

iVMS-4200 クライアントソフトウェア

ユーザーマニュアル V3.3

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 GraspHERE の Web サイト(<https://www.graspHERE.com/>)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。

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。GRASPHERE 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。GRASPHERE 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 GRASPHERE 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。GRASPHERE 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、ウイ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 GRASPHERE 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。

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.....	16
1.1 はじめに.....	16
1.2 変更の概要.....	16
第 2 章 サービス管理.....	17
第 3 章 デバイス管理.....	18
3.1 デバイスの起動.....	18
3.2 デバイスの追加.....	20
3.2.1 単一または複数のオンラインデバイスの追加.....	20
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.....	24
3.2.3 IP セグメントごとのデバイスの追加.....	26
3.2.4 クラウド P2P によるデバイスの追加.....	29
3.2.5 ISUP アカウントによるデバイスの追加.....	31
3.2.6 HiDDNS によるデバイスの追加.....	32
3.2.7 バッチ内のデバイスのインポート.....	34
3.3 デバイスの復元/リセットパスワード.....	37
3.3.1 デバイスのリセットパスワード.....	37
3.3.2 デバイスのデフォルト・パスワードの復元.....	38
3.4 デバイス・ファームウェア・バージョンアップ.....	39
3.5 追加されたデバイスの管理.....	42
3.6 グループ経営.....	43
3.6.1 グループリソース.....	43
3.6.2 リソース・パラメーターの編集.....	44
第 4 章 ライブビュー.....	47
4.1 ライブビューツールバー.....	47
4.2 カスタムビューの追加.....	48
4.3 ライブビューの開始.....	49
4.4 ライブビューのオートスイッチ.....	50

4.4.1	グループ内のオートスイッチカメラ	51
4.4.2	全カメラ自動切替	52
4.4.3	オートスイッチカスタムビュー	53
4.5	PTZ 制御	55
4.5.1	PTZ コントロールパネル	55
4.5.2	プリセット、パトロール、パターンの設定	58
4.6	カスタマイズ・ウィンドウ部門	59
4.7	手動で記録・取得	59
4.7.1	手動でビデオを録画する	60
4.7.2	ローカルビデオの表示	60
4.7.3	撮影した画像	61
4.7.4	撮影した画像を見る	62
4.8	インスタント再生	62
4.9	Fisheye Camera のライブビュー	63
4.9.1	Fisheye モードでライブビューを実行する	63
4.9.2	Fisheye モードでの PTZ 制御	65
4.9.3	プリセットとパトロールの設定	65
4.10	マスタースレーブ連携の実行	66
4.10.1	マスタースレーブ・トラッキング・ルールの設定	66
4.10.2	マスタースレーブトラッキングを有効にする	69
4.11	サーマルカメラ用ライブビュー	69
4.11.1	ライブビュー中の火源情報の表示	69
4.11.2	ライブビュー画像上の温度情報の表示	71
4.11.3	温度を手動で測定	72
4.12	低帯域幅のライブビュー	73
4.13	より多くの機能	73
第 5 章	リモート再生	76
51	フローチャート	76
52	リモート・ストレージ構成	77

5.2.1	DVR、NVR、ネットワークカメラに画像とビデオを保存する.....	77
5.2.2	ビデオを記憶装置に保存する.....	79
5.2.3	店舗の写真とローカル PC の追加情報.....	82
5.2.4	記録スケジュールテンプレートの設定.....	83
5.2.5	取り込みスケジュールテンプレートの設定.....	84
53	通常の再生.....	85
5.3.1	映像検索.....	86
5.3.2	ビデオ映像の再生.....	87
54	アラーム入力再生.....	89
5.4.1	映像検索.....	89
5.4.2	ビデオ映像の再生.....	90
5.5	イベント再生.....	90
5.5.1	映像検索.....	91
5.5.2	ビデオ映像の再生.....	91
5.6	ATM 再生.....	92
5.6.1	映像検索.....	92
5.6.2	ビデオ映像の再生.....	93
5.7	POS 再生.....	93
5.7.1	映像検索.....	94
5.7.2	ビデオ映像の再生.....	94
5.8	VCA 再生.....	95
5.9	同期再生.....	97
5.10	Fisheye Camera のビデオ再生.....	97
5.11	低帯域幅での再生.....	99
5.12	ビデオ映像をダウンロードする.....	99
5.12.1	ビデオ映像を日付でダウンロードする.....	100
5.12.2	複数のカメラのダウンロード.....	100
第 6 章	イベント設定.....	102
6.1	カメラのイベント設定.....	102

6.2	アラーム入力のイベント設定	105
6.3	エンコーディング・デバイスのイベント設定	107
第7章	イベントセンター	110
7.1	デバイスからの受信イベントの有効化	110
7.2	リアルタイムイベントの表示	111
7.3	履歴イベントの検索	113
7.4	デバイスからのイベントの取得	115
7.5	ポップアップ・イベント情報の表示	116
第8章	マップ管理	118
8.1	マップの追加	118
8.2	マップスケールの編集	119
8.3	ホットスポットの管理	119
8.3.1	カメラをホットスポットとして追加する	119
8.3.2	ホットスポットとしてのアラーム入力の追加	121
8.3.3	ホットスポットとしてのアラーム出力の追加	122
8.3.4	ホットスポットとしてゾーンを追加	124
8.3.5	アクセスポイントをホットスポットとして追加	127
8.3.6	セキュリティー・レーダー・ホットスポットの設定	129
8.3.7	ホットスポットの編集	148
8.3.8	プレビューホットスポット	149
8.4	ホットリージョンの管理	153
8.4.1	ホットリージョンの追加	154
8.4.2	ホットリージョンの編集	154
8.4.3	プレビューホットリージョン	155
8.5	人物の移動パターンの表示	155
第9章	ストリームメディアサーバーを介したビデオストリームの転送	158
9.1	ストリーム・メディア・サーバーへの証明書のインポート	158
9.2	IPアドレスによるストリームメディアサーバーの追加	159

9.3	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	160
第 10 章	統計	162
10.1	人数カウント報告書	162
10.2	交差点でカウントしている人の表示レポート	166
10.3	キュー管理	167
10.3.1	キューイングアップ時間解析	168
10.3.2	キューステータス分析	171
10.4	ヒートマップレポート	175
10.5	皮膚表面温度統計の報告	177
第 11 章	データ検索	179
11.1	顔画像検索	179
11.1.1	アップロードした画像で顔を検索する	179
11.1.2	イベント・タイプによる顔の検索	182
11.1.3	人名による顔の検索	184
11.1.4	顔の特徴による顔の検索	187
11.2	人体回収	189
11.2.1	アップロードした画像で人体を検索する	189
11.2.2	人物による人体探索	192
11.3	ビヘイビア分析に関連する画像とビデオの表示	193
11.4	車両回収	194
11.5	ハードハット検索	197
11.6	ピープルフェアサーチ	197
11.6.1	出頭頻度の高い者の検索	198
11.6.2	出頭頻度の低い者の検索	199
11.7	AI ダッシュボードの検索	200
11.7.1	ビデオおよび取り込んだピクチャータスクの検索分析結果	201
11.7.2	インポートされたピクチャータスクの検索分析結果	202
11.8	顔認証チェックイン	203

11.8.1	顔認識チェックイン記録の検索	203
11.8.2	顔認識出席記録の検索	204
第 12 章 AI ダッシュボード		208
12.1	フェイスアプリケーション	208
12.1.1	顔画像ライブラリのリストタイプの設定	208
12.1.2	AI 情報表示カメラの設定	209
12.1.3	人工知能情報の表示	209
12.2	マルチターゲット型検出	211
12.3	AI オープンプラットフォーム	216
12.3.1	プラットフォームパラメータの設定	216
12.3.2	ピクチャータスクの解析	218
12.3.3	AI プラットフォームのリアルタイム表示	219
12.4	連動キャプチャアラーム	220
12.4.1	動作パラメータの設定	220
12.4.2	ライブビューとアラームの表示	220
12.5	交通事故警報	221
12.5.1	表示パラメータの設定	222
12.5.2	交通事故警報の表示	223
12.6	皮膚表面温度	224
12.6.1	皮膚表面温度の表示	224
12.6.2	皮膚表面温度情報表示	225
12.6.3	アラーム情報の表示	229
第 13 章 セキュリティ制御パネル		231
13.1	フローチャート	231
13.2	セキュリティコントロールパネルをリモート設定する	232
13.3	ゾーンイベントのクライアントリンクの設定	232
13.4	リモートコントロールセキュリティコントロールパネル	235
13.4.1	リモートコントロールパーティション	235
13.4.2	リモートコントロールゾーン	237

13.4.3	リモートリレー.....	238
13.4.4	リモートコントロールサイレン.....	238
第 14 章	人事管理.....	239
14.1	組織の追加.....	239
14.2	独身者の追加.....	240
14.2.1	基本情報の設定.....	240
14.2.2	1 人にカードを発行する.....	241
14.2.3	ローカル PC から顔写真をアップロードする.....	245
14.2.4	お客様での撮影.....	246
14.2.5	アクセス制御装置による顔の収集.....	247
14.2.6	クライアント経由で指紋を収集.....	248
14.2.7	アクセス制御装置による指紋の収集.....	249
14.2.8	アクセス制御情報の設定.....	250
14.2.9	個人情報のカスタマイズ.....	252
14.2.10	住民情報の設定.....	253
14.2.11	追加情報の設定.....	254
14.3	本人確認情報の輸出入.....	254
14.3.1	個人情報のインポート.....	254
14.3.2	輸入者の写真.....	255
14.3.3	個人情報のエクスポート.....	256
14.3.4	エクスポート者の写真.....	256
14.4	アクセス制御装置からの個人情報の取得.....	257
14.5	他の組織への人員移動.....	258
14.6	一括発行.....	258
14.7	カード紛失報告.....	258
14.8	リソース統計の表示.....	259
第 15 章	アクセス制御.....	262
15.1	フローチャート.....	262
15.2	スケジュールとテンプレートの設定.....	263

15.2.1	休日追加	264
15.2.2	テンプレートの追加	265
15.3	アクセス許可を個人に割り当てるためのアクセスグループの設定	266
15.4	検索アクセスグループ	269
15.5	詳細機能の設定	270
15.5.1	デバイスパラメータの設定	270
15.5.2	残りのオープン/クローズの設定	280
15.5.3	マルチファクター認証の設定	282
15.5.4	カスタム・ワイガンド・ルールの設定	284
15.5.5	カードリーダー認証モードとスケジュールの設定	286
15.5.6	個人認証モードの設定	288
15.5.7	エレベータコントローラのリレー設定	289
15.5.8	ファーストパーソンの設定	292
15.5.9	パスバック対策の設定	294
15.5.10	マルチドアインターロックの設定	295
15.5.11	認証コードの設定	296
15.6	その他のパラメータの設定	297
15.6.1	複数の NIC パラメータの設定	297
15.6.2	ネットワークパラメータの設定	298
15.6.3	デバイス取り込みパラメータの設定	300
15.6.4	顔認識端子の設定パラメータ	302
15.6.5	M1 カードの暗号化を有効にする	303
15.6.6	RS-485 パラメータの設定	303
15.6.7	Wiegand パラメータの設定	304
15.7	アクセス制御のためのリンクアクションの設定	305
15.7.1	アクセス・イベント用のクライアント・アクションの構成	305
15.7.2	アクセスイベントに対するデバイスアクションの設定	307
15.7.3	カードスウィッピングのためのデバイスアクションの設定	309
15.7.4	個人 ID のためのデバイスアクションの設定	310

15.8	ドア・エレベータ制御	312
15.8.1	制御ドアステータス	312
15.8.2	制御エレベータステータス	314
15.8.3	リアルタイムアクセスレコードのチェック	315
第 16 章	時間と勤怠	317
16.1	フローチャート	317
16.2	出勤パラメータの設定	318
16.2.1	週末設定	319
16.2.2	認証モードの設定	319
16.2.3	残業時間パラメータの設定	319
16.2.4	出勤チェックポイントの設定	320
16.2.5	休日の設定	321
16.2.6	リーブ・タイプの設定	323
16.2.7	認証レコードをサードパーティのデータベースに同期させる	323
16.2.8	勤怠計算精度の設定	324
16.2.9	休憩時間の設定	325
16.3	General Timetable の追加	326
16.4	フレキシブルなスケジュールの追加	329
16.5	Shift の追加	330
16.6	シフトスケジュールの管理	332
16.6.1	部門スケジュールの設定	332
16.6.2	個人スケジュールの設定	334
16.6.3	臨時スケジュールの設定	335
16.6.4	シフトスケジュールの確認	336
16.7	チェックイン/チェックアウトレコードの手動修正	336
16.8	休暇・出張の追加	338
16.9	出勤データの計算	339
16.9.1	出勤データの自動計算	339
16.9.2	出勤データを手動で計算する	340

16.10	勤怠統計	341
16.10.1	従業員の勤怠データの概要を入手する	341
16.10.2	カスタムエクスポート出席記録	342
16.10.3	レポート表示の設定	343
16.10.4	即時レポートの生成	343
16.10.5	定期的にレポートを送信する	344
第 17 章	ビデオ・インターコム	347
17.1	フローチャート	347
17.2	クライアントソフトウェアと屋内/ドアステーション/アクセス制御デバイス間の通話の管理	348
17.2.1	お客さまからの屋内ステーションへの電話	348
17.2.2	クライアントからの電話に出る	350
17.3	リアルタイム通話履歴の表示	351
17.4	住民への通知の発出	351
17.5	ビデオインターコムイベントの設定	352
第 18 章	トポロジー管理	355
181	トポロジー表示の概要	355
182	トポロジーパラメーターの設定	356
183	デバイスの詳細の表示	357
184	リンクの詳細の表示	358
185	信号伝送経路の表示	359
186	トポロジーのエクスポート	360
187	より多くの機能	361
第 19 章	ログ検索	362
第 20 章	ユーザ管理	363
21.1	ユーザの追加	363
第 21 章	システム構成	366
21.1	一般パラメータの設定	366
21.2	ライブビューおよび再生パラメータの設定	367

21.3 画像パラメータの設定.....	369
21.4 ピクチャーストレージ設定	370
21.5 設定したアラーム音	370
21.6 アクセス制御およびビデオインターコムのパラメータの設定	371
21.7 ファイル保存パスの設定.....	372
21.8 ツールバーに表示されるアイコンの設定	372
21.9 キーボードショートカットとジョイスティックショートカットの設定	374
21.10 電子メールパラメータの設定.....	375
21.11 セキュリティ認証の管理.....	376
21.11.1 サービス管理からのエクスポート証明書	376
21.11.2 顧客への輸入証明書.....	376
21.11.3 伝送暗号化のための証明書検証	377
第 22 章 操作と保守.....	378
付録 A. カスタム Wiegand ルールの説明.....	379
付録 B.トラブルシューティング	381
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。.....	381
B.2 ローカル録画とリモート録画が混同されます。.....	381
B.3 ビデオファイルのダウンロードに失敗した、またはダウンロード速度が遅すぎる。382	
付録 C. FAQ (よくある質問).....	383
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?.....	383
C.2 ライブビュー中に、画像がぼやけているのか、それとも滑らかでないのか。383	
C.3 メモリーが漏れ、しばらく走った後にクライアントがクラッシュしたのはなぜですか? 384	
C.4 ライブビュー中、ストリーム・メディア・サーバーを介してストリームを取得する場合、エラー・コード 17 を含むエラー・メッセージがプロンプトを出す理由は何ですか? 384	

C.5 ネットワーク帯域幅が小さい場合、ライブビューや再生のパフォーマンスを向上させるにはどうすればよいでしょうか?.....	384
付録 D.エラーコード	387

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、セキュリティ制御パネル、ビデオインターホン装置、アクセス制御装置などのための汎用的なセキュリティ管理ソフトウェアです。

ソフトウェアは、リアルタイムライブビュー、ビデオ録画、リモート検索および再生、ファイルバックアップ、アラーム受信、個人管理、アクセス制御、ビデオインターホン、セキュリティ制御、時間および立会いなどを含む、複数の機能を、モニタリングタスクのニーズを満たすために、接続されたデバイスに提供する。柔軟な分散構造と使いやすい操作により、クライアントソフトウェアは中小規模のサーベイランスプロジェクトに広く適用されている。

本取扱説明書では、クライアントソフトウェアの機能、構成、操作手順について説明します。ソフトウェアの使用方法や安定性を確保するため、以下の内容を参照し、取扱説明書をよくお読みの上、設置・運転してください。

1.2 変更の概要

以下は、本バージョンと旧バージョンの主な変更点である。

- Reportモジュールに新たに追加された皮膚表面温度の統計情報詳細は「皮膚表面温度統計報告書」を参照のこと。
- AIダッシュボードモジュールに新たに追加された皮膚表面温度モニタリング詳細はこちら
皮膚表面温度
- 顔画像検索の結果を、皮膚表面温度とマスク情報で表示することができます。詳細については、「顔画像取得」を参照してください。
- アクセス制御装置のための皮膚表面温度関連情報の表示をサポートする。詳細については、「Search Historical Events」を参照してください。
- 皮膚表面温度関連情報の表示をサポートする。詳細はこちらをご覧ください。リアルタイムアクセスレコードをチェックします。

第2章 サービス管理

iVMS-4200サービスは、主にデータ保存、データ管理、およびデータ計算に適用できません。連続実行および処理により、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できます。また、iVMS-4200サービスは、ユーザーの許可、デバイス、グループ、ログなどの管理も提供します。

モジュールの動作状態を表示し、「ポートの編集」をクリックしてポートを編集できます。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。

ルータに設定されているISUPポート番号を入力して、クライアントにISUPデバイスを追加して管理できるようにします。

WAN Address をチェックし、ポートマッピングの IP Address を入力するか、Event Upload Port (ISUP 4.0)、Event Upload Port (ISUP 5.0)、および Picture Storage Server Port を編集します。

自動起動をチェックして、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します。

iVMS-4200サービスを実行しても、表示されません。システムトレイを入力し、クリックしてサービス管理ウィンドウを開きます。🔄

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、再度ログインする必要があります。
 - クライアントは、同じコンピュータ上で同時に実行できるオペレーティング・システム・ユーザーは1人だけです。
 - 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 (Digital Video Recorder)、NVR (Network Video Recorder)、セキュリティコントロールパネル、ビデオインターホンデバイス、アクセスコントロールデバイスなど、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ディング装置を追加した後にライブビューまたは再生を表示したり、セキュリティコントロールパネルのゾーンをアームまたは解除したり、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けたり、クライアントにアクセスコントロール装置を追加した後に入退室を制御したり、出席を管理したりすることができます。

3.1 デバイスの起動

非アクティブデバイスの場合、ソフトウェアに追加して正常に動作する前に、アクティブにするためのパスワードを作成する必要があります。

開始前に

アクティブにするデバイスがネットワークに接続されており、クライアントを実行するPCと同じサブネットにあることを確認します。

ステップ

注記

この機能は、装置がサポートする必要があります。

1. [Device Management]ページを入力します。
2. 右パネル上部の[Device]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、ページの下部に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機器が一覧に表示されます。
4. デバイスのステータス(セキュリティレベルの列に表示)を確認し、非アクティブデバイスを選択します。

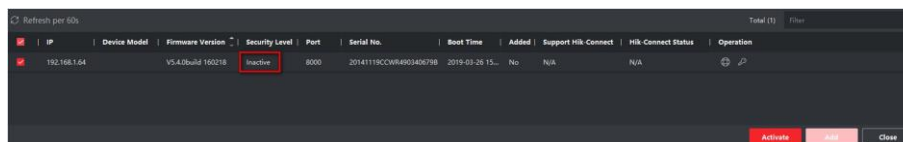


図3-1 オンライン非アクティブデバイス

5. [Activation]をクリックして[Activation]ダイアログを開きます。
6. パスワードフィールドにパスワードを作成し、パスワードを確認します。

**注意**

デバイスのパスワード強度を自動的にチェックすることができます。あなたの製品の安全性を高めるために、あなたが選択したパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3種類以上を含む最低8文字を使用してください)。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、パスワードを毎月または毎週変更することで、製品をより良く保護することができます。

すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストーラーおよび/またはエンドユーザーの責任です。

7. オプション:非アクティブネットワークカメラと接続しているNVRデバイスの場合は、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にパスワードを作成し、NVR経由でネットワークカメラを起動するための確認パスワードを入力します。
8. オプション:デバイスがサポートしている場合、デバイスをアクティブにするときにクラウドP2Pサービスを有効にします。
 - 1) 「クラウドP2Pを有効にする」をチェックして、「Note」ダイアログを開きます。
 - 2) 検証コードを作成する。
 - 3) 検証コードを確認する。
 - 4) 「サービスの条件とプライバシー・ポリシー」をクリックして、要件を読んでください。
 - 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ブにします。
10. オプション: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)を編集するには、「操作」列をクリックします。

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、およびHiDDNSを含む様々なデバイス追加モードを提供する。また、クライアントは、大量のデバイスが追加される場合に、複数のデバイスを一括してインポートすることもサポートします。

3.2.1 単一または複数のオンラインデバイスの追加

クライアントは、クライアントを実行しているPCと同じネットワーク内にあるオンラインデバイスを検出できます。検出されたオンラインデバイスをオンラインデバイスリストに表示して選択し、クライアントに追加することができます。検出されたオンラインデバイスが同じユーザー名とパスワードを共有する場合は、それらを一括してクライアントに追加することができます。

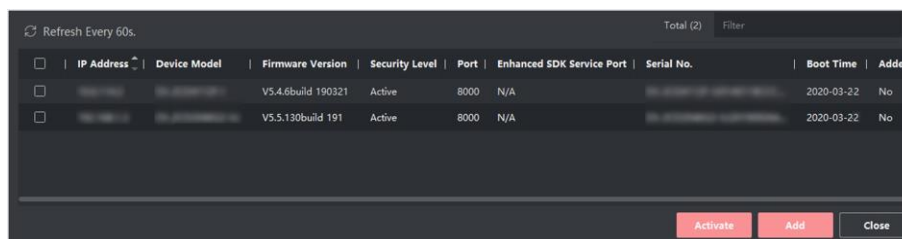
開始前に

- 追加するデバイスは、クライアントを実行しているPCと同じネットワーク内にあります。
- 追加するデバイスがアクティブになっています。

ステップ

1. [Device Management]→[Device]→[Device]をクリックします。
2. 「オンラインデバイス」をクリックして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機器が一覧に表示されます。



The screenshot shows a web interface for managing online devices. At the top, there is a 'Refresh Every 60s.' button and a 'Total (2)' indicator. Below this is a table with columns for IP Address, Device Model, Firmware Version, Security Level, Port, Enhanced SDK Service Port, Serial No., Boot Time, and Added. Two devices are listed in the table. At the bottom right of the table area, there are three buttons: 'Activate', 'Add', and 'Close'.

IP Address	Device Model	Firmware Version	Security Level	Port	Enhanced SDK Service Port	Serial No.	Boot Time	Added
		V5.4.6build 190321	Active	8000	N/A		2020-03-22	No
		V5.5.130build 191	Active	8000	N/A		2020-03-22	No

図3-2 オンラインデバイス

3. 「オンラインデバイス」エリアで、1つ以上のオンラインデバイスをチェックし、「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。

Add ×

Name

IP Address

Transmission Encryptio...

Port

User Name

Password

Synchronize Time

Import to Group

① Set the device name as the group name and add all the channels connected to the device to the group.

Add Cancel

図3-3 オンラインデバイスの追加

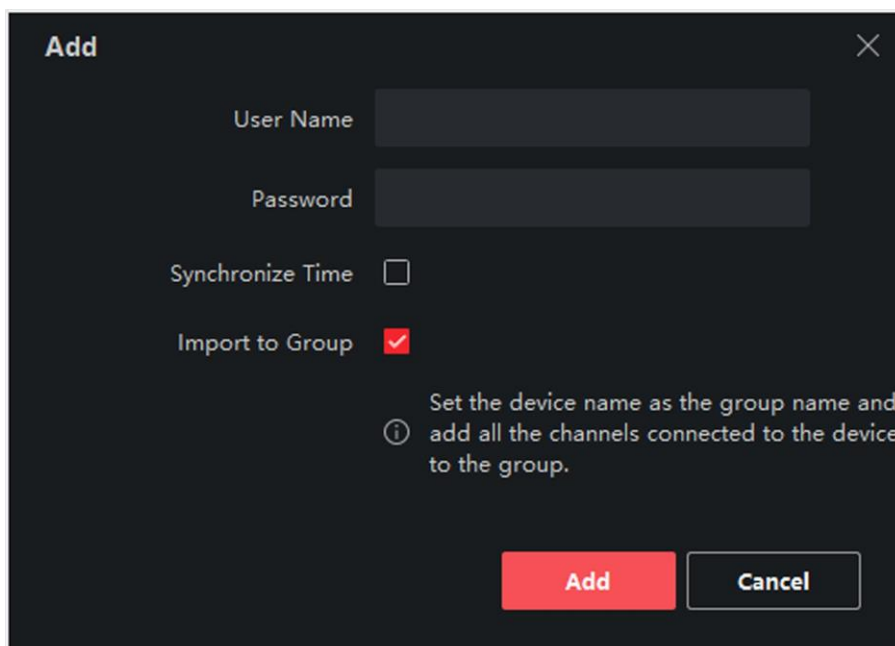


図 3-4 複数のオンラインデバイスの追加

4. 必要な情報を入力します。

氏名

デバイスの説明名を入力します。

IPアドレス

デバイスのIPアドレスを入力します。デバイスのIPアドレスは、この追加モードで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。デバイスのポート番号が自動的に取得されます。

この追加モードでは。

ユーザー名

デフォルトでは、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強度を自動的にチェックすることができます。あなたの製品の安全性を高めるために、あなたが選択したパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3種類以上を含む最低8文字を使用してください)。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、パスワードを毎月または毎週変更することで、製品をより良く保護することができます。

すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストーラーおよび/またはエンドユーザーの責任です。

-
- オプション:TLS(Transport Layer Security)プロトコルを使用して送信暗号化を有効にするために、TLS (Transport Layer Security)をチェックします。

**注記**

- この機能は、装置がサポートする必要があります。
- Certificate Verificationを有効にした場合は、Open Certificate Directory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され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する必要があります。証明書の検証を有効にする方法の詳細については、証明書の検証(Transmission Encryption)を参照してください。
- デバイスにログインして、Webブラウザで証明書ファイルを取得できます。

-
- [Synchronize Time]をチェックして、クライアントを実行しているPCとデバイスの時刻を同期させます。クライアントにデバイスを追加する。
 - オプション:「Import to Group」をチェックして、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

符号化装置については、その符号化チャンネル及びアラーム入出力がこのグループにインポートされる。

アクセス制御装置では、アクセスポイント、アラーム入出力、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。

- 追加をクリックします。

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アドレスまたはドメイン名が分かっている場合は、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して、クライアントにデバイスを追加できます。

ステップ

1. デバイス管理モジュールを入力します。
2. 右パネル上部の[Device]タブをクリックします。
追加したデバイスが右パネルに表示されます。
3. 「追加」をクリックして「追加」ウィンドウを開き、追加モードとして「IP/Domain」を選択します。
4. 必要な情報を入力します。

氏名

デバイスの説明的な名前を作成します。たとえば、デバイスの場所や機能を示すニックネームを使用できます。

住所

デバイスのIPアドレスまたはドメイン名。

ポート

追加するデバイスは同じポート番号を共有します。デフォルト値は8000です。

ユーザー名

デバイスユーザー名を入力します。デフォルトでは、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強度を自動的にチェックすることができます。あなたの製品の安全性を高めるために、あなたが選択したパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3種類以上を含む最低8文字を使用してください)。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、パスワードを毎月または毎週変更することで、製品をより良く保護することができます。すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストーラーおよび/またはエンドユーザーの責任です。

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の追加」をチェックします。
 - 2) 機器のチャンネル番号、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すると、デバイスネットワークのステータスは「オフライン」と表示され、デバイスがオンラインになるとデバイスネットワークのステータスは「オンライン」になり、クライアントが自動的に接続します。

6. オプション:TLS(Transport Layer Security)プロトコルを使用して送信暗号化を有効にするために、TLS (Transport Layer Security)をチェックします。

 注記

- ・ この機能は、装置がサポートする必要があります。
 - ・ Certificate Verificationを有効にした場合は、Open Certificate Directory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され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する必要があります。証明書の検証を有効にする方法の詳細については、証明書の検証(Transmission Encryption)を参照してください。
 - ・ デバイスにログインして、Webブラウザで証明書ファイルを取得できます。
-

7. [Synchronize Time]をチェックして、クライアントを実行している PC とデバイスの時刻を同期させます。クライアントにデバイスを追加する。
8. オプション : 「Import to Group」をチェックして、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

符号化装置については、その符号化チャンネル及びアラーム入出力がこのグループにインポートされる。

アクセス制御装置では、アクセスポイント、アラーム入出力、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。
 - 追加をクリックしてデバイスを追加し、デバイスリストページに戻ります。
 - 「追加」および「新規」をクリックして設定を保存し、他のデバイスの追加を続行します。

10. オプション:以下の操作を行います。

リモート構成	<p>「操作」列をクリックして、該当するデバイスのリモート構成を設定します。</p> <hr/> <p> 注記 リモート構成の詳細な操作手順については、装置のユーザーマニュアルを参照してください。</p>
装置の状況	「操作」欄をクリックすると、カメラ、記録状態、信号状態、ハードウェア状態などの機器の状態が表示されます。
デバイスの編集情報	「操作」列をクリックして、IP アドレス、ユーザー名、およびパスワードなどのデバイス情報を編集します。
オンライン・ユーザーのチェック	「操作」列をクリックして、デバイスにアクセスするオンライン・ユーザー(ユーザー名、ユーザー・タイプ、ユーザーの IP アドレス、およびログイン時刻など)を確認します。
リフレッシュ	「操作」列をクリックして、最新のデバイス情報を取得します。
デバイスの削除	1 つまたは複数のデバイスを選択し、「削除」をクリックして、選択したデバイスをクライアントから削除します。

3.2.3 IP セグメントごとのデバイスの追加

デバイスが同じポート番号、ユーザー名、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する場合、デバイスの開始 IP アドレス、エンド 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することにより、クライアントにそれらを追加できます。

ステップ

1. デバイス管理モジュールを入力します。
2. 右パネル上部の[Device]タブをクリックします。
追加したデバイスが右パネルに表示されます。
3. 「追加」をクリックして、「追加」ウィンドウを開きます。
4. 追加モードとして IP Segment を選択します。
5. 必要な情報を入力します。

IP の開始

開始 IP アドレスを入力します。

エンド IP

始点 IP と同じネットワークセグメントにエンド IP アドレスを入力します。

ポート

デバイス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

デフォルトでは、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強度を自動的にチェックすることができます。あなたの製品の安全性を高めるために、あなたが選択したパスワードを変更することを強くお勧めします (大文字、小文字、数字、特殊文字の 3 種類以上を含む最低 8 文字を使用してください)。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、パスワードを毎月または毎週変更することで、製品をより良く保護することができます。

すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストーラーおよび/またはエンドユーザーの責任です。

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の追加」をチェックします。
- 2) 機器のチャンネル番号、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すると、デバイスネットワークのステータスは「オフライン」と表示され、デバイスがオンラインになるとデバイスネットワークのステータスは「オンライン」になり、クライアントが自動的に接続します。

7. オプション:TLS(Transport Layer Security)プロトコルを使用して送信暗号化を有効にするために、TLS (Transport Layer Security)をチェックします。

 注記

- この機能は、装置がサポートする必要があります。
- Certificate Verificationを有効にした場合は、Open Certificate Folder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され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する必要があります。証明書の検証を有効にする方法の詳細については、証明書の検証(Transmission Encryption)を参照してください。
- デバイスにログインして、Webブラウザで証明書ファイルを取得できます。

8. [Synchronize Time]をチェックして、クライアントを実行しているPCとデバイスの時刻を同期させます。クライアントにデバイスを追加する。
9. オプション: 「Import to Group」をチェックして、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。
 - 追加をクリックしてデバイスを追加し、デバイスリストページに戻ります。
 - 「追加」および「新規」をクリックして設定を保存し、他のデバイスの追加を続行します。
11. オプション:以下の操作を行います。

リモート構成	<p>「操作」列をクリックして、該当するデバイスのリモート構成を設定します。 </p> <hr/> <p> 注記</p> <p>リモート構成の詳細な操作手順については、装置のユーザーマニュアルを参照してください。</p>
装置の状況	「操作」欄をクリックすると、カメラ、記録状態、信号状態、ハードウェア状態などの機器の状態が表示されます。 
デバイスの編集情報	「操作」列をクリックして、IPアドレス、ユーザー名、およびパスワードなどのデバイス情報を編集します。 
オンライン・ユーザーのチェック	「操作」列をクリックして、デバイスにアクセスするオンライン・ユーザー(ユーザー名、ユーザー・タイプ、ユーザーのIPアドレス、およびログイン時刻など)を確認します。 
リフレッシュ	「操作」列をクリックして、最新のデバイス情報を取得します。 
デバイスの削除	1つまたは複数のデバイスを選択し、「削除」をクリックして、選択したデバイスをクライアントから削除します。

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、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クライアントに追加できます。

開始前に

まず、Cloud P2Pアカウントに登録し、ログインしていることを確認します。

ステップ

1. デバイス管理モジュールを入力します。
追加したデバイスが右パネルに表示されます。
2. 右パネル上部の[Device]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。
 - 初めてクラウドP2Pアカウントにログインする必要があります。
 - ログインしたクラウドP2Pアカウントが表示されます。
5. 「ログインする領域を選択」のドロップダウンリストでログインする領域を選択し、クラウドの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。
 - 機器ラベルに表示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、Online Deviceをクリックします。
自動的にシリアル番号を取得するオンラインデバイスを選択します。
6. デバイスの検証コードを入力します。

注記

デバイスをアクティブにし、クラウドP2Pサービスを有効にするときに検証コードを作成することができます。また、ストリーム暗号化を有効にするときに作成した検証コードと同じです。また、デバイス設定ページで作成することもできます。

7. オプション:クラウドP2PドメインからデバイスにアクセスするためにDDNSを有効にします。

デバイスドメイン名

クラウドP2Pサーバに登録された機器のIPアドレスとポートを取得するために

使用する機器ドメイン名をカスタマイズします。

UPnPモード自動

UPnPモードとしてAutoを選択すると、デバイスのポート番号が自動的に取得されます。

マニュアル

UPnP ModeとしてManualを選択し、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

デバイスユーザー名を入力します。デフォルトでは、ユーザー名はadminです。

パスワード

デバイスをアクティブにしたときに作成されるデバイスパスワードを入力します。



注意

デバイスのパスワード強度を自動的にチェックすることができます。あなたの製品の安全性を高めるために、あなたが選択したパスワードを変更することを強くお勧めします（大文字、小文字、数字、特殊文字の3種類以上を含む最低8文字を使用してください）。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、パスワードを毎月または毎週変更することで、製品をより良く保護することができます。

すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストーラーおよび/またはエンドユーザーの責任です。






注記

DDNS機能を無効にすると、クライアント経由で追加したデバイスのステータス表示、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コードの生成などの操作ができなくなります。

8. オプション:グループへのインポートをチェックして、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グループにインポートします。
9. クライアントソフトウェアおよびクラウドP2Pアカウントにデバイスを追加します。
 - 追加をクリックしてデバイスを追加し、デバイスリストに戻ります。
 - 「追加」および「新規」をクリックしてデバイスを追加し、次のデバイスの追加を続けます。

10. オプション:以下の操作を行います。

リモート構成	<p>「操作」列をクリックして、該当するデバイスのリモート構成を設定します。 </p> <hr/> <p> 注記 リモート構成の詳細な操作手順については、装置のユーザーマニュアルを参照してください。</p> <hr/>
デバイスの編集情報	<p>クリックして、デバイスの詳細を編集します。 </p>
デバイスの削除	<p>1つまたは複数のデバイスを選択し、「削除」をクリックして、選択したデバイスをクライアントから削除します。</p>

3.2.5 ISUP アカウントによるデバイスの追加

アクセス制御デバイスがISUP 5.0プロトコルをサポートする場合、サーバアドレス、ポート番号、デバイスIDを設定している場合は、デバイスIDとキーを入力した後、ISUPプロトコルによってクライアントに追加できます。

開始前に

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ます。

ステップ

1. デバイス管理モジュールを入力します。
追加したデバイスが右パネルに表示されます。
2. 「追加」をクリックして、「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プロトコルに登録されているアカウント名を入力します。

ISUPキー

ISUP 5.0デバイスの場合、デバイスのネットワーク・センター・パラメータを設定するときにISUPキーを入力します。



この機能は、装置がサポートする必要があります。

5. オプション:クライアントを実行しているPCとデバイス時刻を同期させるための同期時間をチェックします。クライアントにデバイスを追加した後
6. オプション:「Import to Group」をチェックして、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。
 - 追加をクリックしてデバイスを追加し、デバイスリストに戻ります。
 - 「追加」および「新規」をクリックして設定を保存し、他のデバイスの追加を続行します。



注記

顔写真は、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機器には適用できません。

8. オプション:以下の操作を行います。

装置の状況	「操作」列をクリックして、デバイスのステータスを表示します。
デバイスの編集情報	「操作」列をクリックして、デバイス名、デバイスアカウント、およびISUPキーなどのデバイス情報を編集します。
オンライン・ユーザーのチェック	「操作」列をクリックして、デバイスにアクセスするオンライン・ユーザー(ユーザー名、ユーザー・タイプ、ユーザーのIPアドレス、およびログイン時刻など)を確認します。
リフレッシュ	「操作」列をクリックして、最新のデバイス情報を取得します。
デバイスの削除	1つまたは複数のデバイスを選択し、「削除」をクリックして、選択したデバイスをクライアントから削除します。

3.2.6 HiDDNS によるデバイスの追加

HiDDNSはグラスフィアの無料DNSサーバです。デバイスに十分なIPアドレスがない場合は、デバイスをHiDDNSサーバに登録した後、HiDDNSモードでクライアントにデバイスを追加できます。HiDDNSは、ネットワークへの良質な接続のために、デバイスのIPアドレスとしてドメイン名を解析します。

ステップ

1. デバイス管理モジュールを入力します。
追加したデバイスが右パネルに表示されます。
2. 右パネル上部の[Device]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。

サーバアドレス

www.hik-online.com

ドメイン

HiDDNSサーバに登録されている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強度を自動的にチェックすることができます。あなたの製品の安全性を高めるために、あなたが選択したパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3種類以上を含む最低8文字を使用してください)。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、パスワードを毎月または毎週変更することで、製品をより良く保護することができます。

すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストーラーおよび/またはエンドユーザーの責任です。

-
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の追加」をチェックします。
 - 2) 機器のチャンネル番号、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すると、デバイスネットワークのステータスは「オフライン」と表示され、デバイスがオンラインになると、デバイスネットワークのステータスは「オンライン」になり、クライアントが自動的に接続します。







-
7. オプション: クライアントを実行しているPCとデバイス時刻を同期させるための同

期時間をチェックします。

クライアントにデバイスを追加した後

8. オプション: 「Import to Group」をチェックして、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。
 - 追加をクリックしてデバイスを追加し、デバイスリストページに戻ります。
 - 「追加」および「新規」をクリックして設定を保存し、他のデバイスの追加を続行します。

10. オプション: 以下の操作を行います。

リモート構成	「操作」列をクリックして、該当するデバイスのリモート構成を設定します。   注記 リモート構成の詳細な操作手順については、装置のユーザーマニュアルを参照してください。
装置の状況	「操作」欄をクリックすると、カメラ、記録状態、信号状態、ハードウェア状態などの機器の状態が表示されます。 
デバイスの編集情報	「操作」列をクリックして、IPアドレス、ユーザー名、およびパスワードなどのデバイス情報を編集します。 
オンライン・ユーザーのチェック	「操作」列をクリックして、デバイスにアクセスするオンライン・ユーザー(ユーザー名、ユーザー・タイプ、ユーザーのIPアドレス、およびログイン時刻など)を確認します。 
リフレッシュ	「操作」列をクリックして、最新のデバイス情報を取得します。 
デバイスの削除	1つまたは複数のデバイスを選択し、「削除」をクリックして、選択したデバイスをクライアントから削除します。

3.2.7 バッチ内のデバイスのインポート

あらかじめ定義されたCSVファイルにデバイスパラメータを入力することにより、複数のデバイスを一括してクライアントに追加することができます。

ステップ

1. デバイス管理モジュールを入力します。
2. 右パネル上部の[Device]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、追加モードとしてバッチインポートを選択します。
4. Export Templateをクリックし、あらかじめ定義されたテンプレート(CSVファイル)を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、該当する列に追加するデバイスに必要な情報を入力します。

 注記

必要なフィールドの詳細については、テンプレートの序文を参照してください。

追加モード

0または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

デバイスユーザー名を入力します。デフォルトでは、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強度を自動的にチェックすることができます。あなたの製品の安全性を高めるために、あなたが選択したパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3種類以上を含む最低8文字を使用してください)。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、パスワードを毎月または毎週変更することで、製品をより良く保護することができます。

すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストーラーおよび/またはエンドユーザーの責任です。

オフラインデバイスの追加

1を入力すると、オフラインデバイスを追加できます。

オフラインデバイスをクライアントに追加すると、デバイスネットワークのステータスは「オフライン」と表示され、デバイスがオンラインになるとデバイ

ネットワークのステータスは「オンライン」になり、クライアントが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。

グループへのインポート

デバイス名でグループを作成するには、1を入力します。デバイスのすべてのチャンネルがデフォルトで対応するグループにインポートされます。0を入力すると、本機能は無効になります。

チャンネル番号


「オフラインデバイスの追加」を有効にする場合は、デバイスのチャンネル番号を入力します。Addを無効にすると
オフラインデバイス、このフィールドは必要ありません。

アラーム入力番号

「オフラインデバイスの追加」を有効にする場合は、デバイスのアラーム入力番号を入力します。無効にした場合
[オフラインデバイスの追加]フィールドは不要です。

6. テンプレートファイルをクリックして選択します。📄
7. [追加]をクリックしてデバイスをインポートします。

8. オプション:以下の操作を行います。

<p>リモート構成</p>	<p>「操作」列をクリックして、該当するデバイスのリモート構成を設定します。⚙️</p> <hr/> <p> 注記 リモート構成の詳細な操作手順については、装置のユーザーマニュアルを参照してください。</p>
<p>装置の状況</p>	<p>「操作」欄をクリックすると、カメラ、記録状態、信号状態、ハードウェア状態などの機器の状態が表示されます。📺</p>
<p>デバイスの編集情報</p>	<p>「操作」列をクリックして、IPアドレス、ユーザー名、およびパスワードなどのデバイス情報を編集します。✎</p>
<p>オンライン・ユーザーのチェック</p>	<p>「操作」列をクリックして、デバイスにアクセスするオンライン・ユーザー(ユーザー名、ユーザー・タイプ、ユーザーのIPアドレス、およびログイン時刻など)を確認します。🔍</p>
<p>リフレッシュ</p>	<p>「操作」列をクリックして、最新のデバイス情報を取得します。🔄</p>
<p>デバイスの削除</p>	<p>1つまたは複数のデバイスを選択し、「削除」をクリックして、選択したデバイスをクライアントから削除します。</p>

3.3 デバイスの復元/リセットパスワード

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したり、デバイスのパスワードをリセットすることができます。

3.3.1 デバイスのリセットパスワード

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パスワードをリセットできます。

ステップ

1. [デバイス管理]ページを入力します。
2. 右パネル上部の[Device]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す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、「操作」列をクリックします。🔗
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、デバイスファイルをPCに保存し、当社のテクニカルサポートに送信します。

注記

以下のリセット方法については、弊社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 Codeウィンドウをポップアップし、「ダウンロード」をクリックしてQR CodeをPCに保存します。また、QRコードの写真を撮影して、端末に保存することもできます。この写真を弊社のテクニカルサポートに送ってください。

注記

以下のリセット方法については、弊社テクニカルサポートまでお問い合わせください。

実際のニーズに合わせてセーフモードを選択します。

注記

以下のリセット方法については、弊社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強度を自動的にチェックすることができます。あなたの製品の安全性を高めるために、あなたが選択したパスワードを変更することを強くお勧めします（大文字、小文字、数字、特殊文字の3種類以上を含む最低8文字を使用してください）。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、パスワードを毎月または毎週変更することで、製品をより良く保護することができます。すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストーラーおよび/またはエンドユーザーの責任です。

3.3.2 デバイスのデフォルト・パスワードの復元

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フォルトパスワードを復元できます。

ステップ

1. [デバイス管理]ページを入力します。
2. 右パネル上部の[Device]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、ページの下部に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す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、「Operation」列をクリックすると、「Reset Password」画面が表示されます。
5. デバイスのパスワードを復元します。
 - 端末暗証番号を入力すると、選択した機器のデフォルトパスワードを復元できます。

 注記

暗証番号の取得については、弊社テクニカルサポートまでお問い合わせください。

- 「エクスポート」をクリックして、デバイスファイルをPCに保存し、当社のテクニカルサポートにファイルを送信します。

 注記

以下のリセット方法については、弊社テクニカルサポートまでお問い合わせください

い。

次にすべきこと

adminアカウントのデフォルトパスワード(12345)は、初回ログインの目的にのみ使用されます。製品が適切に機能しない可能性がある、および/または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他者による不正アクセスなどのセキュリティリスクから保護するために、このデフォルトパスワードを変更しなければなりません。



注意

デバイスのパスワード強度を自動的にチェックすることができます。選択したパスワードを変更することを強くお勧めします(少なくとも8文字以上)。

製品の安全性を高めるために、大文字、小文字、数字、特殊文字の3種類のカテゴリーを指定します。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、パスワードを毎月または毎週変更することで、製品をより良く保護することができます。すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストーラーおよび/またはエンドユーザーの責任です。

3.4 デバイス・ファームウェア・バージョンアップ

追加したデバイスで使用できる新しいファームウェアバージョンがある場合は、ファームウェアをアップグレードできます。クライアント経由のバージョン



注記

- デバイスはこの機能をサポートする必要があります。
- [System Configuration]でアップグレードモードを設定できます。詳細は、「一般パラメータの設定」を参照してください。

デバイス管理モジュールを入力し、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。アップグレードモードに応じて、以下の操作を行います。

無効

[Device for Management]パネルで、新しいバージョンのファームウェアがある場合は、デバイスの[Firmware Upgrade]列のステータスが[Upgradeable]になります。アップグレード可能なデバイスを選択し、「アップグレード」をクリックして、デバイスファ



注記

ームウェアのアップグレードを開始します。
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のステータスがアップグレードになります。

ダウンロードおよびアップグレードの場合、迅速にお知らせください。

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。Upgrade All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。

アップグレードの場合は、ダウンロードと迅速なMe

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。Upgrade All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。

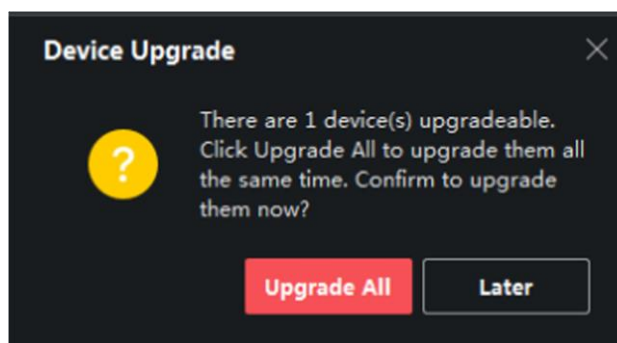


図3-5 デバイスのアップグレード・プロンプト

注記

Upgrade Allをクリックすると、詳細を表示するためのプロンプトが表示されます。
[Device Management]ページにない場合は[View Details]をクリックして[Device Management]ページにジャンプし、[Device Management]ページにある場合はプロンプトを閉じます。

自動的にダウンロードおよび更新する

クライアントは、デバイスの新しいバージョンを検出した後、ユーザに気づかずに新しいバージョンをダウンロードし、新しいバージョンをアップグレードします。
「デバイス管理」ページでは、「ファームウェアアップデート」欄に以下の更新状況が表示されます。


使用可能なバージョンがない

新しいファームウェアバージョンは使用できません。

アップグレード可能

新しいファームウェアバージョンが利用できます。

注記

カーソルを移動すると、現在のバージョン、最新バージョン、およびアップグレードの内容が表示されます。  [ファームウェアのバージョン](#)

待ち

デバイスはアップグレードを待っています。

ダウンロード

クライアントは新しいファームウェアバージョン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行われています。

アップグレード後

アップグレード後のバージョンを表示するには、アップグレードのカーソルをホールドします。

アップグレード失敗

アップグレードに失敗すると、詳細を表示するプロンプトが表示されます。[Device Management]ページにない場合は[View Details]をクリックして[Device Management]ページにジャンプし、[Device Management]ページにある場合はプロンプトを閉じます。アップグレードのカーソルをホールドし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てください。

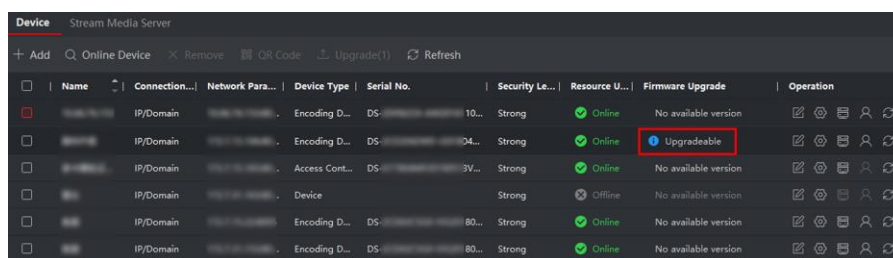



図3-6 ファームウェアのアップグレード

3.5 追加されたデバイスの管理

デバイスリストにデバイスを追加した後、デバイスパラメータの編集、リモート設定、デバイスステータスの表示など、追加したデバイスを管理できます。

表3-1 追加されたデバイスの管理

デバイスの編集	クリックすると、デバイス名、アドレス、ユーザー名、パスワードなどのデバイス情報が編集されます。
デバイスの削除	1つ以上のデバイスをチェックし、削除をクリックして選択したデバイスを削除します。
リモート設定	該当するデバイスのリモート設定を設定するには、をクリックします。詳しくは、機器の取扱説明書をご覧ください。
デバイスステータスの表示	<p>クリックすると、カメラ、記録状態、信号状態、ハードウェア状態などのデバイスステータスが表示されます。</p> <hr/> <p> 注記 異なるデバイスについては、デバイスのステータスに関する異なる情報が表示されます。</p>
オンラインユーザーの表示	クリックすると、デバイスにアクセスするオンラインユーザーの詳細(ユーザー名、ユーザータイプ、IPアドレス、ログイン時間など)が表示されます。
デバイスのリフレッシュ情報	最新のデバイス情報を取得するには、クリックします。
QRコード生成	1つ以上のデバイスをチェックし、QR Codeをクリックして追加したデバイスのQRコードを生成します。QRコードを読み取ることで、モバイルクライアントにデバイスを追加できます。

	 注記 ISUPまたはクラウドP2Pによって追加されたデバイスはQRコードを生成できません。
デバイスのアップグレード	[Firmware Upgrade]列でデバイスのステータスを表示し、1つ以上のアップグレード可能なデバイスを確認し、[Upgrade Device Firmware]をクリックして選択したデバイスをアップグレードします。詳細については、「デバイスファームウェアバージョンのアップグレード」を参照してください。
デバイスからのイベントの取得	1つのデバイスをチェックし、「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させます。詳細については、「デバイスからイベントを取得する」を参照してください。

3.6 グループ経営

クライアントは、異なるグループに追加されたリソースを管理するグループを提供します。リソースの場所に応じて、リソースを異なるグループにグループ化できます。

例

例えば、1階には、カメラ64台、ドア16台、警報入力64台、警報出力16台を設置しました。これらのリソースは、1つのグループ(1st Floorという名前)にまとめて管理することができます。リソースをグループごとに管理した後、ライブビューの取得、ビデオファイルの再生、ドアのステータスの制御、その他の操作を行うことができます。

3.6.1 グループリソース

クライアントは、グループを追加する2つの方法、すなわち、グループをカスタマイズする方法と、デバイス名でグループを作成する方法を提供します。グループをカスタマイズした後、このグループにリソースを手動でインポートする必要があります。デバイス名でグループを作成すると、デバイスのリソースが自動的にグループにインポートされます。実際のニーズに応じてリソースをグループ化する1つの方法を選択できます。

ステップ

1. Maintenance and Managementエリアで、[Device Management]→[Group]をクリックし、グループ管理ページに入ります。
2. グループを追加する。
 - グループのカスタマイズ:グループの追加をクリックし、新しいグループの名前を

作成します。

- [デバイス名でグループを作成]-[デバイス名でグループを作成]をクリックし、追加したデバイスを選択して、選択したデバイス名で新しいグループを作成します。デバイス名でグループを作成すると、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、アラーム出力、アクセスポイントなど)がデフォルトでグループに自動的にインポートされます。

注記

- 最大256のグループを追加できます。
- キーボードのShiftキーまたはCtrlキーを押したままにして、複数のグループを選択できます。

3. グループを追加した後、グループにリソースをインポートする必要があります。

注記

1つのリソースについては、異なるグループに追加できます。

- 1) インポートするリソースのタイプを選択し、インポートをクリックします。
- 2) インポートするリソースを選択し、インポートをクリックして、選択したすべてのリソースをこのグループにインポートします。
4. オプション:グループを追加した後、必要に応じて以下の操作のいずれかを実行します。

リソースリストの展開 または折りたたみ	グループ内のリソース・リストを展開または折りたたむには、/をクリックします。▶▼
検索リソース	キーワードを入力し、クリックしてターゲット・リソースを検索します。🔍
グループからのリソースの削除	リソースを選択し、「削除」をクリックして、選択したリソースをグループから除去します。

3.6.2 リソース・パラメーターの編集

リソースをグループにインポートした後、リソース・パラメーターを編集できます。エンコードチャンネルの場合、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。接続先は接続先の名前を編集できます。アラーム入力は、アラーム入力名を編集します。ここでは、エンコーディングチャンネルを例にとります。

開始前に

グループにリソースをインポートします。

ステップ

1. デバイス管理モジュールを入力します。
2. 「デバイス管理」→「グループ」をクリックして、グループ管理ページに入ります。追加したグループはすべて左側に表示されます。
3. グループリストからグループを選択し、「エンコーディングチャンネル」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ディングチャンネルが表示されます。
4. 「操作」列をクリックして、「リソースの編集」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

カメラのライブビューのストリームタイプを任意に選択します。



有効にするには、もう一度ライブビューを開始する必要があります。

再生ストリームタイプ

カメラの再生に使用するストリームの種類を任意に選択します。



- 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は、このフィールドが表示されます。
 - 有効にするには、もう一度ライブビューを開始する必要があります。
-

回転式

カメラのライブビューまたは再生の回転タイプを任意に選択します。

プロトコルタイプ

カメラの伝送プロトコルを選択します。



有効にするには、もう一度ライブビューを開始する必要があります。

ストリーミングプロトコル

ライブビュー時にストリームを取得するには、プロトコルをRTSPまたはプライベートとして選択します。



有効にするには、もう一度ライブビューを開始する必要があります。

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を介して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。

リフレッシュ

カメラのライブビューの新しい撮影画像を取得します。

6. 「OK」をクリックして、新しい設定値を保管する。











第4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ーのライブビデオをメインビューページで表示できます。また、撮影、手動記録、ウインドウ分割、PTZ制御、ライブビュー中のオートスイッチなど、いくつかの基本操作をサポートしています。

4.1 ライブビューツールバー

ライブビューツールバーは、ライブビューウインドウの操作や管理を簡単かつ迅速に行うことができます。たとえば、ピクチャの取り込み、オーディオの記録、音量の調整、ツールバーのツールの1クリックでウインドウを分割することができます。

表4-1 ツールバーの説明

アイコン	関数名	機能説明と操作
	ビューの保存	現在作成しているビューを保存します。これは、必要なカメラをすばやく表示するのに便利です。 クリックして、保存ビューのウインドウをポップアップします。選択  ビューまたは現在のビュー、およびビューの名前を作成します。
	ライブビューの停止	すべてのライブビューカメラを停止します。
	消音/消音解除	ボリュームバーをポップアップするにはクリックし、ミュートをキャンセルするにはクリックし、音量を調整します。   ボリュームバーをポップアップし、再度クリックしてライブビューカメラをミュートに設定します。 
	窓部	ライブビューの異なるウインドウ分割モードを選択します。クリックして1つのウインドウ分割モード(9ウインドウ分割など)を選択します。  追加をクリックして、ウインドウ分割モードをカスタマイズすることもできます。
	全画面	[ライブビュー]を全画面表示を在全屏モード下 <input type="checkbox"/> 示 <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> します。Escキーを押してフルスクリーンモードを終了します。





	構成	ライブビューパラメータ設定モードにして、設定します。 ライブビューと再生、画像、ファイル、ツールバー。
---	----	--


表 4-2 ライブビューウィンドウのアイコンの説明

アイコン	関数名	機能説明と操作
	キャプチャ	ライブビューウィンドウの写真を手動で撮影します。
	録画開始/録画停止	最初にクリックして録画を開始し、再度クリックして録画を停止し、設定したパスに自動的に録画ファイルを保存します。
	インスタント再生に切り替える	現在の時間では、直前の30秒間、1分間、3分間、5分間、8分間、10分間にビデオを再生するように選択できます。

42 カスタムビューの追加

ビューは、各ウィンドウにカメラを設定したウィンドウ分割であり、表示モードでは、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、後で関連するカメラにすばやくアクセスできます。たとえば、オフィスにあるカメラ1、カメラ2、およびカメラ3をリンクしてウィンドウを表示し、オフィスと呼ばれるビューとして保存することができます。

ステップ

1. メイン・ビュー・ページを入力します。
2. [リソース]タブをクリックします。
3. カーソルをリソース・パネルのカスタム・ビューに移動し、クリックして新しいビューを作成します。 

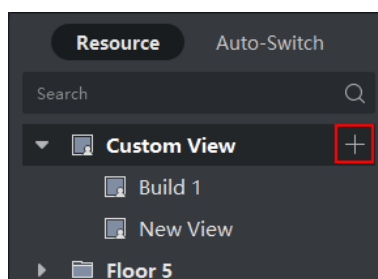



図 4-1 カスタムビューの追加

4. ビューの名前を入力します。
5. オプション:ライブビューツールバーでクリックして、新しいビューのウィンドウ分割モードを設定します。 

6. 指定したカメラのライブビューを、実際の必要に応じて指定したウィンドウで開始します。
7. 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。📁

 注記

最大16のカスタム・ビューをクライアントに追加できます。

8. オプション:カスタムビューを追加した後、以下の操作を行います。

ビュー名の編集 カーソルを新しいビューの上に移動し、クリックしてビュー名を編集します。✎

ビューの削除 新しいビューの上にカーソルを移動し、ビューを削除するにはクリックします。✕

次にすべきこと


再度クリックして、カスタムウィンドウの区分を選択します。📏

4.3 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、ライブビューを開始することができます。これにより、モニターされているエリアをよく知ることができます。1台のカメラまたは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。カスタムビューモードでライブビューを起動することもできます。

「メインビュー」→「リソース」をクリックして、「メインビュー」ページに入ります。左側のリソース・リストでリソースを選択し、以下の方法でライブ・ビューを開始します。

利用可能な方法	説明	操作
1台のカメラのライブビュー起動	グループ内の1台のカメラのみのライブビューを開始します。	<ul style="list-style-type: none"> • カメラを選択し、ウィンドウにドラッグします。 • グループでカメラをダブルクリックします。 • カメラ名の上にカーソルを合わせてクリックします。👉
カメラグループの開始ライブビュー	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期して開始します。	<ul style="list-style-type: none"> • グループを選択し、ウィンドウにドラッグします。 • グループをダブルクリックします。 • グループ名の上にカーソルを合わせてクリックするか、グループ内のすべてのカメラを表示をクリックします。👉 ...

<p>カスタムビューモードでライブビューを開始する</p>	<p>カスタムビューでカメラのライブビューを開始します。</p>	<ul style="list-style-type: none"> • カスタムビューを選択し、ウィンドウにドラッグします。 • カスタムビューをダブルクリックします。 <hr/> <p> 注記 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む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」を参照してください。</p>
-------------------------------	----------------------------------	--

 注記

デバイスがストリーム暗号化をサポートしており、ライブビューのストリームが暗号化されている場合は、ストリームキーを入力して二重に検証する必要があります。

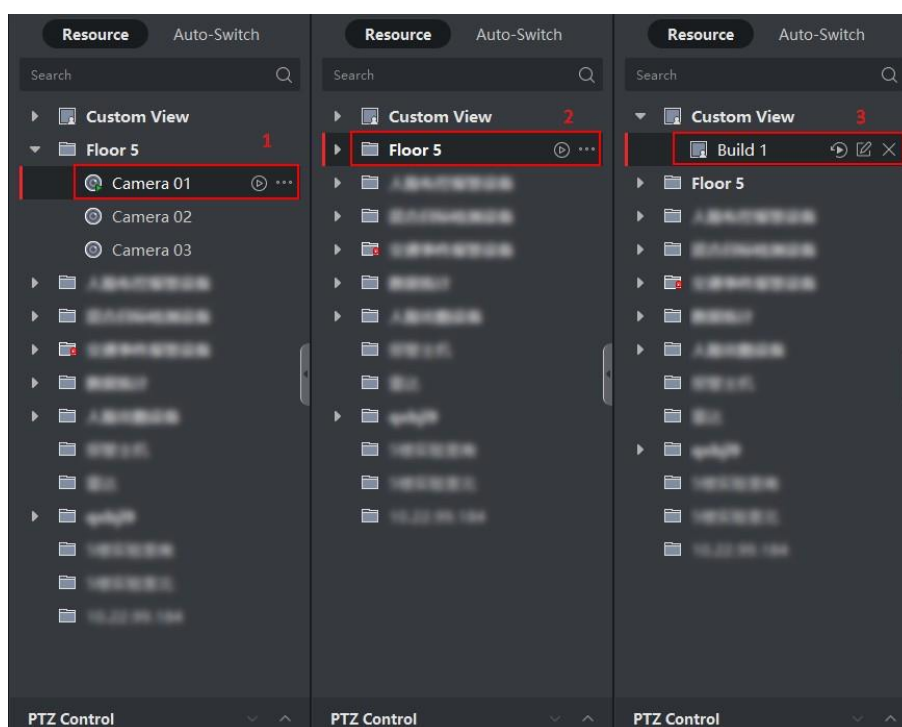


図 4-2 ライブビューの開始

4.4 ライブビューのオートスイッチ

カメラのライブビューを表示したり、「オートスイッチ」と呼ばれるカスタムビューを順に

表示できます。大量のカメラのライブビューを行いたい場合は、選択したカメラを自動的に切り替えることができます。つまり、クライアントはディスプレイウィンドウ内の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的に切り替えることもできます。

ライブビューでオートスイッチングを行うと、3つのモードがあります：

- デフォルト表示のすべてのカメラの自動切り替え
- グループ内のオートスイッチカメラ
- オートスイッチカスタムビュー

4.4.1 グループ内のオートスイッチカメラ

同じグループのカメラのビデオストリームは、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オートスイッチを起動すると、5台のカメラのライブビューが設定可能なインターバルと交互に表示されます。また、表示ウィンドウで再生などの操作を行うこともできます。

ステップ

1. メイン・ビュー・ページを入力します。
2. 左パネルのAuto-Switch → Single Window Auto-Switchをクリックして、グループを表示します。
3. 右パネルの表示ウィンドウを選択します。
4. カーソルをグループ名に合わせてクリック

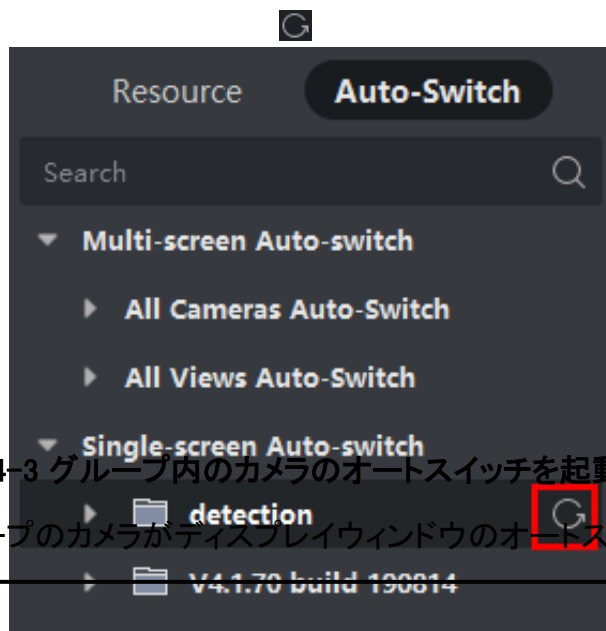



図 4-3 グループ内のカメラのオートスイッチを起動する

選択したグループのカメラがディスプレイウィンドウのオートスイッチを起動します。




オートスイッチ起動後、オーディオはデフォルトではオフになっています。

5. オプション:以下の操作を行います。

操作説明 オートスイッチを一時停止/再開します。 

一時停止/再開オートスイッチ

前ページ/次ページへ移動 クリックオア前後のグループのカメラの表示

Dwell時間設定 現在のオートスイッチを停止した後、オートスイッチ滞留時間をクリックまたは増減するには、ページ下部にある20秒をクリックしてオートスイッチ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。たとえば、インターバルを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。 

4.4.2 全カメラ自動切替

カメラリスト内のすべてのカメラのビデオをセルフアダプティブモードで自動的に切り替えることができます。すべてのカメラのオートスイッチを起動すると、すべてのカメラのライブビューをすばやく表示できます。

ライブビューの有効な方法です。オートスイッチは、設定可能な間隔で動作します。また、オートスイッチウインドウで再生などの操作を行うこともできます。

ステップ

1. メイン・ビュー・ページを入力します。
2. 左パネルのAuto-Switch → Multi-Window Auto-Switchをクリックします。
3. カーソルをオートスイッチAll Camerasに合わせクリック

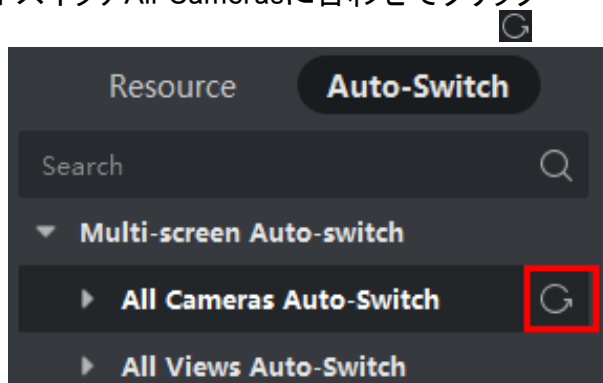


図 4-4 全カメラ起動オートスイッチ

カメラリスト内のすべてのカメラがセルフアダプティブモードで自動切替を開始します。

4. オプション:以下の操作を行います。

操作説明 オートスイッチを一時停止/再開します。||

一時停止/再開オートスイッチ

前ページ/次ページへ移動 前/次ページのカメラをクリックまたは表示します。◀▶

Dwell時間設定 現在のオートスイッチを停止した後、オートスイッチ滞留時間をクリックまたは増減するには、ページ下部にある20秒をクリックしてオートスイッチ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。たとえば、インターバルを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。◀▶

4.4.3 オートスイッチカスタムビュー

ビューは、各ウィンドウにリンクされたリソースチャネル(例えば、カメラ)を持つウィンドウ分割である。表示モードでは、ウィンドウの分割や、カメラとウィンドウの対応関係をお気に入りとして保存することができ、後でこれらのチャンネルにすばやくアクセスできるようになります。フロアにすべてのカメラを含むビューを保存すると、カスタムビューが保存され、フロア上のすべてのカメラのライブビューをワンクリック操作

で順番に表示できます。これにより、ログインのたびにカメラ一覧から検索する必要がなくなります。オートスイッチは、手動で設定できるインターバルで動作します。

開始前に

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」を参照してください。

ステップ

1. メイン・ビュー・ページを入力します。
2. 左パネルの[Resource]→[Multi-Window Auto-Switch]をクリックします。
3. カーソルをすべてのビューの自動切り替えに合わせてクリックします。

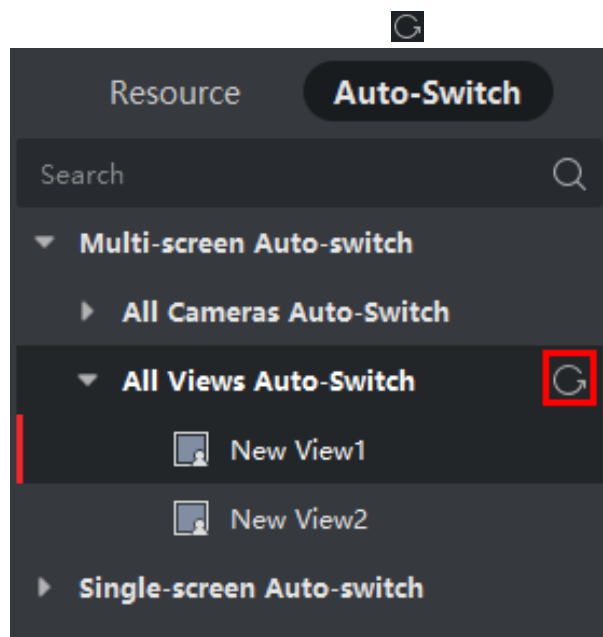


図4-5 カスタムビューを自動的に切り替える

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:以下の操作を行います。

操作説明 オートスイッチを一時停止/再開します。

一時停止/再開オートスイッチ

前ページ/次ページへ移動 クリックするか、前後のビューを表示します。⏪◀▶⏩

Dwell時間設定 現在のオートスイッチを停止した後、オートスイッチ滞留時間をクリックまたは増減するには、ページ下部にある20秒をクリックしてオートスイッチ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。たとえば、イ

インターバルを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。◀▶

4.5 PTZ制御

このソフトウェアは、パン/チルト/ズーム機能を備えたカメラにPTZ制御を提供します。PTZ制御中は、プリセット、パトロール、パターンを設定することができます。また、新しいPTZ制御ウィンドウを開くこともできます。



注意

一部の機能は、デバイスでサポートする必要があります。

4.5.1 PTZコントロールパネル

ソフトウェアは、検出、速度、ズームイン、ズームアウトなどの制御パネルを介して







注記











PTZ制御操作を行います。また、PTZを制御する新しいウィンドウを開くこともできます。










クラウドP2Pデバイスは、上下左右のPTZ移動のみをサポートします。

Main Viewモジュールを入力し、PTZ Controlを選択して、PTZコントロールパネルを開きます。PTZコントロールパネルには以下のアイコンがあります。

表4-3 PTZコントロールパネルのアイコン

アイコン	氏名	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たままにすると、PTZが回転します。 PTZを水平方向に連続的に回転させる場合はクリックし、回転を停止する場合は再度クリックします。 
	速度制御	スライダをドラッグしてPTZの移動速度を調整します。
	ズームイン/ズームアウト	ズームインして詳細を閉じた画像を表示し、ズームアウトしてパノラマ画像を表示します。







アイコン	氏名	説明
	フォーカス+/-	フォーカス + フォーカスポイントを前方に移動をクリックし、フォーカス - をクリックしてフォーカスポイントを後方に移動します。
	虹彩+/-	画像の輝度調整に使用します。虹彩が大きくなればなるほど、光が入り込み、画像が明るくなります。
	3D位置決め	マウスの左キーを使ってビデオイメージ内の希望する位置をクリックし、右下方向に四角形の領域をドラッグすると、ドームシステムはその位置を中心に移動させ、四角形の領域をズームインします。マウスの左キーを使って、左上方向に四角形の領域をドラッグして、位置を中心に移動し、四角形の領域をズームアウトします。
	補助焦点	クリックすると自動的にピントが合います。
	レンズ初期化	レンズを初期化し、再度ピントを合わせると鮮明な画像が得られます。
	光	<p>クリックして、ランプを塗りつぶします。</p> <hr/> <p> 注記 この機能はデバイスでサポートされている必要があります。</p> <hr/>
	ワイパー	ワイパーを使ってカメラレンズのゴミを取り除きます。
	手動追跡	オートトラッキング機能付きスピードドームの場合は、オートトラッキング(右クリックメニュー)を有効にし、アイコンをクリックしてビデオをクリックしてターゲットを手動でトラッキングします。
	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、スピードドームの取扱説明書を参照してください。

	ワンタッチパトロール	ワンタッチ式スピードドームの場合は、アイコンをクリックすると、あらかじめ定義されたプリセットNo.1からプリセットNo.32の順にパトロールが開始されます。 非アクティビティ(パークタイム)公園の設定については 時間については、スピードドームの取扱説明書を参照してください。
	ワンタッチパーク	ワンタッチパーク機能付きスピードドームの場合は、アイコンをクリックすると現在のビューがプリセットNo.32に保存されます。一定時間(パーク時間)が経過すると、プリセット番号32で自動的にパークが開始されます。パークタイムの設定については、スピードドームのユーザーマニュアルを参照してください。
	手動レンズ除氷ヒーターを有効にする	この機能を有効にすると、加熱によってカメラの性能が保証されます。 <hr/>  注記 環境温度が0°C以下の場合に有効にすることをお勧めします。そうしないと、高温がカメラのワークに影響を及ぼす可能性があります。 <hr/>
	手動PT除氷を有効にする	PTZカメラに付着した氷を拭き取り、カメラの性能を確保する機能です。
	手動顔写真撮影	このボタンをクリックし、マウスの左ボタンを押したまま、画像内で顔を選択して取り込みます。画像がサーバーにアップロードされて表示されます。
	FOVの同期化	サーマルカメラ用光チャネルの視野と熱チャネルの視野を同期させるにはクリックします。
	地域別曝露量	速度ドームの場合は、アイコンをクリックし、画像上に四角形を描画して、この領域の露出効果を最適化します。
	地域重視	速度ドームの場合は、アイコンをクリックし、画像上に四角形を描画して、この領域のフォーカス効果を最適化します。

4.5.2 プリセット、パトロール、パターンの設定

PTZコントロールは、プリセット、パトロール、パターンの設定、呼び出しに対応しています。

ホームページでメインビュー→ PTZ Controlをクリックして、PTZ Controlパネルを表示します。

タスク	定義	操作
プリセット	プリセットは、キー領域を移動可能なPTZの位置およびステータスにリンクします。モニタリング担当者は、それを基に、主要地域への迅速なポジショニングを行う。モバイルPTZでは、設定プリセットコマンドを送信することにより、ズーム、フォーカス、アイリスの位置とステータスを記録します。プリセット呼出コマンドを実行すると、モバイルPTZは急速に設定位置に回転し、設定状態に戻ります。	設定方法:プリセットリストからプリセットを選択→カメラを希望の位置に回す→クリック  コール方法: クリック 
パターン	パターンを記録することにより、特定の位置における移動経路および滞留時間を貴重に記録することができる。パターンを呼び出すことにより、携帯PTZは記録されたパスに合わせて全体的に移動を開始します。	設定方法:パターンの記録を開始するにはクリック→パターンを形成するには方向ボタンをクリック→クリックします。  コール方法: クリック 
パトロール	パトロールは、ユーザーが定義されたプリセットのグループを持つスキャントラックを指定する機能です。2つのプリセット間のパトロールは、設定された速度と時間で行われます。	設定方法: → プリセットを選択し、速度と時間を設定する→ OKをクリックします。  コール方法:クリックします。 



