JP-RISSA
情報処理安全確保支援士会

InternetWeek 2020

サイバーセキュリティ人材の多様な活躍と、実践事例

2020年11月24日

一般社団法人情報処理安全確保支援士会

JP-RISSA
情報処理安全確保支援士会

1.当会のご紹介

一般社団法人情報処理安全確保支援士会

JP-RISSA
情報処理安全確保支援士会

●設立目的

「情報処理安全確保支援士」の活躍の場をひろげ、情報化社会におけるサイバーセキュリティを含む情報セキュリティを取り巻く環境が向上することを目的とした団体。2019年8月に設立された任意団体を母体として、2020年4月に一般社団法人に改組。

運営メンバーは、すべて無報酬のボランティアでの活動です。

●主な運営体制

- 代表理事・会長　　山口　敏行
- 副会長　　清土　桂一郎
- 副会長・事務局長　　大島　真言　（理事：17名、監事：2名）

●会員

333名（2020年11月時点）

●WEB

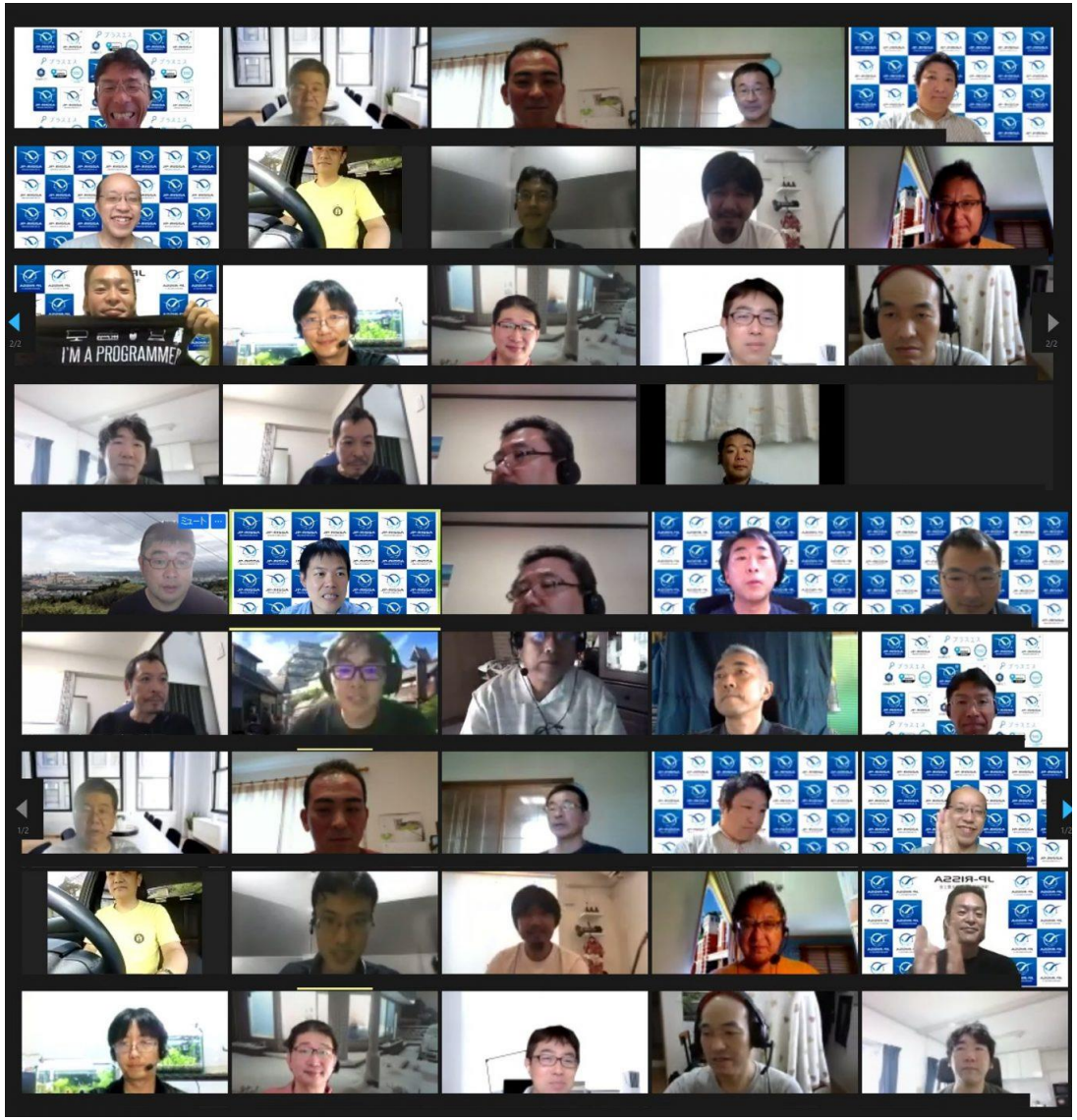
https://www.jp-rissa.or.jp/
https://twitter.com/jp_rissa

