

White paper

ネットワークデバイスのセキュリティ強化ガイド (IP カメラ)

2020年5月8日

V3.0

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	2017.6.13	公式バージョンの制定	
V2.0	2018.1.16	<ul style="list-style-type: none"> - HTML5 ベースの NonPlug-in ウェブビューアーの基本レベル追加 - 安全に SNMP 使用を安全レベルから保護レベルに変更(Default 値を off に変更) - SNMP 無効化削除 - カメラウェブビューアーのバックアップフォーマット STW 削除 - マルチキャストの無効化 SVNP プロトコル削除 	
V3.0	2020.4.	<ul style="list-style-type: none"> - 個別デバイス認証(デバイス/ユーザー認証)追加 - 出荷条件初期化状態で SUNAPI/ONVIF を無効化追加 - Secure Boot 追加 - 安全な通信プロトコルを使用する(HTTP)を保護レベルから安全レベルに変更 - 安全に SNMP 使用を保護レベルから安全レベルに変更 - SNMP の無効化を保護レベルへ追加 - Link-Local IPv4 アドレスの無効化、UPnP 検索の無効化、Bonjour 無効化を安全レベルから保護レベルに変更 - HTTP 認証(Digest 認証のみ使用)項目を安全な通信プロトコルを使用する(HTTP)に変更して保護レベルに追加 - 最新バージョンの TLS 使用追加 - 安全な Cipher Suites 使用追加 - 安全な通信プロトコル(RTSP)追加 - 保存暗号化/バックアップ暗号化追加 	

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	-
	パスワード初期値の削除	Default	-
	連続パスワード失敗時に入力制限	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	-
	初期化する時にログ維持	Default	-
	HTML5 ベースの NonPlug-in ウェブビューアー	Default	-
	個別デバイス認証(デバイス/ユーザー認証)	Default	-
	出荷条件初期化状態で SUNAPI/ONVIF の無効化	Default	-
セキュアブート(Secure Boot)	Default	-	

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
保護レベル	出荷条件初期化を行う	-	-
	ゲストログイン機能の無効化	未設定	-
	認証されていない RTSP への接続許可の無効化	未設定	-
	マルチキャストの無効化	無効化	-
	DDNS の無効化	Off	-
	QoS の無効化	未設定	-
	ftp の無効化	未設定	-
	SNMP の無効化	無効化	-
	Link-Local IPv4 アドレスの無効化	無効化	-
	UPnP 検索の無効化	無効化	-
	Bonjour の無効化	無効化	-
	最新バージョンの TLS 使用	TLS 1.2/1.3	-
	安全な Cipher Suites 使用	Secure Cipher Suites	-
	音声入力の無効化	不使用	-
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+Wisenet/ONVIF	HTTPS+RTSP
	HTTPS(自体認証保安接続モード)	HTTP	HTTPS(自体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
	TLS を用いた E-mail 送信	無効化	有効化
	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	-	-
	ログを点検する	-	-
保存データの暗号化(LUKS 暗号化)	未設定	設定	
バックアップデータの暗号化(ZIP ファイルの暗号化)	未設定	設定	
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
	パスワード初期値の削除	ウェブ UI ログイン時のパスワード初期値を削除
アクセス制御	連続パスワード失敗時に入力制限	ウェブ UI ログイン時に悪意あるユーザーからのパスワードランダム入力攻撃遮断
	出荷条件初期化状態で SUNAPI/ONVIF の無効化	ビデオ映像の流出防止
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流出と分析を防止
		ファームウェアの偽造・変造及び悪質なプログラムの挿入を防止
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	初期化する時にログ維持	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	デバイス及び相互認証(サーバー認証 /クライアント認証)	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
物理保護	セキュアブート(Secure Boot)	ファームウェアの偽造・変造防止

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. パスワード初期値の削除

製品の初期パスワードが存在する状態でユーザーがパスワードを変更せずに使用したり、メーカーの初期パスワード自体を変更したりできない場合、悪意あるユーザーに不正アクセスを許可する深刻なセキュリティ脆弱性をもたらす可能性があります。これにハンファテックウインのすべての製品は、初期パスワードを無くしUIに初回アクセスする時にパスワードを必ず変更してから使用するようし、ユーザーの誤りで発生するセキュリティの脆弱性を事前に防止しています。

3.3. 連続パスワード失敗時に入力制限

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。

3.4. 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。ハンファテックウィ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。

3.5. 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。

- 環境設定情報中の以下の項目は除外
 - : ネットワークメニューのIP&Port、DDNS、IP filtering、HTTPS、802.1x、QoS、SNMP、Auto IP configureのような設定情報は除外

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。

- 設定(IPカメラ)
 - : システム → アップグレード/再起動 → 設定バックアップ&リストア



3.6. 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。

3.7. 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/VMS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、ファイルの偽造・変造を予防しています。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。

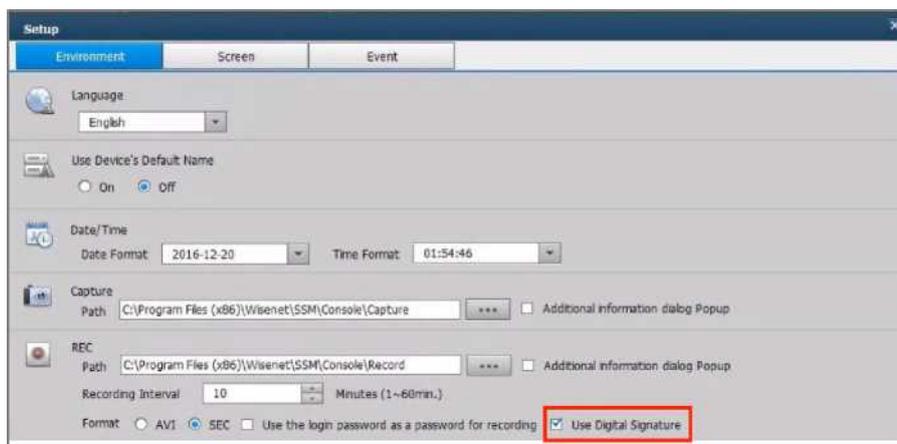
ビデオファイルを法的証拠または個人情報保護の目的で抽出する場合、SECファイルフォーマットに選択した後にパスワードを設定して抽出することができます。こうやって抽出されたSECファイルには、ウォーターマーク及び暗号化が適用されて当該ビデオの変造有無の確認及び機密性を保障することができ、VMS(SSM)からSECファイルに抽出された場合、電子署名機能が追加サポートされ当該ビデオがハンファテックウィンのSSMから抽出されたという技術的な確認ができます。