注記

あらかじめ2つ以上のプリセットを設定しておく必要があります。

4.6 カスタマイズ・ウィンドウ部門

クライアントソフトウェアは、複数の定義済みウィンドウ分割を提供します。また、必要に応じてウィンドウの分割をカスタマイズすることもできます。

ステップ



注記

ウィンドウ分割は最大5分割まで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・ウィンドウの追加」ダイアログを開きます。
4. [Dimension]フィールドに、ウィンドウ番号を水平および垂直の両方の次元で入力します。
キーボードのEnterキーを押します。



注記

リモート再生の場合、最大16画面まで同時に再生できますので、16画面以上の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、Jointをクリックしてウィンドウ全体を結合します。
6. オプション:ジョイントウィンドウを選択し、リストアをクリックしてジョイント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:表示画面に分割モードをクリックまたはドラッグして、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の追加]ディビジョンを開きます。
 - 3) カスタマイズした分割モードを選択し、名前変更、設定などの操作を行います。
寸法、接合/取り外し接合ウィンドウ

4.7 手動で記録・取得

ライブビュー中は、手動でビデオを録画したり、撮影した動画ファイルや撮影した画像をローカルパソコンで見ることができます。


4.7.1 手動でビデオを録画する

Manual recording functionでは、Main Viewページにライブビデオを手動で記録したり、ローカルPCにビデオファイルを保存したりできます。


ステップ

注記

Cloud P2Pデバイスでは、ライブビュー時の手動録画はサポートされません。

1. メインビューページを開きます。
2. ライブビューを起動します。
3. 次のいずれかの操作を行い、手動記録を開始します。
 - カーソルをライブビューの表示ウィンドウに移動してツールバーを表示し、ツールバーをクリックします。
 - 表示ウィンドウを右クリックし、右クリックメニューの「録音開始」をクリックします。

アイコンが変わります。インジケ   表示ウィンドウの右上隅に表示されます。

4. クリックすると、手動記録が停止します。

録画した動画ファイルは自動的にローカルPCに保存され、デスクトップ右下に保存パス情報のある小さなウィンドウが表示されます。

注記

録画した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、Set File Saving Pathを参照してください。

4.7.2 ローカルビデオの表示


ローカルパソコンに保存されている動画ファイルを見ることができます。

開始前に

ライブビデオを録画します。

ステップ

1. 右上隅の→ファイル→ビデオファイルを開くをクリックして、[ビデオファイル]ページ

を開きます。

2. 撮影した動画ファイルを「カメラグループ」の一覧から検索するときは、カメラを選択します。
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した動画ファイルは、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、以下の操作を行います。

ビデオファイルの削除 ビデオファイルを選択し、削除をクリックしてビデオファイルを削除します。

メールを送る ビデオファイルを選択し、「電子メール」をクリックして、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、電子メール設定を設定する必要があります
事前に。詳細は、「電子メールパラメータの設定」を参照してください。

ローカルビデオの保存 ビデオファイルを選択し、「名前を付けて保存」をクリックして、ビデオファイルの新規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。

4.7.3 撮影した画像

ライブビュー中に撮影できます。

ライブビュー中に撮影する必要がある場合に実行します。

ステップ

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. 次の操作のいずれかを行って撮影します。
 - カーソルをライブビューの表示ウィンドウに移動してツールバーを表示し、ツールバーをクリックします。
 - 表示ウィンドウを右クリックし、右クリックメニューのCaptureをクリックします。

撮影した画像は自動的にローカルPCに保存され、デスクトップ右下にピクチャプレビューと保存パスの情報が表示されます。



撮影した画像の保存パスは、[システム設定]ページで設定できます。詳細については、「ファイル保存パスの設定」を参照してください。

4.7.4 撮影した画像を見る

ライブビューで撮影した画像は、ソフトを実行しているパソコンに保存されます。必要に応じて撮影した画像を見ることができます。

開始前に

ライブビューで撮影します。

ステップ

1. 右上隅の→ファイル→取り込んだ画像を開くをクリックして、取り込んだ画像ページを開きます。☰
2. 撮影した画像を「カメラグループ」の一覧から検索するときは、カメラを選択します。
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。
ページのサムネイル表示で、開始時刻と終了時刻の間に撮影された画像。
5. オプション:検索後、以下の操作を行います。

拡大写真 ピクチャのサムネイルをダブルクリックすると、拡大して見やすくなります。

プリントピクチャ 撮影した画像を選択し、「印刷」をクリックして選択した画像を印刷します。

ピクチャの削除 撮影した画像を選択し、「削除」をクリックして、選択した画像を削除します。

メールを送る 撮影した画像を選択し、EメールをクリックしてEメール通知を送信します。
選択した画像が添付されている。

ピクチャ保存 撮影した画像を選択し、保存をクリックして、選択した画像の新しいコピーを保存します。



4.8 インスタント再生

インスタント再生では、動画の中で注目に値する部分、または一見不明な部分が表示されます。そのため、メインビューページでビデオファイルを即座に再生し、必要に応じてすぐに確認することができます。

開始前に

ビデオファイルを記録し、DVR、NVR、ネットワークカメラなどのSD/SDHCカードやHDDなどのストレージデバイス、またはストレージサーバに保存します。


ステップ

1. メインビューページを開き、ライブビューを開始します。
2. 次の操作のいずれかを行うと、プリプレイ再生時間の一覧が表示されます。
 - 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、クリックします。 
 - 表示ウィンドウを右クリックし、右クリックメニューからSwitch to Instant Playbackを選択します。
 - 「表示」パネルの「デフォルト表示」または「カスタム表示」ノードにカーソルを移動し、「クリック」します。プリプレイ時間が30秒、1分、3分、5分、8分、10分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、ライブビューの現在の時刻が09:30:00の場合、インスタント再生は09:27:00から開始します。

即時再生中は、ディスプレイ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:再度クリックして即時再生を停止し、ライブビューに戻ります。 

4.9 Fisheye Cameraのライブビュー

魚眼カメラでは、魚眼モードでライブビューを起動したり、プリセットやパトロールを設定したり、PTZ制御を行うことができます。

4.9.1 Fisheyeモードでライブビューを実行する



魚眼カメラのライブビュー中は、広角の歪んだビュー全体が表示されます。ただし、詳細を表示するのは難しい場合があります。この問題を解決するために、魚眼拡大モードでライブ映像を再生できます。Fisheye展開では、180° パノラマ、360° パノラマ、PTZ、半球などさまざまなモードで画像を展開できます。画像を鮮明に見ることができます。

開始前に

Microsoft DirectXコンポーネントがインストールされていることを確認します。

ステップ

1. メインビューページを開き、魚眼カメラのライブビューを開始します。

2. [Fisheye Expansion]モードにします。
 - ビデオを右クリックし、Fisheye Expansionを選択します。
 - ツールバーでクリックします。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」を参照してください。方向に向かう。
3. 表示ウィンドウの左下隅をクリックして、マウントの種類と展開モードの選択パネルを開きます。
4. 魚眼カメラの実装位置に合わせて取り付け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。

Fisheye

Fisheyeビューモードでは、カメラのワイドビュー全体が表示されます。このビューモードは、魚の凸状の眼の視覚に近似するため、フィッシュェイと呼ばれる。レンズは、広い面積の曲線画像を作成し、画像内の物体の透視と角度を歪めます。

パノラマ

Panorama View Modeでは、歪んだ魚眼画像が正常画像に変換されます。幾つかの較正方法による透視画像

PTZ

PTZビューは、FisheyeビューまたはPanoramaビュー内の一部の定義領域のクローズアップビューであり、e-PTZとも呼ばれる電子PTZ機能をサポートします。

注記

各PTZビューは、FisheyeビューとPanoramaビューに、特定のナビゲーションボックスでマークされます。FisheyeビューまたはPanoramaビューのナビゲーションボックスをドラッグして、PTZビューを調整したり、PTZビューをドラッグして、目的の角度にナビゲーションボックスを調整したりできます。

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、目的の角度に合わせることができます。

検査試薬半球

AR半球モードは、画像が遠く近くに重なり、広角で寸法画像を見ることができます。

シリンダ

円柱モードでは、画像は円柱ページに形成される。

6. オプション:魚眼モードでライブビューを開始した後、以下の操作を行います。

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

全画面表示にする 再生ウィンドウを右クリックし、選択したウィンドウをフルスクリーンモードに切り替えます。

4.9.2 Fisheye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パネルは機器によって異なります。


PTZコントロールパネルには以下の機能があります。

- PTZウィンドウを選択し、方向ボタンをクリックして表示角度を調整します。または、魚眼またはパノラマウィンドウのNo.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、クリックしてオートスキャンを開始し(カメラが水平方向に回転する)、再度クリックしてオートスキャンを停止します。
- スライダーをオンにドラッグして、PTZの移動速度を調整します。
- マウスホイールをクリックまたはスクロールして、選択したPTZウィンドウをズームインまたはズームアウトします。

4.9.3 プリセットとパトロールの設定

PTZは、プリセットの設定と呼び出し、パトロールをサポートします。

メインビューページを入力し、カメラを右クリックして[Fisheye Expansion]を選択します。

タスク	定義	操作
プリセット	プリセットは、キー領域を移動可能なPTZの位置およびステータスにリンクします。モニター	設定方法:プリセットリストからプリセットを選択→カメラを希望の位置に回す→クリック 

	<p>ング担当者は、それを基に、主要地域への迅速なポジショニングを行う。モバイルPTZでは、設定プリセットコマンドを送信することにより、ズーム、フォーカス、アイリスの位置とステータスを記録します。プリセット呼出コマンドを実行すると、モバイルPTZは急速に設定位置に回転し、設定状態に戻ります。</p>	<p>コール方法:クリックします。Ⓧ</p>
<p>パトロール</p>	<p>パトロールとは、ユーザーがスキャントラックを以下のように指定する機能です。</p>	<p>設定方法: → プリセットを選択し、速度と時間を設定する→ OKをクリックします。Ⓡ</p>
	<p>定義済みプリセットのグループ2つのプリセット間のパトロールは、設定された速度と時間で行われます。</p>	<p>コール方法:クリックします。Ⓧ</p>

4.10 マスタースレーブ連携の実行

マスタースレーブのトラッキング機能に対応したボックスカメラやビュレットカメラは、ユーザーの要求に応じてターゲットを探したり、トラッキングしたりすることができます。

注記

- この機能は、特定のボックスまたはビュレットカメラでのみサポートされています。
- 自動追尾機能付きスピードドームは、ボックスカメラまたはビュレットカメラの近くに設置する必要があります。



4.10.1 マスタースレーブ・トラッキング・ルールの設定

ライブビュー中にマスタースレーブトラッキングを実行する前に、VCA検出ルールの設定、スピードドームへのリンク、カメラとスピードドームのキャリブレーションなど、ボックスまたはビュレットカメラのマスタースレーブトラッキングルールを設定する必要があります。

侵入検知ルールの設定

BulletまたはBoxカメラのVCA検出ルールを設定し、VCAイベントがトリガされると、クライアントはターゲットを追跡するために速度ドームをトリガすることができます。ここでは、侵入検知を例にとります。

ステップ


1. [Device Management]ページを開き、ボックスまたは行頭カメラを選択します。
2. [Advanced Configuration]→[VCA Config]→[Rule]→[Rule Settings]をクリックしてルール設定を入力します。
3. 「ルール・リストの追加」パネルをクリックして、ルールを追加します。
4. イベントタイプとして「Intrusion」を選択します。
5. クリックして、ライブビデオ上に検出領域を描画します。
6. 保存をクリックします。

リンク速度ドーム

BoxまたはBulletカメラのマスタースレーブトラッキングを設定する場合、カメラをスピードドームにリンクさせ、スピードドームのPTZ位置を設定してトラッキングすることができます。

このタスクを実行して、マスタースレーブトラッキング用のスピードドームにボックスまたはブレットカメラをリンクします。

ステップ

1. [Device Management]ページを開き、ボックスまたは行頭カメラを選択します。
2. [Advanced Configuration] → [Master-Slave Tracking] をクリックして、master-Slave tracking に入ります。

設定ページ

3. 表示ウィンドウの[ログイン]ボタンをクリックすると、スピードドームのログインウィンドウが開きます。
4. 速度ドームのIPアドレス、ポート番号、ユーザ名、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、方向矢印を使用して速度ドームを水平位置に調整します。

次にすべきこと

Box または Bullet カメラとリンクされたスピードドームのキャリブレーションについては、Calibrate Camera and Speed Dome Automatically または Calibrate Camera and Speed Dome Manually を参照してください。


カメラとスピードドームを自動的にキャリブレーションする

BulletまたはBoxカメラのMaster-Slaveトラッキングルールを設定するときは、カメラとスピードドームをキャリブレーションする必要があります。自動校正と手動校正の2つの校正モードがあります。ここでは、自動校正を紹介します。

開始前に

カメラをスピードドームにリンクします。詳細は「リンクスピードドーム」を参照してください。

ステップ

1. [Device Management]ページを開き、ボックスまたは行頭カメラを選択します。
2. [Advanced Configuration] → [Master-Slave Tracking] をクリックして、master-Slave tracking に入ります。

設定ページ

3. Calibrationパネルの右下隅にあるAuto Calibratingとしてキャリブレーションモードを選択します。
4. スピードドームのビューを移動してズームイン/ズームアウトし、ドームとカメラのライブビューがほとんど同じになるようにします。
5. 保存をクリックします。



カメラとスピードドームのキャリブレーションを手動で行う

BulletまたはBoxカメラのMaster-Slaveトラッキングルールを設定するときは、カメラとスピードドームをキャリブレーションする必要があります。自動校正と手動校正の2つの校正モードがあります。ここでは、手動校正を紹介します。

開始前に

カメラをスピードドームに接続します。詳細は「リンク速度ドーム」を参照してください。

ステップ

1. [Device Management]ページを開き、ボックスまたは行頭カメラを選択します。
2. [Advanced Configuration] → [Master-Slave Tracking] をクリックして、master-Slave tracking に入ります。
設定ページ
3. Calibrationパネルの右下隅にあるManual CalibratingとしてCalibrationモードを選択します。
4. リストからサイトNo.1を選択し、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に表示されます。
5. 手順4を繰り返して、その他の手動校正サイトを追加します。
6. ライブビューページで、4つのキャリブレーションサイト間の距離を均等に調整します。

7. 校正場所1を選択します。
サイトNo.1のデジタルズーム画面が右に表示されます。
8. スピードドームの表示を移動またはズームインまたはズームアウトして、スピードドームのライブ表示と選択したサイトのデジタルズーム表示がほとんど同じであることを確認します。
9. クリックすると、現在のサイト位置情報が保存されます。[※](#)
10. 手順7、8、9を繰り返し、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。

4.10.2 マスタースレーブトラッキングを有効にする

ライブビュー中に、マスタースレーブトラッキングを有効にして、スピードドーム付きの弾丸カメラまたは箱型カメラのビューに表示されたターゲットを見つけたり、トラッキングしたりできます。

開始前に

ボックスカメラまたはビュレットカメラのマスタースレーブトラッキングルールを設定します。

ボックスカメラまたはビュレットカメラのマスタースレーブトラッキングを有効にする必要がある場合に、このタスクを実行します。

ステップ

1. Main Viewページを入力し、BoxまたはBullet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、マスタースレーブトラッキングの有効化をクリックします。
設定されたVCAルールがターゲットによってトリガされると、リンクされた速度ドームが以下を実行します。
自動的なマスター・スレーブ・トラッキングとターゲット・フレームが緑から赤に変わります。

4.11 サーマルカメラ用ライブビュー

サーマルカメラでは、ライブビュー中に火源情報や温度を見ることができます。また、温度を手動で測定して、ライブビュー画像の温度情報を取得することもできます。

4.11.1 ライブビュー中の火源情報の表示

ライブビュー中に、検出された火源情報を見ることができます。

開始前に

熱機器のアラームルールを設定します。詳しくは機器の取扱説明書を参照してください。

ステップ

1. メインビューページを入力し、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については、「ライブビューの開始」を参照してください。

2. ライブビュー画像上で右クリックし、右クリックメニューの[File Source Information]を選択して、情報の種類のリストを表示します。

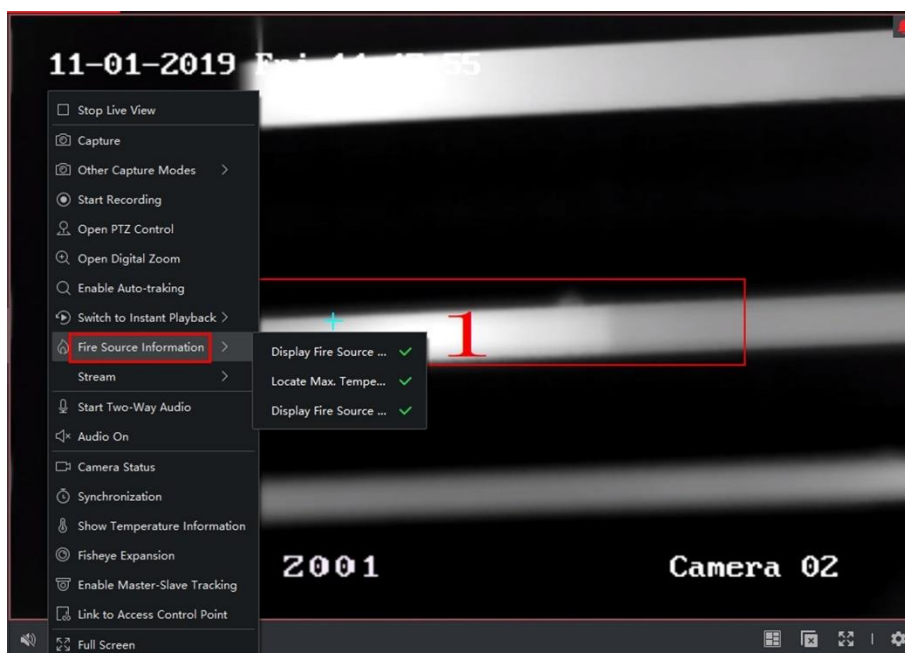


図4-6 火源情報の表示

3. リスト内で情報の種類を選択し、情報を表示します。

消火源領域の表示

設定されたアラームしきい値よりも温度が高い領域。

最大値の位置温度域

火源地域で最も気温が高い地域をマークする。それは緑色でマークされてい

る。
火源ターゲットの表示
装置と火源との距離。

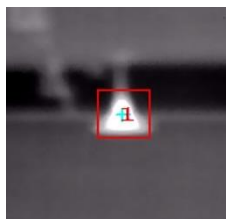


図4-7 ライブビュー画像の火源情報

4.11.2 ライブビュー画像上の温度情報の表示

ライブビデオを表示するときに、モニタリングシーンのリアルタイム温度情報を表示または非表示にできます。

開始前に

- デバイスのVCAソースタイプを「温度測定+挙動解析」に切り替えます。
- 装置温度測定機能を有効にし、温度測定ルールを設定します。詳しくは、装置の取扱説明書を参照してください。

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に実行します。

ステップ

1. メインビューページを入力し、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については、「ライブビューの開始」を参照してください。

2. 温度測定ルールで設定した領域に合わせてシーンを調整します。
3. ライブビュー画像上で右クリックし、右クリックメニューからShow Temperature Informationを選択する。
ライブビュー画像に温度が表示されます。

4. 画像をクリックすると、詳細な温度情報が表示されます。

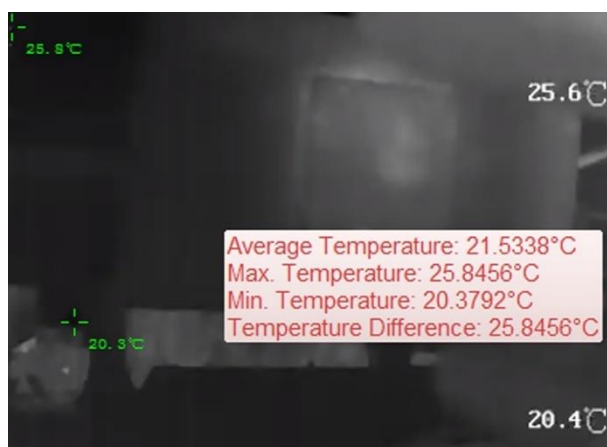


図4-8 ライブビュー画像の温度情報

5. オプション:ライブビュー画像上で右クリックし、温度情報を非表示にするを選択します。

4.11.3 温度を手動で測定

サーマルカメラのライブビュー中は、ライブビュー画像上の任意の場所をクリックして、異なる点の温度を表示し、火源を素早く見つけることができます。

ステップ

注記

- 測定した温度が5秒間画像に表示されます。
- 表示できる温度は1点のみです。
- 複数のクライアントが1台のカメラのライブビデオを取得する場合、1台の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、測定点はクリアされます。

1. メインビューページを入力し、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については、「ライブビューの開始」を参照してください。

2. ライブビュー画像上で右クリックし、Show Temperature Informationを選択します。
3. この位置の温度を表示するには、ライブビュー画像をクリックします。

クリックした点の温度が画像上に表示されます。

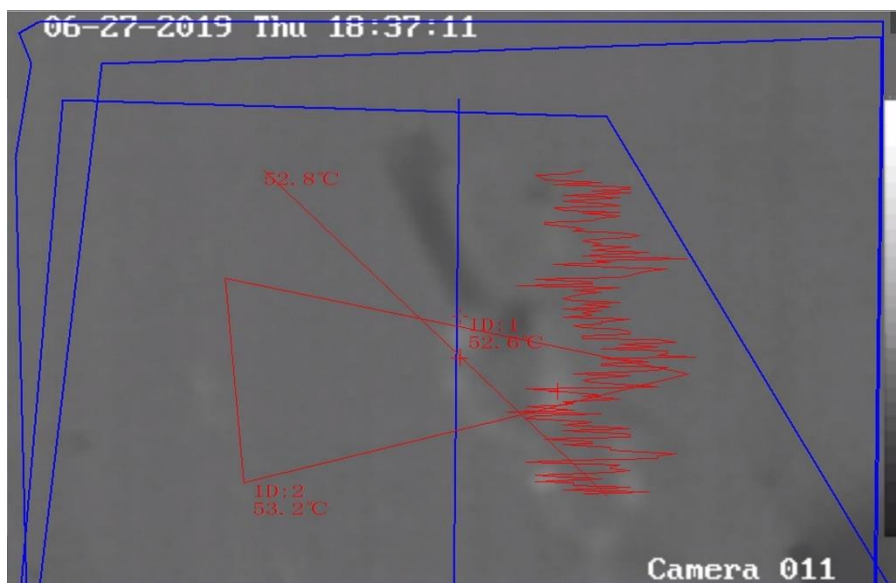


図4-9 点の温度を手動で測定する

4. オプション:ライブビュー画像上で右クリックし、メニューのHide Temperature Informationを選択する。

4.12 低帯域幅のライブビュー

低いネットワーク帯域幅の状況では、ビデオストリーミングの速度は、帯域幅制限のために、はるかに遅くなる可能性がある。低帯域幅のユーザに対してより少ないストリーミング速度で通常の品質を提供するために、クライアントは低帯域幅モードでライブビューを提供する。その前に、ストリーミングプロトコルを設定し、他の操作を最初に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小さい場合のライブビューおよび再生のパフォーマンスを向上させる方法を参照してください。

4.13 より多くの機能

ライブビューでサポートされている機能には、補助スクリーンプレビュー、デジタルズーム、チャンネルゼロ、双方向オーディオ、カメラステータス、同期などがあります。

補助画面のプレビュー

ライブビデオをさまざまな補助画面に表示して、複数のプレビューを簡単に表示しま

す。
シーンのモニタリング

 注記

3つまでの補助スクリーンがサポートされます。

デジタルズーム

マウスをドラッグして、左右下に四角形の領域を描画し、描画領域をズームインまたはズームアウトします。または、マウスホイールを使ってデジタルズームでビューをズームインまたはズームアウトします。

チャンネルゼロ

デバイスのチャンネルゼロの場合は、Ctrlキーを押したままダブルクリックすると特定のチャンネルが表示されます。

channel.Ctrlキーを押したまま再度ダブルクリックして復元します。

ツーウェイ・オーディオ

双方向のオーディオ機能でカメラの音声通話を可能にします。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取得できます。デバイスに複数の2方向オーディオチャンネルがある場合は、2方向オーディオを開始するチャンネルを選択できます。

 注記

- 両方向オーディオは、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、双方向オーディオ中のチャンネル選択には対応していません。
-

カメラの状態

記録状態、信号状態、接続番号などカメラの状態を検出して表示し、確認することができます。ステータス情報は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と装置のクロックを同期させる方法を提供する。

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、表示ウィンドウサイズに応じてストリームの種類を選択します。ウィンドウ分割番号が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、さもなければサブストリームとなる。

ストリームの種類を設定するには、次の3つの方法があります:

- リソース・リストで、カーソルをカメラの名前に置き、ストリーム・タイプを選択するには、ストリーム・タイプをクリックするか、またはストリーム・タイプの自動変更をクリックします。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をクリックし、ストリームの種類を選択します。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参照してください。
- ライブビューウィンドウを右クリックし、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

この機能はデバイスでサポートする必要があります。

全画面モードでクライアントをロックする

キーボードのCtrlキーとLキーを押して、フルスクリーンモードに入った後に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、現在のウィンドウ分割モードでは、他のウィンドウも含めてクライアントを操作できなくなります。上部の[Unlock]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、[Unlock]をクリックしてクライアントのロックを解除します。

第5章 リモート再生

記録スケジュールに従い、ビデオを記録します。ストレージ・サーバーおよびローカル・デバイスに保管されているビデオ・ファイルを表示して、事後分析のためのイベント発生プロセスをリストアップし、さらに判断を下すことができます。価値のあるビデオ映像を保存することは、ビデオ分析およびビデオプルーフのための基本的な資料を提供することができる。クライアントは、VCA再生、イベント再生など、複数の再生モードをサポート

注記

ートします。

再生モードには、Main View モジュールのインスタント再生(詳細については、**インスタント再生**を参照)と、リモート再生モジュールのビデオファイルを検索して再生する再生モードがあります。本章では、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。

5.1 フローチャート

以下のフローチャートに従い、再生してください。

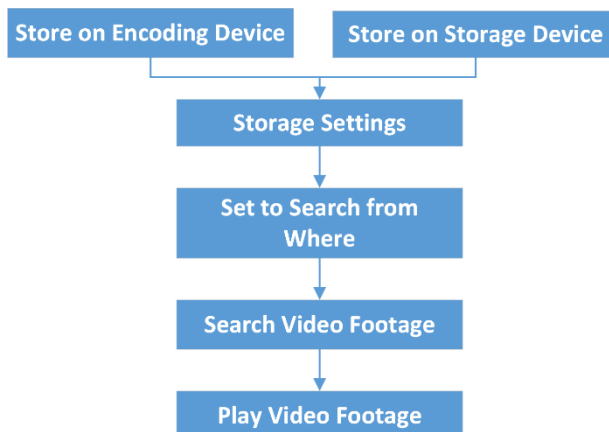


図 5-1 再生のフローチャート

- **保存設定:** 記録スケジュールを設定して、カメラが記録を開始する時期とビデオ素材が保管されている場所を指定します。詳細については、**リモート・ストレージ構成**を参照してください。
- **Search from Where:** Storage Serverまたはエンコーディング装置に保存されているビデオを優先的に再生するように設定します。詳細については、「**ライブビューと再**

生パラメータの設定」を参照してください。

- **ビデオ素材を検索して再生する**:再生を開始します。詳しくは、この章の内容を参照してください。

5.2 リモート・ストレージ構成

ビデオファイルや撮影した画像は、ローカルデバイスのHDD、ネットHDD、SD/SDHCカード、または接続されているストレージサーバに保存できます。



この機能は、装置がサポートする必要があります。

5.2.1 DVR、NVR、ネットワークカメラに画像とビデオを保存する

DVR、NVR、ネットワークカメラなどのローカルデバイスには、HDD、ネットHDD、SD/SDHCカードなどのストレージデバイスをビデオファイルやピクチャファイルに提供するものがあります。ローカル機器のチャンネルの録画スケジュールやキャプチャスケジュールを設定します。

開始前に

新しくインストールした記憶装置がフォーマットされていることを確認します。詳しくは、**フォーマットストレージサーバーのHDD**を参照してください。

この作業は、DVR、NVR、ネットワークカメラなどのエンコーディング装置に画像ファイルとビデオファイルを保存する必要がある場合に実行します。

ステップ



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コンフィギュレーションページで検索できます。

1. ストレージ・スケジュール・モジュールを入力します。
2. 「カメラグループ」の一覧からカメラを選択します。
3. デバイスのローカル録画またはキャプチャを有効にするには、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エンコーディングデバイスエリアのストレージにオンに設定します。

4. ドロップダウン・リストから、記録または取り込みスケジュール・テンプレートを選択します。

終日テンプレート

終日連続撮影。

平日テンプレート

午前 8 時から午後 8 時までの勤務時間連続記録。

イベントテンプレート

全日イベントが記録をトリガしました。

テンプレート 01~08

特定のスケジュール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、*Configure Recording Schedule Template* または *Configure Capture Schedule Template* を参照してください。

5. 「録画スケジュールの詳細設定」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

機器によって表示項目が異なります。

事前記録

イベントが発生する前に記録したいときに、通常、イベントトリガー・レコードに使用されます。

記録後

イベント終了後、一定時間ビデオを録画することもできます。

ビデオファイルの保存

ビデオファイルを記憶装置に保存する時間を超えると、ファイルは削除されます。値を 0 に設定すると、ファイルは永久に保存されます。

冗長記録

ビデオファイルは、R/W HDD だけでなく、冗長 HDD にも保存してください。

録音オーディオ

ビデオファイルをオーディオで記録するかどうかを設定します。

ビデオストリーム

記録するストリームの種類を選択します。



注記

特定の種類のデバイスでは、カメラのメインストリームとサブストリームの両方を記録するために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の種類を切り替えることができます。再生中のストリームスイッチについては、**通常再生**を参照してください。

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。

分解能

連続撮影した画像またはイベント撮影した画像の解像度を選択します。

画質

連続撮影した画像やイベント撮影した画像の画質を設定します。

間隔

2つの取り込みアクション間の期間を参照する間隔を選択します。

撮影した画像番号

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、記録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。

5.2.2 ビデオを記憶装置に保存する

追加されたエンコーディングデバイスによって記録されたビデオ映像を、クライアントで管理されるストレージデバイスに保存することができます。

追加したエンコーディングデバイスのビデオファイルを保存するために、クライアントにストレージデバイスを追加したり、リモート再生のためにファイルを検索したりすることができます。ストレージ・デバイスは、iVMS-4200ストレージ・サーバー、CVR (センタ

ー・ビデオ・レコーダー)、またはその他のNVRであることができます。
ここでは、iVMS-4200 Storage Serverの設定を例にとります。

ストレージ・サーバーの活動化

iVMS-4200 Storage Server を最初に行う場合は、ストレージ・サーバーをアクティブにする必要があります。ストレージ・サーバーを活動化する場合に、このタスクを実行します。

ステップ

1. デスクトップの  をクリックして、iVMS-4200 Storage Server を実行します。



注記

- ストレージ・サーバー・ポート(値: 8000)が他のサービスによって占有されている場合は、ダイアログがポップアップします。ポート番号を他の値に変更して、ストレージ・サーバーが正しく動作するようにする必要があります。
- 別のPCにインストールされているiVMS-4200 Storage Serverにビデオファイルを記録することもできます。

2. 新しい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強度を自動的にチェックすることができます。あなたの製品の安全性を高めるために、あなたが選択したパスワードを変更することを強くお勧めします(大文字、小文字、数字、特殊文字の3種類以上を含む最低8文字を使用してください)。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、パスワードを毎月または毎週変更することで、製品をより良く保護することができます。

すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストーラーおよび/またはエンドユーザーの責任です。

3. OK をクリックしてパスワードを変更します。

パスワードを変更すると、ストレージ・サーバーが自動的に実行されます。

クライアントへのストレージ・サーバーの追加

追加されたエンコーディング装置のビデオ・ファイルを保管するために、ストレージ・サーバーをクライアントに追加できます。

ステップ

1. デバイス管理モジュールを入力します。
2. デバイスタブをクリックします。
3. 追加したデバイスがリストに表示されます。
 - iVMS-4200 Storage Serverを追加します。詳細については、「**シングルまたは複数のオンラインデバイスの追加**」を参照してください。
 - IPアドレスまたはドメイン名を使用して、ストレージ・サーバーを追加できます。詳細は「**IPアドレスまたはドメイン名によるデバイスの追加**」を参照してください。

フォーマットストレージサーバーの HDD


ビデオファイルストレージ用のストレージサーバの HDD をフォーマットしてください。ストレージサーバの HDD をフォーマットするには、このタスクを実行します。

ステップ



注記

HDD をフォーマットするには、ディスク容量と元のデータをあらかじめ割り当てておく必要があります。フォーマットした HDD は削除されません。

1. デバイス管理モジュールを入力します。
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に表示されます。
3. リストから追加されたストレージサーバーを選択します。
4.  をクリックします。
5. 「ストレージ」→「一般」をクリックして、HDD フォーマットウィンドウに入ります。
6. リストから HDD を選択し、フォーマットをクリックします。
プロセスバーからフォーマット処理を確認し、フォーマットされた HDD のステータスを「未フォーマット」から「標準状態」に変更します。

ストレージ設定の設定

ストレージサーバが使用可能な場合は、カメラの撮影スケジュールを設定できます。

開始前に

新しくインストールした記憶装置はフォーマットする必要があります。

ステップ

1. ストレージ・スケジュール・モジュールを入力します。
2. 「カメラグループ」の一覧から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「ON」にして、動画ファイルを保存します。
5. ドロップダウン・リストから、記録するスケジュール・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、Configure Recording Schedule Template を参照してください。

6. オプション:録画スケジュールの場合は、[詳細設定]をクリックして録画前の時間、録画後の時間、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 Storage Server は、メインストリームのみをサポートします。

7. 「保存」をクリックして設定を保存します。

5.2.3 店舗の写真とローカルPCの追加情報

写真やヒートマップ、人物カウント、道路交通データ、などの追加情報をローカルPCに保存できます。

ローカルPCへ写真や追加情報を保存する必要がある場合に実行します。

ステップ

1. ストレージ・スケジュール・モジュールを入力します。
2. 「カメラグループ」の一覧からカメラを選択します。



注記

この機能は、装置がサポートする必要があります。

3. 保存内容を選択します。

画像保存

イベントが発生したときは、カメラのアラーム画像を保存します。システム設定→ファイルをクリックして、画像の保存パスを変更する。

追加情報保存


追加情報(ヒートマップ、カウントデータなど)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。


5.2.4 記録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したりできます。


ステップ

1. ストレージ・スケジュール・モジュールを入力します。
2. テンプレート設定画面を開きます。
ドロップダウンリストから **Template 01 to Template 08** を選択し、「**編集**」をクリックします。
3. 時間枠をドラッグして、カーソルが変わったときに選択したテンプレートの期間を設定します。 


連続

通常および連続撮影。スケジュール・タイム・バーには  マークが付いています。

イベント記録

記録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・バーには  マークが付いています。

コマンド

記録はコマンドによってトリガされます。スケジュール・タイム・バーには  マークが付いています。

注記


コマンドトリガーされた記録は、ATM DVR がクライアントに追加されたときにのみ ATM トランザクションで使用できます。





注記

録画スケジュールでは、1日につき8回まで設定できます。

4. オプション: 期間を設定した後、次のいずれかを実行できます:

移動

カーソルが  に変わったら時間の長さをドラッグし

	て調整します。
LengthenまたはShorten	期間を選択し、カーソルが  に変わったときに期間を延長または短縮します。
正確な時刻を設定する	期間をクリックして、その期間の正確な開始時間と終了時間を設定します。
削除	設定したスケジュール期間を選択し、  をクリックして削除します。
全削除	クリックすると、設定されたすべての期間が削除されます。 
コピー先	1つの日付を選択し、  をクリックして、日付の期間設定を他の日付にコピーします。

- オプション:テンプレート 01~08 の場合は、テンプレート名を任意に編集できます。
- 設定を保存するには、OK をクリックします。




注
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は、スケジュールテンプレートとして保存をクリックし、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。


5.2.5 取り込み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できます。


ステップ

- ストレージ・スケジュール・モジュールを入力します。
- テンプレート設定画面を開きます。
ドロップダウンリストから **Template 01 to Template 08** を選択し、「編集」をクリックします。ドロップダウンリストから **Custom** を選択します。
- 時間枠をドラッグして、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。

連続撮影

正常かつ連続的な捕獲。スケジュール・タイム・バーには  マークが付いています。

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されます。スケジュール・タイム・バーには  マークが付いています。

タグ制御	ビデオファイルのデフォルト(デフォルトのタグ名はTAG)またはカスタマイズタグ(タグ名はカスタマイズ)を追加して、重要なビデオポイントにマークを付けます。タグを編集したり、タグの位置に移動したりすることもできます。
その他の撮影モード	<ul style="list-style-type: none"> • 撮影した画像を印刷する:画像を取り込んで印刷します。 • 電子メールの送信:現在の画像をキャプチャし、1つまたは複数の受信者に電子メール通知を送信します。撮影した画像を添付できます。 • カスタム取り込み:現在の画像を取り込みます。名前を編集して保存することができます。



注記

- クラウドP2Pデバイスは通常再生のみに対応しており、機能もサポートしていません。リバース再生、スローフォワードまたはファストフォワード、タグの追加などがあります。
- デバイスの他のユーザー名(adminを除く)によってクライアントに追加されたNVRの場合、このNVRで「Double Verification」が有効になっている場合、クライアントでビデオを再生するときに、二重検証のために作成されたユーザー名とパスワードを入力する必要があります。二重検証の詳細については、NVRのユーザーマニュアルを参照してください。

5.3.1 映像検索

ビデオ素材を日付で検索したり、キーワードを入力して一致した結果を通常の再生にフィルタリングすることもできます。

ステップ

1. リモート再生モジュールを入力します。
2. 左側の  をクリックして「カメラ再生」ページを入力します。
3. オプション:  をクリックすると、検索期間の開始日と終了日が設定されます。

注記

カレンダーには、スケジュールで録画したビデオ素材の日付と  マークが、イベントに基づいて録画したビデオ素材の日付が  マークと表示されます。

4. カメラの再生を開始し、選択したカメラのビデオ素材を検索します。再生を開始するには、次のいずれかの操作を行います。

注

同時に検索できるカメラは最大 16 台です。

- 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、カメラまたはグループをダブルクリックすると、選択したウィンドウで再生が開始されます。
- カメラをダブルクリックすると、表示画面が自動的に選択され、再生が開始されます。

5.3.2ビデオ映像の再生

通常の再生でビデオ素材を検索した後、タイムラインでビデオを再生できます。

ステップ

1. リモート再生モジュールを入力します。
2. ビデオ素材を検索します。
3. タイムラインでビデオを再生します。

ビデオ映像が自動的に再生されます。タイムラインをクリックすると、指定した時間のビデオセグメントを通常の再生時に配置できます。

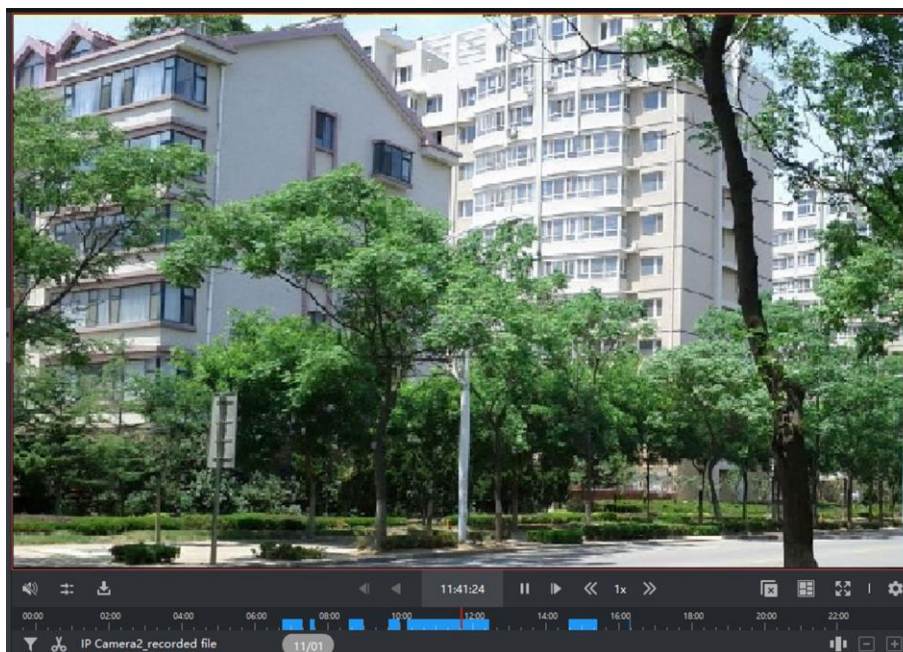




図 5-3 ビデオ映像の再生


注記


- タイムラインは、ビデオ素材の継続時間とビデオ素材の継続時間を示します。異なる


る種類が色分けされています。

- マウスホイール  または  をクリックして、タイムラインバーのスケールアップまたはスケールダウンを行うことができます。

4.オプション:ツールバーで以下の操作を行い、再生を制御します。


単一フレーム(反転)  をクリックまたはマウスホイールをスクロールして、ビデオ映像フレームをフレーム単位で再生します(反転)。

オーディオ・コントロール  または  をクリックしてサウンドのオフ/オンを切り替えます。また、電源を入れるときに音量を調節することもできます。

複数のカメラのダウンロード 複数のカメラのビデオ映像を同時にダウンロードするには  をクリックします。




詳細については、[複数のカメラのダウンロード](#)を参照してください。

ビデオファイルの  をクリックすると、カメラのビデオ素材が日時ごとにダウンロードされ、

日付順のダウンロード ローカルPCに保存されます。ダウンロードの進行状況がページの右上隅に表示され、手動でダウンロードを一時停止することができます。

正確な位置決め **2018/10/19 08:56:11** をクリックすると、ビデオファイルを再生する正確な時点が設定されます。

サムネイルの画像に 右下隅の  をクリックしてサムネイル機能を有効にし、カーソルをタイム

ジャンプする

ラインに合わせてポイントのサムネイルを表示します。サムネイルをクリックすると、画像にジャンプします。

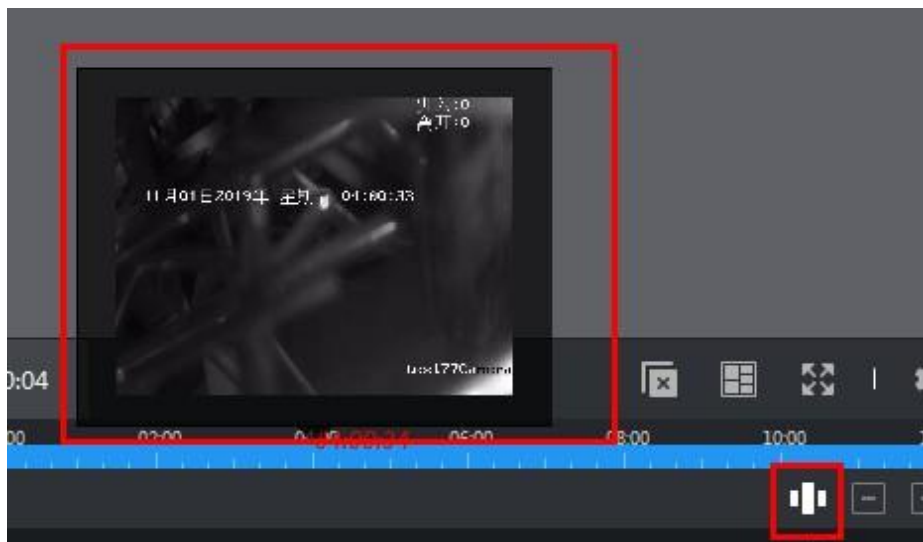


図 5-3 再生サムネイル



注記

この機能はデバイスでサポートされている必要があります。

5.4 アラーム入力再生

アラーム入力トリガーされ、リンクされたビデオでアラーム入力の再生を検索することができます。この機能は、接続されているデバイスのサポートが必要です。

アラーム入力の再生ツールバーと表示ウィンドウの右クリックメニューの説明について



注記



は、「通常再生」を参照してください。

一部のアイコンはアラーム入力再生できない場合があります。

5.4.1 映像検索

ビデオ素材を日付で検索したり、キーワードを入力して一致した結果をアラーム入力再生用にフィルタリングすることもできます。

ステップ

1. リモート再生モジュールを入力します。
2.  をクリックして、Event Playback ページを入力します。
3. アラーム入力チャンネルを選択します。
4. オプション:  をクリックすると、検索期間の開始日と終了日が設定されます。
5. イベントタイプは、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映像が右ページに時系列で表示されます。デフォルトでは、最初のビデオ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。

5.4.2 ビデオ映像の再生

アラーム入力再生のビデオ素材を検索した後、ファイル一覧やタイムラインで再生できます。

ステップ



1. リモート再生モジュールを入力します。
2.  をクリックして、Event Playback ページを入力します。
3. アラーム入力の映像を検索します。



アラーム入力のビデオ映像の検索の詳細については、「ビデオ映像の検索」を参照してください。

4. ファイルリストまたはタイムラインでビデオを再生します。
 - 再生表示ウィンドウでビデオを再生するには、ビデオ素材をダブルクリックします。
 - タイムラインをクリックして、アラーム入力再生時に指定した時間のビデオセグメントを位置決めします。



- タイムラインには、ビデオ素材の継続時間とビデオ素材の継続時間が表示されます。異なる種類が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スケールアップまたはスケールダウンできます。
-

5.5 イベント再生

動き検出、VCA検出、またはビヘイビア分析のようなイベントによってトリガーされる記録ビデオファイルは、イベント再生のために検索することができます。この機能は、接続されているデバイスのサポートが必要です。

イベント再生ツールバーと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、**通常の再生**を参照してください。





注記

アイコンによっては、イベント再生できない場合があります。

5.5.1 映像検索

ビデオファイルは、日付と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と一致した結果を検索することもできます。

ステップ

1. リモート再生モジュールを入力します。
 2. 左側にある  をクリックして、Event Playback ページを入力します。
 3. 左側のカメラを選択します。
 4. オプション:  をクリックすると、検索期間の開始日と終了日が設定されます。
-



注記


カレンダーには、スケジュールで録画したビデオ素材の日付が  マークが、イベントに基づいて録画したビデオ素材の日付が  マークと一緒に表示されます。

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。
マッチしたビデオ素材が右ページに時系列で表示されます。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。

5.5.2 ビデオ映像の再生

イベント再生のビデオ素材を検索した後、ファイル一覧やタイムラインからビデオを再生できます。

ステップ

1. リモート再生モジュールを入力します。
2. 左側にある  をクリックして、Event Playback ページを入力します。
3. イベントに基づいて録画したビデオ素材を検索します。
4. ビデオ素材を再生します。
 - 再生表示ウィンドウでビデオを再生するには、ビデオ素材をダブルクリックします。

- タイムラインをクリックし、指定した時間のイベント再生用のビデオセグメントを位置

**注**

決めます。

- タイムラインには、ビデオファイルと異なるビデオファイルの継続時間が表示され、タイプはカラーコード化されています。
- 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スケールアップまたはスケールダウンできます

5.6 ATM再生

ATM DVRの動画ファイルからATM再生を検索できます。この機能は、トランザクション・ルールで設定された接続されたデバイスのサポートが必要です。

ATM再生ツールバーと表示画面の右クリックメニューの説明については、**通常の再生**を参照してください。



**注記**

一部のアイコンはATM再生できない場合があります。

5.6.1映像検索

ATM DVRのビデオ映像は、カード番号別、トランザクションタイプ別、トランザクション金額別、ファイルタイプ別、または日付別に検索できます。また、キーワードを入力して、一致した結果をATM再生にフィルタリングすることもできます。

ステップ

1. リモート再生モジュールを入力します。
2. 左側の  をクリックして、ATM再生ページを入力します。
3. 左側の ATM DVR のカメラを選択します。
4. オプション:  をクリックすると、検索期間の開始日と終了日が設定されます。
5. 検索条件を設定します。

カード番号別

ATM 情報に含まれるカード番号を入力します。

トランザクションタイプによる検索

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金額を入力します。

ファイルの種類

検索する動画ファイルの種類を選択します。

6.「検索」をクリックして検索を開始します。

選択したATM DVRの映像がリモート再生ページの右側に時系列で表示されます。デフォルトでは、最初のビデオ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。

5.6.2ビデオ映像の再生

ATM DVRに接続されているカメラの映像を検索した後、ファイル一覧やタイムラインで再生できます。

ステップ

1.リモート再生モジュールを入力します。

2.  の左側をクリックして、ATM 再生ページを入力します。



3.ATM DVR に接続されているカメラのビデオ映像を検索します。

4.ビデオ素材を再生します。

- 再生表示ウィンドウでビデオを再生するには、ビデオ素材をダブルクリックします。
- タイムラインをクリックして、指定した時間のATM再生用のビデオセグメントを位置

注記

決めます。

- タイムラインには、ビデオファイルと異なるビデオファイルの継続時間が表示されます。タイプはカラーコード化されています。
 - マウスホイールを使用するか、 または  をクリックして、タイムラインバーをスケールアップまたはスケールダウンできます。
-

5.7 POS再生

POS情報を含む動画ファイルを検索して、POS再生を行うことができます。本機能にはPOSテキストオーバーレイが設定されている接続されたデバイスのサポートが必要です。

表示ウィンドウのPOS再生ツールバーと右クリックメニューの説明については、通常の再生を参照してください。



注記

一部のアイコンは POS 再生できない場合があります。

5.7.1 映像検索

POS情報を含むビデオ素材をキーワードまたは日付で検索できます。

ステップ

1. リモート再生モジュールを入力します。
2.  の左側をクリックして、POS 再生ページを入力します。
3. 左側のカメラを選択します。
4. オプション:  をクリックすると、検索期間の開始日と終了日が設定されます。
5. 検索条件を設定します。

キーワード

ATM 情報に含まれるカード番号を入力します。



注記

一度に入力できるキーワードは 3 つまでです。2 つのキーワードはカンマで区切る必要があります。

コンビネーションモード

複数のキーワードについて、“or (|)” を選択してキーワードを含む POS 情報を検索するか、“and(&)” を選択してすべてのキーワードを含む POS 情報を検索することができます。

大文字小文字の区別

大文字と小文字を区別するキーワードで POS 情報を検索するには、**大文字と小文字を区別する**チェックボックスをオンにします。

6. 「**検索**」をクリックして検索を開始します。
ビデオ映像にPOS情報が含まれている場合は、POS再生ページの右側に時系列で表示されます。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。

5.7.2 ビデオ映像の再生


POS情報を含むビデオ素材を検索した後、ファイルリストやタイムラインで再生できます。

開始前に

POS 情報オーバーレイを設定したカメラの通常再生を開始します。



ステップ

1. リモート再生モジュールを入力します。

2.  の左側をクリックして、POS 再生ページを入力します。
3. POS 情報を含むビデオ素材を検索します。
4. ファイルリストまたはタイムラインでビデオを再生します。
 - 再生表示ウィンドウでビデオを再生するには、ビデオ素材をダブルクリックします。
 - タイムラインをクリックして、指定した時間のPOS再生用のビデオセグメントを位置

 注記

決めします。

- タイムラインには、ビデオファイルと異なるビデオファイルの継続時間が表示されます。タイプはカラーコード化されています。
- マウスホイールを使用するか、 または  をクリックして、タイムラインバーをスケールアップまたはスケールダウンできます。

5.8 VCA再生

検索されたビデオファイルでは、VCAルールを設定して、モーション検出、ラインクロス検出、および侵入検出など、VCAイベントが発生するビデオ映像を検出できます。この機能は、より関心のあるビデオを検索し、赤色でマーク付けするのに役立ちます。



開始前に

VCA 機能付デバイスがインストールされていることを確認してください。

ステップ

 注記

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

1. リモート再生モジュールを入力します。
2.  の左側をクリックして「カメラ再生」ページを入力します。
3. カメラを選択し、カメラのビデオ再生を開始します。
4. 「VCA Search」メニューを入力します。
 - 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ポップアップし、「VCA Search」をクリックします。
 - 再生画面の  の右下隅をクリックします。
5. VCA タイプを有効にし、検出領域を描画して感度を設定します。

動作検出

ビデオの表示が変わると(人が過ぎたときやレンズが動いたときなど)、ビデオ素材はタイムライン上で赤色としてマークされ、自動アラームシーンまたはノーガードシーンに使用されます。

線路横断検知

ビデオ上に仮想線を描くことができ、クライアントが仮想線を横切る人、車両、その他の動いているオブジェクトを双方向に検出すると、ビデオ映像はタイムライン上で赤色としてマークされます。

侵入検知

ビデオに仮想領域を描くことができます。また、あらかじめ定義された領域に人、車両、その他の動いているオブジェクトが侵入したときには、ビデオ素材はタイムライン上で赤色でマークされます。


VCA 設定

性別、年齢、メガネ着用有無などの対象キャラクタを設定して、検索した動画ファイルの感度を設定し、フィルタリングします。ビデオ映像は、(属性が設定属性と一致する)人物がビデオに現れると、タイムライン上で赤色としてマークされます。



注記

感度が高いほど、マッチングした人の精度は高くなります。

6.オプション:  をクリックすると、検索期間の開始日と終了日が設定されます。

7.VCA 再生を開始します。

定義されたエリアで発生したVCAイベントは、タイムライン上で赤色のマークが付



注記

けられます。

- デフォルトでは、該当するビデオの再生速度は1倍、未使用のビデオの再生速度は8倍になります。
- 「システム設定」では、VCA 再生時に未使用のビデオをスキップし、VCA 再生時に未使用のビデオを再生しない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**を参照してください。
- 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、「VCA検索」をクリックしてVCA再生を無効にします。

5.9 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。異なるビデオファイルの再生時間が異なる場合があります。同期再生では、ビデオファイルを同期して再生できます。

ステップ



注記

- 最大16台のカメラの動画を同時に再生できます。
- ATMビデオ再生およびVCA再生モードでは、同期再生および非同期再生はサポートされません。
- イベントビデオ再生およびPOSビデオ再生のみが同期再生に対応しています。複数のカメラをリンクする場合は、「Maintenance and Management」→「Event Management」と入力し、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入力します。
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.  をクリックすると同期再生が無効になります。

5.10 Fisheye Cameraのビデオ再生

魚眼カメラのビデオを再生すると、ビューに歪みが発生する場合があります。詳細を見やすくするために、魚眼拡大機能を有効にして、歪んでいないビューとしてビューを修正することができます。クライアントは、パノラマ、半球、PTZ、フィッシュアイ+PTZモードなどの複数のフィッシュアイ拡張モードをサポートします。

開始前に

Microsoft DirectX コンポーネントがインストールされていることを確認します。

ステップ



注記

その他の再生制御については、通常再生を参照してください。アイコンによっては、フィッシュアイ再生できない場合があります。

1. リモート再生モジュールを入力します。


2.魚眼カメラを選択して再生を開始します。



注記

再生および再生制御の詳細な設定については、「通常再生」を参照してください。



3.[Fisheye Expansion]モードにします。


- 表示ウィンドウを右クリックし、**Fisheye Expansion**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」を参照してください。



注記

ライブビューでは、フィッシュアイエキスパンションの再生時のマウントタイプは、マウントタイプによって設定されます。詳しくは、**Fisheye モードでライブビューを実行する**を参照してください。

 が  に変わります。

4.表示領域の左下隅の  をクリックして、再生の拡張モードを選択します。

フィッシュェイ

Fisheye ビューモードでは、カメラのワイドビュー全体が表示されます。このビューモードは、魚の凸状の眼の視覚に近似するため、フィッシュェイと呼ばれる。レンズは、広い領域の曲線画像を作成し、画像内の対象物の透視と角度を歪めます。

パノラマ/デュアル 180° パノラマ/360° パノラマ

Panorama view mode では、歪んだ魚眼画像を通常の透視像に較正方法にて変換します。

PTZ

PTZ ビューは、Fisheye ビューまたは Panorama ビュー内の一部の定義領域のクローズアップビューであり、e-PTZ と呼ばれる電子 PTZ 機能をサポートします。



注記

各 PTZ ビューは、Fisheye ビューと Panorama ビューに、特定のナビゲーションボックスでマークされます。Fisheye ビューまたは Panorama ビューのナビゲーションボックスをドラッグして、PTZ ビューを調整したり、PTZ ビューをドラッグして、目的の角度にナビゲーションボックスを調整したりできます。

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、目的の角度に合わせることができます。

検査試薬半球

AR半球モードは、画像が遠く近くに重なり、広角で寸法画像を見ることができます。

シリンダ

シリンダモードでは、画像はシリンダページに形成され、任意にドラッグすることができます。検出エリアのどこにでも見えるように柔軟に指示します。

- 5.オプション:Fisheye ビューモードの再生ウィンドウを右クリックし、選択したウィンドウをフルスクリーンモードに切り替えます。



注記

ウィンドウを右クリックし、**全画面表示を終了**を選択して全画面表示モードを終了します。

5.11 低帯域幅での再生

低いネットワーク帯域幅の状況では、ビデオストリーミングの速度は、帯域幅制限のために、はるかに遅くなる可能性がある。低帯域幅のユーザに対してより少ないストリーミング速度で通常の品質を提供するために、クライアントは低帯域幅モードで再生を提供する。その前に、ストリーミングプロトコルを設定し、他の操作を最初に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小さい場合のライブビューおよび再生のパフォーマンスを向上させる方法を参照してください。

5.12 ビデオ映像をダウンロードする

再生中は、1台のカメラ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



注記

ードできます。

- クラウドP2Pで追加した機器のビデオファイルをダウンロードできます。
- デバイスの他のユーザー名(adminを除く)によってクライアントに追加されたNVRの場合、このNVRで「**Double Verification**」が有効になっている場合、クライアントでビデオを再生するときに、二重検証のために作成されたユーザー名とパスワードを入力する必要があります。二重検証の詳細については、NVRのユーザーマニュアルを参照してください。

5.12.1 ビデオ映像を日付でダウンロードする

再生中は、カメラのビデオ素材をダウンロードしてローカルPCに保存できます。

ステップ

1. リモート再生ページを入力し、再生を開始するカメラを選択します。



再生開始の詳細については、リモート再生を参照してください。

2. 画像上で右クリックし、**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素材の開始時刻と終了時刻を設定します。
4. ビデオ素材の名前を入力します。
5. 「OK」をクリックして、ビデオ素材をローカル PC にダウンロードします。

5.12.2 複数のカメラのダウンロード


複数のカメラの再生中に、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せん。

ステップ

1. リモート再生ページを入力し、複数のカメラを選択して再生を開始します。



再生開始の詳細については、リモート再生を参照してください。

2.  をクリックすると、複数カメラのダウンロードウィンドウが開きます。再生中のカメラがすべて表示されます。
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. 各カメラのビデオ継続時間の開始時間と終了時間を設定します。
5. オプション: プレイヤーをダウンロードするには、**Download Player** をチェックします。
6. 「**ダウンロード**」をクリックして、設定した継続時間のビデオファイルをローカル PC にダウンロードします。
プログレスバーには、各カメラのビデオファイルのダウンロード処理が表示されません。

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



カメラの動画を最大 16 件まで同時にダウンロードできます。

第 6 章 イベント設定

イベントは、事態を迅速に処理するのに役立つ特定の事態を警備員に通知するために使用される。イベントは、通知およびイベント処理のための一連のリンク動作(例えば、音声による警告および電子メールの送信)をトリガすることができる。イベントを使用可能にし、クライアントに追加されたリソースのリンク・アクションを設定することができます。選択されたイベントが発生した場合、クライアントはリアルタイムでイベント通知を受信し、詳細を確認し、それに従ってイベントを処理することができます。

ビデオイベント

ビデオイベントは、ビデオ例外、監視領域の例外、アラーム入力、符号化デバイスの例外などによってトリガされる特別なイベントを指します。詳細については、「カメラのイベント設定」、「アラーム入力のイベント設定」、「エンコーディングデバイスのイベント設定」を参照してください。

アクセス制御イベント

アクセス制御イベントとは、アクセス制御装置、ドア、カードリーダ、エレベータ、ビデオインターホン装置などでトリガされる特殊イベントを指す。詳細については、「クライアント・アクションのアクセス・イベントの設定とビデオ・インターコム・イベントの設定」を参照してください。

セキュリティ管理イベント

セキュリティ管理イベントは、セキュリティ管理パネルのゾーンによって起動される特別なイベントを指します。詳細については、「ゾーンイベントのクライアントリンクの設定」を参照してください。

6.1 カメラのイベント設定

カメラのイベントは、ビデオ例外、またはカメラのモニタ領域で検出されたイベント、例えば、動き検出、ビデオ損失、ラインクロスなどを指す。クライアントのカメラでイベントを有効にすることができます。イベントがカメラでトリガーされると、クライアントは、確認のためのイベントを受信し、記録し、通知のための一連のリンク動作(例えば、電子メールの送信)をトリガーすることができます。

ステップ

1. 「イベント設定」→「ビデオイベント」→「カメラ」をクリックします。

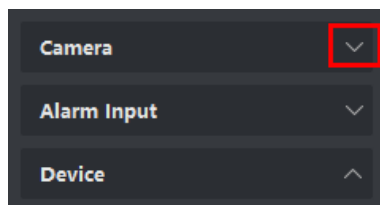


図 6-1 ディスプレイカメラリソース

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。



リソースがオンラインであることを確認します。

選択したカメラでサポートされているイベントタイプがすべて表示されます。

<input type="checkbox"/>	Event Type	Priority	Trigger Client Action	Linked Camera	Enable
<input type="checkbox"/>	Audio Input Exception...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_IPC-1	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Defocus Detection Ala...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_IPC-1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Face Detection Alarm	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_IPC-1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Intrusion Detection Al...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_IPC-1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Line Crossing Detectio...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_IPC-1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Motion Detection Alar...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_IPC-1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Object Removal Detec...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_IPC-1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Region Entrance Dete...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_IPC-1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Region Exiting Detecti...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_IPC-1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Scene Change Detecti...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_IPC-1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Unattended Baggage ...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_IPC-1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Video Tampering Det...	Uncategorized	Audible Warning/Pop-up Window/Display ...	Camera1_IPC-1	<input checked="" type="checkbox"/>

図6-2 カメラのイベントを設定する

3. オプション:「フィルター」フィールドにキーワードを入力して、目的のイベントを素早く見つけます。
4. オプション:[Enable]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、[Enable All]をクリックします。
このカメラのすべてのイベントタイプを有効にします。



使用可能になった後、イベントをクライアントが受信し、リンク動作をトリガすることができます。イベント・タイプを無効にしたり、すべてのイベント・タイプを無効にしたりすることもできます。

5. オプション: イベントを選択し、以下の操作を行います。

優先度の編集 「優先順位の編集」をクリックして、イベントの優先順位を設定します。優先度は、イベントの緊急度を表します。

イベントリンクの編集 [Edit Event Linkage]をクリックして、イベントのリンク動作を設定します。

音声警告

イベントがトリガーされたら、クライアントの音声警告をトリガーします。

ドロップダウンリストから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を追加します(WAV形式)。

クリックすると、選択したオーディオファイルのオーディオがオーディオされます。🔊

メールを送る

アラーム情報の電子メール通知を1つ以上の受信者に送信します。

電子メールパラメータの設定方法については、「電子メールパラメータの設定」を参照してください。

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撮影画像を含む)を表示するポップアップウィンドウ。また、イベントの処理方法についてのコメントも入力できます。

マップ表示

イベントソースがマップ上のホットスポットとして追加されると、イベントがトリガされたときにホットスポットが輝きを放つように表示されます。これは、セキュリティ担当者がイベントの場所を確認するのに役立ちます。📍

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

連動カメラ

イベントがトリガーされたときに、選択したカメラをリンクして、画像を撮影したり、ビデオを録画したりします。

コピーをクリックして、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。

次にすべきこと

アラーム入力が属するデバイスをアーム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の受信を有効にする」を参照してください。

6.2 アラーム入力のイベント設定

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されるイベントを指します。クライアントのアラーム入力に対してイベントを有効にすることができます。アラーム入力がトリガーされると、クライアントは、通知のために一連のリンク動作(例えば、電子メールの送信)を確認しトリガーするためのイベントを受信し、記録することができます。

ステップ

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。

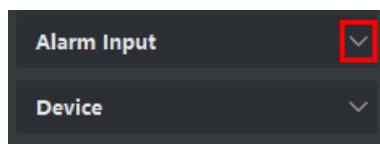


図 6-3 アラーム入力リソースの表示

2. グループを展開し、イベントソースとしてアラーム入力を選択します。



注

リソースがオンラインであることを確認します。

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:「フィルター」フィールドにキーワードを入力して、目的のイベントを素早く見つけます。

4. オプション:[Enable]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、[Enable All]をクリックします。
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
使用可能になった後、イベントをクライアントが受信し、リンク動作をトリガすることができます。イベント・タイプを無効にしたり、すべてのイベント・タイプを無効にしたりすることもできます。

5. オプション:イベントを選択し、以下の操作を行います。

優先度の編集 「優先順位の編集」をクリックして、イベントの優先順位を設定します。
優先度は、イベントの緊急度を表します。

イベントリンクの編集 [Edit Event Linkage]をクリックして、イベントのリンク動作を設定します。

音声警告

イベントがトリガーされたら、クライアントの音声警告をトリガーします。
ドロップダウンリストから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を追加します(WAV形式)。
クリックすると、選択したオーディオファイルのオーディオがオーディオされます。🔊

メールを送る

アラーム情報の電子メール通知を1つ以上の受信者に送信します。
電子メールパラメータの設定方法については、「電子メールパラメータの設定」を参照してください。

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撮影画像を含む)を表示するポップアップウィンドウ。また、イベントの処理方法についてのコメントも入力できます。

マップ表示

イベントソースがマップ上のホットスポットとして追加されると、イベントがトリガされたときにホットスポットが輝きを放つように表示されます。これは、セキュリティ担当者がイベントの場所を確認するのに役立ちます。📍
ホットスポットをクリックして、リンクされたカメラのイベントの詳細やライブビデオを表

示することもできます。

連動カメラ

イベントがトリガーされたときに、選択したカメラをリンクして、画像を撮影したり、ビデオを録画したりします。

[コピー]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。



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。

次にすべきこと

アラーム入力に属するデバイスをアーム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の受信を有効にする」を参照してください。

6.3 エンコーディング・デバイスのイベント設定

エンコーディングデバイスのイベントは、オフラインデバイスなどのエンコーディングデバイスの例外を参照します。クライアントに追加されたエンコーディング装置のイベントを使用可能にすることができます。イベントがデバイス上でトリガされると、クライアントは、確認のためのイベントを受信し、記録し、通知のための一連のリンクアクション(例えば、電子メールの送信)をトリガすることができます。

ステップ

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。

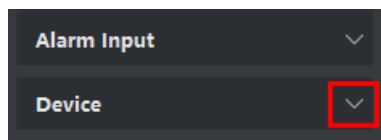


図 6-4 表示デバイスリソース

2. イベントソースとしてデバイスを選択します。



リソースがオンラインであることを確認します。

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:「フィルター」フィールドにキーワードを入力して、目的のイベントを素早く見つけます。
4. オプション:[Enable]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、[Enable All]をクリックします。
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

使用可能になった後、イベントをクライアントが受信し、リンク動作をトリガすることができます。イベント・タイプを無効にしたり、すべてのイベント・タイプを無効にしたりすることもできます。

5. オプション:イベントを選択し、以下の操作を行います。

優先度の編集 「優先順位の編集」をクリックして、イベントの優先順位を設定します。
優先度は、イベントの緊急度を表します。

イベントリンクの編集 [Edit Event Linkage]をクリックして、イベントのリンク動作を設定します。

音声警告

イベントがトリガーされたら、クライアントの音声警告をトリガーします。

ドロップダウンリストから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を追加します(WAV形式)。

クリックすると、選択したオーディオファイルのオーディオがオーディオされます。🔊

メールを送る

アラーム情報の電子メール通知を1つ以上の受信者に送信します。

電子メールパラメータの設定方法については、「電子メールパラメータの設定」を参照してください。

[コピー]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。

次にすべきこと

このデバイスをアーム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の受信を有効にする」を参照してください。

第7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、リアルタイムおよびヒストリカル・イベントの詳細情報を確認したり、イベントリンクビデオを表示したり、イベントを処理したりすることができます。

クライアントがデバイスからイベント情報を受信する前に、リソースのイベントを使用可能にし、デバイスを最初にアームする必要があります。詳細については、「デバイスからイベントを受信するためのイベント設定および有効化」を参照してください。

ポップアップ・アラーム情報を表示する前に、イベント・トリガー・ポップアップ・イメージをイベント・センターで使用可能にする必要があります。詳細は、「ポップアップイベント情報の表示」を参照してください。

7.1 デバイスからの受信イベントの有効化

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前に、最初にデバイスをアームする必要があります。

ステップ

1. [Device Arming Control]ページを開くには、[Tool]->[Device Arming Control]をクリックします。追加したすべてのデバイスがこのページに表示されます。☰
2. Auto-Arming欄では、Auto-Armingを有効にするスイッチをONにします。

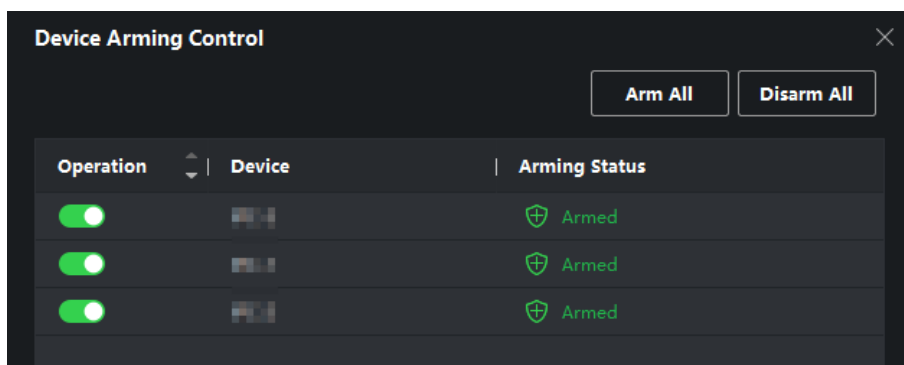


図7-1 アーム装置

電源を入れると、装置は武装化されます。また、武装した装置によって起動されたイベントに関する通知は、リアルタイムでクライアントソフトウェアに自動的に送信されます。

7.2 リアルタイムイベントの表示

接続されている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・タイム、優先度などのリアルタイム・イベント情報を確認できます。

開始前に

クライアントがデバイスからイベントを受信する前に、デバイスからイベントを受信できるようにします。

詳細については、デバイスからの受信イベントを有効にします。

ステップ

1. 「イベントセンター」→「リアルタイムイベント」をクリックしてリアルタイムイベントページを入力し、以下を表示できます。

クライアントが受信したリアルタイムイベント
イベント時間

エンコーディング・デバイスの場合、イベント・タイムは、イベントを受信したクライアント時刻です。その他のデバイスタイプでは、イベント時刻はイベントがトリガされた時刻である。

優先順位

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)プライオリティによるフィルタ

フィルタリングするデバイスタイプおよび(または)プライオリティの選択イベント
キーワードによるフィルタ

イベントをフィルターするキーワードを入力します。

3. オプション: イベント・リストのテーブル・ヘッダーを右クリックして、イベント・リストに表示するイベント関連項目を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・リストでイベントを選択します。
 - 2) ページの右下隅にある展開をクリックします。
 - 3) 関連する絵、詳細な説明、およびイベントの処理記録を表示します。



撮影した画像については、履歴イベントを検索する際に画像を見ることができるよう、画像保存を設定する必要があります。

4) オプション:関連する画像にカーソルを合わせ、画像の右上隅にあるダウンロードアイコンをクリックして、ローカルPCにダウンロードします。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行います。

単一イベントの処理

ハンドルをクリックして処理の提案を入力し、クリックします。

コミットメント



注

イベントが処理されると、ハンドルボタンは「備考の追加」になります。「備考の追加」をクリックして、この処理されたイベントに関する追加の備考を追加します。

バッチ内のイベントの処理

処理する必要のあるイベントを選択し、Handle in Batchをクリックします。処理の提案を入力し、コミットをクリックします。

アラームオーディオの有効/無効

イベントのオーディオを有効/無効にするには、「オーディオを有効/無効にする」をクリックします。

自動的に最新イベントを選択

最新イベントを選択するために、自動選択の最新イベントをチェックする自動的にイベント情報の詳細が表示されます。

イベントのクリア

「クリア」をクリックして、イベント・リスト内のすべてのイベントをクリアします。

メールを送る

イベントを選択し、「電子メールの送信」をクリックすると、このイベントの詳細が電子メールで送信されます。



注

まず、電子メールパラメータを設定します。詳細については、「電子メールパラメータの設定」を参照してください。

7.3 履歴イベントの検索

クライアントで時刻、デバイスタイプ、優先度などの検索条件を設定することで、履歴イベントを検索および表示できます。検索されたイベントについては、それらを処理およびエクスポートすることができます。

開始前に

クライアントがデバイスからイベント情報を受信する前に、デバイスからイベントを受信できるようにする。詳細については、「デバイスからイベントを受信できるようにする」を参照してください。

ステップ

1. 「イベントセンター」→「イベント検索」をクリックして、イベント検索ページに入ります。
2. 必要なイベントのみを表示するようにフィルター条件を設定します。

時間

イベントが開始する時刻。

検索

装置

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。機器から検索する場合は、以下の設定が必要です:

- 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。
- Device Type: イベントを検索するデバイスを選択します。

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

- ビデオインターホンデバイスでは、検索範囲を「すべて」と「ロッキングログ」に設定する必要があります。
 - アクセス制御デバイスの場合、「その他を表示」をクリックすると、ステータス、イベントタイプ、カードリーダータイプ、個人名、カード番号、組織などの条件を設定できます。
-

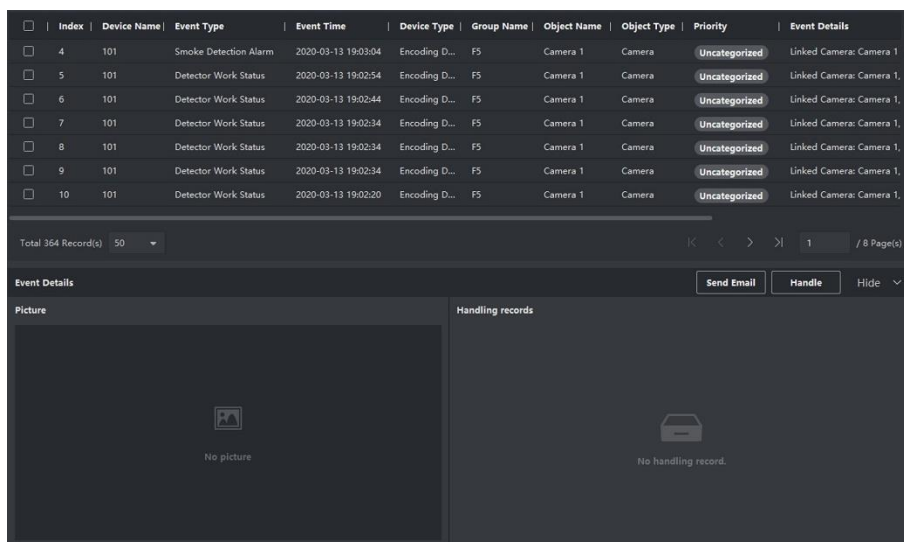
優先順位

イベントの緊急度を示す、低、中、高、およびカテゴリー化されていない優先度。

ステータス

イベントの処理状況。

3. 「検索」をクリックして、設定した条件に従ってイベントを検索します。



<input type="checkbox"/>	Index	Device Name	Event Type	Event Time	Device Type	Group Name	Object Name	Object Type	Priority	Event Details
<input type="checkbox"/>	4	101	Smoke Detection Alarm	2020-03-13 19:03:04	Encoding D...	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1
<input type="checkbox"/>	5	101	Detector Work Status	2020-03-13 19:02:54	Encoding D...	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1
<input type="checkbox"/>	6	101	Detector Work Status	2020-03-13 19:02:44	Encoding D...	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1
<input type="checkbox"/>	7	101	Detector Work Status	2020-03-13 19:02:34	Encoding D...	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1
<input type="checkbox"/>	8	101	Detector Work Status	2020-03-13 19:02:34	Encoding D...	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1
<input type="checkbox"/>	9	101	Detector Work Status	2020-03-13 19:02:34	Encoding D...	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1
<input type="checkbox"/>	10	101	Detector Work Status	2020-03-13 19:02:20	Encoding D...	F5	Camera 1	Camera	Uncategorized	Linked Camera: Camera 1

Total 364 Record(s) 50

Event Details Send Email Handle Hide

Picture No picture

Handling records No handling record.