TLP：WHITE

活動紹介

JP-RISSA
情報処理安全確保支援士会

- 交流会
  - 会員間地域交流イベント
  - テーマ別交流イベント
- 勉強会
  - CTF のWriteup LT大会
  - 経済産業省様、IPA様との意見交換会
    （RISS制度、セキュリティプレゼンター制度、
    中小企業の情報セキュリティマネジメント　など)
  - 法律家観点での解説
  - 機械学習・AI分科会
  - オンライン「もくもく」会
- RISS養成
  - 情報処理安全確保支援士試験対策
    セミナー



TLP：WHITE

2.本日のアジェンダ

お伝えしたいこと

- セキュリティ対応を行う体制は、部署や組織の名前をつけることだけではなく、**必要な機能・役割を定義すること**が求められる

- DXを推進する組織のセキュリティ対応を行う体制は、セキュティ対策を主たる目的とする「セキュリティ人材」だけではなく、**「プラス・セキュリティ人材」が不可欠**である

- 例えば、自社の契約書雛形に盛り込むセキュリティ対策について検討する法務部担当者や、システム監査、報告・助言等を行う監査担当者が、セキュリティの知識を持つことが求められる

参考とした資料

JP-RISSA
情報処理安全確保支援士会

『サイバーセキュリティ体制構築・人材確保の手引き』
https://www.meti.go.jp/press/2020/09/20200930004/20200930004.html

経済産業省

申請・お問合せ | English | サイトマップ | 本文へ | 文字サイズ変更 | アクセシビリティ閲覧支援ツール

ニュースリリース | 会見・談話 | 審議会・研究会 | 統計 | 政策について | 経済産業省について

ホーム ▸ ニュースリリース ▸ ニュースリリースアーカイブ ▸ 2020年度9月一覧 ▸ 『サイバーセキュリティ体制構築・人材確保の手引き』を取りまとめました

English | 印刷

『サイバーセキュリティ体制構築・人材確保の手引き』を取りまとめました

サイバーセキュリティ経営ガイドラインVer2.0の付録として

2020年9月30日

▸ ものづくり/情報/流通・サービス

経済産業省は、企業がサイバーセキュリティ経営ガイドラインに基づいてサイバーセキュリティの体制を構築し、人材を確保するための『サイバーセキュリティ体制構築・人材確保の手引き』（第1版）（以下、「手引き」と言います）を本日公開しました。

1. 背景・趣旨

サイバー攻撃が高度化・巧妙化し、我が国の産業界を脅かす中、サイバーセキュリティに関する体制構築とそのための人材の確保・育成が各企業の急務となっています。そこで、経済産業省では、企業内の経営層から人事担当者、実務者に至る様々な立場の人が、体制構築・人材確保においてどのようなことを考慮すれば良いのかの要点を効率良く把握できる共通言語として本手引きを公開します。

2. 手引きの内容

本手引きは、サイバーセキュリティ経営ガイドラインの10の指示のうち、指示2（サイバーセキュリティリスク管理体制の構築）及び指示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作成しています。

主な対象企業は従業員数300名以上のユーザ企業（大企業・中堅企業）です。ただし、グループ企業等、それ以外の条件の企業・組織においても、条件の違いを考慮した上で御活用いただけます。

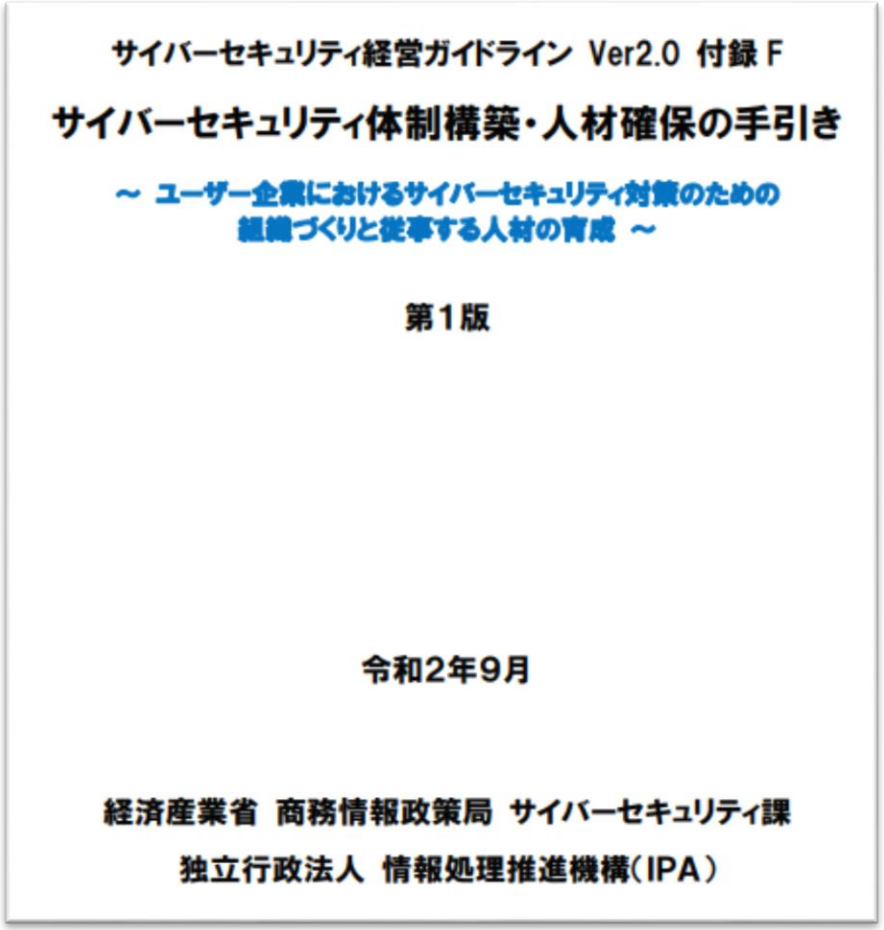
また、重要事項を箇条書きで示した「ポイント」、本文の説明を補足する目的で、有用と思われる内容を囲み記事の形で紹介する「コラム」等、読者の立場に応じて効率良く御覧いただくための工夫を行っています。

