

AXIS Camera Station S1232 Tower Recording Server

目次

デバイスについて	4
使用に当たって	5
デバイスをインストールする	6
インストール前	6
デバイスを構成する	7
Axisレコーダーの初期設定	7
AXIS Camera Station Proの設定	7
ビデオ管理システムを起動する	8
デバイスの追加	8
録画方法の設定	8
ライブビデオを表示する	8
録画の表示	8
ブックマークの追加	8
録画のエクスポート	9
AXIS File Playerでの録画の再生と検証	9
ネットワーク設定	9
サーバーポートの設定	10
セキュリティに関する考慮事項	10
システムをオンラインでライセンスする	10
オフラインのシステムをライセンスする	10
ローカル Windows® ユーザーアカウントの管理	12
ユーザーアカウントの作成	12
管理者アカウントを作成する	12
ローカルユーザーグループを作成する	12
ユーザーアカウントを削除します。	12
ユーザーアカウントのパスワードを変更する	13
ユーザーアカウントのパスワードリセットディスクを作成する	13
AXIS Camera Station Proのユーザーアカウントの管理	14
ユーザー権限	14
ユーザーまたはグループの追加	14
ユーザーまたはグループの権限	15
デバイスを管理する	18
セキュアブートの証明書を更新する	18
証明書のステータスを確認する	18
推奨されるアクション	19
BIOSを通じて証明書を更新する	19
Windows Updateを通じて証明書を更新する	19
現在のBIOSのバージョンを確認する	20
BIOSを更新する	20
Windows®を更新します	20
Windows®の更新プログラムの設定を構成する	20
ハードドライブの追加	21
ワークフロー	21
ホットスワップハードドライブを取り付ける	22
RAIDの変更	22
新しいRAIDアレイの作成	23
Microsoft Windows®の設定	24
iDRACの設定	25
サイバーセキュリティ	26
セキュアブート	26
Trusted Platform Module (TPM)	26
Axisセキュリティ通知サービス	27
脆弱性の管理	27

Axis装置のセキュアな動作	27
トラブルシューティング	28
診断を実行する	28
システムリカバリの実行.....	28
内部リカバリ	28
外部リカバリ	28
SupportAssistコレクションのエクスポート	29
電源ユニットのトラブルシューティング.....	30
メモリーエラーのトラブルシューティング	30
AXIS Camera Station Proのトラブルシューティング	30
製品概要.....	31
前面と背面.....	31
仕様.....	32
.....	32
さらに支援が必要ですか?.....	35
参考リンク.....	35
サポートに問い合わせる.....	35

デバイスについて

AXIS Camera Station S12 Recorderシリーズは、最大4Kまでの高解像度監視に対応したオールインワン型のラックサーバーおよびワークステーションです。迅速かつ簡単にインストールできるように、このレコーダーシリーズにはAXIS Camera Station Proのビデオ管理ソフトウェアが事前に構成されてプリロードされています。ライセンスおよび必要なすべてのシステムソフトウェアも含まれています。システム設定はAXIS Site Designerから簡単にインポートできます。AXIS Camera Station Proを使用することで、Axisの幅広いビデオ監視デバイスを最大限に活用できます。エンタープライズグレードのハードディスク、ソリッドステートドライブに保存されたオペレーティングシステムにより、このレコーダーシリーズはシステムに高いパフォーマンスと信頼性を提供します。

使用に当たって

AXIS Camera Station Pro録画サーバーを設定する標準的なワークフローは次のとおりです。

1. デバイスをインストールする。
2. Windows®の初期設定:装置を設置した後、いくつかの手順に従って、地域、言語、キーボードレイアウト、管理者アカウントとそのパスワードを設定します。
3. Axisレコーダーの初期設定:Windowsの初期設定の後、AXIS Recorder Toolboxが開き、コンピューター名、日付と時刻、ネットワークなど、基本的かつ必要な設定を行う手順が表示されます。Axisレコーダーの初期設定, on page 7を参照してください。
4. Windows®を構成します。以下をお勧めします。
 - Windows®を最新バージョンに更新します。Windows®を更新します, on page 20を参照してください。
 - 標準ユーザーアカウントを作成します。ユーザーアカウントの作成, on page 12を参照してください。
5. AXIS Camera Station Proを最新バージョンに更新します。
 - システムがオンラインの場合：AXIS Recorder Toolboxアプリを開いて、**[Update AXIS Camera Station Pro 2 (AXIS Camera Station Pro2の更新)]** をクリックします。
 - システムがオフラインの場合：axis.com に移動し、最新バージョンをダウンロードしてください。
6. AXIS Camera Station Proクライアントを起動します。
7. AXIS Camera Station Proサーバーに接続します。
8. AXIS Camera Station Proの設定, on page 7.

デバイスをインストールする

インストール前

- ・ 設置に使用する追加のアクセサリ (モニター、マウス、キーボード、ネットワークケーブル) を準備します。
- ・ 異なるユーザーアカウントの使用方法を理解してください。

次の表に、Axisシステムのインストール、設定、操作に使用できるユーザーアカウントを示します。

ユーザーアカウント	説明	注
MyAxis	最新のソフトウェアのダウンロード、ライセンスシステムへのアクセス、Axisセキュアリモートアクセス、システムの健全性監視に使用。	<i>my.axis.com</i> から登録。
Windows®		
Windows® 管理者	Windows® の管理者権限。AXIS Camera Station Proの管理者として使用しないことをお勧めします。	Windows® の初期設定中に作成されます。
AXIS Camera Station Proの管理者権限を持つ Windows® ユーザー	AXIS Camera Station Proの管理者権限が付与されたWindows® ユーザー。システムインテグレーターまたはシステム管理者が設定またはトラブルシューティングに使用。	Windows® の設定で作成されます。
AXIS Camera Station Proのオペレーターまたは閲覧者権限を持つ Windows® ユーザー	AXIS Camera Station Proのオペレーターまたは閲覧者権限が付与された Windows® ユーザー。	Windows® の設定で作成されます。
ハードウェアの管理		
iDRAC	iDRAC (Integrated Dell Remote Access Controller) ツールへのアクセスに使用。	ユーザー名：root パスワード:情報タグの背面に印刷されています。
デバイス		
装置管理者	管理者がビデオ管理システムから、またはデバイスのWebページからカメラにアクセスするために使用。	デバイスのWebページから、またはデバイスをAXIS Camera Station Proに追加したときに作成されます。

デバイスを構成する

Axisレコーダーの初期設定

Windows®の設定が完了すると、AXIS Recorder Toolboxが自動的に開き、初回設定のセットアップアシスタントの説明が表示されます。このセットアップアシスタントで、AXIS Recorder Toolboxで装置を管理する前に、いくつかの基本的で必要な設定を行います。

1. [Light (ライト)] または [Dark (ダーク)] テーマを選択し、[Next] (次へ) をクリックします (ご使用の製品で選択できる場合)。
2. 必要に応じコンピューター名を変更し、[Next] (次へ) をクリックします。
3. [Date and time (日付と時刻)] で以下の設定を行い、[Next] (次へ) をクリックします。
 - タイムゾーンを選択します。
 - NTPサーバを設定するには、[NTP server (NTP サーバー)] を選択し、NTPサーバーのアドレスを入力します。
 - 手動で設定するには、[Manual (手動)] を選択し、日付と時刻を選択します。
4. [Network settings (ネットワーク設定)] で以下の設定を行い、[Next] (次へ) をクリックします。
 - [Use automatic IP settings (DHCP) (自動IP設定 (DHCP) を使用する)] と [Use automatic DNS settings (自動DNS設定を使用する)] は、デフォルトでオンになっています。
 - デバイスがDHCPサーバーを使用してネットワークに接続されている場合は、割り当てられたIPアドレス、サブネットマスク、ゲートウェイ、および優先DNSが自動的に表示されます。
 - デバイスがネットワークに接続されていないか、利用可能なDHCPサーバーがない場合は、ネットワークの要件に応じて、IPアドレス、サブネットマスク、ゲートウェイ、および優先DNSを手動で入力します。
5. **Finish (終了)** をクリックします。コンピューター名を変更した場合、AXIS Recorder Toolboxからデバイスの再起動を求めるメッセージが表示されます。

AXIS Camera Station Proの設定

開始する前に、以下をご確認ください。

- インストール内容に応じてネットワークを設定します。ネットワーク設定を参照してください。
- 必要な場合は、サーバーポートを設定します。サーバーポートの設定を参照してください。
- セキュリティ上の問題を考慮します。セキュリティに関する考慮事項を参照してください。

必要な設定を行ったら、AXIS Camera Station Proで作業を開始ができます。

1. ビデオ管理システムを起動する
2. デバイスの追加
3. 録画方法の設定, on page 8
4. ライブビデオを表示する, on page 8
5. 録画の表示, on page 8
6. ブックマークの追加, on page 8
7. 録画のエクスポート, on page 9
8. AXIS File Playerでの録画の再生と検証, on page 9

