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

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

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．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）
[ISO/IEC27001:2022, 27002:2022]

NISTサイバーセキュリティフレームワーク（CSF）

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）

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：セミナーテキスト7-1-1.】
第7章 - 02

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します。

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：セミナーテキスト7-1-1.】
第7章 - 02

代表的なセキュリティフレームワークの紹介

項番	フレームワーク名	概要
1	ISMS 別途詳細	[ISO/IEC27001,27002] 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

セキュリティフレームワークの選択の重要性

【参照：セミナーテキスト7-1-2.】
第7章 - 03

代表的なセキュリティフレームワークの概要

ISO/IEC27017

- クラウドサービスの情報セキュリティ対策のガイドライン規格が存在。
- ISO/IEC27002をベースに作成。
- 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/IEC 27001は情報セキュリティのマネジメントシステム規格。
- ISO/IEC 27017を通じて、ISO/IEC 27001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。

セキュリティフレームワークの選択の重要性

【参照：セミナーテキスト7-1-2.】
第7章 - 04

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）

- 国際カードブランド5社が共同で策定した国際基準。
- 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。
- 12の要件で規定。

セキュリティフレームワークの選択の重要性

【参照：セミナーテキスト7-1-2.】
第7章 - 04

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：組織が取り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り扱う方法の規定。
- 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。

セキュリティフレームワークの選択の重要性

【参照：セミナーテキスト7-1-2.】
第7章 - 04

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・傾向を基に、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。

セキュリティフレームワークの選択の重要性

【参照：セミナーテキスト7-1-2.】
第7章 - 04

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：セミナーテキスト7-2-1.】
第7章 - 05

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）

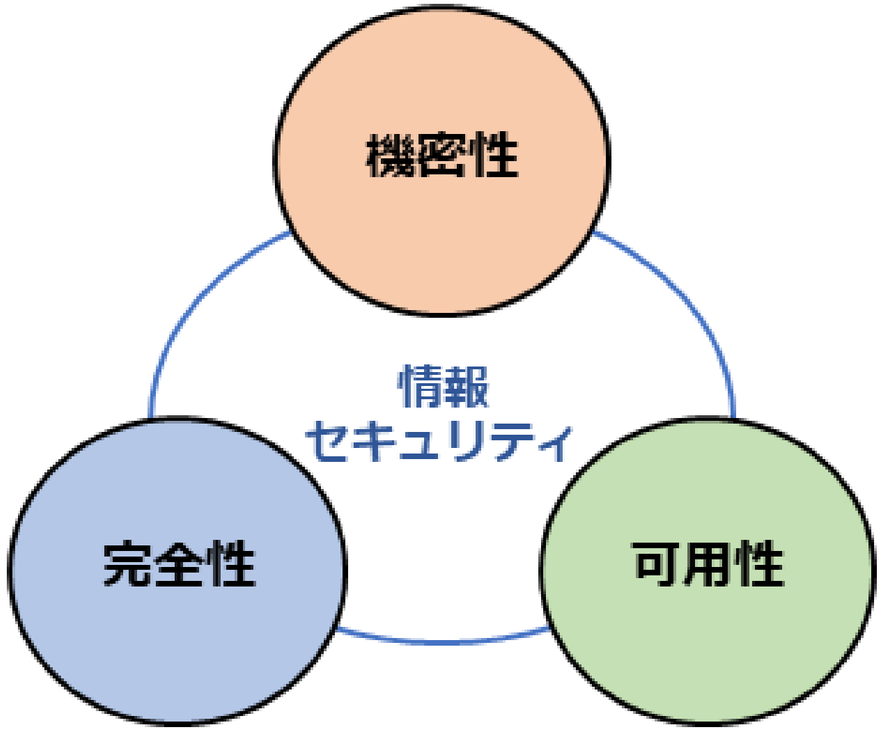
【参照：セミナーテキスト7-2-1.】
第7章 - 05

情報セキュリティの3要素

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



情報セキュリティの3要素
（出典）ISMS-AC「ISMS適合性評価制度」を基に作成

情報セキュリティマネジメントシステム（ISMS）

【参照：セミナーテキスト7-2-1.】
第7章 - 06

ISO/IEC 27001とJIS Q 27001

ISMSのための要求事項をまとめた国際規格が、ISO/IEC 27001
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