3. ダウンロード

こちらのページから最新版の付録Fをダウンロードしてください。

関連資料

『サイバーセキュリティ体制構築・人材確保の手引き』（第1版）（PDF形式：5,868KB）



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

～ ユーザー企業におけるサイバーセキュリティ対策のための組織づくりと従事する人材の育成 ～

第1版

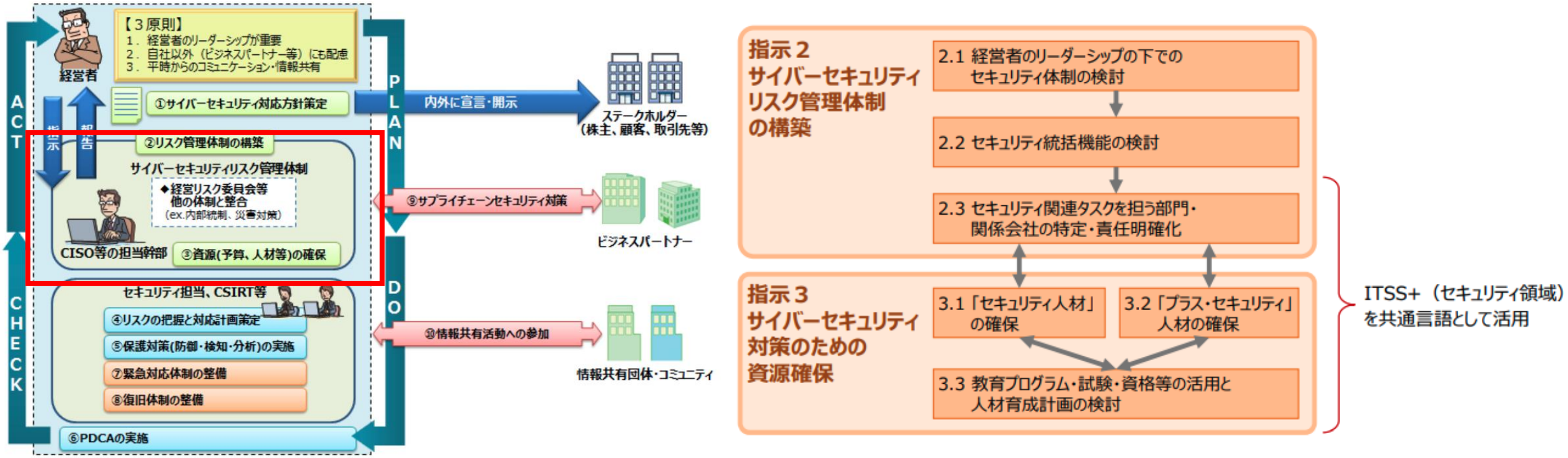
令和2年9月

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）

TLP：WHITE

経営者の役割



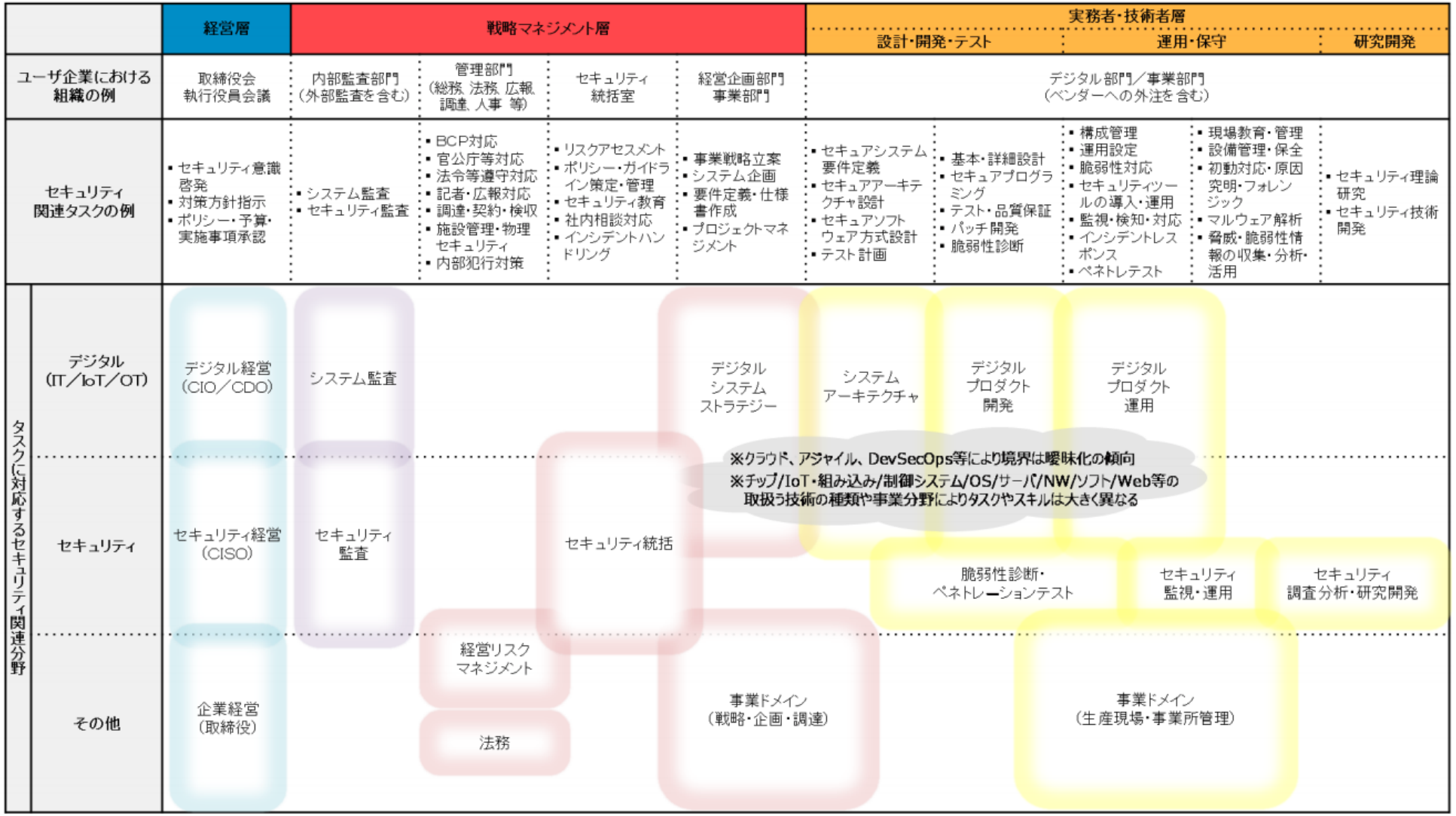
経営者には、**<u>リスク管理体制を構築</u>**し、

<u>資源（予算、人材）を確保すること</u>が求められる。

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

ITSS+（セキュリティ分野）で定義されている17分野



『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

17分野とセキュリティ関連タスク等との対応

JP-RISSA 情報処理安全確保支援士会

	区分	分野名	セキュリティ関連タスクの例	担当部署／機能の例（青字は社外ベンダー等）
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	経営者、経営層（CISOを含む）
	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	監査部門 ITベンダー・監査法人（システム監査サービス）
		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
	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	監査部門 セキュリティベンダー・監査法人（セキュリティ監査サービス）
		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	セキュリティ専門部門、CSIRT セキュリティ委員会 IT・デジタル部門のセキュリティ対策機能
	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、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
