CVIレコーダー操作マニュアル

22.11.Y.02

フォアワード

一般

このクイックスタートガイド(以下「マニュアル」と呼びます)では、CVIレコーダー機器(以下「CVIレコーダー」と呼びます)の機能や操作方法を紹介しています。

安全上の注意

マニュアルには、定義された意味を持つ以下のカテゴリ別の注意喚起語が記載されています。

シグナルワード	意味
DANGER	回避しないと、致命的または重傷につながる可能性のある高危険性を示します。
WARNING	回避しない場合、軽度または中度の傷害を招く可能性がある中程度または低レベルの潜在的な危険性を示します。
CAUTION	回避しない場合、物的損害、データ損失、性能の低下、または予期せぬ結果を招く可能性がある潜在的なリスクを示します。
TIPS	問題の解決または時間の節約に役立つ方法を提供します。
NOTE	テキストの強調と補足として追加情報を提供します。

改訂履歴

バージョン	改訂内容	リリースタイム
V1.0.0	最初のリリース	2022年10月

プライバシー保護通知

CVIレコーダーユーザーは、顔、自動車プレート番号などの他のユーザーの個人情報を収集できます。プライバシーを保護するために、地域のプライバシー保護法および規則を順守する必要があります。監視エリアの存在を知らせ、明確に目に見える形で提供してください。

(看板やステッカーなどで録画されている旨を公開する等)

マニュアルについて

- 本マニュアルは参考用です。取扱説明書と実際の製品の間に矛盾がある場合は、実際の製品が優先されます。
- 取扱説明書に準拠していない操作で生じた損失については、当社は一切責任を負いません。
- マニュアルは、最新の法規制に従って更新されます。紙の取扱説明書と電子版に矛盾がある場合は、電子版が優先されます。
- すべての設計およびソフトウェアは、事前の文書による通知なしに変更されることがあります。製品のアップデートによって、実際の製品とマニュアルとの間に多少の相違が生じる場合があります。
- 技術データ、機能および操作の説明に逸脱がある場合や、印刷上のエラーがある場合があります。
- 取扱説明書(PDF形式)が開けない場合は、リーダーソフトウェアをアップグレードするか、他の主流のリーダーソフトウェアを試してください。
- 本書に記載されているすべての商標、登録商標、および会社名は、それぞれの所有者の所有物です。
- CVIレコーダーの使用中に問題が発生した場合は、Webサイトにアクセスし、サプライヤまたはカスタマーサービスにお問い合わせください。

重要な安全対策と警告

CVIレコーダーの正しい応用方法を以下に説明します。危険と故障を防ぐために、使用前にマニュアルをよくお読みください。ご使用の際は、必ずマニュアルに準拠し適切にマニュアルを保管してください。

動作要件

- CVIレコーダーを直射日光の当たる場所や、発熱する機器の近くに置いたり、設置したりしないでください。
- 湿気、ほこりの多い場所にCVIレコーダーを設置しないでください。
- 水平に設置するか、安定した場所に設置し、落下しないようにしてください。
- CVIレコーダーに液体が流れ込むのを防ぐため、CVIレコーダーの上に液体を落としたりしないでください。
- 通気の良い場所にCVIレコーダーを設置し、通気口をふさがないようにしてください。
- CVIレコーダーは、定格入出力範囲内でのみ使用してください。
- CVIレコーダーを任意に分解しないでください。
- CVIレコーダーの輸送、使用、保管は、許容湿度および温度範囲内で行ってください。

電源要件

- 正しい電源を使用してください。これを守らないと、火災、爆発、バッテリーの焼き付きの危険が発生する可能性があります。
- バッテリーを交換するには、同じ種類のバッテリーのみを使用できます。
- 使い切った電池は、指示に従って廃棄してください。
- 電線は、地域の条例で推奨されている定格仕様のものを使用してください。
- 本CVIレコーダーに適合した標準電源アダプタを使用してください。それ以外の場合は、ユーザーは事故や損害が起きる可能性がございます。
- SELV(安全特別低電圧)要件を満たす電源を使用し、IEC60950-1のLimited Power Sourceに適合した定格電圧の電源を供給してください。特定の電源装置要件については、デバイスラベルを参照してください。
- カテゴリーI構造の製品は、保護アースを装備したグリッド電源出力ソケットに接続します。

目次

フォアワード 1
重要な安全対策と警告 3
I ローカル操作 5
1.1 起動 5
1.2 初期化 5
1.3 エンコード設定の構成 9
1.4 IPカメラの追加 11
1.5.1 チャンネルタイプの変更 11
1.5 録画スケジュールの設定 12
1.6 P2P設定 13
1.7.1 P2Pの有効化 13
1.7 スマートモーション検出 14
1.8 ライブビュー 16
1.9 録音再生 17
I.10 バックアップ 18
2 Webへのログイン 20
付録Iサイバーセキュリティに関する推奨事項 21

1 ローカル操作

型番の異なる画面では、UI等にわずかな違いが見られる場合があります。本書の図はイメージです。実際の製品が優先されます。

1.1 起動

CVIレコーダーを起動する前に、次を確認してください:

- 定格入力電圧は、CVIレコーダーの電源要件に適合します。
- デバイスセキュリティのため、CVIレコーダーを電源アダプタに接続してから、電源ソケットに接続します。
- 常に安定した電流を使用してください。UPSを電源として使用することをお勧めします。

1.2 初期化

はじめに

初めて起動するときは、パスワード情報を設定する必要があります。機器のセキュリティレベルを保証するために、ログインパスワードを適切に保持し、定期的な変更を強くお勧めします。

