令和7年度
中小企業サイバーセキュリティ
実践力強化プログラム

第3回

第6編：ISMSなどのフレームワークの種類と活用法の紹介

東京都産業労働局

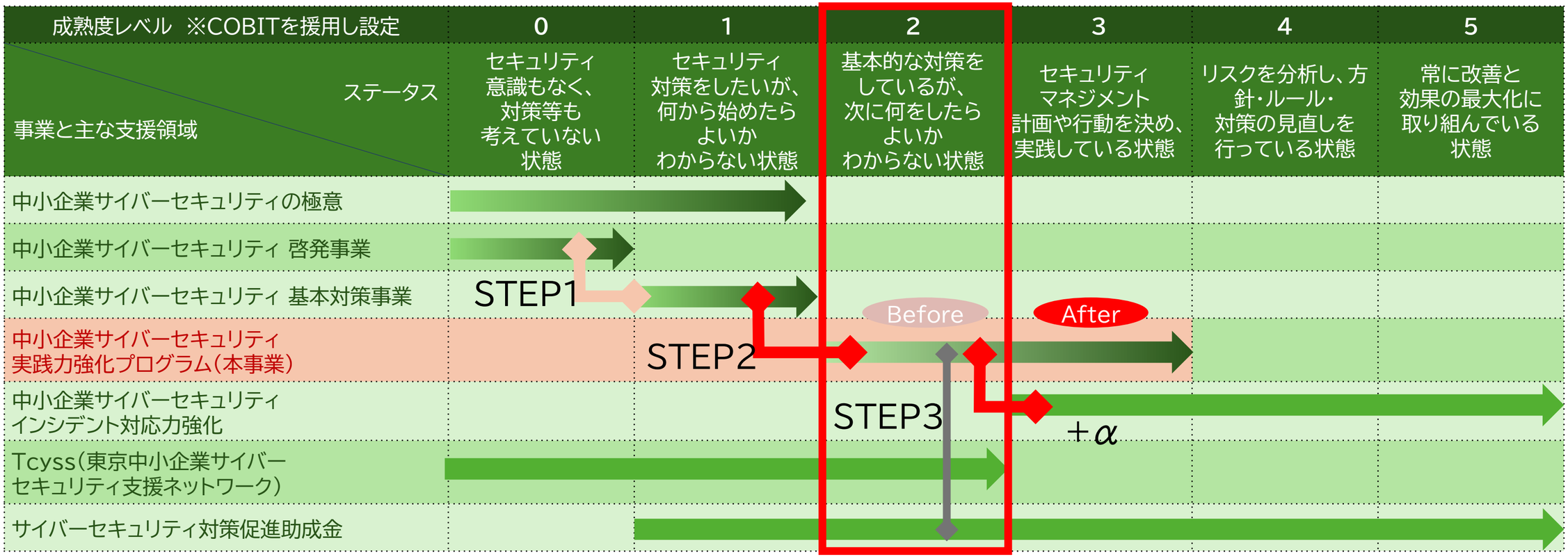
講師紹介

氏名	矢野　泰広（やの　よしひろ）
業務経歴	26年（セキュリティ経験：15年）
専門分野	情報セキュリティ、DX、ICT、クラウド技術、 ネットワーク技術、DB設計・構築、プロジェクト マネジメント、WEBシステム設計・構築、 サーバ設計・構築
保有資格	情報処理安全確保支援士（第004005号） 経済産業省認定 情報処理技術者試験 プロジェクトマネージャ 情報処理技術者第一種、情報処理技術者第二種 インターネット検定 .com Master ADVANCE★★ 生成AIパスポート 家電製品アドバイザー（AV情報家電・生活家電）
コメント	中小企業を中心にDX、ネットワーク、クラウド技術および情報セキュリティに関する構築や導入支援やコンサルティングの経験が豊富。併せて長年にわたり大手通信事業者のSE（技術営業）を対象に指導を行ってきた事から、幅広い業種、業態の企業の状況を認識しており、中小企業の課題点を的確に捉え、各企業が取り組みやすい解決策を提示する対応力に定評がある。

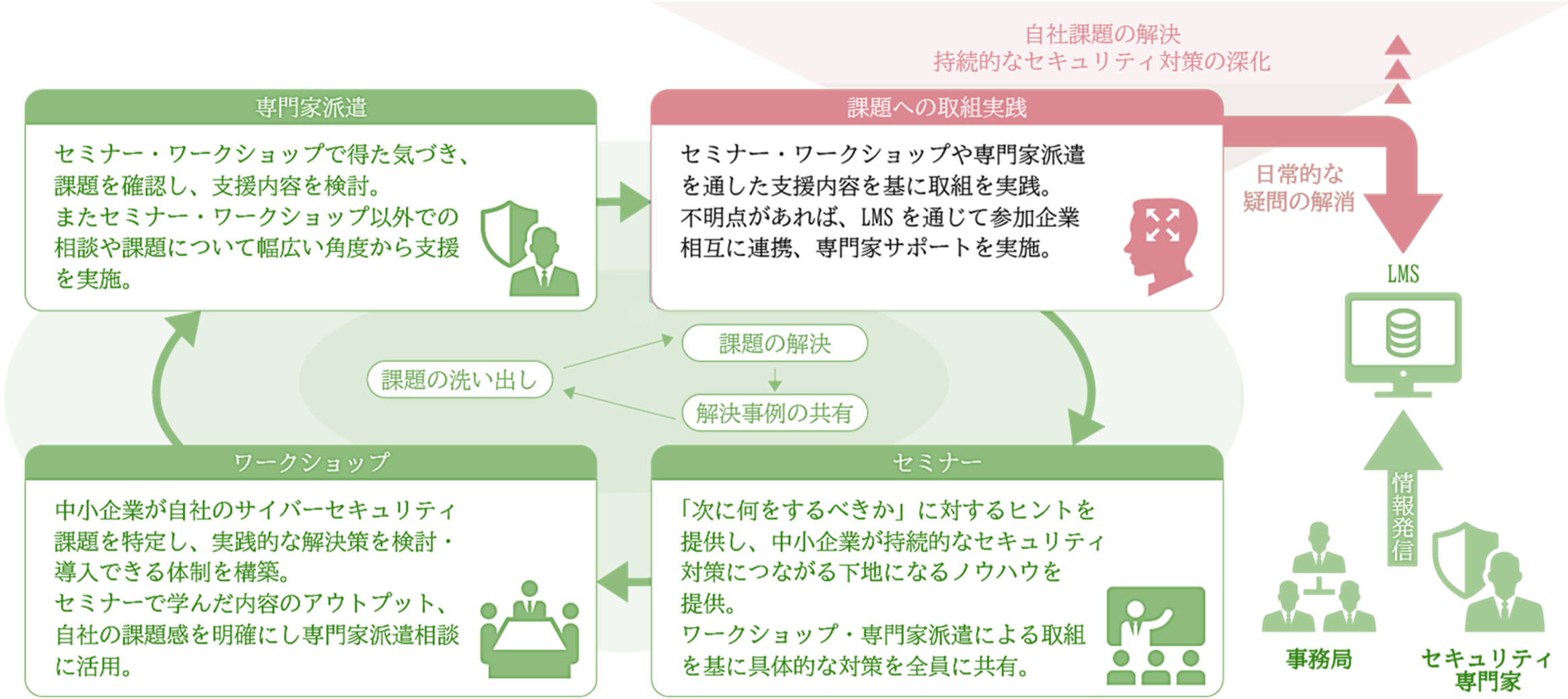
目的

- 継続的なセキュリティ対策の実施を支援する。
- 人材の育成と実践的な課題解決を通じて、サプライチェーン全体のセキュリティ強化を図る。

東京都他事業と本事業の位置づけ



支援内容の全体像


自社課題の解決
持続的なセキュリティ対策の深化
専門家派遣
セミナー・ワークショップで得た気づき、課題を確認し、支援内容を検討。
またセミナー・ワークショップ以外での相談や課題について幅広い角度から支援を実施。
課題への取組実践
セミナー・ワークショップや専門家派遣を通した支援内容を基に取組を実践。
不明点があれば、LMS を通じて参加企業相互に連携、専門家サポートを実施。
日常的な
疑問の解消
LMS
課題の解決
課題の洗い出し
解決事例の共有
ワークショップ
中小企業が自社のサイバーセキュリティ課題を特定し、実践的な解決策を検討・導入できる体制を構築。
セミナーで学んだ内容のアウトプット、自社の課題感を明確にし専門家派遣相談に活用。
セミナー
「次に何をするべきか」に対するヒントを提供し、中小企業が持続的なセキュリティ対策につながる下地になるノウハウを提供。
ワークショップ・専門家派遣による取組を基に具体的な対策を全員に共有。
情報発信
事務局
セキュリティ専門家

