Hanwha Techwin

ユーザーガイド

サイバーセキュリティ

ネットワークデバイスのセキュリティ強化

2020 年 11 月 17 日

Contents

Contents

1. 序論

ネットワークを通じて他のシステムと情報を共有するデバイスやシステムが著しく増え、世の中は次第にコネクテッド時代に向かっています。このようなトレンドの裏には、いつでもどこでもネットワークに接続してデバイスとシステムを簡単に制御できることを望む人々の願いが込められています。

しかし、ネットワークデバイスの急増に伴い、前例のない手軽さを享受できるようになった反面、セキュリティリスクの増加という否定的な部分もあることは見逃せません。各デバイスがネットワークエンドポイントの役割を果たすため、ハッカーをはじめとする悪意に満ちたユーザーはこれを進入点として使用する可能性が常にあります。実際、最近注目を集めたデータ漏えい事例の多くを見ると、ハッカーはデータ流出を防止できる適切なレベルのセキュリティを備えていないPOS、*HVACまたはその他のネットワークシステムを通じて、企業ネットワークに侵入していました。

**HVAC* : 空調機*(Heating、Ventilation and Air Conditioning)*

IPベースの映像監視及びその他のソリューションが人気を集め、新規構築及びアップグレードのための標準として認められていますが、セキュリティシステムも例外ではありません。ハッカーはハッキングの対象となるネットワークデバイスの種類や、どのような機能をしているのか区別しません。弱点として悪用される可能性のある潜在的ネットワークへの参入点に言及する際に、映像監視カメラやその他のデバイスが欠かさず登場するのはそのためです。したがって、ユーザーはネットワーク、IPカメラ、エンコーダー、NVR及びDVRのセキュリティレベルを極大化できる措置を必ず取らなければなりません。デバイスのセキュリティを強化し、無断アクセスを遮断すると同時に、ユーザーの映像監視システム及び全体ネットワークを保護できるモデル事例は数多くあります。ハンファテックウィンは、このような模範事例を熟知しているだけでなく、ユーザーがネットワークセキュリティ強化のための重要な措置をより容易に行えるよう、様々な技術と機能を製品に搭載しております。セキュリティシステムの運営者、IT担当者、システムのインストールを担当するシステム統合企業は、このような技術と機能を検討し、利便性と許容可能な危険性のバランスを保たなければなりません。

本白書には、ネットワークカメラのスクリーンショットが含まれています。ほとんどの設定は、Wisenet Device Managerソフトウェアを使用することで、多数のカメラに一括適用することができます。

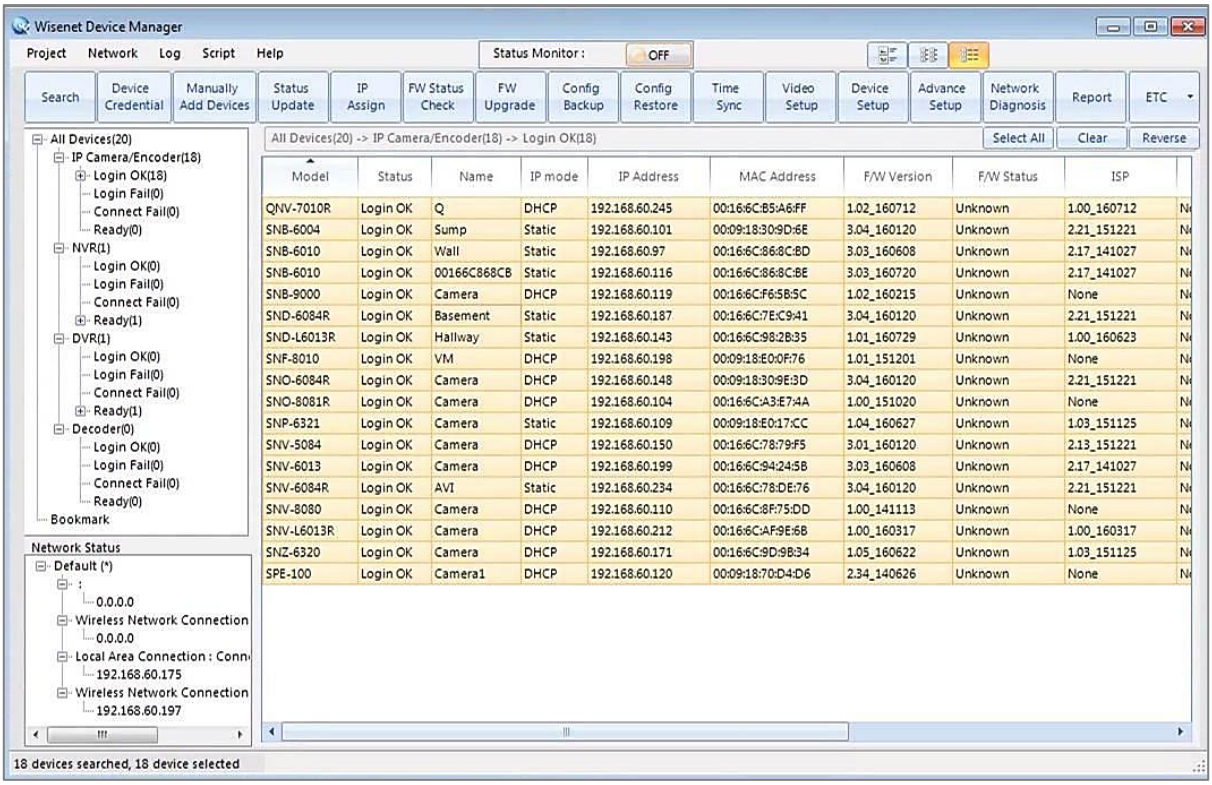

図 1. Wisenet Device Manager の使用画面

2. パスワード設定

スマートフォンのロック解除、PCログイン、メール確認に至るまで、パスワードは全ての日常に欠かせないものです。誰でも自分のデバイスやネットワークを保護できる強力なパスワードの重要性について十分認識していると思いますが、現実にはいつもそうではありません。ここで紹介する模範事例を基に、パスワードのセキュリティを最高レベルに維持するお手伝いをしていただければと思います。

