AXIS A1001 & AXIS Entry Manager

ユーザーマニュアル

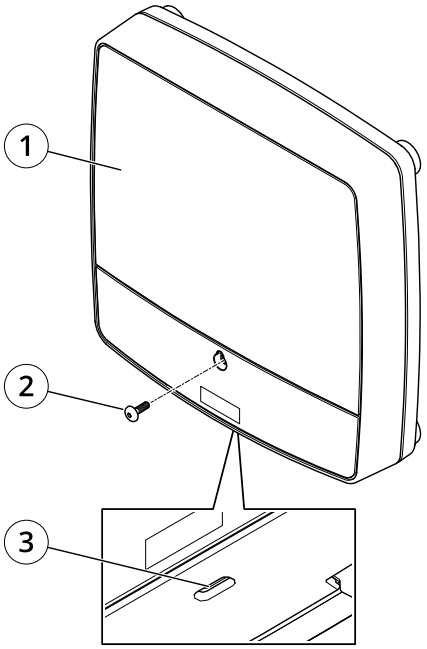
AXIS A1001 & AXIS Entry Manager

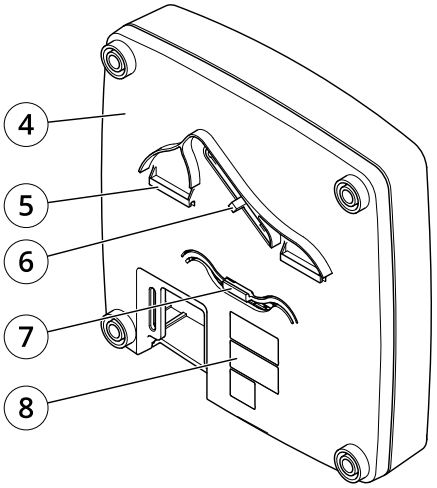
目次

目次

製品の概要

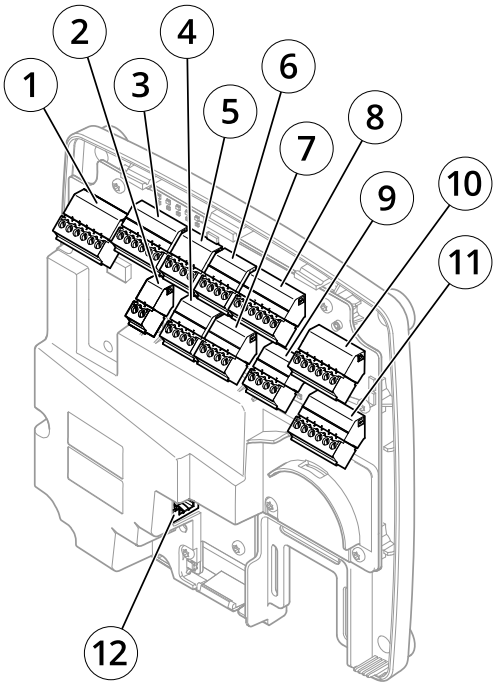
製品の概要





前面および背面:
1 カバー
2 カバーのネジ
3 カバー取り外しスロット
4 ベース
5 DINクリップ – 上
6 いたずら警告スイッチ – 背面
7 DINクリップ – 下
8 型番 (P/N) とシリアル番号 (S/N)

製品の概要

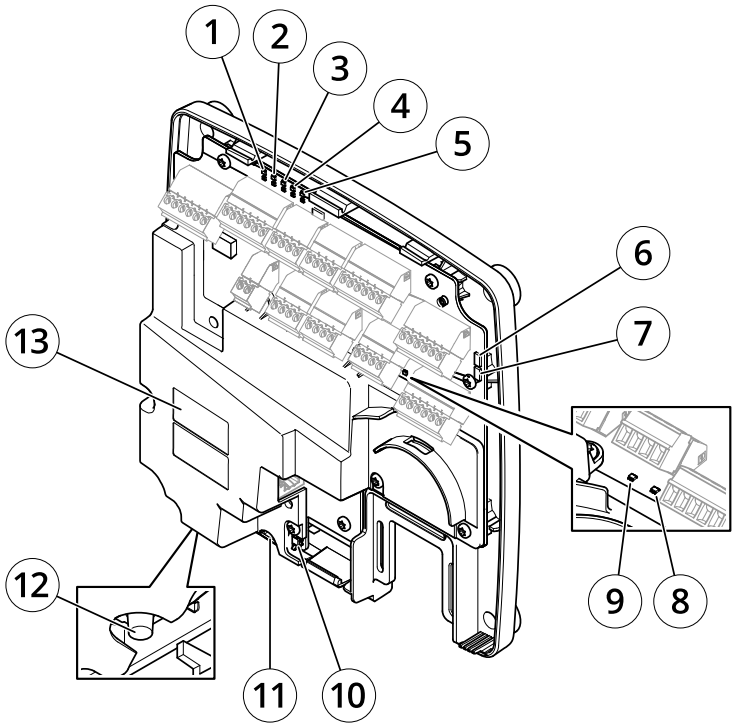


I/Oインターフェース:
1　リーダーデータコネクタ (READER DATA 1)
10　リーダーデータコネクタ (READER DATA 2)
3　リーダーI/Oコネクタ (READER I/O 1)
8　リーダーI/Oコネクタ (READER I/O 2)
4　ドアコネクタ (DOOR IN 1)
7　ドアコネクタ (DOOR IN 2)
6　補助コネクタ (AUX)
5　音声コネクタ (AUDIO) (未使用)

外部電源入力:
2　電源コネクタ (DC IN)
12　ネットワークコネクタ (PoE)

電源出力:
9　電源ロックコネクタ (LOCK)
11　電源およびリレーコネクタ (PWR、RELAY)

製品の概要



LEDインジケーター、ボタン、およびその他のハードウェア:

1 電源LEDインジケーター
2 ステータスLEDインジケーター
3 ネットワークLEDインジケーター
4 リーダー2のLEDインジケーター (未使用)
5 リーダー1のLEDインジケーター (未使用)
6 いたずら警告ピンヘッダー – 前面 (TF)
7 いたずら警告ピンヘッダー – 背面 (TB)
8 ロックLEDインジケーター
9 ロックLEDインジケーター
10 いたずら警告センサー – 前面
11 SDカードスロット (microSDHC) (未使用)
12 コントロールボタン
13 型番 (P/N) とシリアル番号 (S/N)

LEDインジケーター

LED	カラー	説明
ネットワーク	緑	100 Mbit/sネットワークに接続している場合、点灯します。ネットワークパケットを送受信した場合、点滅します。
	黄	10 Mbit/sネットワークに接続している場合、点灯します。ネットワークパケットを送受信した場合、点滅します。
	無点灯	ネットワーク接続なし。
状態	緑	正常動作であれば緑色に点灯します。
	黄	起動時、設定の復元時に点灯します。
	赤	アップグレードに失敗した場合に、ゆっくりと点滅。

電源	緑	正常動作。
	黄	ファームウェアのアップグレード中、緑/黄に交互に点滅します。
ロック	緑	非通電時に点灯します。
	赤	通電時に点灯します。
	無点灯	フロート状態。

注

- ステータスLEDは、イベントの発生時に点滅させることができます。
- ステータスLEDを点滅させ、本製品を識別できるように設定することができます。[Setup > Additional Controller Configuration > System Options > Maintenance (設定 > 追加のコントローラー設定 > システムオプション > メンテナンス)] に移動します。

コネクタとボタン

I/Oインターフェース

リーダーデータコネクタ
リーダーとの通信用のRS485およびWiegandプロトコルに対応する6ピンターミナルブロック (×2)。仕様については、*72ページ*を参照してください。

リーダーI/Oコネクタ
リーダーの入出力用の6ピンターミナルブロック (×2)。リーダーI/Oコネクタは、0 V DC基準点と電力 (DC出力) に加えて、以下へのインターフェースを提供します。

- デジタル入力 – リーダーのいたずら警告などを接続します。
- デジタル出力 – リーダービーパーやリーダーLEDなどを接続します。

仕様については、*72ページ*を参照してください。

ドアコネクタ
ドア監視デバイスと退出要求 (REX) 装置を接続するための4ピンターミナルブロック (×2)。仕様については、*73ページ*を参照してください。

補助コネクタ
設定可能な4ピンI/Oターミナルブロック。外部デバイスを接続し、いたずらの警告、イベントトリガー、アラーム通知などを使用することができます。補助コネクタは、0 V DC基準点と電力 (DC出力) に加えて、以下へのインターフェースを提供します。

- デジタル入力 – オープンサーキットとクローズサーキットの切り替えが可能なデバイス (PIRセンサーやガラス破損検知器など) を接続するためのアラーム入力。
- デジタル出力 – 盗難アラーム、サイレン、ライトなどの外部デバイスを接続します。接続されたデバイスは、VAPIX® アプリケーションプログラミングインターフェースまたはアクションルールによって有効にすることができます。

仕様については、*74ページ*を参照してください。

外部電源入力

注意

本製品は、シールドネットワークケーブル (STP) を使用して接続してください。本製品は、用途に合ったケーブルを使用してネットワークに接続してください。ネットワーク装置がメーカーの指示どおりに設置されていることを確認します。法的要件については、を参照してください。

製品の概要

電源コネクタ
DC電源入力用の2ピンターミナルブロック。定格出力が100 W以下または5 A以下の安全特別低電圧 (SELV) に準拠した有限電源 (LPS) を使用してください。仕様については、*75ページ*を参照してください。

ネットワークコネクタ
RJ45イーサネットコネクタ。Power over Ethernet (PoE) に対応しています。仕様については、*75ページ*を参照してください。

電源出力

電源ロックコネクタ

1つまたは2つのロックの接続用4ピンターミナルブロック。ロックコネクタは、外部デバイスへの電源供給にも使用できます。仕様については、*75ページ*を参照してください。

電源およびリレーコネクタ

電源とドアコントローラーのリレーを外部デバイス (ロックやセンサーなど) に接続するための6ピンターミナルブロック。仕様については、*76ページ*を参照してください。

ボタンとその他のハードウェア

いたずら警告のピンヘッダー
前面および背面のいたずら警告を接続解除するための2つの2ピンヘッダー。仕様については、*76ページ*を参照してください。

コントロールボタン
以下の用途があります。

- 製品を工場出荷時の設定にリセットする。*67ページ*を参照してください。
- AXIS Video Hosting Systemサービスに接続する。*60ページ*を参照してください。接続するには、ステータスLEDが緑色に点滅するまで、ボタンを押し続けます (約1秒間)。
- AXIS Internet Dynamic DNSサービスに接続する。*60ページ*を参照してください。接続するには、ボタンを押し続けます (約3秒間)。

設置

設置

製品のインストールビデオ。

製品のアクセス方法

製品のアクセス方法

本製品のインストールについては、製品に添付されている『インストールガイド』を参照してください。

装置へのアクセス

1. ブラウザーを開き、Axis装置のIPアドレスまたはホスト名を入力します。

   本製品のIPアドレスが不明な場合は、AXIS IP UtilityまたはAXIS Device Managerを使用して、ネットワーク上で装置を見つけます。

2. ユーザー名とパスワードを入力します。初めて装置にアクセスする場合は、rootパスワードを設定する必要があります。を参照してください。

3. ブラウザーでAXIS Entry Managerが開きます。コンピューターを使用している場合は、[Overview (概要)] ページが表示されます。モバイル 装置を使用している場合は、モバイルランディングページが表示されます。

モバイルランディングページについて

モバイルランディングページに、ドアコントローラーに接続されたドアとロックの状態が表示されます。ロックおよびロック解除をテストできます。ページを更新して結果を表示します。

リンクをクリックしてAxis Entry Managerに戻れます。

注

- Axis Entry Managerは、モバイルデバイスをサポートしていません。
- Axis Entry Managerの使用を続ける場合、モバイルランディングページに戻るリンクはありません。

インターネットから本製品にアクセスする方法

プライベートネットワーク (LAN) 上の製品は、ネットワークルーターを使用することにより、インターネットへの接続を共有できます。これは、プライベートネットワークからインターネットにネットワークトラフィックを転送することによって行われます。

ほとんどのルーターは、パブリックネットワーク (インターネット) からプライベートネットワーク (LAN) へのアクセスを阻止するようあらかじめ設定されています。

イントラネット (LAN) 上にあるAxis製品を、NAT (ネットワークアドレス変換) ルーターの外側 (WAN側) から利用できるようにする場合は、**NATトラバーサル**をオンにします。NATトラバーサルを正しく設定すると、NATルーターの外部HTTPポートに着信するすべてのHTTPトラフィックが本製品に転送されます。

NATトラバーサル機能をオンにする方法

- [**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)**] の順に選択します。
- [**Enable (有効にする)**] をクリックします。
- NATルーターを手動で設定して、インターネットからのアクセスを許可します。

AXIS Internet Dynamic DNS Service (*www.axiscam.net*) も参照してください。

製品のアクセス方法

注

- この場合、ルーターとは、NATルーター、ネットワークルーター、インターネットゲートウェイ、ブロードバンドルーター、ブロードバンド共有デバイスなどのネットワークルーティングデバイス、またはファイアウォールなどのソフトウェアを指します。
- NATトラバーサルを機能させるには、ルーターがNATトラバーサルに対応している必要があります。また、UPnP®にも対応している必要があります。

rootパスワードの設定方法

本製品にアクセスするには、デフォルトの管理者ユーザー「**root**」のパスワードを設定する必要があります。このパスワードは、[**Configure Root Password (rootパスワードの設定)**] ダイアログで設定できます。このダイアログは、製品への初回アクセス時に表示されます。

ネットワークの傍受を防ぐには、暗号化されたHTTPS接続でrootパスワードを設定できますが、これにはHTTPS証明書が必要です。HTTPS (Hypertext Transfer Protocol over SSL) は、Webブラウザーとサーバー間のトラフィックを暗号化するために使用されるプロトコルです。HTTPS証明書は、暗号化された情報交換を保証します。*56ページHTTPS*を参照してください。

デフォルトの管理者ユーザー名は、常に「**root**」であり、削除できません。rootのパスワードを忘れた場合は、製品を工場出荷時の設定にリセットする必要があります。*67ページ工場出荷時の設定にリセットする*を参照してください。

パスワードを設定するには、ダイアログでパスワードを直接入力します。

[Overview (概要)] ページ

AXIS Entry Managerの [Overview (概要)] ページには、ドアコントローラーの名前、MACアドレス、IPアドレス、およびファームウェアのバージョン情報が表示されます。また、このページでネットワーク上またはシステム内のドアコントローラーを識別することもできます。

本製品に最初にアクセスすると、[Overview (概要)] ページでは、ハードウェアの設定、日付と時刻の設定、ネットワーク設定、ドアコントローラーをシステムの一部として、またはスタンドアロンユニットとして設定することが求められます。システムの設定の詳細については、*12ページ設定 – 段階的な手順*を参照してください。

本製品の他のWebページから [Overview (概要)] ページに戻るには、メニューバーの [**Overview (概要)**] をクリックします。

システムの設定

システムの設定

本製品の設定ページを開くには、概要ページの右上隅の [**Setup (設定)**] をクリックします。

本製品は、管理者が設定できます。ユーザーや管理者の詳細については、*32*ページ、*41*ページ、および*56*ページを参照してください。

設定 – 段階的な手順

アクセスコントロールシステムの使用を開始する前に、以下の設定手順を完了する必要があります。

1. 英語が母国語でない場合でも、異なる言語でAXIS Entry Managerを利用することができます。*12*ページ*言語の選択*を参照してください。
2. 日付と時刻を設定します。*12*ページを参照してください。
3. ネットワークを設定します。*14*ページを参照してください。
4. ドアコントローラーとリーダー、ロック、退出要求 (REX) 装置などの接続されたデバイスを設定します。*14*ページ*ハードウェアの設定*を参照してください。
5. ハードウェアの接続を確認します。*21*ページを参照してください。
6. カードおよびフォーマットを設定します。*22*ページを参照してください。
7. ドアコントローラーシステムを設定します。*27*ページ*ネットワークドアコントローラーの管理*を参照してください。

システムのドア、スケジュール、ユーザーおよびグループの設定方法と管理方法の詳細については、*32*ページ、*アクセス管理*を参照してください。

推奨メンテナンスの詳細については、*31*ページ*メンテナンス手順*を参照してください。

注

ドアコントローラーの追加および削除、ユーザーの追加、削除、編集、ハードウェアの設定を行うには、システム内の半数以上のドアコントローラーが**オンライン**になっている必要があります。ドアコントローラーのステータスを確認するには、[**Setup > Manage Network Door Controllers in System (設定 > システムのネットワークドアコントローラーを管理)**] に移動します。

言語の選択

AXIS Entry Managerのデフォルトの言語は英語ですが、本製品のファームウェアに含まれるどの言語にも切り替えることができます。利用可能な最新のファームウェアの詳細については、*www.axis.com*を参照してください。

いずれかの製品のWebページ上で言語を切り替えることができます。

言語を切り替えるには、言語のドロップダウンリスト をクリックして言語を選択します。製品のすべてのWebページおよびヘルプページが選択した言語で表示されます。

注

- 言語を切り替えると、日付形式も選択した言語で一般に使用される形式に変更されます。データのフィールドに正しい形式が表示されます。
- 本製品を工場出荷時の設定にリセットすると、AXIS Entry Managerの表示は再び英語になります。
- 本製品を復元すると、AXIS Entry Managerは引き続き、選択した言語を使用します。
- 本製品を再起動すると、AXIS Entry Managerは引き続き、選択した言語を使用します。
- ファームウェアをアップグレードすると、AXIS Entry Managerは引き続き、選択した言語を使用します。

システムの設定

日付と時刻の設定

ドアコントローラーがシステムの一部の場合は、すべてのドアコントローラーに日付と時刻の設定が配布されます。これは、システム内の他のコントローラーに設定が適用されることを意味し、NTPサーバーとの同期、日付と時刻の手動設定、または、コンピューターからの日付と時刻を取得の有無にかかわらず適用されます。変更内容が表示されない場合は、お使いのブラウザーでページを更新してください。ドアコントローラーのシステム管理の詳細については、*27ページネットワークドアコントローラーの管理*を参照してください。

本製品の日付と時刻を設定するには、[**Setup > Date & Time (設定 > 日付と時刻)**] に移動します。

日付と時刻は以下のいずれかの方法で設定できます。

- Network Time Protocol (NTP) サーバーから日付と時刻を取得します。*13ページ*を参照してください。
- 手動で日付と時刻を設定します。*13ページ*を参照してください。
- コンピューターから日付と時刻を取得します。*14ページ*を参照してください。

[**Current controller time (コントローラーの現在時刻)**] ドアコントローラーの現在の日付と時刻 (24時間形式) が表示されます。

[System Options (システムオプション)] ページでも同じ日付と時刻のオプションを利用できます。[] [**Setup > Additional Controller Configuration > System Options > Date & Time (設定 > 追加のコントローラー設定 > システムオプション > 日付と時刻)**] に移動します。

Network Time Protocol (NTP) サーバーから日付と時刻を取得する

1. [**Setup > Date & Time (設定 > 日付と時刻)**] に移動します。
2. ドロップダウンリストから [**Timezone (タイムゾーン)**] を選択します。
3. 夏時間を使用する地域では、[**Adjust for daylight saving (夏時間の調整を行う)**] を選択します。
4. [**Synchronize with NTP (NTPと同期する)**] を選択します。
5. デフォルトのDHCPアドレスを選択するか、NTPサーバーのアドレスを入力します。
6. [**Save (保存)**] をクリックします。

NTPサーバーと同期すると、NTPサーバーからデータが送信されるため、日付と時刻が継続的に更新されます。NTP設定に関する詳細については、*61ページNTP設定*を参照してください。

NTPサーバーとしてホスト名を使用する場合は、DNSサーバーの設定を行う必要があります。*61ページDNS設定*を参照してください。

日付と時刻を手動で設定する

1. [**Setup > Date & Time (設定 > 日付と時刻)**] に移動します。
2. 夏時間を使用する地域では、[**Adjust for daylight saving (夏時間の調整を行う)**] を選択します。
3. [**Set date & time manually (日付と時刻を手動で合わせる)**] を選択します。
4. 希望する日付と時刻を入力します。
5. [**Save (保存)**] をクリックします。

日付と時刻の手動による設定では、日付と時刻が1回設定されますが、自動的には更新されません。これは、外部NTPサーバーとの接続が確立されていないために、日付または時刻を更新する必要がある場合は、変更を手動で行う必要があることを意味します。

システムの設定

コンピューターから日付と時刻を取得する

1. [Setup > Date & Time (設定 > 日付と時刻)] に移動します。
2. 夏時間を使用する地域では、[Adjust for daylight saving (夏時間の調整を行う)] を選択します。
3. [Set date & time manually (日付と時刻を手動で合わせる)] を選択します。
4. [Sync now and save (今すぐ同期して保存)] をクリックします。

コンピューターの時刻を使用する場合、日付と時刻は、コンピューターの時刻と1回同期されますが、その後自動的には更新されません。これは、システムの管理に使用するコンピューターで日付や時刻を変更した場合は、再び同期する必要があることを意味します。

ネットワークの設定

ネットワークの基本設定を行うには、[Setup > Network Settings (設定 > ネットワーク設定)] または [Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 基本設定)] に移動します。

ネットワーク設定の詳細については、*59ページネットワーク*を参照してください。

ハードウェアの設定

ドアや床を管理する前に、[Hardware Configuration (ハードウェア設定)] ページでハードウェアを設定する必要があります。

ハードウェア設定を完了する前に、リーダーやロックなどのデバイスを本製品に接続することはできます。しかし、ハードウェア設定を完了してからの方がデバイスの接続が簡単になります。設定が完了すると、ハードウェアピン配置図が利用可能になるからです。ハードウェアピン配置図は、デバイスをピンに接続する方法のガイドで、メンテナンスの参照表として使用できます。メンテナンスの手順については、*31ページ*を参照してください。

ハードウェアを初めて設定する場合は、以下のいずれかの方法を選択してください。

- ハードウェア設定ファイルをインポートします。*14ページ*を参照してください。
- 新しいハードウェア設定を作成します。*15ページ*を参照してください。

注

製品のハードウェアがまだ設定されていない場合や、設定が削除されている場合は、概要ページの通知パネルで [Hardware Configuration (ハードウェア設定)] が利用可能になります。

ハードウェア設定ファイルをインポートする方法

ハードウェア設定ファイルをインポートすることで、Axis製品のハードウェア設定を素早く完了できます。

ある製品からファイルをエクスポートし、それを別の製品にインポートすることで、何度も同じ手順を繰り返さなくても同じハードウェア設定の複数のコピーを作成できます。エクスポートしたファイルをバックアップとして保存し、それらを使用して以前のハードウェア設定を復元することもできます。詳細については、*15ページハードウェア設定ファイルをエクスポートする方法*を参照してください。

ハードウェア設定ファイルをインポートするには:

1. [Setup > Hardware Configuration (設定 > ハードウェア設定)] に移動します。
2. [Import hardware configuration (ハードウェア設定のインポート)] をクリックします。ハードウェア設定が既に存在する場合は、[Reset and import hardware configuration (ハードウェア設定のリセットとインポート)] をクリックします。
3. 表示されるファイルブラウザーダイアログで、コンピューター上のハードウェア設定ファイル (*.json) を見つけて選択します。

4. [OK] をクリックします。

ハードウェア設定ファイルをエクスポートする方法

Axis製品のハードウェア設定をエクスポートすることで、同じハードウェア設定の複数のコピーを作成することができます。エクスポートしたファイルをバックアップとして保存し、それらを使用して以前のハードウェア設定を復元することもできます。

注

フロアのハードウェア設定は、エクスポートできません。

ワイヤレスロックの設定は、ハードウェアの構成のエクスポートには含まれません。

ハードウェア設定ファイルをエクスポートするには:

1. [Setup > Hardware Configuration（設定 > ハードウェア設定）] に移動します。
2. [Export hardware configuration（ハードウェア設定のエクスポート）] をクリックします。
3. ブラウザーの種類によっては、エクスポートを完了するためにダイアログを経由する必要があります。

   特に指定がない限り、エクスポートされたファイル (*.json) はデフォルトのダウンロードフォルダーに保存されます。Webブラウザーのユーザー設定で、ダウンロードフォルダーを選択できます。

