サイバーセキュリティ経営ガイドラインの全体像における位置付け

企業におけるサイバーセキュリティ対策の推進において、その基盤となる下図の赤枠部分（「リスク管理体制の構築」と「人材の確保」）は経営者が積極的に関わって実践すべき取組。『サイバーセキュリティ体制構築・人材確保の手引き』はその具体的検討のための参考文書。

経営者が認識すべき３原則

1. 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
2. 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
3. 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

経営者の積極的な関与のもとで実践

対外的にどの役職者が対応するのかも経営層の判断事項

ACT

PLAN

CHECK

DO

経営者がCISO等に指示すべき10の重要事項（①～⑩）

①サイバーセキュリティ対応方針策定

②リスク管理体制の構築

サイバーセキュリティ
リスク管理体制

◆経営リスク委員会等
他の体制と整合
（ex.内部統制、災害対策）

自社の状況に応じた役割の割当、権限の付与

CISO等の担当幹部・
戦略マネジメント層

セキュリティ担当、CSIRT等
実務者・技術者層

③資源（予算、人材等）の確保

⑦緊急対応体制の整備

⑧復旧体制の整備

④リスクの把握と対応計画策定

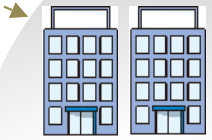
⑤保護対策(防御・検知・分析)の実施

⑥PDCAの実施

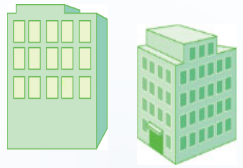
内外に宣言・開示

⑨サプライチェーン
セキュリティ対策

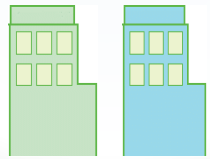
⑩情報共有活動
への参加



ステークホルダー
（株主、顧客、取引先等）



ビジネスパートナー



情報共有団体
・コミュニティ

本手引き書のポイント

- 手引き書における各項のポイントは次のとおり。
- サイバーセキュリティに関する役割の実践にあたっては、責任に見合った権限の付与が重要。特に「プラス・セキュリティ」（＝下表下線部のこと）業務においては組織内のセキュリティ対策における役割の自覚の観点からも重要。

「サイバーセキュリティ体制構築・人材確保の手引き」における検討のポイント

指示２ **サイバーセキュリティリスク管理体制の構築**	**2.1** **経営者のリーダーシップの下でのセキュリティ体制の検討**	①デジタル技術の活用の進展に伴い、従来とは異なる全社的なセキュリティ体制が必要となってきている。 ②全社的なセキュリティ体制の確立は経営者の責務であり、経営者がリーダーシップをとる必要がある。
	2.2 **セキュリティ統括機能の検討**	①全社的なセキュリティ体制の確立のためには、CISO等の経営層を補佐する「セキュリティ統括機能」（次ページ参照）の設置が有効。 ②セキュリティ統括機能には大きく4つの類型があり、自社の状況に合わせて検討する必要がある。
	2.3 **セキュリティ関連タスクを担う部門・関係会社の特定・責任明確化**	①セキュリティ統括機能と連携しつつセキュリティ関連タスクを担う部門・関係会社を特定する際には、ITSS＋（セキュリティ領域）を参考にすることで、外部委託先も含めた見える化が可能。 ②外部委託先の選定に当たっては、情報セキュリティサービス基準適合サービスリスト等が活用可能。
指示３ **サイバーセキュリティ対策のための資源確保**	**3.1** **「セキュリティ人材」の確保**	①まずはサイバーセキュリティに関する専門性を備えたセキュリティ統括人材の確保を目指す。 ②担当する人材の育成を通じて質的充足を図る。
	3.2 **「プラス・セキュリティ」の取組推進**	①「セキュリティ人材」のみならず、デジタル部門、事業部門、管理部門等においてそれぞれの業務に従事する人材が、セキュリティを意識し、業務遂行に伴う適切なセキュリティ対策の実施やセキュリティ人材との円滑なコミュニケーションに必要な能力を育成する「プラス・セキュリティ」の取組も重要。 ②ITSS+（セキュリティ領域）等を活用し、関連部門でセキュリティ関連タスクを担う人材の特定・育成・配置等を検討。
	3.3 **教育プログラム・試験・資格等の活用と人材育成計画の検討**	①各分野に求められる知識・スキルを踏まえ、教育プログラムや試験・資格の活用を検討。 ②自社に必要な人材の配置計画をもとに、キャリアデザインを含めた育成計画を検討。

