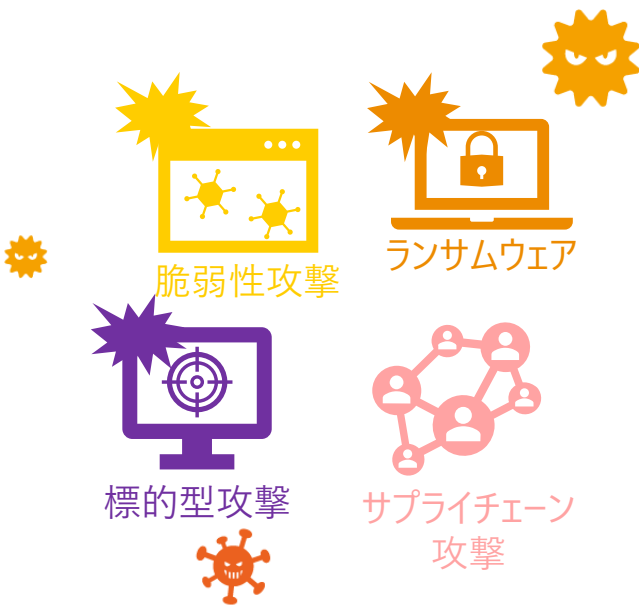
中小企業・小規模事業者の皆様へ

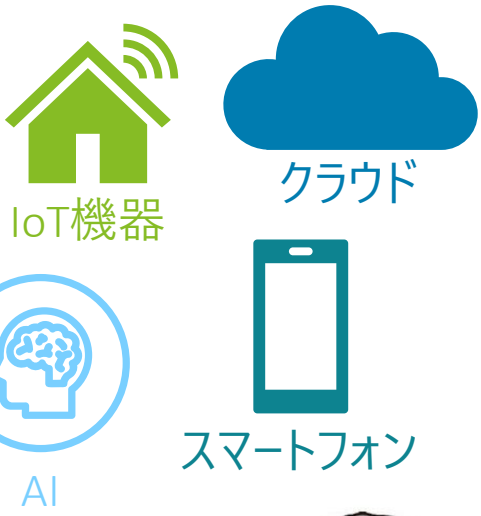
5分でできる！情報セキュリティ自社診断

最新動向への対応、できてますか？

脅威や攻撃の変化



IT環境の変化



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。

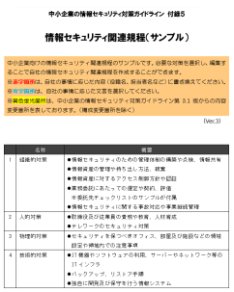
STEP1 できるところから始める

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

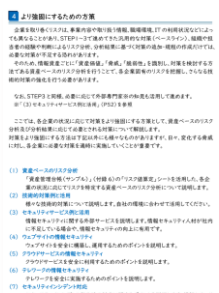
5分でできる!
情報セキュリティ自社診断

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
			点	点		マイナス(-) 点
					A+B+C 合計	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。

Part 1　基本的対策

脆弱性対策

No. 1 OSやソフトウェアは常に最新の状態にする

OSやソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、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やソフトウェアには、修正プログラムを適用する、または最新版を利用するようにしましょう。

対策例
- ☐ WindowsUpdate、（WindowsOSの場合）、ソフトウェア・アップデート（macOSの場合）などベンダの提供するサービスを実行する。
- ☐ Adobe Reader、ブラウザなど利用中のソフトウェアを最新版にする。
- ☐ 利用中のソフトウェアに脆弱性が存在しないか、MyJVNバージョンチェッカで確認する。
- ☐ 脆弱性が存在した場合は、手順に沿って修正パッチを適用する。
- ☐ サポートのあるOS、ソフトウェア、ネットワーク機器を利用する。

ウイルス対策

No. 2 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。
※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

対策例
- ☐ パソコン等の情報機器にウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状態にする。
- ☐ 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。
- ☐ OSやアプリケーションに標準搭載されているセキュリティ機能を有効活用する。

パスワード管理

No. 3 強固なパスワードを使用する

パスワードが推測や解析されたり、ウェブサービスから流出したID・パスワードが悪用されたりすることで、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。