新しいハードウェア設定の作成

要件に応じた手順に従います。

- *15ページ周辺機器なしで新しいハードウェア設定を作成する方法*
- *19ページワイヤレスロックの新しいハードウェア設定を作成する方法*
- *20ページエレベーター制御システム (AXIS A9188) を含む新しいハードウェア設定を作成する方法*

周辺機器なしで新しいハードウェア設定を作成する方法

1. [Setup > Hardware Configuration（設定 > ハードウェア設定）] に移動し、[Start new hardware configuration（新しいハードウェア設定の開始）] をクリックします。
2. Axis製品の名前を入力します。
3. 接続されたドアの数を選択し、[Next (次へ)] をクリックします。
4. 要件に従ってドアモニター (ドアポジションセンサー) とロックを設定し、[Next (次へ)] をクリックします。利用可能なオプションの詳細については、*15ページドアモニターとロックの設定方法*を参照してください。
5. 使用するリーダーとREXデバイスを設定し、[Finish (完了)] をクリックします。利用可能なオプションの詳細については、*18ページリーダーとREX装置の設定方法*を参照してください。
6. [Close (閉じる)] をクリックするか、リンクをクリックしてハードウェアピン配置図を表示します。

ドアモニターとロックの設定方法

新しいハードウェア設定でドアのオプションを選択している場合、ドアモニターとロックを設定することができます。

1. ドアモニターを使用する場合は、[Door monitor (ドアモニター)] を選択してから、ドアモニターの回路の接続方法に適したオプションを選択します。
2. ドアの開放直後にドアロックがすぐにロックされるようにするには、[Cancel access time once door is opened (ドアが開放されるとアクセス時間をキャンセル)] を選択します。

再ロックを遅らせる場合は、[Relock time (再ロックの時間)] で遅延時間をミリ秒で設定します。

3. ドアのモニター時間のオプションを指定します。ドアモニターを使用しない場合は、ロック時間のオプションを指定します。
4. ロック回路の接続方法に適したオプションを選択します。
5. ロックモニターを使用する場合は、[Lock monitor (ロックモニター)] を選択してから、ロックモニターの回路の接続方法に適したオプションを選択します。
6. リーダー、REX装置、およびドアモニターの入力接続を監視する場合は、[Enable supervised inputs (状態監視を有効にする)] を選択します。

   詳細については、*18ページ監視入力の使用方法* を参照してください。

注

- ほとんどのロック、ドアモニター、およびリーダーのオプションは、リセットしたり新しいハードウェア設定を開始したりしなくても、変更することができます。[Setup > Hardware Reconfiguration (設定 > ハードウェアの再設定)] に移動します。
- ドアコントローラーごとに1つのロックモニターを接続できます。したがって、ダブルロックドアを使用する場合、いずれかのロックのみにロックモニターを設定できます。2つのドアを同じドアコントローラーに接続する場合は、ロックモニターを使用できません。
- 電動ロックは、2つ目のロックとして設定する必要があります。

ドアモニターと時間のオプションについて

以下のドアモニターのオプションが利用できます。

- [Door monitor (ドアモニター)] – デフォルトで選択されています。ドアにはそれぞれ個別にモニターが備えられていて、ドアがこじ開けられたり、長時間開放された場合などに信号を送信します。ドアモニターを使用しない場合は選択を解除します。
  - [Open circuit = Closed door (開路 = ドアを閉じる)] – ドアモニターの回路がNO (ノーマルオープン) の場合に選択します。回路が閉じると、ドアモニターはドアが開いている信号を発信します。回路が開くと、ドアモニターはドアが閉じている信号を発信します。
  - [Open circuit = Open door (開路 = ドアを開放)] – ドアモニターの回路がNC (ノーマルクローズ) の場合に選択します。回路が開くと、ドアモニターはドアが開いている信号を発信します。回路が閉じると、ドアモニターはドアが閉じている信号を発信します。
- [Cancel access time once door is opened (ドアが開放されるとアクセス時間をキャンセル)] – 共連れの発生を防ぐために選択します。ドアモニターでドアが開放されていることが通知されると直ちにドアがロックされます。

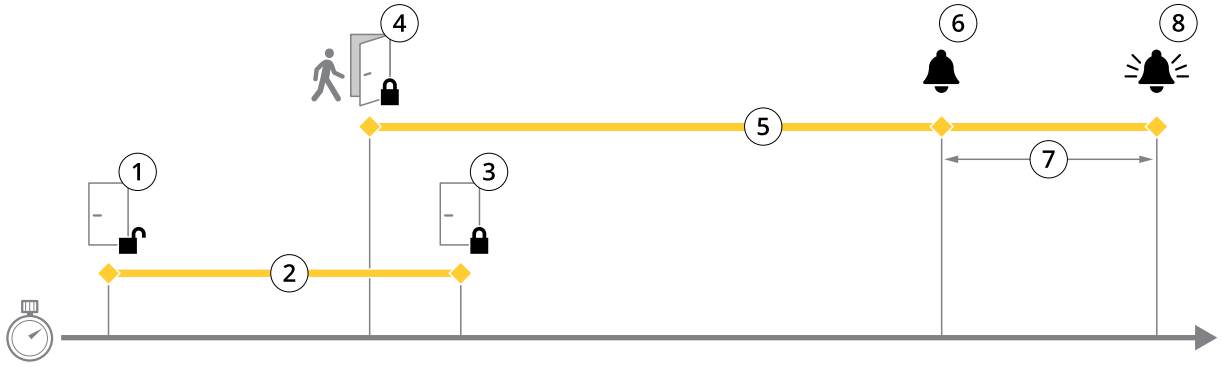
以下のドアの時間のオプションは常時利用できます。

- [Access time (アクセス時間)] – アクセスが許可されてからドアのロック解除を継続する秒数を設定します。ドアが開放されるか設定時間に到達するまでは、ドアはロック解除されたままになります。ドアが閉じられると、アクセス時間が過ぎたかどうかに関わらず、ロックされます。
- [Long access time (長いアクセス時間)] – アクセスが許可されてからドアのロック解除を継続する秒数を設定します。長いアクセス時間は、すでに設定されているアクセス時間を上書きして、長いアクセス時間を選択したユーザーに対して有効になります。詳細については、*42ページユーザー認証情報* を参照してください。

[Door monitor (ドアモニター)] を選択すると、以下のドアの時間のオプションが利用可能になります。

- [Open too long time (長時間のドア開放)] – ドアを開放したままにできる秒数を設定します。設定時間に到達した時点でドアがまだ開放されていると、長時間ドア開放アラームがトリガーされます。アクションルールを設定して、開放が長すぎるイベントでトリガーするアクションを設定してください。

- [Pre-alarm time (プリアラーム時間)] – プリアラームとは、長時間のドア開放になる前にトリガーされる警告信号です。アクションルールの設定方法に応じて、閉じるべきドアから入ろうとしている人物を管理者に通知および警告することで、長時間ドア開放アラームがトリガーされるのを防ぎます。長時間ドア開放アラームのトリガー前に、システムがプリアラームの警告信号を発信する秒数を設定します。プリアラームを無効にするには、プリアラーム時間を0に設定します。



1 アクセス許可 - ロック解除
2 アクセス時間
3 アクションの実行なし - ロック施錠
4 アクションの実行 (ドアの開放) – ロック施錠、またはドアが閉じるまでロック解除状態を維持
5 長時間のドア開放
6 プリアラームの生成
7 プリアラーム時間
8 長時間のドア開放アラームの生成

アクションルールの設定方法については、*48ページアクションルールの設定方法*を参照してください。

ロックのオプションについて

以下のロック回路オプションがあります。

- [12 V]
  - [Fail-secure (フェイルセキュア)] – 停電中は施錠したままにするロックに選択します。通電されると、ロックが解除されます。
  - [Fail-safe (フェイルセーフ)] – 停電中はロック解除するロックに選択します。通電されると、ロックされます。
- [Relay (リレー)] – ドアコントローラーあたり1ロックでのみ使用できます。ドアコントローラーに2つのドアを接続している場合、リレーを使用できるのは、2つ目のドアのロックのみです。
  - [Relay open = Locked (リレー開放 = ロック)] – リレー開放 (フェイルセキュア) 時に施錠したままにするロックに選択します。リレーを閉じると、ロックが解除されます。
  - [Relay open = Unlocked (リレー開放 = ロック解除)] – 停電中 (フェイルセーフ) はロック解除するロックに選択します。リレーを閉じると、ロックされます。
- [None (なし)] – Lock 2でのみ利用できます。ロックを1つのみ使用する場合に選択します。

以下のロックモニターのオプションは、シングルドアの設定で利用できます。

- [Lock monitor (ロックモニター)] – 選択するとロックモニターのコントロールを利用できます。次に監視するロックを選択します。ロックモニターはダブルロックのドアでのみ使用することができ、2つのドアがドアコントローラーに接続されている場合は使用できません。

- [Open circuit = Locked (開路 = ロック)] – ロックモニター回路をNC (ノーマルクローズ) にする場合に選択します。回路が閉じると、ロックモニターはドアのロックが解除されたとの信号を発信します。回路が開くと、ロックモニターはドアがロックされたとの信号を発信します。
- [Open circuit = Unlocked (開路 = ロック解除)] – ロックモニター回路をNO (ノーマルオープン) にする場合に選択します。回路が開くと、ロックモニターはドアのロックが解除されたとの信号を発信します。回路が閉じると、ロックモニターはドアのがロックされたとの信号を発信します。

リーダーとREX装置の設定方法

新しいハードウェア設定でドアモニターとロックを設定している場合、リーダーと退出要求 (REX) 装置を設定できます。

1. リーダーを使用する場合は、チェックボックスを選択してから、リーダーの通信プロトコルに適したオプションを選択します。
2. ボタン、センサー、またはプッシュバーなどのREX装置を使用する場合は、チェックボックスを選択してから、REX装置の回路の接続方法に適したオプションを選択します。

   REX信号がドアの開放に影響しない (メカニカルハンドルまたはプッシュバー付きドアなど) 場合は、[REX does not unlock door (REXでドアをロック解除しない)] を選択します。
3. ドアコントローラーに複数のリーダーまたはREX装置を接続している場合は、それぞれのリーダーまたはREX装置の設定が修正されるまで上記の2つの手順を再度行ってください。

リーダーおよびREX装置のオプションについて

以下のリーダーのオプションがあります。

- [Wiegand] – Wiegandプロトコルを使用するリーダーを選択します。次にリーダーでサポートされているLEDコントロールを選択します。シングルLEDコントロールを備えたリーダーは通常、赤と緑の間で切り替えます。デュアルLEDコントロールを備えたリーダーは、通常、赤、緑のLED用にさまざまな配線を使用します。これは、それぞれのLEDが個別に制御されることを意味します。両方のLEDがオンの場合、ライトは黄色になります。リーダーがサポートするLEDコントロールについては、メーカーの情報を参照してください。
- [OSDP, RS485 half duplex (OSDP、RS485 半二重)] – 半二重をサポートするRS485リーダーを選択します。リーダーがサポートするプロトコルについては、メーカーの情報を参照してください。

以下のREX装置のオプションがあります。

- [Active low (アクティブ低)] – REX装置による閉回路をアクティブにする場合に選択します。
- [Active high (アクティブ高)] – REX装置による開回路をアクティブにする場合に選択します。
- [REX does not unlock door (REXでドアをロック解除しない)] – REX信号がドアの開放に影響しない (メカニカルハンドルまたはプッシュバー付きドアなど) 場合に選択します。ユーザーがアクセス時間内にドアを開いていれば、ドアのこじ開けのアラームはトリガーされません。ユーザーがREX装置をアクティブ化するとドアが自動的にロック解除される場合は選択解除します。

注

ほとんどのロック、ドアモニター、およびリーダーのオプションは、リセットしたり新しいハードウェア設定を開始したりしなくても、変更することができます。[Setup > Hardware Reconfiguration (設定 > ハードウェアの再設定)] に移動します。

監視入力の使用方法

監視入力は、ドアコントローラーと、リーダー、REX装置、およびドアモニターとの間の接続ステータスを報告します。接続が中断されると、イベントが有効になります。

監視入力を使用するには:

1. 使用するすべての監視入力に終端抵抗器を設置します。*77ページ*の接続図を参照してください。
2. [Setup > Hardware Reconfiguration（設定 > ハードウェアの再設定)] に移動し、[Enable supervised inputs (監視入力を有効にする)] を選択します。ハードウェアの設定中に監視入力を有効にすることもできます。

状態監視の互換性について

以下のコネクタは、状態監視をサポートします。

- リーダーI/Oコネクタ – 信号のいたずら。*72ページ*を参照してください。
- ドアコネクタ。*73ページ*を参照してください。

状態監視で使用できるリーダーおよびスイッチは、以下のとおりです。

- 内部プルアップ1 kΩ～5 Vのリーダーおよびスイッチ。
- 内部プルアップなしのリーダーおよびスイッチ。

ワイヤレスロックの新しいハードウェア設定を作成する方法

1. [Setup > Hardware Configuration（設定 > ハードウェア設定)] に移動し、[Start new hardware configuration（新しいハードウェア設定の開始)] をクリックします。
2. Axis製品の名前を入力します。
3. 周辺機器のリストで、ワイヤレスゲートウェイのメーカーを選択します。
4. 有線のドアを接続する場合は、[1 Door (1 ドア)] チェックボックスをオンにし、[Next (次へ)] をクリックします。ドアが含まれない場合は、[Finish (完了)] をクリックします。
5. ロックのメーカーに応じて、以下の箇条書きのいずれかに従って進んでください。
   - ASSA Aperio: リンクをクリックしてハードウェアピン配置図を表示するか、[Close (閉じる)] をクリックし、[Setup > Hardware Reconfiguration（設定 > ハードウェアの再設定)] に移動して設定を完了します。*19ページAssa Aperio™のドアとデバイスの追加*を参照してください。
   - SmartIntego : リンクをクリックしてハードウェアピン配置図を表示するか、[Click here to select wireless gateway and configure doors (ここをクリックしてワイヤレスゲートウェイを選択し、ドアを設定する)] をクリックして設定を完了します。*27ページSmartIntegoの設定方法*を参照してください。

Assa Aperio™のドアとデバイスの追加

ワイヤレスドアをシステムに追加する前に、Aperio PAP (Aperioプログラミングアプリケーションツール) を使用して、接続されたAssa Aperioコミュニケーションハブとドアをペアリングする必要があります。

ワイヤレスドアを追加するには:

1. [Setup (設定)] > [Hardware Reconfiguration（ハードウェアの再設定)] を選択します。
2. [Wireless Doors and Devices (ワイヤレスドアおよびデバイス)] で、[Add door (ドアの追加)] をクリックします。
3. [Door name (ドア名)] フィールドに、わかりやすい名前を入力します。
4. [Lock (ロック)] の [ID] フィールドに、追加するデバイスの6文字のアドレスを入力します。デバイスのアドレスは、製品のラベルに印刷されています。
5. 必要に応じて、[Door position sensor (ドアポジションセンサー)] で、[Built in door position sensor (内蔵ドアポジションセンサー)] または [External door position sensor (外部ドアポジションセンサー)] を選択します。

注

外部ドアポジションセンサー (DPS) を使用する場合は、Aperioロックデバイスを設定する前に、デバイスがドアハンドルの状態検知に対応していることを確認してください。

6. 必要に応じて、[**Door position sensor (ドアポジションセンサー)**] の [**ID**] フィールドに、追加するデバイスの6文字のアドレスを入力します。デバイスのアドレスは、製品のラベルに印刷されています。
7. [**Add (追加)**] をクリックします。

エレベーター制御システム (AXIS A9188) を含む新しいハードウェア設定を作成する方法

重要

ハードウェア設定を作成する前に、AXIS A9188 Network I/O Relay Moduleでユーザーを追加する必要があります。A9188のWebインターフェース > [**Preferences > Additional device configuration > Basic setup > Users > Add > User setup (環境設定 > 追加のデバイス設定 > 基本設定 > ユーザー > 追加 > ユーザーの設定)**] に移動します。

注

それぞれのAxis Network Door Controllerで、最大2つのAXIS 9188 Network I/O Relay Modulesを設定できます。

1. A1001で、[**Setup > Hardware Configuration (設定 > ハードウェア設定)**] に移動し、[**Start new hardware configuration (新しいハードウェア設定の開始)**] をクリックします。
2. Axis製品の名前を入力します。
3. 周辺機器のリストで、[**Elevator control (エレベーターコントロール)**] を選択してAXIS A9188 Network I/O Relay Moduleを含め、[**Next (次へ)**] をクリックします。
4. 接続されたリーダーの名前を入力します。
5. 使用するリーダープロトコルを選択し、[**Finish (完了)**] をクリックします。
6. [**Network Peripherals (ネットワーク周辺機器)**] をクリックして設定を完了するか (*20ページネットワーク周辺機器の追加および設定の方法* 参照)、リンクをクリックしてハードウェアピン配置図を表示します。

ネットワーク周辺機器の追加および設定の方法

重要

- ネットワーク周辺機器を設定する前に、AXIS A9188 Network I/O Relay Moduleでユーザーを追加する必要があります。AXIS A9188のWebインターフェース > [**Preferences > Additional device configuration > Basic setup > Users > Add > User setup (環境設定 > 追加のデバイス設定 > 基本設定 > ユーザー > 追加 > ユーザーの設定)**] に移動します。
- 別のAXIS A1001 Network Door Controllerをネットワーク周辺機器として追加しないでください。

1. デバイスを追加するには [**Setup > Network Periphals (設定 > ネットワーク周辺機器)**] に移動します。
2. [**Discovered devices (検知されたデバイス)**] でデバイスを見つけます。
3. [**Add this device (このデバイスを追加)**] をクリックします。
4. デバイスの名前を入力します。
5. AXIS A9188のユーザー名とパスワードを入力します。
6. [**Add (追加)**] をクリックします。

注

[**Manually add device (デバイスを手動で追加)**] ダイアログにMACアドレスまたはIPアドレスを入力すると、ネットワーク周辺機器を手動で追加できます。

重要

スケジュールを削除する場合は、まずそのスケジュールがネットワークI/Oリレー モジュールで使用されていないことを確認してください。

ネットワーク周辺機器にI/Oおよびリレーを設定する方法

重要

ネットワーク周辺機器を設定する前に、AXIS A9188 Network I/O Relay Moduleでユーザーを追加する必要があります。AXIS A9188のWebインターフェース > [**Preferences > Additional device configuration > Basic setup > Users > Add > User setup (環境設定 > 追加のデバイス設定 > 基本設定 > ユーザー > 追加 > ユーザーの設定)**] に移動します。

1. [**Setup > Network Periphals (設定 > ネットワーク周辺機器)**] に移動し、[**Added devices (追加するデバイス)**] 行をクリックします。
2. フロアとして設定するI/Oとリレーを選択します。
3. [**Set as floor (フロアとして設定)**] をクリックし、名前を入力します。
4. [**Add (追加)**] をクリックします。

これで、[**Access Management (アクセス管理)**] の [**Floor (フロア)**] タブにフロアが表示されます。

注

AXIS Entry Managerで、最大16個のフロアを追加できます。

ハードウェアの接続の確認

ハードウェアの設置と設定が完了すると、ドアコントローラーの有効期限中はいつでも、接続されたドアのモニター、ネットワークのI/Oリレーモジュール、ロック、リーダーの機能を確認することができます。

設定を確認し、検証コントロールにアクセスするには [**Setup > Hardware Connection Verification (設定 > ハードウェア接続の確認)**] に移動します。

ドアの制御の検証

- **ドアの状態** – ドアモニター、ドアのアラームおよびロックの現在の状態を確認します。[**Get current state (現在の状態を取得)**] をクリックします。
- **ロック** – ロックを手動でトリガーします。プライマリロックとセカンダリロックがある場合は両方に適用されます。[**Lock (ロック)**] または [**Unlock (ロックを解除)**] をクリックします。
- **ロック** – アクセス権を付与するロックを手動でトリガーします。プライマリロックにのみ適用されます。[**Access (アクセス権)**] をクリックします。
- **リーダー: フィードバック** – さまざまなコマンドについて、音声やLED信号などのリーダーからのフィードバックを確認します。コマンドを選択し、[**Test (テスト)**] をクリックします。利用可能なフィードバックの種類は、リーダーによって異なります。詳細については、*53ページリーダーからのフィードバック*を参照してください。メーカーの指示も参照してください。
- **リーダー: いたずら** – 前回のいたずらに関する情報を取得します。リーダーがインストールされている場合、最初に試行されたいたずらが登録されます。[**Get last tampering (前回のいたずらに関する情報を取得)**] をクリックします。
- **リーダー: カードの読み取り** – 前回のカード読み取りに関する情報、または、リーダーによって許可された他のユーザートークンの種類に関する情報を取得します。[**Get last credential (前回の認証情報を取得)**] をクリックします。
- **REX** – 前回、押された退出要求 (REX) 装置に関する情報を取得します。[**Get last REX (前回のREXに関する情報を取得)**] をクリックします。

フロアのコントロール検証

- **フロアの状態** – フロアアクセスの現在の状態を確認します。[Get current state (現在の状態を取得)] をクリックします。
- **フロアのロックとフロアのロック解除** – フロアアクセスを手動でトリガーします。プライマリロックとセカンダリロックがある場合は両方に適用されます。[Lock (ロック)] または [Unlock (ロックを解除)] をクリックします。
- **フロアアクセス** – 一時的なフロアアクセスを手動で許可します。プライマリロックにのみ適用されます。[Access (アクセス権)] をクリックします。
- **エレベーターリーダー: フィードバック** – さまざまなコマンドについて、音声やLED信号などのリーダーからのフィードバックを確認します。コマンドを選択し、[Test (テスト)] をクリックします。利用可能なフィードバックの種類は、リーダーによって異なります。詳細については、*53ページリーダーからのフィードバック*を参照してください。メーカーの指示も参照してください。
- **エレベーターリーダー: いたずら** – 前回のいたずらに関する情報を取得します。リーダーがインストールされている場合、最初に試行されたいたずらが登録されます。[Get last tampering (前回のいたずらに関する情報を取得)] をクリックします。
- **エレベーターリーダー: カードの読み取り** – 前回のカード読み取りに関する情報、または、リーダーによって許可された他のユーザートークンの種類に関する情報を取得します。[Get last credential (前回の認証情報を取得)] をクリックします。
- **REX** – 前回、押された退出要求 (REX) 装置に関する情報を取得します。[Get last REX (前回のREXに関する情報を取得)] をクリックします。

カードおよびフォーマットの設定

ドアコントローラーには一般に使用されている定義済みのカードフォーマットがいくつかあり、そのまま使用することも、必要に応じて変更することもできます。カスタムのカードフォーマットを作成することもできます。各カードフォーマットには、カードに保存される情報の体系化の方法を規定する、さまざまなルールセットやフィールドマップがあります。カードフォーマットを定義することで、コントローラーがリーダーから取得する情報をどのように解釈するかがシステムに通知されます。リーダーがサポートするカードフォーマットの詳細については、メーカーの指示を参照してください。

カードフォーマットを有効にするには:

1. [Setup > Configure cards and formats (設定 > カードとフォーマットの設定)] に移動します。
2. 接続するリーダーが使用するカードフォーマットに一致する1つ以上のカードフォーマットを選択します。

カードフォーマットを新規作成するには:

1. [Setup > Configure cards and formats (設定 > カードとフォーマットの設定)] に移動します。
2. [Add card format (カードフォーマットの追加)] をクリックします。
3. Add card format (カードフォーマットの追加)] ダイアログで、カードフォーマットの名前、説明、およびビット長を入力します。*23ページカードフォーマットの説明*を参照してください。
4. [Add field map (フィールドマップの追加)] をクリックして必要な情報をフィールドに入力します。*23ページフィールドマップ*を参照してください。
5. 複数のフィールドマップを追加するには、上記の手順を繰り返します。

[Card formats (カードフォーマット)] リストのアイテムを展開してカードフォーマットの説明とフィールドマップを表示するには、 をクリックします。

カードフォーマットを編集するには、をクリックし、カードフォーマットの説明とフィールドマップを必要に応じて変更します。その後、[Save (保存)] をクリックします。

[Edit card format (カードフォーマットの編集)] ダイアログまたは [Add card format (カードフォーマットの追加)] ダイアログでフィールドマップを削除するには、 をクリックします。

