

White paper

ネットワークデバイスのセキュリティ強化ガイド (NVR)

2020年7月24日

V1.0

1. 序論

2. サイバーセキュリティレベルの定義

3. 基本レベル

4. 保護レベル

5. 安全レベル

6. 最上位安全レベル

| バージョン | 改訂日付 | 改訂内容 | 備考 |
|-------|-----------|------------|----|
| V1.0 | 2020.7.24 | 公式バージョンの制定 | |
| | | | |
| | | | |

昨今、顧客の財産と個人情報を保護するために開発されたネットワーク監視デバイスが、むしろ個人情報を奪取するための手段に使用される逆説的な状況がネットワーク監視マーケットで発生しています。ネットワーク監視デバイスは個人情報として使用できるビデオ映像を処理及び管理しており、ネットワークベースで通信するためグローバルネットワークに接続することで世界中どこからでもリモートアクセスできます。このような特性によってネットワーク監視デバイスはサイバー攻撃の対象となっています。

ハンファテックウィン は顧客の財産と個人情報を守り、サイバーセキュリティ強化のために努めます。本ガイド文書を通じて製品に実装されたセキュリティ機能を理解して安全に使用できるように案内させていただきます。

本ガイドは、次の基準に従ってサイバーセキュリティレベルを定義しました。各レベルは前のレベル達成を前提とします。

- 基本レベルは、ユーザーが別途の設定なくデバイスで基本提供する機能だけでも達成できるセキュリティレベルを意味します。
- 保護レベルは、ユーザーがデバイスを購入した初期状態や出荷条件初期化直後状態で基本設定されている初期設定値だけでも達成できるセキュリティレベルを意味します。
- 安全レベルは、デバイスで提供する機能やサービスによってセキュリティが弱くなる可能性があるため、不要な機能やサービスをユーザーが直接使用しないように設定することでセキュリティを向上するレベルを意味します。
- 最上位安全レベルは、デバイスで提供するセキュリティ機能と共に外部の追加セキュリティソリューションを連携してセキュリティを向上するレベルを意味します。

<表 1>

| サイバーセキュリティレベル | サイバーセキュリティの強化機能 & 策定 | 初期設定 | 推奨設定 |
|---------------|--|---------|------|
| 基本レベル | 複雑なパスワードの使用 | Default | - |
| | 連続パスワード失敗時の入力制限 | Default | - |
| | リモートサービス(Telnet、SSH)の無効化 | Default | - |
| | 環境設定情報の暗号化 | Default | - |
| | ファームウェア暗号化及び安全なアップデート | Default | - |
| | 抽出されたビデオフォーマットのウォーターマーク挿入と暗号化 | Default | - |
| | ログ情報を初期化対象外とする | Default | - |
| | HTML5 ベースの NonPlug-in ウェブビューアー 個別デバイス認証(デバイス認証) | Default | - |
| 保護レベル | 初期設定値の厳格化 | - | - |
| | マルチキャストの無効化 | 無効化 | - |
| | DDNS の無効化 | Off | - |
| | SNMP の無効化 | 無効化 | - |
| | オーディオ機能の無効化 | 不使用 | - |

| サイバーセキュリティレベル | サイバーセキュリティの強化機能&策定 | 初期設定 | 推奨設定 |
|---------------|--------------------------|--------------------|--------------------|
| 安全レベル | 最新バージョンのファームウェア使用有無を確認する | - | - |
| | 最新バージョンのファームウェアにアップデートする | - | - |
| | 正確な日付/時間を設定する | 初期値 | 変更 |
| | 安全な通信プロトコルを使用する(HTTP) | HTTP+HTTPS | HTTPS |
| | 安全な通信プロトコルを使用する(RTSP) | HTTPS+Wisent/ONVIF | HTTPS+RTSP |
| | HTTPS (私設認証保安接続モード) | HTTP | HTTPS(私設認証保安接続モード) |
| | HTTPS(公認保安接続モード) | HTTP | HTTPS(公認保安接続モード) |
| | 基本ポートを変更する | 初期値 | 変更 |
| | IP フィルタリング | 未設定 | 設定 |
| | 安全に SNMP を使用する | 未設定 | SNMP v3 |
| | 追加ユーザーアカウントを作成する | - | 設定 |
| 権限設定 | - | 設定 | |
| ログを点検する | - | - | |
| 最上位安全レベル | 802.1X 証明書ベースのアクセス制御 | 不使用 | 使用 |

※ 初期設定値が初期値になっている場合、ユーザーが選択できるオプションではなく基本設定で提供されることを意味します。ダッシュ(-)になっている場合、ユーザーが選択できるオプションは存在せず、点検/実行する必要がある活動を意味します。

ハンファテックウィンで提供するデバイスは、製品を購入した当時の基本機能または設定された初期値だけでもサイバーセキュリティの脅威から安全を保障するように考慮して開発されました。