対策例
- ☐ パスワードは10文字以上で「できるだけ長く」、大文字、小文字、数字、記号含めて「複雑に」、名前、電話番号、誕生日、簡単な英単語などは使わず、推測できないようにする。
- ☐ 同じID・パスワードを複数サービス間で使い回さない。
- ☐ 特にVPNや重要なシステムを利用する場合は、強固なパスワードを設定し、可能な場合は多段階認証、多要素認証、パスキーなどの認証強化機能を利用する。
- ☐ 初期設定パスワードを見直す。

機器の設定

No. 4 共有設定を見直す

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、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。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。

対策例
- ☐ ウェブサービス、ネットワーク接続の複合機・カメラ、ハードディスク（NAS）などの共有範囲を限定する。
- ☐ 従業員の異動や退職時には速やかに設定を変更（削除）する。
- ☐ 使用するパソコン等は他者と共有しない。共有せざるを得ない場合は、別途ユーザーアカウントを作成する。
- ☐ 外出先でフリーWi-Fiを使うときにはパソコンのファイル共有をオフにする。

バックアップ

No. 5 定期的にバックアップを取る

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たり、暗号化されたりしてしまうことがあります。事業が継続できるよう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。
- ☐ バックアップに使用する装置・媒体は、バックアップ時のみパソコンと接続する。
- ☐ バックアップの取得方法を決める。（オンラインバックアップの活用等）
- ☐ バックアップしたデータを安全な場所に保管する。
- ☐ バックアップしたデータを戻せるか定期的に確認する。

情報収集

No. 6 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を立ち上げたりして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取りましょう。

対策例
- ☐ IPAやNCO※などのセキュリティ専門機関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やウェブサービスなどが提供する注意喚起を確認する。
- ☐ 管理者が従業員に適宜注意喚起し、従業員はセキュリティの懸念は速やかに報告する。

※参考：IPA 情報セキュリティ関連サイト
※参考：NCO みんなで使おうサイバーセキュリティ・ポータルサイト

Part 2　従業員としての対策

電子メール

No. 7　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付けましょう。

対策例
- ☐ 不審な電子メールは安易に添付ファイルを開いたり、URLリンクにアクセスしない。
- ☐ 不審な電子メールの情報を社内で共有する。
- ☐ メールソフトに迷惑メール対策機能がある場合は有効にする。

電子メール

No. 8　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、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
- ☐ 電子メールのTO/CC/BCCの宛先を確認する。
- ☐ 電子メールやFAXを送る前に送信先を再確認する。
- ☐ メールソフトに宛先チェック、送信保留、取り消しなど誤送信防止機能がある場合は有効にする。

電子メール

No. 9　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、電子メール以外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強固なパスワードで保護する、パスワードはあらかじめ決めておくか、携帯電話のショートメッセージサービス（SMS）などの別手段で知らせる。
- ☐ 組織間で重要情報の送受信を行う場合は、盗聴やなりすましを防ぎ、改ざんの検知ができるS/MIME※などの暗号技術を利用する。
- ☐ 法人向けデータ転送サービスやウェブサービスを利用し、社内外の利用者のみがアクセス可能なフォルダで重要情報を受け渡しする。

※Secure/Multipurpose Internet Mail Extensions
電子メールの盗聴及び改ざんを防止する技術

無線LAN

No. 10　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
- ☐ 強固な暗号化方式（WPA3など）を選択する。
- ☐ パスワード（ネットワークセキュリティキー、パスフレーズ等）の初期設定が簡単なものである場合は、文字数を増やし、文字、数字、記号含め辞書にある英単語は使わず容易に推測されないようにする。
- ☐ モバイルルーターやスマートフォンのテザリング機能を使わないときにはオフにする。
- ☐ Wi-Fiルーター接続のためのパスワードや管理用パスワードを強固で推測されにくいものにする。
  - ✓ アクセスポイント（SSID）が正規のものであることを確認する。（偽アクセスポイントに接続しないよう注意する。）
  - ✓ パスワードなしで接続可能、またはパスワードが公開されている場合は秘密情報や個人情報のやりとりはしない。
  - ✓ 重要な情報をやりとりする場合は、HTTPS通信（TLS/SSL）※1に対応したウェブサイト、またはVPN※2通信を利用する。