カメラ、NVR、DVRなどのデバイスに初期パスワードがある場合、通常オンラインやユーザー説明書で簡単に検索することができるため、パスワードが変更されていないデバイスは、悪意を持った第三者の無断アクセスを許可することになります。ユーザーは必ず初期パスワードをそのまま使用せず、固有のパスワードを設定しなければなりません。このような弱点を事前に遮断するため、ハンファテックウィンのすべての製品は初期パスワードを提供せず、デバイスの初期使用時にはパスワードを必ず設定した後に使用するようになっています。しかし、単純にパスワードを変更するだけでは足りません。ユーザー認証を要求する機能やアプリケーションが増え、多くの人がパスワードに関する手軽さを理由に2つの失敗をしており、特にパスワードを作る時、この2つの失敗に該当する場合が頻繁に発生しているからです。

最初の失敗は、全ての登録先に同じパスワードを使うことです。例えば、メールアカウントのパスワードを誰かが解読に成功すれば、当該パスワードで保護しているすべての情報にアクセスできるため、データの盗難、個人情報の盗用などが発生する可能性があります。二番目に最も危険なミスは、便利に利用できるように名前や生年月日など、他人が類推しやすい単語や数字をパスワードとして使用することです。ハッカーはパスワード解読のため、可能な文字の組み合わせを自動で素早く代入する技術など、強力なツールを使用して一層組織化し知能化しました。これらのツールは簡単に記憶できるパスワードを使用する人々に対し、これまでかなりの効果を発揮しました。

また、膨大な量の個人情報がオンラインに露出されると、名前、誕生日、またはその他の意味のある日付を使用したパスワードも簡単に無力化することがあります。そのため、必ず解読困難な強力なパスワードを使用しなければなりません。そのためには文字、数字、特殊記号などを組み合わせて使用することが望まれます。

必須ではありませんが、デバイスごとに異なるパスワードを使用したり、一部のネットワーク機器やクライアントなどシステムごとに異なるパスワードを使用することが望まれます。VMSやその他のクライアントを使用する際は、管理者アカウントを使用せずに固有のユーザーアカウントを作ることも推奨されます。このように管理者パスワードがネットワークを通じて持続的に送信されるのを防止すると、途中で流出する可能性を遮断することができます。

ハンファテックウィンの製品は、8文字で構成されたパスワードを設定する際は、大/小文字、数字及び記号など少なくとも3つ以上の文字を組み合わせる必要があります。10文字以上のパスワードを設定する場合は、2つの文字の組み合わせが必要です。また、4回以上繰り返される同じ文字や4回以上連続する文字は、パスワードとして使用できません。パスワードを設定する際、特殊文字が使用でき、パスワードの最大長さは15文字です。

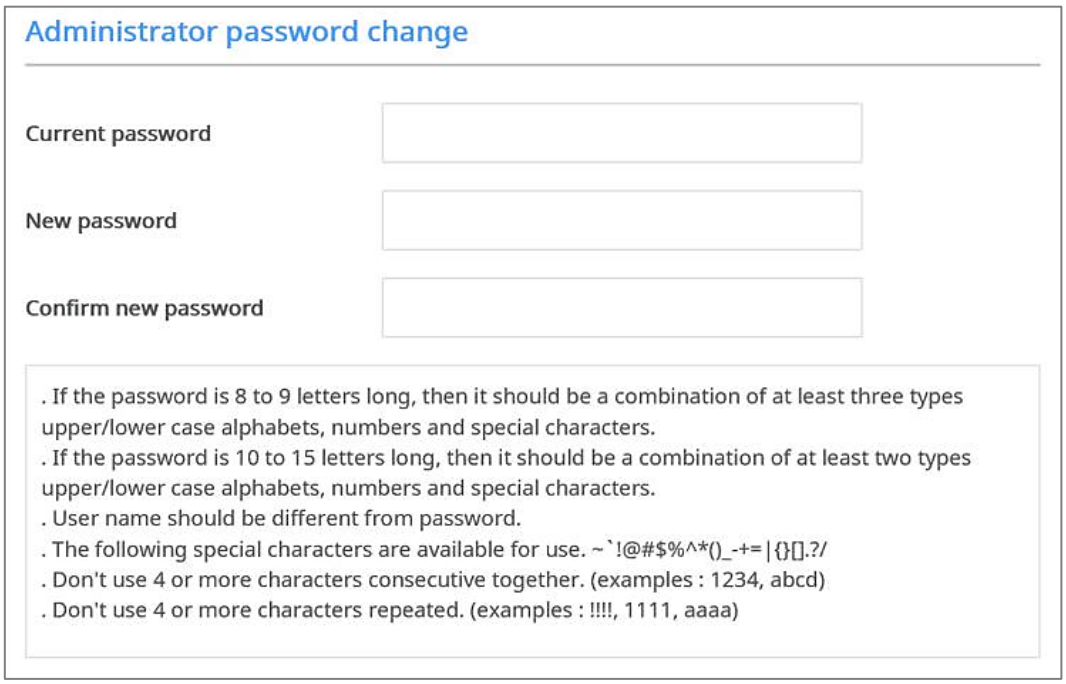

図 2. カメラパスワードの設定画面

3. アカウント権限の分離

ユーザーアカウント別に権限を制限することは、ハッカーのアクセスを遮断するのに非常に効果的です。アカウントが流出しても、設定などをはじめシステム全体にまで影響を及ぼすことを防止でき、ユーザー別に異なるアカウントを使用すると、ログ分析がより容易になるだけでなく、これによって得られる情報もより有用になります。ハンファテックウィンのカメラ、録画デバイス、VMSは様々な権限及びレベル別に、ユーザーまたはユーザーグループを区分して作成できます。

