iVMS-4200 クライアントソフトウェア

ユーザーマニュアル

法規関連情報

このマニュアルについて

このマニュアルには製品の使用および管理についての指示が含まれています。ここに記載されている写真、表、画像などの情報はすべて、説明のみを目的としています。このマニュアルに含まれる情報は、ファームウェア更新やその他の理由で事前の通知なく変更されることがあります。このマニュアルの最新版については Hikvision の Web サイト（***https://www.hikvision.com/en/***）をご確認ください。
この製品に関するサポート訓練を受けている専門家の指導や援助を受けた上でこのマニュアルを使用してください。

商標

HIKVISION およびその他の Hikvision の商標およびロゴは、さまざまな管轄区域における Hikvision の資産です。
このマニュアルに記載されているその他の商標およびロゴはそれぞれの所有者の資産です。

免責事項

適用法により許容される範囲内で、このマニュアル、記載の製品とそのハードウェア、ソフトウェアおよびファームウェアは、あらゆる不具合や瑕疵を含め、現状有姿で提供されるものとします。HIKVISION では明示の有無によらず一切の保証（商品性、十分な品質、特定の目的に対する適合性を含むが、これらに限定しない）を行いません。この製品は、ユーザーの責任で使用してください。HIKVISION は、この製品の利用に関連する事業利益の損失や事業妨害、データの損失、システムの破損、文書の損失に関する損害を含む特別、必然的、偶発的または間接的な損害に対して、契約の違反、不法行為（過失を含む）、製造物責任、その他を問わず、たとえ HIKVISION がそれらについて通知を受けていたとしても、一切の責任を負いません。
ユーザーは、インターネットの性質上、セキュリティリスクが内在していることを承知するものとします。HIKVISION は、異常操作、プライバシー漏えいまたはサイバー攻撃、ハッキング、ウィルス検査やその他のインターネットセキュリティリスクから生じるその他の損害に対して一切の責任を負わないものとします。ただし、必要に応じて HIKVISION は適宜技術サポートを提供します。
ユーザーは、この製品をすべての適用法に従って使用することに同意するものとし、使用方法が適用法に準拠するようにすることについては、ユーザー自身が一切の責任を負うものとします。特に、ユーザーは、第三者の権利（パブリシティ権、知的財産権、データ保護、および他のプライバシー権を含むが、これらに限定しない）を侵害しない方法でこの製品を使用することに責任を負います。ユーザーはこの製品を、大量破壊兵器の開発または製造、生物化学兵器の開発または製造、いかなる核爆発物または安全でない核燃料サイクルに関連する状況または人権侵害の支援での一切の活動を含む、いかなる禁止された最

終用途にも使用しないものとします。
このマニュアルと適用法との間に矛盾が存在する場合は、後者が優先されます。

ポートリスト

ポートリストの詳細については、Hikvision の公式 Web サイトをご覧ください。

記号の定義

このマニュアルで使用する記号は以下のように定義されています。

記号	説明
危険	防止できなかった場合に死亡や重傷を招くおそれのある危険な状況を示します。
注意	潜在的に危険となりうる状況を示しており、防止できなかった場合、機器の損傷、データの消失、性能劣化など、予測不能な結果が生じる可能性があります。
注記	本文内の重要事項を強調または補足する追加情報を提供します。

目次

第 1 章 概要

1.1 はじめに

iVMS-4200 クライアントソフトウェアは、DVR、NVR、IP カメラ、エンコーダ、デコーダ、セキュリティコントロールパネル、ビデオインターコムデバイス、入退室管理デバイスなどに対応した多目的なセキュリティ管理ソフトウェアです。
このソフトウェアは、リアルタイムライブビュー、ビデオ録画、リモート検索と再生、ファイルバックアップ、アラーム受信、人物管理、入退室管理、ビデオインターコム、セキュリティコントロール、時間と出勤などのさまざまな機能を提供していて、これにより接続されているデバイスは監視タスクのニーズを満たすことができます。柔軟な分散構造と使いやすさにより、このクライアントソフトウェアは中小規模の監視プロジェクトで幅広く使用されています。
このユーザーマニュアルでは、クライアントソフトウェアの機能、設定および操作手順について説明します。ソフトウェアを適切に使用し、ソフトウェアを安定した状態で動作させるためにも、インストールおよび操作の前に、以下の内容を参照し、マニュアルを注意深くお読みください。

1.2 変更の概要

このバージョンと以前のバージョンの主な変更点は次のとおりです。

- フィッシュアイ展開用にシリンダーモードを新たに追加しました。詳細については、「*フィッシュアイモードでのライブビューの実行*」および「*フィッシュアイカメラのビデオ再生*」をご覧ください。
- ライブビュー中に、複数の方法でストリームタイプを切り替えることができるようになりました。詳細については、「*その他の機能*」をご覧ください。
- 再生中のサムネイルを新たに追加しました。詳細については、「*ビデオファイルの再生*」をご覧ください。
- [レポート] モジュールのレポート表示を最適化しました。詳細については、「*統計*」をご覧ください。
- [データ検索] モジュールに人体および顔の特徴による検索機能を新たに追加しました。詳細については、「*顔画像の検索*」および「*人体の検索*」をご覧ください。
- 低出現頻度人物検索機能を新たに追加しました。詳細については、「*低出現頻度人物の検索*」をご覧ください。
- 顔認識によって記録された出勤ログの検索機能を新たに追加しました。詳細については、「*顔認識チェックイン*」をご覧ください。
- 対象人物の移動パターンをマップ上に表示する機能を新たに追加しました。詳細につい

ては、「*人物の移動パターンの表示*」をご覧ください。

- ビデオインターコムデバイスのイベント設定を新たに追加しました。詳細については、「*ビデオインターコムイベントの設定*」をご覧ください。
- 入退室管理デバイスからクライアントへのイベントの取得機能を新たに追加しました。詳細については、「*デバイスからのイベントの取得*」をご覧ください。
- アクセスグループの人物とアクセスポイントの表示を最適化しました。詳細については、「*アクセスグループを設定してアクセス認証を人物に割り当てる*」をご覧ください。
- 追加されたアクセスグループの検索機能を新たに追加しました。詳細については、「*アクセスグループの検索*」をご覧ください。
- [入退室管理] モジュールに認証コードの設定機能を新たに追加しました。詳細については、「*認証コードの設定*」をご覧ください。
- [Time & Attendance（時間と出勤）] モジュールのタイムテーブル設定を最適化しました。詳細については、「*一般タイムテーブルの追加*」をご覧ください。
- 1 つのシフトに複数のタイムテーブルを設定できるようになりました。詳細については、「*シフトの追加*」をご覧ください。
- 出勤の元データをエクスポートする際の形式とフィールドのカスタマイズをサポートするようになりました。詳細については、「*出勤記録のカスタムエクスポート*」をご覧ください。
- 入退室管理、時間と出勤、セキュリティコントロールパネル、およびビデオインターコムのフローチャートを新たに追加しました。

第 2 章 サービス管理

iVMS-4200 サービスは、主にデータストレージ、データ管理、およびデータ計算に適用できます。iVMS-4200 サービスは、継続的な実行と処理により、iVMS-4200 クライアントソフトウェアが受信したイベント記録や出勤記録などのデータを管理することができます。また、ユーザー権限、デバイス、グループ、ログなどの管理機能も提供します。
モジュールの実行状態を表示し、HTTP ポートや ISUP ポートなどのポートを編集できます。編集内容を有効にするには、iVMS-4200 サービスを再起動する必要があります。
PC の起動後に iVMS-4200 サービスを自動的に起動できるようにするには、**[自動起動]** にチェックを入れます。
iVMS-4200 サービスは、実行後に表示されなくなります。システムトレイで をクリックしてサービス管理ウィンドウを開きます。**[ポートを編集]** をクリックして、[ポートを編集] ウィンドウを開きます。ルーターに設定されている ISUP ポート番号を入力します。これにより、ISUP デバイスをクライアントに追加して管理できるようになります。

注記

- サービスウィンドウを閉じると、クライアントはログアウトしてログインページに戻ります。サービスを実行してから、再度ログインする必要があります。
- 1 台のコンピュータ上で複数のオペレーティングシステムユーザーがクライアントを同時に実行することはできません。
- サービスは、クライアントと同じコンピュータで実行する必要があります。

第 3 章 デバイス管理

クライアントは、ネットワークカメラ、DVR（デジタルビデオレコーダー: Digital Video Recorder）、NVR（ネットワークビデオレコーダー: Network Video Recorder）、セキュリティコントロールパネル、ビデオインターコムデバイス、入退室管理デバイスなど、さまざまなタイプのデバイスをサポートしています。

例

クライアントにエンコードデバイスを追加した後にライブビューまたは再生を表示できます。セキュリティコントロールパネルのゾーンの警戒を開始したり警戒解除することができます。クライアントにセキュリティコントロールパネルを追加した後にアラーム通知を受信できます。また、クライアントに入退室管理デバイスを追加した後に入口および出口を制御したり、出勤を管理できます。

3.1 デバイスのアクティベーション

非アクティブなデバイスの場合、それらをソフトウェアに追加して適切に動作させるためには、デバイスをアクティベートするためのパスワードを作成するように求められます。

始める前に

アクティベートするデバイスがネットワークに接続されていて、クライアントを実行している PC と同じサブネットにあることを確認してください。

手順

注記

使用するデバイスがこの機能に対応している必要があります。

1.[デバイス管理] ページを表示します。
2.右側のパネルの上にある **[デバイス]** タブをクリックします。
3.**[オンラインデバイス]** をクリックして、ページ下部のオンラインデバイスのエリアを表示します。
検索したオンラインデバイスがリスト内に表示されます。
4.デバイスのステータス（**[セキュリティレベル]** 列に表示）を確認し、非アクティブなデバイスを選択します。

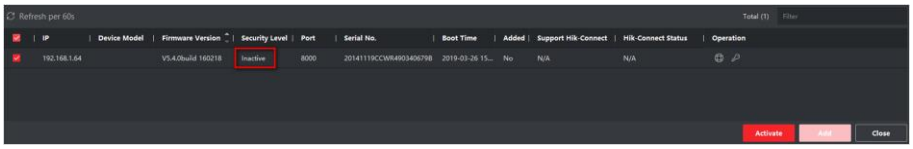

図 3-1 オンラインの非アクティブデバイス

5.**[アクティベート]** をクリックして [アクティベーション] ダイアログを開きます。
6.パスワードフィールドに新たなパスワードを入力し、パスワードを確認します。

⚠注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

7.オプション: NVR デバイスを非アクティブなネットワークカメラに接続する場合は、**[ネットワークカメラのデフォルトパスワード]** フィールドでパスワードを作成し、確認パスワードを入力して、NVR 経由でネットワークカメラをアクティベートします。
8.オプション: デバイスをアクティベートするときにクラウド P2P サービスを有効にします（デバイスがをサポートしている場合）。
1）**[Enable Cloud P2P（クラウド P2P を有効化）]** にチェックを入れて、[メモ] ダイアログを開きます。
2）確認コードを作成します。
3）確認コードを確認します。
4）**[サービス利用規約]** と **[プライバシーポリシー]** をクリックして、条件を読みます。
5）**[OK]** をクリックして、クラウド P2P サービスを有効にします。
9.**[OK]** をクリックしてデバイスをアクティベートします。

3.2 デバイスの追加

クライアントは、IP / ドメイン、IP セグメント、クラウド P2P、ISUP プロトコル、HiDDNS など、さまざまなデバイス追加モードを提供しています。クライアントは、追加するデバイスが大量にある場合に複数のデバイスを一括でインポートすることもサポートしています。

3.2.1 オンラインデバイスの追加

クライアントソフトウェアと同じローカルサブネットに属するアクティブなオンラインデバイスは、**[オンラインデバイス]** エリアに表示されます。**[60 秒ごとに更新]** をクリックして、オンラインデバイスの情報を更新できます。

検出されたオンラインデバイスの追加

オンラインデバイスリストに表示されている検出されたオンラインデバイスを選択して、クライアントに追加できます。

手順

1.[デバイス管理] モジュールを表示します。
2.右側のパネルの上にある **[デバイス]** タブをクリックします。
3.**[オンラインデバイス]** をクリックし、オンラインデバイスエリアを表示します。
検索したオンラインデバイスがリスト内に表示されます。
4.**[オンラインデバイス]** エリアでオンラインデバイスを選択し、**[追加]** をクリックしてデバイスの追加ウィンドウを開きます。

注記

非アクティブなデバイスを使用する場合、デバイスの追加にはパスワードの作成が必要になります。詳細な手順については、「*デバイスのアクティベーション*」をご覧ください。

5.必要な情報を入力します。

名前

デバイスの内容を示す名前を入力します。

IP アドレス

デバイスの IP アドレスを入力します。この追加モードでは、デバイスの IP アドレスが自動的に取得されます。

ポート

ポート番号をカスタマイズできます。この追加モードでは、デバイスのポート番号が自動的に取得されます。

ユーザー名

デフォルトのユーザー名は ***admin*** です。

パスワード

デバイスのパスワードを入力します。

⚠注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

6.オプション: セキュリティを確保するために TLS（トランスポートレイヤーセキュリティ）プロトコルを使用して伝送暗号化を有効化するには、**[伝送暗号化（TLS）]** にチェックを入れます。

注記

- 使用するデバイスがこの機能に対応している必要があります。
- [証明書確認] を有効にした場合は、**[証明書ディレクトリを開く]** をクリックしてデフォルトフォルダを開き、デバイスからエクスポートした証明書ファイルをこのデフォルトディレクトリにコピーしてセキュリティを強化してください。証明書確認を有効にする方法の詳細については、「***伝送暗号化の証明書検証***」をご覧ください。
- デバイスにログインすると、ウェブブラウザで証明書ファイルを入手できます。

7.デバイスをクライアントに追加した後、**[時刻を同期]** にチェックを入れると、クライアントを実行中の PC とデバイスの時刻を同期できます。

8.オプション: **[グループにインポート]** にチェックを入れて、デバイス名でグループを作成し、デバイスのすべてのチャンネルをこのグループにインポートします。

例

エンコードデバイスの場合は、エンコードチャンネルとアラーム入力 / 出力がこのグループにインポートされます。
入退室管理デバイスの場合は、アクセスポイント、アラーム入力 / 出力、およびエンコードチャンネル（存在する場合）がこのグループにインポートされます。

9.**[追加]** をクリックします。

10.オプション: 以下の操作を実行します。

リモート設定 [Operation（操作）] 列で⚙をクリックし、対応するデバイスの

リモート機能を設定します。

注記

詳細については、デバイスのユーザーマニュアルをご覧ください。

デバイスの状態	[Operation（操作）] 列でをクリックすると、カメラ、録画ステータス、信号ステータス、ハードウェアステータスなど、デバイスの各種ステータスを確認できます。
デバイス情報の編集	[Operation（操作）] 列でをクリックすると、IP アドレス、ユーザー名、パスワードなどの各種デバイス情報を編集できます。
オンラインユーザーの確認	[Operation（操作）] 列でをクリックすると、ユーザー名、ユーザータイプ、ユーザーの IP アドレス、ログイン時刻など、デバイスにアクセスするオンラインユーザーを確認できます。
更新	[Operation（操作）] 列でをクリックすると、最新のデバイス情報を取得できます。
デバイスを削除	1 つ以上のデバイスを選択して **[削除]** をクリックすると、選択したデバイスをクライアントから削除できます。

複数の検出されたオンラインデバイスの追加

同じユーザー名とパスワードを共有している検出されたオンラインデバイスの場合は、それらをクライアントに一括で追加できます。

始める前に

追加するデバイスがオンラインになっていることを確認してください。

手順

1.[デバイス管理] モジュールを表示します。
2.右側のパネルの上にある **[デバイス]** タブをクリックします。
3.**[オンラインデバイス]** をクリックして、ページ下部のオンラインデバイスのエリアを表示します。
検索したオンラインデバイスがリスト内に表示されます。
4.複数のデバイスを選択します。

注記

非アクティブなデバイスを使用する場合、デバイスの追加にはパスワードの作成が必要になります。詳細については、「*デバイスのアクティベーション*」をご覧ください。

5.**[追加]** をクリックしてデバイスの追加ウィンドウを開きます。
6.必要な情報を入力します。

ユーザー名

デフォルトのユーザー名は ***admin*** です。

パスワード

デバイスのパスワードを入力します。

注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

7.オプション: デバイスをクライアントに追加した後、**[時刻を同期]** にチェックを入れると、クライアントを実行中の PC とデバイスの時刻を同期できます。
8.オプション: **[グループにインポート]** にチェックを入れて、デバイス名でグループを作成し、デバイスのすべてのチャンネルをこのグループにインポートします。

例

エンコードデバイスの場合は、エンコードチャンネルとアラーム入力 / 出力がこのグループにインポートされます。
入退室管理デバイスの場合は、アクセスポイント、アラーム入力 / 出力、およびエンコードチャンネル（存在する場合）がこのグループにインポートされます。
9.**[追加]** をクリックして、デバイスを追加します。
10.オプション: 以下の操作を実行します。

リモート設定 [Operation（操作）] 列で⚙をクリックし、対応するデバイスのリモート機能を設定します。

注記

詳細については、デバイスのユーザーマニュアルをご覧ください。

デバイスの状態	[Operation（操作）] 列でをクリックすると、カメラ、録画ステータス、信号ステータス、ハードウェアステータスなど、デバイスの各種ステータスを確認できます。
デバイス情報の編集	[Operation（操作）] 列でをクリックすると、IP アドレス、ユーザー名、パスワードなどの各種デバイス情報を編集できます。
オンラインユーザーの確認	[Operation（操作）] 列でをクリックすると、ユーザー名、ユーザータイプ、ユーザーの IP アドレス、ログイン時刻など、デバイスにアクセスするオンラインユーザーを確認できます。
更新	[Operation（操作）] 列でをクリックすると、最新のデバイス情報を取得できます。
デバイスを削除	1 つ以上のデバイスを選択して **[削除]** をクリックすると、選択したデバイスをクライアントから削除できます。

3.2.2 IP アドレスまたはドメイン名によるデバイスの追加

追加するデバイスの IP アドレスやドメイン名がわかっている場合、IP アドレス（またはドメイン名）、ユーザー名、パスワードなどを指定することで、デバイスをクライアントに追加できます。

手順

1.[デバイス管理] モジュールを表示します。
2.右側のパネルの上にある **[デバイス]** タブをクリックします。
追加したデバイスは右側のパネルに表示されています。
3.**[追加]** をクリックして [追加] ウィンドウを開き、追加モードで **[IP / ドメイン]** を選択します。
4.必要な情報を入力します。

名前

デバイスの内容を示す名前を作成します。例えば、デバイスの場所や特徴を示すニックネームも使用できます。

住所

デバイスの IP アドレスまたはドメイン名です。

ポート

追加するデバイスのポート番号はすべて同じです。デフォルト値は ***8000*** です。

ユーザー名

デバイスのユーザー名を入力します。デフォルトのユーザー名は ***admin*** です。

パスワード

デバイスのパスワードを入力します。

注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

5.オプション: オフラインデバイスを追加します。

1）**[オフラインデバイスを追加]** にチェックを入れます。

2）デバイスのチャンネル番号やアラーム入力番号など、必要な情報を入力します。

注記

オフラインデバイスをクライアントに追加した後、デバイスのネットワーク状態は [オフライン] になります。デバイスがオンラインになると、デバイスのネットワーク状態は [オンライン] になり、クライアントはそのデバイスを自動的に接続します。

6.オプション: セキュリティを確保するために TLS（トランスポートレイヤーセキュリティ）プロトコルを使用して伝送暗号化を有効化するには、**[伝送暗号化（TLS）]** にチェックを入れます。

注記

- 使用するデバイスがこの機能に対応している必要があります。
- [証明書確認] を有効にした場合は、**[証明書ディレクトリを開く]** をクリックしてデフォルトフォルダを開き、デバイスからエクスポートした証明書ファイルをこのデフォルトディレクトリにコピーしてセキュリティを強化してください。証明書確認を有効にする方法の詳細については、「*伝送暗号化の証明書検証*」をご覧ください。
- デバイスにログインすると、ウェブブラウザで証明書ファイルを入手できます。

7.デバイスをクライアントに追加した後、**[時刻を同期]** にチェックを入れると、クライアントを実行中の PC とデバイスの時刻を同期できます。

8.オプション: **[グループにインポート]** にチェックを入れて、デバイス名でグループを作成し、デバイスのすべてのチャンネルをこのグループにインポートします。

例

エンコードデバイスの場合は、エンコードチャンネルとアラーム入力 / 出力がこのグループにインポートされます。

入退室管理デバイスの場合は、アクセスポイント、アラーム入力 / 出力、およびエンコードチャンネル（存在する場合）がこのグループにインポートされます。

9.デバイスの追加を終了します。

- **[追加]** をクリックすると、そのデバイスが追加され、デバイスリストのページに戻ります。
- **[Add and New（追加および新規）]** をクリックすると、その設定が保存され、続けて他のデバイスを追加できます。

10.オプション: 以下の操作を実行します。

リモート設定	[Operation（操作）] 列でをクリックし、対応するデバイスのリモート機能を設定します。
	注記 リモート設定の詳細な操作手順については、デバイスのユーザーマニュアルをご覧ください。
デバイスの状態	[Operation（操作）] 列でをクリックすると、カメラ、録画ステータス、信号ステータス、ハードウェアステータスなど、デバイスの各種ステータスを確認できます。
デバイス情報の編集	[Operation（操作）] 列でをクリックすると、IP アドレス、ユーザー名、パスワードなどの各種デバイス情報を編集できます。
オンラインユーザーの確認	[Operation（操作）] 列でをクリックすると、ユーザー名、ユーザータイプ、ユーザーの IP アドレス、ログイン時刻など、デバイスにアクセスするオンラインユーザーを確認できます。
更新	[Operation（操作）] 列でをクリックすると、最新のデバイス情報を取得できます。
デバイスを削除	1 つ以上のデバイスを選択して **[削除]** をクリックすると、選択したデバイスをクライアントから削除できます。

3.2.3 IP セグメントによるデバイスの追加

複数のデバイスが同じポート番号、ユーザー名とパスワード、および同じ IP セグメント内の IP アドレス範囲を共有している場合は、デバイスの開始 IP アドレスと終了 IP アドレス、ポート番号、ユーザー名、パスワードなどを指定して、それらをクライアントに追

加できます。

手順

1.[デバイス管理] モジュールを表示します。
2.右側のパネルの上にある **[デバイス]** タブをクリックします。
追加したデバイスは右側のパネルに表示されています。
3.**[追加]** をクリックし、[追加] ウィンドウを開きます。

4.**[IP セグメント]** を追加モードとして選択します。
5.必要な情報を入力します。

開始 IP

開始 IP アドレスを入力します。

終了 IP

開始 IP と同じネットワークセグメント内に存在する終了 IP アドレスを入力します。

ポート

デバイスのポート番号を入力します。デフォルト値は ***8000*** です。

ユーザー名

デフォルトのユーザー名は ***admin*** です。

パスワード

デバイスのパスワードを入力します。

⚠注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

6.オプション: オフラインデバイスを追加します。
1）**[オフラインデバイスを追加]** にチェックを入れます。
2）デバイスのチャンネル番号やアラーム入力番号など、必要な情報を入力します。

注記

オフラインデバイスをクライアントに追加した後、デバイスのネットワーク状態は [オフライン] になります。デバイスがオンラインになると、デバイスのネットワーク状態は [オンライン] になり、クライアントはそのデバイスを自動的に接続します。

7.オプション: セキュリティを確保するために TLS（トランスポートレイヤーセキュリティ）プロトコルを使用して伝送暗号化を有効化するには、**[伝送暗号化（TLS）]** にチェックを入れます。

注記

- 使用するデバイスがこの機能に対応している必要があります。
- [証明書確認] を有効にした場合は、**[証明書フォルダを開く]** をクリックしてデフォルトフォルダを開き、デバイスからエクスポートした証明書ファイルをこのデフォルトディレクトリにコピーしてセキュリティを強化してください。証明書確認を有効にする方法の詳細については、「*伝送暗号化の証明書検証*」をご覧ください。
- デバイスにログインすると、ウェブブラウザで証明書ファイルを入手できます。

8.デバイスをクライアントに追加した後、**[時刻を同期]** にチェックを入れると、クライアントを実行中の PC とデバイスの時刻を同期できます。

9.オプション: **[グループにインポート]** にチェックを入れて、デバイス名でグループを作成し、デバイスのすべてのチャンネルをこのグループにインポートします。

10.デバイスの追加を終了します。

– **[追加]** をクリックすると、そのデバイスが追加され、デバイスリストのページに戻ります。
– **[Add and New（追加および新規）]** をクリックすると、その設定が保存され、続けて他のデバイスを追加できます。

11.オプション: 以下の操作を実行します。

リモート設定 [Operation（操作）] 列で⚙をクリックし、対応するデバイスのリモート機能を設定します。

注記

リモート設定の詳細な操作手順については、デバイスのユーザーマニュアルをご覧ください。

デバイスの状態 [Operation（操作）] 列で▤をクリックすると、カメラ、録画ステータス、信号ステータス、ハードウェアステータスなど、デバイスの各種ステータスを確認できます。

デバイス情報の編 [Operation（操作）] 列で✎をクリックすると、IP アドレス、ユ

集	ーザー名、パスワードなどの各種デバイス情報を編集できます。
オンラインユーザーの確認	[Operation（操作）] 列でをクリックすると、ユーザー名、ユーザータイプ、ユーザーの IP アドレス、ログイン時刻など、デバイスにアクセスするオンラインユーザーを確認できます。
更新	[Operation（操作）] 列でをクリックすると、最新のデバイス情報を取得できます。
デバイスを削除	1 つ以上のデバイスを選択して **[削除]** をクリックすると、選択したデバイスをクライアントから削除できます。

3.2.4 クラウド P2P によるデバイスの追加

デバイスがクラウド P2P をサポートしていて、そのクラウド P2P 機能が有効になっている場合は、クラウド P2P モードでそれをクライアントとクラウド P2P アカウントの両方に追加できます。クラウド P2P アカウントにすでに追加されているデバイスの場合は、クラウド P2P アカウントにログインした後にそれらをクライアントに追加できます。

始める前に

クラウド P2P アカウントが登録済みで、クラウド P2P アカウントにログインしていることを確認してください。

手順

1.[デバイス管理] モジュールを表示します。
追加したデバイスは右側のパネルに表示されています。
2.右側のパネルの上にある **[デバイス]** タブをクリックします。
3.**[追加]** をクリックし、[追加] ウィンドウを開きます。
4.追加モードとして **[クラウド P2P]** を選択します。
- 初めての場合は、クラウド P2P アカウントにログインするように求められます。
- ログインしているクラウド P2P アカウントが表示されます。

5.**[ログインする地域を選択します]** のドロップダウンリストからログインする地域を選択して、クラウド P2P アカウントにログインするか、デバイスのシリアル番号を入力します。
- デバイスラベルに記載されているシリアル番号を入力します。
- デバイスの IP アドレスがクライアントと同じローカルサブネットにある場合は、**[オンラインデバイス]** をクリックし、オンラインデバイスを選択してシリアル番号を自動的に取得します。

6.デバイスの確認コードを入力します。

注記

デバイスをアクティベートしてクラウド P2P サービスを有効にするときに確認コードを作成できます。これは、ストリーム暗号化を有効にするときに作成される確認コードと同じです。デバイス設定ページでこれを作成することもできます。

7.オプション: **DDNS** を有効にして、クラウド P2P ドメインによってデバイスにアクセスします。

デバイスのドメイン名

デバイスドメイン名をカスタマイズします。これは、クラウド P2P サーバーに登録されているデバイスの IP アドレスとポートを取得するのに使用されます。

UPnP モード

自動

デバイスのポート番号を自動的に取得するには、[UPnP モード] で **[自動]** を選択します。

手動

UPnP モードとして **[手動]** を選択します。この場合は、デバイスのポート番号を手動で入力する必要があります。

ユーザー名

デバイスのユーザー名を入力します。デフォルトのユーザー名は ***admin*** です。

パスワード

デバイスをアクティベートしたときに作成したデバイスのパスワードを入力します。

注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

注記

DDNS 機能が無効になっている場合は、デバイス状態の表示、リモート再生中のビデオファイルのダウンロード、デバイスの QR コードの生成など、追加したデバイスの一部の操作をクライアント経由で実行できません。

8.オプション: **[グループにインポート]** にチェックを入れて、クラウド P2P アカウント名でグループを作成し、デバイスのすべてのチャンネルをこのグループにインポートします。
9.デバイスをクライアントソフトウェアとクラウド P2P アカウントに追加します。
- **[追加]** をクリックすると、デバイスが追加され、デバイスリストに戻ります。
- **[追加および新規]** をクリックすると、デバイスが追加され、続けて次のデバイスを追加できます。

10.オプション: 以下の操作を実行します。

リモート設定	[Operation（操作）] 列で⚙をクリックし、対応するデバイスのリモート機能を設定します。
	注記 リモート設定の詳細な操作手順については、デバイスのユーザーマニュアルをご覧ください。
デバイス情報の編集	✎をクリックしてデバイスの詳細を編集します。
デバイスを削除	1 つ以上のデバイスを選択して **[削除]** をクリックすると、選択したデバイスをクライアントから削除できます。

3.2.5 ISUP アカウントによるデバイスの追加

ISUP 5.0 プロトコルをサポートしている入退室管理デバイスの場合、それらのサーバーアドレス、ポート番号、およびデバイス ID が設定済みであれば、デバイス ID とキーを入力した後に ISUP プロトコルでそれらをクライアントに追加できます。

始める前に

デバイスがネットワークに正しく接続されていることを確認してください。

手順

1.[デバイス管理] モジュールを表示します。
追加したデバイスは右側のパネルに表示されています。
2.**[追加]** をクリックし、[追加] ウィンドウを開きます。

3.追加モードとして **[ISUP]** を選択します。
4.必要な情報を入力します。

デバイスアカウント

ISUP プロトコルに登録済みのアカウント名を入力します。

ISUP キー

ISUP 5.0 デバイスで、デバイスのネットワークセンターのパラメータを設定したときに ISUP キーを設定した場合は、それを入力します。

注記

使用するデバイスがこの機能に対応している必要があります。

5.オプション: デバイスをクライアントに追加した後、**[時刻を同期]** にチェックを入れると、クライアントを実行中の PC とデバイスの時刻を同期できます。
6.オプション: **[グループにインポート]** にチェックを入れて、デバイス名でグループを作成し、デバイスのすべてのチャンネルをこのグループにインポートします。
7.デバイスの追加を終了します。
- **[追加]** をクリックすると、デバイスが追加されて、デバイスリストに戻ります。
- **[Add and New（追加および新規）]** をクリックすると、その設定が保存され、続けて他のデバイスを追加できます。

注記

DS-K1T671 シリーズおよび DS-K1T331 シリーズを除き、ISUP アカウントで追加したデバイスには顔画像を適用できません。

8.オプション: 以下の操作を実行します。

デバイスの状態	[Operation（操作）] 列でをクリックすると、デバイスのステータスを確認できます。
デバイス情報の編集	［操作］列で をクリックすると、デバイス名、デバイスアカウント、ISUP キーなどの各種デバイス情報を編集できます。
オンラインユーザーの確認	[Operation（操作）] 列でをクリックすると、ユーザー名、ユーザータイプ、ユーザーの IP アドレス、ログイン時刻など、デバイスにアクセスするオンラインユーザーを確認できます。
更新	[Operation（操作）] 列でをクリックすると、最新のデバイス情報を取得できます。
デバイスを削除	1 つ以上のデバイスを選択して **[削除]** をクリックすると、選択したデバイスをクライアントから削除できます。

3.2.6 HiDDNS によるデバイスの追加

HiDDNS は、Hikvision の無料の DNS サーバーです。デバイス用の十分な IP アドレスがない場合は、デバイスを HiDDNS サーバーに登録した後に、HiDDNS モードでデバイスをクライアントに追加できます。HiDDNS は、ドメイン名をデバイスの IP アドレスとして解析して、ネットワークへの良好な接続を実現します。

手順

1.[デバイス管理] モジュールを表示します。
追加したデバイスは右側のパネルに表示されています。
2.右側のパネルの上にある **[デバイス]** タブをクリックします。
3.**[追加]** をクリックし、[追加] ウィンドウを開きます。
4.追加モードとして **[HiDDNS]** を選択します。
5.必要な情報を入力します。

サーバーアドレス

www.hik-online.com

ドメイン

HiDDNS サーバーに登録したデバイスのドメイン名を入力します。

ユーザー名

デバイスのユーザー名を入力します。

パスワード

デバイスのパスワードを入力します。

⚠注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

6.オプション: オフラインデバイスを追加します。
1）**[オフラインデバイスを追加]** にチェックを入れます。
2）デバイスのチャンネル番号やアラーム入力番号など、必要な情報を入力します。

注記

オフラインデバイスをクライアントに追加した後、デバイスのネットワーク状態は [オフライン] になります。デバイスがオンラインになると、デバイスのネットワーク状態は [オンライン] になり、クライアントはそのデバイスを自動的に接続します。

7.オプション: デバイスをクライアントに追加した後、**[時刻を同期]** にチェックを入れると、クライアントを実行中の PC とデバイスの時刻を同期できます。
8.オプション: **[グループにインポート]** にチェックを入れて、デバイス名でグループを作成し、デバイスのすべてのチャンネルをこのグループにインポートします。
9.デバイスの追加を終了します。
- **[追加]** をクリックすると、そのデバイスが追加され、デバイスリストのページに戻ります。
- **[Add and New（追加および新規）]** をクリックすると、その設定が保存され、続けて他のデバイスを追加できます。

10.オプション: 以下の操作を実行します。

リモート設定	[Operation（操作）] 列でをクリックし、対応するデバイスのリモート機能を設定します。 **注記** リモート設定の詳細な操作手順については、デバイスのユーザーマニュアルをご覧ください。
デバイスの状態	[Operation（操作）] 列でをクリックすると、カメラ、録画ステータス、信号ステータス、ハードウェアステータスなど、デバイスの各種ステータスを確認できます。
デバイス情報の編集	[Operation（操作）] 列でをクリックすると、IP アドレス、ユーザー名、パスワードなどの各種デバイス情報を編集できます。
オンラインユーザーの確認	[Operation（操作）] 列でをクリックすると、ユーザー名、ユーザータイプ、ユーザーの IP アドレス、ログイン時刻など、デバイスにアクセスするオンラインユーザーを確認できます。
更新	[Operation（操作）] 列でをクリックすると、最新のデバイス情報を取得できます。
デバイスを削除	1 つ以上のデバイスを選択して **[削除]** をクリックすると、選択したデバイスをクライアントから削除できます。

3.2.7 デバイスの一括インポート

定義済みの CSV ファイルにデバイスパラメータを入力することで、複数のデバイスをクライアントに一括で追加できます。

手順

1.[デバイス管理] モジュールを表示します。
2.右側のパネルの上にある **[デバイス]** タブをクリックします。
3.**[追加]** をクリックして [追加] ウィンドウを開き、追加モードで **[一括インポート]** を選択します。

4.**[エクスポートテンプレート]** をクリックし、定義済みのテンプレート（CSV ファイル）をお使いの PC に保存します。
5.エクスポートしたテンプレートファイルを開き、追加するデバイスの必要情報を対応する列に入力します。

注記

必須フィールドの詳細については、テンプレートの概要説明をご覧ください。

モードを追加中

0、***1***、または ***2*** を入力します。

住所

デバイスのアドレスを編集します。

ポート

デバイスのポート番号を入力します。デフォルトのポート番号は ***8000*** です。

ユーザー名

デバイスのユーザー名を入力します。デフォルトのユーザー名は ***admin*** です。

パスワード

デバイスのパスワードを入力します。

注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

オフラインデバイスを追加

オフラインデバイスの追加を有効にするには、***1*** を入力します。
オフラインデバイスをクライアントに追加した後、デバイスのネットワーク状態は [オフライン] になります。デバイスがオンラインになると、デバイスのネットワーク状態は [オンライン] になり、クライアントはそのデバイスを自動的に接続します。オフラインデバイスの追加を無効にするには、***0*** を入力します。

グループにインポート

デバイス名でグループを作成するには、***1*** を入力します。デバイスのチャンネルはすべて、対応するグループにデフォルトでインポートされます。この機能を無効にするには、***0*** を入力します。

チャンネル番号

[オフラインデバイスを追加] を有効にした場合は、デバイスのチャンネル番号を入力します。**[オフラインデバイスを追加]** を無効にした場合は、このフィールドを指定する必要はありません。

アラーム入力番号

[オフラインデバイスを追加] を有効にした場合は、デバイスのアラーム入力番号を入力します。**[オフラインデバイスを追加]** を無効にした場合は、このフィールドを指定する必要はありません。

6. ··· をクリックしてテンプレートファイルを選択します。
7. **[追加]** をクリックし、デバイスをインポートします。
8. オプション: 以下の操作を実行します。

リモート設定	[Operation（操作）] 列で ⚙ をクリックし、対応するデバイスのリモート機能を設定します。

注記

リモート設定の詳細な操作手順については、デバイスのユーザーマニュアルをご覧ください。

デバイスの状態	[Operation（操作）] 列でをクリックすると、カメラ、録画ステータス、信号ステータス、ハードウェアステータスなど、デバイスの各種ステータスを確認できます。
デバイス情報の編集	[Operation（操作）] 列でをクリックすると、IP アドレス、ユーザー名、パスワードなどの各種デバイス情報を編集できます。
オンラインユーザーの確認	[Operation（操作）] 列でをクリックすると、ユーザー名、ユーザータイプ、ユーザーの IP アドレス、ログイン時刻など、デバイスにアクセスするオンラインユーザーを確認できます。
更新	[Operation（操作）] 列でをクリックすると、最新のデバイス情報を取得できます。
デバイスを削除	1 つ以上のデバイスを選択して **[削除]** をクリックすると、選択したデバイスをクライアントから削除できます。

3.3 デバイスのネットワーク情報の編集

デバイスをアクティベートした後に、オンラインデバイスのネットワーク情報（IP アドレス、ポート番号、ゲートウェイなど）を編集できます。

始める前に

デバイスの状態が非アクティブの場合は、デバイスをアクティベートします。

手順

1.[デバイス管理] ページを表示します。
2.右側のパネルの上にある **[デバイス]** タブをクリックします。
3.**[オンラインデバイス]** をクリックし、オンラインデバイスエリアを表示します。
同じサブネットを共有しているすべてのオンラインデバイスがリストに表示されます。
4.**[オンラインデバイス]** エリアでアクティベートされたデバイスを選択します。
5.［操作］列で をクリックして、［ネットワークパラメータを変更］ウィンドウを開きます。

注記

この機能は、**[オンラインデバイス]** エリアでのみ使用できます。

6.オプション: デバイスをクライアントに追加する必要がある場合、デバイスの IP アドレスをお使いの PC と同じサブネットに変更してください。
– IP アドレスを手動で編集します。

– **[DHCP]** にチェックを入れて、IP アドレスを静的 IP アドレスとして設定します。

7.デバイスをアクティベートしたときに作成したパスワードを入力します。

注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

8.**[OK]** をクリックしてネットワークの設定を完了します。

3.4 デバイスのパスワードの復元 / リセット

検出されたオンラインデバイスのパスワードを忘れた場合は、クライアント経由でデバイスのデフォルトパスワードを復元するか、デバイスのパスワードをリセットできます。

3.4.1 デバイスのパスワードリセット

検出されたオンラインデバイスのパスワードを忘れた場合は、クライアント経由でそのデバイスのパスワードをリセットできます。

手順

1.[デバイス管理] ページを表示します。
2.右側のパネルの上にある **[デバイス]** タブをクリックします。
3.**[オンラインデバイス]** をクリックし、オンラインデバイスエリアを表示します。
同じサブネットを共有しているすべてのオンラインデバイスがリストに表示されます。
4.リストからデバイスを選択して、[Operation（操作）] 列でをクリックします。
5.デバイスのパスワードをリセットします。
– **[エクスポート]** をクリックしてお使いの PC にデバイスのファイルを保存し、そのファイルを当社のテクニカルサポートへ送信してください。

注記

パスワードをリセットする以下の操作については、当社のテクニカルサポートまでお問い合わせください。

– **[生成]** をクリックして [QR コード] ウィンドウを表示し、**[ダウンロード]** をクリックして QR コードを PC に保存します。QR コードの写真を撮影して、電話に保存する

こともできます。その写真を当社のテクニカルサポートへ送信してください。

注記

パスワードをリセットする以下の操作については、当社のテクニカルサポートまでお問い合わせください。

– 実際の使用状況に応じてセーフモードを選択します。

注記

パスワードをリセットする以下の操作については、当社のテクニカルサポートまでお問い合わせください。

注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

3.4.2 デバイスのデフォルトパスワードの復元

検出したオンラインデバイスのパスワードを忘れた場合、クライアント経由でそのデバイスのデフォルトパスワードを復元できます。

手順

1.[デバイス管理] ページを表示します。
2.右側のパネルの上にある **[デバイス]** タブをクリックします。
3.**[オンラインデバイス]** をクリックして、ページ下部のオンラインデバイスのエリアを表示します。
同じサブネットを共有しているすべてのオンラインデバイスがリストに表示されます。
4.デバイスを選択して、［操作］列の をクリックして［パスワードをリセット］ウィンドウを開きます。
5.デバイスパスワードを復元します。
– セキュリティコードを入力して、選択したデバイスのデフォルトパスワードを復元できます。

注記

セキュリティコードを取得するには、テクニカルサポートにお問い合わせください。

– **[エクスポート]** をクリックしてお使いの PC にデバイスのファイルを保存し、そのファイルを当社のテクニカルサポートへ送信してください。

注記

パスワードをリセットする以下の操作については、当社のテクニカルサポートまでお問い合わせください。

次に行う操作

管理者アカウントのデフォルトのパスワード（12345）は、初回ログイン専用です。製品が正常に機能しなくなったり、その他の望ましくない結果につながる可能性がある製品への不正アクセスなどのセキュリティリスクに対する保護を強化できるように、このデフォルトのパスワードを変更する必要があります。

注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

3.5 デバイスの QR コードの確認

クライアントは、追加されたデバイスの QR コードを生成できます。QR コードをスキャンした後、モバイルクライアントにデバイスを追加できます。

手順

注記

- ISUP プロトコルで追加されたデバイスは、この機能をサポートしていません。
- **DDNS** が有効な状態でクラウド P2P を介して追加されたデバイスは、この機能をサポートしていません。

1.[デバイス管理] モジュールを表示します。
2.右側のパネルの上にある **[デバイス]** タブをクリックします。

追加したデバイスがリスト内に表示されます。

3.1 つまたは複数のデバイスを選択し、[QR コード] をクリックして **[QR コード]** ウィンドウを開きます。

次に行う操作

QR コードをスキャンした後、デバイスをモバイルクライアントに追加します。詳細については、モバイルクライアントのユーザーマニュアルをご覧ください。

3.6 デバイスファームウェアバージョンのアップグレード

追加したデバイス用の利用可能な新しいファームウェアバージョンがある場合は、クライアント経由でファームウェアバージョンをアップグレードできます。

注記

- デバイスがこの機能をサポートしている必要があります。
- アップグレードモードは、システム設定で設定できます。詳細については、「*全般パラメータの設定*」をご覧ください。

[デバイス管理] モジュールを表示して、**[デバイス]** タブをクリックしてデバイスリストを表示します。

各種アップグレードモードに応じて、以下の操作を実行します。

無効

[管理用のデバイス] パネルで、新しいバージョンのファームウェアが利用可能な場合は、デバイスの [ファームウェアアップグレード] 列の状態が **[アップグレード可能]** になります。

アップグレード可能なデバイスを選択して、**[アップグレード]** をクリックしてデバイスファームウェアのアップグレードを開始します。

注記

アップグレードの進行状況が表示されます。アップグレードが完了すると、デバイスの [ファームウェアアップグレード] 列の状態が **[アップグレードしました]** に変わります。

Prompt Me If Download and Upgrade（ダウンロードとアップグレードの実行確認を表示）

利用可能な新しいバージョンのファームウェアがある場合は、プロンプトウィンドウが表示されます。**[すべてアップグレード]** をクリックして、ダウンロードとアップグレードを開始します。

Download and Prompt Me If Upgrade（ダウンロードして、アップグレードの実

行確認を表示）

新しいバージョンのパッケージをダウンロードした後に、アップグレードするかどうかを選択するダイアログが表示されます。**[すべてアップグレード]** をクリックして、デバイスファームウェアのアップグレードを開始します。

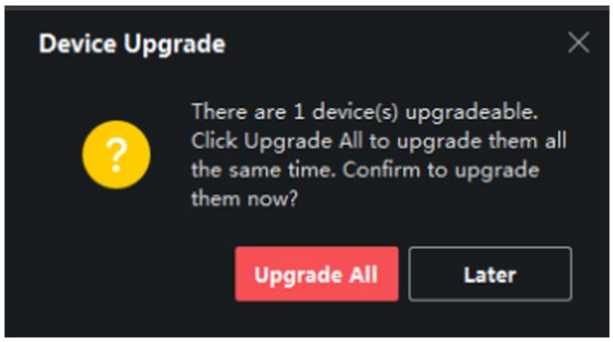

図 3-2 デバイスアップグレードのプロンプト

注記

[すべてアップグレード] をクリックすると、詳細表示用のプロンプトが表示されます。[デバイス管理] ページを表示していない場合は、**[詳細を表示]** をクリックして [デバイス管理] ページにジャンプします。[デバイス管理] ページを表示している場合は、プロンプトを閉じます。

Download and Update Automatically（自動的にダウンロードしてアップグレード）

クライアントは、新しいバージョンのデバイスを検出すると、ユーザーに通知することなく、新しいバージョンをダウンロードして、アップグレードします。
デバイス管理ページの [Firmware Update（ファームウェアアップデート）] 列に、次のアップデート状態が表示されます。

利用可能なバージョンがありません

新しいバージョンのファームウェアがありません。

アップグレード可能

新しいバージョンのファームウェアが利用可能です。

注記

カーソルを の上に移動すると、現在のバージョン、最新バージョン、およびファームウェアバージョンのアップグレード内容が表示されます。

待機中

デバイスはアップグレードを待機しています。

ダウンロード中

クライアントは新しいバージョンのファームウェアのパッケージをダウンロードしています。

アップグレード中

デバイスファームウェアのアップグレードが進行中です。

アップグレードしました

[アップグレードしました] にカーソルを合わせると、アップグレード後のバージョンが表示されます。

アップグレード失敗

アップグレードに失敗すると、詳細表示用のプロンプトが表示されます。[デバイス管理] ページを表示していない場合は、**[詳細を表示]** をクリックして [デバイス管理] ページにジャンプします。[デバイス管理] ページを表示している場合は、プロンプトを閉じます。**[アップグレードに失敗しました]** の上にカーソルを合わせてエラーの詳細を表示し、**[再度アップグレード]** をクリックして再試行します。

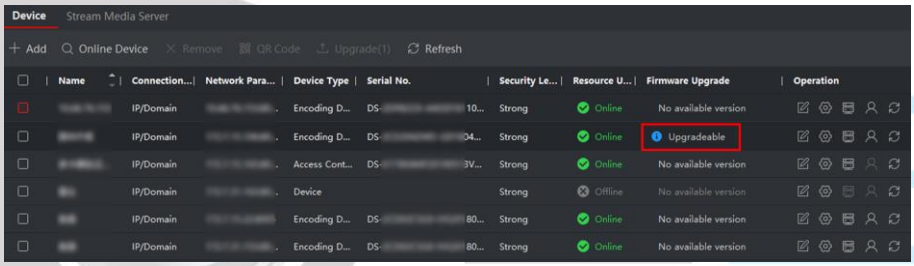

図 3-3 ファームウェアのアップグレード

第 4 章 グループ管理

クライアントは、追加したリソースをさまざまなグループで管理するためのグループを提供します。リソースの場所に応じて、リソースをさまざまなグループにグループ化できます。

例

例えば、1 階に 64 台のカメラ、16 個のドア、64 個のアラーム入力、16 個のアラーム出力がある場合、これらのリソースを 1 つのグループ（「1 階」という名前）に編成して、管理しやすくすることができます。リソースをグループで管理するようにした後に、ライブビューを取得したり、ビデオファイルを再生したり、ドアの状態を制御したり、デバイスのその他の操作を実行することができます。

4.1 グループの追加

グループを追加して、追加したデバイスを編成して、管理しやすくすることができます。

手順

1.[デバイス管理] モジュールを表示します。
2.**[デバイス管理] → [グループ]** の順にクリックして、グループ管理ページを表示します。
3.グループを作成します。
- **[グループを追加]** をクリックして、目的のグループ名を入力します。
- **[デバイス名別にグループを作成]** をクリックして、追加したデバイスを選択して、選択したデバイスの名前別で新しいグループを作成します。

注記

このデバイスのリソース（エンコードチャンネル、アラーム入力 / 出力、アクセスポイントなど）は、デフォルトでグループにインポートされます。

4.2 グループへのリソースのインポート

デバイスリソース（エンコードチャンネル、アラーム入力 / 出力、アクセスポイントなど）を追加したグループに一括でインポートできます。

始める前に

デバイスを管理するためのグループを追加します。「*グループの追加*」をご覧ください。

手順

1.[デバイス管理] モジュールを表示します。
2.**[デバイス管理] → [グループ]** の順にクリックして、グループ管理ページを表示します。

3.グループリストからグループを選択し、**[エンコードチャンネル]**、**[アラーム入力]**、**[アラーム出力]**、**[ゾーン]**、**[アクセスポイント]** などのリソースタイプを選択します。
4.**[インポート]** をクリックします。
5.サムネイルビュー / リストビューで、リソースのサムネイル / 名前を選択します。

注記

または をクリックして、リソース表示モードをサムネイルビューまたはリストビューに切り替えることができます。

6.**[インポート]** をクリックして、選択したリソースをグループにインポートします。

4.3 リソースパラメータの編集

リソースをグループにインポートした後、リソースパラメータを編集できます。エンコードチャンネルの場合は、チャンネル名、ストリームタイプ、プロトコルタイプなどを編集できます。アクセスポイントの場合は、アクセスポイント名を編集できます。アラーム入力の場合は、アラーム入力名を編集できます。ここではエンコーディングチャンネルを例にとって説明します。

始める前に

リソースをグループにインポートします。「*グループへのリソースのインポート*」をご覧ください。

手順

1.[デバイス管理] モジュールを表示します。
2.**[デバイス管理]** → **[グループ]** の順にクリックして、グループ管理ページを表示します。
追加したすべてのグループが左側に表示されます。
3.グループリストでグループを選択して、**[エンコードチャンネル]** をクリックします。
グループにインポートされたエンコードチャンネルが表示されます。
4.[操作] 列で をクリックして、[Edit Resource（リソースを編集）] ウィンドウを開きます。
5.カメラ名、ストリームタイプなどのカメラ情報を編集します。

ビデオストリーム

必要に応じて、カメラのライブビューのストリームタイプを選択します。

注記

ライブビューを再起動して有効にしてください。

再生ストリームタイプ

必要に応じて、カメラの再生のストリームタイプを選択します。

注記

- このフィールドは、デバイスがデュアルストリームをサポートしている場合に表示されます。
- ライブビューを再起動して有効にしてください。

回転タイプ

必要に応じて、カメラのライブビューまたは再生の回転タイプを選択します。

プロトコルタイプ

カメラの転送プロトコルを選択します。

注記

ライブビューを再起動して有効にしてください。

ストリーミングプロトコル

ライブビュー時のストリーム取得用のプロトコルとして RTSP またはプライベートを選択します。

注記

ライブビューを再起動して有効にしてください。

ストリームメディアサーバー

ストリームメディアサーバー経由でカメラのストリームを取得します。使用可能なストリームメディアサーバーを選択して管理できます。

コピー先…

設定したパラメータを他のカメラにコピーします。

更新

カメラのライブビューの新しいキャプチャ画像を取得します。

6.**[OK]** をクリックして新しい設定を保存します。

4.4 グループからのリソースの削除

追加したリソースをグループから削除できます。

手順

1.[デバイス管理] モジュールを表示します。

2.**[デバイス管理]** → **[グループ]** の順にクリックして、グループ管理ページを表示します。
追加したすべてのグループが左側に表示されます。

3.グループをクリックして、このグループに追加されたリソースを表示します。

4.リソースを選択し、**[削除]** をクリックして、グループからリソースを削除します。

第 5 章 クラウド P2P

クライアントソフトウェアは、クラウド P2P アカウントの登録、クラウド P2P アカウントへのログイン、クラウド P2P サービスをサポートするデバイスの管理もサポートしています。

5.1 クラウド P2P アカウントの登録

クライアントは、クラウド P2P サービスをサポートするデバイスを管理するためのクラウド P2P アカウントの登録をサポートしています。

手順

1.クラウド P2P のログインページを表示します。

– クライアントの右上隅の **[ログイン]** をクリックします。

1. **[デバイス管理]** → **[デバイス]** の順にクリックして [デバイス管理] ページを表示します。
2. **[追加]** をクリックして [デバイスを追加] パネルを開きます。
3. 追加モードとして **[クラウド P2P]** を選択します。
4. **[ログイン]** をクリックします。

[ログイン] ウィンドウが表示されます。

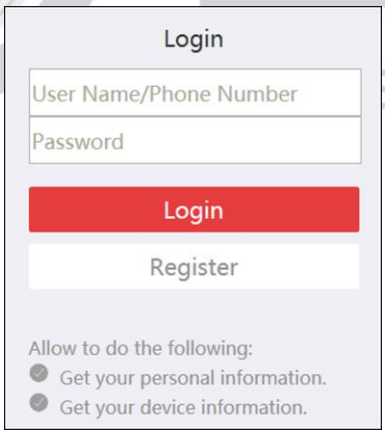

図 5-1 [ログイン] ウィンドウ

2.**[登録]** をクリックして、[Register Account（アカウントを登録）] ウィンドウを開きます。

3.ユーザー名、パスワード、確認パスワード、電話番号 / 電子メールアドレスなど、必要な情報を入力します。

注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

4.**[メッセージを送信]** をクリックして、確認コードを取得します。
システムは、確認コードを電話または電子メールアドレスに送信します。
5.受信した確認コードを **[確認コード]** テキストフィールドに入力します。
6.**[I have read and agreed Terms of Service Privacy Policy（サービス利用規約とプライバシーポリシーを読み、内容に同意しました）]** にチェックを入れます。
7.**[登録]** をクリックして、登録を完了します。

5.2 クラウド P2P アカウントへのログイン

クライアントでクラウド P2P アカウントにログインして、クラウド P2P アカウントで管理するデバイスを操作できます。

始める前に

クラウド P2P アカウントを登録します。

注記

詳細については、「*クラウド P2P アカウントの登録*」をご覧ください。

手順

1.クラウド P2P のログインページを表示します。
– クライアントの右上隅の **[ログイン]** をクリックします。
1. **[デバイス管理]** → **[デバイス]** の順にクリックして [デバイス管理] ページを表示します。
2. **[追加]** をクリックして [デバイスを追加] パネルを開きます。
3. 追加モードとして **[クラウド P2P]** を選択します。
4. **[ログイン]** をクリックします。

[ログイン] ウィンドウが表示されます。
2.ユーザー名 / 電話番号、およびパスワードを入力します。
3.**[ログイン]** をクリックして、アカウントにログインします。

[ログイン] が **[ログインしました]** に変わります。

4.オプション: **[ログインしました]** → **[ログアウト]** の順にクリックして、アカウントからログアウトします。

注記

- クラウド P2P によって追加されたデバイスは、クラウド P2P をログアウトすると非表示になります。
- クラウド P2P に保存されているアラーム関連の画像は 2 時間有効です。

第 6 章 ライブビュー

監視タスクでは、追加したネットワークカメラとビデオエンコーダのライブビデオを [メインビュー] ページに表示できます。また、画像キャプチャ、手動記録、ウィンドウ分割、PTZ 制御、ライブビューでの自動切り替えなど、いくつかの基本操作をサポートしています。

6.1 ライブビューの開始

クライアントにデバイスを追加した後に、ライブビューを開始して、監視エリアを確認することができます。グループ内の 1 台のカメラ、またはすべてのカメラのライブビューを開始できます。また、カスタムビューモードでライブビューを開始することもできます。

注記

デバイスがストリーム暗号化をサポートしていて、そのライブビューのストリームが暗号化されている場合、二段階認証のストリームキーを入力するように求められます。

6.1.1 1 台のカメラのライブビューの開始

1 台のカメラのみのライブビューを開始できます。

始める前に

ライブビュー用にカメラグループを定義する必要があります。

手順

1.[メインビュー] ページを表示します。
2.オプション: ライブビューツールバーの をクリックして、ライブビューのウィンドウ分割モードを選択します。
3.オプション: ライブビューツールバーの をクリックして、表示スケール、再生パフォーマンス、画像の保存パスなどのパラメータを設定します。

注記

パラメータは [システム設定] でも設定できます。詳細については、「*システム設定*」をご覧ください。

4.次のいずれかの操作を実行して、1 台のカメラのライブビューを開始します。
– グループ内のカメラを、リソースリストから表示ウィンドウにドラッグして、ライブビューを開始します。

– 表示ウィンドウを選択した後、カメラ名をダブルクリックして、ライブビューを開始します。
– 表示ウィンドウを選択した後、カーソルをカメラ名に移動し、カメラ名の近くにある をクリックして、ライブビューを開始します。

注記

デバイスがストリーム暗号化をサポートしていて、そのライブビューのストリームが暗号化されている場合、二段階認証のストリームキーを入力するように求められます。

選択したウィンドウでカメラのライブビデオの再生が開始されます。次のウィンドウが自動的に選択されます。

5.オプション: ライブビュー中のカメラのビデオを別のウィンドウにドラッグして、ライブビューの表示ウィンドウを変更します。
6.オプション: カーソルをカメラ名に移動し、カメラ名の近くにある → [**ストリーム**] の順にクリックして、実際の使用状況に応じてストリームタイプを切り替えます。

注記

[すべてのストリームタイプ] をクリックして、右クリックメニューに表示する使用頻度の高いストリームタイプを選択できます。

6.1.2 カメラグループのライブビューの開始

1 つのグループ内のすべてのカメラのライブビューを同時に開始できます。

始める前に

ライブビュー用にカメラグループを定義する必要があります。

手順

1.[メインビュー] ページを表示します。
2.オプション: ライブビューツールバーの をクリックして、表示スケール、再生パフォーマンス、画像の保存パスなどのパラメータを設定します。

注記

パラメータは [システム設定] でも設定できます。詳細については、「*システム設定*」をご覧ください。

3.次のいずれかの操作を実行して、グループ内のすべてのカメラのライブビューを開始します。
– カメラグループを、カメラリストから表示ウィンドウにドラッグして、ライブビューを開始します。
– グループ名をダブルクリックして、ライブビューを開始します。

– カーソルをグループ名に移動し、グループ名の近くにある をクリックして、グループ内のすべてのカメラのライブビューを開始します。

注記

- 表示ウィンドウ番号は、グループ内のカメラの数に応じて自動的に調整されます。
- デバイスがストリーム暗号化をサポートしていて、そのライブビューのストリームが暗号化されている場合、二段階認証のストリームキーを入力するように求められます。

4.オプション: カーソルをグループ名に移動し、グループ名の近くにある → [**ストリーム**] の順にクリックして、実際の使用状況に応じてグループ内のカメラのストリームタイプを切り替えます。

注記

6 番目、7 番目、8 番目、9 番目、10 番目のストリームに切り替える前に、デバイスの Web 設定ページでこれらのストリームタイプを設定する必要があります。詳細については、デバイスのユーザーマニュアルをご覧ください。

6.1.3 カスタムビューの追加

ビューは、各ウィンドウにカメラが設定されたウィンドウ分割です。ビューモードにより、ウィンドウ分割と、カメラとウィンドウの対応をお気に入りとして保存して、後で関連するカメラにすばやくアクセスできます。例えば、オフィスにあるカメラ 1、カメラ 2、カメラ 3 をリンクしてウィンドウを表示し、「オフィス」というビューとして保存できます。事前定義されたデフォルトビューに加えて、ビューをカスタマイズして操作を追加することができます。

手順

1.[メインビュー] ページを表示します。
2.[ビュー] パネルの [カスタムビュー] にカーソルを移動し、 をクリックして新しいビューを作成します。
3.ビューの名前を入力します。

4.オプション: ライブビューのツールバーの をクリックして、新しいビューのウィンドウ分割モードを設定します。

注記

デフォルトでは、新しいビューは 4 ウィンドウ分割になっています。

5.実際の使用状況に応じて、指定されたウィンドウで指定されたカメラのライブビューを開始します。

6. をクリックして現在のビューを保存するか、新しいビューとして保存します。
7.オプション: カスタムビューを追加した後に、次の操作を実行します。

ビュー名を編集	新しいビューの上にカーソルを合わせて、 をクリックしてビュー名を編集します。
ビューを削除	新しいビューの上にカーソルを合わせて、 をクリックしてビューを削除します。

次に行う操作

もう一度 をクリックして、カスタムウィンドウ分割を選択します。

6.1.4 カスタムビューモードでのライブビューの開始

カスタムビューを追加した後、カスタムビューでカメラのライブビューを開始できます。

始める前に

ウィンドウ分割、カメラ、カメラとウィンドウの対応などの情報を含んでいるビューをカスタマイズします。詳細については、「*カスタムビューの追加*」をご覧ください。

手順

1.[メインビュー] ページを表示します。
2.オプション: ライブビューツールバーの をクリックして、表示スケール、再生パフォーマンス、画像の保存パスなどのパラメータを設定します。

注記

パラメータは [システム設定] でも設定できます。詳細については、「*システム設定*」をご覧ください。

3. をクリックして、[ビュー] パネルのカスタムビューリストを展開します。
4.カスタムビューをクリックして、ライブビューを開始します。
選択したビューに、追加したカメラのビデオが表示されます。
5.オプション: カスタムビューモードでライブビューを開始した後に、次の操作を実行します。

インスタント再生を開始	新しいビューの上にカーソルを合わせて、 をクリックしてビュー内のカメラのインスタント再生を開始します。詳細については、「*インスタント再生*」をご覧ください。
すべてのカスタムビューの自動切り替えを開始	[カスタムビュー] の上にカーソルを合わせて、 をクリックしてカスタムビューリスト内のすべてのビューの自動切り替えを開始します。詳細については、「*ライブビューでの自動切り替え*」をご覧ください。

6.2 ライブビューでの自動切り替え

カメラのライブビューまたはカスタムビューを順番に表示することができます。このことを「自動切り替え」といいます。大量のカメラのライブビューを実行する場合、選択したカメラを自動切り替えすることができます。この場合、クライアントは表示ウィンドウでカメラのライブビューを自動的に切り替えます。複数のビューを自動切り替えすることもできます。

ライブビューでの自動切り替えでは、次の 3 つのモードを使用できます。

- デフォルトビューのすべてのカメラの自動切り替え
- グループ内のカメラの自動切り替え
- カスタムビューの自動切り替え

6.2.1 グループ内のカメラの自動切り替え

同じグループのカメラのビデオストリームを、選択した表示ウィンドウで自動的に切り替えることができます。例えば、5 台のカメラを含むグループの自動切り替えを開始すると、5 台のカメラのライブビューが設定可能な間隔で順番に表示されます。また、再生に切り替えて、表示ウィンドウで他の操作を実行することもできます。

手順

1.[メインビュー] ページを表示します。
2.左パネルで **[自動切り替え]** → **[Single Window Auto-Switch（単一ウィンドウの自動切り替え）]** の順にクリックして、グループを表示します。
3.右側のパネルで表示ウィンドウを選択します。
4.グループ名の上にカーソルを合わせて、 をクリックします。

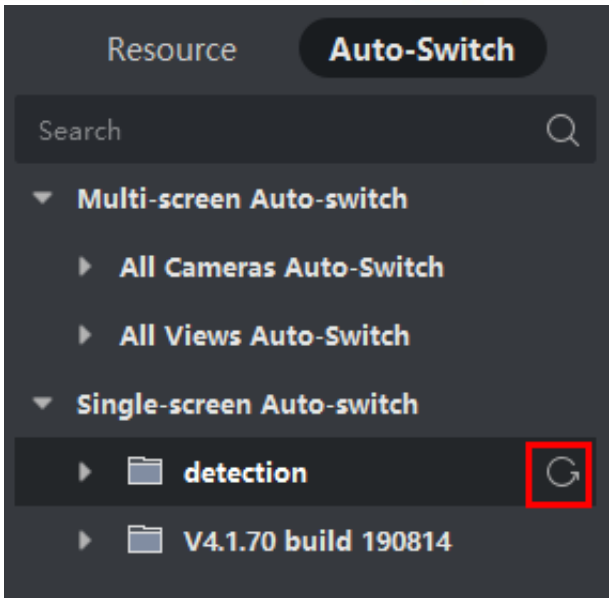

図 6-1 グループ内のカメラの自動切り替えの開始

選択したグループのカメラが、表示ウィンドウで自動切り替えを開始します。

注記

自動切り替えが開始すると、デフォルトでオーディオはオフになります。

5.オプション: 以下の操作を実行します。

操作説明**自動切り替えを一時停止 / 再開**	または をクリックして、自動切り替えを一時停止 / 再開します。
前のページ / 次のページに移動	または をクリックして、前のグループ / 次のグループのカメラを表示します。
滞留時間の設定	現在の自動切り替えを停止した後に、 または をクリックして自動切り替えの滞留時間を減らす、または増やします。または、ページの下部にある［20s］をクリックして自動切り替えの滞留時間を変更します。**[カスタム滞留時間]** をクリックして、必要に応じて滞留時間を設定することもできます。例えば、間隔を 10 秒に設定すると、各グループの画像が 10 秒間表示され、次のグループに切り替わります。

6.2.2 すべてのカメラの自動切り替え

カメラリスト内のすべてのカメラのビデオを、自動適応モードで自動的に切り替えることができます。すべてのカメラの自動切り替えを開始すると、すべてのカメラのライブビューがすばやく表示されます。これは、ライブビューに効果的な方法です。自動切り替えは、設定可能な間隔で実行されます。また、再生に切り替えて、自動切り替えウィンドウで他の操作を実行することもできます。

手順

1.[メインビュー] ページを表示します。
2.左パネルで **[自動切り替え]** → **[Multi-Window Auto-Switch（マルチウィンドウ自動切り替え）]** の順にクリックします。
3.**[Auto-Switch All Cameras（すべてのカメラを自動切り替え）]** の上にカーソルを合わせて、 をクリックします。

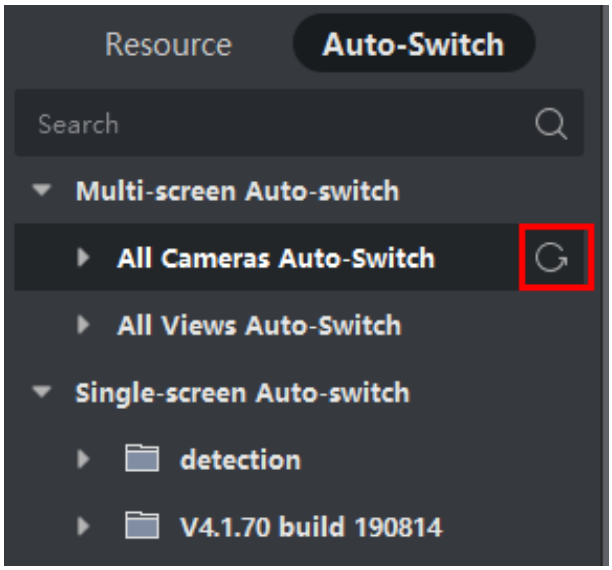

図 6-2 すべてのカメラの自動切り替えの開始

カメラリスト内のすべてのカメラが自動適応モードで自動切り替えを開始します。

4.オプション: 以下の操作を実行します。

自動切り替えを一時停止 / 再開	または をクリックして、自動切り替えを一時停止 / 再開します。
前のページ / 次のページに移動	または をクリックして、前のページ / 次のページのカメラを表示します。
滞留時間の設定	現在の自動切り替えを停止した後に、 または をクリックして自動切り替えの滞留時間を減らす、または増やします。または、ページの下部にある **[20s]** をクリックして自動切り替えの滞留時間を変更します。 **[カスタム滞留時間]** をクリックして、必要に応じて滞留時間を設定することもできます。例えば、間隔を 10 秒に設定すると、各カメラの画像が 10 秒間表示され、次のカメラに切り替わります。

6.2.3 カスタムビューの自動切り替え

ビューは、各ウィンドウにリンクされたリソースチャンネル（カメラなど）が表示されるウィンドウ分割です。ビューモードにより、ウィンドウ分割と、カメラとウィンドウの対応をお気に入りとして保存して、後でこれらのチャンネルにすばやくアクセスできます。フロアにあるすべてのカメラが含まれているビューを保存して、カスタムビューを保存すると、ワンクリック操作でフロアにあるすべてのカメラのライブビューを順に表示できます。この方法により、ログインするたびにカメラリストでこれらのカメラを検索する必要がなくなります。自動切り替えは、一定間隔で実行され、この間隔は手動で設定できます。

始める前に

カスタムビューを追加します。詳細については、「*カスタムビューの追加*」をご覧ください。

手順

1.[メインビュー] ページを表示します。

2.左パネルで **[リソース]** → **[Multi-Window Auto-Switch（マルチウィンドウ自動切り替え）]** の順にクリックします。

3.**[すべてのビューを自動切り替え]** の上にカーソルを合わせて、 をクリックします。

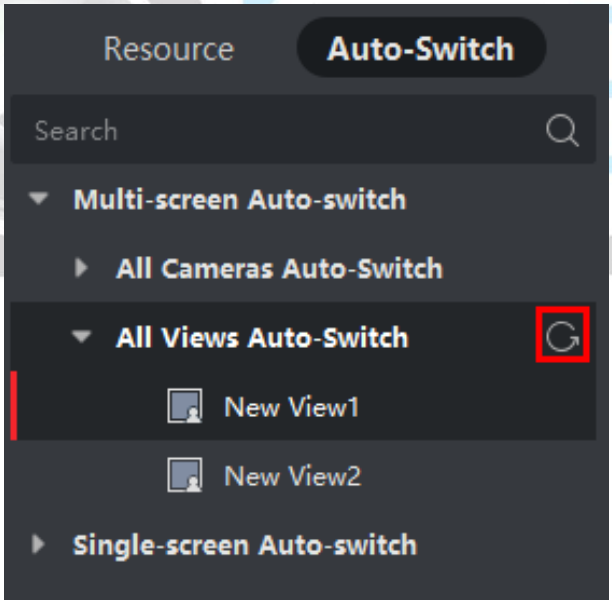

図 6-3 カスタムビューの自動切り替え

すべてのカスタムビューが自動切り替えを開始します。

4.オプション: 以下の操作を実行します。

自動切り替えを一時停止 / 再開	または をクリックして、自動切り替えを一時停止 / 再開します。

前のページ / 次のページに移動

または をクリックして、前のビュー / 次のビューを表示します。

滞留時間の設定

現在の自動切り替えを停止した後に、 または をクリックして自動切り替えの滞留時間を減らす、または増やします。または、ページの下部にある［20s］をクリックして自動切り替えの滞留時間を変更します。**[カスタム滞留時間]** をクリックして、必要に応じて滞留時間を設定することもできます。例えば、間隔を 10 秒に設定すると、各ビューの画像が 10 秒間表示され、次のビューに切り替わります。