手順

ステップ1　CVIレコーダーの電源を入れます。システムがデバイス初期化画面に入ります。

ステップ2　ドロップダウンリストから、必要に応じて地域、言語、ビデオ規格を選択します。

「Japan」、「日本語」、「NTSC」を選択して、「次へ」をクリックします。

これらの設定は、初期化後でも設定ページで変更できます。

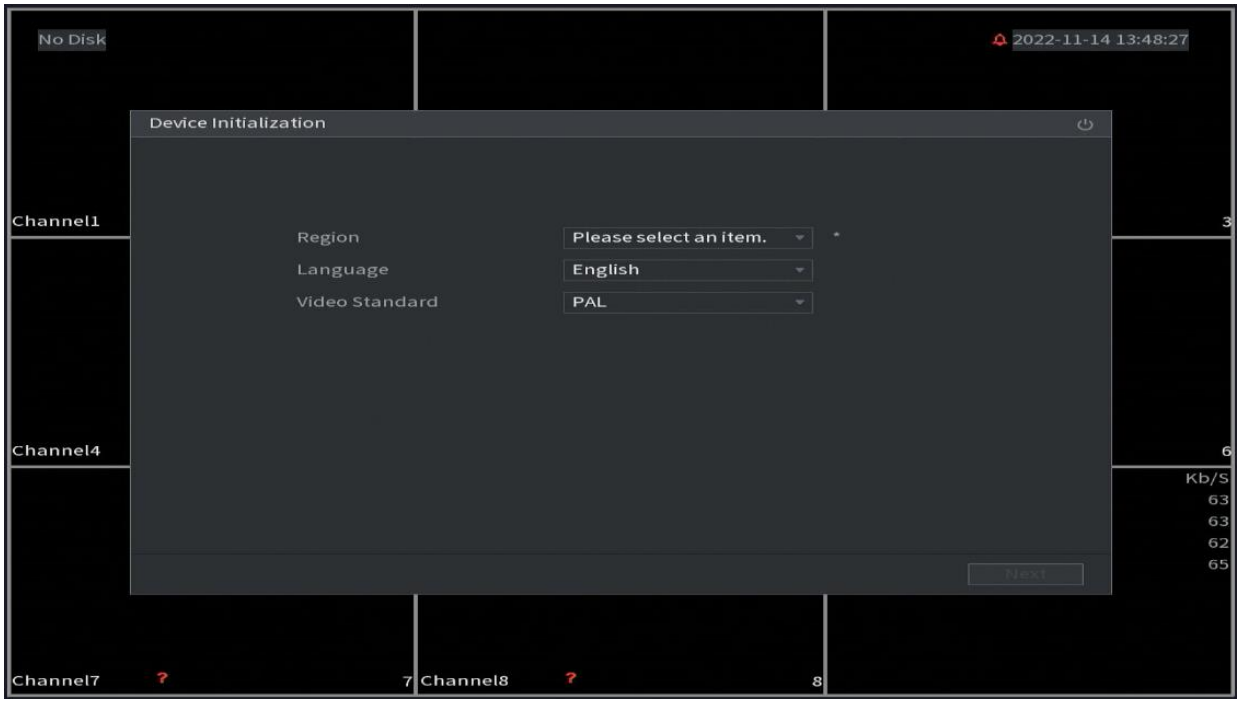

図1-1　位置、言語、ビデオ規格の設定

ステップ3　「次へ」をクリックします。

ステップ4　「ソフトウェア使用許諾契約」を読み、「すべての条件を読んで同意します」

ステップ5　タイムゾーンを選択してシステム時刻を設定し、「次へ」をクリックします。

図1-2　タイムゾーンとシステム時刻の設定

ステップ6　デバイス管理者のパスワード情報を設定し、「次へ」をクリックします。

図I-3　パスワード情報の設定

表I-Iパスワード情報

パラメータ	説明
ユーザー名	デフォルトでは、ユーザーはadminであり、変更することはできません。
パスワード	「パスワード」フィールドにデバイス管理者の新しいパスワードを入力し、次のフィールドでパスワードを確認します。 新しいパスワードは8文字から32文字まで設定でき、数字、文字、特殊文字(”’”、””、”;”、”:”、”&”を除きます)の2種類以上が含まれます。
パスワードの確認	
パスワードのヒント	デバイスのパスワードを呼び出すのに役立つプロンプト質問を入力します。 ログイン画面でをクリックすると、パスワードのリセットに役立つプロンプトが表示されます。

ステップ7　マウスを使用してロック解除パターンを描画し、確認のために再度描画します。

図I-4　ロック解除パターンの描画

- 設定するパターンは、少なくとも4つのポイントをまたぐ必要があります。
- ロック解除パターンを設定しない場合は、スキップをクリックします。
- ロック解除パターンを設定すると、デフォルトの認証方法として使用されます。この設定をスキップする場合は、ログイン用のパスワードを入力します。

ステップ8　Emailアドレスとセキュリティ質問をCVIレコーダーに適用します。

- 電子メールを有効にして、電子メールアドレスを入力します。
- セキュリティ質問を有効にして、質問1、質問2、質問3のドロップダウンリストから質問を選択し、それらの質問に対する回答を入力します。

図I-5 Emailとセキュリティに関する質問の適用

ステップ9　OKをクリックします。

1.3 エンコード設定の構成

各チャンネルのエンコード設定を設定する方法を示します。

手順

ステップ1　メインメニュー>CAMERA>エンコード>オーディオ/ビデオの順に選択します。

ステップ2　メイン/サブストリームのパラメータを設定します。

図1-7　オーディオ/ビデオ

表1-3　オーディオ/ビデオパラメータ

パラメータ	説明
チャンネル	設定を行なうチャンネルを選択します。
スマートコーデック	スマートコーデック機能を有効にします。この機能を使用すると、重要でない録画ビデオのビデオビットストリームを減らして、ストレージスペースを最大にすることができます。
タイプ	● メインストリーム:「種別」ドロップダウンリストから、「一般」、「モーション」、または「アラーム」を選択します。 ● サブストリーム:選択できません。
圧縮	「圧縮(Compression)」リストで、エンコード・モードを選択します。 ● H.265:メインプロファイルのエンコード。この設定をお勧めします。 ● H.264H:ハイプロファイルエンコーディング。高精細度の低ビットストリーム。 ● H.264:一般的なプロファイルエンコード。 ● H.264B:ベースラインプロファイルのエンコード。