3.1. 権限の最小化

権限の最小化は、必要最小限の機能のみユーザーに提供することを意味します。例えば、1年に一回設定メニューを操作するユーザーであれば、アカウントへのすべてのアクセスを許可する代わりに、ウェブインターフェースを通じた代替ユーザーログイン機能を提供するか、当該作業をより高い権限を持つユーザーに任せることをお勧めします。これは意図しない構成変更の防止に役立つだけでなく、高いレベルの資格証明をネットワークで最大限減らすことができます。

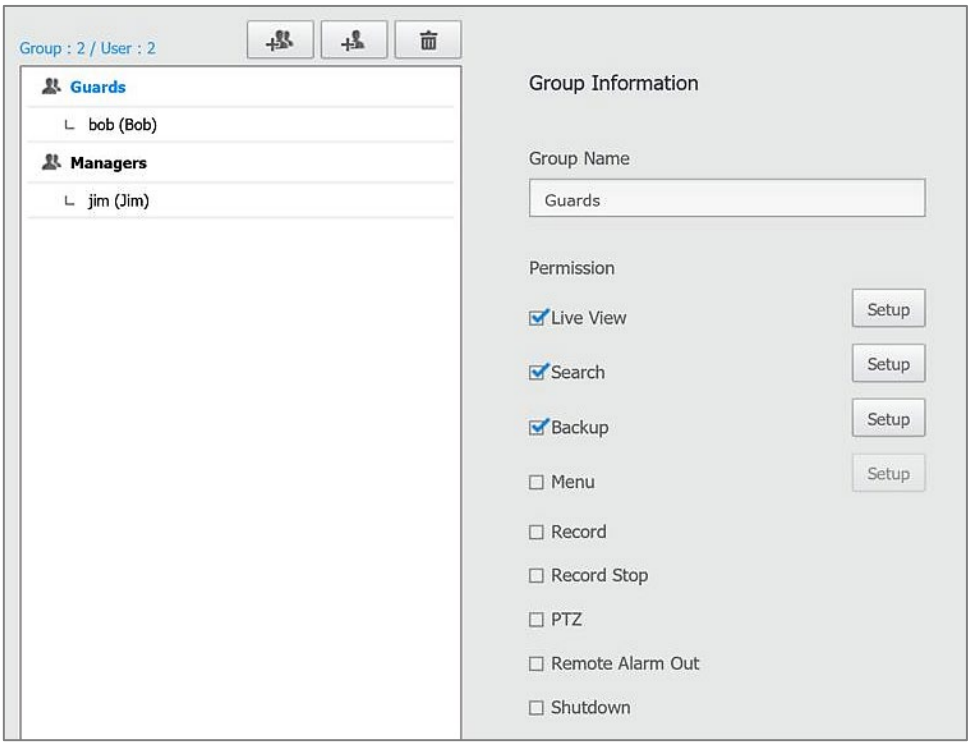

図 3. SSM ユーザーの権限設定画面

3.2. ゲストアクセス

ハンファテックウィンのカメラは、ユーザー名とパスワードが「guest」のゲストログイン機能を別途に提供します。このゲストアカウントは権限が制限的で、基本的に無効化されているため、設定メニューで別途有効化する必要があります。このアカウントはアクセス使用を制限するのに理想的ですが、必要ない場合は無効化状態で維持する必要があります。

4.1. ダイジェスト認証と一般テキスト/ベーシック認証比較

ユーザー認証時、ユーザー名とパスワードをネットワークを通じて平文とBase64エンコードを使用して伝送したり、HTTPプロトコルで使用するベーシック認証を使用して伝送することができます。このような認証方法は、資格証明に対する開放型アクセスを許可するため、任意の誰かが途中でネットワークトラフィックモニタリングが可能となり、デバイスにアクセスできるユーザー名とパスワードがそのまま表示されることになります。

このような脆弱な認証方法に代わり、ハッシュ関数を使用してデータを暗号化するダイジェスト認証があります。このように暗号化されたデータはデバイスでハッシュ処理された資格証明と比較されます。結果的にダイジェスト認証はユーザー名が露出するという小さな短所がありますが、ネットワークを介して実際のパスワードを伝送しないため、安全なユーザー認証の方法の一つです。

ハンファテックウィンの全製品はダイジェストパスワードに対応しており、安全ではないベーシック認証は提供いたしません。しかし、デバイスに接続するすべてのクライアントにも同じように適用されるわけではありません。したがって、すべてのクライアントが動作しながら一般テキストまたはBase64パスワードに切り替わらないようにすることが重要です。

4.2. SSL 暗号化

セキュリティを効果的に維持できる良い方法の1つはSSL暗号化です。この方法を使用すると、ユーザー名とパスワードはもちろん、ユーザーデータを伝達しようとする地点まで安全に伝送でき、デバイスのセキュリティを手軽かつ経済的に強化することができます。

SSL暗号化は、証明書をインストールして実行するのに数秒しかかかりません。その他にもSSL証明書は常用の認証機関で購入したり関連法人を通じて発行したりすることができ、アクセスする際に認証書のセキュリティメッセージが表示されないように設定することもできます。SSLセキュリティは潜在的に安全ではないネットワークまたはクラウドにおいて通信チャネルを強化するのに効果的ではありますが、暗号化が必要またはサポートされるチャネルを決定しなければなりません。これには、カメラからNVR/VMSまで、そしてVMSからクライアントまで含まれます。また、資格証明が一般テキストに伝送されるのを防止するためには、SMTPプロトコルを使用してメールを送信する際にもSSL暗号化を使用する必要があります。そのためには、SMTPサーバーがSSL/TLS をサポートし、使用されているポートも確認する必要があります。

構成オプションでは、デフォルトに提供される固有の証明書または公開証明書を選択するか、または証明書及びキーファイルをインストールして名前を指定することができます。HTTPSオプションを変更するとカメラが再起動され、それ以降はHTTPSポートにより暗号化された通信のみ許可されます。

