

SONY

Network Video Management System
Enterprise Edition 2016 R3

管理者マニュアル

目次

著作権、商標、および免責条項.....	10
はじめに	11
ヘルプのご紹介	11
組み込みヘルプシステムの操作	11
システム概要.....	13
製品概要.....	13
分散型システム設定	14
システムコンポーネント	15
管理サーバー	15
フェールオーバー管理サーバー	15
レコーディング サーバー	15
Event Server	15
Log Server	16
SQL Server.....	16
Active Directory.....	16
仮想サーバー	16
クライアント	17
ライセンスについて.....	19
IPv6 と IPv4 について.....	20
IPv6 を使用するシステムの使用について	20
IPv6 アドレスの記述方法について.....	21
システム要件	22

インストール.....	23
インストールを開始する前に.....	23
Active Directory の準備.....	23
インストール方法.....	23
SQL Server タイプを決定する.....	25
サービスアカウントを選択してください.....	26
Kerberos 認証について.....	26
ウイルススキャンについて.....	27
ソフトウェアライセンスコードを登録する.....	28
システムのインストール.....	29
システムのインストール - シングルサーバーオプション.....	29
システムのインストール - 分散オプション.....	30
システムのインストール - カスタムオプション.....	31
レコーディングサーバーのインストール.....	32
レコーディングサーバーのサイレントインストール.....	33
Kerberos 認証を設定します。.....	36
ワークグループのインストール.....	36
インストールのトラブルシューティング.....	37
Management Client のシステムの構成.....	39
ソフトウェアライセンスコードの変更.....	40
ローカル IP アドレス範囲について.....	41
クライアントのインストール.....	41
Network Video Management System Smart Client のサイレントインストール.....	41
NVMS Mobile サーバーのインストール.....	42
Download Manager/ダウンロード Web ページ.....	43
Download Manager のデフォルト設定.....	44
Download Manager の標準インストーラ (ユーザー).....	44

Download Manager インストーラコンポーネントの追加と公開	45
Download Manager インストーラコンポーネントの非表示および削除	46
デバイスパックのインストーラ - ダウンロードする必要があります	46
アップグレード	47
アップグレードについて	47
アップグレードの前提条件.....	47
アップグレードの推奨手順.....	48
ワークグループの他のアップグレード方法	48
初めての使用.....	50
推奨事例.....	50
記録データベースを破損から守る	50
夏時間について	51
タイムサーバーについて	51
Management Client 概要	52
ログイン概要	52
Management Client ウィンドウ概要	52
ペインの概要	54
メニュー概要	55
Management Client エlement	57
基本	57
ライセンス情報	57
サイト情報	60
サーバーとハードウェア	61
レコーディング サーバー	61
ハードウェア	79
デバイス.....	87

デバイスグループの操作	87
デバイスの使用	90
クライアント	129
クライアントについて	129
ビューグループ	130
Smart Client プロファイル	131
Matrix	136
ルールとイベント	138
ルールとイベントについて	138
アクションとアクションの停止について	139
イベント概要	145
ルール	150
時間プロファイル	156
通知プロファイル	160
ユーザー定義イベント	163
アナリティック イベント	165
ジェネリックイベント	168
セキュリティ	172
役割	172
基本ユーザー	189
システムダッシュボード	190
システムダッシュボードについて	190
システム監視について	190
システム監視の詳細	192
システム監視しきい値	193
現在のタスクについて	194
設定レポートについて	195
サーバーログ	195

ログについて	195
ログの検索	196
ログのエクスポート	196
ログ言語の変更	197
システムログ (プロパティ)	197
監査ログ (プロパティ)	198
ルールログ (プロパティ)	198
アラーム	199
アラーム設定について	199
アラームについて	200
アラーム定義	201
アラームデータ設定	204
音声の設定	206
オプションダイアログボックス	206
一般タブ (オプション)	207
サーバーログタブ (オプション)	209
メールサーバータブ (オプション)	210
AVI 生成タブ (オプション)	210
ネットワークタブ (オプション)	211
ユーザー設定タブ (オプション)	211
アナリティックイベントタブ (オプション)	211
イベントサーバータブ (オプション)	212
ジェネリックイベントタブ (オプション)	213
機能設定	215
フェールオーバー管理サーバー	215
複数の管理サーバー (クラスター)	215
クラスターリングの前提条件	215
クラスターでのインストール	215

クラスタでのアップグレード.....	217
Network Video Management System Smart Wall	218
Network Video Management System Smart Wall について	218
Network Video Management System Smart Wall ライセンス.....	218
Smart Wall の設定.....	218
Network Video Management System Smart Wall のユーザー権限の設定..	220
Smart Wall プリセットのあるルールの使用について	221
Smart Wall のプロパティ	221
モニタープロパティ	223
NVMS Mobile.....	224
NVMS Mobile の概要.....	224
NVMS Mobile 構成	225
Mobile Server Manager	234
よくある質問(FAQ)	237
一方向の信頼のマルチドメイン環境	241
一方向の信頼の設定.....	241
SNMP	242
SNMP のサポートについて	242
SNMP サービスのインストール.....	242
SNMP サービスの設定.....	242
システムのメンテナンス	244
このシステムで使用するポート	244
システム設定のバックアップおよび復元.....	246
システム設定のバックアップおよび復元について.....	246
ログサーバーデータベースのバックアップ	246
システム設定の手動バックアップおよび復元	246
スケジュールされたバックアップと復元.....	248

管理サーバーの移動.....	250
管理サーバーの移動について.....	250
使用できない管理サーバーについて.....	251
システム設定の移動.....	252
SQL Server の管理.....	252
SQL Server アドレスの更新について.....	252
ログサーバーの SQL アドレスの更新.....	252
管理サーバーまたはイベントサーバーの SQL Server アドレスの更新.....	253
ハードウェアの交換.....	254
レコーディングサーバーの交換.....	255
ビデオデバイスドライバー.....	256
ビデオデバイスドライバーについて.....	256
ビデオデバイスドライバーの削除について.....	257
サーバーサービスの管理.....	257
Management Server サービスの開始と停止.....	257
Recording Server サービスの開始と停止.....	258
管理サーバーまたはレコーディングサーバーのステータスメッセージの表示.....	258
Event Server サービスの開始、停止、再起動.....	259
トレイアイコンについて.....	260
Recording Server サービスの設定の変更.....	261
レコーディングサーバーの設定.....	262
Data Collector Server サービスの再起動.....	262
登録済みサービス.....	263
サービスチャンネルについて.....	263
登録済みサービスの追加と編集.....	264
ネットワーク設定の管理.....	264
登録済みサービスのプロパティ.....	264

索引 266

著作権、商標、および免責条項

著作権 : © 2016 Sony Corporation

商標

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。

Sony Corporation 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 Sony 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

ヘルプのご紹介

このヘルプは、特定の目的で2つのセクションに分かれています。セクションは理論的なフローで構成されています。

システム概要 『13ページ』

ここでは、ビデオ監視システム、システムコンポーネントおよび概念を紹介しています。システムに馴染みのないユーザーに有用です。システム概要には、製品の間で最も重要な相違点を一覧表示した比較表も含まれています。

インストール 『23ページ』

システムのインストールとアップグレードに役立つ、インストールの前提条件と手順を追った手続きについて説明しています。

初めてご使用になる前に 『50ページ の"初めての使用"参照』

Management Client の概要と、システムを円滑に実行するためのベストプラクティスに関する情報を提供しています。この概要は、システムに馴染みのないユーザーに有用です。

Management Client 要素 『57ページ の"Management Client エレメント"参照』

Management Client のサイトナビゲーションペインの各ノードについて説明しています。このセクションには、システムの基本的な要素に関する概念および手続き情報が含まれています。

機能の設定 『215ページ の"機能設定"参照』

お使いのシステムでサポートされる追加機能やアドオン製品に関する完全な詳細情報を提供しています。

システムメンテナンス 『244ページ の"システムのメンテナンス"参照』

システムで使用されるポートの概要と、システムのバックアップやシステムパフォーマンスのモニタリングなどの操作について手順を追って説明しています。このセクションは、インストールおよび設定後にシステムのメンテナンス、拡張および最適化する際に有用になります。

組み込みヘルプシステムの操作

F1 キーを押すと関連するヘルプトピックにアクセスできます。または、Management Client のツールバーからヘルプ > 目次を選択するとヘルプ全体が起動します。

ヘルプウィンドウの3つのタブ、目次、索引、検索を使用するか、またはヘルプトピック内のリンクを使用します。

タブ	詳細
目次	ツリー構造を使ってヘルプシステムをナビゲートできます。
索引	必要な単語の最初の文字を選択して、見つかるまでスクロールします。検索結果のリストからトピックのタイトルをクリックすると、トピックのページが開きます。

タブ	詳細
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のリストが検索結果に表示されます。検索結果のリストからトピックのタイトルをクリックすると、トピックのページが開きます。

ヘルプトピックを印刷するには、そのトピックを開いて、ブラウザの印刷ボタンをクリックします。

システム概要

製品概要

この Network Video Management System システムは、異なるベンダーのデバイスをサポートし、常時監視を必要とする大規模のマルチサイト、マルチサーバー施設のために設計された、完全に分散型のソリューションです。このソリューションはすべてのデバイス、サーバー、およびユーザーを集中管理し、スケジュールとイベントによる非常に柔軟なルールシステムを提供します。

このシステムは、以下の主要な要素で構成されています。

- **Management Server** は、インストールの中心で、複数のサーバーで構成されています。
- 1つまたは複数の **Recording Server**
- 1つまたは複数の **Network Video Management System Management Client**
- **Network Video Management System Download Manager**
- 1つまたは複数の **Network Video Management System Smart Client**
- 1つまたは複数の **Network Video Management System Web Client** および必要な場合は **NVMS Mobile** クライアント

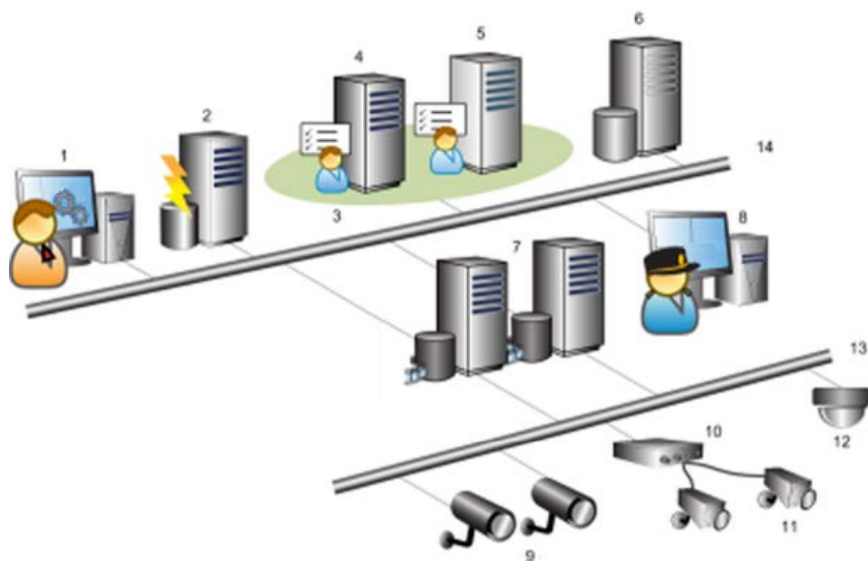
また、このシステムには、監視システムの任意のカメラから Network Video Management System Smart Client をインストールした任意のコンピュータにビデオを配信して表示することができる、統合的な Matrix の機能があります。

Network Video Management System システムは、仮想化されたサーバー、または分散型環境の複数の物理サーバーにインストールできます。

Network Video Management System Smart Client から証拠ビデオをエクスポートする場合に、スタンドアロン Network Video Management System Smart Client – Player を含めることも可能です。Network Video Management System Smart Client – Player を使用すると、証拠ビデオの受信者（警察官、内部または外部捜査官など）は、専用ソフトウェアをコンピュータにインストールしなくても、エクスポートされた録画をブラウザ、再生することができます。

このシステムでは、必要に応じて、複数のサイトにわたって無制限の数のカメラ、サーバー、ユーザーを処理できます。IPv4 に加えて、IPv6 も処理できます。

分散型システム設定



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

凡例：

1. Management Client
2. Event Server
3. Microsoft Cluster
4. 管理サーバー
5. フェールオーバー管理サーバー
6. SQL Server
7. レコーディングサーバー
8. Network Video Management System Smart Client
9. IP ビデオカメラ
10. ビデオサーバー
11. アナログカメラ
12. PTZ IP カメラ
13. カメラのネットワーク
14. サーバーのネットワーク

システムコンポーネント

管理サーバー

管理サーバーは、監視システムの設定を、管理サーバーのコンピュータ自体か、ネットワークにある個別の SQL Server のいずれかのリレーショナルデータベースに保存します。また、ユーザーの認証、ユーザー権限、ルールシステムなども処理します。システムパフォーマンスを改善するために、複数の管理サーバーを 1 つのとして実行することができます。管理サーバーはサービスとして実行され、通常は専用のサーバーにインストールされません。

ユーザーは初期認証のために管理サーバーに接続します。その後は、ビデオ録画などへのアクセスのためにレコーディングサーバーに透過的に接続できます。

フェールオーバー管理サーバー

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

レコーディングサーバー

レコーディングサーバーは、ネットワークカメラやビデオエンコーダーと通信して、取得された音声および動画を記録した上で、ライブおよび記録された音声および動画へのアクセスをクライアントに提供します。

また、レコーディングサーバーは、テクノロジーを使って他の Sony 製品との通信も行います。

デバイスドライバー

- ネットワークカメラとビデオエンコーダーとの通信は、各デバイス専用開発されたデバイスドライバー、または同じメーカーからの類似した複数のデバイス用のデバイスドライバーを通して行われます。
- デバイスドライバーは、レコーディングサーバーがインストールされたときにデフォルトでインストールされていますが、新しいバージョンのデバイスパックをダウンロードしてインストールすることで、後日に更新できます。

メディアデータベース

- 取得された音声および動画データは、メディアデータベースに保存されます。このカスタムメードの高パフォーマンスデータベースは、音声および動画データの記録と保管用に最適化されています。

Event Server

イベントサーバーは、イベント、アラーム、マップ、および MIP ソフトウェア開発キット (SDK) を使ったサードパーティ統合に関連するさまざまなタスクを処理します。

イベント:

- すべてのシステムイベントがイベントサーバーに統合されるため、システムイベントを活用して統合を実行するパートナーは、場所とインターフェースを一元化できます。

- また、イベントサーバーは、ジェネリックイベントまたはアナリティックイベントインターフェースを通してシステムにイベントを送信するためのサードパーティアクセスを提供します。

アラーム：

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

マップ：

- イベントサーバーは、Network Video Management System Smart Client で設定され、使用されているマップもホストします。

MIP SDK：

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

Log Server

ログサーバーは、システム全体のすべてのログメッセージを保存します。ログサーバーでは、管理サーバーと同じ SQL Server を使用し、通常は管理サーバーと同じサーバーにインストールされますが、管理サーバーやログサーバーのパフォーマンスを向上するために必要な場合は、別のサーバーにインストールすることができます。

SQL Server

管理サーバー、イベントサーバー、ログサーバーは、SQL Server を使用して、設定、アラーム、イベント、ログメッセージなどを保存します。

システムインストーラには、最高 300 台のカメラがインストールされたシステムで自由に使用できる Microsoft SQL Server Express が含まれています。

300 台を超えるカメラのあるシステムでは、専用サーバーにインストールされた SQL Server 2008 R2 Standard または Enterprise 版を使用することをお勧めします。これらの版では、より大きいデータベースを処理でき、バックアップ機能を提供しています。

Active Directory

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

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

仮想サーバー

すべてのシステムコンポーネントを、VMware®や Microsoft® Hyper-V®などの仮想化された Windows®サーバーで実行することができます。

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

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

クライアント

Management Client のバージョン情報

システムの設定や日常的な管理のための多機能管理クライアントです。複数の言語で用意されています。

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

Management Client の詳細については、Management Client の概要 『52ページ』の"Management Client 概要"参照』を参照してください。

Network Video Management System Smart Client について

Sony Network Video Management System IP ビデオ管理ソフトウェア用に設計された Network Video Management System 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。Network Video Management System Smart Client でセキュリティのインストールを管理することで、ユーザーはライブおよび録画ビデオ、カメラおよび接続済みのセキュリティデバイスの即時制御、録画の概要表示にアクセスできます。Network Video Management System Smart Client は適応力の高いユーザーインターフェースを、複数の言語で使用できます。各オペレータの作業に応じて最適化し、特定のスキルや権限レベルに応じて調節が可能です。



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

Network Video Management System 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、Network Video Management System システムの Management Client 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。別個のハードウェアは不要です。

Network Video Management System 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 Network Video Management System Download Manager を使用して、Network Video Management System 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。

NVMS Mobile クライアントについて

NVMS Mobile クライアントは、モバイル監視ソリューションで、Network Video Management System システムの他の部分と密接に統合されます。クライアントは、Android タブレットまたはスマートフォン、Apple® タブレットまたはスマートフォン、携帯ミュージックプレーヤー、Management Client でセットアップされたカメラ、ビュー、その他の機能にアクセスすることができます。

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

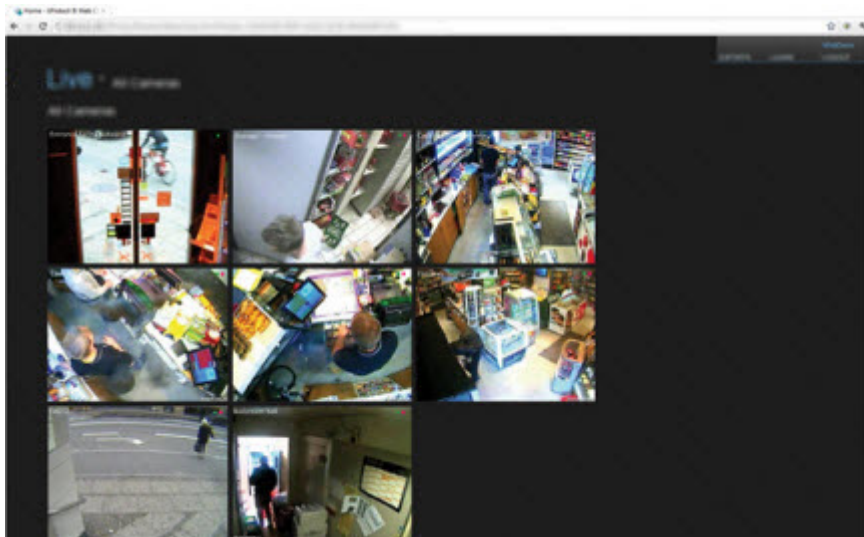


システムで NVMS Mobile クライアントを使用したい場合は、モバイルサーバーを追加して、NVMS Mobile クライアントと使用しているシステムの間での接続を確立する必要があります。モバイルサーバーをセットアップしたら、Google Play、App Store から NVMS Mobile クライアントを無料でダウンロードし、NVMS Mobile の使用を開始します。

ビデオを Network Video Management System システムにプッシュ配信するデバイスごとに必要なデバイスライセンスは 1 つです。

Network Video Management System Web Client について

Network Video Management System Web Client は、Web ベースのクライアントアプリケーションであり、ビデオを表示、再生、共有できます。ライブビデオの表示、録画ビデオの再生、証拠の印刷やエクスポートなど、最も頻繁に使用される監視機能に瞬時にアクセスできます。機能へのアクセスは、管理サーバーでセットアップされる個別のユーザー権限により異なります。



Network Video Management System Web Client へのアクセスを有効にするには、mobile サーバーをインストールして、Network Video Management System Web Client と使用しているシステムの間での接続を確立する必要があります。Network Video Management System Web Client 自体は、インストールを必要とせず、大半のインターネットブラウザで動作します。Mobile サーバーをセットアップしたら、インターネットアクセスが可能なコンピュータやタブレットで、どこからでも（適切な外部/インターネットアドレス、ユーザー名およびパスワードが分かっていることが必要）Network Video Management System システムを監視することができます。

ライセンスについて

ナビゲーションツリーで、**基本 > ライセンス情報**を選択する場合は、SLC も確認することができます。

少なくとも 2 つのライセンスを購入しています。

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

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

詳細については、SonyWeb サイト <http://www.sony.net/CameraSystem/NVMS/Technical-documents> でサポートされているハードウェアの一覧を参照してください。NVMS Mobile でビデオプッシュ機能を使用する

場合は、システムに動画をプッシュするモバイルデバイスまたはタブレットごとに1つのハードウェアデバイスライセンスも必要です。

IPv6 と IPv4 について

システムは、IPv4 と IPv6 をサポートします。同じです Network Video Management System Smart Client。

IPv6 は、インターネットプロトコル (IP) の最新バージョンです。インターネットプロトコルは、IP アドレスのフォーマットおよび使用法を決定します。IPv6 は現在も広く使用されている IP のバージョンである IPv4 と共存しています。IPv6 は、IPv4 のアドレス枯渇を解決するために開発されました。IPv4 アドレスは 32 ビット長であるのに対し、IPv6 アドレスは 128 ビットの長さです。

つまりインターネットのアドレス帳が単一の 43 億のアドレスから 340 澗 (10 の 36 乗) へ増えたという意味です。増大係数は 79000??10 ン 273 乗)。

ますます多くの組織が自社のネットワーク上で IPv6 を実装しています。たとえば、すべての米国連邦政府機関のインフラを IPv6 対応にする必要があります。現在最も広く使用されている IP バージョンであるため、このマニュアルの例やイラストは、IPv4 の使用法を反映しています。IPv6 も同様にシステムに適合します。

IPv6 を使用するシステムの使用について

システムで IPv6 を使用する場合は、次の条件が適用されます。

サーバー

サーバーでは、IPv4 に加えて、IPv6 もよく使用されます。ただし、システム内の 1 つのサーバーで特定の IP バージョンが必要とされる場合、システム内のすべての他のサーバーが、同じ IP バージョンを使用して通信しなければなりません。

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

デバイス

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

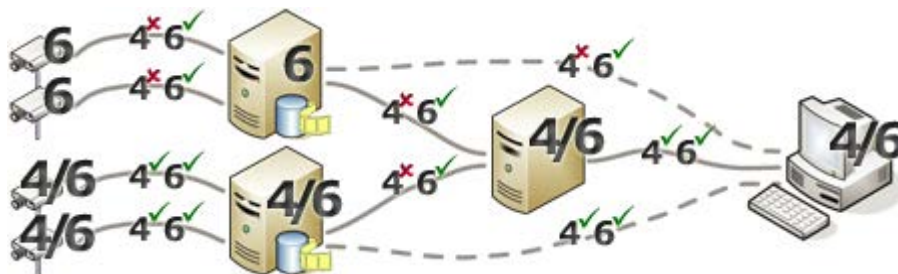
クライアント

システムが IPv6 を使用している場合、ユーザーは Network Video Management System Smart Client を使用して接続する必要があります。Network Video Management System Smart Client は、IPv6 と IPv4 をサポートします。

システム内の 1 つ以上のサーバーで IPv6 しか使用できない場合は、Network Video Management System Smart Client ユーザーは、他のサーバーとの通信に IPv6 を使用する **必要があります**。このようなケースでは、Network Video Management System Smart Client は厳密には最初の認証で管理サーバーに接続し、その後録画にアクセスするために必要なレコーディングサーバーに接続することに注意してください。

ただし、ネットワーク設備で異なる IP バージョン間の通信がサポートされており、コンピュータ上に IPv6 プロトコルがインストールされている場合、Network Video Management System Smart Client ユーザーは IPv6 ネットワーク上にある必要はありません。図も参照してください。クライアントコンピュータに IPv6 をインストールするには、コマンドプロンプトを開き、*Ipv6 install* と入力して **ENTER** を押します。

図例



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

Matrix Monitor との互換性なし

IPv6 を使用している場合、システムで Matrix Monitor アプリケーションを使用できません。Network Video Management System Smart Client での Matrix の機能には影響ありません。

IPv6 アドレスの記述方法について

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

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

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

例：

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

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

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

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

URL での IPv6 アドレスの使用

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

IPv6 アドレスを含む URL の例 :

[http://\[2001:0B80:0000:0000:0000:0F80:3FA8:18AB\]](http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB])、つまり、これは次のように短縮できます。

例 : [http://\[2001:B80::F80:3FA8:18AB\]](http://[2001:B80::F80:3FA8:18AB])

IPv6 アドレスとポート番号を含む URL の例 :

[http://\[2001:0B80:0000:0000:0000:0F80:3FA8:18AB\]:1234](http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]:1234)、つまり、これは次のように短縮で

きます。例 : [http://\[2001:B80::F80:3FA8:18AB\]:1234](http://[2001:B80::F80:3FA8:18AB]:1234)

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

システム要件

各種システムコンポーネントの**最低**システム要件については、Sony Web サイト

<http://www.sony.net/CameraSystem/Product-info> をご覧ください。

インストール

以前の Network Video Management System バージョンからアップグレードする場合は、アップグレードについて『47ページ』を参照してください。

インストールを開始する前に

次のすべての必須および重要な前提条件を理解してから、実際のインストールを開始してください。

Active Directory の準備

Active Directory サービスによってユーザーを追加する場合は、Active Directory がインストールされており、ドメインコントローラとして機能するサーバーがネットワークで使用できることが必要です。

ユーザー/グループを簡単に管理するため、Sony では Network Video Management System システムをインストールする前に、Microsoft Active Directory[®]をインストールして、設定することをお勧めします。システムをインストールしてから、管理サーバーを Active Directory に追加すると、管理サーバーを再インストールして、ユーザーを Active Directory で定義した新しい Windows ユーザーに置き換えなければなりません。

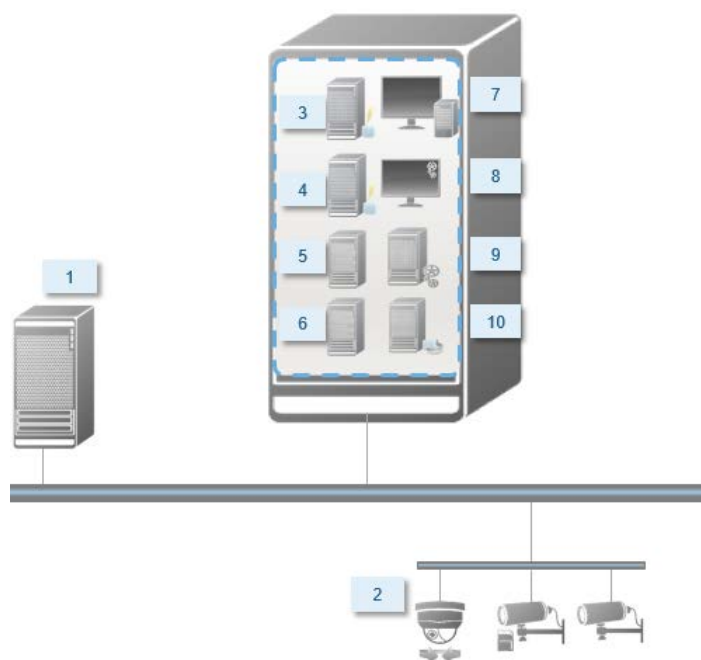
インストール方法

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

オプション	詳細
シングルサーバー	すべての管理サーバーコンポーネント、レコーディングサーバー、および Network Video Management System Smart Client が現在のコンピュータにインストールされます。最小限の項目のみを選択するだけで、すべてのコンポーネントが編集不可のコンポーネントリストで事前選択されます。ハードウェアと構成によっては、最大 50~100 台のカメラから構成される小規模なシステムは 1 台のサーバーで実行できます。SQL Server はリストにありませんが、現在のコンピュータにはインストールされます。
分散型	管理サーバーコンポーネントだけが現在のコンピュータにインストールされます。レコーディングサーバーと Network Video Management System Smart Client は、コンポーネントリストには表示されません。コンポーネントリストではどの項目も編集できません。 レコーディングサーバー、Network Video Management System Smart Client、および SQL Server を他のコンピュータに後からインストールする必要があります。

オプション	詳細
カスタム	<p>管理サーバーは常にシステムコンポーネントリストで選択され、常にインストールされますが、他の管理サーバーコンポーネント、レコーディングサーバー、および Network Video Management System Smart Client など、現在のコンピュータにインストールする項目を自由に選択できます。</p> <p>デフォルトでは、レコーディングサーバーはコンポーネントリストではオフですが、これは変更可能です。選択内容によっては、未選択のコンポーネントと SQL Server を後から他のコンピュータにインストールする必要があります。</p>

シングルサーバー

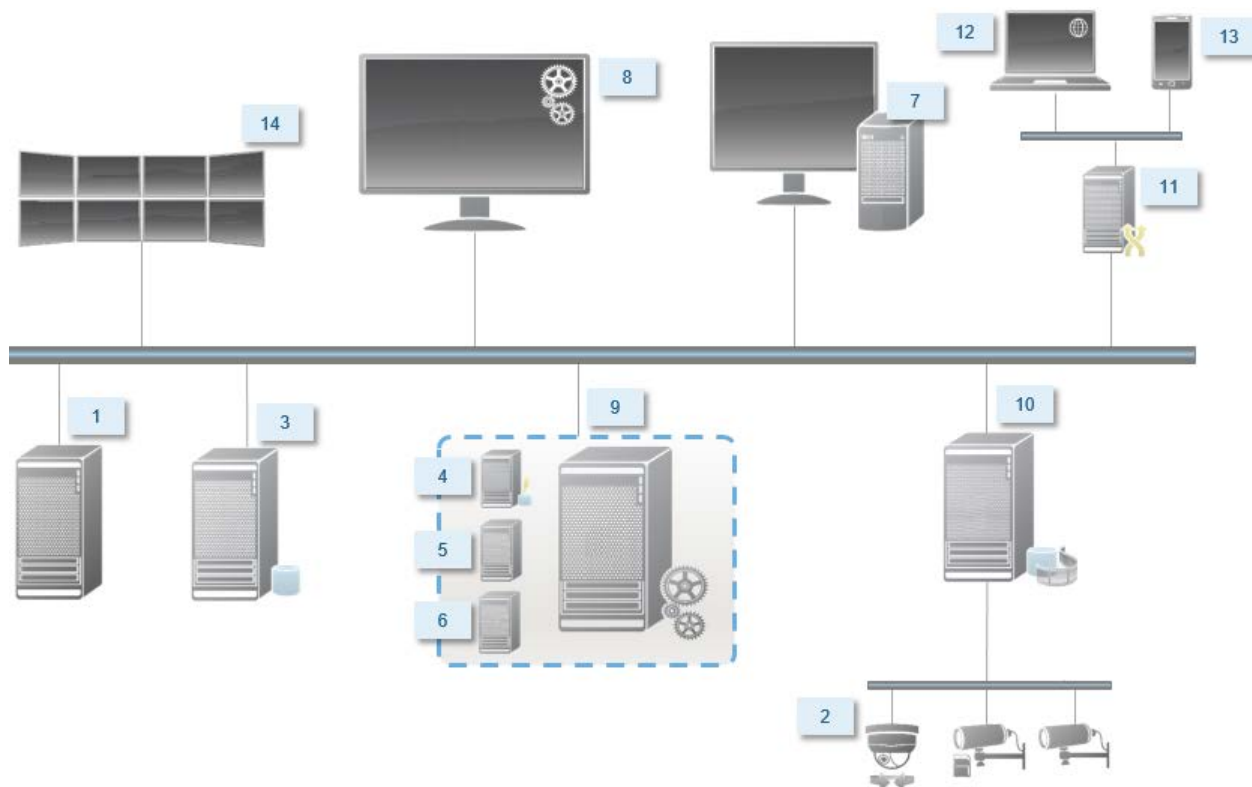


標準システムコンポーネント：

1. **Active Directory**
2. デバイス
3. **SQL Server**
4. イベントサーバー
5. ログサーバー
6. サービスチャンネル
7. **Network Video Management System Smart Client**
8. **Management Client**
9. 管理サーバー
10. レコーディングサーバー
11. **NVMS Mobile** サーバー

- 12. Network Video Management System Web Client
- 13. NVMS Mobile クライアント
- 14. Network Video Management System Smart Client と Network Video Management System Smart Wall

分散型



SQL Server タイプを決定する

Microsoft SQL Server Express Edition は、完全な SQL Server の「簡易」版です。インストールや使用の準備が簡単であり、多くの場合、カメラの数が 299 台以下のシステムには推奨されます。このバージョンの SQL Server は、1 台のサーバーインストールに含まれます。

300 台を超えるカメラを設置する大規模システムでは、Sony は、ネットワーク上の専用コンピュータにインストールされた既存の専用 SQL Server を使用することをお勧めします。SQL server に関する管理者権限が必要です。

Sony は、他の用途で使用しない専用のハードディスクドライブに、データベースをインストールすることをお勧めします。専用ドライブにデータベースをインストールすると、全体的なシステムパフォーマンスが上がります。

インストールウィザードで**分散**または**カスタム**を選択した場合、SQL Server のインストール方法を決定する必要があります。

SQL Server をインストールしていない場合は、次のオプションがあります。

- このコンピュータに **SQL Server Express** をインストールする。

- ネットワーク上の既存の **SQL Server** を使用する。ネットワーク上で SQL データベース専用のコンピュータを使用する場合、アカウントからアクセスできる SQL Server のリストが表示されます。

SQL Server をインストールしてある場合は、次のオプションがあります。

- このコンピュータにインストールされている **Microsoft SQL Server Express** データベースを使用する。
- ネットワーク上の既存の **SQL Server** を使用する。ネットワーク上で SQL データベース専用のコンピュータを使用する場合、アカウントからアクセスできる SQL Server のリストが表示されます。

新しいデータベースを作成するか、既存のデータベースを使用するか、あるいは既存のデータベースを上書きするかどうかを確認するメッセージが表示されます。

- **新しいデータベースを作成する**：新規インストールの場合。
- **既存のデータベースを使用する**：システムのアップグレードの一部としてデータベースをインストールしており、既存のデータベースを使用する場合。

サービスアカウントを選択してください

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

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

ドメイン環境

ドメイン環境：

- Sony は、ビルトインのネットワークサービスアカウントを使用することをお勧めします。システムを複数のコンピュータに拡張する必要がある場合でも、使いやすいアカウントです。

**ドメインユーザーアカウントも使用できますが、構成が少し難しくなる可能性があります。
ワークグループ環境**

ワークグループ環境では、Sony は、すべての必要な権限があるローカルユーザーアカウントを使用することをお勧めします。通常は、これは管理者アカウントです。

重要：複数のコンピュータにインストールされる場合は、選択したユーザーアカウントがインストールするすべてのコンピュータに、同じ名前、パスワード、アクセス権で存在する必要があります。

Kerberos 認証について

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

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

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

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

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

サービス	ポート番号
管理サーバー- IIS	80 -構成可能
管理サーバー -内部	8080
記録サーバー・データ・コレクタ	7609
フェイルオーバー・サーバー	22331

アクティブ・ディレクトリに登録する必要があるサービスの数は、現在のインストール状況に依存します。管理サーバー、記録サーバー、イベント・サーバー、をインストールするときに、データ・コレクタが自動的にインストールされます。

サービスを実行しているユーザーのために 2 つの SPN を登録する必要があります：1 つはホスト名で、1 つは完全修飾ドメイン名です。

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

SonySPN の命名方式:

ビデオ OS/[完全修飾ドメイン名]:[ポート]

ビデオ OS/[完全修飾ドメイン名]:[ポート]

以下は、次の詳細で、コンピュータ上で実行される記録サーバー・サービスの SPN の例です。:

ホスト名:**記録サーバー1**

ドメイン:Surveillance.com

登録する SPN:

ビデオ OS/録画サーバー1:7609

ビデオ OS/記録サーバー1.Surveillance.com:7609

ウイルススキャンについて

他のデータベースソフトウェアの場合と同様に、Network Video Management System 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破損したり、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 Recording Server のディレクトリ（デフォルトでは c:\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。

以下を除外に追加してください。

- ファイルのタイプ : .blk、.idx、.pic

- ディレクトリとすべてのサブディレクトリ：
 - C:¥Program Files¥Sony または C:¥Program Files (x86)¥Sony
 - C:¥ProgramData¥Sony¥MIPSDK
 - C:¥ProgramData¥Sony¥NVMS Mobile Server¥Logs
 - C:¥ProgramData¥Sony¥- Network VMS Data Collector Server¥Logs
 - C:¥ProgramData¥Sony¥- Network VMS Event Server¥logs
 - C:¥ProgramData¥Sony¥- Network VMS Log Server
 - C:¥ProgramData¥Sony¥- Network VMS Management Server¥Logs
 - C:¥ProgramData¥Sony¥- Network VMS Recording Server¥Logs
 - C:¥ProgramData¥Sony¥- Network VMS Report Web Server¥Logs
 - C:¥ProgramData¥Sony¥- Network VMS Service Channel¥Logs
- 以下の TCP ポートでのネットワークスキャンを除外：

製品	TCP ポート
Network Video Management System Enterprise Edition	80, 8080, 7563, 25, 21, 9993
NVMS Mobile	8081

または

- 以下のプロセスのネットワークスキャンを除外：

製品	プロセス
Network Video Management System Enterprise Edition	VideoOS.Recording.Service.exe、VideoOS.Server.Service.exe、VideoOS.Administration.exe
NVMS Mobile	VideoOS.MobileServer.Service.exe

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

ソフトウェアライセンスコードを登録する

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

Sony は、インストールする前で SLC を登録することをお勧めします。ライセンスガイドを参照してください。Web サイト <http://www.sony.net/CameraSystem> 。

システムのインストール

インストールオプションのいずれかを選択します。

- システムのインストール - シングルサーバーオプション 『29ページ』
- システムのインストール - 分散オプション 『30ページ』
- システムのインストール - カスタムオプション 『31ページ』

システムのインストール - シングルサーバーオプション

[シングルサーバー]オプションでは、すべての管理サーバーコンポーネント、レコーディングサーバー、および Network Video Management System Smart Client が現在のコンピュータにインストールされます。ハードウェアと構成によっては、最大 50~100 台のカメラから構成される小規模なシステムは 1 台のサーバーで実行できます。最小限の項目のみを選択するだけで、すべてのコンポーネントが編集不可のコンポーネントリストで事前選択されます。SQL Server はリストにありませんが、現在のコンピュータにはインストールされます。

1. インターネットからダウンロードしたバージョンをインストールする場合は、それを保存した場所から Sony - Network VMS Enterprise Edition Products 2016 R3 System Installer.exe ファイルを実行します。

あるいは、ソフトウェア DVD を挿入します。ダイアログボックスが自動的に開かない場合、DVD から Sony - Network VMS Enterprise Edition Products 2016 R3 System Installer.exe ファイルを実行します。
2. インストールファイルが展開されます。セキュリティの設定によって、1 つまたは複数の Windows® のセキュリティ警告が表示されます。これらを許可すると、展開が続行されます。
3. 完了すると、**Sony Network Video Management System Enterprise Edition** ダイアログボックスが表示されます。
 - a) インストール中に使用する言語を選択します（これは、インストール後にシステムで使用する言語ではありません。システムの言語は後で選択します）。**続行**をクリックします。
 - b) **ライセンスファイルの場所の入力**では、Network Video Management System プロバイダから入手したライセンスファイルを入力します。あるいは、参照機能を使用して検索します。続行する前に、ライセンスファイルがシステムで検証されます。**続行**をクリックします。
 - c) Sony エンドユーザー使用許諾契約を読みます。**使用許諾契約の条項に同意します**チェックボックスを選択します。
4. **シングルサーバー**を選択します。インストールするコンポーネントのリストが表示されます（このリストは編集できません）。**続行**をクリックします。
5. プログラムファイルの**ファイルの場所**を選択します。**製品の言語**では、Network Video Management System 製品をインストールする言語を選択します。**インストール**をクリックします。
6. ソフトウェアがインストールされます。完了すると、正常にインストールされたコンポーネントのリストが表示されます。**閉じる**をクリックします。

処理中には、Microsoft® IIS が自動的にインストールされます。後から、コンピュータを再起動するように指示される場合があります。再起動を実行します。再起動後、セキュリティの設定によって、1 つまたは複数の Windows のセキュリティ警告が表示される場合があります。これらを許可すると、インストールが完了します。

7. 終了すると、インストールが完了し、設定を続行できます。設定プロセス『39ページ の"Management Client のシステムの構成"参照』を参照してください。

システムのインストール - 分散オプション

【分散】オプションでは、管理サーバーコンポーネントだけが現在のコンピュータにインストールされます。レコーディングサーバーと Network Video Management System Smart Client は、編集不可のコンポーネントリストには表示されません。レコーディングサーバー、Network Video Management System Smart Client、および SQL Server を他のコンピュータにインストールする必要があります。

1. インターネットからダウンロードしたバージョンをインストールする場合は、それを保存した場所から Sony - Network VMS Enterprise Edition Products 2016 R3 System Installer.exe ファイルを実行します。

あるいは、ソフトウェア DVD を挿入します。ダイアログボックスが自動的に開かない場合、DVD から Sony - Network VMS Enterprise Edition Products 2016 R3 System Installer.exe ファイルを実行します。
2. インストールファイルが展開されます。セキュリティの設定によって、1 つまたは複数の Windows® のセキュリティ警告が表示されます。これらを許可すると、展開が続行されます。
3. 完了すると、**Sony Network Video Management System Enterprise Edition** ダイアログボックスが表示されます。
 - a) インストール中に使用する **言語** を選択します（これは、インストール後にシステムで使用する言語ではありません。システムの言語は後で選択します）。**続行** をクリックします。
 - b) **ライセンスファイルの場所の入力** では、Network Video Management System プロバイダから入手したライセンスファイルを入力します。あるいは、参照機能を使用して検索します。続行する前に、ライセンスファイルがシステムで検証されます。**続行** をクリックします。
 - c) **Sony エンドユーザー使用許諾契約** を読みます。**使用許諾契約の条項に同意します** チェックボックスを選択します。
4. **分散** を選択します。インストールするコンポーネントリスト（編集不可）が表示されます。**続行** をクリックします。
5. 必要な SQL Server データベースのタイプを選択します。また、SQL Server 名を指定します。**続行** をクリックします。
6. **新しいデータベースを作成する** または **既存のデータベースを使用** を選択し、データベースの名前を入力します。後者を選択した場合、既存データの **保持** または **上書き** を選択します。**続行** をクリックします。
7. プログラムファイルの **ファイルの場所** を選択します。**製品の言語** では、Network Video Management System 製品をインストールする言語を選択します。**インストール** をクリックします。
8. ソフトウェアがインストールされます。完了すると、正常にインストールされたコンポーネントのリストが表示されます。**閉じる** をクリックします。

処理中には、Microsoft® IIS が自動的にインストールされます。後から、コンピュータを再起動するように指示される場合があります。再起動を実行します。再起動後、セキュリティの設定によって、1 つまたは複数の Windows のセキュリティ警告が表示される場合があります。これらを許可すると、インストールが完了します。

9. 1つ以上のレコーディングサーバーと Network Video Management System Smart Client を別のコンピュータにインストールします。

参照

レコーディングサーバーのインストール 『32ページ』

クライアントのインストール 『41ページ』

システムのインストール - カスタムオプション

[カスタム] オプションでは常に管理サーバーをインストールしますが、現在のコンピュータにインストールする他の管理サーバーコンポーネント、レコーディングサーバー、および Network Video Management System Smart Client を自由に選択できます。デフォルトでは、レコーディングサーバーはコンポーネントリストでは選択されていませんが、これは編集可能です。選択内容によっては、SQL Server に加えて未選択のコンポーネントを後から他のコンピュータにインストールする必要があります。

1. インターネットからダウンロードしたバージョンをインストールする場合は、それを保存した場所から Sony - Network VMS Enterprise Edition Products 2016 R3 System Installer.exe ファイルを実行します。

あるいは、ソフトウェア DVD を挿入します。ダイアログボックスが自動的に開かない場合、DVD から Sony - Network VMS Enterprise Edition Products 2016 R3 System Installer.exe ファイルを実行します。
2. インストールファイルが展開されます。セキュリティの設定によって、1つまたは複数の Windows® のセキュリティ警告が表示されます。これらを許可すると、展開が続行されます。
3. 完了すると、**Sony Network Video Management System Enterprise Edition** ダイアログボックスが表示されます。
 - a) インストール中に使用する言語を選択します（これは、インストール後にシステムで使用する言語ではありません。システムの言語は後で選択します）。**続行**をクリックします。
 - b) **ライセンスファイルの場所の入力**では、Network Video Management System プロバイダから入手したライセンスファイルを入力します。あるいは、参照機能を使用して検索します。続行する前に、ライセンスファイルがシステムで検証されます。**続行**をクリックします。
 - c) **Sony エンドユーザー使用許諾契約**を読みます。**使用許諾契約の条項に同意します**チェックボックスを選択します。
4. **カスタム**を選択します。インストールするコンポーネントリストが表示されます。管理サーバーを除き、リストのすべての項目は任意です。デフォルトでは、レコーディングサーバーが選択されていませんが、必要に応じて変更できます。**続行**をクリックします。
5. 必要な SQL Server データベースのタイプを選択します。該当する場合、SQL Server 名も指定します。**続行**をクリックします。
6. **新しいデータベースを作成する**または**既存のデータベースを使用**を選択し、データベースの名前を入力します。後者を選択した場合、既存データの**保持**または**上書き**を選択します。**続行**をクリックします。
7. この**定義済みアカウント**またはこの**アカウント**を選択して、サービスアカウントを選択します。必要に応じて、パスワードを入力して確認します。**続行**をクリックします。
8. 使用可能な IIS Web サイトが複数ある場合は、いずれか1つを選択できます。ただし、Web サイトのいずれかに HTTPS バインドがある場合、その中から1つを選択します。**続行**をクリックします。

9. プログラムファイルの**ファイルの場所**を選択します。**製品の言語**では、Network Video Management System 製品をインストールする言語を選択します。**インストール**をクリックします。
10. ソフトウェアがインストールされます。完了すると、正常にインストールされたコンポーネントのリストが表示されます。**閉じる**をクリックします。

処理中には、Microsoft® IIS が自動的にインストールされます。後から、コンピュータを再起動するように指示される場合があります。再起動を実行します。再起動後、セキュリティの設定によって、1 つまたは複数の Windows のセキュリティ警告が表示される場合があります。これらを許可すると、インストールが完了します。

11. 選択内容によっては、他のコンピュータに残りのサーバーをインストールします。
 - a) Windows の[スタート]メニューから、管理サーバーのダウンロード用ウェブページへ移動します。
 - b) **[プログラム] > Sony > [Administrative Installation (管理インストール)]**ページを選択してから、インターネットのアドレスをコピーします。
 - c) インストールする各コンピュータにログインします。
 - ログサーバー。
 - イベントサーバー。
 - Management Client.
 - d) インターネットブラウザを開き、管理サーバーのダウンロード Web ページのアドレスをアドレスフィールドに入力し、関連するインストーラをダウンロードします。
 - e) インストーラを実行します。
12. レコーディングサーバーに個別のコンピュータをインストールします。レコーディングサーバーのインストール 『32ページ』を参照してください。

レコーディングサーバーのインストール

管理サーバーをインストールした時点で、管理サーバーの Web ページから、個別のレコーディングサーバーインストーラをダウンロードします。

1. 管理サーバーで、Windows の[スタート]メニューから、管理サーバーのダウンロード用ウェブページへ移動します。
2. **[プログラム]**を選択し、**[Sony]**、**[Administrative Installation (管理インストール)]**ページを選択してから、インターネットのアドレスをコピーします。
3. レコーディングサーバーをインストールするコンピュータにログインします。
4. インターネットブラウザを開き、管理サーバーのダウンロード Web ページのアドレスをアドレスフィールドに入力し、レコーディングサーバーインストーラを選択します。適切な場所にインストーラを保存して、ここから実行するか、Web ページから直接実行します。
5. インストール中に使用する**言語**を選択します。**続行**をクリックします。
6. 選択：
標準：デフォルト値でレコーディングサーバーをインストールします。

カスタム：レコーディングサーバーをカスタム値でインストールします。

7. レコーディングサーバー設定の指定：

- 名前。
- サーバーが接続する管理サーバーのアドレス。
- 録画を保存するパス。**続行**をクリックします。

8. **カスタム**を選択した場合：

- a) このコンピュータにインストールするレコーディングサーバー数を指定します。**続行**をクリックします。
 - b) サービスアカウントを指定します。必要に応じて、パスワードを入力して確認します。**続行**をクリックします。
9. プログラムファイルの**ファイルの場所**を選択します。**製品の言語**では、システムをインストールする言語を選択します。**インストール**をクリックします。
10. ソフトウェアがインストールされます。完了すると、正常にインストールされたコンポーネントのリストが表示されます。**閉じる**をクリックします。
- レコーディングサーバーがインストールされると、**Recording Server** サービスアイコンからその状態をチェックできます。
11. 終了すると、インストールが完了し、設定を続行できます。設定プロセス『39ページ の"Management Client のシステムの構成"参照』を参照してください。

レコーディングサーバーのサイレントインストール

サイレントインストールの利点は、リモートで実行できることです。次の手順に従います。

1. レコーディングサーバーのインストールファイルを検索します。
Sony-NetworkVMSRecordingServerInstaller_x64.exe。

1. 管理サーバーにログインします。

2. インターネットブラウザを開き、アドレスを入力します。http://localhost/Installation/Admin/

3. 新しいレコーディングサーバーをインストールするサーバーに、レコーディングサーバーのインストールファイルを保存します。

あるいはファイルを参照できます。標準的なパス：

C:¥Program Files¥Sony¥- Network VMS Management Server¥IIS¥httpdocs¥Admin¥Recording Server Installer¥[バージョン番号] [ビットバージョン]¥All Languages¥en-US

2. 次のオプションを使用してサイレントインストールを実行します。

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。

>Sony-NetworkVMSRecordingServerInstaller_x64.exe --quiet

- b カスタムインストールを実行するには、上書きするパラメータのリストを指定する必要があります。
たとえば、インストールする管理サーバーのパスを変更するには、以下のコマンドを実行します。

**><Sony-NetworkVMSRecordingServerInstaller_x64.exe --quiet
--parameters=SERVERHOSTNAME:DKWS-OKR-02**

これらのパラメータはコマンドラインパラメータから使用できます。

- レコーディングサーバーの名前を変更するには：

RECORDERNAME – Management Client に表示されるレコーダーの名前。

--quiet --parameters=RECORDERNAME:NewRecorderName

- 管理サーバーを変更するには：

SERVERHOSTNAME – Recording Server が接続する管理サーバーのホスト名

SERVERPORT – 管理サーバーのポート(デフォルトは 80)

--quiet --parameters=SERVERHOSTNAME:DKWS-OKR-02

- NT AUTHORITY¥NETWORK SERVICE 以外のユーザーとして Recording Server をインストールするには：

RECUSERACCOUNT – ユーザーアカウントが使用されているか、定義済みアカウントのいずれかが使用されているかどうかを判定するフラグ

RECSERVICEACCOUNT – 使用されているユーザー または定義済みサービスアカウントの名前

RECPASSWORD – 暗号化されています。ユーザーのパスワード。定義済みアカウントの場合は空にします。

暗号化バージョンのパスワードを確認するには、標準のモードでインストーラを実行できます。c:¥ProgramData¥Sony¥Installer¥Sony Network Video Management System Recording Server (64_bit)¥I.log を開きます(複数のインストールがコンピュータで実行された場合に名前の最後に追加される番号があります)。

文字列「Command Line」を検索します。次に、インストール中に使用されるパラメータの一覧を示します。ENCRYPTEDPASSWORD が表示されたパスワードは暗号化されています。

--quiet

--parameters=RECUSERACCOUNT:true:RECSERVICEACCOUNT:Sony¥okr:RECPASSWORD:encryptedpassword

- c デフォルトのインストール場所を変更するには、まず次のコマンドを実行する必要があります。

**><Sony-NetworkVMSRecordingServerInstaller_x64.exe
--generateargsfile=C:¥temp**

指定された場所にあるパラメータを含む.xml ファイルを見つけます。このため、このファイルのパラメータを変更し、新しい修正されたファイルでインストールを実行する必要があります。

- インストールの場所を変更するには：

INSTALLDIR - Recording Server がインストールされるパス

TARGETDIR – INSTALLDIR と同じ

INSTALLLOCATION – INSTALLDIR と同じ

- 録画の場所を変更するには：

MEDIADBPATH – すべての録画があるメディアデータベースへのパス

例：Argements_.xml の変更。新しいインストールの場所は%ProgramFiles(x86)%¥Sony¥bla になり、新しい録画の場所は C:¥MD になります。

```
<KeyValueParametersOfStringString>
  <Value>%ProgramFiles(x86)%¥Sony¥bla </Value>
  <Key>INSTALLDIR</Key>
</KeyValueParametersOfStringString>

<KeyValueParametersOfStringString>
  <Value>%ProgramFiles(x86)%¥Sony¥bla </Value>
  <Key>TARGETDIR</Key>
</KeyValueParametersOfStringString>

<KeyValueParametersOfStringString>
  <Value>%ProgramFiles(x86)%¥Sony¥bla </Value>
  <Key>INSTALLLOCATION</Key>
</KeyValueParametersOfStringString>

<KeyValueParametersOfStringString>
  <Value>C:¥MD </Value>
  <Key>MEDIADBPATH </Key>
</KeyValueParametersOfStringString>
```

以下のコマンドを実行します。

```
>< Sony-NetworkVMSRecordingServerInstaller_x64.exe --quiet
--arguments=C:¥temp¥Arguments_.xml
```

トラブルシューティング

インストールログファイルはどこにありますか。

インストールログファイルは **C:¥ProgramData¥Sony¥Installer¥** にあります。

1 台のサーバーのインストール中に使用されるデフォルトパラメータの一覧はどこで確認できますか。

パラメータとすべてのデフォルト値の一覧を表示するには、

Sony-NetworkVMSRecordingServerInstaller_x64.exe --generateargsfile=C:¥temp を実行できます。

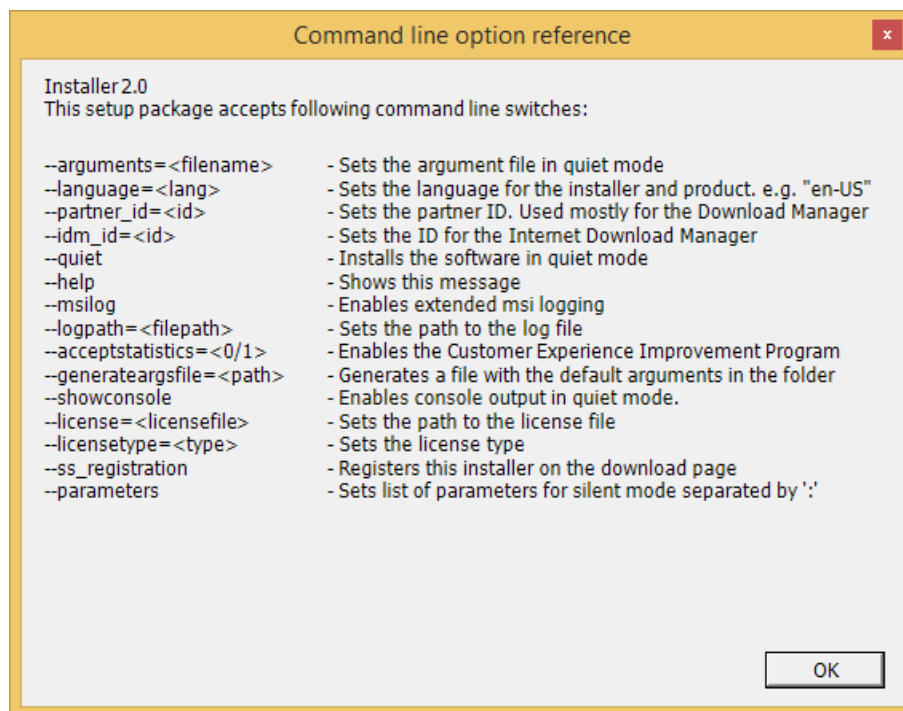
ファイル Arguments.xml が指定されたフォルダに生成されます。

カスタムインストール中に使用されたパラメータはどのように確認できますか。

インストールの実行中に使用されたパラメータの一覧は、**C:¥ProgramData¥Sony¥Installer¥Sony - Network VMS Recording Server (64_bit)I.log** にあります。「Command line」を検索してください。

使用可能なパラメータの一覧はどこで確認できますか。

Sony-NetworkVMSRecordingServerInstaller_x64.exe --help を実行します。



Kerberos 認証を設定します。

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

詳細な内容は Kerberos 認証について 『26ページ』を参照してください。

ワークグループのインストール

Active Directory サーバーのドメイン設定ではなく、ワークグループ設定を使用する場合は、インストール時に以下を実行します。

1. 共通管理者アカウントを使用して、Windows へログインします。

システムのすべてのコンピュータで同じアカウントを使用していることを確認します。

2. 必要に応じて、管理サーバーまたはレコーディングサーバーのインストールを開始し、**カスタム**をクリックします。
3. 選択に応じて、手順 2 で共通の管理者アカウントを使用して、**Management Server** サービスまたは **Recording Server** サービスのインストールを選択します。
4. インストールを終了します。
5. 手順 1~4 を繰り返し、接続する他のすべてのシステムをインストールします。これらはすべて、共通管理者アカウントを使用してインストールしなければなりません。

ワークグループインストールをアップグレードする場合は、この方法を使用できません。「ワークグループの代替アップグレード 『48ページ の"ワークグループの他のアップグレード方法"参照 』」を参照してください。

インストールのトラブルシューティング

Management Server や Recording Server のインストール中、またはその後に、以下のような問題が発生することがあります。それぞれの問題に対して、1 つまたは複数の解決策があります。

問題：ポートの競合により Recording Server の起動が失敗する

この問題が発生するのは、簡易メール転送プロトコル(SMTP)サービスがポート 25 で実行されている場合だけです。ポート 25 がすでに使用中であれば、Recording Server サービスを開始することはできません。レコーディングサーバーの SMTP サービス用に、ポート 25 番が使用可能な状態でなければなりません。

SMTP サービス：検証とソリューション

SMTP サービスがインストールされていることを検証するには、次の手順を実行してください。

1. Windows のスタートメニューで、**コントロールパネル**を選択します。
2. コントロールパネルで、**プログラムの追加と削除**をダブルクリックします。
3. **プログラムの追加と削除**ウィンドウの左側で、**Windows コンポーネントの追加と削除**をクリックします。
4. **Windows コンポーネントウィザード**で、**インターネットインフォメーションサービス(IIS)**を選択し、**詳細...**をクリックします。
5. **インターネットインフォメーションサービス(IIS)**ウィンドウで、**SMTP サービス**のチェックボックスが選択されていることを確認します。選択されていれば、SMTP サービスはインストールされています。

SMTP サービスがインストールされていれば、以下のソリューションのいずれか 1 つを選択します：

ソリューション 1：SMTP サービスを無効にするか、手動起動に設定する

このソリューションでは、毎回 SMTP サービスを停止することなく、Recording Server を起動できます。

1. Windows のスタートメニューで、**コントロールパネル**を選択します。
2. コントロールパネルで、**管理ツール**をダブルクリックします。
3. **管理ツール**ウィンドウで、**サービス**をダブルクリックします。
4. **サービス**ウィンドウで、**簡易メール転送プロトコル(SMTP)**をダブルクリックします。

5. SMTPのプロパティウィンドウで、**停止**をクリックしてから、**スタートアップの種類**を**手動**または**無効**に設定します。

手動に設定すると、SMTPサービスをサービスウィンドウから手動で起動するか、コマンド `net start SMTPSVC` を使用してコマンドプロンプトから起動することができます。

6. **OK** をクリックします。

ソリューション 2：リモート SMTP サービス

SMTP サービスを削除すると、SMTP サービスを使用している他のサービスに影響する場合があります。

1. Windows のスタートメニューで、**コントロールパネル**を選択します。
2. コントロールパネルで、**プログラムの追加と削除**をダブルクリックします。
3. **プログラムの追加と削除**ウィンドウの左側で、**Windows コンポーネントの追加と削除**をクリックします。
4. **Windows コンポーネントウィザード**で、**インターネットインフォメーションサービス(IIS)**アイテムを選択し、**詳細**をクリックします。
5. **インターネットインフォメーションサービス(IIS)**ウィンドウで、**SMTP サービス**のチェックボックスがクリアされます。
6. **OK**、**次へ**、さらに**完了**の順にクリックします。

問題：SQL Server の位置を変更すると、データベースにアクセスできない

たとえばSQL Server を実行しているコンピュータのホスト名を変更するなど、SQL Server の位置を変えると、問題となります。この問題の結果、データベースへのアクセスが失われます。

解決策：トレイアイコンにある **SQL アドレスの更新ツール**を使用します。

Management Client のシステムの構成

以下に、一般的にシステムのセットアップに必要なタスクの一覧を示します。

タスクはチェックリストとして一覧表示されていますが、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組織の要件に一致することを保証しているわけではありません。システムを組織の必要性に一致させるために、Sony は、システムの起動後も、システムを継続的にモニターし、調整することをお勧めします。

たとえば、システムを起動した後、異なる物理的条件（昼/夜、強風/穏やかな天候など）で個々のカメラのモーション検知感度の設定をテストして調整することをお勧めします。

ルールの設定は、システムが実行するアクション（ビデオを録画する場合など）の大半を決定するものであり、組織のニーズに合わせて変更できる設定のもう一つの例です。

<input checked="" type="checkbox"/>	システムの初期インストールが完了しました。 システムのインストール 『29ページ』を参照してください。
<input checked="" type="checkbox"/>	試用版 SLC を恒久版 SLC に変更します（必要な場合）。 ソフトウェアライセンスコードの変更 『40ページ』を参照してください。
<input checked="" type="checkbox"/>	Management Client へログインします。
<input type="checkbox"/>	システムのレコーディングサーバーの使用を許可します。 レコーディングサーバーの認証 『62ページ』を参照してください。
<input type="checkbox"/>	それぞれのレコーディングサーバーのストレージの設定が要件を満たしていることを確認します。 ストレージとアーカイブについて 『65ページ』を参照してください。

<input type="checkbox"/>	それぞれのレコーディングサーバーのアーカイブ設定が要件を満たしていることを確認します。 アーカイブ設定のプロパティ 『72ページ』を参照してください。
<input type="checkbox"/>	それぞれのレコーディングサーバーに追加する必要があるハードウェア（例、カメラおよびビデオエンコーダー）を検出します。 ハードウェアの追加 『79ページ』を参照してください。
<input type="checkbox"/>	それぞれのレコーディングサーバーの個々のカメラを設定します。 カメラデバイスについて 『90ページ』を参照してください。
<input type="checkbox"/>	個別のカメラまたはカメラのグループのストレージとアーカイブを有効にします。この操作は、カメラごと、またはデバイスグループに対して行えます。 個別のデバイスまたはデバイスのグループをストレージに接続する 『68ページ』を参照してください。
<input type="checkbox"/>	デバイスを有効にして設定します。 デバイスの使用 『90ページ』を参照してください。
<input type="checkbox"/>	ルールはシステムの動作を大きく決定します。ルールには、カメラが録画するとき、パン/チルト/ズーム(PTZ)カメラがパトロールするとき、通知が送信される時などが含まれます。 ルールを作成します。 ルールとイベントについて 『138ページ』を参照してください。
<input type="checkbox"/>	役割をシステムに追加します。 役割について 『172ページ』を参照してください。
<input type="checkbox"/>	ユーザーまたはユーザーのグループを各役割に追加します。 ユーザーおよびグループの役割からの削除、役割への割り当て 『175ページ』を参照してください。
<input type="checkbox"/>	ライセンスを認証します。 ライセンスを認証（オフライン） 『59ページ の"ライセンスをオフラインで認証"参照』を参照してください。

ソフトウェアライセンスコードの変更

最初は、試用版のソフトウェアライセンスコード(SLC)を使ってインストールを実行している場合、新しいソフトウェアライセンスファイルを受け取った時点で、アンインストールまたは再インストールを実行せずに永久版SLCに変更できます。

重要：これは管理サーバーでローカルに行う必要があります。 Management Client でこれを実行することはできません。

1. 管理サーバーで、タスクバーの通知エリアへ移動します。



2. 管理サーバーアイコンを右クリックし、**ライセンスの変更**を選択します。
3. **ライセンスのインポート**をクリックします。
4. 次に、この目的で保存したソフトウェアライセンスファイルを選択します。完了すると、**ライセンスのインポート**ボタンのすぐ下に、選択したソフトウェアライセンスファイルの場所が追加されます。
5. **OK** をクリックします。SLC を登録する準備ができました。ソフトウェアライセンスコードの登録 『28 ページ』の"ソフトウェアライセンスコードを登録する"参照』を参照してください。

ローカル IP アドレス範囲について

Network Video Management System Smart Client などのクライアントが、監視システムに接続する場合、連絡先アドレスの交換などの初期データ通信が、バックグラウンドで実行されます。これは自動的に行われ、ユーザーには認識されません。

クライアントはローカルネットワークに加えてインターネットから接続することもあります。それぞれの場合に、レコーディングサーバーからのライブビデオや録画ビデオにクライアントがアクセスできるように、監視システムは適切なアドレスを提供する必要があります。

- クライアントがローカルで接続する場合、監視システムはローカルのアドレスおよびポート番号を返さなければなりません。
- クライアントがインターネットから接続する場合、監視システムはレコーディングサーバーのパブリックアドレス、および異なるポート番号（次にレコーディングサーバーに転送されます）を返さなければなりません。ここでパブリックアドレスとはファイアウォールまたは NAT（ネットワークアドレス変換）ルーターのアドレスです。

したがって、監視システムはクライアントがローカル IP 範囲に属しているのか、あるいはインターネットにあるのかを判断できなければなりません。この目的で、監視システムがローカルネットワークから来ていると認識できる IP 範囲のリストを定義できます。

クライアントのインストール

Network Video Management System Smart Client のクライアントインストール

Microsoft Systems Management Server (SMS) などのツールを使用して、Network Video Management System Smart Client または監視ソフトウェアをユーザーのコンピュータに展開できます。このようなツールを使って、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って、さまざまな操作を実行できますが、その 1 つとして、Network Video Management System Smart Client などの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し、インストールすることができます。

1. 32 ビットおよび 64 ビットバージョンの Smart Client インストールプログラム (.exe) ファイル、*Sony – Network VMS Smart Client 2016 R3 Installer.exe* または *Sony – Network VMS Smart Client 2016 R3 Installer x64.exe* をそれぞれ特定してください。このファイルは、**httpdocs** フォルダの下のサブフォルダにあります。**httpdocs** フォルダは、Sony 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。

パスは、通常、

C:\Program Files\Sony\Network VMS Management Server\IS\httpdocs-

Network VMS Smart Client Installer¥[version number] [bit-version]¥All Languages¥en-US です。

例:

C:¥Program Files¥Sony¥- Network VMS Management Server¥IIS¥httpdocs¥- Network VMS Smart Client Installer¥2016 (32-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。

> Sony – Network VMS Smart Client 2016 R3 Installer.exe --quiet

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

- b xml 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設定をカスタマイズするには、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(cmd.exe)を起動して、以下のコマンドを実行します。

> Sony – Network VMS Smart Client 2016 R3 Installer.exe --generateargsfile=[path]

生成された Arguments.xml ファイルを、Windows のメモ帳などを使用して開き、必要に応じて変更します。次に、これらの変更された値を使用してサイレントインストールを実行するには、同じディレクトリで以下のコマンドを実行します。

> Sony – Network VMS Smart Client 2016 R3 Installer.exe --arguments=args.xml --quiet

NVMS Mobile サーバーのインストール

NVMS Mobile サーバーをインストールすると、NVMS Mobile クライアントと Network Video Management System Web Client を、ご自分のシステムで使用できます。管理サーバーを実行するコンピュータのシステムリソースの使用量を全体的に減らすには、個別のコンピュータ上に NVMS Mobile サーバーをインストールします。

管理サーバーには、ビルトインの公開インストール Web ページがあります。この Web ページでは、管理者およびエンドユーザーが、管理サーバーまたは他のすべてのシステムのコンピュータから必要な Network Video Management System をダウンロードしてインストールできます。

