中小企業・小規模事業者の皆様へ

新 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

- ランサムウェア
- パスワードリスト攻撃
- 標的型攻撃メール

ＩＴ環境の変化

- クラウド
- タブレット
- 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シート」でチェック！

新 5分でできる！自社診断パンフレット

自社診断シートの２５問に回答してください

自社診断シートが手元に無い場合は
以下の URL からダウンロードしてください。

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

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。	点数が低かった項目について、「5 分でできる！情報セキュリティ自社診断パンフレット」の解説編を参考にして、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。

●100点満点から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**
https://security-shien.ipa.go.jp/

■ **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/

この自社診断シートで例示した対策の前提は以下のとおりです。

■ 経営者（代表者）が対策方針を直接指示・確認することができる　　■ 社員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
・自社のホームページはクラウドサービスを利用するなどのように、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

Part 1 基本的対策

No.1～5は企業の規模や形態を問わず、必ず対策していただきたい5項目です。いずれも一度やればよいものではなく、継続的な対策実施が欠かせないため、運用ルールとして社内に定着させる必要があります。

自社診断シート No.1 脆弱性対策

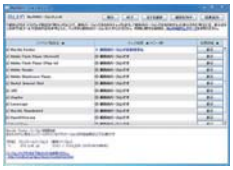
OSやソフトウェアは常に最新の状態にする

OSやソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。お使いのOSやソフトウェアに修正プログラムを適用する、もしくは最新版を利用しましょう。

対策例 Windows Updateを実施する(WindowsOSの場合)、Adobe Flash Player・Adobe Reader・Java実行環境などの利用中のソフトウェアを最新版にするなど。

情報セキュリティ対策に役立つツール

MyJVNバージョンチェッカ



パソコンにインストールされているソフトウェア製品（ウェブブラウザや動画再生ソフトなど）のバージョンが最新であるかを簡単な操作でチェックできるツールです。MicrosoftのWindows Updateと併せて、ソフトウェア製品のバージョンアップを行う習慣を身に付けましょう。

「MyJVNバージョンチェッカ」
http://jvndb.jvn.jp/apis/myjvn/

自社診断シート No.2 ウイルス対策

ウイルス対策ソフトを導入し適切に利用する

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル(パターンファイル)は常に最新の状態になるようにしましょう。

対策例 ウイルス定義ファイルが自動更新されるように設定する、統合型のセキュリティ対策ソフトの導入を検討するなど。

自社診断シート No.3 パスワード管理

強固なパスワードを使用する

パスワードが推測されたり、ひとつのウェブサービスから流出したID・パスワードが悪用されることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使い回さない」ようにして強化しましょう。

※単純なパスワード：自分の姓名や社名、辞書にある簡単な英単語など、第三者が推測しやすいパスワードを指します。

対策例 10文字以上の英数字記号を組み合わせる、名前・電話番号・誕生日などは使わない、複数のウェブサービスで同じパスワードを使い回さないなど。

自社診断シート No.4 機器の設定

共有設定を見直す

データ保管のためのファイルサーバーやオンラインストレージ、ネットワーク接続の複合機などの設定を間違ったため無関係な人に情報を覗き見られるトラブルが増えています。サーバーやネットワーク接続機器は必要な人にのみ共有されるよう設定しましょう。

対策例 クラウドサービスの共有範囲を限定する、ネットワーク接続機器の共有範囲を限定する、従業員の異動や退職時の設定変更を確実に実施するなど。

自社診断シート No.5 情報収集

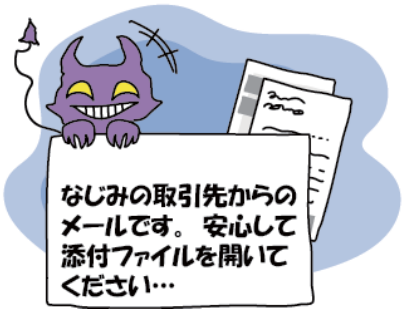
脅威や攻撃の手口を知り、対策に活かす

取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトに誘導してID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

対策例 IPAのウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る、利用中のインターネットバンキングなどが提供する注意喚起を確認するなど。

Part 2 従業員としての対策

No.6～18は従業員として留意すべき項目です。重要情報を日々扱っていると慣れによる人為的ミスが発生しやすくなります。また、脅威の形が日々変化しているので、油断しないように注意する必要があります。



自社診断シート No.6 電子メールのルール

身に覚えのない電子メールは疑ってみる

電子メールに添付されたファイルを開いたり、電子メール本文中に記載されたＵＲＬリンクをクリックしたりすることでウイルス感染する事故が続いています。身に覚えのない電子メールの添付ファイルやＵＲＬリンクへのアクセスに気をつけましょう。

