No.29　令和７年２月

テロ対策ネットワーク 岐阜 通信

発行　テロ対策ネットワーク岐阜事務局

高度な技術を悪用したサイバー攻撃の情勢について

警察庁サイバー警察局より公表された「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」の中に、近年特に注意すべき、機器やソフトウェアのぜい弱性に関する危険性と対策について説明がありましたので紹介します。

【ぜい弱性の危険性と対策】

○　ぜい弱性の危険性

攻撃者は、ぜい弱性があるネットワーク機器を攻撃の足掛かりとして、内部ネットワークに侵入し、不正プログラムへの感染や機密情報の窃取、ランサムウェアによるデータの暗号化等の攻撃を行います。

その結果、攻撃を受けた事業者は被害拡大を防止するためにシステムの運用を停止せざるを得なくなる場合や、業務に必要なファイルが暗号化されることによって業務継続に影響が及ぶ場合があります。

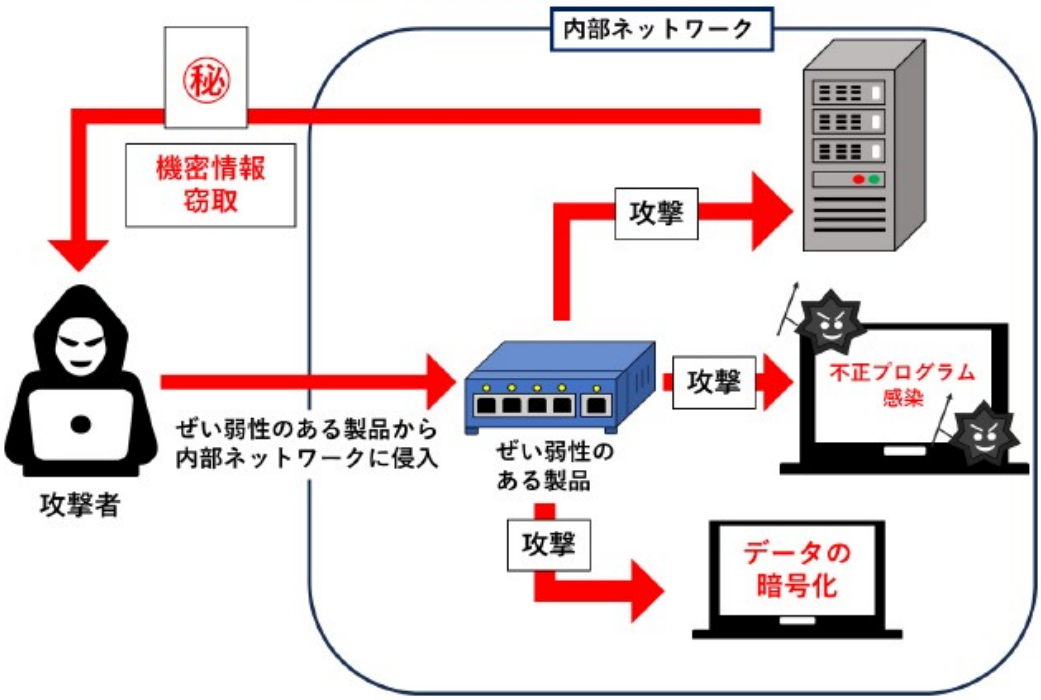
○　ぜい弱性対策

自組織で使用している機器については、そのぜい弱性を放置することなく、各製品のベンダーが公表しているアドバイザリー（ぜい弱性の内容や対策方法をまとめた文書）を基にファームウェアのアップデート、侵害の有無の確認等の対策を確実に実施するほか、平素からぜい弱性情報やアップデートに関する情報を確認し、対処することが必要です。

また、管理外のネットワーク機器が存在しないか確認することも必要です。

システム保守を外部委託している場合は、ぜい弱性の対処が保守契約に含まれているかを確認し、その対処が適切に実施されていることを確認することも重要です。

【ぜい弱性を放置することの危険性】



【出典】　警察庁サイバー警察局「令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf