

DMSS アプリ ユーザーマニュアル



序文

一般事項

本マニュアルでは、DMSSアプリ(以下「DMSS」と記載)の機能および操作方法について説明します。

安全に関する注意事項

本マニュアルには、以下のような**注意喚起語(シグナルワード)**が使用されている場合があります。

シグナルワード	意味
 DANGER	回避しないと 死亡または重傷 を招く可能性が非常に高い危険を示します。
 WARNING	回避しないと 軽傷または中程度の怪我 につながる可能性のある中～低程度の危険を示します。
 TIPS	問題を解決したり、時間を節約したりするのに役立つ方法を提供します。
 NOTE	本文の補足として、追加情報を提供します。

改訂履歴

バージョン	改定内容	リリース時期
V2.0.0以降	アプリのUIデザインを更新	2025年7月

プライバシー保護に関する注意事項

デバイスの使用者またはデータ管理者として、他人の顔、指紋、ナンバープレート番号などの個人データを収集する場合があります。

その際には、**地域のプライバシー保護に関する法律や規制を順守し**、他人の正当な権利と利益を保護する必要があります。

そのために、以下を含むがこれに限定されない措置を講じる必要があります。

- 監視エリアの存在を知らせる明確で見やすい表示を提供すること
- 必要な連絡先情報を明記すること

本マニュアルについて

- 本マニュアルは参考用です。実際の製品と内容に若干の相違がある場合があります。
- マニュアルに従わない操作により生じた損失については、一切の責任を負いかねます。
- 本マニュアルは、関係法令の最新の改正に基づいて更新されることがあります。詳細は、紙のユーザーマニュアル、付属CD-ROM、QRコードの読み取り、または公式ウェブサイトをご参照ください。電子版と紙版において一部異なる内容が存在する場合があります。
- 設計およびソフトウェアは予告なく変更されることがあります。製品のアップデートにより、実物とマニュアルの内容に差異が生じる可能性があります。最新のプログラムおよび補足文書については、カスタマーサービスまでお問い合わせください。
- 機能、操作、技術データに関する記述に誤植や記述の誤りがある可能性があります。不明点や疑義がある場合には、当社が最終的な解釈権を有します。
- 本マニュアル(PDF形式)が開けない場合は、リーダーソフトのアップグレードや他の主流なPDFリーダーの使用をお試しください。
- 本マニュアルに記載されているすべての商標、登録商標、会社名は、それぞれの所有者に帰属します。
- デバイス使用中に問題が発生した場合は、当社の公式サイト、販売元、またはカスタマーサービスにお問い合わせください。
- 内容に不確かな点や争いがある場合には、当社が最終的な解釈権を保有します。

目次

前書き.....	1 (Link)
1 概要.....	1 (Link)
1.1 はじめに	1 (Link)
1.2 対応OS	1 (Link)
2 ログイン	2 (Link)
2.1 新規登録	2 (Link)
2.2 パスワードのリセット	4 (Link)
3 ホーム画面.....	5 (Link)
4 デバイスの追加.....	7 (Link)
4.1 SN/QRコードによる追加	7 (Link)
4.2 IP/ドメイン検索による追加.....	7 (Link)
4.3 LAN 検索による追加	8 (Link)
4.4 手動追加/Bluetooth 検索	9 (Link)
5 基本操作	10 (Link)
5.1 デバイスの設定.....	10 (Link)
5.1.1 アラーム設定.....	11 (Link)
5.1.2 ビデオ再生設定	16 (Link)
5.1.3 一般設定	18 (Link)
5.2 デバイスの共有.....	36 (Link)
5.3 セキュリティサービスの申請	37 (Link)
5.4 デバイスの委託.....	38 (Link)
5.4.1 デバイスの個別委託	38 (Link)
5.4.2 デバイスの一括委託.....	40 (Link)
5.5 デバイスのバインド解除	41 (Link)
5.6 デバイスカードの作成	41 (Link)
5.7 ローカルデバイスのアカウントへの移行	42 (Link)
5.8 デバイスパスワードのリセットと変更	43 (Link)
6 ライブビュー	45 (Link)
7 ビデオ再生	49 (Link)
8 ビデオ通話	51 (Link)
9 アクセスコントロール.....	54 (Link)
10 アラーム操作	56 (Link)
10.1 デバイスサービス.....	57 (Link)
10.2 ファームウェアの更新.....	57 (Link)
10.3 アラームハブ	57 (Link)
10.3.1 デバイスの概要	58 (Link)

10.3.2	ステータスの確認	58	(Link)
10.4	アラームハブの設定	59	(Link)
10.4.1	ハブ設定	60	(Link)
10.4.2	インターコムサービス.....	66	(Link)
10.4.3	ネットワーク構成.....	68	(Link)
10.5	エリア管理.....	70	(Link)
10.6	周辺機器の管理	70	(Link)
10.6.1	周辺機器の概要	72	(Link)
10.6.2	周辺機器の設定	72	(Link)
11	イベント.....	73	(Link)
11.1	アラームメッセージの購読.....	73	(Link)
11.2	メッセージの確認.....	73	(Link)
12	お気に入り.....	75	(Link)
13	マイページ	76	(Link)
付録1	セキュリティに関する推奨事項	80	(Link)

1 概要

1.1 はじめに

DMSSは、リモート監視、ビデオ再生、プッシュ通知、リモート設定、デバイス共有および委任などの機能を備えたモバイル監視アプリです。

IPC、NVR、XVR、VTO、ドアベル、アラームハブ、アクセスコントローラなどのデバイスを追加することができます。

1.2 対応OS

- Android 7.0 以降
- iOS 12.0 以降

2 ログイン

初めて使用する場合は、**アカウントを作成する必要があります**。このユーザーマニュアルでは、iOSでの操作手順を例に説明します。

2.1 アカウント登録

アカウントは、メールアドレスまたは電話番号で登録できます。



※電話番号による登録は、一部の国や地域のみ対応しています。

手順

ステップ1 App Storeで「DMSS」を検索し、アプリをダウンロードします。



Androidユーザーは **Google Play** からDMSSをダウンロードできます。

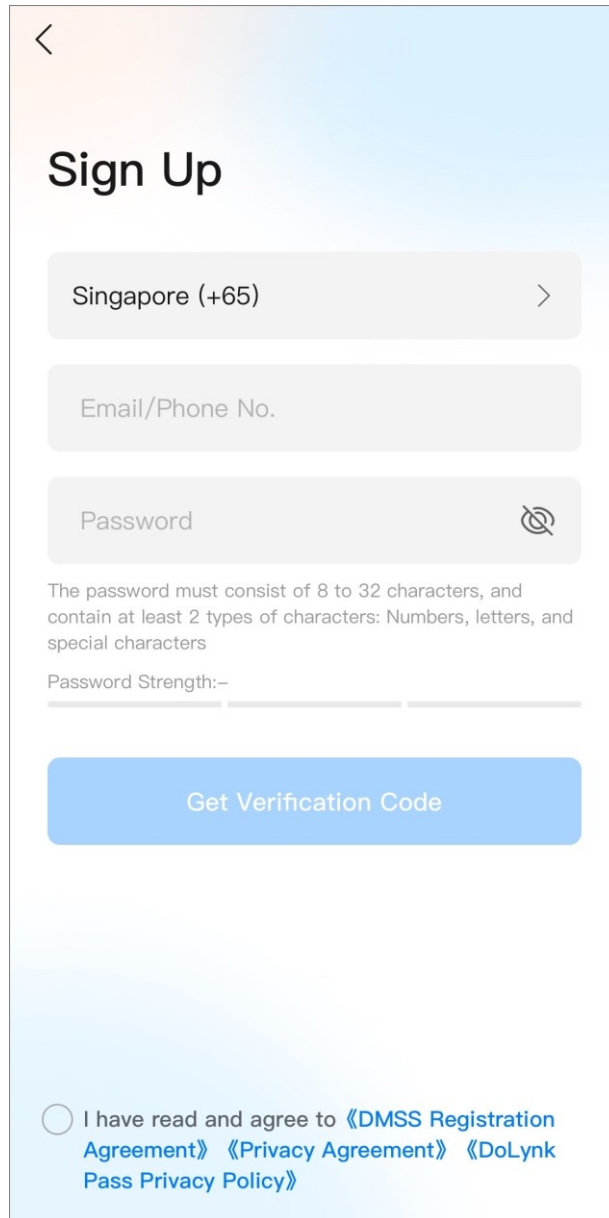
ステップ2 スマートフォンで📱をタップして、アプリを起動します。

図2-1 ログイン画面

ステップ3 アカウントを作成します。

1. ログイン画面で、「サインアップ」をタップします
2. 国または地域を選択します。

図2-2 サインアップ画面

A mobile app sign-up screen with a light blue gradient background. At the top left is a back arrow. The title 'Sign Up' is centered. Below it are three input fields: a country code selector showing 'Singapore (+65)' with a right arrow, an 'Email/Phone No.' field, and a 'Password' field with a toggle icon. Below the password field is a text note: 'The password must consist of 8 to 32 characters, and contain at least 2 types of characters: Numbers, letters, and special characters'. Underneath is a 'Password Strength' progress bar. A large blue button labeled 'Get Verification Code' is centered. At the bottom, there is a radio button followed by the text: 'I have read and agree to 《DMSS Registration Agreement》《Privacy Agreement》《DoLynk Pass Privacy Policy》'.

選択した国または地域によっては、電話番号による登録オプションが表示されます。

3. メールアドレスまたは電話番号とパスワードを入力します。



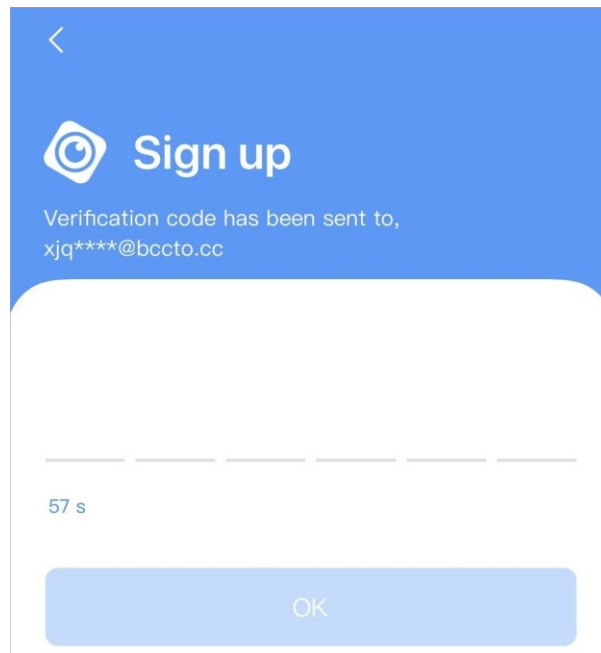
パスワード表示アイコンをタップすると、パスワードの表示／非表示を切り替えられます。

4. 「DMSS登録契約」「プライバシーポリシー」「DoLynk Passプライバシーポリシー」を読み、「読んで同意しました」のチェックボックスにチェックを入れます。
5. 「認証コードを取得」をタップし、メールまたはSMSで送信された認証コードを確認して入力します。



※認証コードは、受信後60秒以内に入力してください。それ以降は無効になります。

図2-3 認証コードの入力



6. 「OK」をタップします。

ステップ4 ログイン画面で、メールアドレスまたは電話番号とパスワードを入力し、「ログイン(Log in)」をタップします。



パスワードは、「マイページ(Me) > アカウント > アカウントセキュリティ > パスワードの変更」から変更することができます。

2.2 パスワードのリセット

ログイン画面では、パスワードのリセットが可能です。

手順

ステップ1 「パスワードをお忘れですか？」をタップします。

ステップ2 「パスワードをお忘れですか？」画面で、登録時に設定したメールアドレスまたは電話番号を入力し、「認証コードを取得」をタップします。

ステップ3 同画面で、メールまたは電話で受け取った認証コードを入力し、「OK」をタップします。



※認証コードは、受信から60秒以内に使用してください。それ以降は無効になります。

ステップ4 新しいパスワードを設定し、「OK」をタップします。

ステップ5 ログイン画面で「ログイン」をタップします。

3 ホーム画面

図3-1 ホーム



表3-1 ホーム画面の説明

No.	名前/アイコン	説明
1		メッセージセンター。 個人メッセージ、エラーメッセージ、システムメッセージを確認できます。
2		デバイスを追加します。 詳細は「4 デバイスの追加」を参照してください。 (Link)

No	名前/アイコン	説明
3		「ライブ映像(Live Video)」をタップすると、ライブビュー画面に移動します。 「ビデオ再生(Video Playback)」をタップすると、再生画面に移動します。 「リスト表示(List View)」または「ギャラリー表示(Gallery View)」をタップして、デバイスリストの表示モードを切り替えることができます。 「マルチウィンドウ(Multi-Window)」をタップすると、すべてのビデオチャンネルを同時に表示できます。このモードでは以下の操作が可能です。 ライブ映像を表示したいチャンネルをタップして選択。 ◇  チャンネルリストの表示モードを切り替え。 ◇  画面を横向き表示(ランドスケープ)に切り替え。
4	...	アイコンをタップすると、以下の項目を選択できます。 デバイス詳細: デバイスの詳細を確認でき、詳細画面からデバイスの設定も可能です。詳細は「5.1 デバイスの設定」を参照してください。(Link) デバイスの委任: 登録済みのインストーラー(設置業者)にデバイスを委託します。詳細は「5.4 デバイスの委任」を参照してください。(Link) トップに移動: デバイスをリストの先頭に移動します。 デバイスの共有: 他のDMSSアカウントにデバイスを共有します。詳細は「5.2 デバイスの共有」を参照してください。(Link)  ※VTOやVTHデバイスは共有できません。 セキュリティサービス(アラームハブの場合): セキュリティ会社とデバイスを紐付け、セキュリティサービスの申請が可能です。  なお、設定できる項目はデバイスの種類によって異なります。詳細は実際のインターフェースをご確認ください。
5		VTOデバイスでは、ドアの解錠が可能です。
6	ナビゲーションバー	「ホーム」「イベント」「私(マイページ)」をタップすると、それぞれのモジュールに移動します。
7	デバイスステータス	デバイスの状態を表示します。 (例: 共有状態、委任状態、借用状態、信号強度、バッテリー残量など)
8	デバイスカテゴリ	- すべて(All): すべてのデバイスのリストを表示します。 - お気に入り(Favorites): ビデオチャンネルごとにお気に入りカテゴリを作成できます。
9	検索ボックス	デバイスのシリアル番号(SN)または名称で検索できます。

4 デバイスの追加

デバイスは、以下のいずれかの方法で追加できます。デバイスのシリアル番号(SN)を手動入力、QRコードをスキャン、デバイスのIPアドレスまたはドメイン名を入力、LAN内で検索。

※デバイスを追加する前に、初期化を行う必要があります。

4.1 SN/QRコードで追加します

デバイスは、QRコードをスキャンするか、シリアル番号(SN)を手動で入力することで追加できます。

手順

ステップ1 デバイス画面で  をタップし、「QRコードをスキャン」を選択します。

ステップ2 デバイスを追加します。

- デバイスのQRコードを直接スキャンするか、 をタップしてQRコード画像をインポートし、デバイスを追加します。
- 「SNを手動で入力」をタップし、デバイスSNを入力して手動でデバイスを追加します。

ステップ3 デバイスタイプを選択します。(例:IPC、NVRなど)

ステップ4 「デバイス追加」画面で「デバイス名(任意の名前)」、「ユーザー名とパスワード」の情報を入力します。

図4-1 SN/QRコードによる追加



4.2 IP/ドメイン検索によるデバイス追加

デバイスのIPアドレスまたは特定のドメイン名(DDNSなど)を直接入力して、DMSSアプリにデバイスを追加する方法です。

手順

ステップ1 デバイス画面で  をタップし、「IP/ドメイン」を選択します。

ステップ2 デバイスタイプ(例:NVR、IPC、PTZなど)を選択します。

ステップ3 必要な情報を入力し、「OK」をタップして追加します。

図4-2 IP/ドメイン検索による追加

図4-2 IP/ドメイン検索による追加のスクリーンショット。左側の「デバイスを追加」画面には、ワイヤレスカメラ、有線カメラ、NVR、DVR/XVR、IVSS、VTO、アクセス制御のアイコンが並んでいる。右側の「デバイスを追加」画面には、追加モード（IP/ドメイン）、住所、ポート（37777）、名前、ユーザー名（admin）、デバイスパスワードの入力欄がある。下部には、アラームはローカルバインディングを通じてバインドされたデバイスには保存できません。DMSSアプリを閉じるたびに、これらのデバイスからのメッセージは失われます。という警告メッセージが表示されている。

4.3 LAN 検索による追加

手順

ローカルネットワーク(LAN)上に接続されているデバイスを検索し、一覧から選択して追加する方法です。

ステップ1 デバイス画面で⁺をタップし、「LANで検索」を選択します。

ステップ2 デバイスの選択画面で、検出された一覧の中から追加したいデバイスを選択します。

ステップ3 デバイスの追加画面で、「デバイス名(任意の名前)」、「ユーザー名とパスワード」の情報を入力します。

図4-3 オンライン検索による追加

図4-3 オンライン検索による追加のスクリーンショット。左側の「デバイスを選択」画面には、デバイスタイプ:IPN-AI5864-H8、デバイスタイプ:IP Camera、デバイスタイプ:IP Camera、デバイスタイプ:IP Cameraのリストが表示されている。右側の「デバイスを追加」画面には、追加モード（P2P）、SN、名前、ユーザー名（admin）、デバイスパスワードの入力欄がある。

4.4 手動で追加/Bluetooth 検索

手順

ステップ1 デバイス画面で  をタップし、「手動追加/Bluetooth検索」を選択します。

ステップ2 システムが Bluetoothを通じて周囲の対応デバイスを自動検索 します。検索結果から対象のデバイスを選び、デバイスタイプを選択します(例:IPC、NVRなど)。

ステップ3 デバイスの追加画面で、「デバイス名(任意の名前)」、「ユーザー名とパスワード」の情報を入力します。

5 基本操作

デバイスの追加後、デバイスの「各種パラメータの設定」、「デバイスの再起動や削除」、「デバイスの共有や委託」、「デバイスカードの作成」、「デバイスのパスワードの設定または変更」など、基本的な操作を実行できます。

インターフェースはデバイスの種類によって異なる場合があります。ここでは、例としてIPC(ネットワークカメラ)を用いて説明します。

5.1 デバイスの設定

手順

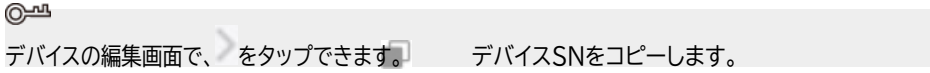
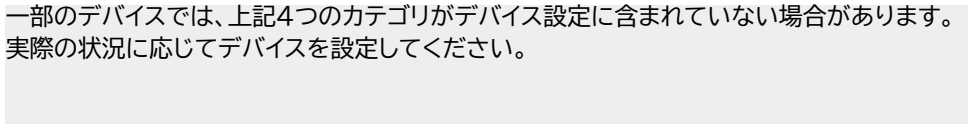
ステップ1 デバイス画面で「...」をタップし、「デバイスの詳細」を選択します。