インストール Web ページにアクセスするには、

1. ブラウザで次の URL を入力します。http://[管理サーバーのアドレス]/installation/admin
[管理サーバーのアドレス]は管理サーバーの IP アドレスまたはホスト名です。
2. NVMS Mobile サーバーインストーラで[すべての言語]をクリックします。
3. ダウンロードしたファイルを実行します。すべての警告で[はい]をクリックします。解凍が開始します。
4. インストーラの言語を選択してください。続行をクリックします。

5. 使用許諾契約を読み、同意します。**続行**をクリックします。
6. インストールのタイプを選択してください。**[標準]**をクリックすると、デフォルトの選択内容でインストールされます。
7. プライマリ監視システムサーバーを指定：
 - 管理サーバーの URL
 - ログイン
 - ユーザー名とパスワード。**続行**をクリックします。
8. ファイルの場所および製品の言語を選択してください。**インストール**をクリックします。インストールが完了したら、正常にインストールされたコンポーネントの一覧が表示されます。**閉じる**をクリックします。

NVMS Mobile の構成 『225ページ の"NVMS Mobile 構成"参照』の準備ができました。

Download Manager/ダウンロード Web ページ

Management Server には、組み込み Web ページがあります。この Web ページを使うと、管理者やエンドユーザーは Network Video Management System システムの必要なコンポーネントを、任意の場所から（ローカルまたはリモートで）ダウンロードしてインストールすることができます。

この Web ページは、デフォルトで、システムインストールの言語と一致する言語バージョンで、次の 2 種類のコンテンツを表示できます。

- **管理者向けの Web ページ**では、主要なシステムコンポーネントをダウンロードしてインストールできます。通常、Web ページは管理サーバーのインストール終了後に自動的に読み込まれ、デフォルトのコンテンツが表示されます。管理サーバーで、Windows のスタートメニューから**プログラム > Sony > 管理インストールページ**の順に選択し、Web ページにアクセスできます。それ以外の場合は、以下の URL を入力してください。

`http://[管理サーバーのアドレス]:[ポート]/installation/admin/`

[管理サーバーのアドレス]は管理サーバーの IP アドレスまたはホスト名であり、[ポート]は管理サーバーで IIS が使用するよう設定されたポート番号です。管理サーバーの Web ページにアクセスできない場合は、管理サーバーの管理者権限を持つアカウントでログインします。

- **エンドユーザー向けの Web ページ**では、デフォルト設定を使用してクライアントアプリケーションにアクセスできます。管理サーバーで、Windows のスタートメニューから**プログラム > Sony > 公開インストールページ**の順に選択し、Web ページにアクセスできます。それ以外の場合は、以下の URL を入力してください。

`http://[管理サーバーのアドレス]:[ポート]/installation/`

[管理サーバーのアドレス]は管理サーバーの IP アドレスまたはホスト名であり、[ポート]は管理サーバーで IIS が使用するよう設定されたポート番号です。

2 つの Web ページにはデフォルトのコンテンツがあるため、インストール後すぐに使用できます。ただし、管理者として Download Manager を使用すると、Web ページの表示内容をカスタマイズできます。また、Web ページの 2 つのバージョン間で、コンポーネントを移動することもできます。コンポーネントを移動するには、コンポーネントをクリックし、コンポーネントを移動する Web ページのバージョンをクリックします。

Download Manager では、ユーザーがダウンロードしてインストールできるコンポーネントを制御できますが、ユーザーの権限管理ツールとして使用することはできません。こうした権限は、Management Client で定義された役割によって決まります。

管理サーバーで、Windows のスタートメニューから **プログラム > Sony > Network Video Management System Download Manager** の順に選択し、Network Video Management System Download Manager にアクセスできます。

Download Manager のデフォルト設定

Download Manager には、デフォルトの設定があります。これにより、組織のユーザーは最初から標準のコンポーネントにアクセスできます。

デフォルト設定では、追加またはオプションのコンポーネントをデフォルト設定によってダウンロードできます。通常は、管理サーバーコンピュータから Web ページにアクセスしますが、他のコンピュータから Web ページにアクセスすることもできます。

- 1 番目のレベル : Network Video Management System 製品を参照します。
- 2 番目のレベル : Web ページの 2 つの対象バージョンを示しています。デフォルトは、エンドユーザーに表示される Web ページのバージョンを示しています。管理は、システム管理者に表示される Web ページのバージョンを示しています。
- 3 番目のレベル : Web ページで使用できる言語を示しています。
- 4 番目のレベル : ユーザーが使用できるか、使用可能にできるコンポーネントを示しています。
- 5 番目のレベル : ユーザーが使用できるか、使用可能にできる各コンポーネントの特定のバージョンを示しています。
- 6 番目のレベル : ユーザーが使用できるか、使用可能にできるコンポーネントの言語バージョンを示しています。

初期状態では標準のコンポーネントだけが使用可能であり、システムと同じ言語バージョンだけが使用可能になっていることで、インストールの時間を短縮し、サーバーのディスク容量を節約するのに役立ちます。誰も使用しないコンポーネントや言語バージョンがサーバーに存在する必要はないためです。

必要に応じてその他のコンポーネントや言語を使用可能にできます。また、不要なコンポーネントや言語を非表示にしたり削除したりできます。

Download Manager の標準インストーラ (ユーザー)

デフォルトでは、次のコンポーネントは、ユーザー向けの管理サーバーのダウンロード Web ページから個別にインストールできます (Download Manager で制御)。

- レコーディング サーバー。
- Management Client
- Network Video Management System Smart Client
- イベントサーバー、マップ機能と組み合わせて使用されます。
- ログサーバーは、システム情報のロギングに必要な機能を提供するために使用されます。
- サービスチャンネルを使用すると、サーバーとクライアント間での自動的で透明な設定の通信が可能になります。

- NVMS Mobile サーバー - ここでのみ使用可能です。
- 組織によって、より豊富なオプションを利用できます。

Download Manager インストーラコンポーネントの追加と公開

次の 2 つの手順を実行し、標準以外のコンポーネントおよび新しいバージョンを管理サーバーのダウンロードページで使用可能にする必要があります。

まず、**新しいコンポーネントまたは標準以外のコンポーネントを Download Manager に追加**します。次に、これを使用して、さまざまな言語バージョンの Web ページで、**どのコンポーネントを使用可能にするかを微調整**します。

Download Manager が開いている場合は、閉じてから、新しいコンポーネントをインストールします。

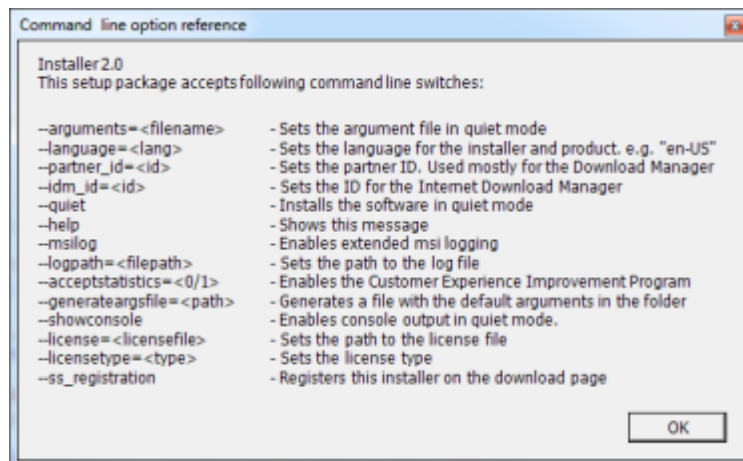
新しいファイルまたは標準以外のファイルを **Download Manager に追加**する：

1. コンポーネントをダウンロードしたコンピュータで、Windows のスタートに移動し、コマンドプロンプトに入ります。
2. コマンドプロンプトで、ファイル名 (.exe) に[space]--ss_registration を付けて実行します。

例：*RecordingServer_setup_x64.exe --ss_registration*

これでファイルが Download Manager に追加されます。ただし、現在のコンピュータにはインストールされません。

インストーラコマンドの概要については、コマンドプロンプトで、[space]--help と入力すると、次のウィンドウが表示されます。



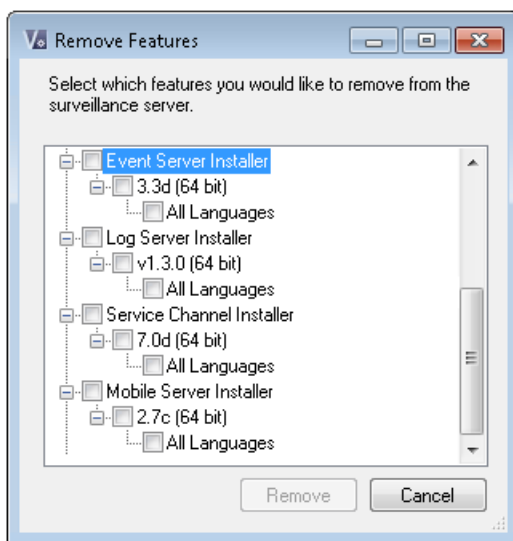
新しいコンポーネントをインストールすると、Download Manager でデフォルトで選択され、Web ページからすぐに使用可能になります。Download Manager のツリー構造でチェックボックスを選択または選択解除することで、Web ページでいつでも機能を表示または非表示にすることができます。

Web ページで、コンポーネントが表示される順番を変更できます。Download Manager のツリー構造で、コンポーネントアイテムをドラッグして必要な場所でドロップすると、順番を変更できます。

Download Manager インストーラコンポーネントの非表示および削除

次の3つのオプションがあります。

- Download Manager のツリー構造のチェックボックスをクリアして、Web ページからのコンポーネントを非表示にすることができます。コンポーネントは Management Server にインストールされたままであり、Download Manager のツリー構造のチェックボックスを選択することで、迅速にコンポーネントを再び利用可能にできます。
 - 管理サーバーにあるコンポーネントのインストールを削除します。コンポーネントは Download Manager に表示されなくなりますが、コンポーネントのインストールファイルは *C:\Program Files (x86)\Sony\Network VMS Download Manager* に保存されるため、必要であれば、この後再インストールすることができます。
1. Download Manager で、**機能の削除**をクリックします。
 2. **機能の削除**ウィンドウで、削除する機能を選択します。



3. **OK** とはいをクリックします。
- **不要な機能のインストールファイル**は、管理サーバーから削除できます。組織では使用しない機能が分かっている場合、これによって、サーバーのディスク容量を削減するのに役立ちます。

デバイスパックのインストーラ - ダウンロードする必要があります

元のインストールに含まれていたデバイスパック（デバイスドライバーを含む）は、ダウンロード Web サイトには含まれていません。このため、デバイスパックを再インストールするか、またはデバイスパックインストーラを使用可能にするためには、Download Manager に最新のデバイスパックインストーラを追加/公開する必要があります。

1. Sony Web サイト <http://www.sony.net/CameraSystem/NVMS/Software> のダウンロードのページで、最新のデバイスパックが入手できます。
2. `--ss_registration` コマンドを使用して呼び出し、Download Manager に追加/公開します。

ネットワークに接続していない場合は、Download Manager からレコーディングサーバー全体を再インストールできます。レコーディングサーバーのインストールファイルは、コンピュータにローカル保存されます。これにより、デバイスパックが自動的に再インストールされます。

アップグレード

アップグレードについて

この情報は、Network Video Management System の以前のインストールからアップグレードする場合にだけ必要です。

重要：現在、Network Video Management System システムでは Microsoft Windows XP をサポートしていません。

アップグレード時には、管理サーバーデータベースを除くすべてのコンポーネントが自動的に削除および置換されます。これにはデバイスパックのドライバーも含まれます。

管理サーバーデータベースは、システム全体の設定（レコーディングサーバーの設定、カメラの設定、ルールなど）を含んでいます。管理サーバーデータベースを削除しない限り、システムの設定を再構成する必要はありません（ただし、新しいバージョンの新機能の設定が必要になる場合もあります）。

現在のバージョンより前の Network Video Management System バージョンのレコーディングサーバーとの後方互換性には制限があります。旧バージョンのレコーディングサーバーの録画にアクセスすることはできますが、それらの設定を変更するには、現在バージョン以上であることが必要です。このため、Sony はシステムのすべてのレコーディングサーバーをアップグレードすることを強くお勧めします。

レコーディングサーバーを含めてアップグレードするときには、ビデオデバイスドライバーを**更新**するか**保持**するかを確認するメッセージが表示されます。更新を選択する場合、システムの再起動後、ハードウェアデバイスが新しいビデオデバイスドライバーと接続するまでに数分かかる場合があります。これは、新しくインストールされたドライバーについて、いくつかの内部チェックが行われるためです。

アップグレードの前提条件

- ソフトウェアライセンスファイル 『19ページ の"ライセンスについて"参照 』（.lic）を用意します。
 - **サービスパックアップグレード：**管理サーバーのインストール中に、ウィザードで、ソフトウェアライセンスファイルの場所を指定しなければならない場合があります。システム(最新のアップグレード)の購入後に入手したソフトウェアライセンスコードと、最後のライセンス認証の後に入手した認証済みソフトウェアライセンスファイルの両方を使用できます。
 - **バージョンアップグレード：**新しいバージョンを購入した後で、新しいソフトウェアライセンスファイルを受け取ります。管理サーバーのインストール中に、ウィザードで、新しいソフトウェアライセンスファイルの場所を指定する必要があります。

続行する前に、ソフトウェアライセンスファイルがシステムで検証されます。既に追加されたハードウェアデバイスとその他のデバイスの場合、ライセンスが猶予期間に入る必要があります。ソフトウェアライセンスファイルがない場合は、Network Video Management System のリセラーまでお問い合わせください。

- **新しい製品バージョンソフトウェア**を用意してください。ソフトウェア DVD を購入していない場合は、Sony Web サイト <http://www.sony.net/CameraSystem/NVMS/Software> のダウンロードページからダウンロードできます。

- システム構成をバックアップ『246ページ』の"システム設定のバックアップおよび復元について"参照』したことを確認します。

管理サーバーは、システムの設定をデータベースに保存します。システム設定データベースは、次の2つの方法で保存できます。

1. 管理サーバー自体の SQL Server Express Edition データベース。
2. ネットワーク上の既存の SQL Server のデータベース

2)を使用する場合、SQL Server に管理サーバーのシステム設定を作成、移動またはアップグレードする際に、**SQL Server に対する管理者権限**が必要になります。作成、移動またはアップグレードが完了した後は、SQL Server にある管理サーバーのシステム設定データベースの所有者であれば十分です。

アップグレードを開始する準備ができれば、「アップグレードの推奨手順『48ページ』」の手順に従います。

アップグレードの推奨手順

実際のアップグレードを開始する前に、SQL データベースバックアップを含むアップグレードの前提条件『47ページ』をお読みください。

システムが単一サーバーシステムの場合は、新しい Network Video Management System Enterprise Edition ソフトウェアを既存のインストールの上にインストールできます。

次の順序でアップグレードを実行します。

1. インストーラで **Distributed** オプションを使用して、管理サーバーをアップグレードします。
1. コンポーネントを選択するウィザードのページでは、すべての管理サーバーコンポーネントがあらかじめ選択されています。
2. SQL Server を指定し、データベースを保持することを選択します。
2. レコーディングサーバーをアップグレードします。インストールウィザードを使用『32ページ』の"レコーディングサーバーのインストール"参照』するか、サイレント『33ページ』の"レコーディングサーバーのサイレントインストール"参照』でレコーディングサーバーをインストールできます。サイレントインストールの利点は、リモートで実行できることです。
3. イベントサーバーをアップグレードします。管理サーバーのダウンロード Web ページから、Event Server をインストールします。

システムの他のサイトでもこの手順を続けます。

ワークグループの他のアップグレード方法

ドメイン設定ではなくワークグループ設定を使用する場合は、アップグレード時に以下を実行する必要があります。

1. 管理サーバーでローカル Windows ユーザーを作成します。
2. Windows のコントロールパネルで、**Sony Network Video Management System Data Collector** サービスを検索します。これを右クリックして**プロパティ**を選択し、**ログオン**タブを選択します。Data Collector サービスを設定して、レコーディングサーバーで作成したローカル Windows ユーザーとして実行します。
3. 管理サーバーで、同じローカル Window ユーザー（同じユーザー名とパスワード）を作成します。

4. Management Client で、このローカル Windows ユーザーを**管理者**グループに追加します。
ワークグループを使用してインストールする場合は、ワークグループのインストール 『36ページ』を参照してください。

初めての使用

推奨事例

記録データベースを破損から守る

カメラデータベースが破損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、Sony は、カメラデータベースが破損しないことを保証する手順を導入することをお勧めします。

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（必ず無停止電源装置（UPS）を使用してください）
- 静電気（ハードディスクドライブを取り扱う場合には、必ず接地してください）
- 火、水など（避けてください）

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。

停電：UPS の使用

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

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

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

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

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。

例：

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

秋：DST から標準時間へ切り替える

秋に DST から標準時間へ切り替えるとき、時計を 1 時間戻します。

例：

時計は 02:00 (DST) から 01:00 (標準時間) に戻されるので、その日は 25 時間となります。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。最初の 01:30 は、2 回目の 01:30 によって上書きされます。

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

タイムサーバーについて

システムが画像を受信すると、ただちにタイムスタンプが付けられます。カメラは別個のユニットであり、別個のタイミングデバイスを持っているので、カメラの時刻と使用しているシステムの時刻が完全に一致していないことがあります。これが混乱の原因になる場合があります。カメラがタイムスタンプをサポートしている場合、Sony 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 <http://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。

Management Client 概要

ログイン概要

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

ログイン認証について

管理者は、ユーザーを設定することで、十分な権限を持つ 2 番目のユーザーがログインを許可した場合にのみシステムにログインさせることができます。この場合、Network Video Management System Smart Client または Management Client では、ログイン中に 2 番目の認証を要求されます。

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

ログイン認証を役割に関連付けるには：

- **【役割】**の下の**【情報】**タブ 『177ページ の"情報タブ(役割)"参照 』で、選択した役割の**【ログイン認証が必要】**を設定し、ユーザーがログイン中に追加の認証を要求されるようにします。
- **【役割】**の下の**【セキュリティ全般】**タブ 『177ページ の"セキュリティ全般タブ (役割) "参照 』で選択した役割の**【ユーザーを認証】**を設定し、ユーザーが他のユーザーのログインを認証できるようにします。

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

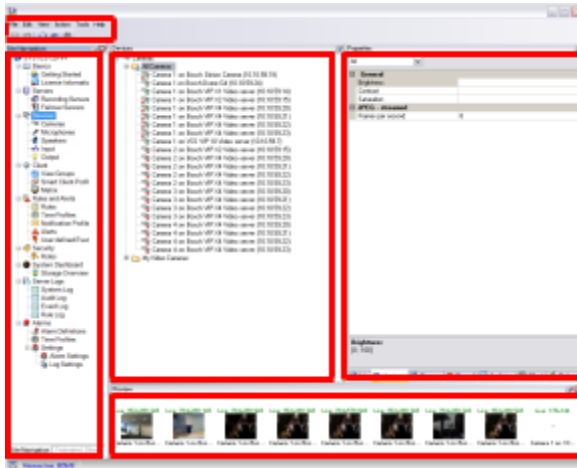
Management Client ウィンドウ概要

Management Client ウィンドウはペインに分割されます。ペインとレイアウトの数は以下によって異なります。

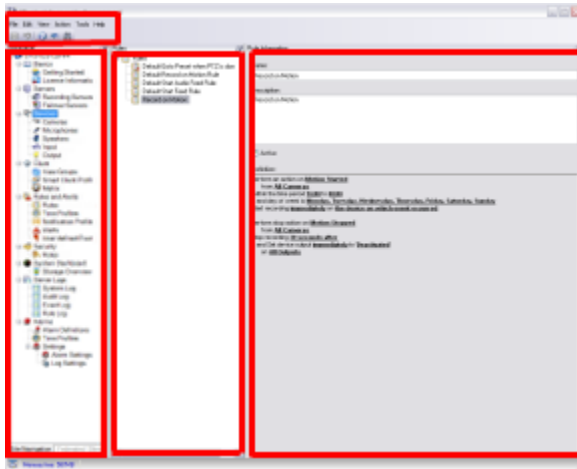
- システム設定
- タスク
- 使用可能な機能。

以下は通常のレイアウト例です：

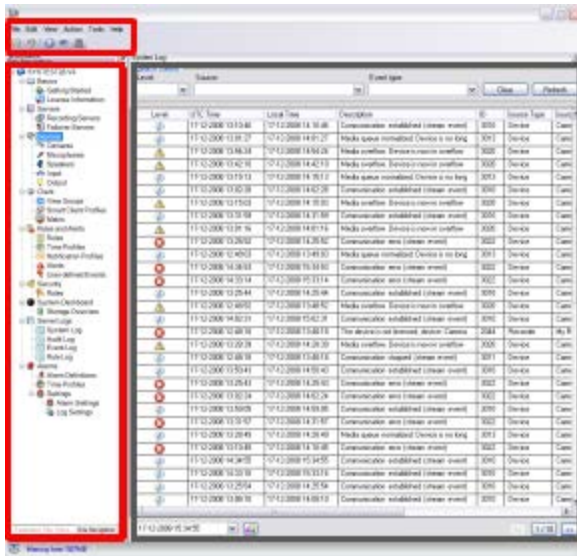
- レコーディングサーバーおよびデバイスで作業する場合：



- ルール、時間および通知プロファイル、ユーザー、ロールで作業する場合：

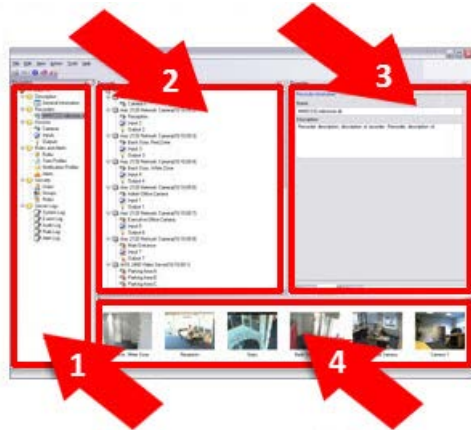


- ログを表示する場合：



ペインの概要

図は通常のウィンドウのレイアウトを概説しています。カスタマイズが可能なので、使用しているコンピュータによってレイアウトは異なります。



1. サイトナビゲーションペイン
2. 概要ペイン
3. [プロパティ] ペイン
4. プレビュー ペイン

サイトナビゲーションペイン：これは Management Client の中心的なナビゲーションエレメントです。ログインしたサイトの名前、設定および構成が反映されます。サイト名はペインの上部に表示されます。ソフトウェアの機能を反映して、機能はカテゴリにグループ化されます。

概要ペイン：**サイトナビゲーションペイン**で選択したエレメント（例えば詳細リストなど）の概要を提供します。**概要ペイン**でエレメントを選択すると、通常は**プロパティペイン**にプロパティが表示されます。**概要ペイン**でエレメントを右クリックすると、管理機能へのアクセスが得られます。

プロパティペイン：**概要ペイン**で選択したエレメントのプロパティを表示します。プロパティは複数の専用タブに表示されます。



タブに表示されたプロパティの例

プレビューペイン：**プレビューペイン**はレコーディングサーバーおよびデバイスで作業するときに表示されます。選択されたカメラからのプレビュー画像を表示したり、デバイスの状態についての情報を表示します。この例では、カメラのプレビュー画像およびカメラのライブストリームの解像度やデータ転送速度の情報を示しています。

Live: 640x480 88kB

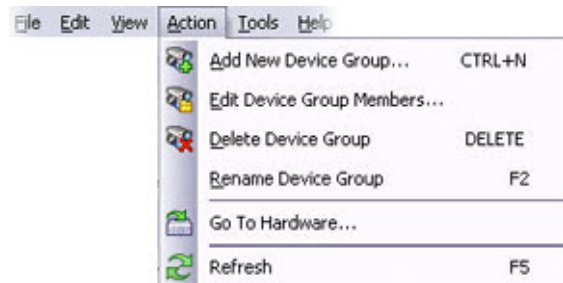


Camera 5

デフォルトでは、カメラのプレビュー画像に表示されている情報はライブストリームに関する情報です。プレビュー画像の上に緑色のテキストで表示されます。代わりにレコーディングストリーム情報（赤色のテキスト）を表示したい場合は、メニューで**ビュー > レコーディングストリームを表示**を選択します。

プレビューペインで、多数のカメラからのプレビュー画像を高いフレームレートで表示すると、パフォーマンスに影響することがあります。プレビュー画像の数やフレームレートをコントロールするには、メニューで、**オプション > 一般**を選択します。

メニュー概要



例、状況によって一部のメニューは異なります。

ファイルメニュー

変更を設定に保存して、アプリケーションを終了します。設定のバックアップもできます。システム設定のバックアップおよび復元について 『246ページ』をご覧ください。

編集メニュー

変更を元に戻すことができます。

ビューメニュー

名前	詳細
アプリケーションレイアウトのリセット	Management Client のさまざまなペインのレイアウトをデフォルトの設定にリセットします。
プレビューウィンドウ(P)	レコーディングサーバーやデバイス进行操作する際に、プレビューペインをオンまたはオフに切り替えられます。
レコーディングストリームを表示(S)	デフォルトでは、プレビューペインのプレビュー画像に表示されている情報は、カメラのライブストリームに関する情報です。代わりにレコーディングストリームに関する情報が必要な場合は、レコーディングストリームを表示を選択します。

アクションメニュー

アクションメニューの内容はサイトナビゲーションペインで選択したエレメントにより異なります。選択できるアクションはエレメントを右クリックする時と同じです。エレメントは Management Client エレメント 『57ページ』で説明されています。

名前	詳細
更新	常に使用可能であり、必要な情報を Management Server から再ロードします。

ツールメニュー

名前	詳細
登録済みサービス	登録済みサービスの管理。 サービスチャンネルについて 『263ページ』 をご確認ください。
有効な役割	選択したユーザーまたはグループの役割をすべて表示します。 Network Video Management System Enterprise Edition を実行している場合のみ該当します。
オプション	オプションダイアログボックスを開き、グローバルなシステム設定を定義および編集することができます。 Network Video Management System Enterprise Edition を実行している場合のみ該当します。

ヘルプメニュー

ヘルプシステムと Management Client のバージョンについての情報にアクセスできます。

Management Client エlement

基本

ライセンス情報

このサイトとすべての他のサイトの両方で、同じソフトウェアライセンスファイルを共有するすべてのライセンス、SUP サブスクリプションを追跡し、ライセンスの認証方法を決定できます。異なる Network Video Management System ライセンスの基本情報については、「ライセンスについて 『19ページ』」を参照してください。

ライセンス付与先

ここでは、インストール前に同意したエンドユーザー使用許諾契約へのリンクが表示されます。

インストールされている製品

Network Video Management System VMS 用のすべてのインストールされた基本ライセンスと、同じソフトウェアライセンスファイルを共有するアドオン製品に関する次の情報が一覧表示されます。

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

ライセンス概要 - すべてのサイト

認証されたハードウェアデバイスライセンスまたはソフトウェアライセンスファイルの他のライセンス数と、システムで使用可能なライセンスの合計数を一覧表示します。追加ライセンスを購入せずにシステムを拡張できるかどうかを簡単に確認できます。

アドオン製品のライセンスがある場合は、**【サイトナビゲーションペイン】**のアドオン製品固有のノードの下に、これらに関する追加詳細情報が表示されます。

ライセンス詳細 - 現在のサイト

【認証】列には、認証されたハードウェアデバイスライセンスまたはこのサイトの他のライセンスの数が一覧表示されます。

また、アクティベーションない使用されたデバイスの変更 『58ページ』の"アクティベーションなしのデバイスの変更"参照』数を確認できます。**【アクティベーションなしの変更】**列では、1年間で使用可能な数も確認できません。

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

猶予期間が終了する前にライセンスを認証し忘れた場合は、動画がシステムに送信されなくなります。これらのライセンスは[終了した猶予期間]列に表示されます。「猶予期限が切れた後にライセンスを認証する『60ページ』」も参照してください。

使用可能なライセンス数よりも使用済みライセンス数の方が多く場合は、[ライセンスなし]列に一覧表示され、システムで使用できません。詳細は、追加ライセンスの入手『60ページ』の"追加ライセンスの取得"参照』を参照してください。

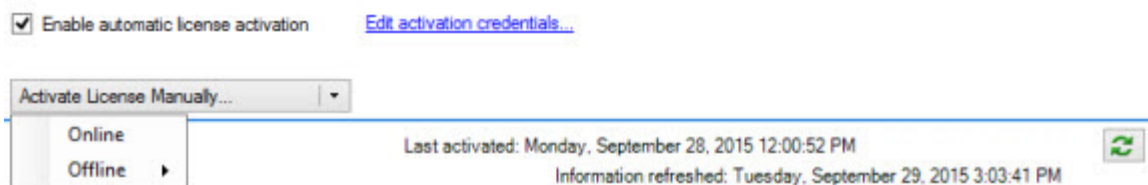
猶予期間中または猶予期間が期限切れのライセンスがある場合、またはライセンスがない場合は、Management Client にログインするたびに、通知メッセージがポップアップ表示されます。

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

ライセンス認証の機能

3つのテーブルの下には、次の項目があります。

- 手動認証するためのドロップダウンリスト。詳細については、「ライセンスを認証 (オフライン) 『59ページ』の"ライセンスをオフラインで認証"参照』) を参照してください。
- ページの右下端には、最後にライセンスを認証(自動または手動)した日時とページの情報が更新された日時が表示されます。日付スタンプは、ローカルコンピュータではなく、サーバーから取得されます。



アクティベーションなしのデバイスの変更

[基本] > [ライセンス情報]ページの[アクティベーションなしの変更]には、ハードウェアデバイスライセンスを認証せずに交換または追加できるハードウェアデバイス数と、前回の認証以降に行った変更数が示されます。アクティベーションなしのデバイスの変更内に追加されたハードウェアデバイスは、完全に認証されたハードウェアデバイスライセンスとして実行されます。

アクティベーションなしのデバイスの変更数の計算方法

アクティベーションなしのデバイスの変更は、3つの変数に基づいて計算されます。Sony ソフトウェアの複数のインストールがある場合は、変数はそれぞれに個別に適用されます。変数は以下のとおりです。

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

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

Sony は 3つのすべての変数の値を定義し、値は通知なく変更される場合があります。変数の値は製品によって異なります。

C% = 15%、Cmin = 10、Cmax =100 に基づく例

お客様が 100 個のハードウェアデバイスライセンスを購入します。100 台のカメラをシステムに追加します。ライセンスを認証すると、アクティベーションなしのデバイスの変更が 15 になります。

お客様が 100 個のハードウェアデバイスライセンスを購入します。100 台のカメラをシステムに追加し、ライセンスを認証します。アクティベーションなしのデバイスの変更は現在 15 です。お客様は、システムからハードウェアデバイスを削除することにしました。現在 99 台のデバイスが認証され、アクティベーションなしのデバイスの変更数は 14 まで減りました。

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

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

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

ライセンスをオフラインで認証

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

1. **【ライセンス情報】**ノードで、**【ライセンスの手動認証】** -> **【オフライン】** -> **【認証するライセンスをエクスポート】**を選択し、追加したハードウェアデバイスに関する情報とともにライセンスリクエストファイル(.lrq)をエクスポートします。
2. ライセンスリクエストファイル(.lrq)には、自動的に SLC と同じ名前が付けられます。複数のサイトがある場合は、必ず名前を一意にし、どのファイルがどのサイトに属しているのかを簡単に識別できるようにしてください。
3. インターネットに接続しているコンピュータにライセンスリクエストファイルをコピーし、Web サイトにログインして、認証済みのソフトウェアライセンスファイル(.lic)を取得します。ライセンスガイドを参照してくださいに Web サイト <http://www.sony.net/CameraSystem> 。
4. ライセンスリクエストファイルと同じ名前の .lic ファイルを Management Client がインストールされたコンピュータにコピーします。
5. Management Client の**【ライセンス情報】**ページで、**【ライセンスをオフラインで認証】** > **【認証されたライセンスのインポート】**を選択し、認証済みのソフトウェアライセンスファイルを選択してインポートし、ライセンスを認証します。
6. **終了**をクリックして、認証プロセスを終了します。

猶予期限が切れた後にライセンスを認証する

猶予期間内に期限切れのライセンスを認証しない場合、デバイスが使用できなくなり、監視システムで使用できません。

- 設定、追加されたカメラ、およびその他の設定は Management Client から削除されません。
- ライセンスはシステム設定から削除されません。

追加ライセンスの取得

現在のライセンス数を超えて、その他のハードウェアデバイス、またはドアを追加する場合または既に追加した場合、追加ライセンスを購入し、デバイスがデータをシステムに送信できるようにする必要があります。

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

既存の監視システムバージョンの新しいライセンス：

- ライセンスを手動で認証し、新しいライセンスを入手します。詳細については、ライセンスを認証 (オフライン) 『59ページ の"ライセンスをオフラインで認証"参照』を参照してください。

新しいライセンスとアップグレードされた監視システムバージョン：

- 更新されたソフトウェアライセンスファイル(.lic) 『19ページ の"ライセンスについて"参照』、新しいライセンス、新しいバージョンを受け取ります。新しいバージョンのインストール中には、新しいソフトウェアライセンスファイルを使用する必要があります。詳細については、「アップグレードの前提条件 『47ページ』」を参照してください。

ライセンスとハードウェアデバイスの交換

システムでライセンス付与されているカメラなど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して、新しいハードウェアデバイスを認証してライセンス付与することができます。

レコーディングサーバーからハードウェアデバイスを取り外すと、ハードウェアデバイスライセンスに空きができます。

あるカメラを同等のカメラ (メーカー、ブランド、およびモデル)と交換し、新しいカメラに同じ IP アドレスを付与すると、すべてのカメラのデータベースへの完全なアクセスを維持できます。この場合、Management Client での設定は一切変更せずに、ネットワークケーブルを古いカメラから新しいカメラへ移動させます。

別のモデルのハードウェアデバイスと交換する場合は、**ハードウェアの交換**ウィザードを使用して、すべてのカメラ、マイク、入力、出力、および設定などの関連データベースをマップする必要があります (ハードウェアの交換 『254ページ』を参照してください)。

サイト情報

大規模な構成の場合など、各サイトを容易に識別できるように、サイトに詳細情報を追加できます。サイト名以外に、次の情報を追加できます。

- アドレス/場所
- 管理者
- 詳細情報

サイト情報の更新

サイト情報を更新するには：

1. **編集**を選択します。
2. タグを選択します。
3. 値フィールドに情報を入力します。
4. **OK**をクリックします。

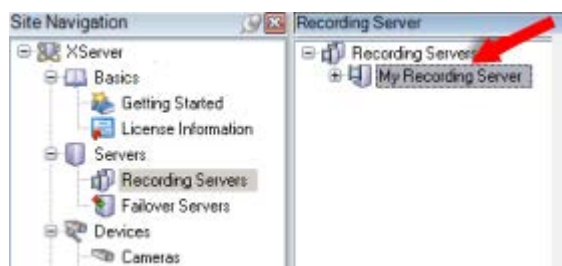
サーバーとハードウェア

レコーディング サーバー

レコーディングサーバーについて

レコーディングサーバーは、ビデオフィードの録画や、カメラおよびその他のデバイスとの通信に使用します。一般的に、監視システムには複数のレコーディングサーバーがあります。

レコーディングサーバーは、レコーディングサーバーソフトウェアがインストールされ、管理サーバーと通信するように構成されているコンピュータです。**【サーバー】**フォルダを展開し、**【レコーディングサーバー】**を選択すると、**【概要】**ペインにレコーディングサーバーが表示されます。



概要ペインに一覧されるレコーディングサーバー

このバージョンの管理サーバーよりも前のレコーディングサーバーのバージョンとの後方互換性は制限されています。旧バージョンのレコーディングサーバーの録画にアクセスすることはできますが、それらの設定を変更するには、このバージョンの管理サーバーと一致していることを確認してください。Sony は、システムのすべてのレコーディングサーバーを管理サーバーと同じバージョンにすることを勧めます。

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

- レコーディングサーバーの認証 『62ページ』
- ハードウェアの追加 『79ページ』
- ハードウェアの移動 『82ページ』
- すべてのハードウェアの削除 『79ページ』の"レコーディングサーバーでのすべてのハードウェアの削除"参照』
- レコーディングサーバーの削除 『79ページ』

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

レコーディングサーバーの認証

初めてシステムを使用するか、システムに新しいレコーディングサーバーが追加された場合、新しいレコーディングサーバーを承認する必要があります。

レコーディングサーバーを認証すると、管理サーバーに接続するように設定できます。

1. **概要** ペインで、必要なレコーディングサーバーを右クリックします。
2. **レコーディングサーバーの認証** を選択します。



3. しばらくすると、レコーディングサーバーが認証され、タブを使用して設定を続けることができます。ハードウェアを追加 『79ページ の"ハードウェアの追加"参照 』することもできます。

レコーディングサーバーの基本設定の変更/確認

Management Client で、インストールしたすべてのレコーディングサーバーが表示されない場合、通常は、インストール中に設定パラメータを正しく設定しなかったことが原因です（管理サーバーの IP アドレスやホスト名など）。

管理サーバーのパラメータを指定するには、レコーディングサーバーを再インストールする必要はありません。次の方法で基本設定を変更/確認できます。

1. レコーディングサーバーを実行しているコンピュータで、通知エリアにある**レコーディングサーバー**アイコンを右クリックします。
2. **Recording Server サービスの停止** を選択します。
3. **レコーディングサーバー**アイコンを再び右クリックし、**設定の変更** を選択します。
レコーディングサーバーの**設定**ウィンドウが表示されます。
4. 以下の設定を確認/変更します。

- **管理サーバーのホスト名/IP アドレス**：レコーディングサーバーを接続する必要がある、管理サーバーの IP アドレスまたはホスト名を指定します。
- **Management Server のポート**：管理サーバーと通信する際に使用するポート番号を指定します。デフォルトポートは **9993** です。必要に応じてこのポートを変更できますが、ポート番号は必ず管理サーバーで設定したポート番号と一致している必要があります。






5. **OK** をクリックします。

6. Recording Server サービスを再度起動するには、**レコーディングサーバーアイコン**を右クリックし、**Recording Server サービスの起動**を選択します。

重要: Recording Server サービスを停止すると、レコーディングサーバーの基本設定を確認/変更している間は、ビデオ録画やビデオのライブ再生ができません。

レコーディングサーバーステータスアイコン

次のアイコンは、個別のレコーディングサーバーの状態を示すために、Management Client で使用されます。

アイコン	詳細
	レコーディングサーバーは実行中です
	レコーディングサーバーは通信中です
	<p>Recording Server は注意が必要です：このアイコンは、通常は、Recording Server サービスが停止している場合に表示されます。</p> <ol style="list-style-type: none"> 1) 通知エリアのレコーディングサーバーアイコンを右クリックします。 2) Recording Server サービスを開始/停止し、レコーディングサーバーステータスメッセージを表示します。
	<p>レコーディングサーバーが承認されている必要があります：レコーディングサーバーを初めてロードしたときに表示されます。初めてレコーディングサーバーを使用する時は、必ず承認する必要があります。</p> <ol style="list-style-type: none"> 1) 必要なレコーディングサーバーアイコンを右クリックします。 2) レコーディングサーバーの許可を選択します。しばらくすると、レコーディングサーバーが承認され、さらに設定できるようになります。
	<p>動作中のデータベース修復：電源障害の場合など、データベースが破損し、レコーディングサーバーが修復している時に表示されます。データベースが大きい場合は、修復に時間がかかります。</p> <p>データベースの破損を避けるための有益な情報は、記録データベースを破損から守る 『50ページ』を参照してください。</p> <p>重要：起動時のデータベースの修復中は、レコーディングサーバーに接続されているカメラからビデオを録画することはできません。ライブ表示のみが可能です。</p> <p>通常動作時のデータベースの修復は、録画に影響しません。</p>

情報タブ（レコーディングサーバー）

情報タブで、選択したレコーディングサーバーの名前や説明を確認または編集することができます。



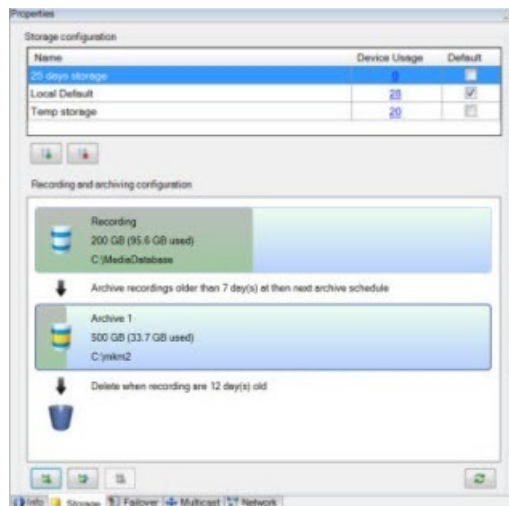
レコーディングサーバーに関する情報を表示している情報タブ

情報タブのプロパティ

名前	詳細
名前	レコーディングサーバーがシステムおよびクライアントで一覧表示されている場合に使用します。名前は一意である必要はありません。 レコーディングサーバーの名前を変更すると、名前は Management Client で一括変更されます。
詳細	説明は、システム内の複数のリストに表示されます。説明は必須ではありません。
ホスト名	レコーディングサーバーのホスト名を表示します。
Web サーバーの URL	レコーディングサーバーの Web サーバーの URL を表示します。PTZ カメラ制御コマンドの処理や、Network Video Management System Smart Client からの参照およびライブリクエストの処理などには、Web サーバーを使用します。URL には、Web サーバー通信（通常はポート 7563）で使用されたポート番号が含まれます。
時間ゾーン	レコーディングサーバーがある時間帯を表示します。

ストレージタブ（レコーディングサーバー）

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



ストレージとアーカイブについて

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

記録データベースの容量が満杯にならないように、追加のストレージを作成『67ページ の"新しいレコーディングストレージの追加"参照』できます。各ストレージ内にアーカイブを作成『67ページ の"ストレージでのアーカイブの作成"参照』し、アーカイブ処理を起動してデータを保存することもできます。

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

ストレージとアーカイブは、レコーディングサーバーごとに設定します。

アーカイブされた記録をローカルまたはアクセス可能なネットワークドライブに保存する限り、**Network Video Management System Smart Client** を使用して表示できます。この方法では、カメラの標準データベースに保存された記録も表示できます。

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

重要： Sony は、レコーディングサーバーのデータベースには専用のハードディスクドライブを使用し、ディスクのパフォーマンス低下を防止することをお勧めします。ハードディスクをフォーマットする際は、**アロケーションユニットサイズ**の設定を 4 KB から 64 KB に変更することが重要です。この変更によって、ハードディスクの記録パフォーマンスが大幅に改善できます。単位サイズの割り当てとヘルプについては、Microsoft 社の Web サイト <http://support.microsoft.com/kb/140365/en-us> をご覧ください。

重要： 空き容量が 5GB 未満になった場合、データベースで最も古いデータは必ず自動アーカイブされます（または、次のアーカイブが定義されていない場合は削除されます）。空き容量が 1GB 未満になった場合は、データは削除されます。データベースには、必ず 250MB の空き容量が必要です。データが十分速やかに削除されていないため、この制限に達した場合、十分な空き容量が確保されるまで、それ以上データベースにはデータが書き込まれません。このため、データベースの実際の最大サイズは、指定したギガバイト数より 5GB 少なくなります。

デバイスをストレージに接続する

レコーディングサーバーに対してストレージおよびアーカイブを設定すると、個別のカメラまたはカメラのグループに対してストレージおよびアーカイブを有効にできます。この操作は、デバイスごと、またはデバイスグループに対して行えます。個別のデバイスまたはデバイスのグループをストレージに接続する『68ページ』を参照してください。

効果的なアーカイブ

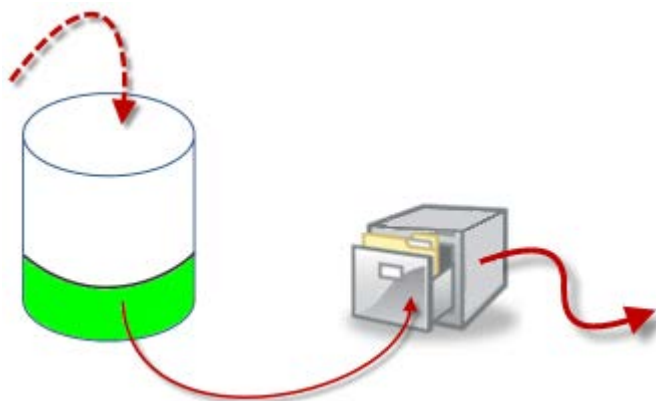
カメラまたはカメラのグループに対してアーカイブが有効であれば、カメラのデータベースの内容は定義した間隔で、自動的にアーカイブへ移動します。

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

アーカイブを効率的な方法で設定することで、必要な場合に、データベースのストレージの使用で無駄を省いて調整することが可能になります。多くの場合、アーカイブされた記録がなるべくディスク容量を必要としないようにすることが望まれます。特に、長期的な観点では、画像品質を少し下げただけでも意味があります。レコーディングサーバーの**ストレージ**タブで、次のような相互依存している設定を調整することで効果的に無駄を省いて、調整することが可能になります。

- 記録データベースの保持
- 記録データベースのサイズ
- アーカイブの保持
- アーカイブのサイズ
- アーカイブスケジュール
- フレーム数/秒(FPS)。

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



記録がデータベースからアーカイブへ、さらに削除へと移動

シリンダーにおける空きエリアによって例証される、記録データベースの保持期間とサイズの設定で、古い記録をアーカイブするまでの期間を定義します。例の図では、アーカイブするのに十分な期間が経過すると、記録がアーカイブされます。

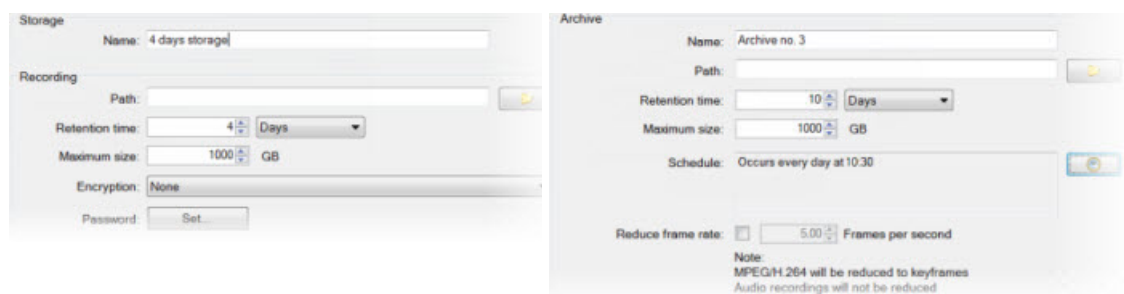
アーカイブの保持期間とサイズ設定は、記録がアーカイブにある期間を定義します。指定した期間、またはアーカイブが指定したサイズ上限に達するまで、記録がアーカイブに保存されます。これらの設定に該当すると、システムはアーカイブにある古い記録を上書きし始めます。

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

FPSによって、データベースにおけるデータのサイズが決まります。

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


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



ルールとイベントを使用してアーカイブをコントロールすることもできます。

新しいレコーディングストレージの追加


Recording という名前の定義済み記録データベースのストレージを、常に 1 つ作成します。この名前は変更できません。記録データベースとは別に、ストレージには多数のアーカイブを保存できます。

1. 選択したレコーディングサーバーにさらにストレージを追加する場合は、**ストレージ設定**リストの下にある  ボタンをクリックします。これにより**ストレージおよび録画設定**ダイアログボックスが開きます。
2. 関連する設定 『71ページ の"ストレージおよび録画設定プロパティ"参照 』を指定します。
3. **OK** をクリックします。

必要であれば、ここで新しいストレージにアーカイブを作成することもできます。ストレージでのアーカイブの作成 『67ページ 』を参照してください。

ストレージでのアーカイブの作成

ストレージを作成した時点では、デフォルトのアーカイブはありません。

1. アーカイブを作成するには、**レコーディングおよびアーカイブの設定**リストで必要なストレージを選択します。
2. **レコーディングおよびアーカイブの設定**リストの下にある  ボタンをクリックします。

3. **アーカイブ設定**ダイアログボックスで、必要な設定を指定します（アーカイブ設定のプロパティ 『72 ページ』を参照してください）。
4. **OK** をクリックします。


個別のデバイスまたはデバイスのグループをストレージに接続する

レコーディングサーバーに対してストレージエリアを設定した後で、個別のデバイス（カメラ、マイク、スピーカー）またはデバイスのグループに対して有効にすることができます。また、個別のデバイスまたはグループに対して、どのレコーディングサーバーのストレージエリアを使用するかを選択することも可能です。

1. **デバイス**を展開し、必要に応じて**カメラ**、**マイク**または**スピーカー**のいずれかを選択します。
2. デバイスまたはデバイスグループを選択します。
3. **記録**タブを選択します。
4. **ストレージ**エリアで、**選択**を選択します。
5. 表示されるダイアログボックスで、デバイスの記録を保存するデータベースを選択し、**OK** をクリックします。
6. ツールバーで**保存**をクリックします。

レコーディングサーバーのストレージタブで、ストレージエリアのデバイス使用数をクリックすると、表示されるメッセージレポートでデバイスを確認できます。

選択したストレージまたはアーカイブ設定の編集

1. **レコーディングおよびアーカイブの設定**リストで、ストレージを編集するには、記録データベースを選択します。アーカイブを編集するには、アーカイブデータベースを選択します。
2. **レコーディングおよびアーカイブの設定**リストの下にある**レコーディングストレージの編集**ボタン  をクリックします。
3. 記録データベースの編集またはアーカイブの編集を行います。

データベースの最大サイズを変更する場合、新しい上限を超える記録は自動アーカイブされます。記録は次のアーカイブに自動アーカイブされるか、アーカイブ設定によっては削除されます。

アーカイブされた記録をバックアップする

多くの組織では、テープドライブや同等のものを使用して、記録をバックアップすることを考えています。これをどのように行うかは、組織で使用しているバックアップメディアによって異なります。ただし、以下の点を覚えておく必要があります：

カメラのデータベースではなくアーカイブをバックアップする

個別のカメラのデータベースではなく、必ずアーカイブの内容に基づいてバックアップを作成します。個別のカメラのデータベースに基づいてバックアップを作成すると、共有違反やその他の誤動作の原因となることがあります。

バックアップをスケジュールする際は、バックアップジョブのアーカイブ時間が決して重複しないように注意してください。ストレージタブを使用すると、各レコーディングサーバーのストレージエリアの、各レコーディングサーバーのアーカイブスケジュールを表示することができます。

アーカイブの構造を知ることでバックアップを効率化する

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

全システムの標準的な使用中に、Network Video Management System Smart Client を使ってすべての記録を参照しているシステムユーザーにとって、サブディレクトリ構造はまったく認識されません。これは、アーカイブ済み記録と未アーカイブ記録の両方に当てはまります。アーカイブされている記録をバックアップする場合には、サブディレクトリ構造を知ることが非常に重要です。アーカイブの構造について『69ページ』と設定のバックアップと復元『246ページ』の"システム設定のバックアップおよび復元"参照』を参照してください。

アーカイブの構造について

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

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

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

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

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

サブディレクトリの名前は、記録がエッジカメラか SMTP のいずれによる記録であるかを示すデバイスの名前に続いて、サブディレクトリに含まれている最新のデータベースレコードの日付と時間を加えた名前になります。

命名構成：

...[ストレージのパス]¥[ストレージ名]¥[デバイス名] - 最新の記録の日付と時間を追加]¥

エッジカメラからの場合：

...[ストレージのパス]¥[ストレージ名]¥[デバイス名] (Edge) - 最新の記録の日付と時間を追加]¥

SMTP からの場合：

...[ストレージのパス]¥[ストレージ名]¥[デバイス名] (SMTP) - 最新の記録の日付と時間を追加]¥

実際の例：

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

サブディレクトリ：

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

- **メディア**：このフォルダには、ビデオまたは音声(両方ではない)の実際のメディアが含まれます。
- **モーションレベル**：このフォルダには、当社のモーション検知アルゴリズムを使用して、ビデオデータから生成したモーションレベルのグリッドが含まれています。このデータで、Network Video Management System Smart Client のスマート検索機能が高速で検索を行うことができます。

- **モーション**：このフォルダに、システムはモーションのシーケンスを保存します。モーションのシーケンスは、ビデオデータ中でモーションが検知されたタイムスライスです。たとえば、この情報は Network Video Management System Smart Client のタイムラインで使用されます。
- **レコーディング**：このフォルダに、システムはレコーディングのシーケンスを保存します。レコーディングのシーケンスは、メディアデータで一貫しているレコーディングのタイムスライスです。たとえば、この情報は Network Video Management System Smart Client でタイムラインを描画するために使用されます。

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

バックアップの例：

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

```
...F:¥OurArchive¥
```


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

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

ストレージでのアーカイブの削除

1. **レコーディングおよびアーカイブの設定**リストで、アーカイブを選択します。

リストで最後にあるアーカイブのみが削除できます。アーカイブを空にする必要はありません。

2. **レコーディングおよびアーカイブの設定**リストの下にある  ボタンをクリックします。
3. **はい**をクリックします。

ストレージの削除

ライブ録画のレコーディングストレージとしてデバイスで使用される既定のストレージを削除することはできません。

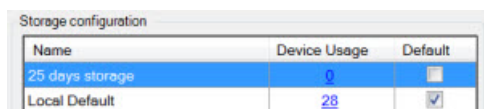
つまり、ストレージを削除する前には、デバイスとアーカイブされていない録画を別のストレージに移動 『82ページ』の「ハードウェアの移動」参照』する必要があります。

1. このストレージを使用するデバイスを一覧表示するには、デバイス使用数をクリックします。

別のレコーディングサーバーに移動されたデバイスのデータがストレージにある場合は、警告が表示されます。リンクをクリックすると、デバイスの一覧が表示されます。

2. 「アーカイブされていない記録のあるストレージから別のストレージへ移動する 『71ページ』」の手順を参照してください。
3. すべてのデバイスを移動し終わるまで続行します。

- 削除するストレージを選択します。



- ストレージ設定リストの下にある  ボタンをクリックします。

- はいをクリックします。

アーカイブされていない記録をあるストレージから別のストレージへ移動する

ある記録データベースから別の記録データベースへのコンテンツの移動は、デバイスの記録タブで行います。

- デバイスタイプを選択します。概要ペインで、デバイスを選択します。
- 録画タブをクリックします。ストレージエリアの上部で、選択をクリックします。
- ストレージの選択ダイアログボックスで、データベースを選択します。
- [OK]をクリックします。
- [記録アクション]ダイアログボックスで、既存のアーカイブされていない録画を削除して新しいストレージに移動するか、削除するかを選択します。
- [OK]をクリックします。

ストレージおよび録画設定プロパティ

ストレージおよび録画設定ダイアログボックスで、次の項目を指定します。

名前	詳細
名前	必要に応じて、ストレージ名を変更します。名前は一意でなければなりません。
パス	このストレージで記録を保存するディレクトリへのパスを指定します。ストレージは、必ずしもレコーディングサーバーのコンピュータに存在する必要はありません。 ディレクトリが存在しない場合は作成できます。ネットワークドライブは、必ず UNC (汎用名前付け規則) のフォーマットを使用して指定する必要があります。例：¥¥server¥volume¥directory¥。
保持期間	アーカイブ設定に応じて、削除または次のアーカイブに移動するまでに、記録がアーカイブに格納される期間を指定します。 保持期間は、前のアーカイブまたはデフォルトの記録データベースの保持期間より必ず長くなるようにしてください。アーカイブに対して指定される保持日数には、プロセスで以前に指定されたすべての保持期間が含まれるためです。

名前	詳細
最大サイズ	<p>記録データベースに保存する記録データの最大ギガバイト数を選択します。</p> <p>指定されたギガバイト数を超える記録データは、指定された場合、自動的にリストの最初のアーカイブに移動されるか、削除されます。</p> <p>重要：空き容量が 5GB 未満になった場合、データベースで最も古いデータは必ず自動アーカイブされます（または、次のアーカイブが定義されていない場合は削除されます）。空き容量が 1GB 未満になった場合は、データは削除されます。データベースには、必ず 250MB の空き容量が必要です。この制限に達した場合（データが十分速やかに削除されていない場合）、十分な空き容量が確保されるまで、それ以上データベースにはデータが書き込まれません。このため、データベースの実際の最大サイズは、指定したギガバイト数より 5GB 少なくなります。</p>
パスワード	パスワードを入力します。

アーカイブ設定のプロパティ

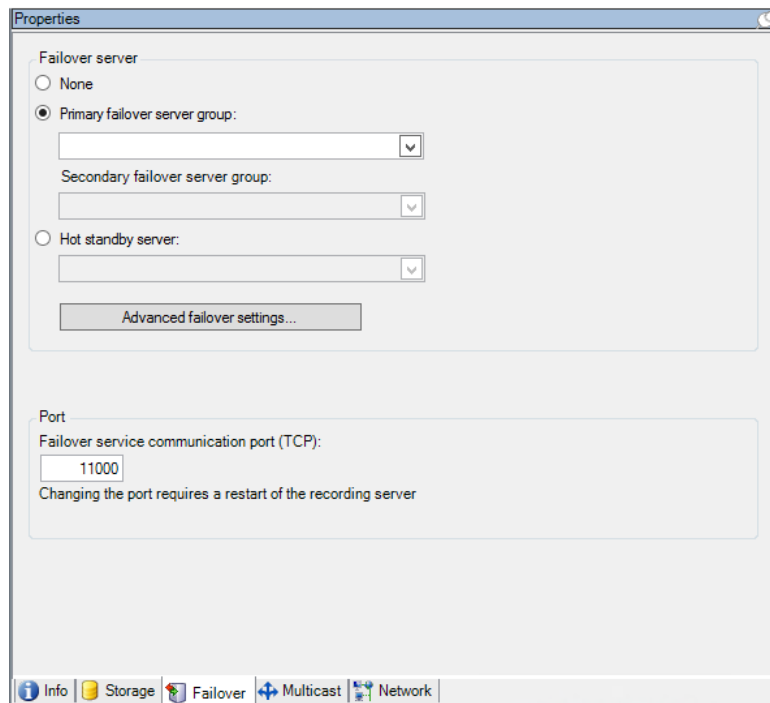
【アーカイブ設定】ダイアログボックスで、次の項目を指定します。

名前	説明
名前	必要に応じて、ストレージ名を変更します。名前は一意でなければなりません。
パス	<p>このストレージで録画を保存するディレクトリへのパスを指定します。ストレージは、必ずしも録画サーバーのコンピュータに存在する必要はありません。</p> <p>ディレクトリが存在しない場合は作成できます。ネットワークドライブは、必ず UNC(汎用名前付け規則)のフォーマットを使用して指定する必要があります。例: ¥¥server¥volume¥directory¥。</p>
保持期間	<p>アーカイブ設定に応じて、削除または次のアーカイブに移動するまでに、録画がアーカイブに格納される期間を指定します。</p> <p>保持期間は、前のアーカイブまたはデフォルトの録画データベースの保持期間より必ず長くなるようにしてください。アーカイブに対して指定される保持日数には、プロセスで以前に指定されたすべての保持期間が含まれるためです。</p>

名前	説明
最大サイズ	<p>録画データベースに保存する録画データの最大ギガバイト数を選択します。</p> <p>指定されたギガバイト数を超える記録データは、指定された場合、自動的にリストの最初のアーカイブに移動されるか、削除されます。</p> <p>重要:空き容量が 5GB 未満になった場合、データベースで最も古いデータは必ず自動アーカイブされます(または、次のアーカイブが定義されていない場合は削除されます)。空き容量が 1GB 未満になった場合は、データは削除されます。データベースには、必ず 250MB の空き容量が必要です。この制限に達した場合(データが十分速やかに削除されていない場合)、十分な空き容量が確保されるまで、それ以上データベースにはデータが書き込まれません。このため、データベースの実際の最大サイズは、指定したギガバイト数より 5GB 少なくなります。</p>
スケジュール	<p>アーカイブプロセスが開始する間隔を示すアーカイブスケジュールを指定します。アーカイブは非常に高い頻度(原則として、1年にわたって毎時にアーカイブ)、あるいは非常に低い頻度(たとえば、36か月ごとに一度、月初の月曜日にアーカイブ)で行うことができます。</p>
フレームレートの低減	<p>【フレームレートの低減】チェックボックスを選択し、アーカイブの際に秒当たりのフレーム数(FPS)を低減できるように、FPSを設定します。</p> <p>選択した数のFPSでフレームレートを低減すると、アーカイブで記録が占める容量を低減できます。ただし、アーカイブ品質も低下します。MPEG-4/H.264/H.265は、最小限として自動的にキーフレームに低減されます。</p> <p>0.1 = 1 フレーム/10 秒</p>

フェールオーバータブ（レコーディングサーバー）

フェールオーバーレコーディングサーバーを使用する場合、**フェールオーバー**タブを使用して、フェールオーバーサーバーをレコーディングサーバーに割り当てます。フェールオーバータブのプロパティ 『75ページ』を参照してください。



フェールオーバーレコーディングサーバー、インストールと設定、フェールオーバーグループ、およびその設定の詳細については、フェールオーバーレコーディングサーバーについて（通常およびホットスタンバイ）を参照してください。

フェールオーバーレコーディングサーバーの割り当て

レコーディングサーバーの**フェールオーバー**タブでは、3種類のフェールオーバー設定の中から選択できます。

- a フェールオーバー設定なし
- b プライマリ/セカンダリフェールオーバー設定
- c ホットスタンバイ設定

bおよび**c**を選択する場合、特定のサーバーまたはグループを選択する必要があります。**b**では、セカンダリフェールオーバーグループも選択できます。レコーディングサーバーが使用できなくなった場合、プライマリフェールオーバーグループのフェールオーバーレコーディングサーバーに切り替わります。セカンダリフェールオーバーグループも選択している場合、プライマリフェールオーバーグループのフェールオーバーレコーディングサーバーがすべてビジーである場合には、セカンダリグループのフェールオーバーレコーディングサーバーに切り替わります。このようにして、フェールオーバーソリューションが機能しないリスクは、プライマリのすべてのフェールオーバーレコーディングサーバーだけでなくセカンダリフェールオーバーグループもビジーである場合だけになります。

1. **サイトナビゲーション**ペインで、**サーバー** > **レコーディングサーバー**を選択します。レコーディングサーバーのリストが表示されます。

2. **概要**ペインで、必要なレコーディングサーバーを選択し、**フェールオーバー**タブに移動します。
3. フェールオーバー設定タイプを選択するには、**無し**、**プライマリフェールオーバーサーバーグループ/セカンダリフェールオーバーサーバーグループ**、**ホットスタンバイサーバー**のいずれかを選択します。同じフェールオーバーグループをプライマリとセカンダリフェールオーバーグループとして選択したり、既にフェールオーバーグループに含まれている標準のフェールオーバーサーバーをホットスタンバイサーバーとして選択することはできません。
4. 次に、**詳細フェールオーバー設定**をクリックします。これで、**フェールオーバー詳細設定**ウィンドウが開き、選択したレコーディングサーバーに接続するすべてのデバイスのリストが表示されます。**無し**を選択した場合でも、フェールオーバー詳細設定を使用できます。選択項目はすべて保持され、後からフェールオーバー設定で使用できます。
5. フェールオーバーサポートのレベルを指定するには、リストの各デバイスで**フルサポート**、**ライブ専用**、**無効**のいずれかを選択します。**OK** をクリックします。
6. 必要に応じて、**フェールオーバーサービス通信ポート (TCP)** フィールドでポート番号を編集します。

フェールオーバータブのプロパティ

名前	説明
無し	フェールオーバーのない設定を選択します。
プライマリフェールオーバーサーバーグループ/セカンダリフェールオーバーサーバーグループ	1つのプライマリフェールオーバーサーバーグループと任意で1つのセカンダリフェールオーバーサーバーグループから成る通常のフェールオーバー設定を選択します。
ホットスタンバイサーバー	ホットスタンバイサーバーとして1つの専用レコーディングサーバーを用意し、ホットスタンバイ設定を選択します。
フェールオーバー詳細設定	<p>フェールオーバー詳細設定ウィンドウを開きます。</p> <ul style="list-style-type: none"> ● フルサポート: 選択すると、デバイスのフルフェールオーバーサポートが得られます。 ● ライブ専用: 選択すると、デバイスのライブフェールオーバーサポートが得られます。 ● 無効: 選択すると、デバイスのフェールオーバーサポートを無効にします。
フェールオーバーサービス通信ポート (TCP)	デフォルトのポート番号は 11000 です。このポートがレコーディングサーバーとフェールオーバーレコーディングサーバー間での通信で使用されます。ポートを変更した場合、レコーディングサーバーが実行中でなければならず、また、その間管理サーバーに接続されていなければなりません。

マルチキャストタブ (レコーディングサーバー)

システムでは、レコーディングサーバーからのライブストリームのマルチキャストをサポートしています。多数の Network Video Management System Smart Client ユーザーが同じカメラからのライブビデオを再生しようとする場合に、マルチキャストによってシステムリソースの消費量を大幅に低減できます。マルチキャストは、複数のクライアントが同じカメラからのライブビデオを頻繁に要求し、Matrix 機能を使用する場合に特に便利です。

マルチキャストは、記録されたビデオ/音声ではなく、ライブストリームでのみ可能です。

レコーディングサーバーに複数のネットワークインターフェースカードがある場合、マルチキャストはその中の 1 つのカードでだけ可能です。どのネットワークインターフェースカードを使用するか、Management Client によって指定できます。

マルチキャストを正しく実装するには、ネットワーク装置がマルチキャストのデータパケットを必要な受信者のグループだけに配信されるように設定されていることも必要です。そうでないと、マルチキャストはブロードキャストと変わらなくなり、ネットワーク通信速度が大幅に低下します。

マルチキャストについて

通常のネットワーク通信で、各データパケットは単一の送信者から単一の受信者に送信され、ユニキャストと呼ばれます。一方、マルチキャストでは、単一のデータパケット（サーバーから）をグループ内の複数の受信者（クライアント）に送信できます。したがって、マルチキャストは帯域幅を節約できます。

- **ユニキャスト**を使用する場合、発信元は必ずそれぞれの受信者に 1 つのデータストリームを転送しなければなりません。
- **マルチキャスト**を使用する場合は、それぞれのネットワークセグメントで単一のデータストリームしか必要ではありません。

ここで説明しているマルチキャストは、カメラからサーバーへのビデオのストリーミングでは**ありません**。サーバーからクライアントへのストリーミングになります。

マルチキャストでは、IP アドレス範囲、各カメラにマルチキャストを有効化/無効化できる能力、最大許容データパケットサイズ(MTU)を定義する機能、データパケットを転送するための最大ルーター数(TTL)などのオプションを基に定義された受信者のグループを使用します。

マルチキャストを、関連のないデータでもネットワークに接続している全員にデータを送信する、**ブロードキャスト**と混合しないよう注意する必要があります。

名前	詳細
ユニキャスト	単一のソースから単一の受信者へデータを送信します。
マルチキャスト	単一のソースから明確に定義されたグループ内の複数の受信者へデータを送信します。
ブロードキャスト	単一のソースからネットワーク上の全員へデータを送信します。このため、ブロードキャストによって、ネットワーク通信速度が大幅に低下する可能性があります。

マルチキャストの有効化

マルチキャストを使用するには、ネットワークのインフラが IP マルチキャスト標準 IGMP（インターネットグループ管理プロトコル）をサポートしている必要があります。

- **マルチキャスト**タブで、**マルチキャスト**チェックボックスを選択します。

マルチキャスト用の IP アドレス範囲の全体が既に 1 つまたは複数のレコーディングサーバーによって使用されている場合は、まずマルチキャスト用の IP アドレスを空けないと、それ以上のレコーディングサーバーでマルチキャストを有効にすることはできません。

IP アドレス範囲の割り当て

選択したレコーディングサーバーからのマルチキャストストリームにアドレスを割り当てる範囲を指定します。クライアントは、対象となるレコーディングサーバーからのマルチキャストビデオを再生する時に、これらのアドレスに接続します。

マルチキャストカメラフィールドのそれぞれについて、IP アドレスとポートの組み合わせは一意でなければなりません。(IPv4 の例 : 232.0.1.0:6000)。1 つの IP アドレスと複数のポートを、あるいは複数の IP アドレスと少数のポートを使用することができます。デフォルトでは、システムは単一の IP アドレスと 1000 のポートの範囲を使用するよう推奨しますが、必要であれば変更できます。

