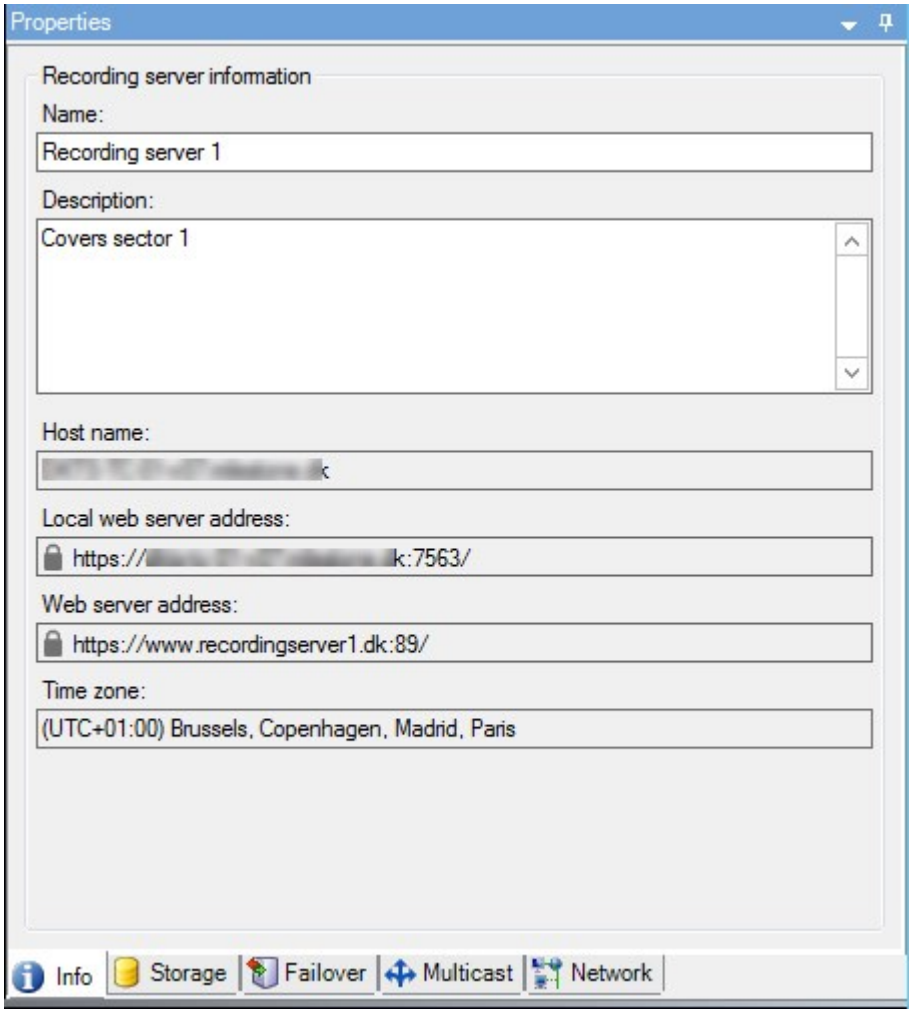
「322ページのレコーディングサーバーの交換」も参照してください。

クライアントの暗号化ステータスを表示する

レコーディングサーバーが接続を暗号化しているかを確認するには、以下を実行します。

1. Management Clientを開きます。
2. **サイトナビゲーション**ペインで、**サーバー> レコーディングサーバー**を選択します。レコーディングサーバーのリストが表示されます。

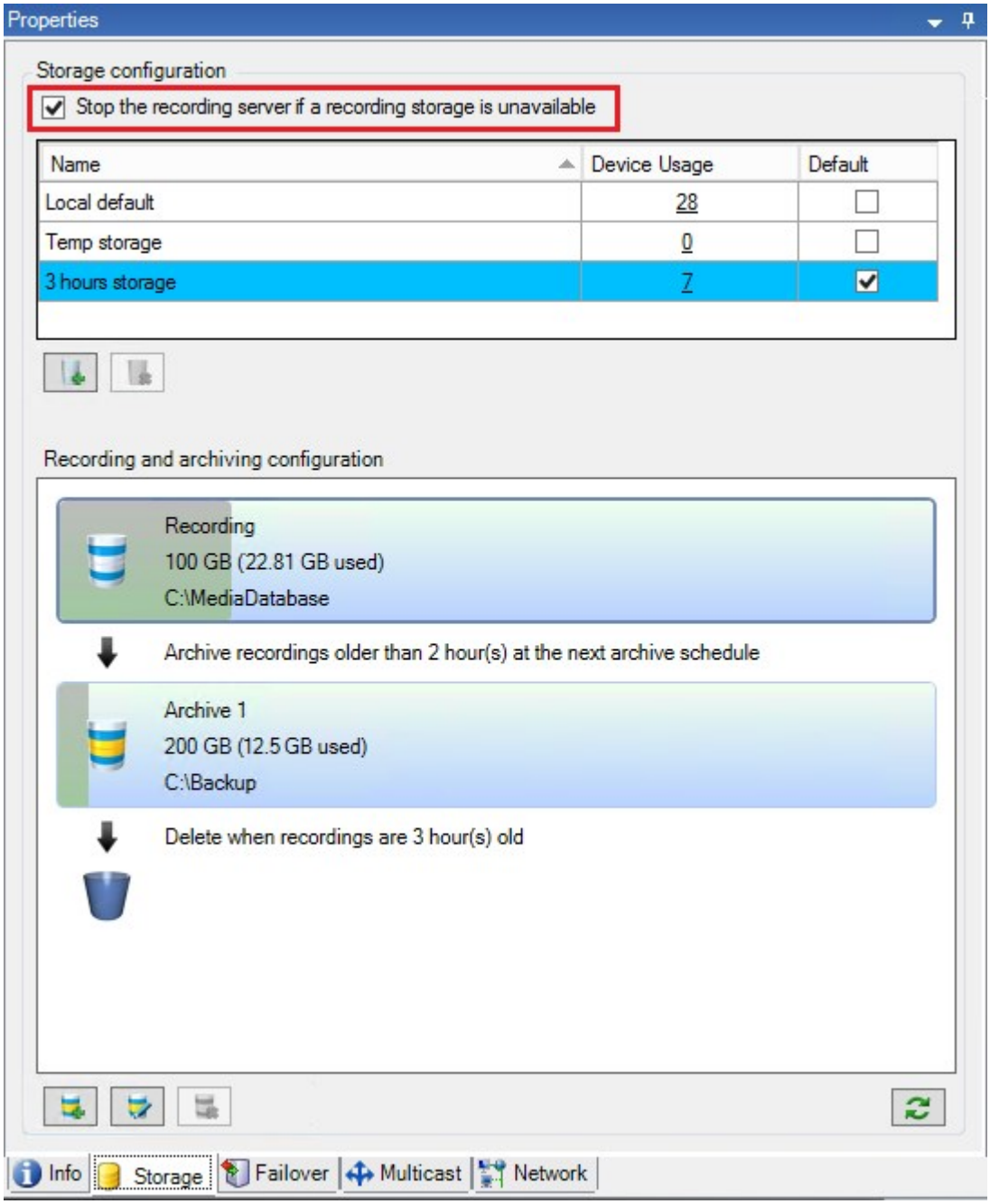
3. **概要**パネルで関連するレコーディングサーバーを選択し**情報**タブに移動します。
   レコーディングサーバーからデータストリームを受け取るクライアントとサーバーで暗号化が有効になっている場合は、ローカルのウェブサーバーアドレスとオプションのウェブサーバーアドレスの前に南京錠アイコンが表示されます。



録画ストレージが利用できない場合の動作を指定

デフォルトでは、レコーディングサーバーは録画ストレージが利用不可となっても稼働し続けます。システムがフェールオーバーレコーディングサーバーで構成されている場合は、レコーディングサーバーの実行を停止し、フェールオーバーサーバーに引き継がせるよう設定できます。

1. 該当するレコーディングサーバーの**ストレージ**タブに移動します。
2. **録画ストレージが利用可能でない場合はレコーディングサーバーを停止**オプションを選択します。



新しいストレージの追加

新しいストレージを追加したときには、**Recording**という名前の定義済み記録データベースの録画ストレージを、常に1つ作成します。データベースの名前を変更することはできません。録画ストレージとは別に、ストレージには多数のアーカイブを保存できます。

1. 選択したレコーディングサーバーにさらにストレージを追加する場合は、  ストレージ設定**リストの下にある**ボタンをクリックします。これにより**ストレージおよび録画設定**ダイアログボックスが開きます。
2. 適切に設定を行います(「394ページのストレージおよび録画設定プロパティ」を参照)。
3. **OK**をクリックします。

これで、必要に応じて新しいストレージ内でアーカイブを作成する準備が整います。

ストレージでのアーカイブの作成

ストレージにはデフォルトのアーカイブはありませんが、作成できます。

1. アーカイブを作成するには、**レコーディングおよびアーカイブの設定**リストで必要なストレージを選択します。
2.  レコーディングおよびアーカイブの設定**リストの下にある**ボタンをクリックします。
3. **[アーカイブ設定]**ダイアログボックスで、必要な設定を行います(「396ページのアーカイブ設定のプロパティ」を参照)。
4. **OK**をクリックします。

個別のデバイスまたはデバイスのグループをストレージに接続する

レコーディングサーバーに対してストレージを設定した後で、個別のデバイス(カメラ、マイク、スピーカー)またはデバイスのグループに対して有効にすることができます。また、個別のデバイスまたはグループに対して、どのレコーディングサーバーのストレージエリアを使用するかを選択することも可能です。

1. **デバイス**を展開し、必要に応じて**カメラ**、**マイク**または**スピーカー**のいずれかを選択します。
2. デバイスまたはデバイスグループを選択します。
3. **記録**タブを選択します。
4. **ストレージ**エリアで、**選択**を選択します。
5. 表示されるダイアログボックスで、デバイスの記録を保存するデータベースを選択し、**OK**をクリックします。
6. ツールバーで**保存**をクリックします。

レコーディングサーバーのストレージタブで、ストレージエリアのデバイス使用数をクリックすると、表示されるメッセージレポートでデバイスを確認できます。

無効なデバイス

無効化されたデバイスは、デフォルトでは**概要**ペインに表示されません。

無効になったデバイスをすべて表示するには、**概要**ペインの上部にある**フィルター**をクリックして**フィルター**タブを開き、**無効なデバイスを表示する**を選択します。

無効なデバイスを再び非表示にするには、**無効なデバイスを表示**をオフにします。

選択したストレージまたはアーカイブ設定の編集

1. **レコーディングおよびアーカイブの設定**リストで、ストレージを編集するには、記録データベースを選択します。アーカイブを編集するには、アーカイブデータベースを選択します。
2. **レコーディングおよびアーカイブの設定**リストの下にある  レコーディングストレージの編集**ボタン**をクリックします。
3. 記録データベースの編集またはアーカイブの編集を行います。

データベースの最大サイズを変更する場合、新しい上限を超える記録は自動アーカイブされます。記録は次のアーカイブに自動アーカイブされるか、アーカイブ設定によっては削除されます。

エクスポートのデジタル署名を有効にします。

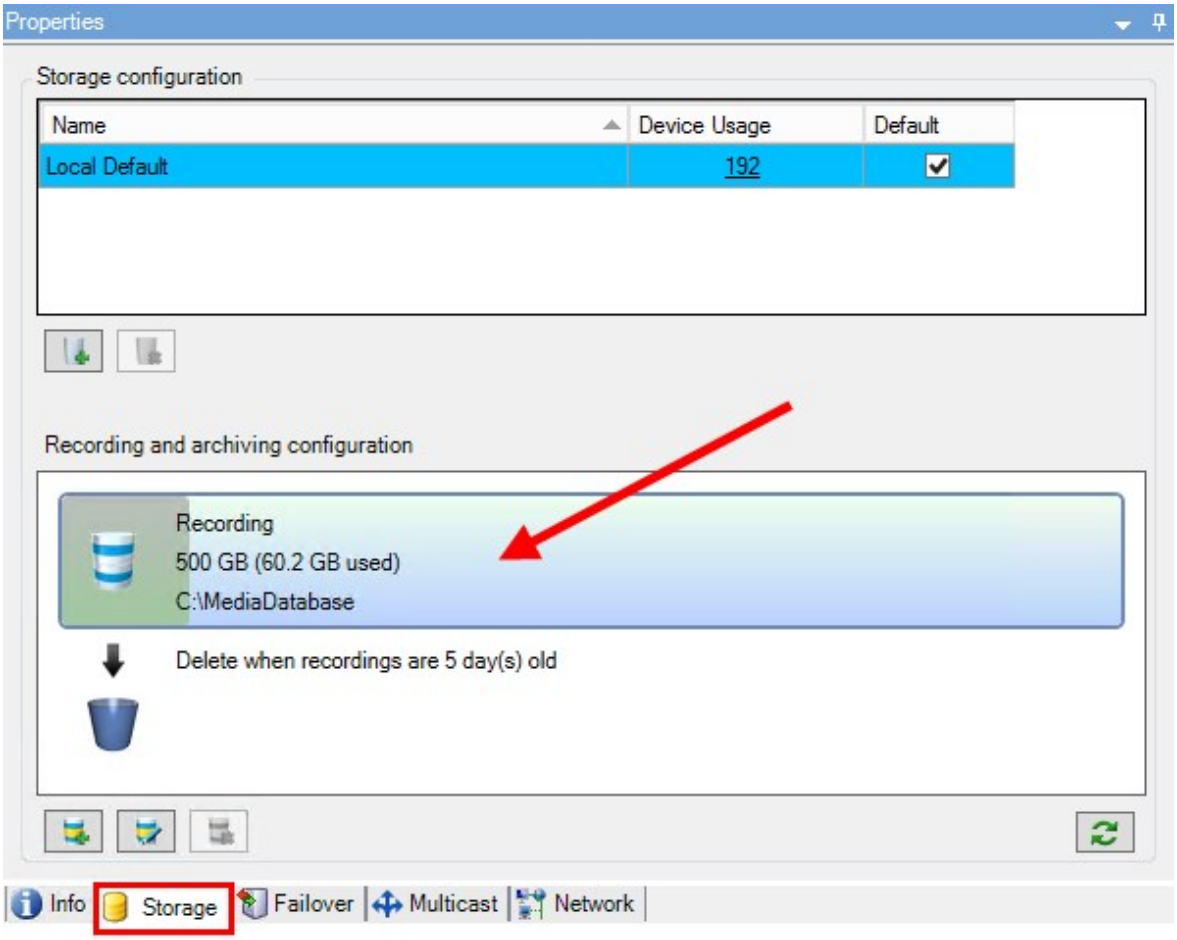
使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

録画ビデオのデジタル署名を有効にすれば、クライアントユーザーは録画ビデオが録画されてから改ざんされていないか検証できます。ビデオの信ぴょう性の検証は、ビデオがエクスポートされた後ユーザーがXProtect Smart Client - Playerで行います。

署名はXProtect Smart Client > **[エクスポート]**タブ > **[エクスポート設定]** > **[XProtect形式]** > **[デジタル署名を含める]**でも有効に設定できます。これを行わなければ、XProtect Smart Client - Playerの**[署名の検証]**ボタンは表示されません。

1. **サイトナビゲーション**ペインで、**サーバー**ノードを展開します。
2. **レコーディングサーバー**をクリックします。
3. 概要ペインで、署名を有効にしたいレコーディングサーバーをクリックします。

4. **[プロパティ]** ペインの下部にある **[ストレージ]** タブをクリックします。



5. **録画およびアーカイブ設定** セクションで、録画データベースを表す水平バーをダブルクリックします。**ストレージとレコーディングの設定** ウインドウが現れます。
6. **署名** チェックボックスを選択します。
7. **OK**をクリックします。

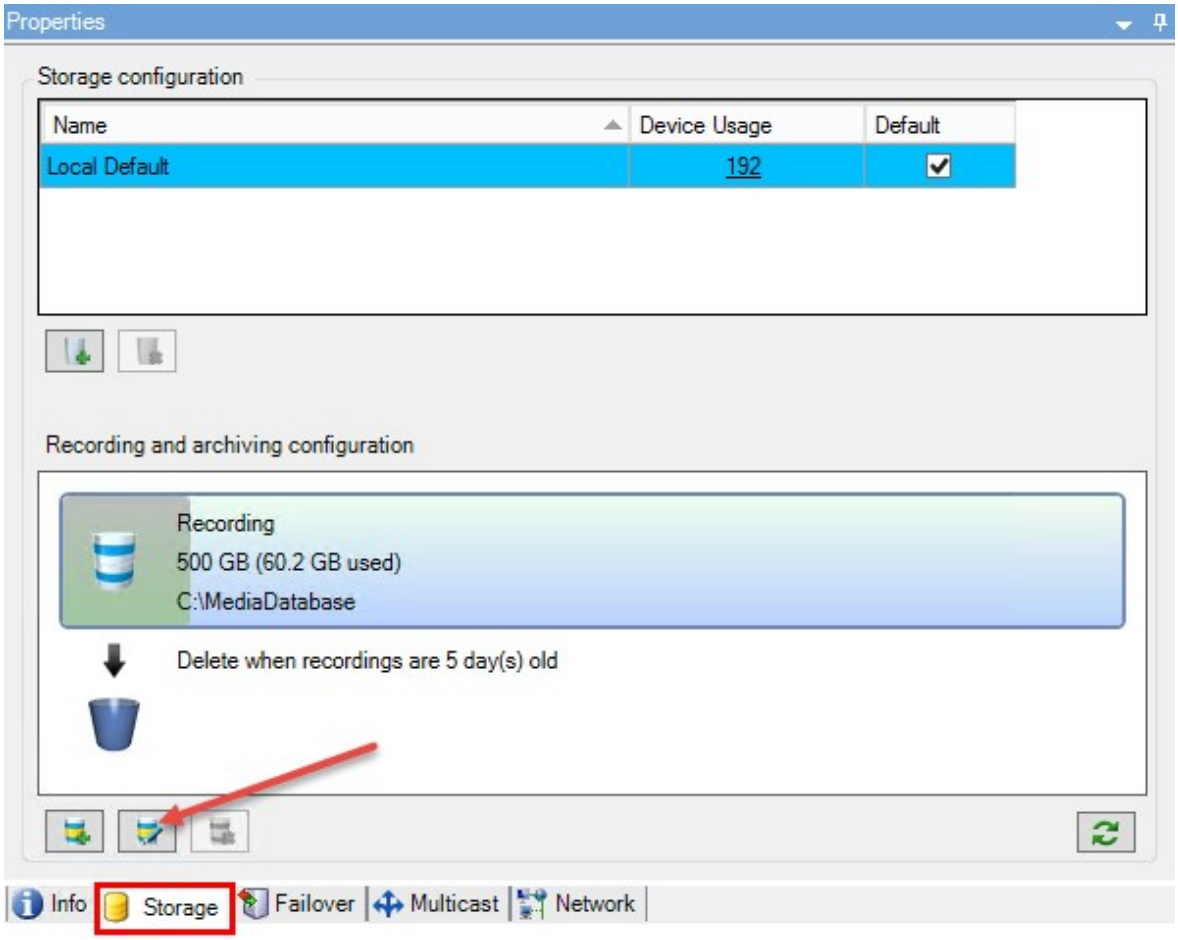
録画を暗号化する

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

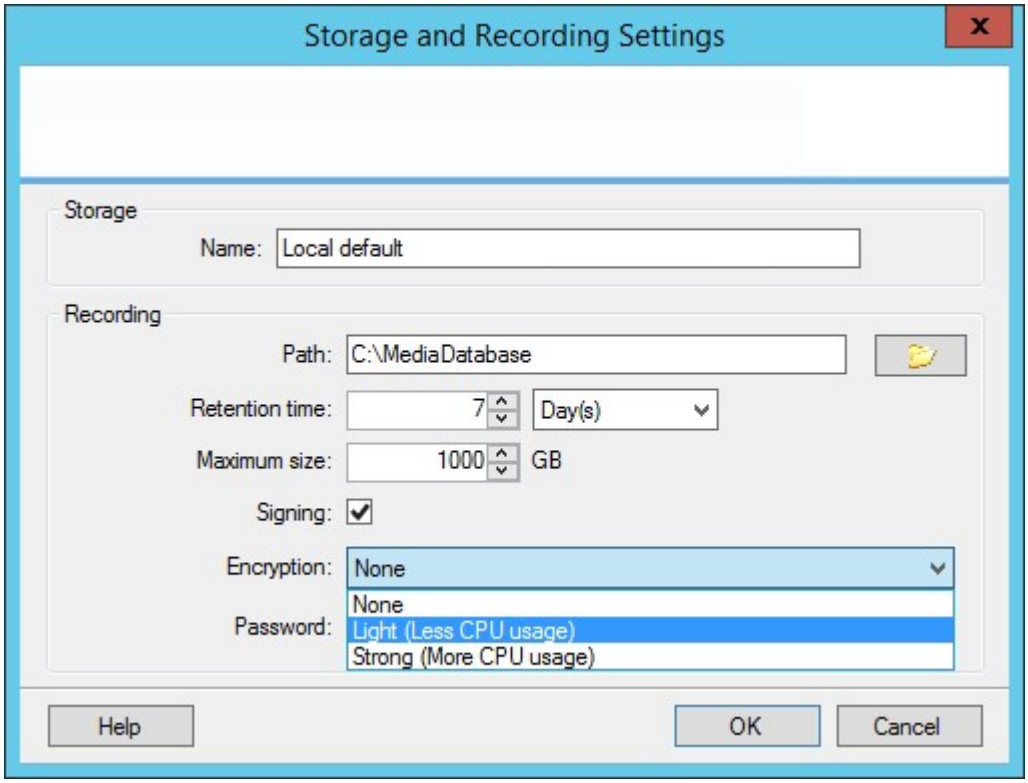
レコーディングサーバーのストレージおよびアーカイブで暗号化を有効にすることで、録画を保護することができます。簡易的な暗号化と、強化された暗号化から選ぶことができます。暗号化を有効にした場合、関連するパスワードも指定しなければなりません。

データベースのサイズとドライブのパフォーマンスによっては、暗号化設定あるいはパスワードを有効にする、あるいは変更する作業には時間がかかる場合があります。**現在のタスク**で、進捗状況を確認できます。タスクの実行中は、レコーディングサーバーを**停止させないでください**。

1. **レコーディングストレージおよびアーカイブの設定**リストの下にある**録画ストレージを編集**ボタンをクリックします。



2. 表示されたダイアログボックスで、暗号化レベルを指定します。



3. **パスワードの設定**ダイアログボックスに、自動的に遷移されます。パスワードを入力し、**OK**をクリックします。

アーカイブされた録画をバックアップする

多くの組織が、テープドライブや同等のものを使用した録画のバックアップを希望します。これをどのように行うかは、組織で使用しているバックアップメディアにより異なります。ただし、以下の点を覚えておく必要があります。

カメラのデータベースではなくアーカイブをバックアップする

個別のカメラのデータベースではなく、必ずアーカイブの内容に基づいてバックアップを作成します。個別のカメラのデータベースに基づいてバックアップを作成すると、共有違反やその他の誤動作の原因となることがあります。

バックアップをスケジュールする際は、バックアップジョブのアーカイブ時間が決して重複しないように注意してください。各レコーディングサーバーのストレージエリア内の各レコーディングサーバーのアーカイブスケジュールを表示するには、**ストレージ**タブを参照してください。

バックアップ中にアーカイブが行われないようにするため、アーカイブをアンマウントしてバックアップを実行し、アーカイブを再度マウントすることができます。アーカイブのマウントとアンマウントは、MilestoneIntegrationPlatformVMSAPIを通じて実行されます。

アーカイブの構造を知ることでバックアップを効率化する

録画をアーカイブすると、アーカイブ内の特定のサブディレクトリ構造に保存されます。

全システムの標準的な使用中に、XProtect Smart Clientを使ってすべての録画を参照しているシステムユーザーにとって、サブディレクトリ構造はまったく認識されません。これは、アーカイブ済み録画と未アーカイブ録画の両方に当てはまります。アーカイブ済みの録画をバックアップ(313ページのシステム設定のバックアップおよび復元を参照)したい場合、サブディレクトリ構造(57ページのアーカイブ構造(説明付き)を参照)について把握しておくことが重要です。

ストレージでのアーカイブの削除

1. **レコーディングおよびアーカイブの設定**リストで、アーカイブを選択します。

   リストで最後にあるアーカイブのみが削除できます。アーカイブを空にする必要はありません。

2.  レコーディングおよびアーカイブの設定**リストの下にある**ボタンをクリックします。

3. **はい**をクリックします。

   利用できないアーカイブ、たとえばオフラインアーカイブの場合、アーカイブにエビデンスロックのあるメディアが含まれているかどうかを確認することはできませんが、ユーザーが確認した後にアーカイブを削除することは可能です。

   エビデンスロックされたメディアを含む利用可能なアーカイブ(オンラインアーカイブ)は、削除できません。

ストレージの削除

ライブレコーディングの録画ストレージとして使用するデフォルトのデバイスを削除することはできません。
そのためストレージを削除するには、デバイスに加え、未アーカイブの録画を他のストレージに移動(「323ページのハードウェアの移動を参照」)しなくてはならない場合があります。

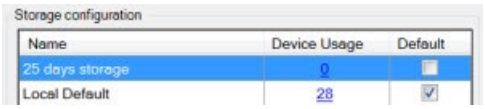
1. このストレージを使用するデバイスを一覧表示するには、デバイス使用数をクリックします。

   別のレコーディングサーバーに移動されたデバイスのデータがストレージにある場合は、警告が表示されます。リンクをクリックすると、デバイスの一覧が表示されます。

2. 「195ページのアーカイブされていない録画を別のストレージへ移動する」の手順を実行します。

3. すべてのデバイスを移動し終わるまで続行します。

4. 削除するストレージを選択します。



5.  ストレージ設定 **リストの下にある**ボタンをクリックします。

6. **はい**をクリックします。

アーカイブされていない録画を別のストレージへ移動する

ある録画データベースから別の録画データベースへのコンテンツの移動は、デバイスの**記録**タブで行います。

1. デバイスタイプを選択します。**概要**ペインで、デバイスを選択します。
2. **録画**タブをクリックします。**ストレージ**エリアの上部で、**選択**をクリックします。
3. **ストレージの選択**ダイアログボックスで、データベースを選択します。
4. **OK**をクリックします。
5. **録画アクション**ダイアログボックスで、既存の**アーカイブされていない**録画を新しいストレージに移動するか、削除するかを選択します。
6. **OK**をクリックします。

フェールオーバーレコーディングサーバーの割り当て

レコーディングサーバーの**フェールオーバー**タブでは、3種類のフェールオーバー設定の中から選択できます。

- フェールオーバー設定なし
- プライマリ/セカンダリフェールオーバー設定
- ホットスタンバイ設定

bおよび**c**を選択する場合、特定のサーバーまたはグループを選択する必要があります。**b**では、セカンダリフェールオーバーグループも選択できます。レコーディングサーバーが使用できなくなった場合、プライマリフェールオーバーグループのフェールオーバーレコーディングサーバーに切り替わります。セカンダリフェールオーバーグループも選択している場合、プライマリフェールオーバーグループのフェールオーバーレコーディングサーバーがすべてビジーである場合には、セカンダリグループのフェールオーバーレコーディングサーバーに切り替わります。このようにして、フェールオーバーソリューションが機能しないリスクは、プライマリのすべてのフェールオーバーレコーディングサーバーだけなくセカンダリフェールオーバーグループもビジーである場合だけになります。

1. **[サイトナビゲーション]**ペインで、**[サーバー]>[レコーディングサーバー]**を選択します。レコーディングサーバーのリストが表示されます。
2. **概要**ペインで、必要なレコーディングサーバーを選択し、**フェールオーバー**タブに移動します。

3. フェールオーバーセットアップのタイプを選択するには、以下から選びます:
   - **無し**
   - **プライマリフェールオーバーサーバーグループ / セカンダリフェールオーバーサーバーグループ**
   - **ホットスタンバイサーバー**

   同じフェールオーバーグループをプライマリとセカンダリフェールオーバーグループとして選択したり、すでにフェールオーバーグループに含まれている標準のフェールオーバーサーバーをホットスタンバイサーバーとして選択することはできません。
4. 次に、**詳細フェールオーバー設定**をクリックします。これで、**フェールオーバー詳細設定**ウィンドウが開き、選択したレコーディングサーバーに接続するすべてのデバイスのリストが表示されます。**無し**を選択した場合でも、フェールオーバー詳細設定を使用できます。選択アイテムはすべて保存され、後からフェールオーバー設定で使用できます。
5. フェールオーバーサポートのレベルを指定するには、リストの各デバイスで**フルサポート**、**ライブ専用**、**無効**のいずれかを選択します。**OK**をクリックします。
6. 必要に応じて、**フェールオーバーサービス通信ポート(TCP)**フィールドでポート番号を編集します。

もしフェールオーバーサポートを有効化し、レコーディングストレージが利用可能でない場合はレコーディングサーバーが実行され続けるように設定した場合、フェールオーバーレコーディングサーバーはテイクオーバーしません。フェールオーバーサポートワークをするには、**レコーディングストレージが利用可能でない場合は**レコーディングサーバーを止めるオプションを、**ストレージ**タブで選択します。

レコーディングサーバーのマルチキャストを有効にする

通常のネットワーク通信で、各データパケットは単一の送信者から単一の受信者に送信され、ユニキャストと呼ばれます。一方、マルチキャストでは、単一のデータパケット(サーバーから)をグループ内の複数の受信者(クライアント)に送信できます。したがって、マルチキャストは帯域幅を節約できます。

- **ユニキャスト**を使用する場合、発信元は必ずそれぞれの受信者に1つのデータストリームを転送しなければなりません。
- **マルチキャスト**を使用する場合は、それぞれのネットワークセグメントで単一のデータストリームしか必要ではありません。

ここで説明しているマルチキャストは、カメラからサーバーへのビデオのストリーミングでは**ありません**。サーバーからクライアントへのストリーミングになります。

マルチキャストでは、IPアドレス範囲、各カメラにマルチキャストを有効化/無効化できる能力、最大許容データパケットサイズ(MTU)を定義する機能、データパケットを転送するための最大ルーター数(TTL)などのオプションを基に定義された受信者のグループを使用します。

レコーディングサーバーが暗号を使用している時でも、マルチキャストストリームは暗号化されません。

マルチキャストを、関連のないデータでもネットワークに接続している全員にデータを送信する、**ブロードキャスト**と混合しないよう注意する必要があります。

名前	説明
ユニキャスト	単一のソースから単一の受信者へデータを送信します。
マルチキャスト	単一のソースから明確に定義されたグループ内の複数の受信者へデータを送信します。
ブロードキャスト	単一のソースからネットワーク上の全員へデータを送信します。このため、ブロードキャストによって、ネットワーク通信速度が大幅に低下する可能性があります。

マルチキャストを使用するには、ネットワークのインフラがIPマルチキャスト標準IGMP(インターネットグループ管理プロトコル) をサポートしている必要があります。

- **[マルチキャスト]**タブで、**[マルチキャスト]**チェックボックスを選択します。

マルチキャスト用のIPアドレス範囲の全体が既に1つまたは複数のレコーディングサーバーによって使用されている場合は、まずマルチキャスト用のIPアドレスを空けないと、それ以上のレコーディングサーバーでマルチキャストを有効にすることはできません。

レコーディングサーバーが暗号を使用している時でも、マルチキャストストリームは暗号化されません。

個々のカメラに対してマルチキャストを有効にする

関連するカメラでこれを有効にした場合にのみ、マルチキャストは動作します。

1. レコーディングサーバーを選択して、**概要**ペインで必要なカメラを選択します。
2. **クライアント**タブで、**ライブマルチキャスト**チェックボックスを選択します。関連するすべてのカメラに対して繰り返します。

レコーディングサーバーが暗号を使用している時でも、マルチキャストストリームは暗号化されません。

パブリックアドレスとポートの定義

パブリックネットワークまたは信頼できないネットワークでXProtect Smart Clientを使用してVMSにアクセスする必要がある場合、MilestoneはVPN経由で安全な接続を使用することを推奨しています。これはXProtect Smart ClientとVMSサーバー間の通信を確実に保護することに役立ちます。

レコーディングサーバーのパブリックIPアドレスは**ネットワーク**タブで定義します。

パブリックアドレスを使用する理由

クライアントはローカルネットワークに加えてインターネットから接続することもあります。いずれの場合にも、レコーディングサーバーからのライブビデオや録画ビデオにクライアントがアクセスできるように、監視システムが適切なアドレスを提供する必要があります。

- クライアントがローカルで接続する場合、監視システムはローカルのアドレスおよびポート番号を返します。
- クライアントがインターネットから接続する場合、監視システムはレコーディングサーバーのパブリックアドレスを返します。これはファイアウォールまたはNAT(ネットワークアドレス変換)ルーターのアドレスであり、多くの場合、異なるポート番号です。アドレスおよびポートは、サーバーのローカルアドレスおよびポートに転送できます。

1. パブリックアクセスを有効にするには、**パブリックアクセスを有効にする**チェックボックスを選択します。
2. レコーディングサーバーのパブリックアドレスを定義します。ファイアウォールまたはNATルーターのアドレスを入力し、インターネットから監視システムにアクセスするクライアントがレコーディングサーバーに接続できるようにします。
3. パブリックポート番号を指定します。ファイアウォールまたはNATルーターで使用するポート番号を、ローカルで使用するポート番号と異なる番号にしておくことをお勧めします。

> パブリックアクセスを使用する場合、使用するファイアウォールまたはNATルーターを設定し、パブリックなアドレスおよびポートに送信されるリクエストが、関連するレコーディングサーバーのローカルなアドレスおよびポートに転送されるようにしてください。

ローカルIP範囲の割り当て

監視システムがローカルネットワークからの通信であると認識できるローカルIP範囲のリストを定義します。

- **[ネットワーク]**タブで、**[設定]**をクリックします。

デバイスツリーのフィルター

多くのデバイスを登録している場合、**概要**ペインのデバイスツリーが非常に大きくなることがあります。デバイスツリーをフィルターすることで、操作したいデバイスを簡単に見つけることができます。

いくつかの特定のデバイスに固有のフィルター条件を用いることで、効果的にその特定のデバイスのみを表示することができます。

デバイスツリーのフィルター

- **概要**ペインの上部にある**フィルター**をクリックして、**フィルター**タブを開きます。
- **デバイスの絞り込み**フィールドで1つまたは複数のフィルター条件を入力し、**フィルターの適用**をクリックしてデバイスリストをフィルターします。

フィルター条件の特徴

フィルター条件は、デバイス名、デバイス略称、ハードウェアアドレス(IP)、デバイスID、およびハードウェアIDのフィールド値に適用されます。

ハードウェアIDおよびデバイスIDのフィールド値をフィルターする場合、フィルターの部分一致は表示されません。そのため、ハードウェアIDやデバイスIDでフィルターする場合は、完全かつ正確な識別番号を定義する必要があります。

デバイス名、デバイスの略称、ハードウェアアドレスの各フィールド値に対して部分一致のフィルターが表示されます。そのため、例えば「カメラ」という語句でフィルターした場合、デバイス名に「カメラ」という単語を含むすべてのデバイスを表示することになります。

フィルター条件は大文字と小文字を区別しないため、「camera」または「Camera」をフィルター条件として使用した場合は同じ結果になります。

複数のフィルター条件の指定

複数の条件を指定することで、デバイスツリーのフィルター結果をさらに絞り込むことができます。フィルターが適用されると、定義されたすべてのフィルター条件はANDで結合されたものとみなされ、累積されます。

例えば、2つのフィルター条件を入力した場合は、次のようになります。「カメラ」と「倉庫」と入力すると、デバイス名に「カメラ」と「倉庫」を含むデバイスがすべて表示されますが、デバイス名に「カメラ」と「駐車場」を含むデバイスや、デバイス名に「カメラ」しか含まないデバイスは表示されません。

フィルターフィールドから個々のフィルター条件を削除して、制限の多いフィルターを指定した場合、フィルターの幅を広げることができます。フィルター条件を削除すると、デバイスツリーに自動的にフィルターが適用されます。

フィルターのリセット

フィルターフィールドからすべてのフィルター条件を削除すると、**概要**ペインはリセットされ、再びすべてのデバイスが表示されます。

また、**F5**を押すとフィルターがリセットされ、**無効なデバイスを表示する**チェックボックスがクリアになります。

無効なデバイス

無効化されたデバイスは、デフォルトでは**概要**ペインに表示されません。

無効になったデバイスをすべて表示するには、**概要**ペインの上部にある**フィルター**をクリックして**フィルター**タブを開き、**無効なデバイスを表示する**を選択します。

無効なデバイスを再び非表示にするには、**無効なデバイスを表示**をオフにします。

フェールオーバーサーバー

フェールオーバーレコーディングサーバーの設定と有効化

フェールオーバーレコーディングサーバーを無効にしている場合、標準のレコーディングサーバーから切り替える前に有効にする必要があります。

次の手順を実行し、フェールオーバーレコーディングサーバーを有効にして、基本プロパティを編集します。

1. **サイトナビゲーション**ペインで、**サーバー>フェールオーバーサーバー**を選択します。インストール済みのフェールオーバーレコーディングサーバーとフェールオーバーグループのリストが表示されます。
2. **概要**ペインで、必要なフェールオーバーレコーディングサーバーを選択します。
3. 右クリックして、**有効**を選択します。フェールオーバーレコーディングサーバーが有効になりました。
4. フェールオーバーレコーディングサーバーのプロパティを編集するには、**情報**タブに移動します。
5. 完了すると、**ネットワーク**タブに移動します。ここで、フェールオーバーレコーディングサーバーのパブリックIPアドレスなどを定義できます。これは、NAT(ネットワークアドレス変換)とポート転送を使用する場合に必要です。詳細については、標準のレコーディングサーバーの**ネットワーク**タブを参照してください。
6. **[サイトナビゲーション]**ペインで、**[サーバー]>[レコーディングサーバー]**を選択します。フェールオーバーサポートを実行したいレコーディングサーバーを選択して、フェールオーバレコーティングーサーバーを割り当てます(397ページのフェールオーバータブ(レコーディングサーバー)を参照)。

フェールオーバーレコーディングサーバーのステータスを見るには、通知エリアにあるFailover Recording Server Managerトレイアイコンの上でマウスをホールドします。フェールオーバーレコーディングサーバーの説明フィールドに、入力された説明文がヒントとして表示されます。ここで、フェールオーバーレコーディングサーバーが、どのレコーディングサーバーを引き継ぐよう設定されているかを確認することができます。

フェールオーバーレコーディングサーバーは、定期的にマネジメントサーバーに対してpingを行い、マネジメントサーバーがオンラインで、必要に応じて、標準レコーディングサーバーの構成に対して要求、応答できることを確認します。pingをブロックすると、フェールオーバーレコーディングサーバーは、標準レコーディングサーバーを代替できなくなります。

コールドスタンバイ用にフェールオーバーレコーディングサーバーをグループ化

1. **サーバー>フェールオーバーサーバー**を選択します。インストール済みのフェールオーバーレコーディングサーバーとフェールオーバーグループのリストが表示されます。
2. **概要**ペインで最上位ノードの**フェールオーバーグループ**を右クリックし、**グループの追加**を選択します。
3. 新しいグループの名前(この例では*Failover Group 1*)と説明(任意)を指定します。**OK**をクリックします。

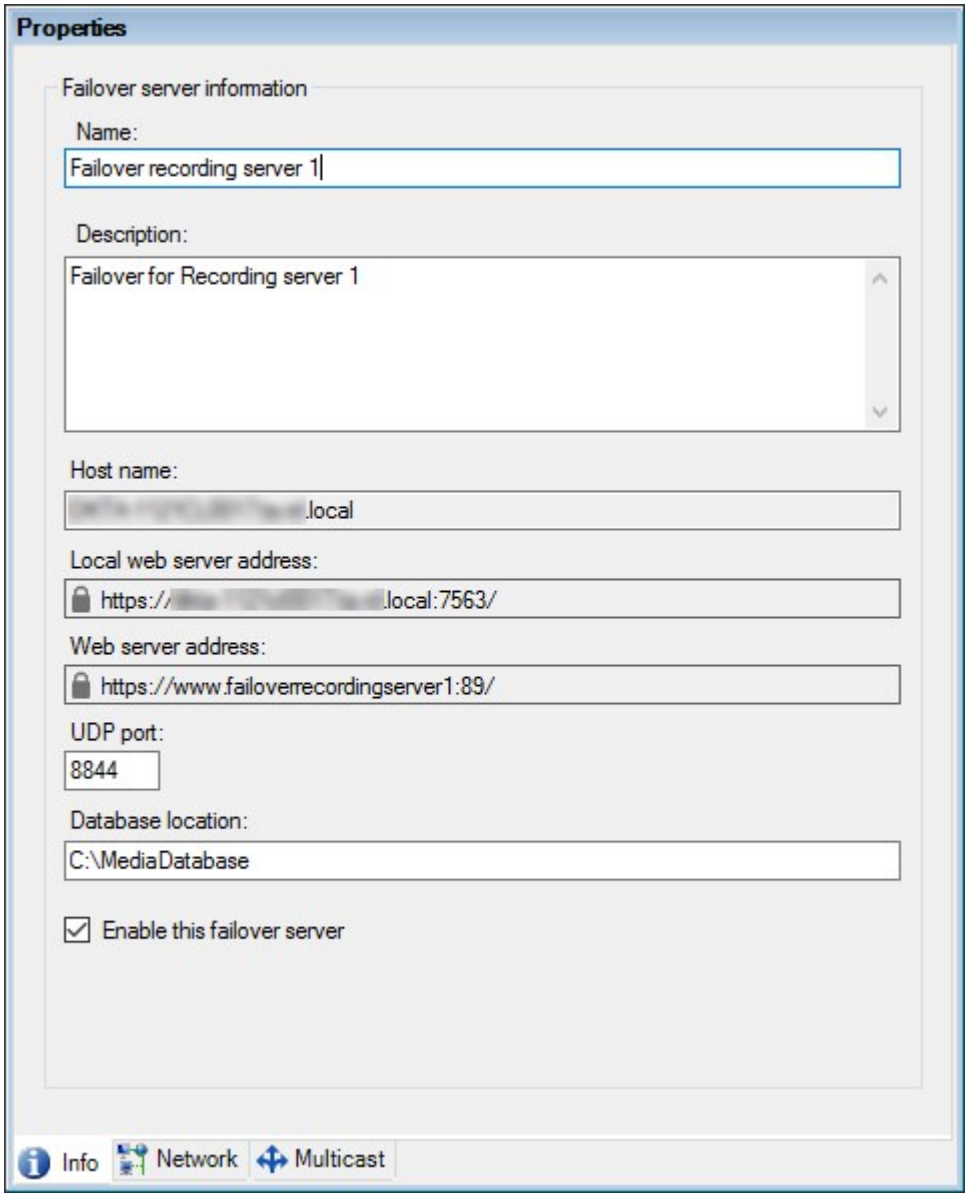
4. 作成したグループ(*Failover Group 1*) を右クリックします。**グループメンバーの編集** を選択します。これにより**グループメンバーの選択** ウィンドウが開きます。
5. ドラッグアンドドロップするか、ボタンを使用して、左側から右側へ選択したフェールオーバーレコーディングサーバーを移動します。**[OK]** をクリックします。これで、選択したフェールオーバーレコーディングサーバーが、作成したグループ (*Failover Group 1*) に含まれます。
6. **シーケンス**タブに移動します。**上** と**下** をクリックし、グループの通常フェールオーバーレコーディングサーバーの内部シーケンスを設定します。

フェールオーバーレコーディングサーバーで暗号化ステータスを表示

フェールオーバーレコーディングサーバーを暗号化する時は、以下を確認します。

1. **サイトナビゲーション**ペインで、**サーバー>フェールオーバーサーバー**を選択します。これでフェールオーバーレコーディングサーバーのリストが開きます。
2. **概要** パネルで関連するレコーディングサーバーを選択し、**情報** タブに移動します。
レコーディングサーバーからデータストリームを受け取るクライアントとサーバーで暗号化が有効になっている場合は、

ローカルのウェブサーバーアドレスとオプションのウェブサーバーアドレスの前に南京錠アイコンが表示されます。



ステータスメッセージの表示

1. フェールオーバーレコーディングサーバーで、**Milestone Failover Recording Server サービス**アイコンを右クリックします。
2. **ステータスメッセージの表示**を選択します。**フェールオーバーサーバーステータスメッセージ**ウィンドウが表示され、タイムスタンプ付きのステータスメッセージが一覧表示されます。

バージョン情報の表示

製品サポートに連絡する必要がある場合、**Failover Recording Server サービス**の正確なバージョンを知っていると便利です。

1. フェールオーバーレコーディングサーバーで、**Milestone Failover Recording Serverサービス**アイコンを右クリックします。
2. **バージョン情報**を選択します。
3. 小さいダイアログが開き、**Failover Recording Serverサービス**の正確なバージョンが表示されます。

ハードウェア

ハードウェアの追加

システム内の各レコーディングサーバーに対して、ハードウェアを追加するための方法は、複数あります。

> ハードウェアがNAT対応ルーターまたはファイアウォールの背後にある場合、別のポート番号を指定し、ルーター/ファイアウォールを構成して、ハードウェアのポートとIPアドレスにマッピングされるようにしなければならない場合があります。

ハードウェアを追加ウィザードを使用して、ネットワーク上でカメラおよびビデオエンコーダーなどのハードウェアを検知し、システムのレコーディングサーバーに追加します。ウィザードでは、Milestone Interconnect設定のリモートレコーディングサーバーも追加できます。ハードウェアは、一度に**1つのレコーディングサーバー**にのみ追加してください。

1. **ハードウェアの追加**にアクセスするには、必要なレコーディングサーバーを右クリックし、**ハードウェアの追加**を選択します。
2. ウィザードオプション(以下を参照)のいずれかを選択し、画面の手順に従います。
3. インストール後、**[概要]**ペインにハードウェアとデバイスが表示されます。

> 初めてハードウェアを追加する際は、特定のハードウェアを事前に設定する必要があります。このようなハードウェアを追加すると、**[ハードウェア デバイスの事前設定]**ウィザードが現れます。詳細については、50ページのハードウェアの事前設定 (説明付き)を参照してください。

ハードウェアの追加(ダイアログ)

ハードウェアは次のいずれかを表します。

- IP経由で監視システムのレコーディングサーバーに直接接続する物理ユニット(カメラ、ビデオエンコーダー、I/Oモジュールなど)。
- Milestone Interconnect設定のリモートサイトのレコーディングサーバー。

ハードウェアをシステムに追加する方法については、「203ページのハードウェアの追加」を参照してください。

名前	説明
高速(推奨)	レコーディングサーバーのローカルネットワークで、新しいハードウェアがシステムにより自動的にスキャンされます。 **他のレコーディングサーバーで実行中のハードウェアを表示**チェックボックスを選択すると、検出したハードウェアが他のレコーディングサーバーで実行中であるかどうかを確認できます。 新しいハードウェアをネットワークに追加し、システムで使用するたびに、このオプションを選択できます。 このオプションを使用して、Milestone Interconnectセットアップでリモートシステムを追加することはできません。 HTTPとHTTPSハードウェアを追加するには、ラジオボタン**[HTTPS(セキュア)]**を選択した状態で**高速**検出を実行し、その後、**[HTTP(セキュアでない)]**を選択した状態で検出を実行してください。
アドレス範囲スキャン	ネットワーク上の関連するハードウェアとMilestone Interconnectリモートシステムがスキャンされます。 • これは、指定されたハードウェアのユーザー名とパスワードに従って実行されます。ハードウェアで出荷時設定のデフォルトユーザー名とパスワードが使用される場合には必要ありません。 • ドライバー • IP範囲(IPv4のみ) • ポート番号(デフォルト= 80) システムを拡張する場合など、ネットワークの一部だけをスキャンするときにはこのオプションを選択できます。
手動	各ハードウェアとMilestone Interconnectリモートシステムの詳細情報を個別に指定します。追加するハードウェア数が限られており、IPアドレス、関連するユーザー名およびパスワードが分かっている場合、またはカメラが自動検出機能をサポートしていない場合には、この選択が適しています。
リモート接続ハードウェア	リモート接続されているサーバー経由で接続されているハードウェアがスキャンされます。 Axis One-clickカメラの接続など、サーバーをインストールした場合にこのオプションを使用できます。 このオプションを使用して、Milestone Interconnectセットアップでリモートシステムを追加することはできません。

ハードウェアを有効/無効にする

追加したハードウェアは、デフォルトでは**有効**になっています。

次の方法でハードウェアが有効化/無効化されたかどうかを確認できます。

有効
(無効)

(ライセンスまたはパフォーマンス上の理由で)追加したハードウェアを無効にするには

1. レコーディングサーバーを展開し、無効にするハードウェアを右クリックします。
2. **有効**を選択して、選択/解除します。

ハードウェアの編集

追加したハードウェアを右クリックし、**[ハードウェアの編集]**をクリックして、Management Client内のハードウェアのネットワーク構成とユーザー認証設定を修正します。

ハードウェアの編集(ダイアログ)

ハードウェアによっては、**[ハードウェアの編集]**ダイアログでも設定をハードウェアデバイスに直接適用できる場合もあります。

[Management Client設定の編集]ラジオボタンが選択されると、**[ハードウェアの編集]**ダイアログに、Management Clientをハードウェアに接続するために使用する設定が表示されます。ハードウェアデバイスがシステムに適切に追加されたことを確認するため、メーカーのハードウェア構成インターフェースに接続する際に使用するものと同じ設定を入力します:

名前	説明
名前	ハードウェアの名前が、検出されたそのIPアドレス(括弧内)とともに表示されます。
ハードウェアURL	メーカーのハードウェア構成インターフェースのウェブアドレスであり、通常はハードウェアのIPアドレスも記されます。ネットワークで有効なアドレスを指定します。
ユーザー名	ハードウェアへの接続に使用したユーザー名。 ここにユーザー名を入力しても、実際のハードウェアデバイスのユーザー名が変化することはありません。**[Management Clientとハードウェア設定の編集]**ラジオボタンを選択して、対応ハードウェアデバイスの設定を変更します。
パスワード	ハードウェアへの接続に使用したパスワード。 ここにパスワードを入力しても、実際のハードウェアデバイスのパスワードが変化することはありません。**[Management Clientとハードウェア設定の編集]**ラジオボタンを選択して、対応ハードウェアデバイスの設定を変更します。

名前	説明
	複数のハードウェアデバイスのパスワードを変更する方法については、「210ページのハードウェアデバイスのパスワードを変更」を参照してください。 あなたはシステム管理者として、Management Clientでパスワードを表示するための権限を他のユーザーに付与する必要があります。詳細については、ハードウェアの役割設定を参照してください。

対応ハードウェアに対して **[Management Clientとハードウェア設定の編集]** ラジオボタンが選択されている場合、同様にハードウェアデバイスに直接適用される設定が **[ハードウェアにの編集]** ダイアログに表示されます。

このラジオボタンが選択された状態で設定を適用すると、ハードウェアデバイスの現在の設定が上書きされます。設定の適用中は、ハードウェアからレコーディングサーバーへの接続が一時的失われます。

名前	説明
名前	ハードウェアの名前が、検出されたそのIPアドレス(括弧内) とともに表示されます。
ネットワーク構成	ハードウェアのネットワーク設定。ネットワーク設定を調整するには、[206ページの構成]を選択します。
構成	**[Pバージョン]** ドロップダウンリストを使用して、対応ハードウェアデバイスのインターネットプロトコルを指定します。 • IPv4の値は以下の形式でなければなりません: **(0-999).(0-999).(0-999).(0-999)** • IPv6の値は、8つの16進数の値(コロン区切り) という形式でなければなりません。サブネットマスクは**0-128**の数値でなければなりません。 **[チェック]** ボタンを押すと、入力したIPアドレスが、現在システム内の他のハードウェアデバイスによって使用されているのかテストできます。 **[チェック]** を使用しても、オフになっている/XProtect VMSシステムの外部にある/他の理由で一時的に応答していないハードウェアデバイス間の競合を検出することはできません。

名前	説明
ユーザー名	ハードウェアへの接続に使用したユーザー名とレベル。ドロップダウンリストから別のユーザーを選択し、以下で説明されている**[パスワード]**フィールドに新しいパスワードを追加します。 207ページのユーザーの追加セクション下部にある下線が付いたアクションを用いてユーザーを追加または削除します(208ページのユーザーの削除またはを参照)。 メーカーが指定した最高レベルが割り当てられていないユーザーを選択すると、一部の機能が利用できなくなる可能性があります。
パスワード	ハードウェアへの接続に使用したパスワード。**[開示]**  アイコンを使用して、現在入力中のテキストを表示します。 パスワードを変更する際には、特定のハードウェアデバイスに伴うパスワード規則について記されたメーカーのマニュアルを参照するか、**[パスワードの生成]**  アイコンを使用して要件を満たしたパスワードを自動的に生成してください。 複数のハードウェアデバイスのパスワードを変更する方法については、「210ページのハードウェアデバイスのパスワードを変更」を参照してください。 あなたはシステム管理者として、Management Clientでパスワードを表示するための権限を他のユーザーに付与する必要があります。詳細については、ハードウェアの役割設定を参照してください。
ユーザーの追加	下線の付いた**[追加]**リンクを選択して**[ユーザーの追加]**ダイアログを開き、ハードウェアデバイスにユーザーを追加します。 ユーザーを追加すると、このユーザーが自動的に現在アクティブなユーザーとして設定され、前回入力した資格情報が上書きされます。 パスワードを作成する際には、特定のハードウェアデバイスに伴うパスワード規則について記されたメーカーのマニュアルを参照するか、**パスワードを生成する**  アイコンを使用して、要件を満たしたパスワードを自動生成してください。 ハードウェアデバイスで検出された最高ユーザーレベルが自動的に事前選択されます。**ユーザーレベル**をデフォルト値から変更することは推奨されません。

名前	説明
	メーカーが指定した最高**ユーザーレベル**以外のレベルを選択すると、一部の機能が利用できなくなる可能性があります。
ユーザーの削除	下線の付いた **[削除]** リンクを選択して **[ユーザーの削除]** ダイアログを開き、ハードウェアデバイスからユーザーを削除します。 現在アクティブなユーザーを削除することはできません。新しいユーザーを設定するには、上記の **[ユーザーの追加]** ダイアログを使用してから、このインターフェースを使用して古いユーザーを削除します。

個々のデバイスを有効/無効にする

カメラは、デフォルトで**有効**です。

マイク、スピーカー、メタデータ、入力および**出力**は、デフォルトで**無効**です。

これは、システムで使用できるようにするには、マイク、スピーカー、メタデータ、入力および出力を個別に有効にしなければならないことを意味しています。理由は、監視システムは本質的にカメラに依存しているものの、マイクなどの使用の有無は、各組織のニーズによって極めて異なる場合が多いためです。

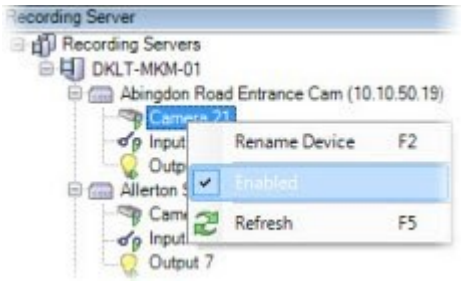
デバイスが有効か無効かを確認できます(例は出力です)。

(無効)

有効

同じ方法でカメラ、マイク、スピーカー、メタデータ、入力、および出力を有効化/無効化することができます。

1. レコーディングサーバーとデバイスを展開します。有効にするデバイスを右クリックします。
2. **有効**を選択して、選択/解除します。



ハードウェアへの安全な接続を設定する

SSL(セキュアソケットレイヤー) を使用して、ハードウェアデバイスとレコーディングサーバーの間で安全なHTTPS接続を設定できます。

以下の手順を実行する前に、カメラのベンダーに連絡してハードウェアの証明書を入手し、ハードウェアへアップロードしてください。

1. **概要** ペインで、レコーディングサーバーを右クリックし、ハードウェアを選択します。

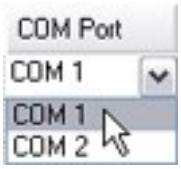
2. **設定** タブでHTTPSを有効にします。デフォルトでは無効になっています。
3. HTTPS接続で使用するレコーディングサーバーのポートを入力します。ポート番号は、デバイスのホームページで設定されたポートに対応している必要があります。
4. 必要に応じて変更し、保存します。

ビデオエンコーダーでのPTZの有効化

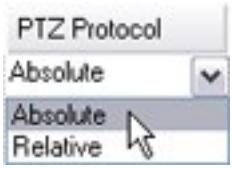
ビデオエンコーダーでPTZカメラの使用を有効にするには、**PTZ**タブで次の手順を実行します。

1. ビデオエンコーダーに接続されているデバイスのリストで、該当するカメラの**PTZを有効化** ボックスを選択します。

2. **PTZデバイスID**列で、各カメラのIDを確認します。
3. **COMポート**列で、PTZ機能を制御するために使用する、ビデオエンコーダーのCOM(シリアル通信) ポートを選択します。



4. **PTZプロトコル**列で、使用する位置スキームを選択します。



- **絶対値**: オペレータがカメラのPTZ(パン/チルト/ズーム) 制御を使用すると、固定位置(カメラのホーム位置) に対して相対的にカメラが調整されます。
- **相対値**: オペレータがカメラのPTZ(パン/チルト/ズーム) 制御を使用すると、現在の位置に対して相対的にカメラが調整されます。

PTZプロトコル列の内容は、ハードウェアによって大きく異なります。5 ~ 8の異なるプロトコルがあります。カメラのマニュアルもあわせて参照してください。

5. ツールバーで**保存**をクリックします。
6. これで、各PTZカメラのプリセット位置とパトロールを設定できます。
   - プリセット位置を追加する(タイプ1)
   - パトロール設定の追加

ハードウェアデバイスのパスワードを変更

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

1回の操作で、複数のハードウェアデバイスのパスワードを変更することができます。

まず、Canon、Axis、Bosch、Hanwa、Panasonic、Sony、Hikvision、ONVIFと互換性のあるハードウェアデバイスのモデルがサポートされており、モデルがサポートされているかどうかはユーザーインターフェイスに直接表示されます。対応モデルについては、弊社Webサイトでもご確認いただけます。https://www.milestonesys.com/community/business-partner-tools/supported-devices/

パスワード管理に対応していないデバイスについては、ハードウェアデバイスのパスワードをWebページで変更してから、Management Clientで手動で新しいパスワードを入力します。詳細については、「205ページのハードウェアの編集」を参照してください。

以下を選択できます。

- 各ハードウェアデバイスに対して個別のパスワードを生成する。システムが、ハードウェアデバイスのメーカーによる条件に基づきパスワードを生成します。
- すべてのハードウェアデバイスに単一のユーザー定義パスワードを使用する。新しいパスワードを適用すると、ハードウェアデバイスはレコーディングサーバーへの接続が一瞬切れます。新しいパスワードの適用後、各ハードウェアデバイスの結果が画面に表示されます。変更に失敗した場合、失敗の理由が表示されます(ハードウェアデバイスがその種の情報に対応している場合) 。ウィザード内からパスワード変更の成否レポートを作成することができますが、その結果は**「サーバーログ」**にも記録されます。

> ハードウェアデバイスにONVIFドライバーと複数のユーザーアカウントがある場合、このハードウェアデバイスの管理者権限を持つXProtect管理者のみVMSからパスワードを変更できます。

要件:

- ハードウェアデバイスのモデルは、Milestoneによるデバイスのパスワード管理に対応しています。

手順:

1. **サイトナビゲーション**ペインで**レコーディングサーバー**ノードを選択します。
2. 概要ペインで、削除するレコーディングサーバーを右クリックします。
3. **[ハードウェアのパスワード変更]**を選択します。ウィザードが表示されます。
4. パスワードは、小文字と大文字、数字、および次の属性を使って入力します。**! ( ) * - . _**

   パスワードの長さは最大64文字です。

   > Bosch FLEXIDOME IP outdoor 5000 MP NDN-50051カメラのパスワードの長さは、最大19文字です。

5. 指示に従って、プロセスを完了してください。

   > **最後に変更したパスワード**フィールドには、最後にパスワードを変更した際のタイムスタンプが表示されます。ここでは、パスワードを変更したコンピュータの現地の時刻設定が反映されます。

6. 最後にページに結果が表示されます。システムでパスワードが更新されなかった場合は、ハードウェアデバイスの横に表示された**[失敗]**をクリックして理由を確認します。
7. また、**[レポートを印刷]**ボタンをクリックして、すべてのデバイスの更新成功と失敗の一覧を出すことができます。
8. 失敗したハードウェアデバイスのパスワードを変更する場合は、**[再試行]**をクリックしてその失敗したハードウェアデバイスについてウィザードを再度始めてください。

再試行を選択すると、ウィザードを初めて完了したときのレポートは表示されなくなります。

セキュリティ上の制限により、数回連続してパスワード変更に失敗すると一定の期間使用不可になるハードウェアデバイスがあります。セキュリティの制限はメーカーにより異なります。

ハードウェアデバイスでのファームウェア更新

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

Management Clientでは、VMSシステムに追加されたハードウェアのファームウェアを更新できます。同じファームウェアファイルと互換性がある場合は、複数のハードウェアデバイスのファームウェアを同時に更新できます。

ユーザーインターフェイスには、モデルがファームウェアの更新に対応しているかどうかが直接表示されます。Milestoneのウェブサイトで、モデルのサポート状況を確認することもできます。https://www.milestonesys.com/community/business-partner-tools/supported-devices/

ファームウェアの更新に対応していないデバイスの場合は、ウェブページからハードウェアデバイスのファームウェアを更新する必要があります。

ファームウェアを更新すると、ハードウェアデバイスはレコーディングサーバーから一時的に切断されます。

ファームウェアを更新すると、各ハードウェアデバイスの更新結果が画面に表示されます。更新に失敗した場合、失敗の理由が表示されます(ハードウェアデバイスがその種の情報に対応している場合)。この結果は、**サーバーログ**にも記録されます。

ハードウェアデバイスにONVIFドライバーと複数のユーザーアカウントがある場合、このハードウェアデバイスの管理者権限を持つXProtectの管理者のみVMSからファームウェアを更新できます。

要件:

- このハードウェアデバイスのモデルは、Milestoneによるファームウェアの更新に対応しています。

手順:

1. **サイトナビゲーション**ペインで**レコーディングサーバー**ノードを選択します。
2. 概要ペインで、該当するレコーディングサーバーを右クリックします。
3. **ハードウェアのファームウェア更新**を選択します。ウィザードが表示されます。

4. 指示に従って、プロセスを完了してください。

> 同じファームウェアファイルと互換性のある複数のハードウェアデバイスのみ更新できます。ONVIFドライバーを介して追加されたハードウェアは、メーカー名ではなく、**その他**に含まれています。

6. 最後にページに結果が表示されます。システムでファームウェアを更新できなかった場合は、ハードウェアデバイスの横に表示された**失敗**をクリックして理由を確認します。

> Milestoneは、互換性のないファームウェアファイルやハードウェアデバイスが選択された場合、ハードウェアデバイスの不具合について責任を負いません。

外部IDPを追加&設定

1. Management Clientで、**ツール** > **オプション**を選択し、**外部IDP**タブを開きます。
2. **外部IDP**セクションで、**追加**を選択します。
3. 外部IDPに必要な情報を入力します。必要な情報の詳細については、外部 IDPを参照してください。

VMSで使用するために外部IDPからの苦情を登録する方法については、外部IDPからの苦情を登録するを参照してください。

デバイス- グループ

デバイスグループの追加

1. **概要**ペインで、デバイスグループを作成するデバイスタイプを右クリックします。
2. **デバイスグループを追加**を選択します。
3. **デバイスグループを追加**ダイアログボックスで、新しいデバイスグループの名前と説明を指定します。

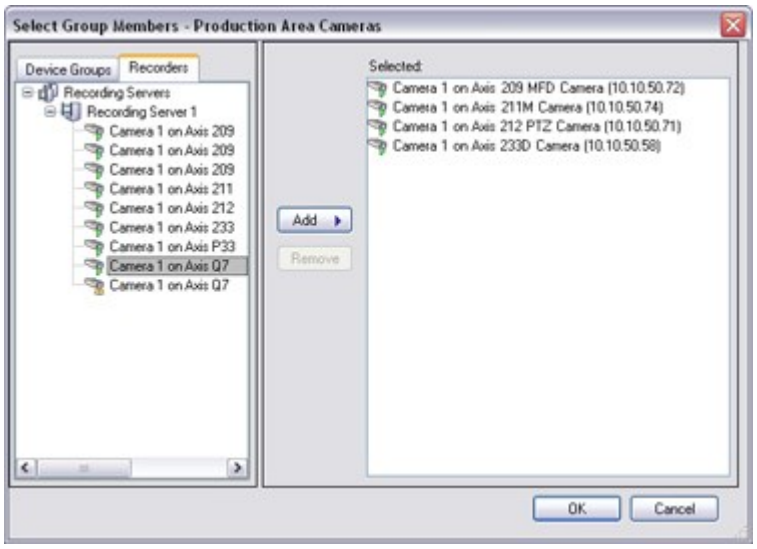
デバイスグループリストのデバイスグループの上にマウスを置くと、説明が表示されます。

4. **OK**をクリックします。新しいデバイスグループであることを示すフォルダーがリストに追加されます。
5. 続いて、どのデバイスをデバイスグループに含めるかを指定します(「214ページのデバイスグループに含めるデバイスの指定」を参照)。

デバイスグループに含めるデバイスの指定

1. **概要**ペインで、関連するデバイスグループフォルダーを右クリックします。
2. **デバイスグループメンバーを編集**を選択します。
3. **グループメンバーを選択**ウィンドウで、デバイスを配置するタブを1つ選択します。

   デバイスは、複数のデバイスグループのメンバーになれます。
4. 含めたいデバイスを選択して、**追加**ボタンをクリックするかデバイスをダブルクリックします。



5. **OK**をクリックします。
6. 1グループに400デバイスの制限を超過する場合は、デバイスグループを他のデバイスグループのサブグループとして追加できます。

無効なデバイス

無効化されたデバイスは、デフォルトでは**概要**ペインに表示されません。

無効になったデバイスをすべて表示するには、**概要**ペインの上部にある**フィルター**をクリックして**フィルター**タブを開き、**無効なデバイスを表示する**を選択します。

無効なデバイスを再び非表示にするには、**無効なデバイスを表示**をオフにします。

デバイスグループのすべてのデバイスに対する共通プロパティの指定

デバイスグループでは、特定のデバイスグループ内のすべてのデバイスの共通設定を指定できます。

1. **概要**ペインで、デバイスグループをクリックします。

   プロパティペインには、**デバイスグループのすべてのデバイスで使用できる**すべてのプロパティが、タブでグループ化されて一覧表示されます。

2. 関連する共通のプロパティを指定します。

   設定タブで、**すべての**デバイスの設定および個々のデバイスの設定の間で切り替えることができます。

3. ツールバーで**保存**をクリックします。設定は個別のデバイスに保存され、デバイスグループには保存されません。

無効なデバイス

無効化されたデバイスは、デフォルトでは**概要**ペインに表示されません。

無効になったデバイスをすべて表示するには、**概要**ペインの上部にある**フィルター**をクリックして**フィルター**タブを開き、**無効なデバイスを表示する**を選択します。

無効なデバイスを再び非表示にするには、**無効なデバイスを表示**をオフにします。

デバイスグループ経由のデバイスの有効化/無効化

設定済みハードウェアからのみデバイスを有効化/無効化できます。ハードウェアの追加ウィザードから手動で有効化/無効化した場合を除いて、カメラデバイスはデフォルトで有効化されており、他のデバイスはデフォルトで無効化されています。

無効化されたデバイスは、デフォルトでは**概要**ペインに表示されません。

無効になったデバイスをすべて表示するには、**概要**ペインの上部にある**フィルター**をクリックして**フィルター**タブを開き、**無効なデバイスを表示する**を選択します。

無効なデバイスを再び非表示にするには、**無効なデバイスを表示**をオフにします。

デバイスを有効または無効にするためにデバイスグループ経由でアクセスする方法

1. **サイトナビゲーション**ペインで、デバイスを選択します。
2. **概要**ペインで、関連グループを展開してデバイスを検索します。
3. デバイスを右クリックして、**ハードウェアに移動**を選択します。
4. **[+]**ノードをクリックして、ハードウェア上のすべてのデバイスを表示します。
5. 有効/無効にするデバイスを右クリックして、**有効にする**を選択します。

デバイス- カメラ設定

カメラ設定の表示または編集

1. **サイトナビゲーション**ペインで、**デバイス**を選択し、**カメラ**を選択します。
2. **概要**ペインで該当するカメラを選択します。
3. **設定**タブを開きます。

以下の設定を表示または編集できます。

- デフォルトのフレームレート
- 解像度
- 圧縮率
- キーフレーム間のフレームの最大数
- 選択したカメラまたは選択したデバイスグループ内のすべての、カメラの画面の日時およびテキスト表示

カメラのドライバーにより、**設定**タブの内容は異なります。ドライバーはカメラのタイプによって異なります。

数種類のストリーム(MJPEGとMPEG-4/H.264/H.265など)がサポートされているカメラについては、マルチストリーミングを使用できます。「222ページのマルチストリーミングの管理」を参照してください。

プレビュー

設定を変更する場合は、**プレビュー**ペインを有効にすると、変更の影響を簡単に確認できます。

- **プレビュー**を有効にするには、**ビュー**メニューをクリックし、**プレビューウィンドウ**をクリックします。

プレビューペインを使用してフレームレート変更の影響を確認することはできません。その理由は、**プレビュー**ペインのサムネイル画像では**オプション**ダイアログボックスで定義された他のフレームレートを使用しているためです。

パフォーマンス

キーフレーム間の最大フレーム数および**キーフレームモード間の最大フレーム数**の設定を変更すると、XProtect Smart Clientの一部の機能のパフォーマンスが低下するおそれがあります。例えば、XProtect Smart Clientはビデオ表示の起動にキーフレームが必要なので、キーフレーム間のインターバルが長いと、XProtect Smart Clientの起動に時間がかかります。

ハードウェアの追加

ハードウェアをシステムに追加する方法については、「203ページのハードウェアの追加」を参照してください。

魚眼レンズサポートを有効/無効にする

魚眼レンズサポートは、既定では無効です。

1. **[サイトナビゲーション]**ペインで、**[デバイス]**を選択してから**[カメラ]**を選択します。
2. **[概要]**ペインで該当するPTZカメラを選択します。
3. **[魚眼レンズ]**タブの**[魚眼レンズサポートを有効にする]**チェックボックスを選択または選択解除します。

魚眼レンズ設定の指定

1. **[魚眼レンズ]**タブで、レンズのタイプを選択します。
2. カメラの物理的位置/方向を**カメラの位置/方向**リストから指定します。
3. **ImmerVisionを可能にする®からばのモーフRPL ナンバー**リストのRegistered Panomorph Lens (RPL)ナンバーを選択

   これは、カメラで使用するレンズを識別し、正しく設定するためです。RPL番号は、通常はレンズ本体またはカメラが入っていた箱に記載されています。ImmerVison、Panomorph(パノモーフ) レンズ、RPLの詳細については、ImmerVision Enables Webサイト(https://www.immervisionenables.com/) を参照してください。

   歪み補正レンズプロファイルを選択する場合は、必ず望ましい**視界**を設定してください。

デバイス - 録画

録画の有効化/無効化

デフォルトでは録画は有効になっています。録画を有効化/無効化する方法

1. **サイトナビゲーション**ペインで**レコーディングサーバー**を選択します。
2. **概要**ペインで関連するデバイスを選択します。
3. **録画**タブで、**録画**チェックボックスを選択します。

> カメラからのデータ録画を可能にするには、デバイスの録画を有効にする必要があります。デバイスの録画を無効にすると、デバイスの録画条件を指定するルールが機能しません。

関連するデバイスで録画を有効にする

カメラデバイスで、マイクなど同じレコーディングサーバーに接続されている関連するデバイスの録画を有効にすることができます。これは、カメラが録画する際に、関連するデバイスも録画することを意味します。

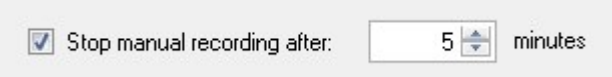
新しいカメラデバイスではデフォルトで関連するデバイスの録画が有効になっていますが、必要に応じて無効または有効にすることができます。システムにある既存のカメラデバイスでは、このチェックボックスはデフォルトでクリアされています。

1. **サイトナビゲーション**ペインで**レコーディングサーバー**を選択します。
2. **概要**ペインで関連するカメラデバイスを選択します。
3. **録画**タブで、**関連するデバイスで録画する**チェックボックスを選択または選択解除します。
4. **クライアント**タブで、このカメラに関連付けるデバイスを指定します。

他のレコーディングサーバーに接続されている関連デバイスで録画を有効にしたい場合は、ルールを作成する必要があります。

手動録画の管理

デフォルトでは、**次の時間が経過すると手動録画を停止**が有効になっており、録画時間は5分です。これは、XProtect Smart Clientユーザーが開始したすべての録画が自動的に停止することを保証するためです。



1. **サイトナビゲーション**ペインで**デバイス**を選択します。
2. **概要**ペインで関連するデバイスを選択します。
3. **録画**タブで、**次の時間が経過すると手動録画を停止**チェックボックスを選択または選択解除します。

有効にする場合は、録画時間を指定します。指定する分単位の時間は、システムに負荷をかけ過ぎることなく、さまざまな手動録画の要件に対応するのに十分な長さにする必要があります。

役割に追加

デバイスタブの**役割**で、各カメラのクライアントユーザーに手動録画を開始および停止する権限を付与する必要があります。

ルールで使用する

手動録画に関連するルールを作成する際に使用できるイベントは、以下の通りです。

- 手動録画の開始
- 手動録画の停止

レコーディングフレームレートを指定する

JPEGのレコーディングフレームレートを指定できます。

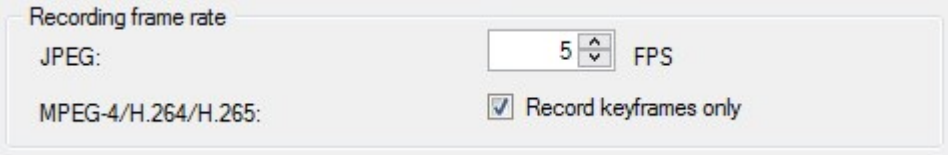
1. **[サイトナビゲーション]**ペインで**[デバイス]**を選択します。
2. **概要**ペインで関連するデバイスを選択します。
3. **[録画]**タブの**[レコーディングフレームレート: (JPEG)]**ボックスで、レコーディングフレームレート(FPS: フレーム数/秒)を選択または入力します。

キーフレームレコーディングの有効化

MPEG-4/H.264/H.265ストリームのキーフレームレコーディングを有効にできます。つまり、ルール設定によって、キーフレームのみの録画とすべてのフレームの録画を切り替えます。

例えば、ビューでモーションがないときにシステムにキーフレームを録画させ、モーションが検出された場合にだけすべてのフレームに切り替えてストレージを節約できます。

1. **サイトナビゲーション**ペインで**デバイス**を選択します。
2. **概要**ペインで関連するデバイスを選択します。
3. **録画**タブで、**キーフレームのみを録画**チェックボックスを選択します。



4. 機能を有効にするためのルールを設定します。「アクションと停止アクション」を参照してください。

関連するデバイスで録画を有効にする

カメラデバイスで、マイクなど同じレコーディングサーバーに接続されている関連するデバイスの録画を有効にすることができます。これは、カメラが録画する際に、関連するデバイスも録画することを意味します。

新しいカメラデバイスではデフォルトで関連するデバイスの録画が有効になっていますが、必要に応じて無効または有効にすることができます。システムにある既存のカメラデバイスでは、このチェックボックスはデフォルトでクリアされています。

1. **サイトナビゲーション**ペインで**レコーディングサーバー**を選択します。
2. **概要**ペインで関連するカメラデバイスを選択します。
3. **録画**タブで、**関連するデバイスで録画する**チェックボックスを選択または選択解除します。
4. **クライアント**タブで、このカメラに関連付けるデバイスを指定します。

他のレコーディングサーバーに接続されている関連デバイスで録画を有効にしたい場合は、ルールを作成する必要があります。

リモート録画の保存および取得

接続が復旧した際に自動的にリモート録画が取得されるよう設定すれば、ネットワーク問題の発生時にもすべてのリモート録画が確実に保存できます。

1. **[サイトナビゲーション]**ペインで**[デバイス]**を選択します。
2. **概要**ペインで関連するデバイスを選択します。
3. **[リモート録画]**で、**[接続が復旧したときに自動的にリモート録画を取得]**を選択します。これにより、接続が復旧した際に録画が自動的に取得されるようになります。

> リモート録画オプションは、選択されたカメラでエッジストレージがサポートされている場合、または選択されたカメラがMilestone Interconnect設定されている場合にのみ使用できます。

選択されたハードウェアのタイプによって、どこから記録を取得するかが決まります。

- ローカル録画ストレージのあるカメラの場合、録画はカメラのローカル録画ストレージから取得されます。
- Milestone Interconnectリモートシステムの場合、録画はリモートシステムのレコーディングサーバーから取得されます。

自動取得とは別に、以下の機能を使用できます。

- 手動録画
- **は、<devices>**ルールからリモート録画を取得および保存します。
- **は<device>**ルールから、<start and end time>間のリモート録画を取得し保存します

録画を削除

1. **[サイトナビゲーション]**ペインで**[デバイス]**を選択します。
2. **[概要]**ペインで該当するデバイスを選択し、**[録画]**タブを選択します。
3. **[すべての録画を削除]**ボタンをクリックして、デバイスまたはデバイスグループの録画をすべて削除します。

この方法は、グループ内の全デバイスを同一のサーバーに追加した場合にしか使用できません。保護されたデータは削除されません。

デバイス - ストリーミング

アダプティブストリーミング(説明付き)

アダプティブストリーミングは、複数のライブビデオストリームが同じビューで表示される場合に使用するストリーミング方式です。これによってクライアントは、ビューアイテムで要求されたストリームと解像度が最も一致するライブビデオストリームを自動的に選択することが可能になります。アダプティブストリーミングは、ネットワーク負荷を軽減し、クライアントコンピュータのデコーディング機能とパフォーマンスを向上します。

XProtect Smart Clientのアダプティブストリーミングを有効にする際に、ビューアイテムで要求された解像度で利用可能なビデオストリームの内、最も一致したものを設定できます。詳細についてはアダプティブストリーミングの有効化をご確認ください。

XProtect Smart Clientで、アダプティブストリーミングはライブおよび再生モードで摘要できます。モバイルクライアントで使用可能なのはライブモードのみです。

再生モードで摘要した場合、このストリーミング方式はアダプティブ再生と呼ばれます。詳細については、「220ページのアダプティブ再生(説明付き)」を参照してください。

アダプティブ再生(説明付き)

アダプティブ再生は、再生モードでアダプティブストリーミングを使用可能にする構成です。

アダプティブ再生は、2つのレコーディングストリーム、プライマリおよびセカンダリストリームを要求します。Management Clientでどちらのストリームも有効にする場合、両ストリームとも録画します。

- セカンダリレコーディングが構成される前にある期間のビデオを再生した場合、プライマリレコーディングだけが再生されます。
- セカンダリレコーディングが構成された後で録画されたビデオを再生する場合、クライアントのビューサイズに最も適したものに合わせて、プライマリまたはセカンダリレコーディングのビデオが再生されます。

使用可能

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

アダプティブストリーミングを有効にする

Smart Clientプロファイルの**高度**タブでアダプティブストリーミングと共にアダプティブ再生を有効にすることができ、XProtect Smart Clientの**設定 > 高度 > アダプティブストリーミング**でも有効にできます。XProtect Smart Clientでアダプティブストリーミングの有効化については、アダプティブストリーミングの有効化を参照してください。

エッジレコーディング

オプションとして、アダプティブ再生のエッジレコーディングを使用できます。エッジレコーディングを使用すると、ストリームの残りの部分とは異なる、通常はもっと高い解像度でストリームのシーケンスを表示することが可能です。例えば、低解像度のプライマリストリームを録画し、高解像度のソースからのレコーディングを結合できます。データを参照する際、結合したエッジレコーディングを有効にできます。

エッジレコーディングはメディアデータベースに保存され、これらレコーディングの解像度は個々のカメラに設定されます。

再生ビデオの解像度

アダプティブ再生を使用する場合、再生ビデオの解像度はプライマリおよびセカンダリレコーディングに設定した現在の解像度で決定されます。これは再生で、プライマリおよびセカンダリストリームのいずれかの選択が、各レコーディングストリームに現在設定されている解像度をベースにしているためです。

ストリームの追加

録画のために追加したストリームは、ライブおよび再生モードで表示されます。

アダプティブストリーミングを有効にしたビューアイテムで、録画したビデオを表示することもできます。再生モードのアダプティブストリーミングをアダプティブ再生と呼びます。

1. **ストリーム**タブで、**追加**をクリックします。この操作で、リストに2番目のストリームが追加されます。
2. **名前**列で、ストリームの名前を編集します。名前はXProtect Smart Clientに表示されます。
3. **ライブモード**列で、いつライブストリームが必要かを選択します。
   - **常時**:XProtect Smart Clientユーザーがストリームを要求しなくても、ストリームは実行されます。
   - **実行しない**:ストリームはオフになります。例えば、高画質で録画したいので帯域幅が必要な場合などに、これを選択します。
   - **必要な時**:クライアントから要求された場合、またはストリームが録画に設定されている場合に、ストリームを開始します。
4. **デフォルトライブストリーム**列で、クライアントが特定のストリームを要求せず、アダプティブストリーミングが無効な場合に、どのストリームをデフォルトとするかを選択します。
5. **録画**列で、**プライマリ**または**セカンダリ**のいずれかを選択します。アダプティブ再生向けに、各タイプのストリームを作成する必要があります。再生するビデオは、プライマリビデオストリームから取得され、必要な場合はセカンダリストリーミングを含みます。プライマリ録画は必ず必要です。また、**プライマリ**として設定したストリームは、モーション検知やXProtect Smart Clientからのエクスポート向けなどのさまざまな状況で使用されます。
6. **デフォルト再生**の下で、どのストリームをデフォルトにするかを選択します。アダプティブ再生を設定していない場合には、クライアントへデフォルトストリームが配信されます。
7. エッジレコーディングを使用したい場合は、**エッジレコーディングを使用**列のチェックボックスを選択します。エッジレコーディングについては221ページのエッジレコーディングを参照してください。
8. **保存**をクリックします。

> 誰もライブビデオを見ていない場合にストリームを実行しないようにするには、**デフォルトのフィード開始ルール**を修正し、要求があった時に、定義済みの**クライアントライブフィードの要求**イベントを使用してストリームを開始するようにします。

マルチストリーミングの管理

ライブビデオの閲覧および録画ビデオの再生には、必ずしも同じビデオ画質とフレームレートが必要とは限りません。

録画に使用するストリームを変更するには

アダプティブ再生は、2つのストリームをレコーディング、プライマリおよびセカンダリストリームに設定することを要求します。ライブストリームには、カメラがサポートする複数のライブストリームを設定し、使用できます。

1. **サイトナビゲーション**ペインで**デバイス**を選択します。
2. **概要**ペインで該当するカメラを選択します。
3. **ストリーム**タブで、レコーディングに使いたいストリームを選択します。

4. **ライブモード**リストで関連するオプションを選択します。オプション**必要な場合**、**常時**および**不可**は、クライアント側でストリームを適用すべきタイミングを示します。クライアントから何も要求が無い場合、レコーディングは**デフォルトライブストリーム**チェックボックスを選択したストリームを使用します。
5. 1つのストリームで録画するためには、**レコーディング**リスト上の**プライマリ**または**セカンダリ**のいずれかを選択します。
6. アダプティブ再生を使用するためには、2つのストリームを設定し、片方を**プライマリ**に、もう片方を**セカンダリ**に設定します。
7. ストリーム上で録画するためには、**レコーディング**リストで**プライマリ**または**セカンダリ**ストリームのいずれかを選択します。

データ転送の制限

クライアントによって閲覧されているときにのみビデオストリームが実行されるよう、条件を設けることができます。

ストリーミングを管理するため、そして不要なデータ転送を制限するため、ストリーミングは以下の条件下では開始しません:

1. **サイトナビゲーション**ペインで**デバイス**を選択します。
2. **概要**ペインで該当するカメラを選択します。
3. **[ストリーム]**タブの**[ライブモード]**リストで**[必要な場合]**を選択します。
4. **[録画]**タブの**[録画]**チェックボックスを選択解除します。
5. **[モーション]**タブの**[モーション検知]**チェックボックスを選択解除します。

これらの条件が満たされた場合、ビデオストリームはクライアントによる閲覧時にのみ実行されます。

例

例1: ライブビデオおよび録画ビデオ:

- **ライブ**ビデオの再生では、組織によって高いフレームレートでのH.264が望ましい場合があります。
- **録画**ビデオを再生する場合、組織によっては低いフレームレートでのMJPEGを使用することで、ディスクの空き容量を保持できる方が望ましい場合もあります。

例2: ローカルビデオおよびリモートライブビデオ:

- **ローカル接続された操作ポイントからライブビデオ**を閲覧する場合、組織によっては可能な限り高品質のビデオを利用するために、高いフレームレートのH.264が望ましい場合があります。
- **リモート接続された操作ポイントからライブビデオ**を閲覧する場合、組織によってはネットワーク帯域を保持するために、低いフレームレートのMJPEGが望ましい場合もあります。

例3: アダプティブストリーミング:

- **ライブビデオを閲覧し、XProtect Smart ClientコンピュータのCPUとGPUの負荷を軽減**するには、組織によっては複数の高フレームレートH.264/H.265を使用するものの、アダプティブストリーミングの使用時にはXProtect Smart Clientによって要求された解像度と一致させるために異なる解像度が使用されることが望ましい場合もあります。詳細については、「441ページのSmart Clientのプロファイル(クライアントノード) 」を参照してください。

カメラの**[クライアント]**タブで**[ライブマルチキャスト]**を有効にした場合(「[クライアント]タブ(デバイス)」を参照)、デフォルトのビデオストリームに対してのみ機能します。

たとえカメラがマルチストリーミングをサポートしていても、カメラによって個々のマルチストリーミングの機能は異なります。詳細については、カメラの文書を参照してください。

カメラで他の種類のストリームを利用できるかを確認するには、**[設定]タブ(デバイス)**を参照します。

デバイス - ストレージ

プリバッファの管理

カメラ、マイクおよびスピーカーがプリバッファをサポートします。スピーカーでは、XProtect Smart Clientユーザーが**スピーカーで話す**機能を使用している場合にのみストリームが送信されます。つまり、スピーカーストリームの記録がどのように起動されるかによって、使用可能なプリバッファがわずかであったり、プリバッファがない場合が生じます。

ほとんどの場合、XProtect Smart Clientユーザーが**スピーカーで話す**機能を使用している場合に、スピーカーを録画するように設定されています。この場合は、スピーカーのプリバッファは利用できません。

プリバッファ機能を使用するには、デバイスを有効にしてストリームをシステムに送信する必要があります。

プレバッファの有効化と無効化

プレバッファは、デフォルトでは3秒のプレバッファサイズで有効になっており、メモリに保存されます。

1. **[サイトナビゲーション]**ペインで**[デバイス]**を選択します。
2. **概要**ペインで関連するデバイスを選択します。
3. **[録画]**タブで、**[プレバッファ]**チェックボックスを選択または選択解除します。
4. **クライアント**タブで、このカメラに関連付けるデバイスを指定します。

ストレージ場所とプレバッファ期間の指定

一時プレバッファ録画はメモリ内またはディスク上のいずれかに保存されます。

1. **[サイトナビゲーション]**ペインで**[デバイス]**を選択します。
2. **[概要]**ペインで該当するデバイスを選択し、**[録画]**タブを選択します。
3. **[場所]**リストで**[メモリ]**または**[ディスク]**を選択し、秒数を指定します。
4. 15秒を上回るプレバッファ期間が必要な場合は、**[ディスク]**を選択します。

指定する秒数は、定義済みの様々な記録ルールでの要件に対応するに十分な大きさである必要があります。

場所を**[メモリ]**に変更すると、期間が自動的に15秒に短縮されます。

ルールでプレバッファを使用

録画を起動するルールを作成する場合、録画が実際のイベントよりも少し前に始まるように選択できます(プリバッファ)。

例:以下のルールでは、カメラがモーションを検知する5秒前にカメラでの録画が始まるように指定しています。

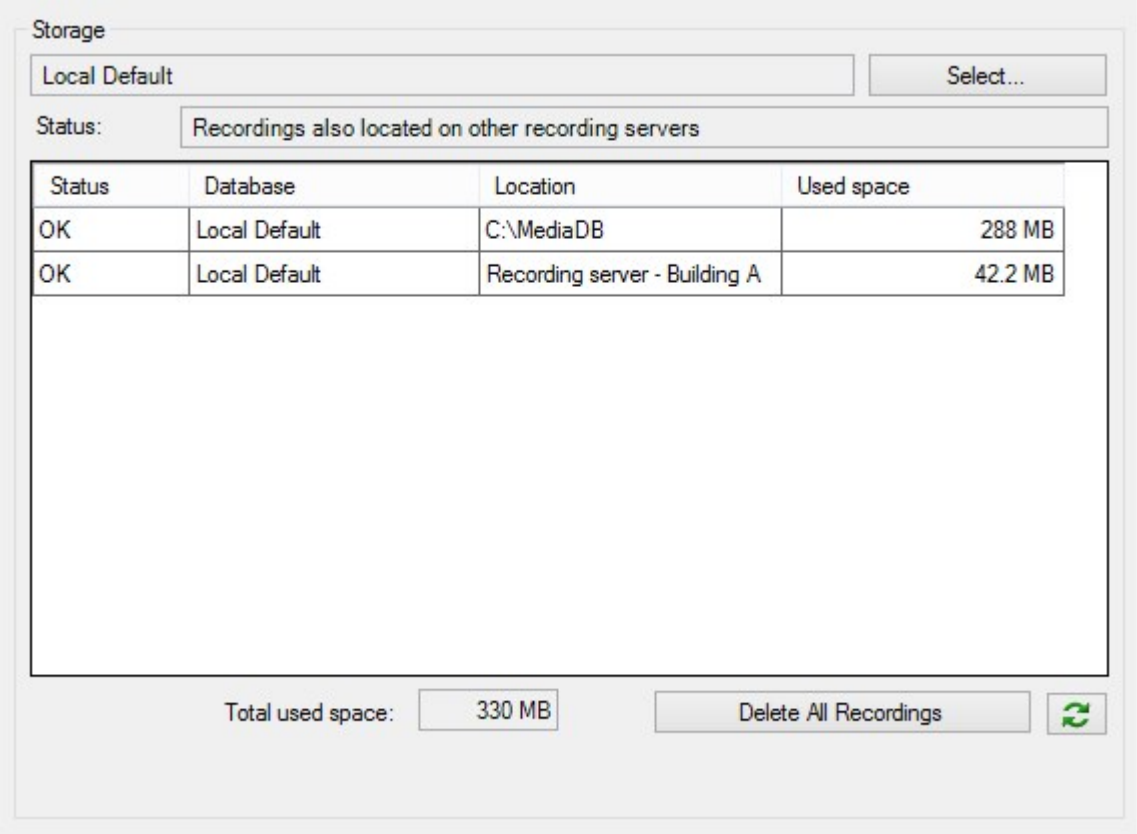
プリバッファ録画機能をルールで使用するには、録画されるデバイスのプリバッファ機能を有効にし、プリバッファ長さを少なくともルールで定義した長さと同じに設定する必要があります。

