ネットワークカメラ

不正アクセス防止対策について

重要 管理者の方はご一読ください。

本書では、ネットワークカメラをより安全に利用するための対策を説明しています。
「2022年以降に発売された機種」と「2021年以前に発売された機種」に分けて説明していますので、お使いの機種を次の表からご確認ください。

2022年以降に発売された機種

▶ A-1 ページ

VB-H47

VB-M46

VB-S32VE

VB-S32D

VB-S820D

VB-S920F

2021年以前に発売された機種

▶ B-1 ページ

ME20F-SHN

VB-H

VB-H761LVE-H / VB-H761LVE / VB-H760VE / H751LE-H / VB-H751LE / VB-H730F Mk II / VB-H730F / VB-H710F / VB-H652LVE / VB-H651VE / VB-H651V / VB-H630VE / VB-H630D / VB-H610VE / VB-H610D / VB-H45 / VB-H43 / VB-H41

VB-M

VB-M741LE-H / VB-M741LE / VB-M740E / VB-M720F / VB-M700F / VB-M641VE / VB-M641V / VB-M640VE / VB-M640V / VB-M620VE / VB-M620D / VB-M600VE / VB-M600D / VB-M50B / VB-M44 / VB-M42 / VB-M40

VB-R

VB-R13VE / VB-R13 / VB-R12VE / VB-R11VE / VB-R11/ VB-R10VE

VB-S

VB-S910F / VB-S905F Mk II / VB-S905F / VB-S900F Mk II / VB-S900F / VB-S805D Mk II / VB-S805D / VB-S800D Mk II / VB-S800VE / VB-S800D / VB-S31D Mk II / VB-S31D / VB-S30D Mk II / VB-S30VE

日本語

2022年以降に発売された機種

この章では次の機種を説明しています。次の機種以外のネットワークカメラについては「2021年以前に発売された機種」を参照してください。

VB-H47

VB-M46

VB-S32VE

VB-S32D

VB-S820D

VB-S920F

目次

はじめに

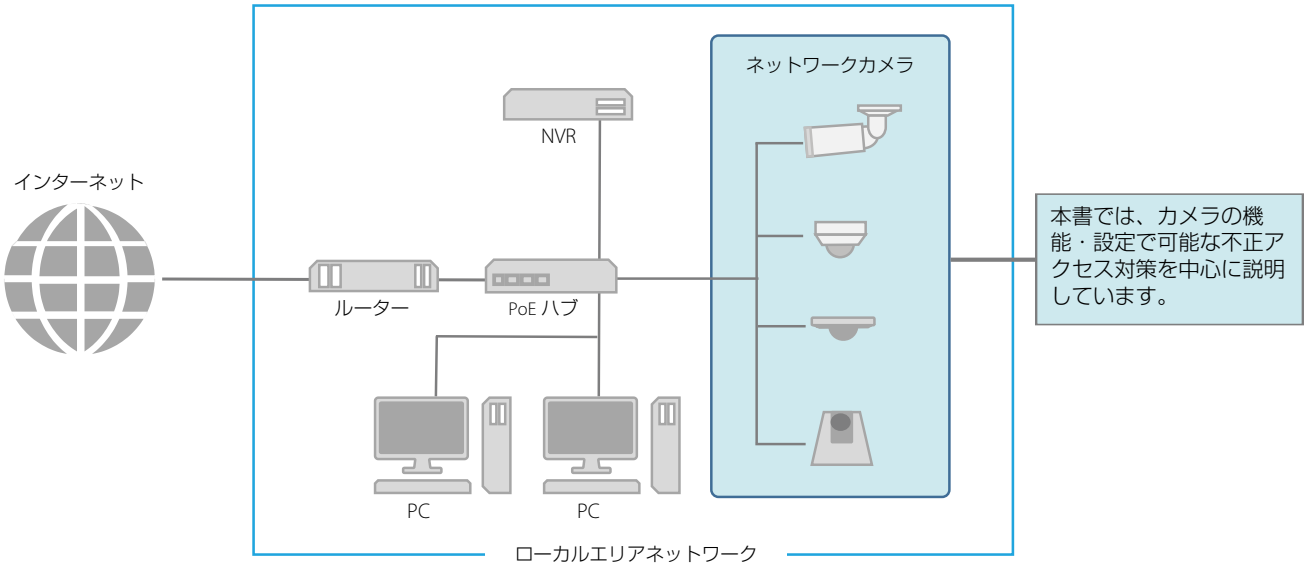
ネットワークにつながる機器は、意図しない第三者 (以下、第三者) からの不正アクセスなど、サイバー攻撃の標的になる可能性があります。特にネットワークカメラは、多様なサーバー機能を搭載しているため、便利である一方、セキュリティ対策を実施せずに運用すると、第三者からの攻撃の対象となる危険性を含んでいます。このような危険性を完全に取り除くことは難しいですが、さまざまな角度からリスクについて検討し、セキュリティポリシーに基づいた対策を講じることで、第三者からの攻撃を受ける可能性を減らすことができます。

本書では、キヤノンネットワークカメラ (以下、カメラ) をお使いのすべてのお客様を対象に、カメラに設定する不正アクセス対策について説明しています。本書を参考に、お客様の責任の下、お使いの環境に合わせて必要な対策を実施することが、より安全なカメラの運用につながります。

本書について

本書で説明する不正アクセス対策は、主にカメラを対象としており、下図に示すとおりシステム全体の一部となっています。システム全体の不正アクセス対策については、お客様のネットワーク環境や、カメラの使用目的に応じて適切に実施してください。

また、サイバー攻撃以外の物理的な破壊行為やいたずらに対する対策も重要です。たとえば、カメラを接続するケーブルを埋設する、録画装置などは、第三者から隔離して設置する、カメラ廃却時にはカメラの設定を初期化し、メモリーカードの抜き忘れに注意する、などがあげられます。



■ 注意事項と記号について

- 本書ではカメラの設定ページの画面を用いて各対策を説明していますが、お使いのカメラ、ファームウェアバージョンによっては、実際の画面と異なる場合があります。また、各機能の設定および注意事項はカメラの使用説明書の『操作ガイド』に詳しく記載されています。実際にカメラを設定するときは、お使いのカメラの 『操作ガイド』を参照してください。
- 本書の内容の一部または全部を無断で転載することは禁止されています。
- 本書の内容について、将来予告なしに変更することがあります。
- ネットワークのセキュリティ上の問題により発生した直接、間接の損害については、弊社は一切の責任を負いかねます。

本書では重要事項/補足説明などには次の記号を使用して説明しています。

重要 の記号は、重要事項や制限事項が書かれています。必ずお読みください。

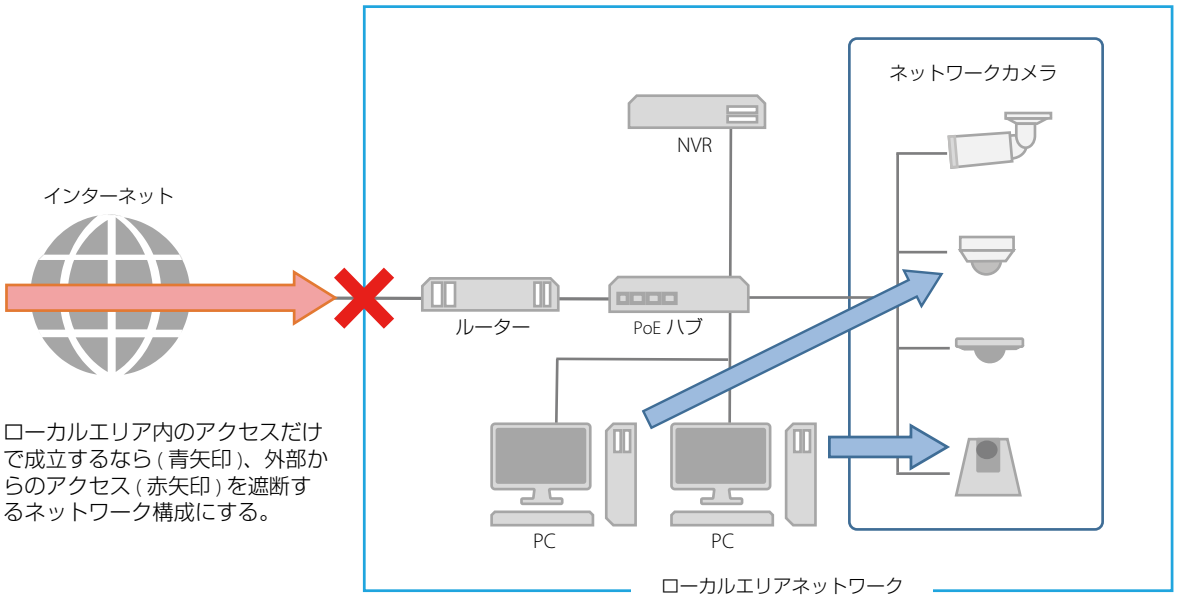
メモ の記号は、操作の参考になることや補足説明が書かれています。

用途に合わせたネットワーク構成で運用する

カメラの機能・設定で可能な不正アクセス対策を説明する前に、ここではカメラの用途に適したネットワーク構成について説明します。ポイントは、カメラに対して外部からのアクセスが必要かどうかです。

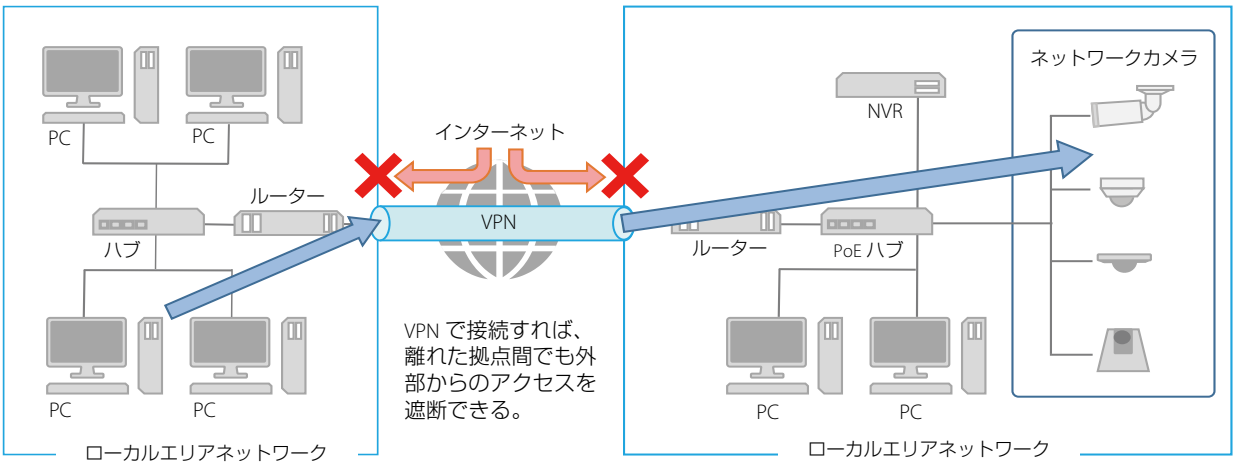
■ 外部からのアクセスを遮断する

カメラの映像を確認したり、設定変更する際に、インターネットなどの外部ネットワークからのアクセスが不要な場合、外部からのアクセスを物理的、論理的に遮断することが、セキュリティリスクを軽減するうえで有効です。
遠隔地からのアクセスが不要で、カメラにアクセスする機器を限定できる場合は、カメラは同じローカルエリアネットワーク内にある特定の機器からのアクセスに限定することがセキュリティ強化につながります。遠隔地からカメラにアクセスする必要がある場合は、外部からのアクセスを遮断できるVPNの利用など、安全に通信できる方法を導入することが重要です。



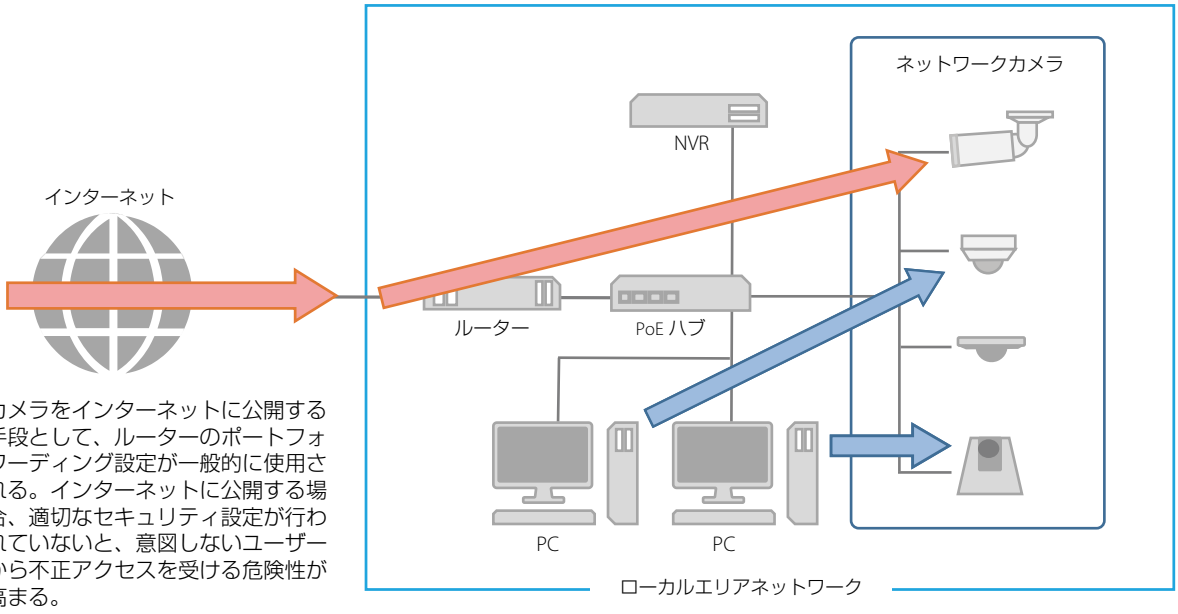
VPN とは？

VPN とは Virtual Private Network (仮想プライベートネットワーク) の略で、通信経路に仮想的なトンネルを作り、その中で安全にデータをやり取りするしくみのことです。本社や支店などの拠点間のローカルエリアネットワークを VPN で接続することで、外部ネットワークからのアクセスを遮断することができます。