情報セキュリティマネジメントシステム（ISMS）

【参照：セミナーテキスト7-2-2.】
第7章 - 07

ISMSの要求事項

ISMS認証取得するために必ず対応し、PDCAの運用サイクルで
情報セキュリティマネジメントを実施すること

要求事項
1. 適用範囲
2. 引用規格
3. 用語および定義

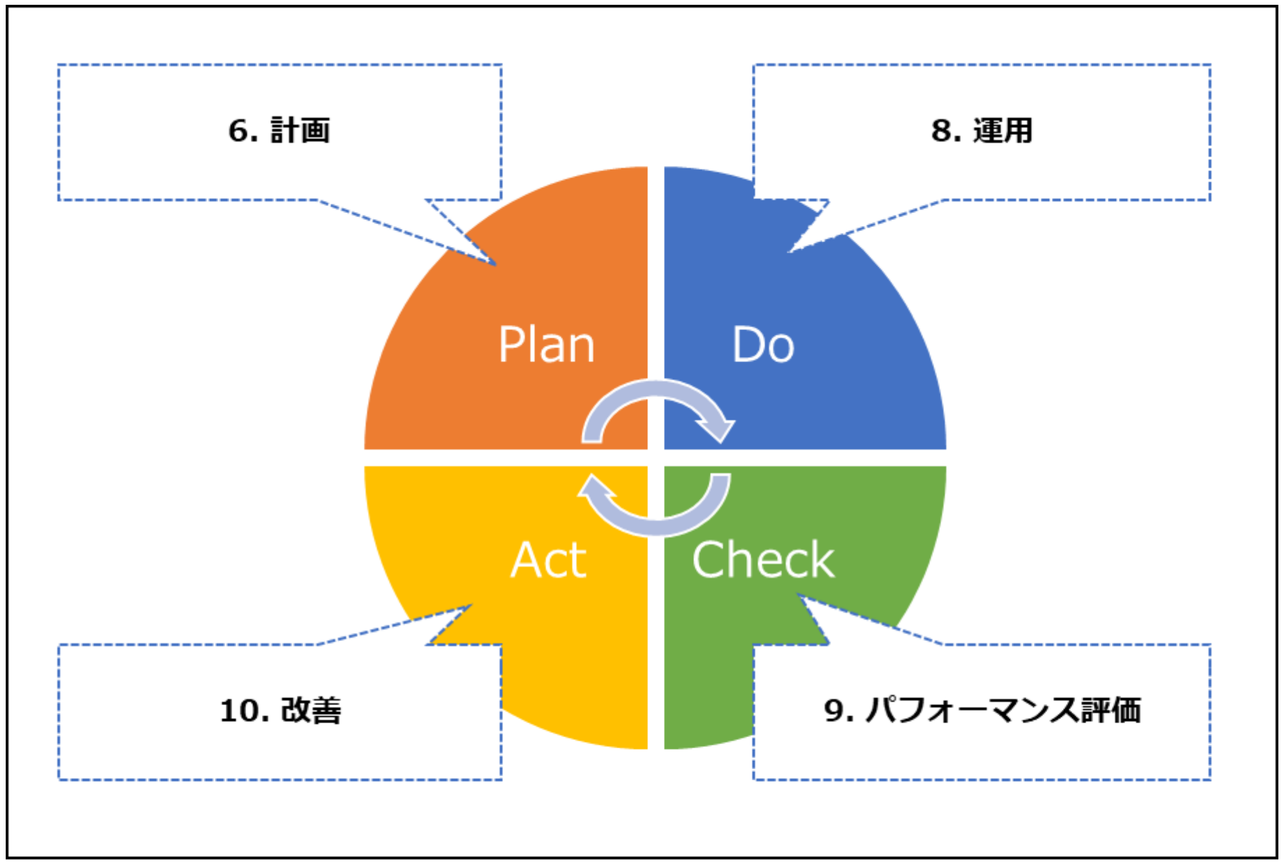
4. 組織の状況
5. リーダーシップ
6. 計画
7. 支援
8. 運用
9. パフォーマンス評価
10. 改善

実質的な要求事項

情報セキュリティマネジメントシステム（ISMS）【参照：セミナーテキスト7-2-2.】第7章 - 08

ISMSの運用プロセス

マネジメントシステムは組織の目標達成のための管理の仕組み。ISMSは情報セキュリティと機密情報の保護を目的とし、そのための方法としてPDCAサイクルを繰り返してスパイラルアップすることがISO/IEC 27001で要求される。

