Hanwha Techwin

White paper

Wisenet7
オリジナルのサイバーセキュリティ

2020 年 6 月 29 日

Contents

1. 背景及び序論

最近、高度なセキュリティが求められるエリアに設置された映像監視カメラにアクセス、リアルタイム映像及び録画映像を奪取または偽造・変造するハッカーに対する懸念が高まっています。カメラメーカーは、基本設定値や、連続する文字と数字を使用したパスワードを許可しないネットワーク設定プロトコルを導入するなどのハッキング脅威に対応しています。そうであるにもかかわらずハッカーは、カメラの「バックドア」をはじめとする様々な方式でデータアクセス方法を模索しています。

犯罪及び悪意のある目的か、アマチュアハッカーの実力誇示を目的としたハッキングかどうかに関係なく、ユーザーの重要なデータを安全に保護することは重要です。映像監視ソリューションに資産、人材の保護に依存する数千社の小型業者だけでなく、強度の高いセキュリティが必須である空港、銀行、地方自治団体、政府、軍事、応急医療サービスなども同じです。

ハンファテックウィンは、このような環境で利用される製品のセキュリティ強化のために努力し続けています。2020年には、豊富なセキュリティ機能及び技術を集約したハンファテックウィンの独自開発SoC(System on Chip)であるWisenet7を搭載した製品を公開しました。Wisenet7には三つの特徴があります。

一つ目は、新たに適用したハードウェアセキュリティ機能により、ソフトウェアセキュリティの限界を克服しました。セキュリティストレージ(Secure Storage)は、安全なデータストレージを提供し、これをベースにセキュアブート、セキュリティOS、セキュリティJTAGなどのハードウェアセキュリティ機能を拡張しました。

二つ目は、End-to-end保護の究極的な目的は通信内容を盗み聞きしたり、重要な資料を偽造・変造するためにデバイスにアクセスしたりして重要な情報を取得、偽造・変造する不正者を遮断ことです。このためにデバイス相互間の識別、認証が必要であり、認証に基づくアクセス統制及び許可、暗号化ロジックを使用したシステム及びデータ保護が求められており、Wisenet7ではそれを実現しました。

三つ目は、製品のデザイン機能及び設定オプションを決定する段階からセキュリティを最重要項目と定めております。強度の高いセキュリティ機能を実装するために製品の性能や下位互換性が低下する可能性がありますが、セキュリティの重要性、また業界のトレンドを考慮しセキュリティ向上に主眼を置いて開発を進めて参りました。

上記で言及した新規機能及び技術の一部は、サイバー攻撃の遮断のために開発されましたが、一部はチップセットの効率性増大のために開発され製品のセキュリティを強化したケースもあります。

本ホワイトペーパーはユーザーがWisenet7を搭載した製品に集約されたハンファテックウィンのワンランク高いサイバーセキュリティ技術説明のために作成されました。

2.1. ハードウェアセキュリティ

ハードウェアベースのセキュリティ技術はソフトウェアベースの技術より、セキュリティの脆弱性をより保護するためのセキュリティ強化においてとても重要です。セキュリティハードウェアから派生したセキュリティソフトウェア(信頼点：root of trust)は偽造・変造がさらに困難です。ハンファテックウィンはWisenet7製品を筆頭に、次の4種類のハードウェアベースのセキュリティ技術を製品に適用します。

2.1.1.セキュアブート(Secure boot)

Wisenet7からセキュアブートに対応します。

セキュアブートはカメラ起動時、カメラに動作するソフトウェアの整合性を検証するメカニズムであり、外部の悪質なコードあるいは悪質なソフトウェアによるソフトウェアの偽造・変造を検査します。

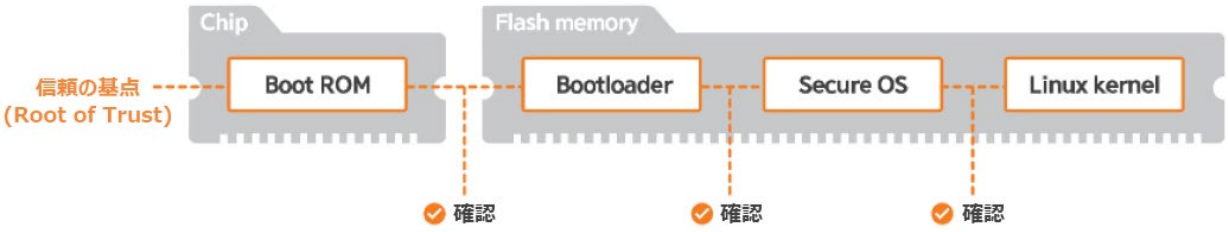

図 1. Wisenet7 製品のセキュアブート

2.1.2.セキュリティストレージ(Secure Storage)