■ 外部アクセス可能なネットワークには万全な対策をする

風景を配信するライブカメラなど、不特定多数に映像を配信するケースでは、インターネットなどの外部ネットワークと接続し、カメラに外部からアクセスできるよう、インターネットに公開する必要があります。



カメラをインターネットに公開する手段として、ルーターのポートフォワーディング設定が一般的に使用される。インターネットに公開する場合、適切なセキュリティ設定が行われていないと、意図しないユーザーから不正アクセスを受ける危険性が高まる。

外部からのアクセスを可能とするネットワークは、利便性が高い反面、ネットワーク上の機器が不正アクセスを受けるリスクが高まります。そのため、このようなネットワーク構成の場合、本書で説明している対策だけでなく、ネットワーク内の各機器の認証設定や各通信の暗号化など、システム全体に対して十分な対策を実施して、セキュリティを確保することが重要です。

重要

カメラは電気通信事業者（移動通信会社、固定通信会社、インターネットプロバイダーなど）の通信回線（公衆無線LANを含む）に直接接続することができません。カメラをインターネットに接続する場合は、必ずルーターなどを経由して接続してください。

1章

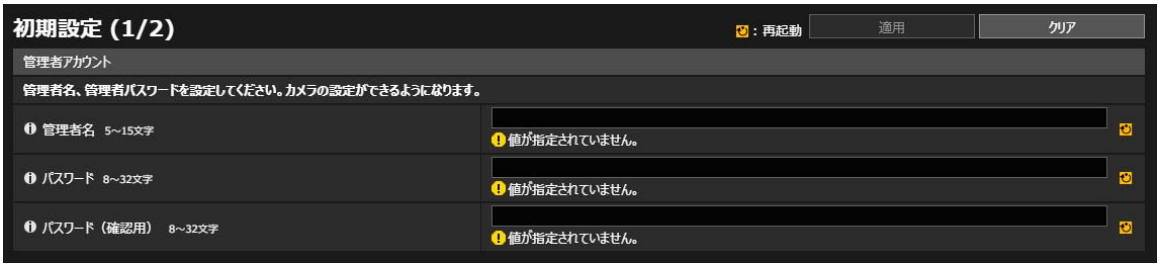
基本的な対策

管理者名とパスワードを設定する

管理者アカウントは、カメラの設定・操作のすべての権限を持つ、アカウントです。管理者アカウントが第三者に不正に使われ、改ざんが行われると、カメラにアクセスできなくなる危険性があります。管理者アカウントのなりすましを防ぐために管理者名とパスワードは、第三者に推測されにくい文字の配列にすることが、カメラを安全に運用するうえで、最も基本的な対策です。また、同じ管理者アカウントを複数のカメラに設定しないなど、管理者アカウントの取り扱いには十分に注意し、厳重に管理してください。

管理者アカウントは、カメラの初回起動時に設定が必要です。また設定後は、カメラの設定ページ、[セキュリティ] > [ユーザー管理] で変更できます。

管理者アカウントは、カメラへの初回アクセス時、[初期設定] で設定します。



管理者名とパスワードは、カメラの設定ページ、[セキュリティ] > [ユーザー管理] でも変更できます。

■ 安全な管理者名とパスワードのポイント

管理者名とパスワードを強化するためには、次の点を考慮してください。

- 英数字、またはカメラで許可されている記号や特殊文字を組み合わせ、少なくとも10文字以上にする
- 大文字と小文字を組み合わせる
- 一般的に使用されている言葉や文字列など、推測されやすいものを避ける

■ 管理者アカウント以外のパスワード

カメラには、管理者アカウント以外にも、登録ユーザー (p. A-12)、サーバー認証、暗号化のためにパスワードを設定します。これらのパスワードも第三者に推測されにくい文字の配列で設定し、適切に管理してください。

最新ファームウェアを利用する

カメラのファームウェアは、機能の性能向上や不具合の修正のため、随時、更新されます。セキュリティの観点からも、既知の脆弱性への対策が施されているため、常に最新にしておくことが重要です。

カメラ購入後の初期設定時、運用時など、お客様がご使用の環境に合わせて、最新のファームウェアが提供されているか、定期的にキヤノンのWebサイトをご確認ください。
なお、ファームウェアのバージョンは、カメラの設定ページ、[メンテナンス] > [機器情報] の [ファームウェアバージョン] で確認できます。

ファームウェアは、カメラの設定ページ、[メンテナンス] > [ファームウェア更新] の [ファームウェア更新] で更新します。

カメラマネジメントツールを使って、ファームウェアを更新することもできます。
カメラマネジメントツールの詳細については、『カメラマネジメントツール 使用説明書』を参照してください。

日付と時刻を設定する

カメラには、正確な日付と時刻を設定してください。不正アクセスが疑われるような兆候があったときは、ログを確認することで、発生した日付と時刻の確認ができる場合もあります。

日付と時刻は、カメラの設定ページ、[システム] > [日付と時刻] の [設定] で設定します。

ログを確認する

カメラの接続状態や動作状況は記録され、ログとしてカメラ本体とメモリーカードに保存されます。ユーザー認証失敗の繰り返しなど、不正アクセスが疑われるような兆候がないか、早期に発見するためにも、定期的にログを確認してください。ログの詳細については、カメラの『操作ガイド』を参照してください。

■ ログの保存先と種類

カメラ本体とメモリーカードでは、保存されるログの内容が異なります。

カメラ本体に保存されるログ：エラーログ、警告ログ、情報ログ

– 再起動、初期化、工場出荷設定に戻す、の操作を行うと、エラーログの発生日時とエラー番号を除き、消去されます。
また、一定のサイズを超過した場合はすべて消去されます。

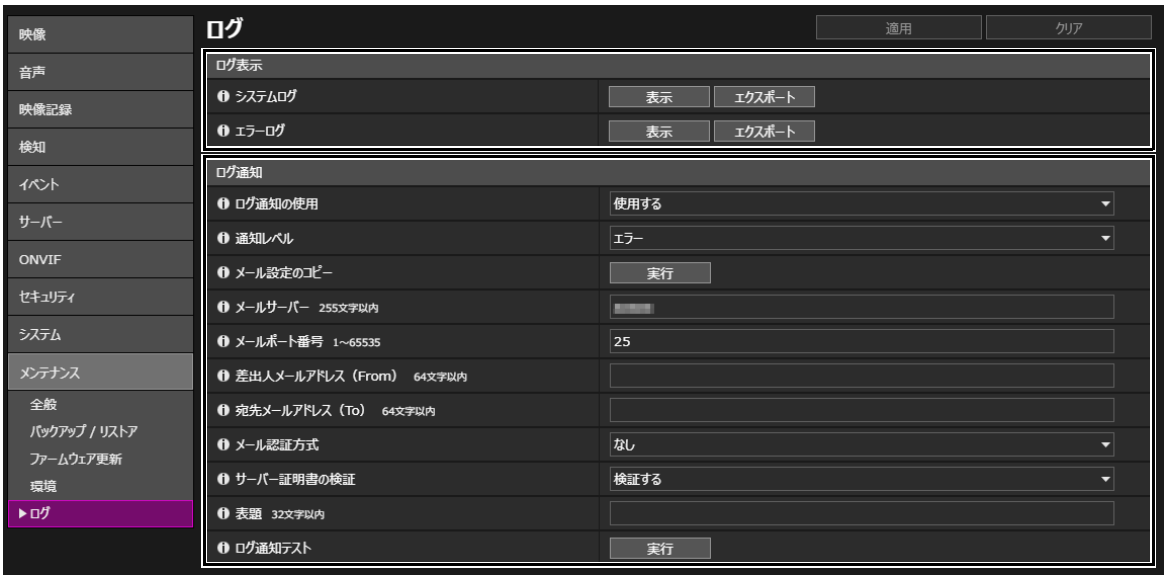
メモリーカードに保存されるログ：エラーログ、一部の警告ログ・情報ログ

– 再起動、初期化、工場出荷設定に戻す、の操作を行っても消去されません。

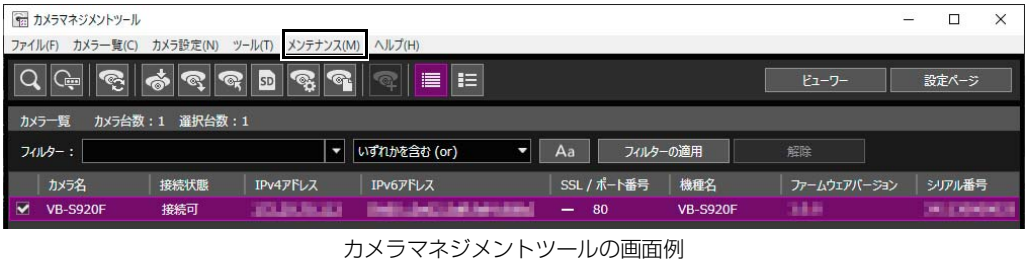
■ ログの表示、通知、ダウンロード

カメラ本体に保存されたログは、設定ページの [ログ表示] で確認できます。また、[ログ通知] を使用すると、[エラー]、[エラーと警告] など設定した通知レベルに応じてユーザーに通知することも可能です。
カメラマネジメントツールを使用すると、カメラ本体とメモリーカードそれぞれに保存されたログが、ログファイルとしてダウンロードできます。

ログは、カメラの設定ページで表示・設定します。
[メンテナンス] > [ログ] > [ログ表示]
[メンテナンス] > [ログ] > [ログ通知]



ログファイルは、カメラマネジメントツール、[メンテナンス] > [ログのダウンロード] で ダウンロードします。



カメラマネジメントツールの画面例

■ ログの内容

ログのレベル、コード、障害の程度、分類は次のとおりです。

ログ	レベル	コード	障害の程度	分類
エラーログ	エラー	4xx 例) S410 イベントサービスの初期化エラー	ソフトレベルの異常 (タスク動作停止)	[crit]
エラーログ	エラー	3xx 例) S302 設定値の保存エラー	動作に支障のある異常 (動作継続)	[err]
警告ログ	警告	2xx 例) S220 PAN/TILT動作警告	動作に支障のない異常	[warning]
警告ログ	警告	1xx 例) H144 パスワードの指定異常	システム外部の異常	[notice]
通知ログ	情報	0xx 例) S001 システムの起動	正常動作に関する情報	[info]

2章

ご利用環境に応じた対策

カメラにアクセスするアカウントを管理する [ユーザー管理]

カメラにアクセスできるアカウントには、「管理者」「登録ユーザー」「一般ユーザー」の3種類があります。
管理者は、カメラのすべての設定・操作ができるアカウントです。設定ページにアクセスできるのも、管理者のみとなります。そのため、管理者アカウントの情報は、第三者に漏えいしないよう、厳重に管理することが重要です。
管理者以外の登録ユーザーと一般ユーザーは、カメラビューワーにアクセスできるユーザーです。登録ユーザーと一般ユーザーでできることを理解し、必要最低限のユーザー設定や権限の付与を行ってください。

■ ユーザー認証が必要な登録ユーザー

管理者を除く特定のユーザーのみがカメラビューワーにアクセスできるようにするには、登録ユーザーを設定します。
登録ユーザーの設定では、アカウント情報 (ユーザー名とパスワード) を登録し、カメラビューワーの権限 (映像配信のみ許可する、カメラの制御も許可する、など) を付与します。すべての登録ユーザーに同じ権限が付与され、また特権カメラ制御など管理者に近いカメラ制御まで設定可能となるため、登録ユーザーへの権限付与は慎重に行う必要があります。
定期的に登録ユーザーの見直しを行い、常に必要最低限のユーザーと権限が付与された状態になるように管理してください。
登録ユーザーにのみアクセスを限定したい場合は、後述する一般ユーザーの権限をすべて無効にすることが重要です。これらを無効にしない限り、せっかく登録ユーザーを設定していても、一般ユーザーからのアクセスを許可していることになります。

■ 一般ユーザーはゲストアカウント

一般ユーザーとは、ユーザー名とパスワードを必要としない、ゲストアカウントのことです。一般ユーザーの権限を有効にすると、カメラビューワーにアクセスする際にユーザー認証を必要とせず、誰でもアクセス可能となります。また、カメラ制御や映像配信のコマンドを、認証なしで受け付けるようになります。したがって、一般ユーザーの権限は、カメラの利用目的が不特定多数に向けての映像の一般公開などの場合のみに設定し、それ以外では一般ユーザーの権限はすべて無効にしてください。
登録ユーザー同様、すべての一般ユーザーには同じ権限が付与されますので、一般ユーザーのアクセスを許可する場合は、必要最低限の権限のみを付与してください。

ユーザー管理は、カメラの設定ページ、[セキュリティ] > [ユーザー管理] > [登録ユーザーアカウント] / [ユーザー権限] で設定します。

一般ユーザー権限を無効にするには、すべてのチェックを外します。

■ カメラビューワーのユーザー認証設定

カメラビューワーにアクセスするときのユーザー認証の有無を設定することができます。ただし、ここでのユーザー認証設定はカメラビューワーでのみ有効であり、他のアプリケーションやビューワーなどでカメラにアクセスする場合には適用されません。したがって、すべてのアクセスにユーザー認証を行いたい場合は、[ユーザー認証] を [認証する] にしたうえで、前述したとおり一般ユーザーの権限をすべて無効にしておくことが重要です。

