●サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う

・迅速に更新プログラムの適用をする
・仮想パッチを導入する
・提供元不明のソフトウェアを利用しない
・不要なサービスを停止、無効化する
・アクセス権限を最小化する
・管理者権限の運用体制を整える
・セキュリティ製品を導入する
・ネットワークを個別遮断できるようにし、ファイアウォールを設置するなどアクセスを制限する
・重要なデータファイルは暗号化する
・外部記憶媒体の接続を制限する

●適切なバックアップ運営を行う

・バックアップの取得方法や日時、間隔を検討する
・3-2-1ルール
　データはコピーして3つ持ち、2種類のメディアでバックアップを保管し、バックアップの1つは違う場所で保管する。

5分でできる自社診断の25項目

診断項目	診断内容	チェック 実施している	一部実施	実施していない	わからない
①基本的対策	パソコンやスマホなど情報機器の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
	パソコンやスマホ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は最新の状態にしていますか	4	2	0	−1
	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
	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	−1
	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
②従業員としての対策	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
	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
	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワード等で保護していますか	4	2	0	−1
	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
	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
	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか	4	2	0	−1
	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
	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策はしていますか	4	2	0	−1
	離席時にパソコン画面をのぞ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
	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
	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
	事務所が無人になるときの施錠忘れ対策を実施していますか	4	2	0	−1
	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
③組織としての対策	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか	4	2	0	−1
	従業員に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
	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
	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
	クラウドサービスやウェブサイトの運用等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
	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
	情報セキュリティ対策項目をルール化し、従業員に明示していますか	4	2	0	−1
合　計					点

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更なる対策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洩することもあります。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対策を検討してください。

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。対策支援サイトなどを参考にして、わからなかった部分や点数が低かった項目を確認し、至急、対策を施しましょう。

〈情報セキュリティ支援サイト〉

中小企業が情報セキュリティ対策を「はじめる」、さらには「強化していく」ことを支援するサイトです。

内容が更に充実！日本商工会議所「サイバー保険」をご紹介

昨今のサイバー攻撃の激化や攻撃手段の高度化等に鑑み、補償拡大や付帯サービスの充実化を図るため、現行制度である「情報漏えい賠償責任保険制度」の提供を終了し、2024年3月より新たな「サイバー保険制度」へ移行します。サイバーリスクやそれによる損害から会社を守るため、更にパワーアップした新保険「サイバー保険」についてご紹介します。

なお、既に旧保険に加入されている方について「サイバー保険制度」への移行手続き（継続手続き）は、取扱代理店もしくは　引受保険会社より順次ご連絡いたします。

保険の概要

外部からのサイバー攻撃（不正アクセスやウイルス感染等）や情報漏えい、またはそのおそれが生じた場合に、事業者が負う法律上の賠償責任・争訟費用の補償や、事故発生時の各種対応費用（事故調査から再発防止策策定までの費用など）を補償します。

サイバー攻撃等によるシステム停止によって営業が休止・阻害されて生じた喪失利益や営業継続費用も補償可能です。

ここがおすすめ

①不正アクセス等が発生した場合の事故原因調査・データ復旧など各種対応費用を手厚く補償
②商工会議所のスケールメリットと加入者ごとのセキュリティ状況を反映した割安な保険料水準
③IT業務を行う事業者向けのオプションとして、「IT業務特約」もご用意
④「標的型メール訓練サービス」やサイバー攻撃時に早期回復を支援するセキュリティソフト等をご提供可能

付帯サービス例

●リスク診断サービス

端末のセキュリティリスクを診断

●標的型メール訓練サービスの提供

従業員に対して標的型メールを想定したメールを送付し、メール内のURLのクリック状況等から標的型メールへの対応状況をレポートして報告。（引受保険会社によって詳細は異なります。）

●専用コールセンター

サイバーセキュリティに関するトラブルについて、電話でお気軽に相談できる窓口です。

事故例

●建設業

得意先からメールが届き、添付ファイルを開封したところ、従業員のパソコンがウイルスに感染。情報漏えいの発生は無かったが、原因調査に高額な費用が。

保証金額は？

感染したPCのフォレンジック調査費用：約200万円

●小売業

パッケージを活用して運営していたECサイトに外部からの不正アクセスを受け、約1000件の顧客クレジットカードが流出。

保証金額は？

〈賠償責任〉
個人情報漏えいについての賠償金：1000万円
〈各種対応費用〉
個人情報漏えいについての見舞金：1000万円
調査費用：800万円
ネットワーク復旧費用：200万円