デバイスのデータベースのステータスをモニター

1. **[サイトナビゲーション]**ペインで**[デバイス]**を選択します。
2. **[概要]**ペインで該当するデバイスを選択し、**[録画]**タブを選択します。

[ストレージ]の下で、デバイス、または同じレコーディングサーバーに追加されたデバイスのグループのデータベースを監視および管理できます。

表の上では、選択されたデータベースとその状態が確認できます。この例では、選択されたデータベースはデフォルトの**ローカルデフォルト**で、ステータスは**録画が他のレコーディングサーバーにも存在する**です。他のサーバーは建物Aのレコーディングサーバーです。



選択したデータベースで生じ得るステータス

名前	説明
録画は他のレコーディングサーバーにもあります	データベースがアクティブで稼動中であり、他のレコーディングサーバーのストレージにも録画があります。
アーカイブも古いストレージにあります	データベースはアクティブで実行中です。また、アーカイブは他のストレージにもあります。
アクティブ	データベースはアクティブで実行中です。
選択されたデバイスの一部に関するデータは現在他の場所に移動中です	データベースはアクティブで実行中です。グループ内の選択された1つ以上のデバイスで、ある場所から他の場所へデータを移動しています。
デバイスのデータは現在他の場所に移動中です	データベースはアクティブで実行中です。選択されたデバイスで、ある場所から他の場所へデータを移動しています。
フェールオーバーモードで利用可能な情報はありません	データベースがフェールオーバーモードの場合は、データベースのステータス情報を収集できません。

さらにウィンドウの下部には、各データベースのステータス(**OK**、**オフライン古いストレージ**)、各データベースの場所、および各データベースが占有する領域が表示されます。

すべてのサーバーがオンラインである場合は、**[合計使用スペース]**フィールドにストレージ全体で使用される合計領域を表示できます。

ストレージの構成について詳しくは、「[ストレージ]タブ(レコーディングサーバー)」を参照してください。

デバイスを元のストレージから別のストレージに移動

記録の保存先となる新しい場所を選択しても、既存の記録は移されません。これまでと同じ場所にとどまり、自身が属するストレージの構成にもとづいた状態が示されます。

1. **[サイトナビゲーション]**ペインで**[デバイス]**を選択します。
2. **[概要]**ペインで該当するデバイスを選択し、**[録画]**タブを選択します。
3. **ストレージ**で**選択**をクリックして、デバイスによる録画先となるレコーディングストレージを選択します。

録画は、選択したストレージの構成に従ってアーカイブされます。

デバイス - モーション検知

モーション検知(説明付き)

モーション検知の設定は、システムの重要な部分です。モーション検知の設定により、システムでモーションイベントを生成するタイミング、さらに通常はビデオを録画するタイミングを決定します。

それぞれのカメラに最適なモーション検知の構成が得られるようにあらかじめ調整しておくことで、後になって不必要な録画などを避けるのに役立ちます。カメラの物理的な位置によっては、異なる物理的条件(昼/夜、強風/無風など)でモーション検知の設定をテストすることをお勧めします。

カメラのビューでモーションとみなされるために必要となる変更の量を設定することができます。たとえば、モーション検知分析を行う間隔や、モーションを無視するビューのエリアを指定できます。モーション検知検出の精度を調整し、それによってシステムリソース上の負荷を調整することもできます。

画質

Milestoneでは、カメラのモーション検知を設定する前に、カメラの画質の設定(解像度、ビデオコーデック、ストリーム設定など)を行うよう強く推奨しています。この操作は、デバイスの**[プロパティ]**ウィンドウの**[設定]**タブで行います。後で画質の設定を変更すると、必ずモーション検知の設定を変更後にテストしなくてはならなくなるからです。

プライバシーマスク

常設のプライバシーマスクでカバーされているエリアが定義されている場合、これらのエリアではモーションが検知されません。

モーション検知の有効化と無効化

カメラのモーション検知のデフォルト設定を行う

1. **ツール**メニューで**オプション**をクリックします。
2. **一般**タブの**新しいカメラデバイスを追加するときに自動的に有効にする**で、**モーション検知**チェックボックスを選択します。

特定のカメラのモーション検知を有効または無効にする

1. **サイトナビゲーション**ペインで、**デバイス**を選択し、**カメラ**を選択します。
2. **概要**ペインで該当するカメラを選択します。
3. **モーション**タブの**モーション検知**チェックボックスを選択または選択解除します。

カメラのモーション検知を無効にすると、カメラのモーション検知関連のルールは機能しません。

ハードウェアアクセラレーションを有効または無効にする

カメラを追加した際には、デフォルトとして、モーション検知に自動ハードウェアアクセラレーションによる映像デコーディングが用いられます。可能な場合は、レコーディングサーバーによってGPUリソースが使用されます。これによってビデオモーション分析中のCPU負荷を軽減し、レコーディングサーバーの一般的なパフォーマンスを向上します。

ハードウェアアクセラレーションを有効または無効にする方法

1. **サイトナビゲーション**ペインで**デバイス**を選択します。
2. **概要**ペインで該当するカメラを選択します。
3. **モーション**タブの**ハードウェアアクセラレーション**で、**自動**を選択してハードウェアアクセラレーションを有効にするか、**オフ**を選択して設定を無効にします。

GPUリソースの使用

モーション検知のハードウェアアクセラレーションによる映像デコーディングでは、以下にGPUリソースが使用されます。

- Intel Quick SyncをサポートするIntel CPU
- NVIDIA®による、レコーディングサーバーに接続されているアダプターの表示

ロードバランスとパフォーマンス

異なるリソース間のロードバランスは自動的に行われます。**システムモニター**ノードでは、NVIDIA GPUリソースにおける現在のモーション分析の負荷が**システムモニターしきい値**ノードの指定の制限内であるかどうか、検証が可能です。NVIDIA GPU負荷の指標は以下の通りです。

- NVIDIAデコード
- NVIDIAメモリ
- NVIDIAレンダリング

負荷が高すぎる場合は、複数のNVIDIAディスプレイアダプタをインストールして、GPUリソースをレコーディングサーバーに追加できます。Milestoneは、NVIDIAディスプレイアダプタのスケーラブルリンクインターフェイス(SLI)構成の使用を推奨していません。

NVIDIA製品の演算能力は、さまざまです。

モーション検出のためのNVIDIA GPUを用いたハードウェアアクセラレーションによる映像デコーディングには、バージョン6.x(Pascal)以上の演算能力が必要です。

- お使いのNVIDIA製品の演算能力は、NVIDIAのウェブサイト(https://developer.nvidia.com/cuda-gpus/)で確認できます。
- ビデオモーション検出が特定のカメラのハードウェアでアクセラレーションされるかどうかを確認するには、レコーディングサーバーのログファイルの監視を有効にします。レベルを**デバッグ**に設定すると、診断結果はDeviceHandling.log.に記録されます。ログは以下のパターンで記録されます。
  [time] [274] DEBUG - [guid] [name] Configured decoding: Automatic: Actual decoding: Intel/NVIDIA

レコーディングサーバーのOSのバージョンとCPUの世代がハードウェアアクセラレーションによるビデオモーション検出のパフォーマンスに影響する場合があります。古いバージョンではGPUメモリ割り当てがしばしば障害となります(一般的な限界値は0.5 GBから1.7 GBです)。

Windows 10 / Server 2016および第6世代CPU(Skylake)以降のシステムは、GPUにシステムメモリの50%を割り当てることによって、この障害を低減または取り除いています。

第6世代のIntel製CPUはH.265のハードウェアアクセラレーションによるデコードをサポートしているため、このバージョンのCPUのパフォーマンスはH.264と同等になります。

手動感度を有効にしてモーションを定義する

感度設定は、画像の中の**各ピクセル数がどれだけ**変化すればモーションとみなすかを決定します。

1. **サイトナビゲーション**ペインで、**デバイス**を選択し、**カメラ**を選択します。
2. **概要**ペインで該当するカメラを選択します。
3. **モーション**タブの**手動感度**チェックボックスを選択します。

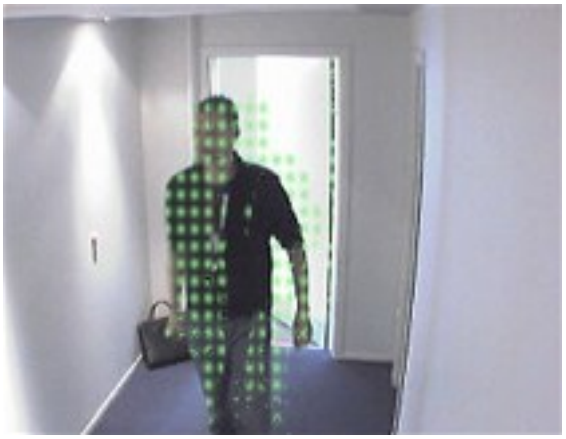
4. スライダーを左に動かすと感度レベルが上がり、右に動かすと感度レベルが下がります。

   感度レベルが**高くなるほど**、より少ない各ピクセルの変化でもモーションとみなされます。

   感度レベルが**低くなるほど**、より多い各ピクセルの変化でモーションとみなされます。

   モーションが検知されたピクセルは、プレビュー画像で緑色に強調表示されます。

5. モーションとみなされたものだけが強調表示されるよう、スライダーの位置を選択します。



スライダーの右側の数字で、カメラ間の実際の感度設定を比較することができます。

しきい値を指定してモーションを定義

モーション検知しきい値は、画像の中の**ピクセル数がどれだけ**変化すればモーションとみなすかを決定します。

1. スライダーを左に動かすとモーションレベルが上がり、右に動かすとモーションレベルが下がります。
2. モーションとみなされたものだけが検知されるよう、スライダーの位置を選択します。

モーション表示バーの黒い縦線はモーション検知のしきい値を示します。検知されたモーションが選択された検知しきい値レベルを超える場合、バーの色が緑から赤に変わり、検知されたことを示します。

モーション検知バー: しきい値を超えると色が緑から赤に変わり、モーションが検知されたことを示します。

モーション検知の除外エリアを指定

カメラのグループのすべての設定を構成できますが、一般的にはカメラごとに除外領域を設定します。

プライバシーマスクはモーション検知から除外されます。それらを表示するには、**プライバシーマスクを表示する**チェックボックスを選択してください。

特定の領域のモーション検知を無効にすると、例えば、カメラの撮影範囲に風で揺れる木があったり、背景に車両が定期的に通過する場合など、無関係なモーションの検知を避けることができます。

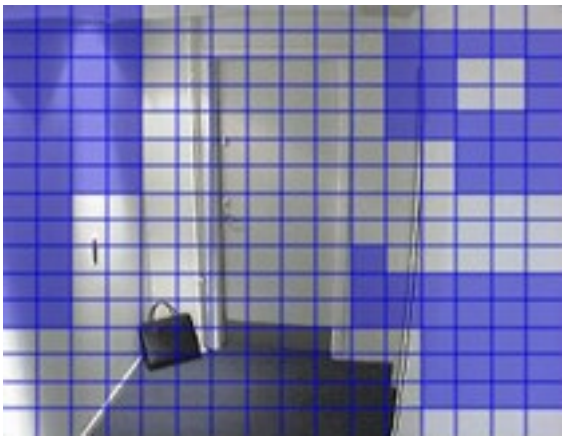
領域の除外をPTZカメラで使用している場合、カメラをパン/チルト/ズームしても、領域は対象ではなくカメラ画像にロックされているので、除外された領域はそれに合わせて移動**しません**。

1. 領域の除外を使用するには、**領域の除外を使用**チェックボックスを選択します。

   グリッドはプレビュー画像を選択可能なセクションに分割します。

2. 領域の除外を定義するには、マウスの左ボタンを押しながら、プレビュー画像の必要なエリアをマウスのポインタでドラッグします。マウスを右クリックすると、グリッドで区切られた部分がクリアできます。

必要な数の除外領域を定義できます。除外領域は青色で表示されます:



青い除外領域は**モーション**タブのプレビュー画像にのみ表示されます。Management Clientやアクセスクライアントの他のプレビュー画像では青く表示されません。

デバイス - カメラ位置のプリセット

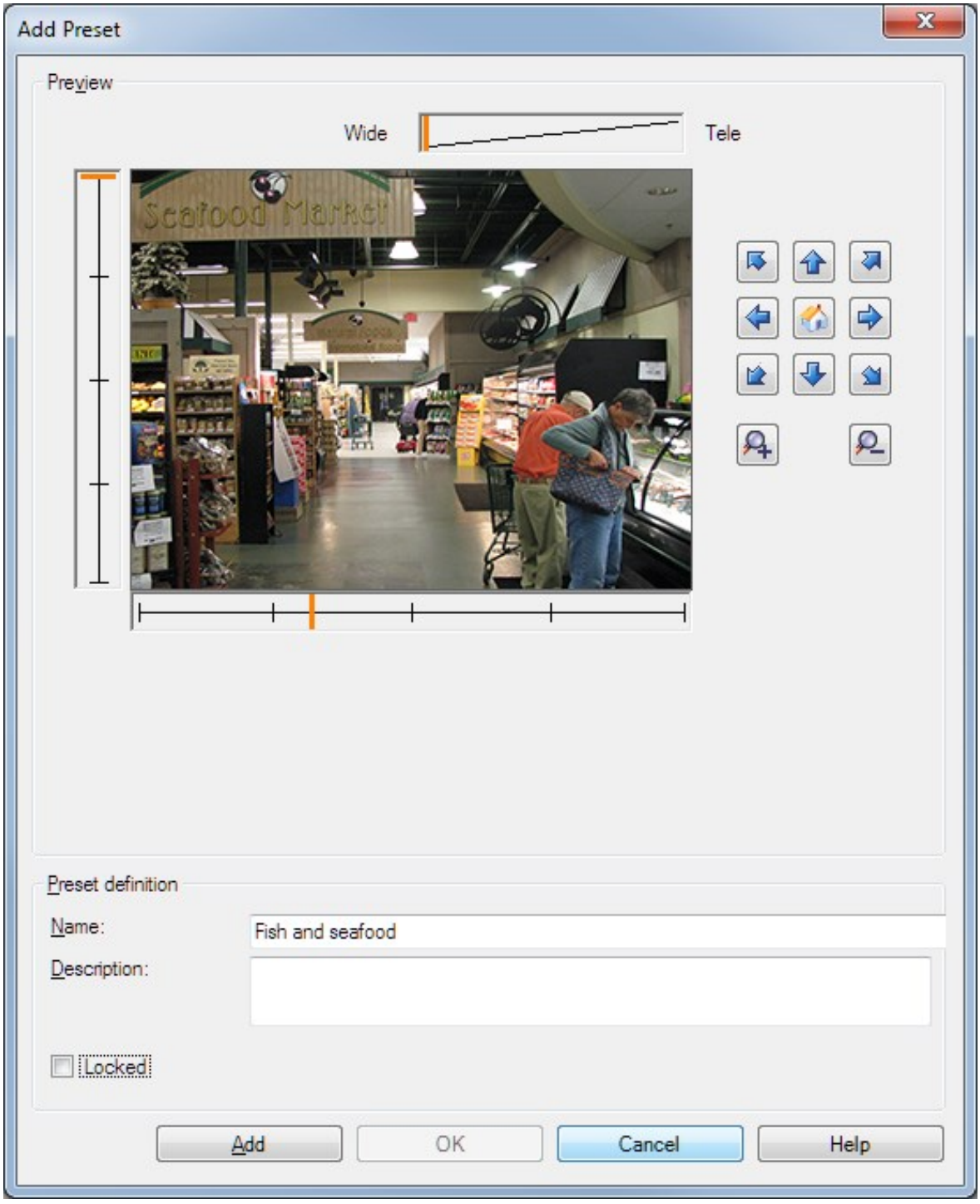
ホームプリセット位置

カメラのホームページで、カメラのホームプリセット位置を定義します。ホームページで利用できるPTZ機能は、カメラによって異なります。

プリセット位置を追加する(タイプ1)

プリセット位置をカメラに追加する方法

1. **サイトナビゲーション**ペインで、**デバイス**を選択し、**カメラ**を選択します。
2. **概要**ペインで該当するPTZカメラを選択します。
3. **プリセット**タブで**新規**をクリックします。**プリセットの追加**ウィンドウが表示されます。



4. **プリセットを追加**ウィンドウはカメラからのライブプレビュー画像を表示します。ナビゲーションボタンおよび/またはスライダーを使用してカメラを必要な位置に移動します。
5. **名前**フィールドにプリセット位置の名前を入力します。
6. オプションとして、**説明**フィールドにプリセット位置の説明を入力します。
7. プリセット位置をロックするには、**ロック**を選択します。十分な権限を持つユーザーのみ、後で位置のロックを解除できます。
8. **追加**をクリックしてプリセットを指定します。必要なプリセットが設定されるまで、追加を続けます。
9. **OK**をクリックします。**プリセットを追加**ウィンドウが閉じ、プリセット位置が**プリセット**タブのカメラの利用可能なプリセット位置のリストに追加されます。

カメラのプリセット位置を使用する(タイプ2)

プリセット位置をシステムに指定する代わりに、カメラでPTZカメラのプリセット位置を指定できます。通常は、デバイス固有の設定ウェブページにアクセスして定義します。

1. **サイトナビゲーション**ペインで、**デバイス**を選択し、**カメラ**を選択します。
2. **概要**ペインで該当するPTZカメラを選択します。
3. **プリセット**タブで**デバイスのプリセットを使用**を選択して、プリセットをシステムにインポートします。

   以前にカメラに定義したプリセットは削除され、定義済みのルールおよびパトロールスケジュールに影響します。また、XProtect Smart Clientユーザーが利用可能なプリセットは削除されます。
4. **削除**をクリックして、ユーザーにとって不要なプリセットを削除します。
5. プリセットの表示名を変更したい場合は、**編集**をクリックします(「プリセット位置の名前を変更(タイプ2のみ)」を参照)。
6. このようにデバイスで定義したプリセットを後で編集するには、カメラで編集してから再インポートします。

カメラのプリセット位置をデフォルトとして割り当てる

必要に応じて、PTZカメラのプリセット位置のいずれかをカメラのデフォルトのプリセット位置に割り当てることができます。

デフォルトのプリセット位置が設定されていると、PTZカメラを手動で操作した後など、特定の状況下でPTZカメラがデフォルトのプリセット位置に移動するように指定するようなルールを定義できるため便利です。

1. **サイトナビゲーション**ペインで、**デバイス**を選択し、**カメラ**を選択します。
2. **概要**ペインで該当するPTZカメラを選択します。
3. **プリセット**タブの**プリセット位置**で、定義済みのプリセット位置のリストからプリセットを選択します。
4. リストの下にある**デフォルトのプリセット**チェックボックスを選択します。

デフォルトのプリセット位置として指定できるのは、1つだけです。

オプション>**一般**で**PTZのホーム位置としてデフォルトのプリセットを使用する**を選択した場合、PTZカメラの定義済みのホーム位置の代わりにデフォルトのプリセット位置が使用されます。

PTZホーム位置としてデフォルトのプリセットを指定する

必要なユーザー権限があるManagement ClientおよびXProtect Smart Clientのユーザーは、クライアントの**ホーム**ボタンを押した際に、PTZカメラのホーム位置の代わりにデフォルトのプリセット位置を使用するようにシステムを設定することができます。

カメラにデフォルトのプリセット位置を定義する必要があります。デフォルトのプリセット位置が定義されていない場合、クライアントで**ホーム**ボタンを有効にしても何も起こりません。

PTZのホーム位置設定を有効にする

1. **ツール > オプション**を選択します。
2. **一般**タブの**レコーディングサーバー**グループで、**PTZのホーム位置としてデフォルトのプリセットを使用**を選択します。
3. プリセット位置をカメラのデフォルトプリセット位置として割り当てます。

デフォルトのプリセット位置を割り当てるには、233ページのカメラのプリセット位置をデフォルトとして割り当てるを参照してください

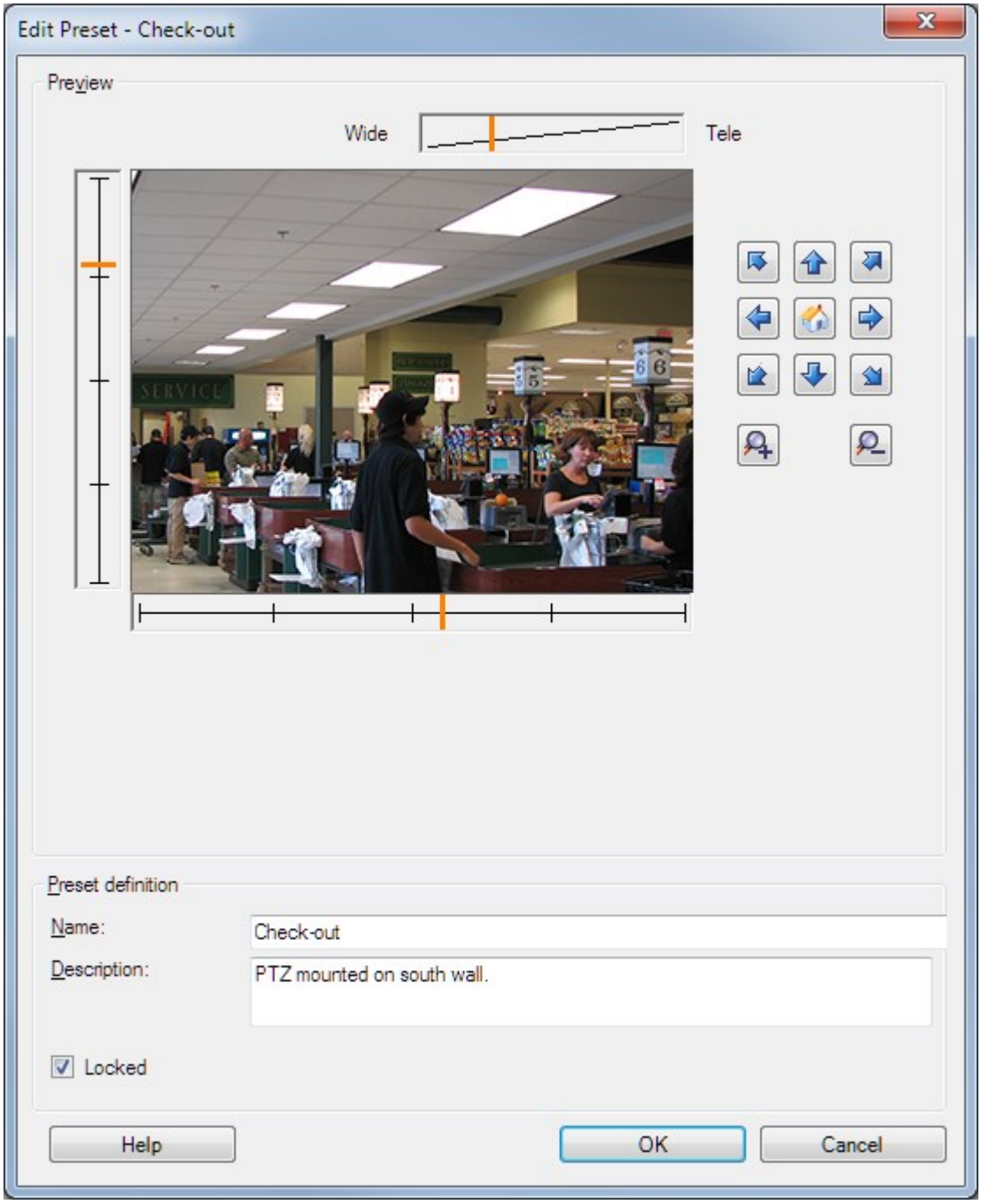
以下も参照：364ページのシステム設定（[オプション]ダイアログボックス）

カメラのプリセット位置を編集（タイプ1のみ）

システムで定義済みの既存のプリセット位置を編集する方法：

1. **[サイトナビゲーション]**ペインで、**[デバイス]**を選択してから**[カメラ]**を選択します。
2. **[概要]**ペインで該当するカメラを選択します。
3. **[プリセット]**タブの[プリセット位置]で、利用可能なプリセット位置のリストからプリセット位置を選択します。

4. **編集** をクリックします。これにより、**プリセットの編集** ウィンドウが開きます。



5. **[プリセットの編集]** ウィンドウにはプリセット位置からのライブビデオを表示します。ナビゲーションボタンおよび/またはスライダーを使用して、プリセット位置を必要に応じて変更します。

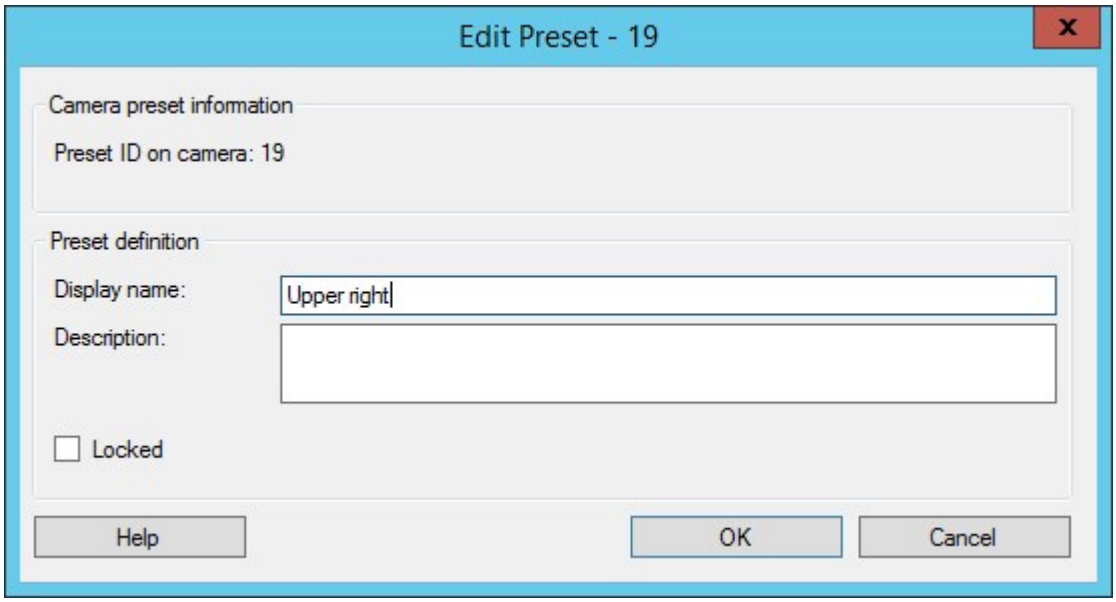
6. 必要に応じて、プリセット位置の名前/番号および説明を変更します。

7. プリセット位置をロックする場合は、**[ロック]**を選択します。十分な権限を持つユーザーのみ、後で位置のロックを解除できます。
8. **OK**をクリックします。

カメラのプリセット位置の名前を変更(タイプ2のみ)

カメラで定義されたプリセット位置の名前を編集するには:

1. **[サイトナビゲーション]**ペインで、**[デバイス]**を選択してから**[カメラ]**を選択します。
2. **[概要]**ペインで該当するPTZカメラを選択します。
3. プリセットタブのカメラで利用可能な**プリセット**のリストから、プリセット位置を選択します。
4. **編集**をクリックします。これにより、**プリセットの編集**ウィンドウが開きます。



5. 必要に応じて、プリセット位置の名前を変更し、説明を追加します。
6. プリセット名をロックする場合は、**ロック**を選択します。XProtect Smart Clientのユーザー、またはセキュリティ権限が制限されたユーザーによるプリセット名の更新またはプリセットの削除を防止するため、プリセット名をロックできます。ロックされたプリセットには アイコンが表示されます。十分な権限を持つユーザーのみ、後でプリセット名のロックを解除できます。
7. **OK**をクリックします。

プリセット位置をテストする(タイプ1のみ)

1. **サイトナビゲーション**ペインで、**デバイス**を選択し、**カメラ**を選択します。
2. **概要**ペインで該当するPTZカメラを選択します。
3. **プリセット**タブのカメラで利用可能なプリセット位置のリストから、プリセット位置を選択します。

4. **実行**をクリックします。
5. カメラが選択されたプリセット位置に移動します。

デバイス - パトロール

パトロール設定と手動パトロール(説明付き)

パトロール設定では、パトロールの実行方法を定義します。これには、カメラがプリセット位置間を移動する順序や、カメラが各位置に停止する時間が含まれます。作成できるパトロール設定の数に制限はなく、作成したパトロール設定はルールで使用できます。例えば、1つのパトロール設定が日中の営業時間中に使用され、別のプロファイルが夜間に使用されるように指定するルールを作成できます。

手動パトロール

たとえば、ルールでパトロール設定を適用する場合は、手動パトロールでパトロール設定をテストできます。PTZ優先度が高い場合は、手動パトロールを使用して、別のユーザーまたはルールによって有効にされたパトロールからパトロールを取得することもできます。

カメラがすでにパトロール中であるか、別のユーザーによって制御されている場合は、自分の優先度が高い場合にのみ手動パトロールを開始できます。

カメラがルールでアクティブ化されたシステムパトロールを実行している間に手動パトロールを開始する場合は、手動パトロールを停止するときにこのパトロールを再開します。別のユーザーが手動パトロールを実行しているときに、自分の優先度が高く、手動パトロールを開始すると、他のユーザーの手動パトロールは再開されません。

手動パトロールを自分で停止しない場合は、より高い優先度のルールに基づくパトロールまたはユーザーに取得されるまで継続します。ルールに基づくシステムパトロールが停止すると、システムは手動パトロールを再開します。別のユーザーが手動パトロールを開始すると、自分の手動パトロールが停止し、再開されません。

パトロール設定の終了位置が定義されている場合、手動パトロールを停止すると、カメラがこの位置に戻ります。

パトロール設定の追加

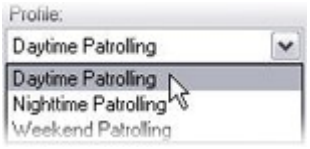
> パトロール設定を開始する前に、**プリセット**タブでカメラに対して少なくとも2つのプリセット位置を指定する必要があります。「プリセット位置を追加(タイプ1)」を参照してください。

1. **サイトナビゲーション**ペインで、**デバイス**を選択し、**カメラ**を選択します。
2. **概要**ペインで該当するPTZカメラを選択します。
3. **パトロール**タブで**追加**をクリックします。**プロファイルを追加**ダイアログボックスが表示されます。
4. **プロファイルを追加**ダイアログボックスで、パトロール設定の名前を入力します。
5. **OK**をクリックします。名前が一意ではない場合は、ボタンは無効です。

新しいパトロール設定が**プロファイル**リストに追加されました。これで、プリセット位置とパトロール設定の他の設定を指定できます。

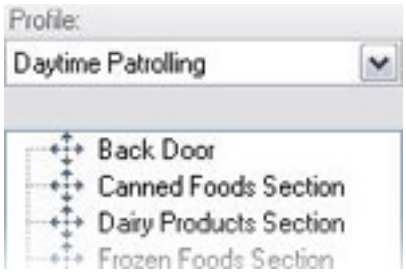
パトロール設定でのプリセット位置の指定

1. **[サイトナビゲーション]**ペインで、**[デバイス]**を選択してから**[カメラ]**を選択します。
2. **[概要]**ペインで該当するPTZカメラを選択します。
3. **[パトロール]**タブの**[プロファイル]**リストで、パトロール設定を選択します:



4. **[追加]** をクリックします。
5. **[PTZプリセットの選択]**ダイアログボックスで、パトロール設定のプリセット位置を選択します:

6. **OK** をクリックします。選択されたプリセット位置は、パトロール設定のプリセット位置のリストに追加されます。



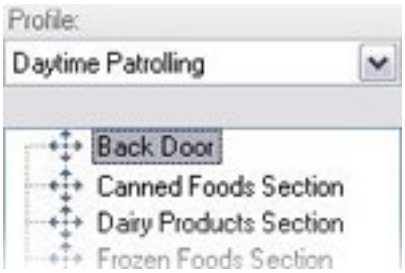
7. カメラはリストの最上位のプリセット位置を、カメラがパトロール設定に従ってパトロールを行うときの最初の停止位置として使用します。上から2番目のプリセット位置は、2番目の停止位置というようになっています。

各プリセット位置での時間を指定

パトロール時に、PTZカメラはパトロール設定で指定された各プリセット位置にデフォルトでは5秒間とどまります。

秒数を変更するには、以下を実行します。

1. **サイトナビゲーション**ペインで、**デバイス**を選択し、**カメラ**を選択します。
2. **概要**ペインで該当するPTZカメラを選択します。
3. **パトロール**タブの**プロファイル**リストで、パトロール設定を選択します。
4. 時間を変更したいプリセット位置を選択します。



5. **位置時間(秒)**フィールドに任意の時間を入力します。
6. 必要に応じて、他のプリセット位置でも繰り返します。

旋回動作(PTZ)をカスタマイズ

デフォルトでは、あるプリセット位置から別の位置に移動するために必要な時間(**旋回動作**)は3秒であると推定されています。カメラがプリセット位置間を移動するときに、関係のないモーションが検知される可能性が高いため、デフォルトでは、この期間のカメラのモーション検知が無効になっています。

カメラがPTZスキャンに対応し、設定されたプリセット位置がシステムのサーバーに保存されるタイプのカメラ(タイプ1 PTZカメラ)でのみ、旋回動作の速度をカスタマイズできます。それ以外のカメラでは、**スピード**スライダがグレイ表示になります。

以下をカスタマイズできます。

- 推定旋回動作時間
- カメラが旋回動作中に移動するスピード

異なるプリセット位置での旋回動作をカスタマイズする方法:

1. **[サイトナビゲーション]**ペインで、**[デバイス]**を選択してから**[カメラ]**を選択します。
2. **[概要]**ペインで該当するPTZカメラを選択します。
3. **[パトロール]**タブの**[プロファイル]**リストで、パトロール設定を選択します。
4. **旋回動作をカスタマイズ**チェックボックスを選択します。

旋回動作表示がプリセット位置のリストに追加されます。

5. リストで、旋回動作を選択します。

6. **[予想時間(秒)]**フィールドに推定旋回動作時間(秒)を入力します。

7. **スピード**スライダを使用して、旋回動作スピードを指定します。スライダが右端の位置に来ると、カメラはデフォルトのスピードで移動します。スライダを左に移動するほど、選択した旋回動作中のカメラの移動スピードが低下します。

8. 必要に応じて、他の旋回動作でも同じ操作を繰り返します。

パトロール中に終了位置を指定

選択したパトロール設定に基づくパトロールが終了した時点で、カメラを特定のプリセット位置に移動するように指定することができます。

1. **[サイトナビゲーション]**ペインで、**[デバイス]**を選択してから**[カメラ]**を選択します。
2. **[概要]**ペインで該当するPTZカメラを選択します。
3. **[パトロール]**タブの**[プロファイル]**リストで、該当するパトロール設定を選択します。
4. **[終了時に特定の位置に移動]**チェックボックスを選択します。これにより、**プリセットの選択**ダイアログボックスが開きます。
5. 終了位置を選択し、**[OK]**をクリックします。

> 任意のカメラのプリセット位置を終了位置として指定できます。パトロール設定で使用するプリセット位置に制限はありません。

6. 選択された終了位置がプロファイルリストに追加されます。

選択されたパトロール設定に基づくパトロールが終了した時点で、カメラは指定された終了位置に移動します。

PTZセッションの予約およびリリース

監視システムによっては、PTZセッションを予約できます。

予約されたPTZセッションを実行するセキュリティ権限を持つ管理者は、このモードでPTZカメラを実行できます。これにより、他のユーザーはカメラを制御できなくなります。予約済みPTZセッションでは、標準PTZ優先度システムが無視され、より高いPTZ優先度のユーザーがセッションを中断しないようになります。

XProtect Smart ClientとManagement Clientの両方から予約済みPTZセッションでカメラを操作できます。

PTZセッションの予約は、他のユーザーによって中断されずに、PTZカメラまたはそのプリセットで緊急の更新またはメンテナンスを行う必要がある場合に有効です。

PTZセッションの予約

1. **[サイトナビゲーション]**ペインで、**[デバイス]**を選択してから**[カメラ]**を選択します。
2. **[概要]**ペインで該当するPTZカメラを選択します。
3. **[プリセット]**タブでPTZセッションを選択し、**[予約済み]**をクリックします。

> 自分よりも高い優先度のユーザーがカメラを制御している場合や、別のユーザーがすでにカメラを予約している場合は、予約済みPTZセッションを開始できません。

PTZセッションのリリース

[リリース]ボタンを使用すると、他のユーザーがカメラを制御できるように、現在のPTZセッションをリリースできます。**[リリース]**をクリックすると、PTZセッションがただちに終了し、最初のユーザーがカメラを操作できます。

セキュリティ権限 **[PTZセッションのリリース]** が割り当てられている管理者には、いつでも他のユーザーの予約されたPTZセッションをリリースする権限があります。たとえば、PTZカメラまたはプリセットを維持する必要がある場合や、他のユーザーが誤って緊急の状況でカメラをブロックした場合などに有用です。

PTZセッションタイムアウトの指定

Management Client および必要なユーザー権限を持つXProtect Smart Clientユーザーは、PTZカメラのパトロールを手動で中断できます。

定期パトロールがシステム上のすべてのPTZカメラで再開される前に経過する時間を指定できます。

1. **[ツール]>[オプション]**を選択します。
2. **[オプション]**ウィンドウの**[全般]**タブの次の場所で時間を選択します。
   - **手動PTZセッションのタイムアウト**リスト(デフォルトは15秒)。
   - **パトロールセッションを一時停止するタイムアウト**リスト(デフォルトは10分)。
   - **予約されたPTZセッションのタイムアウト**リスト(デフォルトは1時間)。

   この設定は、システムのPTZカメラすべてに適用されます。

各カメラのタイムアウトは個別に変更できます。

1. **[サイトナビゲーション]**ペインで、**[カメラ]**をクリックします。
2. 概要ペインで、カメラを選択します。
3. **[プリセット]**タブの次の場所で時間を選択します。
   - **手動PTZセッションのタイムアウト**リスト(デフォルトは15秒)。
   - **パトロールセッションを一時停止するタイムアウト**リスト(デフォルトは10分)。
   - **予約されたPTZセッションのタイムアウト**リスト(デフォルトは1時間)。

   設定はこのカメラにのみ適用されます。

デバイス - ルールのイベント

デバイスのイベントを追加または削除する

イベントの追加

1. **概要**ペインで、デバイスを選択します。
2. **イベント**タブを選択し、**追加**をクリックします。この操作で**ドライバーイベントの選択**ウィンドウが開きます。
3. イベントを選択します。一度に選択できるイベントは1つのみです。
4. すでに追加されたイベントを再び追加できるよう、全イベントの全リストを表示したい場合は、**すでに追加されたイベントを表示**を選択します。
5. **OK**をクリックします。
6. ツールバーで**保存**をクリックします。

イベントの削除

イベントを削除すると、イベントを使用するすべてのルールに影響を与えます。

1. **概要**ペインで、デバイスを選択します。
2. **イベント**タブを選択し、**削除**をクリックします。

イベントプロパティの指定

追加したイベントごとにプロパティを指定できます。プロパティの数は、デバイスとイベントによって異なります。イベントが意図したとおりに機能するようにするには、デバイスと**イベント**タブで、一部またはすべてのプロパティを同じように設定する必要があります。

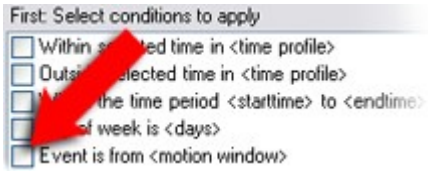
1つのイベントに複数のインスタンスを使用する

1つのイベントに複数のインスタンスでの異なるプロパティを指定できるようにするために、複数のイベントを追加できます。

以下の例は、カメラに固有です。

例：2つのモーションウィンドウ(A1とA2) があるカメラを設定しました。モーション開始(ハードウェア) イベントの2つのインスタンスを追加しました。1つのインスタンスのプロパティで、モーションウィンドウA1の使用を指定しました。もう1つのインスタンスのプロパティで、モーションウィンドウA2の使用を指定しました。

ルールでイベントを使用する場合、イベントはルールをトリガーするための特定のモーションウィンドウで検知されたモーションに基づくように指定できます。



デバイス - プライバシーマスク

プライバシーマスクの有効化/無効化

プライバシーマスク機能は、デフォルトで無効になっています。

カメラのプライバシーマスク機能を有効化/無効化する方法

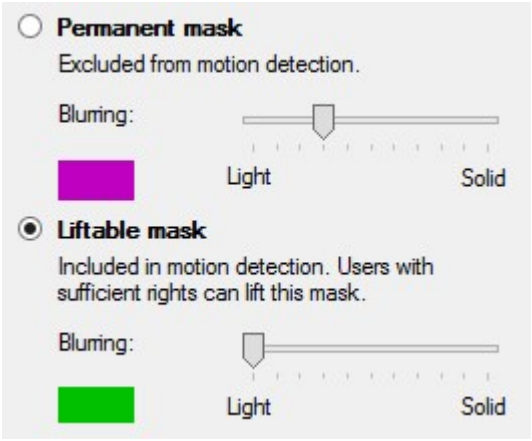
1. **サイトナビゲーション**ペインで**デバイス**を選択します。
2. **概要**ペインで関連するカメラデバイスを選択します。
3. **プライバシーマスク**タブで、**プライバシーマスク**チェックボックスを選択または選択解除します。

Milestone Interconnect設定では、中央サイトは、リモートサイトで定義されたプライバシーマスクを無視します。同じプライバシーマスクを適用するには、中央サイトで再定義する必要があります。

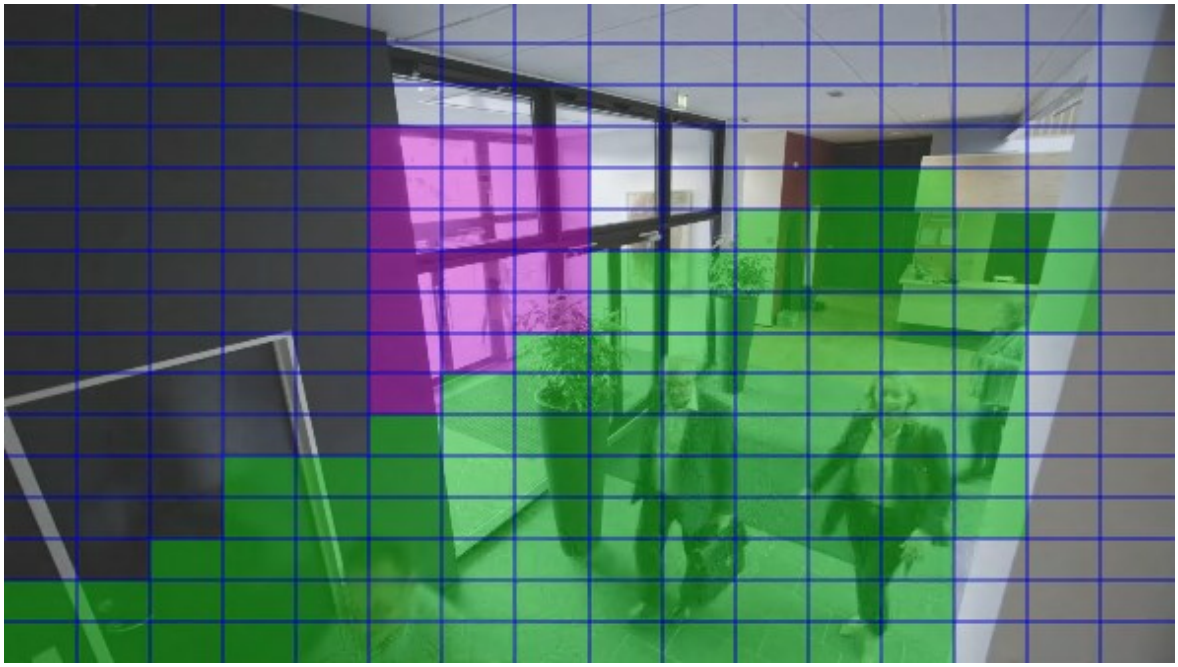
プライバシーマスクを定義する

プライバシーマスクタブで**プライバシーマスク**機能を有効化すると、カメラプレビューにグリッドが適応されます。

1. **[サイトナビゲーション]**ペインで**[デバイス]**を選択します。
2. **[概要]**ペインで該当するカメラを選択します。
3. **[プライバシーマスク]**タブでエリアにプライバシーマスクをかけるには、最初に**[常設のマスク]**または**[除去可能なマスク]**を選択して、常設または除去可能なプライバシーマスクのいずれを適用するかを指定します。



4. マウスをプレビューの上でドラッグします。左クリックして、グリッドセルを選択します。右クリックして、グリッドセルを消去します。
5. 必要な数のプライバシーマスク領域を定義できます。常設のプライバシーマスクを持つ領域は、紫で表示され、除去可能なプライバシーマスクの領域は緑で表示されます。



6. クライアントに見せられる時に、ビデオにおいてカバーされた領域がどのように表示されるかを定義します。簡易的なぼやけたマスクから、完全な不透明のマスクに変更するには、スライダーを使用します。

   常設のプライバシーマスクは、**モーション**タブにも表示されます。

7. XProtect Smart Clientで、プライバシーマスクが、定義した通りに表示されていることを確認してください。

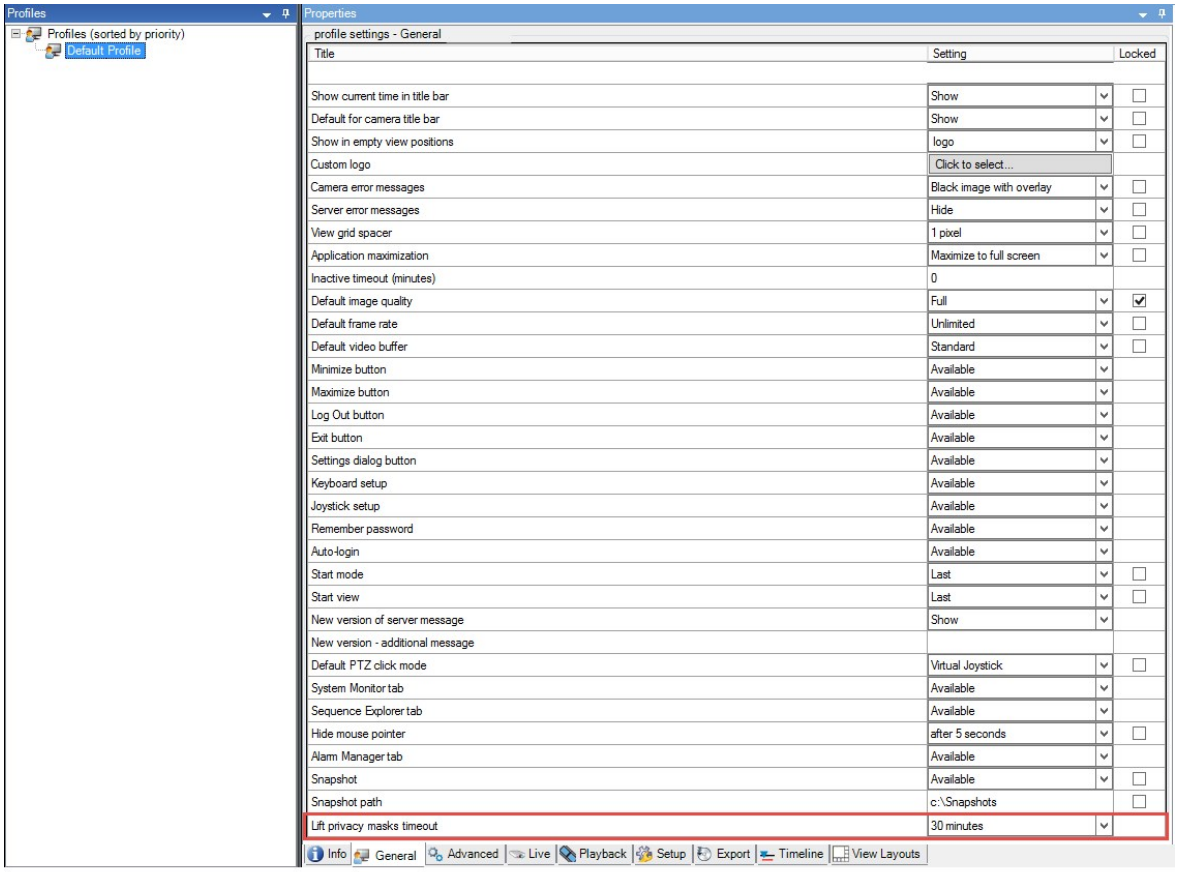
除去されたプライバシーマスクのタイムアウトを変更する

デフォルト設定では、プライバシーマスクはXProtect Smart Clientで30分間除去され、その後は自動的に適用されます。しかし、この設定は変更可能です。

タイムアウトを変更する場合は、その目的が、プライバシーマスク除去の権限を持つ役割と関連するSmart Clientプロファイルのためであることに留意してください。

タイムアウトを変更するには、以下を実行します。

1. **Smart Clientプロファイル**の下で、関連するSmart Clientプロファイルを選択します。
2. **一般**で、**プライバシーマスク除去タイムアウト**を見つけます。



3. 以下の値のいずれかを選択します。
   - **2分**
   - **10分**
   - **30分**
   - **1時間**
   - **2時間**
   - **ログアウトするまで**
4. **保存**をクリックします。

プライバシーマスクの除去権限をユーザーに付与する

デフォルトでは、XProtect Smart Clientにおいていかなるユーザーもプライバシーマスクの除去権限は持っていません。

権限を有効化/無効化するには、以下を実行します。

1. **サイトナビゲーション**ペインで、**セキュリティ**を選択し、**役割**を選択します。
2. プライバシーマスク除去権限を付与したい役割を選択します。
3. **セキュリティ全般**タブで、**カメラ**を選択します。
4. **プライバシーマスク除去**権限を付与するには、**許可**チェックボックスを選択します。

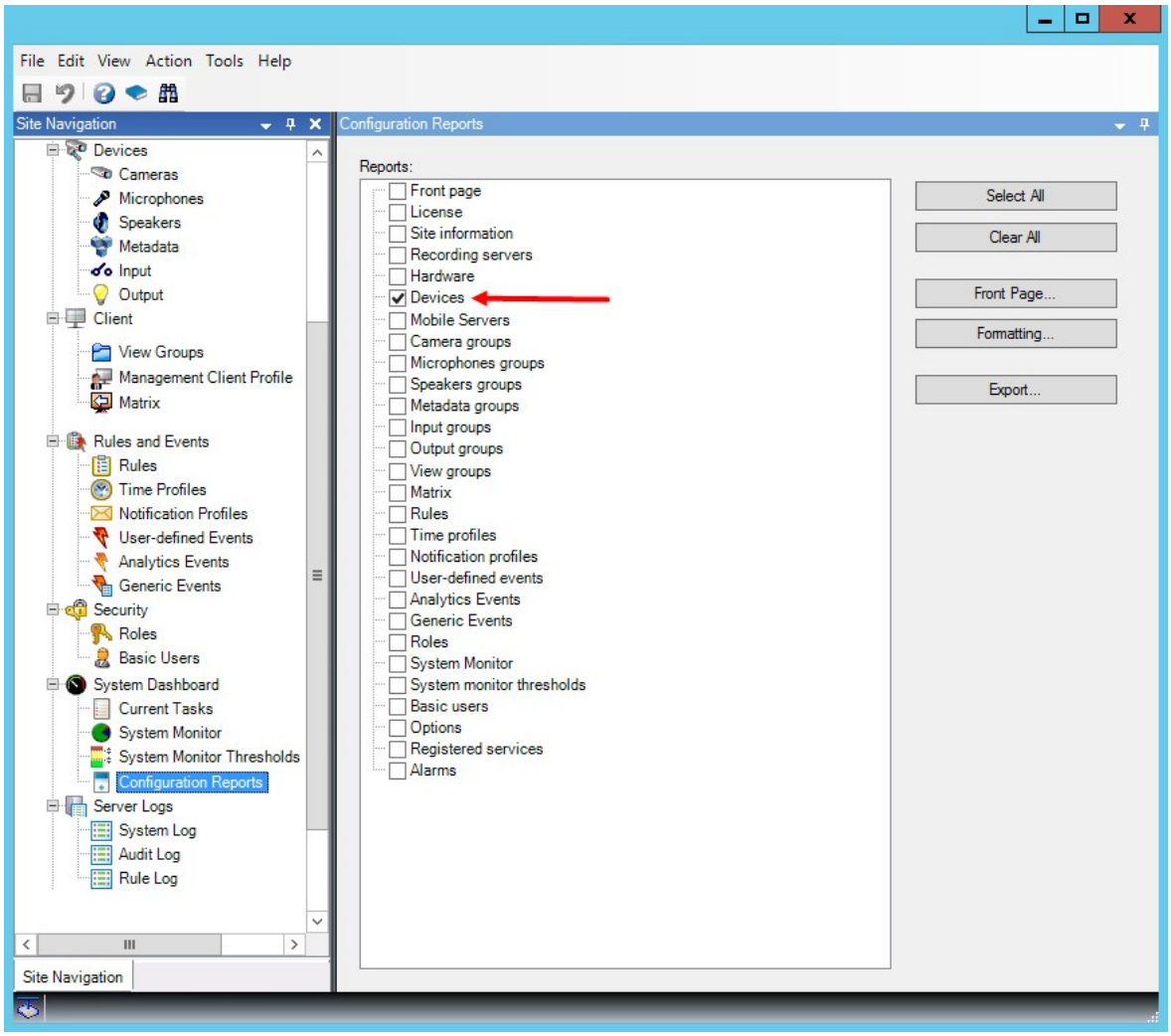
この役割を割り当てられたユーザーは、自分でプライバシーマスクを除去可能なように設定したり、他のXProtect Smart Clientユーザーに除去の権限を付与することができます。

プライバシーマスク設定のレポートを作成します

デバイスレポートは、お使いのカメラの現行のプライバシーマスク設定に関する情報を含んでいます。

レポートを構成するには：

1. **[サイトナビゲーション]**ペインで**[システムダッシュボード]**を選択します。
2. **構成レポート**の下で、**デバイス**レポートを選択します。



3. もしレポートを変更したい場合は、フロントページとフォーマットを変更します。
4. **エクスポート**をクリックすると、システムがレポートをPDFファイルで作成します。

レポートの詳細については、「282ページのシステム構成が記されたレポートを印刷」を参照してください。

クライアント

グループの表示(説明付き)

クライアントでシステムが1つ以上のカメラからのビデオを表示する方法はビューと呼ばれます。ビューグループは、このようなビューの1つ以上の論理グループのコンテナです。クライアントでは、ビューグループは展開可能なフォルダーとして表示されます。ユーザーはこのフォルダーからグループを選択し、表示するビューを選択できます。

XProtect Smart Clientの例:矢印はビューグループを示します。ビューグループには論理グループ(アメニティと呼ばれます)が含まれ、これには3つのビューが含まれます。

デフォルトでは、Management Clientで定義する各役割は、ビューグループとしても作成されます。Management Clientに役割を追加すると、デフォルトで、役割がクライアントで使用できるビューグループとして表示されます。

- ビューグループを役割に基づいて、関連する役割に割り当てられたユーザー/グループに割り当てられます。これらのビューグループの設定は、後で役割にアクセスして設定することで変更できます。
- 役割に基づくビューグループには、役割の名前が付けられます。

  例:Building A Security Staffという名前の役割を作成すると、**Building A Security Staff**という名前のビューグループとして、XProtect Smart Clientに表示されます。

  役割を追加する際に取得するビューグループに加え、必要に応じて他のビューグループも作成できます。また、役割を追加する際に自動的に作成されるビューグループに含まれるビューグループは削除もできます。
- 役割を追加するたびにビューグループが作成されますが、ビューグループは役割に対応する必要はありません。必要に応じてビューグループを追加、名前変更、削除できます。

ビューグループの名前を変更した場合、変更した名前を表示するには、すでに接続済みのクライアントユーザーは一旦ログアウトしてから再度ログインする必要があります。

ビューグループの追加

1. **ビューグループ**を右クリックして、**ビューグループを追加**を選択します。**ビューグループを追加**ダイアログボックスが開きます。
2. 新規ビューグループの名前と、任意で説明を入力し、**OK**をクリックします。

権限を指定しない限り、新規追加されたビューグループを使用できる役割はありません。新規追加されたビューグループを使用できる役割を指定した場合、該当する役割を持つすでに接続されてるクライアントのユーザーがビューグループを表示するには、一旦ログアウトし、ログインし直す必要があります。

Smart Client profiles

Smart Clientプロファイルの追加と設定

まずSmart Clientプロファイルを作成してから、設定する必要があります。

1. **プロファイルSmart Client**を右クリックします。
2. **プロファイル**の追加Smart Clientを選択します。
3. **Smart Clientプロファイルの追加**ダイアログで、新しいプロファイルの名前と説明を入力し、**OK**をクリックします。
4. **概要**ペインで、作成したプロファイルをクリックして設定します。
5. 1つまたは複数、あるいは利用可能なすべてのタブで**OK**をクリックします。

Smart Clientプロファイルのコピー

設定や権限が複雑なSmart Clientプロファイルがあり、同様のプロファイルが必要な場合、新しいプロファイルをゼロから作成するよりも、既存のプロファイルをコピーし、コピーしたプロファイルを微調整する方が簡単な場合があります。

1. **Smart Clientプロファイル**をクリックし、**概要**ペインのプロファイルを右クリックして**Smart Clientプロファイルのコピー**を選択します。
2. ダイアログボックスが表示されたら、コピーしたプロファイルの新しい一意の名前と説明を入力します。**OK**をクリックします。
3. **概要**ペインで、作成したプロファイルをクリックして設定します。この操作を行うには、利用できる1つ、または複数、もしくはすべてのタブで設定を調整します。**OK**をクリックします。

Smart Clientプロファイル、役割、時間プロファイルの作成と設定

Smart Clientプロファイルで作業するときには、Smart Clientプロファイル、役割、時間プロファイルの間の関連性を理解しておくことが重要です。

- Smart Clientプロファイル - 対象の場所でユーザー権限の設定を処理するプロファイル - 対象の場所：XProtect Smart Client
- クライアント、MIP SDKなどでセキュリティの設定を処理する役割
- 時間プロファイルはこの2つのプロファイルタイプの時間的側面を処理します

これらの3つの機能を連携させることで、XProtect Smart Clientのユーザー権限に関して、独自の制御やカスタマイズを行うことができます。

例：XProtectSmartClientの設定で、通常の業務時間(午前8時 ~ 午後4時)に限り、選択したカメラからライブビデオを表示することのみが許可された(再生は不可)ユーザーを設定する必要があるとします。この場合、次の方法で設定が可能です。

1. Smart Clientプロファイルを作成し、例えば**ライブ専用**などの名前を付けます。
2. **ライブ専用**に必要なライブまたは再生設定を指定します。
3. 時間プロファイルを作成し、例えば**日中専用**などの名前を付けます。
4. **日中専用**に必要な期間を指定します。
5. 新規役割を作成し、例えば**警備(選択したカメラ)**などの名前を付けます。
6. **警備(選択したカメラ)**が使用できるカメラを指定します。
7. **[ライブ専用]** Smart Clientプロファイルと**[日中専用]**時間プロファイルを**[警備(選択したカメラ)]**の役割に割り当て、3つの要素をリンクさせます。

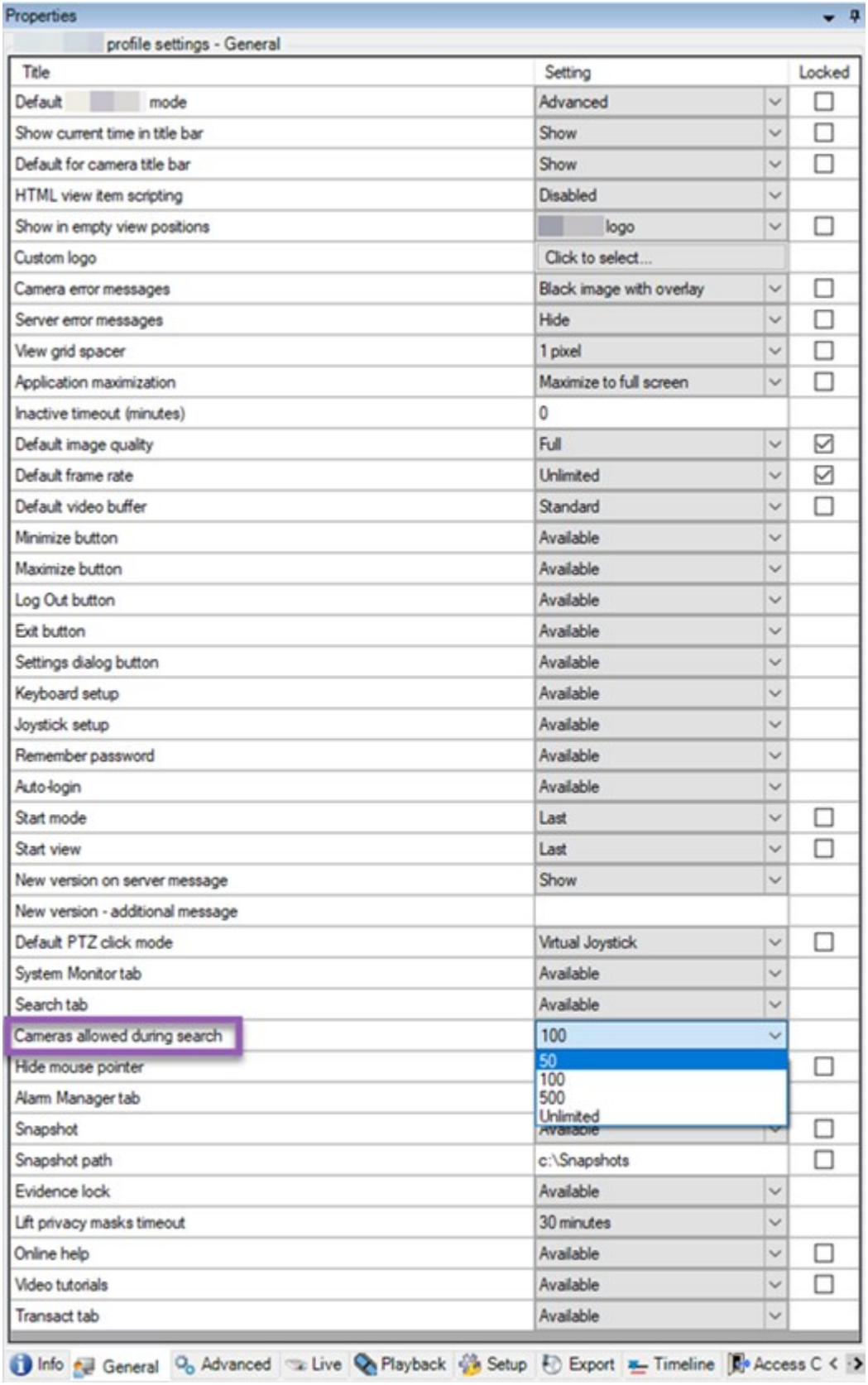
これで、3つの機能が統合され、必要な結果を作成し、簡単に微調整および調節ができるようになりました。さらに、役割を最初に作成して、次にSmart Clientプロファイルおよび時間プロファイルを作成するなど、上記とは異なる順序を含め、その他の任意の順序で設定することができます。

検索中に許可されるカメラの数を設定

XProtect Smart Clientでオペレータが検索に追加できるカメラの数を設定できます。デフォルトは**100**台です。カメラの上限を超えると、警告が表示されます。

1. XProtect Management Clientで、**クライアント > Smart Clientプロファイル**を展開します。
2. 関連するプロファイルを選択します。

3. **全般**タブをクリックします。


Properties
profile settings - General
Title
Setting
Locked
Default mode
Advanced
Show current time in title bar
Show
Default for camera title bar
Show
HTML view item scripting
Disabled
Show in empty view positions
logo
Custom logo
Click to select...
Camera error messages
Black image with overlay
Server error messages
Hide
View grid spacer
1 pixel
Application maximization
Maximize to full screen
Inactive timeout (minutes)
0
Default image quality
Full
Default frame rate
Unlimited
Default video buffer
Standard
Minimize button
Available
Maximize button
Available
Log Out button
Available
Exit button
Available
Settings dialog button
Available
Keyboard setup
Available
Joystick setup
Available
Remember password
Available
Auto-login
Available
Start mode
Last
Start view
Last
New version on server message
Show
New version - additional message
Default PTZ click mode
Virtual Joystick
System Monitor tab
Available
Search tab
Available
Cameras allowed during search
100
50
100
500
Unlimited
Hide mouse pointer
Alarm Manager tab
Snapshot
Snapshot path
c:\Snapshots
Evidence lock
Available
Lift privacy masks timeout
30 minutes
Online help
Available
Video tutorials
Available
Transact tab
Available
Info
General
Advanced
Live
Playback
Setup
Export
Timeline
Access C

4. 検索中に許可されている**カメラ**で、以下の値のいずれかを選択します:
    - **50**
    - **100**
    - **500**
    - **無制限**
5. 変更を保存します。

デフォルトのエクスポート設定を変更する

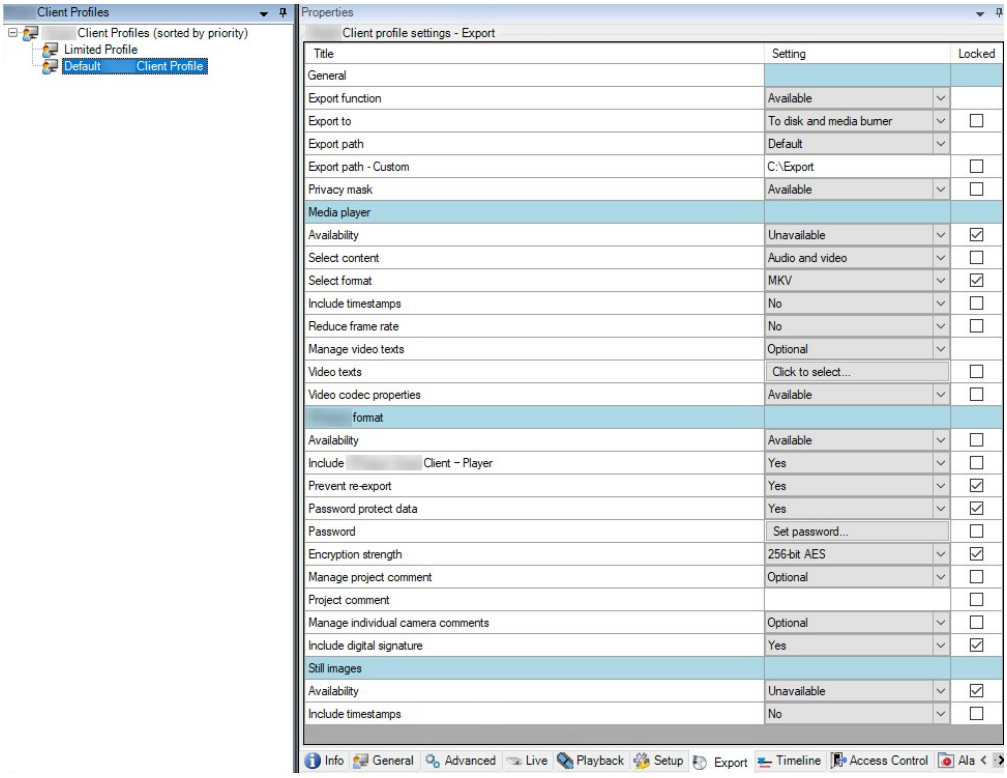
XProtectVMSシステムをインストールすると、最高レベルのセキュリティを確保するために、XProtect Smart Clientエクスポートオプションを定義するデフォルトのエクスポート設定が制限されます。これらの設定を変更して、オペレータにより多くのオプションを与えることができます。

デフォルト設定

- XProtect形式のみ利用できます
    - 再エクスポートが防止されます
    - エクスポートはパスワードで保護されています
    - 256ビットAES暗号化
    - デジタル署名が追加されます
- MKV形式またはAVI形式にエクスポートすることはできません
- 静止画をエクスポートできません

手順:

1. XProtect Management Clientで、**クライアント > Smart Clientプロファイル**を展開します。
2. **デフォルトSmart Clientプロファイル**を選択します。
3. **プロファイル**ペインで、**エクスポート**タブを選択します。



4. XProtect Smart Clientで利用可能な形式を制限するには、設定を見つけ、**利用可能**を選択します。
5. オペレータがXProtect Smart Clientの設定を変更できるようにするには、関連する設定の横にある**ロック**チェックボックスをオフにします。
6. 必要に応じて、他の設定を変更します。
7. (オプション) XProtect Smart Clientにログインして、設定が適用されていることを確認します。

Management Client profiles

Management Clientプロファイルの追加と設定

既定のプロファイルを使用したくない場合は、Management Clientプロファイルを作成してから設定します。

1. **プロファイルManagement Client**を右クリックします。
2. **プロファイル**の追加Management Clientを選択します。

3. **Management Clientプロファイルの追加**ダイアログで、新しいプロファイルの名前と説明を入力し、**OK**をクリックします。
4. **概要**ペインで、作成したプロファイルをクリックして設定します。
5. **プロファイル**タブで、Management Clientプロファイルの機能を選択または選択解除します。

Management Clientプロファイルのコピー

再利用したい設定を持つManagement Clientプロファイルがあれば、すでに存在しているプロファイルをコピーし、新しいプロファイルを最初から作成する代わりに、このコピーに少し修正を加えて作成できます。

1. **Management Clientプロファイル**をクリックし、**概要**ペインのプロファイルを右クリックして、**プロファイルManagement Clientのコピー**を選択します。
2. ダイアログボックスが表示されたら、コピーしたプロファイルの新しい一意の名前と説明を入力します。**OK**をクリックします。
3. **概要**ペインで、プロファイルをクリックし、**情報**タブまたは**プロファイル**タブへ移動して、プロファイルを設定します。

Management Clientプロファイルの機能表示の管理

Management Clientプロファイルを役割と関連付け、それぞれの管理者役割で使用できる機能が表示されるように、ユーザーインターフェースを制限します。

Management Clientプロファイルを役割に関連付ける

1. **[セキュリティ]**ノードを展開し、**[役割]**をクリックします。
2. **役割の設定**ウィンドウの**情報**タブで、プロファイルを役割に関連付けます。詳細については、情報タブ(役割)を参照してください。

役割に関するシステム機能への全体的なアクセスの管理

Management Clientプロファイルは、実際のアクセスではなく、システム機能の視覚的な表示のみに対応します。

役割に関するシステム機能への全体的なアクセスを管理するには:

1. **セキュリティ]**ノードを展開し、**[役割]**をクリックします。
2. **[セキュリティ全般]**タブをクリックして、適切なチェックボックスを選択します。詳細については、「479ページのセキュリティ全般タブ(役割)」を参照してください。

> すべての役割にManagement Serverへのアクセス権を付与するため、**[セキュリティ全般]**タブで、**[接続]**セキュリティ権限を有効に設定します。

定義済みの管理者の役割を除き、**[全般セキュリティ]**タブでマネジメントサーバーの**セキュリティの管理**権限を割り当てられた役割に関連付けられたユーザーのみが、Management Clientプロファイルを追加、編集、および削除できます。

プロファイルの機能表示の制限

すべてのManagement Client要素の表示について、設定を変更できます。デフォルトでは、Management Clientプロファイルはすべての機能をManagement Clientで表示できます。

1. クライアントノードを展開して、Management Clientプロファイルをクリックします。
2. プロファイルを選択して、プロファイルタブをクリックします。
3. このManagement Clientプロファイルに関係する役割を有するすべてのManagement Clientユーザーに対して、Management Clientからの機能表示を削除するために、関連する機能のチェックボックスを選択解除します。

Matrix

MatrixおよびMatrix受信者(説明付き)

Matrixはビデオのリモート配信機能です。

Matrix受信者とは、XProtect Smart Clientを搭載したコンピュータを指します。これは、Management ClientでMatrixとして定義されています。

Matrixを使用すれば、システムのネットワーク上のあらゆるカメラから、稼働中のあらゆるMatrix受信者にビデオをプッシュ配信できます。

Management Clientで追加されたMatrix受信者リストを表示するには、**サイトナビゲーション**ペインで**クライアント**を展開してから、**Matrix**を選択します。Matrix設定のリストが**プロパティ**ペインに表示されます。

Management Clientでは、Matrix受信者をそれぞれ追加しない限り、Matrixによってトリガーされたビデオを受信することはできません。

ビデオをMatrix受信者へ送信するためのルールを定義

Matrix受信者にビデオを送信するには、関連するMatrix受信者へのビデオ転送をトリガーするルールにMatrix受信者を含める必要があります。以下を実行します。

1. **サイトナビゲーション**ペインで、**ルールとイベント**を展開し、**ルール**を選択します。**ルール**を右クリックし、**ルールの管理**ウィザードを開きます。ステップ1でルールタイプを選択し、ステップ2で条件を選択します。
2. **ルールの管理**のステップ3(**手順3: アクション**)で、**設定Matrixを選択して<デバイス>**アクションを表示します。

3. 初期ルール説明のMatrixリンクをクリックします。
4. **設定のMatrix選択**ダイアログボックスで、関連するMatrix受信者を選択し、**OK**をクリックします。
5. 初期ルール説明の**デバイス**リンクをクリックし、Matrix受信者にビデオを送信するカメラを選択して、**OK**をクリックして選択を確定します。
6. ルールを入力して**終了**をクリックするか、必要に応じて別のアクションまたは終了アクションを定義します。

Matrix受信者を削除すると、Matrix受信者を含めるすべてのルールが停止します。

Matrix受信者の追加

Matrixで既存のManagement Client受信者を追加するには、以下を実行します。

1. **クライアント**を展開し、**Matrix**を選択します。
2. **Matrix設定**を右クリックして、**Matrixを追加**を選択します。
3. **Matrixを追加**ダイアログボックスのフィールドに入力します。
    1. **アドレス**フィールドに、目的のMatrix受信者のIPアドレスまたはホスト名を入力します。
    2. **ポート**フィールドに、Matrix受信者のインストールで使用するポート番号を入力します。
4. **OK**をクリックします。

これで、ルールでMatrix受信者を使用できます。

システムは指定されたポート番号またはパスワードが正しいこと、または指定されたポート番号、パスワード、またはタイプが実際のMatrix受信者に対応することを検証しません。情報を正しく入力したことを確認してください。

複数のXProtect Smart Clientビューに同じビデオを送信

ビューのMatrix位置が同じポート番号とパスワードを使用していれば、同じビデオを複数のXProtect Smart Clientビューの Matrix位置に送信できます。

1. XProtect Smart Clientで、関連するビューと、同じポート番号とパスワードを共有するMatrix位置を作成します。
2. Management Clientで、関連するXProtect Smart ClientをMatrix受信者として追加します。
3. Matrix受信者をルールに含めることができます。

ルールとイベント

ルールの追加

ルールを追加する際には、**ルールの管理**ウィザードによって関連オプションのみがリストされます。

ルールに必要な要素が不足していないか確認します。ルールの内容に基づき、ウィザードが自動的に適切な停止アクション(ルールが適用されなくなった後の動作)を提案し、無限にループするルールを誤って作成することを防ぎます。

イベント

イベントベースのルールを追加すると、さまざまなタイプのイベントを選択できます。

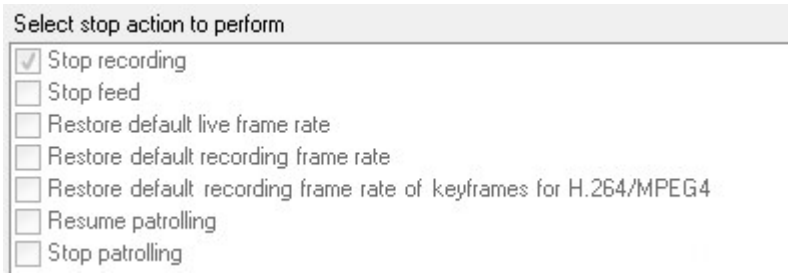
- 選択可能なイベントタイプの概要と説明については、「イベントの概要」を参照してください。

アクションと停止アクション

ルールを追加する際に、さまざまなアクションを選択できます。

一部のアクションには、終了アクションが必要です。例えば、**録画を開始**アクションを選択すると、録画が開始され、無限に続く可能性があります。したがって、**録画を開始**アクションには、**録画停止**という強制終了アクションがあります。

ルールの管理ウィザードでは、必要に応じて停止アクションを指定できます。



終了アクションの選択。この例では、強制終了アクション(選択済み、淡色表示)、該当しない終了アクション(淡色表示)、およびオプションの終了アクション(選択可能)に注目してください。

- 選択可能なアクションと停止アクションの概要については、「アクションと停止アクション」を参照してください。

ルールの作成

1. **ルール**アイテム > **ルールを追加**を右クリックします。**ルールの管理**ウィザードが開きます。ウィザードに従って、ルールの内容を指定します。
2. 新規ルールの名前と説明を**名前**と**説明**フィールドでそれぞれ指定します。
3. ルールに関連する条件の種類を選択します。特定のイベントが発生したときに1つ以上のアクションを実行するルール、または特定の時間を入力すると1つ以上のアクションを実行するルールのいずれかになります。
4. **次へ**をクリックしてウィザードのステップ2に進みます。ウィザードのステップ2で、ルールの詳細条件を定義します。

5. 1つまたは複数の条件を選択します。例えば、**曜日は<曜日>です**。

選択内容に応じて、ウィザードのウィンドウの下側で、ルールの説明を編集します。

太字斜体の下線付きアイテムをクリックして、正確な内容を指定します。例えば、**曜日**リンクをクリックすると、ルールが適用される曜日を選択することができます。

6. 正確な条件を指定したら、ウィザードの**次へ**をクリックし、次のステップに進み、ルールで網羅するアクションを選択します。ルールの内容と複雑性に応じ、停止イベントや停止アクション等、より多くのステップを定義する必要がある場合があります。例えば、特定のタイムインターバルで(例:木曜日の8:00から10:30)デバイスが特定のアクションを実行するようルールを指定した場合、そのタイムインターバル終了時に何が起こるかを指定するようウィザードから指示されます。
7. ルールを作成した時点で条件が満たされる場合は、デフォルトでルールがアクティブになります。ルールをすぐに適用したくない場合、***アクティブ***チェックボックスを外します。
8. **終了**をクリックします。

ルールの検証

個々のルールまたはすべてのルールの内容を一度に検証することができます。ルールを作成する際には、**[ルールの管理]**ウィザードを使用することで、ルールの全要素を有効にさせることができます。

ルールが一定期間存在し、1つまたは複数のルールの要素が他の構成により影響を受けた場合、ルールが機能しなくなる場合があります。例えば、ルールが特定の時間プロファイルで起動された場合、その時間プロファイルが後で削除されるか、権限がなくなると、ルールは機能しなくなります。このような構成上の意図せぬ影響については、確認が困難です。

ルール検証は、どのルールが影響を受けたのかを確認するのに役立ちます。検証はルールごとに行われ、各ルールは個別に検証されます。**すべてのルールの検証**機能を使用しても、互いにルールを検証することはできません(例えば、あるルールが別のルールと矛盾するかを確認する場合など)。

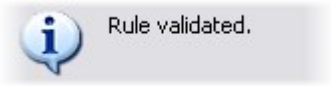
ルールの検証

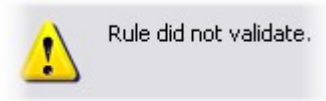
1. **[ルール]**をクリックして、検証したいルールを選択します。
2. ルールを右クリックして、**[ルールの検証]**をクリックします。
3. **OK**をクリックします。

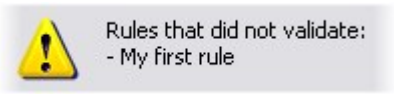
すべてのルールの検証

1. **[ルール]**アイテムを右クリックしてから、**[すべてのルールの検証]**をクリックします。.
2. **OK**をクリックします。

ダイアログボックスが表示され、ルールが正常に検証されたかどうかを示します。1つ以上のルールを変更したり、1つ以上のルールが守られないと、影響するルールの名前をダイアログボックスがリスト化します。







ルール外の要件の構成が、ルールの機能を妨害するかどうかを検証することはできない点に留意してください。例えば、関連するカメラでモーションが検知されたときに録画を開始するというルールでは、そのカメラでモーション検知(ルールではなくカメラレベルで有効になっている)が有効になっていなくても、ルールの要素自体が正しければ、検証結果は合格ということになります。

ルールを編集、コピー、名前変更する

1. **概要**ペインで、関連するルールを右クリックします。
2. 以下のいずれかを選択します。

   ルールを編集、**ルールをコピー**または**ルールの名前変更**。**ルールの管理**ウィザードが開きます。
3. **ルールをコピー**を選択するとウィザードが開き、選択したルールのコピーが表示されます。**終了**をクリックしてコピーを作成します。
4. **ルールを編集**を選択するとウィザードが開き、そこで変更を加えることができます。**終了**をクリックして変更を確定します。

5. **ルールの名前変更**を選択すると、ルールの名前のテキストを直接変更できます。

ルールを無効/有効にする

ルールの条件が適用され、ルールが有効になると、システムは即座にルールを適用します。ルールを有効にしたくない場合は、ルールを無効にすることができます。ルールを無効にすると、ルールの条件が満たされても、システムではルールが適用されません。ルールを無効にした場合も、後で簡単にルールを有効にすることができます。

ルールを無効にする

1. **概要**ペインで、ルールを選択します。
2. **プロパティ**ペインで**有効化**チェックボックスを外します。
3. ツールバーの**保存**をクリックします。
4. 赤のxのついたアイコンは、ルールが**ルール**リストで無効化されたことを示します。

ルールを有効にする

ルールをもう一度有効にしたい場合は、ルールを選択し、**有効化**チェックボックスを選択して、設定を保存します。

時間プロファイルの指定

1. **時間プロファイル**リストで、**時間プロファイル > 時間プロファイルの追加**をクリックします。これにより、**時間プロファイル**ウィンドウが開きます。
2. **時間プロファイル**ウィンドウで、**名前**フィールドに新しい時間プロファイルの名前を入力します。オプションとして、新しい時間プロファイルの説明を**説明**フィールドに入力できます。
3. **時間プロファイル**ウィンドウのカレンダーで、**日ビュー**、**週ビュー**または**月ビュー**を選択してから、カレンダーの内側を右クリックして、**1つの時間を追加**または**繰り返し時間を追加**を選択します。
4. 時間プロファイルの期間を指定し、**時間プロファイル**ウィンドウの**OK**をクリックします。システムが、新規時間プロファイルを**時間プロファイル**リストに追加します。後で時間プロファイルを編集または削除したい場合、**時間プロファイル**リストからも行うことができます。

1つの時間を追加

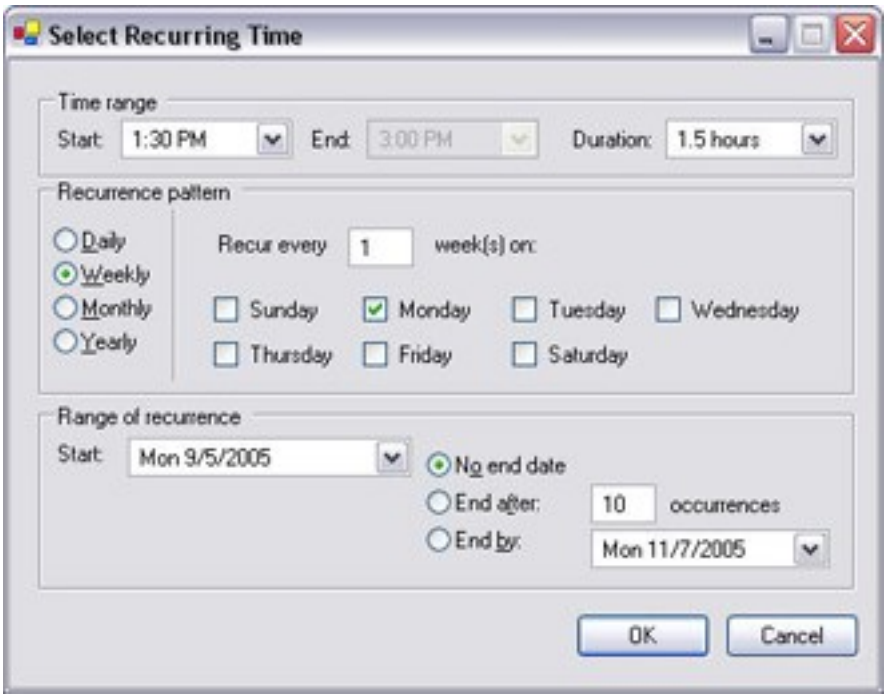
1つの時間を追加を選択すると、**時間を選択**ウィンドウが表示されます。

時刻と日付のフォーマットは、使用しているシステムの設定によって異なります。

1. **時間を選択**ウィンドウで、**開始時刻**と**終了時刻**を指定します。期間が終日にわたる場合は、**終日イベント**ボックスを選択します。
2. **OK**をクリックします。

繰り返し期間の追加

繰り返し時間を追加を選択すると、**繰り返し時間を選択**ウィンドウが表示されます。



1. **時間を選択**ウィンドウで、時間範囲、繰り返しパターン、および繰り返し範囲を指定します。
2. **OK**をクリックします。

時間プロファイルには、複数の期間を含めることができます。時間プロファイルに、さらに期間を含めたい場合は、単独の期間または繰り返し時間を追加します。

繰り返し時間

詳細な定期スケジュールでは、アクションをどの時点で実行するかを設定できます。

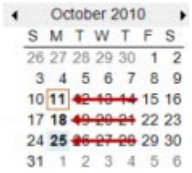
例：

- 毎週火曜日の15:00～15:30の間に1時間おきに実行
- 3か月ごとにその月の15日の11:45に実行
- 毎日15:00～19:00の間に1時間おきに実行

時刻は、ManagementClientがインストールされているサーバーのローカル時刻設定に基づいています。

時間プロファイルの編集

1. **概要**ペインの**時間プロファイル**リストで、該当する時間プロファイルを右クリックし、**時間プロファイルの編集**を選択します。これにより、**時間プロファイル**ウィンドウが開きます。
2. 必要に応じて時間プロファイルを編集します。時間プロファイルに変更を加えたら、**時間プロファイル**ウィンドウの**OK**をクリックします。**時間プロファイル**リストに戻ります。



時間プロファイルの情報ウィンドウで、必要に応じて時間プロファイルを編集できます。時間プロファイルには1つ以上の期間が含まれ、期間は繰り返される場合があります。右上端の小さい月概要には、時間プロファイルが対応する期間の概要が簡単に表示されます。指定された時間を含む日付が太字で強調表示されます。

この例では、太字の日付は、期間が複数の日付で指定され、繰り返し時間が月曜日に指定されていることを示しています。

日中時間プロファイルの作成

1. **ルールとイベント**フォルダー > **時間プロファイル**を選択します。
2. **時間プロファイル**リストで、**時間プロファイル**を右クリックし、**日中時間プロファイルを追加**を選択します。
3. **日中時間プロファイル**ウィンドウで、下表のプロパティを参照しながら必要な情報を入力します。明るくなったり暗くなったりする間の移行時間帯に対応するために、プロファイルの有効/無効をオフセットすることが可能です。さらに、コンピュータの言語/地域設定で使用している言語で、時間と月が表示されます。
4. 入力した地理的座標の位置をマップ上で確認するには、**ブラウザで位置を表示**をクリックします。これによりブラウザが開いて位置を確認できます。
5. **OK**をクリックします。

日中時間プロファイルのプロパティ

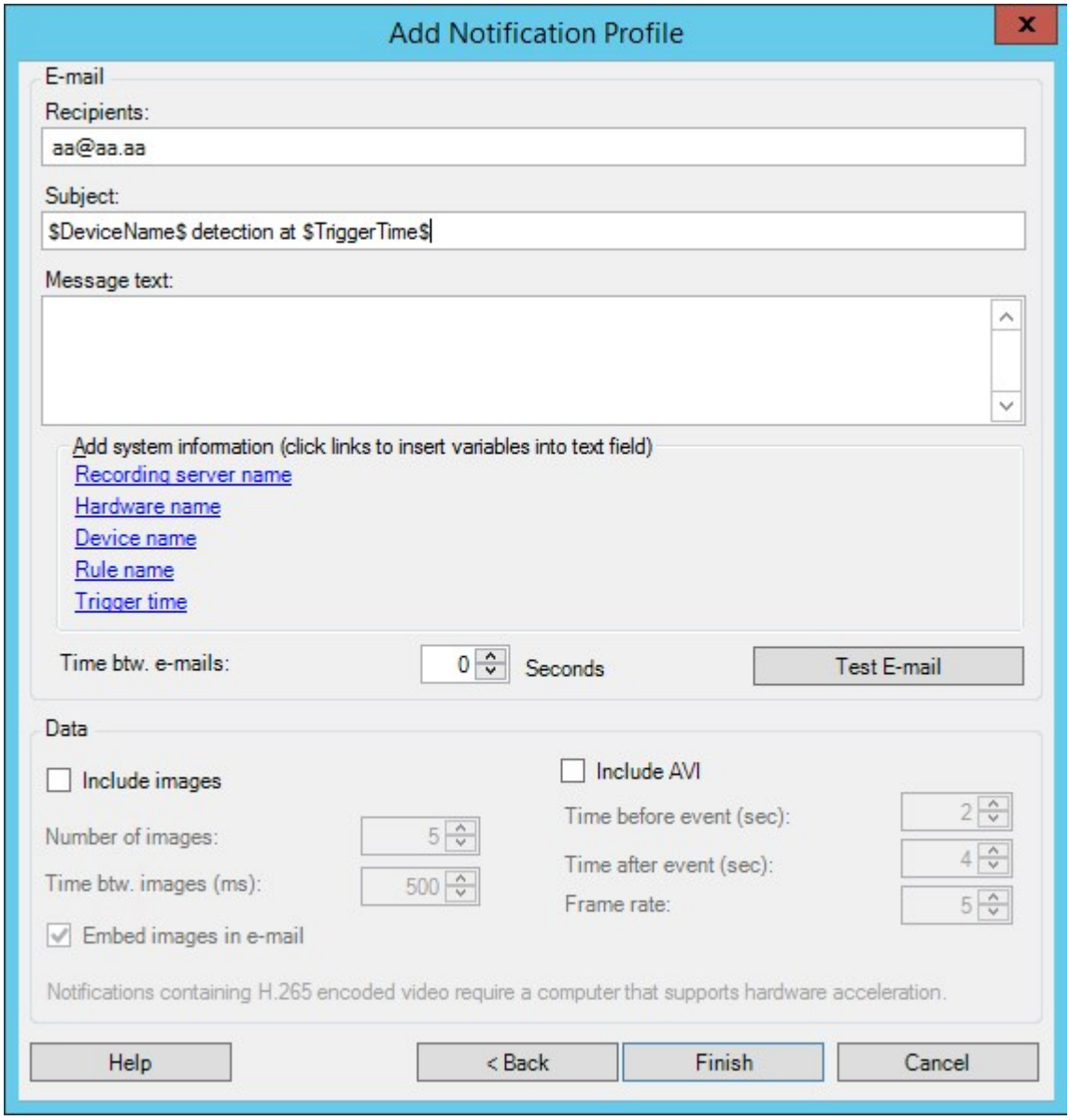
名前	説明
名前	プロファイルの名前。
説明	プロファイルの説明(任意)。
地理的座標	プロファイルに割り当てられた、カメラの物理的な場所を示す地理的座標。
日の出オフセット	日の出によりプロファイルの有効化がオフセットされる分単位の時間(+/-)。
日没オフセット	日没によりプロファイルの無効化がオフセットされる分単位の時間(+/-)。
タイムゾーン	カメラの物理的位置を示すタイムゾーン。