ステップ2 デバイスの詳細画面で必要に応じて各種パラメーターを設定します。

図5-1 デバイスの詳細



表5-1 デバイスの詳細

番号	説明
1	- デバイスの基本情報を表示します。 - タップすると「デバイス編集」画面に移動します。ここでは、デバイス名とパスワードの変更、リンクされたチャンネルおよびシリアル番号(SN)の確認ができます。デバイスパスワードの変更についての詳細は、「5.8 デバイスパスワードのリセットおよび変更」を参照してください。(Link)  デバイスの編集画面で、 をタップできます。 デバイスSNをコピーします。
2	デバイスメッセージ - 通知:デバイスからのメッセージ受信機能を有効または無効にできます。 - デバイスオフライン通知:デバイスがオフラインになった際の通知を有効または無効にできます。
3	デバイスの設定 デバイスの設定は、アラーム設定、ビデオ再生設定、一般設定、その他の5つのカテゴリに分かれます。  一部のデバイスでは、上記4つのカテゴリがデバイス設定に含まれていない場合があります。実際の状況に応じてデバイスを設定してください。  - アラーム設定の操作の詳細については、「5.1.3.5.2 アラーム設定」を参照してください。(Link) - ビデオ再生設定の操作の詳細については、「5.1.2 ビデオ再生設定」を参照してください。(Link) - 一般設定およびその他の操作の詳細については、「5.1.3 一般設定」を参照してください。(Link)

5.1.1 アラーム設定

アラームメッセージの購読、アラーム連動の無効化、プッシュ通知の設定などが行えます。

5.1.1.1 メッセージ

アラームメッセージを購読することで、アラームが発生した際にDMSSシステム通知を送信できるようになります。

送信する通知の種類を設定できます。複数の通知タイプを同時に選択することも可能です。このセクションでは、IPC(ネットワークカメラ)の設定を例に説明します

手順

ステップ1 デバイス画面で対象のデバイスの横にある「」をタップし、「デバイス詳細」を選択。

ステップ2 「基本設定」項目で「メッセージ」をタップします。

ステップ3 「通知」の横にある  スイッチをタップして機能を有効にします。

メッセージがある場合に通知を送信するかどうかを選択できます。

ステップ4 「アラームメッセージタイプ」をタップし、受信したいアラームメッセージを有効にします。

図5-2 アラームメッセージタイプ



表5-2 プッシュ通知の設定

通知タイプ	説明
動体検知	視野内で対象物が異常に動いた場合にアラームが発生します。
スマートモーション検知 (SMD)	「人による動体検知」または「車両による動体検知」のいずれかを選択できます。
侵入警報	トリップワイヤ(横断検知)、侵入、放置物、シーン変更などの定義されたルールが破られた場合にアラームが発生します。
トリップワイヤーアラーム	
シーン変更	
ビデオ改ざん	監視映像が遮られ、出力映像が単色になった場合にアラームが発生します。
ディスクアラーム	ディスク未挿入、ディスクエラーなどの異常が発生した場合にアラームが発生します。

通知タイプ	説明
オブジェクト検出	- スマート放置物検知タイプを選択: 荷物／バッグ／箱 または 非自動車両 - スマート紛失物検知タイプを選択: 荷物／バッグ／箱 または 非自動車両
音の強度の変化	デバイスの音の強さが変化した場合にアラームが発生します。
顔検出	画像内で人の顔が検出されたときにアラームが発生します。
異常温度アラーム	温度が設定されたしきい値を超えた場合にアラームが発生します。
SDカードアラーム	SDカードの挿入または取り外し時にアラームが発生します。
IPCオフラインアラーム	IPC(ネットワークカメラ)がオフラインになったときにアラームが発生します。
ナンバープレート認識	カメラがナンバープレートを認識したときにアラームが発生します。
デフォーカス	カメラが対象物にピントを合わせられず、映像がぼやけた場合にアラームが発生します。
オブジェクト放棄	画像内に物体が放置されたときにアラームが発生します。
オブジェクト紛失	画像内から物体が消えたときにアラームが発生します。
高速移動(速い動き)	画像内で高速に移動する対象物がある場合にアラームが発生します。
徘徊検出	画像内で人が徘徊していると検出された場合にアラームが発生します。
滞留検知(人々は滞在する)	人が指定された時間以上にその場にとどまっているとアラームが発生します。
フレームアラーム	火が検出されたときにアラームが発生します。
喫煙警報	煙が検出されたときにアラームが発生します。
通話検出(アラームを呼び出す)	人が電話をかけていると検出されたときにアラームが発生します。
IPC外部アラーム	IPC(例: NVRなど)に接続されたデバイスがDMSSに追加されている場合、IPCでアラームが発生すると通知されます。
ローカルアラーム	アラームデバイスを追加されたデバイスのアラーム入力ポートに接続することで、アラームがトリガーされると連動動作が実行されます。
ネットワークアラーム	ネットワークに関するアラームが発生したときに通知が送信されます。
ソーラーエネルギーアラーム	ソーラー電力レベルが低下したときにアラームが発生します。
群衆警報	人が多数集まり、群衆密度が設定された限界を超えたときにアラームが発生します。
ビデオロス	映像が失われたときにアラームが発生します。



対応しているアラームメッセージの種類はデバイスによって異なります。詳細は実際のインターフェースをご確認ください。

ステップ5 (任意) 「デバイスオフライン通知」の横にあるスイッチ ☐ をタップして有効にします。

5.1.1.2 AI 検出

カメラのAI検出ルールおよび連動ルールを設定します。スマート動体検知の有効化／無効化、動体検知エリアの設定、感度の調整が可能です。

手順

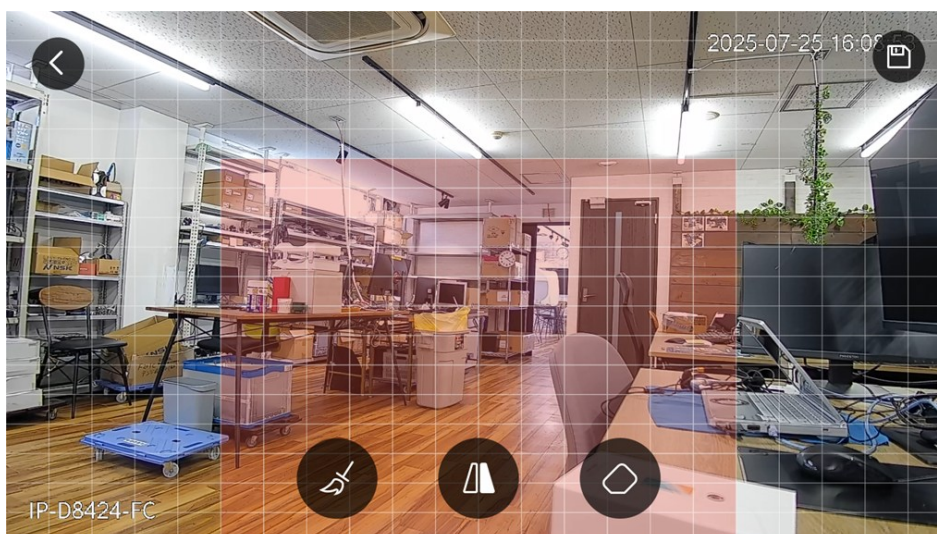
ステップ1 「デバイス」画面で、対象のデバイスの横にある ●●● をタップし、「デバイス詳細」を選択。

ステップ2 「機能設定」項目で「AI」をタップします。

ステップ3 対応する種類のスマート動体検知を有効にします。動体検知、人間検知、車両検知をサポートしています。

ステップ4 「動体検知エリア」をタップして、検知エリアを描画します。

図5-3 モーション検知領域



- :  画面上に検知エリアを描画します。
- :  表示モードを切り替えます。
- :  すべての検知エリアをクリアします。

ステップ5  「保存」をタップして設定を保存。

ステップ6 「検知感度」をタップし、感度の値を設定します。

値が高いほど検知感度が上がりますが、誤検知の可能性も高くなります。推奨設定は「3」です。

ステップ7 「保存」をタップします。

5.1.1.3 画像調整

IPC(ネットワークカメラ)の画像調整をサポートしています。調整可能な項目には、ワイドダイナミックレンジ(WDR)、ビデオプレーヤーのサイズ、画像の反転などがあります。

手順

ステップ1 「デバイス」画面で、対象のデバイスの横にある ●●● をタップし、「デバイス詳細」を選択。

ステップ2 「機能設定」エリアで「画像調整」をタップします。

図5-4 画像調整



表5-3 画像調整のパラメーター説明

パラメータ	説明
ワイドダイナミックレンジ	☐ タップして機能を有効にします。有効にすると、画像の非常に明るい部分や暗い部分もしっかり表示されますが、消費電力が増加します。
ビデオプレーヤーサイズ	ビデオプレーヤーのサイズを「全画面」または「元のスケール」から選択し、「保存」をタップします。
画像反転	☐ タップして機能を有効にします。有効にすると、映像が上下に回転します。

5.1.1.4 ナイトビジョン(夜間映像)

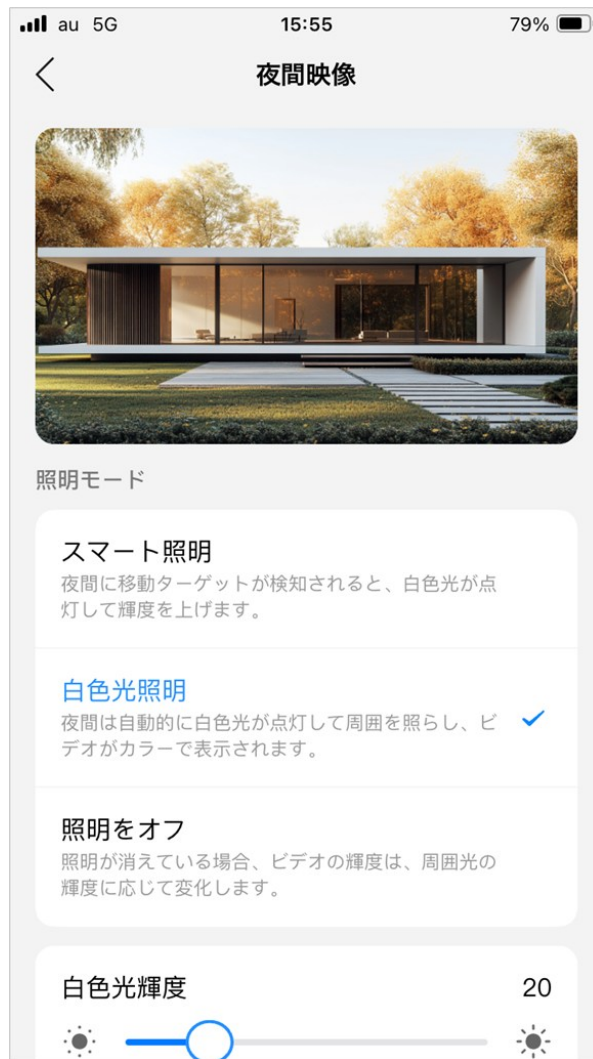
カメラの照明モードを選択します。スマート照明、白色光照明、赤外線(IR)照明のいずれかを選択できます。照明をオフにすることも可能です。

手順

ステップ1 「デバイス」画面で、対象のデバイスの横にある **⋮** をタップし、「デバイス詳細」を選択

ステップ2 「機能設定」エリアで「夜間映像(ナイトビジョン)」をタップします。

図5-5 夜間映像(ナイトビジョン)の構成



ステップ3 実際のニーズに応じて照明モードを選択します。

「照明をオフ」を選択すると、照明装置はオフになり、映像の明るさは周囲の光に依存します。

5.1.1.5 アラーム連動の無効化

「機能設定」項目で「アラーム連動を無効にする」の横にあるスイッチ  をタップし、アラーム連動機能を無効にします。

5.1.2 ビデオ再生設定

ビデオストリームのパラメーター設定、自作音声の追加、ビデオの暗号化などが行えます。

5.1.2.1 ストリーム設定

手順

ステップ1 「デバイス」画面で、対象のデバイスの横にある  をタップし、「デバイス詳細」を選択します。

ステップ2 「機能設定」項目で「その他(もっと)」>「ストリーム設定」をタップします。

ライブビューまたはビデオ再生用に「サブストリーム」または「メインストリーム」からビデオストリームを選択します。

- メインストリーム : ビットレートが大きく、画像の圧縮率が低いため高解像度ですが、その分多くの帯域幅が必要です。
- サブストリーム : ビットレートが小さく、映像がスムーズで帯域幅の使用が少なくなります。利用可能な帯域幅が不足している場合にメインストリームの代わりとして使用されます。

図5-6 ストリーム設定



ステップ3 「保存」をタップします。

5.1.2.2 音声のカスタマイズとビデオの暗号化

背景情報

カスタマイズの音声を設定したり、ビデオの暗号化を行うことができます。

「ビデオの暗号化」を有効にすると、ライブビューや再生(クラウド録画を含む)の際にパスワードの入力が必要になります。

手順

ステップ1 「デバイス」画面で、対象のデバイスの横にある ... をタップし、「デバイス詳細」を選択。

ステップ2 「機能設定」項目の「その他(もっと)」>「ビデオの暗号化」をタップします。

ステップ3 「ビデオの暗号化」の横にある ☐ スイッチをタップして機能を有効にします。

図5-7 音声のカスタマイズとビデオの暗号化



ステップ4 確認プロンプトが表示されたら、「有効にする」をタップします。

ステップ5 「パスワード設定」画面でパスワードを設定し、「保存」をタップします。

パスワード設定後は、「パスワードの変更」および

「パスワードを忘れた」のオプションが「自作音声とビデオ暗号化」画面に表示されます。

関連操作

- パスワードを変更する場合：「カスタマイズ音声とビデオ暗号化」画面で「パスワードの変更」をタップし、旧パスワードと新パスワードを入力します。
- パスワードを忘れた場合：「カスタマイズ音声とビデオ暗号化」画面で「パスワードを忘れた(Forget Password)」をタップすると、登録済みのメールアドレスに確認メールが送信されます。
メール内の認証コードを入力し、新しいパスワードを作成してください。

5.1.3 一般設定

タイムゾーンの設定、デバイスの共有、デバイスのアップデート情報の確認などが行えます。

5.1.3.1 ネットワーク設定

デバイスが接続するWi-Fiを選択できます。

手順

ステップ1 「デバイス」画面で、対象のデバイスの横にある●●●をタップし、「デバイス詳細」を選択。

ステップ2 「設定」セクションで「ネットワーク設定」をタップします。

ステップ3 表示されたWi-Fiリストから接続したいWi-Fiを選択します。

5.1.3.2 音声録音

「デバイス詳細」ページで「その他(もっと)」をタップし、「音声収集」の横にあるスイッチをタップ ☐ して音声録音機能を有効にします。

5.1.3.3 タイムゾーン

お住まいの地域で夏時間(DST)を採用している場合は、タイムゾーンの選択とDSTの設定が可能です。

手順

ステップ1 「デバイス」画面で、対象のデバイスの横にある●●●をタップし、「デバイス詳細」を選択。

ステップ2 「デバイス詳細」画面で「その他(もっと)」>「タイムゾーン」をタップします。

図5-8 タイムゾーン



ステップ3 デバイスが設置されている地域のタイムゾーンを選択します。

ステップ4 「DST(夏時間)」の横にあるスイッチをタップ ☐ して機能を有効にし、夏時間の開始時刻と終了時刻を設定します。

5.1.3.4 クラウドアップデート

「デバイス詳細」画面でデバイスのアイコンをタップすると、「デバイス情報」画面に移動します。
「ファームウェアバージョン」をタップすると、現在のデバイスバージョンを確認でき、新しいバージョンが利用可能な場合はアップグレードが可能です。

図5-9 ファームウェアバージョン



5.1.3.5 リモート設定

ビデオ検出、アラーム設定、カメラ設定、ストレージ管理、画像調整などをリモートで設定することができます。

手順

ステップ1 「ホーム」画面で、対象のデバイスの横にある●●●をタップし、「デバイス詳細」を選択します。

ステップ2 「デバイス詳細」画面で「その他(もっと)」>「リモート設定」をタップします。

図5-10 リモート設定



5.1.3.5.1 ビデオ検出

定義された条件のもとで動く対象が検出された場合や、映像が遮られた場合に、システムはアラーム連動動作を実行します。

動体検知

映像内に移動する対象が現れ、その速度が感度レベルに達すると、アラーム連動動作が実行されます。

1. 「デバイス」画面で、対象のデバイスの横にある ●●● をタップし、「デバイス詳細」を選択します。
2. 「その他」セクションで「リモート設定」>「映像検出」>「動体検知」を選択します。。
3. 設定したいデバイスのチャンネルを選択します。
4. 「有効化」の横にある ☐ スイッチをタップして、機能を有効にします
5. 「詳細設定」の横にある ☐ スイッチをタップして機能を有効にし、その他のパラメーターを設定します。

図5-11 動体検知(詳細設定)



表5-4 動体検知(詳細設定)

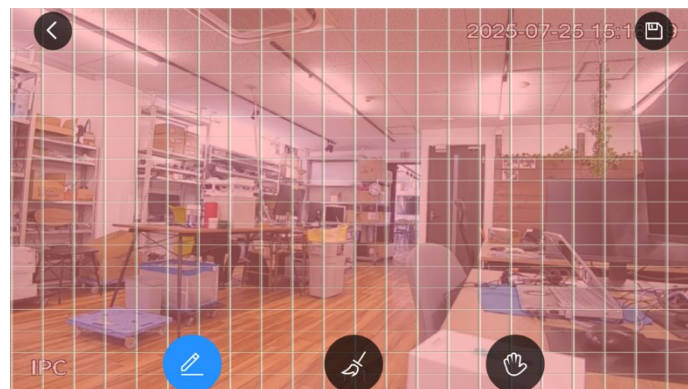
機能	説明
警戒/解除期間	警戒時間帯を設定します。アラームは、定義された時間帯内に発生した場合のみトリガーされます。 日付を選択し、定義された警戒時間の横にある スイッチをタップしてから「保存」をタップします。
アンチディザ	アンチディザ(抑制)時間を0秒～600秒の範囲で設定します。この期間内に発生した動体検知イベントは1回のみ記録されます。
感度	感度の値を0～100の範囲で設定します。感度が高いほどアラームが発生しやすくなります。
エリア設定	動体検知の対象領域を設定します。デフォルトでは映像全体が監視エリアです。 • タップして動体検知エリアを設定します。 • タップして設定済みのゾーンをクリアします。 • タップ後、指をピンチイン・ピンチアウトして画像を拡大・縮小します
録画	「録画」の横にあるスイッチをタップして機能を有効にすると、アラームが発生したときに自動で録画が開始されます。

機能	説明
遅延(ディレイ)	アラームが発生した際、指定された時間に基づいて記録が生成され、アラーム終了後に送信されます。
アラーム出力	「アラーム出力」の横にある ☐ スイッチをタップして機能を有効にすると、アラームがトリガーされたときに接続されたアラーム出力装置が連動します。
遅延(出力)	アラーム終了後、定義された時間の間アラーム出力が継続されます。
スナップショット	「スナップショット」の横にある ☐ スイッチをタップして機能を有効にすると、アラームがトリガーされた際にシステムが自動的に画像をキャプチャします。

図5-12警戒／解除期間



図5-13 エリア設定



ビデオマスク

監視映像が遮られたり、出力映像が単色(黒、白など)になった場合にアラームがトリガーされます。

1. 「デバイス」画面で、対象のデバイスの横にある「:」をタップし、「デバイス詳細」を選択します。...
2. 「その他」セクションで「リモート設定」>「映像検出」>「動体検知」を選択します。
3. 設定したいデバイスのチャンネルを選択します。
4. 「有効化」の横にある ☐ スイッチをタップして、機能を有効にします。
5. 「詳細設定(Advanced Configuration)」の横にある ☐ スイッチをタップして、他のパラメーターを設定します。

図5-14 詳細設定(ビデオマスク)



6. 「保存」をタップします。

5.1.3.5.2 アラーム設定

背景情報

アラームがトリガーされると、録画、スナップショット、アラーム出力などのアクションが連動して実行されます。アラームの種類(主にネットワークビデオレコーダーに対応)には、以下が含まれます。

