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

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．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】 の概要

【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

【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

クイックアプローチ・ベースラインアプローチ

【参照：セミナーテキスト12-1-1.】
第12章 - 02

アプローチ手法概略

【LV.1クイックアプローチ】

即時の対応や緊急事態への対処に適したアプローチ手法。
様々なインシデント事例内容を参考にし、対策基準を策定。

【LV.2ベースラインアプローチ】

組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指すアプローチ手法。
ガイドラインやひな形を参考とし、対策基準を策定。

セキュリティインシデント事例を参考とした実施手順

LV1.クイックアプローチの実施手順

【参照：セミナーテキスト12-2-1.】
第12章 - 03

インシデント事例

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を参考とした実施手順

リスクアセスメントの実施

【参照：セミナーテキスト12-2-1.】
第12章 - 03

リスク特定

- 対象となる資産情報の洗い出し
- 機密性、完全性、可用性の評価
- 重要度の算出

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

セキュリティインシデント事例を参考とした実施手順

リスクアセスメントの実施

【参照：セミナーテキスト12-2-1.】
第12章 - 04

リスク分析

- 重要度と被害発生可能性から、リスクレベルを算出

「リスクレベル」＝「重要度」×「被害発生可能性」

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

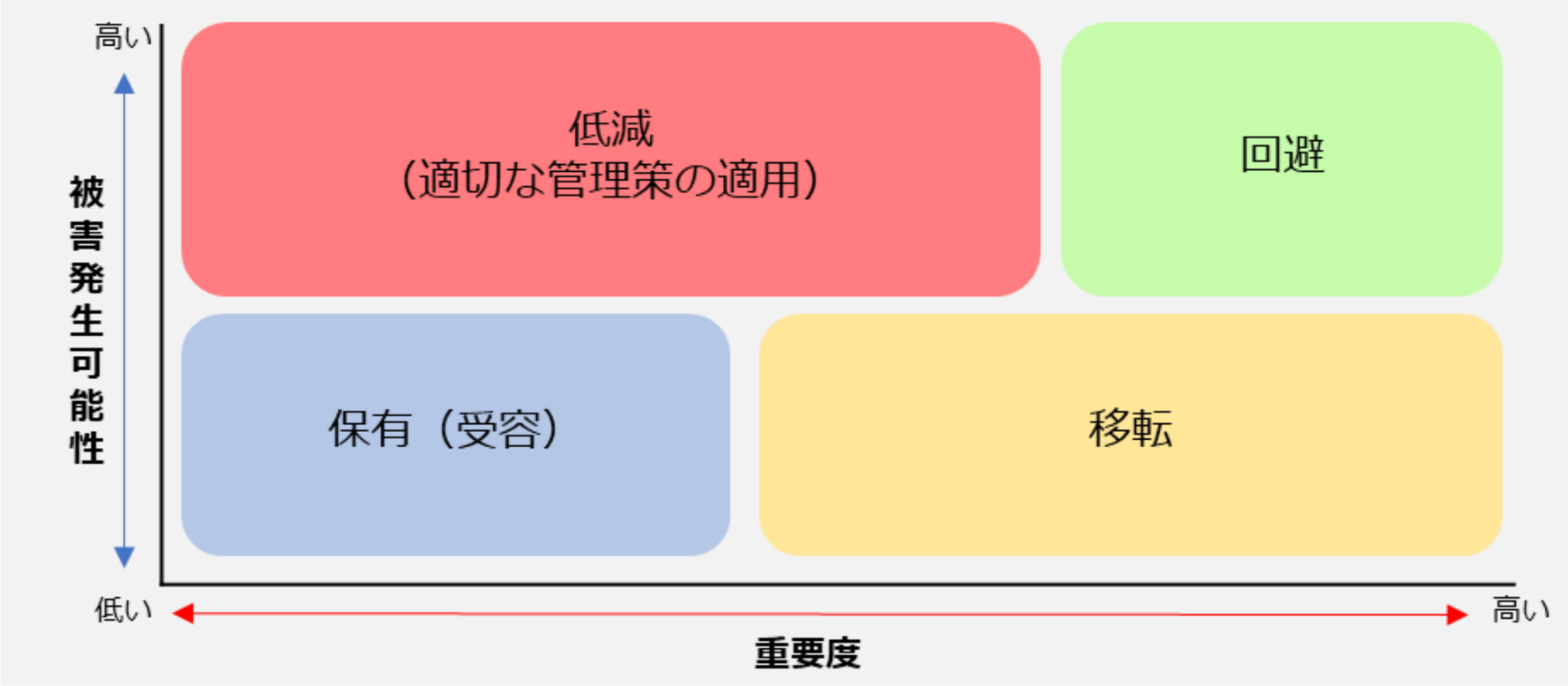
セキュリティインシデント事例を参考とした実施手順

リスクアセスメントの実施

【参照：セミナーテキスト12-2-1.】
第12章 - 04

リスク評価

- リスク対応を検討する



セキュリティインシデント事例を参考とした実施手順

対策基準の策定

【参照：セミナーテキスト12-2-1.】
第12章 - 04

事例を基にした対策基準

- 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

セキュリティインシデント事例を参考とした実施手順

実施手順の作成

【参照：セミナーテキスト12-2-1.】
第12章 - 05

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。

セキュリティインシデント事例を参考とした実施手順

実施手順の作成

【参照：セミナーテキスト12-2-1.】
第12章 - 05

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。

セキュリティインシデント事例を参考とした実施手順

実施手順の作成

【参照：セミナーテキスト12-2-1.】
第12章 - 05

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。

セキュリティインシデント事例を参考とした実施手順

実施手順の作成

【参照：セミナーテキスト12-2-1.】
第12章 - 05

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

ガイドラインを参考とした実施手順

情報セキュリティ対策ガイドラインの活用

【参照：セミナーテキスト12-3-1.】
第12章 - 06

参考にするガイドラインの例

- 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」

ガイドラインを参考とした実施手順

情報セキュリティ関連規程（IPA）の活用

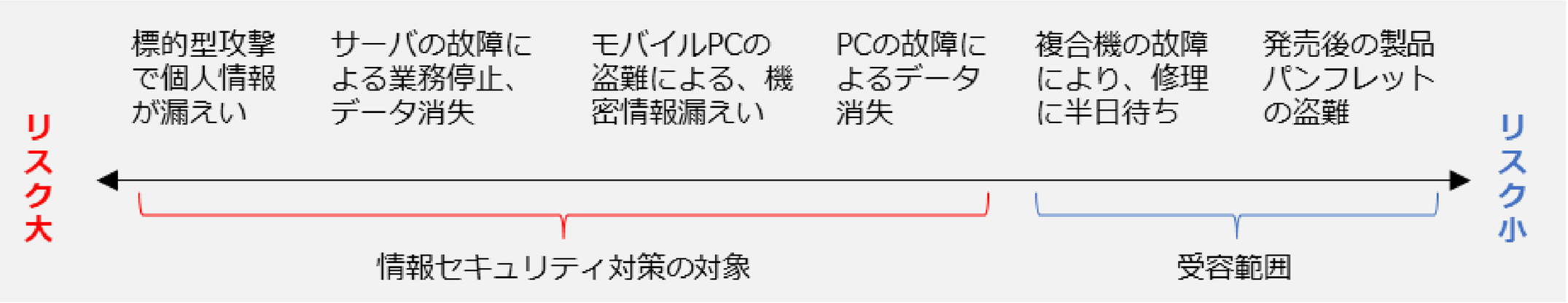
【参照：セミナーテキスト12-3-1.】
第12章 - 12

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

対策決定のヒント

- リスクの受容も視野に入れてリスク評価を実施する



ガイドラインを参考とした実施手順

情報セキュリティ関連規程（IPA）の活用

【参照：セミナーテキスト12-3-1.】
第12章 - 13

規程の作成

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
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

