JVC

ネットワークビデオレコーダー

型名 **VR-X5100**

Milestone XProtect Professional 管理者マニュアル

本書では、本システムの設定について、VR-X5100 取扱説明書に掲載されていない応用設定方法や Management Application の詳細な設定項目について説明しています。

B5A-3416-00

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。

本書に記されているその他の商標はすべて、それぞれ該当する所有者の商標です。

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、まったくの偶然であり、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 Milestone 監視システムのインストールフォルダにあるファイル **3rd_party_software_terms_and_conditions.txt** にあります。

はじめに

このマニュアルについて

この文書には以下の製品が掲載されています。

- XProtect® Professional
- XProtect® Express

この文書は、最も多機能な XProtect Professional VMS 製品、XProtect Professional を使用する際のあらゆる設定と機能について解説しています。

XProtect Express 製品をご使用になる場合、ご利用いただける機能は同じではありません。ここでは、XProtect Professional 製品においてのみご利用いただける機能や装置を説明している場合があります。このような場合、この機能を利用できない旨が関連する項目のトップで表示されます。

ご自分のシステムで利用できる機能については、製品比較表 『12ページ の"製品比較チャート"参照 』を参照してください。

2017 R2 の販売から、XProtect Essential 製品は生産中止となり、XProtect Essential+が、無料でダウンロード、インストールできるようになっています。

これは、特に次のことを意味します。
- MIP SDK に対応しているため、サードパーティのアプリケーションやビジネスシステムを直接 XProtect Essential+に統合、埋め込みが可能です。
- 登録や再登録の必要はありません。ダウンロードしてご利用ください。

XProtect Essential+についての詳細は、弊社ウェブサイト『https://www.milestonesys.com/our-products/video-management-software/xprotect-essential/』をご覧ください。

製品比較チャート

XProtect Professional VMS には以下の製品が含まれます。

- XProtect Professional
- XProtect Express

全製品比較表は、 Milestone ウエブサイト『http://www.milestonesys.com/our-products/xprotect-software-suite』の製品一覧ページでご覧ください。

下記は各製品の主な違いのリストです。

名前	XProtect Express	XProtect Professional
配置の型	単一のサーバー	複数のサーバー

名前	XProtect Express	XProtect Professional
各システムの連結カメラの最大数	48	無制限
バックアップの記録サーバーの最大数	1	無制限
視聴クライアントユーザーの最大数	5	無制限
マイクロソフト・アクティブ・ディレクトリー・サポート	-	✓
アラームマネージャ	不完全	✓
マップ機能	シングル・レイヤーのみ	✓
ネットワークストレージへのアーカイブ	✓	✓
MIP SDK とサードパーティのアプリケーションの統合	✓	✓
Milestone Interconnect™	リモートサイト	リモートサイト
Customer Dashboard (カスタマー ダッシュボード)	✓	✓
リモート接続サービス	✓	✓
DVR 記録を閲覧する	-	-
オーディオ音声サポート	一方通信	両方向通信
パトロール設定済	✓	✓
パトロールを組み合わせて、種目の事前設定に行く	-	✓
外部システムの一般種目	✓	✓
種目ベースのマトリックス管理	-	✓

最低限のシステム要件について

重要：Microsoft® Windows® 2003 は、このシステムのサポート対象ではなくなりました（ただし、引き続き Windows 2003 のコンピュータからクライアントを実行/アクセスできます）。

重要：Microsoft® Windows® 32 ビット版 OS は、このシステムのサポート対象ではなくなりました（ただし、引き続き Windows 32 ビット版 OS のコンピュータから XProtect Web Client および XProtect Smart Client を実行/アクセスできます）。

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『http://www.milestonesys.com/SystemRequirements』をご覧ください。

ホスト名の命名について

VMS システムに関連して使用するホスト名は、Microsoft 命名標準に従う必要があります。つまり、すべてのホスト名は、ASCII 文字「a」から「z」（大文字と小文字を区別しない）、数字「0」から「9」、およびハイフン（「-」）のみ使用する必要があります。国または地域固有の文字が VMS で使用するコンポーネントのホスト名に含まれている場合は、システムとホストコンピュータ間で接続を確立できない場合があります。

監視システムを実行するコンピュータで管理者権限が必要です。管理者権限がない場合は、監視システムを設定できません。

重要なポート番号について

システムがコンピュータ、カメラ、その他のデバイスと通信するときには、特定のポートが使用されます。システムが可能なかぎりスムーズに動作することを保証するためには、システムを使用するときにネットワーク上でデータトラフィック用に次のポートが開いていることを確認してください。

名前	詳細
ポート 20 および 21（インバウンドおよびアウトバウンド）	FTP トラフィックに使用。 FTP（File Transfer Protocol）は、ネットワークでのファイル交換プロトコルの標準です。FTP はデータ転送で TCP/IP 標準を使用し、サーバーとの間でのファイルのアップロードやダウンロードで使用されます。
ポート 25（インバウンドおよびアウトバウンド）	SMTP トラフィックに使用。 SMTP（Simple Mail Transfer Protocol）はサーバー間での E メールメッセージ送信の標準です。一部のカメラは E メールで監視システムに画像を送信するので、このポートが空いている必要があります。
ポート 80（インバウンドおよびアウトバウンド）	監視サーバー、カメラ、XProtect Smart Client の間での HTTP トラフィックに使用。 監視システムの Image Server サービスのデフォルト通信ポートです。
ポート 554（インバウンドおよびアウトバウンド）	H.264 ビデオストリーミング接続時、RSTP トラフィックに使用します。
ポート 1024 (アウトバウンドのみ)	カメラと監視サーバーの間での HTTP トラフィックに使用。
ポート 1234（インバウンドおよびアウトバウンド）	イベントの処理で使用。
ポート 1237（インバウンドおよびアウトバウンド）	XProtect Central との通信で使用。
ポート 8081 および 8082	Mobile サービスとの通信で使用。

名前	詳細
ポート 22331	Event Server サービスとの通信で使用。

他のポート番号も使用できます。たとえば、サーバーアクセス 『156ページ 』ポートをデフォルトの 80 番ポートから別のポート番号に変更できます。

夏時間について

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。

重要：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。

タイムサーバーについて

システムがカメラから画像を受信するときには、これらの画像にはすぐにタイムスタンプが付けられます。ハードウェアデバイス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、ハードウェアデバイスの時刻と使用しているシステムの時刻が完全に同期しないことがあります。結果として、ハードウェアデバイス時刻とシステム時刻間で不一致がある場合は、ハードウェアデバイスの録画をすべて一緒に停止することがあります。

これを防止するには、時刻サーバーを使用して、カメラとシステム時刻を自動的に同期します。これにより、時刻同期を一貫させることができます。タイムスタンプをサポートしないカメラがあるため、時刻サーバーを使用する前に、カメラがこれをサポートすることを確認してください。

必要に応じて、時刻サーバーとして録画サーバーを使用できます 『263ページ の"ハードウェアデバイスの接続" 参照 』。

ウイルススキャンについて

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場所、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中断されたり、データベースが破損する場合さえあります。

ウイルススキャンを実行する必要がある場合は、録画データベースを含んでいる Recording Server ディレクトリをスキャンしないでください。録画サーバーディレクトリはデフォルトで c:¥mediadatabase¥に設定されています。すべてのフォルダもその場所にあります。

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。以前のバージョンのソフトウェアでは、デフォルトで、データベースはインストールフォルダに配置され、それぞれが録画されるデバイスの MAC アドレスを持つサブフォルダとなっています。

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、.pqz、.sts、.ts
- C:¥Program Files¥Milestone または C:¥Program Files (x86)¥Milestone およびすべてのサブディレクトリ。
- 次の 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 Professional VMS 製品	80, 25, 21, 1234, 1237, 22331
Milestone 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 Professional VMS 製品	RecordingServer.exe、ImageServer.exe、ManagementApplication.exe、ImageImportService.exe、RecordingServerManager.exe、VideoOS.ServiceControl.Service.exe、VideoOS.Event.Server.exe
Milestone 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。

システム概要

ソフトウェアとシステムコンポーネント

このシステムは多数のコンポーネントにより構成されており、それぞれ特定のタスクやユーザータイプをターゲットとしています。

ソフトウェアコンポーネント

Management Application	Management Application はカメラを追加し、ユーザーを設定し、システムを構成するメインアプリケーションです。 ライブ、再生、またはアーカイブビデオの表示には、Management Application を使用しません。代わりに、表示クライアントのいずれかを使用します。
XProtect® Smart Client	XProtect Smart Client は、セキュリティインストールの日常的な操作のためのクライアントです。合理化されたインターフェースにより、あらゆるサイズのインストールの監視、セキュリティインシデントの管理、ライブまたは録画されたビデオへのアクセスやエクスポートが簡単に行えます。 システムに接続し、ビデオを表示できるようにする任意のコンピュータで、XProtect Smart Client をインストールする必要があります。 Milestone では、監視システムに含まれている新しい特徴や機能を最大限に利用できるように、必ず最新バージョンの XProtect Smart Client を使用することを推奨しています。
Milestone Mobile	Milestone によって設計された、システムのビデオを表示できる無料のアプリケーションで、スマートフォンやタブレットで、ほぼどこからでも監視映像を見ることができます。 システムに接続し、ビデオを表示できるようにするすべてのデバイスで、Milestone Mobile をインストールする必要があります。 また、ドアの開閉や照明のオン/オフなどの出力を制御することができ、システムでのインシデントをコントロールし、ダイナミックに応答することができます。
XProtect® Web Client	※本機は、XProtect Web Client には対応していません。 大半のオペレーティングシステムや Web ブラウザからのビデオを表示、再生、共有できる、XProtect 監視システム用の簡素化された Web ベースのクライアントアプリケーション。 XProtect Web Client にアクセスするには、ソフトウェアをインストールする必要はありません。XProtect Web Client 経由でシステムにアクセスするには、監視システムのサーバーのアドレスを知っている必要があります。

システムコンポーネント

Recording Server サービス	Recording Server サービスを実行することで､デバイスから確実にビデオストリームがシステムに転送されます｡Recording Server サービスのインストールは自動的に行われ、監視システムサーバーでバックグラウンドで実行されます。 サービスは、Management Application で管理します。
Event Server サービス	組織全体でのマスター/スレーブ設定を含めて、監視システムがインストールされた、すべてのサーバーからのアラームやマップの設定を扱います。 Event Server サービスにより､アラームおよびシステム内で発生する可能性がある技術的な問題のモニターが可能になり、その概要が即時に表示できます。 イベントサーバーは、監視システムサーバーに自動的にインストールされ、バックグラウンドで実行されます。
Microsoft® SQL Server Express データベース	監視システムのアラームデータは、SQL Server Express データベースに保存されます。 SQL データベースは、完全版 SQL Server と比較して軽量にもかかわらず強力なバージョンです。自動的に監視システムサーバーにインストールされ、バックグラウンドで実行されます。
Image Server サービス	クライアントにログインしているユーザーの監視システムへのアクセスを処理します。 Image Server サービスのインストールは自動的に行われ、監視システムサーバーでバックグラウンドで実行されます。サービスは、Management Application で管理できます。
Download Manager	組織のユーザーが、監視システムサーバー上のようこそページからアクセス可能なシステム関連機能を管理します。

クライアント

クライアントは､Management Application でセットアップしたハードウェアデバイスのライブビューおよび録画ビデオの再生に使用するアプリケーションです。
システムでは、次の 3 種類の異なるクライアントをサポートしています。

- XProtect Smart Client
- Milestone Mobile クライアント
- XProtect Web Client　　※本機は、XProtect Web Client には対応していません。

XProtect Smart Client

XProtect Smart Client について

Milestone XProtect® IP ビデオ管理ソフトウェア用に設計された XProtect Smart Client は、セキュリティのインストールを直観的な方法で管理できる使いやすいクライアントアプリケーションです。XProtect Smart Client でセキュリティのインストールを管理することで、ユーザーはライブおよび録画ビデオ、カメラおよび接続済みのセキュリティデバイスの即時制御、録画の概要表示にアクセスできます。XProtect Smart Client は適応力の高いユーザーインターフェースを、複数の言語で使用できます。各オペレータの作業に応じて最適化し、特定のスキルや権限レベルに応じて調節が可能です。

このインターフェースで、部屋の照明やビデオの輝度に応じて、テーマの明暗を選択することで、特定の作業環境に合わせてカスタマイズすることができます。また、作業用に最適化されたタブや、統合ビデオタイムラインによって、監視の操作が簡単になります。MIP SDK を使用すると、さまざまな種類のセキュリティやビジネスのシステム、ビデオ分析アプリケーションを統合し、XProtect Smart Client を通じて管理することができます。

XProtect Smart Client をユーザー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 Application を通じて、クライアントの監視システムへのアクセスを管理します。クライアントが表示する録画データは、XProtect システムの Management Application 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 Smart Client をダウンロードするには、監視システムサーバーに接続する必要があります。接続すると、使用可能なクライアントの言語とバージョンを一覧表示するようこそページが表示されます。システム管理者は XProtect Download Manager を使用して、XProtect Download Manager のようこそページでユーザーに対して使用可能にするクライアントの言語とバージョンをコントロールできます。

Milestone Mobile クライアント

Milestone Mobile クライアントについて

※本機は、Windows Phone デバイスには対応していません。

Milestone 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。クライアントは、Android タブレットまたはスマートフォン、Apple®タブレットまたはスマートフォン、携帯ミュージックプレーヤー、Windows Phone 8 タブレットまたはスマートフォンなどで実行され、Management Client でセットアップされたカメラ、ビュー、その他の機能にアクセスすることができます。

Milestone 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 Milestone Mobile クライアントを使用したい場合は、モバイルサーバーを用意して、Milestone 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。モバイルサーバーをセットアップしたら、Google Play、App Store、Windows Phone Store から Milestone Mobile クライアントを無料でダウンロードし、Milestone Mobile の使用を開始します。

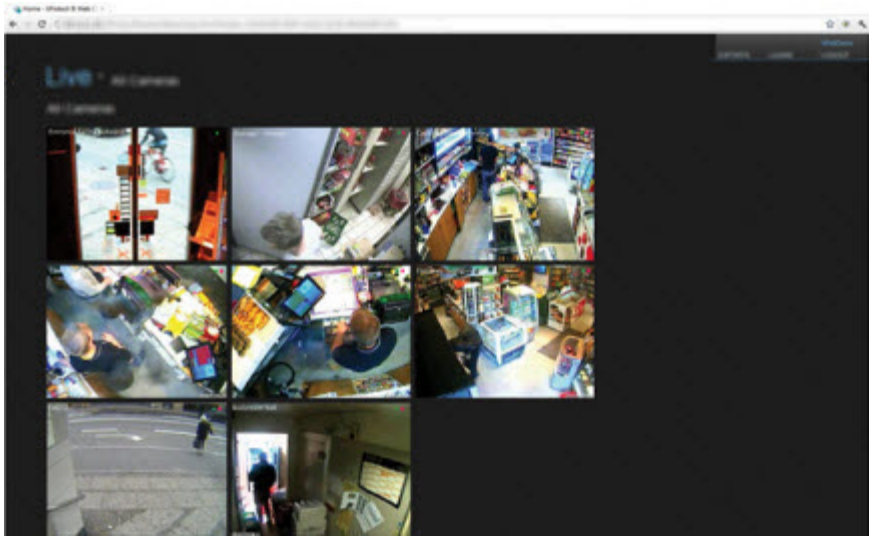
ビデオを XProtect システムにプッシュ配信するデバイスごとに必要なハードウェアデバイスライセンスは 1 つです。

XProtect Web Client

※本機は、XProtect Web Client には対応していません。

XProtect Web Client について

XProtect Web Client は、Web ベースのクライアントアプリケーションであり、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、証拠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。機能へのアクセスは、管理サーバーでセットアップされる個別のユーザー権限により異なります。



XProtect Web Client へのアクセスを有効にするには、モバイルサーバーを用意して、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。モバイルサーバーをセットアップしたら、インターネットアクセスが可能なコンピュータやタブレットで、どこからでも（適切な外部/インターネットアドレス、ユーザー名およびパスワードが分かっていることが必要）XProtect システムを監視することができます。

XProtect Web Client へのアクセス

Milestone 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、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、Milestone 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その他のすべてのコンピュータからアクセスできます。

1. Management Application で Milestone Mobile サーバーを設定します。
2. Milestone 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、システムトレイの Milestone Mobile サーバーアイコンを右クリックし、**[XProtect Web Client を開く]**を選択します。
3. Milestone 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 Explorer、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、Milestone 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：Milestone 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）。

ブラウザのアドレスバーに、標準 HTTP 接続を使用するか、安全な HTTPS 接続を使用するかによって、http://1.2.3.4:8081 または https://1.2.3.4:8082 と入力します。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。Milestone 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、この操作をリモートで強制的に実行する必要があります（この操作を実行できるのは、ドメインでの Internet Explorer だけです）。

Recording Server Manager

Recording Server サービスは、監視システムの重要な部分です。ビデオストリームがシステムに転送されるのは、Recording Server サービスが実行されている間だけです。Recording Server Manager が、Recording Server サービスの状態を通知します。また、サービスの管理も行います。

通知エリア（システムトレイ）で、Recording Server Manager のアイコンが Recording Server サービスが実行中であるかどうかを示します。

 - 通知エリアのアイコンが緑色であれば、Recording Server サービスは実行中です。

 - 通知エリアのアイコンが赤色であれば、Recording Server サービスは停止中です。

このアイコンを右クリックすると、Management Application の起動、Recording Server サービスの開始や停止、ログファイルの表示、バージョン情報の表示などを行うことができます。

システムステータスの監視

通知エリアの Recording Server アイコンを右クリックし、**システムステータスの表示** を選択すると、**ステータス**ウィンドウにアクセスできます。

ステータスウィンドウでは、画像サーバーや接続されているカメラのステータスを表示できます。それぞれのサーバー/カメラのステータスは、色によって示されます。

- **緑色**は、サーバーまたはカメラが正しく実行されていることを示しています。
- **灰色**は、**カメラ**（サーバーではなく）が実行中でないことを示しています。通常、以下の状況では、カメラが灰色で示されます。
  - カメラがオンラインでない（カメラのオンライン期間のスケジュールで指定）。
  - Recording Server サービスが停止している。
- **赤色**は、サーバーまたはカメラが実行されていないことを示しています。これは、接続の問題か、ネットワークまたはハードウェアエラーの可能性があります。エラーは、Recording Server ログファイルにリスト化されます。

ステータスウィンドウでマウスポインタをカメラの上へ移動させると、関連するカメラの詳細が表示されます。情報はポップアップとして表示され、約 10 秒毎に更新されます。

解像度	カメラの解像度。

FPS	現在カメラが使用している 1 秒あたりのフレーム数（フレームレート）。カメラが 50 フレームを受信する毎に、この数が更新されます。
フレームカウント	Recording Server サービスの起動後、カメラから受信したフレームの数。
受信(KB)	Recording Server サービスの起動後、カメラが送信したキロバイト数。
オフライン	エラーによってカメラがオフラインになった回数。

XProtect Download Manager

XProtect Download Manager では、組織がアクセスできるシステム関連機能を管理できます。監視システムサーバーの対象ウェルカムページから、XProtect Download Manager にアクセスできます。

- Windows の**スタート**メニューから Download Manager XProtect にアクセスするには**すべてのプログラム > Milestone XProtect Download Manager** > **Download Manager** を選択します。

ユーザーがアクセスできる機能の例

- **XProtect Smart Client**。ユーザーは、インターネットブラウザを通じて監視サーバーに接続します。ようこそページが表示されます。ようこそページで、XProtect Smart Client ソフトウェアをダウンロードし、使用しているコンピュータにインストールすることができます。
- **さまざまなプラグイン**。組織で監視システムと共にアドオン製品を使用している場合、このようなプラグインのダウンロードがユーザーにとって必要な場合があります。

ようこそページ（監視サーバー**Web** サイトのトップページ）

ようこそページには、さまざまな機能のダウンロードのリンクがあります。ユーザーは、ようこそページの右上のメニューで言語を選択できます。

ようこそページを表示するには、インターネットブラウザ（例、Internet Explorer バージョン 6.0 かそれ以上）を起動して、以下のアドレスに接続します。

```
http://[監視サーバーの IP アドレスまたはホスト名]
```

デフォルトのポート 80 以外のポート番号で Image Server サービスを設定（サーバーアクセスプロパティの一部として設定）している場合、ユーザーは以下のように IP アドレスまたはホスト名に加えて、コロンで区切ったポート番号も指定する必要があります。

```
http://[監視サーバーの IP アドレスまたはホスト名]:[ポート番号]
```

ようこそページの内容は、XProtect Download Manager によって管理されており、組織によって内容は異なります。

システムをインストールすると、ようこそページから、すぐにすべての言語で XProtect Smart Client にアクセスできます。64 ビットのオペレーティングシステムを実行している場合は 32 ビットまたは 64 ビット、32 ビットのオペレーティングシステムを実行している場合は 32 ビットの XProtect Smart Client をダウンロードすることができます。ようこそページの最初の表示内容は、XProtect Download Manager のデフォルト設定によって自動的に決まります。

XProtect Download Manager のデフォルト設定

XProtect Download Manager には、デフォルトの設定があります。これによって、監視システム管理者が何も設定しなくても、組織のユーザーは標準の機能にアクセスできます。XProtect Download Manager の構成は、ツリー構造で表現されます。

Download Manager のツリー構造の説明：

- **ツリー構造の 1 番目のレベル**は、現在作業をしているシステムを示しています。
- **2 番目のレベル**は、これがデフォルトの設定であることを示します。
- **3 番目のレベル**は、ようこそページで使用できる言語を示しています。この例では、ようこそページは多くの言語で使用できます（英語、アラビア語、デンマーク語、オランダ語、フランス語など）。
- **4 番目のレベル**は、ユーザーが使用できる機能を示します。たとえば、これらの機能を XProtect Smart Client に限定することができます。
- **5 番目のレベル（5）**は、それぞれの機能のバージョンを示しています。たとえば、バージョン 4.0、32 ビットなどをユーザーが使用できるようにすることができます。
- **6 番目のレベル（6）**は、ユーザーが使用できる機能の言語バージョンを示します。すべての言語が組み込まれている XProtect Smart Client では、唯一のオプションは**すべての言語**です。

標準機能だけが使用できるように初期設定されていることで、インストール時間が短縮でき、サーバーの容量が節約できます。誰も使用しない機能や言語バージョンをサーバーで有効にする必要はありません。必要であれば、より多くの機能および言語を使用可能にすることができます。

新しい機能を使用可能にする

新しい機能をインストールすると、これらの機能は XProtect Download Manager でデフォルトで選択され、ようこそページを通じてすべてのユーザーがただちに使用できるようになります。

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、ようこそページで機能を表示または非表示にすることができます。項目をドラッグして、関連する位置へドロップすることで、機能や言語がようこそページで表示される順番を変更することができます。

機能の非表示および削除

機能は、複数の方法で削除できます。

XProtect Download Manager のツリー構造のチェックボックスをクリアして、ようこそページで**機能を非表示にする**ことができます。この操作を行っても、その機能は依然として監視システムサーバーに存在しており、ツリー構造でチェックボックスを選択すれば、すぐに再度使用可能にすることができます。

以前に XProtect Download Manager で使用可能であった**機能を削除する**ことができます。この操作は、監視システムサーバーにある機能をアンインストールします。機能は XProtect Download Manager で表示されなくなりますが、その機能のインストールファイルは監視システムサーバーの**インストーラ**または関連する言語フォルダに保持されているので、必要に応じて、後から再インストールすることも可能です。操作方法：

7. XProtect Download Manager で、**機能の削除...**をクリックします。
8. **機能の削除**ウィンドウで、削除したい機能を選択します。
9. **OK** をクリックしてから、**はい**をクリックします。

ライセンス

※本機は、XProtect 標準のライセンス管理方式には対応していません。

ライセンスについて

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。
- ソフトウェアライセンスファイル(SLA)。.lic 拡張子と SLC (ソフトウェアライセンスコード)に基づく名前が付いています。

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 ソフトウェアライセンスファイルには、購入した VMS 製品とライセンスに関するすべての情報が含まれています。 Milestone は、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し、後から見つけられるようにすることをお勧めします。ソフトウェアライセンスファイルには、購入した VMS 製品とライセンスについての情報がすべて含まれています。Milestone は、SLC についての情報とソフトウェアライセンスファイルのコピーを後で探せるように安全な場所に保管することをおすすめします。SLC は**ヘルプ**のメニュー内にある**>概要**でも見られます。

まず、Web サイトからソフトウェアをダウンロードします。ソフトウェアをインストール 『33ページ の"システムソフトウェアのインストール"参照 』している間に、ソフトウェアライセンスファイルを提供する必要があります。 まだソフトウェアライセンスファイルを受け取っていない場合でも、ソフトウェアをインストールし、最大 8 台のカメラを追加し、最大 5 日間の保持期間内で、30 日間の試用期間の間実行することができます。システムを使用し続けるには、試用期間が終了する前に、ソフトウェアライセンスファイルをインポート 『37ページ の"新しいソフトウェアライセンスファイルのインポート"参照 』する必要があります。

いったんインストールを完了してライセンスをアクティブにすると、 **スタート**ページで、現在インストールされているライセンスの概要『26ページ の"ライセンス情報の概要"参照 』を確認できます。たとえば、My Milestone ユーザーアカウントの作成、リセラーへのサポートの連絡、およびシステムを変更する必要がある場合などには、ソフトウェアライセンスファイルまたは SLC が必要になる場合があります。

少なくとも 2 つのライセンスを購入しています。

基本ライセンス：最低限、XProtect 製品のいずれかの基本ライセンスがあります。XProtect アドオン製品には 1 つ以上の基本ライセンスがある場合もあります。

ハードウェアデバイスライセンス：XProtect システムに追加するすべてのハードウェアデバイスには、ハードウェアデバイスライセンスが必要です。カメラに接続されたスピーカー、マイク、または入出力デバイスのハードウェアデバイスライセンスは不要です。複数のカメラをビデオエンコーダーに接続している場合でも、必要なハードウェアデバイスライセンスはビデオエンコーダーIP アドレスにつき 1 つだけです。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。

詳細については、MilestoneWeb サイト 『https://www.milestonesys.com/supported-hardware』でサポートされているハードウェアの一覧を参照してください。Milestone Mobile でビデオプッシュ機能を使用する場合は、システムに動画をプッシュするモバイルデバイスまたはタブレットごとに 1 つのハードウェアデバイスライセンスも必要です。ハードウェア・デバイス・ライセンスが不足している場合は、あまり重要でないハードウエアを無効にして 『73ページ の"カメラの無効化または削除"参照 』、新しいハードウエア・デバイスが代わりに動作するようにできます。また、ご使用のカメラに**付いていない**デバイスのためにハードウエア・デバイス・ライセンスが必要になる場合もあります。カメラに付属していないデバイスの例としては、周辺探知器や一部のタイプのオーディオ・デバイスやインプット/アウトプットボックス等があります。ウエブサイトの

『https://www.milestonesys.com/supported-hardware』「ハードウエア・サイト・サポート」Milestone をご覧ください。

ほとんどの XProtect アドオン製品には追加のライセンスタイプが必要です。ソフトウェアライセンスファイルには、アドオン製品のライセンスの情報も含まれています。一部のアドオン製品には、個別のソフトウェアライセンスファイルがあります。アドオン製品のライセンスについては、以下を参照してください。

- XProtect Access 『148ページ の"XProtect Access ライセンス"参照 』
- XProtect LPR 『173ページ の"LPR ライセンス"参照 』
- XProtect Transact
- XProtect Retail と XProtect Screen Recorder の追加製品ライセンスについては、これらの製品ドキュメンテーションをご覧ください。

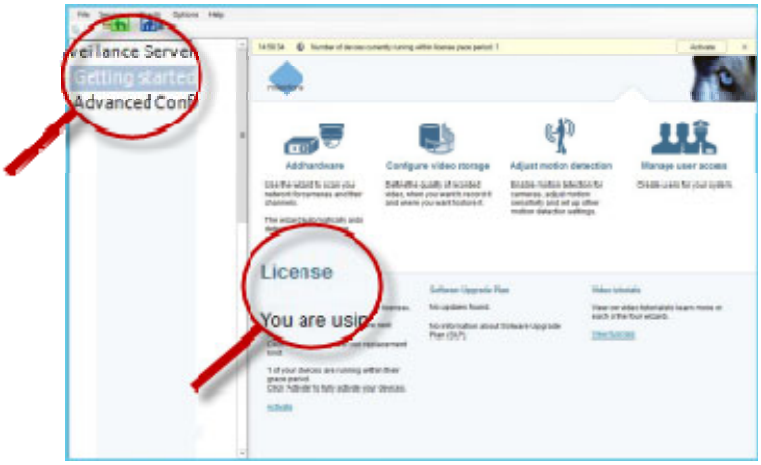
XProtect Express の場合

仮想サーバーに VMS 製品をインストールする場合は、ライセンスを有効にする必要があります。このドキュメントのライセンスの有効化に関する説明、猶予期間、関連する他のライセンス供与はあなたのインストールに適用されます。

ただし、物理サーバーに VMS 製品をインストールする場合は、すべての購入済みライセンスがあらかじめ有効化されているため、任意の数のハードウェアデバイスを変更および交換できます。猶予期間、終了した猶予期間、またはライセンスがない場合は、ライセンスをもつことができません。ライセンスを購入したよりも多くのハードウェアデバイスまたは他のライセンス付きデバイスを追加できないためです。VMS 製品のライセンスまたはアップグレードを追加購入する場合は、手動で有効化して、新しいライセンスまたは新しい機能を利用する必要があります。詳細については、追加ライセンスの取得 『30ページ 』またはアップグレード 『36ページ の"アップグレードについて"参照 』を参照してください。

ライセンス情報の概要

左下端の**[ライセンス]**の下の**[スタート]**ページで、ハードウェアデバイスライセンスに関する次の情報を参照してください。



- このサーバーで人法されたハードウェアデバイスライセンス数と、同じソフトウェアライセンスファイルの一部として購入したハードウェアデバイスライセンスの合計すう。
- マスター/スレーブ設定の複数の監視システムで、同じソフトウェアライセンスファイルが共有される場合は、ライセンス概要には、すべてのシステム用に購入したライセンスの同じ合計数が表示されます。

XProtect Professional のみがマスター/スレーブ設定機能をサポートします。

空きライセンス数を確認するには、すべてのシステムで認証済みのライセンス数を追加し、この数を購入済みライセンスの合計数から差し引きます。あるいは、ソフトウェア登録用の当社の Web サイト『http://online.milestonesys.com/』をご覧ください。

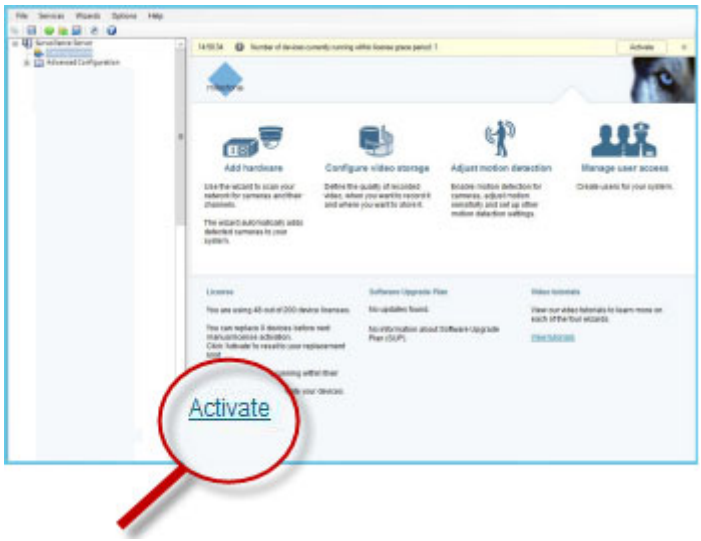
- VMS システムの各サーバーに追加できるハードウェアデバイスの最大数。この最大値を超えるには、より高度な XProtect VMS 製品にアップグレードする必要があります。この場合は、詳細について、リセラーまでお問い合わせください。

- 認証せずに交換または追加した認証済みハードウェアデバイス数。
  [アクティベーションなしの変更]列には、ハードウェアデバイスライセンスを認証せずに交換または追加できるハードウェアデバイス数と、前回の認証以降に行った変更数が示されます。アクティベーションなしのデバイスの変更数内で追加されたハードウェアデバイスは完全に認証されたハードウェアデバイスライセンスとして実行され、[ハードウェアデバイス概要] 『29ページ の"ハードウェアデバイスの概要"参照 』テーブルに**[ライセンス]**ステータスが表示されます。認証なしでデバイスを追加または交換できるため、柔軟にシステムの日常メンテナンスを行えます。詳細については、「アクティベーションなしのデバイスの変更 『28ページ 』」を参照してください。

- 30 日間の猶予期間で実行中のハードウェアデバイス数。認証なしのデバイス変更数を使い切った場合、または購入したライセンスより多いハードウェアデバイスを追加した場合は、追加されたハードウェアデバイスが猶予期間で実行されます。猶予期間が終了すると、カメラが無効になり、システムへのビデオの送信を停止します。ハードウェアデバイスの最初の猶予期間が終了する日時を確認することもできます。

メンテナンスの容易性と柔軟性のため、VMS システムは、ハードウェアデバイスを追加または削除するたびに、自動的にオンラインでライセンスを認証するように設定されています。当然、自動ライセンス認証 『27ページ の"自動ライセンス認証について"参照 』では、システムがインターネットに接続されている必要があります。

システムがインターネットに接続していない状態で、認証なしのデバイス変更数内でハードウェアデバイスを追加または交換したり、猶予期間で実行中のハードウェアデバイスを追加したりした場合は、**[認証]**リンクをクリックして、ハードウェアデバイスライセンスを認証してください。アクティベーションなしのデバイスの変更数は、新しい数の認証済みライセンスを反映します。十分なライセンスを購入すると、以前に猶予期間であったハードウェアデバイスは認証済みになります。詳細については、「ライセンス認証について 『30ページ 』」を参照してください。



自動ライセンス認証について

※本機は、XProtect 標準の自動ライセンス認証には対応していません。独自のライセンス管理により、ハードウェアデバイス追加直後に自動的にライセンスが有効になります。

Milestone は、監視システムをオンラインにし、ライセンスが自動的に認証されるようにすることをお勧めします。

システムがオンラインの場合、変更を行った数分後に、ハードウェアデバイスまたは他のライセンスが認証されます。結果：

- ライセンス認証を手動で開始する必要がありません
- 使用済みのアクティベーションなしのデバイスの変更数は常にゼロです
- 購入したハードウェアデバイスライセンスで許可された数を超えるハードウェアデバイスを追加しないかぎり、ハードウェアデバイスは猶予期間ではありません。

場合によっては、ライセンスを手動で認証しなければならないことがあります。たとえば、追加ライセンスを購入し、Milestone Care サブスクリプション 『45ページ の"スタートページについて"参照 』を購入または予約するか、Milestone がアクティベーションなしのデバイスの変更 『28ページ 』数を引き上げた場合などです。

アクティベーションなしのデバイスの変更**[スタート]**ページの**[アクティベーションなしの変更]**には、ハードウェアデバイスライセンスを認証せずに交換または追加できるハードウェアデバイス数と、前回の認証以降に行った変更数が示されます。

アクティベーションなしのデバイスの変更で追加されたハードウェアデバイスは完全に認証されたハードウェアデバイスライセンスとして実行され、[ハードウェアデバイス概要] 『29ページ の"ハードウェアデバイスの概要"参照 』テーブルに**[ライセンス]**ステータスが表示されます。 最後のライセンス認証から 1 年が経過すると、使用済みの**アクティベーションなしのデバイスの変更**の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、ライセンスを認証せずに、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。

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、「アクティベーションなしのデバイスの変更数の計算方法 『28ページ 』」を参照してください。

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必要がある理由を説明する必要があります。Milestone は個別にそれぞれの依頼を決定します。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数の計算方法

アクティベーションなしのデバイスの変更は、3 つの変数に基づいて計算されます。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。

- 認証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認証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%**変数による認証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、値は通知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。

製品の現在のデフォルト値の詳細については、My Milestone『http://www.milestonesys.com/device-change-calculation』をご覧ください。

C% = 15%、Cmin = 10、Cmax =100 に基づく例

お客様が 100 個のハードウェアデバイスライセンスを購入します。100 台のカメラをシステムに追加します。自動ライセンス認証を有効にしていない場合は、アクティベーションなしのデバイスの変更はゼロです。ライセンスを認証すると、アクティベーションなしのデバイスの変更が 15 になります。

お客様が 100 個のハードウェアデバイスライセンスを購入します。100 台のカメラをシステムに追加し、ライセンスを認証します。アクティベーションなしのデバイスの変更は現在 15 です。お客様は、システムから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 台のデバイスが認証され、アクティベーションなしのデバイスの変更数は 14 まで減りました。

お客様が 1000 個のハードウェアデバイスライセンスを購入します。1000 台のカメラを追加し、ライセンスを認証します。アクティベーションなしのデバイスの変更数は現在 100 です。**C%**変数に従い、アクティベーションなしのデバイスの変更数が 150 になりましたが、**Cmax** 変数のためアクティベーションなしのデバイスの変更数は 100 以下に制限されています。

お客様が 10 個のハードウェアデバイスライセンスを購入します。10 台のカメラをシステムに追加し、ライセンスを認証します。**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数は現在 10 です。数が **C%**変数にのみ基づいて計算されている場合は、1 (10 の 15% = 1.5、1 に切り捨て)しかありません。

お客様が 115 個のハードウェアデバイスライセンスを購入します。100 台のカメラをシステムに追加し、ライセンスを認証します。アクティベーションなしのデバイスの変更は現在 15 です。認証せずに別の 15 台のカメラを追加します。アクティベーションなしのデバイスの変更 15 のうち 15 を使用します。50 台のカメラをシステムから削除し、アクティベーションなしのデバイスの変更は 7 まで下がります。つまり、アクティベーションなしのデバイスの変更 15 を使用して前に追加したカメラ 8 台が猶予期間になります。お客様は 50 台の新しいカメラを追加します。前回ライセンスを認証したときにシステムで 100 台のカメラを認証したため、アクティベーションなしのデバイスの変更は 15 に戻ります。猶予期間になった 8 台のカメラはアクティベーションなしのデバイスの変更として元の状態に戻ります。50 台の新しいカメラは猶予期間になります。

ハードウェアデバイスの概要

ハードウェアデバイスライセンスとチャネルのステータスの概要は、**詳細設定 > ハードウェアデバイス**を展開することで確認できます。**[ハードウェアデバイスの概要]**テーブルには次の情報が含まれます。

名前	詳細
ハードウェアデバイス名	ハードウェアデバイスの名前
ライセンス	ハードウェアデバイスのライセンスステータス。以下のステータスを表示できます。**ライセンス済み**、**猶予期間**、**評価試用期間**、または**期限切れ**の[日数]。
ビデオ チャンネル	ハードウェアデバイスで使用可能なビデオ チャンネルの数。
スピーカー チャンネル	ハードウェアデバイスで使用可能なスピーカー チャンネルの数。
マイク チャンネル	ハードウェアデバイスで使用可能なマイク チャンネルの数。
アドレス	ハードウェアデバイスの HTTP アドレス

名前	詳細
WWW	ハードウェアデバイスの Web アドレスへのリンク。
ポート	ハードウェアデバイスが使用するポート。
デバイスドライバー	ハードウェアデバイスに関連付けられているデバイスドライバーの名前。

ハードウェアデバイスの交換について

レコーディングサーバーからハードウェアデバイスを取り外し、構成を保存すると、デバイスライセンスに空きができます。デバイスを無効にするだけでは、ライセンスが解放されません。ライセンスが適用されたハードウェアデバイスを新しいハードウェアデバイスと交換し、新しいデバイスを認証してライセンスを付与できます。購入したハードウェアデバイスライセンスの総数は、監視システムで同時に実行できるハードウェアデバイスの合計数に対応します。

ハードウェアデバイスを交換する場合、**ハードウェアデバイスの交換**ウィザード『64ページ の"ハードウェアデバイス交換ウィザードについて"参照 』を使用して、カメラ、マイク、入力、出力などのすべての関連するデータベースを割り当てる必要があります。これが完了したら、ライセンスをアクティベートすることを忘れないでください。

追加ライセンスの取得

※本機は、XProtect 標準のライセンス方式には対応していません。追加ライセンスについては本機の取扱説明書を参照してください。

現在所有していないライセンスが必要なその他のハードウェアデバイスまたはその他のコンポーネントを追加する場合は、追加ライセンスを購入し、猶予期間中にデバイスがシステムにデータを送信できるように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バージョンの新しいライセンス：

- ライセンスを手動で認証し、新しいライセンスを入手します。

  詳細については、「ライセンスを認証（オンライン）『31ページ の"ライセンスをオフラインで認証"参照 』）または「ライセンスを認証（オフライン）『31ページ の"ライセンスをオンラインで認証"参照 』）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された監視システムバージョン：

- 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。

ライセンス認証について

※本機は、XProtect 標準のライセンス方式には対応していません。ライセンス認証は不要です。

監視システムがオフラインの場合、または手動ライセンス認証を実行する場合にのみ、このトピックが適用されます。システムがオンラインの場合、ライセンスは自動的に認証されます。詳細については、「自動ライセンス認証について 『27ページ 』」を参照してください。

VMS をインストールし、ハードウェアデバイスを追加すると、30 日間の猶予期間でハードウェアデバイスが実行されます。30 日の猶予期間が終了する前に、ハードウェアデバイスライセンスを認証する必要があります。そうでない場合は、ハードウェアデバイスはビデオを監視システムに送信しなくなります。

Milestone は、システムおよびハードウェアデバイスに最終調整を加える前に、ライセンスを認証することをお勧めしています。詳細については、「ライセンスを認証（オンライン) 『31ページ の"ライセンスをオフラインで認証"参照 』) または「ライセンスを認証 (オフライン)『31ページ の"ライセンスをオンラインで認証"参照 』) を参照してください。

購入したハードウェアデバイスライセンス数を超えるハードウェアデバイスを追加した場合は、ハードウェアデバイスが猶予期間で実行されます。猶予期間が終了した後にこれらのハードウェアデバイスからビデオを表示する場合は、追加のライセンスを購入 『30ページ の"追加ライセンスの取得"参照 』する必要があります。重要性の低いカメラは無効 『64ページ の"ハードウェアデバイスの削除/無効化"参照 』にし、新しいハードウェアデバイスを実行できるようにすることもできます。

マスター/スレーブ設定で複数の VMS 製品がインストールされている場合は、各インストールからライセンスを認証し、各インストールで更新および認証された.lic ファイルを取得します。これは、すべての VMS 製品が同じソフトウェアライセンスファイルを共有する場合にも当てはまります。

ライセンスをオンラインで認証

監視システムがオフラインの場合、または手動ライセンス認証を実行する場合にのみ、このトピックが適用されます。システムがオンラインの場合、ライセンスは自動的に認証されます。詳細については、「自動ライセンス認証について 『27ページ 』」を参照してください。

追加ライセンスを購入したか、アップグレードする場合は、ライセンスを手動で認証する必要があります。Management Application を実行するコンピュータがインターネットに接続している場合は、手動オンライン認証を実行できます。

1. **[ファイル]**メニューで**[ライセンスを認証(オンライン)]**を選択します。
2. **[オンラインでのライセンス取得]**ダイアログボックスが開き、ライセンスが認証されます。

ライセンスをオフラインで認証

監視システムがオフラインの場合、または手動ライセンス認証を実行する場合にのみ、このトピックが適用されます。システムがオンラインの場合、ライセンスは自動的に認証されます。詳細については、「自動ライセンス認証について 『27ページ 』」を参照してください。

次の場合にはライセンスを手動で認証する必要があります。

- 追加ライセンスを購入した、アップグレードしたい
- Milestone Care サブスクリプション 『45ページ の"スタートページについて"参照 』を購入または更新した
- Milestone から付与されたアクティベーションなしのデバイスの変更 『28ページ 』数が増えた

1. **[ファイル]**メニューで**[ライセンスを認証(オフライン)]**を選択します。
2. **[エクスポート]**をクリックして、ライセンスリクエストファイルをエクスポートします。
3. ライセンスリクエストファイルには、自動的に SLC と同じ名前が付けられます。複数のサイトがある場合は、必ず名前を一意にし、どのファイルがどのサイトに属しているのかを簡単に識別できるようにしてください。

4. ライセンスリクエストファイル(.lrq)をインターネットに接続したコンピュータに接続し、当社のソフトウェア登録用 Web サイト 『http://online.milestonesys.com/』にログインします。
5. ライセンスリクエストファイルと同じ名前の認証済みソフトウェアライセンスファイル(.lic)を Management Application がインストールされたコンピュータにコピーします。
6. 手順 1 で開いたダイアログボックスで、**[参照]**をクリックして、認証済みのソフトウェアライセンスファイルを使用します。
7. **実行**をクリックします。

Management Application を実行するコンピュータがインターネットに接続していない場合、ライセンスをオフラインで認証できます。

猶予期限が切れた後にライセンスを認証する

猶予期間内にハードウェアデバイスまたはアドオン製品で使用される他のデバイスのライセンスを認証しない場合、デバイスが使用できなくなり、データを監視システムに送信できません。

- デバイス、構成、およびその他の設定は、システム構成から削除されません。
- 期限切れのデバイスからもう一度データを受信するには、ライセンスを認証します。

詳細については、「ライセンスを認証（オンライン) 『31ページ の"ライセンスをオフラインで認証"参照 』）または「ライセンスを認証（オフライン) 『31ページ の"ライセンスをオンラインで認証"参照 』）を参照してください。

インストールとアップグレード

システムソフトウェアのインストール

※本機は、システムソフトウェアのインストールには対応していません。

監視ソフトウェアは、マウントしたドライブにはインストールしないでください。マウントしたドライブとは、ドライブ文字の代わりにラベルまたは名前が付いている、NTFS（NT ファイルシステム）ボリュームの空のフォルダにマップされたドライブです。マウントしたドライブを使用すると、重要なシステム機能が想定どおりに作動しないことがあります。たとえば、システムがディスクの空き容量を超えて実行されても、警告が表示されません。

はじめに：既存の監視ソフトウェアをすべて停止します。アップグレードする場合は、まず、「ある製品バージョンから、別の製品バージョンへのアップグレード 『36ページ の"ある製品バージョンから、別の製品バージョンへのアップグレード"参照 』」をお読みください。

1. インストールファイルを実行します
2. 以前のシステムがインストールされている場合、または他の XProtect Professional VMS 製品がインストールされている場合、システムがこのインストールを検知して、新しいバージョンのインストール後に以前のバージョンが削除されることを通知します。これを承諾する場合は、**はい**をクリックして、インストールを続行します。以前のバージョンでの記録や設定は、すべて新しいバージョンで使用できます。
3. インストーラで使用する言語を選択してから、**続行**をクリックします。
4. SLC に関連する名前のソフトウェアライセンスファイルがない場合は、**試行**を選択して、システムソフトウェアの 30 日試行版をインストールします。ソフトウェアライセンスファイルがある場合は、まずローカルドライブに保存します。ネットワークドライブまたは USB スティックから直接インポートしないでください。ソフトウェアライセンスファイルの保存場所を入力するか、**[参照]**をクリックしてインポートします。
5. 使用許諾契約を読み、同意します。チェックボックスを選択し、**カスタマーダッシュボード**へのアクセスを有効にします。
6. **標準**または**カスタム**インストールを選択します。**カスタム**インストールを選択した場合、アプリケーション言語、インストールする機能、およびインストール場所を選択できます。インストールウィザードが完了するのを待ちます
7. 試用版をインストールしている場合は、インストール完了後に Management Application を起動し、たとえば XProtect Professional などの XProtect Professional VMS 製品を使用するかどうかを選択します。

これで、システムの設定 『39ページ の"Management Application のシステムの構成"参照 』を始めることができます。

XProtect Smart Client のインストール

XProtect Smart Client を使用するには、事前にコンピュータにインストールする必要があります。XProtect Smart Client を監視システムサーバーからダウンロードして使用するコンピュータへインストールするか、DVD から直接インストールします。

開始する前に、Milestone の Web サイトにアクセスし、使用している PC が XProtect Smart Client の最低限のシステム要件 『http://www.milestonesys.com/SystemRequirements』を満たしていることを確認して下さい。

管理サーバーからの XProtect Smart Client のインストール

1. Internet Explorer を開き、URL またはサーバーの IP アドレスを使用して管理サーバーに接続します。
2. **ようこそ**ページで、**言語**をクリックして、使用する言語を選択します。
3. **XProtect Smart Client 設定**ウィザードが起動されます。ウィザードで、インストール手順に従ってください。

ウィザードがインストールパスを推奨します。通常は、推奨されたインストールパスを使用します。ただし、アドオン製品を以前に使用したことがある場合、このパスが有効ではなくなっていることがあります。

XProtect Smart Client のサイレントインストール

※本機は、XProtect Smart Client のサイレントインストールには対応していません。

監視システム管理者は、Microsoft Systems Management Server (SMS)などのツールを使用して、システムまたは XProtect Smart Client をユーザーのコンピュータに展開できます。このツールを使って、ローカルネットワークにあるハードウェアとソフトウェアのデータベースを構築できます。このデータベースを使用することによって、ソフトウェアアプリケーションをローカルネットワークを通じて配布、インストールすることができます。

サイレントインストールを行うには：

1. XProtect Smart Client .exe ファイル **XProtect Smart Client 2017 R2 Installer x64.exe** を探します。このファイルを、**httpdocs** フォルダの下のサブフォルダで検索します。**httpdocs** フォルダは、Milestone 監視ソフトウェアがインストールされているフォルダの下にあります。

   通常のパスは(英語版の XProtect Smart Client を使用している場合)、
   C:¥Program Files (x86)¥Milestone¥Milestone Surveillance¥httpdocs¥XProtect Smart Client Installer¥[バージョン番号] [ビットバージョン]¥All Languages¥en-US です。

   例:
   C:¥Program Files (x86)¥Milestone¥Milestone Surveillance¥httpdocs¥XProtect Smart Client Installer¥2016 (64-bit)¥All Languages¥en-US

2. 以下の 2 つのオプションのいずれかを使用してサイレントインストールを実行してください。

   a) デフォルトパラメータ設定を使用して実行する:

   すべてのパラメータにデフォルト値を使用してサイレントインストールを実行するには、インストールプログラムが保存されているディレクトリでコマンドプロンプト(cmd.exe)を起動して、以下のコマンドを実行します。

   - XProtect Smart Client:

     XProtect Smart Client 2017 R2 Installer x64.exe --quiet

     使用しているシステム：

     Milestone XProtect Professional VMS Products 2017 R2 System Installer.exe --quiet

このコマンドでは、ターゲットディレクトリなどのパラメータにデフォルト値を使用して XProtect Smart Client のサイレントインストールが実行されます。デフォルト設定を変更する方法については、以下を参照してください。

b) XML 引数ファイルを入力として使用して、デフォルトパラメータをカスタマイズします：

デフォルトインストールの設定をカスタマイズするには、値が変更された XML ファイルを入力として提供する必要があります。デフォルト値が記述された XML ファイルを生成するには、インストールプログラムが保存されているディレクトリでコマンドプロンプトを起動して、以下のコマンドを実行します:

- XProtect Smart Client:

  XProtect Smart Client 2017 R2 Installer x64.exe --generateargsfile=[パス]

- 使用しているシステム：

  Milestone XProtect Professional VMS Products 2017 R2 System Installer.exe --generateargsfile=[パス]

生成された arguments.xml ファイルをテキストエディタで開き、必要な変更を行います。次に、同じディレクトリで以下のコマンドを実行して、修正されたバージョンのサイレントインストールを実行します。

- XProtect Smart Client:

  XProtect Smart Client 2017 R2 Installer x64.exe --arguments=[完全パス]args.xml --quiet

- 使用しているシステム：

  Milestone XProtect Professional VMS Products 2017 R2 System Installer.exe --arguments= [完全パス]args.xml --quiet

ビデオデバイスドライバーのインストール

※本機は、ビデオデバイスドライバーのインストールには対応していません。

ビデオデバイスドライバーは、システムの初回のインストール時に自動的にインストールされます。XProtect Device Pack という新しいバージョンのビデオデバイスドライバーが適宜リリースされ、Milestone の Web サイト 『http://www.milestonesys.com/』で提供されています。Milestone では、常に最新バージョンのビデオデバイスドライバーを使用することを推奨しています。ビデオデバイスドライバー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。

新しいビデオデバイスドライバーのインストールを開始すると、インストールが完了して Recording Server サービスを再起動するまで、システムはカメラデバイスと通信できなくなります。通常、この処理は数分程度で完了しますが、Milestone では、重要な事象が発生する可能性が低いときに更新処理を行うことを強くお勧めしています。

ビデオデバイスドライバーをインストールするには：

1. 新しいバージョンのビデオデバイスドライバーをインストールするシステムサーバーで、実行中の Recording Server サービスを含む、実行中のすべての監視ソフトウェアを停止します。
2. XProtect Device Pack インストールファイルを実行し、ウィザードの指示に従います。
3. ウィザードが完了すると、Recording Server サービスが再起動します。

ウィザードで CSV ファイルからインポートしたハードウェアデバイスを追加するオプションを使用する場合、カメラとサーバーがオフラインであれば、まず追加したいそれぞれのハードウェアの**ハードウェアドライバーID** を

指定する必要があります。ID の現在のリストを表示する方法は、組織で使用している XProtect Device Pack のリリースノートを参照してください。あるいは、Milestone の Web サイト『http://www.milestonesys.com/』で最新情報ご確認ください。

アップグレード

※本機は、アップグレードには対応していません。

アップグレードについて

システムをアップグレードし、その他のより拡張した機能を使用する場合は、複数の方法でこれを実行できます。次の操作に従ってください。

- たとえば XProtect Professional 2013 から XProtect Professional 2016 へアップグレードするなど、あるバージョンの製品から、同じ製品の新しいバージョンへのアップグレード 『36ページ の"ある製品バージョンから、別の製品バージョンへのアップグレード"参照 』。
- たとえば XProtect Express から XProtect Professional へアップグレードするなど、ある XProtect 製品から別の XProtect 製品へのアップグレード。 『36ページ の"現在の製品バージョンから別の最新 XProtect Professional VMS 製品へのアップグレード"参照 』また、必要に応じて製品をダウングレードすることもできます。

更新について

Milestone では、サービスアップデートをリリースし、機能を向上させ、新しいデバイスをサポートしています。新しいバージョンの VMS ソフトウェアが使用可能な場合は、黄色の通知バーにメッセージが表示され、ソフトウェアを更新できることが通知されます。

Milestone は、最新バージョンの監視ソフトウェアを常にインストールし、ソフトウェアが極力スムーズに動作するように保証することをお勧めします。

ある製品バージョンから、別の製品バージョンへのアップグレード

たとえば XProtect Professional 2016 R1 から XProtect Professional 2016 R2 へのアップグレードなど、システム構成全体をある製品バージョンから別の製品バージョンに極めて迅速で簡単にアップグレードすることができます。以前のバージョンを削除するが必要なく、古いバージョンの上に新しい製品をインストールします。

新しいバージョンのシステムをインストールすると、以前にインストールされているバージョン/製品から設定が継承されます。Milestone では、障害時の復旧手段として、使用しているサーバー設定のバックアップを定期的に取ることを推奨しています。サーバーのアップグレード時にも、この手順を実行することをお勧めします。設定（カメラ、スケジュール、ビューなど）が失われることはまれですが、発生する**可能性はあります**。幸い、1 分程度で設定をバックアップできます。

新しいバージョンをインストールする前に、旧バージョンを手動で削除する必要はないことに注意してください。新しいバージョンをインストールするとき、旧バージョンは削除されます。

現在の製品バージョンから別の最新 XProtect Professional VMS 製品へのアップグレード

ある現在の XProtect Professional VMS 製品から別の現在の XProtect Professional VMS 製品へのアップグレード 『37ページ の"新しいソフトウェアライセンスファイルのインポート"参照 』

新しいソフトウェアライセンスファイルのインポート 『37ページ 』

機能がより多彩な **XProtect Professional VMS** 製品へのアップグレードについて

XProtect Professional VMS 製品の一つ（例えば XProtect Express）をご使用中で、別の XProtectVMS 製品（例えば XProtect Professional）にある特性や機能を追加したい場合、ご使用中のシステムをアップグレードできます。

まず、現在ご使用の XProtect Professional VMS 製品の下取り手続きをしてから、より高度な XProtectVMS 製品の基本ライセンスを購入します。購入すると、新しいソフトウエア・ライセンス・ファイルを受け取ります。ソフトウエア・ライセンス・ファイルには、どの XProtect Professional VMS 製品を使用できるかが決められています。そのため、何もインストールする必要はなく、 新しいソフトウエア・ライセンス・ファイルをインポートするだけでご利用いただけるようになります『37ページ の"新しいソフトウェアライセンスファイルのインポート"参照 』。

以前の製品の設定は新しい製品でも同じです。より高度で豊富な機能を備えた XProtect 製品に含まれている新しい機能を使用するためには、古い設定を設定し直し、新しい製品の新機能と特性を設定する必要があります。

例 : XProtect Express から XProtect Professional へアップグレードする場合、以下の点に特に注意する必要があります。

- XProtect Smart Client : XProtect Express で同時に接続できるのは XProtect Smart Client の 5 つのインスタンスだけです。アップグレードすると、さらに多くの XProtect Smart Client のインスタンスを接続できます。XProtect Express からアップグレードされたため、Management Application が一度に XProtect Smart Client へ接続できるのは 5 つのみに設定されています。この設定は、Management Application で**手動**で変更できます。一般に、アップグレードすると、XProtect Smart Client の機能をフルに活用できます。

- カメラの数 : XProtect Express では同時に最大 48 個のカメラを使用できますが、XProtect Professional では個数は制限されていません。貴方が追加したカメラの台数はアップグレード製品にも引き継がれます。但し、**手動**で Management Application の追加カメラを設定する必要があります。

製品間の違いに関する詳細情報は、Milestone のウエブサイト 『http://www.milestonesys.com/』で確認して下さい。

XProtect Professional VMS 製品の試用版をインストールした場合、それをライセンス XProtect Professional VMS 版にアップグレードできます。そのためには、必要なハードウエア・デバイスと共に基本ライセンスを購入し、ソフトウエア・ライセンス・ファイルをインポートします。試用版をインストールした場合、その保有期間は最長 5 日間です。ご注意下さい。つまり、一度ソフトウエア・ライセンス・ファイルをインポートしたら、5 日以上は使用できません。忘れずに、Management Application で手動で保有期間を変更して下さい。

新しいソフトウェアライセンスファイルのインポート

より機能が豊富な XProtect Professional VMS 製品にアップグレードした場合は、次の手順を新しいソフトウェアライセンスファイルをインポートします。

1. 電子メールで受信したソフトウェアライセンスファイルを管理サーバーのローカルドライブにコピーします。
2. Management Application の**[ファイル]**メニューから**[ライセンスのインポート]**を選択します。
3. 新しいソフトウェアライセンスファイルを見つけ、**[開く]**をクリックします。

システムコンポーネントの削除について

監視システム全体（つまり、監視サーバーソフトウェア、関連するインストールファイル、ビデオデバイスドライバー、XProtect Download Manager、XProtect Smart Client、Event Server サービス、Milestone Mobile サーバーのすべて）をサーバーから削除するには、標準の Windows でのプログラムのアンインストール手順に従ってください。詳細については、Windows ヘルプを参照してください。

また、XProtect Smart Client やビデオドライバーなどの個々のコンポーネントを、通常の Windows でのプログラムのアンインストール手順で削除することもできます。

重要：監視システムを削除しても、録画は削除されません。サーバーソフトウェアを削除した後でも、録画はサーバーに残ります。また、設定ファイルもサーバーに残ります。このため、後でシステムを再インストールした場合、設定を再使用することができます。

初めての使用

Management Application のシステムの構成

このチェックリストは、システムを設定するときに通常必要となるタスクを概説しています。

情報はチェックリストとして提供されますが、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 では、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ています。

異なる物理的条件（昼/夜、強風/無風など）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、調整することに時間をかけることをお勧めします。システムの実行中にこのようなテストを実行します。イベントや関連するアクションの設定も、組織の必要性に依存します。

このチェックリストを印刷して、常に携行してください。

☐	**システムのインストール** 「システムソフトウェアのインストール 『33ページ 』」を参照してください。 既存のバージョンのシステムをアップグレードする場合は、「ある製品バージョンから、別の製品バージョンへのアップグレード 『36ページ 』」を参照してください。
☐	**ソフトウェアライセンスファイルの認証** 多くの場合、ベンダーがこのプロセスを行うので、ユーザー自身がこのステップを実行する必要はありません。 ソフトウェアライセンスファイルを認証するには、「ライセンス認証について 『30ページ 』」を参照してください。
☐	**Management Application を開きます** インストール後に Management Application を開きます。ここでは、システムと機能の構成および管理を行います。
☐	**ハードウェアデバイスをシステムに追加** システムを初めて起動すると、**詳細設定**ウィザードが立ち上がり、システムにハードウェアデバイス（カメラ、エンコーダー、専用 I/O ボックス）を追加し、適切なユーザー名およびパスワードで設定できるようにサポートします。「自動設定ウィザード 『45ページ 』」を参照してください。
☐	**ハードウェアデバイスライセンスを認証** 多くの場合、ベンダーがこのプロセスを行うので、ユーザー自身がこのステップを実行する必要はありません。監視システムがオンラインの場合、この手順もスキップできます。 ハードウェアデバイスを追加したため、ハードウェアデバイスライセンスを認証 『30ページ の"ライセンス認証について"参照 』する必要があります。
☐	**カメラの設定** システムに接続されている各カメラの様々な設定を指定できます。設定には、コーデック、解像度、モーション検知の感度、録画の保存およびアーカイブ場所、PTZ（パン/チルト/ズーム）のプリセット位置、マイクおよびスピーカーとの関連付けなどが含まれます。ビデオや録画の設定について 『69ページ 』を参照してください。

☐	**イベント、入力、出力の設定** センサーからの入力に基づくシステムイベントを使用すると、システム上のアクションを自動的にトリガすることができます。 アクションの例：録画の開始・停止、ビデオフレームレートの切り替え、PTZ カメラのプリセット位置への移動。また、イベントを使用して、照明やサイレンなどのハードウェア出力を有効にすることも可能です。イベントの概要 『108ページ の"イベントおよび出力の概要"参照 』を参照してください。
☐	**スケジュールの設定** いつアーカイブを行うか、カメラが常にビデオをシステムへ転送するか、特定のイベント発生時や指定された時間帯だけビデオを転送するか、などを設定します。また、いつシステムから通知を受信するかも指定します。一般的なスケジュールおよびアーカイブの設定 『129ページ 』およびカメラ固有のスケジュールの設定『71ページ の"特定カメラスケジュールの構成"参照 』を参照してください。
☐	**クライアントによるシステムへのアクセス設定** システムには、多数の異なるクライアントアプリケーションが含まれています。クライアントからのインターネット経由でのシステムへのアクセス可否や、同時接続クライアント数などを指定します。サーバーアクセスの設定 『156ページ 』を参照してください。
☐	**マスター/スレーブサーバーの設定** 複数のサーバーを実行するには、以下の手順に従うだけです。この機能は XProtect Professional を実行している場合のみ使用できます。 マスター/スレーブ設定 『158ページ の"マスターおよびスレーブについて "参照 』により、複数のサーバーを組み合わせて、使用できるカメラの合計数を単一のサーバーの許容最大数以上に拡大できます。 このような設定でも、クライアントの接点は、1 つだけに維持されます。クライアントは、マスターサーバーに接続されますが、スレーブサーバーのカメラや録画にも自動的にアクセスできます。マスター/スレーブサーバーの設定 『158ページ の"マスターおよびスレーブサーバーの設定"参照 』を参照してください。
☐	**ユーザーの設定** 誰が、どのようにシステムにアクセスできるかを指定します。必要であれば、Management Application を保護するパスワードを設定します。誰がどのような権限を持つクライアントアクセスを行えるかを決定します。ユーザーアクセスの管理ウィザード『60ページ 』、基本ユーザーの追加『159ページ 』、ユーザーグループの追加 『160ページ 』、ユーザーおよびグループの権限の設定 『161ページ 』を参照してください。
☐	**XProtect Download Manager の設定** ユーザーがシステムサーバーに接続した時に、ようこそページに表示される機能を管理します。含まれる機能としては、クライアントアプリケーションへのアクセス、追加クライアントの言語バージョン、プラグインなどがあります。XProtect Download Manager は、システムサーバーと同じ言語でユーザーが XProtect Smart Client にアクセスできるよう、デフォルト設定が行われています。XProtect Download Manager 『23ページ 』の使用を参照してください。

上記のリストは、一般的に管理者が行う必要のある設定手順を示しています。システムの設定を設定、編集して、正確に組織のニーズにマッチさせることができます。

推奨事例

録画データベースの破損からの保護について

カメラデータベースが破損した場合に実行するアクションを選択できます。アクションにはさまざまなデータベース修復オプションがあります。このようなオプションは便利ですが、Milestone は、カメラデータベースが破損しないことを保証する手順を導入することをお勧めします。

停電：UPS の使用

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。

組織の環境に適した種類の 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。

Windows タスクマネージャ：プロセスの終了時に注意する

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。

ハードディスクの故障：ドライブを保護する

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 UPS 『280ページ 』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、必ず接地してください）
- 火、水など（避けてください）

設定に関する変更の保存について

システムをセットアップする際、システムに適用するために、設定に対して行った変更は必ず保存してください。Management Application で設定を変更する場合、たとえば**カメラの概要**や**ユーザープロパティ**で、黄色の通知バーによって設定を変更したことが通知されます。このバーは、変更がシステムに適用されたことを確認するために表示されます。変更を適用する場合は、**保存**をクリックします。変更を保存したくない場合は、**破棄**をクリックします。

設定を変更し、行った変更を保存すると、システムはシステムサービス（Recording Server サービスや Image Server サービスなど）に通知します。たとえば、カメラの名前を変えたり、モーション検知の設定を変更するなどの設定を変更すると、関連するシステムサービスに新しい設定がロードされ、ただちにクライアントに変更が表示されます。一方、たとえば、新しいイベントを追加するなど、リソースを多く必要とする設定変更を行った場合は、適切に動作させるために関連するサービスを再起動する必要があります。

サービスを再起動する必要がある場合、変更を保存すると、システムが自動的に再起動を実行します。Milestone Mobile サーバーで設定を変更した場合、Milestone Mobile サーバーのサービスを再起動せずに**保存**をクリックすると、システムにすべての変更が適用されます。

重要： システムがサービスを再起動している間は、ビデオを再生したり、録画することはできません。通常は、サービスの再起動は数秒で完了しますが、中断を最小限に抑えるために、重要な事象が発生しないと予想される時間帯にサービスを再起動することをお勧めします。クライアントを通じてシステムに接続しているユーザーは、サービスの再起動中もログインしたままになりますが、短い間ビデオが停止することがあります。

システムは、変更を復元ポイント 『274ページ の"復元ポイントからのシステム設定の復元"参照 』に保存します（そのため、エラーが生じた場合などにも作業設定を復帰することができます）。

組み込みヘルプの使用について

システムの組み込みヘルプを使用するには、Management Application の**ヘルプ**ボタンをクリックするか、キーボードの **F1** キーを押します。

すると既定のインターネットブラウザでヘルプシステムが開きます。このヘルプシステムと Management Application はアクティブ状態を切り替えることができます。このヘルプシステムは、コンテキスト依存ヘルプです。つまり、特定のダイアログでの作業中に F1 キーを押してヘルプを呼び出すと、ヘルプシステムはそのダイアログに応じたヘルプを表示します。

組み込みヘルプシステムの使用

ヘルプタブ**目次**、**索引**、**検索**を使用するか、ヘルプトピック内のリンクを使用します。

- **内容：** ヘルプシステムをツリー構造で表示します。
- **索引：** ヘルプトピックのアルファベット順の索引があります。
- **検索:** 特定のキーワードを含むヘルプトピックを検索できます。たとえば、「**ズーム**」という言葉を検索すると、「**ズーム**」が含まれているすべてのヘルプトピックが検索結果に表示されます。検索結果のリストでヘルプトピックのタイトルをダブルクリックすると、関連するトピックが表示されます。

ヘルプトピックの印刷

トピックの印刷が必要な場合は、インターネットブラウザの印刷機能を使用します。ヘルプトピックの印刷時は、画面上の表示がそのまま印刷されます。つまり、クリックすると展開されるリンク（ドロップダウンリンク）がトピックに含まれていて、表示されるドロップダウンリンクも印刷出力に含めたい場合、関連するドロップダウンリンクをクリックして、テキストが印刷に含まれるように表示させる必要があります。そうすることで、必要な情報がすべて含まれたページを印刷することができます。

サービスの再起動について

Management Application での変更設定の際、いくつかの項目では、Image Server サービスや Recording Server サービスの再起動が要求されます。サービスの再起動が必要な設定項目については、以下のリストを参照してください。

Image Server	Recording Server
ポート番号の変更	ライセンスの変更
最大クライアント数	イベントデータベースのパスの変更
マスターサーバーの有効化または無効化	手動レコーディングの有効化
スレーブサーバーの追加または削除	リモートでの起動
ログのパスの変更	通知の有効化または無効化
ライセンスの変更	イベントの変更
プライバシーマスクの変更	出力の変更
ハードウェアデバイスの削除	ダイナミックアーカイブ パスの追加または削除
	アーカイブ時刻の追加または削除
	スケジュールの変更
	Matrix 機能のセットアップ
	ハードウェアデバイスの交換
	カメラドライバーの変更
	カメラの IP アドレスの変更
	すべてのデバイスの削除
	カスタマーダッシュボードでのアラームの有効化または無効化

ストレージ容量の使用率をモニターする

使用しているシステムにどの程度のストレージ容量があるか、そしてそのうち空き容量がどの程度あるかを確認するには、次の手順を実行してください。

1. **詳細設定**を展開し、**カメラおよびストレージの情報**を選択します。
2. **ストレージ使用の概要**で、どのドライブが使用可能であるか、どのドライブを何に使用しているか、それぞれのドライブのサイズ、ならびにそれぞれのドライブにビデオデータ、その他のデータ、空き容量がどの程度あるかに関する情報を確認できます。

Management Application でカメラからビデオを再生する

Management Application で、単一のカメラから直接ライブビデオを再生できます。

1. **詳細設定**を展開し、**カメラおよびストレージの情報**を展開します。
2. 関連するカメラを選択して、そのカメラからのライブビデオを表示します。ライブビデオの上には、選択したカメラの最も重要なプロパティの概要が表示されます。ライブビデオの下には、カメラの解像度や平均の画像ファイルサイズなどの情報が表示されます。MPEG または H.264 を使用しているカメラの場合、ビットレートは Mbit/秒でも表示されます。

重要： 特定の状況において Management Application でライブビデオを表示すると、関連するカメラからの同時録画に影響することがあります。

次の 3 つのシナリオに特に配慮することが重要です。

マルチストリームをサポートしている一部のカメラでは、2 番目のストリームを開くと、半分のフレームレートになったり、応答にマイナスの影響が出る場合があります。

カメラが非常に高い画質でライブビデオを配信している場合、画像のデコーディングによって Recording Server サービスへの負荷が高まり、録画に対して継続的に悪影響を与える場合があります。

複数の同時ビデオストリーム出力に対応しないカメラは、監視サーバーと Management Application に同時に接続することはできません。Milestone では、そうしたデバイスでモーション検知や PTZ を設定する場合、Recording Server サービスを停止 『168ページ の"サービスを開始および停止する"参照 』することを推奨しています。

Management Application でカメラからのビデオを表示する 『44ページ の"Management Application でカメラからビデオを再生する"参照 』も参照してください。

使用開始

スタートページについて

Management Application を開くと、**スタート**ウィンドウが必ず表示されます。**スタート**ページは、ユーザーの参照場所です。監視システムを迅速に構成するための別のウィザードもあります。ウィザードを実行した後、多くの場合、さらにシステムを微調整する必要があります。詳細については、ヘルプの「詳細設定 『62ページ 』」の章を参照してください。

ページの左下端の**[ライセンス]**見出しの下で、システムのハードウェアデバイスライセンス 『25ページ 』の概要と、アクティベーションなしのデバイスの変更 『28ページ 』数を確認できます。

Milestone Care 見出しの下には、現在の Milestone Care™に関する情報と、インストールの更新があるかどうかを確認できます。インストールには常に Milestone Care Basic が適用され、これにより、MilestoneWeb サイト 『http://www.milestonesys.com/support』のナレッジベース記事、ガイド、チュートリアルなどのさまざまなタイプのセルフヘルプ資料を使用できます。リセラーから Milestone Care Plus サブスクリプションを購入した場合は、アップグレードも利用できます。Customer Dashboard サービス、Smart Connect 機能、および完全プッシュ通知機能も利用できます。 Milestone Care Plus サブスクリプションの有効期限はページに表示されます。Milestone Care Premium サブスクリプションがある場合は、Milestone サポート問い合わせサポートを受けることもできます。Milestone サポートに問い合わせるときには、Milestone Care ID の情報を必ず含めてください。Milestone Care Premium サブスクリプションの有効期限も表示されます。Milestone Care の詳細については、リンクに従ってください。システムをインストールした後に Milestone Care サブスクリプションを購入または更新する場合は、**スタート**ページに正しい Milestone Care 情報が表示される前にライセンスを認証 『30ページ の"ライセンス認証について"参照 』する必要があります。

また、お使いのシステムのウィザードの各ステップを完了する方法を説明しているビデオチュートリアルにアクセスして表示することができます。ビデオチュートリアルにアクセスするには、ページの右下の**チュートリアルの表示**リンクをクリックします。このリンクで、お使いのシステムのビデオチュートリアルのある外部 Web ページに移動します。

自動設定ウィザード

自動設定ウィザードにより、システムを初めてご利用になる際に設定を簡単に行うことができます。ウィザードの段階的な手順に従って、システムに自動的にカメラを追加できます。

自動設定ウィザード：**1** ページ目

Management Application の初回起動時には、自動設定ウィザードが開き、システムへのハードウェアデバイスの追加をガイドします。

システムを初めて使用する場合、**はい、設定します**をクリックし、ネットワークで利用可能なカメラをスキャンして、システムを設定します。終了して、より詳細な方法でお使いのシステムへデバイスを追加するには、**スキップ**をクリックしてウィザードを閉じ、Management Application へ移動すると、より多くのオプションを使用してシステムのデバイスを設定できます。

自動設定ウィザード：スキャンオプション

お使いのシステムからカメラやデバイスをスキャン（検索）する場所を選択します。

デフォルトでは、**ローカルネットワークをスキャン**チェックボックスが選択されているため、ローカルネットワーク内にあるデバイスのみをスキャンします。ただし、カメラやデバイスの IP アドレスまたはそれらの範囲が分かる場合、**スキャンする IP アドレスまたは IP 範囲を追加する**の隣にある[プラス]アイコンをクリックして指定してください。必要な場合、2 つ以上の IP アドレス範囲を追加することができます。

自動設定ウィザード：スキャン対象のハードウェアのメーカーの選択

お使いのハードウェアデバイスのメーカーが分かっている場合、このページのドロップダウンリストから選択します。必要な数のメーカーを選択できます。

注意：デフォルトでは、すべてのメーカーが選択されています。スキャン時間を短縮する場合、あるいはお使いのカメラのうち特定メーカーのデバイスのみを確認したい場合、ご希望のメーカーを表すチェックボックスのみを選択してください。

自動設定ウィザード：ハードウェアデバイスのスキャン

選択したメーカーに一致するハードウェアデバイスのスキャンが開始します。ステータスバーに、スキャン処理の進捗状況が示されます。カメラやデバイスのスキャンが完了した後で、選択したデバイスやカメラのユーザー名とパスワードの入力を求められる場合があります。それらの資格情報を入力した場合、デバイスを追加するには**確認**ボタンをクリックしてください。

注意：デバイスやカメラによっては、ユーザ名とパスワードが不要な場合もあります。そのような場合、資格情報を入力することなくデバイスを追加できます。

自動設定ウィザード：スキャン後の続き

追加するデバイスやカメラの数を追加すると、お使いのシステムがストレージを設定します。ここで、ストレージとは、お使いのシステムが記録を保存する場所のことです。デフォルトでは、空きディスク容量が最も多く利用できる場所がシステムにより選択されます。

ストレージの設定が終了した後は、新しいカメラがネットワーク上で検出されたときに、システムにこれらのカメラを自動的に追加するオプションを設定することができます。これを有効にすると、以後、あるデバイスやカメラがネットワークに接続・認識された時点で、それらをシステムへ自動的に追加・設定されるようにできます。すべてのデバイスやカメラが自動検出に対応しているわけではない点にご注意ください。

ネットワークに接続したデバイスやカメラが自動的に表示されない場合は、手動で追加する必要があります。

デバイス/カメラが以前にシステムに追加され、それを削除した場合は、デバイスは自動的に検出されません。手動で追加する必要があります。

XProtect Smart Client に直接移動するには、ウィザードを完了してから、ウィザードページの左下にあるチェックボックスを選択してください。

ハードウェアの追加ウィザード

カメラ、およびビデオエンコーダーなどその他のハードウェアデバイスは、**ハードウェアの追加ウィザード**を使用してシステムに追加します。ハードウェアデバイスにマイクやスピーカーが付いている場合は、ツールによりこれらも自動的に追加されます。

システムで使用できるカメラ数には制限があります。使用可能な数を超えるカメラを追加することができることに注意してください。システムでビデオエンコーダーデバイスを使用する場合、ビデオエンコーダーデバイスに複数のカメラを接続できます。たとえば、すべて使用されている 4 ポートビデオエンコーダーは 4 台のカメラと認識されます。

