経済産業省

資料６

経済産業省取組状況の報告

2020年7月31日

経済産業省　商務情報政策局

サイバーセキュリティ課

ニーズとシーズのマッチングのための『セキュリティ人材活躍モデル』の構築

● セキュリティ人材の役割定義の共通言語化等により、ニーズとシーズの見える化・マッチングを図る。

ユーザー企業	主にIT・セキュリティベンダー	人材

必要な機能（タスク）

企業において必要なセキュリティ機能は技術者のみでは確保できない

・セキュリティポリシー策定
・リスクマネジメント
・インシデント対応　等

機能を担う役割の整理

役割（ロール）

様々な団体から役割定義が公開されているが、目的や用途の違いもあり共通言語化されていない

自社ビジネスとセキュリティを理解し、事業の企画や調達等を行う役割		指示に基づき、専門的な業務を行う役割
・CISO ・戦略マネジメント層 ・運用担当　等	指示 ⇒ ⇐ 提供	・フォレンジックアナリスト ・脆弱性診断士 ・セキュリティ監査人　等
⇒ 主に内製で育成		⇒ 主に外注で確保

役割とスキルの紐づけ

知識・技能（スキル）

・ITSS+(IPA)
・SecBoK(JNSA)
・統合セキュリティ人材モデル
・NICEフレームワーク（NIST）　等

スキルと資格等の紐づけ

資格・試験

・登録セキスペ
・民間資格　等

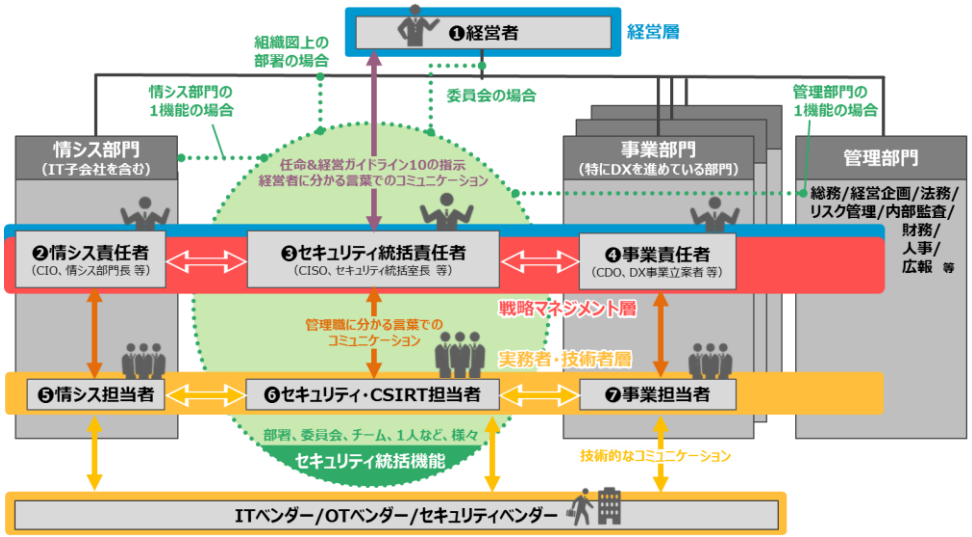
研修

・ICSCoE
・JNSA
・CRIC CSF　等

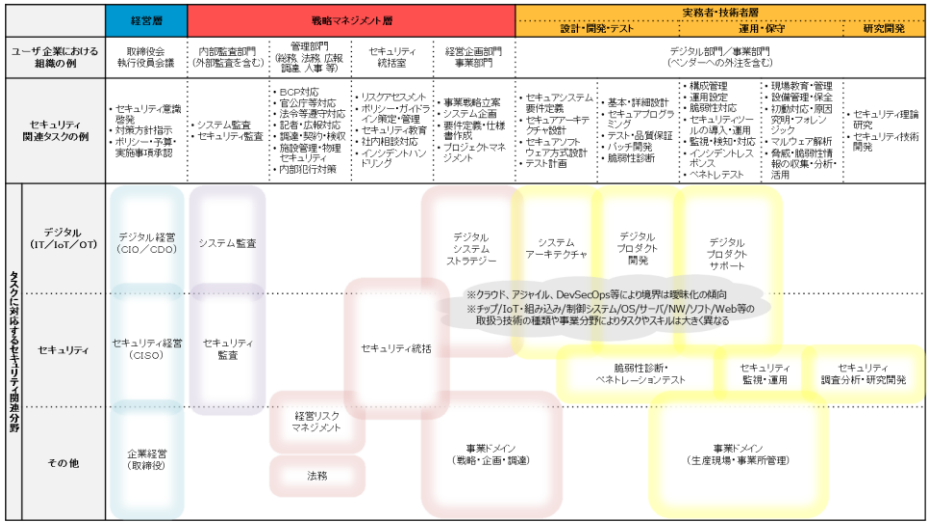
教育

・大学シラバス
・高専カリキュラム　等

論点１：ユーザー企業のセキュリティ体制・人材の見える化

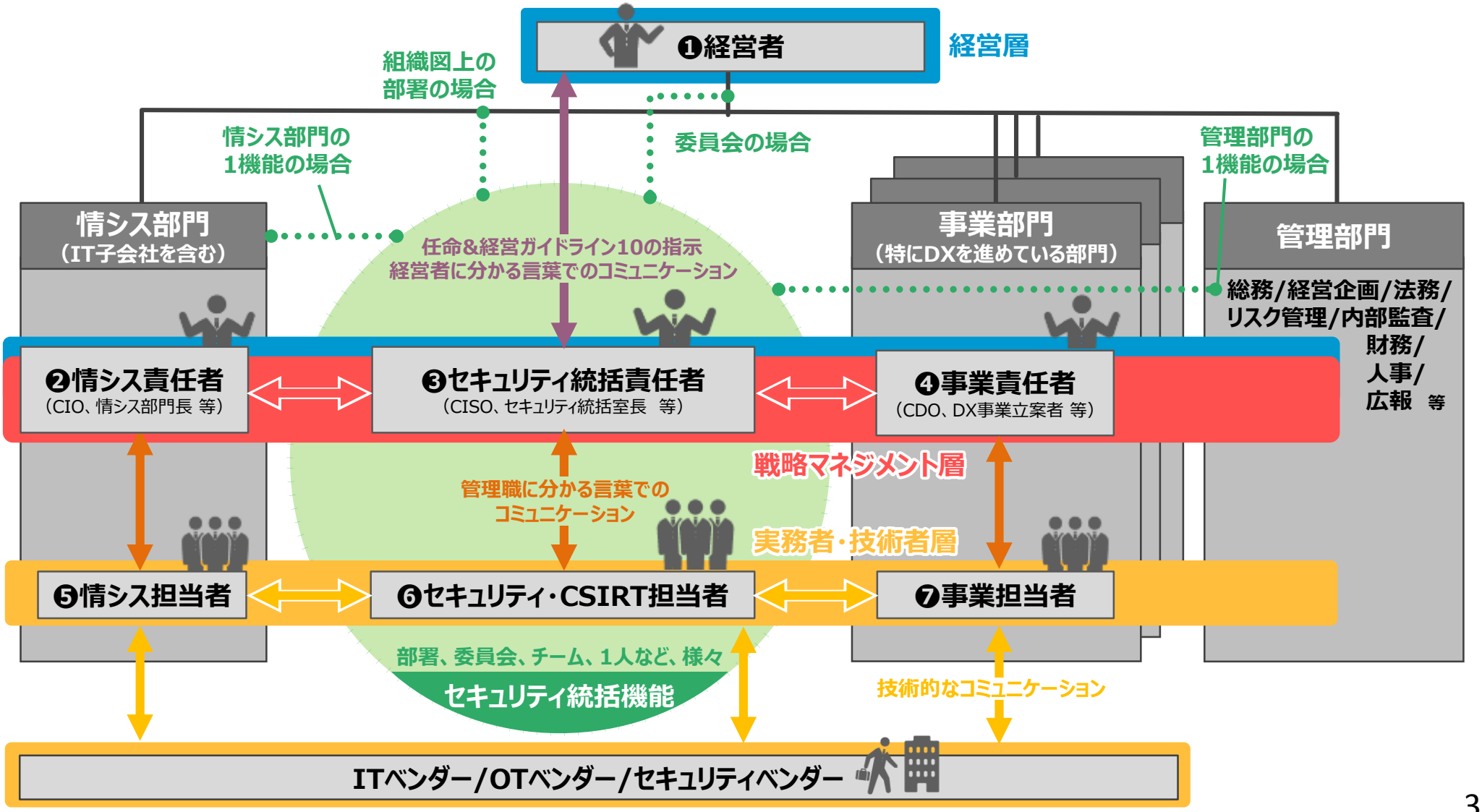


論点２：分野・タスク・スキル等の整理・明確化



（論点１）ユーザ企業におけるセキュリティ体制・人材に関する概念整理

- NISC、IPA、CRIC CSF、JNSA、JUASとの議論を踏まえ、ユーザ企業における諸概念を図式的に整理。
- その後、ユーザー企業におけるセキュリティ体制構築・人材確保のための手引きを開発中。後述のITSS＋とも連動。