6.3 PTZ 制御

ソフトウェアは、パン / チルト / ズーム機能を備えたカメラの PTZ 制御を提供しています。PTZ 制御中に、プリセット、巡回、およびパターンを設定できます。また、PTZ 制御用の新しいウィンドウを開くこともできます。

注記

クラウド P2P デバイスは、上、下、左、右の方向への PTZ 動作のみをサポートしています。

[メインビュー] モジュールに入り、**[PTZ 制御]** を選択して [PTZ 制御] パネルを開きます。[PTZ 制御] パネルでは、次のアイコンを使用できます。

表 6-1 [PTZ 制御] パネルのアイコン

アイコン	名前	説明
	方向ボタン	マウスの左ボタンをクリックまたは押し続けて、PTZ を回転させます。 をクリックして PTZ を水平方向に連続的に回転させます。もう一度クリックして回転を停止します。
	速度制御	スライダーをドラッグして、PTZ の動作速度を調整します。
	拡大 / 縮小	拡大して細部が表示されるように近接画像を表示し、縮小して全景画像を表示します。
	フォーカス + / -	**[フォーカス +]** をクリックして焦点を前方へ移動して、**[フォーカス -]** をクリッ

アイコン	名前	説明
		クして焦点を後方へ移動します。
	絞り +/-	画像の輝度を調整するのに使用します。絞りが大きいほど光が入り、画像が明るくなります。
	3D ポジショニング	マウスの左ボタンを使用して、ビデオ映像内の目的の位置をクリックし、矩形エリアを描くように右下方向に向かってドラッグします。ドームシステムの位置が中央に移動して矩形エリアが拡大表示されます。マウスの左ボタンを使用して、矩形エリアを描くように左上方向に向かってドラッグすると、位置が中央に移動して矩形エリアが縮小表示されます。
	補助フォーカス	クリックして自動的にフォーカスを合わせます。
	レンズの初期化	レンズを初期化して、再度フォーカスを合わせて鮮明な画像を表示します。
	ライト	クリックしてライトを照らします。 **注記** 使用するデバイスがこの機能をサポートしている必要があります。
	ワイパー	ワイパーを使用して、カメラレンズのほこりを取り除きます。
	手動追跡	自動追跡機能を備えたスピードドームの場合は、右クリックメニューを使用して自動追跡を有効にして、アイコンをクリックし、ビデオをクリックして対象を手動で追跡します。
	メニュー	アナログスピードドームの場合は、アイコンをクリックしてローカルメニューを表示します。メニューの詳細な操作については、スピードドームのユーザーマニュアルをご覧ください。

アイコン	名前	説明
	ワンタッチ巡回	ワンタッチ巡回機能を備えたスピードドームの場合は、アイコンをクリックすると、スピードドームは非利用状態が一定期間続いた後（パーク時間）に事前定義したプリセット No.1 からプリセット No.32 まで順番に巡回を開始します。パーク時間の設定については、スピードドームのユーザーマニュアルをご覧ください。
	ワンタッチパーク	ワンタッチパーク機能を備えたスピードドームの場合は、アイコンをクリックすると、スピードドームは現在のビューをプリセット No.32 に保存します。デバイスは、非利用状態が一定期間続いた後（パーク時間）に、プリセット番号 32 で自動的にパークを開始します。パーク時間の設定については、スピードドームのユーザーマニュアルをご覧ください。
	手動除氷ヒーターを有効化	この機能を有効にすると、0℃以下の環境でもカメラの性能が維持されます。
	手動顔キャプチャ	このボタンをクリックして、左マウスボタンを押し続けて画像内の顔を選択してキャプチャします。画像がサーバーにアップロードされ、表示できるようになります。
	FOV を同期化	サーマルカメラ用です。クリックして、光学チャンネルの視野をサーマルチャンネルの視野と同期します。
	領域内露出	スピードドームの場合は、アイコンをクリックして画像上に矩形を描画して、この領域の露出効果を最適化します。
	領域内フォーカス	スピードドームの場合は、アイコンをクリックして画像上に矩形を描画して、この領域のフォーカス効果を最適化します。

6.3.1 プリセットの設定

プリセットは事前定義した画像位置で、パン、チルト、フォーカス、およびその他のパラメータの情報が含まれています。プリセットを設定した後、プリセットを呼び出すことで、カメラをすばやく目的の位置にすることができます。

手順

1.[メインビュー] ページを開いて、PTZ カメラのライブビューを開始します。
2.左側にある **[PTZ 制御]** をクリックして、[PTZ 制御] パネルを展開します。
3.ページの左下隅の [PTZ 制御] パネルを展開します。

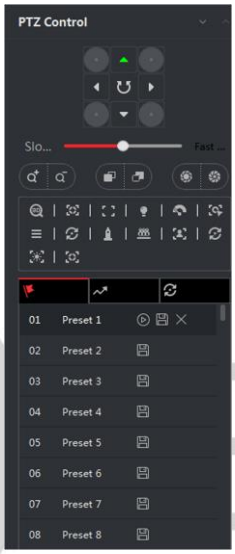

図 6-4 [PTZ 制御] パネル

4.メインビューウィンドウから PTZ ウィンドウを 1 つ選択します。
5.オプション: [PTZ 制御] パネルで、プリセット名([プリセット 1] など)をクリックして、プリセット名を編集します。
6.[PTZ 制御] パネルで、[PTZ 制御] パネルの方向ボタンと機能ボタンをクリックして、プリセットに指定する位置になるようにシーンを調整します。
7. をクリックして、プリセット設定を保存します。
8.オプション: プリセットを設定した後に、次の操作を実行します。

プリセットを呼出 プリセットを選択し、 をクリックしてプリセットを呼び出します。キーボードの数字キー（***4*** など）を押してプリセット 1～9 を呼び出したり、キーボードの ***[***、数字キー（***124*** など）、***]*** を押して別のプリセットを呼び出すこともできます。

プリセットを編集 PTZ カメラの方向、位置、ビューを調整し、 をクリックしてプリセットを再度保存します。古いプリセット設定が置き換えられます。

プリセットを削除 リストから設定済みのプリセットを選択し、 をクリックして削除します。

6.3.2 巡回の設定

巡回とは、ユーザー定義のプリセットのグループで指定されたスキャン追跡で、2 つのプリセット間のスキャン速度とプリセットでの滞留時間を個別に設定できます。

始める前に

1 台の PTZ カメラに 2 つ以上のプリセットを追加します。

手順

注記

クラウド P2P デバイスでは、巡回はサポートされていません。

1.[メインビュー] ページを開いて、PTZ カメラのライブビューを開始します。
2.左側にある **[PTZ 制御]** をクリックして、[PTZ 制御] パネルを展開します。
3. タブをクリックして、PTZ 巡回設定パネルを表示します。

4.ドロップダウンリストからパス番号を選択します。
5. をクリックして、[巡回番号を追加] ダイアログを開きます。
6.ドロップダウンリストからプリセットを選択して、ダイアログでプリセットの滞留時間と巡回速度を設定します。
7.**[OK]** をクリックします。
8.手順 5、6、7 を繰り返して、他のプリセットを巡回に追加します。
9.オプション: 巡回を設定した後に、次の操作を実行します。

巡回を呼出 をクリックして、巡回を呼び出します。

巡回の呼び出しを停止 をクリックして、巡回の呼び出しを停止します。

巡回のプリセットを編集 巡回パスでプリセットを選択し、 をクリックしてプリセットを編集します。

巡回からプリセットを削除 巡回パスでプリセットを選択し、 をクリックして巡回からプリセットを削除します。

6.3.3 パターンの設定

パターンは、繰り返し実行される一連のパン、チルト、ズーム、およびプリセット機能が記憶されたものです。

手順

注記

クラウド P2P デバイスでは、パターンはサポートされていません。

1.[メインビュー] ページを開いて、PTZ カメラのライブビューを開始します。
2.左側にある **[PTZ 制御]** をクリックして、[PTZ 制御] パネルを展開します。
3. タブをクリックして、PTZ パターン設定パネルを表示します。

4. をクリックして、このパターンパスの記録を開始します。
5.方向ボタンを使用して、PTZ の動作を制御します。
6. をクリックして、記録を停止し、記録されたパターンを保存します。
7.オプション: パターンを設定した後に、次の操作を実行します。

パターンを呼出	をクリックして、パターンを呼び出します。
パターンの呼び出しを停止	をクリックして、パターンの呼び出しを停止します。
パターンを削除	パターンを 1 つ選択し、 をクリックしてパターンを削除します。
すべてのパターンを削除	をクリックして、すべてのパターンを削除します。

6.4 ウィンドウ分割のカスタマイズ

クライアントソフトウェアは、複数の種類の事前定義されたウィンドウ分割を提供しています。必要に応じて、ウィンドウ分割をカスタマイズすることもできます。

手順

注記

最大 5 個のウィンドウ分割をカスタマイズできます。

1.[メインビュー] または [リモート再生] ページを開きます。

2.ライブビューまたは再生ツールバーの をクリックして、ウィンドウ分割パネルを開きます。

3.**[追加]** をクリックして、[カスタムウィンドウ分割を追加] ダイアログを開きます。
4.[寸法] フィールドの水平寸法と垂直寸法の両方にウィンドウ数を入力して、キーボードの **Enter** キーを押します。

注記

リモート再生で同時に再生できるウィンドウは最大 16 個であるため、ウィンドウが 16 個を超えるカスタムウィンドウ分割は無効です。

5.オプション: マウスをドラッグして隣接するウィンドウを選択して、**[結合]** をクリックし、それらをウィンドウ全体として結合します。

6.オプション: 結合されたウィンドウを選択し、**[復元]** をクリックし、結合をキャンセルします。
7.**[保存]** をクリックします。
8.オプション: 分割モードをクリックするか、表示しているウィンドウにドラッグして、表示モードを適用します。
9.オプション: カスタマイズしたウィンドウ分割モードを編集します。
1）ライブビューまたは再生ツールバーの をクリックして、ウィンドウ分割パネルを開きます。
2）**[編集]** をクリックして、[カスタムウィンドウ分割を追加] を開きます。
3）カスタマイズした分割モードを選択して、名前の変更、寸法の設定、ウィンドウの結合 / 結合取り消しなどの操作を実行します。

6.5 手動での録画およびキャプチャ

ライブビュー中は、手動でビデオを録画したり画像をキャプチャできます。その後、録画ビデオファイルとキャプチャ画像をローカル PC で表示できます。

6.5.1 手動でのビデオの録画

手動録画機能により、[メインビュー] ページのライブビデオを手動で録画して、ビデオファイルをローカル PC に保存できます。

手順

注記

手動録画は、ライブビュー中のクラウド P2P デバイスではサポートされていません。

1.[メインビュー] ページを開きます。
2.ライブビューを開始します。
3.次のいずれかの操作を実行して、手動録画を開始します。
- ライブビューの表示ウィンドウにカーソルを移動して、ツールバーを表示し、ツールバーの をクリックします。
- 表示ウィンドウを右クリックして、右クリックメニューの **[録画を開始]** をクリックします。

アイコン が に変わります。表示ウィンドウの右上隅にインジケータ が表示されます。

4. をクリックして、手動録画を停止します。

録画ビデオファイルは自動的にローカル PC に保存され、保存先パス情報を示す小さなウィンドウがデスクトップの右下隅に表示されます。

注記

録画ビデオファイルの保存パスは、[システム設定] ページで設定できます。詳細については、「*ファイル保存先パスの設定*」をご覧ください。

6.5.2 ローカルビデオの表示

ローカル PC に保存されている録画ビデオファイルを表示できます。

始める前に

ライブビデオを録画します。

手順

1.右上隅の ☰ →［**ファイル**］→［**ビデオファイルを開く**］の順にクリックして、［ビデオファイル］ページを開きます。
2.録画ビデオファイルを検索するカメラを [カメラグループ] リストから選択します。
3.検索の開始時刻と終了時刻を左下隅に指定します。
4.**[検索]** をクリックします。
開始時刻と終了時刻の間に録画されたビデオファイルが、ページにサムネイル形式で表示されます。
5.オプション: 検索後、次の操作を実行します。

ビデオファイルを削除	ビデオファイルを選択して、**[削除]** をクリックし、ビデオファイルを削除します。
電子メールを送信	ビデオファイルを選択して、**[電子メール]** をクリックし、選択したビデオファイルが添付された電子メール通知を送信します。
	注記 電子メール通知を送信するには、続行する前に電子メール設定を設定する必要があります。詳細については、「*電子メールのパラメータ設定*」をご覧ください。
ローカルビデオを保存	ビデオファイルを選択して、**[名前を付けて保存]** をクリックし、ビデオファイルの新しいコピーを保存します。
再生	ビデオファイルをダブルクリックして、ローカル再生を開始します。

6.5.3 画像のキャプチャ

ライブビュー中に画像をキャプチャできます。

ライブビュー中に画像をキャプチャする必要がある場合は、このタスクを実行します。

手順

1.[メインビュー] ページを開き、カメラのライブビューを開始します。
2.次のいずれかの操作を実行して、画像をキャプチャします。
– ライブビューの表示ウィンドウにカーソルを移動して、ツールバーを表示し、ツールバーの 📷 をクリックします。
– 表示ウィンドウを右クリックして、右クリックメニューの **[キャプチャ]** をクリックします。
キャプチャ画像は自動的にローカル PC に保存され、画像プレビューと保存パス情報を

示す小さなウィンドウがデスクトップの右下隅に表示されます。

注記

キャプチャ画像の保存パスは、[システム設定] ページで設定できます。詳細については、「*ファイル保存先パスの設定*」をご覧ください。

6.5.4 キャプチャ画像の表示

ライブビューでキャプチャされた画像は、ソフトウェアを実行している PC に保存されます。必要に応じて、キャプチャ画像を表示できます。

始める前に

ライブビューで画像をキャプチャします。

手順

1.右上隅の → **[ファイル]** → **[キャプチャ画像を開く]** の順にクリックして、[キャプチャ画像] ページを開きます。
2.キャプチャ画像を検索するカメラを [カメラグループ] リストから選択します。
3.検索の開始時刻と終了時刻を左下隅に指定します。
4.**[検索]** をクリックします。
開始時刻と終了時刻の間にキャプチャ画像が、ページにサムネイル形式で表示されます。
5.オプション: 検索後、次の操作を実行します。

画像を拡大	画像のサムネイルをダブルクリックして、サムネイルを拡大して見やすくします。
画像を印刷	キャプチャ画像を選択して、**[出力]** をクリックし、選択した画像を印刷します。
画像を削除	キャプチャ画像を選択して、**[削除]** をクリックし、選択した画像を削除します。
電子メールを送信	キャプチャ画像を選択して、**[電子メール]** をクリックし、選択した画像が添付された電子メール通知を送信します。
画像を保存	キャプチャ画像を選択して、**[名前を付けて保存]** をクリックし、選択した画像の新しいコピーを保存します。

6.6 インスタント再生

インスタント再生では、注目すべきビデオや一見しただけでは不明瞭なビデオの一部が表示されます。この機能により、[メインビュー] ページでビデオファイルをすぐに再生して、

必要に応じてすぐに確認することができます。

始める前に

ビデオファイルを録画して、ストレージデバイス（DVR、NVR、ネットワークカメラの SD/SDHC カードや HDDなど）、またはストレージサーバーに保存します。

手順

1.[メインビュー] ページを開いて、ライブビューを開始します。
2.次のいずれかの操作を実行して、インスタント再生の事前再生時間リストを表示します。
- カーソルを表示ウィンドウに移動してツールバーを表示し、 をクリックします。
- 表示ウィンドウを右クリックして、右クリックメニューで **[インスタント再生に切り替え]** を選択します。
- [ビュー] パネルのデフォルトビューまたはカスタムビューノードにカーソルを移動して、 をクリックします。

30 秒、1 分、3 分、5 分、8 分、10 分の事前再生時間のリストが表示されます。
3.表示されたリストから時間を選択して、インスタント再生を開始します。

例

3 分を選択し、現在のライブビューの時間が 09:30:00 の場合、インスタント再生は 09:27:00 から開始されます。

インスタント再生中は、表示ウィンドウの右上隅にインジケータ が表示されます。
4.オプション: もう一度 をクリックして、インスタント再生を停止して、ライブビューに戻ります。

6.7 フィッシュアイカメラのライブビュー

フィッシュアイカメラの場合、フィッシュアイモードでライブビューを開始したり、プリセットや巡回を設定したり、PTZ 制御を実行することができます。

6.7.1 フィッシュアイモードでのライブビューの実行

フィッシュアイカメラのライブビュー中は、ゆがみのある全方位広角ビューが表示されます。ゆがみにより、一部の細部を確認するのが困難な場合があります。この問題を解決するには、ライブビデオをフィッシュアイ展開モードで再生します。フィッシュアイ展開では、180° パノラマ、360° パノラマ、PTZ、半球などのさまざまなモードで画像を展開できます。これにより、画像をはっきりと見ることができます。

手順

1.[メインビュー] ページを開き、フィッシュアイカメラのライブビューを開始します。
2.フィッシュアイ展開モードを表示します。
- ビデオを右クリックして、**[フィッシュアイ展開]** を選択します。
- ツールバーの をクリックします。ツールバーの設定の詳細については、「*ツール*

バーに表示されるアイコンの設定」をご覧ください。
が に変わります。

3.表示しているウィンドウの左下隅の をクリックして、[Mounting Type & Expanding Mode Selection（マウントタイプおよび展開モードを選択）] パネルを開きます。

4.実際の取り付け位置に応じて、フィッシュアイカメラのマウントタイプを選択します。

5.必要に応じて、ライブビューの展開モードを選択します。

フィッシュアイ

フィッシュアイビューモードでは、カメラの全方位広角ビューが表示されます。このビューモードは、魚の凸形眼の視覚に近いため、フィッシュアイと呼ばれます。レンズは、画像内の物体の遠近感と角度を歪ませながら、広いエリアの曲線画像を生成します。

パノラマ

[パノラマ] ビューモードでは、いくつかの較正方法によってゆがみのあるフィッシュアイ画像が通常の遠近法画像に変換されます。

PTZ

PTZ ビューは [フィッシュアイ] ビューまたは [パノラマ] ビュー内の定義されたエリアのクローズアップビューで、電子 PTZ 機能（e-PTZ ともいいます）をサポートしています。

注記

[フィッシュアイ] ビューおよび [パノラマ] ビューで、各 PTZ ビューには特定のナビゲーションボックスが表示されます。[フィッシュアイ] ビューまたは [パノラマ] ビューのナビゲーションボックスをドラッグして PTZ ビューを調整するか、PTZ ビューをドラッグしてビューを目的の角度に調整できます。

半球

半球モードでは、画像をドラッグして直径を中心に回転させて、ビューを目的の角度に調整できます。

AR 半球

AR 半球モードは、遠方と近方の画像が重ねられるため、立体画像を広角で表示することができます。

シリンダー

シリンダーモードでは、画像がシリンダー状のページとして表示されます。

6.オプション: フィッシュアイモードでライブビューを開始した後に、次の操作を実行します。

キャプチャ	ウィンドウを右クリックして、**[キャプチャ]** を選択し、ライブビュープロセスで画像をキャプチャします。

全画面モードで表示	再生ウィンドウを右クリックして、選択したウィンドウを全画面モードに切り替えます。

6.7.2 フィッシュアイモードでの PTZ 制御

フィッシュアイモードでは、PTZ を制御して PTZ ウィンドウを調整できます。

注記

PTZ パネルは、デバイスごとに異なります。

[PTZ 制御] パネルでは、次の機能を使用できます。

- PTZ ウィンドウを選択して、方向ボタンをクリックしてビューの角度を調整します。または、フィッシュアイまたはパノラマウィンドウで番号ラベルをドラッグして、PTZ ウィンドウの表示角度を変更します。
- PTZ ウィンドウを選択し、 をクリックして自動スキャンを開始します（カメラは水平方向に回転します）。もう一度クリックして自動スキャンを停止します。
- でスライダーをドラッグして、PTZ の動作速度を調整します。
- をクリックするか、マウスホイールをスクロールして、選択した PTZ ウィンドウを拡大または縮小します。

プリセットの設定

フィッシュアイモードでは、ユーザー定義の監視位置 / ポイントであるプリセットを設定し、プリセット番号を呼び出すだけで監視シーンを定義された位置に変更できます。

手順

注記

特定のフィッシュアイカメラのみがプリセットの設定をサポートしています。フィッシュアイモードでは、最大 256 個のプリセットを設定できます。

1.[メインビュー] ページを開き、フィッシュアイカメラのライブビューを開始します。
2.ビデオを右クリックして、**[フィッシュアイ展開]** を選択して [フィッシュアイ展開] ウィンドウを開きます。
3.ページの左下隅の [PTZ 制御] パネルを展開します。

図 6-5 [PTZ 制御] パネル

4. メインビューウィンドウから PTZ ウィンドウを 1 つ選択します。
5. オプション: [PTZ 制御] パネルで、プリセット名([プリセット 1] など)をクリックして、プリセット名を編集します。
6. [PTZ 制御] パネルで、[PTZ 制御] パネルの方向ボタンと機能ボタンをクリックして、プリセットに指定する位置になるようにシーンを調整します。
7. をクリックして、プリセット設定を保存します。
8. オプション: プリセットを設定した後に、次の操作を実行します。

プリセットを呼出 プリセットを選択し、 をクリックしてプリセットを呼び出します。キーボードの数字キー（***4*** など）を押してプリセット 1～9 を呼び出したり、キーボードの ***[***、数字キー（***124*** など）、***]*** を押して別のプリセットを呼び出すこともできます。

プリセットを編集 PTZ カメラの方向、位置、ビューを調整し、 をクリックしてプリセットを再度保存します。古いプリセット設定が置き換えられます。

プリセットを削除 リストから設定済みのプリセットを選択し、 をクリックして削除します。

巡回の設定

フィッシュアイモードでは、巡回を設定できます。巡回とは、ユーザー定義のプリセットのグループで指定されたスキャン追跡で、2 つのプリセット間のスキャン速度とプリセットでの滞留時間を個別に設定できます。

始める前に

2 つ以上のプリセットを設定します。

手順

注記

特定のフィッシュアイカメラのみが巡回の設定をサポートしています。フィッシュアイモードでは、最大 32 個の巡回を設定できます。

1.[メインビュー] ページを開き、フィッシュアイカメラのライブビューを開始します。
2.ビデオを右クリックして、**[フィッシュアイ展開]** を選択して [フィッシュアイ展開] ウィンドウを開きます。
3. をクリックし、巡回設定パネルを表示します。
4.ドロップダウンリストからパス番号を選択します。
5. をクリックして、[巡回番号を追加] ウィンドウを開きます。
6.**[OK]** をクリックします。
7.手順 5、6、7 を繰り返して、他のプリセットを巡回に追加します。
8.オプション: 巡回を設定した後に、次の操作を実行します。

巡回のプリセットを編集	巡回パスでプリセットを選択し、 をクリックしてプリセットを編集します。
巡回からプリセットを削除	巡回パスでプリセットを選択し、 をクリックして巡回からプリセットを削除します。
巡回を呼出	をクリックして、巡回を呼び出します。
巡回の呼び出しを停止	をクリックして、巡回の呼び出しを停止します。

6.8 マスター / スレーブリンクの実行

マスター / スレーブ追跡機能をサポートするボックスカメラまたはバレットカメラは、必要に応じて対象を特定または追跡できます。

注記

- この機能は、特定のボックスカメラまたはバレットカメラのみがサポートしています。

- 自動追跡機能を備えたスピードドームは、ボックスカメラまたはバレットカメラの近くに設置する必要があります。

6.8.1 マスター / スレーブ追跡ルールの設定

ライブビュー中にマスター / スレーブ追跡を実行する前に、ボックスカメラまたはバレットカメラのマスター / スレーブ追跡ルールを設定する必要があります。これには、VCA 検知ルールの設定、スピードドームへのリンク、カメラとスピードドームの較正が含まれます。

侵入検知ルールの設定

バレットカメラまたはボックスカメラの VCA 検知ルールを設定する必要があります。VCA イベントがトリガーされると、クライアントはスピードドームをトリガーして対象を追跡できます。ここでは侵入検知を例にとって説明します。

手順

1.[デバイス管理] ページを開いて、ボックスカメラまたはバレットカメラを選択します。
2. → **[詳細設定]** → **[VCA 設定]** → **[ルール]** → **[ルール設定]** の順にクリックして、ルール設定ページを開きます。
3.[ルールリスト] パネルで **[追加]** をクリックしてルールを追加します。
4.イベントタイプとして **[侵入]** を選択します。
5. をクリックして、ライブビデオ上に検知領域を描画します。
6.**[保存]** をクリックします。

スピードドームのリンク

ボックスカメラまたはバレットカメラのマスター / スレーブ追跡を設定するときに、カメラをスピードドームにリンクして、追跡用のスピードドームの PTZ 位置を設定できます。

このタスクを実行して、ボックスカメラまたはバレットカメラをマスター / スレーブ追跡用のスピードドームにリンクします。

手順

1.[デバイス管理] ページを開いて、ボックスカメラまたはバレットカメラを選択します。
2. → **[詳細設定]** → **[マスター / スレーブ追跡]** の順にクリックして、マスター / スレーブ追跡設定ページを表示します。
3.表示ウィンドウで **[ログイン]** をクリックして、スピードドームログインウィンドウを開きます。
4.スピードドームの IP アドレス、ポート番号、ユーザー名、およびパスワードを入力します。
5.**[ログイン]** をクリックしてスピードドームにログインします。

6.**[PTZ]** をクリックして、方向矢印を使用してスピードドームを調整して水平位置にします。

次に行う操作

ボックスカメラまたはブレットカメラと、リンクされたスピードドームを較正します。詳細については、「*カメラとスピードドームの自動較正*」または「*カメラとスピードドームの手動較正*」をご覧ください。

カメラとスピードドームの自動較正

バレットカメラまたはボックスカメラのマスター / スレーブ追跡ルールを設定するときに、カメラとスピードドームを較正する必要があります。自動と手動の 2 つの較正モードを使用できます。ここでは自動較正モードについて説明します。

始める前に

カメラをスピードドームにリンクします。詳細については、「*スピードドームのリンク*」をご覧ください。

手順

1.[デバイス管理] ページを開いて、ボックスカメラまたはバレットカメラを選択します。
2. → **[詳細設定]** → **[マスター / スレーブ追跡]** の順にクリックして、マスター / スレーブ追跡設定ページを表示します。
3.[較正] パネルの右下隅で、較正モードとして **[自動較正]** を選択します。
4.スピードドームのビューを移動および拡大 / 縮小して、ドームとカメラのライブビューがほぼ同じであることを確認します。
5.**[保存]** をクリックします。

カメラとスピードドームの手動較正

バレットカメラまたはボックスカメラのマスター / スレーブ追跡ルールを設定するときに、カメラとスピードドームを較正する必要があります。自動と手動の 2 つの較正モードを使用できます。ここでは手動較正モードについて説明します。

始める前に

カメラをスピードドームにリンクします。詳細については、「*スピードドームのリンク*」をご覧ください。

手順

1.[デバイス管理] ページを開いて、ボックスカメラまたはバレットカメラを選択します。
2. → **[詳細設定]** → **[マスター / スレーブ追跡]** の順にクリックして、マスター / スレーブ追跡設定ページを表示します。
3.[較正] パネルの右下隅で、較正モードとして **[手動較正]** を選択します。
4.リストからサイト番号 1 を選択して、 をクリックします。
ライブビューページの中央に青い十字が表示され、選択したサイトのデジタルズームビューが右側に表示されます。

5.手順 4 を繰り返して、他の手動較正サイトを追加します。
6.ライブビューページで、4 つの較正サイト間の距離が均等になるように調整します。
7.較正サイト番号 1 を選択します。
サイト番号 1 のデジタルズームビューが右側に表示されます。
8.スピードドームのビューを移動および拡大 / 縮小して、スピードドームのライブビューと選択したサイトのデジタルズームビューがほぼ同じであることを確認します。
9. をクリックして、現在のサイト位置情報を保存します。
10.手順 7、8、9 を繰り返して、他のサイトの位置を設定します。
11.**[保存]** をクリックします。

6.8.2 マスター / スレーブ追跡の有効化

ライブビュー中に、マスター / スレーブ追跡を有効にして、スピードドームを備えたバレットカメラまたはボックスカメラのビューに表示される対象を特定または追跡できます。

始める前に

ボックスカメラまたはバレットカメラのマスター / スレーブ追跡ルールを設定します。

ボックスカメラまたはバレットカメラのマスター / スレーブ追跡を有効にする必要がある場合は、このタスクを実行します。

手順

1.[メインビュー] ページを表示して、ボックスカメラまたはバレットカメラのライブビューを開始します。
2.ライブビューウィンドウを右クリックし、**[マスター / スレーブ追跡を有効化]** をクリックします。
設定した VCA ルールが対象によってトリガーされると、リンクされたスピードドームが自動マスター / スレーブ追跡を実行し、ターゲットフレームが緑から赤に変わります。

6.9 サーマルカメラのライブビュー

サーマルカメラでは、ライブビュー中に発火元情報と温度を表示できます。また、温度を手動で測定して、ライブビュー画像に温度情報を表示することもできます。

6.9.1 ライブビュー中の発火元情報の表示

ライブビュー中に、検知された発火元情報を表示できます。

始める前に

サーマルデバイスのアラームルールを設定します。詳細については、デバイスのユーザーマニュアルをご覧ください。

手順

1.[メインビュー] ページを表示して、サーマルカメラのライブビューを開始します。

注記

ライブビューの開始と停止については、「***1 台のカメラのライブビューの開始***」およびをご覧ください。

2.ライブビュー画像を右クリックして、右クリックメニューの **[発火元情報]** を選択して、情報タイプのリストを表示します。

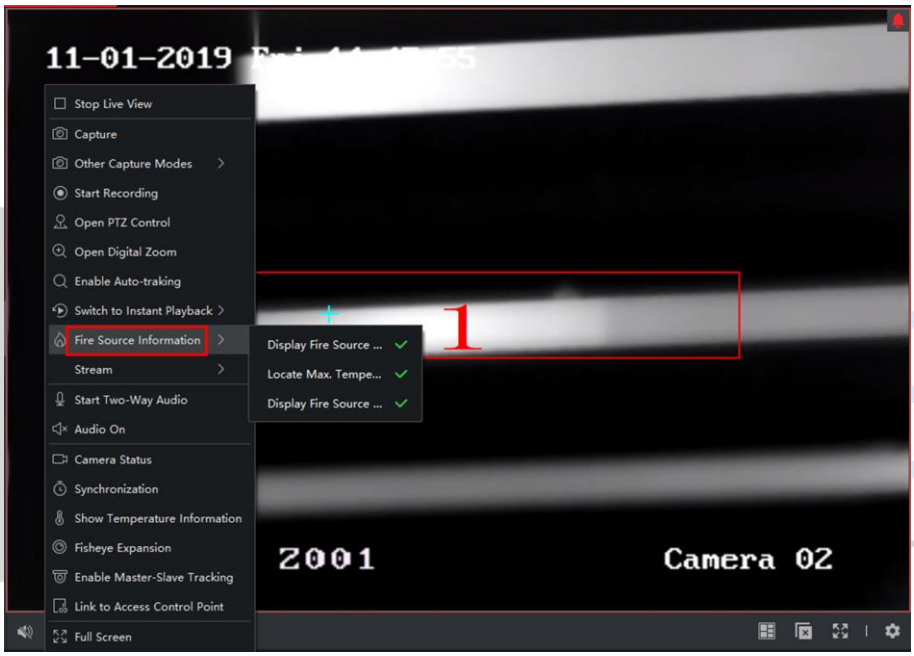

図 6-6 発火元情報の表示

3.リストで情報タイプを選択して、情報を表示します。

発火元領域を表示

設定したアラームしきい値よりも温度が高い領域です。

最高温度領域を特定

発火元領域で温度が最も高い領域がマークされます。緑でマークされます。

発火元対象を表示

デバイスと発火元の間の距離です。

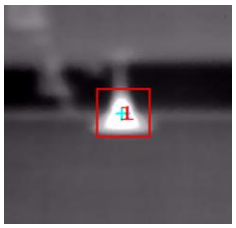

図 6-7 ライブビュー画像での発火元情報

6.9.2 ライブビュー画像での温度情報の表示

ライブビデオを表示しているときに、監視シーンのリアルタイムの温度情報を表示または非表示にすることができます。

始める前に

- デバイスの VCA ソースタイプを **[Temperature Measurement + Behavior Analysis（温度測定 + 動作分析）]** に切り替えます。
- デバイスの温度測定機能を有効にし、温度測定ルールを設定します。詳細については、デバイスのユーザーマニュアルをご覧ください。

ライブビュー画像に温度情報を表示する必要がある場合は、このタスクを実行します。

手順

1.[メインビュー] ページを表示して、サーマルカメラのライブビューを開始します。

注記

ライブビューの開始手順については、「*1 台のカメラのライブビューの開始*」をご覧ください。

2.温度測定ルールが設定された領域になるようにシーンを調整します。

3.ライブビュー画像を右クリックして、右クリックメニューで **[温度情報を表示]** を選択します。

ライブビュー画像に温度が表示されます。

4.画像をクリックして、詳細な温度情報を表示します。

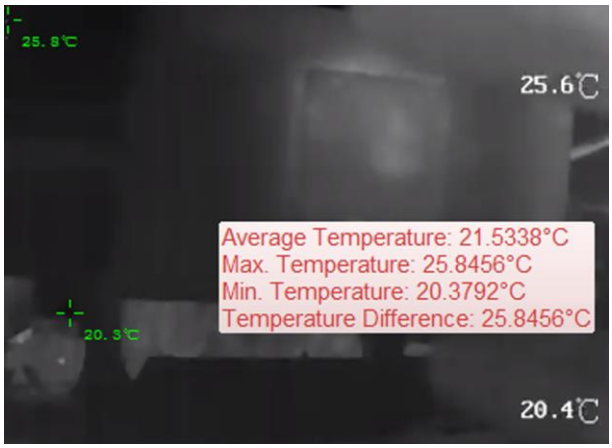

図 6-8 ライブビュー画像上の温度情報

5.オプション: ライブビュー画像を右クリックして、**[温度情報を非表示]** を選択して温度情報を非表示にします。

6.9.3 手動での温度の測定

サーマルカメラのライブビュー中に、ライブビュー画像の任意の場所をクリックしてさまざまなポイントの温度を表示して、発火元をすばやく見つけることができます。

手順

注記

- 測定した温度は画像上に 5 秒間表示されます。
- 1 つのポイントの温度のみを表示できます。
- 複数のクライアントが 1 台のカメラのライブビデオを受信しているときに、あるクライアントが測定ポイントを追加または削除すると、他のクライアントのライブビューも影響を受けます。すべてのユーザーがカメラのライブビューを停止すると、測定ポイントは消去されます。

1.[メインビュー] ページを表示して、サーマルカメラのライブビューを開始します。

注記

ライブビューの開始と停止については、「***1 台のカメラのライブビューの開始***」およびをご覧ください。

2.ライブビュー画像を右クリックして、**[温度情報を表示]** を選択します。
3.ライブビュー画像をクリックして、この位置の温度を表示します。
クリックしたポイントの温度が画像に表示されます。

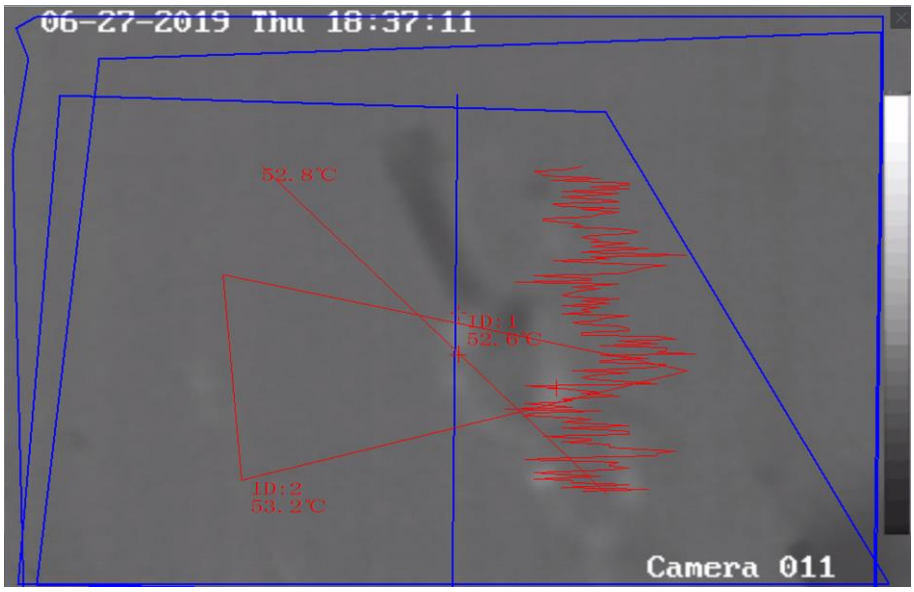

図 6-9 ポイントの温度の手動測定

4.オプション: ライブビュー画像を右クリックして、メニューで **[温度情報を非表示]** を選択します。

6.10 低帯域幅でのライブビュー

ネットワーク帯域幅が狭い場合、帯域幅の制限によりビデオストリーミングの速度が大幅に遅くなることがあります。低帯域幅のユーザーに低いストリーミング速度で通常の品質を提供できるように、クライアントは低帯域幅でのライブビューモードを提供しています。その前に、ストリーミングプロトコルを設定したり、他の操作を実行する必要があります。設定の詳細については、「*ネットワーク帯域幅が狭いときにライブビューと再生のパフォーマンスを向上させるにはどうしたら良いですか?*」をご覧ください。

6.11 その他の機能

ライブビューでは、補助画面プレビュー、デジタルズーム、チャンネルゼロ、双方向オーディオ、カメラの状態、同期などの機能もサポートしています。

補助画面プレビュー

ライブビデオを別の補助画面に表示して、複数の監視シーンを簡単にプレビューできます。

注記

最大 3 つの補助画面をサポートしています。

デジタルズーム

マウスをドラッグして右下 / 左上方向に矩形エリア領域を描画して、描画したエリアを拡大または縮小します。または、マウスホイールを使用して、デジタルズームモードでビューを拡大または縮小します。

チャンネルゼロ

デバイスのチャンネルゼロを表示する場合は、**Ctrl** キーを押しながらダブルクリックして特定のチャンネルを表示します。復元するには、**Ctrl** キーを押しながら再度ダブルクリックします。

2 ウェイオーディオ

2 ウェイオーディオ機能により、カメラの音声通話が有効になります。ライブビデオだけでなく、リアルタイムオーディオもカメラから得られます。デバイスに複数の 2 ウェイオーディオチャンネルがある場合は、チャンネルを選択して 2 ウェイオーディオを開始できます。

注記

- 2 ウェイオーディオは、一度に 1 台のカメラでのみ使用できます。
- クラウド P2P デバイスは、2 ウェイオーディオ中のチャンネルの選択をサポートしていません。

カメラの状態

カメラの状態（録画状態、信号状態、接続番号など）を検知して、確認のために表示できます。状態情報は 10 秒ごとに更新されます。

同期

同期機能は、クライアントソフトウェアを実行する PC とデバイスクロックを同期する方法を提供します。

ストリームタイプの設定

自動変更ストリームタイプ

カメラは、表示ウィンドウのサイズに応じてストリームタイプを選択します。ウィンドウ分割数が 9 より小さい場合、ストリームタイプはメインストリームになり、それ以外の場合はサブストリームになります。

ストリームタイプは、次の 3 つの方法で設定できます。

- リソースリストで、カメラの名前の上にカーソルを合わせて、 → **[ストリーム]** の順にクリックしてストリームタイプを選択するか、**[自動変更ストリームタイプ]** をクリックします。または、デバイスグループに対してこの操作を実行して、このグループ内のすべてのデバイスのストリームタイプを設定できます。
- ライブビューツールバーの をクリックして、ストリームタイプを選択します。ツー

ルバーの編集の詳細については、「*ツールバーに表示されるアイコンの設定*」をご覧ください。

- ライブビューウィンドウを右クリックして、**[ストリーム]** をクリックしてカメラのストリームタイプを選択します。

注記

デバイスがこの機能をサポートしている必要があります。

全画面モードでのクライアントのロック

全画面モードにした後に、キーボードの **Ctrl** キーと **L** キーを押してクライアントをロックします。クライアントをロックすると、他のウィンドウを含んでいるクライアントを現在のウィンドウ分割モードで操作できなくなります。上部の **[ロック解除]** をクリックし、クライアントのログインパスワードを入力して **[ロック解除]** をクリックし、クライアントをロック解除します。

第 7 章 リモートストレージの設定

ビデオファイルとキャプチャ画像は、ローカルデバイスの HDD、Net HDD、または SD / SDHC カード、または接続されているストレージサーバーに保存できます。

注記

使用するデバイスがこの機能に対応している必要があります。

7.1 DVR、NVR、またはネットワークカメラへの画像およびビデオの保存

DVR、NVR、およびネットワークカメラなどの一部のローカルデバイスは、ビデオファイルや画像ファイル用のストレージデバイス（HDD、Net HDD、SD / SDHC カードなど）を提供しています。ローカルデバイスのチャンネルの録画スケジュールまたはキャプチャスケジュールを設定できます。

始める前に

新たに取り付けたストレージデバイスがフォーマット済みであることを確認してください。詳細については、「*ストレージサーバーの HDD のフォーマット*」をご覧ください。

画像ファイルとビデオファイルを DVR、NVR、ネットワークカメラなどのエンコードデバイスに保存する必要がある場合は、このタスクを実行します。

手順

注記

キャプチャスケジュールによってキャプチャされた画像はローカルデバイスに保存され、デバイスのリモート設定ページで検索できます。

1.[ストレージスケジュール] モジュールを表示します。
2.[カメラグループ] リストでカメラを選択します。
3.**[エンコードデバイス上のストレージ]** エリアで **[録画スケジュール]** スイッチまたは **[キャプチャスケジュール]** スイッチをオンに設定して、デバイスのローカル録画またはキャプチャを有効にします。
4.ドロップダウンリストから録画またはキャプチャスケジュールテンプレートを選択します。

終日テンプレート

終日連続録画。

平日テンプレート

8:00 AM～8:00 PM の勤務時間連続録画。

イベントテンプレート

終日イベントトリガー録画。

テンプレート 01～08

特定のスケジュール用の固定テンプレート。必要に応じてテンプレートを編集できます。

カスタム

必要に応じてテンプレートをカスタマイズします。

注記

テンプレートを編集またはカスタマイズする必要がある場合は、「*録画スケジュールテンプレートの設定*」または「*キャプチャスケジュールテンプレートの設定*」をご覧ください。

5.[録画スケジュール] の **[詳細]** をクリックして、録画の詳細パラメータを設定します。

注記

表示される項目は、デバイスによって異なります。

事前録画

通常、イベントによってトリガーされる録画で、イベント発生前の映像を録画する場合に使用します。

事後録画

イベント終了後に、ビデオを一定時間録画することもできます。

Keep Video Files for（ビデオの保存期間）

ストレージデバイスにビデオファイルを保存しておく期間で、この期間が経過するとファイルは削除されます。値を 0 に設定すると、ファイルは永続的に保存されます。

冗長録画

ビデオファイルを R / W HDD だけでなく、冗長 HDD にも保存します。

オーディオを録音

ビデオファイルをオーディオ付きで録画するかどうかを指定します。

ビデオストリーム

録画のストリームタイプを選択します。

注記

特定のタイプのデバイスでは、カメラのメインストリームとサブストリームの両方を録画する **[デュアルストリーム]** を選択できます。このモードでは、リモート再生中にストリームタイプを切り替えることができます。再生中のストリーム切り替えについては、「*通常再生*」をご覧ください。

6.キャプチャスケジュールの **[詳細]** をクリックして、キャプチャの詳細パラメータを設定します。

解像度

連続キャプチャ画像またはイベントキャプチャ画像の解像度を選択します。

画質

連続キャプチャ画像またはイベントキャプチャ画像の画質を選択します。

間隔

2 つのキャプチャ操作間の間隔を選択します。

Captured Picture Number（キャプチャ画像番号）

イベントキャプチャの画像番号を設定します。

7.オプション: **[コピー先...]** をクリックして、録画スケジュール設定を他のチャンネルにコピーします。

8.**[保存]** をクリックして設定を保存します。

7.2 ストレージデバイスへのビデオの保存

追加したエンコードデバイスで録画されたビデオ映像を、クライアントで管理しているストレージデバイスに保存できます。

クライアントにストレージデバイスを追加して、追加したエンコードデバイスのビデオファイルを保存したり、ファイルを検索してリモート再生することができます。ストレージデバイスには、iVMS-4200 ストレージサーバー、CVR（センタービデオレコーダー: Center Video Recorder）、またはその他の NVR を使用できます。

ここでは、iVMS-4200 ストレージサーバーの設定を例にとって説明します。

7.2.1 ストレージサーバーのアクティベート

iVMS-4200 ストレージサーバーを初めて実行する場合は、ストレージサーバーをアクティベートする必要があります。

ストレージサーバーをアクティベートする必要がある場合は、このタスクを実行します。

手順

1.デスクトップで  をクリックして、iVMS-4200 ストレージサーバーを実行します。

注記

- ストレージサーバーポート（値: 8000）が他のサービスで使用されている場合は、ダイアログが表示されます。ストレージサーバーが正しく動作するように、ポート番号を他の値に変更する必要があります。
- また、別の PC にインストールされている iVMS-4200 ストレージサーバー上にビデオファイルを録画することもできます。

2.**[新パスワード]** と **[パスワードを確認]** を入力します。

注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

3.**[OK]** をクリックしてパスワードを変更します。
パスワードの変更後、ストレージサーバーが自動的に実行されます。

7.2.2 クライアントへのストレージサーバーの追加

クライアントにストレージサーバーを追加して、追加したエンコードデバイスのビデオファイルを保存できます。

手順

1.[デバイス管理] モジュールを表示します。
2.**[デバイス]** タブをクリックします。
追加したデバイスがリスト内に表示されます。
3.iVMS-4200 ストレージサーバーを追加します。
- オンラインストレージサーバーを追加できます。詳細については、「***検出されたオンラインデバイスの追加***」をご覧ください。
- ストレージサーバーは IP アドレスまたはドメイン名を使用して追加できます。詳細については、「***IP アドレスまたはドメイン名によるデバイスの追加***」をご覧ください。

7.2.3 ストレージサーバーの HDD のフォーマット

ビデオファイルストレージ用のストレージサーバーの HDD をフォーマットする必要があ

ります。

このタスクを実行して、ストレージサーバーの HDD をフォーマットします。

手順

注記

HDD のフォーマットは、ストレージ用のディスク容量を事前割り当てすることであり、フォーマットされた HDD の元のデータは削除されません。

1.[デバイス管理] モジュールを表示します。
2.**[デバイス]** タブをクリックします。
追加したデバイスがリスト内に表示されます。
3.追加したストレージサーバーをリストから選択します。
4. をクリックします。
5.**[ストレージ]** → **[全般]** の順にクリックして、[HDD Formatting(HDD をフォーマット)] ウィンドウを表示します。
6.HDD をリストから選択して、**[フォーマット]** をクリックします。
進行状況バーでフォーマットの進行状況を確認できます。フォーマットされた HDD の状態が **[未フォーマット]** から **[通常状態]** に変わります。

7.2.4 ストレージ設定の設定

ストレージサーバーが使用可能な場合は、カメラの録画スケジュールを設定できます。

始める前に

ストレージデバイスを新たに取り付けた場合は、それをフォーマットする必要があります。

手順

1.**[ストレージスケジュール]** モジュールを表示します。
2.[カメラグループ] リストでカメラを選択します。
3.**[ストレージサーバー]** ドロップダウンリストからストレージサーバーを選択します。
4.**[録画スケジュール]** スイッチをオンに設定して、ビデオファイルを保存できるようにします。
5.ドロップダウンリストから録画のスケジュールテンプレートを選択します。

注記

テンプレートを編集またはカスタマイズする必要がある場合は、「*録画スケジュールテンプレートの設定*」をご覧ください。

6.オプション: [録画スケジュール] で、**[詳細]** をクリックして、事前録画時間、事後録画時間、ビデオストリーム、およびその他のパラメータを設定します。

注記

iVMS-4200 ストレージサーバーは、メインストリームのみをサポートしています。

7.**[保存]** をクリックして設定を保存します。

7.3 ローカル PC への画像と追加情報の保存

画像と追加情報（ヒートマップ、人数集計データ、道路交通データなど）をローカル PC に保存できます。

画像や追加情報をローカル PC に保存する必要がある場合は、このタスクを実行します。

手順

1.**[ストレージスケジュール]** モジュールを表示します。
2.[カメラグループ] リストでカメラを選択します。

注記

使用するデバイスがこの機能に対応している必要があります。

3.ストレージコンテンツを選択します。

画像ストレージ

イベント発生時にカメラのアラーム画像を保存します。**[システム設定]** → **[ファイル]** の順にクリックして、画像の保存パスを変更できます。

追加情報ストレージ

追加情報（ヒートマップ、人数集計データなど）をローカル PC に保存します。

4.**[保存]** をクリックして設定を保存します。

7.4 録画スケジュールテンプレートの設定

録画スケジュールテンプレートを編集したり、録画スケジュールテンプレートをカスタマイズできます。

手順

1.[ストレージスケジュール] モジュールを表示します。
2.テンプレート設定ウィンドウを開きます。
ドロップダウンリストから **[テンプレート 01]**～**[テンプレート 08]** を選択して、**[編集]** をクリックします。ドロップダウンリストから **[カスタム]** を選択します。
3.タイムラインをドラッグして、カーソルが  に変わったら、選択したテンプレートの期間を設定します。

連続

通常および連続録画。スケジュールタイムバーが  で表示されます。

イベント録画

録画はイベントによってトリガーされます。スケジュールタイムバーが  で表示されます。

コマンド

録画はコマンドによってトリガーされます。スケジュールタイムバーが  で表示されます。

注記

コマンドトリガーによる録画は、ATM DVR がクライアントに追加されている場合に、ATM トランザクションでのみ使用できます。

注記

録画スケジュールでは、1 日に最大 8 つの期間を設定できます。

4.オプション: 期間を設定した後に、次の 1 つまたは複数の操作を実行できます。

移動	カーソルが  に変わったら、期間をドラッグして移動します。
延長または短縮	期間を選択し、カーソルが  に変わったら、期間を延長または短縮します。
正確な時間の設定	期間をクリックして、期間の正確な開始時刻と終了時刻を設定します。
削除	設定されているスケジュール期間を選択し、  をクリックして削除します。
すべてを削除	 をクリックして、設定されているすべての期間を削除します。
コピー先	1 つの日付を選択し、  をクリックして、その日付の期間設定を他の日付にコピーします。

5.オプション: テンプレート 01～08 では、必要に応じてテンプレート名を編集できます。

6.**[OK]** をクリックして設定を保存します。

注記

[カスタム] を選択してテンプレートをカスタマイズする場合、**[スケジュールテンプレートとして保存]** をクリックして、カスタムテンプレートをテンプレート 01～08 として保存できます。

7.5 キャプチャスケジュールテンプレートの設定

キャプチャスケジュールテンプレートを編集したり、キャプチャスケジュールテンプレートをカスタマイズしたりすることができます。

手順

1.[ストレージスケジュール] モジュールを表示します。
2.テンプレート設定ウィンドウを開きます。
ドロップダウンリストから **[テンプレート 01]**～**[テンプレート 08]** を選択して、**[編集]** をクリックします。ドロップダウンリストから **[カスタム]** を選択します。
3.タイムラインをドラッグして、カーソルが  に変わったら、選択したテンプレートの期間を設定します。

連続キャプチャ

通常および連続キャプチャ。スケジュールタイムバーが  で表示されます。

イベントキャプチャ

キャプチャはイベントによってトリガーされます。スケジュールタイムバーが  で表示されます。

4.オプション: 期間を設定した後に、次の 1 つまたは複数の操作を実行できます。

移動	カーソルが  に変わったら、編集した期間を移動できます。表示された時点を編集して、正確な期間を設定することもできます。
延長または短縮	カーソルが  に変わったら、選択した期間を延長または短縮できます。
削除	期間を選択し、  をクリックして削除します。
すべてを削除	 をクリックして、設定されているすべての期間を削除します。
コピー先	1 つの日付を選択し、  をクリックして、その日付の期間設定を他の日付にコピーします。

5.オプション: テンプレート 01～08 では、必要に応じてテンプレート名を編集できます。
6.**[OK]** をクリックして設定を保存します。

注記

[カスタム] を選択してテンプレートをカスタマイズする場合、**[スケジュールテンプレートとして保存]** をクリックして、カスタムテンプレートをテンプレート 01～08 として保存できます。

第 8 章 リモート再生

デバイスは、録画スケジュールに従ってビデオを録画します。ストレージサーバーとローカルデバイスに保存されているビデオファイルを表示して、事後分析のためにイベント発生プロセスを復元し、詳細に判断することができます。価値のあるビデオ映像を保存することで、ビデオ分析およびビデオ証拠の基本的な資料を提供できます。クライアントは、VCA 再生、イベント再生などの複数の再生モードをサポートしています。

- リモート再生を開始する前に、録画スケジュールが設定されていて、ビデオファイルがあることを確認してください。詳細については、「*リモートストレージの設定*」をご覧ください。
- リモート再生モードは 2 つあります。1 つは [メインビュー] モジュールでのインスタント再生です（詳細については、「*インスタント再生*」を参照）。もう 1 つは、[リモート再生] モジュールでのビデオファイルの検索と再生です。ここでは、[リモート再生] モジュールでの再生についてのみ説明します。
- ローカルデバイスとストレージサーバーの両方にビデオファイルがある場合は、ビデオファイルのソースが選択されるように設定できます。ビデオファイルの内容が同じ場合は、ストレージサーバーに保存されているビデオファイルを再生するように設定できます。詳細については、「*ライブビューおよび再生パラメータの設定*」をご覧ください。

8.1 通常再生

カメラまたはグループで通常再生するビデオファイルを検索して、見つかったビデオファイルをローカル PC にダウンロードできます。タグを追加して、重要なビデオ映像などにマークを付けることもできます。

再生ウィンドウを右クリックして、ショートカットメニューから必要な操作を選択できます。一部の操作を次に示します。

名前	説明
温度情報を表示 / 非表示	温度情報を表示 / 非表示 **注記** 温度情報のオーバーレイは、サーマルカメラでのみサポートされています。
タグ制御	ビデオファイルのデフォルトタグ（デフォルトのタグ名は [TAG]）またはカスタムタグ（タグ名は [カスタマイズ]）を追加して、ビデオの重要なポイントをマークします。タ

名前	説明
	グを編集したり、タグの位置に簡単に移動することもできます。
その他のキャプチャモード	● **キャプチャ画像を出力:** 画像をキャプチャして出力します。 ● **電子メールを送信:** 現在の画像をキャプチャして、電子メール通知を 1 つまたは複数の宛先に送信します。キャプチャ画像を添付できます。 ● **カスタムキャプチャ:** 現在の画像をキャプチャします。名前を編集して保存できます。

注記

- クラウド P2P デバイスは通常再生のみをサポートしていて、逆再生、スロー再生と早送り、タグの追加などの機能もサポートしていません。
- デバイスの他のユーザー名（admin 以外）でクライアントに追加した NVR で **[二段階認証]** が有効になっている場合は、クライアントでビデオを再生するときに、二段階認証用に作成したユーザー名とパスワードを入力するように求められます。二段階認証の詳細については、NVR のユーザーマニュアルをご覧ください。

8.1.1 ビデオファイルの検索

ビデオファイルは日付で検索できます。また、キーワードを入力して、通常再生の一致した結果をフィルタリングすることもできます。

手順

1.[リモート再生] モジュールを表示します。
2.左側にある をクリックして、［カメラの再生］ページを表示します。

3.オプション: をクリックして、検索期間の開始日と終了日を設定します。

注記

カレンダーで、スケジュールによって録画されたビデオファイルがある日付には マークが示され、イベントに基づいて録画されたビデオファイルがある日付には マークが示されます。

4.カメラの再生を開始して、選択したカメラのビデオファイルを検索します。次のいずれかの操作を行って、再生を開始できます。

注記

最大 16 台のカメラを同時に検索できます。

- カメラまたはグループを表示ウィンドウにドラッグします。
- 表示ウィンドウを選択して、カメラまたはグループをダブルクリックして、選択したウィンドウで再生を開始します。
- カメラを順番にダブルクリックして、表示ウィンドウを自動的に選択してウィンドウで再生を開始します。

8.1.2 ビデオファイルの再生

通常再生するビデオファイルを検索した後に、タイムラインを使用してビデオを再生できます。

手順

1.[リモート再生] モジュールを表示します。
2.ビデオファイルを検索します。
3.タイムラインを使用してビデオを再生します。

ビデオファイルが自動的に再生されます。タイムラインをクリックして、特定の時間の目的のビデオセグメントに移動して通常再生することができます。

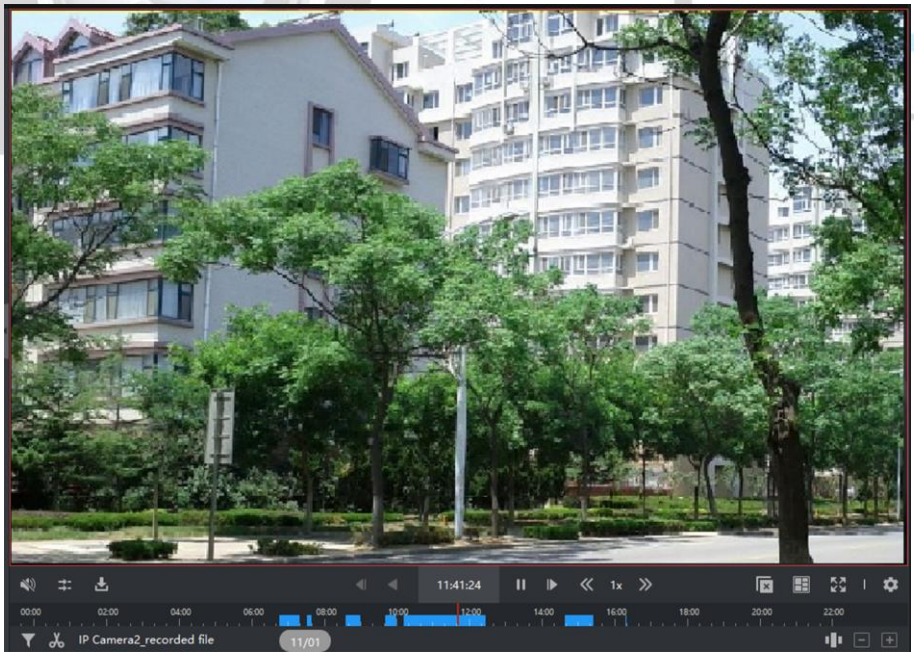

図 8-1 ビデオファイルの再生

注記

- タイムラインは、ビデオファイルの時間帯を示し、ビデオファイルはタイプ別に色分けされています。
- マウスホイールを使用するか、 / をクリックして、タイムラインバーを拡大または縮小できます。

4.オプション: ツールバーで次の操作を実行して、再生を制御します。

シングルフレーム(逆) をクリックするか、マウスホイールを下にスクロールして、ビデオファイルをフレーム単位で再生します（逆方向）。

オーディオ制御 または をクリックして、サウンドのオン / オフを切り替えます。オンにしたときに音量を調整することもできます。

複数カメラのダウンロード をクリックして、複数のカメラのビデオファイルを同時にダウンロードします。

注記

詳細については、「*複数カメラのダウンロード*」をご覧ください。

ビデオファイルを日付別にダウンロード をクリックして、カメラのビデオファイルを日付別にダウンロードしてローカル PC に保存します。

正確なポジショニング 2018/10/19 08:56:11 をクリックして、ビデオファイルを再生する正確な時点を設定します。

サムネイルの画像へジャンプ 右下隅の をクリックしてサムネール機能を有効にし、カーソルをタイムライン上に移動して、そのポイントのサムネールを表示します。サムネイルをクリックして、その画像へジャンプします。

図 8-2 再生サムネイル

注記

デバイスがこの機能をサポートしている必要があります。

8.2 アラーム入力再生

アラーム入力がトリガーされた場合、リンクされたビデオを検索してアラーム入力再生できます。この機能を使用するには、接続されているデバイスがこれをサポートしている必要があります。
アラーム入力再生ツールバーおよび表示ウィンドウの右クリックメニューの説明については、「*通常再生*」をご覧ください。

注記
一部のアイコンは、アラーム入力再生で使用できません。

8.2.1 ビデオファイルの検索

ビデオファイルは日付で検索できます。また、キーワードを入力して、アラーム入力再生の一致した結果をフィルタリングすることもできます。

手順

1.[リモート再生] モジュールを表示します。
2.左側にある をクリックして、[イベント再生] ページを表示します。

3.左側でアラーム入力チャンネルを選択します。
4.オプション: をクリックして、検索期間の開始日と終了日を設定します。
5.イベントタイプとして、ドロップダウンリストから **[アラーム入力]** を選択します。
6.**[検索]** をクリックして検索を開始します。
選択したアラーム入力の一致したビデオファイルが、右ページに時系列順に表示されます。デフォルトでは、最初のビデオファイルが自動的に再生されます。
7.オプション: **[検索]** フィールドにキーワードを入力して、結果をフィルタリングします。

8.2.2 ビデオファイルの再生

アラーム入力再生するビデオファイルを検索した後に、ファイルリストまたはタイムラインを使用してビデオを再生できます。

手順

1.[リモート再生] モジュールを表示します。
2.左側にある をクリックして、[イベント再生] ページを表示します。
3.アラーム入力のビデオファイルを検索します。

注記

アラーム入力のビデオファイルの検索の詳細については、「*ビデオファイルの検索*」をご覧ください。

4.ファイルリストまたはタイムラインを使用してビデオを再生します。
- ビデオファイルをダブルクリックして、再生表示ウィンドウでビデオを再生します。
- タイムラインをクリックして、特定の時間の目的のビデオセグメントに移動してアラーム入力再生します。

注記

- タイムラインは、ビデオファイルの時間帯を示し、ビデオファイルはタイプ別に色分けされています。
- マウスホイールを使用するか、 / をクリックして、タイムラインバーを拡大または縮小できます。

8.3 イベント再生

動体検知、VCA 検知、動作分析などのイベントによってトリガーされた録画ビデオファイルを検索して、イベント再生できます。この機能を使用するには、接続されているデバイスがこれをサポートしている必要があります。
イベント再生ツールバーおよび表示ウィンドウの右クリックメニューの説明については、「*通常再生*」をご覧ください。

注記

一部のアイコンは、イベント再生で使用できません。

8.3.1 ビデオファイルの検索

ビデオファイルは日付またはイベントタイプで検索できます。また、キーワードを入力して、イベント再生の一致した結果をフィルタリングすることもできます。

手順

1.[リモート再生] モジュールを表示します。
2.左側にある をクリックして、[イベント再生] ページを表示します。
3.左側でカメラを選択します。
4.オプション: をクリックして、検索期間の開始日と終了日を設定します。

注記

カレンダーで、スケジュールによって録画されたビデオファイルがある日付には マークが示され、イベントに基づいて録画されたビデオファイルがある日付には マークが示されます。

5.ドロップダウンリストから、イベントタイプを選択します。
6.**[検索]** をクリックして検索を開始します。
一致するビデオファイルが右ページに時系列順に表示されます。デフォルトでは、最初のビデオファイルが自動的に再生されます。
7.オプション: **[検索]** フィールドにキーワードを入力して、結果をフィルタリングします。

8.3.2 ビデオファイルの再生

イベント再生するビデオファイルを検索した後に、ファイルリストまたはタイムラインを使用してビデオを再生できます。

手順

1.[リモート再生] モジュールを表示します。
2.左側にある をクリックして、[イベント再生] ページを表示します。
3.イベントに基づいて録画されたビデオファイルを検索します。
4.ビデオファイルを再生します。
– ビデオファイルをダブルクリックして、再生表示ウィンドウでビデオを再生します。
– タイムラインをクリックして、特定の時間の目的のビデオセグメントに移動してイベント再生します。

注記

- タイムラインは、ビデオファイルの時間帯を示し、ビデオファイルはタイプ別に色分けされています。
- マウスホイールを使用するか、 / をクリックして、タイムラインバーを拡大または縮小できます。

8.4 ATM 再生

ATM DVR のビデオファイルを検索して、ATM 再生することができます。この機能を使用するには、接続されているデバイスがこれをサポートしていて、トランザクションルールが設定されている必要があります。
ATM 再生ツールバーおよび表示ウィンドウの右クリックメニューの説明については、「*通常再生*」をご覧ください。

注記

一部のアイコンは、ATM 再生で使用できません。

8.4.1 ビデオファイルの検索

ATM DVR のビデオファイルは、カード番号、トランザクションタイプ、トランザクションの量、ファイルタイプ、または日付で検索できます。また、キーワードを入力して、ATM 再生の一致した結果をフィルタリングすることもできます。

手順

1.[リモート再生] モジュールを表示します。
2.左側にある をクリックして、[ATM 再生] ページを表示します。
3.左側で ATM DVR のカメラを選択します。

4.オプション: をクリックして、検索期間の開始日と終了日を設定します。
5.検索条件を設定します。

カード番号別

ATM 情報に含まれているカード番号を入力します。

Search by Transaction Type（トランザクションタイプで検索）

検索するトランザクションタイプを選択し、関連するトランザクション量を入力します。

ファイルのタイプ

検索するビデオファイルのタイプを選択します。

6.**[検索]** をクリックして検索を開始します。
選択した ATM DVR の一致したビデオファイルが、[リモート再生] ページの右側に時系列順に表示されます。デフォルトでは、最初のビデオファイルが自動的に再生されます。
7.オプション: **[検索]** フィールドにキーワードを入力して、結果をフィルタリングします。

8.4.2 ビデオファイルの再生

ATM DVR に接続されたカメラのビデオファイルを検索した後に、ファイルリストまたはタイムラインを使用してビデオを再生できます。

手順

1.[リモート再生] モジュールを表示します。
2.左側にある をクリックして、[ATM 再生] ページを表示します。
3.ATM DVR に接続されたカメラのビデオファイルを検索します。
4.ビデオファイルを再生します。

– ビデオファイルをダブルクリックして、再生表示ウィンドウでビデオを再生します。
– タイムラインをクリックして、特定の時間の目的のビデオセグメントに移動して ATM 再生します。

注記

- タイムラインは、ビデオファイルの時間帯を示し、ビデオファイルはタイプ別に色分けされています。
- マウスホイールを使用するか、 / をクリックして、タイムラインバーを拡大または縮小できます。

8.5 POS 再生

POS 情報が含まれているビデオファイルを検索して、POS 再生できます。この機能を使用するには、接続されているデバイスがこれをサポートしていて、POS テキストオーバーレイが設定されている必要があります。
POS 再生ツールバーおよび表示ウィンドウの右クリックメニューの説明については、「*通常再生*」をご覧ください。

注記

一部のアイコンは、POS 再生で使用できません。

8.5.1 ビデオファイルの検索

POS 情報が含まれているビデオファイルは、キーワードまたは日付で検索できます。

手順

1.[リモート再生] モジュールを表示します。
2.左側にある をクリックして、[POS 再生] ページを表示します。

3.左側でカメラを選択します。
4.オプション: をクリックして、検索期間の開始日と終了日を設定します。
5.検索条件を設定します。

キーワード

ATM 情報に含まれているカード番号を入力します。

注記

キーワードは一度に 3 つまで入力できます。各キーワードをカンマで区切る必要があります。

組み合わせモード

複数のキーワードを入力する場合は、「または（|）」を選択していずれかのキーワードを含む POS 情報を検索するか、「および（&）」を選択してすべてのキーワードを含む POS 情報を検索できます。

大文字と小文字を区別

キーワードの大文字と小文字を区別して POS 情報を検索するには、**[大文字と小文字を区別]** にチェックを入れます。

6.**[検索]** をクリックして検索を開始します。

POS 情報が含まれているビデオファイルが、[POS 再生] ページの右側に時系列順に表示されます。デフォルトでは、最初のビデオファイルが自動的に再生されます。

7.オプション: **[検索]** フィールドにキーワードを入力して、結果をフィルタリングします。

8.5.2 ビデオファイルの再生

POS 情報が含まれているビデオファイルを検索した後に、ファイルリストまたはタイムラインを使用してビデオを再生できます。

始める前に

POS 情報オーバーレイが設定されたカメラの通常再生を開始します。

手順

1.[リモート再生] モジュールを表示します。

2.左側にある をクリックして、[POS 再生] ページを表示します。

3.POS 情報が含まれているビデオファイルを検索します。

4.ファイルリストまたはタイムラインを使用してビデオを再生します。

- ビデオファイルをダブルクリックして、再生表示ウィンドウでビデオを再生します。
- タイムラインをクリックして、特定の時間の目的のビデオセグメントに移動して POS 再生します。

注記

- タイムラインは、ビデオファイルの時間帯を示し、ビデオファイルはタイプ別に色分けされています。
- マウスホイールを使用するか、 / をクリックして、タイムラインバーを拡大または縮小できます。

8.6 VCA 再生

検索されたビデオファイルに対して VCA ルールを設定して、動体検知、ラインクロス検

知、侵入検知などの VCA イベントが発生したビデオ映像を検索できます。この機能により、該当するビデオを検索して、それを赤でマークすることができます。

始める前に

VCA 機能を備えたデバイスが設置されていることを確認してください。

手順

注記

VCA 再生は単一ウィンドウでのみサポートされていて、同期再生と非同期再生はサポートされていません。

1.[リモート再生] モジュールを表示します。
2.左側にある をクリックして、[カメラの再生] ページを表示します。
3.カメラを選択して、カメラのビデオ再生を開始します。

4.[VCA 検索] メニューを表示します。
- 再生ウィンドウを右クリックしてショートカットメニューを表示して、**[VCA 検索]** をクリックします。
- 再生ウィンドウの右下隅の をクリックします。

5.VCA タイプを有効にして、検知領域を描画して感度を設定します。

動体検知

ビデオの表示が変わると（人が通過した、レンズが動いたなど）、タイムライン上でビデオ映像が赤でマークされ、自動アラームシーンまたは門番不在シーンに使用されます。

ラインクロス検知

ビデオにバーチャルラインを描画して、人物、車両、その他の動体がバーチャルラインを横切ったこと（両方向からのラインクロス）をクライアントが検知した場合に、タイムライン上でビデオ映像が赤でマークされるようにすることができます。