※1　Transport Layer Security/Secure Socket Layer
インターネット上で通信を暗号化し、第三者による盗聴や改ざんを防ぐ技術

※2　Virtual Private Network 私設仮想回線
インターネットや公衆回線網を使っても、専用線接続と同じようなセキュリティを保つことができる技術

インターネット

No. 11　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した画像を投稿したり重要情報を勝手に掲載して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利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重要です。

対策例
- ☐ インターネットを利用する際の注意・制限をルール化する。
  - ✓ ウェブサイトを閲覧するときには運営者の身分証明書であるサーバー証明書を確認する。
  - ✓ SNSに重要情報や個人情報を記載しない。
- ☐ ブラウザのセキュリティ機能を活用する。
- ☐ Webフィルタリングやプロキシ・サーバーなど技術的対策を利用して、アクセスできるサイトを制限する。

Part 2　従業員としての対策

情報管理

No. 12 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取り出し、終了後に戻すことを励行するようにしましょう。

対策例
- □ 机の上をきれいにして、重要書類は鍵付き書庫に保管する。
- □ 自宅に重要情報または個人情報を含む書類やUSBメモリ、CD/DVDなどの電子媒体を保管する場合は、鍵付き引き出しやケースに保管し、利用時以外は施錠する。

情報管理

No. 13 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読み取られ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必要最小限にする。
- □ 重要情報の持ち出しは許可制にして記録する。
- □ 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。
- □ カフェやホテル、駅など公共の場所でテレワークを行うときにはパソコンや書類を放置しない。

情報管理

No. 14 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
- □ 書類は細断する。電子データは消去ソフトを利用する。
- □ 電子媒体を物理的に壊してから処分する。
- □ 専門サービスに書類の溶解、電子データの消去処分を委託して証明書を取得する。

事務所の安全管理

No. 15 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
- □ 離席時にパソコンにスクリーンロックをかける。
- □ 退社時にパソコンをシャットダウンする。
- □ 不特定多数の人がいる場所ではパソコンにのぞき見防止フィルタを取り付ける。

事務所の安全管理

No. 16 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侵入されてしまい、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断で立ち入りができないようにしましょう。
また、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。施錠と退出記録の管理をしましょう。

対策例
- □ 見知らぬ人は事務所に入れない。
- □ 受付カウンターを設置する。
- □ 出入口や重要な情報の保管場所に監視カメラを設置する。
- □ 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。

事務所の安全管理

No. 17 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、関連する備品などは手軽に持ち運べる便利さがある反面、盗難や紛失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、関連する備品などを引き出しにしまい、施錠する。
- □ ノートパソコンにセキュリティワイヤーを取り付ける。

Part 3　組織としての対策

ネットワーク管理

No. 18 外部から内部ネットワークへの不要な通信を遮断する

内部ネットワークに侵入された場合、悪用される恐れがあります。外部からだけではなく、内部から内部ネットワークおよび内部から外部ネットワークについても、不要と判断される通信は遮断しましょう。

対策例
- □ ネットワークに接続されている機器のファイアウォール機能が有効になっているか確認する。
- □ ネットワーク機器のファームウェアを最新の状態にする。
- □ ネットワーク機器の出荷時パスワードを変更する。

ウェブサイト管理

No. 19 ウェブサイトを安全に運用する

ウェブサイトに情報を公開する前に重要情報が含まれていないか確認しましょう。また、ウェブサイトで非公開情報や不要な古い情報が公開されていないか確認し、公開不要なページや古いファイルは削除しましょう。

対策例
- □ CMS※やECサイト構築ソフトなどのソフトウェアで作ったウェブサイトは脆弱性管理を行う。
- □ 自社のウェブサイトがHTTPS通信に対応しているか確認する。
- □ 開発工程やテスト環境などで使用した不要なアカウントは削除する。
- □ 公開ファイルに個人情報などの非公開情報が含まれていないことを確認する。
- □ 期間限定のページや不要になったウェブサイトは閉鎖する。