（論点２）セキュリティ分野の役割定義

- セキュリティ分野では、目的や用途に応じた様々な役割定義が存在。

＜各団体による役割・専門分野の定義の例＞

ITSS+ (セキュリティ領域) 【METI / IPA】	SecBoK 2019 【JNSA】	人材定義リファレンス 【CRIC CSF】	統合セキュリティ人材モデル 【サイバーセキュリティ人材育成スキーム策定共同プロジェクト】	NICEフレームワーク (Specialty Areas)【NIST】
情報リスクストラテジ	CISO	CISO/ CRO/ CIO等	セキュリティコンサルタント	Risk Management
情報セキュリティデザイン	POC (Point of Contact)	サイバーセキュリティ統括（室等）	セキュアシステムプランナー	Software Development
セキュア開発管理	ノーティフィケーション	システム部門責任者	セキュアシステムデベロッパー	Systems Architecture
脆弱性診断	コマンダー、トリアージ	システム管理者	セキュアアプリケーションデベロッパー	Technology R&D
情報セキュリティアドミニストレーション	インシデントマネージャー、インシデントハンドラー	ネットワーク管理者	セキュリティマネージャー	Systems Requirements Planning
情報セキュリティアナリシス	キュレーター	CSIRT責任者	セキュリティオーディター	Test and Evaluation
CSIRTキュレーション	リサーチャー	サイバーセキュリティ事件・事故担当	システムリスクアセッサー	Systems Development
CSIRTリエゾン	ソリューションアナリスト、セルフアセスメント	セキュリティ設計担当	ペネトレーションテスター	Data Administration
CSIRTコマンド	脆弱性診断士	構築系サイバーセキュリティ担当	ネットワークリスクアセッサー	Knowledge Management
インシデントハンドリング	教育・啓発	運用系サイバーセキュリティ担当	リサーチャー	Customer Service and Technical Support
デジタルフォレンジクス	フォレンジックエンジニア	CSIRT担当	フォレンジックエンジニア	Network Services
情報セキュリティインベスティゲーション	インベスティゲーター	SOC担当	インテリジェンスアナリスト	Systems Administration
情報セキュリティ監査	リーガルアドバイザー	ISMS担当	インシデントレスポンダー	Systems Analysis
	IT企画部門	システム企画担当	セキュアオペレーター	Legal Advice and Advocacy
	ITシステム部門	基幹システム構築担当		Training, Education, and Awareness
	情報セキュリティ監査人	基幹システム運用担当		Cybersecurity Management
		WEBサービス担当		Strategic Planning and Policy
		業務アプリケーション担当		Executive Cyber Leadership
		インフラ担当		Program/Project Management
		サーバ担当		Cyber Defense Analysis
		DB担当		Cyber Defense Infrastructure Support
		ネットワーク担当		Incident Responder
		サポート・教育担当		Vulnerability Assessment and Management
		ヘルプデスク担当		Threat Analysis
		監査責任者		Exploitation Analysis
		監査担当		All-Source Analysis
		特定個人情報取扱責任者		Targets
		特定個人情報取扱担当		Language Analysis
		個人情報取扱責任者		Collection Operations
		個人情報取扱担当		Cyber Operational Planning
				Cyber Operations
				Cyber Investigation
				Digital Forensics

（論点２）改訂中のITSS＋（セキュリティ領域）におけるセキュリティ関連分野の概観

- セキュリティ技術者のみではセキュリティは確保できない。IT/IoT/OT等のシステムの企画・設計・開発・運用・保守を行う人材や、管理部門等の人材にも、セキュリティ関連スキルは必須となってきている。
- こうした観点から、セキュリティ関連分野を以下の通り整理し、各分野に関連する主なタスク等を紐づけ中。

	経営層	戦略マネジメント層				実務者・技術者層				
						設計・開発・テスト		運用・保守		研究開発
ユーザ企業における組織の例	取締役会 執行役員会議	内部監査部門 （外部監査を含む）	管理部門 （総務、法務、広報、調達、人事 等）	セキュリティ統括室	経営企画部門 事業部門	デジタル部門／事業部門 （ベンダーへの外注を含む）				
セキュリティ関連タスクの例	• セキュリティ意識啓発 • 対策方針指示 • ポリシー・予算・実施事項承認	• システム監査 • セキュリティ監査	• BCP対応 • 官公庁等対応 • 法令等遵守対応 • 記者・広報対応 • 調達・契約・検収 • 施設管理・物理セキュリティ • 内部犯行対策	• リスクアセスメント • ポリシー・ガイドライン策定・管理 • 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	• 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	• 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 • テスト計画	• 基本・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 • 脆弱性診断	• 構成管理 • 運用設定 • 脆弱性対応 • セキュリティツールの導入・運用 • 監視・検知・対応 • インシデントレスポンス • ペネトレテスト	• 現場教育・管理 • 設備管理・保全 • 初動対応・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	• セキュリティ理論研究 • セキュリティ技術開発