カードフォーマットを削除するには、 をクリックします。

重要

- カードフォーマットに対するすべての変更は、ドアコントローラーシステム全体に適用されます。
- 最低1つのリーダーが接続された最低1つのドアコントローラーをシステムに設定している場合は、カードフォーマットを有効または無効にのみ設定できます。詳細については、*14ページハードウェアの設定* および *18ページリーダーとREX装置の設定方法* を参照してください。
- 同一ビット長の2つのカードフォーマットを同時にアクティブにすることはできません。たとえば、「Format A」と「Format B」という2つの32ビットカードフォーマットを定義していて「Format A」を有効にしている場合は、先に「Format A」を無効にしない限り、「Format B」を有効にすることはできません。
- 有効にしているカードフォーマットがない場合は、[Card raw only (カード保存未加工データのみ)] および [Card raw and PIN (カード保存未加工データとPIN)] の識別タイプを使用してカードを識別し、さらにユーザーにアクセス権を付与することができます。ただし、リーダーのメーカーまたはリーダーの設定によって異なるカード保存未加工データが生成される場合があるため、この方法はお勧めできません。

カードフォーマットの説明

- [Name (名前)] (必須) – 分かりやすい名前を入力します。
- [Description (説明)] – 必要に応じて追加情報を入力します。この情報は、[Edit card format (カードフォーマットの編集)] ダイアログおよび [Add card format (カードフォーマットの追加)] ダイアログにのみ表示されます。
- [Bit length (ビット長)] (必須) – カードフォーマットのビット長を入力します。1～1000000000の数値にする必要があります。

フィールドマップ

- [Name (名前)] (必須) – フィールドマップ名をスペースなしで入力します。例: `OddParity`。

  一般的なフィールドマップの例は、次のとおりです。

  - [`Parity (パリティ)`] – エラー検知にパリティビットを使用します。通常、パリティビットはバイナリコード文字列の先頭または末尾に追加され、ビット数が奇数と偶数のどちらであるかを示します。
  - [`EvenParity`] – 偶数パリティビットは文字列に偶数のビット数があることを確認します。値1を持つビットがカウントされます。カウントがすでに偶数の場合、パリティビット値は0に設定されます。カウントが奇数の場合は、カウントの合計が偶数の数になるように、偶数のパリティビット値は1に設定されます。
  - [`OddParity`] – 奇数パリティビットは文字列に奇数のビット数があることを確認します。値1を持つビットがカウントされます。カウントがすでに奇数の場合、この奇数のパリティビット値は0に設定されます。カウントが偶数の場合は、カウントの合計が奇数の数になるように、偶数のパリティビット値は1に設定されます。
  - [`FacilityCode`] – トークンが順序付きエンドユーザーの認証情報バッチと一致することを確認するために設備コードが使用される場合があります。従来、使用されていたアクセスコントロールシステムは、検証の精度が低く、合致するサイトコードでエンコードされていた認証情報バッチで、すべての従業員の入場を許可していました。本製品で設備コードを検証するには、大文字と小文字を区別する、このフィールドマップの名前が必須です。
  - [`CardNr`] – カード番号またはユーザーIDは、アクセスコントロールシステムの検証で最も一般に使用されている情報です。本製品でカード番号を検証するには、大文字と小文字を区別する、このフィールドマップの名前が必須です。

- [CardNrHex] – 本製品でカード番号のバイナリデータは小文字の16進数にエンコードされています。これは主に、リーダーから予想したカード番号を取得できない場合のトラブルシューティング目的で使用されます。

- [**Range (範囲)**] (必須) – フィールドマップのビット範囲を入力します。例: 1、2〜17、18〜33、および34。
- [**Encoding (エンコード方式)**] (必須) – 各フィールドマップのエンコード方式を選択します。
  - [**BinLE2Int**] – バイナリデータをリトルエンディアン方式のビット並び順で整数としてエンコードします。整数とは、小数点以下を含めない整数にする必要があることを意味します。リトルエンディアン方式のビット並び順とは、最初のビットが最小 (下位) であることを意味します。
  - [**BinBE2Int**] – バイナリデータをビッグエンディアン方式のビット並び順で整数としてエンコードします。整数とは、小数点以下を含めない整数にする必要があることを意味します。ビッグエンディアン方式のビット並び順とは、最初のビットが最大 (上位) であることを意味します。
  - [**BinLE2Hex**] – バイナリデータをリトルエンディアン方式のビット並び順で小文字の16進数としてエンコードします。16進数システムは、ベース16の番号システムとも呼ばれ、次の16種類の固有の記号で構成されます。数字0〜9および文字a〜f。リトルエンディアン方式のビット並び順とは、最初のビットが最小 (下位) であることを意味します。
  - [**BinBE2Hex**] – バイナリデータをビッグエンディアン方式のビット並び順で小文字の16進数としてエンコードします。16進数システムは、ベース16の番号システムとも呼ばれ、次の16種類の固有の記号で構成されます。数字0〜9および文字a〜f。ビッグエンディアン方式のビット並び順とは、最初のビットが最大 (上位) であることを意味します。
  - [**BinLEIBO2Int**] – バイナリデータはBinLE2Intと同様にエンコードされますが、フィールドマップを使用してエンコードする前に、カード未加工データが逆のバイト順で複数バイトシーケンスに読み出されます。
  - [**BinBEIBO2Int**] – バイナリデータはBinBE2Intと同様にエンコードされますが、フィールドマップを使用してエンコードする前に、カード未加工データが逆のバイト順で複数バイトシーケンスに読み出されます。

ご使用のカードフォーマットでどのフィールドマップが使用されているかについては、メーカーの指示を参照してください。

プリセット設備コード

トークンと設備のアクセスコントロールシステムが一致することを確認するために、設備コードを使用する場合があります。単一設備に発行されたすべてのトークンに同一の設備コードが設定されていることがよくあります。プリセット設備コードを入力することで、大量のカードを手動で登録する際の省力化になります。ユーザーを追加する場合のプリセット設備コードの自動入力については、*42ページユーザー認証情報*を参照してください。

プリセット設備コードを設定するには:

1. [**Setup > Configure cards and formats (設定 > カードとフォーマットの設定)**] に移動します。
2. [**Preset facility code (プリセット設備コード)**] で、設備コードを入力します。
3. [**Set facility code (設備コードの設定)**] をクリックします。

サービスの設定

[Setup (設定)] ページの [Configure Services (サービスの設定)] を使用して、ドアコントローラーで使用できる外部サービスの設定にアクセスします。

AXIS Visitor Access

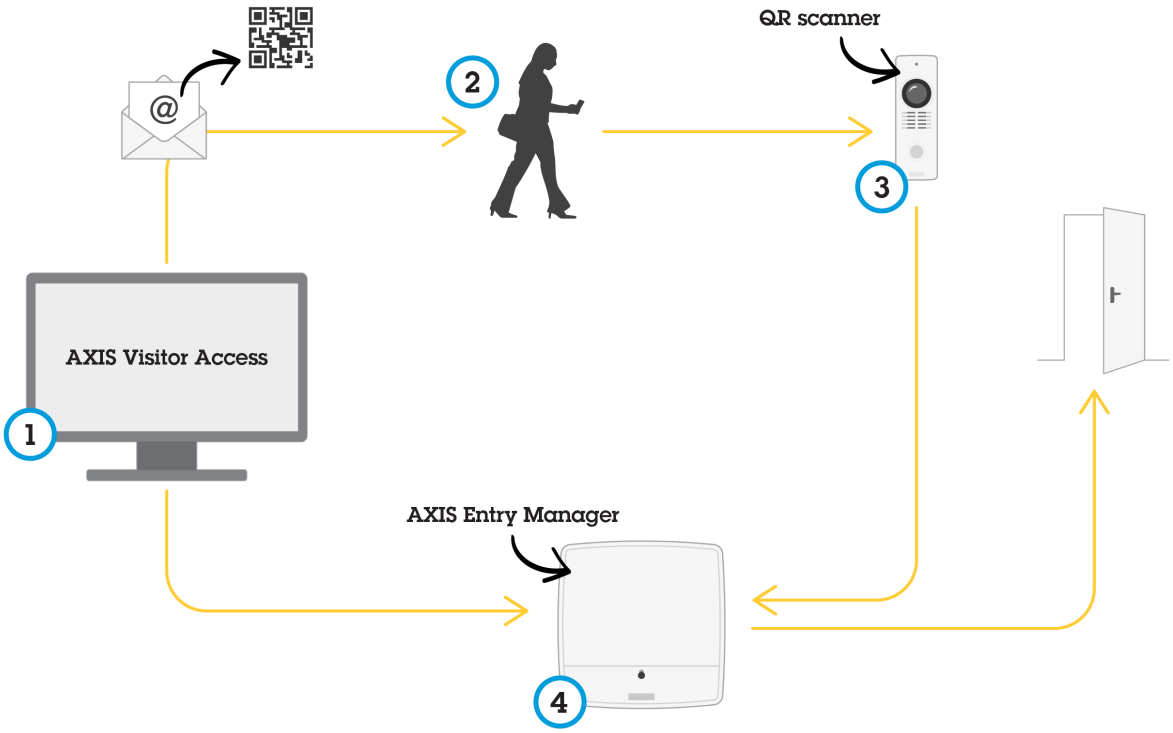
AXIS Visitor Accessを使用する場合、一時的な認証情報をQRコードの形式で作成できます。アクセスコントロールシステムに接続されているAxisネットワークカメラまたはドアステーションは、QRコードをスキャンします。

AXIS A1001 & AXIS Entry Manager

システムの設定

サービスは以下の要素で構成されます。

- AXIS Entry Managerとバージョン1.65.2以降のファームウェアが組み込まれたAxisドアコントローラー
- QRスキャナーアプリケーションがインストールされたAxisネットワークカメラまたはドアステーション
- AXIS Visitor Accessアプリケーションがインストールされた Windows® PC



AXIS Visitor Accessサービスの使用法

ユーザーがAXIS Visitor Accessで招待状を作成し (1)、その招待状を訪問者のメールアドレスに送信します。同時に、ドアのロックを解除する認証情報が作成され、接続されたAxisドアコントローラーに保存されます (4)。訪問者が、招待状に含まれるQRコードをネットワークカメラまたはネットワークドアステーションに示し (3)、それによって訪問者のためにドアのロックを解除するようにドアコントローラーに依頼されます (4)。

QR CodeはDenso Wave, inc.の登録商標です。

前提条件: AXIS Visitor Access

AXIS Visitor Accessサービスを使用する前に、次のことが必要です。

- ドアコントローラーのハードウェアを設定する
- Axisネットワークカメラまたはドアステーションが、ドアコントローラーと同じネットワークに接続され、ドアの近くの訪問者にアクセスできるように配置されている
- AXIS Visitor Accessインストールパッケージがある。パッケージは*axis.com*にあります
- ドアコントローラーに2つの追加ユーザーアカウント (AXIS Visitor Accessサービスだけで使用)。AXIS Visitor Accessアプリケーションに1つ、QRスキャナーアプリケーションに1つ必要です。ユーザーアカウントの作成方法については、*56*ページユーザーを参照してください。

システムの設定

重要

- AXIS Visitor Accessサービスは、システム全体で1つのドアコントローラーにのみ接続できます。
- AXIS Visitor Accessサービスでは、接続されたドアコントローラーによって制御されるドアにのみ対応できます。システム内の他のドアには対応できません。
- 訪問者を変更および削除するには、AXIS Visitor Accessアプリケーションを使用します。AXIS Entry Managerは使用しないでください。
- AXIS Visitor Accessに使用するユーザーアカウントのパスワードを変更した場合は、AXIS Visitor Accessでも同様に更新する必要があります。
- QRスキャナーアプリケーションに使用するユーザーアカウントのパスワードを変更した場合は、QRスキャナーをもう一度設定する必要があります。

AXIS Visitor Accessを設定する

AXIS Visitor Accessサービスを設定するときは、Axisネットワークカメラまたはネットワークドアステーションに、QRスキャナーアプリケーションをインストールします。別のインストールは必要ありません。

1. ドアコントローラーのWebページで、[**Setup > Configure Services > Settings (セットアップ > サービスの設定 > 設定)**] の順に移動します。
2. [**Start a new setup (新しい設定の開始)**] をクリックします。
3. 指示に従って、設定を完了します。

重要

HTTPSの使用を強制する場合は、ドアコントローラーがHTTPSで通信することを確認します。そうでない場合、アプリケーションはドアコントローラーと通信できません。

4. 一時的な認証情報を作成するために使用されるコンピューターに、AXIS Visitor Accessアプリケーションをインストールして設定します。

SmartIntego

SmartIntegoは、ドアコントローラーで処理できるドアの数を増やすワイヤレスソリューションです。

SmartIntegoの必要条件

SmartIntegoの設定を進める前に、以下の必要条件を満たす必要があります。

- csvファイルを作成する必要があります。このcsvファイルには、SmartIntegoソリューションで使用されるGatewayNodeとドアに関する情報が含まれます。このファイルは、SimonsVossパートナーによって提供されるスタンドアロンソフトウェアで作成されます。
- SmartIntegoのハードウェア設定が行われました。*19ページワイヤレスロックの新しいハードウェア設定を作成する方法*を参照してください。

システムの設定

注

- SmartIntego設定ツールは、バージョン2.1.6452.23485、ビルド2.1.6452.23485 (2017年8月31日午後1:02:50) 以降である必要があります。
- Advanced Encryption Standard (AES) はSmartIntegoに対応していないため、SmartIntego設定ツールで無効にする必要があります。

SmartIntegoの設定方法

注

- 示された必要条件を満たしていることを確認します。
- バッテリーの状態がさらにわかりやすくなるように、[**Setup (設定)**] > [**Configure event and alarms logs (イベントとアラームのログ設定)**] の順に選択し、アラームとして [**Door — Battery alarm (ドア — バッテリーアラーム)**] または [**IdPoint — Battery alarm (IdPoint — バッテリーアラーム)**] を追加します。
- ドアモニターの設定はインポートされたCSVファイルに入っています。通常の設置では、この設定を変更する必要はありません。

1. [**Browse... (参照...)**] をクリックし、CSVファイルを選択して、[**Upload file (ファイルのアップロード)**] をクリックします。
2. GatewayNodeを選択し、[**Next (次へ)**] をクリックします。
3. 新しい設定のプレビューが表示されます。必要に応じて、ドアモニターを無効にします。
4. [**Configure (設定)**] をクリックします。
5. 設定に含まれるドアの概要が表示されます。[**Settings (設定)**] をクリックして、各ドアを個別に設定します。

SmartIntegoの再設定方法

1. 一番上のメニューで [**Setup (設定)**] をクリックします。
2. [**Configure Services (サービスの設定)**] > [**Settings (設定)**] をクリックします。
3. [**Re-configure (再設定)**] をクリックします。
4. [**Browse... (参照...)**] をクリックし、CSVファイルを選択して、[**Upload file (ファイルのアップロード)**] をクリックします。
5. GatewayNodeを選択し、[**Next (次へ)**] をクリックします。
6. 新しい設定のプレビューが表示されます。必要に応じて、ドアモニターを無効にします。

注

ドアモニターの設定はインポートされたCSVファイルに入っています。通常の設置では、この設定を変更する必要はありません。

7. [**Configure (設定)**] をクリックします。
8. 設定に含まれるドアの概要が表示されます。[**Settings (設定)**] をクリックして、各ドアを個別に設定します。

ネットワークドアコントローラーの管理

[Manage Network Door Controllers in System (システムのネットワークドアコントローラーを管理)] ページは、ドアコントローラー情報、システムステータス情報およびシステムを構成する他のドアコントローラーに関する情報を表示します。また、このページで管理者がドアコントローラーを追加したり削除したりして、システムの設定を変更できます。

システムの設定

重要

システム内のすべてのドアコントローラーは、同じネットワークに接続し、1か所で使用するように設定する必要があります。

ドアコントローラーを管理するには [**Setup > Manage Network Door Controllers in System (設定 > システムのネットワークドアコントローラーを管理)**] に移動します。

[Manage Network Door Controllers in System (システムのネットワークドアコントローラーを管理)] ページには以下のパネルがあります。

- [**System status of this controller (このコントローラーのシステムステータス)**] – ドアコントローラーのシステムステータスが表示され、システムとスタンドアロンモードを切り替えることができます。詳細については、*28ページドアコントローラーのシステムステータス*を参照してください。
- [**Network door controllers in system (システム内のネットワークドアコントローラー)**] – システムのドアコントローラーに関する情報が表示され、コントローラーをシステムに追加したりシステムから削除したりするためのコントロールが含まれています。詳細については、*28ページシステム内の接続するドアコントローラー*を参照してください。

ドアコントローラーのシステムステータス

ドアコントローラーをドアコントローラーシステムの一部として構成できるかどうかは、システムのステータスによって異なります。ドアコントローラーのシステムのステータスは、[**System status for this controller (このコントローラーのシステムステータス)**] パネルに表示されます。

ドアコントローラーがスタンドアロンモードになっておらず、システムに追加されないように保護する場合は、[**Activate standalone mode (スタンドアロンモードのアクティブ化)**] をクリックしてスタンドアロンモードに移行します。

スタンドアロンモードになっているドアコントローラーをシステムに追加したい場合は、[**Deactivate standalone mode (スタンドアロンモードの非アクティブ化)**] をクリックしてスタンドアロンモードを終了します。

システムモード

- [**This controller is not part of a system and not in standalone mode (このドアコントローラーはシステムの一部ではなくスタンドアロンモードでない)**] – ドアコントローラーはシステムの一部として設定されておらず、スタンドアロンモードでもありません。これは、ドアコントローラーが開放されていて同じネットワーク内の他の任意のドアコントローラーによってシステムに追加できることを意味します。ドアコントローラーがシステムに追加されないように保護するには、スタンドアロンモードをアクティブ化します。
- [**This controller is set to standalone mode (このコントローラーはスタンドアロンモードに設定されている)**] – ドアコントローラーはシステムの一部ではありません。このコントローラーは、ネットワークの他のドアコントローラーでシステムに追加することも、他のドアコントローラーを追加することもできません。通常、スタンドアロンモードは、1つのドアコントローラーと1つまたは2つのドアからなる小規模の設定で使用されます。ドアコントローラーをシステムに追加できるようにするには、スタンドアロンモードを非アクティブ化します。
- [**This controller is part of a system (このコントローラーはシステムの一部である)**] – ドアコントローラーは分散システムの一部です。分散システムでは、ユーザー、グループ、ドア、およびスケジュールを接続するコントローラー間で共有します。

システム内の接続するドアコントローラー

[**Network door controllers in system (システム内のネットワークドアコントローラー)**] パネルには、以下のシステム変更に関するコントロールがあります。

- システムへのドアコントローラーの追加については、*29ページシステムにドアコントローラーを追加する*を参照してください。

- システムからのドアコントローラーの削除については、*30ページシステムからドアコントローラーを削除する*を参照してください。

接続されたドアコントローラーのリスト

[Network door controllers in system (システム内のネットワークドアコントローラー)] パネルには、システム内の接続されているドアコントローラーに関する以下のIDおよびステータス情報を表示するリストも含まれています。

- [Name (名前)] – ユーザーが定義したドアコントローラーの名前。ハードウェアの設定時に管理者が名前を設定しなかった場合は、デフォルトの名前が表示されます。
- [IP address (IPアドレス)]
- [MAC address (MACアドレス)]
- [Status (ステータス)] – システムへのアクセスで使用するドアコントローラーに、ステータス [This controller (このコントローラー)] が表示されます。システム内の他のドアコントローラーには、ステータス [Online (オンライン)] が表示されます。
- [Firmware version (ファームウェアバージョン)]

他のドアコントローラーのWebページを開くには、コントローラーのIPアドレスをクリックします。

リストを更新するには、[Refresh the list of controllers (コントローラーのリストを更新)] をクリックします。

注

システム内のすべてのコントローラーは、常に同じバージョンのファームウェアを使用する必要があります。システム全体のすべてのコントローラーでファームウェアの並列アップグレードを行うには、Axis Device Managerを使用します。

システムにドアコントローラーを追加する

重要

ドアコントローラーをペアリングすると、追加されたコントローラーのすべてのアクセス管理設定は削除され、システムのアクセス管理設定によって上書きされます。

ドアコントローラーのリストからドアコントローラーをシステムに追加するには:

1. [Setup > Manage Network Door Controllers in System (設定 > システムのネットワークドアコントローラーを管理)] に移動します。
2. [Add controllers to system from list (リストからコントローラーをシステムに追加)] をクリックします。
3. 追加するコントローラーを選択します。
4. [Add (追加)] をクリックします。
5. ドアコントローラーをさらに追加するには、上記の手順を繰り返します。

既知のIPアドレスまたはMACアドレスを使用してドアコントローラーをシステムに追加するには:

1. [Manage Devices (デバイス管理)] に移動します。
2. [Add controller to system by IP or MAC address (IPまたはMACアドレスを使用してコントローラーをシステムに追加)] をクリックします。
3. IPアドレスまたはMACアドレスを入力します。
4. [Add (追加)] をクリックします。
5. ドアコントローラーをさらに追加するには、上記の手順を繰り返します。

システムの設定

ペアリングが完了すると、システムのすべてのドアコントローラーによって、すべてのユーザー、ドア、スケジュール、およびグループが共有されます。

リストを更新するには、[Refresh list of controllers (コントローラーのリストを更新)] をクリックします。

システムからドアコントローラーを削除する

重要

- ドアコントローラーをシステムから削除する前に、ドアコントローラーのハードウェア設定をリセットしてください。この手順をスキップすると、削除対象のドアコントローラーに関連するすべてのドアがシステムに残存して削除できなくなります。
- ドアコントローラーを2つのコントローラーシステムから削除すると、両方のドアコントローラーは自動的にスタンドアロンモードに切り替わります。

ドアコントローラーをシステムから削除するには:

1. 削除するドアコントローラー経由でシステムにアクセスし、[Setup > Hardware Configuration (設定 > ハードウェア設定)] に移動します。
2. [Reset hardware configuration (ハードウェア設定のリセット)] をクリックします。
3. ハードウェア設定がリセットされたら、[Setup > Manage Network Door Controllers in System (設定 > システムのネットワークドアコントローラーを管理)] に移動します。
4. [Network door controllers in system (システム内のネットワークドアコントローラー)] リストで削除を希望するドアコントローラーを特定し、[Remove from system (システムから削除)] をクリックします。
5. ダイアログが開き、ドアコントローラーのハードウェア設定をリセットするよう求められます。[Remove controller (コントローラーを削除)] をクリックして確認します。
6. ダイアログが開き、ドアコントローラーの削除を希望するか確認が求められます。[OK] をクリックして確認します。削除したドアコントローラーはこれでスタンドアロンモードになりました。

注

- ドアコントローラーがシステムから削除されると、そのすべてのアクセス管理設定は削除されます。
- オンラインのドアコントローラーのみ削除できます。

設定モード

設定モードは、デバイスに最初にアクセスするときの標準のモードです。設定モードが無効になっている場合は、デバイスのほとんどの設定機能が表示されません。

重要

設定モードの無効化をセキュリティの機能と見なすことはできません。これは、間違った設定を停止することが目的であり、悪意あるユーザーが重要な設定を変更するのを阻止するためのものではありません。

設定モードを無効にする方法

1. [Setup (設定)] > [Disable Configuration Mode (設定モードを無効にする)] に移動します。
2. PINを入力して [OK] を選択します。

注

PINの入力は任意です。

設定モードを有効にする方法

1. [Setup (設定)] > [Enable Configuration Mode (設定モードを有効にする)] に移動します。

2. PINを入力して [OK] を選択します。

注

PINを覚えていない場合は、次のように入力すると設定モードを有効にできます。
`http://[IP-address]/webapp/pacs/index.shtml#resetConfigurationMode`

メンテナンス手順

アクセスコントロールシステムのスムーズな動作を保つために、ドアコントローラーや接続されたデバイスを含めて、アクセスコントロールシステムを定期的にメンテナンスすることをお勧めします。

少なくとも年に一度はメンテナンスを行ってください。提案するメンテナンス手順には以下の手順が含まれますが、これらに限定されません。

- ドアコントローラーと外部デバイスの間がすべてしっかりと接続されていることを確認します。
- すべてのハードウェアの接続を確認します。*21ページドアの制御の検証*を参照してください。
- 接続された外部デバイスも含めて、システムが正常に機能することを確認します。
  - カードを通し、リーダー、ドア、およびロックをテストします。
  - システムにREX装置、センサー、またはその他のデバイスが含まれる場合は、それらもテストします。
  - アクティブになったら、いたずら警告をテストします。