※Contents Management System　入力フォームを用いてページの作成、更新、管理などの作業を行えるように支援するシステムの総称

サイバーセキュリティお助け隊サービスの活用を！

「サイバーセキュリティお助け隊サービス」は、中小企業のサイバーセキュリティ対策に不可欠な各種サービスをワンパッケージで安価に提供するサービスです。

https://www.ipa.go.jp/security/otasuketai-pr/

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/videos/list.html

従業員教育

No. 20 従業員に情報セキュリティ教育を行う

日々の仕事では様々な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。従業員に対して繰り返し意識付けを行うことが有効です。

対策例
- □ 情報管理の大切さや関連する法令などを説明する。
- □ 重要情報を取り扱う場合は十分注意するよう説明する。
- □ 情報セキュリティ対策について、定期的およびインシデント発生時等の必要に応じた適時の研修の機会を設ける。
- □ 採用・退職の際に守秘義務について説明し、守秘に関する覚書を交わす。

私物機器の利用

No. 21 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
- □ 個人所有端末の業務利用を許可制にし、利用時のルールを決める。
- □ テレワークで個人所有端末やWi-Fiルーター、家庭のインターネット回線を利用する場合のルールを決める。

解説編

Part 3　組織としての対策

取引先管理

No. 22　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

- □ 秘密保持や具体的な対策を明記した契約や覚書を交わす。
- □ 情報セキュリティ対応方針を公表している取引先を選定し、情報セキュリティ対策の実施状況を確認する。
- □ 取引先が再委託を行う場合は、取引先と同等の秘密保持を要請する。

外部サービスの利用

No. 23　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っても、補償を受けられない場合もあります。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。
- □ パスワードなどの認証機能について適切に設定・管理を実施する。
- □ 「中小企業のためのクラウドサービス安全利用の手引き」（付録7）を活用し、クラウドサービスを安全に利用する。

事故への備え

No. 24　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、冷静に対応する余裕がなくなてしまいます。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。報道されるセキュリティ事故などを参考に「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し、従業員に周知する。
- □ テレワークでウイルス感染、パソコンや書類の紛失、盗難など事故が起きた場合の連絡先を決め、テレワーク勤務者に周知する。
- □ セキュリティ事故が発生した際に必要な確認ができるよう、相談先となるセキュリティベンダーを前もって決め、システムのログを取得しておく。
- □ 「中小企業のためのセキュリティインシデント対応の手引き」（付録8）を活用し、誰がいつ何をするのかをまとめる。

ルールの周知

No. 25　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、それを具体的な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。

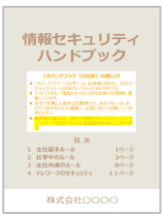
対策例

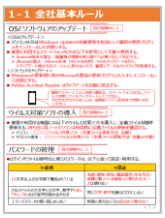
- □ 情報セキュリティ対策として、診断シート項目のNo.1から24までをルール化して社内で共有する。
- □ 一度決めたルールでも問題があれば改善する。
- □ 従業員に周知するための参考資料として「情報セキュリティハンドブック（ひな形）」（付録4）を活用し、ルールを文書化する。

参考情報

自社診断の後は 社内ルールの周知に取り組もう！

中小企業の情報セキュリティ対策ガイドライン付録の「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ひとり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。





情報セキュリティハンドブック（ひな形）
https://www.ipa.go.jp/security/guide/sme/about.html

情報セキュリティ対策の取り組みを 外部にアピールしよう！

「SECURITY　ACTION」は中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度です。「5分でできる！情報セキュリティ自社診断」を実施し、「情報セキュリティ基本方針」を定め、公開することで2段階目の「二つ星」を使用することができます。

Check!! 5分でできる！情報セキュリティ自社診断

Check!! 情報セキュリティポリシー（基本方針）

SECURITY ACTION ★★
セキュリティ対策自己宣言

SECURITY ACTION 二つ星
https://www.ipa.go.jp/security/security-action/

独立行政法人 情報処理推進機構

〒113-6591
東京都文京区本駒込2丁目28番8号 文京グリーンコートセンターオフィス
URL　https://www.ipa.go.jp/security/
電話　03-5978-7530
E-mail　isec-pr-cssp@ipa.go.jp