中小企業の情報セキュリティ対策ガイドライン

第3.1版

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

目　次

付録１　情報セキュリティ５か条
付録２　情報セキュリティ基本方針（サンプル）
付録３　５分でできる！情報セキュリティ自社診断
付録４　情報セキュリティハンドブック（ひな形）
付録５　情報セキュリティ関連規程（サンプル）
付録６　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　リスク分析シート
付録８　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１～８は、それぞれ以下のページからダウンロードしてご利用ください。

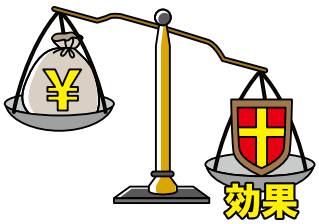
・中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/guide/sme/about.html

はじめに

1 経営者の皆様へ

本ガイドラインは、中小企業の皆様に情報を安全に管理することの重要性についてご認識いただき、中小企業にとって重要な情報[1]を漏えい、改ざん、消失などの脅威から保護するための情報セキュリティ対策の考え方や、段階的に実現するための方策を紹介することを目的としたものです。

情報セキュリティ対策は、経営に大きな影響を与えます！

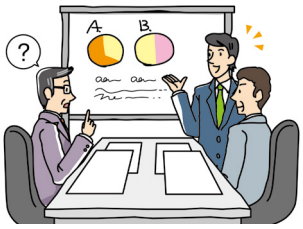


情報セキュリティ対策に取り組むことで、対外的に企業の信頼性が高まり、業績向上に繋がります。その一方で、情報セキュリティ対策を疎かにしたためにシステム障害が発生して事業活動が停止することがあります。また、情報漏えいの場合は、顧客や取引先の信頼を失い、業績が悪化することもあります。さらに、顧客や取引先に被害が及んだ場合には、経営を揺るがしかねない高額な賠償金を請求されることもあります。(➡ 詳細はP6)

対策の不備により経営者が法的・道義的責任を問われます！

現代社会では金銭や物品だけでなく、情報にも価値や権利が認められます。例えば個人情報保護法では、事業者に対して個人の権利利益の保護、安全管理措置などの管理監督が義務付けられており、これらへの違反が認められると場合によっては会社に罰金刑が課されます。さらに、取締役や監査役は、別途、会社法上の忠実義務違反の責任を問われることもあります。(➡ 詳細はP8)

組織として対策するために、担当者への指示が必要です！



企業の継続的な発展のために、また、経営責任を果たすためには、担当者に任せきりにすることなく、経営者が自社の情報セキュリティについて明確な方針を示すとともに自ら実行していくことが必要です。情報セキュリティ対策は、経営者が主導し、必要な範囲を網羅し、関係者と連携して組織的に実施しなければ機能しません。経営者はこれらを認識したうえで、情報セキュリティ対策の取り組みを担当者に指示する必要があります。(➡ 詳細はP12)

1 **▲重要な情報**　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管理責任を伴う情報のことです。経済的価値を指す“資産”を加え“情報資産”と呼ばれることがあり、本ガイドラインでも“重要情報”に加え“情報資産”と表記します。

2 本ガイドラインの対象

本ガイドラインは、業種を問わず中小企業および小規模事業者（法人、個人事業主、各種団体も含む）を対象として、その経営者と情報管理を統括する方を想定読者としています。

3 本ガイドラインの全体構成

本ガイドラインは、本編２部と付録により構成されます（表１）。付録には、情報セキュリティ対策の実施に活用できるドキュメント類のサンプルが含まれています。

【表１】本ガイドラインの全体構成

構　成		概　要
本編	**第１部　経営者編**	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
本編	**第２部　実践編**	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付録	**付録１　情報セキュリティ５か条**	組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明しています。
付録	**付録２　情報セキュリティ基本方針（サンプル）**	組織としての情報セキュリティに対する基本方針書のサンプルです。
付録	**付録３　５分でできる！情報セキュリティ自社診断**	あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。
付録	**付録４　情報セキュリティハンドブック（ひな形）**	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
付録	**付録５　情報セキュリティ関連規程（サンプル）**	情報セキュリティに関する社内規則を文書化したもののサンプルです。
付録	**付録６　中小企業のためのクラウドサービス安全利用の手引き**	クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。
付録	**付録７　リスク分析シート**	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。
付録	**付録８　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**	情報漏えいやシステム停止などのインシデント対応のための手引きです。

第3.1版の主な変更点について

■第１部

- 関連法令を最新の内容に見直しました。

■第２部

- 「テレワークの情報セキュリティ」、「セキュリティインシデント対応」に関する解説を追加しました。

■付録

- 付録１「情報セキュリティ５か条」、付録３「５分でできる！情報セキュリティ自社診断」の対策例を見直しました。
- 付録４「情報セキュリティハンドブック（ひな形）」、付録５「情報セキュリティ関連規程（サンプル）」にテレワークの情報セキュリティに関するひな形、サンプルを追加しました。
- 付録８「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」を追加しました。

4 本ガイドラインの活用方法

本ガイドラインの活用にあたって、情報セキュリティに組織的に取り組んだ経験は必要ありません。本ガイドラインにより、事業の特徴に応じた情報セキュリティ対策を段階的に進めていくことができます。「**第１部 経営編**」は、全ての経営者に読んでいただきたい内容です。まずはご一読ください。「**第２部 実践編**」は、あなたの組織にあったSTEPから進めてください。

取組状況とアクション	本ガイドラインの活用方法
Step1 **まず始めましょう**	これまで情報セキュリティ対策を特に意識していない場合は**「2. できるところから始める」**（P.19）を参照して、「情報セキュリティ５か条」を実行してください。 **進め方** 「情報セキュリティ５か条」を社内で配付するなど、まずできるところから開始してください。
Step2 **現状を知り改善しましょう**	Step1 は実施できていて次に進める場合は **「3. 組織的な取り組みを開始する」**（P.20）を参照して、「５分でできる！情報セキュリティ自社診断」で自社の状況を把握し、できていない対策の実行に努めてください。 **進め方** ・「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成してください。 ・「5 分でできる！情報セキュリティ自社診断」で現状の対策を把握し、実施すべき対策を検討してください。 ・「情報セキュリティハンドブック（ひな形）」を参考に具体的な対策を定めて従業員に周知してください。
Step3 **本格的に取り組みましょう**	Step2 までは実施できていて次に進める場合は **「4. 本格的に取り組む」**（P.24）を参照して、自社のリスクに応じた対策規程を作成し、運用後は点検して改善を図ってください。 **進め方** ・情報セキュリティ管理の体制を構築し、対策の予算を確保してください。 ・対応すべきリスクと対策を検討し、「情報セキュリティ関連規程（サンプル）」を参考に規程を作成してください。 ・委託時に必要となる対策を検討するとともに、点検や改善に努めてください。
Step4 **改善を続けましょう**	**「5. より強固にするための方策」**（P.32）を参照して、自社に必要な対策を追加実施してください。Step1 や Step2 に取り組んでいる企業でも、Step4 を参照して必要な対策があれば実行してください。

第１部　経営者編

経営者編では、情報セキュリティ対策に関して、
経営者が認識し、
自らの責任で考えなければならない
事項について説明します。

1 情報セキュリティ対策を怠ることで企業が被る不利益

ITの普及や利活用により経営効率が向上した反面、ITの普及以前には想定し得なかった秘密情報や個人情報の漏えいによる、高額の賠償請求や金銭的損失を伴う事故が増えています。さらに、近年では事故やその影響も多様化し、金銭的損失以外の不利益も顕著になっています。こうした事故による不利益は、情報セキュリティ対策を行うことで、経営上受容できる範囲まで減らすことができます。

ここでは、情報セキュリティ対策の必要性に対する理解を深めていただくために、対策が不十分なために起きる事故と、それにより企業が被る主な不利益を次に挙げる4点に要約して説明します。

(企業が被る主な不利益)

●金銭の損失　●顧客の喪失　●事業の停止　●従業員への影響

これらを参考に、自社で起きかねない情報セキュリティ上の事故とは何か、どの業務にそのような心配があるか、自社の経営において最も懸念される事態は何かなどを具体的に思い描くことが、経営者が情報セキュリティ対策を認識する第一歩です。このような思考実験が経営者によるリスク認識の基礎となります。

(1) 金銭の損失

取引先などから預かった機密情報や個人情報を万一漏えいさせてしまった場合は、取引先や顧客などから損害賠償請求を受けるなど、大きな経済的損失を受けることになります。

一方、こうした損害賠償などによる損失だけでなく、インターネットバンキングに関連した不正送金やクレジットカードの不正利用などで直接的な損失を被る企業の数も増えています。

事例1　ECサイトへの不正アクセスにより営業機会損失が発生

(所在地：大阪府／業種：卸売業・小売業／従業員規模：5名以下)

自社のECサイトに不正アクセスの痕跡があった。決済方法としてクレジットカード決済も認めているのだが、決済のページに多数のアクセスがあった。具体的にはクレジットカード番号をランダムに入力し、決済を試みていたようである。幸い、決済はすべて失敗していたためクレジットカードの不正利用はなかった。しかし、手当のために1週間程度の期間が必要となってしまい、その間、一部の機能が制限されたこともあり、金銭的にもわずかであるがマイナスが生じてしまった。この出来事は、情報セキュリティ対策強化の重要性を認識するきっかけとしては十分な経験であった。

不正アクセスの被害に気付いた後、サーバーの履歴を確認したところ、海外のIPアドレスから大量にアクセスされていることが判明した。もちろん、クレジットカード会社を含む決済サービスを提供する会社側でも一定の情報セキュリティ対策を行っている所ではあるが、やはり、自社でも対策をする必要があると改めて感じた。これを受けて実施した対策として、海外のIPアドレスからアクセスがあった場合、クレジットカード決済に必要な番号等の入力に失敗した場合のアクセス制限・アクセス遮断を厳格にする取り組みを実施した。

(2) 顧客の喪失

重要な情報に関する事故を発生させると、その原因が何であれ、事故を起こした企業に対する管理責任が問われ、社会的評価は低下します。同じ製品やサービスを提供している

企業が他にあれば、事故を起こしていない企業の製品やサービスを選択する顧客が増えるのは自然なことであり、事故の発覚直後には大きなダメージを受けることになります。

大手メーカーのサプライチェーンに位置する企業の場合は、これまで継続してきた受注が停止に追い込まれることにもなりかねません。事故を起こした企業は再発防止に努め、事故を起こさずに事業を続けていくことが必要ですが、低下した社会的信用の回復には時間を要するため、事業の存続が困難になる場合もあります。

事例2　顧客情報の入ったパソコンの紛失事故により取引先の信用を失墜

（所在地：石川県／業種：建設業／従業員規模：101 ～ 300 名）

従業員が顧客情報の入ったパソコンを持ち出した時に紛失事故が発生した。顧客に対して紛失の報告をしたが信用を失うこととなった。原因は、会社として情報セキュリティに対する意識が高くなかったため、持ち出しに関する明確なルールや手続きを定めておらず、従業員がパソコンを自由に持ち出せる環境であったことである。その後、情報機器の暗号化などの対策を実施するとともに、パソコンの持ち出しルールを含めた情報セキュリティ規程を整備して従業員へ情報セキュリティ教育を行った。

(3) 事業の停止

事業運営にデジタル技術の活用が進むなか、情報システムに事故が発生し、使用できなくなると、生産活動の遅れや営業機会の損失などにより業務が停滞してしまいます。そればかりか、中核となる事業を支えている情報システムの場合は、事業そのものの停止や取引先への影響も余儀なくされ、企業の存続にも影響が出てしまいます。

事例3　ランサムウェア感染により復旧作業のための時間と費用を費やす

（所在地：石川県／業種：建設業／従業員規模：101 ～ 300 名）

ランサムウェアに感染し、サーバー上のファイルが暗号化されて、身代金を要求される被害を経験した。復旧作業のために時間や費用を費やすことになってしまった。その後、社内規程の整備を行い、従業員のリテラシー向上のための周知を継続的に行なっている。また、従業員端末の管理者権限を剥奪することで、ソフトウェアのインストールを制限するなどの技術的な対策を行なっている。

(4) 従業員への影響

情報セキュリティ対策の不備を悪用した内部不正が容易に行えるような職場環境は、従業員のモラル低下を招く要因となります。さらに事故を起こしたにも関わらず、従業員のみを罰して管理職が責任を取らないような対応は、従業員が働く意欲を失うおそれがあります。情報漏えいなどの事故による企業としてのイメージダウンを嫌って、転職する従業員も現れます。また、従業員の個人情報が適切に保護されなければ、従業員から訴訟を起こされることも考えられます。ある経営者は「個別の損害より、職場環境が暗くなったことが一番困った」と語っています。

2 経営者が負う責任

情報セキュリティ対策を的確に指揮しなかったことに起因する業績の悪化などが経営者の責任であることは言うまでもありませんが、それ以外の経営者の「法的責任」と「社会的責任」について説明します。

(1)経営者などに問われる法的責任

企業の経営を委任されている立場の取締役は、民法・会社法により「取締役にふさわしくベストを尽くして経営に当たる義務(善管注意義務[2])」を負い、「その任務を怠ったときは、株式会社に対し、これによって生じた損害を賠償する責任を負う。(任務懈怠(けたい))」と規定されています。

このため、セキュリティ対策について、取締役としてベストを尽くさなかった結果、サイバー攻撃による情報漏えいや製品・サービス供給の停止等、企業や第三者に損害が生じた場合、表2に示すような善管注意義務違反や任務懈怠に基づく損害賠償責任を問われます。

また、法律によっては違反等が発生した場合に、経営者や取締役、担当者に対して表3に示すような刑罰が科せられることもあります。

- 個人情報保護法やマイナンバー法に関する違反の場合は行為者だけでなく事業者にも罰則が科せられるケースがあります。また、個人情報保護委員会[3]による立入検査を受ける責任もあります。
- 会社法の第三者責任や民法の不法行為責任が認められると、経営者が個人として損害賠償責任を負う場合もあります。

【表2】情報セキュリティ対策が不備の場合に責任追及の根拠とされる主な法律

法令	条項	要約
民法	第415条 債務不履行による損害賠償責任	サイバー攻撃により仕事が停滞した場合、会社及び第三者に対する、契約違反による賠償義務を負う。
	第644条 取締役の善管注意義務違反	企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対して、善管注意義務違反による賠償義務を負う。
	第562条 契約不適合責任	請負契約の仕事の目的物(開発システムなど)について、その種類や品質が契約内容に適合しないことが仕事の完成後に判明した場合、会社及び第三者に対する契約不適合となる。
	第709条 不法行為による損害賠償 第715条 使用者等の責任	故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する義務を負う。
会社法	第330条 取締役の善管注意義務違反	企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対する、善管注意義務違反による任務懈怠(けたい)に基づく損害賠償責任を負う。
	第423条第1項 任務懈怠による損害賠償責任	
	第429条第1項 第三者に対する注意義務違反	

2 **▲善管注意義務**　善良な管理者の注意義務の略。裁判所職員総合研修所監修「民法概説(五訂版)」(P271)では、「ベストを尽くす」という表現を用いている。

3 **▲個人情報保護委員会**　個人情報保護委員会は公正取引委員会と同様の高い独立性を有する機関です。

法令	条項	要約
割賦販売法	第35条の17の9　販売店におけるクレジットカードの適切な取り扱い	「クレジットカード・セキュリティガイドライン[4]」において、販売店においては、クレジットカード番号等取扱契約の締結に係る業務に関して、クレジットカード番号を保有しない等、クレジットカード番号等に関する情報の適切な管理のために必要措置を講じる責任を負う。
外国為替及び外国貿易管理法、輸出貿易管理令	暗号機能製品の輸出入における許諾・承認	暗号機能実装製品の輸出入を行う場合には、経済産業大臣の許可や承認が必要となる。

【表３】情報管理が不適切な場合の処罰など

法令	条項	要約
刑法 不正指令電磁的記録に関する罪(ウイルス作成罪)	第168条の2 第168条の3 不正指令電磁的記録作成罪等	正当な理由なく、他人のコンピュータにおいて実行させる目的でウイルスを作成・提供・実行した場合、3年以内の懲役又は50万円以下の罰金。保管した場合は、2年以下の懲役又は30万円以下の罰金。
不正アクセス行為の禁止等に関する法律	第3条 不正アクセス行為の禁止 第4条 不正アクセスにつながる識別符号の不正取得の禁止 第5条 不正アクセス行為を助長する行為の禁止 第6条 不正アクセスにつながる識別符号の保管の禁止	コンピュータに対する不正アクセスや、不正アクセスにつながるID・パスワード等の識別符号の不正取得・保管行為、不正アクセスを助長する行為等をした場合、不正アクセスは3年以下の懲役又は100万円以下の罰金。その他の行為は1年以下の懲役又は50万円等の罰金。
特定電子メールの送信の適正化等に関する法律(迷惑メール防止法)	第3条 特定電子メールの送信の制限 第4条 送信者氏名・名称等の表示義務 第5条 送信者情報を偽った送信の禁止	送信の同意を得ず、広告又は宣伝を行う電子メールの送信、送信者表示義務の違反、送信者情報を偽った送信を行った場合、総務大臣及び内閣総理大臣より改善に必要な措置を命じられる。さらに、送信者情報を偽った送信を行った場合、1年以下の懲役又は100万円以下の罰金。
個人情報保護法 個人情報の保護に関する法律	第173条 委員会からの命令に違反	個人情報保護委員会による勧告に対し、正当な理由なく勧告に係る措置をとらなかった場合、1年以下の懲役又は100万円以下の罰金。
	第174条 個人情報データベース等不正提供罪[5]	業務に関して取り扱った個人情報データベース等を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用した場合、1年以下の懲役又は50万円以下の罰金。
	第177条 報告及び立入検査	委員会による立入検査、帳簿書類等の物件検査及び質問に必要な資料の提供をしない場合又は虚偽の報告をする場合、50万円以下の罰金。
	第179条 両罰規定	従業者等が業務に関し違反行為をした場合、法人に対しても1億円以下の罰金。
	第180条 委員会への虚偽の報告など	偽りその他不正手段により個人情報開示の合意を得た場合、10万円以下の過料。
マイナンバー法(番号法) 行政手続における特定の個人を識別するための番号の利用等に関する法律	第48条 正当な理由なく特定個人情報ファイルを提供	正当な理由がなく業務に関して取り扱った特定個人情報ファイルを提供した場合、4年以下の懲役若しくは200万円以下の罰金又は併科。
	第49条 不正な利益を図る目的で、個人番号を提供又は盗用	業務に関して知り得た特定個人情報を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用した場合、3年以下の懲役若しくは150万円以下の罰金又は併科。
	第50条 情報提供ネットワークシステムに関する秘密を漏えい又は盗用	
	第51条 不正な手段で個人番号を取得	人を欺き、人に暴行を加え、若しくは人を脅迫する行為により、又は財物の窃取、施設への侵入、不正アクセス行為、その他の個人番号を保有する者の管理を害する行為により、個人情報を取得した場合、3年以下の懲役又は150万円以下の罰金。