ガイドラインを参考とした実施手順

情報セキュリティ関連規程（IPA）の活用

【参照：セミナーテキスト12-3-1.】
第12章 - 13

規程の作成

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

1．ISMSの要求事項と構築

【LV.3網羅的アプローチ】の概要

【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

網羅的アプローチ

【参照：セミナーテキスト13-1-1.】
第13章 - 02

アプローチ手法概略

【LV.3網羅的アプローチ】

網羅的な対策を講じることを目指すアプローチ手法。
ISMSなどの認証が可能なレベルを目指して、対策基準を策定。

網羅的アプローチ実施の留意点

- ドキュメントの整備は手段であり目的ではない
- ISMSマネジメントプロセスの導入により、PDCAを実施していくことが重要

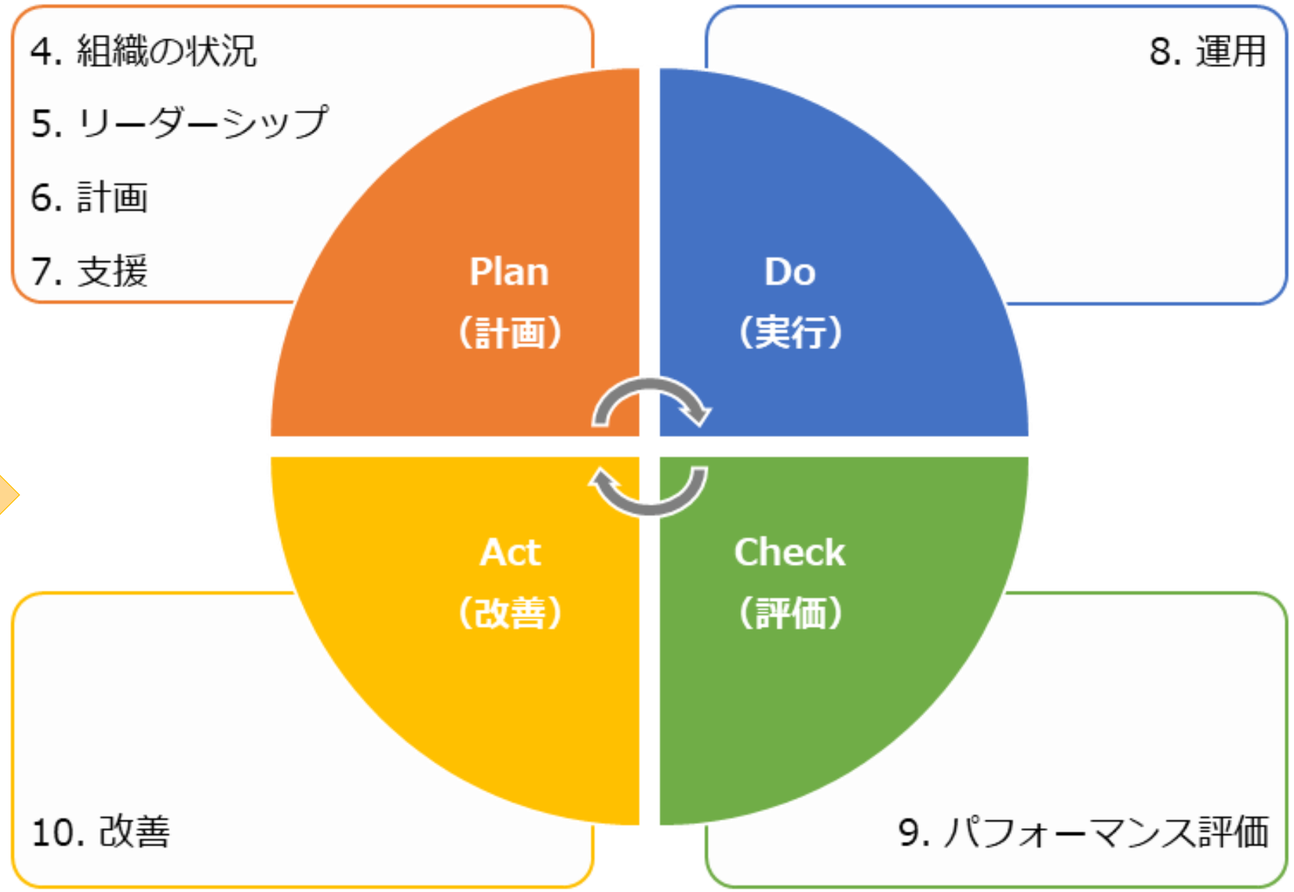
ISMSの概要

【参照：セミナーテキスト13-2-1.】
第13章 - 03

ISMSの確立、運用、監視

要求事項

1. 適用範囲
2. 引用規格
3. 用語および定義
4. 組織の状況
5. リーダーシップ
6. 計画
7. 支援
8. 運用
9. パフォーマンス評価
10. 改善

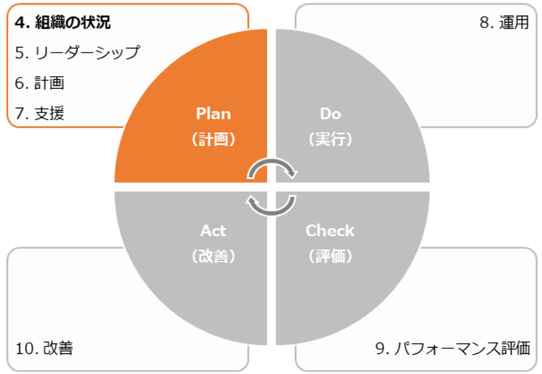


ISMS：4. 組織の状況

【参照：セミナーテキスト13-2-2】
第13章 - 04

