付録

知っておくと役立つサイバーセキュリティに関する手引き・ガイダンス

本書の最後には、知っておくと役立つ手引きやガイダンスなどを紹介します。サイバー攻撃を受けた場合に相談できる公的機関の窓口、スキルアップしたい中小企業等のセキュリティ部門担当者に役立つ情報を解説します。

また、本章では、「一般利用者向け」、「中小企業等向け」と中心となる対象読者を表すタグを付しています。

付録01 セキュリティ担当者は知っておきたい「サイバーセキュリティ関係法令Q&Aハンドブック」とは 中小企業等向け
付録02 サイバー攻撃を受けた場合①～情報関係機関への相談や届け出 一般利用者向け 中小企業等向け
付録03 サイバー攻撃を受けた場合②～警察機関への相談や届け出 中小企業等向け
付録04 IPAが取り組むさまざまな中小企業向けセキュリティ対策支援 中小企業等向け
付録05 IPAのより深いセキュリティ設定資料 中小企業等向け
付録06 セキュリティ系業務のアウトソース 中小企業等向け
付録07 中小企業がもっとクラウドサービスを利用しやすく！～認定情報処理支援機関（スマートSMEサポーター） 中小企業等向け
付録08 セキュリティの資格取得を目指そう 一般利用者向け 中小企業等向け
付録09 セキュリティスキルを向上させるには～「CYDER」と「CTF」 中小企業等向け

付録01 セキュリティ担当者は知っておきたい「サイバーセキュリティ関係法令Q&Aハンドブック」とは

中小企業等向け

インターネットが普及した現代、あらゆる事業、ビジネスを進めるにあたって、インターネットやサイバーセキュリティにまつわる法令、それに基づく対応は必須です。

一方で、企業が気を付けるべきセキュリティにまつわる関連法令は範囲が広いため、担当者は対応に四苦八苦しているのではないでしょうか。

そのような悩みを解決する一助として、内閣官房内閣サイバーセキュリティセンター(NISC)は「サイバーセキュリティ関係法令 Q&A ハンドブック」を公開しています。

サイバーセキュリティ関係法令Q&A ハンドブック Ver2.0(令和 5 年(2023 年)9 月公開)

本ハンドブックは、全体を通じて、次の 3 つの特徴を持ちます。

①サイバーセキュリティ基本法を筆頭に、サイバーセキュリティに関連すると思われる法令を広範に網羅していること

②対象とした法令は、ハードローだけではなくソフトロー(法的な拘束力はないが事実上、社会的規範として使用されるもの)と呼ばれるガイドラインや技術標準を参考に、可能な限り最新版を参照していること

③法令の紹介に加えて、より実際(現場)に即した解説をしていること

これらの特徴のもと、サイバーセキュリティ対策において参照すべき関係法令を、実例をふまえながらQ&A形式で解説しています。

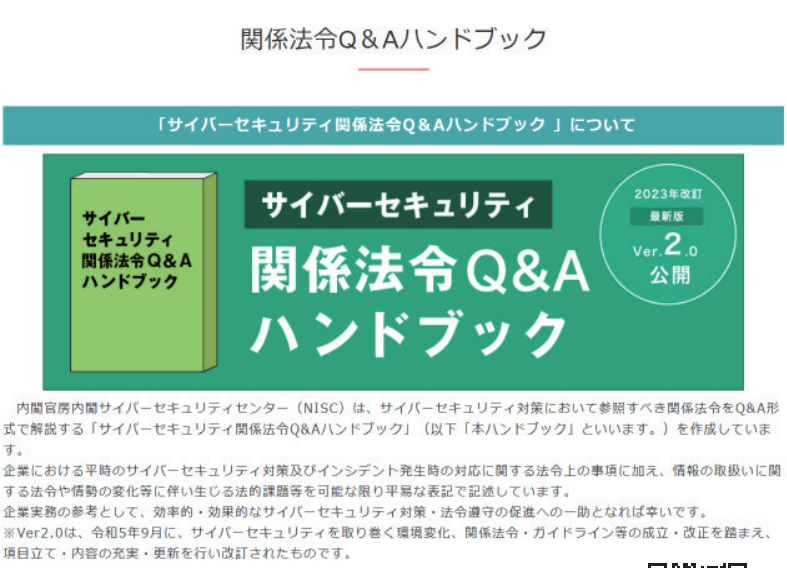
例えば、契約関連(電子署名、システム開発、クラウド等)の法令や、クラウドサービス、モバイル・IoT機器の活用、それらを含めたテレワークなどのコロナ禍により普及しよく見かけるようになったシーンに関係する法令、個人情報保護法、不正競争防止法など、網羅的に扱っています。

また、Q&A方式でサイバーセキュリティ対策やトラブルの対応手順も解説されているため、法律の専門家ではない情報システム部門担当者・セキュリティ担当者でも、実際にトラブルや想定外の出来事に遭遇した際、参考になります。