対策例 不審な電子メールの添付ファイルを安易に開かない、ＵＲＬリンクに安易にアクセスしない、不審な電子メールの情報を社内に共有するなど。

自社診断シート No.7 電子メールのルール

宛先の送信ミスを防ぐ

電子メールやFAXの送り先を間違えて、全く知らない他人に情報が漏えいしてしまう事故が続いています。電子メールやFAXは送り先を十分確認するようにしましょう。また、電子メールアドレスを誤って他人に伝えてしまうことも情報漏えいになります。複数の送り先に送信する際には、送り先の指定方法を十分に確認するようにしましょう。

対策例 電子メールやFAXを送る前に送信先を再確認する、電子メールはTO,CC,BCCを使い分けて指定するなど。

自社診断シート No.8 電子メールのルール

重要情報を送信する時は保護する

重要情報を電子メールで送る場合は、電子メールの本文に書き込まず、文書ファイルなどに記載してパスワードで保護した後、メールに添付します。パスワードはその電子メールには書き込まず、電話等の別の手段で通知することが必要です。

対策例 重要情報は文書ファイルに書いてパスワードで保護する、パスワードは電話等の別手段で知らせるなど。

自社診断シート No.9 無線LANのルール

無線LANの盗聴や無断使用を防ぐ

適切なセキュリティ設定がされていない無線LANは、通信内容を読み取られたり、不正に接続されて犯罪行為に悪用されたりする被害を受ける可能性があります。無線LANの盗聴対策や無断使用を防止するようにセキュリティ設定をしましょう。

対策例 暗号化設定（WPA2-PSK）を利用する、パスフレーズは長くて推測されにくいものを使用するなど。

自社診断シート No.10 ウェブ利用のルール

インターネットを介したトラブルを防ぐ

悪意のあるウェブサイトやセキュリティ上の問題があるウェブサイトを閲覧することでウイルス感染する可能性があります。また、SNSや掲示板へ悪ふざけた投稿や秘密情報の意図せぬ掲載で会社に被害を及ぼすことがあります。業務でのインターネットの使用を制限する仕組みやルールにより、被害を防止することが必要です。

対策例 インターネットの利用ルールを作る、SNSの利用ルールを作る、Webフィルタリング機能を導入することでシステム的にインターネットの利用を制限するなど。

自社診断シート No.11 バックアップのルール

バックアップを励行する

故障や誤操作、ウイルス感染などにより、パソコンやサーバーの中に保存したデータが消えてしまうことがあります。このような不測の事態に備えて、バックアップを取得しておきましょう。

対策例 重要情報のバックアップを定期的に行う、バックアップは元の場所とは別に保存するなど。

自社診断シート No.12 保管のルール

重要情報の放置を禁止する

机の上に放置された情報は、誰かに持ち去られたり、盗み見られたりする危険にさらされています。関係者以外が見たり、触れたりすることができないように、重要情報は放置せず、管理する必要があります。保管場所を定め、作業に必要な場合のみ持ち出し、終了後に戻すことを励行するようにしましょう。

対策例 机の上をきれいにする、重要書類は鍵付き書庫に保管するなど。

自社診断シート No.13 持ち出しのルール

重要情報は安全な方法で持ち出す

重要情報を社外へ持ち出す場合、思わぬ盗難にあったり、うっかり紛失したりすることがあります。ノートパソコンやスマートフォンの利用にあたってパスワードの入力を求めるように設定したり、データファイルを暗号化するなどの対策を事前に行うことで、盗難や紛失の際に情報を簡単にみることができないようにしましょう。

対策例 重要情報の持ち出しは許可制にする、ノートパソコン・スマートフォン・USBメモリなどはパスワードロックをかける、荷物を放置させないなど。

自社診断シート No.14 事務所の安全管理

機器を勝手に操作させない

パソコンを使用した作業の途中でそのまま席を離れたり、パスワードなしでログインできるパソコンなど、誰でも操作できる状態のパソコンは、不正に使用される可能性があります。不正使用からパソコンを守るための対策を行いましょう。

対策例 離席時にコンピュータのロックをする、退社時にパソコンをシャットダウンし、他人がパソコンを使うことを防ぐなど。

自社診断シート No.15 事務所の安全管理

見知らぬ人には声をかける

関係者以外の事務所への立ち入りを制限しなければ、情報を盗み取られる危険性があります。特にサーバーや書庫・金庫など、重要な情報の保管場所の近くには無許可の人が近づけないようにしましょう。

対策例 事務所で見知らぬ人を見かけたら声をかける、受付を設置するなど。

自社診断シート No.16 事務所の安全管理

機器・備品の盗難防止対策を行う

ノートパソコンやタブレット端末、USBメモリなどは気軽に持ち運べる便利さがある反面、盗難の危険性も高くなっています。利用しない場合は、施錠可能な引き出し等に保管するなどの対策を講じましょう。

対策例 退社時に机の上のノートパソコンやタブレット端末、備品（CD、USBメモリ、外付けハードディスクなど）を引き出しにしまうなど。

自社診断シート No.17 事務所の安全管理

オフィスの戸締まりに気を配る

最終退出者と退出時間の記録を残すことは、最終退出者による施錠の責任意識を向上させることにも役立ちます。施錠と記録の管理をしましょう。

対策例 鍵の管理を徹底する、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。

自社診断シート No.18 情報の安全な処分

重要情報は復元できないように消去する

重要情報が記載された書類をゴミ箱にそのまま捨てると、関係者以外の目に触れてしまい、重大な漏えい事故を引き起こすことがあります。また、電子機器・電子媒体に保存された情報は、ファイル削除の操作をしても復元される恐れがあります。重要情報を廃棄する場合は、シュレッダーや消去用ソフトウェアを利用するなど、媒体ごとに適切な処分をしましょう。

対策例 消去ソフトを利用する、物理的に壊してから処分する、専門業者に消去を依頼するなど。

Part 3 組織としての対策

No.19～25は組織としての方針を定めた上で、実施すべき対策です。情報セキュリティのルールは明文化して社内で共有することにより、従業員の意識を高めるようにしましょう。

自社診断シート No.19 守秘義務の周知

従業員に守秘義務について理解してもらう

従業員が業務遂行上知りえた機密を守ることは就業規則などから当然のことと言えますが、そのことを暗黙にせず、明確に従業員に指示しましょう。

対策例 採用の際に守秘義務があることを知らせるなど。

自社診断シート No.20 従業員教育

従業員の定期的な教育を行う

日々の仕事では常に情報を取り扱いますが、日常的であるがゆえに管理の意識がつい疎かになりがちです。従業員に対し繰り返し意識付けを行うことが有効です。

対策例 情報管理の大切さを定期的に説明する、社内研修を開催するなど。

自社診断シート No.21 私物機器の利用

個人所有端末の業務での利用可否を決める

個人所有のパソコンやスマートフォンを業務で使用する場合、管理が行き届かず、セキュリティの確保が難しくなります。個人所有端末の業務利用の可否や業務利用のルールを定めましょう。

対策例 個人所有パソコン、スマートフォンの業務利用を許可制にする、業務利用する場合のルールを決めるなど。

自社診断シート No.22 取引先管理

取引先に秘密保持を要請する

取引先が情報の内容から判断して「当然秘密にしてくれるだろう」という一方的な期待は禁物です。取引先に機密情報を提供する場合には、それを機密として取り扱ってもらうことを明確にすることが必要です。

対策例 秘密保持の内容を明確にした契約書を作るなど。

自社診断シート No.23 外部サービスの利用

信頼できる外部サービスを使う

クラウドサービスなど外部サービスをコスト優先で選んでしまうと障害等でサービスが利用できなくなる場合もあります。事業継続性を大きく左右するような用途で外部サービスを利用する場合は、性能や信頼性、補償内容など十分に吟味しましょう。

対策例 利用規約や補償内容、セキュリティ対策などを確認して事業者を選ぶなど。

情報セキュリティ対策に役立つツール

映像で知る情報セキュリティ

情報セキュリティ上の様々な脅威と対策が学べる映像コンテンツです。10分前後のドラマやデモンストレーションを通じて情報セキュリティを学べます。
YouTube「IPAチャンネル」でも公開中です。組織内研修等でご利用ください。

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

自社診断シート No.24　事故への備え

事故発生に備えて事前に準備する

実際に事故が起きてからだと、それを冷静に考える余裕がなくなってしまいます。また、対応が後手に回り、それが原因でさらに深刻な事態になりがちです。報道される事故内容などを参考に「もし、同じことが自分の会社で起きたら・・・」を想定して、誰がいつ何をするのかをまとめておきましょう。

対策例　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。

自社診断シート No.25　ルールの整備

情報セキュリティ対策をルール化する

経営者が情報セキュリティ対策に関する方針を決めていたとしても、それを自社のルールとして明文化していなければ、従業員は都度経営者の指示を仰がなければなりません。従業員が自らルールに従って行動できるように、「企業としてのルール」をまとめて明文化し、従業員がいつでも見られるようにしておく必要があります。