侵入検知

ビデオにバーチャル領域を描画して、定義済みの領域に人物、車両、その他の動体が侵入した場合に、タイムライン上でビデオ映像が赤でマークされるようにすることができます。

VCA 設定

感度を設定し、対象の特徴（人間の性別や年齢、メガネ着用など）を設定して、検索されたビデオファイルをフィルタリングします。属性が設定した属性と一致する人物がビデオに登場すると、タイムライン上でビデオ映像が赤でマークされます。

注記

感度が高いほど、一致した人物の精度が高くなります。

6.オプション: をクリックして、検索期間の開始日と終了日を設定します。
7.VCA の再生を開始します。
定義された領域で発生した VCA イベントは、タイムライン上で赤でマークされます。

注記

- デフォルトでは、該当するビデオの再生速度は 1 倍速で、該当しないビデオの再生速度は 8 倍速になります。
- [システム設定] で、VCA 再生中に該当しないビデオをスキップするように設定できます。これにより、VCA 再生中に該当しないビデオが再生されなくなります。詳細については、「*ライブビューおよび再生パラメータの設定*」をご覧ください。
- VCA 再生を無効にする必要がある場合は、VCA 再生ウィンドウを右クリックして、**[VCA 検索]** をクリックして VCA 再生を無効にします。

8.7 同期再生

デフォルトでは、クライアントは複数のカメラのビデオファイルを非同期再生モードで再生します。ビデオファイルの再生時間は、ビデオファイルごとに異なります。同期再生では、ビデオファイルを同期された状態で再生できます。

手順

注記

- 最大 16 台のカメラのビデオファイルを同時に再生できます。
- 同期および非同期再生は、ATM ビデオ再生および VCA 再生モードではサポートされていません。
- イベントビデオ再生と POS ビデオ再生は同期再生のみをサポートしています。複数のカメラをリンクするには、**[メンテナンスと管理]** → **[イベント管理]** に移動して、イベントタイプに応じてリンクされたカメラを有効にします。

1.[リモート再生] モジュールを表示します。
2.少なくとも 2 台のカメラの再生を開始します。
3.ツールバーの をクリックして、同期再生を有効にします。

再生中のカメラが同期再生を開始します。
4. をクリックして同期再生を無効にします。

8.8 フィッシュアイカメラのビデオ再生

フィッシュアイカメラのビデオを再生した場合、映像にゆがみが生じることがあります。細部をはっきりと観察するには、フィッシュアイ展開機能を有効にして、ゆがみのないビューに修正します。クライアントは、複数のフィッシュアイレンズ拡張モード（パノラマ、半球、PTZ、フィッシュアイ + PTZ モードなど）をサポートしています。

手順

注記

その他の再生制御手順については、「*通常再生*」をご覧ください。一部のアイコンは、フィッシュアイ再生で使用できません。

1.[リモート再生] モジュールを表示します。
2.フィッシュアイカメラを選択して再生を開始します。

注記

再生と再生制御の詳細については、「*通常再生*」をご覧ください。

3.フィッシュアイ展開モードを表示します。
- 表示ウィンドウを右クリックして、**[フィッシュアイ展開]** を選択します。
- ツールバーの をクリックします。ツールバーの設定の詳細については、「*ツールバーに表示されるアイコンの設定*」をご覧ください。

注記

フィッシュアイ展開の再生でのマウントタイプは、ライブビューでのマウントタイプに応じて設定されます。詳細については、「*フィッシュアイモードでのライブビューの実行*」をご覧ください。

が に変わります。

4.表示エリアの左下隅の をクリックして、必要に応じて再生の展開モードを選択します。

フィッシュアイ

フィッシュアイビューモードでは、カメラの全方位広角ビューが表示されます。このビューモードは、魚の凸形眼の視覚に近いため、**フィッシュアイ**と呼ばれます。レンズは、画像内の物体の遠近感と角度を歪ませながら、広いエリアの曲線画像を生成します。

パノラマ / デュアル 180° パノラマ / 360° パノラマ

[パノラマ] ビューモードでは、いくつかの較正方法によってゆがみのあるフィッシュアイ画像が通常の遠近法画像に変換されます。

PTZ

PTZ ビューは [フィッシュアイ] ビューまたは [パノラマ] ビュー内の定義されたエリアのクローズアップビューで、電子 PTZ 機能（e-PTZ ともいいます）をサポートしています。

注記

[フィッシュアイ] ビューおよび [パノラマ] ビューで、各 PTZ ビューには特定のナビゲーションボックスが表示されます。[フィッシュアイ] ビューまたは [パノラマ] ビューのナビゲーションボックスをドラッグして PTZ ビューを調整するか、PTZ ビューをドラッグしてビューを目的の角度に調整できます。

半球

半球モードでは、画像をドラッグして直径を中心に回転させて、ビューを目的の角度に調整できます。

AR 半球

AR 半球モードは、遠方と近方の画像が重ねられるため、立体画像を広角で表示することができます。

シリンダー

シリンダーモードでは、画像がシリンダー状のページとして表示され、画像を任意の方向にドラッグして検知エリアのあらゆる場所を表示できます。

5. オプション: フィッシュアイビューモードで再生ウィンドウを右クリックして、選択したウィンドウを全画面モードに切り替えることができます。

注記

ウィンドウを右クリックして **[全画面を終了]** を選択して、全画面モードを終了できます。

8.9 低帯域幅での再生

ネットワーク帯域幅が狭い場合、帯域幅の制限によりビデオストリーミングの速度が大幅に遅くなることがあります。低帯域幅のユーザーに低いストリーミング速度で通常の品質を提供できるように、クライアントは低帯域幅での再生モードを提供しています。その前に、ストリーミングプロトコルを設定したり、他の操作を実行する必要があります。
設定の詳細については、「***ネットワーク帯域幅が狭いときにライブビューと再生のパフォーマンスを向上させるにはどうしたら良いですか?***」をご覧ください。

第 9 章 ビデオ映像のダウンロード

再生中に、1 台または複数のカメラのビデオファイルをローカル PC にダウンロードできます。

注記

- クラウド P2P デバイスのビデオファイルはダウンロードできません。
- デバイスの他のユーザー名（admin 以外）でクライアントに追加した NVR で **[二段階認証]** が有効になっている場合は、クライアントでビデオを再生するときに、二段階認証用に作成したユーザー名とパスワードを入力するように求められます。二段階認証の詳細については、NVR のユーザーマニュアルをご覧ください。

9.1 日付別でのビデオ映像のダウンロード

再生中にカメラのビデオ映像をダウンロードして、ローカル PC に保存できます。

手順

1.[リモート再生] ページを表示して、カメラを選択して再生を開始します。

注記

再生の開始方法の詳細については、「*リモート再生*」をご覧ください。

2.画像を右クリックして、**[ダウンロード]** をクリックします。

3.ダウンロードするビデオ映像の開始時間と終了時間を設定します。
4.ビデオ映像の名前を入力します。
5.**[OK]** をクリックして、ビデオ映像のローカル PC へのダウンロードを開始します。

9.2 複数カメラのビデオファイルのダウンロード

複数のカメラの再生中に、日付別で複数のカメラのビデオファイルを同時にダウンロードできます。

手順

1.[リモート再生] ページを表示して、複数のカメラを選択して再生を開始します。

注記

再生の開始方法の詳細については、「*リモート再生*」をご覧ください。

2. をクリックして、[複数のカメラのダウンロード] ウィンドウを開きます。

再生中のすべてのカメラが表示されます。

3.ビデオファイルをダウンロードするカメラを選択します。

4.各カメラのビデオの開始時刻と終了時刻を設定します。

5.オプション: **[プレイヤーをダウンロード]** にチェックを入れて、プレイヤーをダウンロードします。

6.**[ダウンロード]** をクリックして、設定した時間のビデオファイルのローカル PC へのダウンロードを開始します。

進行状況バーに、各カメラのビデオファイルのダウンロードプロセスが表示されます。

7.オプション: 手動でダウンロードを停止するには、**[停止]** をクリックします。

注記

最大 16 台のカメラのビデオファイルを同時にダウンロードできます。

第 10 章イベントの設定

イベントは、特定の状況をセキュリティ担当者に通知するのに使用され、これにより速やかに対処することができます。イベントは、通知とイベント処理の一連のリンク操作（音声による警告や電子メールの送信など）をトリガーできます。イベントを有効にして、クライアントに追加したリソースのリンク操作を設定できます。選択したイベントが発生すると、クライアントはイベント通知をリアルタイムで受信するため、ユーザーは詳細を確認してイベントを適宜処理できます。
次のタイプをサポートしています。

ビデオイベント

ビデオイベントとは、ビデオ例外、監視エリアの例外、アラーム入力、エンコードデバイスの例外などによってトリガーされる特別なイベントのことです。詳細については、「*カメラのイベントの設定*」、「*アラーム入力のイベントの設定*」、「*エンコードデバイスのイベントの設定*」をご覧ください。

入退室管理イベント

入退室管理イベントとは、入退室管理デバイス、ドア、カードリーダー、エレベータ、ビデオインターコムデバイスなどでトリガーされる特別なイベントのことです。詳細については、「*アクセスイベントに対するクライアントアクションの設定*」および「*ビデオインターコムイベントの設定*」をご覧ください。

セキュリティコントロールイベント

セキュリティコントロールイベントとは、セキュリティコントロールパネルのゾーンによってトリガーされる特別なイベントのことです。詳細については、「*ゾーンイベントのクライアントリンケージの設定*」をご覧ください。

10.1 カメラのイベントの設定

カメラのイベントとは、ビデオ例外、またはカメラの監視領域で検知されたイベント（動体検知、ビデオロス、ラインクロスなど）のことです。クライアントでカメラのイベントを有効にすることができます。カメラでイベントがトリガーされたときに、クライアントは確認のためにイベントを受信および記録して、一連のリンク操作（電子メールの送信など）をトリガーして通知することができます。

手順

1.**[イベント設定]** → **[ビデオイベント]** → **[カメラ]** の順にクリックします。

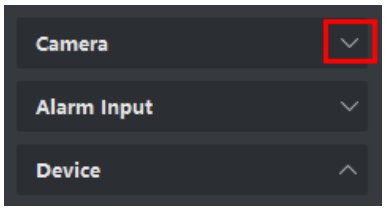

図 10-1 カメラリソースの表示

2.グループを展開し、イベントソースとしてカメラを選択します。

注記

リソースがオンラインであることを確認してください。

選択したカメラでサポートされているすべてのイベントタイプが表示されます。

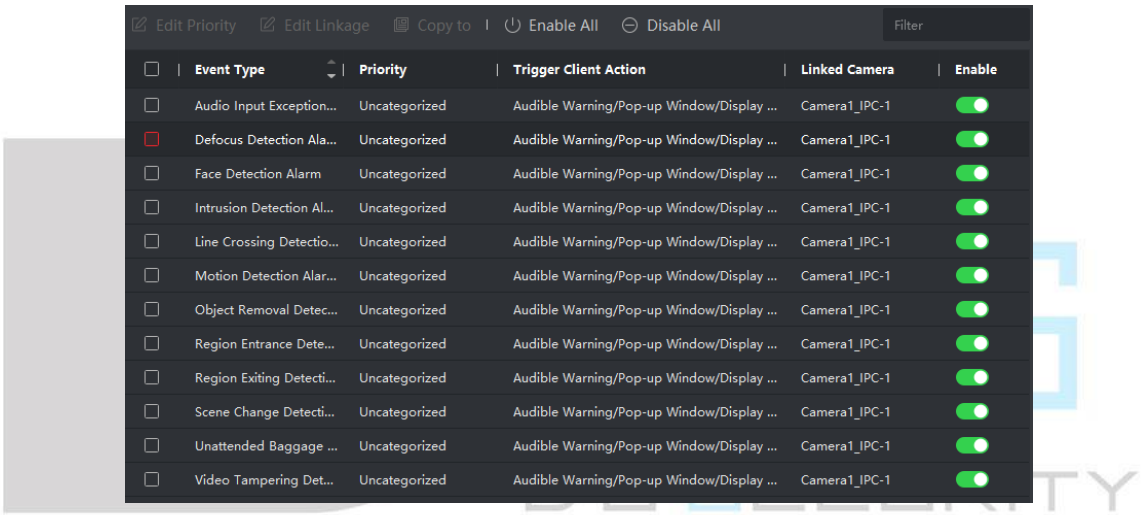

図 10-2 カメラのイベントの設定

3.オプション: **[フィルタ]** フィールドにキーワードを入力して、目的のイベントをすばやく見つけます。

4.オプション: [有効] 列のスイッチをオンにしてイベントタイプを有効にするか、**[すべて有効化]** をクリックしてこのカメラのすべてのイベントタイプを有効にします。

注記

有効にすると、クライアントがイベントを受信して、リンク操作がトリガーされます。また、1 つのイベントタイプを無効にすることも、すべてのイベントタイプを無効にすることもできます。

5.オプション: イベントを選択し、次の操作を実行します。

優先度を編集 **[優先度の編集]** をクリックして、イベントの優先度を設定します。
優先度は、イベントの緊急度を表します。

イベントリンクを編集　**[イベントリンクの編集]** をクリックして、イベントのリンク操作を設定します。

音声による警告

イベントがトリガーされたときに、クライアントの音声による警告がトリガーされます。ドロップダウンリストでオーディオファイルを選択するか、**[追加]** をクリックして新しいオーディオファイル（WAV 形式）を追加できます。

をクリックして、選択したオーディオファイルを試聴することができます。

電子メールを送信

アラーム情報の電子メール通知を 1 つまたは複数の宛先に送信します。

電子メールのパラメータ設定の詳細については、「*電子メールのパラメータ設定*」をご覧ください。

ポップアップウィンドウ

イベントがトリガーされたときに、クライアント上にイベント関連情報（イベントの詳細、ソースカメラのライブビデオ、リンクされたカメラのキャプチャ画像など）を示すポップアップウィンドウが表示されます。イベントの処理方法に関する注記を入力することもできます。

Display on Map（マップ上に表示）

イベントソースをマップ上にホットスポットとして追加すると、イベントがトリガーされたときにホットスポットが表示され、その横で が光ります。これにより、セキュリティ担当者はイベントの場所を容易に確認することができます。

ホットスポットをクリックして、イベントの詳細と、リンクされたカメラのライブビデオを表示することもできます。

リンク済みカメラ

イベントがトリガーされたときに画像をキャプチャするかビデオを録画するには、選択したカメラをリンクします。

[コピー先] をクリックして、このカメラのイベント設定を他のカメラにコピーします。

注記

イベント設定は、同じタイプのリソースにのみコピーできます。

次に行う操作

カメラが属しているデバイスで警戒を開始する必要があります。そうしないと、クライアントは設定されたイベントを受信できません。詳細については、「*デバイスからのイベン*

ト受信の有効化」をご覧ください。

10.2 アラーム入力のイベントの設定

アラーム入力のイベントとは、アラーム入力によってトリガーされるイベントのことです。クライアントで、アラーム入力のイベントを有効にできます。アラーム入力がトリガーされたときに、クライアントは確認のためにイベントを受信および記録して、一連のリンク操作（電子メールの送信など）をトリガーして通知することができます。

手順

1.**[イベント設定]** → **[ビデオイベント]** → **[アラーム入力]** の順にクリックします。

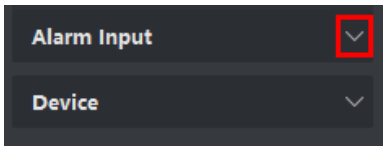

図 10-3 アラーム入力リソースの表示

2.グループを展開して、イベントソースとしてアラーム入力を選択します。

注記

リソースがオンラインであることを確認してください。

選択したアラーム入力でサポートされているすべてのイベントタイプが表示されます。

3.オプション: **[フィルタ]** フィールドにキーワードを入力して、目的のイベントをすばやく見つけます。

4.オプション: [有効] 列のスイッチをオンにしてイベントタイプを有効にするか、**[すべて有効化]** をクリックしてこのアラーム入力のすべてのイベントタイプを有効にします。

注記

有効にすると、クライアントがイベントを受信して、リンク操作がトリガーされます。また、1 つのイベントタイプを無効にすることも、すべてのイベントタイプを無効にすることもできます。

5.オプション: イベントを選択し、次の操作を実行します。

優先度を編集	**[優先度の編集]** をクリックして、イベントの優先度を設定します。 優先度は、イベントの緊急度を表します。
イベントリンクを編集	**[イベントリンクの編集]** をクリックして、イベントのリンク操作を設定します。

音声による警告

イベントがトリガーされたときに、クライアントの音声による警告がトリガーされます。ドロップダウンリストでオーディオファイルを選択するか、**[追加]** をクリックして新しいオーディオファイル（WAV 形式）を追加できます。
をクリックして、選択したオーディオファイルを試聴することができます。

電子メールを送信

アラーム情報の電子メール通知を 1 つまたは複数の宛先に送信します。
電子メールのパラメータ設定の詳細については、「*電子メールのパラメータ設定*」をご覧ください。

ポップアップウィンドウ

イベントがトリガーされたときに、クライアント上にイベント関連情報（イベントの詳細、ソースカメラのライブビデオ、リンクされたカメラのキャプチャ画像など）を示すポップアップウィンドウが表示されます。イベントの処理方法に関する注記を入力することもできます。

Display on Map（マップ上に表示）

イベントソースをマップ上にホットスポットとして追加すると、イベントがトリガーされたときにホットスポットが表示され、その横で が光ります。これにより、セキュリティ担当者はイベントの場所を容易に確認することができます。
ホットスポットをクリックして、イベントの詳細と、リンクされたカメラのライブビデオを表示することもできます。

リンク済みカメラ

イベントがトリガーされたときに画像をキャプチャするかビデオを録画するには、選択したカメラをリンクします。

[コピー先] をクリックして、このアラーム入力のイベント設定を他のアラーム入力にコピーします。

注記

イベント設定は、同じタイプのリソースにのみコピーできます。

次に行う操作

アラーム入力が属しているデバイスで警戒を開始する必要があります。そうしないと、クライアントは設定されたイベントを受信できません。詳細については、「*デバイスからのイベント受信の有効化*」をご覧ください。

10.3 エンコードデバイスのイベントの設定

エンコードデバイスのイベントとは、デバイスのオフラインなど、エンコードデバイスの例外のことです。クライアントに追加したエンコードデバイスのイベントを有効にすることができます。デバイスでイベントがトリガーされたときに、クライアントは確認のためにイベントを受信および記録して、一連のリンク操作（電子メールの送信など）をトリガーして通知することができます。

手順

1.**[イベント設定]** → **[ビデオイベント]** → **[デバイス]** の順にクリックします。

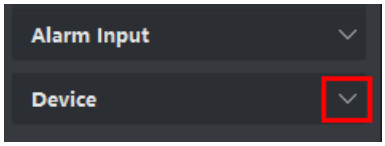

図10-4 デバイスリソースの表示

2.イベントソースとしてデバイスを選択します。

注記

リソースがオンラインであることを確認してください。

選択したデバイスでサポートされているすべてのイベントタイプが表示されます。

3.オプション: **[フィルタ]** フィールドにキーワードを入力して、目的のイベントをすばやく見つけます。

4.オプション: [有効] 列のスイッチをオンにしてイベントタイプを有効にするか、**[すべて有効化]** をクリックしてこのデバイスのすべてのイベントタイプを有効にします。

注記

有効にすると、クライアントがイベントを受信して、リンク操作がトリガーされます。また、1 つのイベントタイプを無効にすることも、すべてのイベントタイプを無効にすることもできます。

5.オプション: イベントを選択し、次の操作を実行します。

優先度を編集	**[優先度の編集]** をクリックして、イベントの優先度を設定します。 優先度は、イベントの緊急度を表します。
イベントリンクを編集	**[イベントリンクの編集]** をクリックして、イベントのリンク操作を設定します。

音声による警告

イベントがトリガーされたときに、クライアントの音声による警告がトリガーされます。

ドロップダウンリストでオーディオファイルを選択するか、**[追加]** をクリックして新しいオーディオファイル（WAV 形式）を追加できます。
をクリックして、選択したオーディオファイルを試聴することができます。

電子メールを送信

アラーム情報の電子メール通知を 1 つまたは複数の宛先に送信します。
電子メールのパラメータ設定の詳細については、「*電子メールのパラメータ設定*」をご覧ください。

[コピー先] をクリックして、このデバイスのイベント設定を他のデバイスにコピーします。

注記
イベント設定は、同じタイプのリソースにのみコピーできます。

次に行う操作

このデバイスで警戒を開始する必要があります。そうしないと、クライアントは設定されたイベントを受信できません。詳細については、「*デバイスからのイベント受信の有効化*」をご覧ください。

第11章 イベントセンター

クライアントが受信したイベント情報（デバイスオフラインなど）が表示されます。イベントセンターでは、リアルタイムイベントと過去イベントの詳細情報の確認、イベントがリンクされたビデオの表示、イベントの処理などを行うことができます。
クライアントがデバイスからイベント情報を受信するには、リソースのイベントを有効にして、デバイスで警戒を開始する必要があります。詳細については、「*イベントの設定*」および「*デバイスからのイベント受信の有効化*」をご覧ください。
ポップアップアラーム情報を表示するには、イベントセンターでイベントトリガーポップアップ画像を有効にする必要があります。詳細については、「*ポップアップイベント情報の表示*」をご覧ください。

11.1 デバイスからのイベント受信の有効化

クライアントソフトウェアがデバイスからイベント通知を受信するには、そのデバイスの自動監視を有効化する必要があります。

手順

1. → **[ツール]** → **[デバイス監視制御]** の順にクリックし、[デバイス監視制御] ページを開きます。
   このページには追加したすべてのデバイスが表示されます。
2. [自動監視] 列内でスイッチを入れ、自動監視を有効化します。

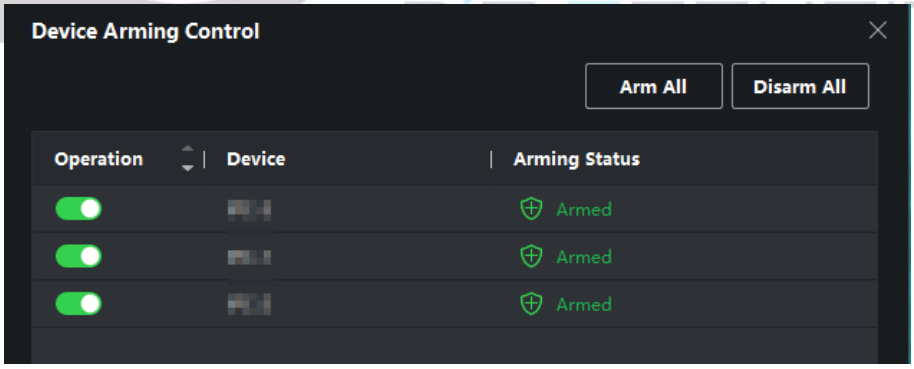

図11-1 デバイスの警戒開始

スイッチをオンにすると、デバイスが自動監視されます。また、警戒が開始されているデバイスによってトリガーされたイベントに関する通知は、クライアントソフトウェアにリアルタイムで自動送信されます。

11.2 リアルタイムイベントの表示

接続されたリソースのクライアントが受信したリアルタイムイベント情報が表示されます。イベントソース、イベント時間、優先度など、リアルタイムイベント情報を確認できます。

始める前に

クライアントがデバイスからイベントを受信するには、デバイスからのイベント受信を有効化する必要があります。詳細については、「*デバイスからのイベント受信の有効化*」をご覧ください。

手順

1.**[イベントセンター]** → **[リアルタイムイベント]** の順にクリックしてリアルタイムイベントのページに入ると、クライアントが受信したリアルタイムイベントを確認できます。

イベント時間

エンコードデバイスの場合、イベント時間とは、クライアントがイベントを受信した時間のことです。他のデバイスタイプの場合、イベント時間はイベントがトリガーされた時間のことです。

優先

優先度は、イベントの緊急度を表します。

2.イベントをフィルタリングします。

デバイスタイプおよび / または優先度でフィルタリング	イベントをフィルタリングするデバイスタイプ / または優先度を選択します。
キーワードでフィルタリング	イベントをフィルタリングするキーワードを入力します。

3.オプション: イベントリスト表のヘッダー部分を右クリックして、イベント関連の項目がイベントリストに表示されるようにカスタマイズします。

4.イベントの詳細を表示します。

1）イベントリストからイベントを選択します。

2）ページ右下隅の **[展開]** をクリックします。

3）イベント関連の画像、詳細説明、処理記録を表示します。

4）オプション: 関連する画像にカーソルを合わせ、画像の右上隅のダウンロードアイコンをクリックすると、ローカル PC へダウンロードできます。保存パスは手動で設定できます。

5.オプション: 必要に応じて以下の操作を実行してください。

単一イベントの処理	**[Handle（処理）]** をクリックして処理の候補ページに入り、**[Commit（コミット）]** をクリックします。

注記

イベントが処理されると、**[処理]** ボタンが **[注記の追加]** になります。この処理済みイベントにさらに注記を追加するには、**[注記の追加]** をクリックします。

イベントの一括処理	処理が必要な複数のイベントを選択し、**[Handle in Batch（一括処理）]** をクリックします。処理の候補ページに入り、**[Commit（コミット）]** をクリックします。
アラーム音声の有効化 / 無効化	**[音声を有効化]** / **[音声を無効化]** をクリックしてイベントの音声を有効化 / 無効化します。
最新のイベントを自動選択	**[最新のイベントを自動選択]** にチェックを入れると、最新のイベントが自動的に選択され、イベントの詳細情報が表示されます。
イベントの消去	**[消去]** をクリックすると、イベントリスト内のすべてのイベントを消去できます。
電子メールを送信	イベントを選択して**[E メール送信]** をクリックすると、そのイベントの詳細情報が電子メールで送信されます。

注記

最初に電子メールのパラメータを設定する必要があります。詳細については、「*電子メールのパラメータ設定*」をご覧ください。

11.3 過去のイベントの検索

イベントセンターページの [イベント検索] モジュールでは、特定のデバイスタイプに合わせて、時刻やデバイスタイプなどの条件で過去のイベントを検索し、イベントを処理できます。

始める前に

クライアントがデバイスからイベント通知を受信するには、デバイスからのイベント受信を有効化する必要があります。詳細については、「*デバイスからのイベント受信を有効化する*」をご覧ください。

手順

1.**[イベントセンター]** → **[イベント検索]** の順にクリックし、イベント検索のページを表示します。
2.フィルター条件を設定して目的のイベントのみを表示させます。

時間

イベントの開始時刻です。

検索条件

デバイス

デバイスまたはデバイスのリソースチャンネルでイベントを検索します。デバイスで検索する場合は、次の項目を設定する必要があります。

- **Include Sub-Node（サブノードを含める）**：デバイスとすべてのリソースチャンネルのイベントを検索します。
- **デバイスタイプ**: 検索するイベントのデバイスタイプです。

グループ

グループ内のリソースチャンネルでイベントを検索します。

注記

- ビデオインターコムデバイスの場合は、検索範囲として [すべて] または [ロックログ] を選択する必要があります。
- 入退室管理デバイスの場合は、**[詳細を表示]** をクリックして、状態、イベントタイプ、カードリーダータイプ、人物名、カード番号、および組織などのその他の条件を設定できます。

優先

優先度には、低、中、高、カテゴリなしがあり、これはイベントの緊急度を示します。

状態

イベントの処理ステータスを示します。

3.**[検索]** をクリックし、設定した条件と一致するイベントを検索します。
4.オプション: イベントリスト表のヘッダー部分を右クリックして、イベント関連の項目がイベントリストに表示されるようにカスタマイズします。

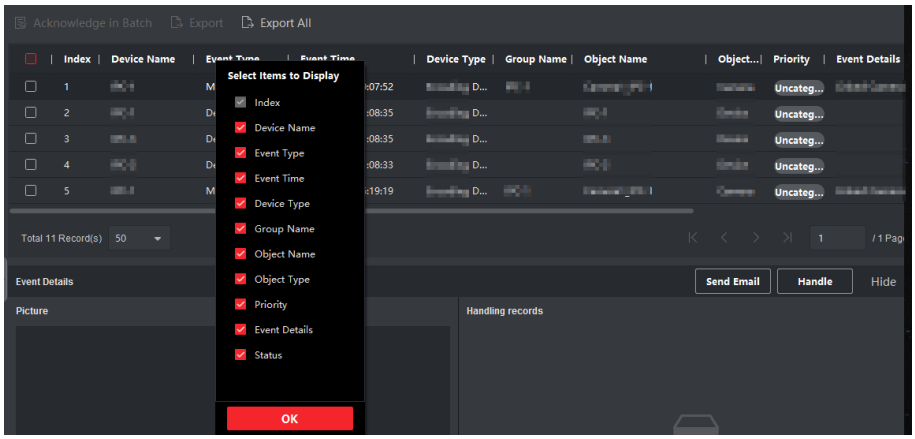

図11-2 表示するイベント関連の項目のカスタマイズ

5.オプション: 以下の操作のうち 1 つを実行します。

単一イベントを処理

単一イベントの処理: 処理の必要な単一のイベントを選択し、イベントの詳細情報ページで **[Handle（処理）]** をクリックして処理の候補ページを表示します。

注記

イベントの処理後、**[Handle（処理）]** ボタンが **[Add Remark（注記の追加）]** に切り替わります。その後、**[Add Remark（注記の追加）]** をクリックし、処理済みイベントの詳細情報を追加します。

イベントを一括処理

イベントの一括処理: 処理の必要なイベントを複数選択して **[Handle in a Batch（一括処理）]** をクリックし、処理の候補ページを表示します。

注記

イベントの処理後、**[Handle（処理）]** ボタンが **[Add Remark（注記の追加）]** に切り替わります。その後、**[Add Remark（注記の追加）]** をクリックし、処理済みイベントの詳細情報を追加します。

電子メールを送信

イベントを選択して**[E メール送信]** をクリックすると、そのイベントの詳細情報が電子メールで送信されます。

注記

最初に電子メールのパラメータを設定する必要があります。詳細

については、「*電子メールのパラメータ設定*」をご覧ください。

イベント情報のエクスポート	**[エクスポート]** をクリックすると、イベントログまたはイベント画像を CSV 形式でローカル PC にエクスポートできます。保存パスは手動で設定できます。
イベント関連の画像のダウンロード	関連する画像にカーソルを合わせ、画像の右上隅のダウンロードアイコンをクリックすると、ローカル PC へダウンロードできます。保存パスは手動で設定できます。

11.4 デバイスからのイベントの取得

一部のシナリオの場合（クライアントが起動できない、他のクライアントによって入退室管理デバイスで警戒が開始されているなど）、クライアントが受信したイベントと、入退室管理デバイスでトリガーされたイベントが一致しません。デバイスからリモートでイベントを取得して、デバイスからのイベントをクライアントのイベントセンターに同期できます。

デバイスからイベントを取得するには、次のいずれかの操作を実行します。

- **[デバイス管理]** → **[デバイス]** → **[デバイス]** の順にクリックして、入退室管理デバイスを選択して、**[Get Events from Device（デバイスからイベントを取得）]** をクリックしてイベントを同期します。
- **[Time & Attendance（時間と出勤）]** → **[出勤統計]** → **[出勤記録]** の順にクリックして、**[Get Events from Device（デバイスからイベントを取得）]** をクリックして、入退室管理デバイスを選択してイベントを同期します。

11.5 ポップアップイベント情報の表示

イベント通知を有効にして、リンク操作として [Event Triggered Pop-up Image（イベントトリガーされたポップアップ画像）] を設定すると、イベント発生時にウィンドウがポップアップされて、イベント情報、関連する画像、および関連するビデオが表示されます。

[イベントセンター] → **[リアルタイムイベント]** に移動して、**[アラームトリガーされたポップアップ画像を有効化]** をクリックして、この機能を有効にします。

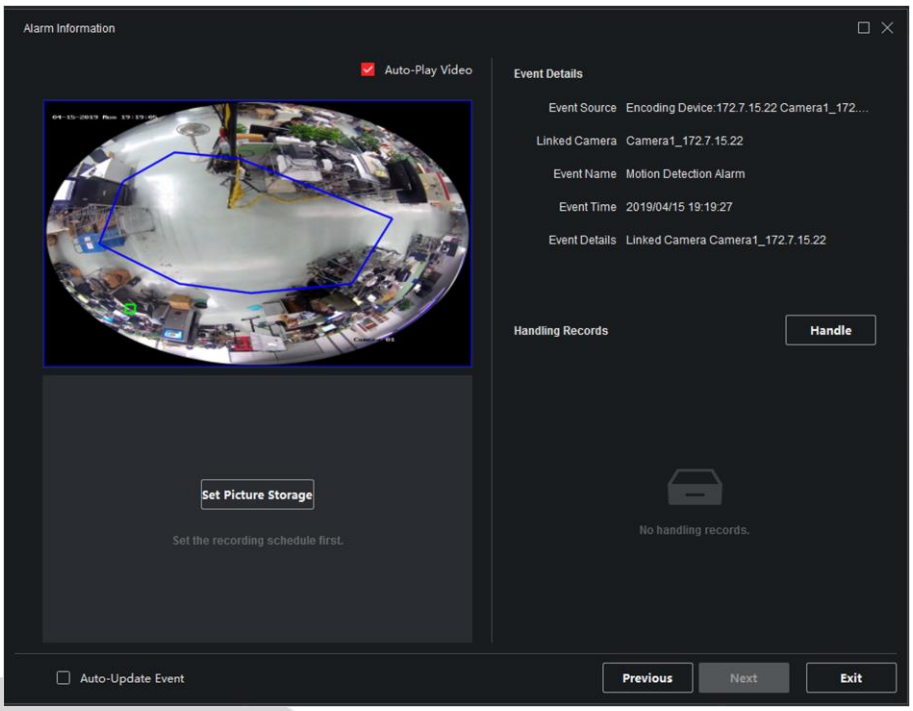

図 11-3 ポップアップイベント情報

イベント関連のビデオ映像（イベントの 30 秒前からイベントの終了まで）、イベント発生時にキャプチャされた画像、イベントソース、リンクされたカメラ、イベントタイプなどのイベントの詳細を表示できます。

注記

- ウィンドウを閉じていない場合、新しいイベントがトリガーされたときに新しいイベント情報を表示するには、**[次へ]** をクリックする必要があります。
- イベント情報を消去していない場合は、**[前へ]** をクリックして前のイベント情報を表示できます。

[Auto-Update Event（イベントの自動更新）] にチェックを入れて、新しいイベントがトリガーされたときにウィンドウが自動的に最新のイベント情報に切り替わるようにすることができます。

第 12 章 マップ管理

E マップ機能は、設置されたカメラとアラーム入力デバイスの位置と分布の視覚的な概要を提供します。マップ上のカメラのライブビューを取得でき、アラームがトリガーされたときにマップから通知メッセージを取得します。
E マップは、ホットスポット（マップ上に配置されたリソース（カメラ、アラーム入力など）のことをホットスポットといいます）の位置と分布の視覚的な概要を提供する静的画像です（地理的なマップである必要はありませんが、多くの場合は地理的なマップです。組織のニーズに応じて、写真やその他の種類の画像ファイルを E マップとして使用することもできます）。カメラとアラーム入力の物理的な位置、およびカメラが向いている方向を確認できます。ホットリージョン機能を使用して、E マップを階層に編成して、広い視野から詳細な視野（フロアレベルから部屋レベル）に移動できます。

12.1 マップの追加

ホットスポットとホットリージョンの親マップとしてマップを追加する必要があります。

手順

注記
1 つのグループに追加できるマップは 1 つだけです。

1.[E マップ] ページを開きます。
2.マップを追加するグループを選択します。

注記
グループの設定の詳細については、「*グループ管理*」をご覧ください。

3.**[マップを追加]** をクリックして、マップの追加ウィンドウを開きます。

4.追加したマップのわかりやすい名前を入力します。
5.ローカルパスからマップ画像を選択します。

注記
マップの画像形式は、PNG、JPEG、または BMP でなければなりません。

6.**[OK]** をクリックします。
7.オプション: マップを追加した後に、次のタスクを実行します。

拡大 / 縮小	マウスホイールを使用するか、[+] または [-] をクリックして、マップを拡大または縮小します。
マップエリアの調整	右下隅の黄色のウィンドウをドラッグするか、方向ボタンとズームバーを使用して、表示するマップエリアを調整します。

12.2 マップスケールの編集

マップスケールは、マップ上の距離とそれに対応する地上の距離の比率です。クライアントは、地上の距離に応じてマップ上の 2 つの場所の距離を計算できます。正確なマップスケールは、レーダーの監視範囲を定義するのに不可欠です。

始める前に

マップを追加したことを確認してください。詳細については、「*マップの追加*」をご覧ください。

セキュリティレーダーをマップに追加する必要がある場合は、このタスクを実行します。

手順

1.[E マップ] モジュールを表示します。
2.マップ編集モードにするには、E マップツールバーの **[編集]** をクリックします。
3.**[Edit Scale（スケールを編集）]** をクリックして、マップ上の 2 つの場所を選択します。
マップ上にカーソルを置くと、カーソルが に変わります。
4.マップをクリックして 2 つの場所を選択します。
[Edit Scale（スケールを編集）] ウィンドウが表示されます。
5.2 つの場所の地上の距離を入力して、**[OK]** をクリックします。
クライアントはマップスケールを自動的に計算します。

12.3 ホットスポットの管理

マップに追加したデバイスのことをホットスポットといいます。ホットスポットにはデバイスの位置が表示され、ホットスポットを通じて監視シナリオのライブビューやアラーム情報を取得することもできます。

12.3.1 ホットスポットとしてのカメラの追加

カメラをホットスポットとしてマップに追加できます。

始める前に

E マップとカメラをクライアントに追加したことを確認してください。詳細については、「*マップの追加*」および「*デバイス管理*」をご覧ください。

手順

1.[E マップ] ページを表示します。
2.右上隅の **[編集]** をクリックして、マップ編集モードを表示します。
3.**[ホットスポットを追加]** → **[カメラのホットスポット]** の順にクリックして、[ホットスポットを追加] ウィンドウを開きます。

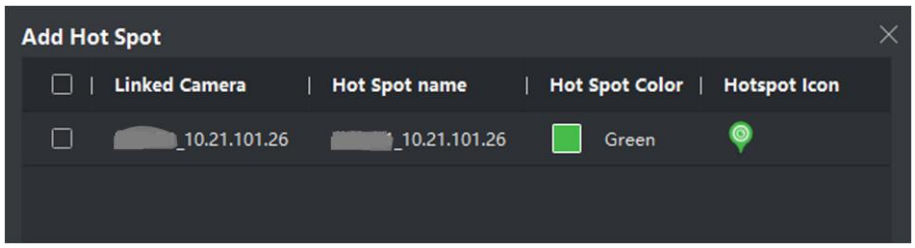

図 12-1 [ホットスポットを追加] パネル

4.マップに追加するカメラを選択します。
5.オプション: ホットスポット名を編集し、名前の色を選択して、ホットスポットアイコンを選択します。
6.**[OK]** をクリックして設定を保存します。

注記

カメラアイコンをグループリストからマップに直接ドラッグして、ホットスポットを追加することもできます。

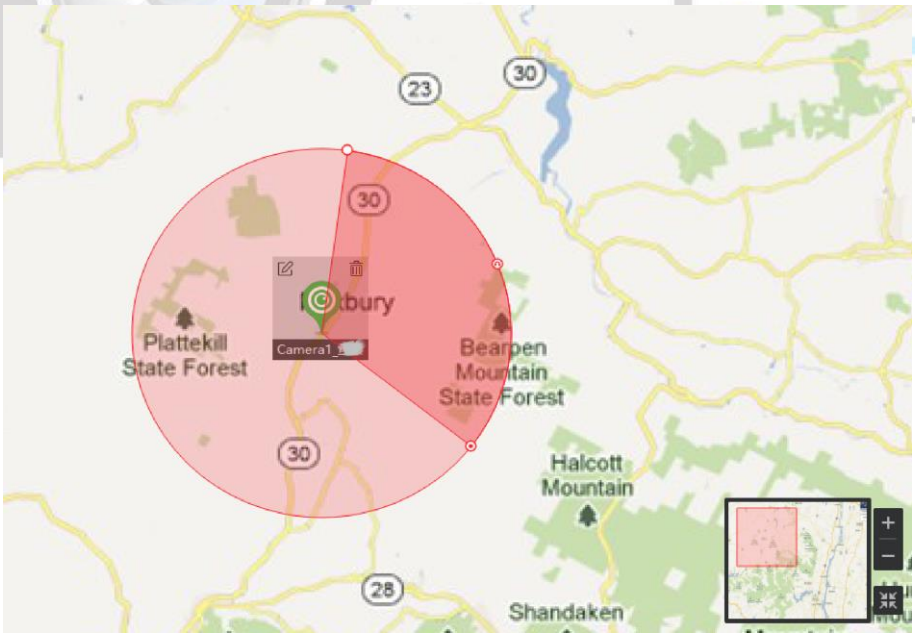

図 12-2 マップ上のカメラ

カメラアイコンがマップにホットスポットとして追加され、グループリストに追加した

カメラのアイコンが から に変わります。セクターはカメラの視野を示します。

7.以下の操作を実行します。

ホットスポットを移動	ホットスポットをドラッグして、特定の位置に移動します。
視野角を変更	/ をドラッグして回して、カメラの視野を変更します。
視野サイズを変更	をドラッグして視野サイズを変更します。

12.3.2 ホットスポットとしてのアラーム入力の追加

アラーム入力をホットスポットとしてマップに追加できます。

手順

1.[E マップ] モジュールを表示します。

2.右上隅の **[編集]** をクリックして、マップ編集モードを表示します。

3.**[ホットスポットを追加]** → **[アラーム入力ホットスポット]** の順にクリックして、[ホットスポットを追加] ウィンドウを開きます。

4.マップに追加するアラーム入力を選択します。

5.オプション: ホットスポット名を編集して、名前の色を選択し、対応するフィールドをダブルクリックしてホットスポットアイコンを選択します。

6.**[OK]** をクリックします。

注記

アラーム入力アイコンをグループリストからマップに直接ドラッグして、ホットスポットを追加することもできます。

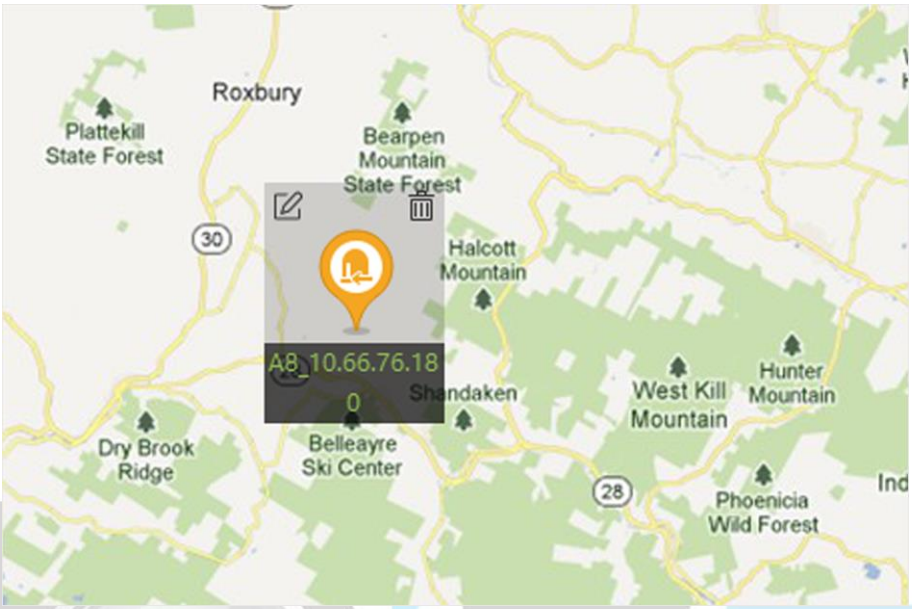

図 12-3 マップ上のアラーム入力

アラーム入力アイコンがマップにホットスポットとして追加され、グループリストに追加したアラーム入力のアイコンが から に変わります。

7.オプション: ホットスポットをドラッグして、特定の位置に移動します。

12.3.3 ホットスポットとしてのアラーム出力の追加

アラーム出力を管理用のホットスポットとしてマップに追加できます。その後、それをすばやく有効または無効にすることができます。マップ上でアラーム出力を有効にすると、それに接続されているセキュリティ制御デバイス（サイレン、ベルなど）が注意を喚起します。

始める前に

E マップとアラーム出力がクライアントに追加されていることを確認してください。詳細については、「*マップの追加*」および「*デバイス管理*」をご覧ください。

手順

1.[E マップ] モジュールを表示します。

2.マップ編集モードにするには、E マップツールバーの **[編集]** をクリックします。

3.**[ホットスポットを追加] → [アラーム出力ホットスポット]** の順にクリックして、[ホットスポットを追加] パネルを開きます。

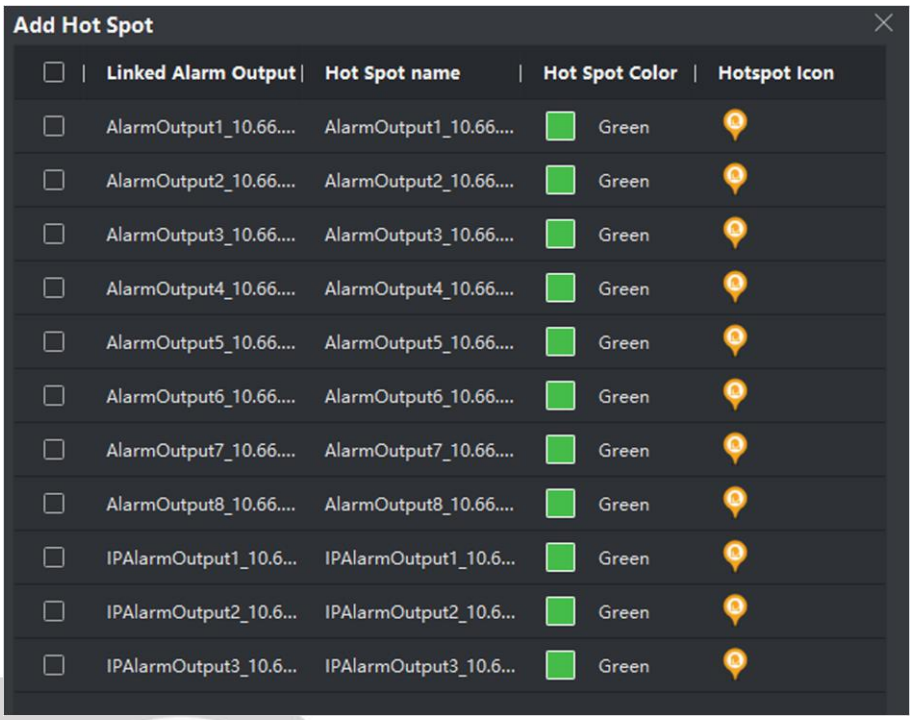

図 12-4 [ホットスポットを追加] パネル

4.マップに追加するアラーム出力を選択します。

5.オプション: ホットスポット名を編集し、名前の色を選択して、ホットスポットアイコンを選択します。

6.**[OK]** をクリックします。

注記

アラーム出力アイコンをアラーム出力リストからマップにドラッグして、ホットスポットを追加することもできます。

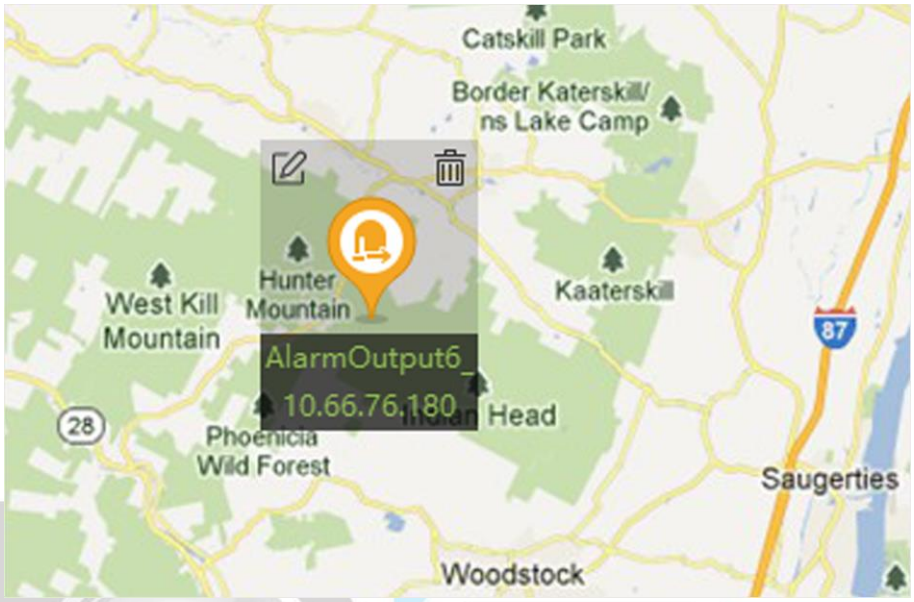

図 12-5 マップ上のアラーム出力

アラーム出力がマップにホットスポットとして追加され、グループリスト内のアイコンが から に変わります。

7.オプション: アラーム出力をドラッグして、特定の位置に移動します。

12.3.4 ホットスポットとしてのゾーンの追加

マップにゾーンを追加して、アラームがトリガーされたときにゾーンをすばやく見つけることができます。

始める前に

マップとゾーンがクライアントに追加されていることを確認してください。詳細については、「*マップの追加*」および「*デバイスの追加*」をご覧ください。

手順

1.[E マップ] モジュールを表示します。

2.マップ編集モードにするには、E マップツールバーの **[編集]** をクリックします。

3.**[ホットスポットを追加]** → **[ゾーンのホットスポット]** の順にクリックして、[ホットスポットを追加] パネルを開きます。

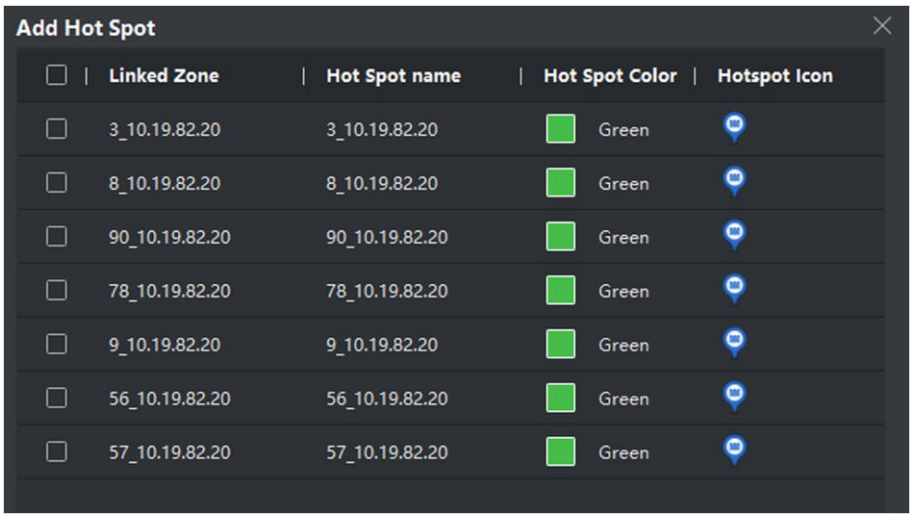

図 12-6 [ホットスポットを追加] パネル

4.マップに追加するゾーンを選択します。

5.オプション: ホットスポット名を編集し、名前の色を選択して、ホットスポットアイコンを選択します。

6.**[OK]** をクリックします。

注記

アラーム出力アイコンをアラーム出力リストからマップにドラッグして、ホットスポットを追加することもできます。

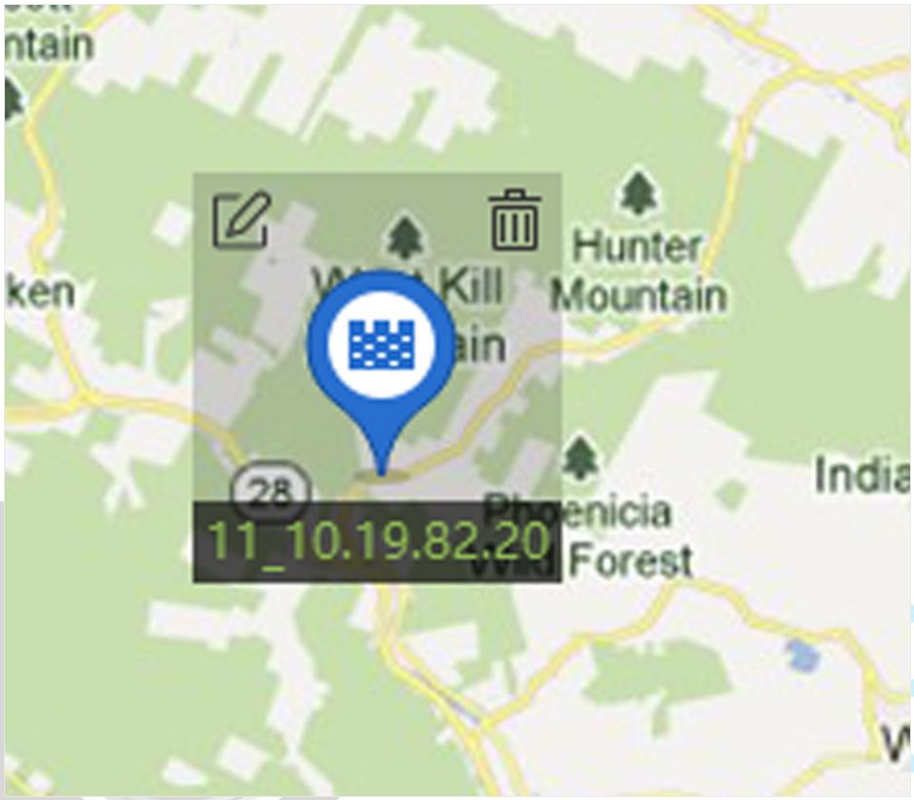

図 12-7 マップ上のゾーン

ゾーンがマップにホットスポットとして追加され、グループリスト内のアイコンが から に変わります。

7. オプション: ゾーンのホットスポットをドラッグして、特定の位置に移動します。
   アラームがトリガーされると、最新アラームの数がゾーンのアイコンに表示されます。番号をクリックして、アラームの詳細を表示できます。

注記

表示できる最新アラームは 10 個以下です。

8. オプション: **[アラームを消去]** をクリックして、現在のマップ上のゾーンのアラームを既読としてマークします。

12.3.5 ホットスポットとしてのセキュリティレーダーの追加

効果的な監視のために、セキュリティレーダーをマップにホットスポットとして追加して、監視フィールドにゾーンを描画できます。これにより、何者かがゾーンに侵入すると、注意を喚起するためにアラームがトリガーされます。

始める前に

E マップとセキュリティレーダーがクライアントに追加されていることを確認してください。詳細については、「*マップの追加*」および「*デバイス管理*」をご覧ください。

手順

1.[E マップ] モジュールを表示します。
2.マップ編集モードにするには、E マップツールバーの **[編集]** をクリックします。
3.オプション: マップスケールを編集します。詳細については、「*マップスケールの編集*」をご覧ください。
4.デバイスリストでセキュリティレーダーを選択して、マップにドラッグします。

5.オプション: 追加したレーダーをクリックし、 をクリックしてホットスポット名を編集し、ホットスポットの色を選択して、ホットスポットアイコンを選択します。
6.**[OK]** をクリックします。
セキュリティレーダーがホットスポットとしてマップに追加され、グループリスト内のアイコンが から に変わります。このセクターは、レーダーの監視フィールドを示しています。

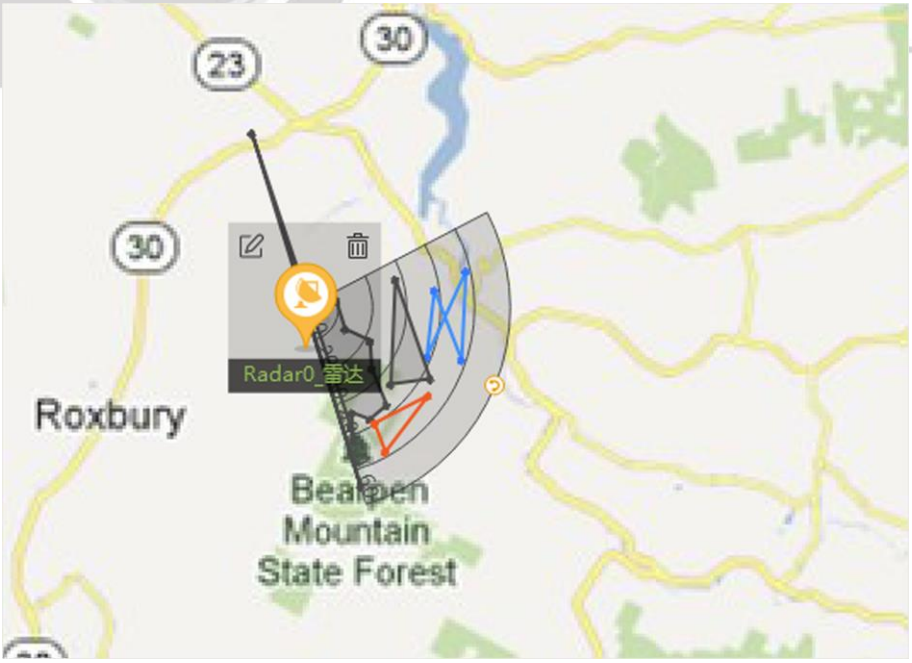

図 **12-8** マップ上のレーダー

注記

- オレンジのセクターは警戒が開始されているレーダーを示し、黒のセクターは警戒が解除されているレーダーを示します。
- 赤の点は、検知された侵入者を示します。

7.セキュリティレーダーの監視フィールドにゾーンを追加します。

注記

セキュリティレーダが警戒解除されていることを確認してください。

1）**[編集]** → **[レーダーゾーンの追加]** の順にクリックして、ゾーンの描画を開始します。
2）オプション: **[Field Assistance（フィールドアシスタンス）]** をオンにして、ゾーン描画アシスタンス機能を有効にします。

例

ゾーンとして描画する必要があるフィールドを人物 A が歩くと、赤の点と破線で構成された移動パターンとして示されます。その後、人物 B が、移動パターンに従ってマップ上にゾーンを描画します。

3）セクターをクリックしてゾーンを描画して、右クリックして描画を完了します。
[ゾーン設定] ウィンドウが表示されます。
4）ゾーン名を入力して、ゾーンタイプを選択します。

警告ゾーン

赤の線で定義されます。何者かが警告ゾーンに侵入すると、アラームがトリガーされて、ゾーン全体が赤に変わります。侵入者の位置と移動パターンは、赤の破線で接続された赤の点で表示されます。侵入者がゾーンから出た場合にのみ、ゾーンが復元されます。

事前警告ゾーン

青の線で定義されます。何者かが警告ゾーンに侵入すると、アラームがトリガーされ、イベントセンターでイベントの詳細を確認できます。

無効ゾーン

紫の線で定義されます。何者かが警告ゾーンに侵入した場合、アラームはトリガーされず、移動パターンは表示されません。

5）オプション: ゾーンの編集: ゾーンをダブルクリックして、ゾーンの編集モードを表示します（ゾーンの周囲に破線の枠が表示されます）。ゾーンの縁にカーソルを合わせて青の + を表示し、クリックしてゾーンの点を追加します。点をドラッグしてゾーンを変更します。任意の場所をクリックして、編集モードを終了します。

8.オプション: セキュリティレーダーをドラッグして、特定の位置に移動します。

12.3.6 ホットスポットとしてのアクセスポイントの追加

アクセスポイントをホットスポットとしてマップに追加して、ホットスポットを検索し、それらの状態とアラーム番号を表示することができます。

始める前に

マップとアクセスポイントがクライアントに追加されていることを確認してください。詳細については、「*マップの追加*」および「*デバイスの追加*」をご覧ください。

手順

1.[E マップ] モジュールを表示します。
2.マップ編集モードにするには、E マップツールバーの **[編集]** をクリックします。
3.**[ホットスポットを追加]** → **[Access Point Hot Spot（アクセスポイントホットスポット）]** の順にクリックして、[ホットスポットを追加] ウィンドウを開きます。

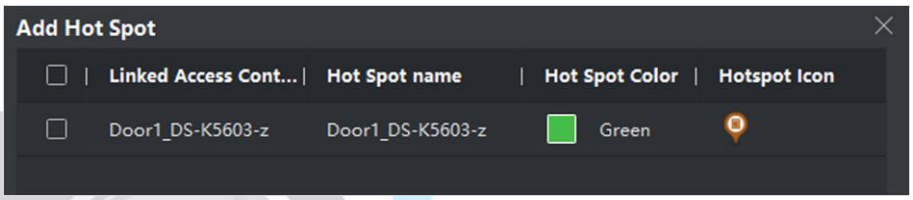

図 12-9 [ホットスポットを追加] パネル

4.マップに追加するアクセスポイントを選択します。
5.オプション: ホットスポット名を編集し、名前の色を選択して、ホットスポットアイコンを選択します。
6.**[OK]** をクリックします。

注記

また、アクセスポイントアイコンをアクセスポイントリストからマップにドラッグすることもできます。

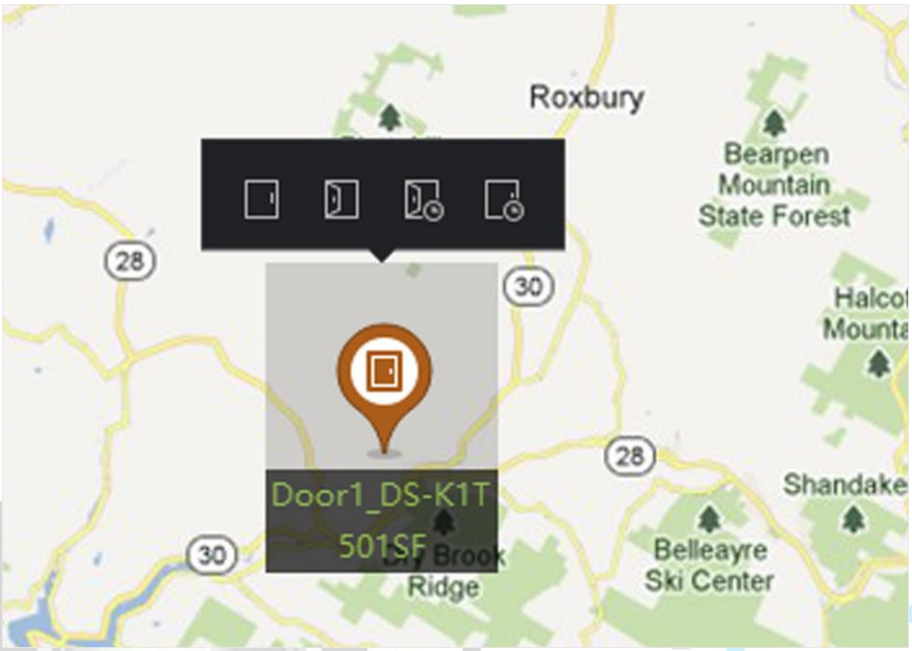

図 12-10 マップ上のアクセスポイント

アクセスポイントがホットスポットとしてマップに追加され、グループリスト内のアイコンが から に変わります。

7.オプション: アクセスポイントホットスポットをドラッグして、特定の位置に移動します。

アラームがトリガーされると、最新アラームの数がホットスポットアイコンに表示されます。番号をクリックして、アラームの詳細を表示できます。

注記

表示できる最新アラームは 10 個以下です。

12.3.7 ホットスポットの編集

名前、色、アイコンなど、マップに追加したホットスポットの情報を編集できます。

手順

1.[E マップ] モジュールを表示します。

2.右上隅の **[編集]** をクリックして、マップ編集モードを表示します。

3.マップ上のホットスポットアイコンを選択し、 をクリックして [ホットスポットを編集] ウィンドウを開きます。
4.テキストフィールドでホットスポット名を編集して、マップに表示されているホットスポット名の色とホットスポットアイコンを選択します。
5.**[Apply to Other Camera Hot Spots（他のカメラのホットスポットに適用）]** / **[Apply to Other Alarm Input Hot Spots（他のアラーム入力のホットスポットに適用）]** / **[Apply to Other Alarm Output Hot Spots（他のアラーム出力のホットスポットに適用）]** / **[Apply to Other Zone Hot Spots（他のゾーンのホットスポットに適用）]** にチェックを入れて、色とアイコンの設定を他のホットスポットに適用します。
6.**[OK]** をクリックします。

7.オプション: ホットスポットアイコンを選択し、 をクリックしてホットスポットを削除します。

12.3.8 ホットスポットのプレビュー

ホットスポット（カメラ、アラーム入力 / 出力、ゾーン、セキュリティレーダー、ゾーンなど）をマップに追加した後に、カメラのホットスポットのライブビューと、マップ上のすべてのタイプのホットスポットのトリガーされたアラーム情報を表示できます。

始める前に

マップにホットスポットを追加したことを確認してください。詳細については、「***ホットスポットの管理***」をご覧ください。

手順

1.[E マップ] モジュールを表示します。

注記

マップ編集モードの場合は、右上隅の **[終了]** をクリックしてマッププレビューモードを表示します。

2.**[表示]** をクリックして、マップ上のホットスポットを表示します。

注記

が表示されているタイプのホットスポットがマップに表示されます。

3.ホットスポットをクリックして、次の操作を実行します。

ホットスポットタイプ操作***カメラ***	ライブビュー: をクリックして、カメラのライブビューウィンドウ表示します。

注記

- ライブ表示中にアラームがトリガされると、クライアントは最初に 30 秒のビデオファイルを再生します。
- ライブビュー中にキャプチャ、録画の開始、およびインスタント再生することができます。

アラーム出力

アラーム出力をクリックして、**[開く]** / **[閉じる]** を選択します。

注記

アラーム出力で管理するセキュリティ制御チャンネルも開かれます、または閉じられます。

アクセスポイント

ドアの状態の表示: アクセスポイントの現在のドアの状態がアイコンに表示されます。アイコンをクリックして、ドアの状態を切り替えます。

ドアを開放

ドアが施錠されている場合、解錠して一度開きます。開放期間の経過後、自動的にドアが閉じて施錠されます。

ドアを閉鎖

ドアが解錠されている場合、ドアを施錠するとドアが閉じます。アクセス認証の権限を有する人物は、認証情報を使用してドアにアクセスできます。

開放状態

（閉鎖または開放の場合を問わず）ドアは解錠されます。認証情報は不要で、すべての人がドアにアクセスできます。

閉鎖状態

ドアが閉じ、施錠されます。スーパーユーザーを除き、認証権限を有するユーザーでもドアにはアクセスできません。

レーダーの監視フィールドの警戒開始 / 警戒解除ゾーン: 編集が終了したら、セキュリティレーダーのアイコンをクリックして、**[Arm（警戒開始）]** / **[Disarm（警戒解除）]** を選択します。

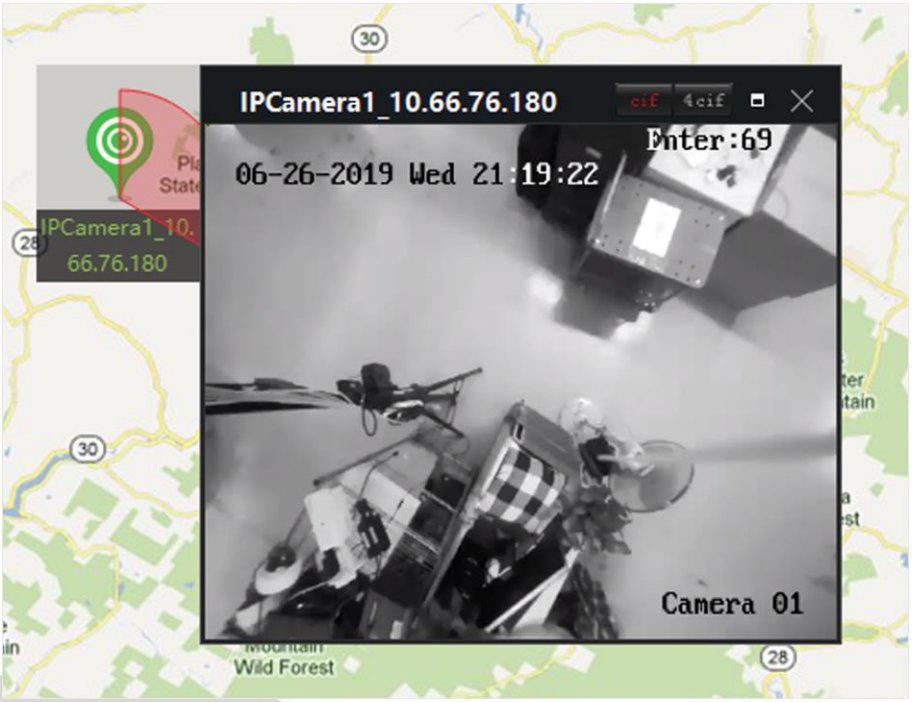

図 12-11 マップ上のカメラのライブビュー

4.オプション: 以下の操作を実行します。

アラーム情報を表示	ホットスポットアイコンのアラーム番号をクリックしてアラーム情報ページを開き、アラームタイプとトリガー時間を表示します。
アラームを消去	マップの上部にある **[アラームを消去]** をクリックして、ホットスポットのすべてのアラームを既読としてマークします。
マップ上に複数のカメラのライブビューを表示	1. **[ライブビュー]** をクリックして、クライアントの下部に 4 つの小さなウィンドウを表示します。 2. デバイスリストからウィンドウにカメラをドラッグして、ライブビューを開始します。