概要

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



ISMS：4. 組織の状況

【参照：セミナーテキスト13-2-2】
第13章 - 05

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

外部の課題

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

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

ISMS：4. 組織の状況

【参照：セミナーテキスト13-2-2】
第13章 - 06

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	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

ISMS：4. 組織の状況

【参照：セミナーテキスト13-2-2】
第13章 – 07, 08

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

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

適用範囲を組織の一部としたときの考慮ポイント

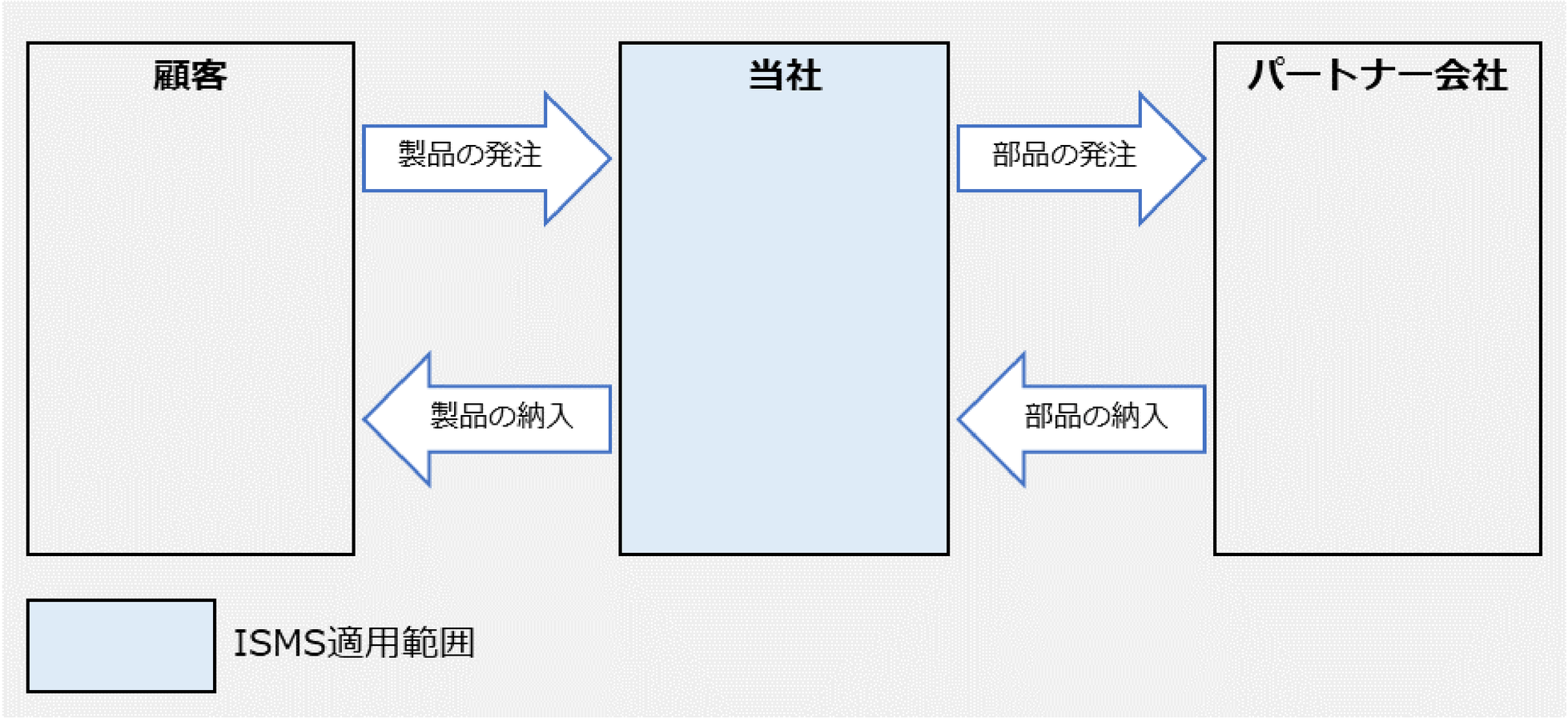
- 人的、組織的境界
- 物理的境界
- 技術的境界
- 資産的境界
- 事業的境界

