サイバーセキュリティ経営ガイドライン Ver2.0 付録F

サイバーセキュリティ体制構築・人材確保の手引き

～ 変化するサイバーセキュリティリスクに対処するための
組織の在り方と従事する人材の配置・役割分担 ～

第２版

経済産業省 商務情報政策局 サイバーセキュリティ課
独立行政法人 情報処理推進機構（IPA）

目次

1. はじめに

1.1 本書の目的

本書は、『サイバーセキュリティ経営ガイドライン』（Ver.2.0）（以下、「経営ガイドライン」といいます。）をもとに自社のサイバーセキュリティ対策を検討しようとする組織※1を対象として、経営ガイドラインにおいて示されている重要１０項目のうち、次の２項目：

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

について具体的な検討を行う場合の参考としていただくことを目的として提供するものです※2。

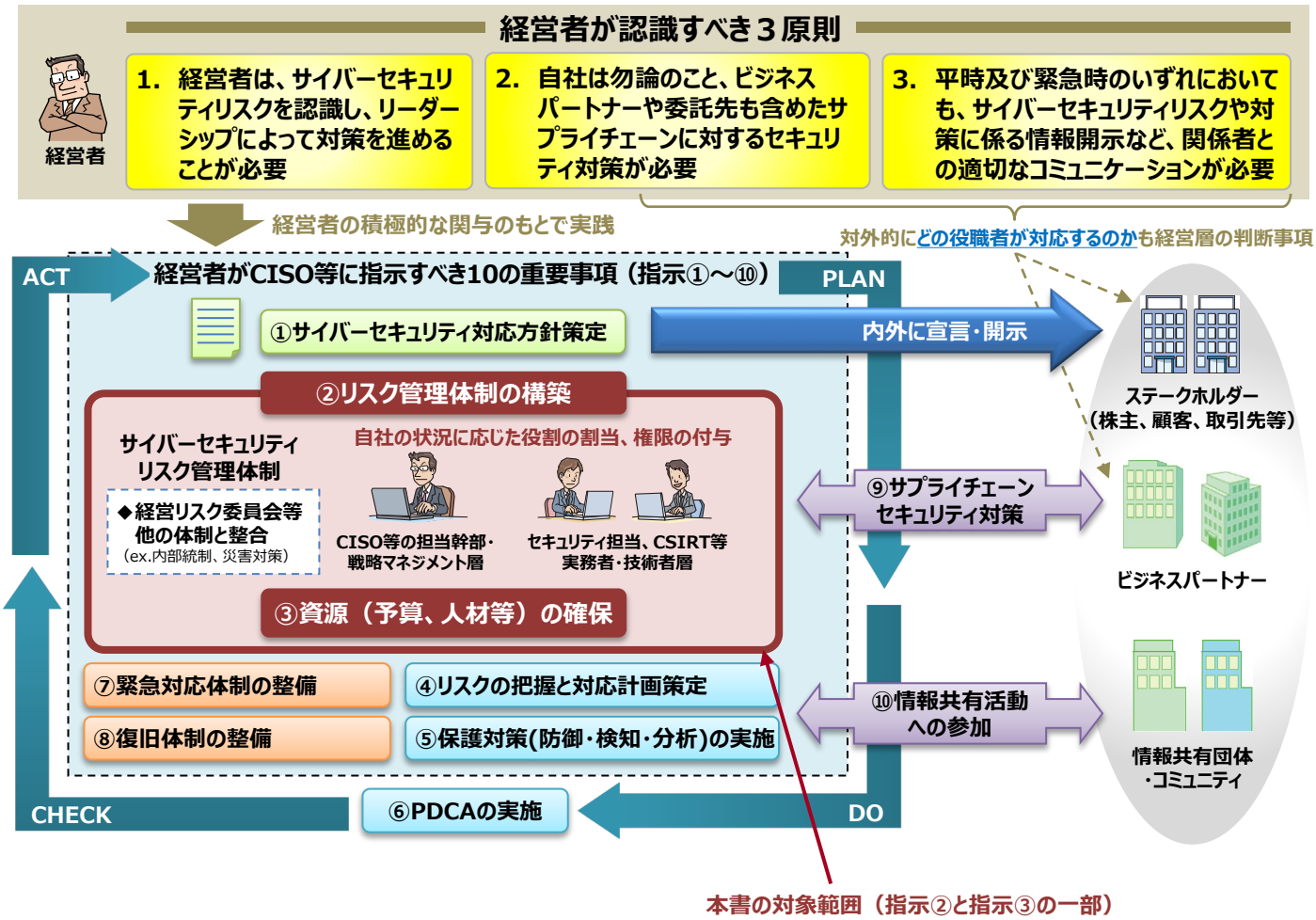
なお、企業の規模や業種・業務内容・企業文化等により異なり、対策の実施に必要な資源も変わってくるため、望ましいサイバーセキュリティ管理体制は、企業毎に検討することになります。

そこで本書では、この検討を支援するため、企業経営の観点から、自社に最適な体制や資源確保に関する適切な判断を行うためのポイントについて解説します。記載している内容は、有識者による検討と企業における実際の実践事例調査の結果に基づいています。

※1　いわゆるユーザ企業（開発された情報システムやソフトウェアを利用する企業）に加え、その他の企業における社内向けのサイバーセキュリティ対策を検討する組織も対象に含みます。

※2　一部、インシデント対応のための体制に関する項目（指示7、指示８）に対応する内容を含みます。
一方、指示３のうち予算の確保に関する内容は含みません。

図表1　サイバーセキュリティ経営ガイドラインの全体像と本書の位置付け



1.2 主な対象読者

① 経営者・経営層

概要版（経営層向けサマリ）に経営層が担うべき役割と本書の内容に関するポイントを挙げていますので、これをご覧になると本書の概要を把握いただくことができます。

② 最高情報セキュリティ責任者（CISO）、セキュリティ統括担当者

本書全体をご覧いただくことが望まれます。ただしコラムで紹介している内容については、自組織に関連する内容のみを参照することで差し支えありません。

③ 事業部門の責任者、人事部門担当者、セキュリティに関心のある方

事業推進上のリスクマネジメントやDX推進の責任者、人事部においてセキュリティに関する人材の配置等を検討する方や、セキュリティに関するキャリアを考えられている方は、３.を中心にご覧ください。

1.3 本書の構成

本書は、効率よくご覧いただくための工夫として、次のように構成されています。

図表2　本書の構成

ポイント	囲み枠の中に重要事項を箇条書きで示しています。ポイントをご覧いただくだけでも、サイバーセキュリティ体制・人材の確保の要点を把握することができます。
本文	各項目についての詳細な説明です。
コラム	本文における説明を補足する目的で、有用と思われる内容を囲み記事の形で紹介しています。

1.4『サイバーセキュリティ経営ガイドライン』指示２と指示３の実践の進め方

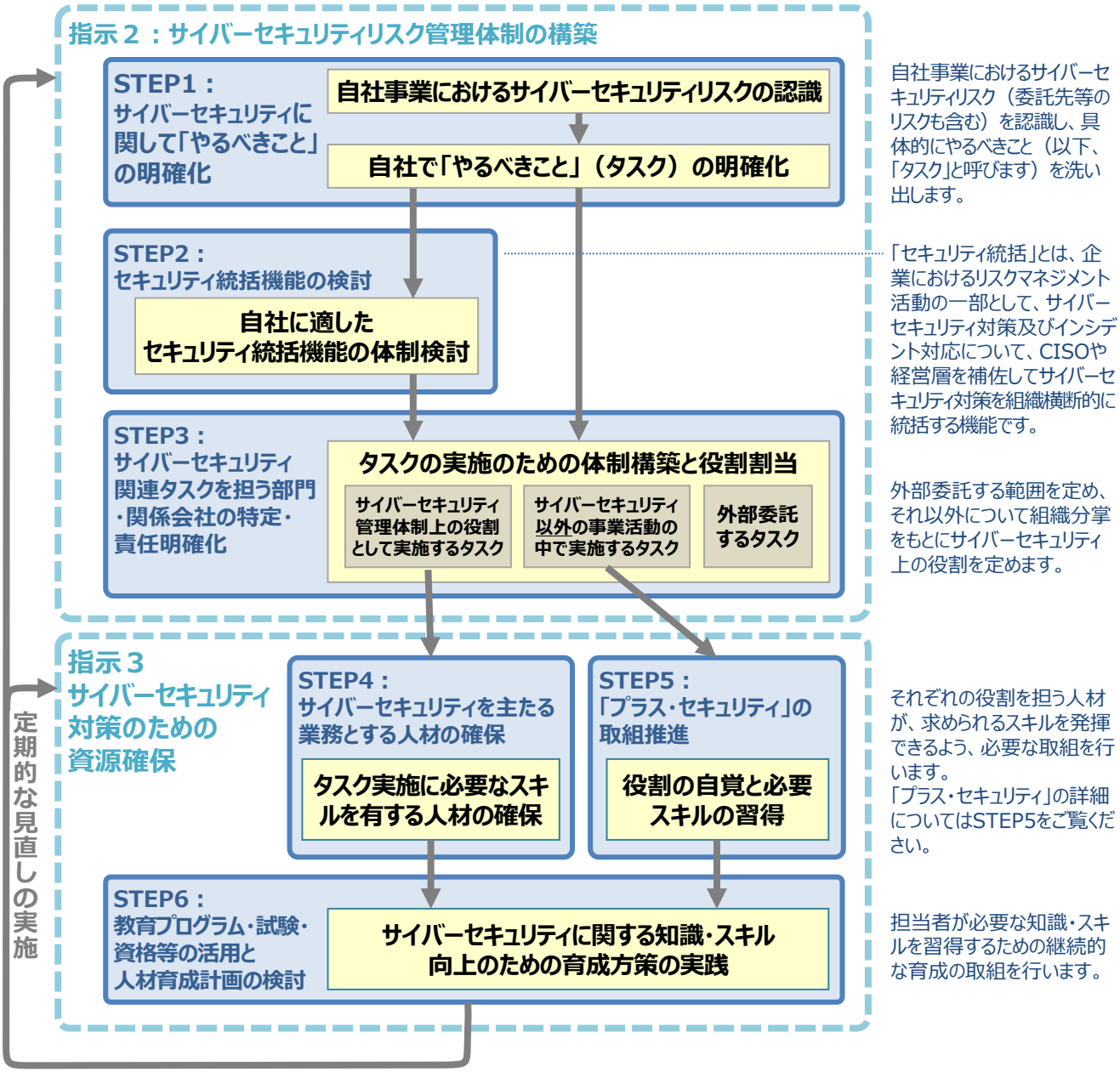
ポイント：

- デジタル社会において、事業リスクの低減のためには、サイバーセキュリティが不可欠です。体制構築そのものの検討に先立ち、経営者の指示の下、インシデントが起きた際の事業への影響などを整理した上で、会社として守るべきことは何かを全社的に検討し、リスク管理の方針を定めることが必要です。
- サイバーセキュリティ対策を担う組織と人材にはさまざまな種類があり、経営ガイドラインの指示１で定めた自社の方針に従って適切に組み合わせた体制を構築し、運営していくことが求められます。
- 体制を構築して安心するのではなく、経営層のリーダーシップのもと、それらが有効に機能し続けるように維持・改善する必要があります。

(1) 検討と実践を効率的に進めるための手順

- 本書では、次図に示す流れに従って、企業が必要なサイバーセキュリティ対策を実践するための体制の構築と人材の確保・育成の進め方について説明します。サイバーセキュリティを取り巻く環境は日々変化しているので、すでにサイバーセキュリティ管理体制がある場合でも定期的に手順に沿って点検することをお勧めします。

図表3　本書の構成と企業における実践の流れ



(2) 目的に応じた本書の活用方法

前ページの手順について、企業における活用イメージは以下のとおりです。

例1：事業部門におけるDX推進に対応した自社体制の見直し

従来の管理体制ではうまく機能しないことが懸念される場合、次のような手順で役割分担の見直しと必要な啓発や教育を行っていくことが考えられます。

STEP1: サイバーセキュリティに関して「やるべきこと」の明確化	DX推進に伴うリスクに対処するために、現状のタスクで不足がないかを確認します。
↓	
STEP3: サイバー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	DX推進に関わる部署が適切な役割を担うように見直しを行います。
↓	
STEP5: 「プラス・セキュリティ」の取組推進	DX推進の場合、事業部門が担う役割が多くなることから、プラス・セキュリティとしてサイバーセキュリティ知識・スキルの習得を促していくことが重要です。
↓	
STEP6: 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	プラス・セキュリティを担う人材が過剰な負担なくサイバーセキュリティスキルを習得するための方法を検討し、実践します。

例2：サプライチェーンにおけるインシデント対応体制の共同化

サプライチェーンにおけるサイバー攻撃による被害連鎖を防ぐため、複数の企業でインシデント対応体制を共同化することになった場合、次の手順で体制の見直しや訓練を行っていくことが考えられます。

STEP2: セキュリティ統括機能の検討	セキュリティ統括組織のタスクとして、組織間連携・共有に関する内容を追加します。
↓	
STEP3: サイバー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	サプライチェーン内での情報のやりとりを行う部署におけるインシデントへの共同対応及び訓練等のタスクを含めるように調整します。
↓	
STEP5: 「プラス・セキュリティ」の取組推進	インシデント対応スキルを向上させるための教育プログラム等の検討を行います。
↓	
STEP6: 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	インシデント対応は実務経験機会が少ないことから、外部の演習サービス等を活用したトレーニングを実施します。

2. サイバーセキュリティリスク管理体制の構築（指示2）

経営ガイドラインでの指示内容

指示２：サイバーセキュリティリスク管理体制の構築

- サイバーセキュリティ対策を行うため、サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる。
- その際、組織内のその他のリスク管理体制とも整合を取らせる。

取組の心構え

- デジタル化技術の活用の進展に伴い、サイバー攻撃の起点が拡大しています。サイバーセキュリティはもはや情報システム部門だけの問題ではなく、多くの部署やグループ会社・海外拠点等を横断的に巻き込んだ全社的な体制構築が必要になっています。
- また、サイバー攻撃の高度化や実業務への影響の増大などにより、サイバー攻撃は、事業継続、人命・安全、損害賠償、レピュテーション（評判）リスクなど、あらゆる経営リスクに直結する問題となっています。
- さらに、サイバー攻撃動向の変化は速く、形だけの体制構築では対処がうまくいきません。自社の置かれた状況（事業内容、規模、特性等）に応じ、適切なサイバーセキュリティ機能とそれを実現するための体制を検討する必要があります。

経営者のリーダーシップの下、次頁以降のポイントを参照しながら、適切な体制を検討しましょう

コラム：体制構築に関するよくある勘違い

①サイバーセキュリティ対策は専門事業者や実務者におまかせ。

→ **NO!** サイバーセキュリティ体制不備による重要情報の漏えいや事業停止は経営者の責任です。会社法は取締役に内部統制システムの構築義務を課しており、経営者は自社のリスクマネジメントの一環として、事業環境を守るサイバーセキュリティ体制を構築するとともに、委託先を監督する責任を負います。

②サイバーセキュリティの事故に遭ったことはないので、まだ体制は構築しなくても大丈夫。

→ **NO!** 事故が起きてからでは遅いんです。ひとたびインシデントが起きると、事業停止、取引先への影響、取引先や顧客における信用失墜など、経営上の大きな支障になります。だからこそ、自社のサイバーセキュリティリスクが顕在化する前に経営層のトップダウンで対策を推進することが必要です。

③外からの攻撃に対する防御技術を導入すれば大丈夫。

→ **NO!** 従業員による操作ミスや内部不正、取引先等の不正・過失、クラウドサービスの仕様変更による影響の確認不足など、脅威は内外に存在します（参考：経営ガイドライン指示４）。技術のみに頼らず、組織として備えるための管理体制が必要です。

④一度、体制構築をしたらそれをずっと継続すべき。

→**NO!** サイバーセキュリティ体制や要員配置を最初からベストな形で作るのは不可能です。また、攻撃手法も日々進化します。不断の見直しを行いましょう（参考：経営ガイドライン指示６）。

⑤完璧な体制を作れば、リスクはゼロにできる。

→**NO!** どんなにすばらしい体制を整備して、高額な対策ツールを導入しても、リスクがなくなることはありません。経営ガイドライン指示４を参照しながら、リスク移転策（サイバー保険の利用等）なども検討しましょう。

2.1【STEP1】サイバーセキュリティに関して「やるべきこと」の明確化

ポイント：
- まず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実現すべきサイバーセキュリティ機能を定めた上で、具体的に「やるべきこと（タスク）」を明確化していきます。
- 検討にあたっては、ITSS+（次ページ参照）など既存の文書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はじめ、継続的に改善をしていきましょう。

(1) 対処すべきリスクの認識及び「やるべきこと」の明確化

- サイバーセキュリティ体制を構築する際に重要なのは、**「形だけ」でなく、適切に機能する体制にすること**です。
- そのためには、下図のように、まずは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、そのリスクを実害にしないために実現すべきサイバーセキュリティ機能を定めます。さらに、この機能をブレイクダウンしてサイバーセキュリティに関して具体的にやるべきこと（タスク）を洗い出します。このタスクを実施する仕組みがサイバーセキュリティ体制です。