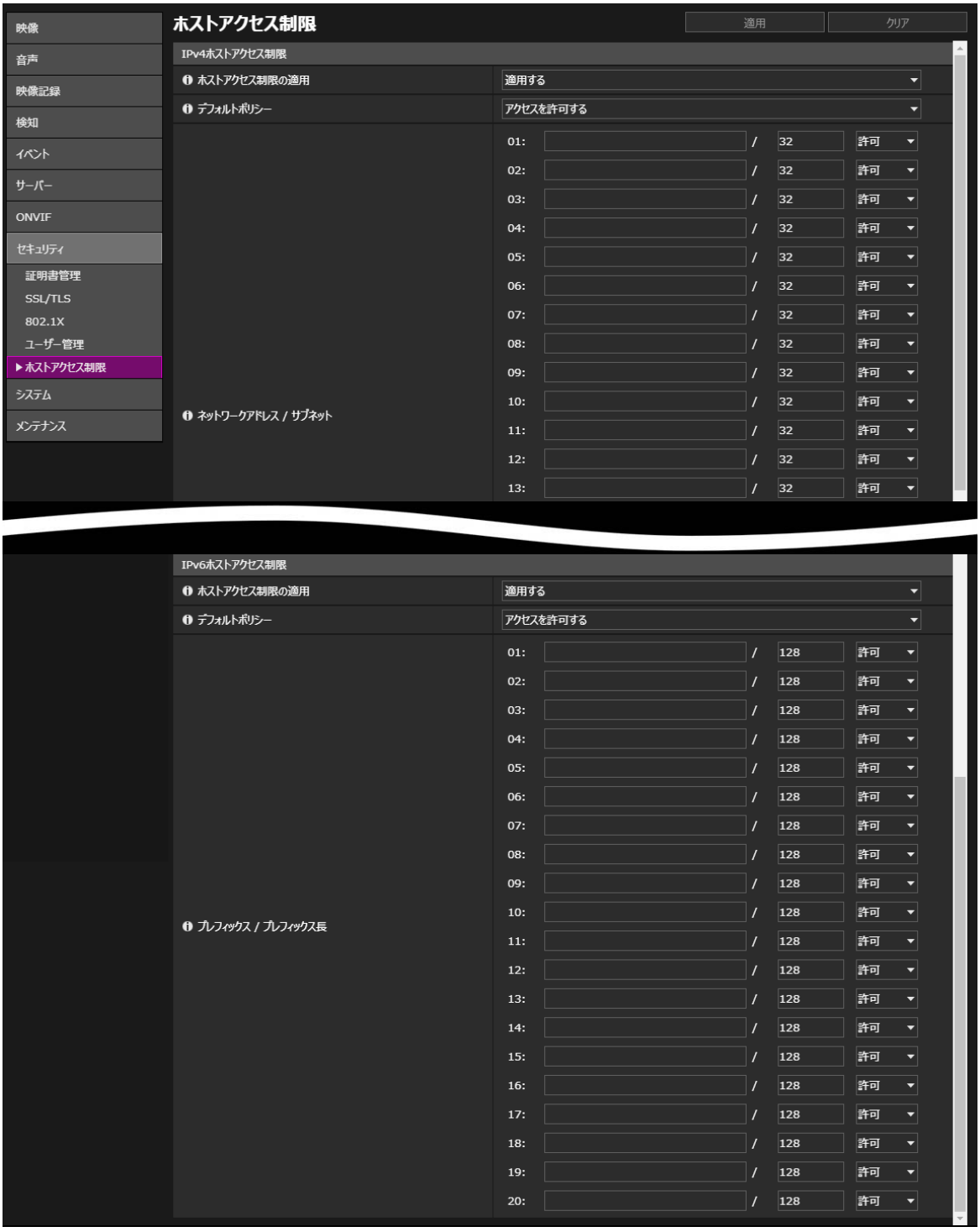
カメラビューワーのユーザー認証は、カメラの設定ページ、[システム] > [ビューワー] > [ビューワー設定] の [ユーザー認証] で設定します。

カメラにアクセスするホストを制限する [ホストアクセス制限]

カメラにアクセスできるホストを制限することにより、第三者から不正にアクセスされるリスクを軽減させることができます。

アクセスするホストを制限するには、指定したホストとの通信だけを許可し、それ以外の通信は禁止します。逆に、指定したホストとの通信だけを禁止し、それ以外の通信は許可する方法もあります。
利用環境に応じて、アクセス制限の範囲をネットワーク単位でまとめたり、ホスト単位に限定して設定することも可能です。ただし、誤って管理者のIPアドレスを通信禁止に設定してしまうと、管理者からのカメラへのアクセスが禁止され、工場出荷設定に戻す以外に復旧する手段がなくなることがありますので、設定には十分ご注意ください。

ホストアクセス制限は、カメラの設定ページ、[セキュリティ] > [ホストアクセス制限] > [IPv4ホストアクセス制限] / [IPv6ホストアクセス制限] で設定します。



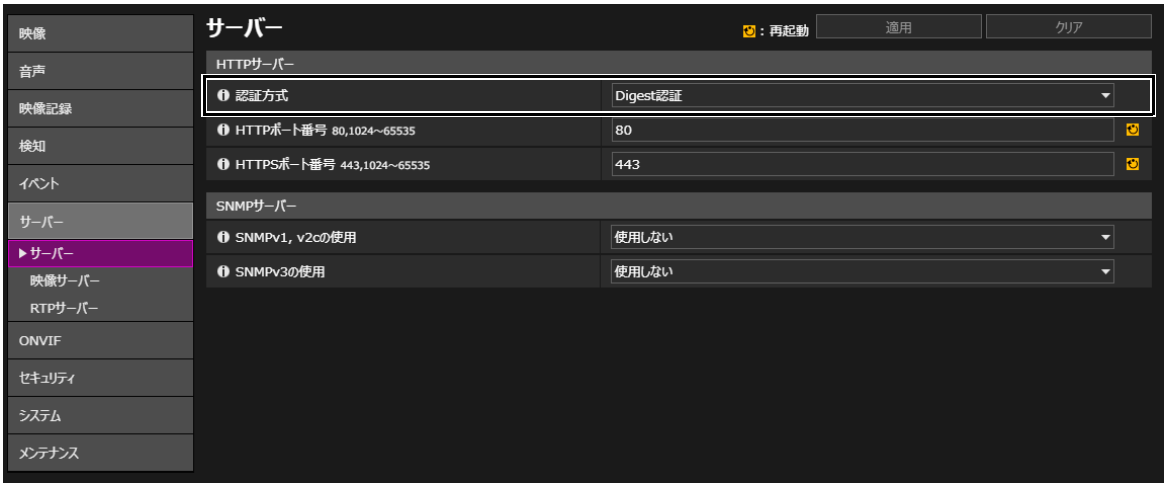
Digest (ダイジェスト) 認証を設定する

カメラにアクセスするときの [HTTPサーバー] と [RTPサーバー] の認証方式は、[Digest認証] に設定してください。[Basic認証] を選択すると、ネットワーク上でパスワードが暗号化されずに送信されるため、第三者による盗聴が行われた場合に、パスワードが容易に第三者に漏れてしまうことになります。

HTTPサーバーとRTPサーバーの認証方式は、個別に設定が必要です。また、使用するアプリケーションがDigest認証に対応していることを確認してください。

■ Digest認証 (HTTP)

HTTPサーバーの認証方式は、カメラの設定ページ、[サーバー] > [サーバー] > [HTTPサーバー] の [認証方式] で設定します。



■ Digest認証 (RTSP)

RTPサーバーのRTSP認証方式は、カメラの設定ページ、[サーバー] > [RTPサーバー] > [RTPサーバー] の [RTSP認証方式] で設定します。

ポート番号を変更する

カメラへの不正なアクセスを防ぐには、不特定のアクセスを制限することが重要です。ポート番号は、カメラと外部機器との通信の出入口であり、通信プロトコルごとに番号が設定されています。それぞれのポート番号は、ネットワーク機器間で広く共通の番号が使われているため接続性が高い反面、第三者の不正な侵入に利用される危険性があります。
セキュリティの懸念により、ポート番号を変更する場合は、他の通信プロトコルとポート番号が重複しないことを確認のうえ、指定された範囲で設定してください。ポート番号を変更した場合、カメラにアクセスするためには、IPアドレスの他にポート番号を指定する必要があります。

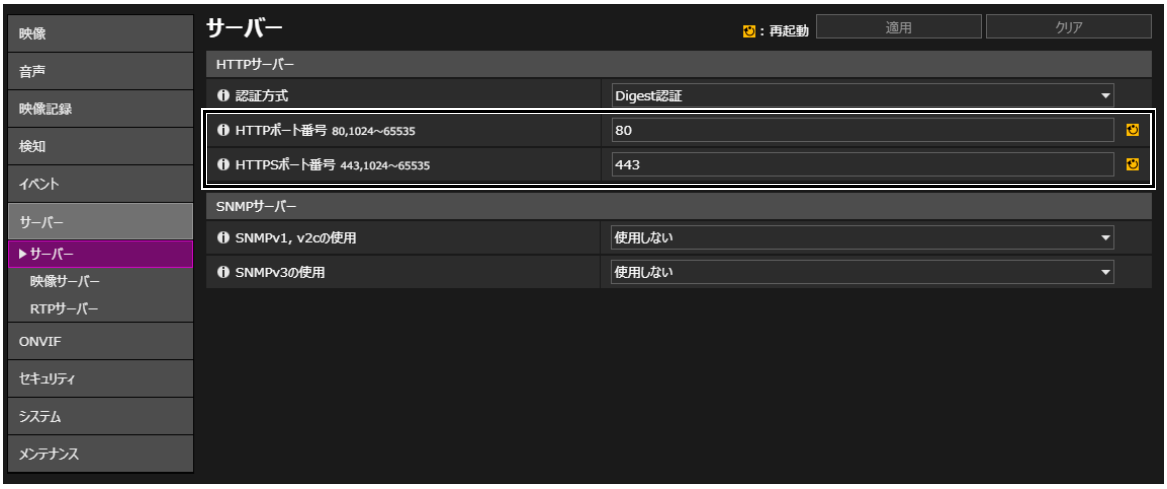
■ ポート番号の変更 (例)

HTTPSで接続する場合、「https:// {カメラのIPアドレス} : {ポート番号}」と指定してください。

HTTPSポート番号が10443に変更されている場合
https://192.168.100.1:10443

■ HTTP ポート番号/HTTPS ポート番号

HTTP/HTTPSのポート番号は、カメラの設定ページ、[サーバー] > [サーバー] > [HTTPサーバー] で設定します。



次のポート番号も変更可能です。

■ RTSP ポート番号

RTSPポート番号は、カメラの設定ページ、[サーバー] > [RTPサーバー] > [RTPサーバー] で設定します。

■ マルチキャストポート番号

マルチキャストポート番号は、カメラの設定ページ、[サーバー] > [RTPサーバー] で設定します。
[音声設定1/2] > [マルチキャストポート番号]
[RTPストリーム 1/2/3/4/5] > [マルチキャストポート番号]

通信を暗号化する [SSL/TLS]

カメラと外部機器との間で安全な通信を行うためには、すべての通信をHTTPS接続 (SSL/TLSとHTTPを組み合わせた暗号化通信) にすることをおすすめします。SSL (Secure Sockets Layer) / TLS (Transport Layer Security) とは、ネットワーク上で通信を暗号化し、第三者による通信内容の盗聴や改ざんを抑止する技術です。万一、通信の途中でデータが盗聴されたとしても、適切な方法で通信を暗号化しておくことで、データの内容は保護されるため、安全性を確保することができます。

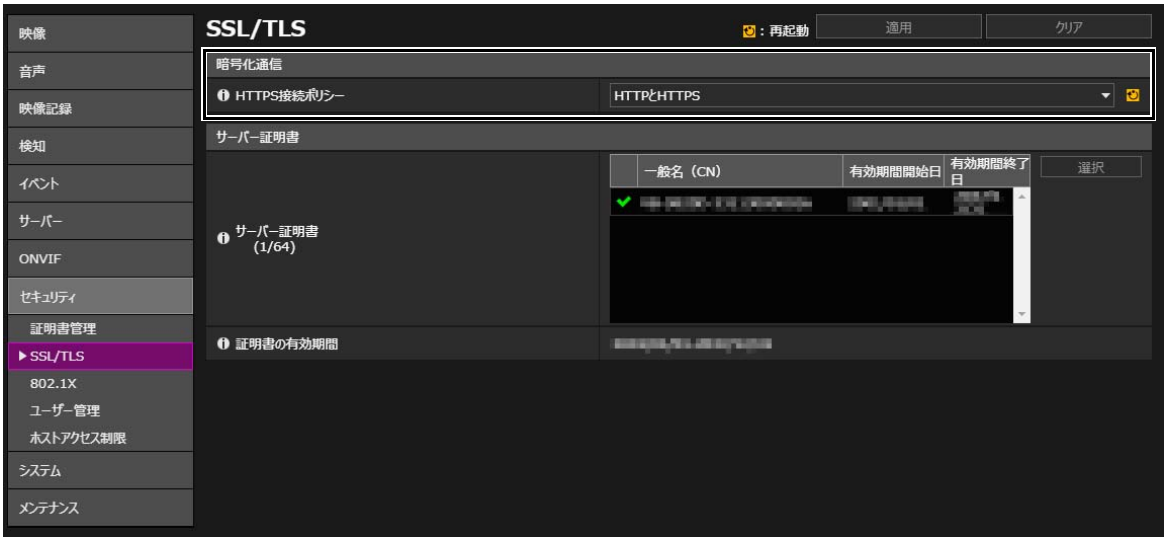
■ 自己署名証明書とサーバー証明書

HTTPS接続での暗号化通信の手段としては、自己署名証明書またはCA局 (証明機関) から発行されるサーバー証明書を使う方法があります。自己署名証明書は、暗号化を行うには十分ですが、Webブラウザーに警告画面が表示されたり、なりすましのリスクが生じます。動作テストなどの場合に使用してください。
本格的なシステム運用時には、CA局から発行されるサーバー証明書を取得し、インポートすることをおすすめします。

