

MAKE THE  
WORLD SEE

# Milestone Systems

---

XProtect® Mobileサーバー 2021 R2

システム管理者マニュアル



## 目次

著作権、商標、および免責条項 .....	5
サポートされるVMS製品とバージョン .....	6
概要 .....	7
XProtect Mobile（説明付き） .....	7
XProtect Mobileサーバー（説明付き） .....	7
製品比較チャート .....	7
要件と注意事項 .....	11
XProtect Mobileを使用するための要件 .....	11
XProtect Mobileシステム要件 .....	11
通知設定の要件 .....	11
スマートコネクト設定の要件 .....	12
ユーザーの2段階認証設定の要件 .....	12
ビデオプッシュ 設定の要件 .....	12
ダイレクトストリーミングの要件 .....	12
インストール .....	13
XProtect Mobileサーバーをインストール .....	13
設定 .....	16
モバイルサーバーの設定 .....	16
一般タブ .....	16
接続タブ .....	19
[サーバーのステータス]タブ .....	21
パフォーマンスタブ .....	22
調査 .....	25
ビデオプッシュタブ .....	27
通知タブ .....	28
要素認証タブ .....	29
ダイレクトストリーミング（説明付き） .....	31
アダプティブストリーミング（説明付き） .....	32

安全な通信 (説明付き) .....	33
サーバーの暗号化を管理(説明付き) .....	34
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を暗号化 (説明付き) .....	35
マネジメントサーバーとData Collector server間の暗号化 (説明付き) .....	36
レコーディングサーバーからデータを取得しているクライアントとサーバーを暗号化 (説明付き) .....	38
レコーディングサーバー データ 暗号化 (説明付き) .....	40
クライアントに対するモバイルサーバー暗号化の条件 .....	41
Milestone Federated Architectureおよびマスター/スレーブサーバー (説明付き) .....	41
スマートコネク (説明付き) .....	41
Smart Connectの設定 .....	42
ルーターでのUniversal Plug and Playの検出可能性を有効化 .....	42
複雑なネットワークでの接続を有効にする .....	42
接続設定の構成 .....	43
電子メールメッセージをユーザーに送信する .....	43
通知の送信 (説明付き) .....	43
XProtect Mobileサーバーでプッシュ通知を設定 .....	44
特定のモバイルデバイスまたはすべてのモバイルデバイスへのプッシュ通知の送信を有効化する .....	45
特定の、またはすべてのモバイルデバイスへのプッシュ通知の送信を停止する .....	45
調査の設定 .....	45
ビデオプッシュを使用したビデオのストリーミング (説明付き) .....	47
ビデオを流すための「ビデオ・プッシュ」の設定 .....	47
ビデオプッシュ・チャンネルをストリーミングビデオに追加 .....	47
ビデオ プッシュ チャンネルの編集 .....	48
ビデオプッシュチャンネルの追加 .....	48
パスワードの変更 .....	48
ビデオプッシュドライバーをハードウェアデバイスとしてに追加するRecording Server .....	49
ビデオプッシュドライバー デバイスをビデオプッシュのためのチャンネルに追加します。 .....	50
既存のビデオプッシュチャンネルに対し音声を有効化する .....	50
電子メールを使用して2段階認証の設定を行います。 .....	51
SMTPサーバーに関する情報を入力します。 .....	51

ユーザーに送られてくる認証コードを指定します。 .....	52
ユーザーとActive Directoryグループにログイン方法を割り当てます。 .....	52
アクション（説明付き） .....	53
XProtect MobileクライアントおよびXProtect Web Clientで使用する出力の名前を決める（説明付き） .....	53
<b>メンテナンス .....</b>	<b>54</b>
Mobile Server Manager（説明付き） .....	54
XProtect Web Clientへのアクセス .....	54
Mobile Serverサービスの起動、停止、再起動 .....	55
データ保護パスワードを変更 .....	55
ポート番号の表示/編集 .....	56
モバイルサーバーで暗号化を有効にする .....	56
ロゴへのアクセスおよび調査（説明付き） .....	57
調査フォルダーを変更 .....	58
ステータスの表示（説明付き） .....	59
<b>トラブルシューティング .....</b>	<b>60</b>
XProtect Mobileトラブルシューティング .....	60

## 著作権、商標、および免責条項

Copyright © 2021 Milestone Systems A/S

### 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

この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危険の責任はすべてその使用者にあるものとします。また、ここに記載されている内容はいずれも、いかなる事項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、特定の契約条件が適用される可能性があるサードパーティ製ソフトウェアを使用することがあります。その場合、詳細はお使いの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。

## サポートされるVMS製品とバージョン

このマニュアルでは、次のXProtectVMS製品によりサポートされる機能が記載されています。

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

Milestoneこのマニュアルに記載されている機能を、XProtect現在のリリースバージョンと以前の2つのリリースバージョンの上記のVMS製品でテストします。

新しい機能が現在のリリースバージョンでのみサポートされており、以前のリリースバージョンではサポートされていない場合は、機能の説明にこれに関する情報が記載されています。

下記の廃止されたXProtectVMS製品でサポートされているXProtectクライアントとアドオンのドキュメントは、Milestoneダウンロードページ (<https://www.milestonesys.com/downloads/>) に掲載されています。

- XProtect Enterprise
- XProtect Professional
- XProtect Express
- XProtect Essential

## 概要

### XProtect Mobile（説明付き）

XProtect Mobileは5つのコンポーネントから成り立っています。

- XProtect Mobileクライアント

XProtect MobileクライアントはAndroidまたは Apple デバイスでインストールするモバイル サーヴェイランス アプリを使用できます。XProtect Mobile任意の数のクライアントのインストールを使用できます。

- XProtect Web Client

XProtectWebClientでは、お使いのWebブラウザでライブビデオを閲覧でき、録画もダウンロードできます。XProtectWebClientは、XProtectMobileサーバーのインストール時に一緒に自動的にダウンロードされます。

- XProtect Mobileサーバー
- XProtect Mobileプラグイン
- Mobile Server Manager

XProtect MobileサーバーXProtect Mobileとプラグイン、およびにMobile Server Managerについては、このマニュアルで説明します。

### XProtect Mobileサーバー（説明付き）

XProtect Mobileサーバーは、XProtect MobileクライアントまたはXProtect Web Clientからのシステムへのログインを処理する役割があります。

XProtect Mobileサーバーは、レコーディングサーバーから送られたビデオストリームをXProtect MobileクライアントまたはXProtect Web Clientに配信する役割を担います。これにより、レコーディングサーバーのインターネットへの接続を伴わない、安全なセットアップが可能です。XProtect Mobileサーバーがレコーディングサーバーからビデオストリームを受信すると、コーデックとフォーマットの複雑な変換を処理し、モバイルデバイス上でビデオストリーミングできます。

XProtect Mobileサーバーは、レコーディングサーバーへのアクセスに使用したい、すべてのサーバーにインストールする必要があります。XProtect Mobileサーバーをインストールする際には、管理者権限を持つアカウントを使用してログインします。そうでない場合、インストールは正常に完了しません（[ページ13のXProtect Mobileサーバーをインストール](#)を参照）。

XProtect Mobileサーバーは、ライブモードでのダイレクトストリーミングとアダプティブストリーミングに対応しています（XProtect ExpertおよびXProtect Corporateのみ）。

### 製品比較チャート

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+

機能に関する詳細リストは、Milestone Webサイトの製品概要ページ (<https://www.milestonesys.com/solutions/platform/product-index/>) で閲覧できます。

下記は各製品の主な違いのリストです。

名前	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
SLC (ソフトウェアライセンスコード) 別の施設	1	1	[複数サイト]	[複数サイト]	[複数サイト]
SLCあたりのレコーディングサーバー	1	1	無制限	無制限	無制限
レコーディングサーバーあたりのハードウェアデバイス	8	48	無制限	無制限	無制限
Milestone Interconnect™	-	リモートサイト	リモートサイト	リモートサイト	中央/リモートサイト
Milestone Federated Architecture™	-	-	-	リモートサイト	中央/リモートサイト
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とホットスタンバイ	コールドスタンバイとホットスタンバイ
リモート接続サービス	-	-	-	-	✓
エッジストレージサポート	-	-	✓	✓	✓
マルチステージビデオスト	ライブデー	ライブ	ライブデータ	ライブデー	ライブデー



名前	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
レージ	データベース + 1アーカイブ	データベース + 1アーカイブ	ベース + 1アーカイブ	データベース + 無制限のアーカイブ	データベース + 無制限のアーカイブ
SNMPトラップ (通知)	-	-	-	✓	✓
時間制限のあるユーザーアクセス権	-	-	-	-	✓
フレームレートの低減 (グルーミング)	-	-	-	✓	✓
ビデオデータ暗号化 (レコーディングサーバー)	-	-	-	✓	✓
データベース署名 (レコーディングサーバー)	-	-	-	✓	✓
PTZ優先レベル	1	1	3	32000	32000
拡張PTZ (PTZセッションとXProtect Smart Clientからのパトロールを予約)	-	-	-	✓	✓
エビデンスロック	-	-	-	-	✓
ブックマーク機能	-	-	手動のみ	手動およびルールベース	手動およびルールベース
ライブマルチストリーミングまたはマルチキャスト (アダプティブストリーミングとも)	-	-	-	✓	✓

名前	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
直接ストリーミング	-	-	-	✓	✓
セキュリティ全般	クライアントのユーザー権限	クライアントのユーザー権限	クライアントのユーザー権限	クライアントのユーザー権限	クライアントのユーザー権限/ 管理者のユーザー権限
XProtect Management Clientプロファイル	-	-	-	-	✓
XProtect Smart Clientプロファイル	-	-	3	3	無制限
XProtect Smart Wall	-	-	-	オプション	✓
システムモニター	-	-	-	✓	✓
スマートマップ	-	-	-	✓	✓
2要素認証	-	-	-	-	✓
DLNAサポート	-	✓	✓	✓	✓
プライバシーマスク	-	✓	✓	✓	✓
デバイスのパスワード管理			✓	✓	✓
メディアデータベースエクスポートの暗号化（モバイルサーバー）	✓	✓	✓	✓	✓
メディアデータベースエクスポートのデジタル署名（モバイルサーバー）	✓	✓	✓	✓	✓

## 要件と注意事項

### XProtect Mobileを使用するための要件

XProtect Mobileの使用を開始する前に、次のアイテムが準備されていることを確認する必要があります。

- 1つ以上のユーザーでインストールおよび構成された実行中のVMS。
- XProtect Smart Clientで設定されたカメラとビュー。
- XProtect Mobileクライアント アプリケーションがダウンロードできるGoogle PlayまたはApp StoreへアクセスできるAndroidまたはiOSのモバイル デバイス
- 実行するWebブラウザXProtect Web Client

要件に関する詳細は、[ページ11のXProtect Mobileシステム要件](#)をご覧ください。

### XProtect Mobileシステム要件

各種システム コンポーネントの最低システム要件については、Milestone Webサイト (<https://www.milestonesys.com/systemrequirements/>) をご覧ください。

- XProtect Mobileクライアントの要件を検索するには、**XProtect Mobile**製品アイコンを選択してください
- XProtect Web Clientのための要件を確認するには、製品アイコン**XProtect Web Client**を選択してください
- XProtect Mobileサーバーの要件を検索するには、インストールしたXProtect製品のアイコンを選択してください
- XProtect Mobileプラグインの要件:
  - 実行中のManagement Client
  - Milestoneプラグインがインストールされ、VMSと統合します。

### 通知設定の要件

- 1つ以上のアラームを1つ以上のイベントとルールに関連付ける必要があります。これはシステム通知では必要ありません。
- Milestone Systemsとの契約が最新であることMilestone Care™を確認します。
- インターネット接続があることを確認します

詳細については以下を参照してください：

[ページ44のXProtect Mobileサーバーでプッシュ通知を設定](#)

[ページ28の通知タブ](#)

## スマートコネクト設定の要件

- XProtect Mobileサーバーは、パブリックIPアドレスを使用する必要があります。アドレスは静的または動的なものが可能ですが、一般的に静的IPアドレスを使用することをお勧めします。
- スマートコネクトの有効なライセンスが必要です

## ユーザーの2段階認証設定の要件

- SMTPサーバーが設置されていること。
- ユーザーおよびグループが **サイトナビゲーションペイン**の役割ノードXProtectのManagement Clientでシステムに追加されていること。関連する役割で、**ユーザーおよびグループ**タブを選択します。
- システムを以前のバージョンのXProtectからアップグレードした場合、モバイルサーバーを再起動して2要素認証機能を有効にしなければなりません。

詳細については以下を参照してください：

[ページ51の電子メールを使用して2段階認証の設定を行います。](#)

[ページ29の要素認証タブ](#)

## ビデオプッシュ 設定の要件

- 各チャンネルでデバイスライセンスが一つ必要です
- ビデオプッシュで音声を有効にするには:
  1. Milestone XProtect Device Packのバージョン 10.3a以降をダウンロードしてインストールします。
  2. XProtectMobileServerInstaller.exeのバージョン13.2a以降をダウンロードしてインストールします。
  3. Recording Serverサービスを再起動します。

## ダイレクトストリーミングの要件

XProtect Mobileは、ライブモードでのダイレクトストリーミングに対応しています（XProtect ExpertおよびXProtect Corporateのみ）。

### 直接ストリーミングのカメラ構成要件

XProtect Web ClientおよびXProtect Mobileクライアントでダイレクトストリーミングを使用するには、以下のカメラ構成が必要となります。

- カメラがH.264コーデック（すべてのクライアント用）またはH.265コーデック（XProtect Mobileクライアント専用）に対応している
- **GOPサイズ**の値には**1秒**を設定し、**FPS**には**10 FPS**を上回る値を設定することが推奨されます。