	この設定では、同じ定義の他の設定よりも高いビットストリームが必要です。
解像度	解像度リストから、ビデオ出力の解像度を選択します。 最大ビデオ解像度は、モデルによって異なる場合があります。
ビットレートタイプ	「ビットレートタイプ」ドロップダウンリストから、ビデオの解像度を選択します。最大ビデオ解像度は、デバイスモデルによって異なる場合があります。
フレームレート(FPS)	ビデオのフレーム/秒を設定します。値を高くするほど、画像がより鮮明で滑らかになります。フレームレートは解像度に合わせて変化します。 通常、PAL形式では1～25の値を選択でき、NTSC形式では1～30の値を選択できます。ただし、選択できるフレームレートの特定の範囲は、CVIレコーダーの機能によって異なります。
品質	この機能は、Bit Rate ListでVBRを選択した場合に使用できます。 値を大きくするほど、画像がより良くなります。
Iフレーム間隔	2つの参照フレーム間の間隔。
ビットレート(Kb/s)	「ビットレート」ドロップダウンリストから、値を選択するか、カスタマイズした値を入力して画質を変更します。値が大きいほど、イメージは向上します。
ビデオ	サブストリームの機能を有効にします。
オーディオ オーディオソース 圧縮	Moreをクリックすると、More画面が表示されます。 ● オーディオ:この機能は、メインストリームではデフォルトで有効になっています。サブストリーム1に対して手動で有効にする必要があります。この機能を有効にすると、録画されたビデオファイルはコンポジットオーディオおよびビデオストリームになります。 ● オーディオソース:「オーディオソース(Audio Source)」リストで、「LOCAL」と「HDCVI」を選択できます。 ◇ LOCAL:オーディオ入力ポートからオーディオ信号を入力します。 ◇ HDCVI:HDCVIカメラから音声を入力します。 オーディオ形式:「圧縮」ドロップダウンリストから、必要に応じて形式を選択します。

ステップ3　適用をクリックします。

「コピー先」をクリックして、設定を他のチャンネルにコピーできます。

1.4 IPカメラの追加

検索結果またはIP情報を手動で入力して、IPカメラを追加できます。IPカメラを追加する前に、少なくとも1つのアナログチャネルをIPチャネルに変更する必要があります。

追加するカメラは、CVIレコーダーと同じネットワーク上にある必要があります。

1.5.1 チャンネルタイプの変更

CVIレコーダーにIPカメラを追加する必要がある場合は、チャンネルタイプをIPチャンネルに変換できます。

背景情報

CVIレコーダーのすべてのチャンネルはデフォルトでアナログチャンネルとして設定されており、IPチャンネルに変換できます。

手順

ステップ1　メインメニュー>CAMERA>チャンネルタイプを選択します。

ステップ2　「IP」列のチェックボックスをオンにします。

- アナログカメラまたはIPカメラのチャンネル選択は順番に行われます。たとえば、IPカメラのチャンネルを変換する場合は、最初にチャンネル8の最後のチャンネル番号から選択する必要があります。つまり、チャンネル8を選択するまで、チャンネル7を直接選択することはできません。
- 次の図の場合、9～16チャンネルはIPカメラ専用で、範囲は購入したモデルによって異なります。実際の製品が優先されます。

