令和5年度
中小企業サイバーセキュリティ対策
継続支援事業

組織的対策と人的対策
【実施手順・実施者マニュアルレベル②】

サイバーセキュリティ
人材育成
社内体制整備支援

目次

第14章. 組織的管理策

14-1. 組織的管理策を参考とした対策基準・実施手順の策定

章の目的
第14章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標
◘ 組織的管理策をもとに、対策基準を策定する手順を理解すること。 ◘ 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。

14-1-1. 対策基準の策定

対策基準を策定する際は、ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考にすることができます。
組織が対策基準を策定する際は、組織の業態や規模によって重視するべき管理策は異なり、適用の必要性がない管理策も存在します。一方で、ISO/IEC 27001:2022の附属書AやISO/IEC 27002:2022にない管理策が必要となるケースもあることをご留意ください。
自組織にとってのリスクを自ら考えて必要な管理策を選択するために、リスクアセスメントの手法を使用し、対策基準を策定します。

ISO/IEC 27001:2022附属書Aの管理策		
カテゴリ	**項目数（合計93）**	**概要**
組織的管理策	37	組織として取組む必要のある管理策。たとえば、情報セキュリティ方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。たとえば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理策。ネットワークのセキュリティ、データの暗号化、データのバックアップ、脆弱性管理、ログ管理、マルウェア対策などが含まれます。

対策基準策定時の注意点
ISMSの認証取得を目標にして情報セキュリティ対策を進めると、ドキュメントの整備が目的になり、本来の情報セキュリティ対策がなおざりになってしまい、ISMSが形骸化するケースが少なくありません。策定した管理策が継続的に実行されていくことが重要となります。

組織は、情報セキュリティリスクを適切にコントロールするために必要となる管理策を念入りに検討し、対策基準を策定することが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

14-1-1. 対策基準の策定

ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022に基づき管理策を決定する（例）　【凡例】採用：○・不採用：×

項目	採用、不採用	項目	採用、不採用
5.1 情報セキュリティのための方針群		5.20 供給者との合意におけるセキュリティの取扱い	
5.2 情報セキュリティの役割及び責任		5.21 ICTサプライチェーンにおける情報セキュリティの管理	
5.3 職務の分離		5.22 供給者のサービス提供の監視、レビュー及び変更管理	
5.4 経営陣の責任		5.23 クラウドサービス利用における情報セキュリティ	
5.5 関係当局との連絡		5.24 情報セキュリティインシデント管理の計画策定及び準備	
5.6 専門組織との連絡		5.25 情報セキュリティ事象の評価及び決定	
5.7 脅威インテリジェンス		5.26 情報セキュリティインシデントへの対応	
5.8 プロジェクトマネジメントにおける情報セキュリティ		5.27 情報セキュリティインシデントからの学習	
5.9 情報及びその他の関連資産の目録		5.28 証拠の収集	
5.10 情報及びその他の関連資産の利用の許容範囲		5.29 事業の中断・阻害時の情報セキュリティ	
5.11 資産の返却		5.30 事業継続のためのICTの備え	
5.12 情報の分類		5.31 法令、規制及び契約上の要求事項	
5.13 情報のラベル付け		5.32 知的財産権	
5.14 情報転送		5.33 記録の保護	
5.15 アクセス制御		5.34 プライバシー及びPIIの保護	
5.16 識別情報の管理		5.35 情報セキュリティの独立したレビュー	
5.17 認証情報		5.36 情報セキュリティのための方針群、規則及び標準の順守	
5.18 アクセス権		5.37 操作手順書	
5.19 供給者関係における情報セキュリティ			

14-1-1. 対策基準の策定

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。

対策基準（例）

5.1 情報セキュリティのための方針群
情報セキュリティ方針およびトピック固有の個別方針は、これを定義し、経営陣によって承認され、発行し、関連する要員および関連する利害関係者へ伝達し認識され、計画した間隔でおよび重要な変化が発生した場合にレビューしなければならない。

5.2 情報セキュリティの役割及び責任
情報セキュリティの役割および責任を、組織の要求に従って定め、割り当てなければならない。

5.3 職務の分離
相反する職務および責任範囲は、分離しなければならない。

5.4 経営陣の責任
経営陣は、組織の確立された情報セキュリティ方針、トピック固有の個別方針および手順に従った情報セキュリティの適用を、すべての要員に要求しなければならない。

5.5 関係当局との連絡
組織は、関係当局との連絡体制を確立および維持しなければならない。

5.6 専門組織との連絡
組織は、情報セキュリティに関する研究会または会議、および情報セキュリティの専門家による協会・団体との連絡体制を確立し維持しなければならない。

5.7 脅威インテリジェンス
情報セキュリティの脅威に関連する情報を収集および分析し、脅威インテリジェンスを構築しなければならない。

One Point

対策基準を策定する際のポイント
ISO/IEC 27001:2022附属書Aの中には、中小企業にとっては負担が大きい管理策があります。ISO/IEC 27001:2022附属書Aに適切な管理策がない場合は、独自の管理策を追加することができます。組織の状況を考慮し、適切な対策基準を策定することが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

14-1-1. 対策基準の策定

対策基準（例）

5.8 プロジェクトマネジメントにおける情報セキュリティ
情報セキュリティをプロジェクトマネジメントに組み入れなければならない。

5.9 情報及びその他の関連資産の目録
管理責任者を含む情報およびその他の関連資産の目録を作成し、維持しなければならない。

5.10 情報及びその他の関連資産の利用の許容範囲
情報およびその他の関連資産の利用並びに取扱い手順の許容範囲に関する規則は、明確にし、文書化し、実施しなければならない。

5.11 資産の返却
要員および必要に応じてその他の利害関係者は、雇用、契約または合意の変更または終了時に、自らが所持する組織の資産のすべてを返却しなければならない。

5.12 情報の分類
情報は、機密性、完全性、可用性および関連する利害関係者の要求事項に基づく組織の情報セキュリティの要求に従って分類しなければならない。

5.13 情報のラベル付け
情報のラベル付けに関する適切な一連の手順は、「5.12 情報の分類」で確立した分類体系に従って策定し、実施しなければならない。

5.14 情報転送
情報転送の規則、手順または合意を、組織内および組織と他の関係者との間のすべての種類の転送設備に関して備えなければならない。

5.15 アクセス制御
情報およびその他の関連資産への物理的および論理的アクセスを制御するための規則を、業務および情報セキュリティの要求事項に基づいて確立し、実施しなければならない。

5.16 識別情報の管理
組織の情報およびその他の関連資産にアクセスする個人およびシステムを一意に特定できるようにし、アクセス権を適切に割り当てなければならない。

5.17 認証情報
認証情報の割り当ておよび管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理しなければならない。

5.18 アクセス権
情報およびその他の関連資産へのアクセス権は、アクセス制御に関する組織のトピック固有の個別方針および規則に従って、提供、レビュー、変更および削除しなければならない。

14-1-1. 対策基準の策定

対策基準（例）

5.19 供給者関係における情報セキュリティ
供給者の製品またはサービスの使用に関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定義し実施しなければならない。

5.20 供給者との合意における情報セキュリティの取扱い
供給者関係の種類に応じて、各供給者と、関連する情報セキュリティ要求事項を確立し合意をとらなければならない。

5.21 ICTサプライチェーンにおける情報セキュリティの管理
ICT 製品およびサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定め、実施しなければならない。

5.22 供給者のサービス提供の監視、レビュー及び変更管理
サービスの供給者の情報セキュリティの実践およびサービス提供の変更を定常的に監視し、レビューし、評価し、管理しなければならない。

5.23 クラウドサービスの利用における情報セキュリティ
クラウドサービスの取得、利用、管理および終了のプロセスを、組織の情報セキュリティ要求事項に従って定めなければならない。

5.24 情報セキュリティインシデント管理の計画及び準備
セキュリティインシデント管理のプロセス、役割および責任を定義、確立および伝達し、セキュリティインシデント管理の計画を定めなければならない。

5.25 情報セキュリティ事象の評価及び決定
情報セキュリティ事象に対して、セキュリティインシデントに分類するか否かを決定するための評価を実施しなければならない。

5.26 情報セキュリティインシデントへの対応
セキュリティインシデントに対し、文書化した手順に従って対応しなければならない。

5.27 情報セキュリティインシデントからの学習
セキュリティインシデントから得られた知識を、情報セキュリティ管理策を強化し、改善するために用いなければならない。

5.28 証拠の収集
情報セキュリティ事象に関連する証拠の特定、収集、取得および保存のための手順を定め、実施しなければならない。

14-1-1. 対策基準の策定

対策基準（例）

5.29 事業の中断・阻害時の情報セキュリティ
事業の中断・阻害時に情報セキュリティを適切なレベルに維持するための方法を定めなければならない。

5.30 事業継続のためのICTの備え
事業継続の目的およびICT 継続の要求事項に基づいて、ICT の備えを計画、実施、維持および試験しなければならない。

5.31 法令・規制及び契約上の要求事項
情報セキュリティに関する法令や契約事項を特定・文書化し、遵守しなければならない。

5.32 知的財産権
知的財産権を保護するための適切な手順を実施しなければならない。

5.33 記録の保護
記録を、消失、破壊、改ざん、認可されていないアクセスおよび不正な流出から保護しなければならない。

5.34 プライバシー及びPIIの保護
適用される法令、規制および契約上の要求事項に従って、プライバシーの維持およびPIIの保護に関する要求事項を特定し、満たさなければならない。

5.35 情報セキュリティの独立したレビュー
情報セキュリティおよびその実施の管理に対する組織の取組みについて、あらかじめ定めた間隔で、または重大な変化が生じた場合に、独立したレビューを実施しなければならない。

5.36 情報セキュリティのための方針群、規則及び標準の順守
組織の情報セキュリティ方針、トピック固有の個別方針、規則および標準を遵守していることを定期的にレビューしなければならない。

5.37 操作手順書
情報処理設備の操作手順を文書化し、必要な要員に対して利用可能な状態としなければならない。

次ページ以降では、策定した対策基準をもとに作成する実施手順について説明します。

14-1-2. 実施手順の策定

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介します。実施手順は、組織の内部文書として作成します。実施手順が抽象的で理解しづらい場合、従業員は具体的に何を遵守して行動すればよいかわからず、セキュリティ対策が不十分になってしまいます。従業員に対してわかりやすい実施手順を策定するよう心掛けることが大切です。

実施手順を策定する際は、ISO/IEC 27002に記載されている各管理策の手引が参考になります。手引の内容をもとに、実施手順の例を紹介します。この例と、ISO/IEC 27002の内容を参考に、自社に適した実施手順を策定してください。

