5分でできる自社診断シート

入門レベルとして最初に取り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するもの1つに○を付けてください。
●「実施している」はすべての従業者が実施している場合に選んでください。
●シートは、経営者または管理者の方がご記入ください。
●チェックが終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

No	診断項目	診断内容	チェック				自社診断パンフレットと対応しています。
			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	
1	保管について	重要情報※1を机の上に放置せず鍵付き書庫に保管し施錠するなどのように、重要情報がみだりに扱われないようにしていますか？	4	2	0	0	P1 No.1 保管についてを参照
2	持ち出しについて	重要情報を社外へ持ち出す時はパスワードロックをかけるなどのように、盗難・紛失対策をしていますか？	4	2	0	0	P1 No.2 持ち出しについてを参照
3	廃棄について	重要な書類やCDなどを廃棄する場合は、シュレッダーで裁断するなどのように、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	P1 No.3 廃棄についてを参照
4		重要情報の入ったパソコン・記憶媒体を廃棄する場合は、消去ソフトを利用したり、業者に消去を依頼するなどのように、電子データが読めなくなるような処理をしていますか？	4	2	0	0	P1 No.4 廃棄についてを参照
5	事務所について	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	P2 No.5 事務所についてを参照
6		退社時に、机の上の備品やノートパソコンを引き出しに片付けるなどのように、盗難防止対策をしていますか？	4	2	0	0	P2 No.6 事務所についてを参照
7		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	P2 No.7 事務所についてを参照
8	パソコンについて	WindowsUpdate※2を行うなどのように、常に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.8 パソコンについてを参照
9		ファイル交換ソフト※3を入れないようにするなどのように、ファイルが流出する危険性が高いソフトウェアの使用を禁止していますか？	4	2	0	0	P3 No.9 パソコンについてを参照
10		社内外での個人パソコンの業務使用を許可制にするなどのように、業務で個人パソコンを使用することの是非を明確にしていますか？	4	2	0	0	P3 No.10 パソコンについてを参照
11		退社時にパソコンの電源を落とすなどのように、他人に使われないようにしていますか？	4	2	0	0	P3 No.11 パソコンについてを参照
12	パスワードについて	パスワードは自分の名前を避けるなどのように、他人に推測されにくいものに設定していますか？	4	2	0	0	P4 No.12.13.14 パスワードについてを参照
13		パスワードを他人が見えるような場所に貼らないなどのように、他人にわからないように管理していますか？	4	2	0	0	P4 No.12.13.14 パスワードについてを参照
14		ログイン用のパスワードを定期的に変更するなどのように、他人に見破られにくくしていますか？	4	2	0	0	P4 No.12.13.14 パスワードについてを参照
15	ウイルス対策について	パソコンにはウイルス対策ソフトを入れるなどのように、怪しいWebサイトや不審なメールを介したウイルスから、パソコンを守るための対策をおこなっていますか？	4	2	0	0	P4 No.15 ウイルス対策についてを参照
16		ウイルス対策ソフトのウイルス定義ファイル※4を自動更新するなどのように、常に最新のウイルス定義ファイルになるようにしていますか？	4	2	0	0	P4 No.16 ウイルス対策についてを参照
17	メールについて	電子メールを送る前に、目視にて送信先アドレスの確認をするなどのように、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	P5 No.17 メールについてを参照
18		お互いのメールアドレスを知らない複数人にメールを送る場合は、Bcc※5機能を活用するなどのように、メールアドレスを誤って他人に伝えてしまわないようにしていますか？	4	2	0	0	P5 No.18 メールについてを参照
19		重要情報をメールで送る場合は、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	P5 No.19 メールについてを参照
20	バックアップについて	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	P5 No.20 バックアップについてを参照
21	従業者について	採用の際に守秘義務があることを知らせるなどのように、従業者に機密を守らせていますか？	4	2	0	0	P6 No.21 従業者についてを参照
22		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、従業者に意識付けを行っていますか？	4	2	0	0	P6 No.22 従業者についてを参照
23	取引先について	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、取引先に機密を守ることを求めていますか？	4	2	0	0	P6 No.23 取引先についてを参照
24	事故対応について	重要情報の流出や紛失、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	P6 No.24 事故対応についてを参照
25	ルールについて	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	P6 No.25 ルールについてを参照

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　重要情報とは、その情報が漏えいしたことによりビジネスに打撃を与えたり、組織の信頼失墜につながる情報
主に顧客情報、職員名簿、設計図面、開発スケジュール、仕入単価、取引額など

