独立行政法人 情報処理推進機構

5分でできる情報セキュリティ自社診断

診断入力

25問の全ての設問について、現在の貴社の情報セキュリティ対策の状況に照らして近いものをC列「回答」のプルダウンにある4つの選択項目から１つを選択してください。

診断項目		診断内容	回答（プルダウンから１つ選択してください）
Part 1 基本的対策	1-1 アップデート	パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	一部実施している
	1-2 ウイルス感染	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル(※1)は最新の状態にしていますか？ （※1:コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれる）	実施している
	1-3 パスワード	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	実施している
	1-4 アクセス制御	重要情報(※2)に対する適切なアクセス制限を行っていますか？ （※2:”重要情報”とは営業秘密など事業に必要で組織にとって価値のある情報や顧客や従業員の個人情報など管理責任を伴う情報のこと）	実施している
	1-5 情報共有	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	実施している
Part 2 従業員としての対策	2-6 電子メール受信	電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつけていますか？	実施している
	2-7 電子メール送信	電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施していますか？	実施している
	2-8 添付重要情報の保護	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	実施している
	2-9 無線LAN	無線LANを安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	実施している
	2-10 インターネット	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	実施している
	2-11 バックアップ	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	実施している
	2-12 保管	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	実施している
	2-13 盗難対策	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	実施している
	2-14 利用者限定	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	実施している
	2-15 立ち入り監視	関係者以外の事務所への立ち入りを制限していますか？	実施している
	2-16 盗難防止	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	実施している
	2-17 施錠管理	事務所が無人になる時の施錠忘れ対策を実施していますか？	実施している
	2-18 破棄	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	実施している
Part 3 組織としての対策	3-19 社内規定周知	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	実施している
	3-20 意識教育	従業員にセキュリティに関する教育や注意喚起を行っていますか？	実施している
	3-21 個人所有	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	実施している
	3-22 取引先	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	実施している
	3-23 外部サービス	クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？	実施している
	3-24 事故対応	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	実施している
	3-25 対策の明確化	情報セキュリティ対策（上記1～24など）をルール化し、従業員に明示していますか？	一部実施している