図表4　サイバーセキュリティに関して自社で具体的にやるべきことの洗い出し手順

	＜具体例＞	＜ポイント＞
①サイバーセキュリティリスクの認識	● マルウェア感染による事業停止 ● 認証不備による情報漏えい ● 内部不正	● デジタル環境活用に伴う事故として、自社で責任もって防ぐべき脅威を抽出します。 ● IPAで簡易的な方法を公表しています。※1
②実現すべきサイバーセキュリティ機能の明確化	● 自社のIT資産の保全 ● 異常の検知 ● 関係者との調整	● 既存のフレームワークを活用しつつ、必要に応じて追加等を検討します。 ● 次ページ(2)で詳細を説明します。
③具体的にやるべきこと（タスク）の洗い出し	● IT資産における構成管理※2 ● 脆弱性対応の実施	● まずやるべきことを洗い出して、次にそれをどこで担当するか割当を検討します。 ● 次ページ(3)で詳細を説明します。

＜体制の検討にあたって留意いただきたいこと＞

- サイバーセキュリティリスクはデジタル技術の進展や企業における利活用環境の変化などに応じてリスクが変化するため、上記の手順を**必要に応じて適宜行う（例：定期的に年1回＋新たなリスクが顕在化した場合）**ことを通じて、自社で実施すべきタスクの内容を更新すべきです。それに応じて体制の見直しが必要になることもあります。
- リスクの認識やタスクの洗い出しは、事業を行っている部門において行うのが最も正確かつ効果的なのですが、現在の多くの企業の事業部門においては、サイバーセキュリティに関する事故がどのように発生するかといった知見が不足していることが想定されます。そこで本書では、事業部門におけるリスクの認識やタスクの洗い出し等の作業を専門的な知識や経験をもとにサポートする仕組みとして、**「セキュリティ統括機能」**の活用を推奨しています。詳細はSTEP2で説明します。

※1 リスクの洗い出しについては、「中小企業の情報セキュリティ対策ガイドライン(IPA)」が参考になります。
https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

※2 構成管理：ここではIT機器やソフトウェア等の構成要素について、その設定・更新等の状況を把握・管理するという意味で用いています。

(参考) サイバーセキュリティ機能の基本は概ね世界共通です

- サイバー攻撃がインターネット経由で国境関係なく展開されている以上、その影響を防ぐために組織において備えるべきサイバーセキュリティ機能はどの国・組織であっても基本的な部分は共通のものとなります。図表5に米国NISTが重要インフラ事業者向けに公表しているサイバーセキュリティ機能のカテゴリ分類を示します。
- 他方、自社が特定の攻撃の標的とされる恐れがある場合や、特別な保護が必要である場合は、独自のサイバーセキュリティ機能を追加する必要があります。

図表5　NISTサイバーセキュリティフレームワーク※が定めるサイバーセキュリティ機能のカテゴリ分類

特定(ID)	組織の資産（データ、要員、設備等）管理
	ビジネス環境の優先度設定
	組織の方針策定と周知
	リスクアセスメントの実施とリスクの把握
	リスク管理戦略の策定と判断への利用
	サプライチェーンリスクの管理プロセスの確立
防御（PR）	資産と施設へのアクセス制御
	意識向上とトレーニング
	データ保護方針に基づく管理
	情報保護プロセスと手順の維持・適用
	システムの保守・修理の実施
	サイバーセキュリティ維持のための対策技術の管理
検知（DE）	異常な活動の検知と影響の把握
	システムと資産の継続的モニタリング
	検知プロセス手順の維持・テスト
対応（RE）	インシデント対応手順の実施・維持
	利害関係者への連絡に関する事前調整
	効果的対応のためのインシデントの分析
	インシデントの影響低減のための活動実施
	対応活動の改善
復旧（RC）	復旧計画の準備・維持
	教訓に基づく復旧計画の改善
	復旧活動に関する関係者との調整

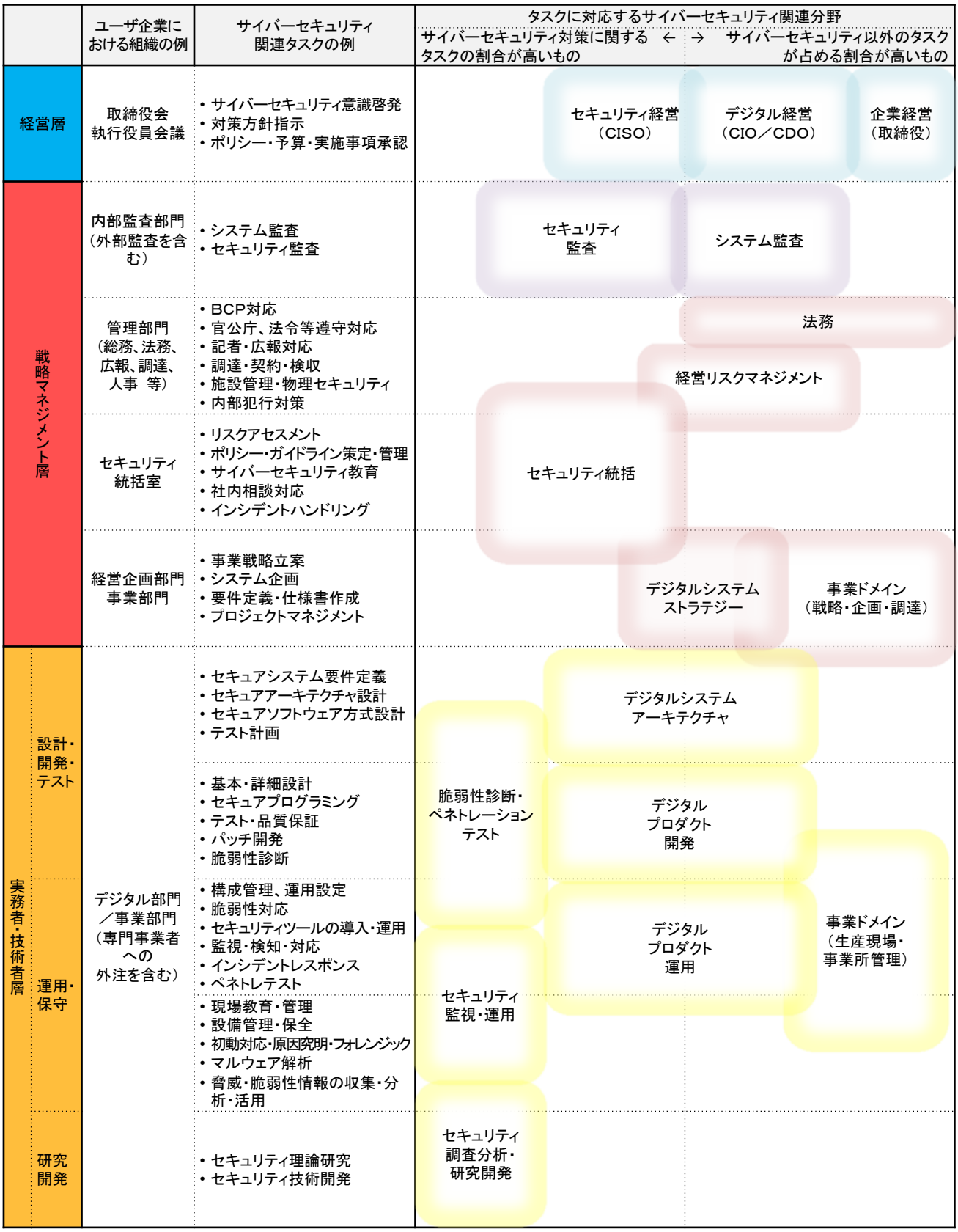
※NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1より趣旨を要約
https://www.nist.gov/cyberframework/framework
（IPAによる日本語訳掲載先）https://www.ipa.go.jp/security/publications/nist/index.html
なお、経営ガイドラインの重要10項目はこのフレームワークの構成と対応づけられています。

(２) ITSS＋を用いたタスクの洗い出し

- (1)に示した検討プロセスをあらゆるリスクについて一から行おうとすると、相当の作業負荷がかかるだけでなく、見落としにも繋がります。そこで、サイバーセキュリティに関する公的機関等が公表し、多くの組織で用いられているサイバーセキュリティ機能やタスクについて整理された資料を用いるのが一般的です。
- 本書では、独立行政法人情報処理推進機構（IPA）が公表しているITSS+（セキュリティ領域）※を用いたタスクの洗い出しを例に説明します。ITSS+は、第4次産業革命に向けて求められる新たな領域の“学び直し”の指針として、データサイエンス、アジャイル等の領域を対象に策定されたスキル標準であり、サイバーセキュリティについても「セキュリティ領域」として次ページ図のように定義されています。
- ITSS+（セキュリティ領域）の特徴として、サイバーセキュリティを生業とする人材のみではなく、デジタル部門、事業部門、管理部門等でサイバーセキュリティ以外の業務を生業とする人材がサイバーセキュリティ知識・スキルを身につける「プラス・セキュリティ」の取組推進のための “学び直し”の指針としても活用できるように工夫していることが挙げられます。「プラス・セキュリティ」については第３章で詳述します。
- ITSS+では、サイバーセキュリティに関するタスクをまとめて17種類の「分野」を設定しています。図表6において、角が丸い四角形で示されている部分に相当し、これをサイバーセキュリティ関連のタスクの占める比率の高さに応じてマッピングしています。
- 図表7 において、17分野の位置付けと具体的なタスクの例を示します。

※ITSS＋の紹介ページ（IPA）　https://www.ipa.go.jp/jinzai/itss/itssplus.html

図表6　ITSS＋（セキュリティ分野）で定義されている17分野



※クラウド、アジャイル、DevSecOps等により境界は曖昧化の傾向
※チップ/IoT・組み込み/制御システム/OS/サーバ/NW/ソフト/Web等の取扱う技術の種類や事業分野によりタスクやスキルは大きく異なる

図表7　ITSS＋（セキュリティ分野）で定義されている17分野毎のタスク例

	分野名	サイバーセキュリティ関連タスクの例
経営層	セキュリティ経営（CISO）	● サイバーセキュリティ意識啓発 ● 対策方針の指示 ● セキュリティポリシー・予算・対策実施事項の承認　等
	デジタル経営（CIO/CDO）	
	企業経営（取締役）	
戦略マネジメント層	セキュリティ監査	● 情報セキュリティ監査、報告・助言　等
	システム監査	● システム監査、報告・助言　等
	セキュリティ統括	● サイバーセキュリティ教育・普及啓発 ● サイバーセキュリティ関連の講義・講演 ● サイバーセキュリティリスクアセスメント ● セキュリティポリシー・ガイドラインの策定・管理・周知 ● 警察・官公庁等対応 ● 社内相談対応 ● インシデントハンドリング 等
	デジタルシステムストラテジー	● デジタル事業戦略立案 ● システム企画 ● 要件定義・仕様書作成 ● プロジェクトマネジメント　等
	経営リスクマネジメント	● 経営リスクマネジメント ● BCP／危機管理対応 ● サイバーセキュリティ保険検討 ● 記者・広報対応 ● 施設管理・物理セキュリティ ● 内部犯行対策　等
	法務	● デジタル関連法令対応 ● コンプライアンス対応 ● 契約管理　等
	事業ドメイン（戦略・企画・調達）	● 事業特有のリスクの洗い出し ● 事業特性に応じたサイバーセキュリティ対応 ● サプライチェーン管理　等
実務者・技術者層	脆弱性診断・ペネトレーションテスト	● 脆弱性診断、ペネトレーションテスト　等
	セキュリティ監視・運用	● セキュリティ製品・サービスの導入・運用 ● セキュリティ監視・検知・対応 ● インシデントレスポンス ● 連絡受付　等
	セキュリティ調査分析・研究開発	● サイバー攻撃捜査、原因究明・フォレンジック ● マルウェア解析、脅威・脆弱性情報の収集・分析・活用 ● セキュリティ理論・技術の研究開発 ● セキュリティ市場動向調査 等
	デジタルシステムアーキテクチャ	● セキュアシステム要件定義 ● セキュアシステムアーキテクチャ設計 ● セキュアソフトウェア方式設計 ● テスト計画　等
	デジタルプロダクト開発	● 基本設計、詳細設計 ● セキュアプログラミング ● テスト・品質保証 ● パッチ開発　等
	デジタルプロダクト運用	● 構成管理 ● 運用設定 ● 利用者管理 ● サポート・ヘルプデスク ● 脆弱性対策・対応 ● インシデントレスポンス　等
	事業ドメイン（生産現場・事業所管理）	● 現場教育・管理、設備管理・保全、QC活動 ● 初動対応　等

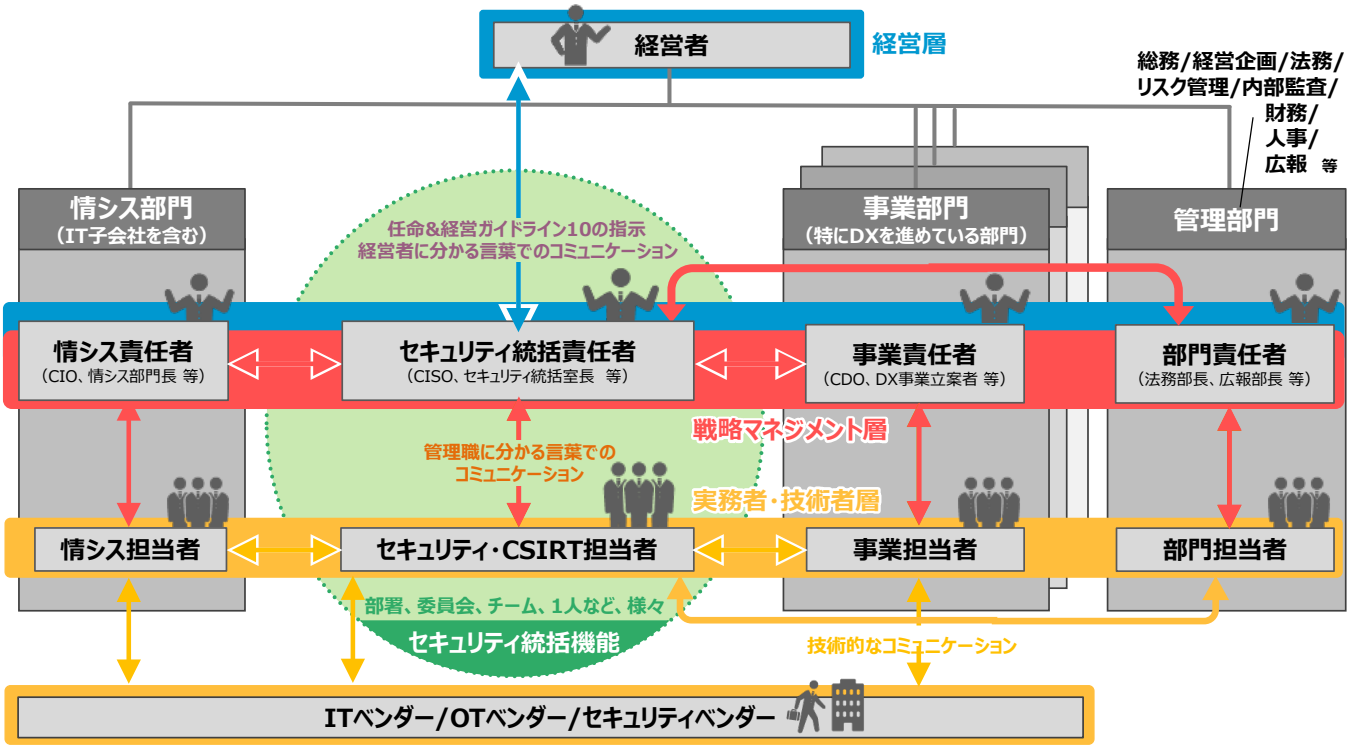
2.2【STEP2】セキュリティ統括機能を検討しましょう

ポイント：
- 全社的なサイバーセキュリティ体制の構築のためには、CISO等の経営層を補佐する「セキュリティ統括機能」の設置が有効です。
- セキュリティ統括機能の形態には大きく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ります。

(1) セキュリティ統括機能とは？

- 全社的なサイバーセキュリティ体制の構築のためには、経営層やCISO等を補佐する「セキュリティ統括機能」の設置が有効です。
- 「セキュリティ統括機能」とは、企業におけるリスクマネジメント活動の一部として、サイバーセキュリティ対策及び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、事業部門におけるサイバー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です。
- なお、サイバーセキュリティリスクへの対応については、経営層や各事業部門が主体的に責任を負いつつ、状況に応じて情報システム部門やセキュリティ統括機能と連携していく形になります。
- セキュリティ統括機能は、主に「戦略マネジメント層（赤帯部分）」と「実務者・技術者層（黄帯部分）」の２層で組織横断的に関係部署と連携し、組織的なサイバーセキュリティ対策を統括します。体制構築にあたっては、こうした機能が適切に維持されるように工夫する必要があります。

