ネットワークカメラを IT 機器として捉えるとそのセキュリティ対策が見えてくる。

ネットワークに接続しているカメラの映像が , その所有者の意図しない形で勝手にオンライン上に公表されていたというニュースが巷をにぎわせたのも記憶に新しいところです。ネットワークカメラを利用する際に私たちが講じるべきセキュリティ対策はどのようなものでしょうか。

それは、使用するカメラや録画機器、接続用のネットワークスイッチなどシステムの構成要素を IT 機器として捉えてシステムの利用に当たるのがベストであると言えそうです。

とはいえ、取り組みそのものはとてもシンプルです

パスワードの設定と管理

カメラ・録画・再生機器にアクセスしようとするユーザーに対してパスワードの入力を求めるよう、システムを必ず設定しましょう。工場出荷時のパスワードのままにしておく、またはパスワード認証を行わないよう設定するのは不正利用の温床となります。誰もが目にする場所にパスワードを記載したメモを残すようなことはしてはいけません。

アクシス製品は、初期設定時にお客様ご自身で管理者ユーザーのパスワードを決め、設定していただくステップを設けています。さらにパスワード認証は初期設定で有効になっています。

ファイアウォールで外部からの攻撃を遮断

システムと外部ネットワークとの間にファイアウォールを設置し、パスワードの漏洩を防ぎましょう。ファイアウォールはネットワークルーターに内蔵されている場合と、別個の専用機器である場合があります。いずれも外部からの攻撃を遮断し、必要と認めたアクセスのみに留める利点があります。

認証・映像の伝送をHTTPSの暗号化で保護

導入したＩＰカメラあるいは録画・再生機器が、デジタル証明書によるＨＴＴＰＳ（ＨＴＴＰの暗号化）に対応しているならば、これを利用してＨＴＴＰを暗号化することを推奨します。これによって、認証・映像の両方を、途中で窃取されることなく安全に伝送できるようになります。

アクシス製品は、すべての機種でHTTPSによる暗号化通信をサポートしています。

拠点間の通信にはVPN（仮想プライベートネットワーク）が有効

複数の拠点から映像情報を得るシステムの場合は、その多くは拠点間の通信にインターネットを利用することになると思われます。とすれば当然、通信途上で情報が窃取されるリスクが考えられます。対策としては、ＶＰＮ（仮想プライベートネットワーク）が有効です。この仕組みは、厳重な認証・暗号化方式により、専用線を用いることなく内部ネットワークのような「閉じた」通信を行える利点があります。

ログ（記録）を定期的にチェック

仕組みをどれだけ厳重にしても、定期的にチェックしないと効果は不十分となります。システムのアクセスログ（記録）やシステムの動作ログの確認は必須です。ログの確認を通じて、不正なアクセスが試みられていないか、システムの不具合が起こっていないかを早期に発見でき、適切な対策につながります。

アクシス製品は、認証に失敗したクライアントに関するログや、接続中のクライアントに関する情報を、カメラの設定ページにて確認することができます。

パスワードやデジタル証明書、ソフトウェアを定期的に更新

パスワードやデジタル証明書の更新、可能であればシステムを構成するソフトウェアの更新も、定期的に実施しましょう。更新することで、メーカーによってセキュリティ上の弱点が改善されたソフトウェアが提供されている場合があります。