※2　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

※3　WinnyやShareなど、インターネット上で不特定多数のコンピュータ間でファイル（データ）をやり取りできるソフトウェア

※4　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

※5　Blind Carbon Copyの略で、他の受信者にメールアドレスを伏せて送信する機能

★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。

1 診断の前にこちらをお読みください。

利用方法

組織で最低実施すべき情報セキュリティ対策を25項目に絞込みました。この項目の実施状況を点検し、パンフレットの解説編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.6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、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メモリー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。
設問の主旨が分からない、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。

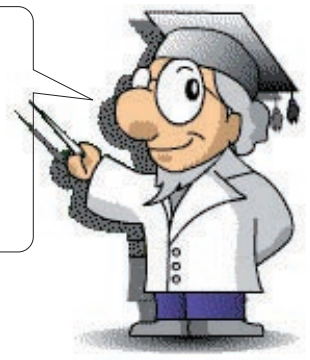
目的とメリット

- どこにどのような問題点があるのかが把握できる。
- 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くる。

5		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？
6	事務所について	退社時に、机の上の備品やノートパソコンを引き出しに片付けるなどのように、盗難防止対策をしていますか？
7		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？

「うちの組織に“重要情報”なんて無いよ」
というあなた、これらの資料も重要情報ですよ！

- お客様や取引先の連絡先一覧
- 組織の経理情報
- 新製品の設計図などの開発情報
- 従業者の住所や給与情報
- 取引先ごとの仕切り額の一覧表や取り引き実績
- 取引先から取り扱い注意と言われた情報



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。
→ セキュリティガイドラインやベンチマークも利用してみましょう。　GOOD!

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。早めに対処しましょう。

組織の業種と、職位に合わせて学習できる「情報セキュリティポイント学習ツール」※を利用し、「実施している」以外を選択した項目の対策方法について学びましょう。実施できていない項目に絞り込んだポイント学習で、100点を目指します。

効果測定や改善・見直しのための情報を参考にしてみましょう。　改善・見直し　効果測定

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を見直し、実施しやすい部分から対策の検討をしていきましょう。

対策・立案や効果測定のための情報を参考にしてみましょう。　効果測定　対策・立案

49点以下だった方
いつ情報流出等の事故が起きても
不思議ではありません。

わからなかった部分や点数が低かった項目を確認し、漏えい事故が発生する前に対策を施しましょう。

現状把握や対策・立案のための情報を参考にしてみましょう。　対策・立案　現状把握

GOOD!

全ての組織に必要な対策と、組織毎にそれぞれの特徴を考慮して実施すべき対策の2つに分けた「組織的な情報セキュリティ対策ガイドライン」も合わせてご覧ください。
http://www.ipa.go.jp/security/manager/know/sme-guide/

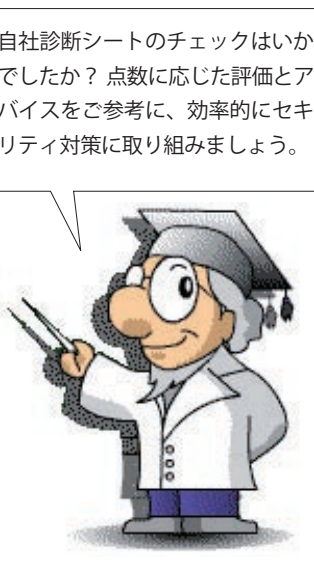
組織のプロフィールと情報セキュリティ対策の取り組み状況を入力することで、
現在の対策レベルがどこに位置しているかを確認することができるWebツール。
http://www.ipa.go.jp/security/benchmark/

改善・見直し　**http://www.ipa.go.jp/security/manager/know/tool/library.html#library_4**

効果測定　**http://www.ipa.go.jp/security/manager/know/tool/library.html#library_3**

対策・立案　**http://www.ipa.go.jp/security/manager/know/tool/library.html#library_2**

現状把握　**http://www.ipa.go.jp/security/manager/know/tool/library.html#library_1**



情報セキュリティポイント学習ツール
～事例で学ぶためのセキュリティ対策～

診断項目ごとに設定された、身近な危険を疑似体験することで、正しい対処法を学ぶことができます。
http://www.ipa.go.jp/security/vuln/5mins_point/


この自社診断シートは以下のような特徴を有する組織を対象としております。

- 情報システム責任者を置けないまたは兼任となる
- 経営資源が限られるため、対策経費はあまりかけられない

■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
- 複雑な設定を必要とするサーバやネットワーク機器を所有していない
  - ・電子メールやホームページはISPのサーバ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を所有していない
  - ・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、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PCを利用する際には、ISP等に直接接続するなどのように、個人所有PCは、職場のネットワークには接続しない
  - ・事業所が1箇所で専用線のWAN回線を持たないなどのように、インターネット以外には社内ネットワークへの接続部分がない