スケジュール

支援内容	7月	8月	9月	10月	11月	12月	1月	2月	3月
セミナー・ワークショップ（全10回）	7/25（金）	8/8（金） 8/27（水）	9/11（木） 9/25（木）	10/10（金） 10/27（月）	11/17（月）	12/12（金）	1/16（金）		
専門家派遣（全4回）	1回目		2回目	3回目		4回目			
事例集						ご参加いただいた企業様への取材	事例集作成期間	公表3月下旬～	

セミナー内容

実施回	編	テーマ
第1回 7/25 （金）	第0編	はじめに
	第1編	サイバーセキュリティを取り巻く背景
	第2編	中小企業に求められるデジタル化の推進とサイバーセキュリティ対策
第2回 8/8 （金）	第3編	これからの企業経営に必要なIT活用とサイバーセキュリティ対策
	第4編	セキュリティ事象に対応して組織として対策すべき対策基準と具体的な実施
	第5編	各種ガイドラインを参考にした対策の実施

セミナー内容

実施回		編	テーマ
第3回	8/27(水)	第6編	ISMSなどのフレームワークの種類と活用法の紹介
第4回 第5回	9/11(木) 9/25(木)	第7編	ISMSの構築と対策基準の策定と実施手順
第6回 第7回	10/10(金) 10/27(月)	第8編	具体的な構築・運用の実践
第8回	11/17(月)	第9編	中小企業が組織として実践するためのスキル・知識と人材育成
第9回	12/12(金)	第10編	サイバーレジリエンス能力の育成
第10回	2026年 1/16(金)	第11編	全体総括

第11章. セキュリティフレームワーク

セキュリティフレームワークの概要

情報セキュリティマネジメントシステム（ISMS）

サイバー・フィジカル・セキュリティ対策フレームワーク（CSF）

サイバーセキュリティ経営ガイドライン

セキュリティフレームワークの概要

【参照:テキスト11-1-1.】
P2～P3

セキュリティフレームワークの役割と重要性

セキュリティフレームワークの定義

セキュリティ対策を行うために定義された指針やセキュリティ対策基準、ガイドライン、ベストプラクティス集のことを指す

セキュリティフレームワークを利用するメリット

- 効果的なセキュリティ対策
- 信頼性の確保

セキュリティフレームワークの概要

【参照:テキスト11-1-1.】
P2～P3

代表的なセキュリティフレームワーク

	フレームワーク名		概要
1	ISMS	別途詳細	[ISO/IEC27001、ISO/IEC27002] 網羅的なセキュリティフレームワーク
2	ISO/IEC27017		クラウドサービス対象のセキュリティフレームワーク
3	CSF	別途詳細	重要インフラ対象のセキュリティフレームワーク
4	CPSF	別途詳細	Society5.0における産業社会が対象のセキュリティフレームワーク
5	サイバーセキュリティ経営ガイドライン	別途詳細	経営者を中心としたセキュリティ対策
6	PCI DSS		クレジットカード産業を対象としたデータセキュリティ基準
7	PMS		個人情報保護
8	CIS Controls		具体的なサイバー攻撃アプローチ
9	ISA/IEC62443		産業オートメーションおよび制御システム

フレームワーク選択の重要性

【参照：テキスト11-1-2.】
P3～P5

代表的なセキュリティフレームワークの概要

ISO/IEC27017

- 対象：クラウドサービスの提供者と利用者
- 目的：クラウドサービスのリスク低減、適切な利用のための組織体制の確立
- ISO/IEC27002をベースに作成
- ISO/IEC27001は情報セキュリティのマネジメントシステム規格
- ISO/IEC27017を通じて、ISO/IEC27001を強化し、クラウドサービス向けの情報セキュリティ管理体制の構築が可能

フレームワーク選択の重要性

【参照：テキスト11-1-2.】
P3～P5

代表的なセキュリティフレームワークの概要

PCI/DSS（国際的なクレジット産業向けのデータセキュリティ基準）

- 対象：　クレジットカード情報を取扱う全ての事業者
- 名称：　Payment Card Industry Data Security Standard
  （略称：PCI DSS）
- 目的：　カード会員情報の適切な管理
- 基準策定：国際カードブランド5社が共同で策定した国際基準
- 基準内容：ネットワークアーキテクチャ、ソフトウェアデザイン、
  セキュリティマネジメント、ポリシー、プロシジャなど
  12の要件で規定

フレームワーク選択の重要性

【参照：テキスト11-1-2.】
P3～P5

代表的なセキュリティフレームワークの概要

PMS（個人情報保護マネジメントシステム）

- 目的：　組織が取扱う個人情報の安全・適切な管理
- 規格：　JIS Q 15001
- 主な内容：　事業者が個人情報を適切に取扱う方法の規定
- プライバシー保護：　直接の目的ではないが、結果的に保護される
- PMSの基本：　個人情報保護方針の設定と、その方針に基づくPDCAサイクルの実行

フレームワーク選択の重要性

【参照：テキスト11-1-2.】
P3～P5

代表的なセキュリティフレームワークの概要

CIS Controls

- 目的：　サイバー攻撃の現状・傾向をもとに、組織のサイバーセキュリティ対策と優先順位を決定するフレームワーク
- 重点：　あらゆる企業の最も基本的・重要な対応
- 特徴：　ネットワークの詳細設定、ログ管理などの具体的・技術的対策が中心
- アプローチ：　多岐にわたる対策から、自社の実施すべき対策と優先順位を導出

フレームワーク選択の重要性

【参照：テキスト11-1-2.】
P3～P5

代表的なセキュリティフレームワークの概要

ISA/IEC62443

- 主題：　産業用自動制御システムのセキュリティ対策・プロセス要件の国際標準規格
- カバー範囲：　ISO/IEC 27001では十分にカバーされない工場やプラントの制御システムのセキュリティ
- 対象：　ソフトウェア・ハードウェアを含む制御関連のデータ処理基盤
- 特徴：　システムだけでなく、運用に関わる「人」と「業務」も対象

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト11-2.】
P6～P7

ISMSの概要

- 定義：　ISMSは情報セキュリティマネジメントシステムの略
- 目的：　組織の情報セキュリティリスクの適切な管理
- 地位：　国際規格の存在により、代表的なセキュリティフレームワークとして認識
- 達成目標：　情報の機密性、完全性、可用性をバランス良く維持・改善し、信頼を提供
- 対策範囲：　技術的対策、従業員教育・訓練、組織体制の整備を含む

情報セキュリティマネジメントシステム(ISMS)

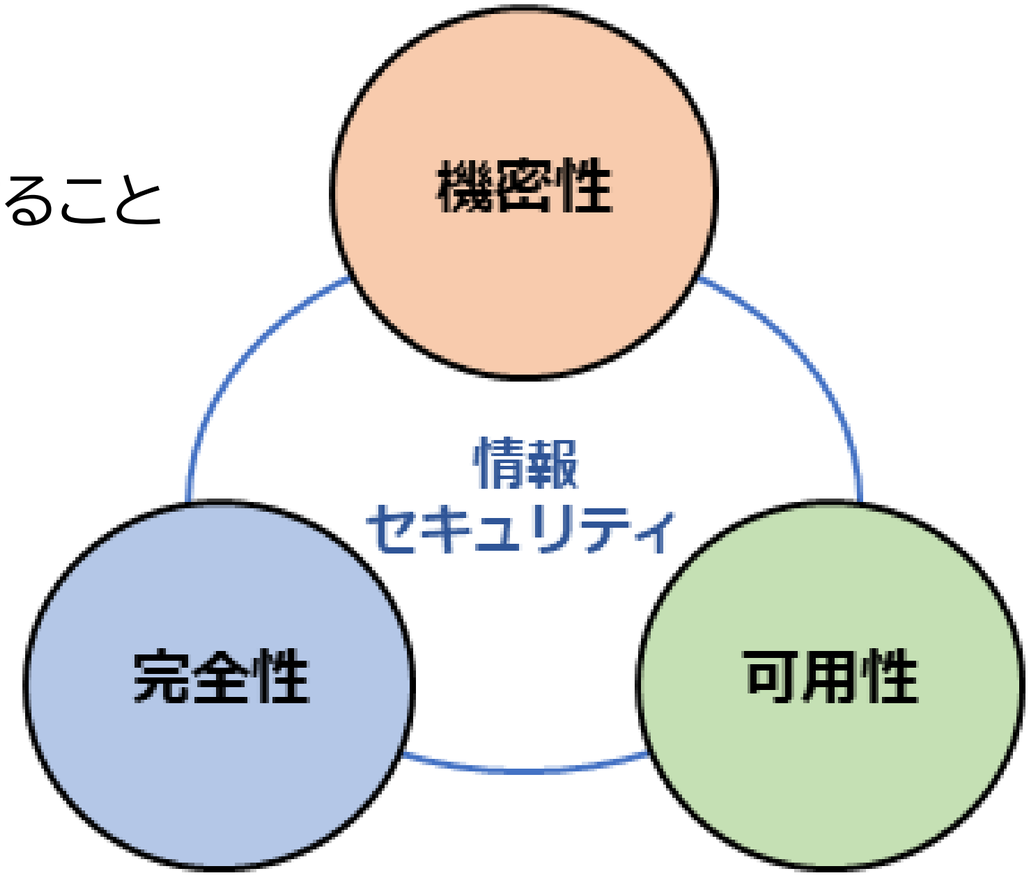
【参照:テキスト11-2.】
P6～P7

情報セキュリティの3要素(情報セキュリティのCIA)