注記

同時に最大 4 台のカメラのライブビューを表示できます。

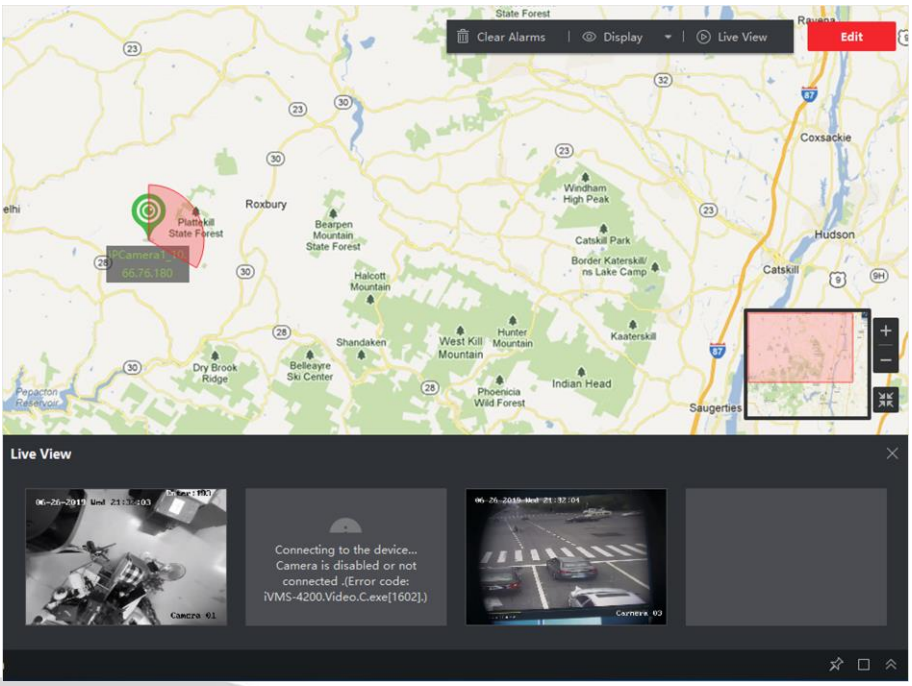

図 12-12 カメラのホットスポットのプレビュー

12.4 ホットリージョンの管理

ホットリージョン機能は、マップを別のマップにリンクします。マップをホットリージョンとして別のマップに追加すると、追加したマップへのリンクのアイコンがメインマップに表示されます。追加したマップのことを子マップといい、ホットリージョンの追加先マップのことを親マップといいます。

子マップを親マップにリンクすると、ホットリージョンアイコンが親マップに表示されます。このアイコンをクリックして子マップを表示して、子マップ上のリソースを簡単に表示できます。

ホットリージョン機能を使用して、E マップを階層に編成して、広い視野から詳細な視野（フロアレベルから部屋レベル）に移動できます。

12.4.1 ホットリージョンの追加

マップを別のマップにホットリージョンとして追加できます。これにより、追加したマップへのリンクのアイコンがメインマップに表示されます。追加したマップのことを子マップといい、ホットリージョンの追加先マップのことを親マップといいます。

始める前に

少なくとも 2 つのマップを追加する必要があります。マップの追加方法の詳細については、「*マップの追加*」をご覧ください。

手順

注記

マップは一度だけホットリージョンとして追加できます。

1.[E マップ] ページを表示します。
2.右上隅の **[編集]** をクリックして、マップ編集モードを表示します。

3.追加したマップを親マップとして選択します。
4.**[ホットリージョンを追加]** をクリックして、[ホットリージョンを追加] ウィンドウを開きます。
5.子マップを選択します。
6.オプション: ホットリージョン名を編集して、対応するフィールドをダブルクリックしてホットリージョンの色とアイコンを選択します。
7.**[OK]** をクリックします。
子マップアイコンは、親マップにホットリージョンとして追加されます。

12.4.2 ホットリージョンの編集

名前、色、アイコンなど、親マップ上のホットリージョンの情報を編集できます。

手順

1.[E マップ] モジュールを表示します。
2.右上隅の **[編集]** をクリックして、マップ編集モードを表示します。
3.親マップでホットリージョンアイコンを選択し、 をクリックして［ホットリージョンを編集］ウィンドウを開きます。

4.テキストフィールドでホットリージョン名を編集して、ホットリージョン名の色とホットリージョンアイコンを選択します。
5.**[Apply to Other Hot Regions（他のホットリージョンに適用）]** にチェックを入れて、色とアイコンの設定を他のホットリージョンに適用します。
6.**[OK]** をクリックします。

12.4.3 ホットリージョンのプレビュー

ホットリージョンを追加した後、親マップ上のホットリージョンアイコンをクリックして、子マップを表示できます。子マップ上でリソースとアラームを表示できます。

手順

1.[E マップ] ページを表示します。

注記

マップ編集モードの場合は、右上隅の **[終了]** をクリックしてマッププレビューモードを表示します。

2.親マップ上のホットリージョンアイコンをクリックして、リンクされた子マップを表示します。
子マップ上でリソースを表示できます。子マップでアラームがトリガーされた場合は、アラームの詳細を確認できます。
3.オプション: 左上隅の **[Back to Parent Map（親マップに戻る）]** をクリックして、親マップに戻ります。

4.オプション: 右上隅の **[アラーム情報を消去]** をクリックして、現在のマップ上のリソースによってトリガーされたアラーム情報を消去します。

12.5 人物の移動パターンの表示

顔認識デバイスの機能を使用して、対象人物の移動パターンをマップ上に表示できます。これは、複数のカメラの位置によって生成されます。E マップにより、個人（容疑者、行方不明の子どもなど）の移動パターンをマップ上で検索して表示し、その人物を容易に見つけることができます。

始める前に

グループのマップを追加したことと、グループ内のカメラをマップに追加したことを確認してください。詳細については、「*マップの追加*」および「*ホットスポットとしてのカメラの追加*」をご覧ください。

手順

1.[E マップ] モジュールを表示します。
2.左側の列にあるリソースリストでグループ名をクリックします。
グループのマップとマップ上のリソースが表示エリアに表示されます。
3.オプション: **[マップを追加]** をクリックしてグループのマップを追加して、グループ内のカメラをマップに追加します。
4.マップの上部にある **[Moving Pattern（移動パターン）]** をクリックして、[Search Moving Pattern（移動パターンを検索）] ページを開きます。
5. をクリックして、移動パターンを検索する期間を設定します。
6.リストで、顔画像分析デバイスにチェックを入れます。

注記

手順 7 でアップロードする画像は、チェックを入れたデバイスに保存されている画像と比較されます。

7.**[画像を選択]** をクリックして、アップロードする顔画像を選択するか、画像を画像エリアにドラッグします。

注記

複数の顔画像が含まれている画像をアップロードできますが、そこから比較用の顔画像を 1 つ選択する必要があります。

8.スライダーをドラッグするか、番号を入力して類似度を選択します。

注記

クライアントは、選択した顔画像分析デバイスに保存されている顔画像のうち、アップロードした画像との類似度が設定された類似度よりも高いものを検索して、一致した人物の移動パターンをマップ上に表示します。

9.**[検索]** をクリックします。

アップロードした画像に似た人物の移動パターンがマップに表示され、カメラのキャプチャ画像に人物の到着順を示す番号が付けられて、キャプチャ記録がキャプチャ画像のサムネイルとともに左側に表示されます。

10.オプション: 移動パターンを検索した後に、次の操作を実行します。

操作説明	
キャプチャ記録をフィルタリング	をクリックして、**[最後の記録を表示]** にチェックを入れて、移動パターン全体にわたるすべてのカメラの最後の記録を表示します。
人物関連のビデオと画像を表示	キャプチャ画像のサムネイルをクリックして [Capture Details（キャプチャの詳細）] ウィンドウを開き、クリックした画像の詳細情報を表示します。カメラでキャプチャされた人物のすべての画像が右側に表示されます。キャプチャ画像を選択して、キャプチャ時間の前後 5 秒間のビデオが含まれた 10 秒間の関連するビデオを左側に表示します。 をクリックしてビデオの表示を開始します。
パターンを無効化	レコードリストの上部にある をクリックするか、[Disable Pattern（パターンを無効化）] をクリックして、移動パターンモードを終了します。

第 13 章 ストリームメディアサーバー経由でのビデオストリームの転送

デバイスのリモートアクセス数には常に制限があります。ライブビューを取得するためにデバイスへのリモートアクセスを求めているユーザーが多い場合は、ストリームメディアサーバーを追加して、ストリームメディアサーバーからビデオデータストリームを取得して、デバイスの負荷を軽減することができます。

注記

ストリームメディアサーバーアプリケーションソフトウェアをインストールする必要があり、これはクライアントインストールパッケージに含まれています。インストールパッケージを実行した後、**[ストリームメディアサーバー]** にチェックを入れて、ストリームメディアサーバーのインストールを有効にします。

13.1 ストリームメディアサーバーへの証明書のインポート

ストリームメディアサーバーをクライアントに追加する前に、まずクライアントのセキュリティ証明書をストリームメディアサーバーにインポートして、セキュリティ認証を実行して、データのセキュリティを確保する必要があります。

次の手順を実行して、セキュリティ証明書をストリームメディアサーバーにインポートします。

手順

1.クライアントから証明書をエクスポートします。

1）クライアントサービスを開きます。

2）**[エクスポート]** をクリックします。

2.ストリームメディアサーバーがインストールされている PC に証明書をコピーします。

3.ストリームメディアサーバーがインストールされている PC のデスクトップで をクリックして実行します。

4.証明書をストリームメディアサーバーにインポートします。

1）タスクバーで を右クリックして、[表示] をクリックします。

2）**[設定]** をクリックして、[設定] ウィンドウを表示します。

3）セキュリティ証明書フィールドで、**[インポート]** をクリックして、手順 1 でクライアントからエクスポートした証明書ファイルを選択します。

4）**[OK]** をクリックします。

5.ストリームメディアサーバーを再起動して有効にします。

注記

クライアントのセキュリティ証明書が更新された場合は、新しい証明書をクライアントからエクスポートして、ストリームメディアサーバーに再度インポートして更新する必要があります。

13.2 IP アドレスによるストリームメディアサーバーの追加

ストリームメディアサーバーは、IP アドレスで 1 台ずつ追加できます。

手順

注記

1 つのクライアントに対して、最大 16 台のストリームメディアサーバーを追加できます。

1.デスクトップで をクリックして、ストリームメディアサーバーを実行します。

注記

- 他の PC にインストールされているストリームメディアサーバーを通じてビデオを転送することもできます。
- ストリームメディアサーバーポート（値: 554）が他のサービスで使用されている場合は、ダイアログボックスが表示されます。ストリームメディアサーバーが正しく動作するように、ポート番号を他の値に変更する必要があります。

2.クライアントソフトウェアで、[デバイス管理] ページを表示します。
3.**[デバイス] → [ストリームメディアサーバー]** に移動します。

4.**[追加]** をクリックし、[追加] ウィンドウを開きます。

5.追加モードとして **[IPアドレス]** を選択します。
6.ストリームメディアサーバーのニックネームと IP アドレスを入力します。

注記

デフォルトのポート値は 554 です。

7.ストリームメディアサーバーの追加を完了します。
– サーバーを追加し、リストページに戻るには、**[追加]** をクリックします。
– 設定を保存して、他のサーバーの追加を続ける場合は、**[追加して続行]** をクリックし

ます。

注記

追加したストリームメディアサーバーのセキュリティ証明書がクライアントのセキュリティ証明書と一致しない場合は、プロンプトが表示されます。例外メッセージを確認して、示されている手順に従って証明書の整合性を保つことができます。

13.3 ストリームメディアサーバーにカメラを追加してビデオストリームを転送する

ストリームメディアサーバー経由でカメラのビデオストリームを取得するには、カメラをストリームメディアサーバーに接続する必要があります。

手順

1.[デバイス管理] モジュールを表示します。
2.**[デバイス] → [ストリームメディアサーバー]** に移動します。
3.サーバーを選択して、[操作] 列で をクリックして、[ストリームメディアサーバーの設定] ウィンドウを開きます。

4.ストリームメディアサーバー経由でビデオストリームを転送するカメラを選択します。
5.**[OK]** をクリックします。
6.[メインビュー] ページに移動して、カメラのライブビューを再度開始します。
ストリームメディアサーバーのコントロールパネルで、ストリームメディアサーバーを通じて転送される、またはストリームメディアサーバーから送信されるビデオストリームのチャンネル番号にチェックを入れます。

注記

- 1 台のストリームメディアサーバーを通じて転送できるビデオストリームは最大 64 チャンネルで、ストリームメディアサーバーからクライアントに送信できるビデオストリームは最大 200 チャンネルです。
- カメラがオフラインの場合も、クライアントはストリームメディアサーバーを介してライブビデオを取得できます。

第 14 章 統計

指定した期間にわたって作成されるレポートは重要なドキュメントであり、ビジネスが円滑かつ効果的に運営されているかどうかを確認するのに使用されます。このソフトウェアでは、レポートを日次、週次、月次、年次、およびカスタム期間で生成できます。レポートは、意思決定、問題への対処、傾向の確認および比較などで基礎データとして使用できます。

14.1 人数集計レポート

人数集計統計とは、人数集計カメラによって、特定のエリアで特定の期間中にラインを横切った人物の数を計算することです。これにより店主は、さまざまな時間の顧客の流れと数を分析して、レポートに従って柔軟にビジネスを調整することができます。人数集計統計は、折れ線グラフまたはヒストグラムで表示でき、詳細データをローカルストレージにエクスポートするためのレポートを生成できます。

始める前に

人数集計デバイスをソフトウェアに追加して、対応するエリアを適切に設定します。追加したデバイスで人数集計ルールが設定されている必要があります。人数集計デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。

手順

1.**[レポート] → [人数集計]** の順にクリックして、[人数集計] ページを表示します。
2.レポートタイプとして、日次レポート、週次レポート、月次レポート、または年次レポートを選択します。

日次レポート

日次レポートには、日単位のデータが表示されます。システムは、1 日の各時間単位で人数を計算します。

週次レポート、月次レポートおよび年次レポート

日次レポートと比較して、週次レポート、月次レポートおよび年次レポートは毎日提出されないため、時間がかかりません。システムは、1 週間の各日、1 ヵ月の各日、1 年の各月単位で人数を計算します。

カスタムレポート

ユーザーは、レポートの日数をカスタマイズして、カスタム時間間隔の各日または各月の人数を分析できます。

注記

カレンダーで選択できる日数は 31 日以内です。

3.統計の時間タイプを選択し、 をクリックして時間を設定します。

1 つの期間

1 つの期間で統計情報を生成します。

Multiple Periods（複数の期間）

2 つの期間で統計を生成します。これにより、2 つの期間で人の流れと数を比較できます。

例えば、レポートタイプを月次レポートとして設定し、3 月と 4 月を統計期間として設定すると、3 月と 4 月の人数集計結果は、同じグラフに異なる色で表示され、各月の異なる日のデータを比較することができます。

4.**[Display by Device（デバイス別に表示）]** または **[Display by Camera（カメラ別に表示）]** を選択します。

デバイス別に表示

デバイス別にレポートを表示します。

例えば、4 台の人数集計カメラが接続された 1 台の NVR を選択した場合、レポートには 4 台の人数集計カメラの合計人数が表示されます。

カメラ別に表示

カメラ別にレポートを表示します。

例えば、4 台の人数集計カメラが接続された 1 台の NVR を選択した場合、レポートには各カメラの統計がそれぞれ表示されます。つまり、統計は 4 / 8 色で表示されます（1 色 / 2 色が 1 台のカメラ）。

5.表示する人数集計カメラを選択します。

6.統計の方向を選択します。

Entered（入室）

入室した人数が集計されます。

Exited（退室）

退室した人数が集計されます。

Passed（通過）

入退室した人数の両方が集計されます。

7.**[Children Only（子供のみ）]** にチェックを入れて、子供と認識された人数のレポートを生成します。

注記

- クライアントは、事前定義した身長未満であると検知された人物を集計します。この身長は、デバイスのリモート設定ページで設定できます。身長のしきい値の設定の詳細については、デバイスのユーザーマニュアルをご覧ください。
- 使用するデバイスがこの機能をサポートしている必要があります。

8.**[検索]** をクリックして、時間、日、または月ごとの人数集計統計と詳細データを取得します。

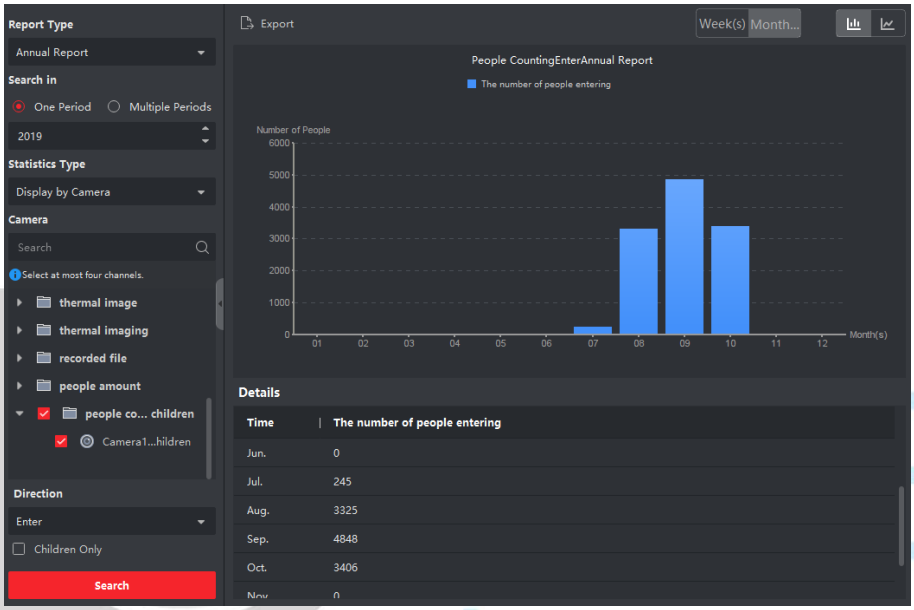

図 14-1 カメラ別に表示

デフォルトでは、統計はヒストグラム形式で表示されます。

9.オプション: 検索後に次の操作を実行します。

折れ線グラフに切り替え	をクリックして、折れ線グラフに切り替えます。 **注記** デフォルトでは、統計は棒グラフで表示されます。
棒グラフに切り替え	をクリックして、棒グラフに切り替えます。
ローカル PC に保存	**[エクスポート]** をクリックして、人数集計の詳細データを PC に保存します。

14.2 交差点での人数集計レポートの表示

交差点分析は、交差点のようなシーンでの人の流れと数を監視するのに使用します。画像内の矢印は異なる方向を示しています。1 つの方向（例えば A）を入口として選択すると、他の方向がデフォルトで出口として設定され、複数の経路が生成されます（A から A、A から B、A から C、A から D など）。各経路を通過した人の人数集計をそれぞれ表示できます。これにより店主は、人の流れをドアごとに分析することができます。統計結果は、日次レポート、週次レポート、月次レポート、および年次レポートとして表示できます。

始める前に

交差点分析機能をサポートしているフィッシュアイカメラが適切に設定され、ソフトウェアに追加されていることを確認してください。デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。

手順

注記

最大 10 個の交差点を分析できます。

1. **[レポート]** → **[交差点分析]** の順にクリックして、[交差点分析] モジュールを表示します。
2. レポートタイプとして、日次レポート、週次レポート、月次レポート、または年次レポートを選択します。

   日次レポート

   日次レポートには、日単位のデータが表示されます。システムは、交差点レポート内の人数を 1 日の各時間単位で計算します。

   週次レポート、月次レポートおよび年次レポート

   日次レポートと比較して、週次レポート、月次レポートおよび年次レポートは毎日提出されないため、時間がかかりません。システムは、交差点レポート内の人数を 1 週間の各日、1 ヵ月の各日、1 年の各月単位で計算します。
3. レポートの開始時刻を設定します。
4. レポートを生成するカメラを選択します。
5. **[フローイン]** フィールドのドロップダウンリストから、入口として 1 つの方向を選択します。
6. **[検索]** をクリックして、統計結果を取得します。

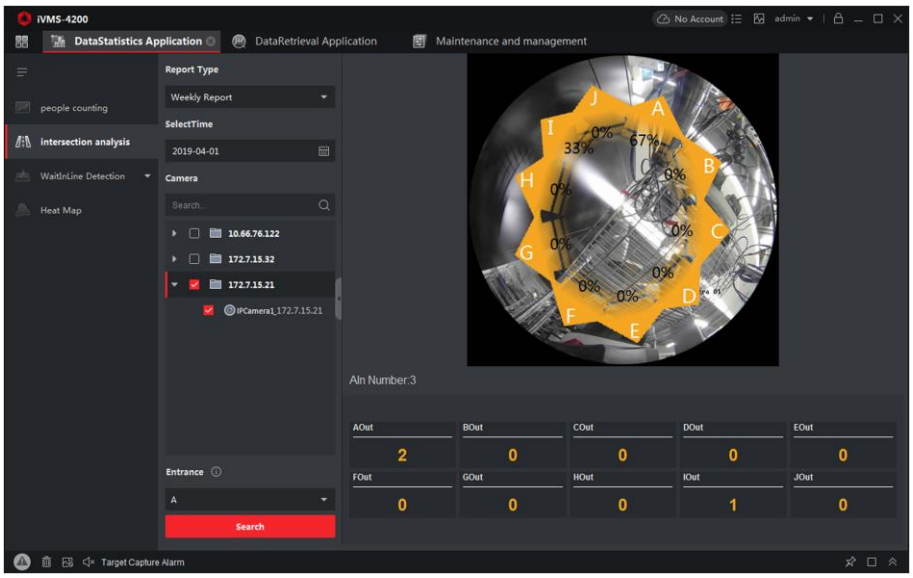

図 14-2 結果

各経路の人数が右側に表示されます。

14.3 待ち行列管理

待ち行列管理は、複数の次元からのデータ分析とレポート出力をサポートしています。
一般的に使用されるデータ分析

- 1 つの待ち行列 / 領域の、特定の待ち時間レベルの待ち行列形成人数を確認するには、待ち行列形成時間分析を使用して、対象領域にチェックを入れて、1 つの待ち時間レベルを設定します。
- 複数の待ち行列 / 領域の、特定の待ち時間レベルの待ち行列形成人数を比較するには、待ち行列形成時間分析を使用して、複数の対象領域にチェックを入れて、1 つの待ち時間レベルを設定します。
- 複数の待ち行列 / 領域の、異なる待ち時間レベルの待ち行列形成人数を比較するには、待ち行列形成時間分析を使用して、複数の対象領域にチェックを入れて、複数の待ち時間レベルを設定します。
- 1 つの待ち行列 / 領域の、待ち行列が特定の長さのままになっている時間と時間帯を確認するには、待ち行列状態分析を使用して、対象領域にチェックを入れて、1 つの待ち行列長レベルを設定します。
- 複数の待ち行列 / 領域の、待ち行列が特定の長さのままになっている時間と時間帯を比較するには、待ち行列状態分析を使用して、複数の対象領域にチェックを入れて、1 つの待ち行列長レベルを設定します。
- 複数の待ち行列 / 領域の、待ち行列が異なる長さのままになっている時間と時間帯を比較するには、待ち行列状態分析を使用して、複数の対象領域にチェックを入れて、複数の待ち行列長レベルを設定します。

14.3.1 待ち行列形成時間分析

待ち行列形成時間分析は、異なる待ち時間レベルの人数を計算します。領域内比較と複数の待ち時間レベルの比較をサポートしています。

異なる領域の待ち行列形成人数の比較

待ち行列形成人数集計用のカメラを使用して、異なる領域での特定の長さの期間の待ち行列形成人数を検索できます。これにより店主は、顧客が行きがちなエリアを見つけることができます。例えば、人数が多い領域のほうが、人数が少ない領域よりも人気があるため、これらの領域に商品を置いて、より多くの商品を販売することができます。

始める前に

- デバイスをソフトウェアに追加して、対応する設定を適切に設定します。デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。
- デバイスのリモート設定ページのカメラの検知エリアに設定した領域が 3 つ以下であることを確認してください。領域の設定方法の詳細については、デバイスのユーザーマニュアルをご覧ください。

手順

注記

接続されているデバイスがこの機能をサポートしている必要があります。

1.**[レポート]** → **[待ち行列管理]** → **[領域の人数]** の順にクリックします。
2.レポートタイプとして、**[日次レポート]** / **[週次レポート]** / **[月次レポート]** / **[カスタムレポート]** を選択します。

日次レポート

日次レポートには、日単位のデータが表示されます。システムは、異なる領域の待ち行列形成時間を 1 日の各時間単位で計算します。

週次レポート、月次レポート

日次レポートと比較して、週次レポートと月次レポートは毎日提出されないため、時間がかかりません。システムは、異なる領域の待ち行列形成時間を 1 週間の各日、1 ヵ月の各日単位で計算します。

カスタムレポート

ユーザーは、レポートの日数をカスタマイズして、カスタム時間間隔の各日または各月の人数を分析できます。

注記

カレンダーで選択できる日数は 31 日以内です。

3. をクリックして、検索する期間を設定します。
4. **[領域]** リストで、カメラと、カメラあたり 3 つ以下の領域を選択します。
5. 統計タイプとして **[領域内比較]** を選択します。
6. レポート生成基準とする待ち時間レベルを選択します。
7. **[検索]** をクリックして、統計結果を生成します。
   指定した待ち時間の計算された人数の折れ線グラフが結果エリアに表示されます。異なる色の線は、選択した領域の人物を示します。

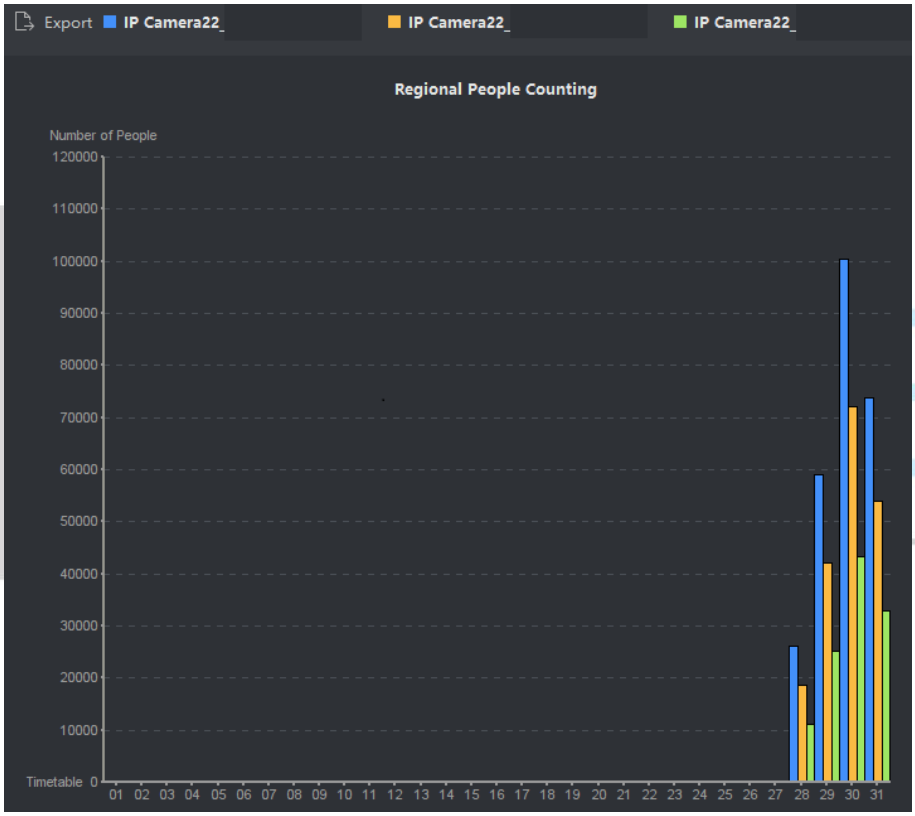

図 14-3 結果

8. オプション: **[エクスポート]** をクリックして、データを Excel ファイル形式でエクスポートします。

異なる待ち時間レベルの待ち行列形成人数の比較

待ち行列形成人数集計用のカメラを使用して、特定の領域での異なる長さの期間の待ち行列形成人数を検索できます。これにより、異なる領域の混雑状況を分析して、いつ、どのようにサービス窓口数やスタッフ数を変更したら良いかと、案内要員を配置すべきかどうかなどを簡単に把握することができます。

始める前に

- デバイスをソフトウェアに追加して、対応する設定を適切に設定します。デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。
- デバイスのリモート設定ページのカメラの検知エリアに設定した領域が 3 つ以下であることを確認してください。領域の設定方法の詳細については、デバイスのユーザーマニュアルをご覧ください。

手順

注記

接続されているデバイスがこの機能をサポートしている必要があります。

1.**[レポート]** → **[待ち行列管理]** → **[領域内人数集計]** の順にクリックします。
2.レポートタイプとして、**[日次レポート]** / **[週次レポート]** / **[月次レポート]** / **[カスタムレポート]** を選択します。

日次レポート

日次レポートには、日単位のデータが表示されます。システムは、異なる領域の待ち行列形成時間を 1 日の各時間単位で計算します。

週次レポート、月次レポート

日次レポートと比較して、週次レポートと月次レポートは毎日提出されないため、時間がかかりません。システムは、異なる領域の待ち行列形成時間を 1 週間の各日、1 ヵ月の各日単位で計算します。

カスタムレポート

ユーザーは、レポートの日数をカスタマイズして、カスタム時間間隔の各日または各月の人数を分析できます。

注記

カレンダーで選択できる日数は 31 日以内です。

3. をクリックして、検索する期間を設定します。
4.**[領域]** リストで、カメラと、3 つ以下の領域を選択します。
5.統計タイプとして **[多重レベル比較]** を選択します。

6.待ち時間レベルを選択して、待ち時間に対する人数を計算するための待ち時間（秒）を入力します。

7.**[検索]** をクリックして、統計結果を生成します。

同じ領域の計算された人数の折れ線グラフが結果エリアに表示されます。異なる色の線は、待ち時間のレベルと一致します。

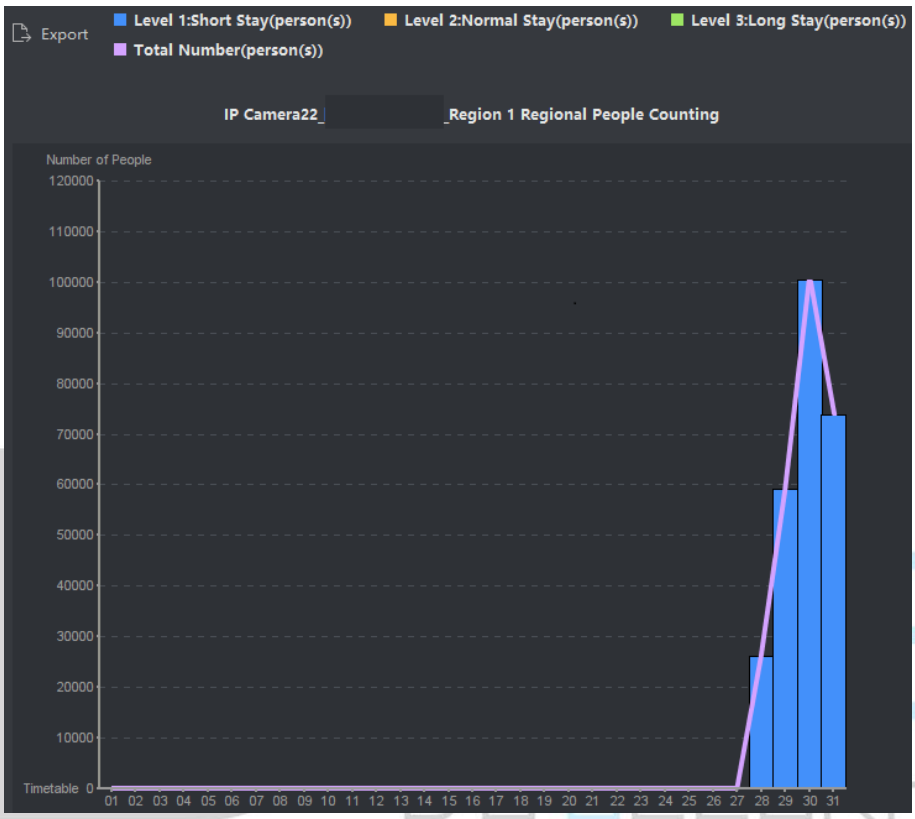

図 14-4 結果

8.オプション: **[エクスポート]** をクリックして、データを Excel ファイル形式でエクスポートします。

14.3.2 待ち行列状態分析

待ち行列状態分析は、待ち行列が特定の長さのままになっている時間と時間帯を計算します。領域内比較と複数の待ち行列長レベルの比較をサポートしています。

異なる領域の待ち行列形成時間の比較

待ち行列形成時間集計用のカメラを使用して、同じ期間中の異なる領域での待ち行列形成時間を検索して比較できます。これにより、異なる領域の混雑状況を分析して、いつ、どのようにサービス窓口数やスタッフ数を変更したら良いかと、案内要員を配置すべきかどうかなどを簡単に把握することができます。

始める前に

- デバイスをソフトウェアに追加して、対応する設定を適切に設定します。デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。
- デバイスのリモート設定ページのカメラの検知エリアに設定した領域が 3 つ以下であることを確認してください。領域の設定方法の詳細については、デバイスのユーザーマニュアルをご覧ください。

手順

注記

接続されているデバイスがこの機能をサポートしている必要があります。

1.**[レポート] → [待ち行列管理] → [待機時間]** の順にクリックします。
2.レポートタイプとして、**[日次レポート]** / **[週次レポート]** / **[月次レポート]** / **[カスタムレポート]** を選択します。

日次レポート

日次レポートには、日単位のデータが表示されます。システムは、異なる領域の待ち行列形成時間を 1 日の各時間単位で計算します。

週次レポート、月次レポート

日次レポートと比較して、週次レポートと月次レポートは毎日提出されないため、時間がかかりません。システムは、異なる領域の待ち行列形成時間を 1 週間の各日、1 ヵ月の各日単位で計算します。

カスタムレポート

ユーザーは、レポートの日数をカスタマイズして、カスタム時間間隔の各日または各月の待ち行列形成時間を分析できます。

注記

カレンダーで選択できる日数は 31 日以内です。

3. をクリックして、検索する期間を設定します。
4. **[領域]** リストで、カメラと、カメラあたり 3 つ以下の領域を選択します。
5. 統計タイプとして **[領域内比較]** を選択します。
6. レポート生成基準とする待ち行列長を設定します。
7. **[検索]** をクリックして、統計結果を生成します。
   指定した待ち行列長のままになる計算された時間の折れ線グラフが結果エリアに表示されます。異なる色の線は、選択した領域と一致します。

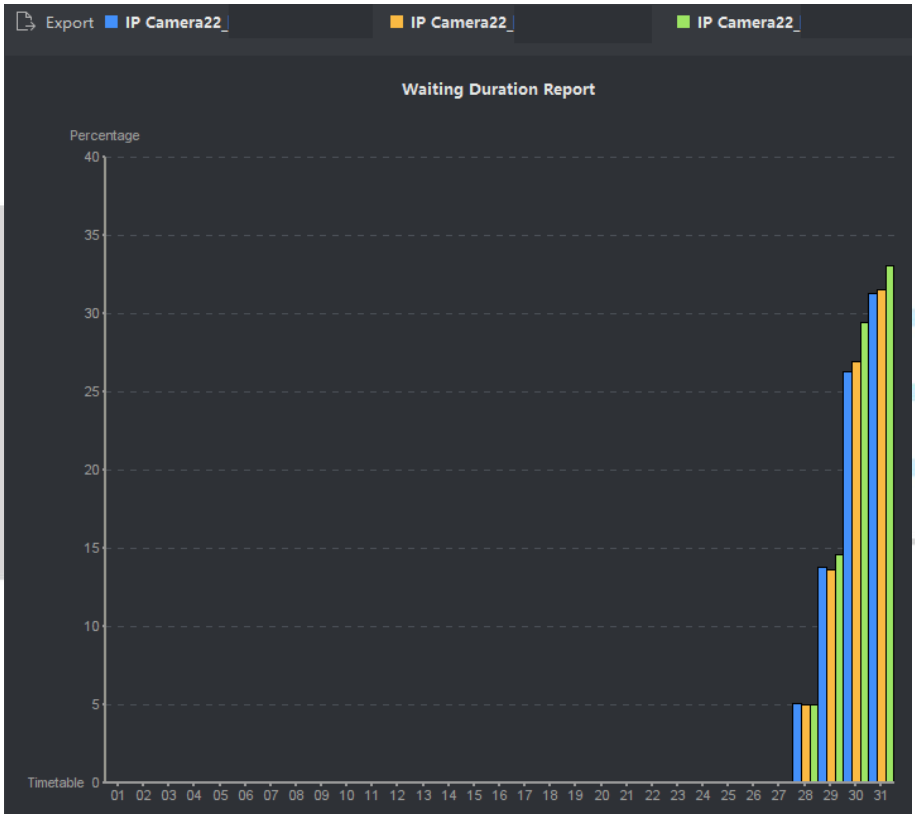

図 14-5 結果

8. オプション: **[エクスポート]** をクリックして、データを Excel ファイル形式でエクスポートします。

異なる待ち行列長レベルの待ち行列形成時間の比較

待ち行列形成時間集計用のカメラを使用して、同じ期間中の異なる長さの待ち行列の待ち行列形成時間を検索して比較できます。これにより、異なる領域の混雑状況を分析して、いつ、どのようにサービス窓口数やスタッフ数を変更したら良いかと、案内要員を配置すべきかどうかなどを簡単に把握することができます。

始める前に

デバイスをソフトウェアに追加して、対応する設定を適切に設定します。デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。

手順

注記

接続されているデバイスがこの機能をサポートしている必要があります。

1.**[レポート]** → **[待ち行列管理]** → **[待機時間]** の順にクリックします。
2.レポートタイプとして、**[日次レポート]** / **[週次レポート]** / **[月次レポート]** / **[カスタムレポート]** を選択します。

日次レポート

日次レポートには、日単位のデータが表示されます。システムは、異なる領域の待ち行列形成時間を 1 日の各時間単位で計算します。

週次レポート、月次レポート

日次レポートと比較して、週次レポートと月次レポートは毎日提出されないため、時間がかかりません。システムは、異なる領域の待ち行列形成時間を 1 週間の各日、1 ヵ月の各日単位で計算します。

カスタムレポート

ユーザーは、レポートの日数をカスタマイズして、カスタム時間間隔の各日または各月の待ち行列形成時間を分析できます。

注記

カレンダーで選択できる日数は 31 日以内です。

3. をクリックして、検索する期間を設定します。
4.**[領域]** リストで、カメラと、3 つ以下の領域を選択します。
5.統計タイプとして **[多重レベル比較]** を選択します。
6.レポート生成基準とする待ち行列長を設定します。
7.**[検索]** をクリックして、統計結果を生成します。
同じ領域の計算された時間の折れ線グラフが結果エリアに表示されます。異なる色の線は、待ち行列長レベルと一致します。

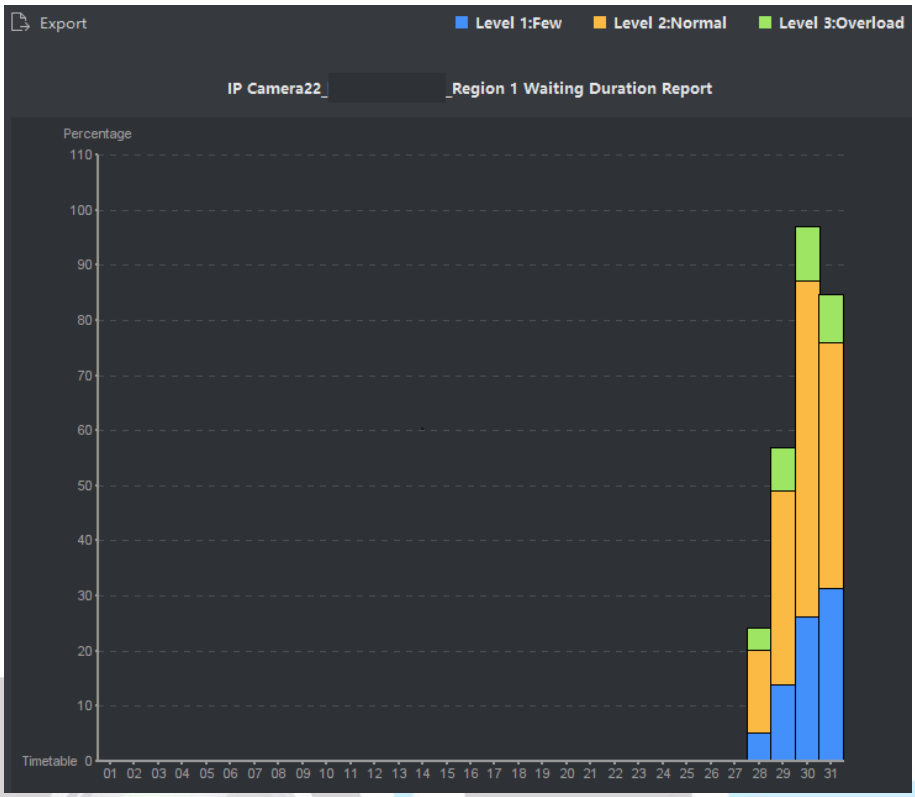

図 14-6 結果

8.オプション: **[エクスポート]** をクリックして、データを Excel ファイル形式でエクスポートします。

14.4 ヒートマップレポート

ヒートマップは、データを色によってグラフィカルに表したものです。ヒートマップデータは折れ線グラフで表示できます。カメラのヒートマップ機能を使用して、設定したエリアの顧客の訪問回数や滞留時間を分析できます。これにより店主は、顧客の関心のあるエリアを分析して、商品を手配することができます。

始める前に

ヒートマップネットワークカメラをソフトウェアに追加して、対応するエリアを適切に設定します。追加したカメラでヒートマップルールが設定されている必要があります。ヒートマップネットワークカメラの追加方法の詳細については、「*デバイスの追加*」をご覧ください。

手順

1.**[レポート]** → **[ヒートマップ]** の順にクリックして、ヒートマップページを表示します。
2.レポートタイプとして、**[日次レポート]** / **[週次レポート]** / **[月次レポート]** / **[年次レポート]** / **[カスタムレポート]** を選択します。

日次レポート

日次レポートには、日単位のデータが表示されます。システムは、ヒートマップのデータを 1 日の各時間単位で計算します。

週次レポート、月次レポートおよび年次レポート

日次レポートと比較して、週次レポート、月次レポートおよび年次レポートは毎日提出されないため、時間がかかりません。システムは、ヒートマップのデータを 1 週間の各日、1 ヵ月の各日、1 年の各月単位で計算します。

カスタムレポート

レポートの日数をカスタマイズして、カスタム時間間隔の各日または各月の滞留時間または混雑傾向を分析できます。

注記

カスタムレポートの期間は 31 日以内でなければなりません。

3.統計タイプとして **[By Dwell Time（滞留時間別）]** または **[By Crowd Trend（混雑傾向別）]** を選択します。

By Dwell Time（滞留時間別）

システムは、人の滞留時間に従ってヒートマップ値（折れ線グラフの縦軸値または画像での色）を計算します。

By Crowd Trend（混雑傾向別）

システムは、検知された人数に応じて、ヒートマップ値（折れ線グラフの縦軸値または画像での色）を計算します。

4.検索する期間を設定します。

5.カメラリストでヒートマップカメラを選択します。

6.**[ヒートマップを生成]** をクリックして、カメラのヒートマップを表示します。

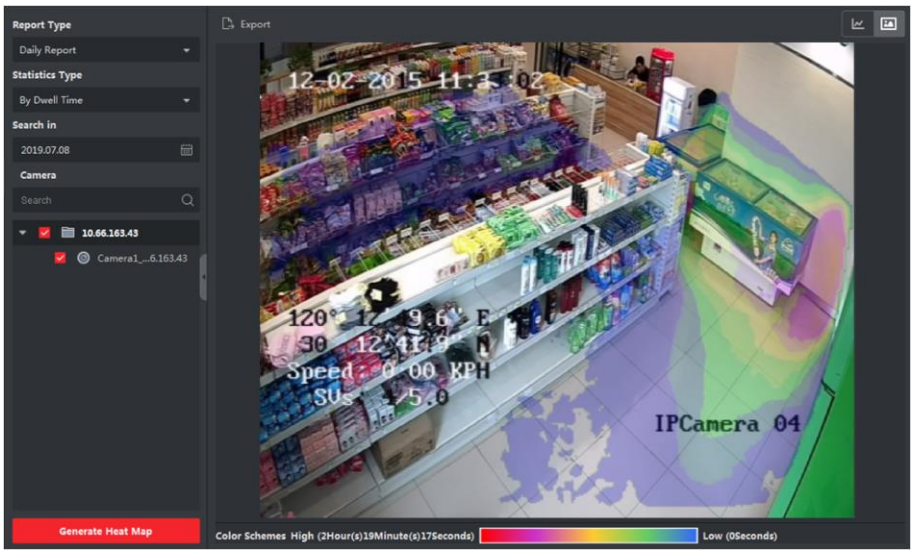

図 14-7 結果

7.オプション: ヒートマップレポートを生成した後に、次の操作を実行できます。

折れ線グラフで表示	をクリックして、統計を折れ線グラフで表示します。
画像モードで表示	をクリックして、統計を画像モードで表示します。 赤のカラーブロック（255、0、0）は最も人気のあるエリアを示し、青のカラーブロック（0、0、255）はあまり人気のないエリアを示します。
統計データを保存	**[エクスポート]** をクリックして、ヒートマップの詳細データを PC に保存します。

第 15 章 データの検索

[データ検索] モジュールでは、顔認識カメラでキャプチャされた顔画像の検索、DeepinMind デバイスでキャプチャされた人体画像の検索、動作分析の関連画像およびビデオの表示、DeepinMind デバイスでキャプチャされた車両画像の検索、DeepinMind デバイスでキャプチャされた頻出人物画像の検索、およびヘルメット未着用画像の検索を実行できます。

15.1 顔画像の検索

接続されているデバイス（NVR や HDVR など）が顔検索をサポートしている場合は、関連する画像を検索して、画像に関連するビデオファイルを再生できます。

15.1.1 アップロードした画像による顔の検索

PC から顔画像をアップロードして、アップロードした画像とキャプチャされた顔画像を比較できます。

始める前に

デバイスをソフトウェアに追加して、対応する設定を適切に設定します。デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。

手順

注記

接続されているデバイスがこの機能をサポートしている必要があります。

1.**[データ検索]** → **[顔画像検索]** の順にクリックして、顔画像検索ページを表示します。
2. をクリックして、キャプチャされた顔画像またはビデオファイルの検索対象とする開始時刻と終了時刻を設定します。
3.カメラパネルでデバイスを選択します。
4.ドロップダウンリストから **[画像]** を選択して、画像で検索します。
5.検索する顔画像を選択します。
   1）**[画像を選択]** をクリックして、PC から画像をアップロードします。
   2）キャプチャされた顔画像との照合用に、アップロードした画像から検知された顔を選択します。

注記

- 画像の解像度は 4096 x 4080 未満でなければなりません。
- JPG および JPEG 形式のみをサポートしています。

6.類似度レベルを設定します。

例

類似度を 40 に設定すると、アップロードした顔画像と 40%以上の類似度のキャプチャ画像が表示されます。

7.表示する結果の最大数を設定します。

8.**[検索]** をクリックして検索を開始します。

画像の検索結果がリストに表示されます。

9.画像をエクスポートして、PC に保存します。

画像をエクスポート

エクスポートする画像を選択して、ローカル PC に保存します。

現在のページをエクスポート

現在のページのすべての画像をエクスポートします。

セグメントをエクスポート

画像をパッケージでダウンロードできます。各パッケージには、最大 1,000 個の画像を含めることができます。

10.オプション: 検索結果に基づいてセカンダリ検索を実行します。

1）検索した画像に移動して、をクリックします。

この画像内のすべての顔が分析されて表示されます。

2）セカンダリ検索を行う顔を選択します。

3）類似度と期間を設定します。

4）**[検索]** をクリックします。

クライアントは、選択した顔画像に基づいて、キャプチャ画像内の顔を検索して比較します。

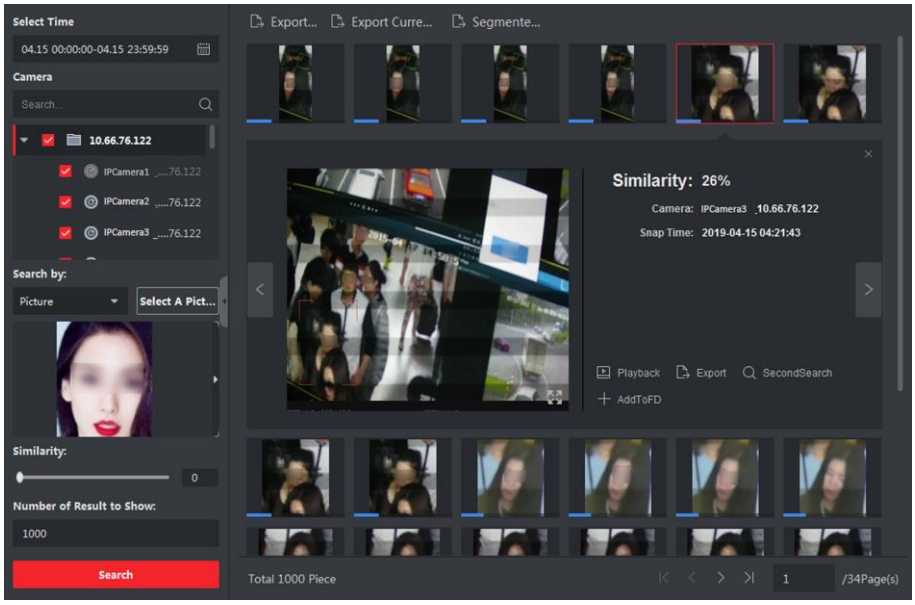

図 15-1 結果

11.オプション: 検索後に、次の 1 つまたは複数の操作を実行できます。

詳細を表示	リストで画像をクリックして、詳細を表示します。 をクリックして画像を大きく表示したり、 をクリックして復元することもできます。
関連するビデオを再生	**[再生]** をクリックして、画像の関連するビデオファイル（キャプチャの前後 5 秒間）を右下のビューウィンドウで再生します。

注記

- をクリックしてビデオを大きく表示したり、 をクリックして復元できます。
- をクリックして再生速度を調整したり、 をクリックしてビデオファイルをフレームごとに再生できます。また、 をクリックしてオーディオを有効にしたり、再生ウィンドウをダブルクリックしてウィンドウを最大化できます。

画像を PC に保存	**[画像のエクスポート]** をクリックして、必要に応じて画像を選択してローカル PC にエクスポートします。

15.1.2 イベントタイプによる顔の検索

さまざまなイベントタイプをフィルタリングして、デバイスのキャプチャされた顔画像を検索できます。

始める前に

デバイスをソフトウェアに追加して、対応する設定を適切に設定します。デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。

手順

注記

接続されているデバイスがこの機能をサポートしている必要があります。

1.**[データ検索]** → **[顔検索]** の順にクリックして、顔画像検索ページを表示します。
2. をクリックして、キャプチャされた顔画像またはビデオファイルの検索対象とする開始時刻と終了時刻を設定します。
3.カメラパネルでデバイスを選択します。
4.ドロップダウンリストから **[イベントタイプ]** を選択して、イベントタイプで検索します。
5.イベントタイプを選択します。

無制限

キャプチャされたすべての顔画像を検索します。

Matched Face（一致した顔）

顔ライブラリ内の顔と一致した顔をキャプチャ画像で検索します。

Mismatched Face（不一致の顔）

顔ライブラリ内の顔と一致しなかった顔をキャプチャ画像で検索します。

不明人物検知アラーム

不明人物検知アラームがトリガーされたときにキャプチャされた画像を検索します。

6.表示する結果の最大数を設定します。

7.**[検索]** をクリックして検索を開始します。

画像の検索結果がリストに表示されます。

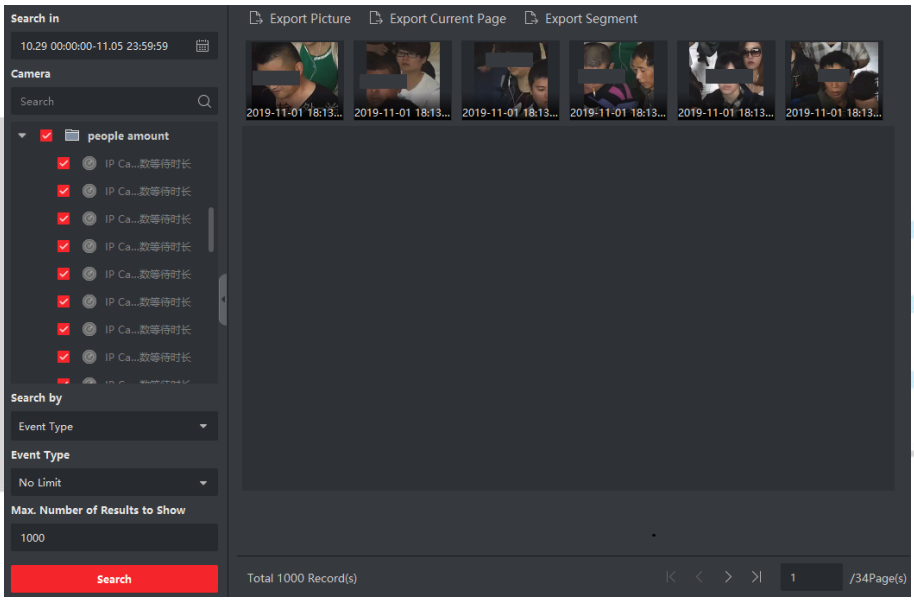

図15-2 検索結果

8.画像をエクスポートして、PC に保存します。

画像をエクスポート

エクスポートする画像を選択して、ローカル PC に保存します。

現在のページをエクスポート

現在のページのすべての画像をエクスポートします。

セグメントをエクスポート

画像をパッケージでダウンロードできます。各パッケージには、最大 1,000 個の画像を含めることができます。

9.オプション: 検索結果に基づいてセカンダリ検索を実行します。

1）検索した画像に移動して、をクリックします。

この画像内のすべての顔が分析されて表示されます。

2）セカンダリ検索を行う顔を選択します。

3）類似度と期間を設定します。

4）**[検索]** をクリックします。

クライアントは、選択した顔画像に基づいて、キャプチャ画像内の顔を検索して比較します。

10.オプション: 検索後に、次の 1 つまたは複数の操作を実行できます。

詳細を表示	リストで画像をクリックして、詳細を表示します。 をクリックして画像を大きく表示したり、 をクリックして復元することもできます。
関連するビデオを再生	**[再生]** をクリックして、画像の関連するビデオファイル（キャプチャの前後 5 秒間）を右下のビューウィンドウで再生します。

注記

- をクリックしてビデオを大きく表示したり、 をクリックして復元できます。
- をクリックして再生速度を調整したり、 をクリックしてビデオファイルをフレームごとに再生できます。また、 をクリックしてオーディオを有効にしたり、再生ウィンドウをダブルクリックしてウィンドウを最大化できます。

画像を PC に保存	**[画像のエクスポート]** をクリックして、必要に応じて画像を選択してローカル PC にエクスポートします。

15.1.3 人物名による顔の検索

デバイスのキャプチャされた顔画像を人物名で検索できます。

始める前に

デバイスをソフトウェアに追加して、対応する設定を適切に設定します。デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。

手順

注記

接続されているデバイスがこの機能をサポートしている必要があります。

1.**[データ検索]** → **[顔検索]** の順にクリックして、顔画像検索ページを表示します。

2.カメラパネルでデバイスを選択します。
3.ドロップダウンリストから **[名前]** を選択して、人物名で検索します。
4. をクリックして、キャプチャされた顔画像またはビデオファイルの検索対象とする開始時刻と終了時刻を設定します。
5.人物名のキーワードを入力します。
6.表示する結果の最大数を設定します。
7.**[検索]** をクリックして検索を開始します。
名前が検索条件に一致するすべての人物が表示されます（あいまい一致もサポートされます）。

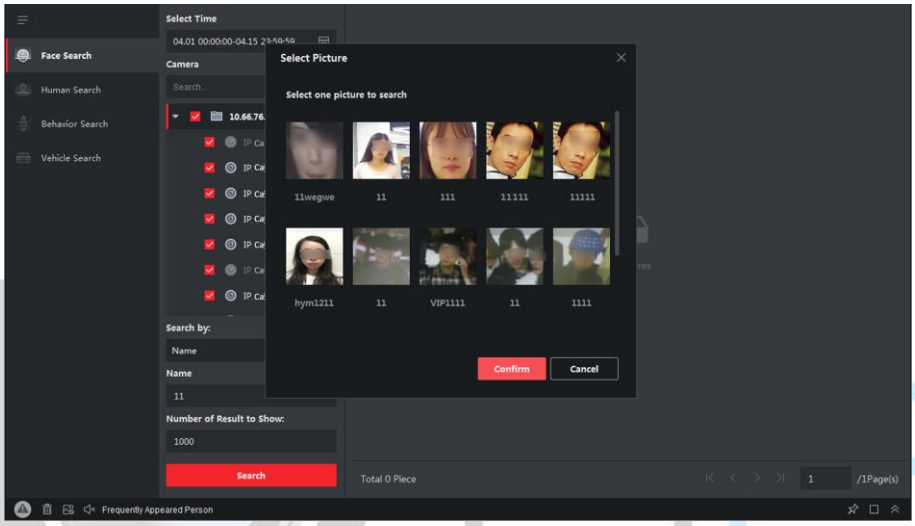

図 15-3 結果

8.検索する画像を 1 つ選択して、**[確認]** をクリックします。

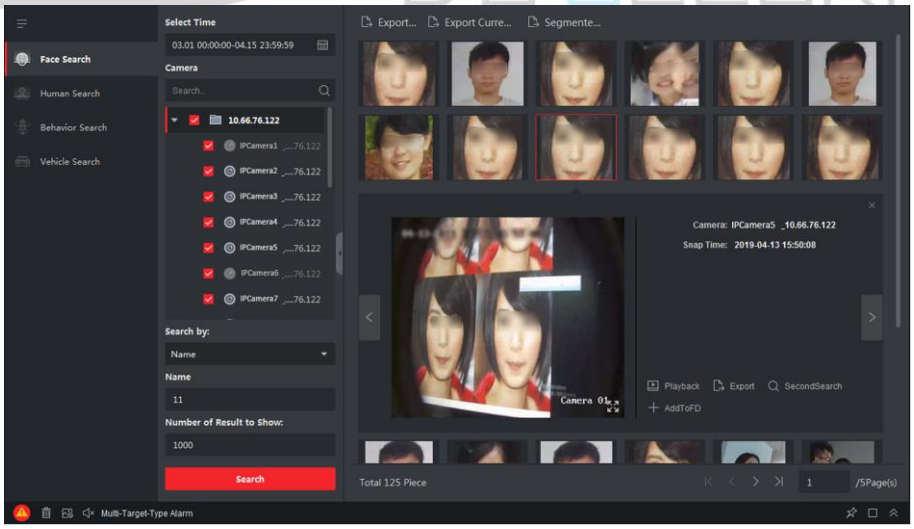

図 15-4 結果

画像の検索結果がリストに表示されます。
9.画像をエクスポートして、PC に保存します。

画像をエクスポート

エクスポートする画像を選択して、ローカル PC に保存します。

現在のページをエクスポート

現在のページのすべての画像をエクスポートします。

セグメントをエクスポート

画像をパッケージでダウンロードできます。各パッケージには、最大 1,000 個の画像を含めることができます。

10.検索結果に基づいてセカンダリ検索を実行します。

1）検索した画像に移動して、をクリックします。

この画像内のすべての顔が分析されて表示されます。

2）セカンダリ検索を行う顔を選択します。

3）類似度と期間を設定します。

4）**[検索]** をクリックします。

画像の検索結果がリストに表示されます。

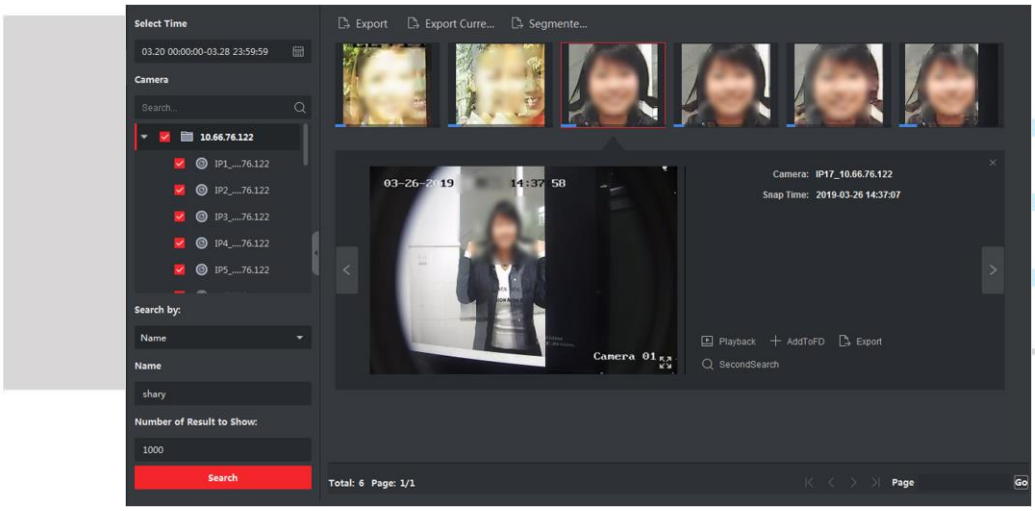

図15-5 検索結果

11.検索後に、次の 1 つまたは複数の操作を実行できます。

詳細を表示	リストで画像をクリックして、詳細を表示します。 をクリックして画像を大きく表示したり、 をクリックして復元することもできます。
関連するビデオを再生	**[再生]** をクリックして、画像の関連するビデオファイル（キャプチャの前後 5 秒間）を右下のビューウィンドウで再生します。

注記

- をクリックしてビデオを大きく表示したり、 をクリック

して復元できます。

- 1x をクリックして再生速度を調整したり、 をクリックしてビデオファイルをフレームごとに再生できます。また、 をクリックしてオーディオを有効にしたり、再生ウィンドウをダブルクリックしてウィンドウを最大化できます。

画像を PC に保存 **[画像のエクスポート]** をクリックして、必要に応じて画像を選択してローカル PC にエクスポートします。

15.1.4 顔の特徴による顔の検索

クライアントは、性別やメガネ着用などの顔の特徴による、検知された顔画像の検索をサポートしています。

手順

1.**[データ検索]** → **[顔画像検索]** の順にクリックします。
2.検索する期間を選択します。
3.カメラリストでカメラを選択します。
4.検索タイプとして **[顔の特徴]** を選択します。
5.検索する顔の特徴を設定します。
6.表示する結果の最大数を入力します。
7.**[検索]** をクリックします。
検索で見つかった顔画像が右側に表示されます。

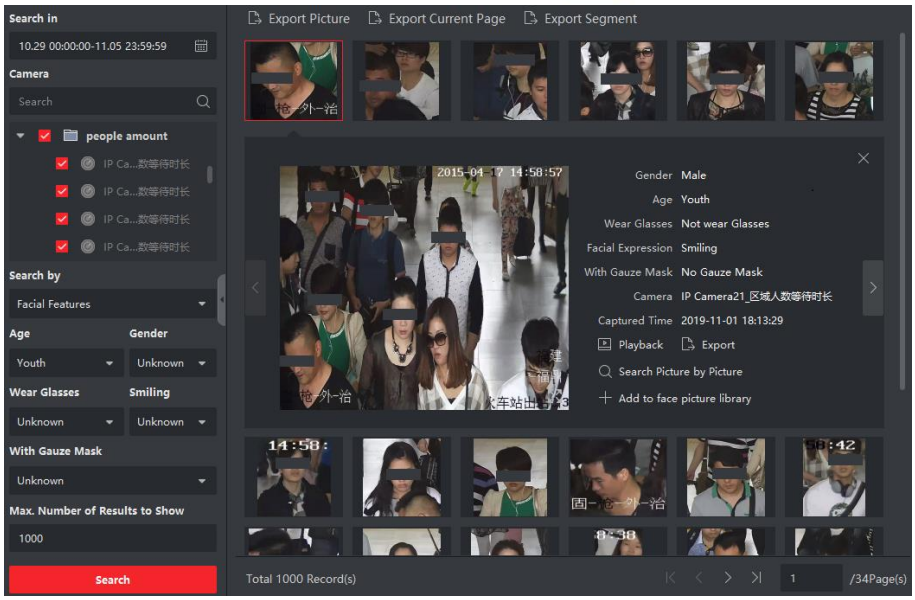

図 15-6 結果

8.オプション: 顔画像を選択して、キャプチャ画像と人物情報を表示します。
9.オプション: 以下の操作を実行します。

操作説明	
画像をエクスポート	**[画像をエクスポート]** をクリックして、画像にチェックを入れてコンピュータに保存します。
現在のページをエクスポート	**[現在のページをエクスポート]** をクリックして、アラームの種類、カメラ、アラーム時間などが含まれた Excel ファイルとしてアラーム情報をコンピュータに保存します。
セグメントをエクスポート	**[セグメントをエクスポート]** をクリックして、1000 以下の数値を入力します。例えば、最初の 10 個の画像をコンピュータに保存する場合は、「10」と入力します。

15.2 人体の検索

DeepinMind デバイスでは、検索条件（ローカル PC からアップロードした画像など）と特徴を設定してキャプチャされた人体画像を検索し、画像の関連するビデオを表示できます。

15.2.1 アップロードした画像による人体の検索

DeepinMind デバイスでは、ローカル PC から人体画像をアップロードして、アップロードした画像をデバイスのキャプチャされた人体画像と比較したり、特定の時間に特定のカメラでキャプチャされたすべての人体画像を検索できます。

始める前に

デバイスをソフトウェアに追加して、対応する設定を適切に設定します。デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。

手順

注記

接続されているデバイスがこの機能をサポートしている必要があります。

1.**[データ検索]** → **[人体検索]** の順にクリックして、人体検索ページを表示します。
2. をクリックして、キャプチャされた人体画像またはビデオファイルの検索対象とする開始時刻と終了時刻を設定します。
3.カメラパネルでデバイスを選択します。
4.[検索条件] フィールドで検索条件を選択します。

画像

画像をアップロードして、アップロードした画像とデバイスのキャプチャされた人体

画像を比較します。この画像内のすべての人体が分析されて表示されます。

1. **[画像を選択]** をクリックして、比較する画像をコンピュータから選択します。

注記

- 画像は 4 MB 未満でなければなりません。
- 画像の解像度は 4096 x 4080 未満でなければなりません。
- JPG および JPEG 形式のみをサポートしています。

2. 類似度レベルを設定します。例えば、類似度を 40 に設定すると、アップロードした人体画像と 40%以上の類似度のキャプチャ画像が表示されます。

すべて

期間中に選択したカメラでキャプチャされたすべての画像を検索します。

5.表示する結果の最大数を設定します。

注記

選択した期間中に選択したカメラでキャプチャされた画像の数が、表示する最大数を超えた場合は、直近の最大数個の画像のみが表示されます。
例えば、選択した期間中に選択したカメラでキャプチャされた画像の数が 2000 個で、表示する最大数が 1000 個の場合、直近の 1000 個の画像のみが表示されます。

6.**[検索]** をクリックして検索を開始します。
画像の検索結果がリストに表示されます。

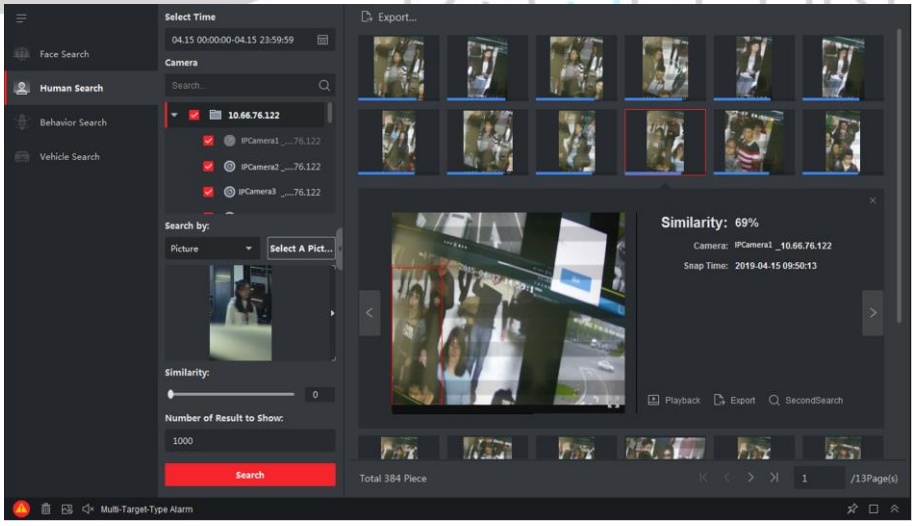

図15-7 検索結果

7.オプション: 検索結果に基づいてセカンダリ検索を実行します。

1）検索した画像に移動して、をクリックします。

この画像内のすべての人体が分析されて表示されます。

2）セカンダリ検索を行う人体を選択します。

3）類似度と期間を設定します。

4）**[検索]** をクリックします。

クライアントは、選択した人体画像に基づいて、キャプチャ画像内の人体を検索して比較します。

8.オプション: 人体を検索した後に、次の 1 つまたは複数の操作を実行できます。

詳細を表示	リストで画像をクリックして、詳細を表示します。 をクリックして画像を大きく表示したり、 をクリックして復元することもできます。
関連するビデオを再生	**[再生]** をクリックして、画像の関連するビデオファイル（キャプチャの前後 5 秒間）を右下のビューウィンドウで再生します。

注記

- をクリックしてビデオを大きく表示したり、 をクリックして復元できます。
- をクリックして再生速度を調整したり、 をクリックしてビデオファイルをフレームごとに再生できます。また、 をクリックしてオーディオを有効にしたり、再生ウィンドウをダブルクリックしてウィンドウを最大化できます。

画像を PC に保存	**[画像のエクスポート]** をクリックして、必要に応じて画像を選択してローカル PC にエクスポートします。

15.2.2 人物の特徴による人体の検索

年齢グループ、性別、服装などの人物の特徴を検索条件として設定することで、デバイスのキャプチャされた人体画像を検索できます。

始める前に

デバイスをソフトウェアに追加して、対応する設定を適切に設定します。デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。

手順

注記

接続されているデバイスがこの機能をサポートしている必要があります。

1.**[データ検索]** → **[人体検索]** の順にクリックして、人体検索ページを表示します。
2. をクリックして、キャプチャされた人体画像またはビデオファイルの検索対象とする開始時刻と終了時刻を設定します。
3.カメラパネルでデバイスを選択します。
4.検索モードとして **[Features（特徴）]** を選択します。
5.人物の特徴（年齢グループ、性別、上着の色、メガネ着用など）を設定します。
6.検索する人体画像のイベントタイプを選択します。
7.表示する結果の最大数を設定します。
8.**[検索]** をクリックして検索を開始します。
画像の検索結果がリストに表示されます。

図15-8 検索結果

9.オプション: 検索結果に基づいてセカンダリ検索を実行します。
1）検索した画像に移動して、をクリックします。
この画像内のすべての人体が分析されて表示されます。
2）セカンダリ検索を行う人体を選択します。
3）類似度と期間を設定します。
4）**[検索]** をクリックします。
クライアントは、選択した人体画像に基づいて、キャプチャ画像内の人体を検索して比較します。
10.オプション: 検索後に、次の 1 つまたは複数の操作を実行できます。