タスクに対応するセキュリティ関連分野

デジタル（IT／IoT／OT）	デジタル経営（CIO／CDO）	システム監査			デジタルシステムストラテジー	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サポート		
セキュリティ	セキュリティ経営（CISO）	セキュリティ監査		セキュリティ統括			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
その他	企業経営（取締役）		経営リスクマネジメント 法務		事業ドメイン（戦略・企画・調達）			事業ドメイン（生産現場・店舗管理）		

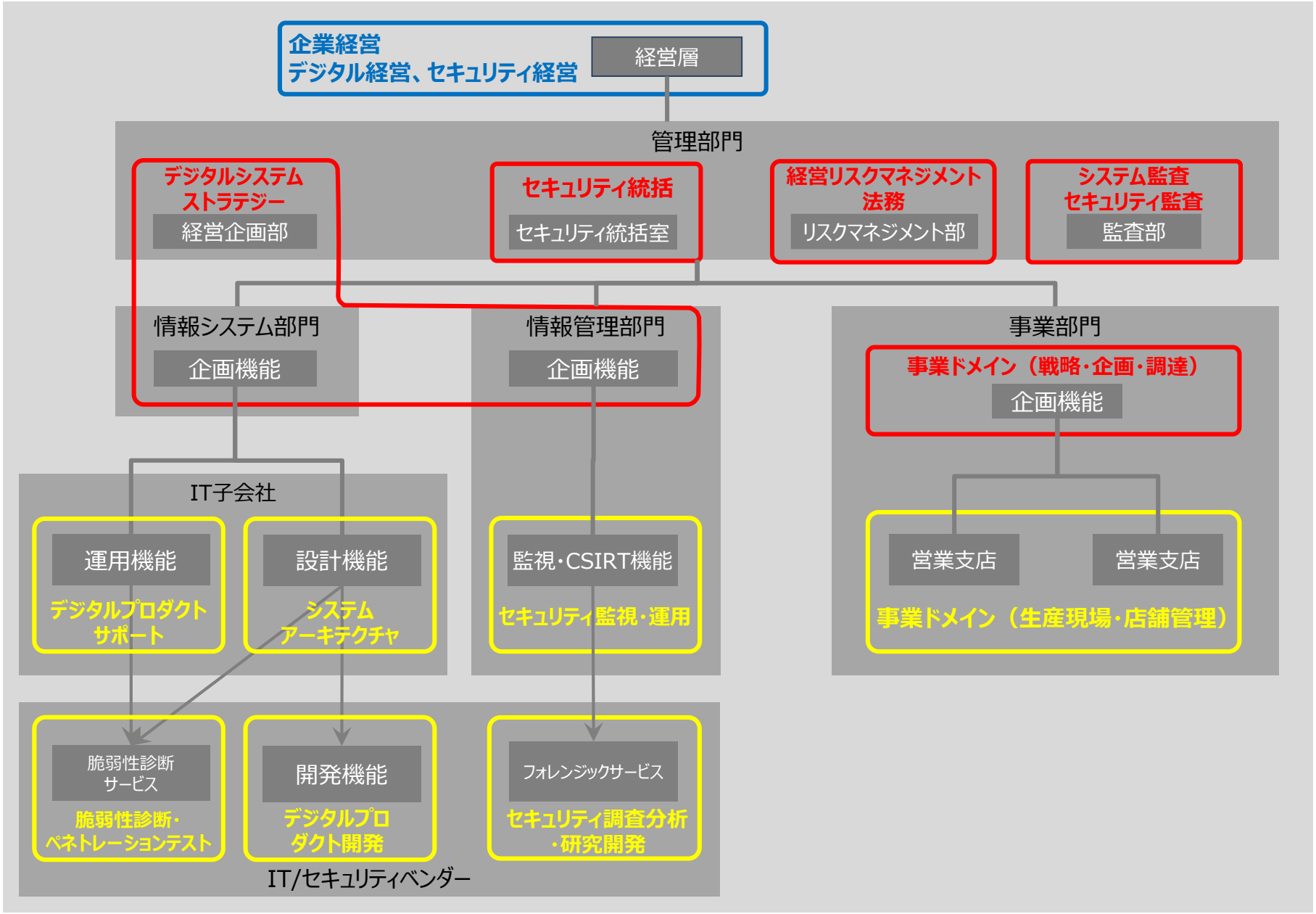
※クラウド、アジャイル、DevSecOps等により境界は曖昧化の傾向
※チップ/IoT・組み込み/制御システム/OS/サーバ/NW/ソフト/Web等の取扱う技術の種類や事業分野によりタスクやスキルは大きく異なる

（論点２）改訂中のITSS＋における各分野に対応するセキュリティ関連タスクの例

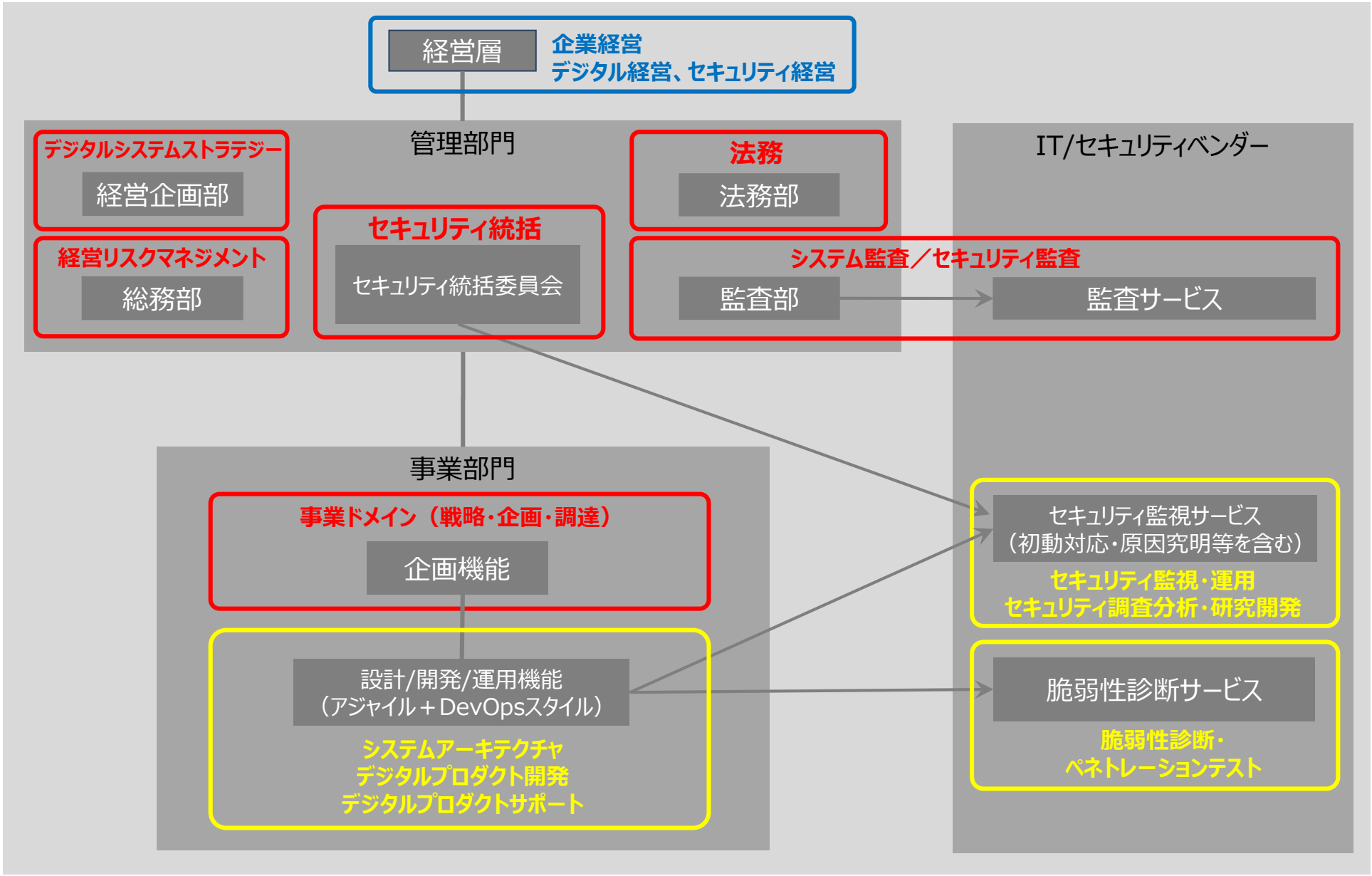
	区分	分野名	セキュリティ関連タスクの例
経営層	デジタル	IT経営（CIO/CDO）	セキュリティ意識啓発、対策方針の指示、セキュリティポリシー・予算・対策実施事項の承認　等
	セキュリティ	セキュリティ経営（CISO）	
	その他	企業経営（取締役）	
戦略マネジメント層	デジタル	システム監査	システム監査、報告・助言　等
		デジタルシステムストラテジー	デジタル事業戦略立案、システム企画、要件定義・仕様書作成、プロジェクトマネジメント　等
	セキュリティ	セキュリティ監査	セキュリティ監査、報告・助言　等
		セキュリティ統括	セキュリティ教育・普及啓発、セキュリティ関連の講義・講演、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
	その他	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、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	デジタル	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サポート※	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
	セキュリティ	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
	その他	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、QC活動、初動対応　等

※「プロダクト」には必ずしも物理的な形をもつ製品に限らず、ソフトウェアやネットワーク経由でのサービス提供等の形態を含む。

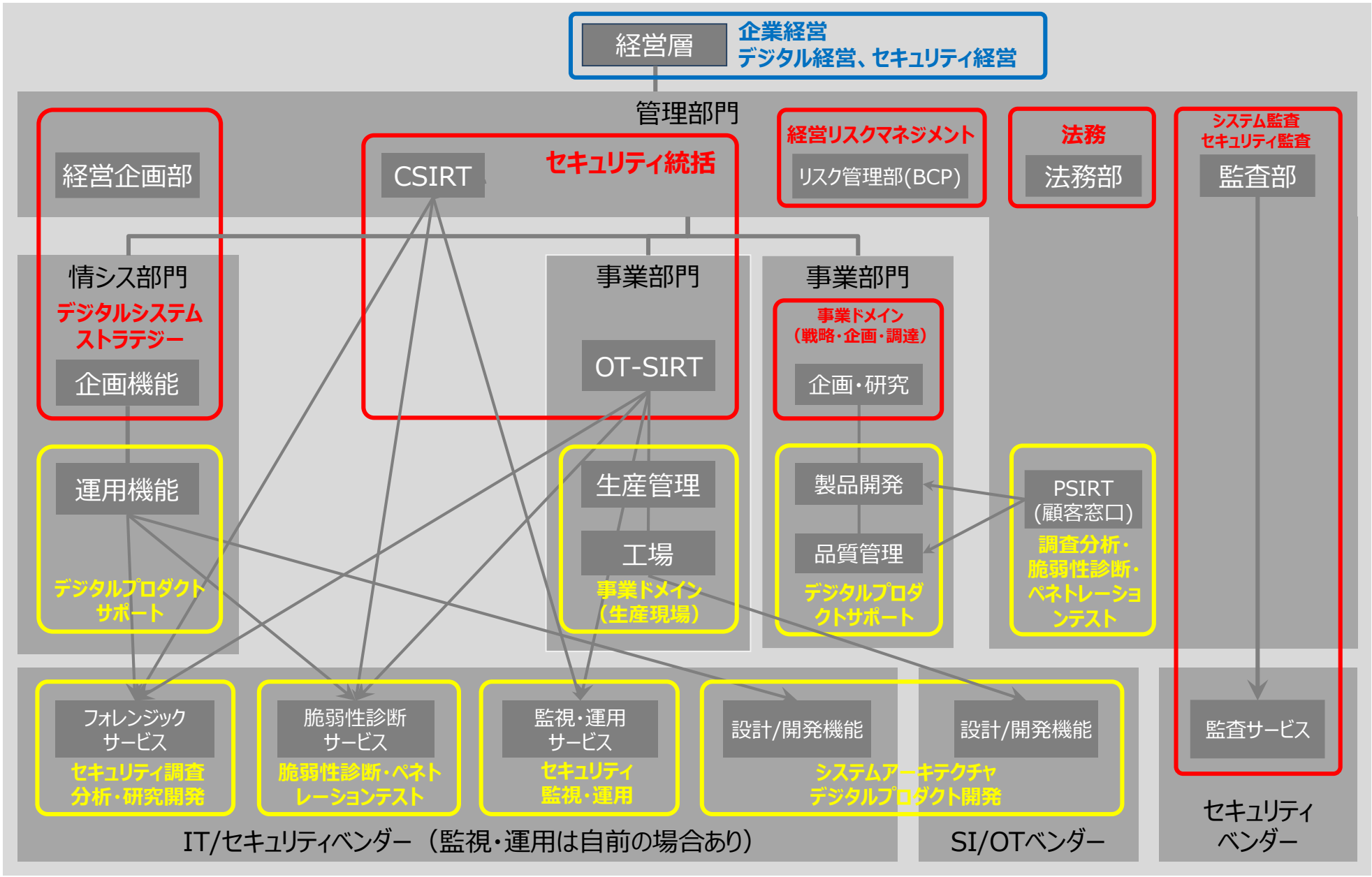
（参考）企業における各分野のマッピングの例① 金融業



（参考）企業における各分野のマッピングの例② ネットサービス業



（参考）企業における各分野のマッピングのイメージ③　製造業



情報処理安全確保支援士試験・情報処理技術者試験の実施

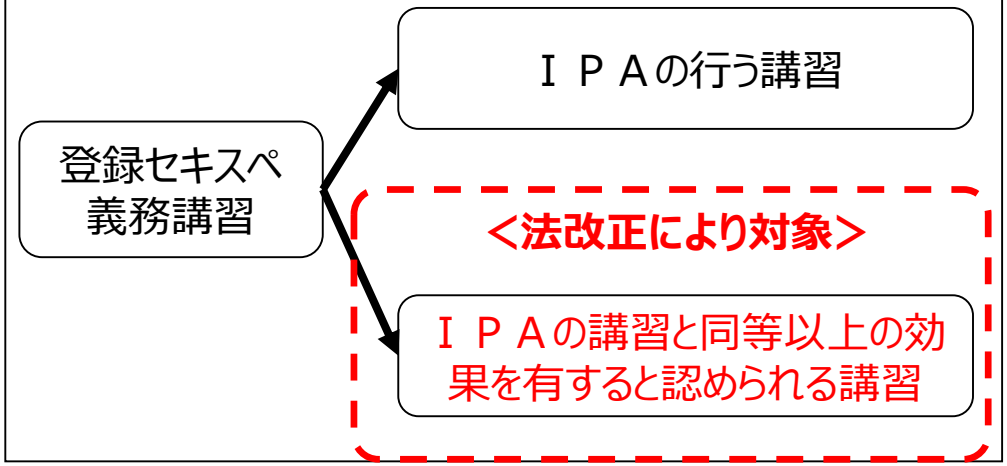
- ＩＴに関する知識・技能を客観的に評価するため、国家試験として「情報処理安全確保支援士試験」及び「情報処理技術者試験」を実施。
- 年間約40万人が受験。うち、情報処理安全確保支援士試験、情報セキュリティマネジメント試験の受験者数は、それぞれ、28,520人、28,116人（令和元年度）
- 高度試験について、2020年実施試験から、情報セキュリティを重点分野に変更するなど、各試験区分においてセキュリティに関する出題を強化。

情報処理安全確保支援士（登録セキスペ）制度の見直し（法改正）

- 「情報処理の促進に関する法律の一部を改正する法律」が第200回臨時国会で成立し、2020年5月15日に施行。
- 改正法により、デジタル技術の急速な発展に伴うサイバーセキュリティ上のリスクに対応するため、登録セキスペの信頼性の向上等を目的とした制度の見直しを実施。
- これにより、**①一定の条件を満たした民間事業者等が行う講習を義務講習の対象に追加、②登録の更新制を導入**。

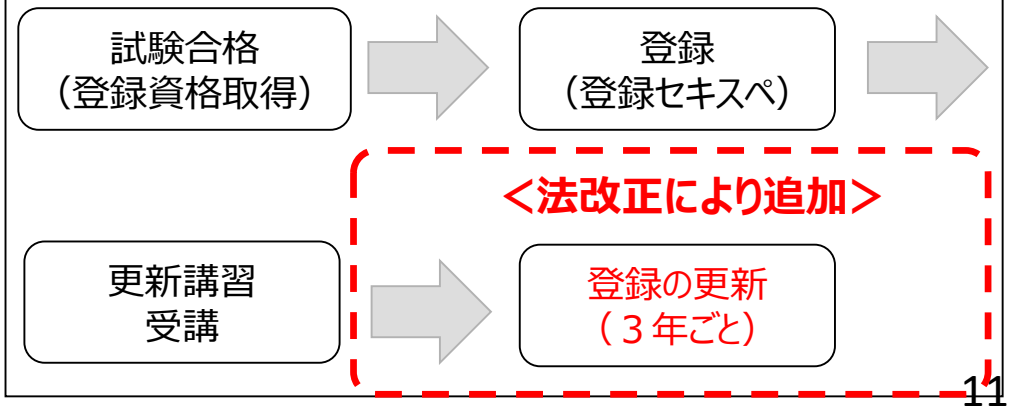
民間事業者等の講習追加

これまで、義務講習として認められる講習は、独立行政法人情報処理推進機構　（ＩＰＡ）が行うものに限られたが、登録セキスペの多様なニーズに応じるため、**一定の条件を満たした民間事業者等が行う講習（特定講習）も対象**に追加。



登録の更新制導入

制度の信頼性を向上させるため、サイバーセキュリティに関する最新の知識・技能を確実に担保できるように、登録に**３年間の有効期限**を設け、義務講習を受講した者のみ更新を認め、**更新が行われない場合**には、**登録が失効**する制度を導入。



国立高専機構と産・官との連携促進・具体化に向けて

- 国立高専におけるセキュリティ教育が産業界の求める人材像とも整合していくためには、産学官の継続的な協力関係が必要。
- このため、国立高専機構がIPAや業界団体（CRIC CSF、JNSA）との協力内容を具体化していくための議論を継続的に実施。

＜高専・産・官の対話の場（イメージ）＞

継続的な協力体制

学

高専機構　等
- ■高度セキュリティ人材、情報系人材、非情報系人材
- ■教員　　等

産

企業・業界団体
- ■CRIC CSF、JUAS、JNSA
- ■ユーザー企業、IT・セキュリティベンダー　等

ニーズ・シーズの整理・具体化 ▶ 協力の検討 ▶ 産業界に求められるセキュリティ人材の育成・輩出

- ・トップガンの育成支援
- ・キャリア教育
- ・機械・建築・生物等の分野別教材の開発・素材提供
- ・セキュリティ教員向けのFD（Faculty Development）
- ・講師派遣
- ・産業界に求められるセキュリティ人材像の共有
- ・適切なプレイヤーとのマッチング