		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	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	IT・デジタル部門の設計機能、IT子会社 IT/OTベンダー
		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ベンダー
		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/セキュリティベンダー
	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	IT・デジタル部門の運用機能、IT子会社 セキュリティベンダー（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 セキュリティベンダー（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 セキュリティベンダー（デジタルフォレンジックサービス）
	その他	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/セキュリティベンダー

大喜

大喜

清土

足立

清土

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

3-1.
セキュリティ統括、セキュリティ監視・運用の立場から

自己紹介

JP-RISSA
情報処理安全確保支援士会

- 清土（せど）桂一郎
  民間企業の情シス部門に所属する社内SE（18年目）
  従業員規模は約5,000名
- ネットワーク、サーバ基盤の構築運用担当
  ＋セキュリティ！
  社内システム構築、アプリ作成からスタート
  社外持ち出しPCの担当時に、セキュリティ対策に触れ始める
  セキュリティスペシャリスト→情報処理安全確保支援士（RISS）に
- RISSのコミュニティ「JP-RISSA」を創設（2019年8月）
  社外の情報収集のため放課後に活動していたら、できちゃいました。

第001975号

TLP：WHITE

自組織内での役割（セキュリティ）

JP-RISSA
情報処理安全確保支援士会

- 組織内CSIRTのメンバー
- 社内システムやPCなどでのインシデント対応（主に二次対応）
- 「システムセキュリティー統括者実務者会議」の統括者

RISSが、現在4名参加

- この会議は、どういったもの？

「セキュリティ点検」 …システム構築時、WEBサイト公開時
「ガイドライン、ルール策定」… 技術者向け→全社員向けのベースに
「よろずお困りごと相談窓口」… ZOOM使いたい

TLP：WHITE

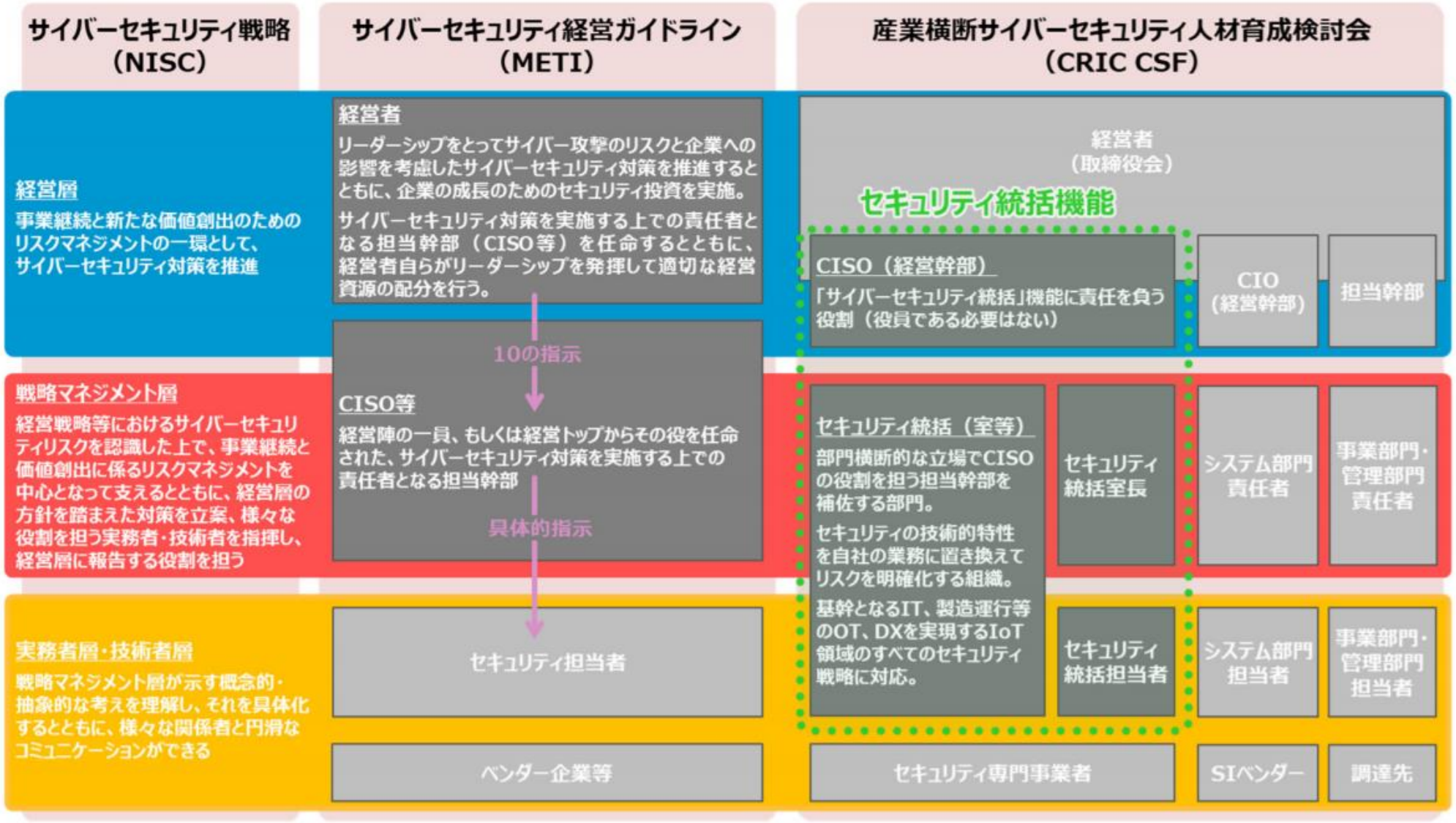


図 5　セキュリティ統括機能の位置付け（1）

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

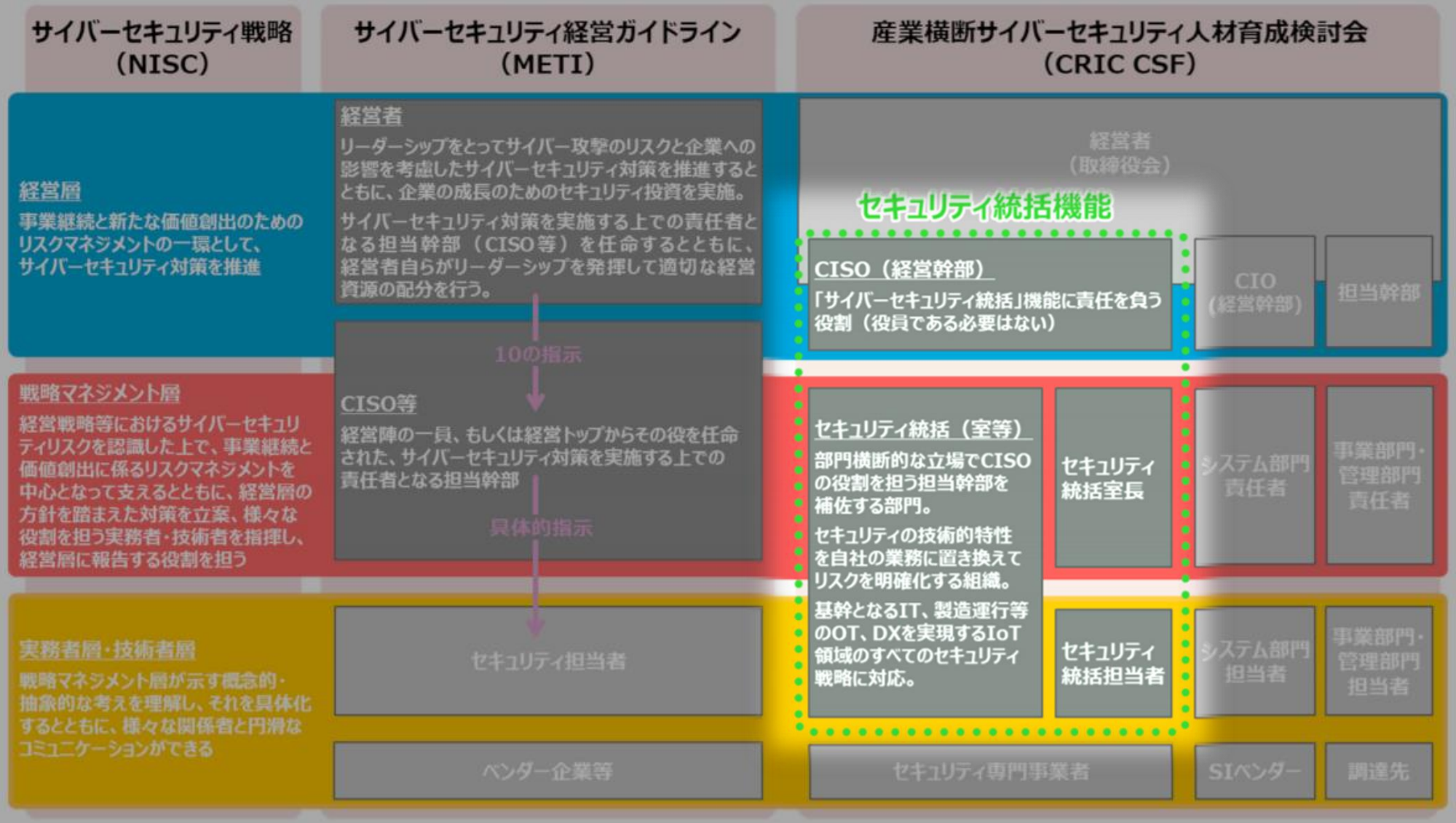


