

JVC

ネットワークビデオレコーダー

型名 **VR-X7100**

Milestone XProtect
Enterprise
管理者マニュアル

目次

はじめに	10
最低限のシステム要件 XPROTECT SMART CLIENT:	10
管理者権限について	11
重要なポート番号について	11
ウイルススキャンについて	12
タイムサーバーについて	13
夏時間について	13
システム概要	15
システムコンポーネント	15
XPROTECT SMART CLIENT	17
XProtect Smart Client について	17
XProtect Smart Client のインストール	18
RECORDING SERVER MANAGER	19
XPROTECT DOWNLOAD MANAGER	20
インストールとアップグレード	23
ビデオデバイスドライバのインストール	23
MILESTONE MOBILE クライアントのインストール.....	23
初めての使用	24
システムの起動および実行	24
推奨事例.....	25

録画データベースの破損からの保護について	25
設定に関する変更の保存について	26
組み込みヘルプの使用について	27
サービスの再起動について	28
モニターストレージ容量の使用率	29
Management Application でカメラからのビデオを表示する	29
スタート	30
スタートページについて	30
ハードウェアの追加ウィザード	30
高速	31
手動	32
ストレージの設定ウィザード	35
ストレージの設定：ビデオ設定とプレビュー	35
ストレージの設定：オンラインスケジュール	36
Motion-JPEG カメラのライブ設定および録画設定	36
MPEG カメラのライブ設定および録画設定	38
ドライブの選択	40
録画およびアーカイブの設定	43
モーション検知の調整ウィザード	44
領域の除外	44
モーション検知	45
ユーザーアクセスの管理ウィザード	47
基本ユーザーと Windows ユーザー	47
アクセスの概要	48
拡張設定	49
ハードウェアデバイス	49

ハードウェアデバイスについて.....	49
マイクについて.....	49
スピーカーについて.....	49
音声録音について.....	49
専用入力/出力デバイスについて.....	50
ハードウェアデバイスの交換について.....	51
ハードウェアデバイスの設定.....	51
ハードウェアデバイスの削除.....	51
ハードウェアデバイス交換ウィザードについて.....	52
ハードウェアプロパティ.....	54
スピーカープロパティ.....	57
カメラとストレージの情報.....	57
ビデオや録画の設定について.....	57
データベースのサイズ変更について.....	58
モーション検知について.....	58
モーション検知および PTZ カメラについて.....	60
カメラ固有のスケジュールの設定.....	60
カメラがいつ、何をやる必要があるかを設定する.....	62
モーション検知の設定.....	62
カメラの無効化または削除.....	63
PTZ タイプ 1 および 3 を、必要な位置へ移動する.....	63
録画およびストレージのプロパティ.....	64
カメラプロパティ.....	81
マイク.....	104
マイクについて.....	104
マイクまたはスピーカーの設定.....	104
マイクやスピーカーの表示/非表示.....	104
マイク (プロパティ).....	105

イベントおよび出力	105
入力および出力について	105
イベントおよび出力について	106
イベントおよび出力の概要	106
アナリティックイベントの追加	109
ハードウェア入力イベントの追加	109
ハードウェア出力の追加	110
手動イベントの追加	111
ジェネリックイベントの追加	111
タイマーイベントの追加	112
イベントでのハードウェア出力の設定	112
一般的なイベント処理の設定	113
アナリティックイベントに基づくアラームの生成	113
ジェネリックイベントのテスト	114
ジェネリックイベントプロパティ	115
イベントおよび出力プロパティ	116
スケジュールおよびアーカイブ	127
スケジュールについて	127
アーカイブについて	127
一般的なスケジュールおよびアーカイブの設定	133
一般的なスケジュールのプロパティ	133
カメラ固有のスケジュールプロパティ	137
MATRIX	139
Matrix ビデオの共有について	139
Matrix 受信 PC について	139
Matrix の設定	140
Matrix のプロパティ	140
ログ	143

ログについて.....	143
システム、イベント、監査ログの設定.....	145
ログプロパティ	145
通知	147
通知について.....	147
E メール	148
SMS.....	151
スケジュール.....	153
CENTRAL	154
Central について.....	154
XProtect Central の有効化.....	154
Central のプロパティ	154
アクセスコントロール	155
アクセスコントロールの統合について	155
アクセスコントロールシステム統合ウィザード	156
アクセスコントロールプロパティ	157
サーバーアクセス.....	164
サーバーアクセスについて	164
登録済みサービスについて	165
サーバーアクセスの設定.....	165
サーバーアクセスプロパティ	166
マスター/スレーブ.....	168
マスターおよびスレーブについて	168
マスターおよびスレーブサーバーの設定	168
マスター/スレーブプロパティ	168
ユーザー	170
ユーザーについて.....	170

基本ユーザーの追加.....	170
Windows ユーザーの追加	171
ユーザーグループの追加.....	171
ユーザーおよびグループの権限の設定.....	172
ユーザープロパティ	173
サービス	177
サービスについて.....	177
サービスを開始および停止する	178
サーバー	178
Mobile サーバー.....	178
アラーム	190
アラームについて.....	190
マップについて	191
アラームの時間プロファイルについて	192
アラームの追加	192
(アラームの) 時間プロファイルの追加	193
アラームプロパティ	193
MIP プラグイン	198
MIP プラグインについて.....	198
設定.....	199
自動デバイス検出について	199
カスタマーダッシュボードについて	199
情報収集の無効化.....	199
デフォルトのファイルパスの変更.....	200
オプション	201
一般	201

ユーザーインターフェース	202
デフォルトのファイルパス	203
プライバシーオプション	203
アナリティックイベント設定	204
イベントサーバー設定	205
システムのメンテナンス	207
バックアップおよび復元の設定	207
設定のバックアップおよび復元について	207
システム設定のバックアップ	207
システム設定の復元	208
アラームおよびマップ設定のバックアップと復元	208
Management Application の設定のエクスポートおよびインポート	211
設定に対する変更のインポート	213
復元ポイントからのシステム設定の復元	213
用語集	215
索引	223

著作権、商標、および免責条項

著作権

© 2014 Milestone Systems A/S.

商標

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

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

本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

最低限のシステム要件 XProtect Smart Client:

コンポーネント	要件
オペレーティングシステム	<ul style="list-style-type: none">Windows Server 2008 R1/R2 (32 ビット版または 64 ビット版)Windows Vista® Business (32 ビット版または 64 ビット版)Windows Vista Enterprise (32 ビット版または 64 ビット版)Windows Vista Ultimate (32 ビット版または 64 ビット版)Windows 7 Professional (32 ビット版または 64 ビット版)Windows 7 Enterprise (32 ビット版または 64 ビット版)Windows 7 Ultimate (32 ビット版または 64 ビット版)Windows 8 Pro (32 ビット版または 64 ビット版)Windows 8 Enterprise (32 ビット版または 64 ビット版)
CPU	Intel Core2™ Duo、2.4 GHz 以上 (複数のカメラが動作し、複数のビューおよび表示を使用する XProtect Smart Client では、より高い性能の CPU を推奨します)。
RAM	最低 1 GB (複数のカメラが動作し、複数のビューおよび表示を使用するシステムでは、これより高い RAM を推奨します)。
ネットワーク	イーサネット (100 Mbit 以上を推奨)
グラフィックアダプタ	AGP または PCI-Express、最低 1280×1024、16 ビット色
ハードディスク容量	1 GB の空き容量
ソフトウェア	<ul style="list-style-type: none">Microsoft .Net 4.0 Framework かそれ以上DirectX 9.0 かそれ以上

Milestone Mobile クライアント :

コンポーネント	要件
オペレーティングシステム	<ul style="list-style-type: none">Apple デバイスの場合、iOS 6.0 かそれ以上。Android デバイスの場合、Android 2.2 かそれ以上。Windows 8 Phone の場合、Windows Phone 8。

XProtect Web Client:

※本機は、XProtect Web Client には対応していません。

コンポーネント	要件
サポートされるブラウザ	HTML 5 および JavaScript をサポートしているブラウザ。XProtect Web Client の実行環境： <ul style="list-style-type: none">• Microsoft Internet Explorer 9 かそれ以上。• Mozilla Firefox 11 かそれ以上。• Google Chrome 16 かそれ以上。• Safari 5 かそれ以上。

管理者権限について

監視システムをインストールする際には、システムを実行するコンピュータの管理者権限が必要です。標準ユーザーの権限のみでは、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

システムでは、他のコンピュータ、カメラなどとの通信の際に特定のポートを使用します。システムを使用する際は、以下のネットワークポートが空いていることを確認してください。

名前	説明
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。設定によって、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 トラフィックで使用され、監視システムの Image Server サービスのデフォルト通信ポートとなります。
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。

名前	説明
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 アドオン製品との通信で使用。
ポート 8081 および 8082	Mobile サービスとの通信で使用。
ポート 22331	Event Server サービスとの通信で使用。

また、組織では他のポートの使用を選択していることもあります。たとえば、サーバーアクセス『166ページ』ポートがデフォルトのポート番号(80)から別のポート番号に変更されていることがあります。

ウイルススキャンについて

※本機にはウイルス対策ソフトウェアをインストールしないでください。

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、録画データベースを含んでいるレコーディングサーバーのディレクトリ（デフォルトでは `d:\mediadatabase\`、ならびにその場所より下位のディレクトリ）はスキャンしないでください。また、アーカイブ保存ディレクトリでもウイルススキャンは実行しないでください。以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® Corporate, XProtect® Expert	80, 8080, 7563, 25, 21, 9993

製品	TCP ポート
XProtect® Enterprise、XProtect® Professional、XProtect® Express、XProtect® Essential、XProtect® Basis+	80, 25, 21, 1234, 1237, 22331
XProtect® Mobile	8081
XProtect® Transact	9001

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 Corporate, XProtect Expert	<i>VideoOS.Recording.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe</i>
XProtect Enterprise, XProtect Professional, XProtect Express, XProtect Essential, XProtect Basis+	<i>RecordingServer.exe, ImageServer.exe, ManagementApplication.exe, ImageImportService.exe, RecordingServerManager.exe, VideoOS.ServiceControl.Service.exe, VideoOS.Event.Server.exe</i>
XProtect Mobile	<i>VideoOS.MobileServer.Service.exe</i>
XProtect Transact	<i>VideoOS.Transact.TransactService.exe</i>

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。

タイムサーバーについて

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

タイムサーバーの設定に関する詳細は、www.microsoft.com でタイムサーバー、タイムサービス、その他類似のトピックを検索してください。

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。

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。通常、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。通常、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 に達すると、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。

このため、システム時刻の変更が 5 分を超えた場合、システムは強制的に現在のビデオをアーカイブします。最初の 01:00 時間は、クライアントから直接表示することはできません。ただし、データは録画され、安全に保存されます。XProtect Smart Client を使用してアーカイブ済みデータベースを直接開けば、閲覧できます。

システム概要

システムコンポーネント

この度はビデオ監視システムをお買い上げいただき、ありがとうございます。この製品は、柔軟で高い機能を持つインテリジェンス監視ソリューションです。このシステムは先進的な IP ビデオ監視システムです。様々なネットワークカメラやビデオエンコーダーに対応しており、オフィスの LAN やインターネットなどの TCP/IP ネットワーク上の機器との接続が可能です。

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。

名前	説明
Management Application	たとえば新規カメラを追加する場合、監視システムサーバーを設定するメインアプリケーションで、ユーザーのセットアップやシステムの設定の変更をします。
Recording Server サービス	監視システムの重要な部分です。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。これにより、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。
XProtect® 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。

名前	説明
XProtect® Smart Client	<p>Milestone XProtect 監視システム用に設計されている、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アプリケーションです。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。</p> <p>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。</p>
XProtect® Web Client	<p>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。追加ソフトウェアをインストールする必要なく、コンピュータまたはインターネット接続経由でシステムを監視することができます。</p> <p>※本機は、XProtect Web Client には対応していません。</p>
Milestone® Mobile クライアント	<p>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。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。</p>

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制御、録画の概要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。Milestone Integration Platform 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。

※本機は、Milestone Integration Platform には対応していません。

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 Image Server 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ウンドで実行されます。別途ハードウェアを用意する必要はありません。

※本機には、XProtect Smart Client があらかじめインストールされています。

別のコンピュータに 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。

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します。

管理サーバーからのインストール

開始する前に、使用している PC が XProtect Smart Client の最低限のシステム要件を満たしていることを確認して下さい。

1. Internet Explorer ブラウザ（バージョン 6.0 かそれ以上）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. 開かれたページで、PC に合わせた XProtect Smart Client の”すべての言語”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、XProtect LPR などの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。

サイレントインストール

※本機は、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 **MilestoneXProtectSmart Client_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\2014 (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:

```
MilestoneXProtectSmart Client_x64.exe --quiet
```

使用しているシステム :

```
MilestoneXProtectProfessionalVMS_installer_x64.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。

- a) 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:

```
MilestoneXProtectSmart Client_x64.exe --generateargsfile=[フルパス]args.xml
```

- 使用しているシステム :

```
MilestoneXProtectProfessionalVMS_installer_x64.exe --generateargsfile=[フルパス]args.xml
```

生成された args.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:

```
MilestoneXProtectSmart Client_x64.exe --arguments=[フルパス]args.xml --quiet
```

- 使用しているシステム :