詳細を表示	リストで画像をクリックして、詳細を表示します。 をクリックして画像を大きく表示したり、 をクリックして復元することもできます。
関連するビデオを再生	をクリックして、画像の関連するビデオファイルを右下のビューウィンドウで再生します。

注記

- をクリックしてビデオを大きく表示したり、 をクリックして復元できます。
- をクリックして再生速度を調整したり、 をクリックしてビデオファイルをフレームごとに再生できます。また、 をクリックしてオーディオを有効にしたり、再生ウィンドウをダブルクリックしてウィンドウを最大化できます。

画像を PC に保存	**[画像のエクスポート]** をクリックして、必要に応じて画像を選択してローカル PC にエクスポートします。

15.3 動作分析の関連画像およびビデオの表示

接続されているデバイスが動作検索（例：ラインクロス、群衆および徘徊）をサポートしている場合は、関連する画像を検索して、関連する画像とビデオファイルを表示できます。

始める前に

デバイスをソフトウェアに追加して、対応する設定を適切に設定します。カメラの追加方法の詳細については、「*デバイスの追加*」をご覧ください。

手順

1.**[データ検索]** → **[動作分析]** の順にクリックして、動作分析ページを表示します。
2. をクリックして、一致する画像の検索対象とする開始時刻と終了時刻を設定します。
3.カメラリストでカメラを選択します。

注記

接続されているデバイス（NVR または DVR）がこの機能をサポートしている必要があります。

4.オプション: **[誤報除去]** にチェックを入れて、結果から誤報を除去します。

例

カメラは、高感度であることなどにより、樹木の揺れを動体検知アラームと見なしたり、動物を人がトリガーしたラインクロスアラームと見なすことがあり、これらは NVR または DVR によって誤報と見なされます。

5.動作分析レポートのイベントタイプを選択します。
6.**[検索]** をクリックして検索を開始します。
7.オプション: 動作を検索した後に、次の操作を実行できます。

詳細を表示	リストで画像をクリックして、詳細を表示します。 をクリックして画像を大きく表示したり、 をクリックして復元することもできます。
関連するビデオを再生	**[再生]** をクリックして、画像の関連するビデオファイル（キャプチャの前後 5 秒間）を右下のビューウィンドウで再生します。

注記

- をクリックしてビデオを大きく表示したり、 をクリックして復元できます。
- をクリックして再生速度を調整したり、 をクリックしてビデオファイルをフレームごとに再生できます。また、 をクリックしてオーディオを有効にしたり、再生ウィンドウをダブルクリックしてウィンドウを最大化できます。

画像を PC に保存　**[画像のエクスポート]** をクリックして、必要に応じて画像を選択してローカル PC にエクスポートします。

15.4 車両の検索

DeepinMind デバイスでは、ナンバープレート番号やキャプチャ時間などを検索条件として設定することで、デバイスのキャプチャされた車両画像を検索できます。

始める前に

デバイスをソフトウェアに追加して、対応する設定を適切に設定します。デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。

手順

注記

接続されているデバイスがこの機能をサポートしている必要があります。

1.**[データ検索]** → **[車両検索]** の順にクリックして、車両検索ページを表示します。
2. をクリックして、キャプチャされた車両画像またはビデオファイルの検索対象とする開始時刻と終了時刻を設定します。
3.検索タイプを選択します。

車両

車両のナンバープレート番号を入力して、キャプチャされた車両画像を検索して表示します。

Plate（ナンバープレート）

車両のナンバープレート番号を入力して、キャプチャされたライセンスプレート番号の画像を検索して表示します。

混合交通検知

車両のナンバープレート番号を入力して、特定車両の混合交通検知の関連画像を検索して表示します。

注記

カメラが混合交通検知をサポートしている必要があります。

交通違反

車両のナンバープレート番号を入力して、特定車両の交通違反の関連画像を検索およ

び表示します。

注記

カメラが交通違反をサポートしている必要があります。

4.カメラパネルでデバイスを選択します。
5.キーボードで、検索するナンバープレート番号を入力します。
6.表示する結果の最大数を設定します。
7.**[検索]** をクリックして検索を開始します。

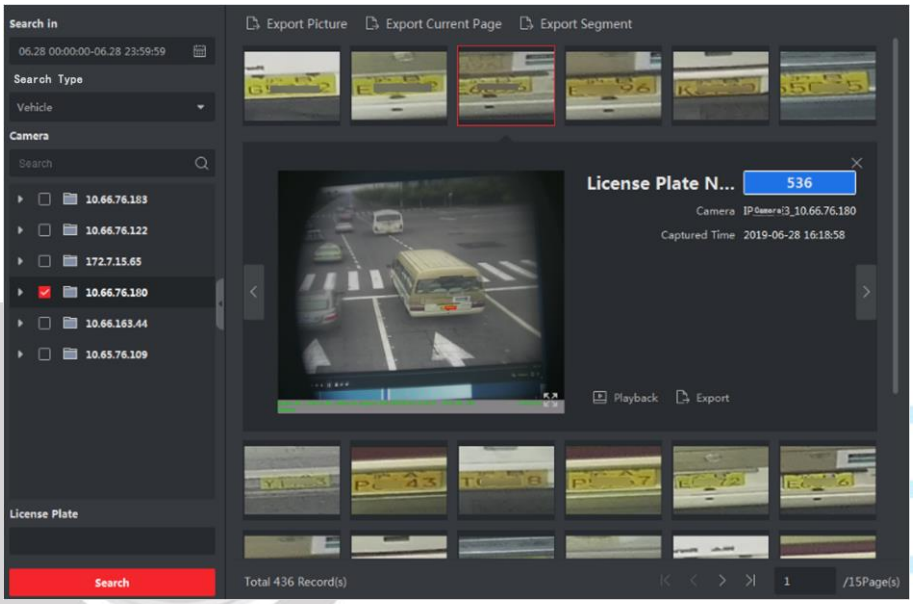

図 15-9 結果

画像の検索結果がリストに表示されます。

8.オプション: 画像をクリックして、キャプチャ画像全体、キャプチャ時間などを表示します。
9.オプション: 画像をローカル PC にエクスポートします。
- **[画像をエクスポート]** をクリックして、エクスポートする画像を選択して **[エクスポート]** をクリックします。
- **[現在のページをエクスポート]** をクリックして、現在のページ上のすべての画像と情報をエクスポートします。
- **[セグメントをエクスポート]** をクリックして、画像とキャプチャ情報をパッケージでダウンロードします。各パッケージには、最大 1000 個の画像を含めることができます。

10.オプション: 必要に応じて、次の操作を実行します。

顔画像ライブラリに追加	**[顔画像ライブラリに追加]** をクリックして、現在の顔画像をライブラリに追加します。
詳細情報を表示	**[ビュー]** をクリックして、この人物の過去のキャプチャ画像と

キャプチャ時間を表示します。

再生	**[再生]** をクリックして、キャプチャ時間の前後 5 秒間のビデオを再生します。
エクスポート	エクスポートする画像をクリックして、**[エクスポート]** をクリックしてこの画像をエクスポートします。

15.5 ヘルメットの検索

ヘルメット検知デバイスをクライアントに追加した後に、デバイスがヘルメットを着用していない人物を検知すると、デバイスはイベントをトリガーし、いくつかの画像をキャプチャして、マネージャに通知します。検知されたヘルメット未着用人物のアラーム画像を検索できます。このようにして、建築業者にヘルメットの着用を促し、建築業者の安全意識を向上させることができます。

始める前に

ヘルメット検知機能を備えたデバイスをクライアントに追加します。

手順

1.**[データ検索]** → **[Hard Hat Search（ヘルメット検索）]** の順にクリックして、ヘルメット検索ページを表示します。
2.検索対象とする開始時刻と終了時刻を設定します。
3.検索するカメラを選択します。
4.**[検索]** をクリックします。
ヘルメットアラームのキャプチャ画像が右側のパネルに表示されます。最大 30 個の画像を 1 ページに表示できます。
5.必要に応じて、次の操作を実行します。

画像をエクスポート	1. **[画像をエクスポート]** をクリックします。 2. 1 つまたは複数の画像を選択するか、ページの下部にある **[すべてを選択]** にチェックを入れます。 3. ページの下部にある **[エクスポート]** をクリックして、選択した画像をエクスポートします。
画像全体を表示	画像をクリックすると、画像全体とキャプチャ時間がページの中央に表示されます。
ビデオを再生	画像をクリックし、**[再生]** をクリックして、キャプチャ時間の前後 5 秒間のビデオを再生します。

15.6 人物の頻度の検索

人物の頻度とは、特定の期間中に検知エリアに現れた人物の出現頻度のことです。頻出人物とは、出現頻度が事前定義したしきい値を超える人物のことで、低出現頻度人物とは、出現頻度が事前定義したしきい値よりも低い人物のことです。クライアントは、頻出人物の検索をサポートしていて、これにより高度なセキュリティが必要な場所を保護することができます。また、低出現頻度人物の検索もサポートしていて、ある人物が特定の期間にめったに出現しない場合、問題が起きている可能性があることを把握できます。

15.6.1 頻出人物の検索

人物のキャプチャされた顔画像を、顔画像ライブラリの顔画像と比較できます。一致しない場合、その人物は頻出人物と判断され、イベントがトリガーされてセキュリティ担当者に通知されます。例えば、高度な安全性が求められるシーン（銀行など）で、不明人物が頻繁に現れた場合、イベントをトリガーしてセキュリティ担当者または関係者に通知できます。一致した場合、その人物はホワイトリストに含まれている人物と判断され、頻出人物アラームはトリガーされません。キャプチャ画像やキャプチャ時間など、特定の時間のイベント情報を検索できます。また、詳細な画像を表示したり、関連するビデオを再生できます。

始める前に

- デバイスで頻出人物アラームが設定されていることを確認してください。
- デバイスで警戒が開始されていることを確認してください。

手順

1.**[データ検索]** → **[People Frequency Search（人物の頻度を検索）]** → **[頻出人物]** の順にクリックします。
2.検索対象とする開始時刻と終了時刻を設定します。
3.検索するデバイスを選択します。
4.**[検索]** をクリックします。
頻出人物アラームに関連する画像が右側のパネルに表示されます。

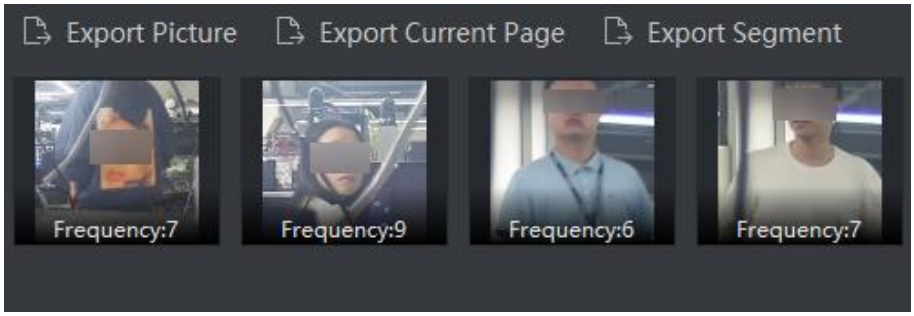

図 15-10 結果

5.オプション: 画像をクリックして、キャプチャ画像全体、キャプチャ時間などを表示します。
6.オプション: 画像をローカル PC にエクスポートします。
- **[画像をエクスポート]** をクリックして、エクスポートする画像を選択して **[エクスポート]** をクリックします。
- **[現在のページをエクスポート]** をクリックして、現在のページ上のすべての画像と情報をエクスポートします。
- **[セグメントをエクスポート]** をクリックして、画像とキャプチャ情報をパッケージでダウンロードします。各パッケージには、最大 1,000 個の画像を含めることができます。

7.オプション: 必要に応じて、次の操作を実行します。

顔画像ライブラリに追加	**[顔画像ライブラリに追加]** をクリックして、現在の顔画像をライブラリに追加します。
詳細情報を表示	**[ビュー]** をクリックして、この人物の過去のキャプチャ画像とキャプチャ時間を表示します。
再生	**[再生]** をクリックして、キャプチャ時間の前後 5 秒間のビデオを再生します。
エクスポート	エクスポートする画像をクリックして、**[エクスポート]** をクリックしてこの画像をエクスポートします。

15.6.2 低出現頻度人物の検索

デバイスは、低出現頻度人物レポートをクライアントに定期的に送信して、一定回数出現しなかった人物などの情報を提供します。これによりセキュリティ担当者は直ちにこのことを把握して、その人物のところへ行って確認することができます。この機能は、通常、一人暮らしの高齢者や拘置人に対して使用します。ある人物が一定期間出現しなかった場合、セキュリティ担当者はその人物を見つけて、問題が発生していないことや、逃亡していないことを確認する必要があります。

始める前に

- デバイスで頻出人物アラームが設定されていることを確認してください。
- デバイスで警戒が開始されていることを確認してください。
- デバイスのリモート設定ページで、検知時間、統計期間、頻度しきい値、および顔画像ライブラリが設定されていることを確認してください。

手順

1.**[データ検索] → [People Frequency Search（人物の頻度を検索）] → [Rarely Appeared Person（低出現頻度人物）]** の順にクリックします。
2.検索対象とする開始時刻と終了時刻を設定します。

3.検索するデバイスを選択します。
4.**[検索]** をクリックします。
低出現頻度人物レポートが右側のパネルに表示されます。

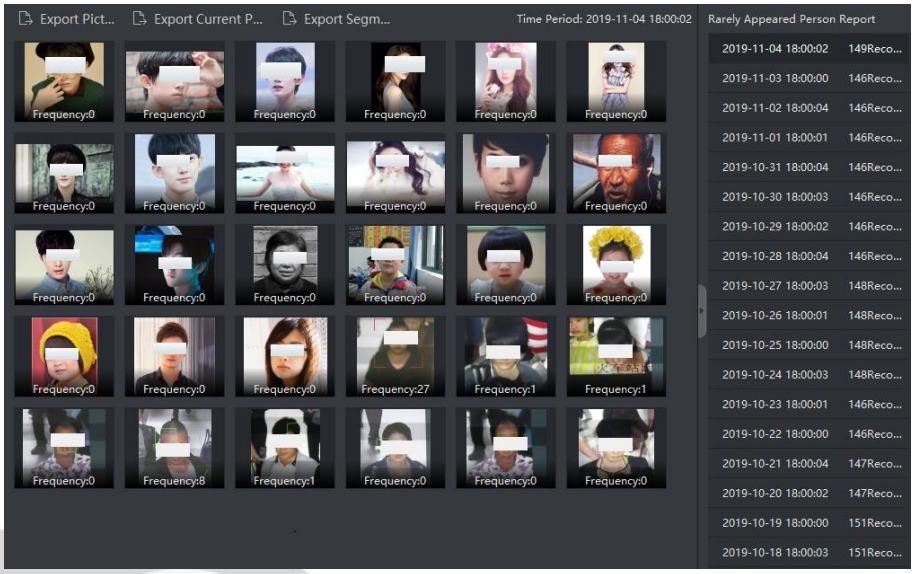

図 15-11 結果

5.レポートをダブルクリックして、低出現頻度人物を表示します。
6.オプション: 画像をクリックして、キャプチャ画像の詳細を表示します。
7.オプション: 画像をローカル PC にエクスポートします。
- **[画像をエクスポート]** をクリックして、エクスポートする画像を選択して **[エクスポート]** をクリックします。
- **[現在のページをエクスポート]** をクリックして、現在のページ上のすべての画像と情報をエクスポートします。
- **[セグメントをエクスポート]** をクリックして、画像とキャプチャ情報をパッケージでダウンロードします。各パッケージには、最大 1,000 個の画像を含めることができます。

15.7 顔認識チェックイン

指定した期間に顔認識でチェックインした人の出勤記録を検索して、データをローカル PC にエクスポートできます。また、出勤回数、遅刻回数、早退回数などを表示することができます。

始める前に

デバイスをソフトウェアに追加して、対応する設定を適切に設定します。デバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。

手順

注記

接続されているデバイスがこの機能をサポートしている必要があります。

1.**[データ検索]** → **[顔認識チェックイン]** に移動します。
2. をクリックして、検索の開始時刻と終了時刻を設定します。
3.**[Check-In Period（チェックイン期間）]** を設定します。
4.顔認識チェックインに使用するカメラにチェックを入れます。
5.1 つまたは複数の顔画像ライブラリにチェックを入れて、選択したライブラリで人物の出勤を検索します。
6.表示する結果の最大数を入力します。
7.**[検索]** をクリックして検索を開始します。
検索結果に、顔画像、顔ライブラリ、名前、チェックイン回数などの出勤記録が表示されます。

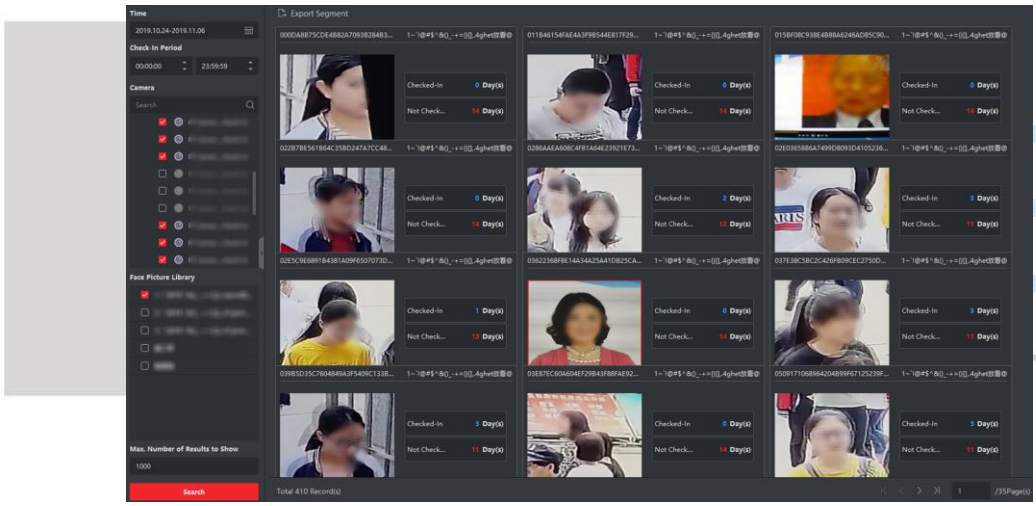

図 15-12 結果

8.オプション: 右上隅の **[すべてをエクスポート]** をクリックして、データをローカル PC にエクスポートします。

第 16 章 AI ダッシュボード

クライアントは [AI ダッシュボード] モジュールを提供していて、これにより顔比較や、固定カメラおよびパノラマカメラのリンクキャプチャなど、AI 機能を備えたデバイスの高度な機能を利用できます。

16.1 顔適用

顔適用機能は、DeepinMind シリーズ、DeepinView シリーズ、デュアルレンズカメラなどの一部のデバイスで、ライブビュー中にブラックリストに登録されている人物、VIP、または通常顧客の顔比較アラームを表示する機能を提供します。検知された顔画像がブラックリストまたは VIP 顔画像ライブラリの人物と一致した場合、セキュリティセンターは関係するアラームを受信して、適切な操作を迅速かつ効果的に実行できます。また、通常顧客を評価するのにも役立ちます。これは、病院、スーパーマーケット、ショッピングモールなどで広く使用されています。

16.1.1 顔画像ライブラリのリストタイプの設定

デバイスの各顔画像ライブラリのリストタイプを設定して、ライブビュー中に検知された人物がブラックリスト、VIP、または通常顧客に含まれているかどうかをソフトウェアが確認できるようにすることができます。

[AI ダッシュボード] → **[Face Application（顔適用）]** の順にクリックして、右上隅の をクリックして、デバイス上の各顔画像ライブラリのリストタイプを選択します。

ブラックリスト

アラームタイプを **[ブラックリスト]** に設定した場合、キャプチャ画像が顔画像ライブラリの画像と一致すると、AI ダッシュボードにブラックリストアラームが表示されます。

VIP

顔画像ライブラリを **VIP** に設定した場合、キャプチャ画像が顔画像ライブラリの画像と一致すると、AI ダッシュボードに VIP アラームが表示されます。

通常

ブラックリストと VIP のどちらにも属さない顔画像ライブラリは、**[通常]** に設定できます。AI ダッシュボードは、キャプチャされた顔画像が顔画像ライブラリ内の画像と一致した場合もアラームを表示しません。

注記

デバイスがこの機能をサポートしている必要があります。また、最初にデバイスで顔画像ライブラリを設定する必要があります。

16.1.2 AI 情報を表示するためのカメラの設定

表示するカメラまたはその他のカメラをカメラリストで指定して、ライブビュー中に AI 情報を表示できます。例えば、VIP 情報表示用カメラ（表示ウィンドウでライブビュー中ではないカメラ）を選択すると、このカメラはバックグラウンドで静的検知を実行し、VIP に関する AI 情報を表示します。

[AI ダッシュボード] → **[Face Application（顔適用）]** の順にクリックして、右上隅の  をクリックして、AI 情報をリアルタイムで表示するカメラを選択します。

各カメラで表示するアラームタイプ（[ブラックリストアラーム]、[VIP アラーム]、または [通常顧客アラーム]）を選択します。

ライブビューのすべてのカメラ

[ライブビューのすべてのカメラ] にチェックを入れると、表示ウィンドウでライブビュー中のカメラの AI 情報のみが表示されます。

カスタムカメラ

[カスタムカメラ] にチェックを入れて目的のカメラを選択すると、カメラがライブビュー中であるかどうかに関係なく、選択したカメラの AI 情報が表示されます。

16.1.3 AI 情報の表示

AI 情報を表示するカメラと顔画像ライブラリのリストタイプを設定した後に、AI 情報を表示できます。

[AI ダッシュボード] → **[Face Application（顔適用）]** の順にクリックして、カメラリストからカメラを選択してライブビューを開始し、AI 情報を表示します。

注記

使用するデバイスがこの機能に対応している必要があります。

カメラリスト

左側のパネルのカメラリストには、クライアントソフトウェアに追加したすべてのリソースが表示されます。適切なウィンドウ分割と目的のカメラを選択して、AI 情報を表示できます。

注記

同時にライブビューを行うチャンネル数は、クライアントを実行している PC のパフォーマンスによって制限されます。

カメラリストでカメラを右クリックして、メインストリームとサブストリームの間でストリームタイプを切り替えることができます。

ライブビューでのインテリジェント情報の表示

選択したカメラのリアルタイムビデオを表示できます。
ライブビューエリアのグローバルツールバーの をクリックして、ウィンドウを選択して目的のインテリジェント表示を有効にします。 例えば、すべてのライブビューウィンドウでラインクロス検知を有効にした場合、認識された対象がすべてのウィンドウの画像上で動的にマークされます。各ウィンドウの下部にある をクリックして、このウィンドウでカメラのインテリジェント表示を有効にすることもできます。

顔比較

[顔比較] スイッチをオンに設定すると、ブラックリストの人物、VIP、または通常顧客を検知したときに、対応する色の関連するアラーム通知が右側のパネルに表示されます。アラーム時間、カメラ、およびその他のアラームの詳細を表示できます。

過去のキャプチャ画像

ページの下部で、過去のキャプチャ画像を表示できます。

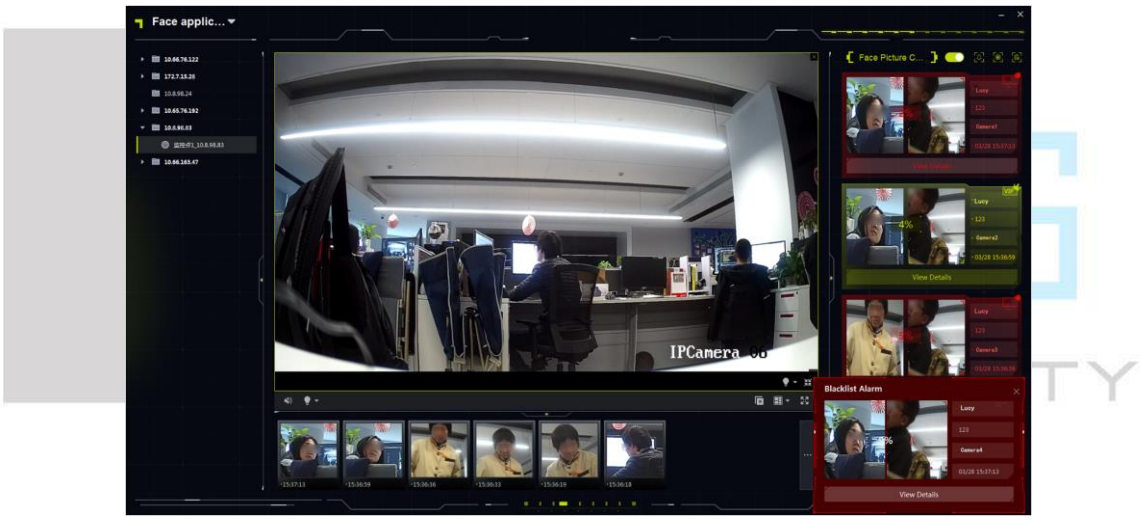

図 16-1 AI 情報の表示

アラームトリガーポップアップウィンドウの有効化

をクリックしてアラームトリガーポップアップウィンドウを有効にします。その後、ブラックリストアラームがトリガーされると、キャプチャ画像とアラーム詳細情報が含まれたウィンドウがポップアップ表示されます。

16.2 マルチ対象タイプ検知

マルチ対象タイプ検知とは、顔、人体、自動車、自動車以外の車両など、さまざまなタイプの検知対象を認識してキャプチャする機能のことです。デバイスが対象を検知した場合、ライブビュー、キャプチャ画像、および対象の特徴を表示できます。キャプチャされた顔

/ 人体画像と画像ライブラリ内の画像の類似度が高い場合、人物 / 車両の出現頻度が高い / 低い場合、または車両の外観がブラックリストに登録されている場合にアラームをトリガーできます。この機能は、交差点や駅などの人や車両が大量に出現する場所や強力なセキュリティが必要な場所でよく使用されます。

16.2.1 対象検知パラメータの設定

クライアントは、検知された対象とその詳細の表示レイアウトのカスタマイズ、検知された対象とともに表示する機能の選択、およびアラームが表示されるカメラの選択をサポートしています。

表示モードの設定

表示レイアウトをカスタマイズして、表示する情報を必要に応じて選択できます。

手順

1.**[AI ダッシュボード]** → **[マルチ対象タイプ検知]** の順にクリックします。
2.右上隅の ⚙ をクリックして、[設定] ウィンドウを開きます。
3.**[基本設定]** タブをクリックします。
4.ライブビューモードを選択します。
- 1 つのライブビューウィンドウを表示する場合は、**[単一チャンネル]** を選択します。
- 2 つのライブビューウィンドウを表示する場合は、**[デュアルチャンネル]** を選択します。

5.対応する位置で、表示する情報にチェックを入れます。
チェックを入れた情報が次のウィンドウに表示されます。
6.オプション: **[画像を保存]** を有効にして、すべてのキャプチャ画像が指定したフォルダに保存されるようにします。その後、保存パスをクリックして変更します。
7.**[保存]** をクリックして設定を保存します。

キャプチャパラメータの設定

キャプチャ画像で、デバイスはキャプチャされた対象の特徴を分析します。必要に応じて、表示する特徴を選択できます。例えば、顔検知の場合は、年齢、性別、メガネ着用などの特徴を選択して、画像とともに表示できます。

手順

1.**[AI ダッシュボード]** → **[マルチ対象タイプ検知]** の順にクリックします。
2.右上隅の ⚙ をクリックして、[設定] ウィンドウを開きます。
3.**[キャプチャパラメータ]** タブをクリックします。
4.**[特徴を表示]** を有効にします。

5.**[Features in Face Detection（顔検知での特徴）]** / **[Features in Motor Vehicle Detection（自動車検知での特徴）]** / **[Features in Human Body Detection（人体検知での特徴）]** / **[Features in Non Motor Vehicle Detection（自動車以外の車両検知での特徴）]** を有効にして、対応する特徴にチェックを入れます。

注記

各機能の特徴は 6 つまで選択できます。

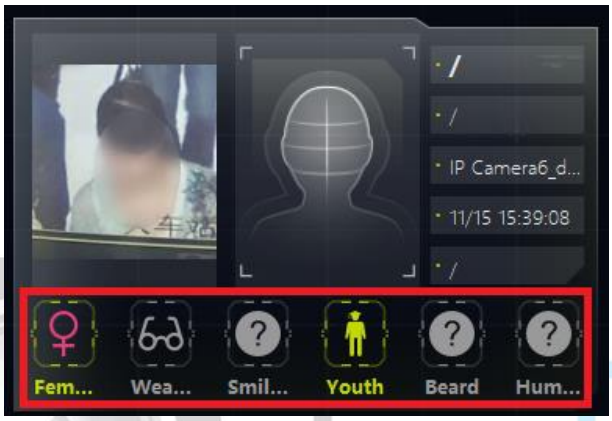

図 16-2 表示された特徴

6.**[保存]** をクリックして設定を保存します。

アラームを受信するカメラの設定

検知アラームが設定されたカメラの場合、アラームと詳細なアラーム情報を右側のパネルに表示するカメラを選択できます。

始める前に

アラームを表示するように選択したカメラでアラームが設定されていることを確認してください。

手順

1.**[AI ダッシュボード]** → **[マルチ対象タイプ検知]** の順にクリックします。
2.右上隅の ⚙ をクリックして、[設定] ウィンドウを開きます。
3.**[Receiving Alarm Settings（アラーム受信設定）]** タブをクリックします。
4.右側のパネルにアラームを表示するカメラにチェックを入れます。

注記

チェックを入れたカメラのアラームが、詳細なアラーム情報とともに右側のパネルに表示されます。

5.**[保存]** をクリックして設定を保存します。

16.2.2 マルチ対象タイプ検知の表示

マルチ対象タイプ検知は、検知した情報（キャプチャカメラのライブビュー、キャプチャ画像、対象の詳細、対象の数、アラームの詳細など）の表示をサポートしています。検知した情報を表示するには、対応するパラメータを設定する必要があります。

注記

デバイスがこの機能をサポートしている必要があります。

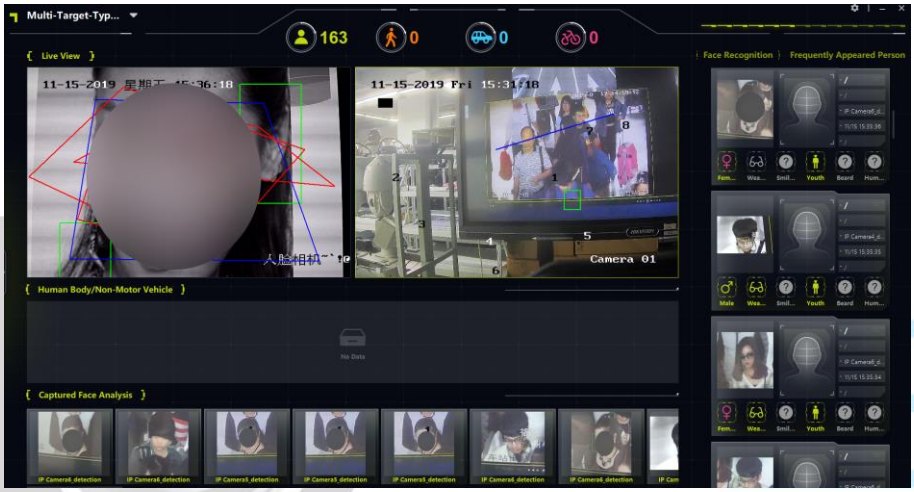

図 16-3 マルチ対象検知表示

ライブビュー

シングルチャンネルモードまたはデュアルチャンネルモードでのライブビューの表示をサポートしています。重要な事柄が発生した場合は、ライブビューウィンドウのツールバーを使用して、画像をキャプチャしたり、すばやく録画を開始できます。また、パノラマ詳細ビューを右クリックして、PTZ 制御または 3D ポジショニングを実行することもできます。

人体 / 自動車以外の車両

キャプチャされた人体 / 自動車以外の車両画像は、対象上に強調表示用のボックスが表示された状態でこのエリアに表示されます。また、キャプチャされた対象の特徴が画像とともに表示されます。

キャプチャされた顔分析

キャプチャされた顔画像が、顔の特徴（年齢層、性別、メガネ着用など）とともに表示されます。

自動車

キャプチャされた自動車の画像が、車両の特徴（ナンバープレート番号、車両の色、車両タイプなど）とともに表示されます。

顔認識 / 頻出人物 / 低出現頻度人物

顔の比較結果、不明人物のキャプチャされた顔画像、人体とキャプチャされた顔画像、および出現頻度が表示されます。

- キャプチャされた顔画像と顔画像ライブラリ内の類似した顔画像が一致した場合は、それらが表示されます。
- 顔画像ライブラリ内の顔画像と一致しなかったキャプチャされた顔画像が表示されます。

注記

不明人物認識をサポートしているデバイスの場合、キャプチャされた顔は、顔画像ライブラリ内の画像と比較されます。人物の顔が顔画像ライブラリ内の顔と一致しなかった場合、その人物は不明人物として認識されます。

- キャプチャされた人体画像の場合は、その人物の顔画像も表示されます。
- 出現頻度: 出現回数がしきい値を超えた人物が頻出人物として表示され、出現回数がしきい値未満の人物が低出現頻度人物として表示されます。

注記

最後にキャプチャされた顔画像、出現回数、アラーム時間などの個人情報は、アラーム情報をクリックすると表示されます。検知された人物を顔画像ライブラリに追加できます。

16.3 リンクキャプチャアラーム

この機能により、デバイスの 2 つの異なるチャンネル（1 つの固定チャンネルと 1 つの PTZ チャンネル）を同時に表示できます。このため、アラームがトリガーされたときに、パノラマ画像とキャプチャされた詳細を同時に表示できます。

注記

使用するデバイスがこの機能をサポートしている必要があります。

16.3.1 基本パラメータの設定

キャプチャ保存機能は、手動で有効または無効にすることができます。また、キャプチャされた画像の保存パスを設定して、キャプチャされた画像を PC で表示できるようにすることもできます。

手順

1.[AIダッシュボード] モジュールを表示します。
2.**[Linked Capture Alarm（リンクキャプチャアラーム）]** を選択して、[Linked Capture Alarm（リンクキャプチャアラーム）] ウィンドウを開きます。
3. をクリックして設定ウィンドウを開きます。
表示された内容の概要が表示されます。
4.**[画像を保存]** をオンにして、画像保存機能を有効にします。
5.**[保存パス]** をクリックして、キャプチャされた画像の保存パスを選択します。
6.**[保存]** をクリックして設定を保存します。
イベントとアラームがトリガーされたときにキャプチャされた画像が設定されたパスに保存されます。

16.3.2 ライブビューとアラームの表示

固定カメラがアラームをトリガーすると、固定カメラはアラームに関連するパノラマ画像をキャプチャし、パノラマにリンクされたアラームウィンドウに画像が表示されます。リンクされた PTZ カメラはアラームに関する詳細とともに画像をキャプチャし、リンクされたチャンネルアラームウィンドウに画像が表示されます。このようにして、パノラマ画像と詳細が同時に表示されます。
一般的に、パノラマチャンネルライブビューウィンドウは固定カメラのライブビューを表示するのに使用され、リンクチャンネルライブビューウィンドウは固定カメラに接続された PTZ カメラのライブビューを表示するのに使用されます。

1. **AI ダッシュボード**を表示し、**[Linked Capture Alarm（リンクキャプチャアラーム）]** を選択して [Linked Capture Alarm（リンクキャプチャアラーム）] ウィンドウを開きます。
2. をクリックしてデバイスリストを展開します。
3. ウィンドウを選択し、カメラをダブルクリックしてライブビューを開始するか、デバイスリストからウィンドウにカメラをドラッグするか、カメラ名の上にカーソルを合わせて をクリックします。

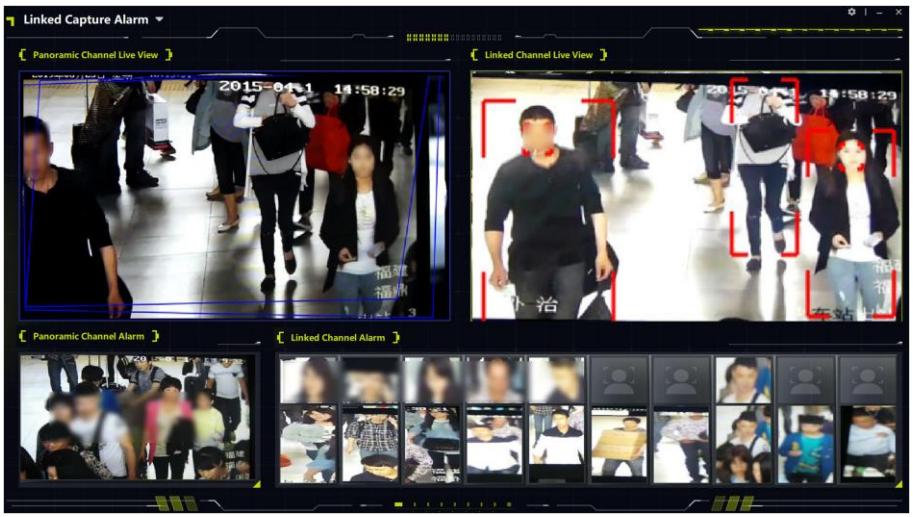

図 **16-4** ライブビューとアラームの表示

4.

第 17 章 セキュリティコントロールパネル

セキュリティコントロールパネルは、事前定義された仮想領域に入る人物や車両などを検知し、イベントをトリガーし、イベント情報（イベントの場所など）をセキュリティ担当者に報告します。[イベントセンター] モジュールは、クライアントを介して、イベント管理とパーティションおよびゾーンのリモート制御機能を提供します。イベント管理ページでクライアントアクションを設定した後、イベント発生時にクライアントで通知を受け取れるようになります。また、セキュリティコントロールパネルを手動で操作できない場合でも、クライアントによってパーティションとゾーンを管理できます。

注記

イベント設定、セキュリティコントロールパネルのリモート制御、およびデバイスの警戒開始と警戒解除には権限が必要です。ユーザー権限の設定方法の詳細については、「*ユーザーの追加*」をご覧ください。

17.1 フローチャート

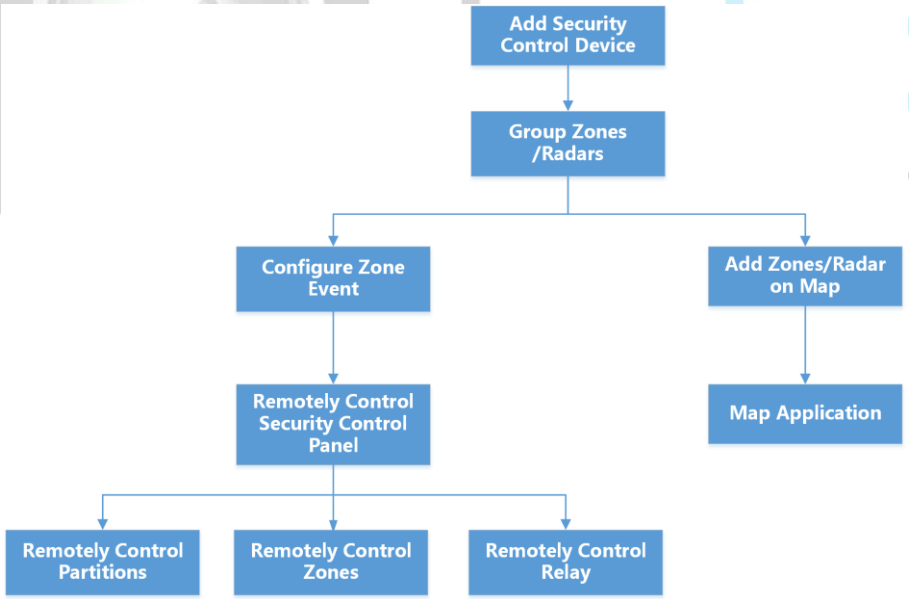

図 17-1 セキュリティコントロールパネルのフローチャート

- **セキュリティコントロールデバイスの追加:** クライアントにセキュリティ制御デバイスを追加できます。詳細については、「*デバイスの追加*」をご覧ください。
- **ゾーン / レーダーのグループ化:** 追加したゾーン / レーダーをグループ化して、管理しやすくすることができます。詳細については、「*グループ管理*」をご覧ください。
- **ゾーンイベントの設定:** クライアントでゾーンイベントのリンク操作を設定すると、イ

ベントがトリガーされたときに通知されます。詳細については、「*ゾーンイベントのクライアントリンケージの設定*」をご覧ください。

- **マップへのゾーン / レーダーの追加:** ゾーン / レーダーをマップにホットスポットとして追加して、クライアントでアラームがトリガーされたときにゾーンをすばやく見つけることができます。詳細については、「*ホットスポットの管理*」をご覧ください。
- **パーティションのリモート制御:** クライアント上のパーティション（不在警戒、滞在警戒、即時警戒、警戒解除など）をリモート制御できます。詳細については、「*パーティションのリモート制御*」をご覧ください。
- **ゾーンのリモート制御:** バイパスおよびバイパス復元など、ゾーンをリモート制御できます。詳細については、「*ゾーンのリモート制御*」をご覧ください。
- **中継のリモート制御:** 中継のオン / オフ状態の変更や、中継のリンクされたイベントの表示など、クライアント上の中継をリモートで制御できます。詳細については、「*中継のリモート制御*」をご覧ください。

17.2 ゾーンイベントのクライアントリンクの設定

ゾーンから遠く離れている場合も、クライアントでゾーンイベントのリンク操作を設定することで、ゾーンの状況とイベントの緊急度を把握できます。イベントに即応できるように、イベント発生時にクライアント側で通知を受け取ります。複数のゾーンのクライアントアクションを一度に一括で設定することもできます。

始める前に

- セキュリティコントロールパネルを追加したことを確認してください。
- ゾーンが事前に定義されていることを確認してください。
- イベントが事前に設定されていることを確認してください。

手順

1.**[イベント管理]** → **[セキュリティコントロールイベント]** の順にクリックします。
2.セキュリティコントロールパネルのゾーンリストを展開し、リストからゾーンを選択します。
3.1 つまたは複数のイベントにチェックを入れます。
4.**[リンクを編集]** をクリックして、クライアントアクションを設定します。

音声による警告

イベントがトリガーされたときに、クライアントソフトウェアが音声による警告を発します。警告に使用するアラーム音を選択できます。

注記

[追加] をクリックしてアラーム音の名前を入力し、PC で音を選択します。詳細については、「*アラーム音の設定*」をご覧ください。

電子メールを送信

アラーム情報の電子メールを 1 つまたは複数の宛先に送信します。
電子メールのパラメータ設定の詳細については、「*電子メールのパラメータ設定*」をご覧ください。

ポップアップウィンドウ

イベントがトリガーされたときに、ソフトウェアクライアント上にイベント関連の情報（イベントの詳細、リンクされたカメラのキャプチャ画像、プロセスレコード、プロセスフィールドなど）を示すポップアップウィンドウが表示されます。

Display on Map（マップ上に表示）

イベントソースをマップ上にホットスポットとして追加すると、イベントがトリガーされたときにホットスポットが赤の数字（イベント数を示し、最大数は 10）とともに表示されます。これにより、セキュリティ担当者はイベントの場所を容易に確認することができます。
ホットスポットをクリックして、イベントの詳細と、リンクされたカメラのライブビデオを表示することもできます。

リンク済みカメラ

ゾーンイベントがトリガーされたときに画像をキャプチャするには、選択したカメラをリンクします。
ドロップダウンリストでカメラを選択します。

注記

最大 4 台のカメラを 1 つのゾーンイベントのリンクされたカメラとして選択できます。

5. オプション: **[優先度の編集]** をクリックして、イベントの優先度をカテゴリなし / 低 / 中 / 高に設定します。
6. オプション: **[コピー先...]** をクリックして、イベント設定（イベントの優先度、トリガーされたクライアントアクション、およびイベントの有効化 / 無効化など）を他のゾーンにコピーします。
7. ゾーンイベントのクライアントアクションを有効または無効にします。
   – すべてのゾーンイベントのクライアントアクションを有効または無効にするには、**[すべて有効化]** または **[すべて無効化]** をクリックします。
   – 1 つのゾーンイベントのクライアントアクションを有効または無効にするには、**[有効]** をオン / オフに切り替えます。

クライアントアクションの有効化

クライアントアクションが有効になっている場合、クライアントがゾーンイベントを受け取ったときにクライアントアクションがトリガーされます。

クライアントアクションの無効化

クライアントアクションが無効になっている場合、クライアントアクションは機能せ

ず、クライアントがゾーンイベントを受け取ったときに操作はトリガーされません。
8.**[保存]** をクリックします。

17.3 セキュリティコントロールパネルのリモート制御

セキュリティコントロールパネルをクライアントに追加した後に、クライアントソフトウェアを使用して、セキュリティコントロールパネルのパーティション、ゾーン、および中継をリモート制御できます。例えば、パーティションとゾーンの両方に対して、警戒開始、警戒解除、バイパス、グループバイパスなどを行うことができます。中継を有効または無効にすることもできます。

注記

- 表示されるインタフェースは、追加したセキュリティコントロールパネルのタイプによって異なります。
- デフォルトでは axiom ハブデバイスは HTTP ポートを使用し、プライベートポートはサポートしていません。

17.3.1 パーティションのリモート制御

クライアントを使用して、セキュリティコントロールパネルのパーティションでリモート操作（不在警戒、滞在警戒、即時警戒、警戒解除、アラーム解除、グループバイパス、グループバイパス復元など）を実行できます。

手順

注記

- サポートされている機能は、追加したデバイスによって異なります。
- パーティションのゾーンが機能しない場合は、パーティションを警戒開始 / 警戒解除する前にゾーンをバイパスして、ゾーンが機能するようになったらバイパスを復元してください。

1.**[イベントセンター]** → **[セキュリティコントロールパネル]** の順にクリックします。
2.セキュリティコントロールパネルを選択し、**[パーティション]** をクリックします。
パーティションの名前、状態、警戒状態、およびリンクされたゾーンがリストに表示されます。
3.1 つまたは複数のパーティションを選択して、次のボタンをクリックします。

不在警戒

監視領域に誰もいない場合に作動する警戒モードです。不在警戒が有効になっている場合、パーティションのすべてのゾーンが正しく機能します。

滞在警戒

監視領域に人物が滞在しているときに作動する警戒モードです。滞在警戒が有効になっている場合、領域内のゾーンで警戒が開始されます。領域外のゾーンはバイパスされ、イベントをトリガーさせることなくゾーンに入ることができます。

即時警戒

パーティションで警戒を開始した後、イベントがトリガーされたときにそのゾーンの警戒が即時開始されます。

警戒解除

クリックすると、パーティション内のすべてのゾーン（24 時間ゾーンを除く）が機能しなくなるため、警戒解除ゾーンでイベントはトリガーされなくなります。

注記

24 時間ゾーン（24 時間アナウンスゾーン、24 時間サイレントアラームゾーンなど）は、パーティションを警戒解除してもイベントを検知してアラームをトリガーします。

アラームを消去

アラームデバイスのアラームを停止します。

グループバイパス

グループバイパスを復元するまで、バイパスされたゾーンでイベントがトリガーされないように、1 つまたは複数のパーティション内のすべてのゾーンをバイパスします。

注記

パーティションをバイパスする前に、パーティションを警戒解除する必要があります。

グループバイパス復元

グループバイパスを復元して、パーティション内のすべてのゾーンが機能するようにします。これにより、グループの警戒を開始できます。

17.3.2 ゾーンのリモート制御

クライアントを使用して、バイパスおよびバイパス復元など、セキュリティコントロールパネルのゾーンをリモート制御できます。

手順

1. **[イベントセンター]** → **[セキュリティコントロールパネル]** の順にクリックします。
2. セキュリティコントロールパネルを選択し、**[パーティション]** をクリックします。
   パーティションの名前、状態、警戒状態、およびリンクされたゾーンがリストに表示されます。

3. をクリックして、[ゾーン操作] パネルを開きます。
パーティションにリンクされているゾーン、ゾーン番号、ゾーン名、ゾーンの状態、ゾーンアラーム状態、バッテリが表示されます。

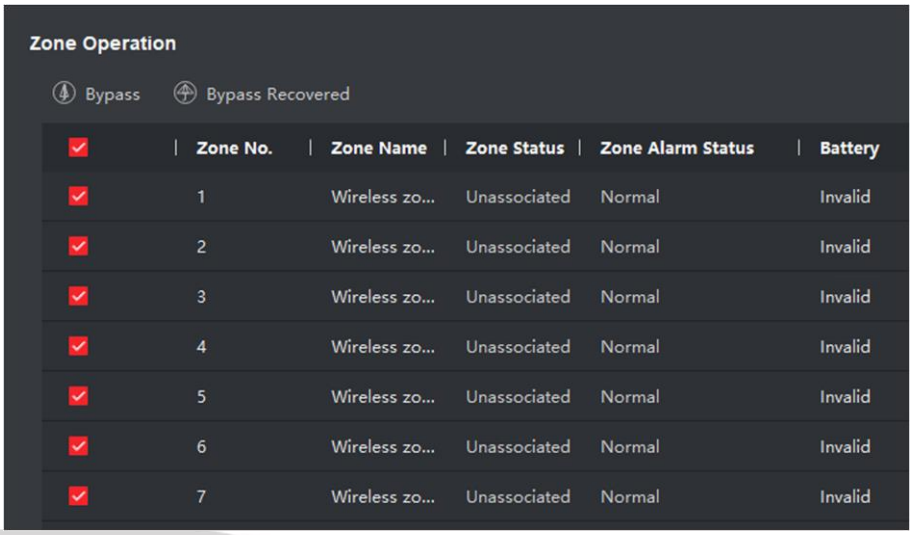

図 17-2 ゾーン操作

ゾーンの状態

ゾーンの状態は、未関連、警戒開始済み、警戒解除、障害、シールド、妨害防止などになります。

バッテリ

ゾーンの検知器の電源です。

4. リストで 1 つまたは複数のゾーンにチェックを入れて、次のボタンをクリックします。

バイパス

ゾーンをバイパスした場合、そのゾーン内でイベントはトリガーされず、そのゾーンを警戒開始または警戒解除できなくなります。他のゾーンは警戒開始または警戒解除できます。

注記

ゾーンをバイパスする前に、そのゾーンを警戒解除する必要があります。

バイパス復元

ゾーンのバイパスを復元した後に、そのゾーンの警戒を開始できます。

17.3.3 中継のリモート制御

クライアントを使用して、中継のオン / オフ状態をリモートで変更したり、中継のリンク

されたイベントを表示できます。

手順

1.**[イベントセンター]** → **[セキュリティコントロールパネル]** の順にクリックします。
2.セキュリティコントロールパネルを選択して、**[中継]** をクリックします。
中継の名前、状態、およびリンクされたイベントが表示されます。
3.1 つまたは複数の中継にチェックを入れて、**[開く]** または **[閉じる]** をクリックします。

注記

Axiom ハブの場合は、[デバイス管理] モジュールで **[中継関連イベント]** を **[手動制御]** に設定する必要があります。

第18章 人物管理

個人情報を追加することで、アクセス制御、ビデオインターコム、時間と出勤などの追加操作を実行できます。カードの一括発行や個人情報の一括インポート / エクスポートなど、追加した個人に対する管理が可能になります。

18.1 組織の追加

組織を追加し、その組織に個人情報をインポートすることで、個人に対する管理が容易になります。また、その組織に下部組織も追加できます。

手順

1.**[人物]** モジュールを表示します。
2.左列の親組織を選択して左上隅の **[追加]** をクリックし、組織を追加します。
3.追加する組織の名前を作成します。

注記
最大 10 階層まで組織を追加できます。

4.オプション: 以下の操作を実行します。

組織を編集	追加した組織にカーソルを合わせ、をクリックすると名前を編集できます。
組織の削除	追加した組織にカーソルを合わせ、をクリックすると名前を削除できます。

注記
- 組織を削除すると、その下部組織も削除されます。
- 組織の下に誰も追加されていないことを確認してください。追加されている場合は、その組織を削除できません。

下部組織の人物を表示	**[Show Persons in Sub Organization（下部組織の人物を表示）]** にチェックを入れて組織を選択し、下部組織に属する人物を表示します。

18.2 1 人の人物の追加

人物はクライアントソフトウェアに 1 人ずつ追加できます。人物情報には、基本情報、詳細情報、プロファイル、入退室管理情報、認証情報、カスタム情報などが含まれます。

18.2.1 基本情報の設定

人物をクライアントソフトウェアに 1 人ずつ追加して、名前、性別、電話番号などの基本情報を設定できます。

手順

1.**[人物]** モジュールを表示します。
2.組織リスト内の組織を選択して人物を追加します。
3.**[追加]** をクリックして人物の追加ウィンドウを開きます。
人物 ID が自動生成されます。
4.個人名、性別、電話番号、電子メールアドレスなどの基本情報を入力します。
5.オプション: その人物に対する有効期間を設定します。有効期間を過ぎると、その人物の認証情報とアクセス制御設定は無効になり、ドア / フロアの入室許可が下りなくなります。

例

例えば、その人物が訪問者の場合、有効期間は短く、一時的なものになります。
6.内容を確認して人物を追加します。
– **[追加]** をクリックすると、その人物を追加して [人物の追加] ウィンドウが閉じます。
– **[Add and New（追加および新規）]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。

18.2.2 個人にカードを発行する

人物を追加するときに、ドアにアクセスするための認証用のカードを発行できます。1 人の人物にカードを発行する前に、カード発行モードを設定してカード番号を読み取る必要があります。カード番号を手動で入力する場合を除き、クライアントはカード番号読み取りモードとして、ローカルモード（カード登録ステーションを使用）とリモートモード（入退室管理デバイスのカードリーダーを使用）の 2 つのモードも提供しています。

注記

1 人にカードを最大 5 枚まで発行できます。

カード番号の入力によるカードの発行

カード番号読み取りデバイス（カード登録ステーション / カードリーダー）がない場合は、

カード番号を手動で入力してカードを発行できます。

手順

1.**[人物]** モジュールを表示します。
2.組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックして [関係者を追加] パネルを表示します。

注記

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「*基本情報の設定*」をご覧ください。

3.**[認証情報]** → **[カード]** エリアの順に進み、**[+]** をクリックします。

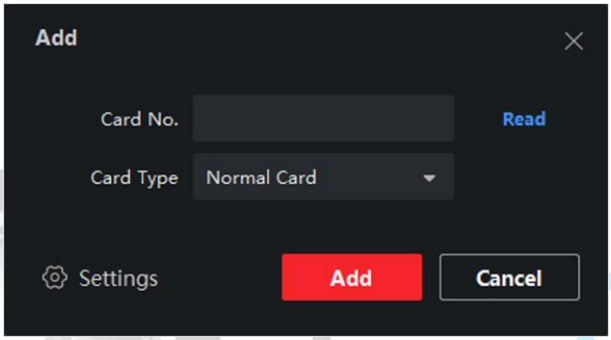

図 18-1 カードの追加ページ

4.[追加] ページで、カード番号を手動で入力します。
5.**[追加]** をクリックします。
その人物にカードが発行されます。

ローカルモードでのカードの発行

カード登録ステーションが利用可能な場合は、ローカルモードでカードを発行できます。カード番号を読み取るには、クライアントを実行中の PC に USB インタフェースまたは COM 経由でカード登録ステーションを接続して、カード登録ステーションにカードを置きます。

手順

1.**[人物]** モジュールを表示します。
2.組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックして [関係者を追加] パネルを表示します。

注記

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「*基本情報の設定*」をご覧ください。

3.**[認証情報]** → **[カード]** エリアの順に進み、**[+]** をクリックします。
4.**[設定]** をクリックして、[設定] ページを表示します。
5.カード発行モードとして **[ローカル]** を選択します。

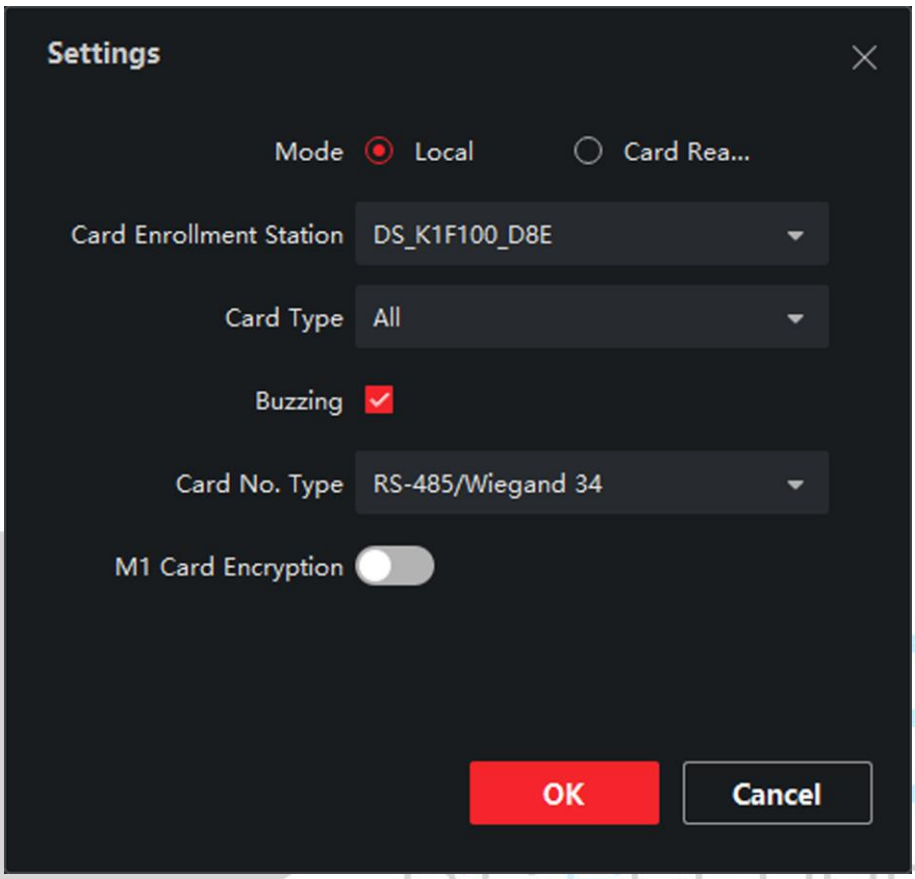

図 18-2 ローカルモードでのカードの発行

6.その他の関連パラメータを設定します。

カード登録ステーション

接続したカード登録ステーションのモデルを選択します。

注記

現在対応しているカード登録ステーションのモデルは、DS-K1F100-D8、DS-K1F100-M、DS-K1F100-D8E、DS-K1F180-D8E などです。

カードタイプ

使用モデルが DS-K1F100-D8E または DS-K1F180-D8E の場合に限り、このフィールドを使用できます。実際のカードタイプに応じて、EM カードまたは Mifare カードを選択します。

ブザー

カード番号の読み取りに成功した時に、ブザーを鳴らすかどうかを選択します。

カード番号タイプ

実際の使用状況に応じて、カード番号のタイプを選択します。

M1 カード暗号化

使用モデルが DS-K1F100-D8、DS-K1F100-D8E または DS-K1F180-D8E の場合に限り、このフィールドを使用できます。使用するカードが M1 カードの場合は、M1 カード暗号化機能を有効にして、カードのセクターを選択して暗号化できます。

7.**[OK]** をクリックして、操作を確定します。

8.カード登録ステーションにカードを置いて、**[読み取り]** をクリックしてカード番号を読み取ります。

カード番号は [カード番号] フィールドに自動的に表示されます。

9.**[追加]** をクリックします。

その人物にカードが発行されます。

リモートモードでのカードの発行

ローカルモードでカードを発行する場合を除き、追加した入退室管理デバイスのカードリーダーでカードをスワイプしてカード番号を読み取ることもできます。この方法は、クライアントとカードを発行する必要がある人が同じ場所にいない場合に使用できます。例えば、クライアントを介してリモートモードで支社の従業員のカードを発行できます。

手順

1.**[人物]** モジュールを表示します。

2.組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックして [関係者を追加] パネルを表示します。

注記

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「*基本情報の設定*」をご覧ください。

3.**[認証情報]** → **[カード]** エリアの順に進み、**[+]** をクリックします。

4.**[設定]** をクリックして、[設定] ページを表示します。

5.カード発行モードとして **[カードリーダー]** を選択します。

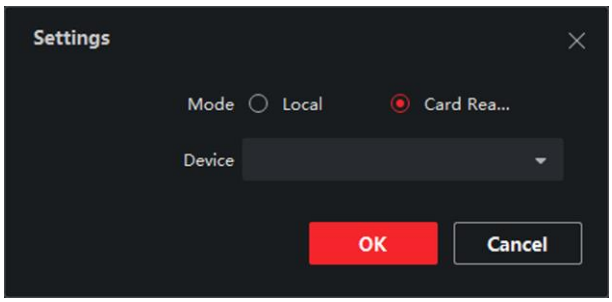

図 18-3 リモートモードでのカードの発行

6.クライアントに追加した入退室管理デバイスを選択します。
7.**[OK]** をクリックして、操作を確定します。
8.カードリーダーにカードを置き、**[読み取り]** をクリックしてカード番号を読み取ります。
カード番号は [カード番号] フィールドに自動的に表示されます。
9.**[追加]** をクリックします。
その人物にカードが発行されます。

18.2.3 ローカル PC から顔写真をアップロードする

人物を追加する際に、ローカル PC に保存した顔写真を人物プロフィールとしてクライアントへアップロードできます。

手順

1.**[人物]** モジュールを表示します。
2.組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。

注記

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「*基本情報の設定*」をご覧ください。

3.[基本情報] パネルで **[顔の追加]** をクリックします。
4.**[アップロード]** を選択します。
5.クライアントを実行中の PC から写真を選択します。

注記

写真は JPG または JPEG 形式で、サイズは 200KB 未満にしてください。

6.オプション: **[デバイスによる認証]** を有効化すると、クライアントで管理している顔認証デバイスが写真内の顔を認識できるかどうかを確認できます。
7.内容を確認して人物を追加します。
- **[追加]** をクリックすると、その人物を追加して [人物の追加] ウィンドウが閉じます。
- **[Add and New（追加および新規）]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。

18.2.4 クライアント経由の写真撮影

人物を追加する際に、クライアントを実行中の PC に搭載したウェブカムでその人物の写真を撮影し、その写真を人物プロフィールとして設定できます。

始める前に

入退室管理デバイスを 1 つ以上追加し、クライアント側で管理する顔認証デバイスで写真内の顔を認識できるか確認してください。

手順

1.**[人物]** モジュールを表示します。
2.組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。

注記

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「*基本情報の設定*」をご覧ください。

3.[基本情報] パネルで **[顔の追加]** をクリックします。
4.**[写真撮影]** を選択します。
5.クライアントを実行中の PC に顔スキャナーを接続します。
6.オプション: **[デバイスによる認証]** を有効化すると、クライアントで管理している顔認証デバイスが写真内の顔を認識できるかどうかを確認できます。
7.写真を撮影します。
1）PC のウェブカムを真正面から見て、自身の顔がキャプチャウィンドウの中央に位置していることを確認します。
2）をクリックして顔写真を撮影します。
3）オプション: をクリックすると、再度撮影できます。
4）**[OK]** をクリックして撮影した写真を保存します。
8.内容を確認して人物を追加します。
– **[追加]** をクリックすると、その人物を追加して [人物の追加] ウィンドウが閉じます。
– **[Add and New（追加および新規）]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。

18.2.5 入退室管理デバイスで顔画像を取り込む

人物を追加する際に、クライアントに追加した入退室管理デバイスを使用して顔画像を取り込むことができます。その場合、クライアントが顔認証機能に対応している必要があります。

手順

1.**[人物]** モジュールを表示します。
2.組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。

注記

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「*基本情報の設定*」をご覧ください。

3.[基本情報] パネルで **[顔の追加]** をクリックします。
4.**[Remote Collection（リモート取り込み）]** を選択します。

5.ドロップダウンリストの中から、顔認証機能に対応する入退室管理デバイスを選択します。
6.顔画像を取り込みます。
1）選択した入退室管理デバイスのカメラを真正面から見て、自身の顔がキャプチャウィンドウの中央に位置していることを確認します。
2）をクリックして顔写真を撮影します。
3）**[OK]** をクリックして撮影した写真を保存します。
7.内容を確認して人物を追加します。
– **[追加]** をクリックすると、その人物を追加して [人物の追加] ウィンドウが閉じます。
– **[Add and New（追加および新規）]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。

18.2.6 クライアントで指紋を取り込む

クライアントを実行中の PC に直接接続した指紋レコーダーを使用することで、指紋をローカルで取り込むことができます。取り込んだ指紋は、ドアへのアクセスを許可するための個人認証用の認証情報として使用できます。

始める前に

クライアントを実行中の PC に指紋レコーダーを接続します。

手順

1.**[人物]** モジュールを表示します。
2.組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。

注記

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「*基本情報の設定*」をご覧ください。

3.**[認証情報]** → **[指紋]** パネルの順に進み、**[+]** をクリックします。
4.ポップアップウィンドウで、取り込みモードに **[ローカル]** を選択します。
5.接続した指紋レコーダーのモデルを選択します。

注記

指紋レコーダーが DS-K1F800-F の場合、**[設定]** をクリックして、指紋レコーダーを接続中の COM を選択できます。

6.指紋を取り込みます。
1）**[開始]** をクリックします。
2）指紋レコーダー上に指を置き、指紋を取り込ませます。
3）**[追加]** をクリックし、取り込んだ指紋を保存します。
7.内容を確認して人物を追加します。

– **[追加]** をクリックすると、その人物を追加して [人物の追加] ウィンドウが閉じます。
– **[Add and New（追加および新規）]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。

18.2.7 入退室管理デバイスで指紋を取り込む

人物を追加する際に、入退室管理デバイスの指紋モジュールを使用して指紋情報を取り込むことができます。取り込んだ指紋は、ドアへのアクセスを許可するための個人認証用の認証情報として使用できます。

始める前に

お使いの入退室管理デバイスが指紋取り込み機能に対応していることを確認してください。

手順

1.**[人物]** モジュールを表示します。
2.組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。

注記

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「*基本情報の設定*」をご覧ください。

3.**[認証情報]** → **[指紋]** パネルの順に進み、**[+]** をクリックします。
4.ポップアップウィンドウで、取り込みモードに **[リモート]** を選択します。
5.ドロップダウンリストの中から、指紋認証機能が使用できる入退室管理デバイスを選択します。
6.指紋を取り込みます。
1）**[開始]** をクリックします。
2）選択した入退室管理デバイスの指紋レコーダーの上に指を置き、指紋を取り込ませます。
3）**[追加]** をクリックし、取り込んだ指紋を保存します。
7.内容を確認して人物を追加します。
– **[追加]** をクリックすると、その人物を追加して [人物の追加] ウィンドウが閉じます。
– **[Add and New（追加および新規）]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。

18.2.8 入退室管理情報の設定

人物を追加する際に、訪問者、ブラックリスト内の人物、特別の権限を有するスーパーユーザーなど、その人物の入退室管理プロパティを設定できます。

手順

1.**[人物]** モジュールを表示します。

2.組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。
3.**[入退室管理]** エリアでその人物の入退室管理プロパティを設定します。

アクセスグループ

人物の 1 つまたは複数のアクセスグループを選択して、選択したアクセスポイントへのアクセス認証をその人物に与えることができます。詳細については、「*アクセスグループを設定してアクセス認証を人物に割り当てる*」をご覧ください。

パスワード

アクセスするときには、カードをスワイプした後または指紋認証した後にパスワードを入力する必要があります。パスワードは単独で使用することはできません。また、4～8 桁でなければなりません。

スーパーユーザー

スーパーユーザーとして設定された人物は、すべてのドア / フロアにアクセスできるだけでなく、閉鎖保持にかかわる制約、すべてのアンチパスバックルール、最初の人物としての認証の適用からも除外されます。

ドア開放時間の延長

ドアにアクセスする時に、ドアの開放時間を延長してドアを通過できるようにします。スムーズに移動することが難しい人物には、この機能を使用してください。
ドア開放時間の設定の詳細については、「*ドア／エレベータのパラメータ設定*」をご覧ください。

ブラックリストに追加

ブラックリストに追加された人物がドア / フロアへのアクセスを試みるとイベントがトリガーされ、クライアントにその情報が送信されてセキュリティ担当者に通知が届きます。

訪問者としてマーキング

訪問者を認証する場合、カードと指紋によるアクセスなどの最大認証回数を設定することで、その訪問者のアクセス回数を制限します。

注記

最大認証回数は 1～100 回の範囲で設定できます。

デバイスオペレーター

デバイスオペレーターの役割を担う人物には、入退室管理デバイスの操作権限が付与されています。

注記

[スーパーユーザー]、[ドア開放時間の延長]、[ブラックリストに追加]、[訪問者としてマーキング] 機能は同時には有効化できません。例えば、ある人物をスーパーユーザーに設定した場合、その人物に対してドア開放時間の延長機能やブラックリスト機能、訪問者機能は設定できません。

4.内容を確認して人物を追加します。
- **[追加]** をクリックすると、その人物を追加して [人物の追加] ウィンドウが閉じます。
- **[Add and New（追加および新規）]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。

18.2.9 個人情報のカスタマイズ

実際の使用状況に応じて、クライアントに事前定義されていない人物プロパティをカスタマイズできます（例: 出身地）。カスタマイズ後に人物を追加すると、そのカスタマイズ情報を入力することで個人情報の登録が完成します。

手順

1.**[人物]** モジュールを表示します。
2.カスタム情報のフィールドを設定します。
1）**[カスタムプロパティ]** をクリックします。
2）**[追加]** をクリックして新規プロパティを追加します。
3）プロパティ名を入力します。
4）**[OK]** をクリックします。
3.人物を追加する際に、カスタム情報を設定します。
1）組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。

注記

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「*基本情報の設定*」をご覧ください。

2）**[カスタム情報]** パネル内でその人物の情報を入力します。
3）**[追加]** をクリックすると、その人物を追加して [人物の追加] ウィンドウが閉じます。または **[Add and New（追加および新規）]** をクリックすると、その人物を追加した後で、引き続き別の人物を追加できます。

18.2.10 居住者情報の設定

登録する人物が居住者の場合、ビデオインターコムを使用するには、その人物の部屋番号を設定してインドアステーションに関連付ける必要があります。関連付けを行った後は、インドアステーションでこの人物を呼び出し、ビデオインターコムで話すことができます。

手順

1.**[人物]** モジュールを表示します。
2.組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。

注記

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「*基本情報の設定*」をご覧ください。

3.**[居住者情報]** パネルで、インドアステーションを選択して人物に関連付けます。

注記

[アナログインドアステーション] を選択した場合には **[ドアステーション]** フィールドが表示され、アナログのインドアステーションで通信するドアステーションの選択が必要になります。