加えて、現場を任されている企業のセキュリティ担当者だけでなく、自社のデータ、情報資産を守る必要のある経営者にとっても、例えば、インシデント対応に関する法令の概要を把握し、これに則った適切な経営判断を行うこと等に役立つ内容のため、関係者はぜひ一読しておくことをおすすめします。(なお、インシデント被害発生時の対応については、被害に係る情報のうち、どのような情報を、どのタイミングで、どのような主体と共有すればよいか、実務上の参考として作成された「サイバー攻撃被害に係る情報の共有・公表ガイダンス」もあります。

本ハンドブックを理解することで、企業実務として効率的・効果的なサイバーセキュリティ対策・法令遵守が促進されることはもちろん、自社・自組織におけるサイバーセキュリティの堅牢性が高まることが期待されます。

企業のセキュリティ部門担当者なら知っておきたい情報が充実



サイバー攻撃被害に係る情報の共有・公表ガイダンス
https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html

関係法令 Q & A ハンドブック 配布ページ
https://security-portal.nisc.go.jp/guidance/law_handbook.html#/

付録02 サイバー攻撃を受けた場合①〜情報関係機関への相談や届け出

一般利用者向け　中小企業等向け

第４章５(P.96)ではサイバー攻撃を受けた場合の対処を説明しました。

では会社や団体として、相談したり必要に応じて届け出を行うものとしてはどのようなことを知っておくとよいのでしょうか。

まず、とりあえずサイバー攻撃を受けたらどこに相談したらいいのか。

代表的なものとして一般利用者向けには、IPAによる「情報セキュリティ安心相談窓口」があります。

同名のウェブサイトを検索すると、「良くある質問」や、過去のサイバーセキュリティに関するレポートなどが掲示されているので、一通り目を通し、それでも解決しない場合は、電話やメールで問合せしてみるとよいでしょう。

企業組織向けには「サイバーセキュリティ相談窓口」があります。

各種インシデント発生時の初動対応に関する相談や、標的型サイバー攻撃に関する相談、その他の情報セキュリティに関する一般的な相談が可能です。

それとは別に、義務ではありませんが、「ウイルスの届け出」、「不正アクセスの届け出」を受け付けているので、可能であれば届け出ましょう。

そうすることで他の人が攻撃に遭うのを避けることが可能になります。

地域の商工会議所がサイバー攻撃対応支援サービスの一環として、有料の相談窓口を設けている場合もあります。

情報セキュリティ10大脅威

https://www.ipa.go.jp/security/vuln/10threats.html
※脆弱性対策(IPA公開資料一覧ページ)https://www.ipa.go.jp/security/vuln/index.html

ランサムウェア対策特設ページ

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

IPA情報セキュリティ安心相談窓口(個人向け)

URL	https://www.ipa.go.jp/security/anshin/about.html
電話での相談	03-5978-7509 (受付時間 10:00～12:00、13:30～17:00、土日祝日・年末年始は除く)
メールでの相談	anshin@ipa.go.jp
FAXでの相談	03-5978-7518
郵送での相談	〒113-6591 東京都文京区本駒込2-28-8 文京グリーンコート センターオフィス18階 IPAセキュリティセンター 安心相談窓口

IPAサイバーセキュリティ相談窓口(企業組織向け)

URL	https://www.ipa.go.jp/security/support/soudan.html
メールでの相談	cs-support@ipa.go.jp

なお業種によって、例えば医療機関でのサイバー攻撃に関しては、厚生労働省が、医政局特定医薬品開発支援・医療情報担当参事官室で連絡を受け付けています。

また、IPAでは、その年のサイバーセキュリティ上の懸念される脅威を「情報セキュリティ10大脅威」として公開しています。

個人編と組織編に分けて公表されており、脅威の内容に加えて、参考事例や注意するポイントがまとまった内容となっています。

さらに、組織を狙った脅威として急激に増えているランサムウェアに関しては、「ランサムウェア対策特設ページ」が用意されています。

万が一、企業や組織でランサムウェアの被害に遭った場合、まずここのページをご覧いただき、迅速かつ正確な対応を進めていきましょう。

IPA 安心相談窓口で対応出来ない例

なお、IPA 安心相談窓口では、下記のような相談は受け付けていません。

- 直接来訪しての相談や面談
- 法的解釈に関する相談
- 電磁波や電波に関する不安・苦情
- インターネットサービスの品質や役務不履行に関する相談
- 契約・支払い方法に関する相談
- 個別の依頼に基づく端末やログの調査、マルウェアの解析、その他調査行為全般の依頼
- 特定の製品やサービスの紹介またはそれらに対する良否の質問
- 他組織への連絡や通報などの仲介
- 犯罪者の検挙、事件捜査の要望

一方、IPA ではなく他の機関が開設している窓口で対応出来る場合もあります。それぞれの窓口の受け付ける事柄を、ウェブサイトなどでよく確認してご相談ください。

●サービス提供または購入などの契約に関するトラブルで困っている場合
消費者ホットライン（消費者庁）
https://www.caa.go.jp/policies/policy/local_cooperation/local_consumer_administration/hotline/