<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
カメラ	ウェブビューアー	AVI	X	X	汎用メディアプレイヤー
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 蔵)
	ウェブビューアー	SEC ¹	O	X	バックアップビューアー (SEC に 内 蔵)
		AVI	X	X	汎用メディアプレイヤー
VMS (SSM)	-	SEC	O	O	バックアップビューアー (SEC に 内 蔵)
		AVI	X	X	汎用メディアプレイヤー

● 設定(SSMコンソール設定)

: 環境設定 → 録画 → フォーマット



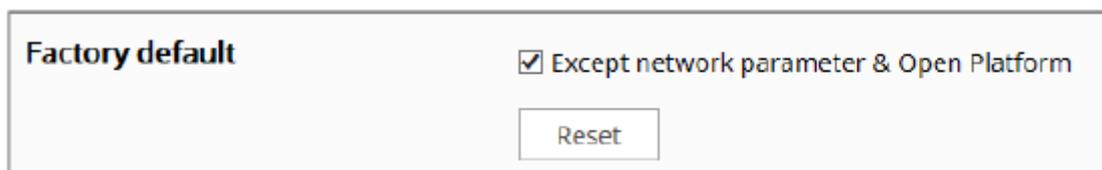
¹NVR ウェブビューアー-SEC ファイル抽出時、NonPlug-in ウェブビューアーでは未対応

3.8. 初期化する時にログ維持

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(IPカメラ)

: システム → アップグレード/再起動 → 出荷条件初期化



3.9. HTML5 ベースの NonPlug-in ウェブビューアー

ユーザーはカメラ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、シルバーライト、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Plugin-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。

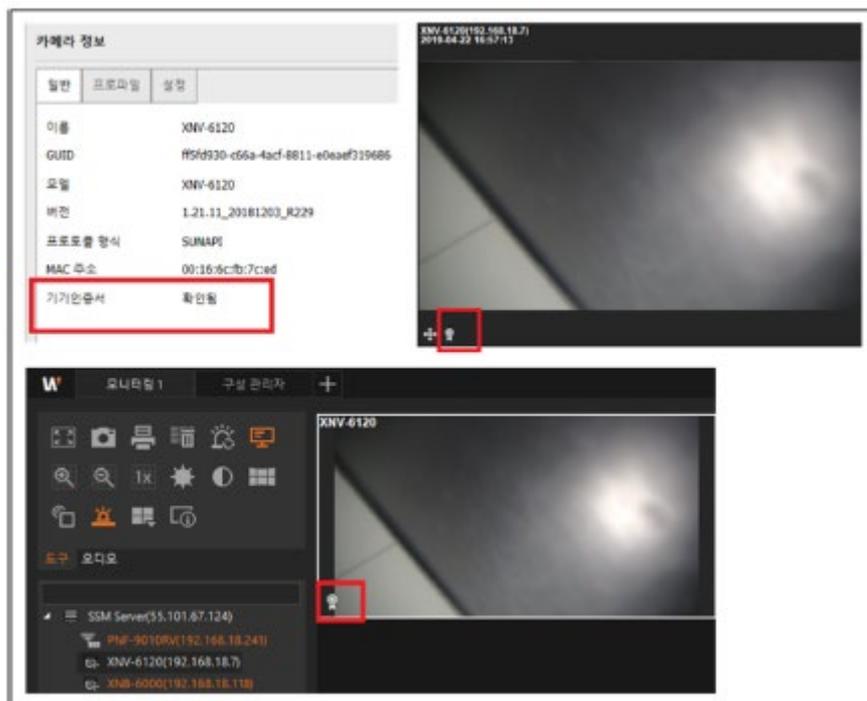
3.10. 個別デバイス認証(デバイス/相互認証(サーバー認証/クライアント認証))

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。

デバイス証明書は、THALES HSMデバイスを使用して各デバイスに対する証明書/プライベートキーを作成して製造過程で各デバイスに挿入します。作成された証明書はPrivate Root CAによってデジタル署名になるため、ハンファテックウィンで発行していることを証明できます。この証明書を使用する場合、ウェブブラウザでセキュリティ警告なく、セキュリティ通信を実行することができ、以下のようにデバイス/相互認証を実装する製品で確認することができます。

- デバイス認証(SSM)

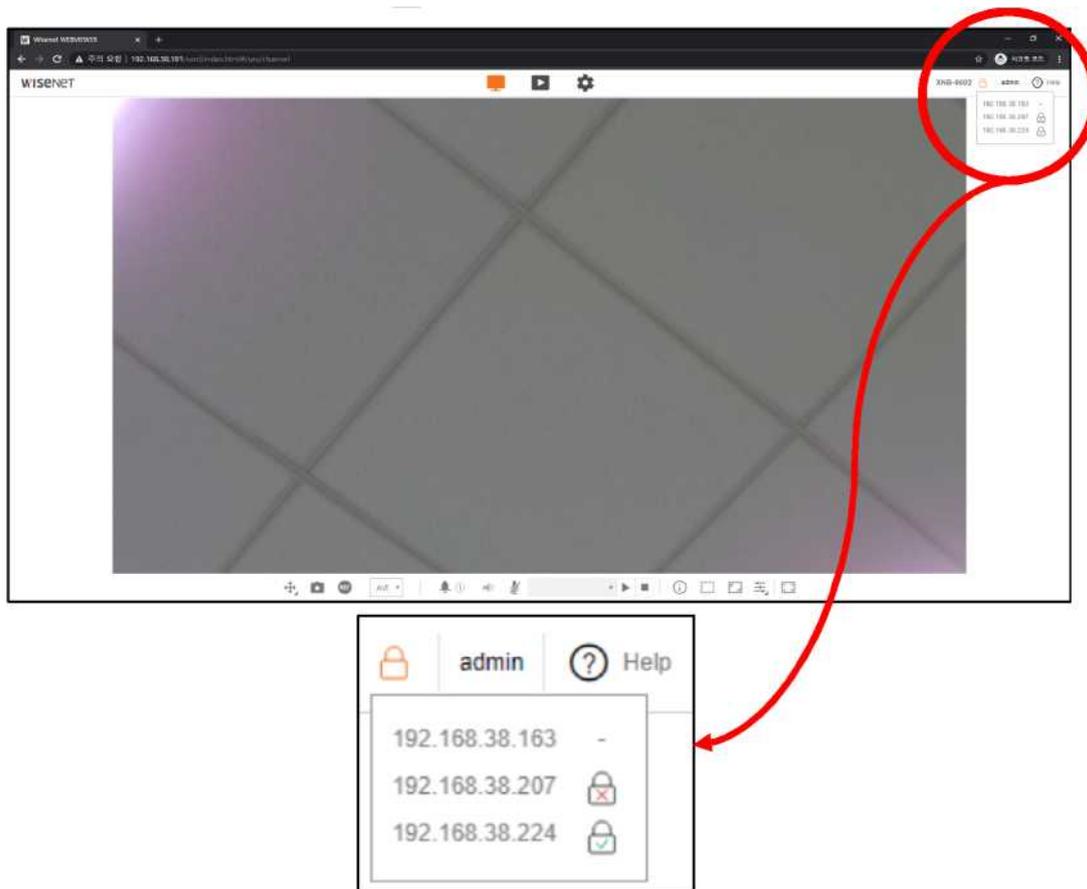
: 登録 → デバイス選択 → カメラ情報 → 一般 → デバイス証明書の「確認済み」情報確認