図7-2 ヒストリカル・イベントの検索

4. オプション: イベント・リストに表示するイベント関連項目をカスタマイズするには、イベント・リストのテーブル・ヘッダーを右クリックします。
5. オプション: 以下の操作のいずれかを実行します。
- 6.

単一イベントの処理

単一のイベントを処理する: 処理する必要があるイベントを1つ選択し、イベント情報詳細ページの「処理」をクリックし、処理案を入力する。



注

イベントを処理した後、ハンドルボタンが「備考の追加」になり、「備考の追加」ボタンをクリックして、この処理済みイベントのさらなる備考を追加します。

バッチ処理イベント

バッチでイベントを処理する: 処理する必要があるイベントを選択し、「バッチで処理」をクリックし、処理の提案を入力します。



イベントを処理した後、ハンドルボタンが「備考の追加」になり、「備考の追加」ボタンをクリックして、この処理済みイベントのさらなる備考を追加します。

メールを送る

イベントを選択し、「電子メールの送信」をクリックすると、このイベントの詳細が電子メールで送信されます。



まず、電子メールパラメータを設定します。詳細については、「電子メールパラメータの設定」を参照してください。

エクスポートイベント情報

「エクスポート」をクリックして、イベントログまたはイベントピクチャをCSV/Excelファイル内のローカルPCにエクスポートします。保存パスは手動で設定できます。

イベント関連画像のダウンロード

関連する画像にカーソルを合わせ、画像の右上隅にあるダウンロードアイコンをクリックしてローカルPCにダウンロードします。保存パスは手動で設定できます。

7.4 デバイスからのイベントの取得

シナリオによっては(例えば、クライアントが起動できない、他のクライアントからアクセス制御デバイスが装備されているなど)、クライアントが受信し、アクセス制御デバイスで起動されるイベントが一貫していない。デバイスからリモートからイベントを取得して、デバイスからクライアントのイベントセンターにイベントを同期させることができます。

[Device Management]→[Device]→[Device]の順にクリックし、[Access Control Device]を選択して[Get Events from Device]をクリックします。

2つの方法でイベントを同期させます:

- **オンライン:** デバイスがオンラインであり、デバイスがリアルタイムでクライアントと通信できる場合、オンラインを選択し、開始時刻と終了時刻を設定して、この期間中のイベントを取得できます。

- インポートファイル:ネットワークが正常でない場合、またはデバイスがリアルタイムでクライアントと通信できない場合は、まず選択したデバイスからイベントファイルをエクスポートし、後で「Import File」を選択して、暗号化されたファイルのパスワードを入力することにより、クライアント上のこのエクスポートされたファイルをインポートできます。

i注

- データセキュリティのためには、デバイス上でエクスポートするときにファイルを暗号化する必要があります。一方、選択したアクセス・コントロール・デバイスは、ファイルをエクスポートしたデバイスである必要があります。
- この機能は、デバイスによってサポートされる必要があります。

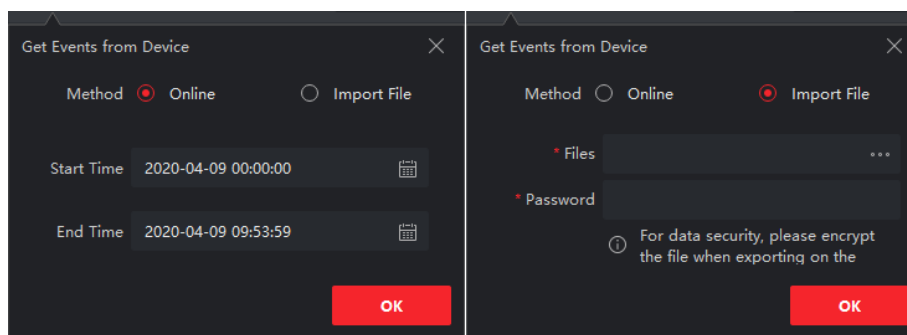


図7-3 デバイスからイベントを取得する

i注記

- 出席のみに関連するイベントを取得したい場合は、[Time & Attendance] → [Attendance Statistics] → [Attendance Records] と入力し、[Get Events from Device] をクリックし、アクセス制御デバイスを選択してイベントを同期させることもできます。
- 出席に関連するイベントは、オンラインモードで「Time & Attendance」に同期されません。
モジュール

7.5 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、イベントトリガー・ポップアップ・イメージをそのリンク・アクションとして設定すると、イベントが発生すると、イベント情報、関連する写真、および関連するビデオが表示されたウィンドウがポップアップします。

「イベントセンター」→「リアルタイムイベント」に進み、「アラームトリガー・ポップアップ・イメージを有効にする」をクリックして機能を有効にします。

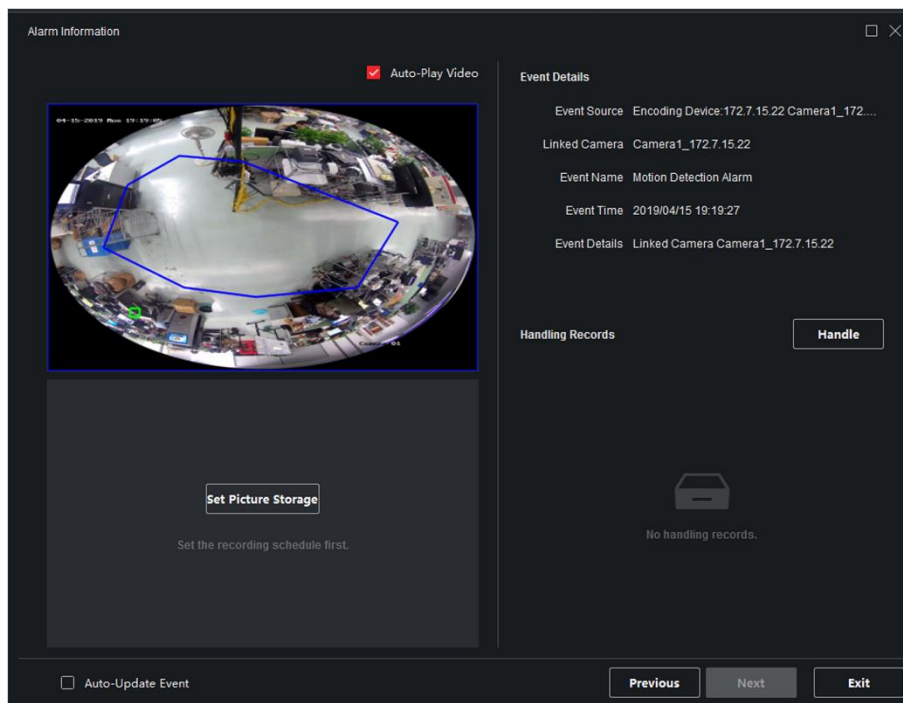


図7-4 ポップアップイベント情報

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最後まで)、イベントが発生したときに撮影された画像、およびイベントソース、リンクされたカメラ、イベントの種類などのイベントの詳細を表示できます。

注記

- ウィンドウが閉じていない場合は、[次へ]をクリックして、新しいイベントが起動されたときに新しいイベント情報を表示する必要があります。
 - イベント情報がクリアされていない場合は、「前へ」をクリックして前のイベントを表示できます。
- 情報

自動更新イベントをチェックして、自動的に最新イベントに切り替えることができます。新規イベントがトリガーされるときの情報。

第 8 章 マップ管理

E-map機能は、設置されたカメラや警報入力装置の位置や分布を視覚的に概観する機能です。地図上にカメラのライブビューを表示することができ、アラームが発生すると地図から通知メッセージが表示されます。

E-mapは静的な画像(地理地図である必要はありませんが、地図である必要はありません。組織のニーズに応じて、写真や他の種類の画像ファイルをe-mapとして使用することもできます)であり、地図上に配置されたホットスポット(カメラ、アラーム入力などのリソース)の位置や分布を視覚的に概観することができます。カメラとアラーム入力の物理的な位置と、カメラがどの方向を向いているかを確認できます。e-mapは、ホットリージョンの機能を利用して階層化することができ、階層化することで、フロアレベルから部屋レベルなど、幅広い視点から詳細な視点へとナビゲートすることができる。

8.1 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。

ステップ

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-map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

グループの設定については、「グループ管理」を参照してください。

3. 「マップの追加」をクリックしてマップの追加ウィンドウを開きます。
4. 追加したマップの説明名を入力します。
5. ローカルパスからマップピクチャを選択します。

注記

マップの画像フォーマットは、PNG、JPEG、BMPのみである。

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、以下のタスクを実行します。

拡大/縮小	マップ上でズームインまたはズームアウトするには、マウスホイールまたは+または-をクリックします。
マップ領域の調整	黄色のウィンドウを右下隅にドラッグするか、方向ボタンとズームバーを使ってマップ領域を調整します。

8.2 マップスケールの編集

地図の目盛は、地図上の距離と地上の対応する距離との比である。地上の距離に応じて、地図上の2箇所の距離を計算することができます。正確な地図スケールは、レーダーの監視範囲を定義するために不可欠である。

開始前に

マップが追加されていることを確認します。詳細については、「マップの追加」を参照してください。

このタスクは、マップにセキュリティレーダーを追加する必要がある場合に実行します。

ステップ

1. E-mapモジュールを入力する。
2. E-mapツールバーの「編集」をクリックして、マップ編集モードに入ります。
3. スケールの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。
カーソルは、マップ上でホバリングすると表示されます。+
4. マップをクリックして2つの場所を選択します。
「スケールの編集」ウィンドウがポップアップします。
5. 2箇所の接地距離を入力し、OKをクリックします。
クライアントは自動的にマップスケールを計算します。

8.3 ホットスポットの管理

マップに追加されたデバイスはホットスポットと呼ばれます。ホットスポットは装置の位置を示し、ホットスポットを通して監視シナリオのライブビューまたはアラーム情報を取得することもできます。

8.3.1 カメラをホットスポットとして追加する

カメラをホットスポットとしてマップに追加できます。

開始前に

クライアントに e-map とカメラを追加したことを確認します。詳細については、Add Map および Device Management を参照してください。

ステップ

1. E-map ページを入力します。
2. 右上の「編集」をクリックして、マップ編集モードに入ります。
3. 「ホットスポットの追加」→「カメラホットスポット」の順にクリックして、「ホットスポットの追加」ウィンドウを開きます。

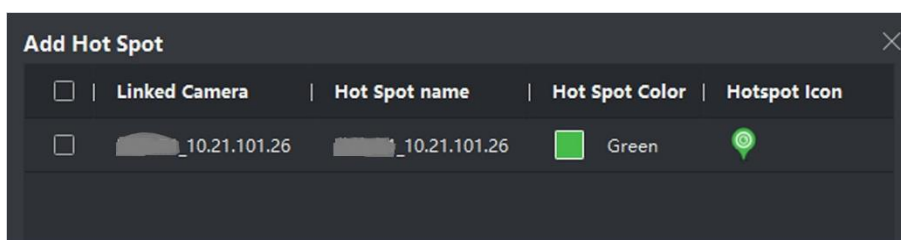


図8-1 ホットスポットの追加パネル

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、ホットスポットアイコンを選択します。
6. 設定を保存するには、OKをクリックします。



注記

グループリストからカメラのアイコンを直接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。

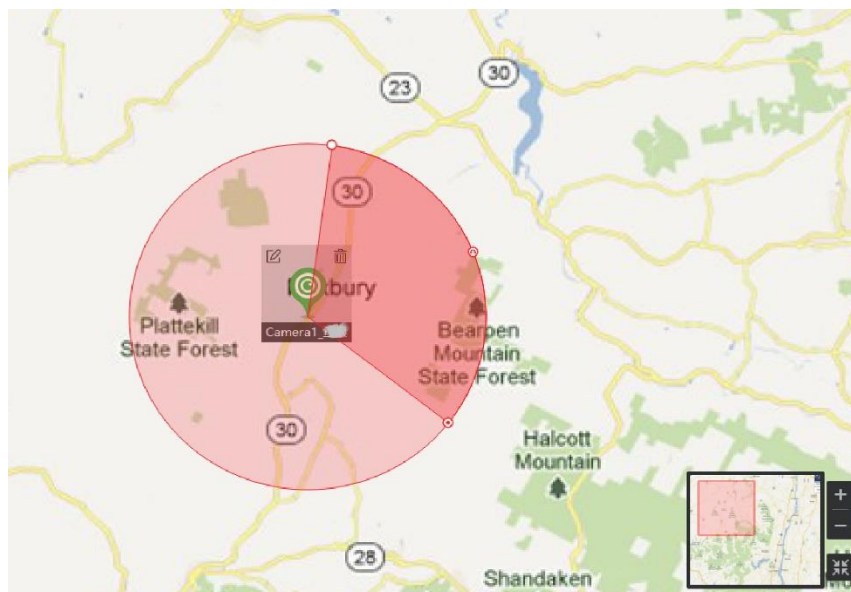


図8-2 地図上のカメラ

カメラのアイコンがホットスポットとしてマップ上に追加され、グループリストに追加されたカメラのアイコンが次々に変更されます。セクターはカメラの視野を示します。📷👁️

7. 以下の操作を行います。

ホットスポットの移動	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。
視野角を変更する	📷/👁️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。

8.3.2 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。

ステップ

1. E-mapモジュールを入力する。
2. 右上の「編集」をクリックして、マップ編集モードに入ります。
3. 「ホットスポットの追加」→「アラーム入力ホットスポット」をクリックして、「ホットスポットの追加」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、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

また、グループリストからアラーム入力アイコンを直接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。

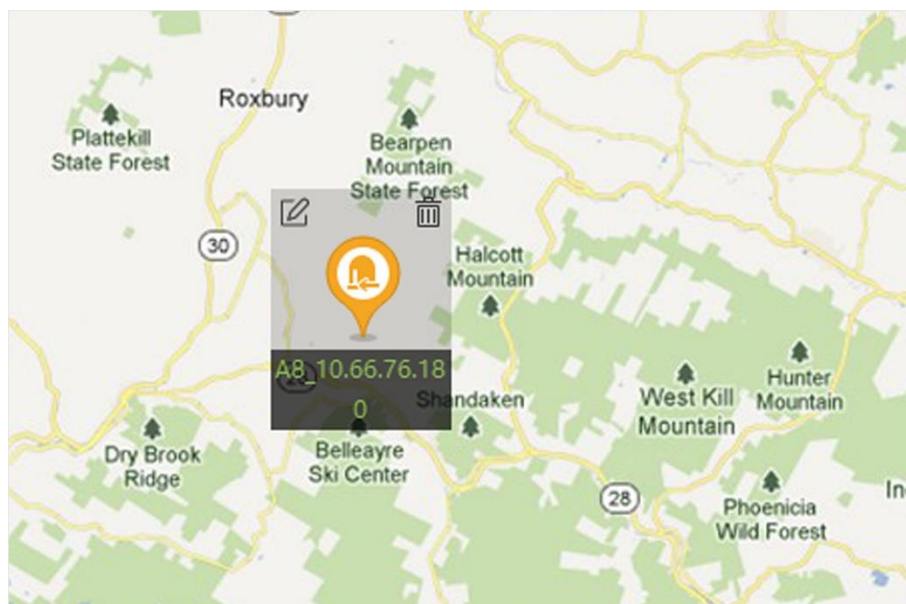



図8-3 地図上のアラーム入力

アラーム入力アイコンはホットスポットとしてマップに追加され、グループリストに追加されたアラーム入力のアイコンが変更されます。

7. オプション:ホットスポットをドラッグして、ホットスポットを特定の位置に移動します。

8.3.3 ホットスポットとしてのアラーム出力の追加

アラーム出力は、管理のホットスポットとしてマップに追加できます。その後、迅速に有効または無効にすることができます。地図上でアラーム出力を有効にすると、アラーム出力に接続されているセキュリティ制御装置(サイレン、ベルなど)が注意を喚起します。

開始前に

クライアントに e-map およびアラーム出力を追加していることを確認します。詳細については、Add Map および Device Management を参照してください。

ステップ

1. E-mapモジュールを入力する。
2. E-mapツールバーの「編集」をクリックして、マップ編集モードに入ります。
3. 「ホットスポットの追加」→「アラーム出力ホットスポット」をクリックして、「ホットスポットの追加」パネルを開きます。

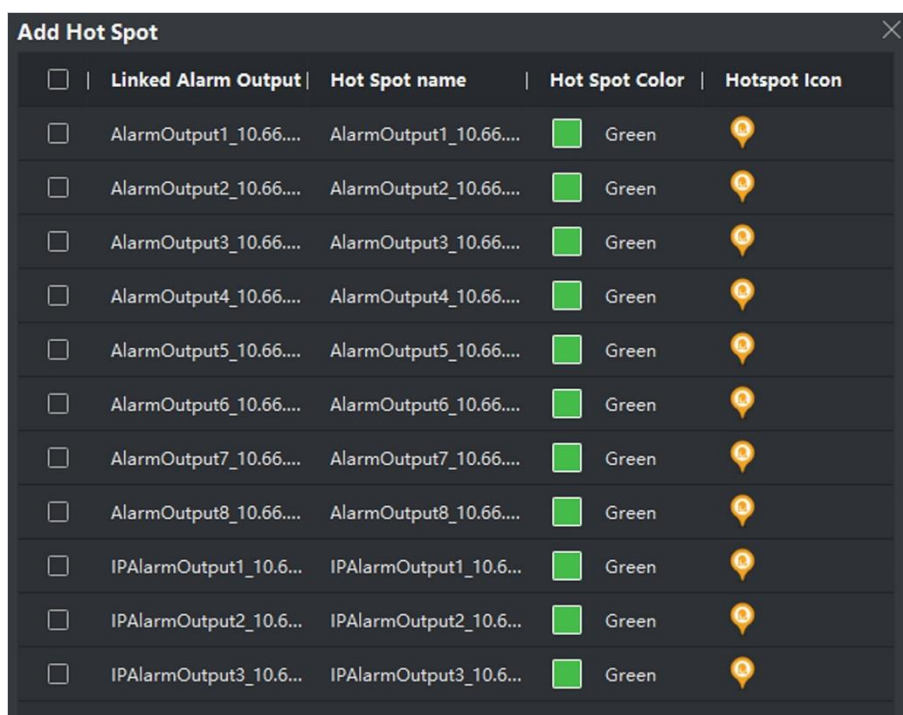


図8-4 ホットスポットの追加パネル

4. 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、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。

i 注記

また、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。

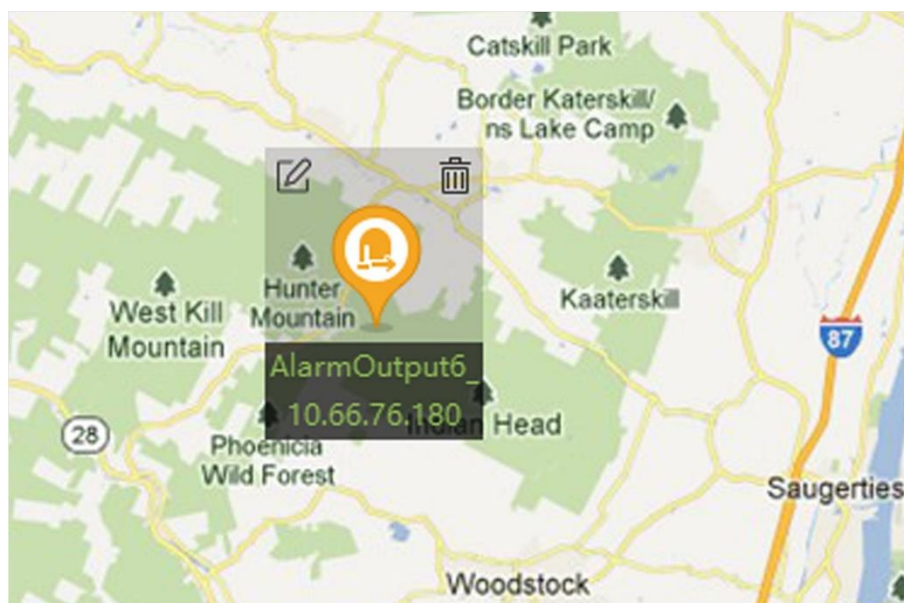


図8-5 マップ上のアラーム出力

アラーム出力はホットスポットとしてマップに追加され、グループリストのアイコンが次の順に変わります。📍🔔

7. オプション:アラーム出力をドラッグして、一定の位置に移動します。

8.3.4 ホットスポットとしてゾーンを追加

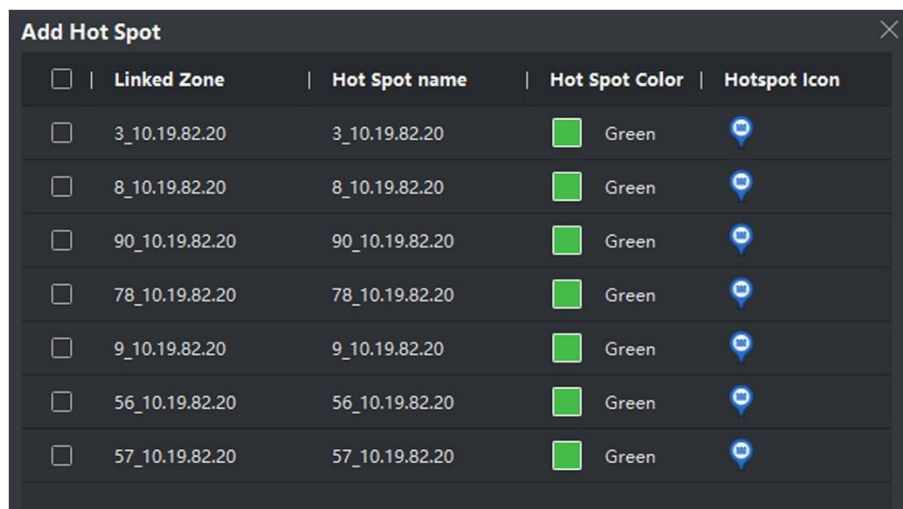
地図にゾーンを追加して、アラームが発生したときにすばやくゾーンを見つけることができます。

開始前に

クライアントにマップとゾーンを追加していることを確認します。詳細については、「デバイスの追加マップ」および「デバイスの追加」を参照してください。

ステップ

1. E-mapモジュールを入力する。
2. E-mapツールバーの「編集」をクリックして、マップ編集モードに入ります。
3. 「ホットスポットの追加」→「ゾーンホットスポット」をクリックして、「ホットスポットの追加」パネルを開きます。

















<input type="checkbox"/>	Linked Zone	Hot Spot name	Hot Spot Color	Hotspot Icon
<input type="checkbox"/>	3_10.19.82.20	3_10.19.82.20	 Green	
<input type="checkbox"/>	8_10.19.82.20	8_10.19.82.20	 Green	
<input type="checkbox"/>	90_10.19.82.20	90_10.19.82.20	 Green	
<input type="checkbox"/>	78_10.19.82.20	78_10.19.82.20	 Green	
<input type="checkbox"/>	9_10.19.82.20	9_10.19.82.20	 Green	
<input type="checkbox"/>	56_10.19.82.20	56_10.19.82.20	 Green	
<input type="checkbox"/>	57_10.19.82.20	57_10.19.82.20	 Green	

図8-6 ホットスポットの追加パネル

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、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。

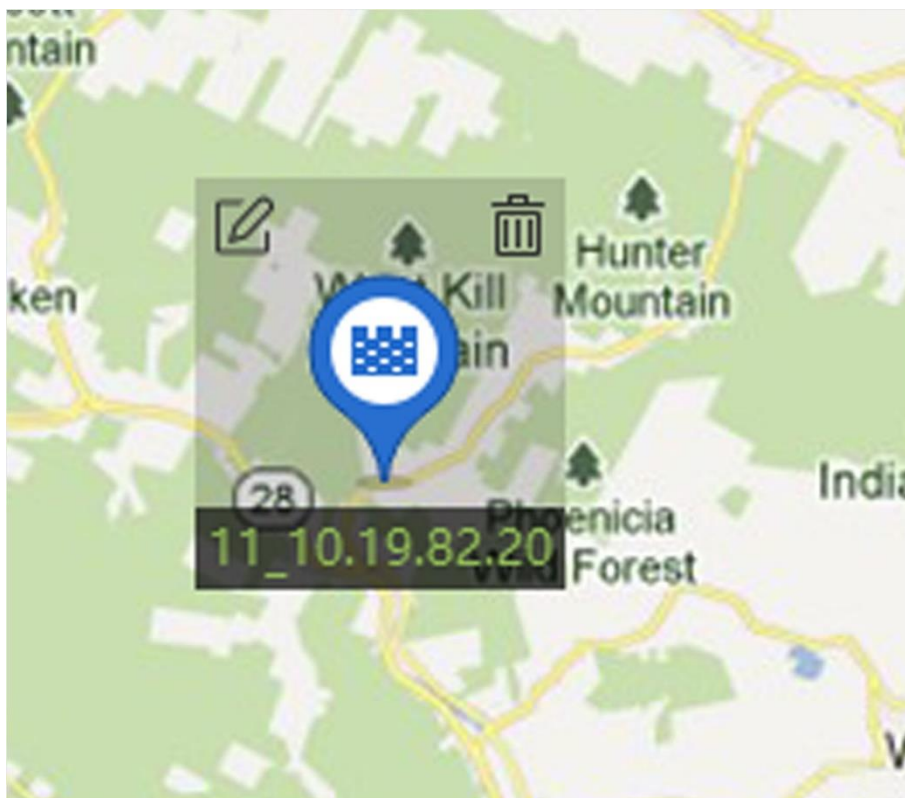


図8-7 地図上のゾーン

ゾーンはホットスポットとしてマップに追加され、グループリストのアイコンが次の順に変更されます。🗺️📌

7. オプション:ゾー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。
アラームがトリガされると、最新のアラームの数がゾーンのアイコンに表示されます。番号をクリックすると、アラームの詳細が表示されます。



注記

最新のアラームは10件まで表示できません。

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読み取りどおりにマークします。

8.3.5 アクセスポイントをホットスポットとして追加

ホットスポットとしてマップにアクセスポイントを追加して、ホットスポットを見つけてステータスとアラーム番号を表示することができます。

開始前に

地図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ます。Add MapおよびAdd Deviceを参照
詳細については、

ステップ

1. E-mapモジュールを入力する。
2. E-mapツールバーの「編集」をクリックして、マップ編集モードに入ります。
3. 「ホットスポットの追加」→「アクセスポイントホットスポット」をクリックして、「ホットスポットの追加」ウィンドウを開きます。

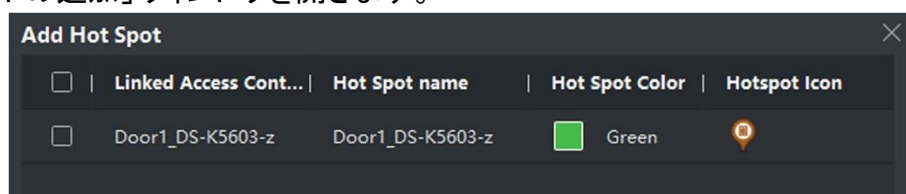


図8-8 ホットスポットの追加パネル

4. 追加する接続先を選択します。
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、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

接続先アイコンを接続先リストからマップにドラッグすることもできます。

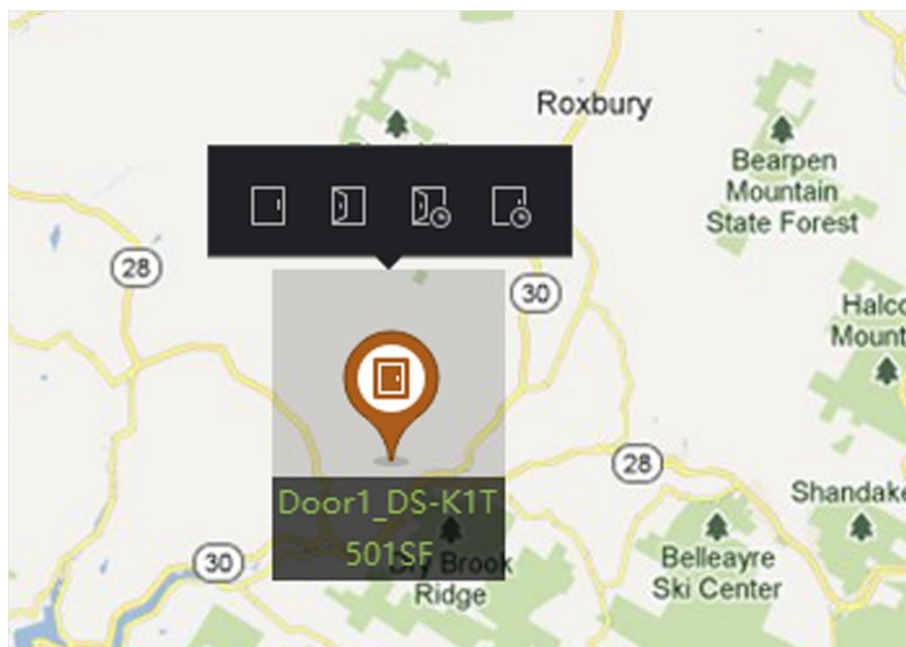


図8-9 マップ上のアクセスポイント

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、グループリストのアイコンが次の順に変わります。■ ■

7. オプション:アクセスポイント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。

アラームが発生すると、ホットスポットアイコンに最新のアラームの数が表示されます。番号をクリックすると、アラームの詳細が表示されます。



注記

最新のアラームは10件まで表示できません。

8.3.6 セキュリティー・レーダー・ホットスポットの設定

クライアントは、ホットスポットとして機能するために、地図にセキュリティーレーダーを追加することをサポートする。その後、レーダーのパラメータ(描画ゾーンやトリガラインの設定、マスタースレーブのトラッキング設定、マップキャリブレーションなど)を設定することができ、設定したパラメータはデバイスに有効になります。このようにして、レーダーの検出領域におけるインテリジェントなモニタリングをクライアントが実現することができる。

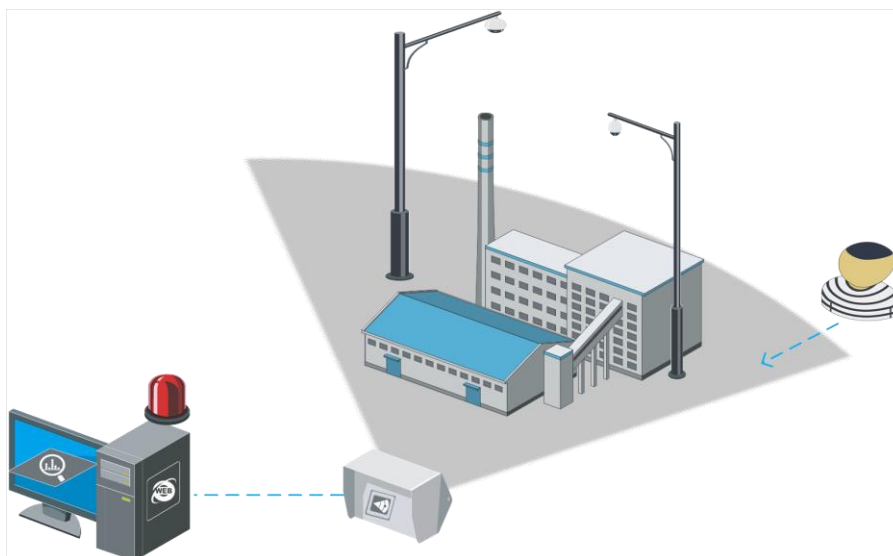


図8-10 レーダーのシナリオ

セキュリティー・レーダーをホットスポットとして追加

効果的なモニタリングを行うには、モニタリングファイルにあるホットスポットとペイントゾーンとして、セキュリティーレーダーをマップに追加します。そのため、誰かがそのゾーンに侵入すると、注意を喚起するための警報が発動される。

開始前に

クライアントに e-map とセキュリティーレーダーを追加していることを確認します。詳細については、Add Map および Device Management を参照してください。

ステップ

1. E-mapモジュールを入力する。
2. E-mapツールバーの「編集」をクリックして、マップ編集モードに入ります。
3. オプション:マップスケールの編集。マップスケールの編集を参照してください。
4. 装置リストでセキュリティーレーダーを選択し、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てホットスポット名を編集し、ホットスポ

ツトの色を選択し、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はホットスポットとしてマップに追加され、グループリストのアイコンが次の順に変わります。セクターはレーダーの監視フィールドを示す。

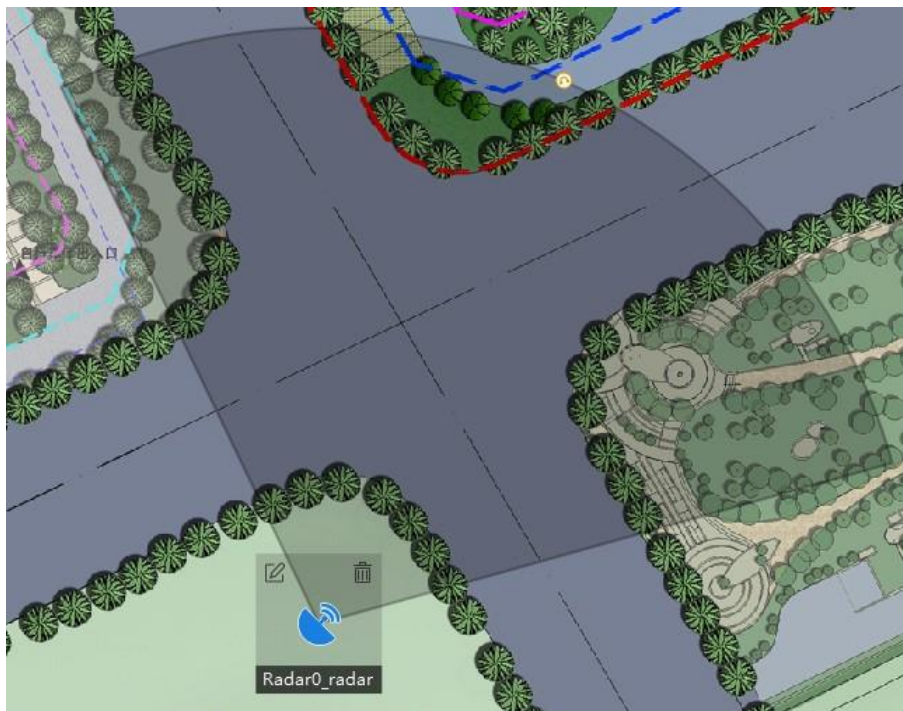


図8-11地図上のレーダー

 注記

- オレンジ・セクターは武装レーダーを、黒・セクターは武装解除レーダーを示す。
- 赤点は侵入者を検出したことを示す。

7. 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。

ゾーンを描く

ゾーンは、セキュリティ管理システムの基本概念である。レーダー検知区域内の防護区域を指し、区域の種類やレーダーの装備状況に応じて警報を発動するかどうかを決定し、警報事象を区別するための最大認識単位と見なされる。アラームが発生した分には、マップ上のターゲットの位置が表示されます。アラームが発生した分には、すぐにアクションが実行されます。

開始前に

レーダーを解除したことを確認します。[完了] をクリックし、レーダーのアイコンをクリックして [解除] を選択します。

ステップ

1. E-Mapモジュールを入力し、右上の「編集」をクリックして編集モードに入ります。
2. オプション: マップの左上にあるフィールドアシスタンスを有効にします。レーダー検知エリアにターゲットトラックが表示されます。トラックを参照してゾーンを描くことができます。
3. 「レーダー設定」→「地図の上部に手動でゾーンを描画」をクリックし、マウスをクリックしてレーダー検知エリアにゾーンを描画します。

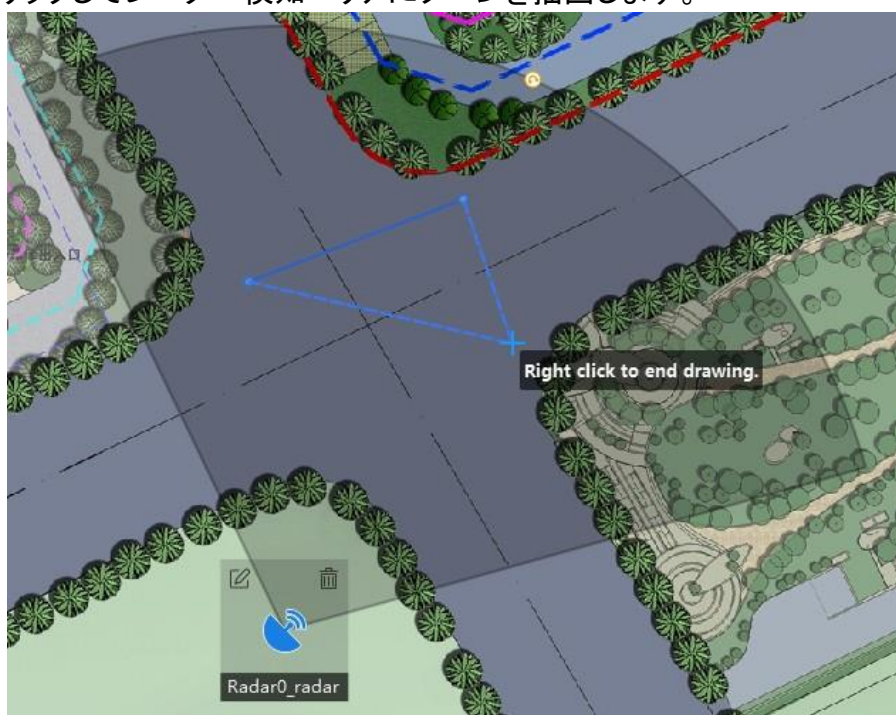


図8-12 ゾーンを描画

4. 右クリックして描画を完了し、ウィンドウがポップアップします。ゾーン名を入力して選択
ゾーンタイプとして、早期警告ゾーン、警告ゾーン、または無効ゾーン。
5. OKをクリックします。

早期警戒区域

早期警戒区域は、事前に潜在的なリスクを有し、警報を発動するが、警報トラックを保管しない目標を特定する。早期警戒区域は緑色である。

警告ゾーン

警報ゾーンは、エリアに入るターゲットを特定し、警報を発する。警告ゾーンはオレンジ色です。

無効ゾーン

無効なゾーンは、エリア内のターゲットトラックをブロックします。無効なゾーンは黒です。

注記

- ・ ゾーンの追加は、バッチ操作です。1つのレーダーのみのゾーンを追加する場合は、残りのレーダー検知エリアを右クリックして、希望するゾーンを描いた後、他のレーダーの検知エリアのゾーンの描画をキャンセルする必要があります。
- ・ ゾーンはオーバーラップする可能性があり、有効オーバーラップするゾーンの優先順位は次のとおりです。無効ゾーン>警告ゾーン>早期警告ゾーンつまり、早期警告ゾーンには警告ゾーンと無効ゾーンを含めることができ、警告ゾーンには無効ゾーンを含めることができます。
- ・ 表示されるレーダー領域のサイズを調整するためにズームイン/ズームアウトすることができます。

6. マップの右上にある「完了」をクリックします。
7. オプション:レーダー解除後にゾーンを編集または削除します。
 - 1) ゾーンをダブルクリックしてゾーン編集モードに入ります。
 - 2) ゾーンのラインにカーソルを合わせると、カーソルが十字に変わり、クリックしてマーカーを追加します。

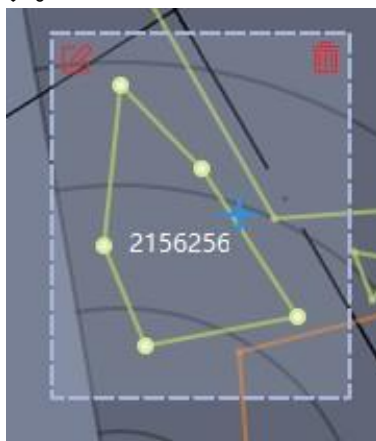


図8-13 マーカーの追加

- 3) マーカーをドラッグして、ゾーンの形状を変更します。

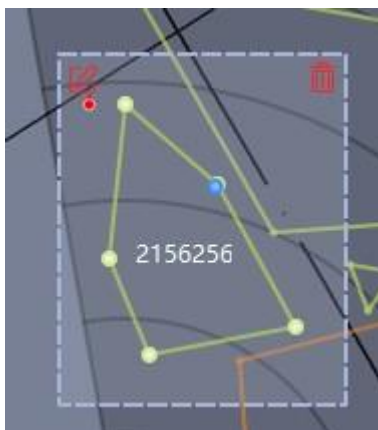


図8-14 マーカーをドラッグする

- 4) 長押しするとゾーンが移動します。

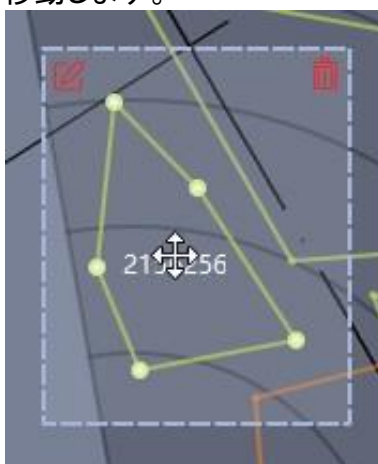


図8-15 ゾーンの移動

- 5) ゾーン外をクリックしてゾーン編集モードを終了します。
 6) ゾーン編集モードに入った後、ゾーンをダブルクリックしてゾーンを削除または編集します。

ゾーン削除	🗑️ クリック	
ゾーンの編集	📄 クリック	ゾーン名とタイプの編集

引抜きトリガ線

トリガラインとは、地図上のレーダーの検知エリアに描かれた仮想線のことです。アラームは、あらかじめ定義された方向に通過したときにトリガされます。

開始前に

レーダーがマップに追加されます。右上の[完了]をクリックして編集モードを終了します。レーダーアイコンをクリックし、「非表示」を選択してレーダーを非表示にします。



ステップ

1. 「E-map」ページで「編集」をクリックし、編集モードに入ります。
2. [レーダ設定]→[トリガラインの作成]の順にクリックし、[トリガライン]または[デュアルトリガライン]を選択します。



注記

デュアルトリガラインを描きすぎると故障の原因となります。

3. 引金線を引く。
 - 1) レーダー検知エリアをクリックして、トリガラインを描きます。
 - 2) ポップアップウィンドウで、Left → Right、Left <RightまたはLeft<->Rightを選択します。
4. オプション:2行間の距離を入力します。(デュアルトリガラインのみ)
 - アラーム規則:1つの矢印  ターゲットがクロスするとアラームがトリガされることを示します。
 - 矢印の方向にあるトリガライン;二重矢印  ターゲットが任意の方向にトリガラインを通過したときにアラームがトリガされることを示します。
 - アラームは、アラームルールに従い、Trigger Lineを通過することによってトリガーすることができます。アラームは、アラームルールに従い、Dual-trigger Lineのダブルラインを通過した後にのみトリガーすることができます。
 - 方向決定:最後のマーカーに向かって2番目に位置するマーカーで、左側の領域が左側を示し、右側の領域が右側を示しているとします。
 - トリガラインは最大4本まで描画できます。
 - 最大1本のデュアルトリガラインを描画できます。

- トリガラインが交差できません。

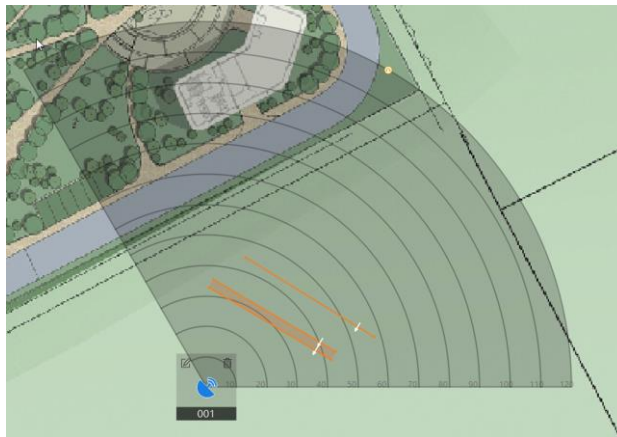


図8-16 引抜きトリガ線

5. OKをクリックします。
6. オプション:トリガラインをクリックすると、「編集」、「削除」、「移動」という別のオプションが表示されます。トリガラインをクリックすると、トリガラインを編集できます。
 - マーカーを追加:行をクリックしてマーカーを追加します。
 - マーカーをドラッグします:トリガライン上のマーカーをドラッグして、マーカーを移動します。
 - Trigger Lineを移動:編集領域を保持してトリガラインを移動します。
 - 編集:クリックすると、トリガライン名、トリガラインルール、距離が編集されます (Dual-trigger Lineのみ)。✎
 - 削除:クリックすると、トリガラインが削除されます。🗑

マスタースレーブトラッキングの設定

マスタースレーブのトラッキングは、レーダーの検知エリアに追加した校正ポイントに基づいて行われます。つまり、キャリブレーションポイントは、ターゲットが検出されたときに、ターゲットのライブビューおよびトラックを得るために、レーダーにリンクされたPTZカメラに向きを変える方向を知らせることができる。



注記

マスタースレーブのトラッキングを設定する前に、以下の操作を行っていることを確認してください:

- 操作前にレーダーを解除する必要がある場合は、右上の[終了]をクリックして終了します。
編集モードレーダーアイコンをクリックし、「非表示」を選択してレーダーを非表示にします。
- 校正前にPTZカメラをゾーンにリンクさせ、PTZカメラの初期位置を設定する必要があります。PTZカメラの初期位置の設定方法については、PTZカメラの取扱説明書をご覧ください。
- レーダーに接続されたPTZカメラをレーダーグループにインポートします。詳細については、「グループリソース」を参照してください。
- 連動型PTZカメラの設置高さは、3m以上とする。
- 本機能に対応しているのはPTZカメラのみです。

レーダとカメラの設置位置に応じて、校正点を選択するためのスケジュール(ワンポイント校正またはマルチポイント校正)を選択する必要があります。

1点校正

レーダーとカメラが同じポールに設置されているシーンや、2mのレーダー中心範囲（カメラとレーダーの高度差にかかわらず）に設置されているシーンに適用できます。



図8-17 ワンポイント校正のシナリオ

多点校正

1点校正に該当しないシーンは、多点校正を採用する必要があります。

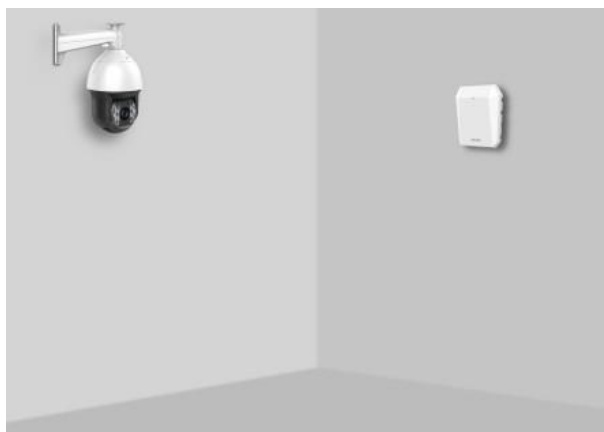


図8-18 多点校正のシナリオ

1点校正

1点校正は、レーダーとカメラが同じポールに設置されているシーンや、レーダー中心2m(カメラとレーダーの高度差にかかわらず)の範囲内に設置されているシーンに適用できます。

開始前に

この機能を実行するには、2人の協力が必要である。人Aが検知エリアに入ると、人B(クライアントのオペレータ)がクライアントがBが校正点を設定したAのトラックを見ることができます。

ステップ

1. マップの右上にある[編集]をクリックします。
2. [レーダー設定]→[マスタースレーブのトラッキング設定]の順にクリックします。
3. Master-Slave Tracking Settingsページで、上部のドロップダウンリストからレーダーを選択します。
左。
4. ライブビューウィンドウをクリックし、リンクされたカメラのリストからカメラを選択します。ライブビューウィンドウにカメラのライブビューが表示されます。
5. カメラのライブビューウィンドウをダブルクリックして拡大します。



注記

+または-をクリックして、マップを拡大/縮小できます。

6. キャリブレーションモードとしてワンポイントキャリブレーションを選択します。

7. 人物Aのトラックを選択し、レーダー検知エリアに移動するには人物Aに依頼します。カメラのライブビューウィンドウの動体とレーダー検知エリアのトラックを比較し、人Bが人Aのトラックを選択してクリックする必要があります。選択したトラックの色が赤色から白色に変わります。

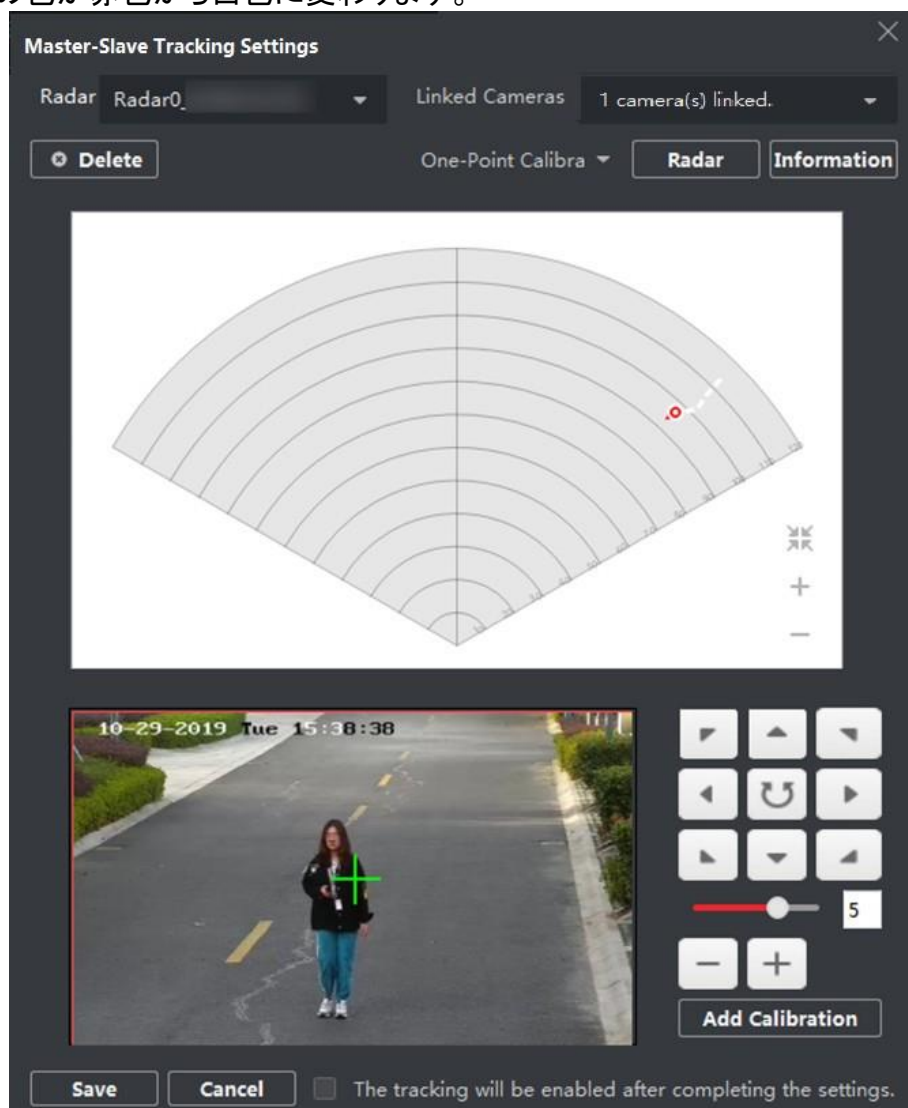


図8-19 トラックの選択

8. レーダーの直前20～40mの範囲内でAにキャリブレーションポイントに移動させ、キャリブレーションポイントに立ちます。
9. ライブビューウィンドウのPTZボタンを調整し、PTZの位置を取得します。+ および - をクリックして、人Aの高度をウィンドウの高度の3分の2に調整し、方向ボタンをクリックして、中央の符号を人Aに合わせます(正確に配置するには、オブジェクトの中心をクリックし、画面が自動的に調整します)。

10. 「キャリブレーションの追加」をクリックして、キャリブレーションポイントを追加します。PTZ位置と人Aのレーダー位置が情報一覧に表示されます。設定が終了すると、自動的にトラッキングが有効になります。

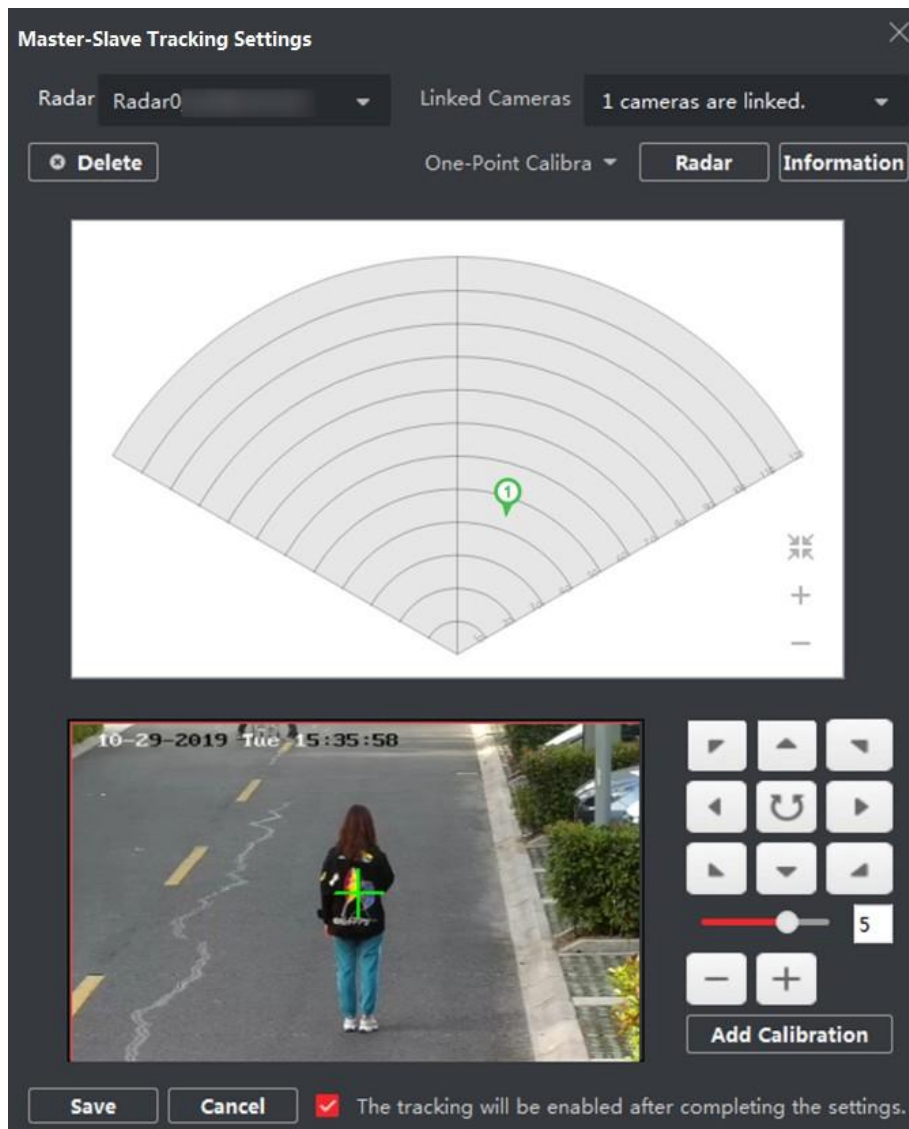


図8-20 キャリブレーションの追加

11. 保存をクリックします。

多点校正

多点校正は、レーダーとそれに接続するカメラの距離が2メートルを超える場合に適用されます。

開始前に

この機能には2名の協力が必要です。人Aが検知エリアに入ると、人B(クライアントのオペレータ)がクライアントがBが校正点を設定したAのトラックを見ることができません。

ステップ

1. Master-Slave Tracking Settingsページで、CalibrationとしてMulti-Point Calibrationを選択します。
モード
2. レーダー検知エリアの中心線上の校正点(均等分布)を選択するには、次の図を参照して点を選択します。



図8-21 複数配布インスタンス

注記

少なくとも4点の校正点が必要です。

3. キャリブレーションポイントにより、人Aがキャリブレーションポイントに移動し、ワンポイントキャリブレーションの手順2～手順5を参照してキャリブレーションポイントをキャリブレーションします。
4. 最初の校正点が設定されたら、黄色のトラックが消えた後、次の校正点に移動させます。次に、1点校正の手順2～手順5を参照し、次の校正点を設定します。

この手順に従い、他のすべての校正点を順番に設定します。

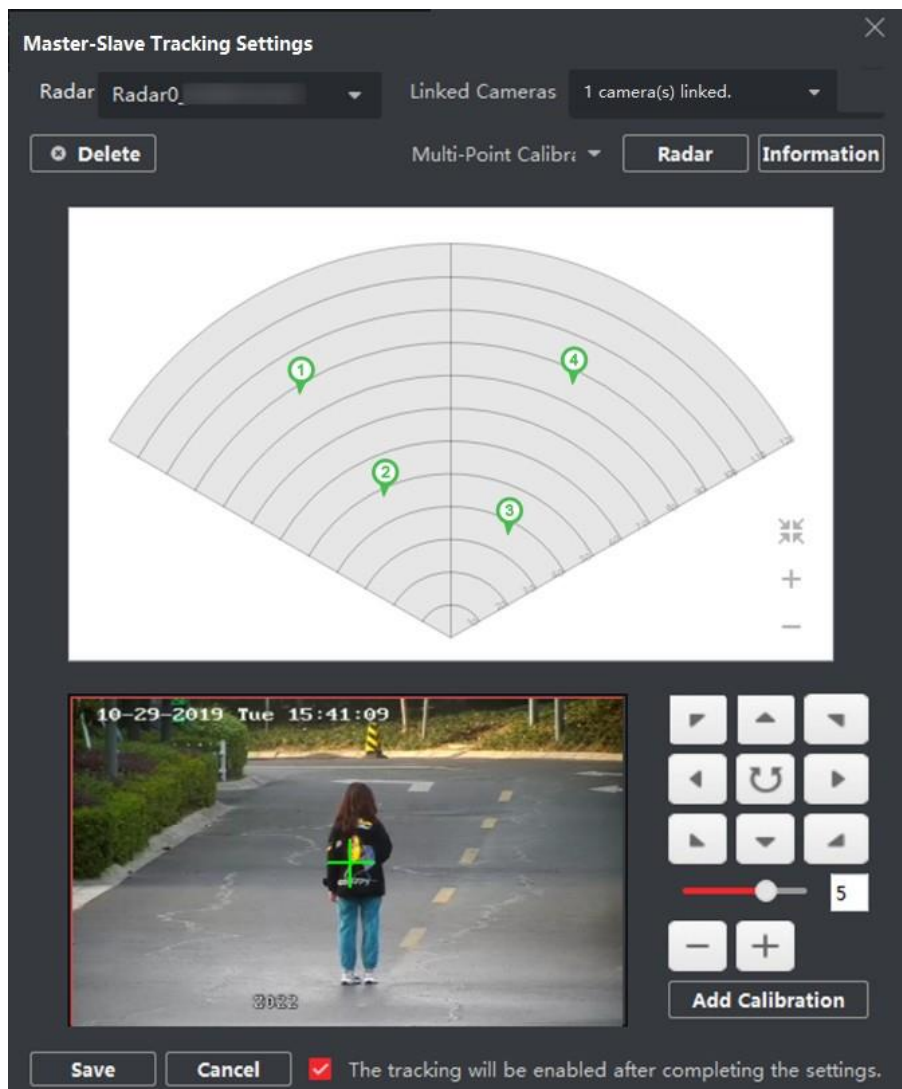


図8-22 マルチキャリブレーションレーダーページ



注記

「情報」で校正点を選択した後、「Delete」をクリックして校正点を削除します。
リスト

5. すべてのキャリブレーションポイントが設定されたら、「保存」をクリックします。



注記

キャリブレーション情報は、4点のキャリブレーションポイントがある場合にのみ正常に保存できます。それ以外の場合は保存できません。

連動カメラの駐車場設定

レーダーパーキングモードを有効にした後、レーダー検知エリアに10秒以内にターゲットが現れない場合、レーダーはリンクされたカメラを設定されたパーキングポイントに戻すように制御します。

開始前に

- レーダーをマップに追加します。
- カメラをレーダーに接続し、クライアントにカメラを追加します。
- カメラを較正し、カメラのマスタースレーブトラッキングを有効にします。
- 操作前にレーダーを解除する必要があります。E-mapページの「完了」をクリックして終了します。
編集モードレーダーアイコンをクリックし、「非表示」を選択してレーダーを非表示にします。

ステップ



注記

本機能は、PTZ制御機能付きカメラにのみ適用されます。

1. マップ右上の「編集」をクリックして、編集モードに入ります。
2. レーダー設定」→「パーキングポイントの設定」をクリックします。
3. 上部のドロップダウンリストからレーダーを選択します。
4. ドロップダウンリストからリンクされたカメラを選択します。
5. 右のボタンでカメラの画面中心位置(クロスアイコン位置)を時計の位置に合わせます。画面をクリックすると、クリックした中心に画面が自動的に調整されます。画像をクリックして、中心をクリックした位置にすることもできます。



カメラの回転速度を1が最も遅く、7が最も速く調整します。

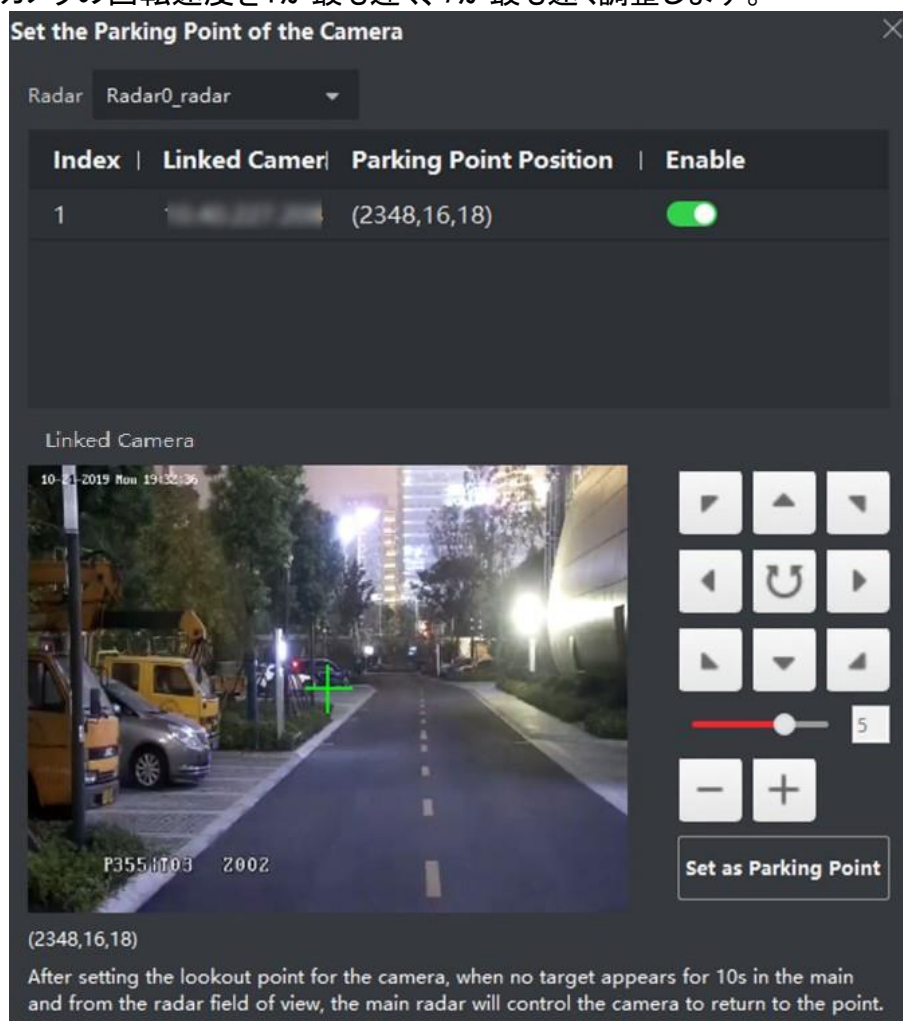


図8-23 駐車場の設置

6. 「パーキングポイントとして設定」をクリックします。

マップキャリブレーション

マップキャリブレーションは、3人の協力でマップの正確なスケールを得るために使用されます。

開始前に

クライアントとマップにレーダーを追加し(デバイスを追加するときは、「グループにインポート」をチェックします)、マップのスケールを設定していることを確認します。

ステップ

1. 「編集」をクリックして編集モードに入ります。

2. [レーダ設定]→[マップキャリブレーション]の順にクリックします。
3. この作業を行うためには、3人の協力が必要である。人Aと人Bがレーダーの検知エリアに入る。Person Cはクライアントによってトラックを選択します。AとBはキャリブレーションポイントで停止し、システムはトラックの末端に2つのマーカーを生成します。
ポップアップウィンドウの「OK」をクリックしてトラックの終端を確認するか、「削除」をクリックして新しいトラックを選択します。

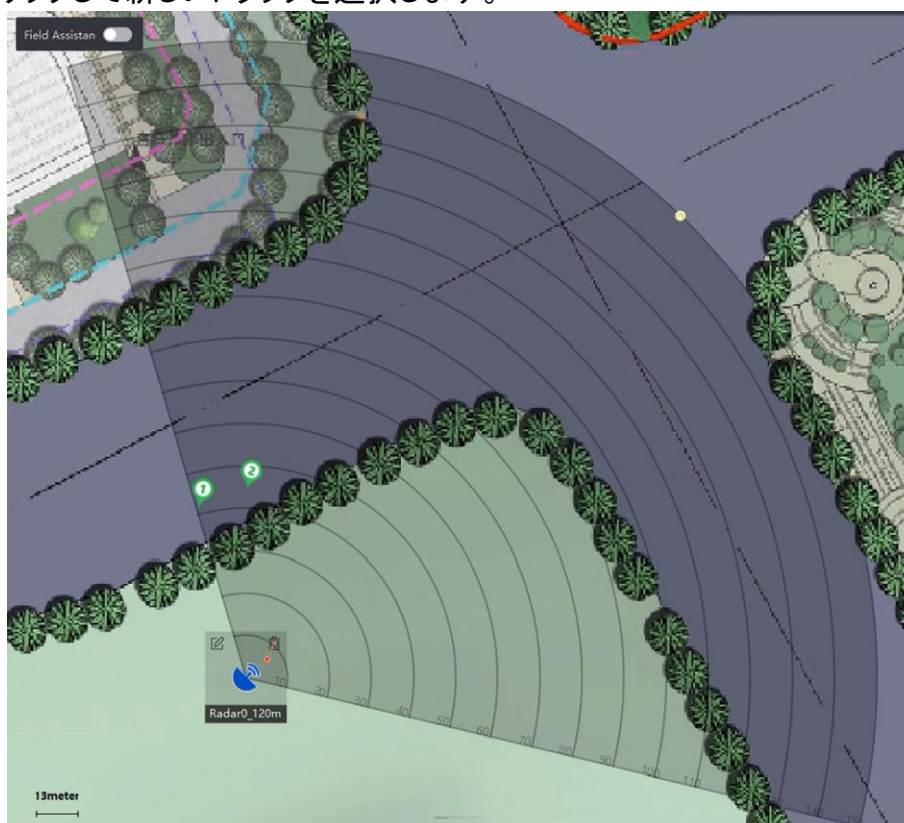


図8-24 端末の確認

4. マップをクリックして、マーカー1とマーカー2の実際の位置を確認します。

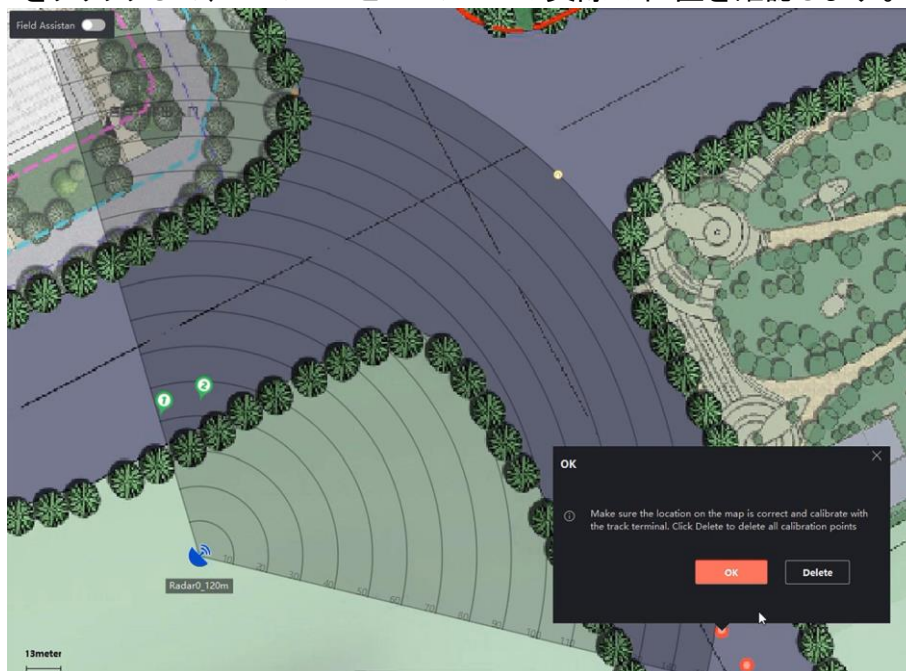


図8-25 実際の場所を確認する

5. ウィンドウがポップアップし、マップ上の位置が正しいことを確認し、トラック端末でキャリブレーションしますか? 「削除」をクリックして、すべての校正点を削除します。ポップアップウィンドウで「OK」をクリックします。システムは、マーカーを実際の位置に自動的にマッチさせます。

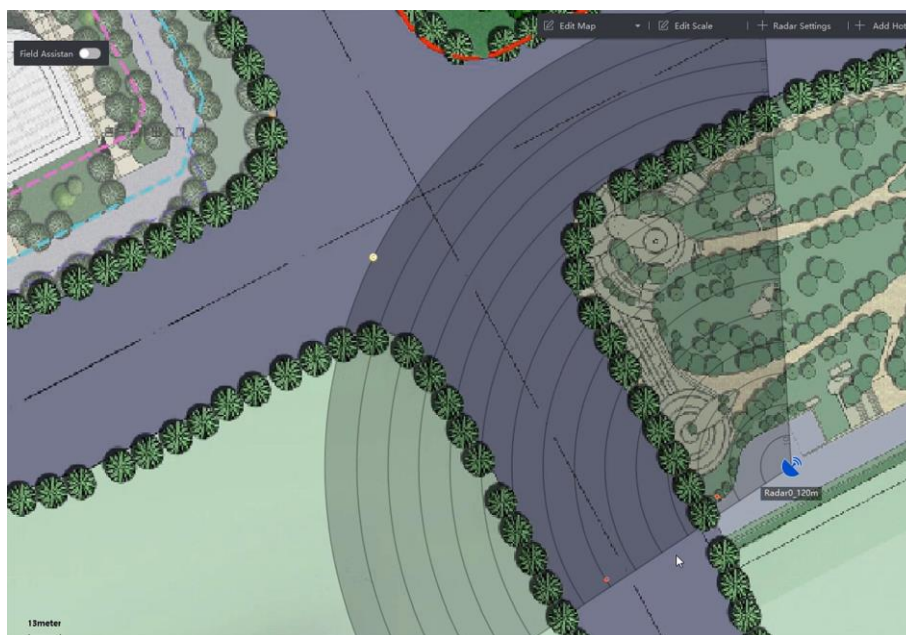


図8-26 マップのキャリブレーションの終了

その他の機能

レーダーを使用するときは、アーミング/解除、レーダーパラメータの更新、OSDおよびPTZカメラのFOV（視野）の表示、アラーム出力などの補助的な機能を実行することができます。



以下の機能を使用する前に、マップ編集モードを終了していることを確認してください。

すべてのレーダーのアーム/非表示

Arm Radar → Arm All Radars / Disarm All Radars をクリックして、マップ上のすべてのレーダーをアームまたは解除します。

単一レーダーのアーム/ディスアーム

編集モードを終了したら、レーダーのアイコンをクリックして、操作メニューを表示します。

レーダーのアーム

レーダーの検知エリアを作動させます。「ゾーン内に標的がある。強制的な武器使用を可能にする」という質問がポップアップで表示されます。警戒区域に標的が存在するときにレーダーをアームすると、「OK」をクリックすると、レーダーを強制的にアーム表示できます。



レーダーは武装していると編集できません。

レーダーの非表示

レーダーの検知エリアを解除します。

イベント

特定のカメラがトリガーしたアラームを、特定の時間帯に検索し、アラーム関連のビデオを表示します。詳細はプレビューホットスポットを参照してください。

アラーム出力を有効にする

警報出力は、レーダーにリンクされたサイレンを指す。アラームやプリアラーム

を有効にすると、アラームが鳴ったり、アラーム音が鳴ったりします。
操作:編集モードに入ったら、「レーダー設定」→「アラーム出力」をクリックします。リレーを選択し、Operation 列のスイッチを入れるか、Enable All をクリックしてリスト内のすべてのリレーを有効にします。☑

OSD の表示

マップ上部の「レーダー設定」→「OSD表示」をクリックすると、検出されたターゲットの移動速度とターゲットとレーダーの距離が表示されます。



図8-27 地図上のOSD

ディスプレイPTZカメラのFOV

マップの上部にある[レーダ設定]→[カメラのFOV]をクリックして、リンクされたPTZカメラのファイルを表示します

マップ上のView(FOV)

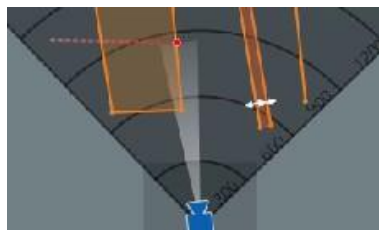


図8-28 PTZカメラの視野

リフレッシュ


「レーダー設定」→「マップ上部の更新」をクリックして、レーダーの最新検出を更新します。

角度、検出距離、トリガライン、およびアーミング状態。

8.3.7 ホットスポットの編集

マップ上に追加されたホットスポットの情報(名前、色、アイコンなど)を編集できます。

ステップ

1. E-mapモジュールを入力する。
2. 右上の「編集」をクリックして、マップ編集モードに入ります。
3. マップ上のホットスポットアイコンを選択し、クリックしてホットスポットの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、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. 他のカメラのホットスポットに適用する/他のアラーム入力ホットスポットに適用する/他のアラーム出力ホットスポットに適用する/他のゾーンホットスポットに適用する/色とアイコンの設定を他のホットスポットに適用する。
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、クリックしてホットスポットを削除します。