```
MilestoneXProtectProfessionalVMS_installer_x64.exe --arguments=[フルパス]args.xml --quiet
```

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ことで、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の障害の可能性があります。エラーは、レコーディングサーバーの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 5 秒毎に更新されます。

名前	説明
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

組織のユーザーが、XProtect Download Manager の使用によって監視システムサーバー上の対象のようこそページからアクセスできるシステム関連の機能を管理します。

※XProtect Download Manager の設定は変更しないでください。

- Windows のスタートメニューから XProtect Download Manager にアクセスします。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。

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（サーバーアクセスの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**すべての言語**のみが選択可能です。

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：

1. XProtect Download Manager で、**機能の削除...**をクリックします。
2. **機能の削除**ウィンドウで、削除したい機能を選択します。
3. **削除**と**はい**をクリックします。

インストールとアップグレード

ビデオデバイスドライバーのインストール

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 サイトで提供されています。動作確認済みのビデオデバイスドライバーの最新バージョンは、お買い上げ販売店またはサービス窓口にお問い合わせ下さい。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せん。

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、重要な記録イベント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. ウィザードが完了したら、必ず Recording Server サービスを再起動してください。

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 サイトで最新情報をご確認ください。

Milestone Mobile クライアントのインストール

1. デバイスで Google Play または App StoreSM にアクセスします。
2. アプリケーション Milestone Mobile を検索してダウンロードします。
3. アプリケーションのダウンロードが完了すると、Milestone Mobile クライアントをモバイルデバイスで使用できます。

Milestone Mobile クライアントの詳細なセットアップ方法については、<http://www.milestonesys.com> から Milestone Web サイトにアクセスしてください。

初めての使用

システムの起動および実行

このチェックリストは、システムを動作させる時に通常必要となる作業を概説しています。

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、調整することを強くお勧めしています。

たとえば、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。これは、システムが起動した後で行います。イベントや関連するアクションの設定も、通常は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。

<input type="checkbox"/>	Management Application を開く インストール後に、Management Application を起動して、システムの機能をセットアップします。
<input type="checkbox"/>	カメラおよびその他のハードウェアデバイスの初期設定の確認 システムにハードウェアデバイス（カメラ、ビデオエンコーダーなど）を追加し、適切なユーザー名およびパスワードで設定します。
<input type="checkbox"/>	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、ビデオ形式、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『57ページ』を参照してください。
<input type="checkbox"/>	イベント、入力、出力の設定 必要であれば、センサーからの入力に基づくシステムイベントを使用して、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、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。イベントの概要を参照してください。
<input type="checkbox"/>	スケジュールの設定 いつアーカイブを行うか、カメラが常に映像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映像を転送するか、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とアーカイブの設定『133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』およびカメラ固有のスケジュールの設定『60ページ』を参照してください。

<input type="checkbox"/>	<p>クライアントによるシステムへのアクセス設定</p> <p>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 『165ページ』を参照してください。</p>
<input type="checkbox"/>	<p>マスター/スレーブサーバーの設定</p> <p>複数のサーバーを一緒に動作させたい場合、以下の手順に従ってください。</p> <p>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、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。</p> <p>このような設定でも、クライアントの接続数は1つだけです。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 『168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。</p>
<input type="checkbox"/>	<p>ユーザーの設定</p> <p>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。ユーザーアクセス設定ウィザード 『47ページの"ユーザーアクセスの管理ウィザード"参照』、基本ユーザーの追加 『170ページ』、ユーザーグループの追加 『171ページ』、ユーザーおよびグループの権限の設定 『172ページ』を参照してください。</p>

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。たとえば **Matrix** 『139ページの"Matrix ビデオの共有について"参照』 動画共有機能を必要とする場合は、さらに多くの設定が必要になります。

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よう注意することをお勧めします。

停電 : UPS の使用

※本機には、必ず **UPS** を接続してください。

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、UPS（無停電電源装置）を接続することです。

UPS は、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。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 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。

Management Application の設定を変更し、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 Server** 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 『213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** のツールバーにある**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操作

ヘルプシステムのコンテンツ間で移動するには、ヘルプタブを使用します。**内容**、**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	手動録画の有効化
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
エビデンス収集モードの有効化・無効化。XProtect Enterprise のみ。	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
	エビデンス収集モードの有効化・無効化。XProtect Enterprise のみ。

モニターストレージ容量の使用率

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. **拡張設定**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 でカメラからのビデオを表示する

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. **拡張設定**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： 特定の状況で **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をサポートしていないカメラは、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。したがって、**Milestone** では、モーション検知や **PTZ** でそのようなデバイスを設定している場合は、**Recording Server** サービスを停止 『178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 『29ページ』、も参照してください。

スタート

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。スタートページには、ウィザードの簡単な使い方が示されており、ユーザーの参照場所として機能します。

お使いのシステムのカメラライセンスの数を確認するには、スタートページの左下の欄でこの情報を見ることができます。

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。これらにアクセスするには、右下の欄にあるこの**チュートリアルの表示**リンクをクリックしてください。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。

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。

サーバーあたり最大 **64** 台のカメラを使用できます。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。

名前	説明
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 『31ページの"高速"参照』を参照してください。

名前	説明
追加するハードウェアを手動で指定します	<p>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。</p> <p>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。</p> <p>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 『32ページの"手動"参照』。</p> <p>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。</p> <p>ハードウェアの追加：CSVファイルからインポートします 『33ページの"CSVファイルからインポート"参照』。</p>

カメラのIPアドレスを変更した際は、ハードウェアの追加をせず、拡張設定 > ハードウェアデバイスから変更するカメラのプロパティを選択し、ネットワークのアドレスを変更してください。

このウィザードの手順：

高速.....	31
手動.....	32

高速

注意：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する必要があります。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 『32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、ユーザー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 『33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	説明
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。デフォルトはポート 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既定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。あなたの組織がこれに該当する場合、<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を入力しないでください。
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、必ず最低限度の情報が必要になります。

名前	説明
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	カメラやサーバーがオフラインであれば、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。大半のシステムインテグレーターは、ハードウェアデバイス情報を 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しています。

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一意でなければならないことと、以下の特殊文字が含まれないことに特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除外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。

このウィザードの手順：

ストレージの設定：ビデオ設定とプレビュー	35
ストレージの設定：オンラインスケジュール	36
Motion-JPEG カメラのライブ設定および録画設定	36
MPEG カメラのライブ設定および録画設定	38
ドライブの選択	40
録画およびアーカイブの設定	43

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場合があります。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『135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	説明
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。

Motion-JPEG カメラのライブ設定および録画設定

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 ビデオ形式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（XProtect Enterprise および XProtect Professional のみ）。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
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。右の列で、必要な秒数を指定します。
秒数 [プリレコーディング]	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 『127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、問題の原因となる場合があります。
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。右の列で、必要な秒数を指定します。
秒数 [ポストレコーディング]	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、問題の原因となる場合があります。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

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。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

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	説明
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。

MPEG カメラのライブ設定および録画設定

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 MPEG ビデオ形式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。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
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。

名前	説明
録画設定	<p>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。</p> <ul style="list-style-type: none"> ● 常時:カメラが有効 『81ページの"一括設定"参照』であり、オンラインになるようスケジュールされている 『137ページの"オンライン期間"参照』場合に録画します（後者によって、時間に基づく録画が可能になります）。 ● 設定しない:録画しません。ライブビデオは表示されますが、ビデオがデータベースに保存されないため、カメラからのビデオを再生することはできません。 ● モーション検知:これを選択すると、モーション 『91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: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。 イベントの設定は拡張設定-イベントおよび出力であらかじめ設定しておいてください。 ● 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、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	<p>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。右の列で、必要な秒数を指定します。</p>
秒数 [プリレコーディング]	<p>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 『127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、問題の原因となる場合があります。</p>

名前	説明
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。右の列で、必要な秒数を指定します。
秒数 [ポストレコーディング]	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、問題の原因となる場合があります。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

キーフレームのみ	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、 キーフレームのみ 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	説明
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。

ドライブの選択

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 『**127**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。

すべての **XProtect** ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
ドライブ	対象となるドライブを表す文字、たとえば C: など。
目的	<p>ドライブを使用する目的を選択します。</p> <p>使用しない： ドライブは使用しません。</p> <p>レコーディング: ドライブが、XProtect Enterprise 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。XProtect Enterprise のデータベース録画に使用するドライブです。</p> <p>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（以下の説明を参照）、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。</p> <p>レコーディングおよびアーカイブ： ドライブが、XProtect Enterprise 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。XProtect Enterprise 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。</p>
レコーディングパス	<p>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、D:\¥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すると、ネットワークドライブが使用できない場合に録画を保存できなくなります。</p> <p>レコーディングパスを変更し、古い場所に既存の録画がある場合、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。</p> <p>ヒント： 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。</p>

名前	説明
アーカイブパス	<p>アーカイブ 『127ページの"アーカイブについて"参照』でダイナミック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、D:\¥MediaDatabase です。</p> <p>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、XProtect Enterprise 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。</p>
合計サイズ	ドライブの合計サイズ。
空き容量	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	<p>このオプションを使用する場合、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。XProtect Enterprise 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、XProtect Enterprise 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、XProtect Enterprise 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、再生する方法には影響を与えません。</p>
アーカイブ時刻	<p>XProtect Enterprise で自動的に録画をアーカイブパスへ移動させたい時刻を指定します。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。</p>
XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：	
ネットワークドライブ	<p>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。</p>

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 『127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。

名前	説明
レコーディングパス	<p>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、D:\¥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すると、ネットワークドライブが使用できない場合に録画を保存できなくなります。</p> <p>レコーディングパスを変更し、古い場所に既存の録画がある場合、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。</p> <p>ヒント：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。</p>
アーカイブパス	<p>アーカイブ 『127ページの"アーカイブについて"参照』でダイナミック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、D:\¥MediaDatabase です。</p> <p>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、XProtect Enterprise 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。</p>
保持期間	<p>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。デフォルトは7日です。</p> <p>保持時間は、録画を保持しておく合計時間です。以前のバージョンの XProtect Enterprise では、データベースとアーカイブで個別に制限時間を指定していました。</p>

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	説明
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をサポートしていないカメラは、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。したがって、**Milestone** では、モーション検知や **PTZ** でそのようなデバイスを設定している場合は、**Recording Server** サービスを停止 『178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 『29ページ』、も参照してください。

このウィザードの手順：

領域の除外.....	44
モーション検知	45

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をサポートしていないカメラは、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** を設定する場合は、**Recording Server** サービスを停止 『178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 『29ページ』、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。

すべてを含める 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したい場合に便利です。その場合は、モーション検知を無効にしたい部分をクリアします。すべてを除外するボタンでは、素早くすべてのグリッドを選択解除できます。

モーション検知

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をサポートしていないカメラは、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 を設定する場合は、**Recording Server** サービスを停止 『178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 『29ページ』、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。



すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
感度	<p>感度 スライダーを調整して、不要なバックグラウ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。</p> <p>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。</p>
モーション	<p>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。</p> <p>または、右のフィールドで 0~10000 の値を指定して、モーション設定を制御します。</p> <p>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。</p>
検知間隔	<p>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。</p> <p>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。</p>
検知解像度	<p>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。</p>

XProtect Enterprise でのみ使用可能なプロパティ：

キーフレームのみ	<p>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、キーフレームのみ を選択します。</p>
----------	---

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 『172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 『165ページ』を参照してください。ユーザーをグループ 『171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。

このウィザードの手順：

基本ユーザーと Windows ユーザー	47
アクセスの概要	48

基本ユーザーと Windows ユーザー

Active Directory®は、XProtect Enterprise および XProtect Professional 2013+ でのみ使用可能です。

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	説明
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。

注意： 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**をクリックして、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アドレスを指定する必要があります。正しく指定したユーザー名の例：**USER001**。正しくない例：**PC001/USER001**。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。

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 『172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。

拡張設定

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『30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、**非表示アイテムの表示**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、（スピーカーから）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 に対して音声は 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せん。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を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。

ハードウェアデバイスの交換について

必要であれば、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 『52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 (パン/チルト/ズーム) 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. **拡張設定**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 『55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 『56ページ』、魚眼レンズ 『96ページの"魚眼 (レンズ)"参照』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

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. **拡張設定**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 『178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. **拡張設定**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 『178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。

名前	説明
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。デフォルトはポート 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既定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。あなたの組織がこれに該当する場合、<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を入力しないでください。
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。

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、ビデオデバイスのドライバーを選択してから、**自動検出/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 -
- **自動検出/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り、**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を決定します。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

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。準備ができたなら、**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。

ハードウェアプロパティ

ハードウェア名およびビデオチャンネル

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。

名前	説明
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、新しい名前の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。

インポートしたライセンスのチャンネル数制限により、ビデオエンコーダーデバイスが持つチャンネルの一部を使用できない場合があります。

例：4チャンネルのビデオエンコーダーデバイスがありますが、そのデバイス用のライセンスではこのうち2つのチャンネルしか使用できません。このような場合、同時に有効にできるチャンネルは2つだけであり、他の2つのチャンネルは無効化されます。どの2つのチャンネルを有効にするかは、ユーザーが自由に選択できます。

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 『51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。

名前	説明
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。 カメラの IP アドレスを変更した際は、ハードウェアの追加を行わず、この画面で IP アドレスを変更して下さい
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。デフォルトポートは 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 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既定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。あなたの組織がこれに該当する場合、<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いった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を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	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（「root」パスワードと呼ばれます）。
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。

名前	説明