4.その人物のフロア番号と部屋番号を入力します。
5.内容を確認して人物を追加します。
- **[追加]** をクリックすると、その人物を追加して [人物の追加] ウィンドウが閉じます。
- **[Add and New（追加および新規）]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。

18.2.11 追加情報の設定

人物を追加する際に、実際の使用状況に応じて、その人物の ID タイプ、ID 番号、国籍などの追加情報を設定できます。

手順

1.**[人物]** モジュールを表示します。
2.組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。

注記

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「*基本情報の設定*」をご覧ください。

3.**[追加情報]** パネル内で、実際の使用状況に応じて、その人物の ID タイプ、ID 番号、役職などの追加情報を入力します。

4.内容を確認して人物を追加します。
- **[追加]** をクリックすると、その人物を追加して [人物の追加] ウィンドウが閉じます。
- **[Add and New（追加および新規）]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。

18.3 ID 情報のインポートとエクスポート

複数の人物の情報と画像をクライアントソフトウェアに一括でインポートできます。また、人物の情報と画像をお使いの PC にもエクスポートできます。

18.3.1 人物情報のインポート

事前定義したテンプレート（CSV ファイル）に複数の人物の情報を入力して、クライアントに一括でインポートできます。

手順

1.[人物] モジュールを表示します。
2.リストに追加した組織を選択するか、左上隅の **[追加]** をクリックして組織を追加した後にその組織を選択します。
3.**[インポート]** をクリックして [インポート] パネルを開きます。
4.インポートモードで **[人物情報]** を選択します。
5.**[人物インポート用テンプレートをダウンロードする]** をクリックし、テンプレートをダウンロードします。
6.ダウンロードしたテンプレートに人物情報を入力します。

注記

- その人物が複数のカードを所有している場合、セミコロンを使用して各カード番号を入力します。
- アスタリスク付きの項目の入力は必須です。
- デフォルトでは、[採用日] は現在の日付になります。

7.…をクリックして個人情報を記載した CSV ファイルを選択します。
8.**[インポート]** をクリックしてインポートを開始します。

注記

- その人物の番号がクライアントのデータベース内にすでに存在する場合、インポート前に既存の情報を削除してください。
- 10,000 名分までインポートできます。

18.3.2 人物画像のインポート

追加した人物の顔画像をクライアントにインポートした後は、追加した顔認証ターミナルでその画像内の人物を識別できます。必要に応じて、人物の画像を 1 枚ずつ、または同時に複数枚をインポートできます。

始める前に

事前に人物の情報をクライアントにインポート済みであることを確認してください。

手順

1.[人物] モジュールを表示します。
2.リストに追加した組織を選択するか、左上隅の **[追加]** をクリックして組織を追加した後にその組織を選択します。
3.**[インポート]** をクリックして [インポート] パネルを開き、**[顔]** にチェックを入れます。
4.オプション: **[デバイスによる認証]** を有効化して、クライアントで管理している顔認証デバイスが写真内の顔を認識できるか確認します。
5.…をクリックして顔画像ファイルを選択します。

注記

- 顔画像のフォルダには ZIP 形式で格納してください。
- 各画像ファイルは JPG 形式で、サイズは 200KB 以下にしてください。
- 各画像ファイルの名前は「人物 ID_名前」で設定してください。インポートした人物情報と同じ人物 ID を使用してください。

6.**[インポート]** をクリックしてインポートを開始します。
インポートの進行状況と結果が表示されます。

18.3.3 人物情報のエクスポート

追加した人物の情報を CSV ファイル形式でローカル PC にエクスポートできます。

始める前に

その人物を組織に追加済みであることを確認してください。

手順

1.[人物] モジュールを表示します。
2.オプション: リスト内の組織を選択します。

注記

組織を選択しない場合、すべての人物の情報がエクスポートされます。

3.**[エクスポート]** をクリックして [エクスポート] パネルを開き、エクスポートするコンテンツで **[人物情報]** にチェックを入れます。

4.エクスポートする項目にチェックを入れます。
5.**[エクスポート]** をクリックし、エクスポートした CSV ファイルをお使いの PC に保存します。

18.3.4 人物画像のエクスポート

追加した人物の顔画像ファイルをエクスポートして、お使いの PC に保存できます。

始める前に

その人物とその顔画像を組織に追加済みであることを確認してください。

手順

1.[人物] モジュールを表示します。
2.オプション: リスト内の組織を選択します。

注記

組織を選択しない場合、すべての人物の顔画像がエクスポートされます。

3.**[エクスポート]** をクリックして [エクスポート] パネルを開き、エクスポートするコンテンツで **[顔]** にチェックを入れます。
4.**[エクスポート]** ボタンをクリックしてエクスポートを開始します。

注記

- ファイルは ZIP 形式でエクスポートされます。
- エクスポートする顔画像の名前は「人物 ID_名前_0」です（「0」は真正面からの顔画像を示します）。

18.4 入退室管理デバイスからの人物情報の取得

入退室管理デバイスに、人物情報（人物の詳細、指紋、発行済みカード情報など）を設定済みの場合、そのデバイスから人物情報を取得した後に、クライアントへインポートして操作できます。

手順

注記

- デバイスに保存した人物名が空白の場合、クライアントにインポートすると、人物名フィールドには発行済みのカード番号が表示されます。
- 人物の性別はデフォルトでは **[男性]** になります。
- デバイスに保存したカード番号または人物 ID（従業員 ID）がクライアントのデータベースに保存済みの場合、このカード番号または人物 ID に該当する人物は、クライ

アントへインポートされません。

1.**[人物]** モジュールを表示します。
2.その人物の情報をインポートする組織を選択します。
3.**[デバイスから取得]** をクリックします。
4.ドロップダウンリストから入退室管理デバイスを選択します。
5.**[取得]** をクリックし、クライアントへの人物情報のインポートを開始します。
人物の詳細、指紋情報（設定済みの場合）、リンク済みカードの場合（設定済みの場合）など、その人物の情報が選択した組織にインポートされます。

18.5 別組織への人物の移動

必要に応じて、追加した人物を別組織に移動できます。

始める前に

- 少なくとも 2 つの組織を追加済みであることを確認してください。
- 人物情報をインポート済みであることを確認してください。

手順

1.**[人物]** モジュールを表示します。
2.左側のパネルで組織を選択します。
その組織に属する人物が右側のパネルに表示されます。
3.移動させる人物を選択します。
4.**[Change Organization（組織を変更）]** をクリックします。
5.その人物の移動先となる組織を選択します。
6.**[OK]** をクリックします。

18.6 複数の人物へのカードの一括発行

クライアントには、複数の人物にカードを一括で発行する便利な機能が備わっています。

手順

1.**[人物]** モジュールを表示します。
2.**[カードの一括発行]** をクリックします。
追加されていて、まだカードが発行されていないすべての人物が右側のパネルに表示されます。
3.オプション: 入力ボックスにキーワード（名前または人物 ID）を入力して、カードを発行する必要のある人物をフィルタリングします。
4.オプション: **[設定]** をクリックして、カード発行パラメータを設定します。詳細については、「*個人にカードを発行する*」をご覧ください。

5.**[初期化]** をクリックしてカードの登録ステーションまたはカードリーダーを初期化し、カード発行の準備をします。
6.**[カード番号]** 列をクリックして、カード番号を入力します。
- カード登録ステーションにカードを置きます。
- カードリーダー上でカードをスワイプします。
- カード番号を手動で入力して、**Enter** キーを押します。

リスト内の人物にカードが発行されます。

18.7 カード紛失の報告

カードを紛失した場合、それを報告することで、カード関連のアクセス認証を無効化できます。

手順

1.**[人物]** モジュールを表示します。
2.カードの紛失を報告する人物を選択して **[編集]** をクリックし[人物を編集] ウィンドウを開きます。
3.**[認証情報] → [カード]** パネルの順に進み、該当する追加カードでをクリックして紛失カードとして設定します。
カードの紛失を報告した後は、そのカードのアクセス認証は無効かつ非アクティブになります。別の人物がこのカードを入手してスワイプしてもドアは開放されません。
4.オプション: 紛失したカードが見つかった場合、をクリックすると紛失設定をキャンセルできます。
カードの紛失設定をキャンセルした後は、その人物のアクセス認証は有効かつアクティブになります。
5.紛失したカードが単一のアクセスグループに追加されていて、そのアクセスグループをデバイスに適用済みの場合、カードの紛失を報告または紛失をキャンセルすると、変更事項をこのデバイスに適用することを要求するウィンドウがポップアップ表示されます。
デバイスに適用した後、そのデバイスで、これらの変更事項が有効になります。

第 19 章 入退室管理

[入退室管理] モジュールは、入退室管理デバイスおよびビデオインターコムデバイスで使用できます。アクセスグループの設定、ビデオインターコム、その他の高度な機能など、複数の機能を提供します。

注記

[入退室管理] モジュールの権限を持っているユーザーは、[入退室管理] モジュールにアクセスして、入退室管理設定を設定できます。[入退室管理] モジュールのユーザー権限の設定については、「*ユーザーの追加*」をご覧ください。

19.1 フローチャート

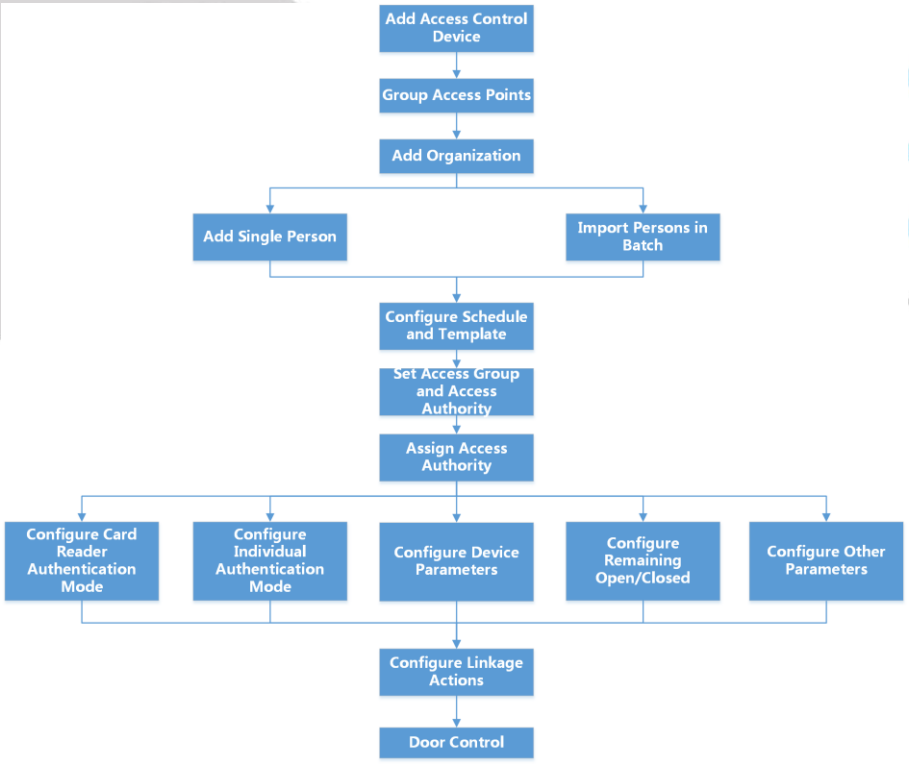

図 19-1 入退室管理のフローチャート

- **入退室管理デバイスの追加:** クライアントに入退室管理デバイスを追加できます。詳細については、「*デバイスの追加*」をご覧ください。
- **アクセスポイントのグループ化:** 追加したアクセスポイントをグループ化して、管理しやすくすることができます。詳細については、「*グループ管理*」をご覧ください。

- **組織の追加:** 組織を追加し、その組織に人物情報をインポートして、人物を管理することができます。詳細については、「*組織の追加*」をご覧ください。
- **スケジュールとテンプレートの設定:** 休日 / 休時間と週のスケジュールを含むテンプレートを設定できます。詳細については、「*スケジュールとテンプレートの設定*」をご覧ください。
- **アクセスグループとアクセス権限の設定**: アクセスグループを設定して、どの人物がどのドアにアクセスできるかを定義し、そのアクセスグループを入退室管理デバイスに適用して権限を有効にすることができます。詳細については、「*アクセスグループを設定してアクセス認証を人物に割り当てる*」をご覧ください。
- **デバイスパラメータの設定:** 入退室管理デバイスのパラメータ（デバイス時間、リンク設定、メンテナンス設定など）を設定できます。詳細については、をご覧ください。
- **開放保持 / 閉鎖保持の設定**: ドアの状態を開放 / 閉鎖に設定したり、エレベータコントローラを未制御または制御済みに設定できます。詳細については、「*開放保持 / 閉鎖保持の設定*」をご覧ください。
- **カードリーダー認証モードの設定:** 実際の使用状況に応じて、入退室管理デバイスで使用するカードリーダーの通過ルールを設定できます。詳細については、「*カードリーダーの認証モードとスケジュールを設定する*」をご覧ください。
- **人物の認証モードの設定:** 実際の使用状況に応じて、指定した入退室管理デバイスに人物の通過ルールを設定できます。詳細については、「*人物認証モードの設定*」をご覧ください。
- **他のパラメータの設定:** 入退室管理デバイスのパラメータ（ネットワークパラメータ、キャプチャパラメータ、RS-485 パラメータ、ウィーガンドパラメータなど）を設定できます。詳細については、をご覧ください。
- **リンク操作の設定:** 入退室管理のリンク操作を設定して、イベントが一連のリンク操作をトリガーしてセキュリティ担当者に通知できるようにすることができます。詳細については、をご覧ください。
- **ドア / エレベータ制御:** 追加した入退室管理デバイスで管理するドアまたはエレベータの状態をリアルタイムで確認できます。詳細については、「*ドア / エレベータ制御*」をご覧ください。

19.2 スケジュールとテンプレートの設定

休日 / 休時間と週のスケジュールを含むテンプレートを設定できます。このテンプレートを設定した後は、アクセスグループの設定時に設定済みのテンプレートをアクセスグループに適用し、テンプレートの期間内でアクセスグループを有効化できるようになります。

注記

アクセスグループ設定については、「*アクセスグループを設定してアクセス認証を人物に割り当てる*」をご覧ください。

19.2.1 休日 / 休時間の追加

休日 / 休時間を作成して、開始日、終了日、1 日内での休時間帯などを設定できます。

手順

> **注記**
> このソフトウェアシステムには休日 / 休時間を最大 64 日追加できます。

1.**[入退室管理]** → **[スケジュール]** → **[Holiday（休日 / 休時間）]** の順にクリックし、[Holiday（休日 / 休時間）] ページを表示します。
2.左側のパネルにある **[追加]** をクリックします。
3.休日 / 休時間の名前を作成します。
4.オプション: [Remark（注記）] ボックスに、休日 / 休時間の説明または連絡事項を入力できます。
5.休日 / 休時間期間を休日 / 休時間リストに追加し、休日 / 休時間の期間を設定します。

> **注記**
> 休日 1 日に対して最大 16 の休時間帯を追加できます。

1）[休日 / 休時間リスト] フィールドで **[追加]** をクリックします。
2）カーソルで時間帯をドラッグ操作して、設定したアクセスグループがその時間中はアクティブの状態になるようにします。

> **注記**
> 休日 / 休時間 1 期間に対して最大 8 つの休時間帯を設定できます。

3）オプション: 以下の操作を実行すると、時間帯を編集できます。
- カーソルを時間帯に移動し、カーソルが  に切り替わると、タイムラインバーの時間帯をドラッグして目的の位置へ移動します。
- 時間帯をクリックし、ダイアログが表示されたら開始時刻 / 終了時刻を直接編集します。
- カーソルを時間帯の開始時刻または終了時刻に移動し、カーソルが  に変わると、ドラッグ操作で時間帯を延長または短縮できます。

4）オプション: 削除する時間帯を選択し、[Operation（操作）] 列で  をクリックすると選択した時間帯を削除できます。
5）オプション: [Operation（操作）] 列で  をクリックすると、タイムバー内の時間帯をすべて削除できます。
6）オプション: [Operation（操作）] 列で  をクリックすると、追加した休日 / 休時間期間を休日 / 休時間リストから削除できます。
6.**[保存]** をクリックします。

19.2.2 テンプレートの追加

テンプレートには、週のスケジュールと休日 / 休時間が含まれています。週のスケジュールを設定して、異なる人物またはグループにアクセス認証期間を割り当てることができます。追加した休日 / 休時間もテンプレートに追加できます。

手順

注記

このソフトウェアシステムには最大 255 件のテンプレートを追加できます。

1.**[入退室管理]** → **[スケジュール]** → **[テンプレート]** の順にクリックし、[テンプレート] ページを表示します。

注記

デフォルトのテンプレートには、全日認証と全日拒否の 2 種類があり、それらの編集や削除は実行できません。

全日認証

このアクセス認証は該当する週の各日で有効であり、休日 / 休時間はありません。

全日拒否

このアクセス認証は該当する週の各日で無効であり、休日 / 休時間はありません。

2.左側のパネルで **[追加]** をクリックし、新しいテンプレートを作成します。
3.テンプレートの名前を作成します。
4.このテンプレートの説明または連絡事項を [Remark（注記）] ボックスに入力します。
5.週のスケジュールを編集し、テンプレートに適用します。
1）下部のパネルで **[Week Schedule（週スケジュール）]** タブをクリックします。
2）該当する週の日付を選択し、タイムラインバーで期間を示します。

注記

週のスケジュールでは、各日あたり最大 8 つの時間帯を設定できます。

3）オプション: 以下の操作を実行すると、時間帯を編集できます。
- カーソルを時間帯に移動し、カーソルが に切り替わると、タイムラインバーの時間帯をドラッグして目的の位置へ移動します。
- 時間帯をクリックし、ダイアログが表示されたら開始時刻 / 終了時刻を直接編集します。
- カーソルを時間帯の開始時刻または終了時刻に移動し、カーソルが に変わると、ドラッグ操作で時間帯を延長または短縮できます。

4）上記の手順を繰り返し、該当する週の別の日付にも時間帯を追加します。

6.休日 / 休時間を追加してテンプレートに適用します。

注記

1 つのテンプレートには最大 4 件の休日 / 休時間を追加できます。

1）**[Holiday（休日 / 休時間）]** タブをクリックします。
2）左側のリストから休日 / 休時間を選択すると、右側のパネルの選択済みリストに追加されます。
3）オプション: **[追加]** をクリックすると、新しい休日 / 休時間を追加できます。

注記

休日 / 休時間の追加方法の詳細については、「*休日 / 休時間の追加*」をご覧ください。

4）オプション: 右側のリストから選択済みの休日 / 休時間を選択し、 をクリックすると、選択した休日 / 休時間を削除できます。また、**[消去]** をクリックすると、右側のリストにある選択済みの休日 / 休時間をすべて消去できます。

7.**[保存]** をクリックして設定を保存し、テンプレートの追加を終了します。

19.3 アクセスグループを設定してアクセス認証を人物に割り当てる

人物を追加してその人物の認証情報を設定した後は、アクセスグループを作成して、どの人物がどのドアにアクセスできるかを定義し、そのアクセスグループを入退室管理デバイスに適用することで設定を有効化できるようになります。

手順

アクセスグループの設定を変更した場合、そのアクセスグループをデバイスに適用して有効化する必要があります。アクセスグループの変更事項には、テンプレート、アクセスグループ設定、人物のアクセスグループ設定、アクセスグループに関連する人物の詳細（例: カード番号、指紋、顔画像、カード番号と指紋の関連付け、またはカード番号と指紋、カードのパスワード、カードの有効期限との関連付け）の変更が含まれます。

1.**[入退室管理]** → **[認証]** → **[アクセスグループ]** の順にクリックし、[アクセスグループ] インタフェースを表示します。
2.**[追加]** をクリックし、[追加] ウィンドウを開きます。
3.**[名前]** テキストフィールドで希望のアクセスグループ名を作成します。
4.アクセスグループのテンプレートを選択します。

注記

アクセスグループの設定前にテンプレートを設定しておく必要があります。詳細については、「*スケジュールとテンプレートの設定*」をご覧ください。

5.[関係者を選択] フィールドの左側のリストで、アクセス権限を割り当てる人物を選択します。

6.[Select Access Point（アクセスポイントを選択）] フィールドの左側のリストで、選択した人物がアクセスするドア、ドアステーション、またはフロアを選択します。

7.**[保存]** をクリックします。

インタフェースの右側で、選択した人物と選択したアクセスポイントを確認できます。

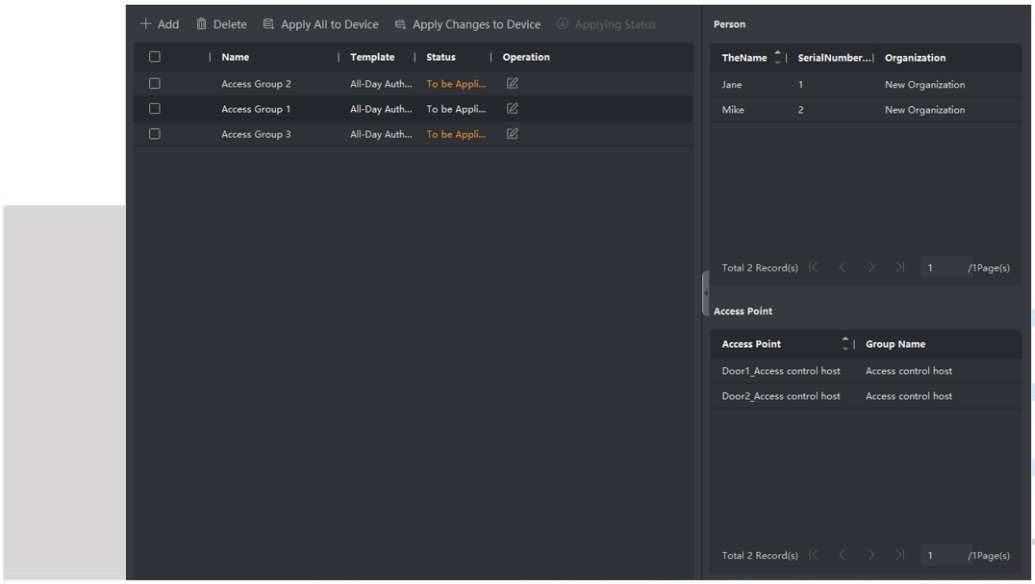

図 19-2 選択した人物とアクセスポイントの表示

図 19-3 選択した人物とアクセスポイントの表示

8.アクセスグループの追加後に、そのグループを入退室管理デバイスに適用して有効化する必要があります。

1）入退室管理デバイスに適用するアクセスグループを選択します。

2）**[デバイスにすべて適用]** をクリックし、入退室管理デバイスまたはドアステーションに対して選択したすべてのアクセスグループの適用を開始します。

3）**[デバイスにすべて適用]** または **[デバイスに変更を適用]** をクリックします。

デバイスにすべて適用

この操作により、選択したデバイスの既存のアクセスグループがすべて消去され、新しいアクセスグループがデバイスに適用されます。

デバイスに変更を適用

この操作では、選択したデバイスの既存のアクセスグループは消去されず、選択したアクセスグループの変更された部分のみがデバイスに適用されます。

4）[状態] 列で適用状態を表示するか、**[適用状態]** をクリックして適用済みのすべてのアクセスグループを表示します。

注記

[Display Failure Only（失敗したもののみを表示）] にチェックを入れて、適用結果をフィルタリングできます。

適用したアクセスグループ内で選択した人物は、リンク済みのカードまたは指紋を使用して、選択したドア / ドアステーションから入室 / 退室する権限を持ちます。

9.オプション: 必要に応じてをクリックし、アクセスグループを編集します。

注記

人物のアクセス情報またはその他の関連情報を変更すると、クライアントの右隅に **[Access Group to Be Applied（適用するアクセスグループ）]** プロンプトが表示されます。プロンプトをクリックして、変更されたデータをデバイスに適用できます。**[今すぐ適用]** または **[後で適用]** を選択できます。

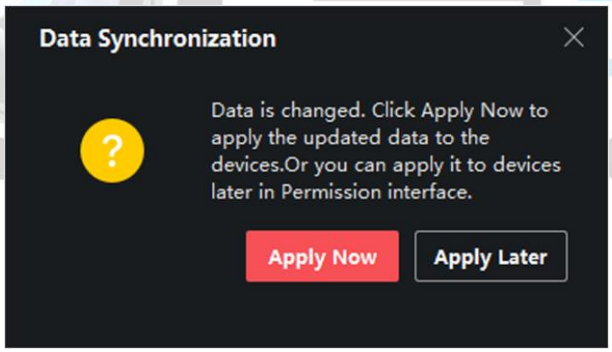

図19-4 データの同期

19.4 アクセスグループの検索

アクセスグループを設定して、人物にアクセス権限を割り当てた後に、人物が属しているアクセスグループを検索して、認証情報番号、認証情報タイプ、適用状態などのその他の関連情報を表示できます。

[入退室管理] → **[認証]** → **[検索]** の順にクリックします。

検索条件を設定します。デバイス名を選択して、人物名（オプション）を入力して、**[検索]**をクリックします。
検索対象の人物が属しているアクセスグループ、および認証情報番号、カード発行状態、注記などのその他の情報を表示できます。

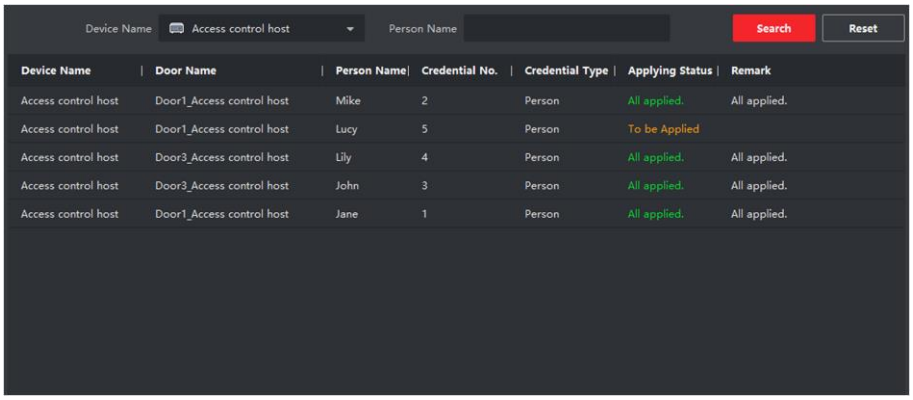

図 19-5 アクセスグループの検索

図 19-6 アクセスグループの検索

19.5 高度な機能設定

多要素認証やアンチパスバックなど、アクセス制御の高度な機能を設定することで、さまざまな状況での特別な要件に対応できます。

注記

- カード関連機能（アクセス制御カード / 多要素認証のタイプ）の場合、カードの追加時には、アクセスグループを適用したカードのみがリストに表示されます。
- デバイスが該当の高度な機能に対応している必要があります。
- [高度な機能] にカーソルを移動して⚙をクリックし、表示する高度な機能をカスタマイズします。

19.5.1 デバイスのパラメータ設定

入退室管理デバイスを追加した後に、入退室管理デバイス（アクセスコントローラ）、入退室管理ポイント（ドアまたはフロア）、アラーム入力、アラーム出力、カードリーダー、およびレーンコントローラのパラメータを設定できます。

入退室管理デバイスのパラメータ設定

入退室管理デバイスを追加した後に、画像へのユーザー情報のオーバーレイ、キャプチャ

後の画像のアップロード、キャプチャ画像の保存などのパラメータを設定できます。

手順

1.**[入退室管理] → [高度な機能] → [Device Parameter（デバイスパラメータ）]** の順にクリックします。

注記

[高度な機能] リストで [Device Parameter（デバイスパラメータ）] が見つからない場合は、カーソルを [高度な機能] の上に合わせて、⚙ をクリックして表示するデバイスパラメータを選択します。

2.右側のページでアクセスデバイスを選択し、そのパラメータを表示させます。
3.スイッチを [ON] にして対応する機能を有効にします。

注記

- 入退室管理デバイスごとに表示するパラメータが異なる場合があります。
- 以下のパラメータの一部は [基本情報] ページにリスト表示されないため、パラメータを編集するには **[More（詳細表示）]** をクリックしてください。

RS-485 通信冗長性

RS-485 カードリーダーを入退室管理デバイスに冗長的に接続する場合は、この機能を有効にする必要があります。

Display Detected Face（検知した顔を表示）

認証時に顔画像を表示します。

カード番号を表示

認証時にカード情報を表示します。

Display Person Information（人物情報を表示）

認証時に人物情報を表示します。

Overlay Person Info. on Picture（人物情報を画像にオーバーレイ）

キャプチャした画像上に人物情報を表示します。

音声プロンプト

この機能を有効にすると、デバイスで音声案内を使用できます。デバイスの動作中、音声案内を聞くことができます。

リンクキャプチャ後に画像をアップロード

関連付けたカメラで取り込んだ画像を、システムへ自動的にアップロードします。

リンクキャプチャ後に画像を保存

この機能を有効にすると、関連付けたカメラで取り込んだ画像をデバイスに保存できます。

Press Key to Enter Card Number（キーを押してカード番号を入力）

この機能を有効にした場合、キーを押してカード番号を入力できるようになります。

Wi-Fi プローブ

この機能を有効にすると、デバイスは周囲の通信デバイスの MAC アドレスをプローブして、MAC アドレスをシステムにアップロードすることができます。見つかった MAC アドレスが、指定した MAC アドレスと一致した場合、システムはリンク操作をトリガーできます。

3G/4G

この機能を有効にすると、デバイスは 3G / 4G ネットワークで通信できるようになります。

NFC アンチクローニング

この機能を有効にすると、複製カードを認証時に使用できなくなり、セキュリティがさらに強化されます。

4.**[OK]** をクリックします。

5.オプション: **[コピー先]** をクリックすると、ページ内のパラメータをコピーする入退室管理デバイスを選択できます。

ドア / エレベータのパラメータ設定

入退室管理デバイスを追加した後に、そのアクセスポイント（ドアまたはフロア）のパラメータを設定することができます。

手順

1.**[入退室管理]** → **[高度な機能]** → **[Device Parameter（デバイスパラメータ）]** の順にクリックします。

2.左側のパネルで入退室管理デバイスを選択し、▸をクリックして選択したデバイスのドアまたはフロアを表示します。

3.右側のページでドアまたはフロアを選択し、そのパラメータを表示します。

4.ドアまたはフロアのパラメータを編集します。

注記

- 入退室管理デバイスごとに表示するパラメータが異なる場合があります。
- 以下のパラメータの一部は [基本情報] ページにリスト表示されないため、パラメータ

を編集するには **[More（詳細表示）]** をクリックしてください。

名前

カードリーダー名を必要に応じて編集します。

ドアの接触装置

ドアセンサーは、閉鎖保持または開放保持に設定できます。通常は閉鎖保持に設定します。

退出ボタンタイプ

出口ボタンは、閉鎖保持または開放保持に設定できます。通常は開放保持に設定します。

ドアロック時間

ノーマルカードをスワイプしてリレー動作を実行すると、ドアを施錠するタイマーが作動します。

延長開放継続時間

アクセス時間の延長が必要な人物が自身のカードをスワイプすると、ドアセンサーが作動して開放時間を適切に延長します。

ドア開放タイムアウトアラーム

設定した時間内にドアが閉鎖しない場合、アラームが作動します。0 に設定するとアラームは作動しません。

Lock Door when Door Closed（ドア閉鎖時の施錠）

[解錠時間] で指定した時間内の場合にもドアを締めると施錠されます。

強要コード

緊急時には、緊急コードを入力するとドアが開きます。同時に、クライアントが緊急イベントを報告することができます。

スーパーパスワード

指定された人物がスーパーパスワードを入力すると、ドアを開くことができます。

解除コード

キーパッドで解除コードを入力して、カードリーダーのブザーを停止するための解除コードを作成します。

注記

- 強要コード、スーパーコード、および解除コードは異なっている必要があります。
- 強要コード、スーパーパスワード、および解除コードは、認証パスワードと異なっている必要があります。

- 強要コード、スーパーパスワード、および解除コードの長さは、デバイスにより異なります。通常は、4～8 桁でなければなりません。

5.**[OK]** をクリックします。
6.オプション: **[コピー先]** をクリックすると、ページ内のパラメータをコピーするドア / フロアを選択できます（複数選択可）。

注記

ドア / フロアの状態継続時間設定も、選択したドアまたはフロアにコピーされます。

カードリーダーのパラメータ設定

入退室管理デバイスの追加後に、そのカードリーダーのパラメータを設定できるようになります。

手順

1.**[入退室管理]** → **[高度な機能]** → **[Device Parameter（デバイスパラメータ）]** の順にクリックします。
2.左側のデバイスリスト内で▸をクリックしてドアの項目を展開し、カードリーダーを選択すると、右側でカードリーダーのパラメータを編集できます。
3.[基本情報] ページでカードリーダーの基本パラメータを編集します。

注記

- 入退室管理デバイスごとに表示するパラメータが異なる場合があります。以下のようなパラメータがリスト表示されます。詳細については、デバイスのユーザーマニュアルをご覧ください。
- 以下のパラメータの一部は [基本情報] ページにリスト表示されないため、パラメータを編集するには **[More（詳細表示）]** をクリックしてください。

名前

カードリーダー名を必要に応じて編集します。

OK LED 極性 / エラー LED 極性 / ブザー極性

カードリーダーのパラメータに従って、メインボードの OK LED 極性 / エラー LED 極性 / ブザー LED 極性を設定します。一般にはデフォルト設定を適用します。

カードスワイプ最小間隔

同じカードのスワイプ間隔が設定値より短い場合、そのカードのスワイプが無効になります。0～255 の範囲で設定できます。

パスワード入力時の最長間隔

カードリーダーにパスワードを入力する時に入力する数字と数字の間隔が設定値より長い場合、直前に入力した数字が自動的に消去されます。

最大試行失敗回数アラーム

カードの読み取り試行回数が設定値を上回った場合、アラーム通知が作動します。

カード試行失敗最大許容回数

カード読み取りで許容する最大の試行回数を設定します。

タンパー検知

カードリーダーの干渉検知を有効にします。

コントローラとの通信頻度

設定時間より長い時間、入退室管理デバイスがカードリーダーに接続できない状態が続いた場合、カードリーダーが自動的にオフラインに切り替わります。

ブザー時間

カードリーダーのブザーの時間を設定します。設定可能な時間は 0～5,999 秒です。0 に設定すると、ブザーが継続的に鳴ります。

カードリーダータイプ / カードリーダー説明

カードリーダーのタイプと説明を示します。読み取りのみに対応しています。

指紋認識レベル

ドロップダウンリストから指紋の認証レベルを選択します。

Default Card Reader Authentication Mode（デフォルトのカードリーダー認証モード）

デフォルトのカードリーダーの認証モードを表示します。

指紋の容量

保存できる指紋の最大個数を表示します。

Existing Fingerprint Number（既存の指紋数）

デバイスに保存されている既存の指紋の数を表示します。

Score（スコア）

デバイスは、ヨーアングル、ピッチアングル、および瞳孔間距離に従って、キャプチャ画像のスコアを判定します。設定された値よりもスコアが低い場合、顔認識は失敗します。

顔認識タイムアウト値

認証にかかる時間が設定時間を上回る場合、デバイスから通知が送られます。

顔認識間隔

認証時における 2 つの連続する顔認証の実行間隔を示します。デフォルト値は 2 秒

です。

顔 1:1 マッチングしきい値

1:1 認証モードで認証する場合に、認証のしきい値を設定します。この値が大きいほど認証時の他人受入率は低下し、本人拒否率は上昇します。

1:N セキュリティレベル

1:N 認証モードで認証する場合に、認証のセキュリティレベルを設定します。この値が大きいほど認証時の他人受入率は低下し、本人拒否率は上昇します。

生体顔検知

生体顔検知機能を有効または無効にします。この機能を有効にすると、認証対象が人間であるかどうかを識別できます。

ライブ顔検知セキュリティレベル

[生体顔検知] 機能を有効にすると、生体顔認証の実行時に作動する認証セキュリティのレベルを設定できます。

顔認証の最大失敗試行回数

生体顔検知の最大試行回数を設定します。設定した試行回数を超えて生体顔検知に失敗すると、そのユーザーの顔では 5 分間認証できなくなります。その間には、本物であると認証されなかったその顔で、同じユーザーが試行しても認証されません。5 分以内に、本物の顔を使用して 2 回連続で認証に成功するとロックが解除されます。

顔のロック認証に失敗

ライブ顔検知機能を有効化した場合、設定した試行回数を超えて生体顔検知に失敗するとそのユーザーの顔の使用が 5 分間ロックされます。その間には、本物であると認証されなかったその顔で、同じユーザーが試行しても認証されません。5 分以内に、本物の顔を使用して 2 回連続で認証に成功するとロックが解除されます。

アプリケーションモード

実際の使用状況に応じて、屋内またはその他のアプリケーションモードを選択できます。

4.**[OK]** をクリックします。

5.オプション: **[コピー先]** をクリックすると、ページ内のパラメータをコピーするカードリーダーを選択できます。

アラーム入力のパラメータ設定

入退室管理デバイスを追加した後に、アラーム入力のパラメータを設定することができます。

手順

> **注記**
> アラーム入力が警戒開始されている場合は、そのパラメータを編集することはできません。まず警戒解除してください。

1. **[入退室管理]** → **[高度な機能]** → **[Device Parameter（デバイスパラメータ）]** の順にクリックします。
2. 左側のデバイスリスト内で▸をクリックしてドアの項目を展開し、アラーム入力を選択すると、右側でアラーム入力のパラメータを編集できます。
3. アラーム入力のパラメータを設定します。

   名前
   アラーム入力名を必要に応じて変更します。

   検知器タイプ
   アラーム入力の検知器タイプです。

   ゾーンタイプ
   アラーム入力のゾーンタイプを設定します。

   感度
   検知器によって検知された信号の継続時間が設定時間に達した場合にのみ、アラーム入力がトリガーされます。例えば、感度を 10 ミリ秒に設定すると、検知器によって検知された信号の継続時間が 10 ミリ秒に達した場合のみ、このアラーム入力がトリガーされます。

   トリガーアラーム出力
   トリガーするアラーム出力を選択します。
4. **[OK]** をクリックします。
5. オプション: 右上隅のスイッチをクリックして、アラーム入力を警戒開始または警戒解除します。

アラーム出力のパラメータ設定

入退室管理デバイスの追加後、アラーム出力にデバイスを関連付けるとパラメータを設定できるようになります。

手順

1.**[入退室管理]** → **[高度な機能]** → **[Device Parameter（デバイスパラメータ）]** の順にクリックし、入退室管理パラメータの設定ページを表示します。
2.左側のデバイスリスト内で▸をクリックしてドアの項目を展開し、アラーム入力を選択すると、右側でアラーム入力のパラメータを編集できます。
3.アラーム出力のパラメータを設定します。

名前

カードリーダー名を必要に応じて編集します。

アラーム出力アクティブ時間

作動後にアラーム出力が有効な時間を示します。

4.**[OK]** をクリックします。
5.オプション: 右上隅のスイッチを **[ON]** にすると、アラーム出力を作動させることができます。

レーンコントローラのパラメータの設定

レーンコントローラをクライアントに追加した後に、レーン通過のパラメータを設定できます。

手順

1.**[入退室管理]** → **[高度な機能]** → **[Device Parameter（デバイスパラメータ）]** の順にクリックして、[パラメータ設定] ページを表示します。
2.左側のデバイスリストで、レーンコントローラを選択して、右側でレーンコントローラのパラメータを編集します。
3.パラメータを編集します。

通過モード

デバイスの防壁状態を制御するコントローラを選択します。

- **[レーンコントローラの DIP 設定に従います]** を選択すると、デバイスはレーンコントローラの DIP 設定に従って防壁を制御します。ソフトウェアの設定が無効になります。
- **[メインコントローラの設定に従います]** を選択すると、デバイスはソフトウェアの設定に従って防壁を制御します。レーンコントローラの DIP 設定が無効になります。

Free Passing Authentication（フリーパス認証）

この機能を有効にすると、入口と出口の両方の防壁モードが [開放状態] の場合、歩行者はレーンを通過するたびに認証を行う必要があります。認証を行わないと、アラー

ムがトリガーされます。

Opening/Closing Barrier Speed（防壁開閉速度）

バリアの開閉速度を設定します。1～10 の値を選択できます。値が大きいほど、ドア開閉速度が速くなります。

注記

推奨値は 6 です。

Audible Prompt Duration（音声プロンプト継続時間）

アラームがトリガーされたときに再生される音声の継続時間を設定します。

注記

0 に設定すると、アラームが終了するまでアラーム音声が再生されます。

温度の単位

デバイス状態に表示される温度単位を選択します。

4.**[OK]** をクリックします。

19.5.2 開放保持 / 閉鎖保持の設定

ドアの状態を開放または閉鎖に設定したり、エレベータコントローラを未制御または制御済みに設定できます。例えば、休日 / 休時間を閉鎖保持、仕事日の特定期間を開放保持に設定できます。

始める前に

システムに入退室管理デバイスを追加しておいてください。

手順

1.**[入退室管理]** → **[高度な機能]** → **[開放保持 / 閉鎖保持]** の順にクリックし、[開放保持 / 閉鎖保持] のページを表示します。

2.左側のパネルで、設定する必要があるドアまたはエレベータコントローラを選択します。

3.平日のドアまたはエレベータコントローラの状態を設定するには、**[週次スケジュール]** をクリックして、次の操作を実行します。

1）ドアの場合は、**[開放状態]** または **[閉鎖状態]** をクリックします。

2）エレベータコントローラの場合は、**[Free（未制御）]** または **[制御済み]** をクリックします。

3）カーソルで時間帯をドラッグ操作して、設定したアクセスグループがその時間中はアクティブの状態になるようにします。

注記

週のスケジュールでは、各日あたり最大 8 つの時間帯を設定できます。

4）オプション: 以下の操作を実行すると、時間帯を編集できます。

- カーソルを時間帯に移動し、カーソルが  に切り替わると、タイムラインバーの時間帯をドラッグして目的の位置へ移動します。
- 時間帯をクリックし、ダイアログが表示されたら開始時刻 / 終了時刻を直接編集します。
- カーソルを時間帯の開始時刻または終了時刻に移動し、カーソルが  に変わると、ドラッグ操作で時間帯を延長または短縮できます。

5）**[保存]** をクリックします。

関連操作

週全体にコピー	タイムバー上で 1 つの時間帯を選択して **[週全体をコピー]** をクリックすると、このタイムバー上のすべての時間帯設定を別の仕事日にコピーできます。
選択対象を削除	タイムバー上で 1 つの時間帯を選択し、**[選択対象を削除]** をクリックすると、その時間帯を削除できます。
消去	**[消去]** をクリックすると、週のスケジュール内のすべての時間帯設定を消去できます。

4.休日 / 休時間中のドアのステータスを設定するには、**[Holiday（休日 / 休時間）]** をクリックして以下の操作を実行します。

1）**[開放保持]** または **[閉鎖保持]** をクリックします。
2）**[追加]** をクリックします。
3）開始日と終了日を入力します。
4）カーソルで時間帯をドラッグ操作して、設定したアクセスグループがその時間中はアクティブの状態になるようにします。

注記

休日 / 休時間 1 期間に対して最大 8 つの休時間帯を設定できます。

5）時間帯を編集するには、以下の操作を実行します。

- カーソルを時間帯に移動し、カーソルが  に切り替わると、タイムラインバーの時間帯をドラッグして目的の位置へ移動します。
- 時間帯をクリックし、ダイアログが表示されたら開始時刻 / 終了時刻を直接編集します。
- カーソルを時間帯の開始時刻または終了時刻に移動し、カーソルが  に変わると、

ドラッグ操作で時間帯を延長または短縮できます。

6）オプション: 削除する時間帯を選択し、[Operation（操作）] 列でをクリックすると選択した時間帯を削除できます。

7）オプション: [Operation（操作）] 列でをクリックすると、タイムバー内の時間帯をすべて削除できます。

8）オプション: [Operation（操作）] 列でをクリックすると、追加した休日 / 休時間期間を休日 / 休時間リストから削除できます。

9）**[保存]** をクリックします。

5.オプション: **[コピー先]** をクリックすると、このドアのステータス設定を別のドアにコピーできます。

19.5.3 多要素認証の設定

グループ別に人物を管理して、1 つの入退室管理ポイント（ドア）に対する複数名の認証を設定できます。

始める前に

アクセスグループを設定し、そのアクセスグループを入退室管理デバイスに適用します。詳細については、「*アクセスグループを設定してアクセス認証を人物に割り当てる*」をご覧ください。

単一の入退室管理ポイント（ドア）に対して複数のカードの認証を設定する場合、このタスクを実行してください。

手順

1.**[入退室管理]** → **[高度な機能]** → **[Multi-Factor Auth（多要素認証）]** の順にクリックします。

2.左側のパネルで、デバイスリストの中から入退室管理デバイスを選択します。

3.この入退室管理デバイスに人物 / カードのグループを追加します。

1）右側のパネルにある **[追加]** をクリックします。

2）希望するグループ名を作成します。

3）その人物 / カードのグループに適用する開始時刻と終了時刻を指定します。

4）[Available（利用可能）] リスト内でメンバーおよびカードを選択して [Selected（選択済み）] リストに追加します。

注記

その人物にカードを発行済みであることを確認してください。
アクセスグループを設定し、そのアクセスグループを入退室管理デバイスへ適用済みであることを確認してください。

5）**[保存]** をクリックします。

6）オプション: 人物 / カードのグループを選択し、**[削除]** をクリックすると、その項目を削除できます。

7）オプション: 人物 / カードのグループを選択して **[適用]** をクリックすると、適用に失敗したアクセスグループを入退室管理デバイスへ再適用できます。

4.左側のパネルで、選択したデバイスの入退室管理ポイント（ドア）を選択します。

5.パスワード入力時の最大間隔を入力します。

6.選択した入退室管理ポイントに使用する認証グループを追加します。

1）[認証グループ] パネルで **[追加]** をクリックします。

2）ドロップダウンリストの中から設定したテンプレートを選択し、認証テンプレートに設定します。

注記

テンプレート設定については、*スケジュールとテンプレートの設定*をご覧ください。

3）ドロップダウンリストの中から、認証タイプとして**[ローカル認証]**、**[ローカル認証と遠隔ドア開放]**、または **[ローカル認証とスーパーパスワード]** を選択します。

ローカル認証

入退室管理デバイスごとの認証設定を示します。

ローカル認証およびリモートでドアを開放

入退室管理デバイス別およびクライアント別の認証設定を示します。デバイスにカードをスワイプすると、ウィンドウがポップアップ表示されます。クライアント経由でドアを解錠できます。

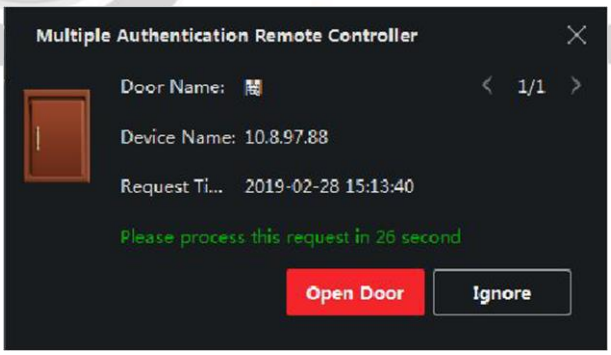

図 19-7 ドアの遠隔開放

注記

入退室管理デバイスがクライアントに接続されていない場合、**[オフライン認証]** にチェックを入れるとスーパーパスワード認証を有効化できます。

ローカル認証およびスーパーパスワード

入退室管理デバイス別、およびスーパーパスワード別の認証設定を示します。

4）左側のリストで追加した人物 / カードのグループを選択すると、認証グループとして右側の [Selected（選択済み）] リストに追加されます。
5）右側のリスト内で追加した認証グループをクリックし、[Auth Times（認証回数）] 列で認証回数を設定します。

注記

- 認証回数は、0 より大きく、人物グループに追加した人数より小さく設定してください。
- 認証回数は最大 16 回です。

6）**[保存]** をクリックします。

注記

- 各入退室管理ポイント（ドア）に対して、認証グループを最大 4 つ追加できます。
- 認証タイプが **[ローカル認証]** の認証グループには、人物 / カードのグループを最大 8 件追加できます。
- 認証タイプが **[ローカル認証とスーパーパスワード]** または **[ローカル認証と遠隔ドア開放]** の認証グループには、人物 / カードのグループを最大 7 件追加できます。

7.**[保存]** をクリックします。

19.5.4 ウィーガンドルールのカスタマイズ設定

サードパーティ製ウィーガンド規格のアップロードルールを理解すると、デバイスとサードパーティ製カードリーダー間の通信に利用するカスタマイズされたウィーガンド規格のルールを複数設定できます。

始める前に

デバイスにサードパーティ製カードリーダーを配線します。

手順

注記

- デフォルトでは、ウィーガンドのカスタム機能は無効化されています。ウィーガンド機能のカスタマイズを有効にすると、カスタマイズしたウィーガンドプロトコルをデバイス内のすべてのウィーガンドインタフェースで使用できます。
- 最大 5つのカスタマイズしたウィーガンドを設定できます。
- ウィーガンドのカスタマイズ設定の詳細については、「*ウィーガンドルールのカスタマイズ設定*」をご覧ください。

1.**[入退室管理]** → **[高度な機能]** → **[Custom Wiegand（カスタムウィーガンド）]** の順にクリックし、[Custom Wiegand（カスタムウィーガンド）] のページを表示します。

2.左側で [Custom Wiegand（ウィーガンドをカスタマイズ）] を選択します。
3.ウィーガンドの名前を作成します。

注記

カスタムウィーガンド名には最大 32 文字まで使用できます。

4.**[Select Device（デバイスを選択）]** をクリックして、カスタムウィーガンドを設定する入退室管理デバイスを選択します。
5.サードパーティ製カードリーダーのプロパティに応じて、パリティモードを設定します。

注記

- 最大 80 ビットまで使用できます。
- 奇数パリティのスタートビット、奇数パリティの長さ、偶数パリティのスタートビット、偶数パリティの長さは、1 から 80 ビットまでで設定します。
- カード ID、メーカーコード、サイトコード、OEM のスタートビットは、1 から 80 ビットまでの間で設定します。

6.出力の変換ルールを設定します。
1）**[ルール設定]** をクリックし、[出力変換ルールを設定] を開きます。

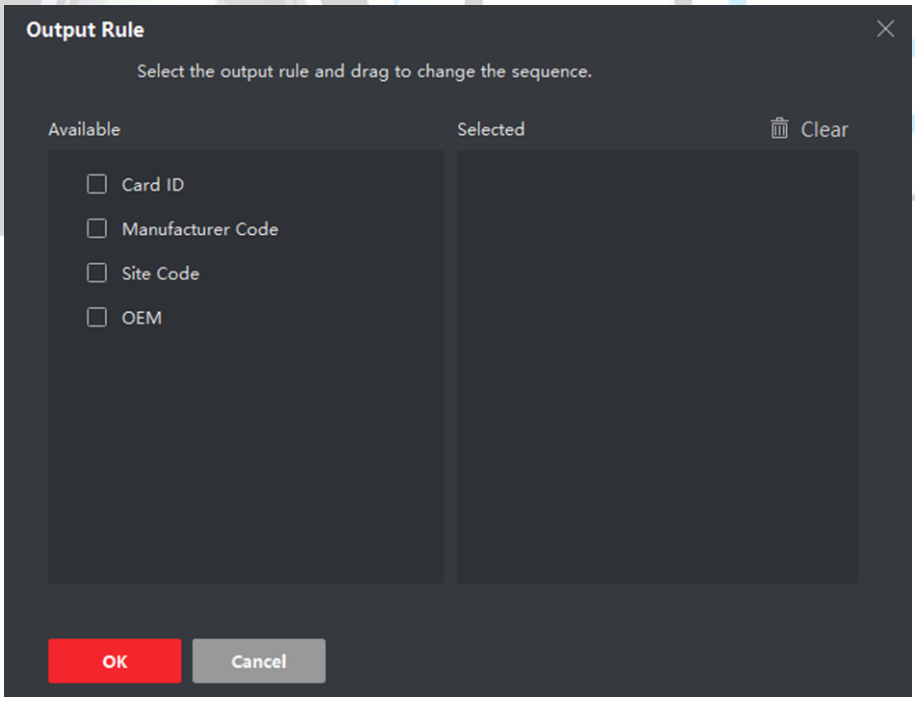

図19-8 出力変換ルールの設定

2）左側のリストからルールを選択します。
選択したルールは右側のリストに追加されます。
3）オプション: ルールをドラッグすると、ルールの順番を変更できます。

4）**[OK]** をクリックします。

5）[Custom Wiegand（カスタムウィーガンド）] タブで、ルールのスタートビット、長さ、および 10 進数字を設定します。

7.**[保存]** をクリックします。

19.5.5 カードリーダーの認証モードとスケジュールを設定する

実際の使用状況に応じて、入退室管理デバイスで使用するカードリーダーの通過ルールを設定できます。

手順

1.**[入退室管理]** → **[高度な機能]** → **[認証]** の順にクリックし、認証モードの設定ページを表示します。

2.左側でカードリーダーを選択して設定します。

3.カードリーダーの認証モードを設定します。

1）**[設定]** をクリックします。

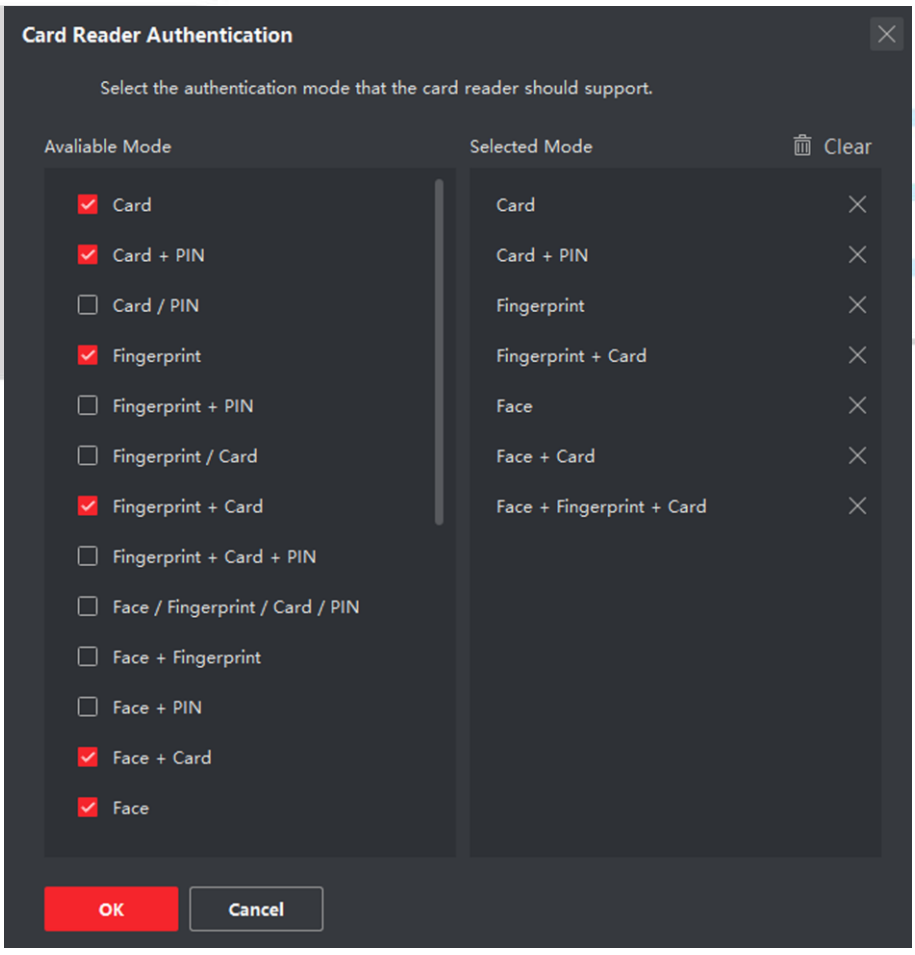

図 19-9 カードリーダー認証モードの選択

注記

PIN は、ドアを開くための PIN コードを意味しています。詳細については、「***入退室管理情報の設定***」をご覧ください。

2）[Available Mode（利用可能モード）] リスト内のモードにチェックを入れると、そのモードが選択したモードリストに追加されます。

3）**[OK]** をクリックします。

モードを選択すると、そのモードが別の色でアイコンとして表示されます。

4.アイコンをクリックしてカードリーダーの認証モードを選択した後に、カーソルをドラッグしてスケジュール上にカラーバーを引くと、その期間中はカードリーダー認証が有効になります。

5.他の期間を設定する場合、上記の手順を繰り返してください。

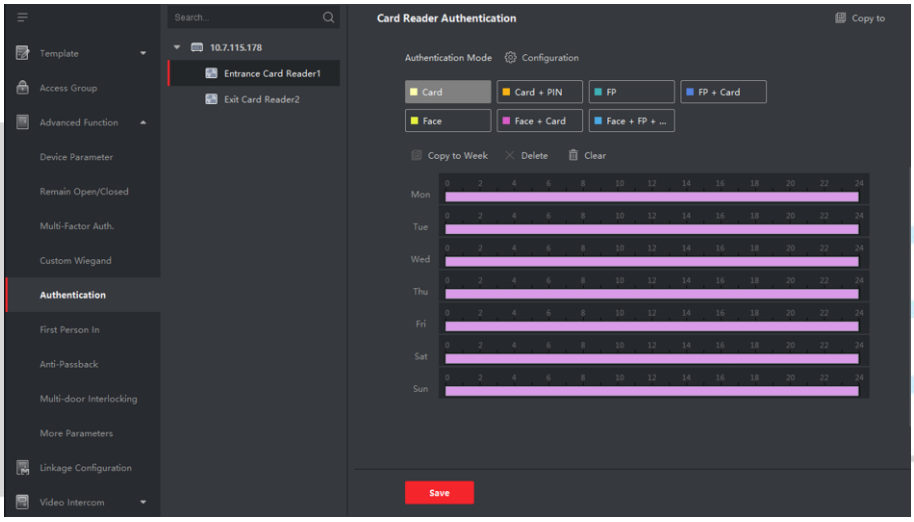

図 19-10 カードリーダーの認証モード設定

6.オプション: 設定済みの日付を選択して **[週全体にコピー]** をクリックすると、同じ設定を週全体にコピーできます。

7.オプション: **[コピー先]** をクリックすると、その設定を他のカードリーダーにコピーできます。

8.**[保存]** をクリックします。

19.5.6 人物認証モードの設定

実際の使用状況に応じて、指定した入退室管理デバイスに人物の通過ルールを設定できます。

始める前に

入退室管理デバイスが人物認証機能をサポートしていることを確認してください。

手順

1.**[入退室管理]** → **[高度な機能]** → **[認証方式]** の順にクリックします。
2.左側のパネルで、人物の認証機能をサポートしている入退室管理デバイスを選択して、人物の [認証モード] ページを表示します。
3.**[追加]** をクリックし、[追加] ウィンドウを表示します。
4.左側のパネルで、設定する必要がある人物を選択します。
選択した人物が右側のリストに追加されます。
5.**[認証モード]** のドロップダウンリストで認証モードを選択します。
6.**[OK]** をクリックします。

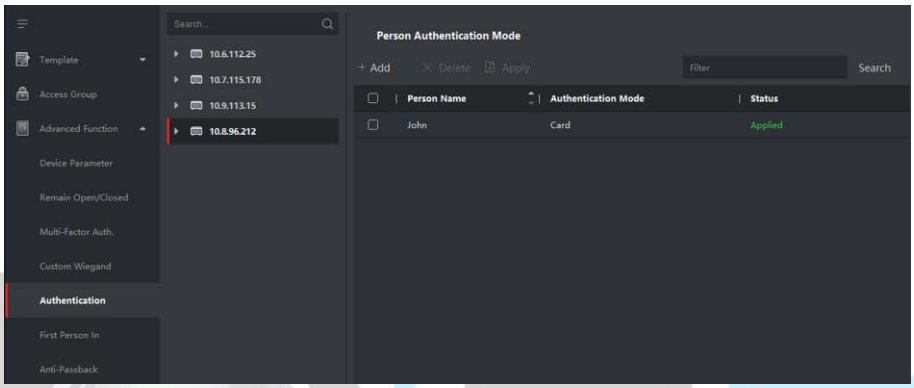

図 19-11 人物の認証モードの設定

7.オプション: 人物認証モードページで人物を選択して、**[適用]** をクリックして人物認証モードをデバイスに適用します。

注記

人物認証は、他の認証モードよりも優先されます。入退室管理デバイスが人物認証モードに設定されている場合、人物は人物認証モードを使用してこのデバイスで認証を行う必要があります。

19.5.7 エレベータコントローラの中継の設定

エレベータコントローラの場合、フロアと中継の関係を管理して、フロアの中継タイプを設定できます。中継タイプごとに異なる機能を実装できます。フロアと中継の関係を設定することで、エレベータにさまざまな機能を割り当てて、エレベータを制御できます。

中継とフロアの関係の設定

目的のフロアに異なる中継タイプを割り当てることができ、各フロアに 3 つの中継タイプを割り当てることができます。このようにすることで、エレベータを呼び出して、異なるフロアの操作を割り当てることができます。

始める前に

エレベータコントローラをクライアントに追加します。

手順

1.**[入退室管理]** → **[高度な機能]** → **[エレベータ設定]** の順にクリックし、[中継設定] ページを表示します。
2.左側でエレベータコントローラを選択します。
3.右側の [未設定の中継] パネルで、未設定の中継を選択します。

3 種類の中継を使用できます。

ボタン

各フロアのボタンの有効性を制御します。

注記

: ボタン中継を表します。

エレベータ呼び出し

インドアステーションまたはアウトドアステーションで、エレベータを呼び出して、指定したフロアへ移動する制御を行います。

注記

: エレベータ呼び出し中継を表します。

自動

ユーザーがエレベータ内でカードをスワイプしたときに、ボタンを押す制御を行います。ユーザーの権限に従って、フロアのボタンが自動的に押されます。

注記

: オートボタン中継を表します。

例

次の図を例にとって説明します。番号 1-2 で、1 は分散エレベータコントローラ番号、2 は中継、アイコン は中継タイプを表します。 中継タイプを変更できます。詳細については、「*中継タイプの設定*」をご覧ください。

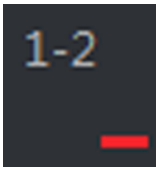

図 19-12 中継

4.中継とフロアの関係を設定します。

– [未設定の中継] パネルから [フロアリスト] パネルの目的のフロアに未設定の中継をドラッグします。
– [フロアリスト] パネルから [未設定の中継] パネルに中継をドラッグします。
– [フロアリスト] パネルで、あるフロアから別のフロアに中継をドラッグします。目的のフロアが、ドラッグした中継と同じタイプの中継ですでに設定されている場合は、同じタイプの既存の中継が置き換えられます。

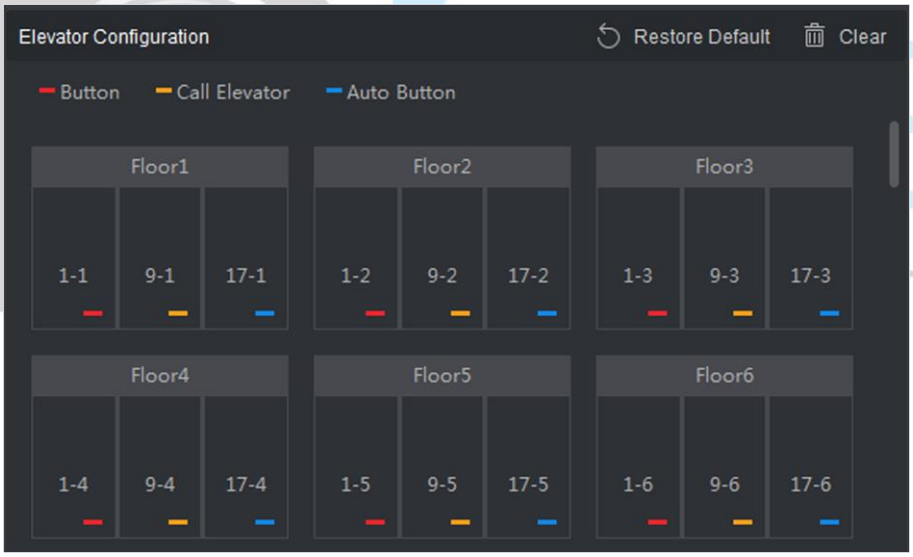

図 19-13 中継とフロアの関係

注記

- エレベータコントローラは、最大 24 台の分散エレベータコントローラにリンクできます。分散エレベータコントローラは、最大 16 個の中継をリンクできます。
- デフォルトでは、中継の合計数は、追加したフロア数の 3 倍（3 種類の中継）です。
- 最大 3 種類の中継を 1 つのフロアにドラッグできます。
- ドアグループ管理でフロア数を変更すると、[中継設定] インタフェースのすべての中継がデフォルト設定に戻ります。

5.**[保存]** をクリックして、選択したエレベータコントローラに設定を適用します。

中継タイプの設定

異なる中継タイプ（ボタン中継、エレベータ呼び出し中継、および自動ボタン中継）を設定して、異なる機能を実装できます。中継タイプごとに異なる機能を実装できます。ボタン中継は、各フロアのボタンの有効性を制御する中継です。エレベータ呼び出し中継は、インドアステーションまたはアウトドアステーションで、指定したフロアにエレベータを呼び出す中継です。自動ボタン中継は、ユーザーがエレベータ内でカードをスワイプしたときにボタンを押す制御を行う中継で、ユーザーの権限に従ってフロアのボタンが自動的に押されます。

手順

1.**[入退室管理]** → **[高度な機能]** → **[エレベータ設定]** の順にクリックし、[中継設定] ページを表示します。
2.ページの左側でエレベータコントローラを選択します。
3.**[中継タイプ設定]** をクリックして、[中継タイプ設定] ウィンドウを開きます。

注記

- [中継タイプ設定] ウィンドウのすべての中継が未設定の中継です。
- 次の 3 種類の中継を使用できます。 はボタン中継を表し、 はエレベータ呼び出し中継を表し、 は自動ボタン中継を表します。

4.1 つの中継タイプパネルから目的のフロアに中継をドラッグします。

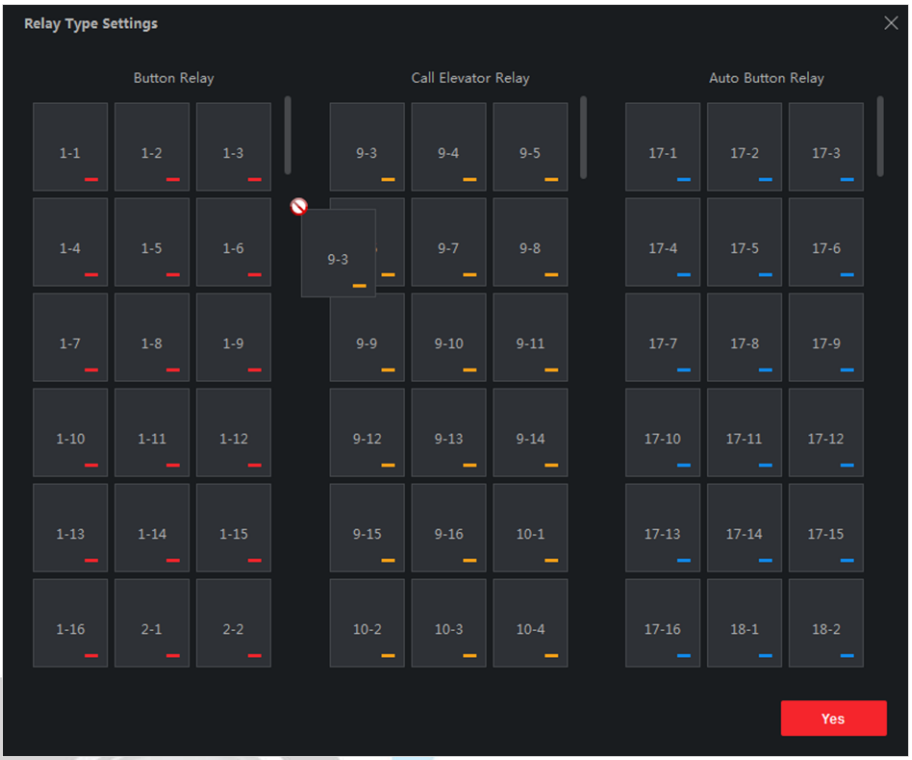

図 19-14 中継タイプの設定

5.**[OK]** をクリックします。

19.5.8 最初の人物の入室設定

1 つの入退室管理ポイントに対して、最初にアクセスする人物を複数設定できます。最初の人物が認証された後に、複数名によるドアへのアクセスなどの認証動作が許可されます。

始める前に

アクセスグループを設定して、そのアクセスグループを入退室管理デバイスに適用します。詳細については、「*アクセスグループを設定してアクセス認証を人物に割り当てる*」をご覧ください。

最初の人物によるドア開放を設定する時に、このタスクを実行してください。

手順

1.**[入退室管理]** → **[高度な機能]** → **[First Person In（最初の人物の入室）]** の順にクリックし、[First Person In（最初の人物の入室）] ページを表示します。
2.左側のパネルで、リストの中から入退室管理デバイスを選択します。
3.選択したデバイスの各入退室管理ポイントのドロップダウンリストから、現在のモードとして **[最初の人物の後、開放保持を有効にする]**、**[最初の人物の後、開放保持を無効にする]**、または **[Authorization by First Person（最初の人物による認証）]** を選択します。

Enable Remaining Open after First Person（最初の人物の後、開放保持を有効にする）

最初の人物の認証後、開放保持期間が終了するまでドアの開放が保持されます。このモードを選択した場合、開放時間を設定してください。

注記

開放保持の期間は、0 から 1440 分までです。デフォルトでは、開放保持の期間は 10 分に設定されています。

Disable Remaining Open after First Person（最初の人物の後、開放保持を無効にする）

最初の人物の入室に関する設定を無効化して、通常の認証モードに切り替えます。

Authorization by First Person（最初の人物による認証）

最初の人物が認証された後にのみ、すべての認証（スーパーカード、スーパーパスワード、強要カード、強要コードの認証を除く）が許可されます。

注記

最初の人物モードを無効化するために、最初の人物で再認証することもできます。

4.[First Person List（最初の人物）] パネルで **[追加]** をクリックします。
5.左側のリスト内で人物を選択すると、ドアの最初の人物としてその人物が選択済み人物に追加されます。
追加した最初の人物は、[First Person List（最初の人物リスト）] に表示されます。
6.オプション: リストから最初の人物を選択して **[削除]** をクリックすると、最初の人物リストからその人物を削除できます。
7.**[保存]** をクリックします。