# インストール

## XProtect Mobileサーバーをインストール

XProtect Mobileサーバーをインストールすると、XProtect MobileクライアントとXProtect Web Clientを自分のシステムで使用できるようになります。マネジメンサーバーを実行するコンピュータのシステムリソースの使用量を全体的に減らすには、個別のコンピュータ上にXProtect Mobileサーバーをインストールします。

マネジメンサーバーには、ビルトインの公開インストールWebページがあります。このWebページでは、システム管理者およびエンドユーザーが、マネジメンサーバーまたは他のすべてのシステムのコンピュータから必要なXProtect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。



「ひとつのコンピュータ」オプションをインストールすると、XProtect Mobileサーバーは自動でインストールされます。

XProtect Mobileサーバーをインストールするには:

1. ブラウザに次の URL を入力します。 `http:// [マネジメンサーバーアドレス] /installation/admin` [マネジメンサーバーアドレス] は、マネジメンサーバーのIPアドレスまたはホスト名です。
2. サーバー・インストーラーの**すべての言語**XProtect Mobileをクリックします。
3. ダウンロードしたファイルを実行します。すべての警告で**[はい]**をクリックします。解凍が開始します。
4. インストーラーの言語を選択してください。その後、**[続行]** をクリックします。
5. 使用許諾契約を読み、同意します。その後、**[続行]** をクリックします。
6. インストールの種類を選択:
  - XProtect Mobileサーバーとプラグインをインストールするには、**[標準]**をクリックします。
  - サーバーのみ、またはプラグインのみをインストールするには、**カスタム**をクリックします。たとえば、Management Clientを使ってXProtect Mobileサーバーを管理したいものの、コンピュータ上でXProtect Mobileサーバーが不要な場合は、プラグインのみをインストールすると便利です。



Management ClientでXProtect Mobileサーバーを管理するには、Management Clientを実行しているコンピュータ上でXProtect Mobileプラグインが必要です。

7. カスタムインストールのみ：インストールしたいコンポーネントを選択します。その後、**[続行]** をクリックします。

8. モバイルサーバーのサービスアカウントを選択します。その後、**[続行]** をクリックします。



後の段階でサービスアカウント資格情報を変更または編集する場合、モバイルサーバーの再インストールが必要となります。

9. **[サーバーURL]** フィールドに、プライマリマネジメントサーバーのアドレスを入力します。
10. カスタムインストールのみ：モバイルサーバーと通信する接続ポートを指定します。その後、**[続行]** をクリックします。



通常のインストールでは、通信ポートにはデフォルトのポート番号が与えられます (HTTPポートが8081、HTTPSポートが8082)。

11. **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。

12. モバイルサーバーの暗号化を指定します。その後、**[続行]** をクリックします。

**暗号化を選択** ページでは、通信フローを安全に保護できます。

- モバイルサーバーと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。内部通信フローの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
- 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モバイルサーバーとクライアント間の暗号化を有効にする場合は、**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



暗号化を有効にしないと、クライアントでいくつかの機能が利用できなくなります。詳しくは、[クライアントに対するモバイルサーバーの暗号化の条件](#)をご参照ください。

システムで安全な通信を確立する方法の詳細については、以下を参照してください：

- [レコーディングサーバー データ 暗号化 \(説明付き\)](#)
- [証明書に関するMilestoneガイド](#)

お使いのオペレーティングシステムのタスクバーにあるMobile Server Managerトレイアイコンからインストールを完了した後も、暗号化を有効にすることができます。( [ページ56のモバイルサーバーで暗号化を有効にする](#)を参照)

13. ファイルの場所と製品の言語を選択し、**インストール**をクリックします。
14. インストールが完了すると、インストールされたコンポーネントのリストが表示されます。その後、**[閉じる]**をクリックします。

XProtect Mobileの設定の準備が整いました ( [ページ16のモバイルサーバーの設定](#)を参照)。

## 設定

### モバイルサーバーの設定

ManagementClientでは、XProtectMobileサーバー設定のリストを作成して編集できます。この設定には、モバイルサーバーの**プロパティ**セクションの最下部にあるツールバーでアクセスできます。ここからは、次のことができます：

- サーバー機能の一般構成の有効化または無効化（[ページ16の一般タブ](#)を参照）
- サーバー接続設定を行う（[ページ19の接続タブ](#)を参照）
- スマートコネクト機能を設定する（[ページ19の接続タブ](#)を参照）
- サーバーの現在のステータスとアクティブなユーザーの一覧を表示（[ページ21の\[サーバーのステータス\]タブ](#)を参照）
- パフォーマンスパラメーターを設定することで、ダイレクトストリーミングまたはアダプティブストリーミングを有効にしたり、トランスコード化したビデオストリーミングの制限を設定したりできます（[ページ22のパフォーマンスタブ](#)を参照）
- 調査設定の構成（[ページ25の調査](#)を参照）
- ビデオプッシュ設定の構成（[ページ27のビデオプッシュタブ](#)を参照）
- システム通知とプッシュ通知の設定、およびオン、オフの切り替え（[ページ28の通知タブ](#)を参照）
- ユーザー向けの追加ログインステップの有効化および設定（[ページ29の要素認証タブ](#)を参照）

### 一般タブ

次の表では、このタブの設定について説明します。

#### 一般

名前	説明
サーバー名	XProtect Mobileサーバーの名前を入力します。
説明	オプションで、XProtect Mobileサーバーの説明を入力します。
モバイルサーバー	現在選択中のXProtect Mobileサーバーの名前を確認します。



名前	説明
ログイン方法	<p>ユーザーがサーバーにログインするときに使用する認証方法を選択します。次から選択できます。</p> <ul style="list-style-type: none"> <li>• 自動</li> <li>• Windows認証</li> <li>• 基本認証</li> </ul>

## 機能

XProtect Mobileの機能をどのように管理するかについて下表に記します。

名前	説明
XProtect Web Clientを有効化	XProtect Web Clientへのアクセスを有効にします。この機能はデフォルトでは有効になっています。
[すべてのカメラ]ビューを有効にする	[すべてのカメラ]ビューを含めます。このビューには、レコーディングサーバーでユーザーが閲覧できるカメラがすべて表示されます。この機能はデフォルトでは有効になっています。
ブックマークを有効にする	ブックマーク機能を有効にして、XProtect MobileクライアントとXProtect Web Clientでビデオシーケンスをすばやく見つけます。この機能はデフォルトでは有効になっています。
アクションを有効（出力およびイベント）	XProtect MobileクライアントおよびXProtect Web Clientでアクションへのアクセスを有効にします。この機能はデフォルトでは有効になっています。 この機能を無効にすると、クライアントユーザーは出力とイベントを（たとえこれらが適切に構成されていても）表示することはできません。
インカム音声を使用可能にする	XProtect Web ClientとXProtect Mobileクライアントで受信音声機能を有効にします。この機能はデフォルトでは有効になっています。
プッシュ・トゥ・トークを使用可能	XProtect Web ClientとXProtect Mobileクライアントで、プッシュ・トゥ・トーク（PTT）機能を有効にします。この昨日はデフォルトで使用可能で

名前	説明
にする	す。
<b>XProtect Mobileサーバーへの組み込みシステム管理者役割アクセスを拒否</b>	組み込まれたシステム管理者役割に割り当てられたユーザーがXProtect MobileクライアントあるいはXProtect Web Clientのビデオにアクセスすることの除外を有効にします。

### ログ設定

ログ設定情報を見ることができます。

名前	説明
<b>ログファイルの場所</b>	システムがログファイルを保存する場所を指定します。
<b>ログの保存期間</b>	ログを保持する日数を確認します。デフォルトは30日です。

### 設定のバックアップ

システムに複数のXProtect Mobileサーバーがある場合、バックアップ機能を使って既存の設定をエクスポートし、その他のXProtect Mobileサーバーにそれらをインポートします。

名前	説明
<b>インポート</b>	新規XProtect Mobileサーバー構成でXMLファイルをインポートします。
<b>エクスポート</b>	XProtect Mobileサーバー構成をエクスポートします。システムは、構成をXMLファイルに保存しています。

## 接続タブ

接続タブの設定は次のタスクで使用できます。

- [ページ43の接続設定の構成](#)
- [ページ43の電子メールメッセージをユーザーに送信する](#)
- [ページ42の複雑なネットワークでの接続を有効にする](#)
- [ページ42のルーターでのUniversal Plug and Playの検出可能性を有効化](#)

詳細については、「[ページ41のスマートコネクト（説明付き）](#)」を参照してください。



インストール中、**Server Configurator**を開いた際にXProtect MobileクライアントとXProtect Web ClientユーザーがXProtect Mobileサーバーに接続する方法を設定できます。インストール後にMobile Server Managerトレイアイコンを右クリックすることも可能です。接続タイプはHTTPSまたはHTTPのいずれかになります。詳細については、[ページ56のモバイルサーバーで暗号化を有効にする](#)を参照してください。

### 一般

名前	説明
クライアントタイムアウト	XProtect MobileクライアントおよびXProtect Web Clientが、自らが実行中であることをXProtect Mobileサーバーに表示すべき時間枠を設定します。デフォルト値は30秒です。  Milestoneでは、この時間枠を長くしないことを推奨しています。
UPnP検出を有効にする	これによってXProtect MobileサーバーがUPnPプロトコルを用いてネットワーク上で発見可能になります。  XProtect Mobileクライアントは、UPnPに基づいてXProtect Mobileサーバーを見つけるためのスキャン機能を有しています。
自動ポートマッピングを有効にする	XProtect Mobileサーバーがファイアウォールの後方にインストールされている場合、クライアントが引き続きインターネットからサーバーにアクセスできるよう、ルーターにポートマッピングが必要となります。  <b>自動ポートマッピングを有効にする</b> オプションを選択すると、XProtect Mobileサーバー自体がポートマッピングを実行できます。ただし、ルーター

名前	説明
	がこれに対応できるよう設定されていなくてはなりません。
<b>Smart Connectを有効にする</b>	Smart Connectは検証を行うためにモバイル機器やタブレットにログインせずに、XProtect Mobileサーバーが正しく設定されたことを確認できるようにします。また、クライアントのユーザーの接続プロセスを簡易化します。

### インターネットアクセス

名前	説明
<b>カスタムインターネットアクセスの構成</b>	<b>IPアドレスまたはホスト名</b> と、接続に使われるポート番号を提供します。たとえば、ルーターがUPnPをサポートしない場合や、ルーターのチェーンがある場合に、これを実行できます。
<ul style="list-style-type: none"> <li>• HTTP</li> <li>• HTTPS</li> </ul>	接続のタイプを選択します。
<b>選択するとIPアドレスを自動的に取得します</b>	IPアドレスが頻繁に変更される場合は、チェックボックスをオンにします。
<b>校正されたURLアドレスのみを使用する</b>	カスタム指定のIPアドレスまたはホスト名のみを使用してモバイルサーバーに接続するには、チェックボックスを選択します。
<b>サーバーアドレス</b>	モバイルサーバーと接続されているすべてのURLアドレスをリストアップします。

### Smart Connect通知

名前	説明
招待を電子メールで送信する:	Smart Connect通知の受信者の電子メールアドレスを入力します。
電子メール言語	電子メールで使用する言語を指定します。
Smart Connect トークン	モバイルデバイスのユーザーがXProtect Mobileサーバーに接続するために使用できる固有の識別子。
Smart Connectへのリンク	モバイルデバイスのユーザーがXProtect Mobileサーバーに接続するために使用できるリンク。

## [サーバーのステータス]タブ

XProtect Mobileサーバーにおけるステータスの詳細を見る。詳細は読み取り専用です：

名前	説明
サーバー有効化日	XProtect Mobileサーバーが前回起動したときの日付と時刻が示されます。
CPU使用率	サーバーでの現在のCPU使用状況を示します。
外部帯域幅	現在のXProtect MobileクライアントあるいはXProtect Web Clientとモバイルサーバーの間の帯域幅を示します。

### アクティブなユーザー

XProtect Mobileサーバーと現在接続されているXProtect Mobileクライアント、あるいはXProtect Web Clientサーバーのステータスの詳細を見ます。

名前	説明
ユーザー名	モバイルサーバーと接続されているXProtect Mobileクライアント、あるいはXProtect Web Clientユーザーのそれぞれのユーザー名を表示します。
ステータス	XProtect Mobileサーバーと、対象となるXProtect Mobile クライアント、あるいはXProtect Web Clientユーザーの間の現在の関係を表示します。考えられる状態： <ul style="list-style-type: none"> <li>● <b>接続済み</b> クライアントとサーバーがキーと暗号化資格情報を交換する時の最初のステータス</li> <li>● <b>ログイン</b> XProtect Mobileクライアント、あるいはXProtect Web ClientユーザーはXProtectシステムにログインしています。</li> </ul>
ビデオ帯域幅使用状況(kB/秒)	各XProtect MobileクライアントまたはXProtect Web Clientユーザーに対して現在開かれている、ビデオストリームの帯域幅の合計が示されます。
音声帯域幅使用状況(kB/秒)	各XProtect Web Clientユーザーに対して現在開かれている、音声ストリームの帯域幅の合計が示されます。
トランスコードされたビデオストリーム	各XProtect MobileクライアントまたはXProtect Web Clientユーザーに対して現在開かれている、トランスコード化ビデオストリームの総数が示されません。
ダイレクトビデオストリーム	各XProtect MobileクライアントまたはXProtect Web Clientユーザーに対して現在開かれている、ダイレクトビデオストリームの総数が示されません (XProtect ExpertおよびXProtect Corporateのみ)。
トランスコードされた音声ストリーム	各XProtect Web Clientユーザーに対して現在開かれている、トランスコード化音声ストリームの総数が示されます。

