テクニカルガイド | SNC シリーズ G6/G7

不正アクセス防止ガイド

SONY

ネットワークカメラ
2018 年 7 月 01 日
G6G7TG001
改訂 1.0.0

目 次

1. 概要 3
1.1. 本書について 3
1.2. CGI バージョンについて 3
2. はじめに 4
2.1. カメラへの不正アクセスを防ぐ 4
2.2. 定期的にファームウェアを確認する 6
2.3. デバイスへの不要なアクセスを避ける 6
2.4. 安全なデバイスアクセスのみ許可する 8
3. おわりに 10
4. 付録—関連資料 11
改訂履歴 12

1. 概要

1.1. 本書について

本書は、ソニーネットワークカメラ（以後「カメラ」と表記）の第 6 世代（G6）および第 7 世代（G7）のための不正アクセス防止ガイドです。

1.2. CGI バージョンについて

お使いのカメラの世代が G6/G7 のいずれに該当するか、以下の CGI コマンドを使ってご確認ください。

```
http://<camera_address>/command/inquiry.cgi?inq=system
```

G6 モデルの場合は次の記述が返されます。

```
CGIVersion=6.0.*.*.*                                    [Each * is a number.]
```

または

```
CGIVersion=6.10.*.*.*                                   [Each * is a number.]
```

G7 モデルの場合は次の記述が返されます。

```
CGIVersion=7.*.*.*.*                                     (* means a number.)
```

それ以外の場合はこのパラメータは存在しません。
本書は G6 モデル（`CGIVersion=6.0.*.*.*`）および G7 モデル（`CGIVersion=7.*.*.*.*`）を対象に記述しています。

2. はじめに

IP 通信を用いたカメラは、簡単に使用できるネットワークハードウェアという特性や、監視システムなどへの統合も容易であることから、様々な場所で使われています。

しかし、インターネット経由でカメラを使用する場合、ほかの IoT 機器と同様に、意図しない第三者からのアクセスにさらされる可能性が高まります。近年、IoT 機器を狙ったサイバー攻撃が世界的にも増加しており、ネットワーク上のデバイスやインフラに対する第三者からの意図しないアクセスを防止することが重要になっています。

IoT デバイスのネットワークの安全性を確保するには、システムのセキュリティについて考慮する必要があります。つまり、インフラやデバイス、およびそれらの設定や編成のプロセスに対するセキュリティを考慮し、設置デバイスの運用期間を通して、ユーザー／パスワード管理などのセキュリティを維持する必要があります。

本書では、カメラに有効なセキュリティ対策を説明します。

2.1. カメラへの不正アクセスを防ぐ

2.1.1. 一般的注意事項

使用環境によっては、意図しない第三者がネットワークを介してカメラにアクセスする可能性があります。はじめにカメラを設置するときに、カメラ管理者のユーザー名とパスワードを初期設定値から推測されにくいパスワードに変更することを強く推奨します。

ブラウザからカメラの設定を行う場合、適切なセキュリティ機能を適用した専用 PC を使用してください。また、ブラウザからカメラへのアクセス中に、他のサイトを閲覧しないでください。

注：設定作業が終了しましたら、必ずブラウザを閉じて、カメラから強制的にログアウトしてください。　ブラウザを開いたままにしますと、カメラにログインした状態が残ります。意図しない第三者の使用や悪意のあるプログラムの実行を防ぐために作業後は必ずブラウザを閉じてください。

2.1.2. 管理者とユーザー

G6/G7 のカメラには、「管理者」または「ユーザー」の権限でログインすることができます。

「管理者」としてログインするとカメラの設定を含め、本カメラのすべての機能を利用することができます。「ユーザー」はカメラの映像・音声のモニターとカメラの操作だけを行うことができます。ユーザーは「ビューアーモード」の設定により、利用できる機能（アクセス権）を限定された 4 種類のユーザーに分類されます。