図表8　セキュリティ統括機能のイメージ



コラム：よくある勘違い

①セキュリティ統括機能を置けば、セキュリティは全部おまかせ。

→ **NO!** サイバーセキュリティ対策の実務は、デジタル技術を活用した製品・サービスの企画・開発・運用や情報の利活用を行う事業部門や管理部門の業務と密接に結びついており、それら部門が主体的にサイバーセキュリティ対策に取り組む方が、効果的・効率的な場合も多いと考えられます。また、一般の役職員が狙われるケースもあるため、それぞれの立場で全社員がサイバーセキュリティを意識し、対策を取っていく必要もあります。次のページにおいて、セキュリティ統括のタスクイメージをご紹介します。

(2) セキュリティ統括機能のタスク

- セキュリティ統括機能が担うタスクには、以下のア～ウがあります。

ア）経営層（CISO等）が行う意思決定等の補佐（図中「方針策定」）
CISOや経営層が担う業務のうち、一定の専門的な知見が必要となるものについて支援し、意思決定や判断の補佐を行います。

イ）自らが主体となって実施する実務（図中「実務」）
組織横断的対応が必要な業務を自らが主体となって実施します。

ウ）他部署が主体となって実施する実務の支援（図中「支援」「実務支援」）
事業部門や管理部門が主体となって行う実務を、一定の専門的な知見を用いて支援します。

図表9　セキュリティ統括機能が担うタスク※1

※1 一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ人材育成検討会（CRIC CSF）：
『ユーザー企業のためのセキュリティ統括室構築・運用キット（統括室キット）Part 1』（2018年11月）
https://cyber-risk.or.jp/contents/Security-Supervisor_Toolkit_Part1_v1.0.pdf

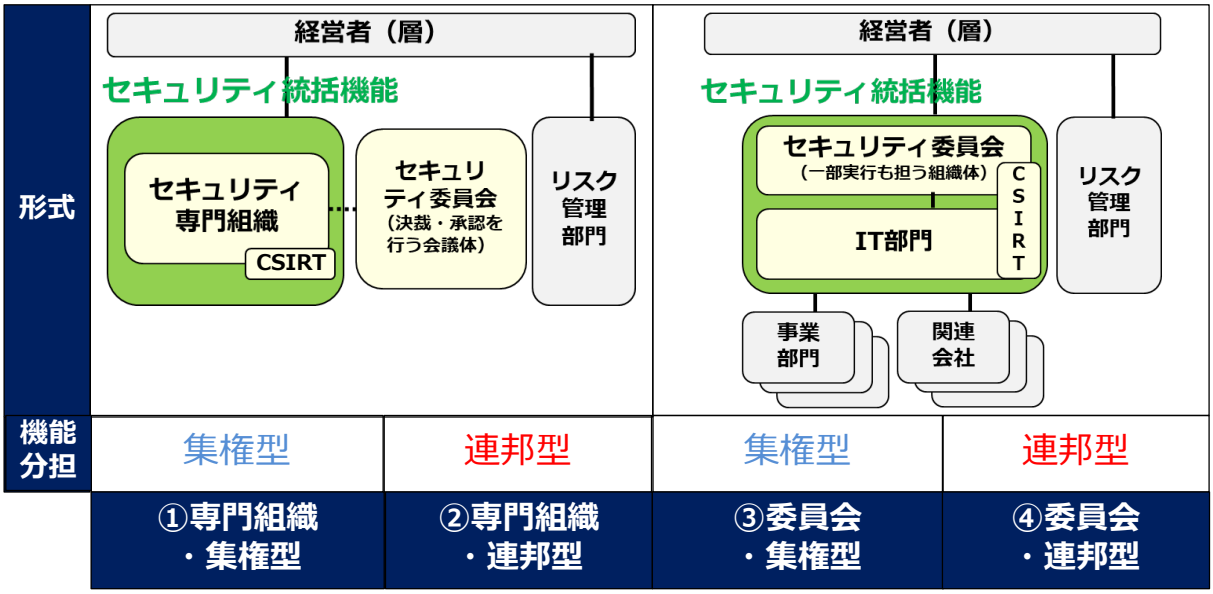
※2 Operational Technology（製造設備や重要インフラなどの制御技術）

(3) セキュリティ統括機能の設置方法

- 平成30年度に経済産業省が一般社団法人日本情報システム・ユーザー協会（JUAS）に委託した調査の報告書においては、企業へのヒアリングやアンケート結果を踏まえ、セキュリティ統括機能について、
  - セキュリティ統括機能の形態：「専門組織型」又は「委員会型」
  - セキュリティ統括機能の担う機能の範囲：「集権型」又は「連邦型」

  の２×２の４象限での類型化を行っています。
- どの形態が自社に適しているかは、企業におけるガバナンスやリスクマネジメントの体制によって変わってくるので、どの案が最良ということはありません。

図表10　セキュリティ統括機能の４類型※



セキュリティ統括機能の形態：「専門組織型」と「委員会型」

- **専門組織型**：セキュリティ統括機能を、セキュリティ統括室等の独立した部門や、情報システム部門の中のセキュリティチームなどの専門組織が担う形態。サイバーセキュリティに関する委員会で決定された方針・規定類の実行機能を担う場合が多い。
  → **セキュリティ統括機能を担うのに適切な部署が存在しない場合、このように新たな専門組織を構築することが適切です。****【参考】「セキュリティ統括室」の作り方（次のページへ）**
- **委員会型**：事業部門・管理部門・情報システム部門・関連会社等からなるセキュリティ委員会が一部の実行機能も担い、その下に情報システム部門が位置づけられ、全社的なガバナンスを行う形式。
  → **全社のIT利活用のマネジメントが情報システム部門等に集約され、すでにセキュリティ統括機能を担っている場合、改めて独立した専門組織を設けるよりも、サイバーセキュリティ対策に係る意思決定機関としての委員会と情報システム部門とでセキュリティ統括機能を分担するのが合理的です。**

セキュリティ統括機能の担う範囲：「集権型」と「連邦型」

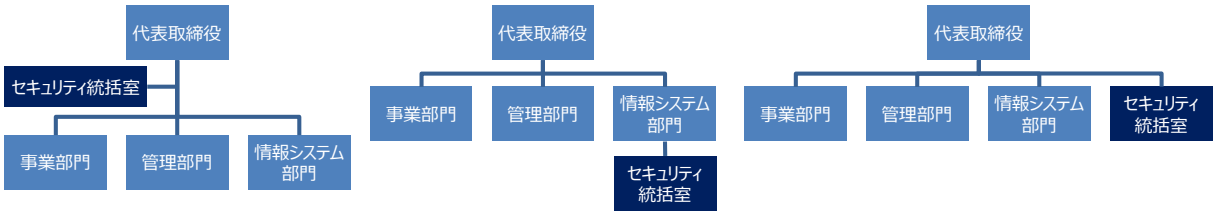
- **集権型**：全社で統一されたサイバーセキュリティ対策のルールに基づき、一元的に管理。
- **連邦型**：サイバーセキュリティ対策のうち、全社システムは一カ所で統括、各事業部・関連会社固有のシステムは各々が担当。

※一般社団法人日本情報システム・ユーザー協会（JUAS）：『平成30年度サイバーセキュリティ経済基盤構築事業（企業におけるサイバーセキュリティ体制の構築及び戦略マネジメント層の育成に関する実態調査）』（2019年3月）
https://www.meti.go.jp/meti_lib/report/H30FY/000632.pdf

（参考）セキュリティ統括室の作り方

セキュリティ統括室には、大きく分けて以下３つの類型があります。メリットデメリットを比較しながら、自組織の状況に合う形を検討してみましょう。

図表11　組織内でのセキュリティ統括機能の位置付けに関する類型※1



	社長直轄型　特命組織	情報システム部門の１機能	管理部門等との同列組織
特徴	直轄型組織は、事業活動を実施するのではなく、経営判断をサポートするために配置される。 企画に力点を置き、経営判断として各事業部門に指示を行う際の支援部署として機能する。 活動内容が明確になると組織化され独立する。	情報システム部門の中で、セキュリティ機能を担う組織として配置。 主に、OA環境※2に対するシステムセキュリティについて活動を行う。法令対応や他事業部との連携は、上位者による調整により進む。IT投資枠内で活動する。	管理部門の1つとして配置され、全社一律の対応を行う組織として配置。 人事や経理と同列にあり、事業部門を問わず、共通の標準化された対策を立案し実行する。IT投資とは別の予算措置がなされる。
メリット	経営層の危機感を直接反映し、タイムリーな意思決定が可能である。	IT予算の中で活動するため、システムに関連するセキュリティ対策の強化を迅速に進められる。	管理部門の1つとして、会社として（全社統一）の方針を出すことができ、各部門に対策を指示できる。
デメリット	ERM※3の一部として、優先順位付けが難しく、サイバーセキュリティが経営課題となるかどうかは、高度な情報収集と調整力にかかってくる。	外注比率が高く、更にセキュリティを非機能要件として後付けで考えている場合は、予算確保が難しく、対策の実効性に欠ける場合がある。	全社のセキュリティ対策を実施できる反面、個別事業に対する対策指針を策定するノウハウを集約しにくく、対策状況のモニタリングを中心とした監査的な機能になる。

※1　一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ人材育成検討会（CRIC CSF）：『産業横断サイバーセキュリティ人材育成検討会 第二期最終報告書』（2018年11月）https://cyber-risk.or.jp/cric-csf/report/

※2　OA環境：おもにオフィスで用いられるIT環境（OA：Office Automation）

※3　ERM：組織のリスクを統合的に管理する手法（Enterprise Risk Management）

コラム：セキュリティ統括機能設置の必要性･合理性

①通常時のサイバーセキュリティ対策の一元的な司令塔の必要性

- 情報システム、制御系システム、IoTシステム、外部のクラウドサービスやソフトウェア（オープンソースソフトウェア等）といった異質なシステムが、企業内の様々な部門で活用され、データ共有等のために相互に接続され複雑に入り組むように、部署ごとにサイバーセキュリティ対策方法やレベルがまちまちだと、弱いところが攻撃に悪用される恐れがあります。

②インシデント対応時の一元的な連絡調整機能の必要性

- インシデント発生時に、迅速かつ的確な判断･対応を行うためには、組織内外との一元的な連絡調整機能が必要です。このため既に多くの組織では組織内CSIRTを構築している組織もありますが、従業員の教育やソフトウェアのアップデートの徹底など、再発防止策の検討等を行うにあたっては、平時のサイバーセキュリティ対策の司令塔との連携も必要です。したがって、通常時のサイバーセキュリティ対策と緊急時のインシデント対応を一元的に統括するセキュリティ統括機能が必要となってきています。

③権限･予算･人材･情報の集約の合理性

- 権限･責任･予算を集約することで組織をスリム化することが可能。
- サイバーセキュリティ関連情報（法令、脅威情報、サービス情報等）を事業部門ごとに収集するとコストがかかるため、集約する方が合理的です。

2.3【STEP3】サイバー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

ポイント：
- セキュリティ統括機能と連携しつつサイバー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、ITSS＋（セキュリティ領域）を参考にすることで、関係部署や委託先がどのような役割を担うかが明確になります。
- サイバーセキュリティの脅威が高度化する中で、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すが、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す。

(1) サイバーセキュリティ関連タスクに関する役割と責任

- このステップでは、STEP1で洗い出したタスクをどの部署で担うかについて、割り当てを行います。
- 11ページの図表7に示したタスクについて、分野毎の担当部署の割り当て例を図表12に示します。なお、こちらはあくまで一例であり、セキュリティ統括機能が受け持つべきタスクや他の部署に割り当てるべきタスクは、組織の構造などにより異なります。また、この中には、実質的な作業を外部委託するものの、その委託先管理を行うことを通じてタスクを実施する場合も含みます。
- タスクの割り当てに際しては、割当先部署が責任に応じた権限を有しているかどうかに留意が必要です。割当先部署に責任に伴う権限がない場合、他部署による協力が十分に得られず、対策が形骸化してしまうことがあります。

図表12　17分野のサイバーセキュリティ関連タスクと担当部署の割り当て例

	分野名	サイバーセキュリティ関連タスクの例	担当部署／機能の例（青字は社外委託先等）
経営層	セキュリティ経営（CISO） デジタル経営（CIO/CDO） 企業経営（取締役）	サイバーセキュリティ意識啓発、対策方針の指示、セキュリティポリシー・予算・対策実施事項の承認　等	経営者、経営層（CISOを含む）
戦略マネジメント層	セキュリティ監査	情報セキュリティ監査、報告・助言　等	監査部門 セキュリティ専門事業者・監査法人（情報セキュリティ監査サービス）
	システム監査	システム監査、報告・助言　等	監査部門 IT専門事業者・監査法人（システム監査サービス）
	セキュリティ統括	サイバーセキュリティ教育・普及啓発、サイバーセキュリティ関連の講義・講演、サイバーセキュリティリスクアセスメント、セキュリティポリシー・ガイドラインの策定・管理・周知、警察・官公庁等対応、社内相談対応、インシデントハンドリング 等	セキュリティ専門部門、CSIRT セキュリティ委員会 IT・デジタル部門のサイバーセキュリティ対策機能
	デジタルシステムストラテジー	デジタル事業戦略立案、システム企画、要件定義・仕様書作成、プロジェクトマネジメント　等	経営企画部門、IT企画部門、IT・デジタル部門の企画機能 IT/セキュリティコンサルタント
	経営リスクマネジメント	経営リスクマネジメント、BCP／危機管理対応、サイバーセキュリティ保険検討、記者・広報対応、施設管理・物理セキュリティ、内部犯行対策　等	総務部門（リスク管理部門を含む） 経営企画部署、総務部署等のリスクマネジメント機能
	システム監査	システム監査、報告・助言　等	監査部門 IT専門事業者・監査法人（システム監査サービス）
	法務	デジタル関連法令対応、コンプライアンス対応、契約管理　等	法務部門、総務部門の法務担当
	事業ドメイン（戦略・企画・調達）	事業特有のリスクの洗い出し、事業特性に応じたサイバーセキュリティ対応、サプライチェーン管理　等	事業部門の企画機能 事業戦略コンサルタント
実務者・技術者層	脆弱性診断・ペネトレーションテスト	脆弱性診断、ペネトレーションテスト　等	IT・デジタル部門の運用機能、IT子会社 セキュリティ専門事業者（脆弱性診断サービス）
	セキュリティ監視・運用	セキュリティ製品・サービスの導入・運用、セキュリティ監視・検知・対応、インシデントレスポンス、連絡受付　等	IT・デジタル部門の運用機能、IT子会社 セキュリティ専門事業者（セキュリティ監視・運用サービス）
	セキュリティ調査分析・研究開発	サイバー攻撃捜査、原因究明・フォレンジック、マルウェア解析、脅威・脆弱性情報の収集・分析・活用、セキュリティ理論・技術の研究開発、セキュリティ市場動向調査 等	CSIRT/IT・デジタル部門のリサーチ機能、IT子会社 セキュリティ専門事業者（デジタルフォレンジックサービス）
	デジタルシステムアーキテクチャ	セキュアシステム要件定義、セキュアシステムアーキテクチャ設計、セキュアソフトウェア方式設計、テスト計画　等	IT・デジタル部門の設計機能、IT子会社 IT/OT専門事業者
	デジタルプロダクト開発	基本設計、詳細設計、セキュアプログラミング、テスト・品質保証、パッチ開発　等	IT・デジタル部門の開発・保守機能、IT子会社 IT/OT専門事業者
	デジタルプロダクト運用	構成管理、運用設定、利用者管理、サポート・ヘルプデスク、脆弱性対策・対応、インシデントレスポンス　等	IT・デジタル部門の運用機能、IT子会社 IT/OT/セキュリティ専門事業者
	事業ドメイン（生産現場・事業所管理）	現場教育・管理、設備管理・保全、QC活動、初動対応　等	運転、保全、計装、品質管理関連部署、PSIRT OT/セキュリティ専門事業者

(2) 部署間での役割分担の考え方

- 社内のサイバーセキュリティ対策をある部署に集中させ、その部署の定めるサイバーセキュリティ対策を一律で適用するような運用は効率的ではありますが、事業部門における多様なデジタル活用が行われる中、事業部門においてサイバーセキュリティ対策の責任を負うべきとの考え方が主流になりつつあります。
- したがって今後は、前ページ（１）でタスクを割り振られたそれぞれの事業関連部署が、サイバーセキュリティ対策の実施に際して専門的な知識や経験を有するセキュリティ統括機能等と適切に連携しつつ、必要なタスクを実施していく場面が増えることが予想されます。図表13に、図表12の例に記載したタスク割当先部署とセキュリティ専門部署間の連携例を示しますが、当然ながら連携方法はこれらに限定されるものではありません。
- たとえば情報システム部門がセキュリティ監視・運用を担う場合、事業部門で利用するクラウドの監視に関する連携を行うことなども考えられます。