上記のいずれかの手順で不良が示されたり、予想通りの動作にならなかったりした場合は、以下の操作を行います。

  - 適切な機器を使用してワイヤーの信号をテストし、ワイヤーまたはケーブルが何らかの損傷を受けていないかチェックします。
  - 損傷を受けたか不良が示されたケーブルおよびワイヤーをすべて交換します。
  - ケーブルとワイヤーを交換したら、すべてのハードウェアの接続をもう一度確認します。*21ページドアの制御の検証*を参照してください。

- すべてのアクセススケジュール、ドア、グループ、およびユーザーが最新であることを確認します。
- ドアコントローラーが予想どおりに動作しない場合は、詳細について*68ページ、トラブルシューティング*と*65ページ保守*を参照してください。

アクセス管理

アクセス管理

ユーザーについて

AXIS Entry Managerでは、ユーザーとは、1つ以上のトークン (識別タイプ) の所有者として登録されている人を指します。各ユーザーには、アクセスコントロールシステム内のドアへのアクセスが許可される、固有のユーザープロファイルを付与する必要があります。ユーザープロファイルは、ユーザー名と、ドアへのアクセスが許可されるタイミングと方法を記載した認証情報で構成されています。詳細については、*41ページ ユーザーの作成および編集* を参照してください。

ここで言うユーザーと管理者とを混同しないようにしてください。管理者には、すべての設定に対する無制限のアクセス権があります。また、アクセスコントロールシステムの管理という観点から、本製品 (AXIS Entry Manager) のWebページでは、管理者をユーザーと呼ぶ場合もあります。詳細については、*56ページユーザー* を参照してください。

[Access Management (アクセス管理)] ページ

[Access Management (アクセス管理)] ページでは、システムのユーザー、グループ、ドア、スケジュールを設定および管理できます。[Access Management (アクセス管理)] ページを開くには、[**Access Management (アクセス管理)**] をクリックします。

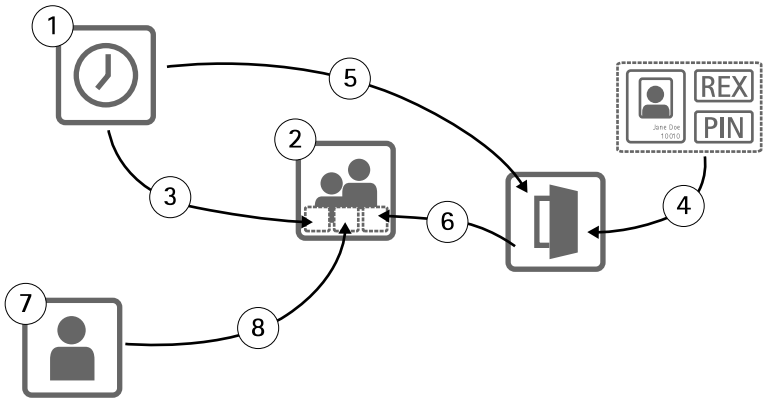
ユーザーをグループに追加して、アクセススケジュールおよびドアを適用するには、[**Groups (グループ)**] リストと [**Doors (ドア)**] リストの該当する宛先に項目をドラッグします。

注

アクションが必要なメッセージが赤色で表示されます。

ワークフローの選択

アクセス管理の構造には柔軟性があり、ニーズに合わせてワークフローを開発することができます。次にワークフローの例を示します。



1. アクススケジュールを作成します。*33ページ*を参照してください。
2. グループを作成します。*35ページ*を参照してください。
3. アクススケジュールをグループに適用します。
4. 識別タイプをドアまたはフロアに追加します。*36ページ*および*37ページ*を参照してください。
5. アクススケジュールを各識別タイプに適用します。

6. ドアまたはフロアをグループに適用します。
7. ユーザーを作成します。*41ページ*を参照してください。
8. ユーザーをグループに追加します。

このワークフローの適用例については、*44ページアクセススケジュールの組み合わせの例*を参照してください。

アクセススケジュールの作成と編集

アクセススケジュールを使用して、ドアにアクセスできるタイミングとできないタイミングの一般的なルールを定義します。また、グループがシステム内のドアにアクセスできるタイミングとできないタイミングに関するルールも定義します。詳細については、*33ページアクセススケジュールタイプ*を参照してください。

新しいアクセススケジュールを作成するには:

1. [**Access Management (アクセス管理)**] に移動します。
2. [**Access Schedules (アクセススケジュール)**] タブで [**Add new schedule (新しいスケジュールを追加する)**] をクリックします。
3. [**Add access schedule (アクセススケジュールの追加)**] ダイアログにスケジュール名を入力します。
4. 正規のアクセススケジュールを作成するには、[**Addition Schedule (追加スケジュール)**] を選択します。

   除外スケジュールを作成するには、[**Subtraction Schedule (除外スケジュール)**] を選択します。

   詳細については、*33ページアクセススケジュールタイプ*を参照してください。
5. [**Save (保存)**] をクリックします。

[**Access Schedules (アクセススケジュール)**] リストのアイテムを展開するには、 をクリックします。追加スケジュールは緑色のテキスト、除外スケジュールは濃い赤色のテキストで表示されます。

アクセススケジュールのカレンダーを表示するには、 をクリックします。

アクセススケジュールの名前またはスケジュールアイテムを編集するには、 をクリックして、変更を行います。その後、[**Save (保存)**] をクリックします。

アクセススケジュールを削除するには、 をクリックします。

注

ドアコントローラーには、サンプルとして使用したり、必要に応じて変更したりできる、定義済みでよく利用されているアクセススケジュールがいくつかあります。ただし、定義済みの [**Always (常時)**] アクセススケジュールは変更または削除できません。

アクセススケジュールタイプ

アクセススケジュールには次の2種類があります。

- **追加スケジュール** – ドアへのアクセスが可能な時刻を定義する正規のアクセススケジュールです。一般的な追加スケジュールは、営業時間、ビジネス時間、就業時間外、または夜間です。
- **除外スケジュール** – 正規のアクセススケジュールに対する例外です。一般に、このスケジュールは、正規のスケジュール (追加スケジュール) の期間内に発生する、特定の期間中のアクセスを制限するために使用されます。たとえば、除外スケジュールは、平日に発生するユーザーの建物へのアクセスを祝祭日に拒否するのに使用できます。

アクセスのスケジュールは両タイプとも、次の2つのレベルで使用できます。

- **識別タイプのスケジュール** – ドアへのユーザーアクセスをリーダーが許可するタイミングと方法を決定します。各識別タイプは、その特定の識別タイプでユーザーのアクセスをいつ許可するかをシステムに通知する、アクセススケジュールに接続する必要があります。各識別タイプには、複数の追加スケジュールと除外スケジュールを追加することができます。識別タイプについては、*37ページ*を参照してください。
- **スケジュールをグループ化** – グループのメンバーがドアへのアクセスを許可されるタイミングを決定します。方法は決定しません。各グループは、グループのメンバーにアクセスが許可されるタイミングをシステムに通知する1つまたは複数のアクセススケジュールに接続する必要があります。各グループには、複数の追加スケジュールと除外スケジュールを追加することができます。グループについては、*35ページ*を参照してください。

グループのスケジュールは、アクセス権限を制限することができますが、入退出に関するアクセス権限を識別タイプが許可する範囲を超えて拡張することはできません。つまり、識別タイプのスケジュールで特定の時刻における入退出を制限する場合、その識別タイプのスケジュールをグループのスケジュールでオーバーライドすることはできません。ただし、グループのスケジュールが識別タイプのスケジュールよりアクセスの制約が大きい場合は、グループのスケジュールで識別タイプのスケジュールがオーバーライドされます。

識別タイプスケジュールとグループスケジュールをいくつかの方法で組み合わせると、さまざまな結果を得ることができます。アクセススケジュールの組み合わせ例については、*44ページ*を参照してください。

スケジュール項目の追加

スケジュールは、追加または削除の両方の場合で、イベントを1回 (シングル) にしたり、イベントを繰り返したりできます。

アクセススケジュールにスケジュール項目を追加するには:

1. [**Access Schedules (アクセススケジュール)**] リストでアクセススケジュールを展開します。
2. [**Add schedule item (スケジュール項目の追加)**] をクリックします。
3. スケジュールの項目の名前を入力します。
4. [**One time (1回)**] または [**Recurrence (繰り返し)**] を選択します。
5. 時間のフィールドに期間を設定します。*34ページ時間のオプション*を参照してください。
6. 繰り返すスケジュールイベントの場合は、[**Recurrence pattern (繰り返しパターン)**] と[**Range of recurrence (繰り返しの範囲)**] のパラメーターを選択します。*34ページ繰り返しパターンのオプション*および*35ページ繰り返し範囲のオプション*を参照してください。
7. [**Save (保存)**] をクリックします。

時間のオプション

以下の時間のオプションがあります。

- [**All day (終日)**] – 1日24時間にわたって継続するイベントの場合に選択します。その後、[**Start (開始)**] に希望する日付を入力します。
- [**Start (開始)**] – 時間フィールドをクリックし、希望する時刻を選択します。必要な場合は、日付フィールドをクリックし、希望する月、日、および年を選択します。フィールドに日付を直接入力することもできます。
- [**End (終了)**] – 時間フィールドをクリックし、希望する時刻を選択します。必要な場合は、日付フィールドをクリックし、希望する月、日、および年を選択します。フィールドに日付を直接入力することもできます。

繰り返しパターンのオプション

以下の繰り返しパターンのオプションがあります。

- [**Yearly (毎年)**] – 毎年繰り返す場合に選択します。

- [Weekly (毎週)] – 毎週繰り返す場合に選択します。
- [Monday (月曜日)]、[Tuesday (火曜日)]、[Wednesday (水曜日)]、[Thursday (木曜日)]、[Friday (金曜日)]、[Saturday (土曜日)]、および [Sunday (日曜日)] ごとに毎週繰り返す – 繰り返す曜日を選択します。

繰り返し範囲のオプション

以下の繰り返し範囲のオプションがあります。

- [First occurenc (最初の発生)] – 日付フィールドをクリックし、希望する月、日、および年を選択します。フィールドに日付を直接入力することもできます。
- [No end date (終了日なし)] – 発生したアクションを無期限に繰り返す場合に選択します。
- [End by (終了)] – 日付フィールドをクリックし、希望する月、日、および年を選択します。フィールドに日付を直接入力することもできます。

グループの作成および編集

グループを使用すると、ユーザーとそのアクセス権をまとめて効率的に管理することができます。グループはシステムに伝える認証情報で構成されています。具体的には、グループを構成するメンバーの名前、ドアへのアクセスをグループのメンバーに許可するタイミングと方法です。

各ユーザーは、1つ以上のグループに所属する必要があります。グループにユーザーを追加するには、対象のユーザーを [Group (グループ)] リストの目的のグループにドラッグアンドドロップします。詳細については、*41ページユーザーの作成および編集*を参照してください。

新しいグループを作成するには:

1. [Access Management (アクセス管理)] に移動します。
2. [Groups (グループ)] タブで [Add new group (新しいグループを追加)] をクリックします。
3. [Add Group (グループを追加)] ダイアログで、グループの認証情報を入力します。*35ページグループの認証情報*を参照してください。
4. [Save (保存)] をクリックします。

[Groups (グループ)] リストのアイテムを展開して、メンバー、ドアへのアクセス権、スケジュールを表示するには、 をクリックします。

グループの名前または有効期間を編集するには、 をクリックして、変更を行います。その後、[Save (保存)] をクリックします。

グループが特定のドアにアクセスできるタイミングや方法を確認するには、 をクリックします。

グループやそのメンバーを削除したり、グループからドアやスケジュールを削除したりするには、 をクリックします。

グループの認証情報

以下のグループ認証情報を利用できます。

- [Name (名前)] (必須)
- [Valid from (発効日)] と [Valid to (期限終了日)] – グループ認証情報の有効期間の開始日と終了日を入力します。日付フィールドをクリックし、希望する月、日、および年を選択します。フィールドに日付を直接入力することもできます。
- [Whitelist (ホワイトリスト)] – ホワイトリストグループのユーザーは、ネットワーク障害や電源障害が発生した場合でも、グループ内のドアに常時アクセスできます。グループのユーザーはドアへの常時アク

セス権があるため、スケジュールや発行日/期限終了日は適用されません。ホワイトリストグループのユーザーがドアを開く場合は、Long access time (長いアクセス時間) はサポートされません。ホワイトリストの機能をサポートするワイヤレスロックを備えたドアのみグループに追加できます。

注

- グループを保存できるようにするには、グループの [**Name (名前)**] を入力する必要があります。
- ユーザーをホワイトリストグループに追加すると、発行日/期限終了日は適用されません。
- ホワイトリストの認証情報をワイヤレスロックに同期させるにはしばらく時間がかかり、通常のドア開放手順に干渉が発生します。ピーク時に大量の認証情報をシステムに追加したりシステムから削除したりするのは避けるようにしてください。更新した認証情報とロックの同期が終了すると、ロックのイベントログには次のように表示されます。`SyncOngoing:  false`

ドアの管理

各ドアの全般的なルールは、[**Doors (ドア)**] タブを使用して管理します。このルールには、ユーザーにドアへのアクセス権をどのように許可するかを決定する識別タイプや、各識別タイプをどのタイミングで有効にするかを決定するアクセススケジュールが追加されます。詳細については、*37ページ識別タイプ*および*33ページアクセススケジュールの作成と編集*を参照してください。

ドアを管理する前に、ハードウェア設定を完了して、アクセスコントロールシステムにドアを追加する必要があります。設定の手順については、*14ページハードウェアの設定*を参照してください。

ドアを管理するには:

1. [**Access Management (アクセス管理)**] に移動し、[**Doors (ドア)**] タブを選択します。
2. [**Doors (ドア)**] リストで、編集するドアの横にある ▶ をクリックします。
3. 少なくとも1つのグループに、ドアをドラッグします。[**Groups (グループ)**] リストが空の場合は、新しいグループを作成します。*35ページグループの作成および編集*を参照してください。
4. [**Add identification type (識別タイプを追加)**] をクリックして、ユーザーがリーダーに提示する必要がある、ドアへのアクセスが許可されるための認証情報を選択します。*37ページ識別タイプ*を参照してください。

   各ドアには、少なくとも1つの識別タイプを追加します。
5. 複数の識別タイプを追加するには、上記の手順を繰り返します。

   [**Card number only (カード番号のみ)**] と [**PIN only (PINのみ)**] の両方の識別タイプを追加すると、ユーザーは、カードをリーダーに通すか、PINを入力するいずれかの方法を選択してドアにアクセスできます。しかし、これらを追加せずに、[**Card number and PIN (カード番号およびPIN)**] の識別タイプを追加した場合は、ドアにアクセスするには、ユーザーはカードをリーダーに通してから、PINを入力する必要があります。
6. 認証情報が有効になるタイミングを決定するには、各識別タイプにスケジュールをドラッグします。

ドアを手動でロック/解除したり、一時的なアクセスを許可したりするには、必要に応じていずれかの手動ドアのアクションをクリックします。*38ページ手動のドアアクションを使用する*を参照してください。

注

ワイヤレスドア/デバイスでは、手動によるドアのロック/解除を管理したり、一時的なアクセス許可を管理したりする機能はご利用いただけません。

[**Doors (ドア)**] リストのアイテムを展開するには、▶ をクリックします。

ドアまたはリーダーの名前を編集するには、✎ をクリックして変更を行います。その後、[**Save (保存)**] をクリックします。

リーダー、識別タイプ、アクセススケジュールの組み合わせを確認するには、  をクリックします。

ドアに接続するロックの機能を確認するには、検証コントロールをクリックします。*21ページドアの制御の検証*を参照してください。

識別タイプまたはアクセススケジュールを削除するには、 をクリックします。

識別タイプ

識別タイプは、ユーザーにドアへのアクセスをどのように許可するかを決定するためのもので、ポータブルな認証ストレージデバイスや記憶された情報が使用されますが、これらをさまざまに組み合わせて使用することもあります。一般的な識別タイプには、カードやキーフォブなどのトークン、個人の識別番号 (PIN)、退出要求 (REX) 装置などが含まれます。

認証情報の詳細については、*42ページユーザー認証情報*を参照してください。

以下の識別タイプを利用できます。

- **設備コードのみ** – ユーザーはリーダーが許可するカードまたは設備コードが記載された他のトークンを使用するとドアにアクセスできます。
- **カード番号のみ** – ユーザーはリーダーが許可するカードや他のトークンを使用した場合にのみドアにアクセスできます。カード番号は、通常、カード面に印刷されている一意の番号です。カード番号の記載場所については、カードの製造業者にお問い合わせください。カード番号はシステムで取得することもできます。接続されているリーダーにカードを通し、リストからリーダーを選択して [**Retrieve (取得)**] をクリックします。
- **カード保存未加工データのみ** – ユーザーはリーダーが許可するカードや他のトークンを使用した場合にのみドアにアクセスできます。情報は未加工データとしてカードに保存されます。カードの未加工データはシステムで取得することができます。接続されているリーダーにカードを通し、リストからリーダーを選択して [**Retrieve (取得)**] をクリックします。この識別タイプは、カード番号が見つからない場合にのみ使用してください。
- **PINのみ** – ユーザーは4桁の個人の識別番号 (PIN) を使用した場合にのみ、ドアにアクセスできます。
- **設備コードとPIN** – ユーザーがドアにアクセスするには、リーダーが許可するカードまたは設備コードが記載された他のトークンと、PINの両方が必要です。ユーザーは、指定どおりに、カード、PINという順序で認証情報を提示する必要があります。
- **カード番号とPIN** – ユーザーがドアにアクセスするには、リーダーが許可するカードまたはトークンとPINの両方が必要です。ユーザーは、指定どおりに、カード、PINという順序で認証情報を提示する必要があります。
- **カード保存未加工データとPIN** – ユーザーがドアにアクセスするには、リーダーが許可するカードまたはトークンとPINの両方が必要です。この識別タイプは、カード番号が見つからない場合にのみ使用してください。ユーザーは、指定どおりに、カード、PINという順序で認証情報を提示する必要があります。
- **REX** – ユーザーは、ボタン、センサー、またはプッシュバーなどの退出要求 (REX) 装置をアクティブにするとドアにアクセスできます。
- **ナンバープレートのみ** – ユーザーは車両のナンバープレート番号を使用した場合にのみドアにアクセスできます。

スケジュールされたロック解除状態の追加

指定した期間にわたり、ドアのロック解除状態を自動的に維持するために、[**Scheduled unlock (スケジュールされたロック解除)**] 状態をドアに追加し、さらにアクセススケジュールをドアに適用することができます。

たとえば、営業時間中にドアがロック解除された状態を維持するには:

1. [**Access Management (アクセス管理)**] に移動し、[**Doors (ドア)**] タブを選択します。

2. 編集対象の [**Door (ドア)**] リストアイテムの横にある ▶ をクリックします。
3. [**Add scheduled unlock (スケジュールされたロック解除を追加)**] をクリックします。
4. [**Unlock state (ロック解除状態)**] を選択します (ドアのロックが1つか2つかによって**ロック解除**または**両方のロックを解除**します)。
5. [**OK**] をクリックします。
6. 定義済みの [**Office hours (営業時間)**] アクセススケジュールを [**Scheduled unlock (スケジュールされたロック解除)**] 状態に適用します。

ドアがロック解除された時刻を確認するには、 をクリックします。

スケジュールされたロック解除状態またはアクセススケジュールを削除するには、⊖ をクリックします。

手動のドアアクションを使用する

ドアはロックまたはロック解除することができ、また、[**Doors (ドア)**] タブの [**Manual door actions (手動のドアアクション)**] を通じて一時的なアクセス権をドアに付与することができます。特定のドアで利用できる手動のドアアクションは、ドアの設定方法によって異なります。

手動のドアアクションを使用するには:

1. [**Access Management (アクセス管理)**] に移動し、[**Doors (ドア)**] タブを選択します。
2. [**Doors (ドア)**] リストで、コントロールするドアの横にある ▶ をクリックします。
3. 目的のドアアクションをクリックします。*38ページ手動のドアアクション*を参照してください。

注

手動のドアアクションを使用するには、対象のドアが接続するドアコントローラーから [Access Management (アクセス管理)] ページを開く必要があります。別のドアコントローラーから [Access Management (アクセス管理)] ページを開くと、手動のドアアクションではなく、対象のドアが接続するドアコントローラーの概要ページへのリンクが表示されます。リンクをクリックして、[**Access Management (アクセス管理)**] に移動し、[**Doors (ドア)**] タブを選択します。

手動のドアアクション

以下の手動のドアアクションを利用できます。

- [**Get door status (ドアステータスを取得)**] – ドアモニター、ドアアラーム、およびロックの現在の状態を確認します。
- [**Access (アクセス)**] – ドアへのユーザーのアクセスを許可します。指定されたアクセス時間が適用されます。*15ページドアモニターとロックの設定方法*を参照してください。
- [**Unlock (ロック解除)**] (ロックを1つ使用) または [**Unlock both locks (両方のロックを解除)**] (ロックを2つ使用) – ドアのロックを解除します。[**Lock (ロック)**] または [**Lock both locks (両方のロックを施錠)**] のいずれかを押すか、スケジュールされたドアの状態をアクティブにする、またはドアコントローラーが再起動されるまでは、ドアはロック解除されたままになります。
- [**Lock (ロック)**] (ロックを1つ使用) または [**Lock both lock (両方のロックを施錠)**] (ロックを2つ使用) – ドアをロックします。
- [**Unlock second lock and lock primary (2つ目のロックを解除し、プライマリロックにする)**] – このオプションは、ドアに2つ目のロックが設定されている場合にのみ利用可能です。ドアをロック解除します。[**Double lock (ダブルロック)**] またはスケジュールされたドアの状態をアクティブにするまでは、セカンダリロックはロックされたままになります。

フロアの管理

AXIS 9188 Network I/O Relay Moduleをシステムにインストールしている場合は、ドアと同様の方法でフロアを管理することができます。

注

A1001をグローバルイベントを有効にしてクラスターモードで使用する場合は、フロアごとに一意のわかりやすい名前を付けていることを確認してください。たとえば、*「Elevator A, Floor 1」*のようにします。

注

それぞれのA1001 Network Door Controllerで、最大2つのAXIS 9188 Network I/O Relay Modulesを設定できます。

各フロアの全般的なルールは、[**Floors (フロア)**] タブを使用して管理します。このルールには、ユーザーにフロアへのアクセス権をどのように許可するかを決定する識別タイプや、各識別タイプをどのタイミングで有効にするかを決定するアクススケジュールが追加されます。詳細については、*40ページフロアの識別タイプ*および*33ページアクススケジュールの作成と編集*を参照してください。

フロアを管理する前に、ハードウェア設定を完了して、アクセスコントロールシステムにフロアを追加する必要があります。設定の手順については、*14ページハードウェアの設定*を参照してください。

フロアを管理するには:

1. [**Access Management (アクセス管理)**] に移動し、[**Floors (フロア)**] タブを選択します。
2. [**Floors (フロア)**] リストで、編集するフロアの横にある ▶ をクリックします。
3. 少なくとも1つのグループに、フロアをドラッグします。[**Groups (グループ)**] リストが空の場合は、新しいグループを作成します。*35ページグループの作成および編集*を参照してください。
4. [**Add identification type (識別タイプを追加)**] をクリックして、フロアへのアクセス許可を得るためにユーザーがリーダーに提示する必要がある認証情報を選択します。*40ページフロアの識別タイプ*を参照してください。

   各フロアには、少なくとも1つの識別タイプを追加します。
5. 複数の識別タイプを追加するには、上記の手順を繰り返します。

   [**Card number only (カード番号のみ)**] と [**PIN only (PINのみ)**] の両方の識別タイプを追加すると、ユーザーは、カードをリーダーに通すか、PINを入力するいずれかの方法を選択してドアにアクセスできます。しかし、これらを追加せずに、[**Card number and PIN (カード番号およびPIN)**] の識別タイプを追加した場合は、ドアにアクセスするには、ユーザーはカードをリーダーに通してから、PINを入力する必要があります。
6. 認証情報が有効になるタイミングを決定するには、各識別タイプにスケジュールをドラッグします。