5.1 情報セキュリティのための方針群

実施手順（例）

情報セキュリティ委員会は、「情報セキュリティ方針」などの情報セキュリティに関する方針を定義し、トップマネジメント（経営層）の承認を得る。また、情報セキュリティ委員会は、情報セキュリティに関する方針を適用範囲内の全従業者に公表する。また、「情報セキュリティ方針」は外部関係者にも公表する。

情報セキュリティ委員会は、「情報セキュリティ方針」以外の情報セキュリティのための方針群を、本手順において定める。方針群には以下を含める。

a. モバイル機器の方針
b. テレワーキング
c. アクセス制御方針
d. 暗号による管理策の利用方針
e. クリアデスク・クリアスクリーン
f. 情報転送の方針（および手順）
g. セキュリティに配慮した開発のための方針
h. 供給者関係のための情報セキュリティの方針

ワンポイントアドバイス

情報セキュリティに関する方針は、関連する従業員および利害関係者に認識されることが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

14-1-2. 実施手順の策定

5.2 情報セキュリティの役割及び責任

実施手順（例）

トップマネジメント（経営層）は、情報セキュリティに関連する役割を持つ情報セキュリティ委員会、内部監査責任者に対して、以下の責任および権限を割り当てる。また、トップマネジメント（経営層）は、これらの役割、責任および権限を従業者に伝達する。情報セキュリティの運用に際し、トップマネジメント（経営層）は、情報セキュリティ委員会の設置および運営を実施する。

情報セキュリティ委員会の役割は以下の通り。
a. リスク対応計画の策定
b. 情報セキュリティ実行体制の構築
c. 選択された管理策の実施
d. 教育・訓練
e. 運用の管理
f. 経営資源の管理
g. 情報セキュリティ事象・セキュリティインシデントの管理
h. 関連当局との連絡（警察・審査機関・コンサル会社・取引先・委託先など）

情報セキュリティ委員会の責任および権限は以下の通り。

役割	責任および権限
情報セキュリティ委員会責任者	管理策の実施・運用について統括する。 管理策の成果をトップマネジメント（経営層）に報告する。
教育責任者	管理策に関する教育計画の立案と実施を行う。
部門管理者（運用委員）	情報セキュリティの部門代表者として、部門を管理する。
情報システム管理者	情報システム部門の管理者で、情報システム管理に関する規定・規則に従い、情報セキュリティを維持するための安全管理対策を実施する。
文書管理責任者	管理策に関する文書や記録などの維持・管理を行う。

内部監査責任者の責任および権限は以下の通り。
内部監査責任者は、管理策とその実施状況に関わる監査を統括する責任と権限を有する。

ワンポイントアドバイス
従業員が少ない場合は、文書管理責任者と教育責任者を同じ者にするなど、役割を兼任させて体制を構築することも有効です。

14-1-2. 実施手順の策定

5.3 職務の分離

実施手順（例）

a. 当組織は、申請者または作業者と、承認者を分離するように組織設計する。
b. 従業員の制約により兼任せざるを得ない場合、別部門などによる監視を行うことを条件に、兼任できる。

ワンポイントアドバイス
小さな組織で、職務の分離が困難である場合には、他の管理策（例：活動の監視、監査証跡、管理層による監督）を考慮することが大切です。

5.4 経営陣の責任

実施手順（例）

トップマネジメント（経営層）はすべての従業者に対し、情報セキュリティ方針、各実施手順、並びにその他情報セキュリティに関する要求事項の遵守を求める。

ワンポイントアドバイス
情報セキュリティ方針、各実施手順、その他情報セキュリティに関する要求事項が、すべての従業員に認識されることが大切です。

5.5 関係当局との連絡

実施手順（例）

情報セキュリティ委員会は、関係当局およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。

関係当局	連絡手段	URL	主目的
【IPA】コンピュータウイルス届出窓口、コンピュータ不正アクセス届出窓口	ウイルス発見・感染の届出 virus@ipa.go.jp 不正アクセスの届出 crack@pa.go.jp	https://www.ipa.go.jp/security/todokede/crack-virus/about.html	ウイルス感染や、不正アクセスによる被害を報告するため。
【IPA】情報セキュリティ安心相談窓口	TEL:03-5978-7509（受付時間10:00～12:00、13:30～17:00 土日祝日・年末年始は除く） anshin@ipa.go.jp	https://www.ipa.go.jp/security/anshin/about.html	ウイルス感染や不正アクセスに関する技術的な内容の相談に対して、アドバイスをもらうため。
【警視庁】サイバー犯罪相談窓口	TEL:03-5805-1731 受付時間：午前8時30分から午後5時15分まで（平日のみ）	https://www.keishicho.metro.tokyo.lg.jp/sodan/madoguchi/sogo.html	サイバー犯罪被害について相談するため。
【個人情報保護委員会】個人情報・マイナンバーの漏えい報告	Webフォームで報告	https://www.ppc.go.jp/personalinfo/legal/leakAction/	個人情報、マイナンバーの漏えいに対処するため。
【JPCERT/CC】インシデント対応依頼	Webフォームまたは、以下のメールアドレスに報告 info@jpcert.or.jp	https://www.jpcert.or.jp/form/	セキュリティインシデント対応を支援してもらうため。

ワンポイントアドバイス
セキュリティインシデントを時機を失せずに報告するために、関係当局の連絡方法を明確にすることが大切です。

14-1-2. 実施手順の策定

5.6 専門組織との連絡

実施手順（例）

情報セキュリティ委員会は、専門組織およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。

専門組織	情報の入手方法	URL	主目的
【IPA】重要なセキュリティ情報	Webページを閲覧	https://www.ipa.go.jp/security/security-alert/2023/index.html	危険性が高いセキュリティ上の問題と対策に関する最新情報を収集するため。
【IPA】ランサムウェア対策特設ページ	Webページを閲覧	https://www.ipa.go.jp/security/anshin/measures/ransom_tokusetsu.html	ランサムウェア対策に関する最新情報を収集するため。
【個人情報保護委員会】注意情報一覧	Webページを閲覧	https://www.ppc.go.jp/news/careful_information/?category=39	セキュリティ・個人情報・マイナンバーに関する、注意事項を把握するため。
【JPCERT/CC】注意喚起	Webページを閲覧	https://www.jpcert.or.jp/at/2023.html	脆弱性に関する最新情報を収集するため。

ワンポイントアドバイス
脆弱性や攻撃など情報セキュリティに関する情報を適時入手するために、入手方法を明確にすることが大切です。

5.7 脅威インテリジェンス

実施手順（例）

1. 既存または新たな脅威に関する情報を、次に示す専門機関から収集する。
   ・IPA
   ・JVN（Japan Vulnerability Notes）
   ・JPCERT/CC
   ・ISAC (Information Sharing and Analysis Center)
   ・個人情報保護委員会
   収集する情報は、以下のようなものとする。
   ・変化する脅威の状況に関する情報（例：攻撃者や攻撃の種類）
   ・攻撃の方法、使用されるツールや技術に関する情報
   ・特定の攻撃に関する詳細な情報
2. 収集した情報を分析する。
   脅威が、自組織にどのような影響を及ぼすか把握するために、収集した情報をもとにリスクアセスメントを実施する。
3. リスク低減の処置を実施する。
   リスクアセスメントの結果をもとに、ファイアウォール・侵入検知システム・マルウェア対策ソリューションなど、技術的に予防、検知を行うための管理策を採用する。

ワンポイントアドバイス
情報の収集から、リスク低減処置を実施するまでの手順を明確にすることが大切です。

14-1-2. 実施手順の策定

5.8 プロジェクトマネジメントにおける情報セキュリティ

実施手順（例）
a. プロジェクト管理者は、プロジェクトにおける必要な管理策を特定する。 b. プロジェクトにおける必要な管理策は、プロジェクト終了後も考慮する。 c. プロジェクト管理者は、情報セキュリティ責任者を任命する。 d. 情報システム管理者は、業務用情報システムの導入・改善にあたっては、必要に応じて情報セキュリティ上の要求事項を、要件定義書や提案依頼書などにより文書化する。 文書には下記から必要な事項を含める。 ・情報システムの設置場所（環境・障害からの対策を含む）に関する事項 ・無停電電源装置などのサポートユーティリティに関する事項 ・保守契約に関する事項 ・システムの冗長化に関する事項 ・通信、データの安全対策に関する事項 ・受け入れテストに関する事項 ・アクセス権限に関する事項
ワンポイントアドバイス プロジェクトが提供する製品またはサービスの情報セキュリティ要求事項は、情報セキュリティ方針、トピック固有の個別方針および規制から遵守すべき要求事項を決定することが大切です。

5.9 情報及びその他の関連資産の目録

実施手順（例）
a. 情報セキュリティ委員会は「資産目録」を作成し、当組織における重要な資産を識別する。また「資産目録」を「年間計画表」に従い、最低年1回見直す。 b. 情報セキュリティ委員会は「資産目録」において特定した資産に対し、同目録上に管理責任者（リスク所有者）を記載することで管理責任を明確にする。
ワンポイントアドバイス 資産の管理責任を個人またはグループに割り当て、管理責任を明確にすることが大切です。

14-1-2. 実施手順の策定

5.10 情報及びその他の関連資産の利用の許容範囲

実施手順（例）

情報の区分ごとの取扱いルールを以下に示す。
情報の区分は「5.12 情報の分類」で、ラベル表示については「5.13 情報のラベル付け」で定める。

【文書・メディアなどの場合】

管理区分	関係者外秘	社外秘	一般
ラベル表示	責任者に一任	責任者に一任	不要
利用者	関係する部署・プロジェクトに所属する従業者	当組織の従業者	誰でも可
再配布	関係する部署・プロジェクト内に限る	社内に限る	特別な配慮不要
保管場所	施錠された場所	責任者に一任	
コピーの使用	必要のある者に限定	社内に限る	
FAX送信	関係する部署・プロジェクト内に限る	社内に限る	
裏紙使用※1	禁止	禁止	
社外便	透かして内容が見えないようにする。※2		
社外での携行	責任者の許可を得た者のみ携行を許可する。※3		
廃棄（文書）※4	シュレッダー・焼却・溶解のいずれか	責任者に一任	
廃棄処（媒体）	廃棄、再利用前の内容を消去する。		

※1 個人情報の記された書類の再利用は禁じる。
※2 紙や記憶媒体による個人情報を、郵便や宅配便などにより移送するときは、誤配、紛失などの危険を最小限にするため、ポストへの施錠、受け取り確認が可能な移送手段の選択などの措置を講じる。
※3 個人情報を外部へ持ち出す際は、目的地以外へ立ち寄らず、手放さない、車中に放置しないよう徹底する。
※4 紙に記された個人情報の廃棄は、シュレッダーによる裁断・焼却・溶解いずれかの方法で処分する。また、廃棄前の一時保管場所からの紛失・盗難防止のため、重要書類は即廃棄する。

【システム内情報】

管理区分	関係者外秘	社外秘	一般
アクセス制御	個人またはグループでのアクセス制御	責任者に一任	特別な配慮不要
個人PCへの保管	責任者に一任	責任者に一任	
サーバへの保管	アクセス制限	責任者に一任	
コピー(複製)※1	コピーの管理	責任者に一任	
メール	添付ファイルにパスワード※2		

※1　コピーは、バックアップの必要上および業務上やむを得ない場合の必要最小限の範囲にとどめるものとする。
※2　取引先との合意がある場合は、その合意に従う。

ワンポイントアドバイス
許容できる行動、許容できない行動を明確に定めることが大切です。

14-1-2. 実施手順の策定

5.11 資産の返却

実施手順（例）

情報セキュリティ委員会は、退職者が発生した際に、以下の対応を部門長に要求し、実施されたことを確認する。
a. 名刺、社員証、IDカードなどの返却
b. 会社が支給したノートPCや携帯電話などの返却
c. 紙で保管する書類の返却、または廃棄

ワンポイントアドバイス
返却するすべての情報およびその他の関連資産を明確に特定し、文書化することが大切です。

5.12 情報の分類

実施手順（例）

情報は一般・社外秘・関係者外秘で分類する。
情報セキュリティ委員会は、情報の分類を最低年1回見直す。

分類	内容
一般	下記以外
社外秘	関係者外秘以外の機密事項であり、当組織の従業者に対してのみ開示が許されるもの。（取引先に開示する必要があるものは除く。）または情報セキュリティに関わる規定・手順書類。
関係者外秘	情報が外に漏れることによって、当組織が重大な損失もしくは不利益を受けるような恐れのある機密事項であり、職務上の限られた関係者のみに開示を許すもの。関係者が明示的に定められていない場合、関係者とは、情報を直接配布された者を指す。

ワンポイントアドバイス
分類は、情報の侵害が組織に与える影響のレベルによって決定できます。分類体系で定義されたレベルには、分類体系の適用において意味をなすような名称を付けることが大切です。

5.13 情報のラベル付け

実施手順（例）

従業員は、取扱う情報が一般・社外秘・関係者外秘の区分のうち、どれに該当するか認識できる必要がある。
書類の分類を容易に認識できない場合は、以下のいずれかの方法により適切なラベル付けを行う。

a. 分類をシールなどの色により識別する。
b. ファイルなどに分類を記入（またはスタンプ）することで識別する。
c. 分類ごとに収納場所を分ける。

ワンポイントアドバイス
ラベル付けは、「5.12 情報の分類」で確立した分類体系を反映していることが大切です。

14-1-2. 実施手順の策定

5.14 情報転送

実施手順（例）

a. 重要な情報を外部に送信する場合は、セキュアなファイル共有サービスを利用する。やむを得ずファイル共有サービスが利用できない場合は、受信者と合意したうえで、メールに添付して送信する。
b. 重要な情報を外部にFAXにて送信する場合は、入力した番号と、名刺や送り状を照合し、間違えがないことを確認してからスタートボタンを押す。また頻繁に送信する送り先は短縮ダイヤルに登録する。
c. 認可されていない者に聞かれる可能性がある場所で、重要な情報を口頭で伝えることは禁じる。
d. 重要な情報を外部に郵送する場合は、配達記録郵便や宅配便など配達記録が残る手段をとる。
e. 重要な情報を格納した媒体は、手渡しを原則とし、やむを得ず郵送する場合は、十分な梱包により媒体を保護する。
f. 個人情報の授受記録
  ・紙や記憶媒体による個人情報の受け渡しに際しては、送付票や受領証などで受け渡しの完了を確認する。
  ・電子メールにより個人情報の受け渡しを行う際には、送信済みメールおよび、受領確認の返信メールのいずれかまたは両方を受け渡し記録とする。
g. 電子メールの利用
  ・電子メールは会社所定のソフトを使用し、その利用は業務上必要な場合に限定する。
  ・社外メーリングリストへの参加は、原則禁止とする。
  ・重要な情報（社外秘以上）はメール本文に記載して送信せず、aに従う。
h. 情報転送に関する合意
  ・情報の転送先との間で、情報転送の手段について、あらかじめ合意を得る。
  ・重要な情報を外部にメール添付またはFAXにて送信する場合は、必要に応じて送信予告、到着確認の電話を掛ける。
  ・宅配便業者を利用する場合は、会社が指定する業者を利用する。
i. 電子的メッセージ通信
  ・当組織のWebサイトに入力する情報の通信は、SSL/TLSにより行う。
  ・電子データによる個人情報をインターネット経由で送受信する際は、SSL/TLSなどの暗号化対策やパスワード設定などの措置を講じる。

ワンポイントアドバイス
情報転送は、電子的な転送、物理的記憶媒体での送付および口頭での伝達によって行われる場合があります。情報転送の規則、手順を定めることが大切です。

14-1-2. 実施手順の策定

5.15 アクセス制御

実施手順（例）
a. 業務に必要な者のみが情報にアクセスできるようにし、アクセス権限および操作権限は、認められた場合以外は与えないようにする。 b. 社内LANは、情報システム管理者の承認を得た従業員、装置に限り接続する。 c. 社内の情報システムへの外部からのアクセスは、ファイアウォールなどによって通信を制限する。 d. 外部から社内のサーバに接続する場合、VPN接続を使用する。 e. 無線LANは物理的・論理的な認証、通信の暗号化などを施したうえで利用する。 f. サーバ室へ入退を行う対象者に対して、入退資格を設け、資格のない者の立ち入りを禁じる。 g. サーバ室は、常時施錠可能とし、入退資格のない者の立ち入りを禁じる。
ワンポイントアドバイス アクセス制御規則を定めるには、「明確に許可していないことは、原則的に禁止する」という最も特権の小さい前提に基づいた規則を設定するようにすることが大切です。

5.16 識別情報の管理

実施手順（例）
a. 情報システムの利用者登録および登録削除は、当該利用者の属する部門長が申請し、情報システム管理者の承認を得る。 b. 利用者登録は業務上必要な範囲で従業者に付与する。
ワンポイントアドバイス 識別情報が不要になった場合、識別情報は時機を失せずに無効化または削除することが大切です。

14-1-2. 実施手順の策定

5.17 認証情報

実施手順（例）

a. 情報システム管理者は、利用者に仮パスワードを発行する場合、利用者本人のみが知ることができる方法で通知する必要がある。
b. 情報システム管理者は、利用者に対し、仮パスワードを直ちに変更することを要求し、通知する。
c. 秘密認証情報の利用
   ・利用者は、英数字と記号を混在した10文字以上のパスワードを設定し、アルファベットには大小文字の両方を含める必要がある。
   ・他人に容易に推測されるようなわかりやすいパスワードの使用を禁じる。
   ・他のサービスと重複するパスワードの利用を禁じる。
   ・各システムにおける管理者IDのパスワードは、情報システム管理者において厳重に管理する必要がある。
   ・利用者および情報システム管理者は、パスワードの代替もしくは補完のために、指紋などの生体認証、専用のアプリやメールなどを利用するワンタイムパスワードによる認証、PINコード・機器認証などを利用するパスキーによる認証方式を採用する。
d. パスワード管理システム
   ・パスワードの入力は対話式とする。
   ・パスワード入力時に画面に表示させないようにする。

ワンポイントアドバイス
パスワードを認証情報として使用する場合、IPAなどが推奨している強力なパスワードの作り方を参考にすることが大切です。

5.18 アクセス権

実施手順（例）

a. 利用者のアクセス権は、重要情報に対しては必要最小限の者がアクセスするという原則のもとに、情報システム管理者が検討し、設定を行う。
b. 情報システム管理者は、定期的（最低年1回）および必要時にアクセス権限の棚卸および見直しを行う。
c. 退職者が発生した際は、業務に支障がないよう調整し、速やかに該当アカウントを削除する必要がある。申請は、当該従業員が最後に所属した部門の長がアクセス権限の削除を申請し、情報システム管理者、またはその指名する従業員が削除する。
d. 他部署への移動が生じた際は、aの手順に従い削除する。また、新規のアクセス権限は移動先部門の長が申請し、同様の手順に従い登録する。

ワンポイントアドバイス
物理的および論理的なアクセス権の定期的レビューでは、同じ組織内での異動、昇進、降格、退職後の利用者のアクセス権、および特権的アクセス権の認可について考慮することが大切です。

14-1-2. 実施手順の策定

5.19 供給者関係における情報セキュリティ

実施手順（例）

a. 当組織における供給者には、以下がある。
- ISP、電話サービス、IT機器などのサービス提供者
- 情報システムの開発・保守における外部委託先
- 会計、税務、法律などの専門サービス提供者
- 清掃業者、廃棄業者
- クラウドサービス

b. 情報セキュリティ委員会は、部外者・外部組織によるオフィスエリアや情報システムへのアクセスを許可する際に生じる可能性があるリスクを考慮し、情報セキュリティ上の要求事項を明確にする。

ワンポイントアドバイス
供給者が提供する製品およびサービスの使用に関連するセキュリティリスクに対処するためのプロセスおよび手順を特定し、実施することが大切です。

5.20 供給者との合意における情報セキュリティの取扱い

実施手順（例）

a. 提供されるサービスの利用は、次の手順に従い行う。
1. 「委託先審査票」による評価・選定を行う。
2. 情報セキュリティ要求事項を考慮し、次の事項を含む契約を締結する。
- 機密保持契約などの情報の取扱いに関する契約
- 使用許諾に関する取り決め、コードの所有権および知的所有権（開発の場合）
- 実施される作業場所および入退室管理
- 外部委託先が不履行となった場合の預託契約に関する取り決め

3. 情報セキュリティ委員会は、「5.19 供給者関係における情報セキュリティ」において検討したリスクを考慮し、必要に応じて第三者との間で契約を締結する。

b. クラウドサービスを介して重要資産を取扱う際は、利用者は多要素認証を有効にしてセキュリティを強化する必要がある。

ワンポイントアドバイス
組織と供給者の間で情報セキュリティ要求事項を満たす義務に関し、当事者間で合意を確立し、文書化することが大切です。

14-1-2. 実施手順の策定

5.21 ICTサプライチェーンにおける情報セキュリティの管理

実施手順（例）
a. ICT製品・サービスの供給者との契約には、必要に応じて再委託に関する事項を盛り込む。 b. クラウドサービスの利用にあたっては、クラウドサービス提供者の事業継続性、および以下のサービスに関する情報セキュリティ事項を考慮のうえ、クラウドサービスを選定する。 ・サービスの導入実績、信頼性 ・利用者サポート機能 ・利用終了後のデータの扱い ・サービスの可用性 ・暗号化など、通信経路の安全対策
ワンポイントアドバイス 信頼できる供給源からICTを取得する手順を明確にすることが大切です。

5.22 供給者のサービス提供の監視、レビュー及び変更管理

実施手順（例）
a. 情報セキュリティ委員会は、サービスの供給者に対して、あらかじめ定められた頻度（最低年1回）において契約の履行状況ならびに「委託先審査票」による遵守状況の確認を行う。 b. サービスの供給者との間で契約内容やサービスレベルに変更があった場合、変更点を受け入れることができるか否かを検証し、契約内容の見直しを実施する。
ワンポイントアドバイス サービスの提供において不完全な点があった場合は、適切な処置をとることが大切です。

14-1-2. 実施手順の策定

5.23 クラウドサービスの利用における情報セキュリティ

実施手順（例）

クラウドサービスを導入する際、以下の評価表をもとにクラウドサービスを評価し、自社のセキュリティ要件事項を満たしているか確認する。

クラウドサービス提供者名	サービス内容

取得している認証
□ ISO/IEC 27001 □ ISO/IEC 27017

セキュリティ対策内容	評価
クラウドサービスに対して、マルウェア対策を行っているか。	
クラウドサービスのバックアップを行っているか。	
サービス解約時のデータの取扱い方法が明確になっているか。	
サービス稼働率、障害発生頻度、障害発生時の復旧時間など、サービス品質は問題ないか。	
データがどの国や地域に配置されたサーバに保存されているか確認したか。	
サービスの利用方法について問い合わせることができるか。	
クラウドサービス提供者の責任範囲を確認したか。	
クラウドサービスのセキュリティインシデント発生時に通知がくるかどうか確認したか。	

（評価）○：できている　△：部分的にできている　×：できていない

ワンポイントアドバイス

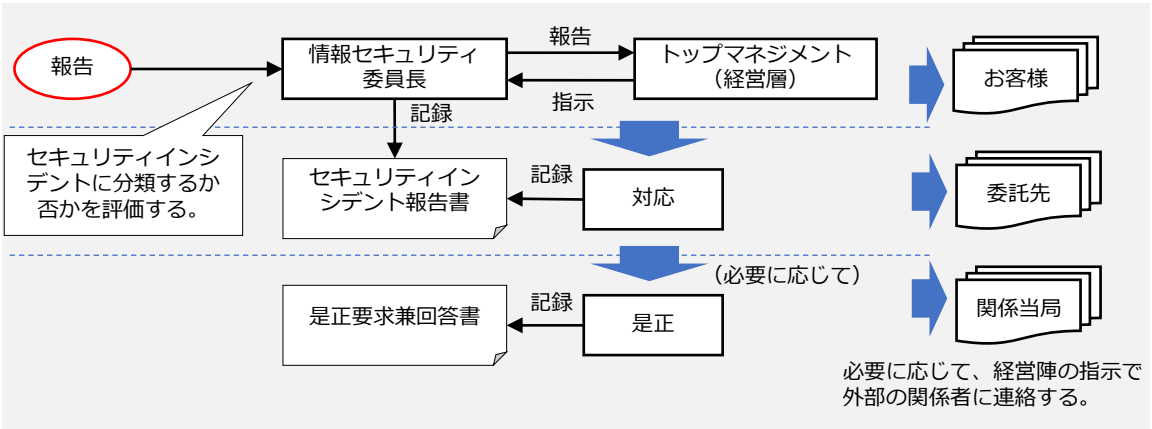
クラウドサービスの利用は、クラウドサービス提供者とクラウドサービス利用組織との間の情報セキュリティに関する責任の共有および分担、共同作業を伴う可能性があります。クラウドサービス提供者と、クラウドサービス利用組織の両方の責任を適切に定義し、実践することが大切です。

14-1-2. 実施手順の策定

5.24 情報セキュリティインシデント管理の計画策定及び準備

実施手順（例）

セキュリティインシデントへの対応は、以下の手順で行う。
管理層の責任のもと、以下の手順を関係者に伝達する。



ワンポイントアドバイス
セキュリティインシデントへの対応を実行するために役割および責任を決定し、関連する関係者に効果的に伝達することが大切です。

5.25 情報セキュリティ事象の評価及び決定

実施手順（例）

a. セキュリティの弱点、脅威に気付いた場合もしくは疑いを持った場合は、情報セキュリティ委員会に報告する。この際、自己で解決することよりも報告を優先させる。
b. 情報セキュリティ事象の評価は、以下の表に従い、部門管理者（情報セキュリティ委員会メンバー）が行う。
・大、中の項目に該当する情報セキュリティ事象は、セキュリティインシデントとして分類する。
・項目の大、中、小の順に優先順位を付ける。

項目	小	中	大
分類	ヒヤリハット・事象	インシデント	インシデント
最終的に被害が及ぶ範囲	現状、事件・事故の発生には及ばない。（将来、被害が発生する可能性がある。）	社員または社内	顧客・取引先
連絡先	情報セキュリティ委員長	情報セキュリティ委員長	情報セキュリティ委員長 トップマネジメント（経営層） 外部関係者

ワンポイントアドバイス
情報セキュリティ事象をセキュリティインシデントに分類する基準を明確に定めることが大切です。

14-1-2. 実施手順の策定

5.26 情報セキュリティインシデントへの対応

実施手順（例）

セキュリティインシデントへの対応手順は以下の表に従う。

影響度	小	中・大
ウイルス感染時	• 感染したPCを、組織内のネットワークから切り離す。 • 発生する可能性がある被害をシステム担当者に報告する。	• 感染したPCを、組織内のネットワークから切り離す。 • 発見した事実をできるだけ速やかに情報システム管理者に連絡する。
不正アクセス発生時	• ネットワークを遮断する。 • 重要なデータを隔離する。 • ログインできる場合は、早急にパスワードを変更する。 • 発生する可能性がある被害をシステム担当者に報告する。	• ネットワークを遮断する。 • 重要なデータを隔離する。 • ログインできる場合は、早急にパスワードを変更する。 • システムやアプリケーションを停止する。 • 発見した事実をできるだけ速やかに情報システム管理者に連絡する。
情報破壊発生時	発見次第、発生する可能性がある被害を部門長に報告する。	発見した事実をできるだけ速やかに部門長に連絡する。
情報改ざん発生時	同上	同上
情報漏えい発生時	同上	同上
サービス停止時・機器故障など	同上	同上

ワンポイントアドバイス
セキュリティインシデント対応に関する手順を確立し、すべての関連する利害関係者に伝達することが大切です。

14-1-2. 実施手順の策定

5.27 情報セキュリティインシデントからの学習

実施手順（例）
a. 情報セキュリティ委員会は、セキュリティインシデントを管理・分析し、問題があれば、計画を立ててトップマネジメント（経営層）へ提議する。計画には、解決に向けての処置方法・費用・実施予定日・責任者を明確にする。 b. 将来のセキュリティインシデントの起こりやすさや影響を減らすため、情報セキュリティ委員会は、セキュリティインシデントから得られた知識を活かして「6.3 情報セキュリティの意識向上、教育及び訓練」を強化・改善する。
ワンポイントアドバイス セキュリティインシデントの形態、規模および費用を定量化および監視するための手順を確立することが大切です。

5.28 証拠の収集

実施手順（例）
情報セキュリティ委員会は、情報システムの事故が特定の個人、または組織に起因するもので、事後処置が法的処置に及ぶ可能性のある場合には、必要な証拠の収集、保全に努める。
ワンポイントアドバイス 懲戒処置および法的処置のために情報セキュリティ事象に関連する証拠を取扱う場合は、内部の手順を定めて従うことが大切です。

14-1-2. 実施手順の策定

5.29 事業の中断・阻害時の情報セキュリティ

実施手順（例）

a. 資産のリスク分析
「資産目録（情報資産管理台帳）」で特定した情報資産のうち、可用性の評価値が3の重要資産を情報セキュリティ継続のリスク分析対象とする。
※可用性の評価値は、「11-2-2. リスク特定」で記載している方法で算出する。

b. aにおいて登録した資産に対して、以下のリスクについて考慮する。
・地震・火災・洪水などの自然災害
・人的なミス
・システム障害
・健康上の問題

c. bのリスクが生じた際に影響を受ける業務プロセスを特定し、リスクが発生した場合のシナリオを作成する。

d. リスクが生じた場合の影響度と、リスクが発生する可能性について検討し、検討結果に基づき優先順位を決定する。

e. dにおいて、優先順位が高いと判断したものに対して「事業継続計画書」を作成し、トップマネジメント（経営層）の承認を得る。
「事業継続計画書」には以下の内容を含む。
・実行開始条件（リスクシナリオの発生）
・非常時手順（発生時の連絡手順）
・回復手順（復旧のための手順）
・回復目標（目標時間を必要に応じて決定）
・再開手順（回復後のリハーサル手順）
・試験のスケジュール
・教育（教育が必要な場合はその計画）

f. 策定した計画および手続について試験を実施し、試験の結果、必要があると判断した場合は計画を更新する。試験は以下のいずれかの方法、またはその組み合わせにより行う。
・机上試験
・模擬試験
・技術的回復試験
・代替施設における回復試験
・供給者施設およびサービスの試験

g. 情報セキュリティ委員会は、事業継続に関する試験を最低年1回、継続的に実施する。

ワンポイントアドバイス
事業の中断または阻害時に、重要な事業プロセスの情報セキュリティを維持または復旧するために、計画を策定、実施、試験、レビューおよび評価することが大切です。

14-1-2. 実施手順の策定

5.30 事業継続のためのICTの備え

実施手順（例）
a. ビジネスインパクト分析（不測のインシデントによって業務やシステムが停止した場合、会社の事業にどのような影響があるかを分析すること）を行い、事業継続が困難な状況を特定する。 b. 事業が中断・停止になった際の対応手順を策定し、文書化する。 c. 策定した対応手順が有効であることを確実にするため、あらかじめ定めた間隔（年1回以上）で試験を実施し検証する。
ワンポイントアドバイス 組織がICTサービス事業の中断・阻害を管理する方法を詳述した対応および復旧手順を含むICT継続計画を、演習および試験を通じて定期的に評価、または経営陣が承認することが大切です。

14-1-2. 実施手順の策定

5.31 法令・規制及び契約上の要求事項

実施手順（例）

a. 情報セキュリティ委員会は、当組織が遵守すべき法令、規制、および契約上の要求事項を識別し、「情報セキュリティに関する法令規制一覧表」に記載する。「情報セキュリティに関する法令規制一覧表」は最低年1回見直す。
b. 情報セキュリティ委員会は、当組織の従業者が「情報セキュリティに関する法令規制一覧表」を、必要に応じていつでも参照できる状態にする。
c. 特定した要求事項を満たすために、必要に応じて教育などのテーマとする。
d. 暗号化した装置を輸出する場合、または海外に持ち出す場合、該当する法規制について調査を行い、必要であれば対応を行う。

情報セキュリティに関連する法律（例）	概要
特定電子メールの送信の適正化等に関する法律	利用者の同意を得ずに広告、宣伝または勧誘などを目的とした電子メールの送信を禁止している。
電子署名及び認証業務に関する法律	「本人による一定の条件を満たす電子署名」がなされた文書は、本人の手書署名・押印がある文書と同様、真正に成立したものと推定されることが定められている。
著作権法	プログラムやマニュアル、ホームページなどは、著作権の対象であり、無断での複製は、著作権法の侵害になる。
不正アクセス禁止法	不正アクセス行為や、不正アクセス行為につながる識別符号（ID、パスワード）の不正取得・保管行為、不正アクセス行為を助長する行為などを禁止している。
刑法	無断でデータを改ざん・破壊する行為や、虚偽の金融機関を名乗ったサイトや電子メールを使い、金銭をだまし取るような行為などは、刑法に違反する。

ワンポイントアドバイス
総務省のWebサイト「国民のためのサイバーセキュリティサイト　サイバーセキュリティ関連の法律・ガイドライン」で、サイバーセキュリティに関する代表的な法律が紹介されています。

詳細理解のため参考となる文献（参考文献）	
国民のためのサイバーセキュリティサイト　サイバーセキュリティ関連の法律・ガイドライン	https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_legal.html

14-1-2. 実施手順の策定

5.32 知的財産権

実施手順（例）
a. 知的財産権を保護するためのルールを策定し、組織内で教育・啓発活動を行う。 b. 知的財産権を侵害する行為を禁止する。 c. 知的財産権を侵害する行為が発生した場合には、速やかに是正措置を講じる。 d. ソフトウェアなどの使用許諾計画を遵守する。 e. 情報システム管理者は、パッケージソフトのライセンス管理を適切に行う。
ワンポイントアドバイス 知的財産権には、ソフトウェアまたは文書の著作権、意匠権、商標権、特許権およびソースコード使用許諾権が含まれます。

14-1-2. 実施手順の策定

5.33 記録の保護

実施手順（例）

当組織における記録は、関連する法令に基づき次表の保存期間にわたり、消失、破壊、改ざん、不正なアクセス、流失などがないように適切に保存する。

記録の種類	保存期間
■定款 ■登記関係書類 ■訴訟関係書類 ■特許など知的所有権に関する書類 ■社則・社規	永久
■「商業帳簿」 会計帳簿（日記帳、仕訳帳、総勘定元帳）、貸借対照表、損益計算書、附属明細書 ■「営業に関する重要な書類」 株主名簿、社債原簿、株主総会議事録、取締役会議事録、営業報告書、利益処分案 （損失処理案）、このほか紛争が生じた場合に重要な証拠となり得る書類（例：契約書）	10年
■仕訳帳、総勘定元帳、現金出納帳、固定資産台帳、売掛帳、買掛帳、経費帳 ■棚卸表、貸借対照表、損益計算書、決算に関して作成された書類 ■注文書、契約書、送り状、領収書、見積書、その他これらに準ずる書類（例：請求書）	7年
■給与所得者の扶養控除など（異動）申告書 ■給与所得者の保険料控除申告書兼給与所得者の配偶者特別控除申告書 ■源泉徴収簿	
■財産形成非課税貯蓄申込書・移動申請書	5年
■雇用保険被保険者に関する書類	4年
■労働者名簿 ■賃金台帳 ■雇入・解雇・災害補償・賃金その他労働関係に関する重要な書類	3年
■労働保険料の徴収に関する書類	
■労災保険に関する書類	
■安全委員会議事録 ■衛生委員会議事録 ■安全衛生委員会議事録	
■健康保険に関する書類	2年
■厚生年金保険に関する書類	
■雇用保険に関する書類	

ワンポイントアドバイス
記録は、記録の種類（会計記録、商取引記録、人事記録、法的記録など）によって分類し、それぞれに保存期間の詳細と、物理的または電子的な保存が可能な保存媒体の種類を記載することが大切です。

5.34 プライバシー及びPIIの保護

実施手順（例）

個人情報は、「5.10 情報およびその他の関連資産の利用の許容範囲」の取扱いルールに従い、厳重に取扱う。

ワンポイントアドバイス
プライバシーの保持およびPII保護のための手順を策定および実施することが大切です。

14-1-2. 実施手順の策定

5.35 情報セキュリティの独立したレビュー

実施手順（例）

a. 年に1度、内部監査により独立したレビューを行う。
b. 以下に例示する、情報セキュリティに影響のある変化が生じた場合も、内部監査により独立したレビューを行う。
・事業の追加/変更、業務手順の大幅な変更
・住所変更、拠点の新設
・情報セキュリティに関する主たる担当者の変更
・関係する法令・規制、または契約の大幅な変更

ワンポイントアドバイス
独立したレビューにおいて、情報セキュリティに関して取組みが不十分であると明確になった場合には、経営陣は是正処理を発議することが大切です。

5.36 情報セキュリティのための方針群、規則及び標準の順守

実施手順（例）

a. 情報セキュリティ委員会は、セキュリティに関する手順や実施標準が正しく実施されていることを確実にするため、「運用チェックリスト」にて、定期的（3ヶ月ごと）に点検を行う。
b. 情報セキュリティ委員会（入退管理責任者）は、入退記録が適切にとられているかどうかを月に1度確認する。また、入退管理が有効かつ適切に実施されていることを定期的に確認し、不備が発見された場合は速やかに是正の処置をとる必要がある。
c. 情報システム管理者は、技術的な遵守事項が正しく実施されていることを確実にするため、上記のa、bに従い点検する。

ワンポイントアドバイス
是正処置が完了しない場合は、確認時に進捗状況を報告することが大切です。

5.37 操作手順書

実施手順（例）

情報処理設備の正確、かつ、セキュリティを保った運用を確実にするために、次の事項を明記した手順書を文書化し、必要に応じて利用者が参照できるようにする。
a. システムが故障した場合の再起動および回復の手順
b. 記憶媒体の取扱い手順
c. バックアップの取得手順
d. 保守手順
e. 容量、能力、パフォーマンスおよびセキュリティなどの監視手順

ワンポイントアドバイス
操作手順書は必要に応じてレビューし、更新することが大切です。

第15章. 人的管理策

15-1. 人的管理策を参考とした対策基準・実施手順の策定

章の目的
第15章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標
◘ 人的管理策をもとに、対策基準を策定する手順を理解すること。 ◘ 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。

15-1-1. 対策基準の策定

ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022に基づき管理策を決定する（例）

【凡例】採用：〇・不採用：×

項目	採用、不採用	項目	採用、不採用
6.1 選考		6.5 雇用の終了又は変更後の責任	
6.2 雇用条件		6.6 秘密保持契約又は守秘義務契約	
6.3 情報セキュリティの意識向上、教育及び訓練		6.7 リモートワーク	
6.4 懲戒手続		6.8 情報セキュリティ事象の報告	

15-1-1. 対策基準の策定

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。

対策基準（例）

6.1 選考
従業員や契約相手を選定する際、個人情報の保護や雇用に関する法令を考慮して経歴などを確認しなければならない。

6.2 雇用条件
雇用契約書には、情報セキュリティに関する要員および組織の責任を記載しなければならない。

6.3 情報セキュリティの意識向上、教育及び訓練
従業員に対し、情報セキュリティに関する教育および訓練を実施しなければならない。

6.4 懲戒手続
情報セキュリティ方針に違反した場合の懲戒手続を、正式に定めなければならない。

6.5 雇用の終了又は変更後の責任
雇用の終了または変更の後も引き続き有効な情報セキュリティの責任や義務を、明確にしなければならない。

6.6 秘密保持契約又は守秘義務契約
組織の要求事項を反映した秘密保持契約または守秘義務契約を従業員や外部の関係者と締結しなければならない。

6.7 リモートワーク
要員が遠隔で作業する場合は、セキュリティ対策を実施しなければならない。

6.8 情報セキュリティ事象の報告
情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告できる仕組みを設けなければならない。

次ページ以降では、策定した対策基準をもとに作成する実施手順について説明します。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

15-1-2. 実施手順の策定

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介します。紹介する例と、ISO/IEC 27002に記載されている各管理策の手引の内容を参考に、自社に適した実施手順を策定してください。

6.1 選考

実施手順（例）
従業者の募集・採用プロセスは以下の点を考慮のうえ行う。 a. 取得した履歴書、スキルシートなどから業務上の要求事項への適合を判断し、選考を行う。 b. 採用時の面接などにおける態度や言葉遣いなどから倫理観を判断し、選考を行う。 c. 役員や管理職の採用に関しては、過去の信用情報など、より詳細な調査を行う場合があるが、この際は本人の同意を得たうえで行う。
ワンポイントアドバイス 選考プロセスはフルタイム、パートタイム、臨時スタッフを含むすべての従業員に対して実行することが大切です。

6.2 雇用条件

実施手順（例）
情報セキュリティに関する責任を理解し、情報セキュリティ方針を守ることを従業員に誓約させるため、雇用契約書に、情報セキュリティに関する事項を盛り込み、誓約書に署名を求める。
ワンポイントアドバイス 従業員に、情報セキュリティに関する雇用条件を同意させることが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

15-1-2. 実施手順の策定

6.3 情報セキュリティの意識向上、教育及び訓練

実施手順（例）

a. すべての従業者は、職務に関連する方針および手順についての適切な、意識向上のための教育および訓練を受ける必要がある。
b. 当組織では従業者が次の事項に関して認識を持てるよう教育・訓練を実施する。
・情報セキュリティ方針
・情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティに対する自らの貢献
・ISO/IEC 27001の要求事項に適合しないことの意味
c. 教育計画は情報セキュリティ委員会が作成し、トップマネジメント（経営層）が承認する。
d. 当組織の主な教育を以下に示す。（以下の教育は「教育実施記録」に残す。）
・新任部門管理者（運用委員）
新任の情報セキュリティ委員会メンバーに実施する。
・入社時・社内異動者の教育（適時）
新入社員、中間採用者に対して、入社時にセキュリティ教育を実施する。
・定期教育（「年間計画表」に基づく）
年に最低1回、適用範囲内の従業者に対して、情報セキュリティの理解、再確認と改善、向上のための教育を実施する。
・再教育
セキュリティ違反者および情報セキュリティに関する低理解度の従業者に対して、再教育を実施し、違反の再発防止に努める。
・実施した教育の有効性評価
上記の教育実施後理解度調査などを実施し、実施した教育の有効性の評価を行う。

ワンポイントアドバイス
知識が伝わったこと、並びに意識向上、教育および訓練プログラムの有効性を確認するため、意識向上、教育および訓練の活動終了時に、従業員理解の評価を行うことが大切です。

15-1-2. 実施手順の策定

6.4 懲戒手続

実施手順（例）
従業者が故意または過失により情報を漏えいした場合、または情報セキュリティ上の遵守事項に違反した場合は、罰則の対象とする。
ワンポイントアドバイス 懲戒手続は、関連する法令、規制、契約および事業上の要求事項、並びに必要に応じてその他の要素を考慮に入れることが大切です。

6.5 雇用の終了又は変更後の責任

実施手順（例）
情報セキュリティの観点から、雇用の終了または変更後も従業員が守るべき義務や責任（たとえば守秘義務）について定め、雇用時の誓約書に盛り込むと同時に、雇用の終了または変更時に再確認する。
ワンポイントアドバイス 雇用の終了または変更を管理する手続では、終了または変更後にどの情報セキュリティの責任および義務を引き続き有効とすることが望ましいかを定義することが大切です。

6.6 秘密保持契約又は守秘義務契約

実施手順（例）
a. 当組織の従業者は、当組織との間で機密情報に関する秘密保持の契約を締結する。なお、同契約には原契約の終了後も一定期間、秘密保持の義務が課せられる旨の条項を含める。 b. 当組織との委託先との間で、必要に応じて秘密保持の契約を締結する。 c. 情報セキュリティ委員会は、年に一度、情報セキュリティ要求事項に照らして、秘密保持の契約書の妥当性を検証する。
ワンポイントアドバイス 秘密保持契約または守秘義務契約に関する要求事項は、定期的または要求に影響する変化が発生した場合に、レビューすることが大切です。

15-1-2. 実施手順の策定

6.7 リモートワーク

実施手順（例）
a. リモートワークは、情報セキュリティ委員長の承認を得たものに限って行える。 b. リモートワークにて使用するPCは、会社から貸与したPCとし、家族などの同居人と共有することは禁じる。 c. リモートワークにて使用するPCは、アンチウイルスソフトを導入し、「8.7 マルウェアに対する保護」に準じた設定を行う。 d. リモートワークにて使用するPCに、ファイル交換ソフトなどの不正なソフトウェアをインストールすることは禁じる。 e. 社内ネットワークへはVPNにて接続する。
ワンポイントアドバイス リモートワークで個人所有のPCを使用する場合は、管理方法や接続方法について実施手順を記載することが大切です。

6.8 情報セキュリティ事象の報告

実施手順（例）
情報セキュリティ事象は、「5.25 情報セキュリティ事象の評価及び決定」に従って報告し、評価を行う。
ワンポイントアドバイス すべての社員が情報セキュリティ事象を報告する連絡先を認識し、報告の仕組みはできるだけ簡単で使いやすく、いつでも利用できるようにすることが大切です。

編集後記

セミナー8日目では、ISMSの管理策を参考に、対策基準・実施手順を策定する手順について解説しました。
本テキストで紹介する対策基準・実施手順の例は、そのまま組織に適用できるものではないため、紹介した例とISO/IEC 27002の内容を参考に、自社にあった対策基準・実施手順を策定していただければと思います。
ドキュメントの作成・更新は重要ですが、本来の目標は、ドキュメント作成ではなく、効果的な情報セキュリティ対策の計画と実行にあることを忘れないようにしてください。

本テキストでは、最初に「組織的管理策」を参考に対策基準を策定する手順について説明し、組織的管理策それぞれに対応する実施手順の例を説明しました。その後、「人的管理策」についても同様に説明を行いました。
次回は、「物理的管理策」・「技術的管理策」について、対策基準と実施手順の例を解説していきます。また、 IT環境構築・運用実施手順、セキュリティ対策状況の有効性評価の考え方について解説します。

参考文献

ISO/IEC 27001:2022

https://www.iso.org/standard/27001

ISO/IEC 27002:2022

https://www.iso.org/standard/75652.html

国民のためのサイバーセキュリティサイト　サイバーセキュリティ関連の法律・ガイドライン

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_legal.html

用語集

■AI
Artificial Intelligenceの略。「AI（人工知能）」という言葉は、1956年に米国の計算機科学研究者ジョン・マッカーシーが初めて使った言葉。1950年代後半から1960年代が第一次AIブーム、1980年代が第二次AIブーム、現在は2000年代からはじまる第三次AIブームである。
「AI」に関する確立した定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている
…… 1-1-1、4-1-1、4-2-5、5-2-1、5-2-2、5-2-3、6-1-1、6-1-3

■BCP
Business Continuity Plan（事業継続計画）の略。企業が災害やテロ攻撃などの緊急事態に直面した際に、被害を最小限に抑え、企業の存続に関わる最も重要な事業を継続または早期復旧するための計画
…… 2-3-2

■CSIRT（シーサート）
Computer Security Incident Response Teamの略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う
…… 2-1-3、6-1-3、7-5-3

■DDoS攻撃（ディードスこうげき）
Distributed Denial of Service Attackの略。攻撃者が複数のコンピュータを操作し、標的となるコンピュータに対して同時に大量の問い合わせを送ることで、過剰な負荷をかけてサービスを利用できなくする攻撃手法
…… 2-2-2、2-2-5、第一回コラム、7-4-4

■DFFT
Data Free Flow with Trustの略。日本が提案したコンセプトであり、ビジネスや社会的な課題を解決するために、データの国際的な自由な流れを促進すると同時に、プライバシー、セキュリティ、知的財産権に対する信頼を確保することを目指している
…… 5-2-1

■EDR
Endpoint Detection and Responseの略。パソコンやスマートフォン、サーバなどのエンドポイントにおける不審な動作を検知し、迅速な対応を支援するソリューション。従来のツールやソリューションでは防げなかった未知のマルウェアや不正アクセスを検知し被害の拡大を防止する
…… 2-2-4、2-2-5、3-1-1、3-4-1、12-3-1

■eKYC
electronic Know Your Customer の略称。オンラインで完結可能な本人確認方法のこと
…… 5-2-1

■GビズID
行政手続きなどにおいて手続を行う法人を認証するための仕組み。1つのID・パスワードで本人確認書類なしに様々な政府・自治体の法人向けオンライン申請が可能になる
…… 5-2-1

■ICSCoE中核人材育成プログラム
2017年4月にIPA内に設置された産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）が実施している人材育成プログラム。制御技術（OT：Operational Technology）と情報技術（IT）の両方の知識・スキルを有し、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応できる人材の育成を目的としている
…… 2-1-2

■ICT
Information and Communication Technologyの略。IT（情報技術）だけでなく、コンピュータやスマートフォンなどを用いて行うコミュニケーションを実現する技術（通信技術）を含んでいる
…… 4-1-2、5-2-1、7-2-2、7-3-1、14-1-1、14-1-2

用語集

■IoT（アイ・オー・ティー）
Internet of Thingsの略。日本語では「モノのインターネット」。インターネットにコンピュータやセンサー、カメラ、産業機械、家電など様々な「モノ」が接続され、データを収集したり、相互に情報をやり取りしたりする概念や仕組み、技術のこと
…… 1-1-1、2-1-2、2-2-2、4-1-1、4-2-5、5-2-2、5-2-3、6-1-2、7-4-3、7-4-4

■IPS
Intrusion Prevention Systemの略。不正侵入防止システムとも呼ばれるセキュリティ確保の仕組み。
IPSは、異常を検知した場合、管理者に通知するだけではなく、その通信を遮断する
…… 2-2-2、3-4-2

■IPアドレス
コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意になる数字の組み合わせ。 IPアドレスは、127.0.0.1のように0～255までの数字を4つ組み合わせたもので、単にアドレスと略されることがある。 現在主に使用されているこれら4つになる数字の組み合わせによるアドレス体系は、IPv4（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電などで大量にIPアドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が進みつつある。なお、IPv6では、アドレス空間の増加だけでなく、情報セキュリティ機能の追加などの改良も加えられている
…… 2-3-1、6-2-2

■ISAC
Information Sharing and Analysis Centerの略。業界内での情報共有・連携の取り組み推進を図る組織のこと。国内では、金融や交通、電力、ICTなどの分野にISACがある。ICT-ISACでは、ICT分野の情報セキュリティに関する情報(インシデント情報を含む。)の収集・調査・分析を行っている。
…… 14-1-2

■ISMS
Information Security Management Systemの略称。情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的な対策を含む、経営者を頂点とした総合的で組織的な取組み。組織がISMSを構築するための要求事項をまとめた国際規格がISO/IEC 27001（国内規格はJIS Q 27001）であり、審査機関の審査に合格すると「ISMS認証」を取得できる
…… 3-3-1、7-1-1、7-1-2、7-2-2、7-2-3、7-3-1、7-3-4、7-4-1、8-1-2、9-1-1、11-1-3、13-1-1、13-2-1、13-2-2、13-2-3、13-2-4、13-2-5、13-2-6、13-2-7、13-2-8、第七回コラム、14-1-1、15-1-1

■ISP
個人や企業などに対してインターネットに接続するためのサービスを提供する事業者のこと。ユーザはISPと契約し、回線を用いてISPが運営するネットワークに接続することで、インターネット上のサーバーなどへアクセスできる。
…… 14-1-2

■ITリテラシー
コンピュータやインターネットをはじめとする情報技術（IT）を適切に活用する基礎的な知識や技能
…… 3-1-1

■JPCERT/CC
日本におけるセキュリティインシデントなどの報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっている組織。政府機関や企業等から独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる。
…… 14-1-2

■JVN
Japan Vulnerability Notesの略。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対策情報を提供する、脆弱性対策情報ポータルサイトのこと。…… 14-1-2

■LockBit2.0
「Your files are encrypted by LockBit」というメッセージを表示させ、身代金を要求するマルウェア（ランサムウェア）。感染するとファイルが暗号化され、拡張子が「.LockBit」に変更される
…… 2-3-2

用語集

■NISC
National center of Incident readiness and Strategy for Cybersecurityの略。内閣サイバーセキュリティセンターの略称。サイバーセキュリティに関する施策の立案や実施、行政各部の情報システムに対するセキュリティ対策の強化を担当
…… 5-2-1、6-1-3、12-3-1

■NIST サイバーセキュリティフレームワーク（CSF）
米国政府機関の重要インフラの運用者を対象として誕生し、防御にとどまらず、検知・対応・復旧といったステップも含み、インシデント対応を含めており、日本も今後普及が見込まれる
…… 3-3-1、7-1-1、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、7-3-4

■PII
Personally Identifiable Informationの略。「個人を特定できる情報」と訳されることが多いが、実際には個人を特定するために使用される情報のこと。個人と1対1に紐づいているマイナンバー、メールアドレス、携帯電話番号、銀行口座番号だけでなく、氏名、生年月日、住所、勤務先などの情報もPIIに含まれる。
…… 14-1-1、14-1-2

■RPA
Robotic Process Automationの略。定型的な業務をソフトウェアのロボットにより自動化すること
…… 4-2-3

■SASE（サシー）
Secure Access Service Edgeの略。2019年に提唱されたゼロトラストセキュリティを実現する方法の1つで、IT環境のネットワークの機能とセキュリティの機能をクラウド上で統合して提供するサービス、また、その考え方・概念
…… 2-2-4

■SBOM（エスボム）
Software Bill of Materialsの略。ソフトウェアを構成する要素を一覧できるリストのこと。SBOMは、ソフトウェアの構成要素の名称やバージョン情報、開発者、依存関係などの情報を含む。SBOMは、ソフトウェアのリスクを把握・管理するのに役立つ
…… 6-1-1

■SDP
Software-Defined Perimeterの略。ゼロトラストを実現するための仕組みで、すべての通信をチェックおよび認証する。VPNは、ネットワーク接続前に一度だけ認証を行うのに対し、SDPは、ユーザの情報（デバイス、場所、OSなど）など複数の要素からネットワーク接続前、接続中、接続後で検証と認証を行う
…… 2-2-5

■SECURITY ACTION
中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度
…… 2-1-2、3-3-1

■Society5.0
サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）
…… 1-1-1、4-1-1、5-2-2、6-1-1、7-1-1、7-4-1、7-4-2、7-4-3

■SSL/TLS
WebサーバとWebブラウザとの通信において、データを暗号化して送受信する仕組みのこと。これにより、通信の途中で情報の盗聴・改ざんや、なりすましを防ぐことができる。過去にはSSLが使われていたが、脆弱性が発見されたため、TLS（v.1.2以降）への移行が進んでおり、今ではSSLは使われなくなってきている。しかし、歴史的経緯でSSLの用語が広く普及しているため、本テキストでは「SSL/TLS」と表記する。
…… 14-1-2

■SWG
Secure Web Gatewayの略。社内と社外のネットワーク境界で通信を中継する役割を持っている。また、やり取りしているデータを分析し、悪意のあるデータを遮断することでセキュアな通信環境を実現
…… 2-2-4

用語集

■VPN
Virtual Private Networkの略。インターネット上で安全性の高い通信を実現するための手法。通信データを暗号化し、送信元から送信先までの通信を保護することで、盗聴やデータの改ざんを防ぐ。このようにVPNを使用することで、ユーザは物理的な専用線で通信しているかのような安全な通信を行うことができる
…… 2-1-3、2-2-2、2-2-5、2-3-1、2-3-2、2-3-3、12-3-1、13-2-2、14-1-2、15-1-2

■WAF（ワフ）
Web Application Firewallの略。 従来のファイアウォールが、IPアドレスとポート番号で通信を制御していたことに対して、Webアプリケーションの脆弱性を狙うサイバー攻撃を防ぐことを目的として、アプリケーションレベルで通信を制御（分析・検知・遮断）するファイアウォールのこと
…… 2-2-2

■アクセス制御
特定のデータやファイル、コンピュータ、ネットワークにアクセスできるユーザを制限する機能のこと
…… 2-2-5、第一回コラム、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、9-1-1、14-1-1、14-1-2

■アセスメント
システムや運用環境などを客観的に調査・評価すること。現在の利用状況を把握することで、システムの再構築や運用改善の参考情報となる
…… 2-2-4、7-3-1、7-4-5、11-1-2

■暗号化
データの内容を変換し、第三者には、内容を見ても解読できないようにすること
…… 2-1-3、2-2-1、2-2-5、2-3-2、3-3-3、3-4-1、第一回コラム、12-2-1、12-3-1、14-1-1、14-1-2

■アンダーグラウンドサービス
合法ではない非公式な活動が行われるオンラインの闇市場やコミュニティでサイバー攻撃を目的としたツールなどを販売しているサービス
…… 2-1-3

■インターネットバンキング
インターネットを利用した銀行や金融機関との取引を行うサービスのこと。銀行の窓口やATMに出向かなくても、スマートフォンやパソコンなどを使って、いつでも利用可能な時間帯に振込や残高照会などの取引を行うことができる
…… 3-2-2、11-1-2

■ウイルス定義ファイル（パターンファイル）
セキュリティソフトがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真付きの手配書のようなもの
…… 3-2-2、3-3-3、12-3-1

■エンティティ
個人、組織、団体、コンピュータシステム、通信機器など、多様な実体のこと
…… 7-2-1

■エンドポイントデバイス
ネットワークに接続して、ネットワークを介して情報を交換するデバイス（デスクトップコンピュータ、仮想マシン、サーバなど）
…… 2-2-4

■改ざん
文書や記録などのすべてまたは一部に対して、無断で修正・変更を加えること。IT分野では、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為
…… 2-1-2、5-2-2、6-1-3、7-4-4、8-1-2、11-2-2、11-3-1、12-3-1、14-1-1、14-1-2

■可用性
許可された者だけが必要なときにいつでも情報や情報資産にアクセスできる特性
…… 第一回コラム、7-1-2、7-2-1、7-2-2、9-1-2、11-2-2、12-2-1、13-2-4、13-2-5、14-1-1、14-1-2

■完全性
参照する情報が改ざんされていなく、正確である特性
…… 第一回コラム、7-1-2、7-2-1、7-2-2、9-1-2、11-2-2、12-2-1、13-2-4、13-2-5、14-1-1

■機密性
許可された者だけが情報や情報資産にアクセスできる特性
…… 第一回コラム、7-1-2、7-2-1、7-2-2、9-1-2、11-2-2、12-2-1、13-2-4、13-2-5、 14-1-1

用語集

■脅威インテリジェンス
サイバー攻撃などの脅威への対応を支援することを目的として、収集・分析・蓄積された情報のこと。一部の産業では、企業横断的にこうした情報（インテリジェンス）を共有する活動が行われている。
…… 14-1-1、14-1-2

■供給者
組織に対して、製品・サービスを供給する企業または個人のこと。製品の場合、PCやサーバ、通信機器などがある。サービスの場合、クラウドサービス、インターネット接続サービス、業務の委託、物流、教育などがある。
…… 14-1-1、14-1-2

■クラッキング
悪意を持って情報システムに侵入し、データの改ざん・機密情報の盗み出し・サーバ攻撃・情報システムの破壊などの行為
…… 第一回コラム

■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る。「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。」
…… 11-2-2

■個人情報保護委員会
個人情報の有用性を考慮しながらも、個人の権利や利益を保護するために、個人情報の適切な取扱を確保することを任務とする、独立した機関のこと。個人情報保護法およびマイナンバー法に基づき、個人情報の保護に関する基本方針の策定・推進や個人情報などの取扱に関する監視・監督、認定個人情報保護団体に関する事務などの業務を行う行政機関（組織的には内閣府の外局）
…… 2-2-3、5-2-1、6-2-1、8-1-2、14-1-2

■サイバー攻撃
インターネットを通じて、別の企業や組織、ときに国家を攻撃する行為の総称。対象は、個人が所有するパソコンやスマートフォンから、企業のサーバやデータベース、国の重要インフラまで様々である。ネット社会となった現代では、インターネット空間をサイバー空間と呼ぶ。サイバー空間において、敵対する国家、企業、集団、個人などを攻撃する行為やその防御をサイバー戦争と呼ぶこともある。
…… 2-1-2、2-1-3、2-2-2、2-2-5、2-3-2、3-3-1、4-3-1、4-3-2、5-2-2、5-2-3、6-1-1、6-1-2、6-1-3、7-1-2、7-3-4、7-4-1、7-5-2、7-5-3、12-3-1、13-2-4、13-2-5、14-1-2

■サイバーセキュリティお助け隊サービス制度
中小企業のサイバーセキュリティ対策に不可欠な各種サービスをワンパッケージで安価に提供するサービス
…… 2-1-2

■サイバーセキュリティ戦略
組織や企業がセキュリティに関する目標を達成するための計画やアプローチ
…… 3-3-1、5-1-1、6-1-1

■サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）
単純なサイバー空間（仮想空間）におけるセキュリティ対策から、サイバー空間とフィジカル空間（現実空間）のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理するためのフレームワーク
…… 3-3-1、7-1-1、7-1-2、7-4-1、7-4-2、7-4-3、7-4-4、7-4-5

■サプライチェーン
製品やサービスの供給に関わる一連のプロセスのこと。具体的には、原材料や部品の調達、生産、物流、販売など、製品やサービスが最終的に消費者に届くまでの流れを指す。サプライチェーンは、製造業者、卸売業者、小売業者などが協力して構築される
…… 2-1-3、2-2-2、2-2-4、4-1-1、4-2-4、4-3-2、5-1-1、5-2-2、6-1-1、6-1-2、6-1-3、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、7-4-1、7-4-2、7-4-3、7-4-5、7-5-1、7-5-2、14-1-1、14-1-2

用語集

■情報資産
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
…… 3-3-1、7-2-1、7-2-2、7-3-4、7-4-4、7-5-1、8-1-2、11-1-1、 11-1-2、11-2-2、11-2-3、12-2-1、12-3-1、13-2-3、13-2-4、13-2-5、13-2-7、第七回コラム、14-1-2

■情報セキュリティ事象
情報セキュリティ上よくない、システムやサービス、ネットワークの状態のこと。
情報セキュリティ事象の中でも、事業運営を危うくしたり、情報セキュリティを脅かしたりする可能性が高いものは、セキュリティインシデントに分類される。
…… 14-1-1、14-1-2、15-1-1、15-1-2

■情報セキュリティの3要素「CIA」
情報セキュリティの3つの要素、機密性（Confidentiality）、完全性（Integrity） 、可用性（Availability）の頭文字をとって「CIA」と呼ぶ
…… 第一回コラム、第五回コラム

■真正性
情報セキュリティマネジメントの付加的な要素で、利用者、プロセス、システム、情報などが、主張どおりであることを確実にする特性のこと。真正性を低下させる例としては、なりすまし行為などがある
…… 2-1-3、第一回コラム、6-1-3、7-2-1、第五回コラム

■信頼性
システムが実行する処理に欠陥や不具合がなく、想定した通りの処理が実行される特性
…… 第一回コラム、6-1-1、6-1-3、7-2-1、7-4-2、7-4-3、7-4-4 、第五回コラム、13-2-5、14-1-2

■スクリーンロック
デバイスの誤動作や勝手に操作されることを防ぐための機能。スクリーンロック画面になっているときはパスワードやロックパターンの入力、指紋や顔の認証をしなければ解除することができない
…… 2-2-2