ISMS：4. 組織の状況

【参照：セミナーテキスト13-2-2】
第13章 - 07

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

適用範囲の記載例

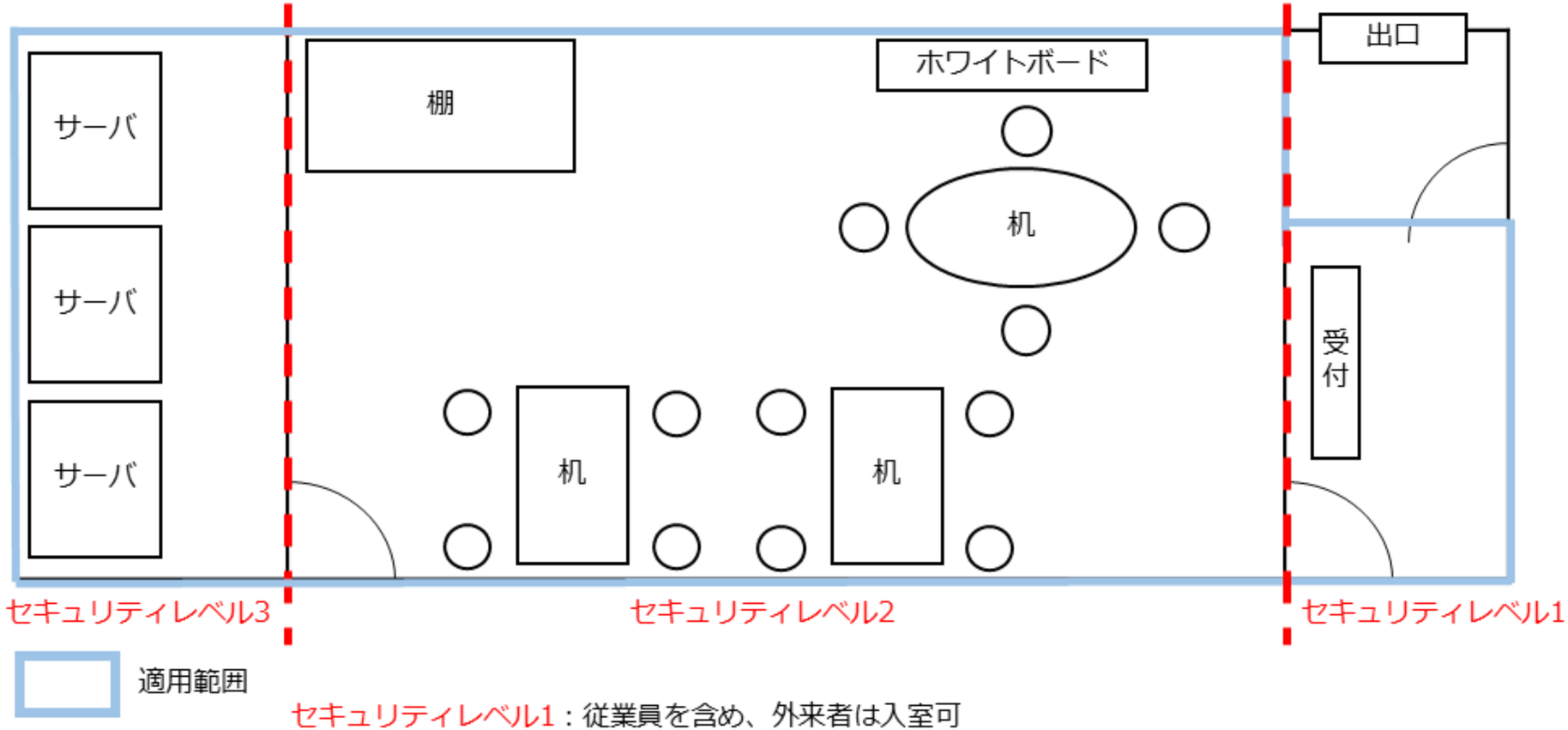


ISMS：4. 組織の状況

【参照：セミナーテキスト13-2-2】
第13章 - 09

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

レイアウト図



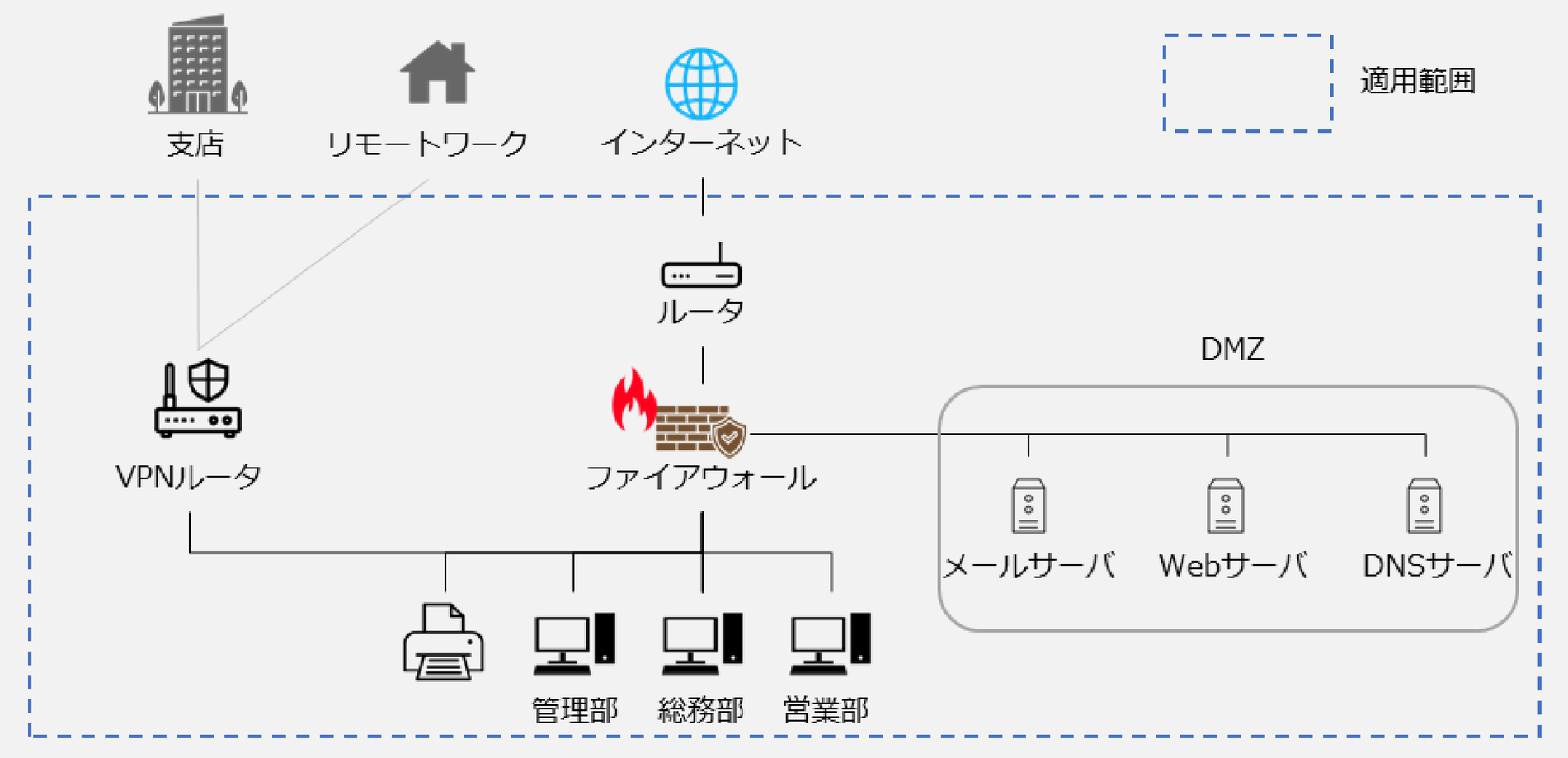
セキュリティレベル1：従業員を含め、外来者は入室可
セキュリティレベル2：対象従業員のみ入室可（対象者以外は入退室管理が必要）
セキュリティレベル3：限られた人員のみ入室可（飲食禁止）

ISMS：4. 組織の状況

【参照：セミナーテキスト13-2-2】
第13章 - 09

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

ネットワーク図

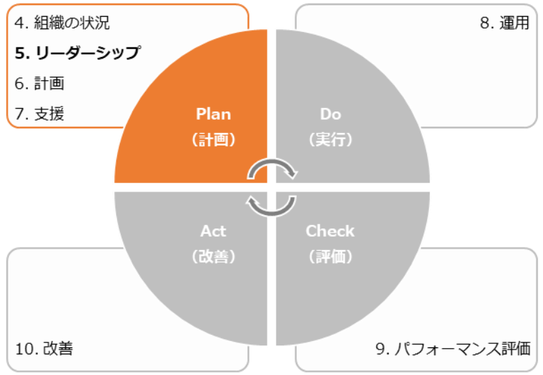


ISMS：5. リーダーシップ

【参照：セミナーテキスト13-2-3】
第13章 – 10

概要

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



ISMS：5. リーダーシップ

【参照：セミナーテキスト13-2-3】
第13章 – 11

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
- 組織のプロセスへのISMS要求事項の統合を確実にする
- ISMSに必要な資源が利用可能であることを確実にする
- 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
- ISMSがその意図した成果を達成することを確実にする
- ISMSの有効性に寄与するよう人々を指揮し、支援する
- 継続的改善を促進する
- 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