8.3.8 プレビューホットスポット

地図にホットスポット(カメラ、アラーム入出力、ゾーン、セキュリティレーダー、ゾーンなど)を追加すると、カメラホットスポットのライブビューと、地図上のすべての種類のホットスポットのトリガーされたアラーム情報を見ることができます。

開始前に

マップにホットスポットを追加したことを確認します。詳細については、ホットスポットの管理を参照してください。

ステップ

1. E-mapモジュールを入力する。




注記

マップ編集モードの場合は、右上隅の Exit をクリックしてマッププレビューモードにします。

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

ホットスポット型  地図に表示される。

3. ホットスポットをクリックして、以下の操作を行います。

**ホットスポットタイプ
オペレーション** ライブビュー:クリックすると、カメラのライブビューウィンドウがポップアップします。📺

カメラ

 注記

- ライブビュー中にアラームが発生すると、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。
 - ライブビュー中に撮影、録音、即時再生ができます。
-

アラーム出力

アラーム出力をクリックし、「開閉」を選択します。

 注記

アラーム出力で管理されているセキュリティ制御チャンネルも開閉します。

アクセスポイント

表示ドアの状態:アイコン上にアクセスポイントの現在のドアの状態が表示されます。アイコンをクリックすると、ドアの状態が切り替わります。

オープンドア

ドアがロックされたら、ロックを解除し、一度開きます。オープン時間が過ぎると、ドアは閉じられ、自動的にロックされます。

ドアを閉じる

ロックが解除されるとロックされ、閉じられます。アクセス権限を持つ人は、資格情報を持ってドアにアクセスすることができます。

オープンのまま

ドアのロックは解除されます(閉じても開いても)。すべての人が、資格証明書を必要とせずにドアにアクセスすることができる。

閉じたまま

扉が閉まり、鍵がかかります。スーパーユーザを除き、認定資格を持っていても、誰もドアにアクセスできない。

**セキュリティ
レーダー**

レーダーのモニタリングフィールドの Arm/Disarm ゾーン:編集終了後、セキュリティレーダーのアイコンをクリックし、Arm/Disarm を選択するか、または Event をクリックして特定の時間帯にトリガされるイベントを検索します。

 注記

- レーダーの検知領域にターゲットがあっても、アームを鳴らすことはできません。
- 警戒区域及び早期警戒区域は、レーダーを装備した後に警戒区域及び早期警戒区域を設定する。この場合、警戒区域及び早期警戒区域に到着したターゲットは、警戒が開始され、警戒が開始された時点でイベントセンターに報告される。

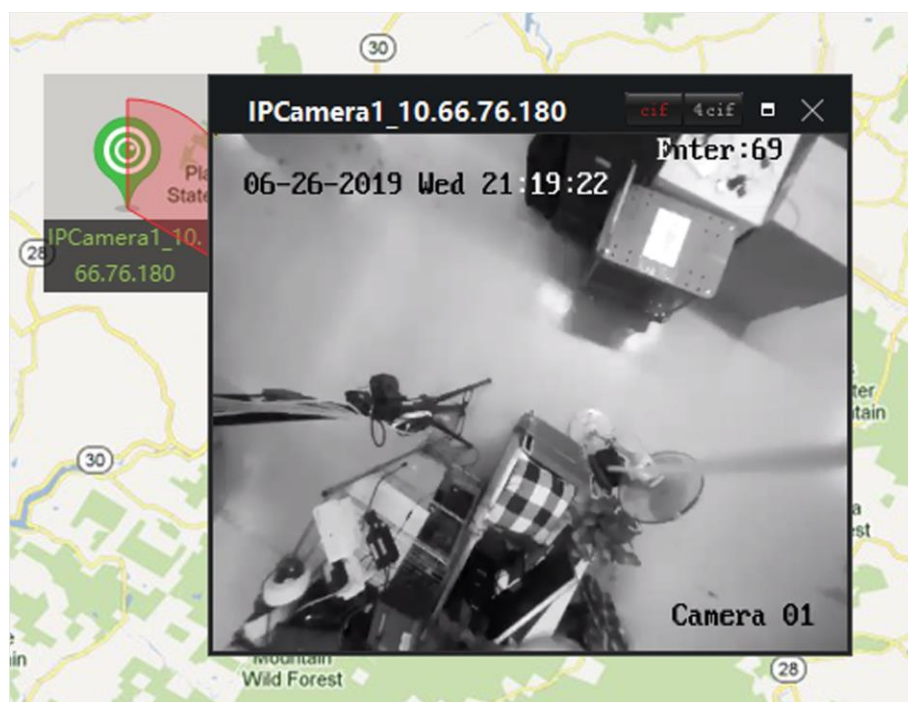


図8-29 地図上のカメラのライブビュー

4. オプション:以下の操作を行います。

- | | |
|---|--|
| アラーム情報
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を開きます。
アラームの種類とトリガー時刻を表示する情報ページ |
| アラームクリア | マップの上部にあるアラームを消去をクリックして、ホットスポットのアラームをすべて読み取り時にマークします。 |
| 複数のカメラの
ライブビューをマップ
に表示する | <ol style="list-style-type: none"> Live View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。 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

最大 4 台のカメラのライブビューが同時にサポートされません。

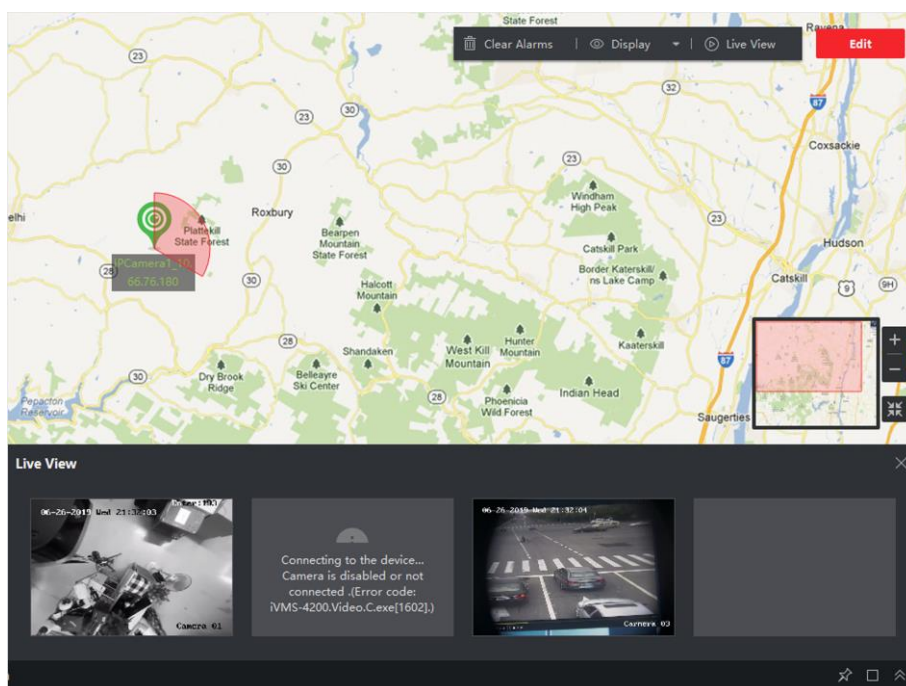


図8-30 プレビューカメラのホットスポット

8.4 ホットリージョンの管理

ホットリージョン関数は、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。追加されたマップは子マップと呼ばれ、ホットリージョンを追加したマップは親マップと呼ばれます。

子マップを親マップにリンクすると、親マップにホットリージョンアイコンが表示されます。これをクリックすると、子マップを入力し、子マップ上のリソースを表示することができます。

ホットリージョン機能により、e-mapを階層構造化し、大きな位置から移動することができます。

床レベルから部屋レベルまでの詳細な視点。

8.4.1 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することができ、追加され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。追加されたマップは子マップと呼ばれ、ホットリージョンを追加したマップは親マップと呼ばれます。

開始前に

少なくとも2つのマップを追加する必要があります。マップの追加の詳細については、「マップの追加」を参照してください。

ステップ



マップは、ホットリージョンとして1回だけ追加できます。

1. E-mapページを入力します。
2. 右上隅の「編集」をクリックしてマップ編集モードに入ります。
3. 親マップとして追加されたマップを選択します。
4. ホット・リージョンの追加をクリックして、ホット・リージョンの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、該当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。

8.4.2 ホットリージョンの編集

親マップ上のホットリージョンの情報(名前、色、アイコンなど)を編集できます。

ステップ

1. E-mapモジュールを入力する。
2. 右上隅の「編集」をクリックしてマップ編集モードに入ります。
3. 親マップ上のホットリージョンアイコンを選択し、クリックしてホットリージョンの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、ホットリージョン名とホットリージョンアイコンを選択します。
5. 「他のホットリージョンに適用」をチェックして、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。

8.4.3 プレビューホットリージョン

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入力できます。子マップ上のリソースとアラームを表示できます。

ステップ

1. E-mapページを入力します。



注記

マップ編集モードの場合は、右上隅の Exit をクリックしてマッププレビューモードにします。

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入力します。
子マップ上のリソースを表示できます。子マップにアラームが発生した場合は、アラームの詳細を表示できます。
3. オプション:左上隅の親マップに戻るをクリックし、親マップに戻ります。
4. オプション:アラーム情報をクリアするには、右上隅にあるアラーム情報クリアをクリックします。
現在のマップ上のリソースによって起動されます。

8.5 人物の移動パターンの表示

顔認識装置を使って、複数のカメラの位置から生成された対象者の移動パターンを地図上で見ることができます。E-mapでは、被疑者や行方不明者など、個人の動きのパターンを地図上で検索・閲覧することで、その人を見つけることができます。

開始前に

グループのマップを追加し、グループ内のカメラをマップに追加したことを確認します。

参照

詳しくは、マップを追加し、カメラをホットスポットとして追加します。

ステップ

1. E-mapモジュールを入力する。
2. 左側の列のリソース・リスト内の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領域に表示されます。

3. オプション:[Add Map]をクリックしてグループのマップを追加し、グループ内のカメラをマップに追加します。
4. マップ上部の「移動パターン」をクリックして、「移動パターンの検索」ページを開きます。
5. クリックすると、動きのあるパターンを検索する期間を設定できます。📅
6. 一覧表の顔画像解析装置を確認する。

 注記

手順7でアップロードした画像は、確認した機器に保存されている画像と比較されます。

-
7. ピクチャの選択をクリックして、ピクチャをピクチャエリにアップロードまたはドラッグする顔ピクチャを選択します。

 注記

複数の顔画像を含む画像をアップロードし、比較のために選択することができます。

-
8. スライダーをドラッグするか、数字を入力して類似性を選択します。

 注記

クライアントは、アップロードされた画像との類似性が、設定された類似性よりも高い、選択された顔画像解析装置に保存された顔画像を検索し、マップ上に一致した人物の移動パターンを表示します。

-
9. 検索をクリックします。

地図上には、アップロードした画像と類似した人物の動きのパターンが表示され、撮影した画像には、人物の到着順序を示す番号が付けられ、撮影した画像のサムネイルも表示されたまま左側にキャプチャレコードが表示されます。

10. オプション: 移動パターンを検索した後、以下の操作を行います。

操作説明

フィルター取り込み

レコード

Show Last Recordをクリックしてチェックすると、各カメラの移動パターンの最後のレコードが表示されます。▼

**人物関連の動画・
映像を見る**

キャプチャした画像サムネイルをクリックして「キャプチャ詳細」ウィンドウを開き、クリックした画像の詳細情報を表示できます。

カメラで撮影した人物の画像がすべて右側に表示されます。キャプチャした画像を選択すると、キャプチャ時間の 5 秒前とキャプチャ時間の 5 秒後を含め、関連するビデオが左側に 10 秒間表示されます。クリックして、ビデオの表示を開始します。🎥

パターンの無効化

レコードリストの最上部をクリックするか、移動を終了するパターンを無効にします。🔴パターンモード

第9章 ストリームメディアサーバーを介したビデオストリームの転送

機器のリモートアクセス番号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にリモートアクセスを行おうとす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、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し、クライアント・インストール・パッケージにパッケージする必要があります。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・サーバーをチェックして、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。

9.1 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実行し、データ・セキュリティを確保する必要があります。

ストリーム・メディア・サーバーにセキュリティ証明書をインポートするには、以下のステップを実行します。

ステップ

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) Exportをクリックします。
2. ストリーム・メディア・サーバーに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・サーバーにインストールされているPCのデスクトップ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) タスクバーを右クリックし、「表示」をクリックします。
 - 2) [Configuration]をクリックして[Configuration]ウィンドウに入ります。
 - 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、手順1でクライアントからエクスポートする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・サーバーを再始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、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。

9.2 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アドレスごとに1つずつ追加することができます。

ステップ

 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

- また、別の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介し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)が他のサービスによって占有されている場合は、ダイアログ・ボックスがポップアップします。ストリーム・メディア・サーバーの適切な動作を保証するために、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、Device Managementページを入力します。
3. デバイスを入力→ストリーム・メディア・サーバー
4. 「追加」をクリックして、「追加」ウィンドウを開きます。
5. 追加モードとしてIP Address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終了します。
- 追加をクリックしてサーバーを追加し、リストページに戻ります。
 - 「追加」および「続行」をクリックして設定を保存し、他のサーバーの追加を続行します。




注記

追加され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。例外メッセージを表示し、付属の手順に従って証明書を一貫性を保つことができます。

9.3 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を介して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。

ステップ

1. デバイス管理モジュールを入力します。
2. デバイスを入力→ストリーム・メディア・サーバー
3. サーバーを選択し、「操作」列をクリックして、「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・サーバーを介してビデオ・ストリームを転送するカメラを選択する。
5. OKをクリックします。
6. 「メインビュー」ページに移動し、カメラのライブビューを再開します。
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・サーバーを通して転送された、またはストリーム・メディア・サーバーから送信されたビデオ・ストリームのチャンネル番号を確認します。

 注記

- 1つのストリームメディアサーバーでは、最大64チャンネルのビデオストリームを転送でき、最大200チャンネルのビデオストリームをクライアントに送信できます。
 - カメラがオフラインの場合でも、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 10 章 統計

一定期間に作成された報告書は必須文書であり、業務が円滑かつ効果的に遂行されているかどうかをチェックするために利用される。このソフトウェアでは、レポートは、毎日、毎週、毎月、毎年、およびカスタム・タイム・ピリオドで作成できます。レポートは、決定の作成、問題への対処、傾向のチェック、比較などの基礎として使用できます。

10.1 人数カウント報告書

集計担当者は、特定のエリア内の回線横断人数と、ある一定期間の回線横断人数をカメラで集計することで、異なる時間に流れる客数や客数を分析することができ、報告書に応じて柔軟に事業調整を行うことができる。統計を数える人は、折れ線グラフまたはヒストグラムで表示し、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。

開始前に

人数計数装置をソフトウェアに追加し、対応するエリアを適切に設定します。追加されたデバイスは、人数カウントルールで設定されている必要があります。人数カウントデバイスの追加の詳細については、「[デバイスの追加](#)」を参照してください。

ステップ

1. [レポート] → [人数カウント] をクリックして [人数カウント] ページに進みます。
2. レポートの種類として、日報、週報、月報、年報を選択します。

日報

Daily Reportには、日単位のデータが表示されます。システムは、1日の各時間の人数を計算します。

週報、月報、年報

日報に比べて、週報、月報、年報は、毎日提出しないので、時間がかからない。1週間の各日、1ヶ月の各日、1年の各月の人数を計算します。

カスタムレポート

ユーザーは、レポート内の日数をカスタマイズして、カスタマイズした時間間隔の各日または月の人数を分析できます。



注記

カレンダーでは31日を超えない範囲で選択できます。

3. 統計時刻の種類を選択し、をクリックして時刻を設定します。

一時期

1期間で統計値を生成します。

複数期間

2つの期間で統計を作成すると、人の流れを比較するのに役立ちます。

そして、2つの期間に数字を出す。

たとえば、レポートの種類を月のレポートに設定し、3月と4月を統計時刻に設定した場合、3月と4月の結果をカウントしている人は、異なる色の同じチャートで表示され、月の異なる日のデータを比較できます。

4. デバイス別表示、カメラ別表示を選択します。

デバイス別表示

デバイス別のレポートを表示します。

たとえば、1つのNVR (4人がカメラをカウントしている)を選択すると、4人がカメラをカウントしている合計人数が表示されます。

カメラ別表示

レポートをカメラで表示します。

たとえば、1つのNVRを選択した場合(4人がカメラをカウントしている場合)、レポートには各カメラの統計値がそれぞれ表示されます。つまり、統計値は4/8色で表示されず(各/2色は1つのカメラを表します)。

5. 表示するカメラをカウントする人を選択します。
6. 表示する内容を設定します。

方向

入場者、退場者、入退場者など、異なる方向の人数を算出する。

入力済み

入力された人数がカウントされます。

終了

撤退した人数がカウントされます。

合格

開業・廃業ともカウントされる。

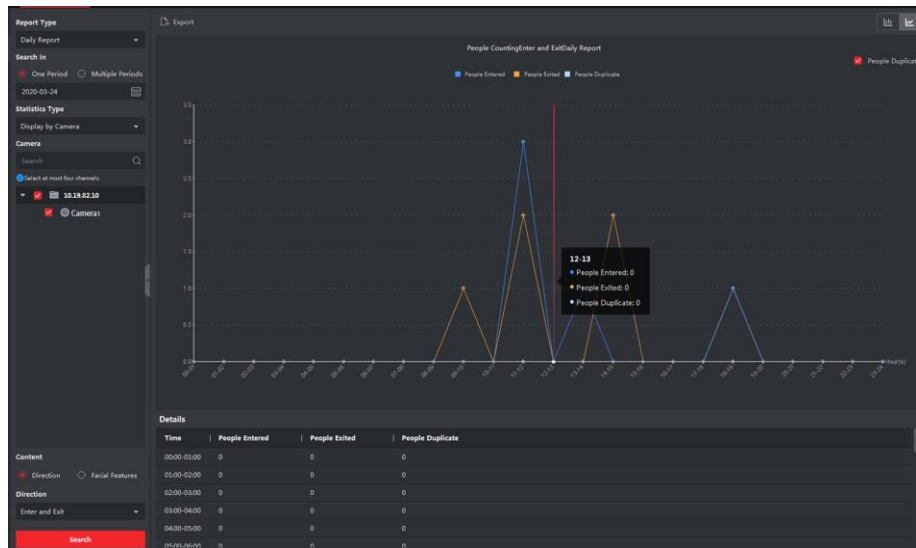


図10-1 人員の方向別カウント

顔の特徴

Gender、Age Group、Age Group などの顔の特徴に基づいてレポートを生成します。

たとえば、[Age Group] をフェイシャルフィーチャとして選択すると、クライアントは異なる年齢グループの人数を計算します。

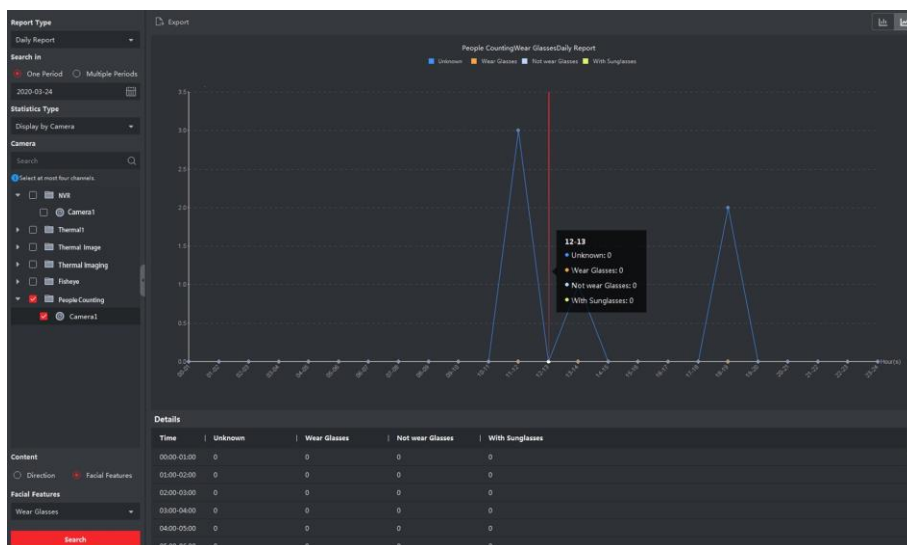


図10-2 人の顔の特徴別カウント

7. Children Children Only、認知された子供のレポートを生成するためにのみチェック。

 注記


- クライアントは、デバイスのリモート設定ページで設定可能な事前定義された高さよりも短い検出された人数をカウントします。高さしきい値の設定の詳細については、装置のユーザーズマニュアルを参照してください。
 - この機能はデバイスでサポートされている必要があります。
-

8. 「検索」をクリックして、時間、日、または月ごとにカウントしている統計値と詳細データを取得します。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:方向別レポートの場合、レポートページの右上隅にある[重複している人]をチェックして、重複している人の数を表示できます。

 注記

重複人数は、装置によって計算されます。同じ顔が複数回認識された場合は、重複者として計算されます。
例えば、出納係が2回以上スーパーマーケットに出入りした場合、重複者として計算される。このようにして、スーパーマーケットは実際に買い物をする人の数を把握することができる。


- 10.オプション:検索後、以下の操作を行います。

折れ線グラフに切り替える クリックすると折れ線グラフに切り替わります。 

 注記

デフォルトでは、統計値は棒グラフで表示されます。

棒グラフへの変更

クリックすると棒グラフに切り替わります。 

ローカルPCに保存

「エクスポート」をクリックして、パソコンにカウントしている人の詳細データを保存します。

10.2 交差点でカウントしている人の表示レポート

交差点解析は、交差点のようなシーンにおける人の流れと数を監視するために使用される。画像中の矢印は、異なる方向を示します。入口として一方の方向(例えばA)を選択することにより、デフォルトでは他方の方向が出口として設定され、複数のパス(例えばA~A、A~B、A~C、A~D)が生成されます。それぞれの道を通じた人を数えて見ることができ、店主が異なるドアで人の流れを分析するのに役立ちます。統計結果は、日次、週次、月次、年次レポートに表示できます。

開始前に

交差点解析機能に対応した魚眼カメラが設定されていることを確認します。ソフトウェアに適切に追加する。デバイスの追加の詳細については、「[デバイスの追加](#)」を参照してください。

ステップ



注記

最大10個の交差点を解析できます。

1. [Report]→[Intersection Analysis]をクリックして、交差解析モジュールを入力します。
2. レポートの種類として、日報、週報、月報、年報を選択します。

日報

Daily Reportには、日単位のデータが表示されます。システムは、入居者数を計算します。1日1時間ごとに交差点が報告されます。

週報、月報、年報

日報に比べて、週報、月報、年報は、毎日提出しないので、時間がかからない。システムは、1週間の各日、1ヶ月の各日、1年の各月の交差点レポートの人数を計算します。

3. レポートの開始時刻を設定します。
4. レポートを作成するカメラを選択します。
5. Flow in fieldのドロップダウンリストから、1つの方向をエントリーとして選択します。

6. [検索]をクリックして、統計結果を取得します。

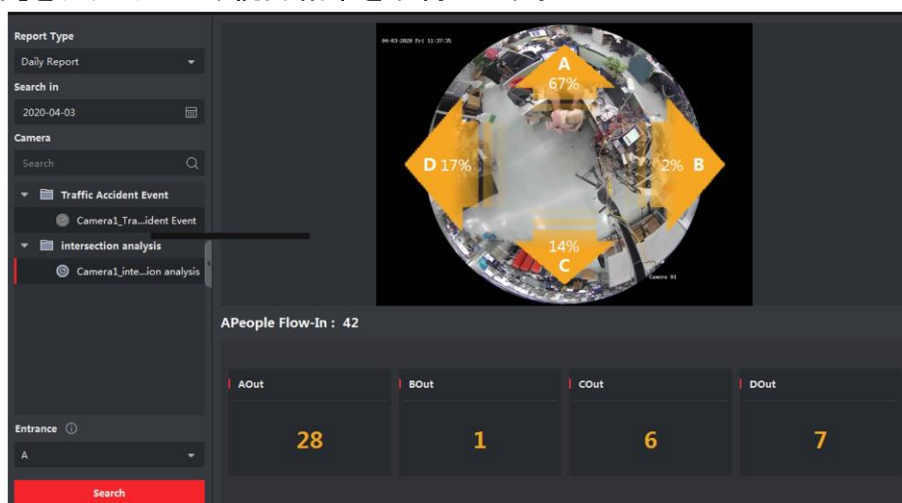


図10-3 結果

各パスの人数が右側に表示されます。

10.3 キュー管理

キュー管理は、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ます。一般的に用いられるデータ分析

- キュー/リージョン内の特定の待ち時間レベルのキューイングアップ人数を確認するには、キューイングアップ時間分析を使用し、対象領域を確認し、待ち時間レベルを設定します。
- 複数のキュー/領域における特定の待ち時間レベルのキューイングアップ人数を比較するには、キューイングアップ時間解析を使用し、対象領域をチェックし、待ち時間レベルを設定する。
- 複数のキュー/領域における異なる待ち時間レベルのキューイングアップ人数を比較するには、キューイングアップ時間分析を使用し、対象領域をチェックし、待ち時間レベルを設定する。
- キューがキュー/領域にある長さのままでいる時間と継続時間を確認するには、キュー・ステータス分析を使用し、ターゲット・リージョンをチェックして、キューの長さレベルを設定します。
- キューが複数のキュー/領域にある長さのままでいる時間と継続時間を比較するには、キューのステータス分析を使用し、対象領域をチェックし、キューの長さレベルを設定します。
- 複数のキュー/領域でキューが異なる長さで継続する時間と継続時間を比較するには、キューのステータス分析を使用し、ターゲット領域をチェックし、キューの長さレベルを設定します。

10.3.1 キューイングアップ時間解析

Queuing-Up Time Analysisは、異なる待機時間レベルの人数を計算します。地域比較、多重待ち時間レベルの比較がサポートされる。

異なる領域のキューイング・ピープルの比較

キューイング・ピープル・アカウント・カメラでは、地域ごとに一定期間のキューイング・ピープル・アカウントを検索することができ、顧客が行きやすい場所を見つけるのに役立ちます。例えば、人数の多い地域の方が少ない地域よりも人気が高いため、これらの地域に商品を投入してより多くの商品を販売することができます。

開始前に

- ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。デバイスの追加の詳細については、「デバイスの追加」を参照してください。
- デバイスリモート設定ページのカメラの検出領域に、3つ以下の領域を設定していることを確認します。リージョンの設定の詳細については、装置のユーザーマニュアルを参照してください。

ステップ

注記

この機能は、接続されている機器がサポートしている必要があります。

1. [Report]→[Queue Management]→[People Amount in Region]の順にクリックします。
2. レポートの種類として、「日報」「週報」「月報」「カスタムレポート」を選択します。

日報

Daily Reportには、日単位のデータが表示されます。システムは待ち行列の継続時間を計算します。1日1時間ごとに、地域ごとに。

週報、月報

日報に比べて、週報や月報は、毎日提出しないため、時間が少なくて済む。システムは、1週間の各日、1カ月の各日における、異なる地域のキューイング・アップ・デューレーションを計算する。

カスタムレポート

ユーザーは、レポート内の日数をカスタマイズして、カスタマイズした時間間隔の各日または月の人数を分析できます。

注記

カレンダーでは31日を超えない範囲で選択できます。

3. クリックすると、検索期間を設定できます。📅
4. [Region]リストでは、カメラを選択し、[Region]リストのカメラごとに3つ以下の領域を選択します。
5. 統計の種類として地域比較を選択します。
6. レポートの生成に基づいて、待機時間の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。

指定された待ち時間の人数計算値の折れ線グラフが結果エリアに表示されます。色の異なる線は、選択した地域の人を示します。

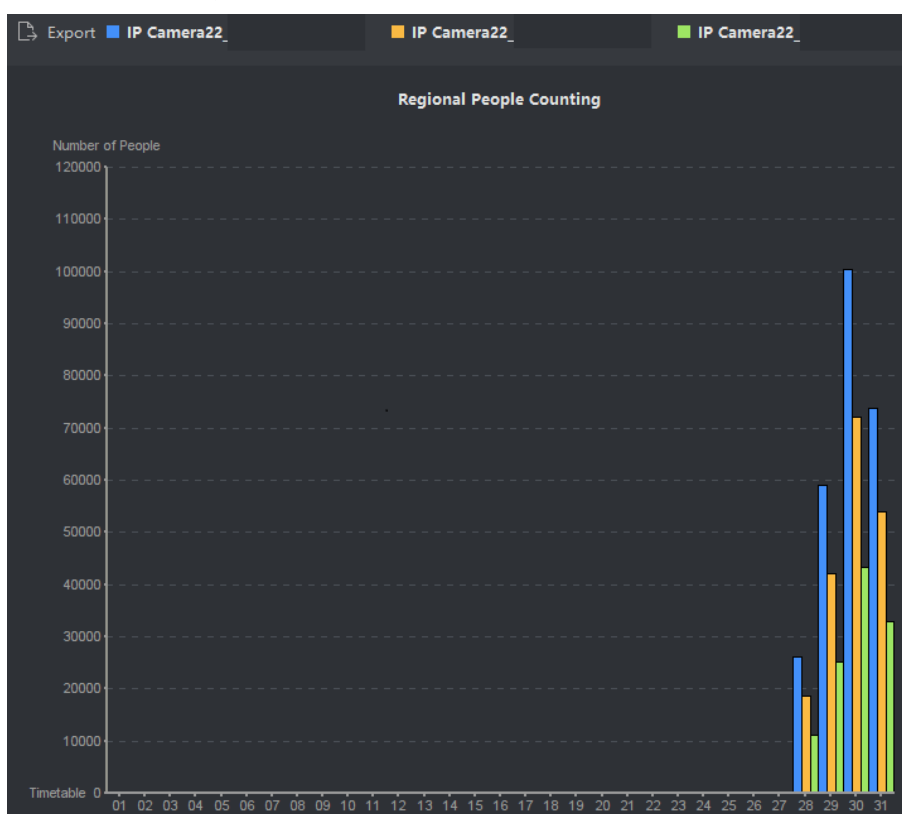


図10-4 結果

8. オプション:[Export]をクリックして、Excelファイル内のデータをエクスポートします。

異なる待ち時間レベルでのキューイング・ピープルの比較

また、キューイング人数カウント用カメラでは、ある地域の長さの異なる時間帯にキューイング人数を検索することができ、地域ごとの混雑感を分析することで、いつ、どのようにサービス窓口数、人員数、人員案内などを変更するかが分かりやすくなります。

開始前に

- ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。デバイスの

追加の詳細については、「**デバイスの追加**」を参照してください。

- デバイスリモート設定ページのカメラの検出領域に、3つ以下の領域を設定していることを確認します。リージョンの設定の詳細については、装置のユーザーマニュアルを参照してください。

ステップ



注記

この機能は、接続されている機器がサポートしている必要があります。

1. [レポート] → [キューの管理] → [リージョナル・ピープル・カウント] をクリックします。
2. レポートの種類として、「日報」「週報」「月報」「カスタムレポート」を選択します。

日報

Daily Reportには、日単位のデータが表示されます。システムは待ち行列の継続時間を計算します。1日1時間ごとに、地域ごとに。

週報、月報

日報に比べて、週報や月報は、毎日提出しないため、時間が少なくて済む。システムは、1週間の各日、1カ月の各日における、異なる地域のキューイング・アップ・デューレーションを計算する。

カスタムレポート

ユーザーは、レポート内の日数をカスタマイズして、カスタマイズした時間間隔の各日または月の人数を分析できます。



注記

カレンダーでは31日を超えない範囲で選択できます。

3. クリックすると、検索期間を設定できます。📅
4. [Region]リストからカメラを選択し、3つ以下の領域を選択します。
5. 統計値の種類として、Multi-level Comparisonを選択します。
6. 待ち時間のレベルを選択し、指定した期間待ちの人数を計算するための秒数を入力します。
7. [検索]をクリックして、統計結果を生成します。

同じ地域の人数計算値の折れ線グラフが結果エリアに表示されます。色の異なる行は、待機時間のレベルに一致します。

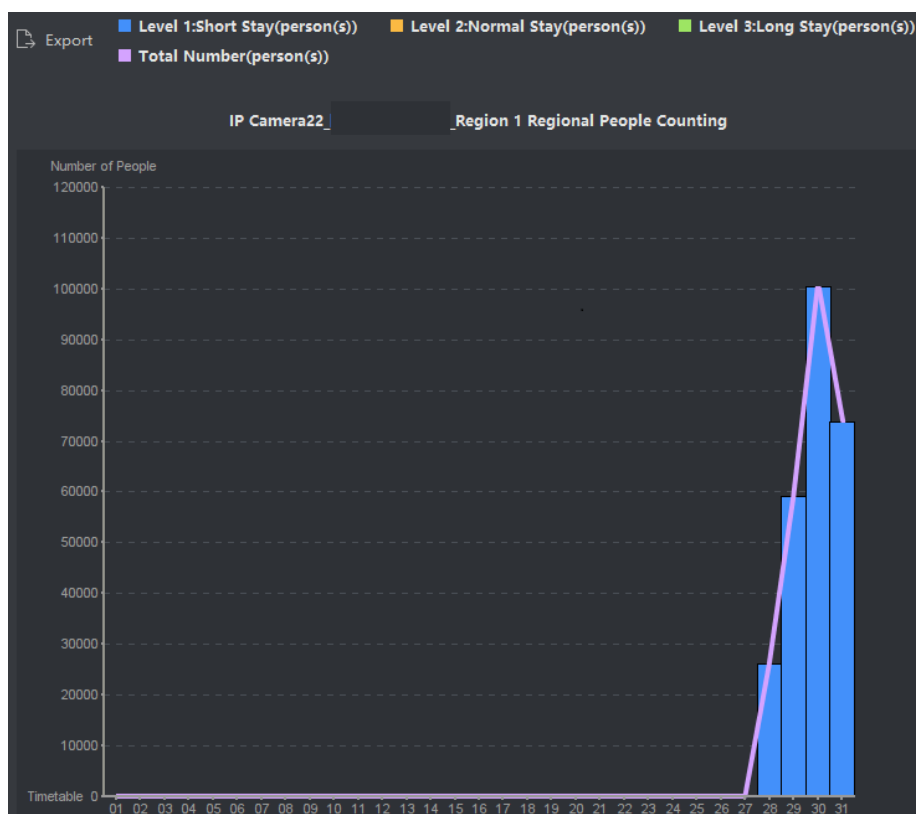


図10-5 結果

8. オプション:[Export]をクリックして、Excelファイル内のデータをエクスポートします。

10.3.2 キューステータス分析

キュー・ステータス分析は、キューが一定の長さで保持される時間と継続時間を計算します。地域比較と多重キュー長レベル比較がサポートされる

異なるリージョンのキューイング期間の比較

また、キューイング・アップ・デューレーション・カウント用のカメラでは、同期間内の各地域のキューイング・アップ・デューレーションを検索・比較することができ、各地域の混雑感を分析することで、いつ、どのようにサービス・ウィンドウ量、スタッフ数、人を案内するかなどを簡単に知ることができます。

開始前に

- ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。デバイスの追加の詳細については、「デバイスの追加」を参照してください。
- デバイスリモート設定ページのカメラの検出領域に、3つ以下の領域を設定している

ことを確認します。リージョンの設定の詳細については、装置のユーザーマニュアルを参照してください。

ステップ



注記

この機能は、接続されている機器がサポートしている必要があります。

1. [レポート] → [キューの管理] → [待ち時間] をクリックします。
2. レポートの種類として、「日報」「週報」「月報」「カスタムレポート」を選択します。

日報

Daily Reportには、日単位のデータが表示されます。システムは待ち行列の継続時間を計算します。1日1時間ごとに、地域ごとに。

週報、月報

日報に比べて、週報や月報は、毎日提出しないため、時間が少なくて済む。システムは、1週間の各日、1カ月の各日における、異なる地域のキューイング・アップ・デューレーションを計算する。

カスタムレポート

ユーザーは、レポート内の日数をカスタマイズして、カスタマイズした時間間隔の各日または月のキューイング継続時間を分析できます。



注記

カレンダーでは31日を超えない範囲で選択できます。

3. クリックすると、検索期間を設定できます。📅
4. [Region]リストでは、カメラを選択し、[Region]リストのカメラごとに3つ以下の領域を選択します。
5. 統計の種類として地域比較を選択します。
6. レポートの生成元となるキューの長さを設定します。
7. [検索]をクリックして、統計結果を生成します。

指定したキューの長さを保つために計算された継続時間の折れ線グラフが結果エリアに表示されます。色の異なる線は、選択した領域に一致します。

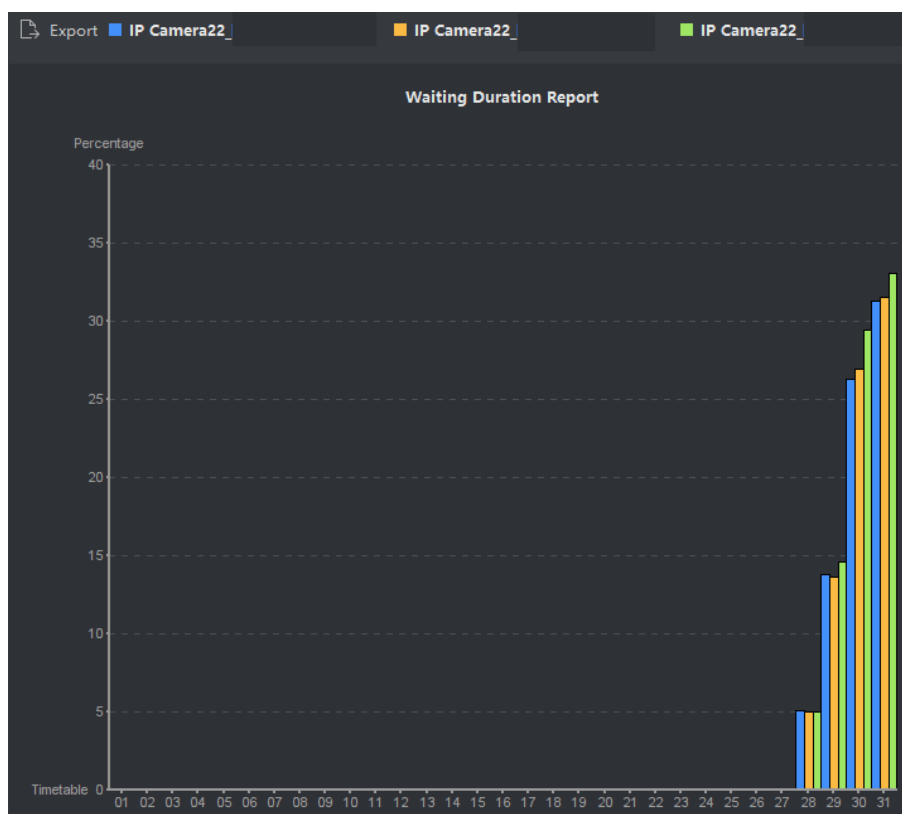


図10-6 結果

- オプション:[Export]をクリックして、Excelファイル内のデータをエクスポートします。

異なるキュー長レベルのキューイング・デュレーションの比較

キューイング・デュレーション・カウント用のカメラでは、同じ時間帯に長さの異なるキューのキューイング・デュレーションを検索・比較することができ、サービス・ウィンドウ量、スタッフ数、ガイドー設定の有無などをいつ、どのように変更するかがわかりやすいように、地域ごとの混雑感を分析することができます。

開始前に

ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。デバイスの追加の詳細については、「デバイスの追加」を参照

ステップ



注記

この機能は、接続されている機器がサポートしている必要があります。

- [レポート] → [キューの管理] → [待ち時間] をクリックします。

2. レポートの種類として、「日報」「週報」「月報」「カスタムレポート」を選択します。

日報

Daily Reportには、日単位のデータが表示されます。システムは待ち行列の継続時間を計算します。1日1時間ごとに、地域ごとに。

週報、月報

日報に比べて、週報や月報は、毎日提出しないため、時間が少なくて済む。システムは、1週間の各日、1カ月の各日における、異なる地域のキューイング・アップ・デュレーションを計算する。

カスタムレポート

ユーザーは、レポート内の日数をカスタマイズして、カスタマイズした時間間隔の各日または月のキューイング継続時間を分析できます。



注記

カレンダーでは31日を超えない範囲で選択できます。


3. クリックすると、検索期間を設定できます。 
4. [Region]リストからカメラを選択し、3つ以下の領域を選択します。
5. 統計値の種類として、Multi-level Comparisonを選択します。
6. レポートの生成元となるキューの長さを設定します。
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継続時間の折れ線グラフが結果領域に表示されます。色の異なる行は、キューの長さのレベルに一致します。



図10-7 結果

8. オプション:[Export]をクリックして、Excelファイル内のデータをエクスポートします。

10.4 ヒートマップレポート

ヒートマップは、データを色で表したグラフであり、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って、設定したエリア内の客の訪問時間や滞留時間を分析することができ、店主が客の関心エリアを分析し、商品の配置を行うのに役立ちます。

開始前に

ソフトウェアにヒートマップネットワークカメラを追加し、該当するエリアを適切に設定します。追加したカメラには、ヒートマップルールを設定する必要があります。ヒートマップネットワークカメラの追加の詳細については、「デバイスの追加」を参照してください。

ステップ

1. [レポート]→[ヒートマップ]をクリックして、ヒートマップページを入力します。

2. レポートの種類として「日報」「週報」「月報」「年報」「カスタムレポート」を選択します。

日報

Daily Reportには、日単位のデータが表示されます。システムは、1日の各時間におけるヒートマップのデータを計算する。

週報、月報、年報

日報に比べて、週報、月報、年報は、毎日提出しないので、時間がかからない。システムは、1週間の各日、1ヶ月の各日、1年の各月のヒートマップのデータを計算します。

カスタムレポート

レポート内の日付をカスタマイズして、カスタマイズした時間間隔の各日または月の滞留時間またはクラウドトレンドを分析できます。



注記

カスタム・レポートの期間は、31日以内とします。

3. 統計の種類として、[Dwell Time]または[Crowd Trend]を選択します。

Dwell時間別

ヒートマップ値(折れ線グラフの縦座標値、写真の色)を住民の滞留時間に応じて計算します。

群集動向別

検出された人数に応じてヒートマップ値(折れ線グラフの縦座標値、画像の色)を算出します。

4. 検索する時間を設定します。
5. カメラ一覧からヒートマップカメラを選択します。

6. [Generate Heat Map]をクリックしてカメラのヒートマップを表示します。

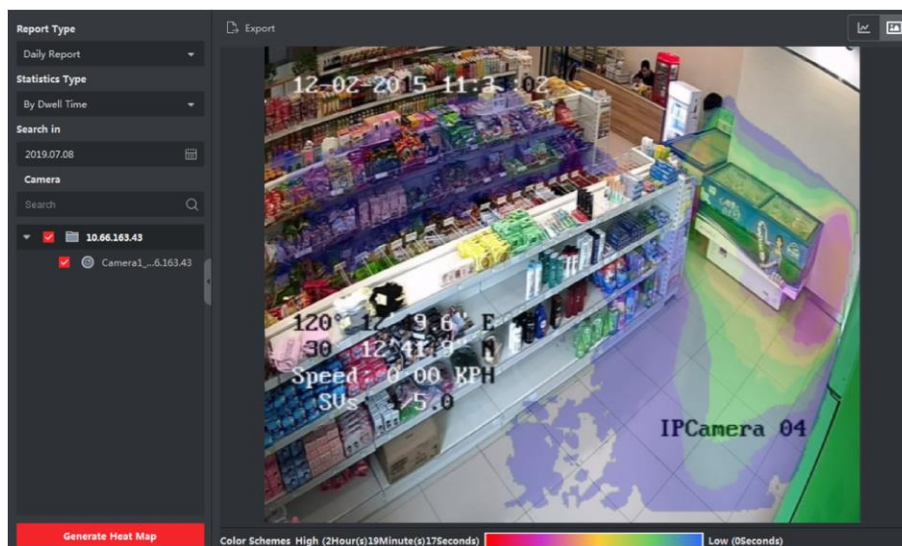



図10-8 結果

7. オプション:ヒートマップレポートの生成後、以下の操作を実行できます。

折れ線グラフの表示 クリックすると、統計が折れ線グラフに表示されます。 

ピクチャーモード中の画面 クリックするとピクチャーモードの統計が表示されます。



赤色ブロック(255, 0, 0)は最もウェルカムなエリアを示し、青色ブロック(0, 0, 255)は人気の低いエリアを示します。

統計データの保存 「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パソコンに保存します。

10.5 皮膚表面温度統計の報告

このシステムでは、総人数、皮膚表面温度が異常な人数、マスクを着用していない人数を算出することができます。このシステムは、皮膚表面温度が異常な人の数とマスクを着用していない人の数の傾向を判断するのに役立つ、1日当たり、1週間当たり、1カ月当たりの統計レポートを提供します。

開始前に

顔の皮膚温度測定機能を備えたインテリジェントデバイスなど、皮膚温測定をサポートするデバイスを追加する。

ステップ

1. 「レポート」→「皮膚表面温度」を選択します。
2. Daily Report、Weekly Report、Monthly Report、Annual Reportなどのドロップダウンリストからレポートの種類を選択します。
3. クリックして、時間範囲を選択します。📅
4. カメラ、デバイス、グループを選択します。
5. 検索をクリックします。
レポートを右側のヒストグラムで表示します。



注記

All, Abnormal, No Mask and Normal Skin-Surface Temperature がレポートの上部に表示され、表示する検出属性を選択できます。

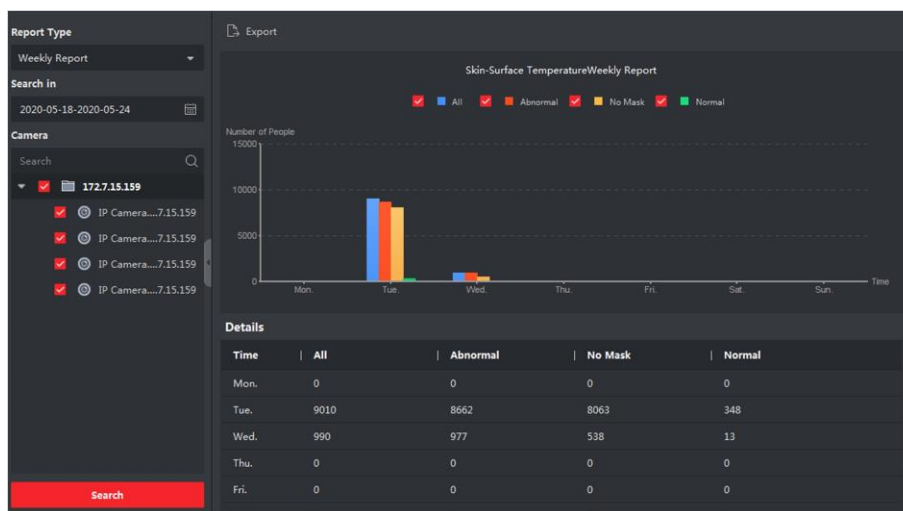


図10-9 皮膚表面温度統計の報告

6. オプション:CSV形式でデータをローカルに保存するには、エクスポートをクリックします。

第 11 章 データ検索

Data Retrievalモジュールでは、顔認識カメラで撮影した顔画像を検索したり、DeepinMind装置で撮影した人体画像を検索したり、行動分析関連の画像やビデオを閲覧したり、DeepinMind装置で撮影した車両画像を検索したり、DeepinMind装置で撮影した頻繁に表示される人物画像を検索したり、ハードハットを装着していない人物画像を検索したりすることができます。

11.1 顔画像検索

接続した機器(NVR、HDVRなど)が顔検索に対応している場合は、関連する画像を検索して、画像関連の動画ファイルを再生できます。

11.1.1 アップロードした画像で顔を検索する

パソコンから顔画像をアップロードし、取り込んだ顔画像と比較することができます。

開始前に


ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。デバイスの追加の詳細については、「デバイスの追加」を参照してください。

ステップ



注記

この機能は、接続されている機器が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、顔画像検索ページに入ります。
2. クリックすると、撮影した顔画像や動画の検索開始時刻、終了時刻が設定されます。
ファイル
3. カメラパネルでデバイスを選択します。
4. ピクチャで検索するには、ドロップダウンリストからピクチャを選択します。
5. 検索する顔画像を選択します。
 - 1) 「ピクチャの選択」をクリックして、パソコンから写真をアップロードします。
 - 2) キャプチャした顔画像とマッチさせるには、アップロードした画像から検出した顔

を選択します。

注記

- 画像の解像度は4096 × 4080より小さくならない。
- JPG形式とJPEG形式のみ対応しています。

6. 類似性レベルを設定します。

例

類似度を40に設定すると、取り込んだ画像とアップロードした顔画像の類似度が40%以上になります。

7. 最大表示件数を設定します。
8. 「検索」をクリックして検索を開始します。
画像の検索結果が右側に表示されます。
9. 画像をエクスポートし、パソコンに保存します。

エクスポートピクチャ

エクスポートする画像を選択し、ローカルパソコンに保存します。

Export Currentページ

現在のページのすべての画像をエクスポートします。

輸出セグメント

パッケージごとに画像をダウンロードできます。1つのパッケージには、1,000枚までの画像が含まれています。

10. 検索した顔画像を選択すると、撮影した顔画像と人物情報が表示されます。











図11-1 結果


11. オプション検索後、次の操作を1つ以上実行できます。

詳細の表示

キャプチャした顔画像、およびページ上の人物情報(類似性、性別、温度状態、キャプチャした時間など)を表示します。

	<p>また、をクリックして大きい画像を表示し、クリックして復元することもできます。</p>
<p>関連ビデオの再生</p>	<p>右下のビューウィンドウで、画像の関連ビデオファイル(キャプチャの5秒前と5秒後)を再生するには、をクリックします。</p> <hr/> <p>注記</p> <ul style="list-style-type: none"> • クリックできます 大きなビデオを表示し、クリックして復元します。 • クリックできます 再生速度を調整するには、クリックしてビデオファイルをフレーム単位で再生し、クリックしてオーディオを有効にし、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します。 • クリックすると、撮影した画像を見ることができます。
<p>画像をパソコンに保存</p>	<p>必要に応じて写真をクリックして選択し、ローカルPCにエクスポートします。クリックすると、撮影した画像が顔画像ライブラリに追加されます。</p>
<p>顔画像ライブラリに画像を追加する</p>	<hr/> <p>注記</p> <p>キャプチャした人物、携帯電話、性別などの画像に対して顔画像ライブラリを選択し、人物情報を入力します。</p> <hr/>

12. オプション:検索結果に基づいて2次検索を実行します。

1)「個人情報」ページで、をクリックします。

このピクチャのすべての顔が分析され、表示されます。

2)ポップアップウィンドウで赤枠を動かして、2次検索を行う顔を選択します。

ピクチャに複数の面がある場合は、選択のためのウィンドウが表示されます。

注記

ピクチャ内に顔が1つしかない場合は、この手順を省略します。

3)OKをクリックします。

お客様は、選択した顔画像に基づいて、撮影した画像の顔を検索し、比較します。

11.1.2 イベント・タイプによる顔の検索

さまざまな種類のイベントをフィルタリングすることで、撮影した顔画像を検索できます。

開始前に


ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。デバイスの追加の詳細については、「デバイスの追加」を参照してください。

ステップ



注記

この機能は、接続されている機器がサポートしている必要があります。

1. 「データ検索」→「顔検索」をクリックして、顔画像検索ページに入ります。
2.  クリックすると、撮影した顔画像や動画の検索開始時刻、終了時刻が設定されます。
ファイル
3. カメラパネルでデバイスを選択します。
4. イベント・タイプ別に検索するには、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。
5. イベントの種類を選択します。

制限なし

撮影した顔画像をすべて検索します。

マッチドフェイス

顔ライブラリの顔とマッチした顔で撮影した画像を検索します。

顔の不一致

顔ライブラリ内の顔と一致しない顔を、撮影した画像から検索します。

迷路検知警報

他人検知アラームが発生したときに撮影した画像を検索します。

6. 最大表示件数を設定します。
7. 「検索」をクリックして検索を開始します。

画像の検索結果が右側に表示されます。

8. 画像をエクスポートし、パソコンに保存します。

エクスポートピクチャ

エクスポートする画像を選択し、ローカルパソコンに保存します。

Export Currentページ

現在のページのすべての画像をエクスポートします。

輸出セグメント

パッケージごとに画像をダウンロードできます。1つのパッケージには、1,000枚までの画像が含まれています。

9. 検索した顔画像を選択すると、撮影した顔画像と人物情報が表示されます。

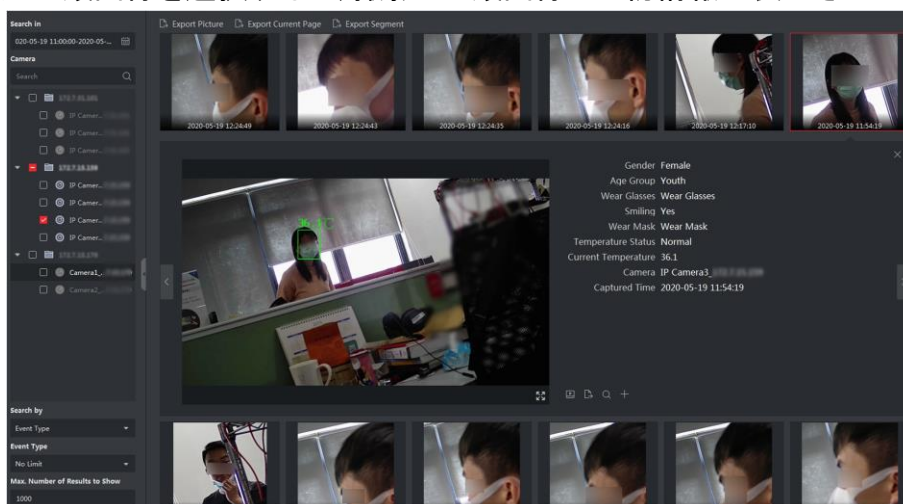










図11-2 結果

10. オプション:検索後、次の操作を1つ以上実行できます。

<p>詳細の表示</p>	<p>キャプチャした顔画像、およびページ上の人物情報(類似性、性別、温度状態、キャプチャした時間など)を表示します。 また、クリックして大きい画像を表示し、クリックして復元することもできます。 </p>
<p>関連ビデオの再生</p>	<p>右下のビューウィンドウで、画像の関連ビデオファイル(キャプチャの5秒前と5秒後)を再生するには、クリックします。  </p> <hr/> <p> 注記</p> <ul style="list-style-type: none"> • クリックできます 大きなビデオを表示し、クリックして復元します。  • クリックできます 再生速度を調整するには、クリックしてビデオファイルをフレーム単位で再生し、クリックしてオーディオを有効にし、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します。  • クリックすると、撮影した画像を見ることができます。 
<p>画像をパソコンに保存</p>	<p>必要に応じて写真をクリックして選択し、ローカルPCにエクスポートします。クリックすると、撮影した画像が顔画像ライブラリに追加されます。 </p>

顔画像ライブラリに画像を追加する



注記

キャプチャした人物、携帯電話、性別などの画像に対して顔画像ライブラリを選択し、人物情報を入力します。

11. オプション:検索結果に基づいて2次検索を実行します。

1)「個人情報」ページで、をクリックします。🔍

このピクチャのすべての顔が分析され、表示されます。

2)ポップアップウィンドウで赤枠を動かして、2次検索を行う顔を選択します。



注記

ピクチャに複数の面がある場合は、選択のためのウィンドウが表示されます。ピクチャ内に顔が1つしかない場合は、この手順を省略します。

3)OKをクリックします。

お客様は、選択した顔画像に基づいて、撮影した画像の顔を検索し、比較します。

11.1.3 人名による顔の検索

撮影した顔画像を人名で検索します。

開始前に

ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。デバイスの追加の詳細については、「デバイスの追加」を参照してください。

ステップ



注記

この機能は、接続されている機器がサポートしている必要があります。

1. 「データ検索」→「顔検索」をクリックして、顔画像検索ページに入ります。
2. カメラパネルでデバイスを選択します。
3. 個人名で検索するには、ドロップダウンリストから[名前]を選択します。
4. クリックすると、撮影した顔画像や動画の検索開始時刻、終了時刻が設定されます。📁ファイル
5. 個人名のキーワードを入力します。

6. 最大表示件数を設定します。
7. 「検索」をクリックして検索を開始します。
検索条件(ファジィマッチ対応)に一致する名前の人がすべて表示されます。

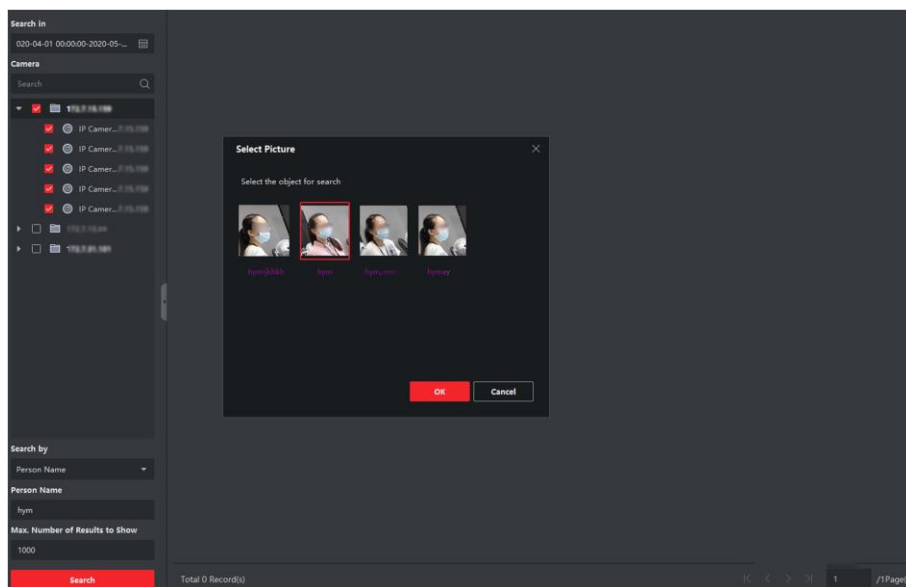


図11-3結果













8. 検索する画像を1つ選択し、確認ボタンをクリックします。
画像の検索結果が右側に表示されます。
9. 画像をエクスポートし、パソコンに保存します。
エクスポートピクチャ
エクスポートする画像を選択し、ローカルパソコンに保存します。
Export Currentページ
現在のページのすべての画像をエクスポートします。
輸出セグメント
パッケージごとに画像をダウンロードできます。1つのパッケージには、1,000枚までの画像が含まれています。

10. 検索した顔画像を選択すると、撮影した顔画像と人物情報が表示されます。



図11-4 結果

11. オプション:検索後、次の操作を1つ以上実行できます。

<p>詳細の表示</p>	<p>キャプチャした顔画像、およびページ上の人物情報(類似性、性別、温度状態、キャプチャした時間など)を表示します。 また、クリックして大きい画像を表示し、クリックして復元することもできます。  </p>
<p>関連ビデオの再生</p>	<p>右下のビューウィンドウで、画像の関連ビデオファイル(キャプチャの5秒前と5秒後)を再生するには、クリックします。 </p> <hr/> <p> 注記</p> <ul style="list-style-type: none"> • クリックできます 大きなビデオを表示し  クリックして復元します。  • クリックできます 再生速度を調整するには、クリックしてビデオファイルをフレーム単位で再生し、クリックしてオーディオを有効にし、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します。   • クリックすると、撮影した画像を見ることができます。 
<p>画像をパソコンに保存</p>	<p>必要に応じて写真をクリックして選択し、ローカルPCにエクスポートします。クリックすると、撮影した画像が顔画像ライブラリに追加されます。  </p>
<p>顔画像ライブラリに画像を追加する</p>	<p> 注記 キャプチャした人物、携帯電話、性別などの画像に対して顔画像ライブラリを選択し、人物情報を入力します。</p>

12. オプション:検索結果に基づいて2次検索を実行します。
 - 1)「個人情報」ページで、をクリックします。🔍
このピクチャのすべての顔が分析され、表示されます。
 - 2)ポップアップウィンドウで赤枠を動かして、2次検索を行う顔を選択します。

**注記**

ピクチャに複数の面がある場合は、選択のためのウィンドウが表示されます。
ピクチャ内に顔が1つしかない場合は、この手順を省略します。

- 3)OKをクリックします。
お客様は、選択した顔画像に基づいて、撮影した画像の顔を検索し、比較します。

11.1.4 顔の特徴による顔の検索

検出した顔画像を性別、メガネ着用などの顔の特徴から検索することができます。

ステップ

1. 「データ検索」→「顔画像検索」をクリックします。
2. 検索する期間を選択します。
3. カメラ一覧からカメラを選択します。
4. 検索の種類として「顔の機能」を選択します。
5. 年齢層、性別、眼鏡の着用、笑顔、マスクの着用など、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。
検索した顔画像が右側に表示されます。
8. 画像をエクスポートし、パソコンに保存します。

エクスポートピクチャ

エクスポートする画像を選択し、ローカルパソコンに保存します。

Export Currentページ

現在のページのすべての画像をエクスポートします。

輸出セグメント

パッケージごとに画像をダウンロードできます。1つのパッケージには、1,000枚までの画像が含まれています。

9. オプション:検索した顔画像を選択すると、撮影した画像と人物情報が表示されま

す。

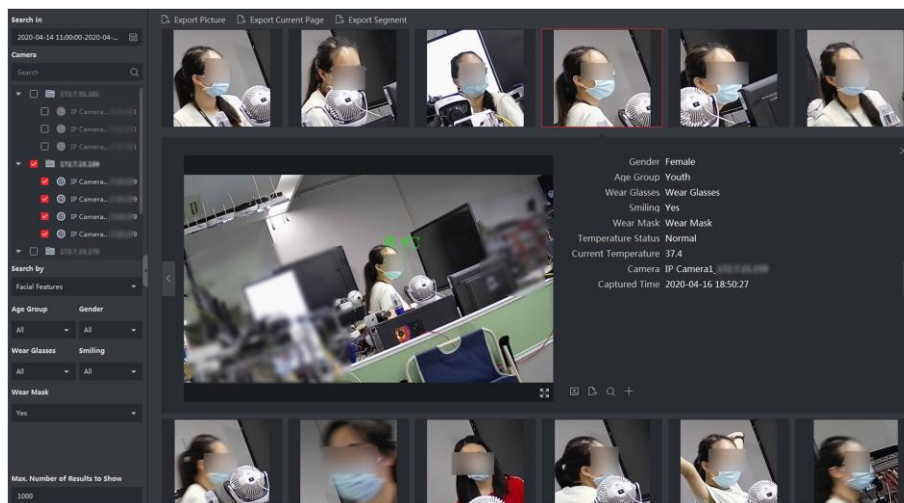














図11-5 結果

10. オプション:検索後、次の操作を1つ以上実行できます。

<p>詳細の表示</p>	<p>キャプチャした顔画像、およびページ上の人物情報(類似性、性別、温度状態、キャプチャした時間など)を表示します。</p> <p>また、クリックして大きい画像を表示し、クリックして復元することもできます。 </p>
<p>関連ビデオの再生</p>	<p>右下のビューウィンドウで、画像の関連ビデオファイル(キャプチャの5秒前と5秒後)を再生するには、クリックします。</p> <hr/> <p> 注記</p> <ul style="list-style-type: none"> • クリックできます 大きなビデオを表示し  クリックして復元します。  • クリックできます 再生速度を調整するには、クリックしてビデオファイルをフレーム単位で再生し、クリックしてオーディオを有効にし、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します。 • クリックすると、撮影した画像を見ることができます。
<p>画像をパソコンに保存</p>	<p>必要に応じて写真をクリックして選択し、ローカルPCにエクスポートします。クリックすると、撮影した画像が顔画像ライブラリに追加されます。</p> <p></p>

顔画像ライブラリに画像を追加する	 注記 キャプチャした人物、携帯電話、性別などの画像に対して顔画像ライブラリを選択し、人物情報を入力します。
------------------	--

11. オプション:検索結果に基づいて2次検索を実行します。

- 1)「個人情報」ページで、をクリックします。
このピクチャのすべての顔が分析され、表示されます。
- 2)ポップアップウィンドウで赤枠を動かして、2次検索を行う顔を選択します。

注記

ピクチャに複数の面がある場合は、選択のためのウィンドウが表示されます。ピクチャ内に顔が1つしかない場合は、この手順を省略します。

- 3)OKをクリックします。
お客様は、選択した顔画像に基づいて、撮影した画像の顔を検索し、比較します。

11.2 人体回収

DeepinMindデバイスでは、ローカルPCからの画像のアップロードや機能の設定などの検索条件を設定して、撮影した人体画像を検索したり、関連ビデオを表示したりできます。

11.2.1 アップロードした画像で人体を検索する

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、アップロードした画像とデバイスで撮影した人体画像を比較したり、特定の時間に特定のカメラで撮影したすべての人体画像を検索したりできます。

開始前に


ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。デバイスの追加の詳細については、「デバイスの追加」を参照してください。

ステップ



注記

この機能は、接続されている機器が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、人体検索画面に入ります。
2. クリックすると、撮影した人体画像や動画ファイルの検索開始時刻、終了時刻が設定されます。
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。

ピクチャ

写真をアップロードして、アップロードした写真と、装置で撮影した人体写真を比較します。この画像に表示されるすべての人体が分析され、表示されます。

1. [ピクチャの選択]をクリックして、コンピュータから比較するピクチャを選択します。



注記

- 画像は4MB未満でなければなりません。
- 画像の解像度は、4096*4080より小さくなければならない。
- JPG形式とJPEG形式のみ対応しています。

2. 類似性レベルを設定します。例えば、類似度を40に設定すると、取り込んだ画像はアップロードした人体画像と40%以上の類似度があります。

全て

選択したカメラで撮影した画像を、時間内にすべて検索します。

5. 最大表示件数を設定します。



注記

選択した継続時間内に選択したカメラで撮影した画像の枚数が表示できる最大枚数を超えた場合は、継続した画像のみが表示されます。

たとえば、選択した継続時間内に選択したカメラで撮影した画像の枚数が2000枚で、最大表示枚数が1000枚の場合は、1000枚までしか表示されません。

6. 「検索」をクリックして検索を開始します。
画像の検索結果が一覧表示されます。

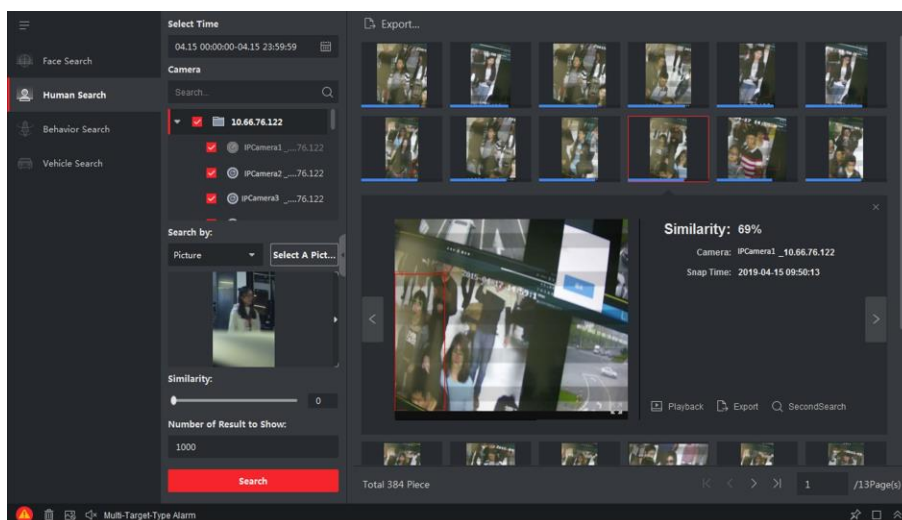










図11-6 検索結果

7. オプション:検索結果に基づいて2次検索を実行します。

- 1) 検索した画像に移動し、クリックする
 - この画像に表示されるすべての人体が分析され、表示されます。
- 2) 二次検索を行う人体を選択します。
- 3) 類似性と期間を設定します。
- 4) 検索をクリックします。

お客様は、選択した人体像に基づいて、撮影した画像の人体を検索し、比較します。

8. オプション:人体を検索した後、以下の操作を1つ以上行うことができます。

<p>詳細の表示</p>	<p>詳細を表示するには、リスト内の画像をクリックします。また、クリックして大きい画像を表示し、クリックして復元することもできます。 </p>
<p>関連ビデオの再生</p>	<p>再生をクリックして、画像に関連するビデオファイル(5秒前と5秒後)を再生します。</p> <p>右下のビューウィンドウのキャプチャ</p> <hr/> <p> 注記</p> <ul style="list-style-type: none"> • クリックできます 大きなビデオを表示、クリックして復元します。 • クリックできます 再生速度を調整するには、クリックしてビデオファイルをフレーム単位で再生し、クリックしてオーディオを有効にし、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します。 

画像をパソコンに保存	「ピクチャの書き出し」をクリックし、必要に応じてピクチャを選択してローカルPCに書き出します。
------------	---

11.2.2 人物による人体探索

年齢、性別、服装などの検索条件を設定することで、撮影した人体画像を検索することができます。

開始前に

ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。デバイスの追加の詳細については、「デバイスの追加」を参照してください。

ステップ



注記

この機能は、接続されている機器が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、人体検索画面に入ります。
2. クリックすると、撮影した人体画像や動画ファイルの検索開始時刻、終了時刻が設定されます。
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「機能」を選択します。
5. 年齢、性別、上の色、眼鏡の着用の有無などの人物の特徴を設定します。
6. 検索したい人体画像のイベントタイプを選択します。
7. 最大表示件数を設定します。
8. 「検索」をクリックして検索を開始します。
画像の検索結果が一覧表示されます。
9. オプション:検索結果に基づいて2次検索を実行します。

- 1) 検索した画像に移動し、クリックする








この画像に表示されるすべての人体が分析され、表示されます。

- 2) 二次検索を行う人体を選択します。
- 3) 類似性と期間を設定します。
- 4) 検索をクリックします。

お客様は、選択した人体像に基づいて、撮影した画像の人体を検索し、比較します。

10. オプション:検索後、次の操作を1つ以上実行できます。

詳細の表示	詳細を表示するには、リスト内の画像をクリックします。また、クリックして大きい画像を表示し、クリックして復元することもできます。
-------	---

関連ビデオの再生	<p>クリックすると、画像の関連ビデオファイルが表示ウインドウで再生されます。</p> <p> 右下</p> <hr/> <p> 注記</p> <ul style="list-style-type: none"> • クリックできます 大きなビデオを表示し  クリックして復元します。  • クリックできます 再生速度を調整する  は、クリックしてビデオファイルをフレーム単位で再生し、クリックしてオーディオを有効にし、再生ウインドウをダブルクリックしてウインドウを最大化します。  
画像をパソコンに保存	<p>「ピクチャの書き出し」をクリックし、必要に応じてピクチャを選択してローカルPCに書き出します。</p>

11.3 ビヘイビア分析に関連する画像とビデオの表示


接続された機器が行動検索(例えば、行交差、人の集まり、反復)に対応している場合は、関連する画像を検索したり、関連する画像やビデオファイルを閲覧することができます。

開始前に

ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。「デバイスの追加」を参照

カメラの追加の詳細については、

ステップ

1. 「データ検索」→「ビヘイビア分析」をクリックして、ビヘイビア分析ページに入ります。
2. クリックすると、一致した画像を検索する開始時刻と終了時刻が設定されます。 
3. カメラ一覧からカメラを選択します。

注記






この機能は、接続されたデバイス(NVRまたはDVR)でサポートする必要があります。

4. オプション:偽アラーム控除をチェックして、偽アラームを結果から除去します。

例

このカメラは、時には、ツリーシェーキングを動き検知アラームとして、または動物をおそらく高感度のために、ライン横断アラームをトリガする人物としてとらえるかもしれません。このアラームは、NVRまたはDVRによって誤警報としてとらえられます。

5. 行動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:ビヘイビアを検索した後、以下の操作を実行できます。

詳細の表示	詳細を表示するには、リスト内の画像をクリックします。また、クリックして大きい画像を表示し、クリックして復元することもできます。 
関連ビデオの再生	<p>再生をクリックして、画像に関連するビデオファイル(5秒前と5秒後)を再生します。</p> <p>右下のビューウィンドウのキャプチャ</p> <hr/> <p> 注記</p> <ul style="list-style-type: none"> • クリックできます 大きなビデオを表示、クリックして復元します。 • クリックできます 再生速度を調整するには、クリックしてビデオファイルをフレーム単位で再生し、クリックしてオーディオを有効にし、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します。
画像をパソコンに保存	「ピクチャの書き出し」をクリックし、必要に応じてピクチャを選択してローカルPCに書き出します。

11.4 車両回収

DeepinMindデバイスでは、プレート番号、キャプチャ時間などの検索条件を設定することで、デバイスのキャプチャされた車両画像を検索できます。

開始前に


ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。「デバイスの追加」を参照

デバイスの追加の詳細については、

ステップ

注記

この機能は、接続されている機器が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」をクリックして、車両検索ページに入ります。
2. クリックすると、撮影した車両の画像や動画を検索する開始時刻と終了時刻が設定されます。
ファイル

3. 検索タイプを選択します。

車両

車両ナンバープレート番号を入力して、撮影した車両画像を検索して表示します。

プレート

撮影したナンバープレートの画像を検索し、車両のナンバープレート番号を入力して表示します。

混在トラフィック検出

車両のナンバープレート番号を入力して、特定の車両の混在交通検知関連画像を検索・表示する。



カメラはトラフィックの混合検知をサポートする必要があります。

交通違反

車両のナンバープレート番号を入力することにより、特定の車両の交通違反関連画像を検索し、表示する。



カメラは交通違反をサポートする必要があります。

4. カメラパネルでデバイスを選択します。
5. 検索するナンバープレート番号のキーボードを入力します。
6. 最大表示件数を設定します。

7. 「検索」をクリックして検索を開始します。

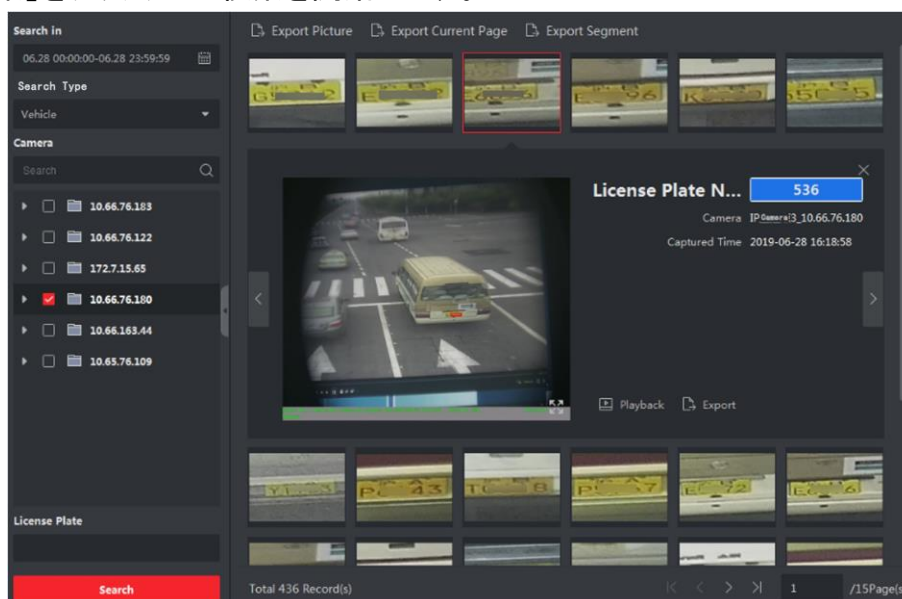


図11-8の結果

画像の検索結果が一覧表示されます。

8. オプション:写真をクリックすると、撮影された写真全体、撮影時間などが表示されます。
9. オプション:画像をローカルPCにエクスポートします。
 - ピクチャのエクスポートをクリックした後、エクスポートするピクチャを選択し、エクスポートをクリックします。
 - 現在のページのエクスポートをクリックして、現在のページのすべての画像と情報をエクスポートします。
 - 「エクスポートセグメント」をクリックして、画像をダウンロードし、パッケージごとに情報を取得します。1つのパッケージには、1000枚までの画像が含まれています。
10. オプション:必要に応じて以下の操作を行います。