マルチキャストの IP アドレスは、IANA によるダイナミックホスト割り当てで定義された範囲内であればなりません。IANA はグローバル IP アドレス割り当てを監視する機関です。

名前	詳細
IP アドレス	開始 フィールドで、必要な範囲の最初の IP アドレスを指定します。次に、範囲で最後の IP アドレスを 終了 フィールドで指定します。
ポート	開始 フィールドで、必要な範囲で最初のポート番号を指定します。次に、範囲で最後のポート番号を 終了 フィールドで指定します。
すべてのマルチキャストストリームの送信元 IP アドレス	<p>マルチキャストは 1 つのネットワークインターフェースカードでだけできるため、レコーディングサーバーに複数のネットワークインターフェースカードがあるか、複数の IP アドレスのネットワークインターフェースカードが 1 つある場合に、このフィールドを使用します。</p> <p>レコーディングサーバーのデフォルトのインターフェースを使用する場合は、フィールドの値を 0.0.0.0 (IPv4 の場合) または :: (IPv6 の場合) のままにします。他のネットワークインターフェースカードを使用する場合、または同じネットワークインターフェースカードで別の IP アドレスを使用する場合、必要なインターフェースの IP アドレスを指定します。</p> <ul style="list-style-type: none"> IPv4: 224.0.0.0 ~ 239.255.255.255。 IPv6、範囲については、IANA Web サイト http://www.iana.org を参照してください。

データグラムオプションの指定

マルチキャストで転送するデータパケット (データグラム) の設定を指定します。

名前	詳細
MTU	最大転送ユニット、許容される物理的データパケットの最大サイズです (単位はバイト)。指定された MTU より大きいメッセージは、送信する前に小さいパケットに分割されます。デフォルト値は 1500 バイトです。これは大半の Windows コンピュータやイーサネットネットワークでのデフォルトでもあります。
TTL	生存時間、廃棄または返却されるまでに、データパケットが移動できるホップの最大数です。ホップとは、2 つのネットワークデバイス (通常はルーター) の間のポイントのことです。デフォルト値は 128 です。

個々のカメラに対してマルチキャストを有効にする

必要なカメラで有効にした場合にだけ、マルチキャストは動作します。

1. レコーディングサーバーを選択して、**概要**ペインで必要なカメラを選択します。
2. クライアントタブで、**ライブマルチキャスト**チェックボックスを選択します。必要なカメラで同じ操作を繰り返します。

ネットワークタブ (レコーディングサーバー)

レコーディングサーバーのパブリック IP アドレスはネットワークタブで定義します。

パブリックアドレスを使用する理由

Network Video Management System Smart Client などのアクセス用クライアントが監視システムに接続する場合、連絡用アドレスの交換を含めて、一定量の初期データ通信がバックグラウンドで共有されます。これは自動的に行われ、ユーザーには全く認識されません。

クライアントはローカルネットワークに加えてインターネットから接続することもあります。いずれの場合にも、レコーディングサーバーからのライブビデオや録画済みビデオにクライアントがアクセスできるように、監視システムが適切なアドレスを提供する必要があります。

- クライアントがローカルで接続する場合、監視システムはローカルのアドレスおよびポート番号を返さなければなりません。
- クライアントがインターネットから接続する場合、監視システムはレコーディングサーバーのパブリックアドレス、および異なるポート番号を返さなければなりません。ここでのパブリックアドレスとは、ファイアウォールまたは NAT (ネットワークアドレス変換) ルーターのアドレスです。アドレスおよびポートは、サーバーのローカルアドレスおよびポートに転送できます。

NAT (ネットワークアドレス変換) ファイアウォールの外側から監視システムにアクセスするには、パブリックアドレスとポート転送を使用します。これによって、ファイアウォールの外側にあるクライアントは、VPN (仮想プライベートネットワーク) を使用することなく、レコーディングサーバーへ接続できます。それぞれのレコーディングサーバーを特定のポートにマップし、ファイアウォールを通じて、このポートをサーバーの内部アドレスへ転送することができます。

パブリックアドレスとポートの定義

1. パブリックアクセスを有効にするには、**パブリックアクセスを有効にする**チェックボックスを選択します。
2. レコーディングサーバーのパブリックアドレスを定義します。ファイアウォールまたは NAT ルーターのアドレスを入力し、インターネットから監視システムにアクセスするクライアントがレコーディングサーバーに接続できるようにします。
3. パブリックポート番号を指定します。ファイアウォールまたは NAT ルーターで使用するポート番号を、ローカルで使用するポート番号と異なる番号にしておくことをお勧めします。

パブリックアクセスを使用する場合、使用するファイアウォールまたは NAT ルーターを設定し、パブリックなアドレスおよびポートに送信されるリクエストが、関連するレコーディングサーバーのローカルなアドレスおよびポートに転送されるようにしてください。

ローカル IP 範囲の割り当て

監視システムがローカルネットワークから来ていると認識できるローカル IP 範囲のリストを定義します。

- ネットワークタブで、**設定**をクリックします。

レコーディングサーバーの削除

重要: レコーディングサーバーを削除すると、そのレコーディングサーバーに関連するすべてのハードウェア（カメラ、入力デバイスなど）を含めて、Management Client でそのレコーディングサーバーに対して指定したすべての設定も削除されます。

1. **概要**ペインで、削除するレコーディングサーバーを右クリックします。
2. **レコーディングサーバーの削除**を選択します。
3. 削除するには、**はい**をクリックします。
4. レコーディングサーバーと、関連するすべてのハードウェアが削除されます。

レコーディングサーバーでのすべてのハードウェアの削除

重要: ハードウェアを削除すると、ハードウェアに関連付けられたすべての録画データが完全に削除されます。

1. すべてのハードウェアを削除するレコーディングサーバーを右クリックします。
2. **すべてのハードウェアの削除**を選択します。
3. 削除を確認します。

ハードウェア

ハードウェアについて

ハードウェアは次のいずれかを表します。

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

システムへのハードウェアの追加方法については、ハードウェアの追加 『79ページ』を参照してください。

ハードウェアの追加

システムで許可された各レコーディングサーバーに対して、ハードウェアを追加するための複数のオプションがあります。

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

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

1. **ハードウェアの追加**にアクセスするには、必要なレコーディングサーバーを右クリックし、**ハードウェアの追加**を選択します。
2. ウィザードオプション（以下を参照）のいずれかを選択し、画面の手順に従います。
3. インストール後、**概要**ペインにハードウェアとデバイスが表示されます。

名前	詳細
高速（推奨）	<p>レコーディングサーバーのローカルネットワークで、新しいハードウェアがシステムにより自動的にスキャンされます。</p> <p>他のレコーディングサーバーで実行中のハードウェアを表示チェックボックスを選択すると、検出したハードウェアが他のレコーディングサーバーで実行中であるかどうかを確認できます。</p> <p>新しいハードウェアをネットワークに追加し、システムで使用するために、このオプションを選択できます。</p> <p>このオプションを使用して、セットアップでリモートシステムを追加することはできません。</p>
アドレス範囲スキャン	<p>ネットワーク上の関連するハードウェアとリモートシステムがスキャンされます。</p> <ul style="list-style-type: none"> • これは、指定されたハードウェアのユーザー名とパスワードに従って実行されます。ハードウェアで出荷時のデフォルトユーザー名とパスワードが使用される場合には必要ありません。 • ドライバー • IP 範囲(IPv4 のみ) • ポート番号(デフォルト= 80) <p>システムを拡張する場合など、ネットワークの一部だけをスキャンするときにはこのオプションを選択できます。</p>
手動	<p>各ハードウェアとリモートシステムの詳細情報を個別に指定します。追加するハードウェア数が限られており、IP アドレス、関連するユーザー名およびパスワードが分かっている場合、またはカメラが自動検出機能をサポートしていない場合には、この選択が適しています。</p>

ハードウェアの有効化/無効化

追加したハードウェアは、デフォルトでは**有効**になっています。

次の方法でハードウェアが有効化/無効化されたかどうかを確認できます。

 有効

 無効

ライセンスやパフォーマンスなどに関する目的で、追加したハードウェアを無効にする方法：

1. レコーディングサーバーを展開し、無効にするハードウェアを右クリックします。
2. **有効**を選択して、選択/解除します。

ハードウェアの編集

追加したハードウェアについて、IP アドレス/ホスト名などの基本設定を編集することができます。

1. レコーディングサーバーを展開し、編集するハードウェアデバイスを右クリックします。
2. **ハードウェアの編集**を選択します。これによって、**ハードウェアの編集**ウィンドウが表示され、関連するプロパティを編集できます。
3. **[OK]**をクリックします。

個々のデバイスの有効化/無効化

カメラは、デフォルトで**有効**です。

マイク、スピーカー、メタデータ、入力および出力は、デフォルトで**無効**です。

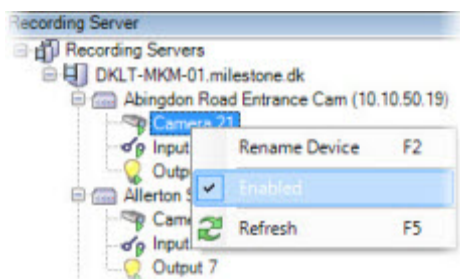
これは、システムで使用できるようにするには、マイク、スピーカー、メタデータ、入力および出力を個別に有効にしなければならないことを意味しています。理由は、監視システムは本質的にカメラに依存しているものの、マイクなどの使用の有無は、各組織のニーズによって極めて異なる場合が多いためです。

デバイスが有効か無効かを確認できます（例は出力です）。

-  無効
-  有効

同じ方法でカメラ、マイク、スピーカー、メタデータ、入力、および出力を有効化/無効化することができます。

1. レコーディングサーバーとデバイスを展開します。有効にするデバイスを右クリックします。
2. **有効**を選択して、選択/解除します。

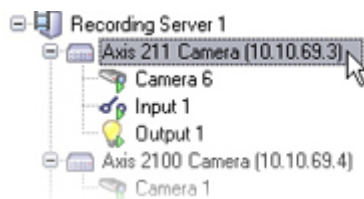


ハードウェアへの安全な接続設定する

SSL（セキュアソケットレイヤー）を使用して、ハードウェアデバイスとレコーディングサーバーの間で安全な HTTPS 接続を設定できます。

以下の手順を実行する前に、カメラメーカーにお問い合わせの上、ハードウェアの証明書の取得とハードウェアへのアップロードを行ってください。

1. **概要** ペインで、レコーディングサーバーを右クリックし、ハードウェアを選択します。



レコーディングサーバーの下でハードウェアを選択

2. **設定** タブで HTTPS を有効にします。デフォルトでは無効になっています。
3. HTTPS 接続で使用するレコーディングサーバーのポートを入力します。ポート番号は、デバイスのホームページで設定されたポートに対応する必要があります。
4. 必要に応じて変更し、保存します。

ハードウェアの移動

ハードウェアの移動

同じサイトに属するレコーディングサーバー間でハードウェアを移動できます。移動後に、ハードウェアとそのデバイスは新しいレコーディングサーバーで実行され、新しい録画がこのサーバーに保存されます。移動はクライアントユーザーに透過的です。

古いレコーディングサーバーの録画は、次の処理が発生するまで保存されたままです。

【録画】 タブで各デバイスの新しいレコーディングサーバーから録画を削除する。まだ録画が含まれるレコーディングサーバーを削除しようとする、警告が表示されます。現在ハードウェアが追加されていないレコーディングサーバーにハードウェアを移動する場合は、クライアントユーザーはログアウトしてからログインし直し、デバイスからデータを取得する必要があります。

ハードウェアの起動機能を使用すると、次のことができます。

- **ロードバランシング** : たとえば、レコーディングサーバーのディスクが過負荷状態の場合、新しいレコーディングサーバーを追加し、一部のハードウェアを移動できます。
- **アップグレード** : たとえば、レコーディングサーバーをホストするサーバーを新しいモデルで置換する場合は、新しいレコーディングサーバーをインストールし、古いサーバーから新しいサーバーにハードウェアを移動できます。
- **障害があるレコーディングサーバーの交換** : たとえば、サーバーがオフラインで、オンラインに戻らない場合は、ハードウェアを他のレコーディングサーバーに移動し、システムを実行し続けることができます。古い録画にはアクセスできません。「レコーディングサーバーの置換 『255ページ の"レコーディングサーバーの交換"参照 』」を参照してください。

リモート録画

ハードウェアを別のレコーディングサーバーに移動すると、相互接続されたサイトまたはカメラのエッジストレージからの実行中の取得または予定された取得はキャンセルされます。録画は削除されませんが、想定通りにデータは取得されず、データベースに保存されません。この場合は警告が表示されます。ハードウェアの移動を開始したときに取得を開始した Network Video Management System Smart Client ユーザーの場合、取得は失

敗します。Network Video Management System Smart Client ユーザーには通知が表示され、後から再試行できます。

別のユーザーがリモートサイトでハードウェアを移動した場合は、**[ハードウェアの更新]**オプションを使用して、手動で中央サイトを同期し、リモートサイトの新しい構成を反映する必要があります。同期しない場合は、移動されたカメラは中央サイトから切断されています。

参照

ハードウェアの移動（ウィザード） 『83ページ』

ハードウェアの移動（ウィザード）

1つのレコーディングサーバーから別のサーバーへハードウェアを移動するには、**[ハードウェアの移動]**ウィザードを実行します。ウィザードは必要な手順を案内し、1つ以上のハードウェアデバイスを移動します。

前提条件

ウィザードを開始する前に行う手順：

- 新しいレコーディングサーバーがネットワーク経由で物理カメラにアクセスできることを確認します。
- ハードウェアの移動先となるレコーディングサーバーをインストール 『32ページ の"レコーディングサーバーのインストール"参照』します。
- 認証 『62ページ の"レコーディングサーバーの認証"参照』し、オンラインであることを確認します。
- 既存のサーバーで実行する新しいレコーディングサーバーに、同じデバイスパックバージョンをインストール 『256ページ の"ビデオデバイスドライバについて"参照』します。

ウィザードを実行するには：

1. **サイトナビゲーション**ペインで、**レコーディングサーバー**を選択します。
2. **[概要]**ペインで、ハードウェアの移動元のレコーディングサーバーを右クリックするか、特定のハードウェアデバイスを右クリックします。
3. **[ハードウェアの移動]**を選択します。

ハードウェアの移動元のレコーディングサーバーが切断されている場合は、エラーメッセージが表示されます。レコーディングサーバーがオンラインにならないことが確かである場合にのみ、切断されたレコーディングサーバーからハードウェアを移動してください。ハードウェアを移動し、サーバーがオンラインに戻った場合は、同じハードウェアが2つのレコーディングサーバーで実行される期間があるため、システムで予期しない動作が発生するおそれがあります。たとえば、ライセンスエラーや、イベントが正しいレコーディングサーバーに送信されないといった問題が生じる可能性があります。

4. レコーディングサーバーレベルでウィザードを開始した場合は、**[移動するハードウェアを選択]**ページが表示されます。移動するハードウェアデバイスを選択します。
5. **[ハードウェアの移動先となるレコーディングサーバーを選択]**ページで、このサイトにインストールされたレコーディングサーバーのリストから選択します。
6. **[将来の録画で使用するストレージを選択]**ページで、ストレージ使用状況バーに、アーカイブではなくライブ録画のみのレコーディングデータベースの空き領域が表示されます。合計保持期間は、レコーディングデータベースとアーカイブの両方の保持期間です。
7. システムが要求を処理します。

8. 移動が成功した場合は、**【閉じる】**をクリックします。Management Client で新しいレコーディングサーバーを選択する場合は、移動されたハードウェアが表示され、録画がこのサーバーに保存されます。

移動が失敗した場合は、以下に従って問題をトラブルシューティングできます。

ハードウェアの移動のトラブルシューティング

移動が失敗した場合は、次の理由のいずれかが原因である可能性があります。


エラータイプ	トラブルシューティング
レコーディングサーバーが接続されていないか。	レコーディングサーバーがオンラインであることを確認してください。承認が必要な場合があります。
レコーディングサーバーが最新バージョンではありません。	レコーディングサーバーを更新し、管理サーバーと同じバージョンで実行されるようにします。
レコーディングサーバーが設定に見つかりません。	レコーディングサーバーを認証したか、レコーディングサーバーが削除されていないことを確認してください。
構成の更新または構成データベースとの通信が失敗しました。	SQL Server が接続され、実行中であることを確認してください。
現在のレコーディングサーバーで停止できませんでした。	別のプロセスがレコーディングサーバーをロックしているか、レコーディングサーバーがエラーモードである可能性があります。 レコーディングサーバーが実行中であることを確認し、再試行してください。
ハードウェアが存在しません。	移動するハードウェアが別のユーザーと同時にシステムから削除されていないことを確認してください。この状況が発生することはほとんどありません。
ハードウェアが削除されたレコーディングサーバーがオンラインに戻りましたが、オフラインのときに無視するように選択しました。	一般的に、 【ハードウェアの移動】 ウィザードを開始したときに古いレコーディングサーバーがオンラインにならないことを確認しましたが、移動中にサーバーがオンラインになりました。 ウィザードをもう一度開始し、サーバーがオンラインに戻らないかどうかを確認する手順で 【いいえ】 を選択します。

ハードウェアの管理

情報タブ (ハードウェア)

リモートサーバーの**情報タブ**の詳細については、**情報タブ (リモートサーバー)** を参照してください。

情報タブ (ハードウェア)

名前	詳細
名前	名前を入力します。この名前は、システムやクライアントでハードウェアが列挙されるたびに使用されます。名前は一意である必要はありません。 ハードウェアの名前を変更すると、名前は Management Client で一括変更されます。
詳細	ハードウェアの説明を入力します (オプション)。説明は、システム内の複数のリストに表示されます。たとえば、 概要 ペインでハードウェア名にマウスポインタを移動すると表示されます。  カメラの例。
モデル	ハードウェアモデルを規定します。
バージョン	製造元から指定されているシステムのファームウェアバージョンを表示します。
シリアル番号	メーカーが指定したハードウェアのシリアル番号。シリアル番号は、MAC アドレスと同じであることがよくありますが、必ず一致するわけでもありません。
ドライバー	ハードウェアへの接続を処理しているドライバーを規定します。
IE	ハードウェア製造元のデフォルトホームページを開きます。このページはハードウェアの管理に使用します。
アドレス	ホスト名、IP アドレス。
MAC アドレス	システムハードウェアのハードウェアメディアアクセスコントロール (MAC) アドレスを指定します。MAC アドレスは、ネットワーク上の各ハードウェアを一意に識別する 12 文字の 16 進数です。

設定タブ (ハードウェア)

設定タブで、ハードウェアの設定を確認または編集できます。

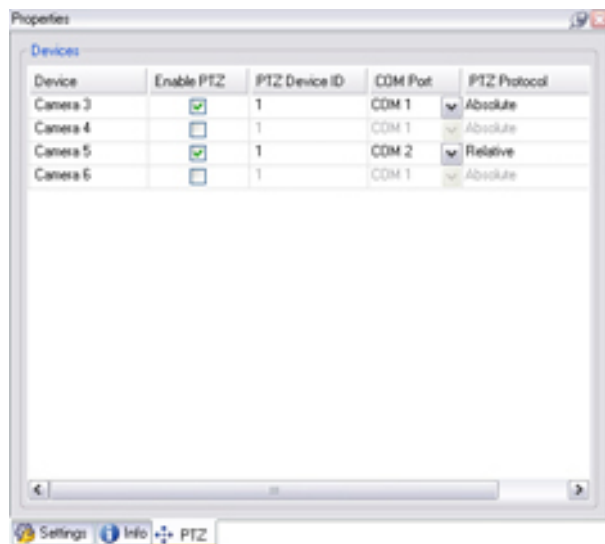
設定タブの内容は、選択したハードウェアによって決定されます。このため、ハードウェアの種類によって内容が異なります。ハードウェアの種類によっては、**設定タブ**の内容がまったく表示されないか、または読み取り専用の場合があります。

PTZ タブ (ビデオエンコーダー)

PTZ タブでは、ビデオエンコーダーの PTZ (パン/チルト/ズーム) を有効にできます。選択されたデバイスがビデオエンコーダーであるか、ドライバーが非 PTZ および PTZ カメラの両方をサポートしている場合に、このタブを使用できます。

PTZ タブの各ビデオエンコーダーのチャンネルで、PTZ の使用を個別に有効にすると、ビデオエンコーダーに接続された PTZ カメラの PTZ 機能を使用できます。

一部のビデオエンコーダーは、PTZ カメラに対応していません。PTZ カメラの使用をサポートするビデオエンコーダーでも、PTZ カメラを使用する前に、設定が必要な場合があります。通常は、デバイスの IP アドレスで、ブラウザベースの設定インターフェースを使用して、追加ドライバーをインストールします。



2つのビデオエンコーダーチャンネルに対して **PTZ** が有効になっている状態の PTZ タブ

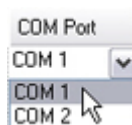
ビデオエンコーダーでの PTZ の有効化

ビデオエンコーダーで PTZ カメラの使用を有効にするには、**PTZ** タブで次の手順を実行します。

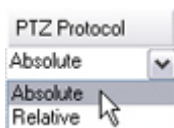
1. ビデオエンコーダーに接続されているデバイスのリストで、該当するカメラの **PTZ** を有効化ボックスを選択します。



2. **PTZ** デバイス ID 列で、各カメラの ID を確認します。
3. **COM** ポート列で、PTZ 機能を制御するために使用する、ビデオエンコーダーの COM (シリアル通信) ポートを選択します。



4. **PTZ** プロトコル列で、使用する位置スキームを選択します。



- **絶対値** : オペレータがカメラの PTZ (パン/チルト/ズーム) 制御を使用すると、固定位置 (カメラのホーム位置) に対して相対的にカメラが調整されます。
- **相対的** : オペレータがカメラの PTZ (パン/チルト/ズーム) 制御を使用すると、現在の位置に対して相対的にカメラが調整されます。

PTZ プロトコル列の内容は、ハードウェアによって大きく異なります。5~8 の異なるプロトコルがあります。カメラのマニュアルも参照してください。

5. ツールバーで**保存**をクリックします。

これで、各 PTZ カメラのプリセット位置とパトロールを設定できます。

- プリセット位置を追加する (タイプ 1) 『109ページ』
- パトロール設定の追加 『116ページ』

デバイス

ハードウェアを**ハードウェアの追加**ウィザードで追加すると、デバイスが **Management Client** に表示されます。

デバイスが同じプロパティであれば、デバイスグループからデバイスを管理できます。デバイスグループについて 『87ページ』をご覧ください。

デバイスを個別に管理することもできます。

- カメラ
- マイク
- スピーカー
- メタデータ
- 入力
- 出力

デバイスについて 『90ページ』を参照してください。

デバイスグループの操作

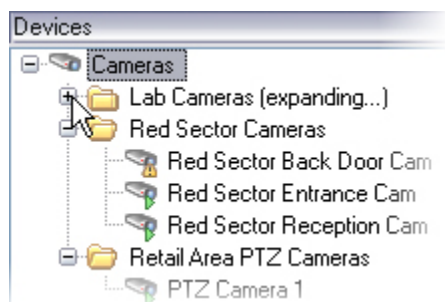
デバイスグループについて

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

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

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

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



例：デバイスグループでグループ化されたカメラ

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

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

以下の例は、カメラのデバイスグループへのグループ化に基づいていますが、原則はすべてのデバイスに適用されます。

デバイスグループの追加 『88ページ』

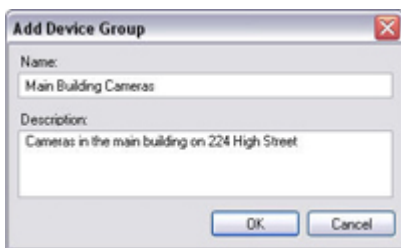
デバイスグループに含めるデバイスの指定 『89ページ』

デバイスグループのすべてのデバイスに対する共通プロパティの指定 『90ページ』

デバイスグループの追加

1. 概要ペインで、アイテムの中から、下にデバイスグループを作成するデバイスタイプを右クリックします。
2. デバイスグループの追加を選択します。

3. **デバイスグループの追加**ダイアログボックスで、新しいデバイスグループの名前と説明を指定します。



デバイスグループリストのデバイスグループの上でマウスポインタを一時停止させると、説明が表示されます。

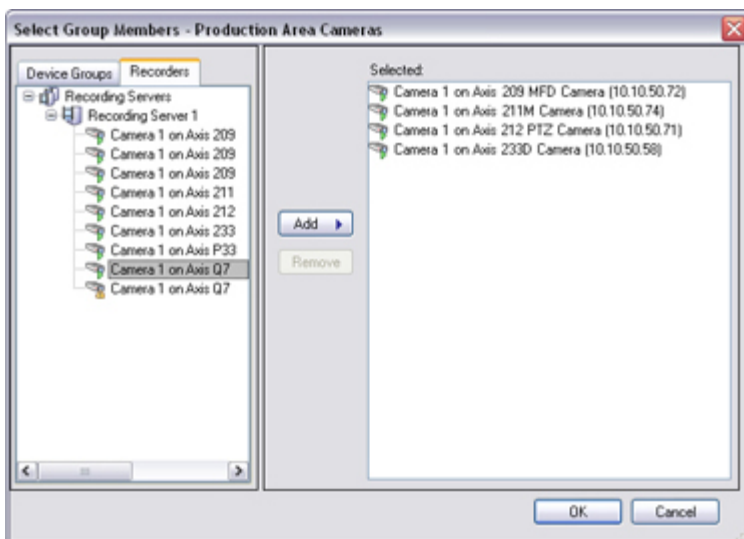
4. **OK** をクリックします。新しいデバイスグループを表すフォルダがリストに追加されます。
5. デバイスグループに含めるデバイスの指定 『89ページ』 を続けます。

デバイスグループに含めるデバイスの指定

1. **概要** ペインで、関連するデバイスグループフォルダを右クリックします。
2. **デバイスグループメンバーを編集** を選択します。
3. **グループメンバーを選択** ウィンドウで、デバイスを配置するタブを1つ選択します。

デバイスは、複数のデバイスグループのメンバーになれます。

4. 含めたいデバイスを選択して、**追加** ボタンをクリックするかデバイスをダブルクリックします。



5. **OK** をクリックします。

- 1 グループに 400 デバイスの制限を超過する場合は、デバイスグループを他のデバイスグループのサブグループとして追加できます。



デバイスグループのすべてのデバイスに対する共通プロパティの指定

デバイスグループでは、特定のデバイスグループ内のすべてのデバイスの共通設定を指定できます。

1. 概要ペインで、デバイスグループをクリックします。

プロパティペインには、**デバイスグループのすべてのデバイスで使用できる**すべてのプロパティが、タブでグループ化されて一覧表示されます。

2. 関連する共通のプロパティを指定します。

設定タブで、**すべてのデバイス**の設定および個々のデバイスの設定の間で切り替えることができます。

3. ツールバーで**保存**をクリックします。設定は個別のデバイスに保存され、デバイスグループには保存されません。

デバイスの使用

デバイスについて

ハードウェアには、以下のように、個別に管理できるデバイスが複数あります。

- 物理カメラには、カメラ部品（レンズ）を表すデバイスおよび、接続型または内蔵型のマイク、スピーカー、メタデータ、入力および出力などのデバイスが付いています。
- ビデオエンコーダーには、複数のアナログカメラが接続されており、デバイスのリスト 1 枚に表示されます。これには、カメラ部品（レンズ）を表すデバイスおよび、接続型または内蔵型のマイク、スピーカー、メタデータ、入力および出力などのデバイスが含まれています。
- I/O モジュールには、ライトなど、入出力チャンネルを表すデバイスが付いています。

音声専用モジュールには、マイクやスピーカーの入出力を表すデバイスが付いています。ハードウェアを追加すると、ハードウェアのデバイスが自動的に追加されます。以下のセクションでは、管理に使用できるタブへのリンク付きの各デバイスタイプについて説明します。

カメラデバイスについて

カメラデバイスは、システムにハードウェアを追加したときに自動的に追加され、デフォルトで有効化されます。

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

システムにはデフォルトの配信開始ルールがあります。このルールにより、接続されているすべてのカメラからの映像配信が自動的にシステムに送られます。他のルールと同様、必要に応じて、デフォルトルールを無効にしたり修正したりできます。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。デバイスグループ経由のデバイスの有効化/無効化 『95ページ』を参照してください。

カメラのその他のすべての設定や管理を行うには、サイトナビゲーションペインで**デバイス**を展開してから、**カメラ**を選択します。概要ペインで、カメラの概要を分かりやすくするためにカメラをグループ化します。初期グループ化は、**ハードウェアの追加**ウィザードの一部です。

この設定順序に従って、カメラデバイスの設定に関連する最も一般的なタスクを実行します。

1. カメラの設定（設定タブ 『98ページ』の"設定タブ(デバイス)"参照』を参照してください）。
2. ストリームの設定（ストリームタブ 『100ページ』の"ストリームタブ(デバイス)"参照』を参照してください）。
3. モーションの設定（モーションタブ 『125ページ』の"モーションタブ(デバイス)"参照』を参照してください）。
4. 記録の設定（記録タブ 『102ページ』の"録画タブ(デバイス)"参照』を参照してください）。
5. 必要に応じて他の設定を設定します。

マイクデバイスについて

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

マイクデバイスは、システムにハードウェアを追加したときに自動的に追加されます。デフォルトでは無効化されているため、使用する前に、**ハードウェアの追加**ウィザードから、または後日に有効化する必要があります。マイクには特にライセンスは必要ありません。システムで必要な数のマイクを無制限に使用できます。

マイクは、完全にカメラとは別に使用できます。

マイクデバイスは、音声ストリームをシステムに送信し、クライアントユーザーはライブ音声として聞くことができます。あるいは、音声ストリームをシステムが録音して、クライアントユーザーは後日に再生できます。関連するアクションをトリガするマイク固有のイベントを受信するように、システムを設定できます。

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

システムにはデフォルトの音声配信開始ルールがあります。このルールに従って、接続されているすべてのマイクからの音声配信が自動的にシステムに送られます。他のルールと同様、必要に応じて、デフォルトルールを無効にしたり修正したりできます。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。デバイスグループ経由のデバイスの有効化/無効化 『95ページ』を参照してください。

カメラのその他すべての設定や管理を行うには、サイトナビゲーションペインで**デバイス**を展開してから、**マイク**を選択します。概要ペインでは、マイクをグループ化して、概要を把握しやすくなることができます。初期グループ化は、**ハードウェアの追加**ウィザードの一部です。

マイクデバイスは、以下のタブを使って設定できます。

- 情報タブ 『97ページ』の"情報タブ(デバイス)"参照』
- 設定タブ 『98ページ』の"設定タブ(デバイス)"参照』
- 録画タブ 『102ページ』の"録画タブ(デバイス)"参照』

- イベントタブ 『119ページ の"イベントタブ(デバイス)"参照 』

スピーカーデバイスについて

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

スピーカーデバイスは、システムにハードウェアを追加したときに自動的に追加されます。デフォルトでは無効化されているため、使用する前に、**ハードウェアの追加**ウィザードから、または後日に有効化する必要があります。スピーカーには特にライセンスは必要ありません。システムに必要な数のスピーカーを無制限に使用できます。

スピーカーは、完全にカメラとは別に使用できます。

ユーザーが Network Video Management System Smart Client の会話ボタンを押すと、スピーカーに音声ストリームが配信されます。スピーカーの音声は、ユーザーがスピーカーに向かって話したときのみ録音されます。役割により、ユーザーがスピーカで話す権限を決定します。Management Client からスピーカーを通して話すことはできません。

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

システムにはデフォルトの音声配信開始ルールがあります。このルールに従って、デバイスが起動され、ユーザーが有効にした音声をデバイスからスピーカーに送信する準備ができます。他のルールと同様、必要に応じて、デフォルトルールを無効にしたり修正したりできます。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。デバイスグループ経由のデバイスの有効化/無効化 『95ページ 』を参照してください。

カメラのその他すべての設定や管理を行うには、サイトナビゲーションペインで**デバイス**を展開してから、**スピーカー**を選択します。概要ペインでは、スピーカーをグループ化して、概要を把握しやすことができます。初期グループ化は、**ハードウェアの追加**ウィザードの一部です。

スピーカーデバイスは、以下のタブを使って設定できます。

- 情報タブ 『97ページ の"情報タブ(デバイス)"参照 』
- 設定タブ 『98ページ の"設定タブ(デバイス)"参照 』
- 録画タブ 『102ページ の"録画タブ(デバイス)"参照 』

メタデータデバイスについて

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

メタデータは以下の方法で生成できます。

- 映像を配信するカメラなど、デバイス自体がデータを配信する。
- サードパーティシステムまたは統合で、汎用メタデータドライバーを経由した配信。

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

役割により、ユーザーがメタデータを参照する権限が決定されます。

システムにはデフォルトの配信開始ルールがあります。このルールに従って、メタデータをサポートする接続されているすべてのハードウェアからのメタデータ配信が自動的にシステムに送られます。他のルールと同様、必要に応じて、デフォルトルールを無効にしたり修正したりできます。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。デバイスグループ経由のデバイスの有効化/無効化 『95ページ』を参照してください。

メタデータデバイスのその他すべての設定や管理を行うには、サイトナビゲーションペインで**デバイス**を展開してから、**メタデータ**を選択します。概要ペインでは、メタデータデバイスをグループ化して、概要を把握しやすくすることができます。初期グループ化は、**ハードウェアの追加**ウィザードの一部です。

メタデータデバイスは、以下のタブを使って設定できます。

- 情報タブ 『97ページ の"情報タブ(デバイス)"参照 』
- 設定タブ 『98ページ の"設定タブ(デバイス)"参照 』
- 録画タブ 『102ページ の"録画タブ(デバイス)"参照 』

入力デバイスについて

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

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

入力デバイスは、完全にカメラとは別に使用できます。

デバイスで外部入力ユニットの使用を指定する前に、デバイス自体がセンサーの動作を認識しているか確認してください。大半のデバイスでは、設定用インターフェースかコモンゲートウェイインターフェース(CGI)スクリプトのコマンドでこれを表示できます。

入力デバイスは、システムにハードウェアを追加したときに自動的に追加されます。デフォルトでは無効化されているため、使用する前に、**ハードウェアの追加**ウィザードから、または後日に有効化する必要があります。入力デバイスには特にライセンスは必要ありません。システムで必要な数の入力デバイスを無制限に使用できます。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。デバイスグループ経由のデバイスの有効化/無効化 『95ページ』を参照してください。

カメラのその他すべての設定や管理を行うには、サイトナビゲーションペインで**デバイス**を展開してから、**入力**を選択します。概要ペインでは、入力デバイスをグループ化して、概要を把握しやすくすることができます。初期グループ化は、**ハードウェアの追加**ウィザードの一部です。

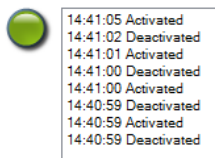
入力デバイスは、以下のタブを使って設定できます。

- 情報タブ 『97ページ の"情報タブ(デバイス)"参照 』
- 設定タブ 『98ページ の"設定タブ(デバイス)"参照 』
- イベントタブ 『119ページ の"イベントタブ(デバイス)"参照 』

手動で入力を有効にしてテストする

ルール機能を使用して、入力を自動的に有効化または無効化するルールを定義するか、または Management Client から手動で有効化してルールをチェックできます。

1. **概要** ペインで、関連する入力デバイスを選択します。
2. 物理的デバイスで入力を有効にします。
3. **プレビュー** ペインで、緑色のインジケータが点灯していることを確認します。これで、入力デバイスが動作します。



出力デバイスについて

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

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

出力は、Management Client および Network Video Management System Smart Client から手動でトリガできます。

デバイスで外部出力ユニットの使用を指定する前に、デバイス自体が出力に接続されたデバイスを制御できるかどうかを確認してください。大半のデバイスでは、設定用インターフェースかコモンゲートウェイインターフェース (CGI) スクリプトのコマンドでこれを表示できます。

出力デバイスは、システムにハードウェアを追加したときに自動的に追加されます。デフォルトでは無効化されているため、使用する前に、**ハードウェアの追加** ウィザードから、または後日に有効化する必要があります。出力デバイスには特にライセンスは必要ありません。システムに必要な数の出力デバイスを無制限に使用できます。

各デバイスの有効化/無効化および名前変更は、レコーディングサーバーのハードウェア上で行われます。デバイスグループ経由のデバイスの有効化/無効化 『95ページ』を参照してください。

カメラのその他すべての設定や管理を行うには、サイトナビゲーションペインで**デバイス**を展開してから、**出力**を選択します。概要ペインでは、入力デバイスをグループ化して、概要を把握しやすくすることができます。初期グループ化は、**ハードウェアの追加** ウィザードの一部です。

出力デバイスは、以下のタブを使って設定できます。

- 情報タブ 『97ページ の"情報タブ(デバイス)"参照』
- 設定タブ 『98ページ の"設定タブ(デバイス)"参照』


手動で出力を有効にしてテストします。

ルール機能を使用して、出力を自動的に有効化または無効化するルールを定義するか、またはクライアントから手動で有効化できます。


Management Client から出力を手動で有効にして、機能をテストできます。

1. **概要**ペインで、関連する出力デバイスを選択します。
2. 通常は、**プレビュー**ペインでそれぞれの出力について以下の要素が表示されます。



3. チェックボックス  を選択/選択解除すると、選択した出力を有効化/無効化します。出力が有効になると、緑色のインジケータが点灯します。



4. あるいは、長方形のボタン  をクリックすると、**設定**タブの**出力トリガ時間**設定で定義される期間、出力が有効になります（この機能/設定はすべての出力で使用できるわけではありません）。定義された期間が過ぎると、出力は自動的に無効になります。

デバイスグループ経由のデバイスの有効化/無効化





設定済みハードウェアからのみデバイスを有効化/無効化できます。ハードウェアの追加ウィザードから手動で有効化/無効化した場合を除いて、カメラデバイスはデフォルトで有効化されており、他のデバイスはデフォルトで無効化されています。

デバイスを有効または無効にするためにデバイスグループ経由でアクセスする方法：

1. **サイトナビゲーション**ペインで、デバイスを選択します。
2. **概要**ペインで、関連グループを展開してデバイスを検索します。
3. デバイスを右クリックして、**ハードウェアに移動**を選択します。
4. **[+]**ノードをクリックして、ハードウェア上のすべてのデバイスを表示します。
5. 有効/無効にするデバイスを右クリックして、**有効**を選択します。

デバイスのステータスアイコン

デバイスを選択すると、現在のステータスについての情報が**プレビュー**ペインに表示されます。以下のアイコンはデバイスのステータスを示します：

カメラ	マイク	スピーカー	メタデータ	入力	出力	詳細
						有効なデバイスおよびデータの取得中： デバイスは有効化されており、ライブストリームを取得します。

カメラ	マイク	スピーカー	メタデータ	入力	出力	詳細
						デバイスは記録中： デバイスはシステムにあるデータを記録中です。
						一時的に停止されているか、入力のないデバイス： 停止している場合は、情報はシステムに転送されません。カメラの場合は、ライブビデオを表示できません。停止したデバイスは、デバイスが無効である場合とは対照的に、レコーディングサーバーと通信してイベントの取得、設定の設定などが可能です。
						無効なデバイス： ルールを通して自動的に開始されず、レコーディングサーバーと通信できません。カメラが無効な場合は、ライブまたは録画されたビデオを表示できません。
						デバイスデータベースを修復中です。
						デバイスに問題が発生しています。 このデバイスは正しく機能しません。マウスポインタをデバイスアイコンの上で一次停止させて、ヒントに書かれている問題の説明を確認します。
						不明なステータスです： デバイスのステータスが不明です。例えば、レコーディングサーバーがオフラインの場合など。
						複数のアイコンを組み合わせることができます。例えばこの場合では 有効なデバイスおよびデータの取得中 が デバイスは記録中 と組み合わせられています。

情報タブ(デバイス)

情報タブについて

情報タブで、デバイスに関する基本情報を複数のフィールドで表示および編集することができます。すべてのデバイスに**情報**タブがあります。

カメラの場合の**情報**タブの例

情報タブのプロパティ

名前	詳細
名前	<p>デバイスがシステムおよびクライアントに一覧されるときにこの名前が使用されます。</p> <p>デバイスの名前を変更すると、名前は Management Client で一括変更されます。</p>
詳細	<p>デバイスの説明を入力します (オプション)。</p> <p>説明は、システム内の複数のリストに表示されます。例えば、概要ペインで名前にマウスポインタを移動すると表示されます。</p>
ハードウェア名	<p>デバイスが接続されているハードウェアの名前を表示します。ここからはフィールドを編集できませんが、その横にある移動をクリックして変更することができます。これによりハードウェア情報に移動し、名前を変更できます。</p>

名前	詳細
ポート番号	デバイスがハードウェアに接続されているポートを表示します。 デバイスが1つしかないハードウェアでは、ポート番号は通常 1 になります。複数のチャンネルがあるビデオサーバーなどのマルチデバイスハードウェアでは、通常、ポート番号はデバイスが接続されているチャンネルを示しています（例、 3 ）。

設定タブ(デバイス)

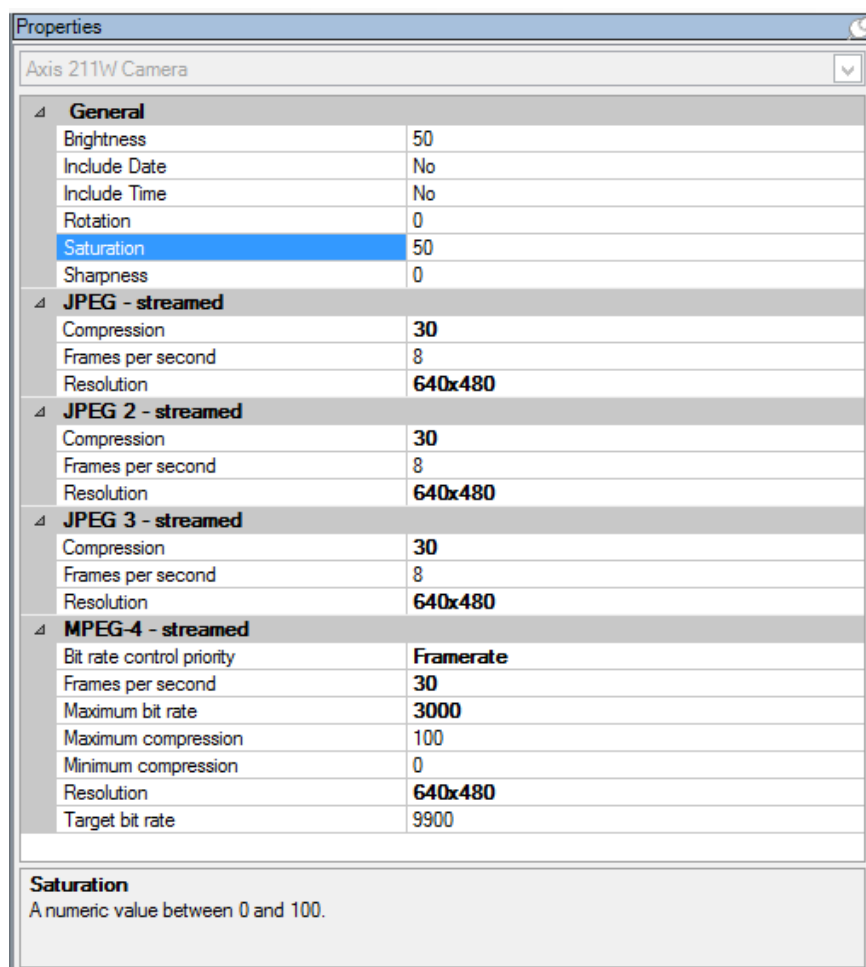
設定タブについて

設定タブで、デバイスの設定を複数のフィールドで表示および編集することができます。
すべてのデバイスに**設定**タブがあります。

表に表示される値は、変更可能または読み取り専用です。設定をデフォルト以外の値に変更した場合は、値が**太字**で表示されます。

テーブルの内容はデバイスドライバーによって異なります。

許可された範囲が設定表の下の情報ボックスに表示されます。



カメラの設定タブの例。

カメラ設定について

以下の設定を表示または編集できます。

- デフォルトのフレームレート
- 解像度
- 圧縮
- キーフレーム間のフレームの最大数

選択したカメラまたは選択したデバイスグループ内のすべてのカメラの画面の日時およびテキスト表示カメラのドライバーが【設定】タブのコンテンツを決定します。ドライバーはカメラのタイプによって異なります。MJPEG、および MPEG-4/H.264/H.265 などの 2 つ以上のストリームのタイプをサポートしているカメラでは、マルチストリーミングを使用できます。マルチストリーミングについて 『100ページ』をご覧ください。

設定を変更する場合は、【プレビュー】ペインを有効にすると、変更の影響を簡単に確認できます。【プレビュー】ペインを使用してフレームレート変更の影響を判断することはできません。その理由は、【プレビュー】ペインのサムネイル画像では【オプション】ダイアログボックスで定義された他のフレームレートを使用しているためです。

【キーフレーム間の最大フレーム】および【キーフレームモード間の最大フレーム】の設定を変更すると、Network Video Management System Smart Client の一部の機能のパフォーマンスが低下するおそれがあります。たとえば、Network Video Management System Smart Client はビデオ表示の起動にキーフレームが必要なので、キーフレーム間の期間が長いと、Network Video Management System Smart Client の起動が長引きます。

ストリームタブ(デバイス)

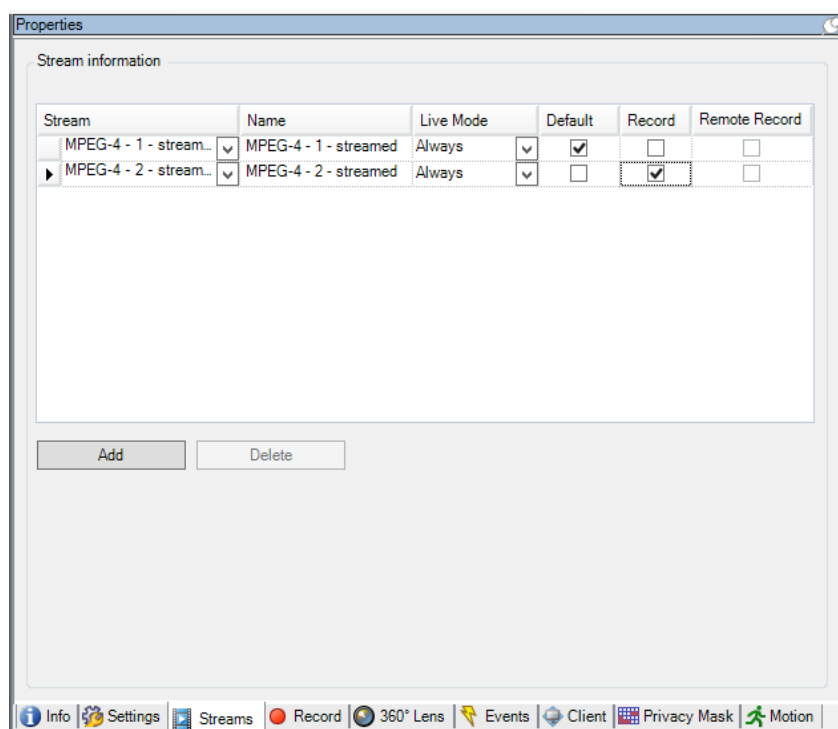
ストリームタブについて

以下のデバイスにストリームタブがあります。

- カメラ

ストリームタブはデフォルトで単一のストリームを一覧表示します。このストリームは、選択したカメラのデフォルトのストリームであり、ライブビデオや、録画したビデオで使用されます。

ライブストリームには、カメラがサポートしている複数のライブストリームを設定できますが、録画には一度に1つのストリームしか選択できません。録画に使用するストリームを変更するには、録画するストリームの**記録**ボックスを選択します。



マルチストリーミングについて

録画済みビデオの再生およびライブビデオの表示で最善の結果を得るには、必ずしも同じビデオ画質やフレームレートが必要とは限りません。ストリームのうちの**いずれか1つ**をライブ表示用にして、もう1つを再生目的で使用することもできますし、**または**複数の独立したライブストリームとして、異なる解像度、エンコーディング、およびフレームレートで使用することも可能です。

例 1、ライブおよび録画されたビデオ：

- ライブビデオの再生では、組織によって高いフレームレートでの MPEG4 が望ましい場合があります。

- 録画ビデオを再生する場合、組織によって低いフレームレートでの MJPEG で、ディスクの空き容量を保持できる方が望ましい場合もあります。

例 2、複数のライブビデオ：

- ローカルな操作ポイントからライブビデオを再生する場合、可能な限り高品質のビデオを利用するために、組織によって高いフレームレートでの MPEG4 が望ましい場合があります。
- リモート接続された操作ポイントからライブビデオを再生する場合、ネットワーク帯域を保持するために、組織によって低いフレームレートでの MJPEG が望ましい場合もあります。

たとえカメラがマルチストリーミングをサポートしていても、カメラによって個々のマルチストリーミングの機能は異なります。詳細については、カメラの文書を参照してください。

カメラが異なるタイプのストリームを提供しているか確認するために、

ストリームの追加

1. ストリームタブで、**追加**をクリックします。この操作で、リストに 2 番目のストリームが追加されます。
2. 名前列で、ストリームの名前を編集します。名前は Network Video Management System Smart Client に表示されます。
3. ライブモード列で、いつライブストリームが必要かを選択します。
 - **常時**：Network Video Management System Smart Client ユーザーがストリームを要求しなくても、ストリームは実行されます。
 - **設定しない**：ストリームはオフです。例えば、ストリームを高画質で録画したいが帯域幅が必要な場合のみ、これを使用します。
 - **必要な場合**：ストリームは Network Video Management System Smart Client ユーザーが要求したときに開始します。
4. デフォルト列では、どのストリームをデフォルトにするかを選択します。
5. 録画列で、このストリームを録画する場合はチェックボックスを選択し、ライブビデオのみに使用する場合はクリアします。
6. リモート録画列で、この録画ストリームをリモートおよびエッジ記録の取得に使用する場合は、チェックボックスを選択します。
7. **保存**をクリックします。

重要：ストリームが**既定**または**記録**に設定されている場合、ストリームは常に**ライブモード**設定とは関係なく実行します。**【必要な場合】**および**【常時】**を選択しても同じ結果になります。また、**【録画しない】**を選択すると、ストリームは実行されますが、ライブ表示はできません。

誰もライブビデオを見ていない場合にストリームを実行しないようにするには、**【デフォルトの映像配信開始ルール】**を修正し、定義済みの**クライアントライブフィードの要求イベント**を使用して要求することで開始できます。

録画タブ(デバイス)

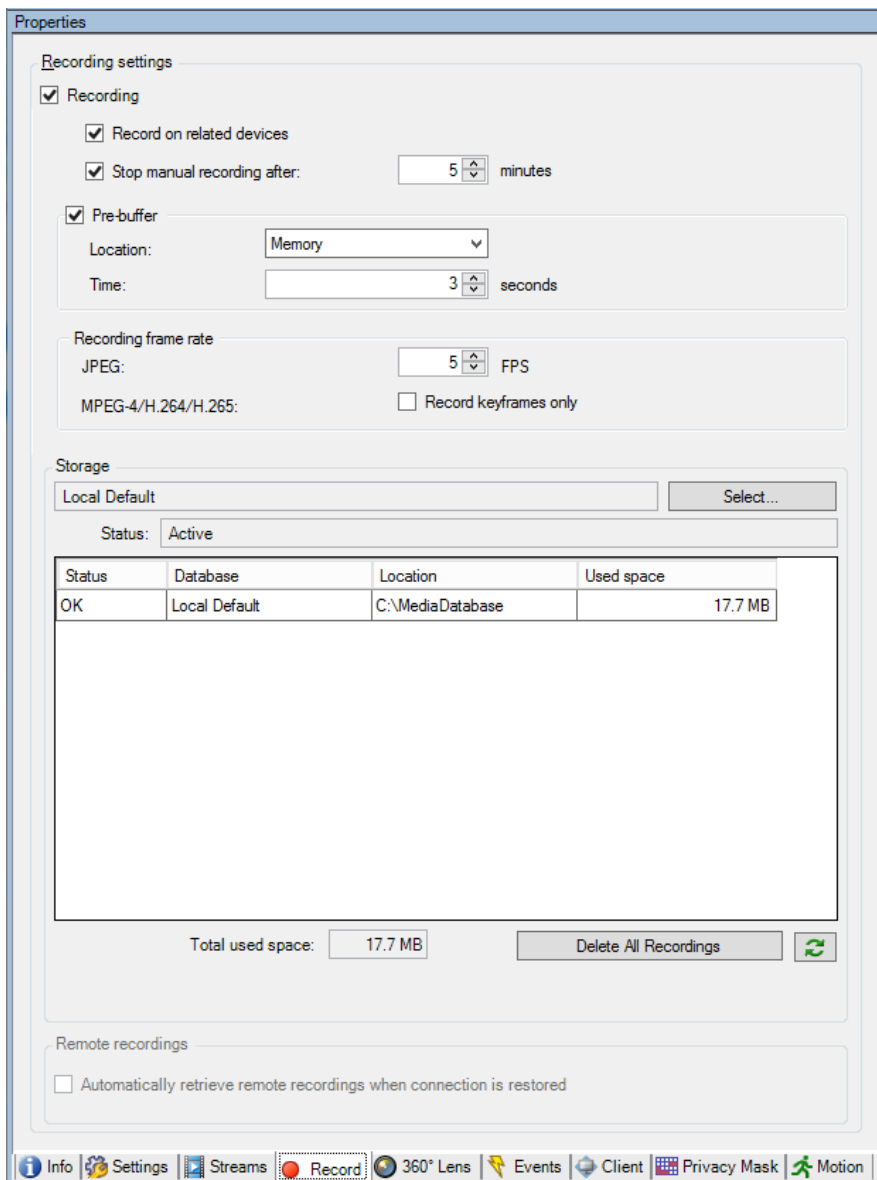
【録画】タブについて

以下のデバイスに【記録】タブがあります。

- カメラ
- マイク
- スピーカー
- メタデータ

デバイスの録画は、録画を有効にし、録画関連ルール条件が満たされたときにだけ、データベースに保存されます。

デバイスで設定できないパラメータは淡色表示されます。



カメラの【録画】タブの例

記録の有効化と無効化

デフォルトでは記録は有効になっています。記録を有効化/無効化する方法：

1. サイトナビゲーションペインで、レコーディングサーバーを選択します。
2. 概要ペインで関連するデバイスを選択します。
3. 録画タブで、録画チェックボックスを選択します。

カメラからのデータの録画を可能にするには、デバイスの録画を有効にする必要があります。デバイスの録画を無効にすると、デバイスの録画状態を指定するルールが動作しません。

関連するデバイスで録画を有効にする

カメラデバイスの場合、マイクやスピーカーなど、同じレコーディングサーバーに接続されている関連するデバイスの録画を有効にすることができます。これは、カメラが録画する際に、関連するデバイスが録画することを意味します。

新しいカメラデバイスではデフォルトで関連するデバイスの録画が有効になっていますが、必要に応じて無効または有効にすることができます。システムにある既存のカメラデバイスの場合、このチェックボックスはデフォルトでクリアされています。

1. サイトナビゲーションペインで、**レコーディングサーバー**を選択します。
2. **概要**ペインで関連するカメラデバイスを選択します。
3. **録画**タブで、**関連するデバイスで録画する**チェックボックスを選択します。
4. **クライアント**タブで、このカメラに関連付けるデバイスを指定します。

他のレコーディングサーバーに接続されている関連デバイスで録画を有効にしたい場合は、ルールを作成する必要があります。

プレバッファについて

プレバッファは、実際のイベントトリガが発生する前に音声およびビデオを記録する機能です。これは、ドアが開くなど、記録をトリガするイベントにつながる音声またはビデオを記録したい時に便利です。

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

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

プレバッファ機能を使用するには、デバイスを有効にしてストリームをシステムに送信する必要があります。

一時プレバッファ録画の保存

一時プレバッファ録画の保存場所は次のいずれかを選択できます。

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

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

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

プレバッファをサポートするデバイス

カメラ、マイク、およびスピーカーがプレバッファをサポートします。スピーカーでは、Network Video Management System Smart Client ユーザーが**スピーカーで話す**機能を使用している場合にのみストリームが

送信されます。つまり、スピーカーストリームの記録がどのようにトリガされるかによって、使用可能なプレバッファがわずかであったり、プリバッファがない場合が生じます。

ほとんどの場合、Network Video Management System Smart Client ユーザーが**スピーカーで話す**機能を使用している場合に、スピーカーを記録するように設定されています。この場合は、スピーカーのプレバッファは利用できません。

プレバッファの管理

プレバッファの有効化と無効化:

プレバッファは、デフォルトでは 3 秒のプレバッファサイズで有効になっており、メモリに保存されます。

1. プレバッファを有効化/無効化するには、**【プレバッファ】**チェックボックスを選択または選択解除します。

保存場所とプレバッファ期間の指定:

一時プレバッファ録画はメモリ内またはディスク上のいずれかに保存されます。

1. **【場所】**で、**【メモリ】**または**【ディスク】**を選択して、秒数を指定します。

指定する秒数は、定義済みのさまざまな記録ルールでの要件に対応するには十分な大きさである必要があります。

15 秒を上回るプレバッファ期間が必要な場合は、**【ディスク】**を選択します。

2. 場所を**【メモリ】**に変更すると、期間が自動的に 15 秒に短縮されます。

プレバッファをルールで使用する:

録画をトリガするルールを作成する場合、録画が実際のイベントよりも少し前に始まるように選択できます(プレバッファ)。

例:以下のルールでは、カメラがモーションを検知する 5 秒前にカメラでの録画が始まるように指定しています。

Perform an action on **Motion Started**
from **Red Sector Entrance Cam**
start recording **5 seconds before** on the device on which event occurred

プレバッファリングに依存するルールの詳細

プレバッファ録画機能をルールで使用するには、録画されるデバイスのプレバッファリング機能を有効にし、プレバッファの長さを少なくともルールで定義した長さと同じに設定する必要があります。

手動記録の管理

デフォルトでは、**次の時間が経過すると手動記録を停止**が有効になっており、記録時間は 5 分です。これは、Network Video Management System Smart Client ユーザーが開始したすべての記録が自動的に停止することを保証するためです。

Stop manual recording after: minutes

1. 手動記録の自動停止を有効または無効にするには、**次の時間が経過すると手動記録を停止**チェックボックスをオンまたはオフにします。

- 有効にする場合は、記録時間を指定します。指定する分数は、システムに負荷をかけ過ぎることなく、さまざまな手動記録の要件に対応するのに十分な長さにする必要があります。

役割に追加：

デバイスタブの**役割**で、各カメラのクライアントユーザーに対して、手動記録を開始および停止する権限を付与する必要があります。

ルールで使用する：

手動記録関連するルールを作成するときに使用できるイベント：

- 手動録画が開始されました
- 手動録画が停止されました

レコーディングフレームレートを指定する

JPEG のレコーディングフレームレートを指定できます。

- レコーディングフレームレート：(JPEG)ボックスで、任意のレコーディングフレームレート（FPS、1秒当りのフレーム数）を選択または入力します。



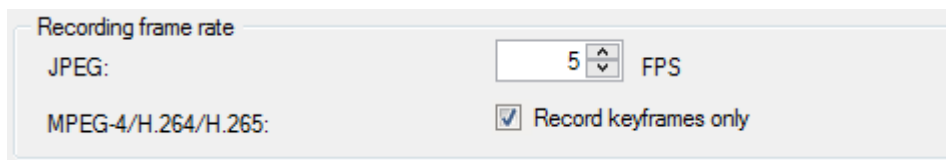
具体的なレコーディングフレームレートの指定

キーフレームレコーディングの有効化

MPEG-4/H.264/H.265 ストリームのキーフレームレコーディングを有効にできます。つまり、ルール設定によって、キーフレームの録画とすべてのフレームの録画を切り替えます。

たとえば、ビューでモーションがないときにシステムにキーフレームを録画させ、モーションが検出された場合にだけすべてのフレームに切り替えてストレージを節約できます。

- 【**キーフレームのみの録画**】ボックスを選択します。



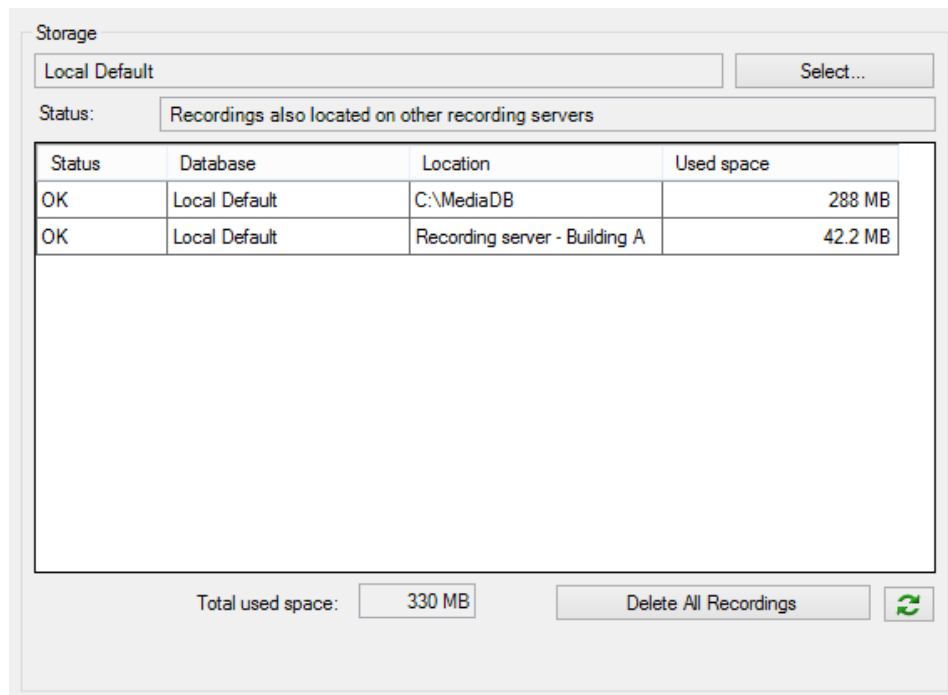
キーフレームレコーディングの有効化

- 機能を有効にするルールを設定します。アクションとアクションの停止について 『139ページ』を参照してください。

ストレージについて

【**ストレージ**】の下で、デバイス、または同じレコーディングサーバーに追加されたデバイスのグループのデータベースを監視および管理できます。

表の上では、選択されたデータベースとその状態が確認できます。この例では、選択されたデータベースはデフォルトのローカルデフォルトで、ステータスは録画が他のレコーディングサーバーにも存在するです。他のサーバーは建物 A のレコーディングサーバーです。



選択したデータベースが取りうるステータス :

名前	説明
録画は他のレコーディングサーバーにもあります	データベースがアクティブで稼動中であり、他のレコーディングサーバーのストレージにも録画があります。
アーカイブも古いストレージにあります	データベースはアクティブで実行中です。また、アーカイブは他のストレージにもあります。
アクティブ	データベースはアクティブで実行中です。
選択されたデバイスの一部に関するデータは現在他の場所に移動中です	データベースはアクティブで実行中です。グループ内の選択された 1 つ以上のデバイスで、ある場所から他の場所へデータを移動しています。
デバイスのデータは現在他の場所に移動中です	データベースはアクティブで実行中です。選択されたデバイスで、ある場所から他の場所へデータを移動しています。

さらにウィンドウの下部には、各データベースのステータス(OK、オフライン、古いストレージ)、各データベースの場所、および各データベースが占有する領域が表示されます。

すべてのサーバーがオンラインである場合は、【合計使用スペース】フィールドにストレージ全体で使用される合計領域を表示できます。

【すべての録画を削除】ボタンを使用すると、グループのすべてのデバイスを同じサーバーに追加した場合に、デバイスまたはデバイスグループのすべての録画を削除できます。

ストレージの設定についての詳細は、ストレージとアーカイブについて 『65ページ』を参照してください。

リモート録画について

ネットワークに問題が発生した場合に確実にすべての録画を保存するには、**接続が復旧したときに自動的にリモート録画を取得する**を選択します。これにより、接続の再設定時に録画の自動取得が有効になります。

選択されたハードウェアのタイプによって、どこから記録を取得するかが決まります。

- ローカル録画ストレージのあるカメラの場合、記録はカメラのローカル録画ストレージから取得されません。

自動取得とは別に、以下の機能を使用できます。

- 手動レコーディング
- <デバイス>ルールからリモートレコーディングを取得および保存します。
- <デバイス>ルールから、<開始時間と終了時間>を取得し保存します

プリセットタブ(デバイス)


プリセットタブについて

以下のデバイスに**プリセットタブ**があります。

- プリセット位置がサポートされている PTZ カメラ

プリセットタブで、プリセット位置を作成またはインポートできます。例：

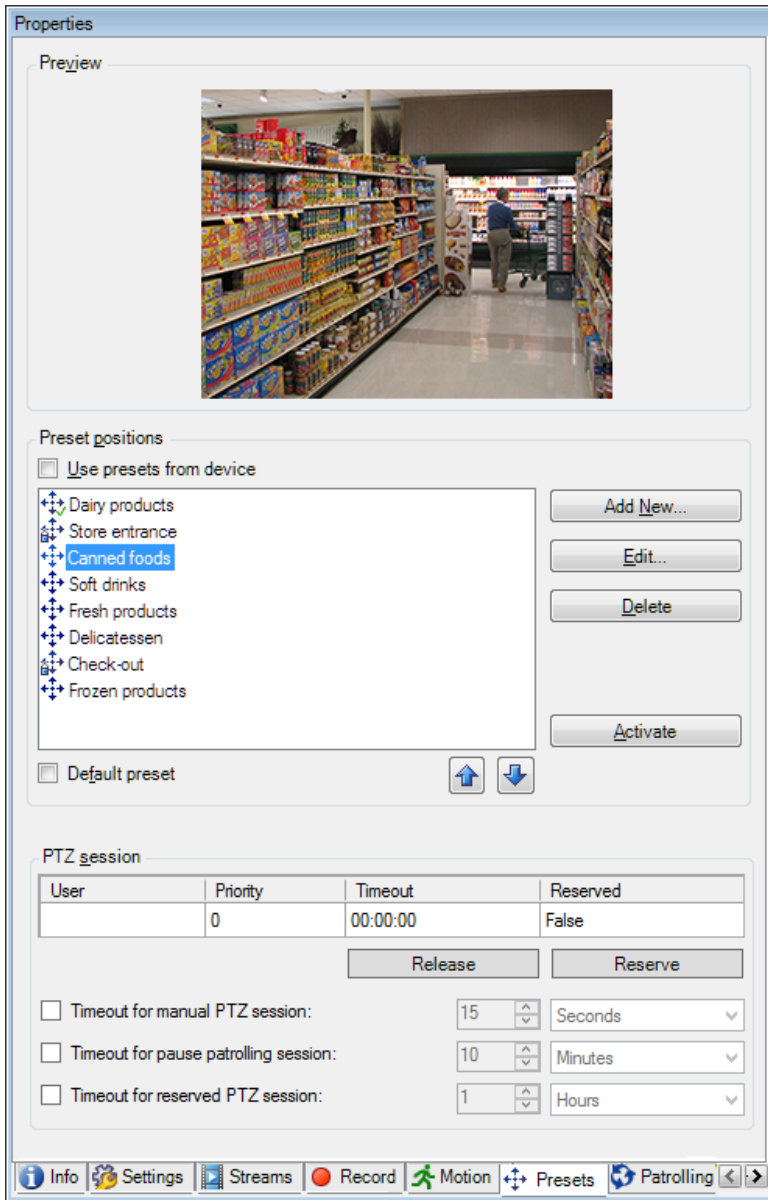
- イベント発生時に PTZ (パン/チルト/ズーム) カメラを特定のプリセット位置に移動させるためのルール。
- 複数のプリセット位置間で PTZ カメラを自動的に移動させるパトロール。
- Network Video Management System Smart Client ユーザーによる手動制御向け。