ISMS：5. リーダーシップ

【参照：セミナーテキスト13-2-3】
第13章 - 12

5.2 方針

作成するドキュメント　情報セキュリティ方針

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。

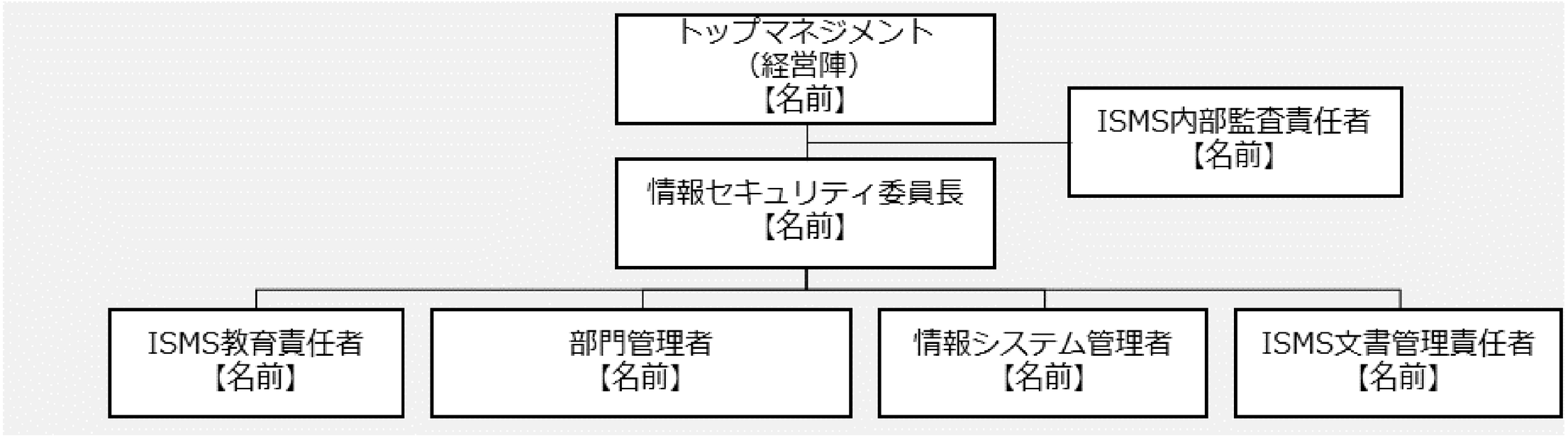
ISMS：5. リーダーシップ

【参照：セミナーテキスト13-2-3】
第13章 - 13

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

ISMS運用組織図



ISMS：5. リーダーシップ

【参照：セミナーテキスト13-2-3】
第13章 - 13

5.3 組織の役割、責任及び権限

責任者または部門の名称と役割を明記した文書

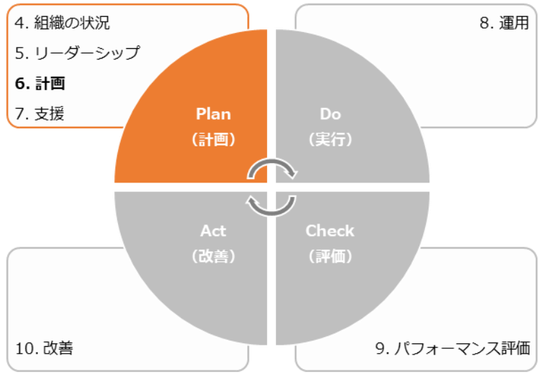
名称	役割
情報セキュリティ委員長	ISMSの実施、運用について統括する
ISMS内部監査責任者	ISMSとその実施状況に関わる監査を統括する
ISMS教育責任者	ISMSに関する教育計画の立案と実施を行う
部門管理者(情報セキュリティ委員)	ISMSの部門代表者として、部門を管理する
情報システム管理者	情報システム部門の管理者で、情報システム管理に関する規程・規則に従い、ISMSを維持するための安全管理対策を実施する
ISMS文書管理責任者	ISMSに関する文書と記録などの維持・管理を行う

ISMS：6. 計画

【参照：セミナーテキスト13-2-4】
第13章 - 14

概要

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。	ー



ISMS：6. 計画

【参照：セミナーテキスト13-2-4】
第13章 – 14

6.1 リスク及び機会に対処する活動

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

リスクアセスメント結果報告

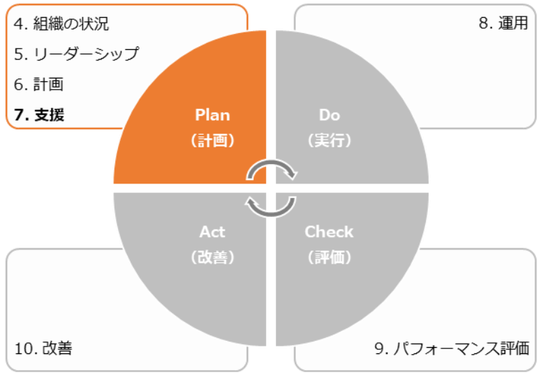
起こり得る結果	リスク分析(一次評価)			優先順位	リスク対応					
	重要度	被害発生可能性	リスクレベル		保有	低減	回避	移転	管理策	対応
機密情報などが漏えいし顧客に影響、信用喪失	3	2	6	2		●			モバイル機器の利用ルールを整備・強化	
機密情報などが漏えいし顧客に影響、信用喪失	2	2	4	3		●			教育訓練	
機密情報などが漏えいし顧客に影響、信用喪失	3	3	9	1		●			• 情報の分類定義 • 分類ごとの情報の取扱いルール • ラベリング	

ISMS：7. 支援

【参照：セミナーテキスト13-2-5】
第13章 - 25

概要

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。	―
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	―
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。	―
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。	―



ISMS：7. 支援

【参照：セミナーテキスト13-2-5】
第13章 - 26

7.1 資源

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

ISMS：7. 支援

【参照：セミナーテキスト13-2-5】
第13章 - 27

7.2 力量

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：7. 支援

【参照：セミナーテキスト13-2-5】
第13章 - 27

7.2 力量

力量確認表

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

ISMS：7. 支援

【参照：セミナーテキスト13-2-5】
第13章 - 28

7.2 力量

教育計画書

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。

ISMS：7. 支援

【参照：セミナーテキスト13-2-5】
第13章 - 29

7.2 力量

理解度確認テスト

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。	

ISMS：7. 支援

【参照：セミナーテキスト13-2-5】
第13章 - 30

7.2 力量

教育実施記録

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

ISMS：7. 支援

【参照：セミナーテキスト13-2-5】
第13章 - 31

7.3 認識

理解するべき内容

- 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

ISMS：7. 支援

【参照：セミナーテキスト13-2-5】
第13章 - 32

7.4 コミュニケーション

コミュニケーション手順

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

ISMS：7. 支援

【参照：セミナーテキスト13-2-5】
第13章 - 33

7.5 文書化した情報

文書化した情報の一覧

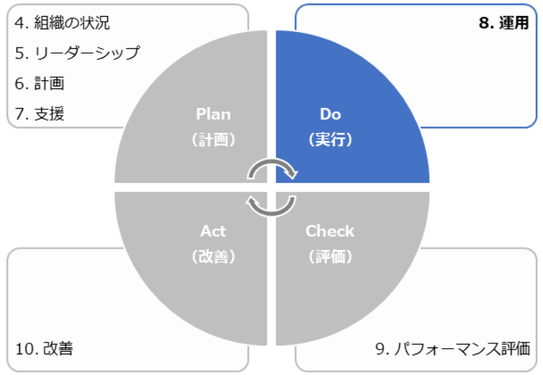
文書化した情報	作成する項番
ISMSの適用範囲	「4. 組織の状況」で作成
情報セキュリティ方針	「5. リーダーシップ」で作成
リスクアセスメントプロセスに関わる文書化された情報	「6. 計画」で作成
リスク対応プロセスに関わる文書化された情報	
情報セキュリティ目的に関わる文書化された情報	
力量の証拠	「7. 支援」で作成
組織が決めた文書化された情報	
ISMSのプロセス実施に関わる文書化された情報	「8. 運用」で作成
リスクアセスメントの結果	
リスク対応の結果	
監視・測定の結果	「9. パフォーマンス評価」で作成
監査プログラムの実施、結果に関わる文書化された情報	
マネジメ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

ISMS：8. 運用

【参照：セミナーテキスト13-2-6】
第13章 - 34

概要

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。	• 情報セキュリティ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」で定めた情報セキュリティリスク対応計画を実施し、結果を文書化します。	• 情報セキュリティリスク対応計画



ISMS：8. 運用

【参照：セミナーテキスト13-2-6】
第13章 - 35

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

年間計画表

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								
			情報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）	情報セキュリティリスク対応計画								
		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								

ISMS：8. 運用

【参照：セミナーテキスト13-2-6】
第13章 - 36

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　情報セキュリティリスクアセスメント結果報告書

結果報告書

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

ISMS：8. 運用

【参照：セミナーテキスト13-2-6】
第13章 - 36

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　情報セキュリティリスク対応計画

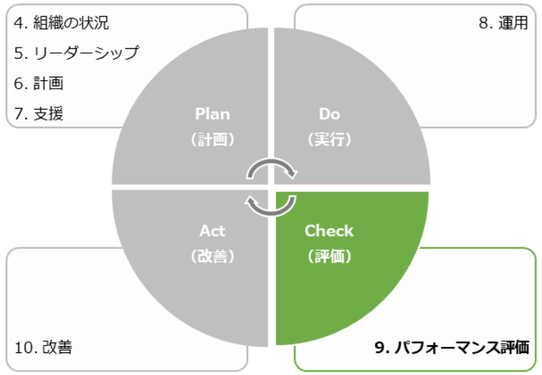
情報セキュリティリスク対応計画

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/-/-	20XX/-/-	終了
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/-/-	20XX/-/-		着手

