Hanwha Techwin

White paper

安全な SNMP 使用ガイド

2020 年 9 月 22 日

Contents

1. DoS 攻撃事例の発生

2. SNMP サービスを安全に使用する

2.1. 「SNMP サービス」の紹介

2.2. パブリックネットワークに接続する際、SNMP サービスを安全に使用する

2.2.1. 最新ファームウェアアップデート

2.2.2. SNMP サービスの無効化

2.2.3. SNMP v3 の使用

2.2.4. SNMP Community String の変更

改訂履歴

バージョン	改訂日付	改訂内容	備考
v1.0	20200922	初回作成	

1. DoS 攻撃事例の発生

最近パブリックネットワークに公開された当社のカメラのSNMPサービスを利用したDoS攻撃が行われた事例が発見されました。本悪用事例は、パブリックネットワークに公開されたカメラであり、内部ネットワークやローカルネットワークにインストールされたカメラは該当しません。また、パブリックネットワークに接続されている場合にもSNMPサービスが無効のカメラには影響がありません。

問題になる当該SNMPサービスは最新バージョンのSNMP v3ではなく、v1、v2cバージョンのみであり、旧バージョン(iPOLiSを含む、2018年以前にリリースされたWisenet製品)のカメラモデルではv2cバージョンが初期値で有効になっているため、当該サービスを使用する意図がなくてもDoS攻撃の手段として悪用されることがあるため注意する必要があります。

これに対しハンファテックウィンは、本「安全なSNMPの使用ガイド」文書を通じて製品に実装されたSNMPサービスのセキュリティ機能を安全に使用するように案内させていただきます。

2. SNMP サービスを安全に使用する

2.1. 「SNMP サービス」の紹介

SNMP(Simple Network Management Protocol)とは、簡単なネットワーク管理のための規約であり、ネットワーク上のデバイスのモニタリング、環境設定及び運用できる管理プロトコルです。ネットワーク管理者はSNMPを通じて以下の内容を実行できます。

2.1.1.1. ネットワーク構成管理

ネットワーク上のホストの接続構造を把握して管理できます。

2.1.1.2. 性能及びデバイス管理

各ネットワークセグメント(Segment)間のネットワーク使用量、エラー量、処理速度、レスポンス時間などの性能分析に必要な統計情報や特定デバイスのシステム情報(CPU、MEMORY、DISKの使用量)を確認できます。

2.1.1.3. セキュリティ管理

情報の制御及び保護機能があります。特に、最新のバージョンのSNMP v3は情報保護のための機能が向上されました。

2.2. パブリックネットワークに接続する際、SNMP サービスを安全に使用する

SNMPサービスは管理の利便性を提供しますが、正しくない動作をする時にDoS攻撃、不正アクセスなどの問題発生の原因になることがあります。

ハンファテックウィンの最新カメラモデルには、DoS攻撃を起こす可能性があるSNMPサービスが初期値で無効状態であり、必要に応じて選択的に有効化するようにオプションを提供しています。また、SNMPサービスを安全に使用できるようにSNMPV3バージョンを提供しています。

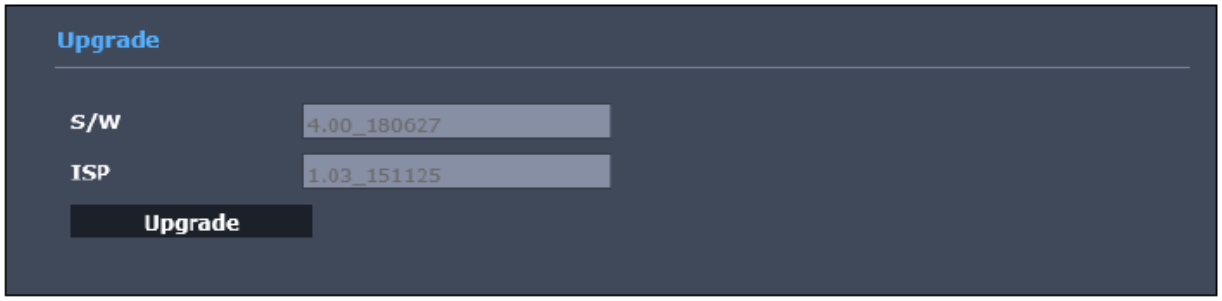
現在使用しているカメラのSNMPサービスを悪用したセキュリティ事故を予防するために次の事項が適用されているかを点検してください。