Network Video Management System Smart Client のユーザーまたは制限されたセキュリティ権限のユーザーがこのプリセットを更新できないようにする場合は、プリセット位置をロックできます。ロックされたプリセットには  アイコンが表示されます。

[セキュリティ全般]タブ 『177ページ の"セキュリティ全般タブ (役割) "参照』または[PTZ]タブ 『185ページ の"PTZ タブ (役割) "参照』で、PTZ 権限をロールに割り当てます。

[PTZ セッション]領域 『114ページ の"PTZ セッションの優先度"参照』で、現在パトロールを実行しているか、ユーザーが制御を取得したかどうかを監視できます。

カメラの PTZ セッションタイムアウトも変更できます。

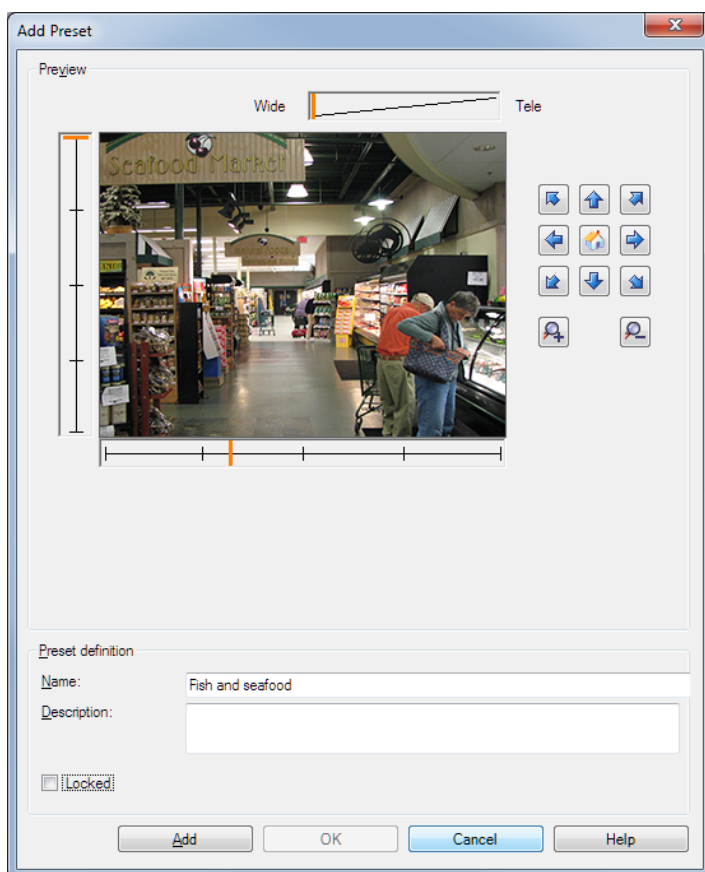


【プリセット】タブと定義済みプリセット位置

プリセット位置を追加する (タイプ 1)

プリセット位置をカメラに追加する方法：

1. 新規追加をクリックします。プリセットの追加ウィンドウが表示されます。



2. プリセットの追加ウィンドウはカメラからのライブプレビュー画像を表示します。ナビゲーションボタンおよび/またはスライダーを使用してカメラを必要な位置に移動します。
3. 名前フィールドにプリセット位置の名前を入力します。
4. オプションで、説明フィールドにプリセット位置の説明を入力します。
5. プリセット位置をロックする場合は、**[ロック]**を選択します。十分な権限を持つユーザーだけが後から位置をロック解除できます。
6. **[追加]**をクリックしてプリセットを指定します。任意のプリセットになるまで、追加し続けます。
7. **[OK]**をクリックします。プリセットの追加ウィンドウが閉じ、プリセット位置がプリセットタブのカメラの利用可能なプリセット位置のリストに追加されます。

カメラからのプリセット位置を使用します (タイプ 2)

プリセット位置をシステムに指定する代わりに、PTZ カメラのプリセット位置をカメラ自体で指定できます。通常は、デバイス固有の設定 Web ページにアクセスして定義します。

1. **プリセットをデバイスから使用**を選択して、プリセットをシステムにインポートします。

以前にカメラに定義したプリセットは削除され、定義済みルールおよびパトロールスケジュールに影響します。また、Network Video Management System Smart Client ユーザーが利用可能なプリセットは削除されます。

2. **【削除】**をクリックするとユーザーが必要ではないプリセットを削除します。
3. プリセットの表示名を変更 『112ページ の"プリセット位置名の編集 (タイプ 2 のみ) "参照 』する場合は、**【編集】**をクリックします。
4. このようなデバイス定義済みプリセットを後で編集する場合は、カメラで編集してから再インポートします。

デフォルトのプリセット位置の割り当て

必要に応じて、PTZ カメラのプリセット位置のいずれかをカメラのデフォルトのプリセット位置に割り当てることができます。

デフォルトのプリセット位置が設定されていると、PTZ カメラが手動で操作された後など、特定の状況下で PTZ カメラがデフォルトのプリセット位置に移動するように指定して、ルールを定義できるため便利です。

1. プリセット位置をデフォルトとして割り当てするには、定義済みのプリセット位置リストからプリセットを選択します。
2. リストの下にある**デフォルトのプリセット**チェックボックスを選択します。

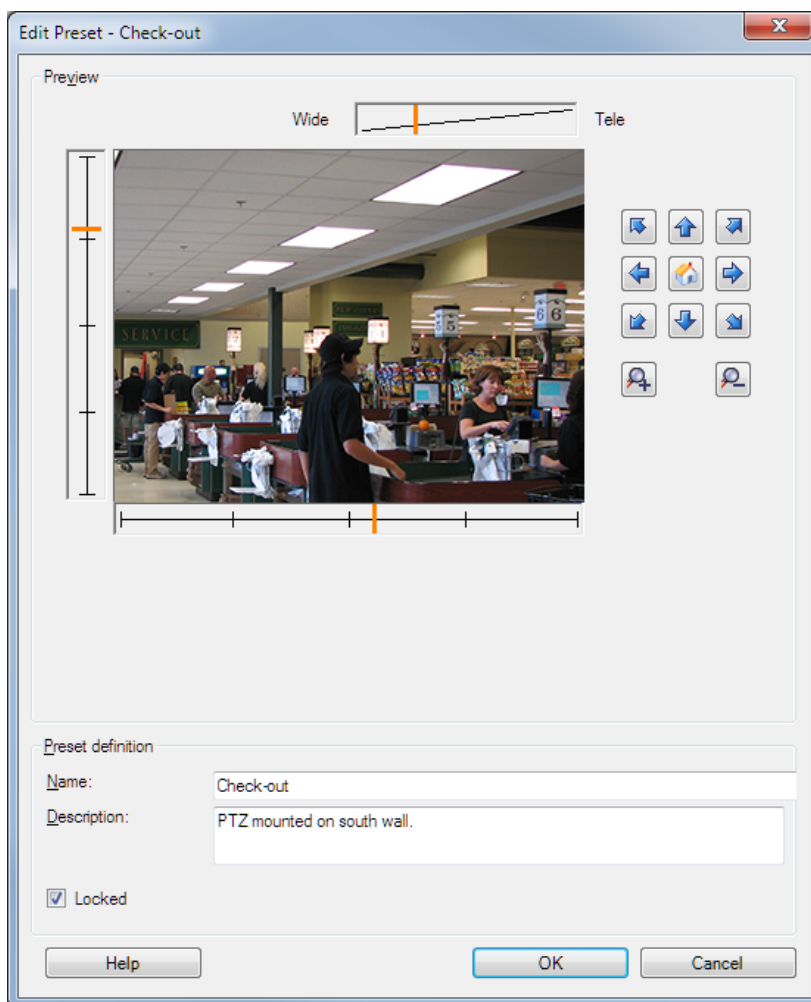
デフォルトのプリセット位置として指定できるのは、1 つだけです。

プリセット位置を編集する (タイプ 1 のみ)

システムで定義済みの既存のプリセット位置を編集する方法：

1. **プリセット**タブのカメラで利用可能なプリセット位置のリストから、プリセット位置を選択します。

2. **編集**をクリックします。これにより、**プリセットの編集**ウィンドウが開きます。



例。機能はカメラによって異なります。

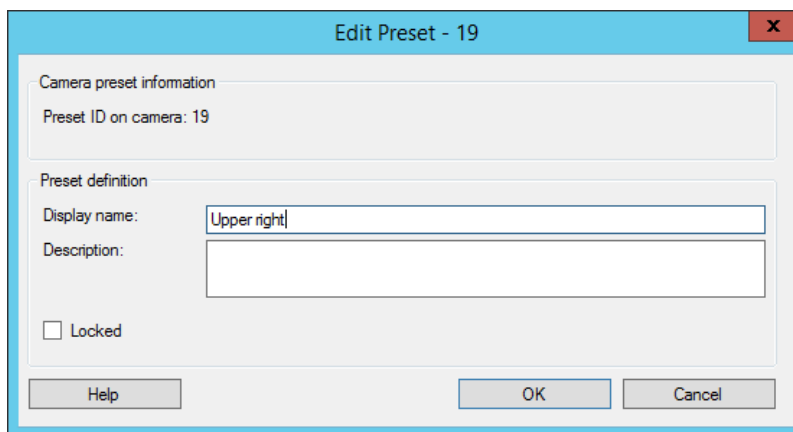
3. **【プリセットの編集】**ウィンドウにはプリセット位置からのライブビデオを表示します。ナビゲーションボタンおよび/またはスライダーを使用して、プリセット位置を必要に応じて変更します。
4. 必要に応じて、プリセット位置の名前/番号および説明を変更します。
5. プリセット位置をロックする場合は、**【ロック】**を選択します。十分な権限を持つユーザーだけが後から位置をロック解除できます。
6. **【OK】**をクリックします。

プリセット位置名の編集（タイプ 2 のみ）


カメラで定義されたプリセット位置の名前を編集するには：

1. **プリセット**タブのカメラで利用可能なプリセットのリストから、プリセット位置を選択します。


2. **編集**をクリックします。これにより、**プリセットの編集**ウィンドウが開きます。



カメラで定義されたプリセットの例

3. 必要に応じて、プリセット位置の名前を変更し、説明を追加します。
4. プリセット名をロックする場合は、**[ロック]**を選択します。Network Video Management System Smart Client のユーザーまたは制限されたセキュリティ権限のユーザーがこのプリセット名を更新またはプリセットを削除できないようにする場合は、プリセット名をロックできます。ロックされたプリセットには  アイコンが表示されます。十分な権限を持つユーザーだけが後からプリセット名をロック解除できます。
5. **[OK]**をクリックします。

プリセット位置のロック

Network Video Management System Smart Client のユーザーまたは制限されたセキュリティ権限のユーザーがこのプリセットを更新または削除できないようにする場合は、プリセット位置をロックできます。ロックされたプリセットには  アイコンが表示されます。

追加 『109ページ の"プリセット位置を追加する (タイプ 1) "参照』と編集 『111ページ の"プリセット位置を編集する (タイプ 1 のみ) "参照』の一部としてプリセットをロックします。

プリセット位置をテストする (タイプ 1 のみ)

1. **プリセット**タブのカメラで利用可能なプリセット位置のリストから、プリセット位置を選択します。
2. **実行**をクリックします。
3. カメラが選択されたプリセット位置に移動します。

PTZ セッションタイムアウトの指定

必要な権限を持つ Management Client および Network Video Management System Smart Client ユーザーは、PTZ カメラのパトロールを手動で中断できます。

定期パトロールがシステム上のすべての PTZ カメラで再開される前に経過する時間を指定できます。

1. ツール > オプションを選択します。

2. **【オプション】**ウィンドウの**【全般】**タブの次の場所で時間を選択します。

- **手動 PTZ セッションのタイムアウトリスト**（デフォルトは 15 秒）。

パトロールセッションを一時停止するタイムアウトリスト（デフォルトは 10 分）。この設定は、システムの PTZ カメラすべてに適用されます。

各カメラのタイムアウトは個別に変更できます。

1. **【サイトナビゲーション】**ペインで、**【カメラ】**をクリックします。
2. 概要ペインで、カメラを選択します。
3. **【プリセット】**タブの次の場所で時間を選択します。

- **手動 PTZ セッションのタイムアウトリスト**（デフォルトは 15 秒）。

パトロールセッションを一時停止するタイムアウトリスト（デフォルトは 10 分）。設定はこのカメラにのみ適用されます。

PTZ セッションの優先度

PTZ セッション表には、PTZ カメラの現在のステータスを示します。

名前	説明
ユーザー	【予約】 ボタンを押し、現在 PTZ カメラを制御しているユーザーを表示します。 パトロールセッションがシステムによってアクティブ化された場合は、パトロールと表示されます。
優先度	ユーザーの PTZ 優先度が表示されます。自分よりも低い優先度のユーザーからのみ PTZ セッションを取得できます。
タイムアウト	現在の PTZ セッションの残り時間が表示されます。

各 PTZ カメラの次のタイムアウトを変更できます。

名前	説明
手動 PTZ セッションのタイムアウト	タイムアウトをデフォルト期間から変える場合には、このカメラの手動 PTZ セッションのタイムアウトを指定します。 【オプション】 の下の 【ツール】 メニューでデフォルト期間を指定します。
一時停止パトロール PTZ のタイムアウト	タイムアウトをデフォルト期間から変える場合には、このカメラの一時停止パトロール PTZ セッションのタイムアウトを指定します。 【オプション】 の下の 【ツール】 メニューでデフォルト期間を指定します。

パトロールタブ(デバイス)

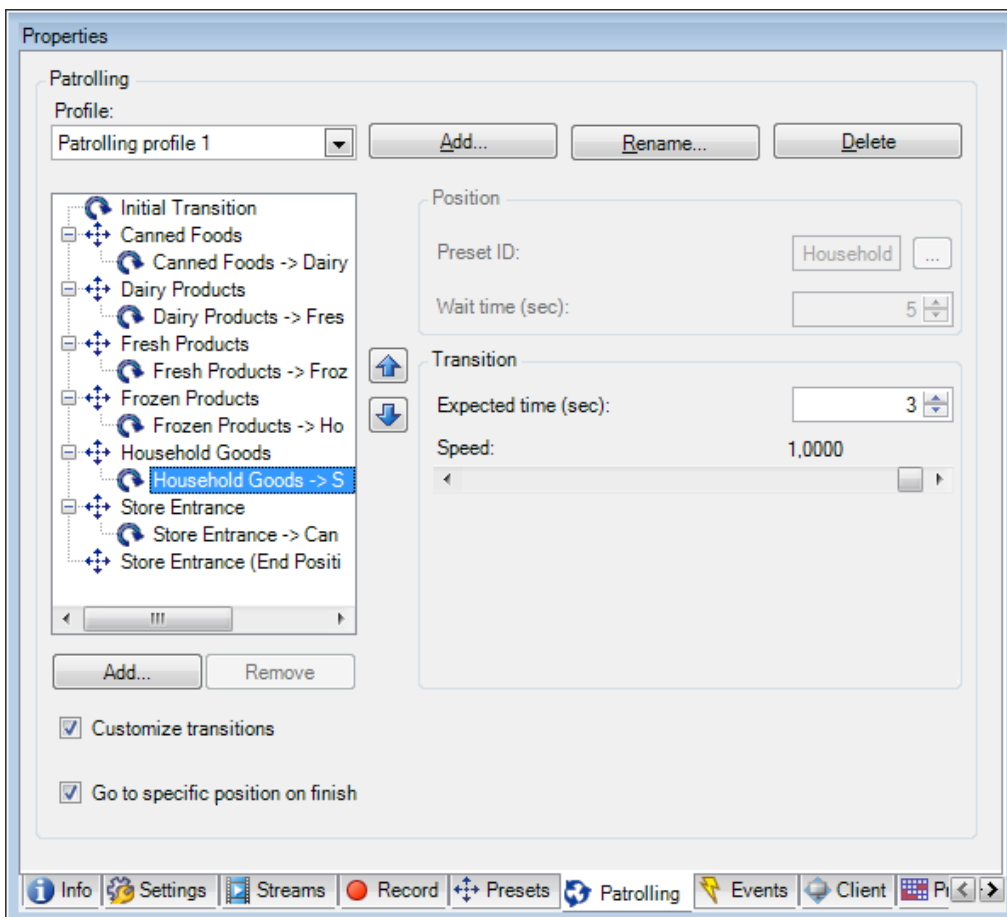
パトロールタブについて

以下のデバイスにパトロールタブがあります。

- PTZ カメラ

パトロールタブで、パトロール設定を作成して、複数のプリセット位置間での PTZ (パン/チルト/ズーム) カメラの自動的な移動を設定できます。パトロールを操作する前に、少なくとも 2 つのカメラのプリセット位置を **プリセットタブ** で指定する必要があります。

パトロール設定では、パトロールの実行方法を定義します。これには、カメラがプリセット位置間を移動する順序や、カメラが各位置に停止する時間が含まれます。作成できるパトロール設定の数に制限はなく、作成したパトロール設定はルールで使用できます。例えば、1 つのパトロール設定が日中の営業時間中に使用され、別のプロフィールが夜間に使用されるように指定するルールを作成できます。



パトロールタブ、旋回動作をカスタマイズ
を含むパトロール設定を表示

パトロール設定の追加

ルールで使用するプロファイルの追加：

1. **追加**をクリックします。**プロファイルの追加**ダイアログボックスが表示されます。
2. **プロファイルの追加**ダイアログボックスで、パトロール設定の名前を入力します。
3. **[OK]**をクリックします。名前が一意ではない場合は、ボタンは無効です。

新しいパトロール設定が**プロファイル**リストに追加されました。これで、プリセット位置とパトロール設定の他の設定を指定できます。

パトロール設定でのプリセット位置の指定

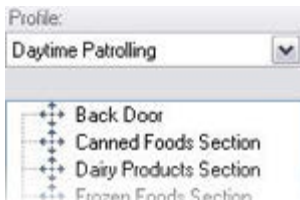
1. プロファイルリストからパトロール設定を選択します。



2. **追加**をクリックします。
3. **プリセットの選択**ダイアログで、パトロール設定のプリセット位置を選択します。



4. **OK**をクリックします。選択されたプリセット位置は、パトロール設定のプリセット位置のリストに追加されます。



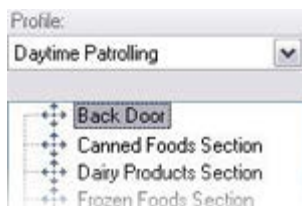
5. カメラはリストの最上位のプリセット位置を、カメラがパトロール設定に従ってパトロールを行うときの最初の停止位置として使用します。上から2番目のプリセット位置は、2番目の停止位置というようになっています。

各プリセット位置での時間を指定

パトロール時に、PTZ カメラはパトロール設定で指定された各プリセット位置にデフォルトでは5秒間とどまります。

秒数を変更するには：

1. プロファイルリストからパトロール設定を選択します。
2. 時間を変更したいプリセット位置を選択します。



3. 【位置の時間 (秒)】フィールドに任意の時間を入力します。
4. 必要に応じて、他のプリセット位置でも繰り返します。

旋回動作をカスタマイズ

デフォルトでは、あるプリセット位置から別の位置に移動するために必要な時間（**旋回動作**）は 3 秒であると推定されています。カメラがプリセット位置間を移動するときに、関係のないモーションが検知される可能性が高いため、デフォルトでは、この期間のカメラのモーション検知が無効になっています。

カメラが PTZ スキャンに対応し、設定されたプリセット位置がシステムのサーバーに保存されるタイプのカメラ（タイプ 1 PTZ カメラ）でのみ、旋回動作の速度をカスタマイズできます。それ以外のカメラでは、スピードスライダがグレイ表示になります。

以下をカスタマイズできます。

- 推定旋回動作時間。
- カメラが旋回動作中に移動するスピード。

異なるプリセット位置での旋回動作をカスタマイズする方法：

1. プロファイルリストからパトロール設定を選択します。
2. **旋回動作をカスタマイズ**チェックボックスを選択します。

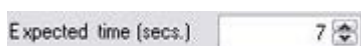


旋回動作表示がプリセット位置のリストに追加されます。

3. リストで、旋回動作を選択します。



4. 【予想時間 (秒)】フィールドに推定旋回動作時間 (秒) を入力します。



5. **スピード**スライダを使用して、旋回動作スピードを指定します。スライダが右端の位置に来ると、カメラはデフォルトのスピードで移動します。スライダを左に移動するほど、選択した旋回動作中のカメラの移動スピードが低下します。
6. 必要に応じて、他の旋回動作でも同じ操作を繰り返します。

終了位置の指定

選択したパトロール設定に基づくパトロールが終了した時点で、カメラを特定のプリセット位置に移動するように指定することができます。

1. **プロファイル**リストからパトロール設定を選択します。
2. **[終了時に特定の位置に移動]**チェックボックスを選択します。これにより、**プリセットの選択**ダイアログボックスが開きます。
3. 終了位置を選択し、**[OK]**をクリックします。

任意のカメラのプリセット位置を終了位置として指定できます。パトロール設定で使用するプリセット位置に制限はありません。

4. 選択された終了位置が**プロファイル**リストに追加されます。

選択されたパトロール設定に基づくパトロールが終了した時点で、カメラは指定された終了位置に移動します。

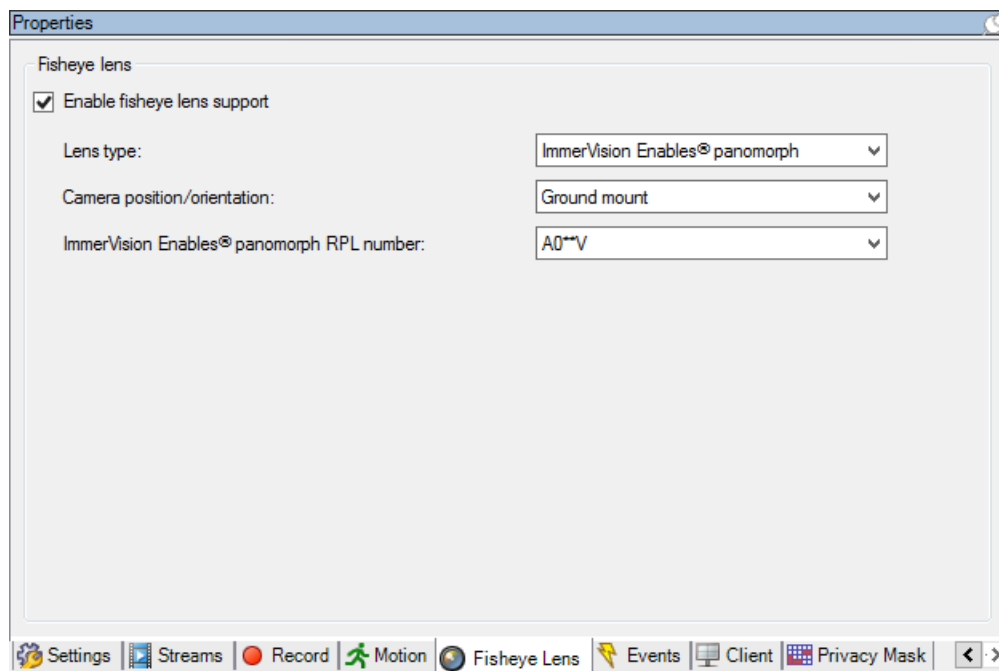
魚眼レンズタブ(デバイス)

魚眼レンズタブについて

以下のデバイスに**魚眼レンズ**タブがあります。

- 魚眼レンズを備えた固定カメラ

魚眼レンズタブでは、選択したカメラの魚眼レンズサポートを有効にして、設定することができます。



魚眼レンズサポートを有効/無効にする

魚眼レンズサポートは、既定では無効です。

有効化または無効化するには、**魚眼レンズタブの魚眼レンズサポートを有効にする**チェックボックスを選択または選択解除します。

魚眼レンズ設定の指定

魚眼レンズサポートを有効にする場合：

1. レンズのタイプを選択してください。
2. カメラ位置/方向を**カメラの位置/方向**リストから指定します。
3. **ImmerVision Enables® panomorph RPL 番号**リストで、登録済み Panomorph レンズ(RPL)番号を選択します。

これは、カメラで使用するレンズを識別し、正しく設定するためです。通常、LPR 番号はレンズ自体かカメラが入っていたボックスに記載されています。ImmerVision、Panomorph レンズおよび RPL の詳細は、ImmerVision 社の Web サイト <https://www.immervisionenables.com/> を参照してください。

イベントタブ(デバイス)

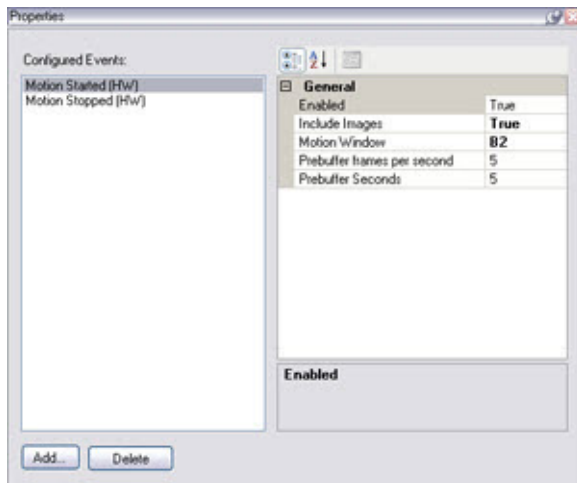
イベントタブについて

以下のデバイスにイベントタブがあります。

- カメラ

- マイク
- 入力

システムのイベントに加えて、一部のデバイスはイベントをトリガするように設定できます。これらのイベントは、システムでイベントベースのルールを作成する場合に使用できます。技術的には、これらのイベントは、監視システムではなく実際のハードウェア/デバイス上で発生します。



イベントタブ、カメラの場合の例

イベントを削除すると、イベントを使用するすべてのルールに影響を与えます。

- イベントの追加 『120ページ』
- イベントプロパティの指定 『120ページ』
- イベントに複数のインスタンスを使用する 『121ページ』

イベントの追加

1. **概要**ペインで、デバイスを選択します。
2. イベントタブを選択し、**追加**をクリックします。この操作で**ドライバーイベントの選択**ウィンドウが開きます。
3. イベントを選択します。一度に選択できるイベントは1つだけです。
4. **OK** をクリックします。
5. ツールバーで**保存**をクリックします。

イベントプロパティの指定

追加したイベントごとにプロパティを指定できます。プロパティの数は、対象となるデバイスやイベントによって異なります。目的どおりに機能するようにするには、デバイスの一部またはすべてのプロパティを、このタブと同一になるように指定する必要があります。

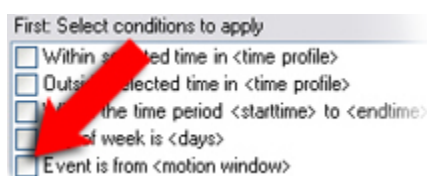
イベントに複数のインスタンスを使用する

1つのイベントに複数のインスタンスでの異なるプロパティを指定できるようにするために、複数のイベントを追加できます。

次の例は、カメラに固有です。

例：2つのモーションウィンドウ（A1、および A2）があるカメラを設定しました。モーション開始（ハードウェア）イベントの2つのインスタンスが追加されました。1つのインスタンスのプロパティで、モーションウィンドウ A1 の使用を指定しました。もう1つのインスタンスのプロパティで、モーションウィンドウ A2 の使用を指定しました。

ルールでイベントを使用する場合、イベントはルールをトリガするための特定のモーションウィンドウで検知されたモーションに基づくように指定できます。



例：
ルールの条件の一部として特定のモーションウィンドウを指定する

イベントタブ（プロパティ）

名前	詳細
設定済みイベント	設定済みイベントリストで、どのイベントを選択して追加できるかは、対象となるデバイスとその設定によって完全に決定されます。デバイスのタイプによっては、リストが空の場合もあります。
一般	プロパティのリストは、対象となるデバイスやイベントによって異なります。目的どおりに機能するようにするには、デバイスの一部またはすべてのプロパティを、このタブと同一になるように指定する必要があります。

クライアントタブ(デバイス)

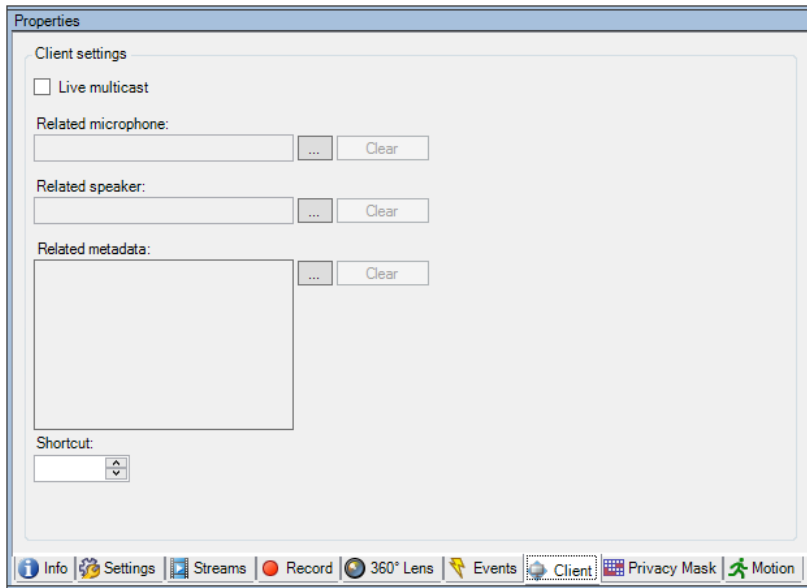
クライアントタブについて

以下のデバイスにクライアントタブがあります。

- カメラ

クライアントタブでは、Network Video Management System Smart Client でカメラを使用する際に視聴できる他のデバイスを指定できます。

カメラが録画する際に、関連するデバイスも録画します。詳細は、関連するデバイスで録画を有効にする 『104ページ』を参照してください。



クライアントタブのプロパティ

名前	詳細
ライブマルチキャスト	<p>このシステムでは、レコーディングサーバーから Network Video Management System Smart Client へのライブストリームのマルチキャストをサポートしています。選択したカメラからのライブストリームのマルチキャストを有効にするには、チェックボックスを選択します。</p> <p>レコーディングサーバーに対してもマルチキャストを設定する必要があります。マルチキャストについて 『76ページ』を参照してください。</p> <p>例えばネットワークや個別のクライアントの制限のためマルチキャストストリームが動作しない場合は、システムはユニキャストに戻ります。</p>
関連するマイク	<p>デフォルトで Network Video Management System Smart Client ユーザーがカメラのどのマイクから音声を受信するかを指定します。必要に応じて Network Video Management System Smart Client ユーザーは別のマイクを手動で選択して聴くことができます。</p> <p>カメラが録画する際に、関連するマイクが録音します。</p>
関連するスピーカー	<p>デフォルトで Network Video Management System Smart Client ユーザーがカメラのどのスピーカーで話すかを指定します。必要に応じて Network Video Management System Smart Client ユーザーは別のスピーカーを手動で選択できます。</p> <p>カメラが録画する際に、関連するスピーカーが録音します。</p>
関連するメタデータ	<p>Network Video Management System Smart Client ユーザーがデータを受信する、カメラ上のメタデータデバイスを 1 つ以上指定します。</p> <p>カメラが録画する際に、関連するメタデータ デバイスが記録します。</p>

名前	詳細
ショートカット	<p>Network Video Management System Smart Client ユーザーがカメラを簡単に選択できるように、カメラにショートカットキーを定義します。</p> <ul style="list-style-type: none"> カメラを一意に識別できるように各ショートカットを作成します。 カメラのショートカット番号は 4 桁以内である必要があります。

プライバシーマスクタブ(デバイス)

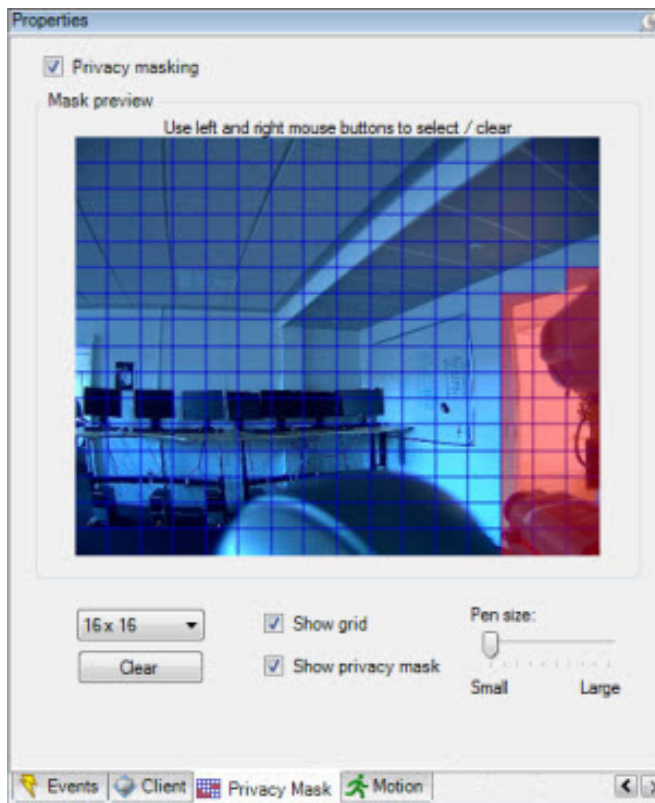
プライバシーマスクタブについて

以下のデバイスにプライバシーマスクタブがあります。

- カメラ

プライバシーマスクタブでは、選択したカメラのプライバシーマスクを有効にして設定できます。配布前に非表示にする画像の領域を定義できます。例えば、監視カメラで大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。

Network Video Management System Smart Client または他のメディアで表示する場合に、プライバシーマスクで非表示にした領域は黒く塗りつぶされ、取り除くことはできません。



赤い領域は、プライバシーマスクが適用されている領域を示します。

プライバシーマスクを PTZ カメラで使用している場合、カメラをパン/チルト/ズームしても、マスクされた領域はカメラ画像にロックされているので、選択したプライバシーマスクの適用領域はそれに合わせて移動しません。その代わりに、位置ベースのプライバシーマスクのカメラ自体への有効化をサポートする PTZ カメラもあります。

設定では、中央サイトは、リモートサイトで定義されたプライバシーマスクを無視します。同じプライバシーマスクを適用する場合は、中央サイトでもう一度定義します。

プライバシーマスクの有効化/無効化

プライバシーマスク機能は、デフォルトで無効になっています。

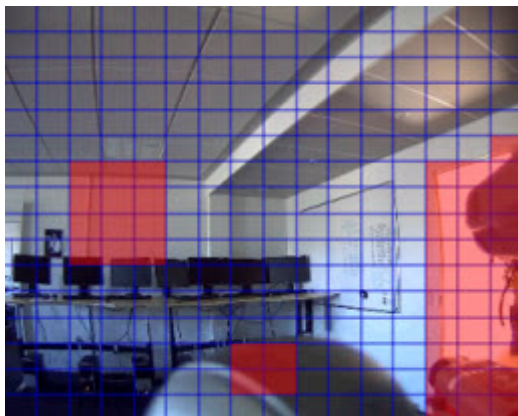
カメラのプライバシーマスク機能を有効化/無効化する方法：

- プライバシーマスクタブのプライバシーマスクチェックボックスを選択/解除します。

プライバシーマスク設定を指定する

プライバシーマスクを有効にすると、プレビュー画像が選択可能な部分にグリッドで分割されます。

1. プライバシーマスク領域を定義するには、プレビュー画像の必要な部分にマウスのポインタを乗せます。マウスの左ボタンを押下して、グリッドで区切られた部分を選択します。マウスを右クリックすると、グリッドで区切られた部分がクリアできます。
2. 必要な数のプライバシーマスク領域を定義できます。プライバシーマスク領域は赤で表示されます。



プレビューウィンドウで定義されている 3 つのプライバシーマスク領域。この場合、グリッドは表示されています。

赤のプライバシーマスク表示は、モーショントブのプレビュー画像にも表示されます。

プライバシーマスクタブ (プロパティ)

名前	詳細
グリッドサイズ	グリッドサイズリストで選択された値は、グリッドが表示されるかどうかにかかわらず、グリッドの密度を決定します。 8×8、16×16、32×32 または 64×64 から値を選択します。
グリッドを表示する	グリッドを表示チェックボックスを選択してグリッドを表示します。

名前	詳細
プライバシーマスクの表示	<p>プライバシーマスクの表示チェックボックス（デフォルト）を選択すると、選択された領域がプレビュー画像に赤色で強調表示されます。</p> <p>領域を非表示にすることで、プレビュー画像がよりはっきり見える場合があります。</p> <p>Sony では、プライバシーマスクの表示ボックスを選択した状態のままにすることを推奨しています。これは、ユーザー（またはユーザーの同僚）が領域の存在に必ず気が付くようにするためです。</p>
ペンサイズ	<p>ペンサイズスライダーを使って、領域をクリック&ドラッグで選択するサイズを示します。デフォルトでは小さく設定されており、グリッドのマス 1 つ分に相当する大きさに設定されています。</p>

モーションタブ(デバイス)

モーションタブについて

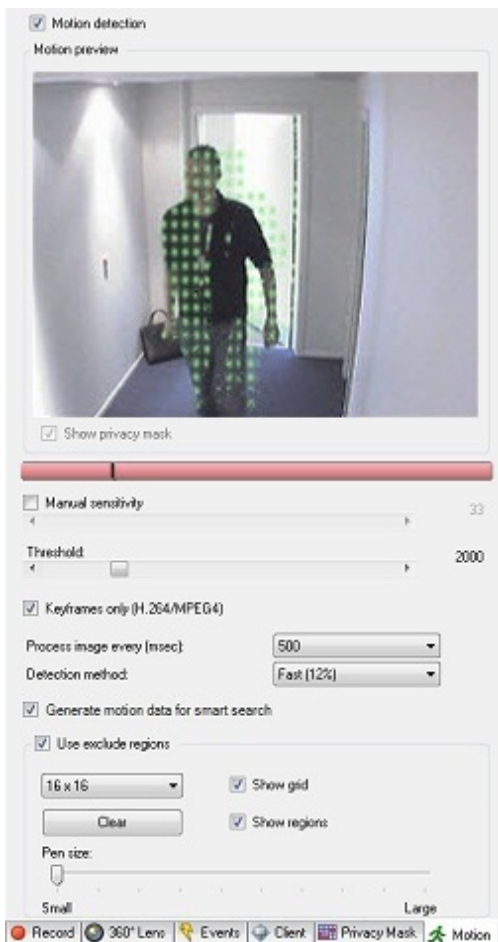
以下のデバイスにモーションタブがあります。

- カメラ

モーションタブでは、選択したカメラのモーション検知を有効にして、設定することができます。モーション検知の設定は、システムの重要な部分です。モーション検知の設定により、システムでモーションイベントを生成するタイミング、さらに通常はビデオを録画するタイミングを決定します。

それぞれのカメラに最適なモーション検知の構成が得られるようにあらかじめ調整しておくことで、後になって不必要な録画などを避けるのに役立ちます。カメラの物理的な位置によっては、異なる物理的条件（昼/夜、強風/無風など）でモーション検知の設定をテストすることをお勧めします。

カメラのモーション検知を設定する前に、Sony では、カメラの画質の設定（解像度、ビデオコーデック、ストリーム設定など）を**設定**タブで設定しておくことを強くお勧めします。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。



カメラプロパティ：モーションタブ、
モーション表示バーに赤い部分あり

カメラのグループのすべての設定を構成できますが、一般的にはカメラごとに除外領域を設定します。

- モーション検知の有効化と無効化 『126ページ』
- モーション検知設定の指定 『126ページ』

モーション検知の有効化と無効化

ツール > オプション > 一般タブで、カメラのモーション検知のデフォルト設定を指定できます。

後からカメラのモーション検知を有効化または無効化する方法：

モーションタブのモーション検知チェックボックスを選択/解除します。**重要**：カメラのモーション検知を無効にすると、カメラのモーション検知関連のルールは機能しません。

モーション検知設定の指定

カメラのビューでモーションとみなされるために必要となる変更の量を設定することができます。例えば、モーション検知分析間の間隔や、モーションが無視されるビューの領域を指定できます。

ダイナミック感度について

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。感度レベルを手動で調整するには、手動感度の有効化 『127ページ』を参照してください。

次の理由により、Sony は手動感度を有効にしないことをお勧めします。

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

手動感度の有効化

感度設定は、画像の中の**各ピクセル数**が**どれだけ**変化すればモーションと見なすかを決定します。

1. モーションタブの**手動感度**チェックボックスを選択/解除します。
2. スライダーを左に動かすと感度レベルが上がり、右に動かすと感度レベルが下がります。

感度レベルが**高くなるほど**、より少ない各ピクセルの変化でもモーションと見なされます。

感度レベルが**低くなるほど**、各ピクセルの変化がより多くなった際にモーションと見なされます。

モーションが検知されたピクセルは、プレビュー画像で緑色に強調表示されます。

3. モーションと見なされたものだけが強調表示されるよう、スライダーの位置を選択します。



プレビュー画像で強調表示されたモーション

スライダーの右側の数により、カメラ間の正確な感度設定を比較することができます。

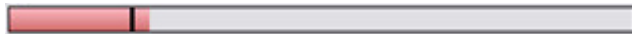
閾値の指定

モーション検知閾値は、画像の中の**ピクセル数**が**どれだけ**変化すればモーションと見なすかを決定します。

1. スライダーを左に動かすとモーションレベルが上がり、右に動かすとモーションレベルが下がります。
2. モーションと見なされたものだけが検知されるよう、スライダーの位置を選択します。

モーション表示バーの黒い垂直線はモーション検知の閾値を示します。検知されたモーションが選択された検知閾値レベルを超える場合、バーの色が緑から赤に変わり、検知されたことを示します。





モーション表示バー：閾値を超えると緑から赤に変わり、モーションが検知されたことを示します。

キーフレーム設定の選択

モーション検知をキーフレームのみで行うか、ビデオストリーム全体に行うかを決定します。MPEG-4/H.264/H.265 のみに適用されます。

キーフレームでのモーション検知により、分析の実施で使用される処理能力の消費量を減らします。

キーフレームのみにモーション検知を行う場合は、**キーフレームのみ(MPEG-4/H.264/H.265)**を選択します。

画像処理間隔を選択

システムがモーション検知分析を実施する頻度を選択できます。

画像処理間隔（ミリ秒）リストで、

間隔を選択します。例えば、1000 ミリ秒ごとは 1 秒ごとです。デフォルト値は 500 ミリ秒ごとです。ここで設定した間隔よりも実際のフレームレートが高い場合に間隔が適用されます。

検知方法の指定

画像の分析を行う範囲を限定するパーセンテージ（たとえば 25%）を指定すると、モーション検知のパフォーマンスを最適化することができます。25%の分析ということは、すべてのピクセルではなく、画像のピクセルを 4 つ毎に 1 つだけ分析することになります。

検知を最適化すると、分析を実行する際の処理能力にかかる消費量は低減できますが、モーション検知の正確性も低下することを意味しています。

- **検出方法**ドロップダウンボックスで、必要な検出方法を選択します。

スマート検索モーションデータの生成について

スマート検索モーションデータの生成が有効な場合、モーション検知で使用する画像のモーションデータが生成されます。たとえば、キーフレームでだけモーション検知を選択すると、モーションデータはキーフレームでだけ生成されます。

追加のモーションデータにより、ユーザーは、スマート検索機能を使用して、画像の選択領域のモーションに基づいて、該当する録画をすばやく検索できます。プライバシーマスクの領域では、モーションデータが生成されません。

モーション検知閾値と除外領域は、生成されたモーションデータに影響しません。

ツール > オプション > 一般タブで、カメラのスマート検索データの生成のデフォルト設定を指定できます。

領域の除外を指定

カメラのビューのうち、特定の領域のモーション検知を無効にできます。

特定の領域のモーション検知を無効にすると、例えば、カメラの撮影範囲に風で揺れる木があったり、背景に自動車が定期的に通過する場合など、無関係なモーションの検知を避けることができます。

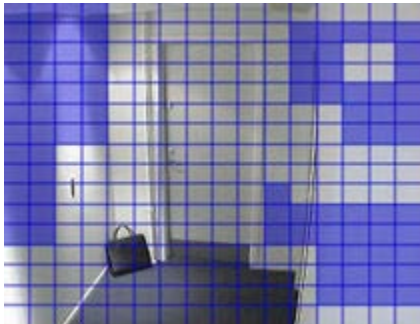
領域の除外を PTZ カメラで使用している場合、カメラをパン/チルト/ズームしても、領域は対象ではなくカメラ画像にロックされているので、除外された領域はそれに合わせて移動しません。

1. 領域の除外を使用するには、**領域の除外を使用**チェックボックスを選択します。

グリッドはプレビュー画像を選択可能なセクションに分割します。

- 領域の除外を定義するには、マウスの左ボタンを押しながら、プレビュー画像の必要なエリアをマウスのポインタでドラッグします。マウスを右クリックすると、グリッドで区切られた部分がクリアできます。

必要な数の除外領域を定義できます。除外領域は青色で表示されます。



プレビューウィンドウで定義されている3つの領域の除外。この場合、グリッドは表示されています。

青い除外領域はモーションタブのプレビュー画像にのみ表示されます。Management Client やアクセスクライアントの他のプレビュー画像では青く表示されません。

クライアント

クライアントについて

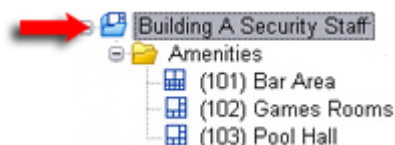
Management Client のクライアントセクションは以下で構成されています。

名前	詳細
Network Video Management System Smart Wall	Network Video Management System Smart Wall はアドオンで、ビューコンテンツを Network Video Management System Smart Client から専用ビデオウォールに送信できます。 Network Video Management System Smart Wall についての詳細は、Network Video Management System Smart Wall について『218ページ』をご覧ください。
ビューグループ	カメラからのビデオを再生する方法をビューと呼びます。Network Video Management System Smart Client を閲覧できる人を制限するために、ビューグループを作成して、論理エンティティのビューをグループ分けすることができます。これらのビューグループへのアクセス権を役割に割り当てることで、特定の役割をもつ個々のビューグループへのアクセスを制限できます。 ビューグループ を選択して、監視のニーズに合うように、ビューグループを設計して作業します。
Smart Client プロファイル	Network Video Management System Smart Client ユーザーを区別するには、Smart Client プロファイルを作成して優先度を付け、手持ちの異なるタスクでの必要に応じてプロファイルをカスタマイズできます。
Matrix	Matrix はビデオをリモートで配信する機能です。Matrix を使用すると、システムのネットワーク上の任意のカメラから、任意の Network Video Management System Smart Client にビデオを配信できます。

ビューグループ

ビューグループについて

クライアントでシステムが1つ以上のカメラからのビデオを表示する方法はビューと呼ばれます。ビューグループは、このようなビューの1つ以上の論理グループのコンテナです。クライアントでは、ビューグループは展開可能なフォルダとして表示されます。ユーザーはこのフォルダからグループを選択し、表示するビューを選択できます。



Network Video Management System Smart Client の例：矢印はビューグループを示します。ビューグループには論理グループが含まれ（アメニティと呼ばれる）、中に3つのビューが含まれます。

ビューグループと役割について

デフォルトでは、Management Client で定義する各役割は、ビューグループとしても作成されます。Management Client に役割を追加すると、デフォルトで、役割がクライアントで使用できるビューグループとして表示されます。

- ビューグループを役割に基づいて、関連する役割に割り当てられたユーザー/グループに割り当てられます。これらのビューグループの権利は、後で特定の役割に設定することで、変更することができます。
- 役割に基づくビューグループには、役割の名前が付けられます。

例：Building A Security Staff という名前の役割を作成する場合、Building A Security Staff という名前のビューグループが Network Video Management System Smart Client に表示されます。

役割を追加するときに取得するビューグループだけではなく、必要に応じて他のビューグループも作成できます。また、役割を追加するときに自動的に作成されるビューグループを含め、ビューグループを削除できます。

- 役割を追加するたびにビューグループが作成されますが、ビューグループは役割に対応する必要はありません。必要に応じてビューグループを追加し、名前を変更したり、削除できます。

ビューグループの名前を変更した場合、すでに接続済みのクライアントユーザーの場合、名前の変更が表示されるには、ログアウトしてから再度ログインする必要があります。

ビューグループの追加

1. ビューグループを右クリックして、ビューグループの追加を選択します。ビューグループの追加ダイアログボックスが開きます。
2. 新しいビューグループの名前とオプションの説明を入力し、OK をクリックします。

注意： このような権限を指定するまで、役割には新規に追加されたビューグループを使用する権限はありません。新しく追加されたビューグループを使用できる役割を指定した場合、該当する役割を持つ接続済みのクライアントユーザーは、ビューグループを使用する前に、ログアウトしてから再度ログインする必要があります。

Smart Client プロファイル

Smart Client プロファイルについて

Smart Client プロファイルを使用すると、システム管理者は Network Video Management System Smart Client の表示および動作方法、ならびに Network Video Management System Smart Client ユーザーがアクセス権限のある機能およびペインを制御できます。以下のユーザー権限を設定できます。ペインとオプション、最小化/最大化オプション、アイドル時間の制御、パスワードの記憶、ログイン後に表示されるビュー、印刷レポートのレイアウト、エクスポートパスなど。

システムで Smart Client プロファイルを管理するには、クライアントを展開して **Smart Client プロファイル** を選択します。また、Smart Client プロファイル、役割、時間プロファイルおよびこれらを同時に使用方法についての関係を説明しています。『131ページ の"Smart Client プロファイル、役割および時間プロファイルの作成および設定"参照』

Smart Client プロファイルの追加と設定

まず Smart Client プロファイルを作成してから、設定する必要があります。

1. **Smart Client プロファイル**を右クリックします。
2. **Smart Client プロファイルの追加**を選択します。
3. **Smart Client プロファイルの追加**ダイアログで、新しいプロファイルの名前と説明を入力し、**OK** をクリックします。
4. **概要**ペインで、作成したプロファイルをクリックして設定します。
5. 1つまたは複数、あるいは利用可能なすべてのタブで **OK** をクリックします。

Smart Client プロファイルのコピー

Smart Client プロファイルの設定や権限が複雑で、同様のプロファイルが必要な場合は、新しいプロファイルをゼロから作成するよりも、既存のプロファイルをコピーし、コピーしたプロファイルを少し修正の方が簡単な場合があります。

1. **Smart Client プロファイル**をクリックして、**概要**ペインのプロファイルを右クリックし、**Smart Client プロファイルのコピー**を選択します。
2. ダイアログボックスが表示されたら、コピーしたプロファイルの新しい一意の名前と説明を入力します。**OK** をクリックします。
3. **概要**ペインで、作成したプロファイルをクリックして設定します。1つまたは複数、あるいは利用可能なすべてのタブで設定の調整を行います。**OK** をクリックします。

Smart Client プロファイル、役割および時間プロファイルの作成および設定

Smart Client プロファイルで作業するときには、Smart Client プロファイル、役割、および時間プロファイルの間の関連性を理解しておくことが重要です。

- Smart Client プロファイルは Network Video Management System Smart Client のユーザー権限設定を処理します

- 役割はクライアント、MIP SDK などでのセキュリティの設定を処理します
- 時間プロファイルはこの 2 つのプロファイルタイプの時間的側面を処理します

これらの 3 つの機能を連携させることで、Network Video Management System Smart Client のユーザー権限が独自の方法で制御でき、カスタマイズが可能になります。

例 : Network Video Management System Smart Client で、通常の業務時間中（午前 8 時～午後 4 時）に限り、選択したカメラからライブビデオの表示のみ許可された（再生は不可）ユーザーを設定する必要があるとします。この場合、次の方法で設定が可能です。

1. Smart Client プロファイルを作成し、例えば**ライブ専用**などの名前を付けます。
2. **ライブ専用**に必要なライブまたは再生設定を指定します。
3. 時間プロファイルを作成し、例えば**日中専用**などの名前を付けます。
4. **日中専用**に必要な期間を指定します。
5. 新規役割を作成し、例えば**警備（選択したカメラ）**などの名前を付けます。
6. **警備（選択したカメラ）**が使用できるカメラを指定します。
7. プロファイルの**ライブ専用** Smart Client と時間プロファイルの**日中専用**を役割の**警備（選択したカメラ）**に割り当て、3 つの要素をリンクさせます。

これで、3 つの機能が統合され、必要な結果を作成し、簡単に微調整および調節ができるようになりました。さらに、役割を最初に作成して、次に Smart Client プロファイルおよび時間プロファイルを作成するなど、上記とは異なる順序を含め、その他の任意の順序で設定することができます。

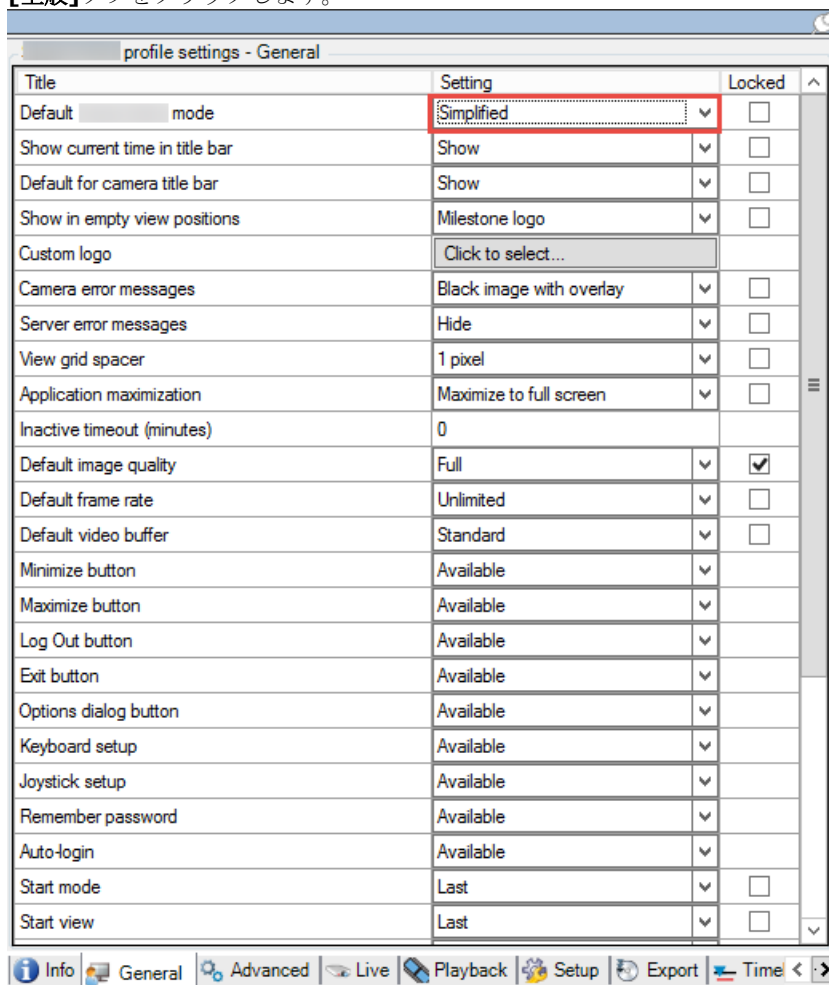
簡易モードをデフォルトモードとして設定

Smart Client プロファイルを使用すると、機能とタブが制限された簡易モードで自動的に Network Video Management System Smart Client を開くようにシステムを構成できます。デフォルトでは、Network Video Management System Smart Client は、すべての機能とタブの詳細モードで開きます。

ある時点で Network Video Management System Smart Client オペレータがデフォルトモード以外のモードに切り替えることを決めた場合、Network Video Management System Smart Client は次回オペレータがプログラムを開くときのためにこの設定を記憶します。

1. Management Client で**【クライアント】**ノードを展開します。

2. 関連する Smart Client プロファイルを選択します。
3. **[全般]** タブをクリックします。



4. デフォルト Smart Client モードリストで、**[簡易]** を選択します。ここで、Network Video Management System Smart Client は、現在の Smart Client プロファイルに関連付けられたユーザーの簡易モードで開きます。

参照

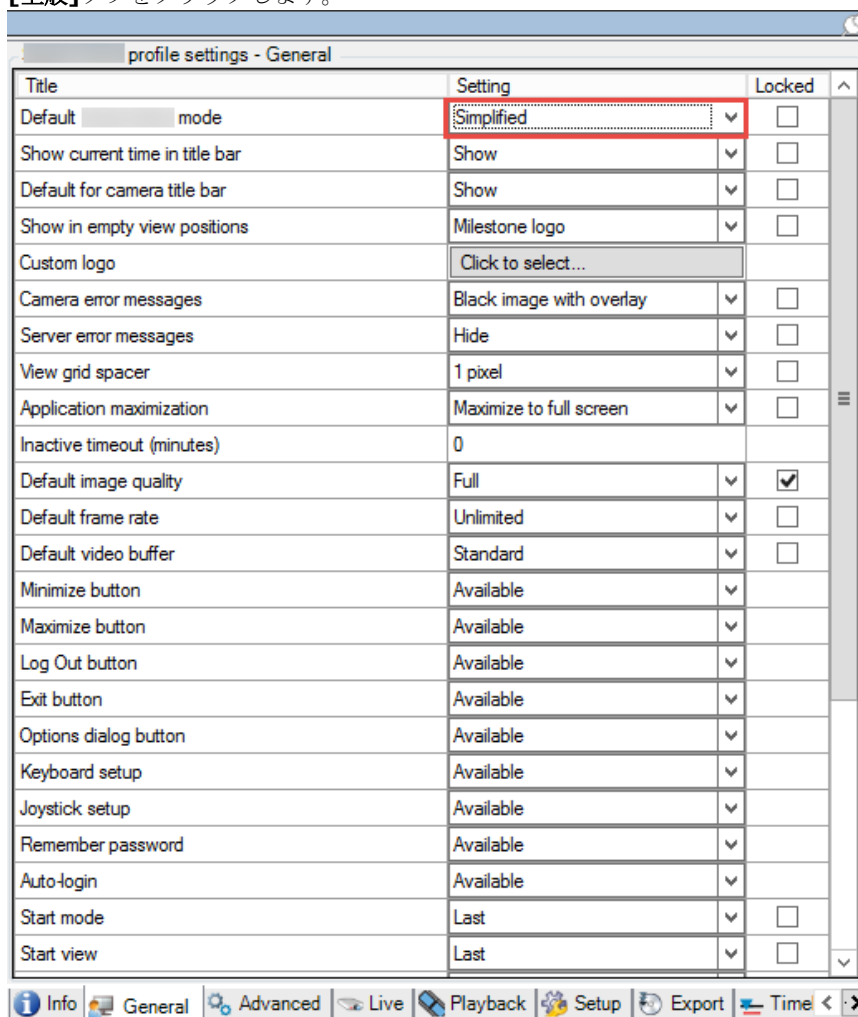
オペレータが簡易モードと詳細モードで切り替えられないようにする 『133ページ』

オペレータが簡易モードと詳細モードで切り替えられないようにする

Network Video Management System Smart Client で、オペレーターは簡易モードと詳細モードを切り替えることができます。ただし、Network Video Management System Smart Client オペレータがモードを切り替えられないようにすることができます。技術的には、Network Video Management System Smart Client が簡易モードまたは詳細モードで開くかどうかを決定する設定をロックする必要があります。

1. Management Client で**[クライアント]**ノードを展開します。

2. 関連する Smart Client プロファイルを選択します。
3. **[全般]** タブをクリックします。



4. デフォルト Smart Client モードリストに適切な値があることを確認します。有効な場合、Network Video Management System Smart Client は簡易モードで開きます。
5. **[ロック]** チェックボックスを選択します。Network Video Management System Smart Client のモード切り替えボタンが非表示になります。

参照

簡易モードをデフォルトモードとして設定 『132ページ』

Smart Client プロファイルのプロパティ

次のタブでは、各 Smart Client プロファイルのプロパティを指定できます。Network Video Management System Smart Client のユーザーが変更できないように、必要に応じて、Management Client で設定をロックできます。

タブ	説明
情報	<p>名前と説明、既存のプロファイルの優先度、プロファイルを使用する役割の概要。</p> <p>ユーザーがそれぞれに Smart Client プロファイルが割り当てられた複数の役割に属している場合、Smart Client プロファイルの取得が最優先されます。</p>
一般	<p>最小化/最大化メニュー設定の表示/非表示、ログイン/ログアウト、起動、タイムアウト、情報とメッセージングオプション、シーケンスエクスプローラ設定などの設定。</p>
詳細	<p>最大デコードスレッド、インターレースの解除、および時間帯の設定などの詳細設定。</p> <p>最大デコードスレッドは、ビデオストリームのデコードで使用されるデコードスレッドの数を制御します。これによって、ライブおよび再生モードで、マルチコアコンピュータのパフォーマンスを改善できます。実際のパフォーマンスの改善は、ビデオストリームによって異なります。この設定は、H.264/H.265 のような高度にコード化された高解像度ビデオストリームを使用している場合に主に適用されます。この場合、大幅なパフォーマンスの改善が見られる可能性があります。たとえば、JPEG または MPEG-4 などを使用している場合は効果が低くなります。</p> <p>インターレースを無効化すると、ビデオはノンインターレース形式に変換されます。インターレースは、画面で画像をどのように更新するかを決定します。まず画像の奇数ラインをスキャンして画像を更新し、次に偶数のラインをスキャンしていきます。スキャン時に処理する情報が少なくなるため、より高速のリフレッシュレートが可能になります。ただし、インターレースによってちらつきが発生したり、画像のラインの半分だけが変化する場合があります。</p>
ライブ	<p>ライブタブ/ペイン、カメラ再生、オーバーレイボタン、ブックマーク、ライブ関連の MIP プラグインの可用性。</p>
再生	<p>再生タブ/ペイン、印刷レポートのレイアウト、独立再生、境界ボックス、再生関連の MIP プラグインの可用性。</p>
設定	<p>一般設定/ペイン/ボタン、設定関連の MIP プラグインの可用性、およびマップの編集権限、ライブビデオバッファの編集権限。</p>
エクスポート	<p>パス、プライバシーマスク、ビデオおよび静止画像フォーマット、ビデオおよび静止画像のエクスポート時に含まれる内容、Network Video Management System Smart Client – Player のエクスポートフォーマットなど。</p>
タイムライン	<p>音声を含めるかどうか、時間とモーションの表示/非表示、および再生ギャップを処理する方法。</p>

Matrix

Matrix について

Matrix で、ビデオをシステムが動作しているネットワーク上のあらゆるカメラから Matrix 受信者に送信できます。Matrix 受信者は Matrix によってトリガされたビデオを表示できるコンピュータです。以下の 2 種類の Matrix 受信者があります。

- 専用の Matrix アプリケーションを実行しているコンピュータと
- Network Video Management System Smart Client を実行するコンピュータ。

Management Client で設定されている Matrix 受信者リストを表示するには、クライアントをサイトナビゲーションペインで展開して、**Matrix** を選択します。Matrix 設定のリストがプロパティペインに表示されます。

コンピュータに Matrix Monitor または Network Video Management System Smart Client のいずれがインストールされている場合でも、各 Matrix 受信者は Matrix によってトリガされたビデオを受信するように設定されていなければなりません。詳細については、Matrix Monitor および Network Video Management System Smart Client マニュアルを参照してください。

Matrix 受信者の追加

Management Client で、既存の Matrix Monitor または Network Video Management System Smart Client インストールなどに既存の Matrix 受信者を追加するには：

1. クライアントを展開し、**Matrix** を選択します。
2. **Matrix 設定**を右クリックして、**Matrix の追加**を選択します。
3. **Matrix の追加**ダイアログボックスのフィールドを入力します。
4. **アドレス**フィールドに、目的の Matrix 受信者の IP アドレスまたはホスト名を入力します。
5. **ポート**フィールドに Matrix 受信者のインストールで使用するポート番号を入力します。ポート番号とパスワードを次の方法で検索できます。Matrix Monitor アプリケーションの場合、Matrix Monitor の**設定**ダイアログボックスに移動します。Network Video Management System Smart Client については、Network Video Management System Smart Client マニュアルを参照してください。
6. **OK** をクリックします。

これで、ルールで Matrix 受信者を使用できます。

注意： システムは指定されたポート番号またはパスワードが正しいこと、または指定されたポート番号、パスワード、またはタイプが実際の Matrix 受信者に対応することを検証しません。情報を正しく入力したことを確認してください。

Matrix 受信者へのビデオ送信ルールの定義

Matrix 受信者にビデオを送信するには、関連する Matrix 受信者へのビデオ転送をトリガするルールに Matrix 受信者を含める必要があります。操作方法：

1. サイトナビゲーションペインで、**ルールとイベント > ルール**を展開します。**ルール**を右クリックし、**ルールの管理**ウィザードを開きます。手順 1 でルールタイプを選択し、手順 2 で条件を選択します。
2. **ルールの管理**の手順 3 (手順 3 : アクション) で、**[<デバイス>を表示するように Matrix を設定]**アクションを選択します。
3. 初期のルール説明の Matrix リンクをクリックします。
4. **Matrix 設定の選択**ダイアログボックスで、関連する Matrix 受信者を選択し、**[OK]**をクリックします。
5. 初期ルール説明の**デバイス**リンクをクリックし、Matrix 受信者にビデオを送信するカメラを選択して、**[OK]**をクリックして選択を確認します。
6. ルールが完了すると**終了**をクリックするか、必要に応じて別のアクションまたは終了アクションを定義します。

Matrix 受信者を削除すると、Matrix 受信者を含めるすべてのルールが動作を停止します。

同じビデオを複数の Network Video Management System Smart Client ビューに送信する

Matrix 受信者が Network Video Management System Smart Client の場合、ビューの Matrix 位置が同じポート番号とパスワードを使用していれば、同じビデオを複数の Network Video Management System Smart Client のビューに Matrix 位置を送信できます。

1. Network Video Management System Smart Client で、関連するビューと、同じポート番号とパスワードを共有する Matrix 位置を作成します。
2. Management Client で、関連する Network Video Management System Smart Client を Matrix 受信者として追加します。
3. Matrix 受信者をルールに含めることができます。

ルールとイベント

ルールとイベントについて

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

```
Perform an action on Motion Start
from Camera 2
start recording 3 seconds before on the device on which event occurred

Perform stop action on Motion End
from Camera 2
stop recording immediately
```

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

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

2つのタイプの条件によってルールがトリガされます。

名前	詳細
イベント	イベントが監視システムで発生した場合（例えば、モーションを検知した時、システムが外部センサーから入力を受信した時）。
時間	特定の時間を入力した場合（例えば、 2007年8月16日火曜日 07:00～07:59 、または毎週土曜日と日曜日。

ルールとイベントで以下の作業ができます。

- **ルール**：ルールは、システムの中心的な要素です。監視システムの動作の大半が、ルールにより決定されます。ルールを作成するときには、すべてのタイプのイベントを使用できます。
- **時間プロファイル**：時間プロファイルは、Management Client で定義する期間です。これを Management Client でルールを作成するときに使用することができます。例えば、特定のアクションが特定の時間プロファイル内に発生することを指定するルールを作成するために使用できます。
- **通知プロファイル**：通知プロファイルを使用して、事前定義された E メール通知を設定できます。この通知は、ルールによってトリガされ、例えば特定のイベントが発生したときに自動的に起動されます。
- **ユーザー定義イベント**：ユーザー定義イベントは、カスタムメイドのイベントであり、ユーザーがシステムで手動でイベントをトリガしたり、システムからの入力に応答することが可能になります。
- **アナリティックイベント**：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。アナリティックイベントはアラームの条件として使用できます。
- **ジェネリックイベント**：ジェネリックイベントでは、単純な文字列を IP ネットワーク経由でシステムに送信し、Network Video Management System イベントサーバーのアクションをトリガできます。

イベントのリストについては、イベントの概要 『145ページ の"イベント概要"参照 』を参照してください。

アクションとアクションの停止について

ルールの管理 『154ページ の"ルールの追加"参照 』ウィザードでルールを追加する場合、次のさまざまなアクションから選択できます。

First: Select actions to perform

- Start recording
- Set live frame rate on <devices>
- Set recording frame rate on <devices>

例：アクションの選択

これらのアクションの一部は、終了アクションが必要です。例：記録の開始アクションを選択する場合は、記録が開始され、無限に続く可能性があります。したがって、記録の開始アクションには、レコーディング停止という強制終了アクションがあります。