図表13　サイバーセキュリティ対策に関する連携例

分野間の連携の組合せ		連携して行うタスクの例
経営リスクマネジメント	セキュリティ統括	サイバーセキュリティ保険加入に関する協議
法務	セキュリティ統括	法規改正への対応方針協議、契約等における対応の検討
法務	セキュリティ監査	サイバーセキュリティ対策におけるコンプライアンスの状況についての監査の実施
事業ドメイン（戦略・企画・調達）	セキュリティ統括	新規サービスに伴うサイバー関連リスクの評価
事業ドメイン（戦略・企画・調達）	セキュリティ監査	クラウドサービスの調達に関する情報セキュリティ監査の実施
事業ドメイン（生産現場・事業所管理）	セキュリティ統括	インシデント発生に備えた訓練の共同実施
事業ドメイン（生産現場・事業所管理）	セキュリティ監視・運用	事業部門で利用するクラウドサービスの監視
事業ドメイン（生産現場・事業所管理）	セキュリティ監査	事業所管理状況に関する情報セキュリティ監査の実施

(3) インシデント対応に備えた機能（xSIRT）の確保に関する検討

- インシデント対応業務には、以下の２種類があります。
  - 通常時：異常の検知・分析や関係機関との情報の共有などの活動
  - インシデント発生時：状態把握と対処、被害抑制、復旧と再発防止等の活動

  このうち後者では、通常のサイバーセキュリティ対策に投じているものとは別に、限られた期間で集中的に人的リソースが必要となる可能性があります。セキュリティ統括機能と比較すると、必要リソースが通常時とインシデント発生時との間で大きく変動することが特徴です。
- このようなインシデントへの対応を行う機能は、一般的にCSIRT（Computer Security Incident Response Team、シーサート）と呼ばれています。企業によっては、セキュリティ統括機能をCSIRTの機能に含めている場合もあります。なお、監視や検知に関する機能はSOC（Security Operation Center）と呼んで区別されることが一般的です。
- 企業の事業活動におけるインシデントには、企業で利用しているITインフラにおけるもののほか、自社で販売した製品に関わるインシデントや、自社で提供するサービスに関わるインシデントも想定されます。事業規模が大きな場合、これら製品の開発・製造やサービス提供はITインフラの管理部署とは別の部署で担当することが一般的であることから、CSIRTとは別の機能として区別して扱うほうが合理的な場合もあります。具体的な例を図表14に示します。このようなインシデント対応機能を総称して、xSIRTと呼ぶこともあります。ただし、表内の複数の機能を備えていても、１つのCSIRTとして運用するほうが合理的であれば、分ける必要はありません。NISCでも、このようなxSIRTのさらなる普及に向けた取組 を行っています。

図表14　インシデント対応に備えた機能の種類

種類	対象とするインシデント	特徴
CSIRT（組織内CSIRT）（Computer～）	組織内で利用する情報システムやネットワークにおいて発生するインシデント	● 情報システム部門やIT部門と連携して設置又は運用されることが多い ● セキュリティ統括機能と一体で運営される場合もある
OT-SIRT（Operational Technology～）	制御系設備の運用において発生するインシデント	● 工場やプラント等の各設備の事情に通じた要員で構成され、IT系のCSIRTと連携して運用されることが多い
PSIRT（Product～）	顧客に販売された製品（おもにネットワークに接続されるもの）において発生が懸念されるインシデント	● 製品開発や品質管理を担う部署と連携して設置又は運用されることが多い ● 製品開発プロセスにおけるセキュリティ・バイ・デザインの管理を兼ねる場合もある
DSIRT（Digital Service～） **SSIRT**（Service～）	顧客が利用するデジタルサービス等において発生するインシデント	● サービス提供部署との横並びの組織又は各部署のセキュリティ担当者で構成される横断組織として設置又は運用されることが多い

- xSIRTの設置方法については以下の２通りが考えられます。
  1. 常設の独立した部署とする方法
  2. 既存の部署に属するメンバーによる仮想的な、またはインシデント発生時に組成される横断的なプロジェクトチームの形で運営する方法

  後者の場合、異常の監視等のインシデント発生に関わらず行う活動は、xSIRT機能を担う既存の部署のいずれかにおける通常業務の一部として実施します。いずれの構築にあたっても、事業内容とサイバーセキュリティの知識を備えた人材の確保、関係部署間の連携、取引先等他社との組織をまたいだ連携などがポイントとなります。

(4) 自社実施と外部委託の切り分けの検討

- サイバーセキュリティの脅威が高度化する一方、多くのユーザー企業において、サイバーセキュリティ対策を担うのに必要な専門性とリソースを社内で確保できず、サイバーセキュリティに関する機能の一部の外部委託が行われています。
- 自社で実施するか外部委託するかの判断はサイバーセキュリティ経営において非常に重要な意味合いを有するものであり、サイバーセキュリティ対策の実務担当者がリソースの充足状況等で判断するのではなく、セキュリティ統括業務等を担う戦略マネジメント層より上位の階層において決定することが適切です 。
- ITSS＋ （セキュリティ領域）を用いて自社のサイバーセキュリティ体制を検討する場合、図表15,16の内容を参考に、17分野を「自社の要員で対応する分野」、「一部業務を外部委託する分野」、「自社では対応しない分野」の３種類に大まかに分類すると後の検討が行いやすくなります。

図表15 「自社では対応しない分野」の例

分野	対応の必要がない場合の条件
システムアーキテクチャ デジタルプロダクト開発 （におけるサイバーセキュリティ関連業務）	● 自社向けのデジタルシステムの開発を行わず、クラウドサービスとして提供されるSaaS※やパッケージアプリケーションのみを利用しているような場合、これらの分野を考慮する必要はない
セキュリティ調査分析・ 研究開発	● これらのタスクを遂行するには高度な専門性が求められるため、一般的な企業が自社で要員を確保して実施することはあまりない ● この分野に該当するサイバーセキュリティ関連業務として、デジタルフォレンジックのための分析等のタスクが含まれるが、こうした業務が必要となった場合はセキュリティ統括やデジタルプロダクトマネジメント、セキュリティ監視・運用等の分野の担当者が外部委託することによって対応することが一般的

図表16 「自社の要員で対応する分野」と「一部業務を外部委託する分野」の区分方法

分野区分	対応の必要がない場合の条件
必ず自社要員で対応すべき分野 **該当する分野：** **経営層が担う全分野** **セキュリティ統括** **経営リスクマネジメント** **法務** **事業ドメイン 等**	● 自社の経営判断に直結する分野や、管理部門が担当すべき分野、事業のリスクマネジメントに相当する分野の外部委託は不適切であり、少なくとも意思決定や管理は自社の要員で対応することが望ましい。 ● 現実には、担うべき役割に応じた知識やスキルを有する人材がいない可能性もあるが、この分野に関してはSTEP4以降に示す方法に従って、可能な限り速やかに確保しつつ、自社要員の責任のもと、外部専門事業者との適切な役割分担のもとで対応することが適切（※判断や管理、方針決定は自社で行うこと）。
実施者により意味合いが異なる分野 **該当する分野：** **システム監査** **セキュリティ監査**	● 監査業務については、社内の要員で行う内部監査と、外部委託して行う外部監査とでは監査の意味合いが異なることに留意し、目的に応じて使い分ける。
その他の分野 **該当する分野：** **脆弱性診断・ペネトレーションテスト** **セキュリティ監視・運用 等**	● 上記以外の分野については、経営方針やインシデント発生時の事業への影響、自社の要員・リソースの状況等に応じて許容される範囲内で業務を外部委託することが可能。 ● 分野のすべての委託は不可。次ページに示すように、「どこまで委託し、どの部分を自社でやるか」「どのような形態で委託するか」等を併せて検討する必要があることに注意。

→詳細は次のページ図表17をご参照ください。

※SaaS（Software as a Service）：ソフトウェアを自社サーバーでインストールせず、インターネット等のネットワーク経由で、サービスとして利用すること。

図表17　ITSS＋（セキュリティ領域）の各分野における外部委託の考え方

記号凡例　※：自社体制で実施すべき分野
◇：自社体制で実施しつつ、高い専門性が必要な業務を外部委託することが考えられる分野
★：自社体制での実施も可能だが外部委託することで別の効果が生じる分野
その他：外部に委託することは可能だが、意思決定・管理は自社で実施すべき分野

分野		担当するサイバーセキュリティ関連タスクの例		当該業務の外部委託の考え方
経営層	セキュリティ経営（CISO）	・サイバーセキュリティ対策に関する意思決定やそのための予算・リソースの確保	※	経営層が担う役割に関する外部委託は不適切 ・専門家を招聘してCIO/CDO /CISOに任命することは可能 ・CISO補佐やアドバイザを外部から招聘することは可能
	デジタル経営（CIO/CDO）	・デジタル利用に関する意思決定やそのための予算・リソースの確保	※	
	企業経営（取締役）	・組織のリスクマネジメントに関する意思決定やそのための予算・リソースの確保	※	（企業経営は外部委託の対象外）
戦略マネジメント層	セキュリティ監査	・サイバーセキュリティマネジメントに関する監査の実施	★	外部監査として実施する場合は外部委託の形態となる
	システム監査	・デジタル環境の管理・利用に関する監査の実施	★	外部監査を委託する場合、結果を踏まえた改善を担う体制も必要
	セキュリティ統括	・リスクアセスメント ・ポリシー・ガイドライン策定・管理 ・サイバーセキュリティ教育・社内相談対応 ・インシデントハンドリング	◇	自組織のリスクマネジメントに直結する業務であり、自社要員の責任のもと、外部専門事業者との適切な役割分担のもとで対応することが適切
	デジタルシステムストラテジー	・デジタル戦略の立案 ・システム企画、要件定義・仕様書作成 ・プロジェクトマネジメント		コンサルティングの外部委託は可能であるが、意思決定や管理は自社で行うことが適切
	経営リスクマネジメント	・BCP対応 ・内部犯行対策	◇	（社内管理部門にて対応すべきタスク）
	法務	・法令等遵守対応	◇	（必要に応じて）弁護士等の助言を得るための契約をしておくことは有用
	事業ドメイン（戦略・企画・調達）	・事業戦略立案 ・システム企画、要件定義・仕様書作成 ・プロジェクトマネジメント		コンサルティング会社等への外部委託は可能であるが、意思決定や管理は自社で行うことが適切
実務者・技術者層	脆弱性診断・ペネトレーションテスト	・脆弱性診断の実施 ・ペネトレーションテストの実施		専門性が求められるタスクであり、社内で確保できない場合は外部委託も可能であるが、委託仕様の策定や委託先からの報告への対応を担う体制が社内に必要
	セキュリティ監視・運用	・監視・検知・初動対応・原因究明 ・インシデントレスポンス		
	セキュリティ調査分析・研究開発	・脅威情報の収集・分析 ・デジタルフォレンジック ・セキュリティ技術開発		
	デジタルシステムアーキテクチャ	・セキュアシステム要件定義 ・セキュアアーキテクチャ設計 ・セキュアソフトウェア方式設計、テスト設計		専門性が求められるタスクであるため、社内で確保できない場合は外部委託も可能（なお、自社向け開発を行わず、SaaSやパッケージのみを利用する場合はこれらの割当を行う代わりに調達担当者またはセキュリティ統括担当者がそのサイバーセキュリティ対策を担当する）
	デジタルプロダクト開発	・基本・詳細設計 ・セキュアプログラミング、パッチ開発 ・テスト・品質保証		
	デジタルプロダクト運用	・構成管理、運用設定 ・脆弱性情報の収集、脆弱性対応 ・セキュリティツールの導入・運用		デジタルシステムの保守・運用の外部委託は可能だが、ユーザー権限管理等、社内で対応するのが適切なタスクも存在
	事業ドメイン（生産現場・店舗管理）	・現場教育・管理 ・設備管理・保全		一部タスクの外部委託は可能であるが、業務で利用するデジタル環境の状況は自社で把握することが適切

（参考）自社に適したサイバーセキュリティ体制の検討

- 自社に適したサイバーセキュリティ体制を検討する際の参考として、サイバーセキュリティ体制に影響を及ぼす要素の代表例を次表に示します。自社におけるこれらの影響を考慮しつつ、どのような割り当てを行うのがよいかを検討しましょう。
- 業種毎にサイバーセキュリティ体制と分野のマッピングを図示した例を巻末資料1に示します。

図表18　サイバーセキュリティ体制に影響を及ぼすと考えられる要素 の例

要素	影響の内容
業種	● 金融系ではITの利用形態が全社を通じて似通っている場合も多く、全社共通のセキュリティ統括部署を設置し、統一的なサイバーセキュリティ対策を講じることが一般的。 ● 一方、製造業では製造部門のOT環境がIT環境とは異なる独自性を有していることが多いため、営業部門を含めた統一的な体制を組むことが必ずしも合理的でない場合もある。 ● サービス業ではサービスの特性に応じて現場部門がセキュリティ統括機能を有した方が合理的な場合もある。
事業規模	● 事業規模が大きくなければ、リスク管理担当者がサイバーセキュリティも扱うことが合理的な場合もある。 ● 逆に超大手企業の場合、中央のみで一元管理しようとしても目が行き届かないこともある。
事業のバリエーション	● 複数の事業が類似している場合、共通のサイバーセキュリティ管理体制で管理するほうが効率的と考えられる。 ● 逆に、事業形態が大きく異なり、事業で扱う情報やサービスの内容等も異なる場合は、事業部毎に異なるサイバーセキュリティ体制を構築するほうが効率的となることもある。
グループ企業	● グループ企業各社の事業内容が異なっていたり、それぞれ独立した事業運営を行っていたりする場合、各社の情報及び情報技術に関するガバナンスの観点から、各社に一定のセキュリティ統括機能及び xSIRT（18ページ参照）を設置してそれぞれ判断し、必要な場合は相互に連携する体制のほうが適切なこともある。 ● 海外子会社の場合、現地の法規制（例：欧州における一般データ保護規則（GDPR））により個人情報の域外持ち出しができずアクセスログを域内で分析できるような体制が必要となることもある。
IT子会社の有無	● 自社や自社グループのITインフラの運用・管理を担うようなIT子会社がある場合、セキュリティ統括機能の一部をその子会社に任せるほうが効率的になる場合もある。
情報システム部門の有無と同部門への依存度	● 自社のITインフラを情報システム部門が一元管理している場合、同部門がサイバーセキュリティ管理に関する多くの作業を担うことが合理的。 ● 他方、情報システム部門が事業部門で扱っているITサービスを把握していない場合、サイバーセキュリティ管理に関する作業を担当する組織を別に設置することが適切なこともある。

3. サイバーセキュリティ関連タスクを担う人材の活用（指示３）

経営ガイドラインでの指示内容

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への対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させる。

取組の心構え

- STEP3で構築したサイバーセキュリティ体制を「絵に描いた餅」で終わらせず、適切に機能させるには当然ながらその運営に必要な資源として、予算と人材を確保することが必要です。
- 指示３の対象となる人材には、図表19に分類するように、セキュリティ統括機能やCSIRTなど、サイバーセキュリティ対策を目的とする業務に従事する人材と、法務、事業企画、サービス設計開発等、サイバーセキュリティ対策を目的としない業務を遂行する中でサイバーセキュリティ対策に関わる人材の２種類が含まれます。
- これまで、サイバーセキュリティ対策というと前者が行うものとのイメージがありましたが、**昨今の急速なデジタル化により、各部門が業務を遂行する上で取らなければならない対策も増えており**、両者の境界が曖昧になりつつあるほか、**後者の役割の重要性も増しています**。そのため後者については、STEP5の内容を参考に自社での対応方法を検討しましょう。
- また、前者についても、「サイバーセキュリティ人材」という単一の専門人材が存在するわけではありません。サイバーセキュリティ分野で求められる専門性はマネジメント、技術、社会、法律など多様であり、STEP3で紹介したITSS＋（セキュリティ領域）の分野等を用いてそれぞれの役割に応じた専門性の習得を目指して行くことになります。
- **サイバーセキュリティ分野は変化の激しい分野**であり、習得した知識・スキルを有効なものとして維持し続けるためには、**学習やトレーニングの継続的実施及び実践の機会確保が必要です**。STEP6に示す教育プログラムや試験・資格等の活用等を参考に、計画的な人材育成に取り組みましょう。