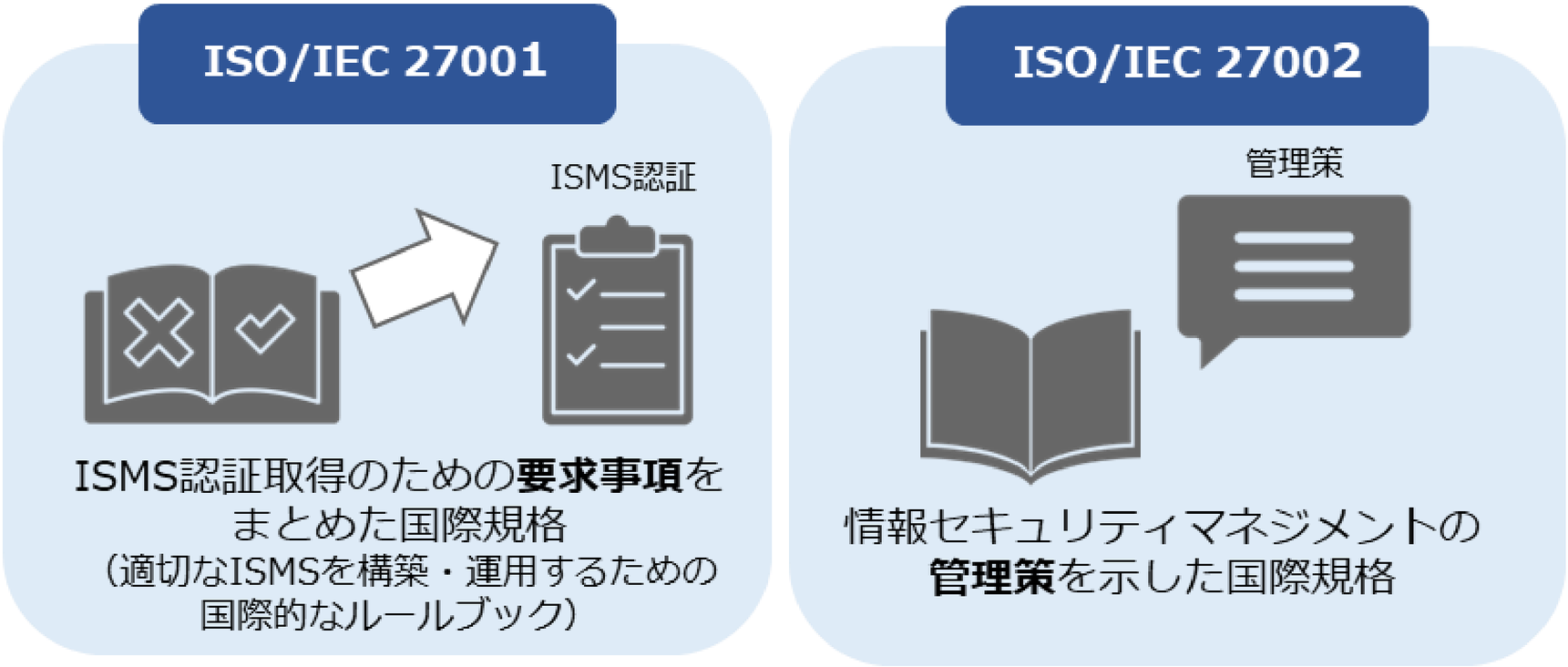


情報セキュリティマネジメントシステム（ISMS）

【参照：セミナーテキスト7-2-2.】
第7章 - 09

ISO/IEC 27001 と ISO/IEC 27002

ISO/IEC 27002は情報セキュリティの管理策を示す規格で、ISO/IEC 27001の付属書Aに反映されている。管理策は具体的な状況に応じて選択・適用され、93の管理策は4つのカテゴリに分けられている。



情報セキュリティマネジメントシステム（ISMS）

【参照：セミナーテキスト7-2-2.】
第7章 - 09

ISMSの管理策

管理策は次の4つのテーマにグループ分けされるようになった。

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

情報セキュリティマネジメントシステム（ISMS）

【参照：セミナーテキスト7-2-2.】
第7章 - 12

ISMSの管理策における属性

ISO 27002 の最新版では、カテゴリー分類をしやすくするため、
管理策に5種類の「属性」が追加されている。

管理策における属性	
属性	**概要**
管理策のタイプ	予防、検知、是正
情報セキュリティ資産	機密性、完全性、可用性
サイバーセキュリティの概念	識別、防御、検知、対応、復旧
運用能力	ガバナンス、資産管理、情報保護、人的資産のセキュリティ、システムおよびネットワークセキュリティ、アプリケーションのセキュリティなど
セキュリティドメイン	ガバナンスとエコシステム、保護、防御、対応力

情報セキュリティマネジメントシステム（ISMS）

【参照：セミナーテキスト7-2-3.】
第7章 - 13

ISMSの構築

ISMS実装のためのステップ

1. 適用範囲の決定
2. 情報セキュリティ方針の策定
3. 体制の確立
4. ISMS文書の作成
5. リスクアセスメントの実施
6. 従業員の教育
7. 内部監査
8. マネジメントレビュー

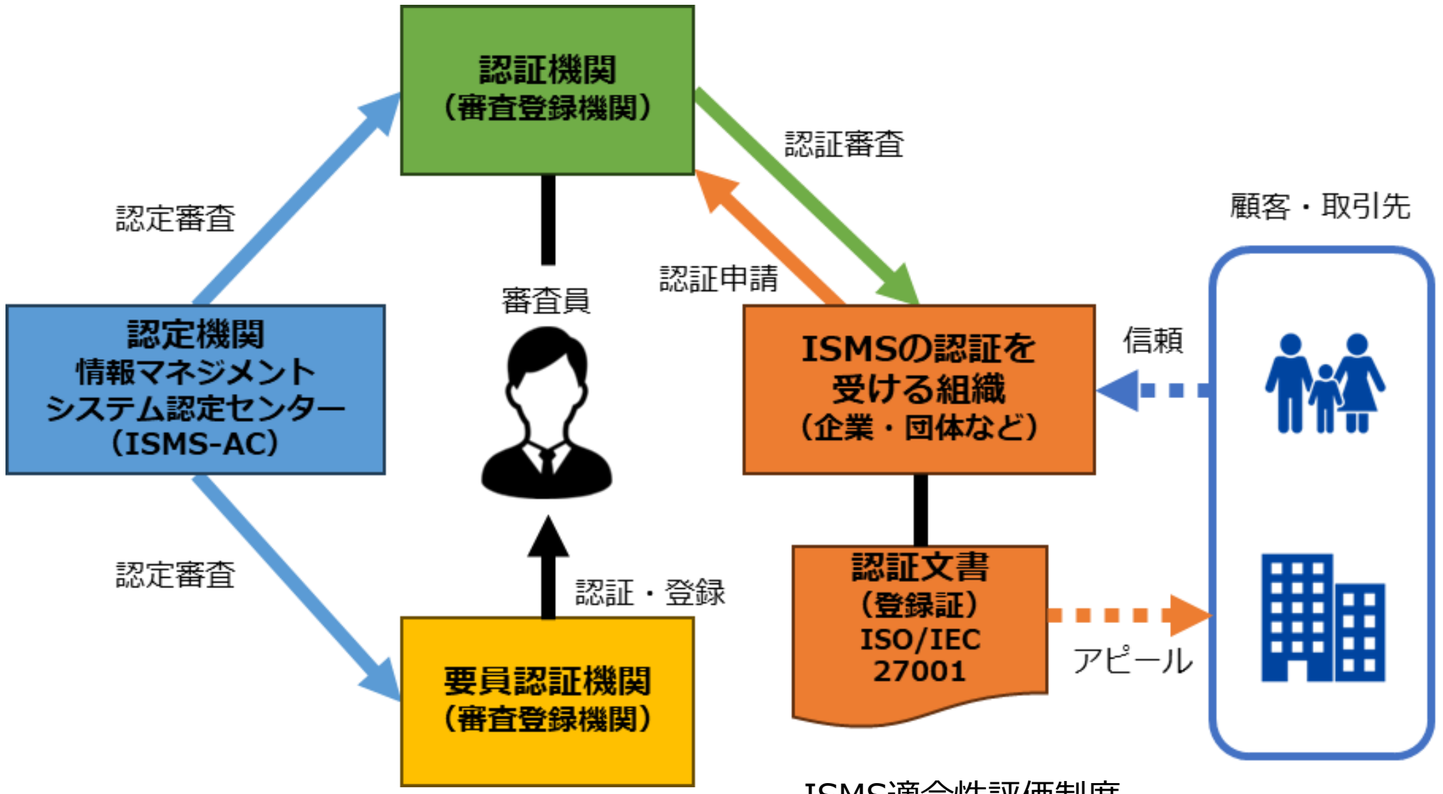
情報セキュリティマネジメントシステム（ISMS）【参照：セミナーテキスト7-2-3.】第7章 - 14

