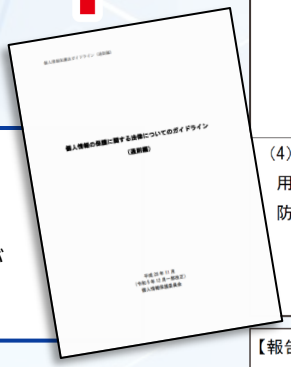
本当に必要なセキュリティ対策できていますか？

情報セキュリティ安全管理措置チェックシート

委託する側、される側 両方に義務があります！

なぜ必要？「講じなければならない」安全管理措置とは？

個人情報取扱事業者は個人情報保護法により安全管理措置を講じることが義務化されています。
具体的な手法は**「個人情報の保護に関する法律についてのガイドライン(個人情報保護法ガイドライン)」**に記載されており、サイバー攻撃などを防ぐことはもちろん、データの扱い方、システムを監視して、不正アクセスがあった際に報告することなどを義務としています。個人情報の漏えいや悪用を防ぐために重要な対策です。



▼「個人情報の保護に関する法律についてのガイドライン」が定める措置 一部抜粋

講じなければならない措置	手法の例示
（3）外部からの不正アクセス等の防止	・情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。 ・情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入し、不正ソフトウェアの有無を確認する。 ・機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 ・ログ等の定期的な分析により、不正アクセス等を検知する。
（4）情報システムの使用に伴う漏えい等の防止	・情報システムの設計時に安全性を確保し、継続的に見直す（情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む。）。 ・個人データを含む通信の経路又は内容を暗号化する。 ・移送する個人データについて、パスワード等による保護を行う。

【報告を要する事例】（※4）
事例 2）ランサムウェア等により個人データが暗号化され、復元できなくなった場合

出典：個人情報の保護に関する法律についてのガイドライン(https://www.ppc.go.jp/files/pdf/240401_guidelines01.pdf)

ガイドラインに沿って講じなければならない措置を確認しましょう

	チェック項目	☑	安全管理措置（講じなければならない措置）
1	 ウイルス対策やウイルス感染を早期に検知できる製品・サービスは導入していますか？	☐	セキュリティ対策ソフトウェア等(ウイルス対策ソフトウェア等)を導入し、不正ソフトウェアの有無を確認する。 ※自動更新機能等の活用
2	 ファイアウォールやUTMを導入するだけではなく、定期的に分析してくれるサービスは導入していますか？	☐	情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。 ログ等の定期的な分析により、不正アクセス等を検知する。
3	 IT資産・ログ管理製品は導入していますか？	☐	ソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。
4	 送信するデータやファイルにパスワードの設定ができるクラウドストレージサービスは導入していますか？	☐	メール等で個人データが含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。
5	 ランサムウェア対策に特化しているバックアップやソフトウェアは導入していますか？	☐	ランサムウェア等により個人データが暗号化され復元できなくなった場合は報告する。

大塚商会

適切な「対策」や「展示コーナー」を会場内でご案内いたします