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

セミナー内容

回数	テーマ
第1回	サイバーセキュリティを取り巻く環境および中小企業に 求められるサイバーセキュリティ対策
第2回	これからの企業経営で必要な攻めと守りのIT活用および サイバーセキュリティ対策
第3回	サイバーセキュリティに関する国の方針・施策および サイバー脅威の動向
第4回	サイバーセキュリティ対策におけるフレームワークの体系
第5回	組織として策定すべき対策基準及び情報セキュリティの 三大要素【対策基準レベル①】

セミナー内容

回数	テーマ
第6回	セキュリティリスク評価及び対策基準に記載されるべき管理策【対策基準レベル②】
第7回	組織として実施すべき具体的な対策事項・手順【実施手順・実施者マニュアルレベル①】
第8回	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】
第9回	技術的対策と物理的対策およびセキュリティ対策状況の有効性評価【実施手順・実施者マニュアルレベル③】
第10回	全体総括

１．組織的管理策

組織的管理策を参考とした対策基準・実施手順の策定

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-1.】
第14章 - 02

対策基準の策定

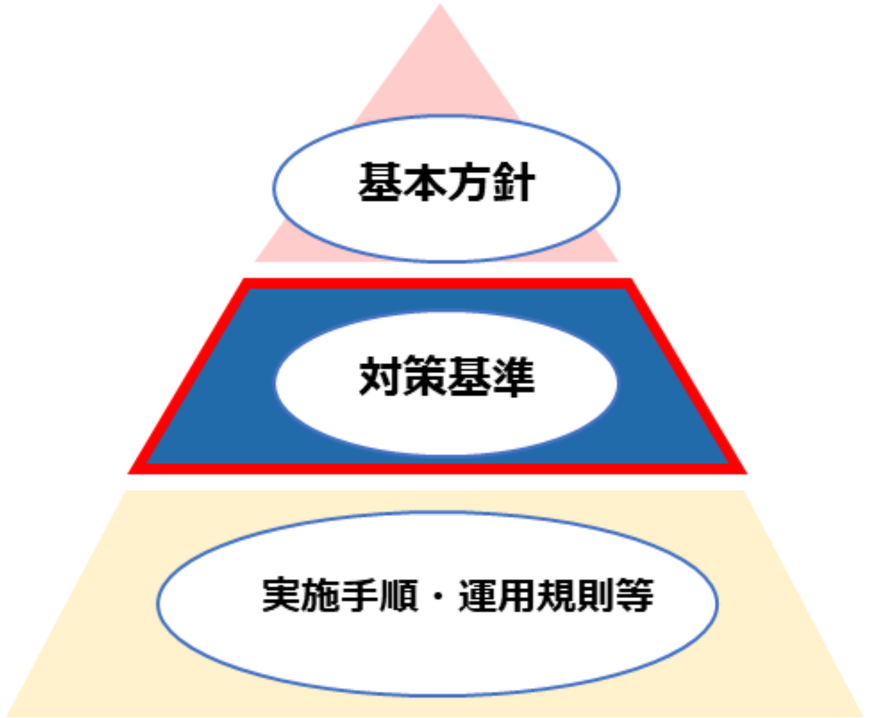
ISO/IEC 27001:2022附属書Aの管理策		
カテゴリ	項目数（合計93）	概要
組織的管理策	37	組織として取組む必要のある管理策。たとえば、情報セキュリティ方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。たとえば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理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

組織的管理策を参考とした対策基準・実施手順の策定

【復習】

対策基準の策定

情報セキュリティポリシーの構成



セキュリティ対策の関係図
（出典）総務省.”情報セキュリティポリシーの内容”

基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則等
対象者や用途によって必要な手続きを記述する

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-1.】
第14章 - 04

対策基準（例）

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-1.】
第14章 - 04

対策基準（例）

対策基準（例）
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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-1.】
第14章 - 05

対策基準（例）

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-1.】
第14章 - 05

対策基準（例）

対策基準（例）

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-1.】
第14章 - 05

対策基準（例）

対策基準（例）
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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-1.】
第14章 - 06

対策基準（例）

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-1.】
第14章 - 06

対策基準（例）

対策基準（例）
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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-1.】
第14章 - 06