ハードウェアデバイスの交換	ウィザード 『52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』 を起動し、必要な場合、選択しているハードウェアデバイスを他のハードウェアデバイスと置き換えることができます。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。このウィザードは、関連する問題をすべて考慮するのに役立ちます。たとえば、古いハードウェアデバイスに接続されているカメラの録画データ処理方法を決定します。

PTZ デバイス

PTZ デバイスタブが使用できるのは、PTZ (パン/チルト/ズーム) カメラの使用が可能なビデオエンコーダーデバイスを設定 『51ページの"ハードウェアデバイスの設定"参照』 してある場合だけです。

名前	説明
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、なしを選択します。

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	説明
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。 <ul style="list-style-type: none"> 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。

名前	説明
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。デジチェー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。

スピーカープロパティ

特定のカメラに対してビデオや録画を設定『57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。

名前	説明
デバイスが有効	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、新しい名前の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	説明
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。
一括設定	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 『127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 『66ページの"ダイナミックパスの選択"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 『177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	Recordings	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	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	Recordings	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	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す。 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 『100ページの"PTZ パトロール"参照 』で指定されます。

カメラ固有のスケジュールの設定

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。

イベントの設定は拡張設定 > イベントおよび出力であらかじめ設定しておいてください。



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。録画は別途設定します。ビデオおよび録画の設定 『57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。

それぞれのカメラについて、以下に基づいてスケジュールプロファイルを作成できます。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

オンライン期間

- 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。

スピードアップ

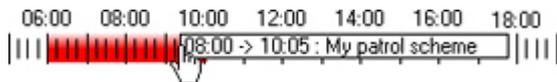
- 期間（例：月曜日の 08:30 から 17:45 まで）、オリーブグリーン色で表示：

E メール通知

- 期間（例：月曜日の 08:30 から 17:45 まで）、青色で表示：

PTZ パトロール

- 期間（例：月曜日の 08:30 から 17:45 まで）、赤色で表示：
- あるパトロールプロファイルの使用の直後に、別の使用が続く場合、マウスポインターを赤いバーの上へ移動させて、どのパトロールプロファイルがいつ適用されているかを確認します。



XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

SMS 通知

※本機は、**SMS** での通知には対応していません。

期間（例：月曜日の 08:30 から 17:45 まで）、緑色で表示： プロファイルのセットアップ

1. スケジュールプロファイルリストで、**新規追加...**を選択します。
2. プロファイルの追加ダイアログで、プロファイルの名前を入力します。名前には、以下の特殊文字を含めることはできません。 **< > & ' " \ / : * ? | []**
3. ダイアログの右上にある、**定時刻にカメラを起動/停止**を選択して期間をベースとするか、**イベント時にカメラを起動/停止**を選択して期間内のイベントをベースとします。
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。XProtect Enterprise ではマウスポインタが位置している時間が表示され、操作をサポートします。



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。

- イベントの設定は**拡張設定 > イベントおよび出力**であらかじめ設定しておいてください。
- 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、何を必要があるかを設定する

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**または**SMS通知**を受信したい場合
- **PTZ**カメラは、パトロールプロファイルに従って、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とアーカイブの設定 『133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』およびカメラ固有のスケジュールの設定 『60ページ』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. **拡張設定 > 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 『58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 『44ページの"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 『91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 『60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 『137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. **拡張設定**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 『51ページの"ハードウェアデバイスの削除"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

ビデオおよび録画を設定『57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。

名前	説明
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、レコーディングパス、アーカイブパス、およびそれらすべての保持時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。

名前	説明
カメラ名	<p>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、新しい名前の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。 < > & ' " ¥ / : * ? []</p>
ショートカット	<p>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。</p> <p>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。</p> <p>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。</p> <p>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、Smart Client の他のマニュアルにあります。</p>
レコーディングパス	<p>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、D:¥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すると、ネットワークドライブが使用できない場合に録画を保存できなくなります。</p> <p>レコーディングパスを変更し、古い場所に既存の録画がある場合、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。</p> <p>ヒント： 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。</p>
アーカイブパス	<p>アーカイブ 『127ページの"アーカイブについて"参照』でダイナミック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、D:¥MediaDatabase です。</p> <p>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、XProtect Enterprise 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。</p>

名前	説明
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。デフォルトは7日です。 保持時間は、録画を保持しておく 合計時間 です。以前のバージョンの XProtect Enterprise 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

ビデオおよび録画を設定 『57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。ダイナミックパスが選択された場合、プロパティがすべてのカメラで共有されます。

ダイナミックアーカイブ 『127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。

名前	説明
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	対象となるドライブを表す文字、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
ドライブ容量	ドライブの合計サイズ。
空き容量	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	選択したパス（以前に手動で追加したもの）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

ビデオおよび録画を設定『57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『86ページの"記録(録画)"参照』指定できることに注意してください。

名前	説明
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、レコーディングパス、アーカイブパス、およびそれらすべての保持時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、新しい名前の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。 < > & ' " ¥ / : * ? []
録画設定	<p>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。</p> <ul style="list-style-type: none"> 常時:カメラが有効 『81ページの"一括設定"参照』であり、オンラインになるようスケジュールされている 『137ページの"オンライン期間"参照』場合に録画します（後者によって、時間に基づく録画が可能になります）。 設定しない:録画しません。ライブビデオは表示されますが、ビデオがデータベースに保存されないため、カメラからのビデオを再生することはできません。 モーション検知:これを選択すると、モーション 『91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: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。 <p>イベントの設定は拡張設定 > イベントおよび出力であらかじめ設定しておいてください。</p> <ul style="list-style-type: none"> 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るから、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。

名前	説明
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（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。
終了イベント	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（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。右の列で、必要な秒数を指定します。
秒数 [プリレコーディング]	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 『127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、問題の原因となる場合があります。
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。右の列で、必要な秒数を指定します。
秒数 [ポストレコーディング]	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、問題の原因となる場合があります。
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。
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。

カメラで MJPEG ビデオ形式を使用する場合

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 : すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ :

名前	説明
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。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ :

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。

スピードアップフレームレートモード :

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ :

名前	説明
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	カメラの映像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。

名前	説明
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必要があります。 イベントの設定は拡張設定 > イベントおよび出力であらかじめ設定しておいてください。
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。
終了イベント	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。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

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。

ヒント：スピードアップは、モーションやイベントに基づいている必要はありません。スケジュール『138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、スピードアップを有効にする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：

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。

名前	説明
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、レコーディングサーバーへの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。

カメラが MPEG ビデオ形式を使用する場合

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。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
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映像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。

XProtect Enterprise、XProtect Professional および XProtect Express でのみ使用可能なプロパティ：

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必要があります。 イベントの設定は拡張設定 > イベントおよび出力であらかじめ設定しておいてください。

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。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、カメラはすべてのフレームの録画を開始します。
終了イベント	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、カメラは再びキーフレームのみを録画します。

デュアルストリーム :

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。

名前	説明
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、レコーディングサーバーへの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。

手動録画

ビデオおよび録画を設定『57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。

有効であれば、個々のカメラの録画『86ページの"記録(録画)"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、手動録画を行うことができます。

XProtect Smart Client から開始した場合、必ず固定の時間（たとえば5分）で、こうしたユーザー主導の録画を行います。

名前	説明
手動レコーディングの有効化	チェックボックスを選択して手動レコーディングを有効にし、詳細を指定します。
手動レコーディング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。

名前	説明
手動レコーディングの最長継続時間	ユーザーによる録画が可能な最長の期間。こうした手動レコーディングは必ず一定時間で行われるので、この最長期間は Smart Client で開始される手動レコーディング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 XProtect Enterprise と統合する場合に、手動レコーディング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があります。このような状況では、最長期間の指定が関連します。単に手動レコーディングを Smart Client と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。

フレームレート - MJPEG

ビデオおよび録画を設定 『57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 『86ページの"記録 (録画)"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	説明
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、レコーディングパス、アーカイブパス、およびそれらすべての保持時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。

名前	説明
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、新しい名前の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

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
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す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。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

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。

スピードアップフレームレートのプロパティ

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
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	カメラの映像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す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。
スピードアップ をオン	<ul style="list-style-type: none"> ● モーション検知:これを選択すると、モーション 『91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、即時に通常のフレームレートに戻ります。 ● イベント:これを選択すると、イベントが発生してから次に別のイベントが発生するまで、スピードアップします。イベントによるスピードアップを使用するには、そのイベントが定義されていて、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いることが必要です。 イベントの設定は拡張設定 > イベントおよび出力であらかじめ設定しておいてください。 ● 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、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	これを選択すると、カメラのスピードアップをスケジュール 『138ページの"スピードアップ"参照』にのみ従ってスピードアップします。
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。
終了イベント	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。
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。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ :

ライブフレームレート :	<p>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。</p> <p>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。</p>
録画フレームレート :	<p>カメラの録画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。</p>

フレームレート - MPEG

ビデオおよび録画を設定 『57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 - MPEG プロパティは、MPEG を使用するそれぞれのカメラに対して個別に 『86ページの"記録 (録画)"参照』指定できることに注意してください。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ :

名前	説明
テンプレート	<p>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、レコーディングパス、アーカイブパス、およびそれらすべての保持時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。</p>
テンプレートを適用	<p>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。</p>
カメラ名	<p>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、新しい名前の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。 < > & ' " ¥ / : * ? []</p>
デュアルストリーム	<p>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 『82ページ』プロパティでこれを有効/無効にできます。</p>
ライブ FPS	<p>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。</p>

名前	説明
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。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

キーフレームのみの録画	<p>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。</p>
すべてのフレームの録画	<p>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。</p> <ul style="list-style-type: none"> 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『91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。 <p>イベントの設定は拡張設定 > イベントおよび出力であらかじめ設定しておいてください。</p> <ul style="list-style-type: none"> 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『138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。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、カメラはすべてのフレームの録画を開始します。
終了イベント	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、カメラは再びキーフレームのみを録画します。

音声録音

特定のカメラに対してビデオや録画を設定『57ページの"ビデオや録画の設定について"参照』する場合、音声を録音するかどうかを指定できます。この選択は、システムのすべてのカメラに適用されません。

名前	説明
常時	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。音声を録音しなくても、 Smart Client でライブ音声を聞くことは可能であることに注意してください。

音声を録音する場合、以下に注意することが重要です。

- 音声録音は、ビデオ保存容量に影響します。音声は、関連するカメラのデータベースに録音されます。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『127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 に対して音声は 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利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。

音声の選択

ビデオおよび録画を設定『57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で選択されているマイクまたはスピーカーからの音声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。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
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、レコーディングパス、アーカイブパス、およびそれらすべての保持時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、新しい名前の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。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

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	説明
ドライブ	対象となるドライブを表す文字、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。
空き容量	ドライブに残っている未使用の容量。

カメラプロパティ

一括設定

特定のカメラについてビデオや録画を設定 『57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。

名前	説明
デバイスが有効	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 『137ページの"オンライン期間"参照』、ビデオを XProtect Enterprise に転送できることを意味します。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、カメラの映像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、新しい名前の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。 < > & ' " ¥ / : * ? []

名前	説明
カメラのショートカット番号	<p>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。</p> <p>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。</p> <p>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。</p>

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。**カメラの設定...** 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場合があります。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

特定のカメラについてビデオや録画を設定 『57ページの"ビデオや録画の設定について"参照』する場合、MJPEG ビデオ形式または MPEG ビデオ形式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 ビデオ形式

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すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ:

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。
---------	---

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ:

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。

スピードアップフレームレートモード

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ:

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	カメラの映像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。
モーション検知時	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を選択してあることが必要です。
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。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ:

ライブフレームレート :	<p>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。</p> <p>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。</p>
録画フレームレート :	<p>カメラの録画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。</p>

注意 : 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、**スピードアップを有効にする**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

専用ライブストリームを有効にする	<p>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、レコーディングサーバーへの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。</p>
ストリーム	<p>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。</p>
解像度	<p>カメラの解像度を選択します。</p>
FPS	<p>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。</p>

MPEG ビデオ形式

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。

フレームレート

すべての **XProtect** ソフトウェアのバージョンで使用可能なプロパティ :

1秒当たりのフレームレート	<p>カメラからのライブビューおよび録画映像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。</p>
---------------	--

XProtect Enterprise、**XProtect Professional** および **XProtect Express** でのみ使用可能なプロパティ :

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。
モーション検知時にすべてのフレームを録画	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。
イベント発生時にすべてのフレームを録画	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を選択してある必要があります。
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。 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、カメラはすべてのフレームの録画を開始します。
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、カメラはキーフレームのみを録画します。

デュアルストリーム

専用ライブストリームを有効にする	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、レコーディングサーバーへの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

特定のカメラについてビデオや録画を設定 『57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で選択されているマイク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/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。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
デフォルトのマイク	デフォルトのマイクを選択します。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

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)

記録という言葉は、**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や録画を設定 『57ページの"ビデオや録画の設定について"参照』する場合、以下の録画プロパティが含まれます。

名前	説明
常時	カメラが有効 『81ページの"一括設定"参照』であり、オンラインになるようスケジュールされている 『137ページの"オンライン期間"参照』場合に録画します (後者によって、時間に基づく録画が可能になります)。
設定しない	録画しません。ライブビデオは表示されますが、ビデオがデータベースに保存されないため、カメラからのビデオを再生することはできません。
条件	<p>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。</p> <p>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停止イベントで、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。</p>