- 相互認証(カメラ) :

ライブ画面 → 相互認証アイコン選択 → 認証状態確認

- ① 該当ない : アイコンなしに - 表示
- ② 相互認証成功 : 成功アイコン🔒
- ③ 相互認証失敗 : 失敗アイコン🔓



ハンファテックウィンのPrivate Root CA証明書の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/cybersecurit/)
(<https://www.hanwha-security.com/ko/technical-guides/cybersecurit/>)

3.11. 出荷条件初期化状態で SUNAPI/ONVIF の無効化

ハンファテックウィンは、SUNAPI/ONVIFを通じたビデオ映像情報の流出を防止するためにパスワードが設定される前までSUNAPI/ONVIFのアクセスを制限しています。

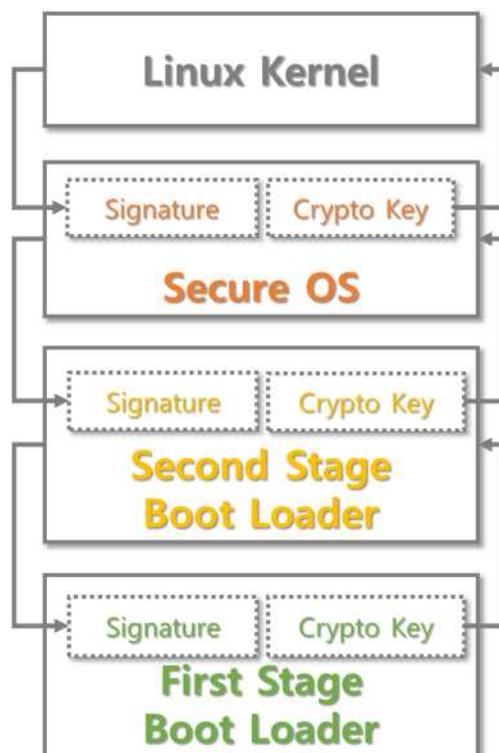
3.12. セキュアブート(Secure Boot)

ハンファテックウインは、独自開発したWN7チップが搭載されたデバイスを提供してセキュリティ強化に集中しています。WN7にはセキュアブート(Secure Boot)機能が内蔵されています。

セキュアブート(Secure Boot)とは、ロードされる各ブート画像の電子署名(Digital Signature)を検証して、偽造/変造されたブート画像が実行されることを防御するセキュリティ技術です。

既存にはファームウェア画像だけを一度暗号化したとしたら、WN7にはブート画像を段階別に検証して最初段階に検証通過してから次の段階のブート画像がロードされます。

検証方法は、ブート画像を作成する時に認証Signatureを積載して製品を起動する場合、当該Signatureを検証して検証結果に異常がない場合に起動します。



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	出荷条件初期化	デバイスに保存された既存情報を初期化
	ゲストログイン機能の無効化	許可されていないユーザーから映像保護
	認証されていない RTSP への接続許可の無効化	許可されていないユーザーから RTSP 映像保護
	マルチキャストの無効化	最初有効になるサービスを最小化して悪意のある攻撃防止
	DDNS の無効化	
	QoS の無効化	
	FTP の無効化	
	SNMP の無効化	
	Link-Local IPv4 アドレスの無効化	
	UPnP 検索の無効化	
	Bonjour の無効化	
音声入力の無効化		
パスワード	安全な通信プロトコルを使用する(HTTPS)	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
	最新バージョンの TLS 使用	セキュリティに安全な最新バージョン使用
	安全な Cipher Suites 使用	セキュリティに安全な暗号アルゴリズム使用

4.1. 出荷条件初期化

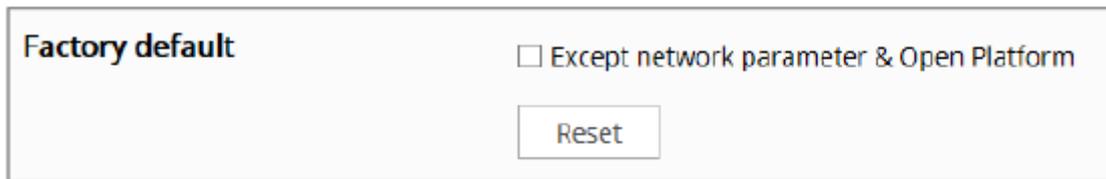
セキュリティを設定するデバイスをユーザーが購入した初期状態ではない使用した状態の場合、デバイスの出荷条件初期化を実行してデバイスの設定を初期化することが必要です。こうして実行した初期状態だけでもハンファテックウィンのデバイスは、保護レベルのセキュリティレベルを達成することができます。

1) システム → アップグレード/再起動 → 出荷条件初期化に移動

2) ネットワーク設定 & Open SDK 除去設定の選択解除

(当該設定を選択解除しない場合、ネットワーク設定や既にインストール済みの Open SDK が除外された状態に初期化されます。)

3) 初期化ボタンをクリック



4.2. ゲストログイン機能の無効化

ハンファテックウィンのカメラでは、ユーザー名やパスワードが「guest」のゲストログイン機能を提供しています。このゲストアカウントは最小限の権限だけを許可するため、非常に制限的ですが、ゲストログイン機能が有効化になっている場合許可されていないユーザーに映像ストリームが表示されることがあるため、当該機能が不要な場合、必ずゲストログイン機能を無効化することが必要です。

• 設定(IPカメラ)

: 基本 → ユーザー → ゲスト設定



4.3. 認証されていない RTSP への接続許可の無効化

この機能は、RTSP映像ストリームを認証なく公開する目的で提供することには役立ちますが、許可されていないユーザーからRTSP映像ストリームを保護する場合には必ず認証のないRTSP接続許可機能を無効化することが必要です。

- 1) 基本 → ユーザー → 認証設定
- 2) 認証されていない RTSP への接続許可の選択解除

Authentication setup <input type="checkbox"/> Allow RTSP connection without authentication