## パフォーマンスタブ

「パフォーマンス」タブでは、XProtect Mobileサーバーのパフォーマンスに対して以下の設定と制限を設けることができます。

**ビデオストリーミング設定 (XProtect ExpertおよびXProtect Corporate専用)**

名前	説明
直接ストリーミングを有効化	XProtect Web ClientおよびXProtect Mobileクライアントでの直接ストリーミングを有効にします (XProtect ExpertおよびXProtect Corporateのみ)。この機能はデフォルトでは有効になっています。
アダプティブストリーミングの有効化	XProtect Web ClientとXProtect Mobileクライアントでアダプティブストリーミングを有効にします (XProtect ExpertとXProtect Corporateの場合のみ)。この機能はデフォルトでは有効になっています。
ストリーミングモード	<p>アダプティブストリーミング機能を有効にすると、ストリーミングモードのタイプをリストから選択できるようになります。</p> <ul style="list-style-type: none"> <li>• <b>ビデオ画質の最適化 (デフォルト)</b> - 利用可能なもっとも低い解像度 (要求したものと同等またはそれ以上の解像度) を持つストリームが選択されます</li> <li>• <b>サーバーパフォーマンスの最適化</b> - 要求された解像度を低下させた後、使用可能なもっとも低い解像度 (低下したものと同等またはそれ以上の解像度) を持つストリームが選択されます</li> <li>• <b>低帯域幅用に解像度を最適化</b> - 利用可能なもっとも低い解像度を持つストリームが選択されます (3Gまたは不安定なネットワークを使用している場合に推奨)</li> </ul>

**トランスコード化ビデオストリームの制限**

**レベル1**

レベル1は、XProtect Mobileサーバーにデフォルトで設定される制限です。ここで設定した制限は、常にXProtect Mobileのトランスコード化ビデオストリームに適用されます。

名前	説明
レベル1	チェックボックスを選択すると、XProtect Mobileサーバーのパフォーマンスに第一レベルの制限が適用されます。
最大FPS	XProtect Mobileサーバーからクライアントへの送信のフレーム数/秒(FPS)の最大数について制限を設定します。
最大画像解像度	XProtect Mobileサーバーからクライアントへ送信される画像の解像度について制限を設定します。

## レベル2

レベル1でデフォルトである制限とは異なるレベルの制限を強制したい場合は、代わりに**レベル2**のチェックボックスを選択します。最初のレベルで設定したレベルより高い設定はできません。たとえば、**レベル1**で最大FPSを45に設定すると、**レベル2**では、最大FPSは44以下にしか設定できません。

名前	説明
レベル2	チェックボックスを選択すると、XProtect Mobileサーバーのパフォーマンスに第二レベルの制限が適用されます。
CPUしきい値	システムがビデオストリームの制限を強制する前に、XProtect MobileサーバーのCPU負荷について閾値を設定します。
帯域幅しきい値	システムがビデオストリームの制限を強制する前に、XProtect Mobileサーバーの帯域負荷について閾値を設定します。
最大FPS	XProtect Mobileサーバーからクライアントへの送信のフレーム数/秒(FPS)の最大数について制限を設定します。
最大画像解像度	XProtect Mobileサーバーからクライアントへ送信される画像の解像度について制限を設定します。

## レベル3



また、**レベル3**チェックボックスを選択して、制限に関する第三レベルを作成することもできます。**レベル1**および**レベル2**で設定したレベルより高い設定はできません。たとえば、**レベル1**で**最大FPS**を45に、**レベル2**で32に設定すると、**レベル3**では**最大FPS**は31以下にしか設定できません。

名前	説明
レベル3	チェックボックスを選択すると、XProtect Mobileサーバーのパフォーマンスに第一レベルの制限が適用されます。
CPUしきい値	システムがビデオストリームの制限を強制する前に、XProtect MobileサーバーのCPU負荷について閾値を設定します。
帯域幅しきい値	システムがビデオストリームの制限を強制する前に、XProtect Mobileサーバーの帯域負荷について閾値を設定します。
最大FPS	XProtect Mobileサーバーからクライアントへの送信のフレーム数/秒(FPS)について制限を設定します。
最大画像解像度	XProtect Mobileサーバーからクライアントへ送信される画像の解像度について制限を設定します。



システムは、あるレベルから別のレベルへすぐに切り替わることはありません。CPUまたは帯域の閾値の変動が指定されたレベルから5パーセント未満であれば、現在のレベルを使用し続けます。

## 調査

### 調査設定

他の人がXProtect MobileクライアントやXProtect Web Clientを使用して以下を実行できるように調査を有効にすることができます。

- 録画ビデオにアクセスする
- インシデントを調査する
- ビデオエビデンスを準備してダウンロードする

名前	説明
調査を有効にする	このチェックボックスを選択すると、ユーザーは調査を作成できます。
調査フォルダー	ビデオがハードドライブのどこにエクスポートされ保存されたかを表示します。
他のユーザーの調査を表示する	このチェックボックスを選択すると、ユーザーが自分が作成していない調査にアクセスできます。
調査フォルダーのサイズ制限を有効にします	このチェックボックスを選択すると、調査フォルダーのサイズ制限を設定し、調査フォルダーに含めることのできる最大メガバイト数を入力できます。デフォルトのサイズは2000 MBです。
調査の保存期間を有効に設定	このチェックボックスを選択すると、調査の保存期間を設定できます。初期設定の保存期間は7日間です。
エクスポートフォーマット	<p>使用したいエクスポートフォーマットのチェックボックスを選択してください。以下のエクスポートフォーマットを利用できます。</p> <ul style="list-style-type: none"> <li>• AVIフォーマット</li> <li>• XProtectフォーマット</li> <li>• MKVフォーマット</li> </ul> <p>デフォルトでチェックボックスは選択されていません。</p>
AVIエクスポートのタイムスタンプを含む	このチェックボックスを選択すると、AVIファイルがダウンロードされた日時が含まれます。
AVIエクスポートで使用されたコーデック	<p>ダウンロード用のAVIパッケージを準備するときに使用する圧縮形式を選択します。</p> <p>選択するコーデックは、オペレーティングシステムによって異なる場合があります。必要なコーデックが表示されない場合は、XProtect Mobileサーバーが稼働しているコンピュータにインストールすると、リストに追加されます。</p>
AVIのエクスポートに使用された音声のビット	エクスポートするビデオに音声が含まれている場合は、リストから適切な音声ビットレートを選択します。デフォルトは160000 Hzです。

## 調査

名前	説明
調査	システムにて現在までに設定されている調査をリストアップする。調査のこれ以上の続行を希望しない場合は、 <b>削除</b> あるいは <b>すべて削除</b> ボタンを使用します。例えば、サーバーでより多くのディスク領域が使用できるようにする場合には、これは非常に便利です。
詳細	調査用にエクスポートされた個別のビデオファイルを削除しながらその調査を保持するには、リストで調査を選択します。 <b>調査の詳細</b> グループで、エクスポート用の <b>XProtect</b> 、 <b>AVI</b> 、または <b>MKV</b> フィールドの右にある削除アイコンを選択します。

## ビデオプッシュタブ

ビデオ配信を有効にする場合、以下の設定を指定します。

名前	説明
ビデオプッシュ	モバイルサーバーでビデオ配信を有効にします。
チャンネル数	XProtectシステムで有効なビデオ配信チャンネルの数が表示されます。
チャンネル	関連するチャンネルのチャンネル数が表示されます。編集不可。
ポート	関連するビデオ配信チャンネルのポート番号。
MACアドレス	関連するビデオ配信チャンネルのMACアドレス。
ユーザー名	関連するビデオ配信チャンネルに関連するユーザー名を入力します。
カメラ名	カメラが特定されている場合、カメラの名前が表示されます。

必要なステップが完了したら（[ページ47のビデオを流すための「ビデオ・プッシュ」の設定](#)を参照）、**カメラの検索**を選択して該当するカメラを検索します。

## 通知タブ

[通知]タブを使用して、システム通知とプッシュ通知をオン/オフにします。

通知をオンにし、1つ以上のアラームとイベントが構成されている場合、XProtect Mobileはイベントが発生するとユーザーに通知します。アプリが開くと、モバイルデバイスのXProtect Mobileで通知が配信されます。プッシュ通知はXProtect Mobileを開いていないユーザーに通知します。これらの通知はモバイルデバイスに配信されます。

詳細については以下を参照：[ページ45の特定のモバイルデバイスまたはすべてのモバイルデバイスへのプッシュ通知の送信を有効化する](#)

次の表では、このタブの設定について説明します。

名前	説明
通知	このチェックボックスを選択すると、通知がオンになります。
デバイス登録の管理	このチェックボックスを選択すると、このサーバーに接続するデバイスとユーザーの情報を保存します。これらのデバイスに通知を送信します。 このチェックボックスをオフにする場合、デバイスのリストもクリアされず、ユーザーがもう一度通知の受信を開始する前に、チェックボックスを選択し、ユーザーはもう一度デバイスをサーバーに接続する必要があります。

## 登録されたデバイス

名前	説明
有効	このチェックボックスを選択すると、デバイスへの通知送信を開始します。
デバイス名	このサーバーに接続されているモバイルデバイスのリスト。 特定のデバイスへの送信を開始または停止するには、[有効]チェックボックスをオンまたはオフにします。
ユーザー	通知を受け取るユーザーの名前

## 要素認証タブ



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。詳細については、[製品比較 Webページ](#)を参照してください。

[2段階認証]タブを使用して、以下のユーザーにおける追加のログインステップを有効にして指定します。

- iOS またはAndroid モバイル デバイスのXProtect Mobileアプリ
- XProtect Web Client


認証の最初のタイプはパスワードです。もう1つのタイプは認証コードで、これらを電子メールでユーザーに送信するように設定できます。

詳細については、「[ページ51の電子メールを使用して2段階認証の設定を行います。](#)」を参照してください。

次の表では、このタブの設定について説明します。

### [プロバイダー設定]>電子メール

名前	説明
SMTPサーバー	2要素認証電子メールの簡易メール転送プロトコル（SMTP）サーバーのIPアドレスまたはホスト名を入力します。
SMTPサーバーポート	電子メールを送信するSMTPサーバーのポートを指定します。 デフォルトのポート番号は、SSLを使用しない場合は25、SSLを使用する場合は465です。
SSLを使用	SMTPサーバーがSSL暗号化をサポートしている場合は、このチェックボックスを選択します。
ユーザー名	SMTPサーバーにログインするユーザー名を指定します。
パスワード	SMTPサーバーにログインするパスワードを指定します。
セキュリティで保護されたパスワード認証（SPA）の	SMTPサーバーがSPAをサポートしている場合は、このチェックボックスを選択します。

名前	説明
使用	
送信者の電子メールアドレス	認証コードを送信する電子メールアドレスを指定します。
電子メールの件名	電子メールの件名を指定します。例：2要素認証コード。
電子メールテキスト	<p>送信するメッセージを入力します。例：あなたのコードは{0}です。</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 10px; margin-top: 10px;">  <p>{0} 変数の入力を忘れた場合、コードはデフォルトでテキストの最後に追加されます。</p> </div>

### 検証コード設定

名前	説明
再接続タイムアウト (0~30分)	<p>たとえば、ネットワークが切断された場合、XProtect Mobileクライアントユーザーがログインを再確認する必要がない期間を指定します。デフォルトの期間は3分間です。</p> <p>この設定はXProtect Web Clientには適応されません。</p>
コードは (1~10分) 後に有効期限が切れます	ユーザーが受け取った認証コードを使用できる期間を指定します。この期間の後はコードが無効となるため、ユーザーは新しいコードを要求する必要があります。デフォルトの期間は5分間です。
コード入力試行 (1~10回試行)	提供されたコードが無効になるまでの、コード入力試行最大回数を指定します。デフォルトの回数は3回です。
コード長 (4~6文字)	コードの文字数を指定します。デフォルトの長さは6文字です。
コードの構成	システムによって課されるコードの複雑度を指定します。次の中から選択できます。

名前	説明
	<ul style="list-style-type: none"> <li>• アルファベット大文字 (A-Z)</li> <li>• ラテン語の小文字(a~z)</li> <li>• 数字 (0~9)</li> <li>• 特殊文字 (!@#...)</li> </ul>

## ユーザー設定

名前	説明
ユーザーおよびグループ	<p>XProtectシステムに追加されたユーザーおよびグループを一覧表示します。</p> <p>グループがActive Directoryで構成されている場合、モバイルサーバーはActive Directoryからの電子メールアドレスなどの詳細情報を使用します。</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;">  Windowsグループは2要素認証をサポートしていません。         </div>
検証方法	<p>各ユーザーまたはグループの認証設定を選択します。次の中から選択できます。</p> <ul style="list-style-type: none"> <li>• <b>ログインなし</b>：ユーザーはログインできません。</li> <li>• <b>2要素認証なし</b>：ユーザーはユーザー名とパスワードを入力しなければなりません。</li> <li>• <b>電子メール</b>：ユーザーはユーザー名とパスワードに加えて認証コードを入力しなければなりません</li> </ul>
ユーザー詳細	各ユーザーがコードを受け取る電子メールアドレスを入力します。

## ダイレクトストリーミング (説明付き)

XProtect Mobileは、ライブモードでのダイレクトストリーミングに対応しています (XProtect ExpertおよびXProtect Corporateのみ)。

ダイレクトストリーミングは、H.264コーデック形式のビデオをXProtectシステムからクライアントに直接転送するためのビデオストリーミング技術です。これは、多くの新型IPカメラでサポートされています。ダイレクトストリーミングにはトランスコーディングは不要なため、XProtectにかかる負荷の一部が軽減されます。