対策基準（例）

対策基準（例）
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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-1.】
第14章 - 07

対策基準（例）

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-1.】
第14章 - 07

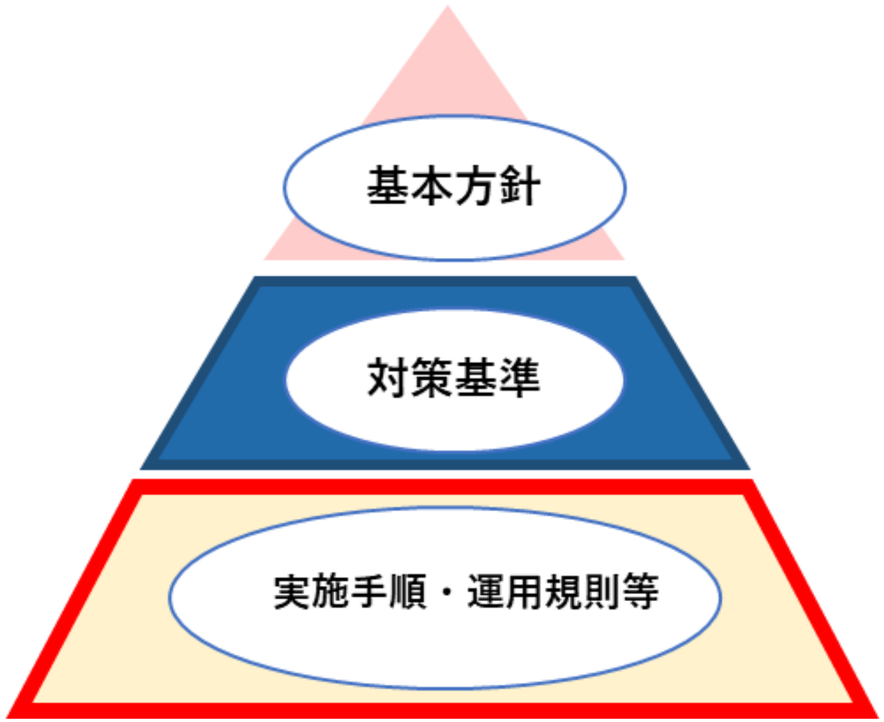
対策基準（例）

対策基準（例）
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。

組織的管理策を参考とした対策基準・実施手順の策定 【復習】

実施手順の策定

情報セキュリティポリシーの構成



セキュリティ対策の関係図
（出典）総務省.”情報セキュリティポリシーの内容”