●国民生活センター
https://www.kokusen.go.jp/

●法的トラブルの相談をしたい場合
法テラス
https://www.houterasu.or.jp/

●インターネット上での違法・有害情報に関し相談したい場合
違法・有害情報相談センター
https://ihaho.jp/

●不正コピーや違法アップロードを見かけた場合
社団法人 コンピュータソフトウェア著作権協会不正コピー情報受付
https://www2.accsjp.or.jp/piracy/

●インターネット上の違法情報を通報したい場合
インターネット・ホットラインセンター
https://www.internethotline.jp/

●迷惑メールの受信に関して困っている場合
財団法人 日本データ通信協会迷惑メール相談センター
https://www.dekyo.or.jp/soudan/ihan/

●インターネットに繋がらないなどのトラブルで困っている場合
利用プロバイダまたはパソコンのメーカー・購入店の各サポート窓口

IPA「他の機関が開設している相談窓口等」より
https://www.ipa.go.jp/security/anshin/external.html

付録03 サイバー攻撃を受けた場合②～警察機関への相談や届け出 中小企業等向け

警察庁では、サイバー事案に関す通報、相談及び情報提供の全国統一オンライン受付窓口を設置しています。

この窓口からはサイバー事案に関する

〇通報(都道府県警察に対し、サイバー事案に関する通報を行うもの。)
※被害に遭った具体的な事実の通知を伴う場合

〇相談(都道府県警察に対し、サイバー事案に関するアドバイスを求めるもの。)

〇情報提供(都道府県警察に対し、サイバー事案に関する情報を提供するもの。)

を行うことができます。

下記リンクでは、「よくある相談事例と対応方法」についても紹介しています。

通報・相談をする前に解決できる内容があるかもしれませんので、ご参考にしてください。

爆破予告、殺人予告、自殺予告等の人命に関わる事案は最寄りの警察署に通報(緊急を要するものは１１０番)してください。

また、被害届を出される場合は、最寄りの警察署等に連絡をお願いします。

サイバー事案に関する相談窓口	https://www.npa.go.jp/bureau/cyber/soudan.html

付録04 IPAが取り組むさまざまな中小企業向けセキュリティ対策支援 中小企業等向け

1 中小企業の情報セキュリティ対策ガイドライン

IPA（独立行政法人情報処理推進機構）は誰もがITの恩恵を享受できるIT社会の実現を目指して、サイバーセキュリティ対策など各種の取組みを行っている経済産業省所管の政策実施機関です。

そのIPAが発行している「中小企業の情報セキュリティ対策ガイドライン」（以下「対策ガイドライン」）は、ITを何らかの形で経営に活用している中小企業であれば、必ず参照しておくべき指針です。

この対策ガイドラインは、中小企業の経営者に対し、対策の必要性に気づいてもらい、サイバーセキュリティ対策に全く取り組んでいない状態から、徐々にステップアップし、しっかりとした社内ルールと体制を作って組織的なサイバーセキュリティのマネジメント体制を構築する道筋を提供することを目的に編集されています。

ウェブサイトにおいてPDFの電子ファイル版で無償配布されている他、印刷版も有償で提供されています。

この対策ガイドラインの構成は、大きく本編と付録に分かれ、さらに本編は、第1部の「経営者編」と第2部の「実践編」で構成されています。

「経営者編」では、経営者がサイバーセキュリティの必要性を認識し、自らの責任で考え、実行しなければならない事項について説明されています。

対策を怠ることで企業が被る不利益や、経営者などが問われる法的な責任、社会的な責任などが、事例や主な関係法令の条項と処罰とともに説明されています。

そして経営者が認識しておかなければならない「3原則」と、経営者自ら、または従業員に指示して実行しなければならない「重要7項目の取組」が記述されています。

「実践編」では、具体的にどのように対策を進めていくかについて記述されています。

規模の小さな会社や、これまで十

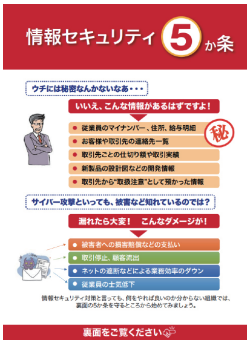
「中小企業の情報セキュリティ対策ガイドライン」とその付録

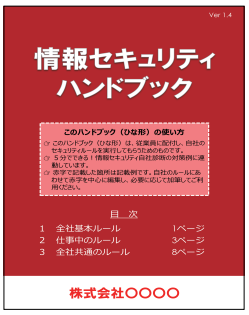
「中小企業のセキュリティ対策ガイドライン」には本編と、各企業が取り組まなければいけないチェック項目や、自社のセキュリティ資料を作るためのひな型、そしてクラウドの安全利用のための手引きが含まれます。

中段左から「情報セキュリティ対策5か条チラシ」、中段中「情報セキュリティ基本方針」のサンプル、中段右「5分でできる自社診断」、下段左「情報セキュリティハンドブック」のひな型、下段中「情報セキュリティ関連規程」のサンプル、そして下段左が「中小企業のためのクラウドサービス安全利用の手引き」となっています。