2.2.1.最新ファームウェアアップデート

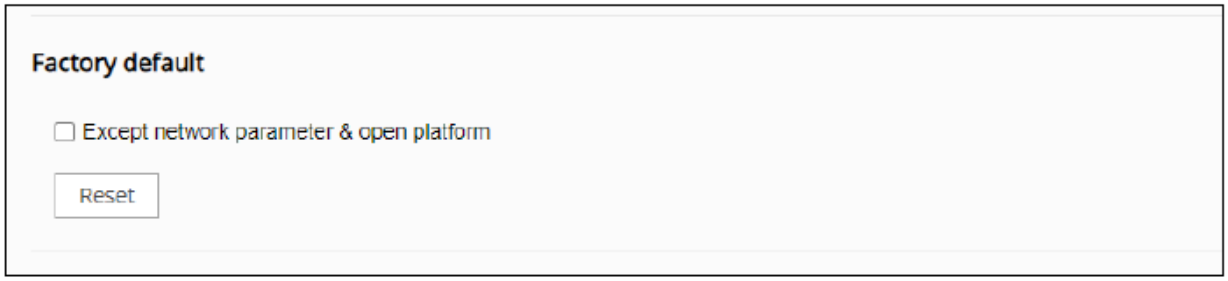
SNMPサービスのセキュリティ強化設定を維持し、今後安全に管理するためには最新ファームウェアにアップデートする必要があります。ファームウェアアップデート後、最新セキュリティ設定環境を適用するため、初期化作業も必要です。

1) ハンファテックウィンのホームページ(www.hanwha-security.com)で当該モデル名を検索した後、最新ファームウェアダウンロード
2) 以下のメニューでファームウェアアップグレード実行
   メニュー：設定 → システム → アップグレード
3) アップグレード完了後、初期化(ネットワーク設定維持解除)

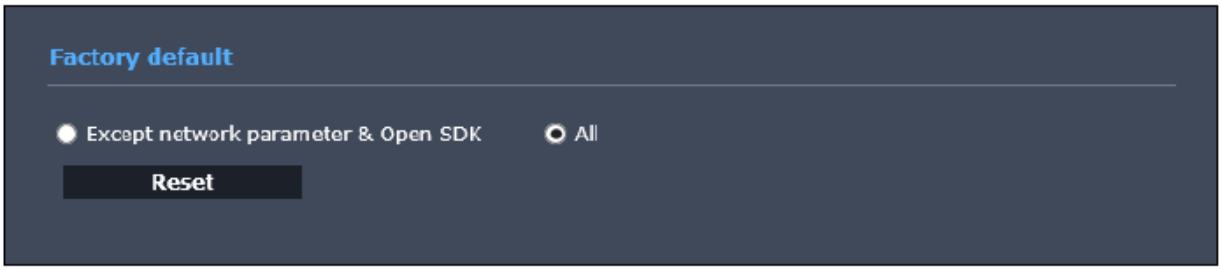
[ファームウェアアップグレード機能]



[旧バージョンカメラのファームウェアアップグレード機能]



[出荷条件初期化する時にネットワーク設定維持のチェック解除]



[旧バージョンカメラの出荷条件初期化する時にネットワーク設定維持のチェック解除]

Q&A) ファームウェアアップグレード後、もう一度 SNMP の設定を変更する必要がありますか？

当社のデバイスはファームウェアアップグレード後にもユーザーの既存設定をそのまま維持するようになっています。したがって、安全なセキュリティ設定のためにはファームウェアアップグレード後、SNMP 設定まで変更する必要があります。

(参照：2.2.2 SNMP サービスの無効化)

