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】

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12章. 具体的手順の作成（LV.1 クイックアプローチ/LV.2 ベースラインアプローチ）

12-1. 【LV.1 クイックアプローチ】【LV.2 ベースラインアプローチ】の概要

12-2. 【LV.1 クイックアプローチ】セキュリティインシデント事例を参考とした実施手順

12-3. 【LV.2 ベースラインアプローチ】ガイドラインを参考とした実施手順

章の目的
第12章では、セキュリティインシデント事例を参考にするクイックアプローチと、ガイドラインやひな形などの資料を参考にするベースラインアプローチにおける対策基準・実施手順の策定方法の理解を目的とします。
主な達成目標
□ クイックアプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること □ ベースラインアプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

12-1-1. クイックアプローチ・ベースラインアプローチ

セキュリティ対策基準を策定し、具体的な実施手順を明確にすることで、情報漏えいなどのリスク対策を行います。対策内容を決めるためのアプローチ手法として、「LV.1 クイックアプローチ」「LV.2 ベースラインアプローチ」「LV.3 網羅的アプローチ」があります。

本章では、「LV.1 クイックアプローチ」と「LV.2 ベースラインアプローチ」における実施手順の作成方法について説明します。LV.1 クイックアプローチは、即時の対応や緊急事態への対処が必要な事例に対して、対策基準や実施手順を策定していくアプローチ手法です。LV.2 ベースラインアプローチは、ガイドラインなどを参考に、対策基準や実施手順を策定するアプローチ手法です。

LV.1 クイックアプローチ（緊急性の高い事象に対応するための対策）

概要

報道される事例や情報セキュリティ10大脅威などから、発生する可能性が高いセキュリティインシデント事例や、セキュリティインシデントが発生した場合に被害が大きい事例を参考にし、対策基準や実施手順を策定します。

メリット

- 小規模な対策や修正を迅速に実施可能。
- 低コストでリスクを軽減。

デメリット

- 短期的な解決策に偏りがちになる。
- セキュリティインシデント事例ごとに策定するため、網羅性は低い。

LV.2 ベースラインアプローチ（即効性のあるアプローチ方法）

概要

IPAや総務省などが発行しているガイドラインやひな形を参考に、対策基準や実施手順を策定します。セキュリティ対策のガイドラインやひな形を参考にすることで、組織全体で一貫性があり、セキュリティの最低基準を満たす対策基準や実施手順を策定します。

メリット

- 組織全体で一貫性を確保できる。
- 最低限実施すべきセキュリティ対策を講じることができる。

デメリット

- 追加のセキュリティ対策やリスクに対する適切な対応策を検討することが必要になる。
- ガイドラインやひな形は、一般的な組織を想定したものであるため、自社の組織やシステム、環境に見合ったものであるかどうかを十分に検討する必要があります。

12-2-1.セキュリティインシデント事例を参考とした実施手順

LV.1 クイックアプローチ（1/3）

クイックアプローチでは、自社で発生する可能性が高い、または実際に発生したときの被害が大きいと考えられるセキュリティインシデント事例を参考に、対策基準を策定します。決定した対策基準をもとに、具体的に実施する内容（実施手順）を作成します。

対策基準・実施手順作成の手順

セキュリティインシデント事例をもとにリスクアセスメントを実施します。以下は、情報セキュリティ10大脅威2023にランクインしている「内部不正による情報漏えい」に関するセキュリティインシデント事例です。

事例：内部不正による情報漏えいの疑い（卸売業・小売業、従業員数6~20名以下）

被害内容

元従業員が退職前に大量にファイルをダウンロードしました。また、同従業員が使用していたPCの履歴が消去され、専門家でも復旧できない状態になっていました。

機密情報の持ち出しをした確定的な証拠が得られなかったため、結果的には被害届を提出しませんでした。しかし、この判断をするまでに2年かかりました。その間、弁護士に情報提供するために、多くの作業が必要になりました。たとえば、経営者と総務担当は、情報漏えいしたと疑われる膨大なログを確認し、どれが機密情報に該当するかチェックする作業を強いられました。トラブル発生時は、人件費だけでなく、心的負担も大きくかかりました。

被害発生の原因

社外からの脅威の対策としてウイルス対策ソフトウェアや電子メールへの対応、アクセス制限などは進めていたが、社内から発生する脅威の対策は不十分であったこと。

セキュリティインシデント事例：内部不正による情報漏えい
(出典) IPA「2021年度 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 -事例集- 」を基に作成

セキュリティインシデント事例をもとに、リスクアセスメントの実施
（リスク特定、リスク分析、リスク評価）

リスク特定（例）

セキュリティインシデント事例を参考に、情報資産の洗い出しと、「機密性」「完全性」「可用性」の観点から重要度を算出します。セキュリティインシデント事例では、従業員が使用していたPCが悪用されていたため、以下の資産目録の例では「媒体・保存先」が従業員が使用するPCである情報資産を洗い出しています。機密性・完全性・可用性の評価値と、重要度は「11-2-2. リスクの特定」で解説した方法で算出します。リスクアセスメントの詳細は「第11章. リスクマネジメント」を参照してください。

機密性・完全性・可用性の評価値は、1~3で記載
重要度は、機密性・完全性・可用性いずれかの最大値

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	管理部署	媒体・保存先	機密性	完全性	可用性	重要度
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	人事担当者のPC	3	3	2	3
経理	当社宛請求書	過去3年分	経理部	経理部長	経理部	経理担当者のPC	3	3	2	3
営業	顧客リスト	得意先	営業部	営業部長	営業部	営業担当者のPC	3	3	3	3

資産目録の例
（出典）IPA 「リスク分析シート」を基に作成

12-2-1.セキュリティインシデント事例を参考とした実施手順

LV.1 クイックアプローチ（2/3）

リスク分析（例）

リスク特定で算出した重要度と、被害発生可能性からリスクレベルを算出します。被害発生可能性は、セキュリティインシデント事例と同様の被害がどの程度起きやすいかを考慮して算出します。被害発生可能性・リスクレベルの詳しい算出方法は、「11-2-3. リスクの分析」を参照してください。

「リスクレベル」＝「重要度」×「被害発生可能性」

リスクレベルの算出方法

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	管理部署	媒体・保存先	機密性	完全性	可用性	重要度	被害発生可能性	リスクレベル
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	人事担当者のPC	3	3	2	3	3	9
経理	当社宛請求書	過去3年分	経理部	経理部長	経理部	経理担当者のPC	3	3	2	3	2	6
営業	顧客リスト	得意先	営業部	営業部長	営業部	営業担当者のPC	3	3	3	3	2	6

リスク評価（例）

リスクレベルをもとに、必要なリスク対応を検討します。今回は、例としてリスク低減や回避を選択します。

リスク低減	セキュリティ対策（管理策）を採用することによって、リスクの発生確率を低くしたり、リスクが顕在化したときの影響の大きさを小さくしたりすること
リスク移転	リスクを他者に移して、自分たちの責任範囲外にしたり、リスクが顕在化したときの損失を他者に引き受けさせたりすること
リスク回避	リスクが発生する可能性のある環境を排除するなど、リスクそのものをなくそうとすること
リスク受容（保有）	対策を行わずにリスクを受け入れるということ

リスク評価をもとに対策基準・実施手順の作成

対策基準の策定（例）

リスク評価の結果を参考に対策基準を策定します。今回の例では、リスク低減や回避に関する対策基準を決定しています。対策基準の例は以下の通りです。

対策基準（例）

- 社内の機密情報に関する社内規定の策定
- 重要情報の管理、保護
- 物理的管理の実施
- 従業員向け研修の実施

12-2-1.セキュリティインシデント事例を参考とした実施手順

LV.1 クイックアプローチ（3/3）

実施手順の作成（例）

情報セキュリティ関連規程を参考に、実施手順を作成します。情報セキュリティ関連規程とは、情報セキュリティに関する社内規則の見本です。情報セキュリティ関連規程から、対策基準に合った規則を選択し、赤字の箇所を自社の状況に合わせて編集することで、実施手順を作成します。

実施手順の作成（例）

- **機密情報に関する社内規定の策定**
  （例）従業員の責務
  従業員は以下を遵守する
  従業員は、当社が営業秘密として管理する情報およびその複製物の一切を許可されていない組織、人に提供してはならない。
  従業員は、当社の情報セキュリティ方針および関連規程を遵守する。違反時の懲戒については、就業規則に準じる。
  従業員は、在職中に交付された業務に関連する資料、個人情報、顧客・取引先から当社が交付を受けた資料またはそれらの複製物の一切を退職時に返還する。
  従業員は、在職中に知り得た当社の営業秘密または業務遂行上知り得た技術的機密を利用して、競合的あるいは競業的行為を行ってはならない。

- **重要情報の管理、保護**
  （例）利用者アカウントの管理
  利用者の認証に用いるアカウントが不要になる場合、システム管理者は、当該アカウントの削除または無効化を、当該アカウントが不要になった日の翌日までに実施する。

- **物理的管理の実施**
  （例）情報資産の社外持ち出し管理
  情報資産を社外に持ち出す場合には、以下を実施する。
  社外秘の場合は所属部門長の許可を得る。
  極秘の場合は代表取締役の許可を得る。
  ノートパソコンのハードディスクに保存して持ち出す場合は、ハードディスク/フォルダー/データを暗号化する。
  スマホ、タブレットに保存して持ち出す場合は、セキュリティロックを設定する。
  USBメモリなどの小型電子媒体は、大きなタグをつける/ストラップで体やカバンに固定する/落としてもすぐに分かるように鈴をつける。
  屋外でネットワークへ接続して極秘または社外秘の情報資産を送受信する場合は、暗号化する。
  携行中は常に監視可能な距離を保つ。

- **従業員向けの研修**
  （例）情報セキュリティ教育
  教育責任者は、以下の点を考慮し、情報セキュリティに関する教育計画を年度単位で立案する。
  対象者：全従業員
  テーマ：以下は必須とする。
  情報セキュリティ関連規程の説明（入社時、就業時）
  最新の脅威に対する注意喚起（随時）
  関連法令の理解（関連法令の公布・施行時）
  個人情報の取扱いに関する留意事項
  コンプライアンス教育

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（1/8）

ベースラインアプローチでは、ガイドラインやひな形などの資料を参考に対策基準、実施手順を作成します。次のページから、以下の資料をもとに対策基準、実施手順を作成する流れを説明します。

- IPA「中小企業の情報セキュリティ対策ガイドライン第3.1版」
- NISC「インターネットの安全・安心ハンドブックVer.5.0」
- 総務省「テレワークセキュリティガイドライン第5版」
- IPA「中小企業のためのクラウドサービス安全利用の手引き」
- IPA「情報セキュリティ関連規程」

各資料の概要は以下の通りです。

IPA「中小企業の情報セキュリティ対策ガイドライン第3.1版」

「中小企業の情報セキュリティ対策ガイドライン」は、情報セキュリティ対策に取組む際の、（1）経営者が認識し実施すべき指針、（2）社内において対策を実践する際の手順や手法をまとめたものです。経営者編と実践編で構成されており、中小企業の利用を想定しています。付録の「5分でできる！情報セキュリティ自社診断」や「情報セキュリティハンドブック（ひな形）」を活用することで、対策基準、実施手順を策定できます。

NISC「インターネットの安全・安心ハンドブックVer.5.0」

「インターネットの安全・安心ハンドブック」は、サイバーセキュリティに関する基本的な知識を、身近な具体例を取り上げながら説明したものです。子供やシニアの方など、インターネットの一般利用者だけでなく、中小企業なども活用できます。中小組織向けにある「インターネットの安全・安心ハンドブックVer 5.00＜中小組織向け抜粋版＞」を活用することで、対策基準、実施手順を策定できます。

総務省「テレワークセキュリティガイドライン第5版」

「テレワークセキュリティガイドライン」は、企業などがテレワークを導入する際のセキュリティ対策についての考え方や対策例を示したものです。テレワークを既に導入している場合は、自社のテレワーク環境がガイドラインに沿ったものであるのか検証できます。テレワークに関する「経営者」、「システム・セキュリティ管理者」、「テレワーク勤務者」の立場からそれぞれのセキュリティ対策について対策基準、実施手順を策定できます。

IPA「中小企業のためのクラウドサービス安全利用の手引き」

「中小企業のためのクラウドサービス安全利用の手引き」は、中小企業の情報セキュリティ対策ガイドラインの付録資料です。クラウドサービスを安全に利用するための手引きが記載されています。「クラウドサービス安全利用チェックシート」と「解説編」を参考にすることで、クラウドサービス利用に関する対策基準、実施手順を策定できます。

IPA「情報セキュリティ関連規程」

「情報セキュリティ関連規程」は、自社に適した規程を作成するためのひな形です。ひな形に修正を加えることで、対策基準、実施手順を策定します。1から文書化する必要がないため、効率的に策定できます。

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（2/8）

IPA「中小企業の情報セキュリティ対策ガイドライン第3.1版」の活用

対象者	• 中小企業および小規模事業者（業種は問わず、法人・個人事業主・各種団体も含む）の経営者と情報管理を統括する方 • 情報セキュリティ対策を部分的に実施してきた企業 • 情報セキュリティに関する知識を十分に有した人材が不足している企業など
目的	情報セキュリティに関する組織的な取組みを開始するため

本ガイドラインは、情報セキュリティに関する組織的な取組みを行う際に活用できます。本ガイドラインをもとに実施手順を策定する際は、「1. 実施状況の把握」「2. 対策の決定と周知」の手順で策定します。

1. 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」を利用し、現在の情報セキュリティ対策の実施状況を把握します。合計25問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ます。設問の例（一部抜粋）は以下の通りです。

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	分からない
Part1 基本的対策	1	パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	4	2	0	-1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？	4	2	0	-1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	-1
	4	重要情報に対する適切なアクセス制限を行っていますか？	4	2	0	-1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	-1

自社診断の設問（一部抜粋）
(出典) IPA「5分でできる！情報セキュリティ自社診断」を基に作成

「5分でできる！情報セキュリティ自社診断」の使い方

- ✓ 経営者や情報システム担当者、部門長など情報セキュリティ対策の実施状況が分かる方が、25問の設問に回答します。
- ✓ 事業所が複数ある、部署数が多いなど、1人で記入することが難しい場合には、事業所や部署ごとに記入し、責任者・担当者が集計します。
- ✓ 実施状況が分からない場合、各従業員に質問して、回答を総合して記入します。
- ✓ チェック欄の該当するもの1つに〇をつけて、「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」「分からない…-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「分からない」になっている項目を把握します。

詳細理解のため参考となる文献（参考文献）	
中小企業の情報セキュリティ対策ガイドライン第3.1版	https://www.ipa.go.jp/security/guide/sme/about.html
5分でできる！情報セキュリティ自社診断	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（3/8）

2.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」（解説編）を参考にし、実行すべき情報セキュリティ対策を検討・決定します。解説編の例（抜粋）は以下の通りです。

診断編　No.3	パスワード管理
強固なパスワードを使用する	
パスワードが推測や解析されたり、Web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。	
対策例	• パスワードは10文字以上で「できるだけ長く」、大文字、小文字、数字、記号含めて「複雑に」、名前、電話番号、誕生日、簡単な英単語などは使わず、推測できないようにする。 • 同じID・パスワードを複数サービス間で使い回さない。 • テレワークでVPNやクラウドサービスを利用する際は、強固なパスワードを設定し、可能な場合は多段階認証や多要素認証を利用する。

解説編の一例
(出典) IPA「5分でできる！情報セキュリティ自社診断」を基に作成

「5分でできる！情報セキュリティ自社診断」（解説編）の使い方

✓ 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を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。

対策の決定後、「情報セキュリティハンドブック（ひな形）」を利用し、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、自社診断の解説編に記載されている対策例と連動しています。ひな形を編集して決定した対策内容を具体的に記述し、従業員に配付します。ひな形の記載例は以下の通りです。

実施手順の例：パスワードの管理
ログインやファイル暗号化に使うパスワードは、以下に従って設定・利用する。

編集前（ひな形）

○必須	×禁止
10文字以上の文字数で構成されている	名前・愛称・地名・電話番号・生年月日・辞書に載っている単語・よく使われるフレーズは使わない

編集後

○必須	×禁止
16文字以上の文字数で構成されている	社員番号・名前・住所・電話番号・生年月日・辞書に載っている単語・他人に推測されやすい文字列は使わない

ひな形の修正例
(出典) IPA「情報セキュリティハンドブック（ひな形）」を基に作成

「情報セキュリティハンドブック（ひな形）」の使い方

✓ 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。
✓ 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。

詳細理解のため参考となる文献（参考文献）	
情報セキュリティハンドブック（ひな形）	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055529.pptx

