

脆弱性の修正の遅れを突かれ…

VPNの暗証番号が流出!!

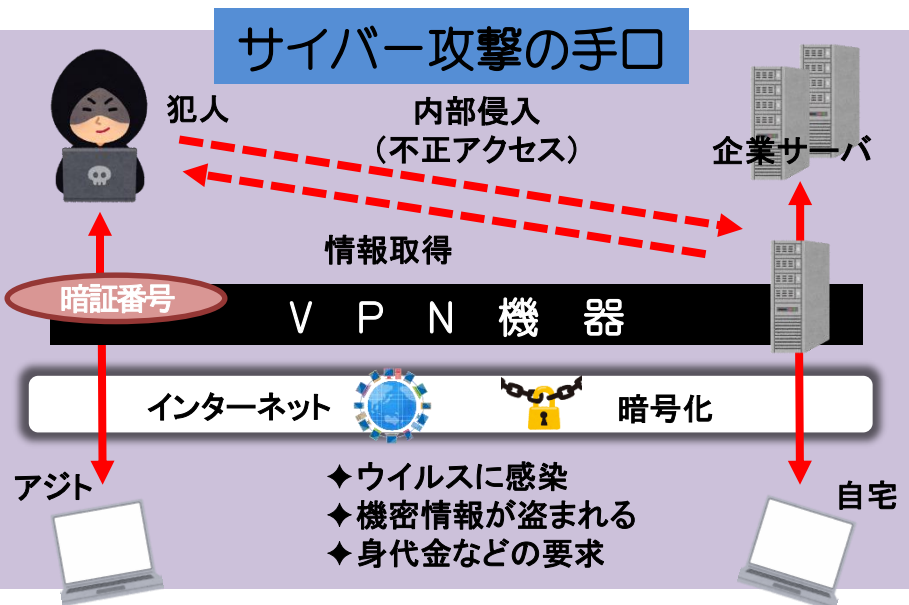


テレワークの導入に伴い、VPN(仮想私設網)を活用する企業が増える中、VPNの脆弱性が原因となり、通信に必要な暗証番号等の流出が確認されています。

問題点

本件については、米専門企業パルスセキュアのVPNサービスの脆弱性に関する修正プログラムが公開されたものの、改善を図らず被害にあった疑いが認められています。

サイバー攻撃の手口



今回の事例で重要なのが、不正侵入を前提とした

「ゼロトラスト」(信頼しない)

と呼ばれる対応が求められています。



《 対策 》



- 利用者(社員)毎にアクセス制限を設ける
- IDや暗証番号のほか、生体認証などと組み合わせる「多要素認証」を採用する
- VPNの認証に暗証番号とワンタイムパスワードを使用する
- 導入サービスの製品情報をチェックし、ソフトウェアや機器を逐一更新する