このウィザードでは、次の 2 種類の方法でカメラを追加することができます。

ハードウェアのスキャン	必要な IP 範囲、検出方法、ドライバー、およびデバイスのユーザー名とパスワードに関する指定に基づいて、ネットワーク上にある関連ハードウェアデバイスをスキャンします。 ハードウェアの追加:ハードウェアのスキャン『47ページ の"高速"参照 』を参照してください。
追加するハードウェアを手動で指定します	それぞれのハードウェアデバイスの詳細を個別に指定します。 数台のハードウェアデバイスを追加したい場合で、かつそれぞれの IP アドレス、必要なユーザー名やパスワードなどを知っている場合に適しています。 ハードウェアの追加 : 追加するハードウェアを手動で指定します 『48ページ の"手動"参照 』。 あるいは、カメラに関するデータを、カンマ区切り値ファイルからインポートします。複数のシステムを設定する場合に効率的な方法です。 ハードウェアの追加 : CSV ファイルからインポートします 『49ページ の"CSV ファイルからインポート"参照 』。

高速

デバイス検出は、ハードウェアデバイスがそれ自体の情報をネットワーク上に提供する方法です。この情報に基づいて、システムは関連ハードウェアデバイス（カメラ、ビデオエンコーダーなど）を迅速に認識し、スキャン対象に含めることができます。

ハードウェアのスキャン方法により、わずか数ステップで、関連ハードウェアデバイスをネットワークでスキャンし、システムに迅速に追加できます。

以下の 2 つのオプションから、ハードウェアを追加する方法を選びます。

- **ローカルネットワークをスキャン**:システムのサーバー自体が位置するネットワークの一部(サブネット)である、デバイス検出をサポートしているローカルネットワークで、使用可能なハードウェアを自動スキャンします。
- **スキャン対象の IP アドレスまたは IP 範囲の追加：** システムがハードウェアのスキャンを開始する IP 範囲およびポートを指定して、ハードウェアをシステムに追加します。

ローカルネットワークをスキャン方法を使用するには、使用しているシステムのサーバーとカメラが同じレイヤー2 ネットワークに存在している必要があります。これはすべてのサーバーやカメラなどが、ルーターを必要とせずに通信できるネットワークに存在することを意味します。理由はデバイス検出がシステムのサーバーとカメラの間での直接通信に依存しているためです。

ネットワークでルーターを使用している場合は、**スキャン対象の IP アドレスまたは IP 範囲の追加**オプションを使用してハードウェアが存在している IP 範囲を指定するか、追加するハードウェアを手動で指定 『48ページ の"手動"参照 』方法のいずれか 1 つを選びます。

ハードウェアの追加：スキャンオプション

お使いのシステムからカメラやデバイスをスキャン（検索）する場所を選択します。

デフォルトでは、**ローカルネットワークをスキャン**チェックボックスが選択されているため、ローカルネットワーク内にあるデバイスのみをスキャンします。ただし、カメラやデバイスの IP アドレスまたはそれらの範囲が分

かる場合、**スキャンする IP アドレスまたは IP 範囲を追加する**の隣にある[プラス]アイコンをクリックして指定してください。必要な場合、2 つ以上の IP アドレス範囲を追加することができます。

ハードウェアの追加：スキャン対象のハードウェアのメーカーの選択

お使いのハードウェアデバイスのメーカーが分かっている場合、このページのドロップダウンリストから選択します。必要な数のメーカーを選択できます。

注意：デフォルトでは、すべてのメーカーが選択されています。スキャン時間を短縮する場合、あるいはお使いのカメラのうち特定メーカーのデバイスのみを確認したい場合、ご希望のメーカーを表すチェックボックスのみを選択してください。

ハードウェアの検出と検証

選択したメーカーに一致するハードウェアデバイスのスキャンが開始します。ステータスバーに、スキャン処理の進捗状況が示されます。カメラやデバイスのスキャンが完了した後で、選択したデバイスやカメラのユーザー名とパスワードの入力を求められる場合があります。それらの資格情報を入力した場合、デバイスを追加するには**確認**ボタンをクリックしてください。

注意：デバイスやカメラによっては、ユーザ名とパスワードが不要な場合もあります。そのような場合、資格情報を入力することなくデバイスを追加できます。

追加するデバイスやカメラの数を追加すると、お使いのシステムがストレージを設定します。ここで、ストレージとは、お使いのシステムが記録を保存する場所のことです。デフォルトでは、空きディスク容量が最も多く利用できる場所がシステムにより選択されます。

手動

追加するハードウェアを手動で指定方法では、それぞれのハードウェアデバイスの詳細を個別に指定できます。

このオプションは、少数のハードウェアデバイスだけを追加する場合で、それらの IP アドレス、ユーザー名とパスワードなどが分かっている場合に適しています。同様に、**ハードウェアのスキャン**オプションを使用するローカルネットワークでの自動検索は、たとえばシステムの**ユニバーサルドライバー**を使用しているカメラなど、一部のカメラでは機能しないことがあります。このようなカメラについては、手動でシステムに追加する必要があります。

あるいは、**CSV ファイルのインポート** 『**49**ページ の"**CSV ファイルからインポート**"参照 』を選択します。このオプションでは、ハードウェアデバイスに関するデータを、カンマ区切り値ファイル(CSV)からインポートします。複数の類似のシステムを設定する場合、これは非常に効率的な方法です。

情報、ドライバーの選択と検証

追加したいハードウェアデバイスのそれぞれの情報を指定します。

名前	詳細
IP アドレス	ハードウェアデバイスの IP アドレスまたはホスト名。
ポート	スキャンするポート番号。デフォルトポートは 80 です。 ハードウェアデバイスが NAT 対応のルーターまたはファイアウォールの背後にある場合、別のポート番号の指定が必要になることがあります。この場合、ハードウェアデバイスが使用しているポートや IP アドレスをマップするように、ルーター/ファイアウォールを設定する必要もあることに留意してください。

名前	詳細
ユーザー名	ハードウェアデバイスの管理者アカウントのユーザー名。 多くの組織では、ハードウェアデバイスの製造元によるデフォルトのユーザー名をハードウェアデバイスで使用しています。あなたの組織の場合であれば、"<デフォルト>"を選択します。システムがメーカーのデフォルトユーザー名を知っていると誤解の原因となるため、メーカーのデフォルトユーザー名は入力しないでください。 たとえば admin や root など、リストから他の一般的なユーザー名を選択することもできます。リストにないユーザー名を使用するときは、新しいユーザー名を入力します。
パスワード	管理者アカウントにアクセスするために必要なパスワードです。一部のハードウェアデバイスでは、アクセスにユーザー名/パスワードを必要としません。
ドライバー	ハードウェアデバイスをスキャンするドライバー。デフォルトでは、ウィザードは自動検出オプションを表示します。自動検出オプションは、関連するドライバーを自動的に検索します。スキャン時間を短縮するため、メーカーが分かっている場合はメーカーを選択します。

追加するデバイスやカメラの数を追加すると、お使いのシステムがストレージを設定します。ここで、ストレージとは、お使いのシステムが記録を保存する場所のことです。デフォルトでは、空きディスク容量が最も多く利用できる場所がシステムにより選択されます。

CSV ファイルからインポート

ハードウェアデバイスやカメラに関するデータを、カンマ区切り値ファイル(CSV)からインポートします。複数の類似のシステムを設定する場合、これは非常に効率的な方法です。

ハードウェアデバイスの追加ウィザード - CSV ファイルからインポート - CSV ファイルの例

以下は、カメラやサーバーがオンラインである場合に使用する CSV ファイルの例です。

HardwareAddress、**HardwarePort**、**HardwareUsername**、**HardwarePassword**、**HardwareDriverID** などのパラメータを含んでいます。HardwareUserName および HardwareDriverID は、オプションのパラメータです。

デバイスについて、デフォルトの HardwareUsername を変更していない場合は、HardwareUsername をそのままにすることもできます。HardwareDriverID は、オプションのフィールドです。空白の場合、自動的に自動検出に設定されます。

```
HardwareAddress;HardwarePort;HardwareUsername;HardwarePassword;HardwareDriverID;
192.168.200.220;80;root;pass;128;
192.168.200.221;80;user;password;165;
192.168.200.222;80;r00t;pass;172;
192.168.200.223;80;;p4ss;
192.168.200.224;80;usEr;pASs;
```

ハードウェアの追加:CSV ファイルからインポート - CSV ファイル形式および要件

CSV ファイルには、ヘッダー行（以後の行にあるそれぞれの値が何に関するものであるかを決定する）が必要であり、以後の行にはそれぞれ 1 つのハードウェアデバイスに関する情報だけが含まれている必要があります。それぞれのハードウェアデバイスに対して、以下の情報が必要になります。

HardwareAddress	ハードウェアデバイスの IP アドレス。
HardwareUsername	ハードウェアデバイスの管理者アカウントのユーザー名。
HardwarePassword	ハードウェアデバイスの管理者アカウントのパスワード。
HardwareDriverID	カメラとサーバーがオフラインの場合:追加したいそれぞれのハードウェアデバイスについて、**HardwareDriverID** を指定します。 例：**ACTi ACD-2100 105** は、ACTi ACD-2100 ハードウェアデバイスを追加する際に、**105** を ID として使用する必要があることを示しています。

CSV ファイルで指定されていない既存の設定パラメータは変更されないままになります。CSV ファイルで個々のカメラのパラメータ値が空白であれば、そのカメラの既存のパラメータ値は変更されないままです。

ハードウェアデバイス情報を、たとえば Microsoft Excel などのスプレッドシートに保存してから、CSV ファイルにカンマ区切り値で保存することができます。

以下は、CSV ファイルに存在する情報に適用されます。

- CSV ファイルの最初の行にはヘッダーが必要であり、以後の行にはそれぞれ 1 つのハードウェアデバイスに関する情報が含む必要があります。
- 区切り記号としてはカンマ、セミコロン、タブが使えますが、混在させることはできません。
- すべての行に有効な値が含まれる必要があります。カメラの名前、ユーザー名や類似のアイテムなどはすべて一意でなければなりません。また、以下の特殊文字が含まれないように注意してください。 **< > & ' " ¥ / : * ? | [ ]**
- 値の順番は固定ではなく、オプションのパラメータは完全に削除することもできます。
- ブーリアン型フィールドは、0、false、no に設定しなければ、真であるとみなされます。
- 区切り記号しか含まない行は無視されます。
- 空白の行も無視されます。

CSV ファイル形式は一般には ASCII のみですが、Unicode 識別子も許可されます。Unicode 識別子がなくても、ファイル全体あるいは個々の文字が Unicode 文字列であることは可能です。

ストレージの設定ウィザード

ビデオストレージのステップは、カメラのビデオや録画のプロパティを迅速に設定するのに便利です。

ストレージの設定：ビデオ設定とプレビュー

ビデオ設定では、帯域、輝度、圧縮、コントラスト、解像度、回転などをコントロールできます。ウィザードウィンドウの左にあるリストを使って、カメラを選択し、ビデオ設定を調整します。その後、次のカメラを選択し

て、設定を調整します。ビデオ設定の大部分はカメラに固有であるため、これらの設定はそれぞれのカメラに対して個別に設定する必要があります。

設定ダイアログを開くをクリックして、別のダイアログでカメラを設定します。ビデオ設定を変更した場合、すぐに変更が適用されます。つまり、大半のカメラでは、設定の効果をプレビュー画像ですぐに確認することができます。ただし、ウィザードを終了しても、行った変更を元に戻すことができません。ビデオ形式に MPEG または H.264 を使用するように設定されているカメラでは、通常、そのカメラでどのライブフレームレートを使用するか選択します。

ビデオ設定機能に、**日時を含む**設定がある場合があります。**はい**に設定すると、カメラからの日付と時刻がビデオに含まれます。ただし、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や電源などで機能しています。したがって、カメラの時刻と XProtect システムの時刻が完全に対応していないことがあり、これが混乱につながることがあります。受信したすべてのフレームにシステムがタイムスタンプを付けるため、それぞれの画像の正確な日付と時刻は既に分かっていることから、Milestone では**いいえ**に設定することを推奨しています。

注意： 一貫性のある時間の同期を行うために、使用しているカメラがサポートしている場合、カメラとシステムの時刻をタイムサーバーで自動同期することができます。

ストレージの設定：オンラインスケジュール

それぞれのカメラをいつオンラインにするかを指定します。オンラインのカメラとは、ライブでの再生やその他の処理のためにビデオをサーバーに転送するカメラです。カメラがオンラインであるという事実だけでは、システムがカメラからのビデオを録画していることを意味しません（録画の設定は、以後のページで行います）。デフォルトでは、システムに追加するカメラは自動的にオンライン（**常にオン**）になるので、特定の時刻やイベントに際してのみカメラをオンラインにしたい場合にだけオンラインスケジュールを変更します。ただし、この既定の状態を、スケジュールオプション 『131ページ 』の一部として変更できることに注意してください。

それぞれのカメラに対して、初期設定で次の 2 種類のオンラインスケジュールのいずれかを選択できます。

- **常にオン：** カメラは、常にオンラインになります。
- **常にオフ：** カメラは、決してオンラインになりません。

これら 2 種類のオプションでは単純過ぎる場合は、**作成/編集...**ボタンを使って、必要に応じたオンラインスケジュールを指定してから、カメラに対してスケジュールを選択します。このようにして、特定の期間でカメラがオンラインであるかどうか、あるいは特定の期間内で特定のイベントが発生した場合にカメラがビデオの転送を開始または停止するかを指定することができます。

テンプレートを使用すると、類似のプロパティが迅速に設定できて便利です。たとえば、20 台のカメラがあり、それらすべてに特定のフレームレートを設定したい場合、テンプレートに一度入力するだけで、そのテンプレートを 20 台のカメラに適用することができます。

名前	詳細
テンプレートを適用	どのカメラにテンプレートを適用するか選択します。2 つの**設定**ボタンのいずれかを使用して、実際にテンプレートに適用します。
全て選択	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択します。
全てクリアする	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択解除します。
選択したカメラにテンプレートを適用する	テンプレートの値を、選択したカメラに適用します。

ストレージの設定：（Motion-JPEG カメラ）ライブ設定および録画設定

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、製品比較チャート『12ページ 』を参照してください。

このウィザードページが表示されるのは、1 台または複数のカメラが MJPEG コーデックを使用している場合だけです。

モーションの検知や指定したイベントの前後の期間の録画を保存できるプリレコーディングやポストレコーディングを選択します。また、それぞれのカメラで使用するフレームレートを指定します。

プリレコーディング	検出したモーションおよび開始イベントの前の期間からの録画を保存できます。このチェックボックスを選択すると、この機能が有効になります。隣接する列で、任意の秒数を指定します。
秒数［プリレコーディングの］	録画開始条件（モーションまたは開始イベント）が満たされる前から、ビデオを録画する秒数を指定します。通常、プリレコーディングが必要になるのは数秒のみですが、最長で 65,535 秒（18 時間 12 分 15 秒）まで指定できます。ただし、非常に長いプリレコーディング時間を指定すると、プリレコーディング時間がスケジュールされた、あるいはスケジュールされていないアーカイブ 『124ページ の"アーカイブについて"参照 』時間にかかることもあります。アーカイブ中は、プリレコーディングが適切に機能しないため、問題の原因となりかねません。
ポストレコーディング	検出したモーションおよび停止イベントの後の期間の録画を保存できます。このチェックボックスを選択すると、この機能が有効になります。隣接する列で、必要な秒数を指定します。
秒数［ポストレコーディングの］	録画停止条件（モーションまたは停止イベント）が満たされた後で、ビデオを録画する秒数を指定します。通常、ポストレコーディングが必要になるのは数秒のみですが、最長で 65,535 秒（18 時間 12 分 15 秒）まで指定できます。ただし、非常に長いポストレコーディング時間を指定すると、ポストレコーディング時間がスケジュールされた、あるいはスケジュールされていないアーカイブ時間にかかることもあります。アーカイブ中は、ポストレコーディングが適切に機能しないため、問題の原因となりかねません。
フレームレート	カメラの映像に必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。
ライブフレームレート	カメラからのライブ映像に必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。 カメラがデュアルストリームをサポートし、デュアルストリームを有効にした場合、**ライブフレームレート**列はデュアルストリーム値で読み取り専用です。これは変更できません。
録画フレームレート	カメラの録画ビデオに必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。このフレームレートは、標準モードで指定するフレームレートより高くなければなりません。

テンプレートを使用すると、類似のプロパティが迅速に設定できて便利です。たとえば、20 台のカメラがあり、それらすべてに特定のフレームレートを設定したい場合、テンプレートに一度入力するだけで、そのテンプレートを 20 台のカメラに適用することができます。

テンプレートを適用	どのカメラにテンプレートを適用するか選択します。2 つの**設定**ボタンのいずれかを使用して、実際にテンプレートに適用します。
全て選択	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択します。
全てクリアする	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択解除します。
選択したカメラにテンプレートを適用する	テンプレートの値を、選択したカメラに適用します。

ストレージの設定：**H.264/MPEG4** カメラのライブ設定および録画設定

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、製品比較チャート『12ページ 』を参照してください。

このウィザードページが表示されるのは、1 台または複数のカメラが H.264/MPEG4 コーデックを使用している場合だけです。

それぞれのカメラでどのフレームレートを使用するか、すべてのフレームを録画するか、あるいはキーフレームだけを録画するかを指定します。また、プリレコーディングやポストレコーディングを選択して、モーションの検知や指定したイベントの前後の期間の録画を保存することも可能です。

それぞれのカメラに対して、すべてのプロパティを個別に指定することも可能であることに注意してください。

ライブフレームレート	カメラからのライブ映像に必要な平均フレームレート。 フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。 カメラがデュアルストリームをサポートし、デュアルストリームを有効にした場合、**ライブフレームレート**列はデュアルストリーム値で読み取り専用です。これは変更できません。

録画オン	カメラからのビデオを録画する条件を以下から選択します。 • **常時 :** カメラが有効 『89ページ の"一般"参照 』で、オンラインになるようにスケジュール 『132ページ の"オンライン期間"参照 』されている場合は常に録画します。後者のオプションでは、時間ベースの録画ができます。 • **設定しない** : 録画しません。ライブビデオが表示されますが、ビデオがデータベースに保持されていないため、ユーザーはカメラからビデオを再生できません。 • **イベント** : これを選択すると、モーション 『98ページ の"モーション検知&と領域の除外"参照 』が検知された時にビデオを録画します。後の録画を追加しなければ、最後のモーションが検知された後すぐに録画が停止します。 他のフィールドの下にある**イベントの設定**リストを使用して、必要に応じたイベントを定義します。 • **モーション検知およびイベント** : これを選択すると、モーションを検知した場合、あるいはイベントが発生していから、別のイベントが発生するまでの間、ビデオが録画されます。隣の列で、開始イベントおよび停止イベントを選択することを忘れないでください。
プリレコーディング	検出したモーションおよび開始イベントの前の期間からの録画を保存できます。このチェックボックスを選択すると、この機能が有効になります。隣接する列で、必要な秒数を指定します。
秒数 [プリレコーディングの]	録画開始条件（モーションまたは開始イベント）が満たされる前から、ビデオを録画する秒数を指定します。通常、プリレコーディングが必要になるのは数秒のみですが、最長で 65,535 秒（18 時間 12 分 15 秒）まで指定できます。ただし、非常に長いプリレコーディング時間を指定すると、プリレコーディング時間がスケジュールされた、あるいはスケジュールされていないアーカイブ 『124ページ の"アーカイブについて"参照 』時間にかかることもあります。アーカイブ中は、プリレコーディングが適切に機能しないため、問題の原因となりかねません。
ポストレコーディング	検出したモーションおよび停止イベントの後の期間の録画を保存できます。このチェックボックスを選択すると、この機能が有効になります。隣接する列で、必要な秒数を指定します。
秒数 [ポストレコーディングの]	録画停止条件（モーションまたは停止イベント）が満たされた後で、ビデオを録画する秒数を指定します。通常、ポストレコーディングが必要になるのは数秒のみですが、最長で 65,535 秒（18 時間 12 分 15 秒）まで指定できます。ただし、非常に長いポストレコーディング時間を指定すると、ポストレコーディング時間がスケジュールされた、あるいはスケジュールされていないアーカイブ時間にかかることもあります。アーカイブ中は、ポストレコーディングが適切に機能しないため、問題の原因となりかねません。
キーフレームだけ	ビデオストリームのキーフレームのみでモーション検知を行うことで、モーション検知で使用するシステムのリソースを減らしたい場合は、**キーフレームだけ**を選択します。

テンプレートを使用すると、類似のプロパティが迅速に設定できて便利です。たとえば、20 台のカメラがあり、それらすべてに特定のフレームレートを設定したい場合、テンプレートに一度入力するだけで、そのテンプレートを 20 台のカメラに適用することができます。

名前	詳細
テンプレートを適用	どのカメラにテンプレートを適用するか選択します。2 つの**設定**ボタンのいずれかを使用して、実際にテンプレートに適用します。
全て選択	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択します。
全てクリアする	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択解除します。
選択したカメラにテンプレートを適用する	テンプレートの値を、選択したカメラに適用します。

ストレージの設定：ドライブの選択

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、製品比較チャート『12ページ 』を参照してください。

どのドライブに、カメラの録画を保存するかを指定します。録画およびアーカイブ 『124ページ の"アーカイブについて"参照 』に対して、別個のドライブ/パスを指定することができます。

ドライブ	たとえば、C:¥ドライブです。
目的	ドライブを使用する目的を選択します。 **使用しない：** ドライブは使用しません。 **録画：**ドライブが監視システムサーバーのローカルドライブの場合のみ使用可能です。ネットワークドライブは録画には使用できません。システムのデータベース録画に使用するドライブです。 **アーカイブ：**ドライブをアーカイブで使用します。アーカイブには、空き容量が十分にあるドライブを使用することをお勧めします。アーカイブでダイナミックパスを選択した場合、ドライブの空き容量について心配する必要はありません。 **録画& アーカイブ：** ドライブが監視システムサーバーのローカルドライブの場合のみ使用可能です。ネットワークドライブは録画には使用できません。システムの通常のデータベースに録画およびアーカイブを保存するドライブを使用します。
録画パス	カメラのデータベースを保存するフォルダへのパス。デフォルトパスは C:¥MediaDatabase です。 他のフォルダを参照する場合は、該当するセルの横にあるアイコンをクリックしてください。指定できるのは、**ローカル**ドライブにあるフォルダへのパスのみです。ネットワークドライブへのパスを指定することはできません。ネットワークドライブを使用している場合、ネットワークドライブが使用不能になると、録画は保存できません。 録画パスを変更し、元の場所に既存の録画がある場合、録画を新しい場所に移動するか（推奨）、元の場所に残すか、削除するかを選択するよう確認されます。 複数のカメラがあり、複数のローカルドライブが使用可能な場合、個別のカメラのデータベースを複数のドライブに分散させることでパフォーマンスを改善できます。

アーカイブ パス	アーカイブ 『124ページ の"アーカイブについて"参照 』の動的パスを使用しない場合のみ、これを編集できます。カメラのアーカイブされた録画を保存するフォルダへのパス。デフォルトは、C:¥MediaDatabase です。 他のフォルダを参照する場合は、関連するセルの横にあるアイコンをクリックしてください。アーカイブ パスを変更し、古い場所に既存のアーカイブされた録画がある場合、アーカイブされた録画を新しい場所へ移動するか（推奨）、古い場所に残すか、あるいは削除するかを選択する必要があります。アーカイブされた録画を移動すると、システムは現在カメラのデータベースにあるものもアーカイブすることに注意してください。そのため、アーカイブされた録画を移動した直後に、カメラのデータベースは空になります。
合計サイズ	ドライブの合計サイズ。
空きスペース	ドライブに残っている未使用の容量。
アーカイブのダイナミックパス選択	このオプションを使用する場合（強く推奨）、アーカイブ用に複数のローカルドライブを選択する必要があります。監視システムデータベースを含んでいるパスが、アーカイブ用に選択したドライブのいずれかにあれば、システムは常にまずそのドライブにアーカイブしようと試みます。そうでない場合、そのドライブを使用するカメラデータベースが存在しない限り、システムは自動的にその時点で最も使用可能な容量が大きいアーカイブドライブにアーカイブします。 使用可能な容量が最も大きいドライブはアーカイブプロセス中も変化するので、同一プロセスで複数のアーカイブドライブに対してアーカイブされることがあります。これにより、ユーザーがアーカイブされた録画を検索し、表示する方法には影響を与えません。
アーカイブ時刻	システムで自動的に録画をアーカイブパスへ移動させる時刻を指定します。1 日に最大で 24 件のアーカイブ時刻を指定できますが、最低でも 1 時間の間隔が必要です。時間、分、秒の値を選択してから、**上**および**下**ボタンをクリックして値を増減させるか、単に選択した値に上書きして、**追加**をクリックします。大量の録画が予想される場合ほど、頻繁にアーカイブする必要があります。
ネットワークドライブ	ネットワークドライブをドライブのリストに追加します。まずネットワークドライブを指定してから、**追加**をクリックします（ネットワークドライブを指定すると、ボタンが使用可能になります）。ネットワークドライブは録画には使用できず、アーカイブ用のみであることに注意してください。

ストレージの設定：録画およびアーカイブの設定

個々のカメラについて、それぞれ録画およびアーカイブ 『124ページ の"アーカイブについて"参照 』のパスを選択します。

白い背景のすべてのプロパティを編集できます。**水色**の背景のプロパティは編集できません。

名前	詳細
録画パス	カメラのデータベースを保存するフォルダへのパス。デフォルトは、C:¥MediaDatabase です。他のフォルダを参照する場合は、該当するセルの横にあるアイコンをクリックしてください。指定できるのは、**ローカル**ドライブにあるフォルダへのパスのみです。ネットワークドライブへのパスを指定することはできません。ネットワークドライブを使用している場合、ネットワークドライブが使用不能になると、録画は保存できません。 録画パスを変更し、元の場所に既存の録画がある場合、録画を新しい場所に移動するか（推奨）、元の場所に残すか、削除するかを選択するよう確認されます。 複数のカメラがあり、複数のローカルドライブが使用可能な場合、個別のカメラのデータベースを複数のドライブに分散させることでパフォーマンスを改善できます。
アーカイブ パス	アーカイブ 『124ページ の"アーカイブについて"参照 』で動的パスを使用していない場合にのみ、編集可能です。カメラのアーカイブされた録画を保存するフォルダへのパス。デフォルトは、C:¥MediaDatabase です。 他のフォルダを参照する場合は、関連するセルの横にあるアイコンをクリックしてください。アーカイブ パスを変更し、古い場所に既存のアーカイブされた録画がある場合、アーカイブされた録画を新しい場所へ移動するか（推奨）、古い場所に残すか、あるいは削除するかを選択する必要があります。アーカイブされた録画を移動すると、システムは現在カメラのデータベースにあるものもアーカイブすることに注意してください。そのため、アーカイブされた録画を移動した直後に、カメラのデータベースは空になります。
保持期間	カメラからの録画（つまり、カメラのデータベースにある録画ならびにアーカイブされている録画）を保持しておく合計時間です。デフォルトの保持期間は 7 日間です。 保持期間は、録画を保持しておく**合計**時間です。以前のバージョンの監視システムでは、データベースとアーカイブで別個に制限時間を指定していました。

テンプレートを使用すると、類似のプロパティが迅速に設定できて便利です。たとえば、20 台のカメラがあり、それらすべてに特定のフレームレートを設定したい場合、テンプレートに一度入力するだけで、そのテンプレートを 20 台のカメラに適用することができます。

名前	詳細
テンプレートを適用	どのカメラにテンプレートを適用するか選択します。2 つの**設定**ボタンのいずれかを使用して、実際にテンプレートに適用します。
全て選択	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択します。
全てクリアする	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択解除します。
選択したカメラにテンプレートを適用する	テンプレートの値を、選択したカメラに適用します。

モーション検知の調整ウィザード

モーション検知の調整ウィザードは、カメラのモーション検知のプロパティを迅速に設定するのに便利です。

複数の同時ビデオストリーム出力に対応しないカメラは、監視サーバーと Management Application に同時に接続することはできません。Milestone では、そうしたデバイスでモーション検知や PTZ を設定する場合、Recording Server サービスを停止 『168ページ の"サービスを開始および停止する"参照 』することを推奨しています。

Management Application でカメラからのビデオを表示する 『44ページ の"Management Application でカメラからビデオを再生する"参照 』も参照してください。

モーション検知の調整：領域の除外

ウィザードの領域の除外セクションで、カメラのビューの特定のエリアでモーション検知を無効にできます。特定エリアのモーション検知を無効にすると、たとえば、カメラの撮影範囲に、風で揺れる木がある、または背景に定期的に自動車が通過する場合など、不適切なモーションの検知を避けることができます。

複数の同時ビデオストリーム出力に対応しないカメラは、監視サーバーと Management Application に同時接続することはできません。Milestone では、そうしたデバイスでモーション検知や PTZ を設定する場合、Recording Server サービスを停止 『168ページ の"サービスを開始および停止する"参照 』することを推奨しています。Management Application でカメラからのビデオ表示 『44ページ の"Management Application でカメラからビデオを再生する"参照 』も参照してください。

同じ除外領域を表示する各カメラでは、ウィザードウィンドウの左側にあるリストを使ってカメラを選択し、領域の除外を定義します。領域の除外は各カメラに固有であるため、必要なそれぞれのカメラで個別にモーション検知を設定する必要があります。

カメラを選択すると、カメラのプレビューを確認できます。プレビューで除外する領域を定義し、グリッドで小さいセクションに分割します。

- グリッドを表示するには、**グリッドを表示**チェックボックスを選択します。
- 除外領域を定義するには、マウスのボタンを押下した状態で、プレビュー画像の必要な部分にマウスのポインタをドラッグします。左マウスボタンでグリッドを選択します。右マウスボタンでグリッドをクリアします。選択されたエリアが、青色で強調表示されます。

すべて除外ボタンを使用すると、プレビュー画像にあるすべてのグリッドセクションを迅速に選択することができます。これは、プレビュー画像の大半のエリアでモーション検知を無効にする場合にお勧めします。その場合は、モーション検知を無効にしない部分をクリアします。**すべてを含む**ボタンを使うと、素早くすべてのセクションを選択解除できます。

モーション検知の調整：モーション検知

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、製品比較チャート『12ページ 』を参照してください。

モーション検知は、ほとんどの監視システムで非常に重要な要素です。モーション検知の設定によって、いつビデオを録画するか（監視システムサーバーに保存）、いつアラーム通知を送信するか、いつ出力（照明やサイレン）をトリガするかなどを決定することができます。

不要な録画やアラーム通知などを避けるために、それぞれのカメラに対して、可能な限り最適なモーション検知の設定をすることが重要になります。カメラの物理的な位置ごとに、さまざまな物理的条件（昼/夜、強風/無風および同様の条件）で設定をテストすることをお勧めします。

複数の同時ビデオストリーム出力に対応しないカメラは、監視サーバーと Management Application に同時接続することはできません。Milestone では、そうしたデバイスでモーション検知や PTZ を設定する場合、Recording Server サービスを停止 『168ページ の"サービスを開始および停止する"参照 』することを推奨しています。Management Application でカメラからのビデオを表示する 『44ページ の"Management Application でカメラからビデオを再生する"参照 』も参照してください。

モーション検知の設定は、それぞれのカメラに対して行うこともできますし、複数のカメラについて同時に行うことも可能です。ウィザードウィンドウの左側のペインにあるリストを使って、カメラを選択します。一度に複数のカメラを選択する場合は、**CTRL** または **SHIFT** を押しながら選択します。カメラを選択すると、カメラのプレビューを確認できます。複数のカメラを選択した場合、最後に選択したカメラからのプレビューを確認できます。プレビュー画像の緑色のエリアがモーションを示しています。

名前	詳細
感度	**感度**スライダーを調整して、不要なバックグランドノイズをフィルタし、実際のモーションだけが緑色で表示されるようにします。または、スライダーの横のフィールドで 0～256 の値を指定して、感度設定を制御します。 スライダーによって、モーションとして認識するために必要な変化するピクセル数を決定します。感度が高いと、モーションとして認識するために必要なピクセルの変化は非常に小さくなります。スライダーを左へ移動させるほど、プレビューの緑色部分が増えます。これは、感度が高いほどわずかなピクセルの変化でもモーションとして認識されるためです。
モーション	必要なレベルのモーションによってのみ、モーション検知がトリガされるように**モーション**スライダーを調整します。選択されたモーションレベルは、スライダーの上にある**レベル**バーの黒い垂直線で示されます。黒い垂直線は、閾値になります。モーションが選択されたレベルを超える場合（右側）、バーの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。 または、左のフィールドで 0～10000 の値を指定して、モーション設定を制御します。 スライダーを左へドラッグするほど、モーション検知に必要な変化が小さくなるので、よりモーション検知が表示されます。モーション検知の回数も録画するビデオの量、受信する通知の量などに影響を与えます。
検知間隔	カメラからのビデオで、どれくらいの頻度でモーション検知分析を行うかを指定します。デフォルトは 240 ミリ秒ごとです（1 秒にほぼ 4 回）。この間隔は、使用しているカメラのフレームレート設定には関係なく適用されます。 この設定を調整すると、モーション検知で使用されるシステムのリソースを低減できます。

名前	詳細
検知解像度	画像全体を分析するか、選択した部分の画像を分析するかを指定します。たとえば 25%と指定すると、すべてのピクセルを分析する代わりに 4 ピクセルごとに分析するので、使用するシステムのリソースは低減しますが、モーション検知の正確度も低下します。
キーフレームだけ	ビデオストリームのキーフレームのみでモーション検知を行うことで、モーション検知で使用するシステムのリソースを減らしたい場合は、**キーフレームだけ**を選択します。

ユーザーアクセスの管理ウィザード

ユーザーアクセスの管理手順を使用して、システムやそのクライアントにアクセスできるように個々のユーザーを追加します。ウィザードの最後にあるアクセスの概要には、アクセス権があるカメラがリスト化されます。

重要： このウィザードを使用すると、後の段階で追加される新しいカメラを含めて、すべてのカメラに対して、追加したすべてのユーザーがアクセスできるようになります。一方、アクセスの設定、ユーザー、ユーザー権限『161ページ の"ユーザーおよびグループの権限の設定"参照 』を別個に指定することができます。サーバーアクセスの設定 『156ページ 』を参照してください。ユーザーをグループ 『160ページ の"ユーザーグループの追加"参照 』に追加することはできません。

ユーザーアクセスの管理：基本ユーザーと Windows ユーザー

Active Directory®は、XProtect Professional。

クライアントユーザーは、次の 2 種類の方法で追加できます。必要に応じて、これらを組み合わせることができます。

名前	詳細
基本ユーザー	それぞれの個別のユーザーについて、基本ユーザー名とパスワード認証で、監視システム専用のユーザーアカウントを作成します。
Windows ユーザー	サーバーでローカルまたは Active Directory で定義されたユーザーをインポートし、それらのユーザーの Windows ログインに基づいて認証します。

ユーザーは、サーバー上でローカル PC ユーザーとして定義し、サーバーの簡易ファイル共有を無効にする必要があります。

基本ユーザーの追加

1. ユーザー名とパスワードを指定して、**基本ユーザーの追加**ボタンをクリックします。必要に応じて、操作を繰り返します。

Windows ユーザーの追加

1. **Windows ユーザーの追加...**をクリックして、**ユーザーまたはグループの選択**ダイアログを開きます。**場所...**ボタンをクリックしても、選択できるのはローカルコンピュータからだけになります。

2. **選択するオブジェクト名を入力してください**の欄にユーザー名を入力してから、**名前の確認**機能を使用して、ユーザー名を確認します。複数のユーザー名を入力する場合は、それぞれの名前をセミコロンで区切ります。例：**Brian; Hannah; Karen; Wayne**。

3. 完了したら、**OK** をクリックします。

重要：ローカルデータベースから追加されたユーザーがクライアントにログインする場合、ユーザーはユーザー名の一部としてサーバー名、PC の名前または IP アドレスを指定してはなりません。正しく指定したユーザー名の例：USER001。正しくない例：PC001/USER001。もちろん、ユーザーはパスワードや関連するサーバーの情報も指定する必要があります。

ユーザーアクセスの管理：アクセスの概要

アクセスの概要には、ユーザーがアクセスできるカメラが一覧されます。ウィザードを使用すると、後の段階で追加した新しいカメラを含めて、すべてのカメラに対して、追加したすべてのユーザーがアクセスできるようになります。ただし、個々の権限『161ページ の"ユーザーおよびグループの権限の設定"参照 』を変更して、個々のユーザーのカメラへのアクセスを制限することもできます。

詳細設定

ハードウェアデバイス

ハードウェアデバイスについて

カメラ、およびビデオエンコーダーなどその他のハードウェアデバイスは、**ハードウェアデバイスの追加...**ウィザード『46ページ の"ハードウェアの追加ウィザード"参照 』を使用してシステムに追加します。マイクやスピーカーがハードウェアデバイスに付属している場合は、これらも自動的に追加されます（使用している XProtect のバージョンでサポートされている場合）。

マイクについて

システムで、**マイク**は通常はハードウェアデバイスに取り付けられるので、物理的にカメラの次に位置します。そこで、必要な権限を持つオペレータは、XProtect Smart Client (XProtect Smart Client を実行しているコンピュータにスピーカーが取り付けられている場合」を通じて録音を聴くことができます。マイクはシステムで管理します。つまり、XProtect Smart Client のオペレータのコンピュータに取り付けられているマイクでは**なく**、カメラに取り付けられているマイクを常に管理できます。

必要以上のマイクをシステムに追加した場合、関連するマイクやスピーカーを右クリックして、**非表示**を選択すると、不要なものを非表示にすることができます。非表示にしたマイクを再度表示したい場合は、マイク全体のアイコンを右クリックして、**非表示の項目を表示**を選択します。

スピーカーについて

スピーカーはデバイスに取り付けられ、通常は物理的にカメラの横に配置します。通常、スピーカーはカメラの近くにいる人に情報を通知します。必要な権限を持つオペレータは、XProtect Smart Client（XProtect Smart Client を実行しているコンピュータにマイクが装備されている場合）を使用して、スピーカーで話しかけることができます。

例：エレベーターが止まってしまいました。エレベーターに取り付けられたカメラを通じて、XProtect Smart Client のオペレータは、年配の女性がエレベーターに乗っていることを確認できます。カメラに取り付けられたマイクから、女性が次のように話すのが録音されます。「怖いわ。助けてください！」カメラに取り付けられたスピーカーを通じて、オペレータが女性に語りかけます。「間もなく救助が到着しますよ。あと 15 分以内に出られます。」

必要以上のスピーカーをシステムに追加した場合、関連するスピーカーを右クリックして、**非表示**を選択すると、不要なスピーカーを非表示にすることができます。非表示にしたスピーカーを再度表示したい場合は、スピーカー全体のアイコンを右クリックして、**非表示アイテムの表示**を選択します。

音声録音について

音声を録音する場合、以下に注意することが重要です。

- システムが録音できるのは、（マイクから）入ってくる音声だけです。システムは、（スピーカから）出ていく音声は録音しません。

- 音声録音は、ビデオ保存容量に影響します。システムは、関連するカメラのデータベースに音声を録音します。したがって、ビデオだけを録画する場合に比べて、音声とビデオを記録する場合、より早くデータベースが満杯になることに留意する必要があります。データベースが満杯になると、システムは自動的にデータをアーカイブするので、データベースが満杯になること自体は問題ではありません。ただし、音声を録音する場合、追加のアーカイブ容量が必要になります。

  - 例 : MPEG4 を使用する場合、それぞれ 1 秒のビデオ GOP（Group Of Pictures）が、データベースの 1 レコードに保存されます。毎秒ごとの音声が、データベースの 1 レコードに保存されます。データベースのレコードの半分は音声の保存に使用されるので、データベースのビデオ保存容量が全体容量の半分に低減します。したがってデータベースはすぐに満杯になり、ビデオだけを録画する場合と比べて、より頻繁にアーカイブが発生します。

  - 例 : MJPEG を使用する場合、音声ブロックのサイズが JPEG 間の時間を超えない限り、すべての JPEG に対して音声が 1 レコードに保存されます。極端な場合は、データベースのレコードの半分が音声の保存で使用されるので、データベースのビデオ保存容量が全体容量の半分に低減します。非常に高いフレームレートを使用すると、各 JPEG 間の時間が短くなることを意味するので、音声の録音に使用するデータベースの割合が小さくなり、その結果ビデオの保存で使用できる部分は大きくなります。その結果として、データベースはすぐに満杯になり、ビデオだけを録画する場合と比べて、より頻繁にアーカイブが発生します。

上記では、単純化した例を示しています。正確な使用可能な保存容量は、GOP/JPEG および音声のキロバイト単位でのサイズにも依存します。

専用入力/出力デバイスについて

システムに、多数の専用の入力/出力(I/O)ハードウェアデバイスを追加することができます。システムがどの I/O ハードウェアデバイスをサポートしているかに関する情報は、リリースノートを参照してください。

I/O ハードウェアデバイスを追加すると、デバイスでの入力がシステムでイベントを生成するために使用され、システムでのイベントは I/O ハードウェアデバイスでの出力を有効化するのに使用されます。これは、カメラと同じ方法で設定されたイベントベースのシステムで I/O ハードウェアデバイスを使用できることを意味します。

一部の I/O ハードウェアデバイスでは、監視システムが定期的にハードウェアデバイスの入力ポートの状態をチェックして、入力を受信したかどうか検出しなければなりません。このような定期的な状態チェックを、**ポーリング**と呼びます。状態チェックの間隔は、**ポーリング頻度**と呼ばれ、一般的なポートとポーリングのプロパティ『115ページ の"ポートとポーリング"参照 』の一部として指定されます。このような I/O ハードウェアデバイスの場合、ポーリング頻度を可能な限り低い値（状態チェックの間隔を 10 分の 1 の秒数）に設定する必要があります。どの I/O ハードウェアデバイスがポーリングを必要とするかに関する情報は、リリースノートを参照してください。

マイクやスピーカーの表示/非表示

システムで必要とされる数以上のマイクやスピーカーを追加した場合、不要なマイクやスピーカーを右クリックして、**非表示**を選択すると、それらを非表示にすることができます。非表示にしたマイク/スピーカーを再度表示したい場合は、マイクやスピーカー全体のアイコンを右クリックして、**非表示アイテムの表示**を選択します。

ハードウェアデバイスの設定

ハードウェアデバイスを追加した後に、IP アドレス、どのビデオチャンネルを使用するか、どの COM ポートを取り付けられた PTZ カメラのコントロールで使用するか、魚眼レンズ技術を使用するかどうかなど、デバイス固有のプロパティを指定/編集することができます。

1. **詳細設定**を展開し、**ハードウェアデバイス**を展開し、関連するハードウェアデバイスを右クリックし、**プロパティ**を選択します。

2. 必要に応じて、名前とビデオチャンネル、ネットワーク、デバイスタイプおよびライセンス 『67ページ の"ネットワーク、デバイスタイプ、ライセンス"参照 』、PTZ デバイス 『68ページ の"PTZ デバイス（プロパティ）"参照 』、魚眼レンズのプロパティを指定します。

3. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

ハードウェアデバイスの削除/無効化

重要： ハードウェアデバイスを削除する場合、ハードウェアデバイスに取り付けられているすべてのカメラ、スピーカー、マイクが削除されるだけではありません。ハードウェアデバイスに取り付けられているカメラの録画もすべて削除されます。

1. **詳細設定**を展開し、**ハードウェアデバイス**を展開し、削除するハードウェアデバイスを右クリックし、**ハードウェアデバイスの削除**を選択します。

2. ハードウェアデバイスおよびそれらに含まれるすべての録画も削除されることを確認します。

3. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

4. Recording Server サービスを再起動『168ページ の"サービスを開始および停止する"参照 』します。

削除する代わりに、ハードウェアデバイスに取り付けられているカメラ、スピーカー、マイクを個別に無効化することも可能です。

1. **詳細設定**を展開し、**ハードウェアデバイス**を展開し、関連するハードウェアデバイスを展開します。

2. 無効にしたいカメラ、スピーカー、マイクを右クリックして、**無効**を選択します。

3. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

4. Recording Server サービスを再起動『168ページ の"サービスを開始および停止する"参照 』します。

ハードウェアデバイスの交換について

システムへ設定済みのハードウェアデバイスを新しいハードウェアデバイスと交換することができます。たとえば、ネットワーク内のカメラを物理的に交換できます。

ハードウェアデバイスの交換ウィザード 『64ページ の"ハードウェアデバイス交換ウィザードについて"参照 』開いてください。このウィザードは、以下の項目を含む監視システムサーバーでの交換プロセス全体を支援します。

- 新規ハードウェアデバイスの検出
- 新規ハードウェアデバイスに対するライセンスの指定
- 古いハードウェアデバイスによる既存の録画に対して何を行うかの決定

ハードウェアデバイス交換ウィザードについて

以前に追加して、監視システムに設定してあるハードウェアデバイスを交換するには、ハードウェアデバイス交換ウィザードを使用します。ハードウェアデバイス交換ウィザードを開くには、交換したいデバイスを右クリックし、**ハードウェアデバイスの交換**を選択します。このウィザードは、新規ハードウェアデバイスの情報ページとデータベースアクションページに分割されます。

新規ハードウェアデバイスの情報

新規ハードウェアデバイスに関する詳細を指定します。

IP アドレス	ハードウェアデバイスの IP アドレスまたはホスト名。
ポート	スキャンするポート番号。デフォルトポートは 80 です。 ハードウェアデバイスが NAT 対応のルーターまたはファイアウォールの背後にある場合、別のポート番号の指定が必要になることがあります。この場合、ハードウェアデバイスが使用しているポートや IP アドレスをマップするように、ルーター/ファイアウォールを設定する必要もあることに留意してください。
ユーザー名	ハードウェアデバイスの管理者アカウントのユーザー名。 多くの組織では、ハードウェアデバイスの製造元によるデフォルトのユーザー名をハードウェアデバイスで使用しています。あなたの組織の場合であれば、"<デフォルト>"を選択します。システムがメーカーのデフォルトユーザー名を知っていると誤解の原因となるため、メーカーのデフォルトユーザー名は入力しないでください。 たとえば admin や root など、リストから他の一般的なユーザー名を選択することもできます。リストにないユーザー名を使用するときは、新しいユーザー名を入力します。
パスワード	管理者アカウントにアクセスするために必要なパスワードです。一部のハードウェアデバイスでは、アクセスにユーザー名/パスワードを必要としません。

デバイスドライバー

新規ハードウェアデバイスで、どのデバイスドライバーを使用するかを指定する方法：

- **ハードウェアデバイスタイプ**リストで、ビデオデバイスドライバーを選択してから、**自動検知/ハードウェアデバイスタイプの確認**をクリックして、ドライバーがハードウェアデバイスと一致しているか確認します。

  - または -

- **自動検知/ハードウェアデバイスタイプの確認**をクリックして自動検出し、適切なドライバーを確認します。

適切なドライバーが見つかると、**シリアル番号（MAC アドレス）**フィールドに、新しいハードウェアデバイスの MAC アドレスが表示されます。完了したら、**次へ**をクリックします。

カメラおよびデータベースアクション

ハードウェア交換ウィザードの最後のページで、カメラおよび古いハードウェアデバイスに属しているカメラからの録画を含んでいるデータベースに対して何を行うかを決定します。ビデオエンコーダーなどのマルチカメラデバイスでは、新しいハードウェアデバイスの各チャンネルで何を行うかを決定する必要があります。

ウィザードページの左側にあるテーブルには、新しいハードウェアデバイスで使用できるビデオチャンネルのリストが表示されます。通常の単一カメラのハードウェアデバイスの場合は、ビデオチャンネルは 1 つだけになります。ビデオエンコーダーの場合は、通常は複数のビデオチャンネルがあります。

1. それぞれのビデオチャンネルで、テーブルの**継承**列を使用して、古いハードウェアデバイスのどのカメラを新規ハードウェアデバイスで継承するかを選択します。

2. カメラデータベースで何を行うか決定します。次の 3 つのオプションがあります。

   - **既存のデータベースを継承：** 新規ハードウェアデバイスで継承を選択したカメラは、古いハードウェアデバイスからカメラの名前、録画データベース、ならびにアーカイブを継承します。データベースとアーカイブの名前は、新しいハードウェアデバイスの MAC アドレスとビデオチャンネルを反映するように変更されます。継承されたカメラに対するユーザーのアクセス権限は自動的に更新されるため、ユーザーは新旧の録画を表示できるようになります。カメラの名前は同じままであるため、ユーザーにはハードウェアデバイスの交換は認識されません。

   - **既存のデータベースを削除：** 新規ハードウェアデバイスで継承を選択したカメラのデータベースは削除されません。今後の録画用に新しいデータベースが作成されますが、ハードウェアの交換前の録画を表示することはできません。

   - **既存のデータベースを残す：** 新規ハードウェアデバイスで継承を選択したカメラのデータベースは削除されません。今後の録画用に新しいデータベースが作成されます。古いデータベースもシステムのサーバーに残りますが、ハードウェアの交換前の録画を表示することはできません。後で古いデータベースを削除したくなった場合は、手動で削除しなければなりません。

3. 新規ハードウェアデバイスのビデオチャンネルの数が古いハードウェアデバイスのビデオチャンネルより少ない場合は、新規ハードウェアデバイスが古いハードウェアデバイスからすべてのカメラを継承することはできません。この場合、新しいハードウェアデバイスによって継承できなかったカメラのデータベースに関して、何を行うか質問されます。次の 2 つのオプションがあります。

   - **継承されていないカメラのデータベースを削除する：** 新規ハードウェアデバイスで継承できなかったカメラのデータベースは削除されます。ハードウェアの交換前の録画を表示することはできません。当然のことながら、新規ハードウェアデバイスによる今後の録画用に、新しいデータベースが作成されます。

   - **継承されていないカメラのデータベースを残す：**新規ハードウェアデバイスで継承できなかったカメラのデータベースは削除されません。システムのサーバーに古いデータベースが残っていても、ハードウェアの交換前の録画を表示することはできません。後で古いデータベースを削除したくなった場合は、手動で削除しなければなりません。当然のことながら、新規ハードウェアデバイスによる今後の録画用に、新しいデータベースが作成されます。

4. **終了**をクリックします。準備ができたら、Recording Server サービスを再起動します。ハードウェアの交換は、Recording Server サービスを再起動するまでクライアントには認識されません。

スピーカープロパティ

特定のカメラに対してビデオおよびレコーディングの設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、音声を録音するタイミングを指定できます。この選択は、システムのすべてのカメラに適用されます。

有効	スピーカーはデフォルトで有効になっており、これはシステムに音声を転送できることを意味します。必要に応じて、個別のスピーカーを無効にすることができます。この場合、スピーカーからシステムへ音声は転送されません。
スピーカー名	Management Application およびクライアントで表示される名前です。既存の名前を、新しい名前で上書きすることができます。 名前は一意であり、以下の特殊文字を含むことはできません。 **< > & ' " ¥ / : * ? | [ ]**

ハードウェアプロパティ

ハードウェア名とビデオ チャンネル

ハードウェアデバイスを設定する時は、以下のプロパティを指定します。

ハードウェア名	Management Application およびクライアントで表示される名前です。既存の名前を、新しい名前で上書きすることができます。 名前は一意であり、以下の特殊文字を含むことはできません。 **< > & ' " ¥ / : * ? | [ ]**
有効にするビデオチャンネル番号	選択したハードウェアデバイスのそれぞれのビデオ チャンネルを有効/無効にします。多くのハードウェアデバイスには単一のビデオチャンネルしかなく、この場合一覧されるチャンネルは 1 つだけです。 他のハードウェアデバイス（通常は、ビデオエンコーダーデバイス）には、複数のビデオ チャンネルがあります。

ネットワーク、デバイスタイプ、ライセンス

ハードウェアデバイスを設定 『63ページ の"ハードウェアデバイスの設定"参照 』する時は、以下のプロパティを指定します。

IP アドレス	ハードウェアデバイスの IP アドレスまたはホスト名。
HTTP ポート	ハードウェアデバイスとの HTTP 通信に使用するポート。デフォルトはポート 80 です。デフォルトのポートを使用するには、**デフォルト HTTP ポートの使用**を選択します。
FTP ポート	ハードウェアデバイスとの FTP 通信に使用するポート。デフォルトのポートは、ポート 21 です。 デフォルトのポートを使用する場合は、**デフォルト FTP ポートの使用**を選択します。
ユーザー名	**サーバーのログインが必要です**を選択した場合にのみ必要です。SMTP サーバーがユーザ認証を必要とする場合、ユーザー名を指定します。
ユーザー名	ハードウェアデバイスの管理者アカウントのユーザー名。 多くの組織では、ハードウェアデバイスの製造元によるデフォルトのユーザー名をハードウェアデバイスで使用しています。この場合は、[<デフォルト>]を選択します。間違いの原因となるので、製造元によるデフォルトのユーザー名を入力しないでください。システムが製造元のデフォルトユーザー名を認識していることを確認します。 たとえば admin や root など、リストから他の一般的なユーザー名を選択することもできます。リストにないユーザー名を使用するときは、新しいユーザー名を入力します。
パスワード	パスワードを編集します。入力確認のため、パスワードを再入力することを忘れないでください。 これを編集できるのは、選択したユーザーが基本ユーザーである場合だけです。

ハードウェアタイプ	ハードウェアデバイスとの通信で使用するビデオデバイスドライバーのタイプを示す、読み取り専用のフィールド。
シリアル番号（MAC アドレス）	デバイスのシリアル番号を示す、読み取り専用のフィールド。このシリアル番号は、通常はハードウェアデバイスの 12 桁/16 進数の MAC アドレスです。（例：0123456789AF）。
ライセンス情報	ハードウェアの現在のライセンス状態。
ハードウェアデバイスの交換	ウィザード『64ページ の"ハードウェアデバイス交換ウィザードについて"参照 』を開き、必要に応じて、選択したハードウェアデバイスを別のデバイスに交換します。 この操作が必要になるのは、ネットワーク上で物理的なカメラを交換する場合のみです。このウィザードでは、接続されたカメラから古いハードウェアデバイスへの録画の処理方法の決定など、すべての関連する問題を考慮できます。

PTZ デバイス（プロパティ）

PTZ を使用できるビデオエンコーダーハードウェアデバイスを設定『63ページ の"ハードウェアデバイスの設定"参照 』する場合にのみ、PTZ デバイスタブを使用できます。

接続されているカメラには、パン/チルト/ズームの機能があります	ビデオエンコーダーデバイスに接続されているいずれかのカメラが PTZ カメラである場合、チェックボックスを選択します。
COM#の PTZ タイプ	PTZ カメラが COM ポート経由で制御される場合、関連するオプションを選択します。オプションはデバイス固有で、デバイスがどの PTZ プロトコルを使用するかに応じて異なります。COM ポート経由で PTZ カメラを制御しない場合は、無しを選択します。

ダイアログの下半分にある表には、ハードウェアデバイスの各ビデオチャンネルに対応する行が表示されます。上から 1 番目の行がビデオチャンネル 1 に対応し、上から 2 番目の行はビデオチャンネル 2 に対応しています。以下も同様になります。

名前	対象となるビデオチャンネルに接続されているカメラの名前。
タイプ	選択したカメラチャンネルにあるカメラが固定であるか、移動可能であるかを選択します。 • **固定**：カメラは、固定位置に取り付けられた標準的なカメラです。 • **移動可能**：カメラは、PTZ カメラです。
ポート	**タイプ**列で**移動可能**が選択されている場合のみ使用可能です。ビデオエンコーダーのどの COM ポートを PTZ カメラの制御で使用するかを選択します。
ポートアドレス	**タイプ**列で**移動可能**が選択されている場合のみ使用可能です。カメラのポートアドレスを指定してください。通常のポートアドレスは 1 です。デイジーチェインで接続されている PTZ カメラを使用する場合、ポートアドレスはそれぞれを識別するため、カメラのマニュアルで推奨されている設定になっているか確認してください。

カメラとストレージの情報

ビデオや録画の設定について

ハードウェアデバイスを追加して、カメラを設置したら、次の 3 つの方法でビデオや録画を設定できます。

名前	詳細
ウィザードによる設定	すべてのカメラに関するビデオ、録画、アーカイブの設定をガイドに従って行います。
一般	すべてのカメラに対して、ビデオ、録画、共有設定（ダイナミックアーカイブパスや音声を録音するかどうかなど）を指定します。
カメラの個別設定	個々のカメラのそれぞれについて、ビデオ、録画、カメラ固有の設定（イベント情報、PTZ プリセット位置、魚眼レンズビューエリア）を指定します。

データベースのサイズ変更について

カメラの録画が予想以上に大きくなった場合、その他の原因で使用可能なドライブスペースが別の理由で急に減少した場合、データベースのサイズ変更が自動的に行われます。

- カメラのデータベースと同じドライブにアーカイブ 『124ページ の"アーカイブについて"参照 』が存在する場合、そのドライブでアーカイブされているすべてのカメラのうち最も古いアーカイブが別のドライブへ移動されるか、あるいは移動できない場合は削除されます（アーカイブの移動が可能になるのは、ダイナミックアーカイブ 『76ページ の"ダイナミックパスの選択（プロパティ）"参照 』を使用していて、複数の異なるドライブへのアーカイブである場合のみ）。
- カメラのデータベースを含んでいるドライブにアーカイブが存在しない場合、最も古い録画の一部を削除し、すべてのデータベースのサイズを一時的に制限することにより、そのドライブのすべてのカメラデータベースのサイズが縮小されます。

このようなデータベースのサイズ変更に伴い、Recording Server サービス 『165ページ の"サービスについて"参照 』を再起動すると、元のデータベースのサイズが使用されます。したがって、まずドライブサイズの問題を解決する必要があります。データベースのサイズ変更の手順が行われた場合、XProtect Smart Client の画面上や、ログファイルに情報が表示されます。また、設定されている場合には通知が送られます。

モーション検知について

モーション検知の設定はカメラの録画プロパティにリンクしており、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。

デフォルトでは、モーション検知が有効になっています。無効にすると、システムの CPU や RAM のパフォーマンスは改善しますが、同時にモーション検知、イベント、アラームの管理にも影響します。

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、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。

カメラのモーション検知を設定する前に、Milestone では、カメラの画質の設定（例、ビデオコーデック、ストリーム設定など）を行っておくことをお勧めします。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。

カメラに対して組み込みモーション検知を有効にした場合（表 1）と無効にした場合（表 2）の違いを以下の 2 つの表に示します。

モーション検知を有効にした場合

録画プロパティの設定	記録	モーション検知によるイベント	モーション検知によらないイベント	シーケンス
常時録音	はい	はい	はい	はい
設定しない	いいえ	はい	はい	いいえ
組み込みモーション検知	はい	はい	はい	はい
組み込みモーション検知 & イベントまたはイベントのみ	はい	はい	はい	はい

モーション検知を無効

カメラの録画の設定	記録	モーション検知によるイベント	モーション検知によらないイベント	シーケンス
常時録音	はい	いいえ	はい	いいえ
設定しない	いいえ	いいえ	はい	いいえ
組み込みモーション検知	いいえ	いいえ	はい	いいえ
組み込みモーション検知およびイベントまたはイベントのみ	はい（設定に依存）	いいえ	はい（設定に依存）	いいえ

モーション検知感度

デフォルトでは、モーション検知がダイナミック感度に設定されています。ただし、**モーション検知と除外エリア**プロパティにおいて、手動で感度レベルを調整することもできます。

次の理由により、Milestone は手動感度を有効にしないことをお勧めします。

- ダイナミック感度の場合、システムは感度レベルを自動的に計算して最適化し、画像のノイズから発生するモーション検知を抑制します。
- 夜間には、画像のノイズにより誤ったモーションが頻繁にトリガされますが、ダイナミック感度によりモーション検知が改善します。
- 録画が多すぎることに起因するシステム過負荷は発生しません。

録画が少なすぎるために結果が見られなくなることもありません。 モーション検知および PTZ カメラ

モーション検知は、一般に、パン/チルト/ズーム(PTZ)カメラでも通常のカメラの場合と同様に機能します。ただし、PTZ カメラの各プリセット位置に対して個別にモーション検知を設定することはできません。

モーション検知および PTZ カメラについて

モーション検知は、一般に、パン/チルト/ズーム(PTZ)カメラでも通常のカメラの場合と同様に機能します。ただし、PTZ カメラの各プリセット位置に対して個別にモーション検知を設定することはできません。

不要な録画、通知などを行わないために、PTZ カメラが 2 つのプリセット位置の間で移動している間は、システムは自動的にモーション検知を無効にします。一定の秒数が経過すると、システムは再び自動的にモーション検知を有効にします。この期間は移行時間と呼ばれ、PTZ カメラの PTZ パトロールプロパティ『102ページ の"PTZ パトロール（プロパティ）"参照 』で指定されます。

特定カメラスケジュールの構成

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、製品比較チャート『12ページ 』を参照してください。

特定の期間内のイベントのスケジュールプロファイル、またはその一部に基づいている場合は、カレンダー選択の下のリストから**開始イベント**および**停止イベント**を選択することを忘れないでください。

他のフィールドの下にあるイベントの**設定**リストを使用して、必要に応じたイベントを定義します。

貴方のシステムで、カメラがビデオの移行することは、必ずしも、カメラからビデオに記録されることではありません。記録は別に構成されています「ビデオと記録の構成」 『69ページ の"ビデオや録画の設定について"参照 』をご覧ください。

各カメラごとに、スケジュール・プロフィールを制作できます。

オンライン期間

- 時間の区分（例：毎月曜日 8:30～17:45）ピンク色で示されます。
- 時間内の出来事（例：出来事 A は、出来事 B が起きるまで生じています毎月曜日 8:30～17:45）黄色で示されます。

二つの選択肢は一緒にできますが、時間内で重複はできません。

スピードアップ

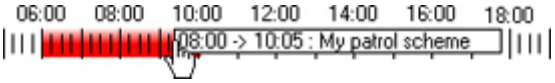
- 時間の区分（例：毎月曜日 8:30～17:45）オリーブ緑色で示されます。 

E メールのお知らせ

- 時間の区分（例：毎月曜日 8:30～17:45）青色で示されます。 

PTZ パトロール

- 時間の区分（例：毎月曜日 8:30～17:45）赤色で示されます。 
- 一つのパトロールを使用していて、すぐに他のパトロールが続く場合には、マウスのポインターを赤いバーにつけて、どのパトロールファイルが作動しているか見て下さい。



SMS のお知らせ

時間の区分（例：毎月曜日 8:30～17:45）緑色で示されます。  プロフィールの設定

1. **スケジュール・プロフィール**の中で、**新規追加**を選んで下さい。
2. **プロフィールの追加**ダイアローグで、プロフィールの名前を入れて下さい。 名前には、以下の特殊文字を含めることはできません。 **< > & ' " ¥ / : * ? | [ ]**
3. ダイアローグのトップ右コーナーで、**「オンタイムでカメラ開始/停止の設定」**を設定し、次に、時間区分を設定し、またはその時間内での出来事に関しては、**「出来事に関するカメラ開始/停止の設定」**を設定してください。
4. カレンダーのセクションで、必要な開始日時へマウスポインタを移動させてから、左マウスボタンを押下し、マウスポインタをドラッグして、希望する終了日時でリリースします。
   - それぞれの日を個別に指定します。
   - 時間は 5 分刻みで指定します。システムではマウスポインタが位置している時間が表示され、操作を助けます。

特定の期間内のイベントのスケジュールプロファイル、またはその一部に基づいている場合は、カレンダー選択の下のリストから**開始イベント**および**停止イベント**を選択することを忘れないでください。

- 他のフィールドの下にあるイベントの**設定**リストを使用して、必要に応じたイベントを定義します。
- スケジュールプロファイルの不要な部分を削除するには、該当部分を右クリックし、**削除**を選択します。
- 終日を速やかに入力またはクリアしたい場合は、その日の名前をダブルクリックします。

- カレンダーのセクションの内側をドラッグする代わりに**開始時刻**、**終了時刻**、**日**のフィールドを使用し、必要に応じて**期間の変更**または**期間の設定**ボタンを使用することもできます。**開始時刻**および**終了時刻**のフィールドを使用する場合、時間を 5 分刻みで指定することを忘れないでください。5 分より短い期間は指定できないため、使用できる時刻は 12:00, 12.05, 12:10, 12:15 などとなります。5 分間隔以外の時刻（たとえば 12:13）を指定すると、エラーメッセージが表示されます。

カメラがいつ、何をする必要があるかを設定する

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。詳細については、製品比較チャート『12ページ 』を参照してください。

いつ実行するかを設定するには、スケジュール機能を使用します。

- カメラはオンラインであり、システムにビデオを転送する必要があります。
- カメラは、スピードアップを使用して、通常より高いフレームレートを使用する必要があります。
- カメラに関して E メールおよび/または SMS 通知を受信したい場合
- PTZ カメラは、パトロール設定に従って、パトロールを行う必要があります。
- アーカイブを発生する必要がある

一般的なスケジュールおよびアーカイブの設定 『129ページ 』およびカメラ固有のスケジュールの設定 『71ページ の"特定カメラスケジュールの構成"参照 』を参照してください。

モーション検知の設定

モーション検知を設定するには、以下を行います。

1. **詳細設定 > カメラおよびストレージの情報**を展開し、関連するカメラを右クリック**> プロパティ**をクリックします。
2. **カメラのプロパティ**ウィンドウで、**録画プロパティ**タブを選択し、>関連する設定 『69ページ の"モーション検知について"参照 』を選択します。
3. **モーション検知**タブを選択します。モーション検知から除外する領域がある場合（たとえば、カメラの撮影範囲に風で揺れる木がある場合）、マウスで選択して、その領域を除外 『58ページ の"モーション検知の調整：領域の除外"参照 』することができます。
4. 関連するプロパティ 『98ページ の"モーション検知&と領域の除外"参照 』を入力します。PTZ カメラ『71ページ の"モーション検知および PTZ カメラについて"参照 』では、モーション検知の動作に違いがあることに注意してください。

カメラの無効化または削除

すべてのカメラは、デフォルトで有効になっています。つまり、カメラがオンラインになるようスケジュールされている 『132ページ の"オンライン期間"参照 』場合、カメラからビデオをシステムに転送できることを意味します。

カメラを**無効にする**には：

1. **詳細設定**を展開し、**カメラおよびストレージの情報**を展開し、無効にしたいカメラをダブルクリックして、**有効**ボックスを選択解除します。

2. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

カメラを**削除**するには、ハードウェアデバイスを削除 『64ページ の"ハードウェアデバイスの削除/無効化"参照 』する必要があります。ハードウェアデバイスを削除する場合、取り付けられているマイクやスピーカーも削除されます。これを行いたくない場合は、代わりにカメラの無効化を検討してください。

PTZ タイプ 1 および 3 を、必要な位置へ移動する

PTZ タイプ 1 および 3 の場合、複数の異なる方法で、PTZ カメラを必要な位置へ移動することができます。

1. カメラプレビューの必要な位置をクリックする（カメラでサポートされている場合）。
2. カメラプレビューの近くにあるスライダーを使って、そのそれぞれの軸に沿って PTZ カメラを移動します。X 軸（左/右へのパン）、Y 軸（上/下へのチルト）、Z 軸（ズームインおよびズームアウト。ズームインするにはスライダーを**望遠**に移動し、ズームアウトするにはスライダーを**広角**に移動します）。
3. ナビゲーションボタンの使用：

 PTZ カメラを左上へ移動

 PTZ カメラを上へ移動

 PTZ カメラを右上へ移動

 PTZ カメラを左へ移動

 PTZ カメラをホームポジションへ移動（デフォルト位置）

 PTZ カメラを右へ移動

 PTZ カメラを左下へ移動

 PTZ カメラを下へ移動

 PTZ カメラを右下へ移動

 ズームアウト（クリックごとに 1 ズームレベル）

 ズームイン（クリックごとに 1 ズームレベル）

録画およびストレージのプロパティ

録画およびアーカイブのパス（プロパティ）

ビデオおよび録画を設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、多くのカメラに対して一定のプロパティを同時に指定することができます。 操作を迅速に行いたい場合や、対象となるプロパティが、個別のカメラではなく、すべてのカメラで共有されている場合が該当します。

白い背景のすべてのプロパティは編集可能で、水色の背景のプロパティは編集できません。 それぞれのカメラに対して、すべてのプロパティを個別に指定することも可能であることに注意してください。

テンプレート	テンプレートを使用すると、類似のプロパティが迅速に設定できて便利です。 たとえば、カメラが 20 台あり、録画パス、アーカイブパス、およびそれらすべての保持期間を変更したいとします。3 種類の同じ情報を 20 回入力する代わりに、テンプレートに一度だけ入力し、2 回クリックするだけで、そのテンプレートを 20 台のカメラに適用することができます。
テンプレートを適用	どのカメラにテンプレートを適用するか選択します。2 つの**設定**ボタンのいずれかを使用して、実際にテンプレートに適用します。
カメラ名	Management Application およびクライアントで表示される名前です。既存の名前を、新しい名前で上書きすることができます。 名前は一意であり、以下の特殊文字を含むことはできません。 **< > & ' " ¥ / : * ? | [ ]**
ショートカット	XProtect Smart Client のユーザーは、キーボードショートカットを活用できます。一例として、複数のカメラの再生を切り替えることができます。こうしたショートカットには数字も含まれており、各カメラを識別するために使用します。 ショートカット番号は、それぞれのカメラで一意でなければなりません。カメラのショートカット番号には、文字または特殊文字を含んではならず、最大で 8 桁以内になるようにしてください。 正しいカメラのショートカット番号の例：3, 12345678. 正しくないカメラのショートカット番号の例：Cam#3、123456789。 キーボードショートカットの使用方法に関する詳細情報は、XProtect Smart Client の他のマニュアルにあります。
録画パス	カメラのデータベースを保存するフォルダへのパス。デフォルトは、C:¥MediaDatabase です。他のフォルダを参照する場合は、該当するセルの横にあるアイコンをクリックしてください。指定できるのは、**ローカル**ドライブにあるフォルダへのパスのみです。ネットワークドライブへのパスを指定することはできません。ネットワークドライブを使用している場合、ネットワークドライブが使用不能になると、録画は保存できません。 録画パスを変更し、元の場所に既存の録画がある場合、録画を新しい場所に移動するか（推奨）、元の場所に残すか、削除するかを選択するよう確認されます。 複数のカメラがあり、複数のローカルドライブが使用可能な場合、個別のカメラのデータベースを複数のドライブに分散させることでパフォーマンスを改善できます。

アーカイブ パス	アーカイブ 『124ページ の"アーカイブについて"参照 』で動的パスを使用していない場合にのみ、編集可能です。カメラのアーカイブされた録画を保存するフォルダへのパス。デフォルトは、C:¥MediaDatabase です。 他のフォルダを参照する場合は、関連するセルの横にあるアイコンをクリックしてください。アーカイブ パスを変更し、古い場所に既存のアーカイブされた録画がある場合、アーカイブされた録画を新しい場所へ移動するか（推奨）、古い場所に残すか、あるいは削除するかを選択する必要があります。アーカイブされた録画を移動すると、システムは現在カメラのデータベースにあるものもアーカイブすることに注意してください。そのため、アーカイブされた録画を移動した直後に、カメラのデータベースは空になります。
保持期間	カメラからの録画（つまり、カメラのデータベースにある録画ならびにアーカイブされている録画）を保持しておく合計時間です。デフォルトの保持期間は 7 日間です。 保持期間は、録画を保持しておく**合計**時間です。以前のバージョンの監視システムでは、データベースとアーカイブで別個に制限時間を指定していました。
カメラ	**開く**ボタンをクリックして、選択したカメラに対して、詳細およびカメラ固有の設定（例：イベント通知、PTZ プリセット位置、魚眼レンズビューエリア）を設定します。
全て選択	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択します。
全てクリアする	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択解除します。
選択したカメラで、選択したテンプレートの値を設定する	テンプレートから選択した値だけを、選択したカメラに適用します。
選択したカメラですべてのテンプレート値を設定する	テンプレートのすべての値を、選択したカメラに適用します。

ダイナミックパスの選択（プロパティ）

ビデオおよび録画を設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、多くのカメラに対して一定のプロパティを同時に指定することができます。 動的パス選択の場合、すべてのカメラがプロパティを共有します。

ダイナミックアーカイブ 『124ページ の"アーカイブについて"参照 』パスでは、通常は複数のドライブに渡る、異なるアーカイブパスを指定します。システムデータベースを含んでいるパスが、アーカイブ用に選択したドライブのいずれかにあれば、システムは常にまずそのドライブにアーカイブしようと試みます。そうでない場合、そのドライブを使用するカメラデータベースが存在しない限り、システムは自動的にその時点で最も使用可能な容量が大きいアーカイブドライブにアーカイブします。使用可能な容量が最も大きいドライブはアーカイブプロセス中も変化するので、同一プロセスで複数のアーカイブドライブに対してアーカイブされることがあります。これにより、ユーザーがアーカイブされた録画を検索し、表示する方法には影響を与えません。

ダイナミックアーカイブパスは一般にすべてのカメラに適用されます。個別のカメラ用にダイナミックアーカイブパスを設定することはできません。

アーカイブ選択のダイナミックパスを有効にする	ダイナミックパス選択の使用を有効にし、使用したいパスを選択できるようにします。当初は、選択可能なパスのリストに、ローカルおよびマップ済みドライブの両方のサーバーのすべてのドライブが表示されます。リストの下にある**新規パス**機能で、さらにパスを追加することができます。
使用	ダイナミックアーカイブパスとして使用する特定のパスを選択します。また、以前に手動で追加したパス（以下の**削除**ボタンの説明を参照）を選択して削除することもできます。
ドライブ	たとえば、C:¥ドライブです。
パス	ファイルを保存する場所へのパス。例：C:¥ または ¥¥OurServer¥OurFolder¥OurSubfolder¥
ドライブ容量	ドライブの合計サイズ。
空きスペース	ドライブに残っている未使用の容量。
新規パス	新しいパスを指定し、追加ボタンを使用してリストに追加します。監視システムサーバーでパスに到達できることが必要です。UNC（Universal Naming Convention）形式を使用して指定する必要があります。例：¥¥server¥volume¥directory¥。新しいパスが追加されると、それを選択して、ダイナミックアーカイブパスとして使用することができます。
追加	**新規パス**フィールドで指定したパスを、リストに追加します。
削除	手動で追加した選択済みのパスをリストから削除します。初期状態のリストにあるパスは、選択しても削除できません。

ビデオ録画（プロパティ）

ビデオおよび録画を設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、多くのカメラに対して一定のプロパティを同時に指定することができます。 操作を迅速に行いたい場合や、対象となるプロパティが、個別のカメラではなく、すべてのカメラで共有されている場合が該当します。

録画という言葉はビデオ（該当する場合は、カメラからの音声）の監視システムサーバーのカメラのデータベースへの保存を意味します。ビデオ/音声は、保存する理由がある場合にだけ保存されます。たとえば、モーションが検知されている間、イベントが発生してから、他のイベントが発生するまでの間、または一定の期間内で保存されます。

白い背景のすべてのプロパティは編集可能で、水色の背景のプロパティは編集できません。

また、すべてのビデオ録画プロパティはそれぞれのカメラに対して個別に 『93ページ の"記録"参照 』指定できることに注意してください。

テンプレート	テンプレートを使用すると、類似のプロパティが迅速に設定できて便利です。たとえば、カメラが 20 台あり、録画パス、アーカイブパス、およびそれらすべての保持期間を変更したいとします。3 種類の同じ情報を 20 回入力する代わりに、テンプレートに一度だけ入力し、2 回クリックするだけで、そのテンプレートを 20 台のカメラに適用することができます。
テンプレートを適用	どのカメラにテンプレートを適用するか選択します。2 つの**設定**ボタンのいずれかを使用して、実際にテンプレートに適用します。

カメラ名	Management Application およびクライアントで表示される名前です。既存の名前を、新しい名前で上書きすることができます。名前は一意であり、以下の特殊文字を含むことはできません。 < > & ' " ¥ / : * ?| [ ]
録画オン	カメラからのビデオを録画する条件を以下から選択します。 • **常時 :** カメラが有効で、オンラインになるようにスケジュールされている場合は常に録画します。後者のオプションでは、時間ベースの録画ができます。 • **設定しない** : 録画しません。ライブビデオが表示されますが、ビデオがデータベースに保持されていないため、ユーザーはカメラからビデオを再生できません。 • **モーション検知** : これを選択すると、モーションが検知された時にビデオを録画します。後の録画を追加しなければ、最後のモーションが検知された後すぐに録画が停止します。 • **イベント** : これを選択すると、イベントが発生してから、別のイベントが発生するまでの間、ビデオが録画されます。イベントによる録画を使用するには、そのイベント 『108ページ の"イベントおよび出力の概要"参照 』が定義されていて、開始イベントおよび停止イベントを選択してあることが必要です。他のフィールドの下にあるイベントの設定リストを使用して、必要に応じたイベントを定義します。 • **モーション検知およびイベント** : これを選択すると、モーションを検知した場合、あるいはイベントが発生していから、別のイベントが発生するまでの間、ビデオが録画されます。隣の列で、開始イベントおよび停止イベントを選択することを忘れないでください。
開始イベント	関連する開始イベントを選択します。開始イベントが発生すると（あるいは、プリレコーディングを使用する場合は、それ以前から。下記を参照）録画が開始します。
停止イベント	関連する停止イベントを選択します。停止イベントが発生すると（あるいは、ポストレコーディングを使用する場合は、それより後に。下記を参照）録画が停止します。
プリレコーディング	検出したモーションおよび開始イベントの前の期間からの録画を保存できます。このチェックボックスを選択すると、この機能が有効になります。隣接する列で、必要な秒数を指定します。
秒数【プリレコーディングの】	録画開始条件（モーションまたは開始イベント）が満たされる前から、ビデオを録画する秒数を指定します。通常、プリレコーディングが必要になるのは数秒のみですが、最長で 65,535 秒（18 時間 12 分 15 秒）まで指定できます。ただし、非常に長いプリレコーディング時間を指定すると、プリレコーディング時間がスケジュールされた、あるいはスケジュールされていないアーカイブ 『124ページ の"アーカイブについて"参照 』時間にかかることもあります。アーカイブ中は、プリレコーディングが適切に機能しないため、問題の原因となりかねません。
ポストレコーディング	検出したモーションおよび停止イベントの後の期間の録画を保存できます。このチェックボックスを選択すると、この機能が有効になります。隣接する列で、必要な秒数を指定します。