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（4/8）

NISC「インターネットの安全・安心ハンドブックVer.5.0」の活用

対象者	• 全社員
目的	一人ひとりが能動的にサイバー空間における脅威を知り、サイバーセキュリティに対する素養・基本的な知識を身につけるため

本ハンドブックは、サイバー攻撃の手口やリスクを身近な具体例を取り上げながら説明しているため、専門知識を必要とせずサイバーセキュリティ対策を知ることができます。インターネットの利用者が実施すべき基本的なサイバーセキュリティ対策に加えて、中小組織向けのサイバーセキュリティ対策を記載しています。企業経営においてセキュリティ対策に投資すべき理由、企業特有のサイバーセキュリティ対策に必要なルール作りといった内容を説明しています。

以下では、第1章の「最低限実施すべきサイバーセキュリティ対策を理解しよう」を用いて、サイバーセキュリティ対策の実施手順の作り方を説明します。

（例）①OSやソフトウェアは常に最新の状態にしておこう

インターネットの安全・安心ハンドブック記載
- OS関連のアップデート処理は自動で行われるか、アップデートを行うよう通知が出るようにする。
- セキュリティ関連ニュースサイトなどでアップデートを促す情報が流れていたら、自主的に更新処理をかけるようにする。
- サイバー攻撃で狙われやすい、ソフトウェアを重点的に更新する。
- 機器そのものの基本プログラムを更新するファームウェアもアップデートする。
- セキュリティソフトをインストールしている場合は、最新のウイルス定義ファイルに自動更新されるよう設定する。
- アップデートが提供されなくなったOSやソフトウェアはセキュリティホールが見つかっても修正用アップデートが提供されず、攻撃に対して非常に脆弱なので、使用しないようにする。

自社の状況
- OS、オフィス系ソフト、セキュリティソフトは法人向けを利用しているため、アップデート管理は情報システム部が担当。
- 情報システム部がブラウザは古いバージョンを使わないように通知している。
- 自宅で使用しているリモート用PCは、一般向けのソフトがインストールされている。

実施手順

対象：PC
システム管理者は、アップデート管理として以下を実施する。
- システム管理者は月末にOS、オフィス系ソフト、セキュリティソフトの更新プログラムを適用する。緊急に対策が必要な場合は、従業員に通知し、更新プログラムを適用する。
- 従業員は、毎月OS、オフィス系ソフトの更新プログラムを適用する。確認方法はチェックリストを用いる。
- 従業員は、ブラウザのアップデートを適宜行い、バージョン○○以前のものは使用しない。
- システム管理者は○○日にセキュリティソフトのウイルス定義ファイルの更新を行う。

詳細理解のため参考となる文献（参考文献）	
インターネットの安全・安心ハンドブックVer.5.00	https://security-portal.nisc.go.jp/guidance/handbook.html

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（5/8）

総務省「テレワークセキュリティガイドライン第5版」の活用

対象者	• 経営者 • システム・セキュリティ管理者 • テレワーク勤務者
目的	テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するため

本ガイドラインでは、セキュリティ対策を整理するため、13個の対策分類に分かれています。「経営者」、「システム・セキュリティ管理者」、「テレワーク勤務者」の立場から対策分類ごとに具体的に実施すべき事項を示しています。

以下では、「6.マルウェア対策」をもとに、自社の状況からセキュリティ対策の実施手順の作成例を説明します。

（例）6. マルウェア対策

システム・セキュリティ管理者が実施すべき対策
- テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。
- セキュリティ対策ソフト（ウイルス対策ソフト）やメールサービスに付属しているフィルタリング機能やフィッシング対策機能などを用いて、テレワーク勤務者がマルウェアの含まれたファイルを開いたり、危険なサイトにアクセスしたりしないように設定する。
- テレワーク端末にEDRを導入し、未知のマルウェアを含めた不審な挙動を検知し、マルウェア感染後の対応を迅速に行えるようにする。
- テレワーク勤務者が利用するテレワーク端末のセキュリティ対策ソフト（ウイルス対策ソフト）について、定義ファイルの更新状況やマルウェアの検知状況が一元管理できるようにする。

テレワーク勤務者が実施すべき対策
- 少しでも不審を感じたメール（添付ファイルやURLリンクなどを含む。）は開かず、必要に応じて送信者に送信状況の確認を行うほか、システム・セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心がける。
- テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。

自社の状況
- テレワーク端末には、法人向けのセキュリティ対策ソフトとEDR製品を導入しており、システム管理者はウイルス定義ファイルの更新などを一元管理できる。
- システム管理者は毎月○○日にセキュリティソフトのレポートを確認している。
- 不審なメールが来た場合は、情報システム部と上長に連絡するようにしている。

実施手順

テレワーク端末のマルウェア対策として以下を実施する。
- システム管理者は会社支給のテレワーク端末にセキュリティ対策ソフトとEDR製品をインストールし、一元管理する。
- システム管理者は、テレワーク端末のウイルス定義ファイルの自動更新とリアルタイムスキャンを設定する。
- システム管理者は毎月○○日にセキュリティソフトとEDR製品のレポートを確認し、不審な点があれば該当のテレワーク端末所有者に対して、確認を行う。
- 従業員は、不審を感じたメール（添付ファイルやURLリンクなどを含む。）は開かず、システム管理者と上長へ連絡する。

詳細理解のため参考となる文献（参考文献）	
テレワークセキュリティガイドライン第5版	https://www.soumu.go.jp/main_content/000752925.pdf

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（6/8）

IPA「中小企業のためのクラウドサービス安全利用の手引き」の活用

対象者	• クラウドサービスを利用する企業
目的	クラウドサービスを安全に利用するため

本ガイドラインは、クラウドサービスを安全に利用するために活用できるガイドラインです。「利用するクラウドサービスを選定するとき」、「クラウドサービスを運用していくとき」、「クラウドサービスのセキュリティ対策を検討するとき」のタイミングで活用することができます。本ガイドラインの使い方としては、「クラウドサービス安全利用チェックシート」でチェックを行います。また、「解説編」を参考に、利用者としての役割や責任を認識し、実施手順を策定します。

以下は、クラウドサービスの運用に関する設問例となります。

運用するときのポイント	
管理担当者を決める	クラウドサービスの特性を理解した管理担当者を社内に確保していますか？
利用者の範囲を決める	クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？
利用者の認証を厳格に行う	パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど）
バックアップに責任を持つ	サービス停止やデータの消失・改ざんなどに備えて、重要情報を手もとに確保して必要なときに使えるようにしていますか？

クラウドサービス安全利用チェックシートの例（一部抜粋）
(出典) IPA「中小企業のためのクラウドサービス安全利用の手引き」を基に作成

解説編をもとに実施手順を作成します。 以下は、チェックシートの設問「バックアップに責任を持つ」の実施手順（例）を記載します。自社の状況に合わせて赤文字の箇所を修正することで、自社に適した実施手順を作成できます。

実施手順の例：バックアップに責任を持つ

バックアップの管理
サービス停止やデータの消失・改ざんなどに備え、重要情報を手もとに確保して、必要なときに使えるようにする。

会計データやホームページなど、消失や改ざんの影響が大きいものは以下の規則を遵守する

クラウドサービスの拡張機能にバックアップがある場合は利用する
月に1度、社内の専用ハードディスクにバックアップを取得する
直前のバックアップよりもさらに過去の状態に遡って復元できるよう、2、3ヶ月前に取得したバックアップを保存しておく

詳細理解のため参考となる文献（参考文献）	
付録6：中小企業のためのクラウドサービス安全利用の手引き	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（7/8）

IPA「情報セキュリティ関連規程」の活用

対象者	• 中小企業
目的	自社のリスクに応じた対策規程を作成するため

情報セキュリティ関連規程とは、自社が対応すべきリスクと対策を検討し、文書化した規程のことです。企業を取り巻くリスクは、事業内容や取扱う情報、職場環境、ITの利用状況などによって異なるため、汎用的な規程をそのまま使っても、自社に適さない場合があります。そこで情報セキュリティ関連規程を活用することで、効率的に自社に適した規程を作成できます。

本ガイドラインを用いて、規程を作成する手順を説明します。

1. 対応すべきリスクを特定する

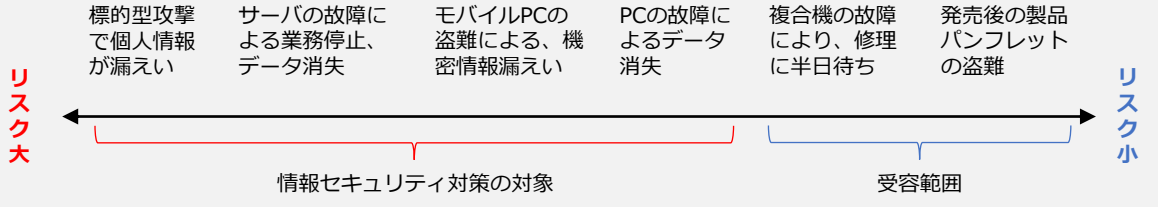
経営者が懸念する情報セキュリティの重大事故などを念頭に、何を起こさないようにするべきかを考えます。このとき、以下のような状況を併せて考えることで、対応すべきリスクを把握します。

- ✓ 関連する業務や情報に関わる外部状況（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）

（例）
- 個人情報保護法への対応
- 取引先のセキュリティに対する要求への対応
- テレワーク時のセキュリティ対応
- 報道されている新たなサイバー攻撃への対応

2. 対策の決定

すべてのリスクに対応しようとすると、対策費用が高額になったり、業務に支障をきたしたりする場合があります。そこで、いつ事故が起きてもおかしくない、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。また、事故が起きる可能性が小さい、発生しても被害が軽微であるなど、リスクが小さなものは、現状のまま受容するなど、合理的に対応します。



12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（8/8）

3. 規程の作成

「2. 対策の決定」で情報セキュリティ対策の対象としたリスクに対して対策を実施するため、文書化した規程を作成します。「中小企業の情報セキュリティ対策ガイドライン 付録5情報セキュリティ関連規程（サンプル）」を編集することで、規程を作成することができます。以下では、「サーバの故障による業務停止、データ消失」に対する対策を文書化した規程の例を記載します。赤文字の箇所を修正することで、自社に適した規程を作成します。

3	情報資産管理	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

バックアップ

バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的に取得する。

機器名	対象	方法	保管先
ファイルサーバ	ユーザーファイル	アプリケーションバックアップ機能	NASサーバ
Webサーバ	ホームページ	同期ツール	NASサーバ
会計システム	アプリケーションデータ	アプリケーションバックアップ機能	クラウドバックアップサービス

バックアップ媒体の取扱い

バックアップに利用した機器および媒体の取扱いは以下に従う。

<保管>

- NASサーバ：施錠つきサーバラックに収納

情報セキュリティ関連規程の一例
(出典) IPA「情報セキュリティ関連規程（サンプル）」を基に作成

3	情報資産管理	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

バックアップ

バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的に取得する。

機器名	対象	方法	保管先
DBサーバ	取引先に関するデータ	アプリケーションバックアップ機能	自社サーバ
Webサーバ	ホームページ	同期ツール	自社サーバ
発注管理システム	アプリケーションデータ	アプリケーションバックアップ機能	クラウド上のサーバ

バックアップ媒体の取扱い

バックアップに利用した機器および媒体の取扱いは以下に従う。

<保管>

- 自社サーバ：ハウジングサービスを利用し、サービス事業者の施設内に保管する

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

第13章. ISMSの要求事項と構築（LV.3 網羅的アプローチ）

13-1. 【LV.3 網羅的アプローチ】の概要

13-2. 【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

章の目的
第13章では、情報セキュリティマネジメントシステム（ISMS）のフレームワークを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成する網羅的アプローチについて理解することを目的とします。

主な達成目標
◘ 網羅的アプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

13-1-1. LV.3 網羅的アプローチ

網羅的アプローチでは、フレームワークとしてISMSを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成します。第13章では、ISMSにおけるPDCAサイクルを回すために重要となるドキュメントの作成方法や、実施すべき事項について焦点を当てて説明していきます。

ISMSの要求事項に関連するドキュメント作成は重要ですが、あくまで手段であり目的ではありません。ドキュメントの作成と維持が目的化してしまうと、ドキュメントが形骸化し、情報セキュリティ対策としての意味がほとんどなくなってしまう場合があります。**ドキュメントを精細に作り込むことより、ISMSマネジメントプロセスを取り入れ、PDCAサイクルを回していくことが大切です。**ISMSに取組み始めたときには理解できていても、ドキュメント作りを始めるとドキュメント作成が目的になってしまうケースが多いため、注意が必要です。

LV.3 網羅的アプローチ（網羅性のあるアプローチ方法）

概要
網羅的なフレームワークとしてISMSを参考にします。ISMSのフレームワークに沿うため、技術的対策といった一部の内容に限らず、運用や監査についても含めて対策基準、実施手順を策定します。

メリット
- ISMS要求事項の導入が可能です。

デメリット
- 時間とコストがかかる。

13-2-1. ISMSの概要（確立・運用・監視）

ISMSの確立、運用、監視

「第7章. セキュリティフレームワーク」でも記載した通り、ISMSはPDCAサイクルに則って運用することとなります。PlanでISMSを確立し、Doで導入および運用、Checkで監視および見直し、Actで維持および改善を行います。ISMSの取組みで、組織の情報セキュリティをより良くするために管理手段レベルでの解決を目指すことになります。同じ失敗を繰り返さない、あるいは現状を改善し続けるために、PDCAサイクルによって継続的な改善を図ることが重要です。

本テキストでは、網羅的アプローチとして必要なドキュメントや項目を抜粋し、詳細に説明していきます。なお、ISMSの要求事項を定めているISO/IEC 27001の1から3はそれぞれ「1.適用範囲」「2.引用規格」「3.用語および定義」なので、実質的な要求事項は「4. 組織の状況」から「10. 改善」までの7項目となっています。

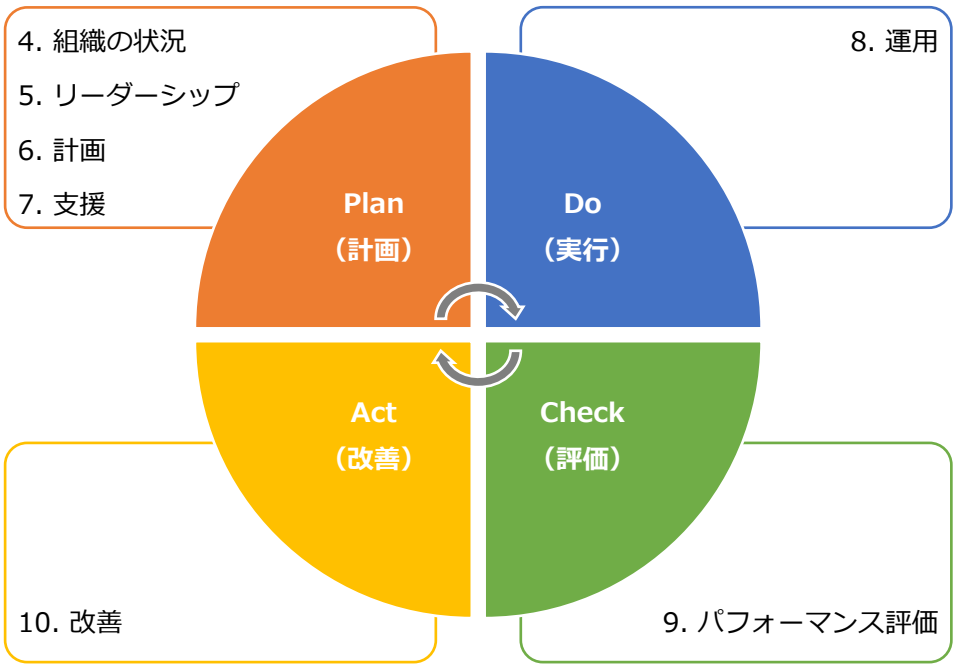
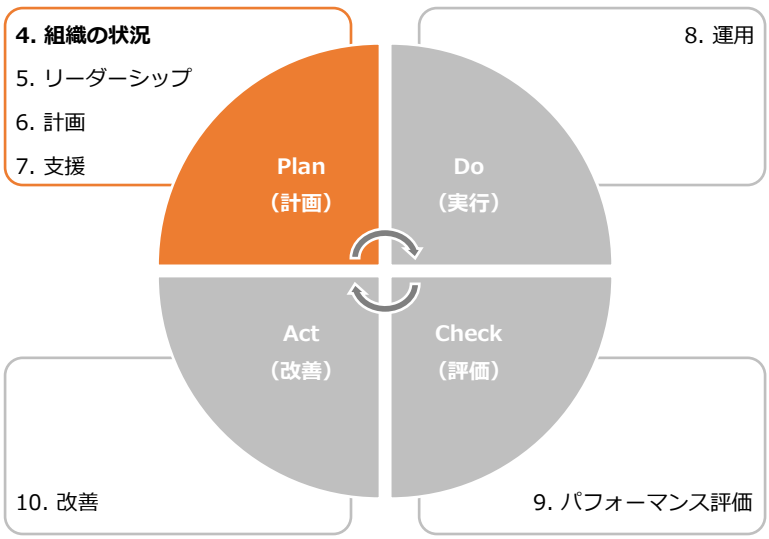