ビデオ管理システムを起動する

AXIS Camera Station Proクライアントアイコンをダブルクリックすると、クライアントが起動します。クライアントの初回起動時には、クライアントが同じコンピューターにインストールされたAXIS Camera Station Proサーバーに自動的にログインしようとします。

複数のAXIS Camera Station Proサーバーに、異なる方法で接続できます。

デバイスの追加

AXIS Camera Station S1232 Tower Recording Serverを初めて起動すると、[Add devices (デバイスの追加)] ページが開き、デバイスを追加するネットワークを検索します。

1. 追加するデバイスをリストから選択します。デバイスが見つからない場合は、[Manual search (手動検索)] をクリックするか、入力して絞り込みます。
2. [追加] をクリックします。
3. [Close (閉じる)] をクリックして設定をスキップし、後で続行します。ここで設定を続行する場合は以下の手順に従います。
 - 3.1. [Quick configuration (クイック設定)] または [Site Designer configuration (Site Designer設定)] を選択します。詳細については、を参照してください。
 - 3.2. [Add image overlay for date, time, and text (日付、時刻、テキストの画像オーバーレイを追加する)] を選択して、オーバーレイが設定されていないAxisカメラにオーバーレイを追加します。
 - 3.3. [Next (次へ)] をクリックします。
 - 3.4. [Recording method (録画方法)] の設定を選択します。
 - 3.5. [Next (次へ)] をクリックします。
 - 3.6. [Retention time (保存期間)] と [Recording storage (録画ストレージ)] を選択し、[Finish (終了)] をクリックして設定を適用します。

録画方法の設定

1. [設定] - [録画とイベント] - [録画方法] を選択します。
2. カメラを選択します。
3. [Motion detection (動体検知)] または [Continuous (連続)] をオンにします。
4. [適用] をクリックします。

ライブビデオを表示する

1. [Live view (ライブビュー)] タブを開きます。
2. ライブビデオを表示するカメラを選択します。

録画の表示

1. [Recordings (録画)] タブを開きます。
2. 録画を表示するカメラを選択します。

ブックマークの追加

1. 録画に移動します。
2. タイムラインで、ズームインとズームアウトを行い、マーカーが目的の位置になるようにタイムラインを動かします。
3.  をクリックします。

4. ブックマークの名前と説明を入力します。キーワードを使用すると、ブックマークが見つけやすくなります。
5. 録画をロックするには、[録画削除を防止] を選択します。

注

録画のロックを解除するには、[Prevent recording deletion (録画削除を防止)] をクリアするか、ブックマークを削除します。

6. [OK] をクリックして、ブックマークを保存します。

録画のエクスポート

1. [Recordings (録画)] タブを開きます。
2. 録画をエクスポートするカメラを選択します。
3.  をクリックすると、選択マーカが表示されます。
4. マーカーをドラッグして、エクスポートする録画を含めます。
5.  をクリックして、[Export (エクスポート)] タブを開きます。
6. [Export... (エクスポート)] をクリックします。

AXIS File Playerでの録画の再生と検証

1. エクスポートした録画を含むフォルダーに移動します。
2. AXIS File Playerをダブルクリックします。
3.  をクリックすると、録画のノートが表示されます。
4. デジタル署名を検証するには、次のようにします。
 - 4.1. [Tools > Verify digital signature (ツール > デジタル署名の検証)] に移動します。
 - 4.2. [Validate with password (パスワードで検証)] を選択し、パスワードを入力します。
 - 4.3. [Verify (検証)] をクリックして検証結果を確認します。

注

- デジタル署名は署名付きビデオとは異なります。署名付きビデオは、そのビデオが録画されたカメラを特定できるため、改ざんされていないことを確認できます。詳細については、署名付きビデオとカメラのユーザーマニュアルを参照してください。
- 保存されたファイルがAXIS Camera Stationデータベースと接続していない場合 (インデックスされていないファイル)、AXIS File Playerで再生できるように変換する必要があります。ファイルの変換については、Axisテクニカルサポートにお問い合わせください。

ネットワーク設定

クライアント、サーバー、接続されているネットワークデバイスが異なるネットワーク上にある場合は、AXIS Camera Station S1232 Tower Recording Server使用する前にプロキシまたはファイアウォールを設定します。

クライアントのプロキシ設定

プロキシサーバーがクライアントとサーバーの間にある場合は、クライアントコンピュータのWindowsでプロキシ設定を行います。詳細については、Axisサポートまでお問い合わせください。

サーバーのプロキシ設定

プロキシサーバーがネットワークデバイスとサーバーの間にある場合は、サーバー上のWindowsでプロキシ設定を行う必要があります。詳細については、Axisサポートまでお問い合わせください。

NATとファイアウォール

クライアントとサーバーがNATまたはファイアウォールで隔てられている場合は、AXIS Camera Station S1232 Tower Recording Server Service Controlで指定されているHTTPポート、TCPポート、ストリーミングポートが、ファイアウォールやNATを通過できるように設定します。ネットワーク管理者にサポートを依頼してください。

サーバーポートの設定

AXIS Camera Station S1232 Tower Recording Serverサーバーでは、ポート55752 (HTTP)、55754 (HTTP)、55756 (モバイル通信)、および55757 (モバイルストリーミング) がサーバーとクライアントの間の通信に使用されます。必要な場合、これらのポートはAXIS Camera Station Service Controlで変更できます。

セキュリティに関する考慮事項

カメラおよび録画への不正アクセスを防ぐには:

- すべてのネットワーク装置 (カメラ、ビデオエンコーダ、補助装置) で強力なパスワードを使用します。
- AXIS Camera Station S1232 Tower Recording Serverサーバー、カメラ、ビデオエンコーダ、補助デバイスをオフィスネットワークから分離された安全なネットワークにインストールします。AXIS Camera Station S1232 Tower Recording Serverクライアントは、インターネットアクセスのあるネットワークなど別のネットワーク上のコンピューターにインストールすることができます。
- すべてのユーザーが強力なパスワードを使用していることを確認してください。

システムをオンラインでライセンスする

自動ライセンスを使用するには、システムを登録し、組織に接続する必要があります。

1. [Configuration (設定)] > [Licenses (ライセンス)] > [Management (管理)] に移動します。
2. [Automatic licensing (自動ライセンス)] がオンになっていることを確認します。
3. [Register... (登録...)] をクリックします。
4. My Axisアカウントを使用してサインインし、画面の指示に従います。
5. [Go to AXIS License Manager (AXIS License Managerに移動)] をクリックして、ライセンスを管理します。詳細については、help.axis.comのMy Systemsユーザーマニュアルをお読みください。

オフラインのシステムをライセンスする

システムを手動でライセンスするには:

1. [Configuration (設定)] > [Licenses (ライセンス)] > [Management (管理)] に移動します。
2. [Automatic licensing (自動ライセンス)] をオフにします。
3. [Export system file... (システムファイルのエクスポート...)] をクリックし、コンピューターにファイルを保存します。

注

AXIS License Managerにアクセスするには、インターネット接続が必要です。クライアントコンピューターにインターネット接続がない場合は、インターネット接続のあるコンピューターにシステムファイルをコピーします。

4. *AXIS License Manager*を開きます。
5. *AXIS License Manager*で:
 - 5.1. 正しい組織を選択するか、まだ作成していない場合は作成します。詳細については、help.axis.comの*My Systems*ユーザーマニュアルをお読みください。
 - 5.2. **[System setup (システム設定)]**に移動します。
 - 5.3. **[Upload system file (システムファイルをアップロード)]** をクリックします。
 - 5.4. **[Upload system file (システムファイルをアップロード)]** をクリックし、システムファイルを選択します。
 - 5.5. **[Upload system file (システムファイルをアップロード)]** をクリックします。
 - 5.6. **[Download license file (ライセンスファイルのダウンロード)]** をクリックします。
6. *AXIS Camera Station S1232 Tower Recording Server*クライアントに戻ります。
7. **[Import license file... (ライセンスファイルのインポート...)]** をクリックし、ライセンスファイルを選択します。
8. **[Go to AXIS License Manager (AXIS License Managerに移動)]** をクリックして、ライセンスを管理します。

ローカル Windows® ユーザーアカウントの管理

ユーザーアカウントの作成

個人データと情報のセキュリティを強化するために、ローカルアカウントごとにパスワードを追加することをお勧めします。

重要

ローカルアカウントのパスワードを作成したら、そのパスワードを忘れないでください。ローカルアカウントのパスワードを紛失したパスワードを回復する方法はありません。

1. [Settings (設定)] > [Accounts (アカウント)] > [Other users (その他のユーザー)] > [Add other user (その他のユーザーを追加)] の順に移動し、[Add account (アカウントを追加)] をクリックします。
2. [I don't have this person's sign-in information (このユーザーのサインイン情報を持っていない)] をクリックします。
3. [Add a user without a Microsoft account (Microsoftアカウントを持たないユーザーを追加する)] をクリックします。
4. ユーザー名、パスワード、およびパスワードのヒントを入力します。
5. [Next (次へ)] をクリックし、指示に従います。