秒数［ポストレコーディングの］	録画停止条件（モーションまたは停止イベント）が満たされた後で、ビデオを録画する秒数を指定します。通常、ポストレコーディングが必要になるのは数秒のみですが、最長で 65,535 秒（18 時間 12 分 15 秒）まで指定できます。 非常に長いポストレコーディング時間を指定すると、ポストレコーディング時間がスケジュールされた、あるいはスケジュールされていないアーカイブ時間にかかるシナリオで実行されることもあります。アーカイブ中は、ポストレコーディングが適切に機能しないため、問題の原因となりかねません。
カメラ	**開く**ボタンをクリックして、選択したカメラに対して、詳細およびカメラ固有の設定（例：イベント通知、PTZ プリセット位置、魚眼レンズビューエリア）を設定します。
全て選択	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択します。
全てクリアする	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラの選択を解除します。
選択したカメラで、選択したテンプレートの値を設定する	テンプレートから選択した値だけを、選択したカメラに適用します。
選択したカメラですべてのテンプレート値を設定する	テンプレートのすべての値を、選択したカメラに適用します。

カメラで MJPEG コーデックを使用する場合

MJPEG では、通常モードならびにスピードアップモードでフレームレートを指定できます。カメラがデュアルストリーム対応の場合は、これを有効にすることも可能です。

フレームレートを設定できる場所は 3 つあります。

- ライブフレームレート - 通常の録画ストリームで使用します
- ライブフレームレート - モーション検知または類似の機能と一緒に、スピードアップ録画で使用します。

FPS（1 秒当りのフレーム数） - ライブを見るための追加のストリームで使用します。 通常のフレームレートモード：

フレームレート	カメラの映像に必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。
ライブフレームレート	カメラからのライブ映像に必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。 カメラがデュアルストリーム対応で、デュアルストリームが有効になっている場合、ライブフレームレート列は読み取り専用になり、変更できないデュアルストリーミングの値が入ります。
録画フレームレート	カメラの録画ビデオに必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。このフレームレートは、標準モードで指定するフレームレートより高くなければなりません。

スピードアップフレームレートモード：

スピードアップフレームレートを有効にする	スピードアップ機能によって、モーションを検知した場合およびイベントが発生した場合に、通常より高いフレームレートを使用できます。スピードアップを有効にすると、スピードアップの詳細を指定するために、より多くの列が使用可能になります。
フレームレート	カメラのビデオを再生するときのスピードアップフレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。このフレームレートは、標準モードで指定するフレームレートより高くなければなりません。
モーション時	このチェックボックスを選択すると、モーションを検知した時にスピードアップフレームレートを使用します。カメラは最後にモーション検知されてから 2 秒後に、通常のフレームレートに戻ります。
イベント発生時	このチェックボックスを選択すると、イベントが発生してから、別のイベントが発生するまでの間、スピードアップフレームレートを使用します。イベントによるスピードアップをオンするには、そのイベントが定義されていて、付随するリストで開始イベントおよび停止イベントが選択されていることが必要です。 他のフィールドの下にあるイベントの設定リストを使用して、必要に応じたイベントを定義します。
開始イベント	必要な開始イベントを選択します。開始イベントが発生すると、カメラはスピードアップフレームレートの使用を開始します。
停止イベント	必要な停止イベントを選択します。停止イベントが発生すると、カメラは通常のフレームレートに戻ります。
ライブフレームレート	カメラからのライブ映像に必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。このフレームレートは、標準モードで指定するフレームレートより高くなければなりません。 カメラがデュアルストリーム対応で、デュアルストリームが有効になっている場合、ライブフレームレート列は読み取り専用になり、変更できないデュアルストリーミングの値が入ります。
録画フレームレート	カメラの録画ビデオに必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。このフレームレートは、標準モードで指定するフレームレートより高くなければなりません。

モーションまたはイベントに基づいてスピードアップする必要はありません。スケジュール 『133ページ の"スピードアップ"参照 』を使用して、特定の期間に基づいてスピードアップを構成することもできます。特定期間のスピードアップを希望する場合も、**スピードアップの有効化**チェックボックスを選択して、スピードアップの使用を有効にする必要があります。

デュアルストリーム：

ライブストリーム専用で使用する	この追加ストリーム機能で、カメラの別のストリームを使用することができます。この機能は、録画サーバーへの 2 つの独立したストリームを有効にします。1 つのストリームはライブビュー用であり、もう 1 つのストリームは（異なる解像度、エンコーディング、フレームレートでの）録画用です。
ストリーム	ライブストリームのタイプを選択します。ライブビューとビデオ録画では、最適な結果を得るためのストリーム設定が異なることがあります。
解像度	カメラの解像度を選択します。
FPS	カメラの 1 秒当たりのライブフレームレート（FPS）を選択します。

重要：この機能が使用できるのは、デュアルストリームをサポートしているカメラのみです。

カメラが MPEG コーデックを使用する場合

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、製品比較チャート『12ページ 』を参照してください。

MPEG では、フレームレートおよびその他の設定を指定できます。

1 秒当たりのフレームレート	カメラからのライブビューおよび録画ビデオ再生のためのフレームレート。1 秒当たりのフレーム数を選択します。
キーフレームのみの録画	キーフレームでは指定された間隔でカメラのビュー全体のデータを保持しますが、他のフレームは変化したピクセルデータだけを保持します。これにより、MPEG ファイルのサイズを大幅に縮小できます。キーフレームだけを録画したい場合は、チェックボックスを選択します。モーションを検知した場合や、イベントが発生した場合など、例外を指定することができます。
イベントのすべてのフレームの録画	キーフレームのみの録画を選択している場合、例外を作成できます。このチェックボックスを選択すると、イベントが発生してから、別のイベントが発生するまでの間、すべてのフレームを録画します。この機能を使用するには、そのイベントが定義されていて、付随するリストで開始イベントおよび停止イベントが選択されていることが必要です。 他のフィールドの下にあるイベントの設定リストを使用して、必要に応じたイベントを定義します。
開始イベント	**イベントまたはモーション検知、およびイベントで録画する場合に使用します。**関連する開始イベントを選択します。開始イベントが発生すると、カメラはすべてのフレームの録画を開始します。
停止イベント	関連する停止イベントを選択します。停止イベントが発生すると、カメラはキーフレームの録画を停止します。

デュアルストリーム：

ライブストリーム専用で使用する	この追加ストリーム機能で、カメラの別のストリームを使用することができます。この機能は、録画サーバーへの 2 つの独立したストリームを有効にします。1 つのストリームはライブビュー用であり、もう 1 つのストリームは（異なる解像度、エンコーディング、フレームレートでの）録画用です。
ストリーム	ライブストリームのタイプを選択します。ライブビューとビデオ録画では、最適な結果を得るためのストリーム設定が異なることがあります。
解像度	カメラの解像度を選択します。
FPS	カメラの 1 秒当たりのライブフレームレート（FPS）を選択します。

重要：この機能が使用できるのは、デュアルストリームをサポートしているカメラのみです。

手動録画

ビデオおよび録画を設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、多くのカメラに対して一定のプロパティを同時に指定することができます。 手動録画の設定では、プロパティがすべてのカメラによって共有されます。

手動録画が有効であれば、必要な権限を持つ XProtect Smart Client ユーザーは、録画中ではないカメラのライブビデオの表示中に、何か関心の対象が見えた場合、手動で録画を開始できます。必ず固定の時間（たとえば 5 分）で、ユーザー主導の録画を行います。

手動録画の有効化	チェックボックスを選択して手動録画を有効にし、詳細を指定します。
手動録画のデフォルト継続時間	ユーザーによる録画を実行する期間（秒単位）。デフォルトの期間は 300 秒で、5 分に相当します。
手動録画の最長継続時間	ユーザーによる録画が可能な最長時間。こうした手動録画は必ず決まった時間で行われるため、この最長時間は、XProtect Smart Client で開始される手動録画とは関係ありません。 ただし、インストールによっては API または類似の機能でこれらをシステムと統合する場合に、手動録画をサードパーティのアプリケーションと組み合わせることもできます。このような状況では、最長時間の指定が関連します。 単に手動録画を XProtect Smart Client とだけ同時に使用する場合、このプロパティは無視してください。

個々のカメラの録画 『93ページ の"記録"参照 』が**録画しない**や**条件付きで録画**に設定されていても、有効であれば手動録画を行うことができます。

フレームレート - MJPEG

ビデオおよび録画を設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、多くのカメラに対して一定のプロパティを同時に指定することができます。 操作を迅速に行いたい場合や、対象となるプロパティが、個別のカメラではなく、すべてのカメラで共有されている場合が該当します。

白い背景のすべてのプロパティは編集可能で、水色の背景のプロパティは編集できません。 すべてのフレームレート - MJPEG プロパティは、MJPEG を使用するそれぞれのカメラに対して個別に 『93ページ の"記録"参照 』指定できることに注意してください。

テンプレートおよび共通プロパティ

名前	詳細
テンプレート	テンプレートを使用すると、類似のプロパティが迅速に設定できて便利です。たとえば、カメラが 20 台あり、録画パス、アーカイブパス、およびそれらすべての保持期間を変更したいとします。3 種類の同じ情報を 20 回入力する代わりに、テンプレートに一度だけ入力し、2 回クリックするだけで、そのテンプレートを 20 台のカメラに適用することができます。
テンプレートを適用	どのカメラにテンプレートを適用するか選択します。2 つの**設定**ボタンのいずれかを使用して、実際にテンプレートに適用します。
全て選択	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択します。
全てクリアする	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラの選択を解除します。
選択したカメラで、選択したテンプレートの値を設定する	テンプレートから選択した値だけを、選択したカメラに適用します。
選択したカメラですべてのテンプレート値を設定する	テンプレートのすべての値を、選択したカメラに適用します。
カメラ名	Management Application およびクライアントで表示される名前です。既存の名前を、新しい名前で上書きすることができます。名前は一意であり、以下の特殊文字を含むことはできません。 < > & ' " ¥ / : * ?| [ ]

通常のフレームレートのプロパティ

以下のフレームレートプロパティを指定します。

フレームレート	カメラの映像に必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。
時間単位	ライブおよび録画のフレームレートに必要な単位（秒、分、時間あたり）を選択します。フレームレートをスピードアップできる時間のみを選択できることに注意してください。例：標準モードで、**秒**あたり 15 フレームを指定したとすると、スピードアップモードで**分**または**時間**あたり 16 フレームを指定することはできません。

カメラ	**開く**ボタンをクリックして、選択したカメラに対して、詳細およびカメラ固有の設定（例：イベント通知、PTZ プリセット位置、魚眼レンズビューエリア）を設定します。
ライブフレームレート	カメラからのライブ映像に必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。 カメラがデュアルストリームをサポートし、デュアルストリームを有効にした場合、ライブフレームレート列はデュアルストリーム値で読み取り専用です。これは変更できません。
録画フレームレート	カメラの録画ビデオに必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。このフレームレートは、標準モードで指定するフレームレートより高くなければなりません。

スピードアップフレームレートのプロパティ

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。詳細については、製品比較チャート『12ページ 』を参照してください。

名前	詳細
スピードアップを有効にする	スピードアップ機能によって、モーションを検知した場合およびイベントが発生した場合に、通常より高いフレームレートを使用できます。スピードアップを有効にすると、スピードアップの詳細を指定するために、より多くの列が使用可能になります。
フレームレート	カメラのビデオを再生するときのスピードアップフレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。 このフレームレートは、標準モードで指定するフレームレートより高くなければなりません。
時間単位	ライブおよび録画のフレームレートに必要な単位（秒、分、時間あたり）を選択します。 フレームレートをスピードアップできる時間のみを選択できることに注意してください。 例：標準モードで、**秒**あたり 15 フレームを指定したとすると、スピードアップモードで**分**または**時間**あたり 16 フレームを指定することはできません。

名前	詳細
スピードアップ　をオン	• **モーション検知：** これを選択すると、モーション 『98ページ の"モーション検知&と領域の除外"参照 』が検知された時にスピードアップします。最後のモーションが検知されると、通常のフレームレートを使用します。 • **イベント：**これを選択すると、イベントが発生してから、別のイベントが発生するまでの間、スピードアップします。イベントを定義した場合、および隣接する列で開始および停止イベントを選択した場合のみスピードアップを使用できます。 他のフィールドの下にあるイベントの設定リストを使用して、必要に応じたイベントを定義します。 • **モーション検知およびイベント：** このオプションを選択すると、モーションを検知した場合、あるいはイベントが発生してから別のイベントが発生するまでの間、スピードアップします。隣の列で、開始イベントおよび停止イベントを選択することを忘れないでください。
スケジュールのみ	このオプションを選択すると、カメラのスピードアップをスケジュール 『133ページ の"スピードアップ"参照 』のみに従ってスピードアップします。
開始イベント	関連する開始イベントを選択します。開始イベントが発生すると、カメラはスピードアップフレームレートの使用を開始します。
停止イベント	関連する開始イベントを選択します。停止イベントが発生すると、カメラは通常のフレームレートに戻ります。
カメラ	**開く**ボタンをクリックして、選択したカメラに対して、詳細およびカメラ固有の設定（例：イベント通知、PTZ プリセット位置、魚眼レンズビューエリア）を設定します。
ライブフレームレート	カメラからのライブ映像に必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。このフレームレートは、標準モードで指定するフレームレートより高くなければなりません。 カメラがデュアルストリームをサポートし、デュアルストリームを有効にした場合、**ライブフレームレート**列はデュアルストリーム値で読み取り専用です。これは変更できません。
録画フレームレート	カメラからの録画ビデオに必要な平均フレームレート。 フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。

フレームレート - MPEG

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、製品比較チャート 『12ページ 』を参照してください。

ビデオおよび録画を設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、多くのカメラに対して一定のプロパティを同時に指定することができます。 操作を迅速に行いたい場合や、対象となるプロパティが、個別のカメラではなく、すべてのカメラで共有されている場合が該当します。

すべてのフレームレート H.264/MPEG4 プロパティは、H.264/MPEG4 を使用するそれぞれのカメラに対して個別に 『93ページ の"記録"参照 』指定できます。

テンプレート	テンプレートを使用すると、類似のプロパティが迅速に設定できて便利です。たとえば、カメラが 20 台あり、録画パス、アーカイブパス、およびそれらすべての保持期間を変更したいとします。3 種類の同じ情報を 20 回入力する代わりに、テンプレートに一度だけ入力し、2 回クリックするだけで、そのテンプレートを 20 台のカメラに適用することができます。
テンプレートを適用	どのカメラにテンプレートを適用するか選択します。2 つの**設定**ボタンのいずれかを使用して、実際にテンプレートに適用します。
カメラ名	Management Application およびクライアントで表示される名前です。既存の名前を、新しい名前で上書きすることができます。名前は一意であり、以下の特殊文字を含むことはできません。 < > & ' " ¥ / : * ?| [ ]
デュアルストリーム	カメラでデュアルストリームが有効かどうかをチェックできます。この情報は読み取り専用であることに注意してください。デュアルストリームをサポートしているカメラの場合、個々のカメラのビデオ 『90ページ 』プロパティでこれを有効/無効にできます。
ライブ FPS	カメラの 1 秒当たりのライブフレームレート（FPS）を選択します。
カメラ	**開く**ボタンをクリックして、選択したカメラに対して、詳細およびカメラ固有の設定（例：イベント通知、PTZ プリセット位置、魚眼レンズビューエリア）を設定します。
全て選択	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択します。
全てクリアする	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択解除します。
選択したカメラで、選択したテンプレートの値を設定する	テンプレートから選択した値だけを、選択したカメラに適用します。
選択したカメラですべてのテンプレート値を設定する	テンプレートのすべての値を、選択したカメラに適用します。
キーフレームのみの録画	キーフレームでは指定された間隔でカメラのビュー全体のデータを保持しますが、他のフレームは変化したピクセルデータのみを記録します。これにより、MPEG ファイルのサイズを大幅に低減できます。キーフレームだけを録画したい場合は、チェックボックスを選択します。

すべてのフレームの　録画	キーフレームのみの録画を選択している場合、例外を作成できます。 • **モーション検知**：これを選択すると、モーションが検知された時のフレームをすべて録画します。最後にモーション 『98ページ の"モーション検知&と領域の除外"参照 』が検知されてから 2 秒後に、カメラはキーフレームのみの録画に戻ります。 • **イベント**：これを選択すると、イベントが発生してから別のイベントが発生するまでの間、すべてのフレームを録画します。そのイベント 『108ページ の"イベントおよび出力の概要"参照 』が定義されており、隣接する列で開始イベントおよび停止イベントを選択してあることが必要です。 他のフィールドの下にあるイベントの設定リストを使用して、必要に応じたイベントを定義します。 • **モーション検知およびイベント**：これを選択すると、モーションを検知した場合、あるいはイベントが発生してから別のイベントが発生するまでの間、すべてのフレームを録画します。隣の列で、開始イベントおよび停止イベントを選択することを忘れないでください。 • **スケジュールのみ**：これを選択すると、カメラのスケジュールをスピードアップ 『133ページ の"スピードアップ"参照 』にのみ従ってすべてのフレームを録画します。
開始イベント	**イベントまたはモーション検知、およびイベントで録画する場合に使用します。**関連する開始イベントを選択します。開始イベントが発生すると、カメラはすべてのフレームの録画を開始します。
停止イベント	関連する停止イベントを選択します。停止イベントが発生すると、カメラはキーフレームの録画のみ停止します。

音声の録音

特定のカメラに対してビデオや録画を設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、音声を録音するタイミングを指定できます。この選択は、システムのすべてのカメラに適用されます。

常時録音	すべての該当するカメラで、音声を常に録音します。
設定しない	どのカメラでも音声を録音しません。音声をまったく録音していなくても、XProtect Smart Client からのライブ音声を聴くことができます。

音声録音とビデオ保存容量

音声を録音する場合、音声録音がビデオ保存容量に影響することを覚えておくことが重要です。

音声は、関連するカメラのデータベースに録音されます。ビデオだけを録画する場合に比べて、音声とビデオを記録する場合、より早くデータベースが満杯になります。データベースが満杯になると、システムは自動的にデータをアーカイブ 『124ページ の"アーカイブについて"参照 』するので、データベースが満杯になること自体は問題ではありません。ただし、音声を録音する場合、追加のアーカイブ容量が必要になります。

- 例：MPEG4 を使用する場合、それぞれ 1 秒のビデオ GOP（Group Of Pictures）が、データベースの 1 レコードに保存されます。毎秒ごとの音声も、データベースの 1 レコードに保存されます。データベースのレコードの半分は音声の保存に使用されるので、データベースのビデオ保存容量が全体

容量の半分に低減します。したがってデータベースはすぐに満杯になり、ビデオだけを録画する場合と比べて、より頻繁にアーカイブが発生します。

- 例:MJPEG を使用する場合、音声ブロックのサイズが JPEG 間の時間を超えない限り、すべての JPEG に対して音声が 1 レコードに保存されます。極端な場合は、データベースのレコードの半分が音声の保存で使用されるので、データベースのビデオ保存容量が全体容量の半分に低減します。非常に高いフレームレートを使用すると、各 JPEG 間の時間が短くなることを意味するので、音声の録音に使用するデータベースの割合が小さくなり、その結果ビデオの保存で使用できる部分は大きくなります。その結果として、データベースはすぐに満杯になり、ビデオだけを録画する場合と比べて、より頻繁にアーカイブが発生します。

上記では、単純化した例を示しています。正確な使用可能な保存容量は、GOP/JPEG および音声のキロバイト単位でのサイズにも依存します。

音声選択（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。詳細については、製品比較チャート『12ページ 』を参照してください。

ビデオおよび録画を設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、多くのカメラに対して一定のプロパティを同時に指定することができます。 操作を迅速に行いたい場合や、対象となるプロパティが、個別のカメラではなく、すべてのカメラで共有されている場合が該当します。 カメラからのビデオを再生する時は、カメラに対してデフォルトのマイクおよび/またはスピーカーからの音声が自動的に使用されます。それぞれのカメラに対して、すべてのプロパティを個別に指定することも可能であることに注意してください。

テンプレート	テンプレートを使用すると、類似のプロパティが迅速に設定できて便利です。たとえば、カメラが 20 台あり、録画パス、アーカイブパス、およびそれらすべての保持期間を変更したいとします。3 種類の同じ情報を 20 回入力する代わりに、テンプレートに一度だけ入力し、2 回クリックするだけで、そのテンプレートを 20 台のカメラに適用することができます。
テンプレートを適用	どのカメラにテンプレートを適用するか選択します。2 つの**設定**ボタンのいずれかを使用して、実際にテンプレートに適用します。
カメラ名	Management Application およびクライアントで表示される名前です。既存の名前を、新しい名前で上書きすることができます。名前は一意であり、以下の特殊文字を含むことはできません。 < > & ' " ¥ / : * ?| [ ]
デフォルトのマイク	デフォルトのマイクを選択します。
カメラ	**開く**ボタンをクリックして、選択したカメラに対して、詳細およびカメラ固有の設定（例：イベント通知、PTZ プリセット位置、魚眼レンズビューエリア）を設定します。
全て選択	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択します。
全てクリアする	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択解除します。
選択したカメラで、選択したテンプレートの値を設定する	テンプレートから選択した値だけを、選択したカメラに適用します。
選択したカメラですべてのテンプレート値を設定する	テンプレートのすべての値を、選択したカメラに適用します。
デフォルトのスピーカー	デフォルトのスピーカーを選択します。

ストレージ情報

ストレージ情報プロパティには、システムにどれだけのストレージ容量があり、そのうちのどの程度を使用できるかが示されます。ディスク容量を円グラフ形式で迅速に表示するには、対象となるドライブを表している行を選択します。

名前	詳細
ドライブ	対象となるトライブを表す文字、たとえばC:など。
パス	ファイルを保存する場所へのパス。例：C:¥ または ¥¥OurServer¥OurFolder¥OurSubfolder¥
使用	たとえば、録画やアーカイブで使用するストレージエリア。
ドライブ容量	ドライブの合計サイズ。
ビデオデータ	ドライブにあるビデオデータの量。
その他のデータ	ドライブにあるその他のデータの量。
空きスペース	ドライブに残っている未使用の容量。

カメラプロパティ

一般

特定のカメラについてビデオおよびレコーディングの設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、以下のプロパティが含まれます。

有効	カメラはデフォルトで有効になっています。つまり、オンラインになるようスケジュールされており 『132ページ の"オンライン期間"参照 』、ビデオをシステムに転送できます。個別のカメラを無効にすることができます。この場合、カメラからシステムへビデオ/音声は転送されません。
プレビュー	このチェックボックスを選択すると、カメラのビデオのプレビューが表示されます。チェックボックスを選択解除すると、システムはカメラのプレビューを表示しません。
カメラ名	Management Application およびクライアントで表示される名前です。既存の名前を、新しい名前で上書きすることができます。 名前は一意であり、以下の特殊文字を含むことはできません。 **< > & ' " ¥ / : * ? | [ ]**

カメラのショートカット番号	XProtect Smart Client のユーザーは、キーボードショートカットを活用できます。一例として、複数のカメラの再生を切り替えることができます。こうしたショートカットには数字も含まれており、各カメラを識別するために使用します。 ショートカット番号は、それぞれのカメラで一意でなければなりません。カメラのショートカット番号には、文字または特殊文字を含んではならず、最大で 8 桁以内になるようにしてください。正しいカメラのショートカット番号の例：3, 12345678. 正しくないカメラのショートカット番号の例：Cam#3、123456789。 キーボードショートカットの使用方法に関する詳細情報は、XProtect Smart Client の他のマニュアルにあります。

これらのプロパティは、大半がカメラに固有です。こうしたプロパティはカメラによって大きく異なるため、以下の説明はあくまでもガイダンス目的です。選択したカメラにアクセスできると、ライブプレビューが表示されます。**カメラ設定中...**ボタンをクリックすると、選択したカメラのプロパティを表示する別個のウィンドウが開きます。

通常、ビデオプロパティでは、選択した新しい値で既存の値を上書きすることで、帯域、輝度、圧縮、コントラスト、解像度、回転などをコントロールできます。ビデオの設定を調整する場合、大半のカメラでは、その設定の効果をフィールドの下の画像でプレビューすることができます。

ビデオ設定機能に、**日時を含む**設定がある場合があります。**はい**に設定すると、カメラからの日付と時刻がビデオに含まれます。ただし、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や電源などで機能しています。したがって、カメラの時刻とシステムの時刻が完全に対応していないことがあり、これが混乱につながることがあります。受信したすべてのフレームにシステムがタイムスタンプを付けるため、それぞれの画像の正確な日付と時刻は既に分かっていることから、**いいえ**に設定することを推奨しています。

カメラが時刻同期機能をサポートしている場合、一貫性のある時刻の同期のために、カメラとシステムの時刻をタイムサーバーで自動同期することができます。

ビデオ

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、製品比較チャート『12ページ 』を参照してください。

特定のカメラについてビデオおよび録画の設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、MJPEG コーデックまたは MPEG コーデックのいずれかを使用することができます。2 つのオプションのいずれかを選択するかによって、カメラに対して異なるオプションを設定できます。

MJPEG コーデック

MJPEG では、通常モードならびにスピードアップモードでフレームレートを指定できます。カメラがデュアルストリーム対応の場合は、これを有効にすることも可能です。フレームレートを設定できる場所は 3 つあります。

- ライブフレームレート - 通常の録画ストリームで使用します
- ライブフレームレート - モーション検知または類似の機能と一緒に、スピードアップ録画で使用します。

FPS（1 秒当りのフレーム数） - ライブを見るための追加のストリームで使用します。 通常のフレームレートモード

フレームレート	カメラの映像に必要な平均フレームレート。 フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。
ライブフレームレート	カメラからのライブ映像に必要な平均フレームレート。 フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。 カメラがデュアルストリームをサポートし、デュアルストリームを有効にした場合、**ライブフレームレート**列はデュアルストリーム値で読み取り専用です。これは変更できません。
録画フレームレート	カメラの録画ビデオに必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。 このフレームレートは、標準モードで指定するフレームレートより高くなければなりません。

スピードアップフレームレートモード

スピードアップフレームレートを有効にする	スピードアップ機能によって、モーションを検知した場合およびイベントが発生した場合に、通常より高いフレームレートを使用できます。スピードアップを有効にすると、スピードアップの詳細を指定するために、より多くの列が使用可能になります。
フレームレート	カメラのビデオを再生するときのスピードアップフレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。 このフレームレートは、標準モードで指定するフレームレートより高くなければなりません。
モーション時	このチェックボックスを選択すると、モーションを検知した時にスピードアップフレームレートを使用します。カメラは最後にモーション検知されてから 2 秒後に、通常のフレームレートに戻ります。
イベント発生時	このチェックボックスを選択すると、イベントが発生してから、別のイベントが発生するまでの間、スピードアップフレームレートを使用します。イベントによるスピードアップをオンするには、そのイベントが定義されていて、付随するリストで開始イベントおよび停止イベントが選択されていることが必要です。
開始イベント	関連する開始イベントを選択します。 開始イベントが発生すると、カメラはスピードアップフレームレートの使用を開始します。
停止イベント	関連する停止イベントを選択します。 停止イベントが発生すると、カメラは通常のフレームレートに戻ります。
ライブフレームレート	カメラからのライブ映像に必要な平均フレームレート。 フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。 このフレームレートは、標準モードで指定するフレームレートより高くなければなりません。 カメラがデュアルストリームをサポートし、デュアルストリームを有効にした場合、**ライブフレームレート**列はデュアルストリーム値で読み取り専用です。これは変更できません。
録画フレームレート	カメラの録画ビデオに必要な平均フレームレート。フレーム数を選択してから、時間間隔の単位（秒、分、時間）を選択します。 このフレームレートは、標準モードで指定するフレームレートより高くなければなりません。

スピードアップは、モーションやイベントに関連付ける必要はありません。スケジュールを使用して、特定の期間にスピードアップを設定することもできます。特定期間のスピードアップを希望する場合も、**スピードアップの有効化**チェックボックスを選択して、スピードアップの使用を有効にする必要があります。

デュアルストリーム

ライブストリーム専用で使用する	この追加ストリーム機能で、カメラの別のストリームを使用することができます。この機能は、録画サーバーへの 2 つの独立したストリームを有効にします。1 つのストリームはライブビュー用であり、もう 1 つのストリームは（異なる解像度、エンコーディング、フレームレートでの）録画用です。
ストリーム	ライブストリームのタイプを選択します。ライブビューとビデオ録画では、最適な結果を得るためのストリーム設定が異なることがあります。
解像度	カメラの解像度を選択します。
FPS	カメラの 1 秒当たりのライブフレームレート（FPS）を選択します。

MPEG コーデック

フレームレート

1 秒当たりのフレームレート	カメラからのライブビューおよび録画ビデオ再生のためのフレームレート。1 秒当たりのフレーム数を選択します。
キーフレームのみの録画	キーフレームでは指定された間隔でカメラのビュー全体のデータを保持しますが、他のフレームは変化したピクセルデータだけを保持します。これにより、MPEG ファイルのサイズを大幅に縮小できます。キーフレームだけを録画したい場合は、チェックボックスを選択します。モーションを検知した場合や、イベントが発生した場合など、例外を指定することができます。
モーションのすべてのフレームの録画	キーフレームのみの録画を選択している場合、例外を作成できます。 このチェックボックスを選択すると、モーションが検知された時のフレームをすべて録画します。最後にモーションが**検知**されてから 2 秒後に、カメラはキーフレームのみの録画に戻ります。
イベントのすべてのフレームの録画	キーフレームのみの録画を選択している場合、例外を作成できます。 このチェックボックスを選択すると、イベントが発生してから、別のイベントが発生するまでの間、すべてのフレームを録画します。この機能を使用するには、そのイベントが定義されていて、付随するリストで開始イベントおよび停止イベントが選択されていることが必要です。
開始イベント	**イベントまたはモーション検知、およびイベントで録画する場合に使用します。** 関連する開始イベントを選択します。 開始イベントが発生すると、カメラはすべてのフレームの録画を開始します。
停止イベント	関連する停止イベントを選択します。 停止イベントが発生すると、カメラはキーフレームのみを録画します。

デュアルストリーム

ライブストリーム専用で使用する	この追加ストリーム機能で、カメラの別のストリームを使用することができます。この機能は、録画サーバーへの 2 つの独立したストリームを有効にします。1 つのストリームはライブビュー用であり、もう 1 つのストリームは（異なる解像度、エンコーディング、フレームレートでの）録画用です。
ストリーム	ライブストリームのタイプを選択します。ライブビューとビデオ録画では、最適な結果を得るためのストリーム設定が異なることがあります。
解像度	カメラの解像度を選択します。
FPS	カメラの 1 秒当たりのライブフレームレート（FPS）を選択します。

音声（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。詳細については、製品比較チャート『12ページ 』を参照してください。

特定のカメラについてビデオおよび録画の設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、そのカメラのデフォルトのマイクおよび/またはスピーカーの選択がプロパティに含まれています。カメラからのビデオを再生する時は、カメラに対してデフォルトのマイクおよび/またはスピーカーからの音声が自動的に使用されます。

マイクまたはスピーカーがカメラと同じハードウェアデバイスに取り付けられている場合、特に設定していなければ、そのマイク/スピーカーがカメラのデフォルトのマイク/スピーカーになります。

デフォルトのマイク	デフォルトのマイクを選択します。
デフォルトのスピーカー	デフォルトのスピーカーを選択します。

カメラに対してデフォルトのマイクやスピーカーを選択できるのは、監視システムのハードウェアデバイスに少なくとも 1 つのマイクおよび/またはスピーカーが取り付けられている場合だけです。

記録

録画という言葉はビデオ（該当する場合は、カメラからの音声）の監視システムサーバーのカメラのデータベースへの保存を意味します。

ビデオ/音声は、保存する理由がある場合にだけ保存されます。たとえば、モーションが検知されている間、イベントが発生してから、他のイベントが発生するまでの間、または一定の期間内で保存されます。

特定のカメラについてビデオおよびレコーディングの設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、以下のレコーディングプロパティが含まれます。

常時録音	カメラが有効 『89ページ の"一般"参照 』で、オンラインになるようにスケジュール 『132ページ の"オンライン期間"参照 』されている場合は常に録画します。後者のオプションでは、時間ベースの録画ができます。
設定しない	録画しません。ライブビデオが表示されますが、ビデオがデータベースに保持されていないため、ユーザーはカメラからビデオを再生できません。

条件	一定の条件を満たした場合に録画します。このオプションを選択する場合、モーションの検知や指定したイベントの前後の期間の録画を保存できるように、必要な条件（以下を参照）を指定します。 例：ドアが開いている間、ビデオを保存するように定義した場合、ドアを開ける直前に発生した状況を確認できることが重要になる場合があります。たとえば、**ドアが開いています**と呼ばれる開始イベントと、**ドアが閉じています**と呼ばれる終了イベントで、イベントによる条件付きでビデオを保存するとします。プリレコーディングが 3 秒の場合、**ドアが開いています**が発生する 3 秒前から、**ドアが閉じています**が発生するまでの期間、ビデオが録画されます。
組み込みモーション検知	このチェックボックスを選択すると、モーション 『98ページ の"モーション検知&と領域の除外"参照 』が検知されたビデオを録画します。ポストレコーディング（以下を参照）を使用しない限り、最後にモーションが検知された後、録画はただちに停止します。
イベント発生時	このチェックボックスを選択すると、イベントが発生してから別のイベントが発生するまでの間、ビデオが録画されます。イベントによる録画を使用するには、そのイベント 『108ページ の"イベントおよび出力の概要"参照 』が定義されていて、付随するリストで開始イベントおよび終了イベントが選択されていることが必要です。 他のフィールドの下にあるイベントの**設定**リストを使用して、必要に応じたイベントを定義します。
開始イベント	関連する開始イベントを選択します。 開始イベントが発生すると（あるいは、プリレコーディングを使用する場合は、それ以前から）録画が開始します。以下を参照してください。
終了イベント	関連する停止イベントを選択します。 終了イベントが発生すると（あるいは、ポストレコーディングを使用する場合は、それより後に）録画が停止します。以下を参照してください。
プリレコーディングの有効化	オプション**条件付き**が選択されている場合だけ使用可能です。 録画開始条件（モーションまたは開始イベント）が満たされる前から、ビデオを録画する秒数を指定します。
ポストレコーディングの有効化	オプション**条件付き**が選択されている場合だけ使用可能です。 録画停止条件（モーション終了または終了イベント）が満たされた後で、ビデオを録画する秒数を指定します。

手動レコーディング 『82ページ の"手動録画"参照 』が有効である可能性があります。手動レコーディングは、必要な権限を持つ XProtect Smart Client ユーザーが、録画中ではないカメラからのライブビデオの表示中に、何か関心の対象が見えた場合、手動で録画を開始できます。有効であれば、個々のカメラの録画が**録画しない**設定や**条件付き録画**に設定されていても、手動レコーディングを行うことができます。

録画およびアーカイブパス

特定のカメラについてビデオおよび録画の設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、以下のプロパティが含まれます。

録画パス	カメラのデータベースを保存するフォルダへのパス。デフォルトフォルダは C:¥MediaDatabase です。他のフォルダを参照する場合は、該当するセルの横にあるアイコンをクリックしてください。指定できるのは、**ローカル**ドライブにあるフォルダへのパスのみです。ネットワークドライブへのパスを指定することはできません。ネットワークドライブを使用している場合、ネットワークドライブが使用不能になると、録画は保存できません。 録画パスを変更し、元の場所に既存の録画がある場合、録画を新しい場所に移動するか（推奨）、元の場所に残すか、削除するかを選択するよう確認されます。 複数のカメラがあり、複数のローカルドライブが使用可能な場合、個別のカメラのデータベースを複数のドライブに分散させることでパフォーマンスを改善できます。
データベースの削除	ボタンをクリックすると、カメラのデータベースにあるすべての録画を削除します。アーカイブされている録画は影響を受けません。 **重要：** 慎重に使用してください。カメラのデータベースにあるすべての録画が完全に削除されます。安全のため、データベースを削除するかを確認する必要があります。
アーカイブ パス	カメラのアーカイブされた録画を保存するフォルダへのパス。デフォルトフォルダは C:¥MediaDatabase です。アーカイブの動的パスを使用しない場合のみ、これを編集できます。 他のフォルダを参照する場合は、関連するセルの横にあるアイコンをクリックしてください。アーカイブ パスを変更し、古い場所に既存のアーカイブされた録画がある場合、アーカイブされた録画を新しい場所へ移動するか、古い場所に残すか、あるいは削除するかを選択する必要があります。Milestone はアーカイブ録画を新しい場所に移動することをお勧めします。 アーカイブされた録画を移動すると、システムは現在カメラのデータベースにあるものもアーカイブすることに注意してください。そのため、アーカイブされた録画を移動した直後に、カメラのデータベースは空になります。
アーカイブの削除	ボタンをクリックすると、カメラのアーカイブされた録画がすべて削除されます。カメラの通常のデータベースにある録画は影響を受けません。単一のアーカイブパスを使用しているか、ダイナミックアーカイブパスを使用しているかに関わらず、削除機能を使用できます。 **重要：** 慎重に使用してください。カメラのすべてのアーカイブ録画が完全に削除されます。安全のため、アーカイブを削除するかを確認する必要があります。
保持期間	カメラからの録画（つまり、カメラのデータベースにある録画ならびにアーカイブされている録画）を保持しておく合計時間です。デフォルトの保持期間は 7 日間です。 保持期間は、録画を保持しておく**合計**時間です。以前のバージョンの監視システムでは、データベースとアーカイブで別個に制限時間を指定していました。

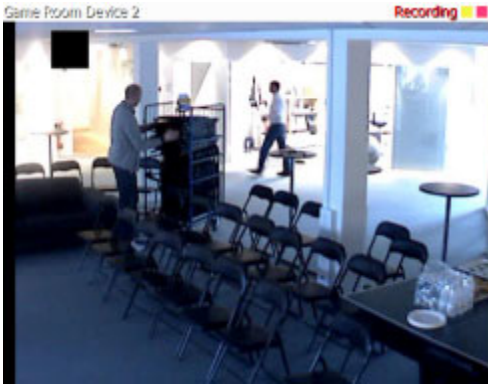
データベース修復アクション	データベースが破損した場合に、どのアクションを行うか選択します。 • **修復。不可能な場合はスキャンし、消去します**：デフォルトのアクションです。データベースが破損した場合、以下の 2 つの異なる修復方法を試みます。高速修復および徹底的な修復。両方の修復方法が失敗した場合は、データベースの内容を削除します。 • **修復。不可能な場合は消去します**：データベースが破損した場合、高速修復を試みます。高速修復が失敗した場合は、データベースの内容を削除します。 • **修復。失敗した場合はアーカイブ**：データベースが破損した場合、高速修復を試みます。高速修復が失敗した場合は、データベースの内容をアーカイブします。 • **削除（修復せず）**：データベースが破損した場合は、データベースの内容を削除します。 • **アーカイブ（修復せず）**：データベースが破損した場合は、データベースの内容をアーカイブします。 • **スキャン。失敗した場合はアーカイブ**:データベースが破損した場合は、データベースのすべてのファイルのエラーがスキャンされ、データベースの完全修復が試行されます。このアクションが完了するには、他の修復アクションよりも時間がかかりますが、データベースのすべてのコンテンツの復元が確実に実行されます。 破損したデータベースを修復するアクションを選択した場合、修復中は破損したデータベースが閉じます。代わりに、新しいデータベースが作成され、録画を続行できます。 XProtect Smart Client では、アーカイブされている場合、破損したデータベースを修復できるケースが大半です。破損したデータベースを XProtect Smart Client で開くと、XProtect Smart Client は、可能な限り、自動的にデータベースを修復しようと試みます。
ダイナミックパスを設定する	ダイナミックアーカイブパスでは、通常は複数のドライブに渡る、異なるアーカイブパスを指定します。ダイナミックアーカイブ用に選択したパスにカメラのデータベースを保存しているドライブが含まれている場合、システムは常にまずそのパスでアーカイブしようと試みます。そうでない場合、そのドライブを使用するカメラデータベースが存在しない限り、システムは自動的にその時点で最も使用可能な容量が大きいアーカイブドライブにアーカイブします。 ダイナミックパスの選択 『76ページ の"ダイナミックパスの選択（プロパティ）"参照 』も参照してください。

イベント通知

特定のカメラについてビデオおよびレコーディングの設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、以下のイベント通知プロパティが含まれます。イベント通知は、XProtect Smart Client のユーザーに、システムでイベントが発生したことを知らせます。イベントが発生したことを迅速に検知できるので、クライアントユーザーにとってイベント通知は重要です。それぞれのカメラに対してイベント通知を個別に設定していたとしても、イベントが手動であるかジェネリックであるか、あるいはイベントがカメラ以外のハードウェアデバイスで発生するかに関わらず、すべてのイベントをシステムで選択することができます。

XProtect Smart Client では、イベント通知は黄色のインジケータ■で表示され、関連するイベントが発生した時に点灯します。また、XProtect Smart Client 自体で、イベント通知にオプションのサウンドを追加することもできます。

XProtect Smart Client のそれぞれのカメラに対して、3 種類のインジケータを使用できます。



- 黄色の■イベントインジケータ。関連するイベントが発生した時に点灯します。
- 赤色の■モーションインジケータ。モーションを検知すると点灯します。
- オプションで緑色の■ビデオインジケータ。カメラからビデオを受信すると点灯します。

XProtect Smart Client で、インジケータが表示されるバーをオフにすることができます。XProtect Smart Client がイベント通知を必要とする場合は、オフにしないでください。

必要なイベントの選択

1. **使用可能なイベント**リストで、関連するイベントを選択します。一度に選択できるイベントは 1 つだけです。
2. **>>**ボタンをクリックして、選択したイベントを**選択したイベント**リストにコピーします。
3. 必要なイベントについて繰り返します。

後で、**選択したイベント**リストからイベントを削除したくなった場合は、関連するイベントを選択して、**<<**ボタンをクリックします。

出力

特定のカメラについてビデオおよびレコーディングの設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、たとえばサイレンのサウンドや照明のスイッチなどの特定のハードウェア出力 『111ページ の"ハードウェア出力の追加"参照 』とカメラを関連付けることができます。

カメラからのビデオでモーションが検知された場合、あるいは、必要な権限 『161ページ の"ユーザーおよびグループの権限の設定"参照 』を持つ XProtect Smart Client ユーザーがカメラからのライブビデオを再生する場合などに、関連付けられた出力を起動することができます。

1. **使用可能な出力**リストで、関連する出力を選択します。一度に選択できる出力は 1 つだけです。まだ適切な出力を定義していない場合、以下の方法で迅速に行うことができます。他のフィールドの下にある**出力の設定**ボタンを使用します。
2. **>>**をクリックして、選択した出力を以下にコピーします。

   手動制御によるリスト。この場合、出力は XProtect Smart Client での手動起動で使用できます。および/または

   - **モーション検知による**リスト。この場合、カメラからのビデオでモーションを検知した場合に出力が起動されます。該当する場合、両方のリストに同じ出力を表示することもできます。
3. 必要な出力について繰り返します。

後で、いずれかのリストから出力を削除したくなった場合は、該当する出力を選択して、**<<**ボタンをクリックします。

モーション検知&と領域の除外

特定のカメラについてビデオおよび録画の設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、モーション検知を調整することが重要になります。これは、いつ録画するか、いつ E メール通知をするか、いつハードウェア出力（照明やサイレンなど）を有効にするかなどを決定するためです。それぞれのカメラに最適なモーション検知が得られるように調整しておくことで、不必要な録画や通知などを避けることができます。カメラの配置によっては、異なる物理的条件（昼/夜、強風/無風など）でモーション検知をテストすることを強くお勧めします。

カメラのモーション検知を設定する前に、圧縮、解像度などのカメラのビデオプロパティ 『89ページ の"一般"参照 』を設定する必要があります。

複数の同時ビデオストリーム出力に対応しないカメラは､監視サーバーと Management Application に同時に接続することはできません。Milestone では、そうしたデバイスでモーション検知や PTZ を設定する場合、Recording Server サービスを停止 『168ページ の"サービスを開始および停止する"参照 』することを推奨しています。

Management Application でカメラからのビデオを表示する 『44ページ の"Management Application でカメラからビデオを再生する"参照 』も参照してください。

有効	組み込みモーション検知を有効または無効『69ページ の"モーション検知について"参照 』にします。
グリッドを表示する	グリッドをオンまたはオフに切り替えます。 グリッドをオフにすることで、プレビュー画像がよりはっきり見える場合もあります。グリッドが表示されている場合と同じ方法で、モーション検知から除外する領域を選択します。グリッドがオンであれば、プレビュー画像はグリッドによって小さいセクションに分割されます。 モーション検知から除外する必要がある領域を定義するには、マウスボタンを押下した状態で、プレビュー画像の領域の上でマウスをドラッグします。左マウスボタンでグリッドを選択します。右マウスボタンでグリッドをクリアします。選択されたエリアが、青色で強調表示されます。
すべてを含める	プレビュー画像で、すべてのグリッドで区切られた部分を迅速に選択できます。これは、画像の大半のエリアでモーション検知を除外したい場合に便利です。その場合、モーション検知を除外したくない部分をクリアします。
すべてを除外する	プレビュー画像で、すべてのグリッドで区切られた部分をクリアします。

手動感度	この機能を有効にすると、モーションの感度スライドを自分で調整することもできます。 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見なされます。 • 感度レベルが**低くなるほど**、各ピクセルの変化がより多くなった際にモーションと見なされます。 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。 次の理由により、Milestone は手動感度を有効にしないことをお勧めします。 • ダイナミック感度の場合、システムは感度レベルを自動的に計算して最適化し、画像のノイズから発生するモーション検知を抑制します。 • 夜間には、画像のノイズにより誤ったモーションが頻繁にトリガされますが、ダイナミック感度によりモーション検知が改善します。 • 録画が多すぎることに起因するシステム過負荷は発生しません。 • 録画が不十分なために結果が見られなくなることもありません。
感度	この設定を使用して、モーションとして認識するために変化する必要があるピクセルの数を決定します。感度が高いと、モーションとして認識するために必要なピクセルの変化は非常に小さくなります。モーションが検知されたエリアは、プレビュー画像で緑色に強調表示されます。 モーションと見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。スライダーを左へ移動させるほど、プレビューで強調表示される部分が増えます。これは、感度を非常に高くすると、各ピクセルのわずかな変化でさえモーションと見なされるからです。 スライダーを使用する代わりに、スライダーの横のフィールドで 0～256 の値を指定して、感度設定を制御することもできます。
モーション	必要なレベルのモーションによってのみ、モーション検知がトリガされるように**モーション**スライダーを調整します。選択されたモーションレベルは、スライダーの上にある**レベル**バーの黒い垂直線で示されます。黒い垂直線は、閾値になります。モーションが選択されたレベルを超える場合（右側）、バーの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。 または、左のフィールドで 0～10000 の値を指定して、モーション設定を制御します。 スライダーを左へドラッグするほど、モーション検知に必要な変化が小さくなるので、よりモーション検知が表示されます。モーション検知の回数も録画するビデオの量、受信する通知の量などに影響を与えます。
キーフレームだけ	ビデオストリームのキーフレームのみでモーション検知を行うことで、モーション検知で使用するシステムのリソースを減らしたい場合は、**キーフレームだけ**を選択します。

検知間隔	カメラからのビデオで、どれくらいの頻度でモーション検知分析を行うかを指定します。デフォルトは 240 ミリ秒ごとです（1 秒にほぼ 4 回）。この間隔は、使用しているカメラのフレームレート設定には関係なく適用されます。 この設定を調整すると、モーション検知で使用されるシステムのリソースを低減できます。
検知解像度	画像全体を分析するか、選択した部分の画像を分析するかを指定します。たとえば 25%と指定すると、すべてのピクセルを分析する代わりに 4 ピクセルごとに分析するので、使用するシステムのリソースは低減しますが、モーション検知の正確度も低下します。

プライバシーマスク

プライバシーマスクには次のプロパティを設定します。

有効	**プライバシーマスク**機能を有効にします。
グリッドを表示する	グリッドをオンまたはオフに切り替えます。グリッドをオフにすることで、プレビュー画像がよりはっきり見える場合もあります。グリッドを表示する場合と同様に、除外したいエリアを選択します。 オンにすると、プレビュー画像は、グリッドで小さな部分に分割されます。プライバシーマスクから除外する必要がある領域を定義するには、マウスボタンを押下した状態で、プレビュー画像の領域の上でマウスをドラッグします。左マウスボタンでグリッドを選択します。右マウスボタンでグリッドをクリアします。選択されたエリアが、赤色で強調表示されます。
プライバシーマスクの表示	プライバシーマスクを示す赤色のエリアをオンまたはオフに切り替えます。赤色のエリアをオフにすることで、プレビュー画像がよりはっきり見える場合もあります。
クリア	プライバシーマスクをクリアします。

魚眼レンズ（プロパティ）

※本機は、魚眼ライセンスキーが必要なカメラには対応していません。

魚眼レンズテクノロジを使用すると、高度なレンズで魚眼レンズのパノラマビデオを再生できます。

魚眼レンズテクノロジを使用する場合、まずテクノロジを有効にし、場合によって特別なライセンスキーの入力が必要な場合があります。特別な魚眼ライセンスキーが必要であるかどうか不明な場合は、システムのベンダーに詳細をお問い合わせください。

魚眼サポートを有効にする	チェックボックスを選択すると、魚眼レンズテクノロジが使用可能となり、さらに多くのプロパティを指定できます。

ImmerVision Enables® Panomorph RPL 番号	Panomorph サポート機能を有効にする場合、**ImmerVision Enables® Panomorph RPL 番号**リストで登録済み Panomorph レンズ（RPL）番号も選択し、レンズが正しく特定され、カメラで使用されるレンズで構成されることを保証する必要があります。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。 • 別のタイプのレンズが必要になった場合、**ファイル**へ移動し、**新しいレンズタイプのインポート**を選択します。レンズタイプに関する情報を含んでいる.xml ファイルを検索し、**OK** をクリックします。 ImmerVison、panomorph（パノモーフ）レンズ、および RPL の詳細については、ImmerVision Enables Web サイト『https://www.immervisionenables.com/』をご覧ください。
カメラの位置/方向	カメラを天井、壁、地上のいずれに取り付けるかを選びます。

PTZ プリセット位置

PTZ 関連のプロパティが使用できるのは、PTZ（パン/チルト/ズーム）カメラを使用している場合だけです。

PTZ プリセット位置を使用すると、特定のイベントが発生したり、PTZ パトロールプロファイルを設定した場合に、PTZ カメラを自動的に特定の位置へ移動させることができます。また、クライアントでプリセット位置を使用して、複数のプリセット位置間で PTZ カメラを移動させる権限『161ページ の"ユーザーおよびグループの権限の設定"参照 』をユーザーに付与することもできます。プリセット位置の名前には、A-Z、a-z、数字 0-9 だけを含めます。カメラからプリセット位置をインポートした場合は、名前にこれら以外の文字が含まれていないか確認してください。含まれている場合は、インポートする前にプリセット位置の名前を変更してください。

複数の同時ビデオストリーム出力に対応しないカメラは、監視サーバーと Management Application に同時に接続することはできません。Milestone では、そうしたデバイスでモーション検知や PTZ を設定する場合、Recording Server サービスを停止 『168ページ の"サービスを開始および停止する"参照 』することを推奨しています。

Management Application でカメラからのビデオを表示する 『44ページ の"Management Application でカメラからビデオを再生する"参照 』も参照してください。

PTZ タイプ	設定オプションは、対象となる PTZ カメラのタイプによります。 • タイプ 1（サーバーに保存）：ウィンドウの上半分にあるコントロールを使用してカメラを移動させてから、必要な位置をそれぞれシステムサーバーに保存して、プリセット位置を定義します。この方法で、最大で 50 のプリセット位置を定義できます。 • タイプ 2（カメラからインポート）：事前に定義され、PTZ カメラ自体に保存されているプリセット位置を、カメラ独自の設定インターフェースでインポートします。許可されるプリセット位置の数は、使用する PTZ カメラおよびドライバーにより異なります。 • タイプ 3（カメラに保存）：ウィンドウの上半分にあるコントロールでカメラを移動させてから、必要な位置をそれぞれカメラ独自のメモリに保存して、プリセット位置を定義します。この方法で、最大で 50 のプリセット位置を定義できます。カメラに対して既にプリセット位置が定義されている場合は、システムで使用するプリセット位置を簡単にインポートできます。

インポート/更新	PTZ タイプ 2 または 3 を選択している場合のみ使用できます。カメラのメモリから、既に定義されているプリセット位置をインポートして、システムで使用することができます。 この方法で既にプリセット位置をインポートした後で、カメラでプリセット位置を追加または変更している場合、このボタンを使用してインポートしたプリセット位置を更新することができます。
新規追加	PTZ タイプ 1 を選択している場合のみ使用できます。ウィンドウ上部のコントロールを使用して、必要な位置へカメラを移動させ、空白のフィールドに位置の名前を入力してから、ボタンをクリックしてその位置を定義済みのプリセット位置のリストに追加します。 プリセット位置の名前には、文字 A～Z、a～z、数字 0～9 しか使用できないことに注意してください。
新しい位置を設定	PTZ タイプ 1 または 3 を選択している場合のみ使用できます。既に定義済みのプリセット位置が変更できます。リストで、変更したいプリセット位置を選択します。次に、ウィンドウ上部のコントロールを使用して、必要な位置へカメラを移動させます。次に、ボタンをクリックして、古い位置の代わりに新しい位置を上書きします。
削除	PTZ タイプ 1 または 3 を選択している場合のみ使用できます。既に定義済みのプリセット位置が削除できます。リストで、削除したいプリセット位置を選択してから、ボタンをクリックします。 プリセット位置を削除する前に、その位置が PTZ パトロールやイベントでの PTZ で使用されていないか確認してください。プリセット位置はカメラに保存されているため、**インポート/更新**ボタンをクリックすると、削除したプリセット位置をシステムに復元することができます。この方法でプリセット位置を復元して、PTZ パトロールやイベントでの PTZ で使用する場合、再度使用するには手動での設定が必要になります。
テスト	プリセット位置を試します。リストで、テストしたいプリセット位置を選択してから、ボタンをクリックして、カメラが選択した位置へ移動することを確認します。
PTZ コントロールホイール	リストで選択したプリセット位置を、上下に移動します。選択したプリセット位置は、一度のクリックで 1 ステップだけ移動します。プリセット位置を上下に移動することで、プリセット位置をクライアントに表示する順番を制御できます。

PTZ パトロール（プロパティ）

複数の同時ビデオストリーム出力に対応しないカメラは、監視サーバーと Management Application に同時に接続することはできません。Milestone では、そうしたデバイスでモーション検知や PTZ を設定する場合、Recording Server サービスを停止 『168ページ の"サービスを開始および停止する"参照 』することを推奨しています。

Management Application でカメラからのビデオを表示する 『44ページ の"Management Application でカメラからビデオを再生する"参照 』も参照してください。

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。詳細については、製品比較チャート 『12ページ 』を参照してください。

PTZ 関連プロパティを設定できるのは、PTZ（パン/チルト/ズーム）カメラに対してだけです。PTZ パトロールとは、複数のプリセット位置間での PTZ カメラの連続的な移動です。パトロールを使用するには、関連する PTZ

カメラに対して少なくとも 2 か所のプリセット位置を指定する必要があります。PTZ パトロールを設定するには、**パトロール設定**リストでパトロールのプロファイルを選択し、関連するプロパティを指定して、パトロール設定の正確な動作を定義します。パトロールプロファイルを定義したら、パトロールプロファイルの使用を忘れずにスケジュールしてください。ユーザーが手動で PTZ カメラを操作すると、パトロール動作が上書きされることに注意してください。必要に応じて、プリセットが 1 つだけのパトロール設定を指定できます。このようなパトロール設定が役に立つのは、以下の 2 つのケースです。 PTZ カメラを指定された時刻に指定された位置へ移動させる場合。および、PTZ カメラを手動操作で指定位置へ移動させる場合。

パトロールプロファイル

PTZ カメラは、複数の異なるパトロールプロファイルに従ってパトロールを行うことがあります。たとえば、スーパーマーケットにある PTZ カメラは、営業時間内はあるパトロール設定に従ってパトロールを行ない、閉店後は別のパトロール設定に従ってパトロールを行なうことができます。他のカメラに対して定義済みパトロールプロファイルの名前を再利用することができます。これにより、単一のパトロール設定名を複数の PTZ カメラで使用し、PTZ パトロールのスケジューリングを簡単にすることができます。複数の PTZ カメラでパトロール設定名を共有している場合にも、プリセット位置間でのそれぞれのカメラの動きは個別になります。

パトロール設定リストから、設定したいパトロール設定を選択します。

新規追加	新しいパトロール設定をリストに追加します。新しいパトロール設定を追加する場合、一意の名前を付けるか、PTZ パトロールを行っている別の PTZ カメラから既存の名前を再利用します。 複数の同じ名前のパトロールプロファイルを使用すると、後でスケジュールを設定する際に便利です。例：25 台の異なるカメラで同じ名前「夜間パトロール」のパトロールプロファイルを設定している場合、たとえ「夜間パトロール」が 25 台のカメラのそれぞれに対して個別のプリセット位置をカバーしていても、25 台のカメラのすべてで「夜間パトロール」の使用を一度にスケジュールできます。
削除	既存のパトロール設定を削除します。選択したパトロール設定は、警告なしでリストから削除されることに注意してください。

パトロールリスト

パトロール設定リストでパトロール設定を選択すると、選択したパトロールのスキームでどの PTZ カメラのプリセット位置を使用するか指定できます。ボタンを使用して、選択したプリセット位置を**パトロールリスト**にコピーします。**プリセット位置**リストでのプリセット位置の順番を変更するには、プリセット位置を選択し、またはボタンを使用して、選択したプリセット位置をリスト内で上下に移動させます。選択したプリセット位置は、一度のクリックで 1 ステップだけ移動します。後で、パトロールリストからプリセット位置を削除したくなった場合は、プリセット位置を選択して、ボタンをクリックします。

待ち時間（秒）	PTZ カメラが、次のプリセット位置へ移動する前に、それぞれのプリセット位置で留まる時間を秒数で指定します。デフォルトは 10 秒です。待ち時間は、パトロール設定にあるすべてのプリセットに適用されます。PTZ カメラは、それぞれのプリセット位置に同じ秒数だけ留まります。

移行時間（秒）	PTZ カメラが、あるプリセット位置から別のプリセット位置へ移動するのに必要な時間を秒数で指定します。デフォルトは 5 秒です。この移行時間に、カメラのモーション検知は自動的に無効になります。これは、カメラがプリセット位置間を移動するときに、不必要なモーションが検出されるためです。指定した秒数が経過すると、モーション検知は再び自動的に有効になります。 移行時間は、パトロール設定にあるすべてのプリセットに適用されます。指定した秒数内で、カメラがパトロール設定のプリセット位置間を切り替えられることが重要です。できない場合、システムは間違ったモーションを検知する可能性があります。PTZ カメラは、物理的に近い位置より、物理的に離れた場所（たとえば、極端に左にある場所から、極端に右にある場所へ）への移動に時間がかかる点に注意してください。

PTZ スキャン

PTZ スキャン（連続パン）をサポートしている PTZ カメラはあまり多くありません。PTZ スキャンを有効にして、チェックボックスの下にあるリストで、PTZ スキャンの速度を選択します。PTZ スキャンが機能するのは、PTZ タイプ 1 のカメラだけです（プリセット位置がサーバー上で設定され、サーバー上に保存されるタイプです）。カメラが PTZ タイプ 2 のカメラで、カメラ独自の設定インターフェースで定義し、PTZ カメラ上に保存されたプリセット位置をインポートしている場合、PTZ スキャンは動作を停止します。

PTZ パトロールの一時停止

ユーザーがカメラを手動で操作したり、システムが**イベントでの PTZ** を使用したりすると、PTZ パトロールは自動的に一時停止します。また、システムがモーションを検知すると、PTZ パトロールが一時停止することもあります。一時停止の設定は、選択したパトロール設定と連結しています。このため、同じカメラで、異なるパトロールプロファイルに異なる一時停止設定をするなど、柔軟性の高い設定ができます。

モーションが検知された場合のパトロール一時停止

システムがモーションを検知した時に PTZ カメラがその位置に特定期間だけ留まるようにするには（PTZ パトロールを一時停止するには）、以下の操作を実行します。

1. **モーションが検知された場合のパトロール一時停止**チェックボックスを選択します。
2. 以下の場合に、PTZ カメラでパトロールを再開する必要があるかどうかを選択します。
   - モーションを追加検知したかどうかに関わらず、最初にモーションを検知してから一定の秒数が経過した後

     または

   - モーションを追加検知せずに、一定の秒数が経過した後
3. 選択したオプションに対する秒数（デフォルトはそれぞれ 10 秒と 5 秒）を指定します。
4. 移行時間をゼロに設定しない限り、カメラがプリセット位置間を移動する際に、システムは自動的にモーション検知を無効にします。無効にしないと、カメラがプリセット位置間を移動している間に、無意味なモーションを検知する可能性があるためです。

PTZ パトロールの再開

ユーザーがカメラを手動で操作したり、イベントでの PTZ が使用されたりすると、システムは自動的に PTZ パトロールを一時停止します。手動操作またはイベントベースの中断があった場合に、システムが通常のパトロールを再開するまでの秒数を指定できます。デフォルトは 30 秒です。

手動コントロールとは別に、XProtect Smart Client のユーザーは、選択した PTZ カメラのパトロールを完全に停止することもできます。したがって、XProtect Smart Client ユーザーの場合、ユーザーが手動で PTZ カメラを制御した場合にのみ、**パトロール設定**セクションで指定した秒数が適用されます。ユーザーが PTZ カメラのパトロールを完全に停止した場合はこれに該当しません。XProtect Smart Client ユーザーが PTZ カメラのパトロールを完全に停止した場合、カメラのパトロールが再開するのは XProtect Smart Client ユーザーが再開を選択した場合だけです。

イベントでの PTZ

PTZ 関連のプロパティが使用できるのは、PTZ（パン/チルト/ズーム）カメラを使用している場合だけです。PTZ カメラがプリセット位置 『101ページ の"PTZ プリセット位置"参照 』をサポートしている場合、特定のイベントが発生 『108ページ の"イベントおよび出力の概要"参照 』した時に、PTZ カメラを自動的に特定のプリセット位置へ移動させることができます。PTZ カメラのプリセット位置にイベントを関連付ける場合、システムで定義されている**すべて**のイベントを選択することができます。特定のハードウェアデバイスで定義されたイベントの選択を制限されることはありません。

コンポーネント	要件
イベント	関連するイベントを選択します。
PTZ プリセット位置	関連するプリセット位置を選択します。この目的で、PTZ カメラでイベントを使用できるのは一度だけです。ただし、別のイベントを使用して、PTZ カメラを同じプリセット位置へ移動させることができます。 例： • イベント 1 は、PTZ カメラをプリセット位置 A へ移動させます。 • イベント 2 は、PTZ カメラをプリセット位置 B へ移動させます。 • イベント 3 は、PTZ カメラをプリセット位置 A へ移動させます。

後で、特定のイベントと特定のプリセット位置の間での関連付けを解消したくなった場合は、イベントを含んでいるフィールドをクリアします。PTZ 設定の変更を完了したら、サービスを再起動 『168ページ の"サービスを開始および停止する"参照 』します。

複数の同時ビデオストリーム出力に対応しないカメラは、監視サーバーと Management Application に同時に接続することはできません。Milestone では、そうしたデバイスでモーション検知や PTZ を設定する場合、Recording Server サービスを停止 『168ページ の"サービスを開始および停止する"参照 』することを推奨しています。

Management Application でカメラからのビデオを表示する 『44ページ の"Management Application でカメラからビデオを再生する"参照 』も参照してください。

マイク

マイクについて

システムで、**マイク**は通常はハードウェアデバイスに取り付けられるので、物理的にカメラの次に位置します。そこで、必要な権限を持つオペレータは、XProtect Smart Client (XProtect Smart Client を実行しているコンピュータにスピーカーが取り付けられている場合」を通じて録音を聴くことができます。マイクはシステムで管理します。つまり、XProtect Smart Client のオペレータのコンピュータに取り付けられているマイクでは**なく**、カメラに取り付けられているマイクを常に管理できます。

必要以上のマイクをシステムに追加した場合、関連するマイクやスピーカーを右クリックして、**非表示**を選択すると、不要なものを非表示にすることができます。非表示にしたマイクを再度表示したい場合は、マイク全体のアイコンを右クリックして、**非表示の項目を表示**を選択します。

マイクまたはスピーカーの設定

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、製品比較チャート『12ページ 』を参照してください。

1. **詳細設定 > ハードウェアデバイス**を展開し、関連するマイクまたはスピーカーが取り付けられているハードウェアデバイスを展開します。
2. 関連するマイクまたはスピーカーを右クリックして、**プロパティ**を選択します。
3. 必要に応じてプロパティ 『66ページ の"スピーカープロパティ"参照 』を指定します。

システムのマイクやスピーカーの設定は、非常に簡単です。音量や類似の設定は、マイクまたはスピーカーユニット自体でコントロールできます。

マイクやスピーカーの表示/非表示

システムで必要とされる数以上のマイクやスピーカーを追加した場合、不要なマイクやスピーカーを右クリックして、**非表示**を選択すると、それらを非表示にすることができます。非表示にしたマイク/スピーカーを再度表示したい場合は、マイクやスピーカー全体のアイコンを右クリックして、**非表示アイテムの表示**を選択します。

マイク（プロパティ）

特定のカメラに対してビデオおよび録画の設定 『69ページ の"ビデオや録画の設定について"参照 』する場合、音声を録音するタイミングを指定できます。この選択は、システムのすべてのカメラに適用されます。

マイクのプロパティ

デバイスが有効	マイクはデフォルトで有効になっており、これはシステムに音声を転送できることを意味します。必要に応じて、個別のマイクを無効にすることができます。この場合、マイクからシステムへ音声は転送されません。

名前	Management Application およびクライアントで表示される名前です。既存の名前を、新しい名前で上書きすることができます。 名前は一意であり、以下の特殊文字を含むことはできません。 **< > & ' " ¥ / : * ? | [ ]**

一部のハードウェアデバイスでは、ハードウェアデバイス自体で音声を有効/無効にすることもできます。通常は、ハードウェアデバイス自体の設定用 Web ページで行います。Management Application で有効にしてもハードウェアデバイスで音声が機能しない場合は、ハードウェアデバイス自体で音声が無効になっていることが原因かどうかを確認する必要があります。

録画設定

常時録音	すべての該当するカメラで、音声を常に録音します。
ビデオに従う	マイクが取り付けられている、カメラからビデオを録画する時だけ、音声を録音します。
設定しない	どのカメラでも音声を録音しません。システムが音声を録音しない場合でも、XProtect Smart Client でライブオーディオを聴くことができます。

イベントおよび出力

入力および出力について

ドアセンサーなどの**ハードウェア入力**を、ハードウェアデバイスの入力ポートに接続することができます。このような外部ハードウェア入力ユニットからの信号により、システムでイベントを生成することができます。

ハードウェア出力ユニットを、さまざまなハードウェアデバイスの出力ポートに接続して、照明、サイレンなどをシステムから起動することができます。こうしたハードウェア出力は、イベントによって自動的にアクティブにすることもできますし、クライアントから手動でアクティブにすることもできます。

ハードウェアデバイスでハードウェア入力ユニットおよびハードウェア出力ユニットの使用を指定する前に、そのセンサーの動作がハードウェアデバイスによって認識されていることを確認してください。大半のハードウェアデバイスは、設定用インターフェースか CGI スクリプトのコマンドで表示できます。また、システムのリリースノートをチェックして、使用するハードウェアデバイスおよびファームウェアが入力や出力の制御・操作に対応していることを確認してください。

ハードウェア入力ユニットを個別に設定する必要はありません。ハードウェアデバイスに接続されているハードウェア入力ユニットは、ハードウェアデバイスをシステムに追加した時点で自動的に検出されます。ハードウェア出力の場合も同様ですが、ハードウェア出力についてはシステムで簡単な設定を行う必要があります。

ハードウェア出力を設定して、たとえばドアが開いたタイミングや、ビデオでモーションが検知されたときに照明をオンにするなど、**イベント発生時に出力を自動的にトリガ**したい場合は、ハードウェア出力の追加 『111ページ 』およびイベントでのハードウェア出力の設定 『112ページ 』を参照してください。

イベントおよび出力について

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、製品比較チャート『12ページ 』を参照してください。

さまざまなタイプのイベントや出力を使用して、システム上のアクションを自動的にトリガすることができます。アクションの例：録画の開始・停止、フレームレートの切り替え、通知のトリガ、PTZ カメラのプリセット位置への移動。また、イベントを使って、ハードウェアの出力をアクティブ化することもできます。さらに、イベントおよび出力を設定して、アラームを生成することができます。

イベントは、以下のように分類されます。

- **内部イベント（システム関連）**：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。
- **外部イベント（統合）**：例：MIP プラグインイベント。

イベントおよび出力の概要

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、製品比較チャート『12ページ 』を参照してください。

イベントのタイプ：

名前	詳細
アナリティックイベント：	※本機は、アナリティックイベントには対応していません。 アナリティックイベントは、アラームとして使用したり、シームレスにアラーム機能と統合したりすることができます。 アナリティックイベントは、一般的に、外部のサードパーティのビデオコンテンツ分析(VCA)プロバイダから受信したデータです。VCA ベースのシステムの例として、アクセスコントロールシステムが挙げられます。
ハードウェア入力イベント：	ドアセンサーなどのハードウェア入力を、ハードウェアデバイスの入力ポートに割り当てることができます。このような外部ハードウェア入力ユニットからの信号により、システムでイベントを生成することができます。 ハードウェアデバイスに取り付けられたハードウェア入力ユニットからの入力に基づくイベントを、ハードウェア入力イベントと呼びます。 一部のハードウェアデバイスには、モーションの検知、移動および静止中の物体の検知などの独自の機能があります（この機能はハードウェアデバイス独自のソフトウェアで設定します。通常は、ハードウェアデバイスの IP アドレスによってアクセスできる、ブラウザベースの設定インターフェースで設定します）。この場合、システムは、このような検知をハードウェアからの入力とみなします。また、この検知を入力イベントとして使うことも可能です。 最後に、ハードウェア入力イベントは、システムでのモーション検知の設定や、カメラからのビデオのシステムによるモーション検知に基づいて発生させることもできます。 また、このタイプのハードウェア入力イベントは、システムモーション検知イベントまたは VMD（ビデオモーション検知）イベントと呼ばれます。以前のバージョンの監視システムでは、VMD イベントは独自のタイプのイベントでした。現在は、ハードウェア入力イベントのタイプのひとつとみなされます。

名前	詳細
ハードウェア出力：	ハードウェア出力ユニットを、さまざまなハードウェアデバイスの出力ポートに割り当てて、照明、サイレン、その他をシステムから起動することができます。こうしたハードウェア出力は、イベントによって自動的にアクティブにすることもできますし、クライアントから手動でアクティブにすることもできます。
手動イベント：	イベントは、ユーザーがクライアントで選択することで、手動で生成することができます。これらのイベントは手動イベントと呼ばれます。 手動イベントは、**グローバルイベント**または**タイマーイベントのタイプになります。** グローバルイベントはすべてのハードウェアに適用されますが、タイマーイベントは別個のイベントで、ハードウェア入力イベント、手動イベント、あるいは定義されたジェネリックイベントによってトリガされます。タイマーイベントは、定義されたイベントが発生した後、指定された時間（秒または分）の後に発生します。タイマーイベントは、幅広い目的で使用されますが、通常は前にトリガされたアクションを停止するために使用されます。 **例：** たとえばドアが開くなどのハードウェア入力イベントに基づいて、カメラが録画を開始します。タイマーイベントにより、15 秒後に録画が停止します。
ジェネリックイベント：	入力を TCP または UDP のパケット形式で受信することも可能です。これはシステムによって分析され、指定された基準に一致する場合に、イベントが生成されます。このようなイベントは、ジェネリックイベントと呼ばれます。
イベントでの出力コントロール：	ハードウェア出力は、イベントが発生した時に自動的に起動できます。たとえば、ドアが開くと（ハードウェア入力イベント）、照明がオンになります（ハードウェア出力）。 出力コントロールを設定する場合、システムで定義されているすべての出力およびイベントの中から選択することができます。特定のハードウェアデバイスで定義された出力やイベントの選択に制限されることはありません。単一のイベントを使って、複数の出力をアクティブ化することができます。

いずれかのタイプのイベントを設定する前に、たとえば、イベントデータのためにどのポートを使用するかなどの**一般的なイベント処理を設定**します。通常は、単にデフォルト値を使用するだけで構いませんが、組織で他の目的でこのポートを使用していないか確認することをお勧めします。一般的なイベント処理の設定 『113ページ 』を参照してください。

ハードウェアデバイスでハードウェア入力およびハードウェア出力ユニットの使用を指定する前に、そのセンサーの動作がデバイスによって認識されていることを確認してください。大半のハードウェアデバイスは、設定用インターフェースか CGI スクリプトのコマンドで表示できます。また、監視システムのリリースノートをチェックして、入力および出力によってコントロールされる動作が、使用しているハードウェアデバイスやファームウェアでサポートされているか確認してください。マスター/スレーブ設定で複数のサーバーを使用する場合、特定のハードウェアデバイスの入力および出力は 1 つのサーバーでのみ定義する必要があります。複数のサーバーで、同じハードウェアデバイス上の同じ入出力を定義しないでください。

ハードウェア入力ユニットを個別に設定する必要はありません。ハードウェアデバイスに接続されているハードウェア入力ユニットは、ハードウェアデバイスをシステムに追加した時点で自動的に検出されます。ハードウェア出力の場合も同様ですが、ハードウェア出力についてはシステムで簡単な設定を行う必要があります。

ハードウェア出力を設定して、たとえばドアが開いたタイミングや、ビデオでモーションが検知されたときに照明をオンにするなど、**イベント発生時に出力を自動的にトリガ**したい場合は、ハードウェア出力の追加 『111ページ 』およびイベントでのハードウェア出力の設定 『112ページ 』を参照してください。

イベントを設定する準備ができたら、ハードウェア入力イベントの追加 『110ページ 』、ジェネリックイベントの追加 『112ページ 』、手動イベントの追加 『111ページ 』を参照してください。他のイベントでタイマーイベントを使用したい場合は、タイマーイベントの追加 『112ページ 』を参照してください。

アナリティックイベントの追加

※本機は、アナリティックイベントには対応していません。

アナリティックイベントを追加するには、次の手順を実行してください。

1. **イベントおよび出力**を展開し、**アナリティックイベント**を右クリックして、**新規作成**を選択します。
2. 必要なプロパティを指定します。 **OK** をクリックします。
3. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

ハードウェア入力イベントの追加

ハードウェア入力イベントでは、ハードウェアデバイスに接続した入力ユニットから受信した入力をシステムでのイベント 『108ページ の"イベントおよび出力の概要"参照 』に変換することができます。

ハードウェアデバイスの入力を指定する前に、ハードウェアデバイスがセンサーの動作を認識できるか確認してください。大半のハードウェアデバイスは、設定用インターフェースか CGI スクリプトのコマンドで表示できます。使用しているハードウェアデバイスやファームウェアが入力制御に対応しているかについては、それらのリリースノートを確認してください。

ハードウェア入力イベントを追加・設定するには、次の手順を実行してください。

1. **詳細設定 > イベントと出力**を展開します。**ハードウェア入力イベント > 新しい入力イベントを有効にする**を右クリックします。
2. **ハードウェア入力イベントプロパティ**ウィンドウのハードウェアデバイスのリストで、関連するハードウェアデバイスを展開し、定義済みのハードウェア入力を表示します。
3. イベントとして使用する必要なタイプの入力を選択します。入力のタイプは、多くの場合、カメラによって異なります。関連するカメラに関して、モーション検知 『98ページ の"モーション検知&と領域の除外"参照 』がシステムで有効になっている場合、**システムモーション検知**の入力タイプをメモします。これによって、カメラのビデオストリームで検知したモーションをイベントにすることができます。

   一部のタイプの入力は、相互に排他的であることに注意してください。ある入力タイプを選択した場合、それに対し排他関係にある入力タイプは選択できなくなります。
4. 選択した入力のそれぞれのタイプについて、必要なプロパティ 『118ページ の"ハードウェア入力イベント"参照 』を選択します。準備が完了したら、**OK** をクリックするか、**追加**ボタンをクリックして、作成したイベントにタイマーイベントを追加 『112ページ の"タイマーイベントの追加"参照 』します。
5. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

ハードウェア出力の追加

ハードウェア出力では、照明、サイレン、ドアの開放などの外部出力ユニットをシステムに追加できます。追加すると、イベント 『108ページ の"イベントおよび出力の概要"参照 』または検知したモーションにより出力を自動的にアクティブ化したり、クライアントユーザーによって手動でアクティブ化することができます。