■脆弱性
情報システム（ハードウェア、ソフトウェア、ネットワークなどを含む）におけるセキュリティ上の欠陥のこと
…… 2-1-1、2-1-3、2-2-1、2-2-2、2-2-4、2-2-5、2-3-1、2-3-2、2-3-3、3-3-1、第一回コラム、6-1-3、7-2-2、7-4-4、7-4-5、9-1-2、10-1-1、11-1-2、11-1-3、11-2-2、11-2-3、11-3-1、13-2-4、14-1-1、14-1-2

■脆弱性診断
システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること
…… 2-3-1

■責任追跡性
情報資産に対する参照や変更などの操作を、どのユーザが行ったものかを確認することができる特性
…… 第一回コラム、7-2-1 、第五回コラム

■セキュリティインシデント
セキュリティの事故・出来事のこと。単に「インシデント」とも呼ばれる。例えば、情報の漏えいや改ざん、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インシデントに該当
…… 2-1-1、2-1-2、2-1-3、2-2-1、4-1-1、7-2-2、7-3-1、7-4-4、9-1-1、9-1-2、12-1-1、12-2-1、13-2-2、13-2-4、13-2-5、13-2-8、14-1-1、14-1-2

■セキュリティ・キャンプ
情報セキュリティに関する高度な技術と倫理に関する講習・演習を行う合宿。審査に通過した22歳以下の学生・生徒が対象。次代を担う情報セキュリティ人材を発掘・育成するために、情報処理推進機構（IPA）と（一財）セキュリティ・キャンプ協議会が実施している
…… 2-1-2

■セキュリティホール
情報システムにおけるセキュリティ上の欠陥のこと。「脆弱性」とほぼ同義であるが、セキュリティホールは、ソフトウェアの設計上のミスやプログラムの不具合によって発生するセキュリティ上の脆弱性のみを指す場合がある
…… 3-3-1

用語集

■セキュリティポリシー
企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと。社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するのが一般的
…… 2-1-1、2-2-1、3-3-1、6-1-2、7-4-4、8-1-1

■ゼロデイ攻撃
OSやソフトウェアに存在する脆弱性が公開された後、修正プログラムや回避策がベンダーから提供されるまでの間に、その脆弱性を悪用して行われるサイバー攻撃のこと
…… 2-1-3

■ゼロトラスト
従来の「社内を信用できる領域、社外を信用できない領域」という考え方とは異なり、社内外を問わず、すべてのネットワーク通信を信用できない領域として扱い、すべての通信を検知し認証するという新しいセキュリティの考え方
…… 2-2-4

■ソリューション
問題や課題を解決するための具体的な解決策や手段を指す。ある特定の課題やニーズに対して提供される解決方法やアプローチのことを指すことが一般的で、ビジネスシーンにおけるソリューションの意味とは「顧客が抱える問題や課題を解決すること」
…… 2-2-5、14-1-2

■ダークウェブ
特別な手法でないとアクセスできない、匿名性の高い非公開のWebサイトのこと。漏えいした個人情報や機密情報、危険な商品、クラッキングツールなど、違法なものが取引されている
…… 2-1-3

■多要素認証
多要素認証は、サービス利用時において利用者の認証を行うために、3つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも2つ以上の要素を組み合わせて認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマートフォンの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年ではFIDO2と呼ばれる、デバイスを使用したパスキーによる認証により、パスワードレスでの認証が広まっている
…… 2-2-5、2-3-3、8-1-2、 、第五回コラム、11-3-1、12-3-1、14-1-2

■データサイエンス
数学、統計、人工知能などの技術を用いて、大量のデータを解析し、ビジネスに有益な知見を抽出すること
…… 1-1-1

■デジタル化
紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション（digitization）と、デジタル技術を用いてビジネス・プロセスを自動化・合理化するデジタライゼーション（digitalization）がある。音楽ビジネスでいえば、アナログ記録のレコードをCD（コンパクトディスク）にするのがデジタイゼーション、音楽をダウンロード販売するのがデジタライゼーションである
…… 1-1-1、2-1-1、2-1-2、3-3-1、4-1-2、4-2-3、5-1-1、6-1-1、6-1-3、7-4-3

■デジタル情報
0、1、2のような離散的に（数値として）変化する量
…… 第一回コラム

■内部監査
内部の独立した監査組織が業務やシステムの評価、監査、アドバイスを行う活動である。情報セキュリティマネジメントシステム（ISMS）に関する国際規格であるISO27001の監査では、ポリシーや規定、手順に適合し、各情報資産が確実に守られているか確認する
…… 3-3-1、7-2-1、7-3-1、13-2-3、13-2-7、13-2-8、14-1-2

■ハウジングサービス
データセンターのラック（サーバを収容する鍵のついた棚）とサーバに接続する回線や電源を貸し出すサービスのこと。自社が所有しているサーバを、物理的にセキュリティが強固なデータセンターに設置し、運用できるため、セキュリティを強化できるメリットがある。
…… 12-3-1

用語集

■ビジネスインパクト分析
災害など不測の事態によって業務やシステムが停止した場合に、会社の事業に与える影響度を評価すること。BCP（事業継続計画）を立てるうえで実行する必要がある。
…… 14-1-2

■ビジネスメール詐欺
攻撃者がビジネス用のメールを装い、企業の担当者をだまして、不正送金や機密情報の流出などの原因となる攻撃。BEC（ベック）Business Email Compromiseとも略される
…… 2-1-3

■ビッグデータ
全体を把握することが困難な程、膨大な規模のデータ群
…… 1-1-1、5-2-2、5-2-3

■否認防止性
システムに対する操作・通信のログを取得や本人に認証させることにより行動を否認させないようにする特性
…… 第一回コラム 、第五回コラム

■標的型攻撃
機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルス付きメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られている。従来は府省庁や大手企業が中心に狙われてきたが、最近では地方公共団体や中小企業もそのターゲットとなっている
…… 2-1-2、2-1-3、12-3-1、13-2-5

■標的型メール攻撃
特定の個人や組織を標的にしたフィッシング攻撃の一種。一般のフィッシング攻撃とは異なり、業界ニュースや社内情報といった情報を利用するため、業務上のメールと見分けがつかない内容や、業務で付き合いがある人物の名前で送られることもある
…… 2-2-4

■ファイアウォール
本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを守るためのソフトウェアやハードウェアを指す。パソコンのOSに付随しているもの、セキュリティソフトに付いているもの、専用のハードウェアになっているものなど形態は様々である
…… 2-3-1、3-4-1、3-4-2、13-2-2、14-1-2

■不正アクセス
利用権限を持たない悪意のあるユーザが、企業や組織で管理されている情報システムやサービスに不正にアクセスすること。不正アクセスにより、正規の個人情報の窃取やデータの改ざんや破壊などの危険がある。日本では、2000年2月に施行された不正アクセス行為の禁止などに関する法律（不正アクセス禁止法）により、法律で固く禁じられている
…… 2-1-1、2-1-2、2-1-3、2-2-1、2-2-2、2-2-3、2-2-5、2-3-1、4-3-2、5-2-1、7-4-4、8-1-2、11-2-2、11-3-1、14-1-2

■踏み台
不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元のIPアドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することで、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ
…… 2-1-3、4-3-2

■フォレンジック
犯罪捜査における分析や鑑識を意味する言葉。サイバーセキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組みを指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる
…… 2-2-3、2-3-2

■ブラックマーケット
広義には、不法な取引が行われる市場を指す。不正に入手した個人情報などを売買するネット上の市場（闇市）
…… 2-1-3

用語集

■フレームワーク
フレームワーク（サイバーセキュリティフレームワーク）とは、マルウェアやサイバー攻撃など様々なセキュリティ上の脅威から、情報システムやデータを守るために、システム上の仕組みや人的な体制の整備を整える方法を「ひな形」としてまとめたもの
…… 2-2-4、3-4-1、7-1-1、7-1-2、7-2-1、7-3-1、7-3-2、7-4-1、8-1-1、8-1-2、9-1-2、13-1-1

■ブロックチェーン
複数のコンピュータを使用し、分散的にデータをブロック単位にまとめて鎖（チェーン）のように記録する仕組み
…… 1-1-1

■ベストプラクティス
何かを行う方法や工程、その実践例の中で、ある基準にしたがって最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例やよい成果をもたらす方法論
…… 2-1-3、2-3-1、7-1-1

■マルウェア
パソコンやスマートフォンなどのデバイスやサービス、ネットワークに害を与えたり、悪用したりすることを目的として作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる
…… 2-2-2、2-2-4、2-2-5、第一回コラム、7-2-2、12-3-1、13-2-4、14-1-1、14-1-2、15-1-2

■ミラサポコネクト
ビッグデータを活用して事業を伸ばしたい中小企業を応援するための「ミラサポコネクト構想」をもとにした、行政、支援者、民間事業者に分散して保有されているデータ（法人情報、決算情報、経営カルテなど）を連携し、経営課題解決に資する支援を提供するための、官民データ連携基盤
…… 5-2-1

■無線LAN
LAN は Local Area Network の略。物理的なケーブルを使わず、電波を利用してネットワークに接続する仕組み。この無線LANを通じて、コンピュータはインターネットにアクセスできる
…… 3-2-3、14-1-2

■ランサムウェア
悪意のあるマルウェアの一種。パソコンなどのファイルを暗号化し利用不可能な状態とし、解除と引き換えに被害者から身代金（ransom）を要求する
…… 2-1-2、2-1-3、2-2-1、2-2-2、2-2-5、2-3-2、2-3-3、7-5-1、8-1-2、14-1-2

■リスクアセスメント
企業や組織が持つ情報資産に対するリスクの分析・評価を行うプロセスのこと。具体的には情報資産の特定、脅威と脆弱性の特定と評価、リスクの分析と評価を行う。リスク評価の結果、許容できるもの以外は何らかの対策を講じる必要がある
…… 3-3-1、7-3-1、7-4-5、第四回コラム、11-1-1、11-1-2、11-1-3、11-2-1、11-2-2、11-3-1、12-2-1、13-2-4、13-2-5、13-2-6、13-2-7、13-2-8、14-1-1、14-1-2、15-1-1

■リスク評価
組織やプロジェクトにおける特定されたリスクに対して、重要度や影響度を評価するプロセス
…… 2-3-2、3-4-1、7-3-2、7-4-5、11-1-2、11-2-4、11-3-1、12-2-1、13-2-4、第七回コラム

■リモートデスクトップ接続
パソコン、タブレット、スマートフォンなどのデバイスを使用して、遠隔地から特定のパソコンに接続する方法
…… 2-2-2

令和5年度
中小企業サイバーセキュリティ対策
継続支援事業