フロアを手動でロック/解除したり、一時的なアクセスを許可したりするには、必要に応じていずれかの手動ドアのアクションをクリックします。*41ページ手動フロアアクションを使用する*を参照してください。

注

ワイヤレスドア/デバイスでは、手動によるフロアのロック/解除を管理したり、一時的なアクセス許可を管理したりする機能はご利用いただけません。

[**Floors (フロア)**] リストのアイテムを展開するには、▶ をクリックします。

フロアまたはリーダーの名前を編集するには、✎ をクリックして変更を行います。その後、[**Save (保存)**] をクリックします。

リーダー、識別タイプ、アクススケジュールの組み合わせを確認するには、  をクリックします。

フロアに接続するロックの機能を確認するには、検証コントロールをクリックします。*22ページフロアのコントロール検証*を参照してください。

識別タイプまたはアクセススケジュールを削除するには、 をクリックします。

フロアの識別タイプ

識別タイプは、ユーザーにフロアへのアクセスをどのように許可するかを決定するためのもので、ポータブルな認証ストレージデバイスや記憶された情報が使用されますが、これらをさまざまに組み合わせて使用することもあります。一般的な識別タイプには、カードやキーフォブなどのトークン、個人の識別番号 (PIN)、退出要求 (REX) 装置などが含まれます。

認証情報の詳細については、*42ページユーザー認証情報*を参照してください。

以下の識別タイプを利用できます。

- **設備コードのみ** – ユーザーはリーダーが許可するカードまたは設備コードが記載された他のトークンを使用するとフロアにアクセスできます。
- **カード番号のみ** – ユーザーはリーダーが許可するカードや他のトークンを使用した場合にのみフロアにアクセスできます。カード番号は、通常、カード面に印刷されている一意の番号です。カード番号の記載場所については、カードの製造業者にお問い合わせください。カード番号はシステムで取得することもできます。接続されているリーダーにカードを通し、リストからリーダーを選択して [**Retrieve (取得)**] をクリックします。
- **カード保存未加工データのみ** – ユーザーはリーダーが許可するカードや他のトークンを使用した場合にのみフロアにアクセスできます。情報は未加工データとしてカードに保存されます。カードの未加工データはシステムで取得することができます。接続されているリーダーにカードを通し、リストからリーダーを選択して [**Retrieve (取得)**] をクリックします。この識別タイプは、カード番号が見つからない場合にのみ使用してください。
- **PINのみ** – ユーザーは4桁の個人の識別番号 (PIN) を使用した場合にのみ、フロアにアクセスできます。
- **設備コードとPIN** – ユーザーがフロアにアクセスするには、リーダーが許可するカードまたは設備コードが記載された他のトークンと、PINの両方が必要です。ユーザーは、指定どおりに、カード、PINという順序で認証情報を提示する必要があります。
- **カードの番号とPIN** – ユーザーがフロアにアクセスするには、リーダーが許可するカードまたは他のトークンとPINの両方が必要です。ユーザーは、指定どおりに、カード、PINという順序で認証情報を提示する必要があります。
- **カード保存未加工データとPIN** – ユーザーがフロアにアクセスするには、リーダーが許可するカードまたは他のトークンとPINの両方が必要です。この識別タイプは、カード番号が見つからない場合にのみ使用してください。ユーザーは、指定どおりに、カード、PINという順序で認証情報を提示する必要があります。
- **REX** – ユーザーは、ボタン、センサー、またはプッシュバーなどの退出要求 (REX) 装置をアクティブにするとフロアにアクセスできます。

スケジュールされたロック解除状態の追加

指定した期間にわたり、全員がフロアにアクセス可能な状態を自動的に維持するために、[**Scheduled unlock (スケジュールされたロック解除)**] 状態をフロアに追加し、さらにアクセススケジュールをフロアに適用することができます。

たとえば、営業時間中、全員がフロアにアクセスできるようにするには:

1. [**Access Management (アクセス管理)**] に移動し、[**Floors (フロア)**] タブを選択します。
2. 編集対象の [**Floors (フロア)**] リストアイテムの横にある をクリックします。
3. [**Add scheduled unlock (スケジュールされたロック解除を追加)**] をクリックします。

4. [**Unlock state (ロック解除状態)**] を選択します (フロアのロックが1つか2つかによって**ロック解除**または**両方のロックを解除**します)。
5. [**OK**] をクリックします。
6. 定義済みの [**Office hours (営業時間)**] アクセススケジュールを [**Scheduled unlock (スケジュールされたロック解除)**] 状態に適用します。

フロアにアクセスできるタイミングを確認するには、 をクリックします。

スケジュールされたロック解除状態またはアクセススケジュールを削除するには、 をクリックします。

手動フロアアクションを使用する

フロアには、制限付きのアクセスや、全員がアクセス可能など、さまざまな種類のアクセスを設定することがができます。一時的なアクセスは、[**Floor (フロア)**] タブの [**Manual floor actions (手動フロアアクション)**] で許可できます。特定のフロアで利用できる手動フロアアクションは、フロアの設定方法によって異なります。

手動フロアアクションを使用するには:

1. [**Access Management (アクセス管理)**] に移動し、[**Floors (フロア)**] タブを選択します。
2. [**Floors (フロア)**] リストで、コントロールするフロアの横にある をクリックします。
3. 目的のフロアアクションをクリックします。*41ページ手動によるフロアアクション*を参照してください。

注

手動フロアアクションを使用するには、対象のドアが接続するフロアコントローラーから [Access Management (アクセス管理)] ページを開く必要があります。別のフロアコントローラーから [Access Management (アクセス管理)] ページを開くと、手動フロアアクションではなく、対象のフロアが接続するフロアコントローラーの概要ページへのリンクが表示されます。リンクをクリックして、[**Access Management (アクセス管理)**] に移動し、[**Floors (フロア)**] タブを選択します。

手動によるフロアアクション

以下の手動によるフロアアクションを利用できます。

- [**Get floor status (フロアステータスを取得)**] – フロアに接続しているリレーの現在の状態を確認します。
- [**Access (アクセス)**] – フロアへのユーザーのアクセスを許可します。指定されたアクセス時間が適用されます。*15ページドアモニターとロックの設定方法*を参照してください。
- [**Unlock (ロック解除)**] – [**Lock (ロック)**] を押すか、スケジュールされたフロアの状態をアクティブにする、またはドアコントローラーが再起動されるまでは、全員がフロアにアクセスできます。
- [**Lock (ロック)**] – [**Unlock (ロック解除)**] を押すか、スケジュールされたフロアの状態をアクティブにする、またはドアコントローラーが再起動されるまでは、全員がフロアにアクセスできません。

ユーザーの作成および編集

各ユーザーには、アクセスコントロールシステム内のドアへのアクセスが許可される、固有のユーザープロファイルを付与する必要があります。ユーザープロファイルは、ユーザー名と、ドアへのアクセスが許可されるタイミングと方法を記載した認証情報で構成されています。

ユーザーのアクセス権を効率的に管理できるようにするために、各ユーザーは1つまたは複数のグループに所属する必要があります。詳細については、*グループの作成および編集*を参照してください。

新しいユーザープロファイルを作成するには:

1. [**Access Management (アクセス管理)**] に移動します。

2. [**Users (ユーザー)**] タブを選択し、[**Add new user (新しいユーザーの追加)**] をクリックします。
3. [**Add User (ユーザーの追加)**] ダイアログで、ユーザーの認証情報を入力します。*42ページユーザー認証情報*を参照してください。
4. [**Save (保存)**] をクリックします。
5. [**Groups (グループ)**] リストの1つまたは複数のグループにユーザーをドラッグします。[**Groups (グループ)**] リストが空の場合は、新しいグループを作成します。*35ページグループの作成および編集*を参照してください。

[**Users (ユーザー)**] リストのアイテムを展開してユーザーの認証情報を表示するには、 をクリックします。

特定のユーザーを検索するには、[filter users (ユーザーの並び替え)] フィールドにフィルターを入力します。完全一致を検索するには、"John"、または "ポッター、バージニア" のように、フィルターテキストを二重引用符で囲みます。

ユーザーの認証情報を編集するには、 をクリックし、必要に応じて認証情報を変更します。その後、[**Save (保存)**] をクリックします。

ユーザーを削除するには、 をクリックします。

重要

AXIS Visitor Managerによって作成されたユーザーを、AXIS Entry Managerで編集または削除しないでください。AXIS Visitor ManagerとQRコードリーダーサービスの詳細については、*24ページAXIS Visitor Access*を参照してください。

ユーザー認証情報

以下のユーザー認証情報を利用できます。

- **名** (必須)
- **姓**
- **発効日**と**期限終了日** – ユーザー認証情報の有効期間の開始日と終了日を入力します。日付フィールドをクリックし、希望する月、日、および年を選択します。フィールドに日付を直接入力することもできます。
- **認証情報を停止** – 選択すると認証情報が停止されます。停止すると、ユーザーはシステム内のドアにこの認証情報ではアクセスできなくなります。選択解除すると、ユーザーに再びアクセス権が付与されます。停止は一時的な使用が目的です。ユーザーのアクセスを永続的に拒否する場合は、ユーザープロファイルを削除する方が得策です。
- **PIN** (カード番号またはカード保存未加工データがない場合に必須) – 選択済みまたはユーザーに割り当てられている4桁の個人の識別番号 (PIN) を入力します。
- **設備コード** – 設備のアクセスコントロールシステムを確認するためのコードを入力します。このフィールドに入力するプリセット設備コードが自動入力されている場合については、*24ページプリセット設備コード*を参照してください。
- **カード番号** (PINまたはカード保存未加工データがない場合に必須) – カード番号を入力します。カード番号の記載場所については、カードの製造業者にお問い合わせください。カード番号はシステムで取得することもできます。接続されているリーダーにカードを通し、リストからリーダーを選択して [**Retrieve (取得)**] をクリックします。
- **カード保存未加工データ** (PINまたはカード番号がない場合に必須) – カード保存未加工データを入力します。このデータはシステムで取得することができます。接続されているリーダーにカードを通し、リストからリーダーを選択して [**Retrieve (取得)**] をクリックします。この識別タイプは、カード番号が見つからない場合にのみ使用してください。
- **長いアクセス時間**– 選択すると既存のアクセス時間がオーバーライドされ、ユーザーにドアを開放するアクセス時間を長くできます。*16ページドアモニターと時間のオプションについて*を参照してください。

- **ナンバープレート** (デフォルトで設置されたドアコントローラーではこの認証情報は利用できません) – パートナー製ソフトウェアでこの認証情報がアクティブ化されている場合、ユーザー車両のナンバープレート番号を入力します。
  この認証情報は、Axisパートナー製ソフトウェアと、ナンバープレート認識ソフトウェアを搭載したカメラとを組み合わせて使用した場合にのみ使用できます。詳細については、Axisパートナーまたはお近くのAxisのセールス担当者にお問い合わせください。

注

[**Retrieve (取得)**] ボタンは、ハードウェア設定が完了済みで、1つ以上のリーダーがコントローラーに接続されている場合にのみ利用できます。

ユーザーのインポート

テキストファイルをカンマ区切りの値 (CSV) 形式でインポートすることにより、ユーザーをシステムに追加できます。多数のユーザーを同時に追加する必要がある場合は、ユーザーをインポートすることをお勧めします。

ユーザーをインポートするには、事前に、ファイルを適切なCSV形式で (*.csvまたは*.txt) 作成および保存する必要があります。値はスペースなしのカンマで区切り、ユーザーごとに改行します。

例:

```
jane,doe,1234,12345678,abc123
john,doe,5435,87654321,cde321
```

ユーザーをインポートするには:

1. [**Setup > Import Users (設定 > ユーザーをインポート)**] に移動します。
2. ユーザーのリストを保存するための*.csvまたは*.txtファイルを見つけて選択します。
3. 列ごとに正しい認証情報のオプションを選択します。
4. ユーザーをシステムにインポートするには、[**Import users (ユーザーをインポート)**] をクリックします。
5. 各列に含まれている認証情報のタイプが正しいことを確認します。
6. 列の情報が正しい場合は、[**Start importing users (ユーザーのインポートを開始)**] をクリックします。列の情報が正しくない場合は、[**Cancel (キャンセル)**] をクリックしてやり直します。
7. インポートの完了後、[**OK**] をクリックします。

以下の認証情報のオプションを利用できます。

- [**First name (名)**]
- [**Last name (姓)**]
- [**PIN code (PINコード)**]
- [**Card number (カード番号)**]
- [**License plate (ナンバープレート)**]
- [**Unassigned (未割り当て)**] – 値はインポートされません。特定の列をスキップするには、このオプションを選択します。

認証情報の詳細については、*ユーザーの作成および編集*を参照してください。

ユーザーのエクスポート

[Export (エクスポート)] ページには、システム内のすべてのユーザーが、カンマ区切りの値 (CSV) リストで表示されます。このリストを使用してユーザーを他のシステムにインポートすることができます。

ユーザーリストをエクスポートするには:

1. プレーンテキストエディターを開き、新しいドキュメントを作成します。
2. [**Setup > Export Users (設定 > ユーザーをエクスポート)**] に移動します。
3. ページ上のすべての値を選択し、これをコピーします。
4. 値をテキスト文書に貼り付けます。
5. この文書をカンマ区切りの値ファイル (* csv) またはテキストファイル (*.txt) として保存します。

アクセススケジュールの組み合わせの例

識別タイプスケジュールとグループスケジュールをいくつかの方法で組み合わせると、さまざまな結果を得ることができます。以下に、*32ページ*で説明したワークフローに従った例を示します。

例:
以下を行う目的で、スケジュールの組み合わせを作成するには

- 警備員にドアへの常時アクセス権を付与する
  - デイシフト時間中 (月～金、午前6時から午後4まで) に警備員のカードを使用する。または、
  - デイシフト時間の前後に警備員のカードとPINを使用する。さらに、
- デイシフト担当者に同じドアへのアクセス権を付与する
  - デイシフト時間中にのみ、この担当者のカードを使用する

1. **デイシフト時間**という名前の [**Addition schedule (追加スケジュール)**] を作成します。*33ページ*を参照してください。
2. 午前6時から午後4時まで繰り返すデイシフト時間 [**Schedule item (スケジュール項目)**] を作成します。
3. 2つのグループを作成します。1つ目の**グループ**は**警備員**という名前にし、2つ目の**グループ**は**デイシフト担当者**という名前にします。*35ページ*を参照してください。
4. 定義済みの [**Always (常時)**] アクセス スケジュールを**警備員**グループにドラッグします。
5. **デイシフト時間**アクセス スケジュールを**デイシフトの担当者**グループにドラッグします。
6. [**Card number and PIN (カード番号およびPIN)**] 識別タイプと [**Card number only (カード番号のみ)**] 識別タイプをドアのリーダーに追加します。
7. 定義済みの [**Always (常時)**] アクセススケジュールを [**Card number and PIN (カード番号およびPIN)**] 識別タイプにドラッグします。
8. アクセススケジュールの**デイシフト時間**を [**Card number only (カード番号のみ)**] 識別タイプにドラッグします。
9. ドアを両方のグループにドラッグします。その後、必要に応じてグループにユーザーを追加します。*41ページ*を参照してください。

例:
以下を行う目的で、スケジュールの組み合わせを作成するには

- 警備員にドアへの常時アクセス権を付与する
  - デイシフト時間中 (月～金、午前6時から午後4まで) に警備員のカードを使用する。または、
  - デイシフト時間の前後に警備員のカードとPINを使用する。さらに、
- 毎日午前6時から午後4時まで、デイシフト担当者に同じドアへのアクセス権を付与する,
  - デイシフト時間中にこの担当者のカードを使用する、または

- 夜間や週末中に、この担当者のカードとPINを次のように使用する

1. **デイシフト時間**という名前の [**Addition schedule (追加スケジュール)**] を作成します。*33ページ*を参照してください。
2. 午前6時から午後4時まで繰り返すデイシフト時間 [**Schedule item (スケジュール項目)**] を作成します。
3. **夜間および週末**という名前の [**Subtraction schedule (除外スケジュール)**] を作成します。
4. 日曜日から土曜日の午後4時から午前6時まで繰り返す、夜間と週末の [**Schedule item (スケジュール項目)**] を作成します。
5. 定義済みの [**Always (常時)**]スケジュールと、アクセススケジュールの**夜間および週末**を、**デイシフト担当者**グループにドラッグします。
6. 2つのグループを作成します。1つ目の**グループ**は**警備員**という名前にし、2つ目の**グループ**は**デイシフト担当者**という名前にします。*35ページ*を参照してください。
7. 定義済みの [**Always (常時)**] アクセススケジュールを**警備員**グループおよび**デイシフト担当者**グループにドラッグします。
8. アクセススケジュールの**夜間および週末**を**デイシフト担当者**グループにドラッグします。
9. [**Card number and PIN (カード番号およびPIN)**] 識別タイプと [**Card number only (カード番号のみ)**] 識別タイプをドアのリーダーに追加します。
10. 定義済みの [**Always (常時)**] アクセススケジュールを [**Card number and PIN (カード番号およびPIN)**] 識別タイプにドラッグします。
11. アクセススケジュールの**デイシフト時間**を [**Card number only (カード番号のみ)**] 識別タイプにドラッグします。
12. ドアを両方のグループにドラッグします。その後、必要に応じてグループにユーザーを追加します。*41ページ*を参照してください。

アラームとイベントの設定

ユーザーによるカードの読み取りやREX装置のアクティブ化など、システムでイベントが発生すると、イベントログにイベントが記録されます。ログに記録されたイベントは、アラームをトリガーするように設定することができ、また、このようなアラームはアラームログに記録されます。

- イベントログを表示します。*46ページ*を参照してください。
- イベントログをエクスポートします。*46ページ*を参照してください。
- アラームログを表示します。*47ページ*を参照してください。
- イベントとアラームのログを設定します。*47ページ*を参照してください。

メール通知などのアクションをトリガーするためのアラームを設定することもできます。詳細については、*48ページアクションルールの設定方法*を参照してください。

イベントログの表示

記録されたイベントを表示するには、[**Event Log (イベントログ)**] に移動します。

グローバルイベントが有効になっていると、システム内のあらゆるドアコントローラーからイベントログを開くことができます。グローバルイベントの詳細については、*47ページイベントとアラームのログ設定*を参照してください。

イベントログのアイテムを展開して、イベントの詳細を表示するには、 をクリックします。

イベントログにフィルターを適用すると、特定のイベントを検索しやすくなります。リストにフィルターを適用するには、1つまたは複数のイベントログフィルターを選択して、[**Apply filters (フィルターを適用)**] をクリックします。詳細については、*46ページイベントログのフィルター*を参照してください。

管理者として、いくつかのイベントが他よりも重要になる場合があります。したがって、記録すべきイベントや対象となるコントローラーを選択することができます。詳細については、*47ページイベントログのオプション*を参照してください。

イベントログのフィルター

以下のフィルターから1つまたはいくつかを選択すると、イベントログの範囲を絞り込むことができます。

- User (ユーザー) – 選択したユーザーに関連するイベントでフィルター処理します。
- Door & floor (ドア&フロア) – 特定のドアまたはフロアに関連するイベントでフィルター処理します。
- Topic (トピック) – イベントタイプでフィルター処理します。
- Source (ソース) – 選択したコントローラーからのイベントでフィルター処理します。このフィルターはグローバルイベントが有効に設定されているコントローラークラスターでのみ使用できます。
- Date and time (日付と時刻) – イベントログを日付と時刻の範囲でフィルター処理します。

イベントログのエクスポート

記録されたイベントをエクスポートするには、[**Event Log (イベントログ)**] に移動します。

1. をクリックします。
2. ポップアップメニューからエクスポート形式を選択して、エクスポートを開始します。

注

CSV形式はすべてのブラウザーでサポートされており、XLSX形式はChrome™とInternet Explorer®でサポートされています。

注

エクスポートが完了すると、エクスポートボタンが  から  に変化します。別のエクスポートを開始するには、Webページを更新してください。エクスポートボタンが再び  になります。

アラームログの表示

トリガーされたアラームを表示するには、[**Alarm Log (アラームログ)**] に移動します。グローバルイベントが有効になっていると、システム内のあらゆるドアコントローラーからアラームログを開くことができます。グローバルイベントの詳細については、*47ページイベントとアラームのログ設定*を参照してください。

アラームログのアイテムを展開して、ドアの識別や状態などアラームの詳細を表示するには、  をクリックします。

アラームの原因を確認した後でリストからアラームを削除するには、[**Acknowledge (承認)**] をクリックします。すべてのアラームを削除するには、[**Acknowledge all alarms (すべてのアラームを承認)**] をクリックします。

管理者として、アラームをトリガーするためのイベントがいくつか必要な場合があります。したがって、アラームをトリガーするイベントや対象となるコントローラーを選択することができます。詳細については、*48ページアラームログのオプション*を参照してください。

イベントとアラームのログ設定

[Configure Event and Alarm Logs (イベントとアラームのログ設定)] ページでは、どのイベントを記録して、アラームをトリガーするかを定義することができます。

接続するすべてのコントローラー間でイベントとアラームを共有するには、[**Global events (グローバルイベント)**] を選択します。グローバルイベントが有効になっている場合、[Event Log (イベントログ)] 1ページと [Alarm Log (アラームログ)] 1ページを開くだけで、システムにあるすべてのドアコントローラーのイベントとアラームが同時に管理されます。グローバルイベントは、デフォルトで有効に設定されています。

グローバルイベントを無効にすると、[Event Log (イベントログ)] 1ページと [Alarm Log (アラームログ)] 1ページをドアコントローラーごとに開く必要があり、そのイベントとアラームを個別に管理する必要があります。

重要

グローバルイベントを有効または無効に設定するたびに、イベントログはクリアされます。つまり、クリアされた時点より前のすべてのイベントは削除され、イベントログが再開されます。

メール通知などのアクションをトリガーするためのアラームを設定することもできます。詳細については、*48ページアクションルールの設定方法*を参照してください。

イベントログのオプション

イベントログに含めるイベントを定義するには、[**Setup > Configure Event and Alarm Logs (設定 > イベントとアラームのログ設定)**] に移動します。

イベントのログ作成には次のオプションが利用できます。

- [**No logging (ログ作成なし)**] – イベントのログ作成を無効にします。イベントは、イベントログに登録されることも、ログが作成されることもありません。
- [**Log for all sources (すべてのソースでログを作成)**] – すべてのドアコントローラーのイベントのログ作成が有効になります。すべてのコントローラーについてイベントがイベントログに登録され、ログが作成されます。

- [Log for selected sources (選択済みのソースでログを作成)] – 選択したドアコントローラーのイベントのログ作成が有効になります。選択したすべてのコントローラーについてイベントがイベントログに登録され、ログが作成されます。イベントを、アラームログのオプション [No alarms (アラームなし)] または [Log alarm for selected controllers (選択済みのドアコントローラーでアラームのログを作成)] のいずれかと組み合わせる場合にこのオプションを選択します。

  [Configure event logging (イベントのログ作成の設定)] リストで、有効にするイベントログの項目で [Select controllers (コントローラーを選択)] を選択します。[Device Specific Event Logging (デバイス別のイベントのログ作成)] ダイアログが開きます。[Log event (イベントのログ作成)] でアラームのログ作成を有効にするコントローラーを選択し、[Save (保存)] をクリックします。

アラームログのオプション

どのイベントでアラームをトリガーするかを定義するには、[Setup > Configure Event and Alarm Logs (設定 > イベントとアラームのログ設定)] に移動します。

アラームのトリガーやログ作成に利用できるオプションは次のとおりです。

- [No alarms (アラームなし)] – アラームのログ作成を無効にします。イベントはアラームをトリガーせず、アラームログに記録されることもありません。
- [Log alarm for all sources (すべてのソースでアラームのログを作成)] – すべてのドアコントローラーでアラームのログ作成を有効にします。イベントはアラームをトリガーし、アラームログに記録されます。
- [Log alarm for selected sources (選択済みのソースでアラームのログを作成)] – 選択済みのドアコントローラーでアラームのログ作成を有効にします。イベントはアラームをトリガーし、アラームログに記録されます。