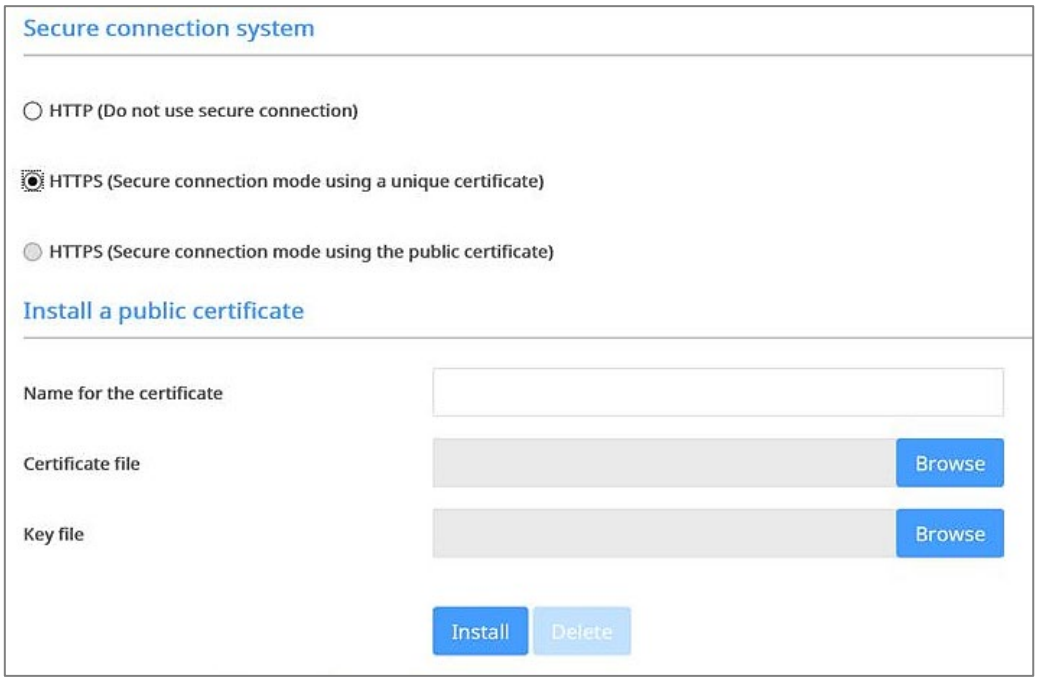

図 4. SSL 暗号化の設定画面

4.3. クラウド使用の最小化

クラウドサービスを使用してシステムの録画や確認を行う場合には、多大な帯域幅が必要となるだけでなく、セキュリティ問題まで発生しかねません。クラウドにデバイスを接続すると、ログイン情報が伝送されるからです。この情報が収集されたり、中間者攻撃(MITM、Main in the middle)が発生した場合には、資格証明の復号化または再生により無断アクセスが可能となります。また、一部のクラウドサービスではSSL暗号化またはダイジェスト認証をサポートしていない場合もあります。

5.1. 物理的なネットワーク分離

セキュリティネットワークの安全性を効果的に高めるためによく使用される技術は、カメラと録画デバイスを企業ネットワークから物理的に隔離することです。こうするとアクセスが難しくなり、攻撃者がアクセス権限を得られなくなります。また、ほとんどのNVRは複数のネットワークインターフェースを採用しているため、録画やワークステーションアクセスは異なるインタフェースで行うことが可能です。したがって、外部に露出し、セキュリティ統制を強化しなければならないデバイスの数が少なくなります。

5.2. VLAN

別途のネットワークを使用しないときは、バーチャルLAN(VLAN)を使用してセキュリティネットワークを企業ネットワークから隔離することが望ましいです。VLANはネットワークスイッチにおいて運用され、スイッチポートからトラフィックを隔離します。したがって、ファイアウォールを介してセキュリティデバイスをネットワーク上の他デバイスから隔離して保護することができます。特定のデバイスへのアクセスが必要な場合は、ファイアウォールルールを作成するか、デバイスをVLANに追加してください。

5.3. IP フィルタリング

IPフィルタリングはネットワークデバイスへのアクセスを許可したり、拒否するユーザーを明示的に指定する方法です。ここではIPアドレス、範囲またはサブネットを指定できます。こうするとPCのIPアドレスにより、正しいユーザーにのみデバイスアクセスを許可し、意図しないローカルネットワークまたはインターネットアクセスの試みを拒否することができます。ハンファテックウィンのデバイスではIPv4及びIPv6 IPアドレス及びプレフィックス(Prefix)を入力することにより、アクセスを拒否したり、許可することができます。

IPとプレフィックスが確認できるようフィルタリング範囲も表示されます。適用する前にこの範囲を必ず確認しないとアクセス拒否を防ぐことができません。IPv4とIPv6項目はそれぞれ最大10個まで追加できます。

図 5. IP フィルタリングの設定画面

5.4. VPN

遠隔地からのアクセスにはVPNソリューションを使用するのが最も良い方法です。VPNを使用すると、安全な暗号化チャンネルを作成し、ユーザー名やパスワードなどの情報が流出する可能性を未然に防止できるからです。VPNソリューションはVPNルーターなどの専用ハードウェアをはじめ、クライアントPCで実行されるソフトウェアのVPNが必要となる場合があります。

5.5. 基本ポートの変更及び未使用ポート/サービス/プロトコルの無効化

現在のようなコネクテッド環境では、意図に関係なく多くのデバイスがインターネットに接続されているため、ハッカーもスキャンを通じてこのようなデバイスを検索できるサービスがたくさんあります。

スクリプトキディーズ(Script kiddies)、意図しない攻撃や不注意なアクセスを含むこれらのスキャンプログラムを簡単に防ぐには、インターネット上で見つけられる程度のよく知られているネットワークデバイスの基本ポート番号を他の番号に変更することです。特に、HTTPウェブポートはほとんどのデバイスでウェブブラウザを通じてアクセスできるようにポート80に基本設定されている点でさらに重要です。例えば、このポートを8000に変更すると、ウェブブラウザにアドレスを入力する際、ポート番号の追加入力が必要になるため、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者から保護することができます。