4.4. 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あり、RTSPプロトコルに対して設定できます。当該サービスが不要な場合、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。

- 1) 基本 → ビデオ profile → マルチキャスト
- 2) マルチキャスト(RTSP)の使用する設定の解除
- 3) 適用ボタンをクリック

Multicast	Multicast (RTSP)	<input type="checkbox"/> Enable
	IP address	<input type="text"/>
	Port	<input type="text" value="0"/>
	TTL	<input type="text" value="5"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

4.5. DDNS の無効化

カメラが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ませんが、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。

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

DDNS

Off
 Wisenet DDNS

Server
Product ID
 Quick connect

Public DDNS

Server
Host name
User name
Password

4.6. QoS の無効化

QoS機能は特定IPに対して映像伝送品質を保障するために優先順位を設定する機能です。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選択解除します。

- 1) ネットワーク → QoS
- 2) QoS に設定されている IP リストを選択した後に削除
- 3) 適用ボタンをクリック

4.7. FTP の無効化

FTP機能は、アラームやイベントが発生する場合、カメラによって撮影された画像を設定したFTPサーバーを通じて伝送するための機能です。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選択解除します。

- 1) イベント → FTP/E-mail → FTP 設定
- 2) 設定されたサーバーアドレス、ID、パスワード情報を削除
- 3) 適用ボタンをクリック

4.8. 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の機能を同時に対応します。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。

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

SNMP		
SNMP v1/v2c	SNMP v1	<input type="checkbox"/> Enable
	SNMP v2c	<input type="checkbox"/> Enable
	Read community	public
	Write community	write
<hr/>		
SNMP v3	Only operates when the SSL/TLS is authenticated.	
	SNMP v3	<input type="checkbox"/> Enable
	Password	

4.9. Link-Local IPv4 アドレスの無効化

リンクローカルIPv4アドレスの自動構成機能は、DHCPサーバーのようにIPを割り当てられないリンクローカルネットワーク(同じスイッチに接続されたカメラとホストのように一つのリンクに接続されているネットワーク)からカメラに169.254.xxx.xxx等のIPを割り当てる機能です。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選択解除します。

- 1) ネットワーク → 自動 IP 設定 → リンクローカル IPv4 アドレス
- 2) 自動設定の選択解除
- 3) 適用ボタンをクリック

Link-Local IPv4 address	Auto configure	<input type="checkbox"/> Enable
	IP address	169.254.7.150
	Subnet mask	255.255.0.0

4.10. UPnP 検索の無効化

UPnP発見機能は、UPnPプロトコルに対応するクライアントとOSで自動にカメラを検索するようにサポートする機能です。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選択解除します。

- 1) ネットワーク → 自動 IP 設定 → UPnP discovery
- 2) UPnP discovery 設定の選択解除
- 3) 適用ボタンをクリック

UPnP discovery	UPnP discovery	<input type="checkbox"/> Enable
	Friendly name	WISENET-XNV-6080R-00166CF92370

4.11. Bonjour の無効化

Bonjour機能は、Bonjourプロトコルに対応するクライアントとOSで自動にカメラを検索するようにサポートする機能です。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選択解除します。

- 1) ネットワーク → 自動 IP 設定 → Bonjour
- 2) Bonjour 設定の選択解除
- 3) 適用ボタンをクリック

Bonjour	Bonjour	<input type="checkbox"/> Enable
	Friendly name	WISENET-XNV-6080R-00166CF92370

4.12. 最新バージョンの TLS 使用

TLSは、SSLプロトコルをベースに開発されたクライアントとサーバー間に安全で暗号化された通信チャンネルを設定することに使用されます。TLSは現在の1.0、1.1、1.2、1.3で4つのバージョンがありますが、TLS初期バージョンのTLS 1.0/1.1はPOODLE²及びBEAST³のような様々な攻撃に弱いです。

ハンファテックウインは、初期設定値としてTLS 1.2/1.3を提供し、必要時に特定TLSバージョンの追加オプションを提供しています。しかし、ユーザーが安全に製品を使用するためには、TLS 1.0/1.2選択を解除する必要があります。

4.13. 安全な Cipher Suites 使用

TLSハンドシェイクのCipher Suitesを通じてTLSで使用する証明書検証及び非対称キーの交換方式、対称キー暗号化及び運用方式、メッセージ認証に対する方式についてクライアントとサーバー間の最終協議を行い、構造は次の通りです。

² POODLE の脆弱性 : Padding Oracle On Downgraded Legacy Encryption の略字で、旧式の暗号化手法を悪用できるプロトコルのダウングレードの脆弱性

³ BEAST の脆弱性 : Browser Exploit Against SSL/TLS の略字で、エンドユーザーブラウザで HTTPS のクッキーを解読して効果のターゲットセッションをハイジャッキングできる脆弱性