経営者のリーダーシップの下、次頁以降のポイントを参照しながら、適切な体制を検討しましょう

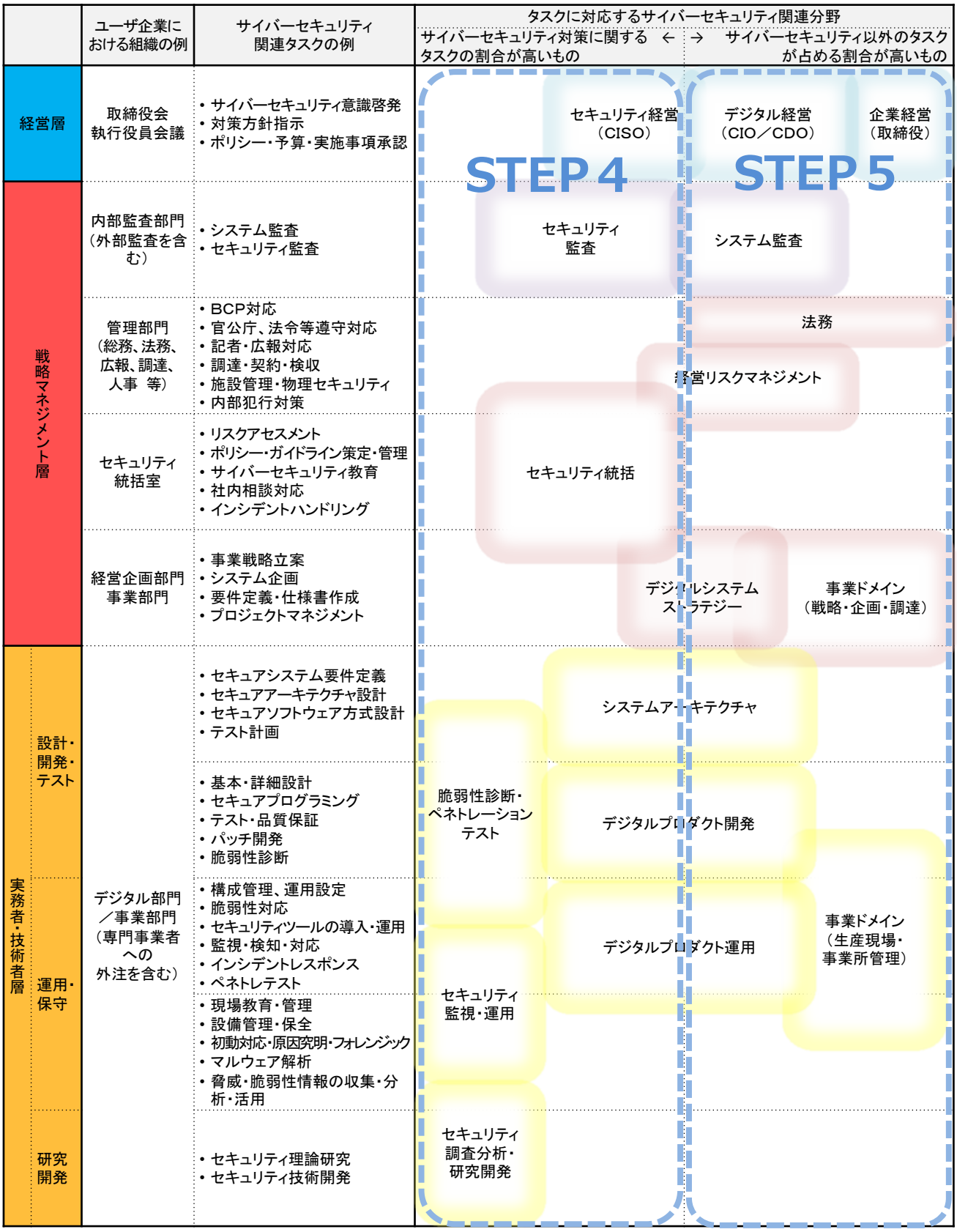
図表19　指示３で扱う人材の区分

	サイバーセキュリティ対策を主たる目的とする業務に従事する人材	サイバーセキュリティ以外を主目的とする業務を遂行する中でサイバーセキュリティ対策に関わる人材（「プラス・セキュリティ」を必要とする業務に従事する人材）
対応上のポイント	業務に必要な知識・スキルを備えた人材をどのように確保するか	サイバーセキュリティ対策の重要性を意識してもらい、その実践に必要な知識・スキルを習得してもらうにはどうすべきか
本書での説明場所	**STEP4:** サイバーセキュリティを主たる業務とする人材の確保	**STEP5:** 「プラス・セキュリティ」の取組推進

※ デジタル化の進展により、両者の境界が曖昧になりつつあり、右側の「プラス・セキュリティ」の重要性が増しています。

→ITSS＋（セキュリティ領域）における両者のイメージを次ページ図表20に示します

図表20　STEP4, STEP5の対象分野



3.1【STEP4】 サイバーセキュリティを主たる業務とする人材の確保

ポイント：

- 外部委託を積極活用していても、自社の要員として自社のサイバーセキュリティリスクを把握し、その対策を推進する立場の人材を割り当てる必要があり、当該人材にはサイバーセキュリティに関するリスクと対策について理解するのに必要な知識・スキルが求められます。
- 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、確保には工夫が必要です。

(1) サイバーセキュリティ対策業務の対象とそれを担う人材

- このステップでは、サイバーセキュリティ体制を担う人材のうち、サイバーセキュリティ対策を主たる目的とする業務や役割を担う人材をどのように確保すべきかの考え方を示します。対象となるのは、ITSS＋（セキュリティ領域）において、「セキュリティ経営（CISO）」、「セキュリティ統括」、「セキュリティ監査」、「脆弱性診断・ペネトレーションテスト」、「セキュリティ監視・運用」、「セキュリティ調査分析・研究開発」の各分野を担う人材に相当します。
- このうち、「セキュリティ統括」分野については、サイバーセキュリティ対策に外部委託を積極活用していても、企業におけるリスクマネジメント活動の一部として、対策を推進する立場の人材を自社の要員として割り当てる必要があり、当該分野を担う人材にはサイバーセキュリティに関するリスクと対策について理解するのに必要な知識・スキルが求められます。
- サイバーセキュリティ対策業務を担う人材が専任である必要はありません。ただし兼務であっても、インシデント対応の際には司令塔としての役割に専念できるようにするなど、STEP3で構築した体制が適切に機能することを意識する必要があります。

(2) サイバーセキュリティを主たる業務とする人材をどのように確保するか

- サイバーセキュリティ対策を主たる業務とする人材を新たに確保するための方法を以下に示します。どの方法が適切かは担当する役割によっても変わってきます。
- 人材を育成する方法についてはSTEP6を参照してください。

図表21　セキュリティを主たる業務とする人材を確保するための方法例

方法例	確保方法の特徴
リスクマネジメントや経営管理に関する業務経験を有する人材の配置転換及び育成	● 災害対策等のリスクマネジメントや経営上の問題への対処を行う部署での業務経験を有する人材が、サイバーセキュリティ対策業務に必要な知識・スキルを習得することによって対応する方法。 ● これまでの業務経験を活用可能な利点を有する反面、適切なサイバーセキュリティ対策を行う上で必要な知識・スキルには技術的なものも含まれることから、その習得に真剣に取り組む意欲をもった人材であることが理想（最低限「情報セキュリティマネジメント試験」に合格する程度は必要）。
ITの管理・運用に関する業務経験を有する人材の配置転換及び育成	● IT部門等で社内の情報システムやネットワークの管理・運用経験者が、サイバーセキュリティ対策業務に必要な知識・スキルを習得することによって対応する方法。 ● ITの知識・スキルがあるとサイバーセキュリティの技術的な概念を理解しやすい上、システムトラブル対応経験はインシデント対応の場面でも活用可能。 ● 反面、多くの企業でIT部門が事業部門の業務に積極的に関わってこなかったことも多く、セキュリティ統括などの機能を担うためには十分な習熟期間が必要。
セキュリティ対策関連の業務経験を有する人材の中途採用	● 他社等でサイバーセキュリティ対策業務に従事した経験を有する人材を中途採用し、自社で活用する方法。 ● 条件に見合う人材が確保できる場合には、この方法がもっとも短期間で人材を戦力化できると見込まれるが、担当する業務内容によっては自社の業務知識の習得や経験を積むのに要する期間等の考慮が必要。 ● 現在の雇用市場に流動性は存在するものの、長年にわたって需要が供給を上回っている状況にあるため、スムースに人材を確保しようとすれば社内の処遇体系を相当に上回る待遇を提示する必要が生ずる可能性。
セキュリティを専門とする教育機関を修了した人材の新卒採用	● サイバーセキュリティに関する専門教育を提供する大学院、大学、高専、専門学校などを修了した人材を新卒採用してサイバーセキュリティ対策業務を行う部署に配属する方法。 ● 一般的に、サイバーセキュリティの専門知識を有していても業務知識や経験がなければ即戦力とすることは困難であり、採用後一定期間の業務経験が必要。セキュリティ研究開発などの分野であれば業務経験よりも専門性が期待される場面もある。 ● 産学連携によるサイバーセキュリティ人材育成の取組※が始まっており、中長期的に見て専門性を有する人材の確保やプラス・セキュリティの取組に好循環を生み出す可能性。
兼業や副業で従事する人材の活用	● 新しい働き方として、他企業等でサイバーセキュリティの専門性を発揮している人材が、兼業や副業の形で別の企業のサイバーセキュリティ対策業務を担う方法も。中小企業などで、専門人材を常勤で雇用する余裕がない場合、特定の曜日のみの非常勤勤務を活用することも有効。また、専門人材が少ない地域で、１名の人材が複数企業で活躍するなどの工夫により、無理なく人材を確保することが可能に。 ● 兼業や副業での対応については、「作業を依頼できる時間に制約が生まれる」「機密保持の観点から、依頼しづらい業務もある」との懸念も示されているが、STEP6で示す情報処理安全確保支援士には、法律に基づき秘密保持義務が課されていることから、企業内の情報管理など高いレベルでの秘密保持が求められる業務も安心感をもって委託することが可能。

※独立行政法人国立高等専門学校機構による取組例（下記資料のP59）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/007_03_00.pdf

3.2【STEP5】「プラス・セキュリティ」の取組推進

ポイント：
- 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、サイバーセキュリティを意識し、業務遂行に伴うサイバーセキュリティ対策の実施に必要な能力を備えることができるように育成する「プラス・セキュリティ」の取組も重要です。
- 「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いましょう。

(1)「プラス・セキュリティ」とは

- 企業のサイバーセキュリティ対策はサイバーセキュリティ担当部署による対応のみでは対処できません。これは、企業におけるデジタル活用が進展する中で、一般的な事業活動においてサイバーセキュリティリスクを意識した対応が欠かせなくなっているためです。そこで、事業活動においてサイバーセキュリティの観点から不適切な対応を講じることで影響が懸念されるような業務を担っている人材にも、サイバーセキュリティに関する意識を養い、対策の実施に求められる知識・スキルを積極的に身につけてもらう必要があります。
- そこで、**自らの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を実現できる能力を身につけること、あるいは身につけている状態のこと**を、「プラス・セキュリティ」と定義します。「プラス・セキュリティ」は企業におけるあらゆる業務において必要です。
- 例えば、次のような業務に従事する人材において、サイバーセキュリティを自分のタスクとして認識されていないことがありますが、サイバーセキュリティリスク対策としていずれも重要です。
  - クラウドを活用した新規事業を立ち上げるプロジェクトの企画担当者
    → サイバーセキュリティの知識が不十分な場合、目的にそぐわない不適切なクラウドを選定することや、シャドークラウド化（自社のサイバーセキュリティ担当者が把握していないクラウド）により、情報漏洩等のインシデントリスクが高まる恐れがあります
  - 製品設計において組込ソフトウェアの機能仕様を設計する担当者
    →サイバーセキュリティの知識が不十分な場合、製品にサイバー攻撃に対する脆弱性を生じさせる恐れがあります
  - 自社の電話、インターネット設備、複合機等の保守契約を扱う総務担当者
    →サイバーセキュリティの知識が不十分な場合、不適切な設定のまま運用してしまうことで、当該機器を介した情報漏えいの原因となる恐れがあります
  - デジタルシステムの開発・運用を循環的に実施するDevOpsモデルでは、計画→設計→開発→テスト→デプロイ※→運用といった一連の流れにおいて、23ページの図表20の「システムアーキテクチャ」「デジタルプロダクト開発」「デジタルプロダクト運用」などの分野を担う担当者が、それぞれの場面でサイバーセキュリティ対策を実施することになります。なお、DevOpsに関しては、サイバーセキュリティ対策を実施することを強調した表現として、"DevSecOps"という表現も用いられています。

※デプロイ：ここではテスト済みのアプリケーション等のソフトウェアを実際の運用環境に導入・設定して利用可能にするプロセスの意味で使用しています。

(2)「プラス・セキュリティ」が必要となる人材の意識付け・責任明確化

- 「プラス・セキュリティ」の重要性は前述の通りですが、事業部門や管理部門の人材は、しばしばサイバーセキュリティを自分のタスクとして認識していない場合があります。こうした状況では、セキュリティ統括人材が関係部門と連携しながら企業全体としてサイバーセキュリティ対策を講じることも難しくなります。
- このため、「プラス・セキュリティ」を必要とする業務を担うこうした人材、例えば総務・法務・調達部門といった管理部門の人材、事業戦略を考える事業部門の人材等に対しては、自社のサイバーセキュリティを確保する上で重要な役割を担っていることを意識させる必要があります。具体的には、自社で実施しなければならないサイバーセキュリティ関連タスクの一部を担っていること、及びその責任・権限がどのようなものかを、組織として明確化し、担当者に自覚させることが求められます。
- さらに、「プラス・セキュリティ」を必要とする業務に従事している人材についても、サイバーセキュリティ対策業務を担う人材と同様、サイバーセキュリティに関する知識・スキル・経験を習得するための教育機会の提供や人材の育成・配置を行うことが必要です。具体的な方法はSTEP6を参照してください。

コラム：「プラス・セキュリティ」を正しく理解する

「プラス・セキュリティ」の重要性に対して注目されるようになってから日が浅いこともあり、誤解されていることもあるようです。誤解されやすい点について以下に補足します。

①「プラス・セキュリティ」人材という人材を別に確保する必要はない

26ページ(1)（「プラス・セキュリティ」とは）に例示したような業務に従事する人材が、サイバーセキュリティの知識やスキルを習得することが「プラス・セキュリティ」の取組に相当します。同様に、「プラス・セキュリティ」知識がこれまでのサイバーセキュリティ知識とは別に存在するわけではありません。

②「プラス・セキュリティ」は、DXに取り組んでいなくても必要

DXへの取り組みの有無に関わりなくITを活用して事業を行うすべての企業等で必要です。

③「プラス・セキュリティ」の取組は技術系以外でも必要

サイバーセキュリティに関する知識の中には、情報の保護方法と法律との関係、ステークホルダーからの信頼感醸成のための情報提供のあり方等、法務や広報のような技術系以外の業務に従事する人材が活用することで有効に機能するものもあります。

④「プラス・セキュリティ」で求められる知識・スキルには高度なものもある

「プラス」の語感から付加的な印象を受けるかもしれませんが、「プラス・セキュリティ」の対象となる業務で求められるセキュリティの知識・スキルと、サイバーセキュリティの専門業務で用いられる知識・スキルとの間でレベルに明確な違いがあるわけではありません。どちらの業務においても、平易なものから高度なものまで幅広く活用します。

3.3【STEP6】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

ポイント：
- 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・資格の活用を検討しましょう。
- 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しましょう。

(1) 各分野に求められる知識・スキルの概観

- STEP4及びSTEP5で紹介した人材にサイバーセキュリティに関する知識・スキルを習得してもらう際には、担当する業務分野によって求められるサイバーセキュリティ関連の知識・スキルの種類や深さが異なることに留意が必要です。例えば、CSIRT業務を担う場合は業種に関わらず、サイバーセキュリティに関する体系的な知識・スキルが求められます。
- 各分野に求められる知識・スキルの概観については、ITSS＋（セキュリティ領域）の各分野とサイバーセキュリティ関連知識・スキルの関係を整理した 図表22を参考にして下さい。
- 知識・スキルの詳細 については、情報処理安全確保支援士試験シラバス※の小項目を参考にして下さい。

図表22 ITSS＋（セキュリティ領域）で求めるサイバーセキュリティ関連知識・スキル

【注釈】
1）「◎」は主導できるレベル（情報処理安全確保支援士試験レベル）、「○」はコミュニケーションが取れるレベル（情報セキュリティマネジメント試験レベル）を想定。
2）企業等によって、「◎」、「○」の付し方の変更や、知識・スキル項目の追加・削除・詳細化が必要。
3）分野に固有のタスクを実施するための知識・スキルについては含まれていない。

	分野	セキュリティ関連知識・スキル（大項目）		
		セキュリティマネジメント	システムセキュリティ	セキュリティオペレーション
戦略マネジメント層	経営リスクマネジメント	○		
	法務			
	システム監査			
	事業ドメイン（戦略・企画）			
	セキュリティ統括	◎	○	○
	セキュリティ監査			
	デジタルシステムストラテジー			
実務者・技術者層	デジタルシステムアーキテクチャ	○	◎	○
	デジタルプロダクト開発			
	脆弱性診断・ペネトレーションテスト	○	◎	◎
	セキュリティ監視・運用			
	セキュリティ調査分析・研究開発			
	デジタルプロダクト運用		○	○
	事業ドメイン（生産現場・店舗管理）			○

大項目	セキュリティマネジメント	システムセキュリティ	セキュリティオペレーション
大項目の概要	経営層の下で組織の特性に応じた適切なセキュリティ体制・ポリシーの構築・運用が行える	セキュアなシステムの企画・設計・開発が行える	セキュリティインシデントへの事前対策・事後対応が適切に行える
情報処理安全確保支援士試験シラバス4つの大項目との対応	(1)情報セキュリティマネジメントの推進又は支援に関すること	(2)情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること	(3)情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること (4)情報セキュリティインシデント管理の推進又は支援に関すること

※独立行政法人情報処理推進機構（IPA）：「情報処理安全確保支援士試験シラバス」
https://www.jitec.ipa.go.jp/1_13download/syllabus_sc_ver2_0.pdf

(2) 教育プログラム・コミュニティ活動の活用

- 各分野の人材が必要な知識・スキルを身に着けるため、及びこれを評価する一つの方法として、教育プログラムやコミュニティ活動の活用が考えられます。
- かつてサイバーセキュリティ対策を担う人材を対象とする教育プログラムは技術系のものが主体でしたが、現在は図表23のようにセキュリティ統括機能を担う人材の育成を対象とした教育コースも多数提供されています。
- 一般の企業において、深刻な脆弱性を悪用した攻撃や悪質なマルウェアの蔓延など、大がかりなインシデント対応を必要とするような事象については、一定の期間でのジョブローテーションを行っていると、任期中に一度も経験しないこともあります。このように、発生頻度の低い業務をOJTで習得させることは必ずしも効率的ではないことから、業務経験させることにこだわらずにインシデント対応演習等の教育・研修サービスを利用することで、実践的なスキルの習得を図ることも検討すべきです。
- NISCのポータルサイト（https://security-portal.nisc.go.jp/ ） では、「対象者」（経営層、戦略マネジメント層、実務者・技術者層）や「難易度」（初級・中級・上級）ごとに活用可能なサイバーセキュリティ関連の教育プログラムやコミュニティ活動等が紹介されていますので、活用を検討ください。
- このほか、民間でもサイバーセキュリティ対策を担う人材の適材配置による人材不足解消を目指して、技術系のスキルに限らずヒューマンスキル等も含めた可視化を行うサービスが提供されています。

図表23　セキュリティ統括機能及び管理部門向け教育プログラム例

プログラム例	提供機関	教育プログラムの内容	お勧めする受講者層
中核人材育成プログラム ※1	独立行政法人情報処理推進機構（IPA）産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）	• 社会インフラ・産業基盤のサイバーセキュリティ対策の強化をテーマに、１年程度のトレーニングを通じてテクノロジー（OT・IT）、マネジメント、ビジネス分野の総合的な学習を通じて経営層と現場担当者を繋ぐ人材（中核人材）を育成。 • OJTで習得することが困難な総合的視点からのサイバーセキュリティを理解した人材の育成が可能。	• 戦略マネジメント層 • 次世代の戦略マネジメント層 • OT・IT系実務者・技術者層
戦略マネジメント系セミナー ※2	独立行政法人情報処理推進機構（IPA）産業サイバーセキュリティセンター（ICSCoE）	• 事業とICT活用をリスクマネジメントの観点で結び付けられる人材の育成に向け、経営層をはじめとする関係者が認知しておくべきサイバーセキュリティ機能の理解を目的としたコースを提供。	• 経営層 • 戦略マネジメント層
キャリアアップMOTサイバーセキュリティ経営戦略コース※3	国立大学法人東京工業大学環境・社会理工学院技術経営専門職学位課程	• サイバーセキュリティ経営及びその戦略立案に求められる知識・能力を備え、企業・組織を先導する人材の育成が目的。 • 経営に影響を及ぼすサイバーセキュリティに関連するリスク・危機管理に重点を置き、グループ発表やワークショップ等を積極的に取り入れたコースを提供。	• 次世代の企業経営を担う人材（戦略マネジメント層、実務者・技術者層等）
実践的サイバー防御演習CYDER（CYber Defense Exercise with Recurrence） ※4	国立研究開発法人情報通信研究機構ナショナルサイバートレーニングセンター	• サイバー攻撃を受けた際の一連の対応（インシデント対応）をパソコンを操作しながらロールプレイ形式で体験できる演習プログラムを提供。 • 全都道府県で実施。	• インシデント対応業務を担う実務者・技術者層（地方公共団体等、重要インフラ事業者）

※1　https://www.ipa.go.jp/icscoe/program/core_human_resource/index.html
※2　https://www.ipa.go.jp/icscoe/program/middle/strategic_management/index.html
※3　https://www.academy.titech.ac.jp/cumot/cy/
※4　https://cyder.nict.go.jp/

(3) 試験・資格の活用

- 各分野の人材が必要な知識・スキルを身に着けるため及びこれを評価する一つの方法として、試験・資格（以下、「資格等」といいます。）の活用が考えられます。企業に在席している人材が資格等を活用することには、次のような利点があります。
  - ある役割や業務を担うために必要なスキルを習得したい場合、当該業務に関する知識を有していることを認定する目的の資格等の取得を目標として教育計画を設計することで、効率よく修得することができます。
  - 取引先等からのサイバーセキュリティ対策に関する取り組み状況の照会に対して、業務従事者における資格等の保有状況を示すことは社外に対する客観的な裏付けとなります。
  - 委託先で同様の試験・資格を取得している人材との間で、試験・資格のシラバスで用いられる用語を共有できるため、コミュニケーションの円滑化が期待できます。
  - 継続教育制度を有する試験・資格の場合、その学習義務を積極的に活用することで、サイバーセキュリティやデジタル分野で重視される最新の知識・スキルの獲得が容易になります。
- 企業の戦略マネジメント層や実務者層のサイバーセキュリティ担当者が活用可能な試験・資格の例を本書の巻末資料2「活用可能な試験・資格の例」に示します。これらのうち、IPAで実施している２種類の資格・試験制度の概要を図表24に示します。
- なお、試験の合格及び資格の取得後も、サイバー脅威環境と技術の進歩についていくためには、たゆまない勉学が必要であり、そのための環境作りも求められます。

図表24　IPAで実施している資格・試験制度の概要

方法例	確保方法の特徴
情報処理安全確保支援士（登録セキスペ）	● 登録セキスペは、サイバーセキュリティの確保を支援するため、サイバーセキュリティに係る最新の知識・技能を備えた専門人材を対象に、2016年10月に創設された国家資格。情報処理安全確保支援士試験の合格によりサイバーセキュリティの専門家として必要とされる専門分野の知識・技能を有することを確認している。 ● 他方、デジタル技術の急速な発展に伴い、サイバーセキュリティ上のリスクも多様化・高度化していることから、登録セキスペには、この知識・技能を維持、向上させるための定期的な講習が義務づけられている。具体的には、以下の２種類の講習を受講することとしている： ➢ 最新のサイバーセキュリティに関する知識・技能及び遵守すべき倫理などの習得を目的としたオンライン形式による講習（共通講習（オンライン講習）） ➢ 知識・技能の実践的な活用力などの習得を目的としたグループ討議等による講習（実践講習） ● 登録セキスペを安心感をもって活用できる仕組みとして、登録セキスペには、無資格者による名称使用の禁止（名称独占）、信用失墜行為の禁止、秘密保持義務があり、特に、無資格者による名称使用と登録者の秘密保持義務違反は、刑罰の対象となっている。
情報セキュリティマネジメント試験	● 情報セキュリティマネジメント試験は、国家試験である情報処理技術者試験の１区分として、2016年4月から開始。本試験は、情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定するもの。 ● 情報システムの利用部門における情報セキュリティリーダーとして、部門の業務遂行に必要な情報セキュリティ対策や組織が定めた情報セキュリティ諸規程の目的・内容を適切に理解し、情報及び情報システムの安全な活用を推進する人材が対象。

(4) 人材育成計画の検討

＜共通事項＞

- サイバーセキュリティ対策に関する知識・スキルの育成においては、マネジメント、技術、法制度等、幅広い分野の学習が必要になります。業務によっては国際情勢や社会、メディア、心理等の知識が必要になることもあって、業務の合間に習得を図ろうとすると、十分な時間をかける必要があります。短期での育成を図ろうとする場合には、「(2) 教育プログラム・コミュニティ活動の活用」で紹介した教育プログラムのように、一定の期間に集中して受講できる制度の活用も検討することが適切です（次ページ事例１参照）。
- 「プラス・セキュリティ」を必要とする部署においては、予め決められたサイバーセキュリティ対策を実践するほかに、「自部署の業務においてサイバーセキュリティに関してどのようなリスクがあって、どのように対応する必要があるか」について、業務の分析及び社内のサイバーセキュリティ対策の関係者との協議を行う役割の人材を育成する必要があります。このような人材の育成には、サイバーセキュリティ対策に際して、「どのような点を意識し、自らの業務に照らしてどのような対策をとる必要があるのか」を考える実践経験が有用となります。このような経験を自部署内のOJTで経験することは難しいので、本人の希望を踏まえ、以下のようなサイバーセキュリティ担当部署との兼務ないし異動を通じて実践を積んだり（次ページ事例２参照）、大学等の社会人向けサイバーセキュリティ教育プログラムを活用したりすることが考えられます。
  - 専門部署型のセキュリティ統括機能をもつ企業の場合：
    セキュリティ統括部署に1～2年程度異動して実務経験を積む。
  - 委員会型のセキュリティ統括機能を有する企業の場合：
    自社のセキュリティ委員会あるいはリスクマネジメント委員会のメンバー又は事務局を兼務することで、2～3年程度の実務経験を積む。
- サイバーセキュリティに関するリスクマネジメント業務を担う際には、「組織マネジメント」と「デジタル技術」の両面の知識・スキルが求められますが、多くの企業においてその両方に長けている人材はまれです。そこでいずれかの知識・スキルを有する人材が他方の知識・スキルを習得することになりますが、一般には組織マネジメントの経験がより重要とされており、こうした経験を有する人材にデジタル技術とそのサイバーセキュリティ対策を学んでもらうのが最も合理的と考えられます。しかしながら、技術的なバックグランドがない中で実用レベルまで知識・スキルを高めるハードルが高いとも言われており、逆パターンであるデジタル技術系の業務経験者を一定期間セキュリティ統括機能等のリスクマネジメント機能を担う部署に異動するなどして、マネジメント系の業務経験を積む方法も活用されています。
- セキュリティ人材や「プラス・セキュリティ」を身につけた人材の確保・育成のためには、こうした人材の職位や給与における厚遇など、組織的な人事制度の見直しを行うことも有効です。

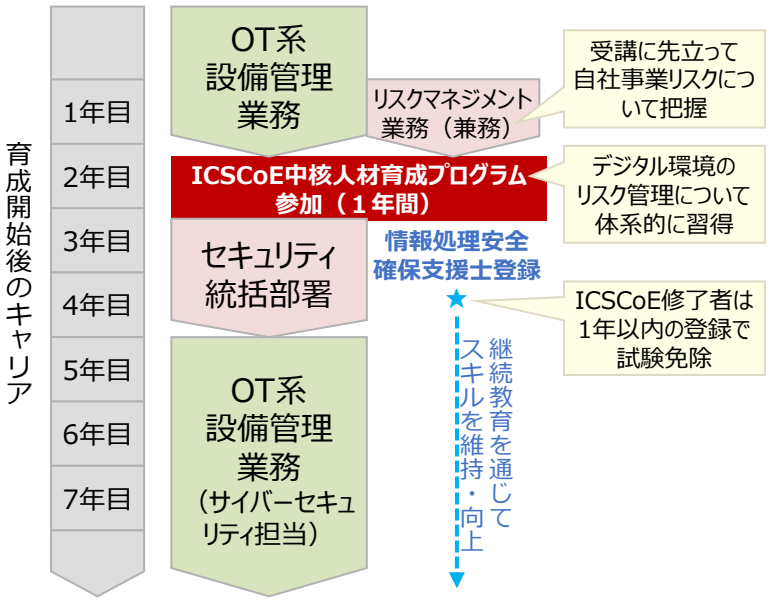
＜業種・業務別事項＞

- 制御系のサイバーセキュリティ対策を担う人材を育成する場合については、OT環境の業務知識を有する人材に対して、デジタル技術とサイバーセキュリティ対策に関する知識・スキルを習得してもらう方法が適切です。これは、デジタル技術やサイバーセキュリティ対策に関しては、市販の書籍や教育プログラムが各種整備されているので学習が比較的容易なのに対し、OT環境については各社固有であることが一般的であるため実用的な知識・スキルを後から短期間で習得することが困難なことによります。なお、その場合でもOT環境のサイバーセキュリティ対策の責任者として育成を図る場合には、上述の「プラス・セキュリティ」の場合と同様、セキュリティ統括機能での実務経験を積むことが望まれます。

(4) 人材育成計画の検討（事例）

事例1：制御系設備全体のサイバーセキュリティ担当者の育成

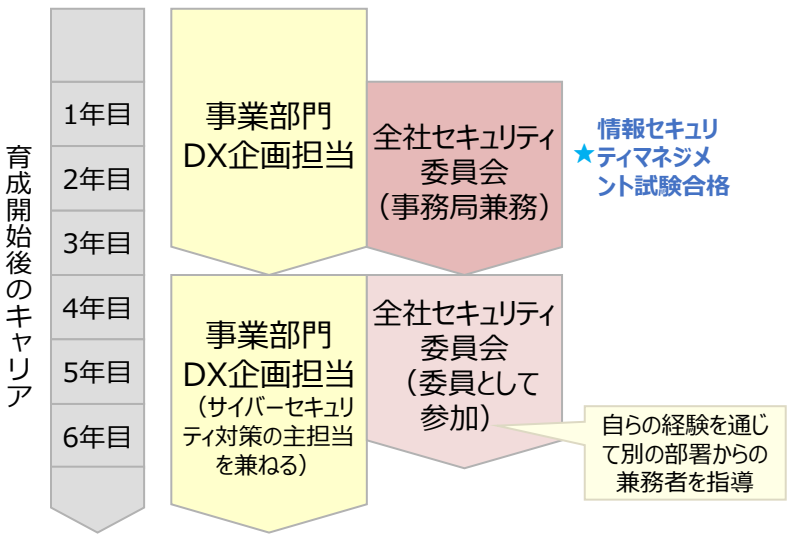
工場におけるOT環境に通じた人材にサイバーセキュリティに関する技術とマネジメントを体系的に学んでもらうことで、将来的にOT環境のサイバーセキュリティ対策の中核メンバーとして活躍してもらうことが考えられます。このような場合、前述のICSCoEで知識・スキルを習得した上で、自社のセキュリティ統括機能に配属し、社内の対策に関する実務経験を積んでもらうことで効率的な育成を図ることができます。



- サイバーセキュリティのリスクマネジメントを行うための実務能力を得るために学ぶべき知識・スキルの範囲は幅広いため、ICSCoEのような１年間の集中講座で体系的に学ぶのは効果的です。
- ただし、受講経験を効果的に活かすためには、受講前の意識付けや、受講後のOJTを通じた習得内容の実務能力化など計画的なローテーションの工夫なども併せて検討することが求められます。
- ICSCoEにはサイバーセキュリティ対策を担う人材同士の社外チャネル形成の効果もあり、復帰後のセキュリティ統括部署の業務での活用が期待できます。
- サイバーセキュリティリスク対応の経験は、将来経営層として迅速な判断を要求される経営リスクマネジメントを担う際にも役立つものと期待されます。

事例2：「プラス・セキュリティ」を身につけた人材の育成

DXを活用した事業の企画担当者が、そのサイバーセキュリティリスクの対処方針を立案・推進するために必要となる「プラス・セキュリティ」のための知識・スキルを習得するため、自社のセキュリティ統括機能を担う「セキュリティ委員会」の事務局業務を通じて実務経験を積むことが考えられます。



- 自部署の事業を通じて発生するサイバーセキュリティリスクに対してどのような対策を講じるべきかは、全社方針を踏まえつつ最終的に事業の内容を熟知している部署において判断することが適切ですが、その判断に必要なスキルを自部署のOJTのみで取得するのは困難です。
- そこでこの例では、全社のセキュリティ委員会の事務局業務を兼務で担当することで対策の考え方や協議すべき内容等について実務を通じて学びます。