「ローカルアラーム、ネットワークアラーム、IPC外部アラーム、IPCオフラインアラーム」

このセクションでは、ローカルアラームの設定を例として説明します。

表5-5 アラーム設定

アラームタイプ	説明
ローカルアラーム	追加されたデバイスのアラーム入力ポートにアラーム装置を接続します。 アラームがトリガーされると、アラーム連動動作が実行されます。
ネットワークアラーム	アラーム信号がネットワークを介してデバイスに送信されると、アラーム連動動作が実行されます。
IPC外部アラーム	IPC(ネットワークカメラ)をアラーム入力デバイスに接続します。 アラームがトリガーされると、アラーム連動動作が実行されます。
IPCオフラインアラーム	追加されたデバイスとIPCが切断された場合に、アラーム連動動作が実行されます。
PIRアラーム	PIR(パッシブ赤外線)ベースのモーションディテクターで物体を検出するとアラームがトリガーされます。

手順

ステップ1 「デバイス」画面で、対象デバイスの横にある●●●をタップし、「デバイス詳細」をタップします。

ステップ2 「その他」セクションで、「リモート設定 > アラーム設定 > ローカルアラーム」を選択します。

ステップ3 設定したいデバイスチャンネルを選択します。

ステップ4 「有効にする」の横にある ☐ [スイッチ] をタップして、機能を有効にします。

ステップ5 「高度な設定」の横にある ☒ [スイッチ] をタップして機能を有効にし、その他のパラメータを設定します

ステップ6 「保存」をタップします。

図5-15 高度な設定(ローカルアラーム)



5.1.3.5.3 カメラ設定

背景情報

ビデオストリームのパラメータを設定できます。
エンコード方式、解像度、フレームレート、ビットレートタイプ、ビットレートなどを設定することが可能です。

手順

- ステップ1 「デバイス」画面で、対象デバイスの横にある●●● [アイコン] をタップし、「デバイス詳細」をタップします。
- ステップ2 「その他」セクションで、「リモート設定 > カメラ設定 > ビデオストリーム」を選択します。
- ステップ3 設定したいデバイスチャンネルを選択します。
- ステップ4 チャンネル名を設定します。



機器の設置場所に応じて、識別しやすい名前を設定することを推奨します。

- ステップ5 メインストリームまたはサブストリームを選択します。

図5-16 ビデオストリーム(メイン)

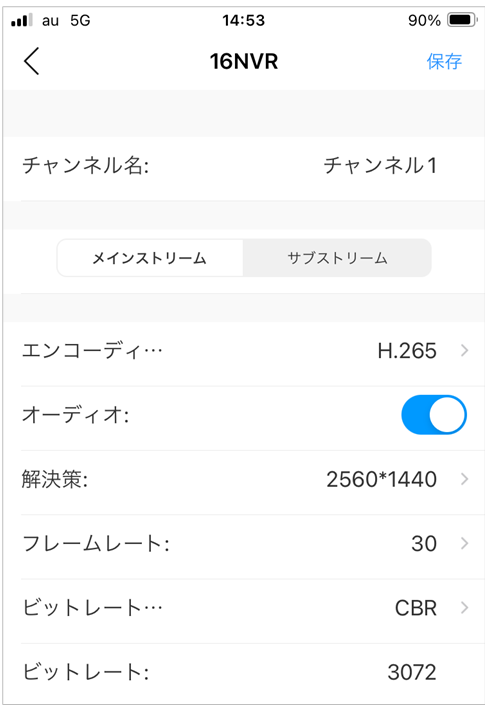


表5-6 ビデオストリームパラメータ

機能	説明
メイン/サブストリーム	- メインストリーム：ビットレートが大きく、画像の圧縮率が低いため高解像度の映像を提供できますが、大きな帯域幅を必要とします。 - サブストリーム：ビットレートが小さく、映像は滑らかで少ない帯域幅で済みます。帯域幅が不足している場合にメインストリームの代替として使用されます。

機能	説明
エンコードモード	• MJPEG：鮮明な画像を確保するには高いビットレートが必要です。より良い画質のために、ビットレートの値を最大に設定することを推奨します。 • H.264：メインプロファイルのエンコードモードです。 • H.264H：ハイプロファイルのエンコードモードです。H.264と同等の画質を維持しながら、より少ない帯域幅を使用します。
ビデオ	このパラメーターはサブストリームを選択した場合にのみ設定できます。「ビデオを有効にする」と、ビデオストリームの種類がサブストリームになります。
オーディオ	オーディオストリームの種類をメインストリームまたはサブストリームに設定します。
解像度	ビデオストリームの解像度を設定します。解像度が高いほど映像の品質は向上しますが、それに伴い必要な帯域幅も大きくなります。  対応している解像度は機器によって異なりますのでご注意ください。
フレームレート	フレームレートを1～25の範囲で設定します。フレームレートが高いほど映像は滑らかで鮮明になりますが、それに伴い必要な帯域幅も大きくなります。
ビットレートタイプ	• CBR(固定ビットレート)：ビットレートの変動がほとんどなく、設定されたビットレート値に近い状態を維持します。シーンが複雑な場合は映像が不鮮明になることがあります。シーンが単純な場合は帯域幅が無駄になる可能性があります。 • VBR(可変ビットレート)：監視シーンに応じてビットレートが変動します。シーンが複雑な場合には映像を鮮明に保ち、シーンが単純な場合には必要な帯域幅を抑えることができます。
画質	このパラメーターは、ビットレートタイプがVBR(可変ビットレート)に設定されている場合にのみ設定できます。画質が高いほど、必要な帯域幅も大きくなります。
ビットレート	ビデオのビットレートを設定します。ビットレートが高いほど、データの転送速度が速くなります。

ステップ6 「保存」をタップします。

5.1.3.5.4 録画プラン

デバイスの録画期間および録画タイプを設定できます。

手順

ステップ1 [デバイス]画面で、対象デバイスの横にある●●●アイコンをタップし、[デバイス詳細]をタップします。

ステップ2 [その他]セクションで、[リモート設定]>[録画プラン]を選択します。

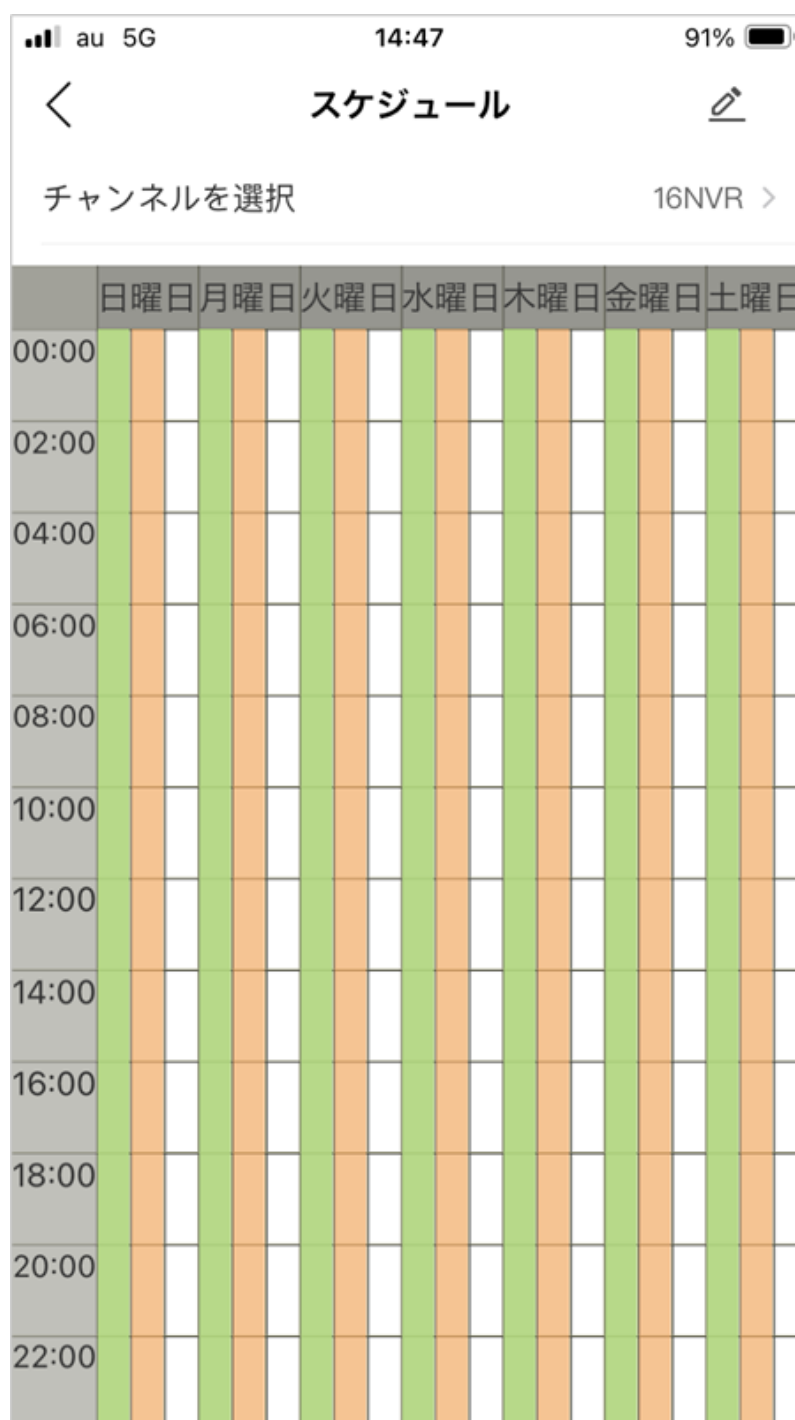
ステップ3 設定したいデバイスのチャンネルを選択します。



録画タイプによって色分けがされています。

- 緑：通常録画。
- オレンジ：動体検知アラームが作動した際の録画。
- 赤：アラーム録画(アラームが作動したときに録画)

図5-17 スケジュール



ステップ4 [✎]をタップし、日付を選択して、開始時刻と終了時刻を設定します(1日に最大6つの時間帯を設定可能)。



[コピー]をタップして他の曜日を選択すると、設定した警戒時間帯が選択した曜日にも適用されます。

図5-18 録画の設定



ステップ5 「保存」をタップします。

5.1.3.5.5 画像調整

ライブビュー映像のフォーカス、ズーム、明るさ、コントラスト、画質などの設定を調整できます。

手順

ステップ1 [デバイス]画面で、対象デバイスの横にある●●●アイコンをタップし、[デバイス詳細]をタップします。

ステップ2 [その他]セクションで、[リモート設定]>[画像調整]を選択します。

ステップ3 設定したいデバイスのチャンネルを選択すると、システムがライブ画面に切り替わります。

ステップ4 アプリ上で各種操作を行います。

図5-19 画像調整

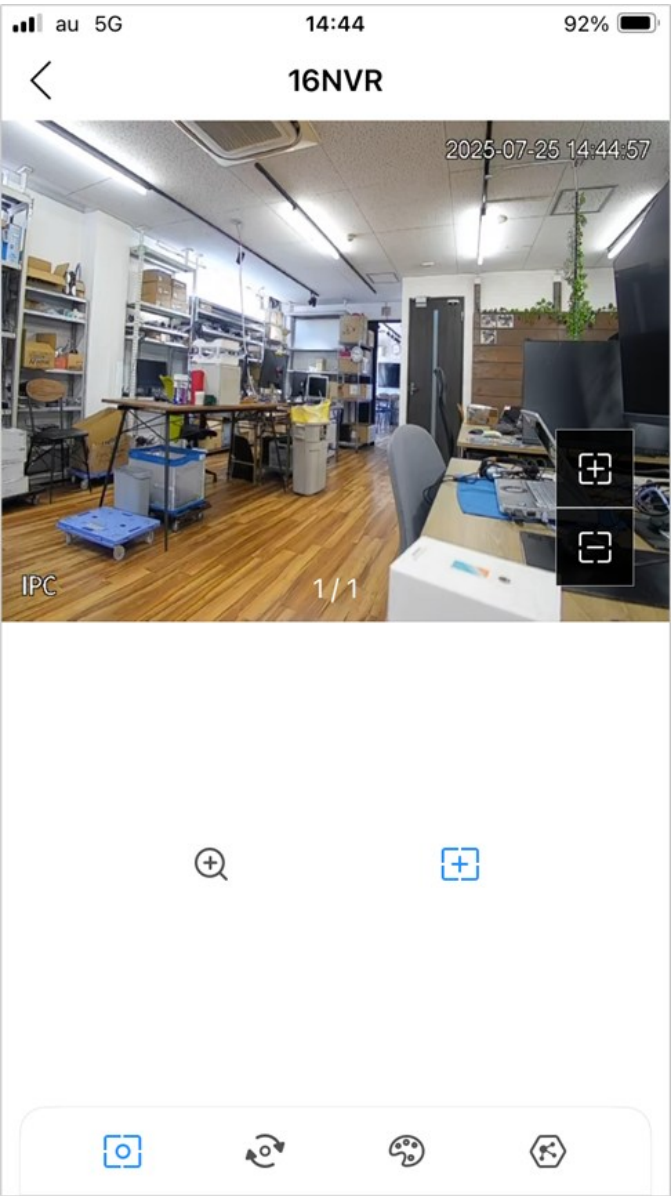


表5-7 機能アイコンの説明

機能	説明
フォーカス/ズーム	⊕ タップして画像をズームイン／ズームアウトします。 ⊞ タップしてフォーカスを調整し、画像をより鮮明にします。  画像上の「+」または「-」をタップすることで、フォーカスやズームの効果を調整できます。

機能	説明
回転/反転	 タップして画像を回転または反転します。  : 左右に反転します。  : 上下に反転します。  : 90°反時計回りに回転します。  : 90°時計回りに回転します。  : 180°回転します。
画像効果	 タップして画像効果を調整します。  : 明るさ  : コントラスト  : 色相  : 彩度  : デフォルトに戻す
ビデオ画質	 タップしてライブ映像の画質を調整します。  : リアルタイムモード  : スムーズモード  : 自動モード

5.1.3.5.6 警戒／解除時間帯の設定

警戒時間帯を設定することで、アラームが発生した場合でもその時間帯内でのみ有効になります。

手順

ステップ1 「デバイス」画面で、対象デバイスの横にある●●●アイコンをタップし、[デバイス詳細]をタップします。

ステップ2 「その他」セクションで[リモート設定]>[警戒／解除時間帯]を選択します。

ステップ3 警戒時間帯を設定します。

警戒時間帯の詳細な設定方法については、「5.1.3.5.1 ビデオ検知」を参照してください。[\(Link\)](#)

5.1.3.6 DDNS の設定

DDNS(Dynamic Domain Name System)パラメーターを設定して、DNSサーバーのドメインをデバイスの外部ネットワークIPにバインドすることで、直接デバイスへアクセスできるようにします。

前提条件

- デバイスがドメイン名解決に対応するサーバーをサポートしていることを確認してください。
- サードパーティーのDDNSにてアカウント登録が完了していることを確認してください。ここでは例として「NO-IP」の登録を使用します。登録には以下のサイトを利用してください。
 - ◇ 登録ページ: <https://www.noip.com/sign-up> [\(Link\)](#)。
 - はじめてガイド: <https://www.noip.com/support/knowledgebase/getting-started-with-no-ip-com/> [\(Link\)](#)

図5-20 無料登録

Create Your No-IP Account

Indicates required fields

Email *

Password *

Minimum of 8 characters

Password Strength

Hostname

Choose a hostname for your account. You can change your hostname or add more later.

☐ Create my hostname later

Why not upgrade?

Upgrade to Enhanced Dynamic DNS Today. Learn more about the benefits of upgrading below.

	Enhanced DDNS	Free DDNS
Domain Choices	0	80+
Hostnames	0	1
No Ads	0	1
No 30-Day Hostname Confirmation	0	1
Phone Support	0	1
Includes 1 TrustCor Standard DV SSL Certificate	0	1
	\$1.99/mo	\$0

Terms of Service and Privacy Policy *

☒ I agree to the Terms of Service and Privacy Policy. I also agree that I will only create one free account.

Email Opt-in

☒ Send me newsletters & special offers



DDNSを有効にすると、サードパーティのサーバーがデバイス情報を収集する可能性があります。

手順

ステップ1 デバイスを追加した後、[デバイス追加]画面に進み、[サードパーティDDNS]をクリックします。

または、[デバイス詳細]>[その他]>[サードパーティDDNS]を選択することもできます。

ステップ2 [タイプ]をタップし、必要に応じて各種パラメーターを設定します。

ステップ3 [保存]をタップします。

図5-21 DDNS パラメータ

< Third-party DDNS Save

Type NO-IP DDNS >

NO-IP DDNS ☐

Address dynupdate.no-ip.com

IP/Domain none

Username none

Password

Update Interval 1440 Min

After DDNS is enabled, the third-party server might collect the information on your device.

表5-8 DDNS パラメータの説明

パラメーター	説明
タイプ	DDNSサーバー提供者の名前とアドレスを指定します。以下の接続先があります:
アドレス	
IP/ドメイン	登録されたドメイン名を入力します。
ユーザー名	DDNSサーバー提供者のウェブサイトで登録したユーザー名を入力します。
パスワード	
更新間隔	デバイスとサーバー間で接続情報を更新する間隔を設定します。

5.1.3.7 UPnP の設定

UPnP(Universal Plug and Play)プロトコルを通じて、イントラネットとエクストラネットの間のマッピングを確立し、伝送速度を向上させてライブ映像を迅速に表示します。

前提条件

- ルーターにログインし、WANポートのIPをエクストラネットに接続する。
- ルーターでUPnPが有効になっている。
- デバイスをルーターのLANポートに接続してイントラネットに接続する。
- Web画面の左上隅で「」をクリックし、[ネットワーク設定] > [TCP/IP] を選択して、ルーターのIPアドレスを設定するか、DHCPを有効にして自動的にIPアドレスを取得する。

手順

ステップ1 デバイスを追加後、「デバイス追加」画面に移動し、UPnPを有効化して設定を行います。
または、[デバイス詳細] > [その他] > [UPnP] を選択することも可能です。

ステップ2 「すべて有効にする」 をタップします。

図5-22 UPnPの設定(1)

