新 5分でできる自社診断シート

組織として最初に取組むべき
情報セキュリティ対策の自社診断シート

IPA

■ 診断の前に、まず裏面の1をご覧ください。
■ 下記の診断内容を読み、チェック欄の該当するもの１つに○を付けてください。
■ シートは、経営者または管理者の方がご記入ください。
■ の項目については、すべての従業員が実施しているかをお答えください。一部の従業員のみが実施している場合には「一部実施している」を選択してください。
の項目については、あなたの会社で実施しているかをお答えください。
■ チェックが修了したら最下段に合計を記入して、裏面の2をご覧ください。

組織名

記入者名

実施年月日　　年　　月　　日

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	自社診断パンフレットと対応しています
Part 1 基本的対策	1	Windows Update※1を行うなどのように、常にOSやソフトウェアを安全な状態にしていますか？	4	2	0	0	P3 No.1「脆弱性対策」を参照
	2	パソコンにはウイルス対策ソフトを入れてウイルス定義ファイル※2を自動更新するなどのように、パソコンをウイルスから守るための対策を行っていますか？	4	2	0	0	P3 No.2「ウイルス対策」を参照
	3	パスワードは自分の名前、電話番号、誕生日など推測されやすいものを避けて複数のウエブサービスで使い回しをしないなどのように、強固なパスワードを設定していますか？	4	2	0	0	P3 No.3「パスワード管理」を参照
	4	ネットワーク接続の複合機やハードディスクの共有設定を必要な人だけに限定するなどのように、重要情報に対する適切なアクセス制限を行っていますか？	4	2	0	0	P3 No.4「機器の設定」を参照
	5	利用中のウェブサービス※3や製品メーカーが発信するセキュリティ注意喚起を確認して社内共有するなどのように、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	0	P3 No.5「情報収集」を参照
Part 2 従業員としての対策	6	受信した不審な電子メールの添付ファイルを安易に開いたり本文中のリンクを安易に参照したりしないようにするなど、電子メールを介したウイルス感染に気をつけていますか？	4	2	0	0	P4 No.6「電子メールのルール」を参照
	7	電子メールを送る前に目視にて送信アドレスを確認するなどのように、宛先の送信ミスを防ぐ仕組みを徹底していますか？	4	2	0	0	P4 No.7「電子メールのルール」を参照
	8	重要情報をメールで送る時は重要情報を添付ファイルに書いてパスワード保護するなどのように、重要情報の保護をしていますか？	4	2	0	0	P4 No.8「電子メールのルール」を参照
	9	無線LANを利用する時は強固な暗号化を必ず利用するなどのように、無線LANを安全に使うための対策をしていますか？	4	2	0	0	P4 No.9「無線LANのルール」を参照
	10	業務端末でのウェブサイトの閲覧やSNSへの書き込みに関するルールを決めておくなどのように、インターネットを介したトラブルへの対策をしていますか？	4	2	0	0	P4 No.10「ウェブ利用のルール」を参照
	11	重要情報のバックアップを定期的に行うなどのように、故障や誤操作などに備えて重要情報が消失しないような対策をしていますか？	4	2	0	0	P4 No.11「バックアップのルール」を参照
	12	重要情報を机の上に放置せず書庫に保管し施錠するなどのように、重要情報の紛失や漏えいを防止する対策をしていますか？	4	2	0	0	P5 No.12「保管のルール」を参照
	13	重要情報を社外へ持ち出す時はパスワード保護や暗号化して肌身離さないなどのように、盗難や紛失の対策をしていますか？	4	2	0	0	P5 No.13「持ち出しのルール」を参照
	14	離席時にコンピュータのロック機能を利用するなどのように、他人に使われないようにしていますか？	4	2	0	0	P5 No.14「事務所の安全管理」を参照
	15	事務所で見知らぬ人を見かけたら声をかけるなどのように、無許可の人の立ち入りがないようにしていますか？	4	2	0	0	P5 No.15「事務所の安全管理」を参照
	16	退社時に机の上のノートパソコンや備品を引き出しに片付けて施錠するなどのように、盗難防止対策をしていますか？	4	2	0	0	P5 No.16「事務所の安全管理」を参照
	17	最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなどのように、事務所の施錠を管理していますか？	4	2	0	0	P5 No.17「事務所の安全管理」を参照
	18	重要情報を廃棄する場合は、書類は細断したり、データは消去ツールを使ったりするなどのように、重要情報が読めなくなるような処分をしていますか？	4	2	0	0	P5 No.18「情報の安全な処分」を参照
Part 3 組織としての対策	19	従業員を採用する際に守秘義務や罰則規定があることを知らせるなどのように、従業員に秘密を守らせていますか？	4	2	0	0	P6 No.19「守秘義務の周知」を参照
	20	情報管理の大切さなどを定期的に説明するなどのように、従業員に意識付けを行っていますか？	4	2	0	0	P6 No.20「従業員教育」を参照
	21	社内外での個人所有のパソコンやスマートフォンの業務利用を許可制にするなどのように、業務で個人所有端末の利用の可否を明確にしていますか？	4	2	0	0	P6 No.21「私物機器の利用」を参照
	22	契約書に秘密保持（守秘義務）の項目を盛り込むなどのように、取引先に秘密を守ることを求めていますか？	4	2	0	0	P6 No.22「取引先管理」を参照
	23	クラウドサービスなど外部サービスを利用する時は利用規約やセキュリティ対策を確認するなどのように、サービスの安全・信頼性を把握して選定していますか？	4	2	0	0	P6 No.23「外部サービスの利用」を参照
	24	秘密情報の漏えいや紛失、盗難があった場合の対応手順書を作成するなどのように、事故が発生した場合に備えた準備をしていますか？	4	2	0	0	P7 No.24「事故への備え」を参照
	25	情報セキュリティ対策（上記1～24など）を会社のルールにするなどのように、情報セキュリティ対策の内容を明確にしていますか？	4	2	0	0	P7 No.25「ルールの整備」を参照