官

関係省庁・独法等
- ■NISC、文科省
- ■IPA、JPCERT/CC　　等

国立高専機構と産・官との連携促進・具体化

- METI、IPA、JPCERT及び業界団体が国立高専機構と連携し、高専生の専攻（セキュリティ、IT、その他（機械、電気等））に応じた教育コンテンツの提供や講師の派遣等、産学官連携の具体化を推進中。

使用できるインフラ
- 演習設備
- 同時中継
  （全国高専間で配信可）
- 仮想空間

国立高専卒業生 約1万人/年の内訳	コンテンツ開発・授業の提供（パワーポイント、ビデオ等）	セキュリティ合宿に関する協力
	パターン①：90分程度 ・高専教員がコンテンツを使って講義 又は 企業等の方が講義（拠点校から全国各校に同時配信も可） **パターン②：15分程度** 授業冒頭や隙間時間でビデオ放映	**高度セキュリティ合宿**（1泊2日） 年2回程度開催（インシデント対応演習等）参加者：35名程度 **KOSENセキュリティコンテスト**（1泊2日） 年1回程度開催（CTF）参加者：130名程度 ※開催期間中の一部の時間を利用して、一線で活躍するホワイトハッカーから講義を実施可能。
約1% トップガンの学生 → 主に**セキュリティ企業**に就職	※トップガンの学生は、全国各校、各学科に散らばっているため、通常の授業時間で集合する機会がない。  ゲーム形式教材のイメージ	• **JNSAが講師の派遣を検討中。** • **METIがセキュリティ専門官を高度セキュリティ合宿に講師として派遣。**  開催の様子@石川高専
約20% 情報系学科の学生 → 主に**IT企業**に就職	• **JNSAのゲーム形式教材を石川高専と連携してアプリ化。** ※JNSA：NPO日本ネットワークセキュリティ協会 • **四国地域企業のIPA ICSCoE終了生が講義を検討中。** • **日立製作所が一関高専生向けに出前授業、インターンシップを実施し、出前授業は全国各校に配信。**	• **JNSAとSECCONビギナーズを石川高専と苫小牧高専で開催。** • **JNSAがCTFビギナーズfor高専生@木更津高専に講師を派遣。** • **IPAが高度セキュリティ合宿に講師を派遣し、App Goat（脆弱性体験学習ツール）の講習会を開催。** • **METIがセキュリティ専門官を高知高専に派遣し、出前授業を実施。**
約80% 非情報系学科の学生 → 主に**ユーザー企業**に就職	• **CRICが佐世保高専と連携し、業界別（例．機械、電気、建築等）ビデオ教材（20分程度）を作成中。** ※CRIC：一般社団法人サイバーリスク情報センター	※セキュリティ合宿のような機会は特段なし。  AppGoat講習の様子
KOSEN 国立高等専門学校機構 国立高専教員	※授業実施側のため。	• **IPAが教員向けにAppGoat講習会を開催。** • **JPCERT/CCが情報担当教員向け研修に講師を派遣。** • **教員がIPAのセキュリティキャンプ全国大会を見学。** • **教師向け合宿で、METIがセキュリティ専門官の派遣を検討中。**

セキュリティスキルレベル

サイバーセキュリティ経営を進める戦略マネジメント層の育成

- 経営層が示す戦略の下、事業継続と価値創出に係るリスクマネジメントを中心となって支える立場である「戦略マネジメント層」の育成が急務。
- IPA産業サイバーセキュリティセンターでは、2018年度に引き続き、2019年度も戦略マネジメント層向けのセミナーを実施。
- 東京工業大学CUMOTは「サイバーセキュリティ経営戦略コース」を新規開催。（IPAが後援）

産業サイバーセキュリティセンター「戦略マネジメント系セミナー」

- 2019年度は2020年２月に実施。
- サイバーセキュリティは経営課題であること及び経営層をはじめ関係者が認知すべきセキュリティ機能の重要性の理解を目指す。
- 体系だった知識の習得のため、「組織管理」と「実務管理」の座学２コースを実施（各２回、合計４回、１回あたり４時間）。延べ68名が参加。

東京工業大学ＣＵＭＯＴ「サイバーセキュリティ経営戦略コース」

- 2020年１月～４月実施
- 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を目的とする。
- 座学だけでなく、受講生同士による議論やワークショップによって理解を深める実践的なスタイルの講義を１回２時間、全14回を予定。