機密性(Confidentiality)
　情報に対するアクセスを適切に管理すること

完全性(Integrity)
　情報が正確であり、完全である状態を保持すること

可用性(Availability)
　情報を必要な時に使えるようにしておくこと



情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト11-2.】
P6～P7

情報セキュリティの7要素　※3要素（CIA）＋追加4要素

真正性（Authenticity）
　情報にアクセスしているユーザー・端末が、許可された人物やシステムであることを明確にする状態

信頼性（Reliability）
　システムの処理やデータ操作が、欠陥や不具合なく実行されること

責任追跡性（Accountability）
　情報やシステムに対する操作が、誰によってどのように行われたのかを明確にすること

否認防止（non-repudiation）
　情報資産に関する問題が発生した際、その原因となる人物が、後から否認できないよう証明すること

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト11-2.】
P6～P7

ISO/IEC27001とJIS Q 27001

ISMSのための要求事項をまとめた国際規格が、ISO/IEC27001
ISO/IEC 27001を日本語訳し、日本産業規格としたものがJIS Q 27001

使用用途

- 組織のマネジメントおよび業務プロセスを取り巻くリスクの変化への対応
- 情報セキュリティ要求事項を満たす組織の能力を内外で評価するための基準

NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-1.】
P8～P15

CSF(Cybersecurity Framework)の概要

- CSFはNIST(米国国立標準技術研究所)が作成したサイバー攻撃対策のフレームワーク
- 防御だけでなく、検知・対応・復旧のインシデント対応が含まれる
- 要求事項は汎用的で、多様な企業に適用可能
- 指示書やノウハウ集ではない
- 利用方法は実施する組織に委ねられている
- CSFを理解し、サイバーセキュリティ対策の検討が必要

NISTサイバーセキュリティフレームワーク（CSF）

【参照：テキスト11-3-1.】
P8～P15

CSF2.0 の3つの構成要素

「コア」の概要
　サイバーセキュリティ対策の一覧

「ティア」の概要
　対策状況を数値化するための成熟度評価基準

「プロファイル」の概要
　サイバーセキュリティ対策の現状とあるべき姿を記述するためのフレームワーク

NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-1.】
P8～P15

コアとは

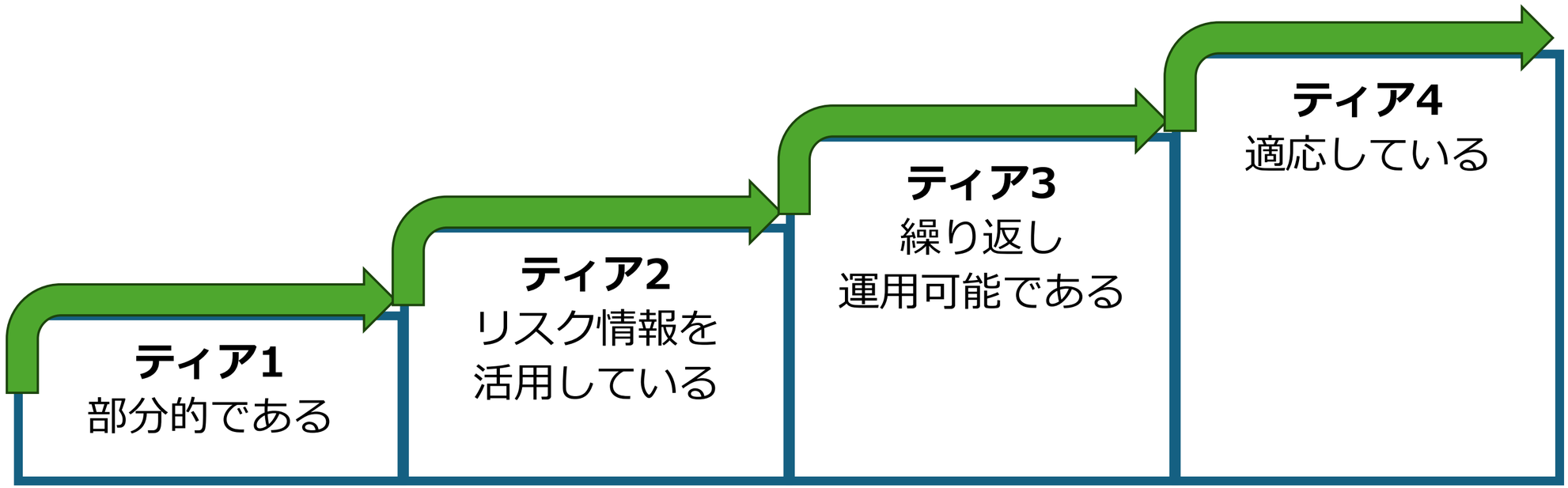
業種・業態や企業規模に依存しない共通のサイバーセキュリティ対策の一覧を定義したものであり、「識別」「防御」「検知」「対応」「復旧」「ガバナンス」の6つの機能に分類される。

NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-1.】
P8～P15

ティアとは

組織におけるサイバーセキュリティリスクへの対応状況を評価する際の指標を定義したものである。
指標はティア1～ティア4まで、下図のように定義が4段階ある。

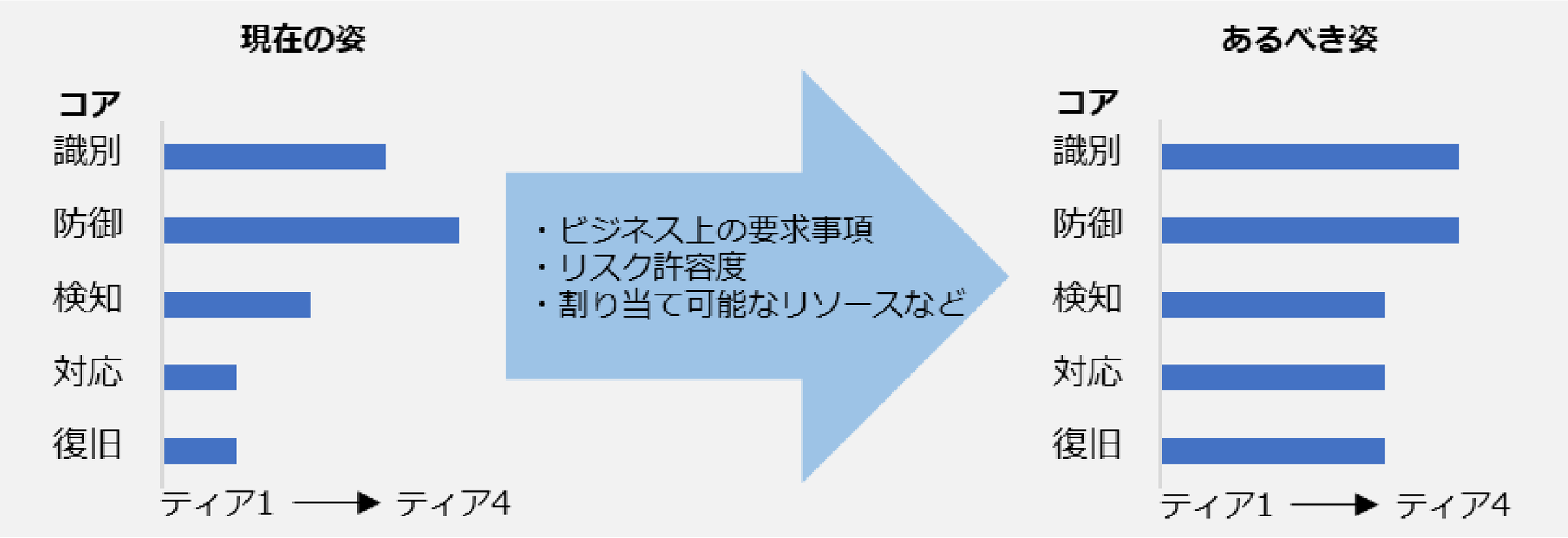


NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-1.】
P8～P15

プロファイルとは

組織ごとの考慮点を整理したもので、サイバーセキュリティ対策の現状と目標状態を明示することにより、必要な改善点のギャップを特定できる。
また、「あるべき姿」は、ビジネス要求やリスク許容度、リソースをもとに策定される。



NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-1.】
P8～P15

CSF 2.0 の特徴

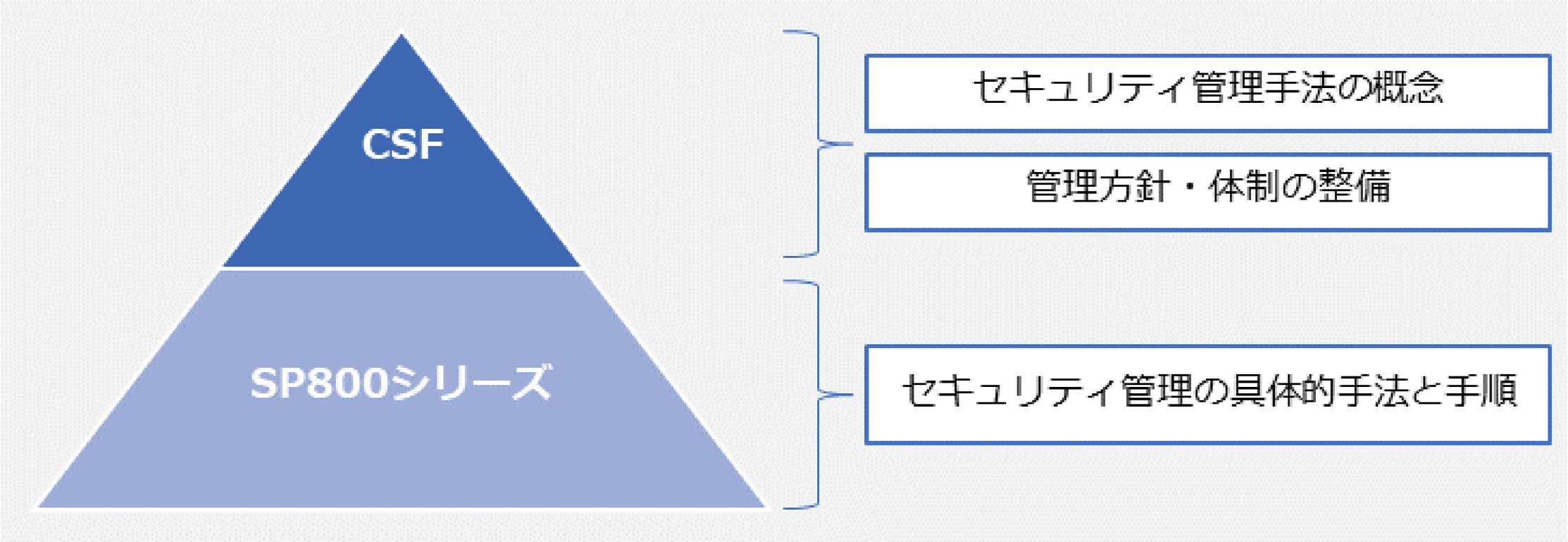
- フレームワークの適用範囲拡大
- 新たな機能「ガバナンス」の追加
- フレームワーク活用のためのコンテンツ強化
- サプライチェーンリスクマネジメントの強化

NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-2.】
P15～P16

NIST SP800シリーズとCSFの関連性

CSFの下位概念に位置づけられているのが、NIST SP800シリーズである。
実施すべきタスクと手順、推奨技術の特定など、セキュリティ管理の手法について具体的に明記されている。



NISTサイバーセキュリティフレームワーク（CSF）

【参照：テキスト11-3-3.】
P16～P17

CSFとISMSの関連性

主な共通点

- 汎用性が高い
- サイバーセキュリティ対策方法
- 任意性がある

主な相違点

- 第三者認証制度の有無
- 目標への到達手段

サイバー・フィジカル・セキュリティ対策フレームワーク

【参照:テキスト11-4.】
P18～P19

CPSFの概要

- Society5.0でサイバー空間とフィジカル空間が融合
- サプライチェーンが「価値創造過程」として変化
- 新しいサプライチェーンにはサイバー攻撃のリスク増
- 政府が「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）」を策定
- CPSFは既存のISMSやCSFをもとに、サイバーとフィジカルの両方のセキュリティ対応

サイバー・フィジカル・セキュリティ対策フレームワーク

【参照:テキスト11-4.】
P18～P19

CPSFの目的と適用範囲

目的

CPSFは新たな産業社会のバリュークリエイションプロセスを理解し、リスクを明確化し、セキュリティ対策を整理すること。

適用範囲

新たな産業社会のバリュークリエイションプロセス全体。

- **新たな産業社会における**バリュークリエイションプロセス全体が適用範囲
- それぞれの組織に応じてセキュリティ対策を選定することが可能

サイバー・フィジカル・セキュリティ対策フレームワーク

【参照:テキスト11-4.】
P18～P19

3層構造モデル

サイバー空間におけるつながり[第3層]

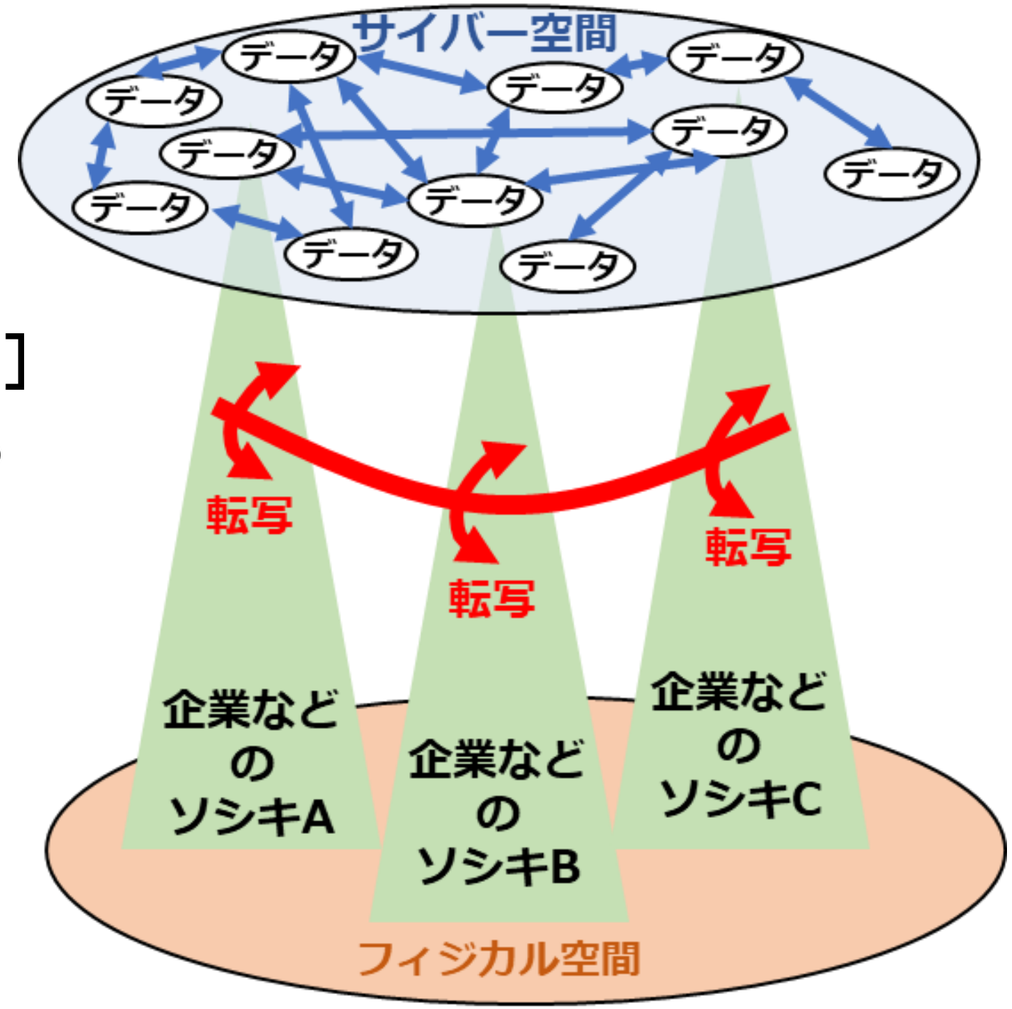
自由に流通し、加工・創造されるサービスを創造するためのデータの信頼性を確保

フィジカル空間とサイバー空間のつながり[第2層]

フィジカル空間・サイバー空間を正確に”転写”する機能の信頼性を確保
※現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラなどの信頼

企業間のつながり[第1層]

適切なマネジメントを基盤に各主体の信頼性を確保



サイバーセキュリティ経営ガイドライン

【参照:テキスト11-5-1.】
P20～P25

経営者が認識するべき3原則

原則1	経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
原則2	サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先など、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
原則3	平時および緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

サイバーセキュリティ経営ガイドライン

【参照:テキスト11-5-1.】
P20～P25

経営の重要10項目(指示1～6)

サイバーセキュリティリスクの管理体制構築

- 指示1　サイバーセキュリティリスクの**認識、組織全体での対応方針の策定**
- 指示2　サイバーセキュリティリスク**管理体制の構築**
- 指示3　サイバーセキュリティ対策のための**資源(予算、人材など)確保**

サイバーセキュリティリスクの特定と対策の実装

- 指示4　サイバーセキュリティリスクの**把握とリスク対応に関する計画の策定**
- 指示5　サイバーセキュリティリスクに**効果的に対応する仕組みの構築**
- 指示6　PDCAサイクルによるサイバーセキュリティ対策の**継続的改善**

サイバーセキュリティ経営ガイドライン

【参照：テキスト11-5-1.】
P20～P25

経営の重要10項目（指示7～10）

インシデント発生に備えた体制構築

指示7　インシデント発生時の**緊急対応体制の整備**

指示8　インシデントによる被害に備えた**事業継続・復旧体制の整備**

サプライチェーンセキュリティ対策の推進

指示9　ビジネスパートナーや委託先などを含めた**サプライチェーン全体の状況把握および対策**

ステークホルダーを含めた関係者とのコミュニケーションの推進

指示10　サイバーセキュリティに関する**情報の収集、共有および開示の促進**

サイバーセキュリティ経営ガイドライン

【参照:テキスト11-5-2.】
P25～P26

ガイドラインの読み方（経営者）

役割

- 「3原則」の理解
- 重要10項目について、情報セキュリティ対策の責任者に指示を出す
- リーダーシップの発揮

認識すべきこと

- ERMにサイバー攻撃のリスクを含めること
- サプライチェーン上のリスクを認識すること
- サイバーセキュリティ対策は担当者に丸投げしてはいけない
- サイバーセキュリティ対策は投資と位置づけること

サイバーセキュリティ経営ガイドライン

【参照:テキスト11-5-2.】
P25～P26

ガイドラインの読み方（担当幹部）

役割

- 重要10項目を理解すること
- 経営者に対して適宜状況報告を行い、経営者が適切な判断を行うために必要な情報を提供すること

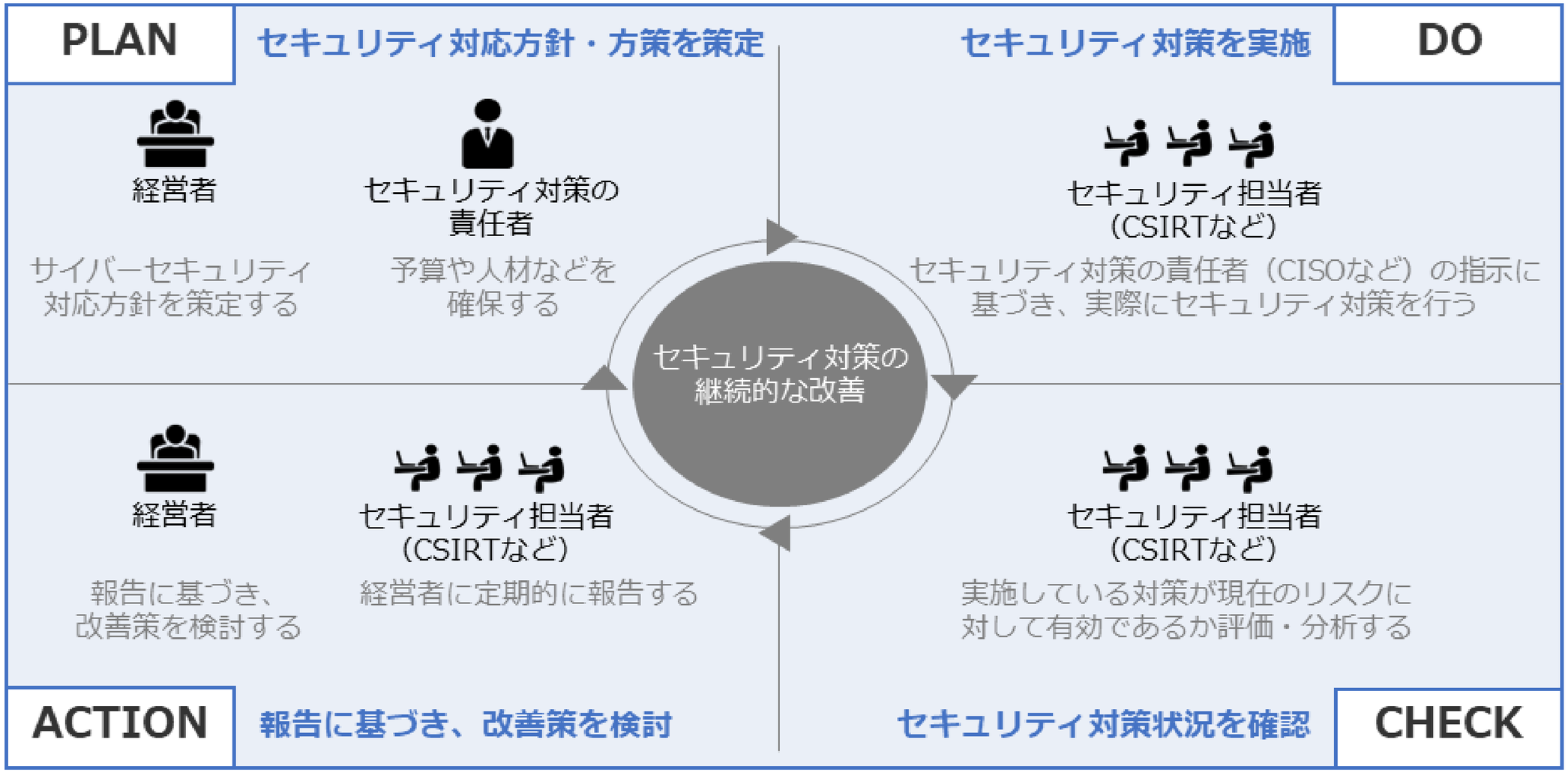
認識すべきこと

- 経営者から指示される内容に関して、より具体的な取組を検討し、セキュリティ担当者に対して指示をする必要があること

サイバーセキュリティ経営ガイドライン

【参照:テキスト11-5-3.】
P27～P28

サイバーセキュリティ経営ガイドラインの実践の流れ



第12章. リスクマネジメント

リスクマネジメント：概要

リスクマネジメント：リスクアセスメント

リスクマネジメント：リスク対応

リスクマネジメント：概要

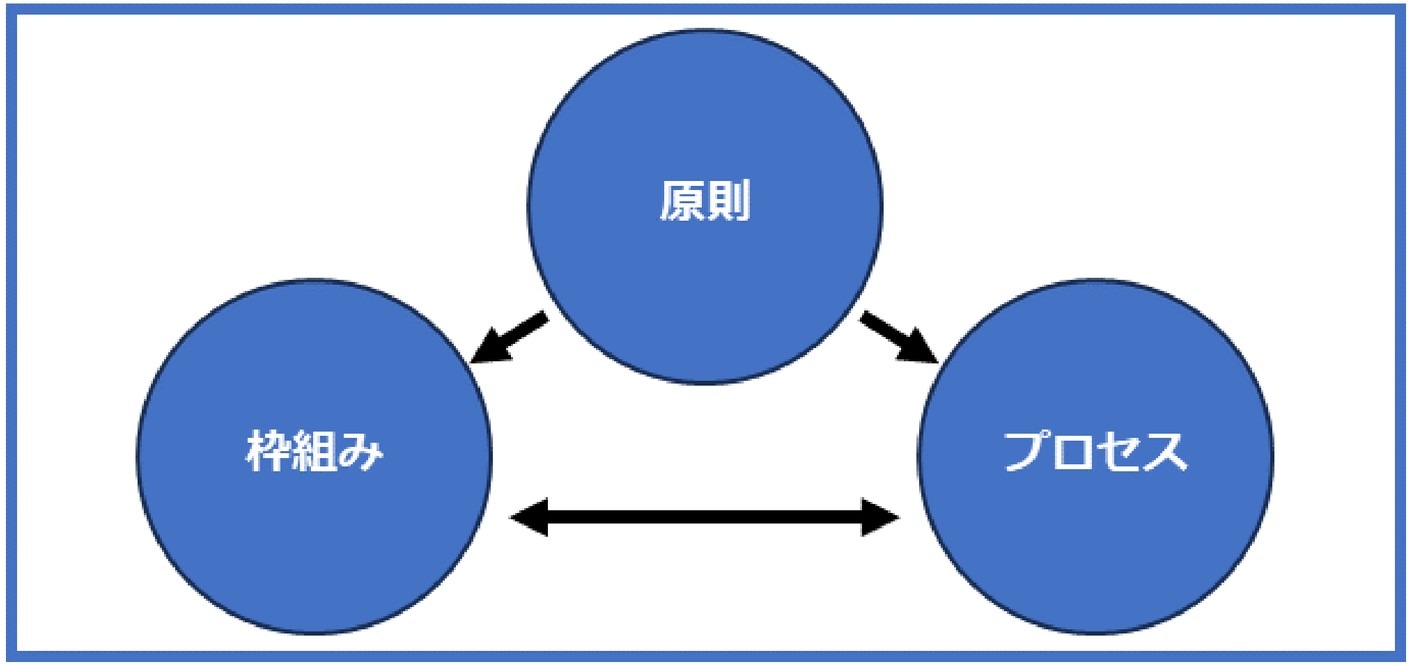
【参照：テキスト12-1-1.】
P30

リスクマネジメントプロセス（ISO31000）

リスクマネジメントとは

存在するリスクを効率的に管理し、発生する可能性がある損失を回避したり低減したりするプロセス全体のこと

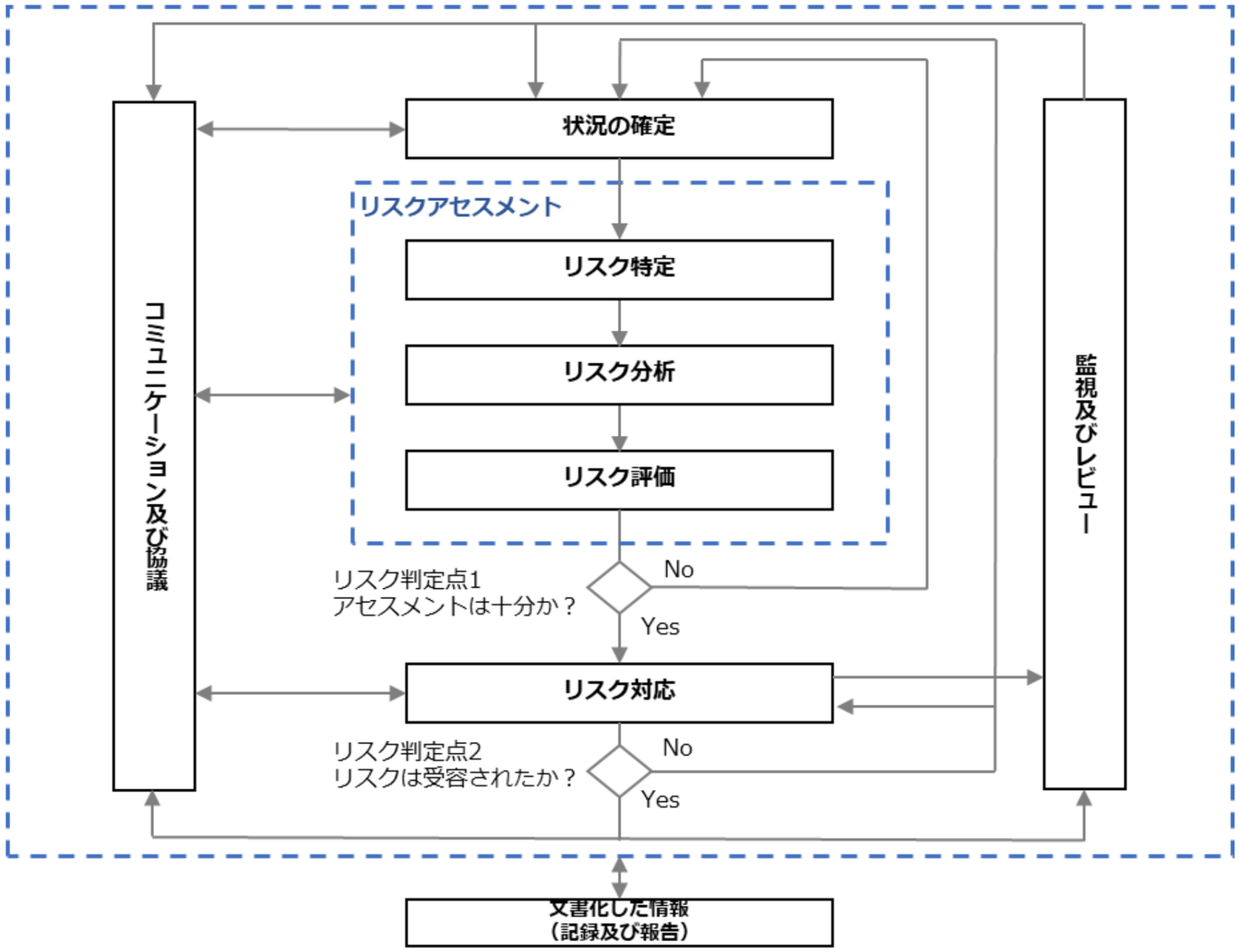
ISO31000での構成要素



リスクマネジメント：概要

【参照：テキスト12-1-2.】
P31～P33

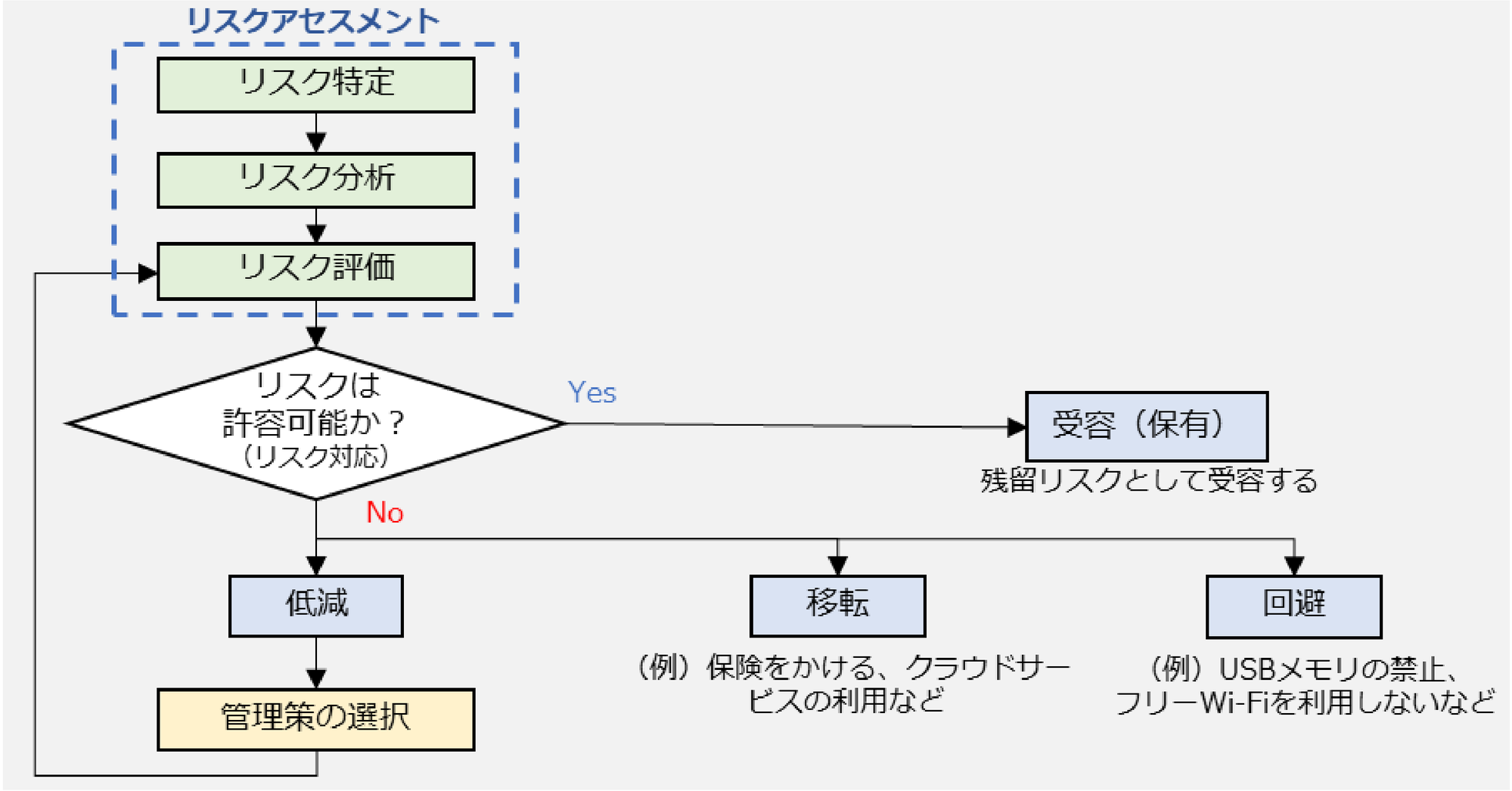
情報セキュリティリスクマネジメント（ISO/IEC27005）



リスクマネジメント：概要

【参照：テキスト12-1-2.】
P31～P33

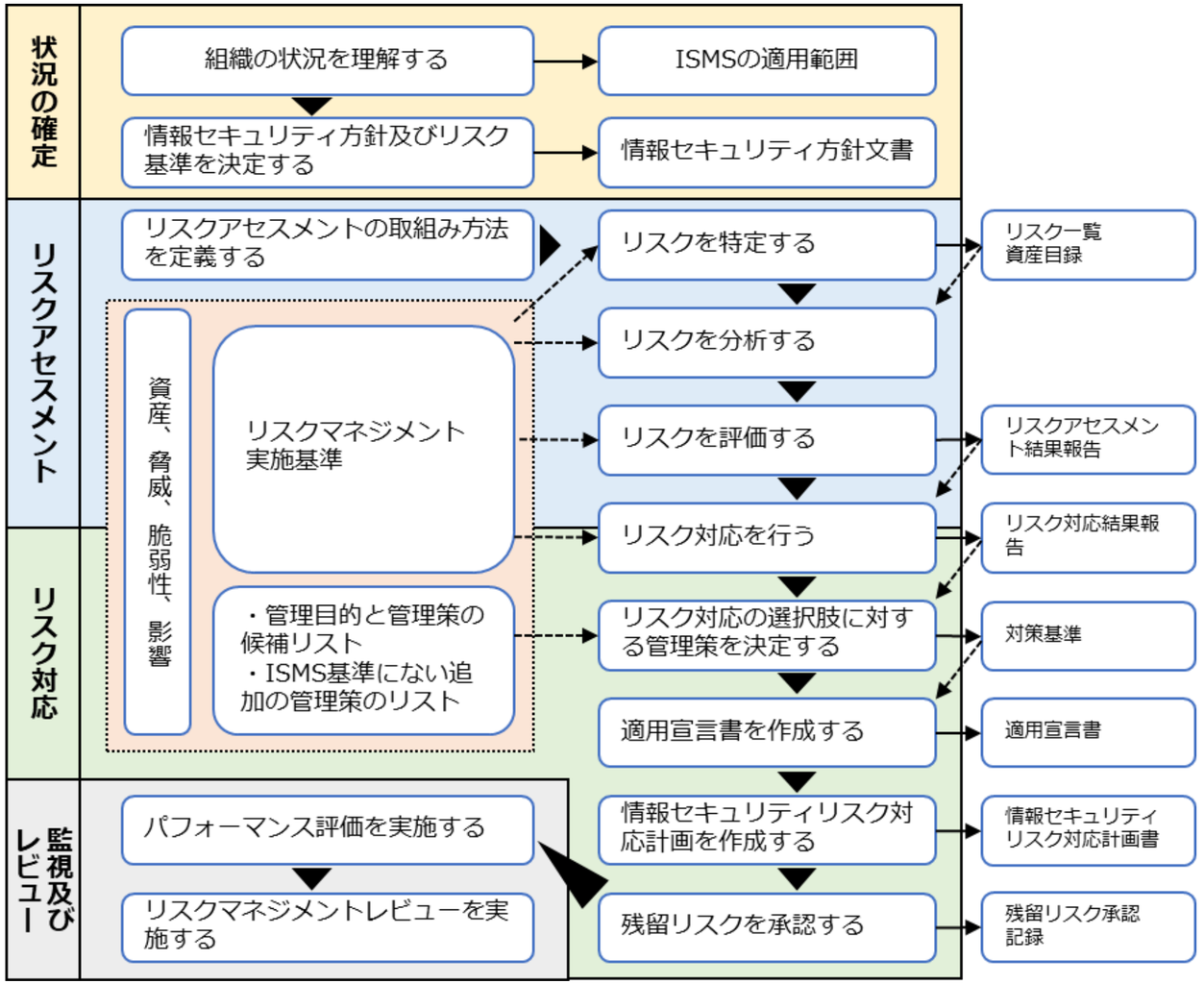
情報セキュリティリスクマネジメント（ISO/IEC27005）



リスクマネジメント：概要

【参照：テキスト12-1-3.】
P33

ISO/IEC 27001におけるリスクマネジメント手順



リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-1.】
P34

リスク基準の確立

必要なリスク基準

状況の確定
- 組織の状況を把握する
- **リスク基準を策定する**

リスクの特定
- リスクを発見、認識、記述する

リスクの分析
- 特定されたリスクのリスクレベルを算出する

リスクの評価
- **リスク分析の結果をリスク基準と比較する**
- **対策の必要性の有無、優先順位を決定する**

リスク対応
- **リスク対応計画を策定する**

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P34～P41

リスク特定

アプローチ手法と特徴

- 資産ベースのアプローチ
- 事象ベースのアプローチ
- リスク所有者の特定

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P34～P41

リスク特定(資産ベースのアプローチ)

アプローチ手法

情報資産の洗い出し

↓

機密性・完全性・可用性が損なわれた場合の影響度を評価

↓

影響度の評価をもとに重要度を算定

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P34～P41

リスク特定(資産ベースのアプローチ)

情報資産の洗い出し(例)

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
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	事務所PC
人事	健康診断の結果	顧入時・定期健康診断	人事部	人事部長	人事部	書類
経理	給与システムデータ	税務署提出用 源泉徴収票	給与計算担当	経理部長	人事部	事務所PC
経理	当社宛請求書	当社宛請求書の原本(過去3年分)	総務部	経理部長	総務部	書類
経理	発行済請求書控え	当社発行の請求書の控え(過去3年分)	総務部	経理部長	総務部	書類
営業	顧客リスト	得意先(直近5年間に実績があるもの)	営業部	営業部長	営業部	可搬電子媒体
営業	受注伝票	受注伝票(過去10年分)	営業部	営業部長	営業部	社内サーバ