名前	説明
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 『91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。 イベントの設定は拡張設定 > イベントおよび出力であらかじめ設定しておいてください。
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（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。
終了イベント	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（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。

手動録画 『73ページ』 が有効である可能性があります。手動録画は、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、手動録画を行うことができます。

録画およびアーカイブのパス

特定のカメラについてビデオや録画を設定 『57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。

コンポーネント	要件
レコーディングパス	<p>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、D:\¥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すると、ネットワークドライブが使用できない場合に録画を保存できなくなります。</p> <p>レコーディングパスを変更し、古い場所に既存の録画がある場合、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。</p> <p>ヒント： 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。</p>
データベースの削除	<p>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。</p> <p>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。安全対策として、削除を確認するメッセージが表示されます。</p>
アーカイブパス	<p>アーカイブ 『127ページの"アーカイブについて"参照』でダイナミック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、D:\¥MediaDatabase です。</p> <p>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、XProtect Enterprise 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。</p>
アーカイブの削除	<p>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。</p> <p>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。安全対策として、削除を確認するメッセージが表示されます。</p>

コンポーネント	要件
保持期間	<p>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。デフォルトは7日です。</p> <p>保持時間は、録画を保持しておく合計時間です。以前のバージョンの XProtect Enterprise 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。</p>
データベース修復アクション	<p>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。</p> <ul style="list-style-type: none"> ▶ 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、データベースの内容を削除します。 ▶ アーカイブ（修復無し）：データベースが破損した場合、データベースの内容をアーカイブします。 <p>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。</p> <p>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。</p> <p>ヒント：データベースの破損を回避 『25ページの"録画データベースの破損からの保護について"参照』するための基本的な注意事項がいくつかあります。</p>

コンポーネント	要件
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のいずれか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、XProtect Enterprise 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、XProtect Enterprise 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 『66ページ』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や録画を設定 『57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や録画を設定『57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『110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『172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 **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。
 - または
 - **検出された動作**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。必要であれば、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や録画を設定『57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の決定要因となるためです。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、圧縮率、解像度などのカメラのビデオプロパティ『81ページの"一括設定"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をサポートしていないカメラは、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。したがって、**Milestone** では、モーション検知や **PTZ** でそのようなデバイスを設定している場合は、**Recording Server** サービスを停止『178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『29ページ』、も参照してください。

名前	説明
有効化	組み込みのモーション検知を有効または無効 『58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	<p>グリッドをオンまたはオフに切り替えます。</p> <p>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。</p> <p>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。</p>
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。

名前	説明
手動感度	<p>この機能を有効にすると、モーシヨンの感度スライドを自分で調整することもできます。</p> <p>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。</p> <ul style="list-style-type: none"> ▶ 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オンと見なされます。 ▶ 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オンと見なされます。 <p>モーシオ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。</p> <p>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。</p> <ul style="list-style-type: none"> ▶ 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オ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オ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オ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。
感度	<p>これを使用して、モーシオ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、モーシオ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。モーシオ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。モーシオ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オ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。</p>

名前	説明
モーション	<p>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。</p> <p>または、右のフィールドで0~10000の値を指定して、モーション設定を制御します。</p> <p>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。</p>
キーフレームのみ	<p>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、キーフレームのみを選択します。</p>
検知間隔	<p>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。</p> <p>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。</p>
検知解像度	<p>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。</p>

プライバシーマスク

カメラの画像の一部が表示されないようにマスクする必要がある場合、以下のプロパティを設定します。

名前	説明
有効化	プライバシーマスク 機能を有効にします。

名前	説明
グリッドを表示	<p>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。</p> <p>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。</p>
プライバシーマスクの表示	<p>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。</p>
クリア	<p>プライバシーマスクをクリアします。</p>

魚眼レンズ

魚眼レンズテクノロジーを使用すると、高度なレンズで **360 度** のパノラマ画像を再生できます。カメラで魚眼レンズテクノロジーを使用する場合、まずテクノロジーを有効にし、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。

名前	説明
魚眼レンズを有効にする	<p>チェックボックスを選択すると、魚眼レンズテクノロジーが使用可能となり、さらに多くのプロパティを指定できます。</p>
panomorph サポートを有効にする	<p>選択すると、Panomorph サポートが有効になります。Panomorph は、従来の魚眼ソリューションよりピクセルの使用量を抑えながら、対象のエリアで高い解像度を提供できる先進的な技術です。</p>
ImmerVision Enables ³ Panomorph RPL 番号	<p>Panomorph サポート機能を有効にする場合、ImmerVision Enables³ Panomorph RPL 番号 リストで登録済み Panomorph レンズ(RPL) 番号も選択しなければなりません。これによりレンズが適切に識別され、カメラで使用されているレンズで設定が行われます。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。</p> <p>ある時点で、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。</p> <p>ImmerVison、Panomorph レンズ、RPL に関する詳細情報は、http://www.immervision.com/en/home/index.php を参照してください。</p>

名前	説明
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。
魚眼サポートを有効にする	選択すると、魚眼サポートが有効になります。魚眼テクノロジーは、広角レンズを使用して半球状の画像を撮影します。次に、対象となるカメラの魚眼設定 『96ページの"魚眼 (レンズ)"参照』によって、これを平面に投影します。
ライセンスキー	必要であれば、特別な魚眼用ライセンスキーを入力して、OK をクリックします。ハードウェアデバイスに取り付けられているカメラの魚眼用設定をすることができます。

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。

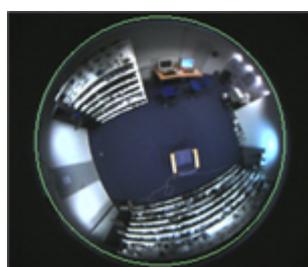
魚眼 (レンズ)

※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。

特定のカメラについてビデオや録画を設定 『57ページの"ビデオや録画の設定について"参照』する場合、魚眼のプロパティが使用できる場合があります：魚眼は、高度なレンズを使用することで 360 度パノラマビデオを再生できる技術です。

以下のような一定の条件を満たすまでは、魚眼のプロパティは表示されません。カメラは、専用の魚眼カメラであるか、特殊な魚眼レンズを装着したカメラでなければなりません。また、特別な魚眼ライセンスキーも必要です。魚眼カメラを取り付けたハードウェアデバイスを設定 『51ページの"ハードウェアデバイスの設定"参照』する時にキーを入力します。

魚眼レンズの実際の画像エリアが丸で囲まれるまで、魚眼ビューの緑色の丸で示される魚眼ビューフィールドを調整して、カメラの魚眼機能を設定します。これで、設定が魚眼テクノロジーによって使用され、丸い魚眼ビューがフラットな長方形のビューに変換されます。



名前	説明
天井取り付け	カメラが天井に取り付けられている場合、チェックボックスを選択して、これを反映するようにプロパティを調整します。
解像度	解像度の値は、自動的に魚眼画像の上に表示されます。魚眼を使用する場合、解像度は自動的に可能な限り高い値に設定されます。

名前	説明
X 半径	緑色の丸の水平(X)方向の半径を調整します。スライダーを左へ移動させるほど丸が小さくなり、右へ動かすと丸が大きくなります。または、スライダーの横のフィールドで 0~800 の値を指定することもできます。スライダーの左端は 0 に相当し、右端は 800 に相当します。
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。
X の中心	緑色の丸の水平(X)方向の位置を調整します。必要に応じて、スライダーを左右へ移動させます。または、スライダーの横のフィールドで 0~800 の値を指定することもできます。
Y の中心	緑色の丸の垂直(Y)方向の位置を調整します。スライダーを左へ移動させると丸は上に、右へ動かすと丸は下に移動します。または、スライダーの横のフィールドで 0~800 の値を指定することもできます。
プレビューを有効化	設定に基づいて、丸い魚眼ビューとフラットな長方形のビューを切り替えます。フラットなビューをプレビュー表示する場合、以下のナビゲーションボタンが使用可能になり、フラットなビュー内を移動できます。
ホームとして設定	ナビゲーションボタンを使用して、適切なビューポイントへ移動した後を使用します。現在のビューポイントをホーム位置（デフォルト位置）に設定します。カメラを表示するクライアントユーザーが、クライアントのホームボタンをクリックすると、カメラの視点がこの位置に切り替わります。
ボタン	説明
	フラットなビューを上へ移動
	フラットなビューを左上へ移動
	フラットなビューを右上へ移動
	フラットなビューを左へ移動
	フラットなビューをホームポジションへ移動（デフォルト位置）
	フラットなビューを右へ移動
	フラットなビューを左下へ移動
	フラットなビューを下へ移動

名前	説明
	フラットなビューを右下へ移動
	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)

PTZ 設定

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) カメラを取り扱っている場合だけです。

PTZ 設定を使用すると、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 『172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 (以下を参照) 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をサポートしていないカメラは、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。したがって、Milestone では、モーション検知や PTZ でそのようなデバイスを設定している場合は、Recording Server サービスを停止 『178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 『29ページ』、も参照してください。

名前	説明
PTZ タイプ	<p>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。</p> <ul style="list-style-type: none"> 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	<p>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、XProtect Enterprise で使用できます。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。</p>
新規追加	<p>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。</p> <p>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。</p>
新しい位置を設定	<p>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。</p>

名前	説明
削除	<p>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。</p> <p>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ので、インポート/更新ボタンをクリックすれば、削除したプリセット位置を XProtect Enterprise に復元できます。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 で使用したい場合、再度使用するには手動での設定が必要になります。</p>
テスト	<p>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。</p>
PTZ コントロールホイール	<p>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。</p>

PTZ パトロール

複数の同時ビデオストリームをサポートしていないカメラは、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。したがって、Milestone では、モーション検知や PTZ でそのようなデバイスを設定している場合は、Recording Server サービスを停止 『178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 『29ページ』、も参照してください。

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、**パトロールプロファイル**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、パトロールプロファイル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プロファイルを指定できます。このようなパトロールプロファイルが役に立つのは、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プロファイルに従ってパトロールを行ない、閉店後は別のパトロールプロファイル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した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、単一のパトロールプロファイル名を複数の 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プロファイル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。

パトロールプロファイルリストから、設定したいパトロールプロファイルを選択します。

名前	説明
新規追加	<p>新しいパトロールプロファイルをリストに追加します。新しいパトロールプロファイルを追加する場合、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。</p> <p>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。</p>
削除	<p>既存のパトロールプロファイルを削除します。選択したパトロールプロファイルは、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。</p>

パトロールリスト

パトロールプロファイルリストでパトロールプロファイルを選択すると、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。

名前	説明
待ち時間 (秒)	<p>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、パトロールプロファイル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。</p>

名前	説明
移行時間 (秒)	<p>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、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。</p> <p>移行時間は、パトロールプロファイル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プロファイル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だけの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。</p>

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プロファイルと連結しています。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 『98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	<p>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。</p> <p>例：</p> <ul style="list-style-type: none"> ○ 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 『178 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をサポートしていないカメラは、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。したがって、Milestone では、モーション検知や PTZ でそのようなデバイスを設定している場合は、Recording Server サービスを停止 『178 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 『29 ページ』、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、**非表示アイテムの表示**を選択します。

マイクまたはスピーカーの設定

1. **拡張設定**を展開し、**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 『57 ページの"スピーカープロパティ"参照』を指定します。

XProtect Enterprise のマイクやスピーカーの設定内容は、非常に簡単なものです。音量等の設定は、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や録画を設定 『57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、XProtect Enterprise 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、新しい名前の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ではないか確認する必要があります。

録画設定

名前	説明
常時	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	ビデオを録画している時だけ、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。音声を録音しなくても、Smart Client でライブ音声を聞くことは可能であることを注意してください。

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、XProtect Enterprise 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 XProtect Enterprise 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、XProtect Enterprise 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。マスター/スレーブ設定で複数の XProtect Enterprise 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。これは、専用の入力/出力デバイスにも適用されます。

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 XProtect Enterprise 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 XProtect Enterprise 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 『110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

XProtect Enterprise で、アクションを自動的にトリガするために、システムではさまざまな種類のイベントや出力を使用することができます。アクションの例：カメラでの録画の開始や停止、特定のビデオフレームレートへの切り替え、通知のトリガ、PTZ カメラを特定のプリセット位置へ移動させる等。また、イベントを使用してハードウェア出力をアクティブにすることも可能です。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

イベントのタイプ :

名前	説明
アナリティックイベント：	<p>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することも可能です。</p> <p>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。</p> <p>※本機は、アナリティックイベントには対応していません。</p>
ハードウェア入力イベント：	<p>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、XProtect Enterprise でイベントを生成することができます。</p> <p>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。</p> <p>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、XProtect Enterprise 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。</p> <p>最後に、ハードウェア入力イベントは、XProtect Enterprise においてカメラからのビデオのモーション検知と、XProtect Enterprise でモーション検知の設定に基づいて発生させることもできます。</p> <p>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 XProtect Enterprise 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。</p>
ハードウェア出力：	<p>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 XProtect Enterprise 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。</p>

名前	説明
手動イベント：	<p>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。</p> <p>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。</p> <p>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。</p> <p>例：</p> <p>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。</p>
ジェネリックイベント：	<p>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 XProtect Enterprise 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。</p>
イベントでの出力コントロール：	<p>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）。</p> <p>出力コントロールを設定する場合、XProtect Enterprise 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。</p>

いずれかのタイプのイベントを設定する前に、たとえば **XProtect Enterprise** 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。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、**XProtect Enterprise** 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 **XProtect Enterprise** 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。これは、専用の入力/出力デバイスにも適用されます。

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を XProtect Enterprise に追加すると、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が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 XProtect Enterprise 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 『110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なら、ハードウェア入力イベントの追加 『109ページ』、ジェネリックイベントの追加 『111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 『116ページの"アナリティックイベント"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。

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された入力ユニットから受信した入力を XProtect Enterprise でのイベント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. Management Application のナビゲーションペインで、**拡張設定**を展開してから、**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を右クリックして、**新しい入力イベントを有効にする**を選択します。
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、必要なハードウェアデバイスを展開して、定義済みのハードウェア入力を確認します。
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。対象のカメラに関して、XProtect Enterprise でモーション検知

『91ページの"モーション検知と領域の除外"参照』が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。XProtect Enterprise の以前のバージョンでは、これは **VMD イベント**と呼ばれていました。

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 XProtect Enterprise システムに追加できます。追加すると、イベント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. Management Application のナビゲーションペインで、**拡張設定** を展開してから、**イベントと出力** を展開します。ハードウェア出力を右クリックして、**新しい出力の追加** を選択します。
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、必要な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 『91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 『172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 『137ページの"オンライン期間"参照』する場合は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 『103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 『147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. Management Application のナビゲーションペインで、**拡張設定**を展開してから、**イベントと出力**を展開します。手動イベントを右クリックして、**新しい手動イベントの追加**を選択します。
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

XProtect Enterprise が受信した TCP および UDP データパッケージを分析します。特定の基準が満たされると、イベントを自動的にトリガします。この方法で、XProtect Enterprise 監視システムを、たとえば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非常に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。受信した TCP および UDP パケットの分析に基づくイベントは、ジェネリックイベントと呼ばれます。

1. Management Application のナビゲーションペインで、**拡張設定**を展開してから、**イベントおよび出力**を展開します。**ジェネリックイベント**を右クリックして、**新しいジェネリックイベントの追加**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、必要なプロパティ 『122ページの"ジェネリックイベント"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。

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 『122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 『110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、XProtect Enterprise 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. **拡張設定**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 『127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。

ヒント: まだ適切なイベントや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。**イベントの設定リスト**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 **XProtect Enterprise** 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. **拡張設定**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

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 『193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。