管理者アカウントを作成する

1. [Settings (設定)] > [Accounts (アカウント)] > [Other people (その他のユーザー)] に移動します。
2. 変更するアカウントに移動し、[Change account type (アカウントの種類の変更)] をクリックします。
3. [Account type (アカウントの種類)] に移動し、[Administrator (管理者)] を選択します。
4. [OK] をクリックします。
5. デバイスを再起動し、新しい管理者アカウントでログインします。

ローカルユーザーグループを作成する

1. [Computer Management (コンピューター管理)] に移動します。
2. [Local Users and Groups (ローカルユーザーとグループ)] > [Group (グループ)] の順に移動します。
3. [Group (グループ)] を右クリックし、[New Group (新しいグループ)] を選択します。
4. グループ名と説明を入力します。
5. グループメンバーの追加:
 - 5.1. [追加] をクリックします。
 - 5.2. [詳細設定] をクリックします。
 - 5.3. グループに追加するユーザー アカウントを見つけて、[OK] をクリックします。
 - 5.4. もう一度 [OK] をクリックします。
6. [Create (作成)] をクリックします。

ユーザーアカウントを削除します。

重要

アカウントを削除すると、ログイン画面からユーザーアカウントが削除されます。また、ユーザーアカウントに保存されているすべてのファイル、設定、およびプログラムデータも削除します。

1. [Settings (設定)] > [Accounts (アカウント)] > [Other people (その他のユーザー)] に移動します。
2. 削除するアカウントに移動し、[Remove (削除)] をクリックします。

ユーザーアカウントのパスワードを変更する

1. 管理者アカウントでログインします。
2. [User Accounts (ユーザーアカウント)] > [User Accounts (ユーザーアカウント)] > [Manage another account in sequence (別のアカウントを順番に管理する)] の順に移動します。
デバイス上のすべてのユーザーアカウントの一覧が表示されます。
3. パスワードを変更するユーザーアカウントを選択します。
4. [Change the password (パスワードの変更)] をクリックします。
5. 新しいパスワードを入力し、[Change password (パスワードの変更)] をクリックします。

ユーザーアカウントのパスワードリセットディスクを作成する

USBフラッシュドライブにパスワードリセットディスクを作成することをお勧めします。このディスクを使用して、パスワードをリセットできます。パスワードリセットディスクがないと、パスワードをリセットできません。

注

Windows® 10以降を使用している場合は、パスワードを忘れたときのために、ローカルアカウントにセキュリティの質問を追加できるため、パスワードリセットディスクを作成する必要はありません。これを行うには、[Start (スタート)] ボタンをクリックし、[Settings (設定)] > [Sign-in options (サインインオプション)] > [Update your security questions (セキュリティに関する質問の更新)] の順にクリックします。

1. ローカルユーザーアカウントを使用してデバイスにログインします。接続されているアカウントのパスワードリセットディスクを作成することはできません。
2. 空のUSBフラッシュドライブを装置に接続します。
3. [Windows® 検索フィールドから、[Create a password reset disk (パスワード リセット ディスクの作成)] に進みます。
4. パスワードディスクの作成ウィザードで、[Next (次へ)] をクリックします。
5. USBフラッシュドライブを選択し、[Next (次へ)] をクリックします。
6. 現在のパスワードを入力し、[Next (次へ)] をクリックします。
7. 画面の指示に従います。
8. USBフラッシュドライブを取り外し、安全な場所に保管してください。パスワードを何度変更しても、新しいディスクを作成する必要はありません。

AXIS Camera Station Proのユーザーアカウントの管理

ユーザー権限

[Configuration (設定)] > [Security (セキュリティ)] > [User permissions (ユーザー権限)] に移動して、AXIS Camera Station S1232 Tower Recording Serverのユーザーとグループを確認します。

注

AXIS Camera Station S1232 Tower Recording Serverサーバーを実行しているコンピューターの管理者には、自動的に AXIS Camera Station S1232 Tower Recording Serverの管理者権限が付与されます。管理者グループの権限を変更したり、削除したりすることはできません。

ユーザーまたはグループを追加する前に、それらがローカルコンピューターに登録されているか、Windows® Active Directory のユーザーアカウントを持っていることを確認してください。ユーザーまたはグループを追加するには、「ユーザーまたはグループの追加」を参照してください。

ユーザーがグループに所属している場合、そのユーザーには、個人またはグループに割り当てられる最も高いフォールの権限が付与されます。たとえば、カメラXへのアクセス権を持つユーザーが、カメラYおよびZへのアクセス権を持つグループにも所属している場合、そのユーザーは3つすべてのカメラへのアクセス権を持ちます。

	エントリが1人のユーザーであることを示します。
	エントリがグループであることを示します。
名称	ローカルコンピューターまたはActive Directoryに表示されるユーザー名。
ドメイン	ユーザーまたはグループが属するドメイン。
役割	ユーザーまたはグループに割り当てられるアクセスロール。表示される値:管理者、オペレーター、閲覧者。
詳細	ローカルコンピューターまたはActive Directoryに表示されるユーザーの詳細情報。
サーバー	ユーザーまたはグループが属するサーバー。

ユーザーまたはグループの追加

Microsoft Windows® と Active Directoryのユーザーとグループは AXIS Camera Station S1232 Tower Recording Serverにアクセスできます。ユーザーを AXIS Camera Station S1232 Tower Recording Serverに追加するには、ユーザーまたはグループをWindows® に追加する必要があります。

Windows® 10および11でユーザーを追加するには：

- Windowsキー + X を押し、[Computer Management (コンピューターの管理)] を選択します。
- [Computer Management (コンピューターの管理)] ウィンドウで、[Local Users and Groups (ローカルユーザーとグループ)] > [Users (ユーザー)]の順に移動します。
- [Users (ユーザー)] を右クリックし、[New user (新規ユーザー)] を選択します。
- ポップアップダイアログで、新規ユーザーの詳細を入力し、[User must change password at next login (ユーザーが次回ログイン時にパスワードを変更する必要があります)] をクリアします。
- [Create (作成)] をクリックします。

Active Directoryドメインをご使用の場合は、ネットワーク管理者にお問い合わせください。

ユーザーまたはグループの追加

1. [Configuration > Security > User permissions (設定 > セキュリティ > ユーザー権限)] に移動します。
2. [追加] をクリックします。利用可能なユーザーとグループがリストに表示されます。
3. [Scope (対象)] で、ユーザーとグループを検索する場所を選択します。
4. [Show (表示)] で、ユーザーまたはグループを表示するかどうかを選択します。ユーザーまたはグループが多すぎる場合、検索結果が表示されないことがあります。フィルターを使用して検索結果を絞り込みます。
5. ユーザーまたはグループを選択し、[追加] をクリックします。

対象	
サーバー	ローカルコンピューター上のユーザーまたはグループを検索する場合に選択します。
ドメイン	Active Directoryのユーザーまたはグループを検索する場合に選択します。
選択したサーバー	複数の AXIS Camera Station S1232 Tower Recording Serverサーバーに接続している場合は、サーバーを選択してそのサーバー上のユーザーまたはグループを検索します。

ユーザーまたはグループの設定

1. リストからユーザーまたはグループを選択します。
2. [Role (権限)] で、[Administrator (管理者)]、[Operator (オペレーター)]、または [Viewer (閲覧者)] を選択します。
3. [Operator (オペレーター)] または [Viewer (閲覧者)] を選択した場合は、ユーザーまたはグループの権限を設定することができます。ユーザーまたはグループの権限を参照してください。
4. Save (保存) をクリックします。

ユーザーまたはグループの削除

1. ユーザーまたはグループを選択します。
2. [削除] をクリックします。
3. ポップアップダイアログで [OK] をクリックするとユーザーまたはグループが削除されます。

ユーザーまたはグループの権限

ユーザーまたはグループに割り当てられるロールは3種類です。ユーザーまたはグループの権限の定義方法については、ユーザーまたはグループの追加を参照してください。

管理者 - すべてのカメラのビューのライブおよび録画ビデオへのアクセス、すべてのI/Oポートへのアクセスなど、システム全体へのフルアクセス。このロールは、システム設定にアクセスすることが求められます。

オペレーター - カメラ、ビュー、I/Oポートを選択して、ライブおよび録画ビデオにアクセスします。オペレーターは AXIS Camera Station S1232 Tower Recording Serverのすべての機能 (システムの設定を除く) へのフルアクセスが許可されます。

ビューワー - 選択したカメラ、I/Oポート、ビューのライブビデオにアクセスします。録画ビデオへのアクセスやシステムの設定を行うことはできません。

カメラ

[Operator (オペレーター)] または [Viewer (閲覧者)] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。