通知プロファイルの追加

通知プロファイルを作成する前に、Eメールによる通知のためのメールサーバー設定を行う必要があります。詳細については、「通知プロファイルの作成要件」を参照してください。

1. **ルールとイベント**を展開し、**通知プロファイル** > **通知プロファイルを追加**を右クリックします。これにより、**通知プロファイルを追加**ウィザードが開きます。
2. 名前と説明を指定します。**次へ**をクリックします。

3. 受信者、件名、本文、Eメールを送信する時間間隔を指定します。



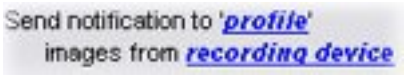
4. Eメールによる通知をテストするために、指定の受信者に送信したい場合は、**Eメールのテスト**をクリックします。
5. プリアラームの静止画像を含めるには、**画像を含める**を選択して、画像数、画像間の時間間隔、画像をEメールに埋め込むか否かを指定します。
6. AVIビデオクリップを含めるには、**AVIを含める**を選択し、イベント前後の時間とフレームレートを指定します。

> H.265でエンコードされた動画を含めるには、ハードウェアアクセラレーションをサポートするコンピュータが必要です。

7. **終了**をクリックします。

ルールによるEメール通知のトリガー

1. **[ルール]**アイテムを右クリックしてから、**[ルールの追加]**または**[ルールの編集]**をクリックします。
2. **[ルールの管理]**ウィザードで**[次へ]**をクリックして**[実行するアクションを選択]**リストに移動し、**[通知を<プロファイル>に送信]**を選択します。
3. 該当する通知プロファイルを選択し、通知プロファイルのEメール通知に含める録画の記録元となるカメラを選択します。



実際に何かが記録されていない限り、通知プロファイルのEメール通知に録画を含めることはできません。静止画像またはAVIビデオクリップをEメール通知に含めたい場合は、録画の開始を指定するルールを検証します。次の例は、**記録の開始**アクションと**通知を送信します**アクションを含むルールの例です。

ユーザー定義イベントの追加

> ユーザー定義イベントをどのように使用するかにかかわらず、各ユーザー定義イベントはManagement Clientで追加する必要があります。

1. **ルールとイベント> ユーザー定義イベント**を展開します。
2. **概要**ペインで、**イベント> ユーザー定義イベントを追加**を右クリックします。
3. 新規ユーザー定義イベントの名前を入力し、**OK**をクリックします。新しく追加したユーザー定義イベントが、**概要**ペインのリストに表示されます。

ユーザーに権限がある場合、ユーザーはXProtectSmartClientでユーザー定義のイベントを手動でトリガーできるようになります。

また、ユーザー定義イベントを削除すると、ユーザー定義イベントが使用されていたルールに影響を及ぼします。さらに、削除されたユーザー定義イベントは、XProtect Smart Clientユーザーがログアウトした後にXProtect Smart Clientから削除されます。

ユーザー定義イベントの名前を変更

ユーザー定義イベントの名前を変更する場合、すでに接続済みのXProtect Smart Clientユーザーの名前の変更が表示されるには、一旦ログアウトしてから再度ログインする必要があります。

1. **ルールとイベント** > **ユーザー定義イベント**を展開します。
2. **概要**ペインで、ユーザー定義イベントを選択します。
3. **プロパティ**ペインで、既存の名前を上書きします。
4. ツールバーで**保存**をクリックします。

アナリティクスイベントの追加と編集

アナリティクスイベントの追加

1. **ルールとイベント**を展開し、**アナリティクスイベント**を右クリックし、**新規追加**を選択します。
2. **プロパティ**ウィンドウで、**名前**フィールドにイベントの名前を入力します。
3. 必要に応じて、**説明**フィールドに説明テキストを入力します。
4. ツールバーで**保存**をクリックします。**イベントのテスト**をクリックして、イベントの妥当性をテストすることができます。テストで表示されるエラーを継続的に修正し、プロセスのどこからでもテストを何度でも実行することができます。

アナリティクスイベントの編集

1. 既存のアナリティクスイベントをクリックして、関連するフィールドを編集する**プロパティ**ウィンドウを表示します。
2. **イベントのテスト**をクリックして、イベントの妥当性をテストすることができます。テストで表示されるエラーを継続的に修正し、プロセスのどこからでもテストを何度でも実行することができます。

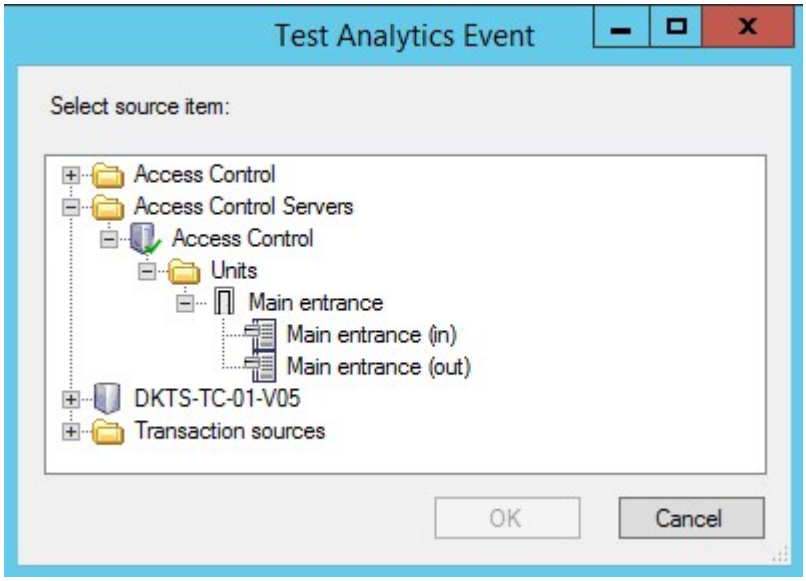
アナリティクスイベント設定の編集

ツールバーで**ツール** > **オプション** > **アナリティクスイベント**タブを選択して、関連する設定を編集します。

アナリティクスイベントのテスト

アナリティクスイベントを作成したら、要件(「268ページのアナリティクスイベントの追加と編集」を参照)をテストすることができます。例えば、そのアナリティクスイベントの機能がManagement Clientで有効になっているかをテストできます。

1. 既存のアナリティクスイベントを選択します。
2. プロパティで、**テストイベント**ボタンをクリックします。可能なすべてのイベントのソースを表示するウィンドウが開きます。



3. 例えば、カメラなどのテストイベントのソースを選択します。ウィンドウが閉じ、アナリティクスイベントが機能するために満たすべき4つの条件を示す新しいウィンドウが開きます。

追加テストとして、XProtect Smart Clientで、アナリティクスイベントがイベントサーバーに送信されたかどうかを確認できます。このためには、XProtect Smart Clientを開いて**アラームマネージャー**タブのイベントを表示します。

ジェネリックイベントの追加

VMSが外部システムからのTCPまたはUDPパケットの特定の文字列を認識できるように、ジェネリックイベントを定義することができます。ジェネリックイベントに基づいて、録画またはアラームの開始などのアクションをトリガーするようにManagement Clientを設定することができます。

要件

ジェネリックイベントを有効にし、許可されるソース宛先を指定していること。詳細については、「379ページのジェネリックイベントタブ(オプション)」を参照してください。

ジェネリックイベントを追加するには、以下を実行します。

1. **ルールとイベント**を展開します。
2. **ジェネリックイベント**を右クリックして、**新規追加**を選択します。
3. 必要な情報とプロパティを入力します。詳細については、「474ページのジェネリックイベントとデータソース(プロパティ)」を参照してください。

4. (オプション) 検索式が有効であることを検証するため、予測されるパッケージに対応する**表現がイベント文字列と一致するかチェック**フィールドに、以下の検索文字列を入力します。
    - **一致** - 文字列が検索式と照らし合わせて検証されました
    - **不一致** - 検索式が無効です。検索式を変更して、再試行してください

XProtect Smart Clientでは、イベントサーバーがジェネリックイベントを受信したかどうかを検証できます。これは、**アラームマネージャ**タブの**アラームリスト**で、**イベント**を選択して実行します。

認証

外部IDPからのクレームの登録

1. Management Clientで、**ツール > オプション**を選択し、**外部IDP**タブを開きます。
2. **外部IDP**セクションで、**追加**を選択します。
3. **[登録済みクレーム]** セクションで、**[追加]** を選択します。
4. クレームに関する情報を入力します。詳細については、「クレームの登録」を参照してください。

XProtectで外部IDPからのクレームを役割にマッピングします

外部IDPサイトで、管理者は名前と値で構成されるクレームを作成する必要があります。その後、クレームがVMS上の役割にマッピングされ、役割別にユーザー権限が決定されます。

1. Management Clientの **[サイトナビゲーション]** ペインで、**[セキュリティ]** ノードを展開し、**[役割]** を選択します。
2. 役割を選択し、**外部IDP**タブを選択してから**追加**を選択します。
3. 外部IDPと苦情名を選択し、苦情の値を入力します。

    苦情名は、外部IDPからの苦情名と全く同じように入力する必要があります。

4. **[OK]** を選択します。

外部IDPを削除すると、外部IDPを介してVMSに接続しているすべてのユーザーも削除されます。外部IDPに関連するすべての登録済み苦情が削除され、役割へのマッピングもすべて削除されます。

外部IDP経由でログインする

外部IDPを使用してXProtect Smart Client、XProtect Management Client、XProtect Web Client、XProtect Mobileのクライアントにログインできます。

1. XProtect Smart ClientまたはXProtect Management Clientのログインダイアログボックスの**認証**で、外部IDPを選択し、**サインイン**を選択します。初めてログインすると、外部IDPに属するウェブページにリダイレクトされます。
2. ユーザー名とパスワードを入力し、サインインします。サインインすると、XProtectクライアントに戻り、ログインされた状態となります。

ツール > オプション > 外部IDPで、**認証**リストに表示される外部IDPの名前を設定できます。

パスワードの復元や変更などによって外部IDPが無効になっている場合、**認証**リストに外部IDPを介してログインするオプションはありません。また、外部IDPが無効になっている場合、外部IDPから受信したクライアントシークレットは、**ツール>オプション**にある**外部IDP**タブの**クライアントシークレット**フィールドに表示されなくなります。

セキュリティ

役割の追加および管理

1. **セキュリティ**を展開して、**役割**を右クリックします。
2. **役割の追加**を選択します。これにより、**役割の追加**ダイアログボックスが開きます。
3. 新しい役割の名前と説明を入力し、**[OK]**をクリックします。
4. 新しい役割が**役割**リストに追加されます。デフォルトでは、新しい役割にはユーザー/グループは関連付けられていませんが、関連付けられたデフォルトのプロファイルがあります。
5. 異なるSmart ClientおよびManagement Clientプロファイル、エビデンスロックプロファイル、時間プロファイルを選択するには、ドロップダウンリストをクリックします。
6. これで、ユーザー/グループを役割に割り当てて、どのシステム機能にユーザー/グループがアクセスできるかを指定できます。

詳細については、272ページのユーザーおよびグループの役割からの削除、役割への割り当ておよび477ページの役割(セキュリティノード)を参照してください。

役割のコピー、名前の変更、削除

役割のコピー

設定や権限が複雑な役割があり、同様の役割またはほぼ同様の役割が必要な場合、新しい役割をゼロから作成するよりも、既存の役割をコピーし、コピーした役割を微調整する方が簡単な場合があります。

1. **セキュリティ**を展開し、**役割**をクリックし、関連する役割を右クリックして、**役割のコピー**を選択します。
2. ダイアログボックスが開いたら、コピーした役割の新しい一意の名前と説明を入力します。
3. **OK**をクリックします。

役割の名前の変更

役割の名前を変更しても、役割をベースとしたビューグループの名前は変更されません。

1. **セキュリティ**を展開して、**役割**を右クリックします。
2. 必要な役割を右クリックし、**役割の名前の変更**を選択します。
3. ダイアログボックスが開いたら、役割の名前を変更します。
4. **OK**をクリックします。

役割の削除

1. **セキュリティ**を展開し、**役割**をクリックします。
2. 対象外の役割を右クリックし、**役割の削除**を選択します。
3. **はい**をクリックします。

> 役割を削除しても、役割をベースとしたビューグループは削除されません。

有効な役割の表示

有効な役割機能により、選択したユーザーまたはグループのすべての役割を表示することができます。この機能は、グループを使用している場合に特に便利であり、個別のユーザーがどのメンバーの役割であるかを表示する唯一の方法です。

1. **セキュリティ**を展開して**有効な役割**を開き、**役割**を右クリックして**有効な役割**を選択します。
2. 基本ユーザーの情報を確認するには、**[ユーザー名]**フィールドに名前を入力します。**更新**をクリックすると、ユーザーの役割が表示されます。
3. Active DirectoryでWindowsユーザーまたはグループを使用する場合、**[...]**参照ボタンをクリックします。オブジェクトタイプを選択して名前を入力し、**OK**をクリックします。ユーザーの役割が自動的に表示されます。

ユーザーおよびグループの役割からの削除、役割への割り当て

Windowsユーザー、グループまたは基本ユーザーを役割から削除したり、役割に割り当てるには、以下を行います。

1. **セキュリティ**を展開し、**役割**を選択します。次に、**概要**ペインで必要な役割を選択します。
2. **プロパティ**ペインの下部で**ユーザーおよびグループ**タブを選択します。
3. **追加**をクリックし、**Windowsユーザー**または**基本ユーザー**から選択します。

役割にWindowsユーザーおよびグループを割り当てる

1. **Windowsユーザー**を選択します。**ユーザーの選択、コンピュータ、およびグループの選択**ダイアログボックスが開きます。
2. 必要なオブジェクトタイプを指定しているか確認します。例えば、コンピュータを追加する必要がある場合、**オブジェクトタイプ**をクリックし、**コンピュータ**をマークします。さらに、**この場所から**フィールドで必要なドメインを指定したか確認します。指定されていなければ、**場所**をクリックして、必要なドメインを参照します。
3. **選択するオブジェクト名を入力**]ボックスで、関連するユーザー名、イニシャル、またはActive Directoryが認識できるその他の識別子タイプを入力します。**名前のチェック**機能を使用して、入力した名前やイニシャルをActive Directoryが認識できることを確認します。または、**[詳細...]**機能でユーザーまたはグループを検索します。
4. **OK**をクリックします。選択したユーザー/グループは、これで選択した役割に割り当てたユーザーの**ユーザーおよびグループ**タブのリストに追加されます。セミコロン(;)で区切って複数の名前を入力することで、さらに多くのユーザーやグループを追加することができます。

役割に基本ユーザーを割り当てる

1. **基本ユーザー**を選択します。これにより、**ロールに追加する基本ユーザーを選択**ダイアログボックスが開きます。
2. この役割に割り当てる基本ユーザーを選択します。
3. オプション:**新規**をクリックすると新しい基本ユーザーを作成できます。
4. **OK**をクリックします。選択した基本ユーザーは、これで選択した役割に割り当てた基本ユーザーの**ユーザーおよびグループ**タブのリストに追加されます。

役割からユーザーおよびグループを削除する

1. **ユーザーおよびグループ**タブで、削除したいユーザーまたはグループを選択し、タブ下の**削除**をクリックします。必要に応じて、複数のユーザーまたはグループ、あるいはグループや個人ユーザーの組み合わせを選択することができます。
2. 選択したユーザーまたはグループを削除することを確認します。**はい**をクリックします。

ユーザーは、グループメンバーを経由して役割を有することもあります。この場合、その役割から個別ユーザーを削除することはできません。グループメンバーは、個人として役割を持つ場合もあります。ユーザー、グループ、または個別のグループメンバーが持っている役割を確認するには、**[有効な役割の表示]**機能を使用します。

基本ユーザーの作成

Milestone XProtect VMSには2つのユーザーアカウントタイプがあります。 基本ユーザーとWindows ユーザー。

基本ユーザーとはMilestone XProtect VMSで作成したユーザーアカウントです。個々のユーザーの基本ユーザー名とパスワード認証を備えた専用のシステムユーザーアカウントです。

Windows ユーザーはMicrosoftのActive Directoryを通して追加したユーザーアカウントです。

基本ユーザーとWindows ユーザーには多少違いがあります。

- 基本ユーザーは、ユーザー名とパスワードの組み合わせによって認証され、システム/サイト固有のものです。あるフェデレーテッドサイトで作成された基本ユーザーが別のフェデレーテッドサイトの基本ユーザーと同じ名前とパスワードを持つ場合でも、基本ユーザーは作成されたサイトにしかアクセスできません。
- Windowsユーザーは Windows ログインに基づいて認証され、1つのマシン固有です。

基本ユーザーのログイン設定

基本ユーザーのログイン設定は、このJSONファイルで定義することができます。`\\Program Files\Milestone\Management Server\IIS\IDP\appsettings.json`.

そのファイルで、次のパラメーターは設定できません。

LoginSettings	
"ExpireTimeInMinutes": 5	ユーザーが操作を行わない場合、ログインセッションを期限切れにするまでに時間(単位:分)を設定します。
LockoutSettings	
"LockoutTimeSpanInMinutes": 5	ユーザーのロックアウト時間(単位:分)を設定します。
"MaxFailedAccessAttempts": 5	ユーザーがロックアウトされずにログインを試行できる回数を設定します。
PasswordSettings	
"RequireDigit": true	パスワードに数字(0~9)を含めることを必須にするか設定します。
"RequireLowercase": true	パスワードの小文字を含めることを必須にするか設定します。
"RequireNonAlphanumeric": true	パスワードに特殊文字(~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)を含めることを必須にするか設定します。
"RequireUppercase": true	パスワードの大文字を含めることを必須にするか設定します。
"RequiredLength": 8	パスワードに必要な文字数を設定します。パスワードの最低文字数は{0}文字で、最大文字数は255文字です。
"RequiredUniqueChars": 1	パスワードに必要な固有の文字の最低数を設定します。 例えば、固有の文字の最低数を2文字に設定した場合、「aaaaaa」、「aa」、「a」、「b」、「bb」、「bbbbbbb」といったパスワードは却下されます。 したがって、abab、abc、aaabなどは、パスワード内に固有の文字が2文字以上含まれているため認められます。 パスワードに使用する固有の文字の数を増やすと、簡単に推測できる連続文字列の反復を避けられるため、パスワードの強度が上がります。

基本ユーザーを作成するには：

1. **[セキュリティ]**を展開し**[基本ユーザー]**をクリックします。
2. **[基本ユーザー]**ペインを右クリックして、**[基本ユーザーの作成]**を選択します。
3. ユーザー名とパスワードの指定。パスワードが正しく指定されていることを確認するために再入力します。

   パスワードは、**appsettings.json**ファイルで設定された複雑さの要件を満たすものである必要があります(274ページの基本ユーザーのログイン設定を参照)。
4. 基本ユーザーが次回ログイン時にパスワードを変更すべきかどうか指定します。Milestoneは、このチェックボックスをオンにして、最初にログインする際に、基本ユーザーが独自のパスワードを指定できるようにすることをお勧めします。

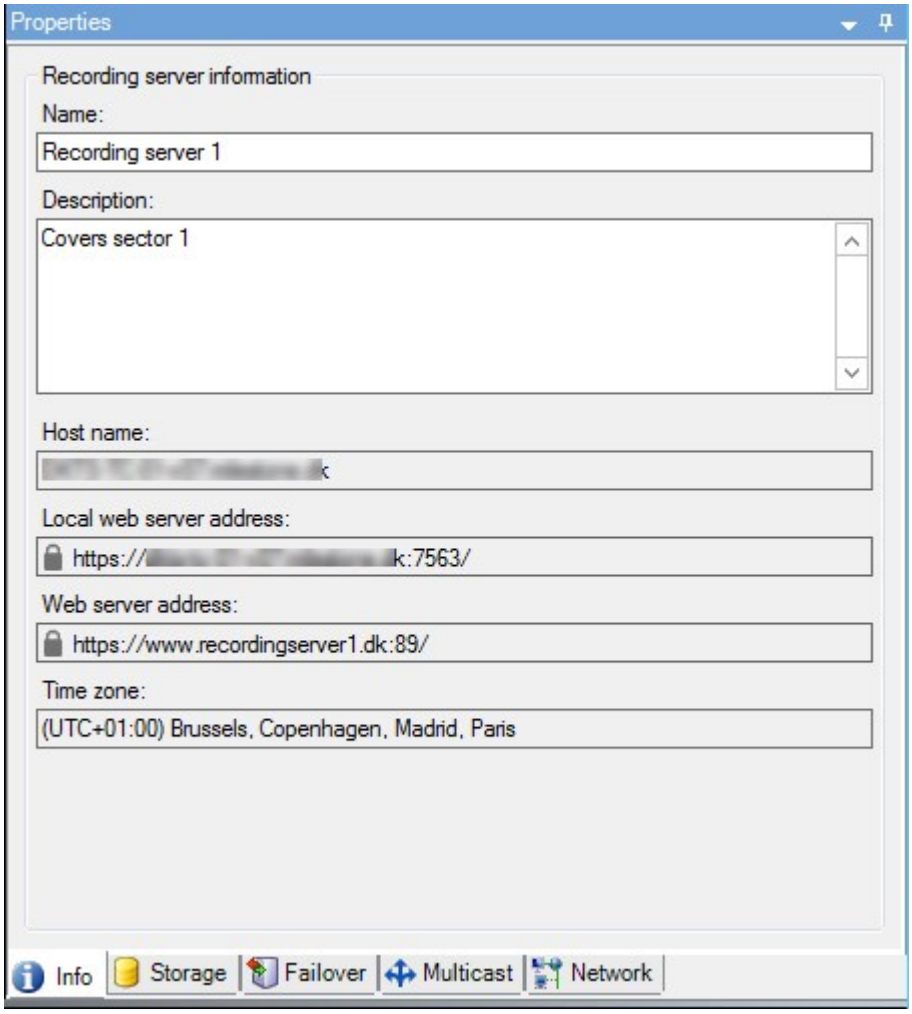
   パスワードを変更できない基本ユーザーを作成した場合、このチェックボックスをクリアするだけで大丈夫です。このような基本ユーザーは、例えば、プラグインやサーバーサービス認証に使用されるシステムユーザーです。
5. 基本ユーザーのステータスを**有効**または**ロックアウト**に指定します。
6. **OK**をクリックして、新しい基本ユーザーを作成します。

クライアントの暗号化ステータスを表示する

レコーディングサーバーが接続を暗号化しているかを確認するには、以下を実行します。

1. Management Clientを開きます。
2. **サイトナビゲーション**ペインで、**サーバー > レコーディングサーバー**を選択します。レコーディングサーバーのリストが表示されます。

3. **概要**パネルで関連するレコーディングサーバーを選択し**情報**タブに移動します。
   レコーディングサーバーからデータストリームを受け取るクライアントとサーバーで暗号化が有効になっている場合は、ローカルのウェブサーバーアドレスとオプションのウェブサーバーアドレスの前に南京錠アイコンが表示されます。



システムダッシュボード

レコーディングサーバーで実行中のタスクを表示

[現在のタスク]には、選択したレコーディングサーバーで実行中のタスクの概要が示されます。長い時間を要するタスクが開始され、これがバックグラウンドで実行されている間は、**[現在のタスク]**ウィンドウでタスクの進行状況を確認できます。ユーザーが開始するタスクのうち、長い時間を要するものの一例として、ファームウェアの更新やハードウェアの移動が挙げられます。ここではタスクの開始時刻、予想終了時刻、進行状況といった情報を確認できます。

タスクが適切に処理されない場合、ハードウェアまたはネットワークが原因となっている可能性があります。一例として、サーバーが稼働していない、サーバーにエラーが発生している、帯域幅が小さすぎる、接続が失われていることが挙げられます。

1. **[サイトナビゲーション]**ペインで、**[システムダッシュボード] > [現在のタスク]**を選択します。
2. レコーディングサーバーを選択して、現在実行中のタスクについて確認します。

[現在のタスク]ウィンドウに表示される情報はリアルタイムのものではなく、ウィンドウを開いた時点で実行されていたタスクのスナップショットとなります。ウィンドウを開いてから時間が経過している場合は、ウィンドウ右下にある**[更新]**ボタンを選択して情報を更新します。

システムモニター(説明付き)

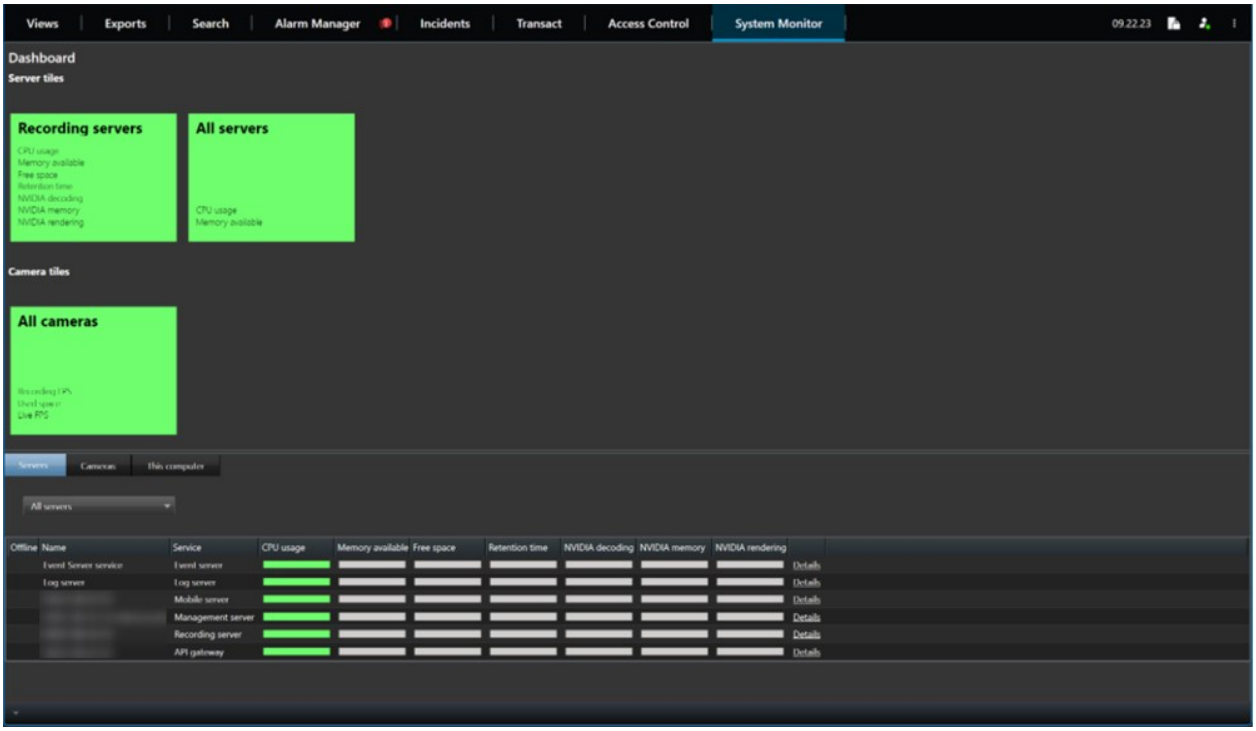
> システムモニター機能を使用するには、DataCollectorサービスが実行されている必要があります。またこの機能は、グレゴリオ暦(西暦)のカレンダーが使用されているコンピュータでしか利用できません。

システム監視ダッシュボード(説明付き)

[システムモニターダッシュボード]では、VMSシステムの健全性についての概要を容易に把握できます。ハードウェアの状態は、タイルとその色によって視覚的に表示されます: 緑(稼働中)、黄(警告)、赤(重大)。タイルには、1つまたは複数のハードウェアに障害が発生したことを示す、エラーまたは警告アイコンも表示できます。

デフォルトでは、すべての**レコーディングサーバー**、**すべてのサーバー**、**すべてのカメラ**を表すタイルが表示されます。これらのデフォルトタイルの監視パラメータをカスタマイズして、新しいタイルを作成することができます。たとえば、1台のサーバー、1台のカメラ、カメラのグループ、またはサーバーグループを表すようにタイルを設定できます。

たとえば、監視パラメータは、CPU利用率またはサーバーの空きメモリなどです。タイルによってモニターされるのは、タイルに追加した監視パラメータに限定されます。詳細については、280ページのシステムモニターダッシュボードでカメラタイルまたはサーバータイルを編集「280ページのシステムモニターダッシュボードで新しいカメラタイルまたはサーバータイルを追加」、「281ページのシステムモニターダッシュボードからカメラタイルまたはサーバータイルを削除」、「」を参照してください。



システムモニターしきい値(説明付き)

システムモニターしきい値を使用すれば、どの時点で**[システムモニターダッシュボード]**にシステムハードウェアの状態変化が視覚的に表示されるようにするかを、しきい値の定義と調整を介して指定できます。たとえば、サーバーのCPU使用率が正常な状態(緑)から警告状態(黄)に変化した際、または警告状態(黄)から重大状態(赤)に変化した際、のように設定できます。

同種のハードウェアにはすべてデフォルトのしきい値が設定されているため、システムをインストールしてハードウェアを追加した瞬間からシステムハードウェアの状態を監視し始めることができます。個々のサーバー、カメラ、ディスク、ストレージのしきい値を設定することもできます。しきい値を変更する方法については、「281ページのハードウェアの状態変化を決めるしきい値を編集」を参照してください。

システムハードウェアの使用/負荷が短時間(1秒前後)しか高しきい値に達しなかった場合に**重大**または**警告**状態が表示されないようにするには、**計算間隔**を使用します。計算間隔を適切に設定することで、しきい値超過に関するアラートの誤発動を防ぐ一方、継続的な問題(CPU使用率やメモリ消費など)に関するアラートのみを表示することが可能となります。

ルールを設定(「ルール(説明付き)」を参照)することで、しきい値がある状態から別の状態に変化した際に、特定のアクションを実行したりアラームを作動したりもできます。

ハードウェアの現在の状態を表示し、必要に応じてトラブルシューティングを実行

[システムモニターダッシュボード]では、VMSシステムの健全性についての概要を容易に把握できます。ハードウェアの状態は、タイルとその色によって視覚的に表示されます: 緑(稼働中)、黄(警告)、赤(重大)。タイルには、1つまたは複数のハードウェアに障害が発生したことを示す、エラーまたは警告アイコンも表示できます。

ハードウェアがどの時点で3種類のいずれの状態に入るかを決めるしきい値は、編集することができます。詳細については、「281ページのハードウェアの状態変化を決めるしきい値を編集」を参照してください。

[システムモニターダッシュボード]では以下について確認できます。サーバーサービスとカメラがすべて稼働しているか? すべてのものを記録して表示できるよう、それぞれのサーバーのCPU使用率と使用可能メモリが適切/十分な状態になっているか?

1. **[サイトナビゲーション]**ペインで、**[システムダッシュボード] > [システムモニター]**を選択します。
2. すべてのタイルが緑色で、警告およびエラーアイコンが一切表示されていなければ、このタイルで示されているすべての監視パラメータと、すべてのサーバー/カメラが正常に稼働しています。
   1つまたは複数のタイルに警告/エラーアイコンが表示されているか、または完全に黄色または赤くなっている場合は、いずれかのタイルを選択してトラブルシューティングを実行します。
3. 監視パラメータが示されているハードウェアリスト(ウィンドウ下部) で、稼働していないハードウェアを特定します。ハードウェアの横に表示される赤いバツ印の上にカーソルを置いて、どのような問題が発生しているかを確認します。
4. 任意で、ハードウェアの右側に表示される**[詳細]**を選択して、問題がどれくらいの期間にわたって発生しているかを確認します。履歴データの収集を有効にしておけば、ハードウェアの経時的な状態について把握できます。詳細については、「280ページのハードウェアの状態に関する履歴データを収集」を参照してください。
5. 問題を修正するための方法を模索します。たとえば、コンピュータを再起動する、サーバーサービスを再起動する、障害のあるハードウェアなどを交換する、といったことが挙げられます。

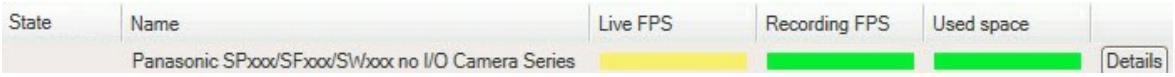
ハードウェアの状態履歴を表示してレポートを印刷

[システムモニター]機能を使用すれば、VMSシステムの健全性についての概要を容易に把握できます。また、より長期間にわたる傾向もつかむことができます。

CPU使用率、帯域幅、または他のハードウェアの問題が発生した期間が存在するかどうかについて**[システムモニター]**機能を介して特定し、将来的にこのような問題を避けるためにハードウェアのアップグレードや新規購入が必要かどうかを判断できます。

履歴データの収集は必ず有効にしてください。280ページのハードウェアの状態に関する履歴データを収集を参照してください。

1. **[サイトナビゲーション]**ペインで、**[システムダッシュボード] > [システムモニター]**を選択します。
2. **[システムモニター]**ウィンドウで、健全性の履歴について確認したいハードウェアが含まれるタイルを選択するか、あるいはウィンドウ下部でサーバーまたはカメラを選択します。
3. 該当するサーバーまたはカメラの右側に表示される**[詳細]**を選択します。



4. サーバーについては、調べたいハードウェアの右側に表示される**[履歴]**を選択します。カメラについては、リンクを選択します。
5. レポートを印刷するには、PDFアイコンを選択します。

デバイスが現在存在するレコーディングサーバーのデータを使用した場合にのみ履歴レポートを作成できます。

サーバーのオペレーティングシステムからシステムモニターの詳細にアクセスした場合、**Internet Explorer Enhanced Security Configuration**に関連するメッセージが表示されることがあります。指示に従って、**「システムモニター]**のページを**[信頼済みサイトゾーン]**に追加してから続行してください。

ハードウェアの状態に関する履歴データを収集

システムのハードウェアに関する履歴データの収集を有効にすれば、ハードウェアの経時的な状態の変化についてのグラフを表示し、レポートを印刷することができます。詳細については、「279ページのハードウェアの状態履歴を表示してレポートを印刷」を参照してください。

1. **[サイトナビゲーション]**ペインで、**[システムダッシュボード] > [システムモニター]**を選択します。
2. **[システムモニター]**ウィンドウで**[カスタマイズ]**を選択します。
3. **[ダッシュボードのカスタマイズ]**ウィンドウが表示されたら、**[履歴データの収集]**を選択します。
4. サンプリング間隔を選択します。間隔が短いほど、SQL Serverデータベース、帯域幅、または他のハードウェアにかかる負荷が増加します。履歴データのサンプリング間隔は、グラフの詳細度にも影響します。

システムモニターダッシュボードで新しいカメラタイルまたはサーバータイルを追加

物理的に配置されたカメラまたは小さめのサーバーグループをモニターしたい場合、または別の監視パラメータを用いて一部のハードウェアをモニターしたい場合は、**[システムモニター]**ウィンドウにタイルを追加できます。

1. **[サイトナビゲーション]**ペインで、**[システムダッシュボード] > [システムモニター]**を選択します。
2. **[システムモニター]**ウィンドウで**[カスタマイズ]**を選択します。
3. **[ダッシュボードのカスタマイズ]**ウィンドウが表示されたら、**[サーバータイル]**または**[カメラタイル]**で**[新規]**を選択します。
4. **[新しいサーバータイル/新しいカメラタイル]**ウィンドウで、監視するサーバーまたはカメラを選択します。
5. **[監視パラメータ]**で、タイルに追加または削除したいパラメータのチェックボックスを選択または選択解除します。
6. **[OK]**をクリックします。新しいサーバーまたはカメラタイルがダッシュボードに表示されるタイルに追加されます。

システムモニターダッシュボードでカメラタイルまたはサーバータイルを編集

別の監視パラメータを用いてカメラまたはサーバーをモニターしたい場合は、これらを調整することができます。

1. **[サイトナビゲーション]**ペインで、**[システムダッシュボード] > [システムモニター]**を選択します。
2. **[システムモニター]**ウィンドウで**[カスタマイズ]**を選択します。
3. **[ダッシュボードのカスタマイズ]**ウィンドウが表示されたら、**[サーバータイル]**または**[カメラタイル]**で変更したいタイルを選択し、**[編集]**を選択します。
4. **[ダッシュボードサーバー/カメラタイルの編集]**ウィンドウで、監視パラメータを変更したいすべてのカメラまたはサーバー、

カメラまたはサーバーのグループ、あるいは個々のカメラまたはサーバーを選択します。

5. **[監視パラメータ]**で、モニターしたい監視パラメータを選択します。
6. **[OK]** を選択します。

システムモニターダッシュボードからカメラタイルまたはサーバータイルを削除

タイル表示のハードウェアをモニターする必要がなくなった場合は、タイルを削除できます。

1. **[サイトナビゲーション]**ペインで、**[システムダッシュボード] > [システムモニター]**を選択します。
2. **[システムモニター]**ウィンドウで**[カスタマイズ]**を選択します。
3. **[ダッシュボードのカスタマイズ]**ウィンドウが表示されたら、**[サーバータイル]**または**[カメラタイル]**で変更したいタイルを選択します。
4. **削除** を選択します。

ハードウェアの状態変化を決めるしきい値を編集

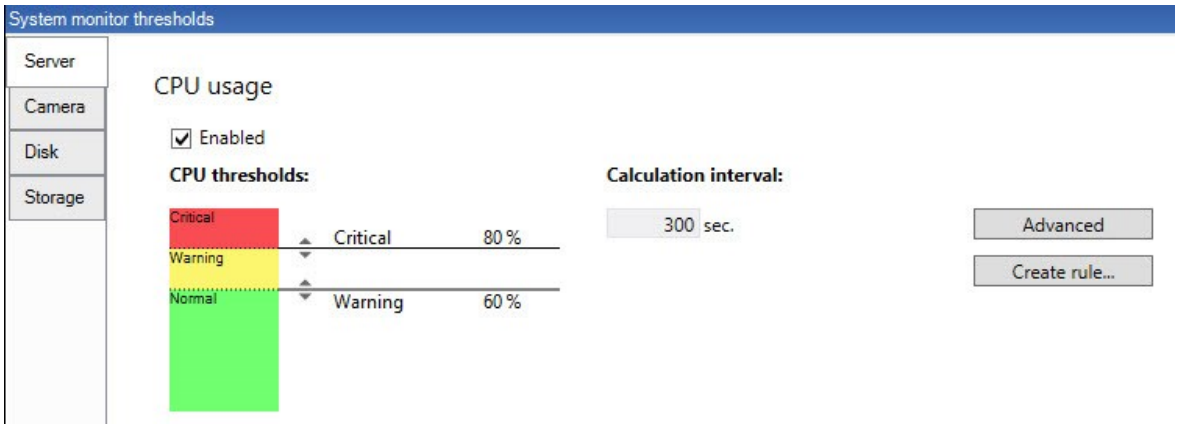
[システムモニターダッシュボード]では、どのような状況でハードウェアの状態が3種類の間で変化するかを決めるしきい値を編集できます。詳細については、「278ページのシステムモニターしきい値(説明付き)」を参照してください。

異なる種類のハードウェアに対してしきい値を変更できます。詳細については、「525ページのシステムモニターしきい値(システムダッシュボードノード)」を参照してください。

デフォルトでは、同種のハードウェアの全ユニット(すべてのカメラやサーバーなど)のしきい値が表示されるよう設定されています。これらのデフォルトのしきい値は編集することができます。

また、一部のカメラで他のカメラよりも高い**ライブFPS**または**レコーディングFPS**が使用されるよう、個々のサーバーまたはカメラ、あるいはこれらのサブセットのしきい値を設定するといったことも可能です。

1. **[サイトナビゲーション]**ペインで、**[システムダッシュボード] > [システムモニターしきい値]**を選択します。
2. 該当するハードウェアがまだ有効になっていない場合は、同ハードウェアの**[有効]**チェックボックスを選択します。以下の値が例として挙げられます。



3. しきい値コントロールスライダを上下にドラッグし、しきい値を増減します。しきい値コントロールに表示される各ハードウェアで使用可能なスライダは2つあり、これによって**[正常]**、**[警告]**、**[重大]**状態が識別されます。
4. 計算間隔のための値を入力、あるいはデフォルトの値を保持します。
5. それぞれのハードウェアで値を設定したい場合は、**[詳細]**を選択します。
6. 特定のイベントに対する、あるいは特定のタイムインターバルにおけるルールを設定したい場合は、**[ルールの作成]**を選択します。
7. しきい値レベルおよび計算間隔を設定したら、メニューから**[ファイル] > [保存]**を選択します。

システムのエビデンスロックを表示

[システムダッシュボード]ノードの**エビデンスロック**には、現在監視システム内で保護されている全データの概要が表示されます。

いつ誰が作成したかなどを基準にフィルターをかけることで、エビデンスロックを検索します。

1. **[サイトナビゲーション]**ペインで、**[システムダッシュボード] > [エビデンスロック]**を選択します。
2. 該当するエビデンスロックの概要を取得して、その検索を行います。エビデンスロックに関連したさまざまなメタデータを基準にフィルターをかけ、これらを並べ替えます。

[エビデンスロック]ウィンドウに表示される情報はすべてスナップショットとなります。F5を押すと画面が更新されます。

システム構成が記されたレポートを印刷

VMSシステムのインストールおよび構成には数多くの設定が伴うため、これらについて記録しなくてはならない場合があります。また、インストールおよび初回の構成以降、あるいは過去数か月のうちに設定にどのような変更を加えたかをすべて記憶することは、時間の経過とともに困難になっていきます。そのために、構成の内容が記されたレポートを印刷することができるようになっています。

設定レポート(PDFフォーマット)を作成する際には、システムのあらゆる要素をレポートに含めることができます。例えば、ライセンス、デバイス設定、アラーム設定などを含めることが可能です。**[機密データを除去]**オプションを選択することで、GDPRに準拠したレポートを作成できます(このオプションはデフォルトで有効となっています)。フォント、ページ設定、表紙ページをカスタマイズすることも可能です。

1. **[システムダッシュボード]**を展開して、**[設定レポート]**を選択します。
2. レポートに追加または除去したい要素を選択します。
3. **オプション**:表紙ページを含めるよう選択した場合は、**[表紙ページ]**を選択して表紙ページの情報をカスタマイズします。ウィンドウが表示されるので、必要な情報を入力します。
4. **[フォーマット]**を選択して、フォント、ページのサイズ、余白をカスタマイズします。表示されるウィンドウで、必要な設定を選択します。
5. エクスポートする準備ができたら**[エクスポート]**をクリックし、レポートの名前と保存場所を選択します。

設定レポートを作成できるのは、VMSシステムで管理者権限を持つユーザーのみとなります。

メタデータ

メタデータ検索カテゴリおよび検索フィルターを表示/非表示にする

管理者権限を持つXProtect Management Clientのユーザーは、Milestoneでデフォルトの XProtect Smart Client メタデータ検索カテゴリと検索フィルターを表示/非表示に設定できます。デフォルトでは、これらの検索カテゴリ/検索フィルターは非表示になっています。お使いのビデオ監視システムが要件を満たしている場合、これらの表示を有効利用できます(「531ページのメタデータ検索の要件」を参照)。

この設定は全XProtect Smart Clientユーザーに適用されます。

この設定は以下の可視性には影響しません。

- 他の非メタデータMilestone検索カテゴリ/検索フィルター(**モーション**、**ブックマーク**、**アラーム**、**イベント**など)
- サードパーティの検索カテゴリ/検索フィルター

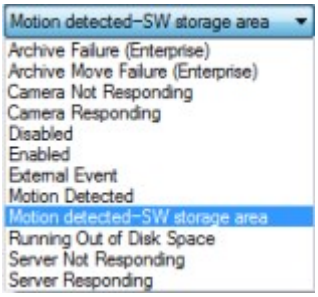
1. XProtectManagementClientの [**サイトナビゲーション**] ペインで、 [**メタデータの使用**] > [**メタデータ検索**] の順に選択します。
2. [**メタデータ検索**] ペインで、可視性設定を変更したい検索カテゴリを選択します。
3. 検索カテゴリ/検索フィルターの可視性を有効にするには、該当するチェックボックスをオンにします。検索カテゴリ/検索フィルターの可視性を無効にするには、チェックボックスをオフにします。

アラーム

アラームの追加

アラームを定義するには、アラーム定義を作成する必要があります。ここでは、アラームをトリガーするアイテム、オペレータが実行する必要がある作業の手順、アラームを停止させる操作やタイミングなどを指定します。設定の詳細については、アラーム定義(アラームノード) を参照してください。

1. **サイトナビゲーション**ペインで、**アラーム**を展開し、**アラーム定義**を右クリックします。
2. **新規追加**を選択します。
3. 次のプロパティを入力します:
    - **名前**: アラーム定義の名前を入力します。アラーム定義が一覧表示されるたびに、アラーム定義の名前が表示されます。
    - **手順**: アラームを受信するオペレータの手順を作成できます。
    - **イベントのトリガー**: ドロップダウンメニューを使用して、アラームがトリガーされる時に使用されるイベントタイプとイベントメッセージを選択します。

      選択可能なトリガーイベントのリスト。アナリティクスイベントを使用して、ハイライトされたイベントが作成され、カスタマイズされます。
    - **ソース**: アラームをトリガーするためのイベントが発生するカメラおよびその他のデバイスを選択します。選択できるオプションは、選択したイベントのタイプにより異なります。
    - **時間設定**: 特定の期間中にアラームをアクティブ化する場合は、ラジオボタンを選択してから、ドロップダウンメニューでタイムインターバルを選択します。
    - **イベントベース**: イベントによってアラーム定義を有効化する場合は、ラジオボタンを選択し、アラーム定義を開始するイベントを指定します。また、アラーム定義を無効にするイベントを指定する必要があります。
4. **[時間制限]**ドロップダウンメニューで、オペレータのアクションが必要なときの時間制限を指定します。
5. **[トリガーされたイベント]**ドロップダウンメニューで、時間制限が経過したときにトリガーするイベントを指定します。
6. 関連するカメラや初期アラーム所有者などの追加設定を指定します。

個々のアラーム定義の権限の変更

特定のユーザーのみにアラームを表示および管理させたい場合は、XProtect Management Clientからアラーム定義の権限を変更できます。これにより、以下が保証されます。

- ユーザーは自分に関連するアラームのみを受け取る。
- 権限のないユーザーはアラームに対応できない。

役割を使用して、すべてのアラーム定義について、同じ権限を持つユーザーをグループ分けできます。

アラーム定義の権限を変更するには、以下を実行します。

1. **サイトナビゲーション**ペインで、**セキュリティ**を展開し、権限を変更する役割を選択します。
2. **アラーム** タブで**アラーム定義**を展開し、定義したアラームのリストを表示します。
3. 権限を変更するには、アラーム定義を選択します。

暗号化を有効にする

マネジメントサーバーとの間で暗号化を有効にする

以下のタイプのリモートサーバーがある場合は、マネジメントサーバーとData Collector関連サーバー間の双方向接続を暗号化できます。

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

システムに複数のレコーディングサーバーまたはリモートサーバーが含まれている場合は、これらすべてで暗号化を有効化する必要があります。

> サーバーグループの暗号化を設定する場合は、同じCA証明書に属する証明書で有効にする必要があります。暗号化が無効な場合は、サーバーグループのあらゆるコンピュータで無効にしなくてはなりません。

前提条件:

- サーバー認証証明書がマネジメントサーバーをホストしているコンピュータで信頼されていること

まず、マネジメントサーバーで暗号化を有効にします。

手順:

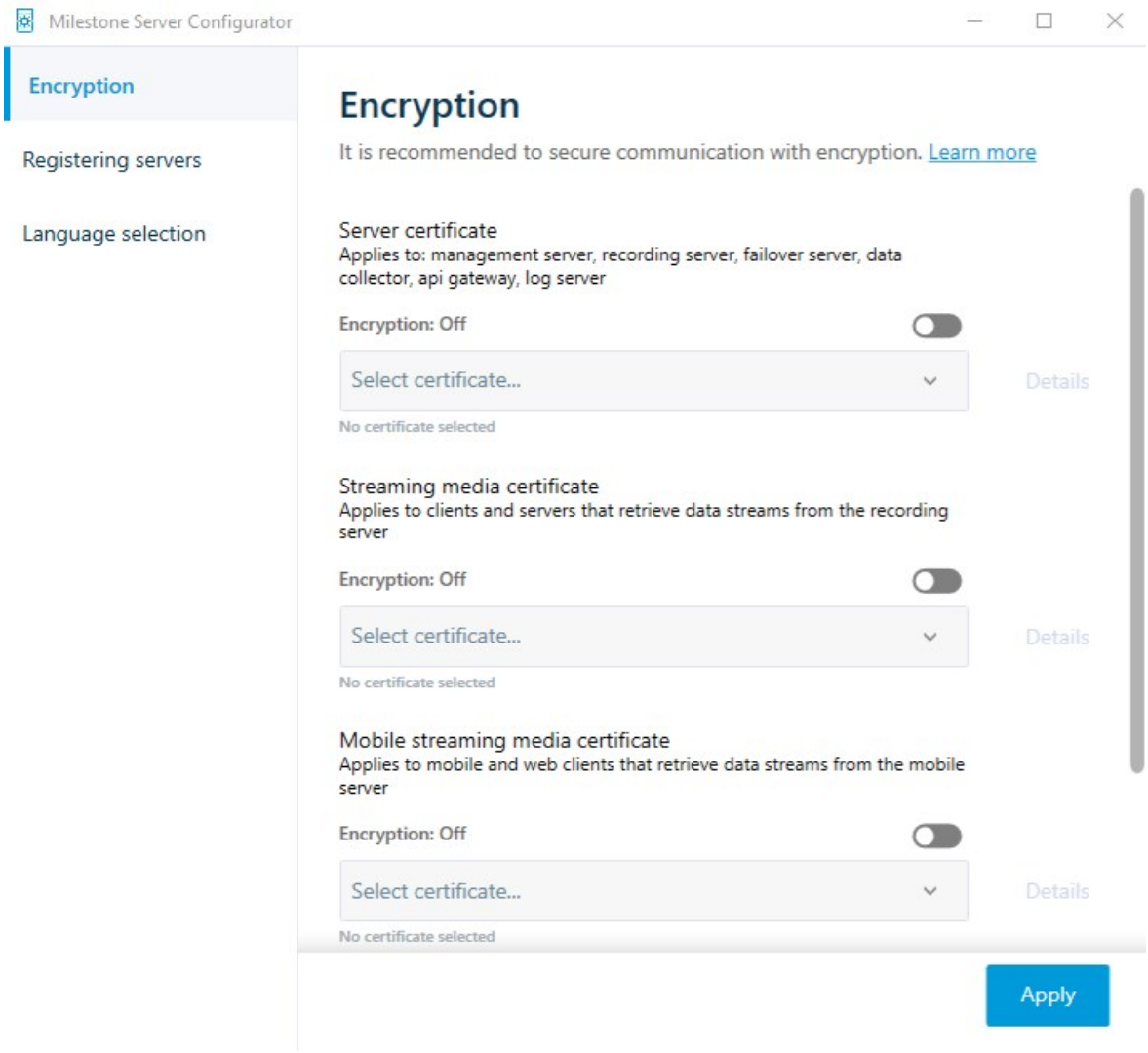
1. マネジメントサーバーがインストールされているコンピュータで、以下から**Server Configurator**を開きます。
   - Windowsのスタート メニュー

   または

   - Management Server Manager、コンピュータのタスクバーでManagement Server Managerアイコンを右クリック
2. **Server Configurator**の**サーバー証明書**で、**暗号化**をオンにします。
3. **証明書を選択**をクリックすると、プライベートキーを持つ、Windows証明書ストアでローカルコンピュータにインストールされている証明書の一意のサブジェクト名のリストが開きます。

4. 証明書を選択して、レコーディングサーバー、マネジメントサーバー、フェールオーバーサーバー、およびData Collector serverの間で通信を暗号化します。

   詳細を選択すると、選択した証明書のWindows証明書ストア情報が表示されます。



5. **適用**をクリックします。

暗号化を有効にするための次のステップは、各レコーディングサーバーと、Data Collector(Event Server、Log Server、LPR Server および Mobile Server) のある各サーバーで暗号化設定をアップデートすることです。

詳細については、「286ページのレコーディングサーバーまたはリモートサーバーのサーバー暗号化を有効にする」を参照してください。

レコーディング サーバーまたはリモート サーバーのサーバー暗号化を有効にする

マネジメントサーバーとレコーディングサーバー、またはData Collectorを使用している他のリモートサーバー間では双方向接続を暗号化できます。

システムに複数のレコーディングサーバーまたはリモートサーバーが含まれている場合は、これらすべてで暗号化を有効に設定する必要があります。

詳細については、XProtect VMSの保護方法に関する証明書ガイドを参照してください。

> サーバーグループの暗号化を設定する場合は、同じCA証明書に属する証明書で有効にする必要があります。暗号化が無効な場合は、サーバーグループのあらゆるコンピュータで無効にしなくてはなりません。

前提条件:

- マネジメントサーバーで暗号化が有効になっています。285ページのマネジメントサーバーとの間で暗号化を有効にするを参照してください。

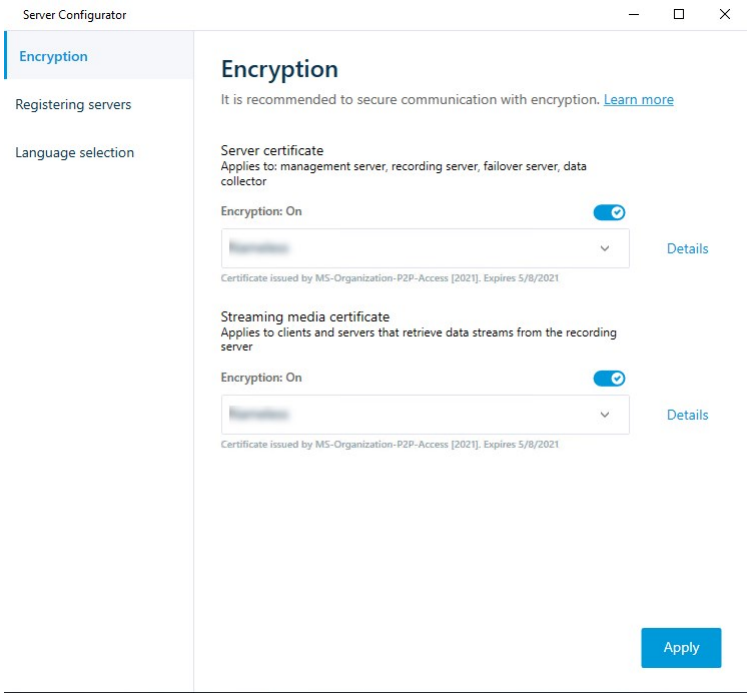
1. Management ServerまたはRecording Serverがインストールされているコンピュータで、以下から**Server Configurator**を開きます:
   - Windowsのスタートメニュー

   または

   - サーバーマネージャー(コンピューターのタスクバーのサーバーマネージャーアイコンを右クリック)
2. **Server Configurator**の**サーバー証明書**で、**暗号化**をオンにします。
3. **証明書を選択**をクリックすると、プライベートキーを持つ、Windows証明書ストアでローカルコンピュータにインストールされている証明書の一意のサブジェクト名のリストが開きます。
4. レコーディングサーバー、マネジメントサーバー、フェールオーバーサーバー、データコレクターサーバー間で通信を暗号化するために証明書を選択します。

   詳細を選択すると、選択した証明書のWindows証明書ストア情報が表示されます。

   Recording Serverサービスユーザーには秘密キーへのアクセスが付与されています。この証明書は、すべてのクライアントで信頼されている必要があります。



5. **適用**をクリックします。

証明書を適用すると、レコーディングサーバーは停止してから再起動します。Recording Serverサービスを停止すると、レコーディングサーバーの基本設定を確認したり、変更したりしている間、ライブビデオを表示できなくなります。

イベントサーバーの暗号化を有効に設定

イベントサーバーと通信するコンポーネント(LPR Serverなど) とイベントサーバー間の双方向接続を暗号化できます。

サーバーグループの暗号化を設定する場合は、同じCA証明書に属する証明書で有効にする必要があります。暗号化が無効な場合は、サーバーグループのあらゆるコンピュータで無効にしなくてはなりません。

前提条件:

- サーバー認証証明書が、イベントサーバーをホストしているコンピューターで信頼されていること

まず、イベントサーバーで暗号化を有効化します。

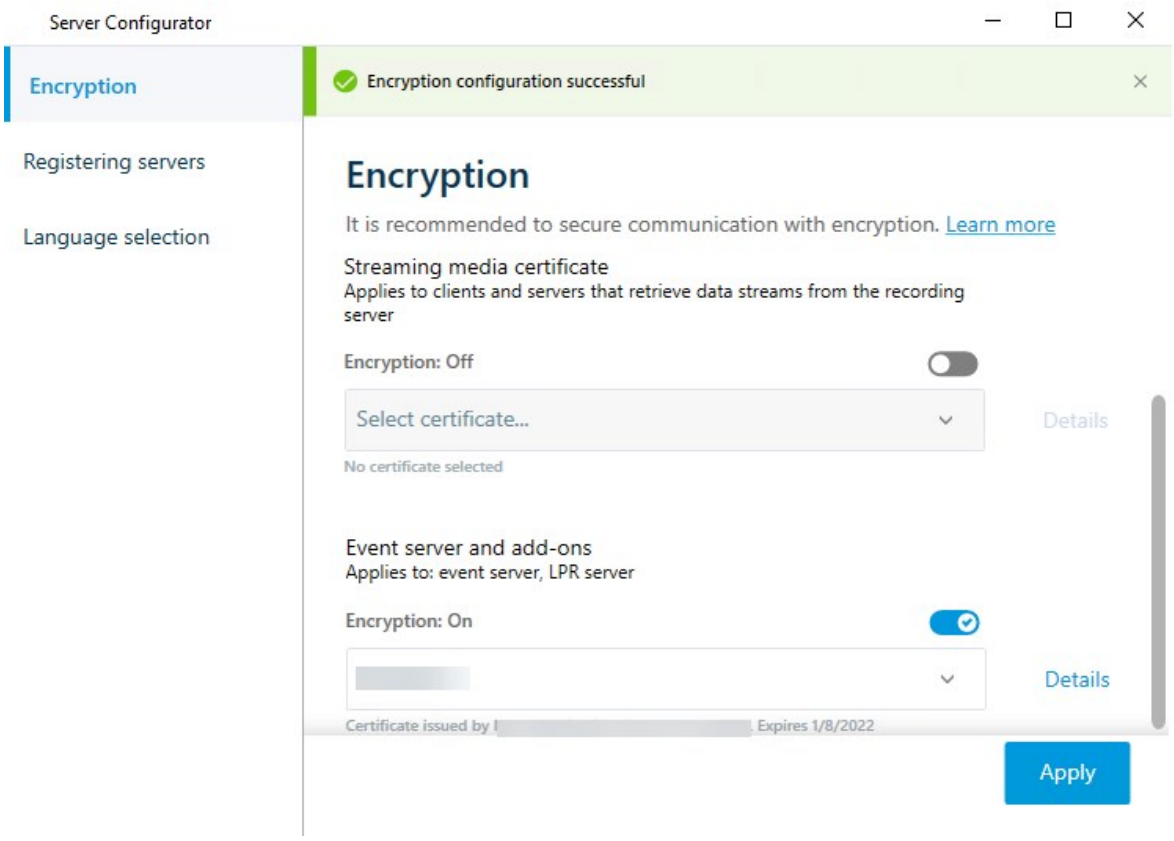
手順:

1. イベントサーバーがインストールされているコンピュータで、以下の場所から**Server Configurator**を開きます。
   - Windowsのスタート メニュー

   または

   - Event Server、コンピュータのタスクバーでEvent Serverアイコンを右クリック
2. **Server Configurator**の**イベントサーバー& アドオン**で**暗号化**をオンに設定します。
3. **証明書を選択**をクリックすると、プライベートキーを持つ、Windows証明書ストアでローカルコンピュータにインストールされている証明書の一意のサブジェクト名のリストが開きます。
4. 証明書を選択し、イベントサーバーと関連アドオン間の通信を暗号化します。

   詳細を選択すると、選択した証明書のWindows証明書ストア情報が表示されます。



5. **適用**をクリックします。

暗号化を有効化するための次のステップは、関連する各拡張機能で暗号化の設定を更新することですLPR Server。

クライアントとサーバーに対して暗号化を有効にする

レコーディングサーバーからデータをストリーミングするクライアントおよびサーバーへのレコーディングサーバーからの接続を暗号化できます。

サーバーグループの暗号化を設定する場合は、同じCA証明書に属する証明書で有効にする必要があります。暗号化が無効な場合は、サーバーグループのあらゆるコンピュータで無効にしなくてはなりません。

前提条件:

- 使用されるサーバー認証は、レコーディング サーバーからデータストリームを取得するサービスを実行しているすべてのコンピュータで信頼されています
- XProtect Smart Clientと、レコーディング サーバーからデータストリームを取得するサービスはすべて、バージョン2019 R1以降でなくてはなりません。
- MIPSDK以前の2019R1バージョンを使用して作られているサードパーティソリューションはアップデートする必要があります。

手順:

1. レコーディング サーバーがインストールされているコンピュータで、以下から**Server Configurator**を開きます。
   - Windowsのスタート メニュー

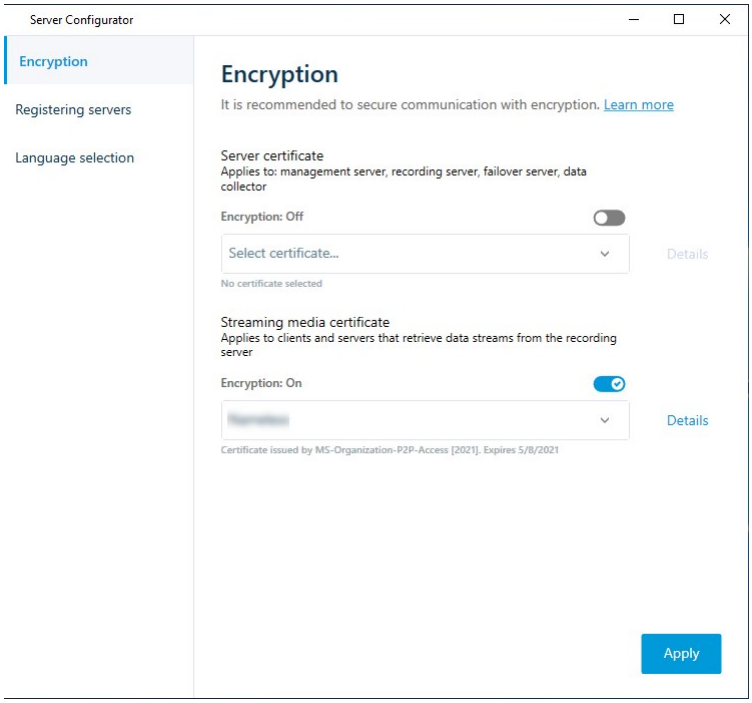
   または

   - Recording Server Manager: コンピュータのタスクバーでRecording Server Managerアイコンを右クリック
2. **Server Configurator**の**ストリーミング メディア証明書**で、**暗号化**をオンにします。
3. **証明書を選択**をクリックすると、プライベートキーを持つ、Windows証明書ストアでローカルコンピュータにインストールされている証明書の一意のサブジェクト名のリストが開きます。
4. レコーディングサーバーからデータストリームを受け取るクライアントとサーバー間の通信を暗号化するために証明書を選択します。

   詳細を選択すると、選択した証明書のWindows証明書ストア情報が表示されます。

   Recording Serverサービス ユーザーには秘密キーへのアクセスが付与されています。この証明書は、すべてのクライア

ントで信頼されている必要があります。



5. **適用**をクリックします。

> 証明書を適用すると、レコーディングサーバーは停止してから再起動します。Recording Serverサービスを停止すると、レコーディングサーバーの基本設定を確認したり、変更したりしている間、ライブビデオを表示できなくなります。

レコーディングサーバーで暗号化が用いられているかどうか確認する方法については、「クライアントの暗号化ステータスを表示」を参照してください。

モバイルサーバーで暗号化を有効にする

HTTPSプロトコルを使用して、モバイルサーバーとクライアント間の安全な接続を確立する場合、サーバー上で有効な証明書を適用する必要があります。この証明書は、証明書所有者が安全な接続を確立する権限を持っていることを裏付けるものです。

詳細については、XProtect VMSの保護方法に関する証明書ガイドを参照してください。

> サーバーグループの暗号化を設定する場合は、同じCA証明書に属する証明書で有効にする必要があります。暗号化が無効な場合は、サーバーグループのあらゆるコンピュータで無効にしなくてはなりません。

CA(証明書システム管理者)によって発行される証明書は証明書チェーンを持っており、このチェーンのルートにはCAルート証明書があります。デバイスまたはブラウザがこの証明書をみるとき、これはそのルート証明書とOS上にあらかじめインストールされているもの(Android、iOS、Windowsなど)とを比較します。ルート証明書があらかじめインストールされている証明書リストのなかにある場合は、サーバーへの接続が十分に安全であることをOSがユーザーに保証します。これらの証明書はドメイン名に対して発行され、無料です。

手順:

1. モバイル サーバーがインストールされているコンピュータで、以下から**Server Configurator**を開きます:
   - Windowsのスタート メニュー

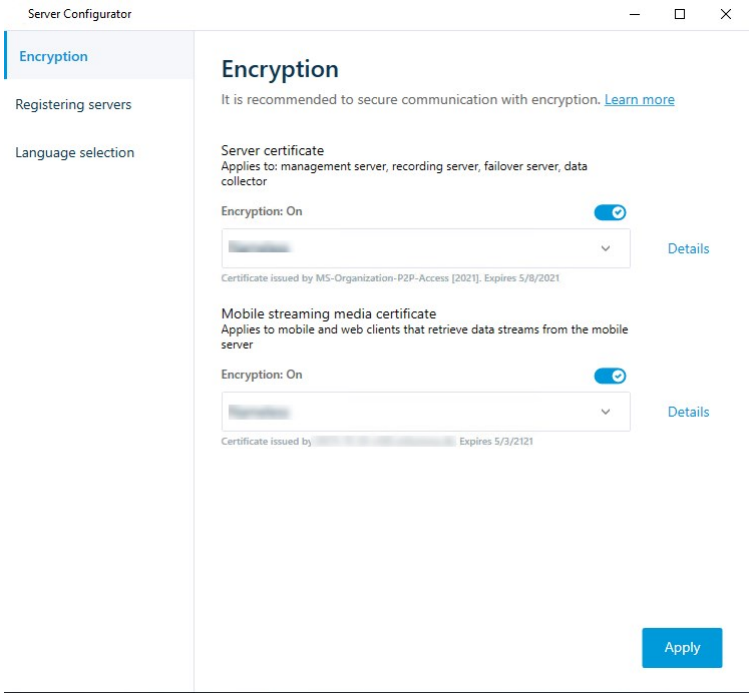
   または

   - Mobile Server Manager: コンピュータのタスクバーでMobile Server Managerアイコンを右クリック
2. **Server Configurator**の**[モバイル ストリーミング メディア証明書]**で**[暗号化]**をオンにします。
3. **証明書を選択**をクリックすると、プライベートキーを持つ、Windows証明書ストアでローカルコンピュータにインストールされている証明書の一意のサブジェクト名のリストが開きます。
4. XProtect MobileクライアントおよびXProtect Web Clientとモバイル サーバーとの通信を暗号化するための証明書を選択します。

   詳細を選択すると、選択した証明書のWindows Certificate Store情報が表示されます。

   Mobile Serverサービス ユーザーには秘密キーへのアクセスが付与されています。この証明書はあらゆるクライアントで

信頼される必要があります。



5. **適用**をクリックします。

証明書を適用すると、Mobile Serverサービスが再起動します。

Milestone Federated Architecture

フェデレーテッドサイトを実行するためのシステムの設定

Milestone Federated Architectureの動作のためにシステムを準備するには、マネジメントサーバーのインストール時に一定の選択が必要です。ITインフラストラクチャの設定によって、3つの異なる代替方法のいずれかを選択します。

代替方法1: 同じドメインからサイトに接続する(共通ドメインユーザーを使用)

マネジメントサーバーのインストール前に、共通ドメインユーザーを作成し、フェデレーテッドサイト階層に関与するすべてのサーバー上の管理者としてこのユーザーを設定する必要があります。サイトにどのように接続するかは、作成されたユーザーアカウントに応じて異なります。

Windowsユーザーアカウントを使用

1. マネジメントサーバーとして使用されるサーバーに製品をインストールし、**カスタム**を選択します。
2. ユーザーアカウントを使用して、Management Serverのインストールを選択します。選択したユーザーアカウントは、すべてのマネジメントサーバーで使用される管理者アカウントである必要があります。フェデレーテッドサイト階層で他のマネジメントサーバーをインストールする場合は、同じユーザーアカウントを使用する必要があります。
3. インストールを終了します。手順1～3を繰り返し、フェデレーテッドサイト階層に追加する他のシステムをインストールします。
4. サイトを階層に追加します(295ページのサイトを階層に追加を参照)。

Windows組み込みユーザーアカウントを使用(ネットワークサービス)

1. マネジメントサーバーとして使用される最初のサーバーに製品をインストールし、**単一のコンピュータ**または**カスタム**を選択します。これにより、ネットワークサービスアカウントを使用して、マネジメントサーバーがインストールされます。このステップを、フェデレーテッドサイト階層のすべてのサイトについて繰り返します。
2. フェデレーテッドサイト階層の中央サイトにするサイトにログインします。
3. Management Clientで、**セキュリティ> 役割 > 管理者**を展開します。
4. **ユーザーとグループ**タブで**追加**をクリックして、**Windowsユーザー**を選択します。
5. ダイアログボックスで、オブジェクトタイプとして**コンピュータ**を選択し、フェデレーテッドサイトのサーバー名を入力して**OK**をクリックし、中央サイトの**管理者**の役割にサーバーを追加します。この方法ですべてのフェデレーテッドサイトのコンピュータを追加するまでこの手順を繰り返し、アプリケーションを終了します。
6. 各フェデレーテッドサイトにログインし、同じ方法で次のサーバーを**管理者**の役割に追加します。
   - 親サイトサーバー。
   - このフェデレーテッドサイトに直接接続する子サイトサーバー。
7. サイトを階層に追加します(295ページのサイトを階層に追加を参照)。

代替方法2:異なるドメインからのサイトの接続

ドメインを超えてサイトに接続するには、これらのドメインが互いに信頼関係にあることを確認します。Microsoft Windowsドメイン構成で相互に信頼するようにドメインを設定します。フェデレーテッドサイト階層で各サイトの異なるドメイン間に信頼関係を確立した場合は、代替方法1と同じ説明に従ってください。信頼されるドメインの設定方法の詳細については、Microsoft Webサイト(https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481(v=technet.10)/)を参照してください。

> Milestoneは、Milestone Interconnectを使用して、接続されたマルチサイトシステムと複数のドメインを作成することを推奨しています。

代替方法3: ワークグループでのサイトの接続

ワークグループ内でサイトを接続する場合、フェデレーテッドサイト階層で接続されるすべてのサーバーに同じ管理者アカウントが存在する必要があります。システムをインストールする前に管理者アカウントを定義する必要があります。

1. **共通管理者アカウントを使用して、**Windowsへログインします。
2. 製品のインストールを開始し、**カスタム**をクリックします。
3. 共通システム管理者アカウントを使用して、Management Serverをインストールするように選択します。
4. インストールを終了します。手順1～4を繰り返し、接続する他のすべてのシステムをインストールします。これらすべてのシステムで、共通の管理者アカウントをインストールする必要があります。
5. サイトを階層に追加します(295ページのサイトを階層に追加を参照)。

Milestoneは、サイトがドメインの一部でない場合、Milestone Interconnectを使用して接続されたマルチサイトシステムを作成することを推奨しています。

ドメインとワークグループを混在させることはできません。これは、ドメインからワークグループのサイトへ、あるいはその逆に接続することはできないことを意味します。

サイトを階層に追加

システムを展開する際に、システムが正しく設定されているなら、最上位サイトとその子サイトの両方に追加できます。

保護されていないサイトを追加するときはMilestone Federated Architecture、Management Clientの**ツール > オプション > 一般設定**で、**サーバーへの保護されていない接続を許可する**が有効になっていることを確認してください。

1. **フェデレーテッドサイト階層**ペインを選択します。
2. 子サイトを追加するサイトを選択し、右クリックして、**サイトを階層に追加**をクリックします。
3. 要求されたサイトのURLを**サイトを階層に追加**ウィンドウに入力し、**OK**をクリックします。
4. 親サイトがリンクリクエストを子サイトへ送信し、しばらくすると2つのサイトの間のリンクが**フェデレーテッドサイト階層**ペインに追加されます。
5. 子サイトの管理者による許可をリクエストすることなく新しい子サイトへのリンクを確立できる場合は、手順7に進みます。

   それ以外の場合は、子サイトの管理者がリクエストを許可するまで子サイトには許可の待機アイコンが表示されます。
6. 子サイトのシステム管理者が親サイトのからのリンクリクエストを承認していることを確認します(296ページの階層に含むことを許可を参照)。
7. 新しい親/子リンクが確立され、**フェデレーテッドサイトの階層**ペインが新しい子サイトのアイコンで更新されます。

階層に含むことを許可

管理者が子サイトへの管理者権限を持っていない潜在的な親サイトからのリンク要求を子サイトが受信すると、子サイトに承認待ちアイコンが表示されます。

リンク要求を許可するには:

1. サイトにログインします。
2. **[フェデレーテッドサイト階層]** ペインで、サイトを右クリックし、**[階層に含むことを許可]** を選択します。

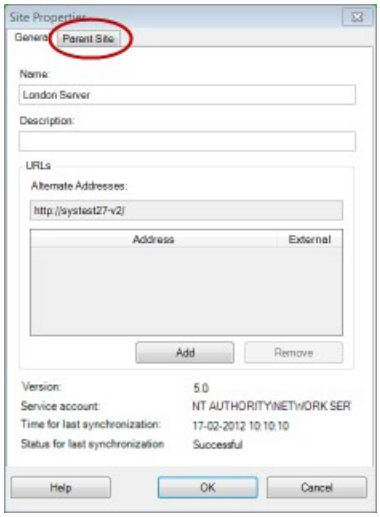
   サイトでXProtect Expertバージョンが実行されている場合は、**サイトナビゲーション**ペインでサイトを右クリックします。
3. **はい**をクリックします。
4. 新しい親/子リンクが確立され、**フェデレーテッドサイト階層**ペインが、選択されたサイトの標準サイトアイコンで更新されます。

> 親サイトから離れている子への変更はすべて、**フェデレーテッドサイト階層**ペインに反映されるまで時間がかかる場合があります。

サイトプロパティの設定

ホームサイトとその子サイトのプロパティを表示し、編集することがおそらく可能です。

1. Management Clientでは、**[フェデレーテッドサイト階層]**ペイン内で、該当するサイトを選択し、右クリックして、**[プロパティ]**を選択します。



2. 必要であれば、以下を変更します。

   一般タブ(545ページの一般タブを参照)

   親サイトタブ(546ページの親サイトタブを参照)**(子サイトでのみ利用可能)**

   > 同期化の問題のため、リモートの子に対して行われた変更が**サイトナビゲーションペイン**に反映されるまで多少時間のかかる場合があります。

サイト階層の更新

システムは、すべてのレベルの親/子設定を通じて、定期的に階層の自動同期化を実行します。反映される変更をすぐに階層で確認したくて、次回の自動同期化まで待ちたくない場合は、手動で更新することができます。

手動での更新を実行するために、サイトにログインする必要はありません。前回の同期化以降にこのサイトによって保存されている変更だけが、更新で反映されます。これは、階層の下の方で行われた変更は、変更がまだサイトに到達していない場合、手動更新では反映されないことを意味しています。

1. 関連するサイトにログインします。
2. **[フェデレーテッドサイト階層]**ペインでトップのサイトを右クリックし、**サイト階層の更新**をクリックします。

   これには、数秒かかります。

階層の他のサイトへのログイン

他のサイトにログインし、これらのサイトを管理できます。ログインしたサイトがホームサイトです。

1. **フェデレーテッドサイト階層**ペインで、ログインするサイトを右クリックします。
2. **サイトにログイン**をクリックします。

   そのサイトのManagement Clientが表示されます。
3. ログイン情報を入力して、**OK**をクリックします。
4. ログイン後、そのサイトの管理タスクを実行できます。

子サイトのサイト情報をアップデート

> このセクションは、XProtect CorporateまたはXProtect Expert2014以降を使用なさっている場合にのみ該当します。

子サイトの数が多い大規模なMilestone Federated Architectureのセットアップでは、概要がおおまかになり、各子サイトシステム管理者の連絡先を見つけるのが難しくなることがあります。

このため、各子サイトに情報をさらに追加できます。この情報はその後、中央サイトのシステム管理者が利用できるようになります。

フェデレーテッドサイト階層ペインでサイト名の上にマウスを動かすと、そのサイトに関する情報が表示されます。サイトに関する情報を更新するには：

1. サイトにログインします。
2. **サイトナビゲーション**ペインをクリックして、**サイト情報**を選択します。
3. **編集**をクリックして、各カテゴリに関連情報を追加します。

階層からのサイトの分離

親サイトからサイトを分離すると、サイト間でのリンクは外れます。中央サイト、サイト自体、または親サイトからサイトを分離できます。

1. **フェデレーテッドサイト階層**ペインで、サイトを右クリックし、**階層からサイトを分離**を選択します。
2. **はい**をクリックして**フェデレーテッドサイト階層**ペインを更新します。

   分離するサイトに子サイトがある場合、階層のこのブランチの新しいトップサイトになり、通常のサイトのアイコンがトップサイトのアイコンに変わります。
3. **OK**をクリックします。

階層への変更は、手動更新または自動同期化後に反映されます。

Milestone Interconnect

リモートサイトを中央Milestone Interconnectサイトに追加

ハードウェアの追加ウィザードを使用して、リモートサイトを中央サイトに追加します。

要件

- 十分なMilestone Interconnectカメラライセンス(86ページのMilestone Interconnectおよびラインセンスを参照)。
- 中央XProtectシステムがアクセスできる必要のあるデバイスの権限があるユーザーアカウント(基本ユーザー、ローカルWindowsユーザー、WindowsActiveDirectoryユーザー)を含む別の設定済みかつ動作中のXProtectCorporateシステム
- リモートサイトで使用されるポートへのアクセスまたはポート転送による、中央XProtect Corporateサイトとリモートサイト間のネットワーク接続

リモートサイトを追加するには：

1. 中央サイトで、**サーバー**を展開し、**レコーディングサーバー**を選択します。
2. **概要**ペインで、該当するレコーディングサーバーを展開して右クリックします。
3. **ハードウェアの追加**を選択して、ウィザードを開始します。
4. 最初のページで、**[アドレス範囲のスキャン]**または**[手動]**を選択して、**[次へ]**をクリックします。

5. ユーザー名とパスワードを指定します。ユーザーアカウントはリモートシステムで定義されている必要があります。**追加**をクリックして、必要なだけユーザー名とパスワードを追加できます。準備ができたら、**次へ**をクリックします。
6. スキャンに使用するドライバを選択します。この場合、Milestoneドライバ間で選択します。**次へ**をクリックします。
7. スキャンするIPアドレスとポート番号を指定します。デフォルトはポート80です。**次へ**をクリックします。

   システムがリモートサイトを検出している間、お待ちください。ステータスインジケータに、検出プロセスが表示されます。正常に検出された場合は、**成功**メッセージが**ステータス**列に表示されます。追加できなかった場合は、**失敗**エラーメッセージをクリックすると、その理由を確認できます。
8. 選択すると、正常に検出されたシステムを有効または無効にします。**次へ**をクリックします。
9. システムがハードウェアを検出し、デバイス固有の情報を収集している間、お待ちください。**次へ**をクリックします。
10. 検出が成功したハードウェアおよびデバイスを有効にするか、無効にするかを選択します。**次へ**をクリックします。
11. デフォルトグループを選択します。**終了**をクリックします。
12. インストール後、**概要**ペインにシステムとデバイスが表示されます。

    リモートサイト上で選択されたユーザーのユーザー権限によって、中央サイトではすべてのカメラおよび機能、またはカメラや機能のサブセットへのアクセス権が得られます。

ユーザー権限を割り当て

役割を作成して機能にアクセスを割り当てることで、他のカメラと同様に、相互接続されているカメラにユーザー権限を設定できます。

1. 中央サイトの**[サイトナビゲーション]**ペインで、**[セキュリティ]**を展開して**[役割]**を選択します。
2. [概要]ペインで組み込み管理者役割を右クリックし、**[役割の追加]**を選択します(「役割の追加と管理」を参照)。
3. 役割に名前を付け、**デバイス**タブの設定(デバイスタブ(役割)を参照)と、**リモート録画**タブの設定(リモート録画タブ(役割)を参照)を行います。

リモートサイトのハードウェアの更新

カメラやイベントの追加や削除など、リモートサイトで構成が変更された場合は、中央サイトで構成を更新し、リモートサイトで新しい構成を反映する必要があります。

1. 中央サイトで、**サーバー**を展開し、**レコーディングサーバー**を選択します。
2. **概要**ペインで、必要なレコーディングサーバーを展開して、該当するリモートシステムを選択します。右クリックします。
3. **ハードウェアの更新**を選択します。これにより、**ハードウェアの更新**ダイアログボックスが開きます。
4. このダイアログボックスには、Milestone Interconnect設定が最後に確立または更新されてから、リモートシステムで行われたすべての変更(デバイスの削除、更新、および追加)のリストが表示されます。**確認**をクリックして、中央サイトにこれらの変更を更新します。

リモートサイトのカメラからの直接再生を可能にする

中央サイトがリモートサイトと常に接続している場合は、システムを構成し、ユーザーがリモートサイトから直接録画を再生できるようにすることができます。詳細については、「86ページのMilestoneInterconnectの設定(説明付き)」を参照してください。

1. 中央サイトで、**サーバー**を展開し、**レコーディングサーバー**を選択します。
2. **概要**ペインで、必要なレコーディングサーバーを展開して、該当するリモートシステムを選択します。関連するInterconnectで接続されたカメラを選択します。
3. プロパティペインで、**記録**タブを選択し、**リモートシステムから録画を再生**オプションを選択します。
4. ツールバーで**保存**をクリックします。

Milestone Interconnect設定では、中央サイトは、リモートサイトで定義されたプライバシーマスクを無視します。同じプライバシーマスクを適用するには、中央サイトで再定義する必要があります。

リモートサイトのカメラからリモート録画を取得する

中央サイトが常にリモートサイトと接続して**いない**場合は、リモート録画を中央で保存するように構成し、ネットワーク接続が最適なときにリモート録画を取得するように構成できます。詳細については、「86ページのMilestone Interconnectの設定(説明付き)」を参照してください。

ユーザーが実際に録画を取得できるようにするには、関連する役割でこの許可を有効にする必要があります(役割(セキュリティ)を参照)。

システムを構成するには:

1. 中央サイトで、**サーバー**を展開し、**レコーディングサーバー**を選択します。
2. **概要**ペインで、必要なレコーディングサーバーを展開して、該当するリモートシステムを選択します。関連するリモートサーバーを選択します。
3. プロパティペインで**リモート取得**タブを選択し、設定を更新します(408ページのリモート取得タブを参照)。

何らかの原因でネットワークが切断されると、中央サイトは録画シーケンスを失います。ネットワークが再確立された時点で、中央サイトで自動的にリモート録画を取得し、停止した期間をカバーするようにシステムを構成できます。

1. 中央サイトで、**サーバー**を展開し、**レコーディングサーバー**を選択します。
2. **概要**ペインで、必要なレコーディングサーバーを展開して、該当するリモートシステムを選択します。関連するカメラを選択します。
3. プロパティペインで、**録画**タブを選択し、**接続の復旧時に自動的にリモート録画を取得する**オプションを選択します(リモート録画の保存および取得を参照)。
4. ツールバーで**保存**をクリックします。

または、ルールを使用するか、必要な場合はXProtect Smart Clientからリモート録画の取得を開始します。

Milestone Interconnect設定では、中央サイトは、リモートサイトで定義されたプライバシーマスクを無視します。同じプライバシーマスクを適用するには、中央サイトで再定義する必要があります。

リモートサイトからのイベントに応答するように中央サイトを構成する

リモートサイトで定義されたイベントを使用して、中央サイトでルールとアラームを起動し、リモートサイトのイベントに即時応答できます。これには、リモートサイトが接続され、オンラインであることが必要です。イベント数とタイプは、リモートシステムで設定および事前定義されたイベントによって異なります。

サポートされているイベントの一覧は、Milestone Webサイト(https://www.milestonesys.com/) を参照してください。

事前定義されたイベントは削除できません。

要件:

- 起動イベントとしてリモートサイトからユーザー定義または手動イベントを使用する場合は、まずリモートサイトでこれらを作成する必要があります。
- リモートサイトからのイベントのリストが更新されていることを確認してください(299ページのリモートサイトのハードウェアの更新を参照) 。

リモートサイトからユーザー定義または手動イベントを追加する:

1. 中央サイトで、**サーバー**を展開し、**レコーディングサーバー**を選択します。
2. 概要ペインで、該当するリモートサーバーと**イベントタブ**を選択します。
3. このリストには定義済みのイベントが含まれます。**追加**をクリックすると、リモートサイトのユーザー定義または手動イベントがリストに追加されます。

リモートサイトのイベントを使用して、中央サイトのアラームを起動する:

1. 中央サイトで、**アラーム**を展開し、**アラーム定義**を選択します。
2. 概要ペインで、**アラーム定義**を右クリックし、**新規追加**をクリックします。
3. 必要に応じて値を入力します。
4. **起動イベント**フィールドでは、サポートされている定義済みのイベントとユーザー定義イベントから選択できます。
5. **ソース**フィールドで、アラームを起動するリモートサイトを表すリモートサーバーを選択します。
6. 完了したら、構成を保存します。

リモートサイトのイベントを使用して、中央サイトのルールに基づくアクションを起動する:

1. 中央サイトで、**ルールとイベント**を展開し、**ルール**を選択します。
2. 概要ペインで、**ルール**を右クリックし、**ルールの追加**をクリックします。
3. 表示されるウィザードで、**<event>でアクションを実行**を選択します。
4. **ルール説明の編集**領域で、**イベント**をクリックして、サポートされている定義済みイベントとユーザー定義イベント間を選択します。**OK**をクリックします。

5. **デバイス/レコーディングサーバー/マネジメントサーバー**をクリックし、中央サイトでアクションを開始するリモートサイトを表すリモートサーバーを選択します。**OK**をクリックします。
6. **次へ**をクリックして、ウィザードの次のページに進みます。
7. このルールに適用する条件を選択します。条件を選択しない場合は、ルールが常に適用されます。**次へ**をクリックします。
8. **ルール説明の編集**領域で、アクションを選択し、詳細を指定します。**次へ**をクリックします。
9. 必要に応じて、停止条件を選択します。**次へ**をクリックします。
10. 必要に応じて、停止アクションを選択します。**終了**をクリックします。

リモート接続サービス

リモート接続サービス(説明付き)

> 使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

リモート接続サービス機能には、Axis Communicationsが開発したAxis One-clickカメラ接続テクノロジーが組み込まれています。これにより、通常はファイアウォールやルーターネットワーク設定によって接続の開始が妨げられるような外部カメラからも、ビデオ(および音声)を取得できるようになります。実際の通信はセキュアトンネルサーバー(STサーバー)を介して行われます。STサーバーではVPNが使用されます。VPN内では有効なキーを持つデバイスしか動作できません。これは、パブリックネットワークでデータを安全にやり取りするための安全なトンネルとなります。

リモート接続サービスにより、以下が可能になります。

- Axis Dispatchサービス内で認証情報を編集する
- リモートSTサーバーを追加、編集、削除する
- Axis One-clickカメラを登録/登録解除して編集
- Axis One-Clickカメラに関連したハードウェアに移動する

One-Clickカメラ接続用のセキュアトンネルサーバー環境をインストールします

Axis One-clickカメラの接続を使用するには、最初に適切なSTサーバー環境をインストールする必要があります。セキュアトンネルサーバー(STサーバー)環境およびAxis One-clickカメラを使用するには、まず、Axis Dispatchサービスに必要なユーザー名とパスワードをシステムプロバイダーから入手する必要があります。

要件

- Axis Dispatchサービスに必要なユーザー名とパスワードを取得するには、システムプロバイダーに連絡してください。
- カメラがAxisビデオホスティングシステムに対応していることを確認します。AxisのWebサイトで、サポートされているデバイスを確認します(https://www.axis.com/products/axis-guardian)
- 必要に応じて、Axisカメラを最新のファームウェアで更新します。AxisのWebサイトでファームウェアをダウンロードします(https://www.axis.com/support/firmware)

1. それぞれのカメラのホームページから**基本設定>TCP/IP**に移動し、**AVHSを有効化**と**常時**を選択します。
2. マネジメントサーバーで、Milestoneダウンロードページ(https://www.milestonesys.com/downloads/) に進み、**AXIS One-Click**ソフトウェアをダウンロードします。プログラムを実行して、適切なAxisセキュアトンネルフレームワークを設定します。

セキュアトンネルサーバーを追加または編集する

リモート接続サービスの通信は、セキュアトンネルサーバー(STサーバー) を介して行われます。

1. 以下のいずれか1つを実行します。
   - STサーバーを追加するには、**Axisセキュアトンネルサーバー**のトップノードを右クリックし、**Axisセキュアトンネルサーバーを追加**を選択します。
   - STサーバーを編集するには、これを右クリックし、**Axisセキュアトンネルサーバーを編集**を選択します。
2. ウィンドウが開くので関連情報を入力します。
3. **Axis One-Click Connectionコンポーネント**のインストール時に認証情報を使用するよう選択した場合、**認証情報を使用**チェックボックスを選択し、**Axis One-Click Connectionコンポーネント**に使用したものと同じユーザー名とパスワードを入力します。
4. **OK**をクリックします。