ひな形やサンプルは、文章中の項目を自社の組織や社員名に書き換えればすぐに使えるよう、作られています。

この他にやや専門的になりますが、EXCEL形式の「リスク分析シート」があります。





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/index.html

分なサイバーセキュリティ対策を実施してこなかった企業などでも、すぐにできることから開始して、ステップバイステップで、企業それぞれの事情に適した対策が実施できるように、進め方を説明しています。

中でも「情報セキュリティ5か条」は、対策ガイドライン実践編の冒頭で紹介しています。

この5か条は、まず取り組んでいただきたい基本的な対策を最小限にまとめられたものです。ぜひここから対策をスタートしてください。

こののち、実践編では、現状を知り改善するステップ、本格的に取り組むステップについて解説しています。

それぞれのステップは、中小企業の実態やサイバーセキュリティ対策のありかたを熟知している有識者により検討された内容となっています。

「付録」は実践編に取り組む際に使用するひな型やシート類です。構成は以下のとおりです。

- 情報セキュリティ対策5か条チラシ
- 情報セキュリティ基本方針(サンプル)
- 5分でできる自社診断
- 情報セキュリティハンドブック(ひな型)
- 情報セキュリティ関連規程(サンプル)
- 中小企業のためのクラウドサービス安全利用の手引き
- リスク分析シート
- 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

これらのうち、「5分でできる自社診断」は、25問のチェック項目に回答することで自社の対策状況を把握することが出来るというものです。

「基本的対策」、「従業員としての対策」及び「組織としての対策」という構成になっており、「基本的対策」は前述の「情報セキュリティ5か条」と同じになっています。

これに加え、「従業員としての対策」では、電子メール利用時や情報を格納した機器などの持ち出し、管理、バックアップなどの13項目、「組織としての対策」では、従業員教育や、取引先との契約時の秘密保持、

5分でできる自社診断の25項目

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
	2	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※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	重要情報※2 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
	5	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	6	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
	7	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
	8	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などで保護していますか？	4	2	0	−1
	9	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
	10	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
	11	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
	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	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
	15	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
	16	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
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	−1
	18	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
Part 3 組織としての対策	19	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
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	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
	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 ものの合計点	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機密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。

3

付録「5分でできる自社診断」の中にある、診断のための25項目。それぞれの項目に答えることで自社のセキュリティレベルが診断できます。

先々どういったセキュリティ項目を満たしていかないといけないか、というビジョンを持つためには目を通しておくとよいでしょう。

情報セキュリティ対策支援サイトでもオンラインで診断ができます。
https://security-shien.ipa.go.jp/learning/

緊急時の体制整備、ルール化など7項目が設けられています。

これら25項目により、サイバーセキュリティ対策の実施状況を点数化し100点満点でどの程度の達成状況か、また、どのような項目が弱点かを測ることができ、対策に取り組むうえでのポイントを見える化することが出来ます。

同じく、付録に収められている「情報セキュリティ基本方針」や「情報セキュリティ関連規程」のサンプルは、それぞれ、自社の状況や方針に沿って記述を選択、あるいは書き換えることで自社固有のものに仕上げることが可能です。

また、「情報セキュリティハンドブック」(ひな型)は、社内ルールに合わせて書き換えができますので、従業員ひとりひとりへのルール徹底に役立ちます。

2 サイバーセキュリティ対策自己宣言「SECURITY ACTION」

「SECURITY ACTION(セキュリティアクション)」制度は、中小企業がサイバーセキュリティ対策に自発的に取り組むことを社の内外に宣言する制度です。

IPAの他、商工団体、中小企業に関係する士業団体などが連携して創設し、IPAが運用を行っています。

サイバーセキュリティ対策を始めたくても「なにをすればよいかわからない」、「経営者が重要性を認識してくれない」という中小企業の実態(IPAが実施した実態調査より)を踏まえ、まず何をすべきか、よりよくするために何をすべきか、ということを示し、実際に取り組んでいることを中小企業に自己宣言してもらおう、というのがこの制度の趣旨です。

SECURITY ACTIONは、現在「一つ星」と「二つ星」の2段階があります。

一つ星は「情報セキュリティ対策5か条」に取組むことを宣言するもの、二つ星は、「5分でできる自社診断」で自社の状況を把握するとともにサイバーセキュリティ基本方針を定めてウェブサイト上などで外部に示したことを宣言するものです。