アクセス	カメラおよびすべてのカメラ機能へのアクセスを許可します。
ビデオ	このカメラからのライブ映像へのアクセスを許可します。
音声を聞く	カメラから受話するアクセスを許可します。
音声送話	カメラに送話するアクセスを許可します。
Manual Recording (手動録画)	手動で録画を開始・停止することができます。
Mechanical PTZ (メカニカルPTZ)	メカニカルPTZコントロールへのアクセスを許可します。メカニカルPTZを搭載したカメラでのみ使用できます。
PTZ優先度	PTZ優先度を設定します。数値が小さいほど、優先度が高いことを意味します。優先度を割り当てない場合は [0] に設定されます。優先度が最も高いのは管理者です。優先度の高い権限を持つユーザーがPTZカメラを操作する場合、デフォルトでは、他のユーザーは同じカメラを10秒間操作することができません。メカニカルPTZを搭載したカメラで、[Mechanical PTZ (メカニカルPTZ)] が選択されている場合のみ使用できます。

ビュー

[Operator (オペレーター)] または [Viewer (閲覧者)] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。複数のビューを選択し、アクセス権を設定することができます。

アクセス	AXIS Camera Station S1232 Tower Recording Serverのビューへのアクセスを許可します。
編集	AXIS Camera Station S1232 Tower Recording Serverで表示を編集することができます。

I/O

[Operator (オペレーター)] または [Viewer (閲覧者)] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。

アクセス	I/Oポートへのフルアクセス権を許可します。
読む	I/Oポートの状態を変更せずに確認することができます。
Write (書き込み)	I/Oポートの状態を変更することができます。

システム

リスト内でグレー表示されているアクセス権限は設定できません。チェックマークは、そのユーザーまたはグループがこの権限を持っていることを意味します。

[Operator (オペレーター)] 権限を持つユーザーまたはグループは次のアクセス権を利用できます。[Take snapshots (スナップショットを撮る)] は [Viewer (閲覧者)] 権限でも利用できます。

スナップショットを撮る	ライブビューおよび録画モードでスナップショットを撮影することができます。
録画のエクスポート	録画のエクスポートを許可します。
事故レポートの生成	事故レポートの生成を許可します。
Prevent access to recordings older than (これより古い録画へのアクセスを防止)	指定した分数よりも古い録画へのアクセスを防止します。ユーザーはこれらの録画を検索しても見つけることができません。
アラーム、タスク、ログへのアクセス	アラーム通知を受け取り、[Alarms and tasks (アラームとタスク)] バーと [Logs (ログ)] タブへのアクセスを許可します。
Access data search (データ検索へのアクセス)	イベント発生時の状況を追跡するためのデータ検索を許可します。
イベントにカテゴリーを追加する	録画 タブでイベントにカテゴリーを追加できるようにします。
イベントからカテゴリーを削除する	録画タブでイベントからカテゴリーを削除できるようにします。

アクセスコントロール

[Operator (オペレーター)] 権限を持つユーザーまたはグループは次のアクセス権を利用できます。[Access Management (アクセス管理)] は [Viewer (閲覧者)] 権限でも利用できます。

アクセスコントロールの設定	ドアとゾーン、識別プロファイル、カードフォーマットとPIN、暗号化通信、マルチサーバーを設定することができます。
アクセス管理	アクセス管理ができます。また、Active Directory設定にアクセスすることができます。

Viewer (閲覧者) のロールを持つユーザーまたはグループは、次のアクセス権を利用できます。

システムのヘルスマニタリング

[Operator (オペレーター)] 権限を持つユーザーまたはグループは次のアクセス権を利用できます。[>システムの健全性監視へのアクセス] は [Viewer (閲覧者)] 権限でも利用できます。

システムの健全性監視の設定	システムの健全性監視を設定することができます。
システムの健全性監視へのアクセス	システムの健全性監視にアクセスすることができます。

デバイスを管理する

セキュアブートの証明書を更新する

Microsoftは2011年に発行されたセキュアブート証明書の提供を2026年6月に終了し、新しい2023年の証明書に切り替えます。レコーダーを安全に保つため、有効期限までに2023年の証明書をインストールしてください。

2023年の証明書のインストールには、Windows 10 LTSC (Long-Term Servicing Channel) または Windows 11 LTSCが必要です。使用しているデバイスが保証期間内であるにもかかわらず、LTSCバージョンではなくWindows 10 SAC (Semi-Annual Channel) が動作している場合は、Axis Technical Supportにお問い合わせください。BIOSの更新や証明書の変更を行う前に、LTSCバージョンにアップグレード可能かどうかをお知らせします。

注

2026年6月以降、2023年の証明書を持たないデバイスは、引き続き通常通り動作しますが、Windows Boot Managerの更新や新たな脆弱性に対する失効リストなど、初期ブートプロセスに対する新しいセキュリティ保護は提供されません。

証明書のステータスを確認する

以下の方法で、2023年の証明書がインストールされており、Windowsのブートローダーが更新されていることを確認します。

方法1:

1. [Registry Editor (レジストリエディタ)] を開きます。
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicingに移動します。
3. UEFICA2023Statusの値を確認します。値が「Updated (更新済み)」となっている場合、2023年の証明書がインストールされています。

ab (Default)	REG_SZ	(value not set)
ab BucketHash	REG_SZ	5a3041a8e6c7476f988f369de06e65e224df7d53cf7f9...
ab ConfidenceLevel	REG_SZ	No Data Observed - Action Required
oi ConfidenceUpdateType	REG_DWORD	0x00000000 (0)
oi LastParsedBucketDataVersion	REG_DWORD	0x0000000c (12)
ab UEFICA2023Status	REG_SZ	Updated
oi WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

方法2:

1. [Windows Security (Windowsセキュリティ)] を選択します。
2. [Device security (デバイスセキュリティ)] に移動します。
3. [Secure boot (セキュアブート)] で、ステータスメッセージを確認します。証明書が最新の場合、カードに“Secure Boot is on and all required certificate updates have been applied. No further certificate changes are needed”(セキュアブートがオンになっており、必要なすべての証明書の更新が適用されました。これ以上の証明書の変更は必要ありません) と表示されます。

Secure boot

Secure Boot is on and all required certificate updates have been applied.
No further certificate changes are needed.

注

Windowsセキュリティは、デバイスに2026年4月14日付けの累積更新プログラム以降がインストールされている場合のみ、証明書のステータスを表示します。証明書の状態に関するメッセージが表示されない場合は、最新のWindows更新プログラムをインストールするか、代わりに方法1をお試しください。

推奨されるアクション

BIOSの更新により、2023年の証明書がファームウェアに永続的に保存されます。これが最も信頼性の高い方法であるため、Windows Updateを通じてすでに証明書をインストール済みの場合もこの方法をお勧めします。

重要

Windows Updateを通じて証明書をインストールしただけでは、その後、BIOSのセキュアブートキーを工場出荷時の設定にリセットすると、証明書が失われ、セキュアブートがオンになっている状態ではデバイスが起動しなくなります。セキュアブートキーをリセットする前に、BIOSを更新して証明書を永続化してください。

BIOSを通じて証明書を更新する

AXIS S12およびS93シリーズについては、Axis.comではなく、DellからBIOSアップデートを入手してください。BIOSを更新する, on page 20を参照してください。

詳細情報

- *Dell: Microsoft 2011 Secure Boot Certificate Expiration (Microsoft 2011セキュアブート証明書の終了)*
- *Dell: PowerEdge Server BIOS Update Guidelines for Secure Boot (セキュアブートのPowerEdge Server BIOSアップデートガイドライン)*

Windows Updateを通じて証明書を更新する

使用しているモデルでBIOSアップデートがまだ提供されていない場合は、代わりにWindows Updateを通じて2023年の証明書を入手することができます。

重要

この方法でインストールされた証明書は、ファームウェアではなく、現在のセキュアブートデータベースに保存されます。BIOSのセキュアブートキーを工場出荷時の設定にリセットすると、証明書が失われ、セキュアブートがオンになっている状態ではデバイスが起動できなくなる可能性があります。この方法をすでに使用している場合も、モデルのBIOSアップデートが利用可能になり次第、インストールしてください。

以下のパスに従って使用します。

1. 使用しているデバイスがWindows 10 LTSCまたはWindows 11 LTSCを実行していることを確認します。
2. 2026年4月14日以降にリリースされたすべてのWindows更新プログラムをインストールします。
3. **[Windows Security (Windowsセキュリティ)] > [Device security (デバイスセキュリティ)] > [Secure Boot (セキュアブート)]** に移動して、証明書のステータスを確認します。
4. 最新のアップデートをインストールしても証明書が更新されない場合は、レジストリ値 **UEFICA2023Status**を確認します。使用しているデバイスで自動アップデートができない場合は、BIOSを更新するか、Axis Technical Supportにお問い合わせください。

重要

使用環境のすべてのリカバリメディア、ブート環境、およびドライバーが2023年の証明書によって署名されていることを確認するまでは、2011年の証明書を手動で取り消さないでください。その前に2011年の証明書を取り消すと、セキュアブートがオンになっている状態でデバイスを起動できなくなります。

現在のBIOSのバージョンを確認する

現在のBIOSを確認するには:

1. デバイスの電源を入れ、Axisロゴが表示されるまでF2キーを繰り返し押します。
2. [Overview (オーバービュー)] の最初の項目として、バージョン番号が表示されます。

BIOSを更新する

1. Dellサポートに移動します。
2. [サービスタグ] のフィールドにデバイスのシリアル番号の下7桁を入力します。たとえば、HW030ABC1234などです。
3. [ドライバーおよびダウンロード] に移動し、「BIOS」で検索します。
4. 使用しているOEM製品名 (例: OEMR XL R760xs) に対応する新しいバージョンが表示されない場合は、シリアル番号の代わりにDellの汎用プラットフォーム名 (例: R760xs) を使用して再検索します。
5. 2026年4月以降にリリースされた最新のBIOSバージョンをダウンロードしてインストールします。

Windows®を更新します

Windows®は定期的に更新プログラムをチェックします。更新プログラムが利用可能になると、デバイスは自動的に更新プログラムをダウンロードしますが、インストールは手動で行う必要があります。

注

スケジュールされたシステムの再起動中に録画が中断されます。

更新プログラムを手動で確認するには、次の手順を実行します。

1. [Settings (設定)] > [Windows Update (Windows更新プログラム)] に移動します。
2. [Check for updates (クリックして更新)] をクリックします。

Windows®の更新プログラムの設定を構成する

必要に応じて、Windows®の更新プログラムを実行する方法とタイミングを変更できます。

注

スケジュールされたシステムの再起動中に、進行中のすべての録画が停止します。

1. 実行アプリを開きます。
 - [Windows System (Windowsシステム)] > [Run (実行)] に移動するか、
2. 「gpedit.msc」と入力して、[OK] をクリックします。Local Group Policy Editor (ローカルグループポリシーエディター) が開きます。
3. [Computer Configuration (コンピューターの構成)] > [Administrative Templates (管理用テンプレート)] > [Windows Components (Windowsコンポーネント)] > [Windows Update (Windows更新プログラム)] の順に移動します。
4. 必要に応じて設定を構成します (例を参照)。

例:

ユーザーの操作なしで更新プログラムを自動的にダウンロードしてインストールし、必要に応じて営業時間外に装置を再起動するには、次の設定を使用します。

1. [Always automatically restart at the scheduled time (常にスケジュールされた時刻に自動的に再起動する)] を開き、次のいずれかを選択します。
 - 1.1. オン

- 1.2. 再起動タイマーにより、ユーザーには作業を保存する15分間の時間的猶予があります。
- 1.3. [OK] をクリックします。
2. [Configure Automatic Updates (自動更新の構成)] を開き、次の項目を選択します。
 - 2.1. オン
 - 2.2. Configure Automatic updates (自動更新を構成する):自動ダウンロードとインストールのスケジュール設定
 - 2.3. Schedule Install day (インストール日のスケジュール):毎週日曜日
 - 2.4. Schedule Install time (インストール時刻のスケジュール): 00:00
 - 2.5. [OK] をクリックします。
3. [Allow Automatic Updates immediate installation (自動更新を直ちにインストールする)] を開き、次を選択します。
 - 3.1. オン
 - 3.2. [OK] をクリックします。

ハードドライブの追加

ストレージの要件が合わないことがあります。保存データの保持期間の延長や高解像度録画の保存は、いずれも追加のストレージ導入が必要になることが多くあります。このセクションでは、さらに多くのハードドライブでAXIS S12シリーズを拡張する方法と、それらをRAID 5構成に追加する方法について説明します。

注

特定のAXIS S12シリーズにストレージを追加する際は、以下の手順に従います。これらの手順は無保証の状態を提供され、Axis Communications ABは手順に従っている間のデータの損失や構成の間違いについて一切の責任を負いません。標準的な対策を講じて、ビジネス上重要なデータをバックアップしてください。次のストレージ拡張手順は、Axisの技術サポートでは対応していません。

注

静電放電を避けるために、システム内部のコンポーネントを操作するときは、常に静電マットと静電ストラップを使用することをお勧めします。

保証

保証の詳細については、www.axis.com/support/warrantyを参照してください。

ワークフロー

1. ホットスワップハードドライブを取り付ける, on page 22
 - 1.1. ベゼルを取り外す, on page 22
 - 1.2. ハードディスクブランクを取り外す, on page 22
 - 1.3. ハードドライブを取り付ける, on page 22
2. 新しいRAIDアレイの作成, on page 23
 - 2.1. Dell PERC 11設定ユーティリティの起動, on page 23
 - 2.2. RAIDストレージアレイの作成, on page 23
 - 2.3. RAIDストレージアレイの再設定, on page 24
- 3.

ホットスワップハードドライブを取り付ける

ベゼルを取り外す

1. ベゼルキーを見つけます。
2. キーを使用してベゼルのロックを解除します。
3. リリースラッチを上スライドさせ、ベゼルの左端を引き出します。
4. 右端のフックを外し、ベゼルを取り外します。

ハードディスクブランクを取り外す

- ハードディスクブランクのリリースボタンを押し、ブランクをハードドライブスロットからスライドさせます。

ハードドライブを取り付ける

▲ 注意

- AXIS S12シリーズでの使用がテストおよび承認されたハードドライブのみを使用してください。
 - ハードドライブを取り付けるときは、隣接するドライブが完全に取り付けられていることを確認します。ハードドライブキャリアを挿入し、部分的に取り付けたキャリアの横にハンドルをロックしようとする、部分的に取り付けたキャリアのシールドスプリングが損傷し、使用できなくなることがあります。
 - 同じRAIDボリューム内でSASとSATAのハードドライブを組み合わせることはサポートされていません。
1. ハードドライブスロットにハードドライブブランクが取り付けられている場合は、それを取り外します。
 2. ハードドライブをハードドライブキャリアに取り付けます。
 3. ハードドライブキャリアの前面にあるリリースボタンを押し、ハードドライブキャリアのハンドルを開きます。
 4. ハードドライブキャリアがバックプレーンと接続されるまで、キャリアをハードドライブスロットに挿入します。
 5. ハードドライブキャリアのハンドルを閉じて、ハードドライブを所定の位置にロックします。

RAIDの変更

▲ 注意

RAIDを変更すると、ディスクからすべてのデータが削除されます。

1. Lifecycle Controllerを起動します:
 - 1.1. デバイスの電源を入れます。
 - 1.2. AXISスプラッシュ画面が表示されたら、F10キーを押します。
2. Lifecycle Controllerで、[Hardware Configuration > Configuration Wizards (ハードウェア設定 > 設定ウィザード)] に移動し、[RAID Configuration (RAID設定)] を選択します。
3. RAIDを作成する [RAID Controller (RAIDコントローラー)] を選択します。選択したコントローラーで使用可能な仮想ディスクの詳細が、コントローラーリストの下ページに表示される表に示されます。サーバーに使用可能な外部HDDまたは初期化されていないHDDがある場合、[Foreign Configuration (外部構成)] が表示されます。

注

- [Clear foreign configuration (外部構成をクリア)] を選択すると、選択したRAIDコントローラーで使用可能なすべての外部HDDがクリアされます。
- [Ignore foreign Configuration (外部構成を無視)] を選択すると、RAIDの作成時にRAIDコントローラーで使用可能な外部HDDが無視されます。
- 4. 外部HDDと初期化されていないHDDをクリアまたは無視します。
必要な場合は、初期化されていないディスクを初期化できます:
 - 4.1. すべてのRAID構成ではない (初期化されていない) HDDのリストで、RAID構成可能に変換する (初期化する) HDDを選択し、[Next (次へ)] をクリックして初期化します。
 - 4.2. 設定ウィザード: RAID設定ページで対応するオプションを選択します。
- 5. RAIDレベルを選択します。
- 6. 表から物理ディスクを選択し、[Next (次へ)] をクリックします。
[Ignore foreign configuration (外部構成を無視)] を選択している場合、外部HDDは表に表示されません。
- 7. 仮想ディスクの属性を入力します。
- 8. [Next (次へ)] をクリックします。
- 9. 設定を確認し、[完了] をクリックします。
- 10. Lifecycle Controllerにより、コントローラーで使用可能な仮想ディスクに関する現在のすべてのデータが失われることを示すメッセージが表示されます。[OK] をクリックして続行します。
- 11. [OK] をクリックし、[Finish (完了)] をクリックします。
- 12. ウィザードを終了し、システムを再起動します。

新しいRAIDアレイの作成

Human Interface Infrastructure (HII) 構成ユーティリティは、システムBIOSに統合されたストレージ管理アプリケーションです。コントローラー、仮想ディスク、および物理ディスクの設定と管理に使用されます。このユーティリティは、オペレーティングシステムから独立しています。

Dell PERC 11設定ユーティリティの起動

1. システムの電源を入れます。
2. システムの起動中に、F2キーを押してシステムセットアップに入ります。
3. [Device Settings (デバイスの設定)] をクリックして、システム内にあるすべてのRAIDコントローラーを表示します。

