F－CSNET通信かわら版

令和８年８月号

知っておきたい！ シャドーITの脅威！

近年、クラウドサービスや生成AIなどの利便性が向上する一方で、**会社のIT担当部門が把握していない**パソコン等の端末・クラウドサービス・VPN等を業務で無断使用する**「シャドーIT」**が企業における重大なリスクになっています。

シャドーITは組織における根本的脅威

会社の**監督・統制が及ばない**通信経路の利用（VPNや公衆Wi-Fi）や**外部サービスでデータが取り扱われた場合**、ネットワーク上の異変が発生した際に、**検知・追跡・探知が困難**となります。

社内で想定される具体例とそのリスク

・管理外VPNの使用 ・公衆Wi-Fiからの接続	・アカウント侵害 ・ランサムウェア感染
・未許可WEBサービス ・個人契約の生成AI利用	・社内規定、ガバナンス違反 ・個人情報漏洩

シャドーIT対策とIT資産管理

① **会社全体のIT資産管理**（資産の見える化）と定期的な点検
会社が所有・許可するPCやサーバ、サービス等を可視化し管理

② **「禁止」**だけではない、**「安全な代替手段」**の確保
現場のニーズに応じ、安全な公式ツールを明示・提供

◆ 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】