また、HTTPSやFTPSを使ってアップロードする際には、CA局から発行されるCA証明書や証明書失効リスト (CRL) をインポートしてサーバー証明書を検証することで、危険なサーバーとの通信を回避し、より安全にサーバーと通信することができます。

証明書のインストールはカメラの設定ページ、[セキュリティ] > [証明書管理] で行います。

HTTPS接続での暗号化通信は、カメラの設定ページ、[セキュリティ] > [SSL/TLS] で設定します。



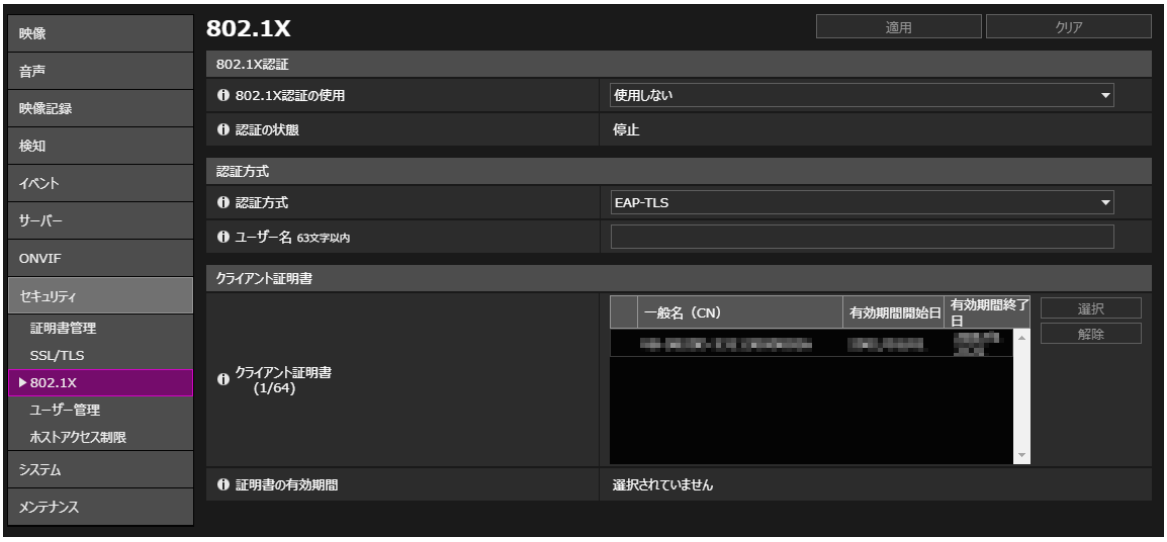
メモ

- 上記HTTPS接続の設定を行っても、RTP/RTSPで配信される映像は自動的に暗号化されません。またアップロードするデータも暗号化できません。これらのデータを安全に通信するためには、システム全体としての対応が必要となります。
- インストールしたCRL証明書は、アップロード時にのみ適用されます。詳しくはカメラの操作ガイドを参照してください。

保護されたネットワークで使用する [802.1X]

IEEE802.1X認証は、あらかじめ決められた機器以外がネットワークにアクセスしないように、認証によって接続を規制する規格です。サーバー認証された機器だけがネットワークに接続できるため、不正なアクセスからネットワークを保護できます。カメラがIEEE 802.1X認証で保護されたネットワークにアクセスできるようにするには、適切な証明書と設定が必要です。

IEEE802.1Xの設定は、カメラの設定ページ、[セキュリティ] > [802.1X] で設定します。



証明書のインストールはカメラの設定ページ、[セキュリティ] > [証明書管理] で行います。

メモ

- IEEE802.1X認証機能をご利用になるには、あらかじめIEEE802.1Xネットワーク環境を構築しておく必要があります。
- 802.1xではCRLをインポートしても、検証は実行されません。

使用しない機能を無効にする

カメラには、さまざまな利用目的やネットワーク環境に対応するための機能が搭載されています。しかし、それらの機能を適切に設定していないと、第三者からの不正アクセスを受ける可能性があります。カメラを安全に使用するためには、使用しない機能の設定を無効にすることも必要です。
運用環境や利用状況において、必要な機能のみ設定を有効にする、設定が終了したら機能を無効にする、などの対応が必要な機能について、次に説明します。

■ AutoIP

[AutoIPの使用] を有効にすると、DHCPサーバーがない環境においても、IPv4リンクローカルアドレス (169.254. xxx.xxx) がカメラに割り当てられます。そのため、このIPv4アドレスと同じセグメントにPCを所属させ、カメラマネジメントツールを使用すれば、カメラが検出され、初期設定をすることができます。
工場出荷設定では、[AutoIPの使用] が有効になっていますが、第三者に不正な目的で使用されないように、ネットワークの初期設定が終了したら無効にすることをおすすめします。

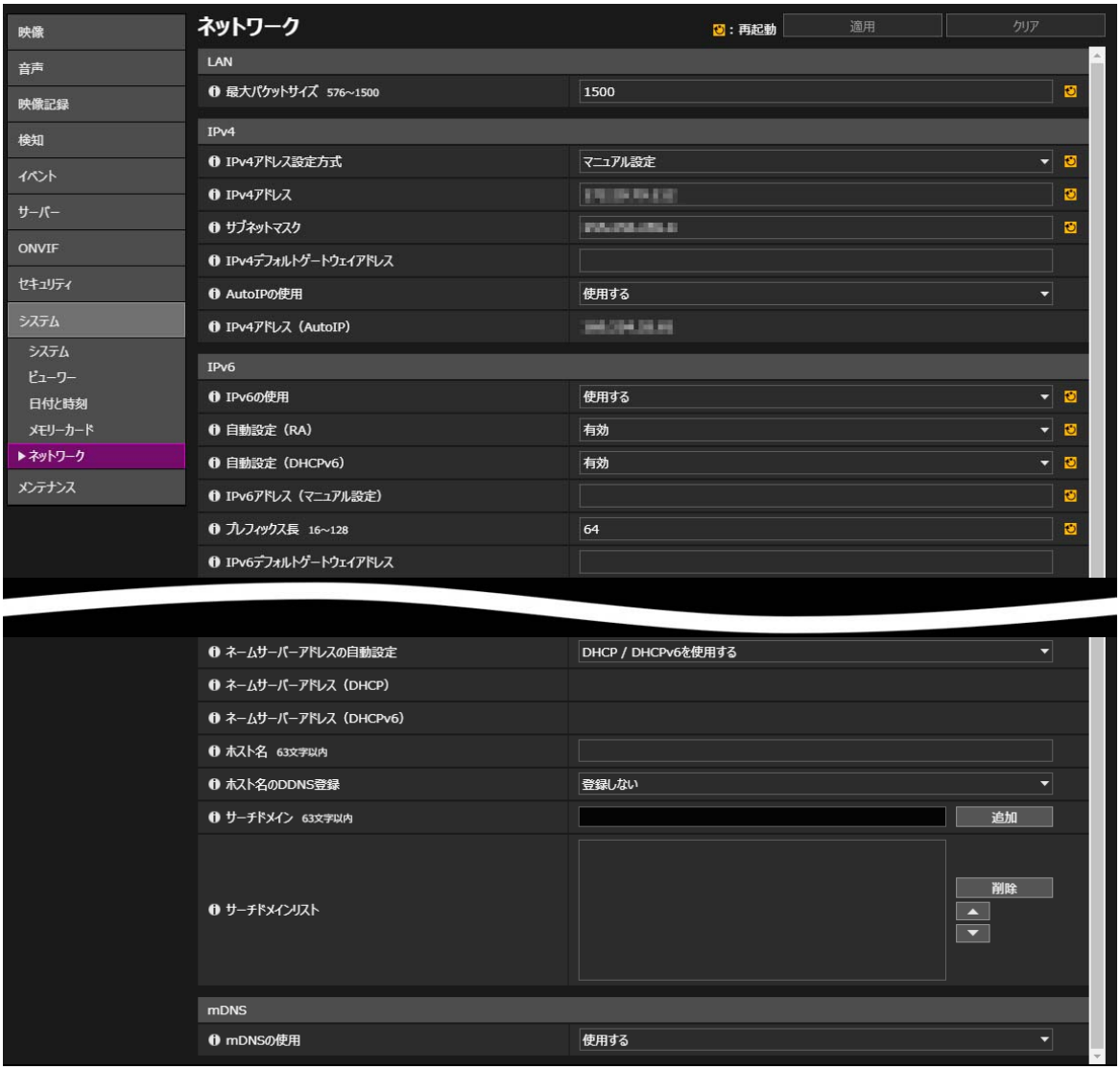
AutoIPは、カメラの設定ページ、[システム] > [ネットワーク] > [IPv4] の [AutoIPの使用] で設定します。

[AutoIPの使用] 工場出荷設定：[使用する]

■ mDNS (multicast Domain Name System)

[mDNS] は、DNSサーバーがない環境でもカメラが検出されるように、ネットワーク上の機器にカメラのIPアドレスとホスト名の情報を一斉に通知する機能です。
工場出荷設定では、[mDNS] の設定が有効になっていますが、第三者に不正な目的で使用されないように、ネットワークの初期設定が終了したら、無効にすることをおすすめします。

mDNSは、カメラの設定ページ、[システム] > [ネットワーク] > [mDNS] で設定します。



[mDNSの使用] 工場出荷設定 : [使用する]

■ SNMP (Simple Network Management Protocol)

[SNMPサーバー] を使用すると、SNMPマネージャーからカメラ (SNMPエージェント) を監視または制御できます。SNMPv3は、認証情報であるユーザー名とパスワードを暗号化して通信することができます。SNMPによる管理を行う場合は、SNMPv1とSNMPv2cに比べ、より安全な通信であるSNMPv3を選択し、暗号化パスワードを設定してください。SNMPv1とSNMPv2cは、運用される環境において必要な場合にのみ、セキュリティ面の安全性が確保されたネットワーク内でご利用ください。

SNMPサーバーは、カメラの設定ページ、[サーバー] > [サーバー] > [SNMPサーバー] で設定します。

[SNMPv1, v2cの使用] 工場出荷設定 : [使用しない]
[SNMPv3の使用] 工場出荷設定 : [使用しない]

■ RTP (Real-time Transport Protocol)

[RTPサーバー] を使用すると、映像や音声を指定したマルチキャストアドレスにも配信できます。カメラと接続する録画システムやビューワーが、RTPプロトコルを必要としない場合は、[RTPの使用] を [使用しない] にすることをおすすめします。

RTPサーバーは、カメラの設定ページ、[サーバー] > [RTPサーバー] > [RTPサーバー] で設定します。

[RTPの使用] 工場出荷設定 : [使用する]

付録

カメラを廃棄するときに

カメラを廃棄するときは、カメラを初期化して、ネットワーク設定や管理者アカウントなどの設定情報をすべて消去してください。また、メモリーカードの抜き忘れにも十分ご注意ください。
カメラの初期化は、設定ページ、[メンテナンス] > [全般] の [初期化] で実施します。廃棄の際は、[ネットワーク設定および管理情報] を [保持しない] に設定してください。また、設定ページにアクセスできないときは、カメラ本体のリセットスイッチを操作して、工場出荷設定に戻してください。
本体リセットスイッチの操作は、カメラの機種ごとに異なるため、『操作ガイド』を参照してください。

バックアップ情報を暗号化する

カメラ設定値のバックアップ情報は、設定値を復元 (リストア) させる際に利用します。バックアップ情報に [暗号化パスワード] を設定することで、より安全に管理することができます。
設定したパスワードの取り扱いには十分ご注意ください。

バックアップ情報の暗号化は、カメラの設定ページ、[メンテナンス] > [バックアップ/リストア] > [バックアップ/リストア] で設定します。

2021年以前に発売された機種

この章では次の機種を説明しています。次の機種以外のネットワークカメラについては「2022年以降に発売された機種」を参照してください。

ME20F-SHN

VB-H

VB-H761LVE-H / VB-H761LVE / VB-H760VE / H751LE-H / VB-H751LE / VB-H730F Mk II / VB-H730F / VB-H710F / VB-H652LVE / VB-H651VE / VB-H651V / VB-H630VE / VB-H630D / VB-H610VE / VB-H610D / VB-H45 / VB-H43 / VB-H41

VB-M

VB-M741LE-H / VB-M741LE / VB-M740E / VB-M720F / VB-M700F / VB-M641VE / VB-M641V / VB-M640VE / VB-M640V / VB-M620VE / VB-M620D / VB-M600VE / VB-M600D / VB-M50B / VB-M44 / VB-M42 / VB-M40

VB-R

VB-R13VE / VB-R13 / VB-R12VE / VB-R11VE / VB-R11/ VB-R10VE

VB-S

VB-S910F / VB-S905F Mk II / VB-S905F / VB-S900F Mk II / VB-S900F / VB-S805D Mk II / VB-S805D / VB-S800D Mk II / VB-S800VE / VB-S800D / VB-S31D Mk II / VB-S31D / VB-S30D Mk II / VB-S30VE