<表 2>

| セキュリティポリシー | サイバーセキュリティ機能 | 簡単な説明 |
|--------------------|--------------------------------|---|
| パスワードポリシー | 複雑なパスワードの使用 | 最小 8 桁以上のパスワード複雑度(2 つまたは 3 つのタイプ)を持つ文字入力要求 |
| アクセス制御 | 連続パスワード失敗時の入力制限 | ウェブ UI ログイン時に不正者からのパスワードランダム入力攻撃遮断 |
| リモートアクセス制御セキュリティ | リモートサービス(Telnet、SSH)の無効化 | リモートでシステムにアクセスできるすべてのサービス除去 |
| 設定情報のバックアップセキュリティ | 環境設定情報の暗号化 | バックアップされた環境設定情報の保護 |
| ファームウェアセキュリティ | ファームウェア暗号化及び安全なアップデート | ファームウェアの重要情報の露出と分析を防止 ファームウェアの偽造・変造及び悪性コード注入防止 |
| 抽出された映像セキュリティ | 抽出されたビデオフォーマットのウォーターマーク挿入と暗号化 | 抽出されたビデオフォーマットの機密性と整合性の保障及び出所認証 |
| ログ記録セキュリティ | ログ情報を初期化対象外とする | 侵入者からの悪意のあるログ削除保護 |
| HTML5 ストリーミング性能の標準 | HTML5 ベースの NonPlug-in ウェブビューアー | Plug-in(ActiveX、シルバーライト、NPAPI)なく最適の映像サービスを提供 |
| 個別デバイス認証 | デバイス認証 | デバイス証明書を用いた暗号化通信時に信頼できるデバイス識別 |

3.1. 複雑なパスワードの使用

ハンファテックウィンデバイスのパスワードを設定するための最小文字は8桁以上であり、パスワードの長さによって英数字、特殊文字の中で3つ(8桁～9桁)または2つ(10桁以上)タイプの文字入力を要求します。このような強制設定はユーザーの不注意による弱いパスワード設定を防止して、悪意あるユーザーがパスワードを突破する可能性を低めます。

3.2. 連続パスワード失敗時の入力制限

ハッカーはデバイスのパスワードを探すためにランダム値を非常に素早い速度でデバイスに入力します。このような作業を許可する場合、デバイスのパスワードが解析されるリスクを取らなければなりません。セキュリティを向上するためにハンファテックウインのデバイスは、パスワード認証を5回連続失敗する時に30秒間入力を制限しています。これによってパスワードのランダム入力攻撃(Brute force attack)を遮断しており、単純にすべての接続を遮断する方法ではなく既存の認証された接続は維持して不正アクセス試行のみ遮断することでランダム入力攻撃を通じて誘発する可能性があるサービス拒否(DoS)攻撃も予防しています。

3.3. リモートサービス(Telnet、SSH)の無効化

ネットワークデバイスでテルネット(Telnet)のようなリモートサービスに対応するデーモンはメーカーが顧客にA/Sを便利に提供できるメリットは与えられますが、ハッカーや悪意のあるメーカーがある場合、最も危険なセキュリティ事故を起こす要因となります。ハンファテックウインの製品はこのようなリスクを取り除くポリシー策定することでセキュリティレベルを向上しました。

3.4. 環境設定情報の暗号化

バックアップ(Backup)機能を使用すると、デバイスの環境設定情報を込めたバイナリーファイルをPCにダウンロードできます。そしてリストア(Restore)機能を通じてバックアップした環境設定情報をリストアできます。

このような機能を活用する場合、一つのデバイス設定だけで同じモデル名を持つすべてのデバイスに対して同じ環境を設定することができます。バックアップした環境設定情報を込めた当該バイナリーファイルには、ユーザーデバイス環境の重要な情報が含まれるため、ハンファテックウィンでは環境設定情報をバックアップする時、安全な暗号化アルゴリズムを使用して保存しています。

3.5. ファームウェア暗号化及び安全なアップデート

ハンファテックウィンの製品は、機能追加/バグ改善及びセキュリティアップデートなどのためのファームウェアを提供する際に暗号化した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を通じて提供しています。また、ファームウェアアップデート時、偽造・変造されたファームウェアを識別し、デバイスの正常動作を保障するために整合性を検証した後にアップデートが完了されるようにしています。これによりハッカーがファームウェアに含まれている重要情報を分析できないようにしています。ファームウェア偽造・変造を通じて悪質なプログラムを挿入した後、デバイスに対する制御権限を奪取し異なる攻撃用ボットに使用できないようにしています。ファームウェアにはハッカーが悪用できる重要情報がたくさん含まれています。ハンファテックウィンの製品は、このようなファームウェアのセキュリティと安全なアップデートのために機密性及び整合性が保障されたファームウェアを配布しています。

3.6. 抽出されたビデオフォーマットのウォーターマーク挿入と暗号化

ハンファテックウィンのNVRを使用してSECファイルフォーマットで抽出したビデオファイルは、一般再生/編集用ソフトウェアでファイルを開くことができないため、録画データの外部への流出を予防しています。そしてウォーターマークを適用して映像の偽造・変造検知ができます。基本再生に必要なプレイヤーがSECファイルから自動抽出されるため、別途にプレイヤーをインストールする必要がありません。ユーザーがSECファイルをダブルクリックすることで、簡単にビデオファイルを再生することができます。

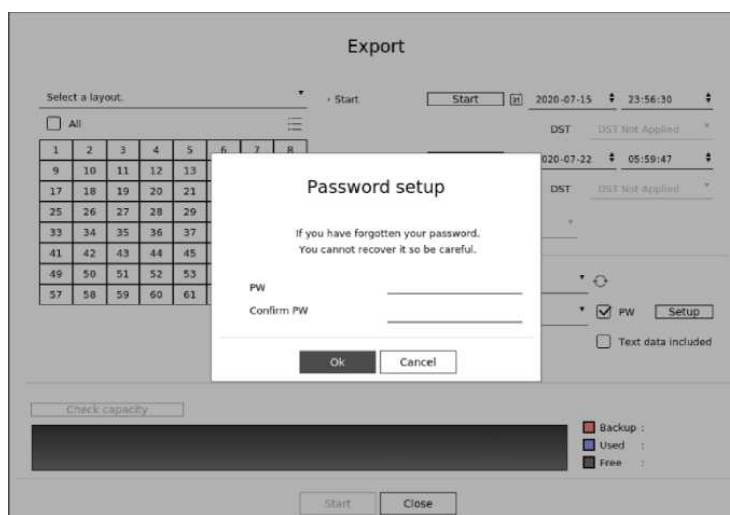
また、SECファイルフォーマットは、ビデオファイルを法的証拠または個人情報保護の目的で変造有無の確認及び機密性を保障できます。