※1　マイクロソフト社が提供しているウインドウズパソコンの不具合を修正するプログラム

※2　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

※3　インターネットバンキング、ソーシャルネットワーキングサービス（SNS）、ウェブメール、カレンダーなどインターネット経由で利用するサービスの総称

★この自社診断シートで例示している対策方法については、これらだけで十分ということを保証するものではありません。

A 実施しているの合計点	B 一部実施しているの合計点	A＋B 合計点
点	点	点

1 診断の前にこちらをお読みください。

利用方法

組織においてあまり費用をかけることなく実行することで効果がある情報セキュリティ対策を25項目に絞り込みました。
この項目の実施状況を点検し、パンフレットの解説欄を参考に未実施の対策を実施してください。

「診断内容」の読み方

診断内容に記載されている具体例にとらわれずに判断してください。例えば、No.16の診断内容は「盗難防止対策をしているか？」が設問の主旨です。ノートパソコンを所有している組織であれば、机の上のノートパソコンを引き出しに片付けるなどの盗難防止対策をしているか？
ノートパソコンを所有していない組織であれば、USBメモリや外付けハードディスクなどの備品を机の上に置いたままにしないなどの盗難防止対策をしているか？・・・という意味の問いになります。設問の趣旨が分からない、あるいは分かりにくければパンフレットを参照してください。

「うちに“秘密情報”なんてほとんどないよな・・・」
というあなた、これらの資料も秘密情報ですよ！

- 従業者のマイナンバー、住所、給与明細
- 取引先ごとの仕切額の一覧表や取引実績
- 組織の経理情報
- お客様や取引先の連絡先一覧
- 新製品の設計図などの開発情報
- 取引先から取扱注意と言われた情報

目的とメリット

- どこにどのような問題点があるのかが把握できます。
- 問題点の把握により、次のステップとして具体的な対策の道筋が見えてきます。

自社で利用していない場合

企業によっては以下の項目の対象を利用していないかもしれません。その場合は「実施している」に○をつけてください。

- No.4　ネットワーク接続の複合機やハードディスク
- No.5　ウェブサービス
- No.9　無線LAN
- No.19　クラウドサービス

このように、組織の中にあって当たり前の情報の中に、秘密として管理しなければならない情報があります。自社にどのような情報が存在しているのかを確認し整理することは、情報セキュリティの第一歩です。

秘

2 診断の後はこちらをお読みください。

100点満点だった方	入門レベルのセキュリティ対策はもう完璧です。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」とその付録3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」とその付録3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。	「5分でできる！情報セキュリティ自社診断パンフレット」で点数が低かった項目を見直し、対策を施しましょう。
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。	「5分でできる！情報セキュリティ自社診断パンフレット」や「対策のしおり」「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。

●さらなる情報セキュリティ対策を検討するには

「5分でできる！情報セキュリティ自社診断」の次のステップとして、ガイドラインを活用した情報セキュリティポリシーの策定やベンチマークでの自己診断を実施してみよう。

■**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/keihatsu/sme/guideline/

■**情報セキュリティ対策ベンチマーク**
https://www.ipa.go.jp/security/benchmark/

●自社診断シートで100点満点を目指すには

「5分でできる！情報セキュリティ自社診断パンフレット」のほか、以下のページで提供されている資料もより具体的な対策の検討に有用ですのでご活用ください。

■**情報セキュリティ対策支援サイト　iSupport**
https://www.ipa.go.jp/security/isec-portal/

■**対策のしおり**
https://www.ipa.go.jp/security/antivirus/shiori.html

■**映像で知る情報セキュリティ**
https://www.ipa.go.jp/security/keihatsu/videos/

●自社診断で例示した対策の前提

■代表者（経営者）が対策方針を直接指示・確認することができる
■全員が顔見知りである
■社内に複雑な設定を必要とするサーバーやネットワーク機器を自社所有していない
・電子メールやホームページは外部サービスを利用しているなどのように、インターネットに直接接続しているサーバーを自社所有していない
・市販のアプリケーションソフトだけを利用しているなどのように、自社発注で開発したアプリケーションソフトはない
・個人所有パソコンは、企業で所有するパソコンと同程度の対策を行った場合のみ業務利用を認めている