目次

はじめに

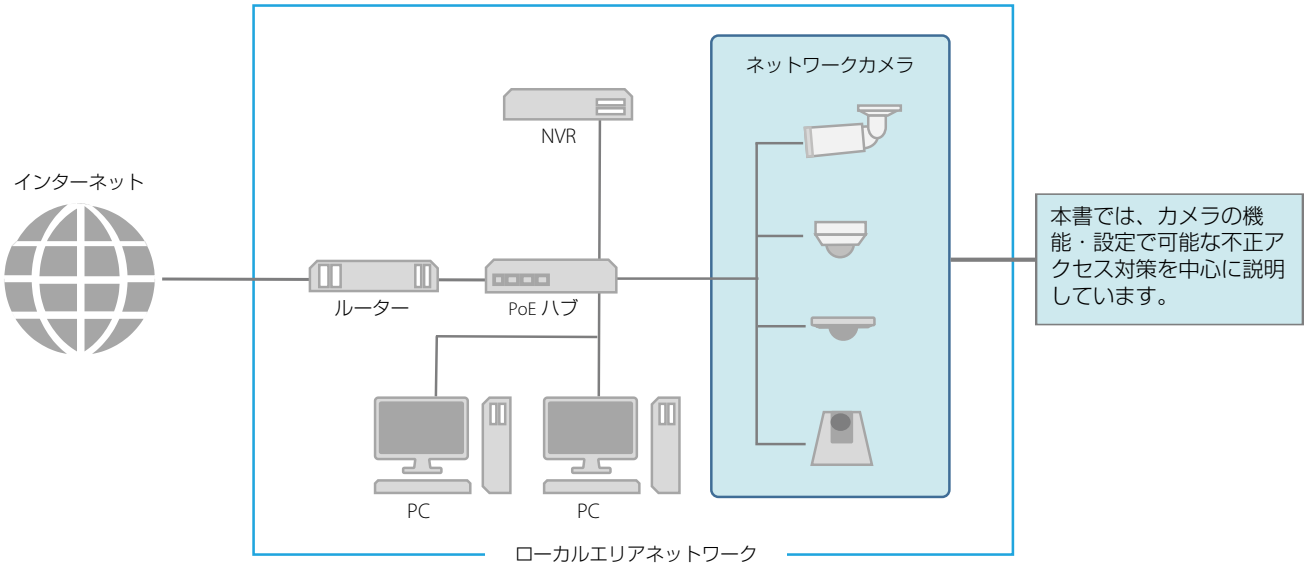
ネットワークにつながる機器は、意図しない第三者 (以下、第三者) からの不正アクセスなど、サイバー攻撃の標的になる可能性があります。特にネットワークカメラは、多様なサーバー機能を搭載しているため、便利である一方、セキュリティ対策を実施せずに運用すると、第三者からの攻撃の対象となる危険性を含んでいます。このような危険性を完全に取り除くことは難しいですが、さまざまな角度からリスクについて検討し、セキュリティポリシーに基づいた対策を講じることで、第三者からの攻撃を受ける可能性を減らすことができます。

本書では、キヤノンネットワークカメラ (以下、カメラ) をお使いのすべてのお客様を対象に、カメラに設定する不正アクセス対策について説明しています。本書を参考に、お客様の責任の下、お使いの環境に合わせて必要な対策を実施することが、より安全なカメラの運用につながります。

本書について

本書で説明する不正アクセス対策は、主にカメラを対象としており、下図に示すとおりシステム全体の一部となっています。システム全体の不正アクセス対策については、お客様のネットワーク環境や、カメラの使用目的に応じて適切に実施してください。

また、サイバー攻撃以外の物理的な破壊行為やいたずらに対する対策も重要です。たとえば、カメラを接続するケーブルを埋設する、録画装置などは、第三者から隔離して設置する、カメラ廃却時にはカメラの設定を初期化し、メモリーカードの抜き忘れに注意する、などがあげられます。



■ 注意事項と記号について

- 本書ではカメラの設定ページの画面を用いて各対策を説明していますが、お使いのカメラ、ファームウェアバージョンによっては、実際の画面と異なる場合があります。また、各機能の設定および注意事項はカメラの使用説明書の『操作ガイド』に詳しく記載されています。実際にカメラを設定するときは、お使いのカメラの 『操作ガイド』を参照してください。
- 本書の内容の一部または全部を無断で転載することは禁止されています。
- 本書の内容について、将来予告なしに変更することがあります。
- ネットワークのセキュリティ上の問題により発生した直接、間接の損害については、弊社は一切の責任を負いかねます。

本書では重要事項/補足説明などには次の記号を使用して説明しています。

重要 の記号は、重要事項や制限事項が書かれています。必ずお読みください。

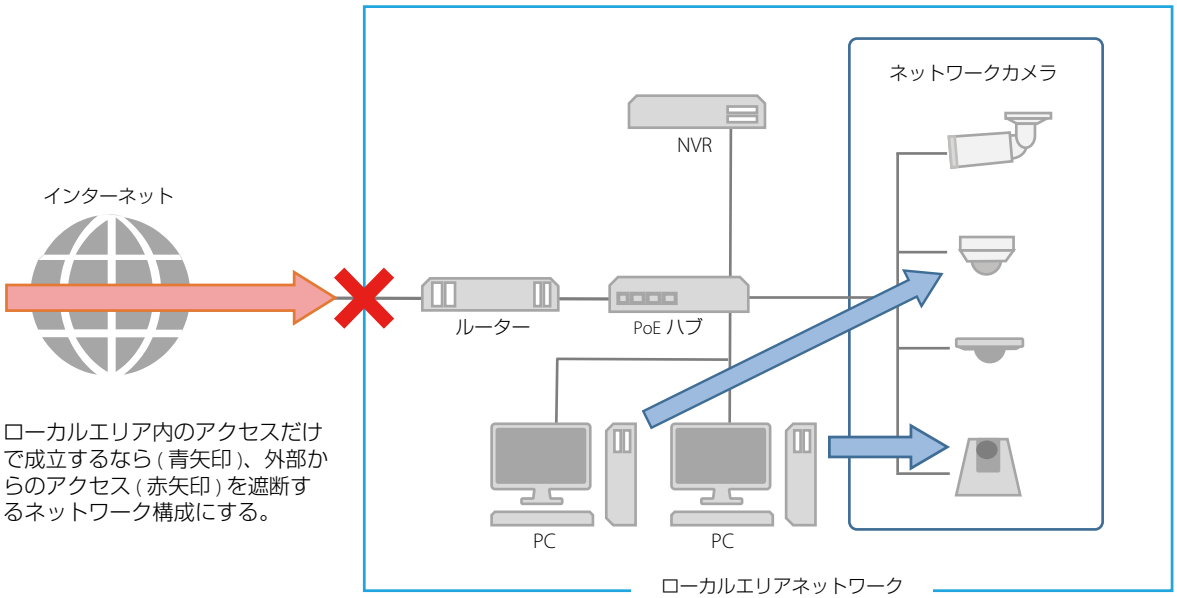
メモ の記号は、操作の参考になることや補足説明が書かれています。

用途に合わせたネットワーク構成で運用する

カメラの機能・設定で可能な不正アクセス対策を説明する前に、ここではカメラの用途に適したネットワーク構成について説明します。ポイントは、カメラに対して外部からのアクセスが必要かどうかです。

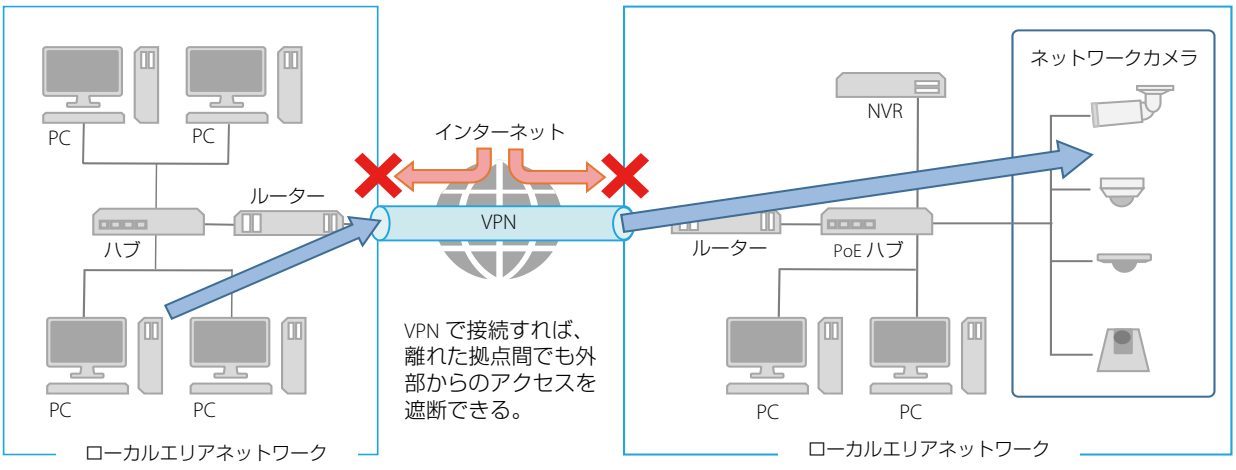
■ 外部からのアクセスを遮断する

カメラの映像を確認したり、設定変更する際に、インターネットなどの外部ネットワークからのアクセスが不要な場合、外部からのアクセスを物理的、論理的に遮断することが、セキュリティリスクを軽減するうえで有効です。
遠隔地からのアクセスが不要で、カメラにアクセスする機器を限定できる場合は、カメラは同じローカルエリアネットワーク内にある特定の機器からのアクセスに限定することがセキュリティ強化につながります。遠隔地からカメラにアクセスする必要がある場合は、外部からのアクセスを遮断できるVPNの利用など、安全に通信できる方法を導入することが重要です。



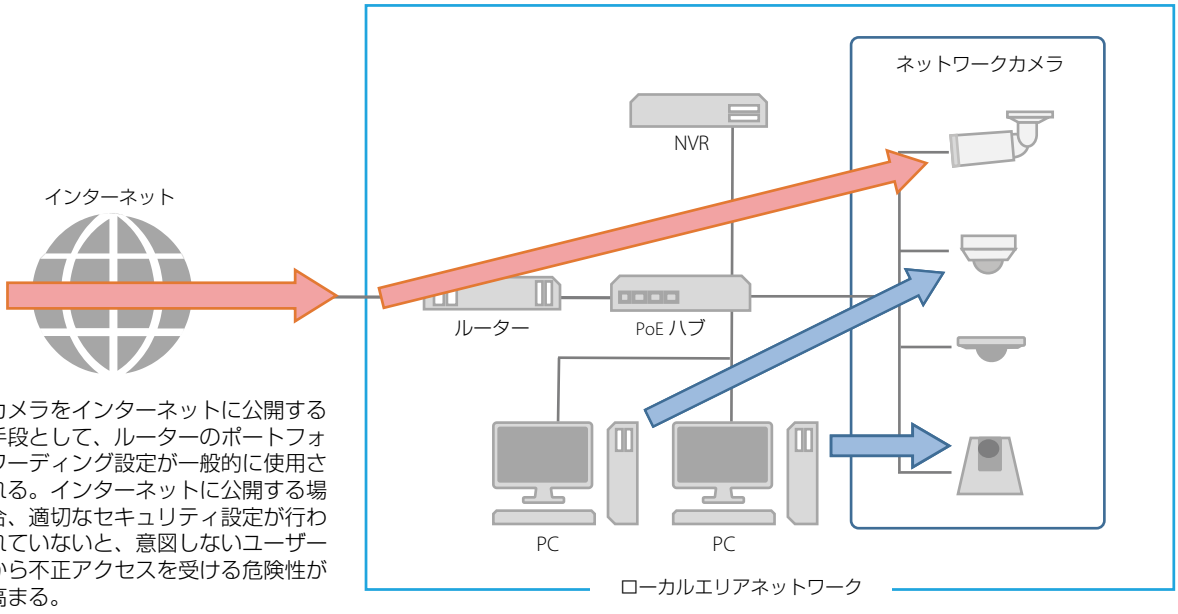
VPN とは？

VPN とは Virtual Private Network (仮想プライベートネットワーク) の略で、通信経路に仮想的なトンネルを作り、その中で安全にデータをやり取りするしくみのことです。本社や支店などの拠点間のローカルエリアネットワークを VPN で接続することで、外部ネットワークからのアクセスを遮断することができます。



■ 外部アクセス可能なネットワークには万全な対策をする

風景を配信するライブカメラなど、不特定多数に映像を配信するケースでは、インターネットなどの外部ネットワークと接続し、カメラに外部からアクセスできるよう、インターネットに公開する必要があります。



カメラをインターネットに公開する手段として、ルーターのポートフォワーディング設定が一般的に使用される。インターネットに公開する場合、適切なセキュリティ設定が行われていないと、意図しないユーザーから不正アクセスを受ける危険性が高まる。

外部からのアクセスを可能とするネットワークは、利便性が高い反面、ネットワーク上の機器が不正アクセスを受けるリスクが高まります。そのため、このようなネットワーク構成の場合、本書で説明している対策だけでなく、ネットワーク内の各機器の認証設定や各通信の暗号化など、システム全体に対して十分な対策を実施して、セキュリティを確保することが重要です。

重要

カメラは電気通信事業者（移動通信会社、固定通信会社、インターネットプロバイダーなど）の通信回線（公衆無線LANを含む）に直接接続することができません。カメラをインターネットに接続する場合は、必ずルーターなどを経由して接続してください。

1章

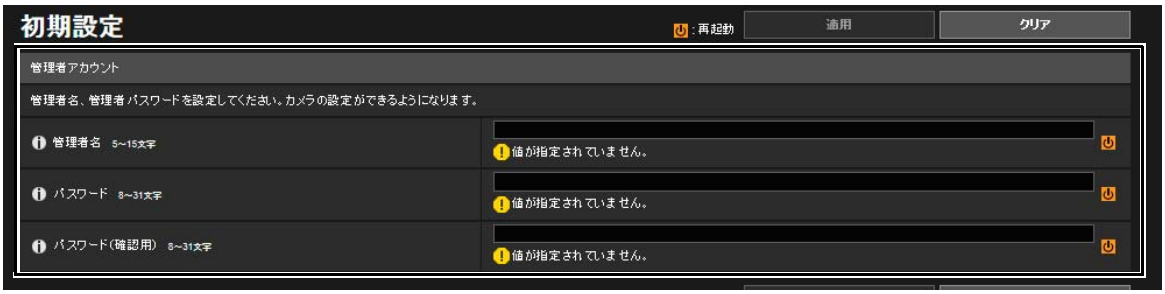
基本的な対策

管理者名とパスワードを設定する

管理者アカウントは、カメラの設定・操作のすべての権限を持つ、アカウントです。管理者アカウントが第三者に不正に使われ、改ざんが行われると、カメラにアクセスできなくなる危険性があります。管理者アカウントのなりすましを防ぐために管理者名とパスワードは、第三者に推測されにくい文字の配列にすることが、カメラを安全に運用するうえで、最も基本的な対策です。また、同じ管理者アカウントを複数のカメラに設定しないなど、管理者アカウントの取り扱いには十分に注意し、厳重に管理してください。