基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則等
対象者や用途によって必要な手続きを記述する

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 - 08

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

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 - 09

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）

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 - 09

5.2 情報セキュリティの役割及び責任

実施手順（例）

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 - 10

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。

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 - 10

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 - 11

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 - 11

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 - 12

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

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 - 12

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 13, 14

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。 分類についてはセミナーテキスト参照

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

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 14

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 14

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 15

5.14 情報伝送

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 16

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。

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 17

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 17

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 18

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。

5.20 供給者との合意における情報セキュリティの取り扱い

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 19

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

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 20

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。 詳細はテキスト参照

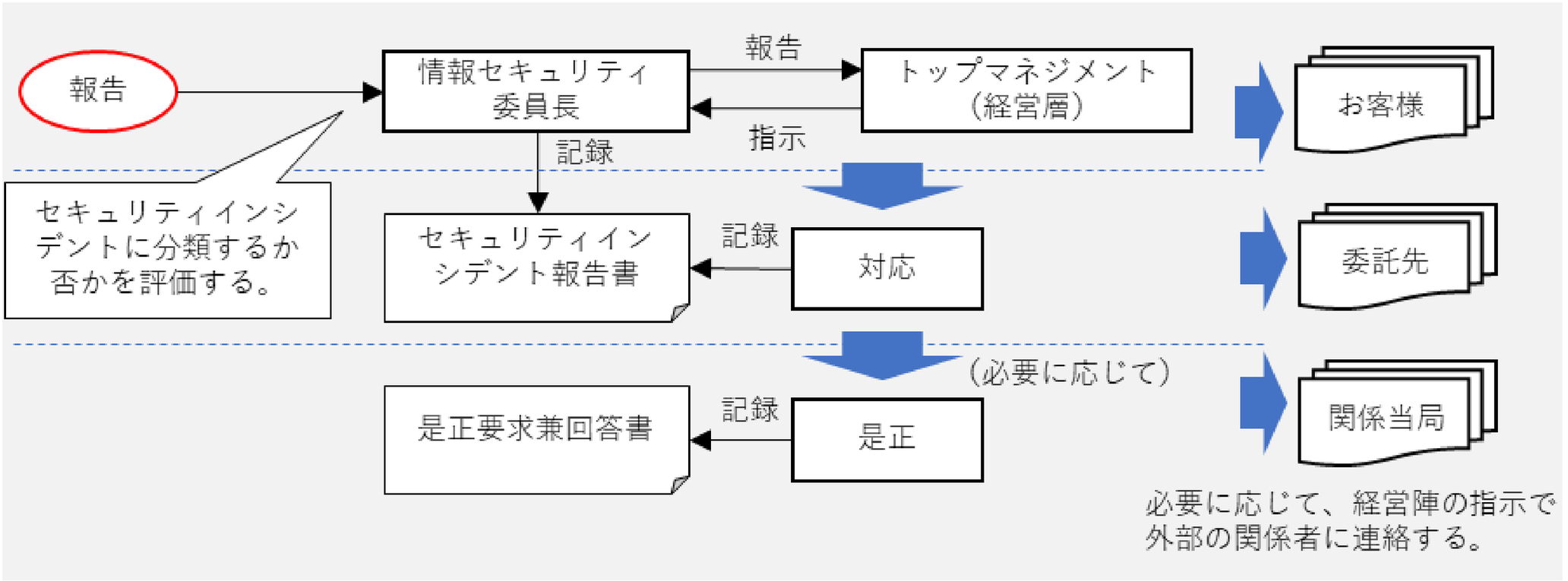
組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 21

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。



組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 21

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

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 22, 23

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。 詳細はテキスト参照

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 23

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 24

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 25

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 26

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 27

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 28

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。 詳細はテキスト参照

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 29

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

5.36 情報セキュリティのための方針群、規制及び標準の順守

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。

組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 29

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

2. 人的管理策

人的管理策を参考とした対策基準・実施手順の策定

人的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-1.】
第14章 – 02

対策基準の策定

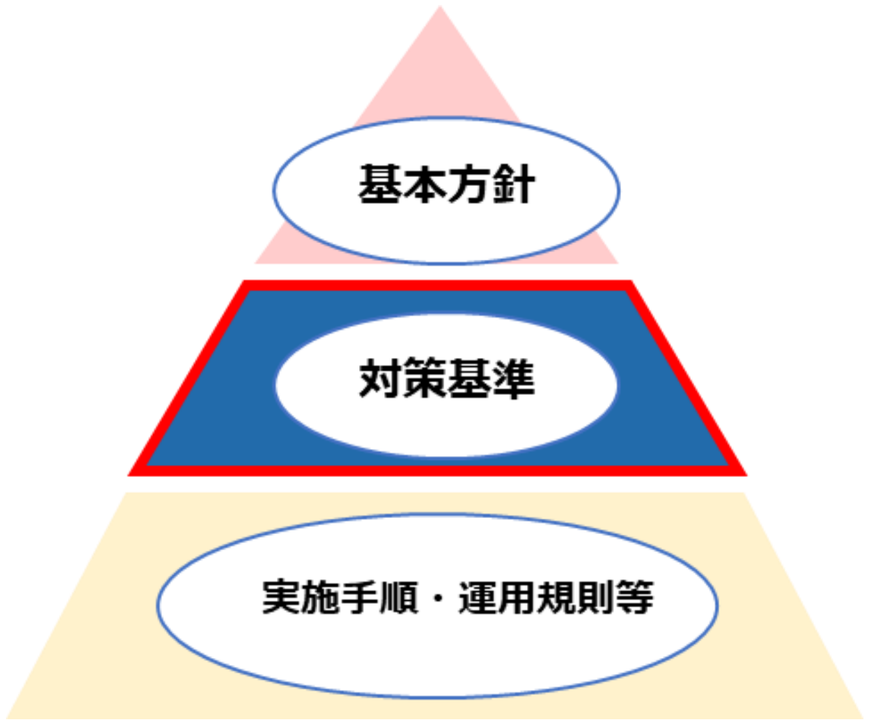
ISO/IEC 27001:2022附属書Aの管理策		
カテゴリ	項目数（合計93）	概要
組織的管理策	37	組織として取組む必要のある管理策。たとえば、情報セキュリティ方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。たとえば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理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