既に説明したとおり、**VCA** ベースのイベントを使用する場合は、データを **XProtect Enterprise** に配信するために、大半の場合にサードパーティー製の **VCA** ツールが必要です。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** に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。

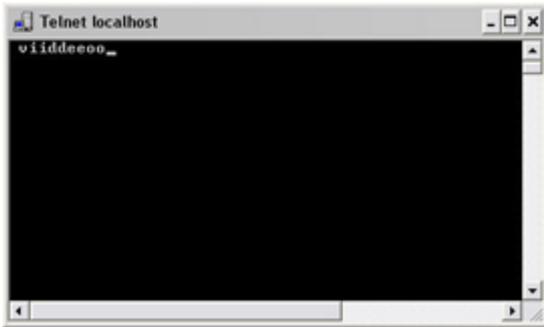
この例では、**Video** と呼ばれるジェネリックイベントを作成しています。このジェネリックイベントでは、受信した TCP データパッケージに **Video** という単語が出現すると、ジェネリックイベントをトリガするように指定しています。使用するジェネリックイベントでは異なるかもしれませんが、概要は以下の通りです。

1. **Management Application** のナビゲーションペインで、**拡張設定**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. **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。
 - XProtect Enterprise 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：XProtect Enterprise 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`

この操作で、**Telnet** ウィンドウが開きます。

上の例で、数字 **1234** は XProtect Enterprise 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。

6. **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。

7. **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。
8. **XProtect Smart Client** へ移動します。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。



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。

名前	説明
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。

名前	説明
SMTP イベントポート	ハードウェアデバイスから XProtect Enterprise 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。デフォルトポートは 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。デフォルトポートは 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 『50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、XProtect Enterprise 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

※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 『109ページの"アナリティックイベントの追加"参照』を設定する際は、以下を指定します。

名前	説明
名前	イベントの名前を入力します。
説明	説明 (オプション) を入力します。
テストイベント	このボタンをクリックすると、イベントの妥当性をテストします (オプション)。 ヒント: アナリティックイベント作成/編集プロセスの任意のステップで、このテストを何度でも実行できます。

イベントのテストをクリックすると、ウィンドウが開き、アナリティックイベントが動作する上で満たさなければならない多数の条件が実行されます。このウィンドウには 2 つのタブがあります。タスクとエラーです。

タスクタブには、テストする条件が一覧表示され、失敗：✖または成功：✔がマークされます。エラータブには、失敗した条件に対応するエラーのリストが表示されます。

テスト中は必ず変更内容を保存してください。

完了したら、XProtect Smart Client アラームリストでテストイベントの有無をチェックします。アラームをテストするタイプで並び替えて、テストイベントがアラームリストの一番上に表示されるようにします。詳細については、XProtect Smart Client マニュアルを参照してください。

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。
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。
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?	Analytics 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:使用しているマシンをアナリティックイベントアドレスリストへ許可される IP アドレス/ホスト名として追加します。 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。
アラーム定義で使用されているアナリティックイベント	アナリティックイベントは、いずれかのアラーム定義で有効に使用されていますか?	アナリティックイベントは、どのアラーム定義でも使用されていません。解決策/説明:アラーム定義でアナリティックイベントを使用してください。
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?	下のテーブルを参照してください。

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:

エラーメッセージ	解決策/説明
イベントサーバーが見つかりません。	Event Server サービスが登録済みサービス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 Event Server サービスに接続できません (通常は、ネットワーク障害、Event Server サービスの停止などの理由による)。
アナリティックイベントの送信エラーが発生しました。	Event Server サービスへの接続は確立されましたが、イベントを送信できません (通常は、タイムアウトなどのネットワークの問題による)。

エラーメッセージ	解決策/説明
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。	イベントがイベントサーバーに送信されましたが、応答がありません（通常は、ネットワークの問題やポートがビジー状態のため（一般的に、ProgramData\Milestone\XProtect Event Server\logsにあるイベントサーバーログを Microsoft メモ帳などのツールで開いて確認してください））。
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。	Event Server サービスがイベントを認識していません。これは通常、イベントまたはイベントの変更が保存されていないためです。
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。 イベントサーバーログを Microsoft のメモ帳などのツールで開きます。ログは、通常は、ProgramData\Milestone\XProtect Event Server\logsにあります。
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、ネットワークの問題の可能性がります。 イベントサーバーログを Microsoft のメモ帳などのツールで開きます。ログは、通常は、ProgramData\Milestone\XProtect Event Server\logsにあります。
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。ポートがビジー状態か、ネットワークの問題の可能性がります。 イベントサーバーログを Microsoft のメモ帳などのツールで開きます。ログは、通常は、ProgramData\Milestone\XProtect Event Server\logsにあります。
予期しないエラーが発生しました。	システムプロバイダー Milestone のサポート (support@milestonesys.com) にお問い合わせください。

ハードウェア入力イベント

ハードウェア入力イベントを追加 『109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、一部のプロパティは選択した入力のタイプに依存します。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
有効化	選択したタイプの入力を XProtect Enterprise 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。

名前	説明
イベント名	<p>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。 < > & ' " ¥ / : * ? []</p> <p>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。</p>
カメラからの画像	<p>アラーム前後の画像を使用する場合にのみ関係します。これは選択したカメラでのみ使用可能な機能で、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ます。アラーム前後の画像と、XProtect Enterprise 独自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 『86ページの"記録(録画)"参照』を混同しないように注意してください。アラーム前後の画像を送信するためのカメラを選択します。</p>
プリアラーム画像の数	<p>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。プリアラーム画像の必要数を指定します。可能な数はカメラによって異なります。可能な範囲はフィールドの右側に表示されます。</p>
秒当りのフレーム数	<p>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。</p>
このイベントが発生すると、Eメールを送信します	<p>Eメール通知 『148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。イベントが発生した場合に、XProtect Enterprise で Eメール通知を自動送信する必要がある場合は選択します。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にも注意してください。</p>
カメラからの画像を添付します	<p>Eメール通知 『148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。</p>
削除	<p>選択したイベントを削除します。</p>
追加	<p>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。</p>

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

<p>イベント発生時、SMSを送信する</p>	<p>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。</p> <p>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。</p>
-------------------------	--

ハードウェア出力

ハードウェア出力を追加 『110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。

名前	説明
出力名	<p>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。 < > & ' " ¥ / : * ? []</p> <p>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。</p>
出力接続先	<p>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。</p>
出力維持時間	<p>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。</p> <p>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。正確な情報は、対象となる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。</p>

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

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。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
【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 『148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。イベントが発生した場合に、XProtect Enterprise で Eメール通知を自動送信する必要がある場合は選択します。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にも注意してください。
カメラからの画像を添付します	Eメール通知 『148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。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

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。

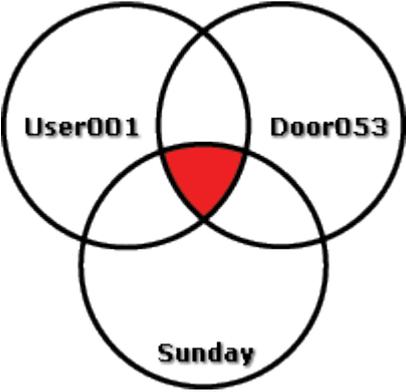
名前	説明
タイマーイベント名	名前を指定します。名前は一意であり、以下の特殊文字を含むことはできません。 <> & ' " ¥ / : * ? [] 一部のカメラは、特定の長さおよび特定の構造のイベント名しかサポートしていません。詳細はカメラのマニュアルを参照してください。
タイマーイベント発生前	メインイベントの発生からタイマーイベントまでに経過する必要がある時間の長さ（秒または分単位）を指定します。

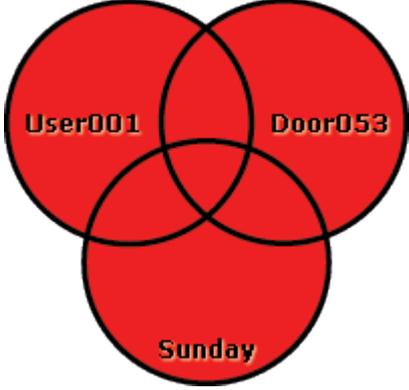
ジェネリックイベント

ジェネリックイベントを追加 『114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。

名前	説明
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、XProtect Enterprise 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。

名前	説明
イベントの部分列	<p>データパッケージを分析する際に、XProtect Enterprise で探すべき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：</p> <ul style="list-style-type: none"> ● 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） <p>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はあるが、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）。</p> <p>ヒント：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、@、#、+、ã、~等の特殊文字を分析する文字列で使用することができます。</p>
イベントメッセージの表現	<p>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。</p> <ul style="list-style-type: none"> ● (： 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、XProtect Enterprise 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。

名前	説明
	<ul style="list-style-type: none"> 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。一般原則として、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。  <p>AND を組み合わせると、結果 (赤色で表示) が少なくなります。</p> <ul style="list-style-type: none"> 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。

名前	説明
	 <p>OR を組み合わせると、結果（赤色で表示）が多くなります。</p> <ul style="list-style-type: none"> 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	<p>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。XProtect Enterprise 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。</p>
イベントプロトコル	<p>イベントを検知するために XProtect Enterprise 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。</p> <ul style="list-style-type: none"> 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し、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し、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し、分析します。

名前	説明
イベントルールタイプ	<p>受信したデータパッケージを分析する時に特定の XProtect Enterprise があるべき状態を選択します。</p> <ul style="list-style-type: none"> 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、他の内容も含まれている可能性があります。例：受信したパッケージに「User001」および「Door053」が含まれるよう指定した場合、受信したパッケージに語句「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ず、他の内容が含まれてはなりません。
このイベントが発生すると、Eメールを送信します	<p>Eメール通知 『148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。イベントが発生した場合に、XProtect Enterprise で Eメール通知を自動送信する必要があるらば選択します。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にも注意してください。</p>
カメラからの画像を添付します	<p>Eメール通知 『148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。</p>
イベント発生時、SMSを送信する	<p>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。</p> <p>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。</p>
削除	<p>選択したイベントを削除します。</p>
追加	<p>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。</p>

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。

名前	説明
イベント	必要なイベントを選択します。
出力	必要な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 『127ページの"アーカイブについて"参照』 を実行する時期
- 一部のカメラから、常に XProtect Enterprise 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することも可能です。セットアップできる場合：

- 1つ以上のカメラがオンラインである場合 (そのカメラからビデオを XProtect Enterprise へ転送)
- 1つ以上のカメラがスピードアップを使用している場合 (そのカメラは、通常より高いフレームレートを使用)
- 1つ以上のカメラに関する通知 『147ページの"通知について"参照』 を受信したい場合
- アーカイブが発生した場合
- PTZ カメラは、パトロールプロファイルに従って、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 を保存することができます。XProtect

Enterprise は、カメラのデータベースが満杯になると、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。

XProtect Enterprise 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を設定を変更できます。また、アーカイブ 『131ページの"アーカイブスケジュールについて"参照』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。

XProtect Enterprise は、カメラのデータベースが満杯になると、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 『64ページの"録画およびアーカイブのパス"参照』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を推奨していません。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、XProtect Enterprise にとって、これは問題にはなりません。XProtect Enterprise 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 『203ページの"デフォルトのファイルパス"参照』

(D:\MediaDatabase) は、XProtect Enterprise 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：

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

他の場所へのアーカイブについて

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

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。

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レコーディング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レコーディング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。XProtect Enterprise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。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可能性があります。ルールは、「録画と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、アーカイブは失敗します。

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。すべてのサーバーで同じ場所にアーカイブしようとする、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、XProtect Enterpriseは、アーカイブするデータに必要な容量に1GB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、アーカイブ場所で、対象となるカメラから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 Worst Case 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 『35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、**拡張設定**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 『136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ています。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ています。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 Xprotect Smart Client の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. Management Application のナビゲーションペインで、**拡張設定**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。
2. すべてのカメラのスケジュール 『133ページ』、スケジュールオプション 『135ページ』、アーカイブ 『136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 『12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。

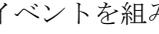
一般的なスケジュールのプロパティ

すべてのカメラのスケジュール

一般的なスケジュールおよびアーカイブ 『133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。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
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、レコーディングパス、アーカイブパス、およびそれらすべての保持時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	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	<p>関連するカメラのオンラインスケジュール 『60ページの"カメラ固有のスケジュールの設定"参照』に必要なプロファイル（例：常にオン）を選択します。</p> <p>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。</p> <ul style="list-style-type: none"> 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： <p>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。</p>
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。
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。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

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 通知の期間を指定します（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 (パン/チルト/ズーム) 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 パトロールのスケジュール 『138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できます。 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 『133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。

名前	説明
クライアントからの要求によるカメラ起動	たとえば、オンライン録画スケジュール 『137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はできません。ただし、 クライアントからの要求によるカメラ起動 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レコーディングを有効にする 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レコーディングを有効にする	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）。 手動レコーディングの権限 『174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レコーディングを有効にする を有効化してもそのユーザーによる手動レコーディングは行えません。

名前	説明
新規カメラのスケジュールプロファイル	XProtect Enterprise システムへ後で追加するカメラが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。これは、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 XProtect Enterprise サーバーに転送することを意味します。
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。XProtect Enterprise がカメラへの接続を失うと、デフォルトでは、10 秒後に接続を再確立できるように試行します。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することもできます。これを行うには、クライアントからの要求による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レコーディングを有効にするオプションを選択します。

アーカイブ

XProtect Enterprise は、カメラのデータベースが満杯になると、自動的に録画をアーカイブ 『127ページの"アーカイブについて"参照』 します（以前のバージョンでは、これはそれぞれのカメラに対して個別に設定するオプションでした）。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

名前	説明
アーカイブ時刻	XProtect Enterprise で自動的に録画をアーカイブパスへ移動させたい時刻を指定します。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 メールを送信します	選択した場合、アーカイブが失敗すると、XProtect Enterprise は自動的に選択した受信者に E メールを送信します。これには、E メール通知機能が有効になっている必要があります。受信者は、E メール通知のプロパティ 『148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。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

アーカイブ障害時に SMS を送信	<p>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る場合は選択します。SMS 通知設定の一部として SMS 通知の受信者を定義します。</p> <p>設定ができるのは、SMS 通知が有効である場合だけです。</p>
-------------------	--

XProtect Enterprise でのみ使用可能なプロパティ：

イベントでのアーカイブ	<p>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。</p>
-------------	--

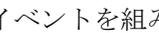
カメラ固有のスケジュールプロパティ

オンライン期間

特定のカメラについてスケジュール 『60ページの"カメラ固有のスケジュールの設定"参照』を設定する場合、おそらく最も重要なのは**オンライン期間**設定です。これは、オンライン期間によって、それぞれのカメラがいつビデオを XProtect Enterprise へ転送するかを決定するためです。

デフォルトでは、XProtect Enterprise 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。ただし、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 『135ページの"スケジュールオプション"参照』の一部として、このデフォルトが変更されている可能性があります。

カメラが XProtect Enterprise にビデオを転送しても、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。録画は別途設定します。ビデオおよび録画の設定 『57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。

名前	説明
オンライン	<p>関連するカメラのオンラインスケジュール 『60ページの"カメラ固有のスケジュールの設定"参照』に必要なプロファイル（例：常にオン）を選択します。</p> <p>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。</p> <ul style="list-style-type: none"> 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： <p>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。</p>

ヒント：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い場合は、クライアントからの要求によるカメラ起動『135ページの"スケジュールオプション"参照』を選択し、必要に応じて、クライアントからの要求で開始した際にレコーディングを有効にする『135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

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です。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）『74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）『82ページの"ビデオ"参照』を参照してください。

名前	説明
スピードアップ	特定の MJPEG カメラについて、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『74ページの"フレームレート - MJPEG"参照』にする必要があります。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： 

PTZ パトロール

パトロール『100ページの"PTZ パトロール"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『60ページの"カメラ固有のスケジュールの設定"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。

名前	説明
PTZ パトロール	PTZ（パン/チルト/ズーム）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 パトロールのスケジュール『138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できます。 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）を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 『60ページの"カメラ固有のスケジュールの設定"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

Matrix 機能では、XProtect Enterprise を操作することで、任意のカメラから、ネットワーク上の Matrix 受信 PC へのライブビデオの配信が可能です。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情報は、XProtect Smart Client ユーザーマニュアル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 PC について

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 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 PC に関する詳細情報は XProtect Smart Client のユーザーマニュアルを参照してください。

Matrix の設定

1. 拡張設定を展開し、**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 『140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** 『141ページの"**Matrix イベントコントロール**"参照』を設定します。準備ができたなら **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

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。

名前	説明
Matrix 有効化	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。そのため、分かりやすく誤解を招かない名前を使用することを推奨します。 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。

名前	説明
ポート	Matrix 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 を使用しますが、当然、他のポート番号を指定することもできます。
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 Smart Client です	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

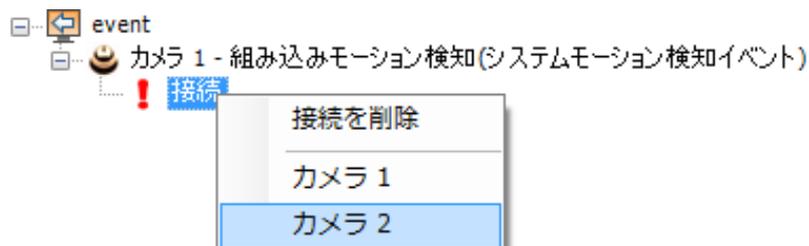