4 ▲クレジットカード・セキュリティガイドライン(一般社団法人日本クレジット協会)
https://www.j-credit.or.jp/download/news20220309b1.pdf

5 **▲データベース等不正提供罪**　改正個人情報保護法で新設され、役員・従業者等が不正な利益を図る目的で個人情報データベース等を他者に提供等したり盗用した場合は処罰対象になります。

法令	条項	要約
マイナンバー法（番号法） 行政手続における特定の個人を識別するための番号の利用等に関する法律	第53条 委員会からの命令に違反	個人番号利用事務等実施者による開示命令に違反した場合、2年以下の懲役又は50万円以下の罰金。
	第54条 委員会への虚偽の報告など	委員会への報告又は立入検査において、報告若しくは資料の提出をせず、若しくは虚偽の報告をし、若しくは虚偽の資料を提出し、又は質問に対して答弁をせず、若しくは虚偽の答弁をし、若しくは検査を拒み、妨げ、若しくは忌避した場合、1年以下の懲役又は50万円以下の罰金。
	第55条 偽りその他不正の手段により個人番号カード等を取得	偽りその他不正の手段により個人番号カードの交付を受けた者は、6月以下の懲役又は50万円以下の罰金。
	第57条 両罰規定	従業者等が業務に関し違反行為をした場合、法人に対しても1億円以下の罰金又は各本条が定める罰金。
不正競争防止法 営業秘密・限定提供データに係る不正行為の防止など	第3条 差止請求権	不正競争によって営業上の利益を侵害され、又は侵害される恐れがある者からの侵害の停止又は予防を請求される。
	第4条 損害賠償	故意又は過失により不正競争を行って営業上の利益を侵害した者は、損害を賠償する責任を負う。
	第14条 信頼回復措置	故意又は過失により不正競争を行って営業上の信用を害された者からの信用回復措置請求がなされた場合、裁判所より信用回復に必要な措置が命じられる。
金融商品取引法 インサイダー取引の規制など	第175条 会社関係者に対する禁止行為等に違反した者に対する課徴金	従業者等が業務に関し違反行為をした場合、法人に対しても罰金。また犯罪行為により得た財産の必要的没収・追徴が行われ、課徴金は違反類型によって異なる。
一般データ保護規則（GDPR：General Data Protection Regulation）	EU域内の個人データ取り扱いの制限	EU域内の個人データ保護について規定する。EU域内の個人データを扱う場合はEU以外の企業も対象となる。違反の内容によっては、2000万ユーロ以下の制裁金、又は直前の会計年度における世界全体における売上総額の4%以下の金額、若しくはいずれか高額の方の制裁金。

(2) 関係者や社会に対する責任

適切に管理することを前提に預かった情報を漏えいしてしまった場合に問われるのは、前述の法的責任に加え、その情報の提供者や顧客などの関係者に対する責任もあります。また、情報漏えい事故は、営業機会の喪失、売上高の減少、企業のイメージダウンなど、自社に損失をもたらしますので、会社役員が会社法上の責任（会社に対する損害賠償責任）を問われ株主代表訴訟を提起されることもあり得ます。さらには、取引先との信頼関係の喪失、業界全体のイメージダウンにもなってしまいます。したがって、情報セキュリティ対策は、顧客・取引先・従業員・株主などに対する経営者としての責任を果たすためにも重要です。

コラム

個人情報保護法

個人情報保護法は、企業や団体に個人情報をきちんと大切に取り扱ったうえで、有効に活用できるよう共通のルールを定めた法律です[6]。「氏名」、「生年月日」、「住所・電話番号・メールアドレス」などの連絡先、「顔写真」など、事業によって取り扱う個人情報は様々です。従業員情報や取引先の名刺も個人情報に当たりますので、従業員名簿やメールのアドレス帳などを作成している事業者は、保有する個人情報が少なくても、個人情報取扱事業者（個人情報データベース等を事業の用に供している者）となり、この法律が適用されます。特に、自身の個人情報に対する意識の高まり、技術革新を踏まえた保護と利活用のバランス、インターネット利用における外国の事業者への個人情報の流通増大に伴う新たなリスクへの対応等の観点から、以下の対応が義務化されていますので、対応を行いましょう。

①個人データの漏えい等が発生し、個人の権利利益を害するおそれがあるときは、個人情報保護委員会への報告及び本人への通知が必要です。
②外国にある第三者へ個人データを提供するに当たっては、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報を本人に提供したうえで本人の同意を得る必要があります。
③保有個人データの利用目的と、どのようなセキュリティ対策を行っているか本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）にします。

個人情報の取扱いについて社内規程を作成する場合は以下が参考になります。

●4 本格的に取り組む　(3)情報セキュリティ規程の作成　P.26
●個人情報保護委員会のウェブサイト
法令・ガイドライン等　お役立ちツール（※中小企業向け）/個人データ取扱要領（例）
https://www.ppc.go.jp/personalinfo/legal/#oyakudati

EU一般データ保護規則（GDPR：General Data Protection Regulation）

個人情報とプライバシー保護強化を目的に、欧州経済領域（EEA）における個人情報の取り扱いについて法的要件を定めた規則です。EU圏内に子会社や支店がある企業、日本からEU圏内に製品やサービスを提供している企業、EU圏内から個人情報の処理について委託を受けている企業等が対象になることがあります。

不正競争防止法

企業が持つ営業情報や技術情報などの中には、秘密とすることで差別化や競争力の源泉となる情報もあります。そのような情報が漏えいすると、研究開発投資の回収機会を失ったり、社会的な信用の低下により顧客を失ったりと大きな損失を被ることになります。秘密としている情報を不正競争防止法により営業秘密として法的保護を受けるためには、次の①～③の要件をすべて満たす必要があります。

①秘密として管理されていること（秘密管理性）
②生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であること（有用性）
③公然と知られていないこと（非公知性）

●経済産業省　不正競争防止法　営業秘密～営業秘密を守り活用する～
https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

なお、その他の関連する法令については、以下を参照ください。

●内閣サイバーセキュリティセンター　関係法令Q＆Aハンドブック
https://security-portal.nisc.go.jp/law_handbook/

6▲個人情報保護法第1条には「個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。」とあることから、個人情報保護とは企業が被る損害の防止だけではなく、個人の人格的、財産的な権利利益に対する侵害防止を目的としていることに留意する必要があります。

3 経営者は何をやらなければならないのか

企業で情報セキュリティを確保するための、経営者の役割を説明します。情報セキュリティの確保に向けて、経営者は、(1)に示す「3原則」について認識したうえで、(2)に示す「重要7項目の取組」の実施を指示する必要があります。

(1)認識すべき「3原則」

経営者は、以下の3原則を認識し、対策を進める必要があります。

原則 1　情報セキュリティ対策は経営者のリーダーシップで進める

経営者は、IT活用を推進する中で、情報セキュリティ対策の重要性を認識し、自らリーダーシップを発揮して対策を進めます。現場の従業員は、安心して業務に従事できる環境を求める一方、利便性が低下し、面倒な作業を伴う対策には抵抗感を示しがちです。そこで、情報セキュリティ対策は、経営者が判断して意思決定し、自社の事業に見合った情報セキュリティ対策の実施を主導します。

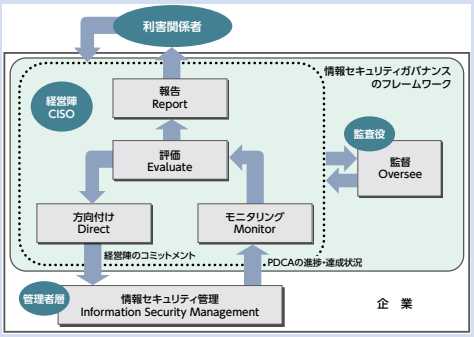
コラム

情報セキュリティガバナンス

情報セキュリティガバナンスは、経営者が企業戦略として情報セキュリティ向上に取り組むための枠組みです。

この枠組みは、経営者が懸念する避けるべき重大事故などを示して「方向付け」を行い、対策の進捗や点検等により状況を「モニタリング」し、その効果を「評価」して方向付けを見直すサイクルを骨格としています。

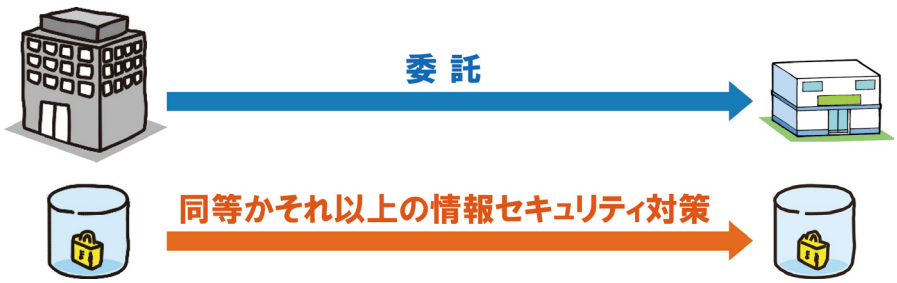
経営者がリーダーシップを発揮する枠組みでもあります。



●経済産業省『情報セキュリティガバナンスの概念』
https://www.meti.go.jp/policy/netsecurity/secgov-concept.html

原則 2　委託先の情報セキュリティ対策まで考慮する

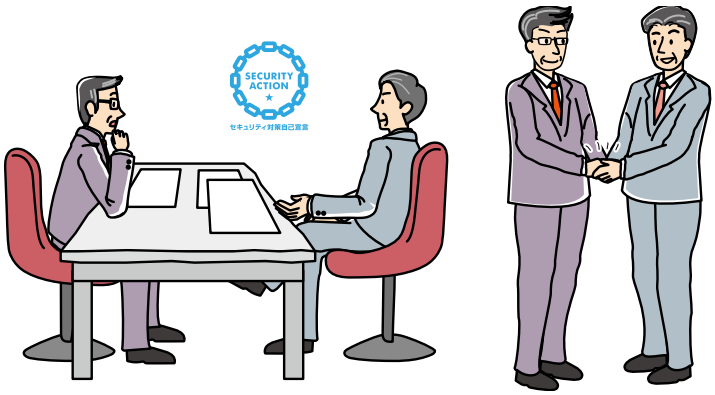
業務の一部を外部に委託するにあたって重要な情報を委託先に提供する場合、委託先がどのような情報セキュリティ対策を行っているか考慮する必要があります。委託先に提供した情報が漏えいしたり、改ざんされたとき、それが委託先の不備だったとしても、事故の影響を受ける者から委託元としての管理責任を問われることになります。そのため、委託先や、共同で仕事を行っているビジネスパートナーなどの情報セキュリティ対策に関しても、自社同様に十分な注意を払います。また、受託している場合には、委託元の要求に応じる必要があります。



原則 3　関係者とは常に情報セキュリティに関するコミュニケーションをとる

業務上の関係者（顧客、取引先、委託先、代理店、利用者、株主など）からの信頼を高めるには、普段から自社の情報セキュリティ対策や、事故が起きたときの対応について、関係者に明確に説明できるように経営者自身が理解し、整理しておくことが重要です。

情報セキュリティに関する取組方針を常日頃より関係者に伝えておくことで、サイバー攻撃によるウイルス感染や情報漏えいなどが発生した際にも、説明責任を果たすことができ、必要以上の不安を与えることなく、信頼関係を維持することができます。



(2) 実行すべき「重要７項目の取組」

中小企業で情報セキュリティを確保するための、経営者の役割を説明します。経営者は、以下の重要７項目の取組について、自ら実践するか、実際に情報セキュリティ対策を実践するうえでの責任者・担当者に対して指示します。場合によっては、経営者自らが実行することも必要になると考えられます。

取組 1　情報セキュリティに関する組織全体の対応方針を定める

情報セキュリティ対策を組織的に実施する意思を、従業員や関係者に明確に示すために、どのような情報をどのように守るかなどについて、自社に適した情報セキュリティに関する基本方針を定め、宣言します。自社の経営において最も懸念される事態は何かを明確にすることで具体的な対策を促し、組織としての方針を立てやすくなります。

取組 2　情報セキュリティ対策のための予算や人材などを確保する

情報セキュリティ対策を実施するために、必要な予算と担当者を確保します。これには事故の発生防止だけでなく、万が一事故が起きてしまった場合の被害の拡大防止や、復旧対応も含みます。情報セキュリティ対策には高度な技術が必要なため、専門的な外部サービス[7]の利用も検討します。

取組 3　必要と考えられる対策を検討させて実行を指示する

懸念される事態に関連する情報や業務を整理し、損害を受ける可能性（リスク）を把握したうえで、責任者・担当者に対策を検討させます。必要とされる対策には予算を与え、実行を指示します。実施する対策は、社内ルールとして文書にまとめておけば、従業員も実行しやすくなり、取引先などにも取り組みを説明する際に役に立つので、併せて指示します。

実行を指示した情報セキュリティ対策がどのように現場で実施されているかにつき、月次や四半期ごとなど適切な機会をとらえて報告させ、進捗や効果を把握します。

取組 4　情報セキュリティ対策に関する適宜の見直しを指示する

取組3で指示した情報セキュリティ対策について、実施状況を点検させ、取組１で定めた方針に沿って進んでいるかどうかの評価をします。また業務や顧客の期待の変化なども踏まえて基本方針なども適宜見直しを行い、致命的な被害につながらないよう、対策の追加や改善などを行うように、責任者・担当者に指示します。

7 ▲専門的な外部サービスについてはIPAが公開している「情報セキュリティサービス基準適合サービスリスト」を活用することができます。(P.49 コラム「情報セキュリティサービス基準審査登録制度」参照)

取組 5　緊急時の対応や復旧のための体制を整備する

万が一に備えて、緊急時の対応体制を整備します。被害原因を速やかに追究して被害の拡大を防ぐ体制を作るとともに、的確な復旧手順をあらかじめ作成しておくことにより、緊急時に適切な指示を出すことができます。整備後には予定どおりに機能するかを確認するため、被害発生を想定した模擬訓練を行うと、意識づけや適切な対応のために効果的です。経営者のふるまいについても、あらかじめ想定しておけば、冷静で的確な対応が可能になります。

取組 6　委託や外部サービス利用の際にはセキュリティに関する責任を明確にする

業務の一部を外部に委託する場合は、委託先でも少なくとも自社と同等の対策が行われるようにしなければなりません。そのためには契約書に情報セキュリティに関する委託先の責任や実施すべき対策を明記し、合意する必要があります。

ITシステム(電子メール、ウェブサーバー、ファイルサーバー、業務アプリケーションなど)に関する技術に詳しい人材がいない場合、自社でシステムを構築・運用するよりも、外部サービスを利用したほうが、コスト面から有利な場合がありますが、安易に利用することなく、利用規約や付随する情報セキュリティ対策などを十分に検討するよう担当者に指示する必要があります。

取組 7　情報セキュリティに関する最新動向を収集する

情報技術の進化の早さから、実施を検討するべき対策は目まぐるしく変化します。自社だけで把握することは困難なため、情報セキュリティに関する最新動向を発信している公的機関[8]などを把握しておき、常時参照することで備えるように情報セキュリティ担当者に指示します。また、知り合いやコミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有します。

8▲情報セキュリティに関する最新動向を発信している公的機関
IPA(独立行政法人情報処理推進機構)のウェブサイト　https://www.ipa.go.jp/security/index.html
NISC(内閣サイバーセキュリティセンター)のウェブサイト　https://www.nisc.go.jp/

コラム

「SECURITY ACTION」一つ星を宣言しよう！

「SECURITY ACTION（セキュリティアクション）」は、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度です。取り組み段階に応じて、「一つ星」「二つ星」のロゴマークを無料で使用することができます。

「SECURITY ACTION」は情報セキュリティ対策に取り組んだことのない企業でも、すぐに始めることができます。規模や業種を問わず共通する基本的な対策を実行することで、顧客や取引先との信頼関係の構築に大いに役立ちます。

さらに、デジタル化やサイバーセキュリティ対策などを支援する公的支援制度の要件になるなど、情報セキュリティのはじめの一歩として、とても有益な制度です。

「SECURITY ACTION」一つ星は、情報セキュリティ５か条に取り組むことを宣言するものです。

情報セキュリティ５か条

1. OSやソフトウェアは常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃の手口を知ろう！

これらの項目は、企業の規模に関わらず、必ず実行すべき重要な対策です。第２部に進む前に経営者のトップダウンで実行を開始して、自社が情報セキュリティ対策の取り組みを開始したことを自己宣言しましょう。