Wisenet7には、安全なハードウェアモジュールであるハンファテックウィンのセキュリティプラットフォームモジュール(HTPM: Hanwha Trusted Platform Module)が内蔵されています。HTPMは暗号処理機(安全な運用のためのマイクロコントローラー)、乱数発生器、セキュリティ保存、セキュリティOSなどで構成されます。

HTPMのセキュリティストレージは、OTPROM (One Time Programmable Read-Only Memory)とEEPROM (Electrically Erasable Programmable Read-Only Memory：電気の供給が切れた状態でも長期間記憶する非揮発性記憶デバイス)で構成され、カメラの重要情報を保存します。信頼性を構築する情報は製造段階でOTPROMに適用され、重要な運用情報はEEPROMで安全に保存されます。

2.1.3.セキュリティ OS(Secure OS)

別途のセキュリティOSは、セキュリティストレージに保存された重要な情報を安全に処理するために必要です。

カメラ外部からはセキュリティOSにアクセスできません。セキュリティOSやセキュリティストレージにアクセスするためには、Linux OSを通じて別途のAPIを使用する必要があります。また、セキュリティOSは独立した暗号化、復号化をサポートし、メインOSの負荷を減らしセキュリティOSに使用されたアプリケーションは偽造・変造を防ぐために検証されます。

2.1.4.セキュリティ JTAG

JTAGインターフェースを通じた不正アクセスを予防する最も良い方法は、JTAG機能を解除することです。しかし、これは製品開発もしくは生産段階でチップやボードに発生する障害の原因を把握する手段も除去されることを意味します。

したがって、秘密鍵に基づく認証メカニズムをWisenet7に適用して、JTAGを安全に使用しながらも強度の高いセキュリティを実現することができます。

認証キーはメーカーのみが所有しており、メーカーが所有した認証キーは顧客情報ではない製品のシステムに関する情報にだけアクセスを許可します。また、製品に障害が発生する場合、メーカーは当該認証キーを活用してリモートではなくローカルでのみ原因分析を実行できるため、不正ユーザーのアクセスができません。

2.2. End-to-End 保護

パスワードを通じた既存のアクセス統制以外にも、デバイスの相互認証のために適用したデバイス証明書を活用して通信の安全性を高めます。このような方式は不正ユーザーの通信妨害を防ぐことができます。また、デジタル署名、暗号化を導入してデータ保存及びバックアップする時、End-to-Endデータセキュリティを強化し、ファームウェアアップデート及び起動時にもEnd-to-Endのシステムセキュリティを向上できます。

2.2.1.デバイス証明書(事前インストール)

ハンファテックウィンは、タレス(Thales) HSMデバイスを使用して各デバイス(Wisenet7製品を含む)の証明書/プライベートキーを発行して製造過程で各デバイスに適用します。証明書の発行者(Root CA)でデジタル署名をするため、メーカーの発行事実を証明できます。証明書があるとウェブブラウザでセキュリティ警告なく安全な通信ができ、証明書はデバイス認証を行う製品で確認できます。

2.2.2.相互認証(Mutual Authentication)

安全な通信のための相互認証は、通信セキュリティの機密性、整合性、認証性を確保する良い方法です。ハンファテックウィンのWisenet7製品はHTTPS(TLSベースのHTTP、HTTPSベースのRTSP)通信を使用するカメラ及びクライアントデバイス(ストレージデバイスもしくはPC NVRタイプSSM)間の相互認証のためにクライアント認証に対応します。

一般的に相互認証は、ユーザーやデバイスで実行できますが、現在はハンファテックウィンから生産したデバイス間にのみ実行できます。

相互認証でサーバー役割を果たすカメラの認証はサーバー認証と呼ばれ、クライアントの役割を果たすデバイスの認証は、クライアント認証と呼びます。サーバー認証はクライアントで実行され、クライアント認証はサーバーで実行されます。

