中小企業・小規模事業者の皆様へ

5分でできる！
情報セキュリティ自社診断

最新動向への対応、できてますか？

脅威や攻撃の変化

脆弱性攻撃

ランサムウェア

標的型攻撃

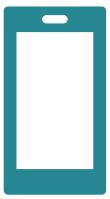
サプライチェーン攻撃

IT環境の変化

IoT機器

クラウド

AI


スマートフォン

取り返しのつかないことになる前に

あなたの会社のセキュリティ状況を

「5分でできる！自社診断」でチェック！

使用方法

① 診断編 (p.3) 25問の質問に回答してください。

↓

② 回答結果をもとに採点し、対策を検討しましょう。

100点満点だった方	入門レベルのセキュリティ対策は達成です。ステップアップを検討しましょう。	「中小企業の情報セキュリティ対策ガイドライン」を参照して、情報セキュリティ対策の強化に取り組みましょう。
70～99点だった方	ほぼ、出来ていますが、部分的に対策が不十分な点があるようです。	小さな隙間から情報が漏えいすることもあります。100 点満点を目指しつつ、「中小企業の情報セキュリティ対策ガイドライン」を参照して対策の強化に取り組みましょう。
50～69点だった方	対策が行き届いていないところが目立ちます。	点数が低かった項目について「解説編」を参考に対策を検討し、「情報セキュリティハンドブック」を活用して周知しましょう。
49点以下だった方	いつ情報流出などの事故が起きても不思議ではありません。	「解説編」や「映像で知る情報セキュリティ」を利用して、分からなかった部分や点数が低かった項目を確認し、対策を施しましょう。

中小企業の情報セキュリティ対策ガイドライン

中小企業向けに、情報セキュリティ対策の進め方を分かりやすくまとめた資料です。
対策の必要性と実践する際の手順・手法について、すぐに使えるひな形やサンプルを含む付録を用いて具体的に解説しており、できるところから始めて段階的なステップアップが目指せます。

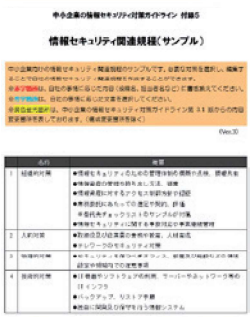
STEP1 できるところから始める

情報セキュリティ6か条

STEP2 組織的な取り組みを開始する

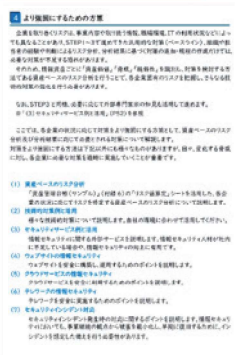
5分でできる!
情報セキュリティ自社診断

STEP3 本格的に取り組む



情報セキュリティ関連規程

STEP4 より強固にするための方策



「中小企業の情報セキュリティ対策ガイドライン」
https://www.ipa.go.jp/security/guide/sme/about.html

診断編

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマートフォンなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	(4)	2	0	-1
	2	パソコンやスマートフォン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？	(4)	2	0	-1
	3	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？	4	(2)	0	-1
	4	データの共有設定を必要な人に限定していますか？	(4)	2	0	-1
	5	故障や誤操作、ウイルス感染などによる重要情報※2の消失に備えて定期的にバックアップを取得していますか？	(4)	2	0	-1
	6	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？	4	(2)	0	-1
Part 2 従業員としての対策	7	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？	4	(2)	0	-1
	8	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？	4	(2)	0	-1
	9	重要情報の受け渡しは、暗号化など安全な手段で行っていますか？	4	(2)	0	-1
	10	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？	(4)	2	0	-1
	11	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？	4	(2)	0	-1
	12	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？	4	(2)	0	-1
	13	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？	4	(2)	0	-1
	14	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？	(4)	2	0	-1
	15	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？	(4)	2	0	-1
	16	関係者以外の事務所への立ち入りを制限していますか？	(4)	2	0	-1
	17	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？	4	(2)	0	-1
Part 3 組織としての対策	18	内部ネットワークを守るため、不正アクセス対策機能を設定していますか？	(4)	2	0	-1
	19	ウェブサイトで公開すべきでない情報を公開していませんか？	(4)	2	0	-1
	20	従業員に情報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？	4	(2)	0	-1
	21	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？	(4)	2	0	-1
	22	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？	4	(2)	0	-1
	23	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？	(4)	2	0	-1
	24	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？	(4)	2	0	-1
	25	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？	4	2	(0)	-1
			A 実施しているの合計点	B 一部実施しているの合計点		C わからないの合計点
			52 点	22 点	0	マイナス(-) 0 点
			A+B+C 合計			74 点

※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」とも呼ばれます。
※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流出した場合に組織のイメージダウンや損害賠償責任を問われるなどの管理責任を伴う情報のことです。

診断の後は次ページ以降を読んで対策を検討してください。