中小企業の情報セキュリティ対策ガイドライン

第4.0版

IPA 独立行政法人 情報処理推進機構

目 次

付録１　中小企業のためのセキュリティ人材確保・育成の実践ガイドブック
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　資産管理台帳（サンプル）
付録７　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

第 4.0 版への改訂にあたって

第3.1版の公開から約3年が経過し、この度第4.0版をお届けすることとなりました。

2023年4月の第3.1版の公開以降、企業のサイバーセキュリティ対策を取り巻く環境においては次のような変化が生じています。

- ランサムウェアによる被害の顕在化により、企業におけるサイバーセキュリティに関する被害は情報漏えいにとどまらず、企業の事業活動の停止へと影響が拡大
- 国内外でのサプライチェーンを介したサイバーセキュリティ関連被害の拡大を踏まえ、サプライチェーン全体としての対策推進の必要性の高まり
- 中小企業等の内部でセキュリティ対策を推進する人材の著しい不足

これらを踏まえ、第4.0版への改訂では、「第1部 経営者編」と「第2部 実践編」の基本的な構成を維持しつつ、最新の環境変化を反映し、中小企業が適切な認識と実践的な対策を進められるよう、特に以下の観点で、記載内容の見直しを行いました。

- 2024年度に実施した「中小企業における情報セキュリティ対策に関する実態調査」ならびに昨今のサイバー攻撃の状況を踏まえ、「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」において、実行性を上げるための対策例の見直しを実施
- 経済産業省及び内閣官房国家サイバー統括室が検討を進める「サプライチェーン強化に向けたセキュリティ対策評価制度（以下、SCS 評価制度）」を踏まえ、組織的な対策や技術的な防御策の考え方を整理
- 2025年５月に公表された、経済産業省「サイバーセキュリティ人材の育成促進に向けた検討会」最終とりまとめで示された「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイドβ版」を踏まえ、中小企業のセキュリティ人材の確保・育成を支援する方策ガイド及び取組事例を付録として追加

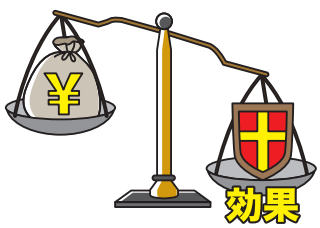
なお、第4.0版への改訂にあたっては、支援機関・団体や中小企業へのヒアリングを行った上で改訂を行いました。

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とともに、事業継続に対する影響（リスク）を未然に防ぐ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！

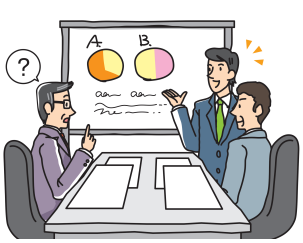


情報セキュリティ対策に取り組むことで、対外的に企業の信頼性が高まり、業績向上に繋がります。その一方で、情報セキュリティ対策を疎かにしたためにシステム障害が発生して事業活動が停止することがあります。また、情報漏えいの場合は、顧客や取引先の信頼を失い、業績が悪化することもあります。さらに、顧客や取引先に被害が及んだ場合には、経営を揺るがしかねない高額な賠償金を請求されることもあります。（➡ 詳細はP10）

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P12）

組織として対策するために、担当者の任命と指示が必要です！



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行うための担当者を任命し、指示をする必要があります。（➡ 詳細はP14）

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及び小規模事業者（法人、個人事業主、各種団体も含む）を対象とし、業務におけるITの活用及び情報資産の管理に関する情報セキュリティ対策を取り扱うものです。なお、工場設備や制御システム等の分野は本ガイドラインの対象外とします。想定読者は、経営者及び情報管理を統括する方です。

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、及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　中小企業のためのセキュリティ人材確保・育成の実践ガイドブック**	セキュリティ対策を実施するために必要な人材の確保・育成のための方策ガイドです。
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ルールを文書化したもののサンプルです。
付録	**付録6　資産管理台帳（サンプル）**	情報資産及び関連するネットワーク機器、ソフトウェア、ハードウェアを一覧化したもののサンプルです。
付録	**付録7　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4.0版の主な変更点について

■第２部

- 中小企業実態調査結果及びSCS評価制度を受けて、第２部実践編を全面的に改訂しました。

■付録

- 付録１「中小企業のためのセキュリティ人材確保・育成の実践ガイドブック」を追加しました。
- 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）」を第２部実践編のSTEP2に合わせて見直しました。
- 付録５「情報セキュリティ関連規程（サンプル）」を第２部実践編に合わせて見直しました。
- 付録６「資産管理台帳」を見直しました。

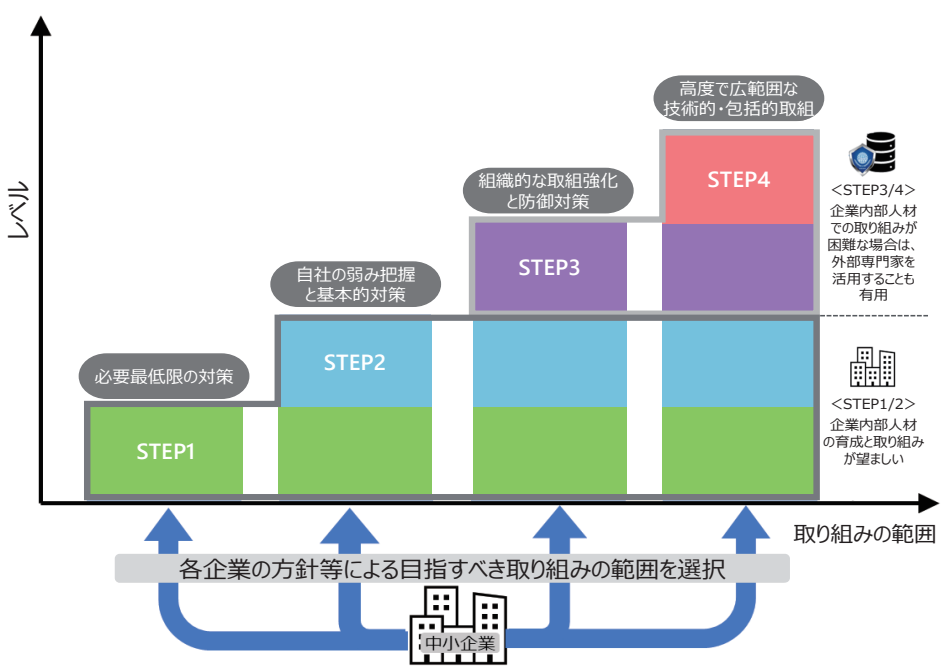
4 本ガイドラインの活用方法

本ガイドラインにより、自社の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、経営者が認識すべき「３原則」と実行すべき「重要７項目の取組」を記載しており、全ての経営者に読んでいただきたい内容です。取り組むべき全体像を把握していただき、実践に当たっては実践編を参照してください。

■**「第2部 実践編」**は、自社にあった STEP の対策を実施してください。

- ●本ガイドラインは、各企業が目指しているセキュリティレベル（成熟度）により、４つの STEP を定めています。各企業の方針やリソースに合致した活動を以下の取り組みの目安を参照しながら活動に繋げていくことが可能な構成としています。
- ●表２の「取組の目安」や「想定している企業の例」を参照し、自社の現在の立ち位置を見極め、目指すべき姿を決めたうえで、取り組む STEP を選択ください。
- ●取り組む STEP を選択したら、各 STEP の内容を参照し、優先順位をつけながら対策を進めてください。
- ●各 STEP で必要な対策の実行に必要な人材の確保と育成については、**「中小企業のためのセキュリティ人材確保・育成の実践ガイドブック」（付録1）**の解説を参照してください。



【表2】取り組みの目安と想定している企業の例

STEP	取り組みの目安	想定している企業の例
STEP1 (P20)	すべての企業が実施すべき基本的なセキュリティ対策であり、「情報セキュリティ６か条」を活用し、自社の業務・情報・従業員・取引先を守る必要最低限の対策から始めます。	STEP を目指すきっかけ ●アナログ中心だったが、近年業務にITを取り入れ始めた 企業をとりまく状況 ●周囲の取引先でセキュリティ被害が発生し、その脅威を身近に感じた　等
STEP2 (P22)	基本的なセキュリティ対策を組織的に取り組むために、「5分でできる！情報セキュリティ自社診断」を活用し、自社の弱みを把握し基本的対策を決定するとともに、組織としての情報セキュリティ基本方針を作成します。	STEP を目指すきっかけ ●業務の効率化や情報共有促進のために、ITシステムの本格導入を進めている 企業をとりまく状況 ●セキュリティ対策が標準化されず、従業員の属人的な対応となっていた　等
STEP3 (P26)	組織的な取り組みを強化し、セキュリティ対策に本格的に取り組む企業は、必要に応じて外部専門家を交え、セキュリティに関する体制を整備し、基本的な組織的対策や技術的な防御対策を実施します。	STEP を目指すきっかけ ●取引先からの要請を受けて、高度なセキュリティ対策が必要となった 企業をとりまく状況 ●日常的に受発注をしているなど、取引先企業が必要不可欠な存在となっている　等
STEP4 (P42)	より強固で広範囲なセキュリティ対策のためには、人的・組織的な対策だけでなく、必要に応じて外部専門家を交えてリスク分析を行い、技術的な対策の強化により包括的なセキュリティ対策を実施します。	STEP を目指すきっかけ ●外部監査への対応や基準達成のため、従来以上に厳格なセキュリティ対策が必要となった 企業をとりまく状況 ●企業活動においてITやデジタル技術が欠かせない存在となり、DXを積極的に推進している　等

「第2部 実践編」では、４つの各STEPにおいて、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具体的に説明します。

「第1部 経営編」で説明する経営者が実行すべき「重要７項目の取組」との対応を示した表3や、実践のために用意した各種の付録を参考に、自社の状況に合わせて対策を進めてください。

【表３】実践編と重要７項目の取り組みの対応表

実践編		ページ	経営者が実行すべき重要７項目						
			1	2	3	4	5	6	7
1	できるところから始める								
	(1) 情報セキュリティ６か条	20			●				●
2	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	22	●						
	(2) 実施状況の把握	22			●		●	●	●
	(3) 対策の決定と周知	24			●				
3	本格的に取り組む								
	(1) 情報セキュリティ基本方針の作成	26	●						
	(2) 体制の整備	26		●					
	(3) 情報セキュリティ規程の作成	27			●				
	(4) 資産管理	29			●				
	(5) 攻撃等の防御	31			●				
	(6) 攻撃等の検知	36			●				
	(7) 点検と改善	37				●			
	(8) インシデント対応体制等の整備	38					●		
	(9) 取引先 / 外部情報サービスの管理	39						●	
	(10) 情報収集と共有	40							●
4	より強固にするための方策								
	(1) 資産ベースのリスク分析	44			●	●			
	(2) 技術的対策例と活用	48			●				
	(3) セキュリティサービス例と活用	52			●				
	(4) ウェブサイトの情報セキュリティ	54			●				
	(5) クラウドサービスの情報セキュリティ	56			●				
	(6) テレワークの情報セキュリティ	58			●				
	(7) セキュリティインシデント対応	62					●		

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重要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性の高い情報や個人情報を万一漏えいさせてしまった場合は、取引先や顧客等から損害賠償請求を受ける等、大きな経済的損失を受けることになります。

一方、こうした損害賠償等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等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約 2.5 億円以上の損失が発生

（所在地：北陸／業種：建設業／従業員規模：20 ～ 999 名）
VPN 機器からの侵入が原因で、コンピュータ及びファイルサーバーがランサムウェアに感染した。年 2 回の頻度でリストア訓練を実施していたこともあり、発覚から 5 日後にはバックアップデータから基幹システムを再稼働させることができたが、各社内システムの利用再開は 41 日、リモートアクセスの利用再開は 4 か月を要した。業務が止まることはなかったものの、約 1 か月間はシステム利用ができないことによる業務への影響が発生し、従業員のパフォーマンスが低下した。加えて、ファイルが暗号化され、結果的に社内のファイルの 2 割強を失った。
本事案への対応として、原因･事故範囲調査、システム復旧、再発防止のために約 2.5 億円以上、45 人月もの金額･工数を対応に費やすことになってしまった。また、個人データ・機密データの漏えいのおそれがあり、個人情報保護委員会への報告等の対応も行うこととなった。
感染の 1 か月前に VPN 機器の入替について社内で議論していたが、別メーカーの機器をすぐに導入するのではなく、後継機種を約半年待つという意思決定を下したことで、その間に感染を許してしまった。
その後、EDR やバックアップ製品、監視サービスの導入などの技術的な対策を強化し、再発防止を図っている。
出典：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「インシデント損害額調査レポート第 2 版　別紙「被害組織調査」」

（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、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。
- 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「サイバーセキュリティ関係法令Q&Aハンドブック[4]」にてQ&A形式で解説しています。企業実務の参考としてご活用ください。

(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。

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ある。
4 ▲サイバーセキュリティ関係法令Q&Aハンドブック(NCO)　企業における平時のサイバーセキュリティ対策及びインシデント発生時の対応に関する法令上の事項に加え、情報の取扱いに関する法令や情勢の変化等に伴い生じる法的課題等を可能な限り平易な表記で記述している。

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。「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。

●3 本格的に取り組む （3）情報セキュリティ規程の作成 P27-P28
●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。
●内閣官房国家サイバー統括室 関係法令Q＆Aハンドブック
https://security-portal.cyber.go.jp/guidance/law-handbook/v2-index.html

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。

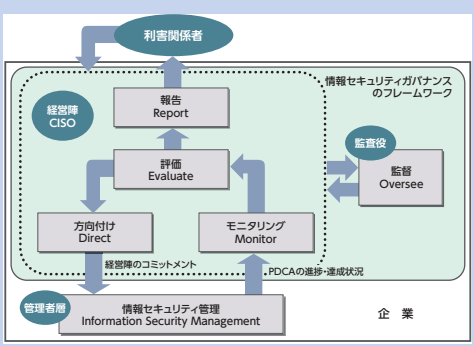
コラム

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。

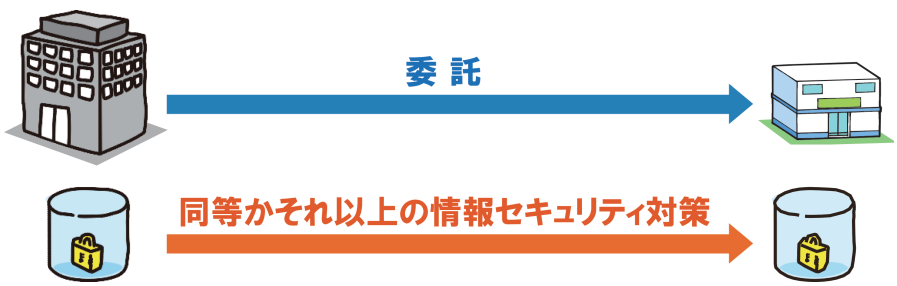
この枠組みは、経営者が懸念する避けるべき重大事故などを示して「方向付け」を行い、対策の進捗や点検等により状況を「モニタリング」し、その効果を「評価」して方向付けを見直すサイクルを骨格としています。

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。



原則２　委託先の情報セキュリティ対策まで考慮する

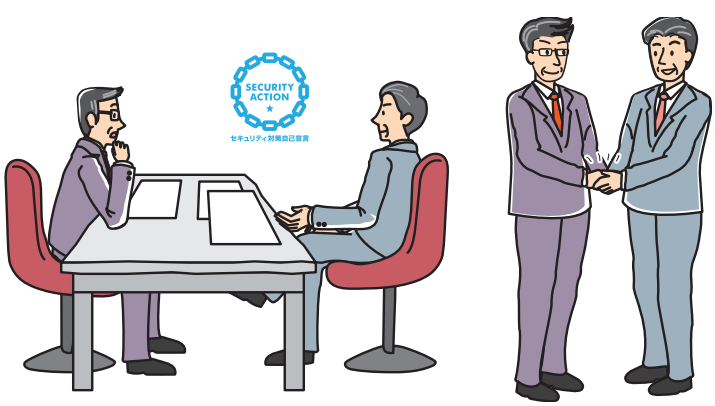
業務の一部を外部に委託するにあたって重要な情報を委託先に提供する場合、委託先がどのような情報セキュリティ対策を行っているか考慮する必要があります。委託先に提供した情報が漏えいしたり、改ざんされたりしたとき、それが委託先の不備だったとしても、事故の影響を受ける者から委託元としての管理責任を問われることになります。そのため、委託先や、共同で仕事を行っているビジネスパートナーなどの情報セキュリティ対策に関しても、自社同様に十分な注意を払います。また、受託している場合には、委託元の要求に応じる必要があります。



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、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[5]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。

5▲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」や「中小企業向けサイバーセキュリティ対策支援者リスト」を活用することができます。

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[6]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。

6▲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
NCO(国家サイバー統括室)のウェブサイト　https://www.nisc.go.jp/
警察庁 サイバー警察局のウェブサイト https://www.npa.go.jp/bureau/cyber/index.html

コラム

セキュリティ対策に関する取引先とのパートナーシップ構築

近年サプライチェーンの弱点を突いたサイバー攻撃が増加しています。サイバー攻撃への対策が不十分な場合、取引先の事業活動にまで影響を及ぼす可能性があるため、セキュリティ対策は、サプライチェーンを構成する企業間において取り組むことが求められています。実際に、取引先からセキュリティ対策の実施を求められることも少なくありません。

一方で、実施するセキュリティ対策の内容によっては費用がかかります。取引先からのセキュリティ対策の要請に対して、限られた予算の中で具体的対策を行っていくためには、取引関係のある企業間でパートナーシップを構築し、必要なセキュリティ対策の実施とともに価格交渉を実施し、企業間で円満に合意することが肝要です。

取引関係にある企業が円満に合意するために覚える必要がある要点は以下の通りです。

- ●価格交渉を適切に行えるよう、セキュリティ対策の必要性や費用負担の考え方等について、日頃から企業間において十分なコミュニケーションを取ること
- ●価格交渉には積極的に対応すること
- ●セキュリティ対策の実施に当たっては国の支援策※1の活用も検討すること
- ●必要に応じて、価格交渉に当たって支援機関※2に相談すること

企業間でパートナーシップを構築することは、セキュリティ対策強化への第一歩です。取引先企業と積極的なコミュニケーションを取り、パートナーシップの構築に努めましょう。

※1　主な国の支援策

- ●**サイバーセキュリティお助け隊サービス**
  https://www.ipa.go.jp/security/otasuketai-pr/
- ●**デジタル化・AI導入補助金**
  https://it-shien.smrj.go.jp/

※2　主な支援機関

- ●**公正取引委員会の相談窓口**
  https://www.jftc.go.jp/soudan/soudan/yuetsutekichii.html
  https://www.jftc.go.jp/soudan/soudan/shitauke.html
- ●**取引かけこみ寺**
  https://www.zenkyo.or.jp/kakekomi/

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 できるところから始める

(1)情報セキュリティ6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。そこで、企業の規模に関わらず、必ず実行すべき重要な対策を情報セキュリティ６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６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。

No 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、または最新版を利用するようにしましょう。

No 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。

※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

No 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。

No 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。

No 5. バックアップを取ろう！

故障や誤操作、ウイルス感染などにより、パソコンやサーバーの中に保存したデータが消えたり、暗号化されたりしてしまうことがあります。事業が継続できるようバックアップを取得しておきましょう。

No 6. 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のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げたりしてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策を取りましょう。

コラム

適切なバックアップ運用を行う

失ったデータの復旧は困難であり、加えて復旧には人手と時間を要します。しかし、バックアップを取得しておくことでこの被害を軽減することが可能です。

以下を参考にし、今後の運用の参考にしてください。

●バックアップを取得する
対象を選定する　／　取得方法や取得日時、間隔を検討する
●バックアップを保管する
保管場所を検討する　／　世代管理を行う　／　保管期間を決める
●バックアップから復旧する
復旧計画を立てる　／　正しく復旧できることを確認する

迅速にデータを復旧し業務継続できなければ、組織の信頼も失墜し、組織存続の問題に繋がりかねない大きなリスクとなります。適切な運用を行いましょう。

●参考：情報セキュリティ10大脅威「組織編」共通対策
https://www.ipa.go.jp/security/10threats/index.html

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、STEP 1（情報セキュリティ6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6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. バックアップを取ろう！
6. 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/

2 組織的な取り組みを開始する

基本的なセキュリティ対策を組織的に取り組むために、自社の弱みを把握し基本的対策を決定します。具体的には、組織としての情報セキュリティ基本方針を作成し、「5分でできる！情報セキュリティ自社診断」を活用して自社のセキュリティ対策の実施状況を把握し、対策を決定・周知します。

(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。ただの確認作業ではなく、現状の対策状況を客観的に可視化し、「今すぐ改善すべき点」や「優先順位の高い対策」を導きます。加えて、定期的に活用することで、常に最新の状態を保ち、変化するリスクに対応できます。

自社診断は、表4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通りです。

- ●経営者または情報セキュリティの担当や部門長など実施状況がわかる人が「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。
- ●実施状況がわからない場合は、各従業員に質問して、総合して記入します。
- ●チェック欄の該当するもの1つに○をつけて、「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４】自社診断のための 25 項目

No		診断内容
Part 1 基本的対策	1	パソコンやスマートフォンなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2	パソコンやスマートフォンなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？
	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	データの共有設定を必要な人に限定していますか？
	5	故障や誤操作、ウイルス感染などによる重要情報※2 の消失に備えて定期的にバックアップを取得していますか？
	6	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
Part 2 従業員としての対策対策	7	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？
	8	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？
	9	重要情報の受け渡しは、暗号化など安全な手段で行っていますか？
	10	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？
	11	インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？
	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	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？
	15	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
	16	関係者以外の事務所への立ち入りを制限していますか？
	17	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
Part 3 組織としての対策	18	内部ネットワークを守るため、不正アクセス対策機能を設定していますか？
	19	ウェブサイトで公開すべきでない情報を公開していませんか？
	20	従業員に情報セキュリティに関する教育や注意喚起を行っていますか？
	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流出した場合に組織のイメージダウンや損害賠償責任を問われるなどの管理責任を伴う情報のことです。

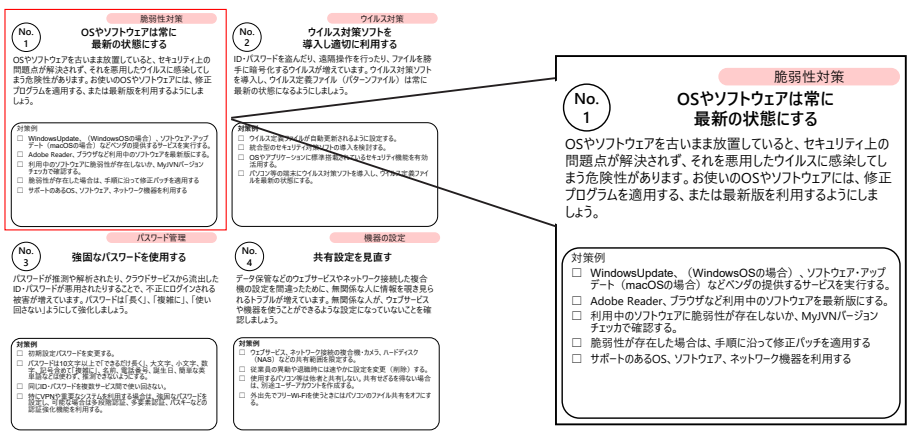
(3)対策の決定と周知

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制度二つ星を宣言することのメリット

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、STEP2（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

コラム

IoT 機器のセキュリティ確保について（JC-STAR の活用）

近年、IoT（Internet of Things ／モノのインターネット）製品は、家庭やオフィス、工場などあらゆる場所で急速に普及しています。スマート家電、監視カメラ、産業用センサーなど、インターネットにつながることで利便性や効率が向上する一方、セキュリティ対策が不十分な場合、大きなリスクも生じます。

IoT 製品におけるセキュリティ対策の重要性が高まっている一方、調達者・消費者から見て IoT 製品のセキュリティ対策が適切か否かについては判断が難しいという課題があります。サプライチェーン管理が重要視される昨今において、自社が取り組むべき、調達製品のセキュリティ対策状況を確認することが難しい現状があります。

IoT 製品に対するセキュリティ対策の適合性を確認・可視化する制度として、我が国ではセキュリティ要件適合評価及びラベリング制度（JC-STAR: Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements）を設けており、インターネットとの通信が行える幅広い IoT 製品を対象として、共通的な物差しで製品に具備されているセキュリティ機能を評価・可視化することが可能です。

JC-STAR の適合ラベルを取得した製品のパッケージ、筐体、取扱説明書、ウェブサイト等に表示される二次元コードを読み取ることで、製品詳細や適合評価、セキュリティ情報・問合せ先等の情報を調達者・消費者が簡単に取得できるようにしています。

●セキュリティ要件適合評価及びラベリング制度（JC-STAR）
https://www.ipa.go.jp/security/jc-star/index.html

3 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(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)情報セキュリティ基本方針※の作成

情報セキュリティ基本方針は、責任の所在や行動指針を明確にし、組織全体で一貫したセキュリティ対策を実現するために不可欠です。

●自社のセキュリティ基本方針を策定し、周知する

セキュリティに取り組む自社の姿勢を社内外に示し、組織の信頼性を向上させるとともに、役職員の意識や行動改善を促しましょう。

そのために、セキュリティ推進活動に係る自社の基本方針を文書化し、役職員や社外要員に周知しましょう。

※「2. 組織的な取り組みを開始する」の「(1)情報セキュリティ基本方針の作成と周知」(P22)を参照ください。

(2)体制の整備

セキュリティ担当の明確化、定期的な経営層への報告、社内ルールの策定・周知等を通じて、リスク管理体制を構築します。これにより、セキュリティインシデントの未然防止と迅速な対応が可能となります。

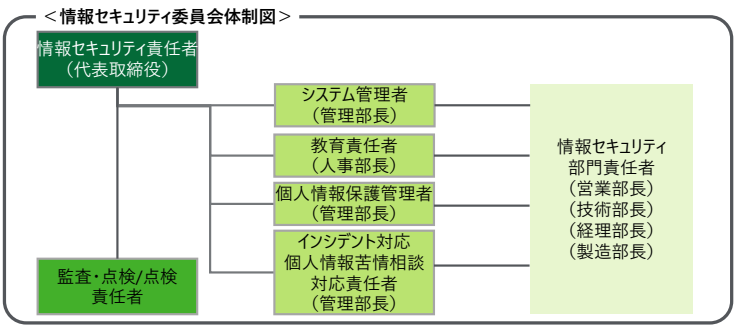
対策の実行に必要な人材の確保と育成については、**「中小企業のためのセキュリティ人材確保・育成の実践ガイドブック」(付録1)**の解説を参照してください。

●セキュリティ推進活動を担当する部署や役職員を決定し、責任及び権限を割り当てる

セキュリティを担当する役職員や部署の役割・責任を文書化し、平時及び有事に備えた連絡先リストを整備しましょう。

また、経営層が参加する情報セキュリティ委員会等で、セキュリティ基本方針や資源配分について審議し、決定した内容の記録、全社への周知とフォローを徹底して確実に実行しましょう。

加えて、サイバー攻撃及び予兆を監視・分析する体制を整備し、入手した情報又はログの分析などによりサイバー攻撃及び予兆、インシデントの発生の検知を可能にしましょう。



●セキュリティに関する法令や、契約等に規定された事項を考慮し、社内ルールを策定及び周知する

法令や契約の違反による罰則や信用失墜というリスクを未然に防ぎ、現場における運用上の判断誤りを抑えるために、法令や契約等の要求を体系的に整理して社内ルールへ反映し、教育と周知まで行いましょう。

●守秘義務のルールを策定し、遵守させる

守秘義務の文書化及び内容の説明により、役職員及び社外要員への機密保持に対する意識付けを行い、機密保持を徹底させましょう。

また、禁止行為を明確にして違反への抑止力を高め、規律の実効性を確保するために、機密性の高い情報を取り扱う役職員（社外要員を除く）に、守秘義務の誓約書を提出させ、書面の保管や更新、回収を計画的に管理しましょう。

（3）情報セキュリティ規程の作成

以下に示す①～③を参照して、組織や担当者の経験や判断によってリスク分析を行い、自社に必要なセキュリティ対策を追加し、自社に適した規程を作成します。

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ます。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）**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。

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)資産管理

自社IT基盤や資産の現状把握、情報の分類・保護の徹底は、情報漏えいや不正アクセスなどのリスクを最小限に抑えるために不可欠です。

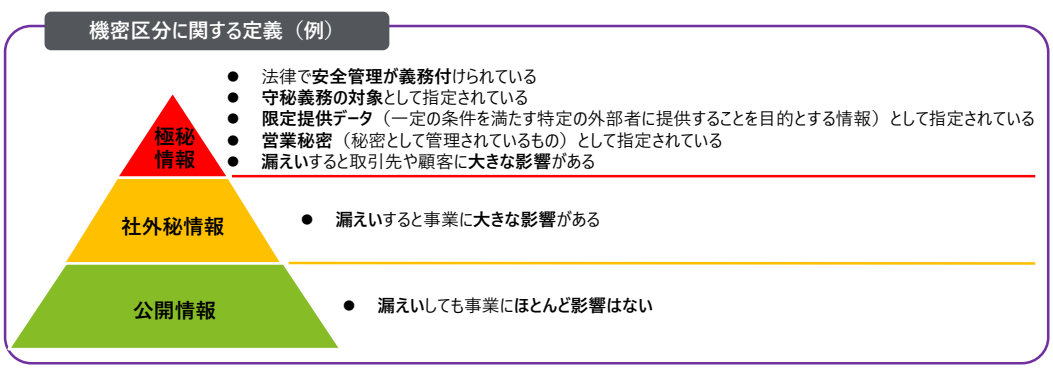
●ハードウェア、OS、ソフトウェア及びネットワークに関する情報を把握する

組織で使用する情報機器やソフトウェアを組織全体で正確に把握し、抜け漏れや管理の属人化を避けるために、ハードウェア、OS及びソフトウェア等の情報を整理しましょう。

また、自社のネットワークに関するインシデントが発生した場合における影響範囲を正確に把握し、的確な対処を可能とするために、本社や事業所等、各拠点におけるネットワークについて、構成機器や保守事業者の情報を整理しましょう。加えて、主要なネットワークセグメントやデバイスの配置等を記載したネットワーク図(構成図)を作成・版管理し、構成変更の度に更新して活用しましょう。

●機密区分に応じた情報の管理ルールを定め、それに基づく管理を行う

重要度の高い情報資産がどこにあるのか把握し、情報の機密性に応じて濃淡をつけたセキュリティ対策に取り組むために、情報の機密区分を設け、区分に応じた取扱方法や取扱エリアの区分及び制限等を定めた文書を整備しましょう。また、役職員の退職や派遣社員等の契約満了後における情報の不正利用を防ぐために、退職/任期満了時に情報や機器・ID・鍵等を回収し、加えて復元できない方法によりデータを消去して、チェックリストや証跡で実行状況を可視化しましょう。



●テレワークで使用する情報機器及び機密性の高い情報についてのルールを定める

テレワークを実施する場合は、使用を許可する機器の申請・承認の方法、個人所有端末にダウンロード可能なファイルの機密区分・種類等を規定し、従業員に周知しましょう。

●脆弱性の管理体制、管理プロセスを定める

自社に対するサイバー攻撃の成功確率を大きく下げ、被害の発生を防止するために、担当部署の役割・責任を定め、情報収集、脆弱性に対するセキュリティパッチの評価、修正対応を行い、対応履歴を定期的に確認して是正しましょう。

コラム

脆弱性対策について

脆弱性とは、ある製品やサービスに含まれる、セキュリティ上の弱点のことを指します。脆弱性を悪用されると、製品やサービスの機能を不正利用され、システムを破壊されたり、情報を消されたり漏えいしたりします。

脆弱性を放置することは非常に危険です。利用している製品のホームページを定期的に確認のうえセキュリティパッチ等を注視し製品を最新の状態にアップデートしましょう。また製品を選択する場合には、その製品の機能や価格だけではなく、脆弱性が発見された場合にはきちんと対応してくれるのか（製品をアップデートしてくれたり、脆弱性対策の方法を公開してくれたりするのか）どうか、サポートの手厚さやサポート期限等も考慮して製品を選択することが肝要です。

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、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイトとして、JVNがあります。情報収集で活用しましょう。

●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））
https://jvn.jp

コラム

IT 資産管理について

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。

IT 資産管理とは、社内で利用している IT 機器やソフトウェア、ライセンス、クラウドサービスなどを正確に把握し、適切に管理することです。具体的には、以下の活動が含まれます。

- ●何の機器やソフトウェアが、どこで、誰によって使われているかの把握
- ●購入・廃棄・更新の履歴管理
- ●ライセンスや契約の期限管理
- ●セキュリティ更新やパッチ適用の状況確認

未管理の機器やソフトウェアは、セキュリティホールになりがちです。資産が把握できていれば、脆弱性のあるソフトウェアや、サポート切れの機器を速やかに洗い出し、適切な対策ができます。万が一の故障や災害時にも、どの IT 資産が事業に不可欠か、どこにバックアップがあるかを把握していれば、迅速な対応が可能です。

IT 資産管理は、単なるリスト作りや棚卸しではありません。事業を守るリスク管理であると同時に、資産の有効活用による業務効率化にもつながります。まずは「資産管理台帳（サンプル）」（付録 6）を参考にして、一覧表や管理台帳の作成から始め、定期的な見直しを習慣化しましょう。

また、事業にリソースを集中する中で IT 資産管理に労力を割くことが難しい場合は、IT 資産管理をすべて自社で賄おうとするのではなく、以下の選択肢についても検討しましょう。

- ●一元管理を可能とする IT 資産管理ツールの導入やクラウドサービスの利用
- ● IT 資産管理代行サービスの利用（IT 資産管理の外部委託）
- ●「中小企業のためのセキュリティ人材確保・育成の実践ガイドブック」（付録 1 ）に沿ったセキュリティ人材の確保と育成

(5)攻撃等の防御

企業の資産や情報を脅威から守るため、認証管理やシステム保護、教育など多様な防御策を実施します。総合的な対策によって、攻撃や事故のリスクを最小限に抑えます。

①IDアクセス制御

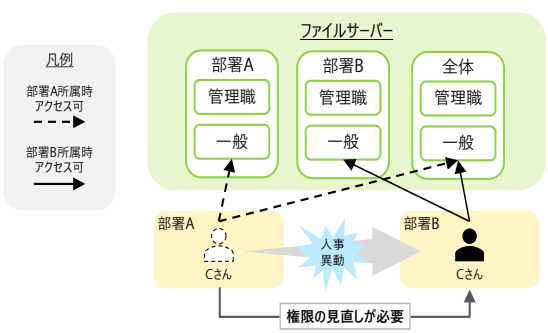
IDやアクセス権の管理、重要な設備への入退室管理等は、内部・外部からの脅威に対するリスク低減に不可欠です。適切なアクセス管理を行うことで、重要な情報資産の漏えいや改ざん、機器の盗難・破壊を防ぎます。

●ユーザーID及び管理者IDの発行・変更・削除の手続を定める

ユーザーIDや管理者ID(管理者権限を保持するID)を漏れなく管理し、不正アクセスの被害等を防止するために、IDの発行から削除までを管理するプロセスを定め、必要最小限の割り当てとなるようにしましょう。また、共有IDはなるべく使わないようにし、やむを得ず使う場合は共有IDを利用したユーザーを特定可能とするような仕組みを整備して規定の通り運用しましょう。

●アクセス権の管理ルールを定める

従業員の異動や退職等に伴う権限の変更・削除漏れ、特定役職員等への権限集中によるシステムの不正利用や権限濫用の被害を防止するために、事業所やフロアの入室、システムのアクセス権限を見直すルールを定め、権限の付与状況を管理しましょう。また、アクセス権限の運用や利用状況を監視する仕組みを整備しましょう。



●パスワードの設定及び管理に関するルールを定め、周知する

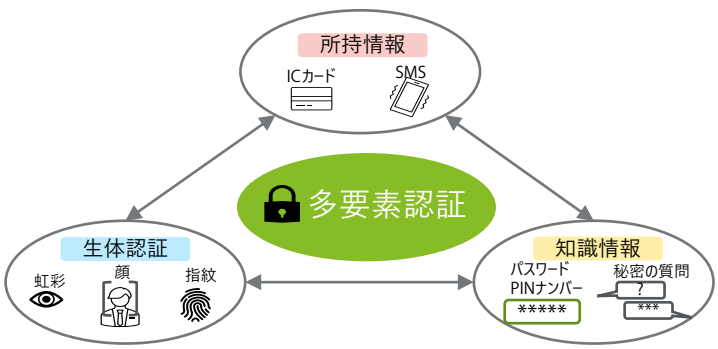
不正アクセスを防止するために、パスワードは複雑さを保持するとともに、社内システムやデバイスで使い回しを防止するルールを定め、従業員に周知しましょう。

また、パスワードの漏洩を防止するために、紙、ファイル、パスワード管理アプリ等、各保管方法の違いを理解し、自社に適したパスワードの全般的な管理ルールを定め、従業員に周知しましょう。

●システム及び情報の重要度に応じて認証の強度及び実装方法を決定する

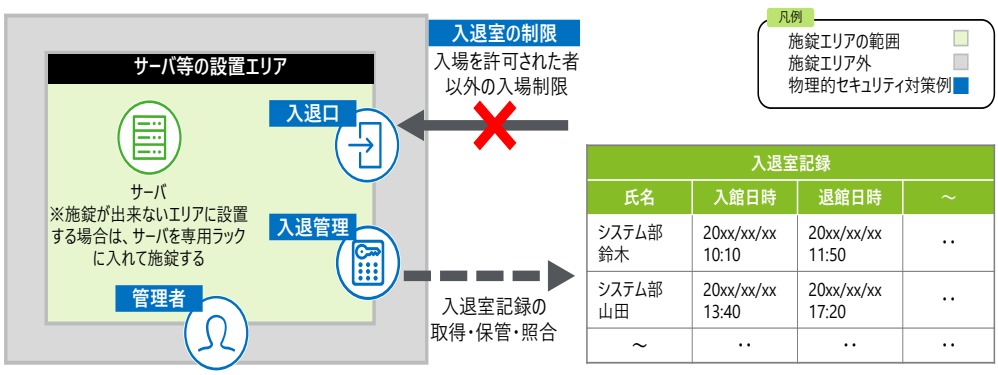
不正アクセスを防ぐために、取り扱う情報の重要性に応じて情報にアクセスするための本人認証方法と管理ルールを定め、複数の要素を組み合わせて認証を行う多要素認証を活用しましょう。情報機器、システムの乗っ取り防止のために、管理者権限のリモート接続や機密性の高い情報に対するインターネットを経由したアクセスについて、接続元制限や端末要件を規定して遵守状況を確認しましょう。

また、不正なログオン、情報流出等の被害の発生を防止するために、社内システムを構成する端末にアカウントロック制御を実装して、ログオン試行回数の制限やアカウントロックの運用を行いましょう。



●サーバー等の設置エリアへの入退室を管理し、記録する

情報の持ち出し、機器障害等を防止するために、サーバー等設置エリアに対する入室可能な者を制限し、入退室記録の取得・保管を行いましょう。



●可搬媒体の持込み・持出しを制限する

情報の持ち出し等を防止するために、可搬媒体（パソコン、カメラ、外部記憶媒体等で個人所有機器を含む）の管理ルールを定め、不要な持込み・持出しを制限するとともに、返却や廃棄等の記録を行いましょう。

②データセキュリティ

暗号化等の情報漏洩時の影響を緩和するための保護措置や適切な保管、バックアップにより、不正アクセスや災害等による重要データの漏洩・消失を防止します。これにより、企業としての信用を維持し、事業継続性を守ります。

●情報機器及び情報システムの保管データに対して、情報漏えい時の影響を緩和するための保護措置を講じる

情報漏えい等を防止するため、暗号化等の情報漏洩時の影響を緩和するための保護措置を講じるルールを定め、従業員に周知しましょう。

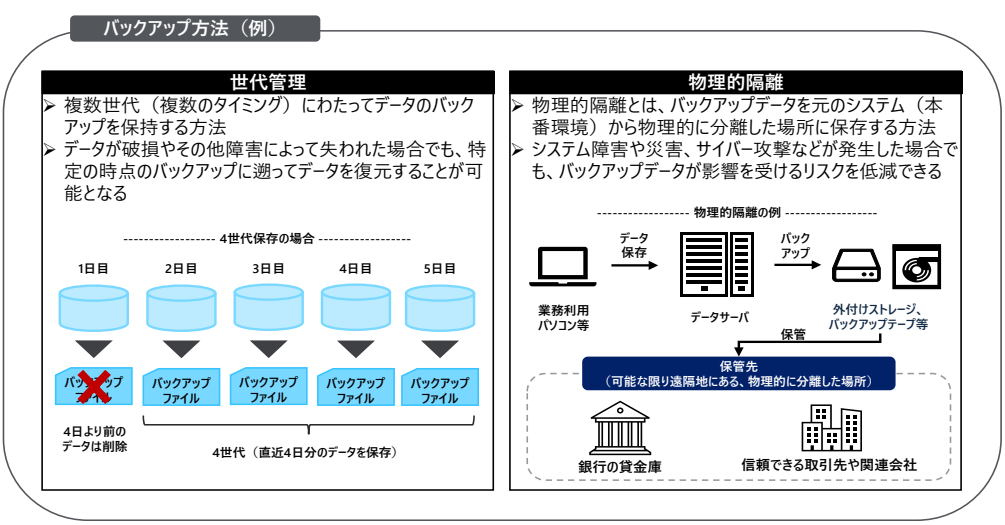
●重要データの保管や、取引先等との情報共有及び情報送信に関するルールを定め、周知する

重要データの消失を防止するために、重要データを端末ではなく安全なサーバーで保管する等のルールを定め、従業員に周知しましょう。

また、取引先等との間でも、履歴が残らない情報の送信方法を禁止し、取り組みの実施状況を記録・ 保管する等のルールを定め、従業員に周知しましょう。

●適切なバックアップを行う

バックアップすべきデータの取得漏れを防止し、データの復旧を可能とするために、バックアップの対象・頻度を定め、遠隔地を含めた保管方法やリストア手順書を整備しましょう。



③プラットフォームセキュリティ

安全な構成の確立、端末やサーバーの基礎的な保護等を通じて、システムの弱点を突いた攻撃やウイルスによる被害を防ぎます。また、ログを取得し、サイバー攻撃に関する予兆を検知します。

●ハードウェア、OS 及びソフトウェアの安全な構成を確立し、維持する

情報漏えいの被害を防止するために、業務で不要な機器の設定やOS及びソフトウェアの利用を無効にしましょう。また、ベンダーによる推奨セキュリティ設定を参考に、標準構成・設定ルールを定めましょう。

●システムをウイルス感染から保護する

ウイルス対策ソフトウェアを導入し、適切な範囲・頻度でスキャンを実行し、ウイルス定義ファイルが常に最新の状態となるよう更新頻度を定めましょう。
また、インターネット経由でのウイルス感染によるセキュリティインシデント発生を防止するために、URL フィルタリング等で不正なウェブサイトへのアクセスを制限しましょう。

●ハードウェア、OS 及びソフトウェアへのセキュリティパッチ及びアップデートの適用に係る手続等を策定し、実行する

自社の情報資産を守るために、ハードウェア、OS及びソフトウェアのセキュリティに関するアップデートについて、速やかに適用する運用を定めましょう。

●サポート期限の切れた OS 及びソフトウェアの利用停止及び更改を実施する

サイバー攻撃の標的となることを防止するために、ハードウェア、OS及びソフトウェアのサポート期限を定期的に確認しましょう。サポート切れのハードウェア、OS及びソフトウェアについては利用停止し、利用の継続が必要なものについてはサポート期限が切れる前に更改を実施しましょう。

●情報機器及びシステムに関するログを取得し、異常を検知するため、定期的にレビューを行う

情報機器や情報システムに対する不審なアクセスを把握し、サイバー攻撃の予兆を検知して被害を防止するため、通信ログや認証ログを取得・保管するとともに、ログの改ざん防止を行った上で、定期的にレビューを行いましょう。

④技術インフラの境界防護

社内外ネットワークの分離と境界部分の防護を行い、不正な通信や侵入のリスクを低減します。適切な境界防御は、組織の情報資産を安全に守る基盤となります。

●内外のネットワークを適切に分離し、境界部分を防護する

不正アクセスによる情報漏えい被害を防止するために、社内と社外のネットワークの境界を明確化し、自社ネットワークを防護するためのファイアウォールを導入し、設定を有効にしましょう。また、公開サーバーや機密性の高い情報を扱うサーバー、工場等、用途と取扱情報が異なるネットワークはセグメント分離して運用しましょう。

※必要に応じて、経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」を参照ください。

⑤意識向上とトレーニング

適切な教育とルールの周知により、情報漏えいやリスクの発生を未然に防ぐことが重要です。組織全体での継続的な学びと意識の共有が、安全な運営の基盤となります。

●経営陣を含むすべての役職員や社外要員に対して、セキュリティの意識向上のための教育・研修を実施する

役職員等のセキュリティ意識を向上し、セキュリティ事故を防止するために、全役職員等に対し意識向上教育を定期的に実施しましょう。

また、実施記録を保管するとともに、理解度と受講状況の評価結果を踏まえて改善しましょう。

●セキュリティインシデント発生時の対応に関する教育・訓練を行う

セキュリティに関する役職員や社外要員の意識付けを行うため、定められた頻度でセキュリティインシデント対応の教育・訓練を実施しましょう。

また、実施状況を記録・保管するよう定めるとともに、定期的に教育・訓練内容の見直しを行いましょう。

（6）攻撃等の検知

サイバー攻撃の予兆や異常を早期に発見するため、システムやネットワーク、機器の状態を継続的に監視・分析します。被害拡大を防ぐとともに、迅速な対応が可能となります。

●ネットワーク上の適切な場所でネットワーク接続及びデータ転送を監視する

不正アクセスをリアルタイムで検知・遮断するために、プロキシサーバーや侵入検知システム、ファイアウォールや端末の通知設定を行い、監視を行いましょう。

●ハードウェア及びソフトウェアの状態及び挙動を監視する

ユーザーによる自由なダウンロード・インストールでウイルスが混入することを避けるために、利用を許可するソフトウェア一覧を作成し、定期的にソフトウェアのインストール状況について点検しましょう。また、外部から受け取ったファイルについては、ウイルス対策ソフト等により安全性を確認しましょう。

コラム

サイバー攻撃被害情報の共有・公表について

サイバー攻撃の脅威は年々増大し、その手口も巧妙化しています。従来は「自社が守れればよい」という考えが通用したかもしれません。しかし、企業はネットワークや取引関係で密接につながっており、一社の被害が他社や社会全体に波及するリスクが高まっています。こうした状況で、サプライチェーンにおけるサイバー攻撃被害情報の共有・公表がいかに重要か、改めて考えてみましょう。

1. 被害の連鎖を防ぐ「早期警報」の役割

サイバー攻撃は、一社が攻撃を受けた情報が迅速に共有されれば、他の組織も同様の攻撃に備えたり、被害を最小限に食い止めることができます。また、自社のサービス提供を支える取引先が被害を受けた場合に、自社の事業継続に支障が出る可能性があるため、被害情報の共有はサプライチェーン全体への「早期警報」となります。

2. 信頼性と透明性の確保

被害を隠すことは、後に外部から発覚した際に「隠ぺい体質」として社会的信用を失う大きなリスクとなります。サプライチェーンにおいては、万が一サイバー攻撃の被害に遭った場合においても被害をきちんと公表し、再発防止策を明示する姿勢は、顧客や取引先からの信頼性向上につながります。透明性を持った情報発信は、危機管理能力の証となります。

サイバー攻撃の脅威は、もはや一企業だけの問題ではありません。被害情報の共有・公表は、サプライチェーン全体でリスクを減らし、次なる被害を防ぐための第一歩です。取引の継続に支障が出ることを懸念して公表を控えるのではなく、被害情報を取引先に共有、公表することで早期の原因究明や復旧態勢が自社で整備されていることを明示し、サプライチェーンにおいて自社が確たるセキュリティ対策を実施済みの企業であることを示しましょう。

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

(7)点検と改善

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を行うことも検討します。

●定期的に経営層へ対策実態に関する報告を行い、報告結果を対策の推進に反映する

セキュリティ対策の現状と今後の対応について経営層の承認を得るために、点検結果と当該結果を踏まえて策定したセキュリティ対策推進計画を定期報告し、指示を文書化・全社共有の上、是正完了まで追跡しましょう。

コラム

情報セキュリティ対策状況の点検方法と点検基準

点検の方法には以下を用いることができます。

① **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

② **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

③ **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

④ **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

⑤ **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

また、点検の基準には以下があります。
(点検基準例)
1. 情報セキュリティ6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
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

（8）インシデント対応体制等の整備

セキュリティ事故時の対応手順や復旧手順の整備等、十分なインシデント対応は、サイバー攻撃による業務中断や、個人情報の不正利用、社会的信用の失墜といった深刻な影響を回避するために不可欠です。

●セキュリティインシデントとして扱う対象範囲を明確にする

不測の事態発生時における判断と初動対応の遅れにより、セキュリティインシデントの被害が拡大することを避けるために、インシデントの対象範囲とレベル、判定基準を定義し、エスカレーションルールを定め、従業員に周知しましょう。

●セキュリティインシデントへの対応手順、対応体制等を定める

初動対応を早く確実に行い、情報セキュリティ責任者や関係者へ必要な情報を報告するために、インシデント対応手順や役割分担、報告事項や連絡体制を定めましょう。また、セキュリティ事故の事例及びその対応策を社内で定期的に共有しましょう。

●事業上重要なシステムについて、事業継続の要件に沿う復旧に必要な準備を行う

自然災害や情報機器の故障・不具合等に対する復旧対応準備の不足による、情報システムの長期停止を防止するために、目標復旧時間（RTO）※1と目標復旧時点（RPO）※2に合わせてバックアップ取得や手順整備を行い、訓練で実効性を検証しましょう。

※1　目標復旧時間（RTO）：RTO は Recovery Time Objective の略語で、目標復旧レベルまでの復旧に要する時間を指す。

※2　目標復旧時点（RPO）：RPO は Recovery Point Objective の略語で、目標とする復旧の時点（直近のバックアップ時点）を指す。

(9)取引先/外部情報サービスの管理

取引先とのルール設定やセキュリティ対策状況の把握、自社の機密性の高い情報を取り扱うクラウドサービスなどの外部サービスの利用状況や安全性の把握は、情報漏えいや不正アクセスなどのリスクを低減するうえで極めて重要です。

●取引先と自社とのビジネス又はシステム上の関係を把握する

自社以外の組織が管理・提供し、自組織の資産が接続している主要な情報システムを把握するための仕組みを整備したうえで、取引先との契約内容やセキュリティ要件が現在の状況に合っているか、問題が起きた際に誰に何を確認すべきかを明確にしましょう。

●取引先との間で、機密性の高い情報の取扱い方法を明確にする

機密性の高い情報として取扱うべき対象の抜け漏れ防止やリスクに応じた対策を策定し、取引先とのやり取りにおけるインシデント発生の未然防止や被害の拡大防止につなげるために、機密性の高い情報に該当する情報資産を定め、取引先とのやり取りにおける管理ルールを整備しましょう。

●自社に影響を及ぼす可能性のある取引先のセキュリティ対策状況を把握する

事業継続リスク及び情報管理リスクの観点から、取引先の対策状況を定期的に評価し、是正と再確認を計画的に実施して結果を記録しましょう。

●セキュリティインシデント発生時の他社との役割及び責任を明確にする

インシデント対応を他社と自社共同で機能させ、初動の遅延を防ぐために、インシデント発生時の通知義務・連絡先を文書化し、役割分担と連絡体制を相手先と合意の上、訓練で実効性を確認しましょう。

●取引先との契約終了時に機密性の高い情報及びアクセス権等を回収又は破棄する

情報資産の不正利用リスクを減らすために、責任者と期限を設定して、契約終了時の機密性の高い情報及びアクセス権の回収/破棄をチェックシートで運用し、記録を保管しましょう。

●自社の機密性の高い情報を扱う外部情報サービスを管理する

情報漏えいや不正アクセスなどのリスクを低減するために、クラウドサービスなどの外部情報サービスを利用する際のセキュリティ要件を定め、利用状況を把握しましょう。

また、外部情報サービスの提供事業者と機密性の高い情報の取扱い方法について取り交わしましょう。

(10)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[7] に登録したり、セミナーに参加したりして積極的な情報収集を行います。

②組織内での共有

収集した情報は、組織内の関係者全員に適切に共有することで、情報セキュリティ対策の精度を向上させることができます。具体的には、定期的な会議やメール配信、社内ポータルサイトを活用する、情報セキュリティに関する最新情報のデータベースを構築するなどにより、情報の共有を徹底します。

③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性の高い情報が含まれる可能性がある場合は、秘密保持契約を交わします。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[8] が組織されている場合があります。

7▲SNSは、Social Networking Service(ソーシャル・ネットワーキング・サービス)の略。登録した利用者だけが参加できるインターネットのWebサイトのこと。(総務省　国民のためのサイバーセキュリティサイト)

8▲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

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 サイバー警察局
https://www.npa.go.jp/bureau/cyber/index.html
■ NCO（国家サイバー統括室）
https://www.cyber.go.jp/index.html
（情報共有の考え方・枠組み）
■一般社団法人日本シーサート協議会
https://www.nca.gr.jp/

コラム

SCS評価制度★3、★4を見据えた準備

経済産業省及び内閣官房国家サイバー統括室が推進する、「サプライチェーン強化に向けたセキュリティ対策評価制度」（SCS評価制度）とは、企業のセキュリティ対策レベルを★3（専門家確認付き自己評価）、★4（第三者評価）で評価する仕組みです。主に中小企業の信頼性向上やサプライチェーン対策強化を目的として、2026年度下期の制度開始を目指して整備が進められています。

制度において設ける段階の考え方

★3　全てのサプライチェーン企業が最低限実装すべきセキュリティ対策として、基礎的な組織的対策とシステム防御策を中心に実施

★4　サプライチェーン企業等が標準的に目指すべきセキュリティ対策として、組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施

★3、★4相当のサイバーセキュリティ対策を行うことで、サプライチェーン強化に向けたセキュリティ対策を実施済みの企業または先進的な企業として自社が認知されることになります。その結果、高いセキュリティレベルと運用力を客観的に示すことができ、取引先・顧客からの信頼向上、取引機会の拡大にも繋がります。

なお、本ガイドラインと★3、★4における要求事項との紐づけは、「情報セキュリティ関連規程（サンプル）」（付録5）P56-57に掲載していますので、必要に応じて参照してください。

4 より強固にするための方策

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、STEP1～3で進めてきた汎用的な対策（ベースライン）、組織や担当者の経験や判断によるリスク分析、分析結果に基づく対策の追加・規程の作成だけでは、必要な対策が不足する恐れがあります。

そのため、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である資産ベースのリスク分析を行うことで、各企業固有のリスクを把握し、さらなる技術的対策の強化を行う必要があります。

なお、STEP3と同様、必要に応じて外部専門家※の知見も活用して進めます。

※「（3）セキュリティサービス例と活用」（P52）を参照

ここでは、各企業の状況に応じて対策をより強固にする方策として、資産ベースのリスク分析及び分析結果に応じて必要とされる対策について解説します。

対策をより強固にする方法は下記以外にも様々なものがありますが、日々、変化する脅威に対し、各企業に必要な対策を適時に実施していくことが重要です。

（1）資産ベースのリスク分析

「資産管理台帳（サンプル）」（付録6）の「リスク値算定」シートを活用した、各企業の状況に応じてリスクを特定する資産ベースのリスク分析について説明します。

（2）技術的対策例と活用

様々な技術的対策について説明します。自社の環境に合わせて活用してください。

（3）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。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。

（4）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。

（5）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。

（6）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。

（7）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。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を行う必要性があります。

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。

一般的な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」を識別しないため、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6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資産ベースのリスク分析

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）システムを構成する各資産（サーバー、端末、通信機器等）に対して、「資産価値」「脅威」「脆弱性」の3つを評価指標として、対策を検討・実施する。

④組み合わせアプローチ

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非形式的アプローチの組合せ。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）内部状況や外部状況、自社診断を参考に、社内の担当者の知見にて、自社に必要な対策項目を追加する。

(1)資産ベースのリスク分析

各企業の状況に応じてリスクを特定する資産ベースのリスク分析の実施方法について解説します。自社の情報資産や関連する機器等を一覧化して管理するための**「資産管理台帳（サンプル）」（付録6）**の「リスク値算定」シートを活用しながら、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**「資産管理台帳（サンプル）」（付録 6）**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、**「資産管理台帳（サンプル）」（付録 6）**の「台帳記入例」・「重要度定義」シートを参考に、以下の要領で作業を進めます。

①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。

②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、評価値３～１を記入します。

③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、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３とします。

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。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５）。

【表５】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

		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
		つけ込みやすさ
脆弱性	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

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。

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。

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重要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」、全国商工会連合会が提供している「商工会の情報セキュリティサポート保険」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 などの認証を取得していたり、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

生成 AI の利用とサイバーセキュリティ ― 安全な活用のために

近年、生成 AI（ジェネレーティブ AI）の進化と普及が著しく、ビジネスや日常のさまざまな場面で活用が広がっています。文章や画像、プログラムコードの自動生成など、業務効率化や新たな価値創造に貢献する一方で、サイバーセキュリティの観点からは新たな課題も浮き彫りになっています。

生成 AI に社内機密や個人情報などの重要データを入力することで、外部に情報が流出する可能性があります。AI サービス提供側がデータを学習に利用する場合、意図しない情報拡散につながる懸念があります。

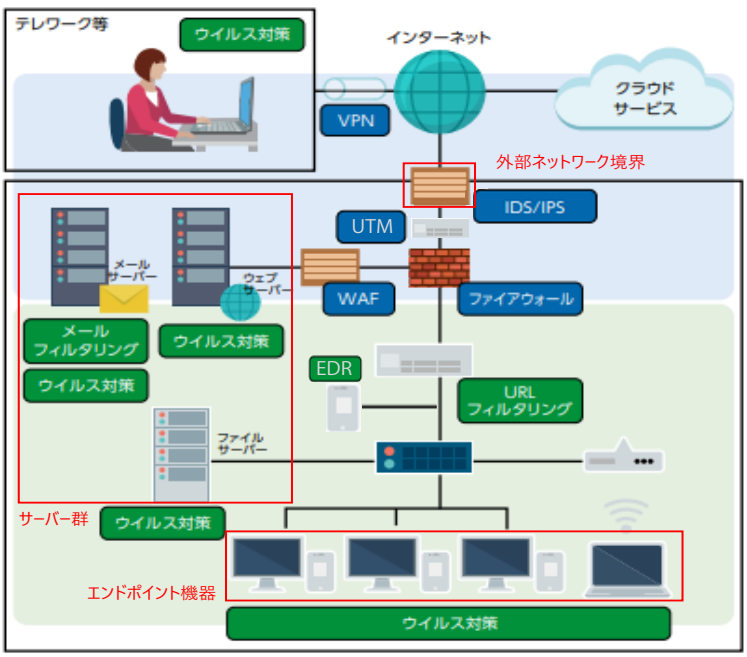
以下のような点に注意して利用することが重要です。

1. 生成 AI の利用規約やプライバシーポリシーを事前に確認し、データの取り扱い方針を把握する
2. 機密性の高い情報や個人情報など、外部に漏れると問題になるデータは AI サービスに入力しない
3. 生成された成果物は必ず人間が確認し、正確性や法的リスクをチェックする
4. AI の出力内容をそのまま業務で利用するのではなく、補助的ツールとして活用する

生成 AI は非常に便利なツールですが、サイバーセキュリティの観点からは慎重な運用が求められます。企業や組織としては、最新の脅威動向に目を配り、必要な対策を講じながら AI を活用することが重要です。安全性を確保しつつ、生成 AI のメリットを最大限に生かすことで、企業価値の向上と持続的な成長につなげていきましょう。

（2）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。資産ベースのリスク分析結果に応じて、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。

(3)セキュリティサービス例と活用

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

⑦機器検証サービス

IoT 機器をはじめとするネットワーク通信機能を持つ機器、その機器に対してネットワークを通じて操作・管理・データ処理等を行うアプリケーションから構成されるシステム（IoT システム）に対して行う次のようなサービスです。

ア　機器検証
イ　機器検証及び Web アプリケーション脆弱性診断
ウ　機器検証及びプラットフォーム脆弱性診断マネージドセキュリティサービス

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。

●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

(4)ウェブサイトの情報セキュリティ

多くの中小企業が自社のウェブサイトを開設していますが、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、対策を講じる必要があります。ここでは、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。

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。運営者は表６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６】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。

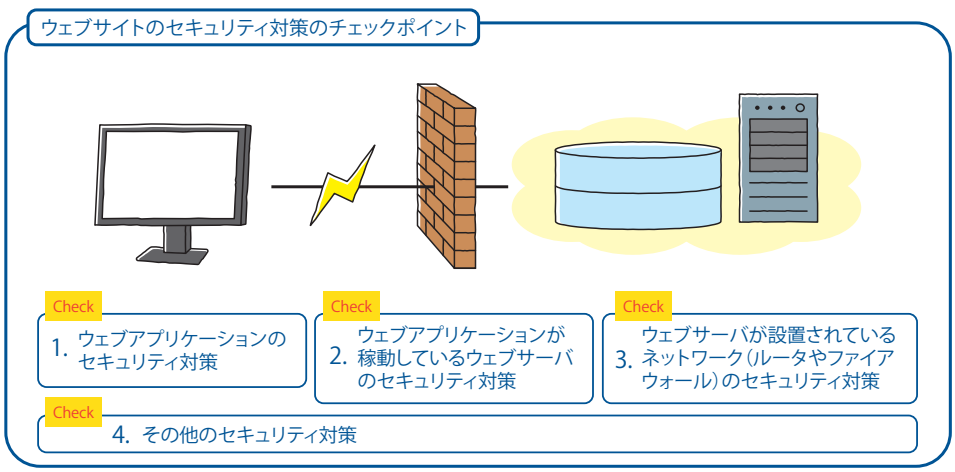
②ウェブサイトの構築

ウェブサイトの安全を維持するためには、ウェブサイトを構成する要素に対して、それぞれに適した対策を実施する必要があります。例えば、サーバー OS やソフトウェアに対しては、脆弱性修正パッチの適用や安全な設定等、共通した対応を実施することができます。

しかし、独自開発する「ウェブアプリケーション」に対しては、セキュリティ対策を個別に実施する必要があり、可能な限り開発段階において脆弱性を解消することが望まれます。ウェブアプリケーションを開発する場合、後述の「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継続的に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。参考情報にある「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。



【重要】EC サイト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が、絶えずサイバー攻撃に晒されており、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していても、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、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」を参照し、十分な対策を講じてください。

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/

(5)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。

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。

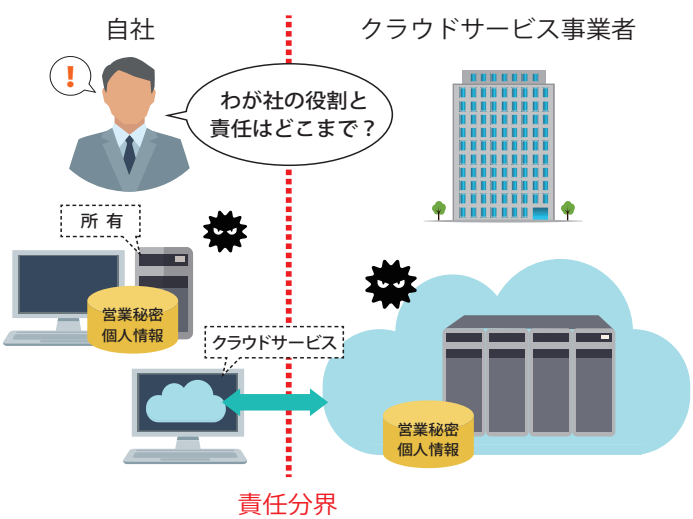
③クラウドサービスのセキュリティ対策

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、**「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）**のクラウドサービス安全利用チェックシートの 15 項目を参照して、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。