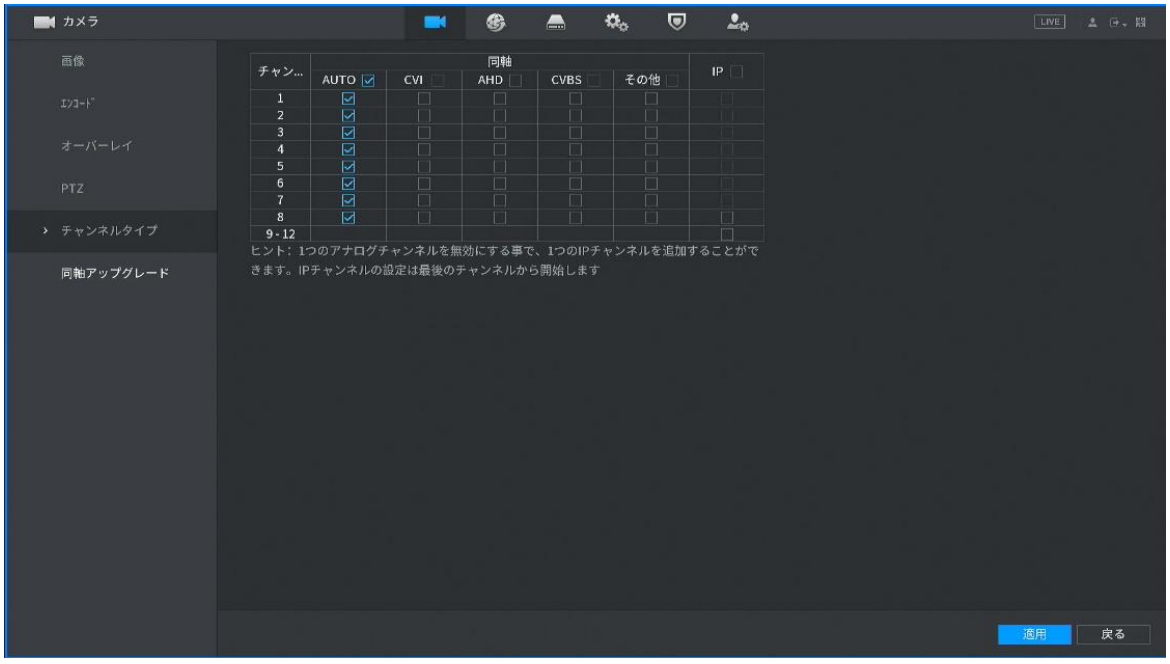

図1-8IPチャネルの選択

ステップ3　「適用」をクリックし、画面の指示に従って設定を完了します。

ステップ6　「次へ」をクリックします。初期化が完了するまで1～2分間待ちます。

ステップ7　完了をクリックします。

1.5 録画スケジュールの設定

デフォルトでは、すべてのカメラは24時間連続してビデオを録画します。必要に応じて設定の変更が可能です。

手順

ステップ1　メインメニュー>ストレージ>スケジュール>録画を選択します。

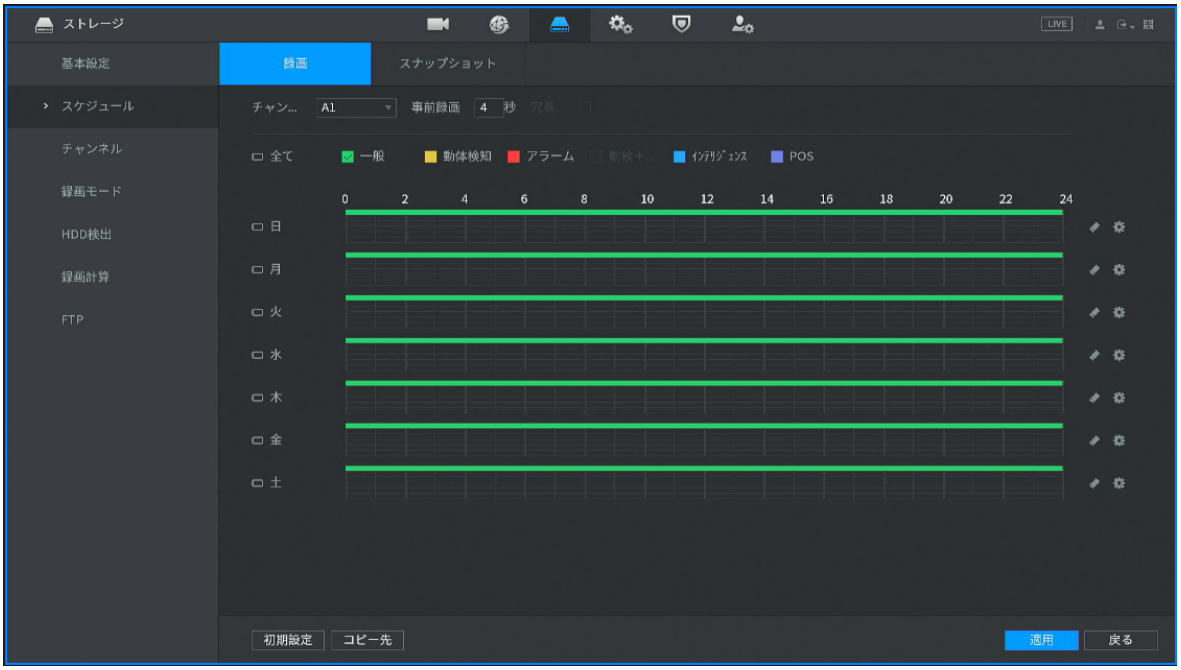

図1-19　レコードスケジュール

ステップ2　パラメータを設定します。

表1-6レコードパラメータ

パラメータ	説明
チャンネル	「チャンネル」ドロップダウンリストから、ビデオ録画設定を変更するチャンネルを選択します。
事前録画	イベントが起きる前の録画期間を設定します。値の範囲:0～30秒。
コピー先	「コピー(Copy)」をクリックして、設定を他のチャンネルにコピーします。