出力を指定する前に、出力を使用しようとしているハードウェアデバイスによって、センサーの動作が認識されることを確認してください。大半のハードウェアデバイスは、設定用インターフェースか CGI スクリプトのコマンドで表示できます。使用しているハードウェアデバイスやファームウェアが出力制御に対応しているかについては、それらのリリースノートを確認してください。

次の手順によりハードウェア出力イベントを追加できます。

1. **詳細設定 > イベントと出力**を展開します。**ハードウェア出力 > 新しい出力の追加**を右クリックします。
2. **ハードウェア出力プロパティ**ウィンドウのハードウェアデバイスのリストで、関連するハードウェアデバイスを選択します。その後、リストの下にある**追加**ボタンをクリックします。
3. 必要なプロパティ 『118ページ の"ハードウェア入力イベント"参照 』を指定します。
4. **OK** をクリックします。
5. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

イベントが発生した時のハードウェア出力の自動アクティブ化の設定に関する詳細は、イベントでのハードウェア出力の設定 『112ページ 』を参照してください。クライアントでの出力の手動アクティブ化、ならびにモーション検知時の自動アクティブ化は、それぞれのカメラに対して個別『97ページ の"出力"参照 』に設定します。

手動イベントの追加

手動イベントでは、必要な権限 『161ページ の"ユーザーおよびグループの権限の設定"参照 』を持つユーザーは、クライアントから手動でイベントをトリガできます。手動イベントは、グローバル（すべてのカメラで共有）、または特定のカメラに関連付けられます（カメラを選択している場合だけ使用可能）。手動イベントは、以下のように様々な用途で使用できます。

- カメラのオンライン期間をスケジューリング 『132ページ の"オンライン期間"参照 』する場合の開始および停止イベントとして。たとえば、手動イベントに基づいて、カメラから監視システムへのビデオの転送を開始または停止することができます。
- カメラのその他の設定をコントロールする開始および停止イベントとして。たとえば、手動イベントによりカメラでより高いフレームレートに切り替えたり、同様にしてイベントで PTZ 『105ページ の"イベントでの PTZ"参照 』をトリガすることができます。
- 出力をトリガする場合。特定の出力を、手動イベントと関連付ける 『112ページ の"イベントでのハードウェア出力の設定"参照 』ことができます。
- イベントベースの通知 『141ページ の"通知について"参照 』をトリガする場合。
- 組み合わせで。たとえば、手動イベントによりカメラに監視システムへのビデオの転送を開始させると同時に、出力をトリガして E メール通知を関係者へ送信することができます。

手動イベントを追加するには、次の手順を実行してください。

1. **詳細設定 > イベントと出力**を展開します。**手動イベント > 新規手動イベントの追加**を右クリックします。
2. 手動イベントプロパティの左側にあるリストで、必要に応じて、グローバルまたはカメラを選択します。

3. **追加**ボタンをクリックして、必要なプロパティ 『118ページ の"ハードウェア入力イベント"参照 』を指定します。準備が完了したら、**OK** をクリックするか、**追加**ボタンを再度クリックして、作成したイベントにタイマーイベントを追加 『112ページ の"タイマーイベントの追加"参照 』します。

4. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

ジェネリックイベントの追加

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、製品比較チャート『12ページ 』を参照してください。

システムは、受信した TCP または UDP またはその両方のデータパッケージを分析して、指定された基準が満たされたときに、イベント 『108ページ の"イベントおよび出力の概要"参照 』を自動的にトリガできます。この方法で、監視システムを、アクセスコントロールシステムやアラームシステムなどの幅広い種類の外部ソースと簡単に統合することができます。

1. **[詳細設定]**を展開してから、**[イベントと出力]**を展開します。**[ジェネリックイベント]**を右クリックして、**[プロパティ]**を選択します。

2. **[ジェネリックイベントのプロパティ]**ウィンドウで、**[追加]**ボタンをクリックして、関連するプロパティを指定します。詳細は、のジェネリックイベント(イベントおよび出力固有のプロパティ) 『121ページ の"ジェネリックイベント"参照 』を参照してください。

3. タイマーイベントをジェネリックイベントに追加するには、**[追加]**ボタンをクリックします。

4. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

タイマーイベントの追加

タイマーイベントとは、定義されたタイプによってトリガされる、別個のイベント 『108ページ の"イベントおよび出力の概要"参照 』です。タイマーイベントは、定義されたイベントが発生した後、指定された秒数または分数の間に発生します。タイマーイベントは、幅広い目的で使用されますが、通常は前にトリガされたアクションを停止するために使用されます。例：

- たとえばドアが開くなどのハードウェア入力イベントに基づいて、カメラが録画を開始します。タイマーイベントにより、15 秒後に録画が停止します。

- 照明がオンになり、カメラは手動イベントに基づいて録画を開始します。1 分後にタイマーイベントにより録画が停止し、2 分後には別のタイマーイベントにより照明がオフになります。

タイマーイベントを追加するには、以前に設定した任意のイベントを選択し、**追加**ボタンをクリックして、必要なプロパティ 『120ページ の"タイマーイベント"参照 』を指定します。システムには、2 つの基本スケジュールプロファイル（**常にオン**と**常にオフ**）があり、これらを編集または削除することはできません。これらが組織のニーズに合わない場合、それぞれのカメラに対してカスタマイズされたスケジュールプロファイルを複数作成できます。カスタマイズされたスケジュールプロファイルは、必要に応じて複数の目的で再利用できます。
Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

ヒント： あるイベントの下に、必要な数のタイマーイベントを追加できます。これにより、たとえばメインのイベントの 10 秒後にあるタイマーイベントをトリガし、メインのイベントの 30 秒後には別のタイマーイベントをトリガし、さらにメインのイベントの 2 分後に 3 番目のタイマーイベントをトリガすることができます。

イベントでのハードウェア出力の設定

照明、サイレン、ドアを開くなどのハードウェア出力を追加 『111ページ の"ハードウェア出力の追加"参照 』すると、ハードウェア出力とイベント 『108ページ の"イベントおよび出力の概要"参照 』を関連付けることが

できます。これにより、イベントが発生した時に、特定のハードウェア出力をアクティブ化することができます。例：ドアが開くと（ハードウェア入力イベント）、照明がオンになります（ハードウェア出力）。

関連付ける場合、監視システムサーバーで定義された**すべて**の出力やイベントの中から選択することができます。特定のハードウェアデバイスで定義された出力やイベントの選択に制限されることはありません。

1. **詳細設定**を展開してから、**イベントと出力**を展開します。**イベントでの出力コントロール**を右クリックして、**プロパティ**を選択します。
2. 関連するプロパティ 『123ページ の"イベントでの出力コントロール（イベントおよび出力固有のプロパティ）"参照 』を入力します。**OK** をクリックします。
3. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

単一のイベントを使って、複数の出力をアクティブ化することができます。関連付けを削除することはできませんが、選択を変更したり、必要であれば両方の列で**なし**を選択することも可能です。

注意： 適切なイベントや出力をまだ定義していない場合、以下の方法で迅速に行うことができます。**イベントの設定**リストおよび/または関連付けのリストの下にある**出力の設定...**ボタンを使います。

一般的なイベント処理の設定

特定のタイプのイベントを設定する前に、たとえばシステムがイベントデータのためにどのポートを使用するかなどの一般的なイベント処理を設定します。通常は、単にデフォルト値を使用するだけで構いませんが、組織で他の目的でこのポートを使用していないか確認することをお勧めします。

1. **詳細設定**を展開し、**イベントと出力**を右クリックし、**プロパティ**を選択します。
2. 必要なプロパティ 『115ページ の"ポートとポーリング"参照 』を指定します。 システムには、2 つの基本スケジュールプロファイル（**常にオン**と**常にオフ**）があり、これらを編集または削除することはできません。これらが組織のニーズに合わない場合、それぞれのカメラに対してカスタマイズされたスケジュールプロファイルを複数作成できます。カスタマイズされたスケジュールプロファイルは、必要に応じて複数の目的で再利用できます。
3. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

アナリティックイベントに基づくアラームの生成

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、製品比較チャート『12ページ 』を参照してください。

アナリティックイベントに基づくアラームの生成には、通常は以下の 3 段階のプロセスがあります。

1. アナリティック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ニングするポートを制御できます。
2. イベントの説明などを使用してアナリティックイベントを作成し、テストします。
3. アラーム定義 『244ページ 』のソースとしてアナリティックイベントを使用します。

上記のとおり、一般的に、システムにデータを渡すためにはサードパーティ VCA が必要です。使用する VCA ツールは、ツールが供給するデータが Milestone アナリティックイベントの開発者マニュアルで説明されているフォーマットルールに適合する限り、任意の VCA ツールを使用できます。詳細については、Milestone までお問い合わせください。

ジェネリックイベントのテスト

ジェネリックイベントを追加した場合、ジェネリックイベントをすばやく簡単にテストする方法は、まずイベント通知をセットアップして、ジェネリックイベント、さらにイベント通知をトリガするデータを **Telnet** を使用して送信することです。

Telnet は旧バージョンの Windows にはデフォルトでインストールされています。詳細は、https://technet.microsoft.com/en-us/library/cc771275(v=ws.10).aspx 『https://technet.microsoft.com/en-us/library/cc771275(v=ws.10).aspx』を参照してください。

この例では、**Video** と呼ばれるジェネリックイベントを作成しています。このジェネリックイベントでは、受信した TCP データパッケージに **Video** という単語が出現すると、ジェネリックイベントをトリガするように指定しています。使用するジェネリックイベントでは異なるかもしれませんが、原則は次の通りです。

1. **[詳細設定]**を展開してから、**[カメラおよびストレージの情報]**を展開します。XProtect Smart Client でアクセス権があるカメラを右クリックして、**[プロパティ]**を選択します。

2. **[イベント通知]**を選択して、必要なジェネリックイベントを選択します。テストを行っている間、ジェネリックイベントが、**[選択したイベント]**リストに表示される唯一のイベントであることを確認してください。そうでない場合、イベント通知をトリガしたのがそのジェネリックイベントであるかどうか判断できません。テストが終わると、一時的に削除したイベントを**[選択したイベント]**リストに戻すことができます。

3. Management Application のツールバーで**[設定の保存]**ボタンをクリックして、設定の変更を保存します。

4. Recording Server サービスが実行中であることを確認してください。また、イベント通知を設定したカメラが表示されており、XProtect Smart Client でカメラのタイトルバーが有効になっていることも確認してください。その場合、黄色のイベントインジケータが表示されます。

5. Telnet を実行して、以下を入力します。

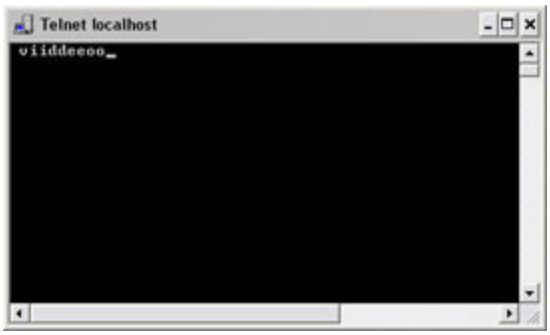
6. Windows の**[スタート]**メニューで、**[ファイル名を指定して実行]**を選択し、**[開く]**フィールドに以下を入力します。

   - システムサーバー自体でテストを実行している場合:`telnet localhost 1234`
   - リモートコンピュータからテストを実行している場合:**localhost** の部分を、システムのサーバーの IP アドレスに置き換えます。例:監視システムサーバーの IP アドレスが 123.123.123.123 であれば、次のように入力します。`telnet 123.123.123.123 1234`

   これにより、**Telnet** ウィンドウが開きます。

   上の例で、数字 **1234** はシステムサーバーがジェネリックイベントをリスニングするポートを示しています。ポート 1234 がデフォルトのポートですが、ジェネリックイベント処理の設定 『113ページ の"一般的なイベント処理の設定"参照 』の一部として別のポートを指定して、ポートを変更することができます。システムでアラートやジェネリックイベントのポート番号を変更した場合、**1234** の代わりにシステムのアラートおよびジェネリックイベントのポート番号を入力してください。

7. **Telnet** ウィンドウで、ジェネリックイベントのトリガに必要な言葉**(イベントの文字列の一部)**を入力します。ここでの例では、単一の言葉 **Video** が必要です。



Telnet ウィンドウでの入力中は、入力した内容がエコーされることがあります。これは、サーバーが受信した文字の一部または全部を繰り返しているためです。正しく入力している限り、これは問題になりません。

8. **Telnet** ウィンドウを閉じます。ウィンドウを閉じるまで、入力した内容が監視システムに送信されないので、ウィンドウを閉じてください。

9. XProtect Smart Client に移動します。対象のカメラについて、黄色のイベントインジケータが点灯していれば、ジェネリックイベントは予測通りに動作しています。

重要:ジェネリックイベントには最大 128 文字を入力できます。128 文字を超えて入力した場合、128 文字を超える文字列は破棄されます。

ジェネリックイベントプロパティ

ポートとポーリング

ジェネリックイベントプロパティウィンドウでは、イベント処理と一緒に使用するネットワークの設定を指定できます。

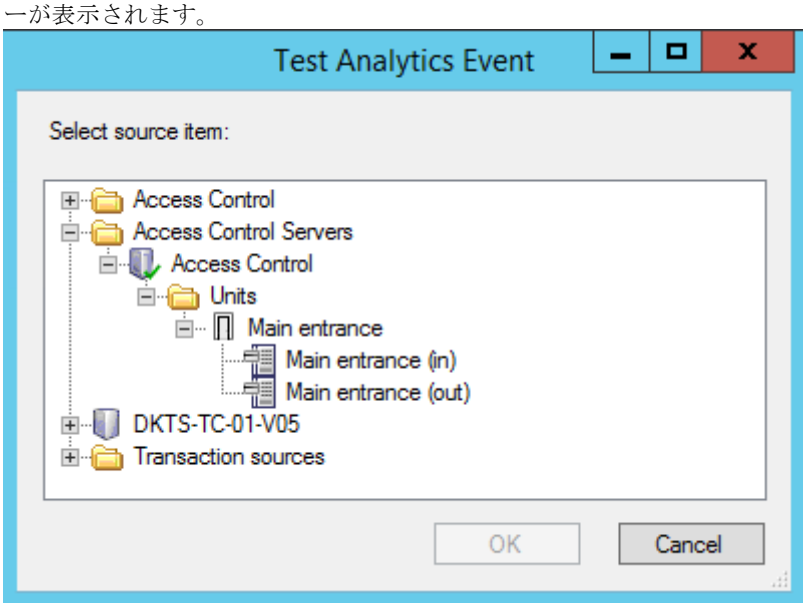
アラートポートおよびジェネリックイベントポート	イベントの処理で使用するポート番号を指定します。デフォルトポートは 1234 です。
SMTP イベントポート	ハードウェアデバイスからシステムへ SMTP 経由でイベント情報を送信する際に使用するポート番号を指定します。デフォルトのポートは、ポート 25 です。
FTP イベントポート	ハードウェアデバイスとの FTP 通信に使用するポート。デフォルトのポートは、ポート 21 です。
ポーリング間隔[1/10]秒	少数のハードウェアデバイスを主に専用の入力/出力装置 『63ページ の"専用入力/出力デバイスについて"参照 』として使用する場合、システムは入力を検知するために、ハードウェアデバイスの入力ポートを定期的にチェックする必要があります。このような定期的な状態チェックを、ポーリングと呼びます。 状態チェックの間隔（1/10 秒単位）を指定することができます。デフォルト値は 10（1 秒）です。専用の入力/出力装置の場合、ポーリングの頻度を可能な限り低い値にすることを強く推奨します（状態チェックの間隔を 1/10 秒）。 どのハードウェアデバイスがポーリングを必要とするかに関する情報は、リリースノートを参照してください。

イベントおよび出力プロパティ

アナリティックイベントのテスト

分析種目を設定した後、要件 『116ページ の"アナリティックイベントをテストする(プロパティ)"参照 』、例えば、分析種目特性が Management Application に機能しているかどうかをテストできます。

1. 現行の分析種目を選んで下さい。
2. プロパティの中から、**「種目テスト」**ボタンをクリックして下さい。可能なすべての種目を示すウインドーが表示されます。



3. 種目テストのソースを、例えば、カメラを選んで下さい。そのウインドーは閉じられ、分析種目が機能するための四つの条件を満たす新しい画面が表示されます。

追加のテストとして、XProtect Smart Client で分析種目が種目サーバーに送信されたかどうか確認できます。そうするためには、XProtect Smart Client を開いて、**警告マネージャー**のタブの種目を表示します。

これも見て下さい。

分析種目について

アナリティックイベントをテストする(プロパティ)

アナリティック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?	**アナリティック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:変更を保存してください。

条件	説明	エラーメッセージと解決策
アナリティックイベントが有効です	アナリティックイベント機能は有効ですか?	**アナリティックイベントは有効ではありません。**解決策/説明:アナリティック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] > [アナリティックイベント]**をクリックし、**[有効]**チェックボックスを選択します。
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(アナリティック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:許可される IP アドレスまたはホスト名のアナリティックイベントアドレスリストに、使用しているマシンを追加します。 **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。
アナリティック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?	以下のテーブルを参照してください。

各ステップは失敗❌または成功で✓マークされます。

条件**アナリティックイベントの送信**に対するエラーメッセージと解決策:

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、イベントサーバーサービスが停止しているため、エラーが発生します。
アナリティック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¥XProtectEvent 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ックイベントです	イベントサーバー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。
イベントサーバーが無効なアナリティック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。	通常は、許可された IP アドレスまたはホスト名のリストにマシンがないためです。
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¥XProtectEvent 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¥XProtectEvent 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¥XProtectEvent 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。

ハードウェア入力イベント

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。詳細については、製品比較チャート『12ページ 』を参照してください。

ハードウェア入力イベントを追加 『110ページ の"ハードウェア入力イベントの追加"参照 』する場合、プロパティは選択した入力のタイプに依存する場合があります。

有効	選択したタイプの入力をシステムでイベントとして使用し、さらにプロパティを指定するには、このチェックボックスを選択します。
イベント名	名前を指定します。名前は一意であり、以下の特殊文字を含むことはできません。 < > & ' " ¥ / : * ?| [ ] 一部のカメラは、特定の長さおよび特定の構造のイベント名しかサポートしていません。詳細はカメラのマニュアルを参照してください。
カメラからの画像	システムでアラーム前後の画像を使用する場合のみ関係します。この機能は、選択したカメラでのみ使用可能であり、イベント発生の直前の画像をカメラから E メールで監視システムへ送信することができるようになります。 アラーム前後の画像は、使用しているシステムに固有のプリレコーディングおよびポストレコーディングの機能 『93ページ の"記録"参照 』と混同しないように注意してください。
プリアラーム画像の数	プリアラーム画像の必要数を指定します。許可された画像数は、カメラによって異なる場合があります。許可された範囲は、フィールドの右に表示されます。 選択したカメラでのみ使用可能な機能であるプレアラーム画像を使用している場合のみ、これが該当します。
1 秒当りのフレーム	プリアラーム画像を使用する場合にのみ関係します。プリアラーム画像は、選択したカメラでのみ使用可能な機能です。必要なフレームレートを指定します。このフィールドは、プリアラーム画像の数フィールドと組み合わせて使用し、イベントのどの程度前の期間からプリアラーム画像を受け取るかをコントロールできます。

このイベントが発生すると、E メールを送信します	E メール通知 『141ページ の"E メール通知の設定"参照 』が有効である場合のみ使用可能です。イベントが発生したときにシステムによってメールを自動的に送信する必要がある場合に選択します。受信者は、E メール通知の設定の一部として定義します。E メール通知を使用する場合、個々のカメラのスケジュールを忘れないでください。
カメラからの画像を添付します	E メール通知 『141ページ の"E メール通知の設定"参照 』が有効な場合にだけ使用できます。選択すると、イベントがトリガされた時に録画された画像が E メール通知に含められます。次に、チェックボックスの横にあるリストで関連するカメラを選択します。
削除	選択したイベントを削除します。
追加	特定のハードウェア入力イベントを選択している場合、追加をクリックすると、選択したハードウェア入力イベントにタイマーイベントが追加『112ページ の"タイマーイベントの追加"参照 』されます。
イベント発生時、SMS を送信する	イベントが発生したときにシステムによって SMS を自動的に送信する必要がある場合に、選択します。SMS 通知の受信者を、SMS 通知設定の一部として定義します。SMS 通知を使用する場合、個々のカメラのスケジュールが設定されている必要があることを忘れないでください。 設定を使用できるのは、SMS 通知が有効になっている場合だけです。

ハードウェア出力

ハードウェア出力を追加 『111ページ の"ハードウェア出力の追加"参照 』する時は、以下のプロパティを指定します。

出力名	名前を指定します。 ハードウェア出力をクライアントでの手動起動で使用できるようにする場合、これがクライアントユーザーに表示される名前となります。 名前は一意であり、以下の特殊文字を含むことはできません。 < > & ' " ¥ / : * ?| [ ] 一部のカメラは、特定の長さおよび特定の構造のイベント名しかサポートしていません。正確な情報については、当該カメラのマニュアルを参照してください。
出力接続先	ハードウェアデバイスのどの出力ポートに出力を接続するかを選択します。多くのハードウェアデバイスには出力ポートが 1 つしかありません。この場合は、**出力 1** を選択します。
出力維持時間	出力を適用する時間の長さを指定します。必要な時間の長さを、1/10 秒単位または秒単位で指定します。 一部のハードウェアデバイスは、たとえば最長で 5 秒などの比較的短い期間だけ、出力を適用することができます。正確な情報については、ハードウェアデバイスのマニュアルを参照してください。

ハードウェア出力が機能していることを確認するには、**出力のテスト**ボタンをクリックします。

手動イベント

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。詳細については、製品比較チャート『12ページ 』を参照してください。

手動イベントを追加 『111ページ の"手動イベントの追加"参照 』する場合、以下のプロパティを指定します。

[定義済みのグローバルイベントおよびカメラのリスト]	グローバルノードおよびすべての定義済みカメラのリストを含みます。必要に応じた数の手動イベントを設定できます。グローバルイベントであるか、カメラ固有であるかは問いません。グローバルノードの横に「+」記号がある場合、1 つまたは複数のグローバル手動イベントが既に設定済みであることを意味します。カメラの横に「+」記号がある場合、そのカメラに対して、1 つまたは複数の手動イベントが既に設定済みであることを意味します。
イベント名	名前を指定します。名前は一意であり、以下の特殊文字を含むことはできません。 < > & ' " ¥ / : * ?| [ ] 一部のカメラは、特定の長さおよび特定の構造のイベント名しかサポートしていません。詳細はカメラのマニュアルを参照してください。
このイベントが発生すると、E メールを送信します	E メール通知 『141ページ の"E メール通知の設定"参照 』が有効である場合のみ使用可能です。イベントが発生したときにシステムによってメールを自動的に送信する必要がある場合に選択します。受信者は、E メール通知の設定の一部として定義します。E メール通知を使用する場合、個々のカメラのスケジュールを忘れないでください。
カメラからの画像を添付します	E メール通知 『141ページ の"E メール通知の設定"参照 』が有効な場合にだけ使用できます。選択すると、イベントがトリガされた時に録画された画像が E メール通知に含められます。次に、チェックボックスの横にあるリストで関連するカメラを選択します。
削除	選択したイベントを削除します。
追加	新規イベントを追加します。**グローバル**または特定のカメラが選択されている場合、**追加**をクリックして、新しい手動イベントを追加します。特定の手動イベントが選択されている場合、**追加**をクリックすると、選択した手動イベントにタイマーイベントが追加 『112ページ の"タイマーイベントの追加"参照 』されます。
イベント発生時、SMS を送信する	イベントが発生したときにシステムによって SMS を自動的に送信する必要がある場合に、選択します。SMS 通知の受信者を、SMS 通知設定の一部として定義します。SMS 通知を使用する場合、個々のカメラのスケジュールが設定されている必要があることを忘れないでください。 設定を使用できるのは、SMS 通知が有効になっている場合だけです。

タイマーイベント

タイマーイベントを追加 『112ページ の"タイマーイベントの追加"参照 』する場合、以下のプロパティを指定します。

タイマーイベント名	名前を指定します。名前は一意であり、以下の特殊文字を含むことはできません。 < > & ' " ¥ / ：* ?| [ ] 一部のカメラは、特定の長さおよび特定の構造のイベント名しかサポートしていません。詳細はカメラのマニュアルを参照してください。
タイマーイベント発生前	メインイベントの発生からタイマーイベントまでに経過する必要がある時間の長さ（秒または分単位）を指定します。

ジェネリックイベント

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。詳細については、製品比較チャート『12ページ 』を参照してください。

ジェネリックイベントを追加 『113ページ の"ジェネリックイベントのテスト"参照 』する場合、以下のプロパティを指定します。

イベント名	名前を指定します。名前は一意であり、以下の特殊文字を含むことはできません。 < > & ' " ¥ / ：* ?| [ ] 一部のカメラは、特定の長さおよび特定の構造のイベント名しかサポートしていません。詳細はカメラのマニュアルを参照してください。
イベントポート	読み取り専用のフィールドで、システムがジェネリックイベントを受信待ちするポート番号を表示します（デフォルトはポート 1234）。ポート番号は、一般的なイベント処理の設定 『113ページ 』の一部として変更できます。
イベントの部分列	データパッケージを分析する際に、システムで探す個々の項目を指定することができます。1 つまたは複数の語を指定してから、**追加**ボタンをクリックして、指定した語をイベントメッセージの表現フィールドに追加すると、その内容が実際の分析で使用されます。例： • **単一の語：** User001（イベントメッセージの表現フィールドに追加すると、この語は「User001」と表示されます） • **複数の語を 1 つのアイテムとして：** User001 Door053 Sunday（イベントメッセージの表現フィールドに追加すると、この語は「User001 Door053 Sunday」と表示されます） 複数の語を 1 つのアイテムとして追加すると（例：イベントメッセージの表現フィールドでは「User001 Door053 Sunday」と表示）、引用符の間のすべてが、指定された順番でパッケージに表示され、条件との一致がチェックされます。語をパッケージとして表示する必要があっても順不同な場合、それぞれの語を 1 つずつ追加します（つまり、**イベント**メッセージの表現フィールドでは「User001」「Door053」「Sunday」と表示されます）。 ジェネリックイベントに使用する TCP および UDP パッケージには、分析する文字列で@、#、+、å、~等の特殊文字を使用することができます。

イベントメッセージの表現	実際のパッケージ分析で使用する文字列を表示します。このフィールドは、直接編集することはできません。ただし、追加ボタン、括弧、あるいは以下で説明するオペレータボタンをクリックする時に、カーソルをフィールド内に配置することで、新しいアイテムを含める場所を指定することができます。同様に、カーソルをフィールド内に配置することで、削除ボタンをクリックした時に、削除されるアイテムの場所を決めることもできます。削除ボタンをクリックすると、カーソルのすぐ左にあるアイテムが削除されます。 • （：開始括弧文字をイベントメッセージの表現フィールドに追加することができます。括弧は、関連用語が論理単位として同時に処理されるようにする際に使用します。つまり、分析で特定の処理順序を強制するために使用します。例：("User001" OR "Door053") AND "Sunday" を使用すると、括弧内の 2 つの用語が先に処理され、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」という用語を含むパッケージを参照し、その後に結果を取得し、「Sunday」という用語を含むパッケージを検索します。 • ）：終了括弧文字をイベントメッセージの表現フィールドに追加することができます。 • **AND**：AND 演算子をイベントメッセージの表現フィールドに追加することができます。AND 演算子により、AND 演算子の両側の用語が存在する必要があることを指定します。例：User001 AND Door053 AND Sunday を使用する場合、条件が満たされるためには、用語 User001 ならびに用語 Door053 ならびに用語 Sunday が存在しなければなりません。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。経験的に、AND で用語を結合すればするほど、復元結果は少なくなります。 • **OR**：OR 演算子をイベントメッセージの表現フィールドに追加することができます。OR 演算子により、いずれか 1 つの語句が存在する必要があることを指定します。例：User001 OR Door053 OR Sunday を使用する場合、条件が満たされるためには、用語 User001 または用語 Door053 または用語 Sunday が存在しなければなりません。いずれか 1 つの用語が存在すれば基準を満たします。一般原則として、OR で用語を結合すればするほど、取得される結果は多くなります。 • **削除**：イベントメッセージの表現フィールドに配置したカーソルのすぐ左にあるアイテムを削除することができます。カーソルをイベントメッセージの表現フィールドに配置していなければ、フィールドにある最後のアイテムが削除されます。
イベントの優先度	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、どのイベントをトリガするか管理することができます。0（最低優先度）～1000（最高優先度）の数値によって優先度を指定してください。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トリガされます。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トリガされます。

イベントプロトコル	イベントを検知するために、システムが受信待ちしなければならないプロトコルを選択します。 • **すべて：** TCP ならびに UDP のプロトコルを使用しているパッケージを受信待ち/分析します。 • **TCP：** TCP プロトコルだけを使用しているパッケージを受信待ち/分析します。 • **UDP：** UDP プロトコルだけを使用しているパッケージを受信待ち/分析します。
イベントルールタイプ	受信したデータパッケージを分析する時に、システムがあるべき特定の状態を選択します。 • **検索：** イベントを発生させるには、受信したパッケージに、イベントメッセージの表現フィールドで指定したメッセージ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すると、受信したパッケージに語句「User001」および「Door053」および「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、イベントがトリガされます。 • **一致：** イベントを発生させるには、受信したパッケージに、**イベント**メッセージの表現フィールドで指定したメッセージが正確に含まれていなくてはならならず、他の内容が含まれていてはなりません。
このイベントが発生すると、E メールを送信します	E メール通知 『141ページ の"E メール通知の設定"参照 』が有効である場合のみ使用可能です。イベントが発生したときにシステムによってメールを自動的に送信する必要がある場合に選択します。受信者は、E メール通知の設定の一部として定義します。E メール通知を使用する場合、個々のカメラのスケジュールを忘れないでください。
カメラからの画像を添付します	E メール通知 『141ページ の"E メール通知の設定"参照 』が有効な場合にだけ使用できます。選択すると、イベントがトリガされた時に録画された画像が E メール通知に含められます。次に、チェックボックスの横にあるリストで関連するカメラを選択します。
イベント発生時、SMS を送信する	イベントが発生したときにシステムによって SMS を自動的に送信する必要がある場合に、選択します。SMS 通知の受信者を、SMS 通知設定の一部として定義します。SMS 通知を使用する場合、個々のカメラのスケジュールが設定されている必要があることを忘れないでください。 設定を使用できるのは、SMS 通知が有効になっている場合だけです。
削除	選択したイベントを削除します。
追加	新規イベントを追加します。**ジェネリックイベント**ノードを選択中に**追加**をクリックすると、新しいジェネリックイベントが追加されます。特定のジェネリックイベントが選択されている場合、**追加**をクリックすると、選択したジェネリックイベントにタイマーイベントが追加 『112ページ の"タイマーイベントの追加"参照 』されます。

イベントでの出力コントロール（イベントおよび出力固有のプロパティ）

イベントでの出力コントロールを追加『112ページ の"イベントでのハードウェア出力の設定"参照 』する場合、以下のプロパティを指定します。

イベント	必要なイベントを選択します。
出力	関連する出力イベントを選択します。

スケジュールおよびアーカイブ

スケジュールについて

スケジュール機能により、以下を指定できます。

- アーカイブを実行する時
- 一部のカメラから、常にシステムにビデオを転送する
- 一部のカメラから、特定の期間だけ、あるいは特定のイベントが発生した場合にだけビデオを転送する
- システムから通知を受信するタイミング

すべてのカメラに対して、一般的なスケジュールプロパティをセットアップしたり、カメラごとに個別のプロパティをセットアップしたりすることも可能です。セットアップできる場合：

- 1 台または複数のカメラがオンラインであり、システムにビデオを転送する必要があります。
- 1 台または複数のカメラがスピードアップを使用していて、そのカメラが通常より高いフレームレートを使用している必要があります。
- 1 台または複数のカメラに関する通知を受信する場合
- アーカイブが発生した場合
- PTZ カメラは、パトロール設定に従って、パトロールを行う必要があります。

アーカイブについて

アーカイブは、統合された自動機能であり、この機能によって録画を移動し、新しい録画容量が確保できます。デフォルトでは、録画はそれぞれのカメラのデータベースに保存されます。それぞれのカメラのデータベースは、最大で 600,000 レコードまたは 40 GB を保持することができます。カメラのデータベースが満杯になると、システムは自動的に録画をアーカイブします。したがって、十分にアーカイブできる容量があることが重要です。

アーカイブを有効にするための特別な操作は必要ありません。アーカイブはバックグラウンドで実行され、システムがインストールされた瞬間から自動的に有効になり、実行されます。保存処理中にネットワーク関連の問題が生じるのを防ぐため、最新の録画はローカルストレージに保存されます。

システムのデフォルト設定では、1 日に 1 回またはデータベースが満杯になった時にアーカイブを行います。Management Application で、アーカイブがいつ、どれくらいの頻度で発生するかの設定を変更できます。また、アーカイブを最大で 1 日に 24 回まで、最低でも 1 時間の間隔でスケジュールすることもできます。こうすることで、データベースが満杯になる前に録画をアーカイブできます。大量の録画が予想される場合ほど、頻繁にアーカイブする必要があります。

また、個々のカメラのプロパティで、保持時間、すなわちカメラからの録画（カメラのデータベースにある録画ならびにアーカイブされた録画）を保持しておく時間を変更することも可能です。

カメラのデータベースが満杯になると、システムは自動的に録画をアーカイブします。一般的な**録画およびアーカイブ**パスのプロパティの一部として、**1 つの**時間制限（保持時間）を指定するだけです。保持時間によって、いつアーカイブが発生するかが決まることに注意してください。保持時間は、カメラからの録画（つまり、カメラのデータベースにある録画ならびにアーカイブされている録画）を保持しておく合計時間です。

アーカイブのバックアップ

Milestone では、共有違反やその他の誤動作の原因となることがあるため、カメラのデータベースの内容に基づいてバックアップを作成することは推奨していません。あるいは、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。個々のカメラに個々のアーカイブ場所を指定していない場合は、デフォルトのローカルアーカイブディレクトリである、**アーカイブ**にバックアップされます。

重要：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。

アーカイブが失敗する場合

まれなケースとして、たとえばネットワークの問題によって、アーカイブが失敗することもあります。ただし、これはシステムに脅威とはなりません。システムは、新しいデータベースを作成し、この新しいデータベースでアーカイブを続行できるからです。他のデータベースの場合と同様に、この新しいデータベースと古いデータベースの両方を操作し、表示することができます。

アーカイブの場所について

デフォルトアーカイブフォルダ『266ページ の"デフォルトのファイルパス"参照 』（C:¥MediaDatabase）は、システムサーバーにあります。デフォルトアーカイブフォルダをローカルの別の場所に変更したり、ネットワークドライブ上の場所を選択してデフォルトアーカイブフォルダとして使用することもできます。アーカイブフォルダでは、それぞれのカメラのアーカイブを保存するための別個のサブフォルダが自動的に作成されます。これらのサブフォルダは、カメラが接続されるハードウェアデバイスの MAC アドレスに基づいて名前が付けられます。

複数日に渡る録画のアーカイブを保持したり、アーカイブが 1 日に数回発生することもあるため、アーカイブの日付と時刻を含む名前を付けられたサブフォルダも自動的に作成されます。

サブフォルダは、以下の構成により名前が付けられます。

```
...¥Archives¥CameraMACAddress_VideoEncoderChannel¥DateAndTime
```

ビデオエンコーダーに複数のチャンネルがない場合は、ビデオエンコーダーチャンネルは常に「_1」になります（例：00408c51e181_1）。

例： MAC アドレスが 00408c51e181 であるカメラのチャンネル 2 に関する、2012 年 12 月 31 日の 23:15 のアーカイブの保存名：

```
C:¥MediaDatabase¥Archives¥00408c51e181_2¥2012-12-31-23-15
```

他の場所へのアーカイブについて

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、製品比較チャート『12ページ 』を参照してください。

デフォルトのアーカイブディレクトリ以外の場所へアーカイブする場合、システムはまずローカルのデフォルトアーカイブディレクトリにアーカイブを一時的に保存し、その後ただちに指定したアーカイブ場所へアーカイブを移動させます。ネットワークドライブに直接アーカイブすることは、使用可能なネットワークの帯域によってアーカイブ時間が大きく変動することを意味します。最初にアーカイブをローカルに保存してから移動すると、アーカイブ手順がスピードアップし、ネットワークの問題があった場合でも遅延を低減できます。

ネットワークドライブにアーカイブする場合、通常のカメラデータベースは、システムのサーバーに接続されているローカルドライブにしか保存できません。

ダイナミックアーカイブパスについて

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、製品比較チャート『12ページ 』を参照してください。

ダイナミックアーカイブパスでは、通常は複数のドライブに渡る、複数の異なるアーカイブパスを指定します。Milestone では、ビデオの録画設定ウィザードでカメラを設定する場合のデフォルト設定でもある、ダイナミックパス 『50ページ の"ストレージの設定ウィザード"参照 』を使用することを推奨しています。

ダイナミックアーカイブ用に選択したドライブのいずれかにカメラの録画パスが含まれている場合、システムは常にまずそのドライブにアーカイブしようと試みます。そうでない場合、カメラデータベースがそのドライブを使用していない限り、システムは自動的にその時点で最も使用可能な容量が大きいアーカイブドライブにアーカイブします。

使用可能な容量が最も大きいドライブはアーカイブプロセス中も変化するので、同一プロセスで複数のアーカイブドライブに対してアーカイブされることもあります。これにより、アーカイブされた録画をユーザーが検索し、再生する方法には影響を与えません。

ダイナミックアーカイブパスは一般にすべてのカメラに適用されます。個別のカメラ用にダイナミックアーカイブパスを設定することはできません。

ダイナミックアーカイブでどのドライブを使用するかを決定する場合、以下の例の良い点と悪い点を考慮してください（デフォルトアーカイブ パスはドライブ C:ですが、ドライブ文字はあくまでも一例であり、別のドライブ文字を指定することも可能です）。

- **カメラがドライブ C:に録画し、ドライブ C:にアーカイブする場合**

  ダイナミックアーカイブ用に選択したドライブのいずれかにカメラの録画パスが含まれている場合、システムはまずそのドライブにアーカイブしようと試みます。アーカイブは迅速に行われますが、ドライブがデータで満杯になるのも早くなります。

- **カメラがドライブ C:に録画し、ドライブ D:にアーカイブする場合：**

  録画とアーカイブは、別のドライブになります。アーカイブは、それほど迅速には行われません。システムは、まず一時的に C:ドライブにあるローカルデフォルトアーカイブディレクトリにアーカイブを保存し、その後すぐにアーカイブを D:ドライブにあるアーカイブ場所に移動させます。したがって、C:ドライブには、一時的アーカイブに対応できる十分な容量が必要です。

- **カメラ 1 がドライブ C:に録画し、ドライブ D:にアーカイブする場合：一方、カメラ 2 はドライブ D:に録画し、ドライブ C:にアーカイブする場合**

  このパターンは避けてください。あるカメラのアーカイブが、他のカメラの録画に必要な容量を奪ってしまう可能性があります。上記の例では、カメラ 1 のドライブ D:へのアーカイブによって、ドライブ D:にはカメラ 2 の録画容量が無くなることがあります。ルールは、「録画およびアーカイブのドライブを交差させない」ということになります。

複数の監視サーバーをマスター/スレーブの設定で使用する場合、アーカイブが機能するために、それぞれの監視サーバーは独自に割り当てられた場所にアーカイブする必要があります。すべてのサーバーが同じマップ場所にアーカイブしようとすると、アーカイブは失敗します。

音声のアーカイブについて

ハードウェアデバイスで音声ソース（例、マイク）が有効になっている場合、音声録音は、ハードウェアデバイスに取り付けられたカメラからのビデオ録画と共にアーカイブされます。ハードウェアデバイスが、複数のチャンネルを持つビデオエンコーダーである場合、音声はチャンネル 1 のカメラと共にアーカイブされます。音声ソ

ースが有効になってている場合、システムは関連するカメラのデータベースに音声を録音します。これは、データベースがビデオを保存できる容量に影響します。したがって、音声とビデオを記録する際は、ビデオだけを録画する場合より頻繁にアーカイブをスケジュールする必要があります。

アーカイブに必要なストレージ容量

アーカイブに必要なストレージ容量は、保存する予定の録画の容量と、どれだけの期間保存するか（保持時間）に完全に依存します。一部の組織では、多数のカメラからのアーカイブ録画を数か月または数年に渡って保存する必要があります。他の組織では、1 台または 2 台のカメラからの録画のアーカイブだけが必要であり、保存したい期間もより短い場合があります。

直後に他のドライブにあるアーカイブ場所に移動される場合にも、まずはアーカイブされた録画が必ず移動されるデフォルトアーカイブディレクトリを含んでいる**ローカル**ドライブの保存容量を常に検討する必要があります。基本的には、ローカルドライブの容量は、少なくともすべてのカメラのデータベースを保存するのに必要な容量の 2 倍が必要になります。

アーカイブする場合、システムは、アーカイブするデータに必要な容量に 1 GB を加えた空きディスク容量がカメラのアーカイブ場所にあるか自動的にチェックします。それだけの空き容量がない場合、アーカイブする新しいデータに十分な空き容量が得られるまで、アーカイブの場所で、関連するカメラの最も古いデータが削除されます。

アーカイブに必要なストレージ容量を推定する場合、まず組織のニーズを考慮し、次にベストケースではなくワーストケースのシナリオを想定するようにしてください。

ヒント： Milestone の Web サイト『http://www.milestonesys.com』のサポートセクションにあるストレージ計算機を使うと、監視システムに必要なストレージ容量を決定するのに便利です。

アーカイブスケジュールについて

アーカイブスケジュールを設定する方法には、次の 2 種類があります。

- ビデオおよび録画の設定ウィザード 『50ページ の"ストレージの設定ウィザード"参照 』でカメラを設定する場合、アーカイブスケジュールはウィザードの**ドライブ選択**ページで設定します。
- 一般的なスケジュールおよびアーカイブのプロパティの一部として、**詳細設定**を展開し、**スケジュールおよびアーカイブ**を右クリックして、**プロパティ**を選択します。ダイアログで**アーカイブ**を選択して、関連するプロパティ 『132ページ の"アーカイブ"参照 』を指定します。

ディスク空き容量が不足した場合の自動応答

アーカイブ中にシステムのディスク空き容量が不足した場合のために、自動応答をセットアップできます。カメラのデータベースドライブがアーカイブドライブとは異なる場合と、同じ場合によって、次の 2 つのシナリオが発生します。

同じドライブである場合：ドライブのディスク空き容量がなくなった場合、アーカイブを自動的に移動または削除

システムサーバーのディスク空き容量が不足し、アーカイブドライブがカメラのデータベースドライブと同一である場合、システムは自動的に空き容量を作るための試行を数回行います。こうした試行の大半では、アーカイブまたはデータベースからデータが失われます。

- まず、システムはアーカイブを移動させようとします。複数の異なるドライブにアーカイブできる、ダイナミックアーカイブを使用している場合にのみ、アーカイブを移動できます。これが発生するのは、以下の場合です。

- 空きディスク容量が 15%を下回っており、使用可能なディスク容量が 40 GB + カメラ 1 台につき 2 GB を下回っている。

  - または -

- 使用可能なディスク容量が 225 MB + カメラ 1 台につき 30 MB を下回っている。例 : 10 台のカメラで、使用可能なディスク容量が 525 MB（225 MB + 10 台のカメラのそれぞれで 30 MB）を下回ると、サーバーの空きディスク容量が不足します。

この差によって、単に残りのディスク容量が 15%未満となるので、非常に大きなディスクではディスク容量の不足を考える必要はありません。

- システムによりアーカイブを移動できない場合、最も古いアーカイブを削除しようとします。これが発生するのは、以下の場合です。

  - 空きディスク容量が 10%を下回っており、使用可能なディスク容量が 30 GB + カメラ 1 台につき 1.5 GB を下回っている。

  - または -

  - 使用可能なディスク容量が 150 MB + カメラ 1 台につき 20 MB を下回っている（例 : 10 台のカメラで、使用可能なディスク容量が 350 MB（150 MB + 10 台のカメラのそれぞれで 20 MB）を下回ると、サーバーの空きディスク容量が不足します。

  この差によって、単に残りのディスク容量が 10%未満となるので、非常に大きなディスクではディスク容量の不足を考える必要はありません。

- 削除できるアーカイブがない場合、システムは最も古い録画を削除してカメラのデータベースのサイズを変更しようとします。これが発生するのは、以下の場合です。

  - 空きディスク容量が 5%を下回っており、使用可能なディスク容量が 20 GB + カメラ 1 台につき 1 GB を下回っている。

  - または -

  - 使用可能なディスク容量が 75 MB + カメラ 1 台につき 10 MB を下回っている（例 : 10 台のカメラで、使用可能なディスク容量が 175 MB（75 MB + 10 台のカメラのそれぞれで 10 MB）を下回ると、サーバーの空きディスク容量が不足します。

  この差によって、単に残りのディスク容量が 5%未満となるので、非常に大きなディスクではディスク容量の不足を考える必要はありません。

データベースのサイズを変更した後、システムがレコーディングサーバーを再起動した場合、ドライブのサイズの問題が解消されていることを確認するか、カメラのデータベースのサイズを調整して、変更されたドライブサイズを反映するようにしてください。

システムがデータベースのサイズ変更手順を実行すると、XProtect Smart Client の画面、ログファイルに情報が表示されます。あるいは通知（セットアップされている場合）が送られます。

異なるドライブ：自動アーカイブ：データベースドライブのディスク容量が不足した場合。

システムサーバーのディスク容量が不足しており、アーカイブドライブがカメラのデータベースドライブと**異なっており**、過去 1 時間以内にアーカイブが行われていない場合、アーカイブは自動的にディスクの空き容量を開放しようとします。これは、アーカイブスケジュールに関わらず行われます。以下の場合、サーバーのディスクの空き容量が不足していると考えられます。

- 空きディスク容量が 10%を下回っており、使用可能なディスク容量が 30 GB + カメラ 1 台につき 1.5 GB を下回っている。

- 使用可能なディスク容量が 150 MB + カメラ 1 台につき 20 MB を下回っている。例:10 台のカメラで、使用可能なディスク容量が 350 MB（150 MB + 10 台のカメラのそれぞれで 20 MB）を下回ると、サーバーの空きディスク容量が不足します。

この差によって、単に残りのディスク容量が 10%未満となるので、非常に大きなディスクではディスク容量の不足を考える必要はありません。

アーカイブドライブで、システムは、カメラからのデータをアーカイブするのに必要な容量に、カメラ当たり 1 GB を加えた空きディスク容量があるかチェックします。それだけの空き容量がない場合、アーカイブする新しいデータに十分な空き容量が得られるまで、アーカイブドライブで、関連するカメラの最も古いデータが削除されます。

アーカイブされた録画の再生について

アーカイブされた録画は、XProtect Smart Client で再生できます。たとえば、アーカイブされた録画に対してエクスポートやブラウズを行うことができます。

ローカルまたはネットワークのドライブに保存されているアーカイブされた録画に対して、XProtect Smart Client の再生機能を使用して、カメラの通常のデータベースに保存されている録画と同様に、関連する録画を検索や再生することができます。また、XProtect Smart Client で、エクスポートされたアーカイブや、ローカルドライブまたはネットワークドライブ以外に保存されているアーカイブを使用することもできます。詳細については、マニュアルとガイドをダウンロードする Milestone Web サイト『http://www.milestonesys.com/support/manuals-and-guides/』にある XProtect Smart Client ドキュメントを参照してください。

一般的なスケジュールおよびアーカイブの設定

一般的なスケジュールおよびアーカイブを設定するには、次の手順を実行してください。

1. **詳細設定**を展開し、**スケジュールおよびアーカイブ > プロパティ**を右クリックします。
2. すべてのカメラのスケジュール 『129ページ 』、スケジュールオプション 『131ページ 』、アーカイブ 『132ページ 』で必要なプロパティを指定します。
3. システムには、2 つの基本スケジュールプロファイル（**常にオン**と**常にオフ**）があり、これらを編集または削除することはできません。これらが組織のニーズに合わない場合、それぞれのカメラに対してカスタマイズされたスケジュールプロファイルを複数作成できます。カスタマイズされたスケジュールプロファイルは、必要に応じて複数の目的で再利用できます。
4. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

アーカイブ時には、カメラのデータベースやアーカイブ場所でのウイルススキャン 『16ページ の"ウイルススキャンについて"参照 』を無効にしてください。

一般的なスケジュールのプロパティ

すべてのカメラのスケジュール

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。詳細については、製品比較チャート『12ページ 』を参照してください。

一般的なスケジュールおよびアーカイブ『129ページ の"一般的なスケジュールおよびアーカイブの設定"参照 』を設定する場合、多くのカメラに対して一定のプロパティを同時に指定することができます。操作を迅速に行い

たい場合や、対象となるプロパティが、個別のカメラではなく、すべてのカメラで共有されている場合が該当します。

オンライン期間、スピードアップ、通知（E メールおよび SMS）、PTZ パトロールなどのプロパティは、それぞれのカメラに対して個別に指定することができます。

テンプレート	複数のカメラがシステムに接続していると、テンプレートでカメラの類似したプロパティを設定し、設定を変更する時間を短縮できます。 例：たとえば、カメラが 20 台あり、録画パス、アーカイブ パス、およびそれらすべての保持期間を変更するとします。使用する設定を 1 回入力し、テンプレートを 20 台のカメラに適用し、すべてのカメラに同じ設定があることを確認します。
テンプレートを適用	どのカメラにテンプレートを適用するか選択します。2 つの**設定**ボタンのいずれかを使用して、テンプレートに適用します。
カメラ	Management Application およびクライアントで表示される名前です。
オンライン	関連するカメラのオンラインスケジュール『71ページ の"特定カメラスケジュールの構成"参照 』に必要なプロファイル（例：**常にオン**）を選択します。 以下に基づいてスケジュールを作成して、カメラのオンライン期間を指定します。 • 期間（例：月曜日の 08:30 から 17:45 まで）、ピンク色で表示：  • 期間内のイベント（例：イベント A の発生からイベント B の発生まで、月曜日の 08:30 から 17:45 まで）、黄色で表示：  2 つのオプション  を組み合わせることができますが、時間で重複することはできません。
E メール	対象となるカメラの E メール通知スケジュールに必要なプロファイルを選択します。 期間に基づいてスケジュールプロファイルを作成することで、カメラの E メール通知の期間を指定します。 例：月曜日の 08:30 から 17:45 まで、青色で表示： 
全て選択	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラを選択します。
全てクリアする	ボタンをクリックして、**テンプレートを適用**列にあるすべてのカメラの選択を解除します。
選択したカメラで、選択したテンプレートの値を設定する	テンプレートから選択した値だけを、選択したカメラに適用します。
新規スケジュールプロファイル	**作成...**ボタンをクリックして、任意のタイプの新しいスケジュールプロファイルを作成します。
SMS	対象となるカメラの SMS 通知スケジュールに必要なプロファイルを選択します。 期間に基づいてスケジュールプロファイルを作成することで、カメラの SMS 通知期間を指定します。 例：月曜日の 08:30 から 17:45 まで、緑色で表示： 

PTZ パトロール	PTZ カメラのパトロールは、複数のプリセット位置の間での PTZ カメラの連続的な動きでのみ使用可能です。 対象となるカメラの PTZ パトロールスケジュール 『133ページ の"PTZ パトロール"参照 』に必要なプロファイルを選択します。 特定の期間内でのパトロールプロファイルに基づいて、カメラのパトロールスケジュールを指定します（例：月曜日の 08:30 から 17:45 まで）、赤色で表示：

スケジュールオプション

一般的なスケジュールおよびアーカイブ『129ページ の"一般的なスケジュールおよびアーカイブの設定"参照 』を設定する場合、多くのカメラに対して一定のプロパティを同時に指定することができます。スケジュールオプションを使用するのは、プロパティがすべてのカメラによって共有されているためです。

クライアント要求時のカメラ起動	たとえば、オンライン録画スケジュール 『132ページ の"オンライン期間"参照 』の終了日時に達したなどの理由でカメラがオフラインになっている場合、クライアントユーザーはカメラからのライブビデオを表示することができません。 **クライアント要求時のカメラ起動**を選択すると、クライアントユーザーは、オンラインスケジュール外でも、録画することなくカメラからのライブビデオを表示することができます。技術的には、オンラインスケジュール外で、カメラを強制的にオンラインにします。 カメラの起動と連動して録画も開始したい場合は、**クライアントからの要求で開始した際に録画を有効にする**を選択する必要があります（以下を参照）。
クライアントからの要求で開始した際に録画を有効にする	**クライアントからの要求によるカメラ起動**を選択している場合に、カメラ起動時の録画連動を有効化できます（前項目を参照）。 手動録画の権限 『163ページ の"カメラアクセス"参照 』を持たないユーザーの場合、**クライアントからの要求で開始した際に録画を有効にする**を有効化しても、そのユーザーによる手動録画を**行うことができません**。
新規カメラのスケジュールプロファイル	後でシステムに追加するカメラをデフォルトとして使用するオンラインスケジュールプロファイルを選択します。この選択が適用されるのはオンラインスケジュールだけであり、他のスケジュールには適用されないことに注意してください。デフォルトの選択は、**常にオン**です。つまり、新しいカメラは常にオンラインであり、ライブ表示やその他の処理のためにビデオをシステムのサーバーに転送します。
再接続試行間の最大遅延	再接続試行の積極性を調整します。システムがカメラへの接続を失うと、デフォルトでは、10 秒後に接続の再確立を試行します。 ワイヤレス接続で車載カメラを使用している場合など、一部の環境ではカメラの接続が頻繁に失われる可能性があるため、再試行の試みの積極性を変更することを検討してください。

オンライン録画スケジュール設定がない場合でも、ライブ映像を見たり、ビデオの録画を開始したりすることもできます。これを行うには、**クライアント要求時のカメラ起動**を選択し、必要に応じて、該当のカメラでスケジュールプロパティをセットアップする際に、以下の**クライアントからの要求で開始した際に録画を有効にする**オプションを選択します。

アーカイブ

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、製品比較チャート『12ページ 』を参照してください。

システムがアーカイブするタイミングとエラー時にシステムが応答する方法を制御するには、次の設定を調整します。カメラのデータベースが満杯になると、システムは自動的に録画をアーカイブ 『124ページ の"アーカイブについて"参照 』します。

アーカイブ時刻	システムで自動的に録画をアーカイブパスへ移動させる時刻を指定します。1 日に最大で 24 件のアーカイブ時刻を指定できますが、最低でも 1 時間の間隔が必要です。時間、分、秒の値を選択してから、**上**および**下**ボタンをクリックして値を増減させるか、単に選択した値に上書きして、**追加**をクリックします。大量の録画が予想される場合ほど、頻繁にアーカイブする必要があります。
アーカイブ障害時に E メールを送信	これを選択した場合、アーカイブが失敗すると、システムは、選択した受信者に自動的に E メールを送信します。E メール通知機能も有効にする必要があります。受信者は、E メール通知のプロパティ 『142ページ の"E メール（プロパティ）"参照 』の一部として定義します。
アーカイブ障害時に SMS を送信	アーカイブが失敗した場合に、SMS を自動送信する必要があれば選択します。SMS 通知の受信者を、SMS 通知設定の一部として定義します。 設定を使用できるのは、SMS 通知が有効になっている場合だけです。
イベントでのアーカイブ	選択すると、特定のイベントが発生したときに、システムによってアーカイブが開始されます。リストからイベントを選択します。

カメラ固有のスケジュールプロパティ

オンライン期間

特定のカメラのスケジュール 『71ページ の"特定カメラスケジュールの構成"参照 』を設定する際に、次の項目を指定することができます。

オンライン	関連するカメラのオンラインスケジュール『71ページ の"特定カメラスケジュールの構成"参照 』に必要なプロファイル（例：**常にオン**）を選択します。 以下に基づいてスケジュールを作成して、カメラのオンライン期間を指定します。 • 期間（例：月曜日の 08:30 から 17:45 まで）、ピンク色で表示：  • 期間内のイベント（例：イベント A の発生からイベント B の発生まで、月曜日の 08:30 から 17:45 まで）、黄色で表示：  2 つのイベントを組み合わせることは可能ですが  、時間を重複することはできません。

ほとんどのユーザーにとって、**オンライン期間**設定は最も重要なスケジュール設定であると考えられます。スケジュール設定は、カメラがビデオをシステムに転送するタイミングを決定するためです。

デフォルトでは、システムに追加されたカメラは自動的にオンラインになるので、特定の時刻やイベントに際してのみカメラをオンラインにしたい場合にだけ、オンライン期間の設定を変更します。後で追加されたカメラが自動的にオンラインにならない場合は、一般的なスケジュールオプション 『131ページ の"スケジュールオプション"参照 』の一部として、このデフォルト設定を変更することができます。

カメラが使用しているシステムにビデオを転送する事実は、必ずしもカメラからビデオが録画されることを意味しません。個別に録画を設定します。ビデオと録画の設定 『69ページ の"ビデオや録画の設定について"参照 』を参照してください。

オンライン録画スケジュール以外のカメラからライブ映像を見たり、録画ビデオを再生したりする場合は、クライアント要求時のカメラ起動 『131ページ の"スケジュールオプション"参照 』を選択し、クライアントからの要求で開始した際に録画を有効にする 『131ページ の"スケジュールオプション"参照 』オプションで、関連するカメラのスケジュールプロパティをセットアップします。

スピードアップ

特定の MJPEG カメラのスピードアップ期間を指定します。このタイプのスケジュールを定義できるようにするためには、スピードアップを有効 『83ページ の"フレームレート - MJPEG"参照 』にする必要があります。

スピードアップ	期間に基づいてスケジュールプロファイルを作成することで、カメラのスピードアップの期間を指定します（例：月曜日の 08:30 から 17:45 まで）、オリーブグリーン色で表示：

スピードアップはイベントに基づいて実行される場合もありますが、他で設定されている場合に限ります。フレームレート - MJPEG（一般的な録画およびストレージのプロパティ）『83ページ の"フレームレート - MJPEG"参照 』およびビデオ（カメラ固有のプロパティ） 『90ページ の"ビデオ"参照 』を参照してください。

PTZ パトロール

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。詳細については、製品比較チャート『12ページ 』を参照してください。

パトロール 『102ページ の"PTZ パトロール（プロパティ）"参照 』に対応している PTZ（パン/チルト/ズーム）カメラのスケジュール 『71ページ の"特定カメラスケジュールの構成"参照 』を設定する場合、特定の時刻にどのパトロールプロファイルを使用するかを指定できます。このタイプのスケジュールを設定する前に、関連するカメラのパトロールを設定する必要があります。

PTZ パトロール	PTZ パトロール機能がある PTZ カメラでのみ使用できます。 対象となるカメラの PTZ パトロールスケジュール 『133ページ の"PTZ パトロール"参照 』に必要なプロファイルを選択します。 特定の期間内でのパトロールプロファイルに基づいて、カメラのパトロールスケジュールを指定します（例：月曜日の 08:30 から 17:45 まで）、赤色で表示：

使用するパトロールプロファイルのすぐ後に、別のパトロールプロファイルの使用。例：日中のパトロールプロファイルが月曜日の 08:30 から 17:45 まで、その後に夜間のパトロールプロファイルが月曜日の 17:45 から 23:00 まで続けることもできます。使用する 2 つのパトロールプロファイル時間を重複することはできません。

他のタイプのスケジュールとは違って、PTZ パトロールのスケジュールプロファイルには、**常にオン**や**常にオフ**などの事前に決められたスケジュールプロファイルはありません。それぞれのカメラに対して、任意の数のカスタマイズされたスケジュールプロファイルを作成できます。あるカメラに対してカスタマイズされたスケジュー

ルプロファイルを作成 『71ページ の"特定カメラスケジュールの構成"参照 』すると、必要に応じて、それを他のカメラで使用する事も可能です。

Matrix

Matrix ビデオの共有について

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、製品比較チャート『12ページ 』を参照してください。

Matrix 機能により、任意のカメラから、使用しているシステムで作動しているネットワーク上の Matrix 受信 PC へのライブビデオの配信表示が可能になります。Matrix によってトリガされたビデオが表示できるコンピュータは、Matrix 受信 PC と呼ばれます。Matrix 受信 PC にするには、コンピュータに XProtect Smart Client をインストールする必要があります。

Matrix ビデオの共有に関する詳細は、Milestone Web サイト 『http://www.milestonesys.com/』から入手できる XProtect Smart Client のユーザーズマニュアル、または XProtect Smart Client に組み込まれているヘルプシステムを参照してください。

Matrix でトリガされたビデオのいずれが、Matrix 受信 PC で表示されるかを確認するには、以下の 2 つの方法があります。

- **手動トリガ**: 他のユーザーが重要なビデオを共有する場合、そのビデオを XProtect Smart Client から、あるいはカスタマイズされている Web ページから、必要な Matrix 受信 PC へ送信します。
- **自動トリガ**: 事前定義イベントが発生すると、ビデオは関連する Matrix 受信 PC へ自動的に送信されます。たとえば、ドアが開いたことをドアセンサーが検知した場合、あるいは監視システムがカメラからのビデオでモーションを検知した場合などです。

Matrix 受信 PC について

Matrix 受信者は、Matrix によってトリガされたビデオが表示できるコンピュータです。Matrix 受信者にするには、コンピュータに XProtect Smart Client をインストールする必要があります。

Matrix でトリガされたビデオのいずれが、Matrix 受信 PC で表示されるかを確認するには、以下の 2 つの方法があります。

- **手動トリガ**: 他のユーザーが重要なビデオを共有したい場合、そのビデオを XProtect Smart Client から、あるいはカスタマイズされている Web ページから、必要な Matrix 受信 PC へ送信します。
- **自動トリガ**: 事前定義イベントが発生すると、ビデオは関連する Matrix 受信 PC へ自動的に送信されます。たとえば、ドアが開いたことをドアセンサーが検知した場合、あるいは監視システムがカメラからのビデオでモーションを検知した場合などです。
- Matrix 受信者に関する詳細は、Milestone Web サイト『http://www.milestonesys.com/』から入手できる XProtect Smart Client のユーザーズマニュアル、または XProtect Smart Client に組み込まれているヘルプシステムを参照してください。

Matrix の設定

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、製品比較チャート『12ページ 』を参照してください。

1. **詳細設定**を展開し、**Matrix** を右クリックし、**プロパティ**を選択します。
2. **Matrix の有効化**チェックボックスを選択すると、Matrix が使用可能になります。
3. 必要なプロパティ 『135ページ の"Matrix 受信 PC"参照 』を指定するか、あるいは自動的にトリガされたビデオ共有に対して、**Matrix イベントコントロール**を選択し、Matrix イベントコントロールプロパティ 『136ページ の"Matrix イベントコントロール"参照 』を設定します。準備ができたら **OK をクリックします。**
4. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

Matrix のプロパティ

Matrix 受信 PC

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、製品比較チャート『12ページ 』を参照してください。

Matrix 受信 PC タブを使用して、Matrix 機能を有効にし、Matrix によってトリガされたライブビデオを表示するコンピュータを定義します。Matrix によってトリガされたビデオが表示できるコンピュータは、Matrix 受信 PC と呼ばれます。Matrix によってトリガされたビデオを表示できるようにするには、ユーザーのコンピュータに XProtect Smart Client がインストールされていることが必要です。

有効 Matrix	チェックボックスを選択すると、Matrix 機能が有効になります。
[定義済み Matrix 受信者のリスト]	既に定義されている Matrix 受信者、つまり Matrix がトリガするビデオを表示できるコンピュータをリスト表示します。 既に定義されている Matrix 受信者のプロパティを変更するには、該当する Matrix 受信者を選択し、リストの下にあるフィールドで変更を行ってから、**更新**ボタンをクリックします。 リストから Matrix 受信者を削除するには、不要な Matrix 受信者を選択してから、**削除**ボタンをクリックします。
名前	Matrix 受信者の名前です。 新しい Matrix 受信者を追加するか、既存の受信者のプロパティを編集する際に使用します。日常的なさまざまな使用状況で、名前が表示されます。Milestone は、わかりやすく覚えやすい名前を使用することをお勧めします。 名前は一意であり、以下の特殊文字を含むことはできません。 < > & ' " ¥ / : * ?| [ ]
アドレス	Matrix 受信者の IP アドレス。新しい Matrix 受信者の追加や、既存の受信者のプロパティの編集に使用します。
ポート	Matrix 受信者にコマンドを送信する際に使用するポート番号を指定します。 新しい Matrix 受信者を追加するか、既存の受信者のプロパティを編集する際に使用します。Matrix 受信者は、このポートのコマンドを受信待ちします。デフォルトでは、ポート 12345 を使用します。必要に応じて、ポート番号を変更できます。

パスワード	Matrix 受信者と通信する際に使用するパスワードを指定します。新しい Matrix 受信者を追加するか、既存の受信者のプロパティを編集する際に使用します。
Matrix 受信者は、XProtect Smart Client	関連する Matrix 受信者が XProtect Smart Client である場合に選択します。XProtect Smart Client を使用している場合、Matrix がトリガするビデオの配信は少し異なります。
クリア	**名前**、**アドレス**、**パスワード**のフィールドの内容を削除します。
更新	選択した Matrix 受信者のプロパティを、編集した内容で更新します。使用できるのは、既存の Matrix 受信者のプロパティが編集されている場合のみです。
追加	新しい Matrix 受信者をリストに追加します。使用できるのは、新しい Matrix 受信者のプロパティを、**名前**、**アドレス**、**ポート**、**パスワード**、および XProtect Smart Client のフィールドに追加する場合のみです。

Matrix イベントコントロール

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。詳細については、製品比較チャート『12ページ 』を参照してください。

Matrix イベントコントロールタブを使用して、事前定義イベントに基づくライブビデオの自動送信を設定します。Matrix 受信 PC ごとに、どのイベントやカメラを使用するか、正確に定義することができます。**Matrix イベントコントロール**タブには、**Matrix 受信 PC** タブで定義した Matrix 受信 PC のリストが表示されます。

Matrix 受信 PC を右クリックすると、イベントに属しているデバイスのリストが表示されます。イベントを選択すると、まず赤い感嘆符（!）で強調表示され、追加設定ができることを示します。イベントを右クリックすると、選択したイベントのオプションのリストが表示されます。

削除［選択したイベント］	選択したデバイスで、選択したイベントを削除します。
接続	カメラに接続します（実際のカメラは、取るべきアクションを選択した後に指定します）。
遮断、続いて接続	既存の接続を切断し、その後再度接続します。 このオプションによって、ライブビデオは先入れ先出しで Matrix 受信者に表示されます。新しいイベントが発生するたびに、最新のイベントからのビデオが Matrix 受信者の特定の部分に優先的に表示され、同時に、古いイベントからのビデオはあまり優先的ではない場所へ移動され、最終的には、より新しいイベントのビデオのためのスペースを作るために、Matrix 受信者から「プッシュアウト」されます。 **接続**オプションでは、既に Matrix 受信者に表示された、あるカメラでのイベントによってビデオがトリガされることがあります。同じカメラで、別のイベントによってトリガされたビデオは、最新のイベントからのビデオほどは優先的に表示されません。これは単に、Matrix 受信者には、そのカメラからのビデオがあまり優先的ではない位置で表示されているためです。 **切断を選択し、それから接続することで、**この問題を回避し、最新のイベントからのビデオが常に優先的に表示されるようにすることができます。
遮断	既存の接続をすべて切断します。ビデオが Matrix 受信者から「プッシュアウト」されるほど古くないにもかかわらず、特定のイベントの使用が Matrix 受信者でのビデオ表示の停止の原因となる場合は、このオプションを使用してください。

接続を選択すると、別の赤い感嘆符（!）が表示され、まだ一部の設定が未完了であることを示します。アクションを右クリックして、アクションを適用するカメラを選択します。

この例では、カメラ B でモーションを検知した時に、選択した Matrix 受信 PC がカメラ B に接続されるように指定しています。

ログ

ログについて

システムは、システム機能の活動を示すさまざまなログを生成します。このシステムでは、以下のタイプのログが使用できます。

名前	詳細
Management Application ログファイル	Management Application の活動を表示する。システムは、Management Application を一日使用するたびに新しいログを作成します。 このタイプのログは無効にはできません。Management Application ログファイルの名前は、AdminYYYYMMDD.log という構造になります。たとえば、Admin20091231.log などです。
Recording Server サービスログファイル	Recording Server サービスの活動を示します。このサービスを使用すると、1 日ごとに新しいログファイルが作成されます。 このタイプのログは無効にはできません。Recording Server サービスログファイルの名前は、RecordingServerYYYYMMDD.log という構造になります。たとえば、RecordingServer20091231.log などです。
Image Server サービスログファイル	Image Server サービスの活動を示します。このサービスを使用すると、1 日ごとに新しいログファイルが作成されます。 このタイプのログは無効にはできません。Image Server サービスログファイルの名前は、ISLog_YYYYMMDD.log という構造になります。たとえば、ISLog_20091231.log などです。

名前	詳細
Image Import サービスログファイル	Image Import サービスの活動が示されます。このサービスはプリアラーム画像を取り込んだり、取り込んだ画像をカメラのデータベースに保存したりする際に使用されます。 プリアラーム画像は、選択したカメラでのみ使用可能な機能です。イベントが発生する直前の画像を、カメラから監視システムへ E メールで送信することができます。このサービスを使用すると、1 日ごとに新しいログファイルが作成されます。 このタイプのログは無効にはできません。Image Import サービスログファイルの名前は、ImageImportLog_YYYMMDD.log という構造になります。たとえば、ImageImportLog20091231.log などです。
イベントログファイル	登録されているイベントの活動を示します。イベントが発生した日ごとに、新しいログファイルが作成されます。 このタイプのログは無効にはできません。イベントログファイルを表示するには、XProtect Smart Client（**再生**タブの**アラート**セクションを使用）を使用する必要があります。
監査ログファイル	XProtect Smart Client ユーザーの活動を示します（監査ログが有効である場合）。 監査ログが有効であれば、毎日クライアントユーザーが活動した日ごとに、新しいログが作成されます。監査ログファイルの名前は、_auditYYYMMDD.log という構造になります。たとえば、_audit20091231.log などです。「_」は、監査ログが Image Server サービスによって生成された事実を示す接頭辞です。

ログの場所

すべてのログファイルは、デフォルトでは、使用しているオペレーティングシステムで該当する**すべてのユーザー**フォルダに配置されます。デフォルトでは、7 日間保存されます。ログを設定する際に、ログファイルの場所や、ログを保存しておく日数を変更することができます。

ログの構造

システムによって生成されるログファイルの大半は、W3C 拡張ログファイル形式に準拠した共有構造を使用しています。それぞれのログファイルは、ヘッダーおよび複数のログ行で構成されます。

- ヘッダーには、ログ行に含まれている情報の概要が示されます。
- ログ行は、主に 2 つの部分で構成されます。ログ自身の情報ならびに暗号化部分です。暗号化部分は、復号化し、比較することによって、ログファイルが改ざんされていないことを確認できます。

ログの整合性チェック

Management Application ログファイル以外のすべてのログファイルは、24 時間ごとに整合性チェックを受けます。整合性チェックは、システムの Log Check サービスによって実行されます。整合性チェックの結果は、LogCheck_YYYYMMDD.log というファイル名構造のファイルに自動的に書きこまれます。たとえば、LogCheck_20091231.log などとなります。ログファイルと同様、ログチェックファイルも、デフォルトでは、使用しているオペレーティングシステムの該当する**すべてのユーザー**フォルダに配置されます。

矛盾があると、ログチェックファイルに書かれたエラーメッセージの形式でレポートされます。

考えられるエラーメッセージ：

名前	詳細
ログの整合性情報が見つかりませんでした。ログの整合性は保証できません。	ログファイルの整合性をチェックできませんでした。
ログ情報が、整合性情報と一致しません。ログの整合性は保証できません。	ログファイルは存在しますが、予期される情報が含まれていません。ログの整合性は保証できません。
[ログファイル名]が見つかりません	ログファイルが存在しませんでした。
[ログファイル名]が空白です	ログファイルは存在しましたが、空白でした。
[ログファイル名]の最後の行が変更/削除されています	ログファイルの最後の行が、検証基準を満たしません。
[ログファイル名]の[#]行近辺に暗号化されたデータがありません	関連するログファイルの暗号化部分がありませんでした。
[ログファイル名]の[#]行近辺で不一致が見つかりました	ログファイルが、暗号化部分と一致しません。
[ログファイル名]のログファイルの先頭部分で不一致が見つかりました	ログファイルのヘッダーが正しくありません。この状況が発生する可能性が高いのは、ユーザーがログファイルの先頭部分を削除しようとした場合です。

注意： ログチェックファイルには、エラー関連以外のメッセージも表示されます。

システム、イベント、監査ログの設定

システムは、さまざまなログを生成することができます。ログを設定するには、次の手順を実行してください。

1. **詳細設定**を展開し、**ログ**を右クリックし、**プロパティ**を選択します。
2. イベントログおよび監査ログを含む、システムログのプロパティ 『139ページ の"ログプロパティ"参照 』を指定します。管理者は、監査ログの有効/無効のみ設定可能です。その他のすべてのログは必須となります。
3. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

ログプロパティ

システムは、さまざまなタイプのログを生成することができます。ログを設定する場合、以下を定義できます。

一般的なログ

Management Application ログ、Recording Server サービスログ、Image Server サービスログ、Image Import サービスログ

パス	これらのログファイルは、デフォルトでは、使用しているオペレーティングシステムで該当する**すべてのユーザー**フォルダに配置されます。 ログファイルに他の場所を指定するには、必要なフォルダへのパスを**パス**フィールドで入力するか、フィールドの横にある参照ボタンをクリックして、必要なフォルダを参照します。
ログ保存日数	イベントが発生した日ごとに、新しいログファイルが作成されます。 このフィールドで指定されている日数よりも古いログファイルは、自動的に削除されます。デフォルトでは、ログファイルは 7 日間保存されます。他の日数（最長で 9999 日）を指定する場合は、フィールドの値を上書きしてください。たとえフィールドの値が 0 でも、当日のアクティビティは必ず記録されます。したがって、0 を指定すると当日のアクティビティのみを記録し、1 を指定すると当日のアクティビティに加えて過去 1 日分が保存されることになります。

イベントログ

パス	これらのログファイルは、デフォルトでは、使用しているオペレーティングシステムで該当する**すべてのユーザー**フォルダに配置されます。 ログファイルに他の場所を指定するには、必要なフォルダへのパスを**パス**フィールドで入力するか、フィールドの横にある参照ボタンをクリックして、必要なフォルダを参照します。
ログ保存日数	イベントが発生した日ごとに、新しいログファイルが作成されます。 このフィールドで指定されている日数よりも古いログファイルは、自動的に削除されます。デフォルトでは、ログファイルは 7 日間保存されます。他の日数（最長で 9999 日）を指定する場合は、フィールドの値を上書きしてください。たとえフィールドの値が 0 でも、当日のアクティビティは必ず記録されます。したがって、0 を指定すると当日のアクティビティのみを記録し、1 を指定すると当日のアクティビティに加えて過去 1 日分が保存されることになります。

監査ログ

監査ログの有効化	監査ログは、システムのログで唯一強制的でないタイプのログです。チェックボックスを選択/選択解除すると、監査ログが有効/無効になります。
パス	これらのログファイルは、デフォルトでは、使用しているオペレーティングシステムで該当する**すべてのユーザー**フォルダに配置されます。 ログファイルに他の場所を指定するには、必要なフォルダへのパスを**パス**フィールドで入力するか、フィールドの横にある参照ボタンをクリックして、必要なフォルダを参照します。

ログ保存日数	監査ログが有効であれば、毎日クライアントユーザーが活動した日ごとに、新しいログが作成されます。このフィールドで指定されている日数よりも古いログファイルは、自動的に削除されます。デフォルトでは、ログファイルは 7 日間保存されます。他の日数（最長で 9999 日）を指定する場合は、フィールドの値を上書きしてください。当日のアクティビティは必ず記録されます(監査ログが有効で、ユーザーのアクティビティがある場合)。したがって、1 を指定すると当日のアクティビティに加えて、過去 1 日分が保存されることになります。0（ゼロ）を指定すると、監査ログは無限に（ディスク容量が許す限り）保存されることに注意してください。

最小ログ間隔	イベントを記録する間隔の最小の秒数。イベントを記録する間隔の秒数を大きく設定することで、監査ログのサイズを小さくできます。デフォルトは 60 秒です。
シーケンス時間	同じシーケンス内とみなす表示画像の秒数です。秒数を大きくすることで、記録される表示シーケンス数を減らすことができ、監査ログのサイズを小さくできます。デフォルトは 10 秒です。

通知

通知について

ハードウェアの障害やカメラでのモーション検知が発生した場合に、SMS および E メールで通知されるように設定することができます。

E メール

E メールについて

E メール通知では、監視システムに異常が発生した場合にただちに通知を受けることができます。以下の場合に、任意の数の宛先へ E メール通知を送信できます：

- モーションが検知された場合
- イベントが発生した場合この場合、それぞれのイベントについて、E メール通知を受信するか否かを個別に選択できます。
- アーカイブが失敗した場合（アーカイブプロパティの一部として、E メール通知を選択している場合）

E メール通知の設定

E メール通知は次のように設定します。

1. **詳細設定**を展開し、**通知**を展開し、**E メール**を右クリックし、**プロパティ**を選択します。
2. **E メールの有効化**チェックボックスを選択すると、E メールの使用が有効化されます。