クライアント認証はサーバー認証を前提としたオプションで提供されるため、包括的意味でクライアントを認証することにより、相互認証を提供します。

2.2.3.セキュリティチェーン(Chain of Trust)検証

最上位証明書の発行者(Root CA)が発行した証明書は、カメラの信頼点を保障するために存在し、証明書チェーンは最上位証明書の発行者(Root CA)が発行した証明書で検証します。Wisenet7製品には、二種類の最上位証明書の発行者(Root CA)が発行した証明書があります。一つはデバイス認証のための最上位証明書の発行者(Root CA)が発行した証明書であり、もう一つはオープンプラットフォームのアプリケーション用途の証明書です。

デバイス認証のための最上位証明書の発行者(Root CA)が発行した証明書はカメラにデバイス証明書をインストールしたり、クライアントのデバイス証明書を活用してクライアント認証を行ったりする場合に使用します。一つ目の用途はデバイス証明書をカメラにインストールする時に証明書チェーンを検証してメーカーの承認がない証明書のインストールを防ぐための目的があります。二つ目の用途はクライアントデバイスの証明書チェーンを検証してハンファテックウィンから製造した信頼できるデバイスであることを裏付ける目的があります。

オープンプラットフォームアプリケーション用の最上位証明書の発行者(Root CA)が発行した証明書は、Wisenet7のオープンプラットフォームアプリケーション署名に使用されたそれぞれ異なる署名キーや証明書がハンファテックウィンから作成、配布されたことを検証して不正アプリケーションのインストールを防ぎます。

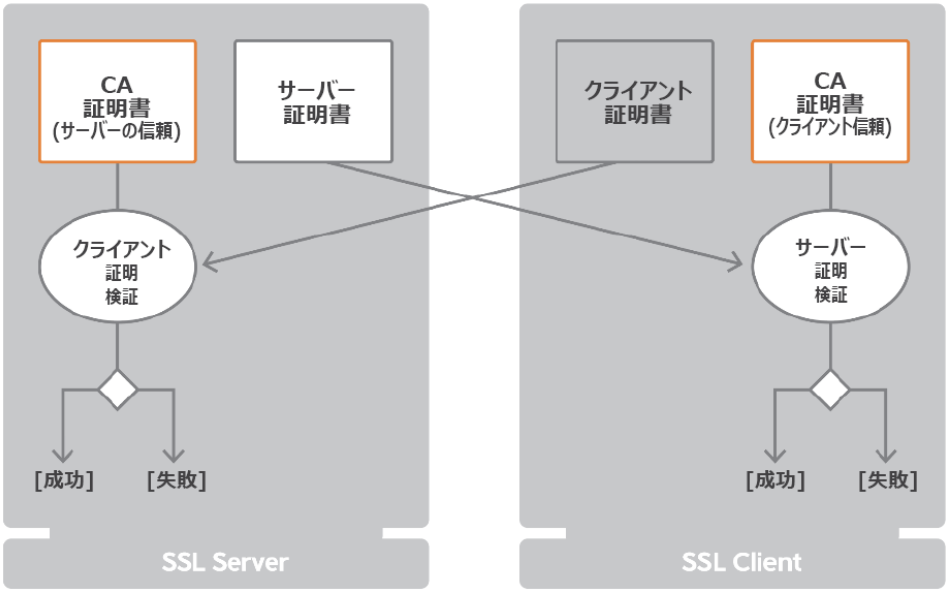

図 2. 信頼点の概念

2.2.4.ファームウェアの偽造・変造検証

ハンファテックウィンの署名された(Signed)ファームウェア技術は、安全なファームウェアアップデート方式です。ファームウェアにデジタル署名を含めてアップデート時に署名値を検証することでユーザーはファームウェアが偽造・変造されていないことを信頼することができます。

ファームウェアのデジタル署名はハンファテックウィンから安全に管理するキーサーバーを通じたプライベートキーで作成され、デジタル署名を検証するパブリックキーはWisenet7のセキュリティストレージ区域(HTPM)で安全に保存されます。

デジタル署名を使用すると、単純なハッシュ、チェックサムなどよりファームウェアの整合性を立証し、セキュリティを強化するのに効果があります。変造されたファームウェアのハッシュやチェックサムは、簡単に計算しなおすことができるからです。