新しいAxis One-Clickカメラの登録

1. カメラをSTサーバーに登録するには対象を右クリックし、**Axis One-Clickカメラの登録**を選択します。
2. ウィンドウが開くので関連情報を入力します。
3. **OK**をクリックします。
4. これでカメラが関連STサーバーに表示されます。

カメラは以下のように色分けできます:

色	説明
赤色	初期状態。登録されていますが、まだSTサーバーに接続されていません。
黄色	登録済み。STサーバーに接続されていますが、まだハードウェアとして追加されていません。
緑色	ハードウェアとして追加済み。STサーバーに接続されている場合も接続されていない場合もあります。

新しいカメラを追加した際には、状態は必ず緑になります。接続状態は、**概要**ペインの**レコーディングサーバー**の**デバイス**に表示されます。**概要**ペインで、カメラを簡単に把握できるようカメラをグループ化します。この時点でカメラをAxis Dipatchサービスに**登録しない**場合でも、後で右クリックメニューから登録を行うことができます(**Axis One-Clickカメラの編集**を選択)。

スマートマップ

地理的背景(説明付き)

XProtect Smart Clientユーザーが地理的な背景を選択する前に、まず、XProtect Management Clientで地理的な背景を設定してください。

- **基本的な世界地図** - XProtect Smart Clientで提供される標準的な地理的背景を使用します。構成は不要です。このマップは一般的な基準として使用することを意図しており、国境や都市、その他の詳細などの機能は含まれていません。ただし、他の地理的背景と同様、地理参照データは含まれています。
- **Bing Maps** - Bing Mapsに接続します。
- **Google Maps** - Google Mapsに接続します。
- **Milestone Map Service** - 無料のマッププロバイダーに接続します。Milestone Map Serviceを有効にすると、さらなるセットアップは不要です。

  Milestone Map Serviceを有効化を参照

- **OpenStreetMap** - 以下に接続します:
  - 選択したコマーシャルタイルサーバー
  - 自身、オンライン、またはローカルタイルサーバー

  OpenStreetMapタイルサーバーの指定を参照

Bing MapsとGoogle Mapsオプションでは、インターネットへのアクセスが必要です。MicrosoftまたはGoogleからキーを購入してください。

Milestone Map Serviceではインターネットへのアクセスが必要です。

自身のローカルタイルサーバーを使用する場合を除き、OpenStreetMapではインターネットアクセスが必要です。

システムでEUGDPRに準拠したインストールを行いたい場合は、以下のサービスを使用しないでください。

- Bing Maps
- Google Maps
- Milestone Map Service

データ保護と使用状況データの収集の詳細については、GDPRプライバシーガイドを参照してください。

デフォルトで、Bing MapsとGoogle Mapsにはサテライト画像が表示されます(サテライト)。XProtect Smart Clientの画像は、航空画像や地形表示などに変更して、他の情報を表示することもできます。

Management ClientでBing MapsまたはGoogle Mapsを有効化

Smart ClientのManagement Clientプロファイルにキーを入力することで、複数のユーザーが使用できるキーを作成できます。プロファイルに割り当てられているすべてのユーザーがこのキーを使用します。

手順:

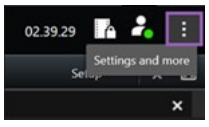
1. Management Clientの**サイトナビゲーション**ペインで、**Smart Clientプロファイル**をクリックします。
2. **Smart Clientプロファイル**ペインで該当するSmart Clientプロファイルを選択します。
3. **プロパティ**ペインで**スマートマップ**タブを以下のようにクリックします。
   - BingMapsについては、お持ちのベーシックキーまたはエンタープライズキーを**BingMapsキー**フィールドに入力します
   - Google Mapsでは、**Google Mapsのプライベートキー**フィールドでMaps Static APIキーを入力します
4. XProtect Smart Clientオペレータが別のキーを使用するのを防ぐため、**ロック済み**チェックボックスを選択します。

XProtect Smart ClientでBing MapsまたはGoogle Mapsを有効化

XProtect Smart Clientオペレータによって Smart Clientプロファイルキー以外の別のキーを使用できるようにするには、そのキーをXProtect Smart Clientの設定に入力する必要があります。

手順:

1. XProtect Smart Clientで**設定**ウィンドウを開きます。



2. **スマートマップ**をクリックします。

3. 利用したい地図により、以下のいずれかを行ってください:
   - Bing Mapsでは、**Bing Maps キー**フィールドに自分のキーを入力します。また、82ページのスマートマップとBing Mapsの統合(説明付き)も参照してください。
   - Google Mapsでは、Google Mapsフィールドの**プライベートキーに自分のキーを**入力します。また、81ページのスマートマップとGoogle Mapsの統合(説明付き)も参照してください。

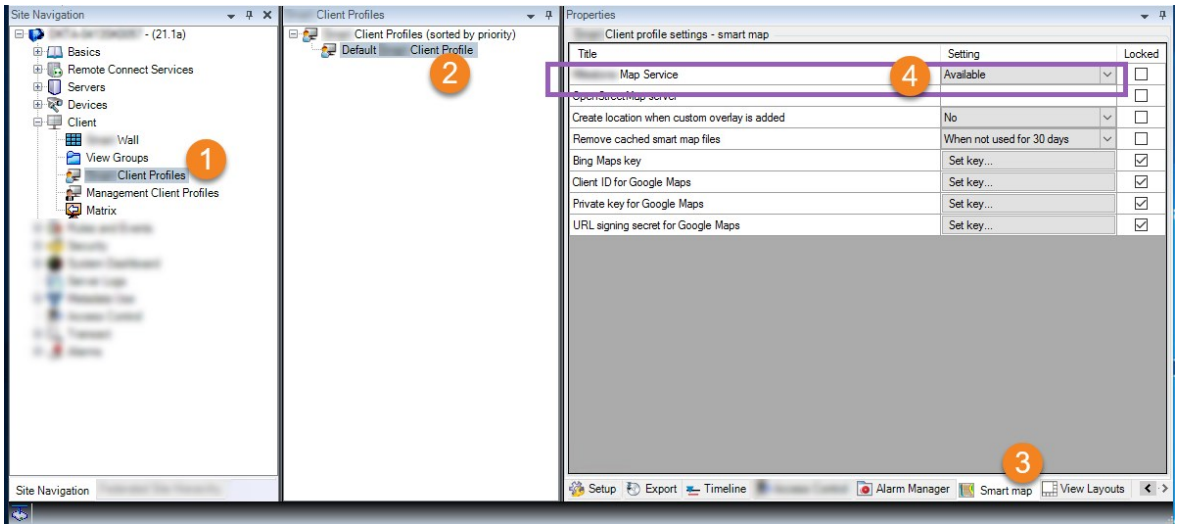
Milestone Map Service を有効にします

Milestone Map Serviceは、Milestone Systemsのタイルサーバーに接続できるオンラインサービスです。このタイルサーバーは無料の市販マップサービスを使用しています。

スマートマップでMilestone Map Serviceを有効にすると、スマートマップは地理的な背景としてMilestone Map Serviceを使用するようになります。

手順:

1. **サイトナビゲーション**ペインで**クライアント**ノードを展開し、**Smart Clientプロファイル**をクリックします。
2. 概要ペインで関連するSmart Clientプロファイルを選択します。
3. **プロパティ**ペインで**スマートマップ**タブをクリックします。



4. **Milestone Map Service**フィールドで、**利用可能**を選択します。
5. XProtect Smart Clientでこの設定を強制するには、**ロック済み**チェックボックスを選択します。その後、XProtect Smart Clientのオペレータは Milestone Map Serviceを有効または無効にできなくなります。
6. 変更を保存します。

Milestone Map Serviceは、XProtect Smart Clientの**設定**ウィンドウで有効にすることもできます。

Milestone Map Serviceではインターネットへのアクセスが必要です。

制限されたファイアウォールがある場合は、中古ドメインへのアクセスを許可することが重要です。Milestone Map Service を実行している各マシンで maps.milestonesys.com を使用した Smart Client の発信トラフィックを許可する必要がある場合があります。

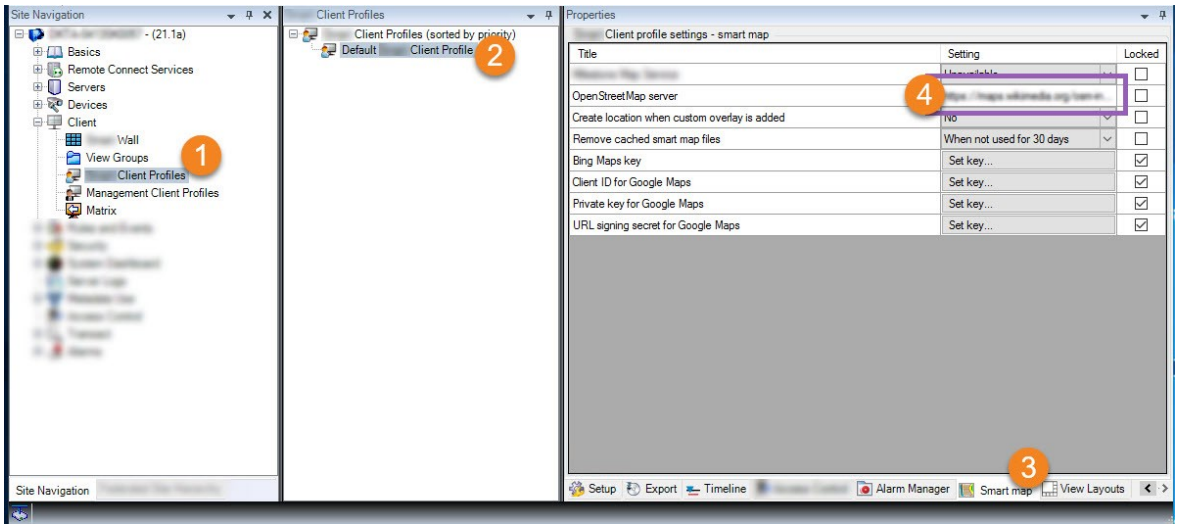
OpenStreetMapタイルサーバーの指定

スマートマップの地理的背景としてOpenStreetMapを使用する場合は、タイル化された画像の取得先を指定する必要があります。これは、コマーシャルタイルサーバーまたはローカルタイルサーバーのいずれかのタイルサーバーアドレスを指定すると実行できます(所属組織に空港や港といった地域の独自の地図がある場合など)。

XProtect Smart Clientの**設定**ウィンドウで、タイルサーバーアドレスを指定することもできます。

手順:

1. **サイトナビゲーション**ペインで**クライアント**ノードを展開し、**Smart Clientプロファイル**をクリックします。
2. 概要ペインで関連するSmart Clientプロファイルを選択します。
3. **プロパティ**ペインで**スマートマップ**タブをクリックします。



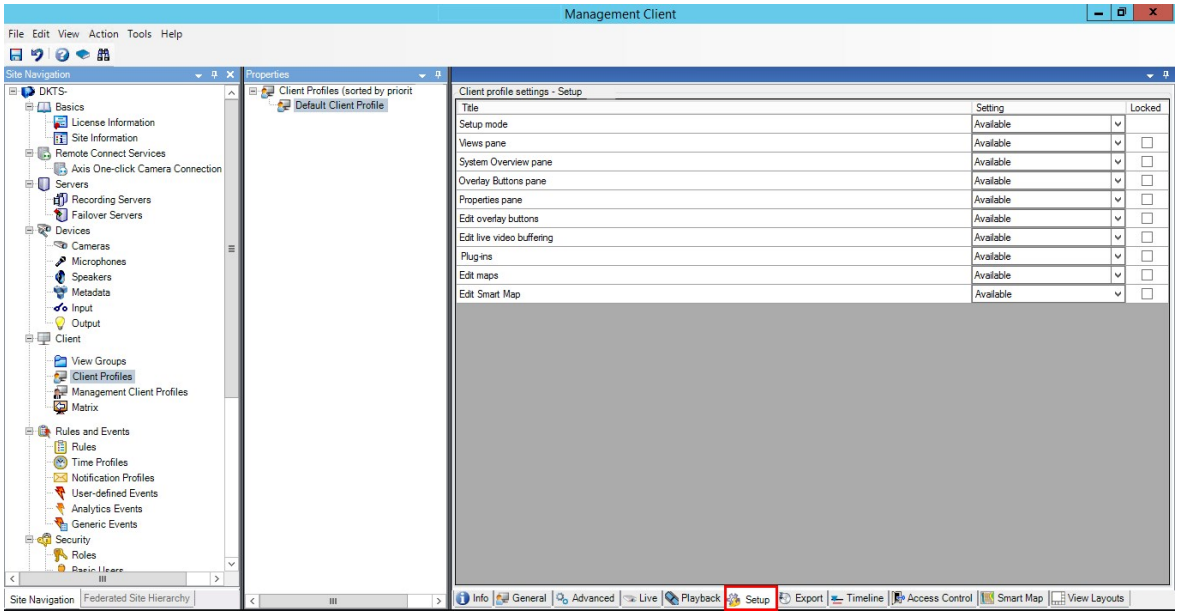
4. **OpenStreetMapサーバー**フィールドにタイルサーバーのアドレスを入力します。
5. XProtect Smart Clientでこの設定を強制するには、**ロック済み**チェックボックスを選択します。その後、XProtect Smart Clientオペレータはアドレスを変更できません。
6. 変更を保存します。

スマートマップの編集を有効にする

オペレータは編集がXProtectSmartClientで有効になっている場合にのみManagementClientのセットアップモードでスマートマップを編集できます。まだ有効になっていない場合、関連する各SmartClientプロファイルの編集を有効にする必要があります。

手順:

1. **サイトナビゲーション**ペインで**クライアント**ノードを展開します。
2. **Smart Clientプロファイル**をクリックします。



3. 概要ペインで関連するSmart Clientプロファイルを選択します。
4. **プロパティ**ペインで**セットアップ**タブをクリックします。
5. **スマートマップの編集**リストで、**使用可能**を選択します。
6. 関連する各Smart Clientプロファイルについてこれらのステップを繰り返します。
7. 変更を保存します。選択したSmart Clientプロファイルに割り当てられたユーザーが次にXProtect Smart Clientにログインする時には、スマートマップを編集できるようになります。

編集を無効にするには、**スマートマップの編集**リストで**使用不可**を選択します。

スマートマップでデバイスの編集を有効にする

オペレータが以下を実行できるようにするには役割ごとにデバイスの編集を有効にする必要があります。

- スマートマップ上に入力デバイスまたはマイクを配置する
- スマートマップ上のカメラの視界を調整する

オペレータはスマートマップで以下のタイプのデバイスを編集できます。

- カメラ
- 入力デバイス
- マイク

要件

始める前に、スマートマップの編集が有効になっているか確認してください(308ページのスマートマップの編集を有効にするを参照) 。これはオペレータの役割に関連するSmart Clientプロファイルで実行します。

手順:

1. **セキュリティ**ノード> **役割**を展開します。
2. **役割**ペインで、オペレータが関連する役割を選択します。
3. 役割に編集権限を付与する場合:
   - **セキュリティ全般**タブを選択し、**役割の設定**ペインでデバイスのタイプを選択します(**カメラ**や**入力**など)
   - **許可**列で、**全制御**または**編集**チェックボックスを選択します。
4. 変更を保存します。

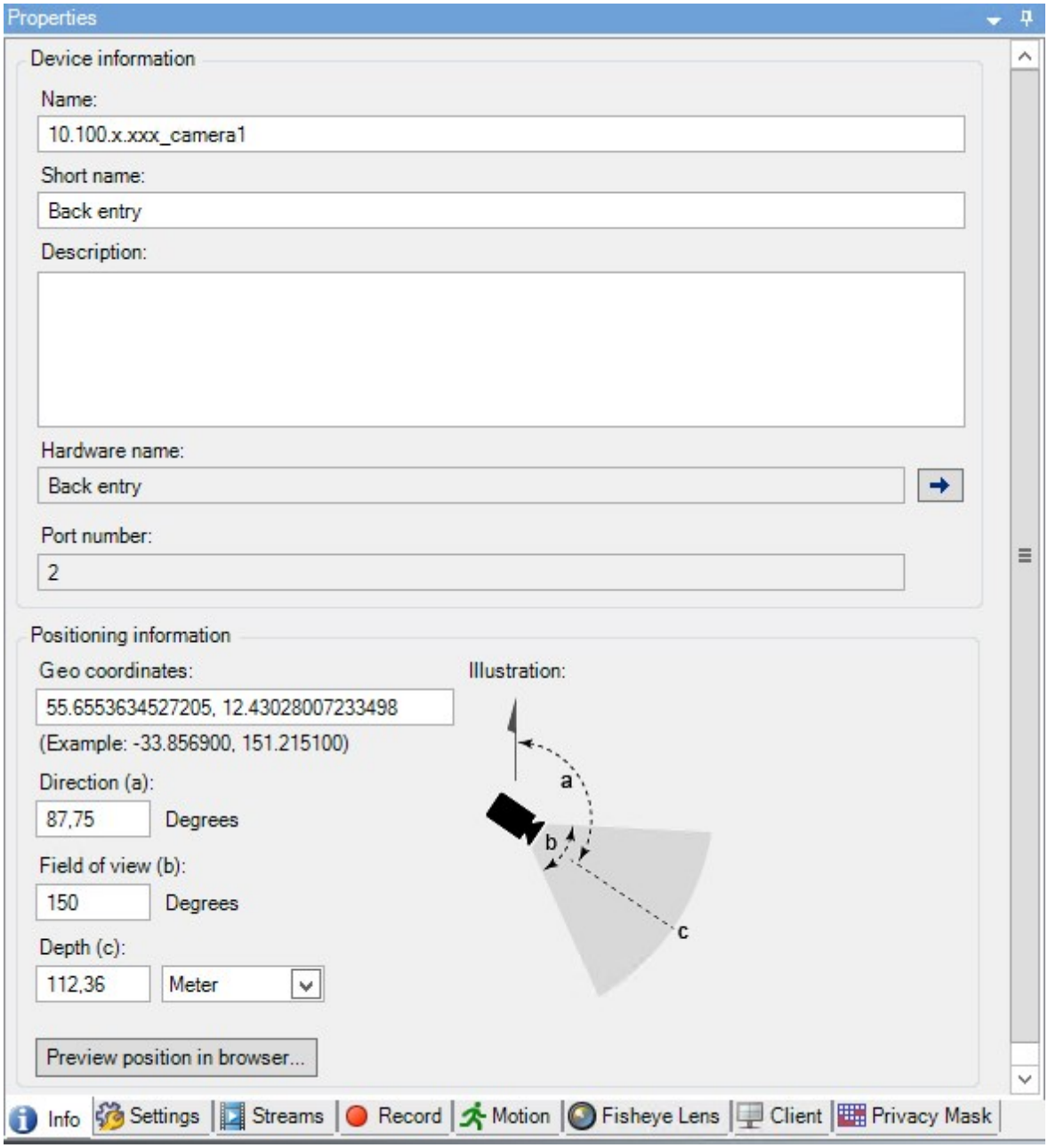
個々のデバイスの編集を有効にするには、**デバイス**タブで該当するデバイスを選択します。

デバイスの位置、カメラの方向、視野、深度を定義する(スマートマップ)

デバイスがスマートマップで適切に配置されるよう、デバイスの地理座標を設定することができます。カメラの場合は、方向や視野、視界深度も設定できます。上記のいずれかを設定すると、オペレータが次回、XProtect Smart Clientでスマートマップを読み込んだ際、そのデバイスがスマートマップに自動的に追加されます。

手順:

1. Management Clientで、**デバイス**ノードを展開し、デバイスのタイプを選択します(**カメラ**、**入力**など) 。
2. **デバイス**ペインで、該当するデバイスを選択します。
3. **情報**タブで、**位置情報**までスクロールダウンします。



4. **地理座標**フィールドで、緯度、経度の順に指定します。小数点としてピリオドを使用し、緯度と経度を分けるためにコンマを使用します。

- カメラの場合：
  1. **方向**フィールドに、0から360度の範囲の値を入力します。
  2. **視野**フィールドに、0から360度の範囲の値を入力します。
  3. **深度**フィールドに、視界深度をメートルまたはフィートのいずれかで入力します。

5. 変更を保存します。

また、レコーディングサーバーのプロパティも設定できます。

スマートマップを設定する: Milestone Federated Architecture

Milestone Federated Architectureでスマートマップを使用すると、接続されているサイトからのデバイスがすべてスマートマップに表示されます。フェデレーテッドアーキテクチャでスマートマップを設定するには、以下の手順に従ってください。

Milestone Federated Architectureの一般的な情報については、87ページのMilestone Federated Architectureの設定を参照してください。

1. 子サイトを持つトップサイトに接続する前に、全サイトのすべてのデバイスでその地理座標が指定されていることを確認します。地理座標は、XProtect Smart Clientでスマートマップにデバイスを配置する際、自動的に追加されますが、デバイスプロパティのManagement Clientで手動で追加することも可能です。詳細については、「309ページのデバイスの位置、カメラの方向、視野、深度を定義する(スマートマップ)」を参照してください。
2. Windowsユーザーとして、Smart Clientオペレータを親サイトおよびすべてのフェデレーテッドサイトに追加する必要があります。少なくともトップサイトでは、Windowsユーザーにスマートマップの編集権限を付与する必要があります。これによって、トップサイトおよびすべての子サイトでスマートマップを編集できるようになります。次に、子サイトのWindowsユーザーにスマートマップを編集する権限が必要かどうかを判断する必要があります。Management Clientで初めにWindowsユーザーを**役割**で作成した後、スマートマップ編集を有効にします。詳細については、「308ページのスマートマップの編集を有効にする」を参照してください。
3. トップサイトで、Windowsユーザーとして管理者権限を持つ役割に子サイトを追加します。オブジェクトタイプを特定する際、**コンピュータ**のチェックボックスを選択してください。
4. 各子サイトにおいては、トップサイトをWindowsユーザーがトップサイトと同じシステム管理者役割を持つユーザーとして追加する必要があります。オブジェクトタイプを特定する際、**コンピュータ**のチェックボックスを選択してください。
5. トップサイトでは、**フェデレーテッドサイト階層**ウィンドウが必ず表示されるようにしてください。Management Clientでは、**ビュー**から**フェデレーテッドサイト階層**を選択してください。各子サイトをトップサイトに追加します。詳細については295ページのサイトを階層に追加を参照してください。
6. それでは、Milestone Federated ArchitectureがXProtect Smart Clientで機能するかテストをしてみましょう。管理者あるいはオペレータとしてトップサイトにログインし、スマートマップを含むビューを開きます。設定が正しく行われていれば、トップサイトおよびすべての子サイトのデバイスがすべてスマートマップ上に現れます。子サイトの一つにログインした場合は、そのサイトと子サイトのデバイスしか表示されません。

カメラの位置やアングルなど、スマートマップ上でデバイスを編集する場合、ユーザーにはデバイスの編集権限が必要となります。詳細については、「308ページのスマートマップでデバイスの編集を有効にする」を参照してください。

メンテナンス

システム設定のバックアップおよび復元

Milestoneは、障害復旧対策として、使用しているシステム設定を定期的にバックアップすることを推奨しています。

通常、設定が失われることはあまりありませんが、失われる可能性はあります。技術的または組織的な対策を通して、バックアップを保護することが重要です。

システム設定のバックアップおよび復元について

システムでは、Management Clientで定義できるシステム設定をすべてバックアップするビルトイン機能が提供されています。監査ログファイルを含む、ログサーバーデーターベースおよびログファイルはこのバックアップには含まれていません。

大規模システムの場合、Milestoneは、スケジュールされたバックアップを定義することを推奨しています。これは、次のサードパーティーツールを使用して実行できます。Microsoft® SQL Server Management Studio。このバックアップには、手動バックアップと同じデータが含まれています。

バックアップ中、システムはオンラインのままになります。

設定をバックアップするには時間がかかることがあります。バックアップの所要時間は以下により異なります。

- システム設定
- ハードウェア
- SQLServer、EventServer、ManagementServerコンポーネントを単一または複数のサーバーのいずれにインストールしたか

手動およびスケジュールされたバックアップ作成を実行するたびに、SQL Serverデータベースのトランザクションログファイルがフラッシュされます。トランザクションログファイルをフラッシュする方法については、126ページのSQL Serverデータベーストランザクションログ(説明付き)を参照してください。

バックアップを作成する際は、システム設定パスワードを把握しておいてください。

FIPS非準拠暗号で暗号化されている2017 R1よりも前のXProtect VMSのバージョンからのエクスポートとアーカイブ済みメディアデータベースを持つFIPS 140-2準拠システムでは、FIPSを有効にした後でもアクセスできる場所でデータをアーカイブする必要があります。FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、ハードニングガイドのFIPS 140-2準拠セクションを参照してください。

共有バックフォルダーの選択

システム設定をバックアップして復元する前に、この目的でバックアップフォルダーを設定しなければなりません。

1. 通知エリアのManagement Serverサービスアイコンを右クリックし、**共有バックフォルダーを選択**を選択します。
2. 表示されるウィンドウで、希望するファイルの場所を参照します。
3. **OK**を2回クリックします。
4. 現在のバックアップフォルダー内のファイルを削除するか尋ねられたら、必要に応じて、**はい**または**いいえ**をクリックします。

システム設定の手動バックアップ

1. メニューバーから、**ファイル>バックアップ設定**を選択します。
2. ダイアログボックスの注記を読んで、**バックアップ**をクリックします。
3. .cnfファイルの名前を入力します。
4. フォルダーの保存先を入力し、**保存**をクリックします。
5. バックアップが終了するまで待ち、**閉じる**をクリックします。

すべての関連するシステム設定ファイルは、1つの.cnfファイルにまとめられ、指定された場所に保存されます。バックアップ中、すべてのバックアップファイルはまず、マネジメントサーバー上の一時システムのバックアップフォルダーにエクスポートされます。通知エリアのManagement Serverサービスアイコンを右クリックし、共有バックアップフォルダーを選択を選択すると、他の一時フォルダーを選択できます。

システム設定の復元(手動バックアップから)

重要な情報

- インストールを実行したユーザーと復元を行ったユーザーの双方とも、SQL Server上のマネジメントサーバー**および**のシステム設定SQL Serverデータベースのローカル管理者でなければなりません。
- レコーディングサーバーを除き、システムは復元中は完全にシャットダウンされます。復元されるまで多少時間がかかる場合があります。
- バックアップは、バックアップが作成されたシステムインストール上でのみ復元できます。設定がバックアップの作成時のものと、できる限り同じであることを確認します。そうしないと、復元が失敗する場合があります。
- 復元中にシステム設定パスワードを聞かれた場合は、バックアップの作成時に有効だったシステム設定パスワードを入力する必要があります。このパスワードがなければ、バックアップから設定を復元できません
- SQL Serverデータベースをバックアップし、これをクリーンなSQL Serverに復元した場合、SQL Serverデータベースから返されたraiseエラーは機能しないため、SQL Serverから一般エラーメッセージを1通のみ受け取ることになります。これを避けるため、まずはクリーンなXProtectを使用してSQL Serverシステムを再インストールしてから、そこでバックアップを復元します。
- 検証フェーズ中に復元できない場合は、変更がないため、古い設定を再度開始できます。
  プロセスの他の段階で復元できない場合は、古い設定
  にロールバックすることはできません。バックアップファイルが破損していない限り、別の復元を実行することができます。

- 復元すると、現在の設定が置き換えられます。これは、前回のバックアップ以降の設定変更がすべて失われることを意味します。
- ログ(監査ログを含む)は復元されません。
- 復元が開始されると、取り消しできません。

復元

1. 通知エリアのManagement Serverサービスアイコンを右クリックし、**設定を復元**を選択します。
2. 重要な注記を読んでから、**復元**をクリックします。
3. ファイルを開くダイアログボックスで、システム設定バックアップファイルの場所を参照して選択し、**開く**をクリックします。

   バックアップファイルは、Management Clientコンピュータ上にあります。Management Clientが他のサーバーにインストールされている場合は、バックアップ先を選択する前にこのサーバーにバックアップファイルをコピーします。

4. **設定を復元**ウィンドウが表示されます。復元が終了するまで待ち、**閉じる**をクリックします。

システム設定パスワード(説明付き)

システム設定パスワードを割り当てると、システム設定全体を保護できます。システム設定パスワードを割り当てると、バックアップはこのパスワードによって保護されます。パスワードの設定は、安全なフォルダーでマネジメントサーバーを実行しているコンピュータに格納されます。以下を行うためにこのパスワードが必要になります。

- 現在のパスワード設定とは異なるパスワード設定を使用して作成された設定バックアップから設定を復元する
- ハードウェアエラーにより、別のコンピュータにマネジメントサーバーを移動またはインストール(復元)する
- クラスタリングを使用してシステムで追加マネジメントサーバーを設定する

システム設定パスワードはインストール中、またはインストール後に割り当てることができます。パスワードは、パスワードに関するWindowsのポリシーで定義されているWindowsの複雑さ要件を満たす必要があります。

システム管理者は、このパスワードを保存して安全に維持しておく必要があります。システム設定パスワードが割り当てられており、バックアップを復元する場合は、システム設定パスワードを入力するよう求められます。このパスワードがなければ、バックアップから設定を復元できません。

システム設定パスワードの詳細

システム設定パスワードの詳細は変更できます。システム設定パスワードについては以下のオプションがあります。

- システム設定パスワードを割り当てて、システム設定をパスワードで保護
- システム設定パスワードを変更
- 割り当てられたシステム設定パスワードを削除し、システム設定をパスワードで保護しないことを選択

システム設定パスワードの設定変更

パスワードを変更する場合は、さまざまなバックアップに関連のあるパスワードをシステム管理者が保存し、安全に維持しておくことが重要になります。バックアップを復元する際、バックアップの作成時に有効だったシステム設定パスワードを入力するよう求められることがあります。このパスワードがなければ、バックアップから設定を復元できません。

マネジメントサーバーとイベントサーバーが個別のコンピュータにインストールされている場合、パスワードを変更した後は、現在のシステム設定パスワードをイベントサーバーにも入力する必要があります。詳細については、「現在のシステム設定パスワードを入力(イベントサーバー)」を参照してください。

変更を適用するには、マネジメントサーバー サービスを再起動する必要があります。

1. マネジメントサーバーのトレイアイコンを見つけて、サーバーが実行していることを確認します。
2. 通知エリアのManagement Serverサービス アイコンを右クリックし、**システム設定パスワードの変更**を選択します。
3. システム設定パスワードの変更ウィンドウが表示されます。

パスワードの割り当て

1. **新しいパスワード**フィールドに新しいパスワードを入力します。
2. **新しいパスワードを再入力**フィールドに新しいパスワードを再入力し、**Enter**を選択します。
3. 通知を読み、**はい**をクリックして変更を承諾します。
4. 変更の確認を待ってから、**閉じる**を選択します。
5. 変更を適用するには、マネジメントサーバー サービスを再起動する必要があります。
6. 再起動後、マネジメントサーバーが実行されていることを確認してください。

パスワード保護を削除する

パスワードによる保護が必要ない場合は、オプトアウトできます。

1. 以下のチェックボックスを選択します。**システム設定パスワードを保護しないことを選択し、システム設定が暗号化されないことを承知する**。その後、**Enter**をクリックします。
2. 通知を読み、**はい**をクリックして変更を承諾します。
3. 変更の確認を待ってから、**閉じる**を選択します。
4. 変更を適用するには、マネジメントサーバーサービスを再起動する必要があります。
5. 再起動後、マネジメントサーバーが実行されていることを確認してください。

システム設定パスワードの設定入力(復元)

パスワードの設定が含まれているフィールドがハードウェアのエラーやその他の理由で削除された場合は、システム設定のあるデータベースにアクセスする際、システム設定パスワードが必要になります。新しいコンピュータでのインストール中、システム設定パスワードを入力するよう求められます。

ただし、パスワードの設定が含まれているファイルが削除されるか、破損した場合、マネジメントサーバーを実行しているコンピュータに他の問題が発生していなければ、システム設定パスワードの設定を入力することができます。

1. マネジメントサーバーのトレイアイコンを見つけます。
2. 通知エリアのManagement Serverサービスアイコンを右クリックし、**システム設定パスワードの入力**を選択します。
3. システム設定パスワードの入力ウィンドウが表示されます。

システム設定がパスワードで保護されている

1. **パスワード**フィールドでパスワードを入力し、**Enter**を選択します。
2. パスワードが承認されるのを待ちます。**閉じる**を選択します。
3. マネジメントサーバーが実行されていることを確認してください。

システム設定はパスワードで保護されていない

1. 以下のチェックボックスを選択します。**このシステムでシステム設定パスワードを使用しない**。その後、**Enter**を選択します。
2. この設定が承諾されるのを待ちます。**閉じる**を選択します。
3. マネジメントサーバーが実行されていることを確認してください。

システム設定の手動バックアップ(説明付き)

システム設定が含まれるマネジメントサーバーのデータベースの手動バックアップを実行したい場合は、システムがオンライン状態に維持されるようにしてください。マネジメントサーバーのデータベースのデフォルト名は**Surveillance**です。

バックアップを開始する前に、次の点を考慮してください。

- SQL Serverデータベースのバックアップを使用して、システム設定を他のシステムにコピーすることはできません
- SQL Serverデータベースのバックアップにはある程度の時間を要します。これは、システム設定やハードウェアに応じて、ならびにSQL Server、マネジメントサーバー、Management Clientが同一のコンピュータにインストールされているかどうかによって異なります。
- ログ(監査ログを含む)はログサーバーのデータベースに保存されているため、マネジメントサーバーのデータベースのバックアップには**含まれていません**。ログサーバーのデータベースのデフォルト名は**SurveillanceLogServerV2**です。双方のSQL Serverデータベースとも同じ方法でバックアップします。

イベントサーバー設定成のバックアップと復元(説明付き)

イベントサーバー設定の内容は、システム設定のバックアップおよび復元を実行する際に含められます。

イベントサーバーを初めて実行する際には、その設定ファイルのすべてが自動的にSQL Serverデータベースへと移動します。イベントサーバーを再起動する必要なく、復元された設定をイベントサーバーに復元できます。イベントサーバーは、設定の復元のロード中にすべての外部通信を開始および停止できます。

システム設定のスケジュールされたバックアップと復元(説明付き)

マネジメントサーバーは、システムの設定をSQL Serverデータベースに保存します。Milestoneは、障害復旧対策として、このデータベースの定期バックアップを実行するよう推奨しています。システム設定が失われることはまれですが、不運な状況のもとではその可能性も否定できません。幸いにもバックアップには1分で完了し、SQL Serverデータベースのトランザクションログがフラッシュされるという追加の利点も得られます。

小規模な設定で定期的なバックアップが必要ない場合には、システム設定を手動でバックアップできます。その方法については、317ページのシステム設定の手動バックアップ(説明付き)を参照してください。

マネジメントサーバーをバックアップ/復元する際には、システム設定が含まれるSQL Serverデータベースがバックアップ/復元に含まれていることを確認してください。

スケジュールされたバックアップおよび復元を使用するための要件

Microsoft® SQL Server Management Studioは、ウェブサイト(https://www.microsoft.com/downloads/)から無料でダウンロード可能なツールです

SQL Serverおよびサーバーデータベースを管理するための多数の機能に加え、使いやすいバックアップおよび復元機能が含まれています。マネジメントサーバーに、ツールをダウンロードしてインストールします。

スケジュールされたバックアップによるシステム設定のバックアップ

1. WindowsのスタートメニューでMicrosoft® SQL Server Management Studioを起動します。
2. 接続時に、必須のSQLServerの名前を指定します。SQLServerデータベースの作成に使用したアカウントを使用します。

1. すべてのシステム設定(イベントサーバー、レコーディングサーバー、カメラ、入力、出力、ユーザー、ルール、パトロール設定などを含む)が含まれるSQL Serverデータベースを探します。このSQLデータベースのデフォルト名は**Surveillance**です。
2. SQL Serverデータベースのバックアップを作成し、以下について確認します。
   - 正しいSQL Serverデータベースが選択されている
   - バックアップのタイプが**フル**になっている
   - 定期バックアップのスケジュールの設定。定期バックアップおよび自動バックアップの詳細については、Microsoftのウェブサイト(https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017)を参照してください。
   - 提案されたパスでよいことを確認するか、代替のパスを選択します
   - **完了時にバックアップを確認**および**メディアに書き込む前のチェックサムを実行**を選択します。
3. ツールの指示に最後まで従います。

また、ログサーバーのデータベースについても、同じ方法でログとともにバックアップすることを検討してください。ログサーバーのSQL Serverデータベースのデフォルト名は**SurveillanceLogServerV2**です。

システム設定の復元(スケジュールされたバックアップから)

要件

システム設定データベースの復元中にシステム設定が変更されるのを防ぐため、以下を停止します。

- Management Serverサービス(332ページのサーバーサービスの管理を参照)
- Event Serverサービス(Windows**サービス**から実行可能。コンピュータで**services.msc**を検索してください。**サービス**内で、**Milestone XProtect Event Server**を検索します)
- World Wide Web Publishingサービス(インターネットインフォメーションサービス(IIS))IISを停止する方法について確認します(https://technet.microsoft.com/library/cc732317(WS.10).aspx/) https://technet.microsoft.com/library/cc732317(WS.10).aspx/

Windowsの**スタート**メニューでMicrosoft® SQL Server Management Studioを開きます。

ツールで、以下を実行します。

1. 接続時に、SQLServerの名前を指定します。SQLServerデータベースの作成に使用したユーザーアカウントを使用します。
2. 全システム設定(イベントサーバー、レコーディングサーバー、カメラ、インプット、アウトプット、ユーザー、ルール、パトロールプロファイルなどを含む)が含まれるSQL Serverデータベース(デフォルト名:**Surveillance**)を探します。

3. SQL Serverデータベースを復元し、以下を確実に実行します。
    - デバイス**から**バックアップするように選択します。
    - バックアップメディアタイプ**ファイル**を選択します。
    - バックアップファイル(**.bak**) を探して選択する
    - **[既存のデータベースを上書きする]**ように選択します。
4. ツールの指示に最後まで従います。

同じ方法を用いて、ログサーバーのSQL Serverデータベースをログとともに復元します。ログサーバーのSQL Serverデータベースのデフォルト名は**SurveillanceLogServerV2**です。

システムは、Management Serverサービスが停止中には動作しません。データベースの復元が完了した後、すべてのサービスを忘れずに再起動することが重要です。

ログサーバーのデータベースのバックアップ

ログサーバーのデータベースは、前述のシステム設定の処理と同じ方法で処理します。ログサーバーのデータベースには、レコーディングサーバーとカメラから報告されたエラーをはじめとする、あらゆるシステムログが含まれています。ログサーバーのデータベースのデフォルト名は**SurveillanceLogServerV2**です。

SQL Serverデータベースは、ログサーバーのSQL Serverに配置されています。通常、ログサーバーとマネジメントサーバー双方のSQL Serverデータベースが同一のSQL Serverに配置されます。ログサーバーデータベースにはシステム設定が一切含まれていないため、そのバックアップは必須ではありませんが、マネジメントサーバーのバックアップ/復元前にシステムログにアクセスできるという利点は得られます。

バックアップ/復元の失敗と問題のシナリオについて(説明付き)

- 前回のシステム設定バックアップ後、イベントサーバーや、ログサーバーなどの登録済みサービスを移動した場合は、新しいシステムにどの登録サービスを設定するか選択する必要があります。システムが古いバージョンに復元された後に、新しい構成を保持することが可能です。サービスのホスト名を見て選択してください。
- イベントサーバーが特定の宛先にない(古い登録済みサービス設定を選択した場合など) ために、システム設定の復元が失敗した場合は、もう1回復元してください。
- 設定バックアップの復元中に、誤ったシステム設定パスワードを入力した場合は、バックアップの作成時に有効だったシステム設定パスワードを入力する必要があります。

マネジメントサーバーの移動

マネジメントサーバーは、システム設定をSQL Serverデータベースに保存します。物理サーバーから別のサーバーへとマネジメントサーバーを移動している最中には、新しいマネジメントサーバーからもこのSQL Serverデータベースにアクセスできていることを確認することが欠かせません。システム設定データベースは、次のつの方法で保存できます:

- **ネットワークSQL Server**: システム構成をネットワーク上にあるSQL ServerのSQL ServerSQLデータベースに保存している場合、マネジメントサーバーソフトウェアを新しいマネジメントサーバーにインストールする際に、そのSQL ServerでSQLデータベースの場所をポイントすることができます。このようなケースにおいては、管理者サーバーのホスト名のあるパラグラフに続く管理者サーバーホスト名についての続くパラグラフのみIPアドレスを適応します。残りのトピックは無視してください:

  管理者サーバーホスト名とIPアドレス: 1つの物理サーバーから別の物理サーバーへとマネジメントサーバーを移動するときには、古いものと同じホスト名とIPアドレスを新しいサーバーに割り当てることが最も簡単な方法です。これは、レコーディングサーバーが古いマネジメントサーバーのホスト名とIPアドレスに自動的に接続するためです。新しいマネジメントサーバーに新しいホスト名および/またはIPアドレスを与えると、レコーディングサーバーはマネジメントサーバーを見つけることができないため、各Recording Serverサービスを手動で止め、マネジメントサーバーのURLを変更し、レコーディングサーバーを再登録して、その後でRecording Serverサービスを起動します。

- **ローカルSQL Server**: システム構成をマネジメントサーバー本体に存在するSQL ServerのSQL ServerSQLデータベースに保存している場合、移動前に、既存のマネジメントサーバーのシステム構成SQLデータベースをバックアップすることが重要です。SQL Serverデータベースをバックアップし、後の段階で新しいマネジメントサーバーのSQL Serverに復元することで、移動後にカメラ、ルール、時間プロファイルなどを再構成する必要がなくなります

> マネジメントサーバーを移動する場合は、バックアップを復元するために現在のシステム構成パスワードが必要となります。「315ページのシステム設定パスワード(説明付き)」を参照してください。

要件

- **新しいマネジメントサーバーにインストールするためのソフトウェアインストールファイル**
- システムを購入し、初めてインストールしたときに受け取った**ソフトウェアライセンスファイル(.lic)**。手動オフラインアクティベーション後に受け取ったアクティベーション済みソフトウェアライセンスファイルを使用しないでください。アクティベーション済みソフトウェアライセンスファイルには、システムがインストールされた特定のサーバーの情報が含まれます。このため、アクティベーション済みソフトウェアライセンスファイルは新しいサーバーに移動すると再利用できません。

移動してシステムライセンスをアップグレードしている場合は、新しいソフトウェアライセンスファイルが提供されます。このファイルを使用してください。

- **ローカルSQL Serverユーザーのみ:: Microsoft® SQL Server Management Studio**
- 321ページの(「」を参照)ローカルユーザーのみ:
- マネジメントサーバーが利用できない間はどうします320ページのログサーバーのデータベースのバックアップか?

(「」を参照)

- ログサーバーデータベースのコピー(「」を参照)現在動作しているレコーディングサーバーはすべて、マネジメントサーバーからの設定のコピーを受け取るので、マネジメントサーバーがダウンしている間でも、動作して記録を保存できます。このため、スケジュールされた録画とモーション起動の録画は動作します。イベント起動録画も、マネジメントサーバーまたはその他のレコーディングサーバーに関連しているイベント(マネジメントサーバーを経由するイベント)に基づいていない限り動作します。

- **レコーディングサーバーは一時的にログデータをローカルに保存します**。マネジメントサーバーが再度利用可能になったときに、レコーディングサーバーは自動的にログデータをマネジメントサーバーへ送信します。
  - **クライアントがログインできません**。クライアントアクセスは、マネジメントサーバーを通じて承認されます。マネジメントサーバーなしではクライアントはログインできません。
  - **すでにログインしているクライアントは、最大4時間ログインした状態を維持できます**: クライアントがログインした場合、マネジメントサーバーによって承認され、最大4時間レコーディングサーバーと通信することができます。新しいマネジメントサーバーを4時間以内に稼働できれば、ユーザーの多くが影響を受けずに済みます。
  - **システムを構成する能力がありません**。マネジメントサーバーがなければ、システム設定を変更することができません。

Milestoneでは、マネジメントサーバーがダウンしている間は、監視システムとの通信が切断される危険性があることをユーザーに通知するようお勧めしています。

システム設定の移動

システム設定の移動は、次の3段階のプロセスに従って行います。

1. システム設定のバックアップを保存します。これは定期的なバックアップを行う場合と同じです。318ページのスケジュールされたバックアップによるシステム設定のバックアップも参照してください。
2. 新しいサーバーに新しいマネジメントサーバーをインストールします。スケジュールされたバックアップの手順2を参照してください。
3. 新しいシステムにシステム設定を復元します。319ページのシステム設定の復元(スケジュールされたバックアップから)も参照してください。

レコーディングサーバーの交換

レコーディングサーバーが動作しないため、新しいサーバーと交換し、古いレコーディングサーバーの設定を継承する場合:

1. 交換するレコーディングサーバーから、レコーディングサーバーIDを取得します。
   1. **レコーディングサーバー**を選択し、**概要**ペインで古いレコーディングサーバーを選択します。
   2. **ストレージ**タブを選択します。
   3. キーボードでCtrlキーを押したままにして、**情報**タブを選択します。
   4. **情報**タブの下の部分にあるレコーディングサーバーID番号をコピーします。文字*ID*の部分はコピーしないで、番号だけをコピーしてください。

2. 新しいレコーディングサーバーで、レコーディングサーバーIDを置き換えます。

1. 古いレコーディングサーバーでRecording Serverサービスを停止してから、Windowsの**サービス**で、サービスの**[スタートアップの種類]**を**[無効]**に設定します。

   > 同じIDを持つ2つのレコーディングサーバーを同時に起動しないことが重要です。

2. 新しいレコーディングサーバーで、エクスプローラを開いて、`C:\ProgramData\Milestone\XProtect Recording Server`またはレコーディングサーバーがあるパスへ移動します。
3. `RecorderConfig.xml`のファイルを開きます。
4. タグ*<id>*と*</id>*の間に記載されているIDを削除します。

5. コピーしたレコーディングサーバーIDを、タグ*<id>*と*</id>*の間に貼り付けます。*RecorderConfig.xml*のファイルを保存します。
6. レジストリに移動します。`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation`
7. **RecorderIDOnMachine**を開き、古いレコーディングサーバーIDを新しいIDに置換します。

3. 新しいレコーディングサーバーをマネジメントサーバーに登録します。RecordingServerManagerトレイアイコンを右クリックして、**[登録]**をクリックします。詳細については、「184ページのレコーディングサーバーを登録する」を参照してください。
4. Recording Serverサービスを再起動します。新しいRecording Serverサービスが起動すると、古いレコーディングサーバーの設定がすべて継承されます。

ハードウェアの移動

同じサイトに属するレコーディングサーバー間でハードウェアを移動できます。移動後に、ハードウェアとそのデバイスは新しいレコーディングサーバーで実行され、新しい録画がこのサーバーに保存されます。移動はクライアントユーザーに透過的です。

古いレコーディングサーバーの録画は、次の処理が発生するまで保存されたままです。

- 保存期間が経過したときにシステムによって録画が削除されます。誰かがエビデンスロックを用いて保護した録画(「69ページのエビデンスロック(説明付き)」を参照)は、エビデンスロックの保存期間が経過するまでは削除されません。エビデンスロックの保存期間はエビデンスロックを作成するときに定義します。保存期間が設定されない可能性もあります。
- **[録画]**タブで各デバイスの新しいレコーディングサーバーから録画を削除する。

まだ録画が含まれるレコーディングサーバーを削除しようとすると、警告が表示されます。

現在ハードウェアが追加されていないレコーディングサーバーにハードウエアを移動する場合は、クライアントユーザーはログアウトしてからログインし直し、デバイスからデータを取得する必要があります。

ハードウェアの起動機能を使用すると、次のことができます。

- **ロードバランシング**:例えば、レコーディングサーバーのディスクが過負荷状態の場合、新しいレコーディングサーバーを追加し、一部のハードウェアを移動できます。
- **アップグレード**:例えば、レコーディングサーバーをホストするサーバーを新しいモデルで置換する場合は、新しいレコーディングサーバーをインストールし、古いサーバーから新しいサーバーにハードウェアを移動できます。
- **障害があるレコーディングサーバーの交換**:たとえば、サーバーがオフラインで、オンラインに戻らない場合は、ハードウェアを他のレコーディングサーバーに移動し、システムを実行し続けることができます。古い録画にはアクセスできません。詳細については、「322ページのレコーディングサーバーの交換」を参照してください。

リモート録画

ハードウェアを別のレコーディングサーバーに移動すると、Interconnectで接続されたサイトまたはカメラのエッジストレージからの実行中の取得または予定された取得はキャンセルされます。録画は削除されませんが、想定通りにデータは取得されず、データベースに保存されません。この場合は警告が表示されます。ハードウェアの移動を開始したときに取得を開始したXProtect Smart Clientユーザーの場合、取得は失敗します。XProtect Smart Clientユーザーには通知が表示され、後から再試行できます。

別のユーザーがリモートサイトでハードウェアを移動した場合は、**[ハードウェアの更新]**オプションを使用して、手動で中央サイトを同期し、リモートサイトの新しい構成を反映する必要があります。同期しない場合は、移動されたカメラは中央サイトから切断されています。

ハードウェアの移動(ウィザード)

1つのレコーディングサーバーから別のサーバーへハードウェアを移動するには、**[ハードウェアの移動]**ウィザードを実行します。ウィザードは必要な手順を案内し、1つ以上のハードウェアデバイスを移動します。

要件

ウィザードを開始する前に行う手順:

- 新しいレコーディングサーバーがネットワーク経由で物理カメラにアクセスできることを確認します。
- ハードウェアの移動先となるレコーディングサーバーをインストールします(「153ページのDownload Managerを介したインストール(説明付き)」または162ページのレコーディングサーバーのサイレントインストール「」を参照)
- 同一のデバイスパックバージョンを、既存のサーバーで実行することになる新しいレコーディングサーバーにインストールします(「135ページのデバイスドライバー(説明付き)」を参照)

ウィザードを実行するには:

1. **[サイトナビゲーション]**ペインで**レコーディングサーバー**を選択します。
2. **[概要]**ペインで、ハードウェアの移動元のレコーディングサーバーを右クリックするか、特定のハードウェアデバイスを右クリックします。
3. **[ハードウェアの移動]**を選択します。

> ハードウェアの移動元のレコーディングサーバーが切断されている場合は、エラーメッセージが表示されます。レコーディングサーバーがオンラインにならないことが確かである場合にのみ、切断されたレコーディングサーバーからハードウェアを移動してください。ハードウェアを移動し、サーバーがオンラインに戻った場合は、同じハードウェアが2つのレコーディングサーバーで実行される期間があるため、システムで予期しない動作が発生するおそれがあります。たとえば、ライセンスエラーや、イベントが正しいレコーディングサーバーに送信されないといった問題が生じる可能性があります。

4. レコーディングサーバーレベルでウィザードを開始した場合は、**[移動するハードウェアを選択]**ページが表示されます。移動するハードウェアデバイスを選択します。
5. **[ハードウェアの移動先となるレコーディングサーバーを選択]**ページで、このサイトにインストールされたレコーディングサーバーのリストから選択します。
6. **[将来の録画で使用するストレージを選択]**ページで、ストレージ使用状況バーに、アーカイブではなくライブ録画のみのレコーディングデータベースの空き領域が表示されます。合計保存期間は、レコーディングデータベースとアーカイブの両方の保存期間です。
7. システムが要求を処理します。
8. 移動が成功した場合は、**[閉じる]**をクリックします。Management Clientで新しいレコーディングサーバーを選択する場合は、移動されたハードウェアが表示され、録画がこのサーバーに保存されます。

   移動が失敗した場合は、以下に従って問題をトラブルシューティングできます。

> Interconnectで接続されたシステムでは、リモートサイトのハードウェアを移動した後に中央サイトを手動で同期し、自分または他のシステム管理者がリモートサイトで行った変更を反映する必要があります。

ハードウェアの移動のトラブルシューティング

移動が失敗した場合は、次の理由のいずれかが原因である可能性があります。

エラータイプ	トラブルシューティング
レコーディングサーバーが接続されていないか、	レコーディングサーバーがオンラインであることを確認してください。登録

エラータイプ	トラブルシューティング
フェールオーバーモードです。	しなければならない場合があります。 サーバーがフェールオーバーモードの場合は、待機してから再試行してください。
レコーディングサーバーは最新バージョンではありません。	レコーディングサーバーを更新し、マネジメントサーバーと同じバージョンで実行されるようにします。
レコーディングサーバーが設定に見つかりません。	レコーディングサーバーが削除されていないことを確認してください。
構成の更新または構成データベースとの通信が失敗しました。	SQL Serverとデータベースが接続されており、稼働していることを確認します。
現在のレコーディングサーバーでハードウェアを停止できませんでした。	他のプロセスによってレコーディングサーバーがロックされているか、レコーディングサーバーがエラーモードに入っている可能性があります。 レコーディングサーバーが実行中であることを確認し、再試行してください。
ハードウェアが存在しません。	移動するハードウェアが別のユーザーと同時にシステムから削除されていないことを確認してください。この状況が発生することはほとんどありません。
ハードウェアが削除されたレコーディングサーバーがオンラインに戻りましたが、オフラインのときに無視するように選択しました。	一般的に、**[ハードウェアの移動]**ウィザードを開始したときに古いレコーディングサーバーがオンラインにならないことを確認しましたが、移動中にサーバーがオンラインになりました。 再度ウィザードを開始して、サーバーが再びオンラインになったかどうかを確認する操作に対して **[いいえ]** を選択します。
ソースのレコーディングストレージが使用できません。	現在オフラインになっているレコーディングストレージのあるデバイスをともなうハードウェアを移動しようとしています。 レコーディングストレージは、ディスクがオフラインまたは何らかの理由で利用できない場合、オフラインになります。 レコーディングストレージがオンラインであることを確認し、再試行してください。
移動先のレコーディングサーバー上にあるレコーディングストレージがすべて使用可能である必要があります。	ハードウェアを、1つ以上のレコーディングストレージが現在オフラインになっているレコーディングサーバーに移動しようとしています。 移動先のレコーディングサーバー上のレコーディングストレージがすべ

エラータイプ	トラブルシューティング
	てオンラインになっていることを確認してください。 レコーディングストレージは、ディスクがオフラインまたは何らかの理由で利用できない場合、オフラインになります。

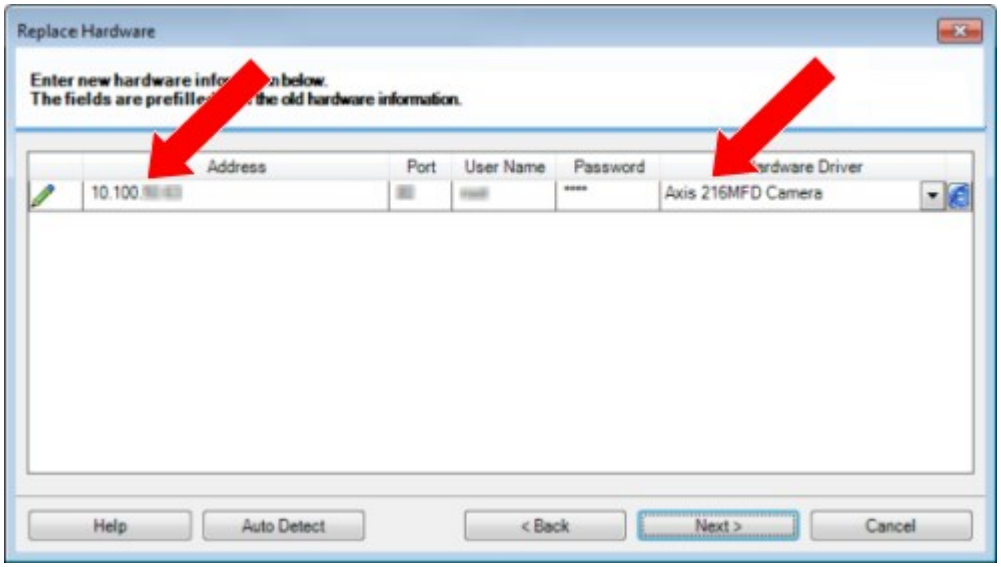
ハードウェアの交換

ネットワーク上のハードウェアデバイスを他のハードウェアデバイスに交換する場合、新しいハードウェアデバイスのIPアドレス、ポート、ユーザー名およびパスワードを知っている必要があります。

自動ライセンスアクティベーション(「108ページの自動ライセンスアクティベーション(説明付き)」を参照)を有効にすることなく、「アクティベーションなしのデバイスの変更」の許容回数(「」を参照)をすべて消費した場合は109ページのアクティベーションなしのデバイスの変更(説明付き)、ハードウェアデバイスを交換した**後**に、手動でライセンスをアクティベートする必要があります。新たなハードウェアデバイスの数がデバイスライセンスの合計数を超えた場合、新しいデバイスライセンスを購入しなければなりません。

1. 必要なレコーディングサーバーを展開し、交換するハードウェアを右クリックします。
2. **ハードウェアの交換**を選択します。
3. **ハードウェアの交換**ウィザードが表示されます。**次へ**をクリックします。

4. ウィザードで、**アドレス**フィールド(図中の赤い矢印)に、新しいハードウェアのIPアドレスを入力します。判明している場合は、**[ハードウェアドライバー]**ドロップダウンリストで該当するドライバーを選択します。それ以外の場合は、**自動検出**を選択します。新しいハードウェアのポート、ユーザー名または/およびパスワードのデータが異なる場合は、**自動検出プロセスが開始する前に(必要な場合)**これらを訂正します。



ウィザードでは、既存のハードウェアのデータが事前入力されます。類似のハードウェアデバイスと交換する場合、たとえばポートやドライバーの情報など、これらのデータを再利用できます。

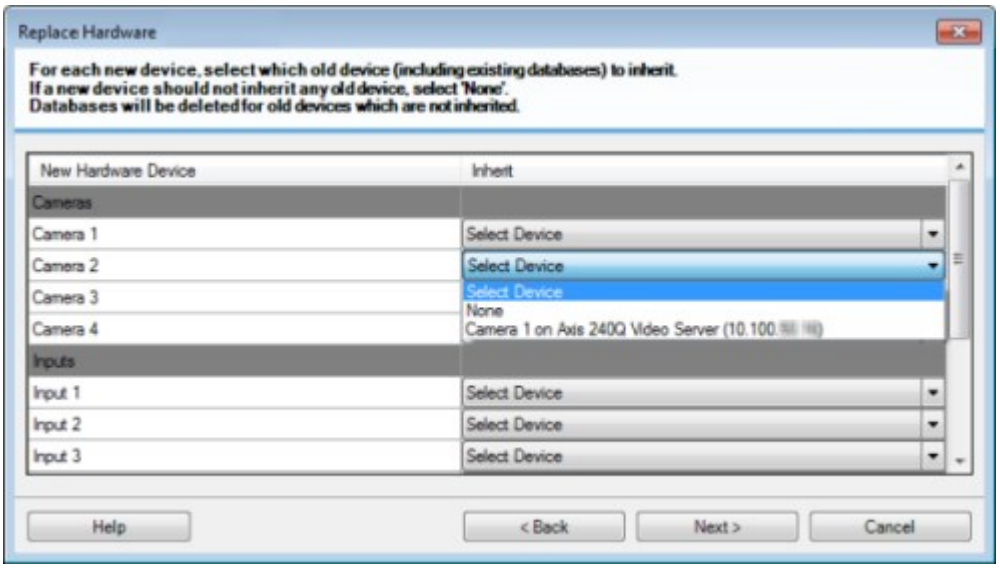
5. 以下のいずれか1つを実行します。

   - 必要なハードウェアデバイスのドライバーをリストから直接選択している場合は、**[次へ]**をクリックします。
   - リストで**[自動検出]**を選択している場合は、**[自動検出]**をクリックし、このプロセスが正常に完了するまで(左端に✔のマークが出るまで)待ってから、**[次へ]**をクリックします。

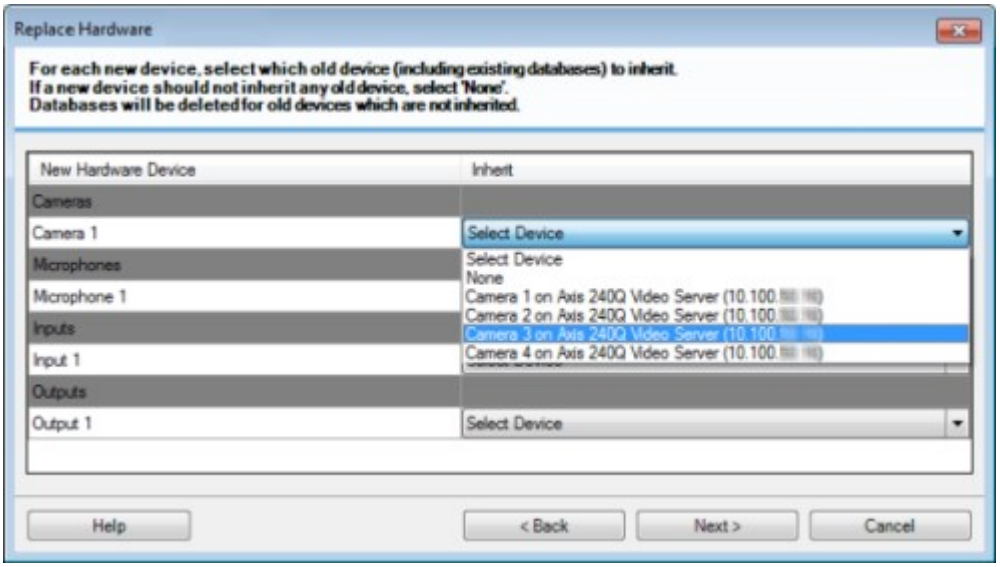
     この手順は、古いハードウェアデバイスと新しいハードウェアデバイスのそれぞれに取り付けられているカメラ、マイク、入力、出力などの数に応じて、デバイスとデータベースをマップするのに役立つように設計されています。

     古いハードウェアデバイスのデータベースから新しいハードウェアデバイスのデータベースへ、**どのように**マップするか検討することが重要です。個々のデバイスの実際のマッピングは、右側の列で対応するカメラ、マイク、入力、出力または**なし**を選択して行います。

     > ⚠ 必ず、**すべて**のカメラ、マイク、入力、出力などをマッピングしてください。**なし**にマッピングされた内容は**失われます**。



古いハードウェアデバイスに、新しいハードウェアデバイスより多くの個別のデバイスがある例



次へをクリックします。

6. 追加、交換または削除されるハードウェアの一覧が表示されます。**確認**をクリックします。
7. 最後の手順は、追加、交換および継承されるデバイスとその設定の概要です。**クリップボードへコピー**をクリックして、内容をWindowsクリップボードコピーするか、**閉じる**をクリックしてウィザードを終了します。

ハードウェアデータを更新してください

お使いのハードウェアデバイスとシステムが同じファームウェアバージョンを使用していることを確認するため、Management Clientでハードウェアデバイスのハードウェアデータを手動で更新する必要があります。Milestoneハードウェアデバイスに対してファームウェアアップデートを行う場合は毎回、アップデート後にハードウェアのデータを更新することを推奨しています。

最新のハードウェアデータを取得する場合：

1. **[サイトナビゲーション]**ペインで**レコーディングサーバー**を選択します。
2. 必要なレコーディングサーバーを拡張し、最新の情報を取得するハードウェアを選択します。
3. **[情報]**タブの**[プロパティ]**ペインの**[ハードウェアデータの最終更新日]**フィールドで**[更新]**ボタンをクリックします。
4. このウィザードは、システムがハードウェアの最新のファームウェアを実行しているかどうかを確認します。

   [確定]を選択し、ManagementClientで情報を更新します。アップデートが完了すると、システムによって検出されるハードウェアデバイスの現在のファームウェアのバージョンが、**[情報]**タブの**[ファームウェアバージョン]**フィールドに表示されます。

SQL Serverデータベースの場所と名前を変更する

マネジメントサーバー、イベントサーバー、ログサーバー、Identity Provider 、XProtectIncident Managerは、接続文字列を使用して異なるSQL Serverデータベースに接続しています。これらの接続文字列は Windowsのレジストリに保存されます。SQL Serverデータベースの場所や名前を変更した場合は、そのSQL Serverデータベースを指すすべての接続文字列を編集する必要があります。

データベース	使用者
監視データベース	• Management Serverサービス • Event Serverサービス • VideoOSManagement Serverアプリプール • VideoOS報告サーバーアプリプール
Surveillance_IDP .	• VideoOS IDPアプリプール
Surveilance_IM	• VideoOS IMアプリプール
Surveillance_LogServerV2	• Log Serverサービス

進む前に:

- SQL ServerデータベースとWindowsレジストリをバックアップします。
- 関連サービスとアプリプールを実行するユーザーがデータベースの所有者であることを確認します。
- 旧SQL Serverデータベースから新データベースへのコンテンツ移行を完了します。

SQL Serverデータベースの新しい場所と名前で接続文字列を更新する:

1. SQL Serverデータベースを使用するすべてのXProtect VMSサービスとアプリプールを停止します。

   > システムアーキテクチャによっては、サービスとアプリプールは異なるコンピューター上で実行されるかもしれません。同じSQL Serverデータベースに接続するすべてのアプリプールとサービスを停止する必要があります。

2. [Registry Editor]で、`HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\ConnectionString`を開きます。

3. SQL Serverデータベースの新しい場所と名前で接続文字列を更新します。

   すべてのSQL Serverデータベースのデフォルトの接続文字列は以下の通りです:

   - **ManagementServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **EventServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ServerService**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ReportServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IDP**:`Data Source=localhost;Initial Catalog=Surveillance_IDP;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IncidentManager**:`Data Source=localhost;Initial Catalog=Surveillance_IM;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **LogServer**: `Data Source=localhost;Initial Catalog=SurveillanceLogServerV2;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`

4. ステップ1で停止したすべてXProtectのサービスとアプリプールを起動します。

サーバーサービスの管理

サーバーサービスを実行するコンピュータでは、通知領域にサーバーマネージャートレイアイコンを見つけることができます。アイコンを使用すると、サービスの情報を取得し、特定のタスクを実行できます。これには、サービスのステータスの確認、ログまたはステータスメッセージの表示、サービスの開始と停止などがあります。

サーバーマネージャーのトレイアイコン(説明付き)

テーブルのトレイアイコンには、マネジメントサーバー、レコーディングサーバー、フェイルオーバーレコーディングサーバー、イベントサーバーを実行しているサービスの各種ステータスが示されます。これらは、サーバーがインストールされているコンピュータの通知領域に表示されます:

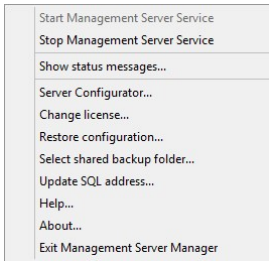
Management Server Manager トレーアイコン	Recording Server Manager トレーアイコン	Event Server Manager トレーアイコン	Failover Recording Server Manager トレーアイコン	説明
				**実行中** サーバーサービスが有効になって起動した際に表示されます。 Failover Recording Serverサービスが実行されている場合、標準レコーディングサーバーに不具合が生じた際に、このサービスが処理を引き継ぎます。
				**停止** サーバーサービスが停止した際に表示されます。 Failover Recording Serverサービスが停止した場合、標準レコーディングサーバーに不具合が生じても、このサービスが処理を引き継ぐことはできません。
				**開始中** サーバーサービスが開始プロセスに入った際に表示されます。通常の状態では、トレーアイコンはしばらくしてから**[実行中]**に変化します。
				**停止中** サーバーサービスが停止プロセスに入った際に表示されます。通常の状態では、トレーアイコンはしばらくしてから**[停止中]**に変化します。

Management Server Manager トレーアイコン	Recording Server Manager トレーアイコン	Event Server Manager トレーアイコン	Failover Recording Server Manager トレーアイコン	説明
				**中間状態** サーバーサービスが最初に読み込まれてから最初の情報を受信するまで表示されます。通常の状態では、トレーアイコンは**[開始中]**に、続いて**[実行中]**に変化します。
				**オフラインで実行** 通常はレコーディングサーバーまたはフェールオーバーレコーディングサーバーが実行されているものの、Management Serverサービスが実行されていない場合に表示されます。

Management Serverサービスの開始または停止

Management Server Managerトレイアイコンは、**実行中**などの、Management Serverサービスのステータスを示します。このアイコンを使用して、Management Serverサービスを開始、停止できます。Management Serverサービスが停止したときには、Management Clientは使用できません。

1. 通知領域で、Management Server Managerアイコンを右クリックします。コンテキストメニューが表示されます。



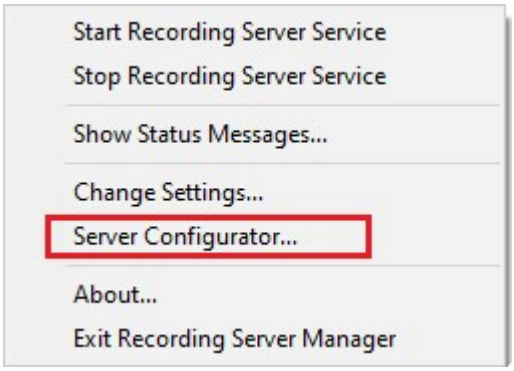
2. サービスが停止した場合は、**Management Serverサービス開始**をクリックして開始します。トレイアイコンが変わり、新しいステータスを示します。
3. サービスを停止するには、**Management Serverサービス停止**をクリックします。

> トレイアイコンの詳細については、332ページのサーバーマネージャーのトレイアイコン(説明付き)を参照してください。

Recording Serverサービスの開始または停止

Recording Server Managerトレイアイコンは、**実行中**などの、Recording Serverサービスのステータスを示します。このアイコンを使用して、Recording Serverサービスを開始、停止できます。Recording Serverサーバーを停止した場合は、サーバーに接続されたデバイスと連携できません。つまり、ライブビデオの表示またはビデオの録画ができません。

1. 通知領域で、Recording Server Managerアイコンを右クリックします。コンテキストメニューが表示されます。

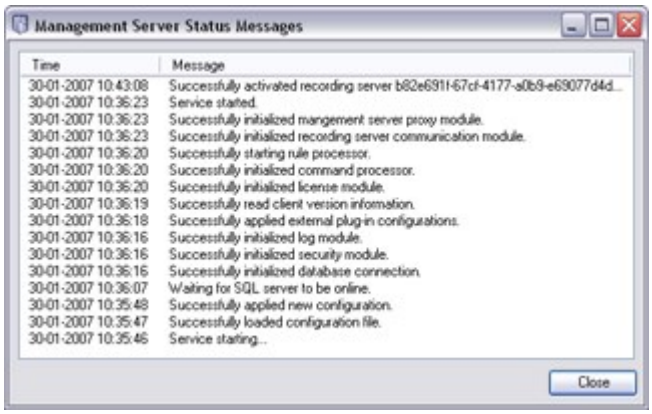


2. サービスが停止した場合は、**Recording Serverサービス開始**をクリックして開始します。トレイアイコンが変わり、新しいステータスを示します。
3. サービスを停止するには、**Recording Serverサービス停止**をクリックします。

> トレイアイコンの詳細については、332ページのサーバーマネージャーのトレイアイコン(説明付き)を参照してください。

マネジメントサーバーまたはレコーディングサーバーのステータスメッセージの表示

1. 通知領域で、該当するトレイアイコンを右クリックします。コンテキストメニューが表示されます。
2. **ステータスメッセージの表示**を選択します。サーバーの種類に応じて、**マネジメントサーバーのステータスメッセージ**または**レコーディングサーバーのステータスメッセージ**ウィンドウが表示され、タイムスタンプの付いたステータスメッセージが一覧表示されます。



暗号化をServer Configuratorで管理する

Server Configuratorを使用して、ローカルサーバーで暗号化された通信用の証明書を選択し、証明書によってサーバーとの通信が許可されるようにするためサーバーサービスを登録してください。

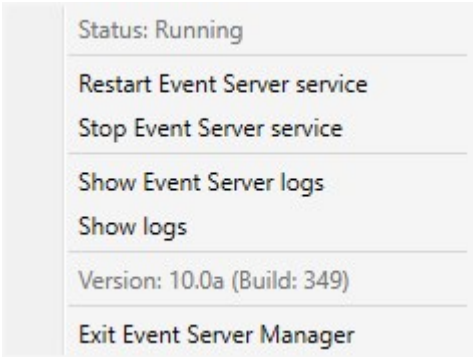
Windowsのスタートメニュー、マネジメントサーバーのトレイアイコンまたはレコーディングサーバーのトレイアイコンのいずれかからServer Configuratorを開きます。382ページのServer Configurator(ユーティリティ)を参照してください。

詳細については、XProtect VMSの保護方法に関する証明書ガイドを参照してください。

Event Serverサービスの開始、停止、再開

Event Server Managerトレイアイコンは、**実行中**などの、Event Serverサービスのステータスを示します。このアイコンを使用して、Event Serverサービスを開始、停止、再起動できます。サービスを停止する場合は、イベントとアラームを含むシステムの一部が動作しません。ただし、ビデオの表示と録画はできます。詳細については、337ページのEvent Serverサービスの停止を参照してください。

1. 通知領域で、Event Server Managerアイコンを右クリックします。コンテキストメニューが表示されます。



2. サービスが停止した場合は、**Event Serverサービス開始**をクリックして開始します。トレイアイコンが変わり、新しいステータスを示します。
3. サービスを再起動または停止するには、**EventServerサービスを再起動**または**EventServerサービス停止**をクリックします。

> トレイアイコンの詳細については、332ページのサーバーマネージャーのトレイアイコン(説明付き)を参照してください。

Event Serverサービスの停止

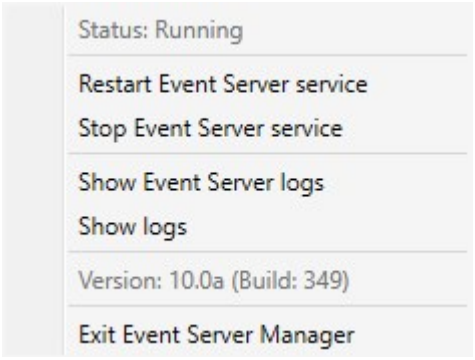
イベントサーバーにMIPプラグインをインストールする際には、まずEvent Serverサービスを停止してから再起動する必要があります。サービスの停止中は、VMSシステムの多くの領域が機能しなくなります。

- イベントやアラームはイベントサーバーに保存されません。ただし、システムおよびデバイスイベントはこの時点でも、録画の開始などのアクションをトリガーします。
- XProtect拡張機能は、XProtectSmartClientでは動作せず、またManagementClientから設定することもできません。
- アナリティクスイベントは動作しません。
- ジェネリックイベントは動作しません。
- アラームはトリガーされません。
- XProtect Smart Clientでは、マップビューアイテム、アラームリストビューアイテム、アラームマネージャーワークスペースは動作しません。
- イベントサーバーのMIPプラグインを実行できません。
- MIPおよびManagement ClientのXProtect Smart Clientプラグインは正しく動作しません。

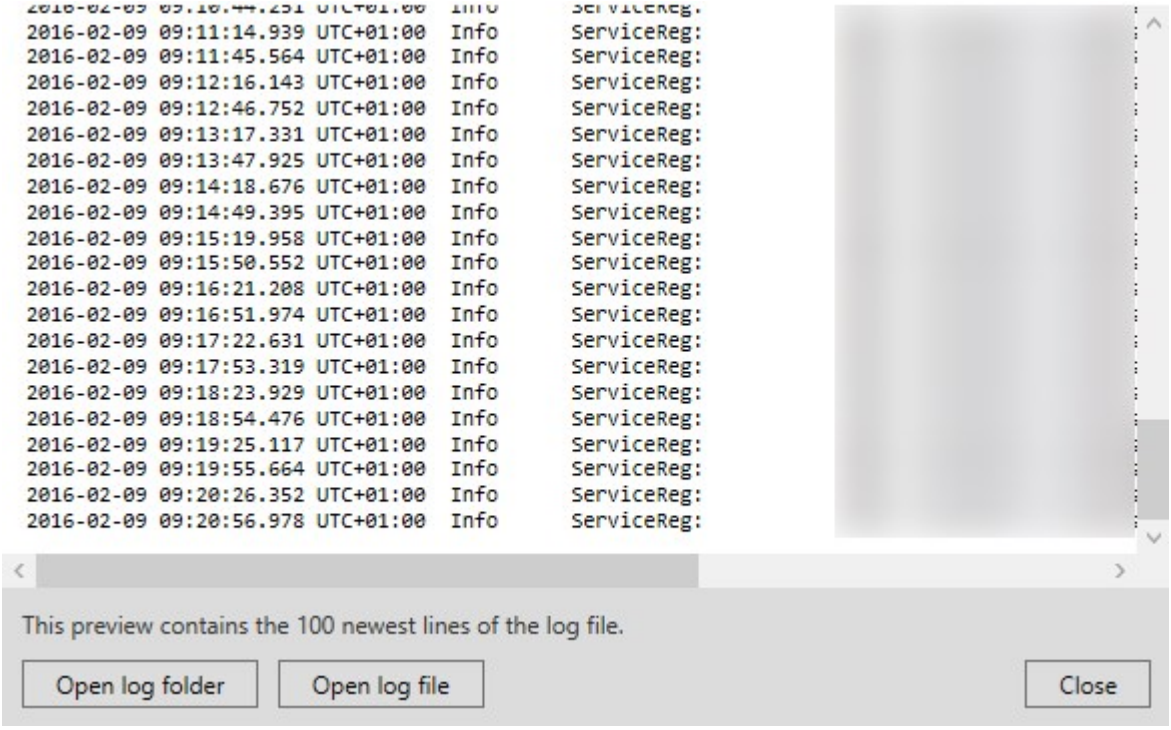
イベントサーバーまたはMIPログの表示

イベントサーバーログでは、イベントサーバーの動作に関するタイムスタンプ付き情報を表示できます。サードパーティ統合に関する情報は、**イベントサーバー**用フォルダーのサブフォルダーにあるMIPログに出力されます。

1. 通知領域で、Event Server Managerアイコンを右クリックします。コンテキストメニューが表示されます。



2. Event Serverログの最新の100行を表示するには、**[イベントサーバーログの表示]**をクリックします。ログビューアが表示されます。



   1. ログファイルを表示するには、**ログファイルを開く**をクリックします。
   2. ログフォルダーを開くには、**ログフォルダーを開く**をクリックします。

3. MIPログで最新の100行を表示するには、コンテキストメニューに戻り、**MIPログを表示**をクリックします。ログビューアが表示されます。

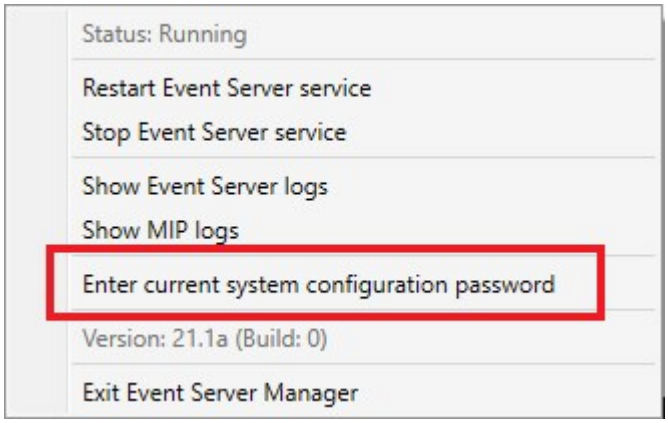
ログ用のディレクトリからログファイルが削除されると、メニューアイテムはグレーで表示されます。ログビューアを開くには、まずはログファイルをそのフォルダーに戻す(コピーする) 必要があります。
C:\ProgramData\Milestone\XProtect Event Server\logsまたは
C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs。

現在のシステム設定パスワードを入力する

マネジメントサーバーでシステム設定パスワードが変更されている場合、現在のシステム設定パスワードをイベントサーバーに入力する必要があります。

イベントサーバーに現在のパスワードを入力しないと、入退室管理といったシステムコンポーネントの機能が停止します。

1. 通知領域で、Event Server Managerアイコンを右クリックします。コンテキストメニューが表示されます。



2. 現在のシステム構成パスワードを入力するには、**現在のシステム設定パスワードを入力**をクリックします。ウィンドウが表示されます。
3. マネジメントサーバーに入力したものと同じシステム設定パスワードを入力します。

登録済みサービスの管理

場合によっては、システムとの通信機能が必要なサーバーまたはサービスのうち、システムに直接含まれていないものがあります。一部のサービスはシステムに自動的に登録できます(自動登録されないものもあります) 。自動登録可能なサービス:

- Event Serverサービス
- Log Serverサービス

自動登録されるサービスは、登録済みサービスのリストに表示されます。

サーバーまたはサービスは、Management Clientで登録済みサービスとして手動で指定できます。

登録済みサービスの追加と編集

1. **登録済みサービスの追加/削除**ウィンドウで、必要に応じて**追加**または**編集**をクリックします。
2. 前の選択により開いた**登録済みサービスの追加**または**登録済みサービスの編集**ウィンドウで、設定を指定または編集します。
3. **OK**をクリックします。

ネットワーク設定の管理

ネットワーク設定で、マネジメントサーバーのサーバーLANアドレスとWANアドレスを指定し、マネジメントサーバーと信頼済みサーバーが通信できるようにします。

1. **登録されているサービスの追加と削除**ウィンドウで、**ネットワーク**をクリックします。
2. マネジメントサーバーのLANおよび/またはWAN IPアドレスを指定します。

   すべての関係するサーバー(マネジメントサーバーと信頼済みサーバーの両方)がローカルネットワークにある場合は、LANアドレスを指定するだけです。1つまたは複数の関係するサーバーがインターネット接続でシステムにアクセスする場合は、WANアドレスも指定する必要があります。

3. **OK**をクリックします。

登録済みサービスのプロパティ

登録済みサービスの追加または**登録済みサービスの編集**ウィンドウで、以下を指定します。

コンポーネント	要件
タイプ	事前に入力されているフィールド。
名前	登録されているサービスの名前です。Management Clientでは名前は表示目的でのみ使用されます。
URL	**追加**をクリックし、登録済みサービスのIPアドレスまたはホスト名を追加します。URLの一部としてホスト名を指定する場合、そのホストが存在し、ネットワークで使用できる必要があります。URLは*http://*または*https://*から始まるものとし、以下の文字を使用してはなりません: *< > & ' " * ? | [ ]*.