セキュリティ装備の多くは、一種のコンピュータのようにOSを基盤に動作し、ハンファテックウィンは、未使用サービスを除去したり、無効化することで、不必要な要素を取り除いたカスタマイズ型のOSを製品に適用してきました。しかし、いくつかのメーカーはデバッグなどの維持及び管理便宜、あるいはセキュリティ認識及びポリシーの不在により、未使用サービスを活性化状態で残す場合があります。最近、他メーカーのデバイスのハッキング事故を調べてみると、ハッカーがファイル全体とサービスに対するすべてのコマンドアクセス権限を与えるテルネットを通じてデバイスにアクセスするケースが多くありました。Windows基盤の録画プラットフォームでは、持続的なセキュリティアップデートとパッチの他にも、時間、トラッキング及びインターネットアクセス情報を要求するサービスが多くあります。

ハンファテックウィンのデバイスは、有用な機能をサポートするプロトコルを多様に利用します。しかし、アプリケーションに必要でないサービスはすべて無効にすることが望ましいです。ここにはマルチキャスト、DDNS(Dynamic DNS)、QoS(Quality of Service)、Bonjour、UPnP(Universal Plug and Play)検索及びポートフォワーディング、リンクローカルアドレス、FTP(File Transfer Protocol)、NAS(Network Attached Storage)、メール通知が含まれることがあります。前述したように、ユーザー別に異なるアカウントを利用し、FTP、NAS、メールの権限を制限するのもセキュリティを強化する良い方法です。自動IPの設定は基本的には有効になっていますが、他のサービスはすべて無効になっています。

5.6. RTSP

ほとんどのVMSは、RTSPプロトコルを使用してビデオをストリーミングします。ハンファテックウィンのカメラは、認証要請なしでRTSPビデオ接続が可能なオプションをサポートします。このオプションは公開視聴時資格証明が露出されないよう保障し、認証がサポートされない第三者サービスを統合できるという点でインターネットを通じたストリーミングに有用です。ハンファテックウィンのカメラは、ユーザーインターフェースでこの機能を手軽に活性化させることができます。すべてのビデオストリームは、セキュリティ上、認証を要求するようにすることが望ましいです。公開視聴が必要な場合は、サードパーティサービス業者が認証されたストリームを収集し、カメラを直接共用アクセスから隔離した他のポータルを通じて共用アクセス権限の提供が可能です。

基本的に、ハンファテックウィンのカメラは、ユーザー認証時にHTTPプロトコルと同様にRTSPプロトコルにおいてもダイジェスト認証方法を使用するため、パスワードが平文化されません。

図 6. RTSP の認証設定画面

6. 攻撃識別及び遮断

ハッカーが最も多く使用する攻撃方法は、ランダム入力攻撃(Brute force attack)、サービス拒否(DoS、Denial of Service attack)とバッファオーバーフローです。これらの攻撃方法はすべて有効性が検証されているため、無断アクセスからデバイスとネットワークを保護できる適切な解決策が必要となります。ハンファテックウィンのカメラは、このような攻撃を効果的に遮断できるよう、次のような検証された方法を提供します。

6.1. ユーザーアカウントロック

ハッカーはデバイスのパスワードを探すため、非常に速いスピードでランダム値をデバイスに入力します。このような行為を許可する場合、一定時間が経つとデバイスのパスワードが露出する恐れがあります。セキュリティを向上させるため、ハンファテックウィンのデバイスは30秒以内5回以上のパスワードランダム入力攻撃(Brute force attack)を遮断しており、単に全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、非認可接続の試みのみを遮断することで、ランダム入力攻撃によって誘発されうるサービス不能(DoS)攻撃まで予防しています。

図 7. パスワード入力が連続 5 回エラーになった場合の、ログイン遮断画面

6.2. バッファオーバーフロー遮断

ハッカーが頻繁に使用するもう一つの攻撃方法は、情報公開、データベースまたはファイルシステムのような他の基本サービス宛に送信するコマンドをデバイスに伝送することです。これらのコマンドは、パーザ(Parser)またはデータベースの弱点を悪用したりインターフェースを破壊して、データベースサーバー、OSまたはファイルシステムに直接伝送されます。ハンファテックウィンのデバイスは、ウェブサーバーやデータベースにコマンドを伝送する前にフィルタリングし、基本的な主要サービスにハッカーがアクセスできないよう遮断することで、バッファオーバーフローと直接ハッキングによる攻撃を防止します。

6.3. 安全なデバイス配置

使用するデバイスが悪意を持った第三者によって変更される可能性があると考えられますが、次のような方法でそのような事態を予防することができます。

1）ネットワークデバイスを鍵のかかるラックに収納したり、ロック機能のあるネットワークプラグを使用する方法があります。これらの方法により、認可されていないデバイスがスイッチなどのネットワーク機器へのアクセスを物理的に防ぐことができます。しかし、侵入者が強制的にロックデバイスを壊す可能性があるため、完璧な防御技術ではないため、他の種類のネットワークセキュリティ技術と並行して使用してシナジーを出すのが効果的です。

2）スイッチに接続されたデバイスに対してポートセキュリティ(port security)を行う方法があります。この方法は、スイッチの特定のポートに許可された特定のデバイスのみ接続できるようにすることです。MACフィルタリングや802.1x証明書ベースのアクセス制御を使用する方法があります。

3）デバイスに適したハウジング手法を適用することで、ユーザーのデバイスへの物理的なアクセスを容易にすることを防ぐ方法があります。ネットワークと電源ケーブルが電線管を通ったり、壁や天井を通ってデバイスに直接接続されたりすると、ケーブルが切断されず、安全に管理できます。ハンファテックウィンの耐衝撃ドーム(Vandal Dome)カメラも同様に、このようなケーブルに対する物理セキュリティの解決策となります。

6.4. 録画の連続性保障

窃盗犯は侵入時、映像の証拠を隠滅する目的で録画デバイスやサーバーを盗んだり、破損することがしばしばあります。これを防ぐためのひとつの方法は、カメラごとにSDカードを使うことです。録画維持期間が短いとはいえ、録画二重化機能をサポートしているからです。この他にも、NVR、VMSに障害が発生したり意図的であれ偶発的であれネットワークが中断する場合でも、ハンファテックウィンのカメラは物理的ネットワーク階層の接続解除を自動的に感知し、電源が供給され続けている限り、SDカードに引き続き録画することができます。