本書で扱う主要な概念の解説

セキュリティ統括機能

- セキュリティ対策及びインシデント対応において、CISOや経営層を補佐してセキュリティ対策を組織横断的に統括することにより、企業におけるリスクマネジメント活動の一部を担う
- 「機能」であって「組織」として設置しなくてもよい（状況に応じて、最適な形態は異なる）
  - 独立した組織として設置
  - 管理部門の１機能として割当
  - 情シス部門の１機能として割当
  - 組織横断的な委員会形態で運用

ITSS+（セキュリティ領域）

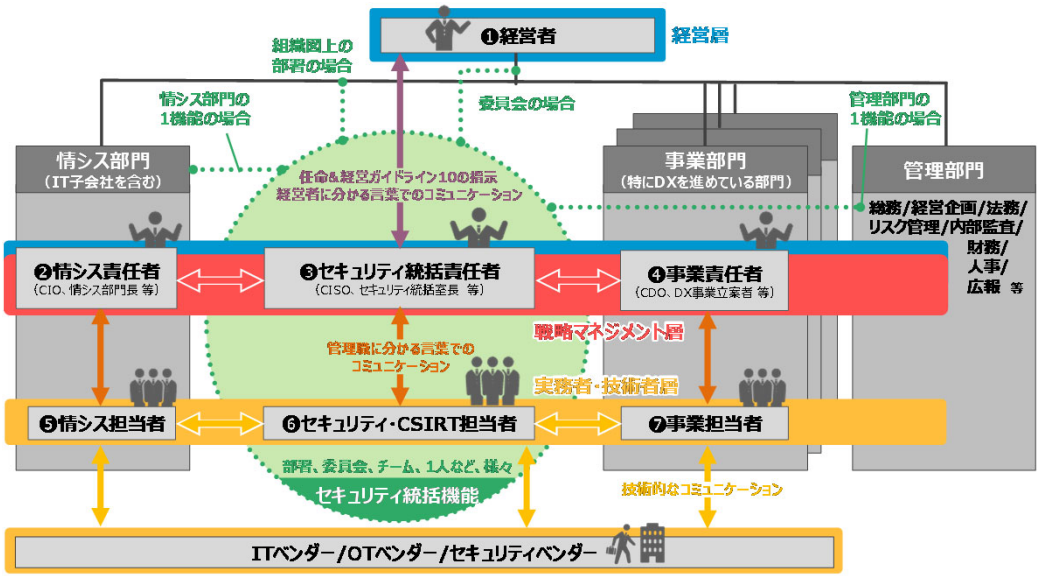
- 企業のセキュリティ対策に必要となる関連業務のまとまりを17分野に整理したもの
- セキュリティの専門性の高い分野だけでなく、経営層や法務部門、事業ドメインまで、サイバーセキュリティ対策に関わる幅広い領域を網羅
- DXの取り組みを通じたクラウド化、アジャイル開発、開発・セキュリティ対策・運用の一体化（DevSecOps）等の動きの中、ITSS＋で定める各分野の境界は曖昧化の傾向

プラス・セキュリティ

- セキュリティ対策を本務としないが、業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策の実践が求められる業務が「プラス・セキュリティ」の対象
- 「プラス・セキュリティ」という人材が業務担当者と別に存在するわけではなく、これまでの業務担当者がサイバーセキュリティの知識・スキルを習得し、実践することを通じて対策を担う
- DXの取り組み有無に関わりなく、ITを活用するすべての企業において必要

セキュリティ統括機能のイメージ

企業の組織構造や事業内容に応じて下図の緑色部分の実現方法の検討が必要



ITSS＋（セキュリティ領域）（赤枠が「プラス・セキュリティ」の分野）