<表 3>

| デバイス | 抽出位置 | バックアップ ファイルフォーマット | ウォーターマーク /暗号化の有無 | 電子署名の有無 | 再生プレイヤー |
|------|----------|----------------------|---------------------|---------|-------------------------|
| NVR | セット | NVR | X | X | セットでのみ再生可能 |
| | | SEC | O | X | バックアップビューアー (SECに内臓) |
| | ウェブビューアー | AVI | X | X | 汎用メディアプレイヤー |

● 設定(NVRセット設定)

: 検索 → Export選択 → チャンネル/時間情報の入力 → デバイス設定 → 保存タイプ (SEC)設定 → パスワードチェックボックスにチェック → パスワード設定

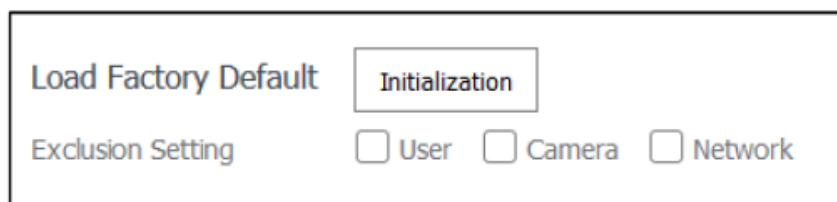


3.7. ログ情報を初期化対象外とする

ネットワークデバイスに誰かが侵入を試行したり、侵入した場合にログを確認して侵入経路を分析したり、事故の経緯を把握することはネットワーク管理者及びセキュリティ管理者にとっても重要な機能です。しかし、ハッカーはこのようなネットワークデバイスのログ機能を知っているため、侵入する時に記録されたログを強制的に削除して自分の痕跡を残さないようにします。ハンファテックウィンのデバイスは、このような悪意のあるログ削除やデバイス初期化を行ってもログが初期状態にならないようにしています。つまり、次のように出荷条件初期化を実行してもカメラに保存されたログは絶対に初期化されません。

- 設定(NVR)

: システム環境 → システム管理 → Settings → 初期化設定



3.8. HTML5 ベースの NonPlug-in ウェブビューアー

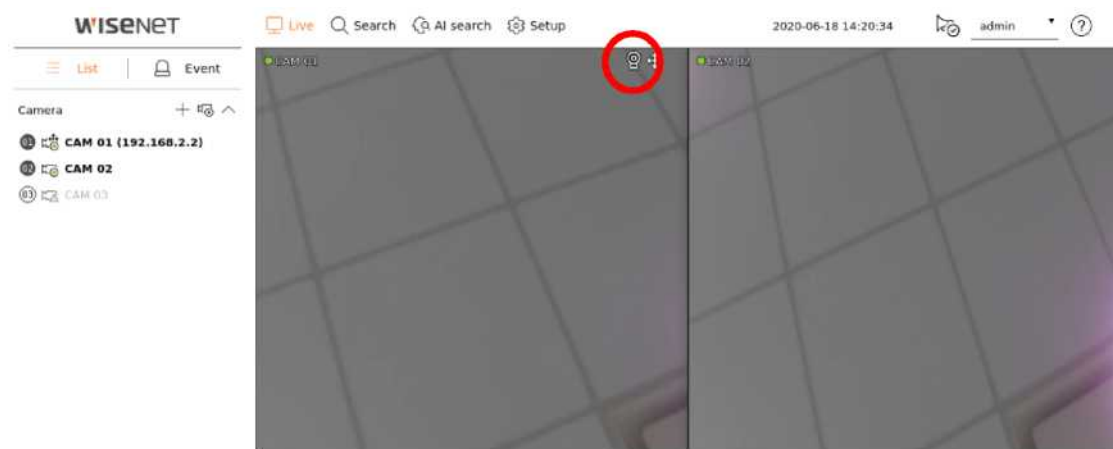
ユーザーはNVRで提供する映像を別途のクライアントをインストールすることなく、汎用ブラウザで簡単に確認できます。業界ほとんどのウェブビューアーはブラウザにインストールされるPlug-in(ActiveX、シルバークライアント、NPAPI)技術を用いて映像ストリーミング性能サービスを提供していますが、このようなPlug-in技術はユーザー環境にインストールされる構造であり、ユーザーリソースに対するセキュリティ脆弱性が発生する可能性が高く、最近ActiveXセキュリティ脆弱性による悪質なプログラム感染事例が頻繁に発生しています。これにブラウザの提供を行っている会社はPlug-inのインストール対応を中止して、映像&音声のようにメディア使用ができるHTML最新標準(HTML5)を通じてサービスを提供する方向で標準化が行われています。このような流れに合わせてハンファテックウィンはPlug-inをインストールすることなく、ウェブ標準化に対応して最適の映像サービスを提供するHTML5ストリーミング性能のウェブビューアーサービスを提供してセキュリティとユーザービリティを強化しました。

