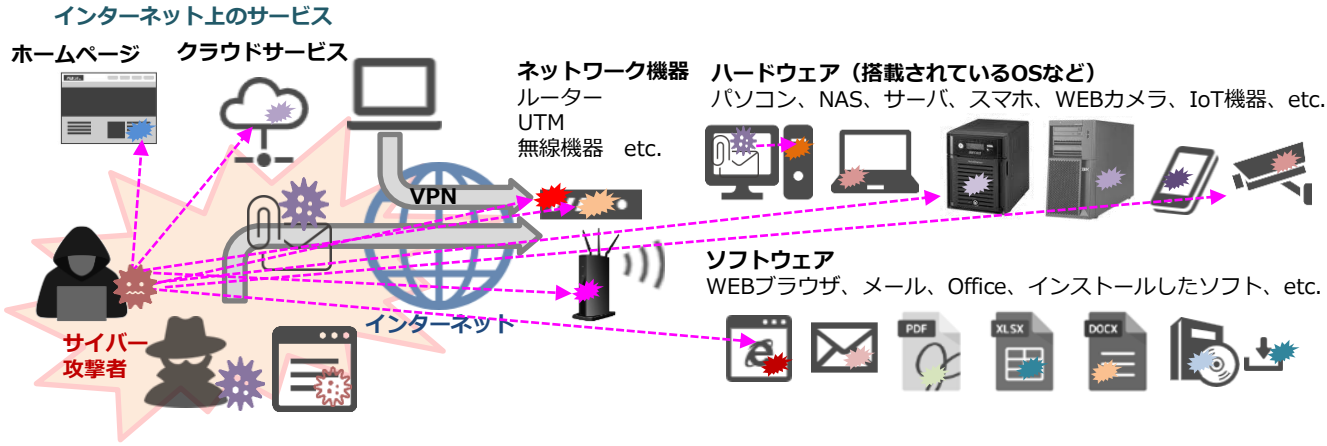
回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security Newsletter Vol.99

あさまセキュリティニュースレター

脆弱性を悪用した攻撃に要注意！

（2023年8月7日）



脆弱性を悪用した攻撃の被害例

- **VPNの機能の脆弱性を悪用**、不正アクセス、**ランサムウェア**被害　**←被害急増中！！**
- NASや**サーバの脆弱性を悪用、ランサムウェア被害**
- **無線ルータの脆弱性を悪用、設定を勝手に変更、不正な通信**されている　**←家庭向け無線ルータで被害急増**
- HPサイトの脆弱性をつき、データ流出やマルウェア置き場にされる
- ネットワークカメラ等、IoTデバイスの脆弱性を悪用、外部組織へ大量通信を送りつける攻撃
- OfficeやPDF閲覧ソフトなどの脆弱性を悪用し、マルウェア感染　・・・etc.

脆弱性（ぜいじゃくせい）について

パソコン等に搭載されているOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことを脆弱性と言います。
攻撃者は数ある脆弱性を悪用し、不正アクセスやウイルス感染等をさせます（目的は金銭）

脆弱性は次から次へと発見され、攻撃を受けていても目には見えない＝被害が出てから脆弱性が悪用されていたことに気づくことが多いため、インターネットにつながる機器やソフト・サービスすべてアップデートが必要になってきます。
脆弱性対策を自動更新で対応できるものもあれば、手動で確認しアップデートをしなければならないもの、古い機器やソフト、サポート切れのものは、新たな脆弱性に対応したアップデートがされないケースもあり、使っているハード、ソフト、サービスも多岐にわたると管理が行き届きません

脆弱性を悪用するウイルスを開いても、その脆弱性が塞がれていれば、被害の拡大を防ぐこともできます

対策

古い機器、ソフト・アプリ・クラウドサービスは使わない、インストールしない
業務で利用するソフトは、常に最新版が利用できる自動更新のサービスを検討する
業務利用のパソコンやスマホ、ソフトは、定期的にアップデートを確認し、アップデートする。
ルータ等、インターネットに直結するネットワーク機器も、定期的に確認しアップデートを怠らない
不要なネットワーク機器は接続しない

情報源
IPA　https://www.ipa.go.jp/security/security-alert/2023/alert20230801.html
総務省　https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_risk_11.html
ESET情報局　https://eset-info.canon-its.jp/malware_info/special/detail/220906.html

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414