図53. ISO/IEC 27001のPDCAサイクル

13-2-2. ISMS：4. 組織の状況

ISMS構築の第一歩は、組織の状況を把握することにあります。 組織が抱えている情報セキュリティ上の課題を明らかにするとともに、組織の利害関係者が情報セキュリティに関してどのようなニーズや期待を持っているのかを整理し、情報セキュリティに取組む意義を確認します。それを踏まえて、「ISMSの適用範囲」を決定することになります。この「4.組織の状況」は、PDCAサイクルの「Plan（計画）」に位置していますが、組織の内外の状況に応じて見直す必要があります。

4. 組織の状況	作成ドキュメント（例）
4.1 組織及びその状況の理解 ISMSを構築することで解決したい課題（組織の目的に関連する内部課題、外部課題）を明確にします。	• 外部および内部の課題
4.2 利害関係者のニーズ及び期待の理解 ISMSに関係する利害関係者（顧客、従業員、取引先など個人や組織）と、利害関係者から要求される情報セキュリティに関係する要求事項を明確にします。	• 利害関係者のニーズ及び期待
4.3 情報セキュリティマネジメントシステムの適用範囲の決定 決定された外部課題・内部課題、利害関係者の要求事項と、業務内容や他の組織との情報のやり取り、ネットワーク構成などを考慮し、ISMSの適用範囲を合理的に決定します。	• ISMS適用範囲 • レイアウト図 • ネットワーク図
4.4 情報セキュリティマネジメントシステム 決定したISMSの適用範囲を対象に、PDCAサイクルに基づくISMSを構築・運用します。	ー



13-2-2. ISMS：4. 組織の状況

4.1 組織及びその状況の理解

作成するドキュメント
- 外部および内部の課題

「組織及びその状況の理解」では、組織を取り巻く外部と内部の課題を整理することが求められています。ここで整理した課題を、ISMSの取組みを通して解決していきます。また、組織のどの部分に対してISMSを適用すべきなのかといった適用範囲を確定する際にも、課題を考慮することとなります。

外部の課題

組織の外部に原因が存在する課題は、以下の情報をヒントに決定することができます。
- 国際、国内、地方または近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然および競争の環境
- 組織の目的に影響を与える主要な原動力および傾向
- 外部ステークホルダーとの関係並びに外部ステークホルダーの認知および価値観

（例）

課題	リスク	機会
個人情報、機密情報の保護（ウイルス感染、情報漏えい、新たな脅威への対応）	情報セキュリティ事故の発生 →信用低下	情報の活用

内部の課題

組織の内部に原因が存在する課題は、以下の情報をヒントに決定することができます。
- 統治、組織体制、役割およびアカウンタビリティ
- 方針、目的およびこれらを達成するために策定された戦略
- 資源および知識として見た場合の能力（たとえば、資本、時間、人員、プロセス、システムおよび技術）
- 情報システム、情報の流れおよび意思決定プロセス（公式および非公式の双方を含む。）
- 内部ステークホルダーとの関係並びに内部ステークホルダーの認知および価値観
- 組織文化
- 組織が採択した規格、指針およびモデル
- 契約関係の形態および範囲

（例）

課題	リスク	機会
ISMSに関する理解の促進	理解不足による情報セキュリティ事故	体勢強化
情報(紙、電子データ)の適切な取扱い	紛失、訪問先などで置忘れ →信頼喪失	信頼向上
ノウハウ、お客様より預かる機密情報などの保護	機密情報の漏えい、ノウハウの流出	ビジネス機会の拡大

13-2-2. ISMS：4. 組織の状況

4.2 利害関係者のニーズ及び期待の理解

作成するドキュメント
- 利害関係者のニーズ及び期待

「利害関係者のニーズ及び期待の理解」では、組織の利害関係者と、その利害関係者が要求する情報セキュリティに関する要求事項を明確化することが求められます。利害関係者には、顧客や従業員、取引先など、さまざまな個人や組織が含まれます。利害関係者に該当する範囲は広いため、組織が管理できる範囲で利害関係者からの要求事項を特定します。また、どの程度のセキュリティレベルで対策するのか、利害関係者とそのニーズから水準を設定することになります。

利害関係者のニーズ及び期待の記入例

利害関係者	情報セキュリティに関する要求事項	リスク	機会
取引先	適切な情報の取扱い	不適切な取扱いで信頼低下 →案件減少	適切な対応で信頼向上 →受注の維持/増加
	法令遵守	未遵守による信頼低下 →案件減少	遵守による信頼向上 →受注の維持/増加
株主	セキュリティインシデントの未然防止	セキュリティインシデントの発生 →ブランドイメージの低下	セキュリティインシデントの発生数減少 →ブランドイメージの向上
従業者	情報セキュリティに関する教育	機密情報/ノウハウの流出	組織の価値向上
	必要な情報へのアクセス	機密情報/ノウハウの流出	効果的・効率的な業務 →競争力アップ
	個人情報の保護	不適切な情報の取扱い →信頼低下	従業者から信頼向上 →人材の確保
国・自治体	法令・その他規範の遵守	セキュリティインシデント発生時の不適切な対応 →社会的信頼の低下	社会的信頼の向上

13-2-2. ISMS：4. 組織の状況

4.3 情報セキュリティマネジメントシステムの適用範囲の決定（1/3）

作成するドキュメント
- ISMS適用範囲
- レイアウト図
- ネットワーク図

ISMSの適用範囲は、必ずしも会社全体とする必要はありません。特に大企業の場合には、特定の業務や特定の部門に限定してISMSを構築することがあります。たとえば、ある取引先の要請によってISMSを構築する場合、その取引先と取引のある部門に適用範囲を限定するケースがあります。

中小企業の場合には、会社全体を適用範囲とすることが多いので、特段の理由がない限り、会社全体を適用範囲にするとよいでしょう。

「情報セキュリティマネジメントシステムの適用範囲の決定」では、ISMSを適用するところと、そうではないところの境界およびその適用される範囲内で、規格の要求事項がどのように適用できるかを決定するよう要求しています。規格などの要求事項によって定められる改善すべき範囲を、適用範囲と言います。

適用範囲の決定に際しては、考慮しないといけない3つの事項があります。2つはこれまでに説明した「外部および内部の課題」と「要求事項」です。もう1つは、「組織が実施する活動と、他の組織が実施する活動との間のインターフェースおよび依存関係」です。異なる部署や委託先など他の組織との業務プロセスにおける依存度を見ながら、適用範囲を広げるのか、分離しておくのかを検討することになります。

インターフェースおよび依存関係の記入例

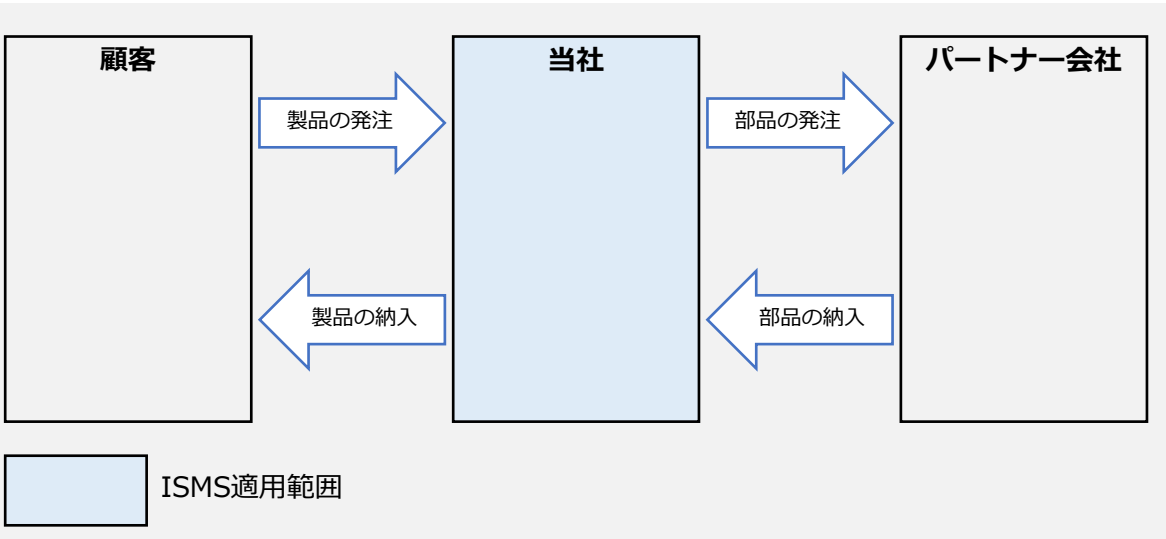


図54. インターフェースおよび依存関係の記入例

13-2-2. ISMS：4. 組織の状況

4.3 情報セキュリティマネジメントシステムの適用範囲の決定（2/3）

適用範囲を組織の一部とした場合、同じ組織内に適用範囲の内と外という境界ができることになります。適用範囲の境界について、いくつかの観点から明確にしておく必要があります。

人的・組織的境界

組織におけるどの人、どの部門が適用範囲の内側に該当するのかを明確にします。それにより、同じ社内の人であっても、適用範囲外の人を外部の人として扱うといった配慮が必要になる場合があります。

物理的境界

適用範囲とする建物や施設、部屋といった空間を明確にします。扉や壁、パーティションなどの物理的な境界によって仕切られていることが望ましいです。

技術的境界

ネットワークにおいて、対象とする範囲を明確にします。物理的境界と同様に、適用範囲のIT環境の境界を明らかにし、管理しなければならない情報システムや、ネットワークの対象や範囲を明確にする必要があります。

資産的境界

業務委託を受けていたり、組織の一部を適用範囲にしたりした場合に、資産的境界が生じる場合があります。顧客から情報や資源の提供を受けた際に、それを指定された管理方法で管理するのか、自組織の管理下となるのかといった場合や、適用範囲内の部門が保有する情報でも、組織全体で共有している場合にはどう管理するのかを明確にする必要があります。

事業的境界

事業（業務）においても対象を明確にします。事業は部門を横断する場合があるため、人的・組織的境界とも合わせて対象を検討し、適用範囲を明確にする必要があります。

13-2-2. ISMS：4. 組織の状況

4.3 情報セキュリティマネジメントシステムの適用範囲の決定（3/3）

物理的境界 レイアウト図（例）

物理的境界では、適用範囲とする空間を明確にし、境界線を記載します。そして境界線で区切られた空間ごとにセキュリティレベルを設定します。

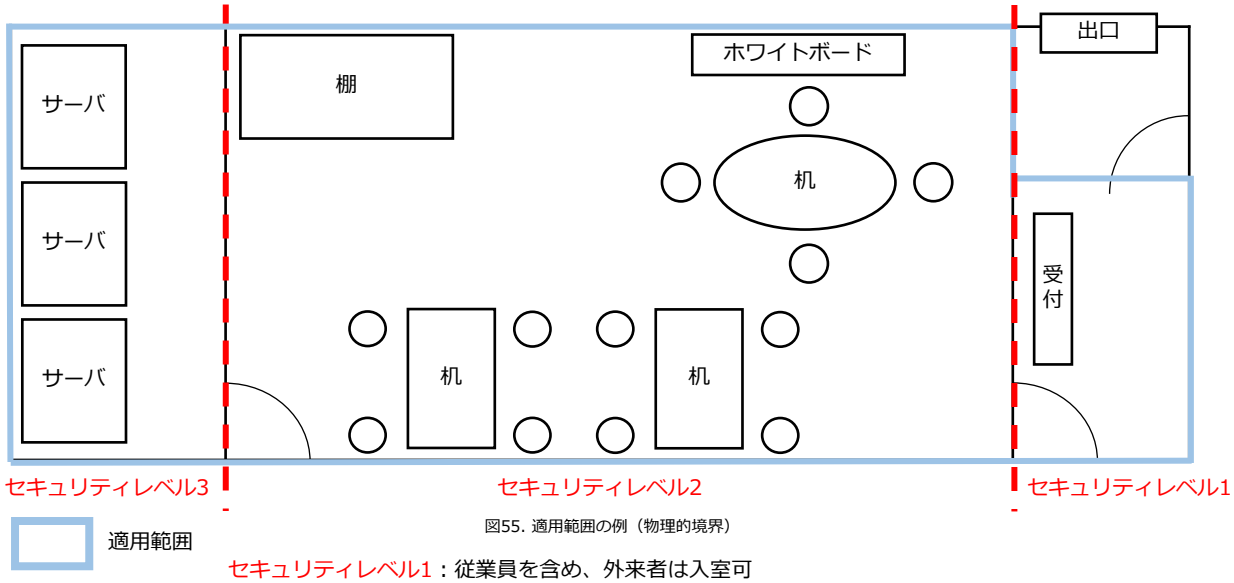


図55. 適用範囲の例（物理的境界）

セキュリティレベル1：従業員を含め、外来者は入室可
セキュリティレベル2：対象従業員のみ入室可（対象者以外は入退室管理が必要）
セキュリティレベル3：限られた人員のみ入室可（飲食禁止）

技術的境界 ネットワーク図（例）

ネットワークにおいて対象とする範囲を明確にするため、ネットワーク構成図を作成し、境界線を記載します。

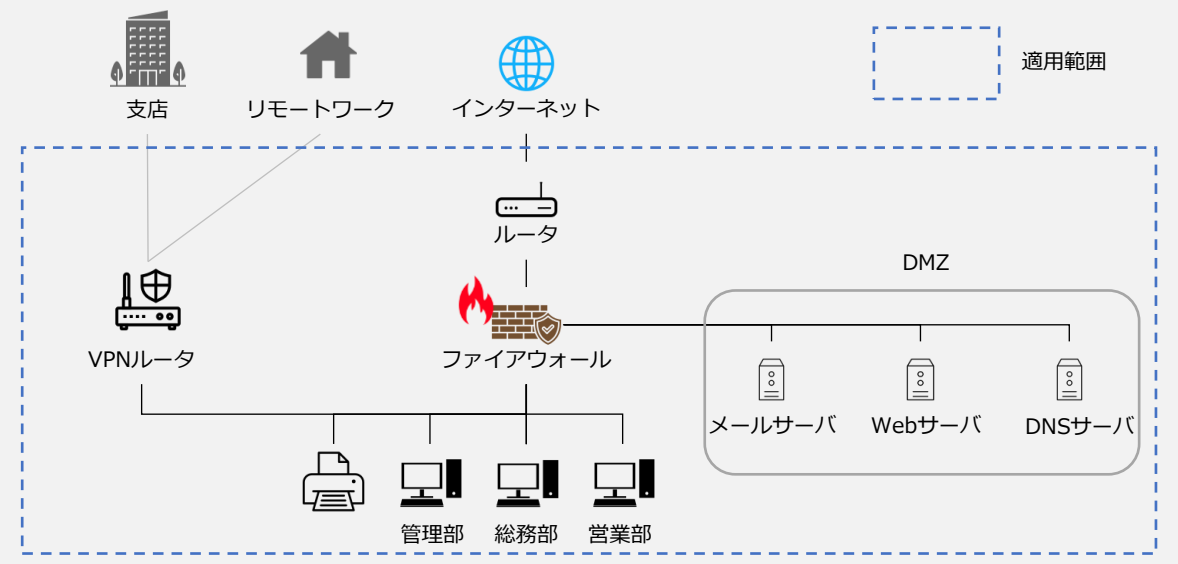
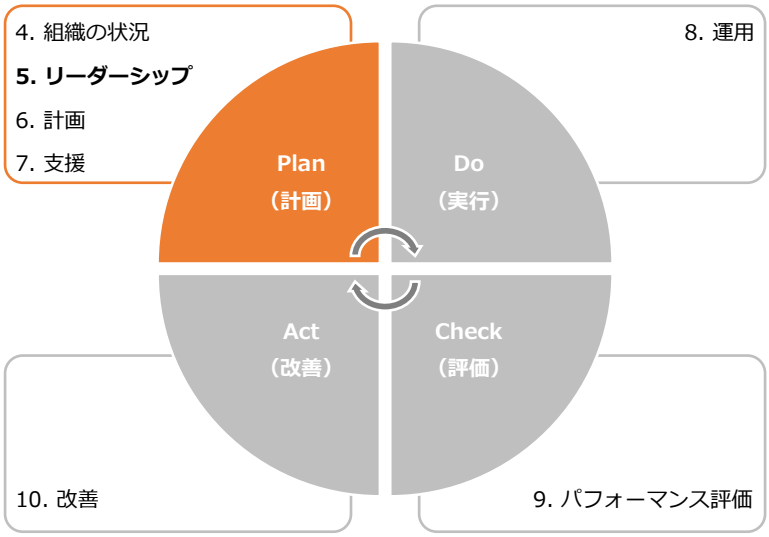