3.9. 個別デバイス認証

ハンファテックウィンで提供するネットワークデバイスは暗号化通信時、デバイス証明書を用いたデバイス識別機能が搭載されています。これによりハンファテックウィンで製造した信頼できるデバイスであるかどうかを確認でき、ハッカーが中間者攻撃で任意にセキュリティ通信を盗聴したり、操作できないようにしたりしてセキュリティを強化できます。つまり、ハンファテックウィンで製造したカメラとの接続時、ストレージデバイスはカメラと暗号化通信実行と同時に以下のようにデバイスに対する検証を行い、信頼できるデバイスであることを証明します。

- デバイス認証(NVR) - セットで確認可能

: セットに接続した後、Live画面でデバイス証明書のアイコン確認



また、当社デバイス間の接続ではなく、ウェブビューアー(ウェブブラウザ)接続に対してもデバイス認証を適用できるように「ハンファテックウィンのPrivate Root CA証明書の事前インストールガイド」を配布/案内しています。

インストールガイドは、当社のホームページにて確認できます。

- [ハンファテックウィンのPrivate Root CAの事前インストールガイド](https://www.hanwha-security.com/ko/technical-guides/cybersecurity/)
(<https://www.hanwha-security.com/ko/technical-guides/cybersecurity/>)

ハンファテックウィンのデバイスは購入初期状態または出荷条件初期化直後の初期設定値でも基本的なセキュリティレベルを確保しております。

<表 4>

| セキュリティポリシー | サイバーセキュリティ機能 | 簡単な説明 |
|------------|--------------|---------------------------|
| サービス保護 | 初期設定値の厳格化 | 初期設定値をセキュリティ優先とする |
| | マルチキャストの無効化 | 不要なサービスは無効として悪意のある攻撃を防止する |
| | DDNS の無効化 | |
| | SNMP の無効化 | |
| | オーディオ機能の無効化 | |

4.1. 初期設定値の厳格化

デバイスが初期状態ではない場合、初期化を実行してデバイスの設定を初期化することが必要になる場合があります。こうして実行した初期状態だけでもハンファテックウィンのデバイスは、保護レベルのセキュリティレベルを達成することができます。

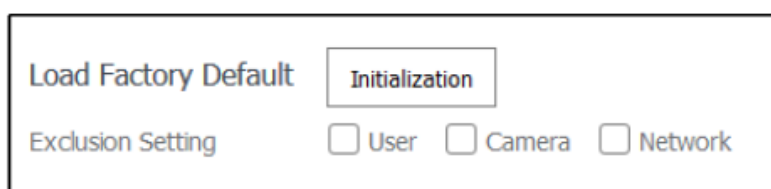
- 設定(NVR)

- 1) システム環境 → システム管理 → Settings → 初期化設定

- 2) User/Camera/Network 設定の選択解除

(当該設定を選択解除しない場合、当該項目の設定値が維持されシステム設定が初期化となる)

- 3) 初期化ボタンをクリック



4.2. マルチキャストの無効化

マルチキャスト使用を指定する機能でRTSPプロトコルを設定することができます。このサービスは基本設定値が無効になっています。当該サービスが不要の場合、セキュリティ強化のために無効化状態に維持することを推奨します。

- 設定(NVR)

- 1) 設定 → ネットワーク → ポート → マルチキャスト

- 2) マルチキャスト(RTSP)の無効化維持

| Port | |
|----------------------|--------------------|
| Protocol Type | TCP |
| RTSP | 558 |
| UDP Port | 8000~8159 |
| Multicast IP Address | 224 . 126 . 63 . 1 |
| Multicast TTL | 3 |
| HTTP port | 80 |
| HTTPS port | 443 |
| Cam Proxy Port | 10001 ~ 10064 |

4.3. DDNS の無効化

ストレージデバイスがDHCP方式のケーブルモデムやDSLモデムもしくはPPPoEモデムに直接接続されている場合、ISPに接続を試すたびにIPアドレスが変更されます。この場合、ユーザーは変更されたIPアドレスを知ることができないが、DDNS機能を通じて製品のIDを事前登録すると、変更されたIPアドレスへ簡単にアクセスできます。当該サービスが不要の場合、セキュリティ強化のためにサービス機能の設定を選択解除してください。

- 設定(NVR)

- 1) ネットワーク → DDNS → 不使用を選択
- 2) 確認ボタンをクリック

4.4. SNMP の無効化

ハンファテックウィンのデバイスはSNMP v1、v2c及びv3の機能と同時に対応します。SNMPサービスが不要の場合、セキュリティ強化のためにサービス機能の設定を選択解除します。

- 設定(NVR)

- 1) ネットワーク → SNMP
- 2) SNMP v1、v2c 及び v3 選択解除


4.5. オーディオ機能の無効化

オーディオ使用機能は、映像と音を共に入力する機能です。当該サービスが不要の場合、セキュリティ強化のためにサービス機能の設定を解除します。オーディオ使用機能は、4チャンネルの録画ファイルごとに個別設定できるため、すでに設定されている各録画ファイルを選択して不使用に設定する必要があります。

• 設定(NVR)

- 1) 設定 → 録画 → 録画設定
- 2) 設定された各録画ファイルを選択した後、オーディオ不使用を選択
- 3) 確認ボタンをクリック

Record setup

Total bitrate (limit/max) 147.2 / 150.0 Mbps  Apply to CH

| CH ▶ | Normal recording▶ | Event▶ | Frame | | | Event | | Audio▶ |
|------|-------------------|--------|-------|---------|-------|-------|--------|--------|
| | | | FULL | I-frame | Limit | Pre▶ | Post▶ | |
| 1 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 2 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 3 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 4 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 5 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 6 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 7 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 8 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 9 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 10 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 11 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 12 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 13 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 14 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 15 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 16 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 17 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |
| 18 | FULL | FULL | - | - | 2.3 M | 5 sec | 30 sec | Off |