ルールの管理ウィザードでは、必要に応じて停止アクションを指定できます：

Select stop action to perform

- Stop recording
- Stop feed
- Restore default live frame rate
- Restore default recording frame rate
- Restore default recording frame rate of keyframes for H.264/MPEG4
- Resume patrolling
- Stop patrolling

終了アクションの選択。この例で、強制終了アクション（選択済み、淡色表示）、関連しない終了アクション（淡色表示）、およびオプションの終了アクション（選択可能）に注目してください。

Network Video Management System システムの各アクションのタイプについて説明されています。システムインストールがベンダー固有のプラグインなどを使用している場合には、追加のアクションを使用できる場合があります。各タイプのアクションでは、終了アクション情報も一覧表示されます。

アクション	説明
<デバイス >で記録を開始します	<p>記録を開始し、選択されたデバイスからのデータベースへのデータの保存を開始します。</p> <p>このタイプのアクションを選択すると、ルールの管理ウィザードにより、以下を指定するように指示されます。</p> <p>記録の開始時期。これは、アクションを起こすデバイス上でただちに開始されるか、またはトリガタイムインターバルを開始する/イベントをトリガする前に何秒か待ってから開始されます。</p> <p>このタイプのアクションでは、アクションがリンクされているデバイス上で記録が有効になっている必要があります。プリバッファリングが該当するデバイスで有効になっている場合のみ、イベントまたはタイムインターバルの前からデータを保存できます。記録タブで、デバイスの記録を有効にし、プリバッファリング設定を指定します。</p> <p>終了アクションが必要:このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。レコーディング停止。</p> <p>この終了アクションがない場合、記録が無制限に続く可能性があります。また、その他の終了アクションを指定することもできます。</p>

アクション	説明
<p><デバイス>で映像配信を開始します</p>	<p>デバイスからシステムにデータ供給を開始します。デバイスからの配信が開始されると、データはデバイスからシステムに転送されます。この場合、データタイプに従ってライブ表示と記録が可能です。</p> <p>このタイプのアクションを選択すると、ルールの管理ウィザードにより、配信を開始するデバイスを指定するように指示されます。システムには、配信が常にすべてのカメラで開始されることを保証するデフォルトのルールが含まれています。</p> <p>終了アクションが必要:このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。 映像配信の停止。</p> <p>また、その他の終了アクションを指定することもできます。</p> <p>強制終了アクションの映像配信の停止を使用してデバイスからの配信を停止すると、データはデバイスからシステムに転送されません。この場合、たとえば、ビデオのライブ表示と録画ができなくなります。ただし、配信を停止したデバイスは、レコーディングサーバーとの通信が維持されます。また、デバイスを手動で無効にしたときは異なり、デバイスからの配信をルールにより自動的に再開することが可能です。</p> <p>重要:このタイプのアクションにより、選択されたデバイスのデータ配信にアクセスできますが、記録設定は個別に指定する必要があるため、データが記録されることを保証するものではありません。</p>
<p><Smart Wall>を設定して<プリセット></p>	<p>Network Video Management System Smart Wall を選択したプリセットに設定します。 Smart Wall プリセットタブでプリセットを指定します。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
<p><Smart Wall> <モニター>を設定して、<<カメラ>>を表示</p>	<p>特定の Network Video Management System Smart Wall モニターに、およびこのサイトからのライブ映像を表示するように設定。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
<p><Smart Wall> <モニター>を設定して、テキスト<メッセージ>を表示</p>	<p>特定の Network Video Management System Smart Wall モニターを設定し、最大200文字のユーザー定義テキストメッセージを表示します。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
<p><<カメラ>>を<Smart Wall>モニター<monitor>から削除します</p>	<p>特定のカメラのビデオの表示を停止します。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
<p><デバイス>のライブフレームレートを設定します</p>	<p>カメラのデフォルトのフレームレートの代わりに、選択したカメラからライブビデオをシステムで表示するときに使用する特定のフレームレートを設定します。この操作は設定タブで行います。</p> <p>このタイプのアクションを選択すると、ルールの管理ウィザードにより、設定するフレームレートとデバイスを指定するように指示されます。必ず、指定するフレームレートが該当するカメラで利用できることを確認してください。</p>

アクション	説明
	<p>終了アクションが必要:このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。 デフォルトのライブフレームレートを復元します。</p> <p>この終了アクションがない場合、デフォルトのフレームレートが復元されない可能性があります。また、その他の終了アクションを指定することもできます。</p>
<p><デバイス>のレコーディングフレームレートを設定します</p>	<p>カメラのデフォルトのレコーディングフレームレートではなく、データベースの選択済みカメラから録画済みビデオを保存するときに使用する特定のフレームレートを設定します。</p> <p>このタイプのアクションを選択すると、ルールの管理ウィザードにより、設定するレコーディングフレームレートとカメラを指定するように指示されます。</p> <p>レコーディングフレームレートは、各フレームが JPEG 画像に圧縮されるビデオコーデックである JPEG でのみ指定できます。また、このタイプのアクションでは、アクションがリンクされているカメラ上で記録が有効になっている必要があります。 記録タブで、カメラの記録を有効にします。指定できる最大フレームレートは、カメラタイプおよび選択された画像の解像度によって異なります。</p> <p>終了アクションが必要:このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。 デフォルトのレコーディングフレームレートを復元します。</p> <p>この終了アクションがない場合、デフォルトのレコーディングフレームレートが復元されない可能性があります。また、その他の終了アクションを指定することもできます。</p>
<p><デバイス>のレコーディングフレームレートをすべてのフレームで MPEG4/H.264/H.265 に設定します</p>	<p>データベースで選択されたカメラから録画済みビデオを保存するときに、キーフレームだけでなく、すべてのフレームを録画するために使用するフレームレートを設定します。 記録タブで、キーフレームのみの録画機能を有効にします。</p> <p>このタイプのアクションを選択すると、ルールの管理ウィザードにより、アクションを適用するデバイスを選択するように指示されます。</p> <p>H.264/H.265 および MPEG4 のキーフレーム録画のみを有効にできます。また、このタイプのアクションでは、アクションがリンクされているカメラ上で記録が有効になっている必要があります。 記録タブで、カメラの記録を有効にします。</p> <p>終了アクションが必要:このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。</p> <p>MPEG4/H.264/H.265 のキーフレームのデフォルトのレコーディング フレームレートを復元</p> <p>この終了アクションがない場合、デフォルト設定が永久に復元されない可能性があります。また、その他の終了アクションを指定することもできます。</p>
<p>PTZ 優先度<優先度>付きの<プロファイル>を使用して<デバイス>のパトロールを開始</p>	<p>特定の優先度が設定された特定の PTZ カメラで、特定のパトロール設定に従って、PTZ パトロールを開始します。ここで、プリセット位置のシーケンス、タイミング設定などを含め、パトロールの実行方法を正確に定義します。</p> <p>このタイプのアクションを選択すると、ルールの管理ウィザードにより、パトロール設定を選択するように指示されます。1つデバイスでは1つのパトロール設定のみを選択できます。複数のパトロール設定を選択することはできません。</p> <p>このタイプのアクションでは、アクションがリンクされているデバイスが PTZ デバイ</p>

アクション	説明
	<p>スである必要があります。</p> <p>デバイスに1つ以上のパトロール設定が定義されている必要があります。パトロールタブで、PTZカメラのパトロール設定を定義します。</p> <p>終了アクションが必要:このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。</p> <p>パトロール停止</p> <p>この終了アクションがない場合、パトロールが停止しない可能性があります。また、その他の終了アクションを指定することもできます。</p>
<p><デバイス>でのパトロールの一時停止</p>	<p>PTZパトロールの一時停止このタイプのアクションを選択すると、ルールの管理ウィザードにより、パトロールを一時停止するデバイスを指定するように指示されます。</p> <p>このタイプのアクションでは、アクションがリンクされているデバイスがPTZデバイスである必要があります。</p> <p>デバイスに1つ以上のパトロール設定が定義されている必要があります。パトロールタブで、PTZカメラのパトロール設定を定義します。</p> <p>終了アクションが必要:このタイプのアクションには、1つまたは複数の終了アクションが必要です。以下の手順の1つでは、ウィザードは自動的に終了アクションの指定を求めます。 パトロールの再開</p> <p>この終了アクションがない場合、パトロールが無制限に一時停止したままになる可能性があります。また、その他の終了アクションを指定することもできます。</p>
<p><デバイス>をPTZ優先度<priority>付きの<プリセット>位置に移動</p>	<p>特定のカメラを特定のプリセット位置に移動します。ただし、必ず優先度に従います。このタイプのアクションを選択すると、ルールの管理ウィザードにより、プリセット位置を選択するように指示されます。1つのカメラで選択できるのは、1つのプリセット位置のみです。複数のプリセット位置を選択することはできません。</p> <p>このタイプのアクションでは、アクションがリンクされているデバイスがPTZデバイスである必要があります。</p> <p>このアクションでは、デバイスに1つ以上のプリセット位置が定義されている必要があります。プリセットタブで、PTZカメラのプリセット位置を定義します。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
<p>PTZ優先度<priority>付きの<デバイス>でデフォルトのプリセットに移動</p>	<p>1つ以上のカメラを該当するプリセット位置に移動します。ただし、必ず優先度に従います。このタイプのアクションを選択すると、ルールの管理ウィザードにより、アクションを適用するデバイスを選択するように指示されます。</p> <p>このタイプのアクションでは、アクションがリンクされているデバイスがPTZデバイスである必要があります。</p> <p>このアクションでは、デバイスに1つ以上のプリセット位置が定義されている必要があります。プリセットタブで、PTZカメラのプリセット位置を定義します。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>

アクション	説明
デバイス出力を<状態>に設定します	<p>デバイスの出力を特定の状態（有効化または無効化）に設定します。このタイプのアクションを選択すると、ルールの管理ウィザードにより、設定する状態とデバイスを指定するように指示されます。</p> <p>このタイプのアクションでは、アクションがリンクされるデバイスはそれぞれ、1つ以上の外部出力装置が出力ポートに接続されていなければなりません。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
ブックマークを<デバイス>に作成します	<p>選択されたデバイスからライブストリーミングまたは記録のブックマークを作成します。ブックマークを使用すると、特定のイベントまたは期間を簡単に再追跡できます。ブックマーク設定は、オプションダイアログボックスで制御されます。このタイプのアクションを選択すると、ルールの管理ウィザードにより、ブックマークの詳細を指定し、デバイスを選択するように指示されます。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
通知を<プロファイル>に送信します	<p>特定の通知プロファイルを使用して通知を送信します。このタイプのアクションを選択すると、ルールの管理ウィザードにより、通知プロファイルとプリアラーム画像を含めるデバイスを選択するように指示されます。1つの通知プロファイルのみを選択できます。複数の通知プロファイルを選択することはできません。1つの通知プロファイルには複数の受信 PC を含めることができます。</p> <p>同じイベントにさらにルールを作成したり、各通知プロファイルへ異なる通知を送信することも可能です。ルールリストのルールを右クリックすることで、ルールの内容をコピーして再利用できます。</p> <p>このタイプのアクションでは、1つ以上の通知プロファイルを設定する必要があります。画像を含むオプションが該当する通知プロファイルで有効になっている場合のみ、プリアラーム画像が含まれます。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
新しい<ログエントリ>を作成します	<p>ルールログにエントリを作成します。このタイプのアクションを選択すると、ルールの管理ウィザードにより、ログエントリのテキストを指定するように指示されます。ログテキストを指定すると、\$DeviceName\$、\$EventName\$などの変数を簡単にログメッセージに挿入できます。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
<デバイス>のプラグインを開始します	<p>1つ以上のプラグインを開始します。このタイプのアクションを選択すると、ルールの管理ウィザードにより、必要なプラグインと、プラグインを起動するデバイスを選択するように指示されます。</p> <p>このタイプのアクションでは、システムで1つ以上のプラグインがインストールされていることが必要です。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行する</p>

アクション	説明
	<p>よう指定できます。</p>
<p><デバイス >のプラグ インを停止します</p>	<p>1つ以上のプラグインを停止します。このタイプのアクションを選択すると、ルール の管理ウィザードにより、必要なプラグインと、プラグインを停止するデバイスを選択するように指示されます。</p> <p>このタイプのアクションでは、システムで1つ以上のプラグインがインストールされていることが必要です。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
<p>新しい設定を<デバイ ス >に適用します</p>	<p>1つ以上のデバイスのデバイス設定を変更します。このタイプのアクションを選択すると、ルール の管理ウィザードにより、必要なデバイスを選択するように指示され、指定したデバイス関連の設定を定義できます。</p> <p>複数のデバイスで設定を定義する場合は、指定したデバイスのすべてで使用可能な設定のみを変更できます。</p> <p>例:アクションがデバイス1およびデバイス2にリンクするように指定します。デバイス1には、設定A、B、およびCがあり、デバイス2には設定B、C、およびDがあります。この場合、両方のデバイスで使用可能な設定BおよびCのみを変更できます。</p> <p>強制停止アクションなし:このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
<p>Matrix をビュー<デバ イス >に設定します</p>	<p>選択されたカメラのビデオが、ビデオをトリガする Matrix を表示可能なコンピュータ (Network Video Management System Smart Client または Matrix Monitor アプリケーションがインストールされているコンピュータ) に表示されるようにします。</p> <p>このタイプのアクションを選択すると、ルール の管理ウィザードにより、Matrix 受信 PC と、選択された Matrix 受信 PC でビデオを表示する1つ以上のデバイスを選択するように指示されます。</p> <p>このタイプのアクションでは、Matrix 受信 PC を一度に1つのみ選択できます。選択されたデバイスのビデオを複数の Matrix 受信 PC で表示するには、各 Matrix 受信 PC のルールを作成するか、Network Video Management System Smart Wall 機能を使用する必要があります。ルールリストのルールを右クリックすることで、ルールの内容をコピーして再利用できます。このようにして、類似したルールをゼロから作成せずに済みます。</p> <p>Matrix 受信 PC 自体の設定の一部として、ユーザーは Matrix 通信に必要なポート番号とパスワードを指定する必要があります。ユーザーがこの情報にアクセスできることを確認してください。一般的に、ユーザーは許可されたホストの IP アドレス (ビデオをトリガする Matrix の表示に関するコマンドが受信されるホスト) も定義する必要があります。この場合、ユーザーは管理サーバー (または使用されるルーターまたはファイアウォール) の IP アドレスも把握していなければなりません。</p>

アクション	説明
SNMP トラップの送信	<p>選択されたデバイスのイベントを記録する小さいメッセージを作成します。SNMP トラップのテキストは自動生成されるため、カスタマイズできません。これにはソースタイプとイベントが発生したデバイス名が含まれています。</p> <p>強制停止アクションなし: このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
<デバイス>からリモートレコーディングを取得または保存します	<p>選択した（エッジ記録をサポートする）デバイスから、指定した期間の前後とトリガイベント後のリモートレコーディングを取得し保存します。</p> <p>このルールは、接続が復旧したときに自動的にリモート録画を取得する設定とは関係ありません。</p> <p>強制停止アクションなし: このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
<デバイス>から<開始時間と終了時間>の間のリモートレコーディングを取得し保存します	<p>選択されたデバイス（エッジ記録に対応するデバイス）からリモートレコーディングを取得して保存します。</p> <p>このルールは、接続が復旧したときに自動的にリモート録画を取得する設定とは関係ありません。</p> <p>強制停止アクションなし: このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
添付画像の保存	<p>画像を受信しましたイベントから画像を受信（カメラから SMTP メール経由で送信）したとき、今後使用できるように画像を保存します。今後、他のイベントでもこのアクションをトリガすることができます。</p> <p>強制停止アクションなし: このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>
<アーカイブ>のアーカイブをアクティブにします	<p>1 つ以上のアーカイブでアーカイブを開始します。このタイプのアクションを選択すると、ルールの管理ウィザードにより、必要なアーカイブを選択するように指示されます。</p> <p>強制停止アクションなし: このタイプのアクションには、停止アクションは必要ありません。イベントまたは一定期間の経過後に、オプションの停止アクションを実行するよう指定できます。</p>

イベント概要

ルールの**管理**ウィザードでイベントベースのルールを追加する場合、さまざまなイベントタイプから選択できます。概要を把握するために、現在の状況に応じて、選択可能なイベントがグループに一覧表示されます。

ハードウェア：

一部のハードウェアでは、モーション検知などのイベントをそれ自体で作成できます。これらはイベントとして使用できますが、システムで使用する前にハードウェア上に設定する必要があります。すべてのタイプのカメラ

で改ざんや温度変化を検知できるとは限らないため、一部のハードウェアで表示されているイベントのみを使用できます。

ハードウェア - 設定可能イベント：

ハードウェアから設定可能なイベントは、デバイスドライバーから自動的にインポートされます。つまり、ハードウェアによって異なるため、ここでは説明していません。設定可能イベントは、ハードウェアの**イベント**タブで設定して、システムに追加されるまでトリガされません。設定可能イベントの中には、カメラ（ハードウェア）自体を設定する必要があるものもあります。

ハードウェア - 事前定義イベント：

イベント	詳細
通信エラー（ハードウェア）	ハードウェアへの接続が失われたときに発生します。
通信が開始しました（ハードウェア）	ハードウェアとの通信が正常に確立されたときに発生します。
通信が停止しました（ハードウェア）	ハードウェアとの通信が正常に停止したときに発生します。

デバイス - 設定可能イベント：

デバイスから設定可能なイベントは、デバイスドライバーから自動的にインポートされます。つまり、デバイスによって異なるため、ここでは説明していません。設定可能イベントは、デバイスの**イベント**タブで設定して、システムに追加されるまでトリガされません。

デバイス - 事前定義イベント：

イベント	詳細
通信エラー（デバイス）	デバイスへの接続が失われたとき、およびデバイスとの通信の試みが発生し、試みが失敗したときに発生します。
通信が開始しました（デバイス）	デバイスとの通信が正常に確立されたときに発生します。
通信が停止しました（デバイス）	デバイスとの通信が正常に停止したときに発生します。
フィードオーバーフローが開始しました	<p>レコーディングサーバーが受信したデータを指定された速度で処理できず、一部の記録が強制的に破棄される場合に、映像配信のオーバーフロー（メディアのオーバーフロー）が発生します。</p> <p>サーバーが正常な場合、通常、映像配信のオーバーフローはディスク書き込み速度が遅いために発生します。書き込むデータ量を減らすか、ストレージシステムのパフォーマンスを改善することで解決できます。カメラのフレームレート、解像度、または画質を下げることで、データ書き込み量を減らすことができますが、これにより画質が落ちる場合があります。録画品質を下げたくない場合は、代わりに、追加のドライブを設置して負荷を分散するか、高速ディスクまたはコントローラを設置して、ストレージシステムのパフォーマンスを改善します。</p> <p>このイベントは、レコーディングフレームレートの低下などの問題を回避するアクションをトリガするために使用できます。</p>

イベント	詳細
フィードオーバーフローが停止しました	映像配信のオーバーフロー（フィードオーバーフローが開始しましたイベントの説明を参照）が終了したときに発生します。
ライブクライアントフィードが要求されました	<p>クライアントユーザーがデバイスからライブストリームを要求するときに発生します。</p> <p>このイベントは要求時に発生します。その後、クライアントユーザーが要求されたライブ映像配信を表示する権限がない場合や、映像配信が何らかの理由で停止した場合など、クライアントのユーザーの要求が失敗した場合にも、イベントが発生します。</p>
ライブクライアントフィードが終了しました	クライアントユーザーがデバイスからライブストリームを要求しなくなったときに発生します。
手動録画が開始されました	<p>クライアントユーザーがカメラの録画セッションを開始したときに発生します。</p> <p>イベントは、デバイスがルールアクションを通してすでに録画している場合でもトリガされます。</p>
手動録画が停止されました	<p>クライアントユーザーがカメラの録画セッションを停止したときに発生します。</p> <p>ルールシステムも録画セッションを開始した場合は、手動の録画が停止した後でも録画が続けられます。</p>
モーションが開始しました	<p>システムがカメラから受信したビデオでモーションを検知したときに発生します。</p> <p>このタイプのイベントでは、イベントがリンクされるカメラのシステムのモーション検知を有効にする必要があります。</p> <p>システムのモーション検知に加え、カメラ自体でモーションを検知して モーション開始（ハードウェア） イベントをトリガできるカメラもありますが、カメラハードウェアやシステムの設定によって異なります。上記のハードウェア - 設定可能イベントを参照してください。</p>
モーションが停止しました	<p>受信したビデオでモーションを検知しなくなったときに発生します。モーション開始イベントの説明も参照してください。</p> <p>このタイプのイベントでは、イベントがリンクされるカメラのシステムのモーション検知を有効にする必要があります。</p> <p>システムのモーション検知に加え、カメラ自体でモーションを検知して モーション停止（ハードウェア） イベントをトリガできるカメラもありますが、カメラハードウェアやシステムの設定によって異なります。上記のハードウェア - 設定可能イベントを参照してください。</p>
出力がアクティブになりました	<p>デバイスの外部出力ポートが有効になったときに発生します。</p> <p>このタイプのイベントでは、システムの1つ以上のデバイスが出力ポートに対応している必要があります。</p>

イベント	詳細
出力が変更されました	デバイスの外部出力ポートの状態が変更されたときに発生します。 このタイプのイベントでは、システムの1つ以上のデバイスが出力ポートに対応している必要があります。
出力が無効になりました	デバイスの外部出力ポートが無効になったときに発生します。 このタイプのイベントでは、システムの1つ以上のデバイスが出力ポートに対応している必要があります。
PTZ 手動セッションを開始しました	(スケジュール済みパトロールまたはイベントによる自動トリガに基づくPTZセッションとは異なり、) 手動で操作したPTZセッションがカメラで開始されたときに発生します。 このタイプのイベントでは、イベントがリンクされているカメラがPTZカメラである必要があります。
PTZ 手動セッションを中止しました	(スケジュール済みパトロールまたはイベントによる自動トリガに基づくPTZセッションとは異なり、) 手動で操作したPTZセッションがカメラで停止されたときに発生します。 このタイプのイベントでは、イベントがリンクされているカメラがPTZカメラである必要があります。
記録が開始しました	記録が開始したときに発生します。手動の記録が開始された場合は、別のイベントが発生します。
記録を中止しました	記録が停止したときに発生します。手動の記録が停止された場合は、別のイベントが発生します。
設定が変更されました	デバイスの設定が正常に変更されたときに発生します。
設定の変更エラー	デバイスの設定変更が試みられ、試みが失敗したときに発生します。

外部イベント - 事前定義イベント :

イベント	詳細
記録の開始を要求	記録の開始が MIP ソフトウェア開発キット (SDK) 経由で要求されたときに有効になります。 MIP ソフトウェア開発キット (SDK) によって、サードパーティーのベンダーは、お使いのシステム用のカスタムプラグイン (たとえば、外部アクセスコントロールシステムまたは同様の機能など) の統合を開発できます。

イベント	詳細
記録の停止を要求	記録の停止が MIP SDK 経由で要求されたときに有効になります。 MIP ソフトウェア開発キット(SDK)によって、サードパーティーのベンダーは、お使いのシステム用のカスタムプラグイン（たとえば、外部アクセスコントロールシステムまたは同様の機能などとの統合）を開発できます。

外部イベント - ジェネリックイベント：

ジェネリックイベントでは、シンプルな文字列を IP ネットワーク経由でシステムに送信し、システムのアクションをトリガできます。ジェネリックイベントの目的は、可能な限り多くの外部ソースがシステムと相互作用できるようにすることです。

外部イベント - ユーザー定義イベント：

各システムに合うようカスタムメイドしたイベントも選択することができます。このようなユーザー定義イベントは、以下で使用できます。

- クライアントユーザーが手動でイベントをトリガしながら、クライアントのライブビデオを視聴できるようにする。
- その他多数の目的。たとえば、特定のデータタイプをデバイスから受信したときに発生するユーザー定義イベントを作成することができます。

詳細についてはユーザー定義イベントについて 『163ページ』を参照してください。

レコーディングサーバー：

イベント	詳細
アーカイブが使用できます	レコーディングサーバーのアーカイブが、使用できなくなってから再び使用できるようになると発生します（ アーカイブが使用できません 参照）。
アーカイブが使用できません	ネットワークドライブにあるアーカイブへの接続が失われた場合など、レコーディングサーバーのアーカイブが使用できなくなったときに発生します。このような場合、記録をアーカイブできません。 イベントを使って、Eメール通知が自動的に組織内の関連するスタッフに送信されるようにするために、アラームまたは通知プロファイルをトリガすることができます。
アーカイブが終了していません	次の予定が開始する際、最後のアーカイブラウンドでレコーディングサーバーのアーカイブが終了していないときに発生します。

イベント	詳細
データベースディスクが一杯です	<p>データベースディスクが一杯のときに発生します。データベースディスクは、ディスクの残り容量が 5GB 未満になると一杯とみなされます。</p> <p>空き容量が 5GB 未満になった場合、データベースで最も古いデータは必ず自動アーカイブされます（または、次のアーカイブが定義されていない場合は削除されます）。空き容量が 1GB 未満になった場合は、次のアーカイブが定義されている場合でも、データは削除されます。データベースには、必ず 250MB の空き容量が必要です。この制限に達した場合（データが十分速やかに削除されていない場合）、十分な空き容量が確保されるまで、それ以上データベースにはデータが書き込まれません。このため、データベースの実際の最大サイズは、指定したギガバイト数より 5GB 少なくなります。</p>
データベースが一杯です - 自動アーカイブ中	レコーディングサーバーのアーカイブが一杯になり、ストレージのアーカイブに自動アーカイブする必要があるときに発生します。
データベースの修復	データベースが破損した場合に発生します。その場合、システムは自動的に以下の 2 つのデータベース修復方法を試行します。高速修復および徹底的な修復。
データベースストレージが使用できません	<p>レコーディングサーバーのストレージが、使用できなくなってから再び使用できるようになると発生します（データベースのストレージエリアが使用できませんを参照）。</p> <p>例えば、データベースのストレージが使用できませんイベントにより停止された場合、このイベントを使って録画を開始することができます。</p>
データベースストレージが使用できません	<p>ネットワークドライブにあるストレージへの接続が失われた場合など、レコーディングサーバーのストレージが使用できなくなったときに発生します。このような場合、記録をアーカイブできません。</p> <p>イベントを使って、E メール通知が自動的に組織内の関連する人に送信されるようにするために、録画を停止して通知プロファイルまたはアラームをトリガできます。</p>

アドオン製品および統合からのイベント：

たとえば、ルールシステムでは、アドオン製品および統合からのイベントを使用できます。

- アナリティックイベントは、ルールシステムでも使用できます。

ルール

ルールについて

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

以下はルールでできることの例です。

- 録画を開始および停止する

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

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

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

デフォルトルールについて

システムには多くのデフォルトルールが設定されており、何も設定しなくても基本的な機能が使用できます。必要に応じてデフォルトルールを無効化または修正できます。デフォルトルールを修正または無効化すると、システムが希望通りに動作しなくなる場合があります。また、映像または音声のシステムへの自動配信が保証されなくなる場合があります。

デフォルトルール	詳細
PTZ が完了したときにプリセットへ移動する	PTZ カメラを手動で操作した後、各デフォルトのプリセット位置に移動することを確認します。このルールはデフォルトでは無効になっています。 ルールを有効にした場合でも、ルールが動作するには、関連する PTZ カメラでデフォルトプリセット位置を定義する必要があります。この操作は プリセット タブで行います。

デフォルトルール	詳細
モーション記録	<p>カメラでモーションが検知される限り、関連するカメラの記録が有効になっていれば、ビデオが録画されることを確認します。デフォルトでは記録は有効になっています。</p> <p>デフォルトルールでは、検知されたモーションに基づいて記録を指定しますが、1つ以上のカメラで個々のカメラの記録が無効になっている場合には、システムがビデオを記録することを保証するものではありません。記録が有効になっている場合でも、記録の品質は個々のカメラの記録設定の影響を受ける場合があることに留意してください。</p>
リクエスト記録	<p>関連するカメラの録画が有効になっていることを前提条件として、外部リクエストが発生するとビデオの録画が自動的に開始されることを確認します。デフォルトでは録画が有効になっています。</p> <p>リクエストは、常にお使いのシステムに外部的に統合されているシステムによってトリガされます。また、ルールは主に外部システムまたはプラグインのインテグレータによって使用されます。</p>
音声配信開始	<p>すべての接続済みマイクとスピーカーからの音声配信がシステムに自動配信されることを保証します。</p> <p>このデフォルトルールにより、システムのインストール時に接続されたマイクとスピーカーの音声配信に即時にアクセスできます。ただし、記録設定は個別に指定する必要があるため、音声記録されることを保証するものではありません。</p>
配信開始	<p>すべての接続済みカメラからの映像配信がシステムに自動配信されることを保証します。</p> <p>このデフォルトルールにより、システムのインストール時に接続されたカメラの映像配信に即時にアクセスできます。ただし、カメラの記録設定は個別に指定する必要があるため、ビデオが録画されることを保証するものではありません。</p>
メタデータ配信開始	<p>すべての接続済みカメラからのデータ配信がシステムに自動配信されることを保証します。</p> <p>このデフォルトルールにより、システムのインストール時に接続されたカメラのデータ配信に即時にアクセスできます。ただし、カメラの記録設定は個別に指定する必要があるため、データが記録されることを保証するものではありません。</p>

デフォルトルールの再作成

誤ってデフォルトのルールを削除した場合には、次の内容を入力することで再作成できます。

デフォルトルール	入力するテキスト
PTZ が完了したときにプリセットへ移動する	<p>すべてのカメラから PTZ 手動セッションを中止したときにアクションを実行します。</p> <p>イベントが発生したデバイスでデフォルトのプリセットに即時に移動します。</p>

デフォルトルール	入力するテキスト
モーション記録	モーション時にすべてのカメラからの開始アクションを実行すると、イベントが発生したデバイスで3秒前から記録を開始します。 モーション時にすべてのカメラからの終了アクションを実行すると、3秒後に記録が停止します。
リクエスト記録	外部からの録画開始リクエスト時にアクションを実行すると、メタデータからデバイスの録画をただちに開始します。 外部から記録の停止を要求した際に停止アクションを実行し、録画がただちに停止されます。
音声配信開始	アクションをある時間間隔で実行し、常にすべてのマイク、すべてのスピーカーで配信を開始します。 時間間隔が終了すると、アクションを実行し、配信をただちに停止します。
配信開始	アクションをある時間間隔で実行し、常にすべてのカメラで映像配信を開始します。 時間間隔が終了すると、アクションを実行し、配信をただちに停止します。
メタデータ配信開始	アクションをある時間間隔で実行し、常にすべてのメタデータで映像配信を開始します。 時間間隔が終了すると、アクションを実行し、配信をただちに停止します。

ルールの検証について

個々のルールまたはすべてのルールの内容を一度に検証することができます。ルールを作成したら、**ルールの管理**ウィザードで、すべてのルールの要素が矛盾していないか確認します。ルールが一定期間存在し、1つまたは複数のルールの要素が他の構成により影響を受けた場合、ルールが機能しなくなる場合があります。例えば、ルールが特定の時間プロファイルでトリガされた場合、その時間プロファイルが後で削除されるか、権限がなくなると、ルールは機能しなくなります。このような構成上の意図せぬ影響については、確認が困難です。

ルール検証は、どのルールが影響を受けたのかを確認するのに役立ちます。検証はルールごとに行われ、各ルールは個別に検証されます。**すべてのルールの検証**機能を使用しても、互いにルールを検証することはできません（例えば、あるルールが別のルールと矛盾するかを確認する場合など）。

ルール外の前提要件の構成が、ルールの機能を妨害するかどうかを検証することはできない点に留意してください。例えば、関連するカメラでモーションが検知されたときに録画を開始するというルールでは、そのカメラでモーション検知（ルールではなくカメラレベルで有効になっている）が有効になっていなくても、ルールの要素自体が正しいければ、検証結果はOKになります。

個々のルールまたはすべてのルールを一度に検証することができます。検証したいルールを右クリックして、**ルールの検証**または**すべてのルールの検証**を選択します。ダイアログボックスが表示され、ルールが正常に検証されたかどうかを示します。ルールが正常に検証されなかった場合、影響を受けたルールがダイアログボックスに表示されます。



Rule validated.



All rules validated.



Rule did not validate.



Rules that did not validate:
- My first rule

ルールの複雑性について

正確なオプション数は、作成するルールのタイプ、およびシステムで使用できるデバイス数により異なります。ルールは非常に高い柔軟性を持っています。イベントと時間条件を組み合わせたり、複数のアクションを1つのルールに指定したり、システムを構成する複数またはすべてのデバイスをカバーするルールを作成することができます。

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

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

組織の要件に応じて異なりますが、複雑なルールを作成するよりも、単純なルールを複数作成することを推奨します。これにより、システムに多数のルールが存在することになったとしても、何を実行するルールであるかについての概要を簡単に管理することができます。ルールを単純に保つことで、個別のルール要素を無効/有効にするときに、柔軟性の高い対応が可能になります。単純なルールであれば、必要に応じてすべてのルールを無効/有効にできます。

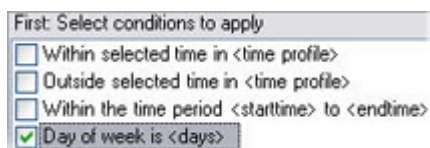
ルールの追加

ルールを作成する際に、関連するオプションを提供する**ルールの管理**ウィザードが表示されます。

ルールに必要な要素が欠如しないようにサポートします。ルールに基づき、ウィザードが自動的に適切な停止アクション (ルールが適用されなくなった後の動作) を提案するため、終わりのないルールを誤って作成することを防止します。

1. **ルール** アイテム > **ルールの追加**を右クリックします。**ルールの管理**ウィザードが開きます。ウィザードに従って、ルールの内容を指定します。
2. 新規ルールの名前と説明を**名前**と**説明**フィールドでそれぞれ指定します。
3. ルールに関連する条件タイプを選択します。特定のイベントが発生したときにアクションを実行するルールか、特定の時間を入力するとアクションを実行するルールのいずれかになります。

4. **次へ**をクリックしてウィザードの手順 2 に進みます。ウィザードの第 2 ステップで、ルールの詳細条件を定義します。
5. 1 つまたは複数の条件を選択します。例：曜日は<日>です。



例。ユーザーのニーズによって選択は異なります。

選択に応じて、ウィザードウィンドウの下側で、ルールの説明を編集します。



例。ユーザーのニーズによって選択は異なります。

太字斜体の下線付き項目をクリックして、正確な内容を指定します。例えば、**日**リンクをクリックすると、ルールが適用される曜日を選択することができます。

6. 正確な条件を指定したら、ウィザードの**次へ**をクリックし、次のステップに進み、ルールでカバーするアクションを選択します。ルールの内容と複雑性に応じ、停止イベントや停止アクション等、より多くのステップを定義する必要がある場合があります。例えば、ある時間で(例、木曜日の 08:00 から 10:30)デバイスが特定のアクションを実行するようルールを指定した場合、期間終了時に何が起こるかを指定するようウィザードから指示されます。
7. ユーザーのルールを作成した時点で条件が満たされる場合は、デフォルトでルールがアクティブになります。ルールをすぐに適用したくない場合、**アクティブ**チェックボックスを外します。
8. **終了**をクリックします。

ルールを編集、コピー、名前を変更する

1. **概要**ペインで、関連するルールを右クリックします。
2. 以下のいずれかを選択します。

ルールの**編集**または**ルールのコピー**または**ルールの名前変更**。ルールの**管理**ウィザードが開きます。

3. ウィザードで、名前を変更するか、ルールを変更します。**ルールのコピー**を選択した場合、ウィザードが開き、選択したルールのコピーが表示されます。
4. **終了**をクリックします。

ルールを無効/有効にする

ルールの条件が適用され、ルールがアクティブになると、システムはすぐにルールを適用します。ルールをアクティブにしたい場合、ルールを無効にすることができます。ルールを無効にすると、ルールの条件が満たされても、システムではルールが適用されません。ルールを無効にした場合も、後で簡単にルールを有効にすることができます。

ルールを無効にする

1. **概要**ペインで、ルールを選択します。
2. **プロパティ**ペインで**アクティブ**チェックボックスを外します。
3. ツールバーの**保存**をクリックします。
4. 赤色の x のついたアイコンは、ルールが**ルール**リストで無効化されたことを示します。



例：アイコンに x が追加されており、3 番目のルールが無効化されたことを示します。

ルールを有効にする

ルールをもう一度有効にしたい場合は、ルールを選択し、**アクティブ**チェックボックスを選択して、設定を保存します。

時間プロファイル

時間プロファイルについて

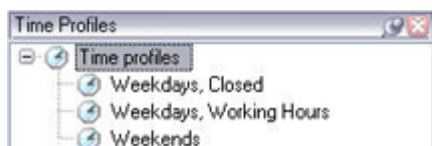
時間プロファイルは、管理者が定義する期間です。時間プロファイルは、ルールを作成するときに使用することができます。例えば、特定のアクションが特定の期間内に発生することを指定するルールを作成するときに使用できます。

時間プロファイルは、**Smart Client** プロファイルだけでなく、役割にも割り当てられます。デフォルトでは、すべての役割はデフォルトの時間プロファイルである**常時**に割り当てられます。これは、デフォルトの時間プロファイルによる役割メンバーは、システムのユーザー権限で、時間ベースの制限がないことを意味します。別の時間プロファイルを役割に割り当てることも可能です。

時間プロファイルは非常に柔軟です。1 回または複数の期間をベースにすることも、何度も発生させることも可能です。1 回と複数回を組み合わせることも可能です。ユーザーの皆様が多くが、**Microsoft® Outlook** などのカレンダーアプリケーションで、1 回および複数回の期間の概念について理解していることでしょう。

時間プロファイルは現地時間で必ず適用されます。つまり、お持ちのシステムが異なる時間ゾーンにレコーディングサーバーを設置している場合、時間プロファイルに関連するアクション（カメラの録画等）は、各レコーディングサーバーの現地時間に基づき実行されます。例：08:30~09:30 の時間をカバーする時間プロファイルを使用する場合、ニューヨークに設置したレコーディングサーバーのアクションは、現地時間 08:30~09:30 に実行され、ロサンゼルスに設置したサーバーは、ロサンゼルスの現地時間が 08:30~09:30 になったときに遅れて実行されます。

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



例

時間プロファイルの代わりとして、日の長さの時間プロファイル 『159ページ の"日の長さの時間プロファイルについて"参照』を参照してください。

時間プロファイルの指定

1. 時間プロファイルリストで、**時間プロファイル > 時間プロファイルの追加**をクリックします。これにより、**時間プロファイル**ウィンドウが開きます。
2. **時間プロファイル**ウィンドウで、**名前**フィールドに新しい時間プロファイルの名前を入力します。オプションとして、新しい時間プロファイルの説明を**説明**フィールドに入力できます。
3. **時間プロファイル**ウィンドウのカレンダーで、**日ビュー**、**週ビュー**または**月ビュー**を選択してから、カレンダーの内側を右クリックして、**1つの時間を追加**または**繰り返し時間を追加**を選択します。
4. 時間プロファイルの必要な時間を指定したら、**時間プロファイル**ウィンドウの**OK**をクリックします。システムが、新規時間プロファイルを**時間プロファイル**リストに追加します。後で時間プロファイルを編集または削除したい場合、**時間プロファイル**リストからも行うことができます。

1つの時間を追加

1つの時間を追加を選択すると、**時間の選択**ウィンドウが表示されます。

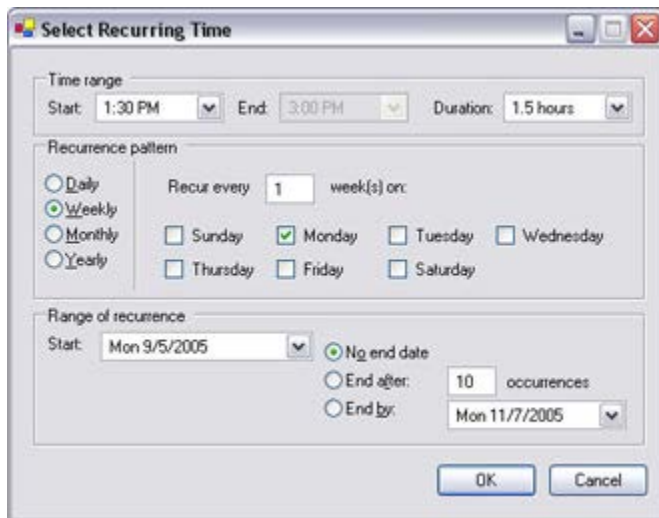


時刻と日付のフォーマットは、使用しているシステムの設定によって異なります。

1. **時間の選択**ウィンドウで、**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。
2. **OK**をクリックします。

繰り返し時間の指定

繰り返し時間を追加を選択すると、繰り返し時間の選択ウィンドウが表示されます。



時刻と日付のフォーマットは、使用しているシステムの設定によって異なります。

1. 時間の選択ウィンドウで、時間範囲、繰り返しパターン、および繰り返し範囲を指定します。
2. **OK** をクリックします。

時間プロファイルには、複数の期間を含めることができます。時間プロファイルに、さらに期間を含めたい場合は、1つの時間または繰り返し時間を追加します。

時間プロファイルの編集

1. 概要ペインの時間プロファイルリストで、関連する時間プロファイルを右クリックし、**時間プロファイルの編集**を選択します。これにより、時間プロファイルウィンドウが開きます。
2. 必要に応じて時間プロファイルを編集します。時間プロファイルに変更を加えたら、時間プロファイルウィンドウの **OK** をクリックします。時間プロファイルリストに戻ります。



小さい戻る/次へボタンをクリックすると、前後の月に移動します。

注意：時間プロファイルの情報ウィンドウで、必要に応じて時間プロファイルを編集できます。時間プロファイルには1つ以上の期間が含まれ、期間が繰り返される場合があります。右上端の小さい月概要には、時間プロファイルが対応する期間の概要が簡単に表示されます。指定された時間を含む日付が太字で強調表示されます。

この例では、太字の日付は、期間が複数の日付で指定され、月曜日に繰り返し時間が指定されていることを示します。

日の長さの時間プロファイルについて

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

このような状況では、日の長さの時間プロファイルを作成して、特定の地勢条件での日の出と日没を定義することができます。GPS 座標から、システムが毎日の日の出時間と日没時間を計算し、さらに夏時間調整も行います。その結果、時間プロファイルが選択した場所の日の出/日没の年間の変化を自動的に追跡し、必要な時だけプロファイルが有効になるようにします。日時はすべて管理サーバーの日時設定に基づきます。また、開始時間（日の出）と終了時間（日没）のプラスまたはマイナスオフセット（分）を設定することも可能です。開始と終了のオフセットは、同一または別にするすることができます。

日の長さの時間プロファイルは、ルールと役割の両方を作成するときに使用できます。

日の長さの時間プロファイルの作成

1. ルールとイベントフォルダ > 時間プロファイルを展開します。
2. 時間プロファイルリストで、時間プロファイルを右クリックし、日の長さの時間プロファイルの追加を選択します。
3. 日の長さの時間プロファイルウィンドウで、必要な情報を入力します。明るくなったり暗くなったりする間の移行期間に対処するために、プロファイルの有効/無効をオフセットすることが可能です。さらに、コンピュータの言語/地域設定で使用している言語で、時間と月が表示されます。
4. 地図で GPS 座標の位置を確認するには、ブラウザの位置を表示をクリックします。これによりブラウザが開いて位置を確認できます。
5. **OK** をクリックします。

日の長さの時間プロファイルのプロパティ

日の長さの時間プロファイルに以下のプロパティを設定します。

名前	詳細
名前	プロファイルの名前。
詳細	プロファイルの説明です（任意）。
GPS 座標	プロファイルに割り当てられたカメラの物理的位置を表示する GPS 座標です。
日の出オフセット	日の出によりプロファイルの作動がオフセットされる分数です（+/-）。
日没オフセット	日没によりプロファイルの無効化がオフセットされる分数です（+/-）。
時間ゾーン	カメラの物理的位置を示す時間帯です。

通知プロフィール

通知プロフィールについて

通知プロフィールにより、事前定義された E メール通知を設定できます。この通知は、ルールによってトリガされ、例えば特定のイベントが発生したときに自動的に起動されます。静止画像と AVI ビデオクリップを E メール通知に添付することができます。

このシステムでは、TLS（トランスポートレイヤーセキュリティ）とその前に使われていた SSL（セキュアソケットレイヤー）はサポートされていません。送信者が TLS または SSL を使用するサーバーに属している場合は、E メール通知は適切に動作しません。また、E メールスキャナがある場合、E メールによる通知を送信するアプリケーションを妨害する可能性があるため、これを無効にする必要があります。

前提条件

通知プロフィールを作成する前に、E メール通知の送信 SMTP メールサーバー設定を指定する必要があります。

E メール通知に AVI ムービークリップを含めるには、使用する圧縮設定も指定する必要があります。指定するには、**ツール > オプション**に進みます。これにより、**オプションウィンドウ**が開きます。**送信 SMTP メールサーバー**をメールサーバータブで指定し、圧縮設定を **AVI 生成**タブで指定します。

通知プロフィールの追加

1. **ルールとイベント**を展開し、**通知プロフィール > 通知プロフィールの追加**を右クリックします。これにより、**通知プロフィールの追加**ウィザードが開きます。
2. 名前と説明を指定します。**次へ**をクリックします。

3. 受信者、件名、本文、Eメール間の時間を指定します。

4. テストの E メール通知を指定の受信者に送信したい場合は、**Eメールのテスト**をクリックします。
5. 静止画像を添付したい場合、**画像を含める**を選択して、画像数、画像間の時間、画像を E メールに埋め込むか否かを指定します。
6. AVI ビデオクリップを含めるには、**AVI を含める**を選択し、イベント前後の時間とフレームレートを指定してください。
7. **終了**をクリックします。

Eメール通知をトリガするルールを使用する

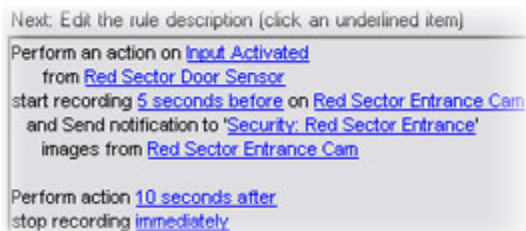
ルールを作成するために**ルールの管理**を使用します。ウィザードがすべての関連するステップをガイドします。ステップに従ってルールのアクションを指定し、通知プロファイルの使用を指定します。

<プロファイル>に通知を送信するアクションを選択すると、関連する通知プロファイルを選択でき、通知プロファイルの E メール通知に含む記録がどのカメラからのものかを選択できます。

Send notification to '[profile](#)'
images from [recording device](#)

例。ルールの**管理**で、選択を行うリンクをクリックします。

実際に何らかの記録がされていない限り、通知プロファイルの E メール通知に記録を含むことができなことにご注意ください。静止画像または AVI ビデオクリップを E メール通知に含めたい場合は、録画の開始を指定するルールを検証します。次の例は、**記録の開始**アクションと**通知を送信します**アクションを含むルールの例です。



通知プロファイル (プロパティ)

通知プロファイルの以下のプロパティを指定します。

コンポーネント	要件
名前	通知プロファイルの分かりやすい名前を入力します。名前は、ルール作成中に通知プロファイルを選択したときに表示されます。
説明 (任意)	通知プロファイルの説明を入力します。説明は、概要ペインの 通知プロファイル リストの通知プロファイルにマウスポインタを合わせると表示されます。
受信者	通知プロファイルの E メールによる通知を送信する宛先となる E メールアドレスを入力します。2 つ以上の E メールアドレスを入力する場合は、セミコロンでアドレスを区切ってください。例： aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc
件名	E メールによる通知で、件名として表示するテキストを入力します。 件名とメッセージテキストフィールドには、 デバイス名 などのシステム変数を挿入できます。変数を挿入するには、フィールド下のボックスの必要な変数リンクをクリックします。
メッセージテキスト	E メールによる通知で、本文として表示するテキストを入力します。メッセージテキストの他に、E メール通知の本文には、以下の情報が自動的に追加されます。 <ul style="list-style-type: none"> • E メールによる通知がトリガされた原因。 • 添付静止画像または AVI ビデオクリップのソース
E メール間の時間	各 E メール通知を送信する間隔の最小時間 (秒) を指定します。例： <ul style="list-style-type: none"> • 120 を指定した場合、2 分経過する前にルールにより通知プロファイルが再びトリガされた場合でも、各 E メール通知は最低 2 分経過するまで送信されません。 • 0 を指定すると、通知プロファイルがルールでトリガされるたびに E メール通知が送信されます。これにより E メール通知が大量に送信される可能性があります。したがって、値に 0 を使用する場合、ルールが頻繁にトリガされる通知プロファイルを送信する際は注意が必要です。

コンポーネント	要件
画像の数	各通知プロファイルの E メール通知に添付する最大静止画像数を指定します。デフォルトの画像数は 5 個です。
画像間の時間 (ミリ秒) :	添付画像に提示された記録間のミリ秒数を指定します。例: デフォルトは 500 ミリ秒で、添付画像は 1/2 秒間隔で記録を表示します。
イベント前の時間 (秒)	この設定は AVI ファイルの開始を指定する際に使用します。デフォルトでは、AVI ファイルには通知プロファイルがトリガされる 2 秒前からの録画が含まれます。これは、必要な秒数に変更できます。
イベント後の時間(秒)	この設定は AVI ファイルの終了を指定する際に使用します。デフォルトでは、AVI ファイルは通知プロファイルがトリガされた 4 秒後に終了します。これは、必要な秒数に変更できます。
フレームレート	AVI ファイルに含める秒当たりのフレーム数を指定します。デフォルトは 1 秒当り 5 フレームです。フレームレートが高ければ高いほど、画質と AVI ファイルサイズが大きくなります。
E メールに画像を埋め込む	選択すると (デフォルト)、画像が E メール通知の本文に挿入されます。選択しなければ、画像は添付ファイルとして E メール通知に添付されます。

ユーザー定義イベント

ユーザー定義イベントについて

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

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

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

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

イベント	詳細
Network Video Management System Smart Client で手動でイベントをトリガできるようにする方法	この場合、エンドユーザーが手動でイベントをトリガしながら、Network Video Management System Smart Client のライブビデオを視聴することができます。Network Video Management System Smart Client ユーザーにより手動でトリガされたためにユーザー定義イベントが発生すると、ルールによりシステムで行うべき 1 つまたは複数のアクションがトリガされます。

イベント	詳細
<p>API を通してイベントをトリガできるようにする方法</p>	<p>この場合、監視システムの外のユーザー定義イベントをトリガできます。この方法でユーザー定義イベントを使用するには、ユーザー定義イベントをトリガする際に、個別の API（アプリケーションプログラムインターフェース。ソフトウェアアプリケーションの作成またはカスタマイズに必要な構築ブロックのセット）が必要です。この方法でユーザー定義イベントを使用するには、Active Directory からの認証が必要です。これにより、ユーザー定義イベントが監視システムの外側からトリガ可能にも関わらず、認証されたユーザーのみが実行可能となります。</p> <p>また、ユーザー定義イベントは、API よりメタデータに関連付けし、特定のデバイスまたはデバイスグループを定義することができます。これは、ユーザー定義イベントを使ってルールをトリガする際に非常に便利です。デバイスごとにルールを適用せずに済むため、同じ操作を繰り返す必要がなくなります。例：ある企業には出入り口が 35 箇所あり、アクセスコントロールを使用しており、それぞれにアクセスコントロールデバイスがあります。アクセスコントロールデバイスを有効にすると、システムでユーザー定義イベントがトリガされます。このユーザー定義イベントをルールで使用して、有効なアクセスコントロールデバイスに関連するカメラで録画を開始することができます。どのカメラがどのルールに関連付けられるかは、メタデータで定義されます。この方法により、企業は 35 個のユーザー定義イベントと 35 個のユーザー定義イベントでトリガされたルールを作成する必要がなくなります。単一のユーザー定義イベントと、単一のルールで十分な管理が可能になります。</p> <p>ユーザー定義イベントをこの方法で使用する場合、Network Video Management System Smart Client の手動トリガで常に使用できるようにしておきたい場合もあるでしょう。役割を使用して、どのユーザー定義イベントが Network Video Management System Smart Client に表示されるか決定することができます。</p>

ユーザー定義イベントをどのように使用しても、各ユーザー定義イベントを Management Client で追加する必要があります。

ユーザー定義イベントの名前を変更した場合、すでに接続済みの Network Video Management System Smart Client ユーザーの場合、名前の変更が表示されるには、ログアウトしてから再度ログインする必要があります。

また、ユーザー定義イベントを削除すると、ユーザー定義イベントが使用されていたルールに影響が出ます。さらに、削除されたユーザー定義イベントは、Network Video Management System Smart Client ユーザーがログアウトしてはじめて Network Video Management System Smart Client で削除されます。

ユーザー定義イベントの追加

1. **ルールとイベント** > **ユーザー定義イベント**を展開します。
2. **概要**ペインで、**イベント**を右クリックし、> **ユーザー定義イベントの追加**を選択します。
3. 新規ユーザー定義イベントの名前を入力し、**OK** をクリックします。新しく追加したユーザー定義イベントが、**概要**ペインのリストに表示されます。
4. ユーザーに権限がある場合は、ユーザーは Network Video Management System Smart Client でユーザー定義イベントを手動でトリガできるようになります。

ユーザー定義イベントの名前変更

1. **ルールとイベント** > **ユーザー定義イベント**を展開します。
2. **概要**ペインで、ユーザー定義イベントを選択します。
3. **プロパティ**ペインで、既存の名前を上書きします。
4. ツールバーで**保存**をクリックします。

アナリティック イベント

アナリティックイベントについて

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)プロバイダから受け取ったデータです。

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

- 1. アナリティ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. アラーム定義のソースとしてアナリティックイベントを使用します。**サイトナビゲーション**ペインの**ルールとイベント**リストでアナリティックイベントを設定します。VCA ベースのイベントを使用する場合は、データをシステムに配信するために、サードパーティー製のVCA ツールが必要です。ユーザーの選択した任意のVCA ツールを使用できます。ただし、ツールが作成するデータは、指定された形式に準拠していなければなりません。詳細はシステムプロバイダにお問い合わせください。サードパーティー製のVCA ツールは、Sony オープンプラットフォームに基づいてソリューションを提供する独立系パートナーによって開発されています。これらのソリューションは、システムのパフォーマンスに影響する場合があります。

分析イベントを追加し、編集。

分析イベントを追加

1. **ルールとイベント**を展開し、**分析イベント**を右クリックし、**新規追加**を選択します。
2. **プロパティ**ウィンドウの中で、**名前**フィールドにイベントの名前を入力します。
3. **説明**フィールドにテキストの説明を入力します。
4. ツールバーで**保存**をクリックします。**テスト・イベント**をクリックすることで、イベントの有効性をテストできます。テストで示されたエラーを修正し、任意の回数およびプロセスの任意の場所からテストを連続的に実行できます。

分析イベントを編集します。

1. 既存の分析イベントをクリックして、関連するフィールドを編集できる**プロパティ**ウィンドウを表示します。

2. テスト・イベントをクリックすることで、イベントの有効性をテストできます。テストで示されたエラーを修正し、任意の回数およびプロセスの任意の場所からテストを連続的に実行できます。

分析種目のテスト

分析種目を設定した後、要件を『166ページの"アナリティックイベントをテストする(プロパティ)"参照』例えば、分析種目特性が機能しているかどうかをテストできます Management Client。

1. 現行の分析種目を選んで下さい。
2. プロパティの中から、「種目テスト」 ボタンをクリックして下さい。可能なすべての種目を示すウィンドウが表示されます。
種目テストのソースを、例えば、カメラを選んで下さい。そのウィンドウは閉じられ、分析種目が機能するための四つの条件を満たす新しい画面が表示されます。

追加のテストとして、 Network Video Management System Smart Client 分析種目が種目サーバーに送信されたかどうか確認できます。そうするためには、 Network Video Management System Smart Client 警告マネージャー のタブを開いて種目を見て下さい。

これも見て下さい。

分析種目について

アナリティックイベントをテストする(プロパティ)

アナリティックイベントの要件をテストする場合は、4つの条件を確認し、エラーがある場合はエラーの説明と解決策を示すウィンドウが表示されます。

条件	説明	エラーメッセージと解決策
保存した変更	イベントが新しい場合は保存されますか？ または、イベント名を変更した場合は、変更内容は保存されますか？	アナリティックイベントをテストする前に変更を保存してください。解決策/説明:変更を保存してください。
アナリティックイベントが有効です	アナリティックイベント機能は有効ですか？	アナリティックイベントは有効ではありません。解決策/説明:アナリティックイベント機能を有効にしてください。これを実行するためには、【ツール】>【オプション】>【アナリティックイベント】をクリックし、【有効】チェックボックスを選択します。
許可されるアドレス	イベントを送信するマシンの IP アドレスまたはホスト名は許可(アナリティックイベントアドレスリストに登録)されていますか？	Analytic Event サービスに対して許可されているアドレスとして、ローカルホスト名を追加する必要があります。解決策/説明:許可される IP アドレスまたはホスト名のアナリティックイベントアドレスリストに、使用しているマシンを追加します。 ローカルホスト名の解決中にエラーがありました。解決策/説明:マシンの IP アドレスまたはホスト名が見つからないか無効です。
アナリティックイベントを送信する	テストイベントはイベントサーバーに正常に送信されましたか？	以下のテーブルを参照してください。

各ステップは失敗✖または成功でマークされます✔。

条件アナリティックイベントの送信に対するエラーメッセージと解決策:

イベントサーバーが見つかりません	イベントサーバーが登録済みサーバーのリストにありません。
イベントサーバーへの接続中にエラーが発生しました	指定されたポートでイベントサーバーに接続できません。一般的には、ネットワークの問題か、イベントサーバーサービスが停止しているため、エラーが発生します。
アナリティックイベントの送信エラーが発生しました	イベントサーバーサービスへの接続は確立しますが、イベントを送信できません。一般的には、タイムアウトなどのネットワークの問題のため、エラーが発生します。
イベントサーバーからの応答の受信中にエラーが発生しました	イベントサーバーにイベントが送信されましたが、応答が受信されません。一般的には、ネットワークの問題またはポートがビジー状態のため、エラーが発生します。 通常は <i>ProgramData\Sony\Network VMSEvent Server\logs</i> にあるイベントサーバーログを確認してください。
イベントサーバーには不明なアナリティックイベントです	イベントサーバーサービスがイベントを認識しません。エラーが発生する最も可能性の高い理由は、イベントまたはイベントの変更が保存されていないことです。
イベントサーバーが無効なアナリティックイベントを受信しました	イベントのフォーマットが正しくありません。
送信者はイベントサーバーによって承認されていません。	通常は、許可された IP アドレスまたはホスト名のリストにマシンがないためです。
イベントサーバーの内部エラーが発生しました。	イベントサーバーエラー。 通常は <i>ProgramData\Sony\Network VMSEvent Server\logs</i> にあるイベントサーバーログを確認してください。
イベントサーバーが無効な応答を受信しました。	応答は無効です。ポートがビジー状態か、ネットワークに問題がある可能性があります。 通常は <i>ProgramData\Sony\Network VMSEvent Server\logs</i> にあるイベントサーバーログを確認してください。
イベントサーバーから不明な応答を受信しました	応答は有効ですが、理解不能です。エラーが発生しているのは、ネットワークの問題またはポートがビジー状態のためである可能性があります。 通常は <i>ProgramData\Sony\Network VMSEvent Server\logs</i> にあるイベントサーバーログを確認してください。
予期しないエラーが発生しました	Sony サポートにお問い合わせください。

アナリティックイベント設定の編集

ツールバーで **ツール > オプション > アナリティックイベント** タブを選択して、関連する設定を編集します。

ジェネリックイベント

ジェネリックイベントについて

重要：この機能は、Network Video Management System イベントサーバーがインストールされていないと動作しません。

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

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

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

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

ジェネリックイベントの追加

video management software が外部システムからの TCP または UDP パケットの特定の文字列を認識できるようにジェネリックイベントを定義することができます。ジェネリックイベントに基づいて、録画またはアラームの開始などのアクションをトリガするように Management Client を設定することができます。

前提条件: ジェネリックイベントを有効にし、許可されるソース宛先を指定しています。詳細は、[ジェネリックイベント] タブ 『213 ページ の"ジェネリックイベントタブ(オプション)"参照』を参照してください。

1. **[ルールとイベント]**を展開します。
2. **[ジェネリックイベント]**を右クリックして、**[新規追加]**を選択します。
3. 必要な情報とプロパティを入力します。詳細は、ジェネリックイベントプロパティ 『169 ページ の"ジェネリックイベント (プロパティ)"参照』を参照してください。
4. (オプション)検索式が有効であることを検証するため、予測されるパッケージに対応する**[表現がイベント文字列と一致するかチェック]**フィールドに次の検索文字列を入力します。
 - **一致する** - 文字列を検索式に対して検証できます。
 - **一致しない** - 検索式は無効です。検索式を変更して、再試行してください。

Network Video Management System Smart Client では、イベントサーバーによってジェネリックイベントが受信されたかどうかを検証できます。これは、**[イベント]**を選択することで、**[アラームマネージャ]**タブの**[アラームリスト]**で実行します。

ジェネリックイベント (プロパティ)

コンポーネント	要件
名前	ジェネリックイベントの一意の名前。名前は、ユーザー定義イベント、分析イベント等すべてのタイプのイベントに対して一意のものでなければなりません。
デバイスが有効	ジェネリックイベントはデフォルトでは有効になっています。イベントを無効にするにはチェックボックスを解除します。
表現	<p>データパッケージの分析時にシステムが参照すべき表現。次の演算子を使用できます。</p> <ul style="list-style-type: none"> • (): 関連項を論理ユニットとして同時に処理するために使用されます。分析で特定の処理順序を強制するために使用されます。 <p>例: 検索条件「(User001 OR Door053) AND (Sunday)」を使用する場合、括弧内の2つの項が先に処理され、その結果が文字列の最後の部分と結合されます。つまり、システムはまず User001 または Door053 という項を含むパッケージを参照し、その後結果を取得し、Sunday という項を含むパッケージを検索します。</p> <ul style="list-style-type: none"> • AND: 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。 <p>例: 検索基準「User001 AND Door053 AND Sunday」は、User001、Door053 および Sunday のすべてが表現に含まれている場合のみ結果を返します。用語のいずれかまたは2つが存在するだけでは足りません。語句を AND で結合すればするほど、返される結果は少なくなります。</p> <ul style="list-style-type: none"> • OR: 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。 <p>例: 検索基準「User001 OR Door053 OR Sunday」は、User001、Door053 または Sunday のいずれかが式に含まれている結果を返します。語句を OR で結合すればするほど、返される結果は多くなります。</p>

<p>表現のタイプ</p>	<p>受信したデータパッケージを分析する時に特定のシステムがあるべき状態を示します。オプションは以下の通りです。</p> <ul style="list-style-type: none"> • 検索: イベントが発生するためには、受信したデータパッケージには、式: フィールドに指定したテキストが存在する必要がありますが、これ以外の内容が含まれることがあります。 <p>例: 受信したパッケージに User001 および Door053 が含まれるよう指定した場合、受信したパッケージに User001、Door053、Sunday が含まれる場合、受信したパッケージに 2 つの必要な語句が含まれるため、イベントがトリガされます。</p> <ul style="list-style-type: none"> • 一致: イベントが発生するためには、受信したデータパッケージには、表現: フィールドに指定したものと全く同一のテキストが存在する必要があります。 • 通常の表現: イベントが発生するには、表現: フィールドに指定したテキストが、受信したデータパッケージの特定のパターンを特定しなければなりません。 <p>検索 または 一致 から 正規表現 に切り替えると、表現 フィールドのテキストは、自動的に正規表現に変換されます。</p>
<p>優先度</p>	<p>0 (最低優先度) ~ 999999 (最高優先度) の数値によって優先度を指定してください。</p> <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。</p> <p>システムが TCP および UDP パッケージを受信した場合、そのパケットの分析が、最高優先度のイベントで開始されます。これにより、パッケージが複数のイベントの基準と一致する場合、最高優先度のイベントのみがトリガされます。パッケージが同じ優先度で複数のイベントの基準と一致した場合、たとえば、優先度 999 のイベントが 2 つある場合、その優先度のすべてのイベントがトリガされます。</p>
<p>表現がイベント文字列と一致するかチェック:</p>	<p>表現: フィールドに入力した表現に対してイベント文字列をテストします。field。</p>

ジェネリックイベントデータソース (プロパティ)

コンポーネント	要件
データソース	<p>2つのデフォルトデータソースから選択してカスタムデータソースを定義できます。選択内容は、お使いのサードパーティ製プログラムおよび/またはインターフェース対象となるハードウェアまたはソフトウェアによって異なります。</p> <p>互換: 工場出荷時のデフォルト設定が有効。すべてのバイトをエコー。TCP および UDP。IPv4 のみ。ポート 1234。区切り文字なし。ローカルホストのみ。現在のコードページエンコーディング(ANSI)。</p> <p>インターナショナル: 工場出荷時のデフォルト設定が有効。統計のみをエコー。TCP のみ。IPv4+6。ポート 1235。<CR><LF>を区切り文字として使用。ローカルホストのみ。UTF-8 エンコーディング。(<CR><LF> = 13,10)。</p> <p>[データソース A] [データソース B] のようになります。</p>
新規作成	クリックすると新しいデータソースを作成できます。
名前	データソースの名前。
デバイスが有効	データソースはデフォルトでは有効になっています。データソースを無効にするにはチェックボックスを解除します。
リセット	クリックして選択されたデータソースのすべての設定をリセットします。 名前 フィールドに入力された名前は残ります。
ポート	データソースのポート番号。
プロトコルタイプセレクタ	<p>システムがジェネリックイベントを検出するために聞き、分析すべきプロトコル。</p> <p>すべて: TCP および UDP。</p> <p>TCP: TCP のみ。</p> <p>UDP: UDP のみ。</p> <p>ジェネリックイベントに使用する TCP および UDP パッケージに、@、#、+、-、等の特殊文字が含まれている場合があります。</p>
IP タイプセレクタ	選択可能な IP アドレスタイプ: IPv4、IPv6、または両方。
区切りバイト	個別ジェネリックイベント記録を分離するために使用するセパレーター バイトを選択します。デフォルトのデータソースタイプ インターナショナル (上記の データソース をご覧ください) は 13、10 です。(13,10 = <CR><LF>)。

コンポーネント	要件
エコータイプセレクト	<p>使用可能なエコーリターン形式：</p> <ul style="list-style-type: none"> エコー統計： 次の形式をエコーします。 [X],[Y],[Z],[ジェネリックイベント名] [X] = 要求番号。 [Y] = 文字数。 [Z] = ジェネリックイベントとの一致数。 [ジェネリックイベント名] = 名前：フィールドに入力された field。 すべてのバイトをエコー：すべてのバイトをエコーします。 エコーなし：すべてのエコーを抑制します。
エンコーディングタイプセレクト	デフォルトでは、もっとも関連のあるオプションのみがリストに表示されます。 すべて表示 チェックボックスを選択し、利用可能なすべてのエンコーディングを表示します。
すべて表示	前の項目を参照してください。
使用可能な外部 IPv4 アドレス	外部イベントを管理するために、管理サーバーが通信可能な IP アドレスを指定します。これを使用して、データを取得しない IP アドレスを除外することも可能です。
使用可能な外部 IPv6 アドレス	外部イベントを管理するために、管理サーバーが通信可能な IP アドレスを指定します。これを使用して、データを取得しない IP アドレスを除外することも可能です。

ヒント：範囲は、**100**、**105**、**110~120** 等 4 つの位置にそれぞれ指定できます。例えば、10.10 ネットワークのすべてのアドレスは、**10.10.[0-254].[0-254]**または **10.10.255.255** により使用可能になります。

セキュリティ

役割

役割について

役割により、ユーザーがアクセスできるデバイスが決定されます。また、役割は権限を決定し、ビデオ管理システムのセキュリティも取り扱います。まず、役割を追加し、次にユーザーとグループを追加して、最後に **Smart Client** プロファイルと共に、それぞれの役割に属しているその他のデフォルトのプロファイルも追加します。システムで作成できる役割には、それぞれに **Network Video Management System Smart Client** における独自のビューグループがあり、これを通じてビューを作成、保存できます。