コンポーネント	要件
	一般的なURL形式の**例**:*http://ipaddress:port/directory*(ポートおよびディレクトリはオプションです)。必要に応じて複数のURLを追加することもできます。
信頼済み	登録済みサービスをすぐに信頼済みにすべき場合に選択します(これが大半の場合に当てはまりますが、登録済みサービスを追加してから後で、これを編集して信頼済みにすることもできます)。 信頼済みステータスに変更すると、その登録済みサービスに定義した1つまたは複数のURLを共有する登録済みサービスの状態も変更されます。
説明	登録されているサービスの説明です。Management Clientでは、説明は表示目的でのみ使用されます。
詳細	サービスが高度な場合、定義するホストアドレスごとに特定のURIスキーマ(http、https、tcp、udpなど)を設定する必要があります。このため、ホストアドレスには複数のエンドポイントが含まれ、それぞれが独自のスキーマ、ホストアドレス、およびスキーマのIPポートを持ちます。

デバイスドライバの削除(説明付き)

デバイスドライバーがコンピュータ上で不要になった場合は、Device Packをシステムから削除できます。その場合は、プログラムを削除するWindowsの標準手順に従います。

複数のDevice Packがインストールされ、ファイルを削除してしまう問題がある場合は、Device Packのインストールフォルダーにあるスクリプトを使って完全に削除します。

デバイスドライバーを削除すると、レコーディングサーバーとカメラデバイスは通信できなくなります。アップグレード時にはDevice Packを削除しないでください。デバイスパックは、システム全体をアンインストールする場合にのみ削除してください。

レコーディングサーバーの削除

> **!** レコーディングサーバーを削除すると、そのレコーディングサーバーに関連付けられた**すべての**ハードウェア(カメラ、入力デバイスなど)について、Management Clientでそのレコーディングサーバーに対して指定したあらゆる設定が削除されます。

1. **概要**ペインで、削除するレコーディングサーバーを右クリックします。
2. **レコーディングサーバーを削除**を選択します。
3. 削除するには、**はい**をクリックします。
4. レコーディングサーバーと、関連するすべてのハードウェアが削除されます。

レコーディングサーバーでのすべてのハードウェアの削除

> ハードウェアを削除すると、ハードウェアに関連付けられたすべての録画データが完全に削除されます。

1. すべてのハードウェアを削除するレコーディングサーバーを右クリックします。
2. **すべてのハードウェアの削除**を選択します。
3. 削除を確認します。

マネジメントサーバーコンピュータのホスト名を変更

マネジメントサーバーのアドレスに完全修飾ドメイン名(FQDN)またはホスト名が含まれている場合、コンピュータのホスト名を変更すると、XProtect内でも影響が出る点を考慮して対応する必要があります。

> 一般的に、マネジメントサーバーのホスト名変更は後で多大なクリーンアップ作業が必要になる可能性があるため、慎重に計画してください。

ホスト名の変更が及ぼす影響の一部について、以下のセクションで概説します。

証明書の有効性

証明書はサービス間の通信を暗号化するために用いられますXProtect。

証明書は、その作成過程によってはインストール先のコンピュータに関連付けられたものとなることもあり、コンピュータ名を変更しない場合に限り有効となります。

証明書を作成する方法について詳しくは、「証明書について」を参照してください。

証明書は、その作成過程によってはインストール先のコンピュータに関連付けられたものとなることもあり、コンピュータ名を変更しない場合にXProtect VMS限り有効となります。システムを再び稼動させるには、以下のステップを完了してください。

- システムを再び稼動させるには、以下のステップを完了してください。
- 新しい証明書を作成し、これらServer Configuratorを環境内のすべてのコンピュータに再インストールします。

これにより、新しい証明書の登録がトリガーされ、システムを再稼働できるようになります。

これにより、新しい証明書の登録がトリガーされ、システムを再稼働できるようになります。

登録済みサービス用の顧客データプロパティの損失マネジメントサーバーアドレスの変更後などにServer Configuratorを使用して登録を完了すると、登録済みサービスの情報編集は上書きされます。登録済みサービスの情報に変更を加えた場合、名称が変更されたコンピュータ上のマネジメントサーバーに登録されている全サービスに対して、これらの変更を再適用する必要があります。

登録済みサービスに対して編集できる情報は、**[ツール] > [登録済みサービス] > [編集]**にあります。

- 信頼済み
- 詳細
- 外部フラグ
- 手動で追加したあらゆるURL

Milestone Customer Dashboardでは、ホスト名は変更されずに表示されます

Milestone Customer Dashboardは、ソフトウェアのインストールとライセンスを管理・Milestoneモニターできるようにパートナー、リセラー、XProtect VMS(Video Management Software[ビデオ管理ソフトウェア]) ユーザーに提供されている無料オンラインツールです。

Milestone Customer Dashboardに接続されているシステム上のマネジメントサーバー名を変更しても、Milestone Customer Dashboardには反映されません。

古いホスト名は、新しいライセンスアクティベーションが完了するまでMilestone Customer Dashboardに表示され続けます。ただし、名前を変更してもMilestone Customer Dashboardは一切の影響を受けません。新しいアクティベーションが実行されれば、記録は新しいホスト名が付けられたデータベース内で更新されます。Milestone Customer Dashboardの詳細については、「Milestone Customer Dashboard(説明付き) 」を参照してください。

ホスト名を変更するとSQL Serverアドレスが変化する可能性がある

SQL Serverがマネジメントサーバーと同じコンピュータに配置されている状態で、このコンピュータの名前が変更されると、SQL Serverのアドレスも変わります。つまり、異なるコンピュータのコンポーネントと、SQL Serverに接続するためにローカルホストではなくコンピュータ名を使用しているローカルコンピュータのコンポーネントで、SQL Serverアドレスを更新する必要があります。これは特にEvent Serverと同じデータベースを使用しているManagement Serverに当てはまります。また、異なるデータベースを使っているものの、SQL Serverが同じ可能性が高いLog Serverにも当てはまります。

331ページのSQL Serverデータベースの場所と名前を変更するを参照してください。

におけるホスト名の変更Milestone Federated Architecture

Milestone Federated Architectureセットアップ内のコンピュータの名前を変更すると、以下のような影響が生じます。これは、サイトが作業グループ内で接続されている場合と、複数のドメインをまたがって接続されている場合の両方に当てはまります。

サイトのホストがアーキテクチャ内のルートノードとなる

アーキテクチャ内の中央サイトが実行されているコンピュータの名前を変更すると、すべての子ノードが新しいアドレスに自動的に再接続されます。この場合、名前を変更するために何らかのアクションを実行する必要はありません。

サイトのホストがアーキテクチャ内の子ノードとなる

1つまたは複数のフェデレーテッドサイトを実行中のコンピュータの名前を変更する際に接続の問題を回避するには、コンピュータ名を変える前に影響の出るサイトに代替アドレスを追加しなくてはなりません。影響を受けるサイトが、ホストコンピュータの名前が変更されるノードである場合。準備不足または予測できないホスト名変更による接続の問題およびその解

決方法については、問題：Milestone Federated Architectureセットアップの親ノードが子ノードに接続できないを参照してください。

代替アドレスは、**プロパティ**ペインの**サイトナビゲーション**または**フェデレーテッドサイト階層**ペインのいずれかで追加してください。以下の前提条件を満たす必要があります。

- ホストコンピュータの名前を変更する前に大チアアドレスを追加して利用できるようにする
- 代替アドレスはホストコンピュータの新しい(変更後の)名前を反映しなくてはならない

プロパティペインへのアクセス方法については、サイトプロパティの設定を参照してください。

> アップデートをスムーズに行うため、ホスト名を変更するノードの親ノードとして機能しているノードでManagement Clientを停止します。これを行わない場合は、コンピュータ名の変更後にクライアントを停止し再起動してください、詳細については、Management Serverサービスの起動または停止を参照してください。

> また、提供した代替アドレスが中央サイトの**フェデレーテッドサイト階層**ペインで反映されていることを確認します。反映されていない場合はManagement Clientを停止し再起動してください。

ホスト名が変更され、コンピュータを再起動した後、フェデレーテッドサイトは自動的に新しいアドレスに切り替わります。

サーバーログの管理

サーバーログには以下の種類があります。

- システムログ
- 監査ログ
- ルールトリガーログ

これらは、システムの利用状況を記録するために用いられます。これらのログは、**[サーバーログ]**のManagement Clientで確認できます。

ソフトウェアエラーの調査およびトラブルシューティング用のログについては、「349ページのデバッグログ(説明付き)」を参照してください。

ユーザーアクティビティ、イベント、アクション、エラーの特定

ログを使用することで、システムにおけるユーザーアクティビティ、イベント、アクション、エラーについての詳細な記録を入手できます。

Management Clientでログを表示するには、**[サイトナビゲーション]**ペインに移動して**[サーバーログ]**を選択します。

ログタイプ	何がログをされているか?
システムログ	システム関連情報
監査ログ	ユーザーアクティビティ
ルール起動ログ	ユーザーが**新しい<ログエントリ>の作成**アクションを指定したルールを録画します。<ログエントリ>アクションの詳細については、「アクションと停止アクション」を参照してください。

別の言語でログを表示する方法については、**[オプション]**の「365ページの一般タブ(オプション)」を参照してください。

コンマで区切られた値(.csv)ファイル形式でログをエクスポートするには、ログのエキスポートをご覧ください。

ログ設定を変更する方法については、「367ページのサーバーログタブ(オプション)」を参照してください。

ログにフィルターをかける

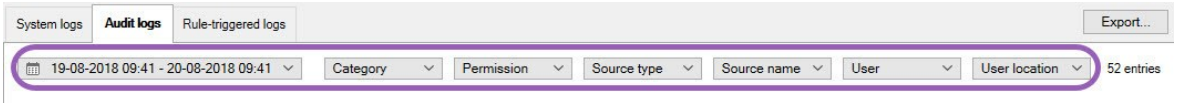
それぞれのログウィンドウでは、ログにフィルターをかけることで、特定の時間帯、デバイス、ユーザーなどに関連するログエントリを確認することができます。

フィルターは、現在ユーザーインターフェースに表示されているログエントリから生成されます。

1. **[サイトナビゲーション]**ペインで、**[サーバーログ]**を選択します。デフォルトでは、**システムログ**タブが表示されます。

   ログタイプ間をナビゲートするには、別のタブを選択してください。

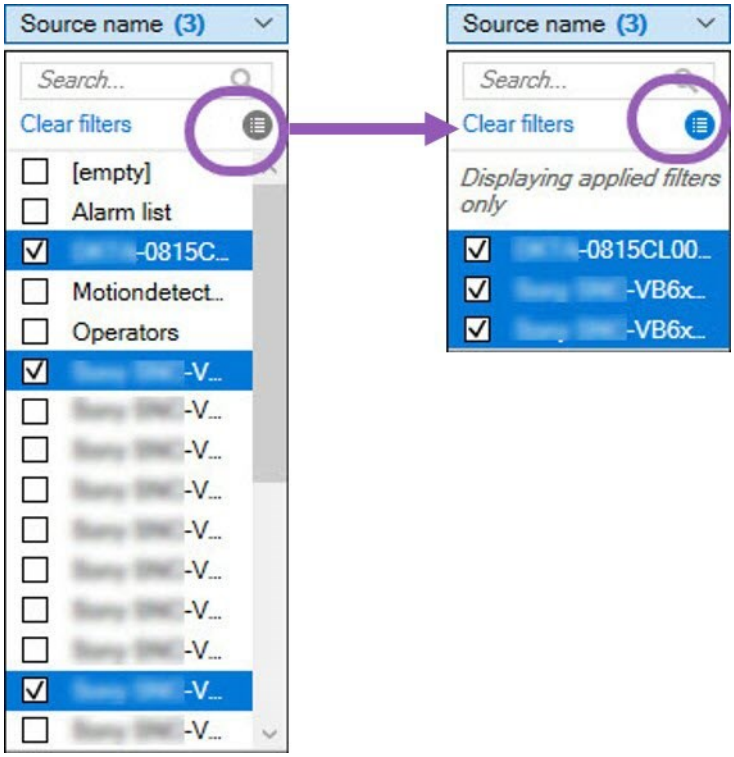
2. このタブの下では、**[カテゴリー]**、**[ソースタイプ]**、あるいは**[ユーザー]**のようなフィルターグループを選択します。



   フィルターのリストが表示されます。フィルターのリストには、最大で1000のフィルターが表示されます。

3. 使用するフィルターを選択します。フィルターを除去するには、もう一度選択します。

   オプション: フィルターのリストで、アプライしたフィルターのみを閲覧するには、**使用したフィルターのみを表示する**を選択します。



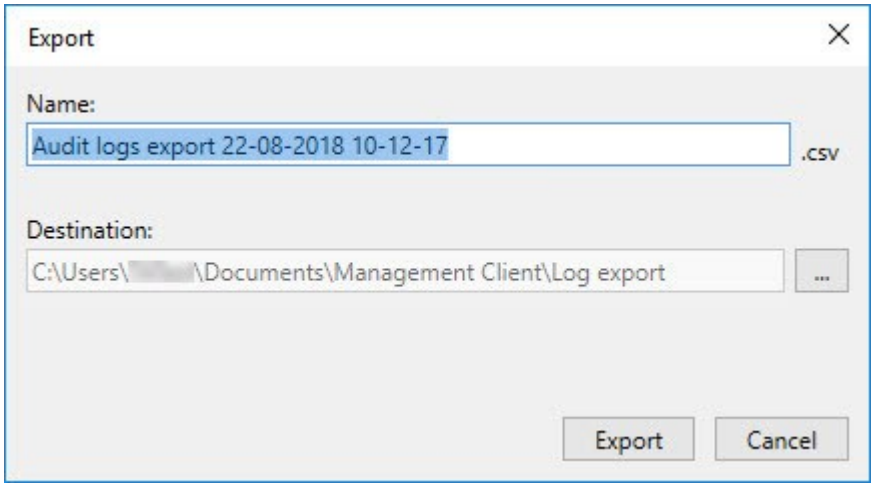
ログのエクスポート時にどのようなコンテンツがエクスポートされるかは、適用したフィルターに応じて変化します。エクスポートの詳細については、ログのエクスポート。

ログのエクスポート

ログのエクスポートは、ログの保存期間を越えてログエントリーを保存する、というように便利に活用できます。ログはコンマ区切り値 (.csv) ファイルとしてクスポートできます。

ログをエクスポートするには:

1. 右上コーナーの**[エクスポート]**を選択します。**Export**ウィンドウが表示されます。



2. **[Name]**ウィンドウにおける**[Export]**フィールドで、ログファイルのための名前を指定します。
3. デフォルトでは、**ログのエクスポート**フォルダーにエクスポートしたファイルが保存されます。別のロケーションを指定するには、...[Destination]**フィールドの右**を選択します。
4. ログをエクスポートするには**[Export]**を選択します。

あなたのエクスポートのコンテンツは、使用されたフィルターによって異なります。エクスポートの詳細については、フィルタログ。

ログの検索

ログを検索するには、[ログ]ペイン上部の**[検索条件]**を以下のように使用します。

1. リストで検索条件を指定します。
2. **[更新]**をクリックして、指定した検索基準をログページに反映させます。検索基準をクリアして、ログの全コンテンツが表示される状態に戻すには、**[クリア]**をクリックします。

いずれの行をダブルクリックすると、すべての詳細が**[ログの詳細]**ウィンドウに表示されます。これにより、テキストが単一の行に収まらないログエントリについても確認できます。

ログの言語を変更

1. [ログ]ペイン下部の**[ログの表示言語]**リストで、希望の言語を選択します。

2. ログが、選択した言語で表示されます。次回ログを開く際には、デフォルトの言語にリセットされます。

ログを録画するため、2018 R2およびそれ以前のコンポーネントを許可します

ログサーバーの2018 R3バージョンは、強化されたセキュリティのため認証を導入します。これにより、2018 R2およびそれ以前のコンポーネントによってログがログサーバーに書き込まれるのを防ぐことができます。

影響を受けるコンポーネント:

- XProtect Smart Client
- XProtect LPRﾌﾟﾗｸﾞｲﾝ
- LPR Server
- アクセスコントロール プラグイン
- イベントサーバー
- アラーム プラグイン

上記に記載されているコンポーネントの、2018 R2あるいはそれ以前のバージョンをお使いの場合、コンポーネントの新しいログサーバーへの書き込みを許可するかどうかを決定しなければなりません:

1. **[ツール]>[オプション]**を選択します。
2. **[サーバーログ]**タブの最下部にある**[オプション]**ダイアログボックスで、**2018 R2およびそれ以前のコンポーネントのログの書き込みの許可**チェックボックスを探します。
    - 2018 R2およびそれ以前のコンポーネントのログの書き込みを許可する場合、チェックを入れます。
    - 2018 R2およびそれ以前のコンポーネントのログの書き込みを許可しない場合、チェックを外します。

トラブルシューティング

デバッグログ(説明付き)

デバッグログは、システムの障害や不具合を特定するために使用します。

システムの使用状況が記録されるログについては、「344ページのサーバーログの管理」を参照してください。

XProtectインストールのログファイルは以下の場所に保管されます:

- C:\ProgramData\Milestone\IDP\Logs

  これには、IISユーザーおよび管理者しかアクセスできません。IISユーザーが変更された場合、これらの許可を更新する必要があります。

- C:\ProgramData\Milestone\MIPSDK
- C:\ProgramData\Milestone\XProtect Data Collector Server\Logs
- C:\ProgramData\Milestone\XProtect Event Server\Logs
- C:\ProgramData\Milestone\XProtect Log Server
- C:\ProgramData\Milestone\XProtect Management Server\Logs
- C:\ProgramData\Milestone\XProtect Mobile Server\Logs
- C:\ProgramData\Milestone\XProtect Recording Server\Logs
- C:\ProgramData\Milestone\XProtect Report Web Server\Logs

問題:SQL Serverとデータベースのロケーションを変更すると、データベースにアクセスできなくなる

SQL Serverを実行しているコンピュータのホスト名が変更されるなどして、SQL ServerとVMSのロケーションが変更されると、レコーディングサーバーからデータベースへのアクセスが失われます。

解決策:接続文字列を変更し、SQL Serverとデータベースの変更を反映する。331ページのSQL Serverデータベースの場所と名前を変更するを参照してください。

問題:ポートの競合が原因でレコーディングサーバーを起動できない

この問題は、ポート25を使用する簡易メール転送プロトコル(SMTP)サービスが実行されている場合にのみ発生します。このサービスによってポート25がすでに使用されている場合は、Recording Serverサービスを起動できない可能性があります。レコーディングサーバーのSMTPサービスに対してポート番号25が使用できる状態になっていることが重要です。

SMTPサービス: 確認と解決策

SMTPサービスがインストールされていることを確認するには:

1. Windowsの**[スタート]**メニューで**[コントロールパネル]**を選択します。
2. **[コントロール パネル]**で**[プログラムの追加と削除]**をダブルクリックします。
3. **[プログラムの追加と削除]**ウィンドウの左側で、**[Windowsコンポーネントの追加と削除]**をクリックします。
4. **[Windowsコンポーネント]**ウィザードで**[インターネットインフォメーションサービス(IIS)]**を選択し、**[詳細]**をクリックします。
5. **[インターネット インフォメーション サービス (IIS)]**ウィンドウで、**[SMTPサービス]**チェックボックスが選択されていることを確認します。選択されていれば、SMTPサービスはインストールされています。

SMTPサービスがインストールされている場合は、以下のいずれかの解決策を講じます:

解決策1: SMTPサービスを無効にするか、手動スタートアップに設定する

この解決策により、毎回SMTPサービスを停止することなく、レコーディングサーバーを起動できます:

1. Windowsの**[スタート]**メニューで**[コントロールパネル]**を選択します。
2. **[コントロール パネル]**で**[管理ツール]**をダブルクリックします。
3. **[管理ツール]**ウィンドウで**[サービス]**をダブルクリックします。
4. **[サービス]**ウィンドウで**[簡易メール転送プロトコル (SMTP)]**をダブルクリックします。
5. **[SMTPプロパティ]**ウィンドウで**[停止]**をクリックし、**[スタートアップの種類]**を**[手動]**または**[無効]**に設定します。

   [手動]に設定した場合、SMTPサービスを**[サービス]**ウィンドウから手動で、または*net start SMTPSVC*コマンドを使用してコマンドプロンプトから起動できます。
6. **OK**をクリックします。

解決策2: SMTPサービスを削除する

SMTPサービスを削除すると、SMTPサービスを使用している他のアプリケーションに影響が及ぶ可能性があります。

1. Windowsの**[スタート]**メニューで**[コントロールパネル]**を選択します。
2. **[コントロール パネル]**ウィンドウで**[プログラムの追加と削除]**をダブルクリックします。
3. **[プログラムの追加と削除]**ウィンドウの左側で、**[Windowsコンポーネントの追加と削除]**をクリックします。
4. **[Windowsコンポーネント]**ウィザードで**[インターネット インフォメーション サービス (IIS)]**のアイテムを選択し、**[詳細]**をクリックします。
5. **[インターネット インフォメーション サービス (IIS)]**ウィンドウで、**[SMTPサービス]**チェックボックスをオフにします。
6. **[OK]**、**[次へ]**、**[終了]**の順にクリックします。

問題：Recording Serverが、Management Serverクラスタノードを切り替える際にオフラインになる

Management Server冗長性に対してMicrosoftクラスタを設定した場合、クラスタノード間でRecording Serverを切り替える際に、Recording ServerまたはManagement Serverもオフラインになる場合があります。

これを修正するには、以下を実行します。

> 構成を変更する場合は、Microsoftフェールオーバークラスターマネージャーで、サービスのコントロールとモニタリングを一時停止し、Server Configuratorが変更を行ってManagement Serverサービスを起動 / 停止できるようにします。フェールオーバークラスターサービスのセットアップタイプを手動に変更しても、Server Configuratorとは矛盾しないはずです。

Management Serverコンピュータで以下を実行します。

1. マネジメントサーバーがインストールされている各コンピュータでServer Configuratorを起動します。
2. **[登録]**ページに移動します。
3. 鉛筆( ) の記号をクリックして、マネジメントサーバーのアドレスを編集可能にします。
4. マネジメントサーバーアドレスをクラスターのURLに変更します(例：`http://MyCluster`) 。
5. **[登録]**をクリックします。

Management Server(Recording Server、Mobile Server、Event Server、API Gatewayなど) を使用するコンポーネントを備えたコンピューターの場合：

1. 各コンピュータでServer Configuratorを起動します。
2. **[登録]**ページに移動します。
3. マネジメントサーバーアドレスをクラスターのURLに変更します(例：`http://MyCluster`) 。
4. **[登録]**をクリックします。

問題：Milestone Federated Architectureセットアップの親ノードが子ノードに接続できない

Milestone Federated Architectureで子ノードとして機能するサイトのホストコンピュータ名を変更すると、親ノードはそれに接続できなくなります。

親ノードとサイトとの間の接続を再度確立するには

- 対象のサイトを親から分離します。詳細については、「階層からサイトを分離」を参照してください。
- ホストの新しい名前を使用してサイトに再接続します。さらなる情報に関しては、階層にサイトを追加するを参照してください。

変更が有効なことを確認するには、ホスト名が変更されたノードの親ノードとして機能するノード上でManagement Clientを停止して再起動します。詳細については、Management Serverサービスの起動または停止を参照してください。

Milestone Federated Architectureセットアップでホスト名を変更することでもたらされる影響については、「Milestone Federated Architectureにおけるホスト名の変更」を参照してください。

問題：Azure SQL Databaseサービスが利用できない

Azure SQL Databaseを使用していて、インストール中または通常の操作中に接続の問題が発生した場合、Azure SQL Databaseサービスが一時的に利用できないことが原因である可能性があります。

Azure SQL Databaseは、従来のデータベースのメンテナンスのほとんどをマイクロソフトが行うサービスです。このサービスは短期間利用できなくなることがありますが、ユーザーによる操作を必要とせず、ある程度まで回復するように設計されています。

データベースエラーは、関連するインシデントIDとともにXProtect VMSログファイルに書き込まれ、Azure SQL Databaseが長時間使用できない場合にMicrosoftサポートに提供されます。

詳細については、Azure SQL Database への一般的な接続に関する問題のトラブルシューティングを参照してください。

アップグレード

アップグレード(説明付き)

アップグレード時には、現在コンピュータにインストールされているすべてのコンポーネントがアップグレードされます。アップグレード中にインストール済みコンポーネントを削除することはできません。インストール済みコンポーネントを削除するには、アップグレードの前後にWindowsの**「プログラムの追加と削除」**機能を使用します。アップグレード時には、マネジメントサーバーのデータベースを除く、すべてのコンポーネントが自動的に削除および置換されます。これにはデバイスパックのドライバーも含まれます。

マネジメントサーバーのデータベースは、システム全体の設定(レコーディングサーバーの設定、カメラの設定、ルールなど)を含んでいます。マネジメントサーバーのデータベースを削除しない限り、システムの設定を再構成する必要はありません(ただし、新しいバージョンの新機能の設定が必要になる場合もあります)。

現在のバージョン以前のXProtectバージョンのレコーディングサーバーとの下位互換性には制限があります。旧バージョンのレコーディングサーバーの録画にもアクセスすることはできますが、設定を変更するには、現在のバージョンと同じバージョンである必要があります。このため、Milestoneはシステムのすべてのレコーディングサーバーをアップグレードすることを推奨しています。

レコーディングサーバーを含めてアップグレードすると、ビデオデバイスドライバーを更新するか保持するかを確認するメッセージが表示されます。更新を選択すると、システムの再起動後、ハードウェアデバイスが新しいビデオデバイスドライバーと接続するまでに数分かかる場合があります。これは、新しくインストールされたドライバーについて、いくつかの内部チェックが行われるためです。

バージョン2017 R3以前のバージョンから、2018 R1以降のバージョンにアップグレードした後に、システムに古いカメラが残っている場合は、弊社ウェブサイト(https://www.milestonesys.com/downloads/)のダウンロードページから、レガシードライバーが含まれるデバイスパックを手動でダウンロードする必要があります。レガシーデバイスパックに含まれるドライバーを使用するカメラが存在するかどうかを確認するには、弊社ウェブサイトの「https://www.milestonesys.com/community/business-partner-tools/device-packs/」ページを参照してください。

2018 R1以前のバージョンから、2018 R2以降のバージョンに更新した場合は、アップグレードを開始する前に、システムのすべてのレコーディングサーバーをセキュリティパッチでアップデートすることが重要です。セキュリティパッチなしでアップグレードすると、レコーディングサーバーに不具合が生じる可能性があります。

レコーディングサーバーにセキュリティパッチをインストールする方法については、弊社ウェブサイト (https://supportcommunity.milestonesys.com/s/article/XProtect-VMS-NET-security-vulnerability-hotfixes-for-2016-R1-2018-R1/) を参照してください。

マネジメントサーバーとレコーディングサーバー間の接続を暗号化するには、すべてのレコーディングサーバーを2019 R2以降のバージョンにアップグレードしてください。

推奨されるアップグレード手順の概要については、356ページのアップグレードのベストプラクティスをご参照ください。

アップグレード要件

- ソフトウェアライセンスファイル(.lic) (106ページのライセンス(説明付き)を参照) を手元に用意します。
  - **サービスパックアップグレード**: マネジメントサーバーのインストール中に、ウィザードで、ソフトウェアライセンスファイルの場所を指定しなければならない場合があります。システム(または最新のアップグレード)の購入後に入手したソフトウェアライセンスコードと、最後のライセンスアクティベーションの後に入手したアクティベーション済みソフトウェアライセンスファイルの両方を使用できます。
  - **バージョンアップグレード**: 新しいバージョンを購入した後で、新しいソフトウェアライセンスファイルを受け取ります。マネジメントサーバーのインストール中に、ウィザードで、新しいソフトウェアライセンスファイルの場所を指定する必要があります

  続行する前に、ソフトウェアライセンスファイルがシステムで検証されます。すでに追加されたハードウェアデバイスとライセンスが必要なその他のデバイスは、猶予期間に入ります。自動ライセンスアクティベーション(112ページの自動ライセンスアクティベーションを有効にするを参照)を有効にしていない場合は、猶予期間が切れる前に必ずライセンスを手動でアクティベートしてください。ソフトウェアライセンスファイルがない場合は、XProtectのリセラーまでお問い合わせください。
- **新しい製品バージョン**のソフトウェアを用意してください。Milestoneウェブサイトのダウンロードページからダウンロードできます。
- システム設定のバックアップが作成済みとなっていることを確認します(313ページのシステム設定のバックアップおよび復元についてを参照)。

  マネジメントサーバーのSQLServerデータベースにはシステム設定が保存されます。SQLServerデータベースは、マネジメントサーバーのマシン本体上のSQLServerインスタンス、またはネットワーク上のSQLServerインスタンスに配置できます。

  SQL Serverデータベースをネットワーク上のSQL Serverインスタンスで使用する場合、SQL Serverデータベースを作成、移動、アップグレードするには、SQL Serverインスタンス上のマネジメントサーバーに管理者権限が必要になります。SQL Serverデータベースの日常的な使用とメンテナンスについては、マネジメントサーバーはデータベース所有者権限のみ必要とします。
- インストール中に暗号化を有効にしたい場合は、該当するコンピュータに適切な認証がインストールされ信頼されている必要があります。詳細については、136ページの安全な通信(説明付き)を参照してください。

アップグレードを開始する準備が整ったら、356ページのアップグレードのベストプラクティスの手順を実行します。

FIPS 140-2準拠モードで実行するようXProtect VMSをアップグレードする

2020 R3バージョンから、XProtect VMSはFIPS 140-2準拠アルゴリズムのインスタンスのみを使用して実行するよう設定されています。

FIPS 140-2準拠モードで実行するようにXProtect VMSを設定する方法の詳細については、ハードニングガイドのFIPS 140-2準拠セクションを参照してください。

> FIPS非準拠暗号で暗号化されている2017 R1よりも前のXProtect VMSのバージョンからのエクスポートとアーカイブ済みメディアデータベースを持つFIPS 140-2準拠システムでは、FIPSを有効にした後でもアクセスできる場所でデータをアーカイブする必要があります。

以下のプロセスで、XProtect VMSをFIPS 140-2準拠モードで実行するよう設定するには、何が必要かを説明します。

1. VMSに含まれているすべてのコンピュータでWindows FIPSセキュリティポリシーを無効にします(SQL Serverをホストしているコンピュータも含まれます)。

   アップグレードの際、FIPSがWindowsオペレーティングシステムで有効になっていると、XProtect VMSをインストールできません。

2. FIPSが有効になっているWindowsオペレーティング システムで、スタンドアロンのサードパーティー統合を実行できることを確認します。

   スタンドアロン統合がFIPS 140-2に準拠していない場合、Windowsオペレーティングシステムを FIPSモードで稼働するよう設定した後、システムを実行できなくなります。

   これを回避するには、以下を行います。

   - XProtect VMSへのすべてのスタンドアロン統合のインベントリを作成します。
   - 統合のプロバイダーに問い合わせ、統合がFIPS 140-2準拠かどうかを確認します。
   - FIPS 140-2準拠のスタンドアロン統合を展開します。

3. ドライバー、つまりデバイスとの通信がFIPS 140-2に準拠していることを確認します。

   XProtect VMSは、以下の基準が満たされると、確実にFIPS 140-2準拠モードの稼働を強制できます。

   - デバイスからXProtect VMSに接続する際には、準拠ドライバーのみが使用されます

     コンプライアンスを保証、強化できるドライバーの詳細については、ハードニングガイドのFIPS 140-2準拠セクションを参照してください。

   - デバイスは、バージョン11.1以降のデバイスパックを使用します

     レガシードライバーデバイスパックのドライバーでは、FIPS 140-2に準拠した接続は保証されません。

   - デバイスはHTTPSを介して接続されるほか、ビデオストリームではHTTPSを介してSecure Real-Time Transport Protocol(SRTP) またはReal Time Streaming Protocol(RTSP) のいずれかで接続されます。

     > ドライバーモジュールは、HTTPを介した接続のFIPS140-2準拠を保証できません。接続は準拠している可能性がありますが、実際に準拠しているという保証はありません。

   - レコーディングサーバーを実行するコンピュータは、FIPSモードが有効になっている状態でWindowsOSを実行します。

4. メディアデータベースのデータがFIPS 140-2準拠の暗号で暗号化されていることを確認します。

   これを行うには、メディアデータベースアップグレードツールを実行します。FIPS140-2準拠モードで実行するようにXProtectVMSを設定する方法の詳細については、ハードニングガイドのFIPS140-2準拠セクションを参照してください。

5. WindowsオペレーティングシステムでFIPSを有効にする前、また、XProtect VMSシステムを設定して、すべてのコンポーネントとデバイスがFIPSの有効な環境で実行できることを確認した後、XProtect Management Clientで既存のハードウェアのパスワードを更新します。

   これを行うには、Management Clientの**レコーディングサーバー**ノードで選択されたレコーディングサーバーで、**ハードウェアを追加**を右クリックして選択します。**ハードウェアを追加**ウィザードを実行します。これにより、現在の認証情報がすべて更新され、FIPSに準拠するよう暗号化されます。

すべてのクライアントを含むVMS全体をアップグレードした後に、FIPSを有効にします。

アップグレードのベストプラクティス

実際にアップグレードを開始する前に、SQL Serverデータベースのバックアップなど、アップグレードの要件を確認してください(354ページのアップグレード要件を参照)。

デバイスドライバーは2つのデバイスパックに分かれています: より新しいドライバーのレギュラーデバイスパックと、古いバージョンのドライバーのレガシーデバイスパックです。レギュラーデバイスパックは常に、更新あるいはアップグレード時に自動でインストールされます。レガシーデバイスパックからのデバイスドライバーを使用する古いカメラがある場合や、レガシーデバイスパックをまだインストールしていない場合、システムはレガシーデバイスパックを自動でインストールしません。

システムに古いバージョンのカメラが含まれる場合、Milestoneは、そのカメラがレガシーデバイスパックに含まれるドライバーを使用しているかどうかを「https://www.milestonesys.com/community/business-partner-tools/device-packs/」ページで確認するよう推奨しています。レガシーパックをすでにインストールしているかどうかをチェックするには、XProtectシステムフォルダーをチェックします。レガシーデバイスパックをダウンロードする必要がある場合は、ダウンロードページ(https://www.milestonesys.com/downloads/) にアクセスします。

シングルコンピュータシステムの場合、新しいソフトウェアを既存のインストールに追加でインストールできます。

Milestone InterconnectまたはMilestone Federated Architectureシステムでは、まず中央サイトをアップグレードし、その後リモートサイトもアップグレードしなくてはなりません。

分散システムでは、以下の順序でアップグレードします。

1. インストーラの**カスタム**オプションを使用してマネジメントサーバーをアップグレードします(147ページのシステムのインストール - カスタムオプションを参照) 。
    1. コンポーネントを選択するウィザードのページでは、すべてのマネジメントサーバーのコンポーネントがあらかじめ選択されています。
    2. SQL Serverとデータベースを指定します。データベース内の既存のデータを維持するため、すでに使用しているSQL Serverデータベースを維持するかどうかを決定します。

    インストールを開始すると、フェールオーバーレコーディングサーバーは機能しなくなります(37ページのフェールオーバーレコーディングサーバー(説明付き) を参照) 。

    マネジメントサーバーで暗号化を有効にすると、レコーディングサーバーはアップグレードされ、マネジメントサーバーの暗号化が有効に設定されるまでオフラインとなります(136ページの安全な通信(説明付き) を参照) 。

2. フェールオーバーレコーディングサーバーをアップグレードします。マネジメントサーバーのダウンロードウェブページから(Download Managerがコントロール) Recording Serverをインストールします。

> ⚠ フェールオーバーレコーディングサーバーにおいて暗号化を有効にする場合、また、フェールオーバー機能を維持する場合は、暗号化をせずにフェールオーバーレコーディングサーバーをアップグレードし、その後で暗号化を有効にします。

この時点で、フェールオーバーサーバー機能が回復します。

3. レコーディングサーバーまたはフェールオーバーレコーディングサーバーからクライアントへの暗号化を有効にする場合は、クライアントがアップグレードの間にデータを取得することができるようにし、レコーディングサーバーのアップグレードの前にレコーディングサーバーからデータストリームを取得するすべてのクライアントとサービスをアップグレードしておくことが重要です。該当するクライアントとサービスは以下のとおりです。
   - XProtect Smart Client
   - Management Client
   - Management Server
   - XProtect Mobileサーバー
   - XProtect Event Server
   - DLNA Server Manager
   - Milestone Open Network Bridge
   - Milestone Interconnectを通してレコーディングサーバーからデータストリームを取得するサイト
   - 一部のMIP SDKサードパーティー統合
4. レコーディングサーバーをアップグレードします。レコーディングサーバーはインストールウィザードを使用してインストールするか(155ページのDownload Managerを介したレコーディングサーバーのインストールを参照)、サイレントでインストールできます(162ページのレコーディングサーバーのサイレントインストールを参照)。サイレントインストールの利点は、遠隔で行うことができることです。

> ⚠ 暗号化を有効にし、選択したサーバー認証が該当する実行中のコンピュータで信頼されない場合は、コンピュータの接続は切断されます。詳細については、136ページの安全な通信(説明付き)を参照してください。

システムの他のサイトでもこの手順を繰り返します。

クラスタでのアップグレード

クラスタを更新する前に、データベースのバックアップを行います。

1. クラスタにあるすべてのマネジメントサーバーで、Management Serverサービスを停止します。
2. クラスタにあるすべてのサーバーから、マネジメントサーバーをアンインストールします。
3. クラスタへのインストールの説明に従って、マネジメントサーバーをクラスタにインストールするための手順を実行します。168ページのクラスタへのインストールを参照してください。

インストール時には、現在システム設定が保存されている既存のSQL Serverと既存のSQL Serverデータベースを必ず再利用してください。システム設定は自動的にアップグレードされます。

ユーザーインターフェイスの詳細

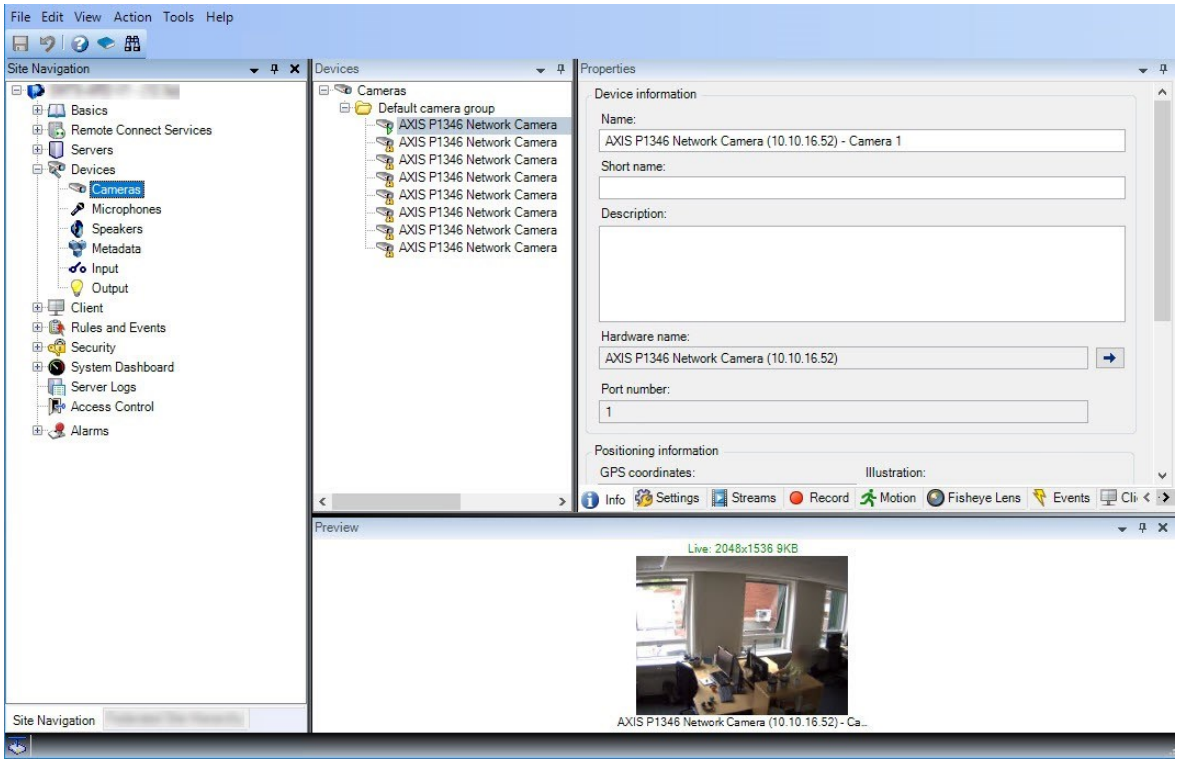
メインのウィンドウとペイン

Management Clientウィンドウはペインに分割されます。ペインとレイアウトの数は以下によって異なります。

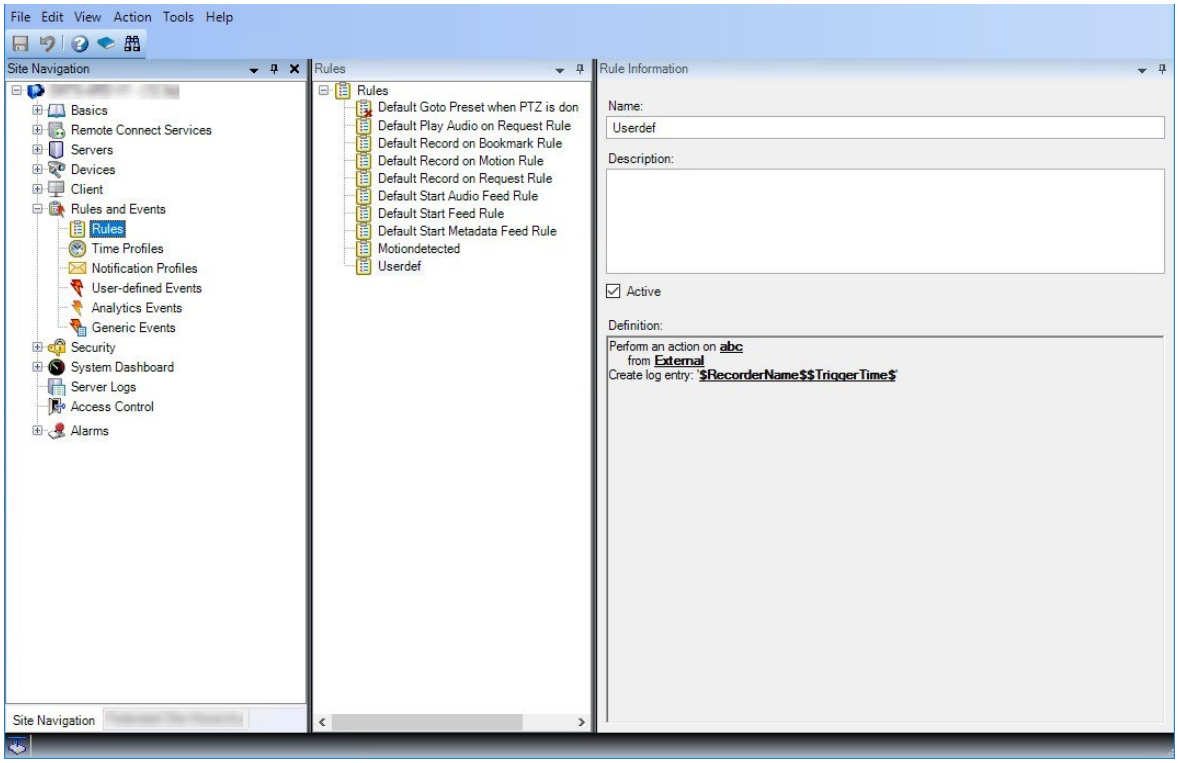
- システム構成
- タスク
- 使用可能な機能

以下は通常のレイアウト例です:

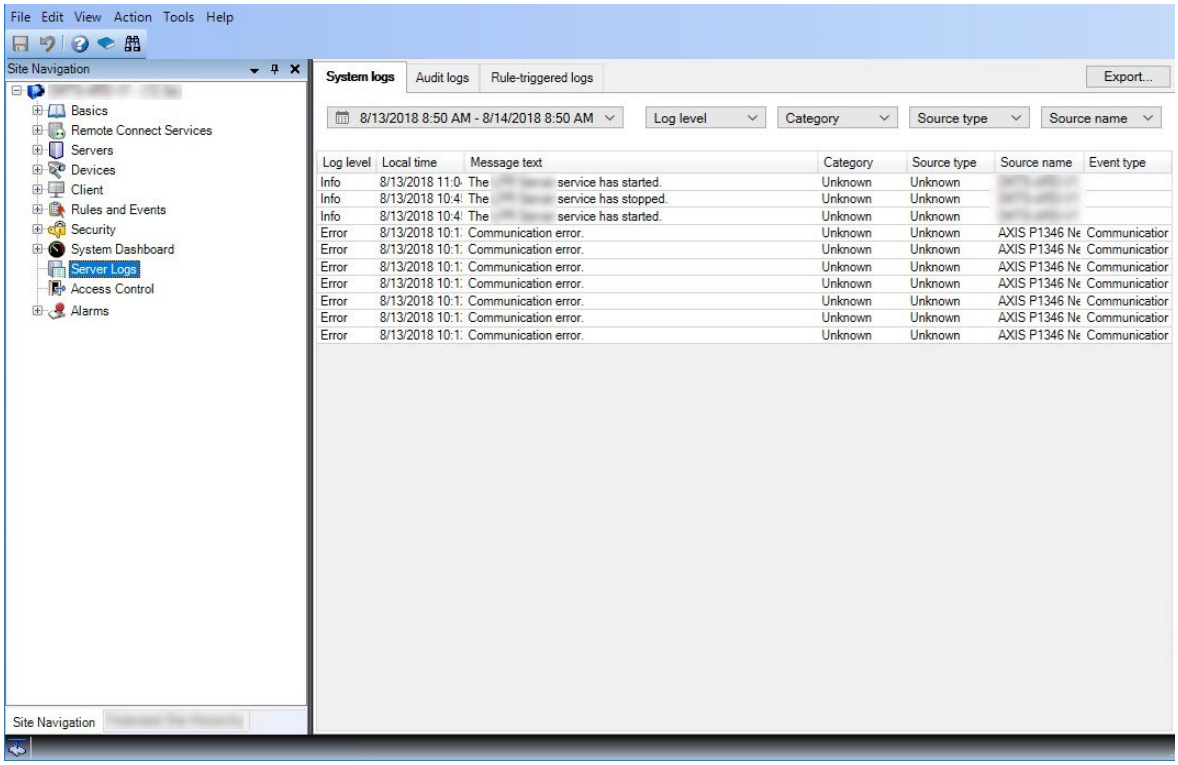
- レコーディングサーバーおよびデバイスで作業する場合：



- ルール、時間および通知プロファイル、ユーザー、ロールで作業する場合：

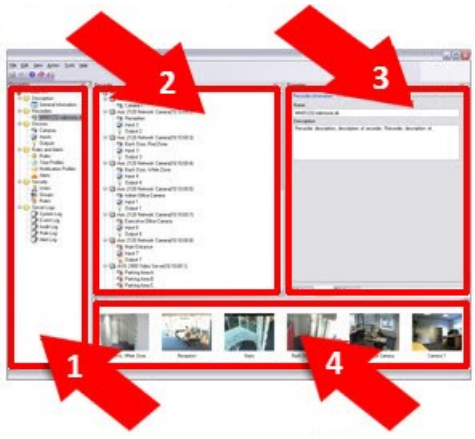


- ログを表示する場合：



ペインのレイアウト

図は通常のウィンドウのレイアウトを概説しています。カスタマイズが可能なので、使用しているコンピュータによってレイアウトは異なります。



1. サイトナビゲーションペインおよびフェデレーテッドサイト階層ペイン
2. 概要ペイン
3. [プロパティ] ペイン
4. プレビューペイン

サイトナビゲーションペイン

これはManagement Clientの中心的なナビゲーションエレメントです。ログインしたサイトの名前、設定および構成が反映されます。サイト名はペインの上部に表示されます。ソフトウェアの機能を反映して、機能はカテゴリにグループ化されます。

[サイトナビゲーション] ペインでは、システムを構成および管理し、ニーズに合わせて設定できます。システムが単一サイトシステムではなく、フェデレーテッドサイトを含む場合には、これらのサイトは**フェデレーテッドサイト階層**ペインで管理されることに注意してください。

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

[フェデレーテッドサイト階層]ペイン

これは親/子階層ですべてのMilestone Federated Architectureサイトを表示するナビゲーション要素です。

任意のサイトを選択して、そのサイトとサイトが起動するManagement Clientにログインできます。ログインしたサイトは、常に階層の最上位にあります。

概要ペイン

[サイトナビゲーション]ペインで選択した要素(例えば詳細リストなど) の概要を提供します。**概要**ペインでエレメントを選択すると、通常は**プロパティ**ペインにプロパティが表示されます。**概要**ペインでエレメントを右クリックすると、管理機能へのアクセスが得られます。

[プロパティ] ペイン

[概要]ペインで選択した要素のプロパティを表示します。プロパティは複数の専用タブに表示されます。

プレビューペイン

プレビューペインはレコーディングサーバーおよびデバイスで作業するときに表示されます。選択されたカメラからのプレビュー画像を表示したり、デバイスの状態についての情報を表示します。この例では、カメラのプレビュー画像およびカメラのライブストリームの解像度やデータ転送速度の情報を示しています。

デフォルトでは、カメラのプレビュー画像に表示されている情報はライブストリームに関する情報です。プレビュー画像の上に緑色のテキストで表示されます。代わりにレコーディングストリーム情報(赤色のテキスト)を表示したい場合は、メニューで**[ビュー]>[レコーディングストリームを表示]**を選択します。

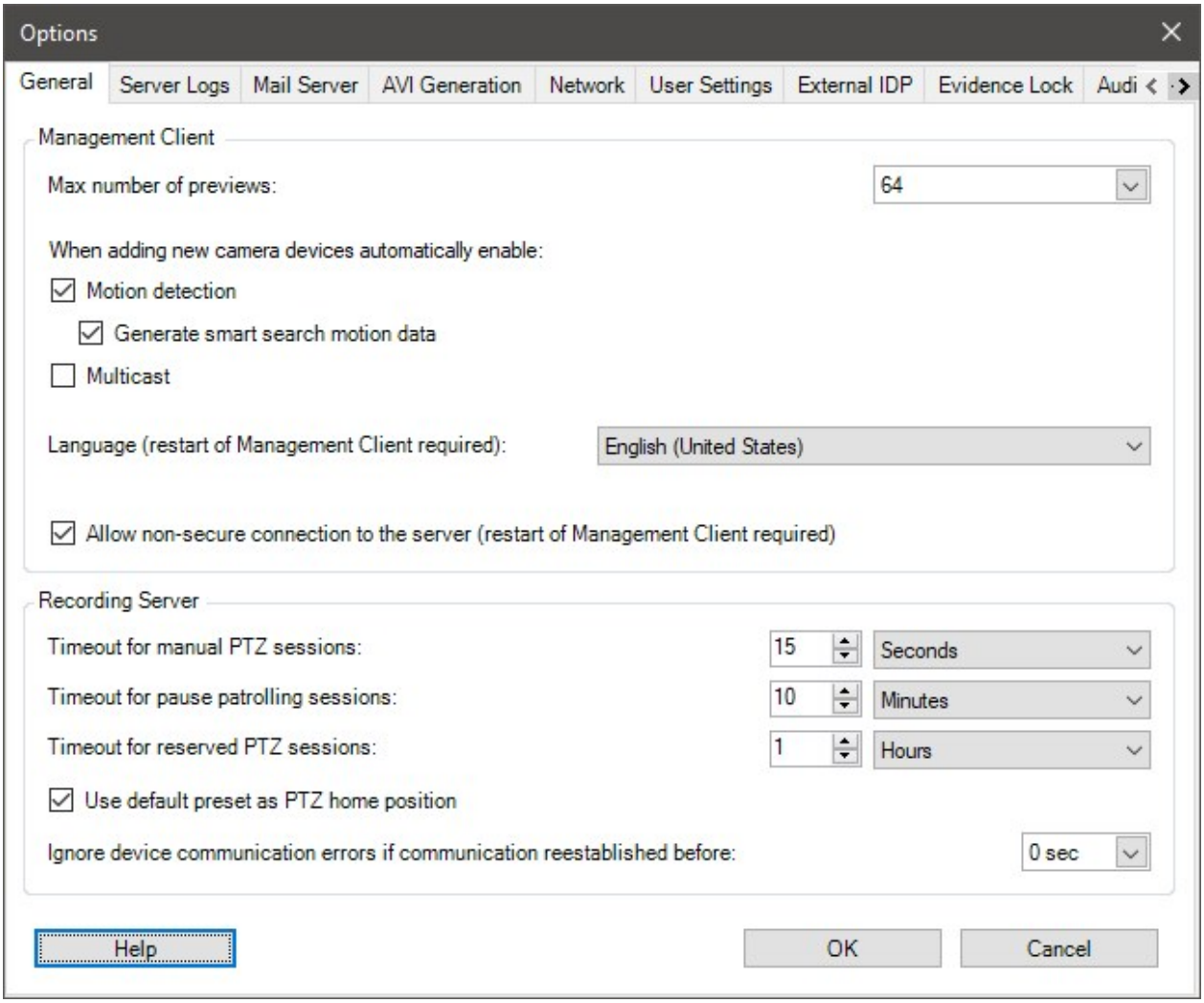
プレビューペインで、多数のカメラからのプレビュー画像を高いフレームレートで表示すると、パフォーマンスに影響することがあります。プレビュー画像の数やフレームレートを制御するには、メニューで、**[オプション]>[一般]**を選択します。

システム設定([オプション]ダイアログボックス)

オプションダイアログボックスで、全般的な表示およびシステムの機能に関連する複数の設定を指定できます。

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

ダイアログボックスにアクセスするには、**ツール > オプション**を選択します。



一般タブ(オプション)

一般タブで、Management Clientおよびレコーディングサーバーの一般設定を指定できます。

Management Client

名前	説明
プレビューの最大数	**プレビュー**ペインに表示されるサムネイル画像の最大数を選択できます。デフォルトは、64個のサムネイル画像です。 メニューから**アクション > 更新**を選択して変更を有効にします。

名前	説明
	サムネイル画像が大量に存在し、かつフレームレートが高い場合、システムが低速になる可能性があります。
新しいカメラデバイスを追加するときに自動的に有効に設定：モーション検知	**ハードウェアの追加**ウィザードを使ってシステムに追加する際に、チェックボックスを選択して新規カメラでモーション検知を有効にします。 この設定は既存のカメラのモーション検知設定に影響しません。 カメラデバイスの**モーション**タブで、カメラのモーション検知を有効化/無効化できます。
新しいカメラデバイスを追加するときに自動的に有効に設定：スマートサーチ用のモーションデータを生成	スマートサーチモーションデータを生成するには、カメラのモーション検知が有効でなければなりません。 **[ハードウェアの追加]**ウィザードでシステムに追加する際に、チェックボックスを選択して新規カメラでスマートサーチモーションデータの生成を有効にします。 この設定は既存のカメラのモーション検知設定に影響しません。 カメラデバイスの**モーション**タブで、カメラのスマートサーチモーションデータの生成を有効化/無効化できます。
新しいカメラデバイスを追加するときに自動的に有効に設定：マルチキャスト	**ハードウェアの追加**ウィザードを使って追加する際に、チェックボックスを選択して新規カメラでマルチキャストを有効にします。 この設定は既存のカメラのマルチキャスト設定に影響しません。 カメラデバイスの**クライアント**タブで、カメラのライブマルチキャストを有効化/無効化できます。
言語	Management Clientの言語を選択します。 新しい言語を使用するには、Management Clientを再起動します。
サーバーへの安全ではない接続を許可	HTTPプロトコルによる安全ではないサーバーへの接続を許可するには、このチェックボックスを選択します。(ユーザーには、安全でないサーバー接続を許可する指示は出されません)。 この設定を使用するには、Management Clientを再起動します。

レコーディングサーバー

名前	説明
手動PTZセッションのタイムアウト	必要な権限を持つクライアントユーザーは、PTZカメラのパトロールを手動で中断できます。手動停止後に通常のパトロールを再開するまでに必要な時間を指定します。この設定は、システムのPTZカメラすべてに適用されます。デフォルトは15秒です。 カメラで個別のタイムアウトを設定する場合は、カメラの**プリセット**タブで指定します。
一時停止パトロールセッションのタイムアウト	十分なPTZ優先度のクライアントユーザーはPTZカメラでのパトロールを一時停止できます。一時停止後に通常のパトロールを再開するまでに必要な時間を指定します。この設定は、システムのPTZカメラすべてに適用されます。デフォルトは10分です。 カメラで個別のタイムアウトを設定する場合は、カメラの**プリセット**タブで指定します。
予約済みPTZセッションのタイムアウト	予約済みPTZセッションのデフォルト期間を設定します。ユーザーが予約済みPTZセッションを実行するときには、セッションが手動でリリースされる前か、期間がタイムアウトするときまで、他のユーザーはPTZカメラを使用できません。デフォルト設定は1時間です。 カメラで個別のタイムアウトを設定する場合は、カメラの**プリセット**タブで指定します。
PTZのホームポジションとしてデフォルトのプリセットを使用する	このチェックボックスをオンにすると、クライアントの**ホーム**ボタンを押した際に、PTZカメラのホーム位置ではなく、デフォルトのプリセット位置が使用されます。 カメラにデフォルトのプリセット位置を定義する必要があります。デフォルトのプリセット位置が定義されていない場合、クライアントで**ホーム**ボタンを有効にしても何も起こりません。 デフォルトでは、このチェックボックスが選択されています。 デフォルトのプリセット位置を割り当てるには、233ページのカメラのプリセット位置をデフォルトとして割り当てるを参照してください
通信が右記より前に再確立される場合は、デバイスの通信エラーを無視します	ハードウェアとデバイス上のシステムの全てのコミュニケーション エラーをこのシステムで記録します。しかしながら、**コミュニケーション エラー** イベントがルールエンジンのきっかけになる前に、どのくらい長くコミュニケーション エラーが存在させるべきかはここで選択します。

サーバーログタブ(オプション)

サーバーログタブで、システムのマネジメントサーバーログの設定を指定できます。

詳細については、「ユーザーアクティビティ、イベント、アクション、エラーの特定」を参照してください。

名前	説明
ログ	設定するログの種類を選択します。 • システムログ • 監査ログ • ルール起動ログ
設定	ログを無効または有効にして、保存期間を指定します。 2018 R2およびそれ以前のコンポーネントにログの書き込みを許可します詳細については、「2018 R2およびそれ以前のコンポーネントによるログへの書き込みを許可する」を参照してください。 **システム**ログで、記録するメッセージレベルを指定します。 • すべて - 未定義のメッセージを含みます • 情報と警告とエラー • 警告とエラー • エラー(デフォルト設定) **監査**ログで、XProtect Smart Clientのすべてのユーザーアクションを記録する場合は、ユーザーアクセスログを有効にします。例えば、エクスポート、出力の有効化、カメラのライブまたは再生での表示が含まれます。 次を指定します。 • 再生シーケンスの長さ つまり、ユーザーがこの期間内で再生している限り、1つのログエントリだけが生成されます。期間外で再生すると、新しいログエントリが作成されます。 • システムがログエントリを作成する前にユーザーが表示する録画(フレーム)数。

メールサーバータブ(オプション)

[メールサーバー]タブで、システムのメールサーバーの設定を指定できます。
詳細については、「通知プロファイル(説明付き)のページ」を参照してください。

名前	説明
送信者のEメールア	すべての通知プロファイルについて、Eメールによる通知の送信者として表示するEメールアドレスを入力します。例:**sender@organization.org**。

名前	説明
ドレス	
メールサーバーアドレス	Eメール通知を送信するSMTPメールサーバーの名前を入力します。例：**mailserver.organization.org**。
メールサーバーポート	メールサーバーへの通信に使用されるTCPポート。デフォルトの暗号化されていないポートは25で、暗号化された通信では通常ポート465または587を使用します。
サーバーへの通信の暗号化	マネジメントサーバーとSMTPメールサーバー間で安全な通信を行いたい場合、このチェックボックスを選択します。 接続は、STARTTLSEメールプロトコルコマンドで保護されています。このモードでは、非暗号化接続でセッションが開始され、SMTPメールサーバーによって、マネジメントサーバーに対してSTARTTLSコマンドが発行され、SSLを使用する安全な通信に切り替わります。
サーバーのログインが必要です	有効になっている場合は、メールサーバーにログインするユーザーのユーザー名およびパスワードを指定します。

AVI生成タブ(オプション)

AVI生成タブで、AVIビデオクリップファイルの生成の圧縮設定を指定できます。これらの設定は、ルール起動通知プロファイルにより送信されるEメール通知にAVIファイルを含める場合に必要になります。

「ルールによるEメール通知のトリガー」も参照してください。

名前	説明
圧縮プログラム	適用するコーデック(圧縮/解凍技術)を選択します。リストに使用可能なコーデックをより多く含むには、マネジメントサーバーにコーデックをインストールします。 すべてのカメラがコーデックに対応しているわけではありません。
圧縮品質	(すべてのコーデックで利用できるわけではありません)。スライダーを使用して、コーデックが実行する圧縮の度合い(**0-100**)を選択します。 **0**は、圧縮なしという意味です。これは通常高画質で、ファイルサイズが大きくなります。**100**は、最大の圧縮と

名前	説明
	いう意味です。これは通常低画質で、ファイルサイズが小さくなります。 スライダーが利用できない場合、圧縮の質は選択されたコーデックによって決定されます。
キーフレームごと	(すべてのコーデックで利用できるわけではありません)。キーフレームを使用する場合、このチェックボックスをオンにして、キーフレーム間の必要なフレーム数を指定します。 キーフレームは、指定された間隔で保存された単一のフレームです。キーフレームはカメラのビュー全体を記録しますが、続くフレームは変化したピクセルだけを記録します。これにより、ファイルのサイズを大幅に縮小できます。 チェックボックスが使用できない、または選択されていない場合は、各フレームにカメラのビュー全体が含まれます。
データ転送速度	(すべてのコーデックで利用できるわけではありません)。特定のデータ転送速度を使用する場合、このチェックボックスをオンにして、秒当たりのキロバイト数を指定します。 データ速度は添付されているAVIファイルのサイズを指定します。 このチェックボックスが利用できない場合、またはオンになっていない場合、データ転送速度は選択されたコーデックによって決定されます。

ネットワークタブ(オプション)

ネットワークタブで、クライアントがインターネット経由で録画サーバーに接続する場合は、ローカルクライアントのIPアドレスを指定できます。これにより、監視システムはローカルネットワークから来ていると認識します。

システムのIPバージョンも指定できます。IPv4またはIPv6。デフォルト値はIPv4です。

ブックマークタブ(オプション)

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

[ブックマーク]タブで、ブックマーク、IDおよびXProtect Smart Clientの機能を指定できます。

名前	説明
ブックマークIDの接頭辞	XProtect Smart Clientのユーザーが作成するすべてのブックマークの接頭辞を指定します。
デフォルトのブックマーク時間	XProtect Smart Clientで設定されるブックマークのデフォルト開始時刻と終了時刻を指定します。 この設定は以下と一致している必要があります。 • デフォルトのブックマークルール(「ルール(ルールノードとイベントノード)」を参照) • 各カメラのプレバッファ期間(「プレバッファの管理」を参照)

役割のブックマーク権限を指定する場合は、「505ページのデバイスタブ(役割)」を参照してください。

ユーザー設定タブ(オプション)

ユーザー設定タブで、リモート記録が有効な場合にメッセージを表示するかどうかなどのユーザーの優先設定を指定できます。

外部IDPタブ(オプション)

Management Clientの**外部IDP**タブで、外部IDPを追加、設定し、外部IDPからの苦情を登録できます。

名前	説明
有効	外部IDPはデフォルトで有効に設定されています。
名前	外部IDPの名前。ここで入力した外部IDPの名前は、クライアントのログインウィンドウの**認証**フィールドに表示されます。
認証機関	外部IDPのURL
追加	外部IDPを追加し設定します。**追加**を選択すると、**外部IDP**ダイアログボックスが開き、設定のための情報を入力できるようになります。表の下の**外部IDPを設定する**を参照してください。
編集	外部IDPの設定を編集する
削除	外部IDPの設定を削除する

名前	説明
	外部IDPの設定を削除すると、外部IDP経由で認証されているユーザーはXProtectのVMSにログインできなくなります。再び外部IDPを追加すると、外部IDPのIDが変更されるため、ログイン時に新規ユーザーが作成されます。

外部IDPを設定する

- 外部IDPを追加するには、**外部IDP**セクションで、**追加** を選択し、下の表の情報を入力します。

名前	説明
名前	ここで入力した外部IDPの名前は、クライアントのログインウィンドウの **認証** フィールドに表示されます。
クライアントIDとクライアントの秘密	外部IDPから取得する必要があります。外部IDPと安全に通信するには、クライアントIDとクライアントシークレットが必要です。
コールバックパス	ユーザーをサインインするための認証リダイレクトフロー用のURLの一部 ユーザーは、外部IDPがホストするサインインページからサインインします。認証プロセスが完了すると、このパスが呼び出され、ユーザーはXProtectのVMSにリダイレクトされます。 デフォルトの値は “/signin-oidc” です。 リダイレクトのフォーマット コールバックパスのURIは、マネジメントサーバーFQID、with/idp/and外部プロバイダで設定されたコールバックパスで構築されます。 例： • XProtect Smart ClientおよびXProtect Management Clientのリダイレクト URIフォーマット: [schema]://[management server address]/idp/[callback path] • XProtect Web ClientおよびXProtect Mobile クライアントのリダイレクトURIフォーマット: [redirect Uri without “/index.html”]/idp/[callback path] コールバックパスの"idp"部分は大文字と小文字が区別されるため、小文字で入力する必要があります。
ログインプロンプト	ユーザーのログインを維持するか、ユーザー認証が必要かを外部IDPに指定します。外部IDPによっては、認証にパスワード認証または完全なログインが含まれる場合があります。

名前	説明
ユーザー名の作成に使用するクレーム	オプションで、VMS上の自動プロビジョニングされたユーザーに対して固有のユーザー名を生成するために使用すべき、外部IDPからの苦情を指定します。苦情によって作成される固有のユーザー名の詳細については、外部IDPユーザーに対する固有のユーザー名を参照してください。
範囲	オプションで、外部IDPから取得する苦情の数を制限するために、範囲を使用します。VMSに関連する苦情が特定範囲内であることが分かっている場合は、範囲を使用して取得する苦情の件数を制限できます。

クレームの登録

外部IDPからの苦情を登録すると、VMSでのユーザー権限を設定するため、VMSで苦情を役割にマッピングできます。詳細については、外部IDPからの苦情をマッピングするを参照してください。

- 外部IDPからの苦情を登録するには、**登録済み苦情**セクションで**追加**を選択し、下の表の情報を入力します。

名前	説明
外部IDP	外部IDPの名前。
クレーム名	フリーテキストでのクレームの表示名。役割を選択すると名前が利用できるようになります。
表示名	クレームの表示名。
大文字と小文字を区別	クレームの値の大文字小文字を区別するかを示します。 通常大文字と小文字が区別される値の例： GUIDなどIDのテキスト表示F951B1F0-2FED-48F7-88D3-49EB5999C923またはOadFgrDesdFesff= 通常大文字と小文字が区別されない値の例： - メールアドレス - 役割名 - グループ名 .
追加、	クレームを登録して管理します。

名前	説明
編集、削除	外部IDPのウェブサイト上で苦情を変更すると、ユーザーはXProtectのクライアントに再度ログインしなければなりません。例えば、そのユーザー「ボブ」をオペレータにする必要があるとします。苦情はその後、外部IDPのウェブサイト上でBobに追加されます。ただし、Bobがすでに XProtectにログインしている場合、変更を反映させるため、再度ログインする必要があります。

Webクライアント用 リダイレクトURIを追加

リダイレクトURIは、ログインした後にユーザーがリダイレクトされるロケーションです。リダイレクトURIは、Webクライアントのアドレスと完全に一致している必要があります。たとえば**https://localhost:8082/index.html** からXProtect Web Clientを開き、追加したWebクライアントのリダイレクトURIが **https://127.0.0.1:8082/index.html**である場合、外部IDP経由でログインすることはできません。

名前	説明
URI	**https://[mobile server]:[port]/index.html**形式のXProtect Web ClientのURI。リダイレクトURIは大文字と小文字を区別しません。
追加、編集、削除	リダイレクトURIを登録・管理します。 URIを削除する場合、システムが機能するには、少なくとも1つのリダイレクトURIを保持する必要があります。

カスタマーダッシュボードタブ(オプション)

[カスタマーダッシュボード]タブで、Milestone Customer Dashboardを有効または無効にできます。

カスタマーダッシュボードは、システム管理者やインストール情報へのアクセス権を持つユーザーに対して、発生の可能性がある技術的問題(カメラの障害など) を含むシステムの現在の状態の概要をグラフィカル表示として提供するオンラインのモニタリングサービスです。

チェックボックスをオンまたはオフにすると、いつでもカスタマーダッシュボード設定を変更できます。

エビデンスロックタブ(オプション)

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

エビデンスロックタブでは、エビデンスロックプロファイルや、クライアントユーザーがデータを保護した状態にするよう選択できる期間を定義および編集できます。

名前	説明
エビデンスロックプロファイル	定義されたエビデンスロックプロファイルのリスト。 既存のエビデンスロックプロファイルを追加および削除できます。デフォルトのエビデンスロックプロファイルは削除できませんが、そのタイムオプションや名称は変更できます。
ロック時間オプション:	クライアントユーザーがエビデンスにロックをかけることを選択する期間。 使用できる時間オプションは時間、日、週、月、年、無期限またはユーザー定義になります。

役割のエビデンスロックのアクセス権を指定するには、「505ページのデバイスタブ(役割)」で役割設定について確認してください。

音声メッセージタブ(オプション)

音声メッセージタブで、ルールによって起動されたメッセージの送信に使用する音声メッセージファイルをアップロードできます。

アップロードできるファイルの最大数は50で、各ファイルの最大サイズは1MBです。

名前	説明
名前	メッセージの名前を記載します。メッセージを追加する際に名前を入力します。メッセージをシステムにアップロードするには**追加**をクリックします。
説明	メッセージの説明を記載します。 メッセージを追加する際に説明を入力します。説明フィールドを使用して目的または実際のメッセージを説明することができます。

名前	説明
追加	音声メッセージをシステムにアップロードできます。 サポートされるフォーマットは、標準のWindows音声ファイルフォーマットです。 • .wav • .wma • .flac
編集	名前と説明を修正するか、または実際のファイルを置き換えることができます。
削除	音声メッセージをリストから削除します。
再生	Management Clientが稼働するコンピュータの音声メッセージを聞くにはこのボタンをクリックします。

音声メッセージの再生を起動するルールを作成するには、ルールの追加を参照してください。

ルールで使用できる一般的なアクションの詳細については、「アクションと停止アクション」を参照してください。

[プライバシー設定]タブ

プライバシー設定タブで、XProtect Mobile Server、XProtect Mobileクライアント、XProtect Web ClientおよびXProtect Smart Clientでの使用データ収集を有効または無効にできます。次に、**[OK]**をクリックします。

使用データ収集を有効にすると、第三者プロバイダーであるGoogleの技術をMilestone Systemsが使用することに同意したとみなされます。データは米国内で処理される可能性があります。データ保護と使用状況データの収集の詳細については、GDPR プライバシーガイドを参照してください。

アクセスコントロール設定タブ(オプション)

XProtect Accessを使用する場合は、この機能の使用を許可する基本ライセンスを購入しておく必要があります。

名前	説明
開発プロパティパネルを表示する	選択すると、**[アクセスコントロール] > [一般設定]**に追加の開発者情報が表示されます。 この設定は、アクセスコントロールシステム統合の開発者のみが使用することを前提としています。

アナリティクスイベントタブ(オプション)

アナリティクスイベントタブで、アナリティクスイベント機能を有効にして指定できます。

名前	説明
有効	アナリティクスイベントを使用するかどうかを指定します。デフォルトでは、この機能は無効になっています。
ポート	この機能で使用するポートを指定します。既定のポートは9090です。 関連するVCAツールプロバイダもこのポート番号を使用するようにしてください。ポート番号を変更した場合、プロバイダのポート番号も変更するようにしてください。
すべてのネットワークアドレスまたは**指定ネットワークアドレス**	すべてのIPアドレス/ホスト名からのイベントが許可されるのか、または**アドレスリスト**(以下を参照)で指定されたIPアドレス/ホスト名からのイベントだけが許可されるのかを指定します。
アドレスリスト	信頼済みIPアドレス/ホスト名のリストを指定します。このリストは、特定のIPアドレス/ホスト名のイベントのみが許可されるように受信されるデータをフィルタリングします。ドメイン名システム(DNS)、IPv4およびIPv6アドレス形式の両方を使用できます。 それぞれのIPアドレスまたはホスト名をマニュアルで入力するか、あるいはアドレスの外部リストをインポートすることにより、リストにアドレスを追加できます。 • **マニュアル入力**: アドレスリストにIPアドレス/ホスト名を入力します。必要なアドレスを繰り返します。 • **インポート**: **[インポート]**をクリックして、アドレスの外部リストを参照します。外部リストは、それぞれのIPアドレスまたはホスト名が別のラインに入力された.txtファイルでなければなりません。

[アラームおよびイベント]タブ(オプション)

[アラームとイベント]タブで、アラーム、イベント、ログの設定を指定できます。これらの設定に関連して、「121ページのデータベースのサイズを制限」も併せて参照してください。

名前	説明
終了したアラームの保	データベース上で**終了**状態のアラームを保存する日数を指定します。値を**0**に設定すると、アラームは終了後に削除されます。

名前	説明
存期間	 アラームには常にタイムスタンプが含まれます。アラームがカメラによりトリガーされる場合は、タイムスタンプにはアラームの時間からの画像が含まれます。アラーム情報自体はイベントサーバーに保存されますが、添付画像に対応するビデオ記録は、関連する監視システムサーバーに保存されます。 アラームの画像を表示するには、ビデオ録画が少なくともイベントサーバーにアラームを保存する期間以上、保存されるようにする必要があります。
他のすべてのアラームの保存期間	**新規**、**処理中**、または**保留中**の状態のアラームを保存する日数を指定します。値を0に設定すると、アラームはシステムに表示されますが、保存はされません。  アラームには常にタイムスタンプが含まれます。アラームがカメラによりトリガーされる場合は、タイムスタンプにはアラームの時間からの画像が含まれます。アラーム情報自体はイベントサーバーに保存されますが、添付画像に対応するビデオ記録は、関連する監視システムサーバーに保存されます。 アラームの画像を表示するには、ビデオ録画が少なくともイベントサーバーにアラームを保存する期間以上、保存されるようにする必要があります。
ログの保存期間	イベントサーバーログの保存日数を指定します。ログの保存期間が長期に及ぶ場合は、イベントサーバーが設置されているマシンのディスクに十分な空き領域があることを確認してください。
詳細ログインを有効にする	イベントサーバー通信のより詳細なログを保持するには、チェックボックスを選択します。**ログの保持**フィールドに指定された日数の間保存されます。
イベントタイプ	イベントをデータベースに保存する日数を指定します。カメラを正しく配置するには次の2つの方法があります。 • イベントグループ全体の保存期間を指定できます。**[グループを受け継ぐ]**の値を有するイベントタイプは、イベントグループの値を受け継ぎます。 • イベントグループの値を設定した場合でも、イベントタイプごとに保存期間を指定できます。  値を**0**に設定すると、イベントはデータベースに保存されません。

名前	説明
	外部イベント(ユーザー定義イベント、ジェネリックイベント、および入力イベント)は、デフォルトで **0** に設定されており、その値を変更することはできません。その理由は、これらの種類のイベントが頻繁に発生するため、データベースに保存するとパフォーマンスの問題が発生する可能性があるからです。

ジェネリックイベントタブ(オプション)

ジェネリックイベントタブで、ジェネリックイベントとデータソース関連の設定を指定できます。

実際のジェネリックイベントの設定方法についての詳細は、ジェネリックイベントについて(説明付き)を参照してください。

名前	説明
データソース	2つのデフォルトデータソースから選択してカスタムデータソースを定義できます。選択内容は、お使いのサードパーティ製プログラムおよび/またはインターフェース対象となるハードウェアまたはソフトウェアによって異なります。 **互換**:工場出荷時のデフォルト設定が有効。すべてのバイトをエコー。TCPおよびUDP。IPv4のみ。ポート1234。区切り文字なし。ローカルホストのみ。現在のコードページエンコーディング(ANSI)。 **インターナショナル**:出荷時設定が有効。統計のみをエコー。TCPのみ。IPv4+6。ポート1235。<CR><LF>を区切り文字として使用。ローカルホストのみ。UTF-8エンコード。(<CR><LF> = 13,10)。 [データソースA] [データソースB] のようになります。
新規	クリックすると新しいデータソースを定義できます。
名前	データソースの名前。
有効	データソースはデフォルトでは無効になっています。データソースを有効にするにはチェックボックスを選択します。
リセット	クリックして選択されたデータソースのすべての設定をリセットします。**名前**フィールドに入力された名前は残ります。

名前	説明
ポート	データソースのポート番号。
プロトコルタイプセレクタ	システムがジェネリックイベントを検出するために聞き、分析すべきプロトコル。 **すべて**: TCPおよびUDP。 **TCP**: TCPのみ。 **UDP**: UDPのみ。 ジェネリックイベントに使用するTCPおよびUDPパッケージに、@、#、+、~、等の特殊文字が含まれている場合があります。
IPタイプセレクタ	選択可能なIPアドレスタイプ: IPv4、IPv6、または両方。
区切り文字列	個別ジェネリックイベントのレコードを分離するために使用するセパレーターバイトを選択します。デフォルトのデータソースタイプ**インターナショナル**(上記の**データソース**をご覧ください) は**13、10**です。(13,10 = <CR><IF>)。
エコータイプセレクタ	使用可能なエコーリターン形式: • **エコー統計**: 次の形式をエコーします。**[X], [Y],[Z],[ジェネリックイベント名]** **[X]** = 要求番号。 **[Y]** = 文字数。 **[Z]** = ジェネリックイベントとの一致数。 **[ジェネリックイベント名] = [名前]** フィールドに入力された名前。 • **すべてのバイトをエコー**: すべてのバイトをエコーします。 • **エコーなし**: すべてのエコーを抑制します。
エンコーディングタイプセレクタ	デフォルトでは、もっとも関連のあるオプションのみがリストに表示されます。**すべて表示** チェックボックスを選択し、利用可能なすべてのエンコーディングを表示します。
使用可能な外部IPv4アドレス	外部イベントを管理するために、マネジメントサーバーが通信可能なIPアドレスを指定します。これを使用して、データを取得しないIPアドレスを除外することも可能です。
使用可能な外部IPv6アドレス	外部イベントを管理するために、マネジメントサーバーが通信可能なIPアドレスを指定します。これを使用して、データを取得しないIPアドレスを除外することも可能です。

コンポーネントメニュー

Management Clientのメニュー

ファイルメニュー

変更を設定に保存して、アプリケーションを終了します。構成をバックアップすることもできます。313ページのシステム設定のバックアップおよび復元についてを参照してください。

編集メニュー

変更を元に戻すことができます。

ビューメニュー

名前	説明
アプリケーションレイアウトのリセット	Management Clientのさまざまなペインのレイアウトをデフォルトの設定にリセットします。
プレビューウィンドウ(P)	レコーディングサーバーやデバイスを操作する際に、**プレビュー**ペインをオンまたはオフに切り替えられます。
レコーディングストリームを表示(S)	デフォルトでは、**プレビュー**ペインのプレビュー画像に表示されている情報は、カメラのライブストリームに関する情報です。代わりにレコーディングストリームに関する情報が必要な場合は、**レコーディングストリームを表示**を選択します。
フェデレーテッドサイト階層	デフォルトでは、**フェデレーテッドサイト階層**ペインは有効になっています。
サイトナビゲーション	デフォルトでは、**サイトナビゲーション**ペインは有効になっています。

アクションメニュー

アクションメニューの内容は**サイトナビゲーション**ペインで選択したエレメントにより異なります。選択できるアクションはエレメントを右クリックする時と同じです。

各カメラのプレバッファ期間(「プレバッファの管理」を参照)

名前	説明
更新	常に使用可能であり、必要な情報をManagement Serverから再ロードします。

ツールメニュー

名前	説明
登録済みサービス	登録済みサービスの管理。 339ページの登録済みサービスの管理を参照してください。
有効な役割	選択したユーザーまたはグループの役割をすべて表示します。
オプション	オプションダイアログボックスが開き、グローバルシステム設定を定義および編集できます。詳細については、364ページのシステム設定([オプション]ダイアログボックス) を参照してください。

ヘルプメニュー

ヘルプシステムとManagement Clientのバージョンについての情報にアクセスできます。

Server Configurator(ユーティリティ)

[暗号化]タブのプロパティ

このタブからは、以下のプロパティを指定できます:

> クラスタ環境では、クラスタ環境内の全コンピュータに対して証明書を作成する前にクラスタを設定し、これが実行されていることを確認する必要があります。これが終われば、証明書をインストールして、クラスタ内の全ノードに対してServer Configuratorを使用して登録を実行できるようになります。詳細については、XProtect VMSの保護方法に関する証明書ガイドを参照してください。

名前	説明	タスク
サーバー証明書	マネジメントサーバー、データコレクタ、ログサーバー、レコーディングサーバー間の双方向接続を暗号化するために使用する証明書を選択します。	マネジメントサーバーとの間で暗号化を有効にする レコーディングサーバーまたはリモートサーバーのサーバー暗号化を有効にする
イベントサーバーと拡張	イベントサーバーと通信するコンポーネント(LPR Serverなど) とイベントサーバー間の双方向接続の暗号化に使用する証明書を選択してください。	288ページのイベントサーバーの暗号化を有効に設定

名前	説明	タスク
機能		
ストリーミングメディアの証明書	レコーディングサーバーとレコーディングサーバーからデータストリームを受け取るすべてのクライアント、サーバー、統合間の通信を暗号化するために使用される証明書を選択してください。	クライアントとサーバーに対して暗号化を有効にする
モバイル ストリーミング メディアの証明書	モバイル サーバーと、モバイル サーバーからデータ ストリームを取得するモバイルおよびWebクライアントの間の通信を暗号化するために使用する証明書を選択します。	モバイルサーバーで暗号化を有効にする

サーバーの登録

名前	説明	タスク
マネジメントサーバーのアドレス	マネジメントサーバーのアドレスには通常、コンピュータのホスト名または完全修飾ドメイン名(FQDN)が含まれます。 デフォルトでは、このアドレスは、マネジメントサーバーがインストールされていないXProtect VMS上のコンピュータに対してのみアクティブとなります。 原則として、マネジメントサーバーのアドレスは、マネジメントサーバーがインストールされているコンピュータからは変更しないでください。 ただし、たとえばフェールオーバーセットアップでServer Configuratorを使用しているような場合は、マネジメントサーバーコンピュータからアドレスを変更しなくてはならない場合もあります。このような状況は、クラスタフェールオーバー環境内で、あるいは他のフェールオーバーセットアップシナリオで発生する可能性があります。	マネジメントサーバーがインストールされているコンピュータからマネジメントサーバーのアドレスを変更することでもたらされる影響については詳しくは、以下をクリックしてください。 マネジメントサーバーコンピュータのホスト名を変更

名前	説明	タスク
	• マネジメントサーバーがインストールされているコンピュータから**マネジメントサーバーアドレス**フィールドを有効にするには、ペン( ) 記号をクリックしてください。 マネジメントサーバーアドレスを更新する場合は、コンポーネントがインストールされている各コンピュータにアクセスし、マネジメントサーバーアドレスを新しいアドレス情報で更新する必要があります。	
登録	指定したマネジメントサーバーを搭載したコンピュータ上で実行されるサーバーを登録します。	レコーディングサーバーを登録する

言語の選択

このタブを使うと、Server Configuratorの言語を選択できます。Server Configuratorの言語セットは、Management Clientの言語セットに呼応します。

名前	説明
言語の選択	ユーザーインターフェースの言語を選択します。

フェールオーバークラスターを使用している場合は、Server Configuratorで作業を始める前にクラスターを一時停止するようお勧めします。変更の適用中にServer Configuratorでサービスを停止する必要があり、フェールオーバークラスター環境がこの操作を妨害する可能性があるためです。

トレイアイコンのステータス

表に示されるトレイアイコンは、XProtect VMSのサーバーで実行されているサービスのさまざまな状態を表します。これらのアイコンは、サーバーがインストールされているコンピュータで利用できます:

Management Server Manager トレーアイコン	Recording Server Manager トレーアイコン	Event Server Manager トレーアイコン	Failover Recording Server Manager トレーアイコン	説明
				**実行中** サーバーサービスが有効になって起動した際に表示されます。 Failover Recording Serverサービスが実行されている場合、標準レコーディングサーバーに不具合が生じた際に、このサービスが処理を引き継ぎます。
				**停止** サーバーサービスが停止した際に表示されます。 Failover Recording Serverサービスが停止した場合、標準レコーディングサーバーに不具合が生じても、このサービスが処理を引き継ぐことはできません。
				**開始中** サーバーサービスが開始プロセスに入った際に表示されます。通常の状態では、トレーアイコンはしばらくしてから**[実行中]**に変化します。
				**停止中** サーバーサービスが停止プロセスに入った際に

Management Server Manager トレーアイコン	Recording Server Manager トレーアイコン	Event Server Manager トレーアイコン	Failover Recording Server Manager トレーアイコン	説明
				表示されます。通常の状態では、トレーアイコンはしばらくしてから**[停止中]**に変化します。
				**中間状態** サーバーサービスが最初に読み込まれてから最初の情報を受信するまで表示されます。通常の状態では、トレーアイコンは**[開始中]**に、続いて**[実行中]**に変化します。
				**オフラインで実行** 通常はレコーディングサーバーまたはフェールオーバーレコーディングサーバーが実行されているものの、Management Serverサービスが実行されていない場合に表示されます。

トレイアイコンからサービスを開始および停止

通知領域のアイコンを右クリックしてトレイアイコンを開き、そこからサービスを開始および停止できます。

- Management Serverサービスの開始または停止
- Recording Serverサービスの開始または停止

Management Server Manager(トレイアイコン)

Management Server Managerからタスクを実行するには、Management Server Managerトレイアイコンのメニューアイテムを使用します。

名前	説明
Management Serverの開始とManagement Serverの停止	該当するメニューアイテムをクリックしてManagement Serverサービスを開始または停止します。Management Serverサービスを停止すると、Management Clientを使用できなくなります。 サービスの状態はトレイアイコンによって示されます。トレイアイコンの状態について詳しくは、

名前	説明
	「Server Managerのトレイアイコン(説明付き)」を参照してください。
ステータスメッセージの表示	タイムスタンプ付きのステータスメッセージのリストを表示します。
システム構成パスワードの設定を変更	システム構成パスワードを割り当てるか、または変更します割り当てられたシステム設定パスワードを削除することで、システム構成をパスワードで保護しないよう選択することもできます。 システム構成パスワードの設定変更
現在のシステム構成パスワードを入力	パスワードを入力します。パスワード設定が保存されているファイルが削除された場合や破損した場合などに実行します。詳細については、「システム構成パスワードの設定を入力」を参照してください。
フェールオーバーマネジメントサーバーの設定/構成	フェイルオーバーマネジメントサーバーの設定ウィザードを起動するか、**[設定を管理]** ページで既存の設定を管理します。フェールオーバークラスタの詳細については36ページのXProtect Management Server Failover を参照してください。
Server Configurator	**Server Configurator**を開いてサーバーを登録し、暗号化を管理します。暗号化の管理について詳しくは、「Server Configuratorを使用して暗号化を管理」を参照してください。
ライセンスの変更	マネジメントサーバーコンピュータで、ソフトウェアライセンスコードを変更します。新しいライセンスコードは、XProtectシステムをアップグレードする際などに入力する必要があります。詳細については、「ソフトウェアライセンスコードの変更」を参照してください。
構成の復元	ダイアログボックスが開き、そこでシステム構成を復元できます。**[復元]**をクリックする前に、ダイアログボックスに示された情報を必ずお読みください。詳細については、「システム構成を手動バックアップから復元」を参照してください。
共有バックフォルダーの選択	システム構成をバックアップする前に、バックアップの保存先となるバックアップフォルダーを設定します。詳細については、「共有バックアップフォルダーの選択」を参照してください。
SQLアドレスの更新	ウィザードが開き、SQL Serverのアドレスを変更できます。まれにホスト名が変更された場合などに、その変更に合わせてSQL Serverのアドレスを調整しなくてはならないことがあります。詳細については、ホスト名を変更するとSQL Serverのアドレスが変化する可能性がある」を参照してください。

基本ノード

ライセンス情報(基本ノード)

[ライセンス情報]ウィンドウでは、このサイトまたは他の全サイトの両方で同一のソフトウェアライセンスファイルを共有している全ライセンスに加え、現在のMilestone Careサブスクリプションを追跡できるほか、ライセンスをどのようにアクティベートするかを指定できます。

[ライセンス情報]ウィンドウで利用できる各種情報や機能については、「116ページのライセンス情報 ウィンドウ」を参照してください。

サイト情報(基本ノード)

子サイトの数が多い大規模なMilestone Federated Architectureのセットアップでは、概要がおおまかになり、各子サイトシステム管理者の連絡先を見つけるのが難しくなることがあります。

このため、各子サイトに情報をさらに追加できます。この情報はその後、中央サイトのシステム管理者が利用できるようになります。

以下の情報を追加することができます。

- サイト名
- アドレス/場所
- 管理者
- 詳細情報

リモート接続サービスノード

Axis One-clickカメラの接続(リモート接続サービスノード)

これらはAxis One-Clickカメラの接続プロパティです。

名前	説明
カメラのパスワード	入力/編集します。購入時にカメラとともに提供されます。詳細については、カメラのマニュアルを参照するか、Axis Webサイト(https://www.axis.com/)を参照してください。
カメラのユーザー	詳細については、**カメラのパスワード**を参照してください。
説明	カメラの説明を入力/編集します。

名前	説明
外部アドレス	カメラが接続しているSTサーバーのWebアドレスを入力/編集します。
内部アドレス	レコーディングサーバーが接続しているSTサーバーのWebアドレスを入力/編集します。
名前	必要に応じて、アイテム名を編集します。
所有者認証キー	**カメラのパスワード**を参照してください。
パスワード(Dispatchサーバー用)	パスワードを入力します。システムプロバイダーから受け取ったものと同じでなければなりません。
パスワード(STサーバー用)	パスワードを入力します。Axis One-Click Connectionコンポーネントをインストールした際に入力したものと同一でなくてはなりません。
Axis Dispatchサービスに登録/登録解除	お持ちのAxisカメラをAxis Dispatchサービスに登録するかどうかが示されます。これは設定時または後で行うことができます。
シリアル番号	メーカーが指定したハードウェアのシリアル番号。シリアル番号は、MACアドレスと同じであることがよくありますが、必ず一致するわけでもありません。
資格情報を使用	このチェックボックスは、STサーバーのインストール時に資格情報を使用する場合に選択します。
ユーザー名(Dispatchサーバー用)	ユーザー名を入力します。ユーザー名は、システムプロバイダーから受け取ったものと同じでなければなりません。
ユーザー名(STサーバー用)	ユーザー名を入力します。**Axis One-Click Connectionコンポーネント**をインストールした際に入力したものと同一でなくてはなりません。

サーバーノード

サーバー(ノード)

このセクションではレコーディングサーバーのインストールと設定方法を説明します。また、システムに新しいハードウェアを追加し、他サイトと相互接続するやり方も学べます。

- 390ページのレコーディングサーバー(サーバーノード)
- 402ページのフェールオーバーサーバー(サーバーノード)

レコーディングサーバー(サーバーノード)

システムは、ビデオフィードの録画、およびカメラと他デバイス間の通信のためにレコーディングサーバーを使用します。一般的に、監視システムは複数のレコーディングサーバーで構成されています。

レコーディングサーバーはRecording Serverソフトウェアをインストールし、マネジメントサーバーと通信するよう設定されたコンピュータです。**サーバー**フォルダーを展開し、**レコーディングサーバー**を選択すると、**概要**ペインにレコーディングサーバーが表示されます。

このバージョンのマネジメントサーバーよりも前のレコーディングサーバーのバージョンとの後方互換性は制限されています。旧バージョンのレコーディングサーバーの録画にアクセスすることはできますが、それらの設定を変更するには、このバージョンのマネジメントサーバーに対応していることを確認してください。Milestoneは、システム内のすべてのレコーディングサーバーを、マネジメントサーバーと同じバージョンにアップグレードすることを推奨しています。

[レコーディング サーバーの設定]ウィンドウ

Recording Server Managerトレイアイコンを右クリックして**[設定の変更]**を選択すると、以下を指定できます:

名前	説明
アドレス	IPアドレス(例: 123.123.123.123) またはレコーディング サーバーを接続するマネジメントサーバーのホスト名(例: ourserver)。レコーディング サーバーはマネジメントサーバーと通信できるため、この情報は必要です。
ポート	マネジメントサーバーと通信する際に使用されるポート番号。デフォルトは9000です。これは必要に応じて変更できます。
Webサーバー ポート	Webサーバーのリクエストに対応する際に使われるポート番号 (例: PTZカメラ コントロール コマンドの対応、参照およびXProtect Smart Clientからのライブ リクエスト)。デフォルトは7563です。これは必要に応じて変更できます。
アラート サーバー ポート	レコーディング サーバーがTCP情報を受信する際に使われるポート番号 (イベント メッセージの送信でTCPを使用するデバイスもあります)。デフォルトはポート5432です (デフォルトで無効になっています)。必要に応じて、この順序は変更できます。
SMTP サーバー	レコーディング サーバーがSMTP情報を受信する際に使われるポート番号。SMTPは、サーバー間で電子メール メッセージを送信する標準です。メッセージや画像を監視システム サーバーに弟子 メールで送信する

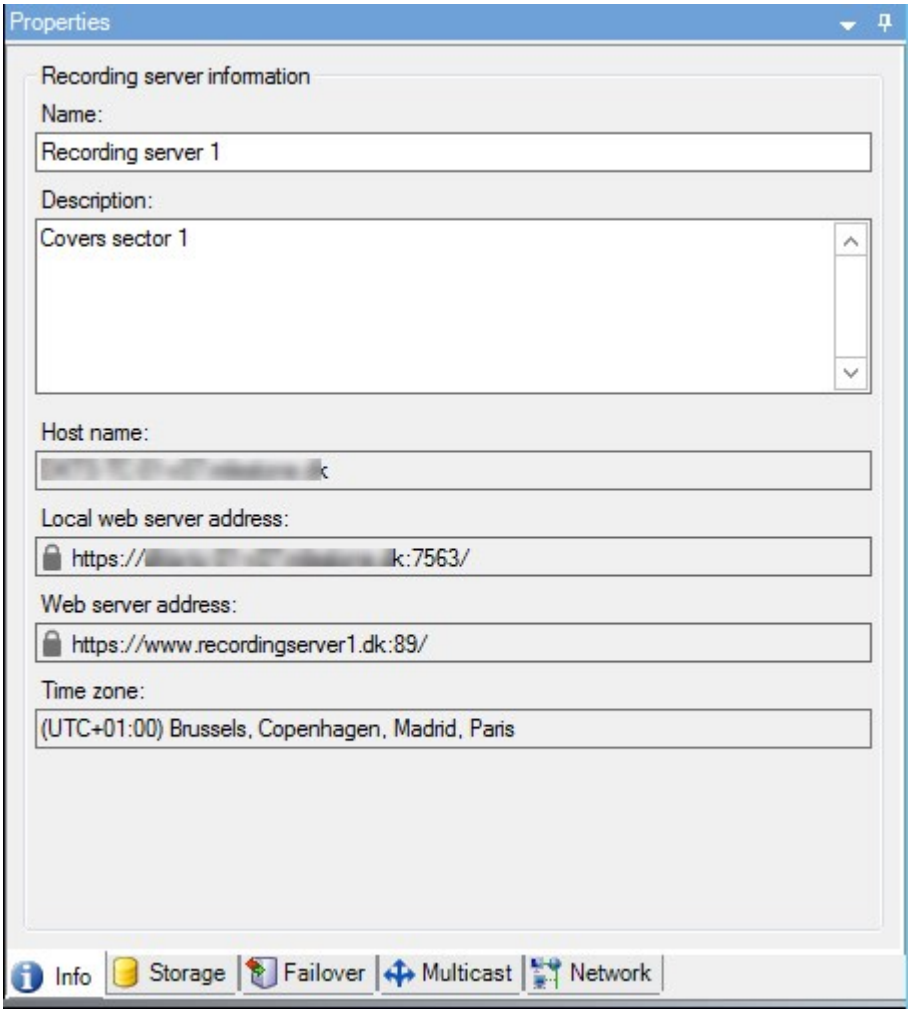
名前	説明
ポート	ためにSMTPを使用するデバイスもあります。デフォルトは25です。これは有効・無効にできます。必要に応じて、ポート番号は変更できます。
マネジメントサーバーからレコーディングサーバーへの接続を暗号化	暗号化を有効にして、リストからサーバー認証証明書を選択する前に、最初にマネジメントサーバーで暗号化を有効にし、マネジメントサーバー証明書がレコーティング サーバーで信頼されていることを確認します。 詳細については、「136ページの安全な通信(説明付き)」を参照してください。
データのストリーミングを行うクライアントとサービスへの接続を暗号化	暗号化を有効にして、リストからサーバー認証証明書を選択する前に、レコーティング サーバーからXProtect Smart Clientデータストリームを取得するサービスを実行しているすべてのコンピュータで証明書が信頼されていることを確認します。と、レコーディング サーバーからデータストリームを取得するサービスはすべて、バージョン2019 R1以降でなくてはなりません。2019 R1よりも前のバージョンのMIP SDKを使用して作成されたサードパーティソリューションは、更新が必要な可能性があります。 詳細については、「136ページの安全な通信(説明付き)」を参照してください。 レコーディングサーバーで暗号化が使用されていることを確認する方法については、「275ページのクライアントの暗号化ステータスを表示する」を参照してください。
詳細	特定の証明書については、Windows Certificate Storeの情報を確認してください。

レコーディングサーバーのプロパティ

情報タブ(レコーディングサーバー)

インフォメーションタブ上で、レコーディングサーバーの名前と詳細を確認したり、変更したりできます。

ホスト名とアドレスを見ることができます。Webサーバーアドレスの前にあるパッドロックアイコンは、このレコーディングサーバーからデータストリームを取得するクライアントとサービスの通信が暗号化されていることを意味します。



名前	説明
名前	入力するレコーディングサーバーの名前を選ぶことができます。この名前は、レコーディングサーバーがリスト化されている際、システムとクライアントにおいて使用されます。名前は一意である必要はありません。 レコーディングサーバーの名前を変更すると、名前はManagement Clientで一括変更されます。
説明	システム内にリスト化されている数字の中に表示される説明を入力することができます。説明は必須ではありません。
ホスト名	レコーディングサーバーのホスト名を表示します。
ローカルWebサーバーアドレ	レコーディングサーバーのWebサーバーのローカルアドレスを表示。例えば、PTZ カメラコントロールコマンドを使用したり、XProtect Smart Clientからのライブリクエストを閲覧する際には、ローカルアドレスを使用します。