ダイレクトストリーミング技術は、（XProtectシステムにより、ビデオがカメラで使用されるコーデックからJPEGファイルへとデコードされる）XProtectのトランスコーディング設定とは対照的です。この機能を有効にすると、カメラとビデオストリーミングの設定を変更することなくCPU使用率が軽減します。ダイレクトストリーミングはまた、同一のハードウェアのパフォーマンスも向上させます（トランスコーディングと比較して最大で5倍の量のビデオストリーミングが可能）。

ダイレクトストリーミング機能を使用して、H.265コーディングに対応しているカメラからビデオを直接XProtect Mobileクライアントに転送することも可能です。

Management Clientでは、クライアント向けのダイレクトストリーミングを有効または無効にできます（[ページ16のモバイルサーバーの設定](#)を参照）。

**ビデオストリームは以下が発生するとダイレクトストリーミングからトランスコーディングにフォールバックします。**

- ダイレクトストリーミング機能がManagement Clientで無効にされたか、要件が満たされていません（[ページ12のダイレクトストリーミングの要件](#)を参照）
- ストリーミングカメラのコーデックがH.264またはH.265ではありません（XProtect Mobileクライアントのみ）
- ビデオを10秒間以上にわたって再生できない
- ストリーミングカメラのフレームレートが秒あたり1フレーム（1 FPS）に設定されている
- サーバーとの接続、またはカメラとの接続が失われました
- ライブビデオ中にプライバシーマスク機能を使用している

## アダプティブストリーミング（説明付き）

XProtect Mobileは、ライブモードでのアダプティブストリーミングに対応しています（XProtect ExpertおよびXProtect Corporateのみ）。

アダプティブストリーミングは、カメラの同一ビューで複数のライブビデオストリームを閲覧する場合に便利です。この機能はXProtect Mobileサーバーのパフォーマンスを最適化し、XProtect MobileクライアントとXProtect Web Clientを実行しているデバイスの復号化能力とパフォーマンスを改善します。

アダプティブストリーミングを活用するには、カメラに解像度の異なる複数のストリームを設定する必要があります。この場合、この機能によって以下が可能となります。

- ビデオ画質の最適化 - 利用可能なもっとも低い解像度（要求したものと同等またはそれ以上の解像度）を持つストリームが選択されます
- サーバーパフォーマンスの最適化 - 要求された解像度を低下させた後、使用可能なもっとも低い解像度（低



下したものと同等またはそれ以上の解像度) を持つストリームが選択されます

- 低帯域幅用に解像度を最適化 - 利用可能なもっとも低い解像度を持つストリームが選択されます (3Gまたは不安定なネットワークを使用している場合に推奨)



ズーム中に要求されるビデオストリームは、常に利用可能なもっとも高い解像度を持つものとなります。



帯域幅の使用はたいいてい、要求したストリームの解像度が下げられるのに併せて減少します。帯域幅の使用は、定義したストリーム構成の他の設定にも依存します。

アダプティブストリーミングの有効化/無効化、またはこの機能における優先ストリーミングモードの設定は、Management Clientのモバイルサーバー設定の**パフォーマンス**タブで行えます (ページ16の**モバイルサーバーの設定**を参照)。

## 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、非対称鍵暗号を伴うSSL/TLS (RSA) を使用することで安全な通信が確立されます。

SSL/TLSは、秘密キー1つと公開キー1つのペアを使用し、安全なコネクションを認証して安全な接続を管理します。

認証管理者 (CA) は、CA証明書を使ってサーバー上のWebサービスに証明書を発行します。この証明書には、秘密キーと公開キーの2種類のキーが含まれています。公開キーは、パブリック証明書をインストールすることにより、Web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。秘密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Webサービスを呼び出すと、必ずWebサービスが公開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公開CA証明書を使用し、サーバー証明書を検証します。これで、クライアントとサーバーはパブリック及びプライベート サーバー証明書を使用して秘密キーを交換することができ、安全なSSL/TLS通信を確立できます。

TLSの詳細については、[https://en.wikipedia.org/wiki/Transport\\_Layer\\_Security](https://en.wikipedia.org/wiki/Transport_Layer_Security)を参照してください

認証は期限付きです。XProtect VMSは、認証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しないため、通信できません
- 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しないため、通信できません
- モバイル機器は、証明書の有効期限が切れたモバイルサーバーを信頼しないため、通信できません



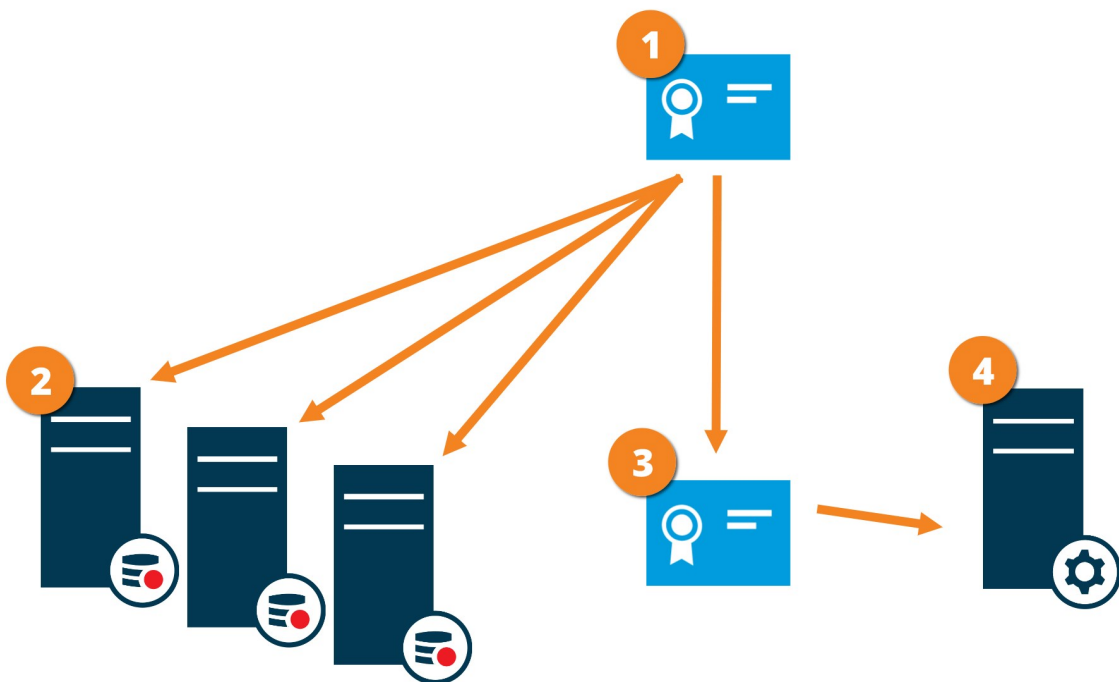
証明書の更新は、証明書を作成したときの要領で本ガイドのステップに従ってください。

## サーバーの暗号化を管理(説明付き)

マネジメントサーバーとレコーディングサーバー間の双方向接続を暗号化できます。マネジメントサーバー上の暗号化を有効にすると、そのマネジメントサーバーに接続するすべてのレコーディングサーバーからの接続に適用されます。マネジメントサーバーの暗号化を有効にした場合、すべてのレコーディングサーバーでも暗号化を有効にする必要があります。暗号化を有効化する前に、マネジメントサーバーとすべてのレコーディングサーバーにセキュリティ証明書をインストールしてください。

### マネジメントサーバーの証明書配布

この図は、証明書が署名され、信頼され、XProtect VMSで配布されて安全にマネジメントサーバーとの通信が行えるという基本コンセプトを表しています。



- ① CA証明書は信頼されたサードパーティのように機能し、サブジェクト/所有者 (マネジメントサーバー) と、証明書を認証する側 (レコーディングサーバー) の双方に信頼されます。
- ② CA証明書はすべてのレコーディングサーバー上で信頼されている必要があります。このようにして、レコーディングサーバーはCAによる証明書の信頼性を確認します
- ③ CA証明書は、マネジメントサーバーとレコーディングサーバー間で安全な接続を確立するために使用されます
- ④ CA証明書は、マネジメントサーバーを実行しているコンピュータにインストールする必要があります。

プライベートマネジメントサーバー証明書の要件:

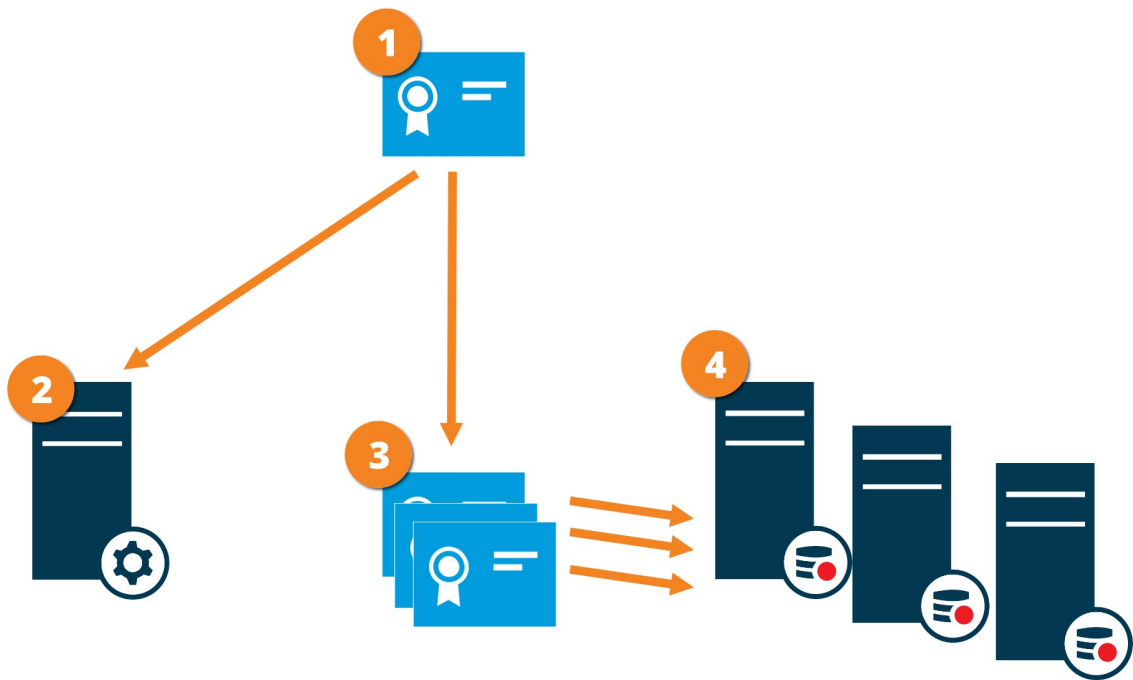
- 認証名にマネジメントサーバーのホスト名が含まれるか、DNS認証される名前前のリストの中にサブジェクト (所有者) としてマネジメントサーバーに発行されます。
- マネジメントサーバー証明書の発行に使用されたCA証明書が信頼されていることから、これがマネジメントサーバーでも信頼されていること。
- マネジメントサーバー証明書の発行に使用されたCA証明書を信用することによって、マネジメントサーバーに接続するすべてのレコーディングサーバーで信用されていること

## 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を暗号化 (説明付き)

マネジメントサーバーとレコーディングサーバー間の双方向接続を暗号化できます。マネジメントサーバー上の暗号化を有効にすると、そのマネジメントサーバーに接続するすべてのレコーディングサーバーからの接続に適用されます。この通信の暗号化は、マネジメントサーバーの暗号化設定に従う必要があります。そのため、マネジメントサーバーの暗号化が有効になっている場合、これをレコーディングサーバーでも有効にしなくてはならず、逆もまた同様です。暗号化を有効にする前に、マネジメントサーバーと全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を含む) にセキュリティ証明書をインストールする必要があります。

### 証明書の配布

図では、証明書が署名され、信頼され、XProtect VMSで配布されて安全にマネジメントサーバーからの通信が行えるという基本コンセプトを表しています。



① CA証明書は信頼されたサードパーティのように機能し、サブジェクト/所有者（レコーディングサーバー）側と、証明書を認証する側（マネジメントサーバー）の双方によって信頼されているとみなされます。

② CA認証はマネジメントサーバーで信頼されている必要があります。このようにして、マネジメントサーバーはCAによる認証の信頼性を確認します

③ CA証明書は、レコーディングサーバーとマネジメントサーバー間で安全な接続を確立するために使用されます

④ CA認証は、レコーディングサーバーが実行されるコンピュータにインストールする必要があります。

プライベートレコーディングサーバー認証のための要件:

- 認証名にレコーディングサーバーのホスト名が含まれるか、DNS認証される名前前のリストの中にサブジェクト (オーナー)としてレコーディングサーバーに発行されます。
- レコーディングサーバー証明書の発行に使用されたCA証明書を信用することによって、マネジメントサーバーで信用されていること