ISMSの実装と認証

「ISMS認証」は、組織のISMSがISO/IEC 27001に準拠しているかを第三者認証機関が審査する制度。この評価は国際的な「ISMS適合性評価制度」のもとで行われます。

認定と認証

認定	認定機関が認証機関を審査し、認証を遂行する能力のあることを公式に承認する行為を認定と言います。
認証	第三者が文書で保証する手続きを認証と言います。



ISMS適合性評価制度
（出典）ISMS-AC「ISMS適合性評価制度」を基に作成

情報セキュリティマネジメントシステム（ISMS）

【参照：セミナーテキスト7-2-3.】
第7章 - 15

ISMS認証審査プロセス

ISMSの認証審査は、次のようなステップで実施されます。

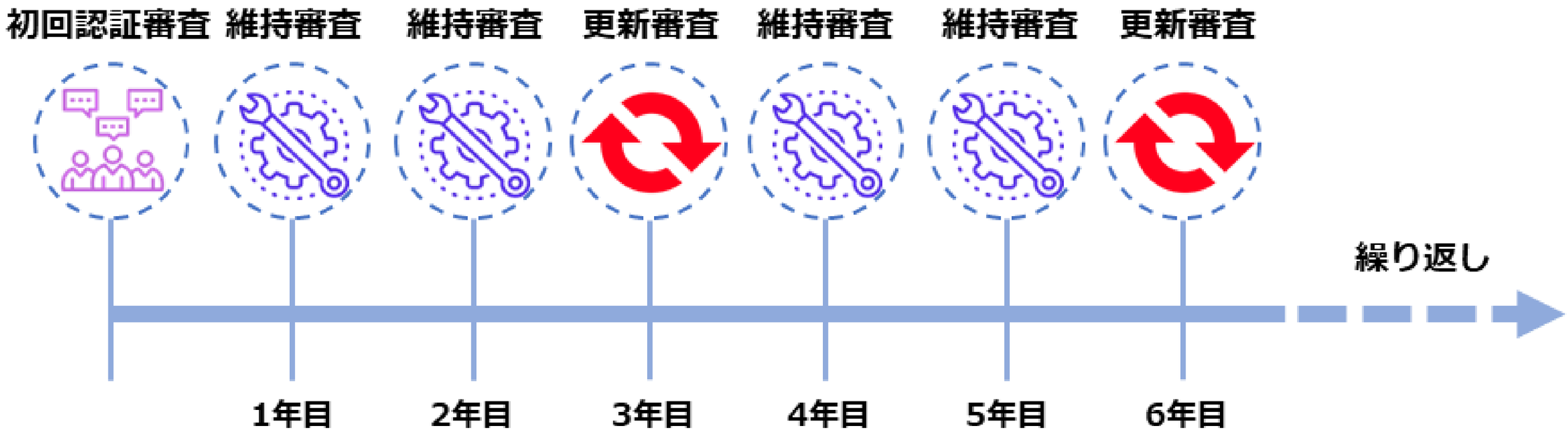
ステップ	申請	審査日程の確認	初回認証審査	認証登録	報告・公開
概要	新規取得する際、今までと異なる認証機関で受診する場合は、申請が必要です。	組織と認証機関との間で、審査日程の確認を行います。	新規の場合は原則として1次審査と2次審査の2回で実施されます。	審査の結果、適合していることが確認されると認証書が発行され、登録完了となります。	認証された旨が認証機関からISMS-ACに報告され次第、ISMS-ACホームページで公開されます。