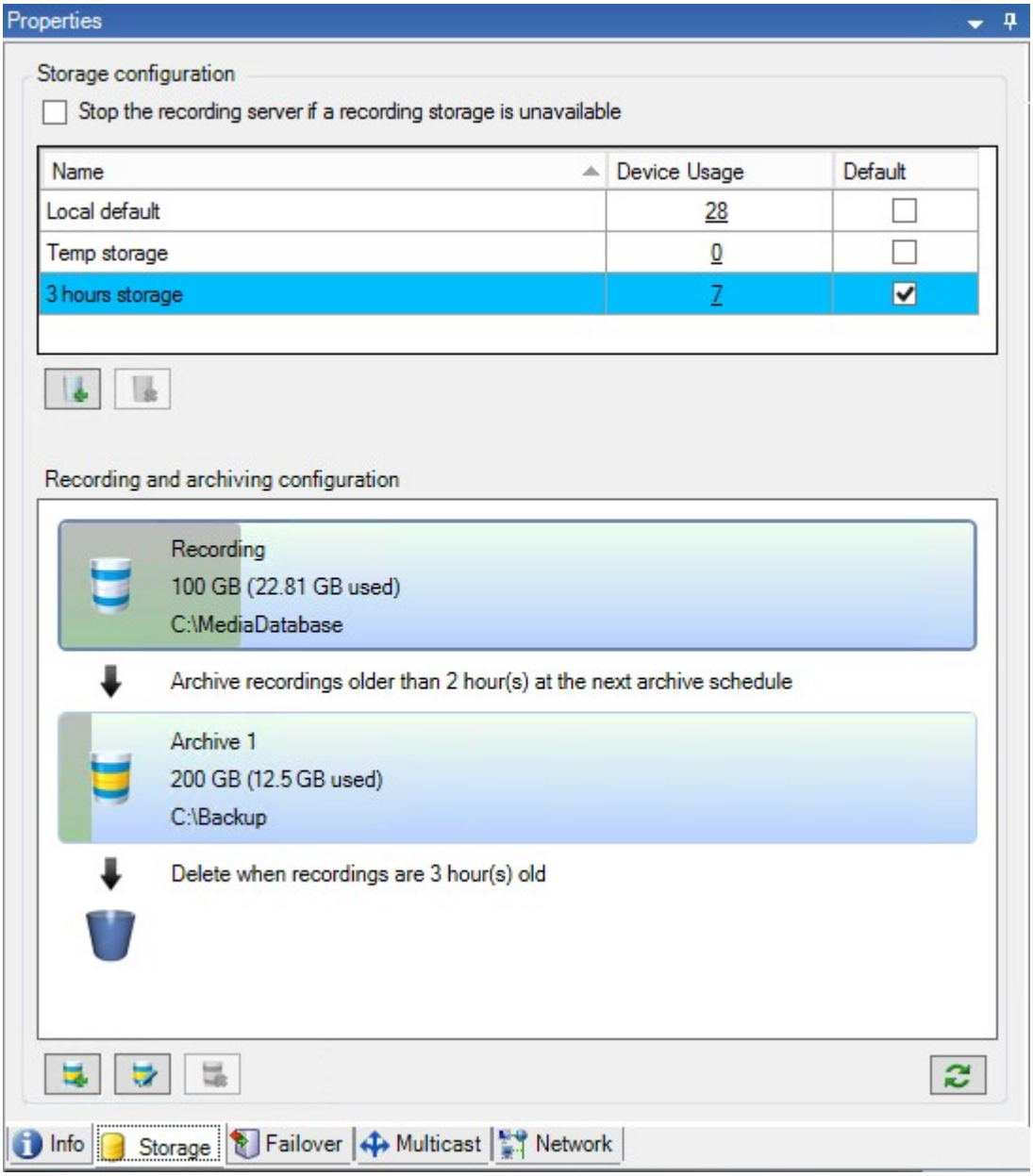
名前	説明
ス	Webサーバーコミュニケーションに使われているポート番号を含むアドレス(標準ポート7563) 。 暗号化を有効にすると、パッドロックアイコンとhttpの代わりにhttpsを含むアドレスが表示されます。
Webサーバーアドレス	インターネット上でレコーディングサーバーのWebサーバーのパブリックアドレスを表示する。 クライアントがインターネット上でレコーディングサーバーに接続できる監視システムにアクセスできるよう、インストールにおいてファイアーオールあるいはNATルーターを使用する際は、ファイアーウォールまたはNAT ルーターのアドレスを入力してください。 パブリックアドレスとネットワークタブ上でポート番号を指定します。 暗号化を有効にすると、パッドロックアイコンとhttpの代わりにhttpsを含むアドレスが表示されます。
時間ゾーン	レコーディングサーバーのあるタイムゾーンを表示する。

ストレージタブ(レコーディングサーバー)

ストレージタブで、選択したレコーディングサーバーのストレージを設定、管理および表示することができます。

録画ストレージとアーカイブでは、横棒は現在の空き容量を示しています。録画ストレージが使用できない場合のレコーディングサーバーの動作を設定することができます。これはほとんどの場合、ご利用のシステムにフェールオーバーサーバーがあるときに関係する設定です。

エビデンスロックを使用している場合、エビデンスロックされた映像に使用される容量を示す縦の赤線があります。



ストレージおよび録画設定プロパティ

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

ストレージおよび録画設定ダイアログボックスで、次のアイテムを指定します。

名前	説明
名前	必要に応じて、ストレージ名を変更します。名前は一意でなければなりません。
パス	このストレージで記録を保存するディレクトリへのパスを指定します。ストレージは、必ずしもレコーディングサーバーのコンピュータに存在する必要はありません。 ディレクトリが存在しない場合は作成できます。ネットワークドライブは、必ずUNC(汎用名前付け規則)のフォーマットを使用して指定する必要があります。例:`\\server\volume\directory\`。
保存期間	アーカイブ設定に応じて、削除または次のアーカイブに移動するまでに、記録がアーカイブに格納される期間を指定します。 保存期間は、前のアーカイブまたはデフォルトの録画データベースの保存期間より必ず長くなるようにしてください。アーカイブに対して指定される保存日数には、プロセスで以前に指定されたすべての保存期間が含まれるためです。
最大サイズ	記録データベースに保存する記録データの最大ギガバイト数を選択します。 指定されたギガバイト数を超える記録データは、指定された場合、自動的にリストの最初のアーカイブに移動されるか、削除されます。 ⚠ 空き容量が5GB未満になった場合、データベースで最も古いデータは必ず自動アーカイブされます(または、次のアーカイブが定義されていない場合は削除されます)。空き容量が1GB未満になった場合は、データは削除されます。データベースには、必ず250MBの空き容量が必要です。この制限に達した場合(データが十分速やかに削除されていない場合)、十分な空き容量が確保されるまで、それ以上データベースにはデータが書き込まれません。このため、データベースの実際の最大サイズは、指定したギガバイト数より5GB少なくなります。
電子署名中	記録への電子署名を有効にします。これはたとえば、再生時に、エクスポートされたビデオが修正や改ざんされていなかったことをシステムが確認することを意味します。 システムはデジタル署名にSHA-2アルゴリズムを使用します。
暗号化	記録の暗号化レベルを選びます。 • 無し • 弱(CPU使用少) • 強(CPU使用大) システムは暗号化にAES-256アルゴリズムを使用します。 **弱**を選択する場合、録画の一部が暗号化されます。**強**を選択する場合、録画の全部が暗号化されます。

名前	説明
	暗号化を有効にする選択をした場合、以下のパスワードも指定しなければなりません。
パスワード	暗号化されたデータの閲覧を許可されるユーザー用パスワードを入力します。 Milestoneは、強いパスワードを使用することを推奨しています。強いパスワードは、辞書で調べられる単語やユーザーの名前の一部は含みません。8文字以上の英数字、大文字および小文字、ならびに特殊文字を含みます。

アーカイブ設定のプロパティ

アーカイブ設定ダイアログボックスで、次のアイテムを指定します。

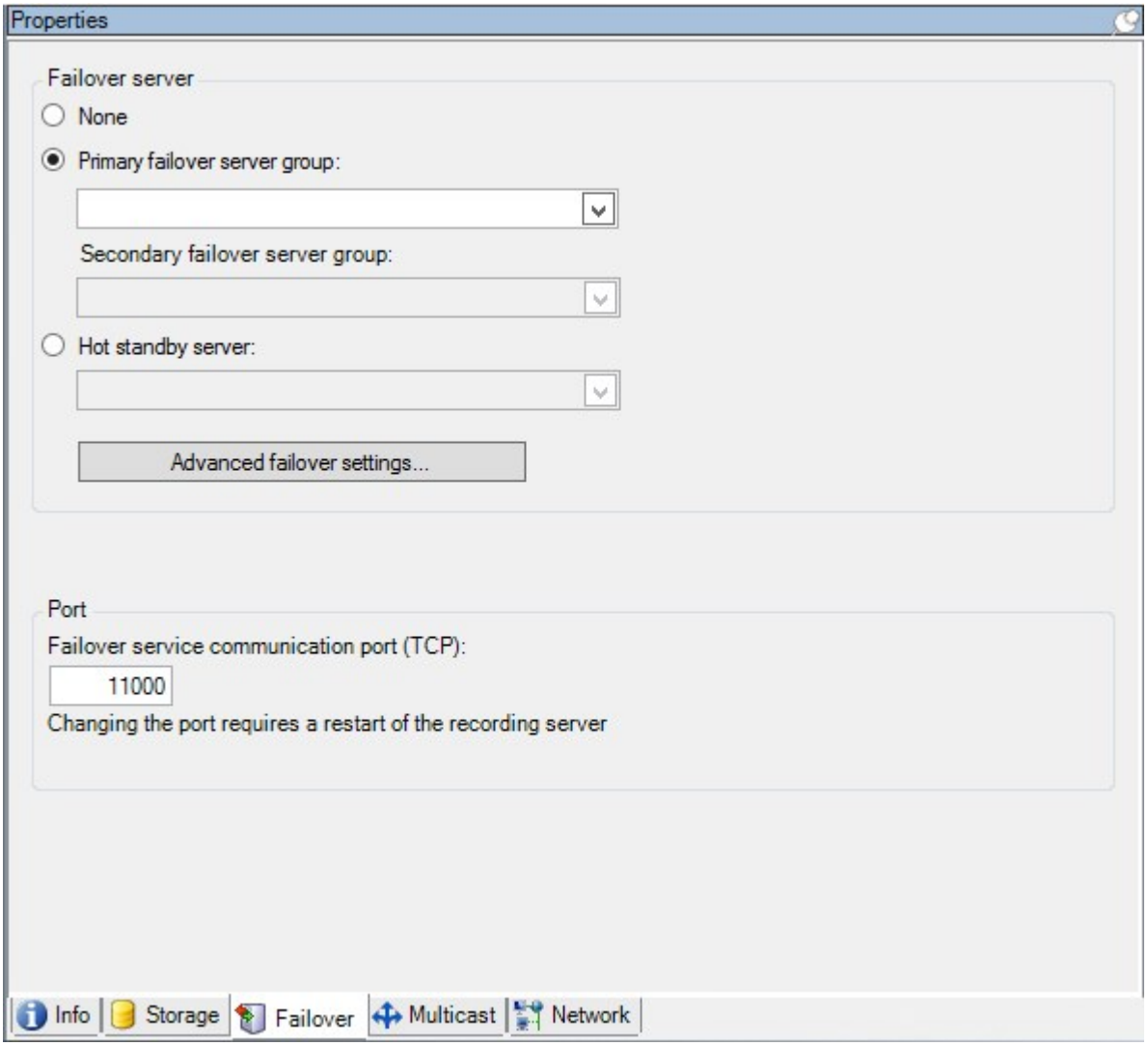
名前	説明
名前	必要に応じて、ストレージ名を変更します。名前は一意でなければなりません。
パス	このストレージで記録を保存するディレクトリへのパスを指定します。ストレージは、必ずしもレコーディングサーバーのコンピュータに存在する必要はありません。 ディレクトリが存在しない場合は作成できます。ネットワークドライブは、必ずUNC(汎用名前付け規則)のフォーマットを使用して指定する必要があります。例:`\\server\volume\directory\`。
保存期間	アーカイブ設定に応じて、削除または次のアーカイブに移動するまでに、記録がアーカイブに格納される期間を指定します。 保存期間は、前のアーカイブまたはデフォルトの録画データベースの保存期間より必ず長くなるようにしてください。アーカイブに対して指定される保存日数には、プロセスで以前に指定されたすべての保存期間が含まれるためです。
最大サイズ	記録データベースに保存する記録データの最大ギガバイト数を選択します。 指定されたギガバイト数を超える記録データは、指定された場合、自動的にリストの最初のアーカイブに移動されるか、削除されます。

名前	説明
	空き容量が5GB未満になった場合、データベースで最も古いデータは必ず自動アーカイブされます(または、次のアーカイブが定義されていない場合は削除されます) 。空き容量が1GB未満になった場合は、データは削除されます。データベースには、必ず250MBの空き容量が必要です。この制限に達した場合(データが十分速やかに削除されていない場合) 、十分な空き容量が確保されるまで、それ以上データベースにはデータが書き込まれません。このため、データベースの実際の最大サイズは、指定したギガバイト数より5GB少なくなります。
スケジュール	アーカイブプロセスが開始する間隔を示すアーカイブスケジュールを指定します。アーカイブは非常に高い頻度(原則として、1年中にわたって毎時毎にアーカイブ) 、あるいは非常に低い頻度(たとえば、36か月ごとに一度、月初の月曜日にアーカイブ) で行うことができます。
フレームレートの低減	**フレームレートの低減**チェックボックスを選択し、アーカイブの際に秒当たりのフレーム数(FPS)を低減できるように、FPSを設定します。 選択した数のFPSでフレームレートを低減すると、アーカイブで記録が占める容量を低減できます。ただし、アーカイブ品質も低下します。 MPEG-4/H.264/H.265は、最小限として自動的にキーフレームに低減されます。 0.1 = 1フレーム/10秒

フェールオーバータブ(レコーディングサーバー)

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

組織がフェールオーバーレコーディングサーバーを使用する場合、**フェールオーバー**タブを使用して、フェールオーバーサーバーをレコーディングサーバーに割り当てます。フェールオーバータブのプロパティを参照してください。



フェールオーバーレコーディングサーバー、インストールと設定、フェールオーバーグループ、およびこれらの設定について詳しくは、「37ページのフェールオーバーレコーディングサーバー(説明付き)」を参照してください。

フェールオーバータブのプロパティ

名前	説明
無し	フェールオーバーレコーディングサーバーなしで設定を選択します。
プライマリフェールオーバーサーバーグループ / セカンダリフェールオーバーサー	1つのプライマリフェールオーバーサーバーグループと任意で1つのセカンダリフェールオーバーサーバーグループから成る通常のフェールオーバー設定を選択します。

名前	説明
バーグループ	
ホットスタンバイサーバー	ホットスタンバイサーバーとして1つの専用レコーディングサーバーを用意し、ホットスタンバイ設定を選択します。
フェールオーバー詳細設定	**[フェールオーバー詳細設定]**ウィンドウを開きます。 • **フルサポート**: デバイスのフェールオーバーサポートを完全に有効にする • **ライブ専用**: デバイス上のライブストリームのフェールオーバーサポートのみを有効にする • **無効**: デバイスのフェールオーバーサポートを無効にする
フェールオーバーサービス通信ポート(TCP)	デフォルトのポート番号は11000です。このポートがレコーディングサーバーとフェールオーバーレコーディングサーバー間での通信で使用されます。ポートを変更した場合、レコーディングサーバーが実行中でなければ**ならず**、また、その間マネジメントサーバーに接続されていなければ**なりません**。

マルチキャストタブ(レコーディングサーバー)

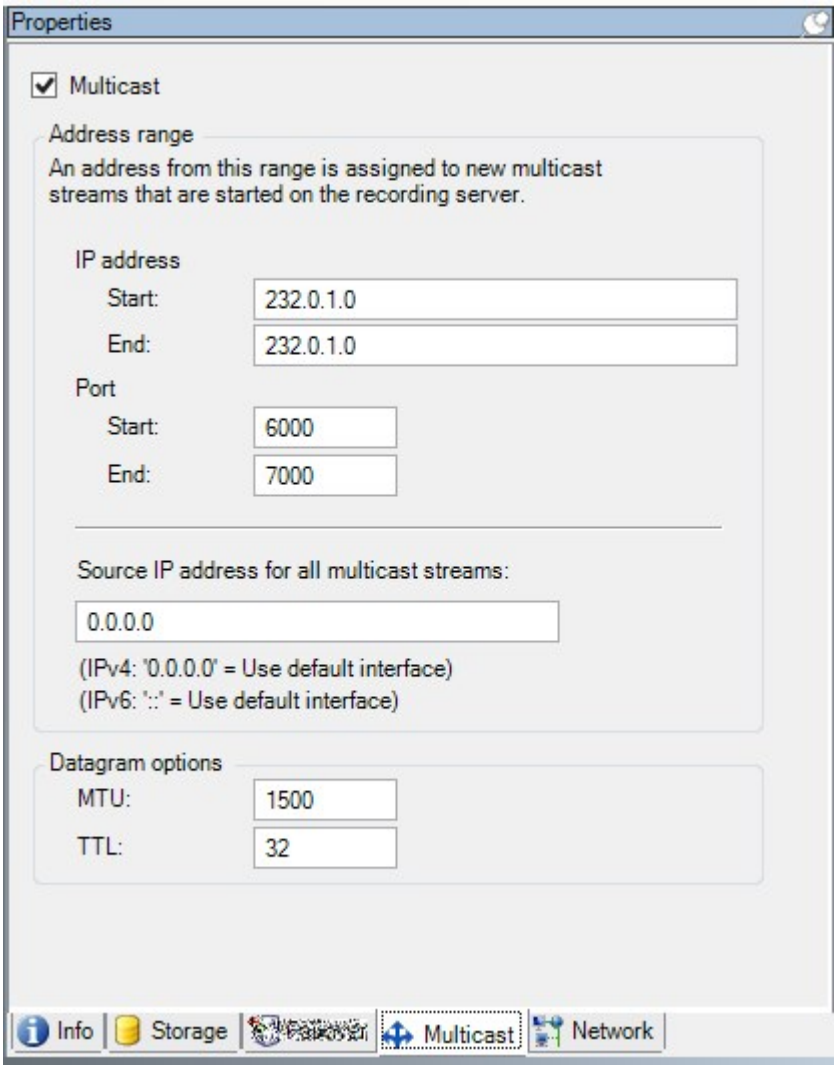
システムは、レコーディングサーバーからのライブストリームのマルチキャストをサポートしています。複数のXProtect Smart Clientユーザーが同じカメラからのライブビデオを再生しようとする場合に、マルチキャストによってシステムリソースの消費量を大幅に低減できます。マルチキャストは、複数のクライアントが同じカメラからのライブビデオを頻繁に要求し、Matrix機能を使用する場合に特に有益です。

マルチキャストは、録画されたビデオ/音声ではなく、ライブストリームでのみ可能です。

レコーディングサーバーに複数のネットワークインターフェイスカードがある場合、マルチキャストはその中の1つのカードでのみ可能です。どのネットワークインターフェイスカードを使用するか、Management Clientによって指定できます。

フェールオーバーサーバーを使用している場合は、フェールオーバーサーバー上のネットワークインタフェイスカードのIPアドレスも必ず指定してください(「405ページのマルチキャストタブ(フェールオーバーサーバー)」を参照)。

マルチキャストを正しく実装するには、ネットワーク装置がマルチキャストのデータパケットを必要な受信者のグループのみに配信されるように設定されていることも必要です。そうでないと、マルチキャストはブロードキャストと変わらなくなり、ネットワーク通信速度が大幅に低下します。



IPアドレス範囲の割り当て

選択したレコーディングサーバーからのマルチキャストストリームにアドレスを割り当てる範囲を指定します。クライアントは、対象となるレコーディングサーバーからのマルチキャストビデオを再生する時に、これらのアドレスに接続します。

マルチキャストカメラフィードのそれぞれについて、IPアドレスとポートの組み合わせは一意でなければなりません。(IPv4の例:232.0.1.0:6000).1つのIPアドレスと複数のポートを、あるいは複数のIPアドレスと少数のポートを使用することができます。デフォルトでは、システムは単一のIPアドレスと1000のポートの範囲を使用するよう推奨しますが、必要であれば変更できます。

マルチキャストのIPアドレスは、IANAによるダイナミックホスト割り当てで定義された範囲内でなければなりません。IANAはグローバルIPアドレス割り当てを監視する機関です。

名前	説明
IPアドレス	**開始**フィールドで、必要な範囲の最初のIPアドレスを指定します。次に、範囲で最後のIPアドレスを**終了**フィールドで指定します。
ポート	**開始**フィールドで、必要な範囲で最初のポート番号を指定します。次に、範囲で最後のポート番号を**終了**フィールドで指定します。
すべてのマルチキャストストリームの送信元IPアドレス	マルチキャストは1つのネットワークインターフェースカードでだけできるため、レコーディングサーバーに複数のネットワークインターフェイスカードがあるか、複数のIPアドレスのネットワークインターフェイスカードが1つある場合に、このフィールドを使用します。 レコーディングサーバーのデフォルトのインターフェースを使用する場合は、フィールドの値を0.0.0.0 (IPv4の場合) または :: (IPv6の場合) のままにします。他のネットワークインターフェースカードを使用する場合、または同じネットワークインターフェースカードで別のIPアドレスを使用する場合、必要なインターフェースのIPアドレスを指定します。 • IPv4:224.0.0.0 ~ 239.255.255.255. • IPv6: 範囲については、IANA Webサイト(https://www.iana.org/) を参照してください。

データグラムオプションの指定

マルチキャストで転送するデータパケット(データグラム) の設定を指定します。

名前	説明
MTU	最大転送ユニット、許容される物理的データパケットの最大サイズです(単位はバイト) 。指定されたMTUより大きいメッセージは、送信する前に小さいパケットに分割されます。デフォルト値は1500バイトです。これは大半のWindowsコンピュータやイーサネットネットワークでのデフォルトでもあります。
TTL	生存時間、廃棄または返却されるまでに、データパケットが移動できるホップの最大数です。ホップとは、2つのネットワークデバイス(通常はルーター) の間のポイントのことです。既定値は128です。

ネットワークタブ(レコーディングサーバー)

パブリックネットワークまたは信頼できないネットワークでXProtect Smart Clientを使用してVMSにアクセスする必要がある場合、MilestoneはVPN経由で安全な接続を使用することを推奨しています。これはXProtect Smart ClientとVMSサーバー間の通信を確実に保護することに役立ちます。

レコーディングサーバーのパブリックIPアドレスは**ネットワーク**タブで定義します。

パブリックアドレスを使用する理由

クライアントはローカルネットワークに加えてインターネットから接続することもあります。いずれの場合にも、レコーディングサーバーからのライブビデオや録画ビデオにクライアントがアクセスできるように、監視システムが適切なアドレスを提供する必要があります。

- クライアントがローカルで接続する場合、監視システムはローカルのアドレスおよびポート番号を返します。
- クライアントがインターネットから接続する場合、監視システムはレコーディングサーバーのパブリックアドレスを返します。これはファイアウォールまたはNAT(ネットワークアドレス変換) ルーターのアドレスであり、多くの場合、異なるポート番号です。アドレスおよびポートは、サーバーのローカルアドレスおよびポートに転送できます。

フェールオーバーサーバー(サーバーノード)

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

フェールオーバーレコーディングサーバーは、予備のレコーディングサーバーで、通常のレコーディングサーバーが使用できなくなったときに使用されます。フェールオーバーレコーディングサーバーは、**コールドスタンバイサーバー**として、または**ホットスタンバイサーバー**として、2つの方法で構成できます。

フェールオーバー レコーディングサーバーは、通常のレコーディングサーバーと同様にインストールされます(158ページのDownload Managerを介したフェールオーバー レコーディングサーバーのインストールを参照) 。フェールオーバーレコーディングサーバーがインストールされると、Management Clientで表示されるようになります。Milestoneはすべてのフェールオーバーレコーディングサーバーを個別のコンピュータにインストールすることを推奨しています。フェールオーバーレコーディングサーバーが、マネジメントサーバーの正しいIPアドレス/ホスト名を用いて構成されていることを確認します。フェールオーバーサーバーサービスを実行するユーザーアカウントのユーザー権限は、インストールプロセス中に付与されます。すなわち:

- フェールオーバーレコーディングサーバーを開始または停止するための開始/停止許可
- RecorderConfig.xmlファイルを読み取る/書き込むための読み取りおよび書き込みアクセス許可

暗号化に対して証明書が選択されている場合、管理者は選択した証明書プライベートキーにおいて、フェールオーバーユーザーに読み取りアクセス許可を付与する必要があります。

Milestoneでは、フェールオーバーレコーディングサーバーが暗号化を使用しているレコーディングサーバーを引き継ぐ際、フェールオーバーレコーディングサーバーも暗号化を使用するよう準備する必要があります。詳細については 136ページの安全な通信(説明付き) と「158ページのDownload Managerを介したフェールオーバーレコーディングサーバーのインストール」を参照してください。

デバイスレベルで必要なフェールオーバーサポートのタイプを指定できます。レコーディングサーバー上の各デバイスで、フル、ライブのみ、フェールオーバーサポートなしを選択できます。これにより、フェールオーバーリソースに優先順位を付けることができます。例えば、ビデオのフェールオーバーのみを設定し、音声には設定しないことも可能です。また、重要性の低いカメラにはフェールオーバーせず、重要なカメラのみをフェールオーバーの対象にできます。

システムがフェールオーバーモードの間は、ハードウェアの置き換えや削除、レコーディングサーバーの更新、ストレージ設定やビデオストリーム設定のようなデバイスの設定を行うことはできません。

コールドスタンバイフェールオーバーレコーディングサーバー

コールドスタンバイフェールオーバーレコーディングサーバーの設定では、1つのフェールオーバーグループに複数のフェールオーバーレコーディングサーバーを集めます。複数の事前に選択されたレコーディングサーバーのいずれかが使用できなくなった場合に、フェールオーバーグループ全体が代わりに対応します。必要な数だけグループを作成することができます(200ページのコールドスタンバイ用にフェールオーバーレコーディングサーバーをグループ化を参照)。

グループ化には明確なメリットがあります。レコーディングサーバーに取って代わるフェールオーバーレコーディングサーバーを後から指定する場合は、フェールオーバーレコーディングサーバーのグループを選択します。選択したグループに複数のフェールオーバーレコーディングサーバーがある場合、レコーディングサーバーを使用できなくなっても引き継ぎの準備ができているフェールオーバーレコーディングサーバーが1台以上あるため、安全です。プライマリグループのすべてのレコーディングサーバーが応答しない場合は、プライマリグループにとって代わるフェールオーバーサーバーのセカンダリグループを特定できます。1つのフェールオーバーレコーディングサーバーは、一度に1つのグループにのみ属することができます。

フェールオーバーグループのフェールオーバーレコーディングサーバーには順序があります。この順序に従い、フェールオーバーレコーディングサーバーが、レコーディングサーバーに取って代わる順序が決定されます。デフォルトでは、フェールオーバーグループでフェールオーバーレコーディングサーバーを統合した順序が反映されます。必要に応じて、この順序は変更できます。

ホットスタンバイフェールオーバーレコーディングサーバー

このため、システムはこのフェールオーバーレコーディングサーバーを「スタンバイ」モードのままにできます。つまり、レコーディングサーバーの現在の正しい構成を使用してすでに起動されており、専用であるため、コールドスタンバイフェールオーバーレコーディングサーバーよりも迅速に切り替えられます。前述の通り、ホットスタンバイサーバーは1つのレコーディングサーバーにのみ割り当てられ、グループ化できません。すでにフェールオーバーグループに含まれているフェールオーバーサーバーは、ホットスタンバイレコーディングサーバーとして割り当てできません。

フェールオーバーレコーディングサーバーの検証

フェールオーバーサーバーからレコーディングサーバーへのビデオデータの統合を検証するには、レコーディングサーバーのサービスを停止するか、レコーディングサーバーのコンピュータをシャットダウンしてレコーディングサーバーを利用できない状態にする必要があります。

ネットワークケーブルを抜くか、テストツールを使ってネットワークをブロックするような手動によるネットワークの中断は有効な方法ではありません。

情報タブのプロパティ(フェールオーバーサーバー)

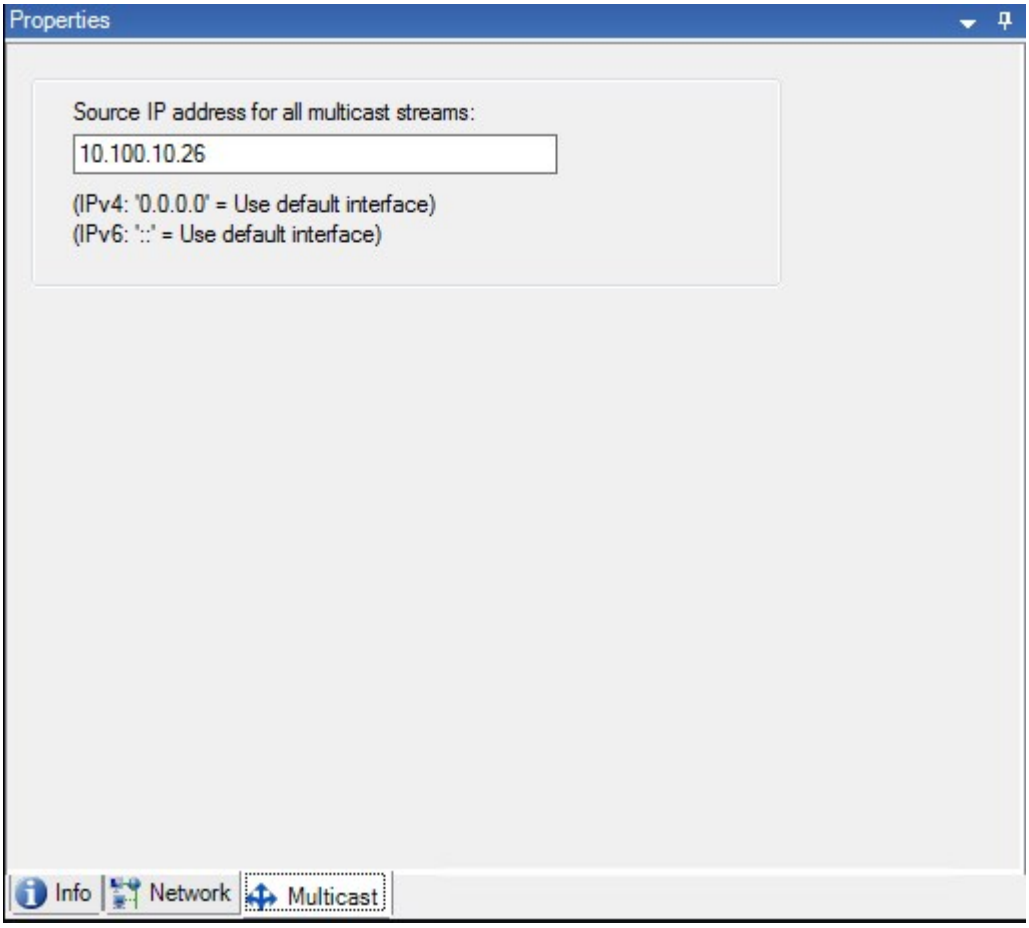
次のフェールオーバーレコーディングサーバーのプロパティを指定します。

名前	説明
名前	Management Client、ログなどに表示されるフェールオーバーレコーディングサーバーの名前。
説明	引き継がれるレコーディングサーバーなど、フェールオーバーレコーディングサーバーを説明するために使用できるオプションのフィールド。
ホスト名	フェールオーバーレコーディングサーバーのホスト名を表示します。これは変更できません。
ローカルWebサーバーアドレス	フェールオーバーレコーディングサーバーのWebサーバーローカルアドレスを表示します。例えば、PTZ カメラコントロールコマンドを使用したり、XProtect Smart Clientからのライブリクエストを閲覧する際には、ローカルアドレスを使用します。 Webサーバーコミュニケーションに使われているポート番号を含むアドレス(標準ポート7563) 。 フェールオーバーレコーディングサーバーが暗号化しているレコーディングサーバーを引き継ぐときは、フェールオーバーレコーディングサーバーも暗号化の準備をする必要があります。 暗号化を有効にすると、パッドロックアイコンと**http**の代わりに**https**を含むアドレスが表示されます。
Webサーバーアドレス	インターネット上のフェールオーバーレコーディングサーバーのWebサーバーパブリックアドレスを表示します。 インストールでファイアウォールまたはNATルーターを使用する際は、ファイアウォールまたはNATルーターのアドレスを入力すると、インターネット上で監視システムにアクセスできるクライアントが、フェールオーバーレコーディングサーバーには接続できません。 パブリックアドレスと**ネットワーク**タブ上でポート番号を指定します。 暗号化を有効にすると、パッドロックアイコンと**http**の代わりに**https**を含むアドレスが表示されます。
UDPポート	フェールオーバーレコーディングサーバー間での通信に使用されるポート番号。デフォルトポートは8844

名前	説明
	です。
データベースの場所	録画の保存用にフェールオーバーレコーディングサーバーで使用されるデータベースへのパスを指定します。 データベースパスは、フェールオーバーレコーディングサーバーがレコーディングサーバーに代替している間には変更できません。ユーザーが行う変更は、フェールオーバーレコーディングサーバーがレコーディングサーバーの代替サーバーではなくなったときに適用されます。
このフェールオーバーサーバーを有効にする	クリアすると、フェールオーバーレコーディングサーバーが無効になります(デフォルトで選択されています)。レコーディングサーバーを切り替える前に、フェールオーバーレコーディングサーバーを無効にする必要があります。

マルチキャストタブ(フェールオーバーサーバー)

フェールオーバーサーバーを使用している場合は、マルチキャストのライブストリームを有効にし、レコーディングサーバーとフェールオーバーサーバーの両方で使用しているネットワークインターフェースカードのIPアドレスを特定する必要があります。



マルチキャストの詳細については、「196ページのレコーディングサーバーのマルチキャストを有効にする」を参照してください。

情報タブの機能(フェールオーバーグループ)

フィールド	説明
名前	Management Client、ログなどに表示されるフェールオーバーグループの名前。
説明	説明(任意)。たとえば、サーバーの物理的な場所。

シーケンスタブのプロパティ(フェールオーバーグループ)

フィールド	説明
フェールオーバーシーケンスの指定	**上**と**下**をクリックし、グループの通常のフェールオーバーレコーディングサーバーの目的のシーケンスを設定します。

のリモートサーバーMilestone Interconnect

Milestone Interconnect™では、物理的に断片化された、より少ない数を統合し、1つのXProtect中央サイトでXProtect Corporateをリモートインストールできます。リモートサイトと呼ばれるこれらの小さいサイトは船舶、バス、電車などのモバイルユニットにインストールできます。つまり、このようなサイトは恒久的にネットワークに接続する必要がありません。

情報タブ(リモートサーバー)

名前	説明
名前	この名前は、システムやクライアントでリモートサーバーが列挙されるたびに使用されます。名前は一意である必要はありません。 サーバーの名前を変更すると、名前はManagement Clientで一括変更されます。
説明	リモートサーバーの説明を入力します(オプション) 。 説明は、システム内の複数のリストに表示されます。たとえば、**概要**ペインでハードウェア名にマウスポインタを移動すると表示されます。
モデル	リモートサイトにインストールされたXProtect製品を表示します。
ﾊﾞｰｼﾞｮﾝ	リモートシステムのバージョンを表示します。
ソフトウェアライセンスコード	リモートシステムのソフトウェアライセンスコード。
ドライバー	リモートサーバーへの接続を処理しているドライバーを規定します。
アドレス	ハードウェアのIPアドレスまたはホスト名。
IE	ハードウェア製造元のデフォルトホームページを開きます。このページはハードウェアまたはシステムの管理に使用します。
リモートシステムID	ライセンスの管理などにXProtectが使用するリモートサイトの一意のシステムID。

設定タブ(リモートサーバー)

設定タブにリモートシステムの名前が表示されます。

イベントタブ(リモートサーバー)

リモートシステムから中央サイトにイベントを追加し、ルールを作成できます。これによって、リモートシステムからのイベントに即時対応できます。イベント数は、リモートシステムで設定されたイベントによって異なります。デフォルトのイベントは削除できません。

表示されるリストが不完全な場合：

1. **概要**ペインで関連するリモートサーバーを右クリックし、**ハードウェアの更新**を選択します。
2. このダイアログボックスには、Milestone Interconnect設定が最後に確立または更新されてから、リモートシステムで行われたすべての変更(デバイスの削除、更新、および追加)のリストが表示されます。**確認**をクリックして、中央サイトにこれらの変更を更新します。

リモート取得タブ

リモート取得タブでは、Milestone Interconnect環境のリモートサイトのリモート記録取得設定を処理できます。

以下のプロパティを指定します。

名前	説明
最大で録画を取得	リモートサイトからの録画の取得に使用する最大帯域幅をキロビット/秒単位で規定します。取得の制限を有効にするには、チェックボックスを選択します。
次の間で録画を取得	リモートサイトからの記録取得を特定の時間間隔に限定するかどうかを決めます。 終了時刻になると、未完了のジョブが完了するまで続行するため、終了時刻が重要な場合、未完了のジョブが完了できるように終了時刻を早く設定する必要があります。 システムが自動取得または取得のリクエストを時間間隔外にXProtect Smart Clientから受け取った場合、リクエストは受け付けられますが、選択された時間間隔に達するまでは開始されません。 ユーザーが開始した保留中のリモート録画取得ジョブは、**システムダッシュボード>現在のタスク**から確認できます。
並列取得デバイス数	記録を同時に取得するデバイスの最大数を規定します。システムの機能にしたがって、容量を増減する必要がある場合にデフォルト値を変更します。

設定を変更すると、変更がシステムで反映されるまでに時間がかかることがあります。

> 上記のいずれも、リモート録画の直接再生には該当しません。
> 直接再生されるように設定されたすべてのカメラは直接再生でき、必要に応じて帯域幅を使用します。

デバイスノード

デバイス(デバイスノード)

ハードウェアをManagement Clientハードウェアの追加 **ウィザードで追加すると、デバイスが**に表示されます。203ページのハードウェアの追加を参照してください。

デバイスのプロパティが同じであれば、デバイスグループからデバイスを管理できます。「52ページのデバイスグループ(説明付き)」を参照してください。

デバイスを個別に管理することもできます。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。デバイスグループ経由のデバイスの有効化/無効化を参照してください。

カメラの他の設定や管理を行うには、いずれも[サイトナビゲーション]ペインで**[デバイス]**を展開してから、デバイスを選択します:

- **カメラ**
- **マイク**
- **スピーカー**
- **メタデータ**
- **入力**
- **出力**

概要ペインで、カメラの概要を分かりやすくするためにカメラをグループ化します。初期グループ化は、**ハードウェアの追加**ウィザードの一部です。

対応ハードウェアについては、MilestoneのWebサイト (https://www.milestonesys.com/support/tools-and-references/supported-devices/) の対応ハードウェアページを参照してください。

デバイスのステータスアイコン

あるデバイスを選択すると、現在のステータスについての情報が**プレビュー**ペインに表示されます。
以下のアイコンはデバイスのステータスを示します:

カメラ	マイク	スピーカー	メタデータ	入力	出力	説明
						**有効なデバイスおよびデータの取得中**:デバイスは有効化され

カメラ	マイク	スピーカー	メタデータ	入力	出力	説明
						ており、ライブストリームを取得します。
						**デバイスは録画中**:デバイスはシステムにあるデータを記録中です。
						**一時的に停止されているか、入力のないデバイス**:停止している場合は、情報はシステムに転送されません。カメラの場合は、ライブビデオを表示できません。停止したデバイスは、デバイスが無効である場合とは対照的に、レコーディングサーバーと通信してイベントの取得、設定の設定などが可能です。
						**無効なデバイス**:ルールを通して自動的に開始されず、レコーディングサーバーと通信できません。カメラが無効な場合は、ライブまたは録画されたビデオを表示できません。
						**デバイスデータベースを修復中です**。
						**デバイスに問題が発生しています**。このデバイスは正しく機能しません。マウスポインタをデバイスアイコンの上で一次停止させて、ヒントに書かれている問題の説明を確認します。
						**不明なステータスです**:デバイスのステータスが不明です。例えば、レコーディングサーバーがオフラインの場合など。
						複数のアイコンを組み合わせることができます。例えばこの場合では**有効なデバイスおよびデータの取得中**が**デバイスは録画中**と組み合わされています。

カメラ(デバイスノード)

カメラデバイスは、システムにハードウェアを追加したときに自動的に追加され、デフォルトで有効化されます。

システムにはデフォルトの配信開始ルールがあります。このルールにより、接続されているすべてのカメラからの映像配信が自動的にシステムに送られます。デフォルトルールは、必要に応じて無効にしたり修正したりできます。

この設定順序に従って、カメラデバイスの設定に関連する最も一般的なタスクを実行します。

1. カメラの設定を行います(「[設定]タブ(デバイス)」を参照)。
2. ストリームの設定を行います(「[ストリーム]タブ(デバイス)」を参照)。
3. モーションの設定を行います(「[モーション]タブ(デバイス)」を参照)。

4. 録画の設定を行います(「[ストリーム]タブ(デバイス) 」および「デバイスのデータベースをモニターする」を参照) 。
5. 必要に応じて他の設定を設定します。

マイク(デバイスノード)

マイクデバイスは、システムにハードウェアを追加したときに自動的に追加されます。デフォルトでは無効化されているため、使用する前に、**ハードウェアの追加** ウィザードから、または後日に有効にする必要があります。マイクには特にライセンスは必要ありません。システムで必要な数のマイクを無制限に使用できます。

マイクは、完全にカメラとは別に使用できます。

システムにはデフォルトの音声配信開始ルールがあります。このルールに従って、接続されているすべてのマイクからの音声配信が自動的にシステムに送られます。デフォルトルールは、必要に応じて無効にしたり修正したりできます。

マイクデバイスは、以下のタブを使って設定できます。

- [情報]タブ(「[情報]タブ(デバイス) 」を参照)
- [設定]タブ(「[設定]タブ(デバイス) 」を参照)
- [録画]タブ(「[録画]タブ(デバイス) 」を参照)
- [イベント]タブ(「[イベント]タブ(デバイス) 」を参照)

スピーカー(デバイスノード)

スピーカーデバイスは、システムにハードウェアを追加したときに自動的に追加されます。デフォルトでは無効化されているため、使用する前に、**ハードウェアの追加** ウィザードから、または後日に有効にする必要があります。スピーカーには特にライセンスは必要ありません。システムで必要な数のスピーカーを無制限に使用できます。

スピーカーは、完全にカメラとは別に使用できます。

システムにはデフォルトの音声配信開始ルールがあります。このルールに従って、デバイスが起動され、ユーザーが有効にした音声をデバイスからスピーカーに送信する準備ができます。デフォルトルールは、必要に応じて無効にしたり修正したりできます。

スピーカーデバイスは、以下のタブを使って設定できます。

- [情報]タブ(「[情報]タブ(デバイス) 」を参照)
- [設定]タブ(「[設定]タブ(デバイス) 」を参照)
- [録画]タブ(「[録画]タブ(デバイス) 」を参照)

メタデータ(デバイスノード)

システムにはデフォルトの配信開始ルールがあります。このルールに従って、メタデータをサポートする接続されているすべてのハードウェアからのメタデータ配信が自動的にシステムに送られます。デフォルトのルールは、必要に応じて無効に設定することや、修正することができます。

メタデータデバイスは、以下のタブを使って設定できます。

- [情報]タブ(「[情報]タブ(デバイス)」を参照)
- [設定]タブ(「[設定]タブ(デバイス)」を参照)
- [録画]タブ(「[録画]タブ(デバイス)」を参照)

入力(デバイスノード)

入力デバイスは、完全にカメラとは別に使用できます。

デバイスで外部入力ユニットの使用を指定する前に、デバイス自体がセンサーの動作を認識しているか確認してください。大半のデバイスでは、設定用インターフェースかコモンゲートウェイインターフェース(CGI)スクリプトのコマンドでこれを表示できます。

入力デバイスは、システムにハードウェアを追加したときに自動的に追加されます。デフォルトでは無効化されているため、使用する前に、**ハードウェアの追加**ウィザードから、または後日に有効にする必要があります。入力デバイスには特にライセンスは必要ありません。システムで必要な数の入力デバイスを無制限に使用できます。

入力デバイスは、以下のタブを使って設定できます。

- [情報]タブ(「[情報]タブ(デバイス)」を参照)
- [設定]タブ(「[設定]タブ(デバイス)」を参照)
- [イベント]タブ(「[イベント]タブ(デバイス)」を参照)

出力(デバイスノード)

出力は、Management ClientおよびXProtect Smart Clientから手動で起動できます。

デバイスで外部出力ユニットの使用を指定する前に、デバイス自体が出力に接続されたデバイスを制御できるかどうかを確認してください。大半のデバイスでは、設定用インターフェースかコモンゲートウェイインターフェース(CGI)スクリプトのコマンドでこれを表示できます。

出力デバイスは、システムにハードウェアを追加したときに自動的に追加されます。デフォルトでは無効化されているため、使用する前に、**ハードウェアの追加**ウィザードから、または後日に有効にする必要があります。出力デバイスには特にライセンスは必要ありません。システムで必要な数の出力デバイスを無制限に使用できます。

出力デバイスは、以下のタブを使って設定できます。

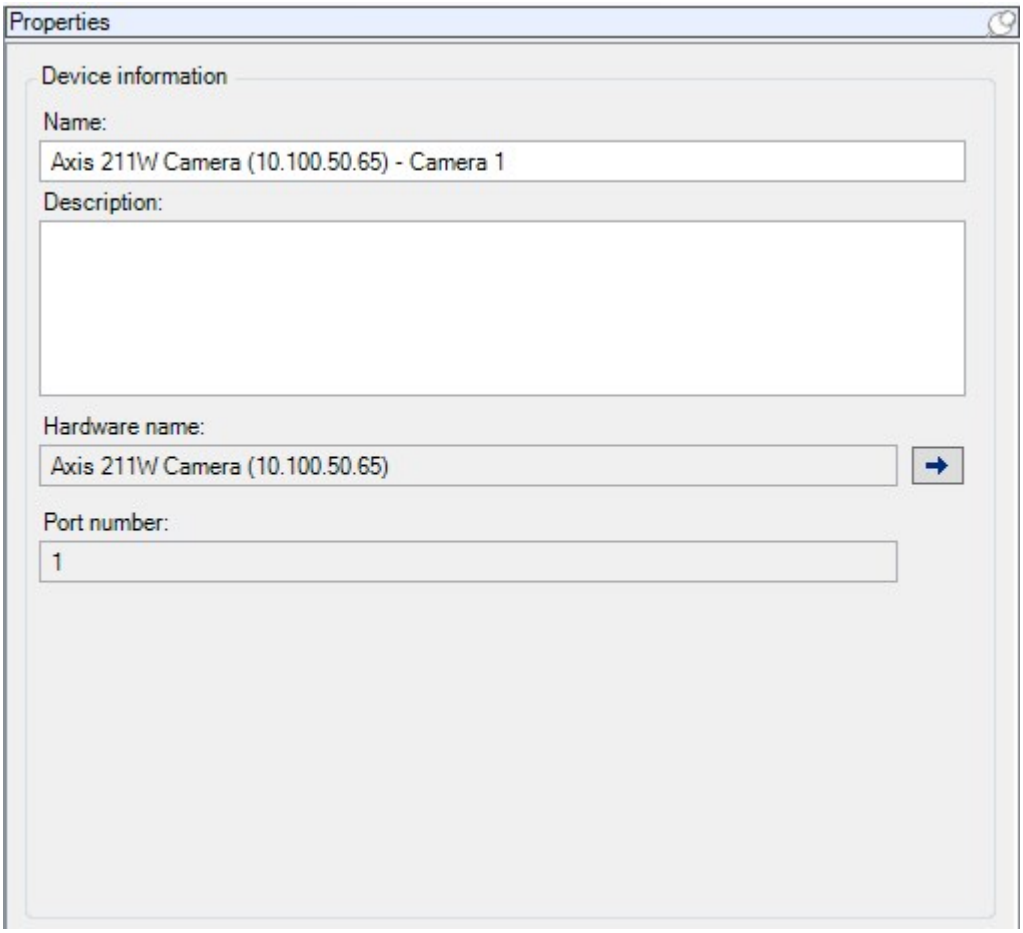
[情報]タブ(以下を参照)

- [情報]タブ(「[情報]タブ(デバイス)」を参照)
- [設定]タブ(「[設定]タブ(デバイス)」を参照)

デバイスタブ

情報タブ(デバイス)

情報タブで、デバイスに関する基本情報を複数のフィールドで表示および編集することができます。
すべてのデバイスに**情報**タブがあります。



情報タブのプロパティ

名前	説明
名前	デバイスがシステムおよびクライアントに一覧されるときにこの名前が使用されます。 デバイスの名前を変更すると、名前はManagement Clientで一括変更されます。
説明	デバイスの説明を入力します(オプション) 。

名前	説明
	説明は、システム内の複数のリストに表示されます。例えば、**概要**ペインで名前の上にマウスポインタを置くと表示されます。
ハードウェア名	デバイスが接続されているハードウェアの名前を表示します。ここからはフィールドを編集できませんが、その横にある**移動**をクリックして変更することができます。これによりハードウェア情報に移動し、名前を変更できます。
ポート番号	デバイスがハードウェアに接続されているポートを表示します。 デバイスが1つしかないハードウェアでは、ポート番号は通常**1**になります。複数のチャネルがあるビデオサーバーなどのマルチデバイスハードウェアでは、通常、ポート番号はデバイスが接続されているチャネルを示しています(例 : **3**) 。
略称	カメラに略称をつけるには、ここに入力してください。最大文字数は128文字です。 スマートマップを使用している場合、スマートマップ上のカメラに自動的に略称が表示されます。または、フルネームが表示されます。
地理的座標	カメラの地理的位置を**latitude, longitude**のフォーマットで入力します。入力する値によって、XProtect Smart ClientおよびXProtect Mobileクライアントのスマートマップ上のカメラアイコンの位置が決まります。 このフィールドは主にスマートマップとサードパーティー統合のためのものです。
方向	垂直軸上の真北の点に対するカメラの視線方向を入力します。入力する値によって、XProtect Smart ClientおよびXProtect Mobileクライアントのスマートマップ上のカメラアイコンの位置が決まります。 デフォルト値は0.0.です。 このフィールドは主にスマートマップとサードパーティー統合のためのものです。
視野	視野の幅を度で入力します。入力する値によって、XProtect Smart ClientおよびXProtect Mobileクライアントのスマートマップ上のカメラアイコンの視野角が決まります。 デフォルト値は0.0.です。 このフィールドは主にスマートマップとサードパーティー統合のためのものです。
深度	視野深度をメートルまたはフィートで入力します。入力する値によって、XProtect Smart ClientおよびXProtect Mobileクライアントのスマートマップ上のカメラアイコンの視野の長さが決まります。 デフォルト値は0.0.です。

名前	説明
	 このフィールドは主にスマートマップとサードパーティー統合のためのものです。
ブラウザで位置をプレビューする...	入力した座標が適切であるかどうかを確認するには、このボタンをクリックします。インターネットブラウザの指定の場所でGoogle マップが開きます。  このフィールドは主にスマートマップとサードパーティー統合のためのものです。

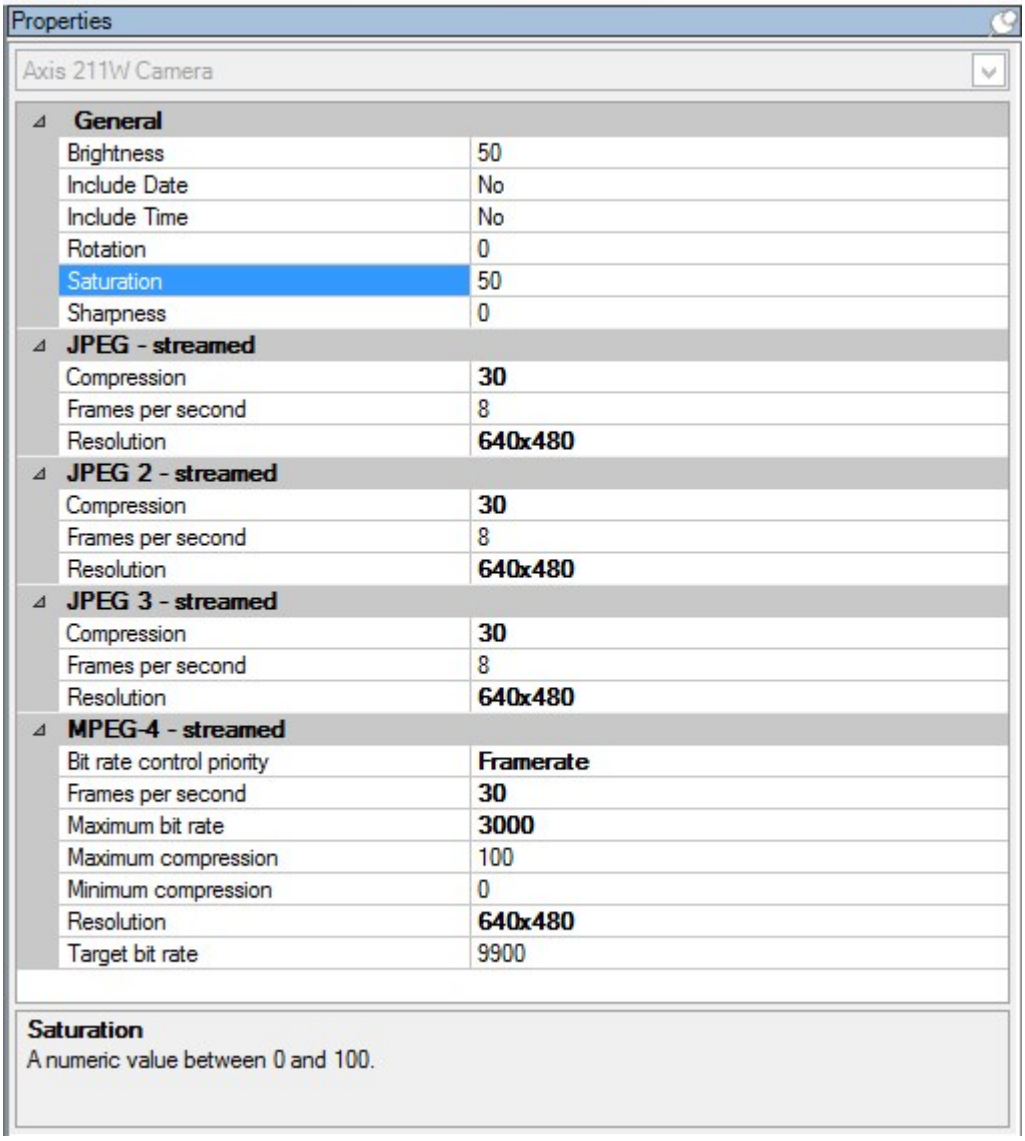
設定タブ(デバイス)

設定タブで、デバイスの設定を複数のフィールドで表示および編集することができます。
すべてのデバイスに**設定**タブがあります。

表に表示される値は、変更可能または読み取り専用です。設定をデフォルト以外の値に変更した場合は、値が太字で表示されます。

テーブルの内容はデバイスドライバーによって異なります。

許可された範囲が設定表の下の情報ボックスに表示されます。



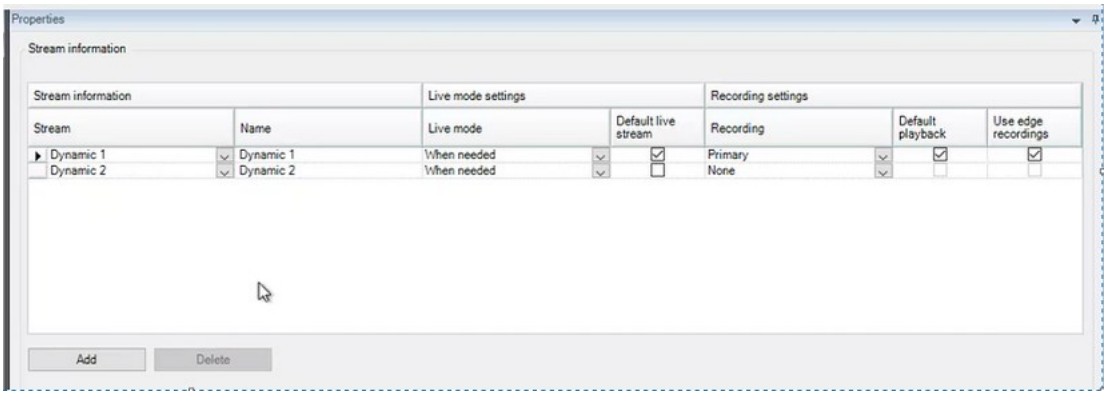
カメラ設定の詳細については、「カメラ設定の表示または編集」を参照してください。

ストリームタブ(デバイス)

以下のデバイスに**ストリーム**タブがあります。

- カメラ

ストリームタブはデフォルトで単一のストリームを一覧表示します。このストリームは、選択したカメラのデフォルトのストリームであり、ライブビデオや、録画したビデオで使用されます。アダプティブ再生を使用する場合、2つのストリームが作成されるはずです。



ストリームタブのタスク

名前	説明
追加	クリックして、ストリームをリストに追加します。 ストリームを追加

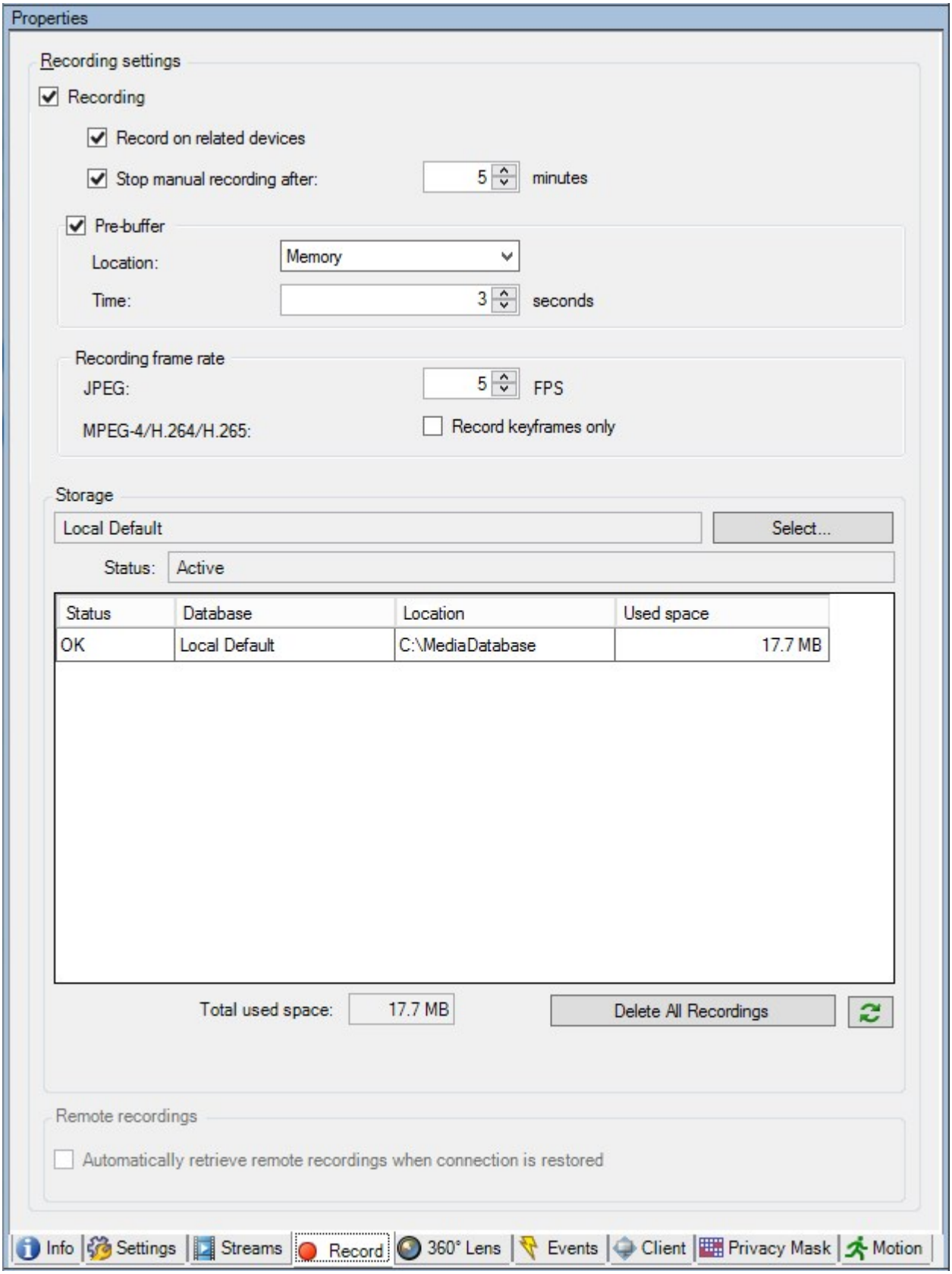
録画タブ(デバイス)

以下のデバイスに**録画**タブがあります。

- カメラ
- マイク
- スピーカー
- メタデータ

デバイスからの録画は、録画を有効にし、録画関連ルール条件が満たされたときにだけ、データベースに保存されます。

デバイスで設定できないパラメータは淡色表示されます。


Properties
Recording settings
Recording
Record on related devices
Stop manual recording after:
5
minutes
Pre-buffer
Location:
Memory
Time:
3
seconds
Recording frame rate
JPEG:
5
FPS
MPEG-4/H.264/H.265:
Record keyframes only
Storage
Local Default
Select...
Status:
Active
Status
Database
Location
Used space
OK
Local Default
C:\MediaDatabase
17.7 MB
Total used space:
17.7 MB
Delete All Recordings
Remote recordings
Automatically retrieve remote recordings when connection is restored
Info
Settings
Streams
Record
360° Lens
Events
Client
Privacy Mask
Motion

録画タブのタスク

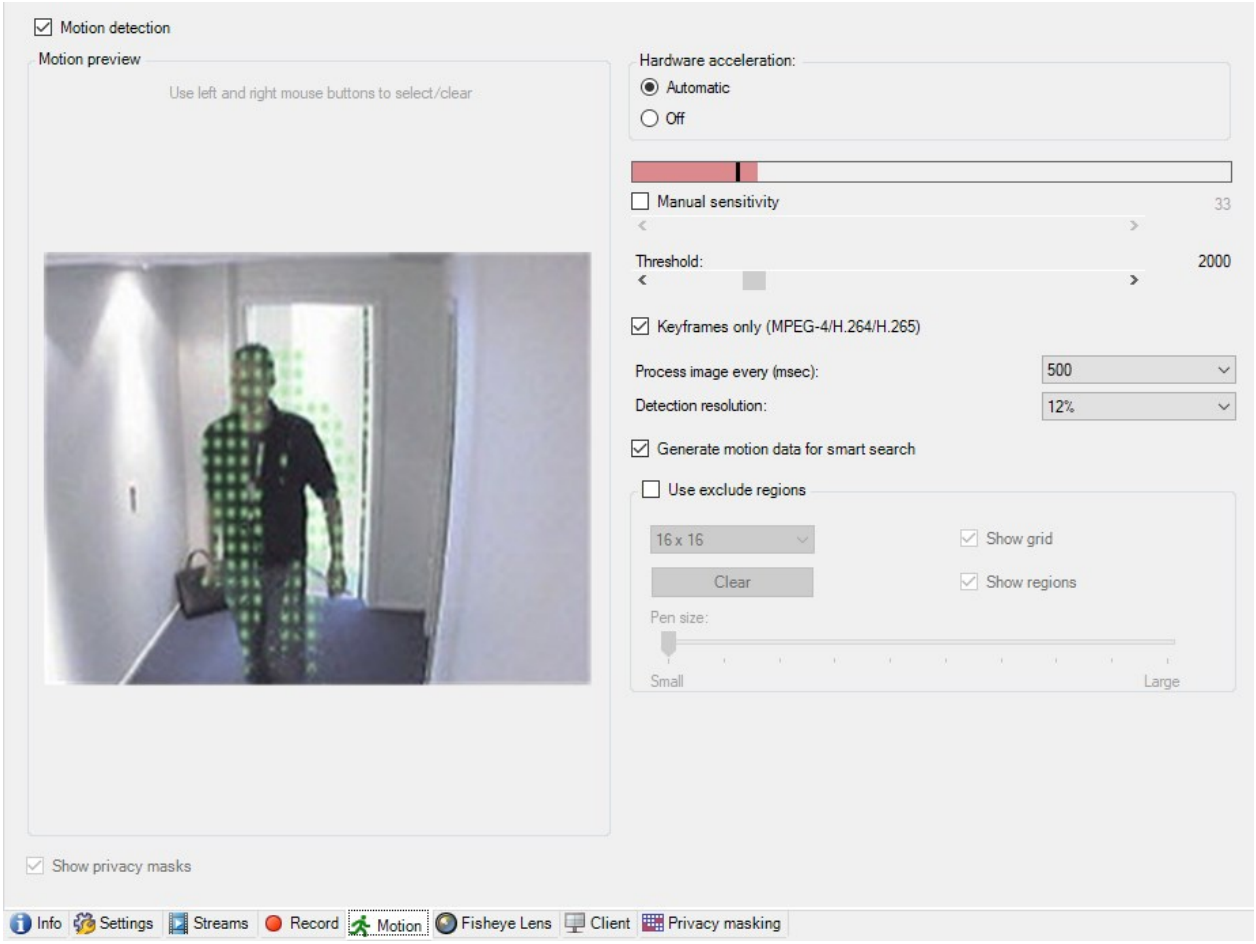
名前	説明
録画	録画を有効/無効にする 関連するデバイスで録画を有効にする
プレバッファ	プレバッファリングとプレバッファ録画のストレージ(説明付き) プレバッファの管理 手動録画の管理
レコーディングフレームレート	レコーディングフレームレートを指定 キーフレームレコーディングを有効にする
ストレージ	デバイスのデータベースのステータスをモニター
選択	デバイスを元のストレージから別のストレージに移動
すべての録画を削除	このボタンは、グループ内の全デバイスを同一のサーバーに追加した場合に使用します。 録画を削除
接続が復旧したときに自動的にリモート録画を取得	リモート録画の保存および取得

モーションタブ(デバイス)

以下のデバイスに**モーション**タブがあります。

- カメラ

モーションタブでは、選択したカメラのモーション検知を有効にして、設定することができます。



モーションタブのタスク

名前	説明
モーション検知	モーション検知を有効/無効にする
ハードウェアアクセラレーション	**自動**を選択してハードウェアアクセラレーションを有効にするか、**オフ**を選択してこの設定を無効にします。詳細については、「ハードウェアアクセラレーションを有効または無効にする」を参照してください。
プライバシーマスク	常時プライバシーマスクがかけられたエリアが定義されている場合、**プライバシーマスク**チェックボックスを選択することで、**モーション**タブにプライバシーマスクを表示することができます。プライバシーマスクがかけられたエリアを定義する操作は、433ページのプライバシーマスクタブ(デバイス)で行います。

名前	説明
	常時プライバシーマスクでカバーされている領域では、モーション検知は行われません。
手動感度	画像において**各ピクセルがどれだけ**変化すればモーションとみなされるかを指定します。 手動感度を有効にしてモーションを定義
しきい値	画像において**ピクセル数がどれだけ**変化すればモーションとみなされるかを指定します。 しきい値を指定してモーションを定義
キーフレームのみ(MPEG-4/H.264/H.265)	このチェックボックスは、モーション検知をビデオストリーム全体ではなく、キーフレームに対してのみ行う場合に選択します。MPEG-4/H.264/H.265のみに適用されます。 キーフレームでのモーション検知により、分析の実施で使用される処理能力の消費量を減らします。
画像処理間隔(ミリ秒)	このリストで画像処理間隔(モーション検知分析をどれくらいの頻度で行うか)を指定します。 例えば、1000ミリ秒ごとにすると1秒間に1回となります。デフォルト値は500ミリ秒ごとです。 ここで設定した間隔よりも実際のフレームレートが高い場合に間隔が適用されます。
検出解像度	このリストで、最適なモーション検知パフォーマンスが得られる検出解像度を選択します。 画像のうち、選択したパーセンテージのみが解析されます(25%など)。25%の分析ということは、すべてのピクセルではなく、画像のピクセルを4つ毎に1つだけ分析することになります。 検知を最適化すると、分析を実行する際の処理能力にかかる消費量は低減できますが、モーション検知の正確性も低下することを意味しています。
スマートサーチ用のモーションデータを生成	このチェックボックスが選択されている場合、モーション検知で使用される画像のモーションデータが生成されます。例えば、キーフレームでのみモーション検知を選択すると、モーションデータはキーフレームでのみ生成されます。 追加のモーションデータにより、ユーザーは、スマートサーチ機能を使用して、画像の選択領域のモーションに基づいて、該当する録画をすばやく検索できます。常設のプライバシーマスクがかけられたエリア内のモーションデータが生成されることはありません。代わりに、除去可能なプライバシーマスクのエリア内のモーションデータのみ生成されます(「モーション検知(説明付き)を参照)。 モーション検知しきい値と除外エリアは、生成されたモーションデータに影響しません。 • **ツール > オプション > 全般**タブで、カメラのスマートサーチデータの生成におけるデフォルト設定を指定します。
除外エリアを使用	カメラビューの特定エリアでのモーション検知を無効にします。 モーション検知の除外エリアを指定

プリセットタブ(デバイス)

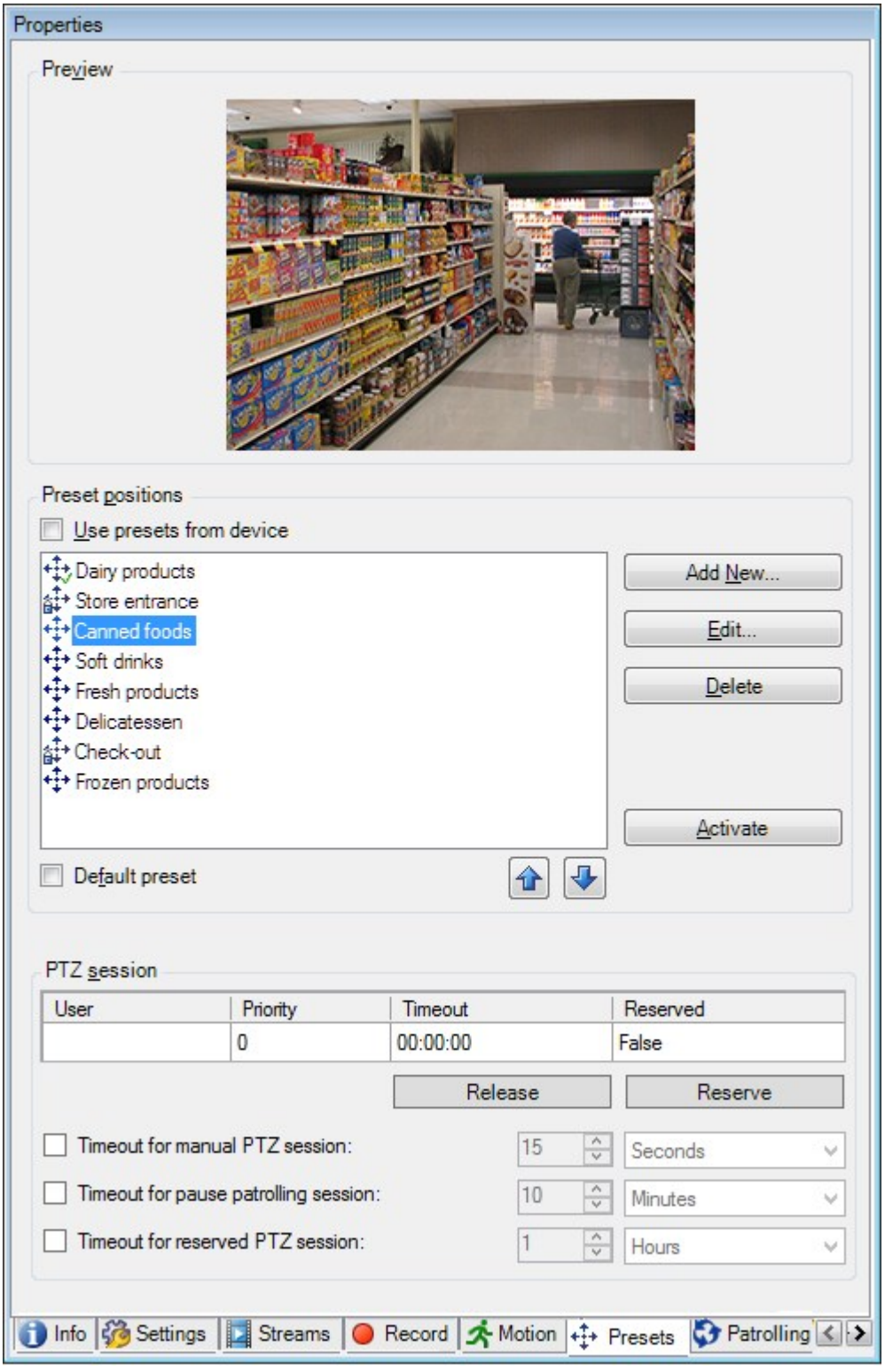
以下のデバイスに**プリセット**タブがあります。

- プリセット位置がサポートされているPTZカメラ

プリセットタブで、プリセット位置を作成またはインポートできます。例:

- イベント発生時にPTZ(パン/チルト/ズーム) カメラを特定のプリセット位置に移動させるためのルール
- 複数のプリセット位置間でPTZカメラを自動的に移動させるパトロール
- XProtect Smart Clientユーザーによる手動アクティベーション向け

セキュリティ全般タブ(479ページのセキュリティ全般タブ(役割) を参照) またはPTZタブ(515ページのPTZタブ(役割) を参照) で、PTZ権限を役割に割り当てます。


Properties
Preview
Preset positions
Use presets from device
Dairy products
Store entrance
Canned foods
Soft drinks
Fresh products
Delicatessen
Check-out
Frozen products
Add New...
Edit...
Delete
Activate
Default preset
PTZ session
User
Priority
Timeout
Reserved
0
00:00:00
False
Release
Reserve
Timeout for manual PTZ session:
15
Seconds
Timeout for pause patrolling session:
10
Minutes
Timeout for reserved PTZ session:
1
Hours
Info
Settings
Streams
Record
Motion
Presets
Patrolling

プリセットタブのタスク

名前	説明
新規	システムにおけるカメラのプリセット位置を追加します。 プリセット位置を追加(タイプ1)
デバイスのプリセットを使用	PTZカメラのプリセット位置を、カメラ自体に追加します。 カメラからのプリセット位置を使用(タイプ2)
デフォルトのプリセット	PTZカメラのプリセット位置のいずれかを、カメラのデフォルトのプリセット位置に割り当てます。 カメラのデフォルトプリセット位置をデフォルトとして割り当て
編集	システムで定義済みの既存のプリセット位置を編集します。 カメラのプリセット位置を編集(タイプ1のみ) カメラで定義されたプリセット位置の名前を編集します。 カメラのプリセット位置の名前を変更(タイプ2のみ)
ロック中	このチェックボックスは、プリセット位置をロックする際に使用します。XProtect Smart Clientのユーザー、またはセキュリティ権限が制限されたユーザーによるプリセットの更新または削除を防止するため、プリセット位置をロックできます。ロックされたプリセットには  アイコンが表示されます。 プリセットのロックは、追加作業(「プリセット位置の追加(タイプ1)」を参照)と編集作業(「プリセット位置の編集(タイプ1のみ)」を参照)の一環として行います。
アクティベート	このボタンをクリックして、カメラのプリセット位置をテストします。 プリセット位置をテスト(タイプ1のみ)します。
予約とリリース	他のユーザーがカメラを制御できないようにしたり、予約をリリースしたりします。 予約されたPTZセッションを実行するセキュリティ権限を持つ管理者は、このモードでPTZカメラを実行できます。これにより、他のユーザーはカメラを制御できなくなります。十分な権限があれば、他のユーザーが予約済みのPTZセッションをリリースできます。

名前	説明
	PTZセッションの予約およびリリース。
PTZセッション	現在システムによってパトロールが実行されているか、またはユーザーが制御しているかをモニターします。 425ページのPTZセッションの優先度。 PTZカメラのステータスを表示して、カメラのタイムアウトを管理します。 PTZセッションタイムアウトを指定

PTZセッションの優先度

PTZセッション表には、PTZカメラの現在のステータスが示されます。

名前	説明
ユーザー	**予約**ボタンを押し、現在PTZカメラを制御しているユーザーを表示します。 パトロールセッションがシステムによってアクティベートされた場合は、**パトロール**と表示されます。
優先度	ユーザーのPTZ優先度が表示されます。自分よりも低い優先度のユーザーからのみPTZセッションを取得できます。
タイムアウト	現在のPTZセッションの残り時間が表示されます。
予約	現在のセッションが予約済みPTZセッションであるかどうかを示します。 • **設定あり**: 予約あり • **設定なし**: 予約なし

PTZセッションセクションのチェックボックスを使用すれば、PTZカメラごとに以下のタイムアウトを変更できます。

名前	説明
手動PTZセッションのタイムアウト	タイムアウトをデフォルト期間から変える場合には、このカメラの手動PTZセッションのタイムアウトを指定します。**オプション**の下の**ツール**メニューでデフォルト期間を指定します。
一時停止パトロールPTZのタイムアウト	タイムアウトをデフォルト期間から変更する場合は、このカメラの一時停止パトロールPTZセッションのタイムアウトを指定します。**オプション**の下の**ツール**メニューでデフォルト期間を指定します。
予約済みPTZセッションのタイムアウト	タイムアウトをデフォルト期間から変更する場合は、このカメラの予約済みPTZセッションのタイムアウトを指定します。**オプション**の下の**ツール**メニューでデフォルト期間を指定します。

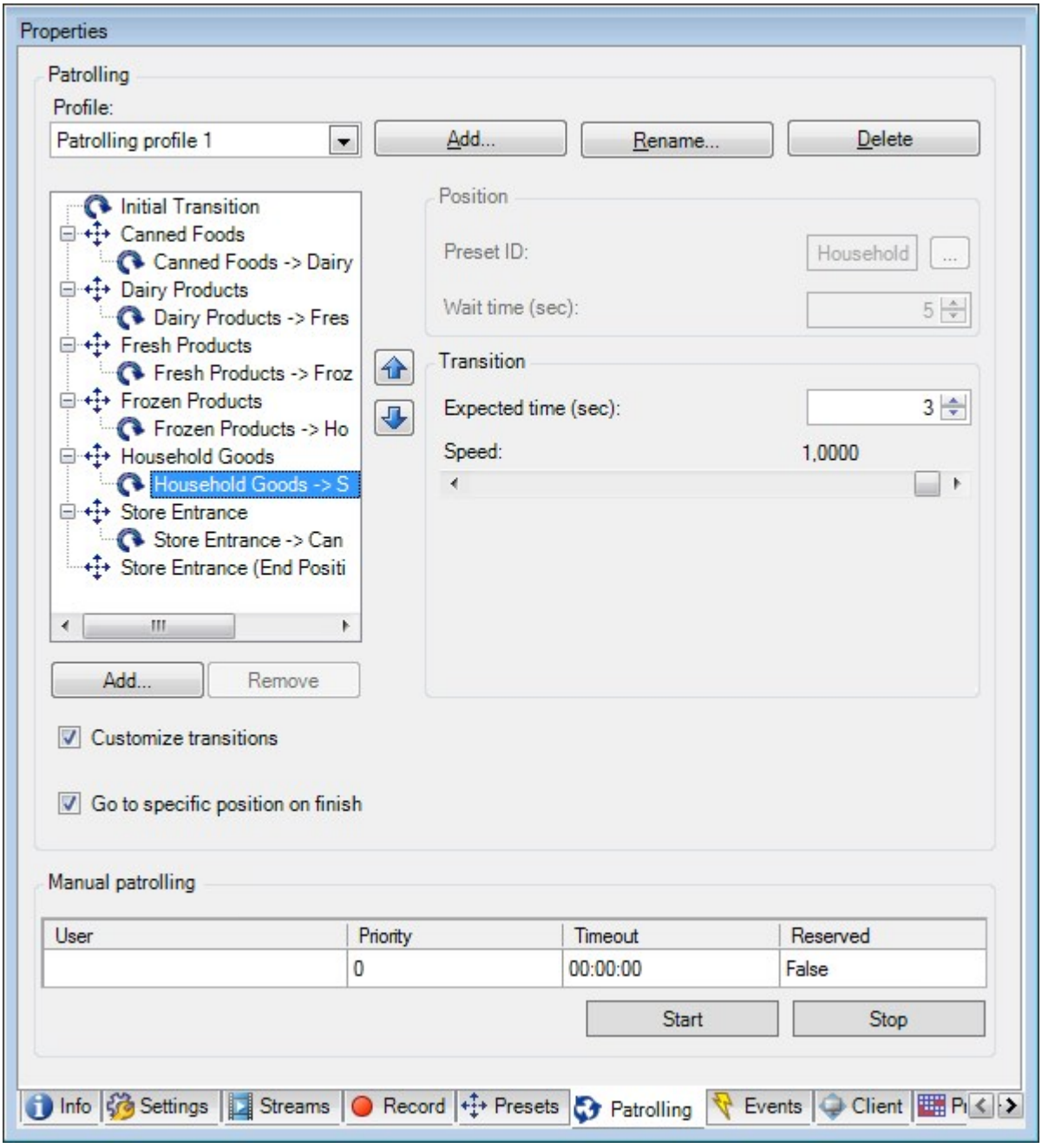
パトロールタブ(デバイス)

以下のデバイスに**パトロール**タブがあります。

- PTZカメラ

パトロールタブでは、パトロール設定を作成して、PTZ(パン/チルト/ズーム)カメラによる多数のプリセット位置間の自動移動を設定できます。
パトロールの設定を開始する前に、**プリセット**タブでカメラに対して少なくとも2つのプリセット位置を指定する必要があります。
「プリセット位置を追加(タイプ1)」を参照してください。

パトロールタブに、カスタマイズした旋回動作が含まれるパトロール設定が表示されています。



パトロールタブのタスク

名前	説明
追加	パトロール設定を追加

名前	説明
プリセットID	パトロール設定でのプリセット位置の指定
待機時間(秒)	各プリセット位置での時間を指定
旋回動作をカスタマイズ	旋回動作(PTZ)をカスタマイズ
終了時に特定の位置に移動	パトロール中に終了位置を指定
手動パトロール	現在システムによってパトロールが実行されているか、またはユーザーが制御しているかをモニターします。
開始および**停止**	**開始**および**停止**ボタンを使用して、手動パトロールを開始および停止します。 どれくらいの時間が経過した後に、すべてまたは個々のPTZカメラに対して定期的なパトロールを再開するかを指定する方法については、「PTZセッションタイムアウトの指定」を参照してください。

手動パトロールプロパティ

PTZパトロール表は、PTZカメラの現在のステータスを示します。

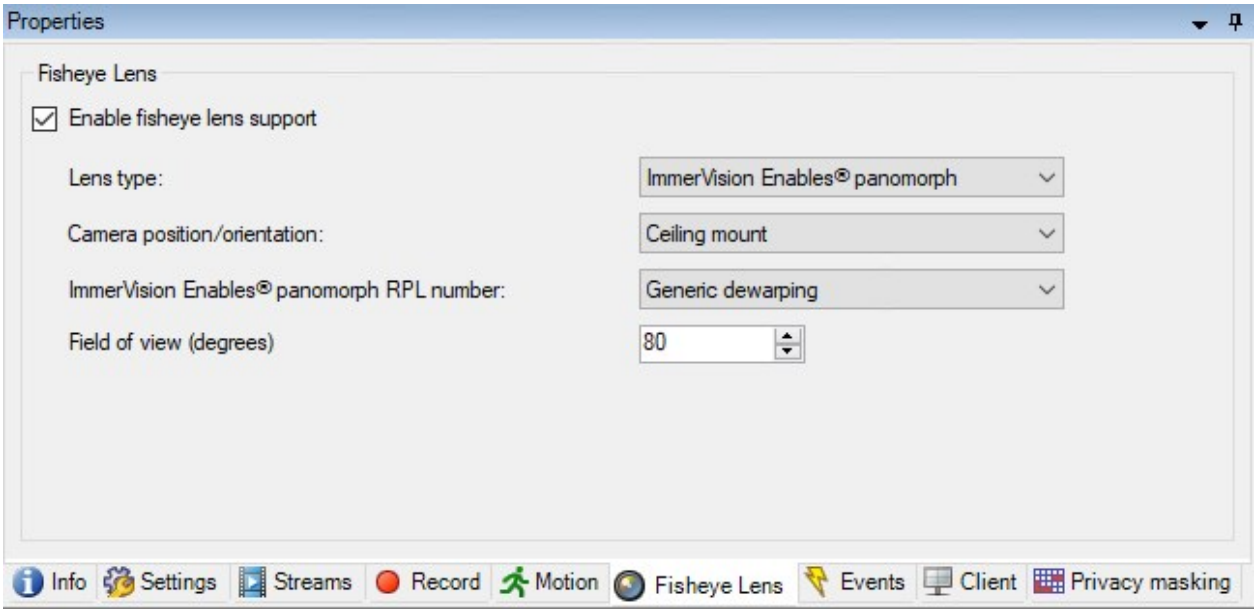
名前	説明
ユーザー	PTZセッションを予約したか、手動パトロールを開始して現在カメラを制御しているユーザーが表示されます。 パトロールセッションがシステムによってアクティベートされた場合は、**パトロール**と表示されます。
優先度	ユーザーのPTZ優先度が表示されます。自分よりも低い優先度のユーザーまたはパトロールプロファイルからのみ、PTZセッションを取得できます。
タイムアウト	現在の予約済みまたは手動PTZセッションの残り時間が表示されます。
予約	現在のセッションが予約済みPTZセッションであるかどうかを示します。 • **設定あり**: 予約あり • **設定なし**: 予約なし

魚眼レンズタブ(デバイス)

以下のデバイスに**魚眼レンズ**タブがあります。

- 魚眼レンズを備えた固定カメラ

魚眼レンズタブでは、選択したカメラの魚眼レンズサポートを有効にして、設定することができます。



魚眼レンズタブのタスク

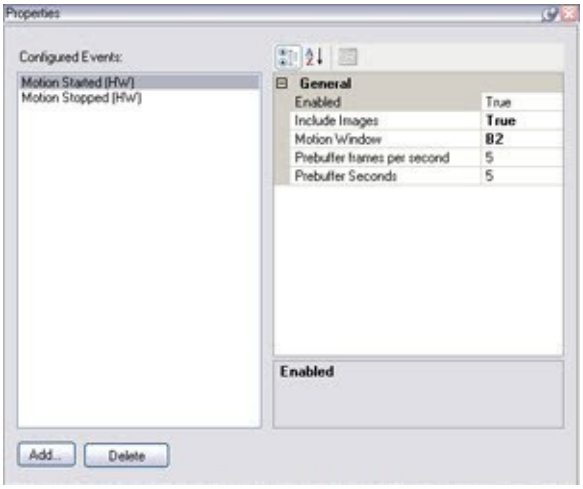
名前	説明
魚眼レンズサポートを有効にする	魚眼レンズサポートを有効/無効にします

イベントタブ(デバイス)

以下のデバイスに**イベント**タブがあります。

- カメラ
- マイク
- 入力

システムのイベントに加えて、一部のデバイスはイベントをトリガーするように設定できます。これらのイベントは、システムでイベントベースのルールを作成する場合に使用できます。技術的には、これらのイベントは、監視システムではなく実際のハードウェア/デバイス上で発生します。



イベントタブのタスク

名前	説明
追加および**削除**	デバイスのイベントを追加または削除します

イベントタブ(プロパティ)

名前	説明
設定済みイベント	**設定済みイベント**リストで、どのイベントを選択して追加できるかは、対象となるデバイスとその設定によって完全に決定されます。デバイスのタイプによっては、リストが空の場合もあります。
一般	プロパティのリストは、対象となるデバイスやイベントによって異なります。目的どおりに機能するようにするには、デバイスの一部またはすべてのプロパティを、このタブと同一になるように指定する必要があります。

クライアントタブ(デバイス)

以下のデバイスに**クライアント**タブがあります。

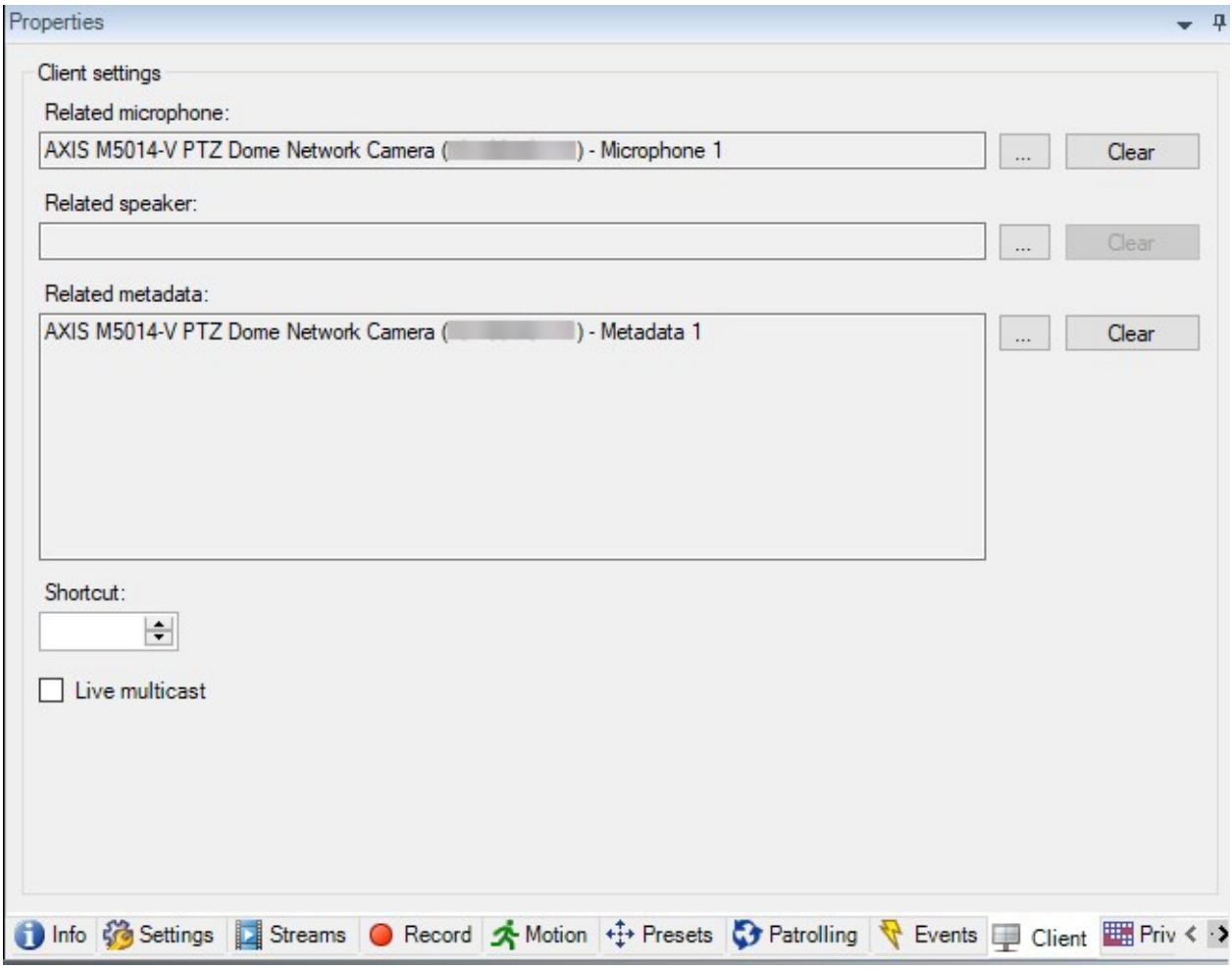
- カメラ

クライアントタブでは、XProtect Smart Clientでカメラを使用する際に閲覧できる他のデバイスを指定できます。

カメラの録画時に、関連デバイスでも録画が行われます219ページの関連するデバイスで録画を有効にする。

カメラの**ライブマルチキャスト**を有効にできます。クライアントのためのレコーディングサーバー経由のカメラマルチキャストライブストリームのことです。

> レコーディングサーバーが暗号を使用している時でも、マルチキャストストリームは暗号化されません。



クライアントタブのプロパティ

名前	説明
関連するマイク	XProtect Smart Clientユーザーがデフォルトでカメラのどのマイクから音声を受信するかを指定します。XProtect Smart Clientユーザーは必要に応じて別のマイクを手動で選択して聞くことができます。

