青い森のサイバーセキュリティ

令和４年10月
青森県警察本部
サイバー犯罪対策課

ネットワークカメラのセキュリティ（具体編）

◎ネットワークカメラにおける情報セキュリティ対策要件

８月号では、インターネットから見える内部システムの被害としてＮＡＳ（Network Attached Storage：ネットワーク共有ファイルサーバ）を取り上げましたが、実は、より以前から対策が呼びかけられていたのは「防犯カメラ」です。

防犯カメラは、インターネットが普及してからは、不在時の対策等としてインターネット経由で遠隔管理が出来、比較的安価な費用で設置可能な、IPカメラタイプの機器が急増しました。

しかし、セキュリティをあまり意識せずに設置されたものも多く、安易なパスワード設定や脆弱性が放置されたままで、部外者から映像が見放題(※1)だったり、ウイルス感染や乗っ取り被害に遭い、サイバー攻撃の踏み台にされている機器が世界中にあふれている状況となっています。

◎情報セキュリティ対策要件チェックリスト

このような状況を踏まえ、ＩＰＡ（独立行政法人情報処理推進機構）では、「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト」(※2)を公表しています。

このチェックリストでは、ある程度の規模のシステムも視野に、調達仕様策定からシステム廃棄までの配意すべき点が記載されていますが、ここでは、事業者自身がＤＩＹで設置するような規模でのチェック項目を取り上げます。

◎自身で出来るチェック項目

1　運用に不要なサービスの停止(UPnP、FTPなど)
2　出荷時設定のユーザーIDの削除，複雑な(英数大小記号などの一定要件)を満たすパスワードの設定
3　接続可能な利用者・端末(IPアドレス)の制限
4　システム時刻の正確性の維持(NTPサービスの利用など)
5　本体ファームウェア、管理用クライアントソフトの最新化
6　別にレコーダーを設置する場合は、レコーダーにおいても上記１～５を確認する
7　録画映像をクラウド上に保管する場合には、クラウドのアクセス制限も実施する
8　レコーダー、クラウド等の関連する機器、サービスのログを定期的に確認する

なお、接続に無線LANを用いる場合には、暗号化方式をWPA2-AES以上とすることや、SSIDの隠蔽、MACアドレス制限なども考慮に入れる必要があります。

※1　Insecam「Live cameras:Japan」 http://www.insecam.org/en/bycountry/JP/
※2　IPA「ネットワークカメラシステム　チェックリスト」 https://www.ipa.go.jp/security/jisec/choutatsu/nwcs/