ハンファテックウィンは、TLS 1.2/1.3基準のCipher Suitesを以下のように提供しています。

※ TLS 1.2 Cipher Suites

TLS RSA WITH NULL MD5	0x00,0x01	Compatible	NULL-MD5
TLS RSA WITH NULL SHA	0x00,0x02	Compatible	NULL-SHA
TLS RSA WITH AES 128 CBC SHA	0x00,0x2F	Compatible	AES128-SHA
TLS DHE DSS WITH AES 128 CBC SHA	0x00,0x32	Compatible	DHE-DSS-AES128-SHA
TLS DHE RSA WITH AES 128 CBC SHA	0x00,0x33	Compatible	DHE-RSA-AES128-SHA
TLS DH anon WITH AES 128 CBC SHA	0x00,0x34	Compatible	ADH-AES128-SHA
TLS RSA WITH AES 256 CBC SHA	0x00,0x35	Compatible	AES256-SHA
TLS DHE DSS WITH AES 256 CBC SHA	0x00,0x38	Compatible	DHE-DSS-AES256-SHA
TLS DHE RSA WITH AES 256 CBC SHA	0x00,0x39	Compatible	DHE-RSA-AES256-SHA
TLS DH anon WITH AES 256 CBC SHA	0x00,0x3A	Compatible	ADH-AES256-SHA
TLS RSA WITH NULL SHA256	0x00,0x3B	Compatible	NULL-SHA256
TLS RSA WITH AES 128 CBC SHA256	0x00,0x3C	Secure/Compatible	AES128-SHA256
TLS RSA WITH AES 256 CBC SHA256	0x00,0x3D	Secure/Compatible	AES256-SHA256
TLS DHE DSS WITH AES 128 CBC SHA256	0x00,0x40	Secure/Compatible	DHE-DSS-AES128-SHA256
TLS DHE RSA WITH AES 128 CBC SHA256	0x00,0x67	Secure/Compatible	DHE-RSA-AES128-SHA256
TLS DHE DSS WITH AES 256 CBC SHA256	0x00,0x6A	Secure/Compatible	DHE-DSS-AES256-SHA256
TLS DHE RSA WITH AES 256 CBC SHA256	0x00,0x6B	Secure/Compatible	DHE-RSA-AES256-SHA256
TLS DH anon WITH AES 128 CBC SHA256	0x00,0x6C	Secure/Compatible	ADH-AES128-SHA256
TLS DH anon WITH AES 256 CBC SHA256	0x00,0x6D	Secure/Compatible	ADH-AES256-SHA256
TLS RSA WITH AES 128 GCM SHA256	0x00, 0x9C	Secure/Compatible	AES128-GCM-SHA256
TLS RSA WITH AES 256 GCM SHA384	0x00, 0x9D	Secure/Compatible	AES256-GCM-SHA384
TLS DHE RSA WITH AES 256 GCM SHA384	0x00, 0x9F	Secure/Compatible	DHE-RSA-AES256-GCM-SHA384
TLS DHE DSS WITH CAMELLIA 128 CBC SHA256	0x00,0xBD	Compatible	DHE-DSS-CAMELLIA128-SHA256
TLS RSA WITH CAMELLIA 256 CBC SHA256	0x00,0xC0	Compatible	CAMELLIA256-SHA256
TLS DHE DSS WITH CAMELLIA 256 CBC SHA256	0x00,0xC3	Compatible	DHE-DSS-CAMELLIA256-SHA256
TLS DHE RSA WITH CAMELLIA 256 CBC SHA256	0x00,0xC4	Compatible	DHE-RSA-CAMELLIA256-SHA256
TLS ECDHE ECDSA WITH AES 128 CBC SHA	0XC0, 0x09	Secure/Compatible	ECDHE-ECDSA-AES128-SHA
TLS ECDHE ECDSA WITH AES 256 CBC SHA	0XC0, 0x0A	Secure/Compatible	ECDHE-ECDSA-AES256-SHA
TLS ECDHE RSA WITH AES 128 CBC SHA	0XC0, 0x13	Secure/Compatible	ECDHE-RSA-AES128-SHA
TLS ECDHE RSA WITH AES 256 CBC SHA	0XC0, 0x14	Secure/Compatible	ECDHE-RSA-AES256-SHA
TLS ECDHE ECDSA WITH AES 256 GCM SHA384	0XC0, 0x2C	Secure/Compatible	ECDHE-ECDSA-AES256-GCM-SHA384
TLS ECDHE ECDSA WITH AES 128 CBC SHA256	0XC0, 0x23	Secure/Compatible	ECDHE-ECDSA-AES128-SHA256
TLS ECDHE ECDSA WITH AES 256 CBC SHA384	0XC0, 0x24	Secure/Compatible	ECDHE-ECDSA-AES256-SHA384
TLS ECDHE RSA WITH AES 128 CBC SHA256	0XC0, 0x27	Secure/Compatible	ECDHE-RSA-AES128-SHA256
TLS ECDHE RSA WITH AES 256 CBC SHA384	0XC0, 0x28	Secure/Compatible	ECDHE-RSA-AES256-SHA384
TLS ECDHE ECDSA WITH AES 128 GCM SHA256	0XC0, 0x2B	Secure/Compatible	ECDHE-ECDSA-AES128-GCM-SHA256
TLS ECDHE ECDSA WITH AES 256 GCM SHA384	0XC0, 0x2C	Secure/Compatible	ECDHE-ECDSA-AES256-GCM-SHA384
TLS ECDHE RSA WITH AES 128 GCM SHA256	0XC0, 0x2F	Secure/Compatible	ECDHE-RSA-AES128-GCM-SHA256
TLS ECDHE RSA WITH AES 256 GCM SHA384	0XC0, 0x30	Secure/Compatible	ECDHE-RSA-AES256-GCM-SHA384
TLS DHE RSA WITH AES 256 CCM 8	0XC0, 0xA3	Secure/Compatible	DHE-RSA-AES256-CCM8
TLS ECDHE RSA WITH CHACHA20 POLY1305 SHA256	0XCC, 0xA8	Secure/Compatible	ECDHE-RSA-CHACHA20-POLY1305
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0XCC, 0xA9	Secure/Compatible	ECDHE-ECDSA-CHACHA20-POLY1305

※ TLS 1.2 Cipher Suites

TLS AES 128 GCM SHA256	0x13,0x01	TLS AES 128 GCM SHA256
TLS AES 256 GCM SHA384	0x13,0x02	TLS AES 256 GCM SHA384
TLS CHACHA20 POLY1305 SHA256	0x13,0x03	TLS CHACHA20 POLY1305 SHA256
TLS_AES_128_CCM_SHA256	0x13,0x04	TLS_AES_128_CCM_SHA256
TLS_AES_128_CCM_8_SHA256	0x13,0x05	TLS_AES_128_CCM_8_SHA256

4.14. 音声入力の無効化

音声入力機能は、映像に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選択解除します。音声入力機能は、ビデオプロファイル毎に個別設定できるため、すでに設定されているビデオプロファイルを選択して解除する必要があります。

- 1) ビデオ profile メニュー移動
- 2) 設定された各ビデオ profile を選択した後、音声入力の選択解除
- 3) 適用ボタンクリック

The screenshot shows the 'Video profile' configuration page. At the top, there are 'Add' and 'Delete' buttons. Below them is a table with columns for Name, Codec, and Type. The table contains four rows: MJPEG (Record / Event), H.264 (Default), H.265, and MOBILE (H.264). The H.264 row is selected. Below the table, there are configuration fields for Name (H.264), Codec (H.264), Profile type (Default profile checked), and Audio in (checkbox, highlighted with a red box). Other fields include ATC mode (Disable), Sensitivity (Very high), and Limit (50 % (10 ~ 50)).