名前	説明
	音声付きビデオをストリームするビデオプッシュカメラに関連するマイクを特定します。 カメラが録画する際に、関連するマイクが録音します。
関連するスピーカー	デフォルトでXProtect Smart Clientユーザーがカメラのどのスピーカーで話すかを指定します。必要に応じてXProtect Smart Clientユーザーは別のスピーカーを手動で選択できます。 カメラが録画する際に、関連するスピーカーが録音します。
関連するメタデータ	XProtect Smart Clientユーザーがデータを受信する、カメラ上のメタデータデバイスを1つ以上指定します。 カメラが録画する際に、関連するメタデータデバイスが記録します。
ショートカット	XProtect Smart Clientユーザーがカメラを簡単に選択できるように、カメラにショートカットキーを定義します。 • カメラを一意に識別できるよう、それぞれにショートカットを作成します • カメラのショートカット番号は4桁以内である必要があります
ライブマルチキャスト	このシステムでは、レコーディングサーバーからXProtect Smart Clientへのライブストリームのマルチキャストをサポートしています。カメラからのライブストリームマルチキャストを可能にするには、チェックボックスを選択します。 **ストリーム**タブ上でカメラのデフォルトストリームとしてストリームを指定している場合のみ、ライブマルチキャスティングが可能です。 レコーディングサーバーに対してもマルチキャストを設定する必要があります。196ページのレコーディングサーバーのマルチキャストを有効にするを参照してください。 レコーディングサーバーが暗号を使用している時でも、マルチキャストストリームは暗号化されません。

プライバシーマスクタブ(デバイス)

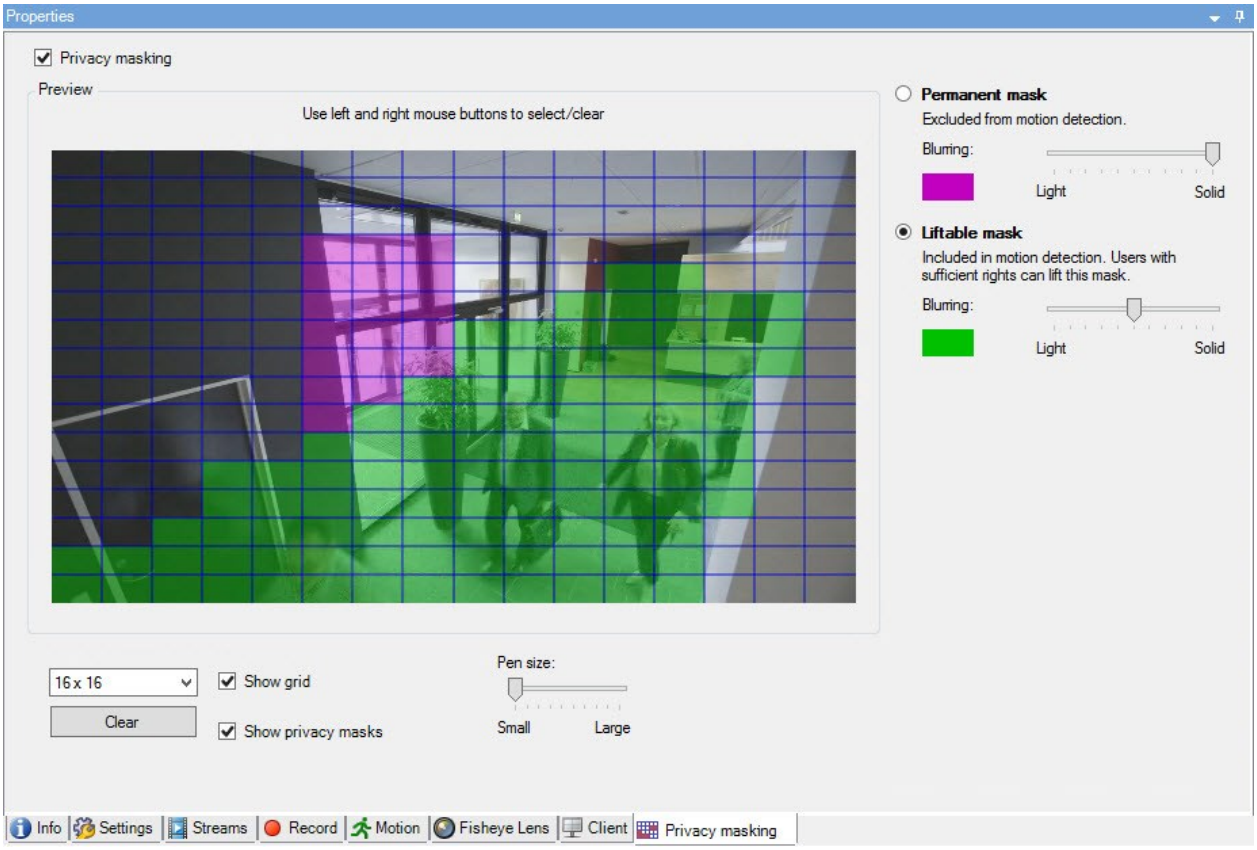
使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

XProtect Essential+ 2018 R1以降は、プライバシーマスクをサポートしません。そのため、プライバシーマスクが適応されたシステムから更新を行った場合には、マスクは除去されます。

以下のデバイスに**プライバシーマスク**タブがあります。

- カメラ

プライバシーマスクタブでは、選択したカメラのプライバシーマスクを有効にして設定できます。



プライバシーマスクタブのタスク

名前	説明
プライバシーマスク	プライバシーマスクの有効化/無効化 プライバシーマスク(説明付き)
常設のマスクおよび**除去可能なマスク**	常設または除去可能なプライバシーマスクのいずれを使用するか指定します。 プライバシーマスクを定義する

プライバシーマスクに関連したタスク

タスク	説明
プライバシーマスク除去の権限を持つ役割に関連付けられた、Smart Clientプロファイル用の除去可能プライバシーマスクのタイムアウトを変更。	除去されたプライバシーマスクのタイムアウトを変更します
特定の役割に対してプライバシーマスクを除去する権限を有効または無効にする。	プライバシーマスクの除去権限をユーザーに付与します
カメラの現在のプライバシーマスク設定に関する情報が記載されたデバイスレポートを作成。	プライバシーマスク設定のレポートを作成します

プライバシーマスクタブ(プロパティ)

名前	説明
グリッドサイズ	選択された値は、グリッドがプレビュー上で表示されるかどうかにかかわらず、グリッドの密度を決定します。 8×8、16×16、32×32または64×64から値を選択します。
クリア	指定した**すべての**プライバシーマスクをクリアします。

名前	説明
グリッドを表示	**グリッドを表示**チェックボックスを選択してグリッドを表示します。
プライバシーマスクを表示	**プライバシーマスクを表示**チェックボックス(デフォルト)を選択すると、常設のプライバシーマスクがプレビューに紫色で表示され、除去可能なプライバシーマスクは緑色で表示されます。 Milestoneこれにより、同僚が現行の**プライバシー**保護設定を見ることができます。
ペンサイズ	**ペンサイズ**スライダーを使って、領域をクリック&ドラッグで選択するサイズを示します。デフォルトでは小さく設定されており、グリッドのマス1つ分に相当する大きさに設定されています。
永続的なマスク	このタブ、および**モーション**タブのプレビューで、紫色で表示されます。 常設のプライバシーマスクは、常にXProtect Smart Clientにて表示され、除去することはできません。公的な場所や、監視が許可されていない場所といったビデオが決して必要とされない領域において、使うことができます。モーション検知は、常設のプライバシーマスクからは除外されます。 プライバシーマスクの範囲を、不透明か、ぼやけたレベルのどちらかに指定します。範囲設定は、ライブおよび録画ビデオの両方に適用されます。
除去可能なマスク	本タブのプレビューに、緑色で表示されます。 除去可能なプライバシーマスクは、ユーザーが十分な権限を持っていればXProtect Smart Clientで除去できます。デフォルト設定では、プライバシーマスクは30分間除去され、その後は自動的に適用されます。ユーザーがアクセス権を持つすべてのカメラのビデオでプライバシーマスクが除去されますのでご注意ください。 XProtect Smart Clientユーザーにプライバシーマスクを除去する権限がない場合、システムは除去権限を持つユーザーに除去の許可を依頼します。 プライバシーマスクの範囲を、不透明か、ぼやけたレベルのどちらかに指定します。範囲設定は、ライブおよび録画ビデオの両方に適用されます。
ぼかし	簡易的なぼやけたマスクから、完全な不透明のマスクに変更するには、スライダーを使用します。 デフォルト設定では、常設のプライバシーマスクの領域は無地(不透明)です。デフォルト設定では、除去可能なプライバシーマスクは、中程度にぼやけています。 クライアントユーザーが、違いを理解できるよう、常設のプライバシーマスクと除去可能なプライバシーマスクの外観の違いを伝えてください。

[ハードウェアプロパティ]ウィンドウ

システム内の各レコーディングサーバーに対して、ハードウェアを追加するための方法は、複数あります。

ハードウェアがNAT対応ルーターまたはファイアウォールの背後にある場合、別のポート番号を指定し、ルーター/ファイアウォールを構成して、ハードウェアのポートとIPアドレスにマッピングされるようにしなければならない場合があります。

ハードウェアを追加ウィザードを使用して、ネットワーク上でカメラおよびビデオエンコーダーなどのハードウェアを検知し、システムのレコーディングサーバーに追加します。ウィザードでは、Milestone Interconnect設定のリモートレコーディングサーバーも追加できます。ハードウェアは、一度に**1つのレコーディングサーバー**にのみ追加してください。

情報タブ(ハードウェア)

リモートサーバーの**[情報]**タブについては、「407ページの情報タブ(リモートサーバー)」を参照してください。

名前	説明
名前	名前を入力します。この名前は、システムやクライアントでハードウェアが列挙されるたびに使用されます。名前は一意である必要はありません。 ハードウェアの名前を変更すると、名前はManagement Clientで一括変更されます。
説明	ハードウェアの説明を入力します(オプション)。説明は、システム内の複数のリストに表示されます。たとえば、**概要**ペインでハードウェア名にマウスポインタを移動すると表示されます: 
モデル	ハードウェアモデルを規定します。
シリアル番号	メーカーが指定したハードウェアのシリアル番号。シリアル番号は、MACアドレスと同じであることがよくありますが、必ず一致するわけでもありません。
ドライバー	ハードウェアへの接続を処理しているドライバーを規定します。
IE	ハードウェア製造元のデフォルトホームページを開きます。このページはハードウェアの管理に使用します。
アドレス	ハードウェアのIPアドレスまたはホスト名。
MACアドレス	システムハードウェアのハードウェアメディアアクセスコントロール(MAC)アドレスを指定します。MACアドレスは、ネットワーク上の各ハードウェアを一意に識別する12文字の16進数です。
ファームウェアの	ハードウェアデバイスのファームウェアバージョン。システムに現在のバージョンを表示させるため、ファーム

名前	説明
バージョン:	ウェアをアップデートする際は毎回、アップデート後に **[ハードウェアデータの更新]** ウィザードを実行してください。
最後に変更したパスワード	**最後に変更したパスワード** フィールドには、最後にパスワードを変更した際のタイムスタンプが表示されます。ここでは、パスワードを変更したコンピュータの現地の時刻設定が反映されます。
ハードウェアデータの最終更新日:	ハードウェアデータの最終更新日時。

設定タブ(ハードウェア)

設定 タブで、ハードウェアの設定を確認または編集できます。

> **設定** タブの内容は、選択したハードウェアによって決定されます。このため、ハードウェアの種類によって内容が異なります。ハードウェアの種類によっては、**設定** タブの内容がまったく表示されないか、または読み取り専用の場合があります。

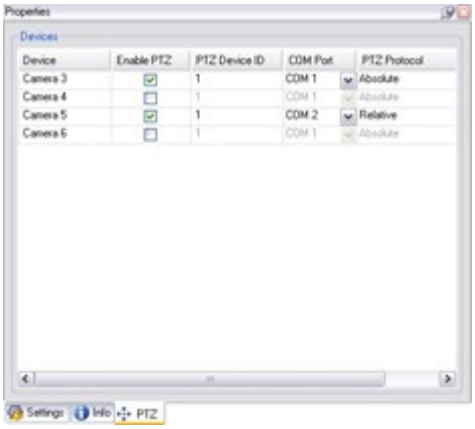
リモートサーバーの**[設定]**タブについては、「407ページの設定タブ(リモートサーバー) 」を参照してください。

PTZタブ(ビデオエンコーダー)

PTZタブでは、ビデオエンコーダーのPTZ(パン/チルト/ズーム) を有効にできます。選択されたデバイスがビデオエンコーダーであるか、ドライバーが非PTZおよびPTZカメラの両方をサポートしている場合に、このタブを使用できます。

PTZタブの各ビデオエンコーダーのチャネルで、PTZの使用を個別に有効にすると、ビデオエンコーダーに接続されたPTZカメラのPTZ機能を使用できます。

> 一部のビデオエンコーダーは、PTZカメラに対応していません。PTZカメラの使用をサポートするビデオエンコーダーでも、PTZカメラを使用する前に、設定が必要な場合があります。通常は、デバイスのIPアドレスで、ブラウザベースの設定インターフェースを使用して、追加ドライバーをインストールします。



2つのビデオエンコーダーチャネルに対してPTZが有効になっている状態の**PTZ**タブ

クライアントノード

クライアント(ノード)

この記事では、XProtect Smart Clientのオペレータ向けのユーザーインターフェイス、ならびにManagement Clientのシステム管理者向けのユーザーインターフェイスをカスタマイズする方法について説明します。

Smart Wall(クライアントノード)

Smart Wall プロパティ

情報タブ

Smart Wall定義の**情報タブ**では、Smart Wallプロパティを追加および編集できます。

名前	説明
名前	Smart Wall定義の名称。XProtect Smart ClientにSmart Wallビューグループ名として表示されます。
説明	Smart Wall定義の説明。説明はXProtect Management Client内部でのみ使用されます。
ステータステキスト	カメラのビューアイテムにカメラとシステムステータスの情報を表示します。
タイトルバーなし	ビデオウォールのすべてのビューアイテムでタイトルバーを非表示にします。
タイトルバー	ビデオウォールのすべてのビューアイテムにタイトルバーを表示します。

[プリセット]タブ

Smart Wall定義の**[プリセット]**タブでは、Smart Wallプリセット[1]を追加および編集できます。

名前	説明
新規追加	Smart Wall定義にプリセットを追加します。 プリセットの名前と説明を入力します。
編集	プリセットの名前と説明を編集します。
削除	プリセットを削除します。
実行	プリセットを使用するために設定されたSmart Wallモニターでプリセットを適用します。プリセットを自動適用するには、プリセットを使用するルールを作成する必要があります。

[レイアウト]タブ

Smart Wall定義の**レイアウト**タブで、ビデオウォール上の物理モニターの配置と一致するよう、モニターを配置します。このレイアウトはXProtect Smart Clientでも使用されます。

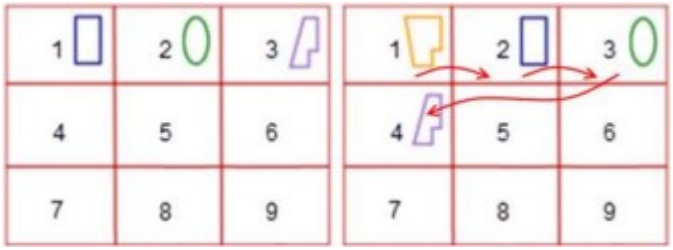
名前	説明
編集	モニターの配置を調整します。
移動	モニターを新しい位置に移動するには、モニターを選択して任意の位置にドラッグするか、あるいは矢印ボタンのいずれかをクリックして、モニターを選択した方向に移動します。
ズームボタン	Smart Wallレイアウトプレビューが拡大/縮小され、モニターを正しく配置できるようになります。
名前	モニターの名前。名前はXProtect Smart Clientに表示されます。
サイズ	ビデオウォールの物理モニターの寸法。
アスペクト比	ビデオウォールの物理モニターの高さおよび幅の比率。

[1]XProtect Smart Clientで1台以上のSmart Wallに対して事前に設定したレイアウトプリセットにより、ビデオウォールの各モニターに表示されるカメラとコンテンツのレイアウト(表示構成)が設定されます。

モニタープロパティ

情報タブ

プリセットに含まれるモニターの[情報]Smart Wallタブで、モニターを追加し、モニター設定を編集できます。

名前	説明
名前	モニターの名前。名前はXProtect Smart Clientに表示されます。
説明	モニターの説明。説明はXProtect Management Client内部でのみ使用されます。
サイズ	ビデオウォールの物理モニターの寸法。
アスペクト比	ビデオウォールの物理モニターの高さおよび幅の比率。
空のプリセット	Smart Wallで新しいXProtect Smart Clientプリセットがトリガーまたは選択された際に、プリセットレイアウトが空になっているモニターに何を表示するかを指定します。 • **保存**を選択すると、モニターの現在のコンテンツが維持されます。 • **クリア**を選択すると、すべてのコンテンツがクリアされ、モニターには何も表示されなくなります。
空のプリセットアイテム:	Smart Wallで新規XProtect Smart Clientプリセットがトリガまたは選択された場合に、空のプリセットアイテムに表示するコンテンツを設定します。 • **保存**を選択すると、レイアウトアイテムの現在のコンテンツが維持されます。 • **クリア**を選択すると、すべてのコンテンツがクリアされ、レイアウトアイテムには何も表示されなくなります。
要素の挿入	XProtect Smart Clientで表示した際に、モニターレイアウトにカメラをどのように挿入するかを指定します。 • **独立** - 対象のレイアウトアイテムのコンテンツのみが変更され、レイアウトの他のコンテンツは同じ状態に維持されます。 • **リンク済み** - レイアウトアイテムのコンテンツが左から右へ押されます。たとえば、この図例では、カメラがポジション1に挿入されると、ポジション1の前のカメラはポジション2に押され、ポジション2の前のカメラはポジション3に押される、というように続きます。 

[プリセット]タブ

Smart Wallプリセットのモニターの **[プリセット]** タブでは、選択したSmart Wallプリセットのモニターのビューのレイアウトとコンテンツを編集できます。

名前	説明
プリセット	選択したSmart Wall定義のSmart Wallプリセットのリスト。
編集	**編集**をクリックして、選択したモニターのレイアウトとコンテンツを編集します。 カメラをダブルクリックして削除します。 **クリア**をクリックすると、Smart Wallプリセットからモニターを除外する新しいレイアウトを定義します。これにより、プリセットによって制御されない他のコンテンツでモニターが使用できるようにSmart Wallなります。  をクリックして、モニターで使用するレイアウトを選択し、**[OK]** をクリックします。

Smart Clientのプロファイル(クライアントノード)

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

次のタブで、各Smart Clientプロファイルのプロパティを指定できます。Management Clientのユーザーが変更できないように、必要に応じて、XProtect Smart Clientで設定をロックできます。

Smart Client プロファイルを作成または編集するには、**クライアント**を展開し、**Smart Client プロファイル**を選択します。

情報 タブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
情報	名前と説明、既存のプロファイルの優先度、プロファイルを使用する役割の概要。 ユーザーがそれぞれにSmart Clientプロファイルが割り当てられた複数の役割に属している場合、Smart Clientプロファイルの取得が最優先されます。

全般タブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
一般	メニュー設定の表示/非表示、および最小化と最大化、ログイン/ログアウト、起動、タイムアウト、情報、メッセージオプション、XProtect Smart Clientの特定のタブの有効化/無効化などの設定。 **カメラエラーメッセージ**、**サーバーエラーメッセージ**および**ライブビデオエラーメッセージ**の設定では、これらのエラーメッセージをオーバーレイで表示するか、オーバーレイ付きの黒い画像で表示するか、または非表示にするかを設定することができます。 カメラのライブビデオが停止しているときは、**ライブビデオの停止メッセージ**がXProtect Smart Clientに表示されます。たとえば、接続されているにもかかわらず、カメラが画像を送信しなくなった場合などです。 ⚠ カメラのエラーメッセージを**非表示**にすると、カメラへの接続が失われたことをオペレータが見落としてしまうリスクが生じます。 **検索中カメラを許可**設定を使用すると、XProtect Smart Clientでオペレータが検索に追加できるカメラの数を制御できます。カメラの上限を設定すると、システムの過負荷防止に役立ちます。 **オンラインヘルプ**設定を使用すると、XProtect Smart Clientのヘルプシステムが無効になります。 **ビデオチュートリアル**設定を使用すると、XProtect Smart Clientの**ビデオチュートリアル**ボタンが無効になります。このボタンを押すとビデオチュートリアルページに移動します。https://www.milestonesys.com/support/help-yourself/video-tutorials/

詳細タブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
詳細	最大デコードスレッド、インターレースの解除、および時間帯の設定などの詳細設定。 **最大デコードスレッド**は、ビデオストリームのデコードで使用されるデコードスレッドの数を制御します。これによって、ライブおよび再生モードで、マルチコアコンピュータのパフォーマンスを改善できます。実際のパフォーマンスの改善は、ビデオストリームによって異なります。この設定は、H.264/H.265のような高度にコード化された高解像度ビデオストリームを使用している場合に主に適用されます。この場合、大幅なパフォーマンスの改善が見られる可能性があります。たとえば、JPEGまたはMPEG-4などを使用している場合は効果が低くなります。

タブ	説明
	インターレースの解除により、ビデオはノンインターレース形式に変換されます。インターレースは、画面で画像をどのように更新するかを決定します。まず画像の奇数ラインをスキャンして画像を更新し、次に偶数のラインをスキャンしていきます。スキャン時に処理する情報が少なくなるため、より高速のリフレッシュレートが可能になります。ただし、インターレースによってちらつきが発生したり、画像のラインの半分だけが変化する場合があります。 **アダプティブストリーミング**を使用すれば、表示アイテムによって要求された解像度に最も近い解像度がXProtect Smart Clientによって自動的に選択されます。これによってCPUとGPUの負荷が軽減するため、結果としてコンピュータのデコード能力とパフォーマンスが上がります。このためには、解像度の異なるライブビデオストリームでマルチストリーミングを設定する必要があります。マルチストリーミングの管理を参照してください。アダプティブストリーミングでは、ライブおよび再生モードの両方を摘要できます。再生モードでは、アダプティブストリーミングはアダプティブ再生と呼ばれます。アダプティブ再生は2つのストリームをレコーディングに設定することを要求します。ライブモードでのアダプティブストリーミングおよびアダプティブ再生用のストリームを追加する方法の詳細は 221ページのストリームの追加 を参照してください。

ライブタブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
ライブ	ライブモード/その他のライブ機能、カメラ再生、カメラオーバーレイボタン、バウンディングボックス、ライブ関連のMIPプラグインの可用性。

再生タブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
再生	再生モード/その他の再生機能、印刷レポートのレイアウト、個別再生、ブックマーク、バウンディングボックス、再生関連のMIPプラグインの可用性。

セットアップタブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
セットアップ	一般設定/ペイン/ボタン、設定関連のMIPプラグイン、マップの編集権限とライブビデオバッファの編集権限の可用性。

[エクスポート] タブ(Smart Clientプロフィール)

このタブからは、以下のプロパティを指定できます:

タブ	説明
エクスポート	パス、プライバシーマスク、ビデオ、静止画像フォーマット、ビデオおよび静止画像のエクスポート時に含まれる内容、XProtect Smart Client - Playerのエクスポートフォーマットなど。

タイムラインタブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
タイムライン	音声を含めるかどうか、時間とモーションの表示/非表示、および再生ギャップを処理する方法。 他のソースから、追加のデータや追加のマーカーを表示するかどうかも選択できます。

アクセスコントロールタブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
アクセスコントロール	イベントによって起動された際に、XProtect Smart Client画面にアクセスリクエスト通知を表示するかどうかを選択します。

アラームマネージャータブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
アラームマネージャ	以下を指定します: • アラームのデスクトップ通知は、XProtect Smart Clientがインストールされているコンピュータに表示する必要があります。通知はXProtect Smart Clientの実行中にのみ(最小化されていても)表示されます アラームのデスクトップ通知は、アラームに特定の優先度(**中**や**高**など)が割り当てられている場合にのみ表示されます。どのアラーム優先度で通知が起動されるかを設定するには、**アラーム > アラームデータ設定 > アラームデータレベル**に移動します。必要なアラーム優先度ごとに**デスクトップ通知を有効化**チェックボックスを選択します。アラームデータ設定(アラームノード)を参照してください。 • アラームは、XProtect Smart Clientがインストールされているコンピュータで音声通知を再生する必要があります。通知はXProtect Smart Clientの実行中にのみ(最小化されていても)再生されます アラームの音声通知は、サウンドがアラームに関連付けられている場合にのみ再生されます。サウンドをアラームに関連付けるには、**アラーム > アラームデータ設定 > アラームデータレベル**に移動します。必要なアラームの優先度ごとに、アラームに関連付けるサウンドを選択します。アラームデータ設定(アラームノード)を参照してください。

スマートマップタブ(Smart Clientプロファイル)

このタブからは、以下のプロパティを指定できます:

タブ	説明
スマートマップ	スマートマップ機能の設定を行います。 以下を指定できます。 • Milestone Map Serviceを地理的背景として利用できるかどうか • OpenStreetMapsを地理的背景として利用できるかどうか

タブ	説明
	• XProtect Smart Clientは、ユーザーがスマートマップにカスタムオーバーレイを追加すると自動的に場所を作成します。 どれくらいの頻度でスマートマップ関連のデータがコンピュータから削除されるようにするかも指定できます。クライアント側では、XProtect Smart Clientでスマートマップがよりすばやく表示されよう、マップデータがお使いのコンピュータのキャッシュに保存されます。これにより、時間が経つにつれて、コンピュータの速度が低下する可能性があります。 コーチングはGoogle Mapsには適用されません。 Bing MapsまたはGoogle Mapsを地理的背景として使用したい場合は、Bing Maps APIキーを入力するか、GoogleからMaps Static APIキーを取得します。

Management Clientのプロファイル(クライアントノード)

この機能が利用できるのはXProtect Corporateのみです。

情報 タブ(Management Clientプロファイル)

情報 タブでは、Management Clientプロファイルについて、以下を設定できます:

コンポーネント	要件
名前	Management Clientプロファイルの名前を入力します。
優先度	上矢印や下矢印キーを使用してManagement Clientプロファイルの優先度を設定します。
説明	プロファイルの説明を入力します。これはオプションです。
プロファイルManagement Clientを使用する役割	このフィールドは、Management Clientプロファイルに関連付けられた役割を表示します。これは編集できません。

プロファイルタブ(Management Clientプロファイル)

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

プロファイルタブで、ManagementClientのユーザーインターフェースで、以下の要素の表示を有効または無効にすることができます:

ナビゲーション

このセクションで、Management Clientプロファイルと関連付けられている管理者ユーザーが、**ナビゲーション**ペインにあるさまざまな特徴や機能を表示できるようにするかどうかを決めます。

ナビゲーションエレメント	説明
基本	Management Clientプロファイルと関連付けられている管理者ユーザーが、**ライセンス情報**および**サイト情報**を表示できるようにします。
リモート接続サービス	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、**Axis One-click**カメラの**接続**を表示できるようにします。
サーバー	Management Clientプロファイルと関連付けられている管理者ユーザーが、**レコーディングサーバー**および**フェールオーバーサーバー**を表示できるようにします。
デバイス	Management Clientプロファイルと関連付けられている管理者ユーザーが、**カメラ**、**マイク**、**スピーカー**、**メタデータ**、**入力**および**出力**を表示できるようにします。
Client	Management Clientプロファイルと関連付けられている管理者ユーザーが、**Smart Wall**、**ビューグループ**、**Smart Clientプロファイル**、**Management Clientプロファイル**および**Matrix**を表示できるようにします。
ルールとイベント	Management Clientプロファイルと関連付けられている管理者ユーザーが、**ルール**、**時間プロファイル**、**通知プロファイル**、**ユーザー定義イベント**、**アナリティクスイベント**および**ジェネリックイベント**を表示できるようにします。
セキュリティ	Management Clientプロファイルと関連付けられている管理者ユーザーが、**役割**および**基本ユーザー**を表示できるようにします。

ナビゲーションエレメント	説明
システムダッシュボード	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、**[システムモニター]**、**[システムモニターしきい値]**、**[エビデンスロック]**、**[現在のタスク]**、**[設定レポート]** を表示できるようにします。
サーバーログ	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、システムログ、監査ログおよびルール起動ログを表示できるようにします。
アクセスコントロール	Management Clientプロファイルと関連付けられている管理者ユーザーが、システムにアクセスコントロールシステム統合またはプラグインを追加している場合、**アクセスコントロール**機能を表示できるようにします。

詳細

このセクションで、Management Clientプロファイルと関連付けられている管理者ユーザーが、たとえばカメラの**設定**タブまたは**録画**タブなど、さまざまなタブで特定のデバイスチャネルを表示できるかどうかを決めます。

デバイスチャネル	説明
カメラ	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、一部または全部のカメラ関連の設定やタブを表示できるようにします。
マイク	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、一部または全部のマイク関連の設定やタブを表示できるようにします。
スピーカー	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、一部または全部のスピーカー関連の設定やタブを表示できるようにします。
メタデータ	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、一部または全部のメタデータ関連の設定やタブを表示できるようにします。
入力	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、一部または全部の入力関連の設定やタブを表示できるようにします。
出力	Management Clientプロファイルと関連付けられているシステム管理者ユーザーが、一部または全部の出力関連の設定やタブを表示できるようにします。

ツールメニュー

このセクションで、Management Clientプロファイルと関連付けられている管理者ユーザーが、**ツール**メニューの一部である要素を表示できるようにします。

ツールメニューのオプション	説明
登録済みサービス	Management Clientプロファイルと関連付けられている管理者ユーザーが、**登録済みサービス**を表示できるようにします。
有効な役割	Management Clientプロファイルと関連付けられている管理者ユーザーが、**有効な役割**を表示できるようにします。
オプション	Management Clientプロファイルと関連付けられている管理者ユーザーが、**オプション**を表示できるようにします。

フェデレーテッドサイト

Management Clientこのセクションでは、プロファイルと関連付けられている管理者ユーザーが、[フェデレーテッドサイト**階層**]ペインを表示できるかどうかを決めます。

ルールとイベントノード

ルール(ルールノードとイベントノード)

システムには多くのデフォルトルールが設定されており、何も設定しなくても基本的な機能が使用できます。必要に応じてデフォルトルールを無効化または修正できます。デフォルトルールを修正または無効化すると、システムが希望通りに動作しなくなる場合があります。また、映像または音声のシステムへの自動配信が保証されなくなる場合があります。

デフォルトルール	説明
PTZが完了したらプリセットへ移動	PTZカメラを手動で操作した後、各デフォルトのプリセット位置に移動することを確認します。このルールはデフォルトでは無効になっています。 ルールを有効にした場合でも、ルールが動作するには、関連するPTZカメラでデフォルトプリセット位置を定義する必要があります。この操作は**プリセット**タブで行います。
要求が	外部リクエストが発生すると、ビデオが自動的に録画されます。

デフォルトルール	説明
あれば音声を再生します。	リクエストは、常にお使いのシステムに外部的に統合されているシステムによって起動されます。また、ルールは主に外部システムまたはプラグインのインテグレータによって使用されます。
ブックマーク記録	オペレータがXProtect Smart Clientにブックマークを設定すると、ビデオが自動的に録画されます。これは関連するカメラの録画が有効になっていることが前提条件です。デフォルトでは録画が有効になっています。 このルールのデフォルトの録画時間は、ブックマークが設定された時点の3秒前、およびブックマークが設定された時点から30秒後です。ルールでデフォルトの録画時間を編集できます。録画タブで設定したプレバッファはプリレコーディング時間以上にする必要があることに留意してください。
モーション記録	カメラでモーションが検知される限り、関連するカメラの記録が有効になっていれば、ビデオが録画されることを確認します。デフォルトでは記録は有効になっています。 デフォルトルールでは、検知されたモーションに基づいて記録を指定しますが、1つ以上のカメラで個々のカメラの記録が無効になっている場合には、システムがビデオを記録することを保証するものではありません。記録が有効になっている場合でも、記録の品質は個々のカメラの記録設定の影響を受ける場合があることに留意してください。
リクエスト記録	関連するカメラの録画が有効になっていることを前提条件として、外部リクエストが発生するとビデオの録画が自動的に開始されることを確認します。デフォルトでは録画が有効になっています。 リクエストは、常にお使いのシステムに外部的に統合されているシステムによって起動されます。また、ルールは主に外部システムまたはプラグインのインテグレータによって使用されます。
音声配信開始	すべての接続済みマイクとスピーカーからの音声配信がシステムに自動配信されることを保証します。 このデフォルトルールにより、システムのインストール時に接続されたマイクとスピーカーの音声配信に即時にアクセスできます。ただし、記録設定は個別に指定する必要があるため、音声が記録されることを保証するものではありません。
配信開始	すべての接続済みカメラからの映像配信がシステムに自動配信されることを保証します。 このデフォルトルールにより、システムのインストール時に接続されたカメラの映像配信に即時にアクセスできます。ただし、カメラの記録設定は個別に指定する必要があるため、ビデオが録画されることを保証するものではありません。
メタデータ配信開始	すべての接続済みカメラからのデータ配信がシステムに自動配信されることを保証します。 このデフォルトルールにより、システムのインストール時に接続されたカメラのデータ配信に即時にアクセスできます。ただし、カメラの記録設定は個別に指定する必要があるため、データが記録されることを保証するものではありません。

デフォルトルール	説明
アクセスリクエスト通知の表示	すべてのアクセスコントロールイベントが「アクセスリクエスト」に必ず分類されるようにします。こうすることで、XProtect Smart Clientプロファイルで通知機能が無効になっていない限り、Smart Clientでアクセスリクエスト通知のポップアップが表示されます。

デフォルトルールの再作成

誤ってデフォルトのルールを削除した場合には、次の内容を入力することで再作成できます。

デフォルトルール	入力するテキスト
PTZが完了したときにプリセットへ移動する	すべてのカメラからPTZ手動セッションを中止したときにアクションを実行します。 イベントが発生したデバイスでデフォルトのプリセットに即時に移動します。
要求があれば音声を再生します。	外部からの音声メッセージ再生要求があればアクションを実行します。 デバイス上でメタデータからの音声メッセージを優先度1のメタデータから再生します
ブックマーク記録	すべてのカメラ、すべてのマイク、すべてのスピーカーからブックマーク参照が要求された時にアクションを実行すると、イベントが発生したデバイスで3秒前から録画が開始されます。 アクションを30秒間実行した後に、録画をすぐに停止します。
モーション記録	モーション時にすべてのカメラからの開始アクションを実行すると、イベントが発生したデバイスで3秒前から記録を開始します。 モーション時にすべてのカメラからの終了アクションを実行すると、3秒後に記録が停止します。
リクエスト記録	外部からの録画開始リクエスト時にアクションを実行すると、メタデータからデバイスの録画をただちに開始します。 外部から記録の停止を要求した際に停止アクションを実行し、録画がただちに停止されます。
音声配信開始	アクションをある時間間隔で実行し、常にすべてのマイク、すべてのスピーカーで配信を開始します。 時間間隔が終了すると、アクションを実行し、配信をただちに停止します。
配信開始	アクションをある時間間隔で実行し、常にすべてのカメラで映像配信を開始します。 時間間隔が終了すると、アクションを実行し、配信をただちに停止します。

デフォルトルール	入力するテキスト
メタデータ配信開始	アクションをある時間間隔で実行し、常にすべてのメタデータで映像配信を開始します。 時間間隔が終了すると、アクションを実行し、配信をただちに停止します。
アクセスリクエスト通知の表示	システム[+ ユニット]からアクセスリクエスト(アクセスコントロールカテゴリ)に対してアクションを実行する 組込みアクセスリクエスト通知の表示

通知プロファイル(ルールノードとイベントノード)

通知プロファイルの以下のプロパティを指定します。

コンポーネント	要件
名前	通知プロファイルの分かりやすい名前を入力します。名前は、ルール作成中に通知プロファイルを選択したときに表示されます。
説明(オプション)	通知プロファイルの説明を入力します。説明は、概要ペインの**通知プロファイル**リストの通知プロファイルにマウスポインタを合わせると表示されます。
受信者	通知プロファイルのEメール通知を送信する宛先となるEメールアドレスを入力します。2つ以上のEメールアドレスを入力する場合は、セミコロンでアドレスを区切ってください。例: aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc
件名	Eメールによる通知で、件名として表示するテキストを入力します。 件名とメッセージテキストフィールドには、**デバイス名**などのシステム変数を挿入できます。変数を挿入するには、フィールド下のボックスの必要な変数リンクをクリックします。
メッセージテキスト	Eメールによる通知で、本文として表示するテキストを入力します。メッセージテキストの他に、Eメール通知の本文には、以下の情報が自動的に追加されます。 • Eメールによる通知が起動された原因 • 添付静止画像またはAVIビデオクリップのソース
Eメール間の時	各Eメール通知を送信する間隔の最小時間(秒) を指定します。例:

コンポーネント	要件
間	• 120を指定した場合、2分経過する前にルールにより通知プロファイルが再び起動された場合でも、各Eメール通知は最低2分経過するまで送信されません • 0を指定すると、通知プロファイルがルールで起動されるたびにEメール通知が送信されます。これによりEメール通知が大量に送信される可能性があります。したがって、値に0を使用する場合、ルールが頻繁に起動される通知プロファイルを送信する際は注意が必要です
画像の数	各通知プロファイルのEメール通知に添付する最大静止画像数を指定します。デフォルトの画像数は5個です。
画像間の時間(ミリ秒):	添付画像に提示された記録間のミリ秒数を指定します。例:デフォルトは500ミリ秒で、添付画像は1/2秒間隔で記録を表示します。
イベント前の時間(秒)	この設定はAVIファイルの開始を指定する際に使用します。デフォルトでは、AVIファイルには通知プロファイルが起動される2秒前からの録画が含まれます。これは、必要な秒数に変更できます。
イベント後の時間(秒)	この設定はAVIファイルの終了を指定する際に使用します。デフォルトでは、AVIファイルは通知プロファイルが起動された4秒後に終了します。これは、必要な秒数に変更できます。
フレームレート	AVIファイルに含める秒当たりのフレーム数を指定します。デフォルトは1秒当り5フレームです。フレームレートが高ければ高いほど、画質とAVIファイルサイズが大きくなります。
Eメールに画像を埋め込む	選択すると(デフォルト)、画像がEメール通知の本文に挿入されます。選択しなければ、画像は添付ファイルとしてEメール通知に添付されます。

イベント概要

ルールの管理ウィザードでイベントベースのルールを追加する場合、さまざまなイベントタイプから選択できます。概要を把握するために、現在の状況に応じて、選択可能なイベントがグループに一覧表示されます。

ハードウェア

一部のハードウェアでは、モーション検知などのイベントを独自に作成できます。これらはイベントとして使用できますが、システムで使用する前にハードウェア上に設定する必要があります。すべてのタイプのカメラで攻撃や温度変化を検知できるとは限らないため、一部のハードウェアで表示されているイベントのみを使用できます。

ハードウェア - 設定可能イベント

ハードウェアから設定可能なイベントは、デバイスドライバーから自動的にインポートされます。つまり、ハードウェアによって異なるため、ここでは説明していません。設定可能イベントは、ハードウェアの**イベント**タブで設定して、システムに追加されるまでトリガーされません。設定可能イベントの中には、カメラ(ハードウェア) 自体を設定する必要があるものもあります。

ハードウェア - 事前定義イベント

イベント	説明
通信エラー(ハードウェア)	ハードウェアへの接続が失われたときに発生します。
通信が開始しました(ハードウェア)	ハードウェアとの通信が正常に確立されたときに発生します。
通信が停止しました(ハードウェア)	ハードウェアとの通信が正常に停止したときに発生します。

デバイス - 設定可能イベント:

デバイスから設定可能なイベントは、デバイスドライバーから自動的にインポートされます。つまり、デバイスによって異なるため、ここでは説明していません。設定可能イベントは、デバイスの**イベント**タブで設定して、システムに追加されるまで起動されません。

デバイス - 事前定義イベント

イベント	説明
ブックマーク参照が要求された	クライアントにおいて、ライブモード中にブックマークが作成された時に発生します。また、デフォルトのブックマーク録画ルールを使用するための要件です。
通信エラー(デバイス)	デバイスへの接続が失われたとき、およびデバイスとの通信の試みが発生し、試みが失敗したときに発生します。
通信開始(デバイス)	デバイスとの通信が正常に確立されたときに発生します。
通信停	デバイスとの通信が正常に停止したときに発生します。

イベント	説明
止(デバイス)	
エビデンスロック変更	デバイスのエビデンスロックが、クライアントユーザーによって、またはMIP SDKを介して変更された時に発生します。
エビデンスロック	デバイスのエビデンスロックが、クライアントユーザーによって、またはMIP SDKを介して作成された時に発生します。
エビデンスロック解除	デバイスのエビデンスロックが、クライアントユーザーによって、またはMIP SDKを介して削除された時に発生します。
フィードオーバーフロー開始	レコーディングサーバーが受信したデータを指定された速度で処理できず、一部の録画が強制的に破棄される場合に、フィードオーバーフロー(メディアのオーバーフロー)が発生します。 サーバーが正常な場合、通常、フィードオーバーフローはディスク書き込み速度が遅いために発生します。書き込むデータ量を減らすか、ストレージシステムのパフォーマンスを改善することで解決できます。カメラのフレームレート、解像度、または画質を下げることで、データ書き込み量を減らすことができますが、これにより画質が落ちる場合があります。録画品質を下げたくない場合は、代わりに、追加のドライブを設置して負荷を分散するか、高速ディスクまたはコントローラを設置して、ストレージシステムのパフォーマンスを改善します。 このイベントは、録画フレームレートの低下などの問題を回避するアクションをトリガーするために使用できます。
フィードオーバーフロー停止	フィードオーバーフロー(455ページのフィードオーバーフロー開始を参照)が終了すると発生します。
ライブクライアントフィード要求	クライアントユーザーがデバイスからライブストリームを要求するときに発生します。 このイベントは、例えばクライアントユーザーがライブフィードを表示させるために必要な権限を持っていない場合や、ライブフィードが何らかの理由で停止した場合など、クライアントのユーザーのリクエストが最終的に失敗するとしても、リクエスト時に発生します。
ライブクライアントフィード終了	クライアントユーザーがデバイスからのライブストリームを要求しなくなったときに発生します。

イベント	説明
手動録画開始	クライアントユーザーがカメラの録画セッションを開始したときに発生します。 イベントは、デバイスがルールアクションを通してすでに録画している場合でもトリガーされます。
手動録画停止	クライアントユーザーがカメラの録画セッションを停止したときに発生します。 ルールシステムも録画セッションを開始した場合は、手動の録画が停止した後でも録画が続けられます。
マーク付きデータ(エビデンスロックまたはブックマーク)参照要求	エビデンスロックが、クライアントによって、またはMIP SDKを介して再生モードで作成された時に発生します。 ルールで使用できるイベントが作成されます。
モーション開始	システムがカメラから受信したビデオでモーションを検知したときに発生します。 このタイプのイベントでは、イベントがリンクされるカメラのシステムのモーション検知を有効にする必要があります。 システムのモーション検知に加え、カメラ自体でモーションを検知して**モーション開始(ハードウェア)**イベントをトリガーできるカメラもありますが、カメラハードウェアやシステムの設定によって異なります。454ページのハードウェア - 設定可能イベントも参照してください。
モーション停止	受信したビデオでモーションが検知されなくなったときに発生します。456ページのモーション開始も参照してください。 このタイプのイベントでは、イベントがリンクされるカメラのシステムのモーション検知を有効にする必要があります。 システムのモーション検知に加え、カメラ自体でモーションを検知してモーション停止(ハードウェア)イベントをトリガーできるカメラもありますが、カメラハードウェアやシステムの設定によって異なります。454ページのハードウェア - 設定可能イベントも参照してください。
出力アクティベート	デバイスの外部出力ポートが有効になったときに発生します。 このタイプのイベントでは、システムの1つ以上のデバイスが出力ポートに対応している必要があります。
出力変更	デバイスの外部出力ポートのステータスが変更されたときに発生します。 このタイプのイベントでは、システムの1つ以上のデバイスが出力ポートに対応している必要があります。
出力非アクティベー	デバイスの外部出力ポートが無効になったときに発生します。 このタイプのイベントでは、システムの1つ以上のデバイスが出力ポートに対応している必要があります。

イベント	説明
ト	
PTZ手動セッション開始	(スケジュール済みパトロールまたはイベントによる自動トリガーに基づくPTZセッションとは異なり) 手動で操作したPTZセッションがカメラで開始されたときに発生します。 このタイプのイベントでは、イベントがリンクされているカメラがPTZカメラである必要があります。
PTZ手動セッション停止	(スケジュール済みパトロールまたはイベントによる自動トリガーに基づくPTZセッションとは異なり) 手動で操作したPTZセッションがカメラで停止されたときに発生します。 このタイプのイベントでは、イベントがリンクされているカメラがPTZカメラである必要があります。
録画開始	録画が開始したときに発生します。手動の録画が開始された場合は、別のイベントが発生します。
録画停止	録画が停止したときに発生します。手動の録画が停止された場合は、別のイベントが発生します。
設定変更	デバイスの設定が正常に変更されたときに発生します。
設定変更エラー	デバイスの設定変更が試みられ、試みが失敗したときに発生します。

外部イベント - 事前定義イベント

イベント	説明
音声メッセージ再生要求	音声メッセージがMIP SDKを通じてリクエストされたときにアクティベートされます。 MIP SDKによって、サードパーティーのベンダーは、システム用のカスタムプラグイン(例えば、外部アクセスコントロールシステムまたは同様の機能などとの統合) を開発できます。
録画開始要求	録画の開始がMIP SDK経由で要求されたときに有効になります。 MIP SDKによって、サードパーティーのベンダーは、システム用のカスタムプラグイン(例えば、外部アクセスコントロールシステムまたは同様の機能などとの統合) を開発できます。
録画停止要求	録画の停止がMIP SDK経由で要求されたときに有効になります。 MIP SDKによって、サードパーティーのベンダーは、システム用のカスタムプラグイン(例えば、外部アクセスコントロールシステムまたは同様の機能などとの統合) を開発できます。

外部イベント- ジェネリックイベント

ジェネリックイベントでは、シンプルな文字列をIPネットワーク経由でシステムに送信し、システムのアクションをトリガーできます。ジェネリックイベントの目的は、可能な限り多くの外部ソースがシステムと相互作用できるようにすることです。

外部イベント- ユーザー定義イベント

各システムに合うようカスタムメイドしたイベントも選択することができます。このようなユーザー定義イベントは、以下で使用できます。

- クライアントユーザーが手動でイベントを起動しながら、クライアントのライブビデオを閲覧できるようにする
- その他多数の目的。例えば、特定のデータタイプをデバイスから受信したときに発生するユーザー定義イベントを作成することができます

76ページのユーザー定義のイベント(説明付き) も参照してください。

レコーディングサーバー

イベント	説明
アーカイブ利用可能	レコーディング サーバーのアーカイブが利用不可になっていた後に利用できるようになった場合に発生します。458ページのアーカイブ利用不可 も参照してください。
アーカイブ利用不可	ネットワークドライブにあるアーカイブへの接続が失われた場合等、レコーディングサーバーのアーカイブが使用できなくなったときに発生します。このような場合、録画をアーカイブできません。 イベントを使って、Eメール通知が自動的に組織内の関連するスタッフに送信されるようにするために、アラームまたは通知プロファイルをトリガーすることができます。
アーカイブ未完了	次の予定が開始する際、最後のアーカイブラウンドでレコーディングサーバーのアーカイブが完了していないときに発生します。
設定保存サイズになる前に、録画データベースを削除	データベースのサイズが制限に達するより先に、保存期間が制限に達した場合に発生します。
設定保存期間になる前に、録画データベースを削除	保存期間が制限に達するより先に、データのサイズが制限に達した場合に発生します。
データベースディスク満杯 - 自動アーカイブ中	データベースディスクが満杯のときに発生します。データベースディスクは、ディスクの残り容量が5MB未満になると満杯となります。

イベント	説明
	空き容量が5GB未満になった場合、データベースで最も古いデータは必ず自動アーカイブされます(または、次のアーカイブが定義されていない場合は削除されます) 。
データベースディスク満杯 - 削除中	データベースディスクが満杯か、1GB未満の空き容量しかない場合に発生します。次のアーカイブが定義されていても、データは削除されます。データベースには、必ず250MBの空き容量が必要です。この制限に達した場合(データが十分速やかに削除されていない場合) 、十分な空き容量が確保されるまで、それ以上データベースにはデータが書き込まれません。このため、データベースの実際の最大サイズは、指定したギガバイト数より5GB少なくなります。
データベース満杯 - 自動アーカイブ中	レコーディングサーバーのアーカイブが満杯になり、ストレージのアーカイブに自動アーカイブする必要があるときに発生します。
データベース修復	データベースが破損した場合に発生します。その場合、システムは自動的に以下の2つのデータベース修復方法を試行します。素早い修復と完全な修復。
データベースストレージ利用可能	レコーディングサーバーのストレージが利用不可になっていた後に利用できるようになった場合に発生します。459ページのデータベースストレージ利用不可も参照してください。 例えば、**データベースストレージ利用不可**イベントにより停止された場合、このイベントを使って録画を開始することができます。
データベースストレージ利用不可	ネットワークドライブにあるストレージへの接続が失われた場合など、レコーディングサーバーのストレージが利用不可になったときに発生します。このような場合、録画をアーカイブできません。 イベントを使って、Eメール通知が自動的に組織内の担当者に送信されるようにするために、録画を停止して通知プロファイルまたはアラームをトリガーできます。
フェールオーバー暗号化通信エラー	フェールオーバーサーバーと監視中のレコーディングサーバーとの間でSSL通信エラーが生じた時に発生します。
フェールオーバー開始	レコーディングサーバーからフェールオーバーレコーディングサーバーに切り替わるときに発生します。「フェールオーバーサーバー(ノード) 」も参照してください。
フェールオーバー停止	レコーディングサーバーが再び利用可能になり、フェールオーバーレコーディングサーバーから引き継ぐことができるようになると発生します。

システムモニターイベント

システムモニターイベントは、**システムモニターしきい値**ノードで設定されたしきい値を超過するとトリガーされます。278ページのハードウェアの現在の状態を表示し、必要に応じてトラブルシューティングを実行も参照してください。

この機能は、Data Collectorサービスが実行中であることが必須です。

システムモニター - サーバー

イベント	説明
CPU使用率重大	CPU使用率が、CPU重大しきい値を上回った時に発生します。
CPU使用率正常	CPU使用率が、CPU警告しきい値を下回った時に発生します。
CPU使用率警告	CPU使用率がCPU警告しきい値を上回った、あるいはCPU重大しきい値を下回った時に発生します。
メモリ使用率重大	メモリ使用率が、メモリ重大しきい値を上回った時に発生します。
メモリ使用率正常	メモリ使用率が、メモリ警告しきい値を下回った時に発生します。
メモリ使用率警告	メモリ使用率がメモリ警告しきい値を上回った、あるいはメモリ重大しきい値を下回った時に発生します。
NVIDIAデコード重大	NVIDIAデコード使用値が、NVIDIAデコード重大しきい値を上回った時に発生します。
NVIDIAデコード正常	NVIDIAデコード使用値が、NVIDIAデコード警告しきい値を下回った時に発生します。
NVIDIAデコード警告	NVIDIAデコード使用率がNVIDIAデコード警告しきい値を上回った、あるいはNVIDIAデコード重大しきい値を下回った時に発生します。
NVIDIAメモリ重大	NVIDIAメモリ使用率が、NVIDIAメモリ重大しきい値を上回った時に発生します。
NVIDIAメモリ正常	NVIDIAメモリ使用率が、NVIDIAメモリ警告しきい値を下回った時に発生します。
NVIDIAメモリ警告	NVIDIAメモリ使用率がNVIDIAメモリ警告しきい値を上回った、あるいはNVIDIAメモリ重大しきい値を下回った時に発生します。
NVIDIAレンダリング重大	NVIDIAレンダリング使用率が、NVIDIAレンダリング重大しきい値を上回った時に発生します。
NVIDIAレンダリング正常	NVIDIAレンダリング使用率が、NVIDIAレンダリング警告しきい値を下回った時に発生します。
NVIDIAレンダリング警告	NVIDIAレンダリング使用率がNVIDIAレンダリング警告しきい値を上回った、あるいはNVIDIAレンダリング重大しきい値を下回った時に発生します。

イベント	説明
使用可能なサービス重大	サーバーサービスが実行を停止した時に発生します。 このイベントには、しきい値は存在しません。
使用可能なサービス正常	サーバーサービスステータスが、実行に変更になった時に発生します。 このイベントには、しきい値は存在しません。

システムモニター - カメラ

イベント	説明
ライブFPS重大	ライブFPS使用率が、ライブFPS重大しきい値を下回った時に発生します。
ライブFPS正常	ライブFPS使用率が、ライブFPS警告しきい値を上回った時に発生します。
ライブFPS警告	ライブFPS使用率がライブFPS警告しきい値を下回った、あるいはライブFPS重大しきい値を上回った時に発生します。
録画FPS重大	録画FPS使用率が、録画FPS重大しきい値を下回った時に発生します。
録画FPS正常	録画FPS使用率が、録画FPS警告しきい値を上回った時に発生します。
録画FPS警告	録画FPS使用率が録画FPS警告しきい値を下回った、あるいは録画FPS重大しきい値を上回った時に発生します。
使用領域重大	特定のカメラによる録画のための使用領域が使用領域重大しきい値を上回った時に発生します。
使用領域正常	特定のカメラによる録画のための使用領域が使用領域警告しきい値を下回った時に発生します。
使用領域警告	特定のカメラによる録画のための使用領域が使用領域警告しきい値を上回った、あるいは使用領域重大しきい値を下回った時に発生します。

システムモニター - ディスク

イベント	説明
空き領域重大	ディスク空き領域が、空き領域重大しきい値を上回った時に発生します
空き領域正常	ディスク空き領域が、空き領域警告しきい値を下回った時に発生します
空き領域警告	ディスク空き領域が空き領域警告しきい値を上回った、あるいは空き領域重大しきい値を下回った時に発生します。

システムモニター - ストレージ

イベント	説明
保存期間重大	システムがストレージが保存期間重大しきい値よりも早く満杯になると予想した時に発生します。例えば、ビデオストリームからのデータが、予想していたよりも早くストレージに保存されている場合などです。
保存期間正常	システムがストレージが保存期間警告しきい値よりも遅く満杯になると予想した時に発生します。例えば、ビデオストリームからのデータが、予想通りの速さでストレージに保存されている場合などです。
保存期間警告	システムが、ストレージが保存期間警告しきい値よりも早く、あるいは保存期間重大しきい値よりも遅く、満杯になるとシステムが予想した時に発生します。例えば、ビデオストリームからのデータが、モーションを録画するように設定されたカメラからより多くのモーション検知があったことにより予想していたよりも早くストレージに保存されている場合などです。

その他

イベント	説明
自動ライセンスアクティベーション失敗	自動ライセンスアクティベーションが失敗した時に発生します。 このイベントにはしきい値は存在しません。
定期的なパスワード変更開始	定期的なパスワード変更が開始した時に発生します。

イベント	説明
定期的なパスワード変更完了	定期的なパスワード変更がエラーなしで完了した時に発生します。
定期的なパスワード変更がエラーで終了	定期的なパスワード変更がエラーで終了した時に発生します。

XProtect拡張機能や統合機能からのイベント

例えば、ルールシステムでは、XProtect拡張機能および統合機能からのイベントを使用できます。

- アナリティクスイベントは、ルールシステムでも使用できます

アクションと停止アクション

ルールの管理ウィザードには、ルールを作成するための一連のアクション/停止アクションが用意されています。システムインストールがXProtect拡張機能またはベンダー固有のプラグインを使用している場合は、追加のアクションを使用できることがあります。該当する場合は、アクションタイプごとに、対応する停止アクションの情報もリストされています。

ルールの管理ウィザード

アクション	説明
<デバイス>で録画を開始	録画を開始し、選択されたデバイスからのデータベースへのデータの保存を開始します。 このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、以下を指定するように指示されます。 録画の開始時期。これは、アクションを起こすデバイス上で、直ちに開始されるか、またはトリガーイベント前/トリガータイムインターバル開始前に数秒待機後、開始されます。 このタイプのアクションでは、アクションがリンクされているデバイス上で録画が有効になっている必要があります。プレバッファが該当するデバイスで有効になっている場合のみ、イベントまたは時間間隔の前からデータを保存できます。**録画**タブで、デバイスの録画を有効にし、プレバッファ設定を指定します。 **終了アクションが必要**：このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。**レコーディング停止**。 この終了アクションがない場合、録画が無制限に続く可能性があります。また、その他の終了アクションを指定することもできます。
<デバイス>でフィードを開始	デバイスからシステムにデータフィードを開始します。デバイスからのフィードが開始されると、データ

アクション	説明
	はデバイスからシステムに転送されます。この場合、データタイプに従ってライブ表示と録画が可能です。 このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、フィードを開始するデバイスを指定するように指示されます。システムには、フィードが常にすべてのカメラで開始されることを保証するデフォルトのルールが含まれています。 **終了アクションが必要**: このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。**フィードの停止**。 また、その他の終了アクションを指定することもできます。 強制終了アクションの**フィードの停止**を使用してデバイスからのフィードを停止すると、データはデバイスからシステムに転送されません。この場合、たとえば、ビデオのライブ表示と録画ができなくなります。ただし、フィードを停止したデバイスは、レコーディングサーバーとの通信が維持されます。 ⚠ また、デバイスを手動で無効にしたときとは異なり、デバイスからのフィードをルールにより自動的に再開することが可能です。このタイプのアクションにより、選択されたデバイスのデータフィードにアクセスできますが、録画設定は個別に指定する必要があるため、データが録画されることを保証するものではありません。
<Smart Wall>を<プリセット>に設定	XProtect Smart Wallを選択したプリセットに設定します。**Smart Wallプリセット**タブでプリセットを指定します。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<Smart Wall><モニター>を<カメラ>を表示するよう設定	特定のXProtect Smart Wallモニターに、このサイトまたはMilestone Federated Architectureで設定されている子サイト上で選択されているカメラからのライブビデオを表示するよう設定します。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<Smart Wall> <モニター>を設定して、テキスト<メッセージ>を表示	特定のXProtect Smart Wallモニターを設定し、最大200文字のユーザー定義のテキストメッセージを表示します。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<Smart Wall>モニ	特定のカメラのビデオの表示を停止します。

アクション	説明
タ―<モニタ―>から<カメラ>を削除	**強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<デバイス>のライブフレームレートを設定	カメラのデフォルトのフレームレートの代わりに、選択したカメラからライブビデオをシステムで表示するときに使用する特定のフレームレートを設定します。この操作は**設定**タブで行います。 このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、設定するフレームレートとデバイスを指定するように指示されます。必ず、指定するフレームレートが該当するカメラで利用できることを確認してください。 **終了アクションが必要**: このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。**デフォルトのライブフレームレートを復元します**。 この終了アクションがない場合、デフォルトのフレームレートが復元されない可能性があります。また、その他の終了アクションを指定することもできます。
<デバイス>の録画のフレームレートを設定	カメラのデフォルトのレコーディングフレームレートではなく、データベースの選択済みカメラから録画済みビデオを保存するときに使用する特定のフレームレートを設定します。 このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、設定するレコーディングフレームレートとカメラを指定するように指示されます。 レコーディングフレームレートは、各フレームがJPEG画像に圧縮されるビデオコーデックであるJPEGでのみ指定できます。また、このタイプのアクションでは、アクションがリンクされているカメラ上で録画が有効になっている必要があります。**録画**タブで、カメラの録画を有効にします。指定できる最大フレームレートは、カメラタイプおよび選択された画像の解像度によって異なります。 **終了アクションが必要**: このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。**デフォルトのレコーディングフレームレートを復元します**。 この終了アクションがない場合、デフォルトのレコーディングフレームレートが復元されない可能性があります。また、その他の終了アクションを指定することもできます。
<デバイス>にあるMPEG-4/H.264/H.265のすべてのフレームのレコーディングフレームレートを設定	データベースで選択されたカメラから録画済みビデオを保存するときに、キーフレームだけではなく、すべてのフレームを録画するために使用するフレームレートを設定します。**録画**タブで、キーフレームのみの録画機能を有効にします。 このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、アクションを適用するデバイスを選択するように指示されます。 MPEG-4/H.264/H.265のキーフレームレコーディングのみを有効にできます。また、このタイプのアクションでは、アクションがリンクされているカメラ上で録画が有効になっている必要があります。**録画**タブで、カメラの録画を有効にします。

アクション	説明
	終了アクションが必要：このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。 **MPEG-4/H.264/H.265のキーフレームのデフォルトのレコーディングフレームレートを復元** この終了アクションがない場合、デフォルト設定が永久に復元されない可能性があります。また、その他の終了アクションを指定することもできます。
PTZ優先度<優先度>で<プロファイル>を使用して<デバイス>でのパトロールを開始	特定の優先度が設定された特定のPTZカメラで、特定のパトロール設定に従って、PTZパトロールを開始します。ここで、プリセット位置、タイミング設定などを含め、パトロールの実行方法を正確に定義します。 システムが古いバージョンのシステムからアップグレードされた場合、古い値(**非常に低い**、**低**、**中**、**高**および**非常に高い**)は次のように解釈されます。 • 非常に低い = 1000 • 低 = 2000 • 中 = 3000 • 高 = 4000 • 非常に高い = 5000 このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、パトロール設定を選択するように指示されます。1つデバイスでは1つのパトロール設定のみを選択できます。複数のパトロール設定を選択することはできません。 このタイプのアクションでは、アクションがリンクされているデバイスがPTZデバイスであることが必要です。 デバイスに1つ以上のパトロール設定が定義されている必要があります。**パトロール**タブで、PTZカメラのパトロール設定を定義します。 **終了アクションが必要**：このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。 **パトロールを停止します** この終了アクションがない場合、パトロールが停止しない可能性があります。また、その他の終了アクションを指定することもできます。
<デバイス>でのパト	PTZパトロールの一時停止 このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、

アクション	説明
ロールの一時停止	パトロールを一時停止するデバイスを指定するように指示されます。 このタイプのアクションでは、アクションがリンクされているデバイスがPTZデバイスであることが必要です。 デバイスに1つ以上のパトロール設定が定義されている必要があります。**パトロール**タブで、PTZカメラのパトロール設定を定義します。 **終了アクションが必要**: このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。**パトロールを再開します** この終了アクションがない場合、パトロールが無制限に一時停止したままになる可能性があります。また、その他の終了アクションを指定することもできます。
PTZ優先度<優先度>で<デバイス>を<プリセット>位置に移動	特定のカメラを特定のプリセット位置に移動します。ただし、必ず優先度に従います。このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、プリセット位置を選択するように指示されます。1つのカメラで選択できるのは、1つのプリセット位置のみです。複数のプリセット位置を選択することはできません。 このタイプのアクションでは、アクションがリンクされているデバイスがPTZデバイスであることが必要です。 このアクションでは、デバイスに1つ以上のプリセット位置が定義されている必要があります。**プリセット**タブで、PTZカメラのプリセット位置を定義します。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
PTZ優先度<優先度>で<デバイス>をデフォルトのプリセットに移動	1つ以上のカメラを該当するプリセット位置に移動します。ただし、必ず優先度に従います。このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、アクションを適用するデバイスを選択するように指示されます。

アクション	説明
	このタイプのアクションでは、アクションがリンクされているデバイスがPTZデバイスであることが必要です。 このアクションでは、デバイスに1つ以上のプリセット位置が定義されている必要があります。**プリセット**タブで、PTZカメラのプリセット位置を定義します。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
デバイス出力を<ステータス>に設定	デバイスの出力を特定のステータス(有効化または無効化)に設定します。このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、設定するステータスとデバイスを指定するように指示されます。 このタイプのアクションでは、アクションがリンクされるデバイスはそれぞれ、1つ以上の外部出力装置が出力ポートに接続されていなければなりません。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
ブックマークを<デバイス>で作成	選択されたデバイスからライブストリーミングまたは録画のブックマークを作成します。ブックマークを使用すると、特定のイベントまたは期間を簡単に再追跡できます。ブックマーク設定は、**オプション**ダイアログボックスで制御されます。このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、ブックマークの詳細を指定し、デバイスを選択するように指示されます。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<デバイス>で音声<メッセージ>を<優先度>で再生	イベントによってトリガーされた選択したデバイスで音声メッセージを再生します。デバイスは主にスピーカーとカメラです。 このタイプのアクションでは、**ツール > オプション > 音声メッセージ**タブでシステムにメッセージがアップロードされている必要があります。 同じイベントにさらにルールを作成したり、各デバイスへ異なるメッセージを送信することも可能です。シーケンスを制御する優先度はルールおよび**スピーチ**タブの役割のためのデバイスに設定されたものです: • メッセージを再生しながら同じ優先度の別のメッセージを同じスピーカーに送信する場合、最初のメッセージが完了してから第2のメッセージが始まります • メッセージを再生しながら優先度の高い別のメッセージを同じスピーカーに送信する場合、最初のメッセージを中断し直ちに第2のメッセージが始まります

アクション	説明
通知を<プロファイル>に送信	特定の通知プロファイルを使用して通知を送信します。このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、通知プロファイルとプリアラーム画像を含めるデバイスを選択するように指示されます。1つの通知プロファイルのみを選択できます。複数の通知プロファイルを選択することはできません。1つの通知プロファイルには複数の受信PCを含めることができます。 同じイベントにさらにルールを作成したり、各通知プロファイルへ異なる通知を送信することも可能です。**ルール**リストのルールを右クリックすることで、ルールの内容をコピーして再利用できます。 このタイプのアクションでは、1つ以上の通知プロファイルを設定する必要があります。**画像を含む**オプションが該当する通知プロファイルで有効になっている場合のみ、プリアラーム画像が含まれます。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
新しい<ログエントリ>を追加	ルールログにエントリを作成します。このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、ログエントリのテキストを指定するように指示されます。ログテキストを指定すると、**$DeviceName$**、**$EventName$**などの変数を簡単にログメッセージに挿入できます。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<デバイス>のプラグインを開始	1つ以上のプラグインを開始します。このタイプのアクションを選択すると、**ルールの管理**ウィザードが開き、必要なプラグインとプラグインを起動するデバイスを選択するよう指示されます。 このタイプのアクションでは、システムで1つ以上のプラグインがインストールされていることが必要です。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<デバイス>のプラグインを停止	1つ以上のプラグインを停止します。このタイプのアクションを選択すると、**[ルールの管理]**ウィザードにより、必要なプラグインと、プラグインを停止するデバイスを選択するように指示されます。 このタイプのアクションでは、システムで1つ以上のプラグインがインストールされていることが必要です。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
新しい設定を<デバイス>に適用	1つ以上のデバイスのデバイス設定を変更します。このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、必要なデバイスを選択するように指示され、指定したデバイス関連の設定を定義できます。

アクション	説明
	複数のデバイスで設定を定義する場合は、指定したデバイスのすべてで使用可能な設定のみを変更できます。 **例**:アクションがデバイス1およびデバイス2にリンクするように指定します。デバイス1には、設定A、B、およびCがあり、デバイス2には設定B、C、およびDがあります。この場合、両方のデバイスで使用可能な設定BおよびCのみを変更できます。 **強制停止アクションなし**:このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
Matrixを<デバイス>を表示するよう設定	選択したカメラのビデオが、Matrixによってトリガーされたビデオの表示が可能なコンピュータ(XProtect Smart Clientがインストールされているコンピュータなど)に表示されるようにします。 このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、Matrix受信PCと、選択されたMatrix受信PCでビデオを表示する1つ以上のデバイスを選択するように指示されます。 Matrixこのタイプのアクションでは、受信PCを一度に1つのみ選択できます。選択されたデバイスのビデオを複数のMatrix受信者で表示するには、各目的のMatrix受信者のルールを作成するか、XProtect Smart Wall機能を使用する必要があります。**ルール**リストのルールを右クリックすることで、ルールの内容をコピーして再利用できます。このようにして、類似したルールをゼロから作成せずに済みます。 Matrix受信PC自体の設定の一部として、ユーザーはMatrix通信に必要なポート番号とパスワードを指定する必要があります。ユーザーがこの情報にアクセスできることを確認してください。一般的に、ユーザーは許可されたホストのIPアドレス(Matrixでトリガーされるビデオの表示に関するコマンドが受信されるホスト)も定義する必要があります。この場合、ユーザーはマネジメントサーバー(または使用されるルーターまたはファイアウォール)のIPアドレスも把握していなければなりません。
SNMPトラップの送信	選択されたデバイスのイベントを録画する小さいメッセージを作成します。SNMPトラップのテキストは自動生成されるため、カスタマイズできません。これにはソースタイプとイベントが発生したデバイス名が含まれています。 **強制停止アクションなし**:このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<デバイス>からリモート録画を取得して保存	選択した(リモート録画をサポートする)デバイスから、指定した期間の前後とトリガーイベント後のリモート録画を取得し保存します。

アクション	説明
	このルールは、**接続が復旧したときに自動的にリモート録画を取得する**設定とは関係ありません。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<デバイス>から<開始時間と終了時間>間のリモート録画を取得して保存	選択されたデバイス(リモート録画に対応するデバイス) からリモート録画を取得して保存します。 このルールは、**接続が復旧したときに自動的にリモート録画を取得する**設定とは関係ありません。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
添付画像の保存	画像を受信しましたイベントから画像を受信(カメラからSMTPメール経由で送信) したとき、今後使用できるように画像を保存します。今後、他のイベントでもこのアクションをトリガーすることができます。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<アーカイブ> のアーカイブを有効化	1つ以上のアーカイブでアーカイブを開始します。このタイプのアクションを選択すると、**ルールの管理**ウィザードにより、必要なアーカイブを選択するように指示されます。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<サイト>で<ユーザー定義イベント>をトリガー	通常はMilestone Federated Architectureに関連していますが、単一サイト設定でも使用可能です。このルールは、サイトでユーザー定義イベントをトリガーするために使用されます。通常は、フェデレーテッド階層内のリモートサイトです。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。
<アクセスリクエスト通知>を表示	イベントをトリガーする条件に一致した場合に、XProtect Smart Clientの画面にアクセスリクエスト通知のポップアップウィンドウが表示されます。一般に、アクセスリクエスト通知は関連するアクセスコントロールコマンドやカメラの操作に対して設定されるため、Milestoneは、このアクションに対するイベントをトリガーするためにアクセスコントロールイベントを使用することをお勧めします。 このタイプのアクションでは、システムで1つ以上のアクセスコントロールプラグインが使用可能であることが必要です。 **強制停止アクションなし**: このタイプのアクションでは、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。

アクション	説明
ハードウェアデバイスのパスワードを変更	選択したハードウェアデバイスのパスワードを、特定のハードウェアデバイスのパスワード要件にもとづいてランダム生成されたパスワードに変更します。対応ハードウェアデバイスのリストは、「ハードウェアの検索」で確認できます。 このアクションは、**<繰り返し時間>へのアクションを実行**ルールタイプを使用してルールを設定した場合にのみ実行できます。 アクションに対して以下のイベントを利用できます: • 462ページの定期的なパスワード変更開始 • 463ページの定期的なパスワード変更完了 • 463ページの定期的なパスワード変更がエラーで終了 このタイプのアクションには、停止アクションがありません。 このアクションの進行状況は**[現在のタスク]**ノードで確認できます。詳細については、「276ページのレコーディングサーバーで実行中のタスクを表示」を参照してください。 アクションの結果を表示するには、**[システムログ]**タブで**[サーバーログ]**ノードに移動します。詳細については、「367ページのサーバーログタブ(オプション)」を参照してください。 詳細については、「システムログ(タブ)」を参照してください。

アナリティクスイベントをテストする(プロパティ)

アナリティクスイベントの要件をテストする場合は、4つの条件を確認し、エラーがある場合はエラーの説明と解決策を示すウィンドウが表示されます。

条件	説明	エラーメッセージと解決策
保存した変更	イベントが新しい場合は保存されますか? または、イベント名を変更した場合は、変更内容は保存されますか?	**アナリティクスイベントをテストする前に変更を保存してください**。解決策/説明:変更を[保存]します。
アナリティクスイベント	アナリティクスイベント機能は有効ですか?	**アナリティクスイベントは有効ではありません**。解決策/説明:アナリティクスイベント機能を有効にしてください。これを実行するためには、**[ツール]** > **[オプション]** > **[アナリティクスイベント]**をクリックし、**[有効]**チェックボックス

条件	説明	エラーメッセージと解決策
が有効です		を選択します。
許可されるアドレス	イベントを送信するマシンのIPアドレスまたはホスト名は許可(アナリティクスイベントアドレスリストに登録)されていますか?	**Analytic Eventサービスに対して許可されているアドレスとして、ローカルホスト名を追加する必要があります**。解決策/説明:を追加します。許可されるIPアドレスまたはホスト名のアナリティクスイベントアドレスリストに、使用しているマシン **ローカル ホスト名の解決中にエラーがありました**。解決策/説明:マシンのIPアドレスまたはホスト名が見つからないか無効です。
アナリティクスイベントを送信する	テストイベントはイベントサーバーに正常に送信されましたか?	下のテーブルを参照してください。

各ステップは失敗❌または成功✔.

条件**アナリティクスイベントの送信**に対するエラーメッセージと解決策:

エラーメッセージ	解決策
イベントサーバーが見つかりません。	イベントサーバーが登録済みサーバーのリストにありません。
イベントサーバーへの接続中にエラーが発生しました	指定されたポートでイベントサーバーに接続できません。一般的には、ネットワークの問題か、Event Serverサービスが停止しているため、エラーが発生します。
アナリティクスイベントの送信エラーが発生しました	イベントサーバーサービスへの接続は確立しますが、イベントを送信できません。一般的には、タイムアウトなどのネットワークの問題のため、エラーが発生します。
イベントサーバーからの応答の受信中にエラーが発生しました	イベントサーバーにイベントが送信されましたが、応答が受信されません。一般的には、ネットワークの問題またはポートがビジー状態のため、エラーが発生します。 通常は`ProgramData\Milestone\XProtect Event Server\Logs\`にあるイベントサーバーログを確認してください。
イベントサーバーには不明なアナリティクスイベントです	Event Serverサービスがイベントを認識しません。エラーが発生する最も可能性の高い理由は、イベントまたはイベントの変更が保存されていないことです。

エラーメッセージ	解決策
イベントサーバーが無効なアナリティクスイベントを受信しました	イベントのフォーマットが正しくありません。
送信者はイベントサーバーによって承認されていません。	認証されたリスト上にIP アドレスまたはホスト名あなたのマシンがないケースがあり得ます。
イベントサーバーの内部エラーが発生しました	イベントサーバーエラー。 通常はProgramData\Milestone\XProtect Event Server\Logs\にあるイベントサーバーログを確認してください。
イベントサーバーが無効な応答を受信しました。	応答は無効です。ポートがビジー状態か、ネットワークに問題がある可能性があります。 通常はProgramData\Milestone\XProtect Event Server\Logs\にあるイベントサーバーログを確認してください。
イベントサーバーから不明な応答を受信しました	応答は有効ですが、理解不能です。エラーが発生しているのは、ネットワークの問題またはポートがビジー状態のためである可能性があります。 通常はProgramData\Milestone\XProtect Event Server\Logs\にあるイベントサーバーログを確認してください。
予期しないエラーが発生しました	Milestoneサポートにお問い合わせください。

ジェネリックイベントとデータソース(プロパティ)

この機能は、XProtectイベントサーバーがインストールされている場合のみ動作します。

ジェネリックイベント(プロパティ)

コンポーネント	要件
名前	ジェネリックイベントの一意の名前。名前は、ユーザー定義イベント、アナリティクスイベント等すべてのタイプのイベントに対して一意のものでなければなりません。
有効	ジェネリックイベントはデフォルトでは有効になっています。イベントを無効にするにはチェックボックスを解除します。

コンポーネント	要件
条件式	データパッケージの分析時にシステムが参照すべき表現。次の演算子を使用できます。 • ( ): 関連項を論理ユニットとして同時に処理するために使用されます。分析で特定の処理順序を強制するために使用されます **例**: 検索条件「(User001 OR Door053)AND Sunday」を使用する場合、括弧内の2つの項が先に処理され、その結果が文字列の最後の部分と結合されます。つまり、システムはまずUser001またはDoor053という項を含むパッケージを参照し、その後に結果を取得し、Sundayという項を含むパッケージを検索します。 • AND: AND演算子では、AND演算子の両側の項が存在する必要があることを指定します **例**: 検索条件「User001 AND Door053 AND Sunday」は、User001、Door053およびSundayのすべてが表現に含まれている場合のみ結果を返します。用語のいずれかまたは2つが存在するだけでは足りません。語句をANDで結合すればするほど、返される結果は少なくなります。 • OR OR演算子により、いずれか1つの項が存在する必要があることを指定します **例**: 検索条件「User001 OR Door053 OR Sunday」は、User001、Door053またはSundayのいずれかが含まれている結果を返します。語句をORで結合すればするほど、返される結果は多くなります。
条件式のタイプ	受信したデータパッケージを分析する時に特定のシステムがあるべき状態を示します。オプションは以下の通りです。 • **検索**: イベントを発生させるには、受信したパッケージに、**[表現]**フィールドで指定したテキストが含まれていなければなりませんが、他の内容も含まれている可能性があります。 **例**: 受信したパッケージにUser001およびDoor053が含まれるよう指定した場合、受信したパッケージにUser001、Door053、Sundayが含まれる場合、受信したパッケージに2つの必要な語句が含まれるため、イベントが起動されます。 • **一致**: イベントが発生するためには、受信したデータパッケージに**[表現]**フィールドに指定したものと全く同一のテキストだけが存在するものとし、他のものは含まれません。 • **通常の表現**: イベントが発生するためには、受信したデータパッケージ内に**[表現]**フィールドで指定した特定のパターンが存在する必要があります。 **検索**または**一致**から**正規表現**に切り替えると、**表現**フィールドのテキストは、自動的に正規表現に変換されます。
優先度	0(最高優先度) ~ 999999(最低優先度)の間の数値で優先度を指定してください。 同じデータパッケージが異なるイベントで分析される場合があります。各イベントに優先度を割り当てる機能により、受信したパッケージが複数のイベントの基準に一致したときに、どのイベントを起動するか管理することができます。

コンポーネント	要件
	システムがTCPおよびUDPパッケージを受信した場合、そのパケットの分析が、最高優先度のイベントで開始されます。これにより、パッケージが複数のイベントの基準と一致する場合、最高優先度のイベントのみが起動されます。パッケージが同じ優先度で複数のイベントの基準と一致した場合、たとえば、優先度999のイベントが2つある場合、その優先度のすべてのイベントが起動されます。
表現がイベント文字列と一致するかチェック:	**表現]** フィールドに入力した表現に対してイベント文字列をテストします。

Webhook(ルールとイベントノード)

Webhook ノードでは、Webhookのエンドポイントを作成、編集、削除できます。

Webhookを作成および編集するときは、次のフィールドを使用できます。

フィールド	説明
名前	Webhookのエンドポイントに固有の名前を入力します。 Webhook名を空にすることはできません。
アドレス	イベントデータを送信する先のWebサーバーのURLまたはアプリケーションURL Webサーバーの が更新された場合は、Webhookのノードで**URL**Webhookを更新する必要があります。 安全でないネットワーク(オープンインターネットなど) を通して**HTTP**を使用すると、すべてのイベントがプレーンテキストで公開されます。
トークン	HTTP POST のソースを検証して、他のアプリケーションとの安全な通信を支援するために使用されるトークンを入力します。 通信ができるだけ安全になるようトークンを使用することはオプションですが、推奨されます。
APIバージョン	Webhookの機能に使用されるWebhookのプラグインとAPIのバージョン

セキュリティノード

役割(セキュリティノード)

情報タブ(役割)

> 使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

役割の**[情報]** タブでは、以下を設定できます。

名前	説明
名前	ロールの名前を入力します。
説明	ロールの説明を入力します。
Management Clientプロファイル	役割と関連付けるManagement Clientのプロファイルを選択します。 これを、デフォルトの**管理者**の役割に適用することはできません。 マネジメントサーバーでセキュリティを管理する権限が必要です。
Smart Clientプロファイル	役割と関連付けるSmart Clientのプロファイルを選択します。 マネジメントサーバーでセキュリティを管理する権限が必要です。
既定の時間設定	役割と関連付けるデフォルトの時間設定を選択します。 これを、デフォルトの**管理者**の役割に適用することはできません。
エビデンスロックプロファイル	役割と関連付けるエビデンスロックのプロファイルを選択します。
Smart Client時間プロファイル内でのログイン	この役割に関連付けられているXProtect Smart Clientユーザーがログインできる時間プロファイルを選択します。 有効期限切れの期間にXProtect Smart Clientユーザーがログインすると、自動的にログオ

名前	説明
	フになります。 これを、デフォルトの**管理者**の役割に適用することはできません。
Smart Clientログインを許可	チェックボックスを選択すると、この役割に関連付けられているユーザーがXProtect Smart Clientへログインすることができます。 デフォルトでは、Smart Clientへのアクセスは許可されていません。チェックボックスをオフにするとXProtect Smart Clientへのアクセスを拒否します。
XProtect Mobileクライアントへのログイン許可	チェックボックスを選択すると、このロールに関連付けられているユーザーがXProtect Mobileクライアントにログインすることができます。 XProtect Mobileクライアントへのアクセスは、デフォルトでは許可されていません。チェックボックスをオフにするとXProtect Mobileクライアントへのアクセスを拒否します。
XProtect Web Clientログインを許可	チェックボックスを選択すると、この役割に関連付けられているユーザーがXProtect Web Clientへログインすることができます。 デフォルトでは、XProtect Web Clientへのアクセスは許可されていません。チェックボックスをオフにするとXProtect Web Clientへのアクセスを拒否します。
ログイン認証が必要	チェックボックスを選択して、ログイン認証を役割と関連付けます。つまり、ユーザーがログインする際には、XProtect Smart ClientまたはManagement Clientは第2認証が必要となることを意味します(通常は、スーパーユーザーまたはマネージャーが認証)。 管理者がユーザーを認証できるようにするため、**[セキュリティ全般]**タブでマネジメントサーバーの**[ユーザーを認証]**権限を設定します。 これを、デフォルトの**管理者**の役割に適用することはできません。
PTZセッション中にユーザーを匿名にする	チェックボックスを非表示にすると、この役割に関連付けられたユーザーがPTZセッションを制御するときに、これらのユーザーの名前を非表示にします。

ユーザーおよびグループタブ(役割)

[ユーザーとグループ]タブで、ユーザーとグループを役割に割り当てます(「272ページのユーザーおよびグループの役割からの削除、役割への割り当て」を参照)。Windowsユーザーとグループ、または基本ユーザーを割り当てることができます(「60ページのユーザー(説明付き)」を参照)。

外部IDP(役割)

外部IDPタブでは、既存のクレームを確認し、新しいクレームを役割に追加できます。

名前	説明
外部IDP	外部IDPの名前。
クレーム名	外部IDPで定義されている変数。
クレームの値	適切な役割をユーザーに割り当てるために使用されるクレームの値(グループ名など)。

セキュリティ全般タブ(役割)

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

[セキュリティ全般]タブで、役割に対して権限全般を設定します。システムで利用できる各コンポーネントに**[許可]**または**[拒否]**を設定し、役割のアクセス権限を設定します。ある役割からのコンポーネントへのアクセスが「拒否」に設定された場合、この役割が割り当てられたユーザーの**[セキュリティ全般]**タブにはそのコンポーネントが表示されません。

オーバーオールセキュリティタブは、無料版のXProtect Essential+では利用できません。

他のXProtect Corporate VMS製品よりも多くのアクセス権限をXProtectに対して設定できます。これは、すべての製品で、XProtect Corporate、XProtect Smart Client、またはXProtect Web Clientクライアントを使用する役割の全体的な権限を設定できるのに対し、XProtect Mobileでは異なる管理者権限の設定しかできないためです。

セキュリティ全般の設定は、現在のサイトだけに適用されます。

ユーザーに複数の役割を関連付ける場合、ひとつの役割のセキュリティ設定で**[拒否]**を選択し、別の役割で**[許可]**を選択すると、**[拒否]**権限が**[許可]**権限を無効にします。

以下の説明には、該当する役割に対して**[許可]**を選択した場合に、異なるシステムコンポーネントの個別の権限に起こることが示されています。XProtect Corporateを使用する場合、それぞれのシステムコンポーネントでどの設定が使用できないかをお使いのシステムで**のみ**表示できます。

すべてのシステムコンポーネントや機能について、完全なシステムシステム管理者は**許可**または**拒否**のチェックボックスを使用して、役割に関するセキュリティ権限を設定できます。ここで設定するセキュリティ権限は、システムコンポーネントや機能の全体の設定に関するものです。したがって、例えば、**カメラ**で**[拒否]**チェックボックスを選択すると、システムに追加されるすべて

のカメラがそのロールでは使用できなくなります。対照的に、**許可**チェックボックスを選択すると、この役割ではシステムに追加されるすべてのカメラを表示できるようになります。カメラでの**許可**または**拒否**の選択は、**デバイス**タブでのカメラの設定となり、特定の役割に対してすべてのカメラが使用可能または使用不能となるように、**セキュリティ全般**タブでの選択が継承されます。

個別のカメラ、あるいはそれに類似するカメラに対してセキュリティ権限を設定したい場合、**セキュリティ全般**タブでシステムコンポーネントあるいは機能に対し、**権限全般の設定はしない**ならば、関連するシステムコンポーネント、あるいは機能のタブで個々の権限を設定することが可能です。

以下の説明は、MIP SDK経由で設定できる権限にも適用されます。

XProtect Corporateから他の製品のいずれかに基本ライセンスを切り替える場合、XProtect Corporateに対してのみ利用できるセキュリティ権限をすべて削除したことを確認してください。これらの権限を削除しないと、切り替えは完了できません。

マネジメントサーバー

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
接続	ユーザーがManagement Serverに接続できるようになります。 この権限はデフォルトで有効となっています。 メンテナンスプロセス時には役割に対する接続権限を一時的に無効にし、後でシステムにアクセスを再適用できます。 システムへのアクセスを許可するには、この権限を選択する必要があります。
読み取り	この権限は、システムで設定された認証情報など機密データへのアクセス権を含む、XProtect VMS, への重大なアクセス権を提供する極めて高い管理者権限です。

セキュリティ権限	説明
	広範な機能にアクセスする権限を有効に設定します。対象となる機能： • 以下を伴うログインManagement Client • 現在のタスクのリスト • サーバーログ また、以下に対するアクセス権も有効にします： • リモート接続サービス • Smart Clientプロファイル • Management Clientプロファイル • Matrix • 時間プロファイル • 登録済みサーバーおよびサービス登録API また、この権限は、クライアントに対して一部の機密情報を公開します。 • 設定された外部IDPの資格情報 • 対象の場所にあるすべてのカメラの認証情報、IPアドレス、その他の情報 - 対象の場所：XProtect VMS • 設定されたメールサーバーの認証情報 • 設定されたマトリックスの認証情報 • 相互接続機能に対して設定された認証情報 • ライセンスのアクティベーションに対して設定された認証情報 この権限は、のユーザーに対して認証情報を公開しませんXProtect VMS。これには基本ユーザー、Windowsのユーザー、外部IDPのユーザーが含まれます。
編集	広範な機能でデータを変更する権限を有効に設定します。対象となる機能： • オプション • ライセンス管理 また、ユーザーが以下を作成、削除、編集できるようにします。 • リモート接続サービス • デバイスグループ • Matrix

セキュリティ権限	説明
	• 時間プロファイル • 通知設定 • 登録済みサーバー  レコーディングサーバーでネットワークを設定する際、ローカルIPの範囲を設定する権限を有効に設定します。
システムモニター	システムモニターのデータを表示する権限を有効に設定します。
ステータスAPI	レコーディングサーバーに存在するステータスAPIでクエリを実行する権限を有効に設定します。つまり、この権限が有効に設定された役割には、レコーディングサーバーに存在するアイテムのステータスを読み取るためのアクセス権があります。
フェデレーテッドサイト階層を管理	フェデレーテッドサイト階層にある他のサイトに現在のサイトを追加および分離する権限を有効に設定します。  この権限を子サイトでのみ有効にしても、ユーザーはサイトを親サイトから分離できます。
バックアップ設定	システムのバックアップ復元機能を使用して、システム構成のバックアップを作成する権限を有効に設定します。
ユーザーを認証	XProtect Smart ClientまたはManagement Clientで2回目のログインを要求された場合、ユーザーを認証する権限を有効に設定します。役割にログイン認証が必要となるかどうかは**情報**タブで指定します。
セキュリティを管理	マネジメントサーバーの権限を管理する権限を有効に設定します。 また、ユーザーが以下の機能を作成、削除、編集できるようにします。 • 役割 • 基本ユーザー • Smart Clientプロファイル • Management Clientプロファイル