システムには、削除できない事前に定義された役割が 1 つ用意されています：**管理者**役割です。**管理者**役割を有するユーザーおよびグループは、システム全体に完全で無制限なアクセス権限を有します。この理由で、**管理者**

役割に対して役割の設定を指定することはできません。**管理者**の役割は、Smart Client プロファイルのデフォルトはありますが、何の時間プロファイルはありません。

管理サーバーが動作するコンピュータのローカルマシン管理者の権限を有するユーザーは、管理サーバーの管理者権限を自動的に有します。システムの管理者として信頼できるユーザーのみが、管理サーバーが動作するコンピュータのローカルマシン管理者の権限を有するべきです。これを無効にすることはできません。ユーザーやグループを**管理者**役割に追加する方法は、他の役割の場合と同じです。ユーザーおよびグループの役割からの削除、役割への割り当て 『175ページ』を参照してください。

管理者役割に加え、必要な数の役割を追加することができます。たとえば、カメラへのアクセス権や類似の制限に応じて、Network Video Management System Smart Client のユーザーに異なる役割を持たせることもできます。システムで役割を設定するには、**セキュリティ > 役割**を展開します。

役割の権限について

システムで役割を作成する際に、関連する役割がアクセス、使用できるシステムのコンポーネントや機能に対して複数の権限をその役割に付与することができます。たとえば、Network Video Management System Smart Client の機能に対する権限だけを有する役割、あるいは特定のカメラを表示できる権限を有する他の Sony 表示クライアントなどを作成する必要があるとします。こうした役割を作成する場合、これらの役割が Management Client に対するアクセス、使用の権限を有する必要はありませんが、Network Video Management System Smart Client またはその他のクライアントにある機能の一部または全部へのアクセスだけは必要です。これを解決するには、たとえば、カメラ、サーバー、類似の機能を追加、削除できる権限など、一部または大半の一般的な管理者権限を有する役割を設定する必要があるかもしれません。

システム管理者の機能の一部または大半を有する役割を作成できます。たとえば、これは組織でシステムのサブセットを管理する人と、システム全体を管理する人を分けたい場合などに関連するものです。この機能によって、たとえば、システムのサーバーまたはカメラの設定の編集できる権限など、システムのさまざまな機能にアクセス、編集、変更ができる異なる管理者権限を提供できるようになります。[セキュリティ全般]タブ 『177ページ』の "セキュリティ全般タブ (役割)"参照』でこれらの権限を指定します。最低限、特別なシステム管理者が Management Client を起動できるようにするには、管理サーバー上でその役割に読み取り権限を付与する必要があります。

このように異なる権限を役割に付与するには、デフォルトの管理者役割を有する人が、**セキュリティ > 役割 > 情報タブ > 新規追加**で役割を設定しなければなりません。新しい役割を設定する場合、システムで他の役割を設定したり、システムのデフォルトのプロファイルを使用したりするのと同じように、役割に関連付けられるのは独自のプロファイルだけです。詳しくは、役割の追加および管理 『174ページ』を参照してください。

どのプロファイルを役割に関連付けるかを指定したら、**セキュリティ全般**タブへ移動して、その役割の権限を指定します。

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。

Windows ユーザー

Active Directory を使用して、Windows ユーザーを追加します。Active Directory (AD)は、Windows ドメインのネットワーク向けに Microsoft が実装した ディレクトリサービス です。これは、ほとんどの Windows Server オペレーティングシステムに搭載されています。このサービスは、ユーザーやアプリケーションがアクセ

スできるネットワーク上のリソースを識別します。Active Directory は、ユーザーおよびグループの概念を使用します。

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



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



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

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

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

Active Directory サービスでユーザーやグループを追加する前に、Active Directory がインストールされているサーバーがネットワーク上に必要です。

基本ユーザー

システムが Active Directory にアクセスできない場合、基本ユーザー 『189ページ』の"基本ユーザーについて"参照』を作成します。基本ユーザーのセットアップ方法については、基本ユーザーの作成 『189ページ』を参照してください。

役割の追加および管理

1. セキュリティを展開して、**役割**を右クリックします。
2. **役割の追加**を選択します。これにより、**役割の追加**ダイアログボックスが開きます。
3. 新しい役割の名前と説明を入力し、**OK**をクリックします。
4. 新しい役割が**役割**リストに追加されます。デフォルトでは、新しい役割にはユーザー/グループは関連付けられていませんが、関連付けられたデフォルトのプロファイルがあります。

- 異なる Smart Client のプロファイル、時間プロファイルを選択するには、ドロップダウンリストをクリックします。
- これで、ユーザー/グループを役割に割り当てて、どのシステム機能にユーザー/グループがアクセスできるかを指定できます。

ユーザーおよびグループの役割からの削除、役割への割り当て 『175ページ』および役割の設定 『177ページ』を参照してください。

役割のコピー、名前の変更、削除

役割のコピー

役割の設定や権限が複雑で、ほぼ同様の役割が必要な場合は、新しい役割をゼロから作成するよりも、既存の役割をコピーし、コピーした役割を少し修正する方が簡単な場合があります。

- セキュリティ**を展開し、**役割**をクリックし、関連する役割を右クリックして、**役割のコピー**を選択します。
- ダイアログボックスが開いたら、コピーした役割の新しい一意の名前と説明を入力します。
- OK**をクリックします。

役割の名前の変更

役割の名前を変更しても、役割をベースとしたビューグループの名前は変更されません。

- セキュリティ**を展開して、**役割**を右クリックします。
- 必要な役割を右クリックし、**役割の名前の変更**を選択します。
- ダイアログボックスが開いたら、役割の名前を変更します。
- OK**をクリックします。

役割の削除

- セキュリティ**を展開し、**役割**をクリックします。
- 対象外の役割を右クリックし、**役割の削除**を選択します。
- はい**をクリックします。

重要： 役割を削除しても、役割をベースとしたビューグループは削除されません。

ユーザーおよびグループの役割からの削除、役割への割り当て

Windows ユーザー、グループまたは基本ユーザーを役割から削除したり、役割に割り当てるには、以下を行います。

- セキュリティ**を展開し、**役割**を選択します。次に、**概要**ペインで必要な役割を選択します。
- プロパティ**ペインの下部で**ユーザーおよびグループ**タブを選択します。
- 追加**をクリックし、**Windows ユーザー**または**基本ユーザー**から選択します。

役割に Windows ユーザーおよびグループを割り当てる

1. **Windows ユーザー**を選択します。**ユーザーの選択、コンピュータ、およびグループの選択**ダイアログボックスが開きます。
2. 必要なオブジェクトタイプを指定しているか確認します。例えば、コンピュータを追加する必要がある場合、**オブジェクトタイプ**をクリックし、**コンピュータ**をマークします。さらに、**この場所から**フィールドに必要なドメインを指定したか確認します。指定されていない場合は、**場所**をクリックして、必要なドメインを参照します。
3. **選択するオブジェクト名**を入力ボックスで、関連するユーザー名、イニシャル、または Active Directory が認識できるその他の識別子タイプを入力します。**名前のチェック**機能を使用して、入力した名前やイニシャルを Active Directory が認識できることを確認します。あるいは、**"詳細設定..."**機能を使用して、ユーザーまたはグループを検索します。
4. **OK** をクリックします。選択したユーザー/グループは、これで選択した役割に割り当てたユーザーの **ユーザーおよびグループ** タブのリストに追加されます。セミコロン (;) で区切って複数の名前を入力することで、さらに多くのユーザーやグループを追加することができます。

役割に基本ユーザーを割り当てる

1. **基本ユーザー**を選択します。これにより、**ロールに追加する基本ユーザー**を選択ダイアログボックスが開きます。
2. この役割に割り当てる基本ユーザーを選択します。
3. オプション：**新規**をクリックすると新しい基本ユーザーを作成できます。
4. **OK** をクリックします。選択した基本ユーザーは、これで選択した役割に割り当てた基本ユーザーの **ユーザーおよびグループ** タブのリストに追加されます。

役割からユーザーおよびグループを削除する

1. **ユーザーおよびグループ** タブで、削除したいユーザーまたはグループを選択し、タブ下の **削除** をクリックします。必要に応じて、複数のユーザーまたはグループ、あるいはグループや個人ユーザーの組み合わせを選択することができます。
2. 選択したユーザーまたはグループを削除することを確認します。**はい** をクリックします。

ユーザーは、グループメンバーを経由して役割を有することもあります。この場合、その役割から個別ユーザーを削除することはできません。グループメンバーは、個人として役割を持つ場合もあります。ユーザー、グループ、または個別のグループメンバーが有する役割を検索するには、**有効な役割の表示**機能を使用します。

有効な役割の表示

有効な役割機能により、選択したユーザーまたはグループのすべての役割を表示することができます。この機能は、グループを使用している場合に特に便利であり、個別のユーザーがどのメンバーの役割であるかを表示する唯一の方法です。

1. **セキュリティ**を展開して**役割**を右クリックして**有効な役割**ウィンドウを開き、**有効な役割**を選択します。
2. 基本ユーザーの情報を確認するには、**ユーザー名**フィールドに名前を入力します。**更新**をクリックすると、ユーザーの役割が表示されます。

- Active Directory で Windows ユーザーまたはグループを使用する場合、[...]参照ボタンをクリックします。オブジェクトタイプを選択して名前を入力し、OK をクリックします。ユーザーの役割が自動的に表示されます。

役割の設定

情報タブ(役割)

役割の**情報**タブで、以下を設定できます:

名前	詳細
名前	役割の名前を入力します。
詳細	役割の説明を入力します。
Smart Client プロファイル	役割と関連付ける Smart Client のプロファイルを選択します。
デフォルトの時間プロファイル	役割と関連付けるデフォルトの時間プロファイルを選択します。 これを、デフォルトの 管理者 役割に適用することはできません。
ログイン認証が必要	チェックボックスを選択して、ログイン認証を役割と関連付けます。つまり、ユーザーがログインする際に、Network Video Management System Smart Client または Management Client が 2 番目の認証を要求することを意味します(通常は、スーパーユーザーまたはマネージャが要求)。 管理者がユーザーを認証できるようにするには、 セキュリティ全般 タブで管理サーバーの ユーザーを認証する 権限を設定します。 これを、デフォルトの 管理者 役割に適用することはできません。

ユーザーおよびグループタブ(役割)

【ユーザーおよびグループ】タブでは、ユーザーとグループを役割に割り当てます 『175ページ の"ユーザーおよびグループの役割からの削除、役割への割り当て"参照』。Windows ユーザーおよびグループまたは基本ユーザー 『173ページ の"ユーザーについて"参照』を割り当てることができます。

名前	説明
名前	この役割に割り当てられたユーザーまたはグループの名前が表示されます。
説明	基本ユーザーが作成されたときに入力した説明が表示されます。

セキュリティ全般タブ (役割)

セキュリティ全般タブで、役割の全般的な権限を設定します。システムで使用できるすべてのコンポーネントについて、権限のある役割のユーザーが関連するコンポーネントを異なるエリアでアクセスし、使用することを許可するか、拒否するかを決定します。

セキュリティ全般の設定は、現在のサイトだけに適用されます。

ユーザーに複数の役割を関連付けることもできます。セキュリティ設定に関して、ある役割で**拒否**を選択し、別の役割で**許可**を選択した場合、**拒否**権限の方が**許可**権限より優先します。

以下の説明は、関連する役割に対して**許可**を選択した場合、さまざまなシステムコンポーネントのそれぞれの権限について個々に何が起こるかを示しています。

すべてのシステムコンポーネントや機能について、完全なシステム管理者は**許可**または**拒否**のチェックボックスを使用して、役割に関するセキュリティ権限を設定できます。ここで設定するセキュリティ権限は、システムコンポーネントや機能の全体の設定に関するものです。したがって、たとえば、**カメラ**で**拒否**チェックボックスを選択すると、システムに追加されるすべてのカメラがその役割では使用できなくなります。対照的に、**許可**チェックボックスを選択すると、この役割ではシステムに追加されるすべてのカメラを表示できるようになります。カメラでの**許可**または**拒否**の選択は、**デバイス**タブでのカメラの設定となり、特定の役割に対してすべてのカメラが使用可能または使用不能となるように、**セキュリティ全般**タブでの選択が継承されます。個々のカメラや類似のデバイスチャンネルに対して、個別にセキュリティ権限を設定する場合、**セキュリティ全般**タブでシステムコンポーネントや機能の全般的設定が無効になっていれば、これらの個々の権限は、関連するシステムコンポーネントや機能のタブでのみ設定できます。

また、下記の説明は、MIP SDK で設定できる権限にも適用されます。

管理サーバー

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
システム監視	システム監視のデータを表示する権限を有効にします。
ステータス API	レコーディングサーバーに存在するステータス API に対するクエリを実行できる権限を有効にします。これは、この権限が有効になっている役割が、レコーディングサーバーに存在するアイテムのステータスの読み取りにアクセスできることを意味します。
ユーザーを認証	Network Video Management System Smart Client または Management Client で第二のログインを求められた際に、ユーザーを認証できる権限を有効にします。役割がログイン認証を必要とするかどうかを 情報 タブで定義します。

カメラ

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	クライアントでカメラデバイスを表示する権限を有効にします。
ライブ表示	クライアントでカメラのライブビデオを表示する権限を有効にします。
再生	クライアントでカメラの録画ビデオを再生する権限を有効にします。

セキュリティ権限	説明
リモート録画の取得	カメラからのエッジ記録の取得、またはリモートサイトにあるカメラからの録画の取得を有効にします。
シーケンスを読み取る	たとえば、クライアントのシーケンスエクスプローラに関連するシーケンス情報を読みとる権限を有効にします。
スマートサーチ	クライアントでスマートサーチを使用する権限を有効にします。
・イ・ツ・ケ・ン・サ・ネ	クライアントから録画をエクスポートする権限を有効にします。
手動録画を開始	クライアントでビデオの手動録画を開始する権限を有効にします。
手動録画を停止	クライアントでビデオの手動録画を停止する権限を有効にします。
AUX コマンド	クライアントからのカメラで補助(AUX)コマンドを使用する権限を有効にします。 AUX コマンド は、たとえばビデオサーバー経由で接続されているカメラのワイパーのコントロールを可能にします。補助接続で接続されているカメラ関連デバイスは、クライアントからコントロールされます。
手動 PTZ	PTZ カメラで PTZ 機能を使用する権限を有効にします。
PTZ プリセットまたはパトロール設定をアクティブ化する	PTZ カメラをプリセット位置に移動し、パトロールプロファイルを開始および停止し、パトロールを再開する権限を有効にします。 この役割がカメラの他の PTZ 機能を使用することを許可するには、 手動 PTZ 権限を有効にします。
PTZ プリセットまたはパトロールプロファイルの管理	Management Client の両方で PTZ カメラの PTZ プリセットとパトロールプロファイルを追加、編集、および削除する権限を有効にします。 この役割がカメラの他の PTZ 機能を使用することを許可するには、 手動 PTZ 権限を有効にします。

マイク

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	クライアントでマイクデバイスを表示する権限を有効にします。
聴く	クライアントのマイクからのライブ音声を聴く権限を有効にします。
再生	クライアントでマイクからの録音された音声を再生する権限を有効にします。
リモート録画の取得	マイクからのエッジ記録の取得、またはリモートサイトにあるマイクからの録音の取得を有効にします。

セキュリティ権限	説明
シーケンスを読み取る	たとえば、クライアントのシーケンスエクスプローラに関連するシーケンス情報を読みとる権限を有効にします。
・イ・ツ・ケ・ン・カ・`・ネ	クライアントから録画をエクスポートする権限を有効にします。
手動録画を開始	クライアントで音声の手動録画を開始する権限を有効にします。
手動録画を停止	クライアントで音声の手動録画を停止する権限を有効にします。

スピーカー

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	クライアントでスピーカーデバイスを表示する権限を有効にします。
聴く	クライアントのスピーカーからのライブ音声を聴く権限を有効にします。
通話	クライアントでスピーカーを通して通話する権限を有効にします。
再生	クライアントでスピーカーからの録音された音声を再生する権限を有効にします。
リモート録画の取得	スピーカーからのエッジ記録の取得、またはリモートサイトにあるスピーカーからの録音の取得を有効にします。
シーケンスを読み取る	クライアントでスピーカーから録音した音声をブラウズしながら、シーケンス機能を使用する権限を有効にします。
・イ・ツ・ケ・ン・カ・`・ネ	クライアントでスピーカーから録音した音声をエクスポートする権限を有効にします。
手動録画を開始	クライアントで音声の手動録画を開始する権限を有効にします。
手動録画を停止	クライアントで音声の手動録画を停止する権限を有効にします。

メタデータ

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	クライアントでメタデータを受け取る権限を有効にします。
ライブ	クライアントでカメラからのライブメタデータを受信する権限を有効にします。

セキュリティ権限	説明
再生	クライアントでメタデータデバイスからの録画データを再生する権限を有効にします。
リモート録画の取得	メタデータデバイスからのエッジ記録の取得、またはリモートサイトにあるメタデータデバイスからの記録の取得を有効にします。
シーケンスを読み取る	たとえば、クライアントのシーケンスエクスプローラに関連するシーケンス情報を読みとる権限を有効にします。
・イ・ツ・ケ・ン・ク・ネ	クライアントで録画をエクスポートする権限を有効にします。
手動録画を開始	クライアントでメタデータの手動録画を開始する権限を有効にします。
手動録画を停止	クライアントでメタデータの手動録画を停止する権限を有効にします。

入力

セキュリティ権限	説明
読み取る	クライアントで入力デバイスを表示する権限を有効にします。

出力

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	クライアントで出力デバイスを表示する権限を有効にします。
実行	クライアントで出力をアクティブ化する権限を有効にします。

Smart Wall

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	クライアントで Smart Wall を表示する権限を有効にします。
操作	たとえば、プリセットの変更や、クライアントでの表示へのカメラの適用など、Smart Wall を操作する権限を有効にします。
再生	クライアントデータを再生する権限を有効にします。

ビューグループ

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	Management Client のクライアントでビューグループを表示する権限を有効にします。
操作	Management Client クライアント内でビューグループを使用する、つまりサブグループやビューを使用する権限を有効にします。

ユーザー定義イベント

セキュリティ権限	説明
完全コントロール	システムのこの部分のすべてのセキュリティエントリを管理する権限を有効にします。
読み取る	Management Client およびクライアントで、ユーザー定義イベントを表示する権限を有効にします。
トリガ	クライアントでユーザー定義イベントをトリガする権限を有効にします。

Matrix

セキュリティ権限	説明
読み取る	ビデオを選択して、クライアントから Matrix 受信者へ送信する権限を有効にします。

デバイスタブ(役割)

デバイスタブでは、各デバイス（カメラ等）またはデバイスグループについて、選択した役割のユーザー/グループが Network Video Management System Smart Client で各デバイス(カメラなど)またはデバイスグループを使用できるかを指定できます。

それぞれのデバイスに対して繰り返すことを忘れないでください。また、デバイスグループを選択し、一度にグループのすべてのデバイスの役割権限を指定することもできます。

この四角で埋められたチェックボックスを選択したり選択解除することはできますが、この場合は、デバイスグループのすべてのデバイスに選択が適用されます。または、デバイスグループの個別デバイスを選択し、どのデバイスに権限が適用されるかを正確に確認することができます。

カメラ関連の権限

カメラデバイスに以下の権限を指定します：

名前	詳細
読み取る	選択したカメラが、クライアントで表示されます。
ライブ表示	クライアントで選択したカメラからビデオのライブ表示ができるようにします。Network Video Management System Smart Clientでは、クライアントの ライブタブ を表示する権限が役割に付与されていることが必要になります。この権限は、アプリケーション権限の一部として付与されます。時間設定を指定するか、デフォルト値のままにします。
再生 > 再生の制限	クライアントで選択したカメラから録画ビデオの再生ができるようにします。再生の制限を指定するか、制限なしを適用します。
シーケンスを読み取る	たとえば、クライアントのシーケンスエクスプローラに関連するシーケンス情報の読み取りを有効にします。
スマートサーチ	クライアントでユーザーがスマートサーチ機能を使用できるようにします。
エクスポート	クライアントから、ユーザーが録画をエクスポートできるようにします。
手動録画を開始	クライアントで選択したカメラからビデオの手動録画を開始できるようにします。
手動録画を停止	クライアントで選択したカメラからビデオの手動録画を停止できるようにします。
AUX コマンド	クライアントからの、補助コマンドの使用を許可します。

マイク関連の権限

マイクデバイスに、以下の権限を指定します：

名前	詳細
読み取る	選択したマイクが、クライアントに表示されます。
ライブ > 聴く	クライアントで選択したマイクからのライブ音声を聞くことができるようにします。 Network Video Management System Smart Clientでは、クライアントの ライブタブ を表示する権限が役割に付与されていることが必要になります。この権限は、アプリケーション権限の一部として付与されます。時間設定を指定するか、デフォルト値のままにします。
再生 > 再生の制限	クライアントで選択したマイクからの録音した音声を再生できるようにします。再生の制限を指定するか、制限なしを適用します。
シーケンスを読み取る	たとえば、クライアントのシーケンスエクスプローラに関連するシーケンス情報の読み取りを有効にします。
エクスポート	クライアントから、ユーザーが録画をエクスポートできるようにします。
手動録画を開始	クライアントで選択したマイクからの音声の手動録音を開始できるようにします。

名前	詳細
手動録画を停止	クライアントで選択したマイクからの音声の手動録音を停止できるようにします。

スピーカー関連の権限

スピーカーデバイスに以下の権限を指定します：

名前	詳細
読み取る	選択したスピーカーが、クライアントで表示されます
ライブ > 聴く	クライアントで選択したスピーカーからのライブ音声を聞くことができるようにします。 Network Video Management System Smart Client では、クライアントの ライブ タブを表示する権限が役割に付与されていることが必要になります。この権限は、アプリケーション権限の一部として付与されます。時間設定を指定するか、デフォルト値のままにします。
再生 > 再生の制限	クライアントで選択したスピーカーから録音した音声を再生できるようにします。再生の制限を指定するか、制限なしを適用します。
シーケンスを読み取る	たとえば、クライアントのシーケンスエクスプローラに関連するシーケンス情報の読み取りを有効にします。
エクスポート	クライアントから、ユーザーが録画をエクスポートできるようにします。
手動録画を開始	クライアントで選択したスピーカーからの音声の手動録音を開始できるようにします。
手動録画を停止	クライアントで選択したスピーカーからの音声の手動録音を停止できるようにします。

メタデータ関連の権限

メタデータデバイスに、以下の権限を指定します：

名前	詳細
読み取る	クライアントでメタデータデバイスを表示し、メタデータデバイスからデータを取得することを有効にします。
編集	メタデータのプロパティを編集する権限を有効にします。また、ユーザーが Management Client で、および MIP SDK を介して、メタデータを有効または無効にすることも可能になります。
ライブ表示	クライアントでカメラからのメタデータを表示する権限を有効にします。 Network Video Management System Smart Client では、クライアントの ライブ タブを表示する権限が役割に付与されていることが必要になります。この権限は、アプリケーション権限の一部として付与されます。

名前	詳細
再生	クライアントでメタデータデバイスからの録画データを再生する権限を有効にします。
シーケンスを読み取る	クライアントでメタデータデバイスからの記録されたデータをブラウズしながら、シーケンス機能を使用する権限を有効にします。
エクスポート	クライアントでメタデータデバイスから録音した音声をエクスポートする権限を有効にします。
手動録画を開始	クライアントでメタデータの手動録画を開始する権限を有効にします。
手動録画を停止	クライアントでメタデータの手動録画を停止する権限を有効にします。

入力関連権限

入力デバイスに、以下の権限を指定します：

名前	詳細
読み取る	選択した入力は、監視システムのステータスとアラームの包括的な概要を提供するために、クライアントならびに Network Video Management System Central、アドオン製品で表示されます。

出力関連権限

出力デバイスに、以下の権限を指定します：

名前	詳細
読み取る	選択した出力は、クライアントで表示されます。表示される場合、出力はクライアントのリストで選択できます。
起動	選択した出力は、Management Client およびクライアントからアクティブ化できます。時間設定を指定するか、デフォルト値のままにします。

PTZ タブ (役割)

PTZ(パン/チルト/ズーム) カメラの権限は、**PTZ** タブで設定します。ユーザー/グループがクライアントで使用できる機能を指定できます。個別の PTZ カメラを選択したり、PTZ カメラを含んでいるデバイスグループを選択することができます。

PTZ に、以下の権限を指定します。

名前	説明
手動 PTZ	<p>選択した役割が、選択したカメラで PTZ 機能を使用し、パトロールを一時停止できるかどうかを決定します。</p> <p>時間設定を指定するか、[常時]を選択するか、その役割の[情報]タブで定義されたデフォルト時間設定に対応するデフォルト値のままにします。</p>
PTZ プリセットまたはパトロールプロファイルのアクティベーション	<p>選択した役割が選択したカメラをプリセット位置に移動し、パトロールプロファイルを開始および停止し、パトロールを一時停止できるかどうかを決定します。</p> <p>時間設定を指定するか、[常時]を選択するか、その役割の[情報]タブで定義されたデフォルト時間設定に対応するデフォルト値のままにします。</p> <p>この役割がカメラの他の PTZ 機能を使用することを許可するには、手動 PTZ 権限を有効にします。</p>
PTZ 優先度	<p>PTZ カメラの優先度を決定します。監視システムの複数のユーザーが同時に同じ PTZ カメラを制御しようとする、競合が発生する可能性があります。</p> <p>選択済みの役割を持つユーザー/グループが選択した PTZ カメラを使用する優先度を指定することで、この状況を回避できます。1~3 の範囲で優先度を指定します。1 が最低優先度です。最高の優先度を持つ役割は、PTZ カメラをコントロールできる人の役割です。</p>
PTZ プリセットまたはパトロールプロファイルの管理	<p>Management Client の両方で選択したカメラの PTZ プリセットとパトロールプロファイルを追加、編集、および削除する権限を決定します。</p> <p>この役割がカメラの他の PTZ 機能を使用することを許可するには、手動 PTZ 権限を有効にします。</p>
PTZ プリセットのロック/ロック解除	<p>役割が選択したカメラのプリセット位置をロックおよびロック解除できるかどうかを決定します。</p>

通話タブ(役割)

スピーカーがシステムで使用できる場合のみ該当します。スピーカーに、以下の権限を指定します：

名前	詳細
通話	<p>選択したスピーカーを通じて、ユーザーが通話を許可されるかどうかを決定します。時間プロファイルを指定するか、デフォルト値のままにします。</p>
通話優先度	<p>複数のクライアントユーザーが同じスピーカーから同時に通話したい場合、対立が生じることがあります。</p> <p>選択済みの役割を持つユーザー/グループが選択したスピーカーを使用する優先度を指定することで、この問題を解決できます。優先度を非常に低い~非常に高いに指定します。最高の優先度の役割は、他の役割に優先してスピーカーを使用できます。</p> <p>同じ役割の 2 人のユーザーが同時に通話しようとする場合、先着順の原則が適用されます。</p>

リモートレコーディングタブ（役割）

リモートレコーディングに対し、以下の権利を特定する：

名前	記述
リモートレコーディングの取得	リモートサイトのカメラ、マイク、スピーカー、ならびにメタデータデバイス、あるいはカメラのエッジストレージからクライアントの記録を取り出す権利を有効にする。

Smart Wall タブ（役割）

クライアントユーザーに対し、役割を通して以下の Smart Wall 機能に対するユーザー関連のユーザー権利を与える Smart Wall ことができます。

名前	記述
読み出し	クライアントの選択アイテムをユーザーが見ること Smart Wall を許可する。
編集	以下の選択アイテムをユーザーが編集することを許 Smart Wall 可する Management Client。
削除	以下の選択アイテムをユーザーが削除することを許 Smart Wall 可する Management Client。
操作	ユーザーがクライアントの選択アイテムにレイアウトを適用し、Smart Wall 選択されたプリセットをアクティブにすることを許可する。
プレイバック	クライアントの選択アイテムから記録されたデータをユーザーがプレイバックする Smart Wall ことを許可する。

外部イベントタブ（役割）

以下の外部イベント権利を特定する：

名前	記述
読み出す	ユーザーが、クライアントや以下の任意の外部システムイベントを検索し、見ることが許可します Management Client。
編集	ユーザーが、クライアントや以下の任意の外部システムイベントを編集することを許可します Management Client。
削除	ユーザーが、クライアントや以下の任意の外部システムイベントを削除することを許可します Management Client。
トリガー	ユーザーが、クライアントや以下の選択された外部システムイベントをトリガーすることを許可します。

ビューグループタブ（役割）

ビューグループ タブで、任意の役割 を持ったユーザーとユーザーグループが、クライアントでどのビューグループを使うことができるか特定します。

ビューグループの以下の権利を特定する。

名前	記述
読み出し	クライアントと以下のビューグループを見る権利を有効にする Management Client。ビューグループが以下に作成されます Management Client。
編集	以下のビューグループのプロパティを編集する権利を有効にする Management Client。
削除	以下のビューグループを削除する権利を有効にする Management Client。
操作	ビューグループを使用する権利を有効にする。 Network Video Management System Smart Client これにより、サブグループとビューの作成と削除が可能になります。

Matrix タブ(役割)

システムで、Matrix 受信者を設定している場合、Matrix 役割権限も設定します。クライアントから、選択した Matrix 受信者へビデオを送信できます。これを受信できるユーザーを Matrix タブで選択します。

以下の権限が利用できます。

名前	詳細
読み取る	選択した役割のユーザーおよびグループが、クライアントからビデオを選択して、Matrix 受信者へ送信できるかどうかを決定します。

警告タブ（役割）

システム設定において警告を使用して、中央部の概観やインストールの制御 Network Video Management System（他の全てのサーバーを含む）を提供する場合、警告 タブを使って、任意の役割を持つユーザー/グループが持つべき警告権（例えば、クライアントの警告の処理の仕方）を指定することができます。

警告に対し、以下の権利を指定する：

名前	記述
管理	警告を管理する（例えば、警告の優先度を変更する）、警告を他のユーザーへ委託する、警告を確認する、複数の警告のステータスを同時に変更する（例えば 新規 to から割り当て済へ変更）権利を有効にする。
ビュー	警告を見て、警告レポートを印刷する権利を有効にする。
警告を無効にする	警告を無効にする権利を有効にする。
通知の受信	クライアントの警告に関する通知を受信する権利を有効にする。

アクセスコントロールタブ(役割)

基本ユーザーや Windows のユーザー、グループを追加または編集する際に、アクセスコントロールの設定を指定できます。

名前	詳細
アクセスコントロールの使用	クライアントのアクセスコントロール関連の機能をユーザーが使用できるようにします。

MIP タブ (役割)

MIP ソフトウェア開発キット(SDK)によって、サードパーティーのベンダーは、お使いのシステム用のカスタムプラグイン（たとえば、外部アクセスコントロールシステムまたは同様の機能などとの統合）を開発できます。



プラグインのどの設定を変更するかは、関連するプラグインによります。**MIP** タブで、プラグインに最適なカスタム設定を見つけます。

基本ユーザー

基本ユーザーについて

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。これは、Active Directory を使用して追加された Windows ユーザーとは対照的です。

基本ユーザーの操作を行う際には、基本ユーザーと Windows ユーザーの違いを理解しておくことが重要です。

-  基本ユーザーは、ユーザー名とパスワードの組み合わせによって認証され、システム固有のものです。
-  Windows ユーザーは、Windows ログインを使って認証され、マシン固有のものです。

基本ユーザーの作成

基本ユーザーを作成するには：

1. セキュリティ > **基本ユーザー**を展開します。
2. 基本ユーザーペインを右クリックして、**基本ユーザーの作成**を選択します。
3. ユーザー名とパスワードを指定し、パスワードを再入力して、正しく入力されていることを確認します。
4. **OK** をクリックして、新しい基本ユーザーを作成します。

システムダッシュボード

システムダッシュボードについて

システムダッシュボードには、システムとコンポーネントを監視する機能があります。

次の機能にアクセスします。

名前	説明
システム監視	定義するパラメータでサーバーとカメラのステータスを監視します。
システム監視しきい値	システム監視で使用されるサーバーおよびモニタータイルで監視されるパラメータのしきい値を設定します。
現在のタスク	選択したレコーディングサーバーの実行中のタスクの概要を把握できます。
設定レポート	印刷する前に、システム設定レポートに何を含めるかを決定します。

システム監視について

システム監視では、システムのサーバーとカメラの現在の状態の概要が、システムハードウェアを表す色付きのタイルによって視覚的に表示され、簡単に確認できます。既定では、すべてのレコーディングサーバー、すべてのサーバー、およびすべてのカメラを表すタイルが表示されます。

タイルの色：

タイルの色	説明
緑	正常状態。すべてが正常に動作しています。
黄色	警告状態。1つ以上の監視パラメータが正常状態のしきい値 『193ページの"システム監視しきい値"参照』を超えています。
赤	重大状態。1つ以上の監視パラメータが正常状態と警告状態のしきい値を超えています。

ダッシュボードに表示するタイルの数を増減する場合は、サーバーおよびカメラタイルをカスタマイズできます。たとえば、1台のサーバー、1台のカメラ、カメラのグループ、またはサーバーグループを表すようにタイルを設定できます。また、タイルを使用しない場合や、監視パラメータを編集する場合は、タイルを削除できます。たとえば、監視パラメータは、CPU利用率またはサーバーの空きメモリなどです。これらのパラメータをサーバータイルから削除すると、タイルは該当するタイルでこれらのパラメータを監視しません。タブの右上端で**[カスタマイズ]**をクリックすると、**[ダッシュボードのカスタマイズ]**ウィンドウが開きます。詳細については、「ダッシュボードのカスタマイズ 『191ページ』」を参照してください。

システム監視しきい値で設定されたしきい値に基づいて、タイルの状態と色が変わります。システムではデフォルトしきい値の一部が設定されませんが、各3つの状態のしきい値を自分で決定できます。しきい値を設定または変更するには、システム監視しきい値を使用できます。「システム監視しきい値 『193ページ』」を参照してください。

タイルの色が変わり、タイルの色の変化につながるサーバー/パラメータを確認する場合は、タイルをクリックします。これにより、画面の下に概要が開き、タイルで有効にした各監視パラメータの色(赤、黄、緑)が表示されます。**【詳細】**ボタンをクリックすると、状態が変わった原因に関する詳細情報が表示されます。

タイルに警告記号が表示される場合は、監視対象のサーバーまたはカメラのいずれかのデータコレクタが実行されていない可能性があります。タイルの上にマウスを置くと、該当するタイルで最後にデータが収集された日時が表示されます。

ダッシュボードのカスタマイズ

新しいカメラまたはサーバータイルの追加

1. [システム監視]ウィンドウで**【カスタマイズ】**をクリックします。
2. **【ダッシュボードのカスタマイズ】**ウィンドウが表示されたら、**【サーバータイル】**または**【カメラタイル】**の下で**【新規】**をクリックします。
3. **【新しいサーバータイル/新しいカメラタイル】**ウィンドウで、監視するサーバーまたはカメラを選択します。
4. **【監視パラメータ】**の下で、該当するタイルから追加または削除するパラメータのチェックボックスをオンまたはオフにします。
5. **【OK】**をクリックします。新しいサーバーまたはカメラタイルがダッシュボードに表示されるタイルに追加されます。

監視パラメータの編集

1. [システム監視ダッシュボード]ウィンドウで**【カスタマイズ】**をクリックします。
2. **【ダッシュボードのカスタマイズ】**ウィンドウが表示されたら、**【サーバータイル】**または**【カメラタイル】**の下で**【編集】**をクリックします。
3. **【サーバータイルの編集】**または**【カメラタイルの編集】**ウィンドウで、編集するサーバーコンポーネントまたはカメラを選択します。
4. **【監視パラメータ】**ボックスで、該当するタイルから追加または削除する監視パラメータのチェックボックスをオンまたはオフにします。
5. **【OK】**をクリックします。変更された監視パラメータは、該当するタイルの一部か、該当するタイルから削除されます。

必要に応じて、システムの履歴データを有効および無効にできます。このデータを無効にする場合は、前のシステムの動作のグラフを表示できません。SQL Server データベースまたは帯域幅の負荷を低減する場合は、履歴データのサンプリング間隔を少なくすることができます。履歴データのサンプリング間隔を低くする場合は、グラフに表示される詳細が少なくなります。

システム監視の詳細

サーバーまたはカメラタイトルをクリックすると、ダッシュボードの下に選択した監視パラメータのステータスがそれぞれ表示されます。

State	Name	Live FPS	Recording FPS	Used space	
	Panasonic SPxxx/SFxxx/SWxxx no I/O Camera Series				Details

例：カメラのライブFPS監視パラメータが警告状態に達しました。

【状態】フィールドにはカメラの状態が表示されます。たとえば、デバイスへの接続が切断された場合は、赤色の警告が表示されます。アイコンにはツールチップがあり、警告の原因となる問題が簡単に説明されています。

【使用されているスペース】フィールドには、デバイスが以前に他のレコーディングサーバー上にあった場合など、このデバイスの録画がある他のレコーディングサーバーのデータが表示されます。

該当するカメラ/サーバーの**【詳細】**ボタンをクリックすると、システム情報を表示し、次の項目に関するレポートを作成できます。

コンポーネント	説明
管理サーバー	選択した管理サーバーのデータを表示します
レコーディングサーバー	選択したレコーディングサーバーのデータを表示します。以下を元に表示できます。 <ul style="list-style-type: none"> • ディスク • ストレージ • ネットワーク • カメラ
追加のサーバー	ログサーバー、イベントサーバーなどでデータを表示します。
カメラ	設定にある任意のカメラグループの任意のカメラでデータを表示します。

これらの各要素は、クリックして展開できます。この領域をクリックすると、このサーバーまたはカメラの関連する動的データが表示されます。

カメラバーには、選択の対象となるカメラグループのリストが含まれています。グループを選択すると、特定のカメラを選択してその動的データを表示することができます。すべてのサーバーで、CPU使用率および使用可能メモリの情報を表示します。レコーディングサーバーも、接続ステータスの情報を表示します。それぞれのビューには、履歴リンクがあります。それをクリックすると、履歴データとレポートが表示されます(カメラのレポートを表示するには、カメラの名前をクリックします)。それぞれの履歴レポートで、最近24時間、7日または30日のデータを表示できます。レポートを保存および/または印刷するには、PDFへ送信アイコンをクリックします。<およびホームアイコンを使用して、システム監視をナビゲートできます。

デバイスが現在存在するレコーディングサーバーのデータを使用した場合にのみ履歴レポートを作成できます。

重要：サーバーのオペレーティングシステムからシステム監視の詳細にアクセスした場合、Internet Explorer Enhanced Security Configurationに関連するメッセージが表示されることがあります。メッセージの指示に従って、システム監視のページを信頼済みサイトゾーンに追加してから続行してください。

システム監視しきい値

システム監視しきい値では、サーバーの CPU 利用率が正常な状態（緑）から警告状態（黄）に変化した場合など、システム監視によってシステムのハードウェア状態が変更されたことが視覚的に示されるときにグローバルしきい値を設定および調整できます。

システムはデフォルトしきい値で設定されているため、システムが設定された時点からシステムハードウェアの監視を開始できます。これらの値は任意の時点で変更できます 『194ページ の"システム監視しきい値の設定"参照』。

デフォルトでは、システムは、すべてのサーバーまたはカメラなど、特定のハードウェアのすべてのユニットのしきい値を表示するように設定されています。個別のサーバーまたはカメラ、あるいはこれらのサブセットに対してしきい値を設定することもできます。たとえば、一部のカメラが他のカメラよりも高い**ライブ FPS**または**録画 FPS**を使用することを許可する場合などに、個別のサーバーまたはカメラのしきい値を設定することが有効な場合があります。

サーバー、カメラ、ディスク、ストレージのしきい値を設定できます。しきい値を変更する場合は、しきい値コントロールスライダを使用できます。しきい値コントロールスライダでは、状態を区別するハンドルを上下にドラッグし、しきい値を増減できます。しきい値コントロールスライダは、システム監視 『190ページ の"システム監視について"参照』のサーバーまたはカメラタイトルで表示されるのと同様の色に分割されます。

システムハードウェアの使用状況または負荷が約 1 秒間高いしきい値に達したときに**重大**または**警告**状態を表示しないようにするには、**【計算間隔】**を使用します。**【計算間隔】**は、システムハードウェア状態の短い変化や頻繁な変化の効果を平均化します。実際には、**【計算間隔】**は経時的なハードウェアの変化の効果を均一化するため、しきい値が超過するたびにアラートを受信することがありません。

たとえば、**【計算間隔】**を 1 分に設定すると、1 分間の平均値がしきい値を超えた場合にのみアラートが発生します。この利点は、ハードウェア状態の頻繁な変化や場合によっては関連のない変化に関するアラートを回避し、CPU の利用率やメモリ消費などの持続的な問題を反映するアラートのみが発生することです。

サーバーしきい値

しきい値	説明	単位
メモリ	監視するサーバーで使用する RAM メモリのしきい値。	MB
CPU 使用率	監視するサーバーの CPU 利用率のしきい値。	%

カメラしきい値

しきい値	説明	単位
使用されているスペース	監視するカメラが使用する領域のしきい値。	GB
FPS を記録	システムが監視するカメラでビデオを記録するときに使用中のカメラの FPS しきい値。	%
ライブ FPS	システムが監視するカメラでライブビデオを表示するときに使用中のカメラの FPS しきい値。	%

ディスクしきい値

しきい値	説明	単位
空きスペース	監視するディスクの空き領域のしきい値。	GB

ストレージしきい値

しきい値	説明	単位
保持期間	ストレージの領域が不足するときの推定時期を表示するしきい値。表示される状態はシステム設定に基づき、1日に2回更新されます。	日

また、ルール『150ページ の"ルールについて"参照』を設定して、特定のアクションを実行するか、しきい値の状態が変化するときアラーム『200ページ の"アラームについて"参照』をアクティブ化できます。

システム監視しきい値の設定

1. まだ有効にしていない場合は、関連するシステムハードウェアの**【有効にする】**チェックボックスを選択します。
2. しきい値コントロールスライダを上下にドラッグし、しきい値を増減します。しきい値コントロールに表示される各システムハードウェアで使用可能なスライダは2つあり、**正常**、**警告**、および**重大**レベルを識別します。
3. 関連するしきい値レベルを設定したら、メニューから**【ファイル】** > **【保存】**を選択します。



しきい値コントロールスライダを設定する方法の例。スライダを上下にドラッグし、3つのしきい値レベルの任意の項目を増減します。赤は重大状態に達したことを意味します。黄色は警告状態で、まもなく重大状態に達することを示します。緑は正常の状態で、選択したしきい値内であることを示します。

現在のタスクについて

現在のタスク ノードは任意の記録サーバーのタスクの概要、始動時刻、推定終了時刻と経過 を表示します。現在のタスク に表示される全ての 情報はスナップショットです。プロパティ パネルの右下角にある **更新ボタン**をクリックして更新することができます。

設定レポートについて

PDF 設定レポートを作成する際、システムのあらゆる要素をレポートに含めることができます。例えば、ライセンス、デバイス設定、アラーム設定などを含めることが可能です。また、フォントとページの設定をカスタマイズしたり、カスタマイズした表紙を含めることができます。

設定レポートの追加

1. システムダッシュボードを展開して、**設定レポート**をクリックします。これによりレポート設定ページが開きます。
2. レポートに含める要素を選択します。
3. **オプション:表紙**をクリックして表紙をカスタマイズします。表示されるウィンドウで、必要な情報を入力します。レポートに含める要素として**表紙**を選択します。選択しないと、カスタマイズする表紙はレポートに含まれなくなります。
4. **フォーマット**をクリックして、フォント、ページのサイズ、余白をカスタマイズします。表示されるウィンドウで、必要な設定を選択します。
5. エクスポートする準備ができたなら、**エクスポート**をクリックし、名前を選択して、レポートの保存場所を選択します。

設定レポートの詳細

以下は、レポート設定時に使用できます。

名前	詳細
全て選択	リストのすべての要素を選択します。
全てクリアする	リストのすべての要素をクリアします。
表紙	レポートの表紙をカスタマイズします。
フォーマット	レポートをフォーマットします。
エクスポート	レポートの保存場所を選択して PDF を作成します。

サーバーログ

ログについて

システムに関連付けられた異なるログから、コンテンツを表示およびエクスポートできます。ログの目的は、後から分析または文書化するために、システムのアクティビティ、イベント、アクション、およびエラーを記録することです。

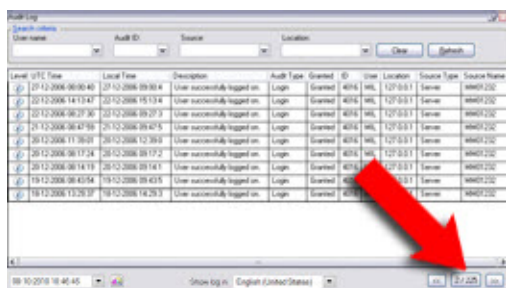
ログにはさまざまな目的があります。

名前	詳細
システムログ	システム関連情報を記録します。
監査ログ	ユーザーアクティビティを記録します。
ルールログ	ユーザーが新しいログエントリの作成アクションを指定したルールを記録します。

システムには異なるログに関連するデフォルト設定があります。設定を変更するには、オプションのサーバーログタブ 『209ページ の"サーバーログタブ(オプション)"参照 』を参照してください。

さまざまな言語でログを表示し、タブ区切りテキスト (.txt) ファイルとしてエクスポートできます。

ログに情報が複数ページ含まれる場合、ログペインの右下角のボタンをクリックして、ログページを移動できます。



左下角で、ログの特定の日時にジャンプできます。



ログの検索

ログを検索するには、ログペインの上部の**検索条件**を使用します。

1. リストから検索条件を指定します。
2. **更新**をクリックし、ログページに検索条件を反映させます。検索条件をクリアし、ログの内容のすべてを表示するには、**クリア**をクリックします。


列をダブルクリックして、**ログの詳細**ウィンドウにすべての詳細を表示することもできます。このように、1行に表示しきれないテキストを含むログエントリを読み取ることもできます。

ログのエクスポート

タブ区切りテキスト (.txt) ファイルとしてログをエクスポートできます。エクスポートに含めるログ、ログ要素、時間範囲を指定して、ログの内容をカスタマイズできます。たとえば、2016年1月2日08:00:00から2016年1月4日07:59:59までの間のシステムログのエラー関連ログエントリのみエクスポートするよう指定することができます。

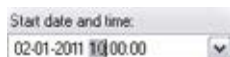
ログをエクスポートするには：

1. **エクスポートログ**ウィンドウの**ファイル名**フィールドで、エクスポートしたログファイルの名前を指定します。

デフォルトでは、**マイドキュメント**フォルダにエクスポートしたファイルが保存されます。ただし、フィールド横の参照ボタンをクリックすれば、別の場所を指定することもできます。

2. エクスポートしたログの内容を対象にするよう選択した条件は、**フィルター**フィールドに記載されます。このフィールドは編集できません。条件を変更する必要性が生じた場合は、ウィンドウを閉じ、手順 1～2 を繰り返します。
3. エクスポートに含める時間を指定します。**開始日時**と**終了日時**の各フィールドを指定します。矢印をクリックすると、日付を選択できます。

正確な時間を指定するには、時間要素（時：分：秒）に必要な値を上書きします。この例では、時間要素が上書きされます。



4. **エクスポート**をクリックし、ログの内容をエクスポートします。

ログ言語の変更




1. ログペインの下部分にある、**ログインを表示**リストで、必要な言語を選択します。



2. ログが選択した言語で表示されます。次回ログを開くと、デフォルト言語にリセットされます。

システムログ（プロパティ）

ログの各列はログエントリを表します。ログエントリにはさまざまな情報フィールドがあります。

名前	詳細
レベル	ログエントリのレベルを示すアイコンを表示します。  - 情報を示します  - 警告を示します  - エラーを示します 「ブランク」 - 未定義のエントリを示します。
協定世界時時刻	協定世界時（UTC）のタイムスタンプ。
ローカル時間	システムのサーバーのローカル時間のタイムスタンプ。
ID	記録されたインシデントの識別番号。
ソースタイプ	記録したインシデントが発生した機器のタイプ（サーバーまたはデバイスなど）。
ソース名	管理サーバー、記録されたインシデントが発生したレコーディングサーバーまたはデバイスの名前。
イベントタイプ	記録されたインシデントで表されたイベントのタイプ。
詳細	記録されたインシデントの説明を表示します。




監査ログ (プロパティ)

ログの各列はログエントリを表します。ログエントリにはさまざまな情報フィールドがあります。

名前	詳細
レベル	<p>ログエントリのレベルを示すアイコンを表示します。</p> <ul style="list-style-type: none">  - 情報を示します  - 警告を示します  - エラーを示します <p>「ブランク」 - 未定義のエントリを示します。</p>
協定世界時時刻	協定世界時 (UTC) のタイムスタンプ。
ローカル時間	システムのサーバーのローカル時間のタイムスタンプ。
ID	記録されたインシデントの識別番号。
ユーザー	記録されたインシデントを引き起こすリモートユーザーのユーザー名。
ユーザーの場所	リモートユーザーが記録されたインシデントを引き起こしたコンピュータの IP アドレスまたはホスト名。
許可	リモートユーザーアクションが可能か (許可されているか) どうかについての情報。
カテゴリ	記録したインシデントのタイプ。
リソースタイプ	記録したインシデントが発生した機器のタイプ (サーバーまたはデバイスなど)。
リソース名	管理サーバー、記録されたインシデントが発生したレコーディングサーバーまたはデバイスの名前。
リソースホスト	<p>記録されたインシデントが発生したデバイスまたはストレージをホストするレコーディングサーバーの名前。</p> <p>記録されたインシデントが発生したレコーディングサーバーまたは管理サーバーをホストする管理サーバーの名前。</p>
詳細	記録されたインシデントの説明を表示します。

ルールログ (プロパティ)

ログの各列はログエントリを表します。ログエントリにはさまざまな情報フィールドがあります。

名前	詳細
レベル	<p>ログエントリのレベルを示すアイコンを表示します。</p> <ul style="list-style-type: none">  - 情報を示します  - 警告を示します  - エラーを示します <p>「ブランク」 - 未定義のエントリを示します。</p>

名前	詳細
協定世界時時刻	協定世界時（UTC）のタイムスタンプ。
ローカル時間	システムのサーバーのローカル時間のタイムスタンプ。
ID	記録されたインシデントの識別番号。
サービス名	記録されたインシデントが発生したサービスの名前。
ルール名	ログエントリをトリガするルールの名前。
ソースタイプ	記録したインシデントが発生した機器のタイプ（サーバーまたはデバイスなど）。
ソース名	管理サーバー、記録されたインシデントが発生したレコーディングサーバーまたはデバイスの名前。
イベントタイプ	記録されたインシデントで表されたイベントのタイプ。
生成プログラムタイプ	記録されたインシデントがトリガされた機器のタイプ。ログエントリは管理者が定義し、システムのインシデントに関連付けられます。
生成プログラム名	記録されたインシデントが生成された機器の名前。
詳細	記録されたインシデントの説明を表示します。

アラーム

アラーム設定について

アラーム設定には以下が含まれます。

- アラーム処理のダイナミックな役割ベース設定
- 全コンポーネントの一元的な技術概要：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
- プラグインの処理、外部アクセスコントロールまたはVCAベースシステムなどの他のシステムとのカスタム統合が可能です。

一般的に、アラームを発生させるオブジェクトの視認性によりアラームが制御されます。これにより、アラームに関する4つの側面を活用でき、制御/管理するユーザーと、制御/管理の度合いが関連します。

名前	詳細
ソース/デバイス視認性。	アラームを発生させるデバイスが、ユーザーの役割で認識できるように設定されていない場合、ユーザーはNetwork Video Management System 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。

名前	詳細
ユーザー定義イベントをトリガする権限	この権限は、ユーザーの役割が Network Video Management System Smart Client の選択したユーザー定義イベントをトリガできるかどうかを決定します。
外部プラグイン	外部プラグインがシステムに設定されている場合、これらは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。
一般役割権限	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します。 アラームのユーザーがアラームにできることは、ユーザーの役割とその役割に課された設定により異なります。

オプションのイベントサーバータブで、アラーム、イベント、ログの設定を指定できます。

アラームについて

重要：この機能は、Network Video Management System イベントサーバーがインストールされていないと動作しません。

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

- 内部システム関連のイベント

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

- 外部統合イベント

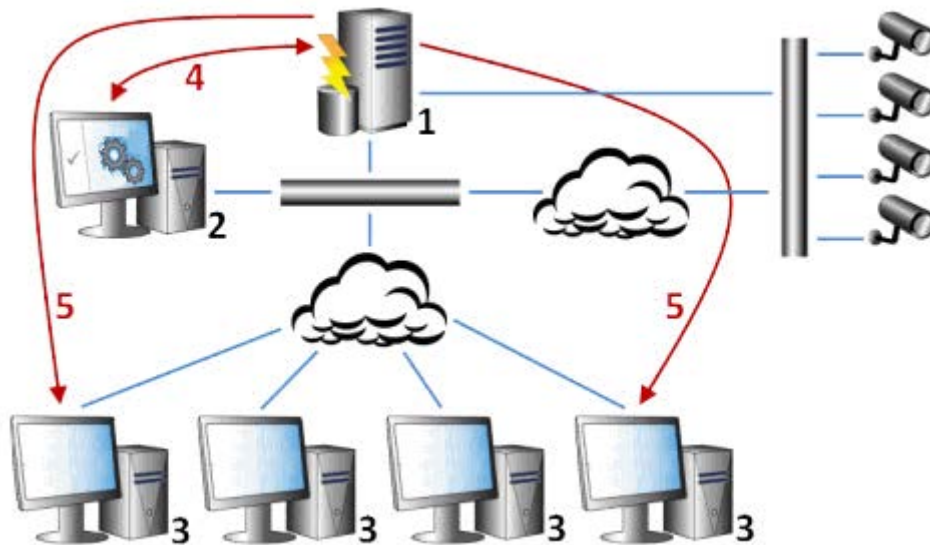
複数の種類の外部イベントからこのグループを構成することができます。

- アナリティック イベント

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)プロバイダから受け取ったデータ。

- MIP プラグインイベント

MIP ソフトウェア開発キット(SDK)によって、サードパーティーのベンダーは、お使いのシステム用のカスタムプラグイン（たとえば、外部アクセスコントロールシステムまたは同様の機能などとの統合）を開発できます。



凡例：

1. 監視システム
2. Management Client
3. Network Video Management System Smart Client
4. アラーム設定
5. アラームデータフロー

アラームを処理し、Network Video Management System Smart Client にあるアラームリストに委譲します。また、アラームを Network Video Management System Smart Client のマップ機能に統合できます。

アラーム定義

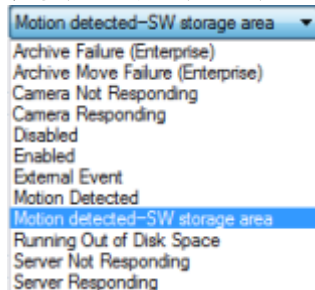
システムがイベントをシステムに登録する際は、システムを Network Video Management System Smart Client でアラームを生成するように設定できます。これらを使用する前にアラームを定義する必要があります。アラームはシステムサーバーに登録したイベントに基づき定義してください。また、ユーザー定義イベントを使用してアラームをトリガすることもできます。同じイベントを使用して複数の異なるアラームをトリガすることもできます。

アラームの追加

アラームを定義するには、アラーム定義を作成する必要があります。ここでは、アラームをトリガーする項目、オペレータが実行する必要がある作業の手順、アラームを停止させる操作やタイミングなどを指定します。設定の詳細については、「アラーム定義（プロパティ）『202ページ』」を参照してください。

1. サイトナビゲーションペインで、アラームを展開し、アラーム定義を右クリックします。
2. 新規追加を選択します。
3. 次のプロパティを入力します：

- **名前** : アラーム定義の名前を入力します。アラーム定義が一覧表示されるたびに、アラーム定義の名前が表示されます。
- **手順** : アラームを受信するオペレータの手順を作成できます。
- **イベントのトリガ** : ドロップダウンメニューを使用して、アラームがトリガされるときに使用されるイベントタイプとイベントメッセージを選択します。



選択可能なトリガイベントのリスト。分析イベントを使用して、ハイライトされたイベントが作成され、カスタマイズされます。

- **ソース** : アラームをトリガするためのイベントが発生するカメラおよびその他のデバイスを選択します。選択できるオプションは、選択したイベントのタイプにより異なります。
 - **時間設定** : 特定の期間中にアラームをアクティブ化する場合、ラジオボタンを選択してから、ドロップダウンメニューでタイムインターバルを選択します。
 - **対象のイベント** : イベントによってアラームをアクティブ化する場合、ラジオボタンを選択し、アラームを開始するイベントを指定します。また、アラームを停止するイベントも指定する必要があります。
4. **【時間制限】**ドロップダウンメニューで、オペレータのアクションが必要なときの時間制限を指定します。
 5. **【トリガされたイベント】**ドロップダウンメニューで、時間制限が経過したときにトリガするイベントを指定します。
 6. 関連するカメラや初期アラーム所有者などの追加設定を指定します。

アラーム定義（プロパティ）

表には、アラーム定義を作成するときに作成できる設定を示します。

アラーム定義の設定 :

名前	詳細
有効	既定では、アラーム定義は有効です。無効にするには、チェックボックスをオフにします。
名前	アラームの名前は一意である必要はありませんが、一意で分かりやすい名前を使用すると、多くの場合に便利です。

名前	詳細
手順	アラームに関する説明や、アラームの原因となる問題を解決する方法についてのテキストを入力します。 ユーザーがアラームを処理すると、テキストが Network Video Management System Smart Client で表示されます。
イベントのトリガ	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。2つのドロップダウンから選択します。 <ul style="list-style-type: none"> 1つ目のドロップダウン:アナリティックイベントやシステムイベントなどのイベントのタイプを選択します。 2つ目のドロップダウン:使用する特定のイベントメッセージを選択します。使用可能なメッセージは、最初のドロップダウンメニューで選択したイベントタイプによって異なります。
ソース	イベントが発生するソースを指定します。カメラまたは他のデバイスから切断し、ソースは、VCA や MIP などの定義済みのソースに接続することもできます。選択できるオプションは、選択したイベントのタイプにより異なります。

アラームトリガ:

名前	詳細
時間設定	[時間設定] ラジオボタンを選択して、アラーム定義がアクティブな間隔を指定します。 [ルールとイベント] ノードで定義した時間設定だけが一覧に表示されます。何も定義されていない場合は、 [常時] オプションのみを使用できます。
対象のイベント	イベントに基づくアラームにするには、このラジオボタンを選択します。選択した後は、開始イベントと停止イベントを指定します。カメラ、ビデオサーバーおよび入力で定義されたハードウェアイベント 『145ページの"イベント概要"参照』を選択できます。また、グローバル/手動イベント定義 『163ページの"ユーザー定義イベントについて"参照』も使用できます。

オペレータのアクションが必要:

名前	詳細
時間制限	オペレータのアクションが必要になる時間制限を選択します。デフォルトは1分です。 [トリガされたイベント] ドロップダウンメニューでイベントを登録するまで、時間制限はアクティブになりません。
イベントがトリガーされました	時間制限が経過した場合に、どのイベントをトリガするかを選択します。

追加設定：

名前	詳細
関連するカメラ	カメラ自身がアラームをトリガしない場合でも、15 台までアラーム定義に含めるカメラを選択します。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。ドア付近のカメラを 1 台または複数定義することで、定義したカメラの録画のインシデントをアラームに関連付けることができます。
関連するマップ	Network Video Management System Smart Client のアラームマネージャのリストに表示されている場合は、アラームにマップを割り当てます。
初期アラームの所有者	アラームに対して責任を負うデフォルトのユーザーを選択します。
初期アラームの優先度	アラームの優先度（高、中、低またはなし）を選択します。優先度を Network Video Management System Smart Client で使用して、アラームの重要度を決定します。
初期アラームのカテゴリ	アラームのカテゴリ、例えば 誤警報 または 要調査 を選択します。
アラームでトリガされるイベント	アラームが Network Video Management System Smart Client でトリガできるイベントを定義します。
アラームを自動で閉じる	特定のイベントによってアラームを自動的に停止する場合は、このチェックボックスを選択します。すべてのイベントがアラームをトリガするわけではありません。最初から新しいアラームを無効にしたい場合は、チェックボックスを選択解除します。

参照

アラームの追加 『201ページ』

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

優先度

名前	詳細
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 または 3）を使用/編集します。これらの優先度レベルは、 初期アラームの優先度 設定を行うために使用されます。
名前	エンティティの名前を入力します。必要な数だけ作成できます。
サウンド	アラームに関連付け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 に追加します。

ステータス

名前	詳細
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、Network Video Management System Smart Client のアラームリストにのみ表示されます。

カテゴリ

名前	詳細
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

名前	詳細
使用できる列	>を使用して Network Video Management System Smart Client のアラームリストに表示される列を選択します。<を使用して選択をクリアします。完了したら 選択した列 には、含める項目が表示されます。

終了の理由タブ

名前	詳細
有効	すべてのアラームが閉じられる前に、閉じる理由を割り当てる必要があるようにするには、選択して有効にします。
理由	アラームを閉じる際にユーザーが選択できる、閉じる理由を追加します。この例は、 解決済み-侵入者 または 偽警告 です。必要な数だけ作成できます。

音声の設定

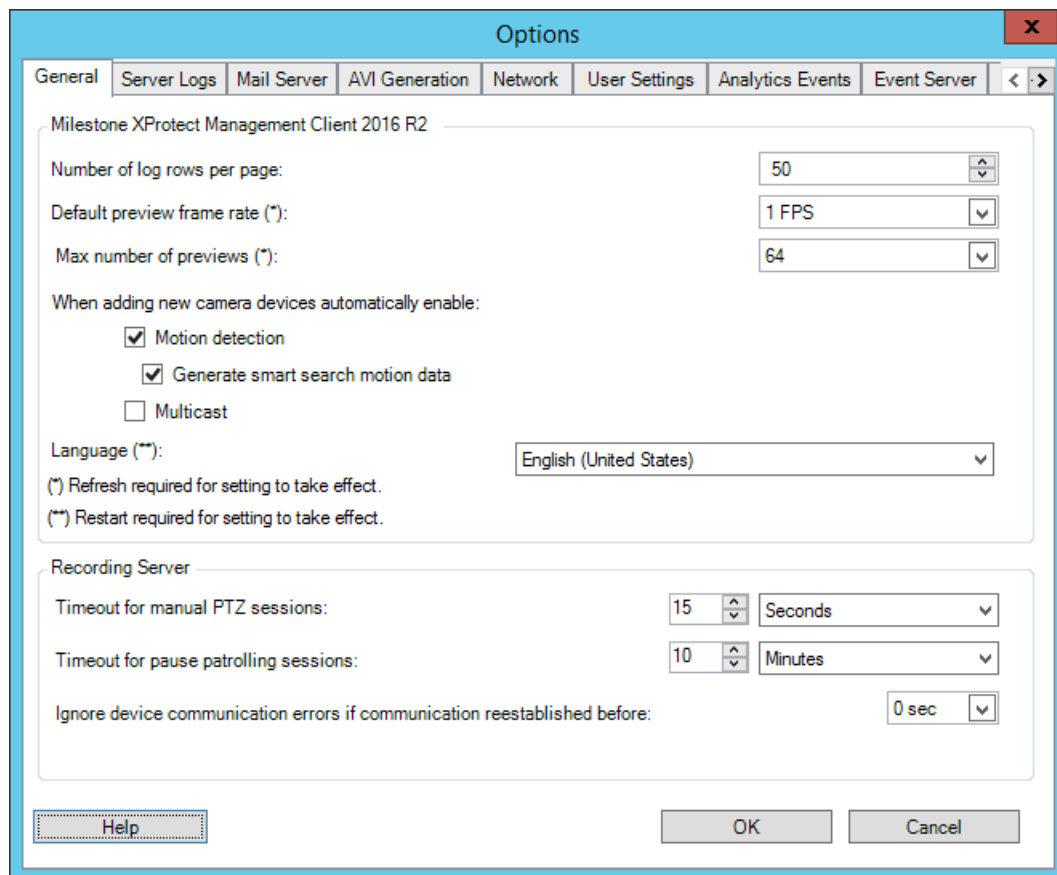
音の設定を行う際には、以下を指定します。

名前	詳細
音声	<p>アラームに関連付け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。</p> <p>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、マシンにより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。</p>
追加	音声を追加します。1 つ以上の.wav ファイルをアップロードするための音をブラウズできます。
削除	選択された音を、手動で追加された音の一覧から削除します。デフォルト音は削除できません。
Test	音をテストします。リストから音を選択します。音が 1 回再生されます。

オプションダイアログボックス

オプションダイアログボックスで、全般的な表示およびシステムの機能に関連する複数の設定を指定できます。

ダイアログボックスにアクセスするには、ツール > オプションを選択します。



オプションダイアログボックスは以下のタブで構成されます。

- 一般タブ 『207ページ の"一般タブ (オプション)"参照 』
- サーバーログタブ 『209ページ の"サーバーログタブ(オプション)"参照 』
- メールサーバータブ 『210ページ の"メールサーバータブ(オプション)"参照 』
- AVI 生成タブ 『210ページ の"AVI 生成タブ(オプション)"参照 』
- ブックマークタブ
- 証拠ロックタブ
- アナリティックイベントタブ 『211ページ の"アナリティックイベントタブ(オプション)"参照 』
- イベントサーバータブ 『212ページ の"イベントサーバータブ(オプション)"参照 』
- ジェネリックイベントタブ 『213ページ の"ジェネリックイベントタブ(オプション)"参照 』

一般タブ (オプション)

一般タブで、Management Client およびレコーディングサーバーの一般設定を指定できます。

Management Client

名前	説明
ページ当りのログ列数 :	単一のログページに含まれる列数を選択します。デフォルトは 50 列です。ログにより多くの列が含まれている場合は、追加のページに追加の列が表示されます。
デフォルトのプレビューフレームレート	プレビューペインに表示されるサムネイルカメラ画像で使用するためのフレームレートを選択できます。デフォルトは、1 秒当たり 1 フレームです。 メニューから アクション > 更新 を選択して変更を有効にします。 プレビューペインで、高いフレームレートで多数のサムネイル画像を同時に使用すると、Management Client を実行するコンピュータの動作が遅くなる場合があります。プレビューの 最大数 設定で、サムネイル画像数の制限を設定することができます。
プレビューの最大数	プレビューペインに表示されるサムネイル画像の最大数を選択できます。デフォルトは、64 個のサムネイル画像です。 メニューから アクション > 更新 を選択して変更を有効にします。 多数のサムネイル画像で高いフレームレートを同時に使用すると、システムの動作が遅くなる場合があることに注意してください。デフォルトの プレビューフレームレート 設定で、サムネイル画像に使用するフレームレートを制限することができます。
新しいカメラデバイスを追加するときに自動的に有効にします : モーション検知	ハードウェアの追加ウィザード を使ってシステムに追加する際に、チェックボックスを選択して新規カメラでモーション検知を有効にします。 この設定は既存のカメラのモーション検知設定に影響しません。 カメラデバイスの モーション タブで、カメラのモーション検知を有効化/無効化できます。
新しいカメラデバイスを追加するときに自動的に有効にします : スマート検索用のモーションデータを生成	スマート検索モーションデータを生成するには、カメラのモーション検知が有効でなければなりません。 ハードウェアの追加ウィザード を使ってシステムに追加する際に、チェックボックスを選択して新規カメラでスマート検索モーションデータの生成を有効にします。 この設定は既存のカメラのモーション検知設定に影響しません。 カメラデバイスの モーション タブで、カメラのスマート検索モーションデータの生成を有効化/無効化できます。
新しいカメラデバイスを追加するときに自動的に有効にします : マルチキャスト	ハードウェアの追加ウィザード を使って追加する際に、チェックボックスを選択して新規カメラでマルチキャストを有効にします。 この設定は既存のカメラのマルチキャスト設定に影響しません。 カメラデバイスの クライアント タブで、カメラのライブマルチキャストを有効化/無効化できます。
言語	Management Client の言語を選択します。 新しい言語を使用するには、Management Client を再起動します。