ISMS：9.パフォーマンス評価

【参照：セミナーテキスト13-2-7】
第13章 - 37

概要



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

ISMS：9.パフォーマンス評価

【参照：セミナーテキスト13-2-7】
第13章 - 38

9.1 監査、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

有効性評価表

【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。

ISMS：9.パフォーマンス評価

【参照：セミナーテキスト13-2-7】
第13章 - 39

9.2 内部監査

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

ISMS：9.パフォーマンス評価

【参照：セミナーテキスト13-2-7】
第13章 - 40

9.2 内部監査

内部監査チェックリスト

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

ISMS：9.パフォーマンス評価

【参照：セミナーテキスト13-2-7】
第13章 - 41

9.2 内部監査

内部監査計画書

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○月
報告手段	報告会の開催

ISMS：9.パフォーマンス評価

【参照：セミナーテキスト13-2-7】
第13章 - 42

9.2 内部監査

内部監査結果報告書

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。

ISMS：9.パフォーマンス評価

【参照：セミナーテキスト13-2-7】
第13章 - 43

9.3 マネジメントレビュー

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

ISMS：9.パフォーマンス評価

【参照：セミナーテキスト13-2-7】
第13章 - 43

9.3 マネジメントレビュー

含める項目

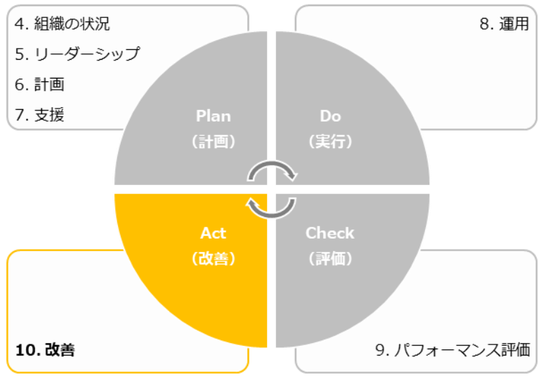
インプットに含める必要がある事項
1. 前回までの指示事項に対する処置の進捗や結果 トップマネジメントから前回指示された改善活動の進捗状況や結果を記載します。初回の場合は記載しません。
2. ISMSに関連する外部および内部の課題の変化 事業の変化、法規制の改正など、昨年と比べた外部および内部の課題の変化について記載します。
3. ISMSに関連する利害関係者のニーズおよび期待の変化 「顧客や取引先、従業員、株主など利害関係者からの情報セキュリティに関する要求」の変化について記載します。
4. 情報セキュリティパフォーマンスの実績報告 以下の内容について、報告します。 • 不適合および是正処置 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。

ISMS：10. 改善

【参照：セミナーテキスト13-2-8】
第13章 - 45

概要

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。	―
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



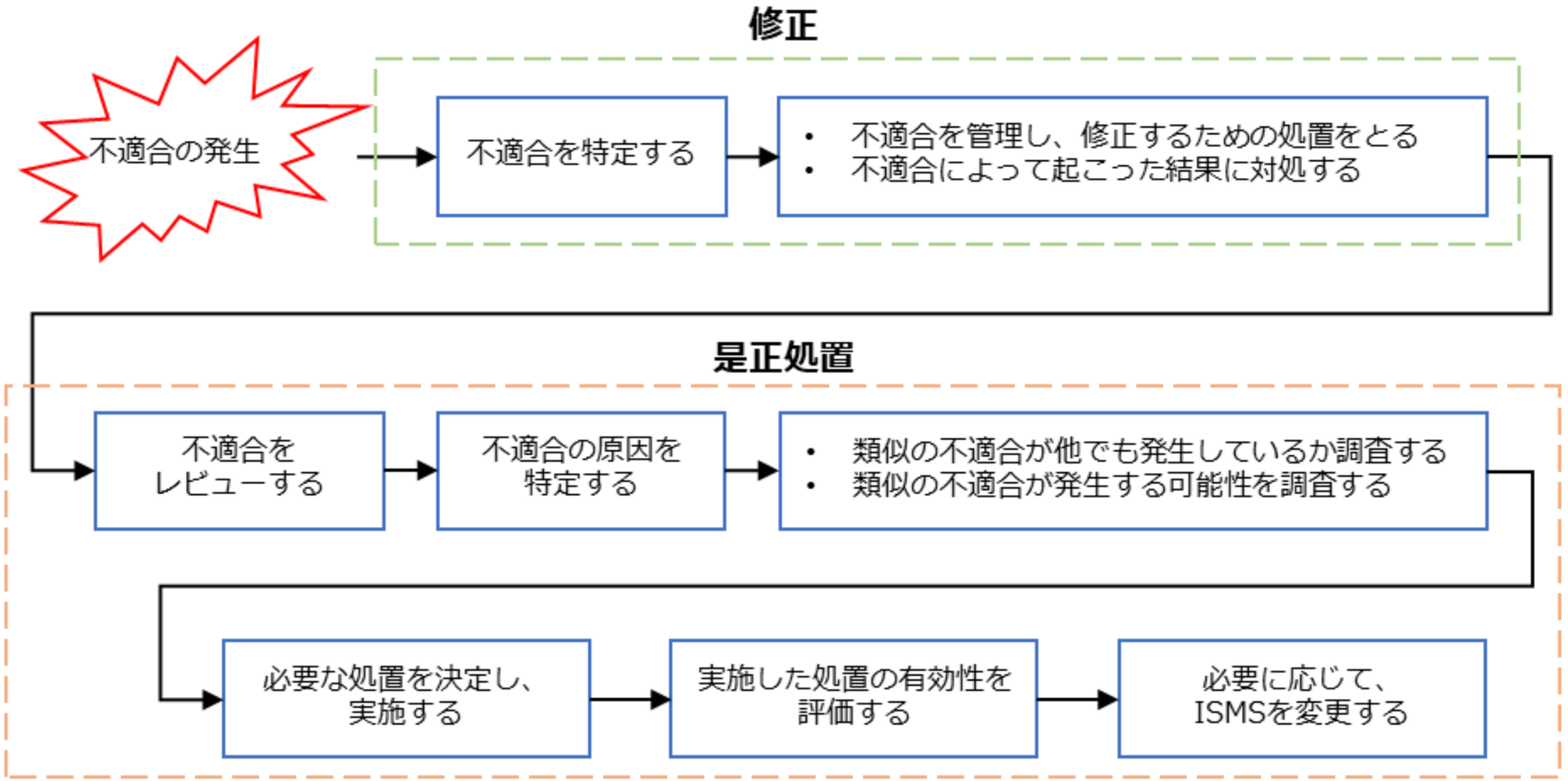
ISMS：10. 改善

【参照：セミナーテキスト13-2-8】
第13章 - 46

10.2 不適合及び是正処置

作成するドキュメント　是正要求書兼回答書

プロセス



ISMS：10. 改善

【参照：セミナーテキスト13-2-8】
第13章 - 47

10.2 不適合及び是正処置

是正要求書兼回答書

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							

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