レコーディングサーバー

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
編集	レコーディングサーバーでプロパティを編集する権限を有効に設定します(ただしマネジメントサーバーでの編集権限が必要なネットワークの構成設定を除きます)。
削除	レコーディングサーバーを削除する権限を有効に設定します。これを行うには、ユーザーに以下の削除権限を与える必要があります: • ハードウェアをレコーディングサーバーに追加している場合は、ハードウェアのセキュリティグループ レコーディングサーバーにあるデバイスにエビデンスロックが含まれているなら、レコーディングサーバーを削除できるのはオフラインである場合だけです。
ハードウェアの管理	レコーディングサーバーにハードウェアを追加する権限を有効に設定します。
ストレージを管理	レコーディングサーバーでストレージコンテナを管理する権限(すなわち、ストレージコンテナを作成、削除、移動、空にする権限)を有効に設定します。
セキュリティを管理	レコーディングサーバーのセキュリティ権限を管理する権限を有効に設定します。

フェールオーバーサーバー

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	Management Clientでフェイルオーバーサーバーを表示し、フェイルオーバーサーバーにアクセスする権限を有効に設定します。
編集	Management Clientでフェイルオーバーサーバーを作成、更新、削除、移動、有効/無効に設定する権限を有効に設定します。
セキュリティを管理	フェイルオーバーサーバーのセキュリティ権限を管理する権限を有効に設定します。

モバイルサーバー

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	Management Clientでモバイルサーバーを表示し、モバイルサーバーにアクセスする権限を有効に設定します。
編集	Management Clientでモバイルサーバーを編集および削除する権限を有効に設定します。
セキュリティを管理	モバイルサーバーのセキュリティ権限を管理する権限を有効に設定します。
作成	モバイルサーバーをシステムに追加する権限を有効に設定します。

ハードウェア

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
編集	ハードウェアのプロパティを編集する権限を有効に設定します。
削除	ハードウェアを削除する権限を有効に設定します。 いずれかのハードウェアデバイスにエビデンスロックが含まれているなら、ハードウェアを削除できるのはレコーディングサーバーがオフラインである場合だけです。
ドライバーコマンド	ドライバに特殊コマンドを送信する権限を有効に設定し、そうすることで、デバイス自体の機能や設定を管理します。 [ドライバコマンド] 権限は、クライアント上の特別に開発されたMIPプラグインのみを対象とした権限です。標準構成タスクは制御できません。
パスワードを見る	[ハードウェアの編集] ダイアログボックスで、ハードウェアデバイスのパスワードを表示する権限を有効に設定します。
セキュリティを管理	ハードウェアのセキュリティ権限を管理する権限を有効に設定します。

カメラ

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	クライアントとManagement Clientでカメラデバイスを表示する権限を有効に設定します。
編集	Management Clientでカメラのプロパティを編集する権限を有効に設定します。また、ユーザーに対してカメラを有効または無効にします。
ライブ表示	クライアントとManagement Clientで、カメラからのライブビデオを表示する権限を有効に設定します。
制限されたライブを見る	クライアントとManagement Clientで、カメラからのライブビデオを表示する権限を有効にします。
再生	すべてのクライアントでカメラから録画されたビデオを再生する権限を有効に設定します。
再生制限された録画を再生	すべてのクライアントでカメラで録画された制限付きビデオを再生する権限を有効にします。
リモート録画を取得	クライアントで、リモートサイトのカメラもしくはカメラのエッジストレージから録画を取得する権限を有効に設定します。
シーケンスを読み取る	クライアントで録画されたビデオの再生などに関連するシーケンス情報を読み取る権限を有効に設定します。
スマートサーチ	クライアントでスマートサーチ機能を使用する権限を有効に設定します。
エクスポート	クライアントから録画をエクスポートする権限を有効に設定します。
ブックマークを作成	クライアントで録画されたビデオやライブビデオにブックマークを作成する権限を有効に設定します。
ブックマークを読み取る	クライアントでブックマークの詳細を検索および読み取る権限を有効に設定します。
ブックマークを編集	クライアントでブックマークを編集する権限を有効に設定します。
ブックマークを削除	クライアントでブックマークを削除する権限を有効に設定します。
エビデンスロックの作成と期間の延長	クライアントでエビデンスロックを作成および延長する権限を有効に設定します。
エビデンスロックを読	クライアントでエビデンスロックを検索および読み取る権限を有効に設定します。

セキュリティ権限	説明
み取る	
エビデンスロックの削除と期間の短縮	クライアントでエビデンスロックを削除または短縮する権限を有効に設定します。
ライブおよび再生制限の作成と拡張	クライアントでの制限の作成および拡張の権限を有効にします。
ライブおよび再生制限について読む	クライアントでの既存の制限リストを確認する権限を有効にします。
ライブおよび再生制限の削除と削減	クライアントで制限を削除または緩和する権限を有効にします。
手動録画を開始	クライアントで手動録画を開始する権限を有効に設定します。
手動録画を停止	クライアントで手動録画を停止する権限を有効に設定します。
AUXコマンド	クライアントからのカメラで補助(AUX)コマンドを使用する権限を有効に設定します。 **AUX コマンド**は、例えばビデオエンコーダー経由で接続されているカメラのワイパーのコントロールを可能にします。補助接続で接続されているカメラ関連デバイスは、クライアントからコントロールされます。
手動PTZ	クライアントとManagement ClientでPTZカメラ上でPTZ機能を使用する権限を有効に設定します。
PTZプリセットまたはパトロールプロファイルの実行	クライアントとManagement Clientで位置のプリセット、パトロールプロファイルの開始・停止、パトロールの一時停止を行うためPTZカメラを動かす権限を有効に設定します。 この役割によるカメラでのPTZ機能の使用を可能にするには、**手動PTZ**権限を有効に設定します。
PTZプリセットまたはパトロールプロファイルの管理	クライアントとManagement ClientでPTZカメラ上でPTZプリセットとパトロールプロファイルを追加、編集、削除する権限を有効に設定します。 この役割によるカメラでのPTZ機能の使用を可能にするには、**手動PTZ**権限を有効に設定します。
PTZプリセットのロック/ロック解除	Management ClientでPTZカメラをロックおよびロック解除する権限を有効に設定します。これにより、他のユーザーがクライアントおよびManagement Clientにおいてプリセット位置を変更することを許可したり、防いだりすることが可能です。

セキュリティ権限	説明
PTZセッションの予約	クライアントとManagement Clientで予約されたPTZセッションモードでPTZカメラを設定する権限を有効に設定します。 予約されたPTZセッションでは、より高いPTZ優先度の他のユーザーでも制御を取得できません。 この役割によるカメラでのPTZ機能の使用を可能にするには、**手動PTZ**権限を有効に設定します。
PTZセッションのリリース	Management Clientから他のユーザーのPTZセッションをリリースする権限を有効に設定します。 この権限がなくても、自分のPTZセッションは常にリリースできます。
録画を削除	Management Client経由でシステムから保存された録画を削除する権限を有効に設定します。
プライバシーマスクの除去	XProtect Smart Clientでプライバシーマスクを一時的に除去する権限を有効に設定します。また、他のXProtect Smart Clientユーザーにプライバシーマスクを除去する権限を与える権限も有効に設定します。 プライバシーマスクの除去は、Management Clientにおいて除去可能なプライバシーマスクとして設定されたプライバシーマスクにのみ適応されます。
セキュリティを管理	Management Clientでカメラのセキュリティ権限を管理する権限を有効に設定します。

マイク

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	クライアントとManagement Clientでマイクデバイスを表示する権限を有効に設定します。
編集	Management Clientでマイクのプロパティを編集する権限を有効に設定します。また、ユーザー

セキュリティ権限	説明
	がカメラを有効または無効にすることも可能になります。
ライブで聞く	クライアントとManagement Clientでスピーカーからライブ音声を聴く権限を有効に設定します。
制限付きライブ音声を視聴	クライアントとManagement Clientでスピーカーからライブ音声を聴く権限を有効にします。
再生	クライアントでマイクから録音された音声を再生する権限を有効に設定します。
再生制限された録画を再生	クライアントでマイクから録音された制限付き音声を再生する権限を有効にします。
リモート録画を取得	クライアントで、リモートサイトのマイクもしくはカメラのエッジストレージから録音を取得する権限を有効に設定します。
シーケンスを読み取る	クライアントで**再生**タブなどに関連するシーケンス情報を読み取る権限を有効に設定します。
エクスポート	クライアントから録画をエクスポートする権限を有効に設定します。
ブックマークを作成	クライアントでブックマークを作成する権限を有効に設定します。
ブックマークを読み取る	クライアントでブックマークの詳細を検索および読み取る権限を有効に設定します。
ブックマークを編集	クライアントでブックマークを編集する権限を有効に設定します。
ブックマークを削除	クライアントでブックマークを削除する権限を有効に設定します。
エビデンスロックの作成と期間の延長	クライアントでエビデンスロックを作成または延長する権限を有効に設定します。
エビデンスロックを読み取る	クライアントでエビデンスロックの詳細を検索および読み取る権限を有効に設定します。
エビデンスロックの削除と期間の短縮	クライアントでエビデンスロックを削除または短縮する権限を有効に設定します。
ライブおよび再生制限の作成と拡張	クライアントでマイクの制限を作成、拡張する権限を有効にします。
ライブおよび再生制	クライアントで既存のマイク制限リストを確認する権限を有効にします。

セキュリティ権限	説明
限について読む	
ライブおよび再生制限の削除と削減	クライアントでマイクの制限を削除、緩和する権限を有効にします。
手動録画を開始	クライアントで音声の手動録音を開始する権限を有効に設定します。
手動録画を停止	クライアントで音声の手動録音を停止する権限を有効に設定します。
録画を削除	システムから保存された録画を削除する権限を有効に設定します。
セキュリティを管理	Management Clientでマイクのセキュリティ権限を管理する権限を有効に設定します。

スピーカー

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	クライアントとManagement Clientでスピーカーデバイスを表示する権限を有効に設定します。
編集	Management Clientでスピーカーのプロパティを編集する権限を有効に設定します。また、ユーザーがスピーカーを有効または無効にすることも可能になります。
ライブで聞く	クライアントとManagement Clientでスピーカーからライブ音声を聴く権限を有効に設定します。
制限付きライブ音声を視聴	クライアントとManagement Clientでスピーカーからライブ音声を聴く権限を有効にします。
通話	クライアントでスピーカーを通して通話する権限を有効に設定します。
再生	クライアントでスピーカーから録音された音声を再生する権限を有効に設定します。

セキュリティ権限	説明
再生制限された録画を再生	クライアントでスピーカーから録音された音声を再生する権限を有効に設定します。
リモート録画を取得	クライアントで、リモートサイトのスピーカーもしくはカメラのエッジストレージから録音を取得する権限を有効に設定します。
シーケンスを読み取る	クライアントでスピーカーから録音された音声を閲覧しつつ、シーケンス機能を使用する権限を有効に設定します。
エクスポート	クライアントでスピーカーから録画した音声をエクスポートする権限を有効に設定します。
ブックマークを作成	クライアントでブックマークを作成する権限を有効に設定します。
ブックマークを読み取る	クライアントでブックマークの詳細を検索および読み取る権限を有効に設定します。
ブックマークを編集	クライアントでブックマークを編集する権限を有効に設定します。
ブックマークを削除	クライアントでブックマークを削除する権限を有効に設定します。
エビデンスロックの作成と期間の延長	クライアントで録音された音声を保護するためのエビデンスロックを作成または延長する権限を有効に設定します。
エビデンスロックを読み取る	クライアントでエビデンスロックによって保護されている録音音声を表示する権限を有効に設定します。
エビデンスロックの削除と期間の短縮	クライアントで保護された音声に対するエビデンスロックを削除または短縮する権限を有効に設定します。
ライブおよび再生制限の作成と拡張	クライアントでスピーカーの制限を作成、拡張する権限を有効にします。
ライブおよび再生制限について読む	クライアントで既存のスピーカー制限リストを確認する権限を有効にします。
ライブおよび再生制限の削除と削減	クライアントでスピーカーの制限を削除、緩和する権限を有効にします。
手動録画を開始	クライアントで音声の手動録音を開始する権限を有効に設定します。
手動録画を停止	クライアントで音声の手動録音を停止する権限を有効に設定します。
録画を削除	システムから保存された録画を削除する権限を有効に設定します。
セキュリティを管理	Management Clientでスピーカーのセキュリティ権限を管理する権限を有効に設定します。

メタデータ

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	クライアントでメタデータを受信する権限を有効に設定します。
編集	Management Clientでメタデータのプロパティを編集する権限を有効に設定します。また、ユーザーがメタデータデバイスを有効または無効にすることも可能になります。
ライブ	クライアントが、メタデータデバイスからライブメタデータを受信する権限を有効にします。
制限されたライブを見る	クライアントでメタデータデバイスから制限付きライブメタデータを受信する権限を有効にします。
再生	クライアントでメタデータデバイスからの録画データを再生する権限を有効に設定します。
再生制限された録画を再生	クライアントでメタデータデバイスからの制限付き録画データを再生する権限を有効にします。
リモート録画を取得	クライアントで、リモートサイトのメタデータデバイスもしくはカメラのエッジストレージから録画を取得する権限を有効に設定します。
シーケンスを読み取る	クライアントで**再生**タブなどに関連するシーケンス情報を読み取る権限を有効に設定します。
エクスポート	クライアントで録画をエクスポートする権限を有効に設定します。
エビデンスロックの作成と期間の延長	クライアントでエビデンスロックを作成する権限を有効に設定します。
エビデンスロックを読み取る	クライアントでエビデンスロックを表示する権限を有効に設定します。
エビデンスロックの削除と期間の短縮	クライアントでエビデンスロックを削除または短縮する権限を有効に設定します。

セキュリティ権限	説明
ライブおよび再生制限の作成と拡張	クライアントでメタデータの制限を作成、拡張する権限を有効にします。
ライブおよび再生制限について読む	クライアントでメタデータの既存の制限リストを確認する権限を有効にします。
ライブおよび再生制限の削除と削減	クライアントでメタデータの制限を削除または緩和する権限を有効にします。
手動録画を開始	クライアントでメタデータの手動録画を開始する権限を有効に設定します。
手動録画を停止	クライアントでメタデータの手動録画を停止する権限を有効に設定します。
録画を削除	システムから保存された録画を削除する権限を有効に設定します。
セキュリティを管理	Management Clientでメタデータのセキュリティ権限を管理する権限を有効に設定します。

入力

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	クライアントとManagement Clientで入力デバイスを表示する権限を有効にします。
編集	Management Clientで入力デバイスのプロパティを編集する権限を有効に設定します。また、ユーザーが入力デバイスを有効または無効にすることも可能になります。
セキュリティを管理	Management Clientで入力デバイスのセキュリティ権限を管理する権限を有効に設定します。

出力

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	クライアントで出力デバイスを表示する権限を有効に設定します。
編集	Management Clientで出力デバイスのプロパティを編集する権限を有効に設定します。また、ユーザーが出力デバイスを有効または無効にすることも可能になります。
実行	クライアントで出力を有効にする権限を有効に設定します。
セキュリティを管理	Management Clientで出力デバイスのセキュリティ権限を管理する権限を有効にします。

Smart Wall

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	XProtect Management Clientですべてのセキュリティ権限を管理するための権限を有効にします。
読み取る	XProtect Smart Clientでビデオウォールを表示する権限を有効にします。
編集	XProtect Management ClientでSmart Wallの定義のプロパティを編集する権限を有効にします。
削除	XProtect Management Clientで既存のSmart Wallの定義を削除する権限を有効にします。
操作	Smart Wallの定義を有効化または修正する権限を有効にします(例:XProtect Smart ClientおよびXProtect Management Clientでプリセットの変更や有効化、もしくはビューへのカメラの適用を行うため)。

セキュリティ権限	説明
	[操作] をユーザー権限の適用時期を定義する時間プロファイルと関連付けることができます。
Smart Wallの作成	XProtect Management Clientで、Smart Wallの新規定義を作成する権限を有効にします。
セキュリティを管理	XProtect Management ClientでSmart Wallの定義について、セキュリティ権限を管理する権限を有効にします。
再生	XProtect Smart Clientでビデオウォールから録画されたデータを再生する権限を有効にします。 [再生] をユーザー権限の適用時期を定義する時間プロファイルと関連付けることができます。

ビューグループ

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	クライアントとManagement Clientで、[ビューグループ] を確認するための権限を有効に設定します。ビューグループが以下に作成されますManagement Client。
編集	Management Clientの [ビューグループ] でプロパティを編集する権限を有効に設定します。
削除	Management Clientでビューグループを削除する権限を有効に設定します。
操作	XProtect Smart Clientで [ビューグループ] を使用する権限、すなわち、サブグループとビューを作成および削除する権限を有効に設定します。
ビューグループの作成	Management Clientで [ビューグループ] を作成する権限を有効に設定します。
セキュリティを管理	Management Clientで [ビューグループ] のセキュリティ権限を管理する権限を有効に設定します。

ユーザー定義イベント

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	クライアントでユーザー定義のイベントを表示する権限を有効に設定します。
編集	Management Clientでユーザー定義イベントのプロパティを編集する権限を有効に設定します。
削除	Management Clientでユーザー定義イベントを削除する権限を有効に設定します。
トリガー	クライアントでユーザー定義イベントをトリガする権限を有効に設定します。
セキュリティを管理	Management Clientでユーザー定義イベントのセキュリティ権限を管理する権限を有効に設定します。
ユーザー定義イベントの作成	Management Clientで新規ユーザー定義イベントを作成する権限を有効に設定します。

アナリティクスイベント

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	Management Clientで解析イベントを表示する権限を有効に設定します。

セキュリティ権限	説明
編集	Management Clientで解析イベントのプロパティを編集する権限を有効に設定します。
セキュリティを管理	Management Clientで解析イベントのセキュリティ権限を管理する権限を有効に設定します。

ジェネリックイベント

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	クライアントとManagement Clientで一般的なイベントを表示する権限を有効に設定します。
編集	Management Clientでジェネリックイベントのプロパティを編集する権限を有効に設定します。
セキュリティを管理	Management Clientでジェネリックイベントのセキュリティ権限を管理する権限を有効に設定します。

Matrix

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	クライアントからビデオを選択し、Matrixの受信者へビデオを送信する権限を有効に設定します。
編集	MatrixでManagement Clientのプロパティを編集する権限を有効に設定します。
削除	MatrixでManagement Clientを削除する権限を有効に設定します。
Matrixの作成	Matrixで新規Management Clientを作成する権限を有効に設定します。
セキュリティを管理	Management Clientですべてのセキュリティ権限を管理する権限を有効に設定します。

ルール

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	Management Clientで既存のルールを表示する権限を有効に設定します。
編集	Management Clientでルールのプロパティを編集し、ルールの動作を設定する権限を有効に設定します。 ユーザーは、ルールに影響される全てのデバイスの読み出し権限を持っていることが要求されます。
削除	Management Clientからルールを削除する権限を有効に設定します。 また、ルールによって影響を受けるすべてのデバイスに、ユーザーの読み取り権限があることも必要です。
ルールを作成	Management Clientで新規ルールを作成する権限を有効に設定します。 また、ルールによって影響を受けるすべてのデバイスに、ユーザーの読み取り権限があることも必要です。
セキュリティを管理	Management Clientですべてのルールのセキュリティ権限を管理する権限を有効に設定します。

サイト

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	Management Clientで他のサイトを表示する権限を有効に設定します。接続されているサイトはMilestone Federated Architectureを経由して接続されています。 プロパティを編集するには、各サイトのマネジメントサーバーにおいて編集権限を持っていなければなりません。
セキュリティを管理	すべてのサイトでセキュリティ権限を管理する権限を有効に設定します。

システムモニター

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	XProtect Smart Clientでシステムモニターを表示する権限を有効に設定します。
編集	Management Clientでシステムモニターのプロパティを編集する権限を有効に設定します。
セキュリティを管理	Management Clientですべてのシステムモニターのセキュリティ権限を管理する権限を有効に設定します。

メタデータ検索

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取り	Management Clientと関連設定で、[メタデータの使用]機能を表示する権限を有効に設定しますが、設定を変更する権限は有効に設定しません。
メタデータ検索設定の編集	Management Clientでメタデータ検索カテゴリ(人物や車両のメタデータなど)を有効または無効に設定する権利を有効に設定します。
セキュリティを管理	メタデータ検索のセキュリティ権限を管理する権利を有効に設定します。

検索

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

セキュリティ権限	説明
パブリックサーチの読み取り	XProtect Smart Clientで保存されているパブリックサーチを表示および開く権限を有効に設定します。
パブリックサーチの作成	XProtect Smart Clientでパブリックサーチとして新規設定された検索を保存する権限を有効に設定します。
パブリックサーチの編集	XProtect Smart Clientに保存されているパブリックリサーチの詳細や設定(名前、説明、カメラ、検索カテゴリなど)を編集する権限を有効に設定します。
パブリックサーチの削除	保存されているパブリックサーチを削除する権限を有効に設定します。
セキュリティを管理	Management Clientで検索のセキュリティ権限を管理する権限を有効に設定します。

アラーム

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
管理	Smart Clientでアラームを管理する権限を有効にします。例えば、アラームの優先度の変更、他のユーザーへのアラームの再割り当て、アラームの確認、複数のアラームのアラームステータスの変更(例えば、**新規**から**割り当て**)。アラーム設定を編集するには、**アラーム設定の編集**権限も必要です。 この設定を許可した場合のみ、**オプション**ダイアログに**アラームおよびイベント**タブが表示されます。
ビュー	APIを通じてXProtect Smart Clientの**アラームマネージャ**タブを表示し、アラームとアラーム設定を取得する権限を有効にします。 XProtect Smart Clientでアラームを表示するには、少なくとも1つのアラーム定義で**表示**権限を有効にする必要があります。デフォルトでは、サードパーティーのソリューションからのアラームが表示されます。
アラームを無効にする	アラームを無効にする権限を有効に設定します。
通知の受信	XProtect MobileクライアントとXProtect Web Clientで、アラームに関する通知を受信する権限を有効に設定します。
セキュリティを管理	アラームのセキュリティ権限を管理する権限を有効に設定します。
アラームの設定を編集	アラーム定義、アラームステータス、アラームカテゴリ、アラーム音、アラーム保持、イベント保持の編集権限を有効にします。アラーム設定を編集するには、**管理**権限も必要です。

アラーム定義

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
ビュー	アラーム定義、アラームステータス、アラームカテゴリ、アラーム音、アラーム保持、イベント保持の表示権限を有効にします。
書き込み	**表示**権限を有効にします。
セキュリティを管理	アラーム定義のセキュリティ権限を管理する権限を有効に設定します。

サーバーログ

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
システムログエントリの読み取り	システムログのエントリを確認する権限を有効に設定します。
音声ログエントリの読み取り	監査ログのエントリを確認する権限を有効に設定します。
ルール起動ログエントリの読み取り	ルールによってトリガーされるログのエントリーを確認する権限を有効に設定します。
ログ設定の読み取り	**[ツール] > [オプション] > [サーバーログ]** でログ設定を読み取る権限を有効に設定します。
ログ設定の更新	**[ツール] > [オプション] > [サーバーログ]** でログ設定を変更する権限を有効に設定します。
セキュリティを管理	アラームのセキュリティ権限を管理する権限を有効に設定します。

アクセスコントロール

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト (https://www.milestonesys.com/products/software/product-index/) の製品概要ページにあります。

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
編集	Management Clientでアクセスコントロールシステムのプロパティを編集する権限を有効に設定します。
入退室管理の使用	クライアントの入退室管理関連の機能をユーザーが使用できるようにします。
カードホルダーの一覧表示	ユーザーがクライアントの**入退室管理**タブでカードホルダーリストを表示することを許可します。
通知の受信	ユーザーがクライアントでアクセスリクエストに関する通知の受信が可能になります。
セキュリティを管理	すべてのアクセスコントロールシステムのセキュリティ権限を管理する権限を有効に設定します。

LPR

システムでXProtect LPRが実行中の場合、ユーザーに対して次の権限を指定します:

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
LPRを使用	クライアントでLPR関連の機能を使用する権限を有効に設定します
マッチリストの管理	Management Clientでナンバープレート一致リストを追加、インポート、変更、エクスポート、削除する権限を有効に設定します。
マッチリストの読み取り	ナンバープレート一致リストを表示する権限を有効に設定します。
セキュリティを管理	Management Clientですべてのトランザクション定義のセキュリティ権限を管理する権限を有効に設定します。

トランザクションソース

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取る	Management Clientでトランザクションソースのプロパティを表示する権限を有効に設定します。
編集	Management Clientでトランザクションソースのプロパティを編集する権限を有効に設定します。
削除	Management Clientでトランザクションソースを削除する権限を有効に設定します。
作成	Management Clientで新規トランザクションソースを作成する権限を有効に設定します。
セキュリティを管理	Management Clientですべてのトランザクションソースのセキュリティ権限を管理する権限を有効に設定します。

トランザクションの定義

セキュリティ権限	説明
完全コントロール	システムのこの部分のセキュリティエントリすべてを管理する権限を有効に設定します。
読み取る	Management Clientでトランザクション定義のプロパティを表示する権限を有効に設定します。
編集	Management Clientでトランザクション定義のプロパティを編集する権限を有効に設定します。
削除	Management Clientでトランザクション定義を削除する権限を有効に設定します。
作成	Management Clientで新規トランザクション定義を作成する権限を有効に設定します。
セキュリティを管理	Management Clientですべてのトランザクション定義のセキュリティ権限を管理する権限を有効に設定します。

MIPプラグイン

MIP SDKによって、サードパーティーのベンダーは、お使いのシステム用のカスタムプラグイン(例 : 外部入退室管理システムまたは同様の機能などとの統合) を開発できます。

デバイスタブ(役割)

使用可能な機能は、使用しているシステムによって異なります。すべての機能に関するリストをご確認ください。リストは、Milestoneウェブサイト(https://www.milestonesys.com/products/software/product-index/)の製品概要ページにあります。

[デバイス]タブでは、各デバイス(カメラ等)またはデバイスグループについて、選択した役割のユーザー/グループがXProtect Smart Clientで各デバイス(カメラなど)またはデバイスグループを使用できるかを指定できます。

それぞれのデバイスに対して繰り返すことを忘れないでください。また、デバイスグループを選択し、一度にグループのすべてのデバイスの役割の権限を指定することもできます。

塗りつぶされた四角のチェックボックスは選択または選択解除できますが、この場合、ここでの選択はデバイスグループ内の**すべて**のデバイスに適用されます。または、デバイスグループの個別デバイスを選択し、該当する権限が適用されるデバイスを確認します。

カメラ関連の権限

カメラデバイスに対して次の権限を指定します:

名前	説明
読み取り	選択したカメラが、クライアントで表示されます。
ライブ表示	クライアントで選択したカメラからビデオのライブ表示ができるようにします。 XProtect Smart Clientでは、クライアントの**ライブ**タブを表示する権限が役割に付与されている必要があります。この権限はアプリケーションの権限の一部として付与されます。時間プロファイルを指定するか、デフォルト値のままにします。
制限されたライブを見る	クライアントで選択したカメラから制限付きビデオのライブビューイングを可能にします。 XProtect Smart Clientでは、クライアントの**ライブ**タブを表示する権限が役割に付与されている必要があります。この権限はアプリケーションの権限の一部として付与されます。時間プロファイルを指定するか、デフォルト値のままにします。
再生 > 時間プロファイル内	クライアントで選択したカメラから録画ビデオの再生ができるようにします。時間プロファイルを指定するか、デフォルト値のままにします。
再生 > 再生の制限	クライアントで選択したカメラから録画ビデオの再生ができるようにします。再生の制限を指定するか、制限なしを適用します。
再生制限された録	クライアントで選択したカメラから制限付き録画ビデオの再生を可能にします。時間プロファイルを

名前	説明
画を再生	指定するか、デフォルト値のままにします。
シーケンスを読み取る	例えば、クライアントのシーケンスエクスプローラに関連するシーケンス情報の読み取りを有効にします。
スマートサーチ	クライアントでユーザーがスマートサーチ機能を使用できるようにします。
エクスポート	クライアントから、ユーザーが録画をエクスポートできるようにします。
手動録画を開始	クライアントで選択したカメラからビデオの手動録画を開始できるようにします。
手動録画を停止	クライアントで選択したカメラからビデオの手動録画を停止できるようにします。
ブックマークを読み取る	クライアントでブックマーク詳細の検索、読み取りを許可します。
ブックマークを編集	クライアントでブックマークの編集を許可します。
ブックマークを作成	クライアントでブックマークの追加を許可します。
ブックマークを削除	クライアントでブックマークの削除を許可します。
AUXコマンド	クライアントからの、補助コマンドの使用を許可します。
エビデンスロックの作成と期間の延長	クライアントが、以下のことをできるようにします。 • カメラを新規または既存のエビデンスロックに追加 • 既存のエビデンスロックの有効期限を延長 • 既存のエビデンスロックの保護期間を延長 エビデンスロックに含まれているすべてのデバイスに対するユーザー権限が必要です。
エビデンスロックの削除と期間の短縮	クライアントのユーザーが、以下のことをできるようにします。 • 既存のエビデンスロックからカメラを削除 • 既存のエビデンスロックを削除 • 既存のエビデンスロックの有効期限を短縮

名前	説明
	• 既存のエビデンスロックの保護期間を短縮 エビデンスロックに含まれているすべてのデバイスに対するユーザー権限が必要です。
エビデンスロックを読み取る	クライアントユーザーが、エビデンスロックの詳細を検索、読み取りを許可します。
ライブおよび再生制限の作成と拡張	クライアントのユーザーが、以下のことをできるようにします。 • カメラでライブ制限を作成 • カメラレコーディングで再生制限を作成 • 新しいカメラをライブまたは再生制限に追加 • カメラレコーディングの制限期間を延期 制限に含まれているすべてのデバイスに対するユーザー権限が必要です。
ライブおよび再生制限について読む	クライアントのユーザーが、以下のことをできるようにします。 • カメラの既存のライブおよび再生制限リストを確認 • カメラのライブおよび再生制限のリストをフィルタリングして検索
ライブおよび再生制限の削除と削減	クライアントのユーザーが、以下のことをできるようにします。 • カメラのライブ制限を削除 • カメラレコーディングの再生制限を削除 • カメラレコーディングの制限期間を短縮 • ライブまたは再生制限の設定を変更 制限に含まれているすべてのデバイスに対するユーザー権限が必要です。

マイク関連の権限

マイクデバイスに対して次の権限を指定します:

名前	説明
読み取り	選択したマイクが、クライアントに表示されます。
ライブで聞く	クライアントが選択したマイクからライブ音声を聞くことができるようになります。 XProtect Smart Clientでは、クライアントの**ライブ**タブを表示する権限が役割に付与されている必要があります。この権限はアプリケーションの権限の一部として付与されます。時間プロファイルを指定するか、デフォルト値のままにします。
制限付きライブ音声を視聴	クライアントで選択したマイクからの制限付きライブビデオを視聴可能にします。 XProtect Smart Clientでは、クライアントの**ライブ**タブを表示する権限が役割に付与されている必要があります。この権限はアプリケーションの権限の一部として付与されます。時間プロファイルを指定するか、デフォルト値のままにします。
再生 > 時間プロファイル内	クライアントで選択したマイクからの録音した音声を再生できるようにします。時間プロファイルを指定するか、デフォルト値のままにします。
再生 > 再生の制限	クライアントで選択したマイクからの録音した音声を再生できるようにします。再生の制限を指定するか、制限なしを適用します。
再生制限された録画を再生	クライアントで選択したマイクからの録音した制限付き音声の再生を可能にします。時間プロファイルを指定するか、デフォルト値のままにします。
シーケンスを読み取る	例えば、クライアントのシーケンスエクスプローラに関連するシーケンス情報の読み取りを有効にします。
エクスポート	クライアントから、ユーザーが録画をエクスポートできるようにします。
手動録画を開始	クライアントで選択したマイクからの音声の手動録音を開始できるようにします。
手動録画を停止	クライアントで選択したマイクからの音声の手動録音を停止できるようにします。
ブックマークを読み取る	クライアントでブックマーク詳細の検索、読み取りを許可します。
ブックマークを編集	クライアントでブックマークの編集を許可します。
ブックマークを作成	クライアントでブックマークの追加を許可します。
ブックマークを削除	クライアントでブックマークの削除を許可します。
エビデンスロックの作	クライアントのユーザーが、以下のことをできるようにします。

名前	説明
成と期間の延長	• 新規または既存のエビデンスロックにマイクを追加 • 既存のエビデンスロックの有効期限を延長 • 既存のエビデンスロックの保護期間を延長 エビデンスロックに含まれているすべてのデバイスに対するユーザー権限が必要です。
エビデンスロックの削除と期間の短縮	クライアントのユーザーが、以下のことをできるようにします。 • 既存のエビデンスロックからマイクを削除 • 既存のエビデンスロックを削除 • 既存のエビデンスロックの有効期限を短縮 • 既存のエビデンスロックの保護期間を短縮 エビデンスロックに含まれているすべてのデバイスに対するユーザー権限が必要です。
エビデンスロックを読み取る	クライアントユーザーが、エビデンスロックの詳細を検索、読み取りを許可します。
ライブおよび再生制限の作成と拡張	クライアントのユーザーが、以下のことをできるようにします。 • マイクのライブ制限を作成 • 音声レコーディングの再生制限を作成 • 新しいマイクをライブまたは再生制限に追加 • 音声レコーディングの制限期間を延期 制限に含まれているすべてのデバイスに対するユーザー権限が必要です。
ライブおよび再生制限について読む	クライアントのユーザーが、以下のことをできるようにします。 • マイクの既存のライブおよび再生制限リストを確認 • マイクのライブおよび再生制限のリストをフィルタリングして検索

名前	説明
ライブおよび再生制限の削除と削減	クライアントのユーザーが、以下のことをできるようにします。 • マイクのライブ制限を削除 • 音声レコーディングの再生制限を削除 • 音声レコーディングの制限期間を短縮 • ライブまたは再生制限の設定を変更 制限に含まれているすべてのデバイスに対するユーザー権限が必要です。

スピーカー関連の権限

スピーカーデバイスに対して次の権限を指定します:

名前	説明
読み取り	選択したスピーカーが、クライアントで表示されます
ライブで聞く	クライアントで選択したスピーカーからのライブ音声を聞くことができるようにします。XProtect Smart Clientでは、クライアントの**ライブ**タブを表示する権限が役割に付与されている必要があります。この権限はアプリケーションの権限の一部として付与されます。時間プロファイルを指定するか、デフォルト値のままにします。
制限付きライブ音声を視聴	クライアントで選択したスピーカーからの制限付きライブビデオを視聴可能にします。 XProtect Smart Clientでは、クライアントの**ライブ**タブを表示する権限が役割に付与されている必要があります。この権限はアプリケーションの権限の一部として付与されます。時間プロファイルを指定するか、デフォルト値のままにします。
再生 > 時間プロファイル内	クライアントで選択したスピーカーから録音した音声を再生できるようにします。時間プロファイルを指定するか、デフォルト値のままにします。
再生 > 再生の制限	クライアントで選択したスピーカーから録音した音声を再生できるようにします。再生の制限を指定するか、制限なしを適用します。
再生制限された録画を再生	クライアントで選択したスピーカーから録音した制限付き音声の再生を可能にします。時間プロファイルを指定するか、デフォルト値のままにします。

名前	説明
シーケンスを読み取る	例えば、クライアントのシーケンスエクスプローラに関連するシーケンス情報の読み取りを有効にします。
エクスポート	クライアントから、ユーザーが録画をエクスポートできるようにします。
手動録画を開始	クライアントで選択したスピーカーからの音声の手動録音を開始できるようにします。
手動録画を停止	クライアントで選択したスピーカーからの音声の手動録音を停止できるようにします。
ブックマークを読み取る	クライアントでブックマーク詳細の検索、読み取りを許可します。
ブックマークを編集	クライアントでブックマークの編集を許可します。
ブックマークを作成	クライアントでブックマークの追加を許可します。
ブックマークを削除	クライアントでブックマークの削除を許可します。
エビデンスロックの作成と期間の延長	クライアントのユーザーが、以下のことをできるようにします。 • 新規または既存のエビデンスロックにスピーカーを追加 • 既存のエビデンスロックの有効期限を延長 • 既存のエビデンスロックの保護期間を延長 エビデンスロックに含まれているすべてのデバイスに対するユーザー権限が必要です。
エビデンスロックの削除と期間の短縮	クライアントのユーザーが、以下のことをできるようにします。 • 既存のエビデンスロックからスピーカーを削除 • 既存のエビデンスロックを削除 • 既存のエビデンスロックの有効期限を短縮 • 既存のエビデンスロックの保護期間を短縮 エビデンスロックに含まれているすべてのデバイスに対するユーザー権限が必要です。

名前	説明
エビデンスロックを読み取る	クライアントユーザーが、エビデンスロックの詳細を検索、読み取りを許可します。
ライブおよび再生制限の作成と拡張	クライアントのユーザーが、以下のことをできるようにします。 • スピーカーのライブ制限を作成 • 音声レコーディングの再生制限を作成 • 新しいマイクをライブまたは再生制限に追加 • 音声レコーディングの制限期間を延期 制限に含まれているすべてのデバイスに対するユーザー権限が必要です。
ライブおよび再生制限について読む	クライアントのユーザーが、以下のことをできるようにします。 • スピーカーの既存のライブおよび再生制限リストを確認 • スピーカーのライブおよび再生制限のリストをフィルタリングして検索
ライブおよび再生制限の削除と削減	クライアントのユーザーが、以下のことをできるようにします。 • スピーカーのライブ制限を削除 • 音声レコーディングの再生制限を削除 • 音声レコーディングの制限期間を短縮 • ライブまたは再生制限の設定を変更 制限に含まれているすべてのデバイスに対するユーザー権限が必要です。

メタデータ関連の権限

メタデータデバイスに対して次の権限を指定します:

名前	説明
読み取り	クライアントでメタデータデバイスを表示し、メタデータデバイスからデータを取得する権限を有効に

名前	説明
	設定します。
編集	メタデータのプロパティを編集する権限を有効に設定します。また、ユーザーがManagement ClientでMIP SDKを介して、メタデータデバイスを有効または無効にすることも可能になります。
ライブ表示	クライアントがカメラからのライブメタデータを表示する権限を有効にします。 XProtect Smart Clientでは、クライアントの**ライブ**タブを表示する権限が役割に付与されている必要があります。この権限はアプリケーションの権限の一部として付与されます。
ライブ制限を表示	クライアントでカメラからの制限付きライブメタデータを表示する権限を有効にします。 XProtect Smart Clientでは、クライアントの**ライブ**タブを表示する権限が役割に付与されている必要があります。この権限はアプリケーションの権限の一部として付与されます。
再生	クライアントでメタデータデバイスからの録画データを再生する権限を有効に設定します。
再生制限された録画を再生	クライアントで制限付きメタデータデバイスからの録画データを再生する権限を有効にします。
シーケンスを読み取る	クライアントでメタデータデバイスからの録画データを閲覧しながら、シーケンス機能を使用する権限を有効に設定します。
エクスポート	クライアントでメタデータデバイスから録音した音声をエクスポートする権限を有効に設定します。
エビデンスロックの作成と期間の延長	クライアントでメタデータのエビデンスロックを作成、延長する権限を有効に設定します。
エビデンスロックを読み取る	クライアントでメタデータのエビデンスロックを表示する権限を有効に設定します。
エビデンスロックの削除と期間の短縮	クライアントでメタデータのエビデンスロックを削除または短縮する権限を有効に設定します。
手動録画を開始	クライアントでメタデータの手動録画を開始する権限を有効に設定します。
手動録画を停止	クライアントでメタデータの手動録画を停止する権限を有効に設定します。
ライブおよび再生制限の作成と拡張	クライアントのユーザーが、以下のことをできるようにします。 • メタデータデバイスでライブ制限を作成 • メタデータデバイスで再生制限を作成

名前	説明
	• 新しいメタデータをライブまたは再生制限に追加 • メタデータデバイスの制限期間を延期 制限に含まれているすべてのデバイスに対するユーザー権限が必要です。
ライブおよび再生制限について読む	クライアントのユーザーが、以下のことをできるようにします。 • メタデータデバイスで既存のライブおよび再生制限リストの確認 • メタデータデバイスでライブおよび再生制限リストをフィルタリングして検索
ライブおよび再生制限の削除と削減	クライアントのユーザーが、以下のことをできるようにします。 • メタデータデバイスでライブ制限を削除 • メタデータデバイスで再生制限を削除 • メタデータデバイスの制限期間を短縮 • ライブまたは再生制限の設定を変更 制限に含まれているすべてのデバイスに対するユーザー権限が必要です。

入力関連の権限

入力デバイスに対して次の権限を指定します:

名前	説明
読み取り	選択した入力は、クライアントで表示されます。

出力関連の権限

出力デバイスに対して次の権限を指定します:

名前	説明
読み取り	選択した出力は、クライアントで表示されます。表示される場合、出力はクライアントのリストで選択できます。
実行	選択した出力は、Management Clientおよびクライアントからアクティブ化できます。時間プロファイルを指定するか、デフォルト値のままにします。

PTZタブ(役割)

[PTZ] タブでパン/チルト/ズーム(PTZ) カメラの権限を設定します。ユーザー/グループがクライアントで使用できる機能を指定できます。個別のPTZカメラを選択したり、PTZカメラを含んでいるデバイスグループを選択することができます。

PTZに対して次の権限を指定します:

名前	説明
手動PTZ	選択した役割が、選択したカメラでPTZ機能を使用し、パトロールを一時停止できるかどうかを決定します。 時間プロファイルを指定するか、**常時**を選択するか、あるいは該当する役割の**情報**タブで定義したデフォルトの時間プロファイルに沿ったデフォルト値のままにします。
PTZプリセットまたはパトロールプロファイルの実行	選択した役割が選択したカメラをプリセット位置に移動し、パトロールプロファイルを開始および停止し、パトロールを一時停止できるかどうかを決定します。 時間プロファイルを指定するか、**常時**を選択するか、あるいは該当する役割の**情報**タブで定義したデフォルトの時間プロファイルに沿ったデフォルト値のままにします。 この役割によるカメラでのPTZ機能の使用を可能にするには、**手動PTZ**権限を有効に設定します。
PTZ優先度	PTZカメラの優先度を決定します。監視システムの複数のユーザーが同時に同じPTZカメラを制御しようとすると、競合が発生する可能性があります。 選択済みの役割を持つユーザー/グループが選択したPTZカメラを使用する優先度を指定することで、この状況を回避できます。1 ~ 32,000の範囲で優先度を指定します。1が最低優先度です。デフォルトの優先度は 3,000 です。最高の優先度を持つ役割は、PTZカメラをコントロールできる人の役割です。
PTZプリセットまたはパトロールプロファイルの管理	Management ClientとXProtect Smart Clientの両方で選択したカメラのPTZプリセットとパトロールプロファイルを追加、編集、および削除する権限を決定します。 この役割によるカメラでのPTZ機能の使用を可能にするには、**手動PTZ**権限を有効に設定しま

名前	説明
	す。
PTZプリセットのロック/ロック解除	役割が選択したカメラのプリセット位置をロックおよびロック解除できるかどうかを決定します。
PTZセッションの予約	予約されたPTZセッションモードで、選択したカメラを設定する権限を決定します。 予約されたPTZセッションでは、より高いPTZ優先度の他のユーザーまたはパトロールセッションでも制御を取得できません。 この役割によるカメラでのPTZ機能の使用を可能にするには、**手動PTZ**権限を有効に設定します。
PTZセッションのリリース	選択した役割が他のユーザーのPTZセッションをManagement Clientからリリースできるかどうかを決定します。 この権限がなくても、自分のPTZセッションは常にリリースできます。

通話タブ(役割)

スピーカーがシステムで使用できる場合のみ該当します。スピーカーに対して次の権限を指定します:

名前	説明
通話	選択したスピーカーを通じて、ユーザーが通話を許可されるかどうかを決定します。時間プロファイルを指定するか、デフォルト値のままにします。
通話優先度	複数のクライアントユーザーが同じスピーカーから同時に通話したい場合、対立が生じることがあります。 選択済みの役割を持つユーザー/グループが選択したスピーカーを使用する優先度を指定することで、この問題を解決できます。優先度を**[非常に低い]** ~ **[非常に高い]**に指定します。最高の優先度の役割は、他の役割に優先してスピーカーを使用できます。 同じ役割の2人のユーザーが同時に通話しようとする場合、先着順の原則が適用されます。

リモート録画タブ(役割)

リモート録画に対して次の権限を指定します:

名前	説明
リモート録画を取得	クライアントで、リモートサイトのカメラ、マイク、スピーカー、メタデータデバイスもしくはカメラのエッジストレージから録音/録画を取得する権限を有効に設定します。

Smart Wallタブ(役割)

役割経由で、Smart Wall関連のユーザー権限をクライアントユーザーに付与できます。

名前	説明
読み取る	ユーザーがXProtect Smart Clientで選択したSmart Wallを確認することを許可します。
編集	以下の選択アイテムSmart Wallをユーザーが編集することを許可するManagement Client。
削除	以下の選択アイテムSmart Wallをユーザーが削除することを許可するManagement Client。
操作	ユーザーがXProtect Smart Clientで選択したSmart Wallにレイアウトを適用し、プリセットを有効にすることを可能にします。
再生	ユーザーがXProtect Smart Clientで選択されたSmart Wallから、録画されたデータを再生することを許可します。

外部イベントタブ(役割)

次の外部イベントの権限を指定します:

名前	説明
読み取り	ユーザーが、クライアントや以下の任意の外部システムイベントを検索し、見ることを許可しますManagement Client。
編集	ユーザーが、クライアントや以下の任意の外部システムイベントを編集することを許可しますManagement Client。
削除	ユーザーが、クライアントや以下の任意の外部システムイベントを削除することを許可しますManagement Client。
トリガー	ユーザーが、クライアントや以下の選択された外部システムイベントを起動することを許可します。

ビューグループタブ(役割)

[ビューグループ]タブで、選択された役割を担うユーザーとユーザーグループが、クライアントで使用できるビューグループを指定します。

ビューグループに次の権限を指定します:

名前	説明
読み取り	クライアントとManagement Clientで、[ビューグループ] を表示するための権限を有効に設定します。ビューグループが以下に作成されますManagement Client。
編集	Management Clientの [ビューグループ] でプロパティを編集する権限を有効に設定します。
削除	Management Clientでビューグループを削除する権限を有効に設定します。
操作	XProtect Smart Clientで [ビューグループ] を使用する権限、すなわち、サブグループとビューを作成および削除する権限を有効に設定します。

サーバータブ(役割)

[サーバー]タブでの役割の権限の指定は、システムがMilestoneFederatedArchitectureの設定で動作する場合のみ有効です。

名前	説明
サイト	Management Clientで選択されたサイトを表示する権限を有効に設定します。接続されているサイトはMilestone Federated Architectureを経由して接続されています。 プロパティを編集するには、各サイトのマネジメントサーバーにおいて編集権限を持っていなければなりません。

詳細については、87ページのMilestone Federated Architectureの設定を参照してください。

Matrixタブ(役割)

システムでMatrixの受信者を設定している場合、Matrixの役割権限も設定できます。クライアントから、選択したMatrix受信者へビデオを送信できます。これを受信できるユーザーをMatrixタブで選択します。

次の権限を利用できます:

名前	説明
読み取り	選択した役割のユーザーおよびグループが、クライアントからビデオを選択して、Matrix受信者へ送信できるかどうかを決定します。

アラームタブ(役割)

インストールした製品(他のXProtectサーバーを含む)の中央監視や制御を実行するためにシステムセットアップでアラームを使用している場合、**[アラーム]** タブを使用して、ユーザーとグループに対して、ユーザーとグループが持つべき役割を選択し、アラーム権限(例えば、クライアントでのアラームの処理方法など)を指定できます。

[アラーム]で、アラームの権限を指定できます:

セキュリティ権限	説明
管理	Smart Clientでアラームを管理する権限を有効にします。例えば、アラームの優先度の変更、他のユーザーへのアラームの再割り当て、アラームの確認、複数のアラームのアラームステータスの変更(例えば、**新規**から**割り当て**)。アラーム設定を編集するには、**アラーム設定の編集**権限も必要です。 この設定を許可した場合のみ、**オプション**ダイアログに**アラームおよびイベント**タブが表示されます。
ビュー	APIを通じてXProtect Smart Clientの**アラームマネージャ**タブを表示し、アラームとアラーム設定を取得する権限を有効にします。 XProtect Smart Clientでアラームを表示するには、少なくとも1つのアラーム定義で**表示**権限を有効にする必要があります。デフォルトでは、サードパーティーのソリューションからのアラームが表示されます。
アラームを無効にする	アラームを無効にする権限を有効に設定します。
通知の受信	XProtect MobileクライアントとXProtect Web Clientで、アラームに関する通知を受信する権限を有効に設定します。
アラームの設定を編集	アラーム定義、アラームステータス、アラームカテゴリ、アラーム音、アラーム保持、イベント保持の編集権限を有効にします。アラーム設定を編集するには、**管理**権限も必要です。

アラーム定義で、特定のアラーム定義の権限を指定できます:

名前	説明
ビュー	アラーム定義、アラームステータス、アラームカテゴリ、アラーム音、アラーム保持、イベント保持の表示権限を有効にします。
書き込み	**表示**権限を有効にします。

アクセスコントロールタブ(役割)

基本ユーザーやWindowsのユーザー、グループを追加または編集する際に、アクセスコントロールの設定を指定できます。

名前	説明
入退室管理の使用	クライアントの入退室管理関連の機能をユーザーが使用できるようにします。
カードホルダーの一覧表示	ユーザーがクライアントの**入退室管理**タブでカードホルダーリストを表示することを許可します。
通知の受信	ユーザーがクライアントでアクセスリクエストに関する通知の受信が可能になります。

LPR タブ(役割)

システムでXProtect LPRが実行中の場合、ユーザーに対して次の権限を指定します:

名前	説明
LPRを使用	クライアントでLPR関連機能を使用する権限を有効に設定します。
マッチリストの管理	Management Clientでナンバープレート一致リストを追加、インポート、変更、エクスポート、削除する権限を有効に設定します。
マッチリストの読み取り	ナンバープレート一致リストを表示する権限を有効に設定します。

[インシデント] タブ(役割)

XProtect Incident Managerがある場合は、役割に以下の権限を指定できます。

Management Client管理者の役割にインシデントプロパティの管理または表示権限を付与するには、**Incident properties (インシデントプロパティ)** ノードを選択します。

定義したインシデントプロパティを表示するXProtect Smart Client権限をオペレータに付与するには、**インシデントプロパティ**を選択して**ビュー**に権限を付与します。インシデントプロジェクトを管理または表示するための一般的な権限を付与するには、**インシデントプロジェクト**ノードを選択します。**インシデントプロジェクト**ノードを選択し、サブノードを選択することで、追加の機能または能力に対する権限を付与します。

名前	説明
管理	機能に関連する設定およびプロパティを管理(表示、作成、編集、削除)、またはManagement ClientかXProtect Smart Clientのいずれかで選択されているノードによって表されるユーザーインターフェイス要素を表示する権限。
ビュー	インシデントプロパティで定義された機能、ビューに関連する設定とプロパティを表示(作成、編集および削除ではない)、またはManagement ClientかXProtect Smart Clientいずれかで選択されているノードによって表されるユーザーインターフェイス要素を表示する権限。

MIPタブ(役割)

MIP SDKによって、サードパーティーのベンダーは、お使いのシステム用のカスタムプラグイン(例:外部入退室管理システムまたは同様の機能などとの統合)を開発できます。サードパーティのプラグインは、それぞれのタブに独自の設定があります。

変更する設定は、実際のプラグインによって異なります。**[MIP]**タブで、プラグイン用のカスタム設定を探します。

基本ユーザー(セキュリティノード)

Milestone XProtect VMSには2つのユーザーアカウントタイプがあります。 基本ユーザーとWindows ユーザー。

基本ユーザーとはMilestone XProtect VMSで作成したユーザーアカウントです。個々のユーザーの基本ユーザー名とパスワード認証を備えた専用のシステムユーザーアカウントです。

Windows ユーザーはMicrosoftのActive Directoryを通して追加したユーザーアカウントです。

基本ユーザーとWindows ユーザーには多少違いがあります。

- 基本ユーザーは、ユーザー名とパスワードの組み合わせによって認証され、システム/サイト固有のものです。あるフェデレーテッドサイトで作成された基本ユーザーが別のフェデレーテッドサイトの基本ユーザーと同じ名前とパスワードを持つ場合でも、基本ユーザーは作成されたサイトにしかアクセスできません。
- Windowsユーザーは Windows ログインに基づいて認証され、1つのマシン固有です。

システムダッシュボードノード

システムダッシュボードノード

システムダッシュボードノードには、システムと様々なシステムコンポーネントを監視する機能が各種含まれています。

名前	説明
現在のタスク	選択したレコーディングサーバーの実行中のタスクの概要を把握できます。
システムモニター	定義するパラメータでサーバーとカメラのステータスを監視します。
システムモニターしきい値	システムモニターで使用されるサーバーおよびモニタータイルで監視されるパラメータのしきい値を設定します。
エビデンスロック	システムで保護されているすべてのデータの概要を把握できます。
設定レポート	システム構成が記されたレポートを印刷します。レポートに何を含めるのか決められます。

現在のタスク(システムダッシュボードノード)

[現在のタスク]には、選択したレコーディングサーバーで実行中のタスクの概要が示されます。長い時間を要するタスクが開始され、これがバックグラウンドで実行されている間は、**[現在のタスク]**ウィンドウでタスクの進行状況を確認できます。ユーザーが開始するタスクのうち、長い時間を要するものの一例として、ファームウェアの更新やハードウェアの移動が挙げられます。ここではタスクの開始時刻、予想終了時刻、進行状況といった情報を確認できます。

[現在のタスク]ウィンドウに表示される情報はリアルタイムのものではなく、ウィンドウを開いた時点で実行されていたタスクのスナップショットとなります。ウィンドウを開いてから時間が経過している場合は、ウィンドウ右下にある**[更新]**ボタンを選択して情報を更新します。

システムモニター(システムダッシュボードノード)

[システムモニター]機能を使用すれば、システムのサーバーとカメラの現在の全体的な健全度についてすばやく視覚的に確認できます。

[システムモニターダッシュボード]ウィンドウ

タイル

[システムモニターダッシュボード]ウィンドウの上部には、システムのサーバーハードウェアとカメラハードウェアの状態を示す、色分けされたタイルが表示されます。

タイルの状態と色は、**[システムモニターしきい値]**ノードで設定したしきい値にもとづいて変化します。詳細については、「525 ページのシステムモニターしきい値(システムダッシュボードノード) 」を参照してください。タイルの色によって以下が示されるよう、しきい値を定義します。

タイルの色	説明
緑色	**正常**状態。すべてが正常に動作しています。
黄色	**警告**状態。1つまたは複数の監視パラメータが**正常**状態のしきい値を超えています。
赤色	**重大**状態。1つ以上の監視パラメータが**正常**状態と**警告**状態のしきい値を超えています。

監視パラメータが記されたハードウェアリスト

タイルをクリックすると、(**[システムモニターダッシュボード]**ウィンドウ下部でタイルとして示される) ハードウェアごとに選択した各監視パラメータの状態を確認できます。

例：カメラのライブFPS監視パラメータが警告状態に達しました。

[ダッシュボードのカスタマイズ]ウィンドウ

ウィンドウ右上にある**[カスタマイズ]**をクリックすると、**[ダッシュボードのカスタマイズ]**ウィンドウが開きます。

[ダッシュボードのカスタマイズ]ウィンドウでは、作成、編集、削除したいタイルを選択できます。タイルを作成または編集する際には、モニターしたいハードウェアと監視パラメータをタイルで選択できます。

[詳細]ウィンドウ

タイルを選択してから、監視パラメータが記されたハードウェアリストに移動し、カメラまたはサーバーの右側にある**[詳細]**ボタンを選択すると、選択したハードウェアによっては、システム情報を表示して以下に関するレポートを作成できます。

ハードウェア	情報
マネジメントサーバー	以下に関するデータが表示されます。 • CPU使用率 • 使用可能なメモリ容量 **[履歴]**を選択し、ハードウェアのこれまでの状態を確認して、上記のデータに関するレポートを作成します。
レコーディングサーバー	以下に関するデータが表示されます。 • CPU使用率

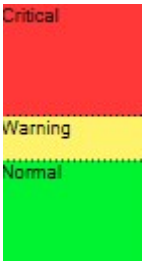
ハードウェア	情報
バー	• 使用可能なメモリ容量 • ディスク • ストレージ • ネットワーク • カメラ **[履歴]**を選択し、ハードウェアのこれまでの状態を確認して、上記のデータに関するレポートを作成します。
フェールオーバーレコーディングサーバー	以下に関するデータが表示されます。 • CPU使用率 • 使用可能なメモリ容量 • モニター対象のレコーディングサーバー **[履歴]**を選択し、ハードウェアのこれまでの状態を確認して、上記のデータに関するレポートを作成します。
ログサーバーやイベントサーバーなど	以下に関するデータが表示されます。 • CPU使用率 • 使用可能なメモリ容量 **[履歴]**を選択し、ハードウェアのこれまでの状態を確認して、上記のデータに関するレポートを作成します。
カメラ	以下に関するデータが表示されます。 • ストレージ • 使用済み領域 • ライブFPS(デフォルト) • レコーディングFPS • ライブビデオフォーマット • レコーディングビデオフォーマット • 受信メディアデータ(Kbit/s)

ハードウェア	情報
	• 使用可能なメモリ容量 カメラ名を選択してその状態の履歴を確認し、以下に関するレポートを作成します。 • カメラから受信したデータ • カメラのディスク使用量

サーバーのオペレーティングシステムからシステムモニターの詳細にアクセスした場合、**Internet Explorer Enhanced Security Configuration**に関連するメッセージが表示されることがあります。指示に従って、**[システムモニター]**のページを**[信頼済みサイトゾーン]**に追加してから続行してください。

システムモニターしきい値(システムダッシュボードノード)

システムモニターしきい値を使用すれば、どの時点で**[システムモニターダッシュボード]**にシステムハードウェアの状態変化が視覚的に表示されるようにするかを、しきい値の定義と調整を介して指定できます。たとえば、サーバーのCPU使用率が正常な状態(緑)から警告状態(黄)に変化した際、または警告状態(黄)から重大状態(赤)に変化した際、のように設定できます。



3種類ある状態のいずれになっているかを決める値の例

サーバー、カメラ、ディスク、ストレージのしきい値は変更することができます。一部のボタンと設定は、すべてのしきい値で共通となっています。

共通のユーザーインターフェース要素

ボタンと設定	説明	単位
計算間隔	他のハードウェアへの接続が短い間途切れるという状態はたびたび発生します。計算間隔を0秒に設定すると、このような短時間の機能停止によっても、ハードウェアの状態変更に関するアラートがトリガーされます。そのため、計算間隔はある程度の長さに設定してください。 たとえば、[計算間隔]を1分間に設定した場合、1分間全体にわたる平均値がしきい値を超えた場合にのみアラートが発生します。計算間隔を適切に設定することでアラートの誤発動を防ぐ一方、継続的な問題(CPU使用率やメモリ消費など)に関するアラートのみを表示することが可能となります。 計算間隔の値を変更する方法については、「281ページのハードウェアの状態変化を決めるしきい値を編集」を参照してください。	秒
詳細	**[詳細]**ボタンを選択すると、個々のサーバー、カメラ、ディスク、ストレージのしきい値および計算間隔を設定できます。詳細については、下記を参照してください。	-
ルールを作成	**[システムモニター]**のイベントをルールと組み合わせることで、サーバーのCPU使用率が重大となった際やディスクの空き容量がほぼなくなった際などに、アクションをトリガーさせることができます。 詳細については、「73ページのルールとイベント(説明付き)」および「」を参照して258ページのルールの追加ください。	-

サーバーのしきい値

しきい値	説明	単位
CPU使用率	モニタリングしているサーバーのCPU使用のしきい値。	%
使用可能なメモリ容量	モニタリングしているサーバーのRAM使用のしきい値。	MB
NVIDIAデコード	モニタリングしているサーバーのNVIDIAデコード使用のしきい値。	%
NVIDIAメモリ	モニタリングしているサーバーのNVIDIA RAM使用のしきい値。	%
NVIDIAレンダリング	モニタリングしているサーバーのNVIDIAレンダリング使用のしきい値。	%

カメラのしきい値

しきい値	説明	単位
ライブFPS	モニタリングしているカメラにライブビデオが表示されている際の、使用中のカメラのFPSのしきい値。	%
レコーディングFPS	モニタリングしているカメラでビデオが録画されている際の、使用中のカメラのFPSのしきい値。	%
使用済み領域	モニタリングしているカメラによって使用されている領域のしきい値。	GB

ディスクのしきい値

しきい値	説明	単位
空き領域	モニタリングしているディスクの空き容量のしきい値。	GB

ストレージのしきい値

しきい値	説明	単位
保存期間	ストレージの領域がどの時点でなくなるかの予測を表すしきい値。状態はシステムの設定にもとづいて表示され、1日に2回更新されます。	日

エビデンスロック(システムダッシュボードノード)

[システムダッシュボード]ノードの**エビデンスロック**には、現在監視システム内で保護されている全データの概要が表示されます。

以下のメタデータは、すべてのエビデンスロックで利用できます。

- 保護データの開始日と終了日
- エビデンスをロックしたユーザー
- エビデンスのロックが解除された時刻

- データの保存場所
- 各エビデンスロックのサイズ

[エビデンスロック]ウィンドウに表示される情報はすべてスナップショットとなります。F5を押すと画面が更新されます。

設定レポート(システムダッシュボードノード)

VMSシステムのインストールおよび構成には数多くの設定が伴うため、これらについて記録しなくてはならない場合があります。また、インストールおよび初回の構成以降、あるいは過去数か月のうちに設定にどのような変更を加えたかをすべて記憶することは、時間の経過とともに困難になっていきます。そのために、構成の内容が記されたレポートを印刷することができるようになっています。

以下の設定は、設定レポートの作成および印刷時に使用できます。

名前	説明
レポート	設定レポートに含めることのできる要素のリスト。
すべて選択	**[レポート]**リストの全要素を設定レポートに追加します。
全てクリアする	**[レポート]**リストの全要素を設定レポートから削除します。
フロントページ	レポートの表紙をカスタマイズします。
フォーマッティング	レポートをフォーマットします。
機密データを除外	GDPRに準拠するよう、ユーザー名やEメールアドレスといった機密性の高いデータを設定レポートから除去します。 ライセンス所有者に関する情報は常にレポートから除外されます。
エクスポート	レポートの保存場所を選択して、PDFレポートを作成します。

サーバーログノード

サーバーログノード

システムログ(タブ)

ログの各列はログエントリを表します。ログエントリにはさまざまな情報フィールドがあります。

名前	説明
ログレベル	情報、警告、あるいはエラー。
現地時間	システムのサーバーのローカル時間のタイムスタンプ。
メッセージテキスト	記録されたインシデントの識別番号。
カテゴリ	録画したインシデントのタイプ。
ソースタイプ	録画したインシデントが発生した機器のタイプ(サーバーまたはデバイスなど) 。
ソース名	録画されたインシデントが発生したサービスの名前。
イベントタイプ	録画されたインシデントで表されたイベントのタイプ。

監査ログ(タブ)

ログの各列はログエントリを表します。ログエントリにはさまざまな情報フィールドがあります。

名前	説明
現地時間	システムのサーバーのローカル時間のタイムスタンプ。
メッセージテキスト	録画されたインシデントの説明を表示します。
許可	リモートユーザーアクションが可能か(許可されているか) どうかについての情報。
カテゴリ	録画したインシデントのタイプ。
ソースタイプ	録画したインシデントが発生した機器のタイプ(サーバーまたはデバイスなど) 。
ソース名	録画されたインシデントが発生したサービスの名前。
ユーザー	録画されたインシデントを引き起こすリモートユーザーのユーザー名。
ユーザーの場所	リモートユーザーが録画されたインシデントを引き起こしたコンピュータのIPアドレスまたはホスト名。

ルールトリガーログ(タブ)

ログの各列はログエントリを表します。ログエントリにはさまざまな情報フィールドがあります。

名前	説明
現地時間	システムのサーバーのローカル時間のタイムスタンプ。
メッセージテキスト	録画されたインシデントの説明を表示します。
カテゴリ	録画したインシデントのタイプ。
ソースタイプ	録画したインシデントが発生した機器のタイプ(サーバーまたはデバイスなど) 。
ソース名	録画されたインシデントが発生したサービスの名前。
イベントタイプ	録画されたインシデントで表されたイベントのタイプ。
ルール名	ログエントリを起動するルールの名前。
サービス名	録画されたインシデントが発生したサービスの名前。

メタデータ使用ノード

メタデータとメタデータ検索

メタデータデバイスの管理と構成については、「283ページのメタデータ検索カテゴリおよび検索フィルターを表示/非表示にする」を参照してください。

メタデータとは?

メタデータとは、あるデータに関するデータを意味します。一例として、ビデオ映像について説明しているデータ、映像内のコンテンツまたはオブジェクト、または録画された映像の場所などが挙げられます。

メタデータは以下の方法で生成できます。

- 自らデータを配信しているデバイス(ビデオを配信しているカメラなど)
- サードパーティシステムまたは統合で、汎用メタデータドライバーを経由した配信

メタデータ検索

メタデータ検索とは、XProtect Smart Clientでのビデオ録画の検索のうち、メタデータに関連した検索カテゴリ/フィルターを使用するものを指します。

デフォルトのMilestoneメタデータ検索カテゴリは以下のとおりです。

- 場所: ユーザーは地理的座標とその座標からの検索半径を定義できます。
- 人物ユーザーは、性別やおおよその身長や年齢を検索できるほか、検索結果を顔写真付きで表示することも可能です。
- 車両 ユーザーは車両の色、スピード、車種を検索でき、特定のナンバープレートを検索することもできます。

メタデータ検索の要件

検索結果を得るには、以下のいずれかひとつが必要となります。

- ビデオ監視システムに、適切に構成されており、かつ映像解析を実行できるデバイスが少なくともひとつ存在する
- ビデオ監視システムで、メタデータが生成されるビデオ処理サービスが有効になっている

いずれの場合も、メタデータは必要なメタデータ形式でなくてはなりません。

詳細については、メタデータ検索の統合に関する文書を参照してください。

アクセスコントロールノード

入退室管理プロパティ

一般設定タブ(入退室管理)

名前	説明
有効	システムはデフォルトで有効に設定されています。つまり、システムはXProtect Smart Clientで十分な権限を持つユーザーに対して表示され、入退室管理イベントはXProtectシステムによって受信されます。 メンテナンス中などにシステムを無効にして、不要なアラームが作成されるのを避けることができます。
名前	入退室管理統合の名前が、そのままManagement Applicationやクライアントで表示されます。既存の名前を、新しい名前で上書きすることができます。
説明	入退室管理統合の説明を提供します。これはオプションです。
統合プラグイン	最初の統合で選択した入退室管理システムのタイプを示します。
最後の設定更新	入退室管理システムから最後にインポートした日付および時刻を示します。
設定の更新	ドアの追加や削除など、XProtectの入退室管理システムで行った変更を反映させる必要がある場合には、このボタンをクリックします。

名前	説明
	入退室管理システムからの設定変更の概要が表示されます。新しい設定を適用する前に、リストを確認して、入退室管理システムに正しく反映されるようにします。
オペレータのログインが必要	入退室管理システムが異なるユーザー権限をサポートしている場合、クライアントのユーザーに対して追加ログインを有効に設定します。このオプションを有効にする場合は、XProtect Mobileクライアントは入退室管理システムを使用できません。 統合プラグインが異なるユーザー権限をサポートしている場合のみ、このオプションが表示されます。

以下のフィールドの名前や内容は、統合プラグインからインポートされます。以下は典型的なレイアウトの例です。

名前	説明
アドレス	統合された入退室管理システムをホストするサーバーのアドレスを入力します。
ポート	入退室管理システムが接続するサーバーのポート番号を指定します。
ユーザー名	入退室管理システムで定義されている、XProtectの統合システムの管理者となるユーザーの名前を入力します。
パスワード	ユーザーのパスワードを指定します。

ドアと関連付けられたカメラタブ(入退室管理)

このタブでは、ドアのアクセスポイントとカメラ、マイク、スピーカーの間のマッピングを提供します。カメラは統合ウィザードの一部として関連付けますが、設定はいつでも変更することができます。マッピングには、カメラに関連付けられたマイクやスピーカーを通じて、マイクやスピーカーも必然的に含まれます。

名前	説明
ドア	入退室管理システムで定義されている、使用可能なドアのアクセスポイントをドア別にグループ化してリストします。 関連するドアへのナビゲーションを容易にするため、入退室管理システムで上部にあるドロップダウンリストボックスを使用し、ドアをフィルターできます。 **有効**:ライセンスを付与されているドアは、デフォルトで有効になっています。ドアを無効にして、ライセンスを解放することができます。

名前	説明
	ライセンス: ドアのライセンスが有効であるか、ライセンスが有効期限切れであるかを示します。ドアが無効であれば、このフィールドは空白です。 **削除**: **削除**をクリックすると、アクセスポイントからカメラを削除します。すべてのカメラを削除すると、関連するカメラのチェックボックスが自動的にクリアされます。
カメラ	XProtectシステムで設定されているカメラを一覧表示します。 リストからカメラを選択し、該当するアクセスポイントにドラッグ & ドロップして、カメラとアクセスポイントを関連付けます。

入退室管理イベントタブ(入退室管理)

イベントをグループ化できるイベントカテゴリです。イベントカテゴリの設定は、XProtectシステムの入退室管理の動作に影響を与えます。例えば、複数のタイプのイベントでの単一のアラームのトリガーを定義することができます。

名前	説明
入退室管理イベント	入退室管理システムからインポートした入退室管理イベントを一覧表示します。統合プラグインが、デフォルトでのイベントの有効化や無効化をコントロールします。イベントは、統合後にいつでも有効または無効にできます。 イベントが有効化されると、XProtectのイベントデータベースに保存され、XProtect Smart Clientでのフィルターなどに使用可能となります。
ソースタイプ	入退室管理イベントをトリガーできる入退室管理ユニットを表示します。
イベントカテゴリ	入退室管理イベントに、「なし」、「1つ」、「複数」のイベントカテゴリのいずれかを割り当てます。システムは、統合中に関連するイベントカテゴリを自動的にイベントにマッピングします。これによって、XProtectシステムのデフォルト設定が有効になります。マッピングは、いつでも変更できます。 ビルトインのイベントカテゴリは、以下のとおりです。 • アクセス拒否 • アクセス許可 • アクセスリクエスト • アラーム • エラー

名前	説明
	• 警告 また、統合プラグインによって定義されるイベントやイベントカテゴリも表示されますが、独自のイベントカテゴリを定義することも可能です。**ユーザー定義カテゴリ**を参照してください。 XProtect Corporateでイベントカテゴリを変更する場合は、既存の入退室管理のルールが正しく機能していることを確認してください。
ユーザー定義カテゴリ	ユーザー定義のイベントカテゴリを作成、変更、削除することができます。 ビルトインのカテゴリが要件を満たさない場合は、イベントカテゴリを作成することができます。例えば、入退室管理のアクションをトリガーするイベントの定義と組み合わせることができます。 カテゴリは、XProtectシステムに追加されたすべての統合システムにグローバルに適用されます。これにより、例えばアラーム定義など、システムをまたいだ操作の設定が可能になります。 ユーザー定義のイベントカテゴリを削除すると、統合で使用されている場合には警告を受け取ります。それでも削除すると、たとえば入退室管理のアクションなど、このカテゴリで行ったすべての設定が機能しなくなります。

アクセスリクエスト通知タブ(入退室管理)

所定のイベントが発生した際にXProtect Smart Client画面に表示されるアクセスリクエスト通知を指定できます。

名前	説明
名前	アクセスリクエスト通知の名前を入力します。
アクセスリクエスト通知を追加	クリックして、アクセスリクエスト通知を追加、定義します。 通知を削除するには、右側の**X**をクリックします。 XProtect Smart Clientのユーザーが Milestone Federated Architecture階層の親サイトへログインすると、子サイトからのアクセスリクエスト通知がXProtect Smart Clientにも表示されます。
アクセスリクエスト通知の詳細	所定のイベントが発生した場合、どのカメラ、マイク、スピーカーをアクセスリクエスト通知に表示するかを指定します。また、通知ポップアップが表示されるときにユーザーに警告する音声を指定します。
コマンドを追	XProtect Smart Clientのアクセスリクエスト通知ダイアログで、どのコマンドをボタンとして使用可能にする

名前	説明
加	かを選択します。 関連するアクセスリクエストコマンド • ソースユニットで使用できるアクセスリクエスト操作に関連するすべてのコマンドを有効にします。例えば、**ドアを開ける**などです。 すべての関連コマンド • ソースユニットで、すべてのコマンドを有効にします。 入退室管理コマンド • 選択した入退室管理コマンドを有効にします。 システムコマンド • XProtectシステムで事前に定義されているコマンドを有効にします。 コマンドを削除するには、右側の**X**をクリックします。

カードホルダータブ(入退室管理)

カードホルダータブを使用して、入退室管理システムにおけるカードホルダーの情報を確認します。

名前	説明
カードホルダーの検索	カードホルダーの名前の文字を入力すると、存在する場合はリストに表示されます。
名前	入退室管理システムから取得したカードホルダーの名前を一覧表示します。
タイプ	例えば以下のようにカードホルダーのタイプを一覧表示します。 • 従業員 • 警備員 • 来客

使用している入退室管理システムが、XProtectシステムでの写真の追加/削除をサポートしている場合、カードホルダーに写真を追加することができます。これは、入退室管理システムにカードホルダーの写真が含まれていない場合に便利です。

名前	説明
写真の選択	カードホルダーの写真ファイルへのパスを指定します。入退室管理システムが写真を管理している場合、このボタンは表示されません。 使用できるファイル形式は、.bmp、.png、.jpgです。 最大に表示されるように、写真はサイズ変更されます。 Milestoneは、四角形の写真を使用することを推奨しています。
写真を削除	クリックすると、写真を削除します。入退室管理システムに写真がある場合、削除後はその写真が表示されます。

インシデントノード

インシデントプロパティ(インシデントノード)

次の情報は、XProtect Incident Managerに関連する設定の説明です。

XProtect Smart Clientのオペレータに対するインシデントプロパティはすべて、これらのタブで定義します。

- タイプ
- ステータス
- カテゴリ
- カテゴリー1 ~ 5

すべてのインシデントプロパティには、以下の設定があります。

名前	説明
名前	インシデントプロパティの名称が一意である必要はありませんが、一意で分かりやすい名称にした方が、多くのメリットがあります。
説明	定義するインシデントプロパティの追加説明。例えば*Location(ロケーション)* という名称のカテゴリーを作成した場合は、*Where did the incident happen?(インシデントの発生場所)* などの説明を付けることができます。

トランザクションノード

トランザクションソース(トランザクトノード)

トランザクションソースのプロパティについて下表で説明します。

ソースの追加について詳しくは、「トランザクションソースの追加(ウィザード)」を参照してください。

トランザクションソース(プロパティ)

名前	説明
有効にする	トランザクションソースを無効にするには、このチェックボックスをオフにします。トランザクションデータのストリームは停止しますが、インポート済みのデータはイベントサーバーに残ります。保存期間中にはXProtect Smart Clientで無効なトランザクションソースからトランザクションを表示することができます。 無効なトランザクションソースでも、トランザクションソースライセンスが必要です。
名前	名前を変更するには、新しい名前をここに入力します。
コネクタ	トランザクションソースを作成した場合は、選択したコネクタを変更できません。別のコネクタを選択するには、新しいトランザクションソースを作成し、ウィザードで任意のコネクタを選択する必要があります。
トランザクションの定義	受信されたトランザクションデータをトランザクションおよびトランザクションラインに変換する方法を定義する別のトランザクション定義を選択できます。これには次の定義が含まれます。 • トランザクションの開始および終了時期 • トランザクションをXProtect Smart Clientに表示する方法
保存期間	イベントサーバーにトランザクションデータを保存する期間を日数で指定します。デフォルトの保存期間は30日です。保存期間が終了すると、データは自動的に削除されます。これにより、データベースのストレージ容量を超過する状況を回避できます。 最小値は1日、最大値は1000日です。
TCPクライアントコネクタ	**TCPクライアントコネクタ**を選択した場合は、次の設定を指定します。 • **ホスト名**:トランザクションソースに関連付けられたTCPサーバーのホスト名を入力します。 • **ポート**:トランザクションソースに関連付けられたTCPサーバーのポート名を入力します。
シリアルポートコネクタ	**シリアルポートコネクタ**を選択した場合は、設定を指定し、トランザクションソースの設定と一致するようにします。 • **シリアルポート**:COMポートを選択します。 • **ボーレート**:1秒当たりに転送されるビット数を指定します。 • **パリティ**:転送のエラー検出方法を指定します。デフォルトでは、**なし**が選択されています。 • **データビット**:データの1文字を表すために使用されるビット数を指定します。

名前	説明
	• **停止ビット**: 1バイトが転送されるタイミングを示すビット数を指定します。ほとんどのデバイスでは1ビットが必要です。 • **ハンドシェイク**: トランザクションソースとイベントサーバー間の通信プロトコルを決定するハンドシェイク方式を指定します。

トランザクション定義(トランザクトノード)

トランザクションソースに使用する定義のプロパティについて下表で説明します。

トランザクション定義の作成と追加について詳しくは、「トランザクション定義を作成および追加」を参照してください。

トランザクション定義(プロパティ)

名前	説明
名前	名前を入力します。
エンコード	レジなどのトランザクションソースで使用される文字セットを選択します。これによりXProtect Transactは、定義を構成する際に、処理できる理解可能なテキストにトランザクションデータを変換できます。 誤ったエンコードを選択すると、データが文字化けして表示される場合があります。
データ収集を開始	接続されたトランザクションソースからトランザクションデータを収集します。データを使用して、トランザクション定義を構成できます。 少なくとも1つ、できれば複数のトランザクションが完了するまで待ちます。
データ収集を停止	定義を構成するのに十分なデータを収集したら、このボタンをクリックします。
ファイルから読み込む	すでに存在するファイルからデータをインポートするには、このボタンをクリックします。典型的には、これは、.captureファイル形式で以前に作成されたファイルです。他のファイル形式にすることもできます。ここで重要なことは、インポートファイルのエンコードが、現在の定義で選択されたエンコードと一致することです。
ファイルに保存	収集された元データをファイルに保存するには、このボタンをクリックします。データは後から再利用できます。
一致タイプ	収集された元データの開始パターンと停止パターンを検索するために使用する一致タイプを選択します。

名前	説明
	• 完全一致を使用：この検索は**開始パターン**と**終了パターン**フィールドに入力したものと同一の内容を含む文字列を特定します。 • ワイルドカードを使用：この検索はワイルドカード記号(*、#、?)を組み合わせ、**開始パターン**と**終了パターン**フィールドに入力したものと同一の内容を含む文字列を特定します。 *は任意の文字数と一致します。例えば、「Start tra*tion」と入力すると、「Start transaction」を含む文字列を特定します。 #は1桁と一致します。例えば、「# watermelon」と入力すると、「1 watermelon」などを含む文字列を特定します。 ?は厳密に1文字と一致します。例えば、検索式「Start trans?ction」を使用して、「Start transaction」を含む文字列を特定できます。 • 正規表現を使用：この一致タイプを使用すると、日付形式やクレジットカード番号などの特定の表記方法や規則を含む文字列を特定します。詳細については、Microsoftのウェブサイト(https://docs.microsoft.com/dotnet/standard/base-types/regular-expression-language-quick-reference/) を参照してください
元データ	接続されたトランザクションソースのトランザクションデータ文字列がこのセクションに表示されます。
開始パターン	トランザクションの開始位置を示す開始パターンを指定します。**プレビュー**フィールドには横線が挿入され、トランザクションの開始および終了位置を視覚的に示し、それぞれのトランザクションを区切ります。
停止パターン	トランザクションの停止位置を示す停止パターンを指定します。停止パターンは必須ではありませんが、実際のトランザクション間で、受信されたデータに開始時間または特別キャンペーンなどの無関係なデータが含まれる場合に便利です。 停止パターンを指定しない場合、レシートの終了は次のレシートの開始場所として定義されます。開始は、**開始パターン**フィールドに入力された内容によって決まります。
フィルターを追加	**フィルターを追加**ボタンを使用して、XProtect Smart Clientで省略するか、他の文字または改行に置換する文字を指定します。 トランザクションソース文字列に出力しない制御文字が含まれている場合は、文字の置換が有益です。XProtect Smart Clientのレシートをオリジナルのレシートと同様に表示するには、改行を追加する必要があります。
テキストをフィルター	**元データ**セクションで現在選択されている文字を表示します。省略または置換する文字を認識し、それが収集された元データ文字列に含まれていない場合は、手動で**文字**フィールドに文字を入力できます。 文字が制御文字の場合は、16進数のバイト値を入力する必要があります。バイト値では次の形式

名前	説明
	を使用します。1文字に複数バイトがある場合は{XX}および{XX,XX,...}。
アクション	追加するフィルターごとに、選択した文字の処理方法を指定してください。 • 省略:選択した文字は除外されます。 • 置換:選択した文字は、指定した文字で置換されます。 • 改行を追加:選択した文字は改行で置換されます。
置換	選択した文字と置き換えるテキストを入力します。**置換**アクションを選択した場合にのみ、使用されます。
フィルターテキストとして定義されていない制御文字を削除	フィルター追加後も削除されていない印刷されない文字を削除します。 **元データ**ペインと**プレビュー**セクションで、この設定を有効または無効にした際にトランザクションデータ文字列がどのように変化するのか確認します。
プレビュー	**プレビュー**セクションを使用して、不要な文字が特定、削除されたことを確認します。ここに表示される出力は、XProtect Smart Clientでの実際のレシートと見た目が似ています。

アラームノード

アラーム定義(アラームノード)

システムがイベントをシステムに登録する際は、システムをXProtect Smart Clientでアラームを生成するように設定できます。これらを使用する前にアラームを定義する必要があります。アラームはシステムサーバーに登録したイベントに基づき定義してください。また、ユーザー定義イベントを使用してアラームを起動したり、同じイベントを使用して複数の異なるアラームを起動することも可能です。

アラーム定義の設定:

名前	説明
有効	既定では、アラーム定義は有効です。無効にするには、チェックボックスをオフにします。
名前	アラームの名前は一意である必要はありませんが、一意で分かりやすい名前を使用すると、多くの場合に便利です。
手順	アラームに関する説明や、アラームの原因となる問題を解決する方法に関する説明テキストを入力します。

名前	説明
	ユーザーがアラームを処理すると、テキストがXProtect Smart Clientで表示されます。
イベントの起動	アラームが起動された時に使用するイベントメッセージを選択します。2つのドロップダウンメニューから選択します: • 1つ目のドロップダウン: アナリティクスイベントやシステムイベントなどのイベントのタイプを選択します。 • 2つ目のドロップダウン: 使用する特定のイベントメッセージを選択します。使用可能なメッセージは、最初のドロップダウンメニューで選択したイベントタイプによって決定されます。
ソース	イベントが発生するソースを指定します。VCAやMIPなどのプラグインで定義したソースもまた、カメラなどのデバイスに並ぶソースとなり得ます。選択できるオプションは、選択したイベントのタイプにより異なります。

アラーム起動:

名前	説明
時間プロファイル	**時間プロファイル**ラジオボタンを選択して、アラーム定義がアクティブな時間間隔を指定します。**ルールとイベント**ノードで定義した時間設定だけが一覧に表示されます。何も定義されていない場合は、**常時**オプションのみを使用できます。
対象のイベント	イベントに基づくアラームにするには、このラジオボタンを選択します。選択した後には、開始イベントと停止イベントを指定します。カメラ、ビデオサーバー、入力で定義されているハードウェアイベントを選択できます。イベント概要もあわせて参照してください。グローバル/手動イベントも使用できます。ユーザー定義イベント(説明付き)も参照してください。

オペレータのアクションが必要:

名前	説明
時間制限	オペレータのアクションが必要になる時間制限を選択します。デフォルトは1分です。**起動されたイベント**ドロップダウンメニューでイベントを登録するまで、時間制限はアクティブになりません。
起動されたイベント	時間制限が経過した場合に、どのイベントを起動するか選択します。

マップ:

名前	説明
アラームマネージャービュー	アラームがXProtect Smart Client>**アラームマネージャー**にリストされている際に、スマートマップまたはマップのいずれかをアラームに割り当てます。 スマートマップには、デバイスで起動された場合、およびデバイスがスマートマップに追加された場合にアラームが表示されます。

その他:

名前	説明
関連するカメラ	カメラ自体がアラームを起動しない場合でも、15台までアラーム定義に含めるカメラを選択します。例えば外部イベントメッセージ(ドアが開いているなど) をアラームのソースとして選択している場合です。ドア付近のカメラを1台または複数定義することで、定義したカメラの録画のインシデントをアラームに関連付けることができます。
初期アラームの所有者	アラームに対して責任を負うデフォルトのユーザーを選択します。
初期アラームの優先度	アラームの優先度を選択します。これらの優先度はXProtect Smart Clientで使用し、アラームの重要度を決定します。
アラームのカテゴリ	アラームのカテゴリ、例えば**誤警報**または**要調査**を選択します。
アラームで起動されるイベント	XProtect Smart Clientでアラームが起動できるイベントを定義します。
アラームを自動で閉じる	特定のイベントによってアラームを自動的に停止する場合は、このチェックボックスを選択します。すべてのイベントがアラームを起動するわけではありません。最初から新しいアラームを無効にしたい場合は、チェックボックスを選択解除します。
管理者にアサインできるアラーム	**アサイン先**リストで管理者の役割のあるユーザーを含めるようチェックボックスを選択します。。 **アサイン先**リストは、XProtect Smart Clientの**アラームマネジャー**タブのアラーム詳細にあります。 チェックボックスをクリアすると、管理者の役割があるユーザーを**アサイン先**リストからフィルターアウトして、リストを短縮できます。

アラームデータ設定(アラームノード)

アラームデータ設定を行う際には、以下を指定します。

アラームデータレベルタブ

優先度

名前	説明
レベル	選択したレベル番号の新しい優先度を追加するか、デフォルトの優先度レベル(1、2、3などの数) を使用/編集します。これらの優先度レベルは、**初期アラームの優先度**設定を行うために使用されます。
名前	エンティティの名前を入力します。必要な数だけ作成できます。
サウンド	アラームに関連付ける音声を選択します。**音声の設定**で、デフォルトの音声を使用するか、さらに追加します。
音声をリピート	音声を1回だけ再生するか、XProtect Smart Clientでオペレータがアラームリストの中のアラームをクリックするまで繰り返すかを決めます。
デスクトップ通知を有効にする	デスクトップ通知はアラームの優先度ごとに有効/無効にできます。XProtectプロファイルに対応しているSmart Client VMSを使用している場合は、必須Smart Clientプロファイルでも通知を有効にする必要があります。444ページのアラームマネージャータブ(Smart Clientプロファイル) を参照してください。

ステータス

名前	説明
レベル	デフォルトのステータスレベル(番号**1**、**4**、**9**、**11**、これらは編集または再利用は不可) に加えて、選択したレベル番号の新しいステータスを追加します。このようなステータスレベルは、XProtect Smart Clientのアラームリストにのみ表示されます。

カテゴリ

名前	説明
レベ	選択したレベル番号の新しいカテゴリを追加します。これらのカテゴリレベルは、**初期アラームの優先度**設定を行

名前	説明
ル	うために使用されます。  レベル99は、XProtect Mobileクライアントの緊急アラートアラーム用に予約されています。
名前	エンティティの名前を入力します。必要な数だけ作成できます。

アラームリストの設定タブ

名前	説明
使用できる列	「>」を使用して、XProtect Smart Clientのアラームリストに表示すべき列を選択します。「<」を使用して選択をクリアします。完了したら**選択した列**には、含めるアイテムが表示されます。

処理済みにする理由タブ

名前	説明
有効にする	すべてのアラームを処理済みにする前に、処理済みにする理由を割り当てる必要があるようにするには、選択して有効にします。
理由	アラームを処理済みにする際にユーザーが選択できる、処理済みにする理由を追加します。例えば、*解決済み-侵入者*または*誤検知*などがあります。必要な数だけ作成できます。

音声の設定(アラームノード)

音の設定を行う際には、以下を指定します。

名前	説明
音声	アラームに関連付けられる音声を選択します。音声リストには、デフォルトのWindows音声が多数含まれていま

名前	説明
	す。新しい音声(.wavまたは.mp3)を追加することもできます。
追加	音声を追加します。音声ファイルをブラウズし、1つ以上の.wavまたは.mp3ファイルをアップロードします。
削除	選択された音を、手動で追加された音の一覧から削除します。デフォルト音は削除できません。
テスト	音をテストします。リストから音を選択します。音が1回再生されます。

フェデレーテッドサイト階層

フェデレーテッドサイトのプロパティ

このセクションでは**一般**タブと**ペアレントサイト**タブについて説明します

一般タブ

現在ログインしているサイトに関連する情報の一部を変更することができます。

名前	説明
名前	サイトの名前を入力します。
説明	サイトの説明を入力します。
URL	リストを使用してこのサイトのURLを追加および削除し、URLが外部URLかどうかを示します。外部アドレスが、ローカルネットワークの外部から到達可能である。
ﾊﾞｰｼﾞｮﾝ	サイトのマネジメントサーバーのバージョン番号。
サービスアカウント	マネジメントサーバーが実行されているサービスアカウント。
最後に同期化した時間	階層の最後の同期化の時刻と日付。
最後の同期時のステータス	階層の最後の同期化のステータス。これは、**成功**または**失敗**のいずれかです。

親サイトタブ

このタブは、現在ログインしているサイトの親のサイトに関する情報を表示します。サイトに親サイトがなければ、タブは表示されません。

名前	説明
名前	親サイトの名前を入力します。
説明	親サイトの説明を表示します(オプション) 。
URL	親サイトのURLを一覧表示し、URLが外部URLであるかどうかを示します。外部アドレスが、ローカルネットワークの外部から到達可能である。
ﾊﾞｰｼﾞｮﾝ	サイトのマネジメントサーバーのバージョン番号。
サービスアカウント	マネジメントサーバーが実行されているサービスアカウント。
最後に同期化した時間	階層の最後の同期化の時刻と日付。
最後の同期時のステータス	階層の最後の同期化のステータス。これは、**成功**または**失敗**のいずれかです。

helpfeedback@milestone.dk

Milestoneについて

Milestone Systemsはオープンプラットフォームのビデオ管理ソフトウェア(VMS)の世界有数のプロバイダーです。お客様の安全の確保、資産の保護を通してビジネス効率の向上に役立つテクノロジーを提供しています。Milestone Systemsは、世界の15万以上のサイトで実証された高い信頼性と拡張性を持つソリューションにより、ネットワークビデオ技術の開発と利用におけるコラボレーションとイノベーションを促進するオープンプラットフォームコミュニティを形成しています。Milestone Systemsは、1998年創業、Canon Group傘下の独立企業です。詳しくは、https://www.milestonesys.com/をご覧ください。