管理者アカウントは、カメラの初回起動時に設定が必要です。また設定後は、カメラの設定ページ、[基本] > [ユーザー管理] で変更できます。

管理者アカウントは、カメラへの初回アクセス時、[初期設定] で設定します。



管理者名とパスワードは、カメラの設定ページ、[基本] または [セキュリティ] > [ユーザー管理] でも変更できます。

■ 安全な管理者名とパスワードのポイント

管理者名とパスワードを強化するためには、次の点を考慮してください。

- 英数字、またはカメラで許可されている記号や特殊文字を組み合わせ、少なくとも10文字以上にする
- 大文字と小文字を組み合わせる
- 一般的に使用されている言葉や文字列など、推測されやすいものを避ける

重要

- 管理者アカウントが工場出荷時に設定されている場合は、必ず変更してください。
- 管理者名とパスワードの設定可能な文字数は、製品により異なります。詳細については、『カメラマネジメントツール 使用説明書』を参照してください。

■ 管理者アカウント以外のパスワード

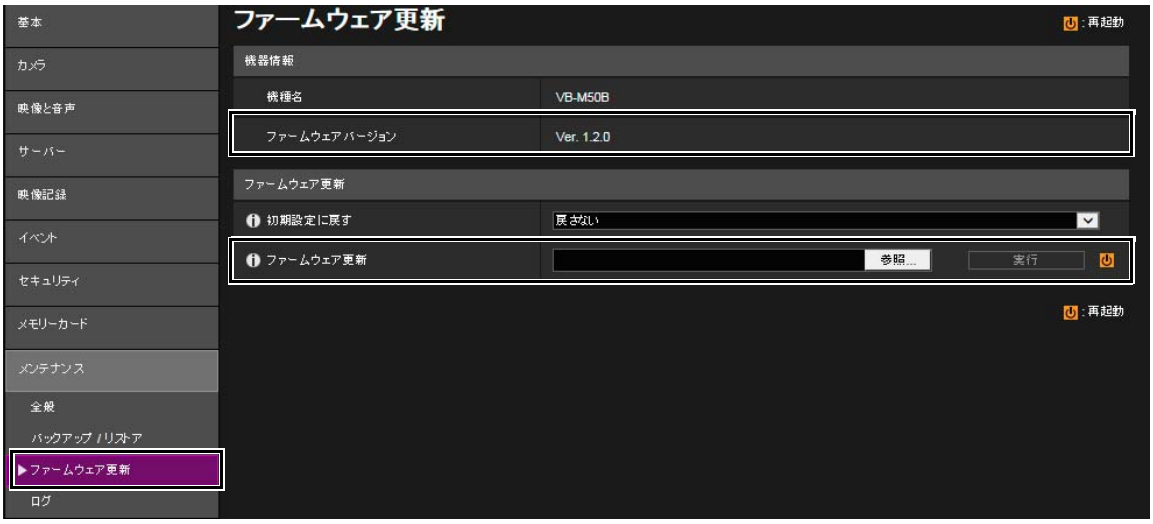
カメラには、管理者アカウント以外にも、登録ユーザー (p. B-12)、サーバー認証、暗号化のためにパスワードを設定します。これらのパスワードも第三者に推測されにくい文字の配列で設定し、適切に管理してください。

最新ファームウェアを利用する

カメラのファームウェアは、機能の性能向上や不具合の修正のため、随時、更新されます。セキュリティの観点からも、既知の脆弱性への対策が施されているため、常に最新にしておくことが重要です。

カメラ購入後の初期設定時、運用時など、お客様がご使用の環境に合わせて、最新のファームウェアが提供されているか、定期的にキヤノンのWebサイトをご確認ください。
なお、ファームウェアのバージョンは、カメラの設定ページ、[メンテナンス] > [機種情報] の [ファームウェアバージョン] で確認できます。

ファームウェアは、カメラの設定ページ、[メンテナンス] > [ファームウェア更新] の [ファームウェア更新] で更新します。



カメラマネジメントツールを使って、ファームウェアを更新することもできます。
カメラマネジメントツールの詳細については、『カメラマネジメントツール 使用説明書』を参照してください。

日付と時刻を設定する

カメラには、正確な日付と時刻を設定してください。不正アクセスが疑われるような兆候があったときは、ログを確認することで、発生した日付と時刻の確認ができる場合もあります。

日付と時刻は、カメラの設定ページ、[基本] > [日付と時刻] の [設定] で設定します。

ログを確認する

カメラの接続状態や動作状況は記録され、ログとしてカメラ本体とメモリーカードに保存されます。ユーザー認証失敗の繰り返しなど、不正アクセスが疑われるような兆候がないか、早期に発見するためにも、定期的にログを確認してください。ログの詳細については、カメラの『操作ガイド』を参照してください。

■ ログの保存先と種類

カメラ本体とメモリーカードでは、保存されるログの内容が異なります。

カメラ本体に保存されるログ：エラーログ、警告ログ、情報ログ

– 再起動、初期化、工場出荷設定に戻す、の操作を行うと消去されます。
また、一定のサイズを超過した場合も消去されます。

メモリーカードに保存されるログ：エラーログ、一部の警告ログ・情報ログ

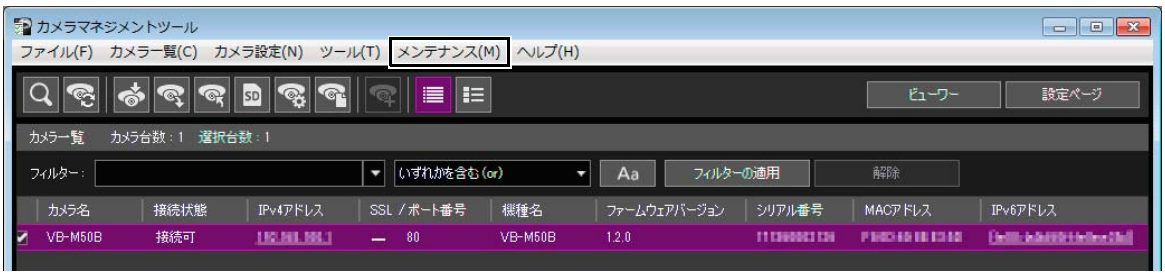
– 再起動、初期化、工場出荷設定に戻す、の操作を行っても消去されません。

■ ログの表示、通知、ダウンロード

カメラ本体に保存されたログは、設定ページの [ログ表示] で確認できます。また、[ログ通知] を使用すると、[エラー]、[エラーと警告] など設定した通知レベルに応じてユーザーに通知することも可能です。
カメラマネジメントツールを使用すると、カメラ本体とメモリーカードそれぞれに保存されたログが、ログファイルとしてダウンロードできます。

ログは、カメラの設定ページで表示・設定します。
[メンテナンス] > [ログ] > [ログ表示]
[メンテナンス] > [ログ] > [ログ通知]

ログファイルは、カメラマネジメントツール、[メンテナンス] > [ログのダウンロード] で ダウンロードします。



カメラマネジメントツールの画面例

■ ログの内容

ログのレベル、コード、障害の程度、分類は次のとおりです。

ログ	レベル	コード	障害の程度	分類
エラーログ	エラー	4xx 例) S410 イベントサービスの初期化エラー	ソフトレベルの異常 (タスク動作停止)	[crit]
エラーログ	エラー	3xx 例) S302 設定値の保存エラー	動作に支障のある異常 (動作継続)	[err]
警告ログ	警告	2xx 例) S220 PAN/TILT動作警告	動作に支障のない異常	[warning]
警告ログ	警告	1xx 例) H144 パスワードの指定異常	システム外部の異常	[notice]
通知ログ	情報	0xx 例) S001 システムの起動	正常動作に関する情報	[info]

2章

ご利用環境に応じた対策

カメラにアクセスするアカウントを管理する [ユーザー管理]

カメラにアクセスできるアカウントには、「管理者」「登録ユーザー」「一般ユーザー」の3種類があります。
管理者は、カメラのすべての設定・操作ができるアカウントです。設定ページにアクセスできるのも、管理者のみとなります。そのため、管理者アカウントの情報は、第三者に漏えいしないよう、厳重に管理することが重要です。
管理者以外の登録ユーザーと一般ユーザーは、カメラビューワーにアクセスできるユーザーです。登録ユーザーと一般ユーザーでできることを理解し、必要最低限のユーザー設定や権限の付与を行ってください。

■ ユーザー認証が必要な登録ユーザー

管理者を除く特定のユーザーのみがカメラビューワーにアクセスできるようにするには、登録ユーザーを設定します。
登録ユーザーの設定では、アカウント情報 (ユーザー名とパスワード) を登録し、カメラビューワーの権限 (映像配信のみ許可する、カメラの制御も許可する、など) を付与します。すべての登録ユーザーに同じ権限が付与され、また特権カメラ制御など管理者に近いカメラ制御まで設定可能となるため、登録ユーザーへの権限付与は慎重に行う必要があります。
定期的に登録ユーザーの見直しを行い、常に必要最低限のユーザーと権限が付与された状態になるように管理してください。
登録ユーザーにのみアクセスを限定したい場合は、後述する一般ユーザーの権限をすべて無効にすることが重要です。これらを無効にしない限り、せっかく登録ユーザーを設定していても、一般ユーザーからのアクセスを許可していることになります。

■ 一般ユーザーはゲストアカウント

一般ユーザーとは、ユーザー名とパスワードを必要としない、ゲストアカウントのことです。一般ユーザーの権限を有効にすると、カメラビューワーにアクセスする際にユーザー認証を必要とせず、誰でもアクセス可能となります。また、カメラ制御や映像配信のコマンドを、認証なしで受け付けるようになります。したがって、一般ユーザーの権限は、カメラの利用目的が不特定多数に向けての映像の一般公開などの場合のみに設定し、それ以外では一般ユーザーの権限はすべて無効にしてください。
登録ユーザー同様、すべての一般ユーザーには同じ権限が付与されますので、一般ユーザーのアクセスを許可する場合は、必要最低限の権限のみを付与してください。

ユーザー管理は、カメラの設定ページ、[基本] または [セキュリティ] > [ユーザー管理] > [登録ユーザーアカウント] / [ユーザー権限] で設定します (以下は [基本] からの画面例)。

一般ユーザー権限を無効にするには、すべてのチェックを外します。

■ カメラビューワーのユーザー認証設定

カメラビューワーにアクセスするときのユーザー認証の有無を設定することができます。ただし、ここでのユーザー認証設定はカメラビューワーでのみ有効であり、他のアプリケーションやビューワーなどでカメラにアクセスする場合には適用されません。したがって、すべてのアクセスにユーザー認証を行いたい場合は、[ユーザー認証] を [認証する] にしたうえで、前述したとおり一般ユーザーの権限をすべて無効にしておくことが重要です。

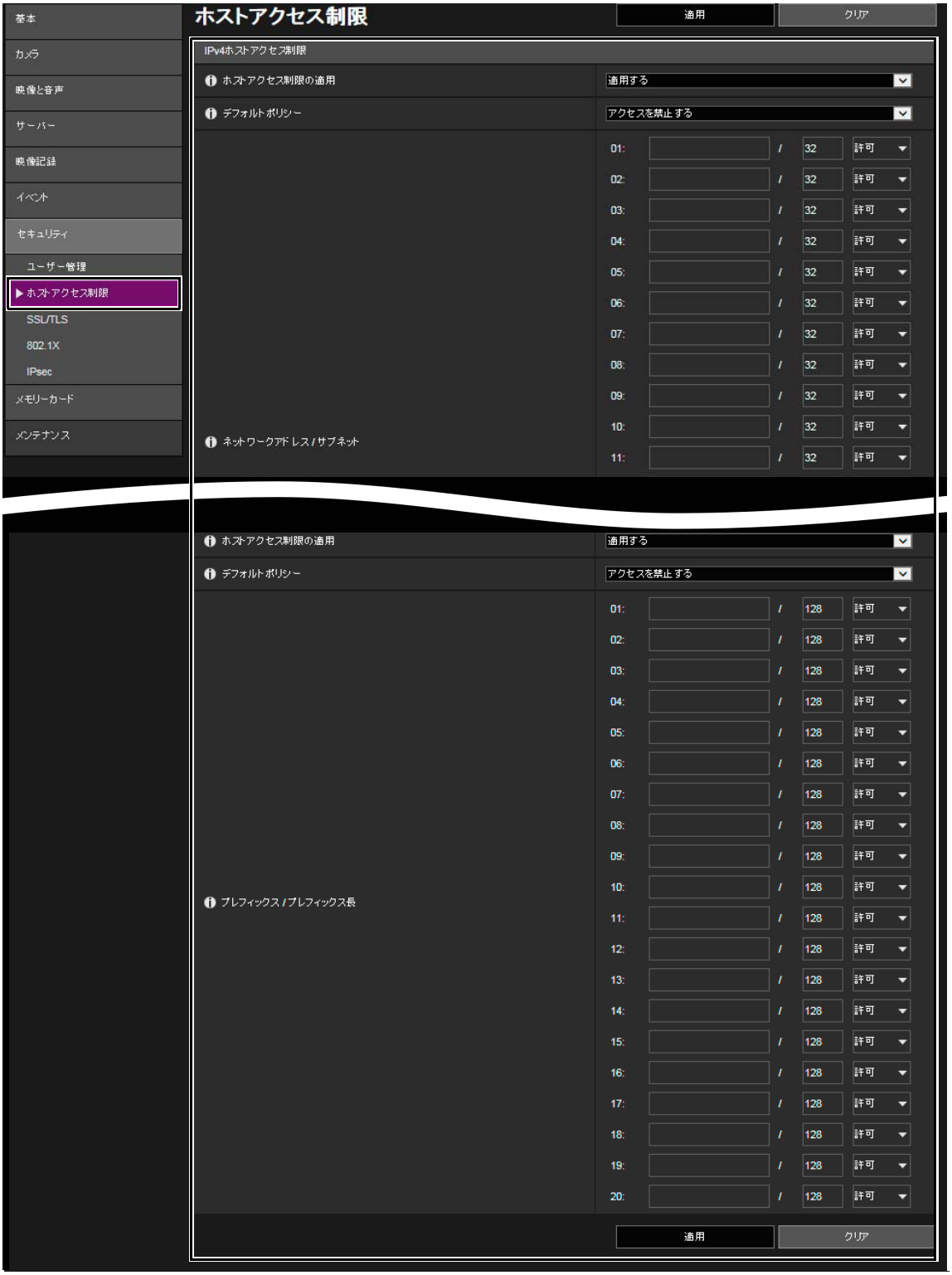
カメラビューワーのユーザー認証は、カメラの設定ページ、[基本] > [ビューワー] > [ビューワー設定] の [ユーザー認証] で設定します。