## マネジメントサーバーとData Collector server間の暗号化（説明付き）

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。

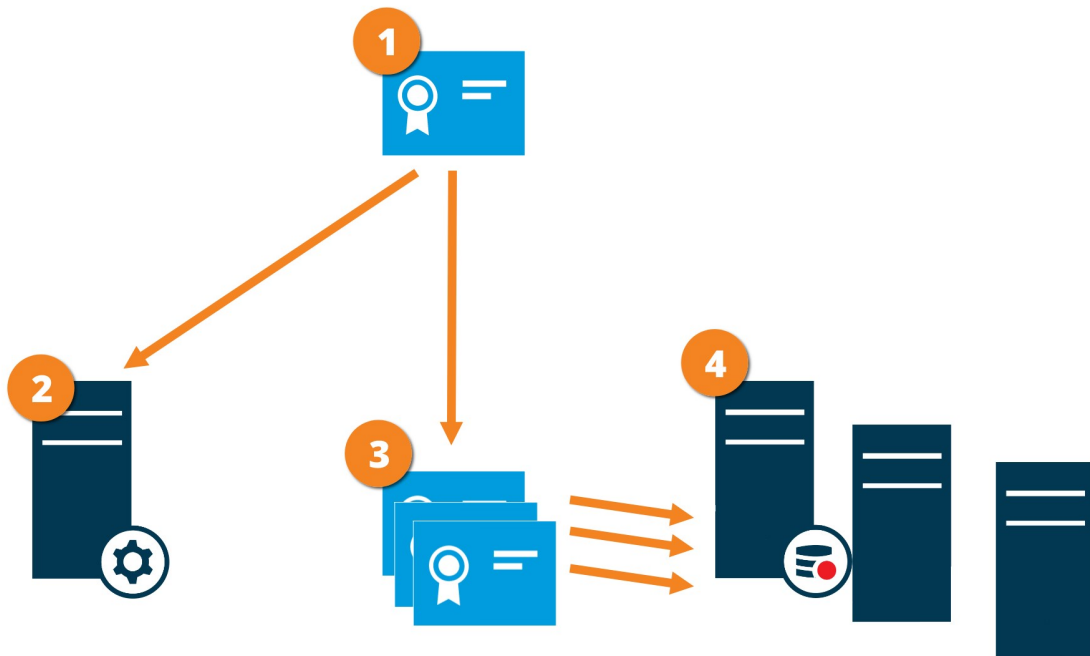
- Recording Server
- Event Server
- Log Server

- LPR Server
- Mobile Server

マネジメントサーバー上で暗号化を有効にする場合、マネジメントサーバーに接続するすべてのData Collectorサーバーからの接続にも暗号化の有効化が適用されます。この通信の暗号化は、マネジメントサーバーの暗号化設定に従う必要があります。マネジメントサーバーの暗号化が有効になっている場合は、これを各リモートサーバーに関連のあるData Collectorサーバーでも有効にしなくてはならず、逆もまた同様です。暗号化を有効化する前に、マネジメントサーバーと、リモートサーバーに関連しているすべてのData Collectorサーバーでセキュリティ証明書をインストールする必要があります。

### 証明書の配布

図では、証明書が署名され、信頼され、XProtect VMSで配布されて安全にマネジメントサーバーからの通信が行えるという基本コンセプトを表しています。



- ① CA証明書は、サブジェクト/所有者側（データコレクタサーバー）と証明書を認証する側（マネジメントサーバー）両方によって信頼されている信頼されたサードパーティとして機能します
- ② CA認証はマネジメントサーバーで信頼されている必要があります。このようにして、マネジメントサーバーはCAによる認証の信頼性を確認します
- ③ CA証明書は、データコレクタサーバーとマネジメントサーバー間の安全な接続を確立するために使用されます
- ④ CA証明書は必ずデータコレクタサーバーを実行するコンピュータにインストールしてください

プライベートデータコレクタサーバー証明書の要件:

- サブジェクト（所有者）として証明書にデータコレクタサーバーのホスト名を含めるか、証明書が発行されるDNS名のリスト内に含める形で証明書にデータコレクタサーバーのホスト名を含めるため、データコレクタサーバーに発行されること
- データコレクタサーバー証明書の発行に使用されたCA証明書を信頼することによって、マネジメントサーバーで信頼されていること

## レコーディングサーバーからデータを取得しているクライアントとサーバーを暗号化 (説明付き)

レコーディングサーバーを暗号化可能にする場合、すべてのクライアント、サーバー、ならびに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インテグレーションは暗号化されます。この文書では「クライアント」と呼んでいます:

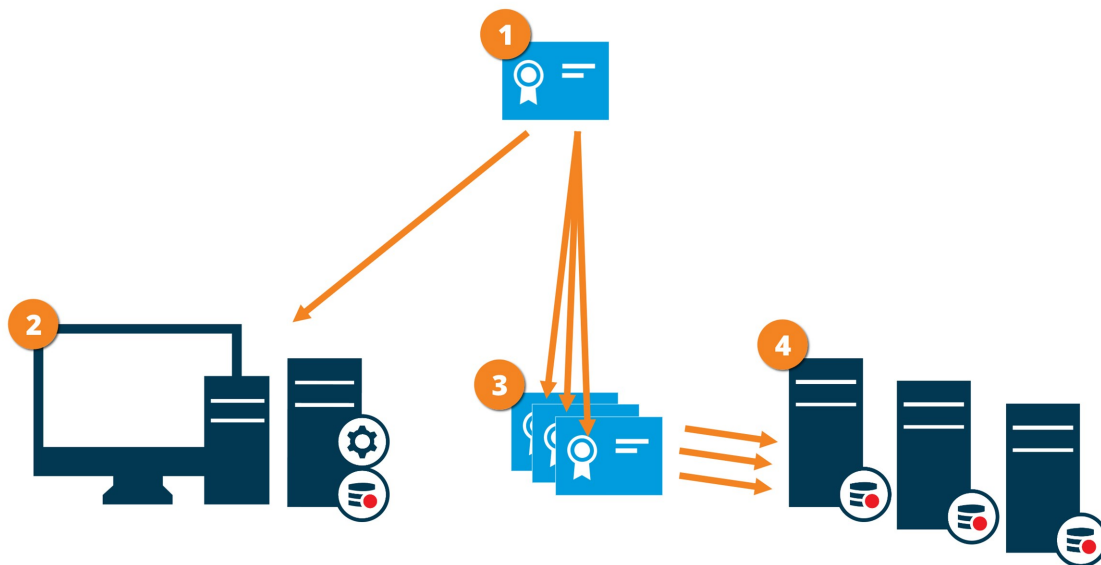
- XProtect Smart Client
- Management Client
- Management Server(メール 通知によるシステム モニター向け、とイメージと AVI ビデオクリップ向け)
- XProtect Mobile Server
- XProtect Event Server
- XProtect LPR
- Milestone Open Network Bridge
- XProtect DLNA Server
- を通してレコーディングサーバーからデータ ストリームを取得するサイトMilestone Interconnect
- サードパーティMIP SDKインテグレーション



レコーディングサーバーにアクセスする、MIP SDK 2018 R3以前のバージョンで構築したソリューション：MIP SDKライブラリを用いて統合が行われた場合、MIP SDK 2019 R1でこれらを再構築する必要があります。統合においてMIP SDKライブラリを使用せずにRecording Server APIと直接通信が行われる場合、インテグレータはご自身でHTTPSサポートを追加する必要があります。

### 証明書の配布

図では、証明書が署名され、信頼され、XProtect VMSで配布されて安全にレコーディングサーバーとの通信が行えるという基本コンセプトを表しています。



- ① CA証明書は信頼されたサードパーティのように機能し、サブジェクト/所有者（レコーディングサーバー）側と、証明書を認証する側（全クライアント）の双方によって信頼されているとみなされます。
- ② CA認証はすべてのクライアント上で信頼されている必要があります。このようにして、クライアントはCAによる認証の信頼性を確認します。
- ③ CA証明書は、レコーディングサーバーと全クライアント/サービス間で安全な接続を確立するために使用されます
- ④ CA認証は、レコーディングサーバーが実行されるコンピュータにインストールする必要があります。

プライベートレコーディングサーバー認証のための要件:

- 認証名にレコーディングサーバーのホスト名が含まれるか、DNS認証される名前リストの中にサブジェクト (オーナー)としてレコーディングサーバーに発行されます。
- レコーディングサーバー認証の発行に使用されたCA認証を信頼することによって、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
- レコーディングサーバーを実行するサービスアカウントは、レコーディングサーバー上のプライベート認証キーへアクセスします。



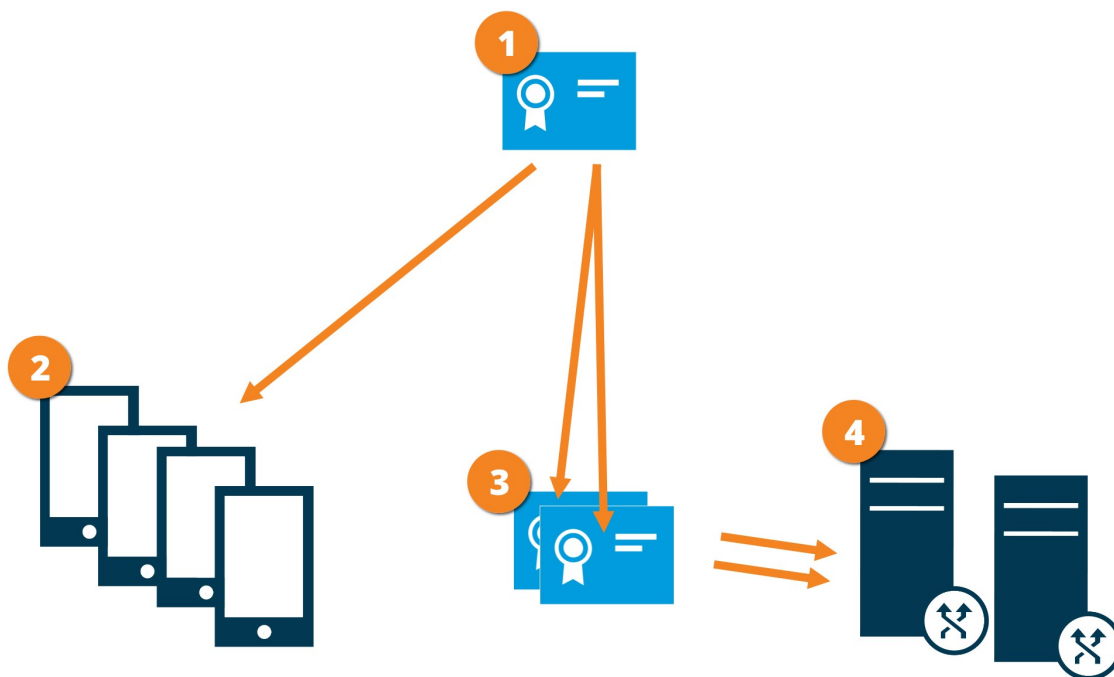
レコーディングサーバーの暗号化が有効化されており、システムがフェールオーバーレコーディングサーバーを適用している場合は、Milestone はフェールオーバーレコーディングサーバーも暗号化する準備をすることをお勧めします。

## レコーディングサーバー データ 暗号化（説明付き）

XProtect VMSでは、暗号化はモバイルサーバーごとに有効化または無効化されます。モバイルサーバーで暗号化を有効にする際、クライアント、サービス、データストリームを取得するインテグレーションすべてとの通信を暗号化するか選択することができます。

### モバイルサーバーの証明書配布

この図は、証明書が署名され、信頼され、XProtect VMSで配布されて安全にモバイルサーバーとの通信が行えるという基本コンセプトを表しています。



- ① CA証明書は信頼されたサードパーティのように機能し、サブジェクト/所有者 (モバイルサーバー) と証明書を確  
認する側 (クライアントすべて) 双方に信頼されます。
- ② CA認証はすべてのクライアント上で信頼されている必要があります。このようにして、クライアントはCAによる  
証明書の信頼性を確認します
- ③ CA証明書は、モバイルサーバーとクライアントおよびサービス間の安全な接続を確立するために使用されます
- ④ CA証明書はモバイルサーバーを実行しているコンピュータにインストールしてください。



#### CA認証要件:

- モバイルサーバーのホスト名は、サブジェクト/所有者として、またはDNS認証される名前リストの認証名に含まれていなくてはなりません
- 認証証明書は、モバイル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デバイスで信頼される必要があります
- モバイルサーバーを実行するサービスアカウントは、CA認証の秘密キーへのアクセス権限が必要です

#### クライアントに対するモバイルサーバー暗号化の条件

安全上の理由からMilestoneでは、ユーザーアカウントの設定を管理する際、モバイルサーバーとクライアント間で安全な通信を使用するよう推奨しています。

暗号化せずにHTTP通信を使用する場合は、XProtect Web Clientのプッシュ ツー トーク機能は利用できません。

## Milestone Federated Architectureおよびマスター/スレーブサーバー (説明付き)

システムがマスター/スレーブ設定でMilestone Federated Architectureあるいはサーバーをサポートする場合は、XProtect MobileクライアントあるいはXProtect Web Clientを使用してこのようなサーバーにアクセスできます。この機能を使用して、マスターサーバーにログインし、すべてのスレーブサーバー上のすべてのカメラへのアクセスを取得します。

Milestone Federated Architecture設定では、中央サイト経由で子サイトへのアクセスを取得します。XProtect Mobileサーバーは中央サイトにのみインストールします。

これは、XProtect MobileクライアントあるいはXProtect Web Clientのユーザーがサーバーにログインして、システムのすべてのサーバーからカメラを表示する場合、マスターサーバーのIPアドレスに接続する必要があるということです。XProtect MobileクライアントあるいはXProtect Web Clientでカメラを表示するには、ユーザーはシステムのすべてのサーバーでシステム管理者権限が必要です。

## スマートコネクト (説明付き)

スマートコネクトを利用すると、検証を行うためにモバイルデバイスやタブレットにログインしなくても、XProtect Mobileが正しく構成されたことを確認できます。また、XProtect MobileクライアントとXProtect Web Clientユーザーの接続プロセスを簡易化します。

この機能では、XProtect MobileサーバーがパブリックIPアドレスを使用していること、システムがMilestone Care Plus購読パッケージのライセンスを受けている必要があります。

Management Clientリモート接続の設定がうまく行われた場合、即座にシステムからフィードバックが送られ、XProtect Mobileサーバーはインターネットからアクセスできます。