  [Configure alarm logging (アラームのログ作成の設定)] リストで、有効にするアラームログの項目で [Select sources (ソースを選択)] をクリックします。[Device Specific Alarm Triggering (デバイス別のアラームトリガー)] ダイアログが開きます。[Trigger alarm (アラームをトリガー)] でアラームのログ作成を有効にするドアコントローラーを選択し、[Save (保存)] をクリックします。

アクションルールの設定方法

イベントページでは、さまざまなイベントが発生したときに本製品がアクションを実行するように設定できます。たとえば、アラームがトリガーされたとき、メール通知を送信したり、出力ポートを有効にしたりできます。いつどのようにアクションをトリガーするかを定義した一連の条件をアクションルールと呼びます。複数の条件が定義されている場合、すべての条件が満たされたときにアクションがトリガーされます。

利用可能なトリガーやアクションの詳細については、*49ページトリガー*と*52ページアクション*を参照してください。

この例では、アラームがトリガーされたときに、電子メール通知を送信するアクションルールを設定する方法を示します。

1. アラームを設定します。*47ページイベントとアラームのログ設定*を参照してください。
2. [Setup > Additional Controller Configuration > Events > Action Rules (設定 > 追加のコントローラー設定 > イベント > アクションルール)] に移動し、[Add (追加)] をクリックします。
3. [**ルールを有効にする**] を選択し、ルールの内容がわかりやすい名前を入力します。
4. [**トリガー**] ドロップダウンリストから [**イベントロガー**] を選択します。
5. 必要に応じて、[**スケジュール**] と [**追加条件**] を選択します。以下を参照してください。
6. [Actions (アクション)] の [Type (タイプ)] ドロップダウンリストから [Send Notification (通知の送信)] を選択します。
7. 電子メールの送信先をドロップダウンリストから選択します。*52ページ送信先を追加する方法*を参照してください。

アラームとイベントの設定

この例では、ドアがこじ開けられたときに、出力ポートを有効にするアクションルールを設定する方法を示します。

1. [Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (設定 > 追加のコントローラー設定 > システムオプション > ポートとデバイス > I/Oポート)] に移動します。
2. 目的の [**I/Oポートタイプ**] ドロップダウンリストから [**出力**] を選択し、[**名前**] を入力します。
3. I/Oポートの [**標準状態**] を選択し、[**保存**] をクリックします。
4. [Events > Action Rules (イベント > アクションルール)] に移動し、[Add (追加)] をクリックします。
5. [**トリガー**] ドロップダウンリストから [**ドア**] を選択します。
6. ドロップダウンリストから [**ドアアラーム**] を選択します。
7. ドロップダウンリストから希望するドアアラームを選択します。
8. ドロップダウンリストから [**ドアのこじ開け**] を選択します。
9. 必要に応じて、[**スケジュール**] と [**追加条件**] を選択します。以下を参照してください。
10. [**アクション**] の [**タイプ**] ドロップダウンリストから [**出力ポート**] を選択します。
11. [**ポート**] ドロップダウンリストから目的の出力ポートを選択します。
12. 状態を [**アクティブ**] に設定します。
13. アクションの [**継続時間**] を入力し、[**指定時間経過後に反対の状態に移行**] を選択します。ここで、アクションの継続時間を入力します。
14. [OK] をクリックします。

アクションルールで複数のトリガーを使用するには、[**追加の条件**] を選択し、[**追加**] をクリックして、トリガーを追加します。追加の条件を使用している場合、すべての条件が満たされたときにアクションがトリガーされます。

アクションが繰り返しトリガーされるのを防ぐには、[**最小待ち時間**] を設定します。アクションが再びアクティブになるまでトリガーを無視する時間を時間、分、秒の形式で入力します。

詳細については、本製品に内蔵されているヘルプを参照してください。

トリガー

アクションルールでは、以下の**トリガー**と**条件**を使用できます。

- Access Point (アクセスポイント)
  - Access Point Enabled (アクセスポイント有効) – ハードウェア設定の完了や識別タイプの追加など、リーダーやREX装置などのアクセスポイント装置が設定されたときにアクションルールをトリガーします。
- Configuration (設定)
  - Access Point Changed (アクセスポイント変更) – ハードウェアの設定や識別タイプの編集、ドアのアクセス方法の変更など、リーダーやREX装置などのアクセスポイント装置の設定が変更されたときにアクションルールをトリガーします。
  - Access Point Removed (アクセスポイント削除) – リーダーやREX装置などのアクセスポイント装置のハードウェア設定がリセットされたときにアクションルールをトリガーします。
  - **エリア変更**– 本バージョンのAXIS Entry Managerではサポートしていません。アクセス管理システムなどのクライアントが、本機能をサポートし、必要な信号を発信するVAPIX®アプリケーションプログラミングインターフェースを使用して設定する必要があります。アクセスエリアが変更されたときに、アクションルールがトリガーされます。

- **エリア削除**– 本バージョンのAXIS Entry Managerではサポートしていません。アクセス管理システムなどのクライアントが、本機能をサポートし、必要な信号を発信するVAPIX®アプリケーションプログラミングインターフェースを使用して設定する必要があります。システムからアクセスエリアが削除されたときに、アクションルールをトリガーします。
- **Door Changed (ドアの変更)** - ドアの名前が変更されたときやシステムにドアが追加されたときなど、ドアの設定が変更されたときに、アクションルールをトリガーします。ドアのインストールや設定がおこなわれたときに通知を送信するなどの用途に使用できます。
- **Door Removed (ドアの削除)** — ドアがシステムから削除されたときに、アクションルールをトリガーします。ドアがシステムから削除されたときに通知を送信するなどの用途に使用できます。

- **Door (ドア)**
  - **Battery Alarm (バッテリーアラーム)** - ワイヤレスドアのバッテリー残量が少ないときやバッテリー切れが生じたときに、アクションルールをトリガーします。
  - **Door Alarm (ドアアラーム)** - ドアモニターがドアのこじ開け、長時間の開放、またはドアの何らかの不具合を検知したときに、アクションルールをトリガーします。ドアがこじ開けられた場合に通知を送信するなどの用途に使用できます。
  - **Door Double-Lock Monitor (ドアのダブルロックモニター)** - 2つ目の錠の状態がロックまたはロック解除のどちらかに変化したときにのみ、アクションルールをトリガーします。
  - **Door Lock Monitor (ドアのロックモニター)** — 通常の錠の状態がロックまたはロック解除のどちらかに変化したときに、アクションルールをトリガーします。たとえば、ドアがロックされているにも関わらず、ドアが開いたことをドアモニターが検知すると、故障がトリガーされます。
  - **Door Mode (ドアモード)** - ドアが使用またはブロックされているとき、あるいは閉鎖モードにあるときなど、ドアの状態が変化したときに、アクションルールをトリガーします。これらのモードの詳細については、オンラインヘルプを参照してください。
  - **Door Monitor (ドアモニター)** - ドアモニターの状態が変化したときに、アクションルールをトリガーします。ドアモニターでドアの開閉が表示された場合に通知を送信するなどの用途に使用できます。
  - **Door Tamper (ドアへのいたずら)** - ドアモニターへのケーブルが切断された場合など、接続が中断されたことをドアモニターが検知したときに、アクションルールをトリガーします。このトリガーを使用するには、[**Enable supervised inputs (監視入力を有効にする)**] が選択され、該当のドアコネクタの入力ポートに終端抵抗器が設置されていることを確認してください。詳細については、*18ページ監視入力の使用方法* を参照してください。
  - **Door Warning (ドア警告)** - 長時間のドア開放アラームが消える前に、アクションルールをトリガーします。たとえば、一定の時間内にドアが閉じられない場合に、本番アラーム、すなわち長時間ドア開放アラームがドアコントローラーによって送信されることを警告する信号を送信する場合などに使用できます。長時間ドア開放アラームの詳細については、*15ページドアモニターとロックの設定方法* を参照してください。
  - **Lock Jammed (ロックの故障)** - ワイヤレスドアロックが物理的に動作しなくなったときに、アクションルールをトリガーします。

- **イベントロガー** — ユーザーがカードを通したり、ドアを開けたりしたときなど、ドアコントローラーに発生したイベントをすべて追跡します。[**Global events (グローバルイベント)**]が有効である場合、イベントロガーはシステムの各コントローラーに発生したイベントをすべて追跡します。アクションルールをトリガーするアラームとイベントを設定するには、[**Setup > Configure Event and Alarm Logs (設定 > イベントとアラームのログ設定)**] に移動します。イベントロガーはシステムに共有され、30,000イベントまで保存できます。イベント数が上限に達すると、イベントロガーは先入れ先出し (FIFO) ルールを使用します。つまり、最初のイベントが最初に上書きされます。
  - **Alarm (アラーム)** – 指定されたアラームの1つがトリガーされたときに、アクションルールをトリガーします。システム管理者は他のイベントより重要なイベントを設定し、特定のイベントがアラームをトリガーするかどうかを選択できます。

- Dropped Alarms (アラーム欠落) - 新しいアラーム記録をアラームログに書き込むことができないときに、アクションルールをトリガーします。たとえば、同時に非常に多くのアラームが発生して、イベントロガーが記録できない場合などです。アラームの記録が欠落したとき、オペレーターに通知を送信できます。
- Dropped Events (イベント欠落) - 新しいイベント記録をイベントログに書き込むことができないときに、アクションルールをトリガーします。たとえば、同時に非常に多くのイベントが発生して、イベントロガーが記録できない場合などです。イベントの記録が欠落したとき、オペレーターに通知を送信できます。

• Hardware (ハードウェア)

- Network (ネットワーク) – ネットワーク接続が失われたときに、アクションルールをトリガーします。[Yes (はい)] を選択すると、ネットワーク接続が失われたときに、アクションルールをトリガーします。[No (いいえ)] を選択すると、ネットワーク接続が回復したときに、アクションルールをトリガーします。[IPv4/v6 address removed (IPv4/v6 アドレスが削除された)] または [New IPv4/v6 address (新しいIPv4/v6 アドレス)] を選択すると、IPアドレスが変更されたときに、アクションルールをトリガーします。
- Peer Connection (ピア接続) – 本製品と別のドアコントローラーとの接続が確立されたとき、装置間のネットワーク接続が失われたとき、またはドアコントローラーのペアリングが失敗したときに、アクションルールをトリガーします。ドアコントローラーのネットワーク接続が失われたことを通知するなどの用途に使用できます。

• Input Signal (入力信号)

- Digital Input Port (デジタル入力ポート) – I/Oポートが接続されているデバイスから信号を受信したとき、アクションルールをトリガーします。*64ページI/O ポート*を参照してください。
- Manual Trigger (手動トリガー) – 手動トリガーがアクティブになったときに、アクションルールをトリガーします。アクセス管理システムなどのクライアントが、VAPIX®アプリケーションプログラミングインターフェースを通じて使用し、アクションルールを手動で開始、または停止することができます。
- Virtual Inputs (仮想入力) – いずれかの仮想入力の状態が変化したときに、アクションルールをトリガーします。アクセス管理システムなどのクライアントが、VAPIX®アプリケーションプログラミングインターフェースを通じて使用し、アクションをトリガーすることができます。管理システムのユーザーインターフェースのボタンなどに仮想入力を接続できます。

• Schedule (スケジュール)

- Interval (インターバル) – スケジュールの開始時間にアクションルールをトリガーして、スケジュールの終了時間になるまでアクティブの状態を継続します。
- Pulse (パルス) – 単発イベントが発生したときに、アクションルールをトリガーします。つまり、特定の時間に発生し、継続しないイベントです。

• System (システム)

- System Ready (システムの準備完了) – システムが準備完了状態になったときに、アクションルールをトリガーします。本製品がシステムの状態を検知して、システムが起動すると管理者に通知を送信するなどの用途に使用できます。

  [Yes (はい)] を選択した場合、本製品が準備完了状態になると、アクションルールがトリガーされます。このルールは、イベントシステムなど、必要なすべてのサービスが開始されている場合にしかトリガーされませんので、ご注意ください。

• Time (時刻)

- Recurrence (繰り返し) - 作成した繰り返し動作をモニタリングすることによって、アクションルールをトリガーします。このトリガーを使用して、1時間ごとに通知を送信するなどの繰り返しアクションを開始できます。繰り返しのパターンを選択するか、新たなパターンを作成します。繰り返しパターンの設定に関する詳細については、*53ページ繰り返しの設定方法*を参照してください。

- Use Schedule (スケジュール使用) – 選択したスケジュールに従って、アクションルールをトリガーします。*53ページスケジュールを作成する方法*を参照してください。

アクション

いくつかのアクションを設定できます。

- [Output Port (出力ポート)] - 外部デバイスを制御するI/Oポートを有効にします。
- [Send Notification (通知を送信する)] - 送信先に通知メッセージを送ります。
- [Status Led (ステータスLED)] – ステータスLEDは、アクションルールの継続期間中、または設定した秒数の間、点滅するように設定できます。たとえば、設置、設定中にドアの長時間開放などのトリガー設定が適切に動作するかを視覚的に検証するために使用できます。ステータスLEDの点滅色を設定するには、[LED Color (LEDの色)] ドロップダウンリストから選択します。

送信先を追加する方法

本製品は、イベントやアラームメッセージを送信することができます。本製品が通知メッセージを送信するには、少なくとも1件以上の送信先を定義する必要があります。利用可能なオプションについては、*52ページ送信先のタイプ*を参照してください。

送信先を追加するには :

1. [Setup > Additional Controller Configuration > Events > Recipients (設定 > 追加のコントローラー設定 > イベント > 送信先)] に移動し、[Add (追加)] をクリックします。
2. わかりやすい名前を入力します。
3. 送信先の [Type (タイプ)] を選択します。
4. 送信先のタイプに必要な情報を入力します。
5. [Test (テスト)] をクリックして、送信先への接続をテストします。
6. [OK] をクリックします。

送信先のタイプ

以下の送信先のタイプを利用できます。

HTTP

HTTPS

電子メール

TCP

電子メールの送信先を設定する方法

電子メールの送信先は、電子メールプロバイダーのリストから選択したり、企業の電子メールサーバーなどのSMTPサーバー、ポート、認証方法を指定して設定することができます。

注

一部の電子メールプロバイダーは、大量の添付ファイルの受信や表示を防止したり、スケジュールにしたがって送信された電子メールなどの受信を防止するセキュリティフィルターを備えています。電子メールプロバイダーのセキュリティポリシーを確認して、メールの送信の問題が発生したり、電子メールアカウントがロックされたりしないようにしてください。

プロバイダーのリストからメール送信先を設定します。

1. [Events > Recipients (イベント > 送信先)] に移動し、[Add (追加)] をクリックします。
2. [**名前**] を入力して、[**タイプ**] リストから [**電子メール**] を選択します。
3. メールの送信先のアドレスを [**送信先**] フィールドに入力します。複数のアドレスを指定する場合は、カンマで区切ります。
4. [**プロバイダー**] リストから電子メールプロバイダーを選択します。
5. 電子メールアカウントのユーザーIDとパスワードを入力します。
6. [**テスト**] をクリックして、テストメールを送信します。

たとえば、企業メールサーバーを使用しているメール送信先を設定するには、上記の手順で、[**プロバイダー**] ではなく [**ユーザー定義**] を選択します。送信元として表示するメールアドレスを、[**送信元**] フィールドに入力します。[**詳細設定**] を選択し、SMTPサーバーのアドレス、ポート、認証方法を指定します。必要に応じて、[**暗号の使用**] を選択し、暗号化された接続を使用してメールを送信します。サーバー証明書の検証には、本製品で利用できる証明書を使用できます。証明書をアップロードする方法については、*57ページ証明書*を参照してください。

スケジュールを作成する方法

スケジュールはアクションルールのトリガーとして、または追加条件として使用できます。既定のスケジュールのどれかを使用するか、または以下のように新しいスケジュールを作成します。

新しいスケジュールを作成するには:

1. [Setup > Additional Controller Configuration > Events > Schedules (設定 > 追加のコントローラー設定 > イベント > スケジュール)] に移動し、[Add (追加)] をクリックします。
2. 分かりやすい名前をつけ、日、週、月、または年のスケジュールを入力します。
3. [OK] をクリックします。

アクションルールでスケジュールを使用するには、[Action Rule Setup] (アクションルール設定) ページの [Schedule (スケジュール)] ドロップダウンリストからスケジュールを選択します。

繰り返しの設定方法

繰り返しは、たとえば5分ごとまたは1時間ごとにアクションルールを繰り返しトリガーする場合に使用します。

繰り返しを設定するには:

1. [Setup > Additonal Controller Configuration > Events > Recurrences (設定 > 追加のコントローラー設定 > イベント > 繰り返し)] に移動し、[Add (追加)] をクリックします。
2. わかりやすい名前と繰り返しのパターンを入力します。
3. [OK] をクリックします。

アクションルールで繰り返しの設定を使用するには、まずアクションルール設定ページの [**トリガー**] ドロップダウンリストから [**時刻**] を選択し、2番目のドロップダウンリストで [繰り返し] を選択します。

繰り返しを変更または削除するには、[**繰り返しリスト**] から [繰り返し] を選択し、[**変更**] または [**削除**] をクリックします。

リーダーからのフィードバック

リーダーはLEDやビーパーを使用してフィードバックメッセージをユーザー (ドアにアクセスしようとしている人物) に送信します。ドアコントローラーは数種類のフィードバックメッセージをトリガーでき、いくつかはドアコントローラーに事前定義され、ほとんどのリーダーでサポートされています。

リーダーにはいくつかのLED動作がありますが、通常は、照明が赤、緑、黄の各色でさまざまに連続して点灯または点滅します。

アラームとイベントの設定

また、さまざまな長短のビーパー信号を繰り返す1ピッチのビープ音でメッセージを送信することもあります。

次表に、リーダーからのフィードバックをトリガーするドアコントローラーに事前定義されているイベントと、そのイベントの代表的なフィードバック信号を示します。AXISリーダーのフィードバック信号は、AXISリーダーに付属のインストールガイドに記載されています。

イベント	Wiegand デュアルLED	Wiegand シングルLED	OSDP	ビーパーのパターン	状態
Idle (待機中)[1]	Off (オフ)	赤	赤	サイレント	通常
RequirePIN (PINが必要)	赤/緑: 点滅	赤/緑: 点滅	赤/緑: 点滅	短いブザー音2回	PINが必要
AccessGranted	緑	緑	緑	ビープ	アクセス許可
AccessDenied	赤	赤	赤	ビープ	アクセス拒否

1. ドアが閉じられ、ロックされた場合に Idle (待機中) の状態になります。

上記以外のフィードバックメッセージは、アクセス管理システムなどのクライアントが、本機能をサポートし、必要な信号を発信することができるリーダーを使って、VAPIX®アプリケーションプログラミングインターフェースを使用して設定する必要があります。詳細については、アクセス管理システム開発者およびリーダーのメーカーによって提供されたユーザー情報を参照してください。

レポート

レポート

[Reports (レポート)] ページを使用すると、システムに関するさまざまなタイプの情報が含まれているレポートの表示、印刷、およびエクスポートができます。利用可能なレポートの詳細については、*55ページレポートタイプ*を参照してください。

レポートの表示、印刷、およびエクスポート

[Reports (レポート)] ページを開くには、[**Reports (レポート)**] をクリックします。

レポートを表示するには、[**View and print (表示と印刷)**] をクリックします。

レポートを印刷するには:

1. [**View and print (表示と印刷)**] をクリックします。
2. レポートに含める列を選択します。すべての列がデフォルトで選択されています。
3. レポートの範囲を絞り込む場合は、関連するフィルターフィールドにフィルターを入力します。たとえば、ユーザーをユーザーが所属するグループでフィルターしたり、ドアをスケジュールでフィルターしたりできます。また、グループをアクセスが許可されているドアでフィルターすることができます。

   完全一致を検索するには、"John" のように、フィルターテキストを二重引用符で囲みます。
4. レポート項目を別の順序で並べ替える場合は、関連する列で ▲▼ をクリックします。標準の順序と逆の順序との間で変更するには、並べ替えのボタンを使用して切り替えます。

   ▲ は、標準の順序 (昇順) で項目を表示しています。

   ▼ は、逆の順序 (降順) で項目を表示しています。
5. [**Print selected columns (選択した列を印刷)**] をクリックします。

レポートをエクスポートするには、[**Export CSV file (CSVファイルのエクスポート)**] をクリックします。

レポートはカンマ区切りの値 (CSV) ファイル形式でエクスポートされ、そのレポートタイプで使用できるすべての列と項目が含まれます。特に指定がない限り、エクスポートされたファイル (*.csv) はデフォルトのダウンロードフォルダーに保存されます。Webブラウザーのユーザー設定で、ダウンロードフォルダーを選択できます。

注

レポートには、認証情報を持つユーザーのみが表示されます。

レポートタイプ

以下のレポートタイプを利用できます。

- アクセススケジュール。アクセススケジュールのタイプとオプションの詳細については、*33ページ*と*34ページ*を参照してください。
- グループ。グループの認証情報の詳細については、*35ページ*を参照してください。
- ドア。ドアおよび識別タイプの詳細については、*36ページ*および*37ページ*を参照してください。
- ユーザー。ユーザー認証情報の詳細については、*42ページ*を参照してください。
- ドアコントローラー。接続されたドアコントローラーとそのIDタイプの詳細については、*29ページ*を参照してください。ドアのモニター時間のオプションの詳細については、*17ページ*を参照してください。

システムオプション

セキュリティ

ユーザー

ユーザーアクセスコントロールは、デフォルトで有効になっていて、[Setup > Additional Controller Configuration > System Options > Security > Users (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > ユーザー)] で設定できます。管理者は、ユーザー名とパスワードを付与して、ユーザーを設定できます。

ユーザーリストには、権限のあるユーザーとユーザーグループ (アクセスレベル) が表示されます。

- **管理者**には、すべての設定に対する無制限のアクセス権があります。管理者は他のユーザーを追加、変更、削除できます。

注

[**暗号化および非暗号化**] オプションを選択すると、Webサーバーがパスワードを暗号化します。暗号化および非暗号化は、新しい製品または工場出荷時の設定にリセットされた製品のデフォルトオプションです。

[**HTTP/RTSP パスワードの設定**] で、許可するパスワードのタイプを選択します。暗号化に対応していないクライアントが閲覧する場合や、最近ファームウェアをアップグレードしたばかりで、既存のクライアントは暗号化に対応しているが、再ログインして設定を行わないと暗号化機能を使用できない場合は、非暗号化パスワードの使用を許可する必要があります。

ONVIF

ONVIFは、インターフェースの標準化を促進して、IPベースの物理的なセキュリティ製品を効果的に相互運用することを目指している、オープンな業界フォーラムです。

ユーザーを作成すると、ONVIF通信が自動的に有効になります。製品とのすべてのONVIF通信には、ユーザー名とパスワードを使用します。詳細については、*www.onvif.org*を参照してください。

IPアドレスフィルター

IPアドレスフィルタリングは、[][Setup > Additional Controller Configuration > System Options > Security > IP Address Filter (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > IPアドレスフィルター)][] で有効にします。IPアドレスフィルタリングが有効になると、リスト内のIPアドレスからの本製品へのアクセスは許可または拒否されます。リストから [**許可**] または [**拒否**] を選択し、[**適用**] をクリックして、IPアドレスフィルタリングを有効にします。

管理者は、最大256のIPアドレスをリストに追加できます (1つのエントリーに複数のIPアドレスを含めることができます)。

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer、またはHTTP over SSL) は暗号化されたブラウジングを可能にするWebプロトコルです。ユーザーやクライアントがHTTPSを使用して、適切なデバイスがアクセスしているかを検証することもできます。HTTPSが提供するセキュリティレベルは、ほとんどの商用情報の交換に十分適合していると考えられています。

本製品は、管理者のログイン時にHTTPSが必要かどうかを設定できます。

HTTPSを使用するには、まずHTTPS証明書をインストールする必要があります。証明書をインストールして管理するには、[][Setup > Additional Controller Configuration > System Options > Security > Certificates (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > 証明書)][] に移動します。*57ページ 証明書* を参照してください。

本製品でHTTPSを有効にするには、以下の操作を行います。

1. [Setup > Additional Controller Configuration > System Options > Security > HTTPS (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > HTTPS)] に移動します。
2. インストール済み証明書のリストからHTTPS証明書を選択します。
3. 必要に応じて、[**暗号**] をクリックして、SSLで使用する暗号化アルゴリズムを選択します。
4. [**HTTPS接続ポリシー**] をユーザーグループごとに設定します。
5. [**保存**] をクリックすると、設定が有効になります。