(6)テレワークの情報セキュリティ

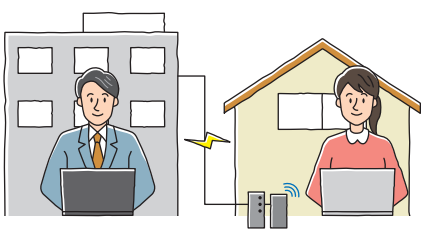
テレワークは、DX の推進や多様な人材の柔軟な働き方を実現するとともに非常時の業務継続にも有効です。しかし、企業の管理下にない環境で業務を行うことや個人所有の端末の業務利用は従来と異なるリスクも想定され、セキュリティ対策を見直す必要があります。ここではテレワークのセキュリティ対策について３つの段階に分けて検討事項を説明します。

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

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**：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、ウイルス対策ソフトの導入や、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、

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 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 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を利用するなどします。

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。

クラウドサービスを利用する場合は、**本編「より強固にするための方策（5）クラウドサービスの情報セキュリティ」、「クラウドサービス安全利用の手引き」（付録 7）**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
■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（IPA）
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/

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/IEC27017）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。

(7)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

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、**「中小企業のためのセキュリティインシデント対応の手引き」（付録 8）**や**「5分でできる！情報セキュリティ自社診断」（付録 3）**の対策例も参照してください。

参考情報
（ 相談窓口 ）
■企業組織向けサイバーセキュリティ相談窓口（IPA）
https://www.ipa.go.jp/security/support/soudan.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/

（ 告示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/
■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.html#nintei

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。

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 33 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 27001:2023（ISO/IEC 27001:2022）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]JIS Q 27002:2024（ISO/IEC 27002:2022）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 27017:2016(ISO/IEC 27017:2015)情報技術－セキュリティ技術－JISQ27002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

JISQ27002 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 27005:2023(ISO/IEC 27005:2022)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－情報セキュリティリスクの管理に関する手引

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 31000:2019(ISO/IEC 31000:2018)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

[11]サイバー攻撃による被害発生時のインシデント報告様式(NCO(国家サイバー統括室))

サイバー攻撃（特に件数の多い DDoS 攻撃事案及びランサムウェア事案）による被害発生時の、被害組織から関係政府機関への統一された報告様式です。

https://www.cyber.go.jp/policy/group/cyber/yoshikiichigenka.html

[12]サプライチェーン強化に向けたセキュリティ対策評価制度(SCS 評価制度)(経済産業省及び内閣官房国家サイバー統括室)

サプライチェーンにおける重要性を踏まえた上で満たすべき各企業の対策を提示しつつ、その対策状況を可視化する仕組みです。

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。

脆弱性

情報セキュリティの文脈では、脆弱性はシステムやソフトウェア、ネットワークに存在するセキュリティ上の弱点を指します。この弱点が悪意のある攻撃者に利用されると、データの漏洩、改ざん、破壊、不正アクセスなどのセキュリティインシデントが発生する可能性が生じます。

暗号化

情報やデータを特定のアルゴリズムを使用して変換し、第三者が容易に解読できない形式に変換するプロセスのことを指します。

ウイルス

コンピュータやネットワークに損害を与える目的で作成されたプログラムやコードの総称です。ユーザーの許可なくシステムに侵入し、不正な活動を行うことを目的としています。

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指します。

(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のことを指します。（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

中小企業が単独でセキュリティを強化するだけでなく、取引先や外部パートナーとの連携を意識した取り組みが求められる時代です。また、ランサムウェアをはじめとする脅威がさらに高度化する中、セキュリティインシデントへの事前準備と迅速な対応の重要性が高まっています。

中小企業には、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課題がありますが、一方で、経営者が迅速な意思決定を行い、従業員と密接に連携できるという強みがあります。この柔軟性を活かしながら、サプライチェーン全体を視野に入れたセキュリティ対策を講じることが、これからの事業環境での競争力を高める鍵となります。

本ガイドラインが、中小企業の皆様の直面するセキュリティ課題に対処する一助となり、さらなる成長を支える一冊となれば幸いです。

（第 4.0 版作成）

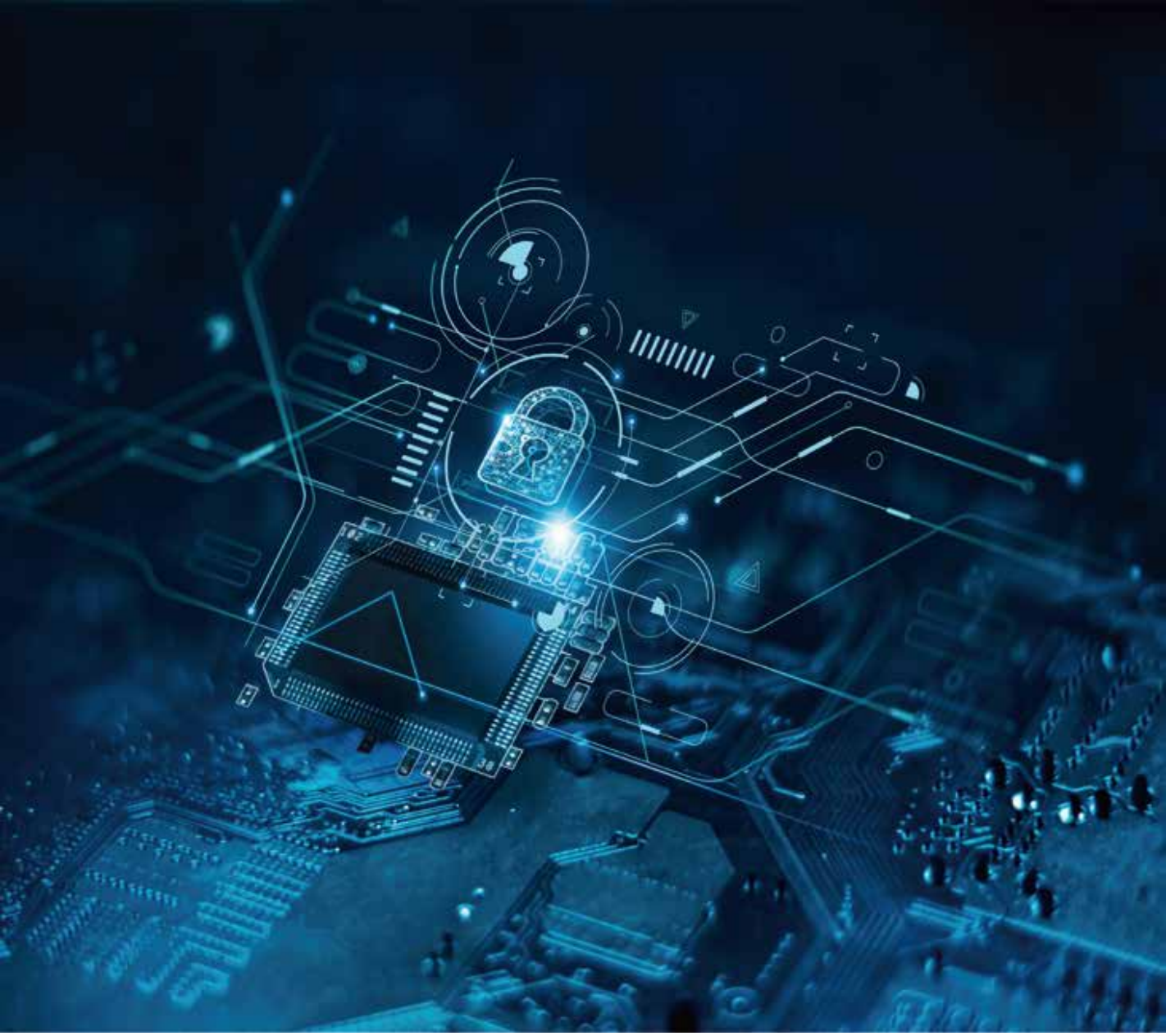
中小企業の情報セキュリティ対策ガイドライン改訂に関する検討会　委員

（五十音順、○は委員長）

原　伸一　日本商工会議所 情報化推進部 部長
福田 徹也　全国商工会連合会 組織支援部 経営情報戦略課 課長
藤岡 友樹　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
古川 英規　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 社会活動部会 中小企業支援施策ワーキング・グループ リーダー
松本 哲也　パナソニックホールディングス株式会社 サイバーセキュリティ統括室 エンタープライズセキュリティ戦略部(兼) 技術部門 テクノロジー本部 製品セキュリティセンター、サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3) 業界連携ワーキング・グループ 座長
○満塩 尚史　順天堂大学 健康データサイエンス学部 准教授
持田 啓司　株式会社ラック サイバー・グリッド・ジャパン シニアコンサルタント、情報セキュリティ教育事業者連絡会（ISEPA）代表
山岡 裕明　八雲法律事務所 弁護士

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 3 月 26 日）● 4.0 版（2026 年 3 月 27 日）



中小企業の情報セキュリティ対策ガイドライン　第 4.0 版

2026 年 3 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 03-5978-7530　FAX 03-5978-7513
E-mail isec-pr-cssp@ipa.go.jp