宣言方法や制度詳細は公式サイトをご確認ください。

●SECURITY ACTION公式サイト
https://www.ipa.go.jp/security/security-action/

「サイバーセキュリティお助け隊サービス」手遅れになる前に手を打とう！

「サイバーセキュリティお助け隊サービス」は、中小企業等に対するサイバー攻撃への対処として不可欠なサービスを要件にまとめ、ワンパッケージで安価に提供するサービスです。

所定の審査機関により要件を満たすことが確認された民間サービスを「サイバーセキュリティお助け隊サービス」としてIPAが登録・公表しています。

ワンパッケージで安価に！

①見守り　24時間365日監視　挙動や問題のある攻撃を検知し、あなたのPCとネットワークを守ります。
②駆付け　問題が発生したときに地域のIT事業者等が駆付け対応します。（リモート支援の場合あり）
③保険　簡易サイバー保険で駆付け支援等のサイバー攻撃による被害対応時に突発的に発生する各種コストが補償されます。

●サイバーセキュリティお助け隊サービスリスト
https://www.ipa.go.jp/security/otasuketai-pr/

第２部　実践編

実践編では、情報セキュリティ対策を実践する
責任者・担当者を対象に、
実務的な進め方について説明します。

1 実践編の進め方

ここでは、経営者の指示に従い、どのように情報セキュリティ対策を実践していくかについて説明します。情報セキュリティ対策に組織全体で取り組むには、実行すべき対策を決めて、従業員に周知する必要があります。

しかし、こうした作業を行うには情報セキュリティに関する知識や経験が必要となるため、それらの知識や経験に長けた人材がいないと対策が進まなくなることも考えられます。

そこで、本ガイドラインでは、規模の小さな企業や、これまで十分な情報セキュリティ対策を実施してこなかった企業などを対象に、すぐにできることから開始して、段階的にステップアップすることで、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するとともに、実践のために各種の付録を用意しました。第1部で説明した重要7項目の取組との対応を示した表4を参考に、自社の状況に合わせて進めてください。

【表4】重要7項目の取り組みと実践編の対応表

経営者が実行すべき重要7項目									
実践編		ページ	1	2	3	4	5	6	7
2	できるところから始める								
	(1) 情報セキュリティ5か条	19			●				●
3	組織的な取り組みを開始する								
	(1) 情報セキュリティ基本方針の作成と周知	20	●						
	(2) 実施状況の把握	20			●				
	(3) 対策の決定と周知	22			●				
4	本格的に取り組む								
	(1) 管理体制の構築	24		●			●		
	(2) デジタルトランスフォーメーション(DX)の推進と情報セキュリティの予算化	25		●					
	(3) 情報セキュリティ規程の作成	26			●				
	(4) 委託時の対策	28						●	
	(5) 点検と改善	30				●			
5	より強固にするための方策								
	(1) 情報収集と共有	33							●
	(2) ウェブサイトの情報セキュリティ	34			●				
	(3) クラウドサービスの情報セキュリティ	38			●				
	(4) テレワークの情報セキュリティ	42			●				
	(5) セキュリティインシデント対応	46					●		
	(6) 情報セキュリティサービスの活用	48			●				
	(7) 技術的対策例と活用	50			●				
	(8) 詳細リスク分析の実施方法	54			●	●			

2 できるところから始める

(1)情報セキュリティ５か条

多くの中小企業にとっては、いきなり精巧な対策を開始するのは大変なことだと思います。**「情報セキュリティ５か条」(付録１)**では、企業の規模に関わらず、必ず実行すべき重要な対策を５か条にまとめています。

インターネットの普及に伴い様々な脅威が現れ、攻撃者の手口は年々巧妙かつ悪質になっていますが、対策には共通する部分があります。情報セキュリティ５か条は、共通する基本的な対策をまとめたものですので、必ず実行しましょう。

① OSやソフトウェアは常に最新の状態にしよう！

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、もしくは最新版を利用するようにしましょう。

② ウイルス対策ソフトを導入しよう！

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。

③ パスワードを強化しよう！

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。

④ 共有設定を見直そう！

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。

⑤ 脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウイルス付き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。

3 組織的な取り組みを開始する

(1) 情報セキュリティ基本方針の作成と周知

経営者が定めた情報セキュリティに関する基本方針を、従業員や関係者に伝えるために、簡潔な文書を作ります。基本方針には、決まった書き方はありませんので、**「情報セキュリティ基本方針(サンプル)」(付録2)**を参考にして、事業の特徴や顧客の期待などを考慮したうえで経営者と連携しつつ、自社に適した基本方針を作成してください。

また、基本方針は従業員の指針であり、関係者に対して取り組みを表明するためのものなので、作成した文書は、従業員や顧客などの関係者に周知しましょう。

情報セキュリティ基本方針の記載項目例

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善　　など

(2) 実施状況の把握

「5分でできる！情報セキュリティ自社診断」(付録3)を利用して、情報セキュリティ対策が、どれくらい実施できているかを把握します。自社診断は、表5に示す25項目の設問に答えるだけで情報セキュリティ対策の実施状況が把握できるツールです。

具体的な使い方は以下のとおりです。

- 経営者または情報システム担当や部門長など実施状況が分かる人が「5分でできる！情報セキュリティ自社診断」の診断編に記入します。
- 事業所が複数ある、部署数が多いなど、一人で記入することが難しい場合には、事業所や部署ごとに記入し、責任者・担当者が集計します。
- 実施状況が分からない場合は、各従業員に質問して、回答を総合して記入します。
- チェック欄の該当するもの1つに○を付けて、「実施している　4点」「一部実施している　2点」「実施していない　0点」「わからない　－1点」で採点します。
- 全項目の合計点で、組織全体のセキュリティ対策の実施状況と、回答が「わからない」になっている項目を把握します。

【表5】自社診断のための25項目

No		診断内容
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？
	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？
	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	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？
	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？
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？
	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？
	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？
	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？
	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？
	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？
	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？
	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？
	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？
	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？
	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？
	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？
	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？
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？
	20	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？
	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？
	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？
	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？
	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？
	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？

※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管理責任を伴う情報のことです。

(3) 対策の決定と周知

診断結果をもとに、「5分でできる！情報セキュリティ自社診断」の解説編を参考に、実行すべき情報セキュリティ対策を検討します。自社診断には、あまり費用をかけず、効果があると考えられる対策例が示されているので、診断結果に基づき、実施すべき対策を検討します。

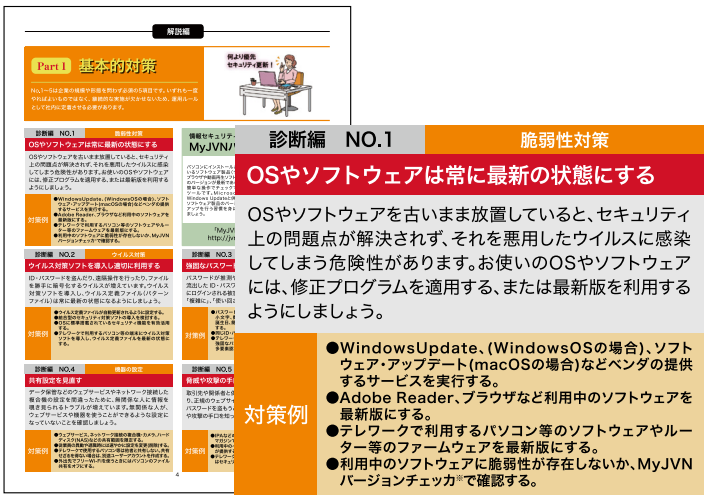
具体的な使い方は以下のとおりです。

●対策の検討と決定は、責任者・担当者と経営者が行います。

●診断項目ごとに対策を実施しない場合に考えられる被害・事故や、防止するための対策例が示されているので、参考にして検討します。

●検討するときには従業員の意見を聞き、職場環境や業務に適した対策を決定します。

「5分でできる！情報セキュリティ自社診断」解説編



対策が決まったら、**「情報セキュリティハンドブック(ひな形)」(付録4)**を利用して、従業員が実行するべき事項を周知します。情報セキュリティハンドブック(ひな形)は、自社診断の対策例と連動したひな形です。決定した対策を具体的に記述して、従業員に配付します。

具体的な使い方は以下のとおりです。

●情報セキュリティハンドブックは、責任者・担当者が作成します。

●ひな形に記載された例文を編集して、決定した対策を社内ルールとして明文化します。

(例)データのバックアップ

編集前(ひな形)

機器名	対象	方法	保管媒体	頻度
○○サーバー	システムファイル ユーザーファイル	Windows バックアップ	外付け HDD	毎週

編集後

機器名	対象	方法	保管媒体	頻度
営業部 ファイルサーバー	売買契約書ファイル	バックアップソフトによる 増分バックアップ	外付け HDD	毎週

●完成した情報セキュリティハンドブックを全従業員に配付し、必要に応じて説明する機会を設けるなどして、情報セキュリティ対策を周知徹底します。

コラム

「SECURITY ACTION」二つ星へステップアップ！

デジタル社会の進展に伴い、情報の取り扱いに関して安心して利用できる、発注できる、取引できる会社であることが求められるようになってきました。しかし、顧客や相手の会社に、自社が情報セキュリティに取り組んでいるかどうかを具体的に示すのは、とても難しいことです。顧客や取引先に情報セキュリティ対策への取り組みを明確に伝えるために、「二つ星」を宣言することで、信頼を獲得することが期待できます。

「二つ星」は、「3. 組織的な取り組みを開始する」を実施したことを宣言するものです。

●「5分でできる！情報セキュリティ自社診断」で自社の状況を把握
●「情報セキュリティ基本方針」を定め、外部に公開

宣言方法や「一つ星」からのステップアップについては公式サイトをご確認ください。

●SECURITY ACTION公式サイト
https://www.ipa.go.jp/security/security-action/

4 本格的に取り組む

自社に適した対策を実行して効果をあげるには、まず、自社にどのような情報セキュリティリスク（事故が発生したとき事業へ損害を与える危険性のこと。以下、「リスク」といいます。）があるかを考えます。経営者が懸念する情報セキュリティ上の重大事故やその関連業務などを踏まえ、事業へ大きな損害を与える事故を防ぐための対策を決めて、具体的に記述します。（対策を記述した文書のことを、以下、「規程」といいます。）

(1) 管理体制の構築

①責任分担と連絡体制の整備

P.20(1)情報セキュリティ基本方針の作成と周知にて作成した情報セキュリティ基本方針を具体的に実現するための、情報セキュリティ対策を推進する管理体制を決めます（表6）。情報セキュリティ責任者から部門責任者を通じて従業員への情報の伝達経路を確立し、また情報セキュリティ上の事故などが発生した場合は、情報セキュリティ責任者へ状況が迅速に報告されるような連絡体制を整備することが重要です。すでに個人情報保護管理体制（特定個人情報事務取扱担当者、個人情報苦情申出先）などが決まっている場合は、既存の管理体制との整合をとるようにしましょう。

【表6】情報セキュリティ管理のための役割と責任分担（例）

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です。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、全責任を負います。
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です。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と権限を有します。
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・導入を行います。
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・実施します。
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点検します。

なお、上記の責任者や管理者がそれぞれの役割を果たすためには、情報セキュリティに関する知識や経験も必要です。知識の習得や経験には時間も必要になるため、中長期の視点で要員を育成することも考えましょう。

また、小規模な企業などでは、表6の例にとらわれずに、実効的な体制（役割分担）を独自に考えることもあり得るでしょうが、誰か一人に情報セキュリティ対策の全てを任せてしまうような体制は望ましいものではありません。

②緊急時対応体制の整備

事業や顧客などに大きな影響があるインシデントが発生した場合に、迅速に対応するための体制をあらかじめ決めておきます（表7）。対応を誤ったり、遅れると、被害が拡大

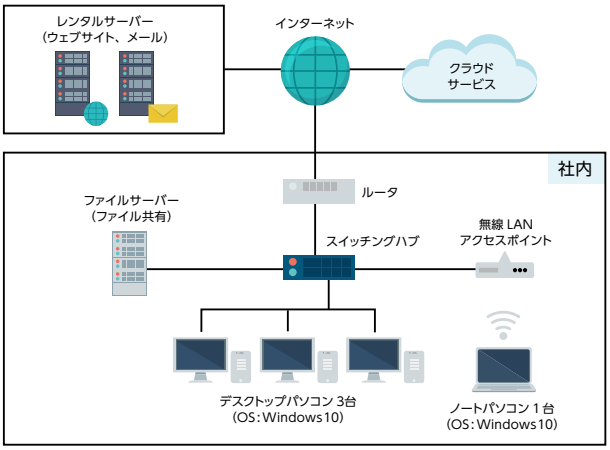
したり、復旧がうまくいかずに、取り返しのつかないことになるため、誰が何をするか役割や手順を明確に決めておく必要があります。また、組織内外の緊急連絡先・伝達ルートを整備し、周知しておくことも重要です。加えて、緊急時対応に関する話し合いや訓練などを実施し、実際に決めたとおりに動けるのかを確認するようにしましょう。関係者やIT製品のメーカー、保守ベンダー等への連絡先もまとめておきます。業務システムが使えなくなるような事故においては、メールや連絡先を確認するためのウェブ閲覧もできなくなる可能性があるため、連絡の代替手段も確認しておきましょう。

【表7】緊急時対応体制の役割と責任（例）

役職名	役割と責任
情報セキュリティ責任者 （例：代表取締役）	事故の影響を判断し、対応について意思決定します。
情報セキュリティ部門責任者 （例：管理部長、営業部長）	・事故の原因を調べて情報セキュリティ責任者に報告します。 ・情報セキュリティ責任者の判断・意思決定に基づき適切な処置を行います。 ・事故の原因や被害が情報システムに関係する場合はシステム管理者と連携して適切な処置を行います。
システム管理者 （例：管理部長兼務）	事故の原因や被害が情報システムに関係する場合は情報セキュリティ部門責任者と連携して適切な処置を行います。
事故・異常を発見した従業員	事故や異常の内容を情報セキュリティ部門責任者に報告します。

(2) デジタルトランスフォーメーション(DX)の推進と情報セキュリティの予算化

中小企業においても競争力維持・強化のために、デジタルトランスフォーメーション(DX[9])を進めていくことが求められています。昨今はクラウドサービスなどデジタル技術やインターネットの活用が多様化し、それに伴いリスクも複雑化しています。そこで、より有効なセキュリティ対策のために、自社の情報システムについて、インターネットとの接続状況を図にするなどして対策を検討するとともに、予算を確保する必要があります。



9 ▲DX(Digital Transformation)　企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。

(3) 情報セキュリティ規程の作成

企業を取り巻くリスクは、事業内容や取り扱う情報、職場環境、ITの利用状況などによっても異なることがあり、汎用的な規程をそのまま使っても、自社に適さないことが考えられます。ここでは、効率的に自社に適した規程を作成する方法を解説します。

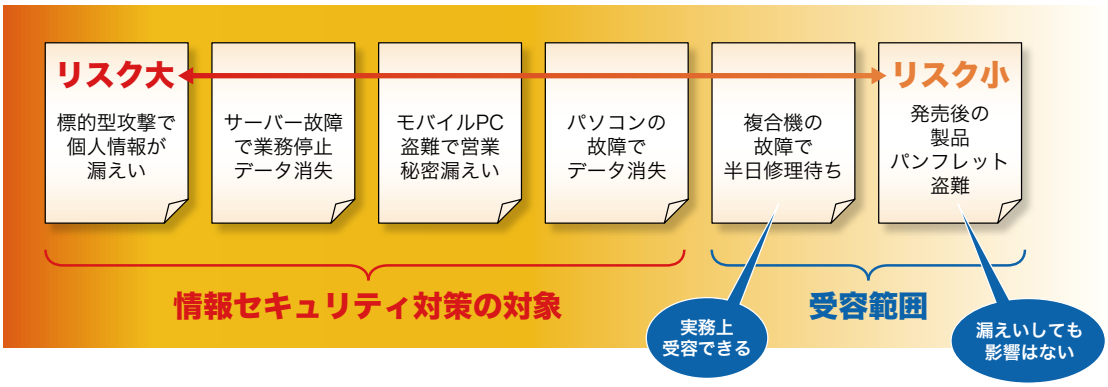
①対応すべきリスクの特定

経営者が懸念する情報セキュリティの重大事故などを念頭に、何が起こらないようにするべきかを考えます。この時、以下のような状況を併せて考えることで、対応すべきリスクを把握します。

- ●関連する業務や情報に係る外部状況(法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など)
- ●内部状況(経営方針・情報セキュリティ方針、管理体制、情報システムの利用状況など)

②対策の決定

全てのリスクに対応しようとすると、費用が多額になったり、仕事が非効率になったりすることがあります。そこで、いつ事故が起きてもおかしくない、あるいは事故が起きると大きな被害になるなど、リスクが大きなものを優先して対策を実施し、事故が起きる可能性が小さいか、発生しても被害が軽微であるなど、リスクが小さなものについては、現状のままにするなど、合理的に対応します。



③規程の作成

②で決定した対策を文書化した規程を作成します。決定した対策を一から文書化するのは経験がないと難しいため、**「情報セキュリティ関連規程（サンプル）」（付録５、概要は表８）**を参考に、自社に適した規程にするために修正を加えます（表８）。

【表８】情報セキュリティ関連規程（サンプル）の概要

	名　称	概　要
1	組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定めます。
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
4	アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルールを定めます。
5	物理的対策	セキュリティを保つべきオフィス、部屋及び施設などの領域設定や領域内での注意事項などのルールを定めます。
6	IT 機器利用	IT 機器やソフトウェアの利用などのルールを定めます。
7	IT 基盤運用管理	サーバーやネットワーク等の IT インフラに関するルールを定めます。
8	システム開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定めます。
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。委託先チェックリストのサンプルが付属します。
10	情報セキュリティインシデント対応ならびに事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。
11	テレワークにおける対策	テレワークのセキュリティ対策についてルールを定めます。

サンプル文中の赤字、青字部分を自社向けに書き換えれば、規程が完成します。なお、サンプルに明記されていなくても必要な対策や有効な対策があれば、追記を行ってください。