カメラにアクセスするホストを制限する [ホストアクセス制限]

カメラにアクセスできるホストを制限することにより、第三者から不正にアクセスされるリスクを軽減させることができます。

アクセスするホストを制限するには、指定したホストとの通信だけを許可し、それ以外の通信は禁止します。逆に、指定したホストとの通信だけを禁止し、それ以外の通信は許可する方法もあります。
利用環境に応じて、アクセス制限の範囲をネットワーク単位でまとめたり、ホスト単位に限定して設定することも可能です。ただし、誤って管理者のIPアドレスを通信禁止に設定してしまうと、管理者からのカメラへのアクセスが禁止され、工場出荷設定に戻す以外に復旧する手段がなくなることがありますので、設定には十分ご注意ください。

ホストアクセス制限は、カメラの設定ページ、[セキュリティ] > [ホストアクセス制限] > [IPv4ホストアクセス制限] / [IPv6ホストアクセス制限] で設定します。



Digest (ダイジェスト) 認証を設定する

カメラにアクセスするときの [HTTPサーバー] と [RTPサーバー] の認証方式は、[Digest認証] に設定してください。[Basic認証] を選択すると、ネットワーク上でパスワードが暗号化されずに送信されるため、第三者による盗聴が行われた場合に、パスワードが容易に第三者に漏れてしまうことになります。

HTTPサーバーとRTPサーバーの認証方式は、個別に設定が必要です。また、使用するアプリケーションがDigest認証に対応していることを確認してください。

■ Digest認証 (HTTP)

HTTPサーバーの認証方式は、カメラの設定ページ、[サーバー] > [サーバー] > [HTTPサーバー] の [認証方式] で設定します。

■ Digest認証 (RTSP)

RTPサーバーのRTSP認証方式は、カメラの設定ページ、[サーバー] > [RTPサーバー] > [RTPサーバー] の [RTSP認証方式] で設定します。

ポート番号を変更する

カメラへの不正なアクセスを防ぐには、不特定のアクセスを制限することが重要です。ポート番号は、カメラと外部機器との通信の出入口であり、通信プロトコルごとに番号が設定されています。それぞれのポート番号は、ネットワーク機器間で広く共通の番号が使われているため接続性が高い反面、第三者の不正な侵入に利用される危険性があります。
セキュリティの懸念により、ポート番号を変更する場合は、他の通信プロトコルとポート番号が重複しないことを確認のうえ、指定された範囲で設定してください。ポート番号を変更した場合、カメラにアクセスするためには、IPアドレスの他にポート番号を指定する必要があります。

■ ポート番号の変更 (例)

HTTPSで接続する場合、「https:// {カメラのIPアドレス} : {ポート番号} 」と指定してください。

HTTPSポート番号が10443に変更されている場合
https://192.168.100.1:10443

■ HTTP ポート番号/HTTPS ポート番号

HTTP/HTTPSのポート番号は、カメラの設定ページ、[サーバー] > [サーバー] > [HTTPサーバー] で設定します。

次のポート番号も変更可能です。

■ RTSP ポート番号

RTSPポート番号は、カメラの設定ページ、[サーバー] > [RTPサーバー] > [RTPサーバー] で設定します。

■ マルチキャストポート番号

マルチキャストポート番号は、カメラの設定ページ、[サーバー] > [RTPサーバー] で設定します。
[音声マルチキャスト] > [マルチキャストポート番号]
[RTPストリーム 1/2/3/4/5] > [マルチキャストポート番号]

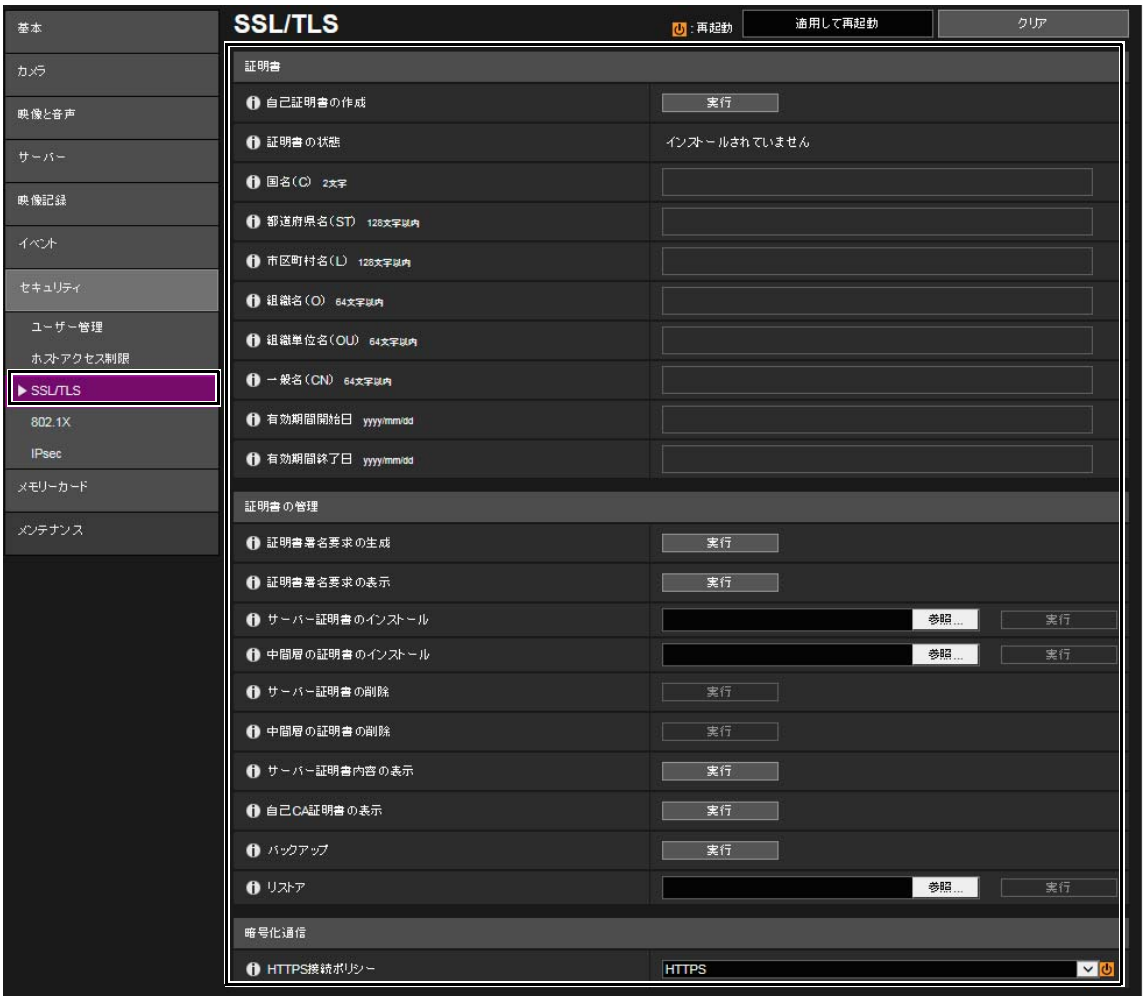
通信を暗号化する [SSL/TLS]

カメラと外部機器との間で安全な通信を行うためには、すべての通信をHTTPS接続 (SSL/TLSとHTTPを組み合わせた暗号化通信) にすることをおすすめします。SSL (Secure Sockets Layer) / TLS (Transport Layer Security) とは、ネットワーク上で通信を暗号化し、第三者による通信内容の盗聴や改ざんを抑止する技術です。万一、通信の途中でデータが盗聴されたとしても、適切な方法で通信を暗号化しておくことで、データの内容は保護されるため、安全性を確保することができます。

■ 自己署名証明書とサーバー証明書

HTTPS接続での暗号化通信の手段としては、自己署名証明書またはCA局 (証明機関) から発行されるサーバー証明書を使う方法があります。自己署名証明書は、暗号化を行うには十分ですが、Webブラウザーに警告画面が表示されたり、なりすましのリスクが生じます。動作テストなどの場合に使用してください。
本格的なシステム運用時には、CA局から発行されるサーバー証明書を取得し、インストールすることをおすすめします。

HTTPS接続での暗号化通信は、カメラの設定ページ、[セキュリティ] > [SSL/TLS] で設定します。



メモ

上記HTTPS接続の設定を行っても、RTP/RTSPで配信される映像は自動的に暗号化されません。またアップロードするデータも暗号化できません。これらのデータを安全に通信するためには、システム全体としての対応が必要となります。

保護されたネットワークで使用する [802.1X]

IEEE802.1X認証は、あらかじめ決められた機器以外がネットワークにアクセスしないように、認証によって接続を規制する規格です。サーバー認証された機器だけがネットワークに接続できるため、不正なアクセスからネットワークを保護できます。カメラがIEEE 802.1X認証で保護されたネットワークにアクセスできるようにするには、適切な証明書と設定が必要です。

IEEE802.1Xの設定は、カメラの設定ページ、[セキュリティ] > [802.1X] で設定します。

メモ

IEEE802.1X認証機能をご利用になるには、あらかじめIEEE802.1Xネットワーク環境を構築しておく必要があります。

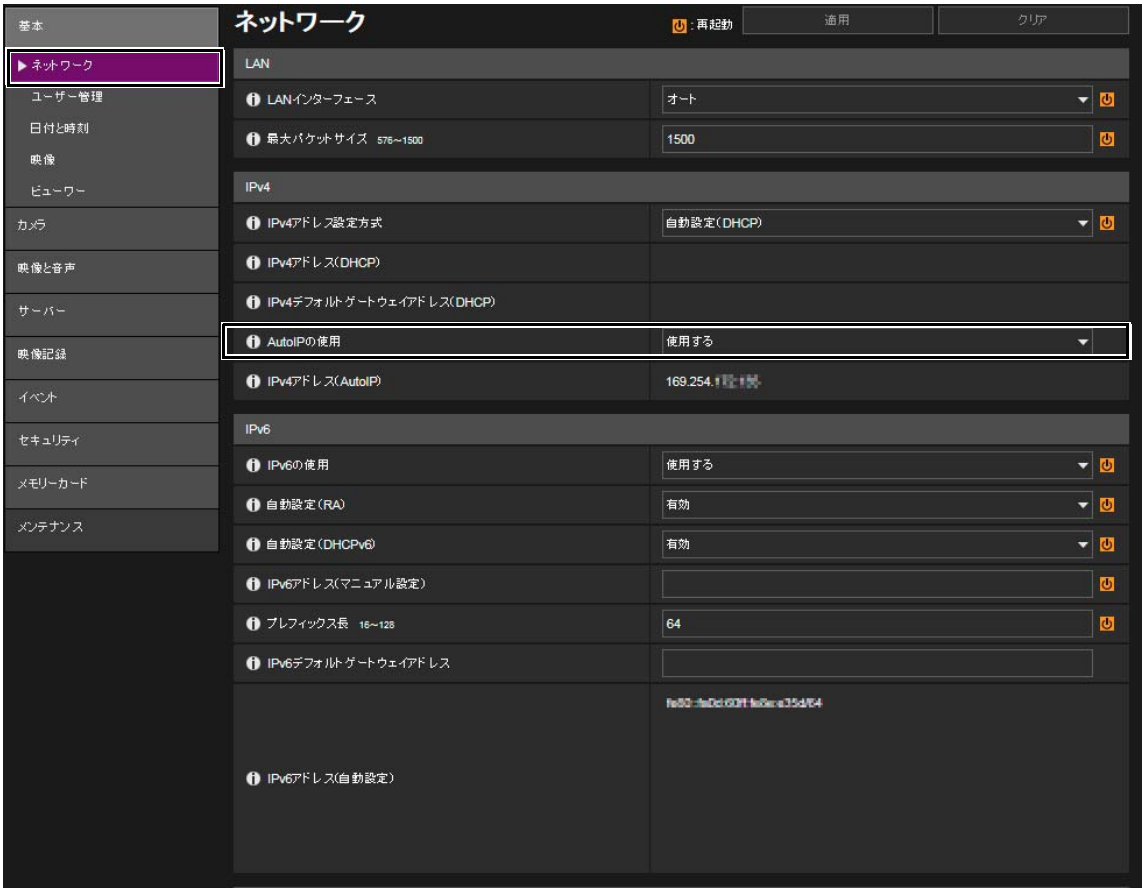
使用しない機能を無効にする

カメラには、さまざまな利用目的やネットワーク環境に対応するための機能が搭載されています。しかし、それらの機能を適切に設定していないと、第三者からの不正アクセスを受ける可能性があります。カメラを安全に使用するためには、使用しない機能の設定を無効にすることも必要です。
運用環境や利用状況において、必要な機能のみ設定を有効にする、設定が終了したら機能を無効にする、などの対応が必要な機能について、次に説明します。