3. 必要なプロパティ 『142ページ の"メッセージ設定（E メール）"参照 』を指定します。

4. E メール通知に関連付けるスケジュールプロファイルを選びます。 システムには、2 つの基本スケジュールプロファイル（**常にオン**と**常にオフ**）があり、これらを編集または削除することはできません。これらが組織のニーズに合わない場合、それぞれのカメラに対してカスタマイズされたスケジュールプロファイルを複数作成できます。カスタマイズされたスケジュールプロファイルは、必要に応じて複数の目的で再利用できます。

E メール（プロパティ）

メッセージ設定（E メール）

E メール通知のメッセージ設定には以下の項目があります。

有効	E メール通知の使用を有効にして、さらにプロパティを指定できるようにします。
受信者	システムがメール通知を送信する E メールアドレスを指定します。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@aa.aa; bb@bb.bb; cc@cc.cc）。
件名	メール通知の件名を入力します。
メッセージテキスト	メール通知のメッセージ本文を入力します。カメラの情報ならびに日付や時刻の情報は、自動的にメール通知に含まれます。
変数	通知に変数を含めるにはリンクをクリックします。オプションは以下のとおりです。 • トリガされたイベントの名前 • カメラ名 • トリガ時間（通知が登録された時刻） • エラーテキスト（例：カメラの障害）
類似したメッセージを無視する期間：	類似した通知の送信を無視する秒数を指定します。この機能によって、関連する問題を解決する前に、何度も同じ通知を受け取ることを防げます。
スケジュールプロファイルを使用する	使用したいスケジュールプロファイルを選択します。デフォルトでは、**常にオン**、**常にオフ**のいずれかを選択します。または**新規追加...** を選択してカスタムスケジュールを設定 『146ページ の"通知スケジュールプロパティ"参照 』します。

添付設定（E メール）

E メール通知の添付設定には以下の項目があります。

画像を含む	チェックボックスを選択して、静止画を E メール通知に含めます。選択すると、それぞれの E メール通知に 1 件または複数の静止 JPEG 画像が含まれます。 添付される画像は、インシデントの前、インシデントの後、実際のインシデントの画像であり、通知の原因となったインシデントが中央になります。 **重要 :** E メール通知がオンになっていても、デバイスに画像が記録されていなければ、送信される E メール通知には画像は含まれません。
画像の数	E メールに含めたい画像の数。1～20 の画像を含めることができます。
画像間の時間（ミリ秒）：	各画像の間での最小時間（ミリ秒単位）。0～300 秒（5 分）の時間を設定できます。
E メールに画像を埋め込む	チェックボックスを選択して、画像を直接 E メールに埋め込みます。

サーバー設定（E メール）

E メール通知のサーバー設定には以下の項目があります。

送信者の E メールアドレス	E メール通知の送信者として使用したい E メールアドレスを入力します。
送信メールサーバーアドレス（SMTP）	E メールによる通知の送信で使用する SMTP（Simple Mail Transfer Protocol）サーバーの名前を入力します。 他のメール転送方法と比較した際に、SMTP には、メールクライアントからトリガされる警告を自動的に回避できるという利点があります。それ以外の場合は、この警告により E メールクライアントが自動的に E メールメッセージを送信しようとしているという通知が送られます。 TLS（Transport Layer Security）およびその前身である SSL（Secure Socket Layer）がサポートされています。
送信メールサーバーのポート（SMTP）	メールサーバーのポートを入力します。デフォルトのポート番号は 25 です。
サーバーのログインが必要です	SMTP サーバーを使用する際にユーザー名とパスワードを使用する必要がある場合は、このチェックボックスを選択します。
セキュリティタイプ	使用したいセキュリティのタイプを選びます。
ユーザー名	SMTP サーバーがユーザ認証を必要とする場合、ユーザー名を指定します。 **サーバーのログインが必要です**を選択した場合にのみ必要です。
パスワード	SMTP サーバーの使用で必要なパスワードを指定します。 **サーバーのログインが必要です**を選択した場合にのみ必要です。
最大添付サイズ（MB）	添付する画像の最大サイズを指定します。

SMS

※本機は、SMS には対応していません。

SMS について

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、製品比較チャート『12ページ 』を参照してください。

SMS 通知により、監視システムに異常が発生した場合に、ただちにモバイルデバイスへ通知を送信することができます。SMS 通知機能を使用するには、システムがインストールされているサーバーに 3G/USB モデムを接続する必要があります。

以下の場合に、自動的に SMS 通知を送信することができます。

- モーションが検知された場合
- イベントが発生した場合それぞれのイベントについて、SMS 通知を受信するか否かを個別に選択できます。
- アーカイブが失敗した場合（アーカイブプロパティの一部として、SMS 通知を選択している場合）

SMS 通知の設定

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、製品比較チャート『12ページ 』を参照してください。

SMS 通知は次のように設定します。

1. **詳細設定**を展開し、**通知**を展開し、**SMS 通知**を右クリックし、**プロパティ**を選択します。
2. **SMS の有効化**チェックボックスを選択すると、SMS 通知が有効化されます。
3. 必要なプロパティを指定します。
4. SMS 通知に関連付けるスケジュールプロファイルを選びます。

注意： システムには、2 つの基本スケジュールプロファイル（**常にオン**と**常にオフ**）があり、これらを編集または削除することはできません。これらが組織のニーズに合わない場合、それぞれのカメラに対してカスタマイズされたスケジュールプロファイルを複数作成できます。カスタマイズされたスケジュールプロファイルは、必要に応じて複数の目的で再利用できます。

SMS プロパティ

メッセージ設定（SMS）

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、製品比較チャート『12ページ 』を参照してください。

SMS 通知のメッセージ設定には以下の項目があります。

SMS を有効化	SMS 通知の使用を有効にして、さらにプロパティを指定できるようにします。

受信者	受信者の電話番号を示します。複数の宛先に SMS を送信するには、セミコロンで電話番号を区切ります。
メッセージテキスト	SMS 通知に必要なメッセージ本文を指定します。メッセージ本文には、以下の文字のみが使用できます。a～z、A～Z、0～9、カンマ（,）、ピリオド（.）。カメラの情報ならびに日付や時刻の情報は、すべて自動的に SMS 通知に含まれます。
変数	通知に変数を含めるにはリンクをクリックします。オプションは以下のとおりです。 • トリガされたイベントの名前 • カメラ名 • トリガ時間（通知が登録された時刻） • エラーテキスト（例：カメラの障害）
類似したメッセージを無視する期間：	類似した通知の送信を無視する秒数を指定します。この機能によって、関連する問題を解決する前に、何度も同じ通知を受け取ることを防げます。
スケジュールプロファイルを使用する	使用したいスケジュールプロファイルを選択します。デフォルトでは、**常にオン**、**常にオフ**のいずれかを選択します。または**新規追加...** を選択してカスタムスケジュールを設定 『146ページ の"通知スケジュールプロパティ"参照 』します。

サーバー設定（SMS）

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、製品比較チャート『12ページ 』を参照してください。

SMS 通知のサーバー設定には以下の項目があります。

シリアルポート	USB/3G モデムで使用するシリアルポートを選択します。ポートを選択できるリストに、システムが動作しているコンピュータで空いているシリアルポートが示されます。
スピード	使用している USB モデムデバイスのボーレート。デフォルト値は 9600 ボーです。ボーレートには任意のカスタム値を指定できますが、Milestone では、非常に経験が豊富なユーザー以外はボーレートを変更しないことを推奨しています。
SIM カード PIN コード	USB/3G モデムに挿入されている SIM カードの PIN コードを指定します。

SMS エンコーディング	世界中のさまざまな言語のニーズに対応するために、さまざまな種類の SMS エンコーディングがあります。使用しているシステムには、以下のオプションがあります。 • 7 ビット • 8 ビット（デフォルト） • 16 ビット 7 ビットの暗号化によって、最大 160 文字までを 1 件の SMS メッセージで使用できますが、使用できる文字の種類には制限があります。 8 ビットの暗号化は、より特殊な文字の使用が可能な標準です。この場合、最大 140 文字までを 1 件の SMS メッセージで使用できます。 ラテン系以外のアルファベット言語では、16 ビットの暗号化が必要です。たとえば、アラビア語、中国語、韓国語、日本語、キリル文字のアルファベット言語では 16 ビットの SMS エンコーディングが必要です。組織でこれらの言語のいずれかを使用している場合、16 ビットのエンコーディングを使用するようにシステムを設定する必要があります。16 ビットの場合、1 件の SMS メッセージで使用できる最大文字数は 70 文字です。

スケジューリング

通知スケジュールについて

通知スケジュールによって、E メール 『142ページ の"メッセージ設定（E メール）"参照 』や SMS 『144ページ の"メッセージ設定 (SMS) "参照 』による通知を使用する際のスケジュールプロファイルを設定できます。

通知スケジュールプロパティ

E メールまたは SMS による通知を使用する通知スケジュールの設定では、以下を指定します。

通知プロファイル	通知スケジュールプロファイルの関連プロファイル（例：**常にオン**）を選択します。 以下に基づいて、スケジュールプロファイルを作成して、通知スケジュールプロファイルを指定します。 • 期間（例：月曜日の 08:30 から 17:45 まで）、青色で表示： 

Central

※本機は、Central には対応していません。

Central について

Central 設定によって、XProtect Central サーバーで必要なログイン設定を指定して、ステータス情報やアラームを取得するために監視システムにアクセスできるようにします。

MIP を使用している場合、これは監視システムにアクセスするための MIP のログイン設定を指定するダイアログにもなります。

XProtect Central の有効化

1. **詳細設定**を展開し、Central を右クリックし、**プロパティ**を選択します。
2. **Milestone XProtect Central の有効化**チェックボックスを選択すると、Central 接続の使用が有効化されます。
3. 必要なプロパティを指定します。
4. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

Central のプロパティ

Central の次のプロパティを指定できます。

Milestone XProtect Central の接続を有効にする	Central 接続の使用を有効にして、さらにプロパティを指定できるようにします。
ログイン名	システムと Central サーバー、または MIP の間での接続で使用する名前を入力します。指定する名前は、Central サーバーまたは MIP の間で一致している必要があります。
パスワード	システムと Central サーバー、または MIP の接続で使用するパスワードを入力します。指定するパスワードは、Central サーバーまたは MIP の間で一致している必要があります。
ポート	XProtect Central サーバーまたは MIP が監視システムサーバーへアクセスする際に接続する必要のあるポート番号を入力します。指定するポート番号は、XProtect Central サーバーまたは MIP の間で一致している必要があります。デフォルトポートは 1237 です。

アクセス コントロール

※本機は、アクセスコントロールには対応していません。

アクセスコントロールの統合について

XProtect Access を使用する場合、XProtect VMS 内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を持つベンダーからのアクセスコントロールシステムで、XProtect Access を使用することができます。

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。詳細については、製品比較チャート『12ページ 』を参照してください。

アクセスコントロール統合機能では、XProtect とお客様のアクセスコントロールシステムを簡単に統合できる新機能が搭載されています。特長：

- XProtect Smart Client 内の複数のアクセスコントロールシステムを操作できる共通のユーザーインターフェース。
- アクセスコントロール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。
- アクセスコントロール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。

統合を開始する前に、基本ライセンスとアクセスコントロールドアライセンスに加え、イベントサーバー上にベンダー固有の統合プラグインをインストールする必要があります。

XProtect Professional VMS 製品と統合できるドアの最大数は 1000 です。アクセスコントロールシステムからインポートする構成で、これより多くのドアが使用できる場合は、統合が停止します。

XProtect Access ライセンス

XProtect Access は、以下のアクセスコントロール関連ライセンスを必要とします。

- XProtect Access の**基本ライセンス**、無制限の台数の Access サーバーをカバーします。
- XProtect Access で統合および制御したい各ドアについて 1 つの**アクセスコントロールドアライセンス**。**XProtect Access の基本ライセンスには、2 つの**アクセスコントロールドアライセンスが含まれています。すべてのドアライセンスは、XProtect Access 製品をインストールすると自動的にインストールされます。ただし、インストールされたドアライセンスはデフォルトでは無効であり、使用したいドアを有効化する必要があります。ライセンスがあれば、ドアはいくつでも有効にできます。

例：5 つのアクセスコントロールドアライセンスがあり、10 個のドアを追加しました。ドアを 5 つ追加すると、それ以上は選択できなくなります。別のドアを追加する前に、一部のドアを削除する必要があります。

アクセスコントロールドアライセンスの現在のステータスを確認するには、**アクセスコントロール**ノードを開きます。

追加の XProtect Access 基本ライセンスまたはドアライセンスを購入するには、ベンダーにお問い合わせください。

アクセスコントロールシステム統合ウィザード

アクセスコントロールシステム統合ウィザードでは、アクセスコントロールシステムの最初のインテグレーションを段階的に設定します。ウィザードを使用して、基本的な設定作業を行うことができます。後日に、さらに詳細な設定を行うことができます。

アクセスコントロール統合ウィザードを開始する前に、イベントサーバーに統合プラグインがインストールされていることを確認します。

一部のフィールドには入力が必要であり、統合プラグインからデフォルト値が継承されるフィールドもあります。したがって、統合するアクセスコントロールシステムに応じて、ウィザードの外観が異なる場合があります。

ウィザードを開始するには、ノードツリーで**アクセスコントロール**を選択し、右クリックして、**新規作成**をクリックします。

アクセスコントロールシステム統合の作成

追加したいアクセスコントロールシステムの名前を入力し、接続詳細を指定します。指定しなければならないパラメータはシステムのタイプによって異なりますが、通常は、アクセスコントロールシステムサーバーのネットワークアドレス、アクセスコントロール管理者のユーザー名とパスワードを指定します。

設定を取得するためにアクセスコントロールシステムにログインする際に、ビデオ管理システムは、指定したユーザー名とパスワードを使用します。

また、統合プラグインでは、ウィザードでリストされないセカンダリパラメータを定義することもありますが、これらは統合を設定した後に **一括設定**で変更することができます。パラメータのデフォルト値は、プラグインまたは XProtect システムによって入力されます。

アクセスコントロールシステムへの接続

プラグインが正常に統合されると、取得されたアクセスコントロールシステムの設定の概要が表示されます。ウィザードの次のステップに進む前に、このリストにすべての項目が統合されていることを確認します。

関連のあるカメラ

アクセスコントロールシステムのアクセスポイントを XProtect システムのカメラとマッピングし、イベントに対してドアからの関連ビデオを表示します。

また、複数のカメラを単一のアクセスポイントにマッピングすることもできます。そして、XProtect Smart Client ユーザーは、たとえばイベントを調査する時などに、すべてのカメラからのビデオを表示できるようになります。

さらに、XProtect Smart Client のユーザーは、**アクセスモニター**の表示項目を設定する場合など、いずれかのカメラを追加することもできます。

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。チェックボックスをクリアすると、ドアが無効になり、アクセスコントロールドアライセンスが解放されます。

最終的な概要

デフォルト設定を統合プラグインから継承したアクセスコントロールシステム統合が、XProtect で正常に作成されました。クライアントユーザーは、XProtect Smart Client にログインして、新しいアクセスコントロールシステムを確認、使用する必要があります。

必要に応じて、この構成を調整できます。

アクセスコントロールプロパティ

※本機は、アクセスコントロールには対応していません。

一般設定タブ（アクセスコントロール）

名前	詳細
有効	システムはデフォルトで有効であり、これは XProtect Smart Client で十分な権限を有するユーザーに対して表示されること、XProtect システムがアクセスコントロールイベントを受信することを意味しています。 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	アクセスコントロールインテグレーションの名前が、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。
詳細	アクセスコントロール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	最初のインテグレーションで選択したアクセスコントロールシステムのタイプを示します。
最後の設定更新	アクセスコントロール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 のアクセスコントロールシステムで行った変更を反映させる必要がある場合は、このボタンをクリックします。 アクセスコントロール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、リストをレビューして、アクセスコントロールシステムに正しく反映されていることを確認します。
オペレータのログインが必要	アクセスコントロール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、クライアントユーザーに対して追加のログインを有効にします。 このオプションが表示されるのは、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だけです。

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、通常みられる一部のフィールドの例です。

名前	詳細
アドレス	統合されたアクセスコントロールシステムを提供するサーバーのアドレスを入力します。
ポート	アクセスコントロール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	アクセスコントロールシステムで定義されている、XProtect の一体型システムの管理者となるユーザーの名前を入力します。

名前	詳細
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（アクセスコントロール）

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、いつでもセットアップを変更することができます。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へのマッピングが内在しています。

名前	詳細
ドア	アクセスコントロール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。 関連するドアへの移動を簡単にするには、アクセスコントロール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、ドアをフィルタリングできます。 **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。 **ライセンス**：ドアのライセンスがあるか、ドア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リストします。 リストからカメラを選択し、関連するアクセスポイントでドラッグおよびドロップして、カメラとアクセスポイントを関連付けます。

アクセスコントロールイベントタブ（アクセスコントロール）

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構成は、XProtect システムのアクセスコントロールの動作に影響を与えます。たとえば、複数のタイプのイベントでの単一のアラームのトリガを定義することができます。

名前	詳細
アクセスコントロールイベント	アクセスコントロールシステムからインポートしたアクセスコントロールイベントをリストします。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制御します。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、たとえば、XProtect Smart Client でのフィルタリングでも使用できます。
ソースタイプ	アクセスコントロールイベントを起動できるアクセスコントロールユニットを表示します。

名前	詳細
イベントカテゴリ	アクセスコントロールイベントに、「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。 統合イベントカテゴリは、以下のとおりです。 • アクセスが拒否されました • アクセスを許可済み • アクセスリクエスト • アラーム • エラー • 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。 **重要**：Corporate システムでイベントカテゴリを変更する場合は、既存のアクセスコントロールのルールが正しく機能す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。 統合カテゴリが要件に適合しない場合は、イベントカテゴリを作成することができます。たとえば、アクセスコントロールのアクションをトリガ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、たとえばアラーム定義など、システムをまたいだ操作のセットアップが可能になります。 ユーザー定義のイベントカテゴリを削除すると、統合によって警告が使用されている場合には警告を受信します。それでも削除すると、たとえばアクセスコントロールのアクションなど、このカテゴリで行ったすべての設定が動作しなくなります。

アクセスコントロールアクション

アクションは、トリガするイベントに基づいて、XProtect Smart Client でのアクセスコントロールの動作を指定します。

以下に関連して、1 つまたは複数のアクションを指定できます。

- イベントカテゴリ
- アクセスコントロールシステムからのイベント
- XProtect システムからのイベント

トリガするイベントは、特定のアクセスコントロールユニットから、またはアクセスコントロールユニットのグループからになります。

名前	詳細
イベントのトリガ	アクションをトリガするイベントカテゴリをリストから選択します。このリストには、組み込み、プラグイン、ユーザー定義のイベントカテゴリが含まれています。 **アクセスコントロールイベント**を選択すると、イベントカテゴリの代わりに特定のアクセスコントロールイベントに基づくトリガが作成されます。 **外部イベント**を選択すると、XProtect システムの入力イベントに基くトリガが作成されます。 それぞれのトリガに対して、**ソース**フィールドで入力ソースを指定します。
ソース	アクションが影響を与えるソースを選択します。オプションは、**トリガイベント**フィールドの設定によって異なります。 イベントカテゴリおよびアクセスコントロールのイベントについて、以下を選択します。 • すべてのドア • 個々のドア • その他... **その他**をクリックして、複数のドア、ドアのアクセスポイント、またはアクセスコントロールシステムの他のユニットを選択します。 外部イベントの場合： XProtect システムのイベントおよび入力デバイスのリストから、ソースを選択します。
時間プロファイル	トリガされた場合に実行するアクションの時間プロファイルを選択します。 **詳細設定**の一部として、時間プロファイルを設定します。
アクション	アクションのタイプの選択： • アクセスリクエスト通知の表示 • PTZ プリセットに移動 • 記録の開始 • システムアクション それぞれのアクションに対して、アクションの詳細を指定します。 複数のアクションを設定するには、**アクセスコントロールアクションの追加**をクリックします。たとえば、週末や営業時間に応じて、同じイベントで別のアクションをトリガする場合に、これを行います。
アクセスコントロールアクションの追加	クリックして、必要に応じて、アクションを追加および定義します。

アクションの詳細	アクションのパラメータを設定： アクセスリクエスト通知を表示： • 特定のイベントが発生したときに、通知ユーザーインターフェースを通して、どのカメラ、マイク、またはスピーカーに XProtect Smart Client ユーザーが接続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。通知でさらに多くのコマンドを有効にするには、**コマンドの追加**を参照してください。 PTZ プリセットに移動： • カメラを指定し、事前に設定されているプリセットから、カメラのパターンや、所定のイベントが発生した場合にプリセットに戻る時間を選択します。 記録の開始： • 所定のイベントが発生した場合に、記録を開始るするカメラおよび期間を指定します。 システム アクション: • XProtect システムで事前に定義されているアクションを指定します。
コマンドの追加	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。たとえば、**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。 アクセスコントロールコマンド： • 選択したアクセスコントロール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、右側で **X** をクリックします。

カードホルダータブ（アクセスコントロール）

カードホルダータブを使用して、アクセスコントロールシステムにおけるカードホルダーの情報をレビューします。

名前	詳細
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	詳細
名前	アクセスコントロールシステムから取得したカードホルダーの名前をリストします。
タイプ	以下のようにカードホルダーのタイプをリストします。 • 従業員 • 警備員 • 来客

使用しているアクセスコントロールシステムが、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、アクセスコントロール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	詳細
画像の選択	カードホルダーの画像ファイルへのパスを指定します。アクセスコントロールシステムが画像を管理している場合は、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、画像はサイズ変更されます。 Milestone では、正方形の画像を使用することを推奨しています。
画像の削除	クリックすると、画像を削除します。アクセスコントロールシステムに画像があった場合、削除後はこの画像が表示されます。

サーバーアクセス

サーバーアクセスについて

以下の 2 通りの方法により、システムのサーバーへのクライアントアクセスを設定できます。

- **ウィザードによる設定：** ガイドに従い、クライアントからのサーバーへのアクセス方法や、クライアントで使用するユーザーについて設定します。このウィザードを使用すると、すべてのカメラ（これ以降に追加するものを含む）に対し、追加したすべてのユーザーがアクセスできるようになります。これが望ましくない場合、アクセス設定、ユーザー、ユーザー権限を個別に指定してください。
- **詳細設定：** これは、以前のバージョンでは画像サーバー管理と呼ばれていました。

登録済みサービスについて

登録済みサービスには、システムにインストール済みで、実行中のサービスが表示されます。個々のサービスについて、以下の情報が表示されます。

名前	詳細
デバイスが有効	関連するサービスが有効であることを示します。
名前	サービスの名前。
詳細	サービスの説明。
アドレス	サービスが使用する内外部のアドレス。

サービスの内外部のアドレスは変更できます。これを行うには、**編集**ボタンをクリックして、関連する内外部のアドレスを入力します。すべてのサービスが編集できるわけではありません。**削除**ボタンをクリックして、システムからサービス登録を削除することもできます。サービスを削除する前に、確認メッセージが表示されます。

サーバーアクセスの設定

1. **詳細設定**を展開し、**サーバーアクセス**を右クリックし、**プロパティ**を選択します。
2. サーバーアクセス、ローカル IP 範囲、言語サポートおよび XML エンコーディングの必要なプロパティを指定します。システムには、2 つの基本スケジュールプロファイル（**常にオン**と**常にオフ**）があり、これらを編集または削除することはできません。これらが組織のニーズに合わない場合、それぞれのカメラに対してカスタマイズされたスケジュールプロファイルを複数作成できます。カスタマイズされたスケジュールプロファイルは、必要に応じて複数の目的で再利用できます。
3. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

このオプションを使用する場合は、クライアントのアクセスからクライアントユーザーを個別に設定します。個別のユーザーの追加、ユーザーグループの追加、ユーザーおよびグループの権限の設定を参照してください。

サーバーアクセスプロパティ

サーバーアクセス

システムサーバーまたはサーバーアクセスへのクライアントアクセスを設定できます。以下を指定します。

サーバー名	監視システムサーバーの名前は、クライアントに表示されるとおりです。クライアントを設定する権限を持っているクライアントユーザーは、ビューを作成した時にサーバーの名前をクライアントで確認できます。
ローカルポート	クライアントと監視サーバーの間での通信で使用するポート番号です。デフォルトのポート番号は 80 ですが、組織でポート 80 を他の目的で使用している場合には変更できます。
インターネットアクセスを有効にする	ルーターまたはファイアウォールを経由して、インターネットからサーバーにアクセスする必要がある場合は、このチェックボックスを選択します。 このオプションを選択する場合、以下のフィールドで、パブリック（外部）IP アドレスとポート番号も指定します。パブリックアクセスを使用する場合、使用するルーターまたはファイアウォールを、パブリック IP アドレスおよびポートに送信される要求が監視システムサーバーのローカル（内部）IP アドレスおよびポートに転送されるように設定する必要があります。
インターネットアドレス	システムサーバーをインターネットから使用できる必要がある場合、使用するパブリック IP アドレスまたはホスト名を指定します。

インターネットポート	システムをインターネットから使用できる必要がある場合、使用するポート番号を指定します。デフォルトのポート番号は 80 です。必要に応じて、ポート番号を変更できます。
最大クライアント数	同時に接続できるクライアントの数を制限することができます。システムの設定や、使用しているハードウェアやネットワークの性能によって、同時に接続するクライアントの数を制限してサーバーの負荷を軽減できます。同時に接続を許可された数を超えるクライアントがログインを試みても、アクセスが許可されるのは指定された数のクライアントだけです。許可される数を超えると、クライアントにはログインを試みた時にエラーメッセージが送られます。 デフォルトでは、最大で 10 のクライアントが同時に接続できます。異なる最大数を指定する場合は、値を上書きしてください。 無制限の数のクライアントに同時接続を許可する場合は、**最大クライアント数**フィールドに **0**（ゼロ）を入力します。 システムのクライアントセッションには、4 分のセッションタイムアウト時間が適用されます。クライアントユーザーはこれに全く気付かない場合がほとんどです。ただし、最大クライアント数の値を 1 に設定すると、このセッションタイムアウト時間が非常に明確になります。この場合、許可される単一のクライアントユーザーがログアウトすると、再度ログインできるようになるまでに 4 分間経過する必要があります。

ローカル IP 範囲

システムがローカルネットワークから受信したことを認識できるローカル IP 範囲を指定できます。これは、ローカルネットワークで異なるサブネットを使用している場合に関係します。

[追加]ボタンをすると、次の項目を設定できます。

開始アドレス	範囲の開始 IP アドレスを指定します。
終了アドレス	範囲の終了 IP アドレスを指定します。

他のローカル IP 範囲を追加するには、手順を繰り返します。

言語サポートと XML エンコーディング

システムのサーバーとクライアントで使用する言語/文字セットを選択できます。

文字エンコード/言語	必要な言語/文字セットを選択します。 例：監視システムサーバーが日本語版 Windows で動作する場合は、日本語を選択します。アクセスクライアントも日本語版 Windows を使用する場合、これで必ずクライアントとサーバー間の通信で正しい日本語および文字エンコーディングが使用されます。 マスター/スレーブ設定を使用する場合、すべての関連するサーバーで同じ言語/文字セットを指定するようにしてください。 XProtect Professional のみがマスター/スレーブ機能をサポートします。

マスター/スレーブ

マスターおよびスレーブについて

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、製品比較チャート『12ページ 』を参照してください。

マスター/スレーブ設定により、複数のサーバーを組み合わせて、使用できるカメラの合計数を単一のサーバーの許容最大数以上に拡大できます。マスター/スレーブの設定を行うことで、リモートユーザーが同時に複数のサーバーに自動的に接続できます。リモートユーザーがマスターサーバーへ接続すると、即座にスレーブサーバーのハードウェアデバイスのフィードにもアクセスできるようになります。

ソフトウェアライセンスファイルごとに無制限の数のマスターおよびスレーブサーバーを指定できます。XProtect Professional マスターサーバーは XProtect Professional スレーブサーバーのみを使用できますが。

マスターおよびスレーブサーバーでは異なる製品バージョンを使用できますが、マスターサーバーでは最新バージョンのソフトウェアを使用する必要があります。また、スレーブサーバーでは、マスターサーバーで実行中の製品よりも 2 バージョン以上前のバージョンを実行することはできません。

スレーブへの接続を確認するには、**ステータス更新**をクリックすると、接続されたスレーブ数が報告されます。

マスターおよびスレーブサーバーの設定

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、製品比較チャート『12ページ 』を参照してください。

1. **詳細設定**を展開し、**マスター/スレーブ**を右クリックし、**プロパティ**を選択します。
2. **マスターサーバーとして有効化**チェックボックスを選択します。
3. **追加**をクリックして、スレーブサーバーを追加します。
4. スレーブサーバーのプロパティを指定します。準備ができたら **OK をクリックします。**

マスター/スレーブプロパティ

マスターサーバーおよびスレーブサーバーには、以下のプロパティを設定できます。

マスターサーバープロパティ

マスターサーバーとして有効化	マスターサーバーとして有効化を選択します。
タイムアウト	スレーブ更新のタイムアウトを設定します。詳細は、下記の**スレーブでのステータスの更新**を参照してください。
追加	スレーブサーバーを追加できます。リストで**マスターサーバー**を選択し、**追加**ボタンをクリックします。

マスターサーバーを選択すると、**削除**ボタンが無効になり、**追加**ボタンが有効になります（**マスターサーバーとして有効化**を選択している場合）。追加ボタンをクリックすることで、スレーブサーバーをマスターサーバーに追加できますが、マスターサーバーは削除できなくなります。

スレーブサーバープロパティ

アドレス	スレーブサーバーの IP アドレス。
ポート	スレーブサーバーのポート番号。
削除	スレーブサーバーのリストから、スレーブサーバーを削除します。リストでスレーブサーバーを選択し、**削除**ボタンをクリックします。

スレーブサーバーをマスターサーバーにしたい場合は、元のマスターサーバーで**マスターサーバーとして有効化**を選択解除して、**OK** をクリックします。ナビゲーションペインで、マスターサーバーにしたいスレーブサーバーを右クリックし、**プロパティ**を選択します。次に、**マスターサーバーとして有効化**を選択します。さらに、**追加**をクリックして、スレーブサーバーを新しいマスターサーバーに追加します。

スレーブでのステータス更新

マスター設定の概要および**スレーブ設定の概要**のテーブルエリアで、**ステータス更新**をクリックすると、追加したスレーブサーバーを確認/更新できます。ステータスダイアログが起動され、その後、スレーブサーバーのステータスを通知します。

ユーザー

ユーザーについて

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。

ユーザーアクセス設定ウィザードでは、両方のタイプのユーザーを追加することも、別個に追加することも可能です（基本ユーザーの追加 『159ページ 』および Windows ユーザーの追加 『160ページ 』を参照）。

ユーザーをグループ化することで、グループ内のすべてのユーザーに対して一度で権限を指定することができます。類似のタスクを実行するユーザーが多数存在する場合、これで大幅に作業量を削減できます。ユーザーグループは、あくまでも Management Application での実用的な目的のためだけに作成・使用します。いかなる方法でも、一元的ディレクトリサービスのユーザーグループと接続されることはありません。グループを使用したい場合、ユーザーを追加する前に必ずグループを作成してください。既存のユーザーをグループに追加することはできません。

最後に、管理者グループも、ユーザーの下にリスト化されます。これは、管理のためのデフォルトの Windows ユーザーグループであり、自動的に Management Application へのアクセス権が与えられます。

基本ユーザーの追加

基本ユーザーを追加する際、個別のユーザーについて、基本ユーザー名とパスワード認証で監視システム専用のユーザーアカウントを作成します。Windows ユーザーを作成することで、セキュリティが向上します。ユーザーをグループに含めたい場合、ユーザーを追加する前に必ず必要なグループを追加したことを確認してください。既存のユーザーをグループに追加することはできません。

基本ユーザーは、次の 2 種類の方法で追加できます。1 つは、**ユーザーアクセス設定**ウィザードによる方法です。あるいは、次の方法で基本ユーザーを追加します。

1. **詳細設定**を展開し、**ユーザー**を右クリックし、**新しい基本ユーザーの追加**を選択します。
2. ユーザー名を指定してください。パスワードを指定し、再入力して、パスワードが正しく入力されていることを確認します。**OK** をクリックします。
3. 一般アクセスおよびカメラアクセスのプロパティを指定します。これらのプロパティによって、ユーザーの権限が決まります。 **OK** をクリックします。
4. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

Windows ユーザーの追加

Windows ユーザーを追加する際、サーバーでローカルに定義されたユーザーをインポートして、Windows ログインに基づいて認証します。この方法は、基本ユーザーの概念より一般的にセキュリティが向上するため、Milestone ではこの方法を推奨しています。ユーザーをグループに含めたい場合、ユーザーを追加する前に必ず必要なグループを追加したことを確認してください。既存のユーザーをグループに追加することはできません。

Windows ユーザーは、次の 2 種類の方法で追加します。1 つは、ユーザーアクセス管理ウィザードによる方法です。あるいは、Windows ユーザーを次の方法で追加します。

1. **詳細設定**を展開し、**ユーザー**を右クリックし、**新しい Windows ユーザーの追加**を選択します。この操作で、**ユーザーまたはグループの選択**ダイアログが開きます。

   場所... ボタン。
2. **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を入力してから、**名前のチェック**機能を使って、ユーザー名を確認します。複数のユーザー名を入力する場合は、それぞれの名前をセミコロンで区切ります。例：**Brian; Hannah; Karen; Wayne**
3. 完了したら、**OK** をクリックします。
4. 一般アクセスおよびカメラアクセスのプロパティを指定します。これらのプロパティによって、ユーザーの権限が決まります。
5. **OK** をクリックします。
6. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

クライアントで**ローカルデータベース**のログから追加されたユーザーは、ユーザー名の一部として、サーバー名、PC 名、IP アドレスを指定してはなりません。正しく指定したユーザー名の例：USER001。正しく指定されていないユーザー名の例：PC001/USER001。さらに、ユーザーはパスワードや必要なサーバーの情報も指定する必要があります。

ユーザーグループの追加

ユーザーグループは、あくまでも Management Application での実用的な目的のためだけに作成・使用します。いかなる方法でも、一元的ディレクトリサービスのユーザーグループと接続されることはありません。

ユーザーをグループ化することで、グループ内のすべてのユーザーに対して一度で権限 『161ページ の"ユーザーおよびグループの権限の設定"参照 』を指定することができます。類似のタスクを実行するユーザーが多数存在する場合、これで大幅に作業量を削減できます。ユーザーを追加する前に、グループを追加したことを確認してください。既存のユーザーをグループに追加することはできません。

1. **詳細設定**を展開し、**ユーザー**を右クリックし、**新しいユーザーグループの追加**を選択します。
2. 名前を指定します。 名前は一意であり、以下の特殊文字を含むことはできません。 **< > & ' " ¥ / : * ? | [ ]**

3. **OK** をクリックします。
4. 一般アクセス 『162ページ 』およびカメラアクセス 『163ページ 』のプロパティを指定します。これらのプロパティによって、以後グループに追加されるメンバーの権限が決まります。
5. **OK** をクリックします。
6. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。
7. これで、ユーザーをグループに追加することができます。ナビゲーションペインで、作成したグループを右クリックし、必要に応じて基本ユーザーの追加**『159ページ 』または** Windows ユーザーの追加『160ページ 』をクリックします。

ユーザーおよびグループの権限の設定

ユーザー/グループの権限は、ユーザー/グループの追加プロセス中に設定します。基本ユーザーの追加 『159ページ 』、Windows ユーザーの追加 『160ページ 』、ユーザーグループの追加 『160ページ 』を参照してください。基本ユーザーおよび Windows ユーザーは、ユーザーアクセスの管理ウィザード 『60ページ 』でも追加できることに注意してください。このウィザードを使用すると、後の段階で追加されるカメラを含めて、すべてのカメラに対して、追加したすべてのユーザーがアクセスできるようになります。

ユーザーまたはグループの権限を編集する場合：

1. **詳細設定**を展開し、**ユーザー**を展開し、該当するユーザーまたはグループを右クリックして、**プロパティ**を選択します。
2. 表示される該当するタブの下に必要なユーザー権限を設定します。これらのプロパティによって、ユーザー/グループの権限が決まります。 **OK** をクリックします。
3. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

ユーザープロパティ

ユーザー情報

以下のユーザー情報を変更できます。

ユーザー名	ユーザー名を編集します。これを編集できるのは、選択したユーザーが基本ユーザーである場合だけです。名前は一意であり、以下の特殊文字を含むことはできません。 < > & ' " ¥ / : * ?| [ ]
パスワード	パスワードを編集します。入力確認のため、パスワードを再入力することを忘れないでください。 基本ユーザーのパスワードのみ編集できます。
ユーザータイプ	このフィールドは編集できません。選択したユーザーが基本ユーザーか、Windows ユーザーグループかどうかを示します。

グループ情報

グループ名	グループ名を編集します。名前は一意であり、以下の特殊文字を含むことはできません。 < > & ' " ¥ / : * ?| [ ]

一般アクセス

基本ユーザー 『159ページ の"基本ユーザーの追加"参照 』や Windows のユーザー 『160ページ の"Windows ユーザーの追加"参照 』、グループ 『160ページ の"ユーザーグループの追加"参照 』を追加・編集する際に、一般アクセスの以下の設定を指定します。

クライアントのアクセス設定

ライブ	XProtect Smart Client の**ライブ**タブへのアクセスを有効にします。
再生	XProtect Smart Client の**再生**タブへのアクセスを有効にします。
設定	XProtect Smart Client の設定モードへのアクセスを有効にします。
共有ビューの編集	XProtect Smart Client の共有グループでユーザーがビューを作成、編集できるようにします。 すべてのユーザーが、共有グループに配置されたビューにアクセスできます。ユーザー/グループにこの権限がない場合、共有グループは保護され、XProtect Smart Client では錠前アイコンで示されます。
プライベートビューの編集	XProtect Smart Client のプライベートグループでユーザーがビューを作成、編集できるようにします。 プライベートグループに置かれたビューは、それを作成したユーザーしかアクセスできません。ユーザー/グループにこの権限がない場合、プライベートグループは保護され、XProtect Smart Client では錠前アイコンで示されます。ユーザーに独自のビューを作成できる権限を拒否することが望ましい場合があります。たとえば、帯域の利用を制限するなどの特定のケースが考えられます。 共有およびプライベートビューに関する詳細情報は、別個の XProtect Smart Client のマニュアルを参照してください。

ライブ、**再生**、**設定**のチェックボックスを選択解除して、ユーザー/グループが XProtect Smart Client を使用できる機能を無効にします。ユーザー/グループが一定期間の間、アカウントを使用しない場合などに、ユーザー/グループを削除する代わりの一時的な代替として利用することができます。

Management Application アクセス

管理者アクセス	ユーザーによる Management Application へのアクセスや操作を有効にします。 管理者のメンバーが複数いる場合、このチェックボックスを選択解除して、他の管理者が Management Application にアクセスできないようにすることができます。

ログイン認証

このユーザー/グループは、他のユーザーでログインするのに認証が必要です	ユーザー/グループに対する制約を有効にします。つまり、ユーザー/グループが XProtect Smart Client または Management Application にログインするためには、第二のユーザーがログインを認証する必要があります。
このユーザー/グループは、他のユーザーからのログインを認証できる	このユーザー/グループが、他のユーザーの XProtect Smart Client または Management Application へのログインを認証できるようにします。

システムで少なくとも 1 人は、ログインに認証が要らない完全な管理者アクセスを有する必要があります。そのため、管理者はシステムの他のユーザーに適切なユーザー権限がすべて付与されていることを確認する必要があります。認証するべきユーザーがいない場合、**このユーザー/グループは、他のユーザーからログインする認証が必要**チェックボックスは使用不可であり、その設定を変更することはできません。

システムに 1 人しかユーザーがいない場合、**このユーザー/グループは、他のユーザーからのログインを認証できる**チェックボックス は使用不可であり、その設定を変更することはできません。

カメラアクセス

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。詳細については、製品比較チャート『12ページ 』を参照してください。

基本ユーザー 『159ページ の"基本ユーザーの追加"参照 』、Windows のユーザー 『160ページ の"Windows ユーザーの追加"参照 』またはグループ 『160ページ の"ユーザーグループの追加"参照 』を追加または編集する際に、カメラのアクセス設定を指定することができます。

カメラのリストで、操作したいカメラを選択します。リストの最後のアイテムである**新規カメラがシステムに追加された場合、そのカメラに対する権限**で、ユーザー/グループに対して今後追加するカメラへのアクセスを許可することができます。

ヒント：SHIFT または CTRL を使用して、複数のカメラのアクセスで同じ機能が使用できる複数のカメラを選択します。選択中にキーボードで SHIFT または CTRL を押すと、複数のカメラを選択できます。

選択したカメラについて、**アクセス**チェックボックスで、ユーザー/グループがライブ表示や再生にアクセスできるかどうかを指定します。許可する場合は、ライブ表示と再生の**両方**にアクセスできるかどうかを指定します。この場合、選択したカメラでどのサブ機能が使用可能であるかを指定します。サブ機能は、ウィンドウの下方にある 2 列にリスト化されます。左の列にはライブ表示に関連する機能が、右の列には再生に関連する機能がリスト化されます。

カメラアクセス設定チェックボックスは、権限の階層構造のように機能します。**アクセス**チェックボックスが選択解除されていると、他のすべてが選択解除され、無効になります。**アクセス**チェックボックスが選択されているが、たとえば**ライブ**チェックボックスが選択解除されていると、**ライブ**チェックボックスの下位にあるものはすべて選択解除され、無効になります。

選択した列によって、選択したカメラで、ライブまたは再生の以下のデフォルト機能が使用できます。

ライブ	機能
PTZ	PTZ（パン/チルト/ズーム）カメラのナビゲーション機能を使用します。 ユーザー/グループは、1 台または複数の PTZ カメラに対するアクセス権限がある場合にだけ使用できます。
PTZ プリセット位置	PTZ カメラを特定のプリセット位置へ移動させるナビゲーション機能を使用します。ユーザー/グループは、ユーザー/グループに、定義されたプリセット位置で 1 台または複数の PTZ カメラに対するアクセス権限がある場合にだけ使用できます。

ライブ	機能
PTZ プリセットの管理	XProtect Smart Client で、PTZ 位置を管理します。
出力	選択したカメラに関連する出力をアクティブ化します。
イベント	選択したカメラに関連する手動トリガイベントを使用します。この機能は、XProtect Smart Client でのみ使用できます。
受信音声	選択したカメラに関連するマイクから入力された音声を聞きます。この機能は、XProtect Smart Client でのみ使用できます。
手動録画	一定時間 (監視システムの管理者が定義 『82ページ の"手動録画"参照 』) の間、録画を手動で開始します。
送信音声	選択したカメラに関連付けたスピーカーを通じて、相手と話します。この機能は、XProtect Smart Client でのみ使用できます。

再生	機能
AVI/JPEG のエクスポート	AVI 形式のムービークリップや JPEG 形式の静止画として、エビデンスをエクスポートします。
データベースのエクスポート	エビデンスをデータベース形式でエクスポートします。この機能は、XProtect Smart Client でのみ使用できます。
シーケンス	選択したカメラからのビデオを再生する際は、**シーケンス**機能を使用します。
スマートサーチ	選択したカメラの画像で、選択した 1 つまたは複数のエリアでモーションを検索します。この機能は、XProtect Smart Client でのみ使用できます。
録音された音声	選択したカメラに関連するマイクから録音された音声を聞きます。

選択したカメラが関連する機能をサポートしていなければ、機能を選択することはできません。たとえば、PTZ 関連の権限が使用できるのは、関連するカメラが PTZ カメラである場合だけです。一部の機能は、ユーザー/グループの一般アクセス 『162ページ 』プロパティに依存しています。

複数のカメラを選択しており、一部のカメラではある機能が該当するが、すべてのカメラには該当しない場合、ウィンドウの下部に四角で埋められたチェックボックスが表示されます。

例：カメラ A では、イベントの使用を許可するように選択しており、カメラ B では許可していません。リストでカメラ A とカメラ B の両方を選択すると、ウィンドウの下部のイベントチェックボックスは四角で埋められています。別の例：カメラ C は PTZ カメラで、PTZ プリセット位置設定が許可されていますが、カメラ D は PTZ カメラではありません。リストでカメラ C とカメラ D の両方を選択すると、PTZ プリセット位置チェックボックスは四角で埋められています。

アラーム管理

基本ユーザー 『159ページ の"基本ユーザーの追加"参照 』、Windows のユーザー 『160ページ の"Windows ユーザーの追加"参照 』またはグループ 『160ページ の"ユーザーグループの追加"参照 』を追加または編集する際に、XProtect Smart Client アラーム管理の権限を指定することができます。

管理	XProtect Smart Client のユーザーは、以下の操作ができます。 • アラームの管理（例えば、アラームの優先度を変更したり、他のユーザーにアラームを委譲したりする） • XProtect Smart Client のアラームリストやマップなどで、アラームを確認する。 • 複数のアラームの状態を同時に変更（例えば**新規**から**割り当て済み**へ変更）します（これを行わない場合はアラームごとに状態を変更する必要があります）。
ビュー	XProtect Smart Client のユーザーは、以下の操作ができます。 • アラームを表示 • アラームレポートを印刷します。
無効	XProtect Smart Client のユーザーが、アラームを無効にできるようにします。

※本機は、”通知の受領”には対応していません。

アクセス コントロール管理

基本ユーザー 『159ページ の"基本ユーザーの追加"参照 』や Windows のユーザー 『160ページ の"Windows ユーザーの追加"参照 』、グループ 『160ページ の"ユーザーグループの追加"参照 』を追加・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。

アクセスコントロールの使用	XProtect Smart Client のアクセスコントロール関連の機能を関連するユーザーが使用できるようにします。

サービス

サービスについて

標準インストールを行うと、以下の機能はすべて自動的にインストールされます。デフォルトでは、サービスはシステムサーバーのバックグラウンドで自動的に実行されます。必要であれば、個別にサービスを起動・停止することもできます。詳細は、サービスの起動および停止 『168ページ の"サービスを開始および停止する"参照 』を参照してください。

サービス	詳細
Milestone Recording Server サービス	監視システムの重要な部分です。ビデオストリームがシステムに転送されるのは、Recording Server サービスが実行されている間だけです。

サービス	詳細
Milestone Image Server サービス	XProtect Smart Client にログインしているユーザーに、監視システムへのアクセスを提供します。 **注意：** Windows サービスで Image Server サービスが、「Local System」以外のアカウント（たとえばドメインユーザーなど）でログインするように設定されている場合、監視サーバー自体以外のコンピュータにインストールされている XProtect Smart Client は、サーバーのホスト名を使用してサーバーにログインすることはできません。それらのユーザーは、サーバーの IP アドレスを入力する必要があります。
Milestone Image Import サービス	アラーム前後の画像を取り込むため、および取り込んだ画像をカメラデータベースに保存するために使用します。 アラーム前後の画像は、選択したカメラでのみ使用可能な機能であり、これによってイベント発生の直前および直後の画像をカメラから監視システムへ、E メールで送信できます。アラーム前後の画像と、システムの録画前後の機能 『93ページ の"記録"参照 』を混同しないように注意してください。
Milestone Log Check サービス	システムのログファイルで、整合性チェックを実行します。
Milestone Event Server サービス	すべてのアラームやマップ関連の通信を管理します。イベント、画像ファイル、マップの設定を保存し、監視システムに関するステータス情報を利用可能にします。
通知サーバーサービス	システムからユーザーに送信される電子メールまたは SMS 通知を管理します。
Milestone Mobile サービス	Recording Server とモバイルデバイス（スマートフォンやタブレットなど）の間、ならびに Recording Server と Web ブラウザの間での通信を管理します。

カスタムインストールを実行する場合は、Event Server をインストールしないよう選択できます。そのような場合、Event Server サービスはサービス概要に表示されません。

トレイアイコンについて

※本機は、フェールオーバーレコーディングサーバーには対応していません。

表のトレイアイコンは、管理サーバー、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、イベントサーバーで実行されるサービスが取り得る状態を示します。これらはすべて、サービス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 サービスアイコン	Recording Server サービスアイコン	Event Server サービスアイコン	Failover Recording Server サービスアイコン	詳細
				**実行中** サーバーサービスが有効で開始したときに表示されます。 Failover Recording Server サービスが実行中の場合、標準のレコーディングサーバーが失敗すると、処理を引き継ぐことができます。
				**停止** サーバーサービスが停止したときに表示されます。 Failover Recording Server サービスが停止しているの場合、標準のレコーディングサーバーが失敗すると、処理を引き継ぐことができません。
				**起動中** サーバーサービスが起動処理中である場合に表示されます。通常、しばらくするとトレイアイコンは **実行中**に変わります。
				**停止中** サーバーサービスが停止処理中である場合に表示されます。通常、しばらくするとトレイアイコンは**停止**に変わります。
				**不確定の状態** サーバーサービスを最初にロードして、最初の情報をまだ受信していない場合に表示されます。最初の情報を受信すると、通常、**起動中**アイコンに変わり、その後**実行中**アイコンに変わります。
				**オフラインで実行中** 通常は、Recording Server サービスまたは Failover Recording サービスが実行されているが、Management Server サービスが実行されていない場合に表示されます。

Manage-ment Server サービスアイコン	Recording Server サービスアイコン	Event Server サービスアイコン	Failover Recording Server サービスアイコン	詳細
				**管理者が承認する必要がある** Recording Server サービスを初めてロードしたときに表示されます。管理者は、Management Client でレコーディングサーバーを承認します。**サーバー**リストを展開し、**レコーディングサーバー**ノードを選択して、**概要**ペインで必要なレコーディングサーバーを右クリックしてから、**レコーディングサーバーの承認**を選択します。

サービスを開始および停止する

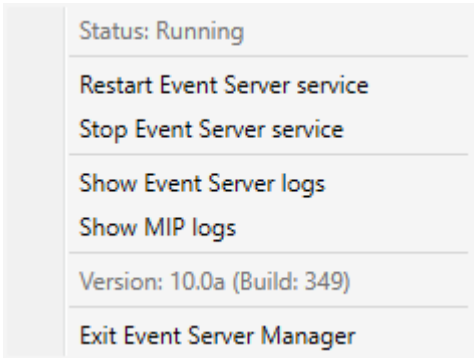
システムサーバーでは、デフォルトでいくつかのサービスがバックグラウンドで実行されています。必要に応じて、それぞれのサービスを個別に開始または停止することができます。

1. **詳細設定**を展開し、**サービス**を選択します。これで、それぞれのサービスのステータスが表示されます。
2. ここで、**停止**ボタンをクリックして、それぞれのサービスを停止することができます。サービスが停止すると、ボタンは**開始**に変わり、必要な時にサービスを再度開始することができます。

Event Server サービスの開始、停止、再起動

通知領域では、トレイアイコンが Event Server サービスの状態(**実行中**など)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、「Event Server サービスの停止 『169ページ 』」を参照してください。

1. 通知領域で、Event Server の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. サービスが停止した場合は、**[Event Server サービスの開始]**をクリックして開始します。トレイアイコンが変わり、新しい状態を示します。
3. サービスを再起動または停止するには、**[Event Server サービスの再起動]**または**[Event Server サービスの停止]**をクリックします。

トレイアイコンの詳細については、「トレイアイコンについて 『166ページ 』」を参照してください。

参照

Recording Server サービスの開始と停止

Event Server サービスの停止

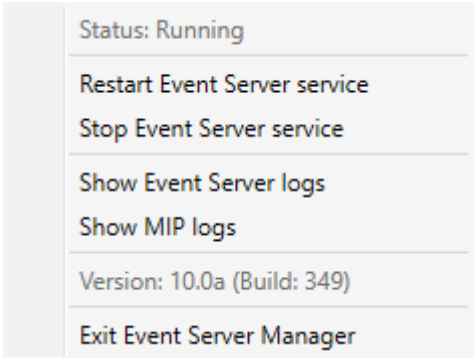
Event Server に MIP プラグインをインストールするときには、まず Event Server サービスを停止してから、再起動する必要があります。ただし、サービスが停止している間は、VMS システムのほとんどの領域が機能しません。

- イベントやアラームは Event Server 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、録画の開始などのアクションをトリガーします。
- XProtect Access、XProtect LPR、および XProtect Transact は構成または XProtect Smart Client で動作しません。
- 分析イベントは動作しません。
- 汎用イベントは XProtect Professional VMS で動作しますが、Event Server に保存されません。
- アラームはトリガーされません。
- XProtect Smart Client では、マップビュー項目、アラームリストビュー項目、およびアラームマネージャワークスペースは動作しません。
- Event Server の MIP プラグインを実行できません。
- Management Application および XProtect Smart Client の MIP プラグインは正しく動作しません。

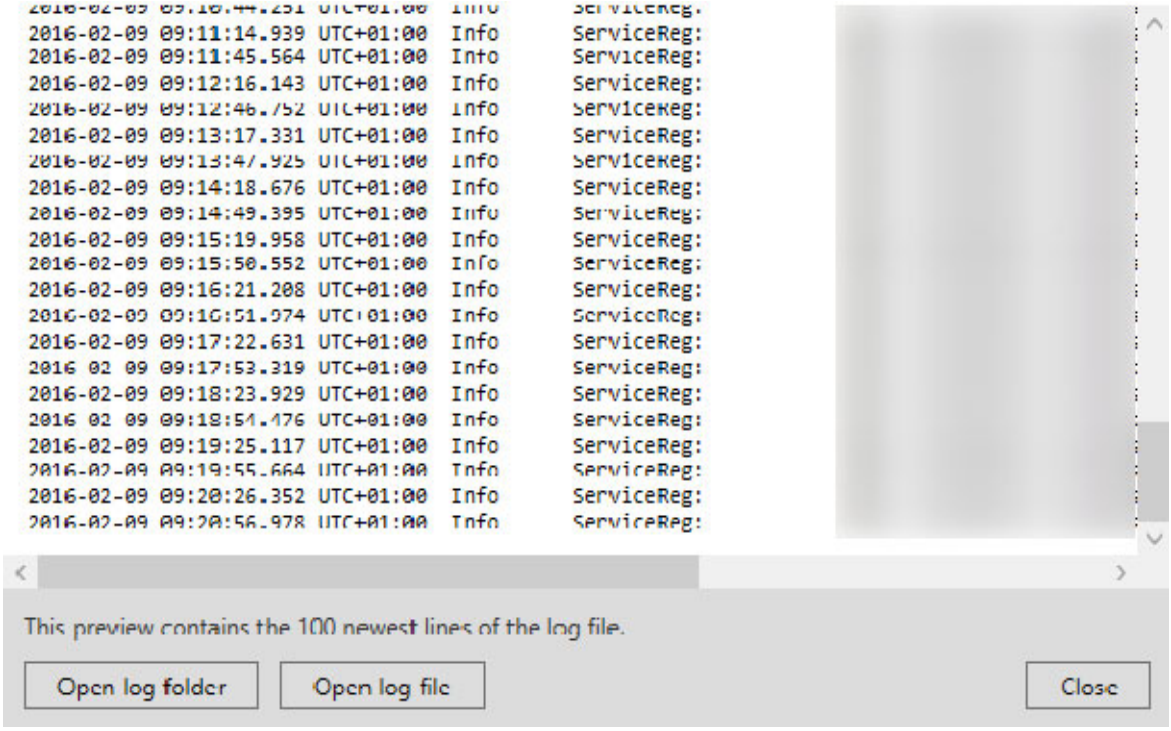
Event Server または MIP ログの表示

Event Server ログで Event Server アクティビティ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、**Event Server** フォルダのサブフォルダにある MIP ログに出力されます。

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. Event Server ログで最新の 100 行を表示するには、**[Event Server 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. ログフォルダを開くには、**[ログフォルダを開く]**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 ログの表示]**をクリックします。ログビューアが表示されます。

ログディレクトリからログファイルが削除された場合、メニュー項目が灰色で表示されます。ログビューアを開くには、まず、ログファイルを次のフォルダのいずれかに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*。

サーバー

LPR サーバー

※本機は、LPR サーバーには対応していません。

LPR システム概要

XProtect LPR について

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、製品比較チャート『12ページ 』を参照してください。

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。

LPR（ナンバープレート認識）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。

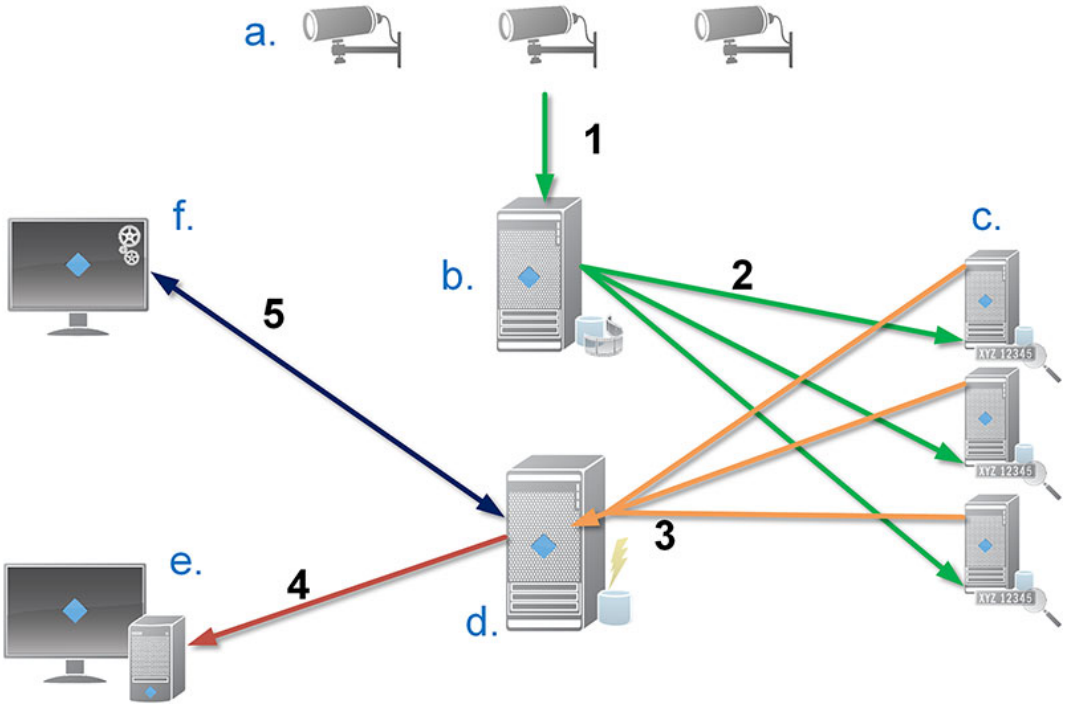
XProtect LPR でのイベントの例：

- 特定の品質での監視システムによる録画をトリガします。
- アラームを有効化します。
- ポジティブ/ネガティブなナンバープレートマッチリストと照合します。
- ゲートを開きます。
- ライトを点灯させます。
- 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します。
- 携帯電話へテキストメッセージを送信します。

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

LPR システムアーキテクチャ

基本的なデータフロー：



1. LPR カメラ(a)がビデオをレコーディングサーバー(b)へ送信します。
2. レコーディングサーバーが、ビデオを LPR サーバー(c)へ送信し、インストールされている国モジュールにあるナンバープレートの特徴と比較して、ナンバープレートを認識します。
3. LPR サーバーが、認識結果をイベントサーバー(d)へ送信し、ナンバープレートマッチリストに対して一致させます。
4. 一致した場合、イベントサーバーはイベントおよびアラームを XProtect Smart Client (e)へ送信します。
5. システム管理者は、LPR の構成全体、たとえば、Management Application (f)からのイベント、アラーム、リストのセットアップを管理します。

LPR サーバー： LPR サーバーは、監視システムが録画した LPR ビデオを処理します。ビデオを分析し、情報をイベントサーバーへ送信します。イベントサーバーはこの情報を使用して、定義されているイベントやアラームをトリガします。Milestone は、この作業を行う専用コンピュータに LPR サーバーをインストールすることをお勧めします。

LPR カメラ： LPR カメラは、他のカメラをビデオとしてキャプチャしますが、一部のカメラは LPR 専用となります。認識を正しく行うには、適切なカメラを使用することが重要です。

国モジュール： 国モジュールとは、特定のタイプや形のナンバープレートを特定の国または地域に属していると定義する一連のルールです。このルールではプレートおよび色、高さ、文字間隔などの特徴を表しており、認識プロセスで使われます。

ナンバープレートマッチリスト： ナンバープレートマッチリストは、ユーザーが作成するリストです。ナンバープレートマッチリストとは、システムに特別な方法で処理させたいナンバープレートの集合のリストです。リストを指定したら、これらのリストでナンバープレートを認識するイベントをセットアップすることで、イベントやアラームをトリガすることができます。

互換性

XProtect LPR は、以下のバージョン 2014 SP3 以降と互換性があります。

- XProtect Corporate
- XProtect Expert
- Milestone Husky™ M30
- Milestone Husky™ M50。

XProtect LPR は、バージョン 2017 R2 以降と互換性があります。

- XProtect Professional+
- XProtect Express+

XProtectLPR は Milestone HuskyM30 と Milestone HuskyM50 に対応しますが、現在これらの製品は XProtect LPR の完全な機能をサポートしていません。

最低限のシステム要件

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『http://www.milestonesys.com/SystemRequirements』をご覧ください。

Milestone は、この作業を行う専用コンピュータに LPR サーバーをインストールすることをお勧めします。

LPR ライセンス

XProtect LPR は、以下の LPR 関連ライセンスを必要とします。

- XProtect LPR の**基本ライセンス**、無制限の台数の LPR サーバーをカバーします。
- XProtect LPR で使用する **LPR カメラ 1 つにつき 1 つのカメラライセンス。** LPR
- XProtect LPR ソリューションで必要な各国、州、地域ついての **LPR 国モジュールライセンス**。**XProtect LPR 基本ライセンスには、LPR 国モジュールライセンスが 5 つ**含まれています。すべての国モジュールは、XProtect LPR 製品をインストールすると自動的にインストールされます。ただし、インストールされたモジュールはデフォルトでは無効であり、使用したい場合はモジュールを有効化 『196ページ の"国モジュールタブ"参照 』する必要があります。ライセンスがあれば、国モジュールはいくつでも有効にできます。

例 : 5 つの LPR 国モジュールライセンスを持ち、10 個の国モジュールをインストールしました。国モジュールを 5 つ選択すると、それ以上は選択できなくなります。他のモジュールをさらに選択するには、まずいずれかの選択を解除する必要があります。

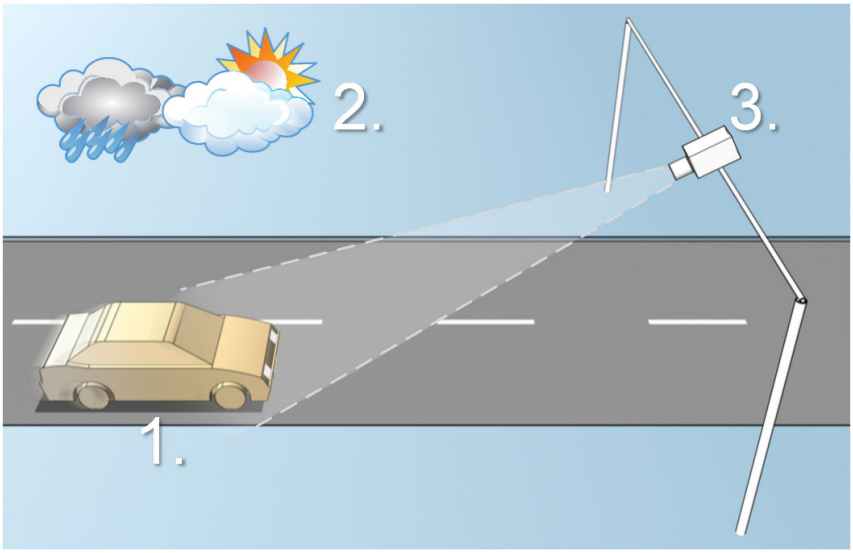
ライセンスの現在のステータスに関する情報は、LPR サーバー情報の表示 『187ページ 』を参照してください。

追加の LPR ライセンスまたは国モジュールを購入するには、ベンダーにお問い合わせください。

LPR 用のカメラの準備について

LPR は、他のビデオ監視とは異なっています。通常は、人間が認識できる最高の画像を提供できる能力に基づいてカメラを選びます。LPR 用にカメラを選ぶ場合、ナンバープレートを検出するのに必要な領域だけが重要になります。このような小さな領域の画像をより鮮明かつ一定の状態でキャプチャできるほど、高い認識率が得られます。

このセクションは、ナンバープレートの認識用にカメラを準備するのに役立ちますが、最適な画像を得るために重要となるカメラおよびレンズに関する重要な原理も紹介しています。



LPR ソリューションの図

LPR の構成に影響を与える要因：

1. 車両

- スピード
- プレートのサイズと位置

2. 周囲の物理的条件

- 照明の条件
- 天候

3. カメラ

- 露光
- 視界
- シャッタースピード
- 解像度
- 位置決め

このような要因はナンバープレート認識の成功に多大な影響を与えるので、これらの要因を十分考慮することが重要です。それぞれの環境に適した方法でカメラを取り付け、XProtect LPR を設定する必要があります。製品が適切に設定されていなければ、正しく機能することを期待できません。LPR に使用するカメラは、通常のカメラより約 5 倍ほど CPU の消費量が大きくなります。カメラが正しく設定されていなければ、認識の成功や CPU の性能レベルに大きな影響を及ぼします。

以下のセクションを読み、LPR ソリューションに影響を与える要因を理解してください。

カメラの位置決め 『175on page 』

カメラの角度 『176on page 』

推奨されるプレート幅 『177on page 』

画像解像度 『178on page 』

カメラの露出の理解 『179on page 』

周囲の物理的条件 『182on page 』

レンズおよびシャッタースピード 『183on page 』

コントラスト 『184on page 』

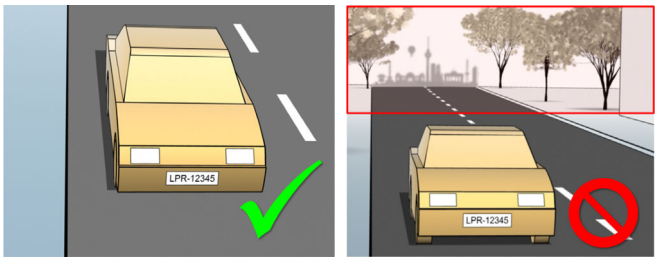
カメラの不要な機能 『185on page 』

カメラの位置決め

LPR で使用するためにカメラを取り付ける場合、プレートを常に検出できるようにするには、対象となる領域がはっきりと鮮明に見えることが重要です。これにより、認識のパフォーマンスを最大限に高め、検出の間違いを低減することができます。

- 車両が画像に出入りする際に、ナンバープレートがはっきり見える部分の画像**だけ**をカバーする必要があります。
- 例えば柱、バリア、フェンス、ゲートなど、カメラの視界を妨げる障害物を避けてください。
- または人、木、交通など、無関係な動く物を避けてください。

無関係な項目があまりに多く含まれていると、検出の邪魔となり、LPR サーバーはナンバープレートではなく、無関係な項目の分析に CPU リソースを浪費することになります。

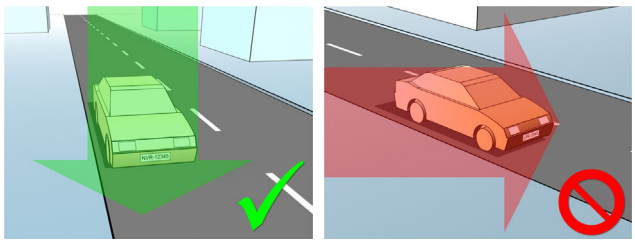


左の図は、視野に対する干渉がない正しい取り付けを示しています。右の図は、誤った取り付けを示しています。カメラの取り付け位置があまりに低く、あまりに多くの背景「ノイズ」があります。

鮮明で邪魔のない視界を得るために、以下を守ってください。

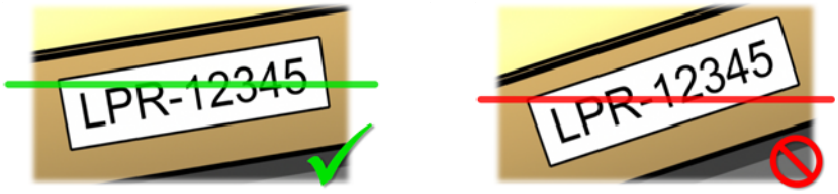
- なるべく対象領域に近い場所にカメラを設置します。
- カメラの角度を調整します。
- ズームを使用します。ズームを使用する場合、必ずカメラの光学ズームを使ってください。

ナンバープレートが右側または左側からではなく、画像の上（または、車両がカメラから遠ざかる方向なら下）から現れるように、カメラを取り付けてください。このようにして、プレートの全体が視界にあるときだけ、ナンバープレートの認識プロセスが始まるようにします。

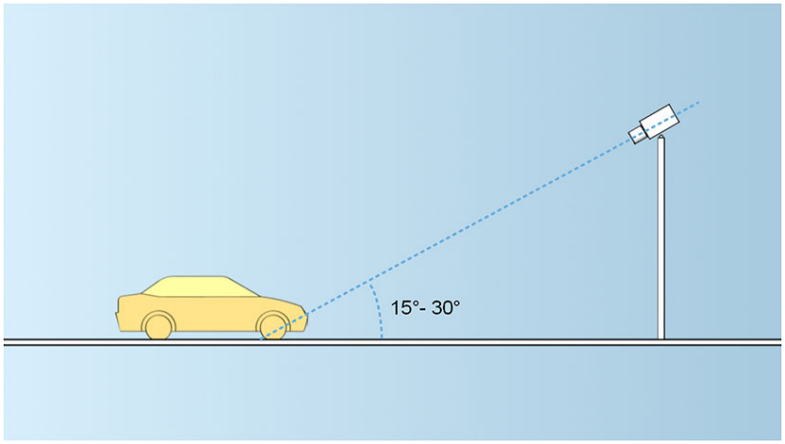


カメラの角度

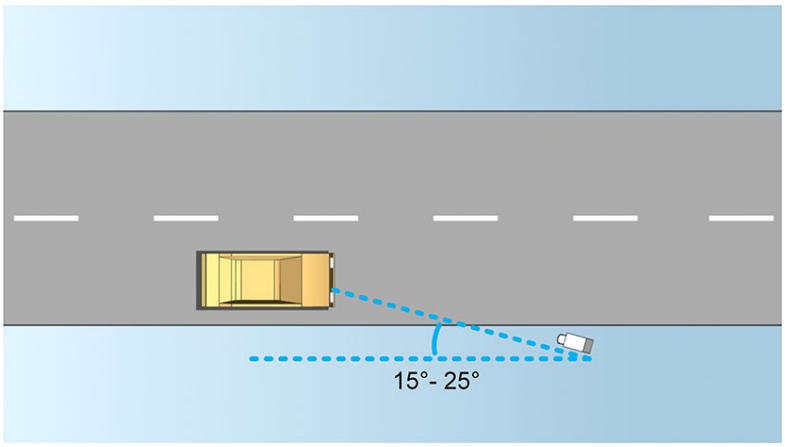
- **単一ラインのルール：** キャプチャした画像でナンバープレートの左端と右端が水平となるように、カメラを取り付けてください。認識に適した正しい角度、間違った角度は下の図を参照してください。



- **垂直角度：** LPR で使用するカメラに推奨される垂直方向の視界の角度は 15°～30°です。

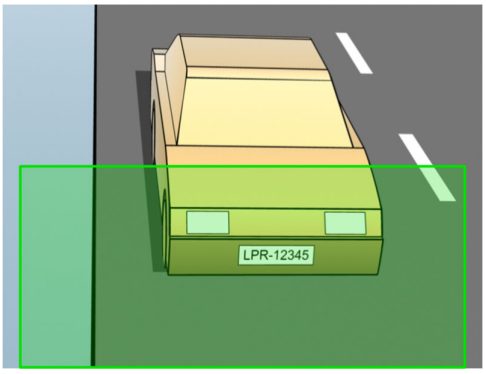


- **水平角度：** LPR で使用するカメラに推奨される水平方向の視界の最大角度は 15°～25°です。



推奨されるプレート幅

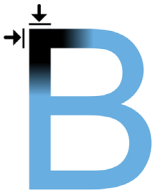
ナンバープレートが画像の中央または下半分にあるときにナンバープレートの理想的なスナップショットをキャプチャできるように、カメラを取り付けてください。



スナップショットを撮り、下記で説明するストローク幅とプレート幅の要件が満たされることを確認してください。標準的な図形エディタを使用して、ピクセル数を数えます。最小プレート幅に達するプロセスが始まるとき、カメラの低解像度から始め、必要なプレート幅に達するまで、より高い解像度へ進めます。

ストローク幅

「*ストローク当たりのピクセル数*」という言葉は、認識されるフォントの最低要件を定義するために使用されます。下の図は、*ストローク*の意味を概説しています。



ストロークの厚みは国やプレートのスタイルによって異なるため、ピクセル/cm やピクセル/インチなどの測定単位は使用しません。

最善の LPR パフォーマンスが得られる解像度は、最低でも 2.7 ピクセル/ストロークが必要です。

プレート幅

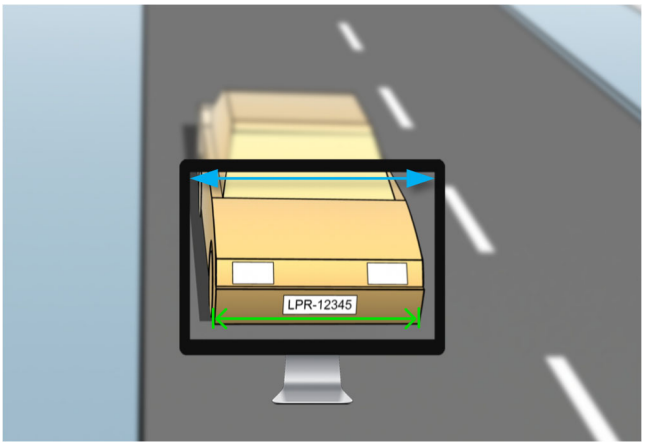
プレートのタイプ	プレート幅	設定	最低プレート幅（ピクセル）
単一行の米国プレート	• プレート幅 12 インチ • ストローク幅約¼インチ	車両停止時、インターレースなし	130
		車両移動時、インターレースあり	215
単一行の欧州プレート	• プレート幅 52 cm • ストローク幅約 1 cm	車両停止時、インターレースなし	170
		車両移動時、インターレースあり	280

停止車両およびインターレースなしの場合と比較して、録画中に車両が移動中でインタレースカメラを使用している場合、画像の半分（偶数ラインのみ）だけが認識で使われます。これは、解像度の要件が約 2 倍であることを意味します。

画像解像度

画質と解像度は、ナンバープレート認識の成功にとって重要です。ただし、ビデオ解像度があまりに高いと、CPU に過負荷となり、スキップや検出の誤りが生じる場合があります。許容できる限り低い解像度にすることで、CPU のパフォーマンスを高め、高い検出率が得られます。

この例では、適切な LPR の解像度を単純な画質計算で得る方法を説明します。計算は、車両の幅に基づきます。



適切な解像度を計算するキャプチャの例。

標準的な車両の幅が 177cm（70 インチ）であると仮定して、横幅が 200cm（78 インチ）であると見積もります。その他に、余分のスペースとして～10%を加えます。正確な幅を知る必要がある場合、対象領域を物理的に測定することもできます。

ストロークの厚さに対して推奨される解像度は 2.7 ピクセル/ストロークです。物理的なストロークの厚さは、ヨーロッパのプレートでは 1cm であり、米国のプレートでは 0.27 インチです。これにより、以下の計算が得られます。

ヨーロッパのプレートの計算（単位 cm）：

200 × 2.7 ÷ 1 = 540 ピクセル

推奨される解像度 = VGA (640×480)

米国のプレートの計算（単位インチ）：

78 × 2.7 ÷ 0.27 = 780 ピクセル

推奨される解像度 = SVGA (800×600)

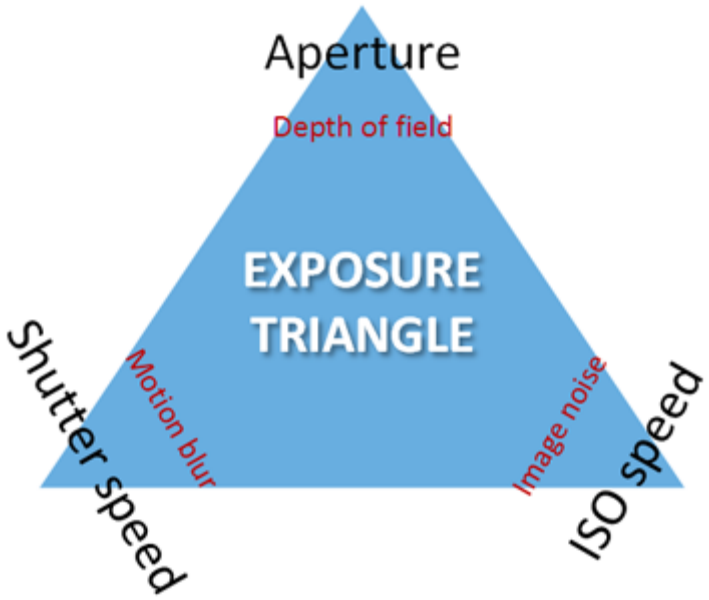
米国のプレートは狭いストロークのフォントを使用しているので、ヨーロッパのプレートより高い解像度が必要になります。

一般的なビデオ解像度

名前	ピクセル (W×H)
QCIF	176×120
CIF	352×240
2CIF	704×240
VGA	640×480
4CIF	704×480
D1	720×576
SVGA	800×600
XGA	1024×768
720p	1280×1024