情報セキュリティマネジメントシステム（ISMS）

【参照：セミナーテキスト7-2-3.】
第7章 - 15

ISMS認証の維持、更新審査プロセス

- 年に1回以上の維持審査（サーベイランス審査）
- 3年ごとに認証の有効期限を更新するための更新審査



NISTサイバーセキュリティフレームワーク

【参照：セミナーテキスト7-3-1.】
第7章 - 16

NISTサイバーセキュリティフレームワーク（CSF）の概要

- CSFはNIST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

【参照：セミナーテキスト7-3-1.】
第7章 - 16

CSFの3つの構成要素（コア、ティア、プロファイル）

「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

【参照：セミナーテキスト7-3-2.】
第7章 - 17

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す

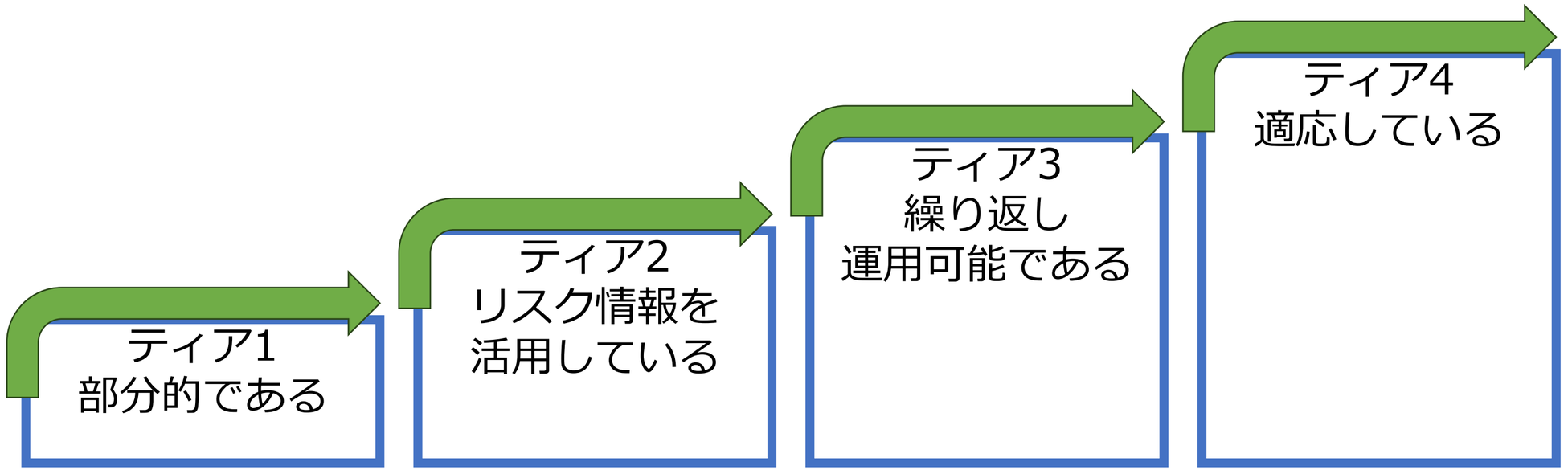
機能	説明	カテゴリ	サブカテゴリ
識別	組織の資産（情報システム、人、データ・情報など）、組織を取り巻く環境、重要な機能を支えるリソース、関連するサイバーセキュリティリスクを特定し理解を深める。	合計23	合計108
防御	重要サービスの提供が確実に行われるよう適切な保護対策を検討し実施する。		
検知	サイバーセキュリティイベントの発生を検知するための適切な対策を検討し実施する。		
対応	サイバーセキュリティインシデントに対処するための適切な対策を検討し実施する。		
復旧	サイバーセキュリティインシデントにより影響を受けた機能やサービスをインシデント発生前の状態に戻すための適切な対策を検討し実施する。これには、レジリエンスを実現するための計画の策定・維持も含む。		

NISTサイバーセキュリティフレームワーク

【参照：セミナーテキスト7-3-2.】
第7章 - 19

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す。指標はティア1～ティア4までの4段階があります。



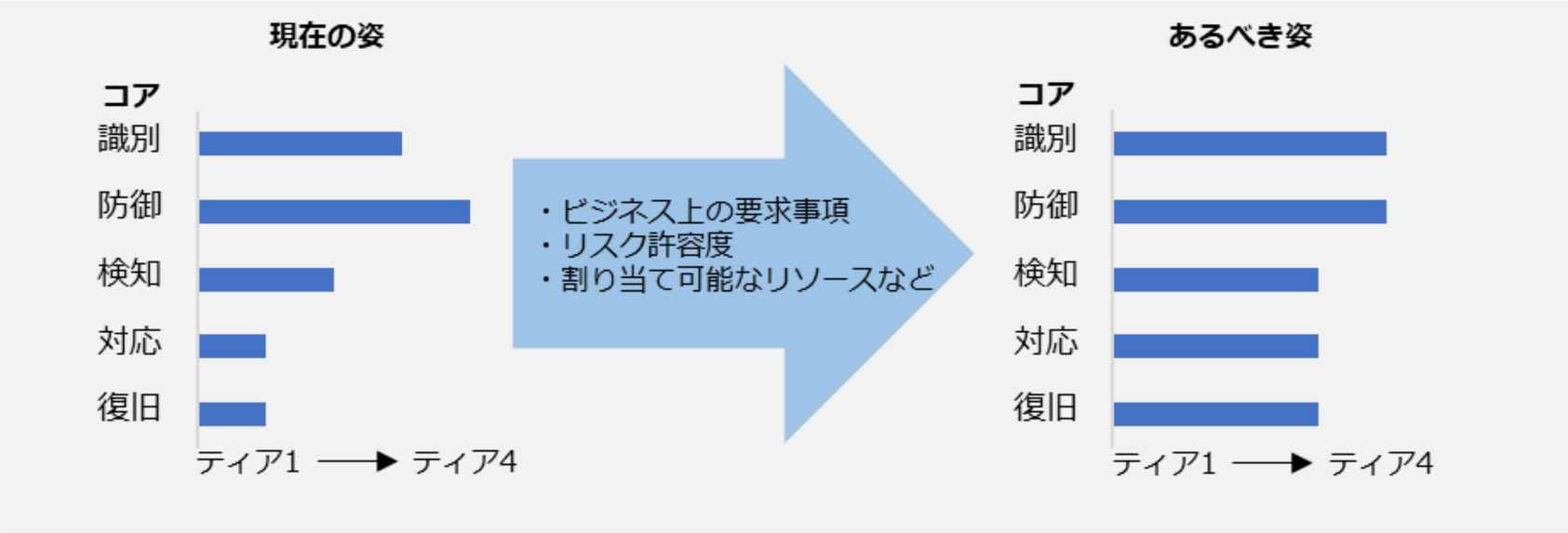
ティアの成熟度イメージ
（出典）デジタル庁 「政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート 」を基に作成

NISTサイバーセキュリティフレームワーク

【参照：セミナーテキスト7-3-2.】
第7章 - 19

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します。これにより、必要な改善点のギャップを特定できます。「あるべき姿」は、ビジネス要求やリスク許容度、リソースを基に策定されます。



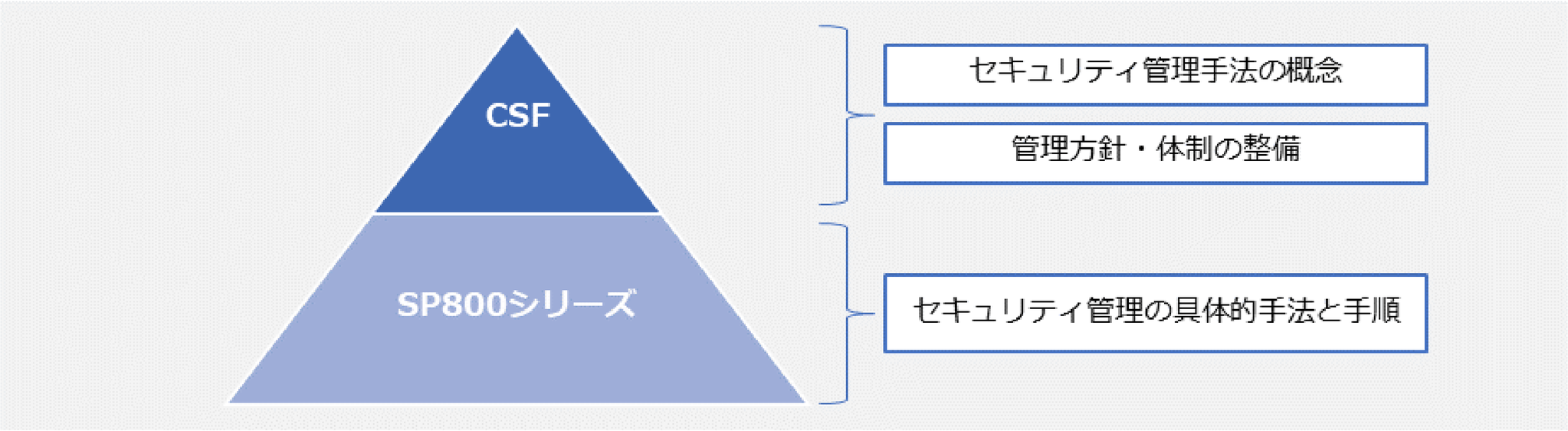
プロファイルの活用イメージ
（出典）デジタル庁 「政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート 」を基に作成

NISTサイバーセキュリティフレームワーク

【参照：セミナーテキスト7-3-3.】
第7章 - 20

NIST SP 800シリーズとCSFの関連性

CSFの下位概念に位置付けられているのが、NIST SP 800シリーズです。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ます。



CSFとSP800シリーズの関係

NISTサイバーセキュリティフレームワーク

【参照：セミナーテキスト7-3-4.】
第7章 - 21

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

CPSFの概要

【参照：セミナーテキスト7-4-1.】
第7章 - 22

- 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を基に、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