巻末資料１．業種別のサイバーセキュリティ体制の考え方

- 以下の４種類のケースについて、サイバーセキュリティ体制の考え方を紹介します。
  - ① 金融業
  - ② ネットサービス業
  - ③ 製造業
  - ④ 重要インフラ（電力・ガス業）
- この事例を自組織のサイバーセキュリティ体制構築の参考にする際には、次の点にご留意ください。
  - ✓ 業務の特徴を踏まえた構成例として示していますが、当然ながら「こうしなければならない」というものではありません。自組織の構成に応じた体制を作ることが肝心です。
  - ✓ STEP2に示した通り、セキュリティ統括機能の実現形態も、企業のガバナンス形態に応じて適した形が変わってきます。また、事業部門や情報システム部門・デジタル部門等との役割の分担方法についても事業内容によって変わります。
  - ✓ CSIRT機能を組織として独立させる必要はありません（②ネットサービス業の例を参照）。
  - ✓ OT環境はそれぞれ固有の環境となるので、組織全体の体制の在り方とは別にOT環境の実態を踏まえたサイバーセキュリティ体制をOTの担当部署を中心に検討する必要があります。③の例ではOT環境向けに全社CSIRTとは別にOT-SIRTを設置していますが、これも全社CSIRTに集中してよい場合もあれば、事業内容（製品種類、プラント種類等）に応じて複数のOT-SIRTを設置した方がよい場合もあります。自社に相応しい体制を選択するためには、以下のような方法が考えられます。
    - ➢ 業界のISAC※や業界団体、ユーザー企業団体のコミュニティ等で有益な情報を共有する
    - ➢ OT系に強いセキュリティコンサルタント等に相談する
    - ➢ ICSCoE等で体系的な知識を習得する

※ ISAC（Information Sharing and Analysis Center）：サイバー攻撃対策に関するセキュリティ情報の共有を目的とする組織のこと。

サイバーセキュリティ体制と分野のマッピング例①：金融業

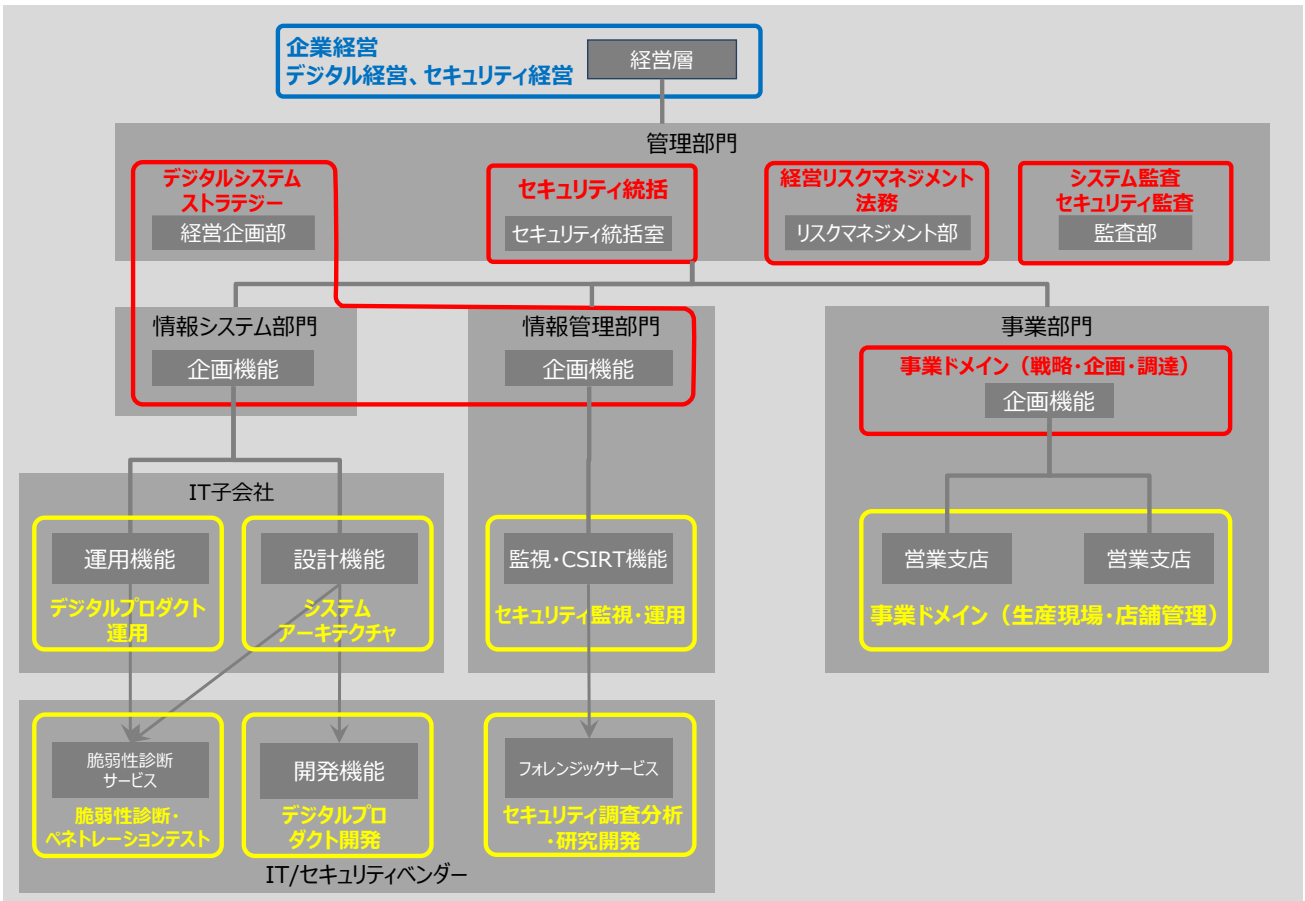
＜特徴＞

- 金融業では複数の異なる事業を行っていても、それぞれのITシステムの利用形態は全社を通じて似通っており、これまでITシステムを集約的に管理してきたことから、こうした実態に親和性の高い**「集権型」**のサイバーセキュリティ体制を構築している。
- デジタル系の戦略・企画を、事業部門と情報システム部門及び情報管理部門の双方で検討しており、両者の中立的な立場でセキュリティ統括機能を**「専門組織型」**の「セキュリティ統括室」として設置している。
- IT子会社がグループ内のITの運用管理に関するアウトソーシング先として機能しており、実務者・技術者層の機能はこのIT子会社と外部専門事業者にて担当している。

＜効果を高めるためのポイント＞

- ITSS＋で定めている分野をそれぞれ異なる部署や子会社/外部専門事業者で担っているため、それらがバラバラに各組織の都合を優先させるのではなく、連携して機能させるためのグループガバナンスが重要になる。

企業における各分野のマッピングの例（金融業）



サイバーセキュリティ体制と分野のマッピング例②：ネットサービス業

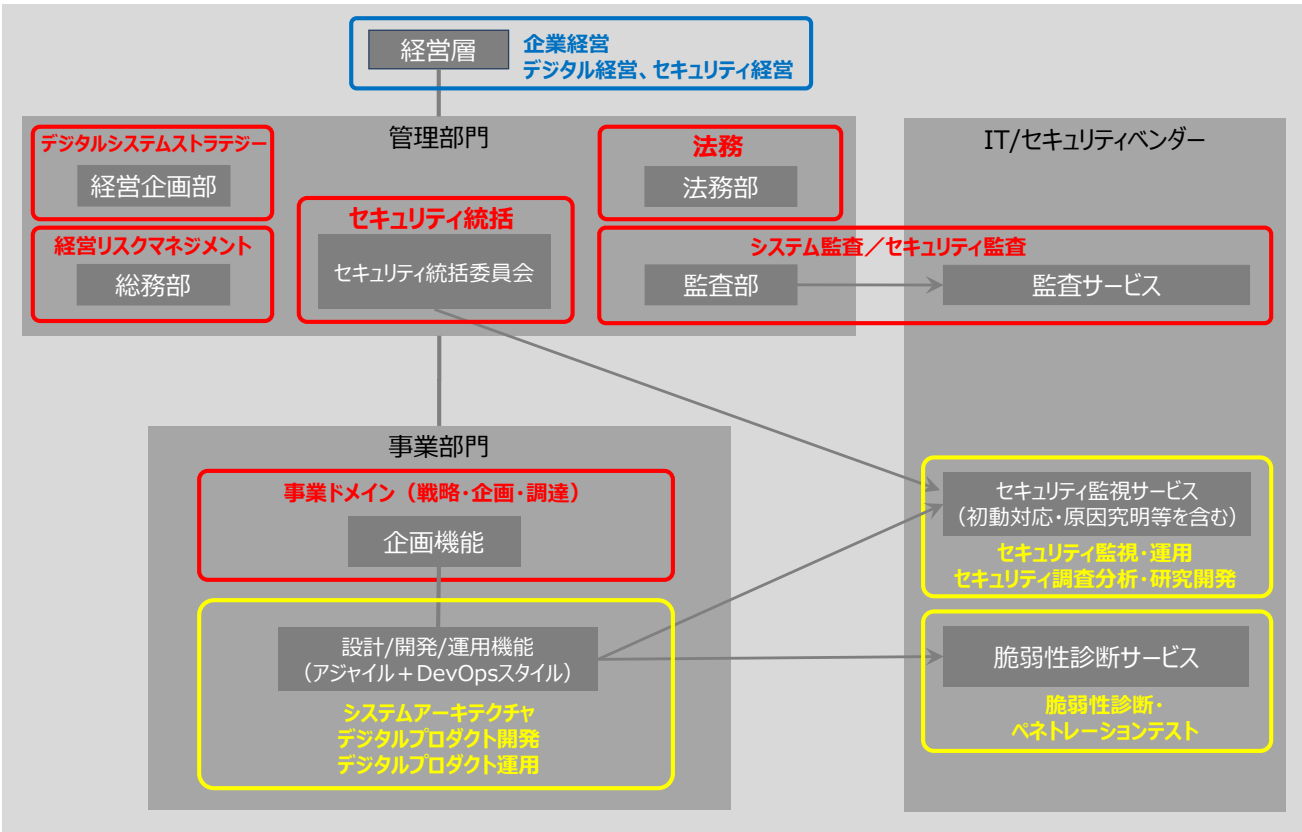
＜特徴＞

- 自社事業において用いるデジタル系のシステム・サービスの開発及び運用について、迅速なサービスインの実現等の観点から社内の事業部門における同一の体制にて実施（DevOps）している。これを踏まえ、サイバーセキュリティ対策についても共通の体制にて対応している。
- 事業戦略部門にサイバーセキュリティを担当させると、事業優先で後回しにされたり、重要度を下げられたりする恐れがあるため、セキュリティ統括機能を**「委員会型」**の「セキュリティ統括委員会」として管理部門内に設置し、事業部門に対するガバナンスを利かせている。
- 自社の従業員数が少ないため、自社の社員が携わるのは必要最小限にとどめ、委託可能なタスクは最大限外部委託により対応している。CSIRT機能についても、委託可能な機能（初動対応・原因究明等を含む）は可能な限りIT/セキュリティ専門事業者への委託とし、判断やコミュニケーションなど自社で担うべき機能のみをセキュリティ統括委員会で担う形態で実現している。

＜効果を高めるためのポイント＞

- 事業部門側の機能が一本化されているのに対し、管理側の機能が複数部署に分かれていることから、管理側が個別に事業部門に照会するなどして事業部門の負担になることのないよう、委員会として窓口を集約するなどの工夫が考えられる。

企業における各分野のマッピングの例（ネットサービス業）



サイバーセキュリティ体制と分野のマッピング例③：製造業

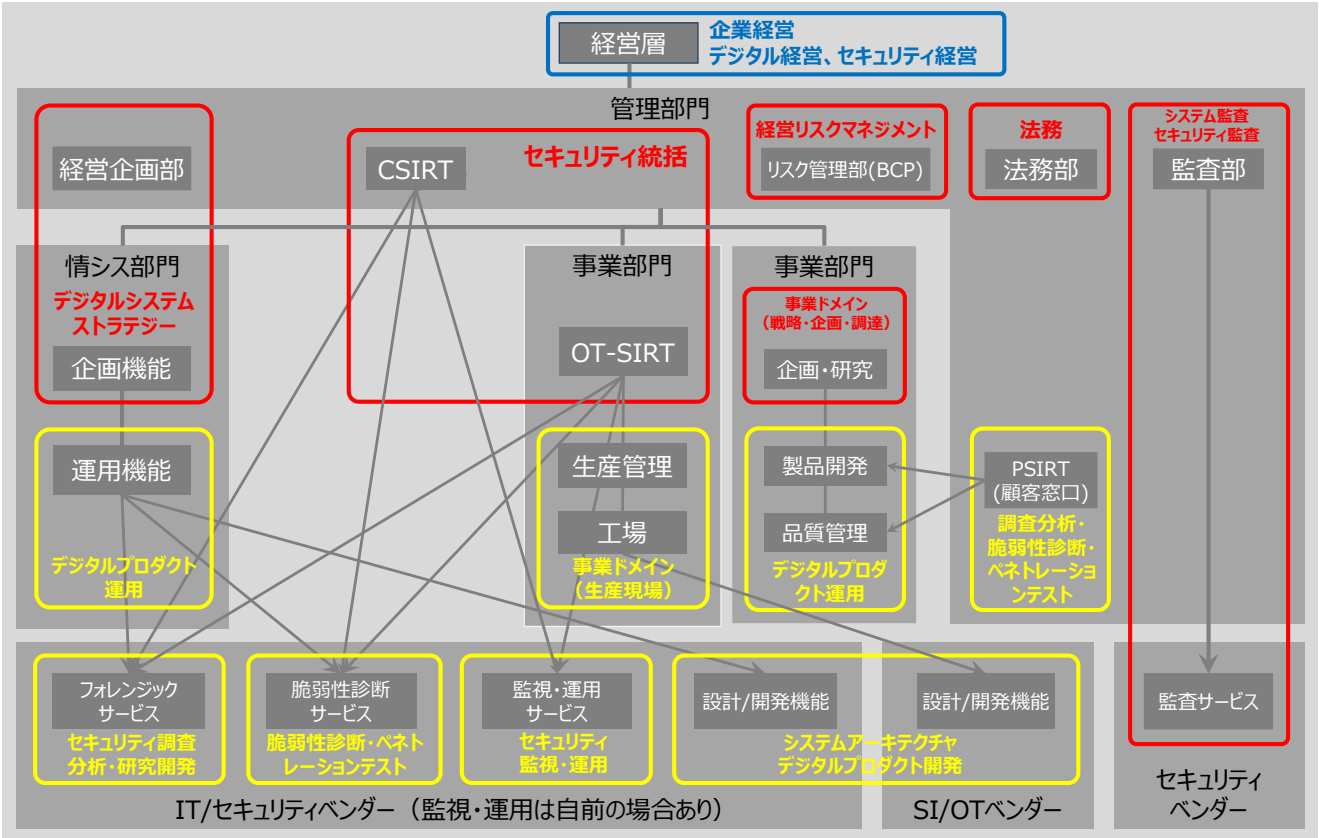
＜特徴＞

- 製造設備の運用上のサイバーセキュリティ機能を担う「OT-SIRT」、製品の品質管理上のサイバーセキュリティ機能を担う「PSIRT」、それ以外のデジタル環境を対象とする「CSIRT」の３者にて、セキュリティ統括機能を担当している。
- PSIRTは製品を利用する顧客に関わるインシデント対応を主たる機能とする。事業部門単位で設置し、製品開発プロセスにおけるセキュリティ・バイ・デザインの管理も兼ねる場合もある。
- 事業部門内でも、研究開発系の現場と生産系の現場とで管理体系が異なっていることを考慮した役割分担を実施している。

＜効果を高めるためのポイント＞

- 事業部門が管理部門のサイバーセキュリティ対策に関する方針に非協力的といった状況を避け、部門間の協調を促進するには、CSIRTとOT-SIRTの間での人事交流や兼務などの工夫を講じることで、両者の意思疎通を緊密化させることが考えられる。