ハンファテックウィンは、実際に使用しない不要なサービスやポートが開いている場合、外部から攻撃対象になるため、ユーザーが直接不要な機能やサービスを使用しないように設定してセキュリティを向上することができます。

<表 5>

| セキュリティポリシー | サイバーセキュリティ機能 | 簡単な説明 |
|------------|--------------------------------|---|
| - | 最新バージョンのファームウェア使用の有無確認及びアップデート | 最新バージョンのファームウェアを使用しているかを確認してセキュリティに弱いファームウェアの場合にはアップデート実行 |
| - | 正確な日付/時間を設定する | ログ分析のために正確な日付&時間を設定 |
| - | 安全な通信プロトコルを使用する(HTTP) | ウェブビューアー上で送受信される個人情報及び映像保護 |
| - | 安全な通信プロトコルを使用する(RTSP) | RTSP を通じて伝送される映像保護 |
| - | HTTPS(私設認証保安接続モード) | 証明書を通じたデバイスとクライアント間のセキュリティアクセス |
| - | HTTPS(公認保安接続モード) | |
| - | 基本ポートの変更 | ポート変更を通じてウェブサービスのアクセス攻撃防止 |
| アクセス統制 | IP フィルタリング | 特定 IP のアクセス許可/拒否を通じてアクセス攻撃防止 |
| サービス保護 | 安全に SNMP を使用する | セキュリティ強化のために SNMP 初期値をすべて解除 |
| - | ユーザーグループ/ユーザー作成 | よく使用する機能は、最小権限のユーザーアカウントを作成してセキュリティを強化 |
| - | 権限設定 | 機能に対するアクセス権限を与えて情報露出防止 |
| 監査 | ログを点検する | 不正者のアクセス記録分析 |

5.1. 最新バージョンのファームウェア使用の有無確認及びアップデート

ハンファテックウインのホームページ(www.hanwha-security.com)を通じて顧客が使用する製品の最新ファームウェアバージョンを確認できます。以下の画像では顧客がPRN-6410DB4モデルを使用する場合、現在配布されている最新ファームウェアバージョンが3.04.64_200515152334であり、その他のMAC Address、RAIDバージョン、オープンソース告知文情報も確認できます。Software Upgradeのためには、ハンファテックウインのホームページで当該製品のファームウェアをダウンロードして、Upgradeボタンをクリックしてアップグレードを行います。現在使用する製品のファームウェアバージョンが常時最新になるように点検してください。

- www.hanwha-security.com → 製品紹介 → 製品の詳細ページ → ファームウェアダウンロード
- 設定(NVR)
 - 1) 設定 → システム環境 → システム管理 → システム情報 → S/W アップグレード
 - 2) 製品の現在 S/W バージョン確認
 - 3) 検索ボタンをクリックして、ダウンロードした最新のファームウェア選択
 - 4) アップグレードボタンをクリック

| System Information | |
|--|---|
| Model Name | PRN-6410DB4 |
| Software Version | 3.04.64_200515152334 |
| MAC Address 1 | 00:09:18:E1:A1:92 |
| MAC Address 2 | 00:09:18:E1:A1:93 |
| MAC Address 3 | 00:09:18:E1:A1:91 |
| RAID Version | 2.0.5.7063 |
| Open Source Announcement | |
| S/W Upgrade | <input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Upgrade"/> |
| Server Upgrade | <input type="text"/> <input type="button" value="Upgrade"/> |
| <input checked="" type="checkbox"/> Enable online upgrade <input type="button" value="Apply"/> | |
| Device Name | PRN-6410DB4 |
| Power Control | <input type="button" value="Shutdown"/> <input type="button" value="Restart"/> |
| <input type="button" value="Ok"/> | |

5.2. 正確な日付/時間を設定する

日付&時間機能は、デバイスで出力するシステムログのような情報を分析する時にログの正確な時間情報を確認するための前提条件であるため、現在システムの時間を正確に設定することは非常に重要なセキュリティ活動です。設定されている現在のシステム時間が正しく設定されていない場合、ユーザーは時間を設定してシステムに適用される時間を設定することができます。

- 設定(NVR)

- 1) 設定 → システム環境 → 日付/時間/言語に移動

- 2) グリニッジ標準時(GMT)基準の現在居住地域のタイムゾーンを設定

(SUMMER TIME(DST)の使用オプションは、タイムゾーンで SUMMER TIME を使用する地域を選択する場合のみ表示され、当該機能が適用される場合に選択します。選択して適用した後は、その地域の標準時より一時間進めた時間に設定される)

- 3) 修正を選択してシステムに適用される時間を設定

- 4) 時間の同期化設定

- 5) システム時間設定の確認ボタンをクリック

Date/Time/Language

System Time: 2020-06-04 15:15:45

Modify:

Date: 2020 * 6 * 4 * YYYY-MM-DD

Time: 15 * 15 * 42 * PM * 24 Hour

Time zone: GMT

Time Sync:

DST: Enable

Start: Mar * Last * Sunday * 1H *

End: Oct * Last * Sunday * 1H *

Language: 한국어

Holiday: 2020 * Apr-Jun *

| Apr | | | | | | | May | | | | | | | Jun | | | | | | |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| Sun | Mon | Tue | Wed | Thu | Fri | Sat | Sun | Mon | Tue | Wed | Thu | Fri | Sat | Sun | Mon | Tue | Wed | Thu | Fri | Sat |
| 29 | 30 | 31 | 1 | 2 | 3 | 4 | 26 | 27 | 28 | 29 | 30 | 1 | 2 | 21 | 1 | 2 | 3 | 4 | 5 | 6 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 26 | 27 | 28 | 29 | 30 | 1 | 2 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 28 | 29 | 30 | 1 | 2 | 3 | 4 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 31 | 1 | 2 | 3 | 4 | 5 | 6 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |

5.3. 安全な通信プロトコルを使用する(HTTP)

ハンファテックウィンのNVRは、サーバーとクライアント間のHTTP+HTTPSモードを初期設定値に提供しています。HTTP/HTTPSの両方ともDigest認証タイプを適用しているため、通信上にユーザーのパスワードは保護でき、HTTPSモードで送受信される映像データのような重要情報を暗号化通信で安全に保護します。

5.4. 安全な通信プロトコルを使用する(RTSP)

HTTPSモード以外にもRTSPを通じて伝送される映像ストリーミング性能も安全に保護される必要があります。RTSPを通じた映像を保護するためには、クライアントからRTSPをHTTPSにトンネリングする追加設定作業が必要です。例えば、IPカメラからNVRに伝送される映像をHTTPSで保護する場合、まずIPカメラのウェブビューアーでHTTPSモードに設定します。そしてNVRにカメラを接続した後、Set UIまたはNVRのウェブビューアーを通じてRTSPモードに設定します。

- 設定(NVR)

: デバイス → カメラ → カメラ登録 → チャンネル選択 → カメラ修正

| Edit Camera | |
|---|---|
| CH | 1 |
| Protocol | <input type="radio"/> Wisenet <input type="radio"/> ONVIF <input checked="" type="radio"/> RTSP |
| Access Address | rtsp://192.168.1.123:443/stream1 |
| ID | admin |
| Password | |
| More Detail | <input type="checkbox"/> |
| Mode | <input type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS |
| <input type="button" value="Ok"/> <input type="button" value="Cancel"/> | |

5.5. HTTPS(私設認証保安接続モード)

最初のセキュリティアクセスタイプは、HTTPとHTTPSを同時に対応します。HTTPS(自体認証保安接続モード)はハンファテックウィンから提供する自体証明書を使用してデバイスとクライアント間のセキュリティアクセスを可能にする機能です。HTTPS(自体認証保安接続モード)を選択する場合には、デバイスに内蔵された自体証明書がセキュリティアクセスモード時に有効となり、ユーザーが別途の証明書を登録する必要がありません。

- 設定(NVR)
 - 1) ネットワーク → HTTPS → セキュリティアクセスタイプ
 - 2) HTTPS(私設認証保安接続モード)を選択
 - 3) 適用ボタンをクリック

HTTPS

Secured Connection System

HTTPS ON / HTTP ON
 HTTPS ON / HTTP OFF
 HTTPS OFF / HTTP ON
 HTTPS OFF / HTTP OFF (Alert)

5.6. HTTPS(公認保安接続モード)

ハンファテックウィンから提供する自体証明書を使用せず、ユーザーが自分の公認証明書を直接登録してデバイスとクライアント間のセキュリティアクセスできる機能です。公認証明書のインストールで公認証明書とプライベートキーを登録すると、HTTPS(公認保安接続モード)の選択が有効になり、登録した公認証明書とプライベートキーがセキュリティアクセスモード時に有効となります。

- 設定(NVR)
 - 1) ネットワーク → HTTPS → 公認証設定
 - 2) 証明書名を入力した後、証明書ファイルに使用する公認証明書を指定
 - 3) キーファイルに使用するプライベートキーを指定した後、インストールボタンをクリック
 - 4) HTTPS(公認保安接続モード)を選択した後、適用ボタンをクリック

- ※ HTTPS(公認保安接続モード)項目は登録された公認証明書がある場合のみ選択できます。
- ※ 登録した公認証明書とプライベートキーを削除する場合、削除ボタンをクリックします。公認証明書の削除は、HTTP(保安接続不使用)やHTTPS(自体認証保安接続モード)にアクセスした場合のみ削除できます。

5.7. 基本ポートの変更

ネットワークデバイスの基本ポートを通じてスキャンしたり、攻撃する場合を防いだりするためには一般的によく知られているポートを使用するよりユーザーがポートを再指定して使用することが安全です。例えば、ウェブブラウザを通じてアクセスできるHTTPウェブサービスポートを80ではなく8000に変更する場合、単純なスキャンプログラムやウェブブラウザにアドレスを直接入力する攻撃からウェブサービスアクセスを保護できます。

● 設定(NVR)

- 1) 設定 → ネットワーク → インターフェース → ポート
- 2) HTTP ポートと HTTPS ポートをそれぞれ 80 と 443 から上位ポートに設定変更
- 3) RTSP ポートを 558 から上位ポートに設定変更
- 4) 確認ボタンをクリック

| Port | |
|----------------------|--------------------|
| Protocol Type | TCP |
| RTSP | 558 |
| UDP Port | 8000-8159 |
| Multicast IP Address | 224 . 126 . 63 . 1 |
| Multicast TTL | 5 |
| HTTP port | 80 |
| HTTPS port | 443 |
| Cam Proxy Port | 10001 ~ 10064 |

| Port | |
|----------------------|--------------------|
| Protocol Type | TCP |
| RTSP | 8558 |
| UDP Port | 8000-8159 |
| Multicast IP Address | 224 . 126 . 63 . 1 |
| Multicast TTL | 5 |
| HTTP port | 8000 |
| HTTPS port | 4443 |
| Cam Proxy Port | 10001 ~ 10064 |