カメラの露出の理解

カメラの露出により、撮影時の画像の明暗およびシャープネス/ブラーが決定されます。これは、3 つのカメラの設定で決まります。開口、シャッタースピード、ISO スピードです。これらを使用する方法や、相互関係を理解することで、LPR 用にカメラを正しく設定するのに役立ちます。



露出のトライアングル

3 つの設定の組み合わせによって、同じ露出を実現できます。それぞれの設定は他の画像の設定にも影響を与えるので、どの点を重視し、バランスを取るかが重要になります。

カメラ設定	コントロール...	影響...
開口	カメラに入る光の量を制限する、調節可能な開口	被写界深度
シャッタースピード	露出する時間	モーションブラー
ISO スピード	与えられた光の量でのカメラのセンサーの感度	画像ノイズ

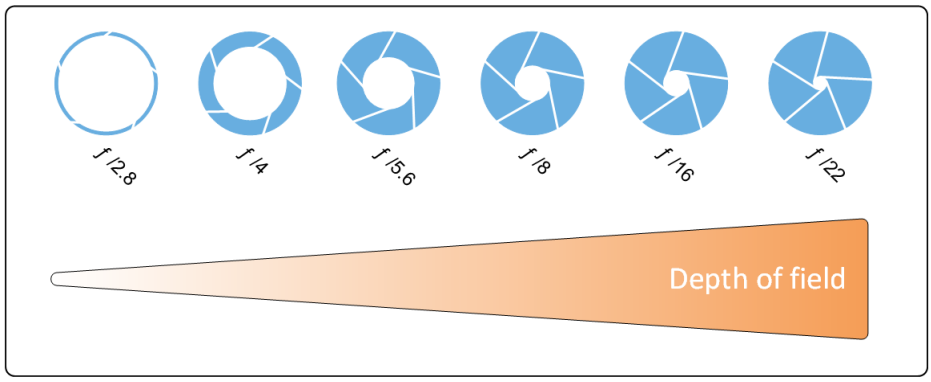
次のセクションでは、各々の設定がどのように指定されるか、それがどのように見えるか、そして、カメラ露出モードがどのようにこの組み合せに影響を及ぼすかを説明します。

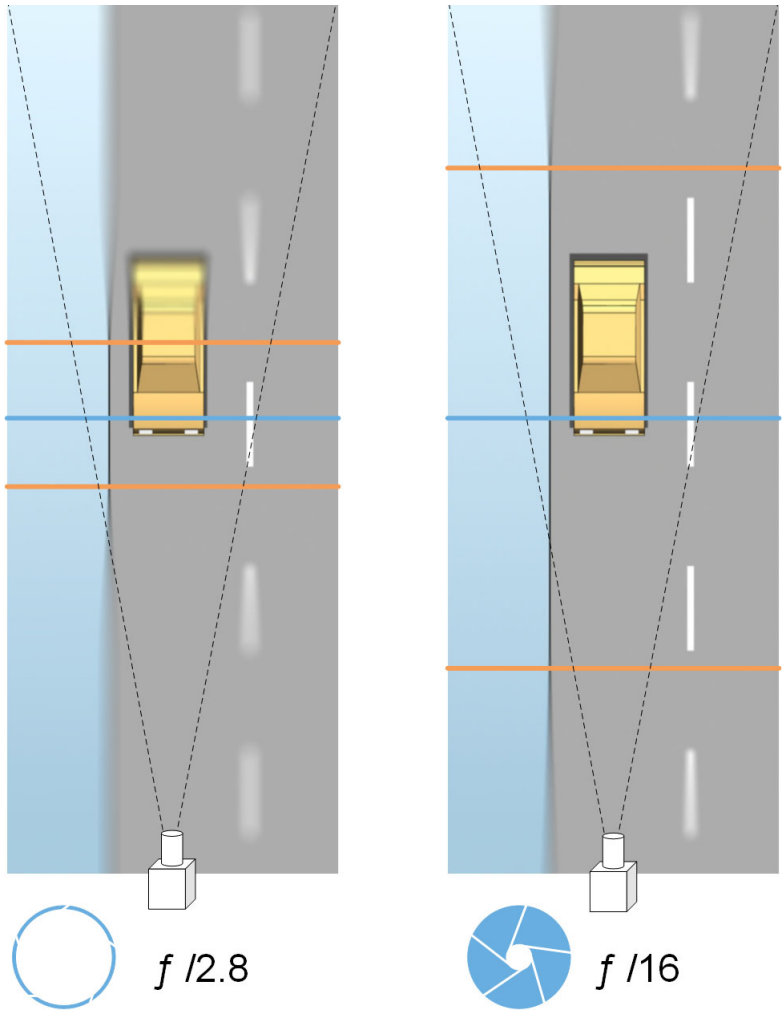
開口設定

開口設定は、レンズからカメラに入る光の量をコントロールします。これはF停止値で指定され、時には直観的に間違っているように感じる場合があります。これは、F停止値が低下すると、開口の領域が増加するためです。

低いF停止値/広い開口 = 狭い被写界深度

高いF停止値/狭い開口 = 広い被写界深度





例の図は、被写界深度がどのようにF停止値の影響を受けるかを説明しています。青いラインは、焦点を示します。

高いF停止値であれば、より遠い距離でもナンバープレートに焦点を合わせることが可能になります。良好な光の状況は、十分な露出にとって重要です。照明の状況が不十分であれば、露出時間をより長く取る必要があり、ぼやけた画像になる危険が増します。

低いF停止値は、焦点エリアを減少させるため、認識で使われるエリアが減少しますが、光が弱い状況に適しています。車両が低速で焦点地域を通行していることが確認できる場合は、低いF停止値でも安定した認識が得られます。

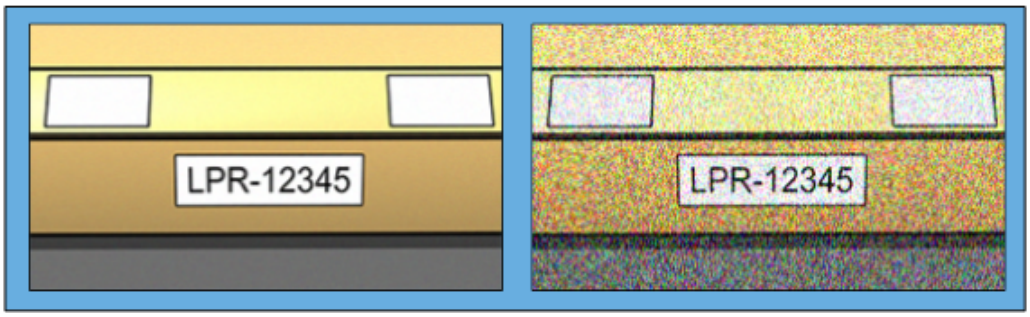
シャッタースピード

カメラのシャッターは、カメラセンサーがいつ開いているか、あるいはカメラレンズから入って来る光によって閉まるかを決定します。シャッタースピードは、シャッターが開いていて、光がカメラに入ることができる期間を意味します。シャッタースピードと露出時間は同じ概念であり、シャッタースピードがより速い場合は、より短い露出時間を意味します。

モーションブラーは、ナンバープレートの認識や監視には望ましくありません。多くの場合、ナンバープレートを検出している間も車両は動いているため、正しいシャッタースピードが重要な要因になります。通常は、モーションブラーを避けるのに十分高いシャッタースピードを保つことが必要ですが、シャッタースピードが高すぎると、光や開口によっては画像の露出不足を引き起こすことがあります。

ISO スピード

ISO スピードは、入って来る光について、カメラの感度の高さを決定します。シャッタースピードと同様に、露出の増減は 1:1 で相関します。ただし、開口やシャッタースピードとは違い、より高い ISO スピードでは画像ノイズが大幅に増えるため、一般には低い ISO スピードが適しています。結果として、ISO スピードを最低値よりも高くするのは、開口やシャッタースピードのみを変更しても望ましい画質が得られない場合に限られます。



低い ISO スピードと高い ISO スピードの画像の例。右の画像では、高い ISO スピードが画像ノイズのレベルに悪影響を及ぼしています。

一般的な ISO スピードは 100、200、400、800 です。ただし、これより値の上下幅が大きなカメラも多く見られます。デジタル一眼レフ (DSLR)カメラでは、多くの場合 50～800（またはそれ以上）の範囲が可能です。

周囲の物理的条件

LPR 用のカメラを取り付けて使用する場合、周囲の環境に関連する以下の要因に注意してください。

- **大量の光：** 周囲の光が強すぎると、露出過度またはシミにつながることがあります。
    - **露出過度**とは、画像が多すぎる光に曝されて、バーンアウトしたり白っぽく見えることがあります。露出過度を避けるため、Milestone は、カメラを高いダイナミックレンジおよびオートアイリスレンズで使うことを推奨しています。**アイリス**は、調節可能な開き口です。この理由により、アイリスは画像の露出に大きく影響します。

- **シミ**は、画像に不要な垂直ラインが現れることです。多くの場合、カメラの電荷結合素子(CCD)画像装置のわずかな欠陥に起因します。CCS 画像装置は、デジタル画像を作成するために使われるセンサーです。

露出過度でシミができたナンバープレートの画像

- **光が少なすぎる：** 周囲の光が少なすぎたり、またはあまりに外部照明が少ない場合、露出不足につながることがあります。
  - **露出不足**とは、画像が曝される光が少なすぎるため、画像が暗くなったりコントラスト 『184ページ 』がほとんどなくなることを指します。自動ゲイン 『185ページ の"カメラの不要な機能"参照 』を無効にできないか、移動している車両の撮影で最大許容シャッター時間 『183ページ の"レンズおよびシャッタースピード"参照 』を設定できない場合、光が少なすぎるとまずは画像にゲインノイズやモーションブラーが発生し、最終的には露出不足となることがあります。露出不足を避けるには、十分な外部照明を使用するか、ゲインを使うことなく暗い環境でも十分に感度が高いカメラを使用してください。
- **赤外線：** 困難な照明状況を克服するもうひとつの方法は、赤外線パスフィルターを赤外線高感度カメラと結合し、人工の赤外線照明を使用することです。回帰反射式のナンバープレートは、特に赤外線照明での使用に適しています。
  - **回帰反射型**は、光源からの光の経路に沿ってまっすぐに送り返す特殊な反射素材で覆うことで実現されています。回帰反射式の物体は、他の物よりはるかに明るく輝いて見えます。これは、夜でもかなりの距離から鮮明に見えることを意味します。回帰反射は道路標識で多用されており、さまざまな種類のナンバープレートでも使われています。
- **天候：** 雪または非常に明るい日光では、カメラを特別に設定することが必要になる場合があります。
- **プレートの条件：** 車両によっては、ナンバープレートが損傷していたり、汚れている場合があります。認識されないように、故意に汚されていることもあります。

レンズおよびシャッタースピード

LPR のカメラのレンズやシャッタースピードを設定するときは、以下に注意してください。

- **フォーカス：**常にナンバープレートに焦点が合っていることを確認してください。
- **自動アイリス：**自動アイリスレンズを使用する場合、必ず開き口を可能な限り開いて、焦点を合わせてください。開き口を開くには、ニュートラルデンシティ(ND)フィルターを使います。あるいは、シャッター時間を手動で設定できるカメラであれば、シャッター時間は非常に短い時間で設定できます。

    - **ニュートラルデンシティ**(ND)フィルター、またはグレーフィルターは、基本的にはカメラに入る光の量を減らします。つまり、カメラに「サングラス」をかけたように機能します。ND フィルターは、画像の露出 『179ページ の"カメラの露出の理解"参照 』に影響を与えます。

- **赤外線 :** 赤外線光源を使用する場合は、可視光と赤外線で切り換える際にフォーカスが変更することがあります。赤外線補正レンズ、または赤外線パスフィルターを使用することで、フォーカスの変更を避けることができます。赤外線パスフィルターを使用する場合は、昼間でも赤外線光源が必要である点に注意してください。

- **車両速度 :** 車両の移動中は、モーションブラーが避けられるよう、カメラのシャッター時間を十分に短くする必要があります。適切な最長シャッター時間を計算する式は、以下の通りです。

    - **車両速度（時速）：** シャッター時間（秒）= 1 秒 /（11 × 最大車両速度、キロメートル/時間）

車両速度（mph）： シャッター時間（秒） = 1 秒 /（18 × 最大車両速度、マイル/時間）ここで、/ は「除算」を意味し、× は「乗算」を意味します。次の表では、異なる車両速度でのカメラシャッタースピードに関するガイドラインを提供しています。

シャッター時間（単位は秒）	最大車両速度（単位はキロメートル/時間）	最大車両速度（単位はマイル/時間）。
1/50	4	2
1/100	9	5
1/200	18	11
1/250	22	13
1/500	45	27
1/750	68	41
1/1000	90	55
1/1500	136	83
1/2000	181	111
1/3000	272	166
1/4000	363	222

コントラスト

LPR カメラに適切なコントラストを決定する際は、ナンバープレートの特性やナンバープレートの背景色の違いによるグレー値（画像を 8 ビットグレースケールに変換する場合）の違いを考慮してください。

良好なコントラスト

許容されるコントラスト、認識が何とか可能です。

8 ビットグレースケール画像のピクセルは 0～255 の値となり、グレースケール値 0 は完全な黒、255 は完全な白になります。入力画像を 8 ビットグレースケール画像に変換する場合、テキストの 1 ピクセルと背景での 1 ピクセルの最小ピクセル値の差異は少なくとも 15 でなければなりません。

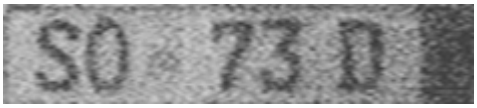
画像のノイズ 『185ページ の"カメラの不要な機能"参照 』、圧縮 『185ページ の"カメラの不要な機能"参照 』の使用、照明の状態などによって、ナンバープレートの文字や背景の色の判断が難しくなる点に注意してください。

カメラの不要な機能

LPR 用のカメラを設定する際は、以下に注意してください。

- **自動ゲイン調整：**最も一般的に見られるカメラに起因する画像干渉には、ゲインノイズが挙げられます。
  - **ゲイン**は、基本的にはカメラがシーンの画像をキャプチャして、それに光を配分する方法です。光が画像に最適であるように配分されないと、結果はゲインノイズになります。

    ゲインを制御するには、複雑なアルゴリズムを適用する必要があり、多くのカメラにはゲインの自動調整機能が備えられています。ただし、こうした機能が LPR で役立つことは残念ながらあまりないため、Milestone は、カメラの自動ゲイン機能を可能な限り低く設定することを推奨しています。あるいは、カメラの自動ゲイン機能を無効にしてください。

    ゲインノイズがあるナンバープレートの画像

    周囲が暗い場合、十分な外部照明を設置することでゲインノイズを回避することができます。

- **自動エンハンス：** 一部のカメラは、輪郭、エッジ、コントラストのエンハンスアルゴリズムを使って、画像が人間の目で見やすいように補正します。このようなアルゴリズムは、LPR プロセスで使用するアルゴリズムに干渉します。したがって、Milestone では、カメラの輪郭、エッジ、コントラストのエンハンスアルゴリズムを可能な限り無効にするよう推奨しています。

- **自動圧縮：** 圧縮率が高くなるほど、ナンバープレートの画像の品質には悪影響があります。高い圧縮率を使用する場合、最適な LPR パフォーマンスを実現するには、より高い解像度 『177ページ の"推奨されるプレート幅"参照 』が必要になります。低い JPEG 圧縮を使用する場合、画像を JPEG 品質レベルの 80%以上で保存しており、画像の解像度、コントラスト、フォーカスは通常通りであり、ノイズレベルも低い限り、LPR に与える悪影響も非常に小さくなります。

左:ナンバープレート画像を JPEG 品質レベル 80%（つまり低圧縮）で保存していれば許容範囲となります。

右:ナンバープレート画像を JPEG 品質レベル 50%（つまり高圧縮）で保存していれば許容範囲外となります。

LPR のインストール

XProtect LPR のインストール

XProtect LPR を実行するには、以下をインストールする必要があります。

- 少なくとも 1 つの LPR サーバー。
- Management Applicationおよびイベントサーバーを実行するすべてのコンピュータにLPRプラグイン。
- LPRServer サービスを実行するために選択されたユーザーが管理サーバーにアクセスできることを確認してください。

Milestone では、管理サーバーやレコーディングサーバーと同じコンピュータに LPR サーバーをインストールしないことを推奨しています。

インストールの開始：

1. Milestone Web サイト 『http://www.milestonesys.com/downloads』のダウンロードのページへ移動します。
2. 次の 2 つのインストーラをダウンロードします。
   - *Milestone XProtect LPRManagement Application およびイベントサーバーを実行するすべてのコンピュータにプラグイン*インストーラ。
   - この目的のために割り当てられたすべてのコンピュータに *Milestone XProtect LPR サーバー*インストーラ。また、1 台のコンピュータに LPR 用の仮想サーバーを作成することもできます。
3. 最初に、すべての *Milestone XProtect LPR プラグイン*インストーラを実行します。
4. 次に、*Milestone XProtect LPR サーバー*インストーラを実行します。

   インストール中に、 製品の管理サーバーまたは 製品の画像サーバーの IP アドレスまたはホスト名を、監視システムの管理者権限を持つユーザーアカウントのドメインユーザー名およびパスワードと共に指定します。
5. Management Application を起動します。

   Management Application のナビゲーションペインで、Management Application が自動的に、インストール済みの LPR サーバーを **LPR サーバー**リストに一覧表示します。
6. 必要なライセンス 『173ページ の"LPR ライセンス"参照 』があることを確認してください。
7. すべての国モジュールは、XProtect LPR 製品をインストールすると自動的にインストールされます。ただし、インストールされたモジュールはデフォルトでは無効であり、使用したい場合はモジュールを有効化 『196ページ の"国モジュールタブ"参照 』する必要があります。ライセンスがあれば、国モジュールはいくつでも有効にできます。

Management Application から LPR サーバーを追加することはできません。

初期インストール後にさらに LPR サーバーをインストールする必要がある場合は、それらのサーバーで *Milestone XProtect LPR サーバー*インストーラを実行します。

XProtect ソフトウェアが動作するコンピュータ上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、C:¥ProgramData¥Milestone¥XProtect LPR フォルダを除外することが重要です。これを除外しない場合、ウ

イルススキャニングにかなりの量のシステムリソースが使用され、スキャニングのプロセスによって一時的にファイルがロックされることがあります。

XProtect LPR のアップグレード

XProtect LPR をアップグレードするには、インストール『186ページ の"XProtect LPR のインストール"参照 』と同じステップに従います。

XProtect LPR 1.0 から XProtect LPR 2016 へアップグレードすると、一部の認識設定は、前の構成と互換性を持ちません。新しい設定を適用するには、構成を保存しなければなりません。以前に使用可能であったフリップ、回転、ビデオの色の反転の設定は除外されました。今後もこれらの機能が必要になる場合、カメラ自体の設定を変える必要があります。

LPR の設定

LPR サーバー情報の表示

LPR サーバーの状態をチェックするには：

1. Management Application のナビゲーションペインで、**サーバー**を展開して、**LPR サーバー**を選択します。

   LPR サーバー情報ウィンドウが開き、サーバーステータスの概要が表示されます。

   - 名前
   - ホスト名
   - ステータス

2. 関連する LPR サーバーを選択して、このサーバーのすべての詳細 『187ページ の"LPR サーバー情報のプロパティ"参照 』を確認します。

LPR サーバー情報のプロパティ

フィールド	詳細
名前	ここで、LPR サーバーの名前を変更することができます。
ホスト名	LPR サーバーのホスト名を表示します。 LPR サーバーの名前の最初の部分は、LPR 監視インストールのホストコンピュータの名前で構成されます。例：*MYHOST.domainname.country*。

フィールド	詳細
ステータス	LPR サーバーのステータスを表示します。 サーバーを追加したばかりであれば、ステータスは次のようになります。 • *LPR カメラが構成されていません。* システムが正しく動作している場合、ステータスは次のようになります。 • *すべての LPR カメラが実行中です。* あるいは、システムは次のように返します。 • *サービスが応答しません。* • *監視システムに接続していません。* • *サービスは実行されていません。* • *イベントサーバーが接続されていません。* • *未知のエラー。* • *X / Y 台の LPR カメラが実行中です。*
サービス起動時間	LPR サーバーが最後にダウンして、LPR Server サービスが起動されるまでのアップタイムを表示します。
コンピュータの CPU 使用率	LPR がインストールされているすべてのコンピュータでの CPU 使用率を表示します。
使用可能なメモリ	LPR サーバーでどれだけのメモリが使用可能であるかを表示します。
認識されたナンバープレート	このセッションで LPR サーバーが認識したナンバープレートの数を表示します。
LPR カメラ	LPR サーバーで実行中の有効な LPR カメラの数とそのステータスを表示します。
使用可能な LPR カメラ	ライセンスに基づき、この数字はすべての LPR サーバーで追加および使用できる LPR カメラの合計数を示しています。
使用可能な国モジュール	ライセンスに基づき、この数字はすべての LPR サーバーで追加および使用できる国モジュールの合計数を示しています。また、既に使用している国モジュールの数も表示されます。

LPR 用のカメラの設定

Management Application の前提条件

カメラを取り付けて、Management Application に追加した後、LPR の要件に適合するようにそれぞれのカメラの設定を調整します。カメラの設定の調整は、それぞれのカメラデバイスのプロパティのタブで行います。

関連するカメラについて、Milestone では、以下のように推奨しています。

- ビデオコードは、JPEG に設定します。

H.264 または H.265 コーデックを使用している場合、サポートされるのはキーフレームだけです。これは、通常は 1 秒当たり 1 フレームであり、LPR にとっては十分ではありません。より高いフレームレートでは、必ず JPEG コーデックを使用してください。

- 1 秒当たり 4 フレームを指定します。
- 圧縮を避けるため、高品質に設定します。
- 可能であれば、1 メガピクセル未満の解像度を指定します。
- 可能であれば、自動シャープネスを低いレベルに保ちます。

LPR の基本を理解するため、LPR 用カメラの準備について 『173ページ の"LPR 用のカメラの準備について"参照 』の情報に精通するようにしてください。

スナップショットについて

システムは、スナップショットを使用して自動的に構成を最適化し、適用された認識設定の効果を視覚化します。

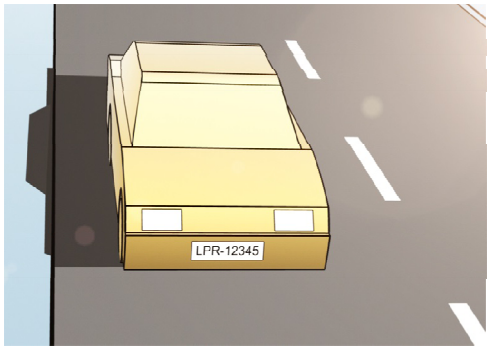
カメラの初期設定を完了するには、有効なスナップショットを少なくとも 1 つ提供する必要があります。

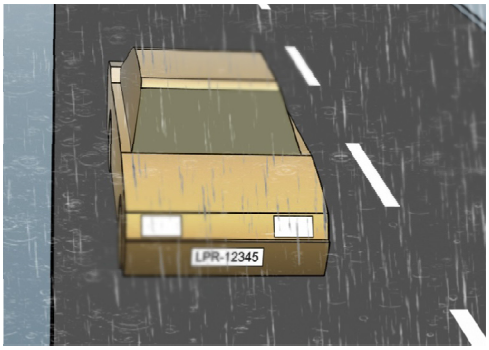
ガイドラインとして、ナンバープレートの認識が必要となる現実的な周囲の物理的状況および条件で車両のスナップショットを撮ります。

下記のリストには、スナップショットをキャプチャおよび選択する場合に考慮しなければならない状況を例示しています。すべてが、実際の周囲状況で適用されるわけではありません。

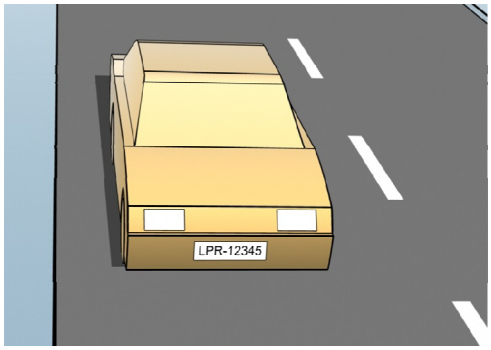
Milestone では、一般的な状況を反映しているスナップショットを最低でも 5～10 枚選択するよう推奨しています。

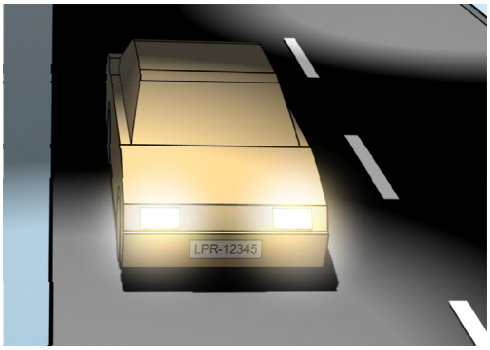
- **例えば天候については、晴れの日および雨の日となります。**



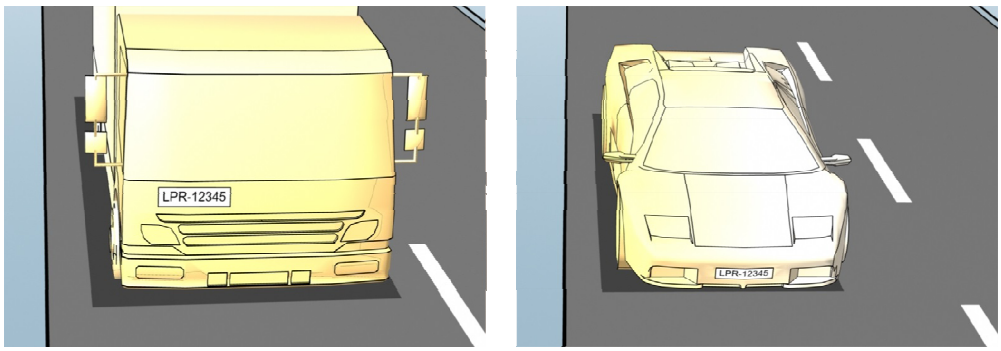


- **また、照明は日光と夜間のものを使用します。**

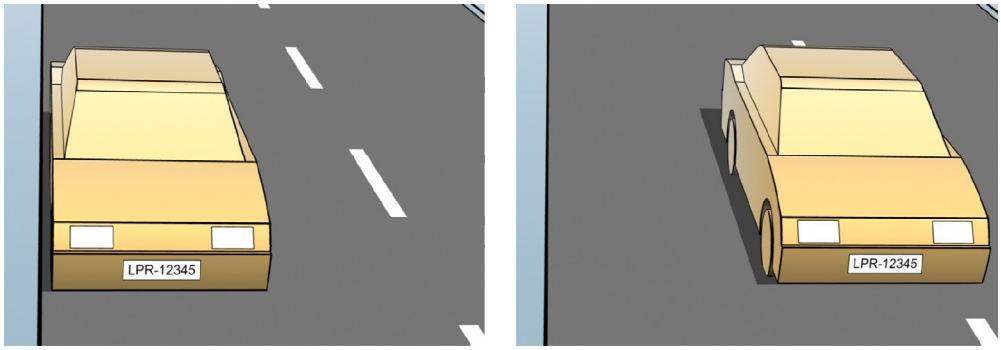




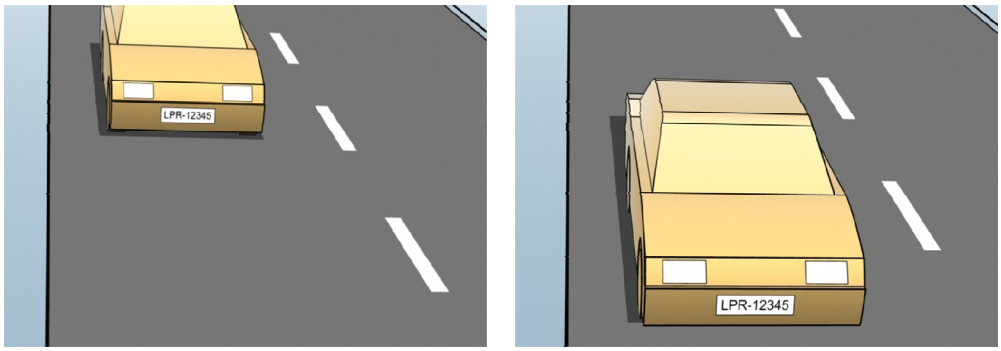
- 車両のタイプ、認識エリアの上下を定義します。



- 車線に位置付け、認識エリアの左および右を指定します。



- 車までの距離、**LPR** がナンバープレートを分析するエリアを定義します。



LPR カメラの追加

LPR のカメラを設定するには、まず **LPR カメラの追加**ウィザードを実行します。ウィザードの指示に従って主要な設定手順を行い、設定を自動的に最適化します。

ウィザードを実行するには：

1. Management Application のナビゲーションペインで、**サーバー**を展開し、**LPR サーバー**を展開してから、**LPR カメラ**を選択します。
2. **LPR カメラ**を右クリックします。

3. 表示されるメニューから、**LPR カメラの追加**を選択して、ウィザードの指示に従います。
   - LPR で設定したいカメラを選択します。
   - LPR カメラで使用したい国モジュール 『196ページ の"国モジュールタブ"参照 』を選択します。
   - 設定の確認で使用するスナップショット 『189ページ の"スナップショットについて"参照 』を選択します。
   - スナップショット分析の結果 『197ページ の"設定の確認"参照 』を確認します。
   - 使用するナンバープレートマッチリスト 『198ページ の"ナンバープレートマッチリストについて"参照 』を選択します。リストをまだ作成していない場合、デフォルトを選択します。
4. 最後のページで、**閉じる**をクリックします。

   LPR カメラが Management Application に表示され、選択に基づいて、システムはカメラの認識設定 『192ページ の"認識設定タブ"参照 』を最適化します。
5. 追加したカメラを選択して、設定を確認します。システムが正しくナンバープレートを認識しない場合にのみ、設定の変更が必要になります。
6. **認識設定**タブで、設定の確認 『197ページ 』をクリックします。

LPR カメラの設定を調整します。

LPR カメラを **LPR カメラの追加**ウィザードで追加すると、システムは自動的に LPR カメラの設定を最適化します。初期設定を変更したい場合は、以下のように行います。

- サーバーの名前を変更するか、サーバーを変更します 『191ページ の"情報タブ"参照 』。
- 認識設定を調整し、確認します 『192ページ の"認識設定タブ"参照 』。
- さらにナンバープレートマッチリストを追加します 『195ページ の"マッチリストタブ"参照 』。
- 追加の国モジュールを有効にします 『196ページ の"国モジュールタブ"参照 』。

情報タブ

このタブは、選択したカメラの情報を提供します。

名前	詳細
有効	LPR カメラは、初期設定後、デフォルトで有効になっています。LPR との接続で使用していないカメラは無効にします。 LPR カメラを無効にしても、監視システムでの通常の録画は停止しません。
カメラ	XProtect Management Application およびクライアントに表示されるのと同様に、選択したカメラの名前が表示されます。
詳細	このフィールドを使用して、説明を入力します（オプション）。

名前	詳細
サーバーの変更	クリックして、LPR サーバーを変更します。 負荷のバランスを取ることが必要な場合、LPR サーバーを変更することをお勧めします。たとえば、LPR サーバーで CPU の負荷が高すぎる場合、Milestone では、1 つまたは複数の LPR カメラを別の LPR サーバーへ移動させることを推奨しています。

認識設定タブ

認識設定は自動設定され、LPR カメラの初期設定中に、主にユーザーが提供したスナップショットに基づいて自動的に最適化されます。

アクションボタン

これらのボタンを使用して、初期設定後に設定を更新および確認します。

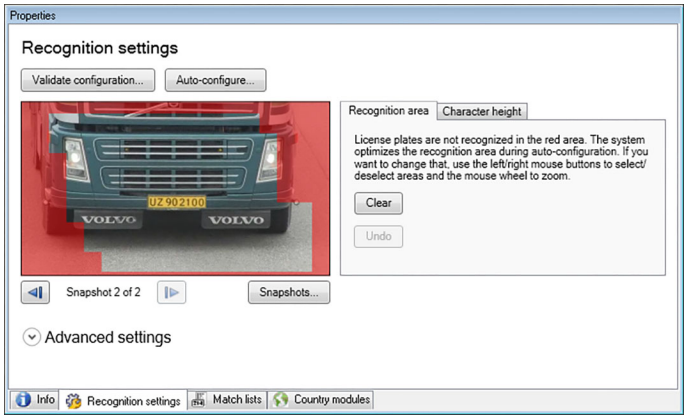
名前	詳細
スナップショット	スナップショット 『197ページ の"スナップショットの選択"参照 』を追加または削除します。
設定の確認	ナンバープレートが正しく 『197ページ の"設定の確認"参照 』認識されるかテストします。
自動設定	手動での変更を無視し、設定を最適化 『198ページ の"自動設定"参照 』します。

認識領域

システムは自動設定中に認識エリアを最適化しますが、これを手動で変更できます。

パフォーマンスを最適化し、検出ミスを低減するために、Milestone では、必ず明確に定義された「準備万端」の認識エリアを選択することを推奨しています。車両が画像に出入りする際に、ナンバープレートがはっきり見える部分の画像**だけ**をカバーする必要があります。認識エリア 『175ページ の"カメラの位置決め"参照 』では人、木、交通など、無関係な動く物を避けてください。

ナンバープレートは、赤いエリアでは認識されません。



認識するエリアを指定する場合、以下のオプションがあります。

名前	詳細
クリア	クリックするとすべての選択が解除され、エリアは LPR で使用されません。新しいエリアを選択します。
元に戻す	クリックすると、認識エリアの最後に保存された設定に戻ります。

LPR カメラの設定を変更した場合、構成を確認 『197ページ の"設定の確認"参照 』して、システムが正しくナンバープレートを認識しているか確認してください。

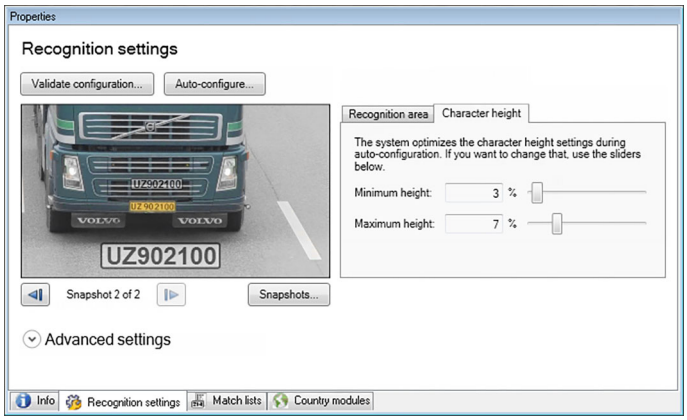
文字の高さ

システムは自動設定中に文字の高さを最適化しますが、これを手動で変更できます。

ナンバープレート文字の最小および最大の高さ（パーセント単位）を定義します。文字の高さは、可能な限り、実際のナンバープレートの文字と同じ高さを選択します。

これらの文字の設定は、認識時間の決定要素となるため、認識プロセスに影響を及ぼします。通常は、文字の最小および最大の高さの差が大きいほど、

- LPR プロセスは複雑になります。
- CPU 負荷は高くなります。
- 結果の待ち時間は長くなります。



スナップショットのオーバーレイは、現在定義されている文字の高さの設定を示します。オーバーレイは、右の文字の高さの設定に従って、比例的に増減します。簡単に比較するには、オーバーレイをスナップショットの実際のナンバープレートの上部へドラッグすることができます。必要に応じてマウスホイールを使用してズームします。

名前	詳細
最低高さ	スライダーを使用して、最小文字の高さを認識プロセスへ含めるように設定します。システムは、指定した値未満の文字を含んでいるナンバープレートでは認識プロセスを開始しません。
最大高さ	スライダーを使用して、最大文字の高さを認識プロセスへ含めるように設定します。システムは、指定した値を超える文字を含んでいるナンバープレートでは認識プロセスを開始しません。

LPR カメラの設定を変更した場合、構成を確認 『197ページ の"設定の確認"参照 』して、システムが正しくナンバープレートを認識しているか確認してください。

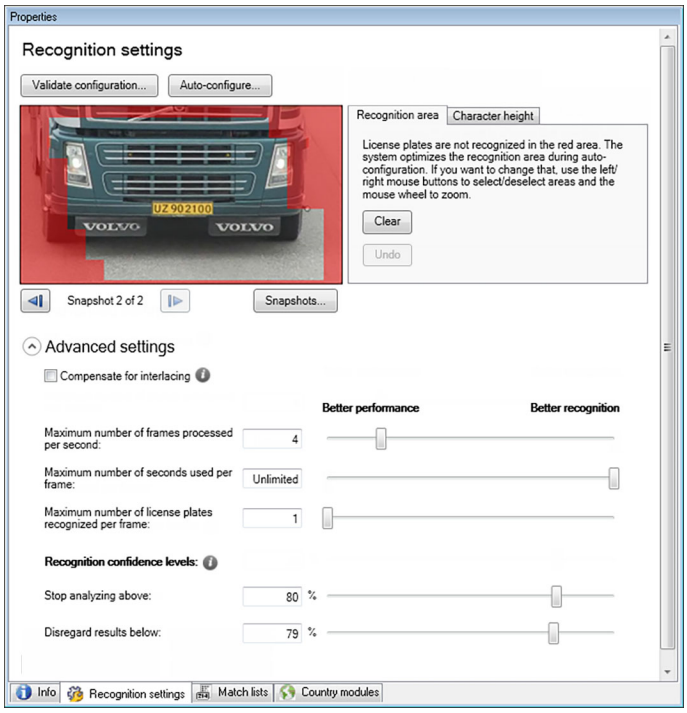
拡張設定

システムは自動設定中に詳細設定を最適化しますが、これを手動で変更できます。

認識プロセスは、次の 2 つのステップに分割できます。プレートを見つけることと、プレートの文字を認識することです。詳細設定によって、処理速度と認識品質の度合いを指定することができます。

一般的なルールとしては、認識品質を高くすると、

- 高い計算能力が必要となります。
- 結果として、CPU 負荷が高くなります。
- そのため結果が返されるまでの時間が長くなります。



詳細設定を調整して、度合いを定義します。いずれかの停止条件が満たされると認識プロセスが停止し、その時点で認識したナンバープレートが返されます。

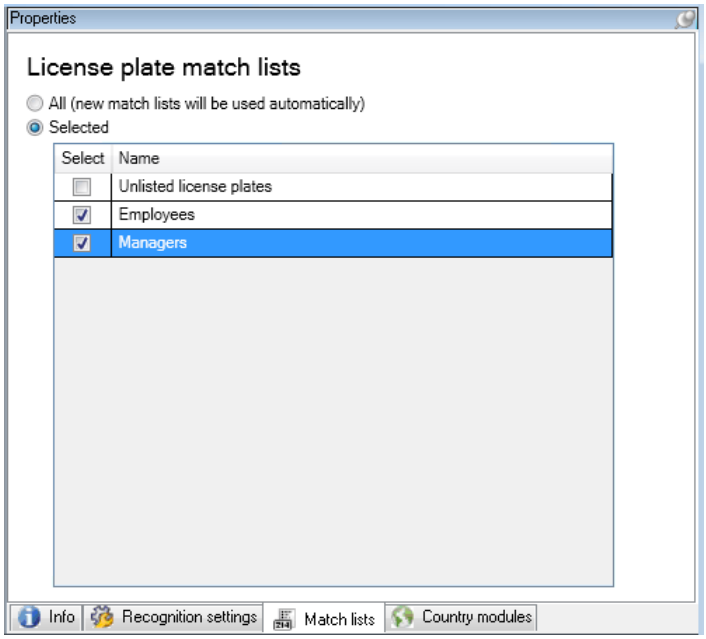
名前	詳細
インターレースの補正	LPR カメラがインターレースビデオを送信し、LPR でインターレースを解除した画像に複数のエフェクトの組み合わせが確認される場合に、この機能を有効にします。これにより画像の品質が向上し、認識結果が改善されます。

名前	詳細
1 秒当たりで処理されるフレームの最大数	LPR ソリューションが 1 秒当たりに処理できるフレームの最大数を指定します。LPR プロセスに対して低い値を指定している場合、不要な負荷を LPR サーバーに与えることなく、録画用のカメラでより高いフレームレートを適用することができます。 **無制限**は、この設定の停止基準を定めていないことを意味します。
フレーム当たりの最大使用秒数	LPR ソリューションが 1 フレームの認識に費やせる最長の秒数を指定します。調整する場合、推奨される値は *200* ms/フレームです。 **無制限**は、この設定の停止基準を定めていないことを意味します。
フレーム当たりの最大ナンバープレート認識数	1 フレーム当たりで、認識できるナンバープレートの最大数を指定します。この設定を変更するのは、たとえば 1 台の LPR カメラで複数のレーンを検出する場合など、本当に必要な場合だけにしてください。 **無制限**は、この設定の停止基準を定めていないことを意味します。
分析の停止	最小信頼性レベルを指定します（パーセント単位）。指定された値と等しいか、より高い信頼性レベルのナンバープレート読み取り結果をシステムが返せるようになるまで、認識プロセスは続きます。
以下の結果を無視する	システムは、指定された値と等しいか、より低い信頼性レベルのナンバープレート読み取り結果を拒否します。 概して、**分析の停止**と**以下の結果を無視する**の値の差を小さく保つと、CPU 負荷が低くなり、システムはより速く認識結果を返せます。

LPR カメラの設定を変更した場合、構成を確認 『197ページ の"設定の確認"参照 』して、システムが正しくナンバープレートを認識しているか確認してください。

マッチリストタブ

このタブで、特定の LPR カメラでナンバープレートと一致させたいナンバープレートマッチリストを選択します。リストは必要な数だけ作成 『199ページ の"ナンバープレートマッチリストの新規追加"参照 』できます。



名前	詳細
すべて	ナンバープレートは、すべての使用可能なリストおよび将来のリストに対して一致が確認されます。
選択済み	ナンバープレートは、選択したリストに対してだけ一致が確認されます。使用可能なリストを 1 つ以上選択します。

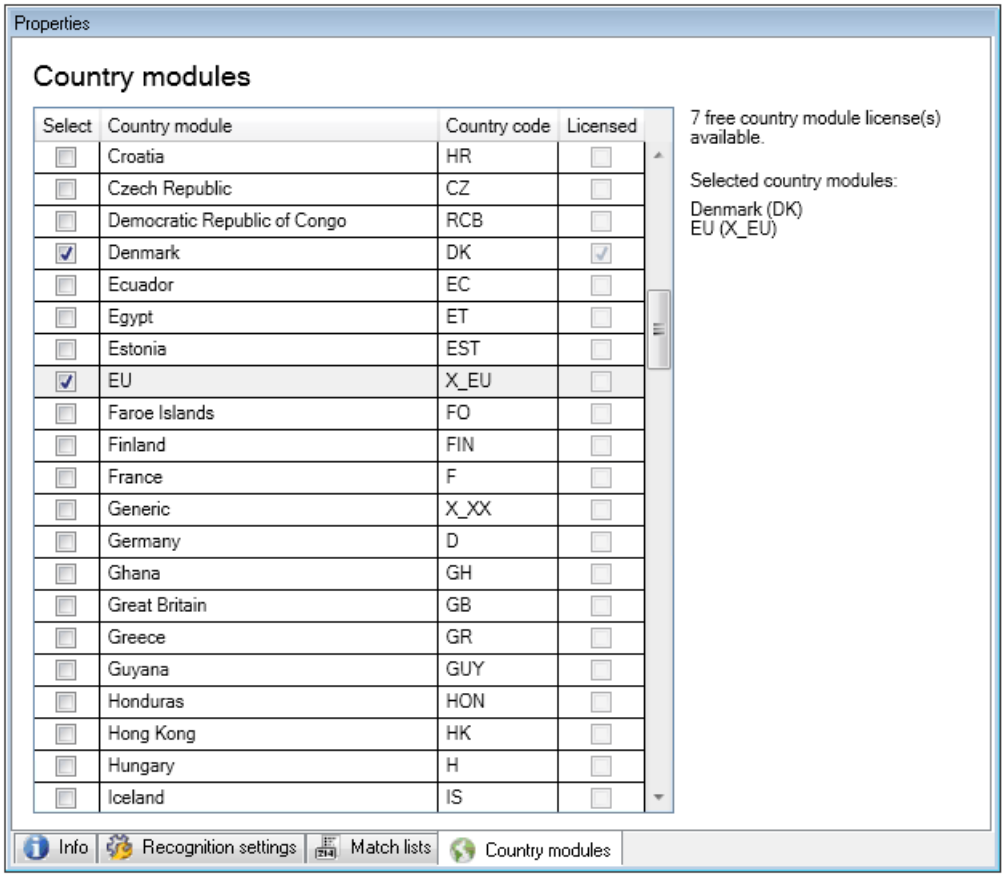
LPR カメラの設定を変更した場合、構成を確認 『197ページ の"設定の確認"参照 』して、システムが正しくナンバープレートを認識しているか確認してください。

国モジュールタブ

ここで、特定の LPR カメラで使用したい国モジュールを選択します。選択できるリストは、インストールしてある国モジュールおよび取得しているライセンス 『173ページ の"LPR ライセンス"参照 』により異なります。

国モジュールとは、特定のタイプや形のナンバープレートを特定の国、州、地域に属していると定義する一連のルールです。

既にライセンスを取得しているモジュールは、**ライセンス**列にチェックマークが示されます。探している国モジュールがリストにない場合は、ベンダーに問い合わせてください。



名前	詳細
選択	クリックして、国モジュールを選択または選択解除します。右側にある選択された国モジュールのリストは、自動的に更新されます。
国モジュール	インストール済みの国モジュールをリストします。
国コード	国モジュールを表す文字です。
ライセンスあり	国モジュールに既にライセンスが付与されているかを表示します。必要な数のカメラに対して、ライセンス済みの国モジュールを選択できます。

LPR カメラの設定を変更した場合、構成を確認 『197ページ の"設定の確認"参照 』して、システムが正しくナンバープレートを認識しているか確認してください。

スナップショットの選択

最初に LPR を **LPR カメラの追加**ウィザードで設定した際に、スナップショット 『189ページ の"スナップショットについて"参照 』も追加しています。構成の最適化を改善するため、代表的なスナップショットをさらに追加することができます。

1. 関連するカメラを選択します。
2. **認識設定**タブで、**スナップショット**をクリックします。
3. ライブビデオからスナップショットを取得するか、外部の場所からインポートしてください。**次へ**をクリックします。

   システムは、カメラ用に選択したスナップショットを分析します。
4. 次のページで、各々のスナップショットを承認または拒否します。システムが認識できるナンバープレートがない場合、**戻る**をクリックして、より画質の高いスナップショットを新規追加します。これでもシステムで正しく認識できない場合は、設定の変更が必要になります。カメラの取り付けや設定が正しい 『173ページ の"LPR 用のカメラの準備について"参照 』ことを確認してください。
5. すべてのスナップショットを承認したら、**次へ**をクリックして、ウィザードを閉じます。
6. **認識設定**タブで、**設定の確認** 『**197**ページ 』をクリックします。

設定の確認

現在の設定を確認して、いずれかの設定を変更する必要があるか、あるいはさらにスナップショットを提供するかを確認します。確認機能では、システムがいくつのナンバープレートを認識するか、および正しく認識されたかどうかが分かります。

これは信頼性レベルが適切に設定されているか、システムの構成が最適であるかを判断するのに役立ちます。

1. 関連するカメラを選択します。
2. **認識設定**タブで、**設定の確認**をクリックします。

   現在の設定に基づいて、システムはカメラに対して選択しているスナップショットを分析し、結果概要を返します。

   - **検出したナンバープレート：** 認識したナンバープレートの数、例、3 / 3。
   - **平均信頼性：** ナンバープレートが認識されたことについての平均信頼性のパーセント値。

- **平均処理時間**：スナップショットを分析して、読み取り結果を返すまでの平均時間（単位は ms）。

License plates detected:	**2 of 2**
Average confidence:	**91 %**
Average processing time:	**112 ms**

3. 現在の設定が要件に適合している場合は、**閉じる**をクリックします。
4. 結果をさらに詳しく調べたい場合、**次へ**をクリックすると、それぞれのスナップショットの結果を確認することができます。これにより、問題の原因となっている状況を特定できます。

設定は必要なだけ何度も確認できます。また、LPR カメラや異なる設定でも確認することができます。

自動設定

LPR カメラの自動設定により、すべての手動での設定変更に上書きされます。たとえば、手動変更をしても良い認識結果が得られなかった場合、このオプションを選択することができます。

1. **認識設定**タブで、**自動設定**をクリックします。

   新しいダイアログボックスが表示されます。

2. **次へ**をクリックして、自動設定された設定に戻すことを確認します。

   システムにより、設定が最適化されます。

3. **閉じる**をクリックします。
4. プロンプトが表示されたら、設定の保存を確定します。
5. 新しい設定を確認し、検証 『197ページ の"設定の確認"参照 』します。

ナンバープレートマッチリストの操作

ナンバープレートマッチリストについて

ナンバープレートリストとは、LPR ソリューションに特別な方法で処理させたいナンバープレートの集合のリストです。ナンバープレートの認識では、これらのリストを比較し、一致があったときにシステムが LPR イベントをトリガします。イベントはイベントサーバーに保存されます。また、XProtect Smart Client の **LPR** タブで検索および確認できます。

デフォルトでは、イベントは 24 時間のみ保存されます。これを変更するには、Management Application で**オプション**ダイアログボックスを開き、**イベントサーバー設定**タブの**次のｲﾍﾞﾝﾄを保持**フィールドに新しい時間枠を入力します。

ナンバープレートマッチリストを指定すると、一致した際にトリガされる追加のイベントやアラームを設定できます。

例：

- ある会社の本社では、役員の車両のナンバープレートのリストを使用して、別個の駐車場へのアクセス権限を付与しています。役員のナンバープレートが認識されると、LPR ソリューションは駐車場のゲートを開く出力信号をトリガします。

- ガソリンスタンドのチェーンでは、以前にガソリン代金を支払わずに逃げた車両のナンバープレートのリストを作成しています。このようなナンバープレートが認識されると、LPR ソリューションで出力信号がトリガされます。これによりアラームが有効になり、一時的に特定のガソリンポンプへのガソリンの供給がブロックされます。

また、トリガされたイベントを使用して、カメラの録画の画質を高品質にすることもできます。さらに、あるイベントを使用して、このようなアクションの組み合わせをトリガすることもできます。

記載されていないナンバープレートのリストについて

通常はリストに含まれているナンバープレートが認識されるとイベントをトリガしますが、リストに含まれて**いない**ナンバープレートが認識された場合にイベントをトリガすることも可能です。

例： ある私有駐車場では、ナンバープレートのリストを使用して、住民に駐車場へのアクセスを許可しています。リストに載っていないナンバープレートの車両が駐車場に接近すると、LPR ソリューションで出力信号がトリガされ、セキュリティオフィスで一時的なゲストとしてのパスを得るようにドライバーに説明するサインを点灯させます。

リストに**ない**ナンバープレートを認識したときに、監視システムのイベントをトリガするには、**記載されていないナンバープレート**リストを使用します。他のリスト 『195ページ の"マッチリストタブ"参照 』などのカメラを選択し、他のリスト 『202ページ の"LPR によってトリガされるイベント"参照 』のように設定します。

ナンバープレートマッチリストの新規追加

1. Management Application のナビゲーションペインで、**ナンバープレートマッチリスト**を選択し、右クリックして、**新規追加**を選択します。
2. 表示されるウィンドウで、リストに名前を付けて、**OK** をクリックします。

   ナンバープレートのリストを作成すると、すぐに**ナンバープレートマッチリスト**、およびすべての LPR カメラの**マッチリスト**タブで表示されます。
3. マッチリストに列を追加する場合は、**カスタムフィールド**をクリックして、表示されるダイアログボックス 『201ページ の"カスタムフィールドのプロパティの編集"参照 』で列を指定します。
4. マッチリストを更新するには、**追加**、**編集**、**削除** ボタン 『199ページ の"ナンバープレートマッチリストを編集"参照 』を使用します。
5. Management Application でマッチリストを直接定義する代わりに、ファイルをインポート 『200ページ の"ナンバープレートマッチリストのインポート/エクスポート"参照 』することもできます。
6. プロンプトが表示されたら、変更の保存を確定します。

ナンバープレートマッチリストを編集

1. Management Application のナビゲーションペインで、**ナンバープレートマッチリスト**を選択します。
2. 関連するリストをクリックします。
3. **ナンバープレートマッチリスト情報**ウィンドウが開きます。
4. 新しい列をリストに追加するには、**追加**をクリックして、フィールドに記入します。
   - 空白は含めないでください。
   - 必ず大文字を使用してください。

     例： *ABC123*（正しい例）、*ABC 123*（正しくない例）、*abc123* （正しくない例）

- ナンバープレートマッチリストでは、ワイルドカードも使えます。ワイルドカードは、特定の位置に任意の数の「?」と文字および数字が現れるように定義することができます。

  例： *?????A*、*A?????*、*???1??*、*22??33*、*A?B?C?* など。

5. プロンプトが表示されたら、変更の保存を確定します。

ナンバープレートマッチリストのインポート/エクスポート

ナンバープレートマッチリストで使いたいナンバープレートのリストが含まれているファイルをインポートすることができます。インポートには、以下のオプションがあります。

- ナンバープレートを既存のリストに追加します。
- 既存のリストを置換します。

たとえば、リストを中央で集中管理している場合には、これが便利です。次に、ファイルを配信することで、すべてのローカルインストールを更新することができます。

同様に、ナンバープレートの完全なリストを、マッチリストから外部の場所へエクスポートすることもできます。

サポートされているファイル形式は.txt または.csv です。

インポートするには：

1. Management Application のナビゲーションペインで、**ナンバープレートマッチリスト**をクリックし、関連するリストを選択します。
2. ファイルをインポートするには、**インポート**をクリックします。
3. ダイアログボックスで、インポートファイルの場所およびインポートのタイプを指定します。**次へ**をクリックします。
4. 確認を待ってから、**閉じる**をクリックします。

エクスポートするには：

1. ファイルをエクスポートするには、**エクスポート**をクリックします。
2. ダイアログボックスで、エクスポートファイルの場所を指定して、**次へ**をクリックします。
3. **閉じる**をクリックします。
4. エクスポートしたファイルは、たとえば、Microsoft Excel で開いて、編集することができます。

ナンバープレートマッチリストのプロパティ

名前	詳細
名前	リストの名前を表示します。必要に応じて、この名前を変更できます。
カスタムフィールド	クリックして、ユーザーが追加情報を追加できるナンバープレートの入力列を指定します。カスタムフィールド（プロパティ） 『201ページ の"カスタムフィールドのプロパティの編集"参照 』を参照してください。
検索	特定のナンバープレート、ナンバー、パターンなどのリストを検索します。必要に応じて、?を単一のワイルドカードとして使えます。

名前	詳細
追加	クリックして、ナンバープレートを追加します。 • 空白は含めないでください。 • 必ず大文字を使用してください。 **例：** *ABC123*（正しい例）、*ABC 123*（正しくない例）、*abc123* （正しくない例） • ナンバープレートのリストでは、ワイルドカードも使えます。ワイルドカードは、特定の位置に任意の数の「?」と文字および数字が現れるように定義することができます。 **例：** *?????A*、*A?????*、*???1??*、*22??33*、*A?B?C?* など。 一部の地域では、このような規則に当てはまらない例もあります。たとえば、空白文字でカスタマイズしたプレートなど。アンダーライン(_)によって区切られ、必ず別個に認識される必要がある文字のセットを 2 つ含んでいるプレート。あるいは、ナンバープレートのパーツで、背景の色が異なる特定の地域のプレート。 **例：** 
編集	クリックして、ナンバープレートを編集します。複数の行を選択して、編集することができます。
削除	クリックして、選択したナンバープレートを削除します。
インポート	クリックして、たとえば.txt ファイルや.csv ファイル 『200ページ の"ナンバープレートマッチリストのインポート/エクスポート"参照 』などのカンマ区切りファイルからナンバープレートをインポートすることができます。
エクスポート	クリックして、たとえば.txt ファイルや.csv ファイル 『200ページ の"ナンバープレートマッチリストのインポート/エクスポート"参照 』などのカンマ区切りファイルに全ナンバープレートをエクスポートすることができます。
ページ当たりの行	1 ページ（1 画面）に表示するナンバープレートの数を選択します。50～1000 行の範囲で選択できます。
リストの一致によってトリガされたイベント	リストの一致によって、どのイベントをトリガするかを選択します 『202ページ の"LPR によってトリガされるイベント"参照 』。システムで定義されているすべての使用可能なイベントのタイプを選べます。

カスタムフィールドのプロパティの編集

ナンバープレートマッチリストに追加情報の列を追加することができます。列の名前や番号、ならびにフィールドの内容を指定します。

XProtect Smart Client のユーザーは、列の情報を更新することはできますが、列自体を変更することはできません。

名前	詳細
追加	列をマッチリストに追加します。列の名前を入力します。
編集	クリックして、列の名前を編集します。
削除	列を削除します。
アップ	列の順番を変更します。
ダウン	列の順番を変更します。

LPR によってトリガされるイベント

ナンバープレートマッチリストを作成 『199ページ の"ナンバープレートマッチリストの新規追加"参照 』したら、システムで定義されているすべてのイベントのタイプを関連付けることができます。

使用可能なイベントのタイプは、システムの設定によります。LPR との接続で、たとえば駐車場のバリアを上げる、カメラの録画の画質を高品質にする、などの出力信号をトリガするためにイベントを使用できます。また、イベントを使用して、このようなアクションの組み合わせをトリガすることもできます。他の例は、ナンバープレートマッチリストについて 『198ページ 』を参照してください。

リストの一致によってトリガされるシステムイベントの設定

1. **サーバー**を展開し、**ナンバープレートマッチリスト**をクリックして、イベントに関連付けたいリストを選択します。
2. **ナンバープレートマッチリスト情報**ウィンドウで、**リストの一致によってトリガされたイベント**選択フィールドの横にある**選択**をクリックします。
3. **トリガされたイベントを選択**ダイアログボックスで、1 つ以上のイベントを選択します。
4. プロンプトが表示されたら、変更の保存を確定します。
5. これで、イベントが選択したナンバープレートマッチリストの認識に関連付けられます。

リストに**ない**ナンバープレートを認識したときに、監視システムのイベントをトリガするには、**記載されていないナンバープレート**リストを設定します。

LPR によってトリガされるアラーム

一部のタイプのアラームは、XProtect LPR のイベントに関連付けることができます。次の手順を実行します。

1. ナンバープレートの一致を確認したいナンバープレートマッチリストを作成 『199ページ の"ナンバープレートマッチリストの新規追加"参照 』します。
2. LPR カメラを追加および設定 『190ページ の"LPR カメラの追加"参照 』します。
3. Management Application のナビゲーションペインで、**アラーム**を展開し、**アラームの定義**を右クリックして、新しいアラームの作成を選択します。
4. **アラーム定義情報**ウィンドウが表示されます。関連するプロパティ 『203ページ の"LPR のアラーム定義"参照 』を選択します。

5. 完了後にプロンプトが表示されたら、変更の保存を確定します。
6. LPR のアラームデータを設定します 『203ページ の"LPR のアラームデータ設定"参照 』。

LPR のアラーム定義

イベントのトリガの定義以外の**アラーム定義**の設定は、システムの残りの部分について LPR と同様になります。

LPR に関連するトリガイベントを定義するには、アラームがトリガされた時に使用するイベントメッセージを選択します。

a) **イベントのトリガ**フィールドの一番上にあるドロップダウンリストで、どのタイプのイベントをアラームで使用するかを決定します。このリストは、**ナンバープレートマッチリスト**および **LPR サーバー** イベント 『198ページ の"ナンバープレートマッチリストの操作"参照 』を提供します。

b) 2 番目のドロップダウンリストで、使用するイベントメッセージを選択します。上のドロップダウンリストで**ナンバープレートマッチリスト**を選択したら、次にナンバープレートのリストを選択します。**LPR サーバー**を選択したら、関連する LPR サーバーのイベントメッセージを以下から選択します。

- LPR カメラの接続が失われています
- LPR カメラが実行中
- LPR サーバーが応答していません
- LPR サーバーは応答しています

残りのアラーム定義の設定の詳細については、**アラーム**のセクションを参照してください。

LPR のアラームデータ設定

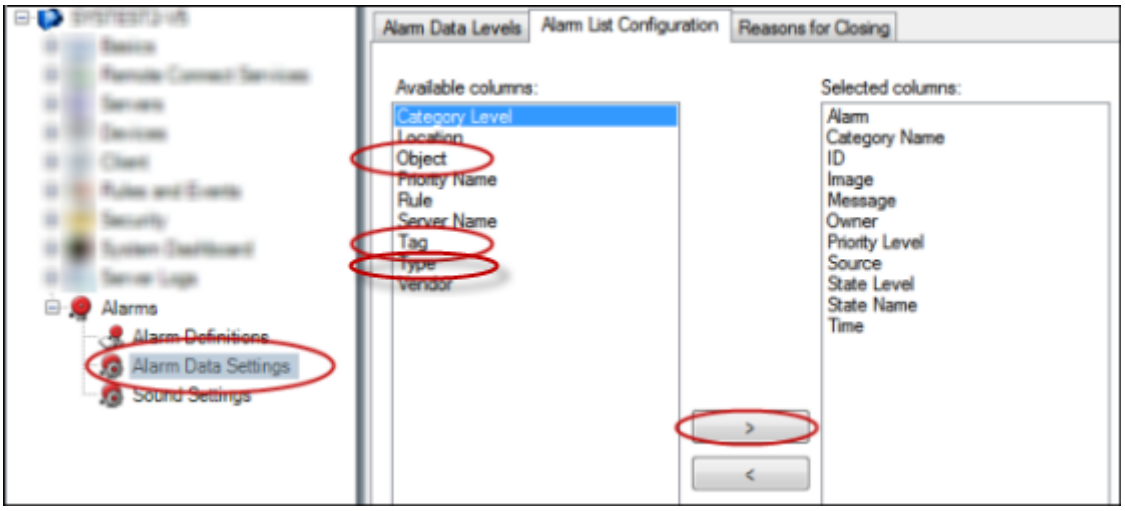
Management Application で、2 つの**アラームリスト設定**要素を XProtect Smart Client で選択可能にする必要があります。

この 2 つの要素は、XProtect Smart Client の**アラームマネージャ**でのアラームリストの設定で使用します。関連する要素は**オブジェクト**、**タグ**、**タイプ**であり、 ナンバープレート番号（オブジェクト）や国コード（タグ）の認識で必須になります。

Management Application で、以下を実行します。

1. Management Application のナビゲーションペインで、**アラーム**を展開し、**アラームデータ設定**を選択します。

2. **アラームリスト設定**タブで、**オブジェクト**、**タグ**、**タイプ**を選択し、**>**をクリックします。



3. プロンプトが表示されたら、変更の保存を確定します。

LPR のメンテナンス

LPR Server Manager について

LPR サーバーをインストールすると、XProtect LPR Server Manager で、サービスの状態をチェックすることができます。たとえば、LPR Server サービスの起動や停止、ステータスメッセージの表示、ログファイルの確認などです。

- LPR サーバーの状態の情報にアクセスするには、LPR サーバーを実行しているコンピュータの通知エリアにある **LPR Server Manager** アイコンをクリックします。

例：通知エリアにある
LPR Server Manager アイコン。

Management Application で、すべての LPR サーバーの完全なステータス概要 『187ページ の"LPR サーバー情報の表示"参照 』を把握することができます。

LPR Server サービスの起動と停止

LPR Server サービスは、インストール後、自動的に起動します。サービスを手動で停止した場合は、手動で再起動する必要があります。

1. 通知エリアで、**LPR Server Manager** アイコンを右クリックします。
2. 表示されるメニューから、**LPR Server サービスの開始**を選択します。
3. 必要であれば、**LPR Server サービスの停止**を選択して、サービスを再度停止します。

LPR サーバーのステータスの表示

1. LPR サーバーの通知エリアで **LPR Server Manager** アイコンを右クリックします。

2. 表示されるメニューから、**LPR サーバーのステータスの表示**を選択します。

   システムが問題なく動作している場合、ステータスは次のようになります。*すべての LPR カメラが実行中です。*

   他のステータス：

   - *サービスが応答しません*
   - *監視システムに接続していません*
   - *サービスは実行されていません*
   - *イベントサーバーが接続されていません*
   - *不明なエラー*
   - *X / Y 台の LPR カメラが実行中です*

LPR Server ログの表示

LPR Server サービスのステータスのモニタリングやトラブルシューティングを行う上で、ログファイルは便利なツールです。すべてのエントリーには時刻が記録されており、最も最近のエントリーが下になります。

1. 通知エリアで、**LPR Server Manager** アイコンを右クリックします。
2. 表示されるメニューから、**LPR Server のログフィルを表示**を選択します。

   ログビューワに、サーバーの活動がタイムスタンプ付きで一覧表示されます。

LPR サーバー設定の変更

LPR サーバーは、管理サーバーと通信できることが必要になります。これを有効にするには、LPR サーバーのインストール時に、管理サーバーの IP アドレス/ホスト名を指定します。

管理サーバーのアドレスを変更したい場合、以下の方法で行います。

1. LPR Server サービスを停止します。
2. 通知エリアで、 **LPR Server Manager** アイコンを右クリックします。
3. 表示されるメニューから**設定の変更**を選択します。**LPR Server サービスの設定**ウィンドウが表示されます。
4. 新しい値を指定して、**OK** をクリックします。
5. LPR Server サービスを再起動します。

XProtect LPR のアンインストール

システムから XProtect LPR を削除したい場合は、通常の Windows の削除の手順で、2 つのコンポーネントを個別にアンインストールします。

- LPR プラグインがインストールされているコンピュータでは、*MilestoneXProtectLPR[バージョン]プラグインをアンインストールします。*
- LPR サーバーがインストールされているコンピュータでは、*MilestoneXProtectLPR[バージョン]サーバーをアンインストールします。*

Milestone Mobile

Milestone Mobile の概要

Milestone Mobile について

Milestone Mobile には次の 3 つのコンポーネントがあります。

- **Milestone Mobile クライアント**
- **Milestone Mobile サーバー**
- **Milestone Mobile プラグイン**

Milestone Mobile クライアントはモバイル監視アプリであり、Android デバイス、Apple デバイス、または Windows Phone デバイスにインストールして使用できます。任意の数の Milestone Mobile クライアントのインストールを使用できます。

※本機は、Windows Phone デバイスには対応していません。

詳細については、Milestone Systems Web サイト『http://www.milestonesys.com/support/manuals-and-guides/』から Milestone Mobile クライアントユーザーガイドをダウンロードしてください。

Milestone Mobile サーバーと Milestone Mobile プラグインについては、このマニュアルで説明します。

Milestone Mobile を使用するための前提条件

Milestone Mobile の使用を開始する前に、次の項目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。
- Android、iOS、または Windows を実行し、Google Play、App Store℠、Windows Phone Store にアクセスして Milestone Mobile クライアントアプリケーションをダウンロードできるモバイルデバイス。

Milestone Mobile システム要件

各種コンポーネントの**最低**システム要件については、Milestone Web サイト『http://www.milestonesys.com/SystemRequirements』をご覧ください。

- Milestone Mobile クライアントの要件については、**Milestone Mobile** エントリをクリックしてください。
- Milestone Mobile サーバーの要件については、インストールした XProtect 製品をクリックしてください。
- Milestone Mobile プラグインの要件:
  - 実行中の Management Application。
  - Milestone プラグインがインストールされ、VMS と統合します。

Milestone Mobile 構成

Milestone Mobile サーバーについて

Milestone Mobile サーバーによって、モバイルデバイスや XProtect Web Client の Milestone Mobile クライアントからシステムへのログインが処理されます。

Milestone Mobile サーバーはレコーディングサーバーから Milestone Mobile クライアントに動画ストリームを配信します。これにより、レコーディングサーバーはインターネットに接続しないため、安全性の高い環境を提供できます。Milestone 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。

レコーディングサーバーへアクセスするためのコンピュータに、Milestone Mobile サーバーをインストールする必要があります。Milestone Mobile サーバーをインストールするときには、管理者権限があるアカウントを使用してログインしてください。そうでない場合、インストールは正常に完了しません。

Milestone Federated Architecture およびマスター/スレーブサーバーについて

※本機は、Milestone Federated Architecture には対応していません。

システムがマスター/スレーブ設定で Milestone Federated Architecture をサポートする場合は、Milestone Mobile クライアント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。Milestone Mobile サーバーは中央サイトにのみインストールします。

つまり、Milestone Mobile クライアント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ります。Milestone Mobile クライアント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管理者権限が必要です。

Mobile サーバーの追加または編集

1. **サーバー > モバイルサーバー**に移動します。表示されるメニューから**新規作成**を選択します。設定を入力または編集します。

重要： 自分または他のユーザーが Milestone Mobile クライアントに接続中に、**ログイン方法**、**すべてのカメラを表示**、**出力とイベント**の設定を編集する場合、新しい設定を有効にするには、Milestone Mobile クライアントを再起動する必要があります。

Smart Connect について

※本機は、Smart Connect には対応していません。

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、モバイル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。

この機能では、Milestone 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 Application 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、Mobile Server サーバーはインターネットからアクセスできます。

Smart Connect は Milestone 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、どこからでもモバイルサーバーに接続できるようにします。

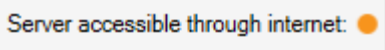
顧客のモバイルクライアントの設定を簡単にするために、Management Application 内からエンドユーザーに直接 E メールを送れます。E メールにはサーバーを直接 Milestone Mobile に追加するリンクが含まれています。これでネットワークアドレスやポートを入力する必要なしに設定が完了します。

Smart Connect の設定

ルーターで Universal Plug and Play (UPnP)検出を有効にする

モバイルデバイスを Milestone 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)を有効にできます。UPnP により、Milestone 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い場合は、そのデバイスのマニュアルを参照してください。

注意：5 分ごとに、Milestone Mobile サーバーサービスは、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。ステータスは、**[プロパティ]**ペインの左上端に表示されます。



要件

- Milestone Mobile サーバーは公開 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にできますが、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。
- Smart Connect の有効なライセンスが必要です。

接続設定の構成

1. Management Application で、ナビゲーションペインで、**[サーバー]**を展開し、**Mobile Server** を選択します。 1
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、次の項目を指定します。
   - 簡単にモバイルデバイスを Milestone Mobile サーバーに接続できるようにするには、**[Smart Connect を有効にする]**チェックボックスを選択します。
   - **[接続タイプ]**フィールドで使用するプロトコルを指定します。
   - **注意：**安全な接続をオンにする場合は、iOS 9.0 および以降または Windows Phone を実行するデバイスは、Milestone Mobile サーバーにインストールされた認証局(CA)が発行した証明書がある場合にのみ接続できます。CA は、インターネットでデータを交換するユーザーと Web サイトの身元を検証するデジタル証明書を発行します。CA の例は、Comodo、Symantec、GoDaddy などの企業です。
   - 安全な接続をオンにする前に、デジタル証明書の知識があることを確認してください。Milestone Mobile サーバーで証明書を追加する方法については、「証明書の編集 『223ページ 』」を参照してください。
   - 接続がタイムアウトする前に、秒数を指定します。
   - モバイルデバイスが範囲内の Milestone Mobile サーバーを検出できるようにするには、**[UPnP 検出を有効にする]**チェックボックスを選択します。

- ルーターがモバイルデバイスを特定のポートに転送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送信してユーザーの接続をサポートする

ユーザーが Milestone Mobile を簡単に開始できるようにするには、接続情報が記載された電子メールメッセージを送信します。Management Application から直接メッセージを送信するか、使用するメッセージングプログラムに情報をコピーできます。

1. **[招待を電子メールで送信する]**フィールドに、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。 複雑なネットワークで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**グループで、次の項目を指定します。

- UPnP ポートマッピングをしようして、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。次に、**[IP アドレスまたはホスト名]**と、接続で使用するポートを入力します。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は、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。

通知の送信について

Milestone Mobile を有効にして、アラームトリガー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。システム通知は、アプリが実行中であるかどうかに関係なく、常に配信されます。Milestone 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、アプリが実行中ではないときでも配信されます。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の場合があります。

また、プッシュ通知を使用すると、Milestone 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、移動中のユーザーが最新情報を常に得られるようにするための優れた方法です。

プッシュ通知の使用

※本機は、プッシュ通知には対応していません。

注意：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。

モバイルデバイスへの通知の送信を設定します

Milestone Mobile を有効にして、アラームトリガー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。

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 Milestone Care™契約が最新であることを確認します。
- システムはインターネットへのアクセスを必要とします。

システム通知の設定

サーバーがオフラインになった場合など、システム関連の通知を送信するには、次の手順を実行します。

1. Management Application では、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. **[通知]**チェックボックスを選択します。

Milestone Mobile サーバーでプッシュ通知を設定する

プッシュ通知を設定するには、次の手順に従います。

1. Management Application では、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。

   注意 : 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停止する

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 Application では、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、Milestone 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

調査を設定し、Web Client と Milestone Mobile を使用して、録画されたビデオにアクセスし、インシデントを調査し、証拠ビデオを準備およびダウンロードできるようにします。

調査を設定するには、次の手順に従います。

1. Management Application 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. **有効**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す。
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. **調査フォルダのサイズを制限する**フィールドで、調査フォルダが含むことができる最大メガバイト数を入力します。
5. 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、**他のユーザーの調査を表示する**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。
6. 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。
7. **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に使用する圧縮形式を選択します。

   注: 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 Application 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。
8. **エクスポートが失敗したときにデータを保持または削除する（MKV および AVI）**フィールドで、正常にダウンロードされ、不完全な可能性があるデータを保持するか、削除するかどうかを指定します。
9. 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、調査用に作成されたすべてのビデオエクスポートを削除するには、リストの調査を選択し、**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**データベース**、**AVI**、または **MKV** フィールドの右にある**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動画のストリーミングについて

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。

ビデオプッシュを使用した動画のストリーミングの設定

ユーザーがモバイルデバイスから XProtect システムに動画をストリーミングできるようにするには、Milestone Mobile サーバーでビデオプッシュを設定します。

要件

- 各チャンネルにはハードウェアデバイスライセンスが必要です。

Management Application で、次の順序で手順を実行します。

1. モバイルデバイスが動画をレコーディングサーバーにストリーミングするために使用できるチャンネルを設定します。
2. 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レコーティングサーバーに追加します。このドライバーはカメラデバイスをシミュレートし、動画をレコーディングサーバーにストリーミングできるようにします。
3. ビデオプッシュドライバーデバイスをチャンネルに割り当てます。

このトピックでは、これらの手順をそれぞれ説明します。

動画ストリーミング用のチャンネルの設定

チャンネルを追加するには、次の手順に従います。

1. ナビゲーションペインで、**Mobile Server** を選択し、モバイルサーバーを選択します。
2. **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ます。
3. 右下にある**追加**をクリックして、ビデオプッシュチャンネルを**チャンネルマッピング**に追加します。
4. 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（**ロール**の下に追加）を入力します。このユーザーアカウントは、Milestone Mobile サーバーとレコーディングサーバーへのアクセスを許可される必要があります（**全体的なセキュリティ**タブ）。

   注意: ビデオプッシュを使用するには、ユーザー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 Milestone Mobile にログインする必要があります。

5. ポート番号を書き留めます。これは、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ビデオプッシュドライバーを追加するときに必要です。
6. **[OK]**をクリックして、[ビデオプッシュチャンネル]ダイアログボックスを閉じ、チャンネルを保存します。

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レコーティングサーバーに追加します

1. ナビゲーションペインで、**[レコーディングサーバー]**をクリックします。
2. 動画をストリーミングするサーバーを右クリックし、**[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. **[手動]**ハードウェア検知方法を選択して、**[次へ]**をクリックします。
4. 次のように、カメラの資格情報を入力します。
   - ユーザー名については、初期設定またはカメラで指定されたユーザー名を入力します。
   - パスワード：***Milestone*** を入力し、**[次へ]**をクリックします。

   注意：これらはユーザーではなくハードウェアの資格情報です。これらはチャンネルのユーザー名に関連していません。
5. ドライバのリストで、**[その他]**を展開し、**[ビデオプッシュドライバー]**チェックボックスを選択して、**[次へ]**をクリックします。

   注意：ビデオプッシュドライバーデバイスの MAC アドレスが生成されます。このアドレスを使用することをお勧めします。ビデオプッシュドライバーデバイスで問題が発生した場合にのみ変更してください。たとえば、新しいアドレスとポート番号を追加する必要がある場合です。
6. **[アドレス]**フィールドに、Milestone 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 アドレスを入力します。
7. **[ポート]**フィールドに、動画をストリーミングするために作成したチャンネルのポート番号を入力します。ポート番号は、チャンネルを作成したときに割り当てられます。
8. **[ハードウェアモデル]**列で、**[ビデオプッシュドライバー]**を選択し、**[次へ]**をクリックします。
9. 新しいハードウェアが検出されたら、**[次へ]**をクリックします。
10. **「ハードウエア名テンプレート」**欄で、ハードウエアのモデルとその IP アドレスを表示するか、またはモデルだけかを決めて下さい。
11. **[有効]**チェックボックスを選択し、関連するデバイスを有効にするかどうかを指定します。有効ではない場合でも、**ビデオプッシュドライバー**のリストに関連するデバイスを追加できます。後から有効にできます。

    注意：動画をストリーミングするときに位置情報を使用する場合は、**メタデータ**ポートを有効にする必要があります。
12. 左側で関連するデバイスのデフォルト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ます。デバイスをグループに追加すると、同時にすべてのデバイスに設定を適用したり、デバイスの交換がより簡単になります。