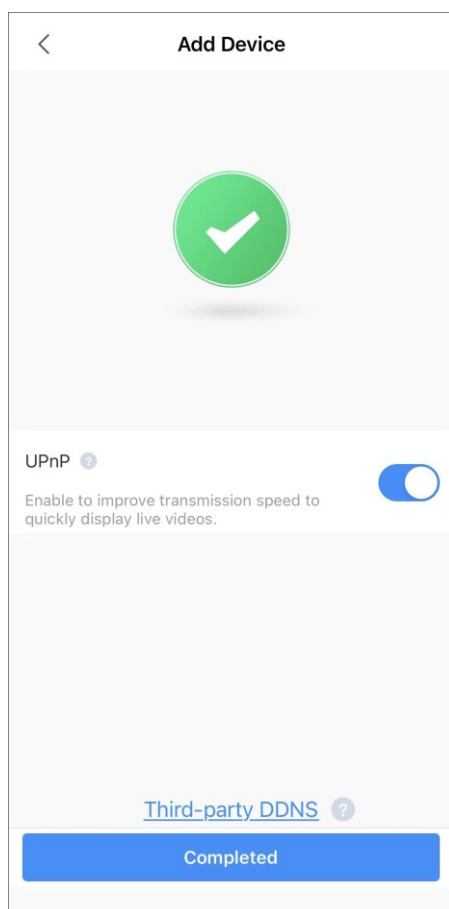
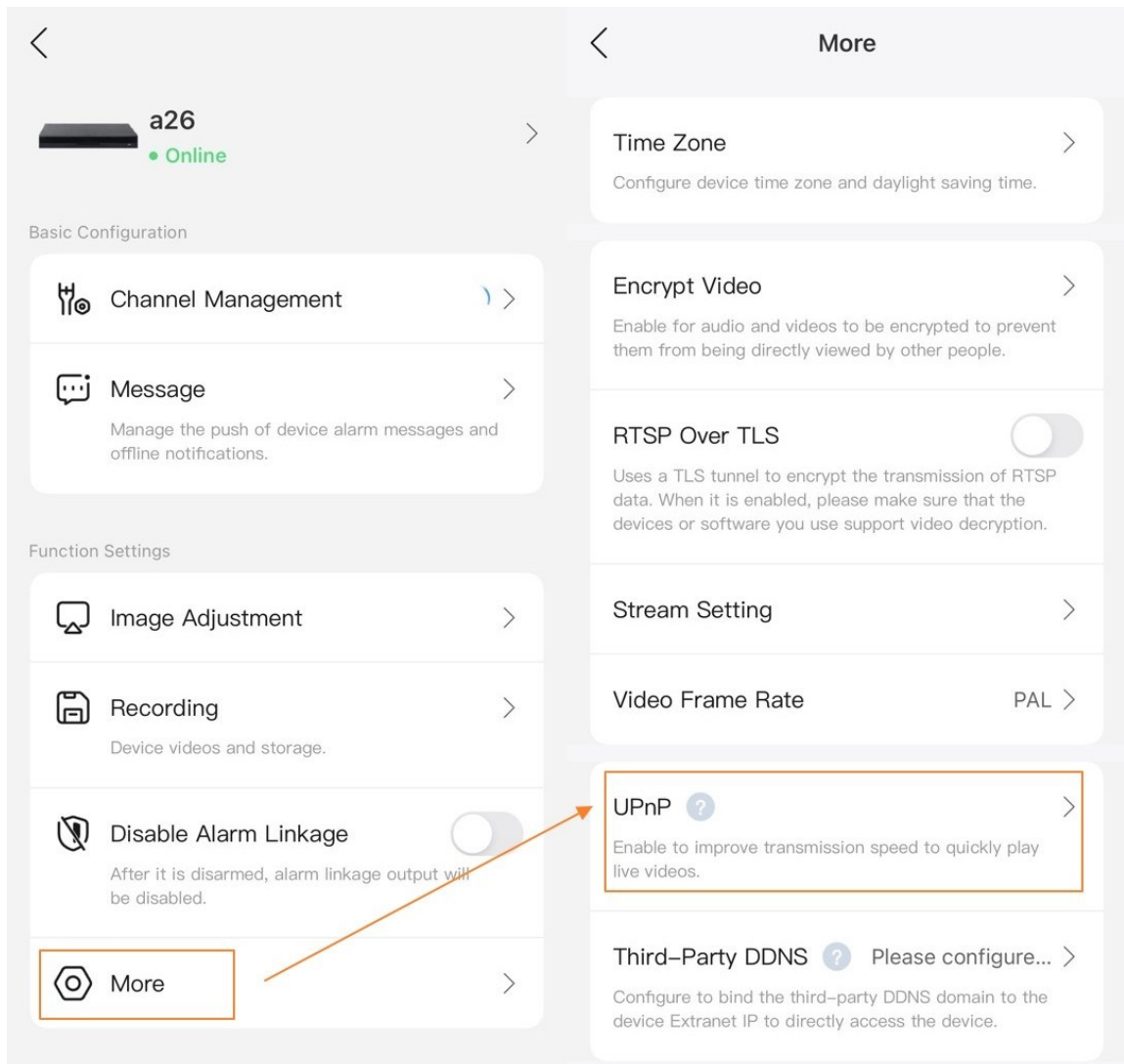


図5-23 UPnP の設定(2)



5.1.3.8 アラーム出力

アラーム出力モードを「無効」「マニュアル(手動)」「オート(自動)」のいずれかに設定できます。
追加されたデバイスがアラーム出力機器に接続されており、ビデオ検知またはアラーム設定内で「アラーム出力」が有効になっている場合は、アラーム連動が有効に機能するように、アラーム出力モードを設定する必要があります。

手順

ステップ1 デバイス画面で、対象のデバイスの横にある「●●●」をタップし、[デバイス詳細] を選択。

ステップ2 [その他] > [アラーム出力] をタップします。

図5-24 アラーム出力



ステップ3 アラーム出力モードを設定します。

- 無効：アラームは無効になります(出力されません)。
- マニュアル：アラームは常時オンになります(常に出力されます)。
- オート：アラームイベントが発生したときのみアラームが作動します(自動出力)。

5.1.3.9 ストレージマネージャー

手順

ステップ1 デバイス画面で、対象のデバイスの横にある「●●●」をタップし、[デバイス詳細] を選択。

ステップ2 [録画]をタップします。

ステップ3 ストレージ情報を確認できます。

[フォーマット]をタップすると、ストレージを初期化できます。



フォーマットを実行すると、ストレージ内のすべてのファイルが削除されます。実行前にご注意ください。

関連操作

NVRまたはXVRデバイスでは、「一般録画機能」を有効にし、録画スケジュールを設定することも可能です。

5.1.3.10 その他の設定

[その他]をタップすることで、以下のパラメーターを設定できます。

表5-9 その他の構成

パラメーター	説明
RTSP over TLS	 /  をタップして機能を有効または無効にします。RTSP over TLS はリアルタイムストリーミングにセキュアでプライベートな保護を提供し、全体的なセキュリティを強化します。
ビデオフレームレート	PAL または NTSC からビデオフレームレートを選択できます。

5.2 デバイスの共有

1台のデバイスは、最大16人のDMSSユーザーと共有することができます。

手順

ステップ1 デバイス画面で、対象のデバイスの横にある「●●●」をタップし、[デバイス共有] を選択します。

ステップ2 「デバイス共有」画面で、共有相手のDMSSアカウントを入力するか、相手のQRコードをスキャンしてデバイスを共有します。また、電話番号を入力して共有することも可能です。



電話番号による共有は、一部の国または地域でのみ対応しています。

ステップ3 必要に応じてアクセス権限(権限)を選択します。

ビデオ再生、アラームプッシュ通知、またはデバイス制御を選択できます。ライブビューはデフォルトで有効化されており、無効にはできません。



アラームデバイスの権限は、その他のデバイスと異なる場合があります。実際の利用目的に応じて適切な権限を設定してください。

ステップ4 [OK] をタップします。

共有されたアカウントは、「デバイス共有」画面の[共有ユーザー]セクションに表示されます。

図5-25 デバイスの共有



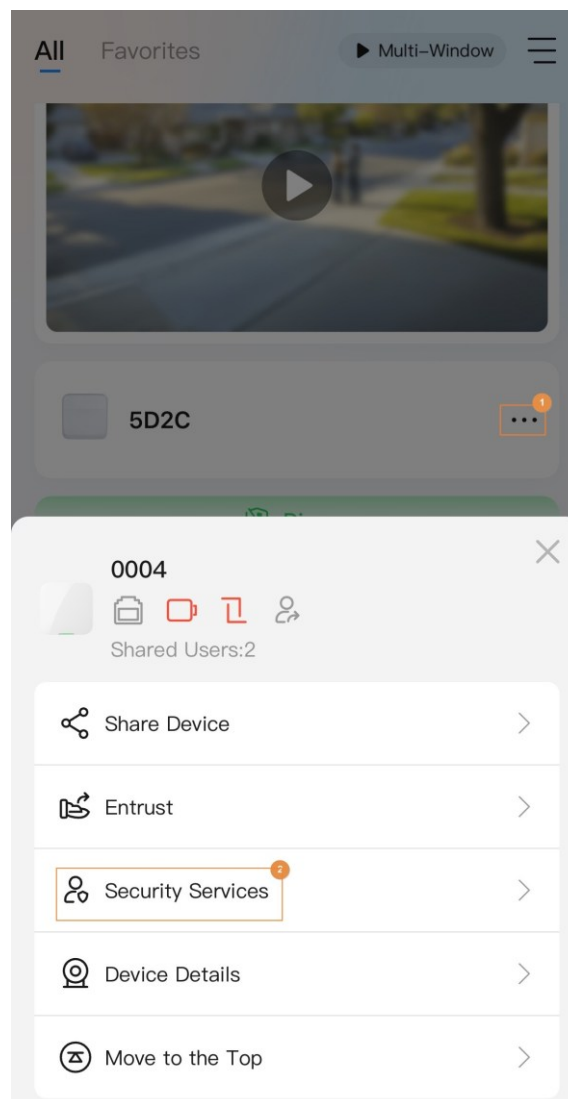
5.3 セキュリティサービスの申請

アラームハブに対してセキュリティサービスを申請することができます。
デバイスをその地域のConverterアカウントにバインド(紐づけ)してください。
アラームハブをConverterアカウントにバインドした後は、すべてのアラームメッセージ、エラー、および通知がConverterに送信されます。

手順

ステップ1 デバイス画面で、アラームハブの横にある  をタップし、「セキュリティサービス」をタップします。

図5-26 セキュリティサービスの申請



ステップ2 「申請」をタップします。

ステップ3 現在のDMSSアカウントと同じ都市にあるセキュリティ会社が表示されます。表示内容には、会社名、メールアドレス、ロゴが含まれます。
会社をタップすると、その会社の詳細が表示され、「申請」をタップできます。



- セキュリティ会社の画面上部で、国や地域を選択できます。
- 会社名を入力して検索することも可能です。

ステップ4 アカウント情報を確認し、「申請」をタップします。

関連操作

バインド申請が送信されると、Converterアカウントが申請内容を確認し、サービスを有効化する必要があります。
申請が承認されると、メッセージを受信することができます。

5.4 デバイスの委任



フランス、ベネルクス、イタリア、スペイン・ポルトガル、ドイツ、ハンガリー、チェコ共和国、トルコ、バルト海地域、ポーランド、ラテンアメリカ、ロシア、ミャンマー、タイ、ベトナム、アルジェリア、チュニジア、タンザニア、南アフリカ、オーストラリア、インドなど。

デバイスは1台ずつ、または一括で委任することができます。
デバイス委任サービスは、以下の国や地域で利用可能です。

5.4.1 デバイスを1つずつ委託する

デバイスをDoLynk Careユーザーに委任することができます。
また、委任する際の権限を設定することも可能です。

前提条件

サービスプロバイダーとバインドされています。詳細は「13 私(マイページ)」を参照してください。[\(Link\)](#)

手順

- ステップ1 デバイス画面で、対象デバイスの横にある[●●●] をタップし、「デバイス詳細」を選択します。
- ステップ2 「デバイス詳細」ページでデバイスアイコンをタップして「デバイス情報」画面に移動し、「委任」をタップします。
- ステップ3 「委任」画面で、バインドされているサービスプロバイダーの情報を確認します。
- または、対応するインストーラーのQRコードを  スキャンすることも可能です。
- ステップ4 委任期間および権限を選択し、「OK(確認)」をタップします。

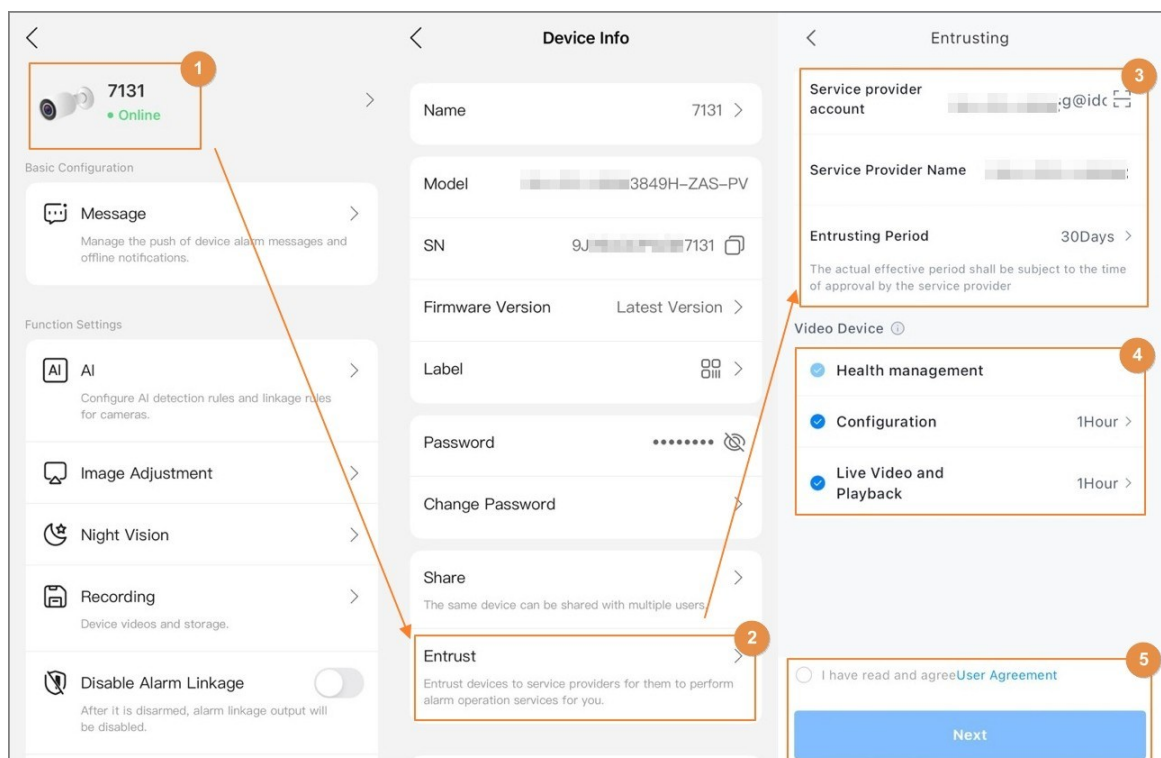
表5-10 権限の説明

許可	説明	注
ヘルス管理	この項目はデフォルトで選択されており、解除することはできません。 以下の権限が含まれます。ワンクリック健康チェック、エラー報告、エラー修復、データ統計、ヘルスレポートの生成	—
ビデオデバイス	デバイス設定、ライブ映像、再生に関する権限をリクエストすることができます。 - 設定権限：デバイスの再起動・アップグレード、SDカードのフォーマット、プラグインの設定などが含まれます。 - ライブ映像と再生: ライブ映像の閲覧、録画の再生、プラグイン映像の閲覧などが可能です。	権限は、1時間や4時間といった一時的な許可を選択することも、委任期間全体にわたる許可を選ぶこともできます。 たとえば、委任期間が30日の場合、30日間すべての期間において権限を付与することが可能です。

許可	説明	注
アラームデバイス	アラームデバイスに対しては、設定権限および操作権限をリクエストすることができます。 - 設定権限: 周辺機器(センサーなど)の追加・削除・設定、ルーム(部屋)の追加・削除・設定、デバイス情報の編集、デバイスのネットワーク設定およびタイムゾーン設定、デバイスのアップグレード、ユーザーの追加・削除、デバイスパスワードの変更、Converterアカウントとのバインド。 - 操作権限: 以下の操作が可能になります: 警戒モードのオン/オフ(SOSを含む)、アラームハブおよび周辺機器のテスト、アラーム出力制御(プラグ、スイッチ、リレーの操作)	
映像連携デバイス	映像連携デバイスに対しては、設定権限および操作権限をリクエストすることができます。 - 設定権限: ネットワーク伝送の設定、SIP(Session Initiation Protocol)の構成、デバイスメンテナンス - 操作権限: 通話(インターホンなど)、ドアの解錠操作	

ステップ5 「ユーザー契約を読み、同意しました」にチェックを入れ、「次へ」をタップします。

図5-27 デバイスの委任



結果

デバイスリスト画面で、委任状況を確認することができます。

委任が正常に完了すると、デバイスのステータスは以下のように変化します:

審査中(Under Reviewing) → 委任中(Entrusting) → ****



※「****」の部分には、最終的なステータス(例:委任完了、使用中など)が表示されます。具体的なステータス名はシステムによって異なります。

関連操作

- 権限を変更するには、「会社への委任」画面に移動し、「権限を変更」をタップします。
- 委任権限を取り消すには、「会社への委任」画面に移動し、「委任を取り消す」をタップします。
- 委任期間を更新するには、「会社への委任」画面に移動し、「更新」をタップします。

5.4.2 デバイスの一括委任

複数のデバイスを一括でサービスプロバイダーに委任することができます。

前提条件

サービスプロバイダーとバインド済みである必要があります。詳細については、「13 私(マイページ)」を参照してください。(Link)

手順

ステップ1 デバイス画面で、「私(マイページ)」>「サービス」>「サービスプロバイダー」を選択し、その後⁺をタップします。

ステップ2 「デバイス委任」画面で、バインドされているサービスプロバイダーの情報を確認します。

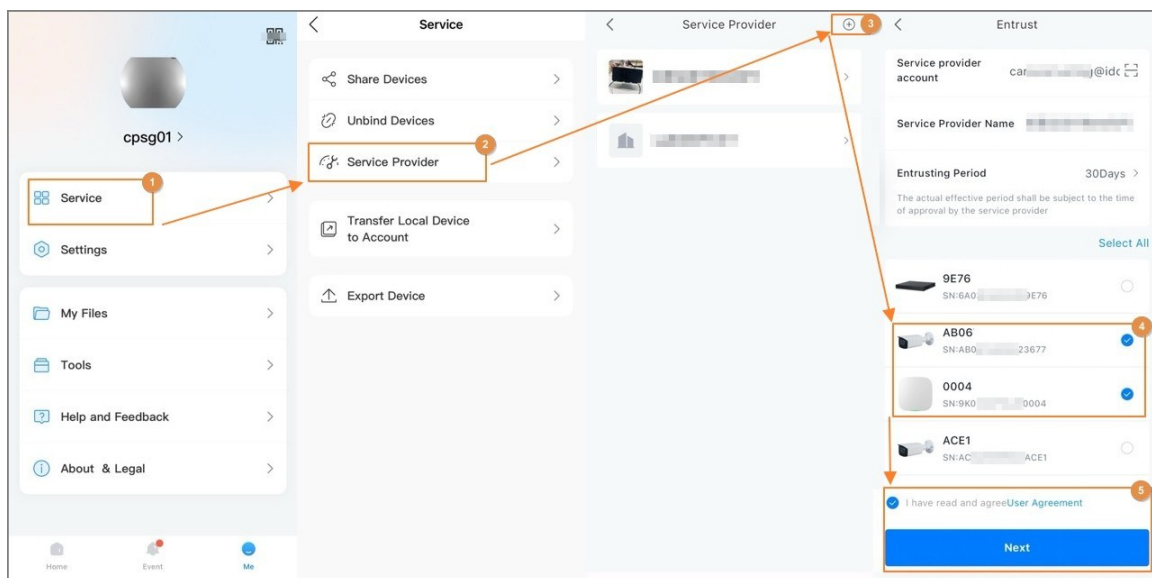
または、サービスプロバイダーのQRコードを[□]スキャンすることも可能です。

ステップ3 委任するデバイスを選択し、それらをDoLynk Careに委任します。

複数のデバイスを委任する手順は、単一のデバイスを委任する場合と同じです。

詳細については、「5.4.1 デバイスを1台ずつ委任する」を参照してください。(Link)

図5-28 デバイスの一括委任



5.5 デバイスのバインド解除

デバイスを追加する際に、すでに他のアカウントにバインドされている場合は、まずそのデバイスのバインドを解除する必要があります。バインド解除後、正常にデバイスを追加することができます。

手順

ステップ1 ホーム画面で「バインド解除」をタップします。

ステップ2 「バインド解除を申請」をタップします。

ステップ3 QRコードをスキャンするか、デバイスのSN(シリアル番号)を手動で入力してください。方法は以下の2通りです。

- バインド解除の申請
 1. システムに認証コードが表示されます。画面の指示に従って、必要な画像をアップロードしてください。
 2. システムが提出された情報を確認します。情報の確認が完了し、承認されると、デバイスのバインドが解除されます。
- デバイスパスワードによるバインド解除: デバイスのパスワードを入力することでバインドを解除できます。