スマートコネクトはXProtect Mobileサーバーが内部および外部のIPアドレス間をシームレスに切り替え、どこからでもXProtect Mobileに接続できるようにします。

顧客のMobileクライアントの設定を簡単にするために、Management Client内からエンドユーザーに直接Eメールを送れます。Eメールにはサーバーを直接にXProtect Mobile追加するリンクが含まれています。これでネットワークアドレスやポートを入力する必要なしに設定が完了します。

## Smart Connectの設定

スマートコネクト機能を設定するには、次の手順に従います。

1. Management Clientで、ナビゲーションペインで、**サーバー**を展開し、**モバイルサーバー**を選択します。
2. サーバーを選択し、**接続**タブをクリック。
3. ルーターでのUniversal Plug and Playの検出可能性を有効にします。
4. 接続を設定する。
5. 電子メールメッセージをユーザーに送信する。
6. 複雑なネットワークでの接続を有効にする。

## ルーターでのUniversal Plug and Playの検出可能性を有効化

モバイルデバイスをXProtect Mobileサーバーに簡単に接続するには、ルーターでUniversal Plug and Play (UPnP)を有効にするという方法があります。UPnPにより、XProtect Mobileサーバーはポート転送を自動的に構成できます。ただし、Webインターフェイスを使用すると、ルーターでポート転送を手動で設定できます。ルーターによっては、ポートマッピングの設定手順が異なる場合があります。ルーターでポート転送を設定する方法がわからなれば、そのデバイスのマニュアルを参照してください。



5分ごとに、XProtectMobileServerサービスは、インターネットのユーザーがサーバーを使用できることを検証します。状態は、**[プロパティ]**ペインの左上に表示されます：

Server accessible through internet: ●

## 複雑なネットワークでの接続を有効にする

カスタム設定がある複雑なネットワークの場合、ユーザーが接続に必要な情報を入力できます。

**インターネットアクセスグループのコネクティビティ**タブで、次のアイテムを指定します。

- UPnPポートマッピングを使用して、接続を特定の接続に向ける場合は、**[カスタムインターネットアクセスの設定]**チェックボックスを選択します。**IPアドレスまたはホスト名**と、接続に使われるポートを提供します。たとえば、ルーターがUPnPをサポートしない場合、またはルーターのチェーンがある場合に、これを実行できます
- IPアドレスが頻繁に変更される場合は、**チェックするとIPアドレスを動的に取得する**チェックボックスを選択します

## 接続設定の構成

1. Management Clientで、ナビゲーションペインで、**サーバー**を展開し、**モバイルサーバー**を選択します。
2. サーバーを選択し、**接続**タブをクリックします。
3. **[全般]**グループのオプションを使用して、次のアイテムを指定します：
  - XProtect MobileクライアントとXProtect Web Clientユーザーが簡単にXProtect Mobileサーバーに接続できるようにするには、**スマートコネクトを有効にする**チェックボックスを選択します
  - XProtect MobileクライアントおよびXProtect Web Clientが、自らが実行中であることをモバイルサーバーに表示すべき時間枠を設定します。
  - UPNp プロトコルを使用したネットワーク上でXProtect Mobile サーバーを検出できるようにするには、**UPNp 発見性を有効にする** チェックボックスを選択します。
  - ルーターがその仕様で構成されている際にXProtect Mobileサーバーがポートマッピングを自ら実行できるようにするには、**[自動]ポートマッピングを有効にする**チェックボックスを選択します。

## 電子メールメッセージをユーザーに送信する

XProtect MobileクライアントとXProtect Web Clientの設定を簡単にするために、Management Client内からエンドユーザーに直接Eメールを送れます。Eメールにはサーバーを直接にXProtect Mobile追加するリンクが含まれています。これでネットワークアドレスやポートを入力する必要なしに設定が完了します。

1. **招待を電子メールで送信する**フィールドに、スマートコネクト通知の受信者の電子メールアドレスを入力し、言語を指定します。
2. 次に、以下のいずれか1つを実行します。
  - メッセージを送信するには、**送信**をクリックします。
  - 使用するメッセージングプログラムに情報をコピーします。

詳細については以下を参照してください：

[ページ12のスマートコネクト設定の要件](#)

[ページ19の接続タブ](#)

## 通知の送信（説明付き）

XProtect Mobileを有効にして、アラーム起動やデバイスまたはサーバーで問題が発生した場合など、イベントが発生したときにユーザーに通知できます。アプリが実行されているかどうかに関わらず、通知は常に配信されます。XProtect Mobileがモバイルデバイスで開くと、通知が配信されます。システム通知は、アプリが実行されていない場合でも配信されます。ユーザーは受信する通知のタイプを指定できます。たとえば、次の状態の通知を受信することを選択できます。

- すべてのアラーム
- 割り当てられたアラームのみ
- システム関連のアラームのみ

これらは、サーバーがオフラインになったとき、またはオンラインに戻ったとき場合があります。

また、プッシュ通知を使用すると、XProtect Mobileを開いていないユーザーにも通知できます。これらはプッシュ通知といいます。プッシュ通知はモバイルデバイスに配信されます。これは、移動中のユーザーが常に最新情報を得られる優れた方法です。

## プッシュ通知の使用



プッシュ通知をしようするには、システムがインターネットにアクセスできる必要があります。

プッシュ通知はApple、Microsoft、Googleからクラウドサービスを使用します。

- Apple Push Notificationサービス(APN)
- Microsoft Azure通知ハブ
- Google Cloud Messaging Push Notificationサービス

システムが特定の期間に送信できる通知数は制限されています。この制限を超過すると、次の期間中に15分ごとに1件の通知のみを送信できます。通知には、15分間に発生したイベントの概要が含まれます。次の期間の後、制限は削除されます。

[ページ11の通知設定の要件](#)と[ページ28の通知タブ](#)も参照してください。

## XProtect Mobileサーバーでプッシュ通知を設定

プッシュ通知を設定するには、次の手順に従います。

1. Management Clientでモバイルサーバーを選択してから、**通知タブ**をクリックします。
2. サーバーに接続するすべてのモバイルデバイスに通知を送信するには、**[通知]**チェックボックスを選択します。
3. サーバーに接続するユーザーとモバイルデバイスの情報を保存するには、**[デバイス登録の管理]**チェックボックスを選択します。



サーバーはリストのモバイルデバイスにのみ通知を送信します。**[デバイス登録の管理]**チェックボックスをオフにし、変更を保存すると、リストが消去されます。もう一度プッシュ通知を受信するには、デバイスを再接続する必要があります。

## 特定のモバイルデバイスまたはすべてのモバイルデバイスへのプッシュ通知の送信を有効化する

XProtect Mobileを有効化するには、特定またはすべてのモバイル デバイスにプッシュ通知を送信することによってイベントが発生したときにユーザーに通知します。

1. Management Clientでモバイルサーバーを選択してから、**通知**タブをクリックします。
2. 以下のいずれか1つを実行します。
  - 個々のデバイスの場合は、**[登録済みデバイス]**テーブルにリストアップされている、各モバイルデバイスのチェックボックスの**[有効化]**を選択します
  - すべてのモバイルデバイスでは、**通知**チェックボックスを選択します

## 特定の、またはすべてのモバイルデバイスへのプッシュ通知の送信を停止する

特定の、またはすべてのモバイルデバイスへのプッシュ通知の送信を停止するには、複数の方法があります。

1. Management Clientでモバイルサーバーを選択してから、**通知**タブをクリックします。
2. 以下のいずれか1つを実行します。
  - 個別のデバイスで、各モバイルデバイスの**[有効]**チェックボックスをオフにします。ユーザーは別のデバイスを使用して、XProtect Mobileサーバーに接続できます。
  - すべてのデバイスの**[通知]**チェックボックスをオフにします。

すべてのデバイスを一時的に停止するには、**[デバイス登録の管理]**チェックボックスをオフにし、変更を保存します。ユーザーが再接続した後に、もう一度通知が送信されます。

## 調査の設定

XProtect Web ClientあるいはXProtect Mobileを使用して録画ビデオへのアクセスとインシデントの調査を行い、ビデオエビデンスを準備してダウンロードできるように調査を設定します。

調査を設定するには、次の手順に従います。

1. Management Clientでは、モバイルサーバーをクリックしてから、**調査**タブをクリックします。
2. **[調査を有効にする]**チェックボックスを選択します。デフォルトでは、チェックボックスが選択されていません。
3. **調査フォルダー**フィールドで、調査のビデオを保存する場所を指定します。
4. オプション：ユーザーが他のユーザーが作成する調査にアクセスできるようにするには、**他のユーザーが作成した調査を表示する**チェックボックスを選択します。このチェックボックスを選択しない場合、ユーザーは自分の調査のみを表示できます。
5. **調査フォルダーのサイズ制限を有効にする**チェックボックスを選択し、調査フォルダーに含めることのできる最大メガバイト数を設定します。

6. **調査の保存期間を有効に設定**チェックボックスを選択すると、調査の保存期間を設定できます。デフォルトで保存期間は7日間に設定されています。
7. **エクスポートフォーマット**で、使用したいエクスポートフォーマットのチェックボックスを選択してください。以下のエクスポートフォーマットを利用できます。
  - AVIフォーマット
  - XProtectフォーマット
  - MKVフォーマット



デフォルトでチェックボックスは選択されていません。

8. (オプション) ビデオがダウンロードされた日時を含めるには、**AVIエクスポートのタイムスタンプを含める**チェックボックスを選択します。
9. **AVIエクスポートで使用されたコーデック**フィールドで、ダウンロード用にAVIパッケージを準備するとき使用する圧縮形式を選択します。



リストのコーデックは、オペレーティングシステムによって異なる場合があります。使用するコーデックが表示されない場合は、Management Clientが実行されているコンピュータにインストールすると、このリストに表示されます。



また、コーデックは異なる圧縮率を使用することがあり、動画品質に影響する場合があります。高圧縮率によりストレージ要件が減りますが、画質が低下する可能性があります。低圧縮率はストレージとネットワーク容量が増えますが、画質が上がります。選択する前にコーデックを調査することをお勧めします。

10. エクスポートするビデオに音声が含まれている場合は、**AVI エクスポートに使用された音声ビットレート**リストから、適切な音声ビットレートを選択します。デフォルトは160000 Hzです。



ユーザーが調査を保存できるようにするには、**エクスポート**権限をユーザーに割り当てたセキュリティ役割に付与する必要があります。

### 調査のクリーンアップ

保持する必要がない調査またはビデオエクスポートがある場合は、削除できます。たとえば、サーバーでより多くのディスク領域が使用できるようにする場合には、これが便利です。

- 調査と、その調査のために作成されたビデオエクスポートをすべて削除するには、リストで調査を選択してから削除をクリックします。
- 調査用にエクスポートされた個別のビデオファイルを削除しながらその調査を保持するには、リストで調査を選択します。調査の詳細グループで、エクスポート用のXProtect、AVI、またはMKVフィールドの右側にある削除アイコンをクリックします。

## ビデオプッシュを使用したビデオのストリーミング（説明付き）

ビデオプッシュを設定すると、ユーザーはモバイルデバイスのカメラからXProtect監視システムに動画をストリーミングし、常に状況に関する通知を受信するか、動画を録画して後から調査できます。ビデオストリームには音声もついている場合があります。

ページ27のビデオプッシュタブとページ12のビデオプッシュ 設定の要件も参照してください。

### ビデオを流すための「ビデオ・プッシュ」の設定

ユーザーが携帯デバイスからXProtectシステムにビデオを流すには、XProtect Mobileサーバーでビデオプッシュを設定する必要があります。

Management Client次の手順で設定が可能です。

1. ビデオプッシュタブで、ビデオプッシュチェックボックスを選択して、この機能を有効にします。
2. ビデオプッシュチャンネルをストリーミングビデオに追加。
3. ビデオプッシュドライバーをRecording Serverのハードウェアデバイスとして追加します。このドライバーはカメラデバイスに影響して、Recording Serverにビデオを流すことができます。
4. ビデオプッシュドライバーデバイスをビデオプッシュのためのチャンネルに追加します。

### ビデオプッシュ・チャンネルをストリーミングビデオに追加

チャンネルを追加するためには、次のステップを踏んで下さい。

1. ナビゲーションペインで[モバイルサーバー]を選択してからモバイルサーバーを選択します。
2. 「ビデオ・プッシュ」のタブ上で、「ビデオ・プッシュ」を選択しボックス内をチェチェックして下さい。
3. [チャンネル マッピング]の左下で[追加]をクリックし、ビデオプッシュチャンネルを追加します。
4. 表示されたダイアログボックスに、チャンネルを使用するユーザーアカウントのユーザー名を入力します ([役割]で追加)。このユーザーアカウントによるXProtect Mobileサーバーとレコーディングサーバーへのアクセスを [セキュリティ全般]タブで許可する必要があります。



「ビデオ・プッシュ」を使用するには、このアカウントのユーザー名とパスワードを使用して、モバイルデバイスでXProtect Mobileにログインする必要があります。



新しいビデオ プッシュ チャンネルを追加すると、レコーディング サーバーでハードウェア デバイスとしてチャンネルを追加する際に使われるポート番号とMACアドレスが生成されます。また、Recording ServerとMobile Serverの接続で使用されるパスワードも生成されます。デフォルトのパスワードは、**Milestone**です。

5. ポート・ナンバーを書き留めておいて下さい。それは、記録サーバーにハードウェア・デバイスとして「ビデオ・プッシュ」を追加する時に必要です。
6. **[OK]**をクリックして、[ビデオ プッシュ チャンネル]ダイアログを閉じます。
7. チャンネルを保存するには、ナビゲーション ペインの左上で**[保存]**をクリックします。