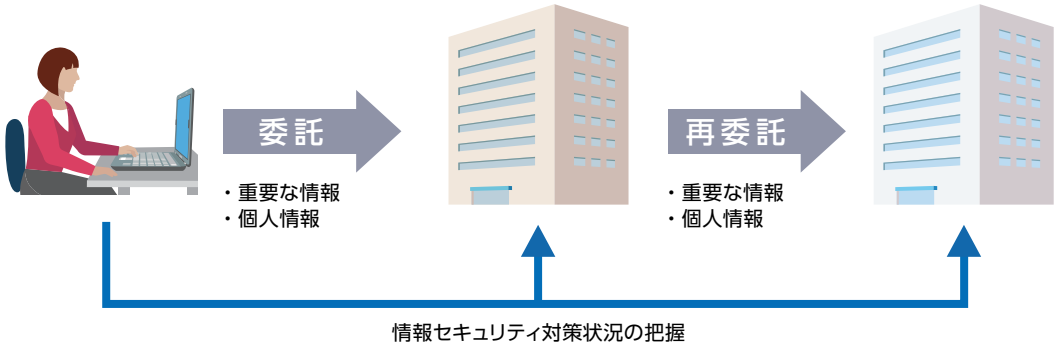
(4) 委託時の対策

社内業務の一部または全部を外部に委託したり、レンタルサーバーやクラウドサービスなどの外部サービスを利用することが一般的になっています。重要な情報を渡したり、処理を依頼する場合には、委託先にも情報セキュリティ対策を実施してもらう必要があります。

直接指示することが難しい外部の組織に、対策を実施してもらうには、取引条件のひとつとして契約書や覚書などに具体的な対策を明記します。個別に契約や覚書を交わすことができない場合は、委託先のサービス規約や情報セキュリティに関わる対応方針を確認したうえで選定します。

また、個人情報保護法では、個人データ[10]の取り扱いを委託する場合は、委託先にも情報セキュリティ対策を実施してもらうように監督することが義務付けられています。委託先の状況を把握し、対策が確実に実施されるように委託元が責任をもつ必要があります。

委託先の対策不足で事故が起きた場合には、委託元は管理責任を問われ、委託先は委託元の信頼を失います。重要な情報や個人情報などセキュリティ事故の影響が大きい情報の授受が行われる場合には、委託元は委託先にセキュリティ対策についての要望や期待をしっかりと伝え、受託する側はそれをきちんと理解し、実行する必要があります。



これらを踏まえ、取り扱う情報の種類、委託する業務に適した情報セキュリティ対策を委託先にも実施してもらいます。機密情報や個人情報を取り扱う場合は、「情報セキュリティ関連規程(サンプル)」(付録5)の「業務委託契約に係る機密保持条項」を参考にして、委託先と契約したり、委託先を選定してください。さらに、情報セキュリティ対策が継続して実施されているか、新たな対策が必要になったときに対応しているかなどを随時確認して、委託先の情報セキュリティ対策が維持されているか、責任をもって管理します。

10 ▲個人情報保護法では「個人情報」、「要配慮個人情報」、「個人情報データベース等」「個人データ」、「保有個人データ」、「個人関連情報」、「仮名加工情報」、「匿名加工情報」等の語を使い分けており、個人情報取扱事業者等に課される義務はそれぞれ異なるので、注意を要します。

コラム

委託と受託

「委託」とは他者に業務を行ってもらうことで、外注、委任、準委任、アウトソーシングなどということもあります。「受託」とは他者の業務を引き受けることです。また、仕事の完成を約する「請負」を意味することもあります。

どのような会社でも事業を行ううえで、全ての業務を自社で行うことは難しいため、委託している業務があり、委託とそれを引き受ける受託とで成り立っています。また、業務を委託するときには、委託元と委託先との間で情報の授受が発生します。

例えば、外部の工場に部品の製造を委託する場合は設計図、税理士に決算書の作成を委託する場合は売上伝票や出金伝票、運送会社に商品の配送を委託する場合は顧客の住所・氏名などの個人情報がそれぞれ授受されます。

このように重要な情報や個人情報を渡す場合に、委託先が対策を怠っていれば、漏えいや改ざんなどの事故が起きやすくなります。さらにこれらのような事故が委託先で起きた場合であっても、委託元の管理責任が問われることもあります。また、委託先がサイバー攻撃を受け、ウイルスに感染したりシステムが停止したりすると、受発注や出荷の停止を引き起こし、その被害が自社の事業に影響を与える場合があります。

業務を受託する場合においては、発注元が求めるセキュリティ対策を実施できることを示す必要があります。自己点検の結果や、「SECURITY ACTION」（自己宣言）のロゴマークを提示する、具体的な規程の内容や、システム上の対策例を説明するなどにより、相手の信頼を得ましょう。

サプライチェーン

近年は、グローバル化やデジタル化が進んだことで、委託や受託の関係も複雑化しています。例えば、部品の製造を受託した場合に原材料の海外調達や部品加工の委託・再委託、完成部品の運送委託などが行われていたりします。このような調達や製造、販売などの一連の流れは「サプライチェーン」と呼ばれていますが、サプライチェーンの中でも情報セキュリティ対策が弱い企業が狙われサイバー攻撃を受けることで、その影響がサプライチェーン内の他の企業にも影響を与えることから、業務を受託する中小企業もサプライチェーンを構成する一員であることを自覚し、情報セキュリティ対策に取組むことが求められています。

【パートナーシップ構築宣言】（内閣府・中小企業庁）
https://www.biz-partnership.jp/

「パートナーシップ構築宣言」は、サプライチェーンの取引先や価値創造を図る事業者の皆様との連携・共存共栄を進め、新たなパートナーシップを構築することを「発注者」側の立場から企業の代表者の名前で宣言するものです。ポータルサイトで「宣言」を公表する企業は指定のロゴマークを広報等に使用することができます。

同宣言には、1．サプライチェーン全体の共存共栄と規模・系列等を超えた新たな連携、2．親事業者と下請事業者との望ましい取引慣行（下請中小企業振興法に基づく「振興基準」）の遵守、を盛り込むことになっています。各企業は積極的に取り組む内容（例：企業間の連携、IT 実装支援（サイバーセキュリティ対策の助言・支援を含む）、専門人材マッチング、グリーン化の取組、健康経営に関する取組）を選択することができ、選択した項目毎に取組内容を具体的に明記することが求められます。

(5) 点検と改善

情報セキュリティの点検とは、計画した情報セキュリティ対策が、本当に実行されているか、見落としている対策はないか、対策がセキュリティ事故防止のために役に立っているか、を確認することです。点検の基準には以下を用いることができます。

その１)「情報セキュリティ５か条」や「５分でできる！情報セキュリティ自社診断」に基づく点検

点検基準例

☑「情報セキュリティ５か条」No.1の対策例を基準にする。

パソコンのWindowsUpdateが「更新プログラムを自動的にインストールする」に設定されていて、更新日が直近の日付であるか

☑「５分でできる！情報セキュリティ自社診断」No.20の対策例を基準にする。

従業員に情報セキュリティ事故のニュースを周知したり、情報セキュリティ啓発サイトの新着情報を配信するなどしているか

その２)策定した情報セキュリティ対策に関するルール・規程に基づく点検

点検基準例

☑ウイルス感染時の初期対応のルールを基準にする。

社内規程の中で、ウイルス感染時の対応に関する記述を理解しているか
(「情報セキュリティ関連規程(サンプル)」No.10「情報セキュリティインシデント対応ならびに事業継続管理」の該当項目を参照)

点検には、以下の方法があります。

- ●質問(インタビュー)：従業員や委託先の管理者などに直接質問して回答してもらう
- ●閲覧(レビュー)：関連する文書や記録、パソコンの設定画面など対策を実行した証拠となるものを確認する
- ●観察(視察)：点検の対象となる職場に出向き、従業員が規程や標準規格などに従った行動をしていることを確認する
- ●技術診断：専用ソフトウェアなどを使ってコンピュータやネットワークのセキュリティ対策が実行されているかを確認する
- ●チェックリスト：チェックリストや質問書を配付して回答してもらう

点検の結果を経営者に報告し、経営者の意図するセキュリティ対策が実現できているかの確認と評価をすることが重要です。経営者の評価を得ることで、場合によってはリスクの特定に戻って対策の見直しをするなどにより、取り組みの精度を高めていくことになります。

なお、営業秘密や個人情報等の特に十分な対策が必要な場合には、第三者による情報セキュリティ監査[11]を行うことも検討します。

11 ▲一般に、点検は点検対象業務に従事している関係者自身が実施するのに対し、監査は監査対象業務に従事していない、独立した監査担当者によって実施されるため、より客観的な確認を行う必要がある場合には監査が適しています。

コラム

情報セキュリティ点検の実施例

「情報セキュリティ５か条」に取り組んでSECURITY ACTION一つ星を自己宣言している会社が、「情報セキュリティ５か条」を基準にして点検するときの実施例です。

①No.1「OSやソフトウェアは常に最新の状態にしよう！」について社員の一人に、質問と閲覧で点検します。


「情報セキュリティ５か条」では OS やソフトウェアは常に最新の状態にすることになっていますが、持出し用のノートパソコンの OS やソフトウェアは最新の状態でしょうか？」


「ノートパソコンをしばらく使っていないので、分かりません。」


「では、Windows Update の更新プログラムのインストール履歴を見せてください。」


「（ノートパソコンの画面に更新プログラムのインストール履歴を表示）」


「画面を見ると最後のインストール履歴が２か月前になっていますが、理由はわかりますか？」


「Windows Update は自動更新に設定していますが、このノートパソコンは社外に出かけるときだけに使うので、普段はネットワークに接続していません。それで更新されていないのだと思います。明日、お客様の事務所に伺い、このノートパソコンをお客様の LAN につないでメールを使いますので、それが終わったら更新しようと思います。」

②ノートパソコンを持ち出すことがある他の社員に、質問やパソコンの画面を見せてもらい、その回答や観察の結果から総合的に判定します。

この例では、「情報セキュリティ５か条」の「OSやソフトは常に最新の状態にしよう！」を実行できていないパソコンがあることを発見しました。その状態でお客様のLANに接続する予定であったことから、影響が社外に及ぶ可能性があり、リスクが大きいと言えます。このようにリスクが大きいと考えられる場合は、すぐに是正するよう助言します。

点検というと難しく思えるかもしれませんが、スポーツの審判のように、ルールを基準とし、選手が基準を満たしているか判定することと同じです。客観的に評価、判定することで、気付かなかった不備が明確になりますので、情報セキュリティのレベルアップにはとても役に立ちます。

5 より強固にするための方策

ITの普及に伴い情報セキュリティ対策も重要視されています。技術の悪用や技術的な攻撃を防ぐためには、人的な注意や対策だけでは限界があり、技術的対策を強化したり、外部の専門サービスを利用する必要があります。

ここでは、事業でコンピュータやインターネットを活用している企業が、より強固な情報セキュリティ対策に取り組むために必要とされる技術的対策や、対策の導き出し方など以下の８つの区分について説明します。

(1)情報収集と共有

情報セキュリティに関する情報収集の方法と情報共有の枠組みについて説明します。

(2)ウェブサイトの情報セキュリティ

ウェブサイトを安全に構築し、運用するためのポイントを説明します。

(3)クラウドサービスの情報セキュリティ

クラウドサービスを安全に利用するためのポイントを説明します。

(4)テレワークの情報セキュリティ

テレワークを安全に実施するためのポイントを説明します。

(5)セキュリティインシデント対応

セキュリティインシデント発生時の対応に関するポイントを説明します。

(6)セキュリティサービス例と活用

情報セキュリティに関する外部サービスを説明します。

(7)技術的対策例と活用

ITを活用する際の技術的対策について説明します。

(8)詳細リスク分析の実施方法

「リスク分析シート」(付録７)を活用した詳細リスク分析の実施方法を説明します。

(1)情報収集と共有

情報セキュリティに関する脅威や攻撃の手口を知って組織内に共有することは、組織の対策レベルの向上につながります。また、その情報を社外の関係者と共有することで、社会全体のセキュリティレベルの向上にもつながります。ここでは、情報セキュリティに関する情報収集の方法と情報共有の枠組みを説明します。

①情報収集の方法

情報収集で重要なことは、定常的に情報収集ができる方法を整備することです。そのためには、情報を得る先を理解し、必要な情報が自動的に得られる仕組みを構築します。

例えば、情報セキュリティの専門機関、IT製品のメーカーや保守ベンダーなどのメールマガジンやSNS[12]に登録したり、セミナーに参加して積極的な情報収集を行います。

②情報共有の枠組み

近年、取引先や同業者を経由したサイバー攻撃が増加しています。そこで、収集した情報は社内の関係者だけでなく、取引先や同業者に対しても共有することで、対策の向上が期待できます。共有する情報に機密情報が含まれる可能性がある場合は、守秘義務契約を交わします。情報共有の枠組みとしては日本シーサート協議会の他、業界別のISAC[13]が組織されている場合があります。

参考情報

(情報収集の方法)

■ここからセキュリティ！
https://www.ipa.go.jp/security/kokokara/

■ IPA セキュリティセンター
https://www.ipa.go.jp/security/

■ IPA サイバーセキュリティ注意喚起サービス「icat for JSON」
https://www.ipa.go.jp/security/vuln/icat.html

■一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
https://www.jpcert.or.jp/

■警察庁 @police
https://www.npa.go.jp/bureau/cyber/index.html

■内閣サイバーセキュリティセンター
https://www.nisc.go.jp/

(情報共有の考え方・枠組み)

■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

■一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会（日本シーサート協議会）
https://www.nca.gr.jp/

12 ▲SNSは、ソーシャルネットワーキングサービス(Social Networking Service)の略で、登録された利用者同士が交流できるWebサイトの会員制サービスのことです。(総務省　国民のためのサイバーセキュリティサイト)

13 ▲**ISAC(Information Sharing and Analysis Center)**　同業界の事業者同士でサイバーセキュリティに関する情報の共有・分析などを行う組織

(2) ウェブサイトの情報セキュリティ

自社のウェブサイトを持ち活用することは顧客獲得や売上増に直結するため、多くの中小企業でもウェブサイトを開設しています。しかし、世界中の誰でもアクセスできるため、攻撃の対象になりやすく、顧客情報の漏えいや、不正サイトに誘導するなどの改ざんによって、自社だけでなく、利用者にも被害が発生することが懸念されます。そのため、ウェブサイトを活用する際は同時に対策を講じる必要があります。ここでは、ウェブサイトの運営形態の検討から実際に運営するまでの３つの段階に分けて検討事項を説明します。

ウェブサイト運営形態の検討

ウェブサイトでの運営形態によってセキュリティ対策が異なるため、**自社の状態に見合った運営形態**を検討しましょう。

ウェブサイトの構築

ウェブサイトの**技術的な脆弱性を認識**したうえで、必要なセキュリティ対策を設計・開発の段階から検討しましょう。

ウェブサイトの運営

運用開始後に発覚した情報セキュリティ上の問題にも適切に対応し、**ウェブサイトの安全性を維持向上**しましょう。

①ウェブサイト運営形態の検討

ウェブサイトをどのような形態で運営するかによって、費用が変化するのはもちろん、サイト運営者が実施する作業内容が異なるため、求められる技術レベルも変化します。また、運営形態ごとにウェブサイト上でどのような機能を提供できるか、ウェブサイトをどこまで自由に変更できるか、どのような情報セキュリティ対策が必要になるかについても異なります。特に企業のウェブサイトでは個人情報を取り扱うことも多く、サイト運営者は情報セキュリティが継続的に維持され、最新の脅威に対し対策ができているかどうかに気を配る必要があります。運営者はウェブサイトを構築する前に表９に示す運営形態ごとの特徴を理解し、組織の状況に応じた運営形態を選定する必要があります。

【表９】運営形態ごとの特徴

運営形態	特徴
サーバー自社設置（オンプレミス）	ネットワークやサーバーなどの用意から、そのうえで稼動するウェブサイトの構築・運用まで、全て自社で行う運営形態。全ての情報セキュリティ対策を自社で行う必要があります。
レンタルサーバー・クラウドサービス（PaaS）	ネットワークやサーバーなどは外部サービスを利用し、ウェブサイトの構築・運用のみ自社で行う運営形態。ネットワークやサーバーの情報セキュリティ対策は外部サービスが行うため、ウェブサイトの構築・運用面に関わる情報セキュリティ対策のみ自社で行う必要があります。
ショッピングモール・ASP	ウェブサイトの開設に必要な機能や運用を一括して外部サービスを利用し、ウェブサイトに掲載する文章や画像、動画などのコンテンツだけを自社で更新する運営形態。外部サービスを利用するための認証情報を、ウェブサイト運営者が適切に管理する必要があります。

②ウェブサイトの構築

ウェブサイトの「安全上の欠陥」（脆弱性）が狙われる事件が後を絶ちません。ウェブサイトの安全を維持するためには、サーバーOSやソフトウェアに対して脆弱性修正パッチの適用や安全な設定などを維持することが重要です。