ステップ3　描画や編集でスケジュールを設定します。

- 描画:マウスの左ボタンを押したままマウスをドラッグすると、ピリオドが描画されます。
- 編集:クリックして期間を設定し、「OK」をクリックします。

ステップ4　適用をクリックします。

1.6 P2P設定

QRコードを使用して、スマートフォンをCVIレコーダーに接続して管理できます。

CVIレコーダーがインターネットに接続されていることを確認し、はいの場合は、P2P画面の「状況」ボックスに「オンライン」と表示されます。

1.7.1 P2Pの有効化

P2Pを有効にし、スマホアプリ（DMSS）で右側のQRコード（機器SN）をスキャンします。

ステップ1　メインメニュー>ﾈｯﾄﾜｰｸ >P2Pを選択します。

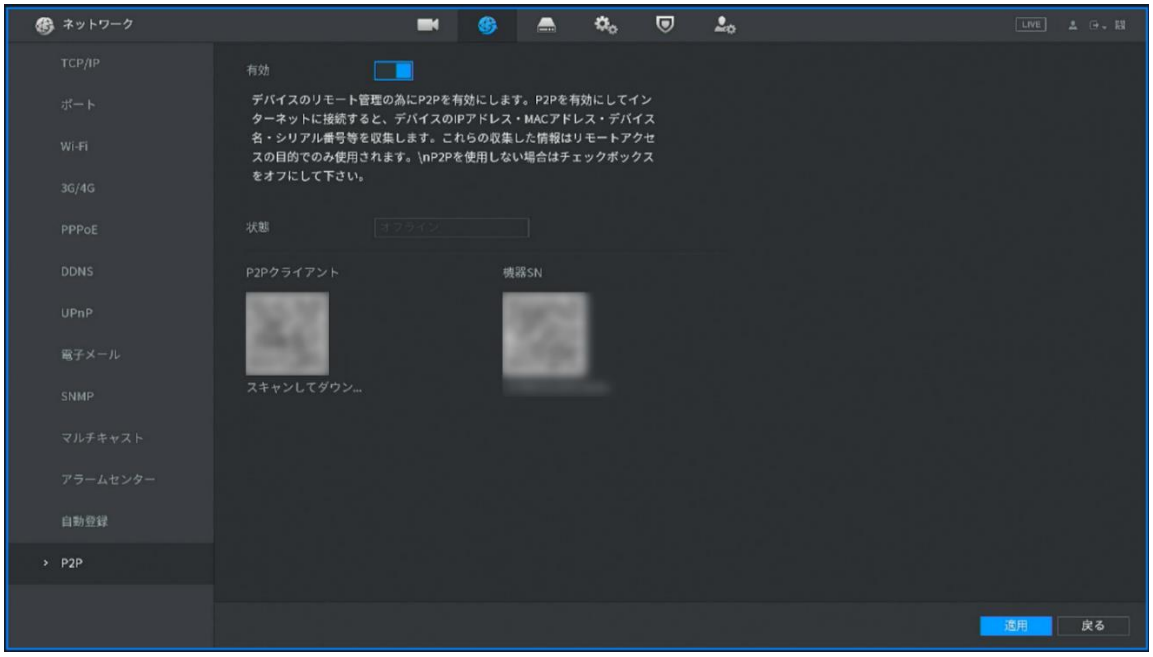

図1-20P2P

ステップ2　有効にチェックをします。

ステップ3　適用をクリックします。

1.7 スマートモーション検出

スマートモーション検出(SMD)を設定する方法を示します。

はじめに

スマートモーション検出(SMD)は、ルールを設定して線を描画しなくても、人や車両のアラートをシーンのどこにでも表示したい、人の少ない領域に最適な監視機能です。

ステップ1メインメニュー>SMART検出 >パラメータ>SMDの順に選択します。

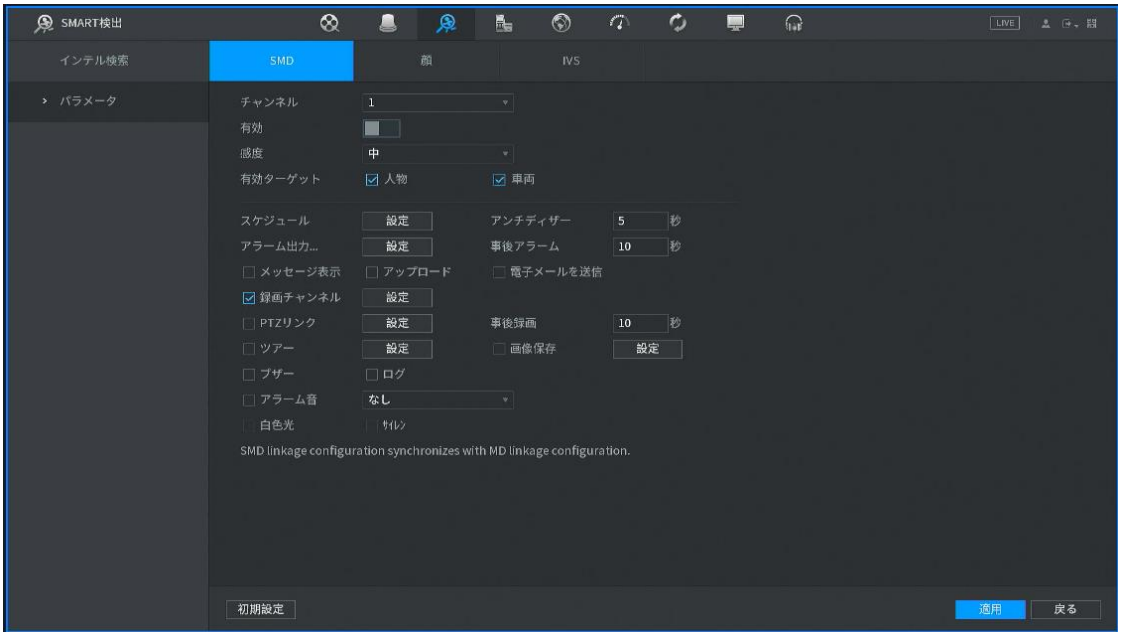

図1-23 SMD

ステップ2　チャネルを選択し、有効にします。

ステップ3　パラメータを設定します。

パラメータ	説明
チャンネル	プルダウンからモーション検出を設定するチャンネルを選択します。
有効	SMD機能の有効/無効を設定します。
感度	高、中、低を含む感度を設定します。感度が高いほど、アラーム確率が大きくなり、誤アラーム率が大きくなります。デフォルトでは、中央が選択されます。
有効なターゲット	人物と車両を含むアラームオブジェクトを選択します。
スケジュール	モーション検出がアクティブになる期間を定義します。
アンチディザー	イベント検出終了からアラーム停止までの時間を設定します。

アラーム出力ポート	設定をクリックすると、設定画面が表示されます。 ● General Alarm:選択した出力ポートに接続されたアラームデバイスを介したアラーム起動を有効にします。 ● 外部アラーム:接続されたアラームボックスを通じてアラーム起動を有効にします。
事後アラーム	外部アラーム解除後、アラームを解除するまでの時間を設定します。値の範囲は0秒から300秒で、デフォルト値は10秒です。0を入力すると、遅延はありません。
メッセージを表示	ローカルホストPCでポップアップメッセージが有効になります。
アップデート	アラームイベントが発生したときに、システムがアラーム信号をネットワーク(アラームセンターを含む)にアップロードできるようになります。
電子メールを送信	アラームイベントが発生したときにシステムが電子メール通知を送信できるようにします。 この機能を使用するには、メインメニュー>ネットワーク >EMAILでメール機能が有効になっていることを確認してください。
録音チャンネル	録音するチャンネルを選択します。選択したチャンネルは、アラームイベントが発生すると記録を開始します。 モーション検出と自動記録機能の記録を有効にする必要があります。
PTZリンク	「設定」をクリックすると、PTZ画面が表示されます。 モーションディテクションはPTZプリセットのみ有効です。
事後録画	アラーム解除後、録音を停止するまでの時間を設定します。値の範囲は10秒から300秒で、デフォルト値は10秒です。
ツアー	ツアーチェックボックスをオンにすると、選択したチャンネルのツアーが有効になります。
画像保存	スナップショットチェックボックスをオンにすると、選択したチャネルのスナップショットが取得されます。 この機能を使用するには、メインメニュー>カメラ >エンコード >スナップショットの順に選択し、タイプリストでイベントを選択します。
ブザー	チェックボックスをオンにすると、デバイスでブザーが有効になります。
ログ	チェックボックスをオンにすると、デバイスがローカルアラームログを記録できるようになります。

アラーム音	モーション検出イベントに応答して音声/アラーム音を有効にする場合に選択します。

ステップ4　適用をクリックして設定を保存します。

1.8 ライブビュー

ログインすると、システムはデフォルトで複数チャネルのライブビューモードになります。各チャンネルのモニタリングビデオを表示できます。表示されるウィンドウの数は、モデルによって異なる場合があります。他の画面からライブビュー画面に入るには、画面右上の　LIVE　をクリックします。