2.2.5.映像の画像暗号化(待機及びバックアップ時)

カメラで作成された映像画像は、ユーザーの重要な情報として扱わなければなりません。そのため、映像画像の伝送時には安全な通信を使用するだけでなく、外部のストレージ媒体に画像を保存したり、カメラをPCにバックアップしたりする場合は、必ずセキュリティメカニズムが適用される必要があります。

Wisenet7製品は、映像画像をSDカードに保存すると、ファイルシステムの暗号化をサポートします。ファイルをそれぞれ別々に暗号化する代わりに、ファイルシステムを暗号化することで、映像を伝送及び再生する際には別途で暗号化解除の必要がありません。また、AES暗号化はユーザーが設定したパスワードセットを使って実行されるため、SDカードを盗まれたとしても保存された映像は安全に保護します。

Wisenet7製品はバックアップ時に映像の暗号化をサポートします。カメラに保存された映像をバックアップする場合やPCのリアルタイム映像をマニュアルで録画する場合、ZIPファイルを暗号化して映像を保護します。

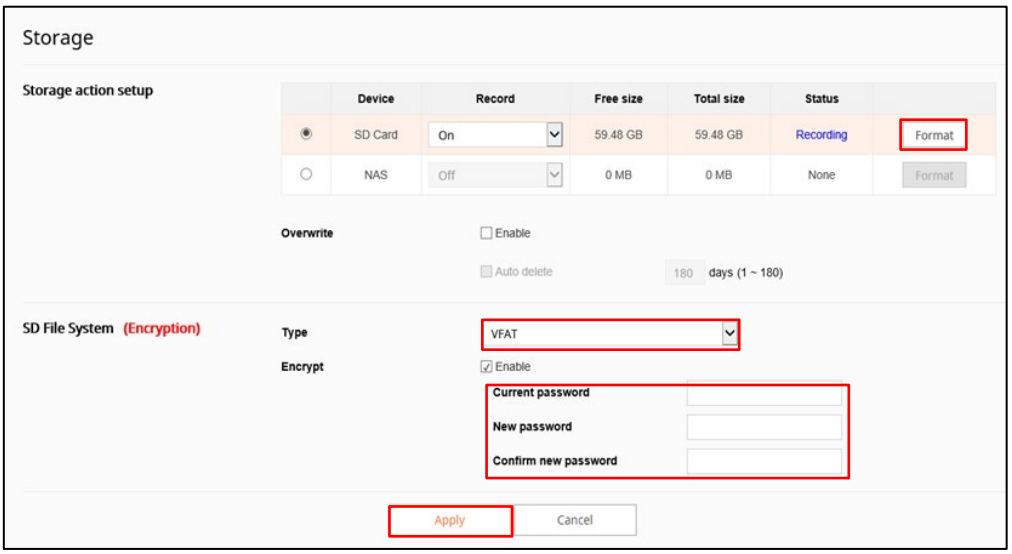

図 3. SD カードの暗号化 UI

2.3. Secure by Default/Design

メーカーは製品開発において、システムやユーザーの重要な情報の機密性、整合性、認証性を確保するためにセキュリティ標準を念頭に置く必要があります。製品の設計段階からセキュリティ標準を反映することが重要であり、これを「Secure by design(セキュリティに最適化された設計)」と呼びます。

「Secure by default(安全性を保障する基本設定)」は、基本設定が最高のセキュリティレベルになっていることを意味し、最もユーザーにフレンドリーまたは下位互換性を持つ設定ではない可能性があります。したがって、ユーザーが各Secure by Defaultの設定において、使用性及び互換性に適合した設定の変更によるセキュリティリスクを分析する必要があります。

2.3.1.セキュリティ設定の強化

Wisenet7製品はボックスから製品を取り出す瞬間から、高いセキュリティを提供するように設計されています。HTTPSモードが最初に適用されると、SNMP(Simple Network Management Protocol：簡易網管理プロトコル)、Link-Localアドレス、UPnP discovery、そしてBonjourなどの不要な初期サービスは無効化されます。SUNAPI/ONVIFも初期には無効化されていますが、ユーザーパスワードが設定されると有効化されます。すべてのハンファテックウィンの製品は、初期に設定された基本パスワード無しで出荷されます。