■ AutoIP

[AutoIPの使用] を有効にすると、DHCPサーバーがない環境においても、IPv4リンクローカルアドレス (169.254. xxx.xxx) がカメラに割り当てられます。そのため、このIPv4アドレスと同じセグメントにPCを所属させ、カメラマネジメントツールを使用すれば、カメラが検出され、初期設定をすることができます。
工場出荷設定では、[AutoIPの使用] が有効になっていますが、第三者に不正な目的で使用されないように、ネットワークの初期設定が終了したら無効にすることをおすすめします。

AutoIPは、カメラの設定ページ、[基本] > [ネットワーク] > [IPv4] の [AutoIPの使用] で設定します。

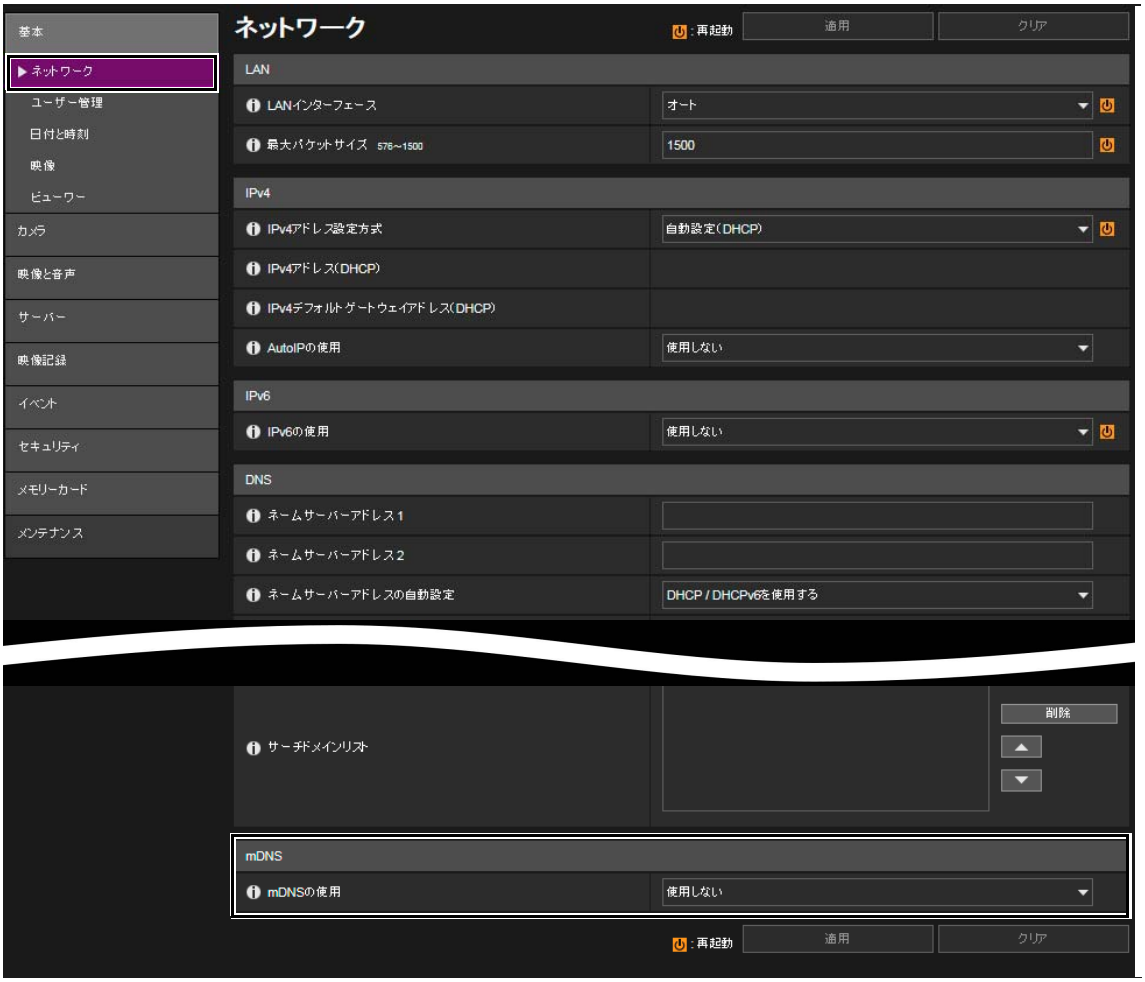


[AutoIPの使用] 工場出荷設定 : [使用する]

■ mDNS (multicast Domain Name System)

[mDNS] は、DNSサーバーがない環境でもカメラが検出されるように、ネットワーク上の機器にカメラのIPアドレスとホスト名の情報を一斉に通知する機能です。
工場出荷設定では、[mDNS] の設定が有効になっていますが、第三者に不正な目的で使用されないように、ネットワークの初期設定が終了したら、無効にすることをおすすめします。

mDNSは、カメラの設定ページ、[基本] > [ネットワーク] > [mDNS] で設定します。

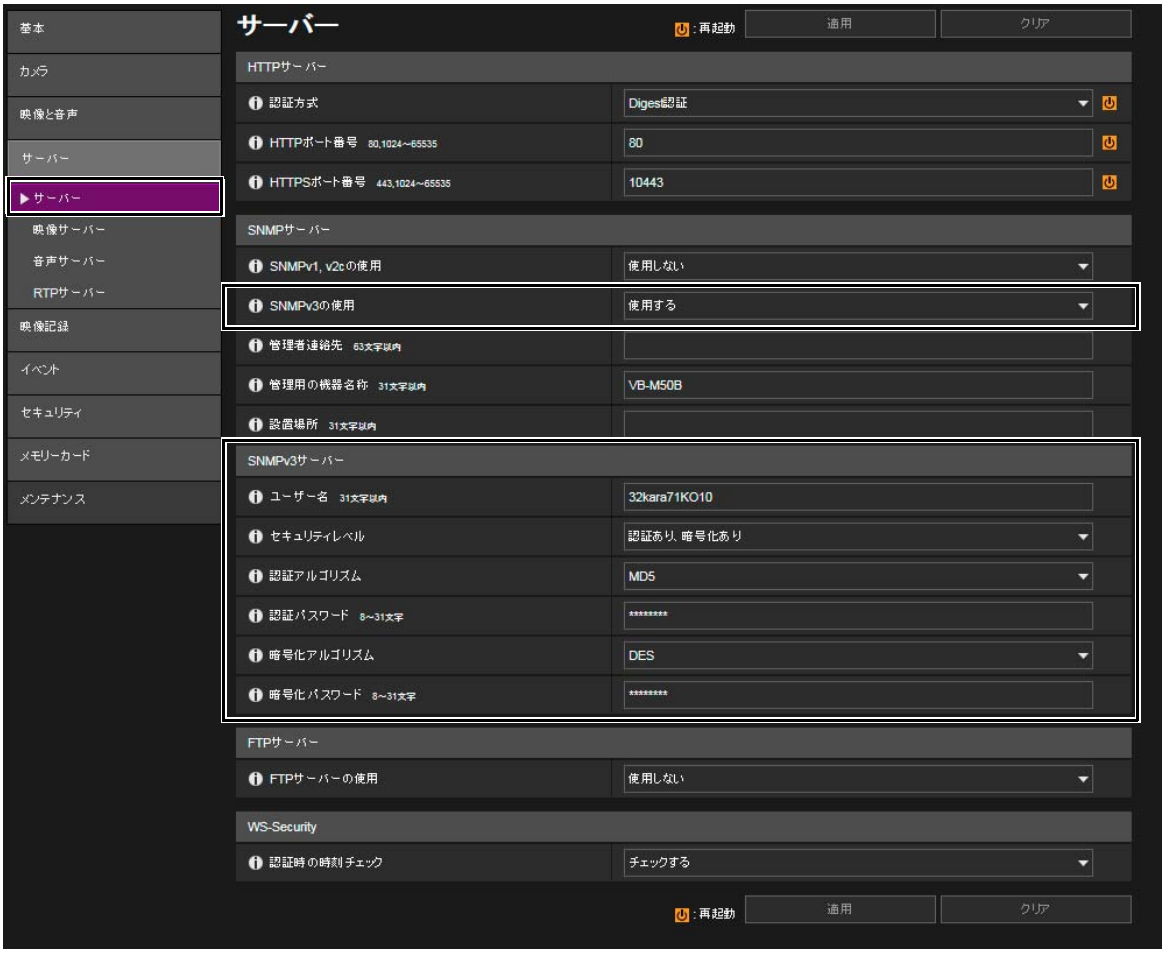


[mDNSの使用] 工場出荷設定 : [使用する]

■ SNMP (Simple Network Management Protocol)

[SNMPサーバー] を使用すると、SNMPマネージャーからカメラ (SNMPエージェント) を監視または制御できます。SNMPv3は、認証情報であるユーザー名とパスワードを暗号化して通信することができます。SNMPによる管理を行う場合は、SNMPv1とSNMPv2cに比べ、より安全な通信であるSNMPv3を選択し、暗号化パスワードを設定してください。SNMPv1とSNMPv2cは、運用される環境において必要な場合にのみ、セキュリティ面の安全性が確保されたネットワーク内でご利用ください。

SNMPサーバーは、カメラの設定ページ、[サーバー] > [サーバー] > [SNMPサーバー] で設定します。



[SNMPv1, v2cの使用] 工場出荷設定 : [使用しない]
[SNMPv3の使用] 工場出荷設定 : [使用しない]

■ FTP (File Transfer Protocol)

映像配信用ホームページのHTMLファイルなどをカメラ本体にアップロードするために、[FTPサーバー] を使用します。FTPによる通信では、認証情報として送信されるユーザー名やパスワードは暗号化されません。また、第三者の不正アクセスによりファイルをカメラにアップロードされる危険性があります。ファイルをアップロードするときにのみ、設定を有効にしてください。

FTPサーバーは、カメラの設定ページ、[サーバー] > [サーバー] > [FTPサーバー] で設定します。

[FTPサーバーの使用] 工場出荷設定 : [使用しない]

■ RTP (Real-time Transport Protocol)

[RTPサーバー] を使用すると、映像や音声を指定したマルチキャストアドレスにも配信できます。カメラと接続する録画システムやビューワーが、RTPプロトコルを必要としない場合は、[RTPの使用] を [使用しない] にすることをおすすめします。

RTPサーバーは、カメラの設定ページ、[サーバー] > [RTPサーバー] > [RTPサーバー] で設定します。

[RTPの使用] 工場出荷設定 : [使用する]

付録

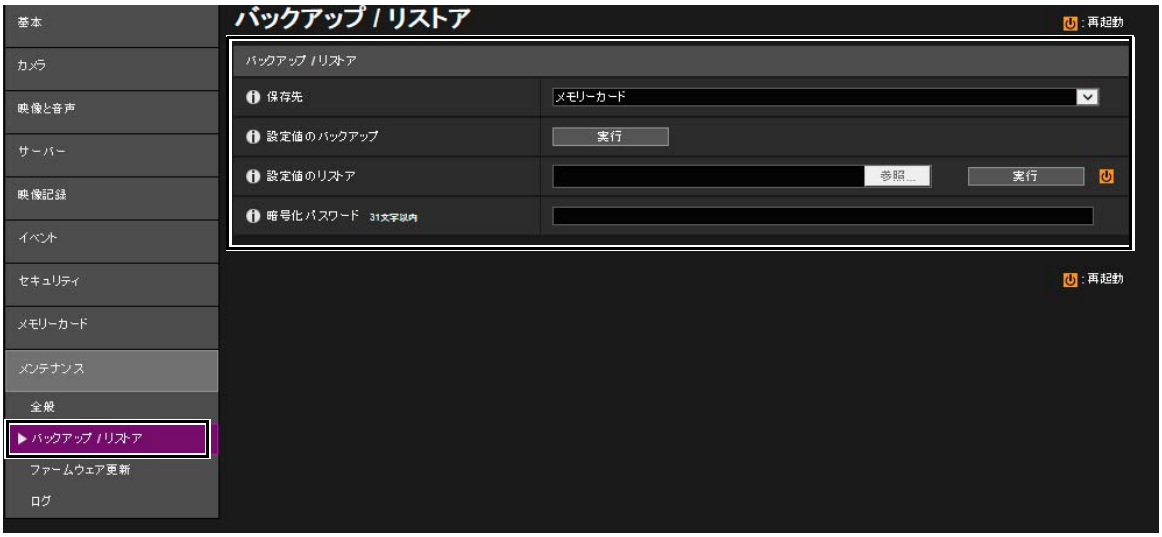
カメラを廃棄するときに

カメラを廃棄するときは、カメラを初期化して、ネットワーク設定や管理者アカウントなどの設定情報をすべて消去してください。また、メモリーカードの抜き忘れにも十分ご注意ください。
カメラの初期化は、設定ページ、[メンテナンス] > [全般] の [初期化] で実施します。廃棄の際は、[ネットワーク設定] を [保持しない] に設定してください。また、設定ページにアクセスできないときは、カメラ本体のリセットスイッチを操作して、工場出荷設定に戻してください。
本体リセットスイッチの操作は、カメラの機種ごとに異なるため、『操作ガイド』を参照してください。

バックアップ情報を暗号化する

カメラ設定値のバックアップ情報は、設定値を復元 (リストア) させる際に利用します。バックアップ情報に [暗号化パスワード] を設定することで、より安全に管理することができます。
設定したパスワードの取り扱いには十分ご注意ください。

バックアップ情報の暗号化は、カメラの設定ページ、[メンテナンス] > [バックアップ/リストア] > [バックアップ/リストア] で設定します。



BIJ-7243-002

2022年5月 発行