

インターネットから見える内部システム

◎インターネット側からアクセス可能なNAS（共有ファイルサーバ）がランサムウェアに感染！

インターネットからアクセス可能にしていたNAS（Network Attached Storage：ネットワーク共有ファイルサーバ）がシステムの脆弱性を突かれ、ランサムウェアに感染する事例が相次いでいます。

NASや高機能複合機などは通常内部ネットワークに接続される機器ですが、低価格な機種においてもWebアクセスに対応したものが増え、業務のためインターネット側にも公開している場合があります。



これらの機器は特定用途専用機であるため、設置者は内部に組み込まれたシステムプログラム（ファームウェアと呼ばれることが多い）についてあまり意識していないことも多く、脆弱性が放置されやすいため、攻撃者に狙われ易い状況となっています。

◎ネットワークにつながる特定用途機器の棚卸しと点検を！

インターネット接続可能な特定用途機器が増えるにつれ、思わぬ装置が外部からアクセス可能になっていることが多く発生しています。

内部・外部を問わず、自社ネットワークに接続された機器が、インターネットから見て適切な状態になっているか、必要なプログラム更新がされているかなど、定期的に確認・検討しましょう。

1 対象となる機器例

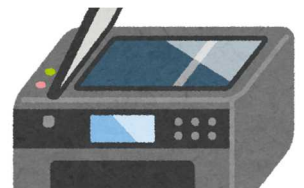
NAS、複合プリンター、複合コピー機、防犯カメラ など

2 点検、更新方法

- (1) 信頼できるポート(※)開放チェックサイト等で自社が管理するインターネット側IPアドレスの開放状況を確認
- (2) 各機器の製造メーカーのサポート情報、ホームページなどをチェック
- (3) 必要に応じメーカーから更新プログラムを入手し、手順に従い更新

3 点検の継続的な実施

自分の管理外のところで機器が導入されることもあることから、上記2を定期的に実施する。



※ TCP/IP通信において、通信に使用するプログラムを識別するための番号。0番～65535番まであり、Web(http)は通常80番(httpsは443番)。