製品に初めてアクセスする際は、ユーザーはWisenet Device Managerを通じて複雑なパスワードを直接設定する必要があります。

2.3.2.最新バージョンのプロトコルを適用

Wisenet7製品は、ハンファテックウィン製品として初めてTLS 1.3バージョンを採用します。Wisenet7製品は安全なTLSバージョン(1.2、1.3)のみをサポートします。TLS1.2は、欠点があるにもかかわらずまだ安全であり、現在、最も多く採用されている標準です。特定のTLSバージョン(1.0、1.1)の追加オプションも、下位互換性などにより必要に応じてサポートされますが、セキュリティの面では推奨しません。

TLS 1.3バージョンで最も大きな変化は、より速くなった実行プロセスと強化されたセキュリティです。

3. セキュリティチェックリスト

カメラのサイバーセキュリティを一層強化するためには、複数段階のセキュリティデバイスを導入することを推奨します。これにより、一段階セキュリティが破られても、他のセキュリティデバイスが正常に動作し、セキュリティネットワーク及びデバイスを保護することができます。また、IT、映像セキュリティ、システムインストラクター、そしてエンドユーザーが協業し、システム全体のセキュリティ要求事項とセキュリティ機能についてそれぞれの責任と義務を明確にすることが望ましいです。以下に、セキュリティネットワークの設定において導入可能なサイバーセキュリティに関する機能リストです。

- 最小限の権限だけが付与されたユーザー段階のアカウント作成
- ゲストアカウントや認証なしでRTSP(Real-Time Streaming Protocol)アクセス可能な機能の無効化
- 定期的なパスワード変更&システム別に異なるパスワードを使用
- システムタイムゾーンのアップデート/NTP (Network Time Protocol)、DST (Daylight Saving Time)、タイムゾーン
- 802.1x証明書ベースのアクセスコントロールを有効化
- 必要な場合のみマルチキャスト(Multicast)を有効化
- 必要な場合のみDDNS (Dynamic Domain Name System)を有効化
- 必要な場合のみBonjourを有効化
- 必要な場合のみUPnP (Universal Plug and Play)を有効化
- 必要な場合のみlink-localアドレスを有効化
- 必要な場合のみFTP (File Transfer Protocol)を有効化
- 必要な場合のみSNMP (Simple Network Management Protocol) v3だけを使用
- E-mailを使用する場合、セキュリティが適用されたSMTP (Simple Mail Transfer Protocol)を使用
- 必要な場合のみQoSを有効化
- ネットワーク環境でVLANを有効化
- カメラを人の手の届かないところに設置、ケーブルの保護
- 基本ポートを広く使用されるポートから類推しにくいポートに変更
- IPフィルタリングを有効化

- 社内ネットワークとは別のネットワークにカメラを接続
- VMS (Video Monitoring System)またはネットワークに問題が発生した場合に備え、バックアップ目的のSDカード保存を有効化
- 文書の環境設定や文書のエクスポート/バックアップを作成
- カメラ画面のスナップショット保存
- タンパリング/初期化などの変化を簡単に把握できるよう設定
- リモートアクセス時、VPNもしくはセキュリティ済みのクラウド活用
- SDカードの保存及びビデオエクスポート機能を使用する場合、汎用ビデオファイルタイプではなくハンファテックウィン独自のビデオファイルタイプを使用
- 無停電電源装置（UPS）を活用したネットワークスイッチ、NVR/VMS、そしてPoEミッドスパン/インジェクター保護
- タンパリング、フォーカスずれ検知機能を有効化
- 低電力状況でのネットワーク切断検知機能を有効化
- デバイスに記録されたログを定期的に点検

4. 結論

Wisenet7は、セキュアブート/セキュリティOS/セキュリティストレージ、署名されたファームウェア/オープンプラットフォームアプリ、セキュリティJTAGなどを活用し、業界最高レベルのサイバーセキュリティポリシーをサポートし、End-to-Endサイバーセキュリティを提供します。ハンファテックウィンは、独自のデバイス認証発行システムを導入し、製品開発段階から製造段階に至るまで、証明書を製品に適用しています。Wisenet7の向上したサイバーセキュリティ機能により、ユーザーはより安全なセキュリティソリューションを構築することができるようになりました。

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