サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和3年
4月28日
Vol.59

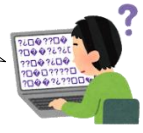
テレワークのセキュリティ対策、万全ですか？

総務省が行ったテレワークセキュリティ実態調査(令和３年１月)の結果

テレワークの導入状況	・規模を縮小しながらも引き続きテレワークを実施している企業が多い。
テレワークの導入課題	・セキュリティの確保やテレワークに必要な端末等の整備が課題となっている。
キーワードの認知度	・Emotet、標的型攻撃、シンクライアントなど、セキュリティ関係者には馴染みのあるキーワードでも一般には通じない場合がある。
情報セキュリティ対策に関する取組の実施状況	・マルウェア対策は７割が十分実施しているが、教育は７割が不十分か未実施である。 ・組織体制整備ができていない。
サポート期限切れOSに対する認識	・サポート期限切れのOSが一部で使用され続けている。 ・製造業や大規模企業での使用が多い。 ・サポート期限切れOSが危険という認識のない企業もある。

参考：総務省「テレワークセキュリティに係る実態調査」(https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/)

総務省の調査結果から、テレワークを実施している企業において、まだまだ適切かつ十分なセキュリティ対策がとられていません。



では、セキュリティ対策って何をどうすればいいの？？

まずは、次の５つの項目を守ることから始めてみましょう。

① OS、ソフトウェアは常に最新の状態にする。
② ウイルス対策ソフトを導入する。
③ パスワードを強化する（長く、複雑にし、絶対に使いまわさない）。
④ 共有設定を見直す（ウェブサービス、ネットワーク機器など）。
⑤ 脅威や攻撃の手口を知る（ウイルス付メール、偽サイトなど）。

※ 参考：IPA「中小企業の情報セキュリティ対策ガイドライン第３版」
（https://www.ipa.go.jp/security/keihatsu/sme/guideline/）

総務省のホームページ（https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/）に掲載されている、「テレワークセキュリティガイドライン第４版」「中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)(初版) 」を確認の上、テレワーク環境のセキュリティを意識した対策をしましょう。

相談窓口

愛媛県警察本部サイバー犯罪対策課 TEL089-934-0110(代)