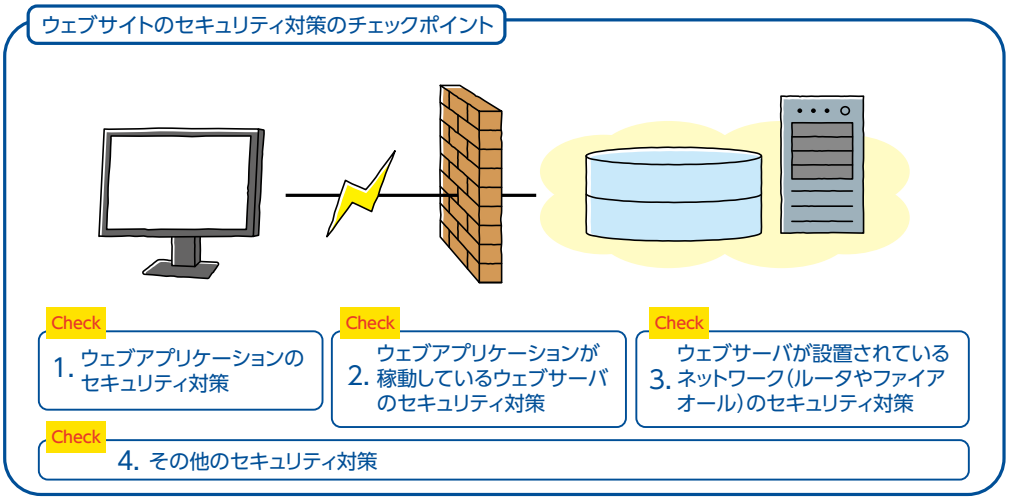
しかし、独自に開発する「ウェブアプリケーション[14]」については、情報セキュリティ上の問題が発覚した場合、サービスの継続提供やコストなどの観点から、設計レベルから修正することは難しい場合が少なくなく、軽減策で済まさざるをえないこともあります。

そのため、開発段階において、可能な限り脆弱性を解消することが望まれます。また、開発を委託して脆弱性が原因で事故が発生した場合には、発注者の責任を問われることもあるため、脆弱性対策については要求仕様に盛り込む必要があります。ウェブアプリケーションを開発する場合、参考情報に示す「安全なウェブサイトの作り方」を参照し、必ず脆弱性の対策を実施してください。

③ウェブサイトの運営

安全にウェブサイトを運営するためには、下図が示す対象ごとに適切な対策を実施することが必要です。どれが欠けても、ウェブサイトの安全性は確保できません。

参考情報に示す「安全なウェブサイトの運用管理に向けての20ヶ条」を参照して、対策がとられていない項目があった場合には早急に対策をしてください。



ウェブサイトのセキュリティ対策のチェックポイント

[1] ウェブアプリケーションのセキュリティ対策

[2] ウェブアプリケーションが稼働しているウェブサーバーのセキュリティ対策

[3] ウェブサーバーが設置されているルーターやファイアウォールのセキュリティ対策

[4] その他のセキュリティ対策

14▲インターネットなどのネットワークを介して使用するアプリケーションソフトウェア

【重要】ECサイト[15]のセキュリティ対策

インターネット上に店舗を構え、商品やサービスを販売するECサイトの活用が中小企業でも進んでいます。一方、インターネット上の店舗は世界中からアクセス可能であり、絶えずサイバー攻撃に晒されています。そのため、中小企業がECサイトで取り扱うクレジットカード情報や個人情報・仕入先情報などの漏えい事件が多数発生しています。さらに、対策としてカード情報を「非保持化[16]」しているにも関わらず、購入者に偽の入力画面を表示し、入力させた情報を盗むという巧妙な手口により、被害が増加しています。

ECサイトが被害を受けた場合は、サイトの一時閉鎖や原因調査に加え、顧客への謝罪や事故対応費用の負担など経済的損失が発生します。企業としての信頼も大きく損なわれ、売上が回復するまで多くの時間を要します。被害を防ぐために、表10に示す運営形態ごとのセキュリティ対策を参考に、自社の対策を確認し、十分な対策を講じてください。詳細な対策については、参考情報にあるECサイト構築・運用セキュリティガイドライン（IPA）をご参照ください。

【表10】ECサイト運営形態とセキュリティ対策

EC サイト運営形態		セキュリティ対策 A：構築・運営の各段階で対策が必要 B：公表される情報をもとに脆弱性の修正が必要 C：パッケージ製品 / サービス提供者の情報を元に脆弱性の修正が必要 D：運営事業者のセキュリティ対策を確認		
		ウェブアプリケーション	ウェブサーバー	ネットワーク
1	EC サイトを自社で独自開発	A	サーバー自社設置：A または B レンタル / クラウドサーバー：C	
2	EC サイト用オープンソースソフトウェアを利用	B		
3	EC サイト用パッケージを利用	C		
4	EC サイト用クラウドサービス /ASP を利用	D	D	D
5	オンラインショッピングモールに出店・出品	D	D	D

15▲EC（Electronic Commerce電子商取引）「ネットショップ」「オンラインショップ」「ネット通販サイト」などの呼称があります。いくつかある決済方法のうちクレジットカード払いが約8割（総務省　令和3年情報通信白書）で最も多くなっています。

16▲自社で保有する機器・ネットワークにおいて「カード情報」を「保存」、「処理」、「通過」しないこと。P.8表2割賦販売法参照

参考情報

■安全なウェブサイトの作り方（IPA）
https://www.ipa.go.jp/security/vuln/websecurity/about.html

■安全なウェブサイトの運用管理に向けての20ヶ条（IPA）
https://www.ipa.go.jp/security/vuln/websecurity/sitecheck.html

■ECサイト構築・運用セキュリティガイドライン（IPA）
https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html

■クレジットカード・セキュリティガイドライン（一般財団法人日本クレジット協会）
https://www.j-credit.or.jp/security/document/

(3) クラウドサービスの情報セキュリティ

インターネットと情報技術の発展・普及により、社内に情報システムを構築せずに、データ共有や機能拡張ができるクラウドサービスの利用が近年著しく進展しています。クラウド化によって社内システムで発生していた費用や手間が削減され、テレワークでも利用できるなどメリットも多く、今後も普及が進むと考えられます。その一方で、情報システムの一部が、サービスを提供する事業者の管理下に置かれることになるため、社内システムとは異なる観点で情報セキュリティ対策を講じる必要があります。ここではクラウドサービスの選定から運用するときのセキュリティ対策まで3つの段階に分けて検討事項を説明します。

クラウドサービスの選定

クラウド化する業務によって重視すべきセキュリティ対策は異なるため、**業務のセキュリティ要件に見合ったサービス**を選定しましょう。

クラウドサービスの運用

クラウドサービスは**提供者と利用者が連携して運用**するため、その特性を理解して運用しましょう。

クラウドサービスのセキュリティ対策

クラウドサービス利用者が対応すべきセキュリティ対策を理解して実施しましょう。

①クラウドサービスの選定

クラウドサービスは、提供される情報システム（ハードウェアやソフトウェア）の範囲によって、次の3形態に大別されます。

（クラウドサービスの3形態）

- **SaaS（Software as a Service サース）**：会計アプリケーションやオフィスソフト、ファイルサーバーなど、一般に利用されているアプリケーションソフトをウェブサービスとして提供します。
- **PaaS（Platform as a Service パース）**：OSやデータベース管理システムなどのミドルウェアを提供します。アプリケーションソフトは別途導入しなければなりません。
- **IaaS（Infrastructure as a Service イアース）**：仮想のサーバーやメモリなどのハードウェアやネットワークなどのシステム基盤のみを提供します。

本ガイドラインではSaaSの利用を念頭に置いた情報セキュリティ対策について説明します。SaaS形態のクラウドサービスは、一つのシステムを複数の企業が利用します。画面レイアウトや表示項目など利用企業ごとの要求に応じてカスタマイズできるものもありますが、セキュリティ対策についてはサービス提供者に依存する部分があります。このため、クラウド化する業務に必要とされるセキュリティ対策をあらかじめ検討し、それらを備えたクラウドサービスを選定する必要があります。

②クラウドサービスの運用

社内で構築した情報システムとは異なり、クラウドサービスは他者が提供する情報システムを利用するため、セキュリティ対策を実施するためには、適切なサービスを選定すると同時に、利用者側も運用上必要な対策を実施します。

クラウドサービスでは、データ処理・保存は全てサービス提供者が管理するサーバーで実行されるので利用者の財務や顧客データなど重要な情報は提供者に預ける状態になります。このため、サーバーやネットワークのセキュリティ対策は主にサービス提供者が実施することになります。

サービス利用者は、インターネットに接続するパソコン・スマートフォンなどの端末を使い、サーバーに対してデータの入出力だけを実行します。このことから利用者の役割と責任範囲は、直接対策を講じることができるパソコン・スマートフォンなどの端末やネットワーク機器、それらにインストールされたソフトウェアに限定されます。

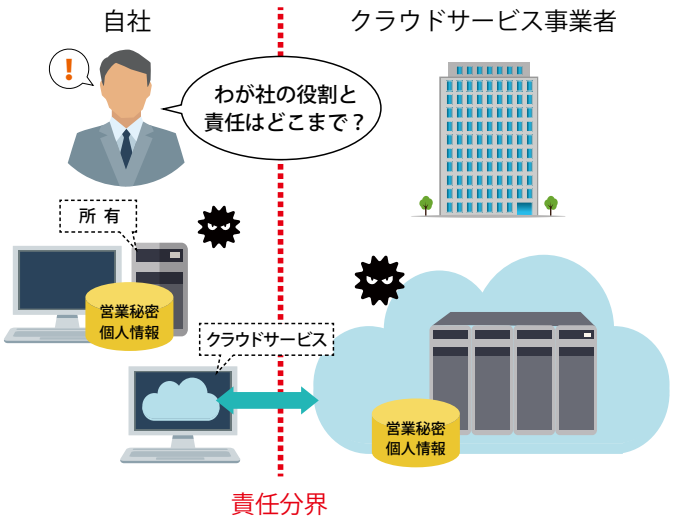
そのため、社内システムよりも、ハードウェアやソフトウェアへの対策に関する負担は軽減されます。しかし、クラウドサービスはインターネットを使うため、いつでも、どこからでも、誰でもアクセス可能であることが、社内システムとは根本的に異なり、インターネット特有の脅威やリスクを考慮して、運用上のセキュリティ対策を検討する必要があります。

③クラウドサービスのセキュリティ対策

クラウドサービスのセキュリティ対策は、以下の観点で検討して、状況に応じた適切な対策を実施してください。

- ●クラウドサービス事業者のセキュリティ対策を把握し、自社のセキュリティに関する期待を満たしたサービスを利用する。
- ●利用者である自社の役割・責任を把握し、自社でしかできない対策を的確に実行する。

詳細は、次頁表11に示すクラウドサービス安全利用のための15項目を参考に、自社の目的や運用計画などに適したクラウドサービスを利用してください。15項目の解説は、**「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６)**を参照してください。



【表11】中小企業のためのクラウドサービス安全利用のための15項目

NO.	項目	内容
Ⅰ．選定するときのポイント		
1	どの業務で利用するか明確にする	どの業務をクラウドサービスで行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましたか？
2	クラウドサービスの種類を選ぶ	業務に適したクラウドサービスを選定し、どのようなメリットがあるか確認しましたか？
3	取り扱う情報の重要度を確認する	クラウドサービスで取り扱う情報が漏えい、改ざん、消失したり、サービスが停止した場合の影響を確認しましたか？
4	セキュリティのルールと矛盾しないようにする	自社のルールとクラウドサービス活用との間に矛盾や不一致が生じませんか？
5	クラウド事業者の信頼性を確認する	クラウドサービスを提供する事業者は信頼できる事業者ですか？
6	クラウドサービスの安全・信頼性を確認する	サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証は示されていますか？
Ⅱ．運用するときのポイント		
7	管理担当者を決める	クラウドサービスの特性を理解した管理担当者を社内に確保していますか？
8	利用者の範囲を決める	クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？
9	利用者の認証を厳格に行う	パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど）
10	バックアップに責任を持つ	サービス停止やデータの消失・改ざんなどに備えて、重要情報を手元に確保して必要なときに使えるようにしていますか？
Ⅲ．セキュリティ管理のポイント		
11	付帯するセキュリティ対策を確認する	サービスに付帯するセキュリティ対策が具体的に公開されていますか？
12	利用者サポートの体制を確認する	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
13	利用終了時のデータを確保する	サービスの利用が終了したときの、データの取り扱い条件について確認しましたか？
14	適用法令や契約条件を確認する	個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？
15	データ保存先の地理的所在地を確認する	データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？

※ No15クラウドサービスのサーバーが日本国外に設置されている場合、扱うデータによってサーバーの設置国・地域の法規制が適用されることがあります。
※ No6・11・12・13はスマートSMEサポーター（認定情報処理支援機関）の開示情報で確認することができます。

コラム

クラウドサービス選択時に参考となる制度等

クラウドサービス事業者が適切なデータ保護やセキュリティ対策を実施していることをマークとして表示する制度があります。いずれもURL記載のページ内でそれぞれの条件を満たすサービスが紹介されており、選定時の参考として利用することができます。

●ISMSクラウドセキュリティ認証

（一般社団法人情報マネジメントシステム認定センター）

https://isms.jp/isms.html

ISMS（Information Security Management System。ISO/IEC27001）認証に加えて、クラウドサービス固有の管理策（ISO/IEC 27017）が適切に導入、実施されていることを認証するものです。

●クラウド情報セキュリティ監査制度

（特定非営利活動法人日本セキュリティ監査協会）

https://jcispa.jasa.jp/cloud_security/

クラウドサービス事業者が基本的な要件を満たす情報セキュリティ対策を実施していることを監査し、その結果をCSマークの表示許諾を通じて利用者に対し、安全性が確保されていることを公開する制度です。外部監査と内部監査で「ゴールド」と「シルバー」の２種類があります。

●クラウドサービスの安全・信頼性に係る情報開示認定制度

（一般社団法人日本クラウド産業協会（ASPIC））

https://www.aspicjapan.org/nintei/

クラウドサービスの利用を考えている企業や地方公共団体などが、事業者やサービスを比較、評価、選択する際に必要な「安全・信頼性の情報開示基準を満たしているサービス」を認定するものです。

●ISMAP　政府情報システムのためのセキュリティ評価制度

https://www.ismap.go.jp/csm

ISMAP（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度です。

(4)テレワークの情報セキュリティ

中小企業においてもテレワークの普及が進んでいます。テレワークは、DXの推進や多様な人材の柔軟な働き方を実現するとともに非常時の業務継続にも有効であり、うまく活用することが企業にとって重要です。

しかし、従業員の自宅やサテライトオフィスなど、企業の管理下にない環境で業務を行うことにより、従来の企業内部の管理だけでは、セキュリティを守ることが難しくなっています。さらに、自宅のパソコンやスマートフォンを業務に利用することで従来と異なるリスクも想定され、セキュリティ対策を見直す必要があります。ここではテレワークのセキュリティ対策について３つの段階に分けて検討事項を説明します。

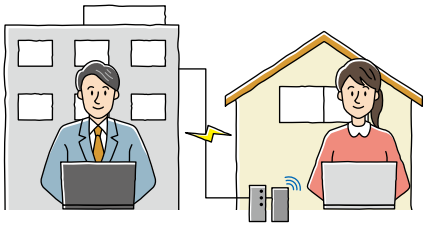
テレワークの方針検討	テレワークのセキュリティ対策	テレワークの運用
テレワークを行う際のシステム構成や機器をどうするか方針を検討しましょう。	テレワークで利用するシステム構成や機器によって必要なセキュリティ対策を構築しましょう。	テレワークに関するルールを定め、テレワーク勤務者に周知し、事故に気をつけて安全に運用しましょう。

①テレワークの方針検討

テレワークを行う場合は、企業としてテレワーク環境(テレワークを行うパソコンやスマートフォンなどのテレワーク端末やネットワーク環境、テレワークを行うためのシステム方式など)をどの程度提供できるか検討します。企業として十分なテレワーク環境を提供できた方が、セキュリティを確保するうえでも望ましいのですが、緊急対応としてテレワークを実施するなど何らかの理由があって十分なテレワーク環境が提供できない場合は、企業は従業員のテレワーク環境構築を支援しましょう。

テレワークを行うための主なシステム方式は以下のとおりです。システム方式によって費用や運用負荷、セキュリティ対策の留意点が異なるため、自社の状況に応じたシステム方式を検討する必要があります。

- **VPN方式**[17]:テレワーク端末から社内ネットワークに通信を暗号化して接続する方式
- **リモートデスクトップ方式**:テレワーク端末から社内パソコン等の端末に接続する方式
- **スタンドアロン(持ち帰り)方式**:テレワーク端末



17▲VPN(Virtual Private Network)はインターネット上で保護された仮想的な専用線環境を構築する技術。テレワークにおけるネットワーク側のセキュリティ対策として、VPNもよく使われるようになりました。VPNは、端末から企業内までの通信を丸ごと暗号化して外部からの侵入等を防ぎ、外部でも企業内と同等のネットワーク環境を使えるようにするものです。外部で業務用端末を安全に利用することができますが、その端末自体がウイルスに感染した、外部から侵入されたといったインシデントが発生すると、VPNを通じて企業内ネットワークにも容易に被害が拡大してしまうデメリットもあります。(総務省 国民のためのサイバーセキュリティサイトから)

を社内ネットワークに接続せずに使用する方式

●**クラウドサービス方式**：インターネット上のクラウドサービスに直接接続する方式

②テレワークのセキュリティ対策

テレワークのセキュリティにおいても、想定される脅威に応じた対策をルールとして定めるとともに、従業員に理解して遵守させるための教育・啓発が必要です。また、ルールだけでは対応できない脅威には専用機器やサービスの導入など技術的対策も必要です。技術的対策については、公的機関のテレワーク専用相談窓口を活用しつつ、IT製品のメーカーや保守ベンダー等の外部専門家に相談し、進めることも有効です。組織の守るべき情報や業務実態などを外部専門家に伝えた上で、脅威を踏まえた適切なセキュリティ対策を検討します。

テレワーク方式ごとのセキュリティ対策における留意点は機器とセキュリティ対策における留意点は以下のとおりです。

●**VPN方式**：テレワーク端末にデータ保存が可能なため、端末の紛失や盗難、不正操作による情報漏えいリスクがあります。防止のためには、テレワーク端末のハードディスクやSSDなどの暗号化やデータの遠隔消去等の対策を行います。