ビデオプッシュドライバーデバイスをビデオプッシュ用のチャンネルに追加する

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. **[カメラの検索]**をクリックします。成功した場合、ビデオプッシュドライバーカメラの名前が**[カメラ名]**フィールドに表示されます。

3. 設定を保存します。

必要がないチャンネルの削除

使用しなくなったチャンネルは削除できます。

- 削除するチャンネルを選択し、右下端で**[削除]**をクリックします。

アクションについて

[一般]タブでこれを有効または無効にすると、Milestone Mobile クライアントの**[アクション]**タブを使用できるかどうかを管理できます。[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。

Milestone Mobile で使用する出力の名前について

アクションを現在のカメラとともに正しく表示するには、出力がカメラと正確に同じ名前を使用することが重要です。

例：

「AXIS P3301,P3304 - 10.100.50.110 - Camera 1」という名前のカメラがある場合は、アクションの名前も「AXIS P3301,P3304 - 10.100.50.110 - Camera 1」にする必要があります。

「AXIS P3301,P3304 - 10.100.50.110 - Camera 1 - Light switch」のような詳細説明を後からタイトルに追加することができます。

重要：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。

Mobile サーバーの設定

一般

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	Milestone Mobile サーバーの名前を入力します。
説明	オプションで、Milestone Mobile サーバーの説明を入力します。
Mobile サーバー	特定のシステムに現在インストールされているすべての Milestone Mobile サーバーから選択します。リストには、実行中の Milestone Mobile サーバーだけが表示されます。
ログイン方法	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。次のいずれかを選択できます。 • **自動** • **Windows 認証** • **基本認証**

機能

名前	説明
有効 XProtect Web Client	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無効になっています。
すべてのカメラビューを有効化	**すべてのカメラ**ビューを含めます。このビューには、ユーザーがレコーディングサーバーで表示できるすべてのカメラが表示されます。この機能はデフォルトでは無効になっています。
アクションを有効化（出力およびイベント）	Milestone Mobile クライアント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無効になっています。
キーフレームを有効化	モバイルデバイスと XProtect Web Client で動画をストリーミングするときにキーフレームのみをストリーミングします。これにより、帯域幅の使用が少なくなります。
Milestone Mobile サーバーへの定義済み管理者ロールアクセスを拒否する	これを有効にすると、定義済みの管理者ロールに割り当てられたユーザーはモバイルデバイスと XProtect Web Client で動画にアクセスできません。

ログ設定

名前	説明
有効	Milestone Mobile クライアントのアクションの別個のログファイルでの記録を有効/無効にします。 ログファイルの記録が不要な場合はチェックを外してください。チェックされている場合は、”ログファイルの場所”に適切なフォルダ(C:¥Log¥MS)を指定する必要があります。
ログファイルの場所	ログファイルを保存する場所を指定します。
ログの保持期間	ログを保持する日数を指定します(デフォルトは 3 日です)。

構成バックアップ

名前	説明
インポート	新しい Milestone Mobile サーバー構成の XML ファイルをインポートします。
エクスポート	Milestone Mobile サーバーの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

[接続]タブの設定は次のタスクで使用されます。

- 接続設定を構成します。

- 電子メールメッセージを送信し、ユーザーがモバイルデバイスを Milestone Mobile サーバーに接続できるようにします。
- 複雑なネットワークで Milestone Mobile サーバーへの接続を有効にします。

これらのタスクの段階的な説明については、「Smart Connect の設定 『208ページ 』」を参照してください。

一般

名前	説明
接続タイプ	クライアントが Milestone Mobile サーバーに接続する方法を選択します。以下のオプションから選択できます。**HTTP のみ**、**HTTP および HTTPS**、または **HTTPS のみ**。 **注意：[HTTPS のみ]**を選択する場合は、iOS 9.0 または Windows Phone を実行するデバイスは、Milestone Mobile サーバーにインストールされた認証局(CA)が発行した証明書がある場合にのみ接続できます。CA は、インターネットでデータを交換するユーザーと Web サイトの身元を検証するデジタル証明書を発行します。CA の例は、Comodo、Symantec、GoDaddy などの企業です。安全な接続をオンにする前に、デジタル証明書の知識があることを確認してください。Milestone Mobile サーバーで証明書を追加する方法については、「証明書の編集 『223ページ 』」を参照してください。
クライアントタイムアウト(HTTP)	※本機は、クライアントタイムアウト(HTTP)には対応していません。変更しないでください。 モバイルサーバーが実行中であることを、Milestone Mobile クライアントで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。

インターネットアクセス

名前	説明
カスタムインターネットアクセスの構成	UPnP ポートマッピングをしようして、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。 次に、**IP アドレス**または**ホスト名**と、接続で使用するポートを入力します。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は、これを実行できます。
選択すると IP アドレスを動的に取得します	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。
自動検出されたアドレス	システムで検出されたこの Mobile Server の IP アドレスを一覧表示します。

Smart Connect 通知

名前	説明
招待を電子メールで送信します	Smart Connect 通知の受信者の電子メールアドレスを入力します。

名前	説明
電子メール言語	電子メールの言語を指定します。
Smart Connect トークン	モバイルデバイスのユーザーが Mobile Server サーバーに接続するために使用できる一意の ID。
Smart Connect へのリンク	モバイルデバイスのユーザーが Mobile Server サーバーに接続するために使用できるリンク。

サーバーステータス

モバイルサーバーのステータス詳細を表示します。詳細は読み取り専用です：

名前	説明
サーバー有効化日	前回の停止後、モバイルサーバーが動作し続けている期間を示します。
CPU 使用	モバイルサーバーでの現在の CPU 使用状況を示します。
外部帯域幅	モバイルデバイスとモバイルサーバーの間で使用されている現在の帯域幅を示します。

アクティブなユーザー

モバイルサーバーに接続されたモバイルデバイスのステータス詳細を表示します。

名前	説明
ユーザー名	モバイルサーバーに接続されている各モバイルクライアントユーザーのユーザー名を表示します。
状態	モバイルサーバーと、対象となる Mobile Server クライアントの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： • **接続済み:**鍵と暗号化資格情報を交換するサーバーへの準備状態。 • **ログイン:**モバイルクライアントユーザーは、XProtect システムにログインしています。
帯域幅使用状況(kB/秒)	対象となるモバイルサーバーのクライアントユーザーによる帯域幅の使用状況を表示します。
トランスコードされたストリーム	各モバイルクライアントユーザーに対して現在開かれている変換されたビデオストリームの数が表示されます。

パフォーマンス

パフォーマンスタブで、Milestone Mobile サーバーのパフォーマンスに関して以下の制限を設定します：

設定

名前	説明
フルサイズの画像を有効にする	Milestone Mobile サーバーが、フルサイズの画像を Milestone Mobile クライアントまたは XProtect Web Client に送信することを有効にします。 フルサイズの画像を有効にすると、帯域幅の使用が増えます。また、このオプションを有効にすると、**[動画ストリーム制限のレベル]**設定のすべてのルールが無効になります。
再生ストリームを制限する	関連するモバイルクライアントユーザーに対して現在開かれている再生ビデオストリームの最大数を有効にして指定します。

ビデオストリーム制限のレベル

レベル 1

レベル 1 は、Milestone Mobile サーバーにデフォルトで設定される制限です。上記のフルサイズ画像の送信を有効にしていない場合、ここで設定するすべての制限は、必ず Milestone Mobile の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、Milestone 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	Milestone 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	Milestone 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、Milestone 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、Milestone 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、Milestone Mobile サーバーの帯域負荷について閾値を設定します。

名前	説明
最大 FPS	Milestone 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	Milestone 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、Milestone Mobile サーバーのパフォーマンスに第 3 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、Milestone 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、Milestone 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	Milestone 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	Milestone 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。

全般タブで**フルサイズの画像を有効にする**を有効にすると、どの**パフォーマンス**レベルも適用されなくなります。

調査

調査設定

調査を設定し、XProtect Web Client と Milestone Mobile を使用して、録画されたビデオにアクセスし、インシデントを調査し、証拠ビデオを準備およびダウンロードできるようにします。

名前	説明
調査フォルダ	調査用のビデオが保存される場所
調査フォルダのサイズを制限します	調査フォルダが含むことができる最大メガバイト数を入力します。既定のサイズは 2000 MB です。
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。
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。

名前	説明
AVI エクスポートで使用されたコーデック	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。 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バイアは、Milestone Mobile が実行され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。
エクスポートが失敗したときにデータを保持または削除する(MKV および AVI)	調査でダウンロード用に正常に準備されていないデータを保持するか、削除するかを選択します。

調査

名前	説明
調査	これまでシステムで設定された調査を一覧表示します。調査を保持しない場合は、**[削除]**または**[すべて削除]**ボタンを使用します。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。
詳細	調査用にエクスポートされたビデオファイルを個別に削除、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**データベース**、**AVI**、**MKV** フィールドの右にある削除アイコンをクリックします。

ビデオプッシュ

ビデオプッシュを有効にする場合、以下の設定を指定できます。

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を表示します。
チャネル	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。

必要なステップすべて 『212ページ の"ビデオプッシュを使用した動画のストリーミングの設定"参照 』が完了したら、**カメラの検索**をクリックして、関連するカメラを検索します。

通知

[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は、Milestone Mobile はイベントが発生したときに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 Milestone Mobile で通知が配信されます。プッシュ通知は Milestone 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、「モバイルデバイスへの通知の送信の設定 『210ページ の"モバイルデバイスへの通知の送信を設定します"参照 』」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。

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ます。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、デバイスに通知を送信します。
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通知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	通知を受信するユーザーの名前。

Mobile Server Manager

Mobile Server Manager について

Mobile Server Manager は、Mobile サーバーに接続されるトレイコントロール機能です。システムトレイで Mobile Server Manager のアイコンを右クリックすると、Mobile サーバーの機能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。

- XProtect Web Client を開く 『21ページ の"XProtect Web Client へのアクセス"参照 』
- Mobile サービスの起動、停止、再起動 『225ページ 』
- 監視サーバーの資格情報の入力または変更 『224ページ の"監視サーバーの資格情報の入力/編集"参照 』
- ポート番号の表示/編集 『225ページ 』
- 証明書の編集 『223ページ 』

- 今日のログファイルを開く 『223ページ の"ログへのアクセスおよび調査について"参照 』
- ログフォルダを開く 『223ページ の"ログへのアクセスおよび調査について"参照 』
- 調査フォルダを開く 『223ページ の"ログへのアクセスおよび調査について"参照 』
- Mobile サーバーのステータスを表示 『222ページ の"ステータスの表示について"参照 』

XProtect Web Client へのアクセス

※本機は、XProtect Web Client には対応していません。

Milestone 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、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、Milestone 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その他のすべてのコンピュータからアクセスできます。

1. Management Application で Milestone Mobile サーバーを設定します。
2. Milestone 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、システムトレイの Milestone Mobile サーバーアイコンを右クリックし、**[XProtect Web Client を開く]**を選択します。
3. Milestone 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 Explorer、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、Milestone 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：Milestone 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）。

   ブラウザのアドレスバーに、標準 HTTP 接続を使用するか、安全な HTTPS 接続を使用するかによって、http://1.2.3.4:8081 または https://1.2.3.4:8082 と入力します。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。Milestone 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、この操作をリモートで強制的に実行する必要があります（この操作を実行できるのは、ドメインでの Internet Explorer だけです）。

ステータスの表示について

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、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	詳細
サーバー実行日	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 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	Mobile サーバーでハードウェアの高速デコードが実行中かどうかを示します。
CPU 使用	現在 Mobile サーバーが使用している CPU の%。
CPU 使用履歴	Mobile サーバーによる CPU 使用の履歴を詳しく示すグラフ。

ログへのアクセスおよび調査について

Mobile Server Manager により、その日のログファイルに迅速にアクセスし、ログファイルが保存されているフォルダを開き、調査が保存されている先のフォルダ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 を右クリックし、**今日のログファイルを開く**、**ログフォルダを開く**、または**調査フォルダを開く**を選択します。

重要 : システムから Milestone 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。適切な権限がある管理者は、後でこれらのログファイルにアクセスすることや、必要でなくなった場合に削除を決定することができます。ログファイルのデフォルトでの場所は、**ProgramData** フォルダです。ログファイルのデフォルトでの場所を変更する場合、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。

証明書の編集

安全な HTTPS プロトコルを使用して、Milestone Mobile サーバーとモバイルデバイスや XProtectWeb Client との間の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。

- **単一のコンピュータ**へのインストールを実行する場合、Milestone Mobile サーバーは目立たないようにインストールを実行し、システムは証明書を作成しません。証明書を作成するには、以下の指示に従います。
- Milestone Mobile サーバーをインストールする場合、**標準**インストールを実行すると、自己署名証明書が生成されます。他の信頼できるサイトで発行された証明書に変更を加えることができます。以下をご覧ください。
- **カスタム**インストールを実行すると、自己署名証明書を生成するか、他の信頼済みサイトが発行した証明書が含まれているファイルをロードするかを、選択できます。

CA 証明書

CA（証明書管理者）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。

自己署名証明書

自己署名証明書は誰でも作成できます。これには CA からのルート証明書がないため、OS はこれをあまり安全でないと見なします。単純な攻撃に対する安全性は提供されますが、状況によっては接続の安全性は保証されていません。Milestone Mobile サーバーにより無料で作成されるという点では、自己署名証明書は便利です。

注 : 安全な接続 (HTTPS) や iOS 9.0 以降または Windows Phone を実行するデバイスを使用する場合は、Milestone Mobile サーバーにインストールされた認証局 (CA) が発行した証明書がある場合にのみ接続できます。CA は、インターネットでデータを交換するユーザーと Web サイトの身元を検証するデジタル証明書を発行します。CA の例は、Comodo、Symantec、GoDaddy などの企業です。安全な接続をオンにする前に、デジタル証明書の知識があることを確認してください。

証明書を作成または変更する場合、以下に従ってください。

1. Management Application がインストールされているコンピュータで、**Milestone Mobile サーバー**アイコンを右クリックし、**証明書の編集...**を選択します。
2. 以下のいずれか 1 つを選択します。
   - 自己署名証明書を生成する。
   - CA 証明書ファイルを読み込む。

自己署名証明書を生成

1. **自己署名証明書を生成**オプションを選んで、**OK** をクリックします。
2. システムが証明書をインストールする間、数秒待ちます。
3. 完了すると、ウィンドウが開いて、証明書が正常にインストールされたことが知らされます。

   Mobile Server サービスが再起動し、変更が適用されます。

CA 証明書ファイルを探す

1. **証明書ファイルを読み込む**オプションを選びます。
2. 証明書ファイルのパスを入力するか、**...**ボックスをクリックすると、ファイルを参照できるウィンドウが開きます。
3. 証明書ファイルのパスワードを入力します。
4. 完了したら、**OK** をクリックします。

   CA で発行されたものでない場合、Mobile クライアントのユーザーは証明書をもう一度承認するように指示されます。

監視サーバーの資格情報の入力/編集

1. Management Application がインストールされているコンピュータで、**Milestone Mobile サーバー**アイコンを右クリックし、**[監視サーバーの資格情報]**を選択します。
2. **サーバーの URL** を入力します。
3. 以下のどのユーザーでログインするかを選択します。
   - ローカルシステム管理者(資格情報は必要なし)、または
   - 指定されたユーザーアカウント(資格情報が必要)。
4. 指定されたユーザーアカウントを選択した場合、**ユーザー名**と**パスワード**を入力します。
5. 完了したら、**OK** をクリックします。

ポート番号の表示/編集

1. Management Application がインストールされているコンピュータで、**Milestone Mobile サーバー**アイコンを右クリックし、**[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. 完了したら、**OK** をクリックします。

Mobile サービスの起動、停止、再起動

必要に応じて Mobile 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、**Mobile Server Manager** を右クリックし、**Mobile サービスの起動**、**Mobile サービスの停止**、または **Mobile サービスの再起動**を選択します。

よくある質問(FAQ)

1. **Milestone Mobile クライアントからレコーディング/Milestone Mobile サーバーに接続できないのはなぜですか。**

   録画に接続するには、お使いの XProtect システムを実行しているサーバーか、専用サーバーに Milestone Mobile サーバーをインストールする必要があります。XProtect ビデオ管理設定で、関連する Milestone Mobile 設定も行う必要があります。これらは、プラグインまたは製品インストールまたはアップグレードの一部としてインストールされます。Milestone Mobile サーバーを取得する方法および Milestone Mobile クライアント関連設定を XProtect システムで統合する方法の詳細については、設定セクション『207ページ の"Milestone Mobile 構成"参照 』を参照してください。

2. **Milestone Mobile を XProtect Corporate サーバーにインストールしたのですが、自分のデバイスからサーバーに接続できません。何が問題ですか。**

   Milestone Mobile サーバーを XProtect Corporate (4.0 以上)にインストールした後、Milestone Mobile プラグインをインストールし、XProtect Corporate 設定で Milestone Mobile サーバーを表示する必要があります。Milestone Mobile プラグインをインストールした後、**[サーバー] > [モバイルサーバー]**の下でプラグインを見つけ、右クリックして新しいモバイルサーバーを追加します。ここでは、お使いの Milestone Mobile サーバーに関する詳細を追加します（サーバー名、説明（オプション）、サーバーアドレス、ポートなど）。完了したら、Milestone Mobile サービス(Windows Services)を再起動し、デバイスに再接続します。

3. **Milestone Mobile サーバー/ロケーション/サイトを Milestone Mobile クライアントに追加するにはどのようにするのですか。**

   Milestone Mobile クライアントからこの手順を実行できます。初めて開くときには、カメラからビデオを取得するために、1 つ以上のモバイルサーバーを追加する必要があります。追加した Milestone Mobile サーバーがアルファベット順に一覧表示されます。必要なログイン資格情報がある場合は、任意の数の Milestone Mobile サーバーを追加できます。

4. **Milestone Mobile クライアントでビデオを表示するときに、時々画質が低下するのはなぜですか。**

   Milestone Mobile サーバーは、サーバーとクライアント間で使用可能な帯域幅に従って、自動的に画質を調整します。XProtect® Smart Client より画質が低くなった場合、Milestone Mobile クライアントを通してフル解像度の画像を取得するには帯域幅が小さすぎる可能性があります。この理由は、サーバーからのアップストリーム帯域幅が小さ過ぎるか、クライアントのダウンストリーム帯域幅が小さ過ぎるかのいずれかが考えられます。Web サイト

『http://www.milestonesys.com/support/manuals-and-guides/』からダウンロードできる **XProtect Smart Client ユーザーマニュアル**を参照してください。

混合ワイヤレス帯域幅のエリアにいる場合は、より良い帯域幅のエリアに入ると、画質が改善される場合があります。

5. **どのようにしてビューを作成するのですか？**

   Milestone Mobile クライアントでビューを作成または設定することはできません。既に XProtect Smart Client で作成されたビューと関連する名前を使用します。ビューを設定していない場合は、**[すべてのカメラ]**ビューを使用して、システムのすべてのカメラを表示できます。後からいつでも XProtect Smart Client にその他のビューを追加できます。

6. **新しい Milestone Mobile ユーザーを追加するにはどのようにするのですか。**

   Milestone Mobile ユーザーは他の XProtect ユーザーとほとんど同じです。新しい Milestone Mobile ユーザーは、Management Application で新しいユーザーを追加する場合と同じ方法で追加します。ナビゲーションペインで**[ユーザー]**を右クリックし、**[新しい基本ユーザーの追加]**または**[新しい Windows ユーザーの追加]**を選択します。新しい基本ユーザーを選択した場合は、システムに応じて、サーバーログイン方法を**自動**または**基本のみ**に変更する必要があります。Management Application の **[サーバー] > [モバイルサーバー]**の下にあるモバイルサーバーエントリの**[全般]**タブにある**[ログイン方法]**ドロップダウンメニューからサーバーログイン方法を変更します。

7. **自分のパン/チルト/ズーム（PTZ）カメラをコントロールして、Milestone Mobile クライアントのプリセットを使用することはできますか。**

   はい。Milestone Mobile クライアントでは、接続された PTZ カメラを制御し、ライブモードでプリセットを使用できます。

8. **どうすれば録画を操作できますか。**

   Android：再生モードで記録映像を操作することができます。再生モードで表示するカメラを選択し、**[メニュー] > [再生]**を選択します。再生モードでは、コントロールボタンを使って記録を検索することができます。また、**[メニュー] > [時間に移動]**を選択して、特定の時間に移動することもできます。**[時間に移動]**を選択したら、表示する日付と時刻を選択します。

   iOS：再生モードで記録映像を操作することができます。再生モードで表示するカメラを選択し、[再生]をタップします。再生モードでは、コントロールボタンを使って記録を検索することができます。また、**[メニュー] > [時間に移動]**を選択して、特定の時間に移動することもできます。**[時間に移動]**を選択したら、表示する日付と時刻を選択して、**[確認]**をクリックします。

9. **ライブビデオと録画済みビデオを同時に見ることはできますか？**

   はい。再生モードでは、同じカメラから小さいピクチャインピクチャ(PiP)ビューを取得します。

10. **3G データプランなしで Milestone Mobile クライアントを使用することはできますか。**

    はい。Wi-Fi 経由で Milestone Mobile を使用できます。XProtect システムと同じネットワークでローカルに使用するか、カフェの公共ネットワークや自宅ネットワークなどの別の場所で使用できます。公共ネットワーク上の帯域幅は変動することがあり、ビデオストリームの画質に影響を与える可能性があることにご注意ください。

11. **4G/LTE データプランで Milestone Mobile クライアントを使用することはできますか。**

    はい、お使いの XProtect 動画管理システムに接続するインターネットにアクセスできるモバイルデバイスのすべてのデータ接続を使用することができます。

12. **複数のサーバーを Milestone Mobile クライアントに追加することはできますか。**

初めて Milestone Mobile クライアントを開くときには、カメラからビデオを取得するために、1 つ以上のモバイルサーバーを追加する必要があります。これらのモバイルサーバーはアルファベット順に一覧表示されます。別のサーバーからビデオを取得する場合は、この手順を繰り返します。関連するログイン資格情報がある場合は、任意の数のモバイルサーバーを追加できます。

13. **自分のオフィスで Wi-Fi を使用して自宅で XProtect 動画管理システムに接続する際の画質が悪いのはなぜですか。**

ご自宅のインターネットの帯域幅を確認してください。多くの民間のインターネット接続は、ダウンロードおよびアップロードの帯域幅が異なります。例えば、20 Mbit/2 Mbit のように記載されています。これは、自宅でのインターネット利用者は大量のデータをインターネットにアップロードする必要がほとんどなく、一方で大量のデータを消費するためです。XProtect 動画管理システムは、Milestone Mobile クライアントにビデオを送信する必要がありますが、お使いの接続のアップロード速度による制限を受けます。Milestone Mobile クライアントのネットワークのダウンロード速度が良好であるのに、複数の場所で低画質のままである場合、ご自宅のインターネット接続のアップロード速度をアップグレードすることで問題が解決される可能性があります。

14. **スクリーンショットはどこに保存されるのですか。**

Android：スナップショットは、デバイスの SD カード（**/mnt/sdcard/XProtect**）に保存されます。

iOS：スナップショットは、お使いのデバイスに保存され、お使いのデバイスの**写真**からアクセスすることができます。

Android または iOS のデフォルト設定は変更できません。

15. **HTTPS 接続を使用して XProtect Web Client を実行するときに、セキュリティ警告を表示させないようにするにはどのようにするのですか。**

認証資格情報のサーバーアドレス情報が正しくないため、警告が表示されます。接続は暗号化されます。Milestone Mobile サーバーの自己署名証明書は、Milestone Mobile サーバーに接続するために使用されるサーバーアドレスと一致する独自の証明書で置換する必要があります。これらの証明書は、Verisign などの正式な証明書署名機関から取得されます。詳細については、選択した署名機関にお問い合わせください。
Milestone Mobile サーバーは Microsoft IIS を使用しません。つまり、IIS を使用して署名機関によって証明書署名要求(CSR)を生成するために提供されている手順は、Milestone Mobile サーバーには適用されません。コマンドライン証明書ツールまたは同様の他社製アプリケーションを使用して、CSR ファイルを手動で作成する必要があります。この手順は、システム管理者または上級ユーザーのみが実行してください。

16. **私のプロセッサはハードウェアアクセラレーションデコードをサポートしていますか。**

Intel の新しいプロセッサのみがハードウェアアクセラレーションデコードをサポートしています。プロセッサがサポートされているかについては、Intel 社の Web サイト『http://ark.intel.com/search/advanced?s=t&MarketSegment=DT&QuickSyncVideo=true』を参照してください。

メニューで、**[技術]> [Intel Quick Sync Video]**が**[はい]**に設定されていることを確認します。

プロセッサがサポートされている場合は、ハードウェアアクセラレーションデコードがデフォルトで有効です。Mobile Server Manager の**[ステータスの表示]** 『**222**ページ の**"ステータスの表示について"** 参照 』で現在のステータスを確認できます。

17. **私の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ションデコードをサポートしていますか。**

Windows 8 および Windows Server 2012 以降のみがサポートされます。

Intel 社の Web サイトから取得した最新のグラフィックドライバをシステムにインストールしてください。これらのドライバは Windows Update からは取得できません。

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は、ハードウェアアクセラレーションデコードはサポートされません。

18. **どのようにモバイルサーバーのハードウェアアクセラレーションデコードを無効にするのですか。(詳細)**

    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ションデコードをサポートする場合、デフォルトで有効です。ハードウェアアクセラレーションデコードをオフにするには、次の手順を実行します。

    1. VideoOS.MobileServer.Service.exe.config ファイルを見つけます。標準的なパス：C:¥Program Files¥Milestone¥Milestone Mobile Server¥VideoOS.MobileServer.Service.exe.config
    2. メモ帳などのテキストエディタでファイルを開きます。必要に応じて、ファイルタイプ.config をメモ帳に関連付けます。
    3. フィールド<add key="HardwareDecodingMode" value="Auto" />を見つけます。
    4. "Auto"の値を"Off"に置換します。
    5. ファイルを保存して閉じます。

19. **ファイアウォールをオンにした後、モバイルデバイスを自分のサーバーに接続できません。なぜですか。**

    Milestone Mobile サーバーのインストール中にファイアウォールをオフにした場合、手動で TCP と UDP 通信を有効にする必要があります。

Milestone ONVIF Bridge

Milestone ONVIF Bridge について

ONVIF は、IP ビデオ製品監視が安全かつ基準に沿って機能するためのオープンでグローバルなフォーラムです。その目的は、ビデオデータの交換を容易にすることです。例えば、警察、監視センター、あるいは同様な機関が IP ベースの監視システムで流れたライブまた記録ビデオに迅速にアクセスできます。

Milestone Systems は、この目的を支援したいと考え、目的に向け Milestone ONVIF Bridge を開発しました。Milestone ONVIF Bridge は、Milestone「オープン・プラットホーム」の一部であり、すべての Milestone video management software 製品からライブまた記録されたビデオを復元させるための ONVIF の部分をサポートする共通領域を提供しています。

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
- Milestone ONVIF Bridge のインストールと構成方法（XProtect VMS 製品に関する）。
- さまざまな種類の ONVIF クライアントがライブまた録画された動画を XProtectVMS 製品からストリーミングできるようにする方法の例。

Milestone ONVIF Bridge と ONVIF 標準

ONVIF 標準は共通プロトコルを規定することで、情報交換を容易にします。プロトコルには ONVIF プロファイルが含まれます。これは、ONVIF 適合デバイス間の相互運用性の仕様のコレクションです。

Milestone ONVIF Bridge は、ONVIF プロファイル G とプロファイル S の部分と適合し、ライブおよび録画された動画へのアクセスを可能にし、またカメラのパン・ティルト・ズーム機能をコントロールできます。

- プロファイル G - 動画の録画、保存、検索、復元をサポートします。詳細については、「ONVIF プロファイル G の仕様」『https://www.onvif.org/wp-content/uploads/2017/01/ONVIF_Profile_G_Specification_v1-0.pdf』を参照してください。
- プロファイル S - H.264 コーデック、音声ストリーミング、およびパン・チルト・ズーム（PTZ）コントロールを使用したライブ動画のストリーミングをサポートします。詳細については、「ONOVIF プロファイル S の仕様」『https://www.onvif.org/wp-content/uploads/2017/01/ONVIF_Profile_-S_Specification_v1-1-1.pdf』を参照してください。

ONVIF 基準に関する詳細情報は、ONVIF®ウエブサイト 『http://www.onvif.org/』をご覧下さい。

ONVIF プロファイルは、データを復元する「get」機能と構成設定をする「set」機能をサポートします。各機能は、「強制」、「条件付き」、または「オプション」となっています。安全上の理由から、Milestone ONVIF Bridge は、次のような強制、オプション、条件付き「get」機能のみをサポートします。

- ビデオリクエスト
- ユーザーの確認
- ビデオを流す
- 記録ビデオを再生

ONVIF クライアントについて

ONVIFクライアントはONVIF Webサービスを使用するコンピュータアプライアンスまたはソフトウェアプログラムです。ONVIF のクライアントの例は、サーバー、メディアプレイヤー、IP ベースの監視システム、Milestone ONVIF Bridge などのブリッジです。

「リアルタイム・ストリーミング・プロトコル（RTSP）」は、二つあるいはそれ以上のメディア・セッションを作り、またコントロールするために使われます。Milestone ONVIF Bridge は、ONVIF プロフィール S と RTSP を ONVIF のクライアントからのビデオリクエストを扱うために使用し、XProtect インストールから ONVIF クライアントにビデオを流します。

既定により、ONVIF クライアントと ONVIF ブリッジサーバーの通信は、次のポートを使います。

- ONVIF ポート 580。ONVIF クライアントは、動画ストリームの要求を送信する際にこのポートを使用します。
- RTSP ポート 554。Milestone ONVIF Bridge このポートを ONVIF クライアントに動画をストリーミングするために使用します。

ONVIF クライアントは、Milestone ONVIF Bridge で RTSP ポートに直接アクセスできます。例えば、VLS メディア・プレイヤーまたはブラウザの VLC プラグインは動画を取得、再生できます。これについては、このドキュメントの「メディアプレイヤーを使用した動画ストリームの表示」を参照してください。

例えば、ポート同士の衝突を避けるために、異なるポートを使うこともできます。ポート番号を変える場合は、ONVIF クライアントの URI の RTSP ストリームを更新する必要があります。

RTSP は H.264 コーデックだけをサポートします。カメラは H.264 コーデックでビデオをストリーミングできる必要があります。

Milestone ONVIF Bridge

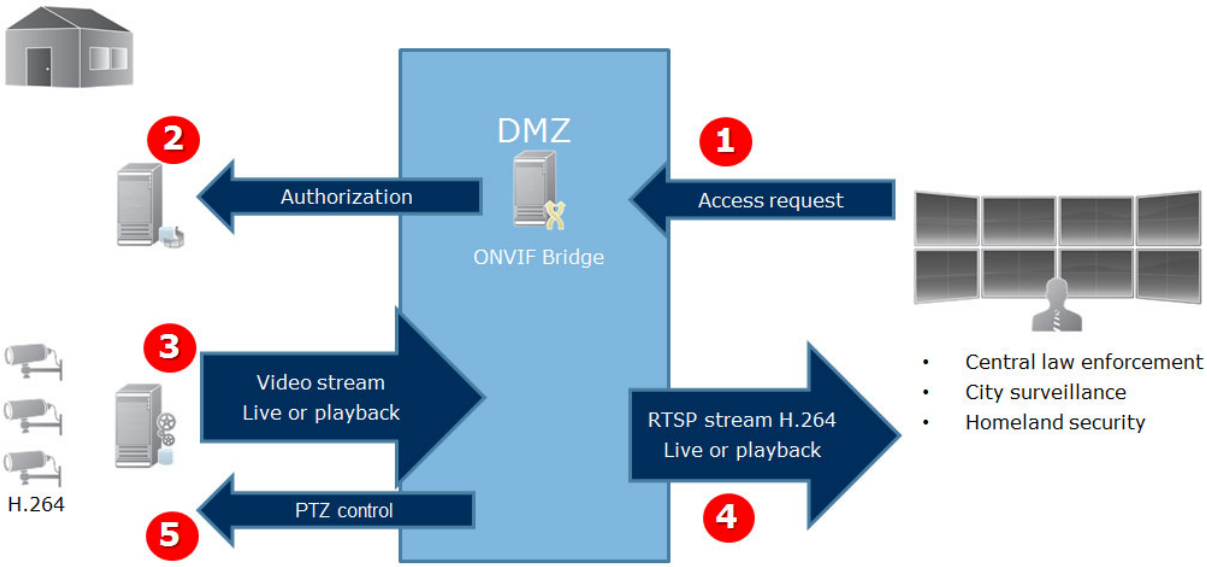
Milestone ONVIF Bridge は、次の構成要素で成立します。

- Milestone ONVIF Bridge サーバー
- Milestone ONVIF Bridge Management Application の 32 ビットプラグイン
- Milestone ONVIF Bridge Management Client の 64 ビットプラグイン

次の画像は ONVIF クライアント、Milestone ONVIF Bridge と XProtectVMS との間の相互作業の高度な画面を示しています。

注意： Milestone は、ONVIF ブリッジサーバーを非軍事ゾーン（DMZ）にインストールすることをお勧めします。

XProtect VMS **ONVIFクライアント**



1. ONVIF クライアントは、インターネットを使用して Milestone ONVIF Bridge 経由で XProtect VMS に接続します。そうするためには、ONVIF クライアントは Milestone ONVIF Bridge がインストールしたの IP アドレス、またはドメイン名および ONVIF ポートナンバーが必要です。
2. ONVIF ブリッジサーバーは、ONVIF クライアントユーザーを認定するため管理サーバーに接続します。
3. 認定が済むと、記録サーバーが、カメラから H.264 ビデオストリームを ONVIF ブリッジサーバーに送信を開始します。

   注意：カメラがマルチストリームをサポートする場合は、既定のストリームだけを送ります。
4. Milestone ONVIF Bridge は RTSP ストリームとして ONVIF クライアントにビデオを送信します。
5. 可能なら、ONVIF クライアントは、PTZ カメラを使用できます。

Milestone ONVIF Bridge セキュリティコントロールの設定

Milestone ONVIF Bridge は、ONVIF クライアントのユーザー認証を施行します。これは、ONVIF クライアントのカメラへのアクセス能力及び ONVIF クライアントのが実施する作業内容を管理します。例えば、ONVIF クライアントが、カメラのパン・ティルト・ズーム（PTZ）機能を使えるかどうかなどです。

Milestone は、貴方に、各 ONVIF クライアントのために、Milestone ONVIF Bridge の専用のユーザーアカウントを作成することをお勧めします。

1. Management Application の基本ユーザーまたは Windows ユーザーを作成します。
2. Management Client で、カメラにアクセスできるロールにユーザーを割り当て、ロールの［全体的なセキュリティ］タブで ONVIF ブリッジセキュリティグループの権限を指定します。
3. インストール中に、Milestone ONVIF Bridge にユーザーを割り当て、各 ONVIF クライアントについて Management Application でユーザーを割り当てます。

Milestone ONVIF Bridge は、ONVIF クライアントだけにカメラのビデオをリクエストし復元することを許可します。ONVIF クライアントは、XProtectVMS システムまたは、Milestone ONVIF Bridge の設定を構成することはできません。

安全上の用意として、Milestone は、ONVIF ブリッジサーバーを非軍事ゾーン（DMZ）にインストールすることをお勧めします。そのブリッジを DMZ にインストールしたら、内部・外部の IP アドレスにポート転送を構成する必要があります。

Milestone ONVIF Bridge のインストール

Milestone ONVIF Bridge をインストールするときには、サーバーと Management Application のプラグインをインストールします。）例えば、これらの構成要素を使ってカメラを管理したり、ユーザー設定したり、許可を与えるなどができます。

システムに一つまたはそれ以上追加 Milestone ONVIF Bridge をインストールできます。しかし、こうした増加はネットワークに関係し、パフォーマンスに影響します。典型的な例としては、Milestone ONVIF Bridge は、複数の ONVIF クライアントが一つのブリッジを経由して接続できるため一つのシステムに一つだけ追加します。

ONVIF ライセンス

Milestone ONVIF Bridge は追加ライセンスを必要としません。Milestone Systems ウエブサイト『http://www.milestonesys.com/』から無料のソフトウエアをダウンロードしてインストールできます。

システム要件

Milestone ONVIF Bridge をインストールしたい場合、そのコンピューターはインターネットへのアクセスが必要で、次のソフトウエアをインストールする必要があります。

- Microsoft® .NET Framework 3.5
- Microsoft® .NET Framework 4.5.1 以上

Visual Studio 2013 (x64)の Visual C++再配布可能パッケージ**重要**: カメラはインターネットを通して H.264 ストリーミングをサポートする必要があります。

何をインストールしていますか？

インストール中、つぎの構成要素がインストールされます。

- Milestone ONVIF Bridge サーバー、Milestone ONVIF Bridge サービスと MilestoneRTSP ブリッジサービス、Milestone ONVIF Bridge 管理を含むサーバーがインストールされます。
- Milestone ONVIF Bridge プラグイン。Management Application のサーバーノードでこのプラグインを使用できます。これは、**標準**インストール方法を使えば、自動的に起動します。**カスタム**インストール方法を使えば、後からインストールできます。

インストールは次の方法でもできます。

- Milestone ONVIF Bridge サービスと Milestone RTSP Bridge サービスに登録して開始します。
- Milestone ONVIF Bridge Manager を起動します。ONVIF ブリッジサーバーがインストールされているサーバーにある Windows 通知領域にあります。

注意：ONVIF Bridge Manager でのアクションは、Milestone ONVIF Bridge サービスと Milestone RTSP Bridge サービスの両方に適用されます。たとえば、ONVIF Bridge サービスを開始または停止すると、Milestone RTSP Bridge サービスも開始または停止します。

インストールする前に、

インストールを開始する前に、次の情報を入手します。

- Milestone ONVIF Bridge のために作成した専用のユーザーアカウントのドメイン名とパスワード。詳細については、「Milestone ONVIF Bridge セキュリティコントロールの設定 『231ページ 』」を参照してください。

管理サーバーの URL または IP アドレス、およびポート番号。インストールの際に、この情報が必要です。

Milestone ONVIF Bridge のインストール

インストールファイルのダウンロード：

1. Milestone ONVIF Bridge をインストールするコンピューターで、Milestone ウエブサイト『https://www.milestonesys.com/support/download-software/』へ行き Milestone ONVIF Bridge 製品を見つけます。
2. Milestone ONVIF Bridge インストールファイルをクリックします。
3. インストーラを実行し、ウィザードの指示に従います。

インストーラの実行：

1. 使いたい言語を選択し**「続行」**をクリックして下さい。
2. 使用許諾契約を読み、受諾したら、**[続行]**をクリックします。
3. 次のインストール方法を選択して下さい。
   - 1 つのコンピューターに ONVIF ブリッジサーバーとプラグインをインストールするためには、既定の設定を適用し、［**標準**］をクリックします。
     1. サーバーURL、ユーザー名、およびパスワードが正しいことを確認し、［**続行**］をクリックします。
     2. ファイルの場所と製品言語を選択し、**[インストール]**をクリックします。

     インストールが完了したら、インストールされた構成要素のリストが表示されます。**閉じる**をクリックします。
   - 別のコンピューターに ONVIF ブリッジサーバーとプラグインをインストールするためには、［**カスタム**］をクリックします。分散システムの場合にはこの方法を使用します。
     1. サーバーをインストールするには、［**Milestone ONVIF Bridge サーバー**］チェックボックスをオンにし、［**続行**］をクリックします。
     2. 管理サーバーとの接続を確立するためには、次を指定します。
        - 管理サーバーの URL または IP アドレス、ポート番号。既定のポートは 80 です。ポート番号を省略すると、ポート 80 が使用されます。

- ［ログインユーザー］フィールドを**ユーザーアカウント**に設定します。
- Windows ユーザーまたはサービスが使用する基本ユーザーのドメインユーザー名とパスワード。
- **続行**をクリックします。

3. ファイルの場所と製品言語を選択し、**[インストール]**をクリックします。

インストールが完了したら、インストールされた構成要素のリストが表示されます。

［閉じる］をクリックし、Management Application がインストールされているコンピュータに ONVIF Bridge プラグインをインストールします。プラグインをインストールするためには、コンピュータで再度インストーラを実行し、［**カスタム**］を選択して、該当するプラグインを選択します。

次のコンポーネントがインストールされます。

- Milestone ONVIF Bridge サーバー
- **サーバー**ノードで Management Application に表示される Milestone ONVIF Bridge プラグイン。
- ONVIF ブリッジサーバーがインストールされたサーバーの通知領域からアクセス可能な実行中の Milestone ONVIF Bridge Manager
- サービスとして登録された Milestone ONVIF Bridge サービス

初期構成 『234ページ の"Milestone ONVIF Bridge を構成する"参照 』の準備ができました。

Milestone ONVIF Bridge を構成する

Milestone ONVIF Bridge をインストール後、ONVIF Bridge サービスが動作すると、システムのアイコンが緑色に変わります。次の段階は

- Management Application への ONVIF Bridge プラグインの追加
- ONVIF クライアントが XProtect video management software 製品にアクセスできるようにします

Milestone ONVIF Bridge を Management Application に追加する

1. Management Application を開きます。
2. **サーバー**を展開し、**ONVIF Bridge** を右クリックして、**新規追加**を選択します。
3. Milestone ONVIF Bridge の名前を入力し、**OK** をクリックします。

ONVIF クライアントのユーザー設定の構成

これらの手順を完了する前に、Management Application の基本ユーザーまたは、ONVIF クライアントの Windows ユーザーを作成する必要があります。ユーザーはカメラを見たり、Milestone ONVIF Bridge にアクセスするため認可されるている必要があります。詳細については、「Milestone ONVIF Bridge セキュリティコントロールの設定 『231ページ 』」を参照してください。Management Application の基本ユーザーの設定方法に関する情報は、プログラムの「ヘルプ」をご覧下さい。

XProtect video management software への ONVIF クライアントアクセスを提供するには､次の手順に従います。

1. Management Application を開きます。
2. **サーバー**を展開し、**ONVIF ブリッジ**を選択してから、追加するブリッジを選択してください。
3. **ユーザー設定**タブで、ONVIF クライアントのために作成した専用ユーザーのドメインユーザー名（ドメイン/ユーザー）とパスワードを入力します。
4. **[ユーザーの追加]**ボタンをクリックします。

ONVIF クライアントのユーザー名は、**ONVIF ユーザー資格情報**リストに表示されます。

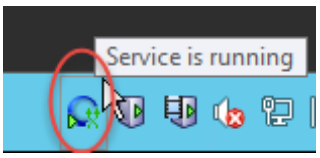
Milestone ONVIF Bridge の管理

Milestone ONVIF Bridge を構成した後には、複数の方法でサービスを監視し、構成設定を変更できます。

ONVIF Bridge サービスのステータスを確認します

ONVIF Bridge サービスのステータスを確認するには、次の手順に従います。

1. ONVIF Bridge サービスがインストールされているコンピュータの通知領域を確認します。ONVIF ブリッジトレイのアイコンが ONVIF Bridge サービスのステータスを示しています。サービスが実行中の場合は、アイコンが緑です。

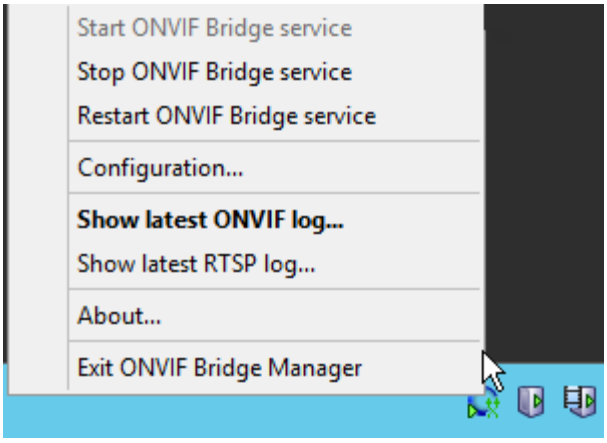


2. 実行中でない場合は、アイコンは黄または赤です。アイコンを右クリックして、**[ONVIF Bridge サービスの起動]**を選択します。

ログの表示

ONVIF Bridge Manager は、Milestone ONVIF Bridge と RTSP ストリームに関するログ情報を保存します。

1. ONVIF ブリッジ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で、ONVIF ブリッジトレイアイコンを右クリックします。



2. **[最新の ONVIF ログを表示]**または**[最新の RTSP ログを表示]**を選択します。

ログの情報レベルの変更

ONVIF Bridge Manager は、Milestone ONVIF Bridge と RTSP ストリームに関するログ情報を保存します。

ログの情報レベルを変更するには、次の段階を踏んで下さい。

1. ONVIF ブリッジのトレイアイコンを右クリックしてから、ONVIF Bridge サービスを停止します。
2. ONVIF ブリッジトレイアイコンをもう一度右クリックしてから、**構成**を選択します。
3. **ONVIF のログレベル**と **RTSP のログレベル**フィールドで、情報のタイプと、ONVIF と RTSP のログに保存する情報の量を指定します。デフォルト値は **Information** です。

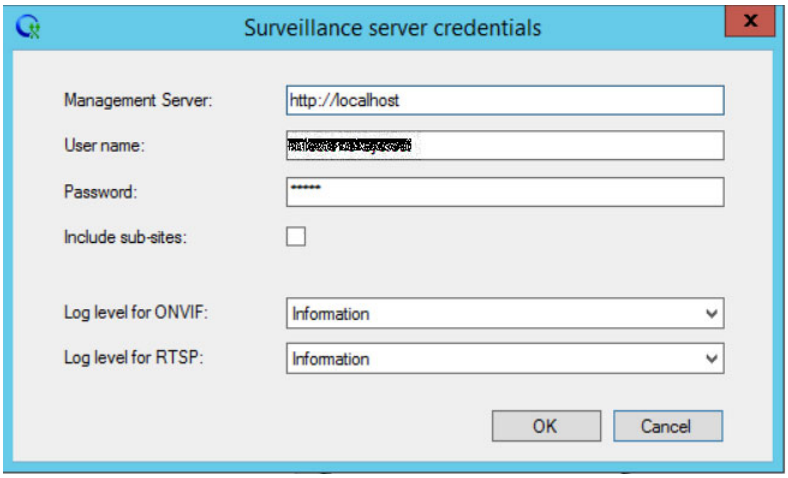
   注意：リストの最初から最後まで、最低レベルから最高レベルの順で並んでいます。リストの中で各レベルにはそれ以上のレベルが含まれています。例えば、**警告**レベルは**エラー**レベルを含んでいます。Milestone は、**エラー**、**警告**、**情報**レベルのみを使用することをお勧めします。**トレース**および**メッセージ**レベルはより多くの情報を収集することができますが、ディスクの容量をより多く使うため、パフォーマンスが低下する可能性があります。
4. [**OK**]をクリックします。
5. ONVIF ブリッジのトレイアイコンを右クリックしてから、ONVIF Bridge サービスを開始します。

Milestone ONVIF Bridge 設定の構成要素の変更

もし IP アドレスまたは監視サーバー名を変更する場合、または監視サーバーにアクセスしたユーザーアカウントを変更した場合は、Milestone ONVIF Bridge 情報を更新する必要があります。

VMS アドレスまたはログイン証明を変更するには、次の手順に従います。

1. Milestone ONVIF Bridge サーバーがインストールされているコンピューターで、ONVIF ブリッジのトレイアイコンを右クリックしてから、ONVIF ブリッジサービスを中止して下さい。
2. ONVIF ブリッジトレイアイコンをもう一度右クリックしてから、**構成**を選択します。



3. 新しい情報を特定してから、**OK** をクリックして下さい。

注意：管理サーバーがインストールされているサーバーの完全修飾ドメイン名または IP アドレスを使用する必要があります。

4. ONVIF ブリッジのトレイアイコンを右クリックしてから、ONVIF Bridge サービスを開始します。

ONVIF Bridge サービスが実行され、トレイアイコンが緑になります。

サブサイトを含みます

既定設定では、Milestone ONVIF Bridge は、補助サイトを排除するように構成されています。つまり、ONVIF クライアントユーザーは、補助サイトにインストールされたカメラのビデオにアクセスできません。

これを補助サイトも含むに変更できます。しかし、Milestone は、補助サイトはカメラを多数保有しないシステムだけにすることをお勧めします。Milestone ONVIF Bridge は、補助サイトのカメラも含むすべてのカメラが、集積された一つのリストに表示されます。たとえば、システムと補助サイトに 51 台以上のカメラがある場合、リストの使用は困難です。

ヒント：補助サイトを含む必要がある場合は、各管理サーバーに Milestone ONVIF Bridge をインストールすることを検討してください。カメラのリストが一つ以上になりますが、カメラを特定したりナビゲートするのは簡単になります。

サブサイトを含めるには

1. ONVIF ブリッジのトレイアイコンを右クリックしてから、ONVIF Bridge サービスを停止します。
2. ONVIF ブリッジのトレイアイコンをもう一度右クリックしてから、**構成**クリックして下さい。
3. **「補助サイトを含む」**のチェックボックスを選択してから、**OK** をクリックしてください。
4. ONVIF ブリッジのトレイアイコンを右クリックしてから、ONVIF Bridge サービスを開始します。

ヒントと豆知識

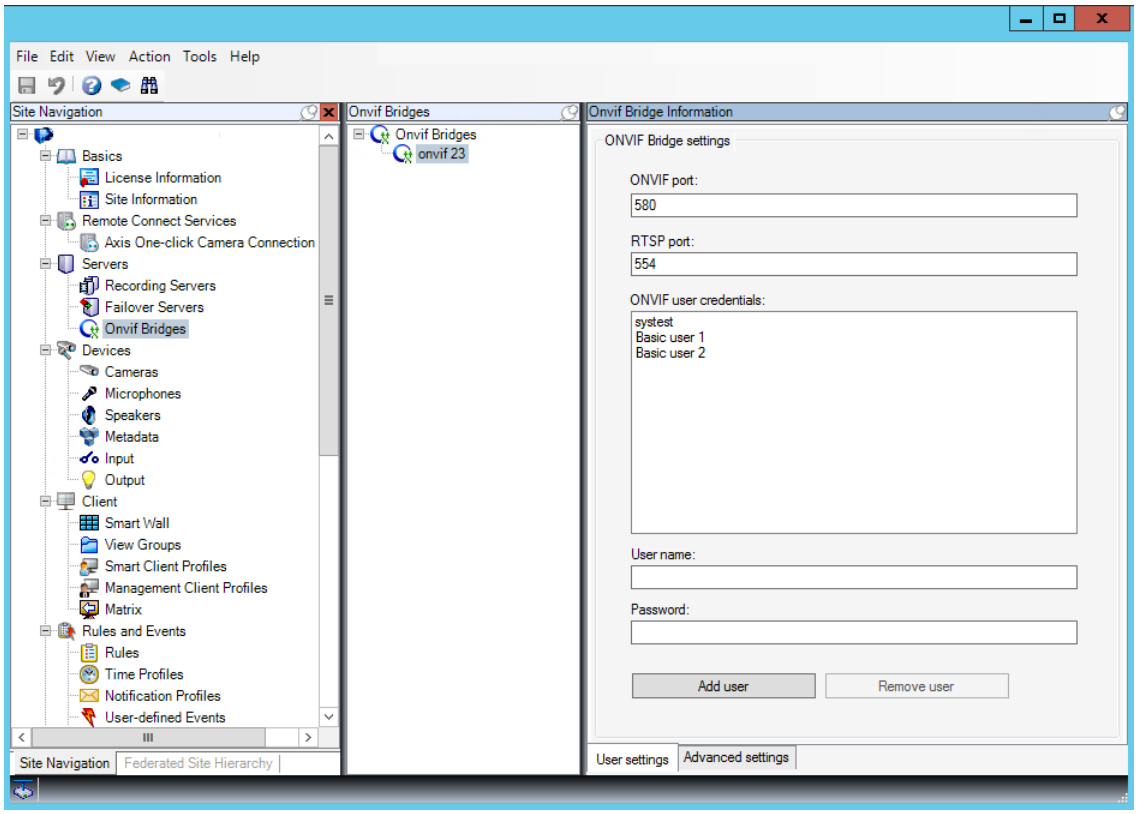
ONVIF ブリッジ管理者によって作成された構成は、ProgramData¥Milestone¥Milestone ONVIF Bridge のファイルに保存されます。このファイルの名前は serverconfiguration.xml となります。このファイルが削除される場合は、ONVIF ブリッジ管理者の構成を更新する必要があります。

構成を更新するには、このドキュメント内の Milestone ONVIF Bridge の構成設定の変更で説明されています。

Milestone ONVIF Bridge のプロパティ

このセクションは、管理ユーザーのための設定、接続、カメラの構成設定などの情報を提供しています。

Management Application を開き、**ONVIF ブリッジ**ノードを選択します。



ユーザー設定タブ（プロパティ）

次のテーブルは、ONVIF ブリッジサーバーと ONVIF クライアントのための設定を説明しています。

名前	説明
ONVIF ポート	ONVIF ポートのポートナンバーONVIF クライアントが ONVIF ブリッジサーバーに接続するために、このポートを使用します。 既定ポートナンバーは 580 です。
RTSP ポート	RTSP ポートのポートナンバーONVIF ブリッジサーバーは、ONVIF クライアントに RTSP ビデオ・ストリームを送信します。 既定ポートナンバーは 554 です。
ONVIF ユーザー情報	ONVIF ブリッジサーバーを通して、XProtectVMS システムにアクセスした ONVIF クライアントユーザーをリストに載せます。
ユーザー名	ONVIF クライアント用に作成されたユーザーのドメインユーザー名 資格要件貴方は、ONVIF クライアントユーザーを Management Application のユーザーとして設定しました。（カメラと Milestone ONVIF Bridge にアクセス可能）
パスワード	ONVIF クライアントユーザー用パスワード
ユーザーの追加	ドメインユーザー名とパスワードを入れてから、**「ユーザーの追加」**ボタンをクリックして下さい。

名前	説明
ユーザーの削除	ONVIF クライアントの Milestone ONVIF Bridge へのアクセスを避ける。**ONVIF ユーザー情報**リストから選択したユーザーを削除して下さい。

詳細設定タブ（プロパティ）

ONVIF Bridge の詳細設定では、クライアントが接続してビデオストリームを要求する際に ONVIF Bridge が ONVIF クライアントに提供するすべてのカメラのデフォルト設定が一覧表示されます。

この設定は、カメラの実際の構成を反映しているものではなく、ビデオ・ストリームに影響するものでもありません。このシステムは、ONVIF クライアントと ONVIF ブリッジとの間のビデオの交換を高速化するために、これらの設定を使用します。ONVIF クライアントは、RTSP ストリームから実際の設定を使用します。

カメラの実際的な構成を反映したいなどの場合は、ONVIF ブリッジが ONVIF クライアントに提供しているデフォルト設定を変更できます。

名前	説明
最大保持日数	デフォルト値は 30 です。
フレーム数/秒	デフォルト値は 5 です。
幅	デフォルト値は 1920 です。これはフル HD 品質に対応します。
高さ	デフォルト値は 1080 です。これはフル HD 品質に対応します。
ビットレート Kbps	デフォルト値は 512 です。
GOP サイズ	デフォルト値は 5 です。
コーデック	H.264 コーデックプロファイルのいずれかを選択します。デフォルト値は H.264 ベースラインプロファイルです。
カメラからの構成の使用	これを有効にして、上記で定義されたデフォルト平均値ではなく、カメラの実際の構成を使用します。 **注意：**この設定を有効にすると、XProtect システムと ONVIF クライアント間の応答時間が長くなります。
コマンドでシーケンスを返します	有効にすると、DESCRIBE コマンド応答でシーケンスの情報を返します。
返される最大シーケンス数	クライアントに送信されるシーケンスの最大数を設定します。デフォルト値は 10 です。
録画の開始または終了から返します	録画の開始または終了から、シーケンスの検索を開始する場所を選択します。
正規化時刻よりも絶対時刻を優先します	この設定は RTSP サーバー再生応答を定義します。ここでは、クライアントの再生時間間隔が指定されていません。 RTSP サーバーが調整または正規化された再生ではなくリアルタイムを使用する場合は、このオプションを選択します。 ただし、クライアントアプリケーションが相対時間間隔またはリアルタイム間隔（UTC）を使用するように設定されている場合は、RTSP サーバーはクライアントで定義された間隔で応答します。

動画再生の管理

再生コントロールは RTSP 標準と ONVIF ストリーミング仕様
『http://www.onvif.org/specs/stream/ONVIF-Streaming-Spec-v210.pdf』に準拠します。

再生の開始

動画再生を表示するときには、既定の速度は 1 です（順方向での標準再生）。

再生は RTSP PLAY メソッドで開始されます。範囲を指定できます。範囲が指定されていない場合、ストリームは開始から最後まで再生されます。ストリームが一時停止する場合は、一時停止された位置から再開します。この例では、「Range: npt=3-20」は RTSP サーバーが 3 秒目から 20 秒目まで再生を開始することを命令します。

例：

```
PLAY
rtsp://basic:basic@bgws-pvv-04:554/vod/943ffaad-42be-4584-bc2c-c8238ed96373
RTSP/1.0

CSeq:123

Session:12345678

Require:onvif-replay

Range:npt=3-20

Rate-Control:番号
```

逆再生

ONVIF デバイスは逆再生をサポートする場合があります。逆再生の場合、負の値の目盛ヘッダーフィールドで示されます。たとえば、データ損失なしで逆再生するには、値-1.0 が使用されます。

Milestone ONVIF Bridge は値 [-32：32]をサポートします。

```
PLAY
rtsp://basic:basic@bgws-pvv-04:554/vod/943ffaad-42be-4584-bc2c-c8238ed96373
RTSP/1.0

CSeq:123

Session:12345678

Require:onvif-replay

Range:clock=20090615T114900.440Z

Rate-Control:番号

Scale:-1.0
```

速度の変更

速度は RTSP Rate-Control ヘッダーで制御されます。「Rate-Control=yes」の場合、サーバーは再生速度を制御します。ストリームは、標準 RTP タイミングメカニズムによってリアルタイムで配信されます。
「Rate-Control=no」の場合、クライアントは再生速度を制御します。レート制御された再生は、一般的に、非 ONVIF 固有のクライアントでのみ使用されます。これらは「Rate-Control=no」を指定しないためです。

クライアントで再生速度を制御するには、提供されたコントローラを使用します。たとえば、VLC メディアプレイヤーで、**再生> 速度 > 高速** または**低速**を選択します。速度が 0.5 単位で増減します。

高速ファインと**低速ファイン**では 0.25 単位で速度が変わります。

コマンドラインエントリで VLC メディアプレイヤー再生を管理します

コマンドラインを使用して、VLC メディアプレイヤーで動画再生を管理できます。詳細については、VLC コマンドラインヘルプ 『https://wiki.videolan.org/VLC_command-line_help/』を参照してください。

このようなコマンドでは、たとえば、逆再生をしたり、再生の開始時間を変更したりできます。

一般的なコマンドラインの例：

```
>vlc.exe --rate=-1.0 --start-time=3600
"rtsp://basic:basic@bgws-pvv-04:554/vod/943ffaad-42be-4584-bc2c-c8238ed96373"
```

ここでは：

- rate は目盛および速度パラメタです
- start-time はデータベース起動後の秒数です

VLC メディアプレイヤーの再生コントロールは次のとおりです。

input-repeat=	<integer [-2147483648 ..2147483647]> 繰り返し入力 同じ入力が繰り返される回数
start-time=	<float> 開始時間 ストリームはこの位置で開始する（秒）
stop-time=	<float> 停止時刻 ストリームはこの位置で終了する（秒）
run-time=	<float> 実行時間 ストリームはこの期間に実行される（秒）
input-fast-seek no-input-fast-seek	高速シーク（既定で無効） シーク中に精度よりも速度を優先します
rate=	<float> 再生速度 再生速度を定義します（名目速度は 1.0）
input-list=	<string> 入力リスト 標準の後に連結される入力のカンマ区切りのリストを指定できます。
input-slave=	<string> 入力スレーブ（実験） これによって、複数の入力から同時に再生できます。この機能は実験であり、一部の形式ではサポートされていません。「#」区切りの入力リストを使用します

bookmarks=	<string> ストリームのリストをブックマークに追加します "{name=bookmark-name,time=optional-time-offset,bytes=optional-byte-off set},{...}"の形式でストリームのブックマークのリストを手動で指定できます

アラーム

アラームについて

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、製品比較チャート『12ページ 』を参照してください。

アラーム機能は、MIP に基づく機能であり、イベントサーバーによって処理される機能を使用します。組織全体での任意数のシステムのインストールにより、アラームを一元的に確認し、管理することができます。

以下のいずれかによりアラームが生成されるように設定できます：

- **内部イベント（システム関連）：** 例：モーション、サーバーの応答/非応答、アーカイブに関する問題、ディスク空き容量不足など。

外部イベント（統合）：例：MIP プラグインイベント。また、アラーム機能は一般的なアラームの設定やアラームのログの処理も含まれます。 アラームの設定アラーム設定には以下が含まれます。

- ユーザーのアクセス権に基づくアラーム処理のダイナミックセットアップ
- 全コンポーネントの一元的確認：サーバー、カメラ、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
- プラグインを使うことで、外部アクセスコントロール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。

アラームの表示

以下に、誰がどの程度アラームを表示/制御/管理できるかなど、アラームについての役割を挙げます。これは、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るためです。

- 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、ユーザーが認識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。
- 手動で定義されたイベントをトリガできる権限：手動で定義されたイベントをシステムで使用できる場合、これらによって、手動で定義されたイベントをユーザーが XProtect Smart Client でトリガできるかどうかが決まります。
- 外部プラグイン：外部プラグインがシステムで設定されている場合、これらがアラームを処理するユーザーの権限をコントロールする場合があります。
- 一般的なアクセス権限：ユーザーがアラームを確認できる（だけ）か、あるいはアラームを管理できるかを決定できます。

アラームの時間プロファイル：

アラームは、（アラームの）時間プロファイル 『244ページ の"（アラームの）時間プロファイルの追加"参照 』に基づきます。アラームの時間プロファイルとは、アラームの定義を作成する際に使用する期間です。たとえば、月曜日の 2:30 PM から 3:30 PM までをカバーするアラームの時間設定を作成し、その時間設定を使ってこの期間内だけ特定のアラーム定義が有効にすることができます。

アラームおよび XProtect Smart Client

アラームは、XProtect Smart Client のアラームリストに表示されます。ここで、アラームを表示および管理して、アラームの処理の概要表示、委任、処理を簡単に行えます。たとえば、アラームの再割り当て、ステータスの変更、アラームのコメント入力ができます。

アラームをマップ機能 『243ページ の"マップについて"参照 』に統合できます。このように、アラーム機能は強力な監視ツールであり、アラームおよび技術的な問題の可能性の概要を即座に提供できます。

アラームおよび XProtect Central

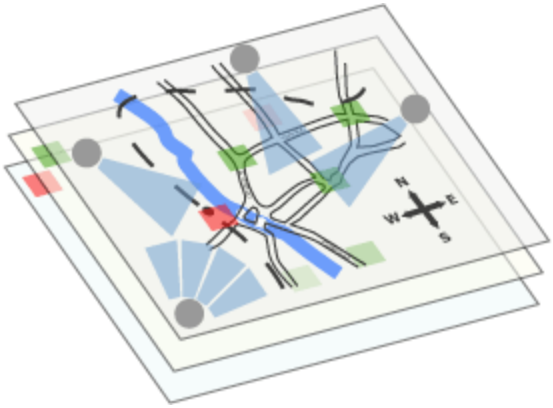
アラーム機能は、ほぼ XProtect Central と同じ機能をカバーし、XProtect Central 機能の設定は、現在はアラーム機能に含まれています。

XProtect Central は、次の 2 つの部分で構成される独立した製品です。専用サーバーと多数の専用クライアントです。他方、アラームはシステムに統合された一部分です。つまり、XProtect Central に必要なほとんどの設定は、アラームの導入と重複します。クライアントごとに、アラーム機能は XProtect Smart Client を使用します。ただし、それでも Management Application でアラーム、（アラームの）時間プロファイル、一般設定を行う必要があります。これらの機能は、XProtect Central と非常に似ています。XProtect Central の古いアラームやマップ定義を再使用することはできません。アラーム機能でアラームやマップ定義を再定義する必要があります。

マップについて

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、製品比較チャート『12ページ 』を参照してください。

マップをアラームの一部として統合することにより、監視システムの物理的配置を把握できます。カメラをマップに配置する機能により、アラームの発生源、カメラの配置、向きなどをいつでも知ることができます。また、俯瞰マップから詳細マップへ（または反対方向へ）移動することもできます。都道府県マップを例として、このマップ上へ、都市・近隣・道路・見取り図などのより詳細なマップへ移動するためのホットゾーン（地図上の小さいアイコン）を配置できます。



例：マップの階層

マップについてのすべての対話処理（マップの追加・管理を含む）は XProtect Smart Client 上で行います。

詳細については、XProtect Smart Client のドキュメントを参照してください。マップを使用するには、Event Server サービスが動作中である必要があります。監視サーバーのインストール 『33ページ の"システムソフトウェアのインストール"参照 』で**標準**インストールを実行していれば、Event Server サービスは自動的に含まれています。

アラームの追加

アラームを追加または設定するには

1. **アラーム**を展開し、**アラーム定義**を右クリックし、**新規作成**を選択します。
2. 必要なプロパティ 『244ページ の"アラーム定義"参照 』を指定します。**OK** をクリックします。
3. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

アラームの詳細概要や機能の動作原理については、アラームについて 『242ページ 』を参照してください。

（アラームの）時間プロファイルの追加

時間プロファイルは、アラーム機能でのみ使用される期間です。

アラームに時間プロファイルを追加するには、次の手順を実行してください。

1. **アラーム**を展開し、**時間プロファイル**を右クリックし、**新規作成**を選択します。**時間プロファイルプロパティ**ウィンドウの右上の小さな月の概要には、時間プロファイルが対応する期間の概略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。
2. カレンダーで、**日ビュー**、**週ビュー**、**月ビュー**のタブを選択してから、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...**のいずれかを選択します。
3. **1 つの時間を追加...**を選択した場合は、**開始時間**と**終了時間**を指定します。時間が終日に渡る場合は、**終日イベント**ボックスを選択します。
   ーあるいはー
   繰り返し時間を追加...を選択する場合は、時間の範囲、繰り返しパターン、および繰り返し範囲を指定します。**OK** をクリックします。
4. Management Application の右上の黄色の通知バーで、**保存**をクリックして、設定の変更を保存します。

既存の時間プロファイルを編集する場合、時間プロファイルには 2 つ以上の期間が含まれ、期間が繰り返される場合もあることに留意してください。

アナリティックイベントは、一般的に、外部のサードパーティのビデオコンテンツ分析(VCA)プロバイダから受信したデータです。VCA ベースのシステムの例として、アクセスコントロールシステムが挙げられます。

アラームプロパティ

アラーム定義

アラーム定義 『244ページ の"アラームの追加"参照 』を設定する際は、以下を指定します。

有効	アラーム機能を有効にします。

名前	名前を入力します。アラームが一覧表示されると、アラームの名前が表示されます。 アラーム名は一意である必要はありません。
詳細	説明（オプション）を入力します。
イベントのトリガ	この最初のリストは、システムレベルのイベントとプラグインからのイベント（たとえば、アクセスコントロールシステムなど）の両方を表示します。 2 番目のリストでは､アラームがトリガされた時に使用するイベントメッセージを選択します。
ソース	アラームをトリガ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。インストールされている場合、たとえばナンバープレート認識などのプラグイン定義の発生源、アクセスコントロールシステム、MIP プラグインなどが、このリストに表示されます。 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ます。
時間プロファイル	**時間プロファイル**を選択した場合は、アラームのトリガがいつ有効になるかを選択しなければなりません。アラームの時間プロファイル 『244ページ の"（アラームの）時間プロファイルの追加"参照 』を指定していない場合は、**常時**だけが選択できます。1 つまたは複数の時間プロファイルを定義している場合、このリストから選択します。
対象のイベント	**対象のイベント**を選択する場合、アラームを開始および終了させるイベントを選択しなければなりません。選択できるイベントは、カメラ、ビデオサーバーおよび入力で定義されたハードウェアイベント 『108ページ の"イベントおよび出力の概要"参照 』です。グローバル/手動イベント定義 『111ページ の"手動イベントの追加"参照 』も使用できます。 **対象のイベント**を選択する場合、出力に基づいてアラームを定義することはできず、入力のみであることに注意してください。
時間制限	その制限内でオペレータがアラームに応答しなければならない時間制限を選択します。
イベントがトリガーされました	**時間制限**で指定される限度内にオペレータが反応しなかった場合にトリガされるイベントを選択します。これには、たとえば E メール、SMS の送信などが挙げられます。
関連するカメラ	そのカメラ自体がアラームをトリガしなくても、アラームの定義に含めるカメラを選択します（最大で 15 台）。これは、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に関係します。ドア付近のカメラ 1 台または複数を定義することで、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。
関連するマップ	アラーム定義と関連付けるマップを選択します。 選択したマップは、アラームがリストされるたびに、XProtect Smart Client で自動的に表示されます。これによって、アラームの物理的位置をよりすばやく特定できます。
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。アラームの原因となったイベントのソースとして選択されている**すべて**のカメラおよびその他のデバイスを表示できるユーザーからだけ選択できます。
初期アラームの優先度	アラームの優先度（**高**、**中**または**低**）を選択します。優先度は、XProtect Smart Client での分類や、ワークフローの管理に使用できます。

初期アラームのカテゴリ	アラームを最初に割り当てるべきカテゴリを選択します。これには、たとえばどのカテゴリが定義されているかに応じて、**ビル 01**、**侵入**、**東エレベータ**などになります。
アラームでトリガされるイベント	XProtect Smart Client でアラームによってトリガされるイベントを定義できます（必要な場合）。
アラームを自動で閉じる	特定のイベントでアラームを自動的に閉じるかどうかを選択できます。これは、一部（全部ではない）のイベントによってトリガされるアラームで可能です。

また、アラーム設定の詳細情報については、アラームデータ設定 『246ページ 』およびアラームサウンド設定 『247ページ の"サウンド設定"参照 』も参照してください。

アラームデータ設定

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、プロパティ

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 『244ページ の"アラーム定義"参照 』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られる音声を選択します。デフォルトの音声を使用するか、音声の設定 『247ページ の"サウンド設定"参照 』に追加します。

アラームデータレベルタブ、ステータス

レベル	選択したレベル番号の新しい状態を追加します。このような状態レベルは、XProtect Smart Client の**アラームリスト**にのみ表示されます。デフォルト状態レベル **1**、**4**、**9**、**11** は、編集や再利用ができません。
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。

アラームデータレベルタブ、カテゴリ

レベル	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 『244ページ の"アラーム定義"参照 』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。

アラームリスト設定タブ

使用可能な列で、**>**を使用して、XProtect Smart Client **アラームリスト**でどの列を使用可能にするか選択します。**<**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、含める項目が表示されます。

終了の理由タブ

有効	すべてのアラームが閉じられる前に、閉じ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	アラームを閉じる際にユーザーが選択できる、閉じる理由を追加します。例として、**解決済み-侵入者**または**偽警告**が挙げられます。必要な数だけ作成できます。

サウンド設定

サウンド設定を行う際には、以下を指定します。

音声	アラームに関連付けられる音声を選択します。音のリストには、デフォルトの Windows 音が多数含まれています。これらは編集できません。ただし、パルス符号変調（PCM）でエンコードされている場合のみ、ファイルタイプ.wav の新しい音を追加できます。 デフォルト音は Windows のサウンドファイルですが、ローカル Windows 設定によっては、マシンによって音が異なる場合があります。ユーザーがこれらのサウンドファイルの一部を削除している場合、再生できない場合もあります。すべての状況で音が同一に再生されるためには、PCM でエンコードされた独自の.wav ファイルをインポートして使用する必要があります。
追加	サウンドをシステムに追加します。1 つ以上の.wav ファイルをアップロードするための音をブラウズできます。
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。 デフォルトのサウンドは削除できません。
テスト	音をテストできます。リストから音を選択します。音が 1 回再生されます。

時間プロファイル

時間プロファイル 『244ページ の"（アラームの）時間プロファイルの追加"参照 』の設定を行う際には、以下を指定します。

名前	時間プロファイルの名前を入力します。
詳細	説明（オプション）を入力します。

1 つの時間を追加	カレンダーを右クリックして、**1 つの時間を追加**を選択します。**開始時間**と**終了時間**を指定します。時間が終日に渡る場合は、**終日イベント**を選択します。
繰り返し時間を追加	カレンダーを右クリックして、**繰り返し時間を追加**を選択します。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。
時間を編集	カレンダーを右クリックし、**時間を編集**を選択します。**開始時間**と**終了時間**を指定します。時間が終日に渡る場合は、**終日イベント**を選択します。 既存の時間プロファイルを編集する場合、時間プロファイルには 2 つ以上の期間が含まれ、期間が繰り返される場合もあることに留意してください。時間プロファイルに追加期間を含めたい場合は、1 つの時間または繰り返し時間を追加します。

MIP プラグイン

※本機は、MIP プラグインには対応していません。

MIP プラグインについて

MIP プラグインは、システムにインストールできるアドオンです。MIP プラグインをインストールすると、ここでプラグイン情報を確認できます。一部の MIP プラグインは Milestone アドオン製品です。アドオン製品をインストールした場合は、購入したアドオン製品ライセンス数と、認証した数が表示されます。

MIP 関連のユーザー権限をユーザーやユーザーグループに割り当てることができます。「ユーザーおよびグループの権限の設定」 『161ページ の"ユーザーおよびグループの権限の設定"参照 』を参照してください。

XProtect Transact

※本機は、XProtect Transact には対応していません。

XProtect Transact の概要

XProtect Transact について

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、製品比較チャート『12ページ 』を参照してください。

XProtect Transact は、Milestone の IP ビデオ監視ソリューションであるのアドオンです。

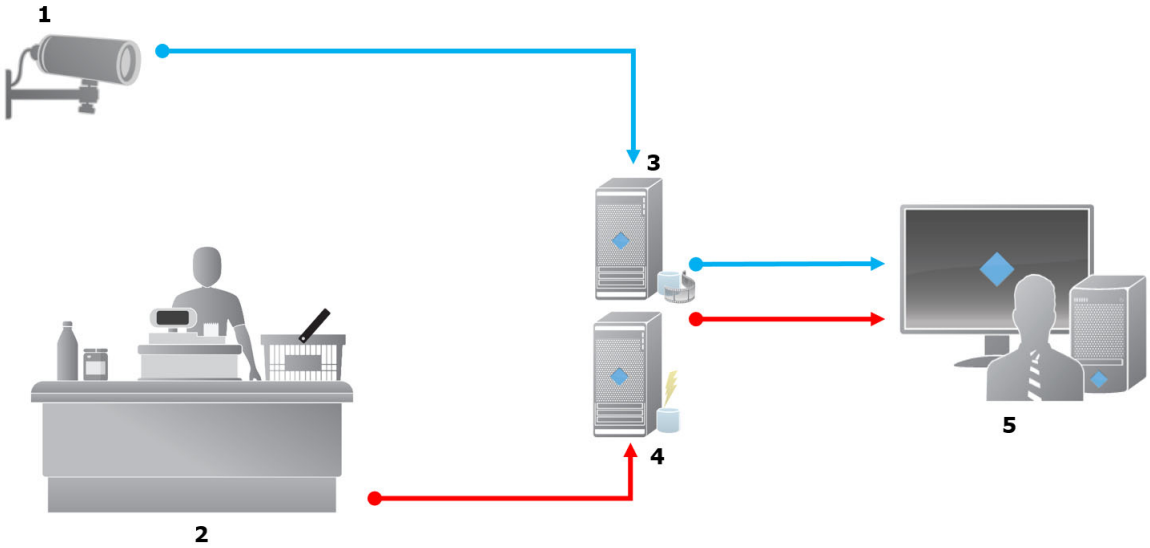
XProtect Transact は、実行中のトランザクションを監視し、過去のトランザクションを調査するためのツールです。トランザクションは、詐欺を証明したり、犯人のエビデンスを提示したりするために、トランザクションを監視するデジタル監視動画にリンクしています。トランザクションラインと動画画像の間には 1 対 1 の関係があります。

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。

XProtect Transact システムアーキテクチャ

XProtect Transact 通信フローには複数のコンポーネントがあります。入力データは、ビデオ監視カメラと、キャッシュレジスターや ATM などのトランザクションデータを提供するトランザクションソースから発生します。トランザクションデータはイベントサーバーに保存され、ビデオストリームはレコーディングサーバーに保存されます。サーバーのデータは XProtect Smart Client に転送されます。

お使いのシステムによって、数種類の録画サーバーが存在します。



図例：

- 1 = カメラ。
- 2 = キャッシュレジスター。
- 3 = Recording サーバー。
- 4 = Event サーバー。
- 5 = Smart Client。
- 青色の矢印は、監視システムの動画録画を示します。

赤色の矢印は、トランザクションソースのトランザクションデータを示します。標準では、 XProtect Transact は 2 つのタイプのトランザクションソースをサポートします。

- シリアルポートクライアント。
- TCP サーバークライアント。

追加のタイプのトランザクションソースは、ERP システムからトランザクションデータを取得するコネクタなど、MIP ソフトウェア開発キット(SDK)によって開発されたカスタムコネクタを使用してサポートすることができます。

コネクタについて

コネクタにより、ATM などのトランザクションソースから未加工トランザクションデータを、video management software に関連付けられたイベントサーバーにインポートしやすくなります。

次の表は、使用可能なビルトインコネクタを示します。

名前	説明
TCP クライアントコネクタ	トランザクションソースが TCP サーバーインターフェイス経由でトランザクションデータを配信するときに使用します。このコネクタには 2 つの設定を指定できます。ホスト名とポート番号です。
シリアルポートコネクタ	イベントサーバーのシリアルポートで入力としてトランザクションデータを受信するときに使用します。

MIP ソフトウェア開発キットによって開発されたソフトウェアも使用できます。

参照

トランザクションソースの追加(ウィザード) 『252ページ 』

トランザクション定義

トランザクション定義は設定のグループであり、トランザクションソースの未加工データを動画録画とともに XProtect Smart Client で表示する方法を制御できます。出力は、レジのレシートや ATM のレシートなど、実際のレシートに似たわかりやすい形式です。

具体的には、トランザクション定義では次のことができます。

- 個別のトランザクションと開始と停止を定義します。
- 必要に応じて改行を挿入します。
- データがプリンタ接続で発生し、改行を示す印刷不能な文字が含まれている場合や、レジのレシートを切るときなど、不要な文字やテキスト文字を除外します。
- 文字を別の文字で置換します。

複数のトランザクションソースで同じトランザクション定義を使用できます。

参照

トランザクション定義の追加 『253ページ 』

トランザクションイベント

トランザクションイベントは、トランザクションソース（キャッシュレジスタなど）からイベントサーバーに転送されるトランザクションデータのストリームにおける特定の単語、数字、または文字の発生です。システム管理者として、イベントを定義する必要があります。これにより、オペレータは XProtect Smart Client のトランザクションイベントを追跡および調査できます。各イベントに対して、完全一致、ワイルドカード、または正規表現の中から方法(一致タイプ)を指定し、トランザクションデータの文字列を特定する必要があります。

参照

トランザクションイベントの定義 『256ページ 』

トランザクションアラームの作成 『257ページ の"トランザクションイベントに基づくアラームの作成"参照 』

互換性

XProtect Transact は、次の製品のバージョン 2016 と互換性があります。

- XProtect Professional
- XProtect Express.