図 5　セキュリティ統括機能の位置付け（1）

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

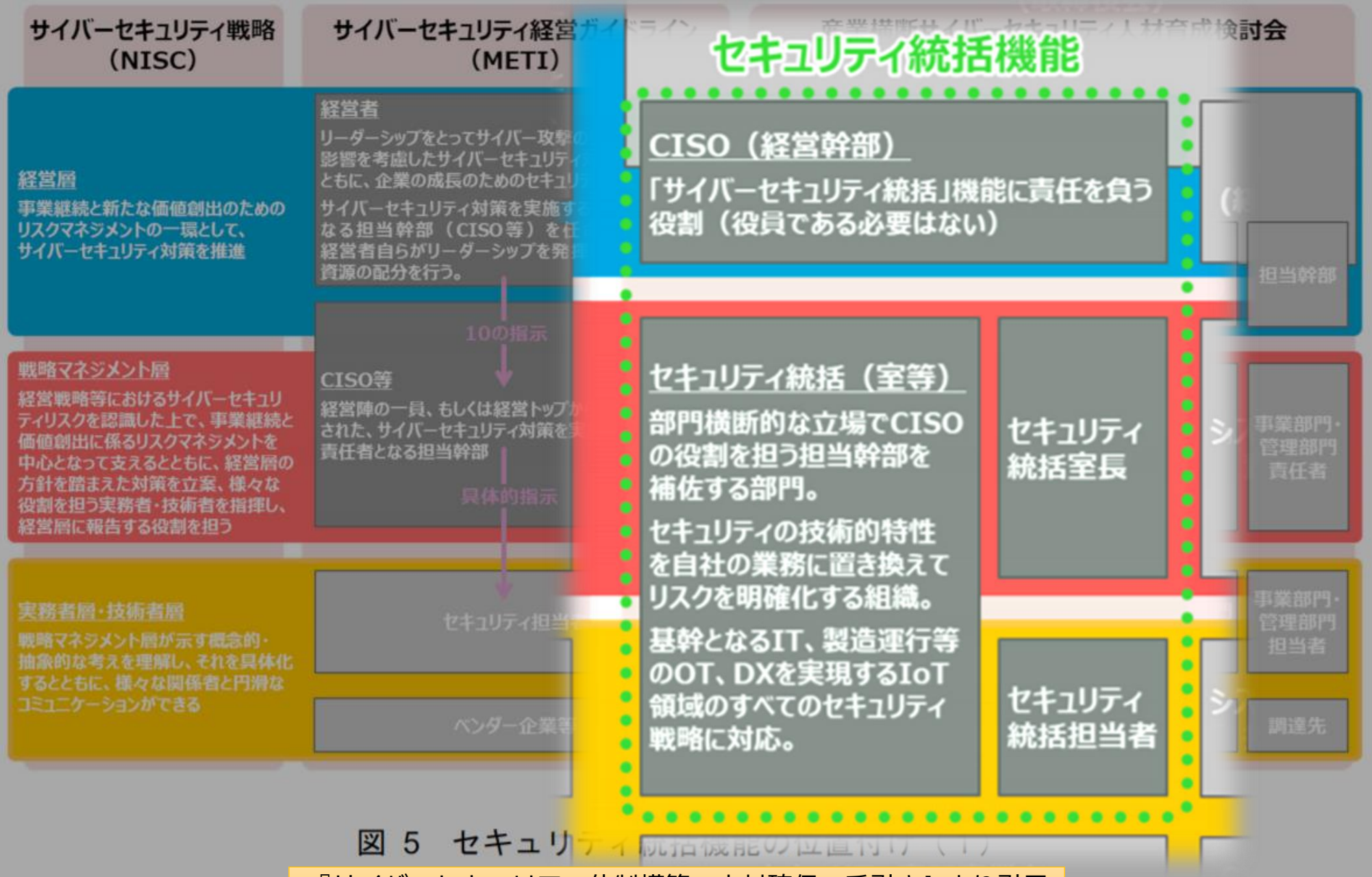


図 5　セキュリティ統括機能の位置付け（イメージ）