Q&A) 初期化する時の、「ネットワーク設定維持」オプションとは何でしょうか？

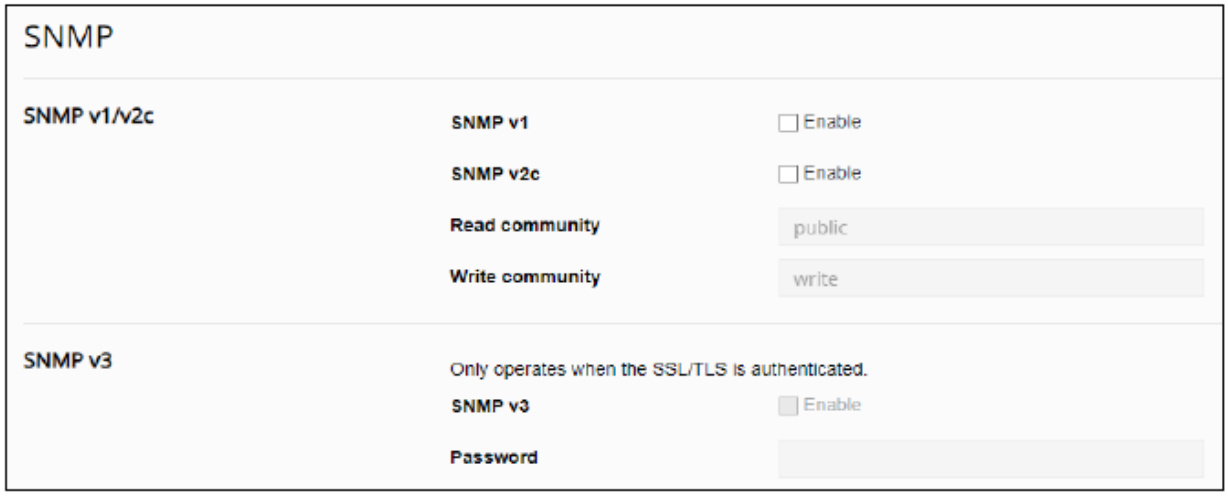
デバイスに設定されたネットワーク関連設定(IP、プロトコルモード、SNMP 設定など)をそのまま維持して出荷条件初期化を行うオプションです。「ネットワーク設定維持」オプションを選択する場合、既存の SNMP 設定が維持されるため、安全なセキュリティ設定のためには「ネットワーク設定維持」オプションを解除した後、初期化する必要があります。

2.2.2.SNMP サービスの無効化

SNMPサービスを使用していない状態で、当該機能が有効になっている場合にはサービス機能設定でSNMPサービスを選択解除して機能を制限することができます。

1) メニュー：設定 → ネットワーク → SNMP

2) SNMPv1、v2c 及び v3 すべて選択解除



[無効な SNMP サービス]

[旧バージョンカメラの無効な SNMP サービス]

Q&A) SNMPが無効になりません

2017 年以前のファームウェアを使用するデバイスは SNMP サービス全体を無効化できません。この場合、保有している当社デバイスの最新ファームウェアをハンファテックウィンのホームページ(www.hanwha-security.com)でアップデートした後、無効化できます。

2.2.3.SNMP v3 の使用

ネットワーク管理のためにSNMPサービスが必要な場合、安全なSNMP v3バージョン使用を推奨します。SNMP v3はネットワークを通じたパケット認証及び暗号化技術を組み合わせてデバイスにセキュリティアクセス(Access)機能を提供します。SNMP v3で提供するセキュリティ機能は次の通りです。

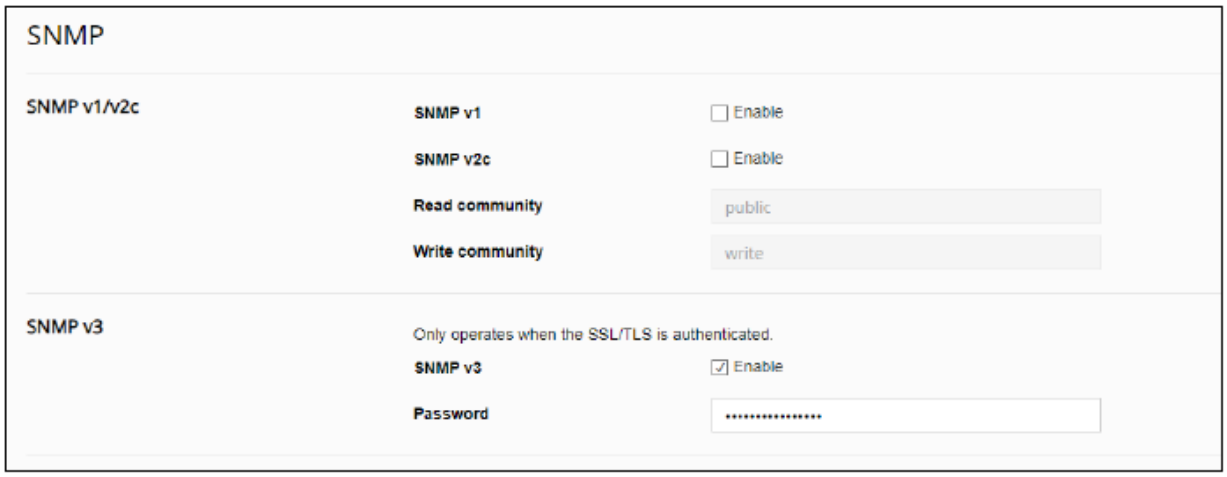
- メッセージの整合性 - パケットが伝送中に操作されないようにします。
- 認証 - メッセージの出所が有効であるかを確認します。
- 暗号化 - 権限のない原本でパケットを確認できないように、パケットコンテンツを暗号化します。