19.5.9 アンチパスバック設定

指定パスのみで入退室管理ポイントを通過できて、カードのスワイプで 1 名のみが入退室管理ポイントを通過できるように設定できます。

始める前に

入退室管理デバイスのアンチパスバック機能を有効化します。

入退室管理デバイスにアンチパスバック機能を設定する場合、このタスクを実行してください。

手順

注記

1 台の入退室管理デバイスに対して、アンチパスバック機能または複数ドアのインターロック機能を同時に設定できます。複数ドアのインターロック設定については、「***複数ドアのインターロックの設定***」をご覧ください。

1.**[入退室管理]** → **[高度な機能]** → **[アンチパスバック]** の順にクリックし、[アンチパスバック] 設定ページを表示します。
2.左側のパネルで入退室管理デバイスを選択します。
3.**[First Card Reader（最初のカードリーダー）]** フィールド内でパスの最初に記載するカードリーダーを選択します。
4.**[その後のカードリーダー]** 列で、選択済みの最初のカードリーダーの をクリックしてカードリーダーの選択ダイアログを開きます。
5.最初のカードリーダーの後続となるカードリーダーを選択します。

注記

1 台のカードリーダーに対して、後続のカードリーダーを最大 4 台まで追加できます。

6.ダイアログ内で **[OK]** をクリックし、選択情報を保存します。
7.[アンチパスバック] 設定ページで **[保存]** をクリックして設定を保存し、その設定を有効化します。

例

カードスワイプのパスを設定します。最初のパスとして「Reader In_01」を、関連付けカードリーダーとして「Reader In_02」と「Reader Out_04」を選択すると仮定します。この場合、「Reader In_01」、「Reader In_02」、「Reader Out_04」の順にカードをスワイプした場合に限り、入退室管理ポイントを通過できます。

19.5.10 複数ドアのインターロックの設定

同じ入退室管理デバイスの複数のドアにインターロックを設定できます。いずれかのドアを開くには、他のドアが閉じている必要があります。つまり、インターロックが設定されたドアグループでは、一度に 1 つのドアのみ開くことができます。

複数ドアのインターロックを実現するには、このタスクを実行します。

手順

注記

- 複数ドアインターロック機能は、複数の入退室管理ポイント（ドア）のある入退室管理デバイスでのみサポートされています。
- 1 台の入退室管理デバイスに対して、アンチパスバック機能または複数ドアのインターロック機能を同時に設定できます。アンチパスバック機能の設定については、「*アンチパスバックの設定*」をご覧ください。

1.**[入退室管理]** → **[高度な機能]** → **[複数ドアインターロック]** の順にクリックします。
2.左側のパネルで入退室管理デバイスを選択します。

3.[複数ドアインターロックリスト] パネルで **[追加]** をクリックして、[入退室管理ポイントを追加] を開き、[追加] ウィンドウを開きます。
4.リストから少なくとも 2 つの入退室管理ポイント（ドア）を選択します。

注記

1 つの複数ドアインターロックの組み合わせに、最大 4 つのドアを追加できます。

5.**[OK]** をクリックして、インターロック用に選択した入退室管理ポイントを追加します。
設定した複数ドアインターロックの組み合わせが、[複数ドアインターロックリスト] パネルに表示されます。
6.オプション: 追加した複数ドアインターロックの組み合わせをリストから選択して、**[削除]** をクリックして組み合わせを削除します。
7.**[適用]** をクリックして、入退室管理デバイスに設定を適用します。

19.5.11 認証コードの設定

クライアントで認証コードを設定できます。設定後は、カードを忘れたときに認証コードを入力してドアを開けることができます。

ドアを開けるための認証コードを設定する場合は、このタスクを実行します。

注記

- 入退室管理デバイスが認証コード機能をサポートしている必要があります。
- 最大 500 枚のカードと認証コードを 1 つの入退室管理デバイスに追加できます。認証コードは一意でなければなりません。

手順

1.**[入退室管理]** → **[高度な機能]** → **[認証コード]** の順にクリックして、認証コード設定ページを表示します。
2.[コントローラリスト] パネルのリストで入退室管理デバイスを選択します。
適用されているすべてのカードと人物が [カードリスト] パネルに表示されます。

注記

権限の設定とデバイスへの権限の適用については、「*アクセスグループを設定してアクセス認証を人物に割り当てる*」をご覧ください。

3.[認証コード] 列の各カードのフィールドをクリックして、認証コードを入力します。

注記

認証パスワードは、4～8 桁でなければなりません。

4.[認証コード] ページの右上隅の **[保存]** をクリックして、設定を保存します。
カードの認証コード機能は自動的に有効になります。

次に行う操作

入退室管理デバイスのカードリーダー認証モードを **[カード / 認証コード]** に設定する必要があります。詳細については、「*カードリーダーの認証モードとスケジュールを設定する*」をご覧ください。

19.6 その他のパラメータの設定

入退室管理デバイスを追加した後に、ネットワークパラメータ、キャプチャパラメータ、RS-485 パラメータ、ウィーガンドパラメータなどのパラメータを設定することができます。

19.6.1 複数の NIC パラメータの設定

デバイスが複数のネットワークインタフェースに対応している場合、クライアント側で IP アドレス、MAC アドレス、ポート番号などの NIC ネットワークのパラメータを設定できます。

手順

注記
使用するデバイスがこの機能に対応している必要があります。

1.[入退室管理] モジュールを表示します。
2.左側のナビゲーションバーで、**[高度な機能]** → **[詳細パラメータ]** の順に表示します。
3.デバイスリスト内で入退室管理デバイスを選択して **[NIC]** をクリックし、[Multiple NIC Settings（複数の NIC パラメータ）] ページを表示します。
4.ドロップダウンリストから、設定する NIC を選択します。
5.該当する IP アドレス、デフォルトゲートウェイ、サブネットマスクなどのネットワークパラメータを設定します。

MAC アドレス

メディアアクセス制御アドレス（MAC アドレス）は、物理的なネットワークセグメント上での通信のために、ネットワークインタフェースに割り当てられる一意の識別子です。

MTU

ネットワークインタフェースの最大転送単位（MTU）を示します。

6.**[保存]** をクリックします。

19.6.2 ネットワークパラメータの設定

入退室管理デバイスを追加した後に、デバイスログのアップロードモードを設定して、有線ネットワークまたは無線ネットワーク経由で ISUP アカウントを作成することができます。

ログのアップロードモード設定

デバイスが ISUP プロトコルでログをアップロードするモードを設定できます。

手順

1.[入退室管理] モジュールを表示します。
2.左側のナビゲーションバーで、**[高度な機能]** → **[詳細パラメータ]** の順に表示します。
3.デバイスリスト内で入退室管理デバイスを選択し、**[ネットワーク]** → **[アップロードモード]** の順に表示します。
4.ドロップダウンリストからセンターグループを選択します。
5.**[有効]** にチェックを入れてアップロードモードの設定を有効化します。
6.ドロップダウンリストからアップロードモードを選択します。
- メインチャンネルまたはバックアップチャンネル用に **[N1]** または **[G1]** を有効化します。

[閉じる] を選択してメインチャンネルまたはバックアップチャンネルを無効化します。

注記

メインチャンネルとバックアップチャンネルで同時に N1 または G1 を有効化することはできません。

7.**[保存]** をクリックします。

有線通信モードでの ISUP アカウントの作成

有線通信モードで、ISUP プロトコルのアカウントを設定できます。その後、ISUP プロトコルでデバイスを追加できます。

手順

注記

使用するデバイスがこの機能に対応している必要があります。

1.[入退室管理] モジュールを表示します。
2.左側のナビゲーションバーで、**[高度な機能]** → **[詳細パラメータ]** の順に表示します。
3.デバイスリスト内で入退室管理デバイスを選択し、**[ネットワーク]** → **[ネットワークセンター]** の順に表示します。
4.ドロップダウンリストからセンターグループを選択します。

5.**[アドレスタイプ]** で **[IP アドレス]** または **[ドメイン名]** を選択します。
6.アドレスタイプに応じて、IP アドレスまたはドメイン名を入力します。
7.プロトコルのポート番号を入力します。

注記

無線ネットワークと有線ネットワークのポート番号は、ISUP のポート番号と一致している必要があります。

8.**[プロトコルタイプ]** で **[ISUP]** を選択します。
9.ネットワークセンターのアカウント名を設定します。
10.**[保存]** をクリックします。

無線通信モードでの ISUP アカウントの作成

無線通信モードで、ISUP プロトコルのアカウントを設定できます。その後、ISUP プロトコルでデバイスを追加できます。

手順

注記

使用するデバイスがこの機能に対応している必要があります。

1.[入退室管理] モジュールを表示します。
2.左側のナビゲーションバーで、**[高度な機能]** → **[詳細パラメータ]** の順に表示します。
3.デバイスリストで入退室管理デバイスを選択して、**[ネットワーク]** → **[Wireless Communication Center（ワイヤレスコミュニケーションセンター）]** に移動します。
4.**[APN 名]** として **[CMNET]** または **[UNINET]** を選択します。
5.SIM カード番号を入力します。
6.ドロップダウンリストからセンターグループを選択します。
7.IP アドレスとポート番号を入力します。

注記

- デフォルトでは、ISUP のポート番号は ***7660*** です。
- 無線ネットワークと有線ネットワークのポート番号は、ISUP のポート番号と一致している必要があります。

8.**[プロトコルタイプ]** で **[ISUP]** を選択します。
9.ネットワークセンターのアカウント名を設定します。
10.**[保存]** をクリックします。

19.6.3 デバイスのキャプチャパラメータ設定

手動キャプチャやイベント作動型キャプチャなど、入退室管理デバイスのキャプチャパラメータを設定できます。

注記

- 使用するデバイスがこのキャプチャ機能に対応している必要があります。
- キャプチャパラメータの設定前に、画像のストレージを設定し、イベントトリガー画像の保存場所を定義しておく必要があります。詳細については、「*画像ストレージの設定*」をご覧ください。

キャプチャ後のパラメータ設定

イベントが発生すると、入退室管理デバイスに搭載のカメラが作動して画像を取り込み、イベント発生時の出来事を記録します。[イベントセンター] のイベント詳細を確認すると、キャプチャ画像を閲覧できます。その前に、一度に取り込む画像数などのキャプチャパラメータを設定しておく必要があります。

始める前に

キャプチャパラメータの設定前に、画像のストレージを設定し、キャプチャ画像の保存場所を定義しておく必要があります。詳細については、「*画像ストレージの設定*」をご覧ください。

手順

注記

使用するデバイスがこの機能に対応している必要があります。

1.[入退室管理] モジュールを表示します。
2.左側のナビゲーションバーで、**[高度な機能]** → **[詳細パラメータ]** → **[キャプチャ]** の順に表示します。
3.デバイスリスト内で入退室管理デバイスを選択し、**[リンクキャプチャ]** を選択します。
4.画像のサイズと画質を設定します。
5.作動後の取り込み回数を設定し、一度に取り込む枚数を定義します。
6.取り込み回数が 1 を上回る場合、取り込みの間隔を設定してください。
7.**[保存]** をクリックします。

手動キャプチャのパラメータ設定

[ステータスモニター] モジュールでは、入退室管理デバイスに搭載のカメラのボタンをクリックして画像を手動で取り込むことができます。その前に、画質などのキャプチャパラメータを設定しておく必要があります。

始める前に

キャプチャパラメータの設定前に、保存パスを設定し、キャプチャ画像の保存場所を定義しておく必要があります。詳細については、「*ファイル保存先パスの設定*」をご覧ください。

手順

注記

使用するデバイスがこの機能に対応している必要があります。

1.[入退室管理] モジュールを表示します。
2.左側のナビゲーションバーで、**[高度な機能]** → **[詳細パラメータ]** → **[キャプチャ]** の順に表示します。
3.デバイスリスト内で入退室管理デバイスを選択し、**[手動キャプチャ]** を選択します。
4.ドロップダウンリストから、キャプチャ画像の解像度を選択します。
5.画質として **[高]**、**[中]**、または **[低]** を選択します。画質が高いほど、画像サイズは大きくなります。
6.**[保存]** をクリックします。

19.6.4 顔認証ターミナルのパラメータの設定

顔認証ターミナルでは、顔画像のデータベース、QR コード認証などのパラメータを設定できます。

手順

注記

使用するデバイスがこの機能に対応している必要があります。

1.[入退室管理] モジュールを表示します。
2.左側のナビゲーションバーで、**[高度な機能]** → **[詳細パラメータ]** の順に表示します。
3.デバイスリスト内で入退室管理デバイスを選択し、**[顔認証ターミナル]** をクリックします。
4.パラメータを設定します。

注記

デバイスのモデルによって表示されるパラメータは異なります。

COM

設定する COM ポートを選択します。COM1 は RS-485 インタフェースで、COM2 は RS-232 インタフェースです。

顔画像データベース

顔画像データベースとして [ディープラーニング] を選択します。

QR コード認証

有効化すると、デバイスのカメラが QR コードをスキャンして認証を実行します。デフォルトでこの機能は無効化されています。

ブラックリスト認証

有効にすると、デバイスはアクセスを求めている人物を、ブラックリストに登録されている人物と比較します。
一致した場合（人物がブラックリストに登録されている場合）、アクセスは拒否され、デバイスはクライアントにアラームをアップロードします。
一致しない場合（人物がブラックリストに登録されていない場合）は、アクセスが許可されます。

Save Authenticating Face Picture（認証中の顔画像を保存）

有効化すると、認証中にキャプチャされた顔画像がデバイスに保存されます。

MCU バージョン

デバイスの MCU バージョンを表示します。

5.**[保存]** をクリックします。

19.6.5 M1 カード暗号化の有効化

M1 カードを暗号化すると、認証のセキュリティレベルが向上します。

手順

注記

入退室管理デバイスとカードリーダーがこの機能に対応している必要があります。

1.[入退室管理] モジュールを表示します。
2.左側のナビゲーションバーで、**[高度な機能]** → **[詳細パラメータ]** の順に表示します。

3.デバイスリスト内で入退室管理デバイスを選択して **[M1 カード暗号化]** をクリックし、[M1 カード暗号化] ページを表示します。
4.スイッチを [ON] にして M1 カードの暗号化機能を有効にします。
5.セクター ID を設定します。

セクター ID は、1～100 の範囲で設定します。

6.**[保存]** をクリックして設定を保存します。

19.6.6 RS-485 パラメータの設定

入退室管理デバイスの RS-485 パラメータを設定します。例えば、ボーレート、データビット、ストップビット、パリティタイプ、フロー制御タイプ、通信モード、動作モード、接続モードなどが該当します。

手順

注記

使用するデバイスが RS-485の設定に対応している必要があります。

1.[入退室管理] モジュールを表示します。
2.左側のナビゲーションバーで、**[高度な機能]** → **[詳細パラメータ]** の順に表示します。
3.デバイスリスト内で入退室管理デバイスを選択して **[RS-485]** をクリックし、[RS-485 設定] ページを表示します。
4.ドロップダウンリストからシリアルポート番号を選択し、RS-485 のパラメータを設定します。
5.ドロップダウンリストで、ボーレート、データビット、ストップビット、パリティタイプ、通信モード、動作モード、接続ポートを設定します。

注記

接続モードが **[入退室管理デバイスを接続]** の場合、出力タイプとして **[カード番号]** または **[人物 ID]** を選択できます。

6.**[保存]** をクリックします。
- 設定したパラメータはデバイスへ自動適用されます。
- 動作モードまたは接続モードを変更すると、デバイスは自動的に再起動します。

19.6.7 ウィーガンドパラメータの設定

入退室管理デバイスのウィーガンドチャンネルと通信モードを設定できます。ウィーガンドパラメータの設定後は、ウィーガンド通信でウィーガンド規格のカードリーダーにデバイスを接続できるようになります。

手順

注記

使用するデバイスがこの機能に対応している必要があります。

1.[入退室管理] モジュールを表示します。
2.左側のナビゲーションバーで、**[高度な機能]** → **[詳細パラメータ]** の順に表示します。
3.デバイスリスト内で入退室管理デバイスを選択して **[ウィーガンド]** をクリックし、[Wiegand Settings（ウィーガンド設定）] ページを表示します。
4.スイッチを [ON] にしてデバイスのウィーガンド機能を有効にします。
5.ドロップダウンリストからウィーガンドのチャンネル番号と通信モードを選択します。

注記

[Communication Direction（通信方向）] を **[Sending（送信）]** に設定する場合、**[ウィーガンドモード]** を **[ウィーガンド 26]** または **[ウィーガンド 34]** に設定する必要があります。

6.**[保存]** をクリックします。
- 設定したパラメータはデバイスへ自動適用されます。
- 通信方向の変更後、デバイスは自動的に再起動します。

19.6.8 出勤ステータスの設定

クライアントを経由してデバイスで出勤モードを設定できます。実際の使用状況に応じて、デバイス上で出勤パラメータをチェックイン、チェックアウト、休憩開始、休憩終了、残業開始、または残業終了に設定できます。

注記

使用するデバイスがこの機能に対応している必要があります。

出勤モードの無効化

出勤モードを無効にすると、デバイスの最初のページで出勤ステータスが表示されなくなります。

始める前に

少なくとも人物を 1 名追加し、その人物の認証モードを設定してください。詳細については、「*人物管理*」をご覧ください。

手順

1.**[入退室管理]** → **[高度な機能]** → **[詳細パラメータ]** の順にクリックし、[詳細パラメータ] ページを表示します。
2.左側のパネルでデバイスを選択します。
3.**[出勤ステータス]** をクリックします。
4.[出勤モード] を **[無効]** に設定します。
5.**[保存]** をクリックします。

結果

出勤ステータス機能を無効にすると、デバイスの最初のページで出勤ステータスの表示、設定ができなくなります。

出勤モードの手動設定

出勤モードを手動設定にすると、デバイスで出勤を記録する時にステータスを手動で選択できます。

始める前に

少なくとも人物を 1 名追加し、その人物の認証モードを設定してください。詳細については、「*人物管理*」をご覧ください。

手順

1.**[入退室管理]** → **[高度な機能]** → **[詳細パラメータ]** の順にクリックし、[詳細パラメータ] ページを表示します。
2.左側のパネルでデバイスを選択します。
3.**[出勤ステータス]** をクリックします。
4.[出勤モード] を **[手動]** に設定します。
5.**[出勤ステータスが必要]** が有効であることを確認してください。

注記

デフォルトでは **[出勤ステータスが必要]** は有効化されています。

6.ドロップダウンリストで、出勤ステータスのショートカットキーを設定します。
7.**[保存]** をクリックします。

結果

デバイスのキーパッド上でキーを押し、出勤ステータスと認証を選択します。定義したショートカットキーに応じて、その認証が設定済みの出勤ステータスとして記録されます。デバイスの最初のページで認証を行う場合、[Select Status（ステータスを選択）] ページを表示します。ステータスを選択して出勤を記録します。

注記

ステータスを 20 秒以内に選択しなかった場合は認証に失敗し、有効な出勤として記録されません。

出勤モードの自動設定

出勤モードを自動に設定すると、出勤ステータスと利用可能な期間を設定できます。設定したパラメータに応じて、出勤ステータスが自動的に変更されます。

始める前に

少なくとも人物を 1 名追加し、その人物の認証モードを設定してください。詳細については、「*人物管理*」をご覧ください。

手順

1.**[入退室管理]** → **[高度な機能]** → **[詳細パラメータ]** の順にクリックし、[詳細パラメータ] ページを表示します。
2.左側のパネルでデバイスを選択します。
3.**[出勤ステータス]** をクリックします。
4.[出勤モード] を **[自動]** に設定します。
5.**[出勤ステータスが必要]** が有効であることを確認してください。

注記

デフォルトでは **[出勤ステータスが必要]** は有効化されています。

6.出勤ステータスの利用可能な時間を設定します。
   1）カーソルを目的の時間に移動すると、有効化チェックボックスが表示されます。
   2）このチェックボックスにチェックを入れ、利用可能な時間を設定します。
   3）ページの任意の場所をクリックし、設定を確認します。設定した時間が白色で表示されます。
7.ドロップダウンリストで、出勤ステータスのショートカットキーを設定します。
8.**[保存]** をクリックします。
   設定した期間内で出勤ステータスが有効になります。

結果

デバイスの最初のページを表示すると、現在の出勤モードが表示されます。最初のページで認証を行うと、その認証は設定時間に応じて設定済み出勤ステータスとして記録されま

す。

例

[Up] キーをチェックイン、[Down] キーをチェックアウト、チェックインのスケジュールを月曜日 08:00、チェックアウトのスケジュールを月曜日 17:00 に設定した場合、その人物による月曜日 17:00 以前の有効な認証はチェックインとして、月曜日 17:00 以降の有効な認証はチェックアウトとして記録されます。

出勤モードの手動および自動設定

出勤モードを [手動および自動] に設定すると、設定したパラメータに従って出勤ステータスが自動的に変更されます。また、認証前に出勤ステータスを手動で変更することもできます。

始める前に

少なくとも人物を 1 名追加し、その人物の認証モードを設定してください。詳細については、「*人物管理*」をご覧ください。

手順

1.**[入退室管理]** → **[高度な機能]** → **[詳細パラメータ]** の順にクリックし、[詳細パラメータ] ページを表示します。
2.左側のパネルでデバイスを選択します。
3.**[出勤ステータス]** をクリックします。
4.[出勤モード] を **[手動および自動]** に設定します。
5.**[出勤ステータスが必要]** が有効であることを確認してください。

> **注記**
> デフォルトでは **[出勤ステータスが必要]** は有効化されています。

6.ステータスの有効期間を設定します。
7.出勤ステータスの利用可能な時間を設定します。
   1）カーソルを目的の時間に移動すると、有効化チェックボックスが表示されます。
   2）このチェックボックスにチェックを入れ、利用可能な時間を設定します。
   3）ページの任意の場所をクリックし、設定を確認します。設定した時間が白色で表示されます。
8.ドロップダウンリストで、出勤ステータスのショートカットキーを設定します。
9.**[保存]** をクリックします。
   設定した期間内で出勤ステータスが有効になります。

結果

デバイスの最初のページを表示すると、現在の出勤モードが表示されます。ステータスを選択しなかった場合、その認証は設定時間に応じて、設定済みの出勤ステータスとして記録されます。キーパッド上のキーを押して、ステータスを選択して出勤を記録すると、そ

の認証は選択済みの出勤ステータスとして記録されます。

例

[Up] キーをチェックイン、[Down] キーをチェックアウト、チェックイン時刻を月曜日 08:00、チェックアウト時刻を月曜日 17:00 に設定した場合、その人物による月曜日 17:00 以前の有効な認証はチェックインとして、月曜日 17:00 以降の有効な認証はチェックアウトとして記録されます。

19.7 入退室管理のリンクアクション設定

入退室管理デバイスが検出したイベントに対して、異なるリンクアクションを設定できます。設定後、イベント発生時にリンクアクションが作動します。この仕組みは、セキュリティ担当者に通知したり、リアルタイムで入退室管理デバイスを作動させたりするために使用します。

サポートされているリンクアクションは以下の 2 種類です。

- **クライアントアクション:** イベントが検出されると、クライアントによる音声警告など、クライアント側の動作を実行します。
- **デバイスアクション:** イベントが検出されると、カードリーダーのブザーやドアの開放 / 閉鎖など、特定デバイスの動作を実行します。

19.7.1 アクセスイベントに対するクライアントアクションの設定

アクセスポイントから遠く離れている場合も、アクセスイベントのクライアントアクションを設定することで、状況とイベントの緊急度をクライアント経由で把握できます。ここでのクライアントアクションは、音声による警告や電子メールの送信など、クライアント自身が自動的に実行する操作のことです。イベントがトリガーされると、クライアントはセキュリティ担当者に通知します。これにより、セキュリティ担当者は速やかにイベントを処理することができます。

手順

1.**[イベント設定]** → **[入退室管理イベント]** の順にクリックします。
追加した入退室管理デバイスがデバイスリストに表示されます。

2.デバイスリストからリソース（例: デバイス、アラーム入力、ドア / エレベータ、カードリーダー）を選択します。
選択したリソースがサポートしているイベントタイプが表示されます。

3.イベントを選択して **[優先度の編集]** をクリックし、そのイベントの優先度を定義します。
この設定は、[イベントセンター] でイベントをフィルタリングするために使用します。

4.選択したイベントのリンクアクションを設定します。
1）イベントを選択して、**[リンクを編集]** をクリックし、イベントがトリガーされたときのクライアントアクションを設定します。

音声による警告

イベントがトリガーされると、クライアントソフトウェアは音声による警告を発します。音声による警告のアラーム音を選択できます。

注記

アラーム音の設定の詳細については、「*アラーム音の設定*」をご覧ください。

電子メールを送信

イベントに関する電子メール通知を 1 つまたは複数の宛先に送信します。
電子メールのパラメータ設定の詳細については、「*電子メールのパラメータ設定*」をご覧ください。

ポップアップウィンドウ

イベントがトリガーされたときに、イベント情報（イベントの詳細、イベント関連のビデオ映像、イベント関連の画像など）を示すウィンドウがソフトウェアクライアントにポップアップ表示されます。

Display on Map（マップ上に表示）

イベントソースをマップ上にホットスポットとして追加すると、イベントがトリガーされたときにホットスポットが赤の数字（イベント数を示し、最大数は 10）とともに表示されます。これにより、セキュリティ担当者はイベントの場所を容易に確認することができます。
ホットスポットをクリックして、イベントの詳細と、リンクされたカメラのライブビデオを表示することもできます。

リンク済みカメラ

アクセスイベントがトリガーされたときに画像をキャプチャするには、選択したカメラをリンクします。
ドロップダウンリストでカメラを選択します。

2）**[OK]** をクリックします。

5. イベントを有効化すると、イベントの検出時にイベントがクライアントに送信され、リンクアクションが作動します。
6. オプション: **[コピー先]** をクリックして、イベント設定を他の入退室管理デバイス、アラーム入力、ドア / エレベータ、またはカードリーダーにコピーします。

19.7.2 アクセスイベントに対するデバイスアクションの設定

入退室管理デバイスの作動イベントに対して、入退室管理デバイスのリンクアクションを設定できます。その後、イベントがトリガーされると、アラーム出力、アクセスコントローラのブザー、およびその他の操作がトリガーされます。

手順

注記

デバイスがリンク操作をサポートしている必要があります。

1.**[入退室管理]** → **[リンク設定]** の順にクリックします。
2.左側のリストで入退室管理デバイスを選択します。
3.**[追加]** をクリックして新しいリンクを追加します。
4.イベントソースとして **[イベントリンク]** を選択します。
5. イベントの種類と詳細を選択してリンクを設定します。
6.[Linkage Target（リンクターゲット）] エリアでプロパティ対象を設定し、この動作を有効化します。

コントローラのブザー

入退室管理デバイスの音声警告が作動します。

キャプチャ

選択したイベントが発生すると、イベント関連の画像を取り込みます。

録画中

選択したイベントが発生すると、イベント関連の画像を取り込みます。

注記

使用するデバイスが録画機能に対応している必要があります。

リーダーのブザー

カードリーダーの音声警告が作動します。

アラーム出力

選択したイベントが発生したときに、通知のためにアラーム出力がトリガーされます。

アラーム入力

アラーム入力を有効化または解除します。

注記

デバイスがアラーム入力機能をサポートしている必要があります。

アクセスポイント

ドアの状態（開放、閉鎖、開放保持、または閉鎖保持）がトリガーされます。

注記

ターゲットドアとソースドアは同じにできません。

オーディオ再生

音声プロンプトが作動します。設定した再生モードに応じて、選択した音声インデックス関連の音声コンテンツが再生されます。

7.**[保存]** をクリックします。

8.オプション: デバイスのリンク設定を追加した後に、以下の操作を 1 つまたは複数実行できるようになります。

リンク設定の編集 デバイスリスト内で設定済みのリンク設定を選択すると、そのイベントソースのパラメータ（イベントソースやリンクターゲットなど）を編集できます。

リンク設定の削除 デバイスリスト内で設定済みのリンク設定を選択して **[削除]** をクリックすると、その設定を削除できます。

19.7.3 カードのスワイプ動作に対するデバイスアクションの設定

特定のカードのスワイプ動作に対して、入退室管理デバイスのリンク操作（ゾーンの警戒解除や音声プロンプトのトリガーなど）を有効にすることができます。これにより、カード所有者の行動と所在を監視できます。

手順

注記

使用するデバイスがこの機能に対応している必要があります。

1.**[入退室管理]** → **[リンク設定]** の順にクリックします。

2.左側のリストで入退室管理デバイスを選択します。

3.**[追加]** をクリックして新しいリンクを追加します。

4.イベントソースとして **[カードリンク]** を選択します。

5.カード番号を入力するか、ドロップダウンリストから該当するカードを選択します。

6.カードをスワイプするカードリーダーを選択します。
7.[Linkage Target（リンクターゲット）] エリアでプロパティ対象を設定し、この動作を有効化します。

コントローラのブザー
入退室管理デバイスの音声警告が作動します。

リーダーのブザー
カードリーダーの音声警告が作動します。

キャプチャ
選択したイベントが発生すると、イベント関連の画像を取り込みます。

録画中
選択したイベントが発生すると、イベント関連の画像を取り込みます。

注記
使用するデバイスが録画機能に対応している必要があります。

アラーム出力
通知用にアラーム出力が作動します。

アラーム入力
アラーム入力を有効化または解除します。

注記
デバイスがアラーム入力機能をサポートしている必要があります。

アクセスポイント
ドアのステータス（開放、閉鎖、開放保持、または閉鎖保持）が作動します。

オーディオ再生
音声プロンプトが作動します。設定した再生モードに応じて、選択した音声インデックス関連の音声コンテンツが再生されます。

8.**[保存]** をクリックします。
（手順 5 で設定した）カードを（手順 6 で設定した）カードリーダーにスワイプすると、（手順 7 で設定した）リンクアクションが作動します。
9.オプション: デバイスのリンク設定を追加した後に、以下の操作を 1 つまたは複数実行できるようになります。

リンク設定の削除　デバイスリスト内で設定済みのリンク設定を選択して **[削除]**

をクリックすると、その設定を削除できます。

リンク設定の編集 デバイスリスト内で設定済みのリンク設定を選択すると、そのイベントソースのパラメータ（イベントソースやリンクターゲットなど）を編集できます。

19.7.4 携帯端末の MAC アドレスのデバイスリンクの設定

携帯端末の指定された MAC アドレスに対して、入退室管理デバイスのリンク操作を設定できます。入退室管理デバイスが指定された MAC アドレスを検出すると、アラーム出力、ホストブザー、およびその他の操作がトリガーされます。

手順

注記

使用するデバイスがこの機能に対応している必要があります。

1. **[入退室管理]** → **[リンク設定]** の順にクリックします。
2. 左側のリストで入退室管理デバイスを選択します。
3. **[追加]** をクリックして新しいリンクを追加します。
4. イベントソースで **[Mac Linkage（MAC リンク）]** を選択します。
5. トリガーする MAC アドレスを入力します。

注記

MAC アドレスの形式は、AA:BB:CC:DD:EE:FF です。

6. [Linkage Target（リンクターゲット）] エリアでプロパティ対象を設定し、この動作を有効化します。

コントローラのブザー

入退室管理デバイスの音声警告が作動します。

リーダーのブザー

カードリーダーの音声警告が作動します。

キャプチャ

選択したイベントが発生すると、イベント関連の画像を取り込みます。

録画中

選択したイベントが発生すると、イベント関連の画像を取り込みます。

注記

使用するデバイスが録画機能に対応している必要があります。

アラーム出力

通知用にアラーム出力が作動します。

アラーム入力

アラーム入力を有効化または解除します。

注記

デバイスがアラーム入力機能をサポートしている必要があります。

アクセスポイント

ドアのステータス（開放、閉鎖、開放保持、または閉鎖保持）が作動します。

オーディオ再生

音声プロンプトが作動します。設定した再生モードに応じて、選択した音声インデックス関連の音声コンテンツが再生されます。

7.**[保存]** をクリックします。

8.オプション: デバイスのリンク設定を追加した後に、以下の操作を 1 つまたは複数実行できるようになります。

リンク設定の編集 デバイスリスト内で設定済みのリンク設定を選択すると、そのイベントソースのパラメータ（イベントソースやリンクターゲットなど）を編集できます。

リンク設定の削除 デバイスリスト内で設定済みのリンク設定を選択して **[削除]** をクリックすると、その設定を削除できます。

19.7.5 人物 ID に対するデバイスアクションの設定

特定の人物 ID に対して、入退室管理デバイスのリンクアクションを設定できます。入退室管理デバイスが特定の人物 ID を検出すると、アラーム出力やブザーなどの動作が実行され、その人物に対して特別のモニタリング体制が敷かれます。

手順

注記

使用するデバイスがこの機能に対応している必要があります。

1.**[入退室管理]** → **[リンク設定]** の順にクリックします。
2.左側のリストで入退室管理デバイスを選択します。
3.**[追加]** をクリックして新しいリンクを追加します。
4.イベントソースで **[Person Linkage（人物リンク）]** を選択します。
5.従業員番号を入力するか、ドロップダウンリストから該当する従業員を選択します。
6.カードをスワイプするカードリーダーを選択します。
7.[Linkage Target（リンクターゲット）] エリアでプロパティ対象を設定し、この動作を有効化します。

コントローラのブザー
入退室管理デバイスの音声警告が作動します。

リーダーのブザー
カードリーダーの音声警告が作動します。

キャプチャ
選択したイベントが発生すると、イベント関連の画像を取り込みます。

録画中
選択したイベントが発生すると、イベント関連の画像を取り込みます。

注記

使用するデバイスが録画機能に対応している必要があります。

アラーム出力
通知用にアラーム出力が作動します。

アラーム入力
アラーム入力を有効化または解除します。

注記

使用するデバイスがゾーン機能に対応している必要があります。

アクセスポイント

ドアのステータス（開放、閉鎖、開放保持、または閉鎖保持）が作動します。

オーディオ再生

音声プロンプトが作動します。設定した再生モードに応じて、選択した音声インデックス関連の音声コンテンツが再生されます。

8.**[保存]** をクリックします。

9.オプション: デバイスのリンク設定を追加した後に、以下の操作を 1 つまたは複数実行できるようになります。

リンク設定の削除 デバイスリスト内で設定済みのリンク設定を選択して **[削除]** をクリックすると、その設定を削除できます。

リンク設定の編集 デバイスリスト内で設定済みのリンク設定を選択すると、そのイベントソースのパラメータ（イベントソースやリンクターゲットなど）を編集できます。

19.8 ドア / エレベータ制御

[モニタリング] モジュールでは、追加した入退室管理デバイスで管理するドア / エレベータの状態をリアルタイムで確認できます。また、離れた場所からクライアントを経由して、ドアの開放 / 閉鎖やドアの開放保持 / 閉鎖保持など、ドアやエレベータを制御することもできます。このモジュールでは、アクセスイベントがリアルタイムで表示されます。アクセスの詳細と人物の詳細も確認できます。

注記

ドア / エレベータの制御権限を有するユーザーは、[モニタリング] モジュールでドア / エレベータを制御できます。また、ドアの制御アイコンは非表示になります。ユーザー権限の設定については、「*ユーザーの追加*」をご覧ください。

19.8.1 ドアステータスの制御

開放、閉鎖、開放保持、閉鎖保持など、1 つのドアのステータスを制御できます。

手順

1.**[モニタリング]** をクリックし、ステータスモニタリングのページを表示します。

2.右上隅でアクセスポイントのグループを選択します。

注記

入退室管理グループの管理については、「*グループ管理*」をご覧ください。

選択したアクセス制御グループ内のドアが表示されます。

3. ドアのアイコンをクリックしてドアを 1 つ選択するか、**[Ctrl]** を押しながら複数のドアを選択します。
4. 以下のボタンをクリックしてドアを制御します。

ドアを開放

ドアが施錠されている場合、解錠して一度開きます。開放期間の経過後、自動的にドアが閉じて施錠されます。

ドアを閉鎖

ドアが解錠されている場合、ドアを施錠するとドアが閉じます。アクセス認証の権限を有する人物は、認証情報を使用してドアにアクセスできます。

開放状態

（閉鎖または開放の場合を問わず）ドアは解錠されます。認証情報は不要で、すべての人がドアにアクセスできます。

閉鎖状態

ドアが閉じ、施錠されます。スーパーユーザーを除き、認証権限を有するユーザーでもドアにはアクセスできません。

キャプチャ

画像を手動でキャプチャします。

注記

使用するデバイスがキャプチャ機能に対応している場合にのみ、この**[キャプチャ]** ボタンを使用できます。キャプチャした画像は、クライアントを実行中の PC に保存されます。保存パスの設定については、「*ファイル保存先パスの設定*」をご覧ください。

結果

正常に動作すると、動作の内容に応じてドアのアイコンがリアルタイムで変更されます。

19.8.2 エレベータのステータス制御

エレベータドアの開放、管理下、自由、エレベータの呼び出しなど、追加したエレベータコントローラのステータスを制御できます。

手順

注記

- 他のクライアントで制御していない場合、現在のクライアントからエレベータを制御できます。エレベータのステータスが変更されると、他のクライアントソフトウェアからエレベータを制御できなくなります。
- 一度に 1 つのエレベータを制御できるクライアントソフトウェアは 1 つのみです。
- エレベータを制御するクライアントは、アラーム情報を受信してエレベータのステータスをリアルタイムで確認できます。

1.**[モニタリング]** をクリックし、ステータスモニタリングのページを表示します。
2.右上隅でアクセスポイントのグループを選択します。

注記

入退室管理グループの管理については、「*グループ管理*」をご覧ください。

選択したアクセスポイントグループ内のエレベータが表示されます。
3.ドアのアイコンをクリックし、エレベータを選択します。
4.以下のボタンをクリックしてエレベータを制御します。

ドアを開放

エレベータのドアが閉じている場合、ドアを開きます。開放期間の経過後、ドアは自動的に閉じます。

制御済み

目的のフロアボタンを押す前に、カードをスワイプする必要があります。その後、エレベータは目的のフロアに移動できるようになります。

無料

エレベータ内の選択したフロアボタンが常時有効になります。

無効

エレベータ内の選択したフロアボタンが無効になり、当該フロアに移動できなくなります。

結果

正常に動作すると、動作の内容に応じてドアのアイコンがリアルタイムで変更されます。

19.8.3 リアルタイムでアクセス記録を確認する

カードのスワイプ記録、顔認証記録、指紋比較記録などのアクセス記録がリアルタイムで表示されます。人物の情報や、アクセス中に撮影した画像を確認できます。

手順

1. **[モニタリング]** をクリックし、右上隅のドロップダウンリストからグループを選択します。
   選択したグループ内のドアに対するアクセス記録がリアルタイムで表示されます。カード番号、人物名、組織、イベント時刻など、詳細な記録を確認できます。
2. オプション: イベントのタイプとイベントのステータスにチェックを入れると、イベントの検出時にそのイベントをリスト内に表示できます。チェックの入っていないタイプまたはステータスのイベントはリストに表示されません。
3. オプション: **[最新のイベントを表示]** にチェックを入れると、最新のアクセス記録が選択され、記録リストの最上部に表示されます。
4. オプション: イベントをクリックすると、人物の画像（取り込み済みの画像とプロフィール）や人物番号、人物名、組織、電話番号、連絡先など、アクセスした人物の詳細を確認できます。

注記

撮影画像をダブルクリックして拡大すると、詳細を確認できます。

5. オプション: アクセスイベント表の列名を右クリックすると、実際の使用状況に応じてその列を表示または非表示にできます。

第 20 章 時間と出勤

[Time and Attendance（時間と出勤）] モジュールには、従業員の始業時刻と終業時刻を追跡およびモニタリングする機能に加えて、遅刻、早退、休憩時間、長期欠勤などの労働時間を完全に管理する機能も備わっています。

注記

このセクションでは、出勤レポートの作成前に設定しておく必要のある各種設定について説明します。これらの設定を行った後に記録されたアクセス記録については、そのデータ内での計算が行われます。

20.1 フローチャート

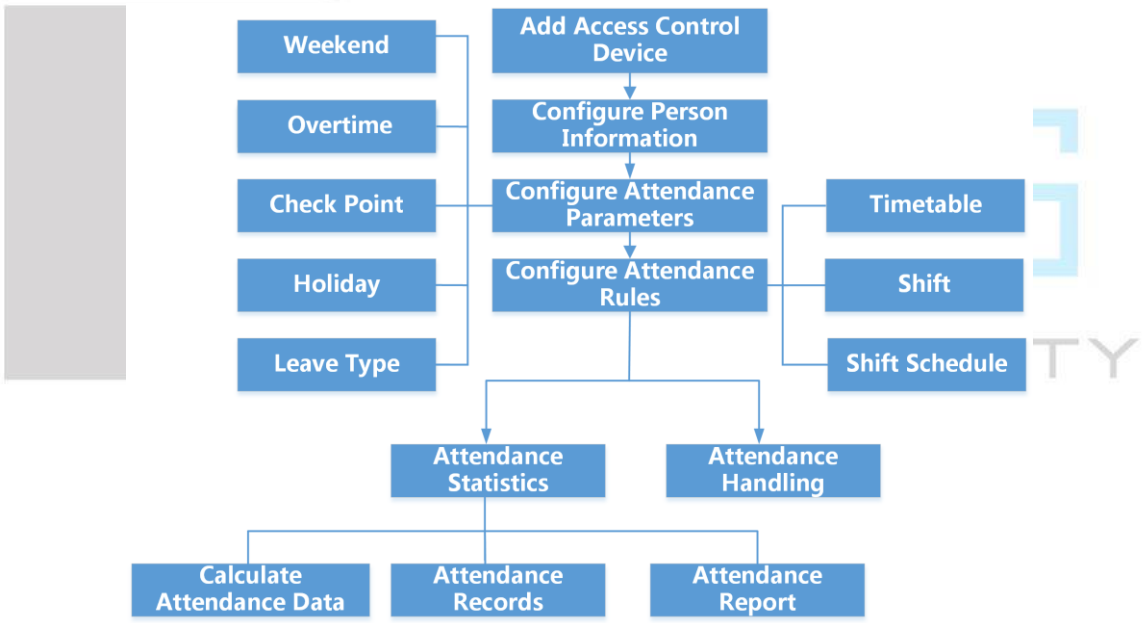

図 20-1 時間と出勤のフローチャート

- **入退室管理デバイスの追加:** クライアントに入退室管理デバイスを追加できます。詳細については、「*デバイスの追加*」をご覧ください。
- **人物情報の設定:** 時間と出勤のパラメータを設定する前に、クライアントに人物情報を追加する必要があります。詳細については、「*人物管理*」をご覧ください。
- **週末の設定:** クライアントで、実際の要件に応じて 1 日または複数の日を週末として選択できます。詳細については、「*週末の設定*」をご覧ください。
- **残業パラメータの設定:** 残業レベルや時給など、平日と週末の残業パラメータを設定できます。詳細については、「*残業パラメータの設定*」をご覧ください。

- **出勤チェックポイントの設定:** クライアントで、アクセスポイントのカードリーダーを出勤チェックポイントとして設定できます。詳細については、「*残業パラメータの設定*」をご覧ください。
- **休日の設定:** クライアントで、チェックインまたはチェックアウトが記録されない期間として休日を追加できます。詳細については、「*休日の設定*」をご覧ください。
- **休暇タイプの設定:** 実際の使用状況に応じて、休暇タイプをカスタマイズできます。詳細については、「*休暇タイプの設定*」をご覧ください。
- **タイムテーブルの追加:** 実際の使用状況に応じて、クライアントで、従業員の一般タイムテーブルとフレックスタイムテーブルを追加できます。詳細については、「*フレックスタイムテーブルの追加*」および「*一般タイムテーブルの追加*」をご覧ください。
- **シフトの追加:** シフト期間や出勤時間の設定など、従業員のシフトを追加できます。詳細については、「*シフトの追加*」をご覧ください。
- **シフトスケジュールの管理:** クライアントで、部門スケジュール、人物スケジュール、臨時スケジュールを設定できます。詳細については、「*シフトスケジュールの管理*」をご覧ください。
- **出勤データの計算:** クライアントは、出勤データを自動的に計算できます。また、手動で計算することもできます。詳細については、「*出勤データの計算*」をご覧ください。
- **出勤記録:** 出勤時間、出勤ステータス、チェックポイントなど、従業員の出勤記録をクライアントで検索して表示できます。詳細については、「*従業員の出勤データの概要の取得*」をご覧ください。
- **出勤レポート:** クライアントは、従業員の出勤結果を示す出勤レポートの生成をサポートしています。また、レポートの内容を事前定義して、電子メールで自動的にレポートを送信することもできます。詳細については、「*インスタントレポートの生成*」および「*レポートの定期送信*」をご覧ください。

20.2 出勤パラメータの設定

一般ルール、残業パラメータ、出勤チェックポイント、休日、休暇タイプなどの出勤パラメータを設定できます。

20.2.1 週末の設定

週末の曜日は国や地域によって異なる場合があります。クライアントは、週末定義機能を提供しています。実際の要件に応じて、週末として 1 つまたは複数の日を選択して、平日とは異なる週末の出勤ルールを設定できます。

手順

注記

ここで設定したパラメータは、新規に追加した時間帯でデフォルトとして設定されます。これは、既存の時間帯には影響を及ぼしません。

1.[Time & Attendance（時間と出勤）] モジュールを表示します。
2.**[出勤設定] → [一般ルール]** の順にクリックします。
3.週末の曜日（土曜日と日曜日など）を選択します。
4.**[保存]** をクリックします。

20.2.2 残業パラメータの設定

残業レベル、時給、残業の出勤ステータスなど、平日と週末の残業パラメータを設定できます。

手順

1.**[Time & Attendance（時間と出勤）] → [出勤設定] → [残業]** の順にクリックします。
2.必要な情報を設定します。

平日の残業レベル

平日の終業時刻以降の勤務に対しては、異なる残業レベル（残業レベル 1、残業レベル 2、残業レベル 3）が適用されます。残業レベルごとに異なる時給を設定できます。

時給

時給は、時給に残業レベルに設定されている値を掛けて勤務時間を計算するのに使用します。平日の終業時刻以降の勤務に対して、異なる残業レベルが適用できます。3 つの残業レベルごとに異なる時給（1～10、10 進数）を設定できます。例えば、残業レベル 1 での有効な残業時間が 1 時間で、残業時間レベル 1 の時給が 2 に設定されている場合、その期間の勤務時間は 2 時間として計算されます。

週末用残業ルール

週末用の残業ルールを有効化して計算モードを設定できます。

3.**[保存]** をクリックします。

20.2.3 出勤チェックポイントの設定

アクセスポイントのカードリーダーを出勤チェックポイントとして設定することで、カードリーダーの認証機能を使用して出勤状況を記録できます。

始める前に

出勤チェックポイントの設定前に、入退室管理デバイスを追加しておく必要があります。詳細については、「*デバイスの追加*」をご覧ください。

手順

注記

デフォルトでは、追加した入退室管理デバイスの全カードリーダーが出勤チェックポイントとして設定されています。

1.[Time & Attendance（時間と出勤）] モジュールを表示します。

2.**[出勤状況]** → **[出勤チェックポイント]** の順にクリックし、[Attendance Check Point Settings（出勤チェックポイント設定）] ページを表示します。

3.オプション: **[すべてのカードリーダーをチェックポイントとして設定]** のスイッチをオフにします。

リスト内のカードリーダーのみが出勤チェックポイントとして設定されます。

4.デバイスリスト内で、目的のカードリーダーを出勤チェックポイントに設定します。

5.チェックポイント機能を **[始業 / 終業]**、**[始業]**、または **[終業]** に設定します。

6.**[チェックポイントとして設定]** をクリックします。

右側のリストに、設定した出勤チェックポイントが表示されます。

20.2.4 休日の設定

休日を追加して、その期間中はチェックインまたはチェックアウトを記録しないように設定できます。

定期休日の追加

1 年のうちで元日、独立記念日、クリスマスなど、有効期間中に定期休日となる休日を設定できます。

手順

1.[Time & Attendance（時間と出勤）] モジュールを表示します。

2.**[出勤設定]** → **[休日]** の順にクリックし、[休日設定] ページを表示します。

3.休日タイプで **[定期休日]** にチェックを入れます。
4.休日の名前をカスタマイズします。
5.休日の開始日を設定します。
6.休日の日数を入力します。
7.従業員が休日に勤務する場合、出勤ステータスを設定します。
8.オプション: **[毎年繰り返し]** にチェックを入れると、その休日の設定を毎年繰り返し適用できます。
9.**[OK]** をクリックします。
追加した休日は、休日リストとカレンダーに表示されます。
その日付が異なる祝日として選択された場合、最初に追加した休日として記録されます。
10.オプション: 休日の追加後に、以下の操作のうち 1 つを実行します。

休日を編集	をクリックし、休日情報を編集します。
休日を削除	1 つ以上の休日を選択して **[削除]** をクリックし、休日リストからその休日を削除します。

不定休日の追加

毎年の法定休日など、有効期間中に不定期で定休日になる休日を設定できます。

手順

1.[Time & Attendance（時間と出勤）] モジュールを表示します。
2.**[出勤設定]** → **[休日]** の順にクリックし、[休日設定] ページを表示します。
3.**[追加]**をクリックして [休日を追加] ページを表示します。
4.休日タイプで **[不定期休日]** にチェックを入れます。
5.休日の名前をカスタマイズします。
6.休日の開始日を設定します。

例

2019 年 11 月第 4 木曜日を感謝祭として祝日に設定する場合、ドロップダウンリストから 2019 年 11 月の第 4 木曜日を選択します。

7.休日の日数を入力します。
8.従業員が休日に勤務する場合、出勤ステータスを設定します。
9.オプション: **[毎年繰り返し]** にチェックを入れると、その休日の設定を毎年繰り返し適用できます。
10.**[OK]** をクリックします。
追加した休日は、休日リストとカレンダーに表示されます。
その日付が異なる祝日として選択された場合、最初に追加した休日として記録されます。
11.オプション: 休日の追加後に、以下の操作のうち 1 つを実行します。

休日を編集	をクリックし、休日情報を編集します。

休日を削除　　1 つ以上の休日を選択して **[削除]** をクリックし、休日リストからその休日を削除します。

20.2.5 休暇タイプの設定

実際の使用状況に応じて、休暇タイプ（主要タイプと二次タイプ）をカスタマイズできます。休暇タイプは編集または削除することもできます。

手順

1.[Time & Attendance（時間と出勤）] モジュールを表示します。
2.**[出勤設定]** → **[休暇タイプ]** の順にクリックし、[休暇タイプ設定] ページを表示します。
3.左側の **[追加]** をクリックし、主要な休暇タイプを追加します。
4.オプション: 主要な休暇タイプに対して、以下の操作のうち 1 つを実行します。

編集　　主要な休暇タイプの上にカーソルを合わせて、をクリックし、主要な休暇タイプを編集します。

削除　　1 つの主要な休暇タイプを選択し、左側の **[削除]** をクリックして主要な休暇タイプを削除します。

5.右側の **[追加]** をクリックし、二次の休暇タイプを追加します。
6.オプション: 二次の休暇タイプに対して、以下の操作のうち 1 つを実行します。

編集　　二次の休暇タイプの上にカーソルを合わせて、をクリックし、二次の休暇タイプを編集します。

削除　　二次の休暇タイプを 1 つ以上選択して右側の **[削除]** をクリックし、選択した二次の休暇タイプを削除します。

20.2.6 サードパーティ製データベースとの認証記録の同期

他のシステムでクライアントソフトウェア内の出勤データ記録を使用して計算などの処理を実行させることができます。同期機能を有効化して、クライアントソフトウェアからの認証記録をサードパーティ製データベースに自動適用できます。

手順

1.[Time & Attendance（時間と出勤）] モジュールを表示します。
2.**[出勤設定]** → **[サードパーティデータベース]** の順にクリックします。
3.**[データベースに適用]** のスイッチをオンにして同期機能を有効化します。
4. データベースのタイプとして **SQLServer** または **MySql** を選択します。

注記

MySql を選択した場合は、ローカル PC から設定ファイル（libmysql.dll）をインポートする必要があります。

5.サードパーティ製データベースのその他の必要なパラメータ（サーバーの IP アドレス、データベース名、ユーザー名、パスワードなど）を設定します。
6.実際の設定状況に応じて、データベース表のパラメータを設定します。
1）サードパーティ製データベースの表名を入力します。
2）クライアントソフトウェアとサードパーティ製データベース間でマッピング済みの表フィールドを設定します。
7.**[保存]** をクリックし、データベースに接続して正常に設定を保存できるかテストします。
- 出勤データがサードパーティ製データベースに書き込まれます。
- 同期中にクライアントがサードパーティ製データベースとの接続を切断すると、クライアントは 30 分ごとに再接続を開始します。再接続後、クライアントは切断期間中に記録されたデータをサードパーティ製データベースと同期します。

20.2.7 出勤計算精度の設定

出勤計算の最小単位や丸め制御ルールなど、さまざまな出勤項目の出勤計算精度を設定して、出勤データを正確に計算できます。例えば、休暇期間の最小単位を 1 時間に設定し、丸め制御ルールを切り上げに設定できます。

手順

1.[Time & Attendance（時間と出勤）] モジュールを表示します。
2.**[出勤設定] → [一般ルール]** の順にクリックします。
3.[高度な機能] エリアで、さまざまな統計項目の最小単位（分、時間、平日など）を設定します。
4.さまざまな統計項目の丸め制御ルール（切り捨て、四捨五入、切り上げなど）を設定します。
5.**[表示形式]** を **[MM]** または **[HH:MM]** に設定します。
6.**[保存]** をクリックします。

例

最小単位を 1 時間に設定して、残業時間の丸め制御ルールを切り捨てに設定すると、残業時間が 1 時間未満の場合は 0 として計算されます。残業時間が 1.5 時間の場合は、1 時間として計算されます。

20.2.8 休憩時間の設定

休憩時間を追加して、開始時刻、終了時刻、継続時間、計算モードなどの休憩パラメータを設定できます。追加した休憩時間は編集したり削除したりできます。

手順

1.**[Time & Attendance（時間と出勤）]** → **[タイムテーブル]** の順にクリックします。
追加したタイムテーブルがリストに表示されます。
2.追加したタイムテーブルを選択するか、**[追加]** をクリックしてタイムテーブルの設定ページを表示します。
3.**[休憩時間]** をクリックして、[休憩時間] ページを表示します。
4.**[Break Time Settings（休憩時間の設定）]** をクリックします。
5.休憩時間を追加します。
1）**[追加]** をクリックします。
2）休憩時間の名前を入力します。
3）休憩時間の関連パラメータを設定します。

開始時刻 / 終了時刻

休憩の開始時刻と終了時刻を設定します。

以降 / 以前

休憩開始の最も早いスワイプ対応時間と休憩終了の最も遅いスワイプ対応時間を設定します。

休憩継続時間

休憩の開始時刻から終了時刻までの時間を示します。

計算

Auto Deduct（自動控除）

指定した休憩時間を勤務時間から控除します。

Must Check（確認必須）

休憩時間を計算して、実際のチェックインとチェックアウト時刻に応じて勤務時間から休憩時間を控除します。

注記

計算方法で **[Must Check（確認必須）]** を選択した場合、休憩から遅くまたは早く戻る時の出勤ステータスを設定しておく必要があります。

6.**[保存]** をクリックして設定を保存します。
7.オプション: **[追加]** をクリックし、休憩時間の追加を継続します。

20.3 一般タイムテーブルの追加

タイムテーブルページでは、従業員の一般タイムテーブルを追加できます。これには、固定された始業時刻と終業時刻が必要です。また、有効なチェックイン / チェックアウト時間、遅延および早退の許容タイムテーブルを設定することもできます。

手順

1.**[Time and Attendance（時間と出勤）]** → **[タイムテーブル]** の順にクリックし、タイムテーブルの設定ページを表示します。
2.**[追加]** をクリックして、タイムテーブルの追加ページを表示します。

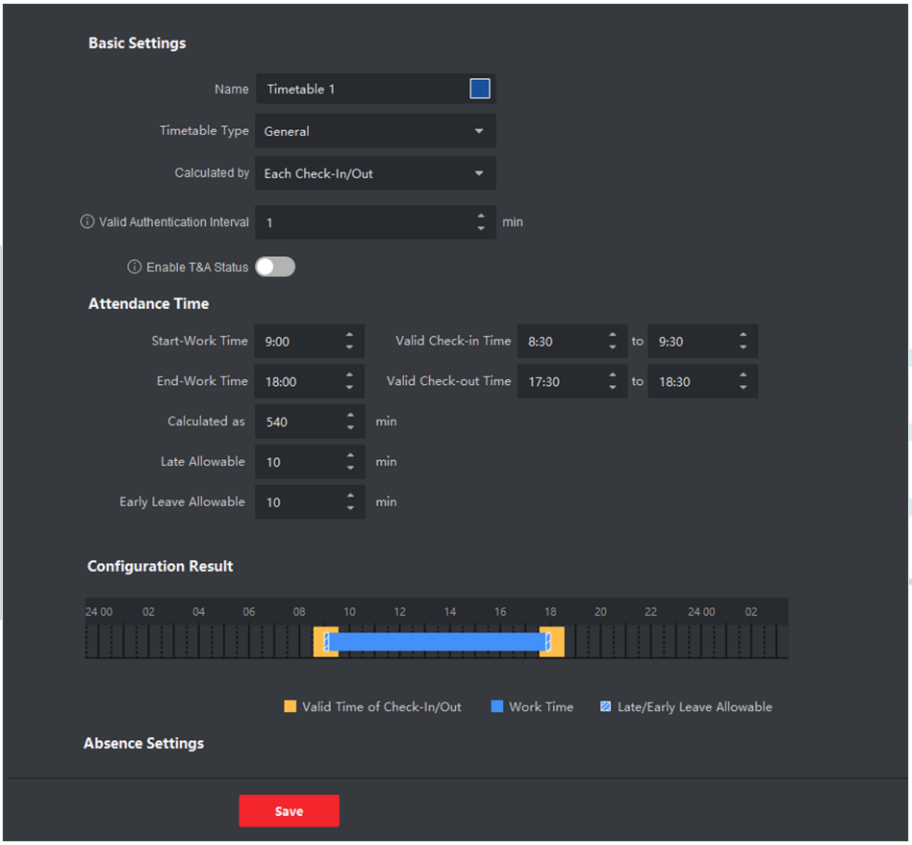

図 20-2 タイムテーブルの追加

3.タイムテーブルの名前を作成します。

注記

名前の横にある色アイコンをクリックして、[設定結果] エリアのタイムバー上の有効なタイムテーブルに使用する色をカスタマイズできます。

4.タイムテーブルのタイプとして一般を選択します。
5.計算方法を選択します。

最初のチェックインと最終チェックアウト

最初のチェックイン時刻が始業時刻として、最後のチェックアウト時刻が終業時刻として記録されます。

各チェックイン / アウト

各チェックイン時刻とチェックアウト時刻が有効である場合、隣接するチェックイン時刻とチェックアウト時刻の間の時間の合計が有効な勤務時間として記録されます。この計算方法では、**[Valid Authentication Interval（有効な認証間隔）]** を設定する必要があります。例えば、同じカードのスワイプ間隔が設定値より短い場合、カードのスワイプが無効になります。

6.オプション: **[T&A ステータスの有効化]** スイッチをオンにし、デバイスの出勤ステータスに応じて計算します。

注記

使用するデバイスがこの機能に対応している必要があります。

7.関連する出勤時間パラメータを次のように設定します。

始業/終業時間

始業時刻と終業時刻を設定します。

有効なチェックイン / アウト時刻

タイムバー上で黄色のバーを調整し、チェックインまたはチェックアウトの時刻が有効なタイムテーブルを設定します。

計算対象

実際の勤務時間として計算する継続時間を設定します。

遅刻 / 早退許容

遅刻 / 早退が許容範囲内となるタイムテーブルを設定します。

8.欠勤関連パラメータを設定します。

Check-In, Late for（チェックイン、遅刻許容時間）

チェックインしたが、遅刻した従業員の遅刻許容時間を設定できます。従業員が許容時間よりも遅く出社した場合、出勤データは欠勤とマークされます。

Check-Out, Early Leave for（チェックアウト、早退許容時間）

通常の退社時間より前にチェックアウトした従業員の早退許容時間を設定できます。許容時間よりも早く退社した場合、出勤データは欠勤とマークされます。

No Check-in（チェックイン未実行）

従業員がチェックインしない場合、出勤データは欠勤または遅刻とマークされます。

No Check-Out（チェックアウト未実行）

従業員がチェックアウトしない場合、出勤データは欠勤または早退とマークされます。

9.**[保存]** をクリックし、タイムテーブルを追加します。

10.オプション: タイムテーブルの追加後、以下の 1 つまたは複数の操作を実行します。

タイムテーブルの編集	リストからタイムテーブルを選択し、関連情報を編集します。
タイムテーブルの削除	リストからタイムテーブルを選択し、**[削除]** をクリックして削除します。

20.4 フレックスタイムテーブルの追加

タイムテーブルページで、従業員のフレックスタイムテーブルを追加できます。フレックスタイムテーブルでは、チェックイン / チェックアウト時刻は必要ありませんが、設定した始業時刻以降の従業員の勤務時間が事前定義した勤務時間以上である必要があります。

手順

1.**[Time and Attendance（時間と出勤）]** → **[タイムテーブル]** の順にクリックし、タイムテーブルの設定ページを表示します。
2.**[追加]** をクリックして、タイムテーブルの追加ページを表示します。
3.タイムテーブルの名前を作成します。

注記

名前の横にある色アイコンをクリックして、タイムバー上の有効なタイムテーブルに使用する色をカスタマイズできます。

4.タイムテーブルのタイプとしてフレックスを選択します。

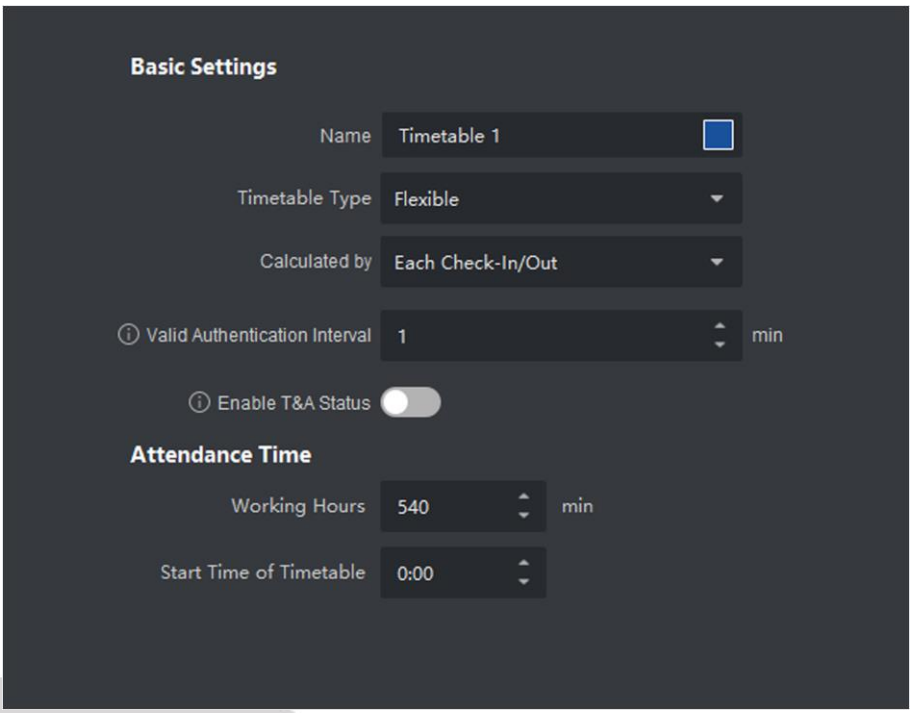

図 20-3 フレックスタイムテーブルの追加

5.計算方法を選択します。

最初のチェックインと最終チェックアウト

最初のチェックイン時刻が始業時刻として、最後のチェックアウト時刻が終業時刻として記録されます。

各チェックイン / アウト

各チェックイン時刻とチェックアウト時刻が有効である場合、隣接するチェックイン時刻とチェックアウト時刻の間の時間の合計が有効な勤務時間として記録されます。この計算方法では、**[Valid Authentication Interval（有効な認証間隔）]** を設定する必要があります。例えば、同じカードのスワイプ間隔が設定値より短い場合、カードのスワイプが無効になります。

6.オプション: **[T&A ステータスの有効化]** スイッチをオンにし、デバイスの出勤ステータスに応じて計算します。

注記

使用するデバイスがこの機能に対応している必要があります。

7.関連する出勤時間パラメータを次のように設定します。

勤務時間

従業員の勤務時間は設定値以上でなければなりません。

タイムテーブルの開始時刻

設定値に基づいて、各日の勤務時間を計算します。
例えば、勤務時間を 8 時間、タイムテーブルの開始時刻を 9:00 am とし、スタッフ A のチェックイン時間を 8:00 am、チェックアウト時間を 5:00 pm（有効な勤務時間は 9:00 am から 5:00 pm までの計 8 時間）と仮定します。その場合、スタッフ A の出勤結果は標準的なケースとして計算されます。

8.**[保存]** をクリックし、タイムテーブルを追加します。
9.オプション: タイムテーブルの追加後、以下の 1 つまたは複数の操作を実行します。

タイムテーブルの編集	リストからタイムテーブルを選択し、関連情報を編集します。
タイムテーブルの削除	リストからタイムテーブルを選択し、**[削除]** をクリックして削除します。

20.5 シフトの追加

シフト期間（日、週、月）や出勤時間の設定など、従業員のシフトを追加できます。実際の要件に応じて、従業員の 1 つのシフトに複数のタイムテーブルを追加できます。この場合、従業員は各タイムテーブルでチェックインおよびチェックアウトする必要があります。

始める前に

最初にタイムテーブルを追加します。詳細については、「*一般タイムテーブルの追加*」をご覧ください。

手順

1.**[Time and Attendance（時間と出勤）]** → **[シフト]** の順にクリックし、シフトの設定ページを表示します。
2.**[追加]** をクリックし、[シフトの追加] ページを表示します。
3.シフトの名前を入力します。
4.ドロップダウンリストからシフト期間を選択します。
5.追加したタイムテーブルを選択し、タイムバーをクリックしてタイムテーブルを適用します。

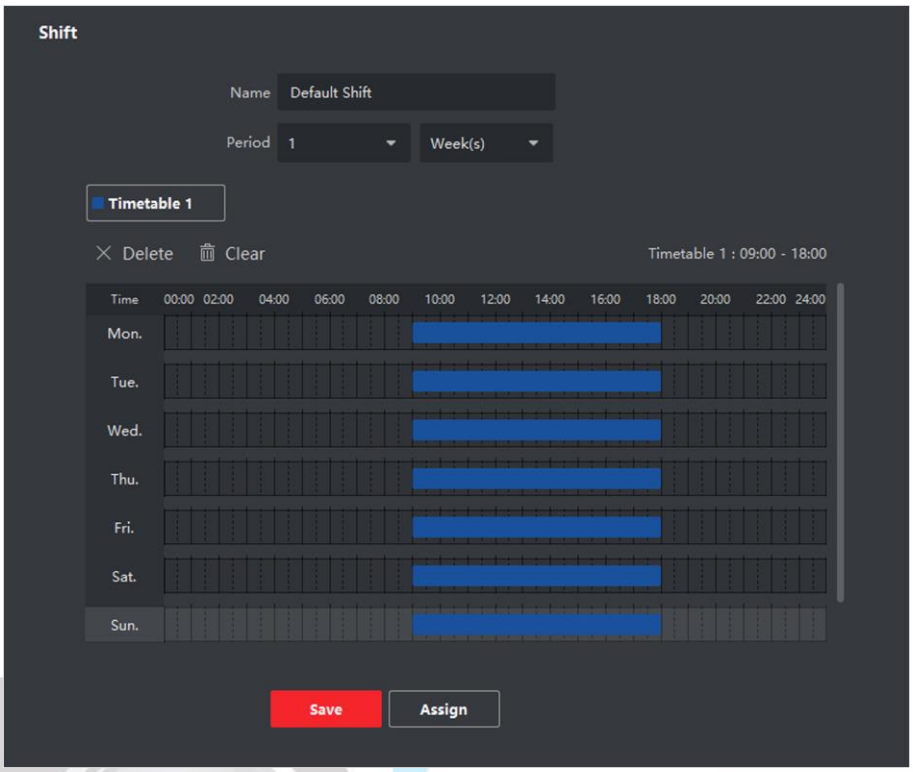

図 20-4 シフトの追加

注記

複数のタイムテーブルを選択できます。それぞれのタイムテーブルの始業および終業時刻と有効なチェックインおよびチェックアウト時刻を重ねることはできません。

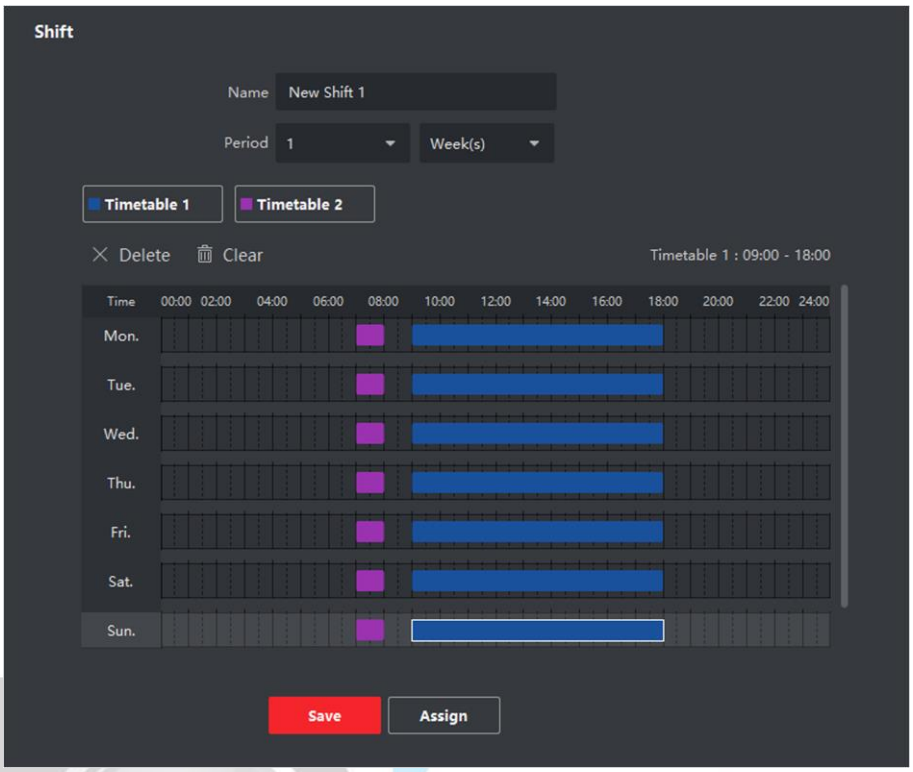

図 20-5 複数のタイムテーブルの追加

6.**[保存]** をクリックします。

追加したシフトがページ左側のパネルに一覧表示されます。最大 64 件のシフトを追加できます。

7.オプション: シフトを組織または人物に割り当てて、クイックシフトスケジュールを作成します。

1）**[割り当て]** をクリックします。

2）**[組織]** または **[人物]** タブを選択し、目的の組織または人物のボックスにチェックを入れます（複数選択可）。

選択した組織または人物がページの右側に表示されます。

3）シフトスケジュールの有効期限を設定します。

4）スケジュールのその他のパラメータを設定します。

チェックイン不要

このスケジュールの人物は、出社したときにチェックインする必要はありません。

チェックアウト不要

このスケジュールの人物は、退社するときにチェックアウトする必要はありません。

Scheduled on Holidays（スケジュールは休日も有効）

このスケジュールは休日も有効で、人物はスケジュールに従って出社する必要があります。

超過勤務に対して有効

このスケジュールで、人物の残業時間が記録されます。

5）**[保存]** をクリックし、クイックシフトスケジュールを保存します。

20.6 シフトスケジュールの管理

交代勤務とは、1 週間の各日で 24 時間を有効に活用するための勤務制度です。この勤務制度では 1 日を複数のシフトに分割し、各シフトに割り当てる時間を設定します。
部門のスケジュール、従業員のスケジュール、臨時スケジュールを設定できます。