顔画像ライブラリに追加	Add to face picture libraryをクリックして、現在のface pictureをライブラリに追加します
詳細情報表示	[表示]をクリックして、この人物の過去の撮影画像、つまり撮影時刻を表示します。
再生	「再生」をクリックして、5秒前のビデオを再生し、キャプチャ時間の後に。

輸出	エクスポートする画像をクリックし、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。
----	---

11.5 ハードハット検索

ハードハット検知装置をクライアントに追加した後、ハードハットを着用していない人を検知すると、イベントがトリガーされ、一部の画像が撮影されてマネージャーに通知されます。検知した人が帽子をかぶっていないアラーム画像を検索します。こうすることで、施工者に堅い帽子を着用することを思い出させることができ、施工者の安全意識を高めることができます。

開始前に

ハードハット検出機能付き機器をクライアントに追加します。

ステップ

1. 「データ検索」→「ハードハット検索」をクリックして、ハードハット検索ページを入力します。
2. 検索の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ぶ。
4. 検索をクリックします。

ハードハットアラームで撮影した画像が右パネルに表示されます。1ページに表示できる画像数は30枚までです。

5. 必要に応じて以下の操作を行ってください。

エクスポートピクチャ	<ol style="list-style-type: none"> 1. ピクチャの書き出しをクリックします。 2. 1つ以上の画像を選択するか、下のページで「すべてを選択」をチェックします。 3. 以下のページの[Export]をクリックして、選択した画像をエクスポートします。
ピクチャ全体を表示する	画像をクリックすると、画面中央に画像全体と撮影時間が表示されます。
ビデオの再生	ピクチャをクリックしてから再生をクリックすると、キャプチャ時間の前後5秒間のビデオが再生されます。

11.6 ピープルフェアサーチ

「人の頻度」とは、一定期間に検知区域内で発生した人の出現頻度をいう。出現頻

度があらかじめ定められた閾値を超える者を「頻繁に出現する者」といい、出現頻度があらかじめ定められた閾値を下回る者を「稀に出現する者」という。クライアントは、高セキュリティを必要とする場所を守るために頻繁に登場する人々を検索することをサポートし、特定の期間にめったに登場しない場合にトラブルに巻き込まれる可能性のある人々をめったに登場させない。

11.6.1 出頭頻度の高い者の検索

撮影した人物の顔画像を、顔画像ライブラリの顔画像と比較することができます。不一致がある場合、頻繁に出現する人物と判断され、イベントをトリガーしてセキュリティ担当者に通知します。例えば、銀行のように安全性が要求される場面では、見知らぬ人が頻繁に現れると、警備員や関係者に通知するためにイベントがトリガーされる。一致した場合、ホワイトリストの人物と判断され、頻繁に出現する人物警報のトリガーとはならない。撮影した画像や撮影した時刻など、イベント情報を一定時間で検索し、詳細な画像を表示して関連する動画を再生できます。

開始前に

- 頻繁に表示される個人アラームが装置に設定されていることを確認します。
- 装置が装備されていることを確認します。

ステップ

1. 「データ検索」→「ピープルフェア検索」→「頻繁に表示される個人」をクリックします。
2. 検索の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。

頻繁に表示される人物警報関連の写真が右パネルに表示されます。



図11-9結果

5. オプション:写真をクリックすると、撮影された写真全体、撮影時間などが表示されます。
6. オプション:画像をローカルPCにエクスポートします。
 - ピクチャのエクスポートをクリックした後、エクスポートするピクチャを選択し、エクスポートをクリックします。
 - 現在のページのエクスポートをクリックして、現在のページのすべての画像と情

報をエクスポートします。

- 「エクスポートセグメント」をクリックして、画像をダウンロードし、パッケージごとに情報を取得します。1つのパッケージには、1,000枚までの画像が含まれています。

7. オプション:必要に応じて以下の操作を行います。

顔画像ライブラリに追加	Add to face picture libraryをクリックして、現在のface pictureをライブラリに追加します。
詳細情報表示	[表示]をクリックして、この人物の過去の撮影画像、つまり撮影時刻を表示します。
再生	再生をクリックすると、5秒前後の動画が再生されます。 キャプチャ時間
輸出	エクスポートする画像をクリックし、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。

11.6.2 出頭頻度の低い者の検索

装置は、セキュリティ担当者が期限内にその担当者を知り、その担当者を確認するために行くために、十分な時間がない人を含む情報を提供する、めったに出現しない人物報告書をクライアントに定期的を送付する。この機能は、一人暮らしの高齢者や受刑者によく使われる。もし、しばらく出現しなかった場合は、警備員は、それらを見つけて、それらがトラブルや逃げ出していないことを確認する必要がある。

開始前に

- 頻繁に表示される個人アラームが装置に設定されていることを確認します。
- 装置が装備されていることを確認します。
- 装置のリモート設定ページで、検出時間、統計期間、周波数しきい値、および顔画像ライブラリを設定していることを確認します。

ステップ

1. [データ検索] → [ピープルフェア検索] → [まれに出頭者] の順にクリックします。
2. 検索の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。

めったに表示されない個人レポートが右パネルに表示されます。

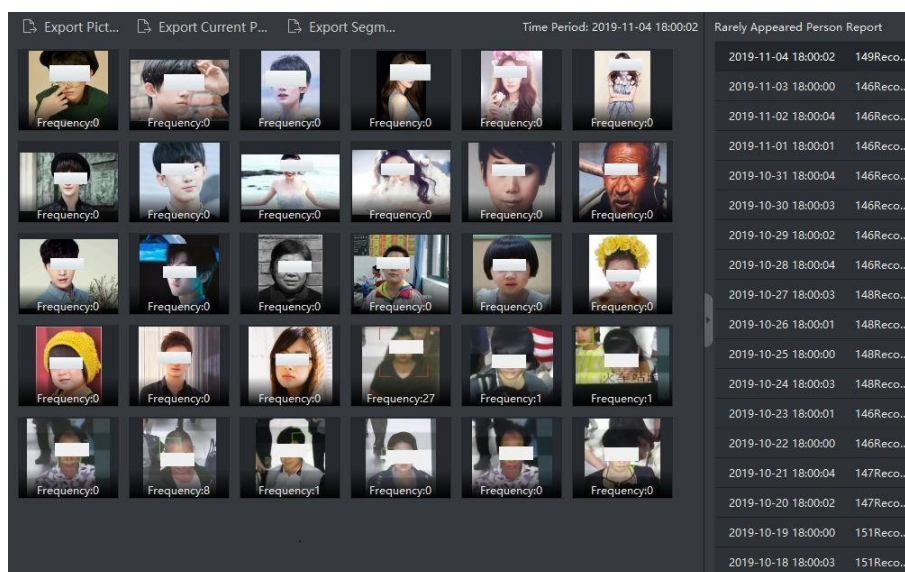


図11-10 結果

5. レポートをダブルクリックすると、めったに表示されない人が表示されます。
6. オプション:キャプチャした画像の詳細を表示するには、画像をクリックします。
7. オプション:画像をローカルPCにエクスポートします。
 - ピクチャのエクスポートをクリックした後、エクスポートするピクチャを選択し、エクスポートをクリックします。
 - 現在のページのエクスポートをクリックして、現在のページのすべての画像と情報をエクスポートします。
 - 「エクスポートセグメント」をクリックして、画像をダウンロードし、パッケージごとに情報を取得します。1つのパッケージには、1,000枚までの画像が含まれています。

11.7 AIダッシュボードの検索

撮影した画像や動画のタスク、読み込んだ画像タスクの結果を検索して、タスクの詳細情報を表示できます。

注記

ビデオ解析タスクはWebクライアントでのみ設定され、画像解析タスクは次のように設定できます。

Webクライアントまたはコントロールクライアントに設定されています。


11.7.1 ビデオおよび取り込んだピクチャータスクの検索分析結果

撮影した動画や画像の解析タスクの結果を検索して、関連する動画や画像を見ることができます。

開始前に




AIダッシュボードプラットフォームをサポートするデバイスをプラットフォームに追加します。

ステップ

1. データ取得モジュールを入力します。
2. 「AIダッシュボード検索」を選択します。
3. クリックすると、タスク検索の時間範囲が設定されます。
4. タスクの種類として「ビデオ & 取り込み分析タスク」を選択します。
5. タスクに設定されているデバイスを選択します。
6. 検索をクリックします。

右側にタスクリストが表示されます。

7. オプション:以下の操作を実際の要求に応じて行います。

エクスポートピクチャ	右側の 画像 または 情報レコード を選択し、「ピクチャのエクスポート」をクリックして、設定したパスに保存します。
詳細の表示	画像または情報レコードを1つ選択し、クリックするとアラームが表示されます 情報やビデオ素材 <hr/>  注記 キャプチャ時間の5秒前または後にビデオが記録されます。再生、一時停止、1コマ再生、音量調節に対応しています。
表示モード	タスクをクリックするか、サムネイルまたはリストで表示します。  

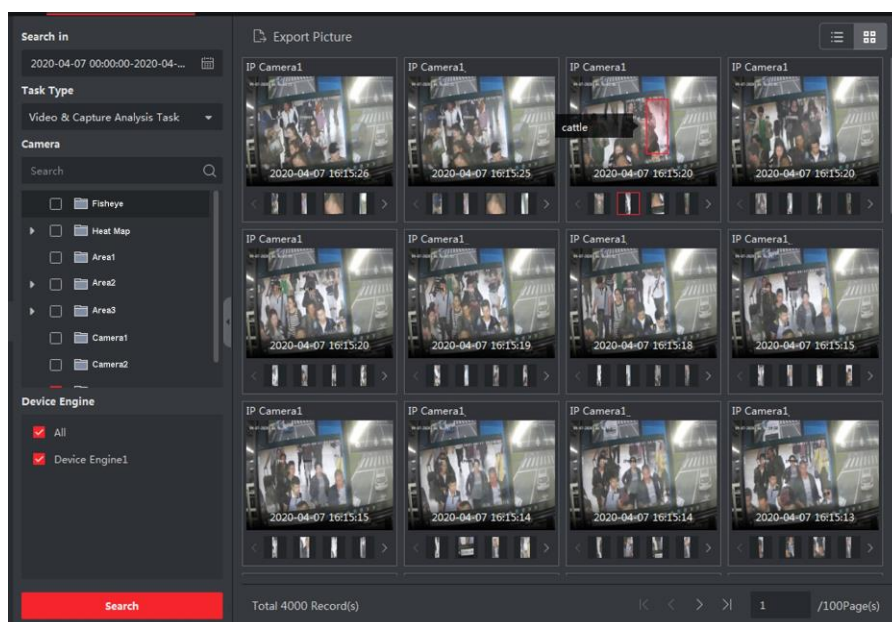


図11-11 ビデオおよび取り込んだピクチャータスクの検索分析結果

11.7.2 インポートされたピクチャータスクの検索分析結果

インポートした画像解析タスクの結果を検索し、関連する画像ファイルや画像情報を表示できます。

開始前に

AIダッシュボードプラットフォームをサポートするデバイスをプラットフォームに追加します。

ステップ

1. データ取得モジュールを入力します。
2. 「AIダッシュボード検索」を選択します。
3. クリックすると、タスク検索の時間範囲が設定されます。
4. タスクの種類として、ピクチャーインポート分析タスクを選択します。
5. タスクに設定されているデバイスを選択します。
6. 検索をクリックします。

右側にタスクリストが表示されます。

7. オプション:以下の操作を実際の要求に応じて行います。

エクスポートピクチャ	右側の画像または情報レコードを選択し、「ピクチャのエクスポート」をクリックして、設定したパスに保存します。
ピクチャの詳細表示	画像または情報レコードを1つ選択し、それをクリックして画像またはタグ情報(車両など)を増幅します。

表示モード

タスクをクリックするか、サムネイルまたはリストで表示します。

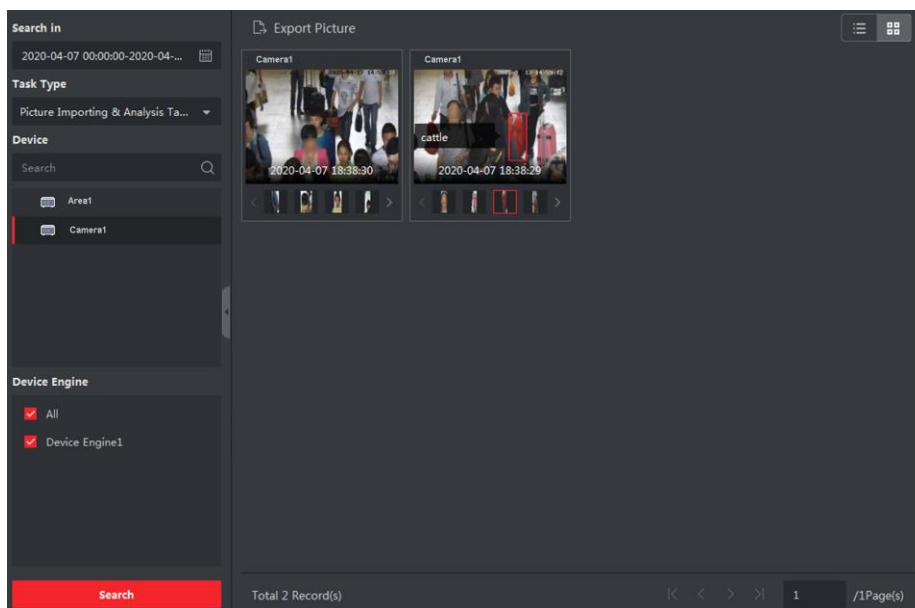


図11-12 インポートされたピクチャータスクの検索分析結果

11.8 顔認証チェックイン

顔認証をサポートする機器は、人物が顔認証でチェックインできます。認識された顔と顔画像ライブラリを比較することにより、一致した場合、システムはそれを成功した顔比較レコードとして記録する。成功した顔比較レコードが次の場合、

チェックイン期間中はチェックイン記録とする。さらに、出席率も記録は、成功した顔の比較記録に基づいて計算することもできる。

必要に応じて、顔認証チェックインレコードまたは顔文字を検索できます。
表彰出席記録

11.8.1 顔認識チェックイン記録の検索

指定した期間内に顔認証でチェックインした人のチェックイン記録を検索し、ローカルPCにエクスポートします。


開始前に

ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。「デバイスの追

加」を参照
デバイスの追加の詳細については、
ステップ

 注記

この機能は、接続されている機器が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」→「チェックイン検索」と入力します。
2. クリックすると、検索開始時刻と終了時刻が設定されます。 

例

チェックインの記録を順次検索する必要がある場合は、時間を2020-03-01と設定できます。2020-03-31. 2020-03-31.

3. チェックイン期間を設定します。
4. 人相認識チェックインに使用するカメラをチェックする。
5. 1つまたは複数の顔画像ライブラリをチェックして、選択したライブラリの参加者を検索します。
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。

検索された結果は、顔写真、顔ライブラリ、名前、チェックインカウントを含む出席記録を示します。

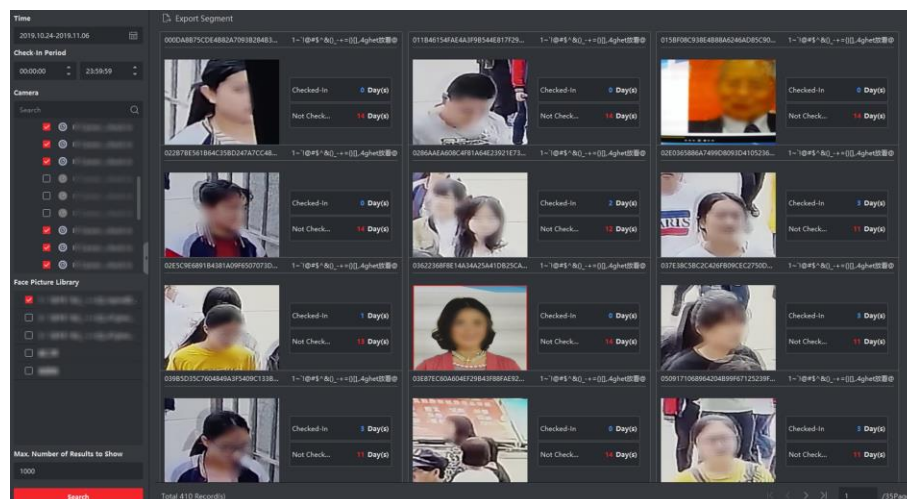


図11-13 結果

8. オプション:データをローカルPCにエクスポートするには、右上隅にあるすべてのエクスポートをクリックします。

11.8.2 顔認識出席記録の検索

顔認証でチェックインした人の出勤記録を検索できます。フェイスピクチャライブラリ

で正常にチェックインした人の日次、月次、年次の出席記録を検索して、スタッフの出席状況(通常、遅刻、早退、欠勤)を知ることができます。出勤状況は、検索条件のチェックイン期間を、成功した顔比較レコード(最も早いものと遅いもの)と比較することによって計算された結果です。出勤記録をエクスポートして、スタッフの出勤データを表示することができます。

開始前に

ソフトウェアにデバイスを追加し、対応する設定を正しく設定します。「デバイスの追加」を参照

デバイスの追加の詳細については、

ステップ

1. 「データ検索」→「顔認識チェックイン」→「出勤検索」の順に選択します。
2. 検索するレコードの時間範囲を設定します。

例

行進の出席記録を検索する必要がある場合は、2020-03-01～2020-03-31と設定できます。

3. チェックイン期間を設定します。

例

チェックイン期間が08:00～17:00に設定されている場合は、チェックインが08:00より早く、チェックアウトが遅い

17:00を超えた場合は、通常出勤とみなします。

4. 勤務日に応じて勤務期間を選択します。

例

週末が休憩の場合は、月曜日、火曜日、水曜日、木曜日、金曜日を次のように選択できます。

出勤期間

5. 顔認証チェックイン用のカメラを選択します。



同じNVR内のカメラのみ選択できます。

6. 顔画像ライブラリを選択します。

フェイスピクチャライブラリを選択すると、ライブラリ内の人の出席履歴のみが検索されます。デバイスのリモート設定ページで顔画像ライブラリを設定するか、設定するデバイスにログインします。

7. 最大値を設定します。表示する結果の数。

8. 検索をクリックします。

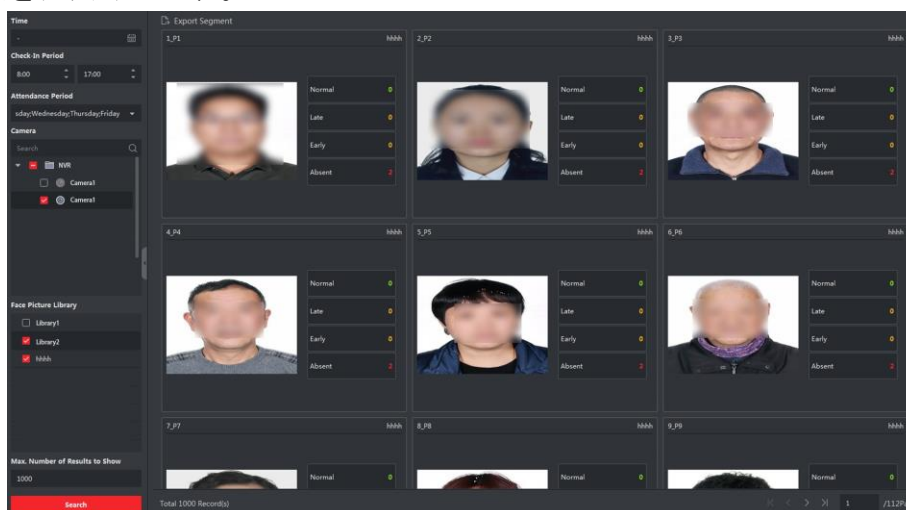


図11-14 顔認識出席者検索

正常

最も早いチェックインレコード(最も早い顔認識比較成功レコード)は、チェックイン開始時刻より遅くはならない。一方、最新のチェックアウトレコード(最新の顔認識比較成功レコード)は、チェックイン終了時刻より遅くはならない。

例えば、チェックイン期間を08:00～17:00に設定した場合、チェックインが08:00より早く、チェックインが17:00より遅い場合は通常出勤とみなします。

後期

チェックインレコード(最も早い顔認識比較の成功レコード)は、チェックイン開始時刻より遅い。

チェックイン期間を08:00～17:00に設定した場合、08:00～17:00のチェックインから17:00以降のチェックインは遅延とみなされます。

早退

チェックアウトレコード(最新の顔認識比較成功レコード)はチェックイン終了時間よりも早い。

チェックイン期間を08:00～17:00に設定した場合、08:00より早いチェックインと08:00～17:00のチェックアウトは遅いとみなされます。

なし

チェックイン時に顔認識の比較に成功したレコードが見つからない場合は、出勤簿は不在とみなす。

検索された結果は、顔写真、顔ライブラリー、名前、チェックインカウントを含む出席記録を示します。

9. オプション:[セグメント別のエクスポート]をクリックして、ローカルPCに出席記録をエクスポートします。


第 12 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ます。このモジュールを通して、固定カメラとパノラマカメラとの顔の比較と連動撮影、交通事故警報、AIオープンプラットフォームを介して、サードパーティのアプリケーションにアクセスすることができます。

12.1 フェイスアプリケーション

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機器では、Face Application機能は、ライブビュー中にブラックリスト、VIP、または通常の衣服着用者の顔比較アラームを表示します。検出された顔画像が、ブラックリストまたはVIP顔画像ライブラリに登録されている人物と照合された場合、セキュリティセンターは、迅速かつ効果的に適切な行動をとるために、関連する警報を受信します。また、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るレギュラー服装の評価にも役立ちます。

12.1.1 顔画像ライブラリのリストタイプの設定

ライブビュー中に検出された人物がブラックリストか、非常に重要な人物か、あるいは普通の服装者かをソフトウェアが確認できるように、機器の各顔画像ライブラリにリストタイプを設定できます。「AIダッシュボード」→「顔アプリケーション」の順にクリックし、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の種類を選択します。

ブラックリスト

アラームの種類が「ブラックリスト」に設定されている場合は、撮影した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

フェイスピクチャライブラリがVIPに設定されている場合、撮影した写真とフェイスピクチャライブラリの写真が一致すると、AIダッシュボードにVIPアラームが表示されます。

通常


ブラックリストにもVIPにも属さない顔画像ライブラリは[通常]に設定することができます。AIダッシュボードは、撮影した顔画像と顔画像ライブラリの顔画像が一致している場合はアラームを表示しません。

 注記

この機能はデバイスでサポートされている必要があり、フェイスピクチャライブラリは最初にデバイスで設定する必要があります。

12.1.2 AI 情報表示カメラの設定

ライブビュー中にAI情報を表示するには、カメラ一覧の表示カメラなどを指定します。たとえば、VIP情報を表示するカメラ(表示ウインドウのライブビューではない)を選択した場合、このカメラは背景で静止検知を行い、VIPに関するAI情報を表示します。

「AIダッシュボード」→「顔アプリケーション」をクリックし、右上隅をクリックしてリアルタイムでAI情報を表示するカメラを選択します。

ブラックリストアラーム、VIPアラーム、または通常のカスタマアラームで、表示するアラームの種類を選択します。

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をチェックすると、表示ウインドウのライブビューのカメラのAI情報のみが表示されます。

カスタムカメラ

カスタムカメラを確認し、希望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かかわらず、選択したカメラのAI情報を表示できます。

12.1.3 人工知能情報の表示

顔画像ライブラリのAI情報表示カメラ、リストタイプを設定した後、AI情報を見ることができます。

「AIダッシュボード」→「顔アプリケーション」をクリックし、カメラ一覧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

この機能は、装置がサポートする必要があります。

カメラリスト

左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されたすべてのリソースが

表示されます。また、適切なウィンドウ区分と希望するカメラを選択して、AI情報を表示することができます。


注記

ライブビューを同時に表示するチャンネルは、クライアントを実行する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すると、ストリームの種類をメインストリームとサブストリームに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をクリックし、ウィンドウを選択して、目的のインテリジェントディスプレイを有効にします。例えば、すべてのライブビューウィンドウでブラックリストアラームが有効になっている場合、認識されたターゲットは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ディスプレイを有効にすることもできます。

顔の比較

「顔の比較」スイッチを「ON」に設定した場合、ブラックリストの個人、VIP、または常連客を検出すると、対応する色のアラーム通知が右パネルに表示されます。アラームの時刻、カメラ、その他の詳細を表示します。

過去のキャプチャ画像

過去のキャプチャ画像をページ下に表示します。

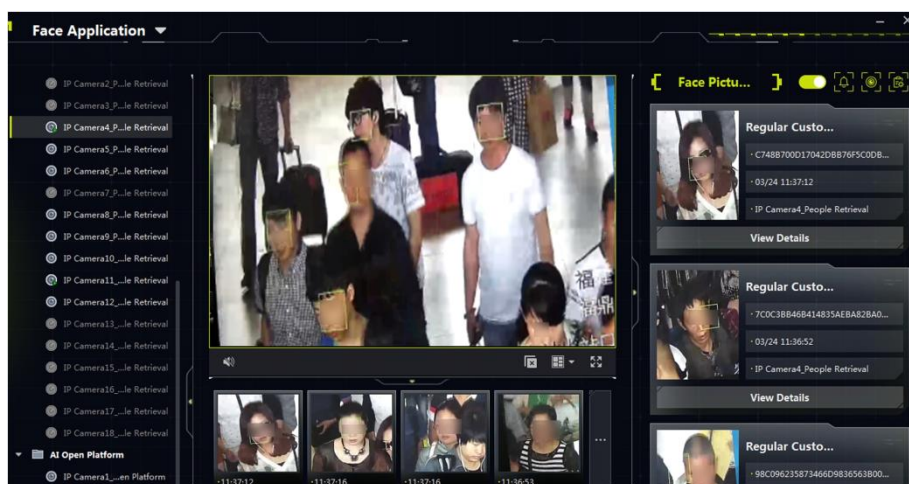


図12-1 AI情報を表示する

アラームトリガードポップアップウィンドウを有効にする

☒ をクリックすると、アラームがトリガされたポップアップウィンドウが有効になり、その後、ブラックリストアラームがトリガされると、キャプチャした写真やアラーム詳細情報を含むウィンドウがポップアップします。

12.2 マルチターゲット型検出

複数ターゲットタイプ検出とは、顔、人体、自動車、および非自動車を含む複数のタイプの検出ターゲットを認識し捕捉する機能を指す。ターゲットを検出すると、ライブビュー、撮影した画像、ターゲットの機能を表示できます。アラームは、撮影された顔・人体画像と画像ライブラリの画像との類似性が高い場合や、人物・車両の出現頻度が高い・低い場合、あるいは車両の出現頻度が高い場合などにトリガーされます。交差点や駅など、乗り物や乗り物が多く、警備が必要な場所で使用されることが多い。

12.2.1 ターゲット検出パラメータの設定

クライアントは、検出されたターゲットの表示レイアウトとその詳細をカスタマイズし、検出されたターゲットで表示する機能を選択し、アラームが表示されるカメラを選択することができます。

ディスプレイモード設定

表示レイアウトをカスタマイズし、必要に応じて表示する情報を選択できます。

ステップ

1. 「AI ダッシュボード」→「マルチターゲットタイプ検出」をクリックします。
2. 右上隅☒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する。
 - 単一チャンネルを選択すると、1つのライブビューウィンドウが表示されます。
 - デュアルチャンネルを選択して、2つのライブビューウィンドウを表示します。
 - チャンネル4を選択すると、4つのライブビューウィンドウが表示されます。

5. 該当箇所に表示する情報を確認する。

 注記

Face Arming機能は、装置がサポートする必要があります。
ページ下部に表示する項目は、最大2項目まで選択できます。

チェックした情報は以下の画面に表示されます。

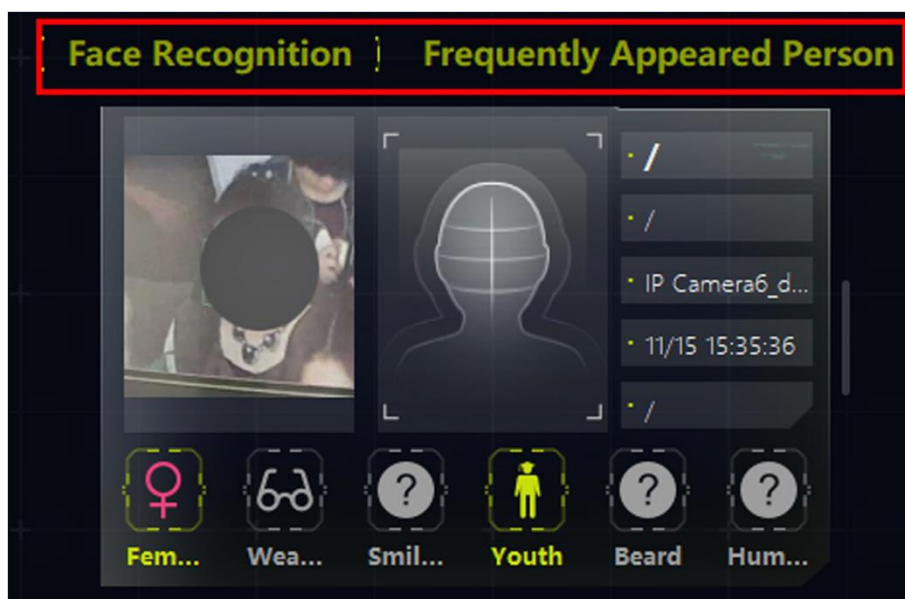


図12-2右図

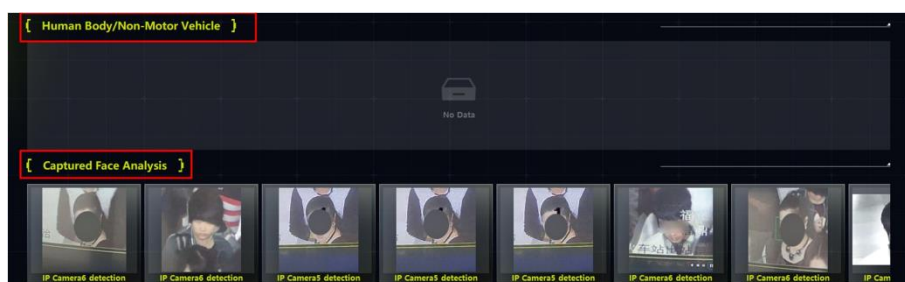



図12-3下部の表示

6. オプション:撮影した画像がすべて指定したフォルダに保存されるように、画像の保存を有効にし、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

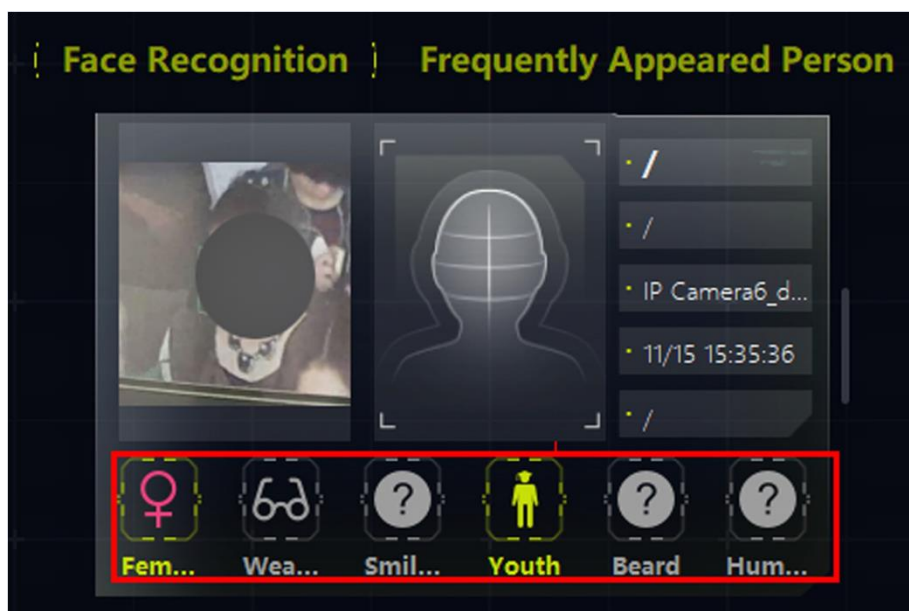
撮影した画像については、撮影したターゲットの特徴を解析します。必要に応じて表示する機能を選択できます。例えば、顔検出を例にとると、年齢、性別、メガネ着用などの機能を選択して写真に表示することができます。

ステップ

1. 「AI ダッシュボード」→「マルチターゲットタイプ検出」をクリックします。
2. 右上隅  をクリックして、Configureウィンドウを開きます。
3. 「取り込みパラメータ」タブをクリックします。
4. 表示機能を有効にします。
5. 車両検知/車両検知/人体検知/車両非検知の機能を有効にし、対応する機能を確認します。

注記

各機能の機能は、6つを超えない範囲で選択できます。



図

12-4 表示機能

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

検出アラームが設定されているカメラでは、アラームの詳細情報を表示して、右パネルにアラームを表示するカメラを選択できます。

開始前に

表示するアラームを選択したカメラにアラームが設定されていることを確認します。

ステップ

1. 「AI ダッシュボード」→「マルチターゲットタイプ検出」をクリックします。
2. 右上隅  をクリックして、Configure ウィンドウを開きます。
3. [アラーム設定の受信] タブをクリックします。
4. 右パネルにアラームが表示されるカメラを確認します。

注記

チェックさ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パネルに表示されません。

-
5. 「保存」をクリックして設定を保存します。

12.2.2 マルチターゲットタイプ検出の表示

Multi-Target-Type Detectionは、対応するパラメータを設定した後、検出された情報（キャプチャカメラのライブビュー、キャプチャ画像、ターゲット詳細、ターゲット量、およびアラーム詳細を含む）を表示することをサポートします。

注記

この機能はデバイスでサポートする必要があります。



図12-5 マルチターゲット検出画面

ライブビュー

シングルチャンネルモード、デュアルチャンネルモード、または4チャンネルモードでライブビューを表示することができます。何か重要なことが起きたときに、ライブビューウィンドウのツールバーを使って、すばやく写真を撮影したり、録画を開始したりできます。また、パノラマ詳細表示の場合は、右クリックでPTZコントロールや3Dポジションを行うこともできます

。

人体・車両以外

撮影した人体/車両以外の写真がターゲットのハイライトボックスとともに表示されます。また、撮影したターゲットの機能が写真とともに表示されます。

捕捉面分析

顔の特徴(年齢層、性別、メガネ着用など)が表示されている顔画像を表示します。

自動車

撮影した自動車の写真を表示し、プレートNo、車色、車種などの車の特徴を表示します。

顔面認知/頻回に出現する/まれに出現する人

顔の比較や顔の武装化の結果、見知らぬ人の撮影した顔の写真、撮影した顔の人体、出現頻度などを表示します。

- 2つの顔が一致している場合は、顔画像ライブラリに、撮影した顔画像と類似した顔画像を表示します。
- フェイスピクチャライブラリのフェイスピクチャと一致しない撮影したフェイスピク

チャを表示します。

注記

不明人物認識をするための装置では、撮影した顔を顔画像ライブラリーの写真と比較します。顔写真ライブラリーで顔と顔が一致しない場合は、見知らぬ人として認識されます。

-
- 撮影した人体写真については、人物の顔写真も表示されます。
 - 出現頻度:出現時間がしきい値より長い出現頻度の人が表示され、出現頻度がしきい値より小さい出現頻度の人が表示されます。

注記

アラーム情報をクリックすると、最後に撮影した顔画像、外観量、アラーム時刻などの個人情報が表示されます。検出した人物を顔画像ライブラリーに追加します。

12.3 AI オープンプラットフォーム

AI Open Platformは、サードパーティのソフトウェアアプリケーション、アルゴリズムなどにアクセスできるソフトウェアプラットフォームです。このようにして、異なるインテリジェント・オブジェクトをネットワークで接続することができ、より多くのソフトウェア開発者がこのプラットフォームで効率的に動作することができます。


12.3.1 プラットフォームパラメータの設定

AI Open Platformに表示するインテリジェントデバイスをクライアントに追加できます。AI Open Platformでは、モデルパッケージの取得、表示するカメラの選択、画像保存用の保存パスの設定、保存モードの設定ができます。

ローカル・ストレージの設定

アラーム情報や画像をローカルパスに保存したり、保存パスや保存モードを設定することができます。

ステップ

1. 「AI ダッシュボード」をクリックし、「AI オープンプラットフォーム」を選択します。
2. 右上隅をクリックして、「ローカル・ストレージ設定」ウィンドウを開きます。

- ローカルストレージをONに設定します。
- 保存パスの入力ボックスをクリックして、保存パスを選択します。

注記

保存領域が2Gより大きいことを確認します。それ以外の場合は画像を保存できません。

- ストレージ・モードを選択します。

オーバーラップ先頭アラーム(各チャンネルで最大10,000個)

このモードでは、チャンネルごとに10000件(写真を含む)までのアラームを保存でき、保存領域がいっぱいの場合、新しいアラームと写真が最も早いアラームと重なります。

重複しないこと

このモードでは、チャンネルごとに10000件(写真含む)までのアラームを保存でき、保存領域がいっぱいの場合新しいアラームや画像は保存されません。

- OKをクリックします。

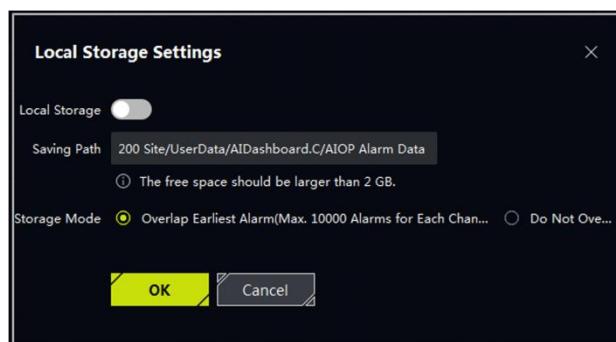


図12-6 ローカルストレージの設定

モデルパッケージの取得

モデルパッケージは、データメモリプールのようなもので、アラーム情報をより正確にするために、カメラがデータを学習し分析するためのルールとアルゴリズムを設定します。モデルパッケージは、デバイスで作成できます。デバイスによってモデルパッケージが変更された場合、デバイスからモデルパッケージを同期させて、データ情報を一致させることができます。

ステップ


- 「AI ダッシュボード」をクリックし、「AI オープンプラットフォーム」を選択します。

2. 右上隅をクリックして、カメラ選択画面を開きます。
3. モデルパッケージを入手するためにカメラを確認します。
4. OKをクリックします。

表示するカメラを設定する

デフォルトでは、AIオープンプラットフォームはすべてのカメラからアラーム情報を受信します。次のように設定できます
警報受信用フィルターカメラ


ステップ

1. 右上隅をクリックして、カメラ選択画面を開きます。
2. アラームが表示されていることを確認します。
3. OKをクリックします。

12.3.2 ピクチャータスクの解析

AI Open Platformは、画像内のオブジェクトを分析し、認識することができます。クライアントは、設計されたパスからオフライン画像を取得して、各画像に固有のIDを割り当て、その画像をデバイスに適用することができます。装置は、画像を分析し、結果(例えば、オブジェクト分類、属性)を表示するためにクライアントにフィードバックする。

ステップ

1. AIダッシュボードを入力します。
2. 「AI Open Platform」を選択します。
3. ページの右上隅をクリックします。Offline Picture Analysisウィンドウがポップアップされます。
4. オフライン画像を保存するフォルダパスを設定します。

注記

画像がJPG形式であること、および各画像が2MB未満であることを確認します。
定義(定義は64×64以上)

-
5. [Device]を選択してオフライン画像を分析します。

注記

オフライン画像解析機能対応機器のみがドロップダウンリストに表示されます。

6. モデルパッケージの分析に使用するデバイスエンジンを選択します。
7. オプション:認識されたターゲット上のフレームを表示するには、ターゲットフレームの表示をチェックします。
8. オプション:分析するターゲットの検出フレームを設定し、精度を向上させます。

注記

装置エンジンタイプが単一の分類(例えば、車両検出のためのエンジンのみ)である場合、検出フレームを設定します。

9. 「開始」をクリックする。

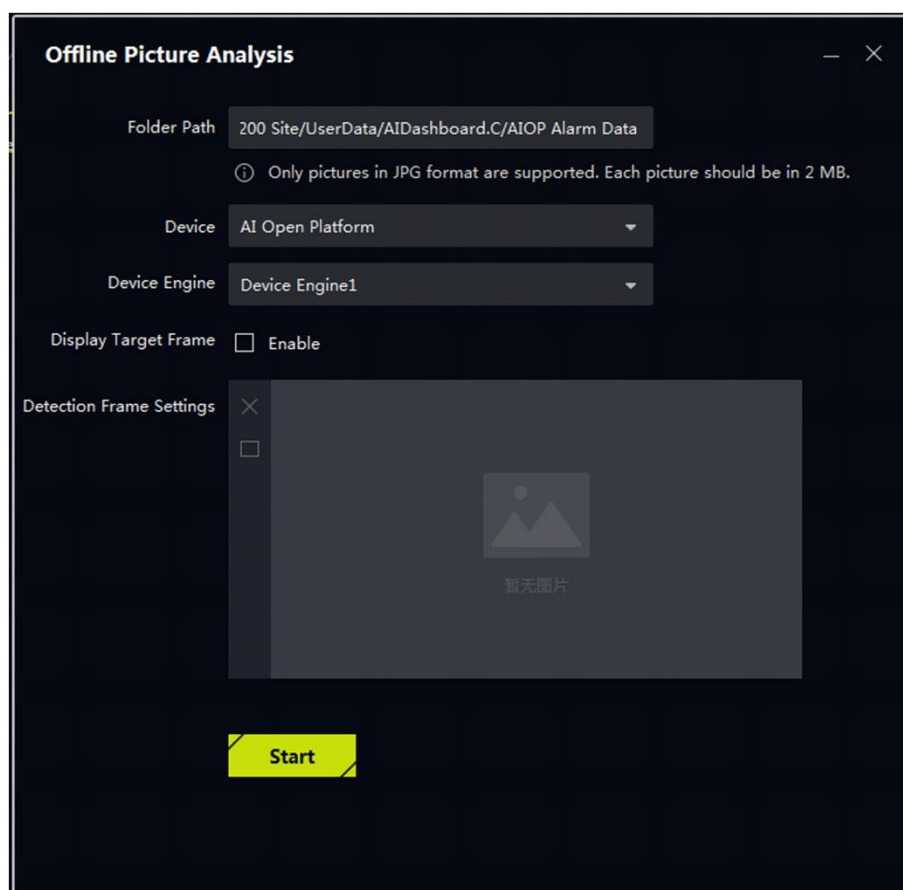


図12-7 オフライン画像分析

12.3.3 AI プラットフォームのリアルタイム表示

AIプラットフォームでは、カメラのライブ映像を表示したり、機器からアップロードした画像やアラーム情報を表示することができます。

AIプラットフォームでは、サーベイランスシーンをモデルによって学習されたシーンと比較し、結果を生成する。アラーム画像、カメラ情報、アラーム時刻、カテゴリ、検出結果が表示されます。オブジェクトが認識されると、カーソルをオブジェクトに移動してカテゴリまたは検出結果を表示し、アラームピクチャをクリックして詳細を表示することができます。

ライブビューウィンドウは、1ウィンドウまたは4ウィンドウに切り替えることができます。ウィンドウは、隠すこともポップアップすることもできます。ウィンドウのポップアップ後、ウィンドウを最大化して表示または復元することができます。

12.4 連動キャプチャアラーム

デバイスの2つのチャンネル(1つの固定チャンネルと1つのPTZチャンネル)を同時に表示することができます。アラームが発生したときに、パノラマ画像と撮影した画像を同時に見ることができます。




この機能はデバイスでサポートされている必要があります。

12.4.1 動作パラメータの設定

キャプチャ保存機能を手動で有効/無効にしたり、キャプチャした画像の保存パスを設定することで、キャプチャした画像をパソコンで見ることができます。

ステップ



1. AIダッシュボードモジュールを入力します。
2. 「アラーム連動」を選択すると、「アラーム連動」画面が表示されます。
3.  をクリックすると設定画面が表示されます。
表示されたコンテンツの紹介が示す。
4. ピクチャの保存をオンにすると、画像保存機能が有効になります。
5. 「保存パス」をクリックして、撮影し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されたときに撮影された画像は設定された状態で保存されます。

12.4.2 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すると、固定カメラがアラームに関連したパノラマ画像を撮影し、これがパノラマ連動アラーム画面に表示され、連動したPTZカメラがアラーム

の詳細画像を撮影し、連動したチャンネルアラーム画面に表示されます。このようにして、ユーザはパノラマ画像を、詳細を同時に表示して表示する。

一般的には、固定カメラのライブビューはパノラマチャンネルのライブビューウィンドウ、固定カメラに接続されたPTZカメラのライブビューはリンクされたチャンネルのライブビューウィンドウで表示します。

1. AIダッシュボードを入力し、リンクされたキャプチャアラームを選択して、リンクされたキャプチャアラームウィンドウを開きます。
2.  をクリックすると、デバイスリストが展開されます。
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、カーソルをカメラ名に移動してクリックします。

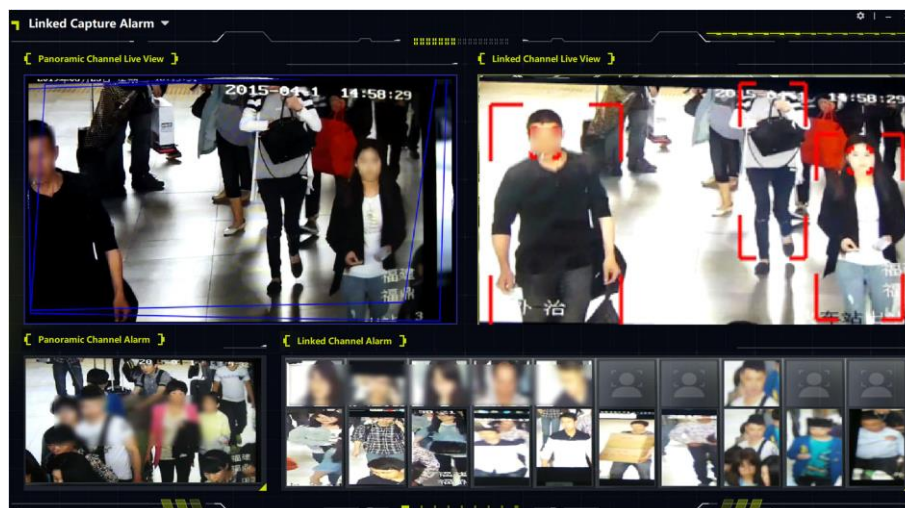


図12-8 ライブビューとアラームの表示

12.5 交通事故警報

インテリジェントトラフィックデバイス(例えば、トラフィック速度ドーム)は、道路上で発生したトラフィック違反または異常トラフィックイベントのリアルタイムライブビューのためにクライアントに追加することができます。カメラが事故を感知すると、カメラは写真を撮影し、写真と事故警報をクライアントにアップロードします。これは、強制するのに便利です。クライアントは、強制警報、交通事故警報および道路交通警報を表示することができます。


12.5.1 表示パラメータの設定

交通事故事象の表示パラメータを設定することができます。これはライブビューウィンドウの右側に表示されます。Save Picture機能を有効にすると、画像をダブルクリックして元の画像を表示できます。Save Picture機能が有効になっていない場合は、画像をダブルクリックして交通事故イベントアラームを表示できます。クライアントに追加された交通機器の交通事故警報ルールを設定できることを確認してください。

開始前に

クライアントに追加された交通機器の交通事故警報ルールを設定できることを確認してください。

ステップ

1. 「AIダッシュボード」→「交通事故警報」の順に選択して、交通事故警報ページに入ります。
2. ページの右上隅をクリックして、パラメータ設定ページを入力します。

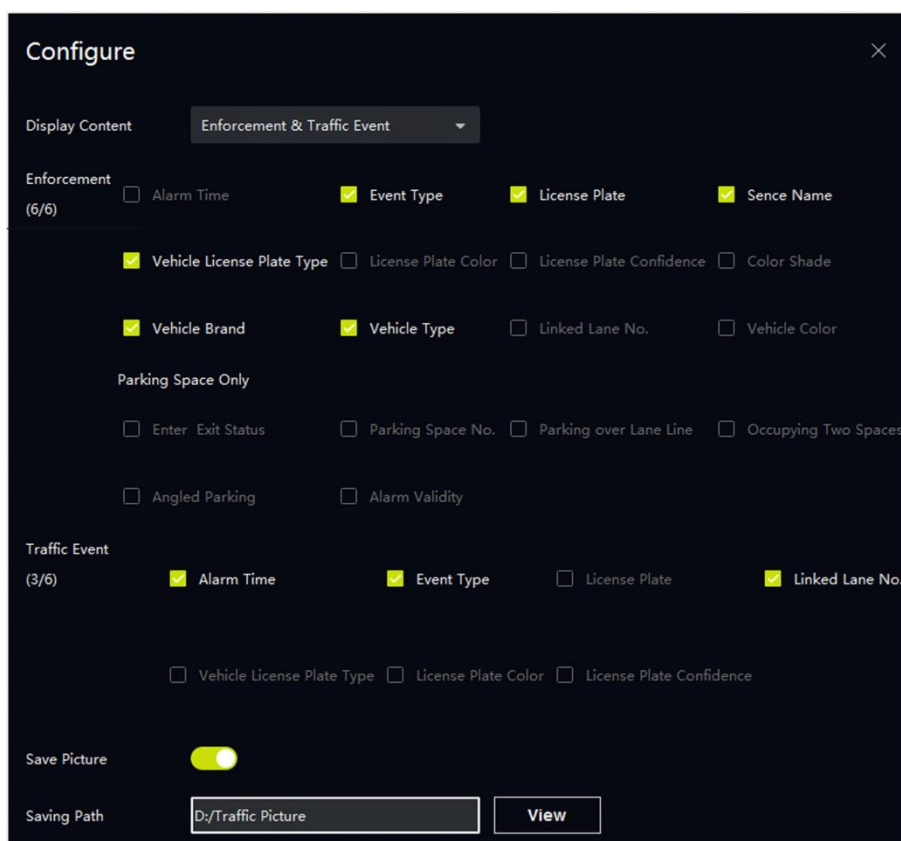


図12-9 パラメータ設定ページ

3. ドロップダウンリストをクリックし、[Enforcement & Traffic Event]などの[Display

Content]を選択します。

- 表示内容のパラメータを設定します。

例

たとえば、レーン・ライン上の駐車、角度の付いた駐車を選択して強制することができます。

注記

表示は最大6項目まで選択できます。

- オプション:Save Pictureを有効にして保存パスを設定します。
- 保存をクリックします。

12.5.2 交通事故警報の表示

交通事故警報モジュールでは、リアルタイムの交通監視画面を表示したり、交通機器がトリガした警報情報を受信したりすることができます。監視ビデオを1チャンネルまたは2チャンネルで表示し、対応するカメラから執行警報、交通事故警報、道路警報を表示できます。

「AIダッシュボードトラフィック」→「事故イベント」を選択して、「交通事故イベント」ページに入ります。

ページの左側をクリックしてライブビュー用のカメラを選択します、



図12-10 交通事故警報



ライブビューウィンドウ

ライブビューウィンドウには、リアルタイムのトラフィック監視ビデオが表示されます。右下隅の1または2をクリックして、ウィンドウの分割を設定します。同時に見ることができ

るカメラは2台までです。

注記

メインストリームモードで1台または2台のカメラのライブビデオを表示します。ストリームスイッチに対応していません。

ライブウィンドウの右下隅をクリックして、カメラのビデオ  またはキャプチャ画像  を手動で記録します。

トラフィックイベントの表示

交通イベント、強制交通イベント、道路交通イベントのパラメータ情報をリアルタイムで表示します。アラーム時刻、車種、イベント種別など、イベントごとに最大6つのパラメータを表示できます。

12.6 皮膚表面温度

特殊なシーンでは、人体の皮膚表面温度を監視することができます。クライアントが皮膚表面温度の異常またはマスクなしのアラーム情報を受信すると、アラームオーディオまたはポップアップウィンドウのリンクがトリガされます。マスクの着用や皮膚温の測定が必要なシーンに適しています。




注記

機能は装置がサポートする必要があります。

12.6.1 皮膚表面温度の表示

「皮膚表面温度」ページでは、ライブビューの人物を表示し、温度が異常な人物、正常な人物、マスクが装着されていない人物の統計番号を取得できます。顔画像比較、温度測定画像、顔キャプチャアラーム、過去のキャプチャ画像のアラーム情報を表示することもできます。

「AIダッシュボード」→「皮膚表面温度」をクリックして、「皮膚表面温度」ページに入ります。Skin-Surface Temperatureページでライブビューを開始します。

- クリック 左パネル  でカメラをダブルクリックすると、カメラのライブビデオが表示されます。
- クリック 左側のパネル  でカメラ  の右側をクリックして、カメラのライブビデオ

を表示します

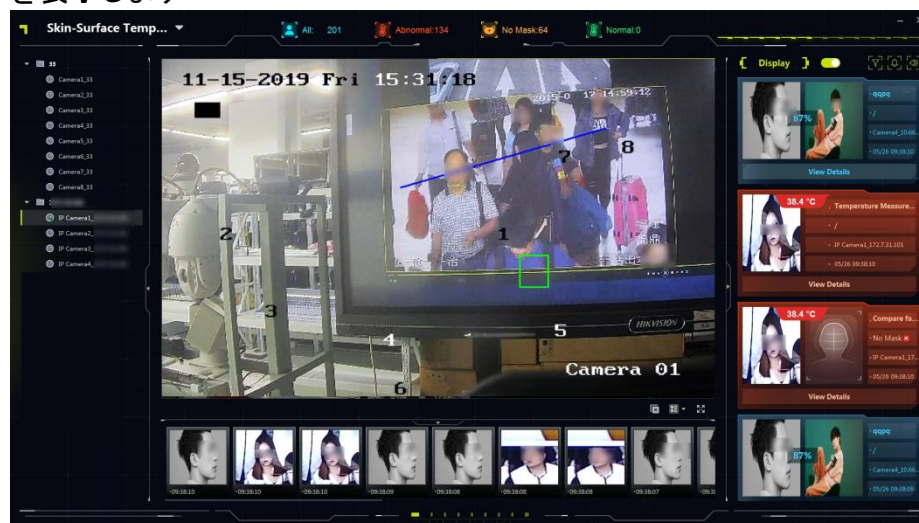



図12-11 皮膚表面温度ページ

12.6.2 皮膚表面温度情報表示

「皮膚-表面温度」ページでは、右側領域に表示するアラームの種類(顔比較アラーム、温度測定画像、顔捕捉アラーム)を選択できます。人数の統計値がページ上部に表示されます。撮影した顔画像がページ下部に表示されます。受信したアラームの音声連動ファイルを設定します。

情報表示を有効にする

クライアントに表示するアラームの種類(顔比較アラーム、温度測定画像、顔キャプチャアラーム)を選択します。アラームの種類は、異なる色で区別されます。

1. Skin-Surface Temperatureページで、表示する  アラームの種類を選択します。
顔比較アラーム

有効にすると、キャプチャされた顔画像と顔画像ライブラリの比較画像が表示され、関連する分類(人名、見知らぬ人、認識されていない人など)もライブラリに表示されます。[詳細の表示]をクリックして、個人名、性別、ID番号などの詳細な個人情報を表示します。

温度測定写真

有効にすると、測定した温度がキャプチャした顔画像に表示され、アラームは正常または異常として色分けされます。



顔写真アラーム

検知エリアで検知した顔画像を表示します。

2. 「表示スイッチ」を「ON」にすると、イベント情報が正しいエリアに表示されます。

表 12-1 異なる色の説明

ピクチャ	説明
	<p>青色は温度情報がないことを示します。 以下の場合、青色が表示されます:</p> <ul style="list-style-type: none"> 皮膚表面温度情報なし+マスク装着 皮膚表面温度情報なし+マスク属性がデバイスによって検出されない
	<p>緑色は体温が正常であることを示します。 以下の場合、緑色が表示されます:</p> <ul style="list-style-type: none"> 正常な皮膚表面温度 + 摩耗マスク 正常な皮膚表面温度+マスク属性がデバイスによって検出されない
	<p>黄色はマスクを着用していないことを示します。 次の場合は黄色で表示されます:</p> <ul style="list-style-type: none"> マスクなし+正常皮膚表面温度 マスクなし+本体は温度測定機能をサポートしていません。

	<p>赤は皮膚の温度が異常であることを示します。</p> <p>次の場合、赤色が表示されます:</p> <ul style="list-style-type: none"> • 皮膚表面温度異常+摩耗マスク • 皮膚表面温度異常+マスクなし • 皮膚表面温度異常+マスク属性がデバイスによって検出されない
	<p> 注記</p> <p>皮膚表面温度異常の閾値は、本体に設定することができます。</p>

統計人数

「皮膚表面温度」ページでは、クライアントは、受信したアラームに基づいて人数を計算し、合格者数、スキン温度が異常な人数、およびマスクを着用していない人数を取得します。

注記


表示スイッチを「ON」にすると、リアルタイム統計値の人数が表示されます。


- すべて:皮膚表面温度ページで受信したアラームの総数。
- 異常:皮膚温が異常な人の数。皮膚温が異常な人を検出すると、異常な温度のアラームが鳴り、異常数と異常数を1ずつ加算します。
- マスクなし:ライブビューでマスクを着用していない人の数。マスクを装着していない人を検出すると、「マスクなし」のアラームが発生し、「マスクなし」と「すべて」の数字に1が加算されます。
- 正常:皮膚温が正常なライブビューの人数。皮膚温が正常な人を検出すると、正常温度のアラームが鳴り、正常とすべての数が1ずつ加算されます。

撮影した顔画像の表示

Skin-Surface Temperatureページの下部には、撮影した顔画像をリアルタイムで表示できます。

 注記

- 表示スイッチを「ON」にすると撮影した顔画像をリアルタイムで受信・表示できます。
- 表示されるのは、顔比較アラーム、温度計測アラーム、顔キャプチャアラームのキャプチャした顔画像です。少なくとも1つのアラームが選択されていることを確認します。

キャプチャした顔画像の下にスライダをドラッグして、前のキャプチャした顔画像を表示します。キャプチャした顔画像の下部にある顔画像をクリックして、顔画像ライブラリに追加し、人物情報を入力します。


オーディオリンク設定

受信したアラームに音声リンクファイルを設定します。

1. 「皮膚表面温度」ページの右上隅をクリックします。
2. 各種アラームのオーディオリンクを有効にするには、スイッチを[ON]にします。


 注記

デフォルトでは、すべてのアラーム(マスクなし、常温、異常温度)のオーディオリンクが有効になっています。

3. クリック 「.wav」のオーディオファイルの選択オーディオファイルを変更するフォーマット

 注記

オーディオファイルをクライアントの設計されたパスにアップロードします。

「オーディオ設定」ウインドウをクリックして、クライアントの設計されたパスを表示します。

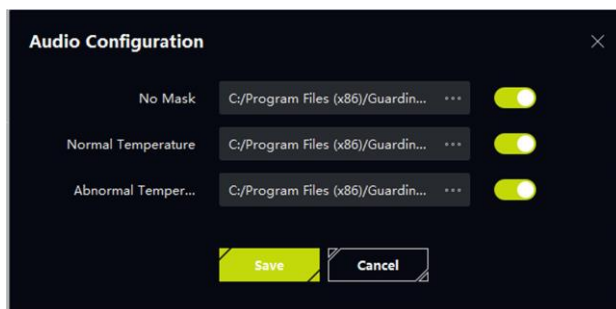


図12-12 オーディオ設定

12.6.3 アラーム情報の表示

皮膚表面温度の異常またはマスクなしのアラームを検出すると、アラームポップアップウィンドウがトリガされ、アラーム情報が表示されます。また、ウィンドウのポップアップ時間を設定することができ、アラーム情報の表示時間を柔軟に制御することができます。



図12-13 アラームポップアップウィンドウ

マスクなし

アラームウィンドウがポップアップし、マスクを装着していない人の顔写真が撮影されます。

温度異常

アラームウィンドウがポップアップし、皮膚の表面温度が異常な人の撮影した顔画像が表示されます。




注記

温度異常アラームの優先度がマスク無しアラームの優先度より高い。「マスクなし」と

「温度異常」の両方が有効になっている場合、クライアントが「no」のアラームを受信したときマスク、温度異常、温度異常警報画面がポップアップし、温度異常の音声が発生されます。(有効になっている場合。詳細は参照)

注記

- アラーム情報を表示する前に、必ずアラーム情報の受信を有効にしてください。詳細は、「デバイスからの受信イベントの有効化」を参照してください。
- 警報ウィンドウのポップアップを受信する前に、必ず警報ポップアップウィンドウを有効にしてください。皮膚表面温度のページで、右上隅をクリックして「アラームポップアップウィンドウ」のウィンドウをポップアップし、設定します。

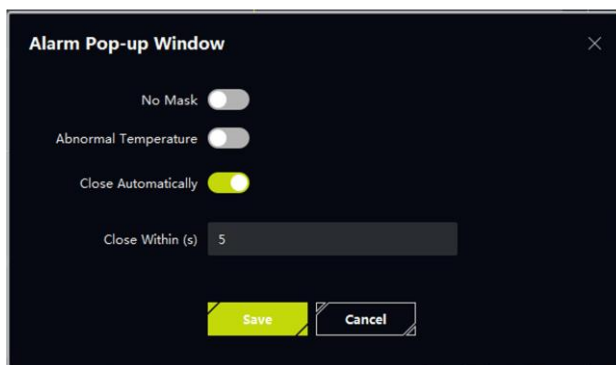


図12-14 アラームポップアップウィンドウの設定

第 13 章 セキュリティ制御パネル

セキュリティ・コントロール・パネルは、事前に定義された仮想領域に入っている人、車両などを検出し、イベントを起動し、イベント情報(イベントの場所など)をセキュリティ・スタッフに報告します。イベントセンターモジュールは、クライアント経由でパーティションとゾーンのエントリ管理とリモートコントロールを提供します。イベント管理ページでクライアント・アクションを構成した後、イベントが発生したときにクライアントに通知を受信します。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くても、クライアント側でパーティションや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コントロール、デバイスのアームング & ディスアームングには許可が必要です。ユーザー許可の設定の詳細については、「ユーザーの追加」を参照してください。

13.1 フローチャート

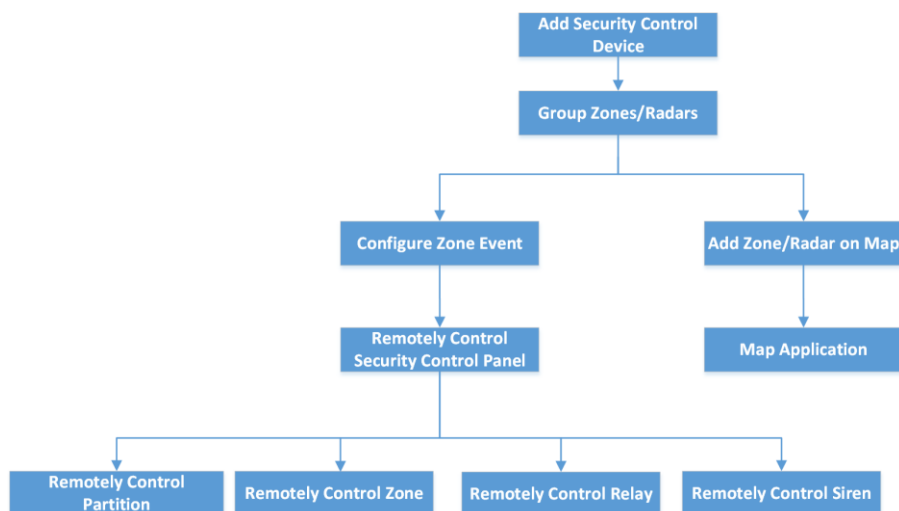


図13-1 セキュリティコントロールパネルのフローチャート

- **セキュリティ制御装置の追加:** クライアントにセキュリティ制御装置を追加できます。詳細については、「デバイスの追加」を参照してください。
- **Group Zones/Radars:** 追加したゾーン/レーダーをグループに分けて管理しやすくします。詳細については、「グループ管理」を参照してください。
- **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されたアクションを設


定すると、イベントがトリガされると通知されます。詳細については、「ゾーンイベントのクライアントリンクの設定」を参照してください。

- **Remotely Control Security Panel:** パーティションを含むリモート セキュリティコントロール パネルを使用できます。ゾーン、リレー、サイレン詳細については、リモートコントロールセキュリティコントロールパネルを参照してください。
- **マップ上のゾーン/レーダーの追加:** マップにゾーン/レーダーをホットスポットとして追加できます。詳細については、「Add Zone as Hot Spot」および「Add Security Radar as Hot Spot」を参照してください。
- **マップアプリケーション:** リソースの検索、アラーム情報の表示、および関連する制御を実行できます。マップ管理を参照してください。

13.2 セキュリティコントロールパネルをリモート設定する

クライアントにセキュリティ制御パネルを追加した後、リモート設定ページに移動して、クライアント経由でデバイスの関連パラメータを設定できます。クラウドP2Pによって追加されたデバイスの場合、2回目の検証が有効な場合は、リモート設定のためにデバイスのユーザー名とパスワードを入力する必要があります。バッチ装置のメンテナンスシナリオに広く使用されている。例えば、インストーラは、クラウドP2Pアカウントを介してログインし、エンドユーザのデバイスをリモートで維持することができます。

ステップ

1. Device Management → Device → Deviceを選択します。
2. 追加したセキュリティコントロールパネルを選択し、「操作」列をクリックします。 
3. オプション:2回目の検証が有効なデバイスの場合、デバイスのユーザー名とパスワードを入力し、[OK]をクリックします。

結果

リモート設定ページが表示されます。

13.3 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でも、クライアントでゾーンイベントのリンクされたアクションを設定することで、何が起きているのか、またそのイベントがゾーン内でどのように緊急に発生しているのかを知ることができます。イベントがトリガーされると、クライアントに通知されます。これにより、イベントに即座に応答できます。また、バッチ内の複数のゾーンのクライアントアクションを一度に設定することもできます。

開始前に

- セキュリティコントロールパネルが追加されていることを確認します。
- あらかじめゾーンが定義されていることを確認する。

- イベントが事前に設定されていることを確認します。

ステップ

1. [イベント設定]→[アラームイベント]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つ以上のイベントをチェックします。
4. 「リンクの編集」をクリックして、クライアント・アクションを構成します。

音声警告

クライアントソフトウェアは、イベントがトリガされたときに、可聴警告を発生します。警報音を選択して警報を聞くことができます。



注記

「追加」をクリックしてアラーム音名を入力し、パソコンで音を選択します。詳細はこちら
アラーム音を設定する。

メールを送る

アラーム情報の電子メールを1つ以上の受信者に送信します。電子メールパラメータの設定方法については、「電子メールパラメータの設定」を参照してください。

ポップアップウィンドウ

イベントがトリガされたときに、イベント関連情報(イベントの詳細、リンクされたカメラの撮影画像、プロセスレコード、およびプロセスフィールドを含む)をソフトウェアクライアントに表示するポップアップウィンドウ。

マップ表示

イベントソースがマップ上のホットスポットとして追加されると、イベントがトリガーされたときに、ホットスポットは赤色の番号(イベントの数を示し、最大数は10)で表示され、警備員がイベントの場所を確認するのに役立ちます。

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

連動カメラ

ゾーンイベントが発生したときに、選択したカメラをリンクして撮影します。ドロップダウンリストからカメラを選択します。

 注記

ゾーンイベントの連動カメラは最大4台まで選択できます。

5. **オプション:** [Edit Priority]をクリックして、イベント優先度を [Uncategorized]/[Low]/[Medium]/[High]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(イベント優先度、起動クライアントを含む)をコピーします。アクション、およびイベントの他のゾーンへの有効化/無効化
 7. リンケージカメラとリンケージPTZを設定します。
-

 注記

- リンクされたカメラは、選択したプリセットに回転したり、選択したパトロールやパターンを実行したりします。
レーダーの検知エリアでアラームが発生した場合。
 - この機能はデバイスでサポートされている必要があります。
-

- 1) 連動カメラ一覧でカメラを確認します。
 - 2) リンクPTZをオンにすると、機能が有効になります。
下に表示されているレーダーに連動したカメラ。
 - 3) カメラを選択し、右側のドロップダウンリストからプリセット/パトロール/パターンを選択します。プリセット/パトロール/パターンリストが表示されます。
-

 注記

カメラのプリセット、パトロール、パターンを設定していることを確認します。

- 4) プリセット、パトロール、またはパターンを選択します。
8. OKをクリックします。
9. **オプション:** 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。
 - Enable AllまたはDisable Allをクリックして、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「ON/OFF」に切り替えます。

クライアント・アクションを使用可能にする

クライアント・アクションが使用可能になると、クライアントがゾーン・イベントを受信すると、クライアント・アクションが起動されます。

クライアント・アクションの無効化

クライアント・アクションが無効の場合、クライアント・アクションは動作せず、クライアントがゾーン・イベントを受信したときにアクションが起動されません。

10. 保存をクリックします。

13.4 リモートコントロールセキュリティコントロールパネル

クライアントにセキュリティ制御パネルを追加した後、クライアントソフトウェアを介して、セキュリティ制御パネルのパーティション、ゾーン、リレー、およびサイレンをリモートで制御できます。たとえば、パーティションとゾーンの両方で、アーム、アーム解除、バイパス、グループバイパスなどを使用することができ、リレーを有効または無

注記

効にすることもできます。

- 表示されるインタフェースは、追加されたセキュリティコントロールパネルの種類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をサポートしません。

13.4.1 リモートコントロールパーティション

セキュリティコントロールパネルのパーティションでは、クライアントを使用して、離脱アーミング、滞在アーミング、即時アーミング、解除、アラームクリア、グループバイパス、グループバイパスなどの操作をリモートで実行できます。

ステップ

注記

- サポートされている機能は、追加されたデバイスの対象となります。
- パーティションのゾーンが機能しない場合は、アーム/ディスアームする前にバイパスする必要があります。
区画をパーティション化し、ゾーンが動作したときにバイパスを復元します。

1. セキュリティコントロールパネルモジュールを入力します。
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、ステータス、アーミングステータス、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、以下のボタンをクリックします。

アウェイ・アーミング

監視対象領域にすべての人がいない場合に動作する軍備モード。アーミングを有効にすると、パーティションのすべてのゾーンが正常に動作します。

ステイ・アーミング

モニターされている領域に人がいるときに動作するアーミングモード。state armingを有効にすると、地域内のゾーンは武装化され、地域外のゾーンはバイパスされ、イベントをトリガすることなくゾーン内を移動できます。

インスタント・アーミング

パーティションをアームした後、イベントがトリガされると、そのゾーンは即座にアラームされます。

Disaring

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)は、クリックしても動作しなくなるため、非武装ゾーンではイベントは発生しません。

注記

24時間帯(例えば、24時間通知ゾーン、24時間サイレントアラームゾーンなど)は、パーティションが解除された場合でも、イベントを検出し、アラームを鳴らすことができます。

アラームクリア

警報装置の警報を停止する。

グループ・バイパス

1つ以上のパーティションのすべてのゾーンをバイパスすると、グループ・バイパス・リカバリーの前に、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なります。

注記

パーティションをバイパスする前に、パーティションを解除する必要があります。

グループ・バイパス回収

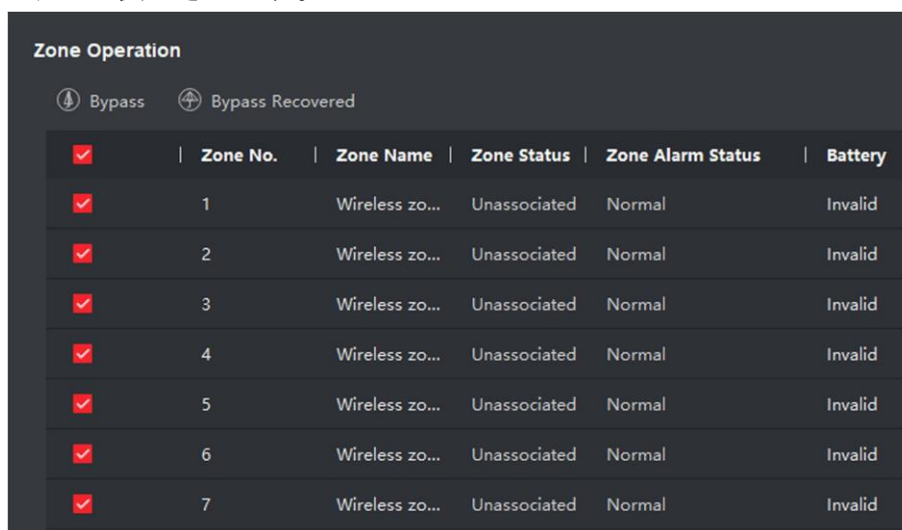
グループバイパスを復元して、パーティション内のすべてのゾーンを作成し、グループをアームできるようにします。

13.4.2 リモートコントロールゾーン

クライアントを使用して、バイパスおよびリカバリを含むセキュリティコントロールパネルのゾーンをリモートで制御できます。

ステップ

1. セキュリティコントロールパネルモジュールを入力します。
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、ステータス、アームステータス、リンクゾーンがリストに表示されます。
3. クリックすると、ゾーン操作パネルが開きます。🔍
区画、ゾーン番号、ゾーン名、ゾーンステータス、ゾーンアラームステータスにリンクされているゾーン。
バッテリーが表示されます。



Zone Operation					
🔍 Bypass		🔄 Bypass Recovered			
<input checked="" type="checkbox"/>	Zone No.	Zone Name	Zone Status	Zone Alarm Status	Battery
<input checked="" type="checkbox"/>	1	Wireless zo...	Unassociated	Normal	Invalid
<input checked="" type="checkbox"/>	2	Wireless zo...	Unassociated	Normal	Invalid
<input checked="" type="checkbox"/>	3	Wireless zo...	Unassociated	Normal	Invalid
<input checked="" type="checkbox"/>	4	Wireless zo...	Unassociated	Normal	Invalid
<input checked="" type="checkbox"/>	5	Wireless zo...	Unassociated	Normal	Invalid
<input checked="" type="checkbox"/>	6	Wireless zo...	Unassociated	Normal	Invalid
<input checked="" type="checkbox"/>	7	Wireless zo...	Unassociated	Normal	Invalid

図13-2 ゾーン操作

ゾーンステータス

ゾーンステータスは、関連付けされていない、武装している、武装解除されている、故障している、遮蔽されている、不正防止されているなどの可能性があります。

バッテリー

ゾーンの検出器の出力。

4. リスト内の1つ以上のゾーンをチェックし、以下のボタンをクリックします。

バイパス

ゾーンがバイパスされると、ゾーン内でイベントはトリガされず、ゾーンのアームまたは解除は許可されず、他のゾーンはアームまたは解除されます。



ゾーンをバイパスする前に、ゾーンを解除する必要があります。

バイパス回収

ゾーンのバイパスを復旧した後、アームを作動させることができます。

13.4.3 リモートリレー

クライアントを使用して、リレーのオン/オフ状態をリモートで変更し、リレーのリンクされたイベントを表示することができます。

ステップ

1. セキュリティコントロールパネルモジュールを入力します。
2. セキュリティコントロールパネルを選択し、「リレー」をクリックします。
リレーの名前、ステータス、リンクイベントが表示されます。
3. 1つまたは複数のリレーをチェックし、「開く」または「閉じる」をクリックします。



Axiom Hub では、Relay Associated Event を Device Management モジュールの Manual Control に設定します。

13.4.4 リモートコントロールサイレン

サイレンの状態は、オープン、クローズを含めてクライアントから遠隔操作することができます。サイレンの状態が開いていると、検出されたアラームがサイレンのアラーム音を鳴らします。

Security Control Panel モジュールを入力し、Security Control Panel を選択し、「Siren」タブをクリックします。サイレンを 1 つまたは複数選択し、「開く」または「閉じる」をクリックして、サイレンを開閉します。

第 14 章 人事管理

アクセス制御、ビデオインターホン、時間、出勤などの操作を行うために、個人情報システムに追加できます。追加した個人を管理することができます。たとえば、一括でカードを発行したり、一括で個人情報をインポートしたりエクスポートしたりできます。

14.1 組織の追加

組織を追加し、組織に個人情報をインポートして、有効にすることができます。者の管理また、追加した組織のサブディネートを追加することもできます。

ステップ

1. 「個人」モジュールを入力します。
2. 左側の列で親組織を選択し、左上隅の「追加」をクリックして追加します。


組織

3. 追加した組織の名前を作成します。

注記

追加できる組織のレベルは10までです。

4. オプション:以下の操作を行います。

編集組織 追加した組織上でマウスを移動し、クリックしてその名前を編集します。 

削除組織 マウスを追加した組織の上に置いてクリックして削除します。 

注記

- 下位組織も削除すると削除されます。
組織
 - 組織の下に追加された人物がないこと、または以下の人物がないことを確認します。
組織は削除できません。
-

サブ組織内の人物を表示する 「サブ組織の人物を表示」をチェックし、そのサブ組織の人物を表示する組織を選択します

14.2 独身者の追加

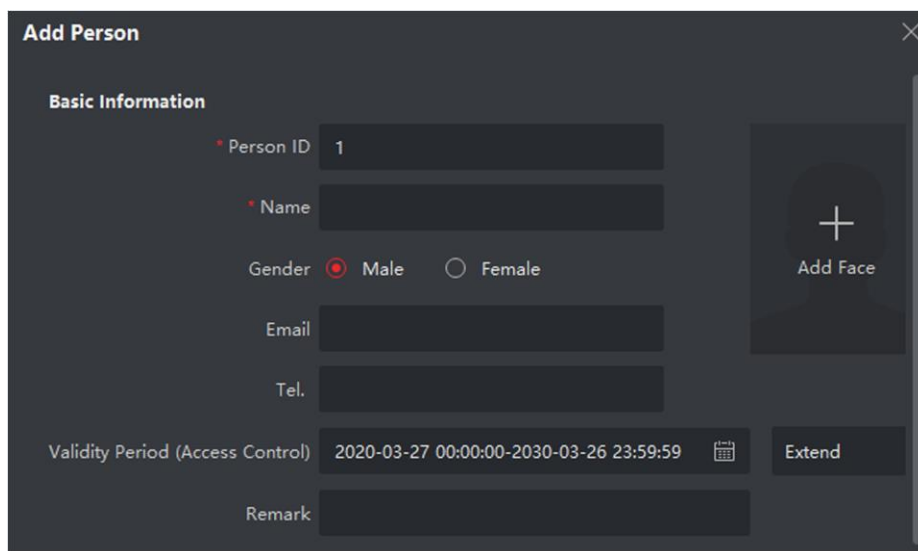
クライアントソフトウェアに個人を1人ずつ追加できます。個人情報には、基本情報、詳細情報、プロフィール、アクセス制御情報、信任状、カスタム情報などが含まれます。

14.2.1 基本情報の設定

クライアントに個人を1人ずつ追加し、名前、性別、電子メール、電話番号などの個人の基本情報を設定できます。

ステップ

1. 「個人」モジュールを入力します。
2. 組織リストから組織を選択し、個人を追加します。
3. 「追加」をクリックして、個人の追加ウィンドウを開きます。個人IDが自動的に生成されます。
4. 人名、性別、電話番号、メールアドレス、有効期限などの基本情報を入力します。



The screenshot shows a dark-themed 'Add Person' dialog box. The 'Basic Information' section contains the following fields: 'Person ID' with the value '1', 'Name' (empty), 'Gender' with radio buttons for 'Male' (selected) and 'Female', 'Email' (empty), 'Tel.' (empty), 'Validity Period (Access Control)' with a date range '2020-03-27 00:00:00-2030-03-26 23:59:59' and a calendar icon, and 'Remark' (empty). On the right side, there is a large '+' button labeled 'Add Face'. At the bottom right, there is an 'Extend' button.