図1-24　ライブビュー

ライブビュー画面

- デフォルトでは、システム時間、チャンネル名、チャンネル番号が各チャンネルウィンドウに表示されます。メインメニュー>カメラ>オーバーレイ>で設定変更を行うことができます。
- 右下の図はチャンネル番号です。チャンネルの位置を変更したり、チャンネル名を変更したりすると、この図でチャンネル番号を認識してから、録音クエリや再生などの操作を行うことができます。

表1-7　アイコンの説明

アイコン	説明
	ビデオ録画中です。

	モーション検出中です。
	ビデオロスが検出されました。
	チャネル監視はロックされます。

1.9 録音再生

録画を再生するには、メインメニュー>再生を選択するか、ライブビュー画面を右クリックして検索を選択します。

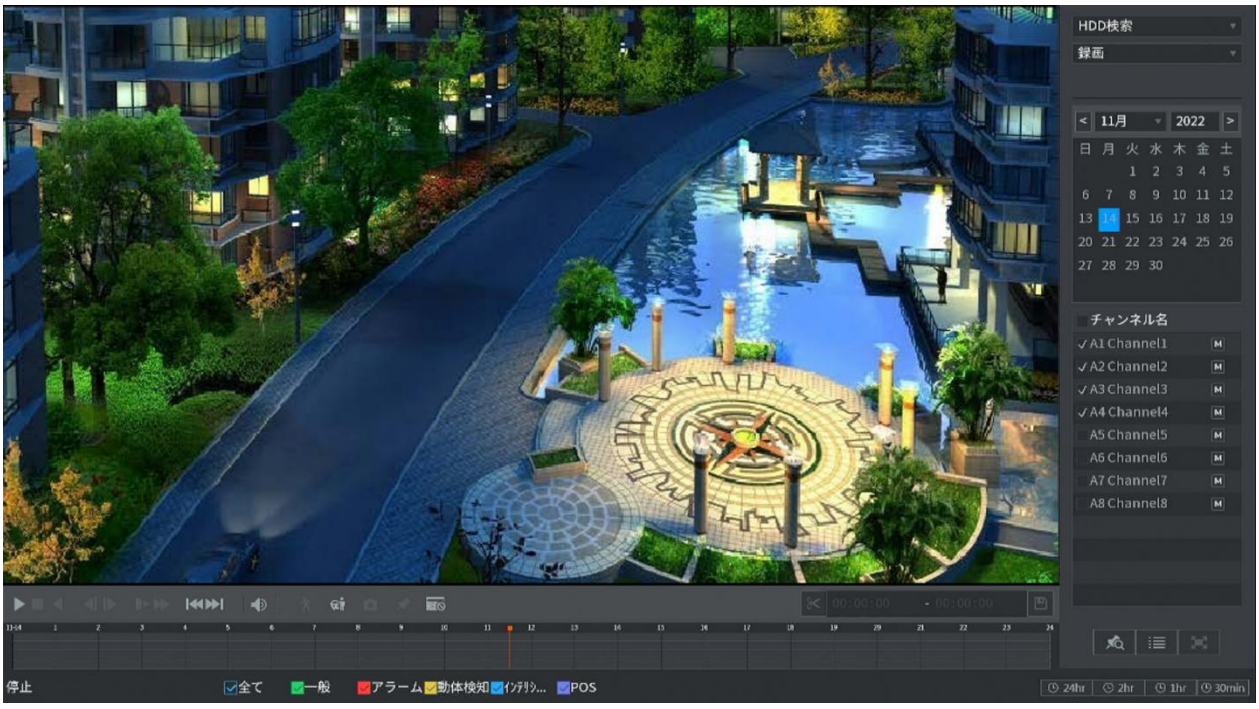

図1-25再生メイン画面

再生メイン画面の操作方法については、ユーザーズマニュアルを参照してください。

インスタント再生

録画した動画のうち、直前の5分～60分を再生できます。

クリックすると、インスタント再生画面が表示されます。

- スライダーを動かして、再生を開始する時間を選択します。
- 再生、一時停止、および再生の終了。
- チャンネル名やステータスアイコンなどの情報は、インスタント再生中はシールドされ、終了するまで表示されません。
- 再生中は、画面分割レイアウトの切り替えはできません。

再生時間を変更するには、メインメニュー>システム>一般>基本を選択し、再生する時間を入力します。

図1-26　インスタント再生時間の設定

スマート検索再生

再生中に、特定の領域を分析して、モーション検出イベントが発生したかどうかを確認できます。システムは、記録されたビデオのモーションイベントを含む画像を表示します。

スマート検索機能を使用するには、メインメニュー>アラーム >ビデオ検出 >動体検知を選択して、チャンネルのモーション検出を有効にする必要があります。

1.10 バックアップ

録画データのバックアップは、USBを挿入しファイルバックアップを選択するか、メインメニュー>バックアップを選択します。

ステップ１ USB(2.0)をUSBポートに挿入します。
ステップ２ ファイルバックアップを選択します。
ステップ３ デバイス、保存先を設定し、録画チャンネル、開始時刻などを選択し検索をクリックします。録画データが一覧で表示されます。
ステップ４ 録画データを選択し、右下のバックアップをクリックします。

