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手引きの位置付け

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「資源（予算、人材等）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。※

※ 指示３のうち予算の確保に関する内容は含みません。

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、最終責任者として対応することが必要
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

DO

CHECK

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

内外に宣言・開示

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

⑨サプライチェーン
セキュリティ対策

⑦緊急対応体制の整備

④リスクの把握と対応計画策定

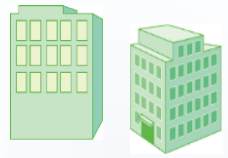
⑧復旧体制の整備

⑤保護対策(防御・検知・分析)の実施

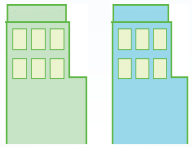
⑩情報共有活動
への参加

⑥PDCAの実施

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。
- 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）は組織内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** **サイバーセキュリティに関して「やるべきこと」の明確化**	①自社で対処すべきサイバーセキュリティリスクを認識し、そのリスクを低減するために具体的に「やるべきこと（タスク）」を明確化していく。 ②ITSS+（セキュリティ領域、次ページ参照）なども参考にしながら、負荷が大きい部分はスモールスタートから始め、継続的に改善する。
	2.2 **セキュリティ統括機能の検討**	① 組織内でサイバーセキュリティ機能をうまく働かせるには、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）を設置すべき。 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。
	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 サイバーセキュリティ体制の具体的な構築にあたっては、ITSS＋（セキュリティ領域）を参考にすることで、関係部署や委託先の役割が明確になる。 ② 実際のところほとんどの企業においてサイバーセキュリティに関する機能の一部を外部委託することが適切であるが、丸投げではない適切な役割分担と、品質の担保されたサービスの選定が重要である。
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** **セキュリティを主たる業務とする人材の確保**	① 外部委託を積極活用していても、サイバーセキュリティリスクの把握と対策を推進する自社要員を割り当てる必要があり、当該人材には役割に応じた知識・スキルが求められる。 ② サイバーセキュリティに関する専門性を有する人材は不足状態にあり、確保には工夫が求められる。
	3.2 **「プラス・セキュリティ」の取組推進**	① 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、DX等のデジタル活用を進めるなかで<u>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</u>「プラス・セキュリティ」の取組が欠かせない。 ②「プラス・セキュリティ」を担う人材に自らの役割と責任の自覚を促すための意識付けを行う。
	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・資格の活用を検討する。 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する。

本書で扱う主要な概念の解説

セキュリティ統括機能

- 企業におけるリスクマネジメント活動の一部として、セキュリティ対策及びセキュリティインシデント対応について、CISOや経営層による意思決定や、事業部門におけるセキュリティ対策の検討及び実施について、専門的な知見や経験をもとにサポートする機能
- 経営層や各事業部門は、セキュリティ統括機能によるサポートを受けつつ、それぞれが責任を負うセキュリティ対策を実践する。
- 「機能」であって「組織」として設置しなくてもよい（企業組織の状況に応じて、最適な形態は異なる：以下は設置方法の例）
  - 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

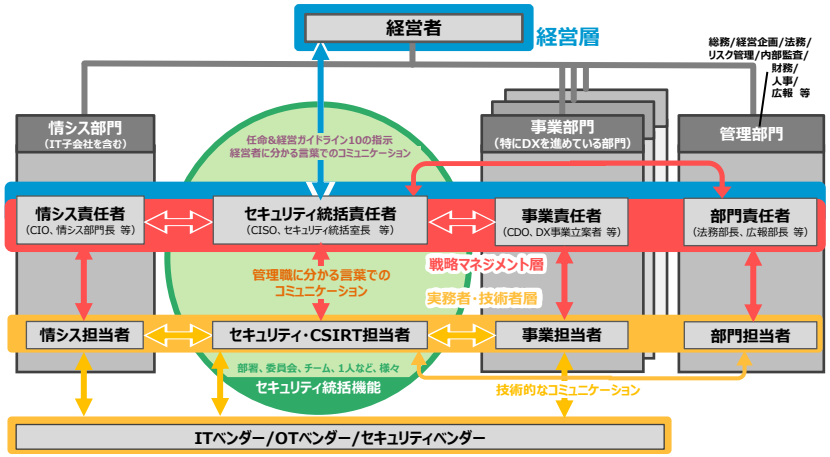
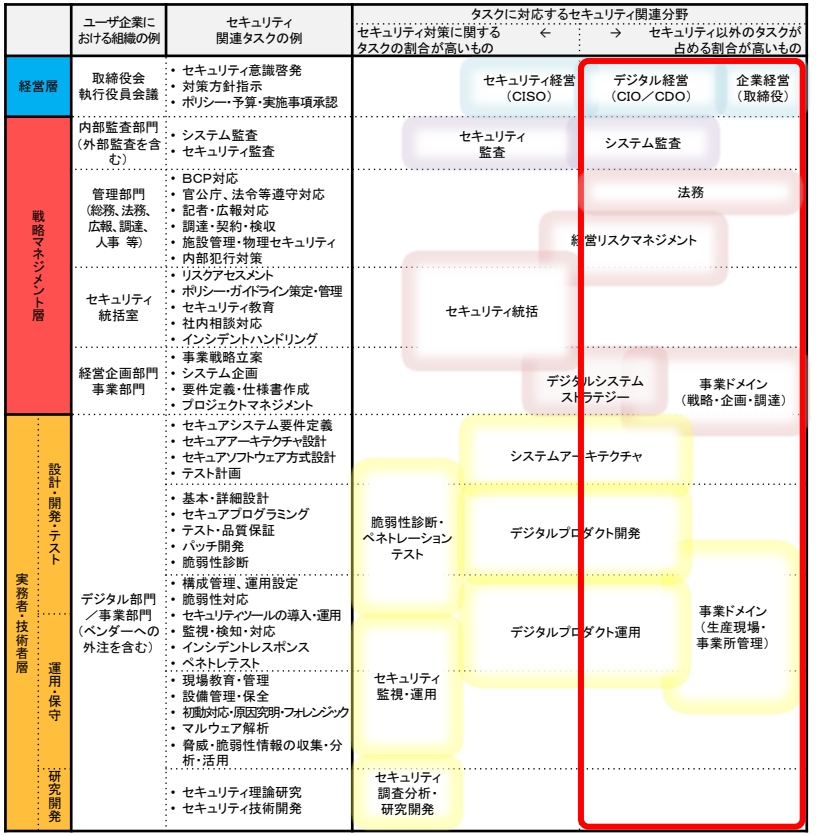
ITSS+（セキュリティ領域）

- 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している
- DXの取組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、各分野の境界は曖昧化の傾向にある

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実践すべき

セキュリティ統括機能のイメージ



ITSS＋（セキュリティ領域）（赤枠が「プラス・セキュリティ」の分野）