図14-1 基本情報の設定

注記

有効期間が過ぎると、その人の資格情報とアクセス制御設定は無効になり、その人はドア¥floorsにアクセスする権限を持たなくなります。「延長」をクリックすると、1ヶ月、

3ヶ月、6ヶ月、1年の有効期間を延長できます。

5. 追加を確認します。

- 追加をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
- 「追加」および「新規」をクリックして、個人を追加し、他の個人を引き続き追加します。

14.2.2 1人にカードを発行する

人物を追加するときは、カードをクレデンシャルとして彼/彼女に発行してドアにアクセスすることができます。1人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取得する必要があります。手動でカード番号を入力する場合を除き、クライアントは以下の2つのモードを提供します。

ローカルモード(カード登録端末経由)またはリモートモード(アクセス制御装置のカードリーダー経由)でカード番号を読み取る。



1人に5枚まで発行できます。

カード番号を入力してカードを発行

カード番号を読み取ることができる機器(カード登録ステーション/カードリーダー)がない場合は、手動でカード番号を入力してカードを発行できます。

ステップ

1. 「個人」モジュールを入力します。
2. 組織リストで組織を選択して個人を追加し、「追加」をクリックして「個人の追加」パネルを入力します。



まず、本人の基本情報を入力します。個人の基本設定の詳細と情報については、「基本情報の設定」を参照してください。

3. [Credential]→[Card]領域で、+をクリックします。

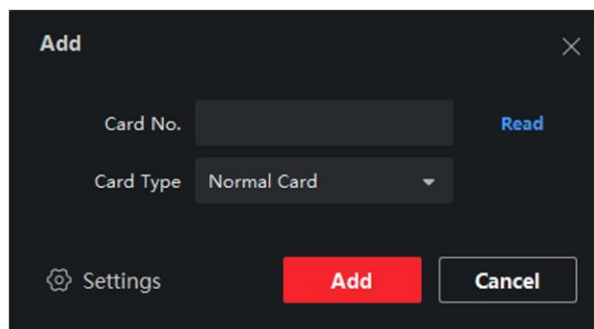


図14-2 カードページの追加

4. [追加]ページに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。
カードは本人に発行されます。

ローカルモードでカードを発行する

カード登録ステーションがある場合は、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、USBインターフェースまたはCOMでカード登録ステーションをクライアントが動作しているパソコンに接続し、カード登録ステーションにカードを置く必要があります。

ステップ

1. 「個人」モジュールを入力します。
2. 組織リストで組織を選択して個人を追加し、「追加」をクリックして「個人の追加」パネルを入力します。



注記

まず、本人の基本情報を入力します。個人の基本設定の詳細については情報については、「基本情報の設定」を参照してください。

3. [Credential]→[Card]領域で、+をクリックします。
4. 「設定」をクリックして、「設定」ページに入ります。
5. カード発行モードとしてローカルを選択します。

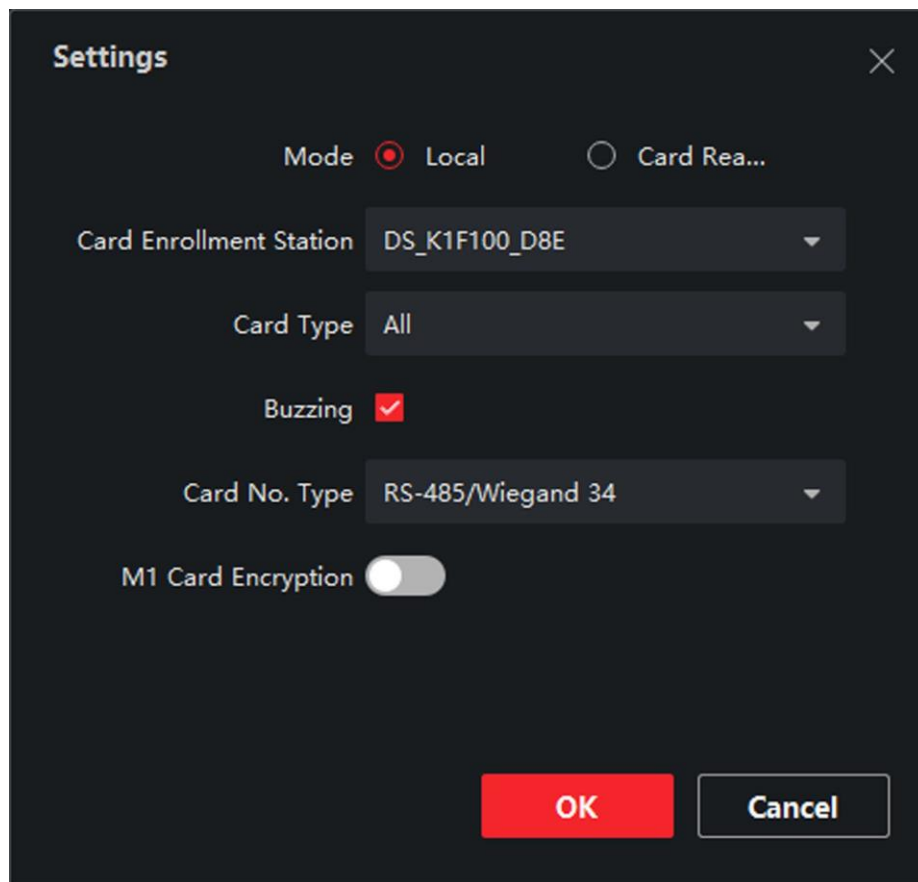


図14-3 ローカルモードでカードを発行する

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局の機種を選択します。

注記

現在、サポートされているカード登録ステーションモデルには、DS-K1F100-D8、DS-K1F100M、DS-K1F100-D8E、DS-K1F180-D8Eがあります。

カードの種類

このフィールドは、モデルがDS-K1F100-D8EまたはDS-K1F180-D8Eの場合にのみ使用できます。実際のカードの種類に合わせて、カードの種類をEMカードまたはMifareカードとして選択します。

バジング

カード番号の読み取りに成功した場合は、ブザー音を有効または無効にします。

カード番号タイプ

カード番号の種類は、必要に応じて選択してください。

M1カードの暗号化

このフィールドは、モデルがDS-K1F100-D8、DS-K1F100-D8E、またはDS-K1F180D8Eの場合にのみ使用できます。カードがM1カードの場合、M1カード暗号化機能を有効にし、暗号化するカードのセクタを選択できます。

7. [OK]をクリックして動作を確認します。
8. カードをカード登録ステーションに置き、「読み取り」をクリックしてカード番号を取得します。カード番号欄にカード番号が自動的に表示されます。
9. 追加をクリックします。
カードは本人に発行されます。

リモートモードでのカード発行

ローカルモードでカードを発行する場合を除き、追加したアクセス制御装置のカードリーダーにカードを押し付けてカード番号を取得することもできます。これは、クライアントと発行者が同じ場所にいない場合に適用される。たとえば、支社の従業員にカードを発行するには、クライアント経由でリモートモードを使用します。

ステップ

1. 「個人」モジュールを入力します。
2. 組織リストで組織を選択して個人を追加し、「追加」をクリックして「個人の追加」パネルを入力します。



注記

まず、本人の基本情報を入力します。個人の基本設定の詳細については情報については、「基本情報の設定」を参照してください。

3. [Credential]→[Card]領域で、+をクリックします。
4. 「設定」をクリックして、「設定」ページに入ります。
5. カード発行モードはカードリーダーを選択します。

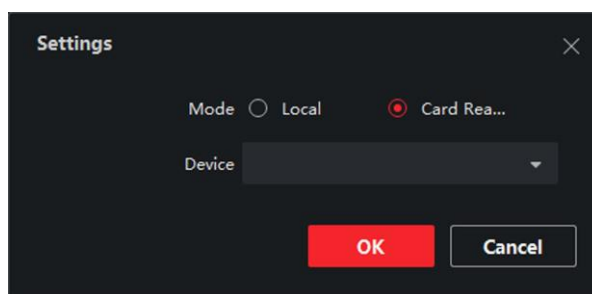


図14-4 リモートモードでカードを発行する

6. クライアントに追加されたアクセス制御デバイスを選択します。
7. ドロップダウン・リストから、追加されたアクセス制御装置または登録ステーションを選択します。

i 注記

登録ステーションを選択する場合は、「ログイン」をクリックして、IPアドレス、ポート番号、ユーザー名、およびパスワードを含むデバイスの関連パラメータを設定する必要があります。また、必要に応じてRFカードの種類を確認してください。

8. [OK]をクリックして動作を確認します。
9. カードリーダーにカードをセットし、「読む」をクリックしてカード番号を取得します。カード番号欄にカード番号が自動的に表示されます。
10. 追加をクリックします。
カードは本人に発行されます。

14.2.3 ローカル PC から顔写真をアップロードする

個人を登録するときは、ローカルPCに保存されている顔写真を個人としてクライアントにアップロードできます。

プロファイル

ステップ

1. 「個人」モジュールを入力します。
2. 組織リストから個人を追加する組織を選択し、「追加」をクリックします。

i 注記

まず、本人の基本情報を入力します。個人の基本設定の詳細については情報については、「基本情報の設定」を参照してください。

3. 「基本情報」パネルの「顔の追加」をクリックします。
4. Uploadを選択します。
5. クライアントを実行しているPCから画像を選択します。



注記

画像はJPGまたはJPEG形式で、200Kバイト未満にしてください。

6. オプション:クライアントで管理されている顔認識装置が写真の顔を認識できるかどうかを確認するために、装置による検証を有効にします。
7. 追加を確認します。
 - 追加をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
 - 「追加」および「新規」をクリックして個人を追加し、他の個人を追加し続けます。

14.2.4 お客様での撮影

人物を追加するときは、クライアント経由で写真を撮影し、その写真を人物のプロフィールとして設定することができます。

開始前に

クライアントを実行しているパソコンにカメラが装備されているか、他のUSBカメラをパソコンに接続していることを確認します。

ステップ

1. 「個人」モジュールを入力します。
2. 組織リストで組織を選択して個人を追加し、「追加」をクリックして「個人の追加」ウィンドウを入力します。



注記

まず、本人の基本情報を入力します。詳細は、「基本情報の設定」を参照してください。

3. 「基本情報」領域の「顔の追加」をクリックします。
4. Take Photoを選択して、Take Photoウィンドウに入ります。
5. オプション:キャプチャした顔写真がアップロード要件を満たしているかどうかを確認するために、「デバイスによる検証」を有効にします。
6. 写真を撮ってください。
 - 1) カメラに顔を向け、顔がコレクションウィンドウの中央にあることを確認します。
 - 2) クリックすると顔写真が撮影されます。📷
 - 3) オプション:再度取り込みをクリックします。🔄
 - 4) OKをクリックして、撮影した写真を保存します。

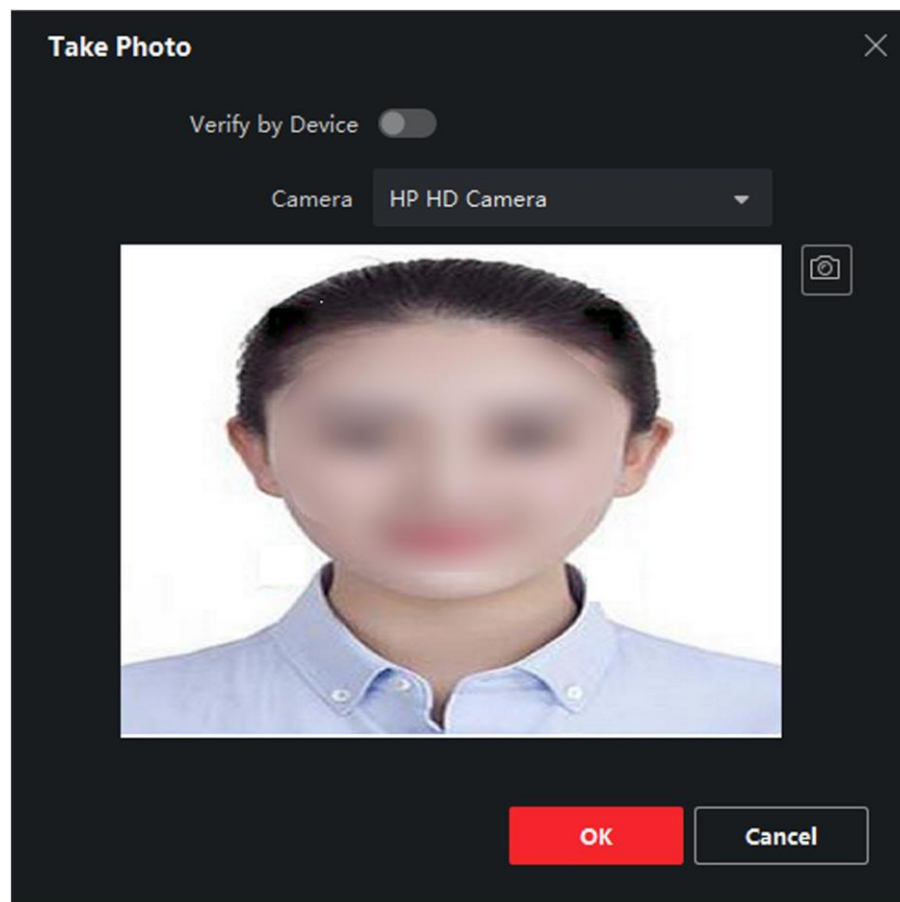


図14-5 クライアント経由での写真撮影

7. 追加を確認します。
- 追加をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
 - 「追加」および「新規」をクリックして、個人を追加し、他の個人を引き続き追加します。

14.2.5 アクセス制御装置による顔の収集

人物を追加するときは、顔認証機能をサポートするアクセス制御装置をクライアントに追加することで、人物の顔を収集することができます。

ステップ

1. 「個人」モジュールを入力します。
2. 組織リストから個人を追加する組織を選択し、「追加」をクリックします。

 注記

まず、本人の基本情報を入力します。個人の基本設定の詳細や情報については、「基本情報の設定」を参照してください。


3. 「基本情報」パネルの「顔の追加」をクリックします。
4. リモートコレクションを選択します。
5. ドロップダウン・リストから、追加されたアクセス制御装置または登録ステーションを選択します。

 注記

登録ステーションを選択する場合は、「ログイン」をクリックして、IPアドレス、ポート番号、ユーザー名、およびパスワードを含むデバイスの関連パラメータを設定する必要があります。また、Face AntiSpoofingをチェックし、Low、Medium、Highのいずれかのライブレベルを選択できます。

顔のなりすまし防止

この機能をチェックすると、収集する顔が次のようなものであるかどうかを検出できます。
本物のもの。

6. 顔を集める。
 - 1) 選択したアクセス制御装置のカメラに顔を向け、顔がコレクションウィンドウの中央にあることを確認します。
 - 2) クリックすると写真が撮影されます。
 - 3) OKをクリックして、撮影した写真を保存します。
7. 追加を確認します。
 - 追加をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
 - 「追加」および「新規」をクリックして個人を追加し、他の個人を追加し続けます。

14.2.6 クライアント経由で指紋を収集

ローカルで指紋を収集するということは、クライアントを実行しているPCに直接接続された指紋レコーダを介して指紋を収集することができます。記録された指紋は、許可されたドアにアクセスするための人物の証明書として使用することができます。

開始前に

クライアントを実行しているPCに指紋レコーダーを接続します。

ステップ

1. 「個人」モジュールを入力します。

2. 組織リストから個人を追加する組織を選択し、「追加」をクリックします。



注記

まず、本人の基本情報を入力します。個人の基本設定の詳細や情報については、「基本情報の設定」を参照してください。

3. 信任状→指紋パネルで、+をクリックします。
4. ポップアップウィンドウで、収集モードをローカルに選択します。
5. 接続している指紋レコーダーの機種を選択します。



注記

指紋レコーダーがDS-K1F800-Fの場合は、「設定」をクリックしてCOMを選択できません。
フィンガープリントレコーダーが接続する。

6. 指紋を採取する。
 - 1) 「開始」をクリックする。
 - 2) 指紋記録装置に指紋を置いて持ち上げ、指紋を回収します。
 - 3) 「追加」をクリックして、記録された指紋を保存します。
7. 追加を確認します。
 - 追加をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
 - 「追加」および「新規」をクリックして、個人を追加し、他の個人を引き続き追加します。

14.2.7 アクセス制御装置による指紋の収集

個人を追加する場合は、アクセス制御装置の指紋モジュールから指紋情報を収集することができます。記録された指紋は、許可されたドアにアクセスするための人物の証明書として使用することができます。

開始前に

指紋採取がアクセス制御装置でサポートされていることを確認します。

ステップ

1. 「個人」モジュールを入力します。
2. 組織リストから個人を追加する組織を選択し、「追加」をクリックします。



注記

まず、本人の基本情報を入力します。個人の基本設定の詳細や情報については、「基本情報の設定」を参照してください。

3. 信任状→指紋パネルで、+をクリックします。
4. ポップアップウィンドウで、リモートとして収集モードを選択します。
5. ドロップダウン・リストから、追加されたアクセス制御装置または登録ステーションを選択します。

 注記

登録ステーションを選択する場合は、「ログイン」をクリックし、デバイスのIPアドレス、ポート番号、ユーザー名、およびパスワードを設定します。

6. 指紋を採取する。
 - 1) 「開始」をクリックする。
 - 2) 選択したアクセス制御装置の指紋スキャナに指紋を置いて持ち上げ、指紋を収集します。
 - 3) 「追加」をクリックして、記録された指紋を保存します。
7. 追加を確認します。
 - 追加をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
 - 「追加」および「新規」をクリックして個人を追加し、他の個人を追加し続けます。

14.2.8 アクセス制御情報の設定

個人を追加するときに、アクセス・コントロール・グループをその人と結び付ける、PINコードを設定する、その人をビジター、ブラックリストの人、スーパーユーザとして設定する、などのアクセス・コントロール情報を設定することができます。

ステップ

1. 「個人」モジュールを入力します。
2. 組織リストから個人を追加する組織を選択し、「追加」をクリックします。
3. Access Control 領域で、個人のアクセス・グループを選択するためにクリックします。▼

 注記

詳細については、「アクセス許可を個人に割り当てるアクセスグループの設定」を参照してください。

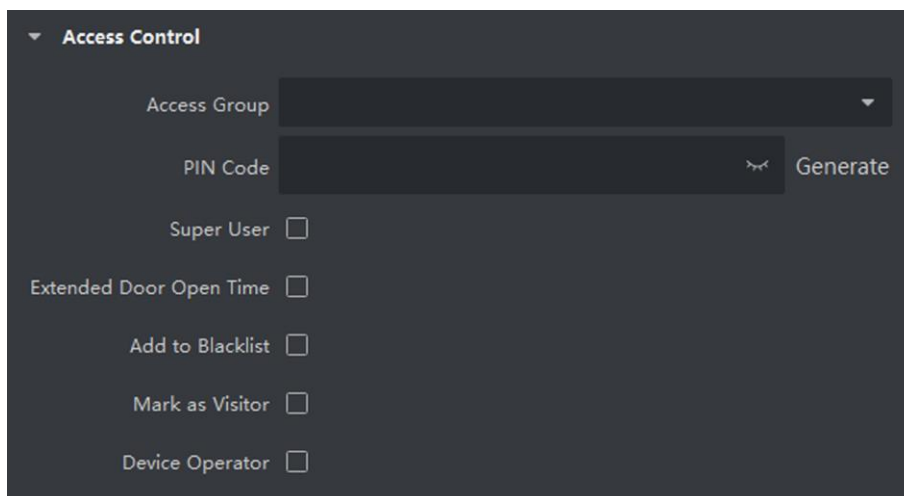


図15-6 アクセス制御情報の設定

4. アクセス認証に使用できる個人固有のPINコードを設定します。
 - 4～8桁のPIN1コードを手動で入力します。

 注記

本人の暗証番号は繰り返せません。

- 「生成」をクリックして、6桁のPINコードをランダムに生成します。

 注記

PINコードが繰り返されると、クライアントにプロンプトが表示されます。管理者は、繰り返されるPINコードに代わる新しいPINコードを生成し、関係者に通知することができます。

5. 操作許可を確認してください。

スーパー・ユーザー

スーパーユーザーに設定されている場合は、すべてのドア/フロアにアクセスする権限を持ち、残りの閉鎖制限、すべてのパスバック防止規則、および一人目の許可を免除されます。

拡張ドア開放時間

動きの悪い方にご使用ください。ドアにアクセスすると、他の人よりもドアを通過する時間が長くなります。

ドアのオープン時間の設定については、ドア/エレベータの設定パラメータを参照してください。

ブラックリストに追加

ブラックリストに人物を追加し、人物がドア/フロアにアクセスしようとする時、イベントがトリガーされてクライアントに送信され、保安要員に通知されます。

ビジターのマーク

ビジターの場合は、ビジターの有効時間を設定してください。



注記

来院の有効期限は1～100です。また、「制限なし」をチェックすると、訪問者がドア/フロアにアクセスする時間が制限されません。

デバイスオペレータ

デバイス・オペレータの役割を持つ者については、アクセス・コントロール・デバイスを操作する権限が与えられています。



注記

Super User、Extended Door Open Time、Add to Blacklist、Mark as Visitor機能は同時に有効にすることはできません。例えば、スーパーユーザに設定されている人は、拡張ドアオープン時間を有効にしたり、ブラックリストに追加したり、ビジターに設定したりすることはできません。

6. 追加を確認します。

- 追加をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
- 「追加」および「新規」をクリックして、個人を追加し、他の個人を引き続き追加します。

14.2.9 個人情報のカスタマイズ

クライアントであらかじめ定義されていない個人情報を、実際のニーズ(出生地など)に応じてカスタマイズできます。カスタマイズ後、個人を追加すると、カスタム情報を入力して、個人情報を完全にすることができます。

ステップ

1. 「個人」モジュールを入力します。
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、新しい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. 個人を追加するときのカスタム情報を設定します。
 - 1) 組織リストから個人を追加する組織を選択し、「追加」をクリックします。



まず、本人の基本情報を入力します。個人の基本設定の詳細については情報については、「基本情報の設定」を参照してください。

- 2) [カスタム情報]パネルで、個人情報を入力します。
- 3) 「追加」をクリックして個人を追加し、「個人の追加」ウィンドウを閉じるか、「追加」と「新規」をクリックして個人を追加し、他の個人を追加し続けます。

14.2.10 住民情報の設定

ビデオインターホンの目的で、居住者の場合、部屋番号を設定し、屋内局を拘束する必要があります。バウンド後は、室内局を呼び、ビデオインターホンを行って呼び出すことができます。

ステップ

1. 「個人」モジュールを入力します。
2. 組織リストから個人を追加する組織を選択し、「追加」をクリックします。



まず、本人の基本情報を入力します。個人の基本設定の詳細や情報については、「基本情報の設定」を参照してください。

3. 「住民情報」パネルで、屋内局を選択し、人物にバインドします。



アナログ室内局を選択すると、ドアステーション欄が表示され、アナログ室内局と通信するドアステーションを選択する必要があります。

4. 本人の床番号、部屋番号を入力する。
5. 追加を確認します。
 - 追加をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
 - 「追加」および「新規」をクリックして、個人を追加し、他の個人を引き続き追加します。

14.2.11 追加情報の設定

人物を追加するときは、人物のような人物の追加情報を設定できます。実際のニーズに応じた識別タイプ、識別番号、国など。

ステップ

1. 「個人」モジュールを入力します。
2. 組織リストから個人を追加する組織を選択し、「追加」をクリックします。



まず、本人の基本情報を入力します。個人の基本設定の詳細や情報については、「基本情報の設定」を参照してください。

3. Additional Informationパネルには、実際の必要に応じて、個人のIDタイプ、ID番号、職位などの個人の追加情報を入力します。
4. 追加を確認します。
 - 追加をクリックして個人を追加し、「個人の追加」ウィンドウを閉じます。
 - 「追加」および「新規」をクリックして個人を追加し、他の個人を追加し続けます。

14.3 本人確認情報の輸出入

複数の人物の情報や写真を一括してクライアントソフトウェアにインポートできます。また、個人情報や画像をエクスポートしてパソコンに保存することもできます。

14.3.1 個人情報のインポート

定義済みのテンプレート(CSV/Excelファイル)に複数の個人の情報を入力して、バッチ内のクライアントに情報をインポートすることができます。


ステップ

1. Personモジュールを入力します。
2. リストで追加した組織を選択するか、左上隅の「追加」をクリックして追加します。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. インポートモードとして「個人情報」を選択します。
5. 「個人のインポート用テンプレートのダウンロード」をクリックして、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個人情報を入力します。



- 複数のカードがある場合は、カード番号をセミコロンで区切ります。

- アスタリスクが付いた項目が必要です。
- デフォルトでは、雇用日が現在の日付になります。

7. クリックすると、ローカルPCから個人情報を含むCSV/Excelファイルを選択できます。
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**

- クライアントのデータベースに既にNo.が存在する場合は、事前に既存の情報を削除してください。
インポート
- インポートできる情報の数は、2,000人までです。


14.3.2 輸入者の写真

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、追加した顔認識端末で画像内の人物を識別することができます。人物の写真を1枚ずつ読み込むか、または必要に応じて複数の写真を一度に読み込むことができます。

開始前に

あらかじめ、お客様に個人情報をインポートしておいてください。

ステップ

1. Personモジュールを入力します。
2. リストで追加した組織を選択するか、左上隅の「追加」をクリックして追加します。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」をチェックします。
4. オプション:クライアントで管理されている顔認識装置が写真の顔を認識できるかどうかを確認するために、装置による検証を有効にします。
5. クリックして顔画像ファイルを選択します。

**注記**

- 顔写真(フォルダ)は、ZIP形式とする。
- 各画像ファイルはJPG形式とし、200Kバイト以下とする。
- 各画像ファイルには「Person ID_Name」という名前を付けてください。個人IDは、インポートした個人情報と同じである必要があります。

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。

14.3.3 個人情報のエクスポート

追加した個人情報をローカルPCにCSV/Excelファイルとしてエクスポートできます。

開始前に

組織に人員を増やしていることを確認しましょう。

ステップ

1. Personモジュールを入力します。
2. オプション:リスト内の組織を選択します。



組織を選択しない場合は、すべての個人情報がエクスポートされます。

3. Exportをクリックして、Exportパネルを開きます。
4. エクスポートするコンテンツとして個人情報をチェックします。
5. エクスポートする項目を確認します。
6. 「エクスポート」をクリックして、エクスポートしたファイルをPCのCSV/Excelファイルに保存します。

14.3.4 エクスポート者の写真

登録した人物の顔画像をエクスポートしてパソコンに保存できます。

開始前に

個人と顔の写真を組織に追加したことを確認します。

ステップ

1. Personモジュールを入力します。
2. オプション:リスト内の組織を選択します。



組織を選択しないと、すべての人物の顔写真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として「顔」をチェックします。
4. 「エクスポート」をクリックしてエクスポートを開始します。



- エクスポートされたファイルはZIP形式です。
- 書き出された顔画像は、“Person ID_Name_0” (“0”は正面の場合)と名付けられます。

14.4 アクセス制御装置からの個人情報の取得

追加したアクセス制御デバイスに個人情報(個人情報、指紋、発行済みカード情報を含む)が設定されている場合は、デバイスから個人情報を取得し、クライアントにインポートして操作を行うことができます。

ステップ

注記

- デバイスに格納されている個人名が空の場合は、クライアントにインポートした後、発行されたカードNo.が入力されます。
- 性別は、デフォルトで男性となる。
- デバイスに格納されているカード番号または個人ID (従業員ID)がすでにクライアントデータベースに存在する場合、このカード番号または個人IDを持つ個人はクライアントにインポートされません。

-
1. 「個人」モジュールを入力します。
 2. 個人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、追加されたアクセス制御装置または登録ステーションを選択します。

注記

登録ステーションを選択する場合は、「ログイン」をクリックし、デバイスのIPアドレス、ポート番号、ユーザー名、およびパスワードを設定します。

-
5. 「インポート」をクリックして、個人情報をクライアントにインポートします。

注記

最大2,000人、5,000枚のカードを輸入することができる。

人物情報(人物の詳細情報を含む)、人物の指紋情報(場合)
設定されているカード、および設定されている場合はリンクされているカードが選択した組織にインポートされます。

14.5 他の組織への人員移動

必要に応じて、追加した個人を別の組織に移動できます。

開始前に

- 少なくとも2つの組織を追加してください。
- 個人情報を入力したことを確認します。

ステップ

1. 「個人」モジュールを入力します。
2. 左パネルで組織を選択します。

組織の下にある人物が右側のパネルに表示されます。

3. 移動する相手を選択します。
4. [組織変更]をクリックします。
5. 移動先の組織を選択します。
6. OKをクリックします。

14.6 一括発行

クライアントは、一括して複数の人にカードを発行する便利な方法を提供します。

ステップ

1. 「個人」モジュールを入力します。
2. 「バッチ発行カード」をクリックします。

カードが発行されていない追加した個人は、すべて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(名前または個人ID)を入力し、発行カードを必要とする人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。詳しくは、「1人にカードを発行する」を参照してください。
5. 「初期化」をクリックして、カード登録ステーションまたはカードリーダーを初期化し、カードの発行準備を行います。
6. カード番号欄をクリックし、カード番号を入力します。
 - カードをカード登録ステーションに置きます。
 - カードリーダーでカードを読み取ります。
 - 手動でカード番号を入力し、Enterキーを押します。名簿に記載された者には、カードが交付される。

14.7 カード紛失報告

カードを紛失した場合は、カードが関連するアクセスができるようにカードの紛失を報告することができます。

許可は非アクティブになります。

ステップ

1. 「個人」モジュールを入力します。
2. カード紛失を報告したい人を選択し、「編集」をクリックして、「個人の編集」ウィンドウを開きます。
3. [クレデンシャル]→[カード]パネルで、追加したカードをクリックして、このカードを紛失カードに設定します。🔑

カード紛失を報告した後、このカードのアクセス権限は無効かつ非アクティブになります。このカードを受け取った他の人は、この紛失したカードを押し流すことではドアにアクセスできません。

4. オプション:紛失したカードが見つかった場合、クリックすると、紛失をキャンセルできます。🔑

カード紛失をキャンセルすると、その人のアクセス権限が有効かつ有効になります。

5. 紛失したカードが1つのアクセスグループに追加され、すでにアクセスグループがデバイスに適用されている場合、カードの紛失またはカードの紛失を報告した後、デバイスに変更を適用することを通知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、これらの変更はデバイスに有効になります。

14.8 リソース統計の表示

デバイスに個人およびアクセス・コントロールの信任状(顔、カード、および指紋を含む)を適用した後、クライアントおよびデバイスのリソース統計を表示して、リソースが正常に適用されたかどうかを知ることができます。デバイスに個人と信任状を適用している。詳細については、「アクセス許可を個人に割り当てるアクセスグループの設定」を参照してください。

[Person Management]→[Resource Statistics]の順にクリックして、[Resource Statistics] ウィンドウに入力します。

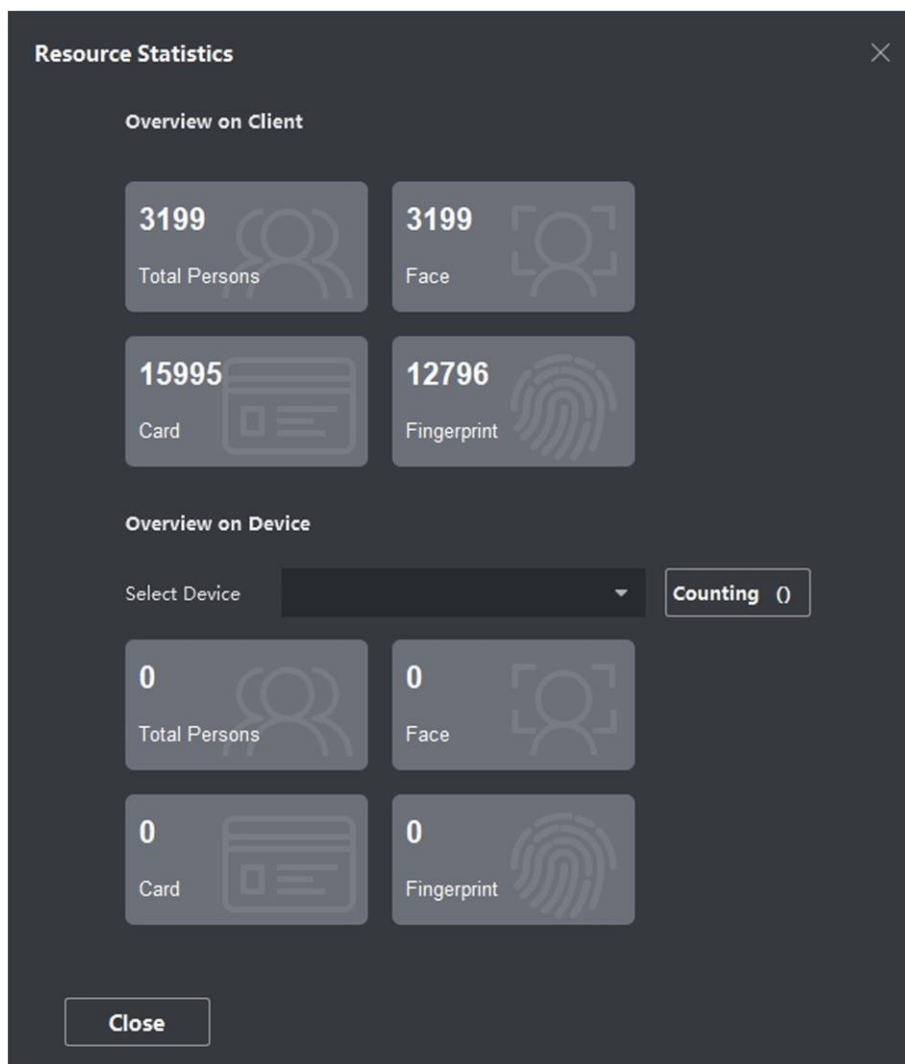


図14-7 クライアントの概要

「デバイスの概要」領域で、ドロップダウンリストからデバイスを選択し、「カウント」をクリックして、人、顔、カード、および指紋を含むデバイスリソースを表示します。クライアント上のリソースとデバイス上のリソースを比較することによって、クライアントリソースがデバイスに適用されたかどうかを知ることができます。

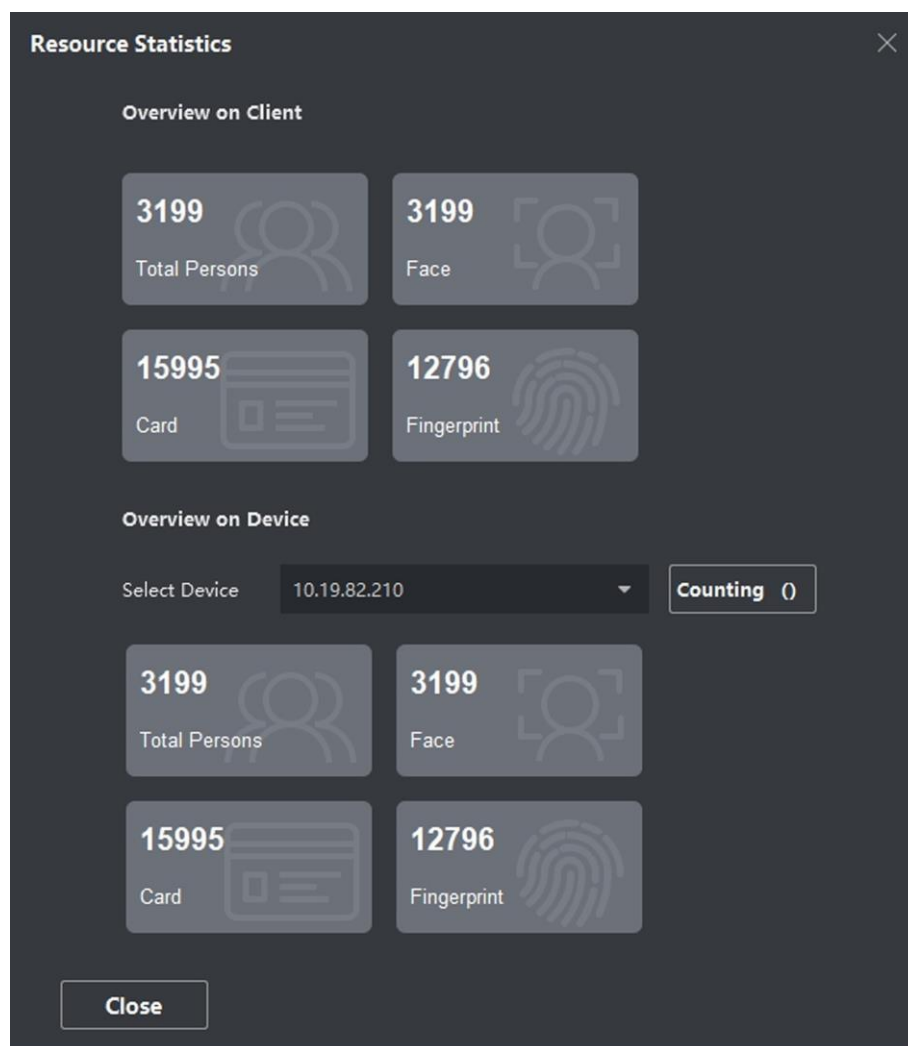


図14-8 デバイスに適用されるクライアント・リソース

i 注記

この機能はデバイスでサポートされている必要があります。デバイスが顔や指紋をサポートしていない場合は、PCデスクトップの右下隅にプロンプトが表示されます。

第15章 アクセス制御

アクセス・コントロール・モジュールは、アクセス・コントロール・デバイスおよびビデオ・インターホン・デバイスに適用できます。アクセスグループの設定、ビデオインターホン、その他の高度な機能を含む、複数の機能を提供します。

注記

アクセス・コントロール・モジュールのアクセス権を持つユーザーは、アクセス・コントロール・モジュールを入力してアクセス・コントロールの設定を行うことができます。アクセス・コントロール・モジュールのユーザー許可の設定については、「ユーザーの追加」を参照してください。

15.1 フローチャート

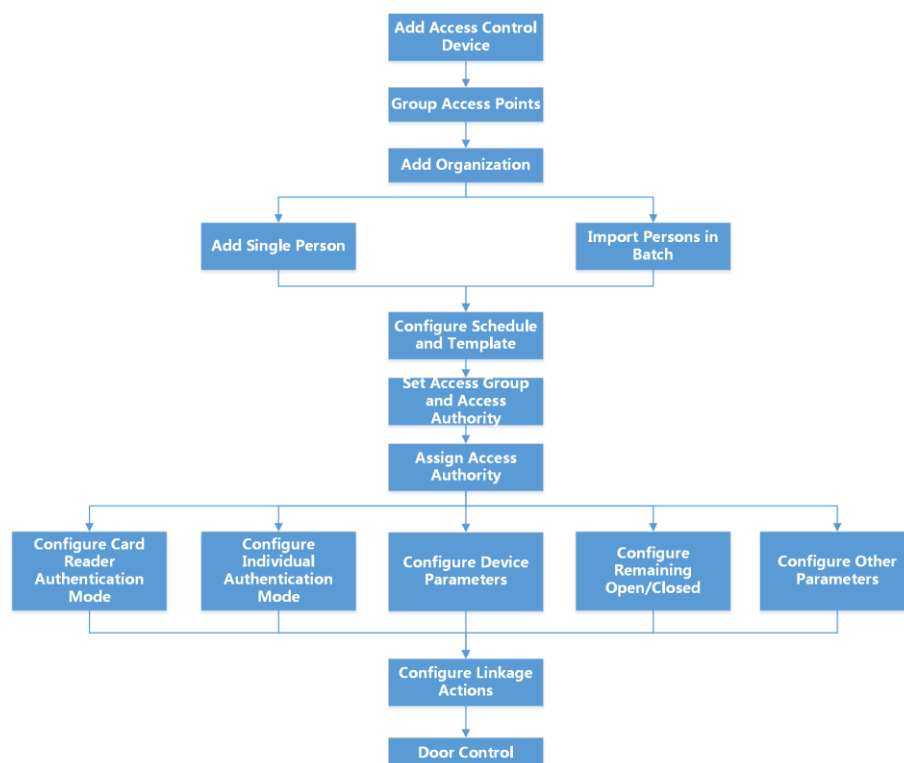


図 15-1 アクセス制御のフローチャート

- **Add Access Control Devices:** クライアントにアクセス・コントロール・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」を参照してください。

- **グループアクセスポイント**: 追加したアクセスポイントをグループにグループ化して管理することができます。詳細については、「グループ管理」を参照してください。
- **組織の追加**: 組織を追加したり、個人情報を入力したりできます。人を管理する組織詳細については、「組織の追加」を参照してください。
- **スケジュールとテンプレートの設定**: 休日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。詳細は、Configure Schedule and Template を参照してください。
- **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、どのドアにアクセスできるかを定義し、アクセスグループをアクセス制御デバイスに適用して有効にすることができます。詳細については、「アクセス許可を個人に割り当てるアクセスグループの設定」を参照してください。
- **デバイスパラメータの設定**: デバイス時間、リンク設定、メンテナンス設定など、アクセス制御デバイスのパラメータを設定できます。詳細については、以下を参照。
- **「残りの開閉」の設定**: ドアの状態を開または閉に設定し、エレベーター・コントローラーをフリーおよびコントロールに設定することができます。詳細については、「残りのオープン/クローズの設定」を参照してください。
- **カードリーダー認証モードの設定**: アクセス制御装置のカードリーダーの通過ルールは、実際のニーズに合わせて設定できます。詳細は、Configure Card Reader Authentication ModeとScheduleを参照してください。
- **個別認証モードの設定**: 実際の必要に応じて、指定されたアクセス制御デバイスへの個人の通過ルールを設定できます。詳細については、個人認証モードの設定を参照してください。
- **その他のパラメータの設定**: 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、Wiegandパラメータなどのアクセス制御デバイスのパラメータを設定できます。詳細については、以下を参照。
- **リンクアクションの設定**: アクセス制御用にリンクアクションを設定することができます。これにより、イベントが一連のリンクアクションを起動してセキュリティ担当者に通知することができます。詳細については、以下を参照。
- **ドア/エレベータ制御**: 追加されたアクセス制御装置によって管理されるドアまたはエレベータのリアルタイムの状態を表示することができます。詳細はドア・エレベータ制御を参照ください。

15.2 スケジュールとテンプレートの設定

休日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。テンプレートを設定した後、アクセスグループを設定するときに、設定されたテンプレートをグループにアクセスすることができます。これにより、アクセスグループは、テンプレートの継続時間内に有効になります。



注記

アクセス・グループの設定については、「アクセス・グループを個人にアクセス権限を割り当てる設定」を参照してください。

15.2.1 休日追加

休日を作成し、開始日、終了日、および休日を含む休日の日付を設定できます。
1日のデュレーション

ステップ



注記

ソフトウェアシステムでは、最大64日間の休日を追加できます。

1. [アクセスコントロール]→[スケジュール]→[休日]をクリックして、[休日]ページを入力します。
2. 左パネルの[Add]をクリックします。
3. 休日の名前を作成します。
4. オプション:この休日の説明または通知を[備考]ボックスに入力します。
5. 休日リストに休日期間を追加し、休日の継続時間を設定します。



注記

1日の休日には、最大16日間の休日を追加できます。

- 1) 「休日一覧」フィールドで「追加」をクリックします。
- 2) カーソルをドラッグして継続時間を描画します。これは、継続時間を意味します。
構成済みのアクセス・グループが活動化されます。





注記

最大8回まで、1休日に設定できます。

- 3) オプション:以下の操作を行って、継続時間を編集します。
 - カーソルをタイムデュレーションに移動し、カーソルが回転したときにタイムラインバーのタイムデュレーションを希望する位置にドラッグします。
 - 継続時間をクリックし、表示されたダイアログで開始/終了時刻を直接編集し

ます。

- 開始時間または終了時間にカーソルを移動してドラッグすると、カーソルが切り替わるまでの時間が長くなるか短くなります。
 - 4) オプション:削除する時間を選択し、クリックします。
選択した継続時間を削除する操作欄。
 - 5) オプション:  クリック「操作」列で、タイムバーのすべての継続時間をクリアします。 
 - 6) オプション: クリック「操作」欄には、この追加した休日の期間を休日リストから削除します。
6. 保存をクリックします。

15.2.2 テンプレートの追加

テンプレートには、週スケジュールと休日が含まれます。週スケジュールを設定し、アクセス許可の時間を個人またはグループごとに割り当てることができます。テンプレートに追加した祝日を選択することもできます。

ステップ

注記

ソフトウェアシステムでは、最大255個のテンプレートを追加できます。

1. [アクセスコントロール]→[スケジュール]→[テンプレート]をクリックして、[テンプレート]ページを入力します。

注記

デフォルトのテンプレートには、All-Day AuthorizedとAll-Day Deniedの2つがあり、編集や削除はできません。

授權終日

アクセス許可は、各曜日に有効で、休日はありません。

終日拒否

アクセス許可は、曜日毎に無効となり、休日はありません。

2. 左パネルの[追加]をクリックして、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通知を[備考]ボックスに入力します。
5. 週スケジュールを編集して、テンプレートに適用します。
 - 1) 下パネルの[Week Schedule]タブをクリックします。
 - 2) 曜日を選択し、タイムラインのバーに時間の継続時間を表示します。



注記

週スケジュールでは、1日につき8回まで設定できます。

- 3) オプション:以下の操作を行って、継続時間を編集します。
 - カーソルをタイムデュレーションに移動し、カーソルが回転したときにタイムラインバーのタイムデュレーションを希望する位置にドラッグします。
 - 継続時間をクリックし、表示されたダイアログで開始/終了時刻を直接編集します。
 - 開始時間または終了時間にカーソルを移動してドラッグすると、カーソルが切り替わるまでの時間が長くなるか短くなります。
- 4) 上記の2つのステップを繰り返して、週の他の日の時間をさらに引き出します。

6. 休日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最大4日間まで追加できます。

- 1) [休日]タブをクリックします。
- 2) 左側のリストで休日を選択すると、右側のパネルで選択したリストに追加されます。
- 3) オプション:「追加」をクリックして、新しい休日を追加します。



注記

休日の追加については、「休日の追加」を参照してください。

- 4) オプション:右側のリストで選択した休日を選択し、をクリックします。 選択した休日を削除するには、選択した休日を削除するには[クリア]をクリックします。
7. Save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。

15.3 アクセス許可を個人に割り当てるためのアクセスグループの設定

個人を追加し、個人の信任状を設定した後、どのドアにアクセスできるかを定義するためにアクセス・グループを作成し、アクセス・グループをアクセス・コントロール・デバ

イスに適用して有効にすることができます。

ステップ

アクセス・グループの設定を変更した場合、アクセス・グループを再度デバイスに適用する必要があります。アクセスグループの変更には、テンプレートの変更、アクセスグループの設定、個人のアクセスグループの設定、関係者の詳細(カード番号、指紋、顔写真、カード番号と指紋の連動、カード番号と指紋の連動、カードパスワード、カード有効期間など)が含まれます。

1. [アクセスコントロール]→[許可]→[アクセスグループ]をクリックして、アクセスグループインターフェースを入力します。
2. 「追加」をクリックして、「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、アクセス・グループの名前を必要に応じて作成します。
4. アクセスグループのテンプレートを選択します。

注記

テンプレートを設定してから、グループの設定を行ってください。詳細については、スケジュールとテンプレートの設定を参照してください。

5. [Select Person]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を選択します。
6. [アクセスポイントの選択]フィールドの左側のリストで、選択したアクセス対象のドア、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。

インターフェースの右側に、選択した個人と選択したアクセスポイントを表示できます。

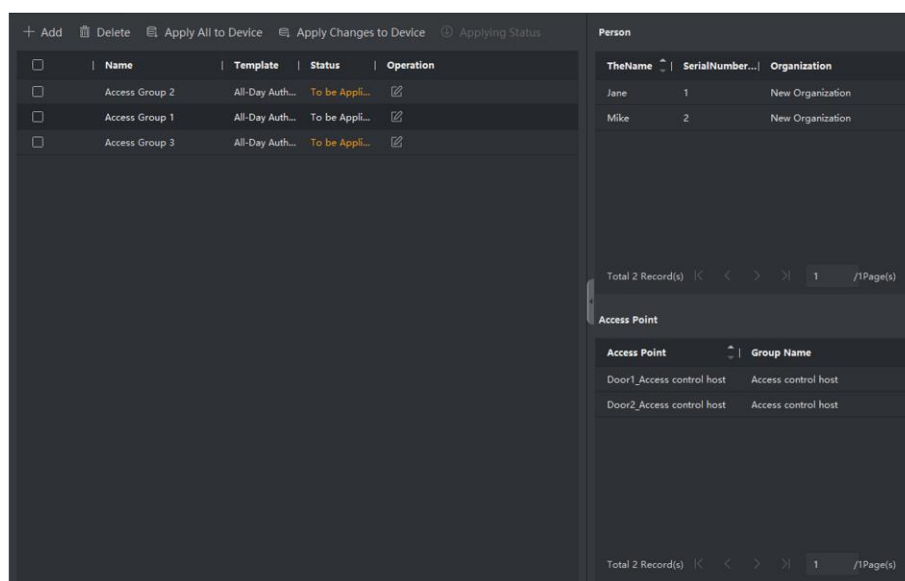


図 15-2 選択した人とアクセスポイントを表示します。

8. アクセス・グループを追加した後、それらをアクセス・コントロール装置に適用する必要があります。

効果

- 1) アクセス制御装置に適用するアクセスグループを選択します。
- 2) 「デバイスへすべて適用」をクリックすると、選択したすべてのアクセス・グループがアクセス・コントロール・デバイスまたはドアステーションに適用されます。
- 3) 「デバイスへのすべての適用」または「デバイスへの更の適用」をクリックします。

デバイスへのすべての適用

この操作により、選択したデバイスのすべての既存のアクセス・グループがクリアされ、新しいアクセス・グループがデバイスに適用されます。

デバイスの変更の適用

この操作では、選択したデバイスの既存のアクセス・グループはクリアされず、選択した

アクセス・グループの変更された部分だけがデバイスに適用されます。

- 4) [Status]列の[Appling status]を表示するか、[Applying Status]をクリックして、適用されているすべてのアクセスグループを表示します。

注記

[Display Failure Only]をチェックして、適用結果をフィルタリングすることができます。

適用されたアクセスグループの選択された人物は、リンクされたカードまたは指紋を用いて、選択されたドア/ドアステーションへの出入りを許可される。

9. オプション:必要に応じてアクセスグループを編集するには、クリックします。

注記

個人のアクセス情報やその他の関連情報を変更すると、クライアントの右隅にプロンプトアクセスグループが表示され、「適用される」になります。

プロンプトをクリックすると、変更したデータをデバイスに適用できます。[Apply Now]または[Apply Later]を選択できます。

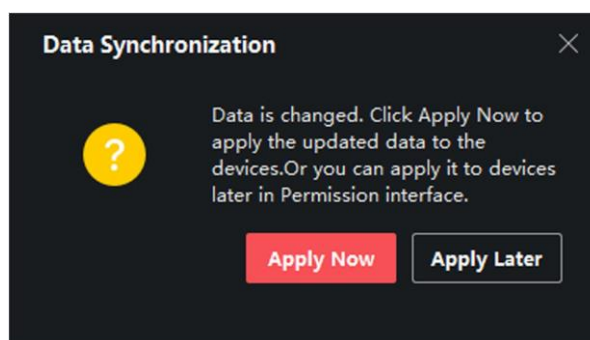


図 15-4 データ同期

15.4 検索アクセスグループ

アクセスグループを設定し、アクセス権限を人物に割り当てた後、その人物が属するアクセスグループを検索し、信任状番号、信任状タイプ、適用状況などの関連情報を表示することができます。

[アクセス制御]→[許可]→[検索]の順にクリックします。

検索条件を設定し、デバイス名を選択し、個人名(オプション)を入力し、「検索」をクリックします。検索した個人が属するアクセス・グループやその他の情報を表示できます。資格番号、カード発行状況、備考等を含む。

Device Name	Door Name	Person Name	Credential No.	Credential Type	Applying Status	Remark
Access control host	Door1_Access control host	Mike	2	Person	All applied.	All applied.
Access control host	Door1_Access control host	Lucy	5	Person	To be Applied	
Access control host	Door3_Access control host	Lily	4	Person	All applied.	All applied.
Access control host	Door3_Access control host	John	3	Person	All applied.	All applied.
Access control host	Door1_Access control host	Jane	1	Person	All applied.	All applied.


図 15-5 検索アクセスグループ

15.5 詳細機能の設定

以下の特殊な要件を満たすようにアクセス制御の高度な機能を設定することができます。

マルチファクター認証、パスバック防止などの異なるシーン

注記

- カード関連機能(アクセス制御カード/マルチファクター認証の種類)については、カード追加時にアクセスグループを適用したカードのみが表示されます。
- 高度な機能は、デバイスがサポートする必要があります。
- Advanced Functionにカーソルを合わせてクリックし、Advancedをカスタマイズします。

表示する機能

15.5.1 デバイスパラメータの設定

アクセス制御装置を追加した後、アクセス制御装置(アクセスコントローラ)、アクセス制御ポイント(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、レールコントローラのパラメータを設定できます。

アクセス制御装置の設定パラメータ

アクセス・コントロール・デバイスを追加した後、オーバーレイ・ユーザーを含むパラメータを設定できます。写真の情報、撮影後の画像のアップロード、撮影した写真の保存など。

ステップ

1. [アクセス制御]→[拡張機能]→[デバイスパラメータ]の順にクリックします。

注記

[Advanced Functions]リストにデバイスパラメータが表示されない場合は、[Advanced Function]にカーソルを合わせてクリックします。表示するデバイスパラメータを選択します。

2. アクセス装置を選択し、そのパラメータを右ページに表示します。
3. スイッチをONにすると、該当する機能が有効になります。

注記

- 表示されるパラメータは、アクセス制御装置によって異なる可能性がある。
 - 以下のパラメータの一部は、[基本情報]ページにリストされていません。[詳細]をクリックしてパラメータを編集します。
-

RS-485 通信冗長性

RS-485カードリーダーをアクセス制御装置に冗長配線する場合は、この機能を有効にしてください。

検出面の表示

認証時に顔画像を表示します。

カード番号表示

認証時にカード情報を表示します。

個人情報を表示する

認証時に個人情報を表示します。

画像上のオーバーレイパーソン情報

撮影した画像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、音声プロンプトがデバイスで有効になります。本体で

操作すると、音声ガイダンスが聞こえます。

アップロード Pic.リンクされた取り込みの後

リンクされたカメラで撮影した画像を自動的にシステムにアップロードします。

保存ピクチャリンクされた取り込みの後

この機能を有効にすると、リンクされたカメラで撮影した画像を機器に保存できます。

カード番号入力ボタンを押す

この機能を有効にすると、キーを押してカード番号を入力できます。

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アドレスを探知し、MACアドレスをシステムにアップロードできます。MACアドレスが指定されたMACアドレスと一致する場合、システムはいくつかのリンク動作をトリガすることができます。

3G/4G

本機能を有効にすると、3G/4Gネットワークで通信できます。

NFC 抗クローニング

この機能を有効にすると、複製されたカードを認証に使用することができなくなり、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:[Copy to to]をクリックし、アクセス制御デバイスを選択して、ページ内のパラメータを選択したデバイスにコピーします。

ドア/エレベータの設定パラメータ

アクセス制御装置を追加した後、アクセスポイント(ドアまたはフロア)を設定できます。
パラメーター

ステップ

1. [アクセス制御]→[拡張機能]→[デバイスパラメータ]の順にクリックします。
2. 左側のパネルでアクセス制御デバイスを選択し、クリックすると、選択したデバイスのドアまたはフロアが表示されます。

3. ドアまたはフロアを選択し、右ページに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**

- 表示されるパラメータは、アクセス制御装置によって異なる可能性がある。
- 以下のパラメータの一部は、[基本情報]ページにリストされていません。[詳細]をクリックしてパラメータを編集します。

氏名

必要に応じてカードリーダー名を編集します。

ドア接点

ドアセンサを閉じたまま、または開いたままにすることができます。通常、閉じたままである。

終了ボタンの種類

終了ボタンを閉じたままにするか、開いたままにするかを設定できます。通常、開いたままである。

ドアロック時間

通常のカードとリレーの動作を入れると、ドアをロックするタイマが動作します。

延長オープンデュレーション

ドア接点は、拡張アクセスを必要とする人が自分のカードをスIPPINGした後、適切な遅延で有効にすることができます。

ドア左開タイムアウトアラーム

設定された時間内にドアが閉じられなかった場合、アラームをトリガすることができます。0に設定するとアラームは発生しません。

ドアが閉じたときのロック・ドア

ドアロック時間に達していなくても、ドアを閉めてからロックすることができます。

強制コード

強制があったときに強制コードを入力することにより、ドアを開けることができます。同時に、クライアントは強制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

スーパーパスワードを入力することにより、特定の人々がドアを開けることができます。

解雇コード

カードリーダーのブザー停止に使用できる解除コードを作成する(キーパッドに解除コードを入力する)。



注記

- 強迫コード、スーパーコード、棄却コードは異なるはずである。
- 強制コード、スーパーパスワード、および却下コードは、以下と異なる必要があります。
認証パスワード
- 強迫符号、スーパーパスワード、解雇符号の長さは、機器に応じたものであり、通常は4~8桁の数字を含むべきである。

5. OKをクリックします。
6. オプション:[Copy to to]をクリックし、ページ内のパラメータを選択したドア/フロアにコピーするにはドア/フロアを選択します。



注記

ドアまたはフロアのステータス継続時間の設定も、選択したドア/フロアにコピーされます。

カードリーダーの設定パラメータ

アクセス制御装置を追加した後、カードリーダーのパラメータを設定できます。

ステップ

1. [アクセス制御]→[拡張機能]→[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で、ドアを展開するためにクリックし、カードリーダーを選択します。右側の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

- 表示されるパラメータは、アクセス制御装置によって異なる可能性があります。以下のパラメータの一部があります。詳しくは、本体の取扱説明書を

参照してください。

- 以下のパラメータの一部は、[基本情報]ページにリストされていません。[詳細]をクリックしてパラメータを編集します。
-

氏名

必要に応じてカードリーダー名を編集します。

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応じて、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。一般的には、デフォルト設定を採用します。

カードの最小スIPPINGインターバル

同一カードのカードスIPPING間隔が設定値以下の場合、カードスIPPINGは無効となります。0～255まで設定できます。

最大障害発生時の入力間隔

カードリーダーにパスワードを入力すると、2桁の入力間隔が設定値を超えている場合は、以前に押していた桁が自動的にクリアされます。

Max のアラーム失敗した試行

カードの読み込みが設定値に達したときにアラームを通知することができます。

最大カード故障回数

カード読取最大失敗回数を設定します。

改ざん検出

カードリーダーのタンパー防止検出を有効にします。

各コントローラとの通信

アクセス制御装置がカードリーダーと接続できない状態が設定より長い場合時間が経過するとカードリーダーが自動的にオフラインになります。

バジング時間

カードリーダーのブザー時刻を設定します。使用可能な時間範囲は0～5,999秒

です。0が表す連続的なブザー音

カードリーダーの種類/カードリーダーの説明

カードリーダーの種類と説明を取得する。それらは読み取り専用である。

指紋認識レベル

ドロップダウンリストから指紋認識レベルを選択します。

デフォルト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認証モードを表示します。

フィンガープリント能力

使用可能な指紋の最大数を表示します。

既存の指紋番号

デバイスに存在する指紋の数を表示します。

スコア

装置は、ヨー角度、ピッチ角度、および瞳孔距離に従って、撮影された画像をスコア化する。スコアが設定値を下回ると、顔認識が失敗します。

顔認識タイムアウト値

認識時間が設定時間を超えている場合は、装置が注意を喚起します。

顔認識間隔

認証時の2つの連続する顔認識の間の時間間隔。デフォルトでは、2です。

顔 1:1 マッチングしきい値

1:1の照合モードで認証するときに、照合しきい値を設定します。値が大きいほど、誤受理率は小さくなり、認証時の誤拒否率は大きくなります。

1:N セキュリティレベル

1:N照合モードで認証する場合のセキュリティレベルを設定します。値が大きいほど、誤受理率は小さくなり、認証時の誤拒否率は大きくなります。

生顔探知

顔検出機能を有効/無効にします。機能を有効にすると、デバイスは人物が生きているかどうかを認識することができます。

生顔探知セキュリティレベル

Live Face Detection機能を有効にした後、Live Face Authenticationを実行するときに、一致するセキュリティレベルを設定できます。

最大フェイスオートの試行に失敗しました。

最大有効顔検出失敗を設定します。設定された試行を超えて検出に失敗した場合、システムはユーザーの顔を5分間ロックします。同じユーザが5分以内に偽の顔で認証することはできません。5分以内に、ユーザは、連続して2回、実顔を介して認証を行い、ロックを解除することができます。

ロック認証失敗顔

Live Face Detection機能を有効にした後、Live Face Detectionに失敗した場合、システムは設定された試行以上にユーザーの顔を5分間ロックします。同じユーザが5分以内に偽の顔で認証することはできません。5分以内に、ユーザは、連続して2回、実顔を介して認証を行い、ロックを解除することができます。

アプリケーションモード

実際の環境に合わせて、室内など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:[Copy to]をクリックし、[Card Reader]を選択して、ページ内のパラメータを選択したCard Readerにコピーします。

アラーム入力の設定パラメータ

アクセス制御装置を追加した後、アラーム入力用のパラメータを設定できます。

ステップ



注記

アラーム入力の設定されている場合、アラーム入力のパラメータは編集できません。最初に解除してください。

1. [アクセス制御]→[拡張機能]→[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で、ドアを展開するためにクリックし、アラーム入力を選択し、右側のアラーム入力のパラメータを編集できます。
3. アラーム入力パラメータを設定します。

氏名

必要に応じてアラーム入力名を編集します。

検出器タイプ

アラーム入力の検出器の種類。

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

検出器が検出した信号の継続時間が設定時間に達すると、アラーム入力が入力がトリガされます。たとえば、感度を10msに設定した場合、検出器が検出した信号の継続時間が10msに達したときにのみ、このアラーム入力が入力がトリガされます。

トリガアラーム出力

トリガ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:アラーム入力をアームまたは解除するには、右上隅のスイッチをクリックします。

アラーム出力の設定パラメータ

アクセス制御装置を追加した後、アラーム出力にリンクする場合は、パラメータを設定できます。

ステップ

1. [アクセス制御]→[拡張機能]→[デバイスパラメータ]の順をクリックして、アクセス制御パラメータ設定ページに入ります。
2. 左側のデバイスリストで、ドアを展開するためにクリックし、アラーム入力を選択し、右側のアラーム入力のパラメータを編集できます。
3. アラーム出力パラメータを設定します。

氏名

必要に応じてカードリーダー名を編集します。

アラーム出力動作時間

アラーム出力がトリガされた後、どのくらい持続するか。

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にして、アラーム出力をトリガします。

レーンコントローラの設定パラメータ

レーン・コントローラをクライアントに追加した後、レーンを通過するためのパラメータを設定できます。

ステップ

1. [アクセス制御]→[拡張機能]→[デバイスパラメータ]の順にクリックし、[パラメータ設定]を入力します。
2. 左側の装置リストで、レーンコントローラを選択し、右側のレーンコントローラのパラメータを編集できます。
3. パラメータを編集する。

合格モード

デバイスのバリア状態を制御するコントローラを選択します。

- [Lane Controller's DIP Settings]を選択すると、装置はレーン・コントローラのパラメータ設定に従い、バリアを制御します。ソフトウェアの設定は無効になります。
- [Main Controller's Settings]を選択すると、デバイスはソフトウェアの設定に従いバリアを制御します。レーンコントローラのパラメータ設定は無効になります。

自由通過認証

この機能を有効にした場合、出入口のバリアモードがオープンのままのときは、通行の都度、歩行者が認証する必要があります。または、アラームが発生します。

障壁の開閉速度

バリアの開閉速度を設定します。1～10の範囲で選択できます。値が大きいほど、速度は速くなります。



推奨値は6です。

可聴プロンプト継続時間

アラームが発生したときに再生されるオーディオの持続時間を設定します。



注記

0はアラームが終了するまでのアラーム音です。

温度単位

デバイスの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。

15.5.2 残りのオープン/クローズの設定

ドアの開閉状態を設定したり、エレベーターコントローラーの開閉状態を設定したりすることができます。例えば、休日のドアを閉じたままにしたり、就業日の指定時間内に開いたままにしたりすることができます。

開始前に

システムにアクセス制御装置を追加する。

ステップ

1. 「アクセス制御」→「拡張機能」→「開いたまま/閉じたまま」の順にクリックし、「開いたまま/閉じたまま」ページを入力します。
2. 左側のパネルに設定する必要があるドアまたはエレベーターコントローラーを選択します。
3. 就業日中にドアまたはエレベーターコントローラーの状態を設定するには、ウィークスケジュールをクリックして以下の操作を行います。
 - 1) ドアの場合は、「開いたまま」または「閉じたまま」をクリックします。
 - 2) エレベーター・コントローラーの場合は、「フリー」または「コントロールド」をクリックします。
 - 3) カーソルをドラッグして継続時間を描画します。これは、継続時間を意味します。
構成済みのアクセス・グループが活動化されます。



注記

週スケジュールでは、各日に最大8回まで設定できます。

- 4) オプション:以下の操作を行って、継続時間を編集します。
 - カーソルをタイムデュレーションに移動し、カーソルが回転したときにタイ

- ムラインバーのタイムデュレーションを希望する位置にドラッグします。
 - 継続時間をクリックし、表示されたダイアログで開始/終了時刻を直接編集します。
 - 開始時間または終了時間にカーソルを移動してドラッグすると、カーソルが切り替わるまでの時間が長くなるか短くなります。
- 5) 保存をクリックします

関連業務

<p>週全体にコピーする</p>	<p>タイムバーで1つの継続時間を選択し、Copy to Whole Week をクリックして、このタイムバーのすべての継続時間設定を別の週の日のコピーします。</p>
<p>選択削除</p>	<p>タイムバーで1つの継続時間を選択し、選択削除をクリックして削除します。</p>
<p>クリア</p>	<p>「クリア」をクリックして、週スケジュールのすべての継続時間設定をクリアします。</p>



4. 休日のドアのステータスを設定するには、休日をクリックし、以下を実行します。
- 事業
- 1) 「開いたまま」または「閉じたまま」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) カーソルをドラッグして継続時間を描画します。これは、継続時間を意味します。
構成済みのアクセス・グループが活動化されます。

 注記

最大8回まで、1休日に設定できます。

- 5) 以下の操作を行って、継続時間を編集します。
 - カーソルをタイムデュレーションに移動し、カーソルが回転したときにタイムラインバーのタイムデュレーションを希望する位置にドラッグします。
 - 継続時間をクリックし、表示されたダイアログで開始/終了時刻を直接編集します。
 - 開始時間または終了時間にカーソルを移動してドラッグすると、カーソルが切り替わるまでの時間が長くなるか短くなります。
- 6) オプション:削除する時間を選択し、クリックします。

選択した継続時間を削除する操作欄。

- 7) オプション:  クリック「操作」列で、タイムバーのすべての継続時間をクリアします。 
 - 8) オプション: クリック「操作」欄には、この追加した休日の期間を休日リストから削除します。
 - 9) 保存をクリックします。
5. オプション: 「コピー」をクリックして、このドアのドアステータスを他のドアにコピーします。

15.5.3 マルチファクター認証の設定

グループごとに管理し、1つのアクセス・コントロール・ポイント(ドア)の複数の個人に認証を設定できます。

開始前に

アクセス・グループを設定し、アクセス・グループをアクセス制御装置に適用します。詳細については、「アクセス許可を個人に割り当てるアクセスグループの設定」を参照してください。

1つのアクセス・コントロール・ポイント(ドア)の複数のカードに認証を設定する場合に、このタスクを実行します。

ステップ

1. [アクセス制御]→[拡張機能]→[マルチファクターオート]の順にクリックします。
2. 左側のパネルのデバイスリストでアクセス制御デバイスを選択します。
3. アクセス制御装置の個人/カードグループを追加します。
 - 1) 右パネルの[追加]をクリックします。
 - 2) 必要に応じてグループの名前を作成します。
 - 3) 個人/カードグループの有効期間の開始時刻と終了時刻を指定します。
 - 4) 「使用可能」リストでメンバーとカードを選択すると、選択したメンバーとカードが「選択」リストに追加されます。

注記

本人にカードを渡してください。

アクセス・グループが設定されていることを確認し、アクセス・グループをアクセス制御装置に正常に適用してください。

- 5) 保存をクリックします。
- 6) オプション: 個人/カードグループを選択し、削除をクリックして削除します。
- 7) オプション: 個人/カード・グループを選択し、「適用」をクリックして、以前にアクセス制御デバイスに適用されなかったアクセス・グループを再適用します。

4. 左側のパネルで選択したデバイスのアクセス制御ポイント(ドア)を選択します。
5. パスワードを入力するときは、最大間隔を入力します。
6. 選択したアクセス・コントロール・ポイントの認証グループを追加します。
 - 1) [Authentication Groups]パネルの[追加]をクリックします。
 - 2) ドロップダウン・リストから、認証テンプレートとして設定されたテンプレートを選択します。

**注記**

テンプレートの設定については、「スケジュールとテンプレートの設定」を参照してください。

- 3) [ローカル認証]、[ローカル認証]、[リモートオーブンドア]、[ローカル認証とスーパーパスワード]のいずれかの認証タイプをドロップダウンリストから選択します。

ローカル認証

アクセス制御装置による認証。

ローカル認証とリモートオーブンドア

アクセス制御装置およびクライアントによる認証。デバイスのカードを押し当てると、ウィンドウが表示されます。クライアント経由でドアのロックを解除できます。

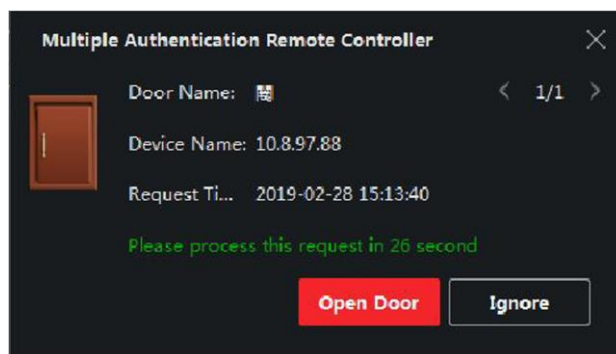


図 15-7 リモートオーブンドア

**注記**

オフライン認証をチェックして、アクセス制御装置がクライアントと切断されたときにスーパーパスワード認証を有効にすることができます。

ローカル認証とスーパーパスワード

アクセス制御装置およびスーパーパスワードによる認証。

- 4) 左側のリストで追加した個人/カードグループを選択すると、右側の選択リストに認証グループとして追加されます。
- 5) 右側のリストの追加された認証グループをクリックして、「オートタイム」列の認証時間を設定します。