●**リモートデスクトップ方式**：社内パソコンの画面をテレワーク端末画面に随時転送して遠隔操作するため、オフィスと同等に業務を行うことができます。しかし、社内パソコンからテレワーク端末にデータをコピーして保存することも可能なため、端末の紛失や盗難、不正操作による情報漏えいリスクがあります。また、通信環境によっては処理が遅くなるなど操作性が低下し、業務に著しく影響することがあります。防止のためには、社内パソコンからテレワーク端末へのコピーを制限する、操作性低下の影響を事前に確認するなどがあります。

●**スタンドアロン（持ち帰り）方式**：テレワーク端末にデータを保存するため、端末の紛失や盗難、不正操作による情報漏えいリスクがあります。防止のためには、端末のハードディスクやSSDなどの暗号化やデータの遠隔消去等の対策を行います。さらに、必要最低限のデータのみ許可を得て持ち出すことや、インターネットを利用する場合は、ウイルスや不正アクセスへの対策等が必要です。

●**クラウドサービス方式**：テレワーク端末から社内ネットワークを経由せず直接インターネットに接続することから、通信の暗号化やサービスにログインするときの認証強化などの対策が必要となります。使用するサービスのセキュリティ仕様を確認し、サービス提供者に相談するなどして、必要な対策を検討します。テレワーク端末には、ウイルスソフトの導入や、テレワーク端末のハードディスクやSSDなどの暗号化やデータの遠隔消去等の対策を行います。また、クラウドサービス上にデータを保存する場合は、どのようなデータが保存されているのかを把握し、管理する必要があります。

テレワークで利用する機器とセキュリティ対策における留意点は以下のとおりです。

●個人所有のパソコンやスマートフォンをテレワーク端末として利用する場合

会社のパソコンと同様にウイルス対策ソフトの導入・更新を行い、許可された端末だけが社内ネットワークに接続できるようにする端末認証を設定します。また、他者との共有や業務データ保存を制限あるいは禁止します。それが難しい場合は、テレワーク端末のユーザアカウントの別途作成や、業務データの暗号化、遠隔消去等の対策を行います。

●個人の無線LANルーター（Wi-Fiルーター）をテレワークに利用する場合

＜盗聴・不正アクセス対策＞

電波の盗聴対策として通信を暗号化する必要があります。暗号化しても暗号化方式が脆弱な場合は解読可能なため、最も強固な方式を設定します。また、接続するときに入力するパスワードを知られてしまうと強固な暗号化方式であっても解読されたり、接続しているパソコン等に不正アクセスされたりするリスクがあるため、推測されないようにします。

＜無線LANルーターの対策＞

ルーターの管理画面にログインするためのパスワードを知られてしまったり、ファームウェア[18]に脆弱性が存在したりすると、不正アクセスして悪用されるリスクがあります。強固で推測されにくいログインパスワードを使用し、ファームウェアは最新に保つようにします。

●自宅のインターネット回線をテレワークに利用する場合

社内ネットワークに接続する場合はVPN、クラウドサービスを利用したりする場合は、VPNやSSL/TLS[19]などの暗号化通信を利用します。また、メールで重要な情報を添付ファイルで送信する場合は、ファイルを暗号化したりS/MIME[20]などでメールを暗号化したりします。

テレワークを行う場所とそれに応じたセキュリティ対策の留意点は以下の通りです。

●自宅でテレワークを行う場合

離席時に画面をロックし、無断操作ができないようにします。

●不特定多数の人がいるシェアオフィス、ワーケーション[21]先や公共の場でテレワークを行う場合

テレワーク端末を置いたまま離席することは避け、安易に重要情報を画面に表示せず、のぞき見防止フィルターを利用するなどします。

18 ▲**ファームウェア**　機器の基本的な制御を行う内蔵ソフトウェアのこと
19 ▲**SSL/TLS (Secure Socket Layer/Transport Layer Security)**　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
20 ▲**S/MIME(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
21 ▲ワーケーション ワーク（仕事）とバケーション（休暇）を組み合わせた造語（ぞうご）。リゾート地などで休みを取りつつ（または引っ越しして）テレワークをする働き方を指す。（総務省　情報通信用語集から）

③テレワークの運用

経営者はテレワークのセキュリティに関するルールを規程として定めます。責任者は、目の届きにくいテレワーク勤務者に対して規程を周知し、徹底させます。また、不明な点や、ウイルス感染などの事故が疑われる場合は迅速に相談や報告を受けることができるように連絡先や対応体制を整備します。さらに、事故発生時にテレワーク勤務者が戸惑わずに対応できる手順書を作成し、速やかな対応・復旧に備えます。

また、テレワークから職場での業務に戻る際には、所属先の規程やルールを理解し、以下について留意することが必要です。

- ●テレワークに利用していたパソコンを職場に戻す前に、あらかじめOSやソフトウェアを最新の状態にし、ウイルス対策ソフトの定義ファイルを最新の状態にしたうえでパソコン内のウイルスチェックを行ってから、職場のネットワークに接続します。
- ●個人所有のパソコンやスマートフォンをテレワークに利用していた場合、その中に保存された業務データやメールについて、所属先の環境への引き渡しを確認したうえで削除します。個人所有のUSBメモリやハードディスクなどで業務データを持ち運ぶ場合は、紛失しないように注意します。

なお、テレワークのセキュリティ対策は、**付録1「情報セキュリティ5か条」**、**付録3「5分でできる！情報セキュリティ自社診断」の対策例**を参照してください。また、クラウドサービスを利用する場合は、**本編5「より強固にするための方策(3)クラウドサービスの情報セキュリティ」**、**付録6「クラウドサービス安全利用の手引き」**も参照してください。

参考情報

■テレワークを行う際のセキュリティ上の注意事項（IPA）
https://www.ipa.go.jp/security/anshin/measures/telework.html

■ IPA 情報セキュリティ啓発映像　テレワークのセキュリティ対策
https://www.ipa.go.jp/security/videos/list.html

■テレワークセキュリティガイドライン（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

■ NTT 東日本 -IPA「シン・テレワークシステム」向けセキュリティポリシー（一般社団法人ソフトウェア協会）
https://www.saj.or.jp/NEWS/committee/security/200428.html

(5) セキュリティインシデント対応

サイバー攻撃が高度になることに伴い、セキュリティインシデント(情報漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象など)が増加しています。重要な情報を有する場合や取引先に大手企業を含む場合などは自社が標的となる場合もあります。そのため、地震や水害、パンデミックへの対応と同様、情報セキュリティにおいても、事業継続の観点から被害を最小化し、早期に復旧するために、インシデントを想定した備え[22]を行う必要性があります。ここではインシデント発生時の対応について、3つの段階に分けて検討事項を説明します。

検知・初動対応	報告・公表	復旧・再発防止
インシデントを検知した場合は、速やかに情報セキュリティ責任者へ連絡し、被害を拡大させないための初動対応を行いましょう。	顧客や関係者、行政機関、一般・メディア等に対して、必要な場合は適時の報告や情報公開を行いましょう。	システム管理者や外部専門組織と協力して、迅速な復旧作業や根本的な再発防止策を検討しましょう。

①検知・初動対応

インシデントが疑われる兆候や実際の発生を検知したり、外部からの通報を受けたりした場合は、速やかに情報セキュリティ責任者に報告します。情報セキュリティ責任者は、対応すべきインシデントであるか判断を行い、速やかに経営者に報告します。経営者は、インシデントが事業や顧客に与える影響を踏まえ、速やかにインシデント対応のための体制を立ち上げ、対応方針を指示します。

初動対応においては、被害の拡大防止を意識します。対象となる情報が外部からアクセスできる状態にある場合や、被害が広がる可能性がある場合は、ネットワークの遮断や、情報や対象機器の隔離、システムやサービスの停止を行います。ただし、対象機器の電源を切るなどの不用意な操作でシステム上に残された記録を消さないように気を付ける必要があります

②報告・公表

インシデントの被害拡大を防ぐために、二次的な被害が想定される場合などは、本人にその事実を報告します。本人への報告が困難な場合や、インシデントの影響が広く一般に及ぶ場合は、状況をウェブサイトやメディアを通じて公表します。公表によって被害の拡大を招かないよう、時期、内容、対象などは考慮する必要があります。また、被害が発生・拡大した場合には、受付専用の問い合わせ窓口を開設するなどして、その動向を速やかに把握し対応します。

インシデント対応完了後は、被害者や、影響を及ぼした

22 ▲災害等を含めたリスクに対応するための計画を事業継続計画「BCP(Business Continuity Plan)」、ITシステムの事業継続計画のことを「IT-BCP」と呼びます。

取引先や顧客など関係者に対して、インシデントの対応状況や再発防止策などについて報告します。また、個人情報やマイナンバーの漏えいの場合は個人情報保護委員会、業法などで求められる場合は所管の省庁、犯罪性がある場合は警察、ウイルス感染や不正アクセスの場合はIPAへ届け出ます。

③復旧・再発防止

インシデントからの復旧にあたって、原因を調査し、対応を検討する際は、発覚・発生日時や表面化している事象・被害・影響、発覚から現時点までの時系列での対応経過、現時点で想定される原因などの情報を整理しておくようにします。原因に応じて、修正プログラムの適用、設定変更、機器の入替、データの復元など、必要な対応を行いますが、自社で調査や対応が難しい場合は、IT製品のメーカー、保守ベンダーなどの外部専門組織や公的機関の相談窓口などに支援や助言を依頼します。

また、訴訟対応が見込まれる場合は、調査において事実関係を裏付ける情報や証拠を保全し、必要に応じてフォレンジック調査（パソコンのハードディスク、メモリ内データ、サーバーやネットワーク機器のログ等の調査）を行います。

インシデント対応後は、停止したシステムやサービスを復旧し、経営者に対応結果を報告します。また、インシデントを再発させないために根本原因を分析し、新たな技術的対策の導入、ルールの策定、教育の徹底、体制整備、運用の改善など、抜本的な再発防止策を検討して実施します。

なお、インシデント対応においては、**付録8「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」**や**付録3「5分でできる！情報セキュリティ自社診断」**の対策例も参照してください。

参考情報

（相談窓口）

■情報セキュリティ安心相談窓口（IPA）
https://www.ipa.go.jp/security/anshin/about.html

■インシデント対応依頼（JPCERT/CC）
https://www.jpcert.or.jp/form/

■サイバーインシデント緊急対応企業一覧（JNSA）
https://www.jnsa.org/emergency_response/

（法律で定められた報告窓口）

■漏えい等報告（個人情報等、マイナンバー）（個人情報保護委員会）
https://www.ppc.go.jp/

（告示で定められた報告窓口）

■コンピュータウイルス届出制度、コンピュータ不正アクセス届出制度（IPA）
https://www.ipa.go.jp/security/todokede/crack-virus/about.html

（活用可能な制度）

■事業継続力強化計画認定制度（中小企業庁）
https://www.chusho.meti.go.jp/keiei/antei/bousai/keizokuryoku.htm

中小企業が策定した防災・減災の事前対策に関する計画を経済産業大臣が「事業継続力強化計画」として認定する制度です。認定を受けた中小企業は、ロゴマークをホームページや名刺でアピールしたり、税制措置や金融支援、補助金の加点などの支援策を受けたりすることができます。情報セキュリティを考慮した事業継続計画を策定することで、本制度を活用することが可能です。

(6) 情報セキュリティサービスの活用

外部の情報セキュリティサービスを利用することで、より強固で有効な対策を実施することができます。昨今では、様々なサービスが提供されています。情報セキュリティ人材が社内に不足している場合や、情報セキュリティの向上に有用です。

①情報セキュリティコンサルテーション

情報セキュリティ管理の体制や対策に関する総合的に支援するサービスです。セキュリティ関連の適合性評価制度等における認証・認定を支援するサービスもあります。

②情報セキュリティ教育サービス

情報セキュリティに関連する知識やスキルの習得、情報セキュリティ対策の解説や周知などを支援するサービスです。

③情報セキュリティ監査サービス

情報セキュリティのためのマネジメント(組織内のしくみ)やリスク対策の運用状況を、専門的な立場から、国際的にも整合性のとれた基準に従って検証または評価し、保証や助言を行うサービスです。

④脆弱性診断サービス

システムやソフトウェア等の脆弱性に関して知見のある専門家が、システムやソフトウェア等に対して次のような診断を行うサービスです。

ア　ウェブアプリケーション脆弱性診断
イ　プラットフォーム脆弱性診断
ウ　スマートフォンアプリケーション脆弱性診断

⑤デジタルフォレンジックサービス

システムやソフトウェア等の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、ならびにそれらの兆候について、法的紛争・訴訟に際し、電磁的記録の証拠保全、調査及び分析を行うとともに、電磁的記録の改ざん及び毀損等について次のような分析及び情報収集等を行うサービスです。

ア　機器や記録デバイスを対象とするデジタルフォレンジックによる調査
イ　デジタルフォレンジックによる調査に付帯する訴訟支援及び電子証拠開示対応(eディスカバリ)等のサービス

⑥セキュリティ監視・運用サービス

システムやソフトウェア等についての情報セキュリティを確保するための監視及び適切な運用についての次のようなサービスです。

ア　マネージドセキュリティサービス(セキュリティインシデントまたはその予兆の検知、防御を目的とするものをいう。)

イ　セキュリティ監視サービス（セキュリティ製品が出力するログの分析、通知、レポート提供を継続的に提供するものをいう。）
ウ　マネージドセキュリティサービスやセキュリティ監視サービスを包含する複合的なサービス。

IT活用及びセキュリティ対策を支援する制度

中小企業の生産性向上に資するITツールの活用促進やIT導入を通じた生産性向上を図る制度や、中小企業に対してセキュリティ対策の導入を支援する制度があります。

●サイバーセキュリティお助け隊サービス制度（IPA）

https://www.ipa.go.jp/security/sme/otasuketai-about.html

中小企業に対するサイバー攻撃への対処方法として必要不可欠なサービスを要件としてまとめ、要件を満たす民間サービスをIPAが登録・公表する制度です。「見守り」「駆付け」「保険」など中小企業のセキュリティ対策に不可欠なサービスをワンパッケージで安価に提供しています。

●認定情報処理支援機関（スマートSMEサポーター）制度（中小企業庁）

https://www.smartsme.go.jp/

中小企業が使いやすいITツールの開発促進や中小企業のIT導入を通じた生産性向上を図ります。認定を受けたITベンダーの情報セキュリティ対策の実施状況を確認できます。

Smart SME Supporter

コラム

情報セキュリティサービス基準審査登録制度

多くの情報セキュリティサービスの中から、専門知識をもたないサービス利用者が、サービス事業者の選定時にそのサービスの品質を判断することは容易ではありません。

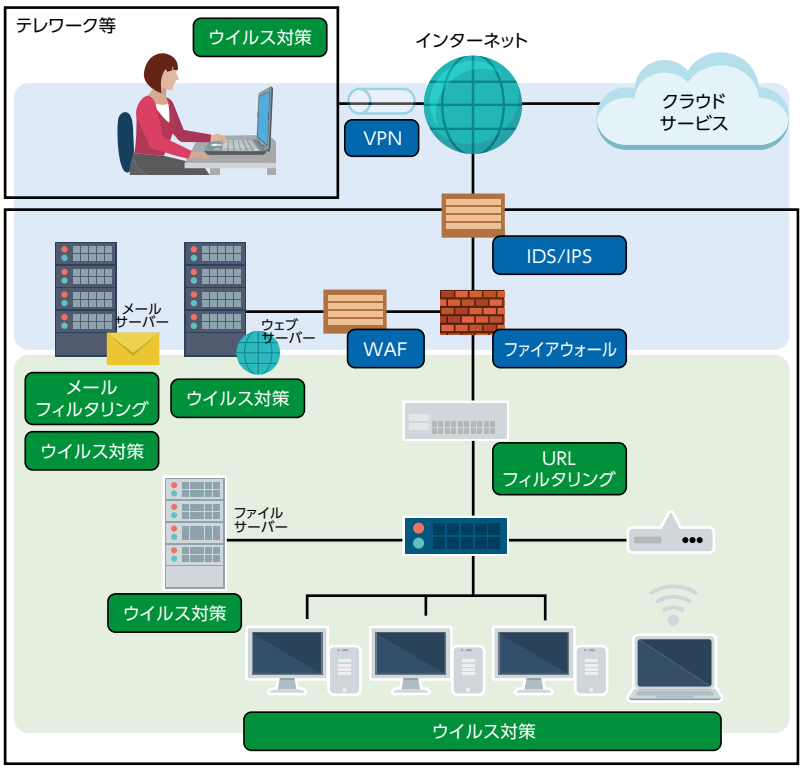
そこで、経済産業省では情報セキュリティサービスに関する一定の技術要件及び品質管理要件を示し、品質の維持・向上に努めている情報セキュリティサービスを明らかにするために「情報セキュリティサービス基準」を設け、この基準に適合するサービスの台帳を公開することで、品質の維持・向上に努めている情報セキュリティサービスを利用者に示し、その普及に結び付けることをねらいとした「情報セキュリティサービス基準審査登録制度」を開始しました。

IPAでは、この「情報セキュリティサービス基準」に適合する情報セキュリティサービスの提供状況について調査を行い、情報セキュリティサービスを利用しようとする者が参照することができるように、「情報セキュリティサービス基準適合サービスリスト」として公開しています。現在は４分野のサービスに限定されていますが、今後の対象分野の拡大についても検討されています。

●情報セキュリティサービス基準適合サービスリスト
https://www.ipa.go.jp/security/service_list.html

(7) 技術的対策例と活用

コンピュータやインターネットを利用するときに施す技術的対策(製品やソフトウェア)を以下に紹介します。自社の環境に合わせて活用してください。



①ネットワーク脅威・端末対策

ネットワークの境界付近に配置して通信の処理や監視を行い、不正な通信の制御と管理を行うことで対策を実施します。

●ファイアウォール

通信をさせるかどうかを判断し許可する、または拒否する技術。例えば、インターネットと社内LANとの間に設置して、外部からの不正なアクセスを社内のネットワークに侵入させないようにできます。

●IDS(Intrusion Detection System:侵入検知システム)

システムやネットワークに対する不正なアクセスなどを検知して管理者に通知する技術。例えば、インターネットとファイアウォールの間に設置することで、不正アクセスと思われる通信を検知して管理者に通知できます。

●IPS(Intrusion Prevention System:侵入防御システム)

システムやネットワークに対する不正なアクセスなどを検知して自動的に遮断する技術。例えば、インターネットとファイアウォールの間に設置することで、不正アクセスと思われる通信を検知して管理者に通知するとともに通信を遮断できます。

●UTM(Unified Threat Management:統合脅威管理)

ファイアウォールやIDS・IPS、メールフィルタリング、URLフィルタリングなど複数の異なるセキュリティ機能を一つのハードウェアに統合して、社内ネットワークとインターネットの脅威であるウイルスの侵入や不正アクセス、サイバー攻撃などを検知し、防御するツールです。

●EDR(Endpoint Detection and Response)

ネットワークに接続されたパソコンやサーバー、スマートフォンなどの端末機器に侵入したウイルスやランサムウェアなどのサイバー攻撃を検出し、管理者に通知する技術です。

●WAF(Web Application Firewall)

ウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保護する技術。例えばファイアウォールやIDS/IPSとウェブサーバーの間に設置することで、ウェブアプリケーションがやり取りするデータを監視して攻撃を検出できます。

●VPN(Virtual Private Network)

インターネットのような公衆ネットワーク上で、保護された仮想的な専用線環境を構築する技術。例えば、テレワーク勤務者が職場との間で機密性の高い電子データをやり取りする際に、VPNを利用することで暗号化による安全な通信ができます。

②コンテンツセキュリティ対策

プログラム実行や電子メール送受信、ウェブ閲覧などを、その内容(コンテンツ)によって制御することで対策を実施します。

●ウイルス対策

ウイルスを検知・駆除することで、ウイルスに感染するのを防ぐための対策。例えば、利用するパソコンにウイルス対策ソフトをインストールしてウイルス定義ファイルを最新の状態にすることで、既知のウイルスを検知できます。

●メールフィルタリング

メールの送受信を監視して、指定した条件によって特定の処理を実行する技術。例えば、メールサーバーでフィルタリング機能を設定することで、迷惑メールやウイルスが添付されたメールをブロックできます。

●URLフィルタリング

ウェブサイトへのアクセスや閲覧について、そのアドレスや内容が所定の条件に合致もしくは違反する場合に停止や警告などを行う技術。例えば、URLフィルタリング機能を持つ機器を導入することにより、業務に関係がないウェブサイトの閲覧を禁止し、不正サイトへアクセスしてしまうリスクを減らすことができます。

③アクセス管理

情報システムの利用者を、認可及び制限する機能を提供します。

●アクセス制御

利用者や情報機器がデータなどにアクセスすることができる権限や認可を制御する技術。例えば、業務で使用するクラウドサービスなどを事務所のみで利用可能とするアクセス制御を行うことで、事務所外からデータへの不正アクセスのリスクを軽減できます。

●多要素認証

サービス利用時に行う利用者認証を、3つの要素(①知っているもの②持っているもの③本人自身に関するもの)のうち、2つ以上の要素を用いて行う技術。例えば、職場の入退室管理システムを利用する際に、本人のみが持つICカード認証に本人のみが知るパスワード認証を追加することで、本人からのアクセスに限定することができます。

●特権ID管理

情報システムの特権(コンピュータを管理するために与えられた最上位の権限)の利用申請や権限付与、操作ログなどを管理する技術。例えば、サイバー攻撃や内部不正などによる、特権の不正利用を防止し、リスクを軽減することができます。

④システムセキュリティ管理

組織が保有するIT資産について、一元的な管理や脆弱性を検出する機能を提供します。

●IT資産管理

パソコンやサーバーなどのハードウェアやソフトウェアの保有状況・構成情報を取りまとめて管理する技術。例えば、IT資産管理ツールを導入することで、セキュリティパッチの適用状況を把握することができ、脆弱性に対する攻撃のリスクを軽減することができます。

●脆弱性検査

サーバーやアプリケーションに対してスキャニングを行い、脆弱性などを検出するための検査。例えば、サービス提供前のウェブアプリケーションに対して、脆弱性を検出するためのリクエストを送ることで、既知の脆弱性の有無を点検することができます。脆弱性がある場合は、脆弱性があるサーバーやアプリケーションに対し、脆弱性修正パッチの適用や安全な設定などの対策を速やかに実施することで、攻撃のリスクを軽減することができます。

●ログ管理

サーバー等に誰がログインしたかや、どのデータに対してアクセスがあったかは、サーバー上にログファイルとして記録されます。ログファイルの内容はサーバー等の運用期間に応じて増えていくので、一定期間(例:1週間、3か月、1年)などの期間で自動

的に削除されるように設定されているのが一般的です。サイバー攻撃があった場合、このログファイルに書かれている内容をもとに、情報漏えいが生じたかどうかを分析するので、ログファイルをどのように管理するかの方針を、組織として定めておくことは重要です。一方で、ログファイルの内容を十分に理解するには専門的な知識が必要となるため、こうした管理を容易にするためのツール類も提供されています。

⑤暗号化

データや通信を暗号化することで覗き見(盗聴)、改ざん、漏えいなどを防止する機能を提供します。

●データ暗号化

特定の法則に基づいてデータを変換し、第三者に内容を知られないようにする技術。例えば、サーバー、パソコン、電子媒体をディスクまたはファイル単位で暗号化することで、メール送信時の添付ファイルの盗聴、社外からの不正アクセスによるデータの持ち出し、パソコンや電子媒体の紛失や盗難などによる情報漏えいのリスクを軽減することができます。

●通信暗号化

インターネット経由でデータの通信を行うとき、データを保護するために用いられる暗号化や認証のための技術規格のうち、最も普及しているものの１つです。過去にSSL(Secure Sockets Layer)として規格化され、現在はTLS(Transport Layer Security)という名前で国際標準となっていますが、TLSのことを今でもSSLと呼んでいる場合もあります。一般的なウェブブラウザはすべて対応しているので、改めて導入する必要がないメリットがあり、世界的に広く利用されています。

⑥データの破棄

情報システムを使わなくなった場合、システム内にデータを保存したまま放置したり、破棄したりするとそれが情報漏えいの原因となるため、速やかにデータの消去を行う必要があります。またクラウドサービスの場合も、不要となったデータをクラウド上に保存したままにするのは、情報漏えいのリスクを不必要に高めることにつながります。

(8) 詳細リスク分析の実施方法

P.26(3)情報セキュリティ規程の作成では、経営者の懸念事項を踏まえ外部状況と内部状況から一般的に想定されるリスクを特定し、対策を決めていく方法を紹介しました。しかし、事業規模が大きくなったり、情報システムが複雑になると、想定外のリスクを見落とし、対策が不十分になることがあります。そこでここでは、もれなくリスクを特定し、対策を検討する手法として「詳細リスク分析」について解説します。詳細リスク分析は、以下の手順で行います。

手順1 情報資産の洗い出し

どのような情報資産があるか洗い出して重要度を判断する

業務で利用する電子データや書類を**「リスク分析シート」(付録7)**の情報資産管理台帳に記入します。記入した情報資産ごとに漏えいや改ざん、誤びゅう(誤記、計算違い)が起きたり、必要な時に利用できないときの、事業への影響の観点から重要度を判断します。

業種、事業内容、IT環境によって保有する情報資産は異なるため、台帳記入例を参考に、以下の要領で作業を進めます。

●情報資産管理台帳の作成
パソコンのハードディスクや机の引き出しを見るのではなく、日常どのような電子データや書類を利用して業務を行っているかを考えて洗い出すと、作成しやすくなります。

●情報資産ごとの機密性・完全性・可用性の評価
機密性、完全性、可用性が損なわれた場合の事業への影響や、法律で安全管理義務があるなど、表12の評価基準を参考に評価値[23]3～1を記入します。

●機密性・完全性・可用性の評価値から重要度を算定
重要度は、機密性、完全性、可用性いずれかの最大値で判断します。前項の作業で「情報資産管理台帳」の所定欄に記入した機密性・完全性・可用性の評価値をもとに、表15の判断基準に従い、重要度を算定します。

なお、事故が起きると法的責任を問われたり、取引先、顧客、個人に大きな影響があったり、事業に深刻な影響を及ぼすなど、企業の存続を左右しかねない場合や、個人情報を含む場合は、前項の算定結果に関わらず、重要度は2とします。

情報資産管理台帳の記入要領は、本書の57ページの説明を参照してください。

23 ▲**評価値**　この他にも数値を使うことがありますが、これは情報資産の重要度やリスクの大きさを定量的に表したほうが、優先的に対策すべき情報資産がわかりやすくなるためです。おおよその見当がつけばよく、緻密に計算する必要はありません。

【表12】情報資産の機密性・完全性・可用性に基づく重要度の定義

評価値		評価基準	該当する情報の例
機密性 アクセスを許可された者だけが情報にアクセスできる	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データ[24]として指定されている 漏えいすると取引先や顧客に大きな影響がある	●取引先から秘密として提供された情報 ●取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため） 漏えいすると自社に深刻な影響がある	●自社の独自技術・ノウハウ ●取引先リスト ●特許出願前の発明情報
	2	漏えいすると事業に大きな影響がある	●見積書、仕入価格など顧客（取引先）との商取引に関する情報
	1	漏えいしても事業にほとんど影響はない	●自社製品カタログ ●ホームページ掲載情報
完全性 情報や情報の処理方法が正確で完全である	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	●取引先から処理を委託された会計情報 ●取引先の口座情報 ●顧客から製造を委託された設計図
	2	改ざんされると事業に大きな影響がある	●自社の会計情報 ●受発注・決済・契約情報 ●ホームページ掲載情報
	1	改ざんされても事業にほとんど影響はない	●廃版製品カタログデータ
可用性 許可された者が必要な時に情報資産にアクセスできる	3	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	●顧客に提供している EC サイト ●顧客に提供しているクラウドサービス
	2	利用できなくなると事業に大きな影響がある	●製品の設計図 ●商品・サービスに関するコンテンツ（インターネット向け事業の場合）
	1	利用できなくなっても事業にほとんど影響はない	●廃版製品カタログ

24 **▲限定提供データ**　不正競争防止法で次のように定義されています。「第二条　7　この法律において「限定提供データ」とは、業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その他人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理されている技術上又は営業上の情報（秘密として管理されているものを除く。）をいう。」

【表13】情報資産の重要度判断基準

判断基準	重要度
機密性・完全性・可用性評価値のうち最大値が「3」の情報資産	3
機密性・完全性・可用性評価値のうち最大値が「2」の情報資産	2
機密性・完全性・可用性評価値すべてが「1」の情報資産	1

（重要度の判断例）

●『独自技術に基づいた設計図』（書類）

機密性：主力製品の設計図であり、流出すると他社との差別化ができなくなり、売上が減少する …… **評価＝3**

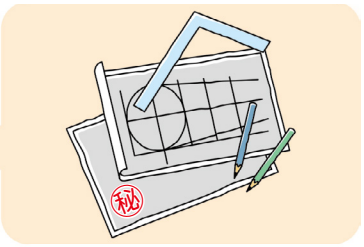
完全性：改ざんや無断の変更があると、製造に支障がある…… **評価＝2**

可用性：原本のCADデータはサーバーに保存してあり、必要なときに閲覧や再印刷が可能なので、利用できなくなっても困ることはない…… **評価＝1**

情報資産管理台帳　重要度欄

評価値			重要度
機密性	完全性	可用性	
3	2	1	3

機密性の3が最大値なので重要度は3



●『自社のホームページ』（電子データ）

機密性：公開しているホームページであり、クレジットカード情報など機密情報の保存はしていない …… **評価＝1**

完全性：不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられると顧客や閲覧者に被害が発生し、信用を失う…… **評価＝3**

可用性：サーバーの障害などでアクセスできなくなると、来店客が減少し、売上も減少する …… **評価＝3**

情報資産管理台帳　重要度欄

評価値			重要度
機密性	完全性	可用性	
1	3	3	3

完全性と可用性の3が最大値なので重要度は3

付録の利用方法（手順１）

「リスク分析シート」（付録７）は本ガイドラインの手順１～３に示した作業を実施する際のツールです。「手順１」で示した情報資産管理台帳は、「情報資産管理台帳」シートに相当します。記入方法は、「台帳記入例」シートと表１４を参考にしてください。

【表 14】情報資産管理台帳への記入要領

台帳記入欄	記入内容解説
① 業務分類	情報資産に関連する業務や部署名を記入します。情報資産は業務に関連して発生しますので、まず関連業務や部署を特定し、その業務や部署で利用している情報を洗い出すと記入漏れが少なくなります。
② 情報資産名称	情報資産の内容を簡潔に記入します。正式名称がないものは社内の通称で構いません。管理方法や重要度が同じものは１行にまとめます。
③ 備考	必要に応じて説明等を記入します。
④ 利用者範囲	情報資産を利用してよい部署等を記入します。
⑤ 管理部署	情報資産の管理責任がある部署等を記入します。小規模事業者であれば担当者名を記入しても構いません。
⑥ 媒体・保存先	情報資産の媒体や保存場所を記入します。書類と電子データの両方で保存している場合は、それぞれ完全性・可用性（機密性は同一）や脅威・脆弱性が異なるので２行に分けて記入します。 例）見積書「電子データを事務所 PC に保存」「印刷物書類をキャビネットに保管」
⑦ 個人情報の種類	各項目が個人情報保護法、マイナンバー法で定義されています。 〈個人情報〉 個人情報が含まれる場合は「有」を記入します。 ―**個人情報の定義**― 「生存する個人に関する情報であって当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの、又は個人識別符号が含まれるもの」 氏名、住所、性別、生年月日、顔画像等個人を識別する情報に限られず、個人の身体、財産、職種、役職等の属性に関して、事実、判断、評価を表す全ての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問わない。 〈要配慮個人情報〉 要配慮個人情報が含まれる場合は「有」を記入します。 ―**要配慮個人情報の定義**― 「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取り扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報」 〈特定個人情報〉 個人番号（マイナンバー）が含まれる場合（マイナンバー法で「特定個人情報」と定義されています。）は「有」を記入します。
⑧ 重要度	情報資産の機密性、完全性、可用性それぞれの評価値を記入します。 ３種類の評価値から、P55 表１２に基づき重要度が表示されます。なお、⑦でいずれかの個人情報が「有」の場合、重要度は自動的に「３」となります。
⑨ 保存期限	法定文書は法律で定められた保存期限を、それ以外は利用が完了して廃棄、消去が必要となる期限を記入します。
⑩ 登録日	登録した日付を記入します。内容を更新した場合は更新日に修正します。

記入上のポイント

●情報資産管理台帳は洗い出した情報資産を「見える化」するための方法の一つです。特にパソコンやネットワークで利用する電子化された情報は人間の五感で感知することができないため、社外のサーバーや個人のスマートフォンに保存されていると気付かないことがあります。電子化された情報を洗い出すときには「普段パソコンで見ているこのデータは、どこに保存されているのだろう。」というように、社内のIT機器や利用しているクラウドサービスを思い浮かべて記入します。

●重要度の判断は立場や見識によっても異なることがあるので、記入する前に「重要ではない」と判断するのではなく、記入した後に組織的に重要度を判断します。

●電子データや書類を保存する際のまとめ方は様々ですが、管理方法や重要度が同じ情報は1件にまとめて記入することで作業負荷を減らすことができます。

【管理方法や重要度が同じ情報の例】

事務所内のパソコンで会計ソフトや表計算ソフトを使って帳簿を作成している場合

◆ 仕訳帳
◆ 総勘定元帳
◆ 現金出納帳
◆ 当座預金出納帳
◆ 小口現金出納帳
◆ 仕訳帳
◆ 売上帳

情報資産名称：「会計データ」
「会計データバックアップ」
（バックアップを取っている場合）など
媒体・保存先：「事務所PC」（会計ソフトの保存先）
「可搬電子媒体」
（USBメモリがバックアップ保存先）

●情報資産の「重要度」は時間経過とともに変化することがありますが、現時点の評価値を記入してください。また時間経過に伴う重要度の変化を台帳上で更新することが難しい場合は、最大値で評価します。

●中規模企業の場合、管理部署ごとにシートを分けて作成すると、内容の見直しの際に便利です。

手順2 リスク値の算定

優先的・重点的に対策が必要な情報資産を把握する

手順１で洗い出した情報資産について、対策の優先度を決めるため、リスク値（リスクの大きさ）を算定します。リスク値を算定するにはいろいろな方法がありますが、本ガイドラインでは「重要度」と「被害発生可能性」の２つの数値の掛け算で行います。「被害発生可能性」は「脅威の起こりやすさ」と「脆弱性のつけ込みやすさ」の２つの数値から算出します（次頁表１７）。これは、脅威が脆弱性を利用して、どの程度被害をもたらす可能性があるかを示す指標です。

リスク値 ＝ 重要度 × 被害発生可能性

重要度 ＝ 手順1にて算定
被害発生可能性 ＝ 脅威・脆弱性から算定

重要度は手順１で算定した３～１の数値、被害発生可能性、脅威、脆弱性は３～１の数値、リスク値は算定結果を大・中・小で表します（表１５）。

【表15】リスク値の算定基準

重要度		情報資産の価値・事故の影響の大きさ
	3	事故が起きると ● 法的責任を問われる ● 取引先、顧客、個人に大きな影響がある ● 事業に深刻な影響を及ぼす など企業の存続を左右しかねない
	2	事故が企業の事業に重大な影響を及ぼす
	1	事故が発生しても事業にほとんど影響はない