CPSFの目的と適用範囲

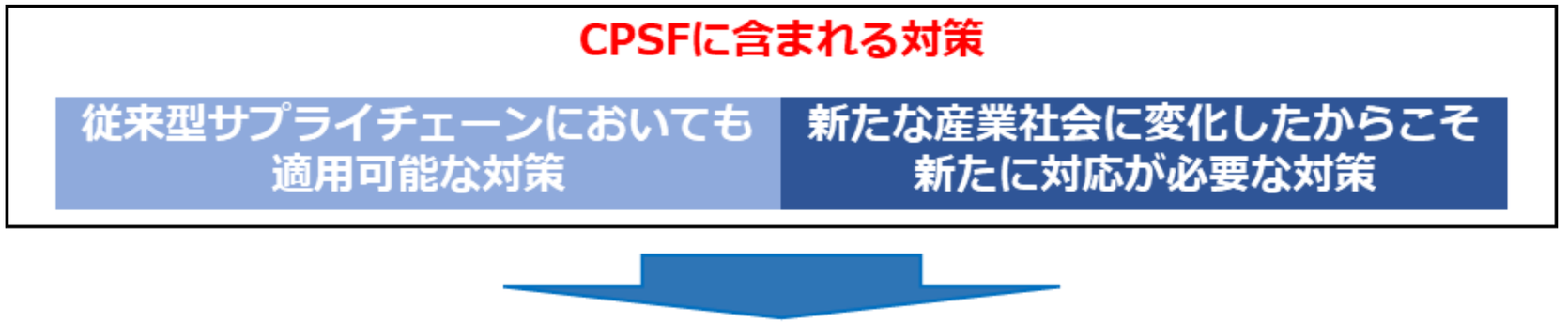
【参照：セミナーテキスト7-4-1.】
第7章 - 22

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

3層構造モデル

【参照：セミナーテキスト7-4-1.】
第7章 - 23

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

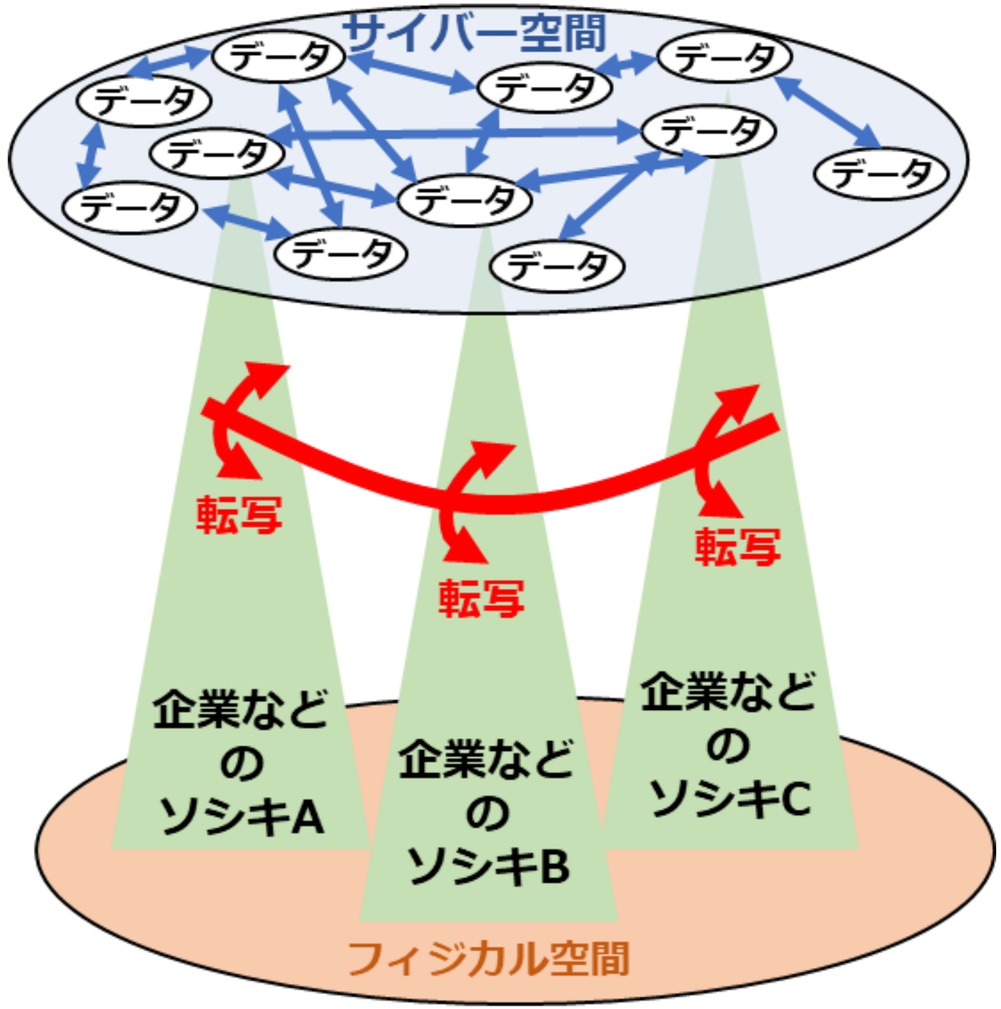
[第2層]

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：セミナーテキスト7-5-1.】
第7章 - 25

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元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：セミナーテキスト7-5-1.】
第7章 - 25

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、人材等）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：セミナーテキスト7-5-1.】
第7章 - 25

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等を含めた**サプライチェーン全体の状況把握及び対策**

【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、共有及び開示の促進**

サイバーセキュリティ経営ガイドライン

【参照：セミナーテキスト7-5-1.】
第7章 - 26

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

【ポイント】

- サイバーセキュリティリスクを経営者が責任を負うべき経営リスクとして認識し、組織全体としての対応方針（セキュリティポリシー）を策定させる。
- 策定した対応方針を対外的な宣言として公表させる。

サイバーセキュリティ経営ガイドライン

【参照：セミナーテキスト7-5-1.】
第7章 - 26

指示2：サイバーセキュリティリスク管理体制の構築

【ポイント】

- サイバーセキュリティリスクの管理に関する各関係者の役割と責任を明確にした上で、リスク管理体制を構築させる。
- サイバーセキュリティリスクの管理体制の構築にあたっては、組織内のガバナンスや内部統制、その他のリスク管理のための体制との整合を取らせる。

サイバーセキュリティ経営ガイドライン

【参照：セミナーテキスト7-5-1.】
第7章 - 26

指示3：サイバーセキュリティ対策のための資源（予算、人材等）確保

【ポイント】

- サイバーセキュリティに関する残存リスクを許容範囲以下に抑制するための方策を検討させ、その実施に必要となる資源（予算、人材等）を確保した上で、具体的な対策に取り組ませる。
- 全ての役職員に自らの業務遂行にあたってセキュリティを意識させ、それぞれのサイバーセキュリティ対策に関するスキル向上のための人材育成施策を実施させる。

サイバーセキュリティ経営ガイドライン

【参照：セミナーテキスト7-5-1.】
第7章 - 26

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

【ポイント】

- 事業に用いるデジタル環境、サービス及び情報を特定させ、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別させる。
- サイバー保険の活用や守るべき情報やデジタル基盤の保護に関する専門ベンダへの委託を含めたリスク対応計画を策定させ、対応後の残留リスクを識別させる。

サイバーセキュリティ経営ガイドライン

【参照：セミナーテキスト7-5-1.】
第7章 - 26

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

【ポイント】

- サイバーセキュリティリスクに対応するための保護対策として、防御・検知・分析の各機能を実現する仕組みを構築させる。
- 構築した仕組みについて、事業環境やリスクの変化に対応するための見直しを実施させる。

サイバーセキュリティ経営ガイドライン

【参照：セミナーテキスト7-5-1.】
第7章 - 27

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

【ポイント】

- リスクの変化に対応し、組織や事業におけるリスク対応を継続的に改善させるため、サイバーセキュリティリスクの特徴を踏まえた PDCA サイクルを運用させる。
- 経営者は対策の状況を定期的に報告させること等を通じて問題の早期発見に努め、問題の兆候を認識した場合は改善させる。
- 株主やステークホルダーからの信頼を高めるため、改善状況を適切に開示させる。

サイバーセキュリティ経営ガイドライン

【参照：セミナーテキスト7-5-1.】
第7章 - 27

指示7：インシデント発生時の緊急対応体制の整備

【ポイント】

- 影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を適時に実施するため、制御系を含むサプライチェーン全体のインシデントに対応可能な体制（CSIRT等）を整備させる。
- 被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。
- インシデント発生時の対応について、適宜実践的な演習を実施させる。

サイバーセキュリティ経営ガイドライン

【参照：セミナーテキスト7-5-1.】
第7章 - 27

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

【ポイント】

- インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をさせる。
- 制御系も含めた BCP との連携等、組織全体として有効かつ整合のとれた復旧目標計画を定めさせる。
- 業務停止等からの復旧対応について、対象を IT 系・社内・インシデントに限定せず、サプライチェーンも含めた実践的な演習を実施させる。