- 認証時間は0より大きく、追加された人員より小さくする必要があります。
人事グループの数量
- 認証時間の最大値は16です。

-
- 6) 保存をクリックします。



- アクセス制御ポイント(ドア)ごとに、最大4つの認証グループを追加できます。
- 認証タイプがローカル認証である認証グループについては、最大8人/カードグループを認証グループに追加することができます。
- 認証タイプがローカル認証・スーパーパスワード・ローカル認証・リモートオープンドアの認証グループについては、最大7人/カードグループを追加することができます。

-
7. 保存をクリックします。

15.5.4 カスタム・ワイガンド・ルールの設定

サードパーティWiegandのルールをアップロードする知識に基づいて、複数を設定できます。

デバイスとサードパーティのカードリーダー間で通信するためのカスタマイズされたWiegandルール

開始前に

サードパーティ製のカードリーダーをデバイスに接続します。

ステップ



- デフォルトでは、デバイスはカスタムワイガンド機能を無効にします。デバイスが

カスタムWiegand機能を有効にすると、デバイス内のすべてのWiegandインターフェースはカスタマイズされたWiegandプロトコルを使用します。

- 5つまでカスタムワイガンドを設定できます。
 - カスタムWiegandの詳細については、「カスタムWiegandルールの説明」を参照してください。
-

1. [アクセス制御]→[拡張機能]→[カスタム・ウィーガンド]の順にクリックして、[カスタム・ウィーガンド]ページを入力します。
 2. 左側のカスタムWiegandを選択します。
 3. Wiegand名を作成します。
-

 注記

カスタムWiegand名には最大32文字まで入力できます。

4. [デバイスの選択]をクリックして、カスタム・ウィーガンドを設定するアクセス制御デバイスを選択します。
 5. 他社製カードリーダーのプロパティに合わせてパリティモードを設定します。
-

 注記

- 合計80ビットまで許容される。
 - 奇数パリティ開始ビット、奇数パリティ長、偶数パリティ開始ビットおよび偶数パリティ長の範囲は1から80ビットである。
 - カードIDのスタートビット、メーカーコード、サイトコード、OEMは1～80ビットの範囲とする。
-

6. 出力変換規則を設定します。

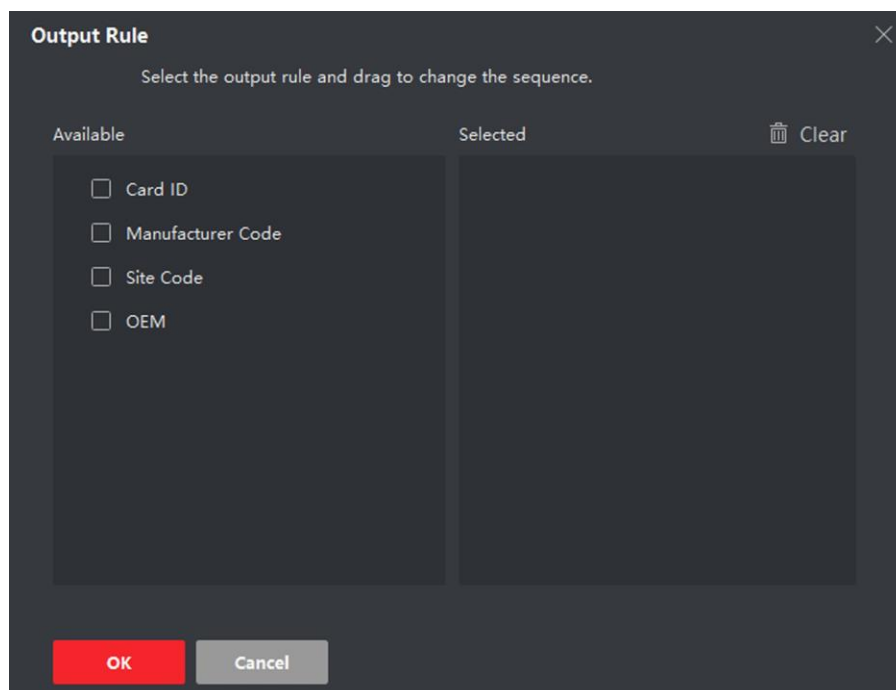


図 15-8 出力変換ルールの設定

- 1) 「ルールの設定」をクリックして、「出力変換ルールの設定」ウィンドウを開きます。
 - 2) 左側のリストでルールを選択します。
選択したルールが右側のリストに追加されます。
 - 3) オプション:ルールをドラッグしてルールの順序を変更します。
 - 4) OKをクリックします。
 - 5) [Custom Wiegand]タブで、ルールの開始ビット、長さ、10進数を設定します。
7. 保存をクリックします。

15.5.5 カードリーダー認証モードとスケジュールの設定

アクセス制御装置のカードリーダーの通過ルールは、実際のニーズに合わせて設定することができます。

ステップ

1. [アクセス制御]→[拡張機能]→[認証]をクリックして認証モードの設定ページを表示します。
2. 左側のカードリーダーを選択して設定します。
3. カードリーダー認証モードを設定します。
 - 1) [構成]をクリックします。

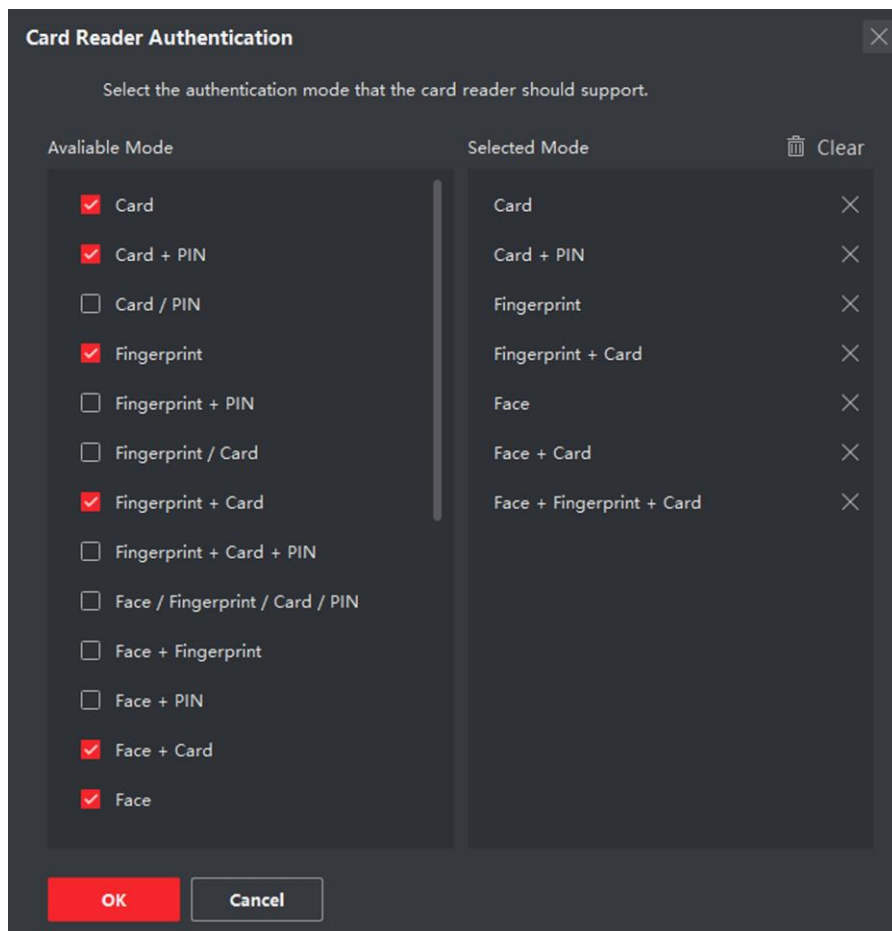


図 15-9 カードリーダー認証モードの選択



注記

PIN1 コードは、ドアを開くために設定された PIN1 コードです。「アクセス制御の設定」を参照してください。

- 2) 「使用可能モード」リストでモードを確認すると、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、選択したモードが色の異なる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認証モードを選択し、カーソルをドラッグしてスケジュールにカラーバーを描画します。この期間はカードリーダー認証が有効です。
5. 上記の手順を繰り返して、他の期間を設定します。

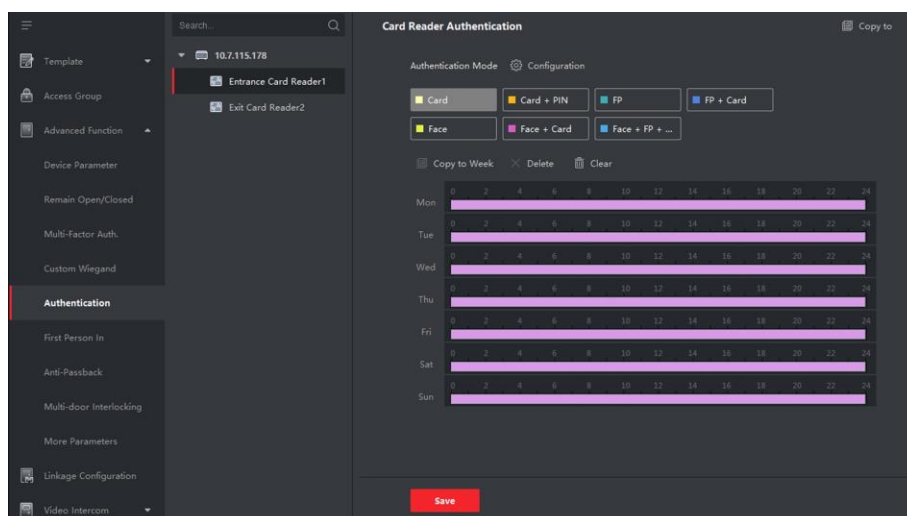


図 15-10 カードリーダーの認証モードの設定

6. オプション:設定した曜日を選択し、「週にコピー」をクリックして、同じ設定を週全体にコピーします。
7. オプション:コピーをクリックして、設定を他のカードリーダーにコピーします。
8. 保存をクリックします。

15.5.6 個人認証モードの設定

実際のニーズに合わせて、指定されたアクセス制御装置に通過ルールを設定することができます。

開始前に

アクセス制御装置が個人認証の機能をサポートしていることを確認してください。

ステップ

1. [アクセス制御]→[拡張機能]→[認証]の順にクリックします。
2. 左パネルでアクセス制御装置(人物認証機能をサポート)を選択し、人物認証モードページに入ります。
3. 「追加」をクリックして、「追加」ウィンドウを入力します。
4. 左側のパネルで設定する必要がある人を選択します。選択した人物が右パネルに追加されます。
5. [Authentication Mode]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。

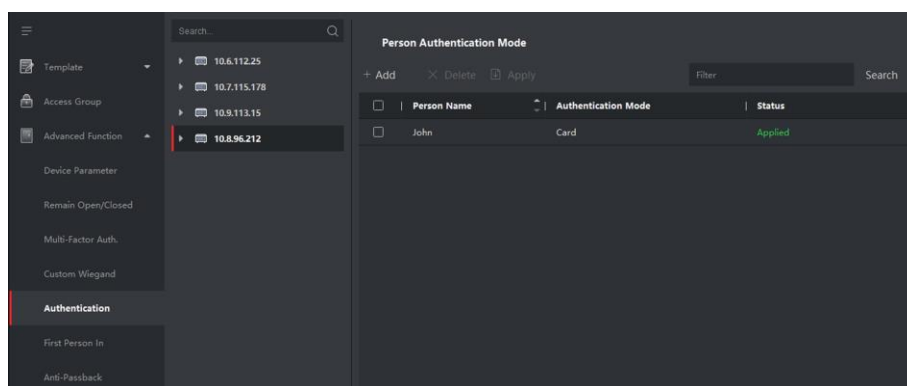


図 15-11 人の認証モードの設定

7. オプション:「個人認証モード」ページで個人を選択し、「適用」をクリックして、個人認証モードをデバイスに適用します。

**注記**

個人認証は、他の認証モードよりも優先順位が高い。アクセス制御デバイスが人物認証モードに設定されている場合、人物認証モードを介して人物認証を行う必要がある。

15.5.7 エレベーターコントローラのリレー設定

エレベーターコントローラでは、フロアとリレーの関係を管理し、フロアのリレータイプを設定できます。異なるリレータイプは異なる機能を実装することができる。フロアとリレーの関係を設定することにより、エレベータに異なる機能を割り当て、エレベータを制御することができます。

リレーとフロアの関係の設定

対象階に異なるリレータイプを割り当てることができ、各階には3つのリレータイプを割り当てることができます。こうすることで、エレベーターを呼び出し、各フロアの操作を割り当てることができます。

開始前に

クライアントにエレベーターコントローラを追加します。

ステップ

1. [アクセス制御]→[アドバンス機能]→[エレベータ構成]の順にクリックし、リレー設定に入ります。

ページ


2. 左側のエレベーターコントローラーを選択します。
3. 右側の[構成されていないリレー]パネルで構成されていないリレーを選択します。リレーには3種類あります。

ボタン

各フロアのボタンの有効性を制御します。



注記


 ボタンリレーを表します。

コールエレベーター

屋内局または屋外局で指定した階にエレベーターを呼び出す制御。



注記


 コールエレベーターリレーを表します。

自動


ユーザがエレベータ内でカードを押し込むときにボタンを押す制御。下記ボタンユーザーの許可により自動的に床を押します。



注記

 自動ボタンリレーを表します。

例

次の写真を例にとります。番号1-2では、1は分散型エレベーターコントローラー番号、2はリレー番号、アイコンはリレータイプを表します。リレーの種類を変更できます。詳細は、Configure Relay Typeを参照してください。

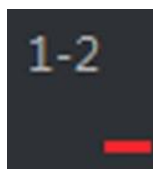


図 15-12 リレー

4. リレーとフロアの関係を設定します。
 - 構成されていないリレーを、[Unconfigured Relay]パネルから[Floor List]パネルの目標フロアにドラッグします。
 - 「フロアリスト」パネルから「構成済みリレー」パネルにリレーをドラッグします。
 - リレーをフロアリストパネルのある階から別の階にドラッグします。対象フロ

アに既にドラッグされたリレーと同じタイプのリレーが設定されている場合は、同じタイプのリレーが置き換えられます。

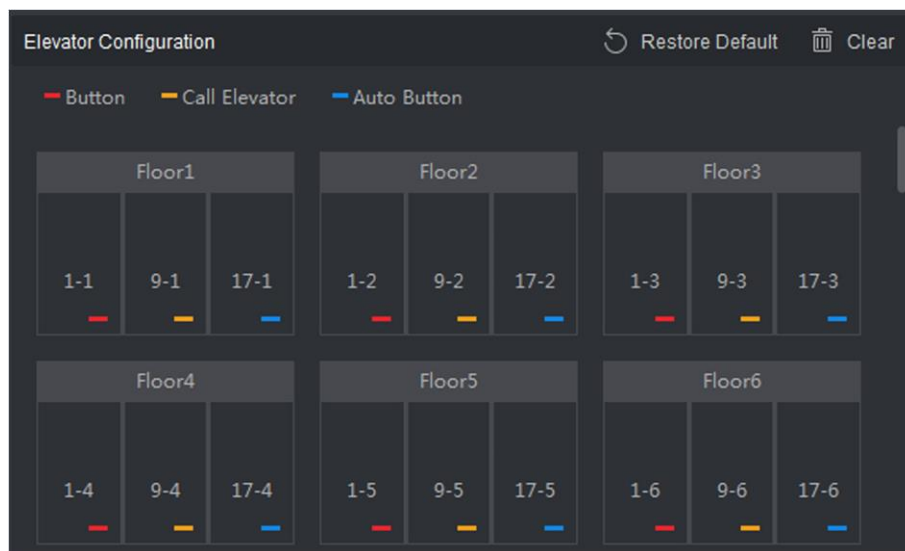


図 15-13 リレーとフロアの関係

注記

- エレベーターコントローラーは、最大24台の分散型エレベーターコントローラーにリンクできます。分散形エレベーターコントローラーは、最大16個のリレーをリンクすることができる。
- デフォルトでは、リレー総量は追加フロア数*3(3種類のリレー)です。
- 最大3種類のリレーを1フロアにドラッグできます。
- ドアグループ管理のフロア番号を変更すると、すべてのリレーがリレー設定になります。インターフェースはデフォルト設定に復元されます。

5. [Save]をクリックして、選択したエレベーターコントローラーに設定を適用します。

リレータイプの設定


各種機能を実現するために、ボタンリレー、コールエレベーターリレー、オートボタンリレーなど、各種のリレーを設定することができます。異なるリレータイプは異なる機能を実装することができる。ボタンリレーは、各フロアのボタンの有効性を制御します。コールエレベーターリレーは、屋内局または屋外局から指定された階にエレベータを呼び出します。自動ボタンリレーは、ユーザがエレベータ内でカードをスウィッピングしたときにボタンを押すように制御するもので、床のボタンはユーザの許可に従って自動的に押される。

ステップ

1. [アクセス制御]→[アドバンス機能]→[エレベータ構成]の順にクリックし、リレー設定に入ります。
2. ページ左側のエレベーターコントローラーを選択します。
3. 「リレータイプ設定」をクリックすると、「リレータイプ設定」画面が表示されます。



注記

- [Relay Type Settings]ウィンドウのすべてのリレーは、構成されていないリレーです。
- リレーにはボタンリレー、コールエレベーターリレー、オートボタンリレーの3種類があります。 

4. リレーを1つのリレータイプのパネルからターゲットのパネルにドラッグします。

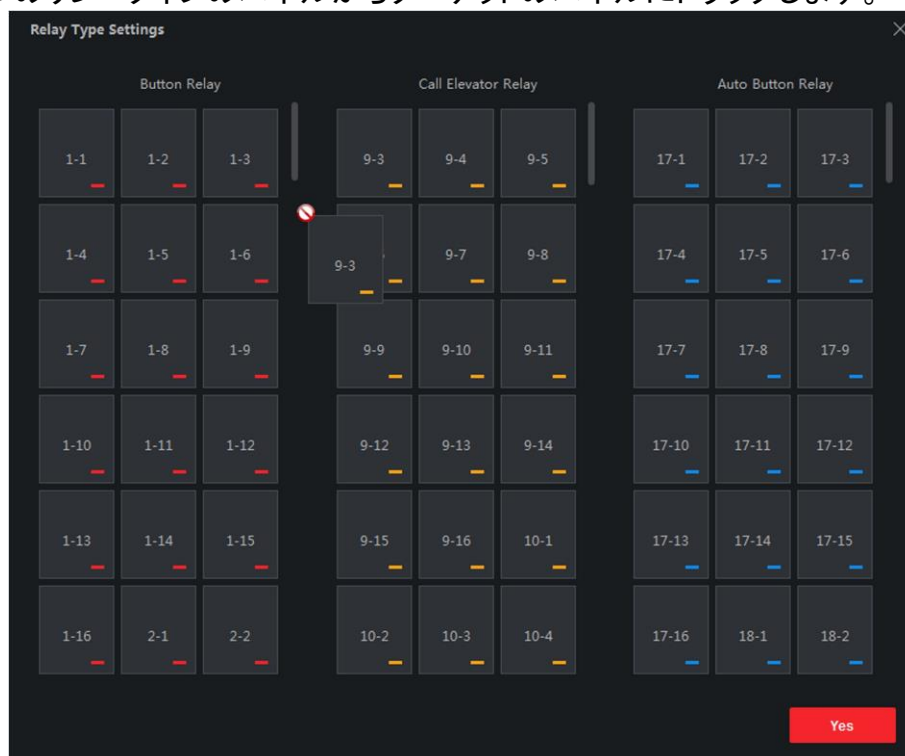


図 15-14 リレータイプの設定

5. OKをクリックします。

15.5.8 ファーストパーソンの設定

1つのアクセス・コントロール・ポイントに複数のファースト・パーソンを設定できます。最初の人物が認可されると、複数の人物がドアまたはその他の認証アクション

にアクセスできるようになります。

開始前に

アクセス・グループを設定し、アクセス・コントロール装置にアクセス・グループを適用します。

アクセス許可を個人に割り当てるようにアクセスグループを設定します。

この作業は、一人称でドアを開くように設定する場合に実行します。

ステップ

1. [アクセス制御]→[拡張機能]→[ファーストパーソンの入力]の順にクリックして、[ファーストパーソンの入力]ページを入力します。
2. 左側のパネルのリストでアクセス制御デバイスを選択します。
3. 選択したデバイスのアクセス制御ポイントごとに、現在のモードを「最初の人物の後の残りのオープンを有効にする」、「最初の人物の後の残りのオープンを無効にする」、または「最初の人物の許可」のいずれかに選択します。

最初の人物の後の残りオープンを有効にする

最初の人物が許可された後、開いたままの時間が終了するまで、設定された時間、ドアは開いたままになります。このモードを選択した場合は、開いたままの時間を設定する必要があります。



注記

オープン時間は0～1440分とする。デフォルトでは、開いたままの時間は10分です。

最初の人オープンした後の残りを無効にする

正常認証の一人前の機能を無効にします。

第一者の承諾

すべての認証(スーパーカード、スーパーパスワード、強制カード、強制コードの認証を除く)は、最初の個人認証後にのみ許可されます。



注記

最初の人物モードを無効にするために、最初の人物によって再度認証することができます。

4. [First Person List]パネルの[Add]をクリックします。
5. 左側のリストで選択した人物が最初に追加されます。

ドアの人員

追加された最初の人物が最初の人物リストにリストされます。

6. オプション:リストから最初の人物を選択し、[削除]をクリックして最初の人物から削除します。
7. 保存をクリックします。

15.5.9 パスバック対策の設定

パスバック防止機能は、カードを認可されていない人に渡す、またはテールドアクセスするなどのアクセス証明書の誤用または不正使用を最小限に抑えるように設計されています。パスバック防止機能は、アクセスを許可するためにアクセス信任状を使用しなければならない特定のシーケンスを確立します。クライアント経由の実際のパスに従ってシーケンスを設定することができます。また、個人が間違っただけのシーケンスで信任状を使用する場合は、アンチパスワードレコードをリセットすることもできます。

開始前に

アクセス制御装置のアンチバック機能を有効にする。

アクセス・コントロール・デバイスのアンチ・パスバックを設定するときに、このタスクを実行します。

ステップ

注記

パスバック防止機能、マルチドアインターロック機能のどちらも、アクセス制御装置に同時に設定することができる。マルチドアインターロックの構成については、「マルチドアインターロックの構成」を参照してください。

1. 「アクセス制御」→「拡張機能」→「パスバック防止」をクリックして、パスワード保護設定を入力します。
ページ
2. 左側のパネルでアクセス制御デバイスを選択します。
3. [First Card Reader]フィールドのパスの先頭にカードリーダーを選択します。
4. 「カードリーダー後方」列で選択した最初のカードリーダーをクリックして、「カードリーダー選択」ダイアログを開きます。
5. 1台目のカードリーダーのアフター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のアフターカードリーダーとして、アフターカードリーダーを4台まで追加できます。

6. ダイアログでOKをクリックして、選択内容を保存します。
7. 「パスバック対策設定」ページの「保存」をクリックして設定を保存し、有効にします。

例

カードスウィッピングパスの設定: 先頭に「リーダーIn_01」を選択し、「リーダーIn_02」を「リーダーアウト_04」をリンクされたカードリーダーとして選択すると、次に、リーダーイン_01、リーダーイン_02、リーダーアウト_04の順にカードを入れることによって、アクセス制御ポイントを通過させることができます。

8. 「パスバック防止のリセット」をクリックし、デバイス上の人物に関する関連するパスバック防止レコードを削除する人物を選択します。



注記

この機能は、装置がサポートする必要があります。

15.5.10 マルチドアインターロックの設定

同一アクセス制御装置の複数ドア間のマルチドアインターロックを設定します。一方のドアを開けるには、他のドアを閉じたままにしておく必要があります。つまり、インターロック付きコンバインドドアグループでは、1つのドアまで同時に開くことができます。

複数のドアを連動させたい場合に実行します。

ステップ



注記

- マルチドアインターロック機能は、複数のアクセス制御点(ドア)を有するアクセス制御装置によってのみサポートされる。
- パスバック防止機能、マルチドアインターロック機能のどちらも、アクセス制御装置に同時に設定することができる。パッシングバック防止機能の設定については、「パスバック防止機能の設定」を参照してください。

1. [アクセス制御]→[拡張機能]→[マルチドアインターロック]の順にクリックします。

2. 左側のパネルでアクセス制御デバイスを選択します。
3. Multi-door Interlocking ListパネルのAddをクリックして、Add Access Control Pointを開き、Addウィンドウを開きます。
4. リストから少なくとも2つのアクセス制御ポイント(ドア)を選択します。

 注記

マルチドアインターロックの組合せでは、4ドアまで追加することができます。

5. [OK]をクリックして、インターロック用に選択したアクセス制御ポイントを追加します。
設定されたマルチドアインターロックコンビネーションがマルチ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:リストから追加されたマルチドアインターロックの組み合わせを選択し、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、設定をアクセス制御デバイスに適用します。

15.5.11 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。それから、入ることでドアを開けることができます。

カードを持参し忘れたときの認証コード

このタスクは、認証コードをドアを開くように設定するときに実行します。

 注記

- 認証コード機能は、アクセス制御装置がサポートする必要がある。
 - 1台のアクセス制御装置に、最大500枚の認証コード付きカードを追加できます。本認証コードは固有であり、互いに同じではありません。
-

ステップ

1. [アクセス制御]→[拡張機能]→[認証コード]をクリックして認証を入力します。
2. 「コントローラー・リスト」パネルでアクセス・コントロール・デバイスを選択します。
カードリストパネルには、適用されているすべてのカードと個人が表示されます。

 注記

デバイスへのアクセス許可の設定と適用については、「アクセスグループを設定し、人にアクセス許可を割り当てる」を参照してください。

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**

認証コードには、4～8桁の数字を含める必要があります。

4. [Authentication Code]ページの右上隅にある[Save]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が自動的に有効になります。

次にすべきこと

アクセス制御装置のカードリーダー認証モードをカード/認証コードとして設定します。詳細については、Configure Card Reader 認証モードとスケジュールを参照してください。

15.6 その他のパラメータの設定

アクセス制御装置を追加した後、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、Wiegandパラメータなどのパラメータを設定できます。

15.6.1 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をサポートする場合は、クライアント経由でこれらのNICのネットワークパラメータ(IPアドレス、MACアドレス、ポート番号など)を設定できます。

ステップ

**注記**

この機能は、装置がサポートする必要があります。

1. アクセス・コントロール・モジュールを入力します。
2. 左側のナビゲーションバーで、「Advanced Function」→「More Parameters」と入力します。
3. デバイスリストでアクセス制御デバイスを選択し、NICをクリックして複数のNIC設定を入力します。
4. ドロップダウン・リストから構成したいNICを選択します。
5. 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、物理ネットワークセグメント上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ある。

MTU

ネットワークインタフェースの最大伝送単位(MTU)。

6. 保存をクリックします。

15.6.2 ネットワークパラメータの設定

アクセス制御デバイスを追加した後、デバイスログのアップロードモードを設定し、有線または無線ネットワーク経由でISUPアカウントを作成できます。

ログアップロードモードの設定

ISUP プロトコルを介してログをアップロードするようにデバイスのモードを設定できます。

ステップ

1. アクセス・コントロール・モジュールを入力します。
2. 左側のナビゲーションバーで、「Advanced Function」→「More Parameters」と入力します。
3. デバイスリストからアクセス制御デバイスを選択し、「ネットワーク」→「アップロードモード」と入力します。
4. ドロップダウンリストから中心グループを選択します。
5. [有効]をチェックして、アップロードモードを有効にします。
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。
 - メインチャンネルとバックアップチャンネルのN1またはG1を有効にします。
 - メインチャンネルまたはバックアップチャンネルを無効にするには、Closeを選択します。

注記

メインチャンネルとバックアップチャンネルは、同時にN1またはG1を有効に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 ISUP アカウントを作成する

有線通信モードでは、ISUP プロトコルのアカウントを設定できます。その後、ISUP プロトコルを介してデバイスを追加できます。

ステップ



注記

この機能は、装置がサポートする必要があります。

1. アクセス・コントロール・モジュールを入力します。
2. 左側のナビゲーションバーで、「Advanced Function」→「More Parameters」と入力します。
3. 機器一覧からアクセス制御機器を選択し、「ネットワーク」→「ネットワークセンター」と入力します。
4. ドロップダウンリストから中心グループを選択します。
5. IP AddressまたはDomain NameとしてAddress Type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

無線ネットワークおよび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. ISUPとしてProtocol Type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 ISUP アカウントを作成する

ワイヤレス通信モードで ISUP プロトコルのアカウントを設定できます。その後、ISUP プロトコルを介してデバイスを追加できます。

ステップ



注記

この機能は、装置がサポートする必要があります。

1. アクセス・コントロール・モジュールを入力します。

2. 左側のナビゲーションバーで、「Advanced Function」→「More Parameters」と入力します。
3. 機器一覧からアクセス制御機器を選択し、「ネットワーク」→「無線通信」と入力する
4. APN NameをCMNETまたはUNINETとして選択します。
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中心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。
 - 無線ネットワークおよび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. ISUPとしてProtocol Type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。

15.6.3 デバイス取り込みパラメータの設定

手動取り込みおよびイベントトリガー取り込みを含む、アクセス制御デバイスの取り込みパラメータを設定できます。

 注記

- キャプチャ機能は、デバイスによってサポートされる必要があります。
 - キャプチャパラメータを設定する前に、まず、イベントがトリガーされた画像が保存される場所を定義するために、画像保存を設定する必要があります。詳しくは、「ピクチャストレージ設定」を参照してください。
-

トリガードキャプチャパラメータの設定

イベントが発生すると、アクセス制御装置のカメラがトリガされて、そのイベントが発生したときに何が起こるかを記録するために、画像を捕捉することができる。イベントセンターでイベント内容を確認すると、撮影した画像を見ることができます。その前に、一度に取り込む画像の枚数などの取り込みパラメータを設定する必要があります。

開始前に

キャプチャパラメータを設定する前に、キャプチャされた画像が保存される場所を定義するために、まずピクチャストレージを設定します。詳しくは、「ピクチャストレージ設定」を参照してください。

ステップ



この機能はデバイスでサポートされる必要があります。

1. アクセス・コントロール・モジュールを入力します。
2. 左側のナビゲーションバーから、「Advanced Function」→「More Parameters」→「Capture」と入力します。
3. デバイスリストからアクセス制御デバイスを選択し、リンクされた取り込みを選択します。
4. 画像サイズと画質を設定します。
5. 一度トリガーされたキャプチャ時間を設定し、1つのキャプチャの数を定義します。
時間
6. キャプチャ時間が1を超える場合は、各キャプチャの間隔を設定します。
7. 保存をクリックします。

手動取り込みパラメータの設定

ステータス・モニタリング・モジュールでは、ボタンをクリックすることにより、アクセス・コントロール・デバイスのカメラ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のパラメータを設定する必要があります。

開始前に

キャプチャパラメータを設定する前に、まず保存パスを設定して、キャプチャした画像の保存先を指定します。詳細については、「ファイル保存パスの設定」を参照してください。

ステップ



この機能はデバイスでサポートされる必要があります。

1. アクセス・コントロール・モジュールを入力します。
2. 左側のナビゲーションバーから、「Advanced Function」→「More Parameters」→

「Capture」と入力します。

3. 機器一覧からアクセス制御機器を選択し、手動撮影を選択します。
4. 取り込んだ画像の解像度をドロップダウンリストから選択します。
5. 高画質、中画質、低画質を選択します。画質が高いほど、画像のサイズは大きくなります。
6. 保存をクリックします。

15.6.4 顔認識端子の設定パラメータ

顔認識端末では、顔画像データベース、QRコードなどの設定ができます。

ステップ



この機能は、装置がサポートする必要があります。

1. アクセス・コントロール・モジュールを入力します。
2. 左側のナビゲーションバーで、「Advanced Function」→「More Parameters」と入力します。
3. 機器リストからアクセス制御機器を選択し、「顔認識端末」をクリックします。
4. パラメータを設定します。



表示されるこれらのパラメータは、デバイスのモデルによって異なります。

COM

設定用のCOMポートを選択します。COM1はRS-485インタフェース、COM2はRS-232インタフェースを指します。

顔写真データベース

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コードによる認証

デバイスカメラを有効にすると、QRコードをスキャンして認証することができます。デフォルトでは、この関数は無効になっている。

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希望する人とブラックリストの人を比較します。

一致した場合(個人がブラックリストにある場合)、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(ブラックリストにない場合)、アクセスが許可されます。

顔画像を保存する

有効にすると、認証時に撮影した顔画像が本体に保存されます。

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。

15.6.5 M1 カードの暗号化を有効にする

M1カード暗号化は、認証のセキュリティレベルを向上させることができます。

ステップ



注記

この機能は、アクセス制御装置とカードリーダーがサポートする必要があります。

1. アクセス・コントロール・モジュールを入力します。
2. 左側のナビゲーションバーで、「Advanced Function」→「More Parameters」と入力します。
3. 機器一覧からアクセス制御機器を選択し、「M1カード暗号化」をクリックして、「M1カード暗号化」ページに入ります。
4. M1カードの暗号化機能を有効にするには、スイッチをオンにします。
5. セクタIDを設定します。
セクターIDは1～100の範囲である。
6. 「保存」をクリックして設定を保存します。

15.6.6 RS-485 パラメータの設定

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、ワークモード、接続モードなど、アクセス制御装置のRS-485パラメータを設定します。

ステップ



注記

RS-485の設定は、装置がサポートする必要があります。

1. アクセス・コントロール・モジュールを入力します。
2. 左側のナビゲーションバーで、「Advanced Function」→「More Parameters」と入力します。
3. 機器一覧からアクセス制御機器を選択し、RS-485をクリックして「RS-485設定」を入力します。
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パラメータを設定します。
5. 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、動作モードを設定します。
ドロップダウン・リストの接続モード



注記

接続モードが Connect Access Control Devices の場合は、カード番号を選択するか、出力タイプとしての個人 ID を選択できます。

6. 保存をクリックします。
 - 設定されたパラメータは、デバイスに自動的に適用されます。
 - 作業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リブートします。

15.6.7 Wiegand パラメータの設定

アクセス制御装置のWiegandチャンネルと通信モードを設定します。Wiegandパラメータの設定後、Wiegand通信を介してWiegandカードリーダーに接続することができます。

ステップ



注記

この機能は、装置がサポートする必要があります。

1. アクセス・コントロール・モジュールを入力します。
2. 左側のナビゲーションバーで、「Advanced Function」→「More Parameters」と入力します。
3. デバイスリストでアクセス制御デバイスを選択し、WiegandをクリックしてWiegandを入力します。
「設定」ページ
4. スイッチをオンにすると、デバイスのWiegand機能が有効になります。
5. ドロップダウンリストからWiegandチャンネルNo.と通信モードを選択します。

 注記

「通信方向」を「送信」に設定した場合は、「ワイガンドモード」を Wiegand 26 または Wiegand 34 に設定する必要があります。

6. 保存をクリックします。
 - 設定されたパラメータは、デバイスに自動的に適用されます。
 - 通信方向を変更すると、自動的にリブートします。

15.7 アクセス制御のためのリンクアクションの設定

アクセス・コントロール・デバイスで検出され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。その後、イベントが発生すると、リンクアクションが起動されます。このメカニズムは、セキュリティ担当者にイベントを通知したり、リアルタイムで自動アクセス制御を起動したりするために使用されます。

2種類のリンク動作がサポートされています:

- **クライアントアクション:** イベントが検出されると、クライアントが可聴警告を発するなど、クライアントのアクションが起動されます。
- **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音やドアの開閉など、特定のデバイスのアクションがトリガされます。

15.7.1 アクセス・イベント用のクライアント・アクションの構成

アクセスポイントから遠く離れている場合でも、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、クライアント経由で何が起き、イベントが緊急に発生するかどうかを知ることができます。ここでのクライアントアクションとは、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アクションを指します。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ー・スタッフに通知し、イベントを適時に処理できるようにします。

ステップ

1. [イベント設定]→[アクセス制御イベント]をクリックします。
追加されたアクセス制御デバイスがデバイスリストに表示されます。
2. 装置リストからリソース(装置、アラーム入力、ドア/エレベータ、カードリーダを含む)を選択します。
選択したリソースがサポートするイベント・タイプが表示されます。
3. イベントを選択し、「Edit Priority」をクリックして、イベントの優先順位を定義します。この優先順位は、イベント・センターでイベントをフィルターするために使用できます。
4. イベントのリンク動作を設定します。
 - 1) イベントを選択し、「リンクの編集」をクリックして、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。

音声警告

クライアントソフトウェアは、イベントがトリガーされたときに音声警告を発生します。警報音を選択します。



注記

アラーム音の設定方法については、「アラーム音設定」を参照してください。

メールを送る

イベントに関する電子メール通知を1つ以上の受信者に送信します。
電子メールパラメータの設定方法については、「電子メールパラメータの設定」を参照してください。

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を含む)をソフトウェアクライアントに表示するためのウィンドウをポップアップします。

マップ表示

イベントソースがマップ上のホットスポットとして追加されると、イベントが起動されたときにホットスポットが赤色(イベントの数を示し、最大数は10)で表示され、セキュリティ担当者がイベントの場所を確認するのに役立ちます。
ホットスポットをクリックして、リンクされたカメラのイベントの詳細やライブビデオを表示することもできます。

連動カメラ

アクセスイベントが発生したときに、選択したカメラをリンクして画像を取得します。ドロップダウンリストからカメラを選択します。

- 2) OKをクリックします。
5. イベントが検出されると、イベントがクライアントに送信され、リンク・アクションが起動されるように、イベントを有効にします。
6. オプション:「コピー」をクリックして、イベント設定を他のアクセス制御装置、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。

15.7.2 アクセスイベントに対するデバイスアクションの設定

アクセス・コントロール・デバイスのトリガー・イベントに対するアクセス・コントロール・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、およびその他のアクションがトリガされます。

ステップ



注記

リンク動作は、デバイスによってサポートされる必要があります。

1. [アクセス制御]→[リンク設定]をクリックします。
2. 左側のリストからアクセス制御装置を選択します。
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. イベントタイプと詳細イベントを選択して、リンクを設定します。
6. Linkage Target領域では、この動作を有効にするプロパティターゲットを設定する。

コントローラ上のブザー

アクセス制御装置の警告音が鳴ります。

キャプチャ

イベント関連の画像は、選択したイベントが発生したときにキャプチャされます。

記録

イベント関連の画像は、選択したイベントが発生したときにキャプチャされます。



注記

機器は記録をサポートする必要があります。

リーダ上のブザー

カードリーダーの警告音が鳴ります。

アラーム出力

アラーム出力は、選択されたイベントが発生すると通知のためにトリガされません。

アラーム入力

アラーム入力をアームまたは解除する。



注記

警報入力機能をサポートすること。

アクセスポイント

ドアが開いている、閉じている、開いている、または閉じている状態がトリガされます。



注記

ターゲットドアとソースドアは同じではありません。

オーディオ再生

オーディオプロンプトがトリガされます。また、設定された再生モードに従って、選択したオーディオインデックス関連のオーディオ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: デバイスリンクを追加した後、以下のいずれかを実行できます:

リンクの編集設定	デバイスリストで設定したリンク設定を選択し、イベントソースおよびリンクターゲットを含むイベントソースパラメータを編集できます。
リンク削除設定	デバイスリストで設定されているリンク設定を選択し、削除をクリックすると削除できます。

15.7.3 カードスウィッピングのためのデバイスアクションの設定

アクセス制御装置のリンク動作(ゾーンの解除やオーディオプロンプトの起動など)を有効にして、特定のカードをスウィッピングすることで、カードホルダの動作や居場所を監視できます。

ステップ



デバイスでサポートする必要があります。

1. [アクセス制御]→[リンク設定]をクリックします。
2. 左側のリストからアクセス制御装置を選択します。
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カードを選択します。
6. カードリーダーを選択します。
7. Linkage Target領域では、この動作を有効にするプロパティターゲットを設定する。

コントローラ上のブザー

アクセス制御装置の警告音が鳴ります。

リーダー上のブザー

カードリーダーの警告音が鳴ります。

キャプチャ

イベント関連の画像は、選択したイベントが発生したときにキャプチャされます。

記録

イベント関連の画像は、選択したイベントが発生したときにキャプチャされます。



機器は記録をサポートする必要があります。

アラーム出力

アラーム出力をトリガしてお知らせします。

アラーム入力

アラーム入力をアームまたは解除する。



注記

警報入力機能をサポートすること。

アクセスポイント

ドアの開、閉、開のまま、または閉のままの状態がトリガされます。

オーディオ再生

オーディオプロンプトがトリガされます。また、設定された再生モードに従って、選択したオーディオインデックス関連のオーディオコンテンツが再生されます。

8. 保存をクリックします。

カードリーダー(手順6で設定)でカード(手順5で設定)をスウィッピングすると、リンクされたアクション(手順7で設定)を起動できます。

9. オプション:デバイスリンクを追加した後、以下のいずれかを実行できます:

リンクの削除設定	デバイスリストで設定されているリンク設定を選択し、削除をクリックします。
リンクの編集設定	デバイスリストで設定したリンク設定を選択し、イベントソースおよびリンクターゲットを含むイベントソースパラメータを編集できます。

15.7.4 個人 ID のためのデバイスアクションの設定

アクセス制御装置のリンク動作を、指定した個人IDに設定することができます。アクセス制御装置は、指定された個人IDを検出すると、アラーム出力、カードリーダーのブザーなどの動作をトリガし、指定された個人に対して特別な監視を行うことができる。

ステップ



注記

デバイスでサポートする必要があります。

1. [アクセス制御]→[リンク設定]をクリックします。
2. 左側のリストからアクセス制御装置を選択します。
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[Person Linkage]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・リストから個人を選択します。
6. カードリーダーを選択します。
7. Linkage Target領域では、この動作を有効にするプロパティターゲットを設定する。

コントローラ上のブザー

アクセス制御装置の警告音が鳴ります。

リーダ上のブザー

カードリーダーの警告音が鳴ります。

キャプチャ

イベント関連の画像は、選択したイベントが発生したときにキャプチャされます。

記録

イベント関連の画像は、選択したイベントが発生したときにキャプチャされます。



注記

機器は記録をサポートする必要があります。

アラーム出力

アラーム出力をトリガしてお知らせします。

アラーム入力

アラーム入力をアームまたは解除する。



注記

装置はゾーン機能をサポートすべきである。

アクセスポイント

ドアの開、閉、開のまま、または閉のままの状態がトリガされます。

オーディオ再生

オーディオプロンプトがトリガされます。また、設定された再生モードに従って、選択したオーディオインデックス関連のオーディオ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:デバイスリンクを追加した後、以下のいずれかを実行できます。

リンク削除設定	デバイスリストで設定されているリンク設定を選択し、削除をクリックします。
リンクの編集設定	デバイスリストで設定したリンク設定を選択し、イベントソースおよびリンクターゲットを含むイベントソースパラメータを編集できます。

15.8 ドア・エレベータ制御

モニタリングモジュールでは、追加されたアクセス制御装置によって管理されているドアまたはエレベーターのリアルタイムステータスを表示することができます。また、ドアの開閉や、ドアの開閉をリモートで行うなど、ドアやエレベーターの制御も行えます。このモジュールにはリアルタイムアクセスイベントが表示されます。アクセス内容、個人情報を表示します。

注記

ドア/エレベータ制御権限を持つユーザは、モニタリングモジュールに入り、ドア/エレベータを制御することができます。または、コントロールに使用されているアイコンが表示されません。ユーザ許可の設定については、「ユーザの追加」を参照してください。

15.8.1 制御ドアステータス

ドアのロック解除、ドアのロック解除などの状態を制御することができます。

ステップ

1. [Monitoring]をクリックして、[status monitoring]ページに入ります。
2. 右上隅の接続先グループを選択します。

注記

アクセスポイントグループの管理については、「グループ管理」を参照してください。

選択したアクセスコントロールグループのドアが表示されます。

3. ドアアイコンをクリックしてドアを選択するか、Ctrlキーを押して複数のドアを選択します。

**注記**

すべてのロックが解除されたままで、すべてのロックが解除されたままである場合は、この手順を無視してください。

4. 以下のボタンをクリックしてドアを操作します。**ロック解除**

ドアがロックされたら、ロックを解除し、一度開きます。オープン時間が過ぎると、ドアは閉じられ、自動的にロックされます。

ロック

ロックが解除されるとロックされ、閉じられます。アクセス権を有する者は認証情報を使用してドアにアクセスできます。

ロック解除のまま

ドアのロックは解除されます(閉じても開いても)。すべての人が、資格証明書を必要とせずにドアにアクセスすることができます。

ロックされたまま

扉が閉まり、鍵がかかります。スーパーユーザを除き、認定資格を持っていても、誰もドアにアクセスできない。

すべてロック解除のまま

グループ内のすべてのドアは、(閉鎖または開放にかかわらず)ロック解除されます。すべての人は、資格証明書を必要とせずにドアにアクセスすることができます。

オールロックのまま

グループ内のすべてのドアは閉じられ、施錠されます。スーパーユーザを除き、認可された資格を持っていても、誰もドアにアクセスすることはできない。

キャプチャ

手動で画像を取り込みます。

**注記**

キャプチャボタンは、デバイスがキャプチャ機能をサポートしている場合に使用できます。画像はクライアントを実行しているパソコンに保存されます。保存パスの設定については、「ファイル保存パス設定」を参照してください。

結果

操作が成功すると、操作に応じてリアルタイムでドアのアイコンが変わります。

15.8.2 制御エレベータステータス

エレベーターのドア開放、コントロール、フリー、呼び出しエレベーターなど、エレベーターのステータスをコントロールすることができます。

ステップ

注記

- エレベーターが他のクライアントによって武装されていない場合は、現在のクライアントを使用してエレベーターを制御できます。エレベータの状態が変化した場合、エレベータを他のクライアントソフトウェアで制御することはできません。
- 一度にエレベーターを制御できるクライアントソフトウェアは1つだけです。
- エレベータを制御しているクライアントは、アラーム情報を受信し、エレベータのリアルタイムステータスを表示することができます。

1. [Monitoring]をクリックして、[status monitoring]ページに入ります。
2. 右上隅の接続先グループを選択します。

注記

アクセスポイントグループの管理については、「グループ管理」を参照してください。

3. ドアアイコンをクリックしてエレベーターを選択します。
4. 以下のボタンをクリックして、エレベーターを制御します。

オープンドア

エレベーターのドアが閉まったら、それを開きます。オープン時間が過ぎると、ドアは自動的に閉じられます。

管理対象

ターゲットフロアのボタンを押す前にカードを押し込んでください。また、エレベーターは目標フロアに向かうことができます。

フリー

エレベーター内の選択したフロアのボタンは常に有効です。

障害あり

エレベーター内の選択したフロアのボタンは無効になり、ターゲットに移動できません。
フロア

結果

操作が成功すると、操作に応じてリアルタイムでドアのアイコンが変わります。

15.8.3リアルタイムアクセスレコードのチェック

リアルタイムアクセスレコードは、カードのスイッピングレコード、顔認識レコード、皮膚表面温度情報などを含むクライアントで表示することができます。また、アクセス中に撮影した画像や人物情報を見ることができます。

開始前に

クライアントに個人とアクセス制御デバイスを追加しました。詳細については、「個人管理とデバイスの追加」を参照してください。

ステップ

1. [Monitoring]をクリックして、モニター・モジュールに入ります。
リアルタイムアクセスレコードがページの下部に表示されます。カード番号、個人名、イベント時刻、ドアの場所、温度、認証の種類などの記録の詳細を表示できます。

Card No.	Person Name	Event Time	Door Location	Temperature	Abnormal Temperature	Authentication Type	Person	Linked Capture Picture
XXXXXXXXXX	XXXXXXXXXX	2020-05-15 17:03:44	Door1	35.8°C	No	Card/Face		
XXXXXXXXXX	XXXXXXXXXX	2020-05-15 17:03:41	Door1	35.8°C	No	Card/Face		
XXXXXXXXXX	XXXXXXXXXX	2020-05-15 17:03:39	Door1	35.8°C	No	Card/Face		
XXXXXXXXXX	XXXXXXXXXX	2020-05-15 17:03:39	101-Door1	-	-	-		

図 15-15 リアルタイムアクセスレコード

注記

アクセス・イベント・テーブルの列名を右クリックして、実際の必要に応じて列を表示または非表示にすることができます。

2. オプション: 右上隅のドロップダウンリストからアクセスポイントグループを選

- 択し、選択したグループのリアルタイムアクセスレコードを表示します。
3. オプション: イベント・タイプおよびイベント・ステータスを確認してください。
検出された検知済みイベントのタイプとステータスは、以下のリストに表示されます。
 4. オプション: 最新のアクセスレコードを表示するには、Show Latest Eventをチェックします。レコードリストは、時系列的に逆に表示されます。
 5. オプション: 異常温度プロンプトを有効にして、皮膚表面温度の異常プロンプトを有効にします。
-

 注記

有効にすると、温度情報に異常がある場合、モニタモジュールに入ると、人物の写真、皮膚表面温度、カード番号、人名などを表示する「温度異常」ウィンドウがポップアップします。

6. オプション: イベントをクリックして、人物の写真(撮影した写真とプロフィールを含む)を表示します。
-

 注記

「リンクされたピクチャ」フィールドで、キャプチャした画像をダブルクリックして、拡大した画像を表示できます。

7. オプション: クリックすると、サーベイランスの詳細情報(人物の詳細情報とキャプチャした画像を含む)が表示されます。
-

 注記

ポップアップウィンドウで、クリックできます。サーベイランスの詳細をフルスクリーンで表示します。

第 16 章 時間と勤怠

「時間と勤務時間」モジュールは、従業員が勤務を開始・終了した時点を追跡・監視し、遅刻、早退、休憩時間、欠勤などの従業員の労働時間を完全に管理するための多面的な機能を提供する。

注記

このセクションでは、出席報告書入手する前に構成について説明します。これらの構成の後に記録されたアクセスレコードは、統計で計算されます。

16.1 フローチャート

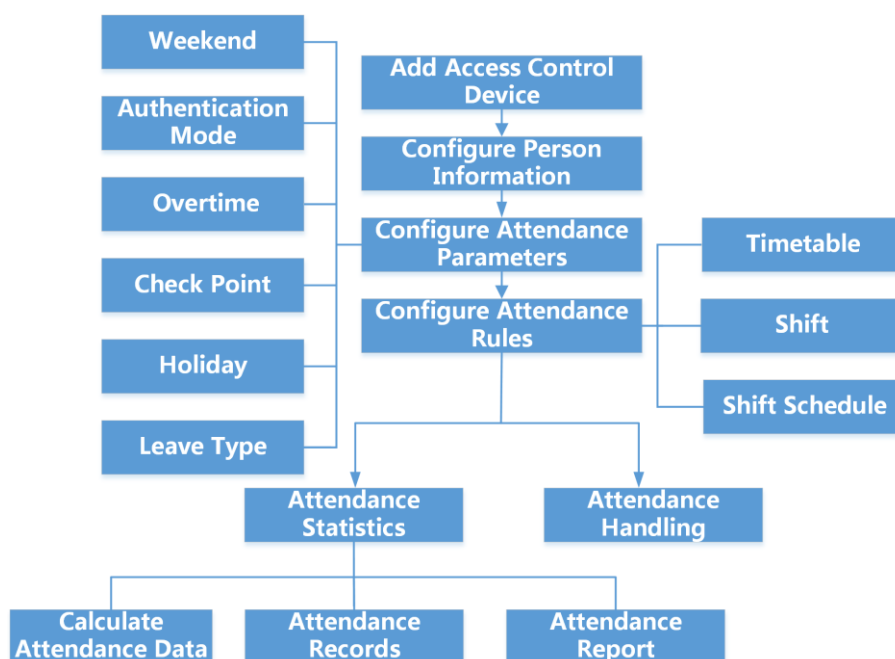


図 16-1 時間と勤怠のフローチャート

- Add Access Control Devices: クライアントにアクセス・コントロール・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」を参照してください。
- 個人情報の設定: クライアントに個人情報を追加してから、時間と出勤率のパラメータを設定してください。詳細については、Person Managementを参照してください。

- **週末の設定**: クライアントの実際の要件に応じて、週末として1日以上を選択できます。詳しくは、「週末の設定」を参照してください。
- **認証モードの設定**: カードなどの認証モードを設定できます。指紋、顔など詳細については、「認証モードの設定」を参照してください。
- **時間外勤務パラメータの設定**: 残業時間レベル、労働時間率など、労働日と週末の時間外勤務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」を参照してください。
- **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以下のように設定できます。クライアントの出勤チェックポイント詳細については、「残業パラメータの設定」を参照してください。
- **Holiday の設定**: クライアントにチェックインまたはチェックアウトが記録されない休日を追加できます。詳細は、「休日の設定」を参照してください。
- **Leave Type の設定**: 実際の必要に応じて、Leave Type をカスタマイズできます。詳細は、Configure Leave Typeを参照してください。
- **スケジュールの追加**: 実際のニーズに応じて、クライアントの従業員のための一般的なスケジュールと柔軟なスケジュールを追加できます。詳細については、「フレキシブル・スケジュールの追加」および「一般的なスケジュールの追加」を参照してください。
- **Add Shift**: シフト期間や有効出勤時間の設定など、従業員のシフトを追加できます。詳細は、「Add Shift」を参照してください。
- **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、個人スケジュール、および一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」を参照してください。
- **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するか、手動で出勤データを計算できます。詳細については、「出勤データの計算」を参照してください。
- **出勤記録**: 出勤時間、出勤状況、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および表示できます。詳細については、「従業員の出勤データの概要」を参照してください。
- **勤怠レポート**: クライアントは、従業員の勤怠レポートを作成して、従業員の勤怠結果を表示することをサポートする。また、レポートの内容を事前に定義し、自動的に電子メールでレポートを送信することもできます。詳細については、「即時レポートの生成と定期的なレポートの送信」を参照してください。

16.2 出勤パラメータの設定

勤怠パラメータ(一般規則、残業パラメータを含む)を設定することができます。
出勤チェックポイント、休日、休暇の種類等

16.2.1 週末設定

土日は国や地域によって異なります。クライアントは週末定義機能を提供する。週末は、実際の必要に応じて1日以上を選択し、就業日から週末までの出勤ルールを変更することができます。

ステップ



ここで設定されたパラメータは、新たに追加された期間のデフォルトとして設定されません。それはできない存在するものに影響する。

1. [Time & Accendance]モジュールを入力します。
2. [出勤設定]→[一般規則]をクリックします。
3. 土曜日や日曜日など、週末の曜日を選択します。
4. 保存をクリックします。

16.2.2 認証モードの設定

クライアントは、カード、指紋、顔、カード、指紋などの認証モードの設定をサポートします。認証モードを設定した後、クライアント経由で設定された認証モードのデバイスイベントを取得することができ、クライアントは設定された認証モードの出席データを計算します。

[出勤設定]→[一般規則]→[認証モード]の順にクリックします。

[すべて]、[カード]、[FP]、[顔]、[カード/FP]、[カード/顔]、[FP/顔]、[カード/FP/顔]のドロップダウンリストから認証モードを選択します。



- この機能はデバイスでサポートされている必要があります。
 - 認証モードを設定した後は、設定された認証モードの出席記録および設定された認証モードの出席データのみを取得できます。
-

16.2.3 残業時間パラメータの設定

残業時間レベル、労働時間率、残業時間の出勤状況など、労働日と週末の残業時間のパラメータを設定できます。

ステップ

1. [Time & Attendance] → [Acceptance Settings] → [Overtime time] をクリックします。
2. 必要な情報を設定する。

就業日の時間外労働の水準

終業後一定期間勤務すると、残業レベル1、残業レベル2、残業レベル3となります。3つの時間外労働について、それぞれ異なる労働時間率を設定することができます。

労働時間率

労働時間率は、残業時間を乗じて算出する。就業日の終業後一定期間勤務すると、残業時間が変わる。

レベル3つの時間外勤務レベルに対して、異なる勤務時間率(1~10、小数点以下)を設定できます。たとえば、有効な残業時間は1時間(残業時間1)で、残業時間1の労働時間率は2に設定され、その期間の労働時間は2時間として計算されます。

就業時間外勤務規程

週末の残業ルールを有効にし、計算モードを設定できます。

3. 保存をクリックします。

16.2.4 出勤チェックポイントの設定

アクセス制御装置のカードリーダーを立ち会いチェックポイントに設定し、カードリーダーの認証を立ち会いのために記録することができます。

開始前に

- アクセス制御装置を追加した。詳細については、「デバイスの追加」を参照してください。
- T&Aステータスを有効にした。詳細については、Add General Timetableを参照してください。

デフォルトでは、追加されたアクセス制御装置のすべてのカードリーダーが開始/終了チェックポイントとして設定されます。カードリーダーのチェックポイント機能を編集する必要がある場合は、以下の操作ができます。

ステップ

1. [Time & Attendance]モジュールを入力する。
2. 「勤怠設定」→「勤怠チェックポイント」をクリックして、勤怠チェックポイントを入力する。
設定ページ
3. 「チェックポイント」スイッチの「全カードリーダー設定」を「オフ」にします。
4. 以下のリストで、希望のカードリーダーを勤怠チェックポイントとして確認します。
5. チェックポイント機能をStart/End-Work、Start-Work、End-Workに設定します。

 注記

「Start-Work」または「End-Work」を選択した場合、デバイスからアップロードされた出勤状態は、ここで設定したチェックポイント機能により決定されます。

始業・仕事

デバイスからアップロードされた出勤状態はすべてチェックインとして計算されます。

エンドワーク

機器からアップロードされた出勤状態は全てチェックアウトとして計算されます。

始業・終業

出勤状況は、実際の出勤状況に応じてチェックイン/アウトとして計算する。
デバイスのステータス

6. 「チェック・ポイントとして設定」をクリックする。
設定された出席チェックポイントが右側のリストに表示されます。
7. オプション:出勤確認ポイントを設定した後、以下の操作を行います。

チェックポイントの編集

出席チェックポイントを1つチェックし、編集をクリックして情報を編集します。

名前、チェックポイント機能など

複数の出勤チェックポイントを確認し、Edit to batch edit check point functionをクリックし、備考を入力するなど

チェックポイントの削除

1つ以上のチェックポイントをチェックし、削除をクリックして削除します。

16.2.5 休日の設定

チェックインやチェックアウトが記録されない休日を追加できます。

レギュラーホリデーの追加

有効期間中、通常の日には毎年有効となる休日を設定できます。

元日、独立記念日、クリスマスなどの時期

ステップ


1. [Time & Attendance]モジュールを入力する。
2. 「出勤設定」→「休日」をクリックして、「休日設定」ページを入力します。

3. レギュラー・ホリデー・タイプをチェックします。
4. 祝日の名前をカスタマイズします。
5. 休日の初日を設定します。
6. 休日の日数を入力します。
7. 休日勤務の場合は、勤務状況を設定する。
8. オプション:この休日設定を毎年有効にするために、毎年繰り返し確認します。
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。

別の休日に設定した場合は、最初に追加した休日として記録されます。

10. オプション:休日を追加した後、以下のいずれかの操作を行います。

休日編集 クリックして、祝日情報を編集します。 

休日削除 追加した休日を1つ以上選択し、削除をクリックして、休日リストから休日を削除します。

変形休暇の追加

休日を設定することができます。この休日は、有効期間中の不規則な日に毎年有効になります。

バンク・ホリデーなどの期間

ステップ

1. [Time & Attendance]モジュールを入力する。
2. 「出勤設定」→「休日」をクリックして、「休日設定」ページを入力します。
3. 「追加」をクリックして、「休日の追加」ページを開きます。
4. 休日タイプとして、不定期休日を確認する。
5. 祝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月の第4木曜日を感謝祭休暇として設定する場合は、4つのドロップダウンリストから2019年、11月、4日、および木曜日を選択します。

7. 休日の日数を入力します。
8. 休日勤務の場合は、勤務状況を設定する。
9. オプション:この休日設定を毎年有効にするために、毎年繰り返しチェック
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。

別の休日に設定した場合は、最初に追加した休日として記録されます。

11. オプション:休日を追加した後、以下のいずれかの操作を行います。

休日編集 クリックして、祝日情報を編集します。■

休日削除 追加した休日を1つ以上選択し、削除をクリックして、休日リストから休日を削除します。

16.2.6 リーブ・タイプの設定

実際のニーズに合わせて、休暇の種類(メジャーリーフ、マイナーリーフ)をカスタマイズすることができます。また、リーブの種類を編集または削除することもできます。

ステップ

1. [Time & Attendance]モジュールを入力する。
2. [出勤率の設定]→[Leave Type]をクリックして、[Leave Type Settings]ページに入ります。
3. 左側の[追加]をクリックして、メジャー・リーブ・タイプを追加します。
4. オプション:メジャー・リーブ・タイプの場合、以下のいずれかの操作を実行します。

編集 カーソルをメジャー・リーブ・タイプに合わせてクリックして、メジャー・リーブ・タイプを編集します。■

削除 1つのメジャー・リーブ・タイプを選択し、左側のDeleteをクリックして、メジャー・リーブ・タイプを削除します。

5. マイナーリーフの種類を追加するには、右側の[追加]をクリックします。
6. オプション:マイナーリーフ・タイプの場合、以下のいずれかの操作を実行します。

編集 マイナーリーフの種類の上にカーソルを合わせ、クリックしてマイナーリーフの種類を編集します。■

削除 1つまたは複数のメジャー・リーブ・タイプを選択し、選択したマイナー・リーブ・タイプを削除するには、右側の[Delete]をクリックします。

16.2.7 認証レコードをサードパーティのデータベースに同期させる

クライアントに記録された出勤データは、他のシステムで計算または他の操作に使用することができます。同期機能を有効にすると、クライアントからの認証レコードをサードパーティのデータベースに自動的に適用できます。

ステップ

1. [Time & Attendance]モジュールを入力します。
2. 「出席設定」→「サードパーティ・データベース」をクリックします。
3. Apply to Databaseスイッチをオンにして、同期機能を有効にします。
4. SQLServerまたはMySQLとしてデータベースの種類を選択します。



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. サーバのIPアドレス、ポート番号、データベース名、ユーザー名、パスワードなど、サードパーティのデータベースに必要なその他のパラメータを設定します。



注記

選択したデータベースタイプのデフォルトポート番号が自動的に表示されます。必要に応じて、ポートNo.をカスタマイズするために、1~65535の範囲の番号を入力できます。

6. データベースのテーブルパラメータを、実際の構成に応じて設定します。
 - 1) サードパーティのデータベースのテーブル名を入力します。
 - 2) クライアントとサードパーティのデータベース間でマップされたテーブルフィールドを設定します。
7. [Save]をクリックして、データベースを接続できるかどうかをテストし、成功した設定を保存します。

接続

 - 出席データはサードパーティの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の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された時間帯に記録されたデータをサードパーティのデータベースに同期させます。

16.2.8 勤怠計算精度の設定

出勤データを正確に計算するために、出勤計算の最小単位や四捨五入制御ルールなど、出勤項目ごとに出勤精度を設定することができます。例えば、リープ時間の最小単位を1時間に設定したり、丸め制御ルールを丸めたりすることができます。

ステップ

1. [時刻と勤怠]モジュールを入力します。
2. [出勤設定]→[一般規則]をクリックします。
3. 詳細機能エリアで、最小単位(分、時間、就業日を含む)を次のように設定します。

異なる統計項目
4. 各統計項目の四捨五入制御(四捨五入、四捨五入、四捨五入を含む)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

残業時間については、最小単位を1時間、四捨五入制御ルールを四捨五入とし、残業時間が1時間未満の場合は、0として算出する。残業時間が1.5時間の場合、1時間として計算される。

16.2.9 休憩時間の設定

ブレイク時間を追加して、ブレイクの開始時間、終了時間、継続時間、計算モード、およびその他のパラメータを設定できます。また、追加した休憩時間を編集・削除することもできます。

ステップ

1. [Time & Attendance]→[Timetable]→[Break Time]の順にクリックします。追加された休憩時間がリストに表示されます。
2. 「休憩時間設定」をクリックし、「休憩時間設定」画面に入ります。
3. 追加をクリックします。
4. 休憩時間の名前を入力します。
5. 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

ブレイクの開始時刻と終了時刻を設定します。

早くない/遅くない

ブレイク開始時刻のうち最も早い時刻と、ブレイク終了時刻のうち最も遅い時刻を設定します。

休憩時間

ブレイクの開始時刻から終了時刻までの継続時間。

計算**オートデダクト**

ブレイク時間は自動的に60分と計算されます。

必須チェック

休憩時間は、実際のチェックイン・チェックアウト時間に応じて算出し、勤務時間から除外する。

早朝休憩からの復帰

実際のチェックインおよびチェックアウト時間は休憩時間を超えず、通常の勤務または時間外勤務としてマークすることができる。

遅延休憩からの返却

実際のチェックイン・チェックアウト時間が休憩時間を超えており、遅刻・欠勤・早退と表示される。

計算者

各チェックイン/チェックアウト: 各チェックイン時間とチェックアウト時

間は有効であり、隣接チェックインとチェックアウト時間の間の全期間の合計は、ブレイクタイム持続時間として記録される。

First In & Last Out: 最初のチェックイン時間は開始ブレイク時間として記録され、最後のチェックアウト時間は終了ブレイク時間として記録されます。

T&Aステータスの有効化

Enable T&A Status スイッチをオンにして、以下の手順で実際の休憩時間を計算します。

デバイスの出席状況



注記

この機能は、装置がサポートする必要があります。

有効な認証間隔

有効な認証インターバルの間、数回の個人カードのスイッピングは、出勤データを計算するときに1回のみ計算されます。

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」をクリックして、休憩時間の追加を続行します。

16.3 General Timetable の追加

タイムテーブルページでは、従業員の全般的なスケジュールを追加することができます。これには、始業時刻と終業時刻が固定されている必要があります。また、有効なチェックイン/アウト時間、遅刻・早退の許容タイムテーブルを設定することができます。

ステップ

1. [Time and Attendance]→[Timetable]をクリックして、[Timetable settings]ページを入力します。
2. [追加]をクリックして、タイムテーブルページの追加を入力します。

Basic Settings

Name: Timetable 1

Timetable Type: General

Calculated by: Each Check-In/Out

Valid Authentication Interval: 1 min

Enable T&A Status:

Attendance Time

Start-Work Time: 9:00

End-Work Time: 18:00

Valid Check-in Time: 8:30 to 9:30

Valid Check-out Time: 17:30 to 18:30

Calculated as: 540 min

Late Allowable: 10 min

Early Leave Allowable: 10 min

Configuration Result

24 00 02 04 06 08 10 12 14 16 18 20 22 24 00 02

Valid Time of Check-In/Out Work Time Late/Early Leave Allowable

Absence Settings

Save

図16-2 スケジュールの追加

3. タイムテーブルの名前を作成します。

注記

名前の横にあるカラーアイコンをクリックすると、Configuration Result 領域のタイムバーの有効なタイムテーブルの色をカスタマイズできます。

4. 一般的には、タイムテーブルの種類を選択します。

5. 計算方法を選択します

ファーストイン&ラストアウト

最初のチェックイン時間は開始時刻として記録され、最後のチェックアウト時間は終了時刻として記録される。

各チェックイン/アウト

各チェックイン時間およびチェックアウト時間は有効であり、隣接するチェックイン時間とチェックアウト時間の間の全期間の合計が有効な作業時間として記録される。

この計算方法では、有効認証間隔を設定する必要があります。例えば、同一カードのカードスウィッピング間隔が設定値を下回ると、カードスウィッピングは無効となります。

6. オプション:「T&A Status」スイッチを「Enable」に設定し、デバイスの出席状況に応じて計算します。

 注記

この機能は、装置がサポートする必要があります。

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・終業時刻

始業・終業時刻を設定します。

有効なチェックイン/アウト時間

タイムバー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が有効なタイムテーブルを設定します。

計算方法

実際の作業時間として計算した時間を設定します。

遅刻・早退可

遅刻・早退のスケジュールを設定する。

8. 欠勤関連パラメータを設定します。

チェックイン、後日

チェックインしたが勤務が遅れた社員の遅刻時間を設定できます。従業員が所定の期間を超えた場合、出勤データは欠勤とマークされる。

点検・早期休暇

通常の休暇より早くチェックアウトした従業員の早期休暇期間を設定することができ、その従業員の出勤データは欠勤としてマークされます。

チェックインなし

従業員がチェックインしない場合、その従業員の出勤データは欠勤または遅刻と表示されることがある。

チェックアウトなし

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期休暇と表示されることがある。

9. 「保存」をクリックして、スケジュールを追加します。
10. オプション:スケジュールを追加した後、以下の操作を1つ以上実行します。

スケジュールの編集 関連情報を編集する時刻表を一覧から選択します。

予定表の削除 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。

16.4 フレキシブルなスケジュールの追加

タイムテーブルページでは、従業員のためのフレックスタイムテーブルを追加することができます。これは、チェックイン/チェックアウト時間を必要としませんが、従業員の労働時間(あなたが設定した開始時間からの時間)が、あらかじめ定義された労働時間以上であることを必要とします。

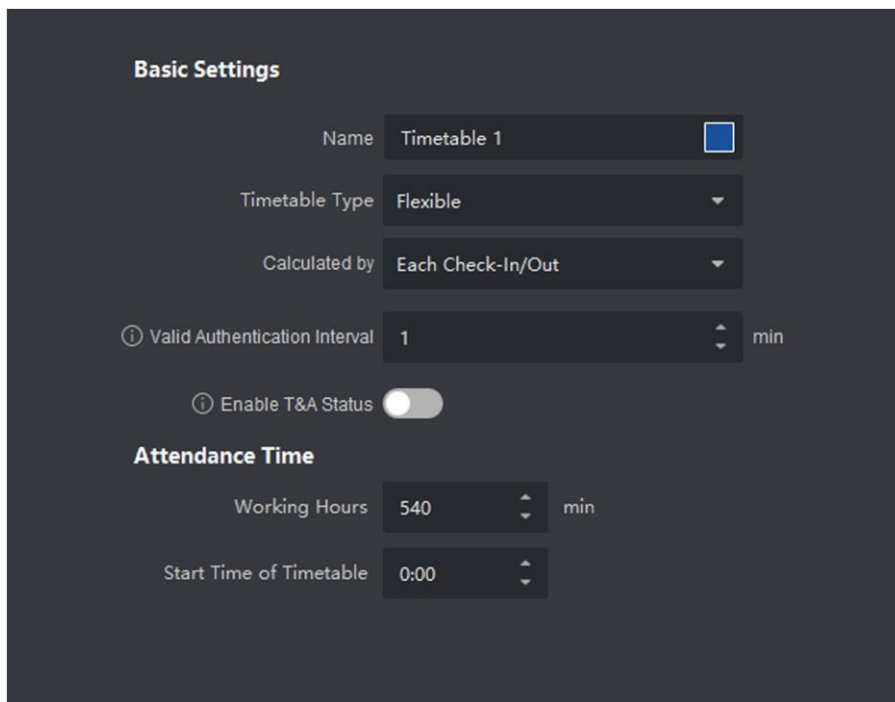
ステップ

1. [Time and Attendance]→[Timetable]をクリックして、[Timetable settings]ページを入力します。
2. [追加]をクリックして、タイムテーブルページの追加を入力します。
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すると、タイムバーの有効なタイムテーブルの色をカスタマイズできます。

4. フレキシブルにタイムテーブルタイプを選択します。



The screenshot shows the 'Basic Settings' configuration for a flexible timetable. The settings are as follows:

Field	Value
Name	Timetable 1
Timetable Type	Flexible
Calculated by	Each Check-In/Out
Valid Authentication Interval	1 min
Enable T&A Status	Disabled
Working Hours	540 min
Start Time of Timetable	0:00

図16-3 柔軟なスケジュールの追加

5. 計算方法を選択します。
ファーストイン&ラストアウト

最初のチェックイン時間は開始時刻として記録され、最後のチェックアウト時

間は終了時刻として記録される。

各チェックイン/アウト

各チェックイン時間およびチェックアウト時間は有効であり、隣接するチェックイン時間とチェックアウト時間の間の全期間の合計が有効な作業時間として記録される。

この計算方法では、有効認証間隔を設定する必要があります。例えば、同一カードのカードスウィッピング間隔が設定値を下回ると、カードスウィッピングは無効となります。

6. オプション:「T&A Status」スイッチを「Enable」に設定し、デバイスの出席状況に応じて計算します。



注記

この機能は、装置がサポートする必要があります。

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。

労働時間

従業員の労働時間が設定値以上であること。

スケジュールの開始時刻

設定した値から、各日の勤務時間を算出します。

例えば、勤務時間を8時間、時刻表の開始時間を9時と設定し、Aが午前8時にチェックインし、午後5時にチェックアウトした場合(有効勤務時間は午前9時から午後5時、合計8時間)、Aの出勤結果は通常通り計算されます。

8. 「保存」をクリックして、スケジュールを追加します。
9. オプション:スケジュールを追加した後、以下の操作を1つ以上実行します。

スケジュールの編集 関連情報を編集する時刻表を一覧から選択します。

予定表の削除 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。

16.5 Shiftの追加

シフト時間(日、週、月)、有効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、従業員は1シフトごとに複数のスケジュールを追加することができます。この場合、各スケジュールのチェックインとチェックアウトが必要になります。

開始前に

まずスケジュールを追加してください。詳細については、Add General Timetableを参照してください。

ステップ

1. [時刻 & 出勤] → [シフト] をクリックして、シフト設定ページを入力します。
2. 「追加」をクリックして、「Add Shift」ページを入力します。
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。

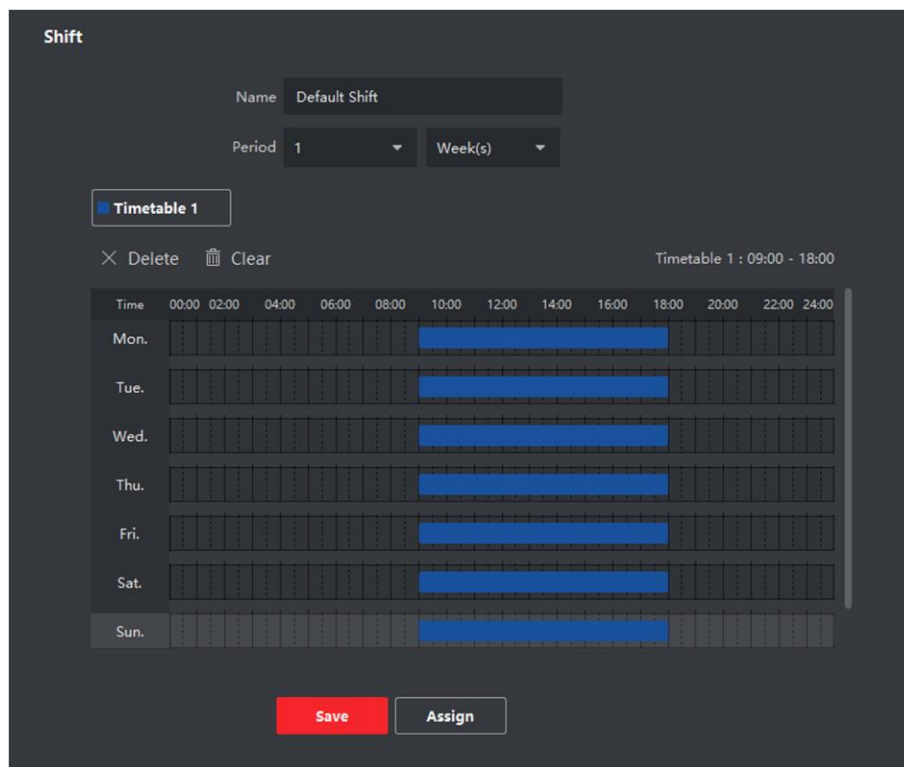


図16-4 追加シフト



注記

複数のタイムテーブルを選択できます。開始と終了の作業時間、および異なるタイムテーブルでの有効なチェックインとチェックアウトの時間は重複できません。

6. 保存をクリックします。
ページの左パネルに追加されたシフトリストが表示されます。最大64回のシフトを追加できます。
7. オプション:組織または担当者へのシフトを割り当てて、迅速な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] タブまたは [個人] タブを選択し、希望する組織または個人をチェッ