- ※ ポートを再指定する時に接続されているカメラや VMS との接続問題が発生する可能性があるため、当該接続デバイスの設定変更も必要です。問題が解決されない場合、基本ポートに復旧してください。

5.8. IP フィルタリング

特定IPに対してアクセスを許可または拒否するように、IPリストを作成できます。

• 設定(NVR)

1) 設定 → ネットワーク → IP フィルタリング

2) フィルタリング形式の選択

(拒否：フィルタリングに登録された IP のアクセス遮断/許可：フィルタリングに登録された IP のみアクセス許可)

3) 入力ウィンドウをクリック

IP filtering

Filtering Type Deny Allow

IPv4 Delete

| <input type="checkbox"/> | Use> | IP Address | Prefix | Filtering Range |
|--------------------------|------|------------|--------|-----------------|
| <input type="checkbox"/> | On | | | |
| <input type="checkbox"/> | On | | | |
| <input type="checkbox"/> | On | | | |
| <input type="checkbox"/> | On | | | |
| <input type="checkbox"/> | On | | | |
| <input type="checkbox"/> | On | | | |
| <input type="checkbox"/> | On | | | |
| <input type="checkbox"/> | On | | | |
| <input type="checkbox"/> | On | | | |
| <input type="checkbox"/> | On | | | |
| <input type="checkbox"/> | On | | | |
| <input type="checkbox"/> | On | | | |

4) 許可または拒否する IP 入力 IP アドレス及び Prefix を入力すると、右側のフィルタリング範囲項目に遮断または許可される IP アドレス範囲が表示される

IPv4 Delete

| <input type="checkbox"/> | Use> | IP Address | Prefix | Filtering Range |
|-------------------------------------|------|--------------|--------|-----------------------------|
| <input checked="" type="checkbox"/> | On | 192.168.0.10 | 31 | 192.168.0.10 ~ 192.168.0.11 |

5) 設定完了後、確認ボタンクリック

※ IP フィルタリングで許可を選択して IPv6 を使用することに設定した場合、現在設定している PC の IPv4 と IPv6 アドレスをすべて登録する必要があります。現在設定している PC の IP は拒否に登録できず、許可に登録する必要があります。この後に設定した IP のみアクセスできます。

5.9. 安全に SNMP を使用する

SNMPはネットワークデバイスを便利に管理できる機能を提供します。基本にハンファテックウィンのセキュリティ強化のためにすべて選択解除されています。安全にSNMPを使用するためには、SNMP v3にのみ設定して使用することを推奨します。

SNMP v1及びv2cは基本にDefaultコミュニティ文字列を通じてSNMP機能が提供されるため、セキュリティに弱いのですが、ユーザーがコミュニティ文字列を変更して使用できます。SNMP v1、v2cを使用する場合、コミュニティ文字列を変更して使用することを推奨します。

• 設定(NVR)

- 1) 設定 → ネットワーク → SNMP
- 2) SNMP v1 と SNMP v2c の使用選択解除
- 3) SNMP v3 使用選択及びパスワード設定

| SNMP | | |
|--|-----------------|---------|
| <input type="checkbox"/> Enable SNMP v1 | | |
| <input type="checkbox"/> Enable SNMP v2c | Read Community | public |
| | Write Community | private |
| <input type="checkbox"/> Enable SNMP v3 | Password | |
| <input type="checkbox"/> Enable SNMP Traps | Trap Manager | 0.0.0.0 |

5.10. ユーザーグループ/ユーザー作成

管理者アカウントでのみデバイスにアクセスして使用する時に、管理者パスワードがネットワークを通じて持続的に伝送する可能性があり、悪意のある目的でネットワークを持続的にモニタリングする人に重要な資格情報が流出するセキュリティの脆弱性が発生することがあります。そのため、よく使用しない設定機能は管理者によって実行することにして、よく使用する映像モニタリング機能の場合、より低い権限を持つ追加ユーザーグループ/ユーザーアカウントを作成して実行することでセキュリティを高めることができます。

• 設定(NVR)

- 1) 設定 → システム環境 → ユーザー → ユーザー
- 2) ユーザーグループ追加後、ユーザーアカウントの追加
- 3) ユーザーグループに対する権限設定

The image displays two screenshots of the WISENET user management interface. The top screenshot shows the 'Group Information' settings for a user group. It includes a 'Group Name' field and a 'Permission' section with checkboxes for Live View, Search, Backup, Menu, Record, Record stop, PTZ, Remote alarm out, and Shutdown. Each permission has a corresponding 'Setup' button. The bottom screenshot shows the 'User Information' form for creating a user. It includes fields for Group, Name, ID, Password, and Confirm PW. There is a 'View password' checkbox and radio buttons for 'Viewer' status (Not Use or Use).