Matrix イベントコントロールタブを使用して、事前定義イベントに基づくライブビデオの自動送信を設定します。Matrix 受信 PC ごとに、どのイベントやカメラを使用するか、正確に定義することができます。Matrix イベントコントロールタブには、Matrix 受信 PC タブで定義した Matrix 受信 PC のリストが表示されます。

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。

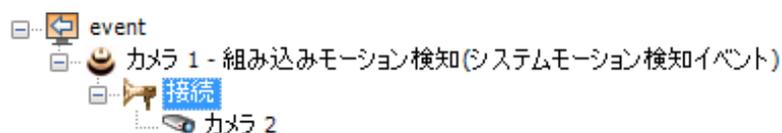
コンポーネント	要件
削除 [選択したイベント]	選択したデバイスで、選択したイベントを削除します。
接続	カメラに接続します（実際のカメラは、取るべきアクションを選択した後に指定します）。

コンポーネント	要件
遮断、続いて接続	<p>既存の接続を切断し、その後再度接続します。</p> <p>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。</p> <p>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。</p>
遮断	<p>既存の接続をすべて切断します。ビデオが「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。</p>

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 2 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 2 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	説明
Management Application ログファイル	<p>Management Application の活動を示します。Management Application 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。</p> <p>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。</p>
Recording Server サービスログファイル	<p>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。</p> <p>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。</p>
Image Server サービスログファイル	<p>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。</p> <p>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。</p>
Image Import サービスログファイル	<p>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する際に使用されます。</p> <p>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。</p> <p>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_YYYYMMDD.log という構造になります。たとえば、ImageImportLog20091231.log などです。</p>

名前	説明
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、is_auditYYYYMMDD.log という構造になります。たとえば、is_audit20091231.log などです。「is_」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込まれます。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	説明
Log integrity information was not found. Log integrity can't be guaranteed.	ログファイルの整合性をチェックできませんでした。
Log information does not match integrity information. Log integrity can't be guaranteed.	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。
[Log file name] not found	ログファイルが存在しませんでした。
[Log file name] is empty	ログファイルは存在しましたが、空白でした。
Encrypted data missing in [log file name] near line [#]	ログファイルの最後の行が、検証基準を満たしません。
Encrypted data missing in [log file name] near line [#]	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。
Inconsistency found in [log file name] near line [#]	ログファイルが、暗号化部分と一致しません。
Inconsistency found in [log file name] at beginning of log file	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

XProtect Enterprise 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. **拡張設定**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 『145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

XProtect Enterprise 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。

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)

名前	説明
パス	<p>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。</p> <p>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。</p>
ログ保存日数	<p>Management Application および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30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となります。</p>

イベントログ

名前	説明
パス	<p>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。</p> <p>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。</p>
ログ保存日数	<p>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となります。</p>

監査ログ

名前	説明
監査ログの有効化	監査ログは、XProtect Enterprise 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。XProtect Enterprise は、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 『91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、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 『127ページの"アーカイブについて"参照』が失敗した場合（アーカイブプロパティ 『136ページの"アーカイブ"参照』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. **拡張設定**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 『148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。

名前	説明
有効化	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。

名前	説明
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。 <ul style="list-style-type: none"> 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『153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。

コンポーネント	要件
画像を含む	<p>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。</p> <p>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。</p> <p>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い場合は、送信される E メール通知には画像は含まれません。</p>

コンポーネント	要件
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。

コンポーネント	要件
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メール通知の送信で使用したい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	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。
パスワード	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サーバーの使用に必要なパスワードを指定します。
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 での通知には対応していません。

SMS について

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

SMS 通知は次のように設定します。

1. **拡張設定**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)

SMS 通知のメッセージ設定には以下の項目があります。

コンポーネント	要件
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。 <ul style="list-style-type: none"> 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『153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)

SMS 通知のサーバー設定には以下の項目があります。

コンポーネント	要件
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。

コンポーネント	要件
SMS エンコーディング	<p>世界中のさまざまな言語に対応するために、さまざまな種類の SMS エンコーディングが存在しています。XProtect Enterprise には、以下のオプションがあります。</p> <ul style="list-style-type: none"> • 7 ビット • 8 ビット (デフォルト) • 16 ビット <p>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。</p> <p>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。</p> <p>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 XProtect Enterprise 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。</p>

スケジュール

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『148ページの"メッセージ設定(Eメール)"参照』や SMS『151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。

コンポーネント	要件
通知プロファイル	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> 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。Milestone 統合プラットフォーム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 Milestone 統合プラットフォームのログイン設定を指定するダイアログでもあります。

XProtect Central の有効化

1. **拡張設定**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

名前	説明
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。

名前	説明
ログイン名	XProtect Enterprise と Central サーバー、または Milestone 統合プラットフォーム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 Milestone 統合プラットフォームの間で一致している必要があります。
パスワード	XProtect Enterprise と Central サーバー、または Milestone 統合プラットフォームの間で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 Milestone 統合プラットフォーム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 Milestone 統合プラットフォームが、XProtect Enterprise サーバーへアクセスする際に接続する必要が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 Milestone 統合プラットフォーム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 Control Module 2014>を使用する場合、この機能の使用を許可するライセンスを購入しておく必要があります。

XProtect <Access Control Module 2014>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 Control Module 2014>を使用することができます。

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
- 追加機能（以下参照）

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

- アクセスコントロール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
- アクセスコントロールイベントの調査
- ドア状態の概要と制御の一元化
- カードホルダー情報

統合を開始する前に、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。

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。

このウィザードの手順：

アクセスコントロールシステム統合の作成.....	156
アクセスコントロールシステムへの接続.....	157
関連付けられたカメラ.....	157
最終的な概要.....	157

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。

関連付けられたカメラ

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、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。

Management Client で、この構成を改良することができます。

アクセスコントロールプロパティ

一般設定タブ(アクセスコントロール)

名前	説明
有効化	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、新しい名前の上書きすることができます。
説明	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	説明
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。

名前	説明
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。
パスワード	ユーザーのパスワードを指定します。

関連付けられたカメラタブ(アクセスコントロール)

ドアのアクセスポイントとカメラ、マイク、スピーカーの間で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	説明
ドア	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
カメラ	<p>XProtect システムで設定されているカメラをリストします。</p> <p>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。</p>

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	説明
アクセスコントロールイベント	<p>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。</p> <p>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。</p>
ソースタイプ	<p>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。</p>
イベントカテゴリ	<p>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。</p> <p>統合イベントカテゴリは、以下のとおりです。</p> <ul style="list-style-type: none"> ▶ 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 <p>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。</p> <p>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。</p>

名前	説明
ユーザー定義カテゴリ	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>

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	説明
イベントのトリガ	<p>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。</p> <p>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。</p> <p>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づくトリガが作成されます。</p> <p>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。</p>

<p>ソース</p>	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • すべてのドア • 個々のドア • その他... <p>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。</p> <p>外部イベントの場合：</p> <p>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。</p>
<p>時間プロファイル</p>	<p>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。</p> <p>拡張設定の一部として、時間プロファイルを設定します。</p>
<p>アクション</p>	<p>アクションのタイプの選択：</p> <ul style="list-style-type: none"> • 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 <p>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。</p> <p>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。</p>
<p>アクセスコントロールアクションの追加</p>	<p>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。</p>

<p>アクションの詳細</p>	<p>アクションのパラメータを設定 :</p> <p>アクセスリクエスト通知を表示 :</p> <ul style="list-style-type: none"> ▶ 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。 <p>PTZ プリセットに移動 :</p> <ul style="list-style-type: none"> ▶ 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。 <p>記録の開始 :</p> <ul style="list-style-type: none"> ▶ 所定のイベントが発生した場合に、記録を開始するカメラおよび期間を指定します。 <p>システムアクション :</p> <ul style="list-style-type: none"> ▶ 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。
<p>コマンドの追加</p>	<p>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。</p> <p>関連するアクセスリクエストコマンド :</p> <ul style="list-style-type: none"> ▶ 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。 <p>すべての関連コマンド :</p> <ul style="list-style-type: none"> ▶ ソースユニットで、すべてのコマンドを有効にします。 <p>アクセスコントロールコマンド :</p> <ul style="list-style-type: none"> ▶ 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。 <p>システムコマンド :</p> <ul style="list-style-type: none"> ▶ 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。 <p>コマンドを削除するには、右側で X をクリックします。</p>

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	説明
カードホルダーの検索	カードホルダーの名前の文字を入力すると、存在する場合はリストに表示されます。
名前	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。 <ul style="list-style-type: none">▶ 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	説明
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。

- **拡張設定**：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	説明
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。
説明	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. **拡張設定**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

サーバーアクセスを設定 『165ページの"サーバーアクセスの設定"参照』 (つまりシステムサーバーへのクライアントのアクセス) する場合、以下を指定します。

名前	説明
サーバー名	XProtect Enterprise 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でき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は、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、XProtect Enterprise 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。

名前	説明
最大クライアント数	<p>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。 XProtect Enterprise の設定や、使用しているハードウェアやソフトウェアの性能によって、同時に接続するクライアントの数を制限することで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ている場合、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。</p> <p>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したい場合は、値を上書きしてください。</p> <p>ヒント： 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。</p> <p>XProtect Enterprise 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期間が適用されます。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期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までに 4 分が経過する必要があります。</p>

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。

1. 追加ボタンをクリックします。
2. 開始アドレス欄で、範囲の最初の IP アドレスを指定します。
3. 終了アドレス欄で、範囲の最後の IP アドレスを指定します。

必要なだけ繰り返して、他のローカル IP 範囲も追加します。

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。

コンポーネント	要件
文字エンコード/言語	<p>必要な言語/文字セットを選択します。</p> <p>例：監視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のサーバーと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。</p>

マスター/スレーブ

マスターおよびスレーブについて

システムサーバーのマスター/スレーブのセットアップを行うことができます。マスター/スレーブのセットアップを行うことで、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へもアクセスできるようになります。

スレーブサーバーの接続をチェックするには、**ステータスの更新**をクリックしてスレーブへの接続をチェックし、接続されているスレーブの数をシステムにレポートさせます。

マスターおよびスレーブサーバーの設定

1. **拡張設定**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。準備ができたなら **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

XProtect Enterprise および **XProtect Professional** でのみ使用可能なプロパティ：

名前	説明
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。

XProtect Enterprise でのみ使用可能なプロパティ：

バージョン 8.0 以前のスレーブ	これを選択すると、バージョン 8.0 以前のバージョンの XProtect Enterprise を実行するスレーブがサポートできます。 バージョン 8.0 以前のスレーブを選択すると、すべてのスレーブ (8.0 以前およびそれ以降) のスレーブ状態更新機能が無効になります。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。
-------------------	--

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

名前	説明
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の更新

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、ステータスの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。

バージョン 8.0 より前のスレーブを選択すると、全スレーブでスレーブステータスの更新ができなくなります。そのためステータスの更新が無効になります。スレーブ設定の概要テーブルでは全スレーブでスレーブサーバーのステータスが適用外となります。
バージョン 8.0 より前のスレーブを選択していなければ、バージョン 8.0 より前のスレーブのスレーブ

ステータスはアクセス不能になります。バージョン 8.0 以降のスレーブのスレーブステータスには、実際のステータスが反映されます。

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 『170ページ』および Windows ユーザーの追加 『171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、管理目的のデフォルトの **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。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. **拡張設定**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（または、XProtect Enterprise 2013+ および XProtect Professional 2013+ でサポートされている Active Directory®から）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. **拡張設定**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。

デフォルトでは、ユーザーはディレクトリ全体からですが、以下をクリックして、これを絞り込むことができます。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、Active Directory®などの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 『172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

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. **拡張設定**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 『173ページ』およびカメラアクセス 『174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 『170ページ』または **Windows** ユーザーの追加 『171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 『170ページ』、**Windows** ユーザーの追加 『171ページ』、ユーザーグループの追加 『171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 『47ページ』でも追加できることに注意してください。ただし、ウィザードを使用すると、追加するすべてのユーザーが、後の段階で追加する新しいカメラを含めて、すべてのカメラに対してアクセスできるようになります。

後の段階で、ユーザーまたはグループの権限を編集したくなった場合：

1. **拡張設定**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. 一般アクセス 『173ページ』およびカメラアクセス 『174ページ』のプロパティを編集します。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

名前	説明
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	編集できるのは、選択したユーザーのタイプが基本ユーザーである場合だけです。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。
ユーザータイプ	選択したユーザーのタイプが基本ユーザーか Windows ユーザーグループかを表示する、編集不可のフィールドです。

グループ情報

名前	説明
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 『170ページの"基本ユーザーの追加"参照』、Windows のユーザー 『171ページの"Windows ユーザーの追加"参照』またはグループ 『171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、一般アクセスの設定を指定することができます。

名前	説明
ライブ	XProtect Smart Client のライブタブにアクセスできるかどうか。
再生	XProtect Smart Client の再生タブにアクセスできるかどうか。
設定	XProtect Smart Client で設定モードにアクセスできるかどうか。 ヒント: ライブ、再生、設定のチェックボックスを選択解除すると、ユーザー/グループが XProtect Smart Client で使用できる機能を効率良く無効にすることができます。たとえば、ユーザーが休暇中である場合などに、ユーザー/グループを削除する代替りの一時的な代替として利用することができます。

名前	説明
共有ビューの編集	<p>XProtect Smart Client の共有グループでビューを作成、編集できる機能。</p> <p>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。</p>
プライベートビューの編集	<p>XProtect Smart Client のプライベートグループでビューを作成、編集できる機能。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。</p> <p>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。</p>
管理者アクセス	<p>チェックボックスを選択すると、Management Application にアクセスし、操作できる権限をユーザーに許可します。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。</p>

カメラアクセス

基本ユーザー 『170ページの"基本ユーザーの追加"参照』、Windows のユーザー 『171ページの"Windows ユーザーの追加"参照』またはグループ 『171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、カメラアクセスの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：複数のカメラのアクセスに対して、同じ機能を使用する必要がある場合は、キーボードで **SHIFT** または **CTRL** を押しながら、複数のカメラを選択することができます。

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。

カメラの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。

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

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。
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 (照明、サイレン、ドアの開放) 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。
手動レコーディング	一定時間 (監視システムの管理者が定義 『73ページの"手動録画"参照』) の間、録画を手動で開始します。

XProtect Enterprise および XProtect Professional でのみ使用可能なプロパティ：

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。
------	---

すべての XProtect ソフトウェアのバージョンで使用可能なプロパティ：

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、証拠をエクスポートします。
データベースのエクスポート	証拠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 『173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 『170ページの"基本ユーザーの追加"参照』、Windows のユーザー 『171ページの"Windows ユーザーの追加"参照』またはグループ 『171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。

名前	説明
管理	<p>XProtect Smart Client のユーザーは、以下の操作ができます。</p> <ul style="list-style-type: none"> 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	<p>XProtect Smart Client のユーザーは、以下の操作ができます。</p> <ul style="list-style-type: none"> アラームを表示 アラームレポートを印刷します。
無効	<p>XProtect Smart Client のユーザーが、アラームを無効にできるようになります。</p>

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、Management Application から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 『178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	説明
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。