営業	受注契約書	受注契約書原本(過去10年分)	営業部	営業部長	営業部	書類

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P34～P41

リスク特定(資産ベースのアプローチ)

機密性・完全性・可用性が損なわれた場合の影響度を評価

評価値		評価基準	該当する情報の例
機密性	3	法律で安全管理(漏えい、滅失又はき損防止)が義務付けられている	• 個人情報(個人情報保護法で定義) • 特定個人情報 (マイナンバーを含む個人情報)
		守秘義務の対象や限定提供データとして指定されている 漏えいすると取引先や顧客に大きな影響がある	• 取引先から秘密として提供された情報 • 取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき (不正競争防止法による保護を受けるため) 漏えいすると自社に深刻な影響がある	• 自社の独自技術・ノウハウ • 取引先リスト • 特許出願前の発明情報
	2	漏えいすると事業に大きな影響がある	• 見積書、仕入価格など顧客(取引先)との商取引に関する情報
	1	漏えいしても事業にほとんど影響はない	• 自社製品カタログ • ホームページ掲載情報

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P34～P41

リスク特定(資産ベースのアプローチ)

機密性・完全性・可用性が損なわれた場合の影響度を評価

評価値		評価基準	該当する情報の例
完全性	3	法律で安全管理(漏えい、滅失又はき損防止)が義務付けられている	• 個人情報(個人情報保護法で定義) • 特定個人情報(マイナンバーを含む個人情報)
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	• 取引先から処理を委託された会計情報 • 取引先の口座情報 • 顧客から製造を委託された設計図
	2	改ざんされると事業に大きな影響がある	• 自社の会計情報 • 受発注・決済・契約情報 • ホームページ掲載情報
	1	改ざんされても事業にほとんど影響はない	• 廃版製品カタログデータ

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P34～P41

リスク特定(資産ベースのアプローチ)

機密性・完全性・可用性が損なわれた場合の影響度を評価

評価値		評価基準	該当する情報の例
可用性	3	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	• 顧客に提供しているECサイト • 顧客に提供しているクラウドサービス
	2	利用できなくなると事業に大きな影響がある	• 製品の設計図 • 商品・サービスに関するコンテンツ(インターネット向け事業の場合)
	1	利用できなくなっても事業にほとんど影響はない	• 廃版製品カタログ

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P34～P41

リスク特定(資産ベースのアプローチ)

影響度の評価をもとに重要度を算定

重要度	情報資産の価値・事故の影響の大きさ
3	事故が起きると、 「 法的責任を問われる」 「 取引先、顧客、個人に大きな影響がある」 「 事業に深刻な影響を及ぼす」 など、企業の存続を左右しかねない
2	事故が企業の事業に重大な影響を及ぼす
1	事故が発生しても事業にほとんど影響はない

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P34～P41

リスク特定(事象ベースのアプローチ)

アプローチ手法

①リスクの特定	業務プロセスや取扱っている重要な資産に対して、業務上起きたら困ること(リスク)もしくは、過去に発生して業務に影響を及ぼしたことを記載します。 例) 「ネットワーク生涯により、リモートによる会議が中断もしくは実施できなくないり、取引先や顧客に及ぼす恐れ」

②リスク所有者の特定	①で特定されたリスクの所有者を記載します。

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P34～P41

リスク特定(事象ベースのアプローチ)