図56. 適用範囲の例（技術的境界）

13-2-3. ISMS：5. リーダーシップ

「5. リーダーシップ」は、PDCAサイクルの「Plan（計画）」に位置しており、トップマネジメントに求められる要求事項を示しています。トップマネジメントとは、ISMSの適用範囲における最高責任者のことを指します。多くの場合、トップマネジメントは、組織の社長が担う傾向にあります。「5. リーダーシップ」は、PDCAサイクルの軸であり、PDCAサイクルを回すには、トップマネジメントのコミットメント（関与、制約）が重要になります。

5. リーダーシップ	作成ドキュメント（例）
5.1 リーダーシップ及びコミットメント トップマネジメントが責任を持って実行しなければならない事項が記載されています。	ー
5.2 方針 トップマネジメントが、ISMSの目的や方向性、実施する内容について文書化し、「情報セキュリティ方針」を作成することを要求しています。	• 情報セキュリティ方針
5.3 組織の役割、責任及び権限 トップマネジメントは、ISMSを運用するために必要な役割や責任、権限を各要員に割り当て、どの要員がどのような役割や責任、権限を持っているかが分かる文書を作成することを要求しています。	• ISMSの運用組織図 • 責任者または部門の名称と役割を明記した文書



13-2-3. ISMS：5. リーダーシップ

5.1 リーダーシップ及びコミットメント

「リーダーシップ及びコミットメント」では、ISMSのトップマネジメントが責任を持たなければならないことを要求しています。トップマネジメントは、以下の事項について責任を持って必ず行う必要があります。

トップマネジメントが行う事項（要求事項）
情報セキュリティ方針および情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にする → 組織の事業の方向性に沿った情報セキュリティ方針と、情報セキュリティ目的を策定することを要求しています。※情報セキュリティ方針、情報セキュリティ目的については後述します。
組織のプロセスへのISMS要求事項の統合を確実にする → 自社の業務に、情報資産を管理する手順を組み込むことを要求しています。
ISMSに必要な資源が利用可能であることを確実にする → ISMSを構築・運用するために、必要な予算や人員など経営資源を確保しておくことを要求しています。
有効な情報セキュリティマネジメントおよびISMS要求事項への適合の重要性を伝達する → 従業員がISMSを構築・運用し、情報資産を適切に管理することの重要性を十分に認識できるよう、周知することを要求しています。
ISMSがその意図した成果を達成することを確実にする → ISMSを構築・運用することで得られる成果を明確にし、その成果を十分に得られるように取組んでいくことを要求しています。
ISMSの有効性に寄与するよう人々を指揮し、支援する → ISMSを構築・運用できるようにするため、従業者に対して教育を受けさせたり、定めた決まりを認識・実施させたり、従業員の意見を聞いたりするなど、サポートすることを要求しています。
継続的改善を促進する → ISMSを構築・運用するにあたり、従業員が不便に感じていることなど、改善が必要だと考えられる場合には、改善を進めるよう要求しています。
その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう、管理層の役割を支援する → 組織の規模や形態によって、トップマネジメントの指示が従業員に適切に伝わらない可能性があります。そのため、各部門の責任者が主導となり、従業員にトップマネジメントの指示を適切に伝え、ISMSを円滑に構築・運用できるようにすることを要求しています。

13-2-3. ISMS：5. リーダーシップ

5.2 方針

作成するドキュメント
- 情報セキュリティ方針

トップマネジメントは、組織の情報セキュリティに対する考え方や取組みの姿勢を利害関係者に示すため、情報セキュリティ方針を文書として作成し、組織内に周知するとともに、必要に応じて、その他の利害関係者が入手できるようにします。たとえば、保護するべき情報資産と保護すべき理由を明示し、利害関係者に周知します。

情報セキュリティ方針の作成方法

情報セキュリティ方針は、以下の事項を満たす必要があります。しかし、規格の内容をそのまま記載するのではなく、内容を理解した上で組織内部の従業員や、利害関係者にとって分かりやすい方針を作成する必要があります。

情報セキュリティ方針が満たさなければならない事項

a) 組織の目的に対して適切である
b) 情報セキュリティ目的を含むか、または情報セキュリティ目的の設定のための枠組みを示す
c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む
d) ISMS の継続的改善へのコミットメントを含む

a) 自社の経営理念に基づいた事業の目的や、情報セキュリティの必要性などを記載します。また、業務に関わる情報資産と、保護すべき理由などを記載します。

b) 情報セキュリティに関する目標を記載します。

情報セキュリティ方針（例）

【第X版】
【日付】
【社名】
【代表取締役社長　名前】

私たち【社名】は、【提供するサービス名】の提供を通じて、お客様、社員とその家族などすべてのステークホルダーの期待に応え、社会に貢献することを使命と考えています。

当社の事業活動において、お客様からお預かりする個人情報を含む多くの情報資産を活用しており、すべてのステークホルダーの期待に応えるためには、これらの情報資産を保護することは、経営上の最重要課題であると認識しています。

よって、私たちは、情報セキュリティ基本方針を策定し、本基本方針に基づいて、ISMSを構築・運用し、当社を取り巻く環境の変化を踏まえ、継続的改善に全社を挙げて取組むことをここに宣言します。

さらに、当社は、以下のセキュリティ目的を設定し、この目的を達成するための諸施策を確実に実施します。
✓ お客様との契約および法的または規制要求事項を尊重し遵守する。
✓ 情報セキュリティ事故を未然に防止する。
✓ 万一情報セキュリティ事故が発生した場合、影響を最小限にする。

以上

c) 自社の業務の特徴や課題を記載します。

d) ISMSに関する取組みを定期的に見直し、改善していく内容を記載します。

13-2-3. ISMS：5. リーダーシップ

5.3 組織の役割、責任及び権限

作成するドキュメント
- ISMS運用組織図
- 責任者または部門の名称と役割を明記した文書

「組織の役割、責任および権限」とは、ISMSを構築・運用するために、トップマネジメントが、組織内で役割を決め、責任と権限を割り当てることです。

ある程度の規模以上の組織になると、ISMSの実際の運用担当者や責任者は、トップマネジメントから権限を委譲された人になります。そうすると、情報セキュリティに関する取組みの実態を、トップマネジメントが十分把握していないという状況になりがちです。そうならないために、ISMSの実施状況をトップマネジメントに報告する仕組みやルールを作っておく必要があります。

ISMS運用組織図の作成方法（例）

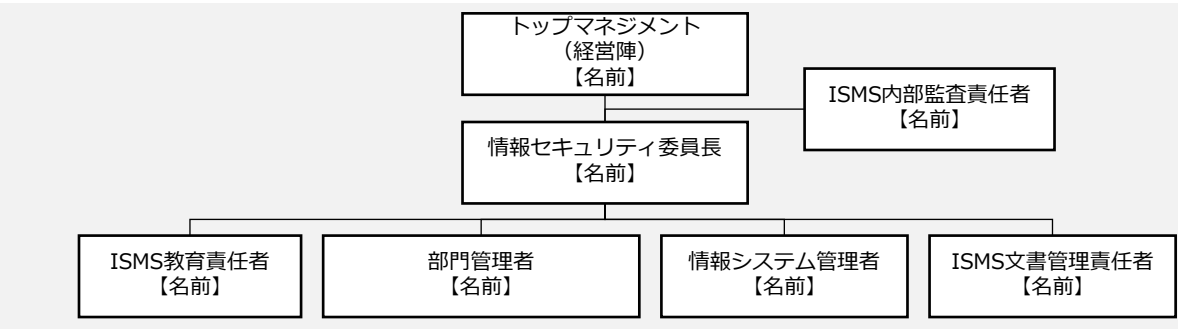


図57. ISMS運用組織図の例

ISMSの運用組織図を作成する流れを説明します。

1. トップマネジメントは、情報セキュリティ委員長を任命し、上記の事項に関する権限や責任を持たせる必要があります。そのため、トップマネジメントの下位に、情報セキュリティ委員長を配置します。
2. ISMS内部監査責任者は、内部監査を実施する際の最高責任者であり、トップマネジメントの下位に設置します。
3. 情報セキュリティ委員長は、ISMSの実施・運用のために必要な役割を持つ責任者を任命します。情報セキュリティ委員長の下位に各責任者を配置します。

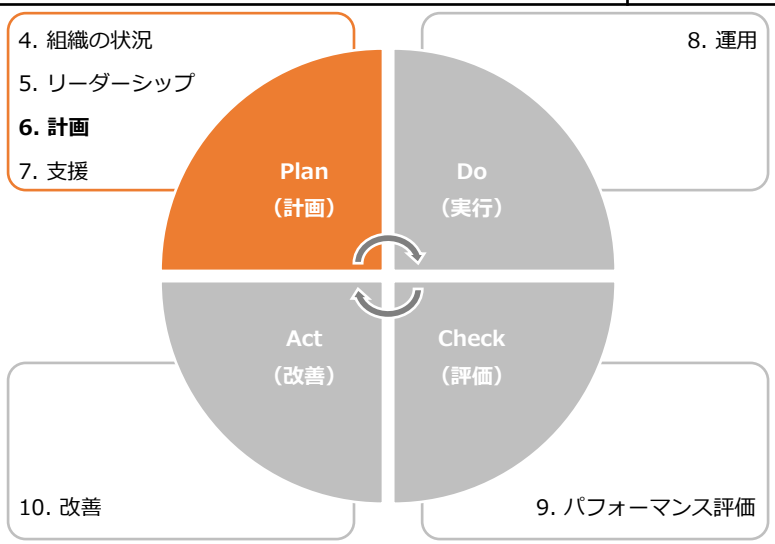
責任者または部門の名称と役割を明記した文書の作成方法（例）

名称	役割
情報セキュリティ委員長	ISMSの実施、運用について統括する
ISMS内部監査責任者	ISMSとその実施状況に関わる監査を統括する
ISMS教育責任者	ISMSに関する教育計画の立案と実施を行う
部門管理者(情報セキュリティ委員)	ISMS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程・規則に従い、ISMSを維持するための安全管理対策を実施する
ISMS文書管理責任者	ISMSに関する文書と記録などの維持・管理を行う

13-2-4. ISMS：6. 計画

「6. 計画」は、PDCAサイクルの「P（計画）」に位置しており、リスクマネジメントの確立、情報セキュリティにおけるリスクアセスメント、リスク対応、情報セキュリティ目的の管理に関する要求事項を示しています。

6. 計画	作成ドキュメント（例）
6.1 リスク及び機会に対処する活動 ① **一般** 特定した内外部の課題と、利害関係者のニーズおよび期待を考慮して、リスク・機会（期待する状況や結果）を決定し、対処するための活動を明確にすることを要求しています。 ② **情報セキュリティリスクアセスメント** 組織や企業の資産に対する、情報セキュリティリスクアセスメントプロセスの確立を要求しています。 ③ **情報セキュリティリスク対応** 情報セキュリティリスク対応の手順を確立することを要求しています。	• 資産目録（情報資産管理台帳） • リスクアセスメント結果報告書 • 適用宣言書 • リスク対応計画
6.2 情報セキュリティ目的及びそれを達成するための計画策定 情報セキュリティ目的を確立し、達成するための計画を策定することを要求しています。	• ISMS有効性評価表
6.3 変更の計画策定 ISMSの変更が必要なときは、計画的な変更を要求しています。	―



13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（1/9）

作成するドキュメント
- 資産目録（情報資産管理台帳）
- リスクアセスメント結果報告書

「リスク及び機会に対処する活動」とは、「ISMSの意図した成果を達成する」「ISMSの望ましくない影響を防止・低減する」「継続的改善を達成する」の3つを実現するために、妨げとなるような機会やリスクを発見し、対処することです。

平たく言えば、情報セキュリティ上のリスクに対して、適切な対策を講じることで、情報セキュリティを確保するための活動になります。

具体的には「リスクアセスメントの実施」「リスク対応策の作成と実施」「リスク対応策の有効性評価」「継続的改善」といった活動が含まれます。

リスクアセスメントは、組織や企業の資産に対するリスクの洗い出しや分析、評価を行い、リスク対応の優先順位づけをしていくプロセスになります。リスクアセスメントの実施により、リスクを評価し、事前にリスクを把握することで必要な投資額を含め、企業が適切な対策を検討することが可能になります。

情報セキュリティのリスク基準を確立し、維持する

リスクアセスメントを実施するにあたり、リスクの重大性を評価するための目安となるリスク基準を決める必要があります。ISMSでは、リスク基準に「リスク受容基準」と「情報セキュリティリスクアセスメントを実施するための基準」を含むように明示されています。
※「11-2-1. リスク基準の確立」を参照

情報セキュリティリスクを特定する

企業が掲げる目的・目標の達成を阻害する可能性のあるリスクをすべて洗い出すことです。そのため、リスクの発生可能性や影響の大きさを考慮せず、少しでも企業に影響を与えそうなリスクを洗い出すことが目的となります。リスク特定として最終的な成果はリスク一覧表の作成になります。
※「11-2-2. リスクの特定」を参照

情報セキュリティリスクを分析する

リスク特定で特定されたリスクに対して、リスク分析を行います。リスク分析を行うことで、「企業にとって対応が必要なリスクはどれか」、「優先的に対応しなければならないリスクは何か」といったことを判断します。リスク分析で求めた結果を、「リスクアセスメント結果報告書」に記載します。
※「11-2-3. リスクの分析」を参照

情報セキュリティリスクを評価する

リスク分析で算出したリスクレベルからリスク受容基準と比較し、リスク対策が必要かどうかを判断します。また、算出したリスクレベルをもとに優先順位をつけます。
※「11-2-4. リスクの評価」を参照

本項では、資産目録（情報資産管理台帳）とリスクアセスメント結果報告書を作成します。2つのドキュメントは、ISO/IEC 27001:2022の管理策「5.9 情報およびその他の関連資産の目録」に対応します。

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（2/9）

資産目録（情報資産管理台帳）の作成方法は「 11-2. リスクマネジメント：リスクアセスメント」で説明しました。作成した資産目録（情報資産管理台帳）から、リスクアセスメントの結果をまとめた「リスクアセスメント結果報告書」について説明します。

リスク特定における、リスクアセスメント結果報告書の作成方法（例）

以下の手順で、リスク一覧表となるリスクアセスメント結果報告書を作成します。

1. 資産目録（情報資産管理台帳）から、「情報セキュリティリスクアセスメントを実施するための基準」で決定した基準をもとに、重要資産を選択します。例では、機密性、完全性、可用性の項目の評価値が1つでも3となった資産を重要資産としています。選択した重要資産を「リスクアセスメント結果報告書」に記載し、リスク一覧表を作成します。

No	資産目録のNo	リスク特定				
		リスク源	影響領域	事象	原因	起こり得る結果
1	9	モバイル機器の利用ルールが十分に整備されていない	外部	持ち出し中に重要な情報を紛失・盗難(機密性の喪失)	【事象】に対し【リスク源】である	機密情報などが漏えいし、顧客に影響、信用喪失
2	40	教育が不十分なため従業者の意識が低い	全社	誤送信(機密性の喪失)	【リスク源】ため【事象】が発生	機密情報などが漏えいし、顧客に影響、信用喪失
3	10、11、13、26、55	電子の情報分類／取扱いが明確でない	外部	情報の紛失・盗難(機密性の喪失)	【リスク源】ため【事象】が発生	機密情報などが漏えいし、顧客に影響、信用喪失

リスクアセスメント結果報告書には、以下の内容を記載します。

- ✓ **資産目録のNo**
  作成した資産目録に対応する項番を記載します。
  ※リスクによっては資産目録のNoは複数になることもあります。
- ✓ **リスク源**
  想定される脅威を記載します。
  （例）モバイル機器の利用ルールが十分に整備されていない　など
- ✓ **影響領域**
  脅威が発生した場合の影響範囲を記載します。
  （例）外部、全社　など
- ✓ **事象**
  発生する可能性のある事象を記載します。
  （例）持ち出し中に重要な情報を紛失・盗難(機密性の喪失)　など
- ✓ **原因**
  事象が発生する原因を記載します。
  （例）【事象】に対し【リスク源】である、【リスク源】ため【事象】が発生　など
- ✓ **起こり得る結果**
  事象が発生した場合に起きる結果を記載します。
  （例）機密情報などが漏えいし顧客に影響、信用喪失　など

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（3/9）

リスク分析・リスク評価における、リスクアセスメント結果報告書の作成方法（例）

事象	原因	起こり得る結果	リスク分析			優先順位
			重要度	被害発生可能性	リスクレベル	
持ち出し中に重要な情報を紛失・盗難（機密性の喪失）	【事象】に対し【リスク源】である	機密情報などが漏えいし顧客に影響、信用喪失	3	2	6	2
誤送信（機密性の喪失）	【リスク源】ため【事象】が発生	機密情報などが漏えいし顧客に影響、信用喪失	2	2	4	3
情報の紛失・盗難（機密性の喪失）	【リスク源】ため【事象】が発生	機密情報などが漏えいし顧客に影響、信用喪失	3	3	9	1