SNMPV3設定は以下の方法で設定できます。

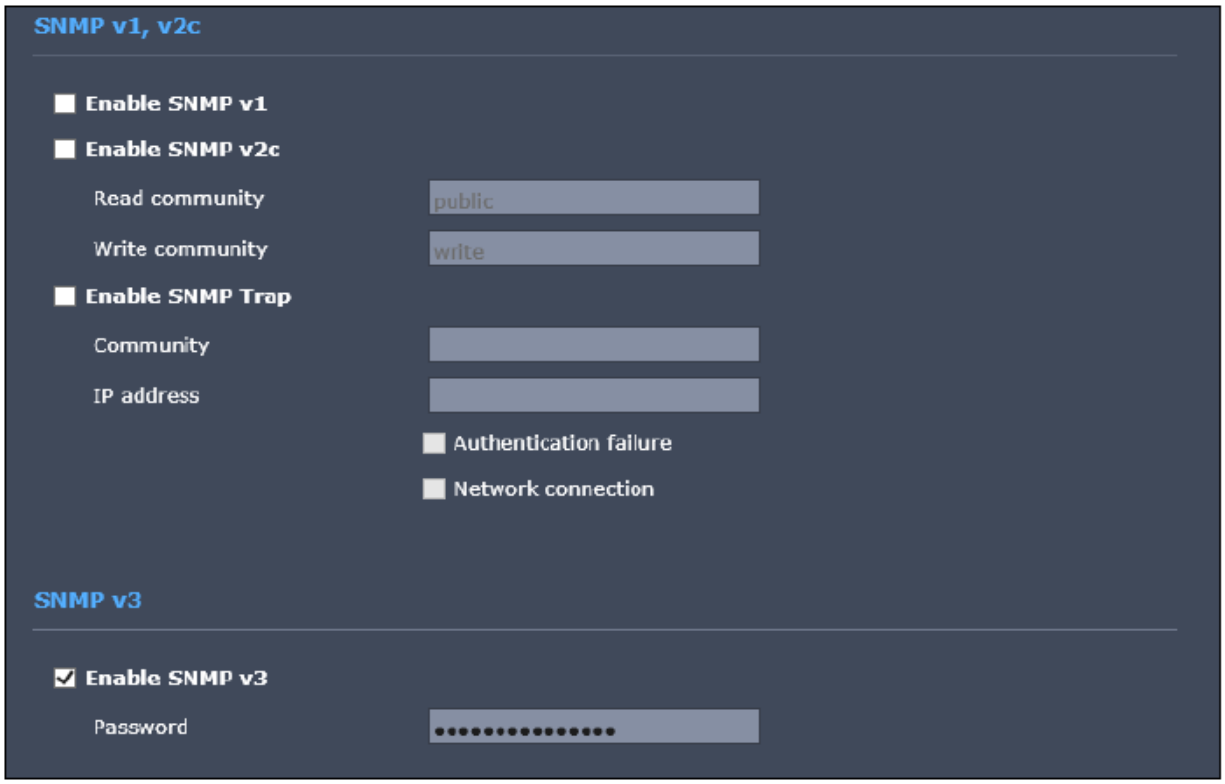
1) HTTPS モード設定(メニュー：設定 → ネットワーク → HTTPS または SSL)

2) SNMPv3 の有効化及びパスワード設定(メニュー：設定 → ネットワーク → SNMP)

※ パスワードは英数字を含めた 8 桁以上の構成を推奨する



[有効な SNMPv3 サービス]