人的管理策を参考とした対策基準・実施手順の策定

対策基準の策定

【復習】

情報セキュリティポリシーの構成



セキュリティ対策の関係図
（出典）総務省.”情報セキュリティポリシーの内容”

基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則等
対象者や用途によって必要な手続きを記述する

人的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト15-1-1.】
第15章 – 03

対策基準（例）

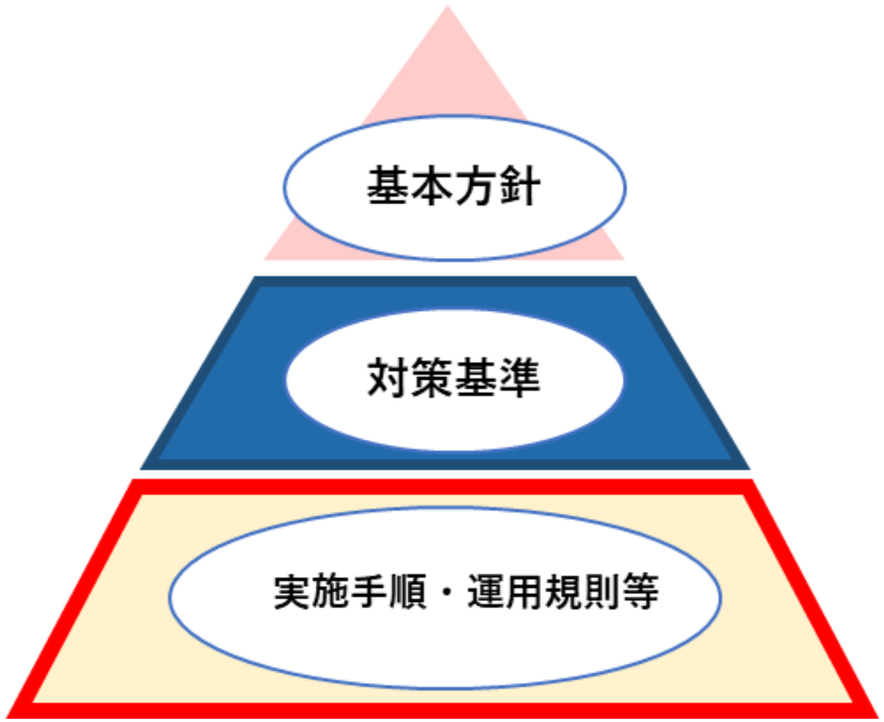
対策基準（例）
6.1 選考 従業員や契約相手を選定する際、個人情報の保護や雇用に関する法令を考慮して経歴などを確認しなければならない。 **6.2 雇用条件** 雇用契約書には、情報セキュリティに関する要員および組織の責任を記載しなければならない。 **6.3 情報セキュリティの意識向上、教育及び訓練** 従業員に対し、情報セキュリティに関する教育および訓練を実施しなければならない。 **6.4 懲戒手続** 情報セキュリティ方針に違反した場合の懲戒手続を、正式に定めなければならない。 **6.5 雇用の終了又は変更後の責任** 雇用の終了または変更の後も引き続き有効な情報セキュリティの責任や義務を、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。

人的管理策を参考とした対策基準・実施手順の策定

実施手順の策定

【復習】

情報セキュリティポリシーの構成



セキュリティ対策の関係図
（出典）総務省.”情報セキュリティポリシーの内容”

基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則等
対象者や用途によって必要な手続きを記述する

人的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト15-1-2.】
第15章 – 04

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。

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。

人的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト15-1-2.】
第15章 – 05

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。

人的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト15-1-2.】
第15章 – 06

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。

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。

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。

人的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト15-1-2.】
第15章 – 07

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。

6.8 情報セキュリティ事象への報告

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。

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