20.6.1 部門スケジュールの設定

部門のシフトスケジュールを設定することで、その部門の全従業員にそのシフトスケジュールが割り当てられます。

始める前に

[Time & Attendance（時間と出勤）] モジュールでは、部門リストは組織と同じになります。最初に [人物] モジュールで組織と人物を追加する必要があります。詳細については、「*人物管理*」をご覧ください。

手順

1. **[Time and Attendance（時間と出勤）]** → **[シフトスケジュール]** の順にクリックし、シフトのスケジュールの管理ページを表示します。
2. **[部門スケジュール]** をクリックし、[部門スケジュール] ページを表示します。
3. 左側の組織リストから部門を選択します。

> **注記**
> 組織を選択する時に **[下部組織を含む]** にチェックが入っている場合、下部組織も同時に選択されます。

4. ドロップダウンリストからシフトを選択します。
5. オプション: **[複数のシフトスケジュール]** を有効にして、追加したタイムテーブルから有効な期間を選択します。

> **注記**
> これは、タイムテーブルが 1 つだけのシフトでのみ使用できます。

Multiple Shift Schedules（複数のシフトスケジュール）

ここには複数のタイムテーブルが含まれています。その人物は、タイムテーブル内の任意の時点でチェックイン / チェックアウトでき、出勤も記録されます。
複数のシフトスケジュールに 3 つのタイムテーブルが含まれている場合（00:00～07:00、08:00～15:00、16:00～23:00）は次のようになります。この複数のシフトスケジ

ュールが適用される人物は、3 つのタイムテーブルのどの時点で出勤しても記録されます。その人物が 07:50 にチェックインする場合、直近のタイムテーブルである 08:00～15:00 に出勤が記録されます。

6.開始日と終了日を設定します。
7.スケジュールのその他のパラメータを設定します。

チェックイン不要

このスケジュールの人物は、出社したときにチェックインする必要はありません。

チェックアウト不要

このスケジュールの人物は、退社するときにチェックアウトする必要はありません。

Scheduled on Holidays（スケジュールは休日も有効）

このスケジュールは休日も有効で、人物はスケジュールに従って出社する必要があります。

超過勤務に対して有効

このスケジュールで、人物の残業時間が記録されます。

8.**[保存]** をクリックします。

20.6.2 人物スケジュールの設定

1 名または複数名にシフトスケジュールを割り当てることができます。その人物のスケジュール詳細も確認して編集できます。

始める前に

[人物] モジュールに部門と人物を追加します。詳細については、「*人物管理*」をご覧ください。

手順

注記

人物のスケジュールは、部門のスケジュールよりも優先されます。

1.**[Time & Attendance（時間と出勤）]** → **[シフトスケジュール]** の順にクリックして、[シフトスケジュール] ページを表示します。
2.**[Person Schedule（人物スケジュール）]** をクリックし、[Person Schedule（人物スケジュール）] ページを表示します。
3.組織と人物を選択します。
4.ドロップダウンリストからシフトを選択します。
5.オプション: **[複数のシフトスケジュール]** を有効にして、追加したタイムテーブルから有効な期間を選択します。

注記

これは、タイムテーブルが 1 つだけのシフトでのみ使用できます。

Multiple Shift Schedules（複数のシフトスケジュール）

ここには複数のタイムテーブルが含まれています。その人物は、タイムテーブル内の任意の時点でチェックイン / チェックアウトでき、出勤も記録されます。
複数のシフトスケジュールに 3 つのタイムテーブルが含まれている場合（00:00～07:00、08:00～15:00、16:00～23:00）は次のようになります。この複数のシフトスケジュールが適用される人物は、3 つのタイムテーブルのどの時点で出勤しても記録されます。その人物が 07:50 にチェックインする場合、直近のタイムテーブルである 08:00～15:00 に出勤が記録されます。

6.開始日と終了日を設定します。
7.スケジュールのその他のパラメータを設定します。

チェックイン不要

このスケジュールの人物は、出社したときにチェックインする必要はありません。

チェックアウト不要

このスケジュールの人物は、退社するときにチェックアウトする必要はありません。

Scheduled on Holidays（スケジュールは休日も有効）

このスケジュールは休日も有効で、人物はスケジュールに従って出社する必要があります。

超過勤務に対して有効

このスケジュールで、人物の残業時間が記録されます。

8.**[保存]** をクリックします。

20.6.3 臨時スケジュールの設定

従業員に臨時スケジュールを追加し、臨時のシフトスケジュールを割り当てることができます。その臨時スケジュールの詳細を確認して編集することもできます。

始める前に

[人物] モジュールに部門と人物を追加します。詳細については、「*人物管理*」をご覧ください。

手順

注記

臨時スケジュールは、部門スケジュールや人物スケジュールよりも優先されます。

1.**[Time and Attendance（時間と出勤）]** → **[シフトスケジュール]** の順にクリックし、シフトのスケジュールの管理ページを表示します。
2.**[Temporary Schedule（臨時スケジュール）]** をクリックし、[Temporary Schedule（臨時スケジュール）] ページを表示します。
3.組織と人物を選択します。
4.臨時スケジュール用に、1 つの日付をクリックするか、ドラッグして複数の日付を選択します。
5.ドロップダウンリストから**[勤務日]** または **[非番日]** を選択します。

[非番日] を選択した場合、以下のパラメータを設定する必要があります。

計算対象

臨時スケジュールに標準レベルと残業レベルのどちらで出勤ステータスを記録するかを選択します。

タイムテーブル

ドロップダウンリストからタイムテーブルを選択します。

複数のシフトスケジュール

ここには複数のタイムテーブルが含まれています。その人物は、タイムテーブル内の任意の時点でチェックイン / チェックアウトでき、出勤も記録されます。
複数のシフトスケジュールに 3 つのタイムテーブルが含まれている場合（00:00～07:00、08:00～15:00、16:00～23:00）は次のようになります。この複数のシフトスケジュールが適用される人物は、3 つのタイムテーブルのどの時点で出勤しても記録されます。その人物が 07:50 にチェックインする場合、直近のタイムテーブルである 08:00～15:00 に出勤が記録されます。

ルール

[Check-in Not Required（チェックイン不要）]、**[Check-out Not Required（チェックアウト不要）]** など、スケジュールに適用する他のルールを設定します。

6.**[保存]** をクリックします。

20.6.4 シフトスケジュールの確認

カレンダーモードまたはリストモードでシフトスケジュールを確認できます。シフトスケジュールを編集または削除することもできます。

手順

1.**[Time and Attendance（時間と出勤）]** → **[シフトスケジュール]** の順にクリックし、シフトのスケジュールの管理ページを表示します。
2.組織と該当する人物を選択します。
3.または をクリックして、カレンダーモードまたはリストモードでシフトスケジュールを表示します。

カレンダー

カレンダーモードでは、1 ヵ月内の各日のシフトスケジュールを確認できます。臨時スケジュール内の特定の日付をクリックして、編集または削除することもできます。

リスト

リストモードでは、シフト名、タイプ、有効期間など、特定の人物または組織についてシフトスケジュールの詳細を確認できます。シフトスケジュールにチェックを入れて **[削除]** をクリックすると、選択したシフトスケジュールを削除できます（複数選択可）。

20.7 チェックイン / チェックアウト記録を手動で修正する

出勤ステータスが正しくない場合、チェックイン / チェックアウト記録を手動で修正できます。チェックイン / チェックアウト記録を編集、削除、検索、エクスポートすることもできます。

始める前に

- [人物] モジュールで組織と人物を追加する必要があります。詳細については、「*人物管理*」をご覧ください。
- その人物の出勤ステータスが正しくない場合。

手順

1.**[Time and Attendance（時間と出勤）]** → **[出勤処理]** の順にクリックし、出勤処理のページを表示します。
2.**[Correct Check-In/Out（チェックイン / チェックアウトを修正）]** をクリックし、チェックイン / チェックアウトの修正ページを表示します。
3.左側のリストから修正する人物を選択します。
4.修正する日付を選択します。
5.チェックイン / チェックアウトの修正パラメータを設定します。
[チェックイン] を選択して正しい始業時刻に設定します。**[チェックアウト]** を選択して正しい終業時刻に設定します。

注記

をクリックすると、複数のチェックイン / チェックアウト項目を追加できます。最大 8 件のチェックイン / チェックアウト項目に対応しています。

6.オプション: 必要に応じて注記を入力します。
7.**[保存]** をクリックします。
8.オプション: チェックイン / チェックアウトの修正後に、以下の操作のうち 1 つを実行します。

表示	または をクリックして、カレンダーモードまたはリストモードに追加済みの出勤処理情報を表示します。
	注記 カレンダーモードで 1 ヵ月内の出勤ステータスを取得するには、**[計算]** をクリックする必要があります。
編集	● カレンダーモードで、日付の関連ラベルをクリックして詳細を編集します。 ● リストモードで [日付]、[処理タイプ]、[時間]、または [注記] 列内の関連フィールドをダブルクリックし、その情報を編集します。
削除	選択した項目を削除します。
エクスポート	出勤処理の詳細をローカル PC にエクスポートします。
	注記 エクスポートした詳細情報は CSV 形式で保存されます。

20.8 休暇と出張の追加

従業員が休暇または出張を申し出た場合、休暇と出張を追加できます。

始める前に

[人物] モジュールで組織と人物を追加する必要があります。詳細については、「*人物管理*」をご覧ください。

手順

1.**[Time and Attendance（時間と出勤）]** → **[出勤処理]** の順にクリックし、出勤処理のページを表示します。
2.**[休暇 / 出張の適用]** をクリックし、休暇 / 出張の追加ページを表示します。
3.左側のリストから人物を選択します。
4.休暇または出張の日付を設定します。
5.ドロップダウンリストから主要な休暇タイプと二次の休暇タイプを選択します。

注記

[出勤設定] で休暇のタイプを設定できます。詳細については、「*休暇タイプの設定*」をご覧ください。

6.休暇の期間を設定します。
7.オプション: 必要に応じて注記を入力します。
8.**[保存]** をクリックします。
9.オプション: 休暇または出張の追加後に、以下の操作のうち 1 つを実行します。

表示	または をクリックして、カレンダーモードまたはリストモードに追加済みの出勤処理情報を表示します。 **注記** カレンダーモードで 1 ヵ月内の出勤ステータスを取得するには、**[計算]** をクリックする必要があります。
編集	● カレンダーモードで、日付の関連ラベルをクリックして詳細を編集します。 ● リストモードで [日付]、[処理タイプ]、[時間]、または [注記] 列内のフィールドをダブルクリックし、関連情報を編集します。
削除	選択した項目を削除します。
エクスポート	出勤処理の詳細をローカル PC にエクスポートします。 **注記** エクスポートした詳細情報は CSV 形式で保存されます。

20.9 出勤データの計算

出勤データ、従業員の詳細な出勤データ、従業員の異常な出勤データ、従業員の残業データ、およびカードのスワイプログの概要を検索および閲覧する前に、出勤データを計算する必要があります。

20.9.1 出勤データの自動計算

クライアントが設定した時間に出勤データを毎日自動で計算するように、スケジュールを設定できます。

手順

注記

計算されるのは前日までの出勤データです。

1.[Time & Attendance（時間と出勤）] モジュールを表示します。
2.**[出勤設定]** → **[一般ルール]** の順にクリックします。
3.[Auto-Calculate Attendance（出勤データの自動計算）] エリア内で、クライアントにデータを毎日計算させる時刻を設定します。
4.**[保存]** をクリックします。

20.9.2 出勤データの手動計算

データ範囲を設定することで、出勤データを手動で計算できます。

手順

1.[Time & Attendance（時間と出勤）] モジュールを表示します。
2.**[出勤統計]** → **[計算]** の順にクリックします。
3.開始時刻と終了時刻を設定し、出勤データの範囲を定義します。
4.部門、名前、人物 ID、出勤ステータスなどのその他の条件を設定します。
5.**[計算]** をクリックします。

注記

過去 3 ヵ月以内の出勤データのみを計算できます。

6.以下の操作のうち 1 つを実行します。

チェックイン/アウトを修正	**[Correct Check-In/Out（チェックイン / チェックアウトを修正）]** をクリックし、チェックイン / チェックアウトの修正を追加します。

表示する項目を選択	をクリックするか、別の項目のタイトルを右クリックして、レポートに表示する項目を選択します。
レポートを生成	**[レポート]** をクリックし、出勤レポートを生成します。
レポートをエクスポート	**[エクスポート]** をクリックし、出勤データをローカル PC にエクスポートします。

注記

エクスポートした詳細情報は CSV 形式で保存されます。

20.10 出勤統計

出勤データの計算結果に基づいて、元の出勤記録を確認したり、出勤レポートを生成およびエクスポートしたりできます。

20.10.1 従業員の出勤データの概要の取得

出勤時間、出勤ステータス、チェックポイントなど、クライアント上の従業員の出勤記録を検索して表示できます。

始める前に

- [人物] モジュールで組織と人物を追加したうえで、その人物がカードをスワイプ済みである必要があります。詳細については、「*人物管理*」をご覧ください。
- 出勤データを計算します。

注記

- クライアントは、翌日 1:00 am に前日の出勤データを自動計算します。
- 1:00 am にはクライアントを起動状態にしておいてください。起動していない場合、前日の出勤データを自動計算できません。自動的に計算されなかった場合も手動で出勤データを計算できます。詳細については、「*出勤データの手動計算*」をご覧ください。

手順

1.[Time & Attendance（時間と出勤）] モジュールを表示します。
2.**[出勤統計] → [出勤記録]** の順にクリックします。
3.検索する出勤の開始時刻と終了時刻を設定します。
4.部署、名前、人物 ID など、その他の検索条件を設定します。

5.データソースとして **[Original Records on Device（デバイス上の元の記録）]** または **[Manual Handling Records（手動処理記録）]** を選択します。
6.オプション: **[Get Events from Device（デバイスからイベントを取得）]** をクリックして、デバイスから出勤データを取得します。
7.オプション: **[リセット]** をクリックして、すべての検索条件をリセットし、検索条件を再度編集します。
8.**[検索]** をクリックします。
検索結果がページ上に表示されます。その従業員の必要な出勤ステータスとチェックポイントを確認できます。
9.オプション: 検索後に、以下の操作のうち 1 つを実行します。

レポートを生成	**[レポート]** をクリックし、出勤レポートを生成します。
レポートをエクスポート	**[エクスポート]** をクリックし、結果をローカル PC にエクスポートします。
カスタムエクスポート	詳細については、「*出勤記録のカスタムエクスポート*」をご覧ください。

20.10.2 出勤記録のカスタムエクスポート

従業員の出勤データを表示した後に、実際の使用状況に応じて出勤記録をエクスポートできます。
必要な出勤記録をエクスポートする前に、従業員の出勤データを検索して取得する必要があります。詳細については、「*従業員の出勤データの概要の取得*」をご覧ください。
[カスタムエクスポート] をクリックして、関連情報を設定します。

開始/終了時間
エクスポートする出勤記録の開始時刻と終了時刻を設定できます。

保存先パス
出勤記録を保存するファイルパスを選択できます。

ファイル名
ファイルには、実際のエクスポート日に従って名前が付けられます。**dd-MM-yyyy** や **dd-MM-yy** などの日付形式を選択できます。

フォーマット
元の出勤記録を .TXT および .CVS 形式でエクスポートできます。

Separator（区切り文字）
エクスポートしたファイル内の各項目を区切るための区切り文字（コンマ、スペース、タブなど）を使用するかどうかを選択できます。

エクスポート

ID、人物名、部門、日付など、エクスポートする必要のある項目を選択できます。

デフォルト値

エクスポート対象として選択した項目の情報がない場合は、デフォルト値を設定して空白を置き換えることができます。

20.10.3 レポート表示の設定

会社名、ロゴ、データ形式、時刻フォーマット、マークなど、出勤レポートに表示するコンテンツを設定できます。

手順

1.[Time & Attendance（時間と出勤）] モジュールを表示します。
2.**[Attendance Statistics（出勤統計）]** → **[Report Display（レポート表示）]** の順にクリックします。
3.出勤レポートの表示を設定します。

会社名

レポートに記載する会社名を入力します。

日付フォーマット / 時刻フォーマット

実際の使用状況に応じて、日付フォーマットと時刻フォーマットを設定します。

レポート内の出勤ステータスのマーキング

マークを入力し、色を選択します。選択したマークと色付きで、レポート内の出勤ステータスに関連するフィールドが表示されます。

レポート内の週末のマーキング

マークを入力し、色を選択します。選択したマークと色付きで、レポート内の週末フィールドが表示されます。

4.**[保存]** をクリックします。

20.10.4 インスタントレポートの生成

一連の出勤レポートを手動で生成し、従業員の出勤結果を確認することができます。

始める前に

出勤データを計算します。

注記

出勤データを手動で計算するだけでなく、スケジュールを設定してクライアント側で毎日自動的にデータを計算することもできます。詳細については、「*出勤データの計算*」をご覧ください。

手順

1.[Time & Attendance（時間と出勤）] モジュールを表示します。
2.**[Attendance Statistics（出勤統計）] → [レポート]** の順にクリックします。
3.レポートのタイプを選択します。
4.部門または人物を選択し、出勤レポートを表示します。
5.出勤データをレポート内に記載する際の開始時刻と終了時刻を設定します。
6.**[レポート]** をクリックして統計レポートを生成し、開きます。

20.10.5 レポートの定期送信

クライアントは複数のレポートタイプに対応しています。レポート内容を事前に定義すると、設定した電子メールアドレスにレポートが自動送信されます。

手順

1.[Time & Attendance（時間と出勤）] モジュールを表示します。
2.**[出勤統計] → [Regularly Send Report（定期的にレポートを送信）]** の順にクリックします。
3.**[追加]** をクリックして、カスタムレポートの追加ページを表示します。
4.レポートの内容を設定します。

レポート名

レポート名を入力します。

レポートタイプ

レポートのタイプを 1 つ選択すると、指定したタイプでレポートが生成されます。

レポート時間

レポートのタイプごとに選択する時間が異なる場合があります。

人物

レポートに出勤記録を記載する人物を選択します。

注記

[人物] エリアの右側に、選択した人物が表示されます。

5.スケジュールを設定して、電子メールアドレスにレポートを自動送信することができます。

注記

[Auto-Send Email（電子メール自動送信）] 機能は、デフォルトで有効になっています。

1）クライアントが、選択した曜日にレポートを送信する有効期間を設定します。
2）クライアントがレポートを送信する曜日を選択します。
3）クライアントがレポートを送信する時刻を設定します。

例

有効期間を ***2018/3/10～2018/4/10***、送信の曜日を ***金曜日***、送信時刻を ***20:00:00*** に設定した場合、クライアント側は 2018/3/10 から 2018/4/10 の間、金曜日の 8 p.m.にレポートを送信します。

注記

送信時刻の前に出勤記録を計算済みであることを確認してください。出勤データを手動で計算するだけでなく、スケジュールを設定してクライアント側で毎日自動的にデータを計算することもできます。詳細については、「***出勤データの計算***」をご覧ください。

4）電子メールの宛先を入力します（複数入力可）。

注記

最大 5 件の電子メールアドレスを追加できます。**[+]** をクリックすると、新しい電子メールアドレスを追加できます。

5）オプション: **[プレビュー]** をクリックすると、電子メールの詳細を表示できます。

6.**[OK]** をクリックします。

7.オプション: カスタムレポートの追加後、以下の操作を 1 つまたは複数実行できます。

レポートを編集	追加したレポートを 1 つ選択し、**[編集]** をクリックして設定を編集します。
レポートを削除	追加したレポートを 1 つ選択し、**[削除]** をクリックして削除します。
レポートを生成	追加したレポートを 1 つ選択し、**[レポート]** をクリックしてレポートを即座に生成し、レポートの詳細を表示できます。

第 21 章 ビデオインターコム

ビデオインターコムは、建物内または棟数の少ない建物群内で使用される AV（視聴覚）通信システムです。双方にマイクとビデオカメラデバイスが搭載されているため、ビデオ信号とオーディオ信号を介した相互通信が可能です。ビデオインターコムシステムは、共同住宅および個人宅向けの安全かつ簡単な監視ソリューションを提供します。
事前にビデオインターコムデバイスをクライアントに追加し、インドアステーションを人物にリンクしてください。また、リンクされたインドアステーションを介してドアを開くためのアクセス認証も設定する必要があります。

注記

- クライアントでは、最大 16 のドアステーションと 512 のインドアステーションまたはマスターステーションを管理できます。ビデオインターコムデバイスの追加方法の詳細については、「*デバイスの追加*」をご覧ください。
- 人物の追加方法の詳細については、「*1 人の人物の追加*」をご覧ください。
- 人物のアクセス認証の設定方法の詳細については、「*アクセスグループを設定してアクセス認証を人物に割り当てる*」をご覧ください。

21.1 フローチャート

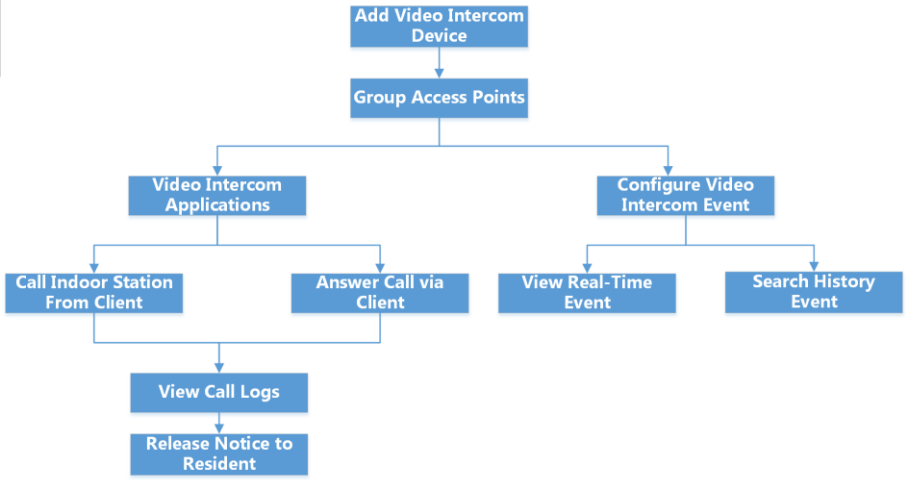

図 21-1 ビデオインターコムのフローチャート

- **ビデオインターコムデバイスの追加:** クライアントにビデオインターコムデバイスを追加できます。詳細については、「*デバイスの追加*」をご覧ください。
- **アクセスポイントのグループ化:** 追加したアクセスポイントをグループ化して、管理しやすくすることができます。詳細については、「*グループ管理*」をご覧ください。

- **クライアントからのインドアステーションの呼び出し:** 追加したインドアステーションをクライアントで呼び出して、ビデオインターコムを実行できます。詳細については、「*クライアントからのインドアステーションの呼び出し*」をご覧ください。
- **クライアント経由での呼び出しへの応答:** 追加したインドアステーションやドアステーションなどからの呼び出しにクライアント経由で応答して、ビデオインターコムを実行できます。詳細については、「*クライアント経由での呼び出しへの応答*」をご覧ください。
- **呼び出しログの表示:** すべての呼び出しの詳細を表示できます。詳細については、「*リアルタイム呼び出しログの表示*」をご覧ください。
- **居住者への通知のリリース:** クライアントで、ワンタッチで居住者に通知を送信できます。詳細については、「*居住者への通知のリリース*」をご覧ください。
- **ビデオインターコムイベントの設定:** クライアントでビデオインターコムイベントのリンク操作を設定して、イベントがトリガーされたときに通知を受け取ることができます。詳細については、「*ビデオインターコムイベントの設定*」をご覧ください。
- **リアルタイム / 過去のイベントの検索:** クライアントで、リアルタイムイベントを表示したり、過去のイベントを検索できます。詳細については、「*イベントセンター*」をご覧ください。

21.2 クライアントソフトウェアとインドアステーション / ドアステーション / 入退室管理デバイス間の通話の管理

クライアントから居住者を呼び出したり、居住者からクライアントを呼び出すことができます。また、インドアステーション / ドアステーションまたは特定の入退室管理デバイスを使用してクライアントを呼び出すこともできます。
呼び出しを行う前に、呼び出し時間と通話時間などのパラメータを設定できます。詳細については、「*入退室管理およびビデオインターコムのパラメータの設定*」をご覧ください。

21.2.1 クライアントからのインドアステーションの呼び出し

追加したインドアステーションをクライアントで呼び出して、ビデオインターコムを実行できます。

始める前に

- 居住者をクライアントに追加したことを確認してください。詳細については、「*1 人の人物の追加*」をご覧ください。
- [人物] モジュールで、居住者をインドアステーションにリンクして、居住者情報（フロア番号と部屋番号など）を設定したことを確認してください。リンクおよび居住者情報の設定方法の詳細については、「*居住者情報の設定*」をご覧ください。

手順

注記

- 1 台のビデオインターコムデバイスを複数のクライアントに追加できますが、一度に 1 つのクライアントとだけビデオインターコムを実行できます。
- [最大呼び出し時間] と [最大通話時間] はリモートで設定できます。

1.**[入退室管理]** → **[ビデオインターコム]** → **[連絡先]** の順にクリックします。
2.左側のパネルで組織リストを展開し、組織を選択します。
選択したグループのすべての居住者の情報（居住者名、デバイス名、フロア番号、および部屋番号など）が右側のパネルに表示されます。
3.居住者を選択するか、[フィルタ] フィールドにキーワードを入力して目的の居住者を検索します。
4. をクリックして、選択した居住者の呼び出しを開始します。

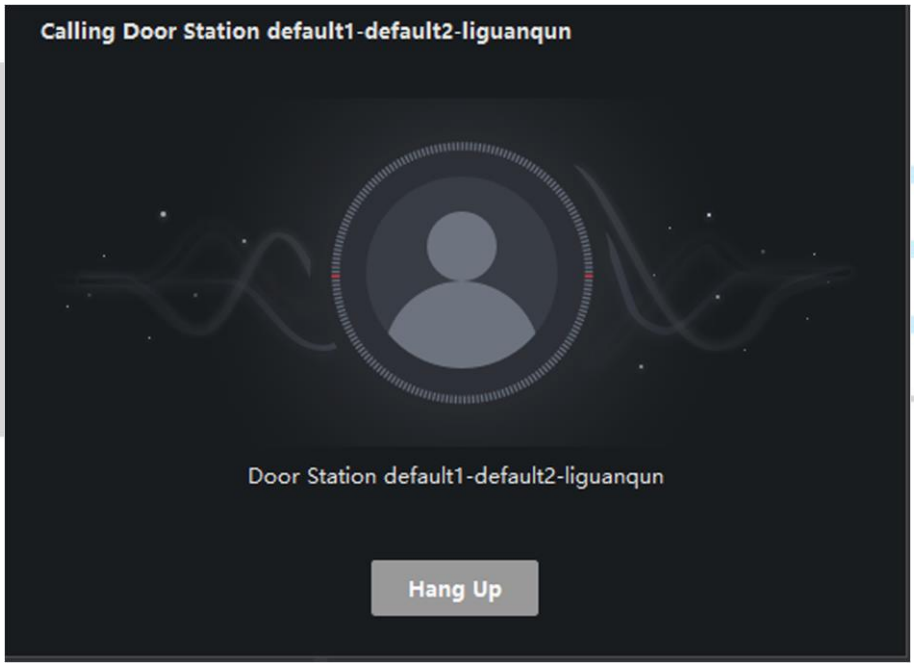

図 21-2 呼び出し開始ウィンドウ

呼び出しに対して居住者が応答すると、[通話中] ウィンドウが表示されます。
5.オプション: 呼び出しに対して居住者が応答した後に、次の操作を実行します。

スピーカー音量を調整	をクリックして、スピーカーの音量を調整します。
通話を終了	**[通話終了]** をクリックして、通話を終了します。
マイク音量を調整	をクリックして、マイクの音量を調整します。

21.2.2 クライアント経由での呼び出しへの応答

追加したインドアステーション、ドアステーション、または特定の入退室管理デバイスからの呼び出しにクライアント経由で応答して、ビデオインターコムを実行できます。

手順

注記

1 台のビデオインターコムデバイスを複数のクライアントに追加できますが、一度に 1 つのクライアントとだけビデオインターコムを実行できます。

1.インドアステーション、ドアステーション、または特定の入退室管理デバイスからクライアントを呼び出します。
呼び出しダイアログが表示されます。

図 21-3 呼び出しダイアログ

2.**[応答]** をクリックして、呼び出しに応答します。
呼び出しに対して居住者が応答すると、[通話中] ウィンドウが表示されます。
3.オプション: [通話中] ウィンドウで、次の操作を実行します。

スピーカー音量を調整	をクリックして、スピーカーの音量を調整します。
通話を終了	**[通話終了]** をクリックして、通話を終了します。
マイク音量を調整	をクリックして、マイクの音量を調整します。
ドアを開放	インドアステーションがドアステーションにリンクされている場合は、 をクリックしてドアステーションにリンクされているドアを開くことができます。

21.3 リアルタイム呼び出しログの表示

すべての呼び出しの詳細を表示したり、必要に応じて居住者を呼び出したり、ログをエクスポートしたりできます。

手順

1.**[入退室管理]** → **[ビデオインターコム]** → **[呼び出しログ]** の順にクリックします。
呼び出し状態、開始時刻、通話時間、デバイスのタイプと名前、居住者の組織と名前など、すべての呼び出しの詳細が右側のパネルに表示されます。
2.オプション: をクリックして、居住者に再ダイヤルします。
3.オプション: ページ上部で検索条件（呼び出し状態、デバイスタイプ、および時間など）を設定して、呼び出しログをフィルタリングします。
4.**[エクスポート]** をクリックして、ログ（CSV ファイル）を PC に保存します。

21.4 居住者への通知のリリース

ワンタッチで居住者に通知を送ることができます。広告、プロパティ、アラーム、および通知情報の 4 つの通知タイプを使用できます。

手順

1.**[入退室管理]** → **[ビデオインターコム]** → **[通知]** の順にクリックします。
2.**[追加]** をクリックして [通知を作成] パネルを開きます。
3. をクリックして、通知の送信先とする居住者を選択します。
4.必要な情報を入力します。

注記

- [Subject（件名）] フィールドには、最大 63 文字入力できます。
- [内容] フィールドには、最大 1023 文字入力できます。
- 最大 6 個の画像を追加できます。各画像は JPG 形式で、サイズは 512 KB 未満でなければなりません。

5.**[送信]** をクリックして、選択した居住者に通知を送信します。
送信した通知に関する情報が左側のパネルに表示されます。通知をクリックすると、その詳細が右側のパネルに表示されます。
6.オプション: **[エクスポート]** をクリックして、すべての通知を PC に保存します。

21.5 ビデオインターコムイベントの設定

ビデオインターコムイベントには、エレベータの呼び出し、ドアベル音発生、ドアロックなどがあります。ビデオインターコムデバイスのイベントは、クライアントで有効にでき

ます。ビデオインターコムデバイスでイベントがトリガーされたときに、クライアントは確認のためにイベントを受信および記録して、一連のリンク操作（電子メールの送信など）をトリガーして通知することができます。

手順

1.**[イベント設定]** → **[入退室管理イベント]** → **[ビデオインターコム]** の順にクリックします。
2.グループを展開して、イベントソースとしてビデオインターコムデバイスを選択します。

注記

リソースがオンラインであることを確認してください。

選択したビデオインターコムデバイスでサポートされているすべてのイベントタイプが表示されます。
3.オプション: **[フィルタ]** フィールドにキーワードを入力して、目的のイベントをすばやく見つけます。
4.オプション: [有効] 列のスイッチをオンにしてイベントタイプを有効にするか、**[すべて有効化]** をクリックしてこのデバイスのすべてのイベントタイプを有効にします。

注記

有効にすると、クライアントがイベントを受信して、リンク操作がトリガーされます。また、1 つのイベントタイプを無効にすることも、すべてのイベントタイプを無効にすることもできます。

5.オプション: イベントを選択した後に、次の操作を実行します。

優先度を編集	**[優先度の編集]** をクリックして、イベントの優先度を設定します。 優先度は、イベントの緊急度を表します。
イベントリンクを編集	**[リンクの編集]** をクリックして、イベントのリンク操作を設定します。

音声による警告

イベントがトリガーされたときに、クライアントの音声による警告がトリガーされます。ドロップダウンリストでオーディオファイルを選択するか、**[追加]** をクリックして新しいオーディオファイル（WAV 形式）を追加できます。
をクリックして、選択したオーディオファイルを試聴することができます。

電子メールを送信

アラーム情報の電子メール通知を 1 つまたは複数の宛先に送信します。
電子メールのパラメータ設定の詳細については、「*電子メールのパラメータ設定*」をご覧ください。

ポップアップウィンドウ

イベントがトリガーされたときに、クライアント上にイベント関連の情報（イベントの詳細、リンクされているカメラのキャプチャ画像など）を示すポップアップウィンドウが表示されます。イベントの処理方法に関する注記を入力することもできます。

Display on Map（マップ上に表示）

イベントソースをマップ上にホットスポットとして追加すると、イベントがトリガーされたときにホットスポットが表示され、その横で が光ります。これにより、セキュリティ担当者はイベントの場所を容易に確認することができます。
ホットスポットをクリックして、イベントの詳細と、リンクされたビデオインターコムデバイスのライブビデオを表示することもできます。

リンク済みカメラ

イベントがトリガーされたときに画像をキャプチャするかビデオを録画するには、選択したカメラをリンクします。

[コピー先] をクリックして、このビデオインターコムデバイスのイベント設定を他のビデオインターコムデバイスにコピーします。

注記

イベント設定は、同じタイプのリソースにのみコピーできます。

次に行う操作

ビデオインターコムデバイスが属しているデバイスで警戒を開始する必要があります。そうしないと、クライアントは設定されたイベントを受信できません。詳細については、「*デバイスからのイベント受信の有効化*」をご覧ください。

第 22 章 ログの検索

操作ログとシステムログの 2 つのタイプのログを提供しています。操作ログには、ユーザーがクライアントで行った通常の操作（デバイスの追加、パスワードのリセット、ライブビューの開始など）が記録され、システムログには、システム情報（ログイン、ログアウト、ロック、ロック解除など）が記録されます。ログファイルを検索して、時間やユーザーなどのログ詳細を表示できます。

手順

1.[ログ検索] モジュールを表示します。
2. をクリックして、開始時刻と終了時刻を指定します。

注記

1 ヵ月以内のログを検索できます。

3.クライアントで、ログファイルの検索対象とするユーザーを選択します。このログファイルは、ユーザーがクライアントで操作を行ったときに生成されます。
4.ログタイプとして、**[操作ログ]** または **[システムログ]** を選択します。
5.**[検索]** をクリックします。
開始時刻と終了時刻の間のログファイルがリストに表示されます。ログの操作時間、タイプ、およびその他の情報を確認できます。
6.オプション: ログファイルが多すぎる場合は、次の操作を実行します。

フィルタ	各テーブルのヘッダー部分にある をクリックして、項目を選択してログをフィルタリングします。
並べ替え	表のヘッダー部分をクリックして、時間または文字の順でログを並べ替えます。

第 23 章 ユーザー管理

システムのセキュリティを向上させるには、管理者は各ユーザーごとに異なるアカウントを作成し、ユーザーに異なる権限を割り当てる必要があります。異なるユーザーが同じユーザーアカウントを共有しないように、ユーザーアカウントを定期的に管理することをお勧めします。

23.1 ユーザーの追加

スーパーユーザーと管理者は、新しいユーザーを追加して、必要に応じてユーザーごとに異なる権限を割り当てることができます。

ユーザーアカウントを追加するには、次のタスクを実行します。

手順

注記

ソフトウェアにログインできるように登録したユーザーアカウントは、スーパーユーザーとして設定されます。

1.[ユーザー管理] モジュールを表示します。
2.**[ユーザーの追加]** をクリックして、ユーザー情報エリアを表示します。
3.ドロップダウンリストからユーザータイプを選択します。

管理者

管理者アカウントは、デフォルトですべての権限が割り当てられていて、すべてのオペレータと自分のパスワードと権限を変更できます。

オペレータ

オペレータアカウントは、デフォルトでは権限が割り当てられていません。手動で権限を割り当てることができます。オペレータは、自分のアカウントのパスワードと、自分が追加したアカウントのパスワードのみを変更できます。

4.ユーザー名、パスワード、確認パスワードを入力します。

注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自分で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を 8 文字以上含むパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。
パスワードなどのセキュリティ設定はすべて、設置者 / エンドユーザーの責任で適切に行ってください。

5.チェックボックスにチェックを入れて、作成したユーザーに権限を割り当てます。
6.オプション: **[デフォルト値]** をクリックして、このユーザーのデフォルトの権限を復元します。
7.**[保存]** をクリックします。

注記

クライアントソフトウェアには最大 50 個のユーザーアカウントを追加できます。

ユーザーアカウントが正常に作成されると、ユーザーアカウントが [アカウント管理] ページのユーザーリストに追加されます。
8.オプション: ユーザーアカウントが作成された後に、次の操作を実行します。

ユーザーを編集 リストでユーザーをクリックして、ユーザー情報を編集します。

注記

スーパーユーザーのパスワードのみ編集できます。

ユーザーを削除 リストからユーザーを選択して、**[ユーザーを削除]** をクリックします。

注記

スーパーユーザーを削除することはできません。

23.2 ユーザーのパスワードの変更

管理者は、通常ユーザーのパスワードを変更する場合は、古いパスワードを入力する必要はありませんが、自分のパスワードを変更する場合は、古いパスワードを入力する必要が

あります。

始める前に

ソフトウェアクライアントにユーザーを追加します。

手順

1.[ユーザー管理] モジュールを表示します。
2.パスワードを変更する必要があるユーザーを選択して、**[変更]** をクリックします。
3.オプション: 古いパスワードを入力します。

注記

管理者のパスワードを変更する場合は、最初に古いパスワードを入力する必要があります。

4.新しいパスワードと確認パスワードを入力します。
5.**[OK]** をクリックします。

第 24 章 システムの設定

24.1 全般パラメータの設定

ログの有効期限やネットワークパフォーマンスなど、頻繁に使用するパラメータを設定できます。

手順

1.[システム設定] モジュールを表示します。
2.**[全般]** タブをクリックして、[General Settings（全般設定）] ページを表示します。
3.全般パラメータを設定します。

ログ有効期限

ログファイルを保持しておく期間です。この期間を超えると、ファイルは削除されます。

最大モード

最大モードとして **[最大化]** または **[全画面]** を選択します。**最大**モードでは、表示を最大化してタスクバーを表示できます。**全画面**モードでは、クライアントを全画面モードで表示できます。

ネットワークパフォーマンス

ネットワークの状態を **[通常]**、**[より良い]**、または **[最高]** に設定します。

キーボードとジョイスティックを有効化

キーボードまたはジョイスティックを有効にします。有効にした後に、キーボードとジョイスティックのショートカットを設定できます。

注記

詳細については、「*キーボードとジョイスティックのショートカットの設定*」をご覧ください。

ソフトウェアの新バージョンを検出

有効にすると、クライアントはソフトウェアの新しいバージョンを自動的に検出して、ソフトウェアをアップグレードすることをユーザーに通知します。

自動時間同期

指定した時点に、追加したデバイスの時刻を、クライアントを実行している PC の時刻と自動的に同期します。

Auto-Upgrade Device（デバイスを自動アップグレード）

デバイスの新しいバージョンが検出された後に、アップグレードモードを設定します。

無効

有効にすると、クライアントは、新しいバージョンのクライアントを検出した場合も、ファームウェアパッケージのダウンロードとアップグレードを実行しません。

Prompt Me If Download and Upgrade（ダウンロードとアップグレードの実行確認を表示）

クライアントは、新しいバージョンのデバイスを検出すると、ファームウェアパッケージのダウンロードとアップグレードを実行するかどうかを確認するメッセージを表示します。

Download and Prompt Me If Upgrade（ダウンロードして、アップグレードの実行確認を表示）

クライアントは、新しいバージョンのデバイスを検出すると、ファームウェアパッケージを自動的にダウンロードして、アップグレードするかどうかを確認するメッセージを表示します。

自動的にダウンロードしてアップグレード

クライアントは、新しいバージョンのデバイスを検出すると、自動的にファームウェアパッケージをダウンロードして、新しいバージョンにアップグレードします。**[Upgrade Time（アップグレード時間）]** フィールドで、クライアントが自動的に新しいバージョンにアップグレードするスケジュールを設定する必要があります。

Cloud P2P Region（クラウド P2P リージョン）

クラウド P2P のサーバーのリージョンを選択します。自分が属しているリージョンまたは最も近いリージョンを選択できます。

4.**[保存]** をクリックします。

24.2 ライブビューおよび再生パラメータの設定

ライブビューおよび再生のパラメータ（画像形式、事前再生時間など）を設定できます。

手順

1.[システム設定] モジュールを表示します。
2.**[ライブビューおよび再生]** タブをクリックします。
3.ライブビューおよび再生のパラメータを設定します。

画像フォーマット

画像を保存する画像形式として、**[JPEG]** または **[BMP]** を選択します。

注記

[キャプチャ画像で温度を表示] スイッチがオンに設定されている場合は、デフォルトで JPEG が画像形式として選択され、変更できません。

ビデオ形式

録画したビデオの形式として **[MP4 / AVI]** を選択します。

ダウンロード済みビデオファイルを結合

日付別でビデオファイルをダウンロードする際の、結合されたビデオファイルの最大サイズを設定します。

次に保存されたビデオファイルを検索

ローカルデバイス、ストレージサーバー、またはストレージサーバーとローカルデバイスの両方に保存されているビデオファイルを検索して再生します。

事前再生

イベント再生の事前再生時間を設定します。デフォルト値は 30 秒です。

Prioritize Playback of Video Files on Storage Server（ストレージサーバー上のビデオファイルを優先的に再生）

ストレージサーバーに録画されたビデオファイルを優先的に再生します。それ以外の場合は、ローカルデバイスに録画されたビデオファイルを再生します。

再起動後に最新のライブビュー状態を再開

クライアントに再度ログインした後に、最新のライブビュー状態を再開します。

単一のライブビューでバックグラウンドビデオを切断

マルチウィンドウ分割モードで 1 つのライブビデオをダブルクリックすると、それが 1 ウィンドウ分割モードで表示され、リソース節約のために他のライブビデオが停止します。

ズームのホイールを有効化

PTZ モードの場合は、マウスホイールを使用してビデオを拡大または縮小できます。デジタルズームモードの場合は、ビデオを拡大または復元できます。このように、マウスをスクロールしてライブビデオを直接拡大または縮小（または復元）できます。

VCA 再生中は該当しないビデオをスキップ

VCA 再生中は、該当しないビデオがスキップされて再生されなくなります。

4.**[保存]** をクリックします。

24.3 画像パラメータの設定

クライアントの画像パラメータ（表示スケール、再生パフォーマンスなど）を設定できま

す。

手順

1.[システム設定] ページを開きます。
2.**[画像]** タブをクリックして、[画像設定] インタフェースを表示します。
3.画像パラメータを設定します。

表示スケール

ライブビューまたは再生中のビデオの表示スケールです。**[全画面]**、**[4:3]**、**[16:9]**、または **[オリジナル解像度]** に設定できます。

注記

[ライブビュー] モジュールで表示スケールを設定することもできます。詳細については、「*ライブビュー*」をご覧ください。

再生パフォーマンス

ライブビデオの再生パフォーマンスです。**[最短遅延]**、**[バランス]**、または **[滑らかさ優先]** に設定できます。
また、**[カスタム]** を選択して、実際の使用状況に応じてフレームを指定することもできます。

ハードウェアデコード優先

設定すると、ライブビューおよび再生でハードウェアによるデコードが有効になります。ハードウェアデコードにより、ライブビューまたは再生中に HD ビデオを再生する際のデコード性能が向上し、CPU 使用率が低下します。

ハイライトを有効化

ライブビューと再生で、検知された物体を緑の矩形でマークします。

トランザクション情報を表示

ライブビュー画像にトランザクション情報を表示します。

VCA ルール

ライブビューに VCA ルールを表示します。

高速再生用のフレーム抽出を有効化

ビデオを高速（8 倍速以上）で再生する場合は、この機能を無効にして、再生画像をより滑らかにして細部を表示できます。

Display Target's Pattern（対象のパターンを表示）

有効にすると、表示ウィンドウに対象者の動体追跡が表示されます。
デバイスがこの機能をサポートしている必要があります。

Overlay Rules on Captured Picture（キャプチャ画像にルールをオーバーレイ）

サーマルデバイスの場合、設定すると温度情報と発火元情報がキャプチャ画像に表示

されます。

注記

この機能を有効にすると、**[システム設定]** → **[ライブビューおよび再生]** の画像形式は JPEG に変更され、編集不可となります。

4.**[保存]** をクリックします。

24.4 画像ストレージの設定

デバイスのイベントによってトリガーされたキャプチャ画像は、iVMS-4200 サービスを実行している PC に保存できます。ここで画像のストレージロケーションを手動で設定できます。

手順

1.[システム設定] モジュールを表示します。
2.**[Event Picture Storage（イベント画像ストレージ）]** をクリックします。
3.**[サーバーに画像を保存]** スイッチをオンにします。
iVMS-4200 サービスを実行している PC のすべてのディスクが表示されます。
4.画像を保存するディスクを選択します。

注記

デフォルトの保存パスは、Disk/iVMS-4200alarmPicture です。

5.**[保存]** をクリックします。

24.5 アラーム音の設定

イベントがトリガーされたときに、クライアントは音声による警告を発してセキュリティ担当者に通知します。このセクションでは、音声による警告の音を設定できます。

手順

1.[システム設定] ページを開きます。
2.**[アラーム音]** タブをクリックして、[Alarm Sound Settings（アラーム音の設定）] ページを表示します。
3.オプション: ··· をクリックして、各種イベントのオーディオファイルをローカルパスから選択します。
4.オプション: カスタマイズされたアラーム音を追加します。
1）**[追加]** をクリックして、カスタマイズされたアラーム音を追加します。
2）**[タイプ]** フィールドをダブルクリックして、必要に応じてアラーム音の名前をカスタマイズします。

3）… をクリックして、各種アラームのオーディオファイルをローカルパスから選択します。

5.オプション: 🔊 をクリックして、オーディオファイルをテストします。

6.オプション:［操作］列で ✕ をクリックして、カスタムサウンドを削除します。

7.**[保存]** をクリックします。

注記

使用可能なオーディオファイルの形式は WAV のみです。

24.6 入退室管理およびビデオインターコムのパラメータの設定

実際の使用状況に応じて、入退室管理パラメータとビデオインターコムパラメータを設定できます。

手順

1.[システム設定] ページを開きます。

2.**[入退室管理とビデオインターコム]** タブをクリックします。

3.必要な情報を入力します。

Ringtone（呼び出し音）

…をクリックして、インドアステーションの呼び出し音のオーディオファイルをローカルパスから選択します。必要に応じて、🔊 をクリックしてオーディオファイルをテストすることができます。

最大呼び出し時間

最大呼び出し時間を秒単位で指定します。最大呼び出し時間は、15～60 秒に設定できます。

インドアステーションとの最大通話時間

インドアステーションとの最大通話時間を秒単位で指定します。インドアステーションとクライアント間の最大通話時間は 120～600 秒に設定できます。

ドアステーションとの最大通話時間

ドアステーションとの最大通話時間を秒単位で指定します。ドアステーションとクライアント間の最大通話時間は、90～120 秒に設定できます。

Max. Speaking Duration with Access Control Device（入退室管理デバイスとの最大通話時間）

入退室管理デバイスとの最大通話時間を秒単位で指定します。入退室管理デバイスとクライアント間の最大通話時間は、90～120 秒に設定できます。

4.**[保存]** をクリックします。

24.7 ファイル保存先パスの設定

ビデオ映像（ライブビュー中に手動で録画し、再生中にクリップしたもの）とキャプチャ画像は、ローカル PC に保存されます。これらのファイルの保存パスを設定できます。

手順

1.[システム設定] ページを開きます。
2.**[ファイル]** タブをクリックして、[File Saving Path Settings（ファイル保存先パスの設定）] ページを表示します。
3.… をクリックし、ファイルのローカルパスを選択します。
4.**[保存]** をクリックします。

24.8 ツールバーに表示されるアイコンの設定

ライブビューおよび再生ウィンドウのツールバーに表示されるアイコンとアイコンの順序をカスタマイズできます。表示するアイコンとアイコンの順序を設定できます。

ツールバーに表示されるアイコンを設定する必要がある場合は、次のタスクを実行します。

手順

1.[システム設定] モジュールを表示します。
2.**[ツールバー]** タブをクリックして、[Toolbar Settings（ツールバー設定）] ページを表示します。
3.ライブビューおよび再生ウィンドウでツールバーを表示できるようにするには、**[画面ツールバーの表示を有効化]** スイッチをオンに設定します。
4.必要なアイコンをクリックして、ツールバーに表示します。
5.オプション: アイコンをドラッグして、ツールバーに表示するアイコンの順序を設定します。

表 24-1 ライブビューツールバーのアイコン

	ライブビュー停止	表示ウィンドウでライブビューを停止します。
	キャプチャ	ライブビュープロセスで画像をキャプチャします。キャプチャ画像は PC に保存されます。
	録画	手動録画を開始します。ビデオファイルは PC に保存されます。
	PTZ 制御	スピードドームの PTZ モードを開始します。ビュー内をクリックしてドラッグし、PTZ 制御を実行します。

	2 ウェイオーディオ	ライブビュー中のデバイスとの 2 ウェイオーディオを開始します。
	デジタルズーム	デジタルズーム機能を有効にします。もう一度クリックすると、機能が無効になります。
	インスタント再生	インスタント再生モードに切り替えます。
	リモート設定	ライブビュー中のカメラのリモート設定ページを開きます。

表 24-2 再生ツールバーのアイコン

	キャプチャ	ライブビュープロセスで画像をキャプチャします。キャプチャ画像は PC に保存されます。
	録画	手動録画を開始します。ビデオファイルは PC に保存されます。
	デジタルズーム	デジタルズーム機能を有効にします。もう一度クリックすると、機能が無効になります。
	ダウンロード	カメラのビデオファイルをダウンロードします。ビデオファイルは PC に保存されます。
	VCA 再生	VCA ルールを設定します。詳細については、「***VCA 再生***」をご覧ください。
	タグ制御	ビデオファイルのデフォルトタグまたはカスタムタグを追加して、ビデオの重要なポイントをマークします。タグを編集することもできます。

6.**[保存]** をクリックします。

24.9 キーボードとジョイスティックのショートカットの設定

キーボードをクライアントに接続して、キーボードを使用して PTZ カメラを制御できます。キーボードとジョイスティックのショートカットを設定して、よく使用する操作にすばやく簡単にアクセスできます。

キーボードとジョイスティックのショートカットを設定する必要がある場合は、このタスクを実行します。

手順

注記

この設定ページは、[General Settings（全般設定）] でキーボードとジョイスティックを有効にすると表示されます。詳細については、「*全般パラメータの設定*」をご覧ください。

1.[システム設定] モジュールを表示します。
2.**[キーボードとジョイスティック]** をクリックして、[キーボードとジョイスティックのショートカット設定] エリアを表示します。
3.クライアントがインストールされている PC にキーボードを接続している場合は、キーボードのドロップダウンリストから COM ポートを選択します。

注記

PC の [デバイスマネージャ] で、キーボードが接続されている COM ポートを確認できます。

4.キーボードとジョイスティックのショートカットを設定します。
   1）[機能] 列で特定の機能名を選択します。
   2）[PC キーボード]、[USB ジョイスティック]、または [USB Keyboard（USB キーボード）] 列の項目フィールドをダブルクリックします。
   3）複合キーの操作または番号をドロップダウンリストから選択して、キーボードまたは USB ジョイスティックの機能のショートカットとして設定します。
5.**[保存]** をクリックします。

例

フォーカス（+）機能の場合、**Home**、**1**、**F1** を [PC キーボード]、[USB ジョイスティック] および [USB Keyboard（USB キーボード）] のショートカットとして設定すると、PC キーボードの Home キーを押すか、ジョイスティックを 1 の方向にするか、USB キーボードの F1 キーを押して拡大表示することができます。

24.10 電子メールのパラメータ設定

イベントのリンク操作として **[電子メールを送信]** を設定し、イベントがトリガーされると、クライアントは受信者に電子メールを送信して通知します。このセクションでは、電子メール設定を設定し、対象とする受信者を指定する必要があります。

手順

1.[システム設定] モジュールを表示します。
2.**[電子メール]** タブをクリックして、[電子メール設定] インタフェースを表示します。
3.必要な情報を入力します。

STMP サーバー

STMP サーバーのホスト名です（例: smtp.263xmail.com）。

暗号化タイプ

ラジオボタンを選択して、**[非暗号化]**、**[SSL]**、または **[STARTLS]** を選択できます。

ポート

SMTP に使用する通信ポートを入力します。デフォルトでは、ポートは 25 です。

送信者のアドレス

送信者の電子メールアドレスです。

セキュリティ証明書（オプション）

電子メールサーバーで認証が必要な場合は、このチェックボックスにチェックを入れて、サーバーへのログインに認証を使用するように設定し、電子メールアカウントのログインユーザー名とパスワードを入力します。

ユーザー名

[サーバー認証] にチェックを入れた場合は、送信者の電子メールアドレスのユーザー名を入力します。

パスワード

[サーバー認証] にチェックを入れた場合は、送信者の電子メールアドレスのパスワードを入力します。

宛先 1～3

宛先の電子メールアドレスを入力します。最大 3 つの宛先を設定できます。

4.オプション: **[テスト電子メールを送信]** をクリックして、テストのために受信者に電子メールを送信します。

5.**[保存]** をクリックします。

24.11 セキュリティ認証の管理

データセキュリティ上、クライアントと追加したサーバー（ストリームメディアサーバー）のセキュリティ証明書は同じでなければなりません。TLS（トランスポートレイヤーセキュリティ: Transport Layer Security）プロトコルを使用して伝送暗号化を有効にする場合は、確認証明書が必要かどうかを設定できます。

ストリームメディアサーバーをクライアントに追加する前に、クライアントサービスからサービス証明書をエクスポートして、それをストリームメディアサーバーにインポートする必要があります。複数のクライアントが同じサーバーを使用する場合は、クライアントとサーバーのセキュリティ証明書を互いに同じにする必要があります。

24.11.1 サービス管理からの証明書のエクスポート

現在のクライアントサービスからセキュリティ証明書をエクスポートして、エクスポートした証明書ファイルをストリームメディアサーバーまたは他のクライアントにインポートできます。

手順

1.[サービス管理] を表示します。
2.**[エクスポート]** をクリックして、ローカル PC に証明書ファイルを保存します。

注記

証明書ファイルは XML 形式です。

次に行う操作

証明書をエクスポートした後に、クライアントがインストールされている PC に証明書をコピーして、それをストリームメディアサーバーまたは他のクライアントにインポートできます。
ストリームメディアサーバーへのインポートについては、「*ストリームメディアサーバーへの証明書のインポート*」をご覧ください。

24.11.2 クライアントへの証明書のインポート

複数のクライアントが同じストリームメディアサーバーにアクセスする場合は、クライアントとサーバーに同じ証明書をインポートする必要があります。

始める前に

いずれかのクライアントサービスからセキュリティ証明書をエクスポートしたことを確認してください。

注記

詳細については、「*サービス管理からの証明書のエクスポート*」をご覧ください。

手順

1.他のクライアントからエクスポートした証明書ファイルをローカル PC にコピーします。
2.[システム設定] モジュールを表示します。
3.**[Security Authentication（セキュリティ認証）]** タブをクリックして、セキュリティ認証設定インタフェースを表示します。
4.**[インポート]** をクリックします。
5.ローカル PC から証明書ファイルを選択して、**[開く]** をクリックします。

注記

クライアントを再起動して有効にします。

24.11.3 伝送暗号化の証明書確認

[Security Authentication（セキュリティ認証）] ページで、伝送暗号化にデバイス証明書の確認が必要かどうかを設定できます。

[システム設定] → **[Security Authentication（セキュリティ認証）]** の順にクリックして、セキュリティ認証インタフェースを表示します。[証明書を検証] で **[はい]** または **[いいえ]** を選択します。

はい

デバイスの追加時に伝送暗号化を有効にする場合、指定されたディレクトリにデバイス証明書を配置する必要があります。デバイスは伝送暗号化で追加され、証明書が検証されるため、セキュリティレベルが向上します。

いいえ

デバイスの追加時に伝送暗号化を有効にする場合、デバイス証明書は必要ありません。デバイスは伝送暗号化で追加されます。

第 25 章 操作とメンテナンス

メニューでメンテナンス操作を実行して、クライアントをトラブルフリーで使いやすい状態に保つことができます。
右上隅の をクリックし、[ファイル] / [システム] / [ツール] をクリックして、次の操作を実行します。

ログファイルを開く

ローカル PC に保存されているログファイル、またはクライアントのログファイルを開くことができます。

設定ファイルをインポート/エクスポート

必要に応じてローカル PC からクライアントに設定ファイルをインポートできます。また、その逆も可能です。

自動バックアップ

設定ファイルとデータベース内のデータをバックアップする日時を選択するか、バックアップしたデータを復元します。

スキン

クライアントのスキン（明色系や黒色系など）を変更します。

一括時刻同期

選択したデバイスの時刻を PC の時刻と同期します。

メッセージ待ち行列

電子メールリンクを設定すると、トリガーされたイベントがここに表示されます。イベントを選択して、受信者への電子メールの送信をキャンセルします。

A. ウィーガンドルールのカスタマイズ設定

ここではウィーガンド 44 を例にとって説明します。[カスタムウィーガンド] タブの設定値は次のとおりです。

カスタムウィーガンド名	Wiegand 44				
合計長	44				
変換ルール（10 進数）	byFormatRule[4]=[1][4][0][0]				
パリティモード	XOR パリティ				
奇数パリティのスタートビット		長さ			
偶数パリティのスタートビット		長さ			
XOR パリティのスタートビット	0	グループごとの長さ	4	合計長	40
カード ID のスタートビット	0	長さ	32	10 進数	10
サイトコードのスタートビット		長さ		10 進数	
OEM のスタートビット		長さ		10 進数	
メーカーコードのスタートビット	32	長さ	8	10 進数	3

ウィーガンドデータ

ウィーガンドデータ = 有効なデータ + パリティデータ

合計長

ウィーガンドデータ長。

変換ルール

4 バイト。有効なデータの組み合わせタイプを表示します。この例では、カード ID とメーカーコードの組み合わせを示しています。有効なデータは、1 つのルール、または複数のルールの組み合わせです。

パリティモード

ウィーガンドデータの有効なパリティ。奇数パリティまたは偶数パリティを選択できます。

奇数パリティのスタートビット、長さ

[奇数パリティ] を選択した場合に、これらの項目を使用できます。奇数パリティのスタートビットが 1 で、長さが 12 の場合、システムは奇数パリティの計算をビット 1 から開始します。12 ビット計算します。結果はビット 0 に格納されます（ビット 0 が最初のビットです）。

偶数パリティのスタートビット、長さ

[偶数パリティ] を選択した場合に、これらの項目を使用できます。偶数パリティのスタートビットが 12 で、長さが 12 の場合、システムは偶数パリティの計算をビット 12 から開始します。12 ビット計算します。結果は最後のビットに格納されます。

XOR パリティのスタートビット、グループごとの長さ、合計長

[XOR パリティ] を選択した場合に、これらの項目を使用できます。上記の表で、スタートビットは 0、グループごとの長さは 4、合計長は 40 です。この場合、システムはビット 0 から計算し、4 ビットごとに計算し、合計 40 ビット（合計 10 グループ）を計算することを意味します。結果は最後の 4 ビットに格納されます（結果の長さは、グループごとの長さと同じです）。

カード ID のスタートビット、長さ、および 10 進数

変換ルールを使用する場合に、これらの項目を使用できます。上記の表で、カード ID のスタートビットは 0、長さは 32、10 進数は 10 です。ビット 0 から 32 ビットがカード ID であることを表しています（ここでの長さはビットで計算されます）。また、10 進数の長さは 10 ビットです。

サイトコードのスタートビット、長さ、および10進数

変換ルールを使用する場合に、これらの項目を使用できます。詳細については、カード ID の説明をご覧ください。

OEM のスタートビット、長さ、および 10 進数

変換ルールを使用する場合に、これらの項目を使用できます。詳細については、カード ID の説明をご覧ください。

メーカーコードのスタートビット、長さ、および 10 進数

変換ルールを使用する場合に、これらの項目を使用できます。上記の表で、メーカーコードのスタートビットは 32、長さは 8、10 進数は 3 です。これは、ビット 32 から 8 ビットがメーカーコードであることを表しています(ここでの長さはビットで計算されます)。10 進数の長さは 3 です。

B. トラブルシューティング

ここでは、クライアントソフトウェア操作時の一般的な問題について説明します。また、問題を解決するのに役立つ、考えられる原因とその解決策について説明します。

B.1 特定のデバイスのライブビューの取得に失敗しました。

問題

特定のデバイスのライブビューの取得に失敗しました。

考えられる原因

- ネットワークが不安定か、ネットワークのパフォーマンスが十分ではありません。
- デバイスはオフラインです。
- リモートデバイスへのアクセスが多すぎることによって、デバイスの負荷が高くなりすぎています。
- 現在のユーザーはライブビューの権限を持っていません。
- クライアントソフトウェアのバージョンが、必要なバージョンよりも古いバージョンです。

解決策

- ネットワークの状態を確認し、PC で使用していない他のプロセスを無効にします。
- デバイスのネットワークの状態を確認します。
- デバイスを再起動するか、デバイスへの他のリモートアクセスを無効にします。
- 管理者ユーザーでログインし、再試行します。
- 最新バージョンのクライアントソフトウェアをダウンロードします。

B.2 ローカル録画とリモート録画を混同しています。

問題

ローカル録画とリモート録画を混同しています。

解決策

- このマニュアルでローカル録画とは、ローカルデバイスの HDD、SD / SDHC カードにビデオファイルを保存する録画のことです。
- リモート録画とは、リモートデバイス側のクライアントよって制御される録画操作のことです。

B.3 ビデオファイルのダウンロードに失敗したか、またはダウンロード速度が遅すぎます。

問題

ビデオファイルのダウンロードに失敗したか、またはダウンロード速度が遅すぎます。

考えられる原因

- ネットワークが不安定か、ネットワークのパフォーマンスが十分ではありません。
- NIC タイプが互換性のないタイプです。
- リモートデバイスへのアクセスが多すぎます。
- 現在のユーザーは再生の権限を持っていません。
- クライアントソフトウェアのバージョンが、必要なバージョンよりも古いバージョンです。

解決策

- ネットワークの状態を確認し、PC で使用していない他のプロセスを無効にします。
- クライアントを実行している PC をデバイスに直接接続して、NIC カードの互換性を確認します。
- デバイスを再起動するか、デバイスへの他のリモートアクセスを無効にします。
- 管理者ユーザーでログインし、再試行します。
- 最新バージョンのクライアントソフトウェアをダウンロードします。

C. FAQ（よくある質問）

ここでは、クライアントソフトウェアの操作に関するよくある質問のいくつかについて説明します。ユーザーが問題を解決するのに役立つ回答を示します。

C.1 ライブビュー中に、エラーコード 91 のエラーメッセージが表示されるのはなぜですか?

質問

ライブビュー中に、エラーコード 91 のエラーメッセージが表示されるのはなぜですか?

回答

複数のウィンドウのライブビューの場合、チャンネルがサブストリームをサポートしていないことがあります。**[システム設定]** → **[画像]** で **[自動変更ストリームタイプ]** 機能を無効にして、ライブビューに適したストリームタイプを選択してください。

C.2 ライブビュー中に、画像がぼやけたり、滑らかでないのはなぜですか?

質問

ライブビュー中に、画像がぼやけたり、滑らかでないのはなぜですか?

回答

ビデオカードのドライバを確認してください。ビデオカードのドライバを最新バージョンにアップデートすることを強くお勧めします。

C.3 しばらく実行した後に、メモリリークが発生し、クライアントがクラッシュするのはなぜですか?

質問

しばらく実行した後に、メモリリークが発生し、クライアントがクラッシュするのはなぜですか?

回答

クライアントソフトウェアのインストールディレクトリで、**Setup.xml** ファイルをメモ帳で開いて、**EnableNetandJoystickCheck** の値を **false** に変更してください。クライアントを再起動しても問題が解決しない場合は、テクニカルサポートにお問い合わせください。

C.4 ライブビュー中、ストリームメディアサーバー経由でストリームを取得しているときに、エラーコード 17 のエラーメッセージが表示されるのはなぜですか?

質問

ライブビュー中、ストリームメディアサーバー経由でストリームを取得しているときに、エラーコード 17 のエラーメッセージが表示されるのはなぜですか?

回答

ストリームメディアサーバーのポートマッピング（特に RTSP ポート）を確認してください。

C.5 ネットワーク帯域幅が狭いときにライブビューと再生のパフォーマンスを向上させるにはどうしたら良いですか?

質問

ネットワーク帯域幅が狭いときにライブビューと再生のパフォーマンスを向上させるにはどうしたら良いですか?

回答

使用するデバイスがこの機能に対応している必要があります。次の操作を実行して、低帯域幅でライブビューを実現できます。

注記

事前に **[自動変更ストリームタイプ]** を無効にする必要があります。

- まず、エンコードデバイスをクライアントに追加した後に、カメラのストリーミングプロトコルを設定する必要があります。
  - **[デバイス管理]** → **[グループ]** に移動します。

- [エンコードチャンネル] リストでカメラを選択して、 をクリックします。
- [カメラを編集] ウィンドウで、**[プロトコルタイプ]**（ライブビューの場合）または **[Playback Protocol Type（再生プロトコルタイプ）]**（再生の場合）を **[アダプティブ UDP]** に設定します。

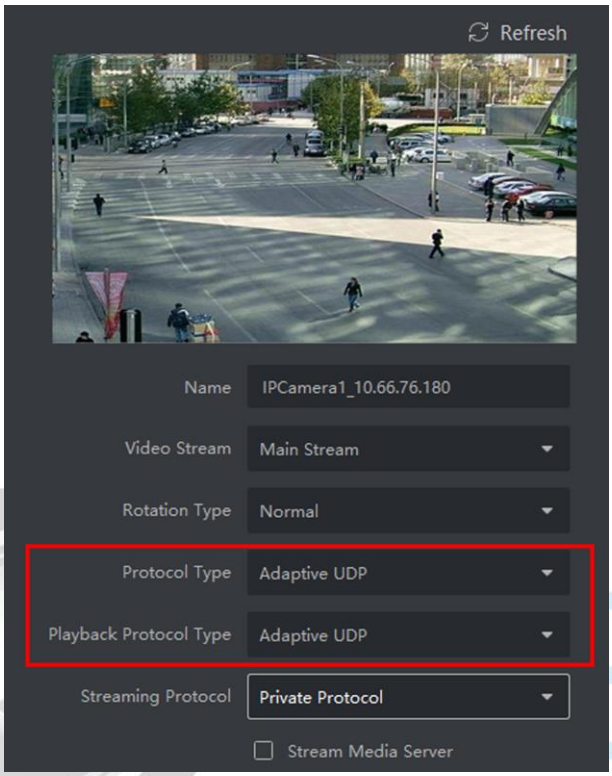

図 C-1 プロトコルタイプの設定

- **[OK]** をクリックして設定を保存します。

- ライブビューのストリームタイプを選択します。
  - [メインビュー] モジュールを表示します。
  - 左側のデバイスリストで、カーソルをカメラ名に移動して、 → **[ストリーム]** の順にクリックします。

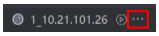

図 C-2 ストリームタイプの選択

  - ネットワークカメラの場合は、ストリームタイプを **[ストリーム 3]** に設定します。DVR または NVR の場合は、ストリームタイプを **[バーチャルストリーム]** に設定します。
  - ライブビューを開始します。

D. エラーコード

コード	エラー名	説明
iVMS-4200		
317	ビデオはありません。	ユーザーに再生する権限がない場合に表示されます。
HCNetSDK.dll		
1	ユーザー名またはパスワードが無効です。	
2	権限がありません。	デバイスのユーザーに十分な権限がありません。
4	チャンネル番号が無効です。	リモート画面制御のライブビューで表示されます。
5	これ以上デバイスを接続できません。	
7	デバイスの接続に失敗しました。	
23	サポートされていません。	
29	操作に失敗しました。	
43	バッファがありません。	デバイスの追加時に、デバイスポートが Web サーバーによって使用されている場合に表示されます。
55	IP アドレスが無効です。	
56	MAC アドレスが無効です。	
91	チャンネルが操作をサポートしていません。	サブストリームの取得に失敗した場合に表示されます。
96	デバイスは DDNS に登録されていません。	
153	ユーザーはロックされています。	
250	デバイスがアクティベートさ	

コード	エラー名	説明
	れていません。	
404	チャンネル番号エラー、またはデバイスがサブストリームをサポートしていません。	サブストリームの取得に失敗した場合、またはサブストリームが存在しない場合に表示されます。
424	RTSP SETUP のデータの受信に失敗しました。	外部ネットワーク経由でソフトウェア DVS のライブビューを追加しているときに表示されます。
800	使用可能な帯域幅の上限に達しています。	
Playctrl.dll		
2		ストリームが [ビデオ＆オーディオ] ストリームではありません。
6		64 ビットオペレーティングシステムで H.265 を採用すると、再生ウィンドウが黒くなります。
SMS		
3		ソフトウェアとストリームメディアサーバー間の接続の問題です。
17		ストリームメディアサーバーとデバイス間のストリーミングの問題です。

D'S SECURITY