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 のインスタンスは、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、システムのレコーディング前後の機能 『86ページの"記録（録画）"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。詳細については、ログの概要を参照してください。
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。
Milestone Mobile サービス	レコーディングサーバー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、ならびにレコーディングサーバーと 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、Mobile サーバーおよびイベントサーバーをインストールしないよう選択できます。インストールしないよう選択した場合、Mobile サービスおよび Event Server サービスはサービス概要に表示されません。

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. **拡張設定**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。

サーバー

Mobile サーバー

Mobile サーバーについて

Mobile サーバーが、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を処理します。

正しいログイン情報が入力されると、Mobile サーバーは関連するレコーディングサーバーから Milestone Mobile クライアントへビデオ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。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。

直接ストリーミングについて

※本機は、直接ストリーミングには対応していません。

デフォルトでは、システムがカメラからシステムへビデオを転送する際に、Milestone Mobile サーバーはビデオ画像をカメラで使用されているコーデックから JPEG ファイルヘデコードします。このデコードのプロセスは、Milestone Mobile サーバーのリソースをかなり消費します。直接ストリーミングによって、Milestone Mobile サーバーは元のコーデックのフォーマットで画像を XProtect Web Client へ転送できるので、デコードが不要となり、そのため Milestone Mobile サーバーに対する負荷を軽減できます。

Milestone Mobile サーバーの**一般設定**で、Milestone Mobile サーバーの直接ストリーミングを有効にして、XProtect Web Client のユーザーが直接ストリーミングを使用できるようにすることができます。ただし、管理者は XProtect Web Client ですべてのユーザーが必ず直接ストリーミングを使用しなければならぬように選択することもできます。管理者がこの設定を選択すると、すべてのユーザーが必ず直接ストリーミングを使用することになります。直接ストリーミングを必須とすると、Milestone Mobile クライアントのすべてのインスタンスは接続できなくなるので、管理者は、ユーザーが厳密に

Milestone Mobile サーバーを XProtect Web Client との接続だけのために使用している場合以外はこの設定を使用してはなりません。

直接ストリーミングを使用するには、XProtect Web Client にアクセスする PC にプラグインをインストールする必要があります。XProtect Web Client は、このプラグインをインストールするかどうかを自動的にユーザーに確認します(サポートされているブラウザ経由で接続する場合)。

ビデオプッシュについて

ビデオプッシュは Milestone Mobile クライアントの機能であり、これによってモバイルデバイスのカメラを使用して、たとえばアラームやイベントを調査する際に証拠を収集できます。これは、モバイルデバイスからシステムへ、ビデオストリームを送信することによって、行われます。Mobile サーバーの設定で、システムでビデオプッシュ機能を使用できるユーザーの数を設定できます。

Mobile サーバーの追加と編集

1. 以下のいずれか 1 つを実行します。
 - 新しいサーバーを追加するには、**Mobile サーバー**を右クリックします。表示されるメニューから**新規作成**を選択します。
 - **Mobile** サーバーを編集するには、目的のサーバーを選択します。
2. 目的のプロパティを入力または編集します。
3. 右下端で、**OK** をクリックします。
4. 上部のツールバーで**ファイル > 保存**をクリックします。

重要：ログイン方法、すべてのカメラビューを有効化、出力およびイベント、およびキーフレームを有効化を編集する場合、変更を有効にするには、XProtect Mobile クライアントをシステムに再接続する必要があります。

ビデオプッシュチャンネルの追加

それぞれのビデオプッシュチャンネルには、個別にカメラのライセンスが必要です。

ビデオプッシュチャンネル 『179ページの"ビデオプッシュについて"参照』を追加するには、次の操作を実行してください。

1. **ビデオプッシュ**タブで、**ビデオプッシュ**チェックボックスを選択して、この機能を有効にします。
2. 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。
3. チャンネルは、ユーザー名を通じてデバイスにマッピングされます。システムで既にセットアップされているユーザーアカウントからユーザー名を選択して、関連するビデオプッシュチャンネルに関連付けます。(例:admin)

ビデオプッシュチャンネルを既に作成済みのユーザーと関連付けないと、ログインしても Milestone Mobile クライアントでビデオプッシュを使用することができません。

4. システムに、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追加 『180ページの"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追加する"参照』します。ビデオプッシュドライバーは自動ハードウェア検索では表示されないので、**手動**でハードウェアデバイスを検出する方法を選択しなければなりません。
5. **ビデオプッシュ**タブで、**カメラの検索**をクリックします。成功すると、新しく追加されたビデオプッシュドライバーがこのリストに表示されます。構成を保存して、ビデオプッシュドライバーを使用する準備をします。

必要ない場合には、ビデオプッシュチャンネルを削除できます。これを行うには、関連するチャンネルを選択し、右下の**削除**をクリックします。

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追加する

ビデオプッシュチャンネルを追加する場合、Management Application にビデオプッシュドライバーを追加する必要があります。操作方法：

1. Management Application で**新しいハードウェアの追加ウィザード**を開きます。
2. **手動**オプションを選択します。ビデオプッシュドライバーは、自動ハードウェア検索では検出されません。
3. 手動でハードウェアデバイス設定 『180ページの"ハードウェアデバイス設定の追加"参照』を指定し、ハードウェアドライバーを選択します。
4. 完了すると、ビデオプッシュドライバーがビデオプッシュチャンネルに関連付けられているはずです。これを行うには、**Mobile** サーバー > **ビデオプッシュ**タブに戻り、**カメラの検索**をクリックします。

ハードウェアデバイス設定の追加

ハードウェアデバイスの追加ウィザードでビデオプッシュドライバーを追加する際に、以下の設定を指定します。

名前	説明
IP アドレス	Milestone Mobile サーバーの IP アドレスを入力します。通常は本機のアドレスを入力します。
ポート	ビデオプッシュドライバーのポート番号を入力します。このポートは、Milestone Mobile サーバーと、XProtect サーバーの間での通信で使用されます。 重要 ：設定するポート番号は、ビデオプッシュの設定を指定した時と同じポート番号でなければなりません 『183ページの"ビデオプッシュ"参照』。ポート番号が同一でなければ、ビデオプッシュチャンネルは動作できません。(例：40001)

名前	説明
ユーザー名	これを追加した『179ページの"ビデオプッシュチャンネルの追加"参照』時のビデオプッシュチャンネルに関連付けられているものと同じユーザー名を選択します。(例 : admin)
パスワード	ビデオプッシュドライバーのパスワードを入力します。ビデオプッシュドライバーのパスワードは、 Milestone です (これは変更できません)。
ドライバー	Video Push Driver を選択します。

完了したら、Milestone Mobile サーバーの > **ビデオプッシュタブ**へ移動し、**カメラの検索**をクリックして、ビデオプッシュチャンネルの設定を完了させます。

Mobile サーバーの設定

一般設定

Milestone Mobile サーバーの一般設定を入力します。

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	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、特定の XProtect システムまでの間で選択します。リストには、実行中の Milestone Mobile サーバーだけが表示されます。
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 。
クライアントタイムアウト (HTTP)	Mobile 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。
ログイン方法	Mobile サーバーへのログインがどのように行われるかを選択します。以下のオプションから選択できます。 自動 、 Windows 認証 、 基本認証 。通常は基本認証を使用します。
XProtect Web Client を有効化	XProtect Web Client の使用を有効にします。 ※本機は、XProtect Web Client には対応していません。
すべてのカメラビューを有効化	すべてのカメラビューの表示を有効/無効にします。この表示には、レコーディングサーバーのすべてのカメラが含まれています (ユーザー権限で許可されている場合)。

名前	説明
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を有効/無効にします。
キーフレームを有効化	ビデオストリームを有効/無効にして、キーフレームだけをストリームします。キーフレームだけを有効にすることで、帯域幅の使用のみを減らせます。
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、このオプションを有効にすると、パフォーマンス設定のすべてのルール設定が無効になることに注意してください。 ※本機ではこの設定は表示されません
直接ストリーミング	XProtect Web Client での直接ストリーミングの処理方法を選びます。ユーザーに直接ストリーミングを強制する、可能な場合にユーザーに直接ストリーミングを強制する、あるいは直接ストリーミングの使用をまったく強制しない、のいずれかを選択します。 ※本機ではこの設定は表示されません
構成のバックアップ	Milestone Mobile サーバーの構成をインポートまたは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。

サーバーステータス

Mobile 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、Mobile サーバーが動作し続けている期間を示します。
CPU 使用状況	Mobile サーバーでの現在の CPU 使用状況を示します。
内部帯域幅	Mobile サーバーと関連するレコーディング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。
外部帯域幅	モバイルデバイスと Mobile 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。
ユーザー名	Mobile サーバーのユーザーで、Mobile サーバーに接続されているユーザー名を表示します。
ステータス	Mobile サーバーと、対象となる Milestone Mobile 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。ユーザーが接続されているか(キーおよび暗号化用の認証資格情報を交換するサーバーの準備状態)、ユーザーが実際にログインしているかのいずれかを、 接続中 または ログイン で表示します。

名前	説明
帯域幅使用状況	対象となる Mobile 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。
ライブストリーム	対象となる Milestone Mobile クライアントのユーザーに対して現在開かれているビデオストリームの数を表示します。
ストリームの再生	関連する Mobile クライアントユーザーに対して現在開かれているビデオストリーム再生の数が表示されます。
ビデオプッシュストリーム	関連する Mobile クライアントユーザーに対して現在開かれているビデオプッシュストリームの数が表示されます。 ※本機では表示されません
直接ストリーム	関連する Mobile のユーザーに対して現在開かれている直接ストリーミングを使用しているライブビデオストリームの数を表示します。 ※本機では表示されません

ビデオプッシュ

ビデオプッシュを有効にする場合、以下の設定を指定します。

名前	説明
ビデオプッシュ	Mobile サーバーでビデオプッシュを有効にします。
チャンネル数	XProtect システムで有効なビデオプッシュチャンネルの数を指定します。
チャンネル	関連するチャンネルのチャンネル数が表示されます。編集不可。
ポート	関連するビデオプッシュチャンネルのポート番号。
MAC アドレス	関連するビデオプッシュチャンネルの MAC アドレス。
ユーザー名	関連するビデオプッシュチャンネルに関連するユーザー名を入力します。(例: admin)
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 『179ページの"ビデオプッシュチャンネルの追加"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。

エクスポート

エクスポートされる録画データについて、以下の設定を指定します。

名前	説明
エクスポート	選択すると、クライアントによるエクスポートが可能になります。
タイムスタンプを含める	選択すると、エクスポートされるビデオにタイムスタンプを追加します。
AVI ファイルで使用されたコーデック	AVI ビデオファイルをエクスポートする際のエンコードで使用するコーデックを選択します。 ※コーデックのリストは Mobile サーバーを新規作成完了後に表示されます。
エクスポート先	録画をエクスポートする場所を指定します。 通常は D: ドライブ等の HDD 上に新規でフォルダーを作成し、そのフォルダーを指定してください。
次の期間が経過したエクスポート済み録画を削除する	録画が削除されるまでの日数を入力します。 この値を 1 日に設定した場合でも、エクスポートされたファイルはすぐには削除されません。変更を適用してから最長で 10 分後に削除されることに注意してください。 Mobile サーバーを手動で再起動して、変更がすぐに反映されるようにすることもできます。
エクスポートフォルダのサイズの上限	録画をエクスポートするフォルダサイズの上限を入力して、設定します。
他のユーザーが作成したエクスポートを見る	このチェックボックスを選択すると、ユーザーは他のユーザーによって行われたエクスポートを表示できるようになります。

自動エクスポート

特定のイベント発生時に自動的にエクスポートさせたい場合、自動エクスポートの実行ルールを設定する必要があります。

有効	このチェックボックスを選択すると、自動エクスポートが有効になります。
----	------------------------------------

有効チェックボックスの下の列に、自動的にエクスポートされたビデオのリストがあります。個々の自動エクスポートの詳細は以下を参照してください。

名前	ルールの名前です。
項目	自動エクスポートをトリガする項目です。
イベント	自動エクスポートをトリガするイベントを表示します。
カメラ	ビデオを録画するカメラです。
継続時間	エクスポートするビデオファイルの長さです。
エクスポートのタイプ	エクスポートファイルの形式が、データベース形式であるか、AVI 形式であることを示します。

エクスポートされた録画

この列では、個々のルールによりエクスポートされた録画について、以下が詳細表示されます。

名前	エクスポートされた録画の名前です。
ステータス	エクスポートされた録画の状態です。
カメラ	エクスポートされた録画を提供したカメラです。
タイムスタンプ	エクスポートが開始された時刻を示します。
継続時間	エクスポートされた録画の長さです。
ユーザー	エクスポートされた録画を提供したユーザーの名前です。
MB	エクスポートされた録画のサイズです。

注意： 更新をクリックすると、表示されているエクスポートされた録画のリストが更新されます。

設定なしの自動エクスポートのルール

自動エクスポートを起動させるために新しいルールを追加する際は、以下を指定します：

名前	説明
名前：	たとえば、 ドアが開いている または モーションの検知 など、作成したルールの名前を提供します。
項目：	自動エクスポートをトリガする項目を選択します。これは、カメラ、入力、出力、イベントなどです。 カメラを選択すると、カメラがビデオを受け取れるように、これが自動的に選択されます。
項目タイプ：	選択したアイテムの種類を表示します。
イベント：	自動エクスポートをトリガために使用するイベントを表示します。 使用可能なイベントのタイプは、選択した項目によります。
カメラ：	ビデオを録画する、カメラを選択します。
継続時間：	ビデオクリップをエクスポートする必要がある時間の長さ。
エクスポートタイプ：	エクスポートされたビデオクリップが XProtect データベースフォーマットであるか、あるいは AVI ファイルとしてエクスポートするかを選びます。

パフォーマンス

※本機は、パフォーマンススタブには対応していません。

パフォーマンススタブで、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：

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。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 1 秒当たりのフレーム数(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。

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。
最大 FPS	Milestone Mobile サーバーからクライアントへの送信の 1 秒当たりのフレーム数(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。

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。
最大 FPS	Milestone Mobile サーバーからクライアントへの送信の 1 秒当たりのフレーム数(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。

ログ設定

入力して、以下のログ設定を指定します：

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。
ログファイルの場所:	ログファイルが保存される場所へのパスです。
ログの保持期間:	ログを保持する日数です(デフォルトは 3 日です)。
CPU 使用状況:	ログでの警告をトリガする CPU 使用状況のデフォルトでのレベルです。
内部帯域幅:	ログでの警告をトリガする CPU 使用状況のデフォルトでのレベルです。
外部帯域幅:	ログでの警告をトリガする外部帯域幅使用状況のデフォルトでのレベルです。
確認頻度:	警告レベルを確認する時間枠のデフォルト(30 秒)です。

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
- Mobile サービスの起動、停止、再起動 『190ページ』
- 監視サーバーの資格情報の入力または変更 『189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 『190ページ』
- 証明書の編集 『189ページ』
- 今日のログファイルを開く 『188ページの"ログへのアクセスおよびエクスポートについて"参照』
- ログフォルダを開く 『188ページの"ログへのアクセスおよびエクスポートについて"参照』
- エクスポートフォルダを開く 『188ページの"ログへのアクセスおよびエクスポートについて"参照』
- Mobile サーバーのステータスを表示 『188ページの"ステータスの表示について"参照』
- Milestone Mobile ヘルプの Web サイト (マニュアル、よくある質問(FAQ)、製品のデモビデオがあります)へのアクセス

ステータスの表示について

Mobile Server Manager を右クリックして、**ステータスの表示...**を選択(あるいは Mobile Server Manager アイコンをダブルクリック)すると、Mobile サーバーのステータスを示すウィンドウが開きます。以下を表示できます。

名前	説明
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。
CPU 使用状況:	現在 Mobile サーバーが使用している CPU の%。
CPU 使用状況履歴:	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エクスポートについて

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、エクスポート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**エクスポートフォルダを開く**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、[プログラムデータ]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。

証明書編集

安全な HTTPS プロトコルを使用して、使用しているモバイルデバイスや XProtect Web Client と Mobile サーバーの間の接続を確立する場合、デバイスまたは Web ブラウザが警告なしで受け入れる有効な証明書が必要です。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。

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。**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。使用する証明書を後で変更する場合は、**Mobile Server Manager** でこれを実行できます。

1. **Mobile Server Manager** を右クリックして、**証明書の編集...**を選択します。
2. 以下のどちらを希望するかを選びます。
 - 自己署名証明書を生成、または
 - 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。変更を有効にするため、**Mobile** サービスが再起動されます。

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。

HTTPS は、Windows XP および Windows 2003 オペレーティングシステムではサポートされておらず、Windows Vista または新しい Windows OS のみで動作することに注意してください。

監視サーバーの資格情報の入力/編集

1. Mobile Server Manager を右クリックして、**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. Mobile Server Manager を右クリックして、**ポート番号の表示/編集...**を選択します。
2. ポート番号を編集するには、関連するポート番号を入力します。標準ポート番号(HTTP 接続用)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。

アラーム

アラームについて

アラーム機能は、Milestone 統合プラットフォーム(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セットアップされている場合、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 『193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プロファイルを作成し、その時間プロファイル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 Central

多くの場合、アラーム機能は XProtect Central と同じ機能をカバーします。

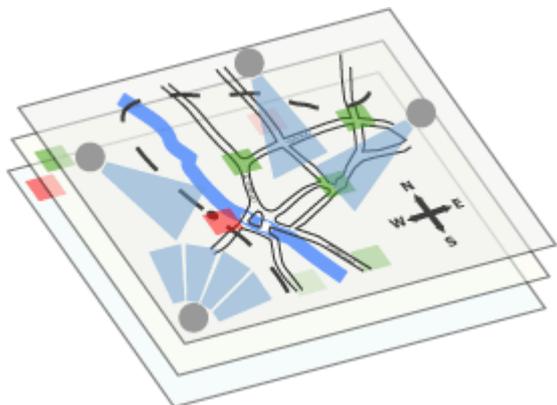
ただし、前者の XProtect Central の機能の設定は、アラーム機能に含まれています。

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

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。



例：XProtect Smart Client 内のマップ

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 『23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。

アラームの時間プロファイルについて

特定のアラーム定義を特定の期間内（たとえば月曜日の 14:30 から 15:30 の間）だけ有効化するには、アラームの時間プロファイルを作成する必要があります。時間プロファイルは、1 つまたは複数の単一期間、1 つまたは複数の繰り返し期間、あるいはそれらの組み合わせにより構成することができます。単一期間と繰り返し期間の概念については、Microsoft Outlook 等のカレンダーアプリケーションにおけるものと同様です。時間プロファイルは必ずシステムサーバーの現地時間で適用されます。

アラームの追加

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 『190ページ』を参照してください。

アラームを追加/設定するには、次の手順を実行してください。

1. アラームを展開し、**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 『193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) 時間プロファイルの追加

ここで追加する時間プロファイルは、アラーム機能からのみ使用されるものです。

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**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。
—あるいは—
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 『192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。

名前	説明
有効化	アラーム機能を有効にします。

名前	説明
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。
説明	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の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『193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できます。
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。
トリガされるイベント	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台または複数を選択することで、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。

名前	説明
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、Smart Client でソートに使用したり、ワークフローのコントロールで使用できます。
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	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 『195ページ』およびアラームサウンド設定 『196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

名前	説明
レベル	選択したレベル番号の新しい優先度を追加するか、デフォルトの優先度レベル (1 、 2 、 3 などの数) を使用/編集します。これらの優先度レベルは、初期アラームの優先度設定 『193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 『196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	デフォルトの状態レベル（番号 1 、 4 、 9 、 11 、編集または再利用は不可）に加えて、選択したレベル番号の新しい状態を追加します。このような状態レベルは、 Smart Client のアラームリストにのみ表示されます。
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 『193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せん。

閉じる理由タブ有効化	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。

名前	説明
音声	アラームに関連付けられる音声を選択します。音のリストには、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。

名前	説明
追加	音を追加できます。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。 デフォルト音は削除できません。
テスト	音をテストできます。リストから音を選択します。音声が一度だけ再生されます。

時間プロフィール

時間プロフィール 『193ページの" (アラームの) 時間プロフィールの追加"参照』 の設定を行う際には、以下を指定します。

コンポーネント	要件
名前	時間プロフィールの名前を入力します。
説明	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。 既存の時間プロフィールを編集する場合、時間プロフィールには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。時間プロフィー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 (Milestone インテグレーションパートナー) プラグインをシステムにインストールする際は、ナビゲーションペインでプラグインを検索します。**拡張設定 > MIP プラグイン**を展開します。

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。**拡張設定**を展開し、**ユーザー**を展開し、関連するユーザーを右クリックして、**プロパティ**を選択します。**アラーム管理**タブの下に、選択したユーザーに関する MIP 設定にアクセスできるタブがあります。

設定

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カメラを設定します。自動インストールが完了したカメラは、すぐに XProtect Smart Client のデフォルトビューでアクセス可能になります。

注意：

- すべてのカメラが、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。
- カメラ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。
- カメラに対して、手動でライセンスを有効化しなければなりません。これは、サーバーの 1 つに複数のサーバーが存在する環境で、カメラ設定だけを確実にアクティブ化するためです。

カスタマーダッシュボードについて

システムをインストールした時に、システムがカスタマーダッシュボードに通知を送信するかどうかの確認が表示されます。

カスタマーダッシュボードは、システム管理者やインストール情報へのアクセス権を持つユーザーに対して、発生の可能性がある技術的問題（カメラの障害など）を含むシステムの現在の状態の概要をグラフィカル表示として提供するオンラインのモニタリングサービスです。カスタマーダッシュボードのユーザーは、MilestoneWeb サイトの My Milestone ポータルを通じてアクセスします。システムのインストール時に行った選択によって、カスタマーダッシュボードの設定を変更するチェックボックスを選択または選択解除します。

情報収集の無効化

1. Management Application のツールバーで、オプション > 設定 > プライバシーオプションの順にクリックします。
2. プライバシーオプションタブで、はい、XProtect Enterprise の改善に協力しますチェックボックスを選択解除します。
3. OK をクリックします。

デフォルトのファイルパスの変更

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のパスを変更する場合は、このステップは不要です。
2. **Management Application** のメニューバーで、**オプション > デフォルトのファイルパス...**を選択します。
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（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。

4. 変更を確認したら、すべてのサービスを再起動します。

オプション

このセクションの内容

一括設定	201
ユーザーインターフェース	202
デフォルトのファイルパス	203
プライバシーオプション	203
アナリティックイベント設定	204
イベントサーバー設定	205

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。

自動デバイス検出

自動デバイス検出 『199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。カメラがデフォルトのユーザー名やパスワード以外に追加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。

注意： 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。システムがカメラを検出せず、システムに追加されない場合、カメラを手動で追加する必要があります。

カスタマーダッシュボード

システムがシステム情報をカスタマーダッシュボード 『199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、クラシックモードと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 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、証拠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。
Management Application でデバイスを削除した場合	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。
XProtect Smart Client 再生モード：	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ので、XProtect Smart Client では再生できなくなります。	Management 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ので、引き続き XProtect Smart Client で再生できます。
保持期間	記録の保持時間を設定し、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、記録に対して保持時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証拠であると考えられ、ストレージに残す必要がある場合に適しています。

言語

Management Application 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。

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。たとえば、デフォルトでは、**Management Application** は多くのアクションでユーザーに確認を求めます。これが不要であると感じられる場合、**Management Application** の動作を変更して、確認を求めないようにできます。**ユーザーインターフェース**へ移動して、それぞれのアクションを変更します。

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しようとする場合に、**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。
- 単一のシステムサーバーで、最大 **64** のカメラを同時に使用できます。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。

リストの下の**デフォルト設定の復元**をクリックすると、システムの動作をデフォルトの動作に復元できます。

デフォルトのファイルパス

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。

ファイルパス	説明
新しいカメラのデフォルトレコーディングパス	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、各カメラのレコーディングパスを、各カメラの個別の設定『 87 ページの"録画およびアーカイブのパス"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、デフォルトのレコーディング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『 127 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、デフォルトのレコーディング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『 66 ページの"ダイナミックパスの選択"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	デフォルトで、システム設定の保存に使用するパスです。

プライバシーオプション

システムをインストールすると、**顧客経験改善プログラムのオプションダイアログ**が表示されます。顧客経験改善プログラムは、システムをより使いやすいものにし、顧客経験を改善するために用意されています。