対策例　情報セキュリティ対策として、診断シート項目のNo.1から24までをルール化して社内で共有する、一度決めたルールでも問題があれば改善するなど。

情報セキュリティ対策に役立つツール

対策のしおり

情報セキュリティ上の様々な脅威への対策をテーマ別にわかりやすく解説した小冊子シリーズです。IPAのホームページからダウンロード(PDF)もできます。

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

情報セキュリティ対策に役立つツール

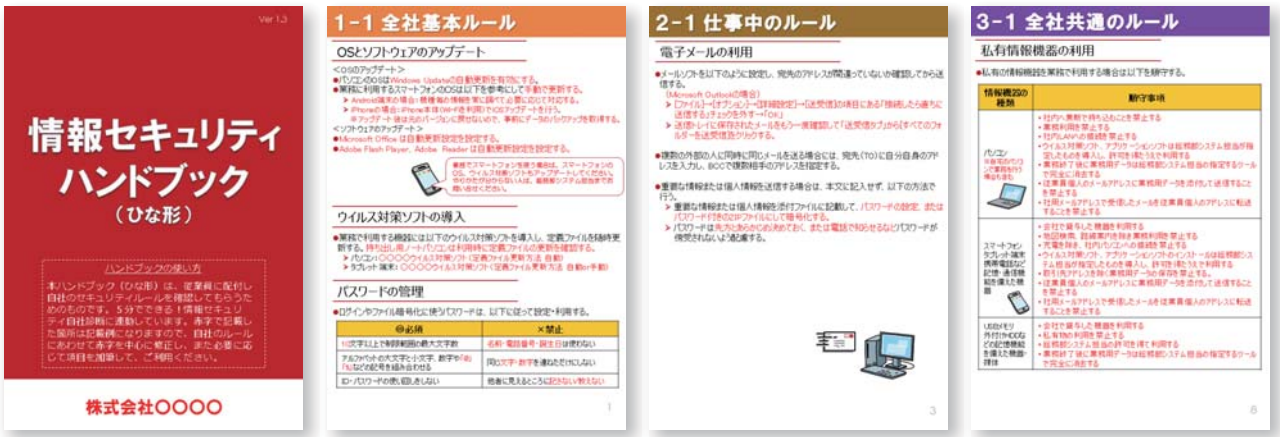
情報セキュリティ対策支援サイト

中小企業の情報セキュリティ対策を支援するポータルサイトです。対策構築や社内教育に使える資料を多数掲載しています。

情報セキュリティ対策支援サイト
https://security-shien.ipa.go.jp/

5分でできる！情報セキュリティ自社診断で改善点を把握したら 自社の情報セキュリティハンドブックを作成して社内ルールの周知に取り組みましょう！

中小企業の情報セキュリティ対策ガイドラインに付録する「情報セキュリティハンドブック（ひな形）」を自社のルールに合わせて編集し、全従業員に配付するなどして一人一人が実施すべき対策の周知に取り組んでください。自社診断で100点満点が取れるよう組織全体のレベルアップを図りましょう。



中小企業の情報セキュリティ対策ガイドライン　付録2「情報セキュリティハンドブック（ひな形）」
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

組織の大切な情報を
安全に守るために、各種情報をご活用ください。

セキュリティ対策に役立つ情報

情報セキュリティ対策支援サイト

中小企業の情報セキュリティ対策を支援するサイトです。社内の啓発・教育のサポートサイトと、情報セキュリティの普及啓発を行うセキュリティプレゼンター向けのサイトで構成されています。

https://security-shien.ipa.go.jp/

中小企業の情報セキュリティ対策ガイドライン

中小企業の情報セキュリティ対策として経営者層の役割と担当者が実施することを解説するとともにすぐに使えるひな形等を付録にまとめました。

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

組織の情報セキュリティ対策自己診断テスト　情報セキュリティ対策ベンチマーク

Web上の質問に答えると、診断結果が自動的に表示され、他社との比較もできます。

https://www.ipa.go.jp/security/benchmark/

情報セキュリティ　対策のしおり

一般のご家庭や企業(組織)内でパソコンを利用する方々を対象に、情報セキュリティ上の様々な脅威への対策を分かりやすく説明しています。下記のアドレスにアクセスしていただくとダウンロードすることができます。

https://www.ipa.go.jp/security/antivirus/shiori.html

映像で知る情報セキュリティ

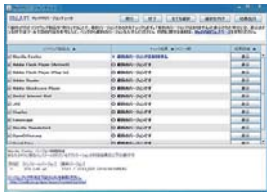
情報セキュリティ上の様々な脅威と対策をドラマなどを通じて学べる映像コンテンツです。社内研修などでご活用下さい。

https://www.ipa.go.jp/security/keihatsu/videos/

ＭｙＪＶＮバージョンチェッカ

利用者のPCにインストールされているソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツールです。

http://jvndb.jvn.jp/apis/myjvn/



情報セキュリティ安心相談窓口

IPAが国民に向けて開設している、ウイルスおよび不正アクセスに関する技術的なご相談を受け付ける窓口です。

https://www.ipa.go.jp/security/anshin/

IPA 独立行政法人 情報処理推進機構
セキュリティセンター

〒113-6591 東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコートセンターオフィス
TEL: 03-5978-7508　FAX: 03-5978-7546
E-mail：isec-info@ipa.go.jp　URL：https://www.ipa.go.jp/security/

2017.12.25 Version4.2