それぞれが利用できる機能は次のとおりです。

機能	管理者	ユーザー			
		フル	パン・チルト	ライト	ビュー
ライブ画像を見る	○	○	○	○	○
日付・時刻を見る	○	○	○	○	○
フレームレートを操作する（JPEG モード時のみ利用可）	○	○	×	×	×
画像表示サイズを操作する	○	○	○	○	×
静止画像と動画画像をコンピューターに保存する	○	○	○	○	×
TCP/UDP 通信を切り換える（H.264 モード時のみ利用可）	○	○	×	×	×
パン・チルト・ズーム操作を行う	○	○	○	×	×
音声を受信する	○	○	○	○	○
コーデックを選択する	○	○	○	○	×
設定メニューを操作する	○	×	×	×	×
メモリーカードに記録したファイルを再生する	○	○	×	×	×
メモリーカードに記録したファイルを削除する	○	×	×	×	×

○ 利用できる機能

× 利用できない機能

ユーザーには常に必要最低限の権限を付与し、定期的にユーザーの見直しを行い、必要最低限の権限のみ付与された状態になるように管理してください。

2.1.3. ユーザーアカウントとパスワードの設定

［パスワードの管理］

カメラのセキュリティを確保する上で最も重要な手順の 1 つが、カメラで有効にしたすべ

てのユーザーに個別の推測されにくいパスワードを設定することです。
特に、管理者のパスワードは工場出荷時のパスワードから必ず変更してください。
また、パスワードを決めるときは、次の点を考慮してください。

- 通常の利用に際し、工場出荷時の初期設定値の ID とパスワードを使用せずに必ず推測されにくいパスワードに変更してください。
- 複数のデバイス、システム、サービスにパスワードを使い回すと、パスワードの漏洩や悪用のリスクが高まります。他の機器やサービスに用いるパスワードとは異なるパスワードを設定してください。
- 推測されにくいパスワードを使ってください。セキュリティ強化のため、数字と文字またはカメラで許可されている特殊文字を含む 8 文字以上のパスワードを使用してください。
（詳細についてはユーザーガイドを参照してください。）

2.2. 定期的にファームウェアを確認する

ソニーは、新しい機能やセキュリティの強化を含むファームウェアアップデートを必要に応じて提供しています。ファームウェアアップデートファイルは、https://www.sony.jp/snc/support/の「サポート・お問い合わせ」から検索することができますので、定期的にファームウェアの更新の有無を確認してください。

ファームウェアアップデートファイルをダウンロード後、SNC toolbox PC ソフトウェアを使って各カメラに適用してください。
アップデートされる内容はリリースノートに記載されています。
セキュリティ強化のために、常に最新のファームウェアと SNC toolbox を使用することを推奨します。

2.3. デバイスへの不要なアクセスを避ける

2.3.1. インターネットに不用意に接続しない

日常の業務の観点から、カメラを接続するネットワークが完全に LAN 環境内に限られている場合、ネットワークの安全性を維持するために、たとえ一時的にでもインターネットには接続しないことを推奨します。

最新ファームウェアは、インターネットに接続した PC を用いて、ソニーの Web サイト

からダウンロードする必要がありますが、SNCtoolbox を用いたファームウェアアップデートはインターネットへのアクセスがない環境でも実行可能です。

2.3.2. クライアント／サーバー認証に外部の証明書を使う

SSL または TLS 機能（以後「SSL」と表記）を使用する場合、SSL サーバー認証の CA 証明書によりカメラの認証を行うことができます。CA 証明書を SSL クライアント認証に用いることで、カメラが信頼できるクライアントからの接続であることを確認することもできます。サポートされる証明書の形式やインストール方法については、各カメラのユーザーガイドを参照してください。

2.3.3. 使用しない機能を無効にする

使用しないカメラ機能を無効にすると、潜在的な攻撃経路を遮断してカメラの安全性を向上できます。

- 工場出荷状態で有効なもの：
  UPnP ディスカバリー、ONVIF WS-Discovery
- 工場出荷状態で無効なもの：
  FTP 静止画送信（クライアント）、SMTP メール送信（異常送信を含む）、HTTP アラーム通知など

2.3.4. 工場出荷時構成のオープンポート

次の表は、工場出荷時構成のカメラのオープンポートを示しています。
ネットワークシステム管理者はこれを考慮し、必要に応じてネットワークスイッチのポートフィルタリングを行います。