	Name	Codec	Type
<input type="radio"/>	MJPEG	MJPEG	Record / Event
<input checked="" type="radio"/>	H.264	H.264	Default
<input type="radio"/>	H.265	H.265	
<input type="radio"/>	MOBILE	H.264	

Name:

Codec:

Profile type: Default profile
 Record profile
 Digital PTZ profile
 Frame Lock profile

Audio in: Enable

ATC mode:

Sensitivity:

Limit: % (10 ~ 50)

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 (RTSP)	RTSPを通じて伝送される映像保護
-	HTTPS(自体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
-	TLSを用いたE-mail送信	TLSを用いた安全なE-mail送信
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
-	追加ユーザーアカウントの作成	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
監査	ログを点検する	悪意あるユーザーのアクセス記録分析
保存データ保護	保存データの暗号化(LUKS暗号化)	保存データの保護
バックアップデータの保護	バックアップデータの暗号化 (ZIPファイル暗号化)	バックアップデータの保護

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

ハンファテックウィンのホームページ(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XNO-8080Rモデルを使用する場合、現在配布された最新ファームウェアバージョンが1.40.00であり、Infoボタンをクリックすると19年7月3日に配布されたバージョンあることを確認できます。その他にSUNAPI、ONVIF、UWA、ISP、Open platform関連のバージョン情報を確認できます。Software Upgradeのためには、ハンファテックウィ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
- 1) システム → アップグレード/再起動 → 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



Version information	
Build number	1.40.00_20190703_R425
SUNAPI	2.5.6
ONVIF	18.6
UWA	2.6.0_190702
ISP	1.50_190618
Open platform	3.51_190403

Close

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、ユーザーは三つの方法から一つの方法を選択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。

- 1) 基本 → 日付&時間に移動
- 2) グリニッジ標準時(GMT)基準の現在居住地のタイムゾーンを設定
(SUMMER TIME 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) タイムゾーンの適用ボタンをクリック
- 4) 次の三つの方法から一つの方法を選択してシステムに適用される時間を設定
 手動：手動でデバイスの現在時間を設定
 PC ウェブビューアと同期化：現在ウェブビューアを実行中の PC の時間に設定
 NTP サーバーと同期化：入力されたサーバーアドレスの時間と同期化
- 5) システム時間設定の適用ボタンをクリック

The screenshot displays the system time configuration interface. It is divided into two main sections: 'Current system time' and 'System time setup'.

Current system time: Shows the current date and time as 2000-01-01 00:58:47.

Time zone: A dropdown menu is set to '(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'. Below it, there is a checkbox for 'Daylight saving time' which is checked. The 'Start time' is set to 'March.last.Sun/01:00:00' and the 'End time' is set to 'October.last.Sun/02:00:00'. There are 'Apply' and 'Cancel' buttons.

System time setup: This section has three radio buttons: 'Manual' (selected), 'Synchronize with PC viewer', and 'Synchronize with NTP server'.

- Manual:** The time is set to Y-M-D 2000-1-1 and h:m:s 0:58:27.
- Synchronize with PC viewer:** A checkbox is unchecked. Below it, the PC viewer time is shown as 2018-01-15 15:09:47.
- Synchronize with NTP server:** Five radio buttons are listed with their respective addresses:
 - Address 1: pool.ntp.org
 - Address 2: asia.pool.ntp.org
 - Address 3: europe.pool.ntp.org
 - Address 4: north-america.pool.ntp.org
 - Address 5: time.nist.gov

At the bottom of the 'System time setup' section, there are 'Apply' and 'Cancel' buttons.

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IPカメラ及びNVRデバイス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。ただし、HTTPS設定モードはウェブビューアー上で設定されたモードであるため、ウェブビューアー上で送受信される映像データ、ユーザーパスワード及びIDは保護できます。また、ユーザーがHTTPモードに変更する場合、Digest認証方式を適用しているため、ユーザーパスワードを保護できます。

<表 6>

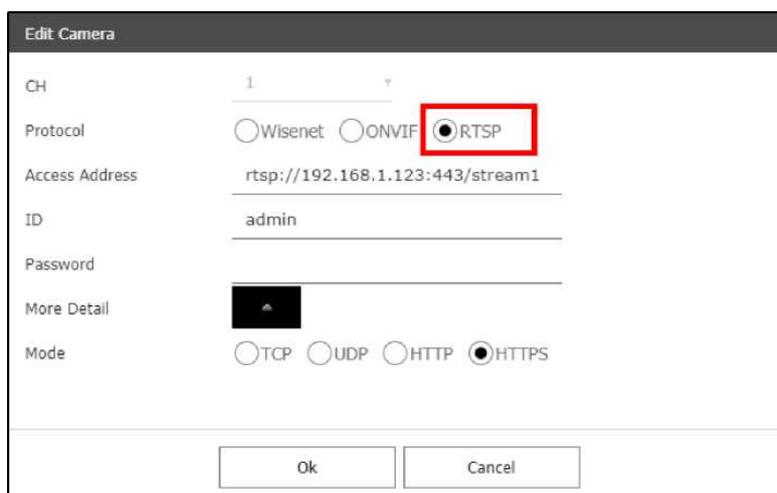
通信接続モード	ユーザーパスワード保護	映像データ保護	使用の有無
HTTP(Digest認証)	O	X	HTTPSと同時対応
HTTPS	O	O*	使用(初期設定)

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ウェブビューアー)

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



5.5. HTTPS(自体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。

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

Secure connection system

HTTP (Do not use a secure connection)

HTTPS (Secure connection mode using a unique certificate)

Change host name

Mutual authentication

HTTPS (Secure connection mode using the public certificate)

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。

- 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。

Install a public certificate	
Name for the certificate	<input type="text"/>
Certificate file	<input type="text"/> ...
Key file	<input type="text"/> ...
<input type="button" value="Install"/> <input type="button" value="Delete"/>	

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。普通に提供される基本ポート番号をより高いポート番号に変更します。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。

- 1) Basic → IP&ポート → 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 ポートとデバイスポートをそれぞれ 554 と 4520 から上位ポートに設定変更
- 4) 適用ボタンをクリック

IP address	Port								
Port	<table border="1"> <tr> <td>HTTP</td> <td><input type="text" value="80"/></td> </tr> <tr> <td>HTTPS</td> <td><input type="text" value="443"/></td> </tr> <tr> <td>RTSP</td> <td><input type="text" value="554"/></td> </tr> <tr> <td>Time out</td> <td><input checked="" type="checkbox"/> Enable</td> </tr> </table>	HTTP	<input type="text" value="80"/>	HTTPS	<input type="text" value="443"/>	RTSP	<input type="text" value="554"/>	Time out	<input checked="" type="checkbox"/> Enable
HTTP	<input type="text" value="80"/>								
HTTPS	<input type="text" value="443"/>								
RTSP	<input type="text" value="554"/>								
Time out	<input checked="" type="checkbox"/> Enable								
→									
Port	<table border="1"> <tr> <td>HTTP</td> <td><input type="text" value="8000"/></td> </tr> <tr> <td>HTTPS</td> <td><input type="text" value="4443"/></td> </tr> <tr> <td>RTSP</td> <td><input type="text" value="8554"/></td> </tr> <tr> <td>Time out</td> <td><input checked="" type="checkbox"/> Enable</td> </tr> </table>	HTTP	<input type="text" value="8000"/>	HTTPS	<input type="text" value="4443"/>	RTSP	<input type="text" value="8554"/>	Time out	<input checked="" type="checkbox"/> Enable
HTTP	<input type="text" value="8000"/>								
HTTPS	<input type="text" value="4443"/>								
RTSP	<input type="text" value="8554"/>								
Time out	<input checked="" type="checkbox"/> Enable								