希望するプロトコルを使用して本製品にアクセスするには、ブラウザーのアドレスフィールドに、HTTPSプロトコルの場合は「`https://`」、HTTPプロトコルの場合は「`http://`」を入力します。

HTTPSポートは [System Options > Network > TCP/IP > Advanced (システムオプション > ネットワーク > TCP/IP > 詳細設定)] ページで変更できます。

IEEE 802.1X

IEEE 802.1X はポートベースのNetwork Admission Control用の標準規格であり、有線およびワイヤレスのネットワークデバイスを安全に認証します。IEEE 802.1Xは、EAP (Extensible Authentication Protocol) に基づいています。

IEEE 802.1Xで保護されているネットワークにアクセスするには、デバイスは認証される必要があります。認証を実行するのは認証サーバーで、一般的には、FreeRADIUS、Microsoft Internet Authentication Serverなどの**RADIUS サーバー**です。

Axisの実装においては、本製品と認証サーバーは、EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) を使用するデジタル証明書で自己証明を行います。証明書は、**認証局 (CA)** が発行します。以下の証明書が必要です。

- 認証サーバーを認証するCA証明書。
- CAが署名した、本製品を認証するクライアント証明書

証明書を作成し、インストールするには、[][Setup > Additional Controller Configuration > System Options > Security > Certificates (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > 証明書)][] に移動します。*57ページ証明書*を参照してください。

本製品がIEEE 802.1Xで保護されているネットワークにアクセスするのを許可するには、以下の手順を実行します。

1. [Setup > Additional Controller Configuration > System Options > Security > IEEE 802.1X (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > IEEE 802.1X)] に移動します。
2. インストールされている証明リストから [**CA証明書**] と [**クライアント証明書**] を選択します。
3. [**設定**] からEAPOLバージョンを選択して、クライアント証明書に関連付けられているEAPのIDを入力します。
4. チェックボックスにチェックを入れて、IEEE 802.1Xを有効にし、[**保存**] をクリックします。

注

認証を正しく行うには、本製品の日付と時刻をNTPサーバーと同期させる必要があります。*58ページ日付と時刻*を参照してください。

証明書

証明書は、ネットワーク上のデバイスの認証に使用されます。一般的なアプリケーションには、暗号化されたWebブラウジング (HTTPS)、IEEE 802.1Xによるネットワーク保護、電子メールなどによるメッセージの通知などがあります。本製品では、以下の2種類の証明書を使用できます。

サーバー/クライアント証明書 - 本製品を認証します。**サーバー/クライアント** 証明書は、自己署名証明書と認証局 (CA) 発行の証明書のどちらでも使用できます。自己署名証明書による保護には制限がありますが、認証局発行の証明書を取得するまで利用できます。

CA証明書 - ピア証明書 (たとえば、本製品がIEEE 802.1Xで保護されたネットワークに接続している場合の認証サーバーの証明書など) を認証します。本製品には、CA証明書が何種類かプリインストールされています。

注

- 製品が工場出荷時の値にリセットされると、プリインストールされたCA証明書以外のすべての証明書が削除されます。
- 製品が工場出荷時の値にリセットされると、プリインストールされたCA証明書以外のすべての証明書が削除されます。

自己署名証明書の作成方法

1. [][Setup > Additional Controller Configuration > System Options > Security > Certificates (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > 証明書)][] に移動します。
2. [**自己署名証明書の作成**] をクリックして、必要な情報を入力します。

CA署名済み証明書を作成し、インストールする方法

1. 自己署名証明書を作成するには、を参照してください。
2. [][Setup > Additional Controller Configuration > System Options > Security > Certificates (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > 証明書)][] に移動します。
3. [**証明書の署名要求の作成**] をクリックして、必要な情報を入力します。
4. PEM形式の証明書請求をコピーして、希望するCAに送信します。
5. 署名付き証明書を受け取ったら、[**証明書のインストール**] をクリックして、証明書をアップロードします。

追加のCA証明書をインストールする方法

1. [][Setup > Additional Controller Configuration > System Options > Security > Certificates (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > 証明書)][] に移動します。
2. 証明書をアップロードするには、[**証明書のインストール**] をクリックして、証明書をアップロードします。

日付と時刻

本製品の日付と時刻の設定は、[][Setup > Additional Controller Configuration > System Options > Date & Time (設定 > 追加のコントローラー設定 > システムオプション > 日付と時刻)] で行います。

[Current Server Time (現在のサーバー時刻)] には、現在の日付と時刻 (24時間形式) が表示されます。

日付と時刻の設定を変更するには、[New Server Time (新しいサーバー時刻)] から希望の [Time mode (時刻モード)] を選択します。

- [Synchronize with computer time (コンピューターの時刻に合わせる)] は、コンピューターの時計に合わせて日付と時刻を設定します。このオプションでは、日付と時刻は一度だけ設定され、その後自動的には同期されません。
- [Synchronize with NTP Server (NTPサーバーと同期する)] - NTPサーバーから日付と時刻を取得します。このオプションでは、日付と時刻の設定が継続的に更新されます。NTPの設定の詳細については、*61 ページNTP設定*を参照してください。

  NTPサーバーとしてホスト名を使用している場合は、DNSサーバーの設定を行う必要があります。*61 ページDNS設定*を参照してください。
- [Set manually (手動で合わせる)] - 日付と時刻を手動で設定できます。

NTPサーバーを使用している場合は、ドロップダウンリストから [**Time zone (タイムゾーン)**] を選択します。必要に応じて、[**Automatically adjust for daylight saving time changes (夏時間の調整を自動的に行う)**] を選択します。

ネットワーク

TCP/IPの基本設定

本製品はIPバージョン4 (IPv4) をサポートします。

本製品は、以下の方法でIPv4アドレスを取得できます。

- **動的IPアドレス** – [**Obtain IP addres via DHCP (DHCPを使用してIPアドレスを取得する)**] がデフォルトで選択されています。これは、本製品が Dynamic Host Configuration Protocol (DHCP) 経由で自動的にIPアドレスを取得するように設定されていることを意味します。

  ネットワーク管理者は、DHCPを使用することでIPアドレスの一元管理と自動割り当てができます。

- **静的IPアドレス** – 静的IPアドレスを使用するには、[**Use the following IP address (次のIPアドレスを使用する)**] を選択し、IP アドレス、サブネットマスクおよびデフォルトのルーターを指定します。その後、[**Save (保存)**] をクリックします。

DHCPは、動的IPアドレス通知を使用しているか、DHCPでDNSサーバーを更新可能な場合 (これによって名前 (ホスト名) で本製品にアクセスできます) にのみ有効にしてください。

DHCPを有効にして本製品にアクセスできなくなった場合は、AXIS IP Utilityを実行し、ネットワークで接続されているAxis製品を検索するか、本製品を工場出荷時の設定にリセットしてからインストールをやり直す必要があります。工場出荷時の値にリセットする方法については、*67ページ*を参照してください。

ARP/Ping

製品のIPアドレスはARPおよびPingを使用して割り当てることができます。手順については、*59ページARP/Pingを使用したIPアドレスの割り当て*を参照してください。

ARP/Pingサービスはデフォルトで有効になっていますが、製品の起動後2分、または、IPアドレスが割り当てられた直後に自動的に無効になります。ARP/Pingを使用してIPアドレスの再割り当てを行うには、製品を再起動して、ARP/Pingを再び2分間有効にする必要があります。

サービスを無効にするには、[][**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 基本設定)**][] に移動し、オプション [**Enable ARP/Ping setting of IP address (IPアドレスのARP/Ping 設定を有効にする)**] をクリアします。

このサービスが無効になっていても、本製品にPingを送信することは可能です。

ARP/Pingを使用したIPアドレスの割り当て

デバイスのIPアドレスはARP/Pingを使用して割り当てることができます。このコマンドは電源を投入してから2分以内に発行する必要があります。

1. お使いのコンピューターと同じネットワークセグメントで使用されていない静的IPアドレスを取得します。
2. デバイスのラベルに記載されているシリアル番号 (S/N) を確認します。
3. コマンドプロンプトを開き、以下のコマンドを入力します。

   Linux/Unix 構文

   ```
   arp -s <IPアドレス> <シリアル番号> temp
   ping -s 408 <IPアドレス>
   ```

   Linux/Unix の例

```
arp -s 192.168.0.125 00:40:8c:18:10:00 temp
ping -s 408 192.168.0.125
```

Windows 構文 (コマンドプロンプトは、管理者として実行する必要があります)

```
arp -s <IPアドレス> <シリアル番号>
ping -l 408 -t <IPアドレス>
```

Windows の例 (コマンドプロンプトは、管理者として実行する必要があります)

```
arp -s 192.168.0.125 00-40-8c-18-10-00
ping -l 408 -t 192.168.0.125
```

4. ネットワークコネクタを接続し直して、デバイスを再起動します。
5. 「`Reply from 192.168.0.125:...`」のようなメッセージが表示されるのを確認し、コマンドプロンプトを終了します。
6. ブラウザーを開き、アドレスフィールドに「`http://<IPアドレス>`」と入力します。

IPアドレスを割り当てる他の方法については、*www.axis.com/support*にあるドキュメント『*IPアドレスを割り当ててデバイスにアクセスする方法*』を参照してください。

注

- Windowsでコマンドプロンプトを開くには、[**スタート**] メニュー を開き、`cmd`を検索します。
- Windows 8/Windows 7/Windows VistaでARPコマンドを使用するには、コマンドプロンプトアイコンを右クリックし、**[管理者として実行]** を選択します。
- Mac OS Xでコマンドプロンプトを開くには、[**Application > Utilities (アプリケーション > ユーティリティ)**] から [**Terminal utility (ターミナルユーティリティ)**] を開きます。

AXIS Video Hosting System (AVHS)

AVHSをAVHSサービスと共に使用すると、インターネットを介して、コントローラー管理やログにどこからでも簡単、安全にアクセスできます。近くのAVHSサービスプロバイダーを見つけるには、www.axis.com/hosting を参照してください。

AVHSの設定は、[][**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 基本設定)**][] で行います。AVHSサービスへの接続はデフォルトで有効になっています。無効にするには、[**Enable AVHS (AVHSを有効にする)**] ボックスをオフにします。

[One-click enabled (ワンクリックを有効にする)] - 製品のコントロールボタン (*4 ページ、製品の概要* を参照) を約3秒間押し続けて、インターネットを介してAVHSサービスに接続します。登録後は、[**Always (常時)**] が有効になり、本製品はAVHSサービスに接続し続けます。ボタンを押してから24時間以内に本製品を登録しなかった場合、本製品とAVHSサービスの接続が切断されます。

[Always (常時)] - 本製品は、インターネットを介したAVHSサービスへの接続を継続的に試行します。本製品は、いったん登録されると、AVHSサービスに接続し続けます。本製品がすでにインストール済みで、ワンクリックインストールを使用する必要がない場合、このオプションを使用することができます。

注

AVHSサポートは、サービスプロバイダーからのサブスクリプションの可用性に依存します。

AXIS Internet Dynamic DNS Service

AXIS Internet Dynamic DNS Serviceは、ホスト名を割り当てて、本製品へのアクセスを容易にします。詳細については、*www.axiscam.net*を参照してください。

本製品をAXIS Internet Dynamic DNS Serviceに登録するには、[][**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 基本設定)**][] に移動します。[**Services (サービス)**] でAXIS Internet Dynamic DNS Serviceの

[Settings (設定)] ボタンをクリックします (インターネットへのアクセスが必要)。製品に関してAXIS Internet Dynamic DNS Serviceに現在登録されているドメイン名は、いつでも削除することができます。

注

AXIS Internet Dynamic DNS ServiceにはIPv4が必要です。

TCP/IPの詳細設定

DNS設定

DNS (Domain Name Service) は、ホスト名からIPアドレスへの変換を行います。DNS設定は、[][Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)][] で行います。

DHCPサーバーから提供されるDNS設定を使用するには、[Obtain DNS server address via DHCP (DHCPを使用してDNSサーバーアドレスを取得する)] を選択します。

手動設定を行うには、[Use the following DNS server address (次のDNSサーバーアドレスを使用する)] を選択して、次のように指定します。

ドメイン名 - 本製品が使用するホスト名を検索するドメインを入力します。セミコロンで区切って、複数のドメイン名を指定することができます。ホスト名には、完全修飾ドメイン名の最初の部分を使用します。たとえば、完全修飾ドメイン名が`myserver.mycompany.com`の場合、`myserver`がホスト名です (`mycompany.com` はドメイン名)。

Primary/Secondary DNS server (プライマリ/セカンダリDNSサーバー) - プライマリDNSサーバーとセカンダリDNSサーバーのIPアドレスを入力します。セカンダリDNSサーバーは、プライマリDNSサーバーが使用できない場合に使用されます。セカンダリDNSサーバーの指定は省略可能です。

NTP設定

NTP (Network Time Protocol) は、ネットワーク上の機器の時刻を同期するために使用します。NTP設定は、[][Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)][] で行います。

DHCPサーバーから提供されるNTP設定を使用するには、[Obtain NTP server address via DHCP (DHCPを使用してNTPサーバーアドレスを取得する)] を選択します。

手動で設定を行うには、[Use the following NTP server address (次のNTPサーバーアドレスを使用する)] を選択して、NTPサーバーのホスト名またはIPアドレスを入力します。

ホスト名の設定

IPアドレスの代わりにホスト名を使用して本製品にアクセスすることができます。通常、ホスト名は割り当てられたDNS名と同じです。ホスト名は []、[Setup > Additional Controller Configuration> System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細)]、[] で設定します。

IPv4で実行されているDHCPサーバーによって提供されるホスト名を使用するには、[Obtain host name via IPv4 DHCP (IPv4のDHCPを使用してホスト名を取得)] を選択します。

ホスト名を手動で設定するには、[Use the host name (ホスト名を使用する)] を選択します。

[Enable dynamic DNS updates (DNSの動的更新を有効にする)] を選択すると、本製品のIPアドレスが変わるたびに、ローカルのDNSサーバーが動的に更新されます。詳細については、オンラインヘルプを参照してください。

リンクローカルIPv4アドレス

[Link-Local IPv4 Address (リンクローカルIPv4アドレス)] は、デフォルトで有効であり、本製品に追加のIPアドレスを割り当てます。この追加のIPアドレスは、ローカルネットワーク上の同じセグメントにある他のホストから本

システムオプション

製品にアクセスするために使用されます。本製品は、リンクローカルIPアドレスと、静的IPアドレスまたはDHCPによって提供されるIPアドレスの両方を同時に持つことができます。

この機能は、[Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)] で無効にできます。

HTTP

本製品で使用するHTTPポートは、[Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)] で変更できます。デフォルト設定の80に加えて、1024～65535の範囲のポートを使用できます。

HTTPS

本製品で使用するHTTPSポートは、[Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)] で変更できます。デフォルト設定の443に加えて、1024～65535の範囲のポートを使用できます。

HTTPSを有効にするには、[Setup > Additional Controller Configuration > System Options > Security > HTTPS (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > HTTPS)] に移動します。詳細については、*56ページHTTPS*を参照してください。

IPv4用NATトラバーサル (ポートマッピング)

プライベートネットワーク (LAN) 上のデバイスは、ネットワークルーターを使用することにより、インターネットへの接続を共有できます。これは、プライベートネットワークから「外部」(つまり、インターネット) へネットワークトラフィックを転送することによって行われます。ほとんどのネットワークルーターが、パブリックネットワーク (インターネット) からプライベートネットワーク (LAN) へのアクセスを阻止するようあらかじめ設定されており、プライベートネットワーク (LAN) のセキュリティは高いものになっています。

NATトラバーサルは、イントラネット (LAN) 上にある本製品を、NATルーターの外側 (WAN) から利用できるようにしたい場合に使用します。NATトラバーサルを正しく設定すると、NATルーターの外部HTTPポートに着信するすべてのHTTPトラフィックが本製品に転送されます。

NATトラバーサルは、[Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)] で設定します。

注

- NATトラバーサルを機能させるには、ルーターがNATトラバーサルに対応している必要があります。また、UPnP®にも対応している必要があります。
- この場合、ルーターとは、NATルーター、ネットワークルーター、インターネットゲートウェイ、ブロードバンドルーター、ブロードバンド共有デバイスなどのネットワークルーティングデバイス、またはファイアウォールなどのソフトウェアを指します。

有効化/無効化 - 有効にすると、本製品はUPnPを使用してネットワーク上のNATルーターにポートマッピングを設定します。本製品でUPnPを有効にする必要があります ([Setup > Additional Controller Configuration > System Options > Network > UPnP (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > UPnP)] を参照してください)。

Use manually selected NAT router (手動で選択したNATルーターを使用する) - このオプションを選択すると、手動でNATルーターを選択して、フィールドにルーターのIPアドレスを入力できます。ルーターを指定しなかった場合、本製品がネットワーク上でNATルーターを自動的に検索します。複数のルーターが検出された場合は、デフォルトのルーターが選択されます。

Alternative HTTP port (代替HTTPポート) - このオプションを選択すると、外部HTTPポートを手動で定義できます。1024～65535の範囲でポートを入力してください。ポートフィールドが空白の場合や、デフォルトの設定 (0) が表示されている場合、NATトラバーサルを有効にしたときにポート番号が自動的に選択されます。

システムオプション

注

- NATトラバーサルが無効になっている場合でも、代替のHTTPポートを使用したり、アクティブにすることができます。これは、NATルーターがUPnPをサポートしておらず、NATルーターでポート転送を手動設定する必要がある場合に便利です。
- すでに使用されているポートを手動で入力しようとすると、別の使用可能なポートが自動的に選択されます。
- ポートが自動的に選択されると、このフィールドに表示されます。この選択を変更するには、新しいポート番号を入力して、[**Save (保存)**] をクリックします。

FTP

本製品でFTPサーバーを実行することにより、新しいファームウェア、ユーザーアプリケーションなどのアップロードができるようになります。FTPサーバーは、[][**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)**][] で無効にできます。

RTSP

本製品でRTSPサーバーが動作している場合、接続先のクライアントからイベントストリームを開始できます。RTSPポート番号は [**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)**] で変更できます。デフォルトポートは554です。

注

RTSPサーバーが無効になっている場合、イベントストリームは使用できません。

SOCKS

SOCKSは、ネットワークプロキシプロトコルです。SOCKSサーバーを使用してファイアウォールやプロキシーサーバーの外側のネットワークにアクセスするように本製品を設定できます。この機能は、ファイアウォールの内側のローカルネットワーク上の本製品からローカルネットワークの外側 (インターネットなど) に通知やアラームを送信したり、アップロードなどを行う必要がある場合に役立ちます。

SOCKSは、[][**Setup > Additional Controller Configuration > System Options > Network > SOCKS (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > SOCKS)**][] で設定します。詳細については、オンラインヘルプを参照してください。

QoS (Quality of Service)

QoS (Quality of Service) は、ネットワーク上の特定のトラフィックに対してそのサービスの品質を保証します。QoSに対応したネットワークでは、トラフィックに優先順位を付け、アプリケーションで使用できる帯域幅を制御することができるので、ネットワークの信頼性が高まります。

QoS は、[**Setup > Additional Controller Configuration > System Options > Network > QoS (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > QoS)**] で設定できます。本製品では、DSCP (Differentiated Services Codepoint) 値を使用して、イベント/アラームトラフィックおよび管理トラフィックにマークを付けることができます。

SNMP

SNMP (Simple Network Management Protocol) を使用すると、離れた場所からネットワーク装置を管理できます。SNMPコミュニティは、SNMPを実行しているネットワーク装置と管理ステーションのグループです。各グループは、コミュニティ名で識別されます。

本製品でSNMPを有効にするには、[][**Setup > Additional Controller Configuration > System Options > Network > SNMP (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > SNMP)**][] ページに移動します。

必要なセキュリティのレベルに応じて、使用するSNMPのバージョンを選択してください。

トラップは、本製品によって重要なイベントやステータスの変化に関して管理システムにメッセージを送るために使用されます。[**Enable traps (トラップを有効にする)**] をチェックして、トラップメッセージの送信先IPアドレスとメッセージを受け取る [**Trap community (トラップコミュニティ)**] を入力します。

注

HTTPSを有効にした場合は、SNMP v1とSNMP v2cは無効にしてください。

[**Traps for SNMP v1/v2 (SNMP v1/v2トラップ)**] は、重要なイベントやステータスの変化に関して管理システムにメッセージを送るために本製品によって使用されます。[**Enable traps (トラップを有効にする)**] をチェックして、トラップメッセージの送信先IPアドレスとメッセージを受け取る [**Trap community (トラップコミュニティ)**] を入力します。

本製品では、以下のトラップを使用することができます。

- コールドスタート
- ウォームスタート
- リンクアップ
- 認証失敗

SNMP v3は、暗号化と安全なパスワードを提供します。SNMP v3でトラップを使用するには、SNMP v3管理アプリケーションが必要です。

SNMP v3を使用するには、HTTPSを有効にする必要があります (*56ページHTTPS*を参照してください)。SNMP v3を有効にするには、ボックスにチェックマークを入れ、初期ユーザーパスワードを指定してください。

注

初期パスワードは1回しか設定できません。パスワードを忘れた場合は、本製品を工場出荷時の設定にリセットする必要があります。*67ページ工場出荷時の設定にリセットする*を参照してください。

UPnP

本製品は、UPnP®に対応しています。UPnPはデフォルトで有効になっているため、本製品は、このプロトコルをサポートしているオペレーティングシステムとクライアントによって自動的に検出されます。

UPnPは、[][**Setup > Additional Controller Configuration > System Options > Network > UPnP (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > UPnP)**][] で無効にできます。

Bonjour

本製品は、Bonjourに対応しています。Bonjourはデフォルトで有効になっているため、本製品は、このプロトコルをサポートしているオペレーティングシステムとクライアントによって自動的に検出されます。

Bonjourは、[][**Setup > Additional Controller Configuration > System Options > Network > Bonjour (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > Bonjour)**][] で無効にできます。

ポートとデバイス

I/O ポート

本製品の補助コネクタは、外部装置との接続に使用する、設定可能な入出力ポートを2つ備えています。外部装置を接続する方法については、Axisのホームページ (*www.axis.com*) でインストールガイドを参照してください。

I/Oポートの設定は、[**Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (設定 > 追加のコントローラー設定 > システムオプション > ポートとデバイス > I/Oポート)**] で行います。ポートの方向 ([**入力**] または [**出力**]) を選択します。ポートには分かりやすい名前を付けることかできます。ポートの [**標準状態**] は、[**開路**] または [**接地回路**] に設定できます。

システムオプション

ポートの状態

[System Options > Ports & Devices > Port Status (システムオプション > ポートとデバイス > ポートの状態)] ページのリストには、本製品の入出力ポートの状態表示されます。

保守

本製品は保守機能を備えています。これらは、[][Setup > Additional Controller Configuration > System Options > Maintenance (設定 > 追加のコントローラー設定 > システムオプション > メンテナンス)][] で使用できます。

本製品が予想どおりに動作しない場合は、[**再起動**] をクリックして、本製品を正しく再起動します。この場合、現在の設定には影響がありません。

注

再起動により、サーバーレポートのすべてのエントリーが消去されます。

[**再起動**] をクリックすると、設定の大半が工場出荷時の値にリセットされます。以下の設定はリセットされません。

- ブートプロトコル (DHCPまたは静的)
- 静的IPアドレス
- デフォルトルーター
- サブネットマスク
- システム時刻
- IEEE 802.1X設定

[**デフォルト**] をクリックすると、IPアドレスなど、すべての設定が工場出荷時の値にリセットされます。このボタンは慎重に使用する必要があります。本製品は、コントロールボタンを使用してリセットすることもできます。*67ページ工場出荷時の設定にリセットする* を参照してください。

ファームウェアのアップグレードについては、*68ページファームウェアのアップグレード方法* を参照してください。

アプリケーションデータをバックアップする

[Setup > Create a backup (設定 > バックアップの作成)] の順に移動して、アプリケーション データのバックアップを作成します。バックアップされるデータには、ユーザー、資格情報、グループ、およびスケジュールが含まれます。バックアップを作成すると、データを含むファイルがコンピュータにローカルに保存されます。