使用開始

XProtect Transact の機能は Management Application の標準です。XProtect Smart Client で XProtect Transact 機能を使用する前に、次のことを行う必要があります。

1. XProtect Transact の基本ライセンスが認証されたことを確認します。また、監視が必要な各トランザクションソース用のトランザクションソースライセンスがあることを確認してください。ライセンス情報は **MIP プラグイン**ノードで使用できます。

   トランザクションソースライセンス数が十分ではない場合、30 日間の猶予期間が終了する前に追加ライセンスを取得したことを確認します。

2. キャッシュレジスターなどのトランザクションデータを提供するソースを追加および構成します。詳細については、「トランザクションソースの追加(ウィザード) 『252ページ 』」を参照してください。

3. (任意)トランザクションデータを定義、ルールまたはアラームをトリガーするように構成できます。XProtect Smart Client では、オペレータはトランザクションイベントを調査できます。

XProtect Transact ライセンスを購入していない場合でも、試用版ライセンスで XProtect Transact を試すことができます。詳細については、「XProtect Transact 試用版ライセンス 『251ページ 』」を参照してください。

参照

トランザクションの設定 『252ページ 』

イベント設定 『256ページ の"トランザクションイベントとアラームの設定"参照 』

XProtect Transact 試用版ライセンス

XProtect Transact 試用版ライセンスを使用して、最大 30 日まで XProtect Transact 機能を試すことができます。すべての関連する機能が有効になり、キャッシュレジスターなどのトランザクションソースを 1 つ追加できます。30 日間の試用期間が終了したら、**Transact** ワークスペースとトランザクションビュー項目を含む、すべての XProtect Transact の機能が無効になります。XProtect Transact 基本ライセンスと必要なトランザクションソースライセンスを購入して認証すると、もう一度 XProtect Transact を使用でき、設定とデータは維持されます。

XProtect Professional VMS 製品を使用している場合は、試用版ライセンスはビルトインライセンスです。システム管理者が構成にトランザクションソースを追加すると、試用版ライセンスが認証されます。

その他の製品については、Milestone から試用版ライセンスを取得する必要があります。システム管理者は構成で試用版ライセンスを認証する必要があります。

XProtect Transact 構成

トランザクションの設定

このセクションでは、トランザクションソースの追加および構成方法、およびトランザクション定義の作成方法について説明します。

トランザクションソースの追加(ウィザード)

トランザクションソースから XProtect Transact にデータを接続するには、ATM などのトランザクションのソースを追加する必要があります。ウィザードでは、コネクタを選択し、1 つ以上のカメラを接続できます。

追加するトランザクションソースのトランザクションソースライセンスがない場合は、30 日間の猶予期間中はシステムが動作します。追加のトランザクションソースライセンスを取得し、期限内に認証してください。

手順：

1. Management Application のナビゲーションペインで**[トランザクト]**を展開します。
2. **[トランザクションソース]**ノードを右クリックし、**[ソースの追加]**を選択します。ウィザードが表示されます。
3. ウィザードの手順に従います。
4. 選択するコネクタによって、フィールドに表示される必須入力フィールドが異なります。詳細については、「トランザクションソース(プロパティ) 『252ページ 』」を参照してください。ウィザードを完了した後に、これらの設定を変更できます。
5. 必要なトランザクション定義が使用できない場合は、**[新規追加]**をクリックして、新しいトランザクション定義を作成できます。

参照

トランザクション定義の追加 『253ページ 』

コネクタについて 『249ページ 』

トランザクションソース(プロパティ)

トランザクションソースの設定は表で説明します。

名前	説明
有効	トランザクションソースを無効にする場合は、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が停止しますが、既にインポートされたデータはイベントサーバーに残ります。保持期間中には 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	名前を変更する場合は、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するときには、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。

名前	説明
トランザクション定義	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行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。 • トランザクションが開始および終了するとき。 • トランザクションが XProtect Smart Client に表示される方法。
保持期間	イベントサーバーでトランザクションデータを保持する期間を日数で指定します。デフォルトの保持期間は 30 日です。保持期間が終了すると、自動的にデータが削除されます。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、これらの設定を指定し、トランザクションソースの設定と一致することを確認します。 • **シリアルポート**：COM ポートを選択します。 • **ボーレート**：1 秒間に転送されるビット数を指定します。 • **パリティー**：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。 • **ストップビット**：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。

参照

トランザクションソースの追加(ウィザード) 『252ページ 』

Add transaction definitions 『253ページ の"トランザクション定義の追加"参照 』

トランザクション定義の追加

トランザクションソースの定義の一部として、ソースの定義を指定します。定義は、受信された未加工データを表示可能なデータに変換します。これにより、ユーザーは、実際の受信と一致する形式で XProtect Smart Client のデータを表示できます。一般的に、未加工データはデータの 1 つの文字列であり、個別のトランザクションの開始および終了位置を確認することが困難になる可能性があるため、この処理が必要になります。

手順：

1. Management Application のナビゲーションペインで**[トランザクト]**を展開します。
2. **トランザクションの定義**を選択します。
3. **[トランザクションの定義]**を右クリックし、**[行の追加]**を選択します。複数の設定が**[プロパティ]**セクションに表示されます。
4. **[開始パターン]**と**[終了パターン]**フィールドを使用して、受信の開始および終了を定義するデータを指定します。
5. **[データ収集の開始]**をクリックし、接続されたデータソースから未加工データを収集します。収集するデータが多くなるほど、制御文字などの置換または省略したい文字が見つからないリスクが低くなります。
6. **[未加工データ]**セクションで、置換または省略する文字をハイライト表示します。文字を手動で入力する場合は、この手順を省略し、**[フィルタの追加]**をクリックします。
7. **[フィルタの追加]**をクリックし、トランザクションソースデータから選択した文字が XProtect Smart Client に表示される方法を定義します。
8. フィルタごとに、文字を変換する方法を決定するアクションを選択します。**[プレビュー]**セクションには、定義されたフィルタでデータを表示する方法がプレビュー表示されます。

フィールドの詳細については、「トランザクション定義（プロパティ） 『254ページ 』」を参照してください。

また、コンピュータにローカル保存された、以前に収集されたデータを読み込むこともできます。この場合、**[ファイルから読み込む]**をクリックします。

トランザクション定義（プロパティ）

トランザクション定義の設定は表で説明します。

名前	説明
名前	名前を入力します。
エンコーディング	キャッシュレジスターなど、トランザクションソースによって使用される文字セットを選択します。これにより、XProtect Transact は、定義を構成するときに操作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。 間違ったエンコーディングを選択すると、データが意味のない文字として表示される場合があります。
データ収集の開始	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使用できます。 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機します。
データ収集の停止	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	既に存在するファイルからデータをインポートする場合は、このボタンをクリックします。一般的に、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ディングが、現在の定義で選択されたエンコーディングと一致することです。

名前	説明
ファイルに保存	収集された未加工データをファイルに保存する場合は、このボタンをクリックします。後から再利用できます。
一致タイプ	収集された未加工データで開始マスクと停止マスクを検索するために使用する一致タイプを選択します。 • 完全一致を使用：**[開始マスク]**および**[終了マスク]**フィールドに入力したものとまったく同じ内容を含む文字列を特定します。 • ワイルドカードの使用：ワイルドカード記号(*、#、?)を組み合わせ、**[開始マスク]**および**[終了マスク]**フィールドに入力したものと同じ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。たとえば、「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。たとえば、「# watermelon」と入力すると、「1 watermelon」などを含む文字列を特定します。 ?は 1 文字と一致します。たとえば、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。 • 正規表現の使用：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 社の Web サイト『https://msdn.microsoft.com/en-us/library/az24scfc(v=vs.110).aspx』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。
開始マスク	トランザクションの開始位置を示す開始マスクを指定します。**[プレビュー]**フィールドには横の線が挿入され、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、個別のトランザクションを区切ります。
停止マスク	トランザクションの停止位置を示す停止マスクを指定します。停止マスク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。 停止マスクを指定しない場合は、受信の終了は次の受信の開始場所として定義されます。開始は、**[開始マスク]**フィールドに入力された内容によって決まります。
フィルターの追加	**[フィルタの追加]**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で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、文字の置換が有効です。XProtect Smart Client での受信を元の受信のように表示するには、改行の追加が必要です。
テキストのフィルター	**[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、収集された未加工データ文字列に出現していない場合は、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,...}。

名前	説明
アクション	追加するフィルタごとに、選択した文字が処理される方法を指定してください。 • 除外：選択する文字は除外されます。 • 代替：選択した文字は、指定した文字で置換されます。 • 改行の追加：選択した文字は改行で置換されます。
置換	選択した文字を置換するテキストを入力します。**[代替]**を選択した場合にのみ必要です。
プレビュー	**[プレビュー]**セクションを使用して、不要な文字を特定して除外したことを確認します。ここに表示される出力は、XProtect Smart Client での実際の受信内容と似ています。

参照

Add transaction definitions 『253ページ の"トランザクション定義の追加"参照 』

トランザクションイベントとアラームの設定

このセクションでは、トランザクションイベントを定義し、アラームを設定する方法について説明します。

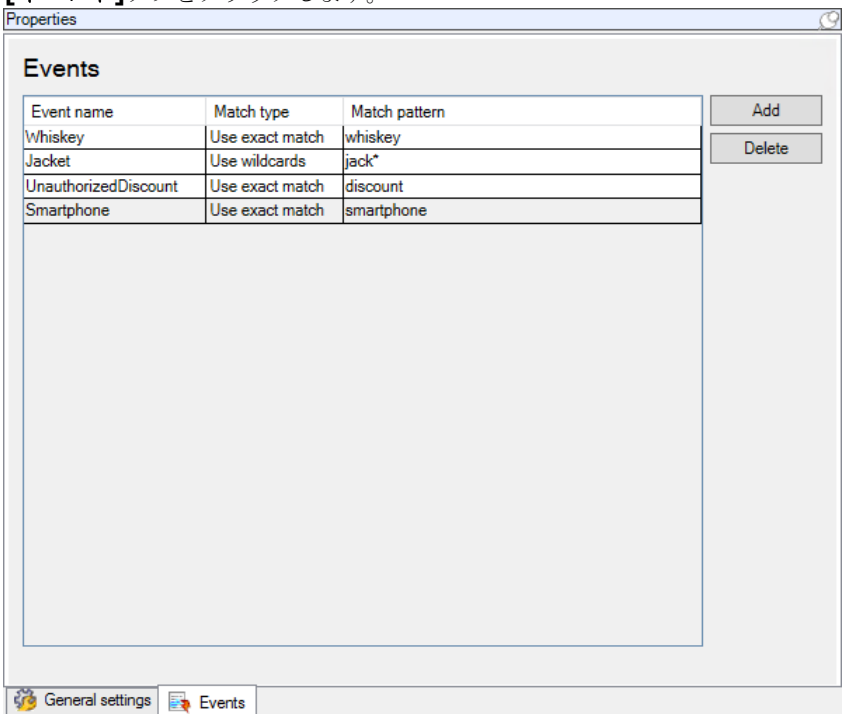
トランザクションイベントの定義

XProtect Smart Client でトランザクションイベントを追跡および調査するには、まず、スマートフォンの取得といったイベントを定義する必要があります。トランザクション定義でトランザクションイベントを定義し、定義されたイベントが、キャッシュレジスタなどのトランザクション定義を使用するすべてのトランザクションソースに適用されるようにします。

手順：

1. Management Application のナビゲーションペインで**[トランザクト]**を展開します。

2. イベントを定義するトランザクション定義を選択します。
3. **[イベント]**タブをクリックします。



4. **[プロパティ]**ペインで**[追加]**をクリックします。新しい行が追加されます。
5. イベントの名前を入力します。
6. トランザクションデータの固有の文字列をイベントとして指定するために使用する一致タイプを選択します。完全一致、ワイルドカード記号、および正規表現から選択できます。詳細については、「トランザクション定義(プロパティ) 『254ページ の"トランザクション定義（プロパティ）"参照 』」の一致タイプの説明を参照してください。
7. **[一致パターン]**列で、「スマートフォン」など、システムがイベントとして特定する項目を指定します。
8. 各イベントに対して上記の手順を繰り返します。

参照

ルールとイベントについて

トランザクション定義 『250ページ 』

トランザクションイベントに基づくアラームの作成

特定のトランザクションイベントが発生するたびに XProtect Smart Client オペレータに通知するには、まず、Management Application でトランザクションアラームを作成する必要があります。アラームは XProtect Smart Client の**[アラームマネージャ]**タブに表示され、オペレータはイベントを調査し、必要に応じてアクションを実行できます。

手順：

1. Management Application のナビゲーションペインで**[アラーム]**を展開します。

2. **[アラーム定義]**ノードを右クリックし、**[新規追加...]**をクリックします。**[プロパティ]**ペインの設定がアクティブになります。
3. **[説明]**フィールドにアラームの名前と、必要に応じて XProtect Smart Client オペレータが実行するアクションの手順も入力します。
4. **[トランザクションイベント]**ドロップダウンメニューで、**[トランザクションイベント]**を選択します。
5. **[トランザクションイベント]**の下のドロップダウンメニューで、特定のイベントを選択します。
6. **[ソース]**フィールドで**[選択...]**ボタンをクリックします。ポップアップウィンドウが表示されます。
7. **[サーバー]**タブをクリックし、トランザクションソースを選択します。
8. 追加の設定を指定します。詳細については、「アラーム定義」を参照してください。

参照

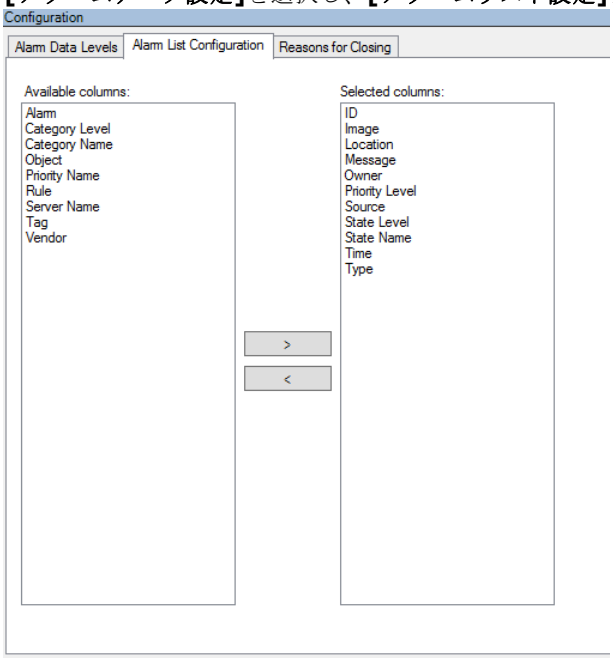
トランザクションイベントの定義 『256ページ 』

トランザクションイベントまたはアラームのフィルタリングを有効にする

XProtect Smart Client オペレータがトランザクションによってイベントまたはアラームをフィルタリングするできるようにする場合は、まず、Management Application の**[タイプ]**フィールドを有効にする必要があります。有効にすると、フィールドは、XProtect Smart Client の**[アラームマネージャ]**タブのフィルタセクションで使用できます。

手順：

1. Management Application のナビゲーションペインで**[アラーム]**を展開します。
2. **[アラームデータ設定]**を選択し、**[アラームリスト設定]**タブをクリックします。



3. **[使用可能な列]**セクションで、**[タイプ]**フィールドを選択します。
4. フィールドを**[選択した列]**に追加します。

5. 変更を保存します。このフィールドは、XProtect Smart Client でのみ使用できます。

トランザクション設定の維持

このセクションでは、トランザクションソースを編集、無効化、および削除する方法について説明します。

トランザクションソース設定の編集

トランザクションソースを追加した後は、名前を変更するか、別のトランザクション定義を選択できます。選択したコネクタによっては、接続した TCP サーバーのホスト名とポート番号など、その他の設定も修正できる場合があります。また、トランザクションソースを無効にすることもできます。これにより、トランザクションソースからイベントサーバーへのトランザクションデータのフローが中断されます。

コネクタを選択すると、変更できません。

手順：

1. Management Application のナビゲーションペインで**[トランザクト]**を展開します。
2. **トランザクションソース**を選択します。
3. Right-click the transaction source and select Properties.
4. 必要な変更を行い、保存します。詳細については、「トランザクションソース(プロパティ) 『252ページ 』」を参照してください。

参照

トランザクションソースの追加(ウィザード) 『252ページ 』

トランザクションソースを無効にする 『259ページ 』

トランザクションソースを無効にする

ATM が一時的に故障している場合や、登録されたキャッシュレジスターが無効な場合などに、トランザクションソースを無効にできます。イベントサーバーへのトランザクションデータのフローは中断されます。

手順：

1. Management Application のナビゲーションペインで**[トランザクト]**を展開します。
2. **トランザクションソース**を選択します。
3. Right-click the transaction source and select Properties.
4. **[有効]**チェックボックスをオフにして、変更を保存します。トランザクションソースが無効になります。

参照

トランザクションソースの追加(ウィザード) 『252ページ 』

トランザクションソースを削除 『260ページ 』

トランザクションソースを削除

追加したトランザクションソースを削除できます。そのソースから保存されたトランザクションデータはイベントサーバーから削除されます。

代替方法として、トランザクションソースを無効にし、保存されたトランザクションデータが削除されないように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。

手順：

1. Management Application のナビゲーションペインで**[トランザクト]**を展開します。
2. **トランザクションソース**を選択します。
3. **[トランザクションソース]**項目をクリックします。削除するソースを右クリックします。
4. **[削除]**を選択します。ダイアログボックスが表示されます。
5. **[OK]**をクリックして、トランザクションソースを削除することを確認します。

参照

トランザクションソースの追加(ウィザード) 『252ページ 』

XProtect Transact 構成の確認

XProtect Transact とコンポーネントの構成が完了したら、XProtect Smart Client で想定されるとおりに Transact が動作することをテストできます。

1. すべての必要なトランザクションソースが Management Application で正しく追加されたことを確認します。
    1. XProtect Smart Client を開き、**[トランザクト]**タブをクリックします。
    2. **[すべてのソース]**ドロップダウンメニューをクリックし、すべてのトランザクションソースが表示されることを確認します。
2. トランザクション定義が Management Application で正しく構成されたことを確認します。正しく構成されている場合は、トランザクションごとに 1 つの受信があり、正しく改行されます。
    1. XProtect Smart Client を開き、**[トランザクト]**タブをクリックします。
    2. アクティブなトランザクションソースを選択し、  をクリックします。今日のトランザクション行が表示されます。
    3. 行をクリックすると、関連付けられた受信と動画の録画が表示されます。
3. トランザクションイベントが正しく構成されていることを確認します。
    1. キャッシュレジスターなどの接続されたトランザクションソースで購入および登録された可能性が高い項目など、Management Application でトランザクションテストイベントを定義します。
    2. イベントが発生したら、XProtect Smart Client を開き、**[アラームマネージャ]**タブをクリックします。
    3. アラームリストを開き、**[イベント]**を選択します。最新のイベントは、一覧の一番上に表示されます。作成したテストイベントは一覧に表示されます。

オプション

自動デバイス検出について

※本機は、自動デバイス検出には対応していません。

自動デバイス検出により、ネットワークへ接続したハードウェアデバイスを、直ちにかつ自動的にシステムへ追加することができます。自動デバイス検出を有効にすると、システムはユーザーによる操作を必要とせず自動的にハードウェアデバイスを設定します。自動インストールが完了したハードウェアデバイスは、すぐに XProtect Smart Client でアクセス可能になります。

注意：

- すべてのハードウェアデバイスが、自動デバイス検出をサポートしているわけではありません。
- ハードウェアデバイスの自動デバイス検出への応答は異なります。システムは、一部のハードウェアデバイス（Axis モデル P3301 および P3304 など）は自動的にシステムに追加できますが、他のベンダーの一部のデバイス（ソニーのモデル SNC-EB520、EM520、E521 など）では、システムに自動的に追加されるためにカメラを一度オフにして、再度オンにする必要があります。
- システムがオンラインではない場合、必ず、ハードウェアデバイスライセンスをオフラインで認証してください。

デフォルトのファイルパスの変更

※本機は、デフォルトのファイルパスの変更には対応していません。

デフォルトのファイルパスを変更するには：

1. 設定パスを変更したい場合は、すべてのサービスを停止します。デフォルトの録画やアーカイブ パスを変更する場合は、このステップは不要です。
2. **オプション > デフォルトのファイルパス**へ移動します。
3. これで、必要なパスが上書きされます。あるいは、フィールドの横にある参照ボタンをクリックして、場所を参照することも可能です。デフォルトの録画パスについては、**ローカル**ドライブのフォルダへのパスしか指定できません。ネットワークドライブを使用している場合、ネットワークドライブが使用不能になると、録画は保存できません。

   デフォルトの録画やアーカイブのパスを変更し、古い場所に既存の録画ある場合、録画を新しい場所へ移動するか、古い場所に残すか、あるいは削除するかを選択する必要があります。Milestone は録画を新しい場所に移動することをお勧めします。
4. 変更を確認したら、すべてのサービスを再起動します。

カスタマーダッシュボードについて

※本機は、カスタマーダッシュボードには対応していません。

Customer Dashboard 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、起こり得る技術的問題（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 Customer Dashboard 設定を変更できます。

設定

一般

一般設定で、Management Application の一般的な動作や外観に影響する設定の数を変更することができます。

カスタマーダッシュボード

※本機は、カスタマーダッシュボードには対応していません。

システムがシステム情報をカスタマーダッシュボード 『261ページ の"カスタマーダッシュボードについて"参照 』に送信する必要がある場合に選択します。

システムモード

重要：保存後、新しい設定をただちに有効にすることに確信がある場合以外は、システムモードは変更**しない**でください。

システムに記録を保存しているある時点で、記録保存用のストレージが満杯になることがあります。システムには、こうした状況に異なる対応を示す 2 つのシステムモード、**クラシックモード**または**エビデンス収集モード**があります。

※本機は、エビデンス収集モードには対応していません。

- **クラシック**モードでは、新しい記録スペースを作るために、システムは最も古い記録を自動的に削除します。これは、以前のバージョンのシステムで、今まで保存された記録を処理していたのと同じ方法です。Management ApplicationManagement Application でハードウェアデバイスを削除すると、関連するデバイスからの記録もストレージから削除されます。XProtect Smart Client で削除した記録は、ストレージから削除されるので、再度再生することはできません。
- **エビデンス収集**モードは、ストレージの容量が満杯になると、システムが記録を停止することを意味します。すべての古い記録はストレージに保存され、システムは新しい記録を保存しません。これによって、エビデンスとして録画されたビデオは決して自動的に削除されることがなく、システムの設定を変更するか、ストレージから手動で削除するまで、ハードディスクに残ります。同様に、Management Application からハードウェアデバイスを削除しても、そのデバイスの記録はストレージに残ります。Management Application でデバイスを削除しても、XProtect Smart Client で記録を再生することができます。

概要：

	クラシックモード	エビデンス収集モード
ストレージが記録で満杯になった場合	システムは、最も古い記録を削除して、新しい記録スペースを作ります。	システムは、新しい記録の保存を停止し、最も古い記録は保持されます。
デバイスを削除した場合 Management Application	システムは、削除されたデバイスの記録をすべて削除します。	システムは、削除されたデバイスの記録をすべて保持します。

	クラシックモード	エビデンス収集モード
XProtect Smart Client で再生	Management Application からデバイスを削除すると、削除したデバイスの記録をシステムが削除するため、XProtect Smart Client では再生できなくなります。	Management ApplicationManagement Application からデバイスを削除しても、システムは記録を保持しているため、引き続き XProtect Smart Client で再生できます。
保持期間	記録の保持期間を設定し、カスタマイズすることができます。	システムは記録を決して削除しないので、記録に対して保持期間を設定することはできません。

システムでの必要性に適したシステムモードを選びます。ユーザーの大半は、最新の記録がストレージで使用できることが必要なので、**クラシック**モードを選ぶ必要があります。**エビデンス**モードは、代替的な方法であり、録画したすべてのビデオがエビデンスであると考えられ、ストレージに残す必要がある場合に適しています。

重要：システムを試用版モードで実行している場合、[**クラシック**]モードだけが使用できます。

重要： どの以前のバージョンのシステムからアップグレードした場合、システムでは**クラシックモード**がデフォルトの選択となります。**エビデンスモード**を使用するには、選択を手動で変更する必要があります。

言語

MA>は、複数の言語で使用できます。言語のリストで、使用したい言語を選択します。Management Application を再起動すると、言語の変更が反映されます。

ハードウェアデバイスの接続

自動デバイス検出

※本機は、自動デバイス検出には対応していません。

自動デバイス検出 『261ページ の"自動デバイス検出について"参照 』は、システムのデフォルトではオフになっています。この機能を有効にするには、チェックボックスを選択します。

検出されたカメラがデフォルトのユーザー名やパスワード以外に別のユーザー名やパスワードを使用する必要がある場合は、**カメラのデフォルトのユーザー名とパスワードに加え、次の認証資格情報を使用する**チェックボックスを選択して、関連する資格情報を入力します。

すべてのデバイスが、自動デバイス検出をサポートしているわけではありません。システムがデバイスを検出せず、システムに追加されない場合、デバイスを手動で追加する必要があります。

接続されたハードウェアデバイスでの時刻の同期

接続されたハードウェアデバイスとシステムのタイムスタンプが同じであることを保証するには、時刻サーバー『15ページ の"タイムサーバーについて"参照 』の使用を有効にします。ハードウェアデバイスとシステムの時刻が同期されていることを保証する時刻サーバーに対して、ハードウェアデバイスがリンクアップしていない場合は、システムがハードウェアデバイスからの録画をすべて一緒に停止するリスクがあります。

設定	詳細
時刻サーバーとしての録画サーバーの使用（推奨）	システムのソフトウェアの以前のインストールからアップグレードした場合のデフォルトシステム設定。 録画サーバーを使用して、ハードウェアデバイスとシステム間で時刻を同期します。 Milestone は、この設定を使用することをお勧めします。
このネットワーク時刻プロトコル（NTP）サーバーを使用する	録画サーバーではなく、時刻同期用に NTP サーバーを使用します。 使用するには、NTP サーバーの正確なアドレスを入力する必要があります。Milestone は、上級者のシステム管理者のみがこの設定を使用することをお勧めします。
接続されたハードウェアデバイスでの時刻を同期しない	システムのソフトウェアの以前のインストールからアップグレードした場合のデフォルト設定。 ハードウェアデバイスとシステム間で時刻同期を実行しない場合は、この設定を使用します。 システムがハードウェアデバイスとシステム間で一貫した時刻を検出した場合は、ハードウェアデバイスは録画を停止することがあります。

IP アドレス割り当て設定

※本機は、XProtect 標準の IP アドレスの割り当て設定には対応していません。

ネットワークに接続するときに IP アドレスをハードウェアデバイスに割り当てるための 3 つの設定があります。各設定には固有の利点と問題点があります。DHCP サーバーの使用をサポートしていないカメラがあることにご注意ください。

設定	詳細	利点	問題点
IP アドレスを接続されたデバイスに割り当てるための DHCP サーバーの使用	動的ホスト構成プロトコル（DHCP）サーバーを使用して、システムに接続するデバイスに自動的に IP アドレスを割り当てます。 DHCP サーバーを使用しない場合は、デバイスはあらかじめ割り当てられた IP アドレスを保持するか、動作しない可能性がある自己構成された IP アドレスを使用します。	DHCP サーバーは使用可能な IP アドレスを追跡し、ネットワークに追加されたときにデバイスに追加します。 再構成せずに、ネットワーク間でデバイスを移動できます。 これはシステムのソフトウェアの以前のインストールからアップグレードした場合のデフォルトシステム設定です。	デバイスは IP アドレスを変更できるため、構成の IP アドレスは一致しなくなります。

設定	詳細	利点	問題点
デバイスを接続するときに、IP アドレスを割り当てないでください。	IP アドレスは、システムに接続されたデバイスに割り当てられません。デバイスは現在の設定を保持します。たとえば、固定 IP アドレスまたは DHCP で割り当てられた IP アドレスがあります。	IP アドレスの割り当てに関するあらゆることをご自分で制御してください。 これはシステムのソフトウェアの以前のインストールからアップグレードした場合のデフォルトシステム設定です。	使用可能な IP アドレスを自分で追跡する必要があります。
この範囲から固定 IP アドレスを接続されたデバイスに割り当てる：	指定された範囲の固定 IP アドレスは、システムに追加された各個別のデバイスに割り当てられます。	割り当てられた IP アドレスは変更されません。	別のネットワークに移動する前に、デバイスを再構成する必要があるため、すべてのデバイスを再構成してネットワークを変更する必要があります。

動的ホスト構成プロトコル（DHCP）サーバーは、動的にネットワーク構成パラメータを配布するために IP ネットワークで使用される標準ネットワークプロトコルです。DHCP では、デバイスは DHCP サーバーから自動的に IP アドレスとネットワークパラメータを要求します。DHCP サーバーの使用により、ネットワーク管理者またはユーザーがこのような設定を手動で構成する必要性が減ります。

ユーザーインターフェース

Management Application の動作方法を変更することができます。

カメラプレビュー	Management Application でカメラをプレビューするときにライブビデオまたはスナップショットを表示するか、何も表示しないかを指定します。
動作設定	自分または他の Management Application ユーザーが実行するさまざまなアクションに対して Management Application が動作する方法を指定します。 Management Application はさまざまなアクションを確認するように要求します。これが不要であると思う場合、Management Application の動作を変更して、確認を求めないようにできます。 変更できるアクションの例： • ハードウェアデバイスを削除する場合に、Management Application にハードウェアデバイスの削除を確認させるか、確認なしでハードウェアデバイスを削除できるようにすることができます。 • 使用しているシステムに応じて、システムで使用できるカメラ数には制限があります。許可されるカメラの数を超えて、カメラを追加しようとした場合にシステムに警告させるように選択できます。 • カメラをプレビューする際にライブビデオを表示するか、あるいはスナップショットを表示したり、カメラのプレビューを行わないようにできます。

デフォルトの復元の設定	すべての動作設定をデフォルト値に復元する場合は、このボタンをクリックします。

デフォルトのファイルパス

※本機は、デフォルトのファイルパスには対応していません。

システムでは、多数のデフォルトファイルパスを使用します。必要に応じて、これらのパスを変更できます。

新しいカメラのデフォルト録画パス	追加するすべての新しいカメラは、デフォルトでは、録画の保存でこのパスを使用します。 必要であれば、各カメラの録画パスを、各カメラの個別の設定 『94ページの"録画およびアーカイブパス"参照 』の一部として変更できますが、追加するすべての新しいカメラが選択したパスを使用するようにしたい場合は、デフォルトの録画パスを変更することもできます。
新しいカメラのデフォルトアーカイブパス	追加するすべての新しいカメラは、デフォルトでは、アーカイブ 『124ページ の"アーカイブについて"参照 』でこのパスを使用します。 必要であれば、各カメラのアーカイブパスを、各カメラの個別の設定の一部として変更できますが、追加するすべての新しいカメラが選択したパスを使用するようにしたい場合は、デフォルトの録画パスを変更することもできます。アーカイブでダイナミックパスを選択 『76ページ の"ダイナミックパスの選択（プロパティ）"参照 』している場合、カメラ固有のアーカイブパスは関係しないことに注意してください。
設定パス	システム設定の保存に使用するデフォルトパスです。

アクセスコントロール設定

※本機は、アクセスコントロール設定には対応していません。

XProtect Access を使用する場合、XProtect VMS 内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。

名前	説明
開発プロパティパネルを表示する	選択すると、開発者情報がアクセスコントロールのプロパティの下に表示されます。 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。

オーディオ・レコーディング（音声記録）

新しいカメラをシステムに追加する際、既定の音声記録を特定して下さい。

決して	システムは、貴方のカメラから決して音声を記録しません。

決して	システムは、貴方のカメラから決して音声を記録しません。
ビデオを記録する場合だけ	貴方のシステムがビデオを記録する際にだけ、貴方のカメラの音声を記録します
常に	このシステムは、貴方のカメラの音声を常に記録します。

後で、各カメラの設定を個別に変更できます。

アナリティックイベント（プロパティ）

※本機は、アナリティックイベントには対応していません。

アナリティックイベントでは、以下を指定できます。

デバイスが有効	アナリティックイベント機能を有効にしてください。
ポート	このサービスで使用するポートを指定します。デフォルトポートは 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、これらの VCA ツールプロバイダも各ポート番号を変更するようにしてください。
次によって許可されるイベント： **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使用可能か、またはリストにある IP アドレス/ホスト名からのイベントのみが許可されるかを指定できます。 **アドレス**リストで、このサービスに認識して欲しい信頼できる IP アドレス/ホスト名のリストを指定できます。このリストは、特定の IP アドレス/ホスト名からのイベントだけが許可されるように受信データをフィルタリングするために使用します。 リストでは、ドメインネームシステム（DNS）と IPv4 アドレス形式の両方を使用できます。 リストにアドレスを追加する方法は 2 種類あります。 • 手動 : アドレスリストに必要な 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。 • 外部リストをインポート：以下を参照してください。
インポート	**インポート...**ボタンをクリックして、必要なアドレスの外部リストを参照します。外部リストをインポートするには、.txt ファイル形式でリストを保存します。各 IP アドレスまたはホスト名はファイルの各行に表示される必要があります。

アラームおよびイベント

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。詳細については、製品比較チャート『12ページ 』を参照してください。

終了したアラームの保持期間	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。 通常、この値は容量要件を低く抑えるために低い値に設定されていますが、サーバー領域に応じて最大 99999 日までの数値を定義できます。
他のすべてのアラームの保持期間	**新規**、**進行中**、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。
ログの保持期間	イベントサーバーログの保持日数を指定します。ログの保持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	イベントサーバーの通信の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**フィールドに指定する日数の間保持されます。
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。これには以下の 2 つの方法があります。 • イベントグループ全体の保持期間を指定できます。**グループをフォローする**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。 • イベントグループに値を設定した場合でも、個々のイベントタイプについて保持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。 **外部イベント**グループには、カスタムイベント、ジェネリックイベント、および入力イベントの各タイプがありますが、これらのタイプに個別に保持期間を設定することはできません。

重要：アラームは多くの場合、ビデオ録画と関連付けられています。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、関連するビデオ録画は、ユーザーが表示したいときに関連する監視システムサーバーからフェッチできます。したがって、すべてのアラームからビデオ録画にアクセスできることが不可欠であり、関連カメラからのビデオ録画が、イベントサーバーにアラームを保存する期間以上、関連する監査システムサーバーに保存されるようにする必要があります。

システムのメンテナンス

バックアップおよび復元の設定

設定のバックアップおよび復元について

Milestone では、障害時の復旧手段として、使用しているシステム設定（カメラ、スケジュール、ビューなど）のバックアップを定期的に取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。幸い、1 分程度で既存の設定をバックアップできます。

システム設定のバックアップ

※本機は、システム設定のバックアップには対応していません。

以下では、Milestone が、すべての対応オペレーティングシステムで実行中のサーバーのシステムデフォルトの設定パス『266ページ の"デフォルトのファイルパス"参照 』（**C:¥Program Data¥Milestone¥Milestone Surveillance**）をユーザーが変更していないことを前提としています。デフォルトの設定パスを変更した場合、以下に説明する方法を使用するとき、実施した変更を考慮する必要があります。

ここで説明するバックアップは、監視システムのセットアップ全体のバックアップです（ログファイル、イベントおよびの設定、復元ポイント、ビューグループならびに Management Application および XProtect Smart Client の設定を含む）。あるいは、設定をバックアップとしてエクスポート 『273ページ の"Management Application 設定のエクスポートとインポート"参照 』することも可能ですが、これは Management Application の設定に限られます。

バックアップするには：

1. フォルダ **C:¥Program Data¥Milestone¥Milestone Surveillance** とそのコンテンツすべてをコピーします。
2. **C:¥Program Files¥Milestone¥Milestone Surveillance¥devices** フォルダを開き、**devices.ini** ファイルが存在することを確認します。ファイルが存在する場合、これをコピーします。特定のタイプのカメラのビデオプロパティを設定している場合、このファイルが存在します。このようなカメラでプロパティを変更すると、カメラ自体ではなくファイルに保存されます。
3. コピーをサーバーから離れたところに保管して、サーバーが損傷を受けたり、盗難やその他の影響を受けたりした場合に喪失しないようにします。

バックアップは、使用しているシステム設定の、バックアップ時のスナップショットです。後で設定を変更した場合、手元にあるバックアップは、最も新しい変更を反映しなくなります。このため、使用しているシステム設定のバックアップを定期的に行います。説明に従って設定をバックアップする場合、バックアップには復元ポイントが含まれます。これにより、バックアップした設定を復元するだけでなく、必要に応じてその設定の前のポイントまで戻ることができます。

システム設定の復元

※本機は、システム設定の復元には対応していません。

1. サポート対象オペレーティングシステムが実行されているサーバーでシステムを使用する場合、バックアップされた **Milestone Surveillance** フォルダのコンテンツを **C:¥Program Data¥Milestone¥Milestone Surveillance** にコピーします。

2. **devices.ini** ファイルのバックアップを取った場合、そのファイルを **C:¥Program Files¥Milestone¥Milestone Surveillance¥devices** にコピーします。

アラームおよびマップ設定のバックアップと復元

※本機は、アラームおよびマップ設定のバックアップと復元には対応していません。

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、製品比較チャート『12ページ 』を参照してください。

アラームおよびマップ設定を定期的にバックアップすることが重要です。これを行うには、アラームおよびマップ設定、ならびにアラームのデータを保存している Microsoft® SQL Server Express データベースを取り扱うイベントサーバーをバックアップします。この操作により、発生する可能性がある障害時の復旧手段として、アラームおよびマップ設定を復元することができます。また、バックアップには、 SQL Server Express データベースのトランザクションログをフラッシュするという追加の利点もあります。

アラームおよびマップ設定をバックアップ・復元する場合は、必ず以下の順番で実行してください。

前提条件

- **SQL Server Express でアラーム設定データベースをバックアップまたは復元する場合、SQL Server Express データベース**の管理者権限が必要です。バックアップまたは復元を完了した後は、SQL Server Express データベースのデータベース所有者権限だけで十分です。

- **Microsoft® SQL Server Management Studio Express**、Microsoft Web サイト『http://www.microsoft.com/downloads』から無料でダウンロードできるツール。SQL Server Express データベースを管理するための多数の機能があり、使いやすいバックアップおよび復元機能が含まれます。既存の監視サーバーおよび将来の監視システムサーバーとなりうるサーバーに、ツールをダウンロードしてインストールします（バックアップおよび復元で必要になります）。

手順 1：Event Server サービスの停止

設定の変更が行われないように、Event Server サービスを停止します。

1. 監視システムサーバーで、**スタート > コントロールパネル > 管理ツール > サービス**の順にクリックします。

2. イベントサーバーを右クリックして、**停止**をクリックします。

これは、バックアップを作成した時点から、復元する時点までの間に行われたアラーム設定が失われるため、重要な手順となっています。バックアップ後に変更を行った場合は、新しいバックアップを作成する必要があります。Event Server サービスが停止した状態ではシステムはアラームを生成しません。SQL データベースのバックアップが完了した後、必ずサービスを再起動する必要があります。

手順 2：SQL Server Express データベースへのアラームデータのバックアップ

SQL Server Management Studio Express がない場合は、Microsoft Web サイト『http://www.microsoft.com/downloads』から無料でダウンロードできます。

1. Windows の**スタート**メニューで、**すべてのプログラム > Microsoft SQL Server 2008 > SQL Server Management Studio Express** の順に選択して、Microsoft SQL Server Management Studio Express を開きます。

2. ツールが開くと、サーバーへ接続するように求められます。必要な SQL Server の名前を指定して、管理者ユーザーの資格情報で接続します。SQL server の名前を入力する必要はありません。サーバー名フィールド内をクリックして、**<詳細を参照...>**を選択すると、リストから SQL Server を選択できます。
3. 接続すると、ウィンドウの左側にある**オブジェクトエクスプローラ**にツリー構造が表示されます。SQL Server の項目を展開し、次にアラーム設定全体が含まれている**データベース**の項目を展開します。
4. **VIDEOOSDB** データベースを右クリックし、**タスク > バックアップ...**の順に選択します。
5. **データベースのバックアップ**ダイアログの**一般**ページで、以下を行います。
   - **ソース**で、選択したデータベースが **VIDEOOSDB** であり、そのバックアップのタイプが**フル**であることを確認します。
   - **保存先**で、バックアップの保存先パスは、自動的に推奨のパスが設定されます。そのパスで良いかどうか確認します。そのパス以外を設定したい場合、推奨されているパスを削除し、選択した別のパスを入力します。
6. **データベースのバックアップ**ダイアログの**オプション**ページの**信頼性**で、**終了時にバックアップの確認**および**メディアに書き込む前のチェックサムの実行**を選択します。
7. **OK** をクリックすると、バックアップが始まります。バックアップが完了すると、確認が表示されます。
8. Microsoft SQL Server Management Studio Express を終了します。

手順 3：システムの再インストール

監視ソフトウェアは、マウントしたドライブにはインストールしないでください。マウントしたドライブとは、ドライブ文字の代わりにラベルまたは名前が付いている、NTFS（NT ファイルシステム）ボリュームの空のフォルダにマップされたドライブです。マウントしたドライブを使用すると、重要なシステム機能が想定どおりに作動しないことがあります。たとえば、システムがディスクの空き容量を超えて実行されても、警告が表示されません。

はじめに：既存の監視ソフトウェアをすべて停止します。

1. インストールファイルを実行します。セキュリティ設定によっては、1 つまたは複数のセキュリティ警告メッセージが表示される場合があります。警告が表示された場合は、**実行**ボタンをクリックします。
2. インストールウィザードが起動したら、インストーラの言語を選択して**続行**をクリックします。
3. システムの評価版のインストールを選択するか、ソフトウェアライセンスファイルの場所を指定します。
4. 使用許諾契約を読んで同意し、Milestone データ収集プログラムに参加するかどうかを指定します。
5. **標準**または**カスタム**インストールを選択します。**カスタム**インストールを選択した場合、アプリケーション言語、インストールする機能、およびインストール場所を選択できます。インストールウィザードが完了するのを待ちます。

システムの構成を開始できます。「Management Application でのシステムの構成 『39ページ の "Management Application のシステムの構成"参照 』」を参照してください。

手順 4：SQL Server Express データベースのアラームデータの復元

幸いにも大半のユーザーは、バックアップされたアラームデータを復元する必要がありませんが、必要になった場合、次の手順を実行します。

1. Windows のスタートメニューで、Microsoft SQL Server Management Studio Express を開きます。

2. サーバーに接続します。必要な SQL Server の名前を指定して、データベースを作成した時のユーザーアカウントで接続します。

3. 左側の**オブジェクトエクスプローラ**で、**SQL Server > データベース**を展開し、**VIDEOOSDB** データベースを右クリックしてから、**タスク > 復元 > データベース...**の順に選択します。

4. **データベースの復元**ダイアログの**一般**ページの**復元のソースで、デバイスから**を選択して、フィールドの右にある**<詳細を参照...>**をクリックします。**バックアップの指定**ダイアログで、**ファイル**が**バックアップメディア**のリストで選択されていることを確認します。**追加をクリックします。**

5. **バックアップファイルを探す**ダイアログで、バックアップファイル **VIDEOOSDB.bak** を探して、選択します。次に **OK** をクリックします。これで、バックアップファイルへのパスは、**バックアップの指定**ダイアログに一覧表示されています。

6. これで、**データベースの復元**ダイアログの**一般**ページに戻ると、**復元するバックアップの選択**の下にバックアップが一覧表示されています。**復元**列のチェックボックスを選択して、バックアップが選択されていることを確認します。

7. ここで、**データベースの復元**ダイアログの**オプション**ページに移動し、**既存のデータベースを上書きする**を選択します。他のオプションはそのままにして、**OK** をクリックすると、復元が始まります。復元が完了すると、確認が表示されます。

8. Microsoft SQL Server Management Studio Express を終了します。

注意：データベースが使用中であることを知らせるエラーメッセージが表示される場合は、Microsoft SQL Server Management Studio Express を完全に終了させてから、手順 1～8 を繰り返してください。

手順 5：Event Server サービスの再起動

復元プロセス中は、Event Server サービスが停止して、完了するまで設定が変更されることを防ぎます。サービスを再起動することを忘れないでください。

1. 監視システムサーバーで、**スタート > コントロールパネル > 管理ツール > サービス**の順にクリックします。

2. イベントサーバーを右クリックして、**開始**をクリックします。

SQL Server Express トランザクションログと、それをフラッシュする理由について

システムのアラームデータの変更が発生するたびに、SQL Server はトランザクションログに変更を記録します。トランザクションログは基本的に、SQL Server Express データベースへの変更をロールバックして取り消すことができる機能です。SQL Server はデフォルトで、無期限にトランザクションログを保存するので、トランザクションログは時間の経過とともに、エントリが増え続けます。

SQL Server の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あり、トランザクションログが増え続けると、Windows が正しく実行できなくなります。したがって、SQL Server のトランザクションログを時々フラッシュすることをお勧めします。フラッシュすること自体で、トランザクションファイルが小さくなることはありませんが、極端に大きくなることがなくなります。一方、システムでは、SQL Server のトランザクションログは特定の間隔で自動的にフラッシュされません。これは、ユーザーによってニーズが異なるからです。あるユーザーは非常に長い期間、変更を元に戻すことができる状態を保つことを望みますが、別のユーザーにはこのようなニーズはありません。

SQL Server 自体で複数の作業を行って、トランザクションログを切り取り、縮小したりして、トランザクションログのログのサイズが大きくならないように抑えることができます（このトピックについては、support.microsoft.com 『http://support.microsoft.com』へ移動し、SQL Server のトランザクションログを検索すると、多くの記事を確認することができます）。ただし、一般にシステムのデータベースをバックアッ

プする方が良い選択となります。SQL Server のトランザクションログがフラッシュされ、予期せぬ事態が発生した場合にシステムのアラームデータを復元できるようにするためです。

Management Application 設定のエクスポートとインポート

設定のバックアップを取るための安全な手段として、あるいは他の場所で類似の Management Application 設定を使用するためのコピーとして、Management Application の現在の設定をエクスポートすることができます。後から、以前にエクスポートした Management Application 設定をインポートすることができます。

バックアップとして Management Application 設定をエクスポート

このオプションでは、関連するすべての Management Application 設定ファイルが単一の.xml ファイルに結合され、その場所を指定できます。設定に保存していない変更がある場合、設定をエクスポートする際にこれらは自動的に保存されます。

1. **ファイル**メニューで、**設定のエクスポート - バックアップ**を選択します。
2. エクスポートした設定を保存したい場所を参照し、適切なファイル名を指定し、**保存**をクリックします。

同一バージョンの監視システムを他の場所でセットアップする場合は、設定を**バックアップ**としてエクスポート**しないでください**。このような操作により、同じデバイス情報が二度使用され、クライアントに以下のエラーメッセージが表示される原因となります。**2 台（以上）のカメラが同じ名前または ID を使用しているため、アプリケーションが起動できません。** 代わりに、設定を**コピー**としてエクスポートします。コピーとしてエクスポートする場合、たとえ新しいシステムが既存のシステムと同一であったとしても、エクスポートでは物理的に全く同じカメラなどを使用していないという事実が考慮されます。

この Management Application 設定のバックアップと、Milestone 監視フォルダで行ったシステム設定のバックアップでは、これら 2 つは別物であるため、違いがあることに注意してください。ここで説明しているバックアップは、Management Application の設定のバックアップに限定されます。Milestone 監視フォルダのバックアップを行った場合は、監視システムのセットアップ全体をバックアップします（ログファイル、イベントの設定、復元ポイント、ビューグループならびに Management Application および XProtect Smart Client の設定を含む）。

クローンとして Management Application 設定をエクスポート

このオプションでは、すべての関連する Management Application の設定ファイルが収集されます。GUID（Globally Unique IDentifiers、カメラなどの個々のシステムコンポーネントを識別するために使用される一意の 128 ビットの数値）はマークされ、後で置換されます。GUID は、特定のコンポーネント（カメラなど）を参照しているので、マークされて後で置換されます。類似のタイプのカメラを使用する新しい類似のシステムのセットアップで、コピーした設定を使用したい場合でも、新しいシステムはコピーされたシステムと全く同じ物理的なカメラは使用しません。後で新しいシステムでコピーされた設定を使用する場合、GUID は新しいシステムに固有のコンポーネントを表す GUID と置換されます。

置換用に GUID をマークした後、設定ファイルが単一の.xml ファイルに結合され、これを指定の場所に保存することができます。設定に保存していない変更がある場合、設定をエクスポートする際にこれらは自動的に保存されます。

1. **ファイル**メニューで、**設定のエクスポート - コピー**を選択します。
2. エクスポートした設定を保存したい場所を参照し、適切なファイル名を指定し、**保存**をクリックします。

以前にエクスポートされた Management Application 設定のインポート

Management Application の設定がバックアップとしてエクスポートされたか、コピーとしてエクスポートされたかに関わらず、同じインポート方法を使用します。

1. **ファイル**メニューで、**設定のインポート**を選択します。
2. 設定をインポートしたい場所を参照し、関連する設定ファイルを選択し、**開く**をクリックします。
3. 設定をインポートしようとしているシステムに、インポートされる設定に存在しないデバイス（例、カメラ）が含まれている場合にだけ関連します。影響を受けるデバイスからの録画の、削除または保持のいずれを希望するかが確認されます。録画を保持したい場合は、影響を受けるデバイスを再度システムに追加するまでは、それらの録画にはアクセスできないことに注意してください。必要なオプションを選択して、**OK** をクリックします。
4. **詳細設定 > サービス**を展開します。
5. Recording Server サービスおよび Image Server サービスのそれぞれに対して、**再起動**ボタンをクリックします。2 つのサービスを再起動すると、インポートされた Management Application の設定が適用されます。

復元ポイントからのシステム設定の復元

復元ポイントにより、以前の設定状態に戻すことができます。Management Application で設定の変更を適用するたびに、新しい復元ポイントが作成されます。

復元ポイントは、最新のものから 5 つ前までのものがすべて保存され、再度選択することができます。Management Application を起動するたび、および設定全体を保存するたびに、新しいセッションが開始します。最新の 5 つのセッションより古いセッションについては、各セッションの最後の復元ポイントだけが保存されます。**維持する古いセッションの数**フィールドで、古いセッションをいくつまで保存するかを管理できます。

復元ポイントから設定を復元するよう選択すると、選択した復元ポイントからの設定が適用され、サービスを再起動すると使用されます。

復元ポイントの作成後に新しいカメラやその他のデバイスを追加した場合、復元ポイントをロードするとそれらは失われます。これは、復元ポイントが作成された時点でシステムに存在していなかったためです。このようなケースでは、影響を受けるデバイスからの録画の処理方法を決定するよう通知が表示されます。

1. **ファイル**メニューで、**復元ポイントからの設定のロード...**を選択します。
2. **復元ポイント**ダイアログの左の部分で、該当する復元ポイントを選択します。
3. **復元ポイントのロード**ボタンをクリックします。
4. 選択した復元ポイントからの設定で、現在の設定を上書きしても構わない場合には、**OK** をクリックします。
5. 現在の設定に、選択した復元ポイントに存在しないカメラやその他のデバイスが含まれている場合のみ該当します。影響を受けるデバイスからの録画の、削除または保持のいずれを希望するかが確認されます。録画を保持する場合は、影響を受けるデバイスを再度システムに追加するまでは、それらの録画にはアクセスできないことに注意してください。関連するオプションを選択し、**OK** をクリックします。
6. 復元ポイントダイアログで **OK** をクリックします。
7. **詳細設定**を展開し、**サービス**を選択します。
8. Recording Server サービスおよび Image Server サービスのそれぞれに対して、**再起動**ボタンをクリックします。2 つのサービスを再起動すると、選択した復元ポイントからの設定が適用されます。

注意： 復元ポイントを選択する際に、ダイアログの該当する部分で選択した時点での設定状態に関する情報を確認できます。この情報は、最善の復元ポイントを選択するのに役立ちます。

設定に対する変更のインポート

設定に対する変更のインポートについて

設定に対する変更をインポートすることができます。これは、たとえばある店舗チェーンの各店舗で同じタイプのサーバー、ハードウェアデバイス、カメラを使用する場合など、多数の類似のシステムをインストールする場合に該当します。こうしたケースでは、既存の設定を他のインストール用のテンプレートとして使用することができます。

これらのインストールは完全に同一ではないため（ハードウェアデバイスやカメラは同じタイプであるが、物理的には同一ではないので、MAC アドレスが異なる）、変更を簡単にテンプレート設定にインポートできる方法が必要になります。ハードウェアデバイスやカメラに関する変更を、カンマ区切り値ファイル(CSV)としてインポートすることができます。

段階的なガイドについては設定に対する変更のインポート 『276ページ 』、CSV ファイルに含める必要があるフィールドについては、設定に対して変更をインポートするときの CSV ファイルの必須フィールドについて 『275ページ の"変更を構成にインポートするときに必要な CSV ファイルのフィールドについて"参照 』を参照してください。

変更をインポートする場合、ハードウェア検知も行われませんし、ソフトウェアもカメラのハードウェア機能を変更しません。たとえば、PTZ カメラを PTZ 以外のカメラに交換すると、ソフトウェアは引き続き交換されたカメラを PTZ カメラと表示します。

変更を構成にインポートするときに必要な CSV ファイルのフィールドについて

CSV ファイルには、ヘッダー行（以後の行にあるそれぞれの値が何に関するものであるかを決定する）が必要であり、以後の行にはそれぞれ 1 つのハードウェアデバイスに関する情報だけが含まれている必要があります。フィールド名は大文字と小文字を区別するため、以下のように正確にフィールドを記述したことを確認してください。

それぞれのハードウェアデバイスに対して、以下の情報が必要になります。

HardwareOldMacAddress	プロパティが変更されるデバイスを検出するために使用されます。これは必須フィールドであり、CSV ファイルの変更を構成にインポートするために入力する必要があります。
HardwareNewMacAddress	ハードウェアデバイスの新しい IP アドレス。
HardwareAddress	ハードウェアデバイスの IP アドレス。
HardwarePort	ハードウェアデバイスのポート。
HardwareUserName	ハードウェアデバイスの管理者アカウントのユーザー名。
HardwarePassword	ハードウェアデバイスの管理者アカウントのパスワード。
HardwareDriverID	カメラとサーバーがオフラインの場合：追加したいそれぞれのハードウェアデバイスについて、**HardwareDriverID** を指定します。 例：**ACTi ACD-2100 105** は、ACTi ACD-2100 ハードウェアデバイスを追加する際に、**105** を ID として使用する必要があることを示しています。

変更をインポートするときには、ハードウェアが検出されず、ハードウェア機能が変更されません。たとえば、PTZ 機能がないデバイスで PTZ デバイスを置換すると、新しいデバイスは PTZ デバイスとしてリスト表示されます。

以下は、CSV ファイルに存在する情報に適用されます。

- CSV ファイルの最初の行にはヘッダーが必要であり、以後の行にはそれぞれ 1 つのハードウェアデバイスに関する情報が含む必要があります。
- 区切り記号としてはカンマ、セミコロン、タブが使えますが、混在させることはできません。
- すべての行に有効な値が含まれる必要があります。カメラの名前、ユーザー名や類似のアイテムなどはすべて一意でなければなりません。また、以下の特殊文字が含まれないように注意してください。 **< > & ' " ¥ / : * ?| [ ]**
- 値の順番は固定ではなく、オプションのパラメータは完全に削除することもできます。

設定に対する変更のインポート

1. メニューバーで、**ファイル > 設定に対する変更のインポート...**の順に選択します。
2. CSV ファイルにリスト化されている新しいハードウェアデバイスやカメラがサーバーに接続されていて、使用できることを確認したい場合は、**オンライン検証**を選択します。
3. CSV ファイルにカーソルを合わせて、**ファイルからの設定のインポート**ボタンをクリックします。

設定に対する変更のインポートについて 『275ページ 』も参照してください。

用語集

A

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を作成またはカスタマイズするためのツールや構築ブロックのセット。

ATM

現金自動預払機 — 個人情報がコード化されたカードを使って、お金を引き出す機械。

AVI

ビデオでよく使用されるファイル形式。この形式のファイルには.avi というファイル拡張子が付いています。

C

Central

XProtect Central は、場所に関わらず、システムサーバーのステータスやアラームに関する完全な概要を提供します。

CSV

データをテーブル形式で保存するカンマ区切り値によるデータ形式。単純なファイルで、各行がテーブルの行を表し、カンマが列を定義します。たとえば、カメラに関するデータは.csv ファイルのカンマ区切り値として表示され、これをシステムにインポートできます。複数の類似のシステムを設定する場合、これは効率的な方法です。

D

DirectX

高度なマルチメディア機能を提供する Windows の拡張機能。

DNS

Domain Name System（ドメインネームシステム） — アルファベットによるホスト名（例、mycomputer）またはドメイン名（例、www.mydomain.com）および数字による IP アドレス（例、192.168.212.2）の間での変換を可能にするシステム。多くの人にとって、数字による IP アドレスより、アルファベットによる名前の方が覚えやすいようです。

DST

夏時間：夕方の日照時間を長く、朝の日照時間を短くするために、夏季の間は時計を進める制度。

F

FPS

秒当りのフレーム数 — 動画に含まれている情報量を示す測定単位です。各フレームは 1 つの静止画像を表しますが、数多くのフレームを連続して表示することで運動錯視を生じさせ、画像が動いているように見えます。FPS の値が高いほど、より滑らかな動きになります。ただし、FPS が高くなるとビデオを保存したときのファイルサイズも大きくなります。

G

GOP

画像グループ：個別のフレームをグループ化し、動画像のシーケンスを形成します。

GUID

グローバル一意識別子（Globally unique identifier） — 一意の 128 ビットの番号であり、Windows システムでコンポーネントを識別するために使用されます。

H

H.264

ビデオデータを圧縮および解凍する際の標準規格（コーデック）です。H.264 は、以前のコーデックより効率的にビデオを圧縮できるコーデックであり、

さまざまなネットワーク環境で使用できる柔軟性があります。

I

I/O

入力/出力：コンピュータとユーザー間での通信を意味します。入力とはシステムが受信する信号やデータであり、出力はシステムから送信される信号またはデータです。

Image Server

XProtect Smart Client でリモートユーザーがログインするために、システムへのアクセスを処理するサービスです。

Image Server サービスは、監視システムサーバーのバックグラウンドで動作するので、別個のハードウェアは必要としません。Image Server サービスは、システムの Management Application で設定されているので、個別には設定しません。

IPIX

panomorph 魚眼画像を作成、表示できるテクノロジーです。

I フレーム

イントラフレーム（intra-frame）の略語。デジタルビデオ圧縮の MPEG 規格で使用されます。I フレームは、指定された間隔で保存された 1 つのフレームです。I フレームはカメラのビュー全体を記録しますが、その後のフレーム（P 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、MPEG ファイルのサイズを大幅に縮小できます。I フレームはキーフレームと類似しています。

J

JPEG

（あるいは JPG）ジョイントフォトグラフィックエキスパートグループ（Joint Photographic Experts Group）は画像の不可逆圧縮方法で、幅広く使用されています。

L

LPR カメラライセンス

XProtect LPR で使用するカメラを設定する権限を付与するライセンス。

LPR 国モジュールのライセンス

XProtect LPR で使用できる異なる国または地域ライセンスプレート形式にアクセスできるライセンス。

M

MAC アドレス

メディアアクセスコントロールアドレス（Media Access Control address） — ネットワーク上の各デバイスを一意に識別する 12 文字の 16 進数です。

Matrix

分散表示用にリモートコンピュータでライブカメラの表示をコントロールできる機能。設定すると、XProtect Smart Client で Matrix トリガのライブビデオを表示できます。

Matrix 受信者

XProtect Smart Client ソフトウェアを搭載しており、そのため Matrix トリガのライブビデオを表示できるコンピュータ。

MJPEG

モーション JPEG（Motion JPEG） — 各フレームが個別に JPEG 画像に圧縮される圧縮ビデオ形式です。使用する方法は、MPEG で使用する I フレームに極めて似ていますが、フレーム間予測が使用されません。これにより、編集が簡単になり、モーションの量によらず、圧縮することができます。

MPEG

動画専門家集団（Moving Pictures Experts Group、MPEG）によって開発された、デジタルビデオの圧縮標準とファイル形式。MPEG 標準は不可逆圧縮を使用しており、フレーム間の変化だけを保存し、冗長な情報の多くを除去します。キーフレームでは指定された間隔で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、MPEG ファイルのサイズを大幅に縮小できます。

N

NTLM

Windows ネットワークでは、NT LAN Manager がネットワーク認証プロトコルです。

P

Panomorph

魚眼テクノロジー画像を作成・表示できるようなレンズの種類です。

PIN

個人識別番号（Personal Identification Number または Personal Identity Number） — ユーザーの識別や認証を行うために使用する数値です。

Ping

IP アドレスが利用できるかどうか決定するコンピュータネットワーク管理ユーティリティ。応答するかどうか見るために少量のデータを送ります。Ping（ピング）という用語は、ソナーの発する音に由来しています。Ping コマンドは、Windows のコマンドプロンプトを使用して送信します。

POS

（あるいは PoS）販売時点情報管理:たとえばレジなどの、販売が行われる具体的な場所。

PUK

パーソナルアンブロックキー（Personal Unblocking Key）または PIN アンロックキー（PIN Unlock Key） — SIM カード向けの特別なセキュリティ措置として使用される番号。

P フレーム

予測フレーム（Predictive Frame） — デジタルビデオ圧縮の MPEG 標準で、P フレームは I フレームと共に使用されます。I フレームはキーフレームとも呼ばれ、指定した間隔で保存される 1 つのフレームです。I フレームはカメラのビュー全体を記録しますが、その後のフレーム（P 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、MPEG ファイルのサイズを大幅に縮小できます。

R

Recording Server サービス

ビデオの録画や再生で、システムによって使用される Windows サービス（ユーザーインターフェースなし）。ビデオが監視システムに転送されるのは、Recording Server サービスが実行されている間だけです。

S

SCS

クライアントのコントロールを目的とする種類のスクリプトに使用されるファイル拡張子(.scs)です。

SDK

ソフトウェア開発キット（Software Development Kit） — 特定のプラットフォームを使用して、ソフトウェア開発者がアプリケーションを作成できるプログラミングパッケージ。

SIM

加入者識別モジュール（Subscriber Identity Module） — 携帯電話またはコンピュータに挿入される小さいカードに保存される回路または他のモバイル機器。SIM カードは、ユーザーを特定して、認証するのに用いられます。

SMTP

簡易メール転送プロトコル（Simple Mail Transfer Protocol） — メールサーバー間での E メールメッセージ送信の標準化されたプロトコルです。

T

TCP

通信制御プロトコル（Transmission Control Protocol） — ネットワーク上でデータパケットを送信する際に使用するプロトコル（標準）です。TCP は、多くの場合、別のプロトコルである IP (Internet Protocol)と組み合わせて使用されます。この組み合わせを TCP/IP と呼び、ネットワーク上の 2 つのポイント間でデータパケットを長時間にわたって送受信することができます。コンピュータとインターネ

ット上にある別のデバイスを接続するためにも使用します。

TCP/IP

通信制御プロトコル/インターネットプロトコル（Transmission Control Protocol/Internet Protocol）ー インターネットを含むネットワーク上でコンピュータと他のデバイスを接続する際に使用するプロトコル（標準）の組み合わせです。

Telnet

TCP/IP ネットワークで使用する端末エミュレーションプログラムです。Telnet を使用することで、ネットワークのコンピュータからサーバーに接続し、サーバーに直接入っているかのように、Telnet からコマンドを実行することができます。Windows には、Telnet で使用するクライアントが含まれています。

U

UDP

ユーザーデータグラムプロトコル ー ネットワークでデータパケットを送信するための無接続のプロトコルです。主に、メッセージのブロードキャストで使用します。UDP は、たとえば TCP プロトコルと比較してエラーリカバリ機能が少ない、極めて単純なプロトコルです。

UPS

UPS (無停電電源装置)は、電池駆動の第 2 電源として動作し、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。

V

VCA

ビデオコンテンツ分析(VCA)は、人間や車両の両方について、事前に指定したさまざまなタイプの動作を検出するシステムです。VCA ベースのシステムは、サードパーティ製ビデオコンテンツ分析を提供し、顔認識、先進モーション検知から、複雑な動作分析まで幅広い検知が可能です。VCA システムとその出力は、**アラーム**機能とシームレスに統合することができ、たとえばアラームのトリガなどで使用できます。VCA システムから発生するイベントはアナリティックイベントと呼ばれます。

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。

X

XProtect Transact

XProtect 監視システムへのアドオン。XProtect Transact は、時刻に紐付けした POS または ATM のトランザクションデータとビデオの証拠の組み合わせで、紛失や減少を防ぐのに役立ちます。

アクセスコントロールドアライセンス

XProtect Access でアクセスコントロール用のドアを設定する権限を付与するライセンス。

アクティベーションなしのデバイスの変更

手動ライセンス認証を実行する前に XProtect システムがオフラインの場合に、交換または追加できるハードウェアデバイス数。

アスペクト比

画像の縦横比。

アナリティック イベント

アナリティックイベントは、外部のサードパーティ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です。VCA ベースのシステムの例として、アクセスコントロールシステムが挙げられます。アナリティックイベントは、**アラーム**機能とシームレスに統合することが可能です。

イベントサーバー

すべてのシステムサーバーから受信するアラームデータやイベントを保存・処理するサーバーです。イベントサーバー機能により、強力なモニタリングが

可能になります。また、アラームやシステム内の技術的な問題について即時の概要表示が提供されます。

ウィザード

すべての関連するパラメータを確実に入力しながら、特定のタスクを迅速に実行することを支援するユーティリティです。たとえば、[モーション検知の調整]ウィザードは、重要なパラメータの設定を忘れることなく、システムのそれぞれのカメラのモーション検知を速やかに設定するのに役立ちます。

キーフレーム

デジタルビデオ圧縮の MPEG 標準で使用されます。キーフレームは指定間隔で保存される 1 つのフレームです。キーフレームはカメラのビュー全体を記録しますが、キーフレームに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、MPEG ファイルのサイズを大幅に縮小できます。

コーデック

エクスポートされた AVI ファイルなど、音声とビデオデータを圧縮および解凍する技術。よく使用されるコーデックとして、MPEG や Indeo があります。

サブネット

ネットワークの一部。ネットワークをサブネットに分けると、管理とセキュリティ上の理由で有利であり、場合によってはパフォーマンスが改善することもあります。TCP/IP ベースのネットワークで、サブネットは基本的にネットワークの一部であり、すべてのデバイスがその IP アドレスで同じ接頭辞を共有します。たとえば、123.123.123.xxx となり、ここで最初の 3 つの番号(123.123.123)が共有接頭辞です。ネットワーク管理者は、サブネットマスクを使用して、ネットワークをサブネットに分割します。

ジェネリックイベント

システムは、入力を TCP または UDP データパッケージの形式で受信および分析することができます。指定された基準に一致する場合、これをイベントの生成で使用できます。このようなイベントは、ジェネリックイベントと呼ばれます。

ソフトウェアライセンスコード (SLC)

ソフトウェアライセンスコード(SLC)は、監視システムソフトウェアを使用するために必要な製品の登録コードです。ソフトウェアライセンスファイルの名前は、ソフトウェアライセンスコード(SLC)に関連付けられています。システム管理者の責任を担当している場合を除き、SLC を扱う必要はありません。システム管理者は、ソフトウェアのインストールおよび登録中に SLC を使用します。

ソフトウェアライセンスファイル

システム用に付与されたすべての権限（基本ライセンスとその他のライセンス）を含むファイル。

ファイルの名前はソフトウェアライセンスコード（SLC）に関連付けられています。

デバイス

XProtect 監視システムで：録画サーバーに接続されているカメラ、ビデオエンコーダー、入力デバイス、出力デバイスなど。

デバイスライセンス

XProtect システムでカメラまたはエンコーダーを実行する権限を付与するライセンス。モバイルデバイスまたはタブレットでビデオプッシュ機能を使用する場合は、デバイスごとにデバイスライセンスが必要です。

デュアル ストリーム

一部のカメラは 2 つの独立したストリーム（録画サーバーへ送信可能）をサポートしています：一方はライブビュー用であり、他方は再生用です。これらのストリームは、それぞれ独立した解像度・エンコーディング・フレームレート設定を持っています。

ドライバー

デバイスの制御/通信で使用するプログラム。

トランザクションソースライセンス

カメラを ATM および POS に関連付け XProtect Transact 用に設定する権限を付与するライセンス。

ハードウェアデバイス

システムにデジタルカメラを追加する場合、カメラ自体だけを追加するのではなく、ハードウェアデバイスを追加します。ハードウェアデバイスには独自の IP アドレスやホスト名があります。システムは IP ベースであるため、主に IP アドレスやホスト名に基づいて装置が認識されます。

各ハードウェアデバイスには独自の IP アドレスやホスト名がありますが、1 つのハードウェアデバイスに複数のカメラ、マイクなどが付いている場合は、同じ IP アドレスやホスト名を共有していることになります。これは、ビデオエンコーダーデバイスに複数のカメラが付いている典型的なケースです。

1 つのハードウェアデバイスに複数のカメラ、マイク、類似のチャンネルなどが接続されていても、それらを個別に設定して使用することができます。

パンチルトズーム(PTZ)

PTZ（パン/チルト/ズーム）動きと柔軟性に優れたカメラです。

ビデオエンコーダ

多数の接続されているクライアントカメラからビデオストリームを流すことができる、通常はスタンドアロンのデバイス。ビデオエンコーダには、画像デジタイザが含まれており、アナログカメラをネットワークに接続できます。

ビデオサーバー

ビデオエンコーダの別名。

ビデオモーション検知(VMD)

ビデオモーション検知。一連の画像で、画像データや相違点を分析して、シーンのアクティビティを定義する方法。

ビュー

1 つまたは複数のカメラからのビデオ群で、XProtect Smart Client で表示します。ビューには、カメラからのビデオに加えて、HTML ページや静止画像などのその他のコンテンツが含まれる場合もあります。

プライバシーマスキング

カメラのビューの選択した領域を配信前に非表示にするかどうかを定義し、非表示にする場合はその方法を定義できる機能。たとえば、カメラがある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。

プリアラーム

プリアラーム画像は、選択したカメラでのみ使用可能な機能です。イベントが発生する直前の画像を、カメラからシステムへ E メールで送信することができます。

プリレコーディング

検出したモーションや指定されたイベントの前の期間からの録画を保存する機能。この機能は、システムサーバーにバッファされている受信ビデオに基づいており、モーションやイベントでトリガされる録画が必要になります。

たとえば、ドアが開いている間、ビデオを録画するよう定義した場合に、ドアを開ける直前に発生した状況を確認できるのが重要になる場合があります。

フレームレート

動画に含まれている情報量を示す測定単位であり、通常は FPS で測定します。

プレバッファ

プリレコーディングの説明を参照してください。

ポート

データトラフィックの論理的終点。ネットワークでは、データトラフィックの異なる種類ごとに異なるポートが使用されます。そのため、場合によっては、特定のデータ通信でどのポートを使用するかを指定する必要があります。ほとんどのポートは、通信に含まれるデータの種類に基づいて自動的に使用されます。TCP/IP ネットワークの場合、ポート番号は 0 から 65536 ですが、0 から 1024 までは特定用途のために予約されています。たとえば、ポート 80 は Web ページの表示に使用される HTTP トラフィック用です。

ポーリング

何かの状態を定期的にチェックすること。たとえば、入力がデバイスの特定の入力ポートで受信されたかどうかなど。このような状態をチェックするための定義済みの間隔を、しばしばポーリング頻度と呼んでいます。

ホスト

TCP/IP ネットワークに接続されているコンピュータ。ホストには専用の IP アドレスがありますが、ネットワーク設定によっては、**識別しやすくするためにホスト名**が付いている場合があります。

ポストレコーディング

モーションや指定されたイベントの後の期間から記録を保存できる機能。

システムサーバーにバッファされている受信ビデオに基づいて、モーションやイベントでトリガされる録画が必要になります。

たとえば、ゲートが開いている間、ビデオを録画するよう設定した場合に、ゲートが閉められた直後に発生した状況を確認できるのが重要になる場合があります。

ホットスポット

XProtect Smart Client で、拡大または高品質で表示されているビデオの特定の位置。

マスター/スレーブ

あるサーバー（マスターサーバー）が、他のサーバー（スレーブサーバー）より重要であるサーバーのセットアップ形態。システムでのマスター/スレーブ設定により、複数の監視システムサーバーを組み合わせて、使用できるカメラの数を単一のサーバーの許容最大数以上に拡大できます。

このような設定でも、クライアントの接点は、1 つだけに維持されます。クライアントは、マスターサーバーに接続されますが、スレーブサーバーのカメラや録画にも自動的にアクセスできます。

モニター

1) コンピュータの画面。2) 以前のバージョンの XProtect Corporate でビデオの録画や再生を行う際に使用するアプリケーション。モニターアプリケーションは現在は廃止されています。

漢字

画面自動切替

1 つのカメラ位置で複数のカメラからのビデオを次々に表示することができる機能です。必要なカメラと切り替えの間隔は、システム管理者が指定します。この画面自動切替機能は、XProtect Smart Client でのみ使用できます。

管理者

1) システム管理者。2) システムの以前のバージョンの場合：システム管理者が、監視システムサーバーを設定するために使用するメインのアプリケーション。現在は、Management Application と呼ばれます。

基本ライセンス

XProtect VMS 製品または XProtect アドオン製品のソフトウェアを使用する権限を付与するライセンス。

記録

IP ビデオ監視システムの場合、記録（録画）とは**ビデオを保存することを意味し、場合によってはカメラからの音声を監視システムのデータベースへ保存することも意味します。**多くの IP 監視システムでは、カメラから受信したビデオと音声のすべてを保存する必要はありません。ビデオと音声のカメラのデータベースへの保存は、多くの場合、モーションが検知された、イベントが発生した、あるいは特定の時刻になったなどの理由がある場合のみ開始されます。そのため、記録は、たとえばモーションが検知されなくなったり、あるイベントが発生したり、期間が終了したときなどに停止されます。元々**記録**とは、録画ボタンを押すまで画像をテープに保存できなかったアナログビデオの用語です。

魚眼

魚眼画像を作成・表示できるようなレンズの種類です。

手動イベント

イベントをクライアントから手動で生成することができます。これらのイベントは手動イベントと呼ばれます。

復元ポイント

復元ポイントにより、以前の設定状態に戻すことができます。システムで設定の変更が適用されると、復元ポイントが作成されます。設定でエラーが生じた場合、復元ポイントを参照して、適切な状態に戻すことができます。

猶予期間

システムをインストールおよび構成し、レコーディングサーバーとカメラを追加すると、ライセンスを認証するまで、異なるデバイスは試用期間で実行されます。この試用期間が猶予期間です。猶予期間が終了するか、システムの動作が停止する前に、ライセンスを認証する必要があります。システムがオンラインの場合、ライセンスは自動的に認証されます。

索引

JVCケンウッド
カスタマーサポートセンター

固定電話 0120–2727–87

携帯電話・PHS 0570–010–114

一部のIP電話など 045-450-8950

FAX 045-450-2308

〒221-0022　神奈川県横浜市神奈川区守屋町3-12

ご相談窓口におけるお客様の個人情報は、お問合せへの対応、修理およびその確認に使用し、適切に管理を行い、お客様の同意なく個人情報を第三者に提供または開示することはありません。

株式会社 JVCケンウッド・公共産業システム

〒 221-0022　神奈川県横浜市神奈川区守屋町 3-12

ホームページ　https://jkpi.jvckenwood.com/

B5A-3416-00