具体的には、以下の内容を記載します。

✓ **重要度**
「機密性」「完全性」「可用性」いずれかの最大値で判断します。
（例）機密性：1、完全性：2、可用性：3 →　重要度：3
　　機密性：2、完全性：1、可用性：1 →　重要度：2

✓ **被害発生可能性**
脅威の起こりやすさと脆弱性のつけ込みやすさから換算表に当てはめて算出します。

被害発生可能性の換算表		つけ込みやすさ（脆弱性）		
		3	2	1
起こりやすさ（脅威）	3	3	2	1
	2	2	1	1
	1	1	1	1

起こりやすさ：2、つけ込みやすさ：1 → 被害発生可能性：1
起こりやすさ：3、つけ込みやすさ：3 → 被害発生可能性：3

✓ **リスクレベル**
重要度と被害発生可能性から算出します。
（例）重要度：3、被害発生可能性：1 →　リスクレベル：3
　　重要度：2、被害発生可能性：3 →　リスクレベル：6

✓ **優先順位**
リスク受容基準をもとに、リスクレベルから優先順位づけを行います。

（例）1：早急に対応、2：今期中に対応、3:：今期対応が望ましい
リスクレベル：9　→　優先順位：1
リスクレベル：4　→　優先順位：3
リスクレベル：6　→　優先順位：2

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（4/9）

作成するドキュメント
- リスクアセスメント結果報告書
- 適用宣言書
- リスク対応計画

リスクアセスメントにおいて、自社の情報セキュリティリスクを洗い出します。リスク対応では、洗い出したそれぞれのリスクに対してどう対策するのか、ISMSの管理策を実施の有無を含めて検討します。リスク対応は以下のプロセスになります。

リスク対応のプロセス

1.適切な情報セキュリティリスク対応の選択肢の選定
リスク対応の選択肢（リスクの回避、低減、移転、受容（保有））から選定する。
2.情報セキュリティリスク対応の選択肢の実施に必要なすべての管理策の決定
ISO/IEC 27001:2022の附属書A、ISO/IEC 27017などの管理策集から、リスクの回避、低減、移転、受容（保有）の中から選択したリスク対応に必要なすべての管理策を決定します。
3.決定した管理策とISO/IEC 27001:2022附属書A の管理策との比較
必要なすべての管理策を、ISO/IEC 27001:2022附属書Aに挙げられている管理策と比較します。
4.適用宣言書の作成
必要なすべての管理策と、その理由および実施状況を文書化します。適用宣言書に含まれるすべての管理策の実施状況は、“実施された”、“一部実施された”または“実施されていない”として記述できます。
5.情報セキュリティリスク対応計画
組織がリスクに対応する必要性を含んだリスク対応計画を作成します。リスク対応計画とは、組織のリスク受容基準を満たすようにリスクを修正するための計画のことです。 - 組織の必要な管理策を実施するためのプロジェクト計画 - リスクを修正するために管理策が環境と相互にどのように作用するかを記述した設計計画
6.リスク所有者による承認
リスク所有者は、リスク対応計画を承認します。
7.残留している情報セキュリティリスクの受容
リスク所有者は、残留リスクが受容可能かどうかを判断し、決定します。

本項では、リスクアセスメント結果報告書、適用宣言書、リスク対応計画とISMS有効性評価表を作成します。リスクアセスメント結果報告書は、リスクアセスメントで作成したドキュメントにリスク対応と二次評価を記載します。

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（5/9）

1.適切な情報セキュリティリスク対応の選択肢の選定

リスク対応には、以下の4つがあります。

リスク回避	リスクが発生する可能性のある環境を排除するなど、リスクそのものをなくそうとすることです。たとえば、個人情報を受け取らないようにしたり、その業務自体をやめたりするといった方法です。
リスク低減	セキュリティ対策（管理策）を採用することによって、リスクの発生確率を低くしたり、リスクが顕在化したときの影響の大きさを小さくしたりすることです。「軽減」「修正」と呼ばれることもあります。
リスク移転	リスクを他者に移して、自分たちの責任範囲外にしたり、リスクが顕在化したときの損失を他者に引き受けさせたりすることです。たとえばクラウドのサーバを利用することによって、サーバが破壊されたり、盗難されたりするリスクを移転することができます。「共有」と呼ばれることもあります。
リスク受容（保有）	対策を行わずにリスクを受け入れるということです。被害は大きいが発生可能性がほとんどない場合や、発生しても被害がほぼない場合が該当します。

2.選択肢の実施に必要なすべての管理策の決定

リスク対応を実施することが決まった場合は、管理策を決める必要があります。管理策は、リスクの回避、低減、移転、受容（保有）の中から選択したリスク対応に必要な管理策をすべて決定します。

リスク対応における、リスクアセスメント結果報告書の作成方法（例）

リスク対応した結果を、リスクアセスメント結果報告書に記載します。

起こり得る結果	リスク分析(一次評価)			優先順位	リスク対応					
	重要度	被害発生可能性	リスクレベル		保有	低減	回避	移転	管理策	対応
機密情報などが漏えいし顧客に影響、信用喪失	3	2	6	2		●			モバイル機器の利用ルールを整備・強化	
機密情報などが漏えいし顧客に影響、信用喪失	2	2	4	3		●			教育訓練	
機密情報などが漏えいし顧客に影響、信用喪失	3	3	9	1		●			• 情報の分類定義 • 分類ごとの情報の取扱いルール • ラベリング	

具体的には、以下の内容を記載します。

✓ **保有、低減、回避、移転**
リスク対応で決定した対応について「●」を記載します。

✓ **管理策**
リスク対応で決定した内容を記載します。
（例）モバイル機器の利用ルールを整備・強化　など

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（6/9）

3.決定した管理策とISO/IEC 27001:2022附属書A の管理策との比較

附属書Aは、ISO/IEC 27001で記載されている要求事項をもとに情報セキュリティ上のリスクを低減するための目的と、その目的を達成するための管理策で構成されています。ISO/IEC 27001:2022では、合計93種の管理策が、以下の4つのカテゴリに分類されています。

- 組織的管理策
- 人的管理策
- 物理的管理策
- 技術的管理策

リスク対応で決定した管理策を附属書Aと比較し、必要な管理策を見落としていないか確認します。附属書Aの管理策のリストは包括的なものではないので、必要に応じてリストにない管理策を採用してもかまいません。

（例）
リスクアセスメント結果報告書で記載の管理策：
- 情報の分類定義
- 分類ごとの情報の取扱いルール
- ラベリング

附属書Aに記載の管理策：
- 5.12 情報の分類
- 5.13 情報のラベル付け

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（7/9）

4.適用宣言書の作成

「適用宣言書」は、ISMS認証を取得するすべての組織に作成が義務づけられています。認証を取得しない組織では、 必須ではありませんが、情報セキュリティに対する取組みを明確にするために「適用宣言書」を作成することが望ましいとされています。

適用宣言書は以下の内容を含むように作成します。

- 必要な管理策
- それらの管理策を含めた理由
- それらの管理策を実施しているか否か
- 附属書Aに規定する管理策を除外した理由

管理目的および管理策			適用	実施・未実施	管理策を含めた理由 管理策を除外した理由	規程・手順書
5 組織的管理策						
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することが望ましい。	○	○	情報セキュリティのための経営層の方向性および支持を、事業上の要求事項、関連する法令および規則に従って規定するため	情報セキュリティ方針
5.2	情報セキュリティの役割および責任	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、割り当てることが望ましい。	○	○	ISMSの構築・運用を円滑に行うため	情報セキュリティ手順書
5.3	職務の分離	相反する職務および責任範囲は、分離することが望ましい。	○	○	許可されていないもしくは意図しない変更または不正使用の危険性を低減するため	情報セキュリティ手順書
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することが望ましい。	○	○	ISMSの取組みが、経営陣の経営戦略の一部であることを確実にするため	情報セキュリティ手順書
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することが望ましい。	○	○	セキュリティインシデントが発生したことを迅速に報告するため	情報セキュリティ手順書
…	…	…	…	…	…	…

適用宣言書には、以下の内容を含めます。

✓ **管理目的および管理策**
ISO/IEC 27001の附属書Aの管理策を記載します。
（例）5.1 情報セキュリティのための方針群　など

✓ **適用**
適用または適用除外を記載します。
（例）○：適用、×：適用除外

✓ **実施・未実施**
実施したか否かを記載します。
（例）○：実施、未：未実施、ー：適用除外

✓ **管理策を含めた理由または管理策を除外した理由**
管理策を行う場合も理由を記載します。
（例）情報セキュリティのための経営層の方向性および支持を、事業上の要求事項、関連する法令および規則に従って規定するため など

✓ **規程・手順書**
管理策が含まれている規程または手順書を記載します。
（例）情報セキュリティ手順書5.1.1、A-02 情報セキュリティ方針　など

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（8/9）

5.情報セキュリティリスク対応計画

「リスク対応計画」は、それぞれのリスクに対して、どのような管理策を、誰が、いつまでに、どのように実施するのかを表にまとめたものになります。表には、対策の実績やステータスを記載する欄もありますが、これらの欄については「8. 運用」で説明します。

リスク対応計画の作成方法（例）

リスクアセスメント結果報告書から、リスク対応を行う管理策をすべて記載し、それぞれの具体的な内容や、担当者などを記載します。リスク対応を行った場合、実績やリスク対応のステータスを記載する必要があります。
※実績とステータスは、「8.運用」で記載します。

No	管理策	タスク	担当	予定		実績		ステータス
				開始	終了	開始	終了	
1	モバイル機器の利用ルールを整備・強化	• ルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-			
2	教育訓練	• ルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-			
3	• 情報の分類定義 • 分類ごとの情報の取扱いルール • ラベリング	• 情報の分類定義 • 分類ごとの取扱いルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-			

リスク対応計画では、以下の内容を記載します。

✓ **管理策**
リスクアセスメント結果報告書の管理策を記載します。
（例）モバイル機器の利用ルールを整備・強化　など

✓ **タスク**
管理策を実施する上で、具体的な業務を記載します。
（例）ルール検討
　　関係者に周知

✓ **担当**
管理策の担当者を記載します。
（例）委員長

✓ **予定**
リスク対応予定の開始日と終了日を記載します。
（例）開始：2023/08/10
　　終了：2023/09/29

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（9/9）

二次評価

「二次評価」とは、リスクに対する管理策の有効性評価のために行うものです。
リスク対応を実施した結果は、二次評価としてリスクアセスメント結果報告書に記載します。リスク分析で使用した値を用いて、リスク対応を実施した結果をもとに、情報資産に対する再評価を実施します。

リスク対応における、リスクアセスメント結果報告書の作成方法（例）

優先順位	リスク対応						二次評価		
	保有	低減	回避	移転	管理策	対応	重要度	被害発生可能性	リスクレベル
2		●			モバイル機器の利用ルールを整備・強化	済	2	1	2
3		●			教育訓練	済	1	1	1
1		●			情報の分類定義 分類ごとの情報の取扱いルール ラベリング	済	2	3	6

具体的には、以下の内容を記載します。

- ✓ **重要度（係数）**
  「機密性」「完全性」「可用性」いずれかの最大値で判断します。
  （例）機密性：1、完全性：2、可用性：3 →　重要度：3
  　　機密性：2、完全性：1、可用性：1 →　重要度：2
- ✓ **被害発生可能性**
  脅威の起こりやすさと脆弱性のつけ込みやすさから換算表に当てはめて算出します。
  （例）起こりやすさ：2、つけ込みやすさ：1 → 被害発生可能性：1
  　　起こりやすさ：3、つけ込みやすさ：3 → 被害発生可能性：3
- ✓ **リスクレベル**
  重要度と被害発生可能性から算出します。
  （例）重要度：3、被害発生可能性：1 →　リスクレベル：3
  　　重要度：2、被害発生可能性：3 →　リスクレベル：6

6.リスク所有者による承認/7.残留している情報セキュリティリスクの受容

リスク対応計画と残留リスク（管理策の適用後に）は、リスク特定で決めたリスク所有者の承認が必要になります。リスク所有者が承認する際は、記録をする必要があるため、ワークフローやチェック欄などを用います。

（例）
承認プロセスとして、作成した書類にチェック欄（電子印欄など）を作成します。

作成者／更新者	【名前】	作成日／更新日	【日付】
承認者	【名前】	承認日	【日付】

作成	承認

13-2-4. ISMS：6. 計画

6.2 情報セキュリティ目的及びそれを達成するための計画策定

作成するドキュメント
- ISMS有効性評価表

情報セキュリティ目的の基本要件として以下の要件を満たす必要があります。

a. 情報セキュリティ方針と整合
b. 測定可能
c. 適用される情報セキュリティ要求事項、並びにリスクアセスメントおよびリスク対応の結果を考慮
d. 伝達すること
e. 必要に応じて、更新すること

情報セキュリティ目的と、それを達成するための計画をISMS有効性評価表に記載します。「8. 運用」で計画を実施し、「9. パフォーマンス評価」で評価を行います。評価結果の記載方法は、「9. パフォーマンス評価」で説明します。

ISMS有効性評価表の作成方法（例）

【計画】
情報セキュリティ目的：
・お客様との契約および法的または規制要求事項を尊重し遵守する
・情報セキュリティ事故を未然に防止する
・情報セキュリティ上の脅威から情報資産を保護する
・当社ISMSの意味を理解した活動の開始

評価指標：
ISMS教育受講／合格　100%(全従業者)
【備考】
取組みの初年度であるため、全従業者が活動に関与、さらには、活動を理解し、全社のセキュリティ目的の達成に向けた活動開始ができたことを確認する。

情報セキュリティ目的達成のための計画

実施事項	必要な資源	責任者	達成期限	評価方法
教育による活動の意味の理解	適用範囲の従業者がISMS教育を受講	ISMS事務局長	20XX年-月	受講者数および合格者数をカウントし、評価する

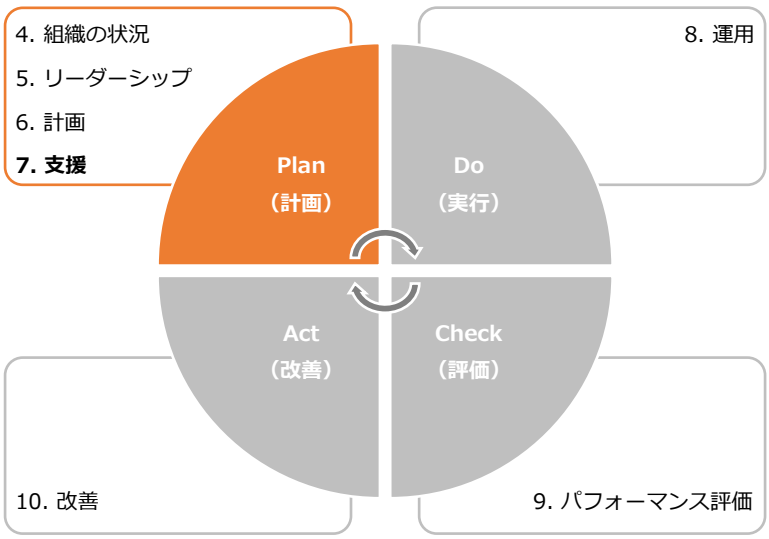
ISMS有効性評価表では、以下の内容を記載します。

- **情報セキュリティ目的**
  適用範囲（組織全体、各部署ごと）でのセキュリティ目的を記載します。
  （例）
  重大なセキュリティインシデントを発生させない、マルウェア感染およびサイバー攻撃によるシステム停止の防止　など
- **評価指標**
  測定可能な値を記載します。
  （例）マルウェアの感染の有無、システム停止の有無　など
- **実施事項**
  情報セキュリティ目的を達成するための実施内容を記載します。
  （例）ウイルス対策ソフトのインストール、標的型メール訓練の実施　など
- **必要な資源**
  実施事項のために必要な資源を記載します。
  （例）ウイルス対策ソフト、標的型メール訓練　など
- **責任者**
  計画の責任者を記載します。
  （例）部長各自　など
- **達成期限**
  計画の期限を記載します。
  （例）年度末、2023年9月　など
- **評価方法**
  具体的な評価方法を記載します。
  （例）年度末に発生したセキュリティインシデントをカウントし、評価する　など

13-2-5. ISMS：7. 支援

「7. 支援」は、PDCAサイクルの「Plan（計画）」に位置しており、ISMSの運用をサポートするための要求事項が規定されています。

7. 支援	作成ドキュメント（例）
7.1 資源 ISMSに必要な資源（人、物、金、情報）を決定し、提供します。	ー
7.2 力量 ISMS適用範囲の要員に求められる力量（知識、技能など）を定義し、要員が力量を備えているか評価を行います。力量評価の結果、力量が不足している場合は、力量を身につけるための教育を計画し、実施します。教育の実施後、力量を取得・維持できたか確認テストを行います。最後に、実施した教育内容を記録として保持します。	• 力量確認表 • 教育計画書 • 理解度確認テスト • 教育実施記録
7.3 認識 ISMS適用範囲のすべての要員に、以下の内容を認識させる必要があります。 ・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るメリットや、自身の業務とISMSの関係、実施すべきセキュリティ対策 ・ISMSによって割り当てられた責任を果たさなかった際の影響	ー
7.4 コミュニケーション ISMSを運用するにあたり、必要な意思疎通ができるプロセスを確立する必要があります。	ー
7.5 文書化した情報 ISMSに必要な文書化した情報の作成、更新、管理についての要求事項が記載されています。	**ー**