[旧バージョンカメラの有効な SNMPV3 サービス]

2.2.4.SNMP Community String の変更

やむを得ずSNMP v1、SNMP v2cを使用する場合、認証のために使用されるSNMPプロトコルの初期Community Stringを「public」の代わりに第3者が推測できない文字列構成に変更して適用すると、より安全なネットワーク管理環境を構築できます。

例) 8桁以上の英文+数字の組み合わせ文字列：owa3fxpzmj

1) メニュー：設定 → ネットワーク → SNMP

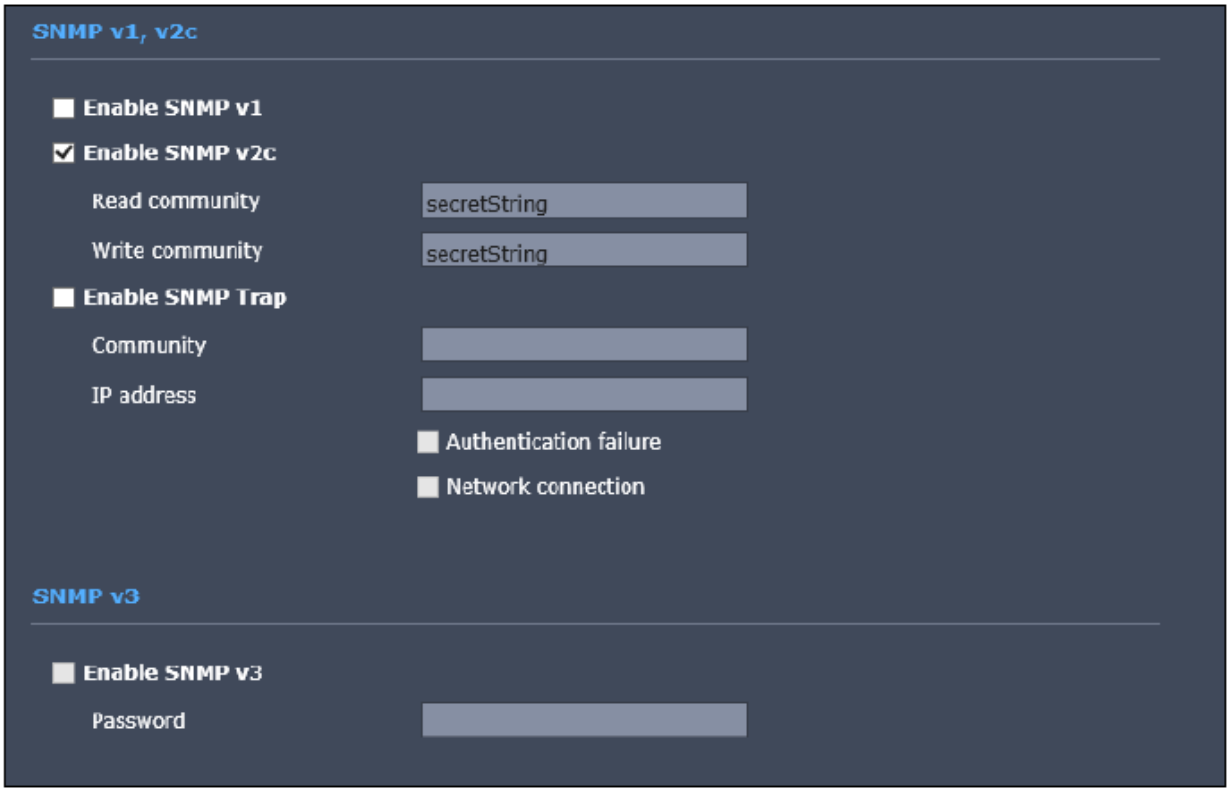
2) Read Community String を推測しにくい文字列に変更

3) Write Community String を推測しにくい文字列に変更

4) SNMP v1、SNMP v2c 適用

※ Community String は英数字を含めた 8 桁以上の構成を推奨する

[Community String の変更]



[旧バージョンカメラの Community String の変更]

WISENET

Hanwha Techwin Co.,Ltd.
13488 京畿道城南市盆唐区板橋路 319 番ギル 6
ハンファテックウィン R&D センター
TEL 070.7147.8771-8
FAX 031.8018.3715
http://hanwha-security.com

Hanwha Techwin