プロトコル	ポート番号	サービス	用途
TCP	80	HTTP	構成および／またはストリーミング
TCP	554	RTSP	ストリーミング
TCP/UDP	52323	SSDP	UPnP SSDP ディスカバリー
UDP	68	DHCP	DHCP クライアント
UDP	2380	-	ソニー独自のプロトコル（IP SETUP）
TCP	3702	WS-Discovery	ONVIF

ほかにも、送信に使用するランダム UDP ポート（UPnP）があります。

2.4. 安全なデバイスアクセスのみ許可する

クライアントとカメラの間の通信のセキュリティを強化するために、HTTPS、802.1x、アクセス制限、Referer チェックなどの機能があります。またカメラには、クライアントからモニタリングできる機能もあります。

HTTPS 暗号化接続をサポート

カメラとクライアントの間の通信を HTTPS で暗号化します。通信チャネルから情報が抽出されたとしても、内容の覗き見や改ざんが難しくなります。
ソニーのカメラは次のプロトコルをサポートしています。

- TLS v1.0：互換性のためにサポートしていますが、通常は使用しません。
- TLS v1.2：推奨（デフォルト）

クライアント認証を使用する場合、CA 局発行の証明書がインストールされたクライアントからのみカメラにアクセスできます。

自己署名証明書は暗号化に使用できますが、「証明書が信頼できません」という警告がクライアントに通知されます。
（詳細についてはユーザーガイドを参照してください。）

802.1x で保護されたネットワークに対応

802.1x 機能は、証明書ベースの認証によりデバイスのネットワーク接続を制御します。承認されたデバイスだけがネットワークに接続できるので、ネットワークを不正なアクセスから保護できます。このネットワークに参加するには、カメラへの適切な設定と証明書のインストールが必要になります。

アクセス制限

どのコンピューターにカメラへのアクセス権を与えるかを制御できます。同様に、IPv6 を使用している場合、各ネットワークにセキュリティ設定を構成することができます。

Referer チェック

Referer チェックでは、カメラへのアクセスに関連している Web ページ、またはカメラへのアクセスを要求する Web ページが承認されているかどうかを確認します。Web ページが承認されていない場合、カメラは、その Web ページからカメラへのアクセスを拒否

します。

カメラが規定する以外の Web ページからアクセスするには、その Web ページのホスト名とポート番号を例外リストに登録します。

SNMP モニタリング

SNMP プロトコルを使ってネットワーク上のカメラを監視および制御できます。ソニーのカメラは次のプロトコルをサポートしています。

- SNMP v1、v2c：互換性のためにサポートしていますが、通常は使用しません。
- SNMP v3：強化された認証方法とデータ送受信の安全性の点で使用をお勧めします。

詳細については、『Technical Guide – G6/G7 TG010 SNMP Function Support』のドキュメントを参照してください。

3. おわりに

システムオペレーターにとって、IP システムに関するサイバー攻撃など不正アクセスによるリスクは深刻な懸念事項となっています。カメラへの不正アクセスを防ぐため、ぜひ本書をお役立てください。

4. 付録―関連資料

本書のさらに詳細な内容については、以下に示す各製品の関連 Web サイト／ドキュメントを参照してください。

ファームウェア／リリースノート／ユーザーガイド
テクニカルガイド（メンバー登録が必要です）
https://www.sony.net/CameraSystem

ソフトウェア脆弱性防止の取り組み
https://www.sony.co.jp/SonyInfo/procurementinfo/software/

本書で取り上げた組織およびフレームワーク

- CERT/CC：CERT/Coordination Center
  https://www.cert.org

- NIST：National Institute of Standards and Technology
  https://csrc.nist.gov

改訂履歴

日付	改訂	詳細
2018/07/01	1.0.0	初版

免責事項

本書は、いかなる目的であっても、ソニー株式会社の書面による事前の承認なしに、全部または一部を複製または転載することを禁じられています。
ソニー株式会社は、本書または本書に含まれる情報を、予告なくいつでも変更できる権利を留保します。
ソニー株式会社は、製品および関連ドキュメントに起因するいかなる損害、逸失利益および第三者の請求にも責任を負わないものとします。

著作権について

本書に含まれる登録商標および商標は、各会社が所有しています。