※ ポートを再指定する時に接続されているストレージデバイスや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。

1) 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) 追加ボタンをクリックすると、IP リストウィンドウの作成

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

5) 設定完了後、適用ボタンクリック

※ 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. TLS を用いた E-mail 送信

カメラではアラームやイベントが発生する場合、撮影された画像をE-mailを通じて送信できる機能があります。この機能を使用する場合、TLSモードを使用するとカメラからメールサーバーまで安全なE-mail送信ができます。

- 1) イベント → FTP/E-mail → E-mail 設定
- 2) サーバーアドレスにアラーム及びイベント画像を伝送する E-mail サーバーの IP アドレス入力
- 3) 認証使用と TLS 使用を使用するに設定
- 4) E-mail サーバーにログインするためにアクセスするユーザーのアカウント ID とパスワード入力
- 5) TLS を使用しない E-mail サーバーポートの初期値は 25 であるが、TLS を使用する場合に当該ポートは 465 に設定される
- 6) 受信者に E-mail 受信者のアドレスを入力、発信者に E-mail 発信者のアドレスを入力
 - ※ 発信者アドレスが正確ではない場合、E-mail サーバーが当該発信者の E-mail を迷惑メールに分類して伝送されないことがあります。
- 7) E-mail 題名や E-mail 内容を入力した後、適用ボタンをクリック、E-mail 送信時にアラーム及びイベントの画像が添付ファイルに伝送される

E-mail configuration	
Server address	<input type="text"/>
Authentication	<input checked="" type="checkbox"/> Enable
TLS	<input type="checkbox"/> Enable
ID	<input type="text"/>
Password	<input type="password"/>
Port	<input type="text" value="25"/>
Recipient	<input type="text"/>
Sender	<input type="text"/>
Subject	<input type="text"/>
Message	<input type="text"/>

5.10. 安全に SNMP 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イ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 v3に使用する場合、HTTPS設定が前提条件であり、前節のHTTPS(自体認証保安接続モード)がすでに設定されている場合、次の過程の中で1)~3)は省略できます。

SNMP v1及びv2cは平文になっているコミュニティ文字列を通じてSNMP機能が提供され、セキュリティに弱いため使用しないでください。

- 1) ネットワーク → HTTPS → セキュリティアクセスタイプ
- 2) HTTPS(自体認証保安接続モード)を選択
- 3) 適用ボタンをクリック
- 4) ネットワーク → SNMP
- 5) SNMP v1 と SNMP v2c の使用選択解除
- 6) SNMP v3 の使用選択及びパスワード設定(HTTPS モード変更後、v3 選択可能)

SNMP

SNMP v1/v2c	SNMP v1	<input type="checkbox"/> Enable
	SNMP v2c	<input type="checkbox"/> Enable
	Read community	<input type="text" value="public"/>
	Write community	<input type="text" value="write"/>

SNMP v3	Only operates when the SSL/TLS is authenticated.	
	SNMP v3	<input type="checkbox"/> Enable
	Password	<input type="text"/>

SNMP traps	SNMP traps	<input type="checkbox"/> Enable
	Community	<input type="text"/>
	IP address	<input type="text"/>
	<input type="checkbox"/> Authentication failure notification	
	<input type="checkbox"/> Network connection notification	

5.11. 追加ユーザーアカウントの作成

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公開され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、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。

- 1) Basic → ユーザー → 現在のユーザー
- 2) 追加するアカウントを選択すると、設定できる項目が有効化する
- 3) 「使用する」を選択した後に名前、パスワード設定
- 4) 音声入力、音声出力、アラーム出力の使用有無を選択します。
- 5) プロファイルを選択した後、適用ボタンクリック(全体に設定する時、すべてのプロファイルの映像利用可能)

Current users							
		<input type="button" value="Add"/>	<input type="button" value="Delete"/>				
	Use	Name	Password	Audio in	Audio out	Alarm output	Profile
<input checked="" type="radio"/>	<input type="checkbox"/>	user1		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default <input type="button" value="v"/>
<input type="radio"/>	<input type="checkbox"/>	user2		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default <input type="button" value="v"/>
<input type="radio"/>	<input type="checkbox"/>	user3		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default <input type="button" value="v"/>
<input type="radio"/>	<input type="checkbox"/>	user4		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default <input type="button" value="v"/>
<input type="radio"/>	<input type="checkbox"/>	user5		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default <input type="button" value="v"/>
<input type="radio"/>	<input type="checkbox"/>	user6		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default <input type="button" value="v"/>
<input type="radio"/>	<input type="checkbox"/>	user7		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default <input type="button" value="v"/>
<input type="radio"/>	<input type="checkbox"/>	user8		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default <input type="button" value="v"/>
<input type="radio"/>	<input type="checkbox"/>	user9		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default <input type="button" value="v"/>
<input type="radio"/>	<input type="checkbox"/>	user10		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default <input type="button" value="v"/>

5.12. ログを点検する

デバイスに悪意あるユーザーが悪意ある目的で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欠陥を含む)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。

例えば、パスワード入力が連続で失敗した場合、アカウントがロックになりますが、アクセスログ(Access Log)検索を通じて大量のログイン失敗またはアカウントロックのようなタイプの攻撃を確認できます。

- 設定(IPカメラ)

: システム → ログ → アクセスログ/システムログ/イベントログ

No.	Date & Time	Description	Information
1	2000-01-01 00:01:45	AdminLogout	RTSP admin log out: 192.168.1.225
2	2000-01-01 00:01:19	AdminLogin	RTSP admin log in: 192.168.1.225
3	2000-01-01 00:00:25	AdminLogout	RTSP admin log out: 192.168.1.225
4	2000-01-01 00:00:19	AdminLogin	RTSP admin log in: 192.168.1.225
5	2000-01-01 00:06:51	AdminLogout	RTSP admin log out: 192.168.1.123
6	2000-01-01 00:06:47	AdminLogin	RTSP admin log in: 192.168.1.123
7	2000-01-01 00:01:42	AdminLogout	RTSP admin log out: 192.168.1.123
8	2000-01-01 00:01:38	AdminLogin	RTSP admin log in: 192.168.1.123
9	2000-01-01 00:42:47	AdminLogout	RTSP admin log out: 192.168.1.123
10	2000-01-01 00:41:14	AdminLogin	RTSP admin log in: 192.168.1.123
11	2000-01-01 00:40:30	AdminLogout	RTSP admin log out: 192.168.1.123
12	2000-01-01 00:40:26	AdminLogin	RTSP admin log in: 192.168.1.123
13	2000-01-01 00:40:24	AdminLogout	RTSP admin log out: 192.168.1.123
14	2000-01-01 00:40:21	AdminLogin	RTSP admin log in: 192.168.1.123
15	2000-01-01 00:39:54	AdminLogout	RTSP admin log out: 192.168.1.123