RAIDストレージアレイの作成

1. *Dell PERC 11設定ユーティリティの起動, on page 23.*
2. [Main Menu > Configuration Management > Create Virtual Disk (メインメニュー > 構成管理 > 仮想ディスクの作成)] をクリックし、以下の仮想ディスクパラメーターを定義します。
 - **Select RAID Level (RAIDレベルの選択):** RAIDレベルを選択します。
 - **Select Physical Disks (物理ディスクの選択):** 仮想ディスクの作成元の物理ディスクを選択します。このオプションは、物理ディスク容量として [Unconfigured Capacity (未設定容量)] を選択した場合に表示されます。
 - **Configure Virtual Disk (仮想ディスクの設定):** 以下の仮想ディスクパラメーターを設定します。
 - **Virtual Disk Name (仮想ディスク名):** 仮想ディスクの名前を入力します。使用できる文字は、A～Z、a～z、0～9、アンダースコア (_)、およびハイフン (-) のみです。

- Virtual Disk Size (仮想ディスクのサイズ):仮想ディスクの容量を設定します。

3. [Create Virtual Disk (仮想ディスクの作成)] をクリックします。

▲ 注意

変更できるパラメーターは他にもあります。ただし、Axis Communications ABは、これらのパラメーターの変更時に起こる可能性がある設定の間違いについて一切の責任を負いません。パラメーターを変更する際は、常に注意してください。

RAIDストレージアレイの再設定

オンラインの仮想ディスクは、その容量を拡張してRAIDレベルを変更する方法で再設定できます。

▲ 注意

- RAID 50や60などのスパン仮想ディスクは再設定できません。
 - 通常、仮想ディスクを再設定すると、再設定操作が完了するまでディスクのパフォーマンスに影響を与えます。完了時間は最大数日までで、大きなばらつきがあります。メンテナンス期間中に操作を行うことを強くお勧めします。
 - 操作を開始する前に、常にデータの検証済みバックアップを作成してください。
1. Dell PERC 11設定ユーティリティの起動, on page 23.
 2. [Main Menu > Virtual Disk Management (メインメニュー > 仮想ディスクの管理)] をクリックします。RAIDコントローラーに関連付けられたすべての仮想ディスクが表示されます。
 3. プロパティを表示するには、仮想ディスクをクリックします。
 4. [Operations (操作)] ドロップダウンリストで、[Reconfigure Virtual Disks (仮想ディスクの再設定)] を選択し、[GO] を押します。
 5. [RAID Level (RAIDレベル)] を選択し、[Choose the Operation (操作を選択する)] を押します。
 6. 仮想ディスクに追加するディスクを選択し、[Apply Changes (変更を適用する)] を押します。
 7. 操作を確認し、[YES (はい)] をクリックします。
 8. [Start Operation (操作を開始する)] をクリックします。
 9. [OK] をクリックします。

[Virtual Disk Management (仮想ディスクの管理)] ページに、変更した仮想ディスクの再構成の状態が表示されます。

システムの再構成が開始された後、処理が完了するまで、システムをDell PERC 11設定ユーティリティに残すことも、システムをオペレーティングシステムに再起動することもできます。

システムをオペレーティングシステムに再起動すると、再構築が完了するまで、システムのパフォーマンスに影響があります。

また、再構築が完了するまで、Windows®でディスクを拡張することはできません。

▲ 注意

再構築時間はシステムによって異なり、最大数日かかることがあります。

Microsoft Windows®の設定

新しいボリュームを設定するには:

1. [Start (スタート)] メニューを右クリックし、[Disk Management] (ディスクの管理) を選択します。

2. ハードディスク上の割り当てられていない領域を右クリックし、[New Simple Volume (新しいシンプルボリューム)] を選択します。
3. [New Simple Volume Wizard (新しいシンプルボリュームウィザード)] で [Next (次へ)] をクリックします。
4. 作成するボリュームのサイズをメガバイト (MB) 単位で入力するか、デフォルトの最大サイズのままで、[Next (次へ)] をクリックします。
5. パーティションを識別するドライブ文字をデフォルトのままにするか、別のドライブ文字を選択し、[Next (次へ)] をクリックします。
6. [Format Partition (パーティションのフォーマット)] ダイアログで、次の操作を行います。
 - すぐにボリュームをフォーマットしない場合は、[Do not format this volume (このボリュームをフォーマットしない)] を選択し、[Next (次へ)] をクリックします。
 - デフォルト設定でボリュームをフォーマットするには、[Next (次へ)] をクリックします。
7. 選択した項目を確認し、[Finish (完了)] をクリックします。
[Disk Management (ディスクの管理)] に新しいボリュームが表示されます。[Disk Management (ディスクの管理)] を閉じると、システムは新しいボリュームを使用する準備ができています。

既存のボリュームを設定するには:

1. [Start (スタート)] メニューを右クリックし、[Disk Management] (ディスクの管理) を選択します。
2. ボリュームを右クリックし、[Extend Volume (ボリュームの拡張)] を選択します。
3. [Extend Volume Wizard (ボリュームの拡張ウィザード)] で、[Next (次へ)] をクリックします。
4. 未使用の領域があるディスクを選択し、[Next (次へ)] をクリックします。通常、デフォルトでこのディスクが選択されています。
5. 選択した項目を確認し、[Finish (完了)] をクリックします。
[Disk Management (ディスクの管理)] に拡張されたボリュームが表示されます。[Disk Management (ディスクの管理)] を閉じると、システムは新しいボリュームを使用する準備ができています。

iDRACの設定

Integrated Dell Remote Access Controller 9 (iDRAC9) with Lifecycle Controllerは、システム管理者の生産性を高め、Dellシステムの全体的な可用性を向上させる目的で設計されています。iDRACは、システムの問題を管理者に警告し、リモート システム管理の実行を支援し、システムへの物理的なアクセスの必要性を軽減します。iDRACと相互に通信できるように、ネットワークインフラストラクチャーを基にして初期ネットワークを設定する必要があります。

1. パワーオンセルフテスト (POST) 実行時に、F10キーを押します。

注

Lifecycle Controllerの初期設定ウィザードが初回のみ表示されます。初期設定ウィザードを使用して、言語とキーボードの選択、ネットワーク設定の構成、iDRAC ネットワーク設定、認証情報設定、および設定の概要の表示を行います。後で設定を変更するには、Lifecycle Controller ホームページから [Settings (設定)] を選択します。

2. 言語とキーボードを設定し、[Next (次へ)] をクリックします。
3. 製品の概要を確認し、[Next (次へ)] をクリックします。
4. Lifecycle Controllerのネットワーク設定の設定:
 - 4.1. [NIC Card (NICカード)] ドロップダウンリストから、設定するNICポートを選択します。

- 4.2. [IPv4 Network Settings > IP Address Source (IPv4ネットワーク設定 > IPアドレスソース)] ドロップダウンリストから、以下のいずれかのオプションを選択します。
 - DHCPは、DHCPサーバーからのIPアドレスを使用してNICを設定する必要があることを示します。DHCPはデフォルトのオプションで、DHCP IPアドレスはNetwork Settings (ネットワーク設定) ページに表示されます。
 - Static IPは、静的なIPを使用してNICを設定する必要があることを示します。IPアドレスサブネットマスク、デフォルトゲートウェイ、DNSアドレスなどのIPアドレスプロパティを入力します。この情報がない場合は、ネットワーク管理者にお問い合わせください。
 - No Configuration:は、NICを設定する必要がないことを示しています。
- 4.1. VLANを使用する場合は、[Enabled (有効にする)] をクリックし、[Lifecycle Controller VLAN Settings (Lifecycle Controller VLAN設定)] で [VLAN ID] と [Priority (優先度)] を入力して、NICのVLAN設定を行います。
- 4.2. [Next (次へ)] をクリックします。Lifecycle Controllerの設定が正しく設定されていない場合、エラーメッセージが表示されます。
5. iDRACネットワークと認証情報の設定:
 - 5.1. [IPv4 Configuration > IP Address Source (IPv4設定 > IPアドレスソース)] に移動し、以下のいずれかのオプションを選択します。
 - Staticは、静的なIPを使用してネットワークを設定する必要があることを示します。IPアドレスサブネットマスク、デフォルトゲートウェイ、DNSアドレスソース、DNSアドレスなどのIPアドレスプロパティを入力します。この情報がない場合は、ネットワーク管理者にお問い合わせください。
 - DHCPは、DHCPサーバーからのIPアドレスを使用してNICを設定する必要があることを示します。DHCPはデフォルトのオプションで、DHCP IPアドレスはNetwork Settings (ネットワーク設定) ページに表示されます。
 - 5.1. [Credentials (認証情報)] で、iDRACネットワークにアクセスするための [Account Username Username (アカウントのユーザー名)] と [Password (パスワード)] を入力します。
 - 5.2. [Next (次へ)] をクリックします。
6. Lifecycle Controller とiDRACネットワーク設定の概要を確認し、[Finish (完了)] をクリックします。