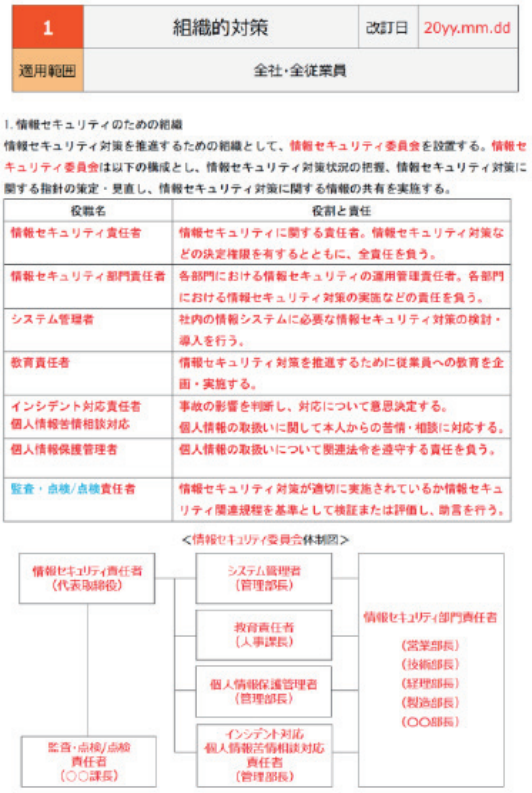
これらは、「中小企業向け情報セキュリティ対策ガイドライン」と同調しています。

この宣言をすることにより、社内意識の醸成、また、社外からは取組みを評価され、信頼の獲得と向上につながるなどの効果が期待できます。

まずはじめる、その一歩としてSECURITY ACTIONを宣言してはいかがでしょうか？

(執筆：IPA)

情報セキュリティ関連規程のサンプル



1	組織的対策	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

1. 情報セキュリティのための組織

情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。
インシデント対応責任者 個人情報苦情相談対応	事故の影響を判断し、対応について意思決定する。 個人情報の取扱いに関して本人からの苦情・相談に対応する。
個人情報保護管理者	個人情報の取扱いについて関連法令を遵守する責任を負う。
監査・点検/点検責任者	情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う。

<情報セキュリティ委員会体制図>

付録「情報セキュリティ関連規程」のサンプルの中の「組織内対策」のページ。

用意されたサンプルの中の赤字の部分を自社の情報に書き換えていくことで、自社の「情報セキュリティ関連規程」が完成するようになっています。

関連規程といってもなにを盛り込んでよいかわからないといったことが、このサンプルをなぞることで解決されます。

ウェブサイトに掲載するSECURITY ACTIONのマーク

セキュリティ対策自己宣言

セキュリティ対策自己宣言

SECURITY ACTIONの条件を満たした上で、これらのマークをウェブサイトに掲載することで、外部の企業などに対して自社のサイバーセキュリティに対する取り組みの「本気度」を示すことができます。

3 サイバーセキュリティお助け隊サービス

前述したガイドライン、「SECURITY ACTION」の内容を読めばセキュリティ対策の知識を深めることはできますが、実際にサイバー攻撃を防ぐための対策を講じると、費用面でも時間面でもコストがかかります。

人材・体制・資金などのリソースが限られている多くの中小企業にとって、通常業務をこなしながらセキュリティ対策を講じるための負担は少なくありません。

そんな中小企業の負担を軽減するためにも、IPAでは「サイバーセキュリティお助け隊サービス」を2021年度から運用しています。

IPAは2019年度、2020年度の時点から、中小企業への攻撃実態把握や中小企業向けのサイバーセキュリティ対策支援のしくみを構築するため、「サイバーセキュリティお助け隊実証事業」を実施し、この事業で得られた知見をもとに中小企業にとって不可欠なセキュリティサービスを示す「サイバーセキュリティお助け隊サービス基準」を制定しました。

そしてこのサービス基準を充足する民間サービスには「サイバーセキュリティお助け隊マーク」を付与し普及を促進することで、多くの中小企業へ無理なくサイバーセキュリティ対策を導入・運用することを支援しています。

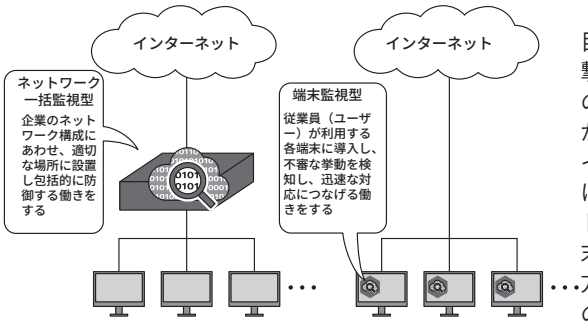
2025年2月時点で、「サイバーセキュリティお助け隊サービス」ではサービス基準を満たす58のセキュリティサービスが提供されています。サービスの具体的内容は、

- 中小企業のサイバーセキュリティ対策を支援するための相談窓口
- UTM（Unified Threat Management・統合脅威管理）などのネットワークセキュリティ監視装置を用いたユーザーのネットワーク通信の異常を一括監視、またはEDR（Endpoint Detection and Response）などエンドポイントセキュリティソフトウェアを用いたユーザーの端末の異常を監視（両方が提供されるサービスもあり）
- サイバー攻撃発生時の初動対応（駆付け支援など）
- 被害に遭った際に備える簡易サイバー保険