デバイスはオンライン状態である必要があります。
パスワードを忘れた場合や、パスワードが正しくない場合は、バインド解除を申請することができます。

5.6 デバイスカードの作成

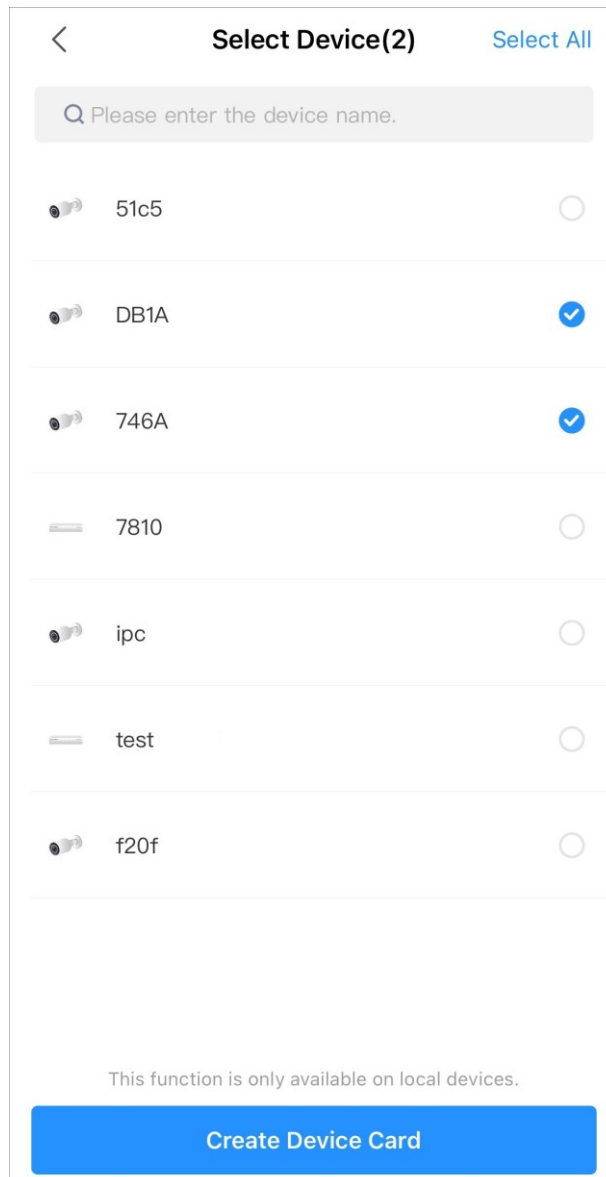
デバイスカードをスキャンすることで、デバイスを素早く追加することができます。

手順

ステップ1 「私(マイページ)」画面で、「サービス」>「デバイスをエクスポート」をタップします。

ステップ2 デバイスを選択します(最大10台まで)、その後「デバイスカードを作成」をタップします。

図5-29 デバイスカードの作成



ステップ3 (任意) デバイスカードを暗号化する場合は、「OK」をタップします。パスワードを入力し、「OK」を再度タップします。



デバイスカードをスキャンしてデバイスをインポートする際は、パスワードの入力が必要です。

ステップ4 デバイスカードのQRコードをアルバムに保存します。

5.7 ローカルデバイスをアカウントに移行する

ローカルデバイスを追加した後、そのデバイスをアカウントにバインドすることができます。
バインド後は、どの端末からでもアカウントにログインすることで、そのデバイスを確認できます。

手順

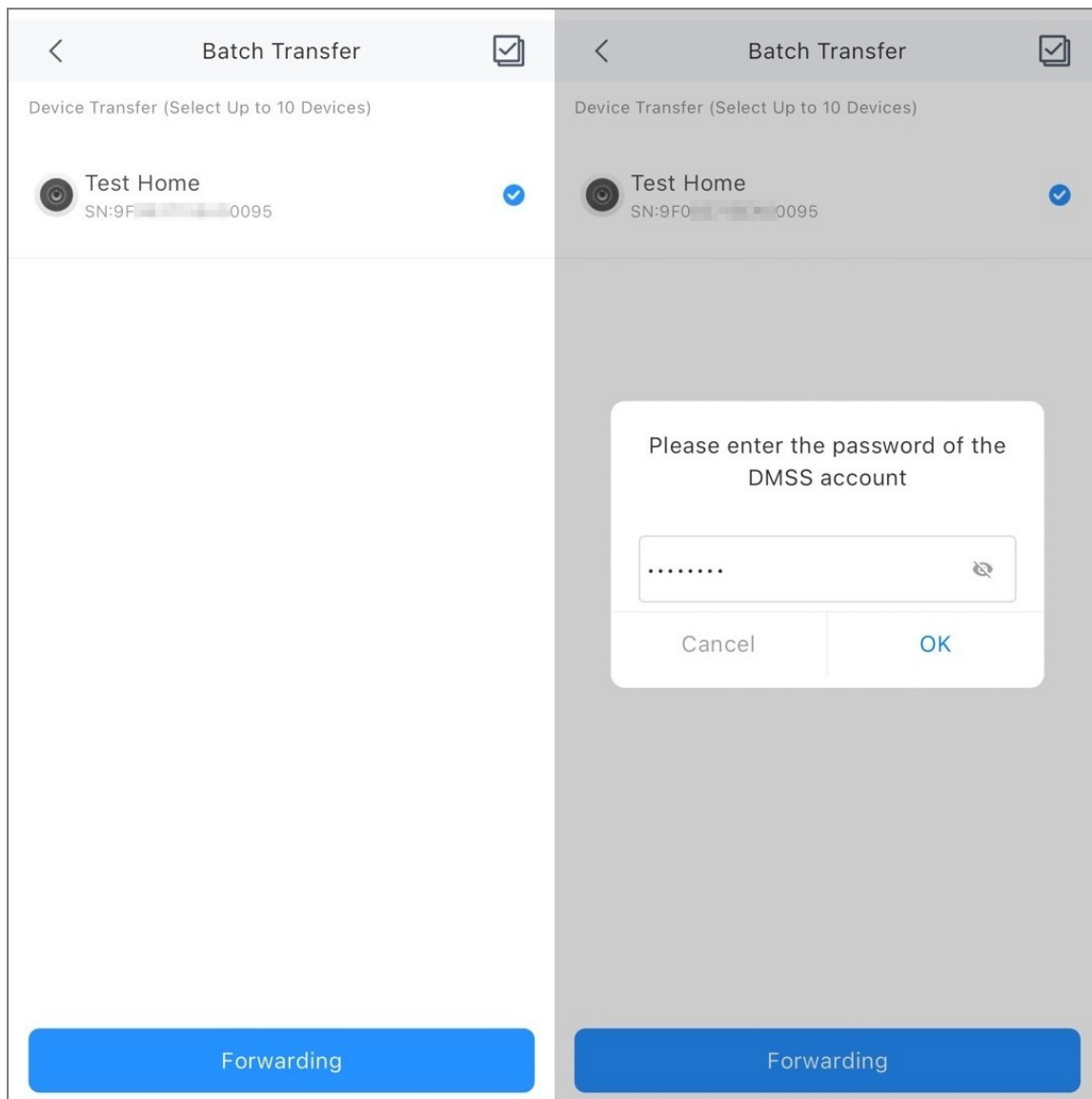
ステップ1 「私(マイページ)」>「サービス」をタップします。

ステップ2 「ローカルデバイスをアカウントに移行」をタップします。

ステップ3 デバイスリストから移行したいローカルデバイスを選択し、「転送(Forwarding)」をタップします。

ステップ6 システムがデバイスの移行を完了するのを待ち、「完了」をタップします。

図5-30 アカウントへのローカルデバイスの転送



結果

デバイスの移行が正常に完了すると、デバイスのステータスは「ローカルデバイス」から「アカウント配下のデバイス」に変更されます。

5.8 デバイスパスワードのリセットおよび変更

デバイスのパスワードを変更するには、「●●●」>デバイス詳細>デバイス情報>パスワード変更に進んでください。パスワードを忘れた場合は、「私(マイページ)>ツール>デバイスパスワードをリセット」からリセットできます。

これら2つの手順はほぼ同じ流れとなっており、このセクションでは「デバイスパスワードのリセット」を例として説明します。

手順

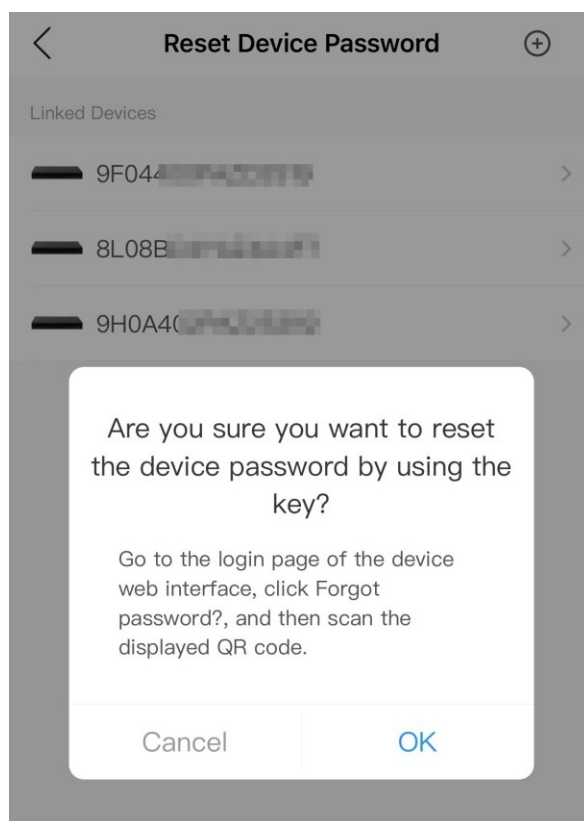
ステップ1 「私(マイページ)」画面で、「ツール」をタップします。

ステップ2 「デバイスパスワードをリセット」をタップします。

ステップ3 「デバイスパスワードをリセット」画面で、パスワードをリセットしたいデバイスをタップし、画面上の案内(プロンプト)を確認します。

ステップ4 「OK」をタップします。

図5-31 デバイスパスワードのリセット



6 ライブビュー

各チャンネルのライブ映像を閲覧することができ、スナップショットの撮影、録画、チャンネルのお気に入り追加などの操作を行うことができます。

手順

ステップ1 デバイス画面で、「 ライブビデオ」をタップします。

ステップ2 チャンネルまたは複数チャンネルの再生

- システムは、前回プレビューしたチャンネルのライブ映像をデフォルトで再生します。
- 他のチャンネルを再生するには、「」をタップし、デバイスリストから再生したいチャンネルを選択します。
※複数のチャンネルを同時に選択・再生することも可能です。。



表示されるチャンネル数が利用可能なウィンドウ数を超える場合、左右にスワイプすることで、他のライブ映像を閲覧できます。

ステップ3 ライブ映像を表示し、各種操作を実行します。

図6-1 ライブビュー

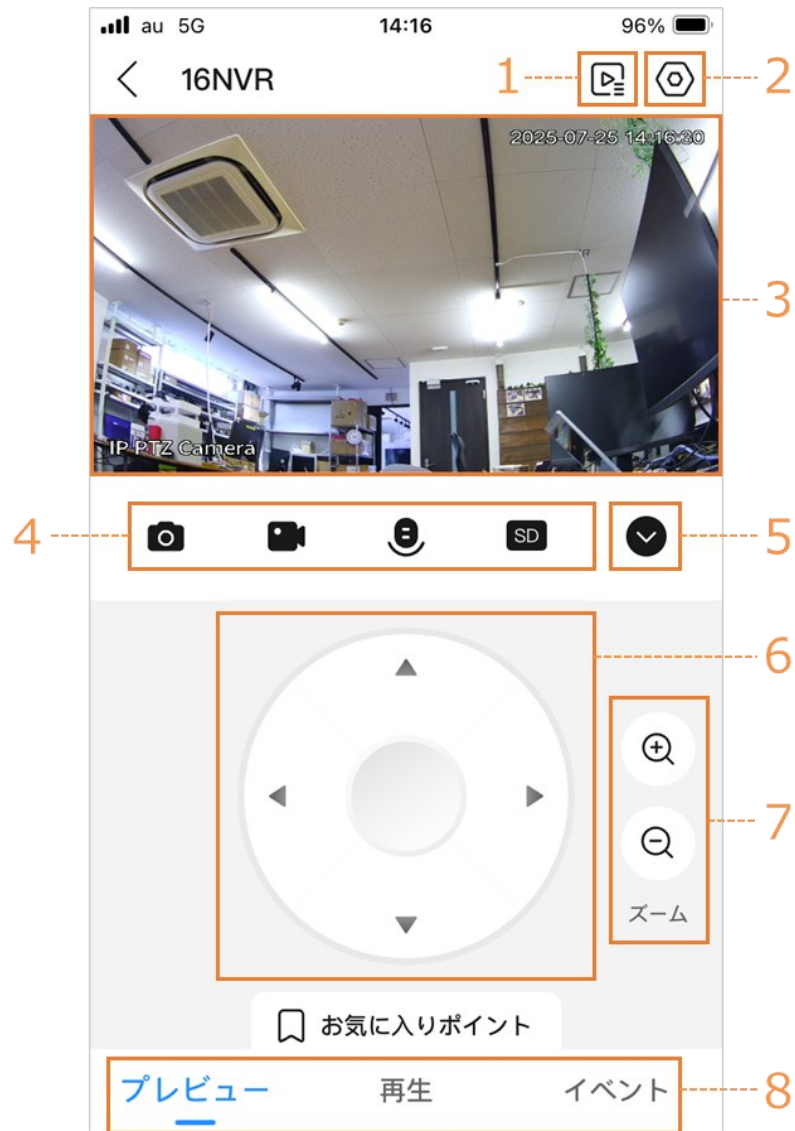


表6-1 ライブビュー機能アイコンの説明

番号	アイコン/機能	説明
1		ライブ映像を表示したいチャンネルを選択します。
2		デバイスの詳細 「デバイス詳細」画面に移動することで、デバイスの設定を行うことができます。 詳細については、「5.1 デバイスの設定」を参照してください。 (Link)

番号	アイコン/機能	説明
3	ライブビュー	- ビデオの位置を変更するには、ビデオを長押しして、目的のウィンドウにドラッグします。 - ウィンドウを拡大するには、ビデオをダブルタップします。元のサイズに戻すには、再度ダブルタップします。 - ビデオを削除するには、ビデオを長押しし、画面上部にゴミ箱アイコンが表示されたら、ビデオをゴミ箱にドラッグして指を離します。 - ビデオが正常に再生されない場合は、ウィンドウ内の「ヘルプ」をタップして、問題解決のための対処方法を確認してください。 - ライブ映像をタップすると、ツールバーが表示されます。   : 音声の有効化／無効化  : 魚眼(フィッシュアイ) ビデオを選択し、 をタップしてから、「 魚眼を有効にする」をタップします。画面上をスワイプして、映像表示の効果を調整します。  この機能は、一部のモデルでのみ利用可能です。  : 分割表示。1画面、4画面、9画面、または16画面で映像を表示することができます。 1つのウィンドウにフォーカスするには、対象のウィンドウ内のビデオをダブルタップしてズームインします。  : 画像の向きを横向きに変更します。
4	    	ビデオストリーム。アイコンをタップすることで、SD(標準画質)とHD(高画質)を切り替えることができます。 スナップショットを撮影する  「私(マイページ)>設定」でキャプチャモードを設定できます。詳細は「13 私(マイページ)」を参照してください。(Link) - 撮影したスナップショットは「アルバム」に保存されます。詳細についても「13 私(マイページ)」を参照してください。(Link) ビデオ録画  録画した動画はアルバムに保存されます。詳しくは「13 私(マイページ)」を参照してください。(Link) 双方向音声 - チャンネルトーク:再生中のチャンネルを通じて相手と会話します。 - デバイストーク:デバイス本体を通じて相手と会話します。  - 双方向音声機能は、一部のモデルでのみ利用可能です。 - デバイストークが対応している場合、システムが「チャンネルトーク」と「デバイストーク」のどちらを使用するか選択するように案内します。対応していない場合は、「チャンネルトーク」のみが利用可能です。

番号	アイコン/機能	説明
		画像の向きを横向きに変更します。
5		 アイコンをタップして、詳細を表示します。 •  : プリセットポイントを選択し、「OK」をタップすると、PTZカメラが指定の監視対象に向きます。 •  : ワイパー操作。時刻を選択して、以下の操作を行います。 *「1回実行」をタップすると、ワイパーが1回作動して停止します。 *「有効化(Enable)」をタップすると、ワイパーが一定の時間間隔で作動するように設定できます。 *「停止」をタップすると、ワイパーの動作が停止します。  この機能は、一部のモデルでのみ利用可能です。 •  : 映像を拡大または縮小します。 •  : ビデオの明るさを調整します。
6		PTZ 操作 PTZカメラの方向を操作できます。左、右、上、下、左上、右上、左下、右下のすべてに対応しています。  • ジェスチャー操作にも対応しています。 画面をスワイプしてPTZの方向を操作し、指をピンチイン／ピンチアウトすることでズームイン・ズームアウトができます。 • PTZ操作中は1つのウィンドウのみが表示されます • PTZ機能は、一部の対応モデルでのみ利用可能です。
7		画像をズームイン(拡大)またはズームアウト(縮小)します。
8	メニューバー	• プレビュー：ライブ映像の画面です。 • 再生：録画映像の再生画面です。再生画面での操作方法については、「7 録画映像の再生」を参照してください。(Link) • イベント：アラームメッセージを表示します。日付を選択すると、その日時のイベント映像を確認できます。



機能はデバイスの種類によって異なる場合があります。実際のインターフェースをご確認ください。

7 ビデオ再生

時間、ビデオタイプ、およびチャンネルに基づいて録画を検索して再生できます。

前提条件

録画を再生する前に、チャンネルに対してアラームルールおよび録画計画を設定する必要があります。

手順

ステップ1 デバイス画面で、下部の「再生」をタップします。

ステップ2 デフォルトで最新の録画が再生されます。

図7-1 ビデオ再生

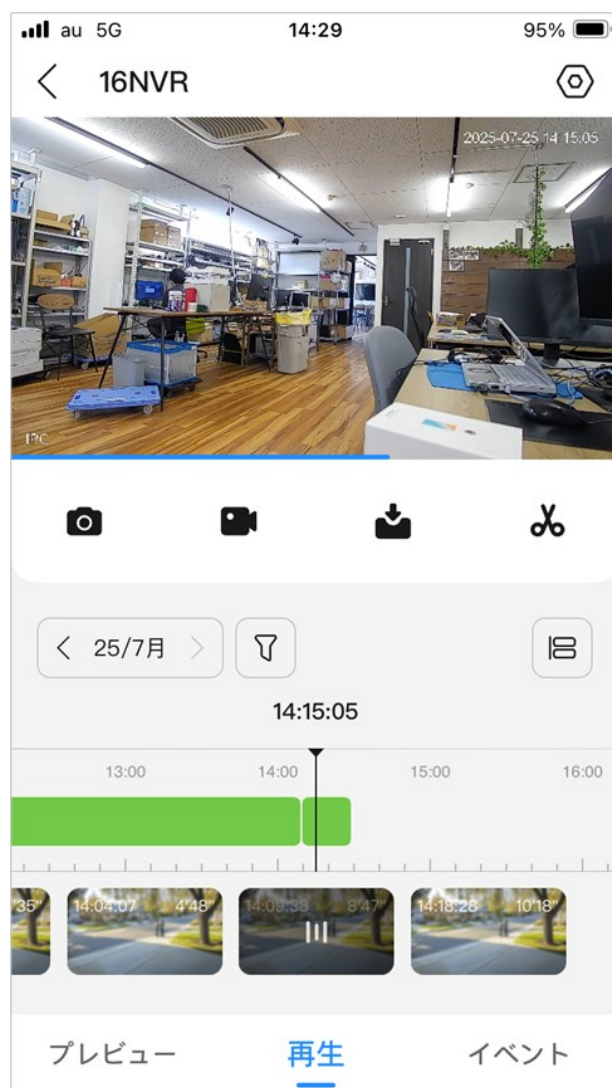


表7-1 ビデオ再生機能アイコン

機能	説明
	この機能はライブ映像と同じです。 アイコンの詳細については、表6-1 を参照してください。 (Link)