くします。選択した組織または人物が右ページに一覧表示されます。

- 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は、入社時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

このスケジュールでは、作業終了時にチェックアウトする必要はありません。

休日予定

休日には、このスケジュールはまだ有効であり、スケジュール通りに仕事に行く必要があります。

時間外勤務に有効

このスケジュールでは、人の残業が記録されます。

- 5) 「保存」をクリックして、クイックシフトスケジュールを保存します。

16.6 シフトスケジュールの管理

シフト勤務とは、毎日24時間勤務することを目的とした雇用慣行のことである。実務では、通常、日を交替勤務に分割し、交替勤務の時間帯を設定し、交替勤務の時間帯を設定します。

部門スケジュール、個人スケジュール、および一時スケジュールを設定できます。

16.6.1 部門スケジュールの設定

1つの部署のシフトスケジュールを設定することができ、その部署の全員にシフトスケジュールが割り当てられます。

開始前に

[Time & Attendance]モジュールでは、部門リストは組織と同じです。まず、「個人」モジュールの組織と個人を追加します。詳細については、Person Managementを参照してください。

ステップ

1. [Time & Attendance] → [Shift Schedule] をクリックして、[Shift Schedule Management] ページを入力します。
2. [Department Schedule]をクリックして[Department Schedule]ページに入ります。
3. 左側の組織リストから部署を選択します。

 注記

Include Sub Organization(サブ組織を含む)をチェックしている場合は、組織の選択時にそのサブ組織を選択します。

同時に選択される。

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、追加された人のスケジュールから有効期間を選択します。
-

 注記

これは、1つのスケジュールでのみシフトすることができます。

複数のシフトスケジュール

それには複数のタイムテーブルが含まれている。いずれかのスケジュールでチェックイン/チェックアウトができます

出席は有効となります。

複数のシフトスケジュールが、00:00～07:00、08:00～15:00、16:00～23:00の3つのタイムテーブルを含む場合。この複数のシフトスケジュールを採用する人員の出席は、3つのスケジュールのいずれかで有効となる。7:50にチェックインした場合は、08:00～15:00に最も近いスケジュールを適用します。

6. 開始日と終了日を設定します。
7. スケジュール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は、入社時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

このスケジュールでは、作業終了時にチェックアウトする必要はありません。

休日予定

休日には、このスケジュールはまだ有効であり、スケジュール通りに仕事に行く必要があります。

時間外勤務に有効

このスケジュールでは、人の残業が記録されます。

8. 保存をクリックします。

16.6.2 個人スケジュールの設定

シフトスケジュールを1人または複数の人に割り当てることができます。また、個人スケジュールの詳細を表示および編集することもできます。

開始前に

Person モジュールの部署と担当者を追加します。詳細については、Person Management を参照してください。

ステップ



注記

個人スケジュールは、部門スケジュールよりも優先順位が高い。

1. [Time & Attendance] → [Shift Schedule] をクリックして、[Shift Schedule] ページを入力します。
2. 「個人スケジュール」をクリックして、「個人スケジュール」ページを入力します。
3. 組織を選択し、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、追加された人のスケジュールから有効期間を選択します。



注記

これは、1つのスケジュールでのみシフトすることができます。

複数のシフトスケジュール

それには複数のタイムテーブルが含まれている。いずれかのスケジュールでチェックイン/チェックアウトができます

出席は有効となります。

複数のシフトスケジュールが、00:00～07:00、08:00～15:00、16:00～23:00の3つのタイムテーブルを含む場合。この複数のシフトスケジュールを採用する人員の出席は、3つのスケジュールのいずれかで有効となる。7:50にチェックインした場合は、08:00～15:00に最も近いスケジュールを適用します。

6. 開始日と終了日を設定します。
7. スケジュール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は、入社時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

このスケジュールでは、作業終了時にチェックアウトする必要はありません。

休日予定

休日には、このスケジュールはまだ有効であり、スケジュール通りに仕事に行く必要があります。

時間外勤務に有効

このスケジュールでは、人の残業が記録されます。

8. 保存をクリックします。

16.6.3 臨時スケジュールの設定

担当者の一時スケジュールを追加することができ、担当者はシフトとともに割り当てられます。

一時的にスケジュールする。また、一時スケジュールの詳細を表示および編集することもできます。

開始前に

Person モジュールの部署と担当者を追加します。詳細については、Person Management を参照してください。

ステップ



臨時スケジュールは、部門スケジュールおよび人員スケジュールよりも優先順位が高い。

1. [Time & Attendance] → [Shift Schedule] をクリックして、[Shift Schedule Management] ページを入力します。
2. [Temporary Schedule] をクリックして [Temporary Schedule] ページを入力します。
3. 組織を選択し、人物を選択します。
4. 1つの日付をクリックするか、またはクリック&ドラッグして、一時スケジュールの複数の日付を選択します。
5. ドロップダウン・リストから「就業日」または「非就業日」を選択します。
「Non-Workday」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。

計算方法

臨時の勤務状況を示すために、通常勤務または時間外勤務のレベルを選択する。

時刻表

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。

多重シフトスケジュール

それには複数のタイムテーブルが含まれている。いずれかのスケジュールでチェックイン/チェックアウトができます

出席は有効となります。

複数のシフトスケジュールが、00:00～07:00、08:00～15:00、16:00～23:00の3つのタイムテーブルを含む場合。この複数の交替勤務スケジュールを採用した者の出席は、次の通りとする。

3つのタイムテーブルのいずれかで有効です。7:50にチェックインした場合は、08:00～15:00に最も近いスケジュールを適用します。

規則


チェックイン不要、チェックアウト不要など、スケジュールの他のルールを設定します。

6. 保存をクリックします。

16.6.4 シフトスケジュールの確認

カレンダーやリストモードでシフトスケジュールを確認できます。シフトを編集または削除することもできます。

ステップ

1. [Time & Attendance] → [Shift Schedule] をクリックして、[Shift Schedule Management] ページを入力します。
2. 組織と担当者を選択します。
3. 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クリックまたは表示します。

カレンダー

カレンダーモードでは、各日のシフトスケジュールを1ヶ月で表示できます。1日分の一時スケジュールをクリックして、編集または削除できます。

リスト

リストモードでは、シフトの名前、タイプ、有効期間など、1人または組織に関するシフトスケジュールの詳細を表示できます。シフトスケジュールを確認し、削除をクリックして選択したシフトスケジュールを削除します。

16.7 チェックイン/チェックアウトレコードの手動修正

出勤状態が正しくない場合は、チェックインまたはチェックアウトレコードを手動で修正することができます。チェックインまたはチェックアウトレコードを編集、削除、エクスポートすることもできます。

開始前に

- 「個人」モジュールに組織と個人を追加する必要があります。詳細について

ては、「人物管理」を参照してください。

- 出勤状況が間違っている。

ステップ




1. 「時刻と出勤」→「出勤処理」をクリックして、出勤処理ページに入ります。
2. 「チェックイン/アウトの修正」をクリックして、チェックイン/アウトの修正ページを追加します。
3. 修正対象の左リストから1人以上を選択します。
4. 修正日を選択します。
5. チェックイン、チェックアウト、ブレイクイン、ブレイクアウトなどの補正タイプを選択します。正しく設定してください
時間




注記

クリックできます。複数の修正項目の追加チェックイン/チェックアウト項目は最大8項目まで追加できます。

6. オプション:必要に応じてリマーク情報を入力します。
7. Saveをクリックして、上記の設定を保存します。
8. オプション:チェックイン/チェックアウト補正を追加した後、以下のいずれかの操作を行います。

<p>ビュー</p>	<p>カレンダーまたはリストモードで、追加した出席処理情報をクリックまたは表示します。 </p>
<p>編集</p>	<ul style="list-style-type: none"> ・ カレンダーモードで編集→編集をクリックし、詳細を編集します。  ・ リストモードでは、Date、Handling Type、Time、Remark 列の関連するフィールドをダブルクリックして、詳細を編集します。 <hr/> <p> 注記 編集されたチェックイン/アウトの修正は影響を受けます。</p>
<p>削除</p>	<ul style="list-style-type: none"> ・ カレンダーモードで、チェックイン/チェックアウトの修正を1つ選択し、削除をクリックして選択した項目を削除します。 ・ リストモードで、チェックイン/チェックアウトの修正を1つ以上 チェックし、削除をクリックして選択した項目を削除します。

	 注記 削除されたチェックイン/アウトの修正は、もはや影響を受けない。
輸出	リストモードで、1つ以上のチェックイン/アウトの修正をチェックして参加者をエクスポートします。 ローカルPCへの詳細(CSVファイル)の取り扱い。

16.8 休暇・出張の追加

休暇の申請や出張を希望する場合には、休暇や出張を追加することができます。

開始前に

「個人」モジュールに組織と個人を追加する必要があります。詳細については、「人物管理」を参照してください。

ステップ




1. 「時刻と出勤」→「出勤処理」をクリックして、出勤処理ページに入ります。
2. 「休暇・出張申請」ボタンを押下し、休暇・出張ページを追加する。
3. 左リストから人物を選択します。
4. 休暇や出張の日程を設定します。
5. ドロップダウンリストから、メジャー・リーブ・タイプとマイナー・リーブ・タイプを選択します。



注記

「勤怠設定」では、リーブの種類を設定できます。詳細は、「リーブタイプの設定」を参照してください。

6. 休暇の時間を設定します。
7. オプション:必要に応じてリマーク情報を入力します。
8. 保存をクリックします。
9. オプション:休暇・出張を加算した後、次のいずれかの操作を行います。

ビュー	<p>カレンダーまたはリストモードで、追加した出席処理情報をクリックまたは表示します。</p> <hr/> <p> 注記 カレンダー・モードでは、「計算」をクリックして、1ヶ月後の出席状況を取得する必要があります。</p> <hr/>
編集	<ul style="list-style-type: none"> ・ 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。 ・ リストモードでは、Date、Handling Type、Time、Remark 欄のファイルをダブルクリックし、関連情報を編集します。
削除	<p>選択項目を削除します。</p>
輸出	<p>出勤処理の詳細をローカルPCにエクスポートします。</p> <hr/> <p> 注記 エクスポートされた詳細は CSV 形式で保存されます。</p> <hr/>

16.9 出勤データの計算

出勤データ、従業員詳細出勤データ、従業員の異常出勤データ、従業員の残業データ、カードスウィッピングログを検索・閲覧する前に、出勤データを計算する必要があります。

16.9.1 出勤データの自動計算

クライアントが毎日設定した時刻に前日の出席データを自動的に計算できるようにスケジュールを設定できます。

ステップ

1. [Time & Attendance]モジュールを入力する。

2. [出勤設定]→[一般規則]をクリックします。
3. 「出席状況の自動計算」エリアで、クライアントがデータを計算する時間を設定します。
4. 保存をクリックします。
クライアントは、前日の出勤率データを、あなたが持っている時刻から計算します。構成されている。

16.9.2 出勤データを手動で計算する

出勤時間などの条件を設定することで、出勤データを手動で計算することができます。

部門、出席状況等


ステップ

1. [Time & Attendance]モジュールを入力する。
2. 「出勤統計」→「計算」をクリックします
3. 開始時刻と終了時刻を設定し、勤怠データの範囲を設定します。
4. ドロップダウンリストから部署を選択します。
5. オプション:その他の条件(名前と個人IDを含む)を設定します。
6. 出勤状況を確認する(複数選択対応)。
7. [計算]をクリックします。

注記

3ヶ月以内の出勤データのみ集計可能です。

8. オプション:以下の操作のいずれかを実行します。

正しいチェックイン/アウト	1名を選択し、「チェックイン/チェックアウトを修正」をクリックしてチェックイン/チェックアウトを追加します。
表示項目の選択	右上隅をクリックするか、テーブルのヘッダーを右クリックします。  リストに表示する項目をカスタマイズするための出席データリスト
項目シーケンスの調整	1つの項目(個人IDを除く)をクリックし、マウスを動かして、異なる項目のシーケンスをカスタマイズします。
レポートの生成	[レポート]をクリックして、出席報告を作成します。

	<hr/>  注記 設定したシーケンスにレポートアイテムが表示されます。 <hr/>
輸出報告書	[Export]をクリックして、出席データ(CSV ファイル)をローカル PC にエクスポートします。 <hr/>  注記 設定したシーケンスにレポートアイテムが表示されます <hr/>

16.10 勤怠統計

出勤記録の原本を確認し、計算された出勤データに基づいて出勤報告書を作成およびエクスポートすることができます。

16.10.1 従業員の勤怠データの概要を入手する

出勤時間、出勤状況、チェックポイントなど、社員の出勤データをクライアントで検索、表示できます。

開始前に

- 「Person」モジュールに組織と人物を追加し、「Person」カードを押し下げた人物がいることを確認します。詳細については、「人物管理」を参照してください。
- 出勤データを計算する。

注記

- ・クライアントは、翌日の午前 1 時に前日の出勤データを自動的に計算します。
 - ・クライアントは、午前 1:00 の状態を維持するか、前日の出勤データを自動的に計算できません。自動的に計算されない場合は、出勤データを手動で計算できます。詳細については、「出勤データの手動計算」を参照してください。
-

ステップ

1. [Time & Attendance]モジュールを入力する。
2. 「出勤統計」→「出勤記録」をクリックします。

3. 検索したい出勤開始時刻と終了時刻を設定します。
4. 他の検索条件(部署、名前、個人IDなど)を設定します。
5. データソースをAll、Original Records on DeviceまたはManually Handled Recordsとして選択します。
6. オプション:[デバイスからイベントを取得]をクリックして、デバイスから出席データを取得します。
7. オプション:すべての検索条件をリセットし、再度検索条件を編集するには、リセットをクリックします。
8. 検索をクリックします。
9. オプション:表示された検索結果に対して、以下のいずれかの操作を行います。

出席状況の編集	不正なレコードを1つ選択し、「出勤状況」列のフィールドをダブルクリックし、ドロップダウン・リストから選択して、単一の出勤状況を編集します。 複数の間違ったレコードをチェックし、左上隅の「出席状況の編集」をクリックし、ドロップダウンリストから選択して複数の出席状況を一括編集します。
レポートの生成	[レポート]をクリックして、出席報告を作成します。
輸出報告書	[Export]をクリックし、[Save path]を選択して、勤怠レポート(CVS)をローカル PC へエクスポートします
カスタムエクスポート	[カスタムレポート]をクリックし、実際のニーズに応じて出席記録をエクスポートする条件を設定します。詳細については、「カスタムエクスポート出席記録」を参照してください。

16.10.2 カスタムエクスポート出席記録

従業員の出勤データを閲覧した後、実際の必要に応じて出勤記録をエクスポートすることができます。

必要な出勤記録をエクスポートする前に、従業員の情報を検索して取得する必要があります。

出勤データ詳細については、「従業員の出勤データの概要」を参照してください。[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

エクスポート出席記録の開始時刻と終了時刻を設定します。

パスの保存

出席記録を保存するためのファイルパスを選択できます。

ファイル名

ファイルは実際のエクスポート日付に従って名前が付けられます。dd-MM-yyyy、dd-MM-yyyなどの日付の形式を選択できます。

フォーマット

.TXTおよび.CVSのオリジナル出席記録をエクスポートできます。フォーマット

セパレータ

エクスポートされたファイル内の異なる項目を区切るための区切り文字(カンマ、スペース、タブを含む)の有無を選択できます。

輸出

ID、個人名、部署、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

エクスポートするように選択した項目の情報がない場合は、空白を置き換えるためにデフォルト値を設定できます。

16.10.3 レポート表示の設定

会社名、ロゴ、日付フォーマット、時刻フォーマット、マークなど、出席報告書に表示される表示内容を設定できます。

ステップ

1. [Time & Attendance]モジュールを入力します。
2. [出勤統計]→[レポート表示]の順にクリックします。
3. 出席報告の表示設定を行います。

会社名

レポートに名前を表示するには、会社名を入力します。

出席状況マーク

マークを入力し、色を選択します。レポート内の出席状況の関連フィールドには、マークとカラーが表示されます。

週末マーク

マークを入力し、色を選択します。レポートの週末フィールドには、マークと色が表示されます。

4. 保存をクリックします。

16.10.4 即時レポートの生成

従業員の一連の出席報告書を手動で作成して閲覧することができます。

出席結果

開始前に

出勤データを計算する。

注記

出勤データを手動で計算したり、クライアントが毎日自動的にデータを計算できるようにスケジュールを設定することができます。詳細については、「出勤データの計算」を参照してください。

ステップ

1. [Time & Attendance]モジュールを入力する。
2. [出勤統計]→[レポート]をクリックします。
3. レポートの種類を選択します。
4. 出席報告書を閲覧する部署または担当者を選択します。
5. 出勤データがレポートに表示される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。

16.10.5 定期的にレポートを送信する

クライアントは、複数のレポートの種類をサポートしており、レポートの内容を事前に定義することができます。また、設定した電子メールアドレスにレポートを自動的に送信することができます。

ステップ

1. [Time & Attendance]モジュールを入力する。
2. 「出勤統計」→「定期的にレポートを送信」をクリックします。
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入力します。
4. レポートの内容を設定します。

レポート名

レポートの名前を入力します。

報告書の種類

1つのレポートタイプを選択すると、このレポートが生成されます。

レポート時刻

選択する時間は、レポートの種類によって異なります。

人

レポートの出席記録を生成する追加された人を選択します。

注記

「個人」領域の右側に、選択した人物を表示できます。

5. レポートを自動的にEメールアドレスに送信するスケジュールを設定します。



注記

自動送信機能は、デフォルトで有効になっています。

- 1) 選択した送信日にクライアントが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送信日を選択します。
- 3) クライアントがレポートを送信する送信時刻を設定します。

例

有効期間を2018/3/10～2018/4/10に設定し、送信日を金曜日に設定し、送信時間を20:00:00に設定すると、クライアントはレポートを2018/3/10の金曜日午後8時から2018/4/10の間に送信します。



注記

送信時刻の前に出勤記録が計算されていることを確認します。出勤データを手動で計算したり、クライアントが毎日自動的にデータを計算できるようにスケジュールを設定することができます。詳細については、「出勤データの計算」を参照してください。

- 4) 受信者のEメールアドレスを入力します。



注記

メールアドレスは5件まで追加できます。+をクリックすると、新しい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して、電子メールの詳細を表示します。
6. OKをクリックします。
7. オプション:カスタムレポートを追加した後で、次のいずれかを実行できます。

レポートの編集	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。
レポートの削除	1つの追加レポートを選択し、削除をクリックして削除します。

レポートの生成	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 17 章 ビデオ・インターコム

ビデオインターホン、建物または建物の小さなコレクション内で使用される視聴覚通信システムである。マイクとビデオカメラを両側に配置することで、ビデオ信号とオーディオ信号を介した通信を可能にします。ビデオ・インターホン・システムは、マンションや民家の安全で簡単なモニタリング・ソリューションを提供することができる。

あらかじめ、クライアントにビデオインターホン装置を追加し、屋内局を人とリンクさせておいてください。また、リンクされた屋内局を介してドアを開ける人のアクセス権限も設定してください。

注記

- ドアステーションは16局、マスターステーションは512局までクライアントで管理できます。ビデオインターホンデバイスの追加の詳細については、「デバイスの追加」を参照してください。
- 個人の追加の詳細については、「単一個人の追加」を参照してください。
- 個人のアクセス権限の設定の詳細については、「アクセスグループの設定を個人にアクセス権限を割り当てる」を参照してください。

17.1 フローチャート

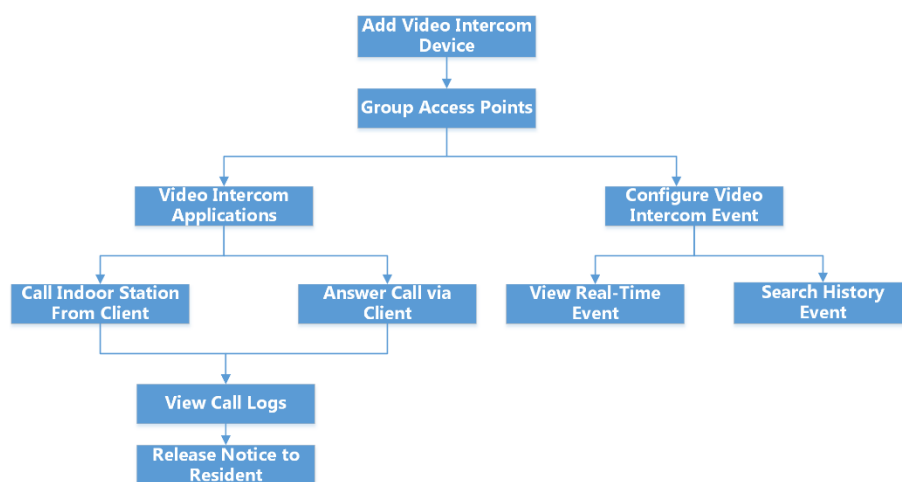


図17-1 ビデオインターコムのフローチャート

- **Video Intercom Devicesの追加:** クライアントにVideo Intercom Devicesを追加できます。詳細については、「デバイスの追加」を参照してください。
- **グループアクセスポイント:** 追加したアクセスポイントをグループにグループ化して

管理することができます。詳細については、「グループ管理」を参照してください。

- **クライアントからの屋内局の呼び出し:**追加した屋内局をクライアントから呼び出して、ビデオインターホンを実行できます。詳しくは、「お客様ご相談窓口」をご覧ください。
- **クライアント経由で電話に出る:**追加した室内局、ドアステーションなどからクライアント経由で電話に出ることで、ビデオインターホンを行うことができます。詳しくは、「クライアントからの着信」を参照してください。
- **コールログの表示:**すべてのコールの詳細を表示できます。詳細については、「リアルタイムコールログの表示」を参照してください。
- **住民へのお知らせ:**お客さまにワンタッチで住民にお知らせします。詳細については、「居住者への通知の解除」を参照のこと。
- **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されたアクションを設定すると、イベントがトリガされると通知されます。詳細は、「ビデオインターコムイベントの設定」を参照してください。
- **Search Real-Time/History Events :**リアルタイムイベントを表示し、クライアントの履歴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参照してください。

17.2 クライアントソフトウェアと屋内/ドアステーション/アクセス制御デバイス間の通話の管理

顧客は住民に電話をかけることができ、その逆もできます。また、室内局・ドアステーションや指定のアクセス制御装置を利用してクライアントを呼び出すこともできます。

電話をかける前に、呼出時間や発言時間などの設定を行います。詳細は、「アクセス制御およびビデオインターコムパラメータの設定」を参照してください。

17.2.1 お客さまからの屋内ステーションへの電話

追加した室内局をクライアントから呼び出して、ビデオインターホンを行うことができます。


開始前に

- クライアントに必ずレジデントを追加してください。詳細については、「独身者の追加」を参照してください。
- 必ず、居住者を室内局と連動させ、居住者情報(床番号、部屋番号を含む)を「Person」モジュールに設定する。リンクおよび常駐情報の設定の詳細については、「常駐情報の設定」を参照してください。

ステップ

 注記

- ビデオインターホン装置は、複数のクライアントに追加することができますが、一度に1つのクライアントのみでビデオインターホンを実行します。
- Maxをリモートで設定できます。呼出時間と最大値話す時間。

1. [アクセス制御]->[ビデオインターコム]->[連絡先]をクリックします。
2. 左パネルの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住民全員の情報(住民名、機器名、フロア番号、室番号を含む)が右側のパネルに表示されます。
3. レジストレーションを選択するか、フィルタフィールドにキーワードを入力して目的のレジストレーションを検索します。
4. クリックすると、選択した常駐者に電話をかけ始めます。 

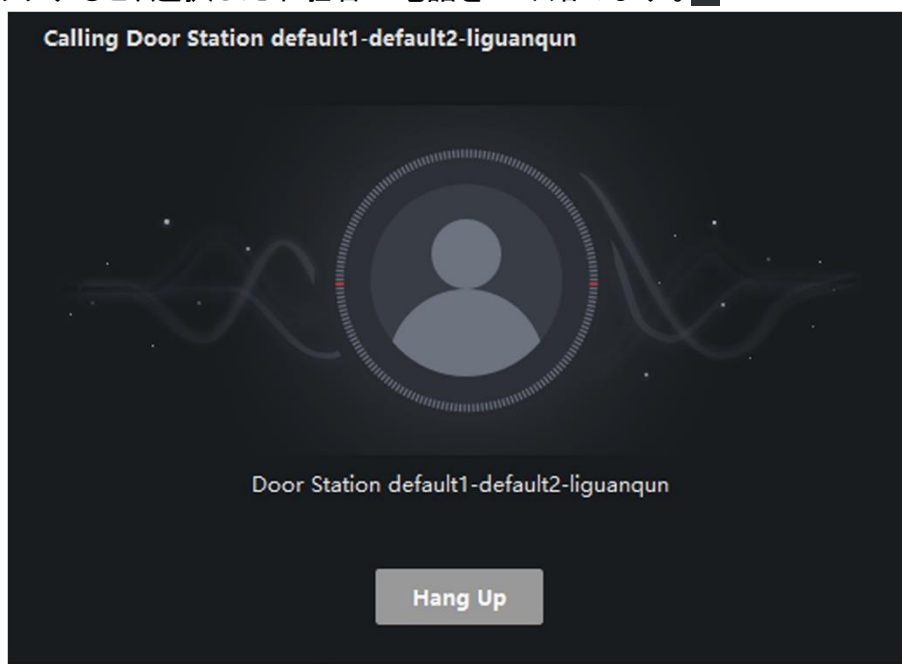


図17-2 コールの開始ウィンドウ

応答後、「着信中画面」になります。

5. オプション:着信後、以下の操作を行います。

スピーカー音量の調整	クリックして、スピーカーの音量を調整します。🔊
発言終了	発言を終了するには、ハングアップをクリックします。
マイク音量を調節する	クリックすると、マイクの音量を調節できます。🔇

17.2.2 クライアントからの電話に出る

追加した室内局、ドアステーション、または特定のアクセス制御装置からクライアント経由で電話に出て、ビデオインターホンを行うことができます。

ステップ

注記

ビデオインターホン装置は、複数のクライアントに追加することができますが、一度に1つのクライアントのみでビデオインターホンを実行します。

1. 屋内局、ドアステーション、または特定のアクセス制御装置でクライアントに電話をかける。着信ダイアログがポップアップします。

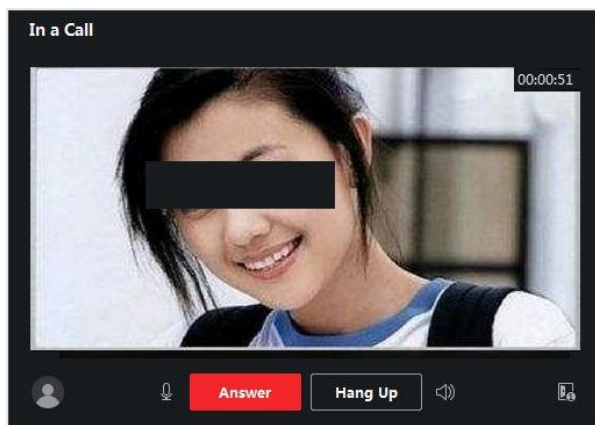





図17-3着信


2. 「応答」をクリックして、電話に出ます。
応答後、「着信中画面」になります。
3. オプション:コールインウィンドウで、以下の操作を行います。

スピーカー音量の調整	クリックして、スピーカーの音量を調整します。 
発言終了	発言を終了するには、ハングアップをクリックします。
マイク音量を調節する	クリックしてマイクの音量を調整します。 
オープンドア	屋内局とドアステーションが連動している場合は、次のボタンをクリックします。  ドアステーションにつながったドアを開けてください。

17.3リアルタイム通話履歴の表示

すべての通話の詳細を表示したり、必要に応じて住民に電話したり、ログをエクスポートしたりできます。


ステップ

- [アクセス制御]→[ビデオインターコム]→[コールログ]の順にクリックします。
すべての通話の詳細は、通話状態、開始時刻を含めて右側のパネルに表示されます。
発言時間、デバイスの種類と名前、居住者の組織と名前。
- オプション:クリックしてレジデントに再ダイヤルします。
- オプション:ページ上部の検索条件(呼び出しステータス、デバイスタイプ、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。
- 「エクスポート」をクリックして、ログ(GSVファイル)をPCに保存します。

17.4住民への通知の発出

住民にワンタッチでお知らせします。広告には4つの種類があります。
プロパティ、アラーム、通知情報

ステップ

- [アクセス制御]→[ビデオインターコム]→[通知]をクリックします。
- 「追加」をクリックして、「通知の作成」パネルを開きます。
- クリックして、通知先の住民を選択します。
- 必要な情報を入力します。

 注記

- [件名]フィールドには最大63文字まで入力できます。
 - Contentフィールドには最大1023文字まで入力できます。
 - 画像は最大6枚まで登録できます。各画像は、JPG形式で、512KB未満であること。
-

5. [送信]をクリックして、選択した住民に通知を送信します。
送信され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、お使いのパソコンにすべての通知を保存します。

17.5ビデオインターコムイベントの設定

ビデオインターホンイベントには、エレベータ、ドアベルリング、ドアロックなどの呼び出しが含まれる。クライアント上のビデオインターホンデバイスのイベントを有効にすることができます。イベントがビデオインターホン装置上でトリガされると、クライアントは、確認のためのイベントを受信し、記録し、通知のための一連のリンク動作(例えば、電子メールの送信)をトリガすることができる。

ステップ

1. [イベント設定]→[アクセス制御イベント]→[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、イベントソースとしてビデオインターホン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ます。

選択したビデオインターホン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:「フィルター」フィールドにキーワードを入力して、目的のイベントを素早く見つけます。
4. オプション:[Enable]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、[Enable All]をクリックします。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

使用可能になった後、イベントをクライアントが受信し、リンク動作をトリガすることができます。イベント・タイプを無効にしたり、すべてのイベント・タイプを無効にしたりすることもできます。

5. オプション: イベントを選択後、以下の操作を行います。

優先度の編集 「優先順位の編集」をクリックして、イベントの優先順位を設定します。優先度は、イベントの緊急度を表します。

イベントリンクの編集 「リンクの編集」をクリックして、イベントのリンク動作を設定します。

音声警告

イベントがトリガーされたら、クライアントの音声警告をトリガーします。ドロップダウンリストから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を追加します(WAV形式)。クリックすると、選択したオーディオファイルのオーディオがオーディオされます。




メールを送る

アラーム情報の電子メール通知を1つ以上の受信者に送信します。電子メールパラメータの設定方法については、「電子メールパラメータの設定」を参照してください。

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、クライアントにイベント関連情報(イベントの詳細、リンクされたカメラの撮影画像を含む)を表示するポップアップウィンドウ。また、イベントの処理方法についてのコメントも入力できます。

マップ表示

イベントソースがマップ上のホットスポットとして追加されると、イベントがトリガーされたときにホットスポットが輝きを放つように表示されます。これは、セキュリティ担当者がイベントの場所を確認するのに役立ちます。ホットスポットをクリックして、リンクされたビデオインターホン装置のイベント詳細とライブビデオを表示することもできます。

連動カメラ

イベントがトリガーされたときに、選択したカメラをリンクして、画像を撮影したり、ビデオを録画したりします。

[コピー]をクリックして、このビデオインターホンデバイスのイベント設定を他のビデオインターホン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。

次にすべきこと

ビデオ・インターコム・デバイスが属するデバイスをアームする必要があります。そうでなければ、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の受信を有効にする」を参照してください。

第 18 章 トポロジー管理


トポロジー管理モジュールは、正常なリンク送信とネットワーク内のリソースのより良い使用を保証するために、ハードウェアとソフトウェアに基づいてネットワークヘルス状況モニタ機能を提供します。主にネットワークの保守・管理に使用されています。管理者は、トポロジー・ビューを介してデバイスとその接続されたデバイスのステータスを確認し、リアルタイム・ネットワークのステータスを知ることができます。

18.1 トポロジー表示の概要

トポロジー表示ページには、クライアントに追加されたデバイス、SADPを介して検索されたデバイス、および追加されたデバイスまたは検索されたデバイスに接続されたデバイスなど、クライアントによって取得された異なるデバイス間の関係が表示されます。デバイス情報、リンク送信状態などを確認できます。

注記

- SADPを介してデバイスを検索する場合、トポロジー・ビューのデバイス名は、IPアドレスと一致します。
- 未知のデバイスの場合、トポロジー・ビューにはデバイス・タイプのみが表示されません。

Topologyモジュールを入力し、クリックして最新のデバイスリストを取得し、トポロジー関係を表示します。初めてTopologyページを入力した場合は、ガイドに従い、Add Topologyをクリックしてトポロジー・ビューを生成します。クリックすると、実際の必要に応じてリフレッシュできます。 

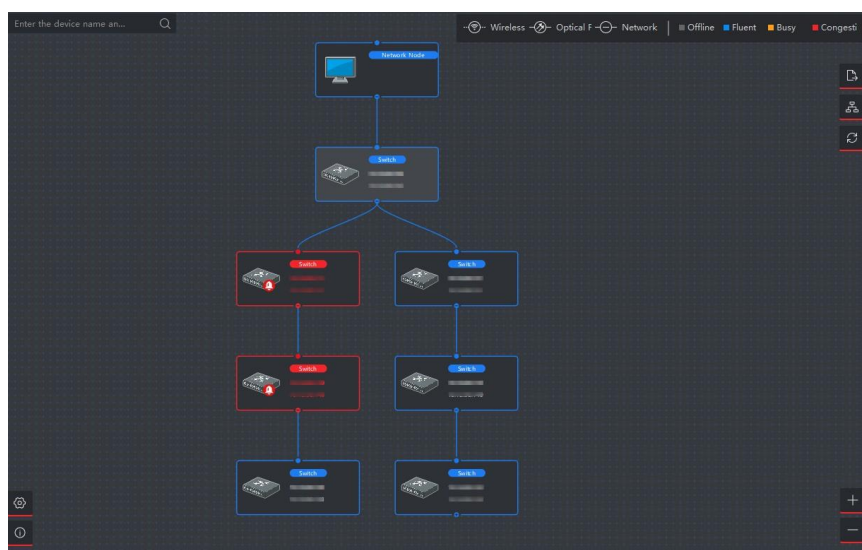



図18-1 トポロジー

デバイスノード

- **デバイス情報の表示:** デバイスの種類とIPアドレスを確認できます。

注記

デバイス名、IPアドレス、オンラインステータスなどのデバイス情報を編集すると、トポロジー・ビューのデバイス情報が同期的に変化します。

- **Expand / Hide :** 特定の装置のサブノードを展開または非表示にするには、[或] を押します。 
- **Topology View の調整:** 右下隅にあるアイコンをクリックするか、マウスホイールをスクロールして、Topology を拡大または縮小できます。
- **検索トポロジー:** 左上隅にデバイスの別の名前またはIPアドレスを入力して、対応するトポロジーを表示することができます。

ライン

右上隅には、回線(ワイヤレス、光ファイバ、ネットワーク)のアイコンと異なる色の意味が表示されます。

18.2 トポロジーパラメーターの設定

表示レベルおよび帯域幅アラームしきい値を含むトポロジー・ディスプレイのパラメーターを設定できます。

Topologyモジュールを入力し、左下隅をクリックして、関連パラメーターを以下のよう

に設定します。🔍

表示レベルの設定

複雑なトポロジーに結合されたデバイスが多すぎる場合は、メイン構造をより明確に表示するように表示レベルを設定できます。類型設定を変更した後、最新のトポロジーを表示するためにクリックする必要があります。デバイスノードが隠れている場合は、クリックして隠れているデバイスノードを展開できます。🔍➡

上流側帯域幅L1/L2アラーム設定

上り帯域幅のL1アラーム、L2アラームを設定できます。行が黄色(ビジー)/赤色に変わります。

帯域幅がL1/L2アラームのしきい値を超える場合(輻輳)。

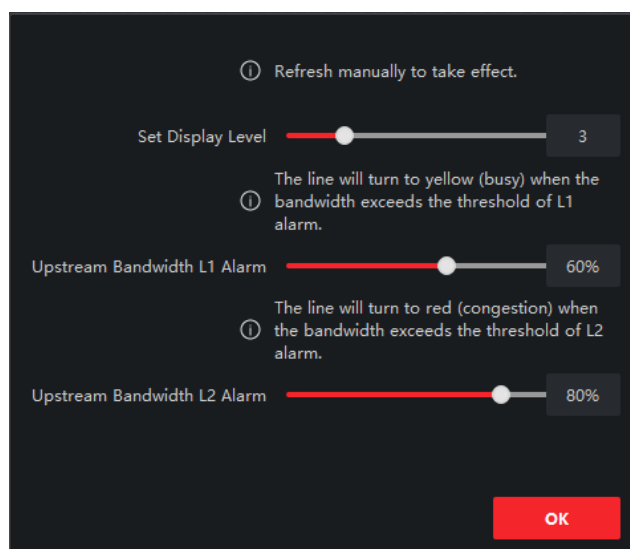


図 18-2 トポロジーパラメーターの設定

18.3 デバイスの詳細の表示

基本情報、デバイスの使用状況、デバイス・パネルのステータス、およびポート情報など、デバイスの詳細をトポロジーで表示できます。

[Topology]ページで、デバイスノードをダブルクリックすると、以下のようにデバイスの詳細が表示されます。

基本情報

基本情報は、デバイスのタイプ、モデル、およびIPアドレスを示します。

デバイス・パネル・ステータス

デバイス・パネル・ステータスは、サポートされているポート・タイプとポートの使用状況を示します。

港湾情報

ポート情報は、デバイスのポートとピアデバイス情報を表示します。

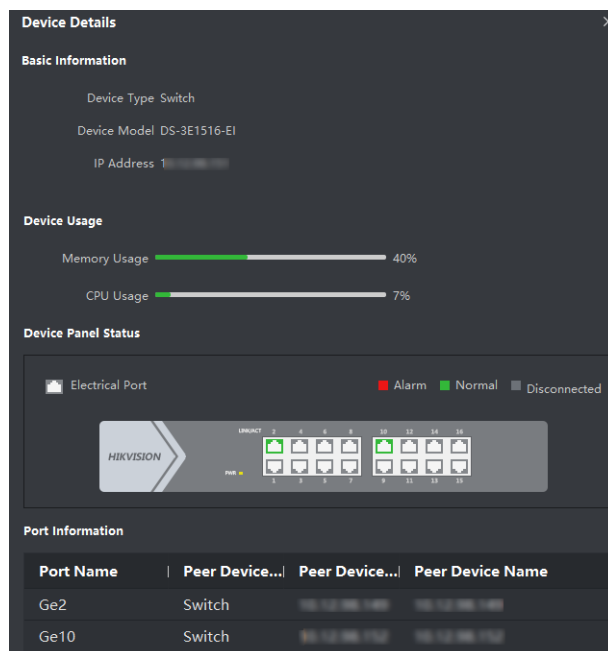


図18-3 装置の詳細

18.4 リンクの詳細の表示

送信レート、デバイスタイプ、ポートステータス、IPアドレス、各デバイスのポート名など、2つのデバイスノード間のリンクの詳細を表示できます。

[Topology]ページで、2つのデバイスノード間の行をダブルクリックすると、リンクの詳細が以下のように表示されます。

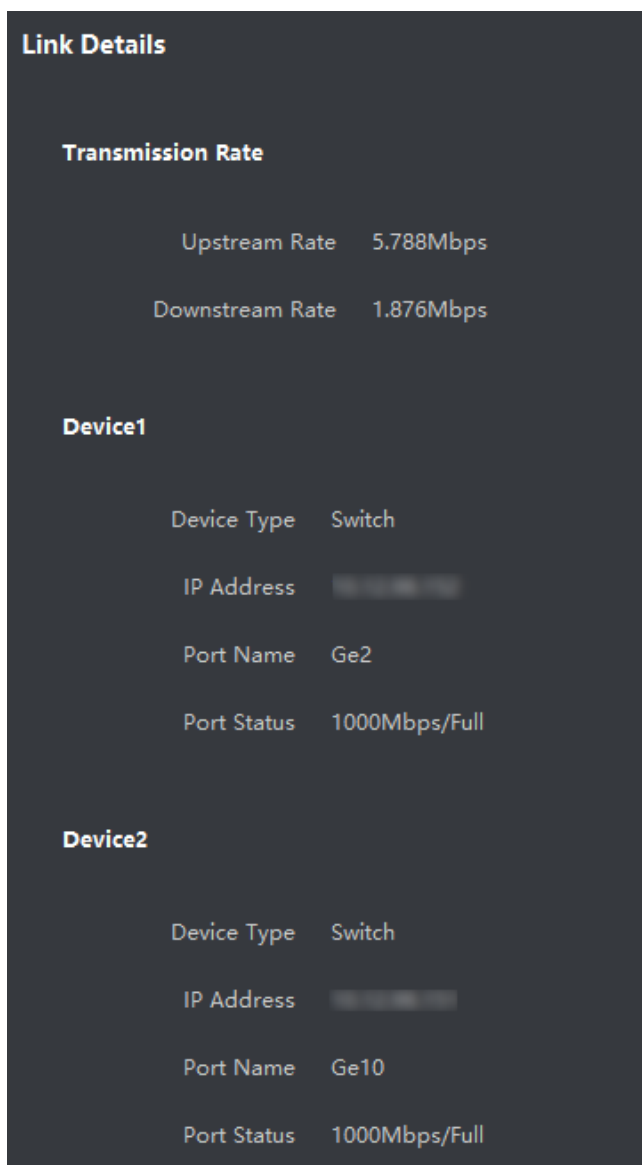



図18-4 リンクの詳細

18.5 信号伝送経路の表示

ネットワークカメラとスイッチ間のデータ伝送が異常な場合、信号伝送経路を確認し、異常なリンクを見つけてリンクメンテナンスを行うことができます。

[Topology]ページで、右上隅をクリックし、ネットワークカメラとNVR/伝送デバイスを選択して、2つのデバイス間の信号伝送(リンクとデバイスを含む)のフラッシュを表示します。 

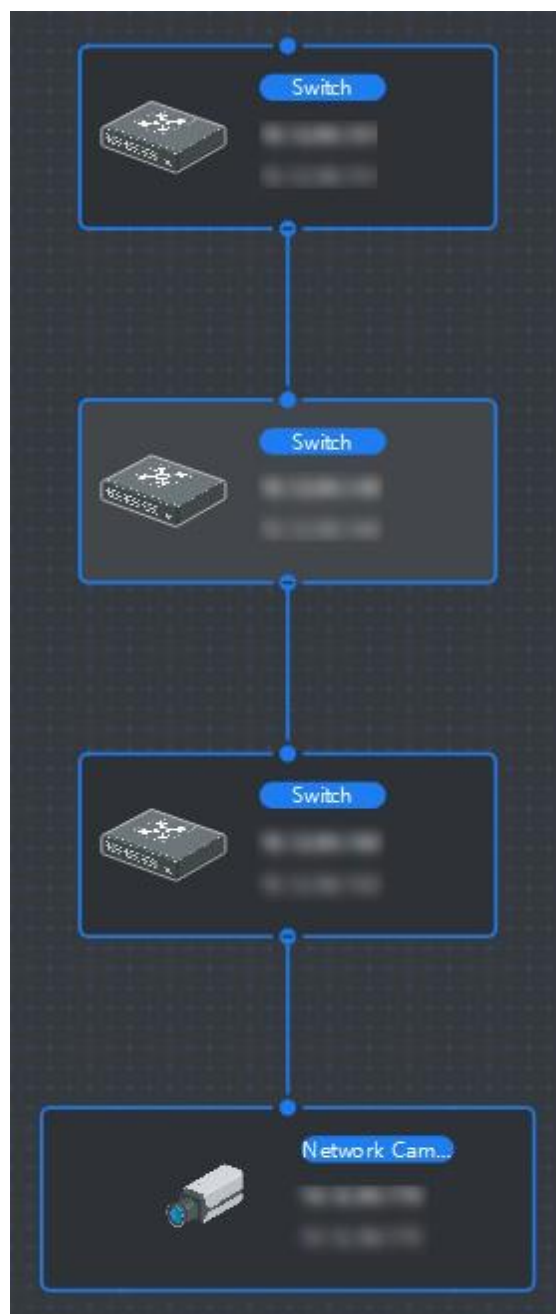


図 18-5 信号伝送経路の表

18.6 トポロジーのエクスポート

トポロジー・ビューをPDFファイルとしてエクスポートして、デバイスの接続状態、レベル、タイプ、IPアドレス、およびその他の情報を表示することができます。

[Topology]ページで、[Path]をクリックし、[Topology]をエクスポートするパスを選択します。📄

18.7 より多くの機能

Topologyモジュールでは、イベントの処理、デバイスステータスの表示、リモート設定などの機能がサポートされています。



注記

表示される機能は機器によって異なる場合があります。

トポロジーでデバイスノートを右クリックし、以下の操作のいずれかを実行します。

イベント処理

デバイスのイベントが検出されると、デバイスノードに赤色のアラームアイコンが表示されます。イベント処理ページを入力すると、イベント情報(イベントソース、イベント時間、イベントの詳細など)を表示できます。

リストから1つまたは複数のイベントを選択し、イベントのクリアをクリックして選択したイベントを削除します。すべてのイベントをクリアすると、デバイスノードの赤色のアラームアイコンは消えます。



注記

この機能は、スイッチ、ワイヤレスネットワークブリッジ、およびファイバコンバータでサポートされています。

リモート設定

リモートコンフィグレーション機能は、システムパラメータ、ネットワークパラメータ、ポートコンフィグレーション、リンクアグリゲーションなど、関連するデバイスパラメータを設定するための簡単なエントリを提供します。

名前の編集

デバイス名を任意に編集できます。

ルートに設定

トポロジー構造と接続を調整するために、デバイスをルートノードとして設定できます。そのあと設定するとトポロジーが自動的に更新されます。



注記

この機能は、スイッチ、ワイヤレスネットワークブリッジ、ファイバコンバータ、および仮想スイッチでサポートされています。

第 19 章 ログ検索

操作ログとシステムログの2種類があります。操作ログは、デバイスの追加、パスワードのリセット、ライブビューの起動など、ユーザがクライアントで行った通常の操作を指し、システムログは、ログイン、ログアウト、ロック、ロック解除など、システム情報を記録します。ログファイルを検索し、時間、ユーザーなどのログの詳細を表示できます。

ステップ

1. Log Searchモジュールを入力します。
2. クリックして開始時刻と終了時刻を指定します。■

注記

ログは1ヶ月以内に検索できます。

3. このユーザーがクライアントで操作するとき生成されるログ・ファイルを検索するには、ユーザーを選択します。
4. ログの種類として[オペレーションログ]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一覧に表示されます。確認できます
ログの動作時間、タイプおよびその他の情報。
6. オプション:ログファイルが多すぎる場合は、以下の操作を実行します。

ファイラー	各テーブルヘッダーをクリックし、ログをフィルタリングするために選択します。■
ソート	テーブルヘッダーをクリックして、時間または文字シーケンスでログを並べ替えます。

第 20 章 ユーザ管理

システムセキュリティを改善するために、管理者は、異なるユーザに対して異なるアカウントを作成し、ユーザに異なる許可を割り当てる必要があります。同じユーザアカウントを共有する人が異なることを避けるために、ユーザアカウントを定期的に管理することをお勧めします。

21.1 ユーザの追加

スーパーユーザと管理者は、新しいユーザを追加し、異なる許可を割り当てることができます。

必要に応じてユーザー

このタスクを実行して、ユーザー・アカウントを追加します。

ステップ



注記

ソフトウェアにログインするために登録したユーザアカウントがスーパーユーザとして設定されます。

1. User Managementモジュールを入力します。
2. 「ユーザの追加」をクリックして、ユーザ情報領域を表示します。
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

アドミニストレーター・アカウントは、デフォルトではすべての許可を持っており、すべてのオペレーターとそれ自身のパスワードと許可を変更することができます。

操作者

オペレータアカウントはデフォルトでは許可を持たず、許可を手動で割り当てることができます。オペレータは、自身のアカウントと、それによって追加されたアカウントのパスワードのみを変更できます。

4. 必要に応じて、ユーザー名、パスワード、および確認パスワードを入力します。デバイスのパスワード強度を自動的にチェックすることができます。あなたの製品の安

**注意**

全性を高めるために、あなたが選択したパスワードを変更することを強くお勧めします (大文字、小文字、数字、特殊文字の3種類以上を含む最低8文字を使用してください)。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、パスワードを毎月または毎週変更することで、製品をより良く保護することができます。

すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストーラーおよび/またはエンドユーザーの責任です。

5. チェックボックスをオンにして、作成したユーザーに許可を割り当てます。
6. オプション: このユーザーのデフォルトの許可を復元するには、Default Valueをクリックします。
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、[アカウント管理]ページのユーザーリストにユーザーアカウントが追加されます。

8. オプション: ユーザー・アカウントの作成後に、以下の操作を実行します。

ユーザーの編集 ユーザー情報を編集するには、リストからユーザーをクリックします。

**注記**

スーパーユーザーのパスワードのみ編集できます。

ユーザーの削除 リストからユーザーを選択し、ユーザーの削除をクリックします。

**注記**

スーパーユーザーは削除できません。

21.2 ユーザーのパスワードの変更

管理者は、旧パスワードを入力することなく、通常のユーザのパスワードを変更することができます。一方、管理者は、自身のパスワードを変更するときには、旧パスワードを入力する必要があります。

開始前に

ユーザをソフトウェアクライアントに追加します。

ステップ

1. User Managementモジュールを入力します。
2. パスワードを変更する必要があるユーザーを選択し、「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. 新しいパスワードを入力し、パスワードを確認します。
5. OKをクリックします。

第 21 章 システム構成

21.1 一般パラメータの設定

ログ期限切れ時間、ネットワークパフォーマンスなど、頻繁に使用されるパラメータを設定できます。

ステップ

1. System Configurationモジュールを入力します。
2. 「全般」タブをクリックして、「全般設定」ページを入力します。
3. 一般パラメータを設定します。

日付フォーマット/時刻フォーマット

関連するページの日付と時刻の表示スタイル。

ログ有効期限

ログ・ファイルを保管する時間。超えたファイルは削除されます。

最大モード

最大モードとしてMaximizeまたはFull Screenを選択します。最大化モードは、ディスプレイを最大化し、タスクバーを表示できます。フルスクリーンモードでは、クライアントをフルスクリーンモードで表示することができます。

ネットワークパフォーマンス

ネットワーク条件を「標準」、「より良い」、「最良」に設定します。

キーボードとジョイスティックを有効にする

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、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

詳細は、Set Keyboard および Joystick Shortcuts を参照してください。

新しいソフトウェアバージョンの検出

有効にした後、クライアントは自動的に新しいソフトウェアバージョンを検出し、ソフトウェアをアップグレードするようにユーザーに注意を促すことができます。

自動時刻同期

追加されたデバイスの時刻を、指定された時点でクライアントが動作しているPCの時刻と自動的に同期させます。

自動アップグレード・デバイス

デバイスの新バージョン検出後のアップグレードモードを設定します。

無効

有効にした後は、クライアントが新しいバージョンのクライアントを検出しても、クライアントはファームウェアパッケージをダウンロードせず、アップグレードしません。

ダウンロードおよびアップグレードの場合、迅速にお知らせください。

クライアントが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ダウンロードしてアップグレードするかどうかをユーザーに確認するプロンプトが表示されます。

アップグレードの場合は、ダウンロードと迅速なMe

クライアントがデバイスの新しいバージョンを検出すると、ファームウェアがダウンロードされます。

パッケージを自動的に作成し、ユーザーにアップグレードするかどうかを確認します。

自動的にダウンロードおよびプロンプト

クライアントがデバイスの新しいバージョンを検出すると、ファームウェアがダウンロードされます。

新しいバージョンのパッケージとアップグレードを自動的に行います。

[Upgrade Time]フィールドにスケジュールを設定し、その間にクライアントが新しいバージョンを自動的にアップグレードする必要があります。

クラウドP2P領域

クラウドP2Pのサーバーのリージョンを選択し、所属するリージョンまたは周辺の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。

21.2 ライブビューおよび再生パラメータの設定

ライブビューや再生のパラメータ(画像フォーマット、プリプレイ時間など)を設定し、等

ステップ

1. System Configurationモジュールを入力します。
2. 「ライブビューと再生」タブをクリックします。
3. ライブビューおよび再生パラメータを設定します。

ピクチャーフォーマット

画像を保存する画像フォーマットとして、JPEGまたはBMPを選択します。



注記

撮影画像の表示温度スイッチを「ON」に設定している場合は、お買い上げ時はJPEGに設定されていますので、変更することはできません。

ビデオフォーマット

録画した動画のフォーマットとしてMP4/AVIを選択します。

ダウンロードしたビデオファイルのマージ

ビデオファイルを日付単位でダウンロードするときの、マージしたビデオファイルの最大サイズを設定します。

保存されている動画ファイルの検索

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。

プレプレー

イベント再生のプリプレイ時間を設定します。デフォルトでは30台です。

ストレージサーバー上のビデオファイルの再生を優先させる

ストレージサーバーに記録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、ローカル機器で録画した動画ファイルを再生してください。

再起動後の最新のライブビュー状態の再開

クライアントに再度ログインした後、最新のライブビューのステータスを再開します。

シングルライブビューでの背景ビデオの切り離し

マルチウィンドウ分割モードでは、ライブビデオをダブルクリックして1ウィンドウ分割モードで表示し、他のライブビデオを停止してリソースを保存します。

Wheel for Zoomを有効にする

マウスホイールを使用して、PTZモードでビデオをズームインまたはズームアウトしたり、デジタルズームモードでビデオをズームインまたは復元したりできます。この方法では、マウスをスクロールすることで、ライブビデオを直接ズームインまたはズームアウト(またはリストア)できます。

VCA再生中に無関係なビデオをスキップする

VCA再生中に未処理ビデオをスキップすると、VCA再生中は未処理ビデオは再生されません。

4. 保存をクリックします。

21.3 画像パラメータの設定

クライアントの画像パラメータは、表示スケール、再生性能などを設定することができます。

ステップ

1. [システム設定]ページを開きます。
2. [Image]タブをクリックして、[Image Settings]インタフェースを入力します。
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ビュースケール。全画面表示4:3、16:9、または当初の決議



注記

また、Live View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、Live Viewを参照してください。

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最短遅延、バランス、フルエンシーに設定できます。[カスタム]を選択して、実際の必要に応じてフレームを指定することもできます。

望ましいハードウェア復号化

ライブビューと再生のためにハードウェアでデコードを有効にするように設定します。ハードウェアデコーディングは、ライブビューまたは再生中にHDビデオを再生するときに、より優れたデコーディング性能とCPU使用率を提供することができます。

強調表示を有効にする

検出されたオブジェクトを、ライブビューと再生で緑色の長方形でマークします。

トランザクション情報の表示

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規則

ライブビューにVCAルールを表示します。

高速再生のためのフレーム抽出を有効にする

高速(8倍速以上)で再生する場合は、この機能を無効にすることができます。
再生画像の詳細を見やすくするために。

ディスプレイターゲットのパターン

有効にした後、対象者のモーショントラックを表示ウインドウで表示
できます。デバイスはこの機能をサポートする必要があります。

撮影した画像のオーバーレイルール

熱機器の場合は、温度情報と火源を表示するように設定してください。
撮影した画像の情報



注記

この機能を有効にすると、「システム設定」→「ライブビューと再生」の
「ピクチャーフォーマット」がJPEGに変わり、編集できなくなります。

4. 保存をクリックします。

21.4 ピクチャーストレージ設定

iVMS-4200サービスを実行しているパソコンでは、デバイス上のイベントによって撮影された画像を保存できます。ここで手動で画像の保存場所を設定します。

ステップ

1. System Configurationモジュールを入力します。
2. イベント・ピクチャー・ストレージをクリックします。
3. 「Server」スイッチの「Store Pictures」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. ディスクを選択して、画像を保存します。



注記



デフォルトの保存パスは次のとおりです。Disk/iVMS-4200alarmPicture

5. 保存をクリックします。

21.5 設定したアラーム音

イベントがトリガーされると、クライアントは警備員に通知する音声警告を発することができます。このセクションでは、警告音の音を設定できます。

ステップ

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、「アラーム音の設定」ページに進みます。
3. オプション:さまざまなイベントのローカルパスからオーディオファイルをクリックして選択します。■
4. オプション:カスタマイズしたアラーム音を追加します。
 - 1) 「追加」をクリックして、カスタマイズしたアラーム音を追加します。
 - 2) [種類]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名をカスタマイズします。
 - 3) 異なるアラームのローカルパスからオーディオファイルをクリックして選択します。■
5. オプション:クリック  オーディオファイルのテスト用
6. オプション:クリック  「操作」欄にカスタム音を削除します。
7. 保存をクリックします。

注記

オーディオファイルのフォーマットは WAV のみ可能です。

21.6 アクセス制御およびビデオインターコムのパラメータの設定

実際のニーズに合わせてアクセス制御やビデオインターホンのパラメータを設定することができます。

ステップ

1. [システム設定]ページを開きます。
2. [アクセスコントロールとビデオインターコム]タブをクリックします。
3. 必要な情報を入力する

着信音

屋内局の着信音のローカルパスからオーディオファイルをクリックして選択します。オプションで、オーディオファイルのテストをクリックすることができます。■



最大着信時間

リングが長く続く秒数を指定します。最大呼出時間は、15秒から60秒まで設定できます。

最大室内局との話し時間

室内局との通話時間が長くなるまでの秒数を設定します。屋内局とクライアント間の最大通話時間は、120秒から600秒まで設定できます。

最大ドアステーションで話す時間

ドアステーションとの通話が長時間継続する秒数を指定します。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秒から120秒まで設定できます。

最大アクセス制御装置を使用した通話時間の設定

アクセス制御装置を装備した呼び出しが最大でも継続する秒数を指定します。アクセス制御装置とクライアント間の最大通話時間は、90～120秒の間で設定することができます。

4. 保存をクリックします。

21.7 ファイル保存パスの設定

ビデオ素材(ライブビュー中に手動で記録され、再生中に切り取られます)と撮影した画像はローカル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。

ステップ

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、[ファイル保存パス設定]ページを入力します。
3. ファイルのローカルパスをクリックして選択します。■
4. 保存をクリックします。

21.8 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インドウのアイコンとツールバーの順番をカスタマイズできます。どのアイコンを表示するか、アイコンの順序を設定します。

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、以下のタスクを実行します。

ステップ

1. System Configurationモジュールを入力します。
2. 「ツールバー」タブをクリックして、「ツールバーの設定」ページを入力します。
3. [画面ツールバー表示の有効化] スイッチを [ON] にして、ライブビューおよび再生ウインドウにツールバーを表示できます。
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ときのアイコンの順序を設定します。

表22-1 ライブビューツールバーのアイコン















	ライブビューの停止	ディスプレイウィンドウのライブビューを停止します。
	キャプチャ	ライブビュー処理で撮影します。撮影した画像はパソコンに保存されます。
	記録	手動記録を開始します。ビデオファイルはパソコンに保存されます。
	PTZ制御	スピードドームのPTZモードを起動します。ビューをクリックアンドドラッグして、PTZコントロールを実行します。
	双方向オーディオ	ライブビューのデバイスで双方向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。再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	カメラのリモート設定ページをライブビューで開きます。

表22-2 再生ツールバーのアイコン

	キャプチャ	ライブビュー処理で撮影します。撮影した画像はパソコンに保存されます。
	記録	手動記録を開始します。ビデオファイルはパソコンに保存されます。
	デジタルズーム	デジタルズーム機能を有効にします。再度クリックすると機能が無効になります。
	ダウンロード	カメラとビデオのビデオファイルをダウンロードするパソコンに保存されます。
	VCA再生	VCAルールを設定します。詳細については、VCA再生を参照してください。
	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、重要なビデオポイントにマークを付けます。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

21.9 キーボードショートカットとジョイスティックショートカットの設定

キーボードはクライアントに接続することができ、PTZカメラを制御するために使用することができます。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、一般的に使用されるアクションへの簡単で簡単なアクセスを得ることができます。

このタスクは、キーボードおよびジョイスティック・ショートカットを設定する必要がある場合に実行します。

ステップ



注記

この設定ページは、General Settingsでキーボードとジョイスティックを有効にした後に表示されます。詳細は、「一般パラメータの設定」を参照してください。

1. System Configurationモジュールを入力します。
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. クライアントと一緒にインストールされたPCにキーボードが接続されている場合は、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を入力して、キーボードが接続されているCOMポートを確認することができます。

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) [Function]列で特定の機能名を選択します。
 - 2) PC Keyboard、USB Joystick、またはUSB Keyboardの下にある項目フィールドをダブルクリックします。
 - 3) 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するには、ドロップダウンリストから複合キーの操作または番号を選択します。
5. 保存をクリックします。

例

フォーカス(+)機能では、PCキーボード、USBジョイスティック、USBキーボードのショートカットにHome、1、F1を設定すると、PCキーボードのHomeキーを押したり、ジョイ

スティックを1方向に制御したり、USBキーボードのF1キーを押すとズームインできません。

21.10 電子メールパラメータの設定

イベントがトリガーされたときに、このイベントのリンクアクションとして「電子メールの送信」を設定できる場合、クライアントは通知の受信者に電子メールを送信します。このセクションでは、Eメールの設定と宛先を指定する必要があります。

ステップ

1. System Configurationモジュールを入力します。
2. [Email]タブをクリックして、[Email Settings]インタフェースを入力します。
3. 必要な情報を入力します。

SMTPサーバ

ホスト名のSMTPサーバIPアドレス(例えば、smtp.263xmail.com)

暗号化タイプ

ラジオを確認して、Non-Encrypted、SSL、STARTTLS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。ポートはデフォルトで25です。

送信元アドレス

送信者の電子メールアドレス。

セキュリティ証明書(オプション)

電子メール・サーバーが認証を必要とする場合、このチェック・ボックスをチェックして、認証を使用してサーバーにログインし、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

[サーバ認証]をチェックする場合は、送信元メールアドレスのユーザー名を入力します。

パスワード

[サーバ認証]をチェックしている場合は、送信元のEメールアドレスのパスワードを入力します。

受信機1~3

宛先のメールアドレスを入力します。受信機は3台まで設定できます。

4. オプション:[Test Emailの送信]をクリックして、テストのために受信者にEmailを送信します。
5. 保存をクリックします。

21.11 セキュリティ認証の管理

データセキュリティの目的のためには、クライアントと追加されたサーバ(ストリームメディアサーバ)のセキュリティ証明書は同じである必要があります。TLS (Transport Layer Security)プロトコルを使用して送信暗号化を有効にするときに、検証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、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を使用する場合、クライアントとサーバ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。

21.11.1 サービス管理からのエクスポート証明書

現在のクライアント・サービスからセキュリティー証明書をエクスポートし、エクスポートしたセキュリティー証明書をインポートできます。

ストリーム・メディア・サーバーまたは他のクライアントへの証明書ファイル

ステップ

1. コール管理を入力します。
2. 「エクスポート」をクリックして、証明書ファイルをローカルPCに保存します。



証明書ファイルはXML形式です。

次にすべきこと

証明書をエクスポートした後、証明書をクライアントとともにインストールされたPCにコピーし、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することができます。

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、「証明書のストリーム・メディア・サーバーへのインポート」を参照してください。

21.11.2 顧客への輸入証明書

同じ蒸気メディア・サーバーにアクセスする複数のクライアントがある場合、同じクライアントをインポートする必要があります。

クライアントとサーバーへの証明書

開始前に

クライアント・サービスの1つからセキュリティー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」を参照してください。

ステップ

1. 他のクライアントからローカルPCにエクスポートされた証明書ファイルをコピーします。
2. System Configurationモジュールを入力します。
3. [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に入ります。
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、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てください。

21.11.3 伝送暗号化のための証明書検証

[Security Authentication]ページで、送信暗号化にデバイス証明書の検証が必要かどうかを設定できます。

[システム設定]→[セキュリティ認証]をクリックして、セキュリティ認証を入力します。

インターフェースVerify Certificate as YesまたはNo.

はい

デバイスの追加時に送信暗号化を有効にする場合は、デバイス証明書を設計ディレクトリに配置する必要があります。また、機器は伝送暗号化と共に追加され、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送信暗号化を有効にする場合は、デバイス証明書は必要ありません。そして、このデバイスは、伝送暗号化によって追加されます。

第 22 章 操作と保守

メニューのメンテナンス操作を行うことで、クライアントをスムーズかつ便利にご利用いただけます。

右上隅をクリックし、File/System/Toolをクリックして以下を実行します。
事業

ログファイルを開く

ローカルPCに保存された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。

構成ファイルのインポート/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することができます。その逆も可能です。

自動バックアップ

データベース内の構成ファイルおよびデータをバックアップするか、バックアップしたデータをリストアする日時を選択します。

皮膚

ブライトカラーシリーズ、ブラックカラーシリーズなど、お客様の肌を変える。

バッチ時間同期

選択したデバイスの時刻とPCの時刻を同期させます。

メッセージキュー

Eメールリンク設定後、起動されたイベントが表示されます。イベントを選択し、受信側へのメール送信をキャンセルします。

付録 A. カスタム Wiegand ルールの説明

Wiegand 44を例にとると、Custom Wiegand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	ウィーガンド44				
全長	44				
変換規則(10進数)	byFormatRule[4]=[1][4][0][0]				
パリティモード	XORパリティ				
奇パリティ開始ビット		長さ			
偶数パリティ開始ビット		長さ			
XORパリティ開始ビット	0	グループごとの長さ	4	全長	40
カードID開始ビット	0	長さ	32	10進数字	10
サイトコード開始ビット		長さ		10進数字	
OEMスタートビット		長さ		10進数字	
メーカーコードスタートビット	32	長さ	8	10進数字	3

Wiegandデータ

Wiegandデータ=有効データ+パリティデータ

全長

Wiegandデータ長。

運送規則

4バイトです。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と製造者コードの組み合わせが表示されます。有効なデータは、単一のルール、または複数のルールの組み合わせが可能です。

パリティモード

Wiegand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のいずれかを選択できます。

奇数パリティ開始ビットと長さ

奇数パリティを選択すると、これらの項目を使用できます。奇数パリティ開始ビットが1で、長さが12の場合、システムはビット1から奇数パリティ計算を開始します。

12ビットを計算する。結果はビット0(ビット0が最初のビット)となる。

偶数パリティ開始ビット、および長さ

「偶数パリティ」を選択すると、これらの項目を使用できます。偶数パリティ開始ビットが12で、長さが12である場合、システムは、ビット12から偶数パリティ計算を開始する。12ビットを計算する。結果は最後のビットになります。

XORパリティ開始ビット、グループ当たりの長さ、および合計長

XOR Parityを選択すると、これらのアイテムが使用可能になります。上の表に応じて、開始ビットは0、グループごとの長さは4、合計の長さは40です。これは、システムがビット0から計算し、4ビット毎に計算し、合計40ビット(合計10グループ)を計算することを意味する。結果は最後の4ビットになります。(結果の長さは、グループごとの長さと同じです)。

カードID開始ビット、長さ、10進数

変換ルールを使用する場合、これらの項目を使用できます。上記の表に応じて、カードIDの開始ビットは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(ここではビット単位で計算)を表し、10進数の長さは10ビットである。

サイトコード開始ビット、長さ、10進数

変換ルールを使用する場合、これらの項目を使用できます。詳細については、以下を参照してください。

カードIDの説明

OEM開始ビット、長さ、10進数

変換ルールを使用する場合、これらの項目を使用できます。詳細については、以下を参照してください。

カードIDの説明

メーカーコード開始ビット、長さ、10進数

変換ルールを使用する場合、これらの項目を使用できます。上記の表に応じて、メーカーコード開始ビットは32、長さは8、小数点は3となります。ビット32から、8ビットが製造者コードであることを表す。(ここでの長さはビット単位で計算されます)および10進数の長さは3です。

付録 B.トラブルシューティング

クライアントソフトウェアを操作するときによくみられる症状を次に示します。私たちは、問題解決のために、考えられる原因とその解決策を提供します。

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。

考えられる理由

- 不安定なネットワークやネットワークの性能が不十分である。
- 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と、デバイスの負荷が高すぎます。
- 現在のユーザーはライブビューを許可されていません。
- 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を下回っている。

ソリューション

- 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。
- 管理ユーザーでログインし、再試行してください。
- 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が混同されます。

問題

ローカル録画とリモート録画が混同されます。

ソリューション

- 本書におけるローカル録画とは、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をいいます。
- リモート録画とは、リモートデバイス側のクライアントが指令する録画アクションを指します。

B.3ビデオファイルのダウンロードに失敗した、またはダウンロード速度が遅すぎる。

問題

ビデオファイルのダウンロードに失敗した、またはダウンロード速度が遅すぎる。

考えられる理由

- 不安定なネットワークやネットワークの性能が不十分である。
- NICタイプが互換性がありません。
- リモートデバイスへのアクセス数が多すぎる。
- 現在のユーザーは再生を許可されていません。
- クライアントソフトウェアのバージョンが必須バージョンを下回っている。

ソリューション

- 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。
- NICカードの互換性を確認するために、クライアントを実行しているPCを直接デバイスに接続します。
- 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。
- 管理ユーザーでログインし、再試行してください。
- 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。

付録 C. FAQ (よくある質問)

ここでは、クライアントソフトウェアを操作する際によく使う質問をいくつか示します。対応する回答を提供し、ユーザーの問題解決に役立てています。

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では、チャンネルはサブストリームをサポートしない場合があります。「システム設定」→「画像」で「自動変更ストリームタイプ」の機能を無効にし、ライブビューに適した蒸気タイプを選択する必要があります。

C.2 ライブビュー中に、画像がぼやけているのか、それとも滑らかでないのか。

質問

ライブビュー中に、画像がぼやけているのか、それとも滑らかでないのか。

回答

ビデオカードのドライバを確認する。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 メモリーが漏れ、しばらく走った後にクライアントがクラッシュしたのはなぜですか？

質問

しばらくの間、メモリーリークとクライアントがクラッシュしたのはなぜですか？

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Notepadで開き、EnableNetandJoystickCheckの値をfalseに変更します。クライアントを再起動し、問題がまだ解決されていない場合は、弊社のテクニクサポートに連絡してください。

C.4 ライブビュー中、ストリーム・メディア・サーバーを介してストリームを取得する場合、エラー・コード17を含むエラー・メッセージがプロンプトを出す理由は何ですか？

質問

ライブビュー中、ストリーム・メディア・サーバーを介してストリームを取得する場合、エラー・コード17を含むエラー・メッセージがプロンプトを出す理由は何ですか？

回答

Stream Media Server のポートマッピング、特にRTSP ポートを確認します。

C.5 ネットワーク帯域幅が小さい場合、ライブビューや再生のパフォーマンスを向上させるにはどうすればよいのでしょうか？

質問

ネットワークの帯域幅が小さい場合、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すればよいのでしょうか？

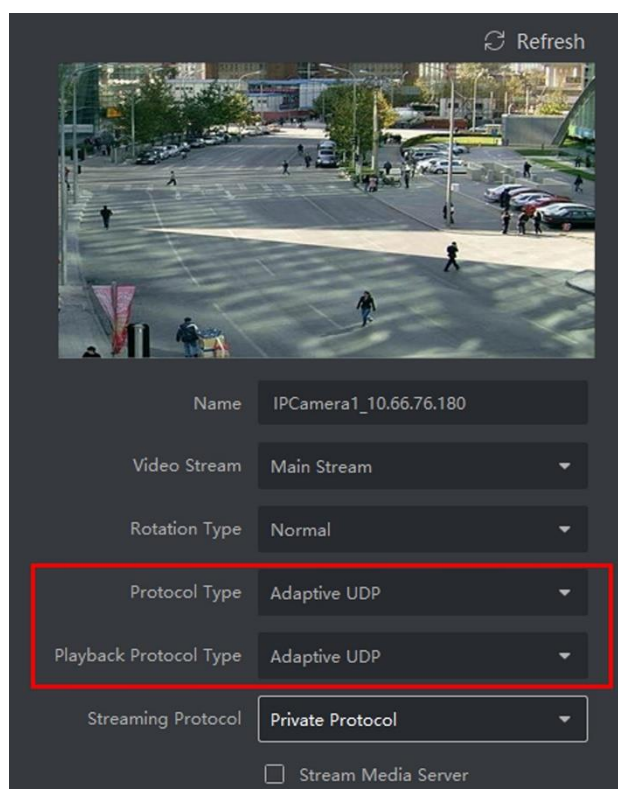
回答

この機能は、装置がサポートする必要があります。低帯域幅でライブビューを実現するには、以下の操作を実行します。

注記

あらかじめ、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。

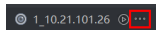
- まず、エンコーディングデバイスをクライアントに追加した後、カメラのストリーミングプロトコルを設定する必要があります。
 - 「デバイス管理」→「グループ」と入力します。
 - 「エンコーディングチャンネル」リストでカメラを選択し、クリックします。☑
 - [Edit Camera] ウィンドウで、[Protocol Type](ライブビュー用)と[Playback Protocol Type]を設定します。
(再生用)アダプティブ UDP



図C-1セットプロトコルタイプ

- 設定を保存するには、OKをクリックします。
- ライブビューのストリームタイプを選択します。
 - Main View モジュールを入力します。

2. 左側のデバイスリストで、カーソルをカメラ名に移動し、「ストリーム」をクリックします。...



図C-2 ストリームタイプの選択

3. ネットワークカメラの場合は、ストリームの種類をThird Streamに設定します。DVRまたはNVRの場合は、ストリームの種類を仮想ストリームに設定します。
4. ライブビューを開始します。

付録 D.エラーコード

コード	エラー名称	説明
iVMS-4200		
317	ビデオはありません。	再生が許可されていないときにプロンプトが表示されます。
HCNetSDK.dll 		
1	無効なユーザー名またはパスワード。	
2	許可なし。	デバイス内のユーザーは、十分な許可を持っていません。
4	不正なチャンネル番号。	リモート画面コントロールのライブビューに表示されません。
5	これ以上デバイスを接続できない。	
7	デバイスの接続に失敗しました。	
23	サポートしていません。	
29	動作失敗	
43	バッファなし。	デバイスを追加すると、Webサーバがデバイスポートを占有しているかどうかを確認されます。
55	IPアドレスが不正。	
56	MACアドレスが不正。	
91	チャンネルがサポートしていない手術	サブストリームの取得に失敗した場合にプロンプトが出されます。
96	デバイスはDDNSに登録されていません。	
153	ユーザーがロックされる。	
250	デバイスがアクティブになっていない。	

404	チャンネル番号エラーまたは装置がサブストリームをサポートしない。	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プロンプトが出される。
424	RTSP SETUPの受信に失敗しました。	ライブビューを追加するとプロンプトが表示されます。 外部ネットワーク経由のソフトウェアDVS
800	それ以上の帯域幅は使用できません。	
プレイクトル・ドリル		
2		ストリームはビデオおよび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・サーバー間の接続問題。
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問題。