などがあり、中小企業がサイバー攻撃への対処として不可欠なサービスを効果的、網羅的にカバーし、かつ安価に提供しています。

企業経営において省くことはできないセキュリティ対策に悩んでいる中小企業にとって、効果的なセキュリティサービスをワンパッケージで利用できるようになっています。

「サイバーセキュリティお助け隊サービス」における異常監視のしくみ

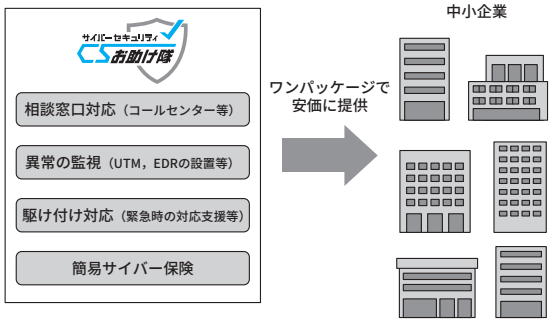


セキュリティ対策では、目に見えないサイバー攻撃を可視化し、侵入などの異常に早く気付くことがもっとも大切です。サイバーセキュリティお助け隊サービスでは、ネットワーク一括監視型、端末監視型、またはその両方（併用型）による異常の監視を提供しています。

「サイバーセキュリティお助け隊サービス」案内ページ

ユーザー向けサイト	https://www.ipa.go.jp/security/otasuketai-pr/
IPA案内ページ	https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html

「サイバーセキュリティお助け隊サービス」で提供するサービス内容



中小企業がサイバー攻撃への対処として不可欠なサービスを効果的、網羅的にカバーし、かつ安価に提供しています。

付録05 IPAのより深いセキュリティ設定資料 中小企業等向け

ITの特徴は、多くの人の目的に合致するように柔軟に作られていることで、機器であれソフトであれ多くの設定項目が用意されており、それを調整することでより自分の目的に適した使い方が可能になります。

基本的には標準設定のままでも十分使えるようになっていますが、まずはそのままで生産性を上げることを目指すのが大事です。

しかし、将来的にもっとセキュリティ性を高めて安全に使いたいと思う時期がやってきます。

そうしたときにはIPA(独立行政法人情報処理推進機構)のウェブサイトに紹介されているマニュアルなどが参考になります。

「情報漏えいを防ぐためのモバイルデバイス等各種設定マニュアル」では、一般従業員層にもできれば最低限知っておいてほしい暗号化の必要性や仕組み、情報漏えい対策として機能させるために必要なことなどを、平易な表現でまとめています。

「TLS暗号設定ガイドライン」ではウェブサイトを作成し公開するときに、適切な暗号化通信の運用について解説しています。

「IT製品の調達におけるセキュリティ要件リスト活用ガイドブック」では、経済産業省が公開している「IT製品の調達におけるセキュリティ要件リスト」に対し、これを実際にどのように活用するかの辞書的な役割を担うものです。

「IT製品の調達におけるセキュリティ要件リスト」は「国際標準ISO/IEC 15408に基づくセキュリティ要件」に適合することが認証されたセキュリティ製品のリストで、それをどう活用するかが解説されています。

いずれも、本書に書かれているセキュリティ知識を習得した上で、次のステップに進む手引きとなる資料です。

情報漏えいを防ぐためのモバイルデバイス等各種設定マニュアル
https://www.ipa.go.jp/security/ipg/documents/dev_setting_crypt.html
TLS暗号設定ガイドライン～安全なウェブサイトのために(暗号設定対策編)～
https://www.ipa.go.jp/security/crypto/guideline/ssl_crypt_config.html
IT製品の調達におけるセキュリティ要件リスト活用ガイドブック
https://www.ipa.go.jp/security/it-product/guidebook.html

付録06 セキュリティ系業務のアウトソース 中小企業等向け

中小企業等のみなさんがより責任ある立場になっていくためには、本格的にサイバーセキュリティに取り組む必要があります。

ただし、中小企業等にとって、それらを自ら習得するのは困難です。

そういった状況で、インターネットの特性を生かし、専門の企業にアウトソースすることで、堅牢性を担保するのも1つの手でしょう。

しかし、みなさんにとっては「どういった企業が信頼できるのか」というところからのスタートになると思いますので、そういったシーンに向けて、経済産業省とIPAでは「情報セキュリティサービス基準適合サービスリスト」を公開しています。

つまり、一定の基準を満たしたセキュリティ系企業のリストを公開しています。

リスクアセスメントを行う「情報セキュリティ監査」、ウェブサイトやシステムの弱点を見つける「脆弱性診断」、被害に遭ったときの鑑識的業務を行う「デジタルフォレンジック」、そして日々の問題無く業務を行えるか常にチェックをする「セキュリティ監視・運用」、IoT機器等の機器検証、脆弱性診断を行う「機器検証」の、それぞれのリストがあります。

情報セキュリティサービス基準適合サービスリスト(IPA)
https://www.ipa.go.jp/security/service_list.html
情報セキュリティサービス審査登録制度(経済産業省)
http://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html
情報セキュリティサービス基準(経済産業省)
https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun4.pdf

付録07 中小企業がもっとクラウドサービスを利用しやすく！～認定情報処理支援機関（スマートSMEサポーター）

中小企業等向け

認定情報処理支援機関（スマートSMEサポーター）とは、経済産業省の外局である中小企業庁が運営する、中小企業のIT活用を支援するITベンダーなどを中小企業等経営強化法に基づいて「情報処理支援機関」として認定する制度です。