13-2-5. ISMS：7. 支援

7.1 資源

ISMSのPDCAサイクルを回すために必要な資源を決定し、利用できるようにする必要があります。必要な資源を決定し提供することは、トップマネジメントが行う必要があります。（リーダーシップ及びコミットメントの箇所で要求されています。）

ISMSのPDCAサイクルを回すために必要となる資源を決定し、提供する

資源の具体例を以下に示します。例を参考に、ISMSのPDCAサイクルを回すために自社で必要となる資源を決定し、利用可能にします。

資源	具体例
人	• ISMSを構築・運用するために必要となる要員 • ISMSの推進体制の確立 • 必要に応じた外部の専門家　など
物	• 情報を処理するための機器（サーバ、ネットワーク機器など） • コミュニケーション手段（パソコン、スマホなど） • 活動に必要な施設　など
金	• 人、物の資源を確保するための予算 • 要員の教育費用 • ISMSの維持費　など
情報	• 文書化した情報 • ISMSのPDCAサイクルを回すために有用な情報 • 情報セキュリティに関する最新情報　など

13-2-5. ISMS：7. 支援

7.2 力量（1/4）

作成するドキュメント
- 力量確認表
- 教育計画書
- 理解度確認テスト
- 教育実施記録

ISMS適用範囲の要員に必要な力量（知識、技能など）を明確にし、実際に要員が力量を備えているか評価を行います。力量が不足している場合、力量を身につけるための教育を計画し、実施する必要があります。教育の結果、力量が取得できたかを評価します。

力量確認表の作成方法（例）

要員の力量を評価し、確認するための力量確認表を作成する方法について説明します。

以下は、部門管理者の力量評価の例です。以下の手順で赤文字の箇所を自社の状況に合わせたものに修正することで、自社に適した力量確認表を作成できます。

1. 各要員ごとに、「組織の役割、責任及び権限」で割り当てられた役割や責任を果たすために必要となる力量を、「必要条件」として定義します。
2. 責任者として任命できるかどうか判断するための任命基準を定義します。
3. 定義された力量をどれほど備えているか、評価基準を決めて評価を行います。
4. 評価の結果、力量が不足している場合は教育・訓練を実施します。
5. 教育・訓練の実施後、どれほど改善できたか評価を行い、任命基準をもとに責任者として任命できるか判断します。

役　割	部門管理者
氏　名	○○ ○○

任命基準	A	B	C
区分	任命可	改善確認後任命可※	任命不可 再任命

A：項目のすべてが"3"以上。
B：項目の"2"以下について改善の予定がある。
C：項目の"2"以下について改善の予定がない。

※改善確認までは暫定的に任命し、改善確認後に正式任命とする

	必要条件	評価	改善予定日	改善内容	改善後評価	改善確認日
1	情報セキュリティ基本方針および社内の規程、基準などに精通していること	2	20XX/-/-	ISMS構築作業を通して獲得	3	20XX/-/-
2	ISMSに関する知識があること	2	20XX/-/-	ISMS構築作業を通して獲得	3	20XX/-/-
3	情報セキュリティ全般に関する知識があること	2	20XX/-/-	ISMS構築作業を通して獲得	3	20XX/-/-
4	公正な判断ができること	5				

評価基準	内容
5	十分な力量がある。指導・教育ができる
4	力量がある。支援なしに対応ができる
3	力量がある。他の支援により対応ができる
2	改善の余地がある
1	改善が必要

13-2-5. ISMS：7. 支援

7.2 力量（2/4）

教育計画書の作成方法（例）

力量評価の結果をもとに、必要な力量を身につけるための教育を計画します。以下の例をもとに、教育計画書の作成方法を説明します。

教育目的	ISO27001認証取得のため
教育対象者	全従業者
教育方法	方法：eラーニングによる自己学習、確認テスト。 委員会より、受講対象者に受講案内のメールを送付。 受講者は、案内にあるURLからeラーニングのシステムにアクセスし、受講(テキストのダウンロード)／確認テストを行う。
教育内容	ISMSに対する意識向上 ・　当社の方針や手順について（情報セキュリティ基本方針など） ・　ISMSの有効性に対する自らの貢献 ・　ISMS要求に適合しないことの意味 ・　当社のルールの遵守
実施期間	20XX年-月-日(-)～20XX年-月-日(-)
教育の有効性評価	情報セキュリティハンドブックを用いて教育を実施。 教育終了後、アンケート／確認テストを実施し記録に残す。 確認テストは、合格点は100点以上とする。 確認テストは、合格点に達するまで繰り返す。

教育計画書には、以下の内容を含めます。

✓ **教育目的**
教育を実施する目的を記載します。

✓ **教育対象者**
教育を受ける対象者を記載します。

✓ **教育方法**
教育・訓練方法は、集合研修や、職場訓練（OJT）、資格試験の受験、eラーニングなどさまざまあります。必要な力量を身につけるために適切と考えられる方法を選択します。

✓ **教育内容**
どのような教育を実施するのか、教育内容を記載します。

✓ **実施期間**
教育を実施する期間を記載します。

✓ **教育の有効性評価**
必要な力量を身につけることができたか評価する方法を記載します。
明確に評価が可能であれば、どのような方法でも問題ないです。たとえば、テストやアンケートの実施が挙げられます。次のページでテストの作成方法について説明します。

13-2-5. ISMS：7. 支援

7.2 力量（3/4）

理解度確認テストの作成方法（例）

教育の実施後、必要な力量を身につけることができたか評価するため、教育内容に関するテストを行うことが有効です。テストは、理解度が点数という数値で可視化されるため、評価がしやすく、多くの企業が実施しています。テストの作成例は以下の通りです。

次の【　　】に入る言葉として最も適したものを選びなさい（各10点）

設問			答え
①【　　】とは、ISMSを構築・運用するための国際規格である。			C
A. ISO9001	B.ISO14001	C.ISO27001	
② 情報セキュリティという言葉は、一般的に、情報の【　　】、完全性、可用性を維持改善することと定義されている。			C
A. 信頼性	B.整合性	C.機密性	
③ 2023年度の当社の情報セキュリティ目標は、【　　】である。			A
A.ISMS教育受講／合格　100%(全従業者)	B.予防処置の発行件数を四半期に1件以上	C.セキュリティインシデント発生件数／2件以内	
④【　　】とは、企業や個人の情報を盗みとるため、特定の相手（企業組織や社員）をメールなどの手段で狙う攻撃のことです。			A
A. 標的型攻撃	B. ウイルス型攻撃	C. サイバー攻撃	
⑤ ④【　　】メールの特徴はどれか。			B
A. 支払う必要がない料金を振り込ませるために、債権回収会社などを装い無差別に送信される。	B. 件名や本文に、組織の担当者の業務に関係する内容が記述されている。	C. 偽のホームページにアクセスさせるために、金融機関などを装い無差別に送信される。	

次の文章のうち正しいものには○、間違っているものには×をつけなさい（各10点）

設問	答え
⑥ ISMSでは、情報資産とは、書類、データだけでなく、ハードウェア、ソフトウェア、設備、ファームウェア（媒体など）、要員までも包括する。	○
⑦ 私物の外部記録媒体(USBメモリ、外づけHDDなど)の使用は原則禁止である。	○
⑧ 当社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情報を社外へ持ち出す場合は、責任者の許可を得て、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。	○
⑨ PCのログインパスワードは英数混合8文字以上のパスワードとする。	○
⑩ PCのパスワードつきスクリーンセーバーの設定時間は、15分以内とする。	×

実施日：	
所属：	
氏名：	
点数：	点/100点

✓ テストは、選択問題や正誤形式にすることで採点がしやすくなります。
✓ 教育内容に合った問題を考え、作成します。たとえば、今回の教育内容に「当社のルールの遵守」が含まれているため、⑥～⑩のような設問を作成します。

13-2-5. ISMS：7. 支援

7.2 力量（4/4）

教育実施記録の作成方法（例）

教育を実施した際、実施記録を文書化する必要があります。以下の例をもとに、教育実施記録の作成方法を説明します。

教育の名称	ISMS教育（基本方針、目標、ルール）
実施期間	20XX年-月-日(-)～20XX年-月-日(-)
実施方法	eラーニング
使用テキスト	情報セキュリティハンドブック
教育の概要	情報セキュリティハンドブックなどによるISMSに対する意識向上 ・当社の方針や手順について（情報セキュリティ基本方針など） ・ISMSの有効性に対する自らの貢献 ・ISMS要求に適合しないことの意味 ・当社のルールの遵守 学習後にテスト実施
受講対象者・部門	上記教育実施期間において在籍する全従業者
参加者	別紙：「教育受講者一覧」を参照
備考	特になし

教育実施記録には、以下のような内容を含めます。

✓ **教育の名称**
どのような教育を実施したのか、教育テーマを記載します。

✓ **実施期間**
教育を実施する期間を記載します。

✓ **教育方法**
教育・訓練方法は、集合研修や、職場訓練（OJT）、資格試験の受験、eラーニングなどさまざまあります。その中で、実際に実施した方法を記載します。

✓ **教育の概要**
実施した教育の概要や、教育を実施した目的を記載します。

✓ **受講対象者・部門**
教育を受講する対象者を記載します。

✓ **参加者**
教育を実際に受講した者を記載します。以下の例のように、「教育の受講者一覧」を別紙で作成し、実施記録と分けて記載すると分かりやすくなります。

No	所属	氏　　名	受講日
1	営業	○○○○	20XX/-/-
2	管理	○○○○	20XX/-/-

13-2-5. ISMS：7. 支援

7.3 認識

ISMS適用範囲で働くすべての社員、従業員が情報セキュリティ方針を理解し、それを実現することの重要性を認識する必要があります。逆に、セキュリティ対策を実施せず、セキュリティ方針を実現できなかった場合、どのようなことが起きるのかについて理解する必要もあります。

具体的には、以下の内容について教育を行い、ISMSの重要性を十分理解させる必要があります。

- **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るメリットや、自身の業務とISMSの関係、実施すべきセキュリティ対策の具体的な内容**
- **ISMSによって割り当てられた責任を果たさなかった場合の組織に与える影響**

これらの内容について認識を持たせるために、教育や訓練を実施します。
具体的な教育・訓練の実施手順は、「力量」や「コミュニケーション」で説明します。

力量

上記の内容について、各要員が認識しているか評価を行い、認識が不十分の場合は教育を実施し、認識させます。

コミュニケーション

情報提供・共有によって、上記の内容の認識を深めるようにします。

13-2-5. ISMS：7. 支援

7.4 コミュニケーション

ISMSのPDCAサイクルを回すためには、内部および外部とのコミュニケーションを円滑に行う必要があります。そのため、組織内および組織外の関係者とコミュニケーションをとる手順などを定め、必要なときに円滑なコミュニケーションが行える体制を整えておくことが重要です。コミュニケーションの手順などには、以下の内容が含まれます。

- コミュニケーションの内容
- コミュニケーションの実施時期
- コミュニケーションの対象者
- コミュニケーションの方法

ISMSに関連するコミュニケーションをとる手順を確立した例を、以下に示します。例を参考に、自社のISMSのPDCAサイクルを回す上で必要なコミュニケーションをとる手順を確立します。

内容	実施時期	対象者	実施者	方法
情報セキュリティ方針の伝達	随時	利害関係者	トップマネジメント（ISMS事務局）	外部 ・当社HPに公表 内部 ・ISMS定期教育にて ・当社HPに公表 ・社内掲示
各見直し結果の伝達	見直後、 1週間以内	従業者	ISMS事務局	承認後、ISMS事務局より通達
セキュリティ調査結果の報告	依頼入手時	お客様	ISMS事務局	・お客様より調査票などを入手した場合、主管部門にて回答を作成 ・ISMS事務局責任者が確認の上、お客様に提出
セキュリティインシデントの伝達	発見時	ISMS事務局	発見者	「情報セキュリティ手順書：セキュリティインシデント対応フロー」の通り
	適時	トップマネジメント	ISMS事務局	同上
	適時	関係当局	ISMS事務局	同上

✓ **内容**：コミュニケーションで伝える情報

✓ **実施時期**：伝えるタイミング

✓ **対象者**：誰に伝えるのか、情報を伝える対象者

✓ **実施者**：誰が伝えるのか、情報を対象者に伝える者

✓ **方法**：情報を伝える手段

13-2-5. ISMS：7. 支援

7.5 文書化した情報

ISMSに必要な文書化した情報の作成、更新、管理方法を決めます。

一般

以下の情報をISMSに含める必要があります。

- ISO/IEC 27001が要求する文書化した情報
- ISMSの有効性のために必要であると組織が判断した文書化した情報

以下は、ISO/IEC 27001が要求する文書化した情報の一覧です。

文書化した情報	作成する項番
ISMSの適用範囲	「4. 組織の状況」で作成
情報セキュリティ方針	「5. リーダーシップ」で作成
リスクアセスメントプロセスに関わる文書化された情報	「6. 計画」で作成
リスク対応プロセスに関わる文書化された情報	
情報セキュリティ目的に関わる文書化された情報	
力量の証拠	「7. 支援」で作成
組織が決めた文書化された情報	
ISMSのプロセス実施に関わる文書化された情報	「8. 運用」で作成
リスクアセスメントの結果	
リスク対応の結果	
監視・測定の結果	「9. パフォーマンス評価」で作成
監査プログラムの実施、結果に関わる文書化された情報	
マネジメントレビューの結果	
不適合の内容と処置、処置の結果	「10. 改善」で作成

作成および更新

ISMSに必要な文書化した情報を作成・更新する際に、以下の事項を確実にする必要があります。

1. 適切な識別と記述

文書化した情報を識別できるよう、以下の例のように採番方法を決めたり、各文書には適切なタイトル、作成者、承認者、日付などを記載したりします。

文書の種類	採番方法
基本文書	A-□□（01から採番を始める）
ISMSマニュアル	B-01
手順書	C-01
記録類	D-01
外部文書	採番せずに文書名、作成社名などの名称にて識別する

2. 適切な形式

文書化する情報を記載する媒体として、紙や電子データなどを指定し、適切な形式（文字、図表など）を用いて読みやすく、簡潔に記載します。

3. 適切なレビューと承認

文書化した情報は、適切な承認とレビューを行い策定します。

文書化した情報の管理

ISMSの文書化した情報を管理する必要があります。

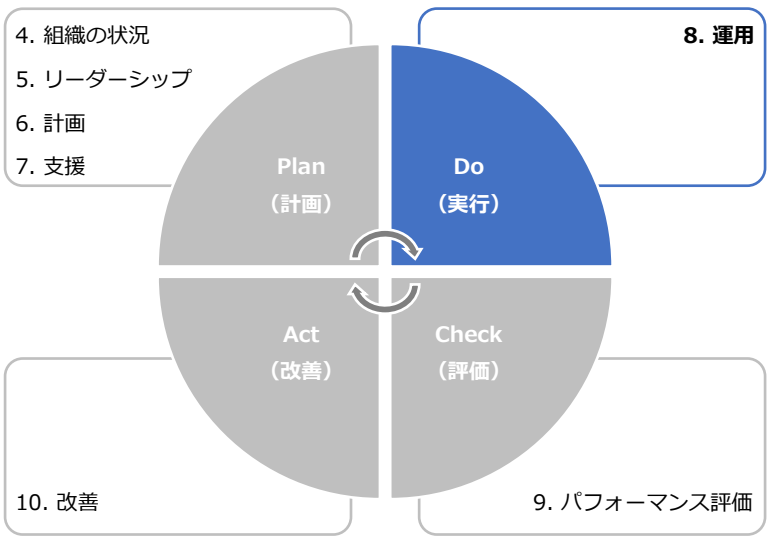
（管理方法の例）

- 文書化した情報は、ISMS事務局責任者が、最新版を紙の媒体としてファイリングし、キャビネットにて保管し、適用範囲内の対象者が必要なときに、必要なところで利用可能にする

13-2-6. ISMS：8. 運用

「8. 運用」は、PDCAサイクルの「Do（実行）」に位置しており、「6. 計画」で計画した活動や、要求事項を満たすための活動を実施し、管理します。そして、計画通りに実施した証拠となる情報を文書化し、保持する必要があります。

8. 運用	作成ドキュメント（例）
8.1 運用の計画及び管理 「6. 計画」で計画した活動や、要求事項を満たすための活動の実施状況を管理するための一覧表を作成します。	• ISMS年間計画表
8.2 情報セキュリティリスクアセスメント 「6. 計画」で定めたリスクアセスメントのプロセスを実施し、結果を文書化します。	• リスクアセスメント結果報告書
8.3 情報セキュリティリスク対応 「6. 計画」で定めたリスク対応計画を実施し、結果を文書化します。	• リスク対応計画