構成オプションとしては、SDカード機能の有効/無効、Full/I-Frame/Noneによる連続/イベント録画、イベント前後の録画持続時間、録画ファイル形式(AVI/STW)、オーバーライト、自動削除/持続時間、一般録画予約及びSDカードファイルシステムがあります。録画する時は、プロファイルまたはコーデックを制限なく選択できます。

また、SDカードの代わりにNASを構成したり、SDカードは障害措置のための選択的バックアップ録画メディアとして使用し、NASを基本録画デバイスとして構成することもできます。NAS録画は、IPアドレス、ユーザーID、パスワード及び基本フォルダが追加されることを除いて、構成オプションが同じです。

6.5. デバイスに対する物理的アクセス遮断

ネットワークセキュリティデバイスへの物理的なアクセスは、何よりも重要です。物理的アクセス時、ほとんどのデバイスで初期化が可能であるため、権限のないユーザーが新しい設定を構成できます。DID(Defense in Depth)セキュリティモデルによれば、ネットワークデバイスはむやみにアクセスできないようにインストールすることが重要であるため、アクセス制御及び/またはビデオセキュリティモニタリング機能などを使用することが効果的です。これによりセキュリティ階層が多重化され、単一のメカニズムに依存しなくなります。

例えば、スイッチの空いているポートにネットワークケーブルを接続して内部ネットワークにアクセス可能となり、使用しないスイッチポートを無効にすることで、認可されていないデバイスへのアクセスを予防することができます。スイッチの特定のポートを無効にする機能は、スイッチが基本的に持っているオプションなので、低コストで難なく実現できます。

ただし、この方法は、既に接続されている認可済みのデバイスをスイッチから取り外し、

新しい非認可デバイスを接続してアクセスする方法だと、アクセスを防げないのがデメリットです。このようなデメリットを補完する方法として802.1x証明書ベースのアクセス制御方式を使用することを推奨します。

6.6. 802.1x 証明書ベースのアクセス制御

ほとんどの建物ではネットワークポートに近づいたり、カメラの電源プラグを抜くことや、ケーブル操作によりイーサネットネットワーク施設へのアクセス権限を得ることができます。802.1x標準はこのような方式のアクセスを防止できます。

802.1x標準はポート基盤のネットワークアクセス制御をサポートし保護中のネットワークにアクセスしようとするデバイスに対する認証手続きを行うことができます。したがって、デバイスごとに識別証明書をインストールしなければならず、有効でないデバイスによってネットワークにアクセスしようとするとアクセスを拒否します。

Wisenet Device Managerを使用すると、カメラ一台ずつ設定する必要はなく、ネットワーク内のカメラの802.1x認証を簡単に有効化し、証明書を配布することができます。構成オプションとしては、EAPタイプやEAPOLバージョンの選択、ユーザーID及びパスワードの設定、証明書/キーインストールなどがあります。

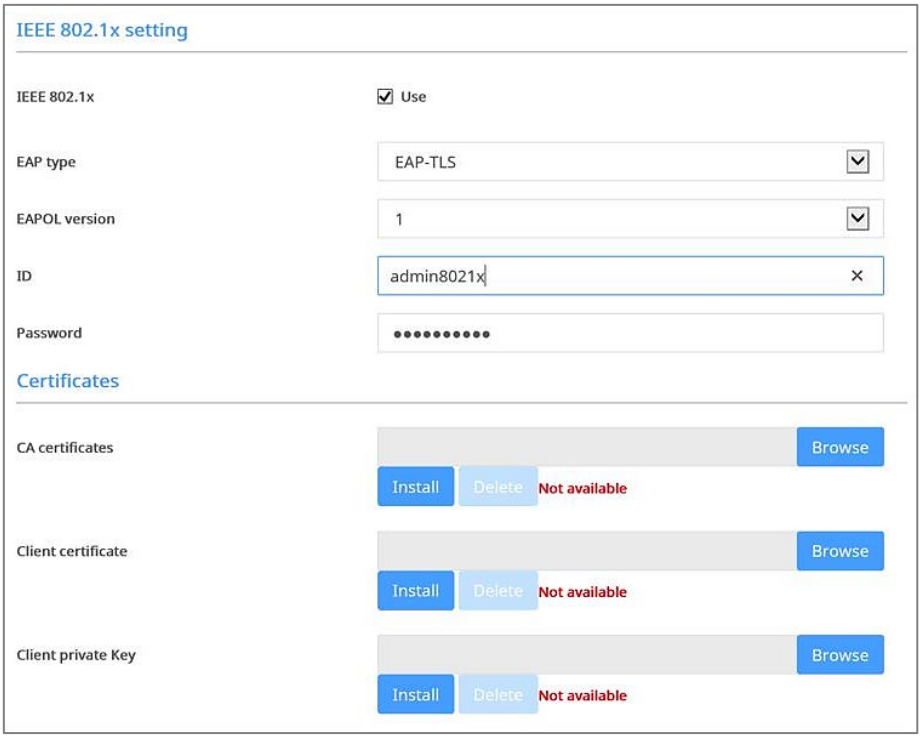

図 8. 証明書のインストールメニュー画面

6.7. 電源

UPSは停電、節電及び計画された遮断をはじめ、偶発的または悪意的な電源遮断時にネットワークデバイスの電源供給を維持すると同時に、瞬間電力の急増による損傷を防止することができます。ほとんどのIPカメラはPoE電力予算が超過する場合に備えて電源二重化機能を提供し、モデルによってはPoEや低電圧12v DC/24v ACを電源として使用できます。ほとんどのネットワークスイッチもデバイスタイプ(電話機、カメラ、WAPなど)や電力不足時のポート重要度を表す優先順位を指定することができます。また、管理目的でUPSがネットワークに接続された場合には、安全性を確認し、セキュリティアップデートをインストールしなければなりません。UPSなどのモニタリング目的でLANやインターネットに接続された補助デバイスを介してネットワークにアクセスしようとする攻撃事例もあったためです。