5.11. 権限設定

デバイスを使用する時の機能、ネットワーク及びログインに対するアクセス権限を設定できます。機能及びネットワークアクセス制限は、すべてのユーザーに認証なく使用を許可するか、パスワード認証後に権限のあるユーザーにのみ使用を許可するかを設定できます。ただし、機能別のアクセス権限はLive、Search、Backup機能の特定チャンネルに対してのみ権限が設定されている場合、当該チャンネルでのみ権限が設定された機能を使用することができます。

ログインに対するアクセス権限は設定された時間の間に入力がないと自動ログアウトされます。また、ID手動入力に対する設定はログインする時にIDを直接入力するかIDの入力なく、IDリストを通じて選択するかを設定できます。

• 設定(NVR)

- 1) 設定 → システム環境 → ユーザー → 権限設定
- 2) アクセス制限/ネットワークアクセス制限/自動ログアウト/ID 手動入力設定

Permission Setup

Restricted Access

| | | | | |
|---|--|--|--|---|
| <input checked="" type="checkbox"/> All | <input checked="" type="checkbox"/> Live View | <input checked="" type="checkbox"/> PTZ | <input checked="" type="checkbox"/> Record | <input checked="" type="checkbox"/> Record stop |
| | <input checked="" type="checkbox"/> Remote alarm out | <input checked="" type="checkbox"/> Search | <input checked="" type="checkbox"/> Backup | <input checked="" type="checkbox"/> Shutdown |

Restriction on Network Access

| | |
|--------------------------------------|-------------------------------------|
| <input type="checkbox"/> All Network | <input type="checkbox"/> Web Viewer |
|--------------------------------------|-------------------------------------|

Auto Logout 3 min ▼

Manual Input of ID On Off

5.12. ログを点検する

デバイスに悪意のあるユーザーがアクセスした場合の痕跡を探すために、管理者はシステムに保存されているログを分析できます。当該ログを通じてデバイスアクセス/システム設定変更/イベントなどの様々な情報を確認でき、デバイスを含むネットワークシステムのセキュリティを高める重要なデータに活用できます。ログデータの点検及び分析が必要な理由は次の通りです。

- システムで発生するすべての問題(エラー及びセキュリティの問題を含む)が記録され、唯一の手がかりになります。
- システムで発生したエラー及びセキュリティの問題に関する検索ができます。
- 潜在的なシステム問題を予測するために使用することがあります。
- 障害発生時、復旧に必要な情報に活用できます。
- セキュリティ事故の発生時、証拠資料として活用できます。
- 各種法規及び指針でログ管理が義務化されています。
- 設定(NVR)


: 設定 → システム環境 → ログ情報 → システムログ/イベントログ/バックアップログ

| System log | | | |
|------------|----------|---|---------------------|
| All CHs | View all | Today | 2020 6 16 |
| No. | CH | Log List | Date/Time |
| 24 | - | Setup Start (Admin) : IP-192.168.2.70 (WEB) | 2020-06-16 10:31:23 |
| 23 | - | Setup Start (Admin) : IP-192.168.2.70 (WEB) | 2020-06-16 10:26:35 |
| 22 | - | Setup Start (Admin) : IP-192.168.2.70 (WEB) | 2020-06-16 10:18:19 |
| 21 | - | Setup Start (Admin) : IP-192.168.2.70 (WEB) | 2020-06-16 10:01:59 |
| 20 | - | Setup Start (Admin) : IP-192.168.2.70 (WEB) | 2020-06-16 09:57:04 |
| 19 | - | Logout (Admin) : Local | 2020-06-16 08:38:14 |
| 18 | - | Network2 connected | 2020-06-16 08:34:53 |
| 17 | - | Network3 Disconnected | 2020-06-16 08:34:51 |
| 16 | - | Login (Admin) : Local | 2020-06-16 08:33:26 |
| 15 | - | DSP(Display) Start | 2020-06-16 08:33:10 |

< 1 / 3 >

Export

Event log

All CHs ▾ View all ▾  Today 2020 ▾ 6 ▾ 16 ▾

| No. ▾ | CH | Log List | Date/Time |
|--|----|----------|-----------|
| < <input type="text" value="0"/> / 0 > | | | |

Backup log

~ | | | | | |

| No. ▾ | User | Date/Time |
|-------------------------------------|------|-----------|
| < <input type="text" value=""/> / > | | |

ハンファテックウィンのデバイスで提供するセキュリティ機能と外部追加セキュリティソリューションを連携してセキュリティを向上することができます。

<表 7>

| セキュリティポリシー | サイバーセキュリティ機能 | 簡単な説明 |
|------------|----------------------|----------------------------|
| " | 802.1X 証明書ベースのアクセス制御 | ポートベースのアクセス制御設定でセキュリティ環境強化 |

6.1. 802.1x 証明書ベースのアクセス制御

ネットワークスイッチ、ブリッジ、無線アクセスポイント(AP)などに接続されたネットワークデバイスに対してポートベースのアクセス制御を設定すると、より強力なネットワークセキュリティ環境を構成することができます。ハンファテックウィンNVRのCamera, Viewer、iSCSIに対応する802.1xは証明書を必要とする標準方式のEAP-TLSを使用します。

802.1Xに対応するネットワークスイッチ(またはブリッジ、無線APなど)と802.1x認証サーバー、デバイス別の証明書及びプライベートキーが必要であり、次のようにデバイス別の証明書及びプライベートキーは設定ページを通じてインストールします。

• 設定(NVR)

- 1) 設定 → ネットワーク → 802.1X
- 2) カメラまたはビューアーまたは iSCSI 選択
- 3) EAPOL バージョンを 1 または 2 に設定
- 4) クライアントの証明書 ID とプライベートキーのパスワード入力
 - ※ 暗号化されていないプライベートキーファイルを使用する場合、入力する必要がありません。
- 5) 公認証明書を通じて認証サーバーの CA 公認証明書をインストール
- 6) ポートベースのアクセス制御を使用する場合、クライアント証明書とプライベートキーのインストール
 - ※ インストール済みの証明書とプライベートキーは RADIUS サーバーと Client デバイス間の TLS 通信にのみ使用されます。
- 7) 確認ボタンをクリック

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>

Copyright © 2020 Hanwha Techwin. All rights reserved.