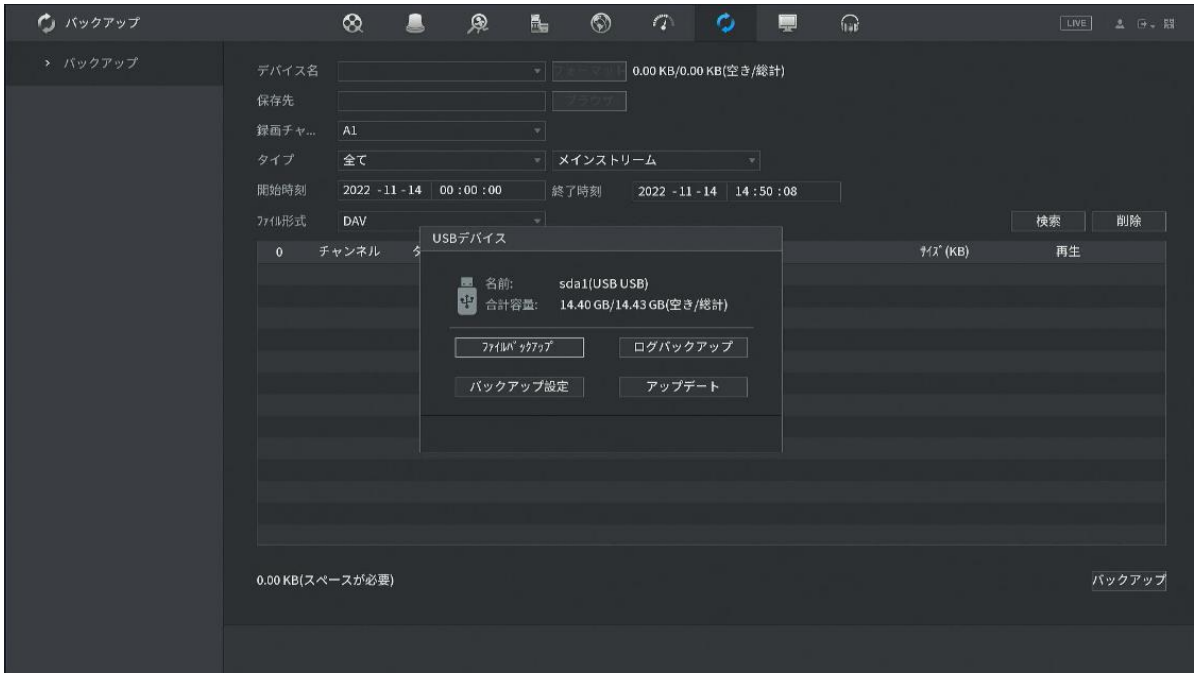

図1-27 USB　挿入時のポップアップ

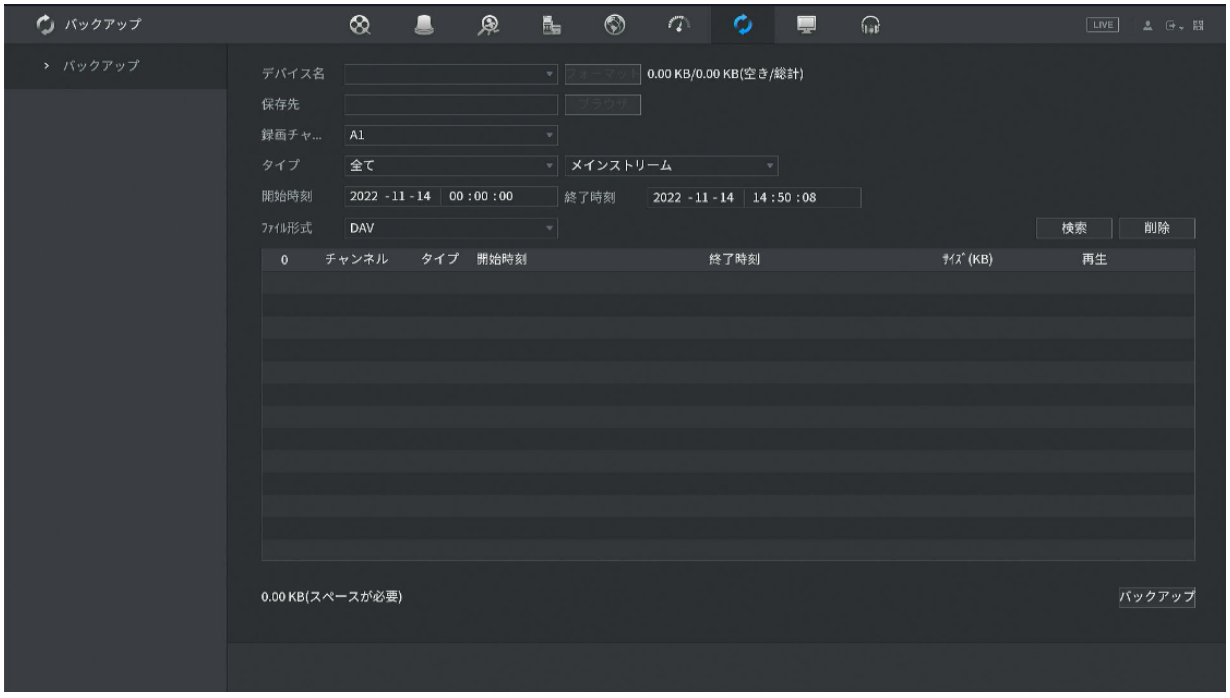

図1-28 バックアップ設定画面

2 Webへのログイン

手順

ステップ1　ブラウザを開き、CVIレコーダーのIPアドレスを入力して、Enterキーを押します。

ステップ2　ユーザー名とパスワードを入力します。

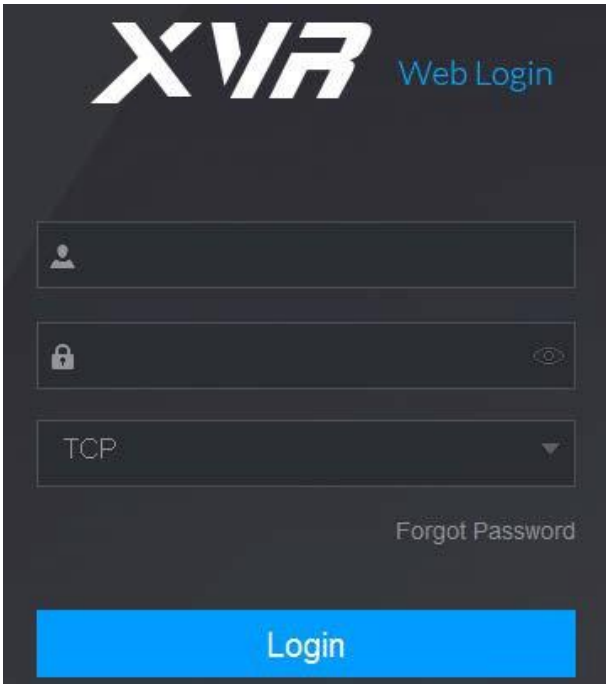

図2-1ログイン

- デフォルトの管理者アカウントはadminです。パスワードは、初期設定時に設定されたものです。アカウントをセキュリティ保護するために、パスワードを適切に保持し、定期的に変更することをお勧めします。