レコーディングサーバー

名前	説明
PTZセッションのタイムアウト	必要な権限を持つクライアントユーザーは、PTZカメラのパトロールを手動で中断できます。手動停止後に通常のパトロールを再開するまでに必要な時間を指定します。この設定は、システムのPTZカメラすべてに適用されます。
一時停止パトロールセッションのタイムアウト	十分なPTZ優先度のクライアントユーザーはPTZカメラでのパトロールを一時停止できます。一時停止後に通常のパトロールを再開するまでに必要な時間を指定します。この設定は、システムのPTZカメラすべてに適用されます。デフォルトは10分です。 カメラで個別のタイムアウトを設定する場合は、カメラの【プリセット】タブで指定します。
通信が右記より前に再確立される場合は、デバイスの通信エラーを無視します	通信エラーが発生してから、システムログにエラーが記録され、通信エラーイベントがトリガされるまでの時間を選択します。

サーバーログタブ(オプション)

サーバーログタブで、システムの管理サーバーログの設定を指定できます。

詳細はログについて 『195ページ』 もご覧ください。

名前	詳細
ログ	設定するログを選択します。 <ul style="list-style-type: none"> システムログ 監査ログ ルールログ

名前	詳細
ヤロカ	<p>ログを無効/有効にして各ログの保持時間および最大行数を指定します。 システムログで、記録するメッセージレベルを指定します。</p> <ul style="list-style-type: none"> • すべて - 未定義のメッセージを含みます • 情報、警告およびエラー • 警告とエラー • エラー (デフォルト設定) <p>監査ログで、Network Video Management System Smart Client のすべてのユーザーアクションを記録する場合は、ユーザーアクセスログを有効にします。たとえば、エクスポート、出力の有効化、ライブまたは再生での表示が含まれます。</p> <p>次を指定します。</p> <ul style="list-style-type: none"> • 再生シーケンスの長さ。つまり、ユーザーがこの期間内で再生している限り、1つのログエントリだけが生成されます。期間外で再生すると、新しいログエントリが作成されます。 • システムがログエントリを作成する前にユーザーが表示する記録(フレーム)数。

メールサーバータブ(オプション)

メールサーバータブで、システムの送信 SMTP メールサーバーの設定を指定できます。
通知プロファイルについて 『160ページ』 もご覧ください。

名前	詳細
送信者の E メールアドレス	すべての通知プロファイルで、E メールによる通知の送信者として表示する E メールアドレスを入力します。例：sender@organization.org
送信メール(SMTP)サーバー名	E メール通知を送信する SMTP メールサーバーの名前を入力します。例：mailserver.organization.org
サーバーのログインが必要です	メールサーバーにログインするユーザーのユーザー名およびパスワードを指定します。

AVI 生成タブ(オプション)

AVI 生成タブで、AVI ビデオクリップファイルの生成の圧縮設定を指定できます。これらの設定は、ルール起動通知プロファイルにより送信される E メール通知に AVI ファイルを含める場合に必要になります。

E メール通知をトリガするルールを使用する 『161ページ』 もご覧ください。

名前	詳細
圧縮プログラム	適用するコーデック（圧縮/解凍技術）を選択します。リストに使用可能なコーデックをより多く含むには、管理サーバーにコーデックをインストールします。 すべてのカメラがコーデックに対応しているわけではありません。
圧縮品質	（すべてのコーデックで利用できるわけではありません）。スライダーを使用して、コーデックが実行する圧縮の度合い（ 0-100 ）を選択します。 0 は、圧縮なしという意味です。これは通常高画質で、ファイルサイズが大きくなります。 100 は、最大の圧縮という意味です。これは通常低画質で、ファイルサイズが小さくなります。 スライダーが利用できない場合、圧縮の質は選択されたコーデックによって決定されます。
キーフレームごと	（すべてのコーデックで利用できるわけではありません）。キーフレームを使用する場合、このチェックボックスをオンにして、キーフレーム間の必要なフレーム数を指定します。 キーフレームは、指定された間隔で保存された単一のフレームです。キーフレームはカメラのビュー全体を記録しますが、続くフレームは変化したピクセルだけを記録します。これにより、ファイルのサイズを大幅に縮小できます。 チェックボックスが使用できない、または選択されていない場合は、各フレームにカメラのビュー全体が含まれます。
データ転送速度	（すべてのコーデックで利用できるわけではありません）。特定のデータ転送速度を使用する場合、このチェックボックスをオンにして、秒当たりのキロバイト数を指定します。 データ速度は添付されている AVI ファイルのサイズを指定します。 このチェックボックスが利用できない場合、またはオンになっていない場合、データ転送速度は選択されたコーデックによって決定されます。

ネットワークタブ(オプション)

ネットワークタブで、クライアントがインターネット経由で録画サーバーに接続する場合は、ローカルクライアントの IP アドレスを指定できます。これにより、監視システムはローカルネットワークから来ていると認識します。

システムの IP バージョンも指定できます。IPv4 または IPv6。デフォルト値は IPv4 です。

ユーザー設定タブ(オプション)

ユーザー設定タブで、リモート記録が有効な場合にメッセージを表示するかどうかなどのユーザーの優先設定を指定できます。

アナリティックイベントタブ(オプション)

アナリティックイベントタブで、アナリティックイベント機能を有効にして指定できます。

名前	詳細
有効	アナリティックイベントを使用するかどうかを指定します。デフォルトでは、この機能は無効になっています。
ポート	この機能で使用するポートを指定します。デフォルトポートは 9090 です。 関連する VCA ツールプロバイダもこのポート番号を使用するようにしてください。ポート番号を変更した場合、プロバイダのポート番号も変更するようにしてください。
すべてのネットワークアドレスまたは指定ネットワークアドレス	すべての IP アドレス/ホスト名からのイベントが許可されるのか、またはアドレスリスト（以下を参照）で指定された IP アドレス/ホスト名からのイベントだけが許可されるのかを指定します。
アドレスリスト	信頼済み IP アドレス/ホスト名のリストを指定します。このリストは、特定の IP アドレス/ホスト名のイベントのみが許可されるように受信されるデータをフィルタリングします。ドメイン名システム (DNS)、IPv4 および IPv6 アドレス形式の両方を使用できます。 各 IP アドレスまたはホスト名を手動で入力するか、またはアドレスの外部リストをインポートすることで、アドレスをリストに追加できます。 <ul style="list-style-type: none"> ● マニュアル入力: アドレスリストに IP アドレス/ホスト名を入力します。必要なアドレスを繰り返します。 ● インポート: インポートをクリックして、アドレスの外部リストを参照します。外部リストは.txt ファイル形式で、各 IP アドレスまたはホスト名は別の行に表示させる必要があります。

イベントサーバータブ(オプション)

イベントサーバータブで、アラーム、イベント、ログの設定を指定できます。

名前	詳細
終了したアラームの保持期間	終了したアラームを保存する日数を選択します。終了したアラームは 処理済み、無視、および拒否 ステータスです。
他のすべてのアラームの保持期間	処理済み、無視、および拒否 ステータス以外の他のすべてのアラームの保存日数を選択します。 重要: アラームには常にタイムスタンプが含まれます。アラームがカメラによりトリガされる場合は、タイムスタンプにはアラームの時間からの画像が含まれます。アラーム情報自体はイベントサーバーに保存されますが、添付画像に対応するビデオ記録は、関連する監視システムサーバーに保存されます。 アラームの画像を表示するには、ビデオ録画が少なくともイベントサーバーにアラームを保存する期間以上、保存されるようにする必要があります。
イベントの保持期間	イベントの保存日数を指定できます。

名前	詳細
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。サーバーの容量が許す限り99.999日まで設定することができます。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。
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する場合は、チェックボックスを選択します。

ジェネリックイベントタブ(オプション)

ジェネリックイベントタブで、ジェネリックイベントとデータソース関連の設定を指定できます。

実際のジェネリックイベントの設定方法についての詳細は、ジェネリックイベントについて『168ページ』をご覧ください。

名前	詳細
データソース	<p>2つのデフォルトデータソースから選択してカスタムデータソースを定義できます。選択内容は、お使いのサードパーティ製プログラムおよび/またはインターフェース対象となるハードウェアまたはソフトウェアによって異なります。</p> <p>互換: 工場出荷時のデフォルト設定が有効。すべてのバイトをエコー。TCPおよびUDP。IPv4のみ。ポート1234。区切り文字なし。ローカルホストのみ。現在のコードページエンコーディング(ANSI)。</p> <p>インターナショナル: 工場出荷時のデフォルト設定が有効。統計のみをエコー。TCPのみ。IPv4+6。ポート1235。<CR><LF>を区切り文字として使用。ローカルホストのみ。UTF-8エンコーディング。(<CR><LF> = 13,10)。</p> <p>[データソース A] [データソース B] のようになります。</p>
新規作成	クリックすると新しいデータソースを定義できます。
名前	データソースの名前。
デバイスが有効	データソースはデフォルトでは有効になっています。データソースを無効にするにはチェックボックスを解除します。
リセット	クリックして選択されたデータソースのすべての設定をリセットします。 名前 フィールドに入力された名前は残ります。
ポート	データソースのポート番号。

名前	詳細
プロトコルタイプセレクト	<p>システムがジェネリックイベントを検出するために聞き、分析すべきプロトコル。</p> <p>すべて： TCP および UDP。</p> <p>TCP： TCP のみ。</p> <p>UDP： UDP のみ。</p> <p>ジェネリックイベントに使用する TCP および UDP パッケージに、@、#、+、~、等の特殊文字が含まれている場合があります。</p>
IP タイプセレクト	<p>選択可能な IP アドレスタイプ： IPv4、IPv6、または両方。</p>
区切りバイト	<p>個別ジェネリックイベント記録を分離するために使用するセパレーター バイトを選択します。デフォルトのデータソースタイプインターナショナル（上記のデータソースをご覧ください）は 13、10 です。（13,10 = <CR><IF>）。</p>
エコータイプセレクト	<p>使用可能なエコーリターン形式：</p> <ul style="list-style-type: none"> ● エコー統計： 次の形式をエコーします。 <p style="margin-left: 20px;">[X],[Y],[Z],[ジェネリックイベント名]</p> <p style="margin-left: 20px;">[X] = 要求番号。</p> <p style="margin-left: 20px;">[Y] = 文字数。</p> <p style="margin-left: 20px;">[Z] = ジェネリックイベントとの一致数。</p> <p style="margin-left: 20px;">[ジェネリックイベント名] = 名前： フィールドに入力された field。</p> ● すべてのバイトをエコー： すべてのバイトをエコーします。 ● エコーなし： すべてのエコーを抑制します。
エンコーディングタイプセレクト	<p>デフォルトでは、もっとも関連のあるオプションのみがリストに表示されます。すべて表示チェックボックスを選択し、利用可能なすべてのエンコーディングを表示します。</p>
使用可能な外部 IPv4 アドレス	<p>外部イベントを管理するために、管理サーバーが通信可能な IP アドレスを指定します。これを使用して、データを取得しない IP アドレスを除外することも可能です。</p>
使用可能な外部 IPv6 アドレス	<p>外部イベントを管理するために、管理サーバーが通信可能な IP アドレスを指定します。これを使用して、データを取得しない IP アドレスを除外することも可能です。</p>

機能設定

フェールオーバー管理サーバー

複数の管理サーバー（クラスタ）

管理サーバーは、サーバーのクラスタ内の複数のサーバーにインストールできます。これにより、システムのダウンタイムがほとんどなくなります。クラスタ内のサーバーに障害が発生すると、クラスタにある別のサーバーが、管理サーバーを実行している障害のあるサーバーの仕事を自動的に引き継ぎます。Server サービスをクラスタの他のサーバーに切り換えて実行する自動プロセスには、非常に短い時間（最長でも 30 秒）しかかかりません。

監視のセットアップ毎に有効な管理サーバーを 1 つしか持てませんが、障害の場合に他の管理サーバーが代わりに使われるように設定できます。

許可されているフェールオーバーの回数は、6 時間で 2 回に限られています。この制限を超えると、Management Server サービスはクラスタリングサービスによって自動的に起動されません。許可されるフェールオーバーの回数は、必要に応じて変更できます。詳細情報は、Microsoft® のホームページ <http://technet.microsoft.com/en-us/library/cc787861%28WS.10%29.aspx> を参照してください。

クラスタリングの前提条件

- クラスタで 2 台以上のサーバーがインストールされていること。
 - Microsoft Windows 2008®でのクラスタについては、フェールオーバークラスタ [http://technet.microsoft.com/en-us/library/cc732488\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732488(WS.10).aspx)を参照してください。
- サーバークラスタ外に外部 SQL データベースがインストールされているか、あるいはサーバークラスタ内に内部 SQL（クラスタ化された）サービスがインストールされていること（内部 SQL サービスを作成するには、クラスタ化された SQL サーバーと動作できる標準以上の SQL サーバーを使用する必要があります。）
- Microsoft® Windows® Server（Enterprise または Data Center 版）。

クラスタでのインストール

説明および図例は、お使いの画面の表示内容と異なる場合があります。

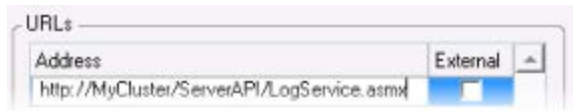
インストールと URL アドレスの変更：

- クラスタの最初のサーバーに管理サーバーとすべてのサブコンポーネントをインストールします。

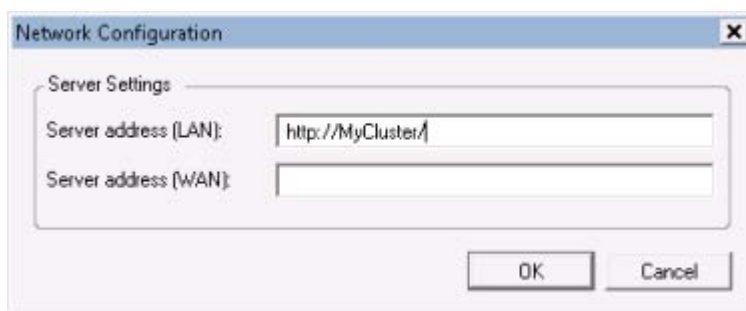
管理サーバーは、必ず特定のユーザー名でインストールし、ネットワークサービスとしてインストールしないでください。このためには、カスタムインストールオプションを使用する必要があります。さらに、その特定のユーザーは、共有ネットワークドライブへアクセスする必要があります。また、パスワードの有効期限が限られていないことが望まれます。

- クラスタの最初のサーバーに Management Server と Management Client をインストールした後、Management Client を開いてから、ツールメニューで登録済みサービスを選択します。

- a) 登録されているサービスの追加と削除ウィンドウで、リストの中の **Log サービス** を選択してから、**編集** をクリックします。
- b) 登録済みサービスの編集ウィンドウで、Log サービスの URL アドレスをクラスタの URL アドレスに変更します。



- c) 登録されているサービスの追加と削除ウィンドウに一覧表示されているすべてのサービスについて、手順 a と手順 b を繰り返します。 **ネットワーク** をクリックします。
- d) **ネットワーク設定** ウィンドウで、サーバーの URL アドレスをクラスタの URL アドレスに変更します。（この手順は、クラスタの最初のサーバーだけに適用されます。） **[OK]** をクリックします。



3. 登録されているサービスの追加と削除ウィンドウで、**閉じる** をクリックします。Management Client を終了します。
4. Management Server サービスを停止し、IIS を停止します。IIS を停止する方法は、Microsoft® のホームページ [http://technet.microsoft.com/en-us/library/cc732317\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx) で確認できます。
5. クラスタにある残りのすべてのサーバーに対して、手順 1~4 を繰り返します。今回は既存の SQL データベースを参照します。ただし、管理サーバーがインストールされているクラスタの**最後**のサーバーでは、Management Server サービスを停止しないでください。

次に、有効にするために、**Management Server** サービスをフェールオーバークラスタの汎用サービスとして設定する必要があります。

1. 管理サーバーをインストールした最後のサーバーで、**スタート > 管理ツール**に移動し、Windows の **フェールオーバー クラスタ管理**を開きます。フェールオーバー クラスタ管理ウィンドウで、クラスタを展開し、**サービスとアプリケーション**を右クリックしてから、**サービスまたはアプリケーションの構成**を選択します。



2. **高可用性**ダイアログボックスで、**次へ**をクリックして、**汎用サービス**を選択し、**次へ**をクリックします。ダイアログボックスの3番目のページでは何も指定しないで、**次へ**をクリックします。
3. **Sony Network Video Management System Management Server** サービスを選択してから、**次へ**をクリックします。サービスにアクセスする時にクライアントが使用する名前（クラスタのホスト名）を指定してから、**次へ**をクリックします。
4. サービスにストレージが不要なら、**次へ**をクリックします。レジストリの設定を変更する必要がなければ、**次へ**をクリックします。クラスタサービスが、ニーズに沿って設定されているかを確認し、**次へ**をクリックします。これで、管理サーバーが、フェールオーバークラスタの汎用サービスとして設定されました。**終了**をクリックします。
5. クラスタの設定で、管理サーバーが停止したときにイベントサーバーも停止するよう、イベントサーバーと Data Collector が管理サーバーの依存サービスとして設定されている必要があります。
6. **Sony Network Video Management System Event Server** サービスを **Sony Network Video Management System Management Server Cluster** サービスのリソースとして追加するには、Cluster サービスを右クリックして、リソースの追加 > **4 - 汎用サービス**をクリックして、**Sony Network Video Management System Event Server** を選択します。

クラスタでのアップグレード

クラスタを更新する前に、データベースのバックアップを行います。

1. クラスタにあるすべての管理サーバーで、**Management Server** サービスを停止します。
2. クラスタにあるすべてのサーバーから、**Management Server** をアンインストールします。
3. クラスタでのインストールの説明に従って、クラスタで複数の **Management Server** をインストールする手順を実行します。クラスタでインストール 『215ページ の"クラスタでのインストール"参照』を参照してください。

重要： インストールする際は、既存の SQL 設定データベースを再利用していることを確認してください（古い既存のデータベースのバージョンから、新しいバージョンへ自動的にアップグレードされます）。

Network Video Management System Smart Wall

Network Video Management System Smart Wall について

Network Video Management System Smart Wall は、大規模な監視センターに優れた状況認識を提供できる最先端のビデオウォール製品です。効率性が改善され、応答時間が短縮されることで、監視オペレータは重要な事象に焦点を絞ることができます。



Network Video Management System Smart Wall を使用することにより、ビデオウォールに表示されるライブビデオをすばやく切り替えることが可能になるため、特定のセキュリティシナリオやニーズに適合できます。ビデオウォールの表示を切り替える方法のひとつに、Smart Wall プリセットが挙げられます。監視管理者は、Management Client の Smart Wall プリセットを定義して、再発するさまざまな監視シナリオに対応できるように監視範囲を最適化します。Smart Wall プリセットは、ビデオウォール全体またはビデオウォールの一部に適用され、ビデオウォールのモニター上のコンテンツのレイアウトと、どのカメラが表示されるかが決定されます。

Smart Wall プリセットを使用することで、表示切り替えをルールによって自動的にトリガすることが可能です。表示切り替えは、Network Video Management System Smart Client を使用してビューやカメラを Network Video Management System Smart Client のビデオウォールの論理的表示面にドラッグアンドドロップするか、監視管理者によって定義された複数の Smart Wall プリセットを選択することで、監視オペレータによって手動でトリガすることもできます。

Network Video Management System Smart Client で Network Video Management System Smart Wall 機能を使用する方法の詳細については、Network Video Management System Smart Client のマニュアルを参照してください。

Network Video Management System Smart Wall ライセンス

Network Video Management System Smart Wall は、以下のビデオウォール関連ライセンスを必要とします。

- ビデオウォールで動画表示する無制限の数のモニターを対象とする Network Video Management System Smart Wall の基本ライセンス。

個別に Network Video Management System Smart Wall の基本ライセンスを購入できます。

Smart Wall の設定

Smart Wall の設定では、Smart Wall を定義し、モニターを追加し、モニターレイアウトを定義し、オプションとして Smart Wall プリセットや、異なるモニターのレイアウトとコンテンツを指定します。

Smart Wall プリセットは、Network Video Management System Smart Client ユーザーがビデオウォールに手動でプッシュできるカメラや、Network Video Management System Smart Client ビューのみを表示する場合は定義する必要はありません。

ルールを使用して、ビデオウォールに表示されるものを自動的に切り替えたり、あるいはシナリオが発生するたびにビデオウォールに同じコンテンツを表示する典型的な監視シナリオがある場合は、Smart Wall プリセットを定義する必要があります。

Smart Wall の設定は非常に柔軟です。1 つの Smart Wall のビデオウォールにすべてのモニターを含めたり、モニターをグループ化してグループごとに Smart Wall を設定できます。Smart Wall プリセットは、Smart Wall のすべてのモニター、または一部のモニターのレイアウトやコンテンツを変更できます。モニターは複数の Smart Wall と Smart Wall プリセットの一部として含めることができます。典型的な監視シナリオに対応するために、Smart Wall と Smart Wall プリセットを、必要な数だけ無制限に作成できます。

a. Smart Wall を定義する

1. クライアントを展開し、**Smart Wall** を選択します。
2. **概要** ペインで、**Smart Wall** を右クリックし、**Smart Wall の追加** を選択します。
3. Smart Wall の設定を指定します。
4. **全般ビューアイテムのプロパティ** 設定で、システムステータス情報とタイトルバーを、カメラのレイアウトアイテムの上に表示するかどうか指定します。
5. **OK** をクリックします。

b. モニターを追加し、モニターレイアウトを指定する


1. Smart Wall を右クリックし、**モニターの追加** を選択します。
2. ビデオウォール上の物理モニターと同一になるように、モニターの寸法を設定します。
3. プリセット動作設定、**空のプリセット** および **空のプリセットアイテム** を使用して、空のプリセットレイアウトがモニターで表示する内容を定義します。または新しい Smart Wall プリセットが自動的にトリガされたり、あるいは Network Video Management System Smart Client で手動で選択されたときに、プリセットの空のプリセットアイテムに表示する内容を定義します。空のプリセットおよび空のプリセットアイテムは、Smart Wall プリセットによって制御されないコンテンツに使用できます。
4. プリセット動作設定、**エレメントの挿入** を使用して、Network Video Management System Smart Client ユーザーが、Smart Wall プリセットのレイアウトアイテムにカメラをドラッグしたときの動作を定義します。**独立** を選択して、プリセットアイテムに既にあるカメラと新しいカメラを置き換えます。または **リンク済み** を選択して、新しいカメラを挿入したところから、レイアウトアイテムのコンテンツを左から右に押します。
5. 物理ビデオウォールにある数だけのモニターを追加します。
6. Smart Wall を選択し、**レイアウト** タブで、**編集** をクリックして、ビデオウォールの物理モニターの配置と同一になるように、複数のモニターを配置します。
7. **OK** をクリックします。同じレイアウトが Network Video Management System Smart Client で使用されます。

c. Smart Wall プリセットを追加する (任意)

1. Smart Wall を選択し、**プリセット** タブから、**新規追加** をクリックします。

2. 名前と説明を入力して、**OK** をクリックします。
3. **実行** をクリックすると、Smart Wall プリセットがビデオウォールに表示されます。
4. 必要な数の Smart Wall プリセットを作成します。

d. モニターにレイアウトとカメラを追加する (Smart Wall プリセットが必要)

1. 作成したモニターのいずれかを選択し、**プリセット** タブから、選択した Smart Wall プリセットを使用する場合に、選択したモニターに表示する内容を設定するため、リストからプリセットを選択します。
2. **編集** をクリックします。
3. レイアウトボタンをクリックして、モニターで使用するレイアウトを選択し、**OK** をクリックします。

4. **デバイスグループ** または **レコーディングサーバー** タブからカメラを各レイアウトアイテムにドラッグします。Smart Wall プリセットによって制御されない他のコンテンツで使用できるようにするには、レイアウトアイテムを空のままにします。
5. 選択されたプリセットのレイアウトが、モニターに既にある場合は、**クリア** をクリックして新しいレイアウトを定義するか、Smart Wall プリセットによって制御されない他のコンテンツにモニターを使用できるように、Smart Wall プリセットからモニターを除外します。
6. **OK** をクリックします。
7. Smart Wall プリセットに含めるモニターに、レイアウトやカメラが追加されるまで手順を繰り返します。

Network Video Management System Smart Wall のユーザー権限の設定

役割のユーザー権限を指定すると、Network Video Management System Smart Client ユーザーが Network Video Management System Smart Wall で実行できるタスクを制御できます。ユーザー権限は、役割に割り当てられるすべてのユーザーに適用されます。詳細については、「Smart Wall 権限プロパティのある役割」『187 ページ の「Smart Wall タブ (役割)」参照』を参照してください。

読み取り、**編集**、**削除** ユーザー権限の選択は常に適用されます。**操作** および **再生** ユーザー権限については、時間設定を選択し、特定の期間の間にユーザー権限を付与できます。たとえば、標準の業務時間内のみユーザーが Smart Wall で表示されるコンテンツを変更できるようにする場合に便利です。

役割のユーザー権限を指定するには、次の手順に従います。

1. サイトナビゲーションペインで、**セキュリティ** を展開し、**役割** を選択します。
2. **[役割]** ペインで役割を選択するか、ペインを右クリックし、**[役割の追加]** を選択して新しい役割を作成します。
3. **[役割設定]** ペインの上部で Smart Wall を選択します。
4. **[役割設定]** ペインの下部で、**Smart Wall** タブをクリックしてから、割り当てるユーザー権限を選択します。
 - **読み取り** - クライアントアプリケーションで Smart Wall を表示
 - **編集** - クライアントアプリケーションで Smart Wall を変更

- **削除** - クライアントアプリケーションで Smart Wall を削除
- **操作** - クライアントアプリケーションで選択したモニターにレイアウトを適用し、プリセットをアクティブ化
- **再生** - ライブおよび録画されたビデオを確認して管理

注意： 再生権限を選択しない場合、ユーザーは、ビデオウォールに表示されるコンテンツを表示できますが、変更はできません。ユーザーが変更を行った場合は、システムが共有状態から自動的に切断され、ビデオウォールのコンテンツは影響を受けなくなります。共有ビューに戻るには、**[Smart Wall モニターの再接続]**をクリックします。

5. オプション：特定の期間に**操作**または**再生**ユーザー権限を付与するには、チェックボックスを選択してから、時間設定を選択します。

Smart Wall プリセットのあるルールの使用について

ルールと Smart Wall プリセットを組み合わせることによって、カメラなどの動作をシステムがルールを使って制御する方法と同様に、ビデオウォールに表示される内容を制御できます。たとえば、あるルールがビデオウォールをトリガして、特定の日に特定の Smart Wall プリセットを表示することができます。さらに、ルールを使ってビデオウォールディスプレイで各モニターに何が表示されるかを制御できます。ルールの作成方法については、ルールの追加 『154ページ』を参照してください。

```
Perform an action in a time interval
day of week is Thursday
Set smart wall London to preset Factory
and Set smart wall London monitor UK Monitor 9 using current layout
to show Camera 1 starting in position 6
```

ルールが Smart Wall プリセットをトリガする例。

Smart Wall のプロパティ

情報タブ (Smart Wall プロパティ)

Smart Wall の**情報**タブでは、Smart Wall を追加および編集できます。

名前	詳細
名前	Smart Wall の名前。Network Video Management System Smart Client に Smart Wall ビューグループ名として表示されます。
詳細	Smart Wall の説明。説明は Management Client 内部でのみ使用されません。
ステータステキスト	選択すると、カメラとシステムステータス情報が、ビデオウォールのカメラのレイアウトアイテム全体で表示されます。
タイトルバーなし	選択すると、ビデオウォールに表示されるすべての Smart Wall レイアウトアイテムにタイトルバーが表示されません。
タイトルバー	選択すると、ビデオウォールに表示されるすべての Smart Wall レイアウトアイテムにタイトルバーが表示されます。

名前	詳細
ライブインジケータ付きのタイトルバー	選択すると、ビデオウォールに表示されるすべての Smart Wall レイアウトアイテムのタイトルバーにライブおよびモーションインジケータが表示されます。

プリセットタブ (Smart Wall プロパティ)

Smart Wall のプリセットタブでは、Smart Wall プリセットを追加および編集できます。

名前	詳細
新規追加	クリックして、Network Video Management System Smart Wall インストールにプリセットを追加します。 新しい Smart Wall プリセットの名前と説明を定義します。
編集	Smart Wall プリセットの名前および説明を編集します。
削除	Smart Wall プリセットを削除します。
起動	クリックすると、Smart Wall プリセットがビデオウォールに表示されます。Smart Wall プリセットの表示が自動的にトリガされるようにするには、Smart Wall プリセットを使ってルールを作成する必要があります。Smart Wall プリセットのあるルールの使用について『221ページ』も参照してください。

レイアウトタブ (Smart Wall プロパティ)

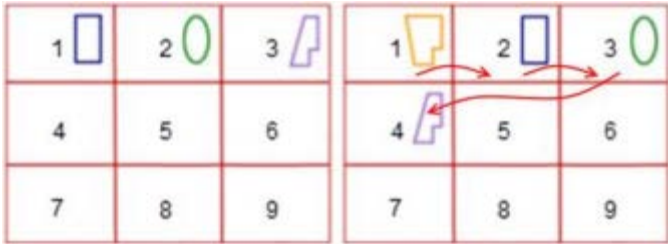
Smart Wall のレイアウトタブで、ビデオウォール上の物理モニターの配置と一致するよう、Smart Wall のモニターを配置します。また、レイアウトは Network Video Management System Smart Client でも使用されません。

名前	詳細
編集	クリックして、モニターの配置を調整します。
移動	モニターを新しい位置に移動するには、関連するモニターを選択し、任意の位置にドラッグするか、あるいは矢印ボタンのいずれかをクリックして、モニターを選択した方向に移動します。
ズームボタン	ボタンをクリックすると、Smart Wall レイアウトプレビューが拡大/縮小され、モニターを正しく配置することができます。
名前	モニターの名前。名前は Network Video Management System Smart Client に表示されます。
サイズ	ビデオウォールの物理モニターの寸法。
アスペクト比	ビデオウォールの物理モニターの高さおよび幅の比率。

モニタープロパティ

情報タブ (モニタープロパティ)

Smart Wall プリセットのモニターの**情報**タブで、モニターを追加し、モニター設定を編集できます。

名前	詳細
名前	モニターの名前。名前は Network Video Management System Smart Client に表示されます。
詳細	モニターの説明。説明は Management Client 内部でのみ使用されます。
サイズ	ビデオウォールの物理モニターの寸法。
アスペクト比	ビデオウォールの物理モニターの高さおよび幅の比率。
空のプリセット	<p>Network Video Management System Smart Client で新しい Smart Wall プリセットがトリガされたり、選択されたときに、プリセットレイアウトが空のモニターに表示する内容を定義します。</p> <p>保存を選択すると、モニターの現在のコンテンツが維持されます。</p> <p>クリアを選択すると、すべてのコンテンツがクリアされ、モニターには何も表示されなくなります。</p>
空のプリセットアイテム :	<p>Network Video Management System Smart Client で新しい Smart Wall プリセットがトリガされたり、選択されたときに、空のプリセットレイアウトアイテムに表示する内容を定義します。</p> <p>保存を選択すると、レイアウトアイテムの現在のコンテンツが維持されます。</p> <p>クリアを選択すると、すべてのコンテンツがクリアされ、レイアウトアイテムには何も表示されなくなります。</p>
要素の挿入	<p>Network Video Management System Smart Client で表示したときに、モニターのレイアウトにどのようにカメラが挿入されるかを定義します。独立を選択すると、影響のあるレイアウトアイテムのコンテンツのみが変更され、レイアウトの他のコンテンツは同じままで維持されます。リンク済みを選択すると、レイアウトアイテムのコンテンツは左から右へ押されます。たとえば、この図例では、カメラがポジション 1 に挿入されると、ポジション 1 の前のカメラはポジション 2 に押され、ポジション 2 の前のカメラはポジション 3 に押される、というように続きます。</p>  <p>新しいカメラが挿入される前および挿入後。</p>

プリセットタブ (モニタープロパティ)

Smart Wall プリセットのモニターのプリセットタブでは、選択した Smart Wall プリセットでモニターのレイアウトとコンテンツを編集できます。

名前	詳細
プリセット	選択された Smart Wall の Smart Wall プリセットのリスト。
編集	<p>編集をクリックして、選択したモニターのレイアウトとコンテンツを編集します。</p> <p>カメラをダブルクリックして、単一のカメラを削除します。</p> <p>クリアをクリックすると、Smart Wall プリセットからモニターを除外する新しいレイアウトを定義します。これにより、Smart Wall プリセットによって制御されない他のコンテンツでモニターが使用できるようになります。</p> <p>をクリックして、選択したプリセットのモニターで使用するレイアウトを選択し、OKをクリックします。</p> <p>デバイスグループまたはレコーディングサーバタブからカメラを各レイアウトアイテムにドラッグします。Smart Wall プリセットによって制御されない他のコンテンツで使用できるようにするには、レイアウトアイテムを空のままにします。</p>

NVMS Mobile

NVMS Mobile の概要

NVMS Mobile について

NVMS Mobile には次の 3 つのコンポーネントがあります。

- **NVMS Mobile クライアント**
- **NVMS Mobile サーバー**
- **NVMS Mobile プラグイン**

NVMS Mobile クライアントはモバイル監視アプリであり、Android デバイス、または Apple デバイスにインストールして使用できます。任意の数の NVMS Mobile クライアントのインストールを使用できます。

詳細については、Sony Corporation Web サイト <http://www.sony.net/CameraSystem/NVMS/Manuals> から NVMS Mobile クライアントユーザーガイドをダウンロードしてください。

NVMS Mobile サーバーと NVMS Mobile プラグインについては、このマニュアルで説明します。

NVMS Mobile を使用するための前提条件

NVMS Mobile の使用を開始する前に、次の項目が準備されていることを確認する必要があります。

- 1つ以上のユーザーでインストールおよび構成された実行中の VMS。
- Network Video Management System Smart Client で設定されたカメラとビュー。
- Android、または iOS、を実行し、Google Play、App StoreSMにアクセスして NVMS Mobile クライアントアプリケーションをダウンロードできるモバイルデバイス。

NVMS Mobile 構成

NVMS Mobile サーバーについて

NVMS Mobile サーバーによって、モバイルデバイスや Network Video Management System Web Client の NVMS Mobile クライアントからシステムへのログインが処理されます。

NVMS Mobile サーバーはレコーディングサーバーから NVMS Mobile クライアントに動画ストリームを配信します。これにより、レコーディングサーバーはインターネットに接続しないため、安全性の高い環境を提供できます。NVMS Mobile サーバーがレコーディングサーバーからビデオストリームを受信すると、コーデックとフォーマットの複雑な変換を処理し、モバイルデバイス上でビデオストリーミングできます。

レコーディングサーバーへアクセスするためのコンピュータに、NVMS Mobile サーバーをインストールする必要があります。NVMS Mobile サーバーをインストールするときには、管理者権限があるアカウントを使用してログインしてください。そうでない場合、インストールは正常に完了しません。

Mobile サーバーの追加または編集

1. **サーバー > モバイルサーバー**に移動します。表示されるメニューから**新規作成**を選択します。設定を入力または編集します。

重要：自分または他のユーザーが NVMS Mobile クライアントに接続中に、**ログイン方法**、**すべてのカメラを表示**、**出力とイベント**の設定を編集する場合、新しい設定を有効にするには、NVMS Mobile クライアントを再起動する必要があります。

調査の設定

調査を設定し、Web Client と NVMS Mobile を使用して、録画されたビデオにアクセスし、インシデントを調査し、証拠ビデオを準備およびダウンロードできるようにします。

調査を設定するには、次の手順に従います。

1. Management Client では、モバイルサーバーをクリックしてから、**【調査】**タブをクリックします。
2. **【有効】**チェックボックスを選択します。デフォルトでは、チェックボックスが選択されています。
3. **【調査フォルダ】**フィールドで、調査のビデオを保存する場所を指定します。
4. **【調査のサイズを制限する】**フィールドで、調査フォルダが含むことができる最大メガバイト数を入力します。

5. オプション：ユーザーが他のユーザーが作成する調査にアクセスできるようにするには、**【他のユーザーが作成した調査を表示する】**チェックボックスを選択します。このチェックボックスを選択しない場合、ユーザーは自分の調査のみを表示できます。
6. オプション：ビデオがダウンロードされた日時を含めるには、**【AVI エクスポートのタイムスタンプを含める】**チェックボックスを選択します。
7. **【AVI エクスポートで使用されたコーデック】**フィールドで、ダウンロード用に AVI パッケージを準備するときに使用する圧縮形式を選択します。

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

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

8. **【失敗したエクスポートデータ (MKV および AVI エクスポート)】**フィールドで、正常にダウンロードされ、不完全な可能性があるデータを保持するか、削除するかどうかを指定します。
9. ユーザーが調査を保存できるようにするには、次の権限をユーザーに割り当てられたセキュリティ役割に付与する必要があります。
 - Network Video Management System Enterprise Edition 製品では、エクスポート権限を付与します。
 - Network Video Management System Standard Edition 製品では、データベース権限を付与します。

調査のクリーンアップ

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

- 調査と、調査用に作成されたすべてのビデオエクスポートを削除するには、リストの調査を選択し、**【削除】**をクリックします。
- 調査用にエクスポートされたビデオファイルを個別に削除、調査を保持するには、リストで調査を選択します。**【調査の詳細】**グループで、エクスポート用の**データベース**、**AVI**、**MKV** フィールドの右にある**削除**アイコンをクリックします。

ビデオプッシュを使用した動画のストリーミングについて

ビデオプッシュを設定すると、ユーザーはモバイルデバイスのカメラから Network Video Management System 監視システムに動画をストリーミングし、常に状況に関する通知を受信するか、動画を録画して後から調査できます。

ビデオを流すための「ビデオ・プッシュ」の設定

ユーザーが携帯デバイスから管理システムにビデオを流すためには、Network Video Management System サーバーで「ビデオ・プッシュ」を設定する必要があります NVMS Mobile 。

Management Client 次の手順で設定が可能です。

1. 携帯デバイスが記録サーバーにビデオを流すためのチャンネルを設定します。
2. 記録サーバー上のハードウェア・デバイスである「ビデオ・プッシュ・ドライバー」を追加します。
このドライバーはカメラ・デバイスに影響して、記録サーバービデオを流すことができます。
3. 「ビデオ・プッシュ・ドライバー」デバイスをチャンネルに選定して下さい。

ここではこれらの各ステップを説明します。

ビデオを流すためのチャンネル設定

注各チャンネルは一つのハードウェア・デバイス・ライセンスを必要とします。

チャンネルを追加するためには、次のステップを踏んで下さい。

1. ナビゲーションの窓で **Mobile Server** を選んでから、携帯サーバーを選んで下さい。
2. 「ビデオ・プッシュ」のタブ上で、「ビデオ・プッシュ」を選択しボックス内をチェ チェックして下さい。
3. 下の右コーナーの「追加」をクリックして、**チャンネル・マッピング**の下のビデオ・プッシュ・チャンネルを追加して下さい。
4. チャンネルを使用するには、ユーザー・アカウントのユーザー名を入れて下さい。ユーザー・アカウントは、NVMS Mobile サーバーと記録サーバーにアクセスが許可されているはずで

注「ビデオ・プッシュ」を使用するためには、携帯デバイスに、NVMS Mobile 登録されたユーザー名とパスワードを使ってログインする必要があります。

5. ポート・ナンバーを書き留めておいて下さい。それは、記録サーバーにハードウェア・デバイスとして「ビデオ・プッシュ」を追加する時に必要です。
6. ボタンをクリックして、「ビデオ・プッシュ・チャンネル」ダイアログ・ボックスを開いて、チャンネルを保存します。

記録サーバーにハードウェア・デバイスとして、「ビデオ・プッシュ・ドライバー」を追加します。

1. ナビゲーションの窓で、「記録サーバー」をクリックして下さい。
2. ビデオを流したいサーバーを右クリックして、「ハードウェアの追加」をクリックして、「ハードウェアの追加」ウィザードを開いて下さい。
3. ハードウェア探知方法として「手動」を選択し、「次へ」をクリックして下さい。
4. カメラの認定情報を以下の手順で入れて下さい。
 - カメラ工場からの工場設定認定を使用するには、「次へ」をクリックして下さい。典型的な工場設定が使用されています。
 - デバイスの設定を変えるには、その情報を入れて、「次へ」をクリックして下さい。

注これらはハードウェアのための認定設定で、ユーザーのためのものではありません。チャンネルのためのユーザー名とは関係ありません。

5. ドライバーズリストから「その他」を展開し、「ビデオ・プッシュ・ドライバー」を選択してボックス内をチェックしてから「次へ」をクリックして下さい。

注このシステムは「ビデオ・プッシュ・ドライバー」デバイスのために MAC アドレスを作成していません。このアドレスを使用することをお勧めしますそのアドレスは「ビデオ・プッシュ・ドライバー」デバイスに問題が生じた時だけ、変更して下さい。例えば、新しいアドレスやポートナンバーを追加する必要がある場合です。

6. 「アドレス」欄で、サーバーにインストールされているコンピューターの IP アドレスを入れて下さい NVMS Mobile。
7. 「ポート」欄で、ビデオを流すために作成したチャンネル用のポートナンバーを入れて下さい。ポートナンバーはチャンネルを作成した時に割り当てられています。
8. 「ハードウェア・モデル」内で、「ビデオ・プッシュ・ドライバー」を選択し、「次へ」をクリックして下さい。
9. システムが新しいハードウェアを探知したら、「次へ」をクリックして下さい。
10. 「ハードウェア名テンプレート」欄で、ハードウェアのモデルとその IP アドレスを表示するか、またはモデルだけかを決めて下さい。
11. 関係するデバイスが作動するかどうかは、「作動可」チェックボックスを選択して決めて下さい。「ビデオ・プッシュ・ドライバー」の関連デバイスは、作動不可でも、追加することができます。後で、作動可にできます。

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

12. 左にある関連デバイスの既定グループを選択するか、あるいは「グループ追加」欄の具体的なグループを選択して下さい。一つのグループにデバイスを追加すれば、同時にすべてのデバイスを設定したり、あるいはデバイスの入れ替えが簡単にできます。

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

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

必要のないチャンネルは削除して下さい。

もう使わないチャンネルは削除できます。

- 削除するチャンネルを選択し、下の右コーナーの「削除」をクリックして下さい。

アクションについて

[モバイルサーバー]タブでこれを有効または無効にすると、NVMS Mobile クライアントの【アクション】タブを使用できるかどうかを管理できます。【アクション】はデフォルトで有効であり、接続されたデバイスのすべての使用可能なアクションがここに表示されます。

NVMS Mobile で使用する出力の名前について

アクションを現在のカメラとともに正しく表示するには、出力がカメラと正確に同じ名前を使用することが重要です。

例：

「AXIS P3301,P3304 - 10.100.50.110 - Camera 1」という名前のカメラがある場合は、アクションの名前も「AXIS P3301,P3304 - 10.100.50.110 - Camera 1」にする必要があります。

「AXIS P3301,P3304 - 10.100.50.110 - Camera 1 - Light switch」のような詳細説明を後からタイトルに追加することができます。

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

自動エクスポートルールの追加

1. Management Client で、該当するモバイルサーバー > 【エクスポート】タブをクリックします。
2. 【自動エクスポート】の下で、【追加】をクリックして、【自動エクスポートルール】ウィンドウを開きます。
3. 該当する自動エクスポートルールウィンドウ設定を設定します。
4. 完了したら、**OK** をクリックします。

Mobile サーバーの設定

一般

次の表では、このタブの設定について説明します。

名前	詳細
サーバー名	NVMS Mobile サーバーの名前を入力します。
詳細	オプションで、NVMS Mobile サーバーの説明を入力します。
Mobile サーバー	特定のシステムに現在インストールされているすべての NVMS Mobile サーバーから選択します。リストには、実行中の NVMS Mobile サーバーだけが表示されます。
ログイン方法	ユーザーがサーバーにログインするときに使用する認証方法を選択します。以下のオプションから選択できます。 自動 、 Windows 認証 、または 基本認証 。
有効 Network Video Management System Web Client	Network Video Management System Web Client へのアクセスを有効にします。
すべてのカメラビューを有効化	すべてのカメラビュー を含めます。このビューには、ユーザーがレコーディングサーバーで表示できるすべてのカメラが表示されます。
アクションを有効化（出力およびイベント）	NVMS Mobile クライアントでアクションへのアクセスを有効にします。

名前	詳細
キーフレームを有効化	動画をストリーミングするときにキーフレームのみをストリーミングします。これにより、帯域幅の使用が少なくなります。
フルサイズの画像を有効にする	NVMS Mobile サーバーが、フルサイズの画像を NVMS Mobile クライアントまたは Network Video Management System 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ることに注意してください。また、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が無効になります。
直接ストリーミングを有効化	Network Video Management System 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。
デバイスが有効	NVMS 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)。
構成バックアップ	NVMS 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。

接続

【全般】セクションで、次の設定を指定します。

名前	詳細
接続タイプ	クライアントが NVMS Mobile サーバーに接続する方法を選択します。以下のオプションから選択できます。 HTTP のみ 、 HTTP および HTTPS 、または HTTPS のみ 。 注意：【HTTPS のみ】 を選択する場合は、iOS 9.0 を実行するデバイスは、NVMS Mobile サーバーにインストールされた認証局(CA)が発行した証明書がある場合にのみ接続できます。CA は、インターネットでデータを交換するユーザーと Web サイトの身元を検証するデジタル証明書を発行します。CA の例は、Comodo、Symantec、GoDaddy などの企業です。安全な接続をオンにする前に、デジタル証明書の知識があることを確認してください。NVMS Mobile サーバーで証明書を追加する方法については、「証明書の編集 『236ページ』」を参照してください。
クライアントタイムアウト(HTTP)	モバイルサーバーが実行中であることを、NVMS 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。 Sony では、この時間枠を 長くしない ことを推奨しています。

【インターネットアクセス】セクションの設定は、次のタスクで使用されます。

- 接続設定の構成

- 電子メールメッセージを送信し、ユーザーがモバイルデバイスを NVMS Mobile サーバーに接続できるようにする
- 複雑なネットワークで NVMS Mobile サーバーへの接続を有効にする

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	詳細
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	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。
ユーザー名列	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一名を表示します。
状態列	Mobile サーバーと、対象となる NVMS 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。ユーザーは接続されていますか(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)、あるいはユーザーは実際にログインしていますか?考えられる状態: 接続中 および Network Video Management System にログイン中。
帯域幅使用状況列	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。
ライブストリーム列	対象となる NVMS 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。
ストリームの再生列	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。
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。

ビデオプッシュ

ビデオ配信を有効にする場合、以下の設定を指定します。

名前	詳細
ビデオプッシュ	Mobile サーバーでビデオ配信を有効にします。
チャンネル数	Network Video Management System システムで有効なビデオ配信チャンネルの数を指定します。

名前	詳細
チャンネル列	関連するチャンネルのチャンネル数が表示されます。編集不可。
ポート	関連するビデオ配信チャンネルのポート番号。
MAC	関連するビデオ配信チャンネルの MAC アドレス。
ユーザー名	関連するビデオ配信チャンネルに関連するユーザー名を入力します。
カメラ名	カメラが特定されている場合、カメラの名前が表示されます。

必要なステップすべて 『226ページ の"ビデオを流すための「ビデオ・プッシュ」の設定"参照』が完了したら、**カメラの検索**をクリックして、関連するカメラを検索します。

調査

調査を設定し、Network Video Management System Web Client と NVMS Mobile を使用して、録画されたビデオにアクセスし、インシデントを調査し、証拠ビデオを準備およびダウンロードできるようにします。

次の表は、調査の設定を示します。

名前	詳細
調査フォルダ	調査用のビデオが保存される場所
調査のサイズを制限する	調査フォルダが含むことができる最大メガバイト数を入力します。
他のユーザーの調査を表示する	このチェックボックスを選択すると、ユーザーが自分が作成していない調査にアクセスできます。
AVI エクスポートのタイムスタンプを含む	このチェックボックスを選択すると、AVI ファイルがダウンロードされた日時が含まれます。
AVI エクスポートで使用されたコーデック	ダウンロード用の AVI パッケージを準備するときに使用する圧縮形式を選択します。 選択するコーデックは、オペレーティングシステムによって異なる場合があります。必要なコーデックが表示されないバイアは、NVMS Mobile が実行されているコンピュータにインストールすると、リストに追加されます。
失敗したエクスポートデータ (MKV および AVI エクスポート)	調査でダウンロード用に正常に準備されていないデータを保持するか、削除するかを選択します。

パフォーマンス

パフォーマンスタブで、NVMS 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、NVMS 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 NVMS 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、NVMS 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	NVMS Mobile サーバーからクライアントへの送信のフレーム数/秒(FPS)の最大数について制限を設定します。
最大画像解像度	NVMS 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、NVMS 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、NVMS 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、NVMS 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	NVMS Mobile サーバーからクライアントへの送信のフレーム数/秒(FPS)の最大数について制限を設定します。
最大画像解像度	NVMS 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、NVMS 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、NVMS 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、NVMS 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	NVMS Mobile サーバーからクライアントへの送信のフレーム数/秒(FPS)について制限を設定します。
最大画像解像度	NVMS 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	詳細
デバイスが有効	NVMS 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。

- Network Video Management System Web Client を開く 『235ページ の"Network Video Management System Web Client へのアクセス"参照 』
- Mobile サービスの起動、停止、再起動 『237ページ 』
- 監視サーバーの資格情報の入力または変更 『237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 『237ページ 』
- 証明書の編集 『236ページ 』
- 今日のログファイルを開く 『236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 『236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 『236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 『235ページ の"ステータスの表示について"参照 』

Network Video Management System Web Client へのアクセス

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

1. Management Client で NVMS Mobile サーバーを設定します。
2. NVMS Mobile サーバーがインストールされているコンピュータを使用している場合、システムトレイの NVMS Mobile サーバーアイコンを右クリックし、**[Network Video Management System Web Client を開く]**を選択します。
3. NVMS Mobile サーバーがインストールされているコンピュータを使用しない場合は、ブラウザからアクセスできます。このプロセスで手順 4 を続行します。
4. インターネットブラウザ(Internet Explorer、Mozilla Firefox、Google Chrome、Safari)を開きます。
5. 外部 IP アドレスを入力します。これは、NVMS Mobile サーバーが実行されているサーバーの外部アドレスとポート番号です。

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

ブラウザのアドレスバーに、標準 HTTP 接続を使用するか、安全な HTTPS 接続を使用するかによって、http://1.2.3.4:8081 または https://1.2.3.4:8082 と入力します。これで、Network Video Management System Web Client を使用できます。

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

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

ステータスの表示について

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

名前	詳細
サーバー実行日	Mobile サーバーが前回起動されたときの日付と時刻。

名前	詳細
接続済みユーザー	現在 Mobile サーバーに接続されているユーザーの数。
ハードウェアのデコード	Mobile サーバーでハードウェアの高速デコードが実行中かどうかを示します。
CPU 使用	現在 Mobile サーバーが使用している CPU の%。
CPU 使用履歴	Mobile サーバーによる CPU 使用の履歴を詳しく示すグラフ。

ログへのアクセスおよび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 NVMS 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。

証明書の編集

安全な HTTPS プロトコルを使用して、NVMS Mobile サーバーと、使用しているモバイルデバイスや Network Video Management System Web Client との間の接続を確立する場合、デバイスまたは Web ブラウザが接続を許可す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。

NVMS 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。

注意：iOS 9.0 を実行する安全な接続(HTTPS)デバイスを使用する場合は、NVMS Mobile サーバーにインストールされた認証局(CA)が発行した証明書がある場合のみ接続できます。CA は、インターネットでデータを交換するユーザーと Web サイトの身元を検証するデジタル証明書を発行します。CA の例は、Comodo、Symantec、GoDaddy などの企業です。安全な接続をオンにする前に、デジタル証明書の知識があることを確認してください。

別の証明書を使用する場合は、次の手順を実行できます。

1. Management Client がインストールされているコンピュータで、**NVMS Mobile** サーバーアイコンを右クリックし、**【証明書の編集...】**を選択します。
2. 以下のいずれか 1 つを選択します。
 - 自己署名証明書を生成
 - 証明書ファイルの読み込み

自己署名証明書を生成

1. **自己署名証明書を生成**オプションを選んで、**OK** をクリックします。
2. システムが証明書をインストールする間、数秒待ちます。

3. 完了すると、ウィンドウが開いて、証明書が正常にインストールされたことが知らされます。Mobile サービスが再起動し、変更が適用されます。

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。

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)および/または安全なポート番号(HTTPS 接続用)を指定できます。
3. 完了したら、**OK** をクリックします。

Mobile サービスの起動、停止、再起動

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

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

よくある質問(FAQ)

1. **NVMS Mobile** クライアントからレコーディング/**NVMS Mobile** サーバーに接続できないのはなぜですか。

録画に接続するには、お使いの Network Video Management System システムを実行しているサーバーか、専用サーバーに NVMS Mobile サーバーをインストールする必要があります。Network Video Management System ビデオ管理設定で、関連する NVMS Mobile 設定も行う必要があります。これらは、プラグインまたは製品インストールまたはアップグレードの一部としてインストールされます。NVMS Mobile サーバーを取得する方法および NVMS Mobile クライアント関連設定を Network Video Management System システムで統合する方法の詳細については、設定セクション 『225ページ の "NVMS Mobile 構成"参照』を参照してください。

2. **NVMS Mobile を Network Video Management System Enterprise Edition サーバーにインストールしたのですが、自分のデバイスからサーバーに接続できません。何が問題ですか。**

NVMS Mobile サーバーを Network Video Management System Enterprise Edition (4.0 以上)にインストールした後、NVMS Mobile プラグインをインストールし、Network Video Management System Enterprise Edition 設定で 『42ページ の"NVMS Mobile サーバーのインストール"参照』 NVMS Mobile サーバーを表示する必要があります。NVMS Mobile プラグインをインストールした後、**[サーバー] > [モバイルサーバー]**の下でプラグインを見つけ、右クリックして新しいモバイルサーバーを追加します。ここでは、お使いの NVMS Mobile サーバーに関する詳細を追加します（サーバー名、説明（オプション）、サーバーアドレス、ポートなど）。完了したら、NVMS Mobile サービス(Windows Services)を再起動し、デバイスに再接続します。

3. **NVMS Mobile サーバー/ロケーション/サイトを NVMS Mobile クライアントに追加するにはどのようにするのですか。**

NVMS Mobile クライアントからこの手順を実行できます。初めて開くときには、カメラからビデオを取得するために、1 つ以上のモバイルサーバーを追加する必要があります。追加した NVMS Mobile サーバーがアルファベット順に一覧表示されます。必要なログイン資格情報がある場合は、任意の数の NVMS Mobile サーバーを追加できます。

4. **NVMS Mobile クライアントでビデオを表示するときに、時々画質が低下するのはなぜですか。**

NVMS Mobile サーバーは、サーバーとクライアント間で使用可能な帯域幅に従って、自動的に画質を調整します。Network Video Management System Smart Client より画質が低くなった場合、NVMS Mobile クライアントを通してフル解像度の画像を取得するには帯域幅が小さすぎる可能性があります。この理由は、サーバーからのアップストリーム帯域幅が小さすぎるか、クライアントのダウンストリーム帯域幅が小さすぎるかのいずれかが考えられます。Web サイト

<http://www.sony.net/CameraSystem/NVMS/Manuals> からダウンロードできる **Network Video Management System Smart Client ユーザーマニュアル**を参照してください。

混合ワイヤレス帯域幅のエリアにいる場合は、より良い帯域幅のエリアに入ると、画質が改善される場合があります。

5. **どのようにしてビューを作成するのですか？**

NVMS Mobile クライアントでビューを作成または設定することはできません。既に Network Video Management System Smart Client で作成されたビューと関連する名前を使用します。ビューを設定していない場合は、**[すべてのカメラ]**ビューを使用して、システムのすべてのカメラを表示できます。後からいつでも Network Video Management System Smart Client にその他のビューを追加できます。

6. **新しい NVMS Mobile ユーザーを追加するにはどのようにするのですか。**

NVMS Mobile ユーザーは他の Network Video Management System ユーザーとほとんど同じです。新しい NVMS Mobile ユーザーは、Management Client で新しいユーザーを追加する場合と同じ方法で追加します。ナビゲーションペインで**[ユーザー]**を右クリックし、**[新しい基本ユーザーの追加]**または**[新しい Windows ユーザーの追加]**を選択します。新しい基本ユーザーを選択した場合は、システムに応じて、サーバーログイン方法を**自動**または**基本のみ**に変更する必要があります。Management Client の**[サーバー] > [モバイルサーバー]**の下にあるモバイルサーバーエントリの**[全般]**タブにある**[ログイン方法]**ドロップダウンメニューからサーバーログイン方法を変更します。

7. 自分のパン/チルト/ズーム (PTZ) カメラをコントロールして、NVMS Mobile クライアントのプリセットを使用することはできますか。

はい。NVMS Mobile クライアントでは、接続された PTZ カメラを制御し、ライブモードでプリセットを使用できます。

8. どうすれば録画を操作できますか。

Android: 再生モードで記録映像を操作することができます。再生モードで表示するカメラを選択し、**[メニュー]** > **[再生]** を選択します。再生モードでは、コントロールボタンを使って記録を検索することができます。また、**[メニュー]** > **[時間に移動]** を選択して、特定の時間に移動することもできます。**[時間に移動]** を選択したら、表示する日付と時刻を選択します。

iOS: 再生モードで記録映像を操作することができます。再生モードで表示するカメラを選択し、**[再生]** をタップします。再生モードでは、コントロールボタンを使って記録を検索することができます。また、**[メニュー]** > **[時間に移動]** を選択して、特定の時間に移動することもできます。**[時間に移動]** を選択したら、表示する日付と時刻を選択して、**[確認]** をクリックします。

9. ライブビデオと録画済みビデオを同時に見ることはできますか？

はい。再生モードでは、同じカメラから小さいピクチャインピクチャ (PiP) ビューを取得します。

10. 3G データプランなしで NVMS Mobile クライアントを使用することはできますか。

はい。Wi-Fi 経由で NVMS Mobile を使用できます。Network Video Management System システムと同じネットワークでローカルに使用するか、カフェの公共ネットワークや自宅ネットワークなどの別の場所で使用できます。公共ネットワーク上の帯域幅は変動することがあり、ビデオストリームの画質に影響を与える可能性があることにご注意ください。

11. 4G/LTE データプランで NVMS Mobile クライアントを使用することはできますか。

はい、お使いの Network Video Management System 動画管理システムに接続するインターネットにアクセスできるモバイルデバイスのすべてのデータ接続を使用することができます。

12. 複数のサーバーを NVMS Mobile クライアントに追加することはできますか。

初めて NVMS Mobile クライアントを開くときには、カメラからビデオを取得するために、1 つ以上のモバイルサーバーを追加する必要があります。これらのモバイルサーバーはアルファベット順に一覧表示されます。別のサーバーからビデオを取得する場合は、この手順を繰り返します。関連するログイン資格情報がある場合は、任意の数のモバイルサーバーを追加できます。

13. 自分のオフィスで Wi-Fi を使用して自宅で Network Video Management System 動画管理システムに接続する際の画質が悪いのはなぜですか。

ご自宅のインターネットの帯域幅を確認してください。多くの民間のインターネット接続は、ダウンロードおよびアップロードの帯域幅が異なります。例えば、20 Mbit/2 Mbit のように記載されています。これは、自宅でのインターネット利用者は大量のデータをインターネットにアップロードする必要がほとんどなく、一方で大量のデータを消費するためです。Network Video Management System 動画管理システムは、NVMS Mobile クライアントにビデオを送信する必要がありますが、お使いの接続のアップロード速度による制限を受けます。NVMS Mobile クライアントのネットワークのダウンロード速度が良好であるのに、複数の場所で低画質のままである場合、ご自宅のインターネット接続のアップロード速度をアップグレードすることで問題が解決される可能性があります。

14. スクリーンショットはどこに保存されるのですか。

Android: スナップショットは、デバイスの SD カード (`/mnt/sdcard/Network Video Management System`) に保存されます。

iOS : スナップショットは、お使いのデバイスに保存され、お使いのデバイスの**写真**からアクセスすることができます。

Android または iOS のデフォルト設定は変更できません。

15. **HTTPS 接続を使用して Network Video Management System Web Client を実行するときに、セキュリティ警告を表示させないようにするにはどのようにするのですか。**

認証資格情報のサーバーアドレス情報が正しくないため、警告が表示されます。接続は暗号化されます。NVMS Mobile サーバーの自己署名証明書は、NVMS Mobile サーバーに接続するために使用されるサーバーアドレスと一致する独自の証明書で置換する必要があります。これらの証明書は、Verisign などの正式な証明書署名機関から取得されます。詳細については、選択した署名機関にお問い合わせください。NVMS Mobile サーバーは Microsoft IIS を使用しません。つまり、IIS を使用して署名機関によって証明書署名要求 (CSR) を生成するために提供されている手順は、NVMS Mobile サーバーには適用されません。コマンドライン証明書ツールまたは同様の他社製アプリケーションを使用して、CSR ファイルを手動で作成する必要があります。この手順は、システム管理者または上級ユーザーのみが実行してください。

16. **私のプロセッサはハードウェアアクセラレーションデコードをサポートしていますか。**

Intel の新しいプロセッサのみがハードウェアアクセラレーションデコードをサポートしています。プロセッサがサポートされているかについては、Intel 社の Web サイト <http://ark.intel.com/search/advanced?s=t&MarketSegment=DT&QuickSyncVideo=true> を参照してください。

メニューで、**[技術] > [Intel Quick Sync Video]** が **[はい]** に設定されていることを確認します。

プロセッサがサポートされている場合は、ハードウェアアクセラレーションデコードがデフォルトで有効です。Mobile Server Manager の **[ステータスの表示]** 『235 ページ の "ステータスの表示について" 参照』 で現在のステータスを確認できます。

17. **私のオペレーティングシステムはハードウェアアクセラレーションデコードをサポートしていますか。**

Windows 8 および Windows Server 2012 以降のみがサポートされます。

Intel 社の Web サイトから取得した最新のグラフィックドライバをシステムにインストールしてください。これらのドライバは Windows Update からは取得できません。

モバイルサーバーが仮想環境にインストールされている場合は、ハードウェアアクセラレーションデコードはサポートされません。

18. **どのようにモバイルサーバーのハードウェアアクセラレーションデコードを無効にするのですか。(詳細)**

モバイルサーバーのプロセッサがハードウェアアクセラレーションデコードをサポートする場合、デフォルトで有効です。ハードウェアアクセラレーションデコードをオフにするには、次の手順を実行します。

1. VideoOS.MobileServer.Service.exe.config ファイルを見つけます。標準的なパス : C:\Program Files\Sony\NVMS Mobile Server\VideoOS.MobileServer.Service.exe.config
2. メモ帳などのテキストエディタでファイルを開きます。必要に応じて、ファイルタイプ.config をメモ帳に関連付けます。
3. フィールド `<add key="HardwareDecodingMode" value="Auto" />` を見つけます。
4. "Auto" の値を "Off" に置換します。
5. ファイルを保存して閉じます。

19. **ファイアウォールをオンにした後、モバイルデバイスを自分のサーバーに接続できません。なぜですか。**

NVMS Mobile サーバーのインストール中にファイアウォールをオフにした場合、手動で TCP と UDP 通信を有効にする必要があります。

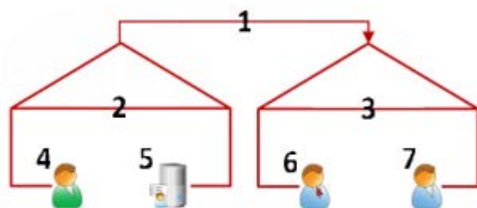
一方向の信頼のマルチドメイン環境

一方向の信頼の設定

システムをマルチドメイン環境で実行する場合、この設定を一方向の信頼で設定することができます。システムは**信頼する側**のドメインにインストールされており、ユーザーは**信頼する側**および**信頼済み**のドメインからログインします。

1. **信頼済み**のドメインで、サービスアカウントを作成します。たとえば、**svcSony** など、好きな名前が付けられます。
2. 新しいサービスアカウントを、**信頼する側**のドメインでシステムを実行しているサーバーのローカルな Windows ユーザーのグループに追加します。
 - 管理者
 - IIS_IUSRS (Windows Server 2008、インターネットインフォメーションサービス(IIS)アプリケーションプール用に必要)
 - IIS_WPG (Windows Server 2003、IIS アプリケーションプール用に必要)
3. サービスアカウントが、直接または **BUILTIN\Administrators** グループを通じて、SQL データベースまたは SQL Server Express でシステム管理者権限を持っていることを確認します。
4. IIS の **ManagementServerAppPool** アプリケーションプールの識別子を、サービスアカウントに設定します。
5. サーバーを再起動して、すべてのグループメンバーおよび権限の変更を有効にします。

重要: 既存のまたは新しい Network Video Management System システム役割に**信頼済み**のドメインユーザーを追加するには、Windows に**信頼済み**のドメインユーザーとしてログインします。次に、Management Client を起動して、**信頼する側**のドメインまたは**信頼済み**のドメインのユーザーとしてログインします。**信頼する側**のドメインのユーザーとして Windows にログインする場合は、ユーザーを参照するために**信頼済み**のドメインの認証情報が求められます。



一方向の信頼のマルチドメイン環境の図例

凡例：

1. ドメインへの一方向の信頼
2. MyDomain.local
3. OtherDomain.edu

4. 信頼する側のドメインのユーザー
5. 管理サーバー
6. Sony サービスアカウント
7. 信頼済みのドメインのユーザー

SNMP

SNMP のサポートについて

システムは、ネットワークデバイスの監視と制御、設定の管理、または統計の収集に使用される標準プロトコル、SNMP（簡易ネットワーク管理プロトコル）をサポートします。

システムは SNMP エージェントとして機能し、トリガされたルールの結果として SNMP トラップを生成します。サードパーティー製の SNMP 管理コンソールにより、次に、ルールトリガイメントに関する情報が受信できるようになります。また、SNMP 管理コンソールのオペレーターは、必要に応じてさらなるアクションのためにシステムを設定できます。

この実装では、SNMP トラップをトリガするために Microsoft® Windows® SNMP サービスを使用しています。つまり、レコーディングサーバーに SNMP サービスをインストールする必要があります。SNMP サービスが独自のユーザーインターフェースを介して設定されている場合、レコーディングサーバーは、.mib（管理情報ベース）ファイルを SNMP 管理コンソールへ送信することができます。

SNMP サービスのインストール

1. 関連するレコーディングサーバーで、Windows のプログラムと機能を開きます。
2. プログラムと機能ダイアログボックスの左側で、Windows 機能のオンまたはオフをクリックします。この操作で Windows の機能ウィンドウが開きます。
3. ダイアログボックスで、簡易ネットワーク管理プロトコル (SNMP) の隣のチェックボックスをオンにしてから、OK をクリックします。

SNMP サービスの設定

1. 必要なレコーディングサーバーで、スタート > コントロールパネル > 管理ツール > サービスを選択します。
2. SNMP サービスをダブルクリックします。
3. トラップタブを選択します。
4. コミュニティ名を指定し、リストに追加をクリックします。
5. 宛先タブを選択します。
6. 追加をクリックし、サードパーティー製 SNMP 管理ステーションソフトウェアを実行しているサーバーの IP アドレスまたはホスト名を指定します。
7. OK をクリックします。

システムのメンテナンス

このシステムで使用するポート

指定されていない限り、ポートは送受信両用です。ポート番号はデフォルト番号です。必要に応じて、ポート番号は変更できます。Management Client で構成できないポートを変更する必要がある場合は、Sony サポートまでお問い合わせください。