近年、IT技術の進展や通信回線の高速化によって、サーバーなどの設備を持たなくてもソフトウェアの利用が可能なクラウドサービスの提供が増えてきました。

クラウドサービスは、設備やソフトウェアを購入する必要が無いため、初期導入コストが低く、しかも経営指導の専門家などとも情報共有がしやすく、クラウドサービス同士を組み合わせて活用することができるなど、中小企業にとっても数々のメリットがあります。

一方で、セキュリティ実装状況や保存したデータの取扱い条件などに関する情報提供が、クラウドサービスを提供するITベンダーによって異なり、中小企業にとっては分かりにくい部分がありました。

中小企業庁では、専門家との検討により、①クラウドサービスの安全・信頼性に関する情報、②セキュリティ対策状況、③利用者のサポート体制、④利用終了時のデータの取扱い、などの確認すべき項目を定めて、スマートSMEサポーターの認定申請時にITベンダーから申告させ、認定後には中小企業庁が特設サイトにて公開しています。

上記の項目の詳しい確認方法については、IPAが「中小企業のためのクラウドサービス安全利用の手引き」で解説していますので、参照下さい。

その他、同じくIPAが提供する「中小企業の情報セキュリティ対策ガイドライン」、「SECURITY ACTION セキュリティ対策自己宣言」や経済産業省が提供する「中小企業のサイバーセキュリティ対策」も参考になります。

便利なITツールでも、利用者がデータを取り出せなかったり、セキュリティ対策がおろそかでは、安心して使い続けることができません。

スマートSMEサポーターとして公開されている情報を参考にして、クラウドサービスなどの中小企業にとって生産性向上に役立ち安全・安心に使えるITツールを上手に選んで活用しましょう。

情報処理支援機関検索

情報処理支援機関として認定された、みなさんの生産性を高めるITツールを提供するITベンダーが検索出来ます。

本書ではコンテンツを作る業種を例に挙げましたが、この検索を用いることで、業種別、サービス別、そして地域別に、必要としているベンダーの情報を得ることが出来ます。

例えば、「東京都」で「飲食・サービス」業で、「予約」システムを提供してくれる会社を知りたい、というように検索します。

Smart SME Supporter 情報処理支援機関検索（中小企業庁）
https://www.smartsme.go.jp/SSS_SearchPage

付録08 セキュリティの資格取得を目指そう

一般利用者向け　中小企業等向け

セキュリティについて深く知りたい、もっと詳しく学びたいと考えているのであれば、オススメしたいのが資格の取得を目指した勉強です。

すでにセキュリティ関連の資格は数多く存在していて、自分自身のレベルや目的に合わせて選択できる環境が整っている他、資格取得のための勉強を進めることで、体系立てて知識を獲得できるメリットがあります。

そうしたセキュリティ関連の資格として、比較的取り組みやすいものの1つに「情報セキュリティマネジメント試験（セキュマネ）」があります。

これは、脅威から継続的に組織を守るための基本的なスキルを認定する試験であり、業務で個人情報を取り扱ったり、情報管理を担当したりするすべての人を対象としています。

サイバーセキュリティについて、基礎知識からバランスよく学習したいと考えているのであれば、まずはここからチャレンジするのも1つの方法です。

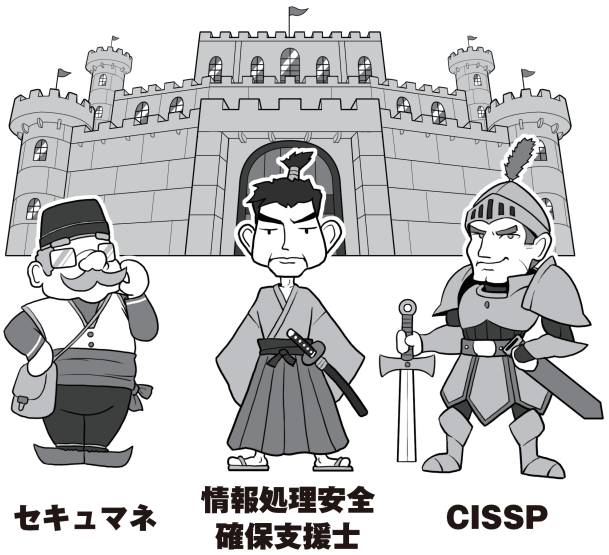
さらに、高度な資格としては、「情報処理安全確保支援士」やグローバルで普及している「CISSP」（Certified Information Systems Security Professional）などがあります。

情報処理安全確保支援士はサイバーセキュリティに関する実践的な知識や技能を有する専門人材の育成や確保を目的とした国家資格制度であり、サイバーセキュリティに関する高度な知識と技能を持つことを証明することができます。

一方、CISSPはISC2（International Information Systems Security Certification Consortium）が認定を行う、国際的なサイバーセキュリティのプロフェッショナル認証資格です。