サイバーセキュリティ経営ガイドライン

【参照：セミナーテキスト7-5-1.】
第7章 - 27

指示9：ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策

【ポイント】

- サプライチェーン全体にわたって適切なサイバーセキュリティ対策が講じられるよう、国内外の拠点、ビジネスパートナーやシステム管理の運用委託先等を含めた対策状況の把握を行わせる。
- ビジネスパートナー等との契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化するとともに、対策の導入支援や共同実施等、サプライチェーン全体での方策の実効性を高めるための適切な方策を検討させる。

サイバーセキュリティ経営ガイドライン

【参照：セミナーテキスト7-5-1.】
第7章 - 27

指示10：サイバーセキュリティに関する情報の収集、共有及び開示の促進

【ポイント】

- 有益な情報を得るには自ら適切な情報提供を行う必要があるとの自覚のもと、サイバー攻撃や対策に関する情報共有を行う関係の構築及び被害の報告・公表への備えをさせる。
- 入手した情報を有効活用するための環境整備をさせる。

サイバーセキュリティ経営ガイドライン

【参照：セミナーテキスト7-5-2.】
第7章 - 28

サイバーセキュリティ経営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付けること

サイバーセキュリティ経営ガイドライン

【参照：セミナーテキスト7-5-2.】
第7章 - 29

サイバーセキュリティ経営ガイドラインの読み方（担当幹部等）

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

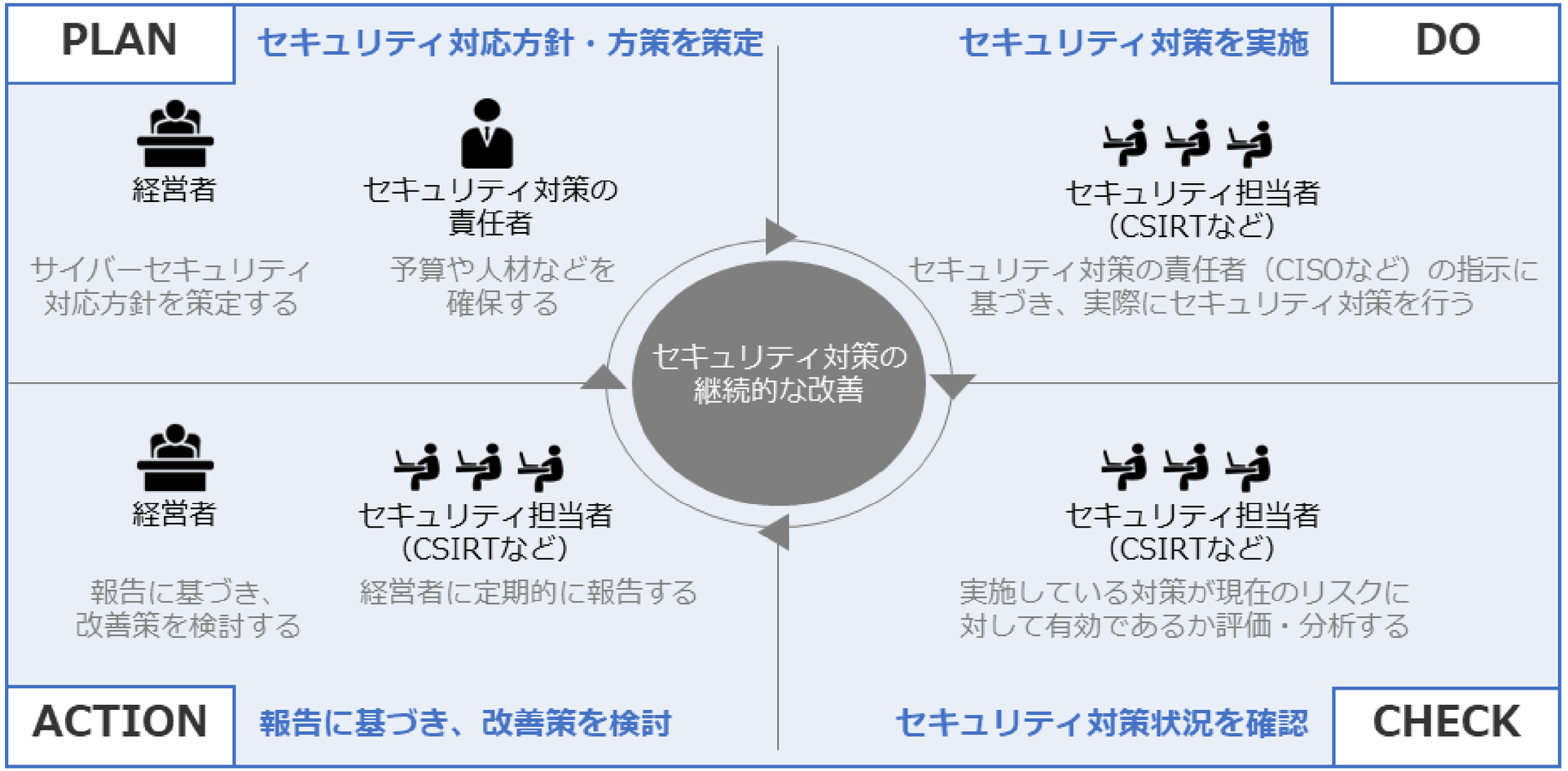
認識すべきこと

- 経営者から指示される内容に関して、より具体的な取組み方を検討し、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：セミナーテキスト7-5-3.】
第7章 - 30

サイバーセキュリティ経営ガイドラインの実践の流れ



サイバーセキュリティ経営ガイドラインの全体の流れ
（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」を基に作成

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