ポート番号	プロトコル	使用期限	目的
25	SMTP	レコーディング サーバー	デバイスからのメッセージをリスンしてイベントをアクティブ化し、録画前後の画像を受信します。 デフォルトではポートは無効です。
80	HTTP	管理サーバー上の IIS	Management Server サービスを実行しています。
443	HTTPS	管理サーバーおよびサービスチャンネル	基本ユーザーの認証。
554	RTSP	レコーディング サーバー	カメラからのストリーミングを制御するトラフィック。
1024 以上 (下記のポート以外)	HTTP	レコーディング サーバー	送信のみ。カメラとサーバー間のトラフィック。
1234	TCP/UDP	イベントサーバー	外部システムまたはデバイスからのジェネリックイベントをリスンします。
1235	TCP	イベントサーバー	外部システムまたはデバイスからのジェネリックイベントをリスンします。
1433	TCP	システム内のすべてのプロセス (管理サーバー、ログサーバーおよびイベントサーバーなど)	SQL Server との通信。
5432	TCP	レコーディング サーバー	デバイスからのイベントメッセージをリスンします。

ポート番号	プロトコル	使用期限	目的
7474	TCP	レコーディング サーバー	SNMP 拡張エージェントとの通信。 システムが SNMP を適用しない場合でも、他の目的でこのポートを使用しないでください。
7475	TCP	管理サーバー	SNMP 拡張エージェントとの通信。 システムが SNMP を適用しない場合でも、他の目的でこのポートを使用しないでください。
7563	TCP	レコーディングサーバーと Network Video Management System Smart Client	ImageServer インターフェースとの通信。 PTZ カメラ制御コマンドおよびクライアントなどからの画像ストリームの取得も処理します。
7609	HTTP	レポートサーバーおよび Data Collector Server サービス	両者間の通信。 Data Collector Server サービスを実行しているサーバー上でポートを常に開いている必要があります。
8080	UDP	管理サーバー	サーバー上の内部プロセス間の通信。
9090	TCP	イベントサーバー	外部システムまたはデバイスからのアナリティックイベントをリスンします。
9993	TCP	レコーディングサーバーと管理サーバー	両者間の通信。
12345	TCP	管理サーバーと Network Video Management System Smart Client	システムと Matrix 受信 PC の間の通信。 Management Client のポート番号は変更できます。
22331	TCP	イベントサーバー、Network Video Management System Smart Client および Management Client	Network Video Management System アドオン製品、Network Video Management System Smart Client マップ、Network Video Management System Smart Client アラームリスト、および MIP プラグインが動作するには、受信ポートを有効にする必要があります。
52111	TCP	Network Video Management System Screen Recorder とレコーディングサーバー	両者間の通信。 Management Client のポート番号は変更できます。
65101	UDP	レコーディング サーバー	ドライバーからのイベント通知をリスンします。

システム設定のバックアップおよび復元

システム設定のバックアップおよび復元について

Sony 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のバックアップを定期的に取りをお勧めします。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。

システムでは、Management Client で定義できるシステム設定をすべてバックアップする内蔵機能が提供されています。監査ログファイルを含む、ログサーバーデータベースおよびログファイルはこのバックアップには含まれていません。

大規模システムの場合、Sony は、スケジュールされたバックアップを定義することをお勧めします。これは、次のサードパーティツールを使用して実行できます。Microsoft® SQL Server Management Studio。このバックアップには、手動バックアップと同じデータが含まれています。

バックアップ中、システムはオンラインのままになります。システム設定、ハードウェア、および SQL Server、Event Server サービスおよび Management Client が単一のサーバーまたは複数のサーバー（分散設定）にインストールされているかどうかによって、バックアップ設定に多少時間がかかる場合があります。

手動およびスケジュールのいずれの場合にも、バックアップのたびに、SQL Server のトランザクションログファイルがフラッシュされます。このログファイルのフラッシュ方法については、Microsoft 社の Web サイトにアクセスして「SQL Server transaction log」で検索してください。

ログサーバーデータベースのバックアップ

このトピックの前半で説明した、システム構成を処理するときと同じ方法を使用して、**SurveillanceLogServer** データベースを処理します。**SurveillanceLogServer** データベース（システム構成データベース名を変更した場合は、異なる名前になります）には、レコーディングサーバーとカメラが報告するエラーを含む、すべてのシステムログが含まれます。

データベースはログサーバーの SQL Server がインストールされている場所にあります。通常は、管理サーバーの SQL Server と同じ場所です。このデータベースにはシステム構成が含まれていないため、バックアップは重要ではありません。ただし、後から管理サーバーのバックアップと復元を行う前にシステムログにアクセスできると便利な場合があります。

システム設定の手動バックアップおよび復元

システム設定の手動バックアップについて

システム設定の手動バックアップを行う際には、システムがオンラインの状態に維持されていることを確認してください。バックアップを開始する前に、次の点を考慮してください。

- 他のシステムに設定をコピーするためにバックアップは使用できません。
- 設定をバックアップするには時間がかかることがあります。システム設定、ハードウェア、および SQL Server、管理サーバーおよび Management Client が同じコンピュータにインストールされているかどうかによって異なります。

- ログ（監査ログを含む）は、設定バックアップの一部ではありません。

イベントサーバー設定のバックアップおよび復元について

イベントサーバー設定の内容は、システム設定のバックアップおよび復元を実行する際に含まれます。

イベントサーバーを初めて実行するとき、すべての設定ファイルが自動的に SQL Server に移動されます。イベントサーバーを再起動する必要なく、復元された設定をイベントサーバーに復元できます。イベントサーバーは、設定の復元のロード中にすべての外部通信を開始および停止できます。

バックアップ/復元の失敗と問題のシナリオについて

前回のシステム設定バックアップ後、イベントサーバーや、ログサーバーなどの登録済みサービスを移動した場合は、新しいシステムにどの登録サービスを設定するか選択する必要があります。システムが古いバージョンに復元された後に、新しい構成を保持することが可能です。サービスのホスト名を見て選択してください。

イベントサーバーが特定の宛先がない（古い登録済みサービス設定を選択した場合など）ために、システム設定の復元が失敗した場合は、もう 1 回復元してください。

システム設定の手動バックアップ

1. メニューバーから、**ファイル > バックアップ設定**を選択します。
2. ダイアログボックスの注記を読んで、**バックアップ**をクリックします。
3. .cnf ファイルの名前を入力します。
4. フォルダの宛先を入力し、**保存**をクリックします。
5. バックアップが終了するまで待ち、**閉じる**をクリックします。

注意：すべての関連するシステム設定ファイルは、1つの.cnf ファイルにまとめられ、指定された場所に保存されます。バックアップ中、すべてのバックアップファイルはまず、管理サーバー上の一時システムのバックアップフォルダにエクスポートされます。通知エリアの **Management Server** サービスアイコンを右クリックし、共有バックフォルダの選択を選択すると、他の一時フォルダを選択できます。

システム設定の復元（手動バックアップから）

重要な情報：

- インストールしているユーザーと復元を実行しているユーザーは両方とも、管理サーバー上と SQL Server 上のデータベースのローカル管理者である必要があります。
- レコーディングサーバーを除き、システムは復元の期間中完全にシャットダウンされます。復元されるまで多少時間のかかる場合があります。
- バックアップは、バックアップが作成されたシステムインストール上でのみ復元できます。設定がバックアップの作成時のものと、できる限り同じであることを確認します。そうしないと、復元が失敗する場合があります。
- データベースのバックアップを実行し、クリーンな SQL Server で復元する場合は、データベースのエラー処理が動作せず、SQL Server から 1 つの汎用エラーメッセージのみが表示されます。これを回避するには、まず、クリーンな SQL Server を使用して Network Video Management System システムを再インストールしてから、その上にバックアップを復元します。

- 確認段階で復元が失敗した場合、変更はされていないため、古い設定を再開することが可能です。復元がプロセスの途中で失敗した場合は、古い設定にロールバックできません。バックアップファイルが壊れていない限り、復元を再実行できます。
- 復元すると、現在の設定が置き換えられます。これは、前回のバックアップ以降の設定変更がすべて失われることを意味します。
- ログ（監査ログを含む）は復元されません。
- 復元が開始されると、取り消しできません。

復元：

1. 通知エリアの Management Server サービスアイコンを右クリックし、**設定の復元**を選択します。
2. 重要な注記を読んでから、**復元**をクリックします。
3. ファイルを開くダイアログボックスで、設定バックアップファイルの場所を参照し、それを選択して**開く**をクリックします。

バックアップファイルは、Management Client コンピュータ上にあります。Management Client が他のサーバーにインストールされている場合は、バックアップ先を選択する前にこのサーバーにバックアップファイルをコピーします。

4. **設定の復元**ウィンドウが表示されます。復元が終了するまで待ち、**閉じる**をクリックします。

共有バックフォルダの選択

システム設定をバックアップして復元する前に、この目的でバックアップフォルダを設定しなければなりません。

1. 通知エリアの Management Server サービスアイコンを右クリックし、**共有バックフォルダの選択**を選択します。
2. 表示されるウィンドウで、希望するファイルの場所を参照します。
3. **OK**を2回クリックします。
4. 現在のバックアップフォルダ内のファイルを削除するか尋ねられたら、必要に応じて、**はいまたはいいえ**をクリックします。

スケジュールされたバックアップと復元

システム設定のスケジュールされたバックアップと復元について

Sony 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のバックアップを定期的にとることをお勧めします。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。定期的なバックアップでは、Microsoft® SQL Server のトランザクションログがフラッシュされるという追加の利点があります。

小規模な設定で定期的なバックアップが必要ない場合には、システム設定を手動でバックアップできます。手順については、システム設定の手動バックアップおよび復元 『246ページ』を参照してください。

管理サーバーは、システムの設定をデータベースに保存します。管理サーバーをバックアップ/復元する場合は、このデータベースがバックアップ/復元に含まれていることを確認してください。

スケジュールされたバックアップおよび復元を使用するための前提条件

Microsoft® SQL Server Management Studio は、Web サイト <http://www.microsoft.com/downloads> から無料でダウンロードできるツールです。

SQL Server データベースを管理するための多数の機能に加え、使いやすいバックアップおよび復元機能が含まれています。お使いの管理サーバーに、ツールをダウンロードしてインストールします。

SQL Server トランザクションログについて

システムでデータの変更が起こるたびに、SQL Server は、ネットワーク上の SQL Server であるか SQL Server Express Edition であるかにかかわらず、この変更をトランザクションログに記録します。

トランザクションログは基本的に、SQL Server 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ため、トランザクションログのエントリは時間の経過とともに増え続けます。SQL Server のトランザクションログは、デフォルトでは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。

このような状況を避けるためには、SQL Server のトランザクションログを定期的にフラッシュすることが有効な対策です。ただし、フラッシュでは、ログが膨大な規模に拡大するのを制御できるだけであり、トランザクションログファイルが小さくなるわけではありません。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。SQL Server 自体で複数の作業を行って、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、Microsoft 社のサポートページ <http://support.microsoft.com> にアクセスして、「SQL Server transaction log」で検索してください。

スケジュールされたバックアップによるシステム設定のバックアップ

1. Windows のスタートメニューから、Microsoft® SQL Server Management Studio を起動します。
2. 接続するとき、必要な SQL Server の名前を指定します。データベースが作成されたアカウントを使用します。
 - a) イベントサーバー、レコーディングサーバー、カメラ、入力、出力、ユーザールール、パトロール設定などがある、システム設定全体を含む **Surveillance** データベースを見つけます。

ここでは、データベースでデフォルト名が使用されていることを想定しています。

- b) **Surveillance** データベースのバックアップを作成し、以下のことを確認します。
 - 選択されたデータベースが **Surveillance** であることを確認します。
 - バックアップのタイプが**フル**であることを確認します。
 - 繰り返しバックアップのスケジュールの設定。スケジュールされたバックアップと自動バックアップの詳細については、Microsoft Web サイト <https://support.microsoft.com/en-us/kb/2019698> を参照してください。
 - 提案されたパスでよいことを確認するか、代替のパスを選択します。
 - **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**を行うように選択します。

3. ツールの指示に最後まで従います。

同じメソッドを使用して、**SurveillanceLog** データベースのバックアップをすることも考慮してください。

イベントサーバー設定のバックアップおよび復元

イベントサーバー設定の内容は、システム設定のバックアップおよび復元を実行する際に含まれます。イベントサーバーを初めて実行するとき、すべての設定ファイルが自動的に SQL Server に移動されます。イベントサーバーを再起動する必要なく、復元された設定をイベントサーバーに復元できます。イベントサーバーは、設定の復元のロード中にすべての外部コミュニケーションを開始および停止できます。

システム設定の復元（スケジュールされたバックアップから）

前提条件: システム設定データベースの復元中に設定が変更されるのを防止するため、以下を停止してください。

- Management Server サービス 『257ページ の"サーバーサービスの管理"参照 』
- Event Server サービス（Windows サービスから実行可能（お使いのコンピュータで **services.msc** を検索してください。サービスで、**Sony Network Video Management System Event Server** を特定します。））
- World Wide Web Publishing サービス（別称インターネットインフォメーションサービス(IIS)）IIS を停止 [http://technet.microsoft.com/en-us/library/cc732317\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx)する方法については以下を参照してください。

Microsoft® SQL Server Management Studio を、Windows のスタートメニューから開きます。

ツールで、以下を実行します。

1. 接続するとき、必要な SQL Server の名前を指定します。データベースが作成されたアカウントを使用します。
2. イベントサーバー、レコーディングサーバー、カメラ、入力、出力、ユーザールール、パトロール設定などがある、システム設定全体を含む **Surveillance** データベースを見つけます。
3. **Surveillance** データベースを復元し、以下のことを確認します。
 - デバイスからバックアップするように選択します。
 - バックアップメディアタイプファイルを選択します。
 - バックアップファイル **Surveillance.bak** を見つけて選択します。
 - 既存のデータベースを上書きするように選択します。
4. ツールの指示に最後まで従います。

古いログサーバーから **SurveillanceLog** データベースもバックアップする場合には、同じ方法で新しいログサーバー上で復元します。

Management Server サービスが停止した状態ではシステムは機能しません。データベースのバックアップが完了したら、必ずサービスを再起動する必要があります。

管理サーバーの移動

管理サーバーの移動について

1 つの物理サーバーから別のサーバーに管理サーバーのインストールを移動する必要がある場合があります。管理サーバーは、システム設定をデータベースに保存します。1 つの物理サーバーから別のサーバーへ管理サーバー

を移動する場合、新しい管理サーバーもこのデータベースにアクセスできることを確認することが非常に重要です。システム設定データベースは、次の2つの方法で保存できます。

- **ネットワーク SQL Server :** ネットワーク上の既存の SQL Server にあるデータベースに、システムの設定を保存する場合、新しい管理サーバーに管理サーバーソフトウェアをインストールするときに、その SQL Server のデータベースの場所を参照するだけで済みます。その場合、以下のトピックでは管理サーバーホスト名と IP アドレスに関する次の段落のみを参照し、それ以外は無視してください。

管理サーバーホスト名と IP アドレス : 1つの物理サーバーから別の物理サーバーへと管理サーバーを移動するときには、古いものと同じホスト名と IP アドレスを新しいサーバーに割り当てることが最も簡単な方法です。これは、レコーディングサーバーが古い管理サーバーのホスト名と IP アドレスに接続するためです。新しい管理サーバーに新しいホスト名または IP アドレスが割り当てられた場合には、レコーディングサーバーは管理サーバーを検出できません。システムで各レコーディングサーバーを手動で停止して、管理サーバーの URL を変更します。完了した時点で再起動します。

- **ローカル SQL Server :** 管理サーバー自体のローカル SQL Server データベースにシステムの設定を保存している場合、移動する前に既存の管理サーバーのシステム設定データベースをバックアップすることが重要です。データベースをバックアップし、その後新しいサーバーに復元する場合、カメラ、ルール、時間プロファイルなどを移動後に再設定する必要がなくなります。

前提条件

- **新しい管理サーバーにインストールするためのソフトウェアインストールファイル**
- システムを最初に購入し、初めてインストールしたときに受け取った**ソフトウェアライセンスファイル (.lic)**。手動オフラインアクティベーション後に受け取ったアクティベーション済みソフトウェアライセンスファイルを使用しないでください。アクティベーション済みソフトウェアライセンスファイルには、システムがインストールされた特定のサーバーの情報が含まれます。このため、アクティベーション済みソフトウェアライセンスファイルは新しいサーバーに移動すると再利用できません。

移動してシステムライセンスをアップグレードしている場合は、新しいソフトウェアライセンスファイルが提供されます。このファイルを使用してください。

- **ローカル SQL Server ユーザー専用 : Microsoft® SQL Server Management Studio。**
- 管理サーバーが利用できない間は どうしますか? 『251ページ の"使用できない管理サーバーについて"参照』
- ログサーバーデータベースのコピー 『246ページ の"ログサーバーデータベースのバックアップ"参照』

使用できない管理サーバーについて

- **レコーディングサーバーは現在も以下の記録ができます。** 現在動作しているレコーディングサーバーはすべて、管理サーバーからの設定のコピーを受け取るので、管理サーバーがダウンしている間でも、動作して記録を保存できます。そのため、スケジュールされた録画とモーショントリガの録画は動作します。イベントトリガ録画も、管理サーバーまたはその他のレコーディングサーバーに関連しているイベント（管理サーバーを経由するイベント）に基づいていない限り動作します。
- **レコーディングサーバーは一時的にログデータをローカルに保存します。** 管理サーバーが再度利用可能になったときに、レコーディングサーバーは自動的にログデータを管理サーバーへ送信します。
 - **クライアントがログインできません。** クライアントアクセスは、管理サーバーを通じて承認されます。管理サーバーなしにクライアントはログインできません。

- **すでにログインしているクライアントは、最大 1 時間ログインした状態を継続できます。**クライアントがログインした場合、管理サーバーによって承認され、最大 1 時間レコーディングサーバーと通信することができます。新しい管理サーバーを 1 時間以内に稼働できれば、ユーザーの大半に影響が及ぶことはありません。
- **システムを構成する能力がありません。**管理サーバーなしには、システム設定を変更することができません。

Sony では、管理サーバーがダウンしている間は、監視システムとの通信が切断される危険性があることをユーザーに通知することをお勧めします。

システム設定の移動

システム設定の移動は、次の 3 段階のプロセスに従って行います。

1. システム設定のバックアップを保存します。これは、スケジュールされたバックアップ 『249ページ の "スケジュールされたバックアップによるシステム設定のバックアップ"参照 』と同じです。
2. 新しいサーバーに新しい管理サーバーをインストールします。スケジュールされたバックアップの手順 2 を参照してください。
3. 新しいシステムにシステム設定を復元します。システム設定の復元（スケジュールされたバックアップから） 『250ページ 』を参照してください。

SQL Server の管理

SQL Server アドレスの更新について

評価版システムをインストールする場合、またはインストールの大規模な再構成を行った場合は、別の SQL データベースを使用する必要がある場合もあります。これは、**SQL Server アドレスの更新**ツールを使用して処理できます。

このツールを使用して、管理サーバー、イベントサーバーおよびログサーバーによって使用されている SQL Server のアドレスを変更できます。唯一の制限は、ログサーバー SQL アドレスと、管理サーバーおよびイベントサーバーの SQL アドレスを同時に変更できない点です。変更は 1 つずつ順番に行います。

SQL の更新は、管理サーバー/イベントサーバー**または**ログサーバーをインストールしたコンピュータでローカルに行う必要があります。Management Client からは実行できません。管理サーバーとイベントサーバーが同一コンピュータ上にない場合でもツールは使用できますが、管理サーバーがインストールされているものと、イベントサーバーがインストールされているコンピュータの両方で実行する必要があります。

次へ進む前に SQL データベースをコピーする必要があります。

ログサーバーの SQL アドレスの更新

管理サーバーとログサーバーが同じコンピュータにある場合

1. 管理サーバーがインストールされているコンピュータに移動します。

2. タスクバーの通知エリアに移動します。**管理サーバー**アイコンを右クリックし、**SQL アドレスの更新**を選択します。**SQL Server アドレスの更新**ダイアログボックスが表示されます。
3. **Log Server** を選択して、**次へ**をクリックします。
4. SQL Server を入力するか、新しく選択して**次へ**をクリックします。
5. SQL データベースを新しく選択して、**選択**をクリックします。
6. アドレスが変更されるまで待ちます。**OK** をクリックして確定します。

管理サーバーとログサーバーが異なるコンピュータにある場合

1. 管理サーバーがインストールされているコンピュータに移動して、*%ProgramFiles%¥Sony¥- Network VMS Management Server¥Tools¥ChangeSqlAddress¥*ディレクトリ（コンテンツ）をイベントサーバーの一時ディレクトリにコピーします。
2. コピーしたディレクトリを、ログサーバーがインストールされているコンピュータの一時領域にコピーし、その中のファイル：*VideoOS.Server.ChangeSqlAddress.exe* を実行します。**SQL Server アドレスの更新**ダイアログボックスが表示されます。
3. **Log Server** を選択して、**次へ**をクリックします。
4. SQL Server を入力するか、新しく選択して**次へ**をクリックします。
5. SQL データベースを新しく選択して、**選択**をクリックします。
6. アドレスが変更されるまで待ちます。**OK** をクリックして確定します。

管理サーバーまたはイベントサーバーの SQL Server アドレスの更新

1. 管理サーバーおよびイベントサーバーが、
 - a) 同一コンピュータ上にあり、両方の SQL アドレスを更新する場合は、管理サーバーがインストールされているコンピュータに移動します。
 - b) 異なるコンピュータ上にあり、管理サーバーの SQL アドレス（およびその後でイベントサーバー SQL アドレス）を更新する場合は、管理サーバーがインストールされているコンピュータに移動します。
 - c) 異なるコンピュータ上にあり、イベントサーバー SQL アドレスのみを更新する場合（または管理サーバー上ですでに更新した場合）は、管理サーバーがインストールされているコンピュータに移動して、*%ProgramFiles%¥Sony¥- Network VMS Management Server¥Tools¥ChangeSqlAddress¥*ディレクトリ（およびコンテンツ）をイベントサーバーの一時ディレクトリにコピーします。
2. また、
 - **a** および **b** の場合、タスクバーの通知エリアに移動します。**管理サーバー**アイコンを右クリックし、**SQL アドレスの更新**を選択します。
 - **c** の場合、コピーしたディレクトリをイベントサーバーがインストールされているコンピュータの一時領域にコピーし、その中のファイル：*VideoOS.Server.ChangeSqlAddress.exe* を実行します。

3. **SQL Server アドレスの更新**ダイアログボックスが表示されます。**Management Server** および **Event Server** を選択し、**次へ**をクリックします。
4. SQL Server を入力するか、新しく選択して**次へ**をクリックします。
5. SQL データベースを新しく選択して、**選択**をクリックします。
6. アドレスが変更されるまで待ちます。確認メッセージが表示されたら、**OK**をクリックします。

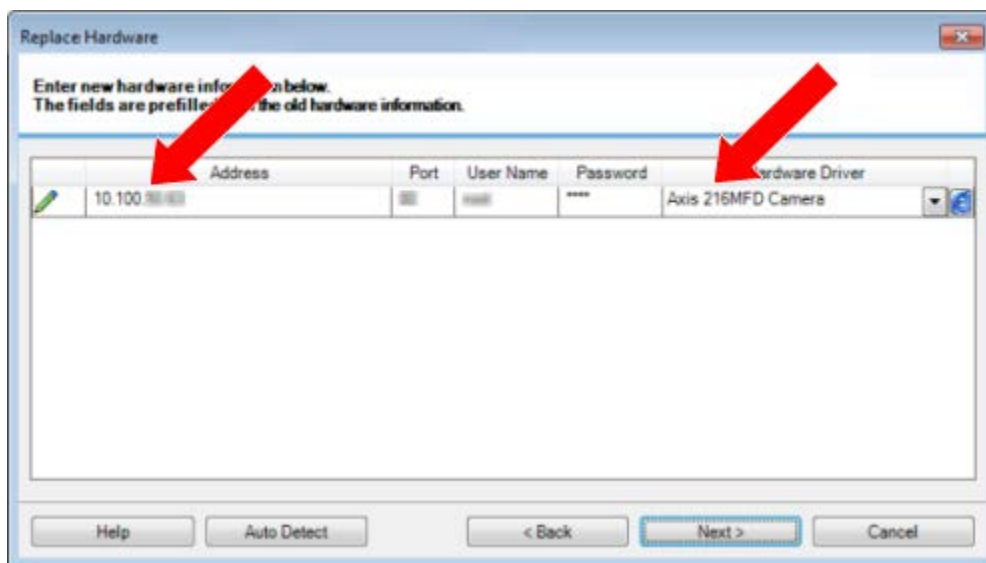
手順 **2 b** に従って操作した場合は、**管理サーバー**の SQL アドレスのみが更新されました。**イベントサーバー**の SQL アドレスを更新するには、同じ手順を繰り返してください。その場合、手順 **2 c** のシナリオを必ず選択してください。

ハードウェアの交換

ネットワーク上のハードウェアデバイスを他のハードウェアデバイスに交換する場合、新しいハードウェアデバイスの IP アドレス、ポート、ユーザー名およびパスワードを知っている必要があります。

手動でライセンスを認証する必要があります。ハードウェアデバイスの新しい数がハードウェアデバイスライセンスの合計数を超えた場合、新しいハードウェアデバイスライセンスを購入する必要があります。

1. 必要なレコーディングサーバーを展開し、交換するハードウェアを右クリックします。
2. **ハードウェアの交換**を選択します。
3. **ハードウェアの交換**ウィザードが表示されます。**次へ**をクリックします。
4. ウィザードで、**アドレス**フィールド（図中の赤い矢印）に、新しいハードウェアの IP アドレスを入力します。既知であれば、**ハードウェアドライバー**のドロップダウンリストから、関連するドライバーを選択します。それ以外の場合は、**自動検出**を選択します。新しいハードウェアのポート、ユーザー名または/およびパスワードのデータが異なる場合は、**自動検出プロセスが開始する前に（必要な場合）** これらを訂正します。



ウィザードでは、既存のハードウェアのデータが事前に入力されています。類似のハードウェアデバイスと交換する場合、たとえばポートやドライバーの情報など、これらのデータを再利用できます。

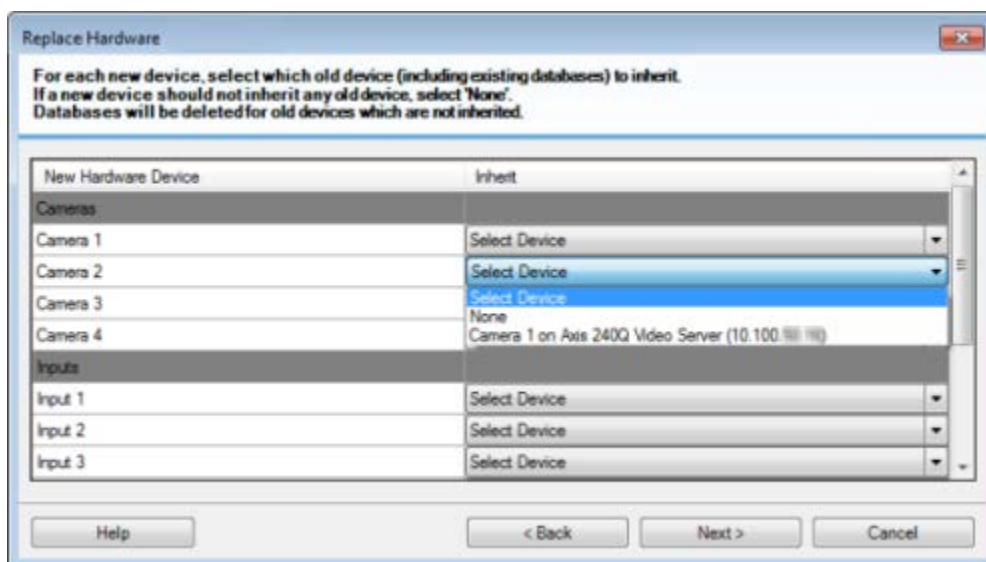
5. 以下のいずれか 1 つを実行します。

- 必要なハードウェアデバイスドライバーをリストから直接選択している場合は、**次へ**をクリックします。
- リストで**自動検出**を選択している場合は、**自動検出**をクリックし、このプロセスが正常に完了するまで（左端に✓のマークが出るまで）待ってから、**次へ**をクリックします。

この手順は、古いハードウェアデバイスと新しいハードウェアデバイスのそれぞれに取り付けられているカメラ、マイク、入力、出力などの数に応じて、デバイスとデータベースをマップするのに役立つように設計されています。

古いハードウェアデバイスのデータベースから新しいハードウェアデバイスのデータベースへ、**どのように**マップするか検討することが重要です。個々のデバイスの実際のマッピングは、右側の列で対応するカメラ、マイク、入力、出力または**なし**を選択して行います。

重要：必ず、**すべての**カメラ、マイク、入力、出力などをマッピングしてください。コンテンツは、**なし**にマッピングされ、**失われます**。



古いハードウェアデバイスに、新しいハードウェアデバイスより多くの個別のデバイスがある例

次へをクリックします。

6. 追加、交換または削除されるハードウェアの一覧が表示されます。**確認**をクリックします。
7. 最後の手順は、追加、交換および継承されるデバイスとその設定の概要です。**クリップボードへコピー**をクリックして、内容を Windows クリップボードコピーするか、**閉じる**をクリックしてウィザードを終了します。

レコーディングサーバーの交換

レコーディングサーバーが動作しないため、新しいサーバーと交換し、古いレコーディングサーバーの設定を継承する場合：

1. 交換するレコーディングサーバーから、レコーディングサーバーIDを取得します。
 - a) **レコーディングサーバー**を選択し、**概要**ペインで古いレコーディングサーバーを選択します。

- b) ストレージタブを選択します。
- c) キーボードで Ctrl キーを押したままにして、**情報**タブを選択します。
- d) **情報**タブの下の部分にあるレコーディングサーバーID 番号をコピーします。文字 **ID** の部分はコピーしないで、番号だけをコピーしてください。



2. 新しいレコーディングサーバーで、レコーディングサーバーID を置き換えます。
 - a) 古いレコーディングサーバーで Recording Server サービスを停止してから、Windows のサービスで、サービスの**スタートアップの種類**を**無効**に設定します。

同じ ID を持つ 2 つのレコーディングサーバーを同時に起動しないことが重要です。

- b) 新しいレコーディングサーバーで、エクスプローラを開いて、**C:¥ProgramDataSony¥- Network VMS Recording Server** またはレコーディングサーバーがあるパスへ移動します。
- c) **RecorderConfig.xml** のファイルを開きます。
- d) タグ **<id>** と **</id>** の間に記載されている ID を削除します。

```
- <recorderconfig>
- <recorder>
  <id>ff0b3d62-4b19-4e86-90ac-40053f6a27e2</id>
```

- e) コピーしたレコーディングサーバーID を、タグ **<id>** と **</id>** の間に貼り付けます。**RecorderConfig.xml** のファイルを保存します。
- f) レジストリに移動します。
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥VideoOS¥Recorder¥Installation
- g) **RecorderIDOnMachine** を開き、古いレコーディングサーバーID を新しい ID に置換します。
- h) Recording Server サービスを再起動します。新しい Recording Server サービスが起動すると、古いレコーディングサーバーの設定がすべて継承されます。

ビデオデバイスドライバー

ビデオデバイスドライバーについて

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

システムをインストールする際に、ビデオデバイスドライバーは初期インストールプロセスに含まれています。Sony は新しいバージョンのビデオデバイスドライバーを適時リリースしており、Web サイトのダウンロードペ

ージ <http://www.sony.net/CameraSystem/NVMS/Software> ページで無料でご利用いただけます。ビデオデバイスドライバーを更新するときには、インストール済みのバージョンに最新バージョンを上書きインストールできます。インストールする前にレコーディングサーバーを停止します。そうでない場合、コンピュータを再起動する必要があります。

最高のパフォーマンスのためにも、常に最新バージョンのビデオデバイスドライバーをご使用ください。

ビデオデバイスドライバーの削除について

ビデオデバイスドライバーがコンピュータ上で不要になった場合は、デバイスパックをシステムから削除できます。その場合は、プログラムを削除する Windows の標準手順に従います。

ビデオデバイスドライバーを削除すると、レコーディングサーバーとカメラデバイスは通信できなくなります。アップグレード時にはデバイスパックを削除しないでください。古いバージョンの上に新しいバージョンをインストールできます。システム全体をアンインストールする場合にのみ、デバイスパックを削除します。

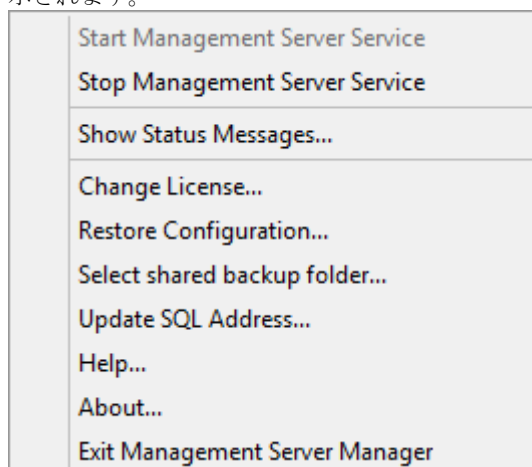
サーバーサービスの管理

サーバーを実行するコンピュータには、トレイアイコンがある通知領域があります。アイコンを使用すると、サーバーサービスの情報を取得し、特定のアクションを実行できます。これには、サービスの状態の確認、ログまたはステータスメッセージの表示、サービスの起動と停止などがあります。

Management Server サービスの開始と停止

通知領域では、トレイアイコンが Management Server サービスの状態(実行中など)を示します。このアイコンを使用して、Management Server サービスを開始、停止できます。Management Server サービスを停止する場合は、Management Client を使用できません。

1. 通知領域で、Management Server のトレイアイコンを右クリックします。コンテキストメニューが表示されます。



2. サービスが停止した場合は、**[Management Server サービスの開始]**をクリックして開始します。トレイアイコンが変わり、新しい状態を示します。
3. サービスを停止するには、**[Management Server サービスの停止]**をクリックします。

トレイアイコンの詳細については、「トレイアイコンについて 『260ページ』」を参照してください。

参照

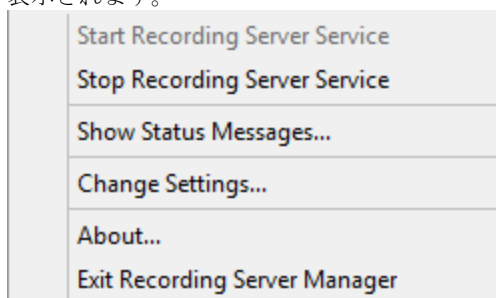
Event Server サービスの開始、停止、再起動 『259ページ』

Recording Server サービスの開始と停止 『258ページ』

Recording Server サービスの開始と停止

通知領域では、トレイアイコンが Recording Server サービスの状態(実行中など)を示します。このアイコンを使用して、Recording Server サービスを開始、停止できます。Recording Server サーバーを停止する場合は、サーバーに接続されたデバイスと連携できません。つまり、ライブビデオの表示またはビデオの録画ができません。

1. 通知領域で、レコーディングサーバーのトレイアイコンを右クリックします。コンテキストメニューが表示されます。



2. サービスが停止した場合は、**[Recording Server サービスの開始]**をクリックして開始します。トレイアイコンが変わり、新しい状態を示します。
3. サービスを停止するには、**[Recording Server サービスの停止]**をクリックします。

トレイアイコンの詳細については、「トレイアイコンについて 『260ページ』」を参照してください。

参照

Event Server サービスの開始、停止、再起動 『259ページ』

Management Server サービスの開始と停止 『257ページ』

管理サーバーまたはレコーディングサーバーのステータスメッセージの表示

サーバーを実行するコンピュータの通知領域では、トレイアイコンが管理サーバーとレコーディングサーバーの状態を示します。これらのアイコンを使用すると、「サービス開始」などのステータスメッセージが表示されません。

1. 通知領域で、該当するトレイアイコンを右クリックします。コンテキストメニューが表示されます。

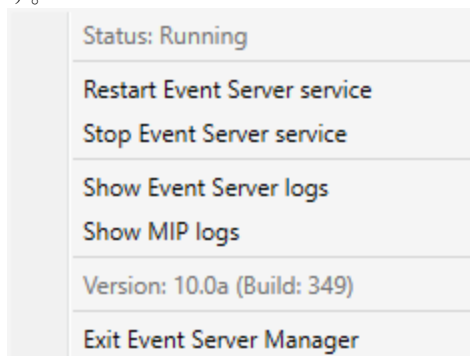
- ステータスメッセージの表示を選択します。サーバータイプに応じて、**管理サーバーのステータスメッセージ**または**レコーディングサーバーのステータスメッセージ**ウィンドウが表示され、タイムスタンプの付いたステータスメッセージが一覧表示されます。



Event Server サービスの開始、停止、再起動

通知領域では、トレイアイコンが Event Server サービスの状態(**実行中**など)を示します。このアイコンを使用して、Event Server サービスを開始、停止、再起動できます。サービスを停止する場合は、イベントとアラームを含むシステムの一部が動作しません。ただし、ビデオの表示と録画はできます。詳細については、「Event Server サービスの停止」を参照してください。

- 通知領域で、Event Server のトレイアイコンを右クリックします。コンテキストメニューが表示されます。



- サービスが停止した場合は、**[Event Server サービスの開始]**をクリックして開始します。トレイアイコンが変わり、新しい状態を示します。
- サービスを再起動または停止するには、**[Event Server サービスの再起動]**または**[Event Server サービスの停止]**をクリックします。

トレイアイコンの詳細については、「トレイアイコンについて 『260ページ』」を参照してください。

参照

Recording Server サービスの開始と停止 『258ページ』

Event Server サービスの停止

Event Server に MIP プラグインをインストールするときには、まず Event Server サービスを停止してから、再起動する必要があります。ただし、サービスが停止している間は、VMS システムのほとんどの領域が機能しません。

- イベントやアラームは Event Server に保存されません。ただし、システムおよびデバイスイベントは、録画の開始などのアクションをトリガーします。
- 分析イベントは動作しません。
- 汎用イベントは Network Video Management System Enterprise Edition で動作しません。
- アラームはトリガーされません。
- Network Video Management System Smart Client では、マップビュー項目、アラームリストビュー項目、およびアラームマネージャワークスペースは動作しません。
- Event Server の MIP プラグインを実行できません。
- Management Client および Network Video Management System Smart Client の MIP プラグインは正しく動作しません。

トレイアイコンについて

表のトレイアイコンは、管理サーバー、レコーディングサーバー、イベントサーバーで実行されるサービスが取り得る状態を示します。これらはすべて、サービスがインストールされているコンピュータの通知領域に表示されます。

Management Server サービスアイコン	Recording Server サービスアイコン	Event Server サービスアイコン	詳細
			実行中 サーバーサービスが有効で開始したときに表示されます。
			停止 サーバーサービスが停止したときに表示されます。
			起動中 サーバーサービスが起動処理中である場合に表示されます。通常、しばらくするとトレイアイコンは 実行中 に変わります。
			停止中 サーバーサービスが停止処理中である場合に表示されます。通常、しばらくするとトレイアイコンは 停止 に変わります。

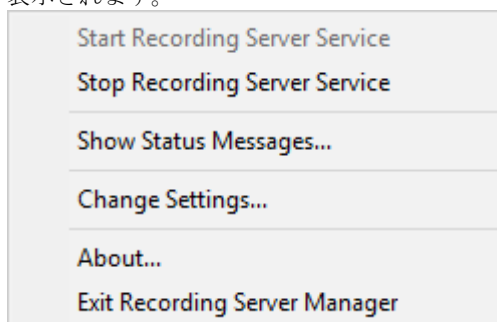
Management Server サービスアイコン	Recording Server サービスアイコン	Event Server サービスアイコン	詳細
			<p>不確定の状態</p> <p>サーバーサービスを最初にロードして、最初の情報をまだ受信していない場合に表示されます。最初の情報を受信すると、通常、起動中アイコンに変わり、その後実行中アイコンに変わります。</p>
			<p>オフラインで実行中</p> <p>通常は、Recording Server サービスが実行されているが、Management Server サービスが実行されていない場合に表示されます。</p>
			<p>管理者が承認する必要がある</p> <p>Recording Server サービスを初めてロードしたときに表示されます。管理者は、Management Client でレコーディングサーバーを承認します。サーバーリストを展開し、レコーディングサーバーノードを選択して、概要ペインで必要なレコーディングサーバーを右クリックしてから、レコーディングサーバーの承認を選択します。</p>

Recording Server サービスの設定の変更

使用するポート番号などの Recording Server サービスの基本的な設定を変更できます。

前提条件：設定を変更するには、まず、Recording Server サービスを停止する必要があります。Recording Server サービスが停止している間、システムはレコーディングサーバーに接続されているデバイスと通信できません。つまり、ライブビデオの表示またはビデオの録画ができません。

1. 通知領域で、レコーディングサーバーのトレイアイコンを右クリックします。コンテキストメニューが表示されます。



2. **Recording Server サービスの停止**を選択します。

3. トレイアイコンをもう一度右クリックします。
4. **設定の変更**を選択します。レコーディングサーバーの設定ウィンドウが表示されます。適切な設定を変更します。

参照

レコーディングサーバーの設定 『262ページ』

レコーディングサーバーの設定

レコーディングサーバーの設定を行う際には、以下を指定します。

名前	説明
アドレス	IP アドレス (例 : 123.123.123.123) またはホスト名 (例 : ourserver) を指定します。この情報は、レコーディングサーバーが管理サーバーと通信できるようにするために必要です。
ポート	管理サーバーと通信する際に使用するポート番号。デフォルトのポートは 9993 ですが、必要に応じて変更できます。
Web サーバーのポート	PTZ 制御コマンドの処理や、Network Video Management System Smart Client からの参照およびライブ要求の処理など、Web サーバーの要求に対応するために使用するポート番号。デフォルトのポートは 7563 ですが、必要に応じて変更できます。
アラートサーバーポート	レコーディングサーバーが TCP 情報をリスンする際に使用するポート番号 (一部のデバイスは、イベントメッセージを送信するために TCP を使用します)。デフォルトのポートは 5432 ですが、必要に応じて変更できます。
SMTP サーバーポート	レコーディングサーバーが簡易メール転送プロトコル(SMTP)情報をリスンする場合に使用します。SMTP は、サーバー間での E メールメッセージ送信の標準です。一部のデバイスは SMTP を使用して、イベントメッセージまたは画像を監視システムサーバーに電子メールで送信します。既定値は 25 番ポートです。このポートは有効および無効にできます。必要に応じて、ポート番号を変更できます。

Data Collector Server サービスの再起動

システムは Data Collector Server サービスを、管理サーバー、レコーディングサーバー、ログサーバー、イベントサーバーおよび NVMS Mobile サーバーと同じコンピュータに自動的にインストールします。

通常は、Data Collector Server サービスにはメンテナンスは必要ありませんが、サービスが停止した場合は、ライブフィードはシステムモニターに送信されません。これは、エラーメッセージによりシステムモニターに表示されます。

1. Data Collector Server サービスがインストールされているコンピュータで次の手順を実行します。
2. Windows のスタートメニューで、コントロールパネルを選択してから...
 - カテゴリビューを使用している場合、システムとセキュリティカテゴリを特定し、管理ツールをクリックします。

- 小さいアイコンまたは大きいアイコンを使用している場合、**管理ツール**をクリックします。
3. サービスをダブルクリックします。
 4. **Sony Network Video Management System Data Collector Server** を特定します。右クリックして**開始**を選択して、サービスを再開します。

登録済みサービス

場合によっては、システムとの通信機能が必要なサーバーまたはサービスのうち、システムに直接含まれていないものがあります。一部のサービスはシステムに自動的に登録できます（自動登録されないものもあります）。自動登録可能なサービス：

- Event Server サービス
- Log Server サービス
- Service Channel サービス

自動登録されるサービスは、登録済みサービスのリストに表示されます。

サーバーまたはサービスは、Management Client で登録済みサービスとして手動で指定できます。

サービスチャンネルについて

サービスチャンネルを使用すると、システムでサーバーとクライアント間での自動的に透明な設定の通信が可能になります。たとえば、共有ビューがクライアント上で変更されると、関連する共有ビューを使用してその変更が他のクライアント上に即座に反映されるようにするのは、サービスチャンネルです。また、サービスチャンネルにより、システムで多様なプラグインやアドオン製品を使用する場合に、サーバーとクライアント間での設定関連の通信が容易にできます。

通常は、サービスチャンネルは管理サーバーのインストールの一部としてインストールしますが、必要に応じて、監視システムの別のサーバーにサービスチャンネルをインストールすることもできます。

一度インストールされると、サービスチャンネルはシステムに自動的に登録されます（自動的に Management Client の登録済みサービス機能のリストに追加されます）。システムによって場所が認識されているため、システムにログインするクライアントは、自動的にサービスチャンネルを利用できます。

Service Channel サービスを実行しているサーバーの IP アドレスまたはホスト名を後で変更する場合、Management Client のツール > **登録済みサービス** で、情報を手動で編集する必要があります。また、Service Channel サービスがインストールされていたユーザーを後で変更する必要がある場合、Service Channel サービスを削除し、その後で新しいユーザーとして再度インストールする必要があります。

Network Video Management System Smart Client のインスタンスの時刻が、Service Channel サービスを実行しているコンピュータと同期していることが非常に重要です。Network Video Management System Smart Client の時刻が、管理サーバーや Service Channel サービスを実行しているコンピュータと同期されていない場合、Network Video Management System Smart Client で他のユーザーが行った設定の変更に関する情報が Network Video Management System Smart Client で更新されません。この場合、互いに他のユーザーの設定変更を上書きしてしまう危険性があります。Network Video Management System Smart Client の時刻が Service Channel サービスを実行しているコンピュータの時刻と同期されていない場合には、それを通知するエラーが表示されます。

登録済みサービスの追加と編集

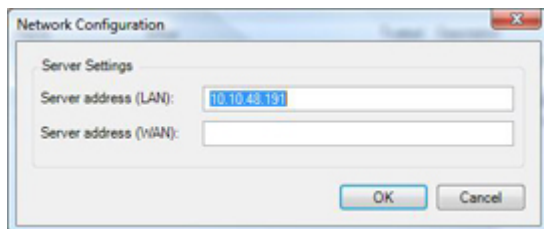
1. 登録済みサービスの追加/削除ウィンドウで、必要に応じて**追加**または**編集**をクリックします。
2. 前の選択により開いた**登録済みサービスの追加**または**登録済みサービスの編集**ウィンドウで、設定を指定または編集します。
3. **OK** をクリックします。

ネットワーク設定の管理

ネットワーク設定で、管理サーバーのサーバーLAN アドレスと WAN アドレスを指定し、管理サーバーと信頼済みサーバーが通信できるようにします。

1. 登録されているサービスの追加と削除ウィンドウで、**ネットワーク**をクリックします。
2. 管理サーバーの LAN および/または WAN IP アドレスを指定します。

すべての関係するサーバー（管理サーバーと信頼済みサーバーの両方）がローカルネットワークにある場合は、LAN アドレスを指定するだけです。1 つまたは複数の関係するサーバーがインターネット接続でシステムにアクセスする場合は、WAN アドレスも指定する必要があります。



3. **OK** をクリックします。

登録済みサービスのプロパティ

登録済みサービスの追加または登録済みサービスの編集ウィンドウで、以下を指定します。

コンポーネント	要件
タイプ	事前に入力されているフィールド。
名前	登録されているサービスの名前です。Management Client では名前は表示目的でのみ使用されます。
URL	<p>追加をクリックし、登録済みサービスの IP アドレスまたはホスト名を追加します。URL の一部としてホスト名を指定する場合、そのホストが存在し、ネットワークで使用できる必要があります。URL は http://または https://から始まるものとし、以下の文字を使用してはなりません:< > & ' " * ? / [] "。</p> <p>代表的 URL フォーマットの例 : http://ipaddress:port/directory (ポートおよびディレクトリはオプション) 必要であれば複数の URL を追加することもできます。</p>

コンポーネント	要件
信頼済み	<p>登録済みサービスをすぐに信頼済みにすべき場合に選択します（これが大半の場合に当てはまりますが、登録済みサービスを追加してから後で、これを編集して信頼済みにすることもできます）。</p> <p>信頼済みステータスに変更すると、その登録済みサービスに定義した1つまたは複数の URL を共有する登録済みサービスの状態も変更されます。</p>
詳細	<p>登録されているサービスの説明です。Management Client では、説明は表示目的でのみ使用されます。</p>
詳細	<p>サービスが高度な場合、定義するホストアドレスごとに特定の URI スキーマ（http、https、tcp、udp など）を設定する必要があります。このため、ホストアドレスには複数のエンドポイントが含まれ、それぞれが独自のスキーマ、ホストアドレス、およびスキーマの IP ポートを持ちます。</p>

索引

- [
- [録画]タブについて - 102
- A**
- Active Directory - 16
- Active Directory の準備 - 23
- AVI 生成タブ(オプション) - 207, 210
- D**
- Data Collector Server サービスの再起動 - 262
- Download Manager/ダウンロード Web ページ - 43
- Download Manager インストーラコンポーネントの追加と公開 - 45
- Download Manager インストーラコンポーネントの非表示および削除 - 46
- Download Manager のデフォルト設定 - 44
- Download Manager の標準インストーラ (ユーザー) - 44
- E**
- Event Server - 15
- Event Server サービスの開始、停止、再起動 - 258, 259
- Event Server サービスの停止 - 260
- E メール通知をトリガするルールを使用する - 161, 210
- I**
- IPv6 と IPv4 について - 20
- IPv6 アドレスの記述方法について - 21
- IPv6 を使用するシステムの使用について - 20
- IP アドレス範囲の割り当て - 77
- K**
- Kerberos 認証について - 26, 36
- Kerberos 認証を設定します。 - 36
- L**
- Log Server - 16
- M**
- Management Client ウィンドウ概要 - 52
- Management Client エlement - 11, 55, 57
- Management Client のシステムの構成 - 30, 33, 39
- Management Client のバージョン情報 - 17
- Management Client 概要 - 17, 52
- Management Server サービスの開始と停止 - 257, 258
- Matrix - 136
- Matrix タブ(役割) - 188
- Matrix について - 136
- Matrix 受信者の追加 - 136
- Matrix 受信者へのビデオ送信ルールの定義 - 137
- MIP タブ (役割) - 189
- Mobile Server Manager - 234
- Mobile Server Manager について - 234
- Mobile サーバーの設定 - 229
- Mobile サーバーの追加または編集 - 225
- Mobile サービスの起動、停止、再起動 - 234, 237
- N**
- Network Video Management System Smart Client について - 17

- Network Video Management System Smart Client のサイレントインストール - 41
- Network Video Management System Smart Wall - 218
- Network Video Management System Smart Wall について - 129, 218
- Network Video Management System Smart Wall のユーザー権限の設定 - 220
- Network Video Management System Smart Wall ライセンス - 218
- Network Video Management System Web Client について - 19
- Network Video Management System Web Client へのアクセス - 234, 235
- NVMS Mobile - 224
- NVMS Mobile クライアントについて - 18
- NVMS Mobile サーバーについて - 225
- NVMS Mobile サーバーのインストール - 42, 238
- NVMS Mobile で使用する出力の名前について - 229
- NVMS Mobile について - 224
- NVMS Mobile の概要 - 224
- NVMS Mobile を使用するための前提条件 - 225
- NVMS Mobile 構成 - 43, 225, 238
- P**
- PTZ セッションタイムアウトの指定 - 113
- PTZ セッションの優先度 - 108, 114
- PTZ タブ (ビデオエンコーダー) - 86
- PTZ タブ (役割) - 108, 185
- R**
- Recording Server サービスの開始と停止 - 258, 259
- Recording Server サービスの設定の変更 - 261
- S**
- Smart Client プロファイル - 131
- Smart Client プロファイル、役割および時間プロファイルの作成および設定 - 131
- Smart Client プロファイルについて - 131
- Smart Client プロファイルのコピー - 131
- Smart Client プロファイルのプロパティ - 134
- Smart Client プロファイルの追加と設定 - 131
- Smart Wall タブ (役割) - 187, 220
- Smart Wall のプロパティ - 221
- Smart Wall の設定 - 218
- Smart Wall プリセットのあるルールの使用について - 221, 222
- SNMP - 242
- SNMP サービスのインストール - 242
- SNMP サービスの設定 - 242
- SNMP のサポートについて - 242
- SQL Server - 16
- SQL Server アドレスの更新について - 252
- SQL Server タイプを決定する - 25
- SQL Server トランザクションログについて - 249
- SQL Server の管理 - 252
- W**
- Windows タスクマネージャ : プロセスの終了時に注意する - 50

あ

アーカイブされた記録をバックアップする - 68

アーカイブされていない記録をあるストレージから別のストレージへ移動する - 70, 71

アーカイブの構造について - 69

アーカイブ設定のプロパティ - 40, 68, 72

アクションとアクションの停止について - 106, 139

アクションについて - 228

アクセスコントロールタブ(役割) - 189

アクティベーションなしのデバイスの変更 - 57, 58

アクティベーションなしのデバイスの変更数の計算方法 - 58

アップグレード - 47

アップグレードについて - 23, 47

アップグレードの推奨手順 - 48

アップグレードの前提条件 - 47, 48, 60

アナリティック イベント - 165

アナリティックイベントタブ(オプション) - 207, 211

アナリティックイベントについて - 165

アナリティックイベントをテストする(プロパティ) - 166

アナリティックイベント設定の編集 - 167

アラーム - 199

アラームデータ設定 - 204

アラームについて - 194, 200

アラームの追加 - 201, 204

アラーム設定について - 199

アラーム定義 - 201

アラーム定義 (プロパティ) - 201, 202

イベントサーバータブ(オプション) - 207, 212

イベントサーバー設定のバックアップおよび復元 - 250

イベントサーバー設定のバックアップおよび復元について - 247

イベントタブ(デバイス) - 92, 93, 119

イベントタブ (プロパティ) - 121

イベントタブについて - 119

イベントに複数のインスタンスを使用する - 120, 121

イベントの追加 - 120

イベントプロパティの指定 - 120

イベント概要 - 139, 145, 203

インストール - 11, 23

インストールのトラブルシューティング - 37

インストールを開始する前に - 23

インストール方法 - 23

ウイルススキャンについて - 27

オプションダイアログボックス - 206

オペレータが簡易モードと詳細モードで切り替えられないようにする - 133

か

カメラからのプリセット位置を使用します (タイプ 2) - 110

カメラデバイスについて - 40, 90

カメラ設定について - 99

- キーフレームレコーディングの有効化 - 106
- キーフレーム設定の選択 - 128
- クライアント - 17, 129
- クライアントタブ(デバイス) - 121
- クライアントタブについて - 121
- クライアントタブのプロパティ - 122
- クライアントについて - 129
- クライアントのインストール - 31, 41
- クラスタでのアップグレード - 217
- クラスタでのインストール - 215, 217
- クラスタリングの前提条件 - 215
- このシステムで使用するポート - 244
- さ
- サーバーサービスの管理 - 250, 257
- サーバーステータス - 231
- サーバーとハードウェア - 61
- サーバーログ - 195
- サーバーログタブ(オプション) - 196, 207, 209
- サービスアカウントを選択してください - 26
- サービスチャンネルについて - 56, 263
- サイト情報 - 60
- サイト情報の更新 - 61
- ジェネリックイベント - 168
- ジェネリックイベント (プロパティ) - 168, 169
- ジェネリックイベントタブ(オプション) - 168, 207, 213
- ジェネリックイベントデータソース(プロパティ) - 171
- ジェネリックイベントについて - 168, 213
- ジェネリックイベントの追加 - 168
- システムコンポーネント - 15
- システムダッシュボード - 190
- システムダッシュボードについて - 190
- システムのインストール - 29, 39
- システムのインストール - カスタムオプション - 29, 31
- システムのインストール - シングルサーバーオプション - 29
- システムのインストール - 分散オプション - 29, 30
- システムのメンテナンス - 11, 244
- システムログ (プロパティ) - 197
- システム概要 - 11, 13
- システム監視しきい値 - 190, 193
- システム監視しきい値の設定 - 193, 194
- システム監視について - 190, 193
- システム監視の詳細 - 192
- システム設定のスケジュールされたバックアップと復元について - 248
- システム設定のバックアップおよび復元 - 69, 246
- システム設定のバックアップおよび復元について - 48, 55, 246
- システム設定の移動 - 252
- システム設定の手動バックアップ - 247
- システム設定の手動バックアップおよび復元 - 246, 248

- システム設定の手動バックアップについて - 246
- システム設定の復元（スケジュールされたバックアップから） - 250, 252
- システム設定の復元（手動バックアップから） - 247
- システム要件 - 22
- スケジュールされたバックアップと復元 - 248
- スケジュールされたバックアップによるシステム設定のバックアップ - 249, 252
- ステータスの表示について - 235, 240
- ストリームタブ(デバイス) - 91, 100
- ストリームタブについて - 100
- ストリームの追加 - 101
- ストレージおよび録画設定プロパティ - 67, 71
- ストレージタブ（レコーディングサーバー） - 65
- ストレージでのアーカイブの作成 - 65, 67
- ストレージでのアーカイブの削除 - 70
- ストレージとアーカイブについて - 39, 65, 107
- ストレージについて - 106
- ストレージの削除 - 70
- スピーカーデバイスについて - 92
- スマート検索モーションデータの生成について - 128
- セキュリティ - 172
- セキュリティ全般タブ（役割） - 52, 108, 173, 177
- ソフトウェアライセンスコードの変更 - 39, 40
- ソフトウェアライセンスコードを登録する - 28, 41
- た
 - ダイナミック感度について - 127
 - タイムサーバーについて - 51
 - ダッシュボードのカスタマイズ - 190, 191
 - データグラムオプションの指定 - 77
 - デバイス - 87
 - デバイスグループについて - 87
 - デバイスグループに含めるデバイスの指定 - 88, 89
 - デバイスグループのすべてのデバイスに対する共通プロパティの指定 - 88, 90
 - デバイスグループの操作 - 87
 - デバイスグループの追加 - 88
 - デバイスグループ経由のデバイスの有効化/無効化 - 91, 92, 93, 94, 95
 - デバイスタブ(役割) - 182
 - デバイスについて - 87, 90
 - デバイスのステータスアイコン - 95
 - デバイスの使用 - 40, 90
 - デバイスパックのインストーラ - ダウンロードする必要があります - 46
 - デフォルトのプリセット位置の割り当て - 111
 - デフォルトルールについて - 151
 - トレイアイコンについて - 257, 258, 259, 260
- な
 - ネットワークタブ(オプション) - 211
 - ネットワークタブ（レコーディングサーバー） - 78
 - ネットワーク設定の管理 - 264

は

ハードウェア - 79

ハードウェアについて - 79

ハードウェアの移動 - 61, 70, 82

ハードウェアの移動 (ウィザード) - 83

ハードウェアの管理 - 85

ハードウェアの交換 - 60, 254

ハードウェアの追加 - 40, 61, 62, 79

ハードウェアの編集 - 81

ハードウェアの有効化/無効化 - 80

ハードウェアへの安全な接続設定する - 81

ハードディスクの故障: ドライブを保護する - 50

はじめに - 11

バックアップ/復元の失敗と問題のシナリオについて - 247

パトロールタブ(デバイス) - 115

パトロールタブについて - 115

パトロール設定でのプリセット位置の指定 - 116

パトロール設定の追加 - 87, 116

パフォーマンス - 232

パブリックアドレスとポートの定義 - 78

パブリックアドレスを使用する理由 - 78

ビデオエンコーダーでの PTZ の有効化 - 86

ビデオデバイスドライバー - 256

ビデオデバイスドライバーについて - 83, 256

ビデオデバイスドライバーの削除について - 257

ビデオプッシュ - 231

ビデオプッシュを使用した動画のストリーミングについて - 226

ビデオを流すための「ビデオ・プッシュ」の設定 - 226, 232

ビューグループ - 130

ビューグループタブ (役割) - 188

ビューグループと役割について - 130

ビューグループについて - 130

ビューグループの追加 - 130

フェールオーバータブ (レコーディングサーバー) - 74

フェールオーバータブのプロパティ - 74, 75

フェールオーバーレコーディングサーバーの割り当て - 74

フェールオーバー管理サーバー - 15, 215

プライバシーマスクタブ(デバイス) - 123

プライバシーマスクタブ (プロパティ) - 124

プライバシーマスクタブについて - 123

プライバシーマスクの有効化/無効化 - 124

プライバシーマスク設定を指定する - 124

プリセットタブ (Smart Wall プロパティ) - 222

プリセットタブ(デバイス) - 108

プリセットタブ (モニタープロパティ) - 224

プリセットタブについて - 108

プリセット位置のロック - 113

プリセット位置をテストする (タイプ 1 のみ) - 113

プリセット位置を追加する (タイプ 1) - 87, 109, 113

プリセット位置を編集する (タイプ 1 のみ) - 111, 113

プリセット位置名の編集 (タイプ 2 のみ) - 111, 112

プレバッファについて - 104

プレバッファの管理 - 105

ペインの概要 - 54

ヘルプのご紹介 - 11

ポート番号の表示/編集 - 234, 237

ま

マイクデバイスについて - 91

マルチキャストタブ (レコーディングサーバー) - 75

マルチキャストについて - 76, 122

マルチキャストの有効化 - 76

マルチストリーミングについて - 99, 100

メールサーバータブ(オプション) - 207, 210

メタデータデバイスについて - 92

メニュー概要 - 55

モーションタブ(デバイス) - 91, 125

モーションタブについて - 125

モーション検知の有効化と無効化 - 126

モーション検知設定の指定 - 126

モニタープロパティ - 223

や

ユーザーおよびグループタブ(役割) - 177

ユーザーおよびグループの役割からの削除、役割への割り当て - 40, 173, 175, 177

ユーザーについて - 173, 177

ユーザー設定タブ(オプション) - 211

ユーザー定義イベント - 163

ユーザー定義イベントについて - 149, 163, 203

ユーザー定義イベントの追加 - 164

ユーザー定義イベントの名前変更 - 165

よくある質問(FAQ) - 237

ら

ライセンスとハードウェアデバイスの交換 - 60

ライセンスについて - 19, 47, 57, 60

ライセンスをオフラインで認証 - 40, 58, 59, 60

ライセンス情報 - 57

リモートレコーディングタブ (役割) - 187

リモート録画について - 108

ルール - 150

ルールとイベント - 138

ルールとイベントについて - 40, 138

ルールについて - 150, 194

ルールの検証について - 153

ルールの追加 - 139, 154, 221

ルールの複雑性について - 154

ルールログ (プロパティ) - 198

ルールを編集、コピー、名前を変更する - 155

ルールを無効/有効にする - 155

レイアウトタブ (Smart Wall プロパティ) - 222

レコーディング サーバー - 15, 61

レコーディングサーバーステータスアイコン - 63

レコーディングサーバーでのすべてのハードウェアの削除 - 61, 79

レコーディングサーバーについて - 61

レコーディングサーバーのインストール - 31, 32, 48, 83

レコーディングサーバーのサイレントインストール - 33, 48

レコーディングサーバーの基本設定の変更/確認 - 62

レコーディングサーバーの交換 - 82, 255

レコーディングサーバーの削除 - 61, 79

レコーディングサーバーの設定 - 262

レコーディングサーバーの認証 - 39, 61, 62, 83

レコーディングフレームレートを指定する - 106

ローカル IP アドレス範囲について - 41

ローカル IP 範囲の割り当て - 79

ログイン概要 - 52

ログサーバーデータベースのバックアップ - 246, 251

ログサーバーの SQL アドレスの更新 - 252

ログについて - 195, 209

ログのエクスポート - 196

ログの検索 - 196

ログへのアクセスおよびエクスポートについて - 234, 236

ログ言語の変更 - 197

ログ設定 - 234

わ

ワークグループのインストール - 36, 49

ワークグループの他のアップグレード方法 - 37, 48

索引

漢字

一般 - 229

一般タブ (オプション) - 207

一方向の信頼のマルチドメイン環境 - 241

一方向の信頼の設定 - 241

音声の設定 - 206

仮想サーバー - 16

夏時間について - 51

画像処理間隔を選択 - 128

外部イベントタブ (役割) - 187

各プリセット位置での時間を指定 - 116

監査ログ (プロパティ) - 198

監視サーバーの資格情報の入力/編集 - 234, 237

管理サーバー - 15

管理サーバーの移動 - 250

管理サーバーの移動について - 250

管理サーバーまたはイベントサーバーの SQL Server アドレスの更新 - 253

管理サーバーまたはレコーディングサーバーのステータスメッセージの表示 - 258

簡易モードをデフォルトモードとして設定 - 132, 134

関連するデバイスで録画を有効にする - 104, 122

基本 - 57

基本ユーザー - 189

基本ユーザーについて - 174, 189

基本ユーザーの作成 - 174, 189

機能設定 - 11, 215

- 記録データベースを破損から守る - 50, 63
- 記録の有効化と無効化 - 103
- 魚眼レンズサポートを有効/無効にする - 119
- 魚眼レンズタブ(デバイス) - 118
- 魚眼レンズタブについて - 118
- 魚眼レンズ設定の指定 - 119
- 共有バックフォルダの選択 - 248
- 警告タブ (役割) - 188
- 検知方法の指定 - 128
- 現在のタスクについて - 194
- 個々のカメラに対してマルチキャストを有効にする
- 78
- 個々のデバイスの有効化/無効化 - 81
- 個別のデバイスまたはデバイスのグループをストレ
ージに接続する - 40, 66, 68
- 使用できない管理サーバーについて - 251
- 時間プロファイル - 156
- 時間プロファイルについて - 156
- 時間プロファイルの指定 - 157
- 時間プロファイルの編集 - 158
- 自動エクスポートルールの追加 - 229
- 手動で出力を有効にしてテストします。 - 94
- 手動で入力 を有効にしてテストする - 94
- 手動感度の有効化 - 127
- 手動記録の管理 - 105
- 終了位置の指定 - 118
- 出力デバイスについて - 94
- 初めての使用 - 11, 50
- 索引
- 証明書の編集 - 230, 234, 236
- 情報タブ (Smart Wall プロパティ) - 221
- 情報タブ(デバイス) - 91, 92, 93, 94, 97
- 情報タブ (ハードウェア) - 85
- 情報タブ (モニタープロパティ) - 223
- 情報タブ (レコーディングサーバー) - 64
- 情報タブ(役割) - 52, 177
- 情報タブについて - 97
- 情報タブのプロパティ - 64, 97
- 新しいレコーディングストレージの追加 - 65, 67
- 推奨事例 - 50
- 製品概要 - 13
- 接続 - 230
- 設定タブ(デバイス) - 91, 92, 93, 94, 98
- 設定タブ (ハードウェア) - 85
- 設定タブについて - 98
- 設定レポートについて - 195
- 設定レポートの詳細 - 195
- 設定レポートの追加 - 195
- 旋回動作をカスタマイズ - 117
- 選択したストレージまたはアーカイブ設定の編集 -
68
- 前提条件 - 160
- 組み込みヘルプシステムの操作 - 11
- 著作権、商標、および免責条項 - 10
- 調査 - 232
- 調査の設定 - 225

- 追加ライセンスの取得 - 58, 60
- 通知プロファイル - 160
- 通知プロファイル (プロパティ) - 162
- 通知プロファイルについて - 160, 210
- 通知プロファイルの追加 - 160
- 通話タブ(役割) - 186
- 停電 : UPS の使用 - 50
- 登録済みサービス - 263
- 登録済みサービスのプロパティ - 264
- 登録済みサービスの追加と編集 - 264
- 同じビデオを複数の Network Video Management System Smart Client ビューに送信する - 137
- 日の長さの時間プロファイルについて - 157, 159
- 日の長さの時間プロファイルのプロパティ - 159
- 日の長さの時間プロファイルの作成 - 159
- 入力デバイスについて - 93
- 複数の管理サーバー (クラスタ) - 215
- 分散型システム設定 - 14
- 分析イベントを追加し、編集。 - 165
- 分析種目のテスト - 166
- 問題 : SQL Server の位置を変更すると、データベースにアクセスできない - 39
- 問題 : ポートの競合により Recording Server の起動が失敗する - 37
- 役割 - 172
- 役割について - 40, 172
- 役割のコピー、名前の変更、削除 - 175
- 役割の権限について - 173
- 役割の設定 - 175, 177
- 役割の追加および管理 - 173, 174
- 有効な役割の表示 - 176
- 猶予期限が切れた後にライセンスを認証する - 58, 60
- 領域の除外を指定 - 128
- 録画タブ(デバイス) - 91, 92, 93, 102
- 閾値の指定 - 127