サイバーセキュリティ

サイバーセキュリティに関する製品固有の情報については、axis.comの製品データシートを参照してください。

AXIS OSのサイバーセキュリティの詳細情報については、『AXIS OS強化ガイド』を参照してください。

セキュアブート

セキュアブートは、システム上でマルウェアや安全でないソフトウェアが実行されるのを防ぐ機能です。この機能はシステム起動時に実行され、デジタル署名を使用してソフトウェアおよびOSの証明書を検証します。信頼されたソフトウェアとOSのみがシステム上で実行されます。

Trusted Platform Module (TPM)

TPMは、不正アクセスから情報を保護するための暗号化機能を提供するコンポーネントです。デフォルトで有効になっており、オフにすることはお勧めしません。

Axis装置のサイバーセキュリティ機能の詳細については、axis.com/learning/white-papersにアクセスし、サイバーセキュリティを検索してください。

Axisセキュリティ通知サービス

Axisは、Axis装置に関する脆弱性やその他のセキュリティ関連事項についての情報を提供する通知サービスを運営しています。通知を受け取るには、axis.com/security-notification-serviceで購読手続きを行うことができます。

脆弱性の管理

お客様の脆弱性リスクを最小限に抑えるため、Axisは**CVE (共通脆弱性識別子) 採番機関**として業界標準に従って、装置、ソフトウェア、およびサービスで発見された脆弱性の管理と対応を行っています。Axisの脆弱性管理ポリシー、脆弱性の報告方法、すでに公開されている脆弱性、対応するセキュリティ勧告の詳細については、axis.com/vulnerability-managementをご覧ください。

Axis装置のセキュアな動作

工場出荷時の設定のAxis装置は、セキュアなデフォルトの保護メカニズムで事前に設定されています。装置の設置時には、より多くのセキュリティ設定を使用することをお勧めします。装置のセキュリティを確保するためのベストプラクティス、リソース、ガイドラインなど、Axisのサイバーセキュリティに対する取り組みの詳細については、axis.com/about-axis/cybersecurityをご覧ください。

トラブルシューティング

診断を実行する

診断を実行すると、システムの問題の原因を特定するのに役立ちます。診断には追加の機器は不要で、データ損失のリスクなしにシステムハードウェアがテストされます。

1. システム起動中に、F10キーを押して、Lifecycle Controllerを開きます。
2. [Hardware Diagnostics (ハードウェア診断)] に移動し、[Run Hardware Diagnostics (ハードウェア診断の実行)] をクリックします。
3. エラーコードをメモして、Axisの技術サポートにお問い合わせください。

システムリカバリの実行

内部リカバリ

装置にシステム障害が発生した場合は、内部リカバリを実行してシステムをリストアします。

1. Windowsの [Settings (設定)] を開きます。
2. [System (システム)] を選択します。
3. メニューから [Recovery (回復)] を選択します。
4. [Recovery options (リカバリオプション)] で [Reset this PC (このPCをリセット)] を選択します。
5. [Keep my files (ファイルを保持する)] または [Remove everything (すべて削除)] を選択します。
 - [Keep my files (ファイルを保持する)] を選択すると、すべての個人ファイル、ユーザーデータ、Axisがインストールしたソフトウェアがすべて保持されます。
 - すべて削除すると、個人ファイルやユーザーデータはすべて消去されますが、Axisがインストールしたソフトウェア (工場出荷時の設定) はすべて残ります。
6. 画面の指示に従います。

注

[Reset (リセット)] を選択する前に、この処理によって削除されるアプリのリストを確認できます。リカバリ後、Axisのアプリはリストアされますが、その他のユーザーがインストールしたその他のアプリはリストアされません。

重要

正常にリカバリされた後、Windowsに管理者アカウントでログインしてリカバリプロセスを完了する必要があります。

外部リカバリ

デバイスで完全なシステム障害が発生した場合は、回復イメージを使用してWindows® システムを再作成する必要があります。AXIS Network Video Recovery Kitをダウンロードするには、AXISテクニカルサポートに連絡し、お使いのデバイスのシリアル番号を知らせてください。

注

AXIS Network Video Recorder Recovery Kitには、以下の2つのバージョンがあります。

- **sb11** — 2011年の証明書を使用しているデバイス向けです。
- **sb23** — 2023年の証明書に移行したデバイス向けです。

Recovery Kitをダウンロードする前に、証明書のステータスを確認し、それに応じたバージョンを選択してください。間違ったバージョンを選択すると、インストール後に起動できる結果が生成されず、正しい画像で最初からやり直す必要があります。これによってデバイスが損傷することはありません。

デバイスにすでに2023年の証明書がインストールされている場合、2011年の証明書を手動で失効していない限り、sb11バージョンは引き続き安全に使用できます。失効すると、sb23のみが機能します。

1. AXIS Network Video Recovery Kitと任意のISO to USB書き込みツールをダウンロードします。
2. USBドライブをコンピューターに挿入します。
 - 16 GBのUSBドライブを使用します。
 - USBドライブがフォーマットされ、既存のデータはすべて消去されます。
3. ISO to USB書き込みツールを実行し、画面の指示に従います。
 - USBドライブへのデータ書き込みには、おおよそ10～15分ほどかかります。プロセスが完了するまで、USBドライブを取り外さないでください。
4. ISOからUSBへのツールが完成したら、USBドライブをコンピューターから取り外してデバイスに接続します。
5. デバイスを起動します。Axisのスプラッシュ画面が表示されたら、**F12**を押して、ブートメニューを開きます。
6. USBドライブを選択し、**Enter**キーを押します。システムがAXIS Network Video Recorder Recovery Kitで起動します。
7. **[Start (開始)]** をクリックし、画面の指示に従います。
 - リカバリが完了するまでに約10～15分かかります。

SupportAssistコレクションのエクスポート

SupportAssistコレクションをUSBドライブまたはネットワーク共有 (CIFS/NFS) にエクスポートすることができます。コレクションには、以下のデータが含まれています。

- ハードウェア
- RAIDコントローラーのログ

SupportAssistコレクションをエクスポートするには:

1. パワーオンセルフテスト (POST) 実行時に、F10キーを押して、Lifecycle Controllerを起動します。
2. **[Hardware Diagnostics > Export SupportAssist collection (ハードウェア診断 > SupportAssistコレクションのエクスポート)]** に進みます。
3. 使用条件を読み、**[Next (次へ)]** をクリックします。
技術サポートがSupportAssistコレクションデータを使用できるようにするには、使用条件に同意する必要があります。
4. SupportAssistコレクションに含めるデータオプションを選択し、**[Next (次へ)]** をクリックします。
5. 必要なエクスポート設定情報を入力し、**[Next] (次へ)]** をクリックします。
 - USBドライブにエクスポートするには：USBドライブオプションを選択し、USBドライブの名前を選択して、コレクションのエクスポート先のファイルパスの詳細を入力します。
 - NFSにエクスポートするには：NFSオプションを選択して、必要な情報を入力します。
 - CIFSにエクスポートするには：CIFSオプションを選択して、必要な情報を入力します。
[Test Network Connection (ネットワーク接続のテスト)] をクリックして、Lifecycle Controllerが指定されたIPアドレスに接続できるかどうかを確認します。デフォルトでは、ゲートウェイIP、DNSサーバーIP、ホストIP、およびプロキシIPに対してpingが実行されます。
6. 選択内容を確認し、**[Finish (完了)]** をクリックします。

Lifecycle Controllerが、選択されたコレクションデータを取得し、レポートファイルを指定された場所にエクスポートします。これには数分かかることがあります。

電源ユニットのトラブルシューティング

注

電源ユニットを取り付けた後、システムが電源ユニットを認識し、電源ユニットが正しく機能するかどうかを判定するまで数秒待ちます。

1. 接続不良がないことを確認します。たとえば、電源ケーブルの接続不良です。
2. 電源のハンドルLEDが、電源が正常に作動していることを示していることを確認します。
3. 電源ユニットの電源 LEDの状態を確認します。仕様, on page 32を参照してください。
4. 冗長電源構成の場合は、両方の電源ユニットの種類とワット数が同じであることを確認してください。
5. 背面にExtended Power Performance (EPP) ラベルが付けられた電源ユニットのみを使用していることを確認します。
6. 電源ユニットをリセットします。
7. 問題が解決しない場合は、Axisの技術サポートにお問い合わせください。