- プログラムへの参加を**拒否**した場合、システムの統計情報を収集するソフトウェアは一切インストールされません。

- プログラムへの参加を**承諾**した場合、グローバル一意識別子（GUID）を発行するクッキーがインストールの一部に含まれます。これにより、インストールや操作に関する匿名化された情報を定期的に収集します。収集する情報の詳細については、以下を参照してください。

インストール時にこの情報収集について承諾した場合でも、その後いつでも拒否に変更することができます。情報収集についての設定変更は **Management Application** 上で行えます。

システムから収集する情報について

システムがインストールされている装置に関する情報や、録画データに関する情報は一切収集しません。

Milestone が収集する情報:

- ソフトウェアがインストールされた国
- オペレーティングシステムのバージョン、Microsoft .NET Framework のバージョン、CPU の種類およびメモリ容量などのハードウェアプラットフォーム情報
- 製品のバージョン情報
- システムと併用するハードウェアデバイス（カメラ）の数と種類に関する情報
- システムで使用した機能と、その機能の使用頻度に関する情報
- どのシステムメニューやボタンが有効化されたかと、その使用頻度に関する情報
- システムのインストールにおける特定の操作の実行時間
- システムのインストールで生成されたエラーレポートおよび例外情報

これらの情報の収集は、**Management Application** または **XProtect Smart Client** の動作中のみ行われません。システムをアンインストールするか、**Management Application** 上で無効にすることで、情報の自動収集を行わないようにできます。

収集した情報の保護について

Milestone は、システムのインストールで収集した情報の機密を保護することを確約します。**Milestone** では、収集した情報の消失や誤用を防止するためのセキュリティ措置を実施しています。収集した情報は、外部からの干渉や不正アクセスを防止するため、ファイアウォールおよび他の高度な技術を駆使した安全なサーバー環境に保管されます。

アナリティックイベント設定

※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設定では、以下を指定できます。

名前	説明
デバイスが有効	アナリティックイベント機能が有効になります

ポート	<p>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。</p> <p>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。</p>
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	<p>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（以下を参照）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。</p> <p>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。</p> <p>リストにアドレスを追加する方法は2種類あります。手動で追加するか、アドレスの外部リストをインポートします。</p> <p>マニュアル入力: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。</p>
インポート	<p>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、外部リストを .txt ファイル形式で保存し、それぞれの IP アドレスまたはホスト名をファイルの別の行に表示させる必要があります。.txt ファイルの作成には、Windows のシンプルテキストエディタである Microsoft のメモ帳が適しています。</p>

イベントサーバー設定

以下のイベントサーバー設定を指定します。

名前	説明
終了したアラームの保持期間	<p>処理済のアラーム（処理済、無視、および拒否ステータスのアラーム）の保存日数を指定できます。これは通常、たとえば3日などの小さい数に設定しますが、サーバーの要領が許す限り、最大で99999日まで指定できます。値を0にすると、終了したアラームをサーバーの容量が許す限り無制限に保存することができます。</p>

名前	説明
他のすべてのアラームの保持期間	<p>他のすべてのアラームの保存日数を指定できます（つまり、処理済、無視、および拒否ステータスでないアラーム）。これは通常、たとえば 30 日などのある程度大きい数に設定しますが、サーバーの要領が許す限り、最大で 99999 日まで指定できます。値を 0 にすると、その他すべてのアラームをサーバーの容量が許す限り無制限に保存することができます。</p> <p>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、関連する監視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。</p>
ログの保持期間	アラームログの保存日数を指定できます。デフォルトは 30 日です。値を 0 にすると、サーバーの容量で可能な限り、ログが無期限に保存されます。
ログサーバー通信	一定の日数、通常のログに加えサーバー通信のログを保存したい場合に指定します。

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と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

以下では、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（『203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（中でも、ログファイル、イベントおよび Matrix 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『211ページの"Management Application の設定のエクスポートおよびインポート"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『81ページの"一括設定"参照』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、最も最近の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

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

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**、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、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：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。
 - **バックアップ先**：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、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。
6. インストールウィザードが完了するのを待ちます。

これで、**Management Application** でシステムの設定を開始できるようになりました。詳細は、システムの起動と実行 『24ページの"システムの起動および実行"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はありません。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るように抑えることができます（このトピックについては、<http://support.microsoft.com>の中で 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 の設定のエクスポートおよびインポート

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。

Management Application 設定をバックアップとしてエクスポートする

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. Management Application の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は、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 の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 の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）。

Management Application 設定をコピーとしてエクスポートする

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)を参照しているため、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. Management Application の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した Management Application の設定のインポート

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. Management Application の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. **拡張設定**を展開し、**サービス**を選択します。
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。

設定に対する変更のインポート

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。ただし、各店舗でのインストールは完全に同一ではない（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。

これが、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)からインポートできる理由です。

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、それらに達せ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。

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、たとえば **Management Application** のツールバーで**設定の保存**ボタンをクリックした場合など、**Management Application** の設定を保存するたびに、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. **拡張設定**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。

用語集

3

360 度 Panomorph サポート

360 度 Panomorph サポートのカメラは、名前が示すように、360 度の視界をカバーし、盲点や画像の歪みなしで全域を見渡すことができます。

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 Enterprise に対するアドオンとして利用可能な製品。XProtect Central は、場所に関わらず、XProtect Enterprise の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 XProtect Enterprise にインポートすることができます。複数の似たようなシステムを設定する場合に、単純かつ効果的な方法です。

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、http://www.mydomain.com) および数字による IP 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。

DVR

デジタルビデオレコーダー — DVR 自体に埋めこまれたハードディスク装置にデジタル形式でビデオを録画するデバイス。

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。

FTP

ファイル転送プロトコル (File Transfer Protocol) — インターネット上でファイルを交換するための規格。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。

G

GOP

画像グループ：個別のフレームをグループ化し、動画のシーケンスを形成します。

GSM

汎欧州デジタル移動電話方式 (Global System for Mobile communications) — 携帯電話通信の標準。

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。

HTTP

ハイパーテキスト転送プロトコル (HyperText Transfer Protocol) — インターネット上でファイルを交換するための規格。HTTP は、WWW (ワールドワイドウェブ、World Wide Web) 上でのデータ形式の規定と転送に使用される標準規格です。

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

Smart Client でリモートユーザーがログインするために、XProtect Enterprise へのアクセスを取り扱うサービス。Image Server サービスは、XProtect Enterprise 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、XProtect Enterprise の Management Application で設定されているので、個別には設定しません。

IP

インターネットプロトコル — 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形式とアドレススキームを規定するプロトコル (標準) です。TCP は、別のプロトコルである IP と組み合わせて使用されることがよくあります。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。

IPIX

360° の Panomorph 画像 (魚眼) を作成、表示できる技術です。

IP アドレス

インターネットプロトコルアドレス。ネットワーク上のコンピュータやデバイスを識別するために使用します。データトラフィックを指定した宛先へ転送するために TCP/IP プロトコルで使用します。IP アドレスには、0 から 256 までの数字が 4 つ並んでおり、ピリオドで区切られています (例: 192.168.212.2)。

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。

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

360°のパノラマ画像を作成・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。

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。

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、XProtect Enterprise 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。

SLC

ソフトウェアライセンスコード (Software License Code) — XProtect Enterprise ソフトウェアを使用するために必要な製品登録コード。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や登録を行う際に SLC を使用します。

SMS

ショートメッセージサービスまたはシステム管理サーバー。

1) ショートメッセージサービスとは、テキストメッセージを携帯電話へ送信するシステムです。

2) システム管理サーバーとは、システム管理者がローカルネットワーク上に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る Microsoft のツールです。このデータベースを使ってさまざまな操作を実行できますがその 1 つとして、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に渡って配布しインストールすることができます。

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) — 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。

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 XProtect Enterprise 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。

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。

デバイス

XProtect Enterprise 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せん：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。

ハードウェアデバイス

技術的には、カメラは XProtect Enterprise に追加されるのではなく、ハードウェアデバイスに追加されます。これは、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るためです。システムは IP ベースであるため、XProtect Enterprise は主に IP アドレスやホスト名に基づいて、ユニットを識別します。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となります。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、マイクなどが接続されていても、カメラ、マイクなどを個別に設定して使用することができます。

プライバシーマスク

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。

ブラウザー

Web ページの検索や表示を行うソフトウェアアプリケーション。

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前に、カメラから XProtect Enterprise へ、メールで画像をすぐに送信することができます。

プリバッファ

プリレコーディングの説明を参照してください。

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できる機能。場合によっては、XProtect Enterprise 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。プリレコーディングの有効な使用方法：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。

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の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、入力デバイス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。場合によって、XProtect Enterprise 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。ポストレコーディングの有効な使用方法：た

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

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。XProtect Enterprise でのマスター/スレーブ設定により、複数のXProtect Enterprise サーバーを組み合わせ、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 Enterprise 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、XProtect Enterprise 管理者が指定します。画面自動切替機能は、Smart Client で設定した場合に使用可能になります。

管理者（アドミニストレータ）

1) システム管理者。2) XProtect Enterprise の以前のバージョンの場合：XProtect Enterprise 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 と呼ばれません。

にアクティブ化する必要があります。この期間が猶予期間です。

記録（録画）

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（レンズ）

360°のパノラマ画像を作成・表示できるようなレンズの種類です。

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。XProtect Enterprise 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

システムのインストール・設定・録画サーバーやカメラの追加をした際に、一時的なライセンスを使用してシステムを動作させられます。ライセンスは、一定の期間が終了する前

索引

(
(アラームの) 時間プロファイルの追加 - 191,
193, 194, 197

3
360 度 Panomorph サポート - 215

A
API - 215
ATM - 215
AVI - 215

C
Central - 154, 215
Central について - 154
Central のプロパティ - 154
CSV - 215
CSV ファイルからインポート - 31, 32, 33

D
DirectX - 215
DNS - 215
DST - 215
DVR - 215

E
E メール - 148
E メール (プロパティ) - 136, 148
E メールについて - 148
E メール通知の設定 - 119, 121, 126, 148

F
FPS - 215
FTP - 216

G
GOP - 216
GSM - 216
GUID - 216

H
H.264 - 216
HTTP - 216

I
I/O - 216
Image Server - 216
IP - 216
IPIX - 216
IP アドレス - 217
I フレーム - 217

J
JPEG - 217

M
MAC アドレス - 217
Management Application でカメラからのビデオを表示する - 29, 44, 45, 91, 98, 100, 104
Management Application の設定のエクスポートおよびインポート - 207, 211
Matrix - 139, 217
Matrix イベントコントロール - 140, 141
Matrix のプロパティ - 140

Matrix の設定 - 140
 Matrix ビデオの共有について - 25, 139
 Matrix 受信 PC - 140
 Matrix 受信 PC について - 139
 Matrix 受信者 - 217
 Milestone Mobile クライアントのインストール
 - 23
 MIP プラグイン - 198
 MIP プラグインについて - 198
 MJPEG - 217
 Mobile Server Manager - 187
 Mobile Server Manager について - 187
 Mobile サーバー - 178
 Mobile サーバーについて - 178
 Mobile サーバーの設定 - 181
 Mobile サーバーの追加と編集 - 179
 Mobile サービスの起動、停止、再起動 - 188,
 190
 Motion-JPEG カメラのライブ設定および録画
 設定 - 36
 MPEG - 217
 MPEG カメラのライブ設定および録画設定 -
 38
 N
 NTLM - 217
 P
 Panomorph - 217
 PIN - 218
 Ping - 218
 POS - 218
 PTZ - 218
 PTZ タイプ 1 および 3 を、必要な位置へ移動す
 る - 63
 PTZ デバイス - 51, 56
 PTZ パトロール - 60, 100, 135, 138
 PTZ プリセット位置 - 98, 103
 PUK - 218
 P フレーム - 218
 R
 Recording Server Manager - 19
 Recording Server サービス - 218
 S
 SCS - 218
 SDK - 218
 SIM - 218
 SLC - 218
 SMS - 151, 218
 SMS について - 151
 SMS プロパティ - 151
 SMS 通知の設定 - 151
 SMTP - 219
 T
 TCP - 219
 TCP/IP - 219

Telnet - 219

W

Windows ユーザーの追加 - 170, 171, 172, 173, 174, 176

X

XProtect Central の有効化 - 154

XProtect Download Manager - 20

XProtect Smart Client - 17

XProtect Smart Client について - 17

XProtect Smart Client のインストール - 18

あ

アーカイブ - 131, 133, 136, 148

アーカイブされた録画の再生について - 133

アーカイブスケジュールについて - 128, 131

アーカイブについて - 37, 39, 40, 42, 43, 58, 65, 66, 69, 79, 88, 127, 136, 148, 203

アーカイブに必要なストレージ容量 - 130

アーカイブの場所について - 128

アクセスコントロール - 155

アクセスコントロールアクション - 161

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) - 159

アクセスコントロールシステムへの接続 - 157

アクセスコントロールシステム統合ウィザード - 156

アクセスコントロールシステム統合の作成 - 156

アクセスコントロールの統合について - 155

アクセスコントロールプロパティ - 157

アクセスの概要 - 48

アスペクト比 - 219

アナリティックイベント - 109, 116, 219

アナリティックイベントに基づくアラームの生成 - 113

アナリティックイベントの追加 - 109, 116

アナリティックイベント設定 - 204

アラーム - 190

アラームおよびマップ設定のバックアップと復元 - 208

アラームデータ設定 - 195

アラームについて - 190, 192

アラームの時間プロファイルについて - 192

アラームの追加 - 192, 193

アラームプロパティ - 193

アラーム管理 - 176

アラーム定義 - 113, 193, 195, 196

イベントおよび出力 - 105

イベントおよび出力について - 106

イベントおよび出力の概要 - 106

イベントおよび出力プロパティ - 116

イベントサーバー - 219

イベントサーバー設定 - 205

イベントでの PTZ - 103, 111
 イベントでのハードウェア出力の設定 - 106,
 109, 110, 111, 112, 127
 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) - 113, 127
 イベント通知 - 90
 インストールとアップグレード - 23
 ウイルススキャンについて - 12, 133
 エクスポート - 183
 オプション - 201
 オンライン期間 - 39, 63, 68, 81, 86, 111, 135,
 137
か
 カードホルダータブ(アクセスコントロール) -
 164
 カスタマーダッシュボードについて - 199,
 201
 カメラアクセス - 135, 172, 174
 カメラおよびデータベースアクション - 53
 カメラが MPEG ビデオ形式を使用する場合 -
 72
 カメラがいつ、何を必要とするかを設定する - 62
 カメラで MJPEG ビデオ形式を使用する場合 -
 70
 カメラとストレージの情報 - 57
 カメラの無効化または削除 - 63
 カメラプロパティ - 81
 カメラ固有のスケジュールの設定 - 24, 60, 62,
 134, 137, 138, 139
 カメラ固有のスケジュールプロパティ - 137
 キーフレーム - 219
 グループ情報 - 173
 コーデック - 219
さ
 サーバー - 178
 サーバーアクセス - 12, 164, 166
 サーバーアクセスについて - 164
 サーバーアクセスの設定 - 25, 47, 165, 166
 サーバーアクセスプロパティ - 166
 サーバーステータス - 182
 サーバー設定 (E メール) - 150
 サーバー設定 (SMS) - 152
 サービス - 177
 サービスについて - 58, 177
 サービスの再起動について - 28
 サービスを開始および停止する - 29, 44, 45,
 51, 52, 91, 98, 100, 104, 177, 178
 サイレントインストール - 18
 サウンド設定 - 195, 196
 サブネット - 220
 ジェネリックイベント - 112, 122

ジェネリックイベントのテスト - 114, 122
 ジェネリックイベントの追加 - 109, 111
 ジェネリックイベントプロパティ - 115
 システム、イベント、監査ログの設定 - 145
 システムコンポーネント - 15
 システムソフトウェアのインストール - 192
 システムのメンテナンス - 207
 システムの起動および実行 - 24, 210
 システム概要 - 15
 システム設定のバックアップ - 207
 システム設定の復元 - 208
 スケジュール - 153
 スケジュールオプション - 36, 133, 135, 137, 138
 スケジュールおよびアーカイブ - 127
 スケジュールについて - 127
 スタート - 30
 スタートページについて - 30
 ステータスの表示について - 188
 ストレージの設定：オンラインスケジュール - 36
 ストレージの設定：ビデオ設定とプレビュー - 35
 ストレージの設定ウィザード - 35, 131
 ストレージ情報 - 81
 スピーカーについて - 49
 スピーカープロパティ - 57, 104
スピードアップ - 71, 76, 78, 138
 スピードアップフレームレートのプロパティ - 75
 すべてのカメラのスケジュール - 133
た
 ダイナミックアーカイブパスについて - 129
 ダイナミックパスの選択 - 58, 66, 90, 203
 タイマーイベント - 112, 122
 タイマーイベントの追加 - 109, 110, 111, 112, 119, 121, 122, 126
 タイムサーバーについて - 13
 ディスク空き容量が不足した場合の自動応答 - 131
 データベースのサイズ変更について - 58
 デバイス - 220
 デフォルトのファイルパス - 128, 203, 207
 デフォルトのファイルパスの変更 - 200
 デュアルストリーム - 220
 テンプレートおよび共通プロパティ - 74
 ドライバー - 220
 ドライブの選択 - 40
な
 ネットワーク、デバイスタイプ、ライセンス - 51, 55

は

ハードウェアデバイス - 49, 220

ハードウェアデバイスについて - 49

ハードウェアデバイスの交換について - 51

ハードウェアデバイスの削除 - 51, 63

ハードウェアデバイスの設定 - 51, 55, 56, 96

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 - 33

ハードウェアデバイス交換ウィザードについ
て - 51, 52, 56

ハードウェアデバイス設定の追加 - 180

ハードウェアの検出と検証 - 32

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 - 34

ハードウェアの追加: スキャンオプション - 32

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 - 32

ハードウェアの追加ウィザード - 30, 49

ハードウェアプロパティ - 54

ハードウェア出力 - 120

ハードウェア出力の追加 - 91, 106, 109, 110,
112, 120

ハードウェア入力イベント - 110, 111, 118

ハードウェア入力イベントの追加 - 109, 118

ハードウェア名およびビデオチャンネル - 54

はじめに - 10

バックアップおよび復元の設定 - 207

パフォーマンス - 185

ビデオ - 77, 82, 138

ビデオデバイスドライバのインストール -
23

ビデオや録画の設定について - 24, 57, 60, 64,
66, 67, 73, 74, 77, 79, 80, 81, 82, 85, 86, 87,
90, 91, 96, 105, 137

ビデオ配信 - 180, 183

ビデオ配信チャンネルの追加 - 179, 181, 183

ビデオ配信ドライバーをハードウェアデバイ
スとして追加する - 180

ビデオ配信について - 179

ビデオ録画 - 67

プライバシーオプション - 203

プライバシーマスク - 94, 220

ブラウザ - 220

プリアラーム - 220

プリバッファ - 220

プリレコーディング - 220

フレームレート - 221

フレームレート - MJPEG - 74, 138

フレームレート - MPEG - 77

ポート - 221

ポートとポーリング - 50, 113, 115

ポート番号の表示/編集 - 188, 190
 ポーリング - 221
 ホスト - 221
 ポストレコーディング - 221
 ホットスポット - 221
ま
 マイク - 104
 マイク (プロパティ) - 105
 マイクについて - 49, 104
 マイクまたはスピーカーの設定 - 104
 マイクやスピーカーの表示/非表示 - 104
 マスター/スレーブ - 168, 221
 マスター/スレーブプロパティ - 168
 マスターおよびスレーブサーバーの設定 - 25, 168
 マスターおよびスレーブについて - 168
 マップについて - 191
 メッセージ設定 (Eメール) - 148, 153
 メッセージ設定 (SMS) - 151, 153
 モーション検知 - 45
 モーション検知および PTZ カメラについて - 60, 63
 モーション検知と領域の除外 - 39, 63, 68, 76, 78, 87, 91, 110, 148
 モーション検知について - 58, 63, 92
 モーション検知の設定 - 62
 モーション検知の調整ウィザード - 44
 モニター - 221
 モニターストレージ容量の使用率 - 29
や
 ユーザー - 170
 ユーザーアクセスの管理ウィザード - 25, 47, 172
 ユーザーインターフェース - 202
 ユーザーおよびグループの権限の設定 - 25, 47, 48, 91, 98, 111, 171, 172
 ユーザーグループの追加 - 25, 47, 171, 172, 173, 174, 176
 ユーザーについて - 170
 ユーザープロパティ - 173
 ユーザー情報 - 173
ら
 ローカル IP 範囲 - 167
 ログ - 143
 ログについて - 143
 ログプロパティ - 145
 ログへのアクセスおよびエクスポートについて - 188
 ログ設定 - 187
漢字
 一括設定 - 39, 68, 81, 86, 91, 181, 201, 207
 一般アクセス - 172, 173, 176

一般設定タブ(アクセスコントロール) - 158
 一般的なイベント処理の設定 - 108, 113, 114, 122
 一般的なスケジュールおよびアーカイブの設定 - 24, 62, 133, 135
 一般的なスケジュールのプロパティ - 133
 音声 - 85
 音声のアーカイブについて - 130
 音声の選択 - 80
 音声録音 - 79
 音声録音について - 49
 夏時間について - 13
 画面自動切替 - 221
 監視サーバーの資格情報の入力/編集 - 188, 189
 管理サーバーからのインストール - 18
 管理者 (アドミニストレータ) - 221
 管理者権限について - 11
 関連付けられたカメラ - 157
 関連付けられたカメラタブ(アクセスコントロール) - 159
 基本ユーザーと Windows ユーザー - 47
 基本ユーザーの追加 - 25, 170, 172, 173, 174, 176
 記録 (録画) - 67, 73, 74, 77, 86, 119, 177, 222
 魚眼 (レンズ) - 51, 96, 222
 魚眼レンズ - 95
 言語サポートと XML エンコーディング - 167
 高速 - 30, 31
 最終的な概要 - 157
 最低限のシステム要件 - 10
 時間プロファイル - 197
 自動デバイス検出について - 199, 201
 手動 - 31, 32
 手動イベント - 120
 手動イベントの追加 - 109, 111, 120, 194
 手動録画 - 73, 87, 175
 重要なポート番号について - 11
 出力 - 91, 110
 初めての使用 - 24
 証明書の編集 - 188, 189
 詳細設定 - 49
 情報、ドライバーの選択と検証 - 33
 情報収集の無効化 - 199
 新規ハードウェアデバイスの情報 - 52
 推奨事例 - 25
 設定 - 199
 設定なしの自動エクスポートのルール - 185
 設定に関する変更の保存について - 26
 設定に対する変更のインポート - 213

設定のバックアップおよび復元について - 207

専用入力/出力デバイスについて - 50, 116

組み込みヘルプの使用について - 27

他の場所へのアーカイブについて - 129

著作権、商標、および免責条項 - 9

直接ストリーミングについて - 178

通常フレームレートのプロパティ - 75

通知 - 147

通知スケジュールについて - 153

通知スケジュールプロパティ - 149, 152, 153

通知について - 111, 127, 147

添付設定 (E メール) - 149

登録済みサービスについて - 165

入力および出力について - 105

復元ポイント - 222

復元ポイントからのシステム設定の復元 - 27,
213

猶予期間 - 222

領域の除外 - 44, 63

録画およびアーカイブのパス - 64, 87, 128,
203

録画およびアーカイブの設定 - 43

録画およびストレージのプロパティ - 64

録画データベースの破損からの保護について -
25, 89

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。

ホームページ <http://www3.jvckenwood.com/>

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