機能	説明
	
	
	
	
	
	アイコンをタップして、再生速度を選択します。
	ビデオを10秒巻き戻す、または早送りすることができます。
	ビデオをクリップします。
	録画をダウンロードします。 ダウンロードしたファイルは、「私(マイページ)」>「アルバム」>「録画」で確認できます。
	ビデオクリップを表示します。
タイムバー	カラーブロックは、さまざまな種類の録画ビデオを示しています。 - グレー：すべてのビデオ - 緑：通常のビデオ - 赤：アラームビデオ - オレンジ：動体検知ビデオ - 黄色：スマートビデオ タイムバーをドラッグして、さまざまな時間帯に対応する録画を表示します。 指をつまんだり広げたりして、タイムバーをズームイン／ズームアウトできます。

ステップ3  02-24  タップして、日付と録画タイプを変更します。

録画タイプは以下のとおりです：

- すべて：すべての録音タイプを再生します。
- 通常：通常の録画です。
- アラーム：音声アラームやローカルアラームなど、アラームが発生した際の録画です。
- 動体検知：動体検知アラームがトリガーされた際の録画です。
- スマート：顔検出・認識、IVS、ビデオメタデータなどのスマートイベントアラームがトリガーされた際の録画です。
- 動体検知：車両：車両が検出され、動体検知アラームがトリガーされた際の録画です。
- 動体検知：人物：人が検出され、動体検知アラームがトリガーされた際の録画です。

関連操作

「プレビュー(Preview)」をタップすると、ライブビュー画面に戻ることができます。

詳細については、「6 ライブビュー(Live View)」を参照してください。[\(Link\)](#)

8 ビデオ通話

ライブビューの視聴、ビデオインターホンへのアクセス、デバイスとアプリ間でのビデオ通話、ドアの施錠・解錠などが可能です。ここではVTO(ビデオドアホン)を例に説明します。

手順

ステップ1 デバイス画面で、VTO をタップします。

ステップ2 「プレビュー」をタップして、VTOのライブ映像ページに移動します。

下部の「再生」または「イベント」をタップすると、それぞれのモジュールに移動できます。

図8-1 VTO

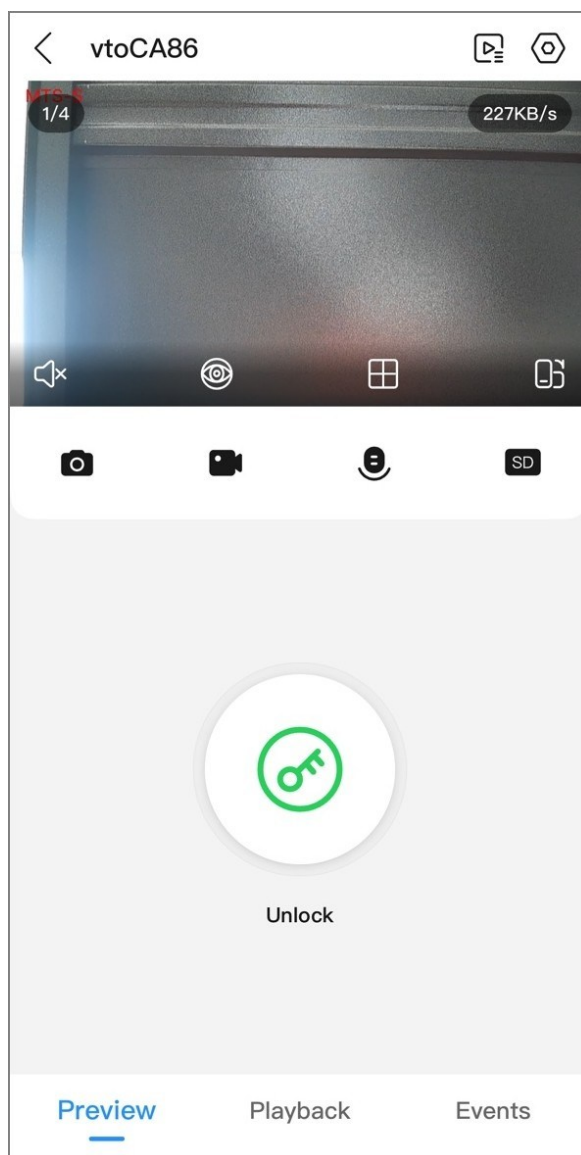


表8-1 TVコール機能のアイコン

機能	説明
	アイコンの詳細については、表6-1 を参照してください。(Link)

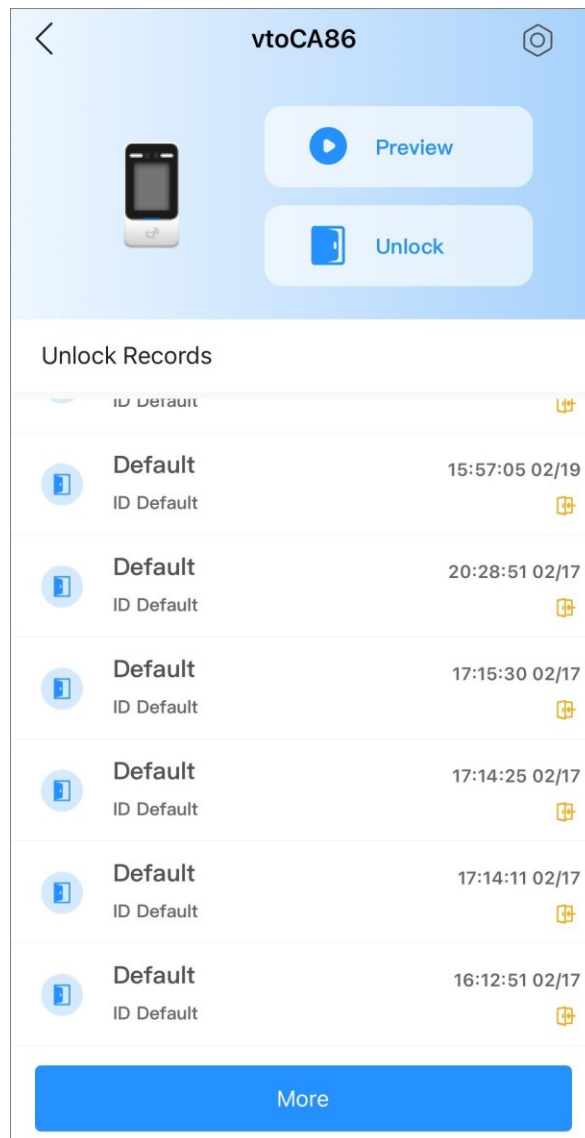
機能	説明
       	
 	通話の応答／終了。 アプリでVTOからの通話を受信：  タップして通話に応答、または  タップして通話を拒否／終了します。  VTOからDMSSで通話を受けるには、VTOのアラームサブスクリプションを有効にしてください。
	ドアを解錠します。  2つのロックを備えたVTOは、DMSSに追加することができます。 「」をタップし、解錠したいドアを選択します。 

関連操作

VTOデバイス画面では、以下の操作が可能です：

- **解錠**：[解錠]をタップしてドアを解錠します。
- **解錠履歴**：解錠の履歴を表示します。[その他]をタップし、日付を選択すると、さらに多くの履歴を確認できます。

図8-2 その他の操作



9 アクセスコントロール

ドアの状態の確認、解錠履歴の表示、遠隔でのドアの解錠、アクセスコントロール機器のライブ映像の視聴などが可能です。
デバイス画面で、アクセスコントロール機器をタップします。

図9-1 アクセスコントロール機器

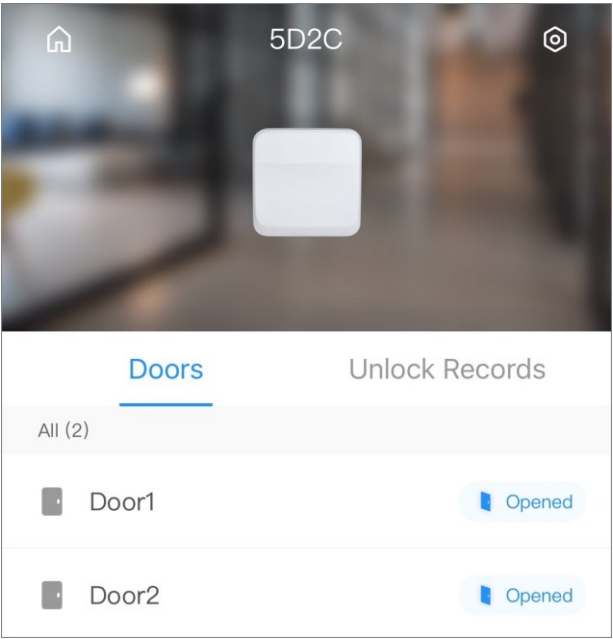


表9-1 機能アイコンの説明

機能	説明
デバイス詳細	🔍 タップして「デバイス詳細」画面に移動します。 📖 また、ホーム画面でアクセスコントロール機器の「」をタップし、その後「デバイス詳細」をタップすることもできます。
解錠	 Opened タップしてドアを解錠します。

機能	説明
解錠履歴	「解錠履歴」をタップすると、システムは氏名、ID、解錠時間、および解錠方法を表示します。各アイコンの意味は以下の通りです。  : アプリを使用して遠隔で解錠  : カードによる解錠  : 指紋による解錠  : パスワードによる解錠  : 鍵による解錠  : 顔認証による解錠  : 脅迫下での解錠(デュレス解錠)   : 複数の解錠方法の組み合わせによる解錠。  : グループの組み合わせによる解錠  : 解錠失敗

10 アラーム操作

アラームハブおよび周辺機器の管理を行います。ログの表示および送信にも対応しています。ホーム画面でアラームハブデバイスをタップすると、デフォルトで操作画面が表示されます。下部の「デバイス(Device)」をタップすると、アラームハブのデバイス画面に移動します。

図10-1 アラームハブデバイス画面

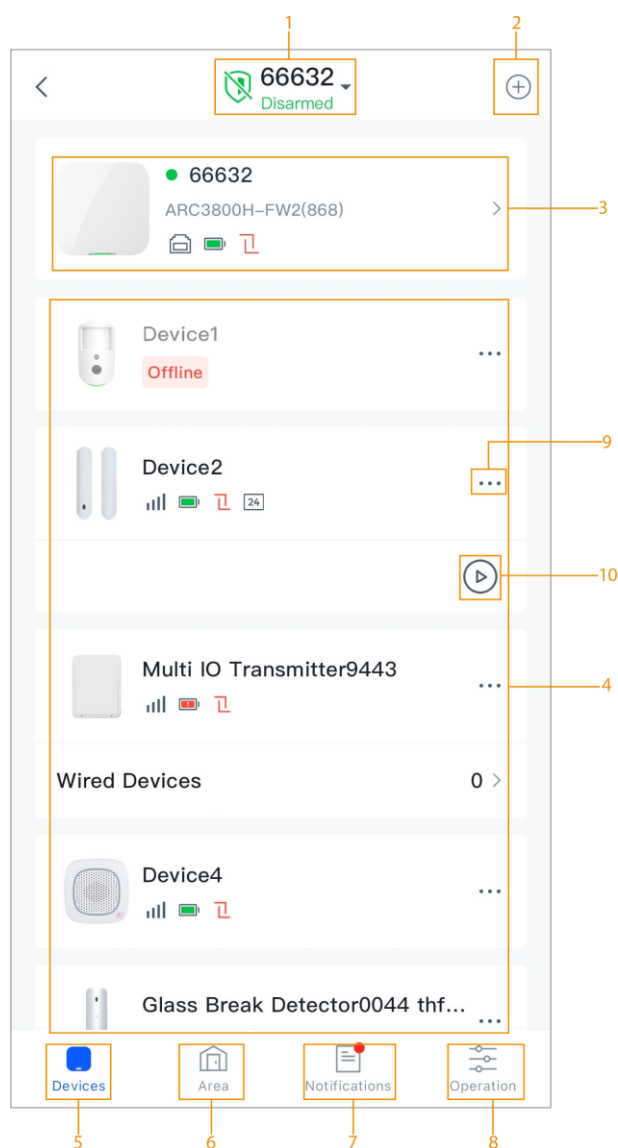


表10-1 アラームハブホーム画面の紹介

番号	名前	説明
1	アラームハブデバイス	異なるアラームハブを選択し、それぞれのデバイスのホームページに移動することができます。
2	デバイスを追加	アラームハブにデバイスを追加することができます。詳細については、「5.7 ローカルデバイスのアカウントへの移行」を参照してください。 (Link)

番号	名前	説明
3	アラームハブ情報	デバイスの情報(名称、モデル、警戒／解除状態、信号およびバッテリーの状態)を確認できます。 デバイスをタップすると、デバイスの詳細ページに移動します。
4	周辺機器リスト	アラームハブに追加された周辺機器が表示されます。 周辺機器の状態やデバイス情報を確認できます。 また、周辺機器の管理および設定にも対応しています。
5	デバイスタブ	デバイスのホーム画面です。
6	エリア	部屋の一覧ページです。部屋の管理、警戒／解除の操作、およびその部屋にある周辺機器リストの確認が可能です。 詳細については、「10.5 エリア管理」を参照してください。 (Link)
7	通知	アラームハブのメッセージセンターです。 アラームハブに関するメッセージを確認できます。メッセージには、アラーム、警戒／解除、操作、エラーに関する内容が含まれます。
8	操作	アラームハブの操作画面です。 - 解除中の部屋が表示されます。部屋をタップすると、そのエリアを警戒状態に切り替えることができます。 「」または「」をタップして、アラームハブを警戒／解除することができます。  システム整合性チェック機能が有効になっている場合、アラームハブがAPモードのときは正常に警戒状態にすることができません。システムは例外を通知し、「強制的に警戒」を選択することができます。 APモード中は、キーフォブやキーパッドによる警戒操作も無効になります。 - 緊急時には「」をタップして緊急アラームを発報できます。メッセージはメッセージセンターに送信されます
9	周辺機器の詳細	周辺機器の管理、設定、または移動を行うことができます。
10	ライブビュー	周辺機器に対してアラーム連動ビデオチャンネルの機能を有効にした後、アイコンをタップすると、そのチャンネルのライブ映像を表示できます。 ただし、IPC(ネットワークカメラ)があなたのアカウントに登録されている必要があります。登録されていない場合は、まずIPCをアカウントに追加してください。

10.1 デバイスサービス

アラームハブに対して、デバイスの共有、委託、権限設定、セキュリティサービスの申請を行うことができます。
詳細は「5 基本操作」を参照してください。[\(Link\)](#)

10.2 ファームウェアアップデート

デバイスのファームウェアを一括でアップデートすることができます。操作方法は、デバイスモードでのファームウェア更新と同様です。詳細は「5.1.3.4 クラウドアップデート」を参照してください。[\(Link\)](#)

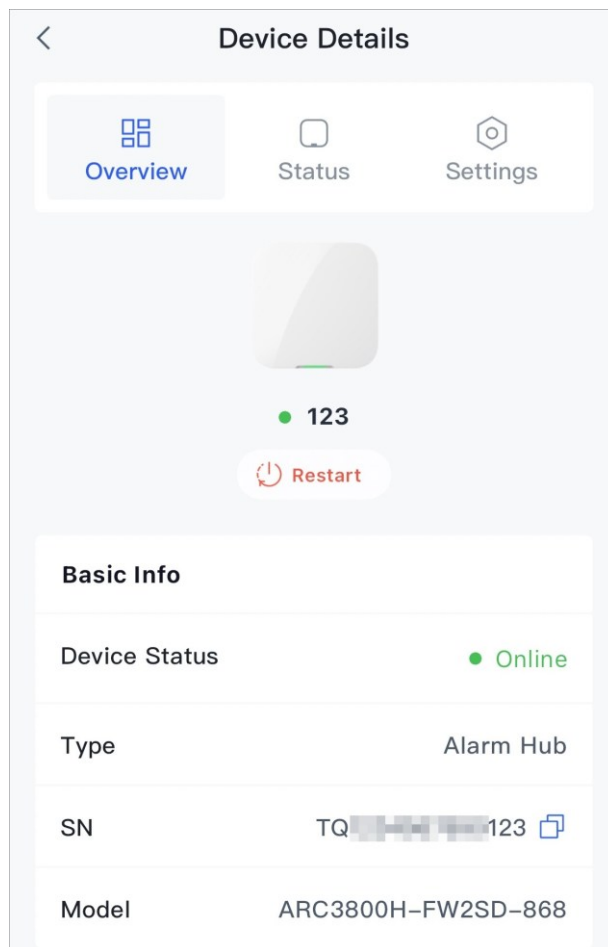
10.3 アラームハブ

10.3.1 デバイス概要

アラームハブをタップすると、デバイスの詳細ページに移動します。初期表示はデバイス概要ページです。

- 基本情報: デバイスのモデル名やシリアル番号(SN)など、基本的な情報を確認できます。
- ハブ情報: 警備会社、委託期間、貸出期間など、アラームハブに関する情報を確認できます。
- デバイスの再起動: [🔄] をタップします

図10-2 アラームハブのデバイス情報



10.3.2 ステータスの確認

アラームハブをタップし、次に「ステータス」をタップすると、デバイスの状態を確認できます。

表10-2 ステータスの説明

パラメータ	説明
LTE 信号強度	アクティブなSIMカードにおけるモバイルネットワークの信号強度を示します。 •  : 極めて弱い •  : 弱い •  : 中程度 •  : 強い •  : なし
Wi-Fi 信号強度	Wi-Fi経由でのハブのインターネット接続ステータス。より高い信頼性を得るために、信号強度が少なくとも2bar 以上の場所にハブを取り付けることをお勧めします。 •  : 極めて弱い •  : 弱い •  : 中程度 •  : 強い •  : 接続なし
バッテリー残量	バッテリーの残り電力を表示します。
タンパー	アクセサリーのタンパーモードで、本体の取り外しに反応します。
外部電源	外部電源の接続状態を表示します。
LTE	SIMカード、Wi-Fi、Wi-Fiイーサネットによるハブのインターネット接続状況を表示します。
Wi-Fi	
イーサネット	
SIM カード	SIMカードの接続状態を表示します。
プログラムバージョン	ハブのプログラムバージョンを表示します。

10.4 アラームハブの設定

本プラットフォームは、アラームハブ1.0およびアラームハブ2.0の両方に対応しています。対応するデバイスによって、表示される項目や設定可能な項目が若干異なる場合があります。正確な情報については、実際のインターフェースをご確認ください。

手順

ステップ1 アラームハブをタップして、デバイスの詳細画面に移動します。

ステップ2 「設定」をタップします。

表10-3 パラメーターの説明

パラメーター	説明
デバイス	「デバイス」をタップして、デバイス名の変更およびデバイスのパスワード変更を行います。

パラメーター	説明
ハブ設定	アラームハブの設定画面に移動します。 詳細は「10.4.1 ハブ設定」を参照してください。 (Link)
貸出期間/貸出中	ステータスが「貸出中」のデバイスについては、ここで貸出期間を確認できます。
ネットワーク	デバイスのネットワークを設定します。詳細は「10.4.3 ネットワーク設定」を参照してください。 (Link)
タイムゾーン	- デバイスに適用するタイムゾーンを選択します。  /  をタップして夏時間(DST)を有効／無効にします。
デバイス共有	ステータスが「貸出予定」のデバイスについては、「デバイスの共有」をタップして貸し出すことができます。
言語	アラームハブの言語を選択します。 アラームハブから送信されるメッセージの言語も含まれます。
ユーザーマニュアル	アラームハブデバイスおよび周辺機器のユーザーマニュアルを表示します。
ファームウェアアップデート	最新バージョンがあるかどうかを確認し、利用可能な場合はデバイスを最新バージョンにアップデートできます。
ログの表示	デバイスログ、アプリログ、リモートログを表示できます。  タップすることで、ログを自分のメールアドレスに送信することも可能です。
ログの収集	 タップしてこの機能を有効にします。 収集時間や収集レベルの設定が可能です。収集されたリモートログの閲覧も行えます。
警備会社	デバイスが警備会社に紐付けられている場合、その警備会社の情報を確認できます。
削除	タップしてアラームハブを削除します。