メモリーエラーのトラブルシューティング

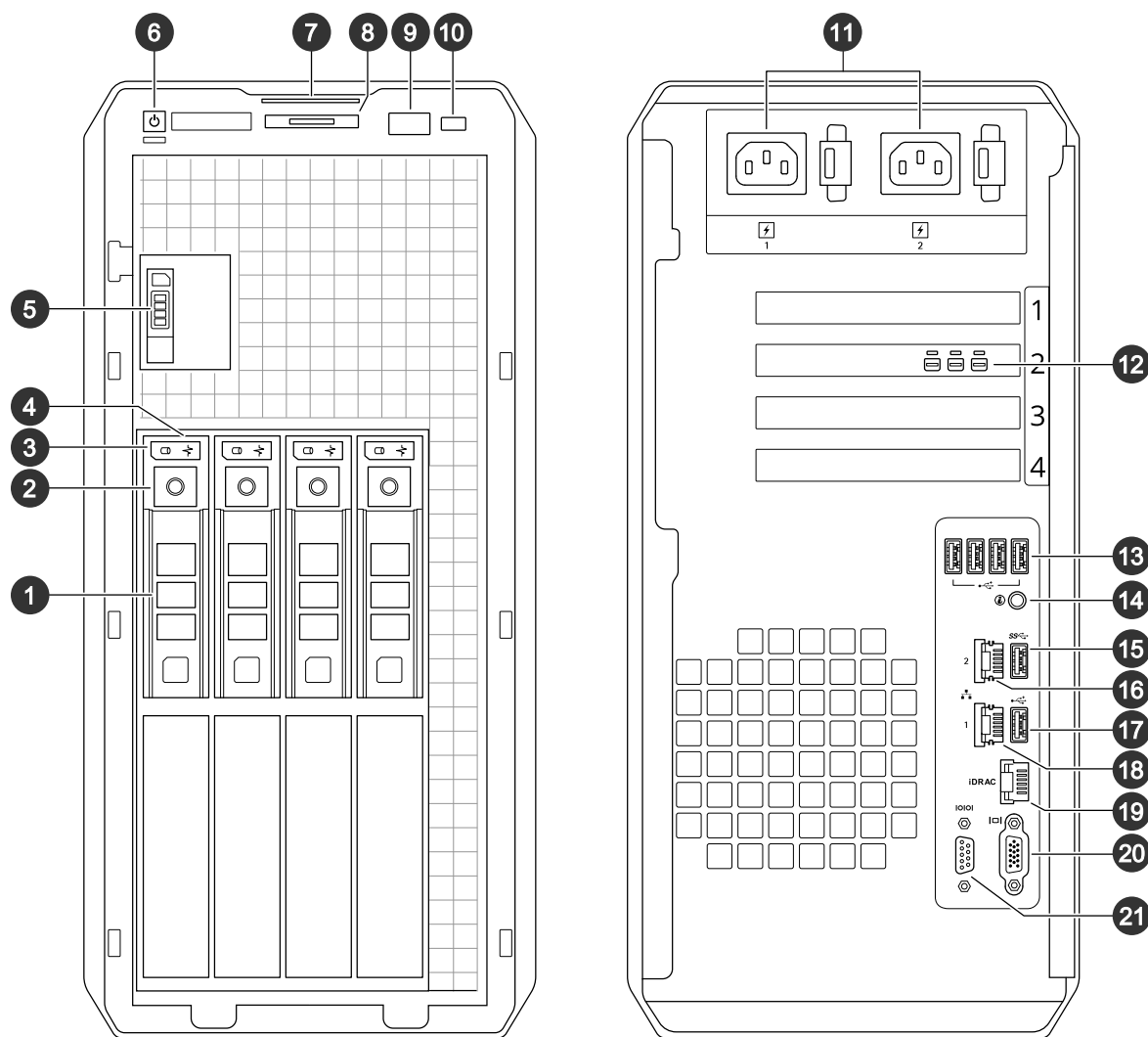
1. BIOSを最新バージョンにアップグレードします。
2. エラーが解決しない場合は、Axisの技術サポートにお問い合わせください。

AXIS Camera Station Proのトラブルシューティング

AXIS Camera Station Proのトラブルシューティング方法については、*AXIS Camera Station Pro*ユーザーマニュアルを参照してください。

製品概要

前面と背面



- 1 ハードドライブトレイ
- 2 ハードドライブトレイリリースボタン
- 3 ハードドライブアクティビティLED
- 4 ハードドライブステータスLED
- 5 ソリッドステートドライブトレイ
- 6 電源ボタン/電源LED
- 7 情報タグ
- 8 システム識別ボタンとインジケータ
- 9 USB 3.0ポート
- 10 iDRACダイレクトポート
- 11 電源ユニット
- 12 Mini DisplayPortコネクタ
- 13 USB 2.0ポート
- 14 システム識別ボタンとインジケータ
- 15 USB 3.0ポート
- 16 1 GbEイーサネットポート2
- 17 USB 2.0ポート
- 18 1 GbEイーサネットポート1
- 19 iDRAC専用イーサネットポート
- 20 VGAポート (使用しないでください)
- 21倍 シリアルポート

仕様

システムの健全性とシステムIDのインジケータ

LED	説明	動作
青色で点灯	システムの電源が入っており、健全であり、システムIDモードはアクティブではありません。	[system health and system ID (システムの健全性とシステムID)] ボタンを押して、システムIDモードに切り替えます。
青色で点滅	システムIDモードがアクティブです。	[system health and system ID (システムの健全性とシステムID)] ボタンを押して、システムの健全性モードに切り替えます。
黄色で点灯	システムはフェイルセーフモードです。	
黄色で点滅	システムに障害が発生しています。	具体的なエラーメッセージについては、システムイベントログをチェックしてください。

iDRACダイレクトLEDインジケータ

LED	説明
緑色で2秒間点灯	ノートPCまたはタブレットが接続されています。
緑で点滅 (2秒間点灯、2秒間消灯)	接続されているノートPCまたはタブレットが認識されました。
オフ	ノートPCまたはタブレットのプラグが抜けています。

NICインジケータ

LED	説明
リンクインジケータとアクティビティインジケータが消灯	NICはネットワークに接続されていません。
リンクインジケータが緑色で、アクティビティインジケータが緑色で点滅	NICは最大ポート速度で有効なネットワークに接続され、データが送受信されています。
リンクインジケータが黄色で、アクティビティインジケータが緑色で点滅	NICは最大ポート速度より低い速度で有効なネットワークに接続され、データが送受信されています。
リンクインジケータが緑色で、アクティビティインジケータが消灯	NICは最大ポート速度で有効なネットワークに接続され、データは送受信されていません。
リンクインジケータが黄色で、アクティビティインジケータが消灯	NICは最大ポート速度より低い速度で有効なネットワークに接続され、データは送受信されていません。

電源ユニット (PSU) のインジケータ

LED	説明
緑	有効な電源がPSUに接続され、PSUが動作可能です。
黄色で点滅	PSUに問題があります。
電源がオンになっていない	電源がPSUに接続されていません。
緑色で点滅	PSUのファームウェアが更新中です。 ▲ 注意 ファームウェア更新中は、電源コードを抜いたりPSUの電源を切断したりしないでください。更新が中断されると、PSUは動作しなくなります。
緑色で点滅してから消灯	PSUをホットプラグ接続すると、4 Hzの速度で5回緑色に点滅してから消灯します。これは、効率、機能セット、健全性ステータス、またはサポートされている電圧によるPSUの不一致を示しています。 ▲ 注意 2つのPSUが設置されている場合は、両方のPSUのラベルの種類が同じでなければなりません。たとえば、Extended Power Performance (EPP) ラベルです。前世代のPowerEdgeサーバーのPSUを混在させることはサポートされていません。PSUの電力定格が同じ場合でも同様です。混在させると、PSUの不一致状態が発生したり、システムの電源が入らなくなったりします。 2つのPSUを使用する場合は、それらの種類が同じで、最大出力電力が同じでなければなりません。 - PSUの不一致を修正する際は、インジケーターが点滅しているPSUのみを交換してください。一致するペアを作るためにPSUを交換すると、エラー状態になり、予期しないシステムシャットダウンが発生することがあります。高出力設定から低出力設定に変更する場合、またはその逆の場合は、システムの電源をオフにする必要があります。

ドライブインジケーター

LED	説明
緑色で1秒間に2回点滅	ドライブを識別中または取り外しの準備中です。
オフ	ドライブは取り外し可能な状態です。 注 システムの電源投入後、すべてのドライブの初期化が完了するまでドライブのステータスインジケーターは点灯しません。この間はドライブを取り外さないでください。

緑色、黄色で点滅してから消灯	予期しないドライブ故障が発生しています。
黄色で1秒間に4回点滅	ドライブが故障しました。
緑色でゆっくりと点滅	ドライブは再構築中です。
緑で点灯	ドライブはオンラインです。
緑色で3秒間点滅し、黄色で3秒間点滅してから6秒後に消灯	再構築が停止しました。

さらに支援が必要ですか？

参考リンク

- [AXIS Camera Station Proユーザーマニュアル](#)
- [AXISセキュアリモートアクセスにサインイン](#)
- [Axis Secure Remote Access v2にサインインする](#)
- [AXIS Camera Stationのウイルス対策許可リストに含める内容](#)

サポートに問い合わせる

さらにサポートが必要な場合は、axis.com/supportにアクセスしてください。

T10177843_ja

2026-07 (M6.2)

© 2022 – 2026 Axis Communications AB