6.8. ネットワーク管理

セキュリティを維持するために、ネットワーク管理者はカメラやその他のデバイスをインストールした後も、様々な作業を継続的に実施しなければなりません。システム改善や一貫した設定管理、ソフトウェアアップデート、ソフトウェアの企業セキュリティ標準の遵守などがあり、中でも特に全ての変更点の検討が非常に重要です。

ハンファテックウィンは、前述したように、デバイスを厳格に管理し、ハッカーからネットワークを保護することが非常に重要な役割だということを正確に認識し、強力かつ包括的な戦略を遂行しています。

6.9. デバイスログ確認

ハンファテックウィンのカメラはすべてのデバイスの設定変更事項を記録するため、ログを確認してどのような内容を変更し、誰が変更したのかを把握することができます。ほとんどのログ項目には、ロールバックが容易になるよう以前の設定と新しい設定が含まれているだけでなく、工場出荷状態に初期化する場合にも、このようなログがそのまま維持されるようになっています。

ログを初期化できないようにする機能は、ハッカーが自分の侵入を隠すため、故意にデバイスを初期化する場合を予防し、悪意を持った第三者の侵入経路の分析及びトラッキングにおいて非常に有効に利用されます。Wisenet Device Managerを使用すると、複数デバイスでログを一度に手軽にダウンロードできます。

設定が有効か検証できない場合は、出荷条件初期化を進め、正しい基本設定に戻すことができます。ハンファテックウィンのカメラでは、電源を入れた状態で初期化ボタンを5秒間押すと、工場出荷時設定に切り替わります。カメラを初期化した後は、必ずIPアドレスを再構成して基本管理者パスワードを設定しなければなりません。工場出荷状態に初期化する場合でも、必要に応じてすべての「IP&ポート」や「ネットワーク」の設定は維持する事が可能です。

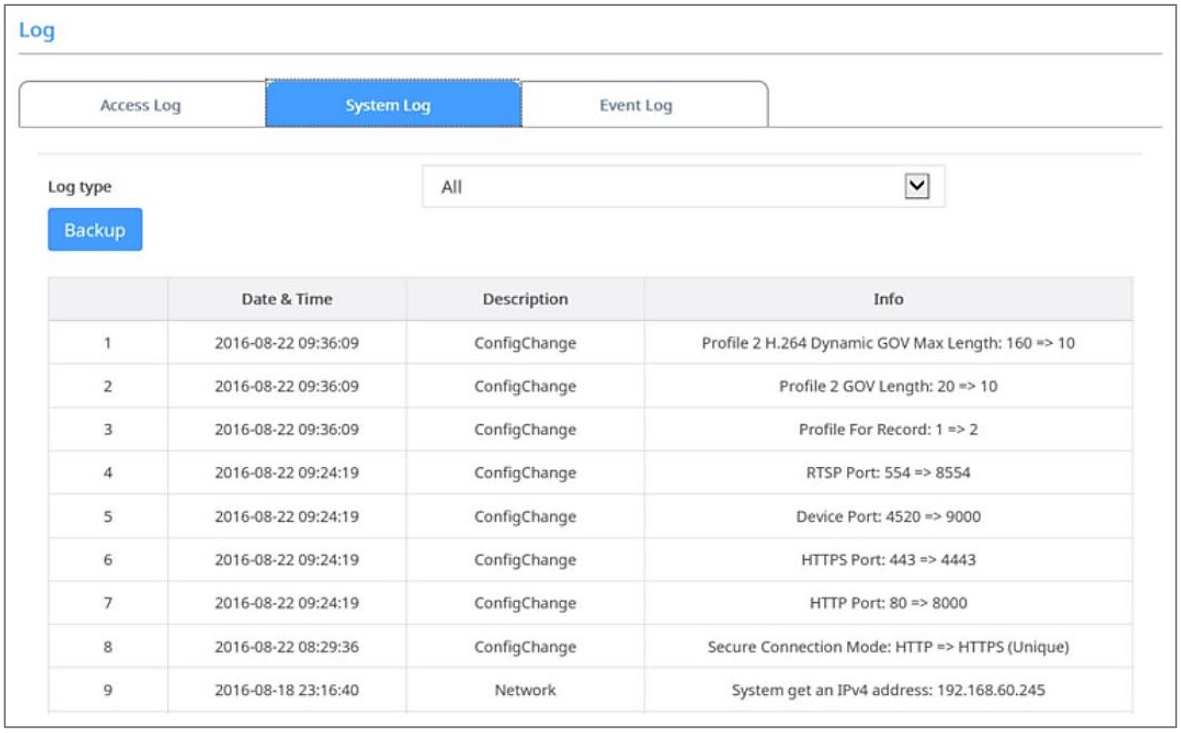

図 9. システムログ中の設定変更項目確認

6.10. 定期的なファームウェアアップデート

ハッカーは、長い間セキュリティアップデートをインストールしていなかった旧バージョンソフトウェアの弱点を悪用するため、虎視眈々と機会を狙っています。一度弱点が見つかるとオンラインに急速に伝播するため、不特定の個人が以前のファームウェアバージョンのデバイスはもちろん、さらにネットワークまで容易に浸透できる経路が開かれるわけです。ソフトウェア供給企業はこのような事実を認識し、問題を改善したアップデートをはじめ、無断アクセスを防止できるパッチを持続的に配布しています。

ハンファテックウィンのすべてのデバイスに使用されるファームウェアには、管理者が最新バージョンを運用するために参照できるアップデートリストが含まれています。ファームウェアは最新の状態を確認してから、定期的にアップデートを続けることをお勧めします。ほとんどのインストーラーも、システムインストールに先立ってファームウェアの最新状態の確認及びアップデートを行う傾向にあります。