リスク特定【例】

ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ

評価値			重要度	リスク所有者
機密性	情報が漏えいする類の事象ではない	1	3	○○○○
完全性	ネットワーク障害の原因がサイバー攻撃やマルウェアの場合、情報が被害を受ける可能性がある事象である	3		
可用性	ネットワークが利用できなくなり、自社や取引先、顧客に大きな影響をおよぼす事象である	3		

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-3.】
P41～P42

リスクの分析

リスク分析の例

「リスクレベル」＝「重要度」×「被害発生可能性」

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-3.】
P41～P42

リスクの分析

被害発生可能性とは

起こりやすさ（脅威）	
3	通常の状況で脅威が発生する （いつ発生してもおかしくない）
2	特定の状況で脅威が発生する （年に数回程度）
1	通常の状況で脅威が発生することはない （通常発生しない）

つけ込みやすさ（脆弱性）	
3	対策を実施していない （ほぼ無防備）
2	部分的に対策を実施している （一部対策を実施）
1	必要な対策をすべて実施している （対策を実施）

「起こりやすさ（脅威）」と「つけ込みやすさ（脆弱性）」の換算表で算出する

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-3.】
P41～P42

リスクの分析

被害発生可能性の換算表

被害発生可能性		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

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-4.】
P43～P44

リスクの評価

「リスクレベル」＝「重要度」×「被害発生可能性」

リスク評価(例)

リスクレベル評価値		被害発生可能性		
		3	2	1
重要度	3	9	6	3
	2	6	4	2
	1	3	2	1

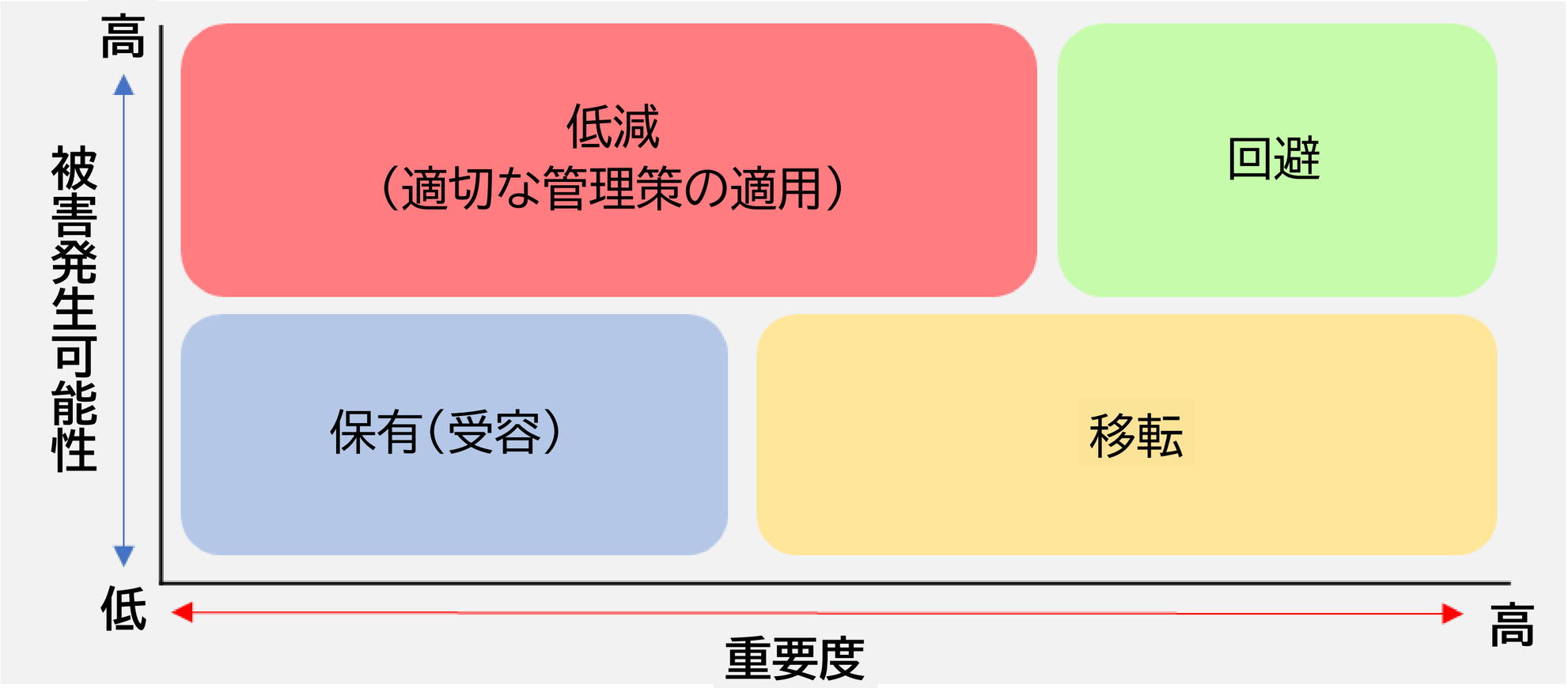
リスクレベル	リスク評価	記述
低	そのままで受容可能	それ以上の活動なしにリスクを受容可能
中	管理下で受容可能	リスクマネジメントの観点からフォローアップを実施し、中長期にわたる継続的改善の枠組みにおいて活動を設定することが望ましい
高	受容できない	リスクを低減するための対策を短期間で行うことが絶対に望ましい そうでない場合、活動の全部又は一部を拒否することが望ましい

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-4.】
P43～P44

対応策の検討

リスク対応の選択肢の選定方法

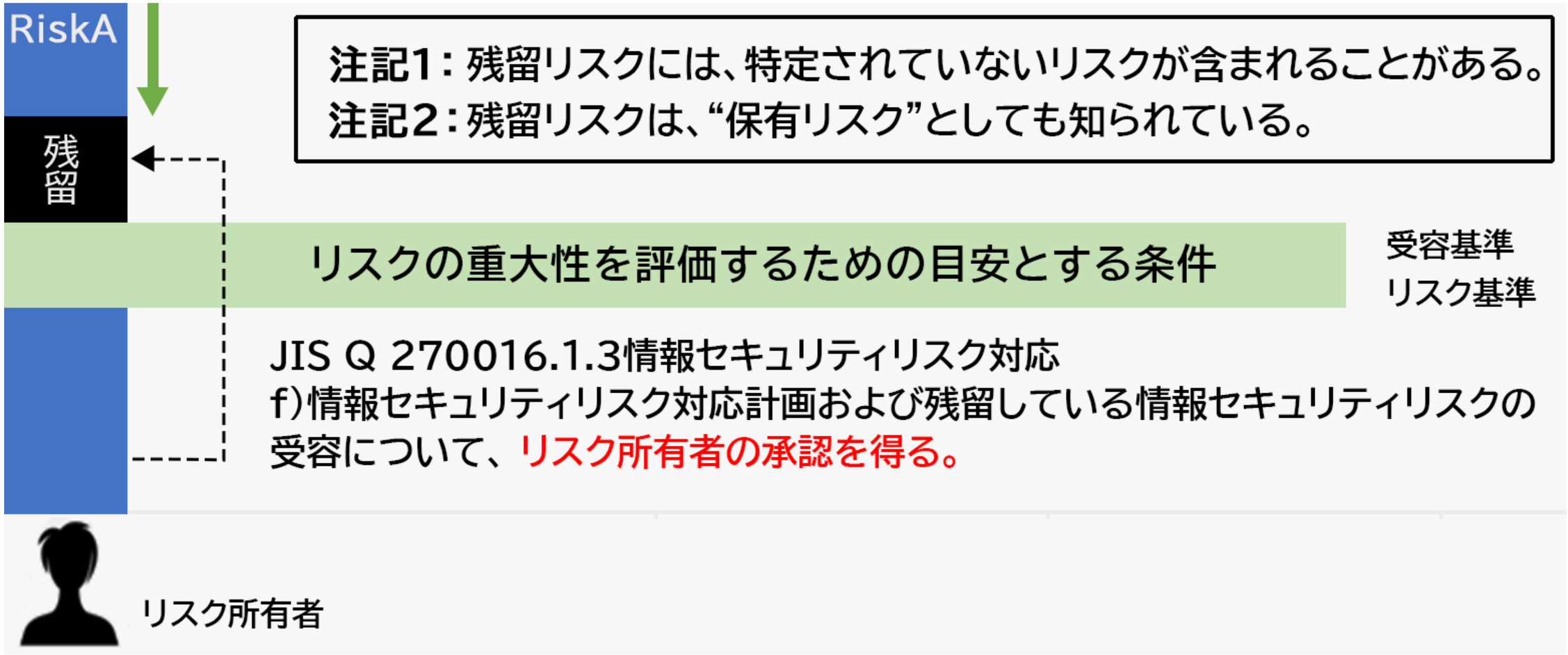


リスクマネジメント:リスクアセスメント

【参照:テキスト12-3.】
P45～P47

対応策の検討

残留リスク



令和7年度
中小企業サイバーセキュリティ
実践力強化プログラム

東京都産業労働局