[Setup > Upload a backup (設定 > バックアップのアップロード)] の順に移動して、以前に作成したバックアップファイルを使用してアプリケーションデータを復元します。バックアップファイルをアップロードする前に、デバイスを工場出荷時の設定にリセットする必要があります。手順については、*67ページ工場出荷時の設定にリセットする* を参照してください。

サポート

サポートの概要

[][Setup > Additional Controller Configuration > System Options > Support > Support Overview (設定 > 追加のコントローラー設定 > システムオプション > サポート > サポートの概要)][] ページには、トラブルシューティングに関する情報や技術支援が必要な場合の連絡先情報があります。

*68ページ、トラブルシューティング*も参照してください。

システムオプション

システムの概要

本製品の状態および設定の概要を確認するには、[Setup > Additional Controller Configuration > System Options > Support > System Overview (設定 > 追加のコントローラー設定 > システムオプション > サポート > システムの概要)] に移動します。ここでは、ファームウェアバージョン、IPアドレス、ネットワークとセキュリティの設定、イベントの設定、最近のログの内容などの情報が表示されます。

Logs & Reports (ログとレポート)

[][Setup > Additional Controller Configuration > System Options > Support > Logs & Reports (設定 > 追加のコントローラー設定 > システムオプション > サポート > ログとレポート)][] ページでは、システム分析やトラブルシューティングに役立つログとレポートが生成されます。Axisの技術サポートに連絡する場合は、質問と共にサーバーレポートをお送りください。

System Log (システムログ) - システムイベントに関する情報を表示します。

Access Log (アクセスログ) - 製品へのアクセスに失敗したすべてのログをリストします。本製品への接続をすべて表示するように設定することもできます (下記参照)。

View Server Report (サーバーレポートを表示) - 製品ステータスに関する情報をポップアップウィンドウに表示します。アクセスログは自動的にサーバーレポートに含まれます。

Download Server Report (サーバーレポートをダウンロード) - UTF–8テキスト形式の完全なサーバーレポートを含んだ.zipファイルを生成します。ライブビューのスナップショットを含めるには、[Include snapshot from Live View (ライブビューからスナップショットを撮影してレポートに含める)] を選択してください。Axisのサポートに連絡する際には、必ず、.zipファイルを添えて問い合わせを行ってください。

Parameter List (パラメーターリスト) - 本製品のパラメーターと現在の設定を表示します。トラブルシューティングを行う場合やAxisのサポートに問い合わせを行う場合に役立ちます。

Connection List (接続リスト) - メディアストリームに現在アクセスしているすべてのクライアントを表示します。

Crash Report (クラッシュレポート) - デバッグ情報を含むアーカイブを生成します。レポートの生成には数分かかります。

システムログとアクセスログのログレベルは、[][Setup > Additional Controller Configuration > System Options > Support > Logs & Reports > Configuration (設定 > 追加のコントローラー設定 > システムオプション > サポート > ログとレポート > 構成)] で設定します。アクセスログは、本製品への接続をすべて表示するように設定することもできます ([Critical, Warnings & Info (致命的、警告、情報)] を選択します)。

詳細設定

スクリプト処理

上級ユーザーは、スクリプト処理を使用して、スクリプトをカスタマイズし、使用することができます。

注意

使い方を誤ると、予期せぬ動作が発生したり、本製品にアクセスできなくなる場合があります。

Axisでは、どのような結果になるかを理解するまで、この機能を使用しないことを強くお勧めします。Axisは、スクリプトのカスタマイズによって発生した問題についてはサポートを行いませんのでご注意ください。

スクリプトエディターを開くには、[][Setup > Additional Controller Configuration > System Options > Advanced > Scripting (設定 > 追加のコントローラー設定 > システムオプション > 詳細設定 > スクリプト処理)][] に移動します。スクリプトが問題を引き起こす場合は、本製品を工場出荷時の設定にリセットしてください (*67*ページ参照)。

詳細については、*www.axis.com/developer*を参照してください。

システムオプション

ファイルのアップロード

ファイル (Webページや画像) を本製品にアップロードし、カスタム設定として使用することができます。ファイルをアップロードするには、[][Setup > Additional Controller Configuration > System Options > Advanced > File Upload (設定 > 追加のコントローラー設定 > システムオプション > 詳細設定 > ファイルのアップロード)][] に移動します。

アップロードしたファイルには、`http://<IP`**アドレス**`>/local/<`**ユーザー**`>/<`**ファイル名**`>` を介してアクセスします。<**ユーザー**>には、アップロードしたファイル用に選択したユーザーグループ (管理者) を指定します。

工場出荷時の設定にリセットする

重要

工場出荷時の設定へのリセットは慎重に行ってください。工場出荷時の設定へのリセットを行うと、IPアドレスを含むすべての設定が工場出荷時の値にリセットされます。

本製品を工場出荷時の設定にリセットするには、以下の手順を実行します。

1. 本製品の電源を切ります。
2. コントロールボタンを押した状態で電源を再接続します。 *4 ページ、製品の概要*を参照してください。
3. ステータスLEDが再びオレンジ色に変わるまで、コントロールボタンを押し続けます (25秒間)。
4. コントロールボタンを離します。プロセスが完了すると、ステータスLEDが緑色に変わります。これで本製品は工場出荷時の設定にリセットされました。ネットワーク上に利用可能なDHCPサーバーがない場合、デフォルトのIPアドレスは`192.168.0.90`になります。
5. インストールおよび管理ソフトウェアツールを使用して、IPアドレスの割り当て、パスワードの設定、製品へのアクセスを行います。

Webインターフェースを使用して、各種パラメーターを工場出荷時の設定に戻すこともできます。**Setup > Additional Controller Configuration > Setup > System Options > Maintenance (設定 > 追加のコントローラー設定 > 設定 > システムオプション > メンテナンス)** を選択し、**Default (デフォルト)** をクリックします。

トラブルシューティング

現在のファームウェアの確認方法

ファームウェアは、ネットワークデバイスの機能を決定するソフトウェアです。問題のトラブルシューティングを行う際には、まず、現在のファームウェアバージョンを確認してください。最新バージョンには、特定の問題の修正が含まれていることがあります。

本製品の現在のファームウェアバージョンは、概要ページに表示されます。

ファームウェアのアップグレード方法

重要

- ユーザーが正しくアップグレードしなかったことに起因する修理については、販売店は費用を請求する権利を保有します。
- あらかじめ設定済みの設定とカスタム設定は、(その機能が新しいファームウェアで利用できる場合)、ファームウェアのアップグレード時に保存されます。ただし、この動作をAxisが保証しているわけではありません。
- 以前のバージョンのファームウェアをインストールする場合は、その後、本製品を工場出荷時設定にリストアする必要があります。

注

- アップグレードのプロセスが完了すると、本製品は自動的に再起動します。本製品のアップグレード後に手動で再起動する場合、アップグレードが失敗した疑いがある場合でも、5分間待ってください。
- データベースのユーザーやグループ、証明書、その他のデータのアップデートは、ファームウェアのアップグレード後に行われるため、最初の起動が完了するまで数分かかることがあります。必要な時間はデータの量によって異なります。
- 最新のファームウェアをダウンロードして製品をアップグレードすると、製品に最新機能が追加されます。ファームウェアを更新する前に、ファームウェアとともに提供されるアップグレード手順とリリースノートを必ずお読みください。

スタンドアロンのドアコント ローラー:

1. 最新のファームウェアファイルをコンピューターにダウンロードします。ファームウェアファイルはAxisサポートページ (*www.axis.com/support*) から無料で入手できます。
2. 製品のWebページで、[**Setup > Additional Controller Configuration > System Options > Maintenance (設定 > 追加のコントローラー設定 > システムオプション > メンテナンス)**] に移動します。
3. [**Upgrade Server (サーバーのアップグレード)**] で、[**Choose file (ファイルの選択)**] をクリックして、コンピューター上のファイルを指定します。
4. 本製品をアップグレード後、工場出荷時の設定に自動的にリストアする場合は、[**Default (デフォルト)**] チェックボックスをオンにします。
5. [**Upgrade (アップグレード)**] をクリックします。
6. 本製品がアップグレードされて再起動するまで、約5分間待ちます。そのあと、Webブラウザーのキャッシュをクリアします。
7. 製品にアクセスします。

システム内のドアコントローラー:

AXIS Device ManagerまたはAXIS Camera Stationを使用して、システム内のすべてのドアコントローラーをアップグレードできます。詳細については、AxisのWebサイト (*www.axis.com*) をご覧ください。

重要

- アップグレードで [Sequence (シーケンス)] は選択しないでください。

注

- システム内のすべてのコントローラーは、常に同じバージョンのファームウェアを使用する必要があります。
- AXIS Device ManagerまたはAXIS Camera Stationで、[Parallel (パラレル)] オプションを使用して、システム内のすべてのコントローラーを同時にアップグレードします。

緊急リカバリーの手順

アップグレード中に本製品への電源またはネットワーク接続が失われた場合は、アップグレードプロセスが失敗し、本製品が応答しなくなる可能性があります。アップグレードに失敗すると、ステータスLEDが赤く点滅します。本製品をリカバリーするには、下記の手順を実行してください。シリアル番号は、本製品のラベルに記載されています。

1. **UNIX/Linux** の場合 - コマンドラインから、次のコマンドを入力します。

   ```
   arp -s <本製品のIPアドレス> <シリアル番号> temp
   ping -l 408 <本製品のIPアドレス>
   ```

   Windows の場合 - コマンド/DOSプロンプトから、次のコマンドを入力します (コマンドプロンプトは、管理者として実行する必要があります)。

   ```
   arp -s <本製品のIPアドレス> <シリアル番号>
   ping -l 408 -t <本製品のIPアドレス>
   ```

2. 30秒以内に製品が応答しない場合は、再起動し、応答を待ちます。Pingを停止するには、CTRL+C を押します。
3. ブラウザーを開き、本製品のIPアドレスを入力します。開いたページで、[**参照**] ボタンを使用し、使用するアップグレードファイルを選択します。[**読み込み**] ボタンをクリックして、アップグレードプロセスを再開します。
4. アップグレードが完了すると (1～10分)、本製品が自動的に再起動し、ステータスインジケーターが緑色に点灯します。
5. 本製品を再インストールします (『インストールガイド』を参照)。

緊急リカバリーを行っても本製品が起動、動作しない場合は、Axisのサポート (*www.axis.com/support*) までご連絡ください。

現象、考えられる原因、対策

ファームウェアのアップグレードで問題が発生する

ファームウェアのアップグレード失敗	ファームウェアのアップグレードに失敗した場合、製品は以前のファームウェアを再度読み込みます。ファームウェアのファイルを確認して、もう一度試してください。

IPアドレスの設定で問題が発生する

ARP/Pingを使用している	再インストールを行います。本製品の電源投入後、2分以内にIPアドレスを設定する必要があります。Pingの長さは408に設定します。手順については、*axis.com*の『インストールガイド』を参照してください。
本製品が別のサブネット上にある	本製品のIPアドレスと本製品にアクセスするコンピューターのIPアドレスが異なるサブネットにある場合は、IPアドレスを設定できません。ネットワーク管理者に連絡して、適切なIPアドレスを取得してください。

トラブルシューティング

IPアドレスが別のデバイスで使用されている	本製品をネットワークから切断します。Pingコマンドを実行します (コマンドウィンドウまたはDOSウィンドウで、`ping`コマンドと本装置のIPアドレスを入力します)。 • もし、「`Reply from <`**本製品のIPアドレス**`>: bytes=32; time=10...`」という応答を受取った場合は、ネットワーク上の別のデバイスでIPアドレスがすでに使用中の可能性があります。ネットワーク管理者から新しいIPアドレスを取得し、本製品を再度インストールしてください。 • もし、「`Request timed out`」が表示された場合は、本製品でそのIPアドレスを使用できます。この場合は、すべてのケーブル配線をチェックし、本製品を再度インストールしてください。
同じサブネット上の別のデバイスとIPアドレスが競合している可能性がある	DHCPサーバーによって動的アドレスが設定される前は、本製品の静的IPアドレスが使用されます。つまり、デフォルトの静的IPアドレスが別のデバイスでも使用されていると、本製品のアクセスに問題が発生する可能性があります。

ブラウザーから本製品にアクセスできない

ログインできない	HTTPSが有効な場合は、正しいプロトコル (HTTPまたはHTTPS) を使用してログインしてください。ブラウザーのアドレスフィールドに、手動で「`http`」または「`https`」と入力する必要がある場合があります。 rootユーザーのパスワードを忘れた場合は、製品を工場出荷時の設定にリセットする必要があります。*67ページ工場出荷時の設定にリセットする*を参照してください。
DHCPによってIPアドレスが変更された	DHCPサーバーから取得したIPアドレスは動的なアドレスであり、変更されることがあります。IPアドレスが変更された場合は、AXIS IP UtilityまたはAXIS Device Managerを使用して本製品のネットワーク上の場所を特定してください。本製品のモデルまたはシリアル番号、あるいはDNS名 (設定されている場合) を使用して製品を識別します。 必要に応じて、静的IPアドレスを手動で割り当てることができます。手順については、製品ページ (*axis.com*) にある『*IPアドレスを割り当ててデバイスにアクセスする方法*』のドキュメントを参照してください。
IEEE 802.1X使用時の証明書エラー	認証を正しく行うには、本製品の日付と時刻をNTPサーバーと同期させる必要があります。*58ページ日付と時刻*を参照してください。

本製品にローカルにアクセスできるが、外部からアクセスできない

ルーターの設定	本製品への着信データトラフィックを許可するようにルーターを設定するには、NATトラバーサル機能を有効にします。この機能を有効にすると、本製品へのアクセスを許可するようにルーターが自動設定されます。*62ページIPv4用NATトラバーサル (ポートマッピング)*を参照してください。ルーターはUPnP®に対応している必要があります。
ファイアウォールによる保護	インターネットのファイアウォールについて、ネットワーク管理者に確認してください。
デフォルトルーターが必要	ルーターを設定する必要があるかどうか、[**Setup > Network Settings (設定 > ネットワーク設定)**] または [**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 基本設定)**] で確認してください。

ステータスインジケーターとネットワークインジケーターのLEDが赤く、素早く点滅する

ハードウェアの故障	Axisの販売店に連絡してください。

トラブルシューティング

製品が起動しない	
製品が起動しない	製品が起動しない場合、ネットワークケーブルに接続されていることを確認します。次に、電源ケーブルをミッドスパンに再度挿入します。

仕様

仕様

コネクタ

コネクタの位置については、を参照してください。

接続図とハードウェア設定により生成されるハードウェアピン配置図については、*77ページ接続図*と*14ページハードウェアの設定*を参照してください。

次のセクションで、コネクタの技術仕様について説明します。

リーダーデータコネクタ

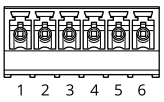
リーダーとの通信用のRS485およびWiegandプロトコルに対応する6ピンターミナルブロック。

RS485ポートが対応する通信方式:

- 2ワイヤーRS485半二重
- 4ワイヤーRS485全二重

Wiegandポートが対応する通信方式:

- 2ワイヤーWiegand



機能		ピン	備考
RS485	A-	1	全二重RS485用 半二重RS485用
	B+	2	
RS485	A-	3	全二重RS485用 半二重RS485用
	B+	4	
Wiegand	D0 (データ0)	5	Wiegand用
	D1 (データ1)	6	

重要

RS485ポートは9600ビット/秒の固定ボーレートです。

重要

ケーブルの推奨最大長は30 mです。

重要

このセクションの出力回路はClass 2の有限電源です。

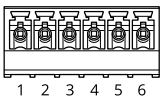
リーダーI/Oコネクタ

6ピンターミナルブロック:

仕様

- 補助電源 (DC出力)
- デジタル入力
- デジタル出力
- 0 V DC (-)

リーダーI/Oコネクタのピン3は状態監視できます。接続が中断されると、イベントが有効になります。状態監視入力を使用するには、終端抵抗器を設置します。状態監視入力の接続図を使用します。*77ページ*を参照してください。



機能	ピン	備考	仕様
0 V DC (-)	1		0 V DC
DC出力	2	補助装置への電源供給用。 注: このピンは、電源出力としてのみ使用できます。	12 V DC 最大負荷 = 300 mA
設定可能 (入力または出力)	3–6	デジタル入力 — 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。	0～40 V DC (最大)
		デジタル出力 — 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。リレーなど、誘導負荷とともに使用する場合は、過渡電圧から保護するために、ダイオードを負荷と並列に接続する必要があります。	0～40 V DC (最大)、オープンドレイン、100 mA

重要

ケーブルの推奨最大長は30 mです。

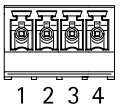
重要

このセクションの出力回路はClass 2の有限電源です。

ドアコネクタ

ドア監視デバイス用4ピンターミナルブロック (×2) (デジタル入力)。

すべてのドア入力ピンを状態監視できます。接続が中断されると、アラームがトリガーされます。状態監視入力を使用するには、終端抵抗器を設置します。状態監視入力の接続図を使用します。*77ページ*を参照してください。



仕様

機能	ピン	備考	仕様
0 V DC (-)	1, 3		0 V DC
入力	2, 4	ドアモニターとの通信用。 デジタル入力 — 動作させるには、それぞれピン1または3に接続し、動作させない場合はフロート状態 (未接続) のままにします。 注: このピンは入力用にのみ使用できます。	0〜40 V DC (最大)

重要

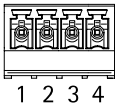
ケーブルの推奨最大長は30 mです。

補助コネクタ

設定可能な4ピンI/Oターミナルブロック:

- 補助電源 (DC出力)
- デジタル入力
- デジタル出力
- 0 V DC (-)

接続図の例については、*77ページ接続図*を参照してください。



機能	ピン	備考	仕様
0 V DC (-)	1		0 V DC
DC出力	2	補助装置への電源供給用。 注: このピンは、電源出力としてのみ使用できます。	3.3 V DC 最大負荷 = 100 mA
設定可能 (入力または出力)	3–4	デジタル入力 — 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。	0〜40 V DC (最大)
		デジタル出力 — 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。リレーなど、誘導負荷とともに使用する場合は、過渡電圧から保護するために、ダイオードを負荷と並列に接続する必要があります。	0〜40 V DC (最大)、オープンドレイン、100 mA

重要

ケーブルの推奨最大長は30 mです。

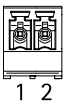
重要

このセクションの出力回路はClass 2の有限電源です。

仕様

電源コネクター

DC電源入力用2ピンターミナルブロック。定格出力が100 W以下または5 A以下の安全特別低電圧 (SELV) に準拠した有限電源 (LPS) を使用してください。



機能	ピン	備考	仕様
0 V DC (-)	1		0 V DC
DC入力	2	Power over Ethernetを使用しないときのコントローラーへの電源供給用。 注: このピンは、電源入力としてのみ使用できます。	10～28 V DC、最大36 W 出力の最大負荷 = 14 W

ネットワークコネクタ

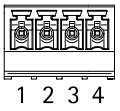
RJ45イーサネットコネクタ。Category 5eケーブル以上を使用します。

機能	仕様
電力とイーサネット	Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3、44～57 V DC 出力の最大負荷 = 7.5 W

電源ロックコネクタ

1つまたは2つのロックへの電源供給用4ピンターミナルブロック (DC出力)。ロックコネクタは、外部デバイスへの電源供給にも使用できます。

ハードウェア設定により生成されたハードウェアピン配置図に従って、ロックと負荷をピンに接続します。



機能	ピン	備考	仕様
0 V DC (-)	1, 3		0 V DC
0 V DC、フロート状態、または12 V DC	2, 4	最大2つの12 Vロックの制御用。ハードウェアピン配置図を使用します。*14ページハードウェアの設定*を参照してください。	12 V DC 最大総合負荷 = 500 mA

注意

ロックに極性がない場合は、外部フライバックダイオードを追加することをお勧めします。

重要

このセクションの出力回路はClass 2の有限電源です。

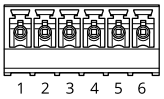
仕様

電源およびリレーコネクタ

内蔵リレーを備えた6ピンターミナルブロック:

- 外部デバイス
- 補助電源 (DC出力)
- 0 V DC (-)

ハードウェア設定により生成されたハードウェアピン配置図に従って、ロックと負荷をピンに接続します。



機能	ピン	備考	仕様
0 V DC (-)	1, 4		0 V DC
リレー	2–3	リレー装置の接続用。ハードウェアピン配置図を使用します。*14ページハードウェアの設定*を参照してください。 2つのリレーピンは回路の残りの部分から直流的に分離されています。	最大電流 = 700 mA 最大電圧 = +30 V DC
12 V DC	5	補助装置への電源供給用。 注: このピンは、電源出力としてのみ使用できます。	最大電圧 = +12 V DC 最大負荷 = 500 mA
24 V DC	6	使用しません	

注意

ロックに極性がない場合は、外部フライバックダイオードを追加することをお勧めします。

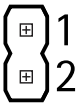
重要

このセクションの出力回路はClass 2の有限電源です。

いたずら警告ピンヘッダー

バイパス用の2ピンヘッダーx2:

- 背面のいたずら警告 (TB)
- 前面のいたずら警告 (TF)



機能	ピン	備考
背面のいたずら警告	1–2	前面および背面のいたずら警告を同時にバイパスするには、それぞれTB 1、TB 2とTF 1、TF 2の間のジャンパーを接続します。いたずら警告をバイパスすると、システムはいたずらの試みを識別できなくなります。
前面のいたずら警告	1–2	

仕様

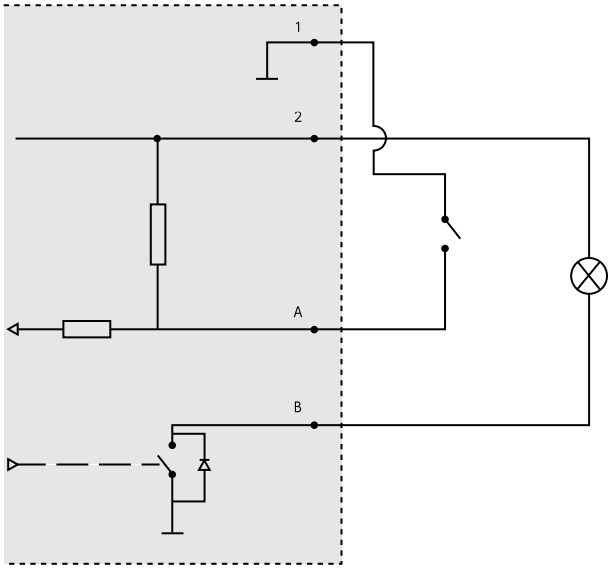
注

前面および背面のいたずら警告は、デフォルトで接続されています。ケーシング開放のトリガーは、ドアコントローラーが開けられた場合や、ドアコントローラーが壁や天井から取り外された場合にアクションを実行するように設定できます。警告とイベントを設定する方法については、*46ページ、アラームとイベントの設定*を参照してください。

接続図

ハードウェア設定により生成されたハードウェアピン配置図に従ってデバイスを接続します。ハードウェア設定とハードウェアピン配置図の詳細については、*14ページハードウェアの設定*を参照してください。

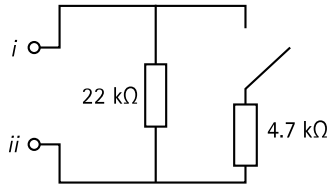
補助コネクタ



1　0 V DC (-)
2　DC出力: 3.3 V、最大100 mA
A　I/O (入力として設定)
B　I/O (出力として設定)

状態監視入力

状態監視を使用するには、下図に従って終端抵抗器を設置します。



i　入力
ii　0 V DC (-)

仕様

注

シールド付きツイストケーブルを使用することをお勧めします。シールドを0ＶDCに接続します。

安全情報

安全情報

危険レベル

⚠危険

回避しない場合、死亡または重傷につながる危険な状態を示します。

⚠警告

回避しない場合、死亡または重傷につながるおそれのある危険な状態を示します。

⚠注意

回避しない場合、軽傷または中程度の怪我につながるおそれのある危険な状態を示します。

注意

回避しない場合、器物の破損につながるおそれのある状態を示します。

その他のメッセージレベル

重要

製品を正しく機能させるために不可欠な重要情報を示します。

注

製品を最大限に活用するために役立つ有用な情報を示します。

ユーザーマニュアル
AXIS A1001 & AXIS Entry Manager

バージョン M25.2
日付: 2023年12月
製品番号 T10010336