Wisenet Device Managerを使用すると、すべてのデバイスのファームウェアバージョン及び最新バージョンを一度に確認することができ、数回のクリックだけで便利にファームウェアをダウンロードしてインストールすることができます。

6.11. ファームウェア暗号化

ほとんどのセキュリティデバイスのメーカーは、ユーザーが機能追加、バグ改善、セキュリティアップグレードを行えるよう、自社のサイトを通じてファームウェアを提供しています。このように改善のために提供されるファームウェアもハッカーのターゲットになり得ます。

ファームウェアの中には私たちが思っている以上に非常に重要な情報が含まれています。例えば、ユーザーアカウントを確認するアルゴリズム、重要情報を暗号化するために使用する暗号化アルゴリズムとキー情報、運用システムファイルや重要ウェブサービスのURLなどがさらされる可能性があり、バックドア(Back Door)を浸透させることができる弱点がさらされる可能性もあります。このような弱点に付け込んで、変造されたファームウェアの流布とアップデートが可能になり、これによりハッカーにデバイスの制御権が移ると、他の周辺システム攻撃の前線基地として使用されることになります。

ネットワークセキュリティデバイスを含むほとんどのエンベデッドデバイスは、現在のところ、ファームウェアセキュリティのために特別な安全デバイスを設けていません。ハンファテックウィンは、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グレードのため、暗号化されたファームウェアを配布しており、業界で勧告する安全な暗号化アルゴリズムを使用しているため、新しいファームウェアが配布されたら、最新のファームウェアに安心してアップデートしてください。

6.12. ビデオフォーマット

ほとんどのセキュリティデバイスは、産業標準、開放型ビデオフォーマット及び固有のビデオフォーマットをサポートします。ユーザーにとっては、自身のお気に入りのメディアプレーヤーで動画ファイルを開くことができるという点で、開放型動画フォーマットが理想に見えるかもしれません。しかし、セキュリティアプリケーションは編集、修正または操作が不可能なフォーマットが必要となります。これは、ビデオファイルをダウンロードする際に、ビデオ認証をはじめ改ざんされていないことを保障するメカニズムが必ず必要という意味で必須です。しかし、開放型フォーマットではこれを実現することはできません。

ハンファテックウィンのビデオフォーマットは、このように重要な保護機能をサポートするだけでなく、複雑なパスワードを選択的に適用し、ビデオを証拠として使用できるようにサポートします。ハンファテックウィンのNVR/VMSからSECファイルフォーマットで抽出したビデオファイルには、再生に必要なプレイヤーが自動的に含まれており、別途のプレイヤーをインストールする必要がなく、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できます。SECファイルとして保存すると、ビデオのハッシュ情報をフレームごとに一緒に保存し、ビデオの変造を確認できるウォーターマーク機能を提供します。パスワードを設定して保存すると、暗号化されたSECフォーマットで保存されるため、当該ビデオファイルが流出しても個人情報を保護することができます。

ハンファテックウィンのVMSであるSSMでは、ウォーターマーク機能だけでなくデジタル署名を追加でサポートし、全体のビデオ映像に対するハッシュ情報を使用して署名及び検証することで、該当ビデオの変造の有無と出所を確認できます。このウォーターマークとデジタル署名の検証はバックアップビューアーツールを使用して確認できます。

録画デバイスのウェブブラウザからはAVIファイルフォーマットでも抽出が可能で、当該ビデオファイルは開放型ビデオフォーマットなので、汎用メディアプレーヤーとして再生が可能です。ハンファのIPカメラはハンファ固有のファイルフォーマット(STW)でビデオを保存でき、ウェブブラウザを通じてエクスポートできます。また、別途のSDカードプレーヤーを使って再生することもでき、AVIファイル形式で変換することも可能です。

6.13. オープンプラットフォームのアプリケーション

ほとんどのハンファテックウィンカメラは、他社アプリケーションをインストールし、ナンバープレート識別、リテールビジネスインテリジェンス、人数カウントなどの機能を追加することができます。カメラでアプリケーションを実行する際は、インストールされたアプリケーションとソフトウェアのパッケージソースを知っておくことが重要です。ハンファテックウィンカメラは、アプリケーションインストール時、そのアプリケーションで要求される権限を表示します。この情報を注意して検討し、インストールと使用の可／不可を判断する必要があります。

アプリケーションの有効性を検証できなかったり、その目的が分からない場合には、直ちにインストールを中断、除去した後、信頼できるパートナーのアプリケーションを利用してください。構成オプションとしては、自動起動の設定、優先順位レベル、アプリケーションの起動/停止、アプリケーションのインストール/除去、アプリケーションのウェブページの実行などがあります。

7. 結論

今日のようなコネクテッド環境で、特定の個人やグループがネットワークの弱点を悪用し、セキュリティを無力化しようとする試みは後を絶ちません。ネットワークを介して多数のデバイスに接続して得られる利便性は大きなメリットですが、これらのデバイスにより、悪意を持った第三者がネットワークに無断でアクセスできる可能性が増加することも現実です。したがって、ハッカーがこのようなデバイスを進入点として悪用しないように防止するためには、セキュリティ強化が必須です。前述のモデルケースを活用すれば、ネットワーク映像監視デバイスやシステムを進入点として悪用しないように保護できるだけでなく、主要な機能の完全性と連続性を維持することで人と資産を安全に守ることができるベースとなります。

エンドユーザー、IT担当者、インストール会社及びシステム統合企業間の具体的な情報に基づいた会話は、各企業または機関に適した最適なセキュリティソリューションを見つけるためのキーとなり、多くの模範事例はネットワークセキュリティを重要かつ慎重に考える企業と議論を始める出発点としても立派な役割を果たすことになります。

ハンファテックウィンは、セキュリティ専担チームを設け、製品開発の段階からセキュリティを事前に点検し、専門機関に依頼して危険診断を実施しています。徹底したセキュリティのため、ユーザー認証、データベース、ファームウェアの暗号化及びバックドア除去ポリシーを全製品に適用しており、ID/パスワードポリシーも業界で最も強力なレベルで適用しています。

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