ステップ3　ログインをクリックします。

付録Iサイバーセキュリティに関する推奨事項

IPビデオ監視はサイバーリスクに影響されませんが、ネットワークとネットワークを保護し、強化するための基本的なステップを踏むことで、攻撃の影響を受けにくくなります。以下に、セキュリティシステムをより安全に作成する方法に関するヒントと推奨事項をいくつか示します。

基本的な機器ネットワークセキュリティのために取るべき必須の措置:

1. 強力なパスワードの使用

   パスワードを設定するには、次の提案を参照してください:

   - 長さは8文字未満にすることはできません;
   - 文字種には、大文字、小文字、数字、記号の2種類以上を含みます;
   - アカウント名またはアカウント名を逆の順序で含めないでください;
   - 123、abcなどの連続した文字は使用しないでください。;
   - 111、aaaなど、重複する文字は使用しないでください。;

2. ファームウェアとクライアントソフトウェアを時間単位で更新します

   - テクニカル業界の標準手順に従って、お使いの機器(NVR、CVIレコーダー、IPカメラなど)のファームウェアを最新の状態に保ち、システムに最新のセキュリティパッチと修正が確実に適用されるようにすることをお勧めします。本器をパブリックネットワークに接続する場合は、アップデートの自動チェック機能を有効にして、メーカーがリリースしたファームウェアアップデートのタイムリーな情報を取得することをお勧めします。

1. 物理的保護

   機器、特にストレージデバイスに対して物理的な保護を実行することをお勧めします。

   例えば、装置を特別なコンピュータルームやキャビネットに設置し、十分に完了したアクセス制御許可や鍵管理を実施して、ハードウェアの破損、リムーバブル装置(USB、シリアルポートなど)の不正な接続などの物理的な接触を許可されていない人員が行うことを防止します。

2. パスワードを定期的に変更します

   パスワードを定期的に変更して、推測または解読されるリスクを減らすことをお勧めします。

3. パスワードの設定と更新による情報のタイムリーなリセット

   本器はパスワードリセット機能に対応しています。エンドユーザーのメールボックスやパスワード保護の質問など、パスワードリセットの関連情報を時間単位で設定してください。情報が変更された場合は、時間内に修正してください。パスワード保護の質問を設定する場合は、簡単に推測できるものを使用しないことをお勧めします。

4. アカウントロックを有効にします

   アカウントロック機能はデフォルトで有効になっており、アカウントセキュリティを保証するためにオンにしておくことをお勧めします。攻撃者が間違ったパスワー

ドで何度かログインしようとすると、対応するアカウントと送信元IPアドレスがロックされます。

5. デフォルトのHTTPおよびその他のサービスポートの変更
   デフォルトのHTTPおよびその他のサービスポートを1024～65535の任意の数字のセットに変更することをお勧めします。これにより、外部者が使用しているポートを推測できるリスクが軽減されます。
6. HTTPSの有効化
   安全な通信チャネルを介してWebサービスにアクセスできるように、HTTPSを有効にすることをお勧めします。
7. ホワイトリストの有効化
   ホワイトリスト機能を有効にして、指定したIPアドレスを除くすべてのユーザーがシステムにアクセスできないようにすることをお勧めします。そのため、必ずコンピュータのIPアドレスと付属機器のIPアドレスをホワイトリストに追加してください。
8. MACアドレスバインディング
   ゲートウェイのIPアドレスとMACアドレスを機器にバインドすることをお勧めします。これにより、ARPのリスクが軽減されます。
9. 適切なアカウントと権限の割り当て
   ビジネスおよび管理の要件に従って、合理的にユーザーを追加し、それらに最小限の権限セットを割り当てます。
10. 不要なサービスの無効化と安全モードの選択
    不要な場合は、SNMP、SMTP、UPnPなどの一部のサービスをオフにしてリスクを軽減することをお勧めします。
    必要に応じて、以下のサービスを含むセーフモードを使用することを強くお勧めします:
    - SNMP:SNMP v3を選択し、強力な暗号化パスワードと認証パスワードを設定します。
    - SMTP:メールボックスサーバにアクセスするには、TLSを選択します。
    - FTP:SFTPを選択し、強力なパスワードを設定します。
    - APホットスポット:WPA2-PSK暗号化モードを選択し、強力なパスワードを設定します。
11. 音声・映像暗号化伝送
    オーディオとビデオのデータコンテンツが非常に重要または機密である場合は、伝送中にオーディオとビデオのデータが盗まれるリスクを減らすために、暗号化された伝送機能を使用することをお勧めします。
    注意:暗号化された送信は、送信効率に多少の損失をもたらします。

12. セキュア監査
    - オンラインユーザーを確認する:CVIレコーダーが認証なしでログインしているかどうかを確認するために、オンラインユーザーを定期的に確認することをお勧めします。
    - 機器ログの確認:ログを表示することで、機器へのログインに使用されたIPアドレスとそのキー操作を知ることができます。
13. ネットワークログ
    装置の記憶容量が限られているため、保存されるログには制限があります。ログを長時間保存する必要がある場合は、ネットワークログ機能を有効にして、重要なログがトレースのためにネットワークログサーバに確実に同期されるようにすることをお勧めします。
14. 安全なネットワーク環境の構築
    機器の安全性を確保し、潜在的なサイバーリスクを軽減するために、以下をお勧めします:
    - ルータのポートマッピング機能を無効にして、外部ネットワークからイントラネットデバイスに直接アクセスしないようにします。
    - ネットワークは、実際のネットワークのニーズに応じて分割し、隔離する必要があります。2つのサブネットワーク間の通信要件がない場合は、使用することをお勧めします。

      ネットワーク分離効果を実現するために、ネットワークを分割するためのVLAN、ネットワークGAP、およびその他のテクノロジ。
    - プライベートネットワークへの不正アクセスのリスクを軽減するため、802.1xのアクセス認証システムを確立します。
15. デバイスのファイアウォールまたはブロックリストとホワイトリスト機能を有効にして、デバイスが攻撃されるリスクを軽減することをお勧めします。