企業における各分野のマッピングの例（製造業）



サイバーセキュリティ体制と分野のマッピング例④：重要インフラ（電力・ガス業）

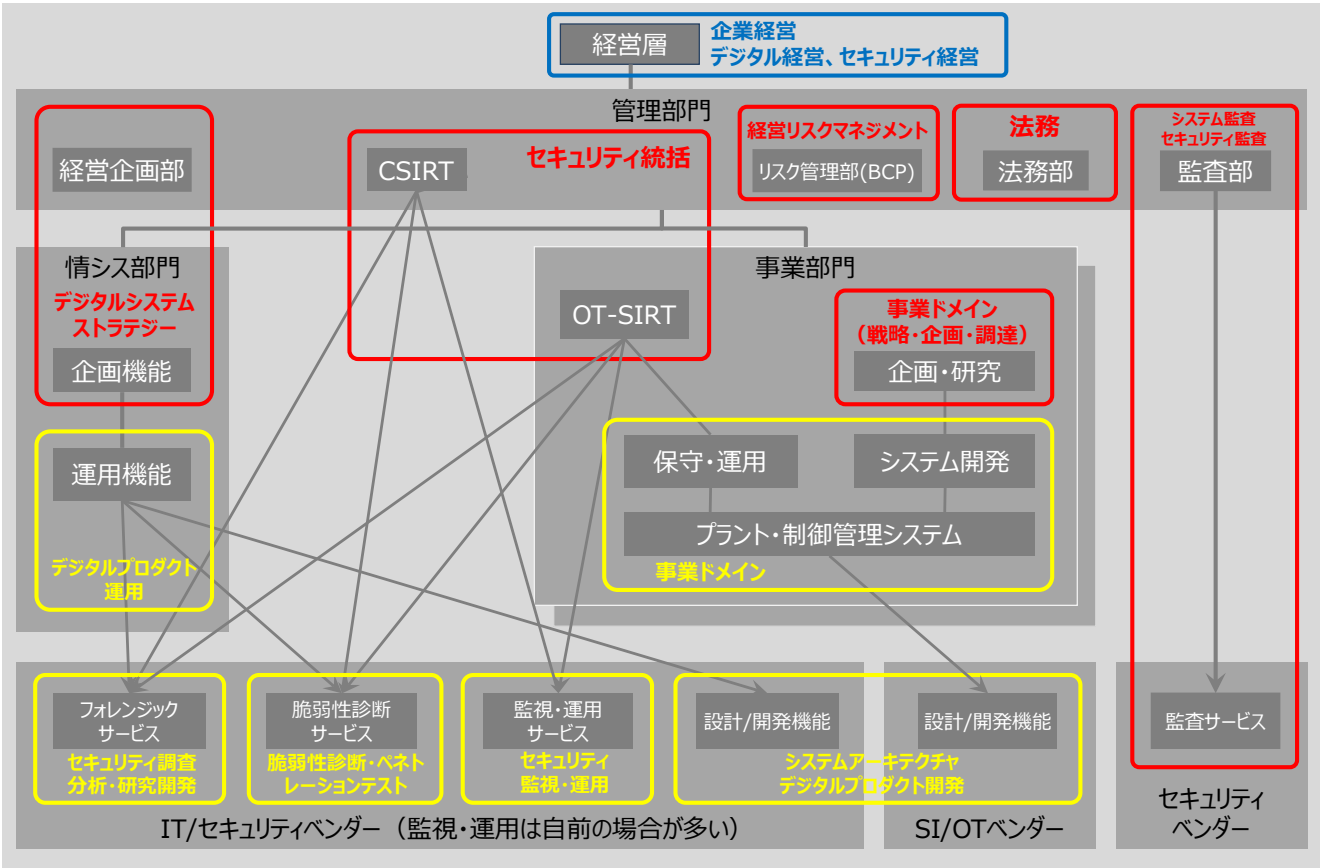
＜特徴＞

- 社内の情報系ネットワークは本社で一元管理されており、これらを管理する情報システム部門において、情報系の設備・環境を対象とする企画から運用に至るまでのサイバーセキュリティ対策を担当している。
- 事業部門ではプラント等に対応した専用かつ独立性の高いOT環境を運用していることから、OT環境の管理単位ごとにインシデント対応等を担う「OT-SIRT」を設置。これと全社のサイバーセキュリティ対策を統括するCSIRTとの連携によってセキュリティ統括機能を提供している。
- セキュリティ監視・運用に関するタスクに関しては、自社設備の異常に関する監視を情報システム部門・事業部門それぞれの保守・運用部署にて担当。部門間及び社外とのネットワークにおける監視についてはCSIRTの統括のもとでセキュリティ専門事業者に外部委託している。

＜効果を高めるためのポイント＞

- 図では明示されていないが、グループ子会社等が多数存在する場合があり、グループ全体での機能確保、グループガバナンス等に配慮することが望ましい。

企業における各分野のマッピングの例（電力・ガス業）



巻末資料２．活用可能な試験・資格の例

	ITSS+（セキュリティ領域）の分野	試験・資格名称	対象者等	日本語試験	運営主体
共通	（分野不特定）	情報処理安全確保支援士試験	サイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し、また、サイバーセキュリティ対策の調査・分析・評価を行い、その結果に基づき必要な指導・助言を行う人材	有	IPA
		情報セキュリティマネジメント試験	情報システムの利用部門にあって、情報セキュリティリーダとして、部門の業務遂行に必要な情報セキュリティ対策や組織が定めた情報セキュリティ諸規程（情報セキュリティポリシを含む組織内諸規程）の目的・内容を適切に理解し、情報及び情報システムを安全に活用するために、情報セキュリティが確保された状況を実現し、維持・改善する人材	有	IPA
		ITパスポート試験	ITを利用するすべての社会人、これから社会人となる学生	有	IPA
		CISSP	情報セキュリティ分野でリーダーとして活躍する人材	有	(ISC)[2]
		CompTIA Security+	エンタープライズ環境のセキュリティ体制の評価から、適切なセキュリティソリューションを推奨および実装、運用するITセキュリティに携わる全ての人材	有	CompTIA
		CSBM（SEA/J基礎）	情報セキュリティに関係する営業、サービスエンジニア、初級技術者、社内システム部門担当者、およびシステム関係企業の従業員	有	SEA/J（セキュリティ・エデュケーション・アライアンス・ジャパン）
		GSEC	情報セキュリティの専門家になるためのスタートとして、実務的な基礎スキルの習得を目指す人材	有	SANS
戦略マネジメント層	経営リスクマネジメント	CRISC	組織におけるリスクマネジメント（リスク認識・評価）や情報システムコントロールの設計・導入・運用に携わる人材	無	ISACA
	システム監査	公認情報システム監査人(CISA)	情報システムの監査および、セキュリティ、コントロールに携わる人材	有	ISACA
		システム監査技術者試験	監査対象から独立した立場で、情報システムや組込みシステムを総合的に点検・評価・検証して、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性などに対する保証を与える、又は改善のための助言を行う人材	有	IPA
	セキュリティ監査	公認情報セキュリティ監査人(CAIS)	情報セキュリティ監査の計画立案、監査実施、報告書の作成及び監査結果の被監査主体への報告等を担う人材	有	JASA
	セキュリティ統括	公認情報セキュリティマネージャー(CISM)	企業・団体等の情報セキュリティプログラムに係る、マネジメント、設計、監督を行う人材	有	ISACA
	デジタルシステムストラテジー	ITストラテジスト試験	企業の経営戦略に基づいて、ビジネスモデルや企業活動における特定のプロセスについて、情報技術（IT）を活用して事業を改革・高度化・最適化するための基本戦略を策定・提案・推進する人材等	有	IPA

（次ページに続く）

（前ページからの続き）

	ITSS+（セキュリティ領域）の分野	試験・資格名称	対象者等	日本語試験	運営主体
実務者・技術者層	（分野横断的）	CompTIA Advanced Security Practitioner(CASP+)	リスクマネジメント、エンタープライズセキュリティの運用とアーキテクチャ、調査とコラボレーション、およびエンタープライズセキュリティの統合を行うセキュリティアーキテクト	有	CompTIA
	デジタルシステムアーキテクチャ	システムアーキテクト試験	ITストラテジストによる提案を受けて、情報システム又は組込みシステム・IoTを利用したシステムの開発に必要となる要件を定義し、それを実現するためのアーキテクチャを設計し、情報システムについては開発を主導する人材	有	IPA
	デジタルプロダクト開発	CSSLP	ソフトウェアライフサイクルのセキュリティ対策に携わる人材	無	(ISC)^2
	脆弱性診断・ペネトレーションテスト	CompTIA PenTest+	ネットワーク上の脆弱性を特定、報告、管理するため、業務を理解し、実践的なペネトレーションテストを行うサイバーセキュリティプロフェッショナル	有	CompTIA
		CEH	情報セキュリティの責任者/監査人/専門家、サイト管理者等	有	EC-Council
		GPEN	ベストプラクティスの手法と方法論を使用して、ペネトレーションテストを適切に実施する実務者	無	SANS
		GWAPT	侵入テストとWebアプリケーションのセキュリティ問題の完全な理解を通じて、組織をより安全に保護する実務者	無	SANS
		SecuriST/認定脆弱性診断士	WebシステムやWebアプリケーション、ネットワークシステムの要件定義、開発、テスト、品質管理等の担当者	有	グローバルセキュリティエキスパート
	セキュリティ監視・運用	GCIH	セキュリティインシデントを検出、対応、および解決する実務者	無	SANS
		GCIA	ネットワークとホストの監視、トラフィック分析、および侵入検知に関する実務者	無	SANS
		GMON	SOC等における監視業務の実務者	無	SANS
	セキュリティ調査分析・研究開発	CompTIA CySA+	ネットワークとデバイスのビヘイビア分析を適用し、継続的なセキュリティモニタリングを通しサイバーセキュリティの脅威を検出、防止、対処するサイバーセキュリティアナリスト	有	CompTIA
		GCFE	デジタルフォレンジック解析の実務者	無	SANS
		GCFA	高度なインシデント対応とデジタルフォレンジックの実務者	無	SANS
		GNFA	ネットワークに関する侵入調査とフォレンジックに関する実務者	無	SANS
		デジタル・フォレンジック・プロフェッショナル資格認定	デジタル・フォレンジック関連業務に携わる人材及びデジタル・フォレンジックに関する知識を得ようとする人材	有	デジタル・フォレンジック研究会
	デジタルプロダクトマネジメント	SSCP	ネットワーク・システム開発や運用などに従事し、組織の観点からセキュリティを理解することを目指す人材	有	(ISC)^2
		ITサービスマネージャ試験	サービスの要求事項を満たし、サービスの計画立案、設計、移行、提供及び改善のための組織の活動及び資源を、指揮し、管理する人材	有	IPA
	事業ドメイン（生産現場・事業所管理）	GICSP	産業分野における制御システムエンジニアなどの実務者	無	SANS

巻末資料３．サイバーセキュリティ体制・人材に関する参考文献

企業におけるサイバーセキュリティ体制・人材の確保に関する検討のための参考文献として、本書で参照したものを以下に示します。なお、サイバーセキュリティ分野の変化の速さを踏まえ、本書の公表以降にそれぞれの文献が改訂されている可能性があります。その場合は最新の版を参照するようにしてください。

名称	**サイバーリスクハンドブック　取締役向けハンドブック　日本版**
発行者	一般社団法人日本経済団体連合会（経団連）
概要	米国と英国においてそれぞれ取締役向けに公表されていたサイバーリスクに関する文献において示されていた、サイバーセキュリティに関する５つの原則が日本企業においても当てはまると考えられることから、サイバーセキュリティに関する国際的な業界団体であるInternet Security Alliance（ISA）、日本電信電話株式会社（NTT）ならびに株式会社日立製作所の協力を得て、経団連において翻訳・整理の上公表したものです。
URL	https://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.html
公表時期	2019年10月31日

名称	**産業横断サイバーセキュリティ人材育成検討会報告書（第一期・第二期） ユーザー企業のためのセキュリティ統括室構築・運用キット（統括室キット）**
発行者	産業横断サイバーセキュリティ検討会
概要	産業横断サイバーセキュリティ人材育成検討会※における2016年9月までの活動成果が第一期報告書で、2018年12月までの活動成果が第二期報告書でそれぞれ公表されています。本書で紹介している統括室キットは、ユーザー企業がセキュリティ機能を実現するための構築ステップを可視化する方法について、組織体制の特徴に応じて整理しています。 （2020年10月20日より産業横断サイバーセキュリティ検討会に名称変更）
URL	第一期報告書　https://cyber-risk.or.jp/sansanren/ 第二期報告書　https://cyber-risk.or.jp/cric-csf/report/ 統括室キット他　https://cyber-risk.or.jp/contents/
公表時期	統括室キット：2019年月日Part1 ver1.0、2019年9月30日 Part2 ver1.0

名称	**サイバーセキュリティ経営ガイドラインVer2.0実践のためのプラクティス集**
発行者	独立行政法人情報処理推進機構（IPA）
概要	「情報セキュリティの取組みはある程度進めてきたが、サイバー攻撃対策やインシデント対応は強化が必要。それに向けた体制づくりや対策は何から始めるべきか」と考えている経営者やCISO等、セキュリティ担当者を主な読者と想定し、ガイドラインの「重要10項目」を実践する際に参考となる考え方やヒント、実施手順、実践事例を記載しています。
URL	https://www.ipa.go.jp/security/fy30/reports/ciso/index.html
公表時期	2022年3月30日公表（第3版）

（前ページからの続き）

名称	**セキュリティ対応組織（SOC/CSIRT）の教科書 ～機能・役割・人材スキル・成熟度～**
発行者	特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）／ 日本セキュリティオペレーション事業者協議会（ISOG-J）
概要	企業におけるSOCやCSIRT等の組織を対象に、これらのセキュリティ対応組織において求められる共通的な機能や役割を洗い出した上で、それらをどのように組合せ、実行していくべきかをセキュリティ専門事業者の知見をもとにまとめたものです。「教科書」に相当する本編のほか、概要版に相当するハンドブックやセルフチェックシート等も提供されています。
URL	https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html
公表時期	2018年3月30日　第2.1版（2019年2月にセルフチェックシート更新）

名称	**CISOハンドブック　業務執行のための情報セキュリティ実践ガイド**
発行者	（著者）特定非営利活動法人日本ネットワークセキュリティ協会（JNSA） 社会活動部会CISO支援ワーキンググループ （発行）技術評論社
概要	CISOが経営陣の一員としてセキュリティ業務を執行する上で前提となる、ビジネス（経営）の基本的な枠組みを整理し、明確にすべき目標と指標、そして施策を評価する判断基準を提供することを目的として、次のような活用を想定して作成されています。 ・経営会議で資料を作る際のひな型として ・技術担当からCISOになった人がビジネスを理解するための参考として ・セキュリティ担当経験の少ないCISOがセキュリティ業務を理解するための参考として ・経営会議で話される業務執行の概要を理解する参考として ・ビジネスに関連付けた計測項目と判断基準の例として ・ビジネスに沿ったセキュリティ計画や、事業継続計画の策定の資料として
書籍情報	ISBN978-4-297-11835-8
公表時期	2021年2月2日（初版）

名称	**Framework for Improving Critical Infrastructure Cybersecurity** （重要インフラのサイバーセキュリティを改善するためのフレームワーク）
発行者	National Institute of Standards and Technology（NIST）
概要	重要インフラのサイバーセキュリティリスクへの対策を組織が効果的に検討するための「共通言語」として、以下の３要素を提示しています。（本書9ページに主要カテゴリを掲載） ・フレームワークコア：重要インフラに共通するセキュリティ機能のカテゴリの体系 ・インプリメンテーションティア：リスクに対する組織のアプローチを考察するための視点 ・フレームワークプロファイル：組織の特徴に応じて選択するカテゴリの組合せ これらのフレームワークは重要インフラに限らず、あらゆる業界、組織で利用可能です。
URL	原文　https://www.nist.gov/cyberframework IPAによる和訳　https://www.ipa.go.jp/security/publications/nist/index.html
公表時期	2018年4月16日　Version 1.1

本文書について

本文書は、2019年から2021年にわたって実施した経済産業省『令和元年度サイバーセキュリティ経済基盤構築事業（企業におけるサイバーセキュリティ人材・体制に関する実態調査）』及び『令和２,3年度サイバー・フィジカル・セキュリティ対策促進事業（サイバーセキュリティ経営に関する調査）』ならびに独立行政法人情報処理推進機構『Reスキル・人材流動の実態調査及び促進策検討』の各事業成果をもとに、以下に示す有識者会合における議論を通じてとりまとめられたものです。

関連有識者会合一覧

	有識者会合名称	設置期間	開催数
①	セキュリティ人材活躍モデル検討ワーキンググループ	2019年7月～2019年12月	5回
②	DXに対応する人材の在り方研究会 セキュリティワーキンググループ	2020年1月～2020年3月	3回
③	セキュリティ経営・人材確保の在り方検討タスクフォース	2020年4月～2022年3月	18回
④	サイバーセキュリティ人材政策に関する非公式勉強会	2018年～（不定期）	9回

有識者会合委員一覧

対象者名（敬称略）	所属（2022年3月時点）	参加会合（上表①～④）			
		①	②	③	④
荒川　大	一般社団法人サイバーリスク情報センター 事務局長 株式会社ENNA 代表取締役	●	●	●	●
佐々木 弘志	フォーティネットジャパン株式会社 OTビジネス開発部 部長			●	
武智　洋	一般社団法人サイバーリスク情報センター 代表理事 日本電気株式会社 サイバーセキュリティ戦略本部 エグゼクティブエキスパート	●	●	●	●
平山　敏弘	学校法人電子学園 情報経営イノベーション専門職大学（iU）教授 特定非営利活動法人日本ネットワークセキュリティ協会 教育部会長	●	●	●	●
宮下　清	一般社団法人日本情報システム・ユーザー協会 主席研究員			●	●
持田　啓司	情報セキュリティ教育事業者連絡会（ISEPA）代表 株式会社ラック　シニアコンサルタント	●	●	●	●
④については上記メンバー以外に以下の関係者が参加： 学校法人岩崎学園情報セキュリティ大学院大学 独立行政法人国立高等専門学校機構 産業横断サイバーセキュリティ検討会※ 一般社団法人日本情報システム・ユーザー協会 特定非営利活動法人日本ネットワークセキュリティ協会					
オブザーバ：　内閣サイバーセキュリティセンター、総務省、経済産業省、独立行政法人情報処理推進機構					

※　2020年10月19日までは産業横断サイバーセキュリティ人材育成検討会