13-2-6. ISMS：8. 運用

8.1 運用の計画及び管理

作成するドキュメント
- ISMS年間計画表

「6. 計画で決定した活動」および「要求事項を満たすための活動」を実施するにあたり必要なプロセスを計画し、ISMS年間計画表を作成します。　ISMS年間計画表は、「6. 計画で決定した活動」および「要求事項を満たすための活動」の実施状況を管理するための計画表のことです。

ISMS年間計画表の作成方法

以下の例は、「6. 計画」で決定した活動に関する計画表の例です。

No	実施事項		文書名	スケジュール							
				2023年5月				2023年6月			
				8	15	22	29	5	12	19	26
6.1	「リスク及び機会に対処する活動」の検討	外部および内部の課題に対する活動の検討	外部および内部の課題								
		リスクアセスメントの実施	資産目録								
			リスクアセスメント結果報告書								
		リスク対応のための計画作成	適用宣言書								
		（アクションプランの作成）	リスク対応計画								
		管理策(ルール)の検討	情報セキュリティ手順書								
6.2	部門ごとに「情報セキュリティ目的及びそれを達成するための計画」を作成		ISMS有効性評価表								

- ✓ **No**：ISO/IEC 27001の要求事項の項番を記載します。
- ✓ **実施事項**：行う活動の内容を記載します。
- ✓ **文書名**：実施事項で記載した活動を行う際に利用したり、作成したりする文書名を記載します。
- ✓ **スケジュール**：実施事項を行う予定日を記載します。

13-2-6. ISMS：8. 運用

8.2 情報セキュリティリスクアセスメント

追記するドキュメント
- リスクアセスメント結果報告書

リスクアセスメントを実施する際は、結果を「リスクアセスメント結果報告書」に追記します。

リスクアセスメント結果報告書の追記方法

リスクアセスメント結果報告書の「対応」の箇所に記載します。

✓ **対応**：管理策の実施状況を記載します。
- ・管理策を実施した場合は「済み」
- ・管理策を実施する予定がある場合は「予定」
- ・管理策を実施する予定が未定の場合は「未定」

起こり得る結果	リスク分析(一次評価)			優先順位	リスク対応					
	重要度	被害発生可能性	リスクレベル		保有	低減	回避	移転	管理策	対応
機密情報などが漏えいし顧客に影響、信用喪失	3	2	6	2		●			モバイル機器の利用ルールを整備・強化	済み
機密情報などが漏えいし顧客に影響、信用喪失	2	2	4	3		●			教育訓練	予定
機密情報などが漏えいし顧客に影響、信用喪失	3	3	9	1		●			• 情報の分類定義 • 分類ごとの情報の取扱いルール • ラベリング	未定

8.3 情報セキュリティリスク対応

追記するドキュメント
- リスク対応計画

リスク対応を実施する際は、結果を「リスク対応計画」に追記します。

リスク対応計画の追記方法

リスク対応計画の「実績」、「ステータス」の箇所に記載します。

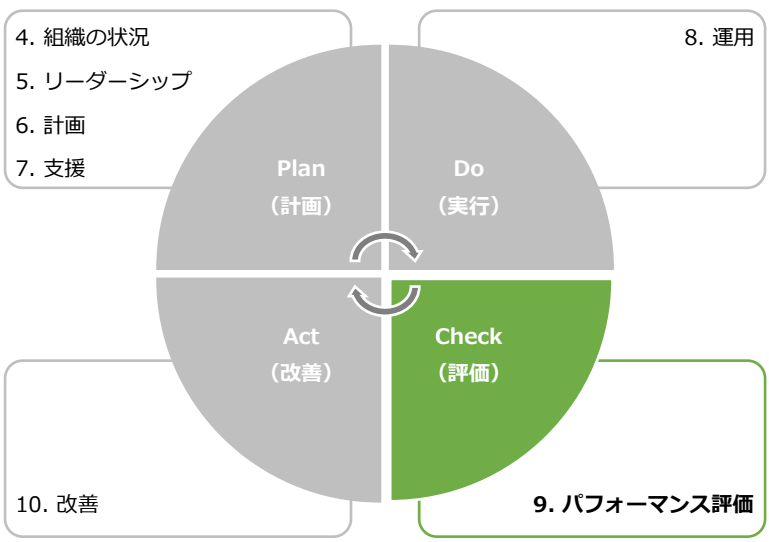
✓ **実績の開始の箇所**：実際にタスクを開始した日付を記載します。
✓ **実績の終了の箇所**：実際にタスクが完了した日付を記載します。
✓ **ステータスの箇所**：タスクの進捗状況を記載します。
- ・タスクが完了した場合は「終了」
- ・タスクを実行中の場合は「着手」
- ・タスクに着手していない場合は「未着手」

No	管理策	タスク	担当	予定		実績		ステータス
				開始	終了	開始	終了	
1	モバイル機器の利用ルールを整備・強化	• ルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-	20XX/-/-	20XX/-/-	終了
2	教育訓練	• ルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-	20XX/-/-		着手
3	• 情報の分類定義 • 分類ごとの情報の取扱いルール • ラベリング	• 情報の分類定義 • 分類ごとの取扱いルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-			未着手

13-2-7. ISMS：9. パフォーマンス評価

「9. パフォーマンス評価」は、PDCAサイクルの「Check（評価）」に位置しており、定めた情報セキュリティ目標を達成するための取組み（構築したISMS）が有効であるかどうかを評価します。

パフォーマンス評価	作成ドキュメント（例）
9.1 監視、測定、分析及び評価 情報セキュリティのパフォーマンスと、ISMSの有効性を評価します。	• ISMS有効性評価表
9.2 内部監査 ISMSの適合性、有効性について、あらかじめ定めた間隔で監査を実施します。	• 内部監査チェックリスト • 内部監査計画書 • 内部監査結果報告書
9.3 マネジメントレビュー トップマネジメントが、ISMSの有効性を評価します。	• マネジメントレビュー報告書



13-2-7. ISMS：9. パフォーマンス評価

9.1 監視、測定、分析及び評価

作成するドキュメント
- ISMS有効性評価表

ISMSの効果について判断するために、有効性評価を実施します。ISMSに沿って実施している活動が、情報セキュリティ目標の達成に繋がっているのか、有効に作用しているのかを評価し、課題があるのであれば改善することになります。　前項で説明した通り、PDCAサイクルによる継続したスパイラルアップによって、改善し続けることが重要です。計画時に定めた評価指標および評価方法により、ISMSが有効だったか、そうではなかったかを判断します。この有効性の評価は、マネジメントレビューの際にトップマネジメントが実施するのが効果的です。

【計画】
情報セキュリティ目的：・お客様との契約および法的または規制要求事項を尊重し遵守する
・情報セキュリティ事故を未然に防止する
・情報セキュリティ上の脅威から情報資産を保護する
・当社ISMSの意味を理解した活動の開始

評価指標：　ISMS教育受講／合格　100%(全従業者)
【備考】
取組みの初年度であるため、全従業者が活動に関与、さらには、活動を理解し、全社のセキュリティ目的の達成に向けた活動開始ができたことを確認する。

情報セキュリティ目的達成のための計画

実施事項	必要な資源	責任者	達成期限	評価方法
教育による活動の意味の理解	適用範囲の従業者がISMS教育を受講	ISMS事務局長	20XX年00月	受講者数および合格者数をカウントし、評価する

【評価】　**評価日：【20XX/00/00】**

情報セキュリティ目的達成に関する評価結果　**凡例　○：有効　×：有効ではない**

結果	備考
○	全従業員eラーニングでのテストを100点にて合格。有効性があるものと判断する。

✓ 情報セキュリティ目的達成のための計画には、計画時に定める実施事項、必要な資源、責任者、達成期限、評価方法を記載します。
※【計画】の詳しい記載方法については、「6. 計画」で説明しています。

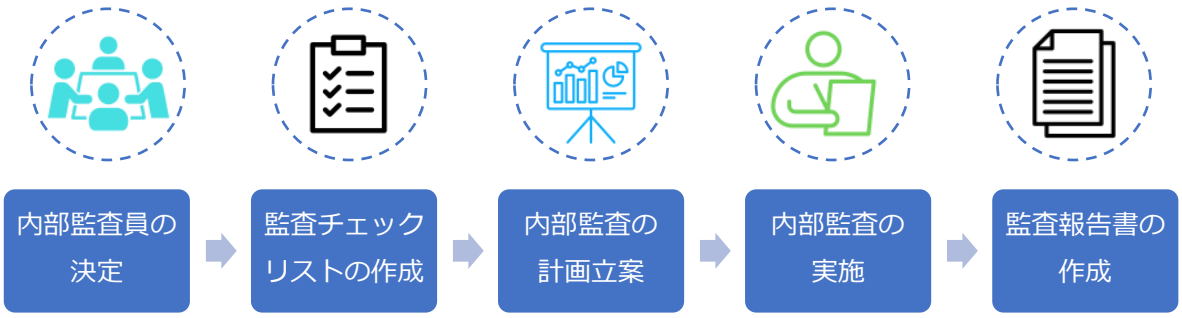
✓ 情報セキュリティ目的達成に関する評価結果には、ISMSが有効だったか否かという結果を記載します。

13-2-7. ISMS：9. パフォーマンス評価

9.2 内部監査（1/4）

作成するドキュメント
- 内部監査チェックリスト
- 内部監査計画書
- 内部監査結果報告書

内部監査とは、社内のルールや扱っている文書がISO/IEC 27001の要求事項を満たしており、従業員などがそのルールを守って仕事をしているかどうかをチェックすることです。内部監査結果報告書をもとに、マネジメントレビューで「自社のISMSはこのままでいいのか」「自社のISMSのどこに欠陥があり、どう修復しなくてはならないのか」を経営層が判断し、随時対策をとります。内部監査は一般的に以下のプロセスで進めます。



13-2-7. ISMS：9. パフォーマンス評価

9.2 内部監査（2/4）

1. 内部監査員の選定

内部監査とは、組織内部において、専門的知識を持った人が、経営者や役員などの立場にない第三者として、ISMSが適切に構築され、適正に運用されているかどうかを評価することです。内部監査員には、監査の公正さや客観性の観点から、監査対象となる部門に所属していない者を任命する必要があります。内部監査員に資格などは不要ですが、下記に当てはまるような人が適任です。社内に適した者がいない場合は、研修により内部監査員を育成したり、外部の専門家へ依頼したりするといった手段をとることが有効です。

・ISMSの内容を理解している人
・ISMSの内部監査の体制や実施方法といった手順に関する知識を有している人
・自社のISMSを把握している人
・監査対象となる部署の業務内容を把握している人

2. 内部監査チェックリストの作成

内部監査員がチェックリストを作成します。事前にチェックリストを作成することで、監査するべき範囲やポイントが明確になったり、チェック漏れを減らせたり、内部監査員ごとの偏った評価を防止したりといった効果が期待できます。また、チェックリストは内部監査を行った文書記録とすることができます。

内部監査チェックリストの作成方法（例）

ISMSの項目に沿ってチェック事項をまとめ、内部監査を実施の際には確認したISMSの根拠となる確認結果や文書類を記録します。

監査項目	チェック事項	確認結果・文書類
4. 組織の状況		
4.1 組織及びその状況の理解	組織は、組織の目的に関連し、かつ、そのISMSの意図した成果を達成する組織の能力に影響を与える、外部および内部の課題を決定しているか。	• 外部および内部の課題
4.2 利害関係者のニーズ及び期待の理解	次の事項を決定したか。 a) ISMSに関連する利害関係者 b) その利害関係者の、情報セキュリティに関連する要求事項	• 外部および内部の課題
4.3 情報セキュリティマネジメントシステムの適用範囲の決定	ISMSの適用範囲は、文書化されているか。	• ISMSマニュアル • ISMS適用範囲 • レイアウト図 • ネットワーク図
5. リーダーシップ		
5.1 リーダージップ及びコミットメント	トップマネジメントは、 a) 情報セキュリティ方針および情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にしているか。	• 情報セキュリティ方針 • 質問で確認
5.2 方針	情報セキュリティ方針は、 e) 文書化した情報として利用可能であるか。	• 情報セキュリティ方針

事前に作成する部分　　**監査時に記載する部分**

13-2-7. ISMS：9. パフォーマンス評価

9.2 内部監査（3/4）

3. 内部監査の計画立案

内部監査の計画を立てます。いつ、誰が、どの部門の誰に、何についてチェックするか、といったことを事前に段取りしておきます。

内部監査計画書の作成方法（例）

監査概要	
監査名称	ISO27001認証取得に関する内部監査
監査目的	ISO/IEC27001:2022認証取得に向けた当社ISMSの整備、運用状況を確認
監査テーマ	・管理策の運用状況、および有効性の確認 ・第一段階審査の指摘に対する改善状況の確認
監査方法	被監査部門に対するヒアリング、文書化された情報の閲覧、およびオフィスの視察
監査基準	JISQ27001:2022（ISO/IEC27001:2022)の要求事項、当社ISMSマニュアル、および情報セキュリティ手順書

詳細監査計画				
No	被監査部門名	監査人	応対者	日時
1	情報システム部	○○　○○	△△　△△	20XX/-/- 00:00
2	管理部	○○　○○	△△　△△	20XX/-/- 00:00
3	営業部	○○　○○	△△　△△	20XX/-/- 00:00
4	総務部	○○　○○	△△　△△	20XX/-/- 00:00

内部監査結果報告（予定）	
報告予定日	20XX年〇月
報告手段	報告会の開催

✓ **監査概要**：監査の名称、目的、テーマ、方法、基準を記載します。

✓ **詳細監査計画**：監査の対象となる部門名、監査人名、監査への対応者名、監査実施の日時といった予定を記載します。

✓ **内部監査結果報告（予定）**：監査結果の報告予定日と報告手段を記載します。

13-2-7. ISMS：9. パフォーマンス評価

9.2 内部監査（4/4）

4. 内部監査の実施

内部監査計画に沿って、内部監査チェックリストを用いて監査を実施します。

5. 内部監査結果報告書の作成

内部監査の結果をとりまとめ、報告書を作成します。どの部署で、どのルールが守られなかったかといったことを明確にしておきます。　内部監査結果報告書をもとに、経営層は自社のISMSをどのようにするか判断することになるため、内容に不明瞭な点や不足があると、適切な見直しができなくなってしまうため、注意が必要です。

内部監査結果報告書の作成方法（例）

監査名称	ISO27001認証取得に関する内部監査		
監査実施日時	20XX年-月		
監査目的	ISO/IEC27001:2022認証取得に向けた当社ISMSの整備状況を確認		
監査体制			
被監査部門①	情報システム部	監査人①	【名前】/【社名】
被監査部門②	管理部	監査人②	
被監査部門③	営業部	監査人③	
被監査部門④	総務部	監査人④	

監査総評

ISMSの整備状況を確認
当組織でのISMSは、ISO27001:2022規格に基づく体制構築（文書化）をほぼ完了し、要求事項に対する重大な不適合は検出されなかった。全体として適切な有効な仕組みにより運用を開始したと判断できる。
また社員の周知に関しては、ISMS教育の実施などにより体制や方針などの周知を行っていた。

不適合・観察事項
一部ではあるが、対応が十分でない事項があったため○件を軽微な不適合、○件を観察事項とした。重大な不適合は、検出されなかった。

【軽微な不適合】

No	規格	内容
1	5.2 方針	規格では「情報セキュリティ方針は、次の事項を満たさなければならない。g) 必要に応じて、利害関係者が入手可能である。」としている。しかし、「情報セキュリティ方針」について、お客様などの利害関係者が入手可能であることを確認できなかった。

【観察事項】

No	規格	内容
1	4.3 情報セキュリティマネジメントシステムの適用範囲の決定	ISMSマニュアルとネットワーク図で適用範囲の表現が同じであることの確認が難しい状況でした。ISMSマニュアルでは、ルータまで。ネットワーク図では、ONUまで。
2	7.3 認識	実施中のISMS教育の終了をお願いします。

備考（フォローアップなど）	次回の内部監査にて対応のフォローを行う

13-2-7. ISMS：9. パフォーマンス評価

9.3 マネジメントレビュー（1/2）

作成するドキュメント
- マネジメントレビュー報告書

マネジメントレビューとは、経営者（トップマネジメント）が行うレビュー活動です。トップマネジメントは、内部監査の結果や利害関係者からのフィードバックをもとに、組織のISMSが適切に運用されているかどうかを判断し、必要に応じて改善方法を指示します。この活動は、少なくとも年に1回定期的に実施することが求められています。トップマネジメントに報告した内容（インプット）と、トップマネジメントの指示や提案（アウトプット）を文書化したものが、マネジメントレビュー報告書です。