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

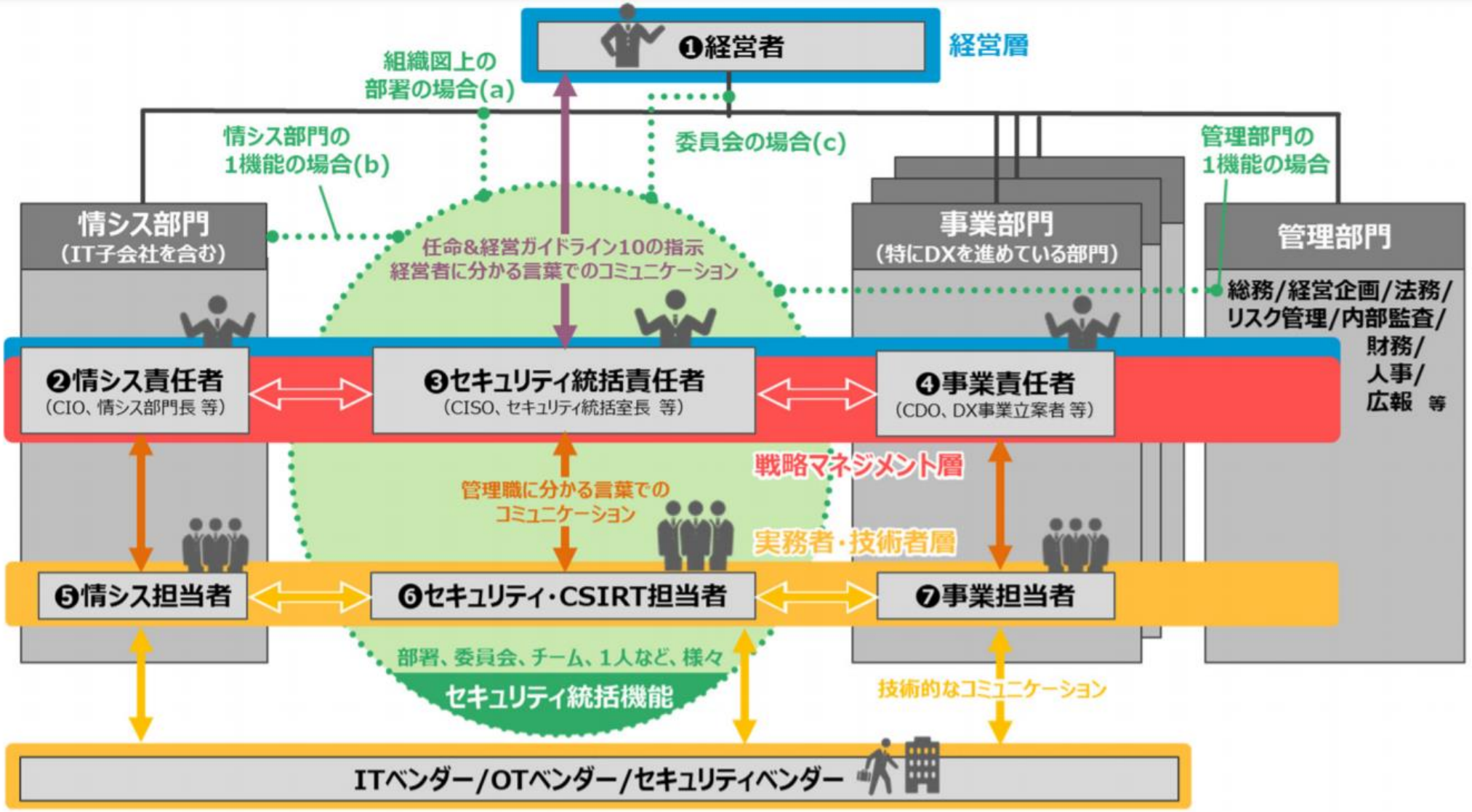


図 6　セキュリティ統括機能の位置付け（2）

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