10.4.1 ハブ設定

アラームハブをタップし、設定＞ ハブ設定を選択します。

図10-3 ハブ設定

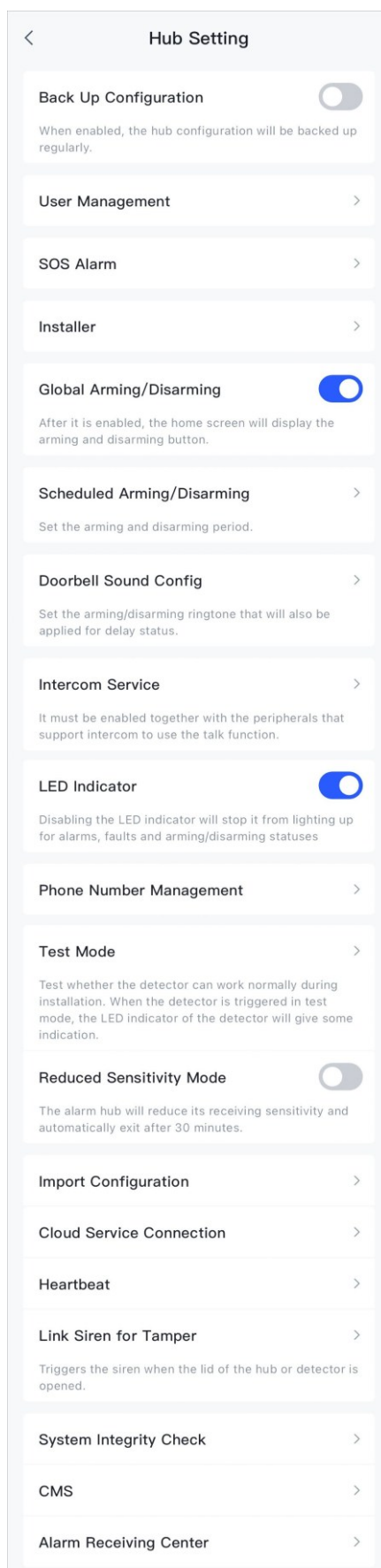


表10-4 ハブ設定のパラメータ説明

パラメーター	説明
設定のバックアップ	 /  をタップして、この機能を有効または無効にします。 有効にすると、アラームハブの設定がバックアップされ、定期的にクラウドプラットフォームへアップロードされます。
ユーザー管理	アラームハブが解除状態のときに、キーパッドユーザーの追加・編集・削除が可能です。 - アプリユーザー: DMSSアプリのユーザーおよび共有ユーザーが表示されます。アプリユーザーをタップすると権限の設定が可能です。設定できる権限は以下の通りです: - 警戒/解除操作、SOSボタンの操作、周辺機器(リレー、ウォールスイッチ、スマートプラグ)のスイッチ制御、バイパス操作、スナップショット撮影、アラームビデオの確認 また、通知の受信権限も設定できます。通知が無効になっている場合、該当する通知はそのユーザーには送信されません。 - キーパッドユーザー: 「追加」をタップしてユーザーを追加します。 ユーザー名、パスコード、デュレスコード(任意)を入力し、部屋ごとに警戒/解除の権限を設定します。  ◇ パスコードおよびデュレスコードは4～6桁の数字。 ◇ 最大で32人のユーザーを作成可能です。 ◇ 最初に作成されたユーザーは管理者(admin)となり、すべての権限を持ちます。 - キーパッドユーザーの削除:  をタップし、「削除」を選択します。  管理者(admin)ユーザーは、最後に削除する必要があります。 - キーパッドのユーザー情報の編集: 編集したいユーザーをタップし、「詳細」を選択します。ユーザー情報ページでは、以下の項目を編集できます。 ユーザー名、パスコード、デュレスコード、警戒/解除の権限。
カード管理	- カードの追加: ユーザー情報ページの右上にある  アイコンをタップして、ユーザーにカードを追加します。キーパッドのいずれかのキーを押して起動し、30秒以内にカードをキーパッドのカードリーダー部分にかざして、リンク処理を行います。 カード情報が正しく認識されると、カードIDがユーザー情報ページに表示され、キーパッドが1回ビープ音を鳴らします。 設定を保存すると、そのカードにはユーザーの権限が付与されます。  1人のユーザーに対して最大8枚までのカードをリンクできます。 - カードの削除: 削除したいカードを選択し、左にスワイプして削除します。
SOSアラーム	SOSアラームを有効/無効に設定でき、アラームをサイレンに連動させることも可能です。 アラームの種類には、SOS アラーム、医療アラーム、火災アラームがあります。
グローバル警戒/解除	 /  をタップして、ハブのホーム画面に表示される警戒/解除ボタンの表示を有効/無効に切り替えます。 

パラメーター	説明
スケジュール警戒/ 解除	エリアごとにスケジュールで警戒・解除を行うことができます。 「追加」をタップして、新しいスケジュールを登録します。 - 名前: スケジュールの名称を入力します。 - エリア: ハブが動作する対象のエリアを選択します。 - コマンド設定: 「在宅」「外出」「解除」のいずれかのモードをタップして選択します。 - 時刻: ハブが動作する時間帯を設定します。 - 繰り返し: 設定した警戒または解除のスケジュールを繰り返します。 - 強制警戒: この機能を有効にすると、スケジュールによる警戒／解除コマンドは無効になります。 ➤ システム整合性チェックが有効で、この機能が無効になっている場合、エリアに異常があると警戒に失敗します。 ◇ ➤ この機能を有効にすれば、エリアに異常があっても強制的に警戒を実行できます。 ◇ 📖 スケジュール警戒／解除は最大8件まで追加可能です。 登録済みのスケジュールを削除するには、左にスワイプし「削除」をタップします。
ドアベル音設定	- アラームハブ1.0の場合: 警戒モードへの移行時／解除時の着信音を有効／無効に設定できます。 - アラームハブ2.0 の場合:着信音の各種パラメータを設定できます。 ◇ 着信音の音量を設定 ◇ アラーム音およびダンパー音の通知を有効／無効に設定 ◇ アラームの通知回数を設定 ◇ 警戒／解除の入退時音通知の有効／無効を設定 入退時の警戒／解除遅延機能が有効な場合、その音声通知の有効／無効も設定可能
インターホンサービス	詳細については、「10.4.2 インターホンサービス」を参照してください。 (Link)
LED インジケーター	アラームハブのインジケーターライトの有効／無効を設定します。 有効にすると、アラーム、異常、警戒／解除の状態に応じてLEDインジケーターが点灯します。

パラメーター	説明
電話番号管理	「追加」をタップして、イベント通知を受信する電話番号を登録します。その後、SMSを送信するイベントタイプを選択します。 対応するイベントタイプは以下のとおりです：アラーム、障害、操作、アラームが電話と連動しているかどうか ※電話番号は最大12件まで追加可能です。 追加後は、登録済みの電話番号の右側にある「」アイコンをタップして、以下の操作が可能です： SMSテスト、通話テスト→現在の電話番号が有効かどうかを確認できます。 また、「削除」をタップして電話番号を削除することもできます。 登録済みの電話番号をタップすると編集画面が表示され、番号の編集やSMS通知対象イベントの変更が行えます。  この機能は2G/4G対応デバイスのみで利用可能です。
テストモード	部屋ごとに周辺機器のテストを行うことができます。 部屋を選択して「開始」をタップすると、各エリアでハブに接続されている周辺機器の状態をテストします。 テストが完了したら「停止」をタップしてください。
感度低減モード	この機能を有効にするには  タップしてください。ハブの送信出力が低下します。
構成のインポート	旧型のアラームハブから構成データをインポートすることができます。 1. 「アラームハブを選択」をタップして、構成をインポートしたいデバイスを選択します。 2. 画面上の指示を読み、「開始」をタップして処理を開始します。  現在のアラームハブのプログラムバージョンが、構成データをインポートする元のアラームハブよりも古い場合、インポートは成功しません。まずプログラムバージョンをアップグレードする必要があります。
クラウドサービス接続	サーバーとハブ間のping間隔を150～900秒の範囲で設定できます(初期値は300秒)。 D-cloudがハブのオフライン状態が300秒を超えていることを検出すると、アプリを通じてユーザーにハブのステータスを通知します。

パラメーター	説明
ハートビート	ハブと検出器(周辺機器)とのping間隔を設定します。この設定により、ハブが周辺機器とどのくらいの頻度で通信するか、および接続が失われた場合にどれだけ早く検出されるかが決まります。 - 検出器のPing間隔：ハブが制御する周辺機器との通信頻度を設定します。設定範囲は12秒～300秒で、初期値は60秒です。  ※Ping間隔が短いほどバッテリー寿命は短くなります。 - パケット損失回数:未配信パケットのカウント数を設定します。設定範囲は3回～60回で、初期値は15回です。  値が小さいほど、周辺機器のオフライン状態がより頻繁に検出・報告されます。 ◇ ハブが周辺機器との接続を継続的に失い、設定されたハートビートを検出できない場合、その周辺機器のオフライン状態がシステムに報告されます。
タンパー用サイレン連動	- 警戒状態の場合:この機能を有効にすると、ハブはアラーム音と連動します。  ハブや周辺機器のカバーが開けられた際に、サイレンが警告音を鳴らします。 - 常時有効の場合: この機能を  タップして有効にすることができます。有効にすると、警戒状態か解除状態かに関係なく、常にサイレンが連動します。
システム整合性チェック	この機能を有効にすると、ハブは警戒前にすべての検出器の状態を確認します。確認内容には、バッテリー残量、タンパー(不正開封)検知、接続状況などが含まれます。エラーが検出されると警告が表示されます。システムがチェックし通知するエラーの種類を選択することができます。  - 主電源障害検知を有効にすると、すべてのシステムデバイスが関連出力を作動させるまでの遅延時間を設定できます。 - キーフォブの場合:インジケータが緑に点滅し、その後赤に変わります。 - アプリの場合:アラームメッセージがポップアップ表示されます。 - キーパッドの場合:1秒間ビーブ音が鳴り、警戒・解除インジケータが2秒間緑に点滅し、その後通常状態に戻ります。
CMS	 タップして機能を有効にすると、ハブをコンバーターに登録できるようになります。  この機能は、DMSSアプリのバージョンが 1.96以降、かつハブのバージョンが V1.001.0000000.6.R.211215以降 の場合にのみ使用可能です。

アラーム受信センター	- アラームハブ1.0 の場合、 をタップして機能を有効にし、アラーム受信センター（ARC）向けのSIAプロトコルパラメータを設定します。 IPアドレス:ARCのIPアドレスとポート番号を入力します。代替IPアドレス:ARCの代替IPアドレスとポート番号を入力します。   - 優先IPアドレスでメッセージの受信に失敗した場合のみ、代替IPアドレスにメッセージが送信されます。 「ハートビート間隔」が有効な場合、システムが優先IPか代替IPへ送信するかを判断します。 IPプロトコル:デフォルトはTCPです。 ハートビート間隔:0秒～24時間の範囲で設定できます(初期値は60秒)。   0秒に設定すると、ハートビート送信は無効になります。 中央アカウント:ARCで作成されたアカウント番号を入力します。ハブがARCに情報を送信する際の識別に使用されます。 暗号化:ARCを構成する際に情報のセキュリティを確保するため、暗号化形式を使用します(初期設定はAES128)。 イベントのアップロード:各イベント横のボタンをタップしてアップロードを有効にします。 - アラーム:アラーム通知。 - エラー:停電、バッテリー低下、タンパー、オフラインなど。 - イベント:周辺機器の使用禁止、追加・削除、ユーザーの追加・削除。 - 警戒/解除:システムの警戒・解除の通知。 - アラームハブ 2.0 の場合: 2つのアラーム受信センターの設定に対応しています。 任意の受信センターを選択し、有効化を  タップしてください。パラメータの設定内容はアラームハブ 1.0 と同様です。
通知	受信したいメッセージの種類をタップして選択してください。

10.4.2 インターホンサービス

インターホンサービスを有効にして設定することができます。設定が完了すると、アラームがトリガーされた際に、インターホンサービスに対応したデバイスと通話が可能になります。



インターホンサービスを使用するには、対応するデバイス側でもインターホンサービスを有効にしておく必要があります。

手順

ステップ1 アラームハブをタップし、「設定」をタップします。

ステップ2 「ハブ設定」>「インターホンサービス」をタップします。

ステップ3 タップ  し、機能を有効にします。

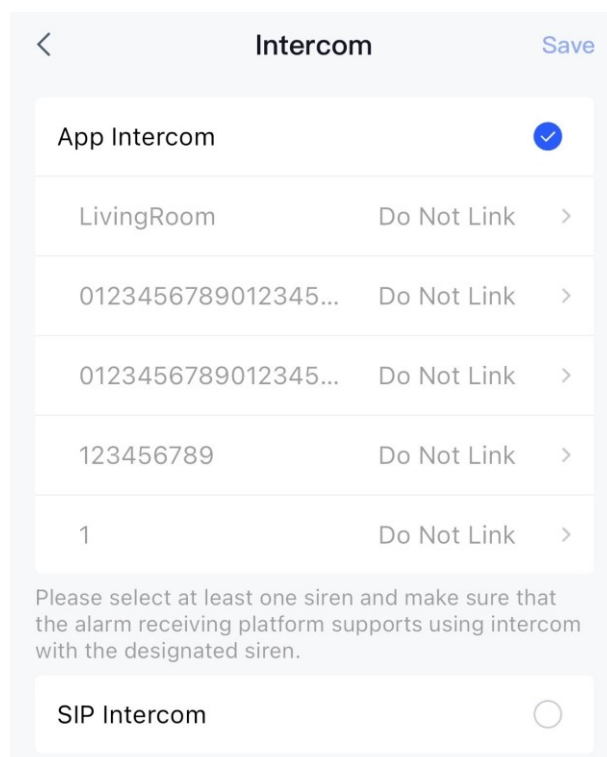
ステップ4 インターホンの有効時間を選択します(初期設定は10分)。

インターホンの有効時間とは、アラームがトリガーされた瞬間から始まる時間制限のことです。
設定されたインターホン時間内であれば、該当するアラームのデバイスとインターホンを開始することができます。
ただし、この時間を超えるとインターホンは利用できなくなります。

ステップ5 インターホンモードを選択し、各パラメータを設定します。

- Appインターホンを選択：スマートフォンにインストールされた **DoLink Care**アプリ または **DMSS**アプリ を使用して、インターホンサービスに対応した周辺機器と通話することができます。
部屋にリンクされたデバイスを選択し、「OK」をタップしてください。

図10-4 アプリインターコムサービスの設定



- SIPインターホンを選択：サードパーティープラットフォーム上でインターホンサービスに対応している周辺機器と、SIP(Session Initiation Protocol)を利用したインターホン通話を行うことができます。

図10-5 SIP インターコムサービスの設定

表10-5 SIP インターコムパラメータの導入

モード	パラメーター	説明
サイレンで選択	サイレン	ドロップダウンリストからインターホンサイレンを選択します。アラームハブに追加されたインターホンサイレンを選択することで、アラームがトリガーされた際にそのサイレンを通じて通話が可能になります。
	SIP サーバ設定	◇ SIPサーバーのユーザー名とパスワードを入力します(サーバー側と同じ内容にしてください)。 ◇ サーバーのIPアドレスとポート番号を入力します。 ◇ ローカルポート番号を入力します。登録状態はデバイスから返され、編集はできません。
ゾーンで選択	部屋名	部屋にリンクされたインターホンサイレンを選択します。サイレンの選択は「サイレンで選択」と同様です。
	サイレン	
	SIP サーバ設定	設定内容は「サイレンで選択」の場合と同じです。

ステップ6 「OK」をクリックします。

10.4.3 ネットワーク設定

アラームハブをタップし、「設定」>「ネットワーク」を選択します。

ハブのネットワークとして以下のいずれかを選択できます。

有線ネットワーク、無線ネットワーク（Wi-Fi）、セルラーネットワーク（モバイル通信）

10.4.3.1 イーサネット設定

手順

ステップ1 「ネットワーク」>「イーサネット」を選択します。

ステップ2 有線ネットワーク接続のパラメーターを設定します。

表10-6 有線ネットワークパラメーターの説明

パラメーター	説明
DHCP	ネットワーク内にDHCPサーバーが存在する場合、このオプションを有効にすると、ハブは自動的に動的IPアドレスを取得します。
IP アドレス	IPアドレス :手動でIP情報を設定する場合、ハブのIPアドレスを手動で入力します。
サブネットマスク	サブネットマスク :ネットワークの範囲を指定するための値を設定します。
ゲートウェイ	ゲートウェイ :デフォルトゲートウェイのIPアドレスを設定します。ネットワーク外部との通信に使用されます。
DNS	DNS :ドメイン名をIPアドレスに変換するためのプライマリDNSサーバーのアドレスを設定します。
DNS 2	DNS 2 :セカンダリDNSサーバーのアドレスを設定します(オプション)。
MACアドレス	MACアドレス :ハブの物理アドレスを表示または設定します。通常は自動的に割り当てられた値が使用されます。

10.4.3.2 Wi-Fi ネットワーク設定

手順

ステップ1 ネットワーク> Wi-Fi を選択します。

ステップ2 Wi-Fi機能を有効にします。周囲の利用可能なWi-Fiネットワークの一覧からネットワークを選択し、パスワードを入力して接続します。

10.4.3.3 セルラー設定

手順

ステップ1 「ネットワーク設定」>「セルラー」を選択します。

ステップ2 セルラーネットワークのパラメーターを設定します。

表10-7 セルラーパラメータの説明

パラメーター	説明
セルラー	「セルラー」の横にあるスイッチをタップして、この機能を有効にします。
優先順位	「優先」の横にあるスイッチをタップして、ネットワーク選択時にセルラー接続を優先するよう設定します。
SIM 1	- デュアルSIMに対応(シングルスタンバイ方式)。 - SIMカードを挿入することで、ハブはセルラーデータ通信が可能になり、アラーム通知のプッシュ送信が行えます。
SIM 2	
APN	APNは、キャリアのセルラーネットワークとインターネットとの間にあるゲートウェイへの接続をデバイスが設定するための名前です。正しいAPN設定により、ハブがセルラー通信経路でデータを送受信できるようになります。

パラメーター	説明
認証モード	セルラーネットワーク接続時の認証方式を設定します。
ユーザー名	セルラーネットワークの接続に使用するユーザー名を入力します。 セルラーネットワークの接続に使用するパスワードを入力します。
パスワード	
ダイヤル番号	ハブが接続時に発信するダイヤル番号を設定します。。
モバイルデータ使用量	現在のモバイルデータ通信の使用量を確認できます
統計のリセット	モバイルデータ使用量の統計をリセットし、カウントを再スタートします。

10.5 エリア管理

部屋(ルーム)の追加、編集、削除を行うことができます。また、各部屋に対して警戒モード(アーミングモード)を設定することが可能です。

さらに、各エリア(部屋)に周辺機器(ペリフェラル)を追加することもできます。

手順

ステップ1 アラームハブをタップします。

ステップ2 画面下部の「エリア」タブをタップします。

-  「追加」をタップし、エリア名を入力します。画像をアップロードするか、選択して「OK」をタップします。
- 追加したエリアをタップすると、そのエリアの周辺機器管理ページに入ります。周辺機器を選択し、その横のアイコンをタップしてください。
 - ◇ 「デバイス詳細」を選択すると、周辺機器の情報を確認および設定できます。
 - ◇ 他のエリアに移動を選択すると、その周辺機器を他の追加済みエリアや新しく作成した部屋に移動できます。
 - ◇ 削除を選択すると、その周辺機器を削除します。
- エリア名の横にあるアイコンをタップすると、新しい周辺機器の追加、エリア情報の編集、またはエリアの削除が可能です。
- エリアごとの警戒モード(アーミングモード)も設定できます。エリアの横にあるアイコンをタップし、希望のモードを選択してください。



