F－CSNET通信かわら版

令和８年７月号

見落としていませんか？「IT資産管理」の必要性と対応

クラウドサービスの利用や自社システムDX化の推進により、パソコンやスマートフォン、ルータ・各種サーバ・VPN機器・Wi-Fiなどの**「自社ネットワークへの接続機器（IT資産）」**の認証情報を含めた**管理不備**を突いたサイバー攻撃が増加しています。

1　IT資産管理上の危険な３つの放置

①通信機器の放置

管理者が不明なままのルータ、無断で設置されたWi-Fi機器

⇩

ログ取得設定の不備

機器の乗っ取り

②脆弱性の放置

VPN機器やルータ、サーバの未更新による脆弱性が存在

⇩

脆弱性攻撃対象

③アクセス権の放置

退職者アカウント、委託終了外部業者のアクセス権が放置

⇩

正規の認証情報を使用した不正アクセス

⇩

【３つの放置が連鎖した場合に起きること】

1　自社の**ネットワーク乗っ取りによる「踏み台化」**

2　全社的な**ランサムウェア被害**

3　IT資産管理不足による**長期の業務停止**

2　ＩＴ資産管理のキホン

①　ＩＴ資産の可視化

自社で使用するパソコン・ルータ・Wi-Fi・サーバ等の通信機器を**「資産管理台帳」**に登載して一元管理を実施

（機器種別・設置場所・IPアドレス・メーカー・バージョン等）

②　システムの最新状態の維持

管理するIT資産のファームウェアやバージョン、脆弱性に関する更新を随時行い、システムの状態を最新に保つ。

③　アクセス権・パスワード等の見直し

- 使用していない通信機器の遮断・停止
- 退職者や外部委託先などのアカウントの棚卸し
- 初期パスワードの変更、多要素認証（MFA）の導入

3　ＩＴ資産管理台帳の作成

① **必須の管理項目を定義する（フォーマット作成）**

表計算ソフトなどで管理する際の基本項目を定義

(機器種別・設置場所・IPアドレス・メーカー・バージョン等)

② **現有資産の棚卸しと可視化（資産の確認・データ入力）**

ツールの使用や現物確認による台帳への登載

③ **運用ルールの策定**

・台帳と実態の不整合の防止（年に数回の確認）

・管理外ＩＴ資産のネットワークへの接続禁止　等

◆　福岡県中小事業者サイバーセキュリティ支援ネットワーク（通称：F-CSNET）とは、県内中小事業者のサイバー犯罪被害の未然防止･拡大防止を目的として、県内の中小企業支援団体と公的機関で構築したネットワークです。

【X】

【ホームページ】