### ビデオ プッシュ チャンネルの編集

追加したビデオ プッシュ チャンネルの設定詳細は編集できます。

1. **[チャンネル マッピング]**で編集するチャンネルを選択し、**[編集]**をクリックします。
2. 編集を終了したら、**[OK]**をクリックして[ビデオ プッシュ チャンネル]ダイアログボックスを閉じます。
3. 編集内容を保存するには、ナビゲーション ペインの左上で**[保存]**をクリックします。



ビデオ プッシュ チャンネルのポート番号とMACアドレスを編集する場合は、レコーディングサーバーで以前に追加したビデオ プッシュ チャンネル設定の詳細も必ず新しい情報に置き換えてください。これを行わなければ、Recording ServerとMobile Serverの接続が失われます。

### ビデオプッシュチャンネルの追加

不要になったチャンネルは削除できます：

1. **[チャンネル マッピング]**で削除するチャンネルを選択し、**[削除]**をクリックします。
2. 変更を保存するには、ナビゲーション ペインの左上で**[保存]**をクリックします。

### パスワードの変更

自動的に生成され、Recording ServerとMobile Serverの接続で使用されるパスワードは変更可能です。

1. **[チャンネル マッピング]**の右下で**[パスワードの変更]**をクリックします。
2. **[ビデオ プッシュのパスワード変更]**ダイアログボックスで、最初のフィールドに新しいパスワードを入力し、2番目のフィールドでも新しいパスワードを繰り返して**[OK]**をクリックします。
3. 変更を保存するには、ナビゲーション ペインの左上で**[保存]**をクリックします。





ビデオ プッシュ チャンネルのパスワードを変更する場合は、すでにリストに含まれているビデオ プッシュ チャンネル、または将来、追加されるビデオ プッシュ チャンネルすべてに変更が適用されます。既存のビデオ プッシュ チャンネルをすべてリストから削除する場合でも、新しいパスワードは有効なままで、将来のチャンネルに適用されます。



変更を保存した後、既存のビデオ プッシュ チャンネルはすべて機能しなくなります。Recording ServerとMobile Serverの間の接続が切断されるためです。この接続を回復するには、ナビゲーション ペインで[レコーディング サーバー]タブを右クリックして[ハードウェアの置き換え]ウィザードを実行し、Recording Serverでハードウェア デバイスとして追加したビデオ プッシュ ドライバーの新しいパスワードを入力します。

## ビデオプッシュドライバーをハードウェアデバイスとしてに追加するRecording Server

1. ナビゲーションの窓で、「記録サーバー」をクリックして下さい。
2. ビデオを流したいサーバーを右クリックして、[ハードウェアの追加]をクリックして、[ハードウェアの追加]ウィザードを開きます。
3. ハードウェア探知方法として[手動]を選択し、[次へ]をクリックして下さい。
4. カメラのログイン資格情報を入力します：
  - ユーザー名: 工場設定のデフォルトを入力するか、カメラで指定したユーザー名を入力します。
  - パスワード: Milestone (システムによって生成されたパスワード) を入力するか、モバイル サーバーでビデオ プッシュ チャンネルを追加した際にパスワードを変更している場合は、使用したいパスワードを入力してから、[次へ]を入力します



これはユーザーではなく、ハードウェアの資格情報です。資格情報は、ビデオ プッシュチャンネルへのアクセスで使用されるユーザー アカウントには関係していません。

5. ドライバーズリストでMilestoneを展開し、「ビデオ・プッシュ・ドライバー」のチェックボックスを選択してから[次へ]をクリックします。
6. アドレスフィールドには、XProtect MobileサーバーがインストールされているコンピュータのIPアドレスを入力してください。



システムの生成したMACアドレスを使用するようお勧めします。ビデオ プッシュ ドライバーで問題が発生した場合、またはモバイル サーバーでビデオ プッシュ チャンネルのポート番号とMACアドレスを編集した場合などにのみ変更します。

7. 「ポート」欄で、ビデオを流すために作成したチャンネル用のポート番号を入れて下さい。ポート番号はチャンネルを作成した時に割り当てられています。
8. 「ハードウェア・モデル」内で、「ビデオ・プッシュ・ドライバー」を選択し、「次へ」をクリックして下さい。
9. システムが新しいハードウェアを探知したら、「次へ」をクリックして下さい。
10. **ハードウェア名**テンプレートフィールドで、ハードウェアのモデルとそのIPアドレスを表示するか、モデルのみを表示するか決めてください。
11. 関係するデバイスが作動するかどうかは、「**作動可**」チェックボックスを選択して決めて下さい。「**ビデオ・プッシュ・ドライバー**」の関連デバイスは、作動不可でも、追加することができます。後で、作動可にできます。



ビデオを流す際にロケーション情報を使いたい場合は、「**メタデータ・ポート**」を起動させる必要があります。



ビデオをストリームするときに音声を再生したい場合は、ビデオストリーミングに使うカメラのマイクを有効にしてください。

12. 左側で該当するデバイスのデフォルトのグループを選択するか、**グループに追加**フィールドで特定のグループを選択してください。一つのグループにデバイスを追加すれば、同時にすべてのデバイスを設定してり、あるいはデバイスの入れ替えが簡単にできます。


## ビデオプッシュドライバーデバイスをビデオプッシュのためのチャンネルに追加します。

ビデオプッシュドライバーデバイスをビデオプッシュのためのチャンネルに追加するには、以下の手順に従ってください。

1. 「**サイト・ナビゲーション**」で、「**携帯サーバー**」をクリックしてから、「**ビデオ・プッシュ**」タブをクリックして下さい。
2. 「**カメラを見つける**」をクリックして下さい。成功すると、**カメラ名**欄に、ビデオプッシュドライバーカメラの名前が表示されます。
3. あなたの構成を保存して下さい。

## 既存のビデオプッシュチャンネルに対し音声を有効化する

ビデオプッシュで音声を有効にする要件を満たした後（[ページ12のビデオプッシュ 設定の要件](#)を参照）、Management Clientでは：

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、[レコーディングサーバー]をクリックします。
2. 概要ペインで該当するレコーディングサーバーのフォルダーを選択し、**Video Push Driver**フォルダーを展開してからビデオプッシュに該当するマイクを右クリックします。
3. [有効化]を選択してマイクを有効にします。
4. 同じフォルダー内で、ビデオプッシュに該当するカメラを選択します。
5. **プロパティ**ペインで、**クライアント**タブをクリックします。  
詳細については、[クライアントタブ \(デバイス\)](#) を参照してください。
6. [該当するマイク]フィールドの右側にある  をクリックします。[選択したデバイス]ダイアログボックスが開きます。
7. **レコーディングサーバー**タブで、レコーディングサーバーフォルダーを展開し、ビデオプッシュ関連のマイクを選択します。
8. **OK**をクリックします。

## 電子メールを使用して2段階認証の設定を行います。



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。詳細については、[製品比較](#) Webページを参照してください。

XProtect MobileクライアントまたはXProtect Web Clientのユーザーに追加のログイン手順を課すには、XProtect Mobileサーバー上で2要素認証の設定を行います。標準のユーザー名とパスワードに加えて、ユーザーは電子メールで送信される認証コードを入力しなければなりません。

2段階認証により監視システムの保護レベルが高まります。

Management Clientで以下の手順に従ってください。

1. ページ51のSMTPサーバーに関する情報を入力します。。
2. ページ52のユーザーに送られてくる認証コードを指定します。。
3. ページ52のユーザーとActive Directoryグループにログイン方法を割り当てます。。

ページ12のユーザーの2段階認証設定の要件とページ29の要素認証タブも参照してください。

## SMTPサーバーに関する情報を入力します。

プロバイダーはSMTPサーバーに関する情報を使用します。

1. ナビゲーションペインで、**モバイルサーバー**を選んでから、該当するモバイルサーバーを選択します。
2. **2段階認証**タブで、**2段階認証を有効にする**チェックボックスを選択します。
3. **プロバイダー設定**の下の、**電子メール**タブで、SMTPサーバーに関する情報を入力した後、ログイン時および2次ログインで設定する電子メールを指定します。各パラメータの詳細については、[ページ29の要素認証タブ](#)を参照してください。

詳細については、「[ページ29の要素認証タブ](#)」を参照してください。

## ユーザーに送られてくる認証コードを指定します。

認証コードの複雑度を指定するには:

1. **認証コード設定**セクションの**2段階認証**タブで、XProtect Mobileクライアントユーザーが、ネットワーク切断の際などに再確認することなくログインできる期間を指定します。デフォルトの期間は3分間です。
2. ユーザーが受け取った認証コードを使用できる期間を指定します。この期間終了後はコードが無効となるため、新しいコードを要求する必要があります。デフォルトの期間は5分間です。
3. 提供されたコードが無効になるまでの、コード入力試行最大回数を指定します。デフォルトの回数は3回です。
4. コードの文字数を指定します。デフォルトの長さは6文字です。
5. システムによって課されるコードの複雑度を指定します。

詳細については、「[ページ29の要素認証タブ](#)」を参照してください。

## ユーザーとActive Directoryグループにログイン方法を割り当てます。

**ユーザー設定**セクションの**2段階認証**タブに、XProtectシステムに追加されたユーザーとグループのリストが表示されます。

1. **ログイン方法**列で、各ユーザーまたはグループの検証方法を選択します。
2. **詳細**フィールドで、各ユーザーの電子メールアドレス等の配信の詳細を追加します。次回ユーザーがXProtect WebClientまたはXProtect Mobileアプリにログインすると、セカンダリログインが求められます。
3. グループがActive Directoryで構成されている場合、XProtect MobileサーバーはActive Directoryからの電子メールアドレスなどの詳細情報を使用します。



Windowsグループは2要素認証をサポートしていません。

4. あなたの構成を保存して下さい。

電子メールによる2段階認証のユーザー設定手順を完了しました。

詳細については、「[ページ29の要素認証タブ](#)」を参照してください。

## アクション（説明付き）

XProtect Mobileクライアント内またはXProtect Web Client内の**アクション**タブの有効性は、**一般**タブで**アクション**を有効化、または無効化することで管理できます。**[アクション]**はデフォルトで有効であり、接続されたデバイスのすべての使用可能なアクションがここに表示されます。

詳細については、「[ページ16の一般タブ](#)」を参照してください。

## XProtect MobileクライアントおよびXProtect Web Clientで使用する出力の名前を決める（説明付き）

現行のカメラでアクションを正しく表示するには、出力グループにカメラと同じ名前を付ける必要があります。

例：

「AXIS P3301 - 10.100.50.110 - Camera 1」という名前のカメラに接続されている出力を使って出力グループを作成する場合、**名前**フィールド（**デバイスグループ情報**の下）で同じ名前を入力する必要があります。

**説明**フィールドで、「AXIS P3301 - 10.100.50.110 - Camera 1 - Light switch」のように詳細な説明を追加できます。



これらの命名規則に従わない場合、アクションは関連付けられたカメラのビューのアクションリストで使用できません。代わりに、アクションは**[アクション]**タブの他のアクションのリストに表示されます。

詳細については、[出力デバイス（説明付き）](#)を参照してください。

## メンテナンス

### Mobile Server Manager（説明付き）

MobileServerManagerは、モバイルサーバーに接続されるトレイコントロール機能です。通知エリアでMobile ServerManagerトレイアイコンを右クリックすると、モバイルサーバーに簡単にアクセスできるメニューが開きます。

次の操作に従ってください。

- ページ54のXProtect Web Clientへのアクセス
- ページ55のMobile Serverサービスの起動、停止、再起動
- ページ55のデータ保護パスワードを変更
- ページ56のポート番号の表示/編集
- ページ56のモバイルサーバーで暗号化を有効にする（**Server Configurator**を使用）
- 今日のログファイルを開く（ページ57のロゴへのアクセスおよび調査（説明付き）を参照）
- ログフォルダーを開く（ページ57のロゴへのアクセスおよび調査（説明付き）を参照）
- 調査フォルダーを開く（ページ57のロゴへのアクセスおよび調査（説明付き）を参照）
- ページ58の調査フォルダーを変更
- XProtect Mobile Serverのステータスを参照（ページ59のステータスの表示（説明付き）を参照）

### XProtect Web Clientへのアクセス

XProtect Mobileサーバーがコンピュータにインストールされている場合は、XProtect Web Clientを使用してカメラとビューにアクセスできます。XProtect Web Clientをインストールする必要はないため、XProtect Mobileサーバーをインストールしたコンピュータまたはこの目的で使用する他のすべてのコンピュータからアクセスできます。

1. Management ClientでXProtect Mobileサーバーを設定します。
2. XProtect Mobileサーバーがインストールされているコンピュータを使用している場合は、通知エリアのMobile Server Managerトレイアイコンを右クリックして**XProtect Web Clientを開く**を選択します。
3. XProtect Mobileサーバーがインストールされているコンピュータを使用しない場合は、ブラウザからアクセスできます。このプロセスで手順4を続行します。
4. インターネットブラウザ（Internet Edge、Mozilla Firefox、Google Chrome、Safari）を開きます。

5. 外部IPアドレスを入力します。これは、XProtect Mobileサーバーが実行されているサーバーの外部アドレスとポート番号です。

例：XProtect MobileサーバーがIPアドレス127.2.3.4のサーバーにインストールされ、ポート8081でHTTP接続を許可し、ポート8082でHTTPS接続を許可するように設定されます（インストーラのデフォルト設定）。

標準HTTP接続をご希望の場合は、お使いのブラウザのアドレスバーに**http://127.2.3.4:8081**と入力します。安全に確立されたHTTPS接続を使用するには**https://127.2.3.4:8082**と入力してください。これで、XProtect Web Clientを使用できます。

6. 今後、XProtect Web Clientに簡単にアクセスできるように、アドレスをブラウザのブックマークに追加します。XProtect MobileサーバーをインストールしたローカルコンピュータでXProtect Web Clientを使用する場合は、インストーラで作成されたデスクトップショートカットも使用できます。ショートカットをクリックしてデフォルトのブラウザを起動し、XProtect Web Clientを開きます。



XProtect Web Clientの新しいバージョンを使用するには、XProtect Web Clientを実行しているインターネットブラウザのキャッシュをクリアする必要があります。システム管理者は、アップグレードの際にXProtect Web Clientユーザーにブラウザのキャッシュのクリアを依頼するか、このアクションをリモートで強制的に実行する必要があります（このアクションを実行できるのは、ドメイン内のInternet Explorerだけです）。

## Mobile Serverサービスの起動、停止、再起動

必要に応じてMobile ServerサービスをMobile Server Managerから起動、停止、再起動できます。

- これらのタスクのいずれかを実行するには、MobileServerManagerアイコンを右クリックし、**Mobile Serverサービスの起動**、**Mobile Serverサービスの停止**、または**Mobile Serverサービスの再起動**を選択します

## データ保護パスワードを変更

モバイルサーバーのデータ保護パスワードは、調査を暗号化するために使われます。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。

モバイルサーバーのデータ保護パスワードを変更するには：

1. Mobile Server Manager アイコンを右クリックして、**データ保護パスワードの設定を変更**を選択します。ダイアログボックスが表示されます。
2. **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。
3. **新しいパスワードを再入力**フィールドで新しいパスワードを再入力します。
4. (オプション) 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。
5. **OK**をクリックします。



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。

## ポート番号の表示/編集

1. Mobile Server Managerアイコンを右クリックして、**ポート番号の表示/編集**を選択します。
2. ポート番号を編集するには、関連するポート番号を入力します。標準ポート番号(HTTP接続用)および/または安全なポート番号(HTTPS接続用)を指定できます。
3. **OK**をクリックします。

## 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、証明書所有者が接続を確立することを承認されていることを裏付けます。詳細については、「[ページ40のレコーディングサーバー データ 暗号化 \(説明付き\)](#)」および「[ページ41のクライアントに対するモバイルサーバー暗号化の条件](#)」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見るとき、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：

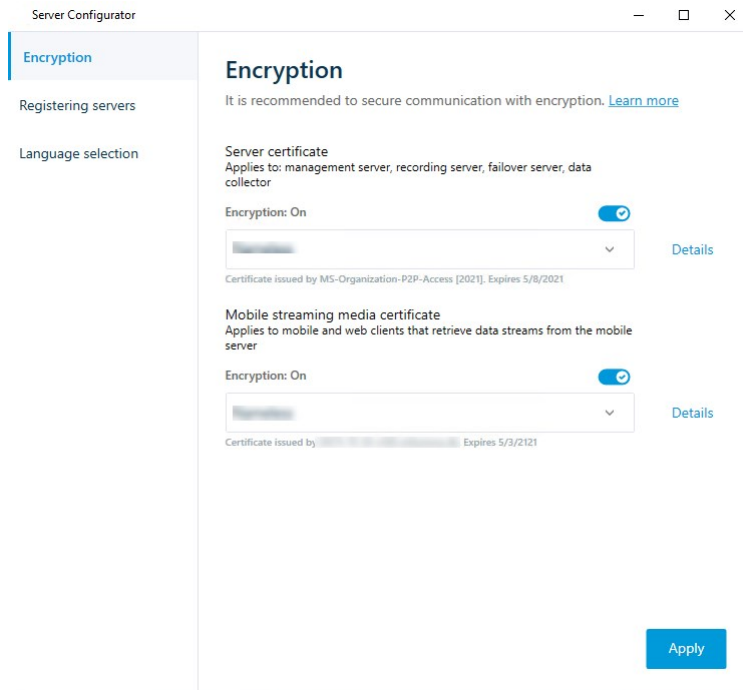
1. モバイルサーバーがインストールされているコンピュータで、以下から**Server Configurator**を開きます：
  - Windowsのスタートメニューまたは
  - Mobile Server Manager：コンピュータのタスクバーでMobile Server Managerアイコンを右クリック
2. **Server Configurator**の[モバイル ストリーミング メディア証明書]で[暗号化]をオンにします。



3. **証明書**の選択をクリックすると、秘密キーがあり、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証明書ストア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。

## ログへのアクセスおよび調査（説明付き）

Mobile Server Managerにより、その日のログファイルにアクセスし、ログファイルが保存されているフォルダーを開き、調査が保存されている先のフォルダーを開くことができます。

これらのいずれかを開くには、Mobile Server Managerアイコンを右クリックし、以下から選択します：

- 今日のログファイルを開く
- ログフォルダーを開く
- 調査フォルダーを開く

まだManagement ServerまたはRecording Serverによってログされていないアクションすべてに対して監査ログが作成されます。

以下のアクションは常にログされます（拡張監査ログが有効になっていない場合も同様です）。

- あらゆる管理作業（この監査ログメッセージには以前の値と新しい値が含まれます）
- 調査の作成、編集または削除に関するあらゆるアクション、エクスポートされた資料の準備とダウンロード、該当する構成の変更。監査ログには何が起きたのかに関する詳細が含まれます。



ビデオプッシュストリーミングは、拡張監査ログが有効になっている場合にのみログされません。



お使いのシステムから XProtect Mobileをアンインストールする場合、そのログファイルは削除されません。適切なユーザー権限のある管理者は後日、ログファイルにアクセスしたり、不要になれば削除したりできます。ログファイルのデフォルトでの場所は、**[プログラムデータ]**フォルダーです。ログファイルのデフォルトの場所を変更しても、既存のログは新しい場所へコピーされず、削除もされません。

## 調査フォルダーを変更

調査のデフォルトでの場所は、「**プログラムデータ**」フォルダーです。調査フォルダーのデフォルトの場所を変更しても、既存の調査は新しい場所に自動的にコピーされず、削除されることもありません。お使いのハードディスク上で調査エクスポートを保存するロケーションを変更するには。

1. Mobile Server Managerアイコンを右クリックし、**調査フォルダーの変更**をクリックします。  
**調査ロケーション**ウィンドウが開きます。
2. 既存のフォルダーの閲覧、あるいは新しいフォルダーを作成するには、**フォルダー**フィールドの隣の、現在のロケーションが表示されている場所にて、フォルダーアイコンをクリックし、**OK**をクリックします。

3. **以前の調査**リストから、現在のロケーションに保管されている既存の調査に適応したいアクションを選択します。オプションは以下のとおりです。

- **移動** 既存の調査を新しいフォルダーに移動します



もし既存の調査を新しいフォルダーに移動させない場合、それを閲覧することはできなくなります。

- **削除**：既存の調査を削除します
- **なにもしない** 既存の調査は現在のフォルダーの場所に残ります。調査フォルダーのデフォルトの場所を変更した後は、それらは表示できなくなります。

4. **[適応]** をクリックし、>をクリック**OK**。

## ステータスの表示（説明付き）

Mobile Server Managerアイコンを右クリックし、**ステータスの表示**を選択するか、Mobile Server Managerアイコンをダブルクリックしてウィンドウを開き、XProtect Mobileサーバーのステータスを確認します。以下の情報を表示できます。

名前	説明
サーバー実行日	XProtect Mobileサーバーが前回起動されたときの日付と時刻。
接続済みユーザー	現在XProtect Mobileサーバーに接続されているユーザーの数。
ハードウェアのデコード	XProtect Mobileサーバーでハードウェアアクセラレーションによるデコードが実行中かどうかを示します。
CPU使用率	現在XProtect Mobileサーバーが使用しているCPUの%。
CPU使用履歴	XProtect MobileサーバーによるCPU使用の履歴を詳しく示すグラフ。

## トラブルシューティング

### XProtect Mobileトラブルシューティング

#### 接続

1. **なぜXProtect Mobileクライアントから自分のレコーディング/XProtect Mobileサーバーに接続できないのでしょうか？**

録画コンテンツに接続するには、XProtectシステムを実行するサーバー、または専用サーバーにXProtect Mobileサーバーがインストールされていなければなりません。また、XProtectビデオ管理設定において、関連するXProtect Mobile設定も必要となります。これらはプラグインとして、または製品インストールやアップグレードの一環としてインストールされます。XProtect Mobileサーバーを取得する方法、およびXProtect Mobileクライアント関連の設定をXProtectシステムに統合する方法の詳細については、構成セクション（[ページ16のモバイルサーバーの設定](#)）を参照してください。

2. **ファイアウォールをオンにしましたが、モバイルデバイスをサーバーに接続できません。なぜでしょうか？**

XProtect Mobileサーバーのインストール時にファイアウォールをオフにしていた場合は、TCPとUDP通信を手動で有効にする必要があります。

3. **HTTPS接続を介してXProtect Web Clientを実行する際に、セキュリティ警告を避けるにはどうすればよいのでしょうか？**

警告は、証明書のサーバーアドレス情報が誤っていることが原因で発せられます。接続は暗号化されたままとなります。

XProtect Mobileサーバー内の自己署名証明書を、XProtect Mobileサーバーとの接続に使用するサーバーアドレスと一致している独自の証明書に置き換える必要があります。これらの証明書は、Verisignとった公式の証明書署名機関を介して取得します。詳細については、該当する署名機関にお問い合わせください。

XProtect MobileサーバーではMicrosoft IISは使用されません。つまり、署名機関によるIISを用いた証明書署名要求（CSR）ファイルの生成に関する説明は、XProtect Mobileサーバーには適用されません。CSRファイルは、コマンドライン証明書ツール、または類似したサードパーティの他のアプリケーションを使用して手動で作成する必要があります。このプロセスは、システム管理者および上級ユーザー以外は実行しないでください。

## 画質

### 1. XProtect Mobileクライアントでビデオを閲覧する際に、画質が良くないのはなぜでしょうか？

XProtect Mobileサーバーには、サーバーとクライアント間で利用できる帯域幅に応じて、自動的に画質を調整する機能があります。XProtect® Smart Clientよりも画質が悪い場合は、帯域幅が小さすぎるためにXProtect Mobileクライアントでフル解像度の画像を表示できないという状況が考えられます。その原因として、サーバーからの上流帯域幅が小さすぎるか、またはクライアントの下流帯域幅が小さすぎる可能性があります。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。

ワイヤレス帯域幅が混在しているエリアでは、帯域幅の良いエリアに入った時点で画質が改善することに気付くかもしれません。

### 2. オフィスのWiFiを介して自宅からXProtectビデオ管理システムに接続すると画質が悪くなるのはなぜでしょうか？

自宅のインターネットの帯域幅をお調べください。多くの家庭用インターネット接続では、ダウンロード/アップロード帯域幅が異なります（通常は20 Mbit/2 Mbitなど）。これは、ホームユーザーは大量のデータをダウンロードすることはあっても、インターネットにアップロードすることはほとんどないためです。XProtectビデオ管理システムではビデオをXProtect Mobileクライアントに送信する必要があり、そのプロセスは接続のアップロード速度に大きく依存します。XProtect Mobileクライアントのネットワークのダウンロード速度は良好でも、複数の場所で常に画質が低い場合は、自宅のインターネット接続のアップロード速度を高めると問題が解決する可能性があります。

## ハードウェアアクセラレーテッドデコーディング

### 1. 私が所有しているプロセッサはハードウェアアクセラレーテッドデコーディングに対応していますか？

Intelから販売されている比較的新しいプロセッサのみがハードウェアアクセラレーテッドデコーディングに対応しています。お持ちのプロセッサが対応しているかどうかは、Intelのウェブサイト (<https://ark.intel.com/Search/FeatureFilter?productType=processors/>) を参照してください。

メニューで [テクノロジー] > [Intel Quick Sync Video] が [はい] に設定されていることを確認してください。

お持ちのプロセッサが対応している場合、ハードウェアアクセラレーテッドデコーディングはデフォルトで有効になります。現在のステータスは、Mobile Server Managerの **ステータスを表示** で確認できます ([ページ59のステータスの表示 \(説明付き\)](#) を参照)。

### 2. 私が使用しているオペレーティングシステムはハードウェアアクセラレーテッドデコーディングに対応していますか？

XProtectがサポートしているオペレーティングシステムは、いずれもハードウェアアクセラレーションに対応しています。

必ずIntelウェブサイトに記載されている最新のグラフィックドライバーをシステムにインストールしてください。これらのドライバーは、Windowsアップデートでは入手できません。

モバイルサーバーが仮想環境にインストールされている場合、ハードウェアアクセラレーテッドデコーディングには対応しません。

3. どうすればモバイルサーバーでのハードウェアアクセラレーションデコーディングを無効にできますか？  
(上級)

モバイルサーバーのプロセッサがハードウェアアクセラレーテッドデコーディングに対応している場合、これはデフォルトで有効になります。ハードウェアアクセラレーテッドデコーディングをオフにするには、以下の手順に従います：

1. VideoOS.MobileServer.Service.exe.configを探します。パスは通常以下のようになっています：  
C:\Program Files\Milestone\XProtect Mobile Server\VideoOS.MobileServer.Service.exe.config
2. このファイルをメモ帳などのテキストエディターで開きます。必要に応じて、.configファイルタイプをメモ帳に関連付けます。
3. `<add key="HardwareDecodingMode" value="Auto" />`フィールドを探します。
4. 「Auto」値を「Off」に置き換えます。
5. ファイルを保存して閉じます。



[helpfeedback@milestone.dk](mailto:helpfeedback@milestone.dk)

#### Milestoneについて

Milestone Systemsはオープンプラットフォームの監視カメラ管理ソフトウェア (Video Management Software: 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ます。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Milestone Systemsの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。