システム整合性チェック機能が有効な場合、アラームハブが **APモード** のときは警戒モード(アーミング)を正常に設定することができません。

また、キーフォブやキーパッドを使用しても、APモード中は警戒状態にすることはできません。

10.6 周辺機器管理

周辺機器を追加したり、周辺機器の情報を確認・設定することができます。

手順

ステップ1 サイトを選択します。

ステップ2 アラームハブをタップすると、アラームハブのホーム画面に移動します。

- 周辺機器をタップすると、その情報を確認したり、設定を行うことができます。



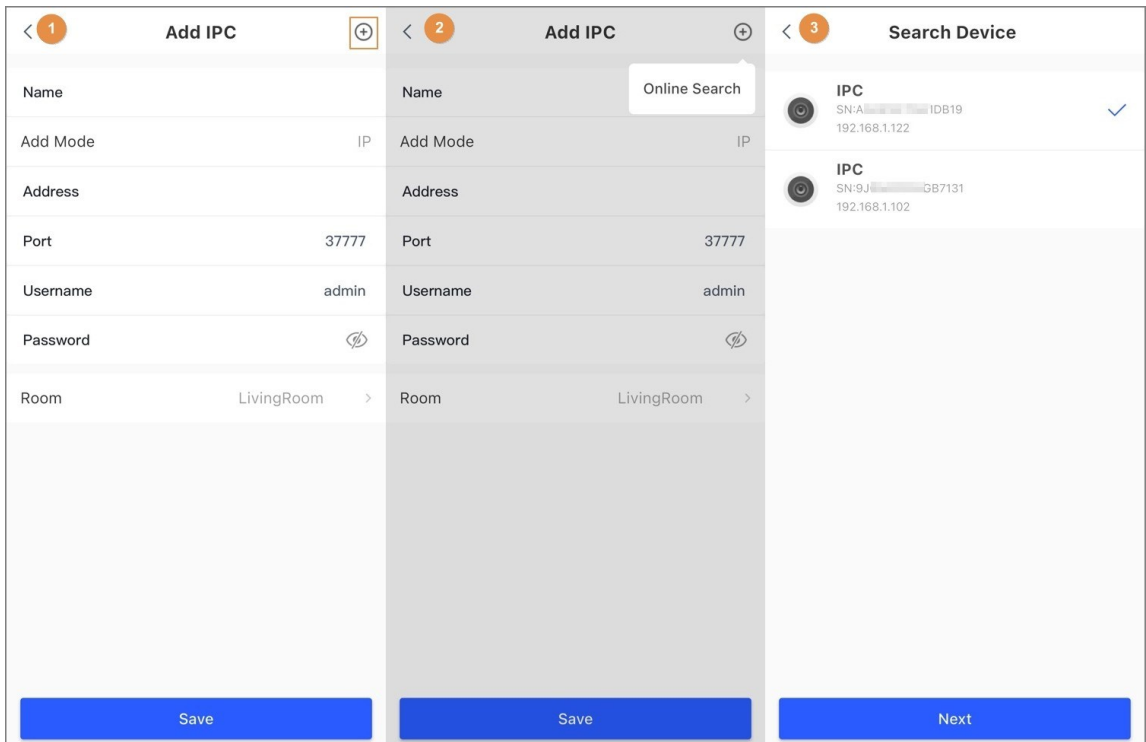
※ 警戒モード(アーミングモード)中は、周辺機器の設定を変更することはできません。

-  追加をタップして周辺機器を追加します。

表10-8 周辺機器の追加

タイプ	説明
周辺機器	「周辺機器を追加」を選択して、デバイス追加画面に入ります。
カード	「カードを追加」を選択し、キーパッドの読み取り領域にカードをかざしてください。
IPC	◇ デバイス名、IPアドレス、ユーザー名、パスワードを入力し、エリアを選択した後、「保存」をタップします。 ◇ オンライン検索によるIPCの追加。 1.  をタップし、「オンライン検索」を選択します。 2. アラームハブと同一ネットワーク上にあるIPCを自動的に検索します。検出結果からIPCを選択し、「次へ」をタップしてください。

図10-6 オンライン検索によるIPCの追加



The figure shows three sequential screenshots of a mobile application interface for adding an IPC (Intrusion Prevention Controller) via online search.

- Screenshot 1 (Step 1):** The 'Add IPC' screen. It features a top bar with a back arrow, a step indicator '1', and the title 'Add IPC'. A '+' icon is in the top right. The form includes fields for Name, Add Mode (set to IP), Address, Port (37777), Username (admin), Password (with a toggle for visibility), and Room (LivingRoom). A blue 'Save' button is at the bottom.
- Screenshot 2 (Step 2):** The 'Add IPC' screen with the 'Online Search' button highlighted in a white box. The step indicator is '2'.
- Screenshot 3 (Step 3):** The 'Search Device' screen. It shows a list of detected IPCs. Two devices are listed: one with SN: A..., MAC: 1DB19, and IP: 192.168.1.122; the other with SN: 9J..., MAC: GB7131, and IP: 192.168.1.102. A blue 'Next' button is at the bottom.

- サイレン、キーパッド、キーフォブ、リレー、緊急ボタンなどの周辺機器タイプのデバイスについては、カード上にデバイス番号が表示されます。
- デュアルテック、PIR、PIRカメラ、水漏れセンサー、ドア開閉センサーなどのセンサータイプのデバイスについては、カード上にゾーン番号が表示されます。
- ビデオ連動機能が有効にされ、リンクチャンネルが設定されたセンサーについては、デバイスのステータス領域にライブ映像再生アイコンが表示されます。

10.6.1 周辺機器の概要

温周辺機器の状態を確認することができます。確認可能な項目には、以下のような情報が含まれます：
温度、信号強度、バッテリー残量、その他の状態情報。

手順

ステップ1 アラームハブをタップして、デバイスのホーム画面に移動します。

ステップ2 周辺機器一覧から確認したい周辺機器をタップします。

ステップ3 デフォルトで「概要ページ」が表示されます。このページでは以下の情報を確認できます：

周辺機器の温度、信号強度、バッテリー残量、その他の状態情報、デバイスのプログラムバージョン。



使用可能なステータス情報は、ペリフェラルのタイプによって異なります。

- ビデオリンク機能を有効にし、リンクされたチャンネルを設定したセンサーの場合、デバイスステータスエリアにライブビデオの再生アイコンが表示されます。周辺機器が屋外トリプルテクディテクタとして追加されている場合は、カメラを追加できます
-

デバイスの一部。タップ  デバイスイメージの下にカメラを挿入し、画面に表示されるカウントダウンの中にカメラを手動で挿入します。

カメラをデバイスに追加すると、周辺機器アイコンが屋外のPIRCamとして手動スナップショットアイコンとともに表示されます。

10.6.2 周辺機器の設定方法

周辺機器をタップし、「設定」をタップすると、その周辺機器の各種設定を行うことができます。
詳細な設定内容については、該当周辺機器のユーザーマニュアルをご参照ください。

11 イベント

- **すべて**：追加されたすべてのデバイスから生成されたメッセージがDMSSアプリにプッシュ通知されます。イベントに関連する録画映像、ライブ映像、画像を確認することができます。



アラームを受信するには、デバイスまたはチャンネルでアラームルールを設定し、アラーム機能を有効にする必要があります。

- **カメラ**：カメラに関連するイベントメッセージやアラーム通知が対象です。
- **アラーム**：アラームハブに関連するアラーム通知が対象です。

11.1 アラームメッセージの購読

アラームメッセージを購読することで、アラームがトリガーされた際にDMSSアプリに通知がプッシュされるようになります。アラームメッセージの購読手順についての詳細は、「5.1.1.1 メッセージ」をご参照ください。
[\(Link\)](#)

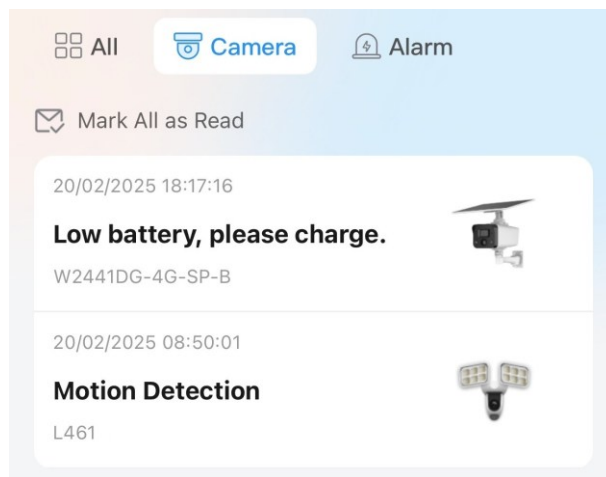
11.2 メッセージの表示

イベント画面では、アラームやイベントに関するメッセージを確認することができます。
ここでは、**動体検知メッセージ**を例として使用しています。

手順

ステップ1 デバイス画面で「イベント」をタップします。

図11-1 イベント



ステップ2 「カメラ」をタップし、次に動体検知メッセージをタップして詳細を確認します。

図11-2 動体検知



赤いドットが付いているメッセージは、まだ未読であることを意味します。



メッセージを既読にするには、個別のメッセージをタップするか、「アラームメッセージ」画面で「すべて既読にする」をタップしてください。

ステップ3 アラームメッセージをタップします。



をタップすると、再生画面が表示されます。再生画面での操作方法の詳細については、「7章 ビデオ再生」を参照してください。[\(Link\)](#)

関連操作



日付をタップして選択することで、該当するメッセージを表示することができます。

12 お気に入り

チャンネルを「お気に入り」に保存することで、簡単にアクセスできるようになり、必要なときにすぐにライブビュー画面に移動することができます。



再生中の映像をお気に入りに保存する方法の詳細については、「6章 ライブビュー」を参照してください。[\(Link\)](#)

手順

ステップ1 デバイス画面で「お気に入り」をタップします。

ステップ2 お気に入りカテゴリを作成します。カテゴリ名を入力し、チャンネルタイプを選択します。

1. 「お気に入りを作成」をタップして、新しいカテゴリを作成します。
2. カテゴリ名を入力し、チャンネルタイプを選択します。
3. 「OK」をタップします。

ステップ3 チャンネルをお気に入りに追加します。

1. 「チャンネルを追加」の横にある  アイコンをタップします。
2. 同じデバイスタイプから1つまたは複数のチャンネルを選択し、「保存」をタップします。

関連操作

- このフォルダー内のチャンネルを**同時再生**するには、 再生アイコンをタップします。
- チャンネルの**詳細**を表示したり、チャンネルを**追加・削除**したり、フォルダー名を**変更**するには、 設定アイコンをタップします。
- フォルダを削除するには、「**削除**」をタップします。

13 私(マイページ)

アカウントの管理、アプリの設定、ツールの利用ができます。
また、「ヘルプセンター」でアプリのユーザーマニュアルを閲覧することも可能です。

図13-1 私(マイページ)



表13-1 私(マイページ)

番号	名前	説明
1	アカウント管理	アカウント名をタップすると「アカウント」画面に移動します。 • 個人情報の表示・編集が可能です。 • パスワードの変更 「アカウントセキュリティ」>「パスワード変更」をタップし、旧パスワードと新パスワードを入力して「OK」をタップします。 • 端末のバインド(ターミナルバインド) 「アカウントセキュリティ」>「端末バインド」をタップし、スイッチ( / )で機能を有効にします。 • 端末の管理 「アカウントセキュリティ」>「端末管理」をタップして、端末情報を編集したり、複数端末を一括削除できます。 • 指紋認証・パターン認証 スイッチ( / )をタップして、指紋認証やパターンロックによる認証を有効にできます。 • アカウントの削除 「アカウント削除」>「削除を申請」を選択すると、アカウント削除の手続きが可能です。 • アカウントの情報のエクスポート 1. 「アカウント情報のエクスポート」>「エクスポート」を選択 2. メールアドレスを入力し、「次へ」をタップ 3. 入力したメールに届いた認証コードを入力(60秒以内に使用してください。それ以降は無効になります。) 4. メールでエクスポートされたアカウント情報を確認 • DMSSからログアウト 「ログアウト」をタップしてDMSSを終了します。 • サードパーティアカウントとの連携 「サードパーティアカウント」をタップし、対応するプラットフォームやアプリの横にある「今すぐバインド」をタップして連携します。 連携が完了すると、DMSSにサードパーティアカウントでログインできるようになります。
2	アカウントQRコード	アカウントのQRコードを表示するには、をタップしてください。 「アルバムに保存」をタップすると、QRコードをスマートフォンに保存することができます。

番号	名前	説明
3	サービス	• デバイスの共有についての詳細は、「5.2 デバイスの共有」(Link) • 「5.4.2 デバイスの一括委託」を参照してください。(Link) • デバイスの登録解除については、「5.5 デバイスの登録解除」を参照してください。(Link) • 一括委託についての詳細は、「5.4.2 デバイスの一括委託」を参照してください。(Link)  ※一括委託に対応している国または地域でのみ、ボタンが表示されます。 • セキュリティサービスの申請については、「5.3 セキュリティサービスの申請」を参照してください。(Link) • ローカルデバイスをアカウントに移行する方法については、「5.7 ローカルデバイスのアカウントへの移行」を参照してください。(Link) • デバイスのエクスポートについての詳細は、「5.6 デバイスカードの作成」を参照してください。(Link)
4	設定	• 携帯電話の位置情報 スマートフォンの現在位置を確認できます。手動で位置を変更することも可能です。 • デフォルトページ アプリ起動時に表示する初期ページを設定します。「ホーム」または「アラームコントロール」から選択できます。 • 外観 「システム設定と一致させる」機能を  /  タップで有効／無効にできます。 • セルラーネットワークで再生  /  をタップしてこの機能を有効／無効にします。有効にすると、モバイル通信でも常に映像を再生できます。 • ハードウェアデコーディング タップして有効にすると、ビデオストリームのパフォーマンスが向上します。 • メッセージ内のビデオの長さ アラームメッセージ内で再生される動画の再生時間を設定します。 • 通知設定 ◇ タップして通知機能を有効にします。有効にすると、アラーム通知を受信する時間帯を設定できます。 バナー表示を有効にすると、通知が画面上に表示されます。 • アラーム音声の設定 ◇ アラームの種類ごとに通知音を個別に設定できます。 • 電話機能 ◇  タップして有効にすると、アプリがバックグラウンドで動作している間に着信があった場合、通話用のウィンドウが表示されます。 • 権限 位置情報、写真、カメラなどのアクセス権限をスマートフォンから取得可能。 • キャッシュの削除 アプリのキャッシュデータを削除します。
5	アルバム	スナップショットや録画されたビデオは、「アルバム」に保存されます。

番号	名前	説明
6	ツール	• Wi-Fi ステータスをテストするには、 をタップします。 • デバイスのパスワードをリセットするには、 をタップします。 • 通知プッシュをテストするには、 をタップします。 • モバイルキャリアのドメイン名を設定するには、 をタップし、DNS を入力した後、「テスト」をタップして確認します。 •  タップして関連するログファイルをアップロードします。
7	ヘルプとフィードバック	• アプリ内でよくある質問(FAQ)やユーザーマニュアルを閲覧することができます。 • 製品に関するフィードバックを送信することも可能です。「フィードバック」をタップし、製品に関するご意見や情報を入力してください。
8	概要と法的情報	• DMSSのプライバシーポリシーを閲覧できます。 • 利用規約やオープンソースソフトウェアに関する通知を確認できます。 • アプリのバージョン情報、ユーザー契約、オープンソースライブラリ情報など、DMSSに関する詳細情報を表示できます。

付録1 セキュリティに関する推奨事項

1. アカウント管理

a. 強力なパスワードを使用する

- パスワードの長さは**8文字以上**にしてください。
- **2種類以上の文字種**(大文字・小文字の英字、数字、記号)を含めてください。
- **アカウント名やその逆順**を含めないでください。
- 「123」「abc」などの**連続した文字列**は使用しないでください。
- 「111」「aaa」などの**同一文字の繰り返し**は避けてください。

b. 定期的にパスワードを変更する

パスワードは**定期的に変更**することを推奨します。これにより、推測や不正解析によるリスクを低減できます。

c. アカウントと権限を適切に割り当てる

業務や管理のニーズに応じて、ユーザーを**適切に追加し、最小限の必要な権限**だけを割り当ててください。

d. アカウントロックを有効にする

アカウントロック機能は**初期設定で有効**になっています。セキュリティを維持するため、無効にせずそのまま利用することを推奨します。不正ログイン(パスワード誤入力)を複数回試みられた場合、**対象アカウントと元のIPアドレスがロック**されます。

e. パスワードリセット情報を適時に設定・更新する

プラットフォームには**パスワードリセット機能**があります。攻撃リスクを下げるために、**リセット用の情報を早めに設定し、変更があれば速やかに更新**してください。パスワード保護の質問を設定する際は、簡単に推測できる内容は避けてください。

f. アカウントのIP/MACバインディングを有効にする

アカウントに対して**IPアドレスまたはMACアドレスのバインド機能**を有効にすることで、アクセスセキュリティをさらに強化できます。

2. サービス構成

a. HTTPSを有効にする

HTTPSを有効にすることで、Webサービスへのアクセスが安全な通信経路(SSL/TLS)を通じて行われ、盗聴や改ざんのリスクを軽減できます。

b. 不要なサービスを無効化し、安全なモードを選択する

使用しない場合は、SNMP(Simple Network Management Protocol)やSMTP(メール送信)などのサービスを無効化することを推奨します。これによりセキュリティリスクを低減できます。

必要なサービスを使用する場合は、以下のような**安全な通信モード**を使用してください:

- SMTP: メールサーバーへの接続には**TLS(Transport Layer Security)**を使用してください。
- FTP: 通常のFTPではなく、**SFTP(Secure FTP)**を選択し、強力なパスワードを設定してください。

3. ネットワーク構成

a. ファイアウォールの許可リストを有効にする

許可されたIPアドレス以外からのアクセスを遮断するために、ファイアウォールの許可リスト機能を有効にすることを推奨します。その際は、自分のパソコンのIPアドレスや関連機器のIPアドレスをリストに追加しておく必要があります。

b. ネットワークの分離

ネットワークは、スイッチやルーターで映像監視ネットワークとオフィスネットワークを異なるVLANに分割することで分離すべきです。

これにより、攻撃者がオフィスネットワークを経由して**ピボット攻撃(Pivoting attack)**を映像監視ネットワークに対して行うことを防止できます。

4. セキュリティ監査

a. オンラインユーザーの確認

不定期に現在ログインしているユーザーを確認し、不正ユーザーのログインがないかをチェックすることを推奨します。

b. プラットフォームログの確認

ログを確認することで、以下の情報を取得できます。プラットフォームへのログイン試行のIPアドレス情報、ログインユーザーによる重要な操作履歴。

5. 物理的保護

プラットフォームがインストールされているデバイスに対しては、物理的な保護対策を講じることが推奨されます。

たとえば、「機器を専用のサーバールームやキャビネットに設置する」・「アクセス制御や鍵管理を適切に実施する」

これにより、不正な人物による物理的接触(例:機器の破壊や改ざん)を防止できます。

6. 境界セキュリティ

ソフトウェアプラットフォームのセキュリティを確保するために、境界防御用のセキュリティ製品の導入が推奨されます。また、以下のような対策を実施してください。

- ・ 認証されたアクセスのみを許可する
- ・ アクセス制御を厳格に設定する
- ・ 侵入防止(IPS)や侵入検知(IDS)システムを活用して、不正侵入を未然に防ぐ

これらの対策により、外部からの攻撃や不正アクセスに対する防御を強化できます。