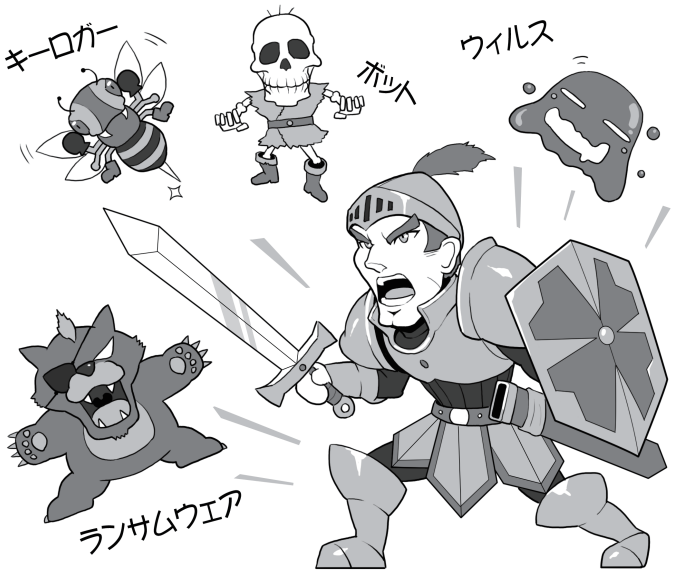
これらの資格取得に向けた勉強を積み重ねれば、自身のスキルアップにもつながるでしょう。

数多くあるセキュリティ資格



現在、セキュリティに関する資格試験は数多くあり、自分のレベルや目的に合わせて取得することが可能です。サイバーセキュリティに特化した試験にチャレンジする前に、ITに関する全般的な知識が問われる「ITパスポート試験」を受けてみてもよいでしょう。そして、情報処理安全確保支援士の「士」は騎士や武士の「士」。現代の騎士や武士としてセキュリティを守りましょう。

セキュリティを網羅的に学ぶことができる



資格取得を目指して勉強する大きなメリットは、その領域に関する知識を段階的かつ網羅的に学べることにあります。また、自分の知識レベルを判断する上でも、こうした試験は大いに役立ちます。

付録09 セキュリティスキルを向上させるには～「CYDER」と「CTF」 中小企業等向け

専任のセキュリティ担当者がいない中小企業等の場合、サイバー攻撃から身を守る手段は、主として「攻撃を受けにくくなる」ようにすることや、自社のウェブサイトを持つ場合でも、ホスティングサービスを利用することで、セキュリティに割く労力をアウトソースすることといった対応が現実的です。

しかし、サイバー攻撃に対して「立ち向かう」ことが求められる状況も出てきます。では実際にどうやって立ち向かえばよいのでしょう。

●CYDER

そこで参考にしたい取組が、国立研究開発法人情報通信研究機構（NICT）が国・地方公共団体・独法・重要インフラ事業者などの情報システム担当者などを対象に提供している実践的サイバー防御演習「CYDER（CYber Defense Exercise with Recurrence）」です。

CYDERの受講者は、事前オンライン学習によって攻撃手法や対策技術に対する理解を深め、集合演習（ハンズオン＆グループワーク）を通じて、一連のインシデントハンドリングを体験することにより、組織で役立つセキュリティポリシーやコミュニケーションの重要性を学ぶことができます。

とくに小さな組織では、情報システム担当者を専任で配置することが困難な場合があります。しかし、サイバー空間では、組織の規模に関係なく、攻撃されるリスクにさらされています。

経営者1人で対策を考えるのではなく、CYDERのようにコンパクトにまとまった訓練の機会を積極的に利用するとよいでしょう。組織のサイバー攻撃対応力をつけることが、有事に備えることにつながるのです。

●CTF

体系的な訓練以外に、さまざまな団体がコンテスト形式で行うサイバーセキュリティコンテストも存在します。それがCTF（Capture The Flag）です。

参加者は自身の知識や技術を活用して隠された答え（Flag）を見つけ出し、時間内に獲得した合計点数を競います。その他、ネットワーク内で擬似的なサイバー空間での攻防を行い競い合う形式のものもあります。

有名なものでは、アメリカで毎年夏に開催される世界最大のセキュリティ国際会議DEFCONが主催するCTF、また、日本国内では特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）SECCON実行委員会が主催する「SECCON」が有名です。

実践的サイバー防衛演習「CYDER」

CYDERのウェブサイトではCYDERのリーフレットや、その実習内容を紹介するPDFなどが公開されています。

左図のように仮想空間上に現実のネットワークに似たネットワークを構築して、サイバー攻撃への対処方法を実践的に体得できます。

2024年12月現在、CYDERにはレベルに応じたAコース、B-1コース、B-2コース、Cコースおよびプレ CYDERオンラインコースが用意されています。とくに初級レベルのAコースは全国47都道府県で開催されますので、国・地方公共団体・独法・重要インフラ事業者などの情報システム担当者などでご興味のある方は参加をおすすめします。

実践的サイバー防御演習「CYDER」	https://cyder.nict.go.jp/
セキュリティ国際会議「DEFCON」	https://defcon.org/
特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）SECCON実行委員会主催「SECCON」	https://www.seccon.jp/13/