インプット、アウトプットに含める必要がある内容は以下の通りです。

インプットに含める必要がある事項
1. 前回までの指示事項に対する処置の進捗や結果 トップマネジメントから前回指示された改善活動の進捗状況や結果を記載します。初回の場合は記載しません。
2. ISMSに関連する外部および内部の課題の変化 事業の変化、法規制の改正など、昨年と比べた外部および内部の課題の変化について記載します。
3. ISMSに関連する利害関係者のニーズおよび期待の変化 「顧客や取引先、従業員、株主など利害関係者からの情報セキュリティに関する要求」の変化について記載します。
4. 情報セキュリティパフォーマンスの実績報告 以下の内容について、報告します。 • 不適合および是正処置 不適合に対する是正処置の実施状況を報告します。 • 監視および測定の結果 情報セキュリティパフォーマンスや、ISMSの有効性についての監視、測定結果を報告します。 • 監査結果 内部監査の結果を報告します。 • 情報セキュリティ目的の達成 情報セキュリティ目的の達成数や未達成数など、情報セキュリティ目的の達成状況を報告します。
5. 利害関係者からのフィードバック 利害関係者から、情報セキュリティに関する要望などについて、対応した結果を報告します。
6. リスクアセスメントの結果およびリスク対応計画の状況 リスクアセスメントにより、新しく特定したリスクや、リスク対応計画の進捗状況を報告します。
7. 継続的改善の機会 トップマネジメントに改善策を提案します。
アウトプットに含める必要がある事項
1. 継続的改善の機会 改善すべき内容について指示を記載します。
2. ISMSのあらゆる変更の必要性 ISMSに関して、次年度以降変更すべき内容について指示を記載します。

13-2-7. ISMS：9. パフォーマンス評価

9.3 マネジメントレビュー（2/2）

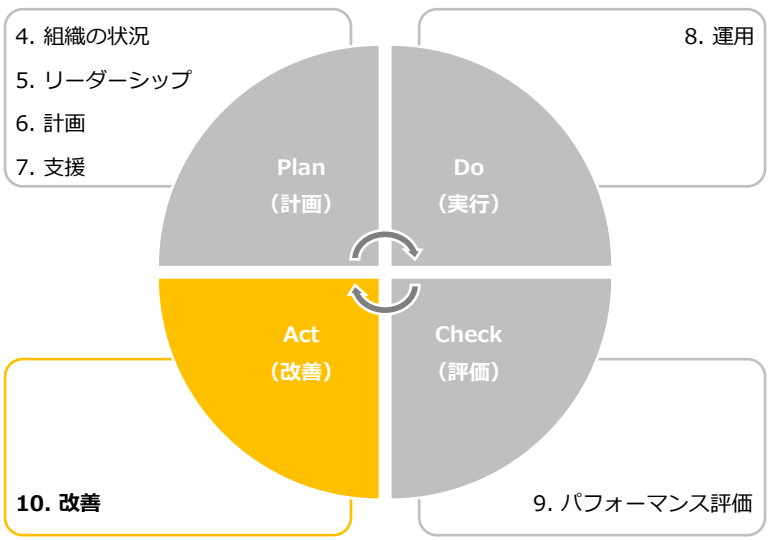
マネジメントレビュー報告書の作成方法（例）

<table>
<tr><td rowspan="3">出席者</td><td>トップマネジメント</td><td>【名前】</td><td rowspan="3">日時</td><td rowspan="2">20XX年〇月</td></tr>
<tr><td>情報セキュリティ委員長</td><td>【名前】</td></tr>
<tr><td>ISMS内部監査責任者</td><td>【名前】</td><td>00：00　～　00：00</td></tr>
<tr><td colspan="5">インプット（報告事項）</td></tr>
<tr><td>1</td><td>前回までの指示事項に対する処置の進捗や結果</td><td colspan="3">初回マネジメントレビューのためありません。</td></tr>
<tr><td>2</td><td>ISMSに関連する外部および内部の課題の変化</td><td colspan="3">「外部および内部の課題」にて報告の通りです。
その後、課題の変化は発生しておりません。</td></tr>
<tr><td>3</td><td>ISMSに関連する利害関係者のニーズおよび期待の変化</td><td colspan="3">お客様からの情報セキュリティに関する要求の変化はありませんでした。</td></tr>
<tr><td rowspan="4">4</td><td rowspan="4">情報セキュリティパフォーマンスの実績報告</td><td>1）不適合および是正処置</td><td colspan="2">20XX年〇月に実施した初回の内部監査で検出された“観察事項”1件は、是正対応中です。
今月末までに対応を予定しています。
そのほか現在対応中の不適合はありません。</td></tr>
<tr><td>2）監視および測定の結果</td><td colspan="2">次回のマネジメントレビューにて測定結果を報告します。</td></tr>
<tr><td>3）監査結果</td><td colspan="2">【内部監査】
20XX年〇月に1回目の内部監査を実施し、主にISMSの文書類整備状況の確認を行いました。
①ISO27001規格に基づく体制構築（文書化）をほぼ完了し、要求事項に対する重大な不適合は検出されませんでした。全体として適切な仕組みにより運用を開始したと判断します。
②一部ではありますが、対応が十分でない事項があり、観察事項1件が検出されました。
詳細は、「内部監査結果報告書」(20XX年〇月)にて報告の通りです。</td></tr>
<tr><td>4）情報セキュリティ目的の達成</td><td colspan="2">次回のマネジメントレビューにて報告します。</td></tr>
<tr><td>5</td><td>利害関係者からのフィードバック</td><td colspan="3">お客様からのクレームは現状ありませんでした。</td></tr>
<tr><td>6</td><td>リスクアセスメントの結果およびリスク対応計画の状況</td><td colspan="3">【リスクアセスメントの状況】
「情報リスクアセスメント結果報告書」(20XX年〇〇月〇〇日)にて報告の通りです。
【リスク対応計画の状況】
・リスク対応計画にリストアップした管理策：〇件
・対応が終了した管理策：〇件
・対応が終了していない管理策2件は以下の通りです。
<table><tr><td>対応</td><td>予定</td></tr><tr><td>サービス供給者の管路</td><td>今月下旬</td></tr><tr><td>情報セキュリティ継続</td><td>今月下旬</td></tr></table>※詳細は、「リスク対応計画」(作成：20XX年〇〇月〇〇日、見直：20XX年〇月)にて報告の通りです。</td></tr>
<tr><td>7</td><td>継続的改善の機会</td><td colspan="3">現状はISMSを従業者が理解するための活動を主として行っています。</td></tr>
<tr><td colspan="5">アウトプット（トップマネジメントの指示事項）</td></tr>
<tr><td>1</td><td>継続的改善の機会</td><td colspan="3">現状認識している各課題を確実に実施すること。</td></tr>
<tr><td>2</td><td>ISMSのあらゆる変更の必要性</td><td colspan="3">コンサルタント会社のひな形にとらわれず、より当社の状況を反映した仕組み・ルールに見直しを行っていくこと。</td></tr>
</table>

13-2-8. ISMS：10. 改善

「10. 改善」は、PDCAサイクルの「Act（改善）」に位置しており、ISMSの改善を行います。

10. 改善	作成ドキュメント（例）
10.1 継続的改善 ISMSのPDCAサイクル（「4. 組織の状況」から「10. 改善」までの活動）を継続して実施し、情報セキュリティパフォーマンスを向上させるために必要となる改善を行っていきます。具体的には、情報セキュリティ方針や情報セキュリティ目的の計画、リスクアセスメントやリスク対応をもとに決定した管理策の実施を継続して行い、改善していきます。	ー
10.2 不適合及び是正処置 不適合が発生した際に是正処置を実施します。不適合とは、ISMSの要求事項を満たしていないことです。具体的には、管理策の不備や未実施、セキュリティインシデントの発生などのことです。	• 是正要求書兼回答書

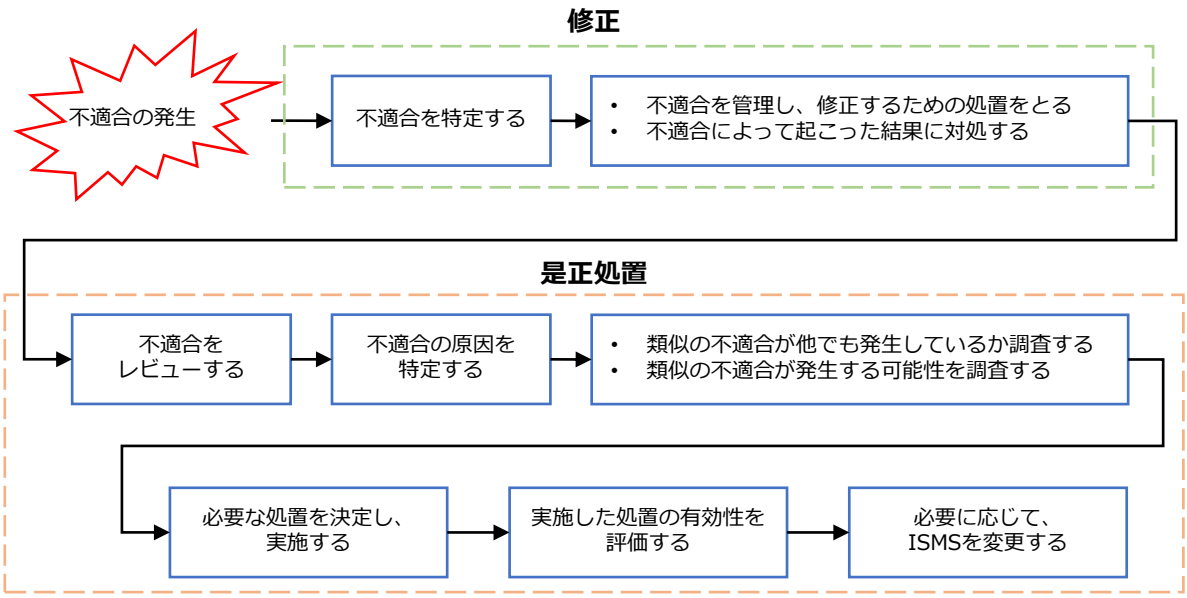


13-2-8. ISMS：10. 改善

10.2 不適合及び是正処置（1/2）

作成するドキュメント
- 是正要求書兼回答書

審査でISMSに不適合が検出された場合は、是正処置をしなければなりません。是正処置とは、不適合について、その原因を取り除き、再発防止を図る処置を指します。是正処置は以下の図のようなプロセスで実施されます。



「不適合の性質および講じた処置」と「是正処置の結果」について、文書化した情報を残さなければなりません。そのため、内部監査で不適合が出た際は、是正要求書とその回答書を記載して保存することになります。

13-2-8. ISMS：10. 改善

10.2 不適合及び是正処置（2/2）

是正要求書兼回答書の作成方法（例）

前ページで説明した「不適合の性質および講じた処置」と「是正処置の結果」についての内容を記載します。

整理番号	00-00	対象部門	○○○○部門	発効日	20XX 年 - 月 - 日

入力情報	分類	監査	■	内部監査における指摘事項												
			□	外部機関が実施した監査における指摘事項　(機関名：　　)												
			監査年月日		年		月		日	監査者						
			指摘のランク	観察事項						要求事項項番	7.2 力量					
		監査以外	□	セキュリティインシデントの関連した改善事項												
			□	外部の利害関係者からのニーズに基づく改善事項												
			□	内部において提案された改善事項												
			□	その他（　　）												
	内容	一部情報セキュリティ委員会担当者が仮任命のため、今後本任命を行っていく。												承認	作成	
処置計画	修正	力量の確認。任命力量確認表の更新。														
		実施予定日		年		月		日								
	評価	類似の不適合の有無		無	発生する可能性		無									
		原因	対応の認識はあり、あくまでも観察事項としての取扱いのため、原因などはなし。													
		原因を除去するための計画の必要性		有	※有の場合原因除去の計画を記載											
	原因除去	対応の認識はあり、あくまでも観察事項としての取扱いのため、原因などはなし。												承認	作成	
		実施予定日		年		月		日								
実施報告	内容	上記の通り、「ISMS年間計画表」を修正し、運用チェックリストによる点検を実施した。												承認	作成	
		実施完了日		年		月		日								
処置確認	確認	「ISMS年間計画表」の修正、運用チェックリストによる点検記録を確認した。												承認	作成	
		確認日		年		月		日								
	有効性	セキュリティ手順の実行、および技術的遵守について、点検漏れのリスクが低減された。														
		評価日		年		月		日	フォロー監査の要・不要							

コラム

ISMSの導入：成功の鍵とよくある落とし穴

組織が顧客データや機密情報などの情報資産を守るためには、適切に情報セキュリティを確保する仕組みが必要となります。そのために、ISMSの導入と運用は重要になります。そこで、ISMSを導入・運用していく際に成功の鍵となるポイントと、陥りやすい失敗例をいくつか紹介します。

成功の鍵となるポイント

■ トップマネジメントのコミットメント
ISMSの導入には経営陣からのコミットメントが不可欠です。経営層が情報セキュリティの重要性を理解し、リーダーシップを発揮することで、組織全体が情報セキュリティの確保に向けて協力的になります。

■ 従業員の教育と意識向上
従業員への教育は、従業員に基本方針や対策基準などを理解させ、策定された実施手順を実践してもらうために重要です。定期的なトレーニングや教育プログラムを通じて、従業員が脅威に対処できるようにサポートしていくことが大切です。

■ リスク評価と適切な対応策
リスク評価を行い、特定のリスクに対して適切な対応策を策定することで、情報資産の保護と事業の継続性を確保できます。

陥りやすい失敗例

■ 実施手順の抽象性
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分からず、セキュリティ対策が不十分になってしまいます。分かりやすい実施手順を策定し、従業員に浸透させることが重要です。

■ 不十分な監査と改善の実施
ISMSの運用において監査と改善を怠ってしまうと、新たな脅威に適応できず、セキュリティ体制が陳腐化してしまいます。定期的な監査と、その結果をもとにした改善活動を継続的に行うことが必要です。

ISMSの導入を成功させるためには、経営層のリーダーシップ、従業員の教育、リスクマネジメントの適切な実施が欠かせません。常に変化するセキュリティ環境に適応する柔軟性や継続的な改善が、組織の情報セキュリティを確保することに繋がります。

編集後記

セミナー7日目では、具体的に実施する手順についてレベルごとに説明しました。特に、最もレベルが高く、漏れがない手法である網羅的アプローチに重点を置いた内容となりました。フレームワークにISMSを用いることで、単にセキュリティ対策を検討するだけではなく、PDCAサイクルによってISMS自体を継続的に改善し、より自社に適した対策を検討できるようになっています。緊急性や即効性についてはクイックアプローチ、ベースラインアプローチが勝りますが、じっくりと対策を検討する余裕がある場合、網羅的アプローチを推奨します。

本テキストでは、対策基準から実施手順を策定する3つの手法を説明するにあたり、クイックアプローチ、ベースラインアプローチ、網羅的アプローチの順に説明しました。クイックアプローチは、実際のセキュリティインシデントの事例について、自社での発生可能性や被害規模を検討した上で対策基準や実施手順を策定していくため、社会的に影響の大きい事案への対策がとりやすいと考えられます。ベースラインアプローチは、ガイドラインやひな形などによる既存の手法を参考にして対策基準や実施手順を策定していくため、自社に適した参考元があれば、それをもとに簡易な手順で策定ができると考えられます。網羅的アプローチは、フレームワークとしてISMSを参考にして対策基準や実施手順を策定していくため、時間はかかりますが、会社としてセキュリティを確保するにあたって高いレベルでのセキュリティ対策ができると考えられます。3つのアプローチ手法のうち、自社にあっていると考えられるものを選んで対策を検討してみてください。

次回は、作成すべきドキュメントや実施すべき対策手順を通して、組織的対策や人的対策の考え方について説明します。

引用文献

2021年度 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 -事例集-

https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000098149.pdf

リスク分析シート

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx

5分でできる！情報セキュリティ自社診断

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf

情報セキュリティハンドブック（ひな形）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055529.pptx

中小企業のためのクラウドサービス安全利用の手引き

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

情報セキュリティ関連規程（サンプル）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

参考文献

情報セキュリティ関連規程（サンプル）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

中小企業の情報セキュリティ対策ガイドライン第3.1版

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

5分でできる！情報セキュリティ自社診断

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf

情報セキュリティハンドブック（ひな形）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055529.pptx

インターネットの安全・安心ハンドブックVer 5.00

https://security-portal.nisc.go.jp/guidance/handbook.html

テレワークセキュリティガイドライン第5版

https://www.soumu.go.jp/main_content/000752925.pdf

中小企業のためのクラウドサービス安全利用の手引き

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

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

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

■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

■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

■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

■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

■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

用語集

■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

■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

■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

■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

■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、12-2-1、12-3-1、第一回コラム

■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

用語集

■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

■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

■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

■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

■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

■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

■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

用語集

■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

■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

■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、

■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

■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

■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

用語集

■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

■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

■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

■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

用語集

■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

■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

■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

■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

■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

■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

■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

■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