× 掛け算

算定のしかたは表17参照

		起こりやすさ
脅威	3	通常の状況で脅威が発生する（いつ発生してもおかしくない）
	2	特定の状況で脅威が発生する（年に数回程度）
	1	通常の状況で脅威が発生することはない
脆弱性		つけ込みやすさ
	3	対策を実施していない（ほぼ無防備）
	2	部分的に対策を実施している
	1	必要な対策をすべて実施している

被害発生可能性		
	3高	通常の状況で被害が発生する（いつ発生してもおかしくない）
	2中	特定の状況で被害が発生する（年に数回程度）
	1低	通常の状況で被害が発生することはない

リスク値		
	9～6 大	深刻な事故が起きる可能性大
	4 中	重大な事故が起きる可能性有
	3～1 小	事故が起きる可能性小、起きても被害は受容範囲

中小企業でも想定される脅威と、放置しがちな脆弱性から、それらがもたらすリスク値の算定例を表16に示します。この例からも分かるように、脅威の起こりやすさをコントロールすることは困難ですが脆弱性は対策を改善することで減少し、その結果リスクを低減することができます。

【表16】脆弱性対策に応じたリスク値の変化

脅威の例	重要度(a)	脅威	脆弱性	被害発生可能性(b)	重要度(a)×被害発生可能性(b)	リスク値
1,000人を超える顧客の個人データを保存しているノートパソコンの盗難 (脆弱性) データを暗号化していない	3	2	**3**	**2**	**6**	**リスク大**
(対策改善) ハードディスクやデータを暗号化する	3	2	**1**	**1**	**3**	**リスク小**
クレジットカード番号を含む顧客の個人データを保持したECサイトへ不正アクセスされることによる情報漏えい (脆弱性) ウェブサイトの技術的脆弱性を認識せず対策が不十分	3	3	**3**	**3**	**9**	**リスク大**
(対策改善) ECサイトの設計・開発段階から脆弱性を作り込まないように技術的セキュリティを実装する	3	3	**1**	**1**	**3**	**リスク小**
メールの添付ファイルを開いてしまいランサムウェアに感染し、サーバーのデータとオンラインバックアップが暗号化される (脆弱性) オンラインバックアップしか取得していない	3	3	**2**	**2**	**6**	**リスク大**
(対策改善) 定期的にオフラインバックアップを取得する	3	3	**1**	**1**	**3**	**リスク小**

【表17】被害発生可能性　換算表

		脆弱性		
		3	2	1
脅威	3	**3**	**2**	**1**
	2	**2**	**1**	**1**
	1	**1**	**1**	**1**

計算式　脅威÷(4－脆弱性)　小数第1位を切り上げ

付録の利用方法（手順２）

個々の情報資産ごとにリスク値を算定する方法を説明します。

①「重要度」の分類

「情報資産管理台帳」シートに記入した重要度をそのまま使用します。

②「脅威」の識別

「脅威の状況」シートで、媒体・保存先ごとの脅威がどのくらいの頻度で発生する可能性があるかを「対策を講じない場合の脅威の発生頻度」欄に表示されるリストから１～３のいずれかを選択します。

社内サーバー	情報窃取目的の社内サーバーへのサイバー攻撃	3：通常の状況で脅威が発生する（いつ発生してもおかしくない）
	情報窃取目的の社内サーバーでの内部不正	2：特定の状況で脅威が発生する（年に数回程度）
	社内サーバーの故障による業務に必要な情報の喪失	1：通常の状況で脅威が発生することはない

媒体・保存先　個別の脅威　脅威の発生頻度（1～3から選択）

③「脆弱性」の認識

「対策状況チェック」シートで55項目の「情報セキュリティ診断項目」ごとに自社における実施状況を「実施状況」欄に表示されるリストから１～４のいずれかを選択します。

物理的セキュリティ対策	業務を行う場所に、第三者が許可なく立ち通りができないようにするための対策（物理的に区切る、見知らぬ人には声をかける、等）が講じられていますか？	2：一部実施している
	最終退出者は事務所を施錠し退出の記録（日時・退出者）を残すなどのように、事務所の施錠をしていますか？	1：実施している
	高いセキュリティを確保する区域には、許可された者以外は接近できないような保護措置がなされていますか？	3：実施していない／わからない
	秘密情報を保管および扱う場所への個人所有のパソコン・記録媒体等の持込み・利用は禁止されていますか？	4：自社に該当しない

情報セキュリティ診断項目（チェック項目）　実施状況（1～3+4:自社に該当しない）

④リスク値の算定

以上①から③を記入すると「情報資産管理台帳」シートの右側「リスク値」欄に情報資産ごとのリスク値が表示されます。リスク値に応じて以下のように対応を検討します。

- リスク大　優先的に対策を実施
- リスク中　対策を実施
- リスク小　現状維持

現状の状況から想定されるリスク（入力不要・自動表示）					
脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性※「対策状況チェック」シートに入力すると表示	被害発生可能性		リスク値	
3：通常の状況で脅威が発生する（いつ発生してもおかしくない）	2：部分的に対策を実施している	2	可能性：中	4	リスク大
2：特定の状況で脅威が発生する（年に数回程度）	2：部分的に対策を実施している	1	可能性：低	2	リスク中

情報資産ごとの脅威の発生頻度　情報資産ごとの脆弱性（対策状況）　情報資産ごとの被害発生可能性（高・中・低の3段階）　情報資産ごとのリスク値（大・中・小の3段階）

手順3　情報セキュリティ対策の決定

リスクの大きな情報資産に対して必要とされる対策を決める

続いて、リスク値の大きいものから対策を検討し、自社に適した対策を決定します。なお、対策は以下のように区分して検討します。

①リスクを低減する

自社で実行できる情報セキュリティ対策を導入ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げます。

②リスクを保有する

事故が発生しても受容できる、あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持します。

③リスクを回避する

仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくします。

例えば、従来は商品の発送先である住所や氏名などの個人情報を発送完了後もパソコンに保存し続けていたが、保存中の漏えいを避けるために、利用後はすぐに消去する、インターネットバンキングに使用するパソコンでメールやウェブ閲覧をしていたが、ウイルスに感染しないようにインターネットバンキング専用のパソコンを設置し、ウイルス感染の原因となるメールやウェブ閲覧に利用せず、USBメモリ、外付けHDDも接続を禁止する、などがあります。

また、リスク値が大きく自社の対策だけでは不十分であったり、多額の費用がかかり、実施できない場合は以下を検討します。

④リスクを移転する

自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することで自社の負担を下げます。

例えば、商品を販売するウェブサイトではクレジットカード番号を非保持化し、代金の決済はセキュリティ対策を十分行っている外部の決済代行サービスに変更する、社内のサーバーで運用していた業務システムをセキュリティ対策の充実した外部クラウドサービスに移行する、情報漏えい、システム障害などの事故発生に伴う損失に対して保険金が支払われる情報セキュリティに関連した保険商品に加入する、などがあります。

付録の利用方法（手順 3）

P61④リスク値の算定で示した、「情報資産管理台帳」シートの右側「リスク値」で「リスク大」と表示されたものから対策を検討します。このとき参考になるのが「診断結果」シートの「対策状況チェックの診断結果」です。これは「対策状況チェック」シートで回答した実施状況を対策の種類ごとに集計したものです。

情報セキュリティ対策の種類（付録５ 情報セキュリティ関連規程名称）		情報セキュリティ関連規程策定の必要性	対策状況チェックの診断結果（対策の実施率）	対策検討・実施の要否
1	組織的対策	◎	62.5%	不足する対策を検討・実施してください
2	人的対策	◎	33.3%	不足する対策を検討・実施してください
3	情報資産管理	○	14.3%	不足する対策を検討・実施してください
4	アクセス制御及び認証	○	100.0%	対策を維持し適切性・妥当性・有効性を継続的に改善してください

この「対策の実施率」が低いことでリスク値が大きくなっている可能性があります。実施率が低くなっている対策の種類について「対策状況」シートを見直し、対策を行ったと仮定して「3:実施していない／わからない」や「2:一部実施している」となっている項目を「1:実施している」に直すと、リスク値が変化しますので、全てのリスク値が「中」以下になり、かつ自社で今後実施が可能と見込まれる対策について検討してください。

コラム

「情報セキュリティに関連した保険商品」とは

個人情報保護法の施行後、個人情報を漏えいしてしまった企業に対して、損害賠償金ならびに法律相談、事故対応、見舞金などの費用損害相当額を支払う保険が登場しました。現在は個人情報以外にも、不正アクセスなどにより取引先企業の秘密情報の漏えい事故にも対応するものが、「サイバーセキュリティ対策保険」として損害保険各社から提供されています。また、中小企業が加入しやすい団体型の商品として日本商工会議所が会員向けに提供している「情報漏えい賠償責任保険制度～サイバーリスク補償型」や、その他業界団体などによるサイバー保険の各種団体制度があります。こうした保険では、SECURITY ACTIONの宣言や、プライバシーマーク・ISMSなどの認定を取得していたり、適切な情報管理体制を導入していたりすると保険料が割引になるため、情報セキュリティ対策を行うことが経済的な利点となっています。

コラム

リスク分析の手法あれこれ

コンピュータやネットワークを利用する時のリスクは、技術的な知識がないと分かりにくく、見落とすことがありますが、リスクがあることを知らずに対策を怠った結果、事故が起きてしまった、ということも多いので、リスク分析を通じて、適切な対策を導き出す必要があります。

(8)詳細リスク分析の実施方法では、対策の優先順位を判断しやすいように、情報資産の価値と、関連する脅威や脆弱性からリスクを定量的に捉える方法を説明しています。以下に、広く参照されている「ISO/IEC TR 13335(JIS TR X 0036)ITセキュリティマネジメントのガイドライン」より、4つのリスク分析方法を紹介しますので、事業やIT環境に適した手法を選択して活用してください。

①ベースラインアプローチ

既存の標準や基準を参照して対策を検討する方法。
情報資産ごとに「資産価値」「脅威」「脆弱性」を識別しないので、簡単にできる方法であるが、参照する標準や基準によって、対策のレベルが高すぎたり、低すぎたりする場合がある。
例)「情報セキュリティ5か条」「5分でできる!情報セキュリティ自社診断」を参照して対策を実施する。

②非形式的アプローチ

組織や担当者の経験や判断によってリスク分析を行い、対策を検討する方法。
短時間に実施することが可能であるが、属人的な判断に偏るおそれがある。
例)システム管理者が情報セキュリティに詳しいIT製品のメーカー、保守ベンダーにアドバイスしてもらい対策を実施する。

③詳細リスク分析

情報資産ごとに「資産価値」「脅威」「脆弱性」を識別し、対策を検討する方法。
個々の情報資産に適した対策が可能だが手間がかかる。
例)P.52(8)詳細リスク分析の実施方法に従って対策を実施する。

④組合せアプローチ

複数の方法を併用し、それぞれの長所短所を補完する方法。
よく用いられるのは、ベースラインアプローチと詳細リスク分析の組合せ。
重要な情報資産に対する対策とその他の情報資産に対する対策とのバランスがとりやすい。
例)基幹システムに関連する情報資産と個人情報を詳細リスク分析の対象として、その他は「5分でできる!情報セキュリティ自社診断」を参照して対策を実施する。

情報セキュリティに関する参考情報

本ガイドラインを実施するうえで参考となる文献やウェブサイトなどを以下に示します。規格、ガイドラインは改定されますので、適宜に最新版を参照してください。

[1] サイバーセキュリティ経営ガイドライン（経済産業省 /IPA）

大企業及び中小企業（小規模事業者を除く）のうち、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため策定されたガイドラインです。
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

[2] 組織における内部不正防止ガイドライン（IPA）

組織における内部不正を防止するために実施すべき対策として、10の観点（コンプライアンス、職場環境など）のもと30項目の対策を提示したガイドラインです。
https://www.ipa.go.jp/security/guide/insider.html

[3] 脆弱性対策情報ポータルサイト（IPA/一般社団法人JPCERTコーディネーションセンター（JPCERT/CC））

日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供している脆弱性対策情報ポータルサイトです。
https://jvn.jp/

[4] JIS Q 27001（ISO/IEC 27001）情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項

ISMS（Information Security Management System：情報セキュリティマネジメントシステム）適合性評価制度の認証基準として、要求事項を定めた規格です。
※マネジメントシステムとは管理のしくみのことです。

[5] ISO/IEC 27002情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策

情報セキュリティ管理策を実施するための手引として用いることを意図して作成された規格です。
※情報セキュリティ管理策とは本ガイドラインでいう情報セキュリティ対策のことです。

[6] JIS Q 27017（ISO/IEC 27017）情報技術－セキュリティ技術－ JISQ 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範

JIS Q 27002を基に、クラウドサービス利用者及びクラウドサービス事業者のための情報セキュリティ管理策の実施を支援する指針を提示した規格です。

[7] JIS Q 27005（ISO/IEC 27005）情報技術－セキュリティ技術－情報セキュリティリスクマネジメント

組織の情報資産を安全に保つための情報セキュリティリスクマネジメントのプロセスを示した規格です。

[8] JIS Q 31000（ISO/IEC 31000）リスクマネジメント－指針

組織が直面するリスクのマネジメントに関する指針を提示した規格です。

[9] 情報セキュリティマネジメント試験

情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、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す。
https://www.ipa.go.jp/shiken/kubun/sg/index.html

[10] 技術情報管理認証制度（経済産業省）

Technology Information Control System
企業の情報セキュリティ対策を、国の認定を受けた機関が国が策定した基準に基づいて審査・認証する制度です。
https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html

本書で用いている主な用語の説明

インシデント

リスクが発現・現実化した事象のことをいいます。本ガイドラインでは事故とインシデントとを併用します。情報システムの場合、情報の漏えい、改ざんや消失の発生、日常使用している機能の停止または極端な性能の低下などがインシデントに相当します。

(情報の)可用性

許可された者が、必要な時に、情報や情報資産にアクセスできることを確実にする特性のことをいいます。

(情報の)完全性

情報や情報の処理方法が正確で完全であるようにする特性のことをいいます。

(情報の)機密性

アクセスを認可された者だけが、情報にアクセスできるようにする特性のことをいいます。

クラウドサービス

サーバーなどを自前で所有する代わりとして、インターネット経由で同様の機能を提供するものをいいます。レンタルサーバー、SaaS(Software as a service)、ASP(Application Service Provider)などは、いずれもクラウドサービスの一種です。

個人情報

①「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。

(1)当該情報に含まれる氏名、生年月日その他の記述等(文書、図画若しくは電磁的記録(電磁的方式(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第2号において同じ。)で作られる記録をいう。以下同じ。)に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項(個人識別符号を除く。)をいう。以下同じ。)により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)

(2)個人識別符号が含まれるもの

②「特定個人情報」とは、個人番号をその内容に含む個人情報をいう。(マイナンバー法(行政手続における特定の個人を識別するための番号の利用等に関する法律))

サイバーセキュリティ

①サイバーセキュリティ基本法における定義：「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式(以下本項において「電磁的方式」という。)により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置(情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。)が講じられ、その状態が適切に維持管理されていること」をいいます。

②サイバーセキュリティ経営ガイドラインにおける定義：「サイバーセキュリティとは、電子データの漏えい・改ざん等や、期待されていたITシステムや 制御システム等の機能が果たされないといった不具合が生じないようにすること」をいいます。

③NIST(米国標準技術研究所)における定義：「攻撃を防止し、検知し、攻撃に対応することにより情報を保護するプロセス」のことをいいます。

情報セキュリティ

情報の機密性、完全性、可用性を維持することをいいます。

情報セキュリティに関連した保険商品

情報セキュリティ上の損害が生じた場合に保険金が支払われるものをいい、個人情報が漏えいした場合の賠償責任などに備える個人情報取扱事業者保険や、不正アクセスなどのサイバー攻撃による被害を受けた企業が事業を存続できるように備えるためのサイバー保険、サイバーリスク保険などの種類があります。

おわりに

第3版の公開から約4年が経過し、この度第3.1版をお届けすることとなりました。この第3.1版では、中小企業においても急速に導入が進むテレワークのセキュリティ対策について追加しました。また、巧妙化するサイバー攻撃などにより、被害が拡大していることから、セキュリティインシデント発生時の対応を追加し、いざというときの手引きを付録にまとめました。

中小企業は、情報セキュリティ対策に十分な経営資源を割り当てることが難しいという制約を抱える一方で、経営者が意思決定を迅速に行うことができ、従業員とのコミュニケーションも容易であるなど、変化に応じた柔軟な対応が出来るという強みがあります。DXへの取り組みが企業の成長を左右するといわれる中、サイバー攻撃等による被害も増加しています。デジタル技術特有のリスクから会社を守るためにも、本ガイドラインをご活用いただければ幸いです。

（第3.1版作成）
中小企業の情報セキュリティ対策ガイドライン改訂に関する研究会　委員
（五十音順、○は委員長）

	稲垣　隆一	稲垣隆一法律事務所
○	大木　榮二郎	工学院大学　名誉教授
	佐藤　健志	日本商工会議所情報化推進部 部長
	下村　正洋	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事務局長
	比留間　貴士	特定非営利活動法人ITコーディネータ協会　常務理事・事務局長
	洞田　慎一	一般社団法人JPCERTコーディネーションセンター経営企画室兼早期警戒グループ担当部門長
	吉井　裕之	全国商工会連合会　産業政策部　経営情報戦略課長

改訂履歴
• 1.0版（2009年3月18日）　• 2.0版（2016年11月15日）全面改訂 • 2.1版（2017年1月24日）用語、図の修正
• 3.0版（2019年3月19日）　• 3.1版（2023年4月26日）

はじめましょう 情報セキュリティ!

中小企業の情報セキュリティ対策ガイドライン　第 3.1 版
2023 年 4 月

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
電話　03-5978-7508　　FAX　03-5978-7546
E-mail　isec-pr-nw@ipa.go.jp