5.13. 保存データの暗号化(LUKS 暗号化)

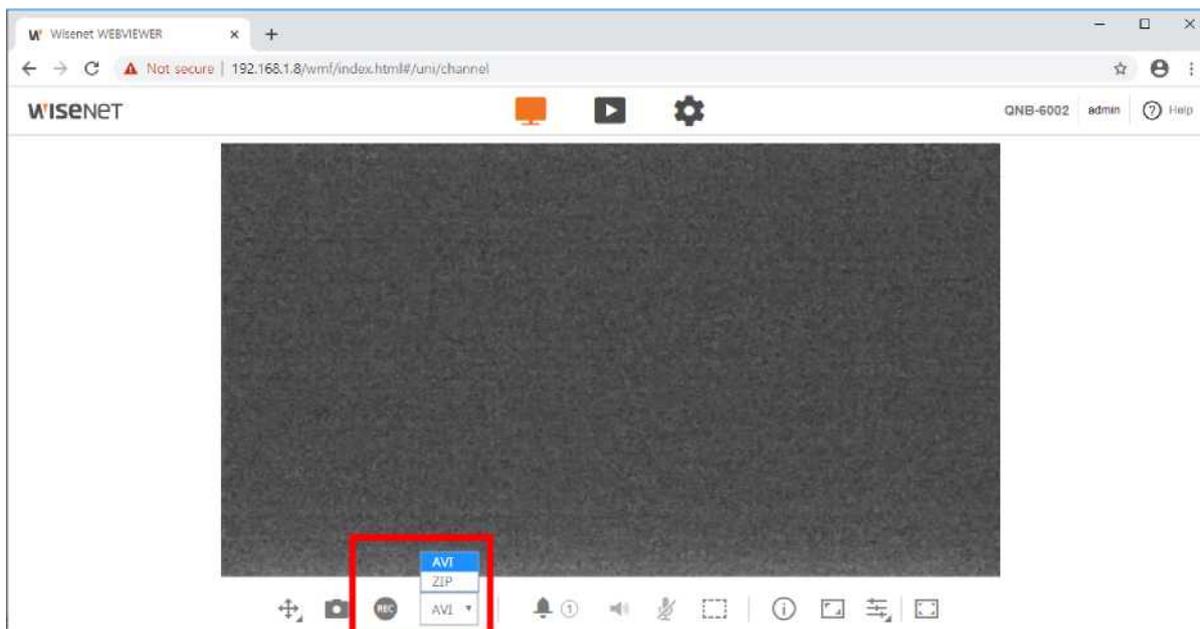
保存データの暗号化機能は、SDカードに保存されたデータが流出されても確認できないように暗号化する機能です。初期値は無効化されているため、SDカードにデータ保存時、当該設定を有効化して使用します。使用時、パスワードは必ず要求されます。SDカードの暗号化機能設定を変更する時にも設定したパスワードは必ず要求され、パスワード紛失時にはSDカードをフォーマットした後、新しく使用する必要があるため、パスワードの安全な管理が必要です。

SD File System	Type	VFAT
Encryption		
		Unencrypted
		<input type="checkbox"/> Enable
New password		<input type="password"/>
Confirm new password		<input type="password"/>
ⓘ A forgotten password cannot be recovered but only reset.		
<ul style="list-style-type: none"> • If the password is 8 to 9 characters long, then it must include a combination of at least 3 of the following character types: alphabet letters with uppercase or lowercase, numbers, and special characters. • If the password is longer than 10 characters, then it must include a combination of at least 2 of the following character types: alphabet letters with uppercase or lowercase, numbers, and special characters. • The following special characters can be used: ~!@#\$%^&*()_-=+ {}[]?/. • You may not use more than 4 consecutive characters. (example: 1234, abcd, etc.) • You may not use the same character 4 or more times consecutively. (example: !!!!, 1111, aaaa, etc.) 		

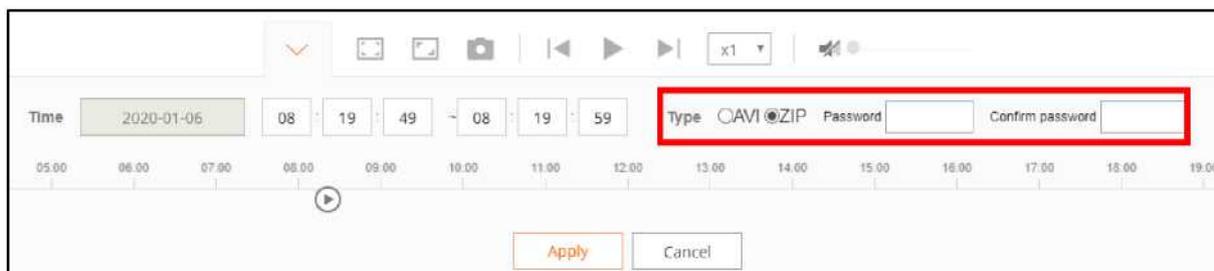
5.14. バックアップデータの暗号化(ZIP ファイル暗号化)

SDカードに保存されたデータを外部に抽出する時やライブ映像を録画する時、バックアップファイルはAVIまたはZIPファイルに設定できます。AVIに設定する場合、暗号化されていないため重要情報が流出することはありますが、ZIPファイルに設定すると暗号化できるため、流出を防ぐことができます。ZIPファイルを暗号化する時にパスワード入力が必要であり、パスワードを入力しない場合にはZIPファイル暗号化が適用されません。

- ライブ画面で映像録画時



- Playback画面で映像バックアップ時



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のカメラに対応する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。使用する場合、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。

- 1) ネットワーク → 802.1X → IEEE 802.1x
- 2) IEEE 802.1x「使用する」を選択
- 3) EAP タイプを EAP-TLS に設定、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) 適用ボタンをクリック

IEEE 802.1x setup	
IEEE 802.1x	<input type="checkbox"/> Enable
EAP type	EAP-TLS
EAPOL version	1
ID	<input type="text"/>
Password	<input type="password"/>
Certificates	
CA certificates	... Install Delete Not available
Client certificate	... Install Delete Not available
Client private Key	... Install Delete Not available
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

WISENET

Hanwha Techwin Co.,Ltd.

13488 京畿道城南市盆唐区板橋路 319 番ビル 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.