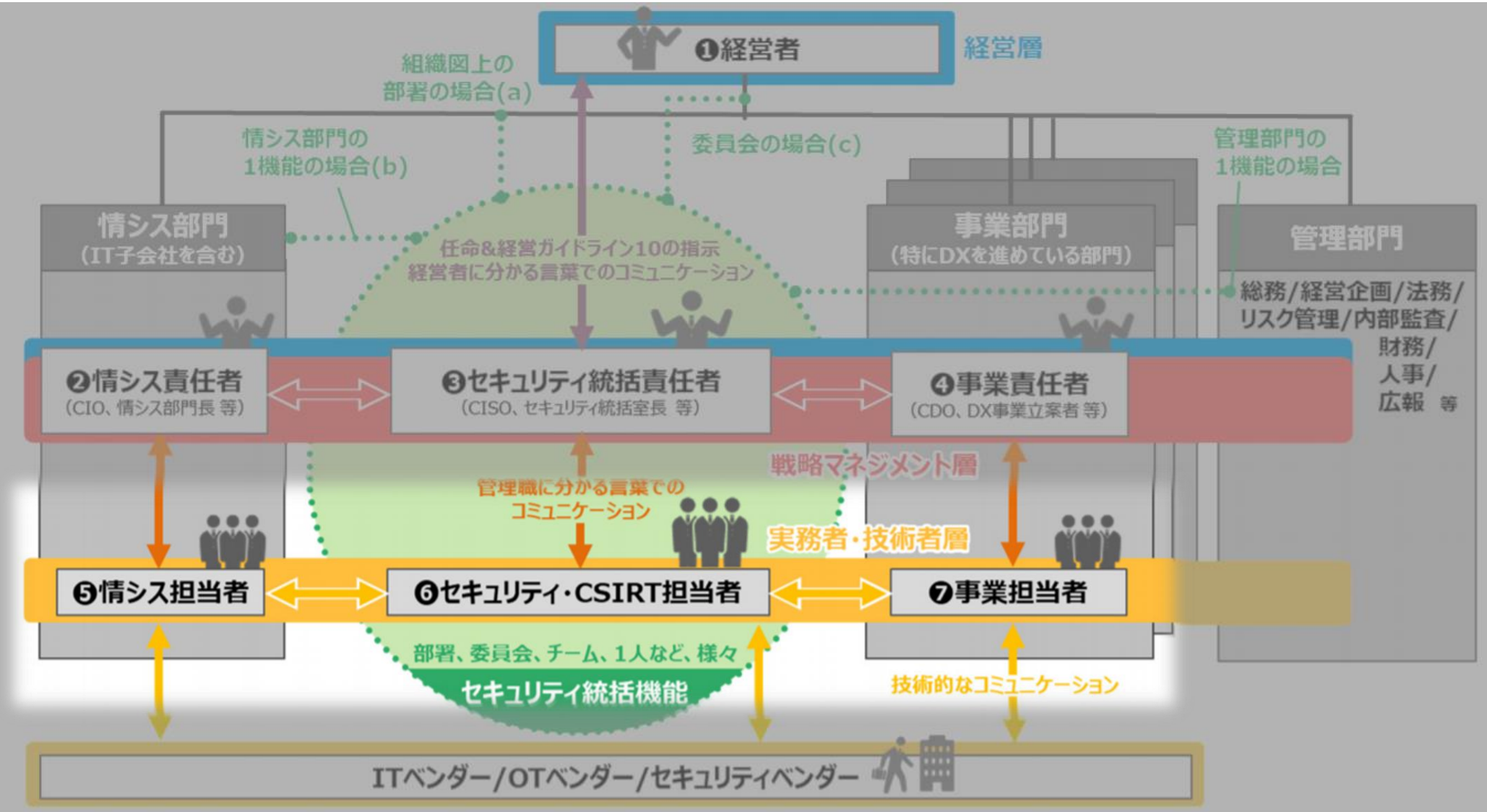


図 6　セキュリティ統括機能の位置付け（2）

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

セキュリティ点検

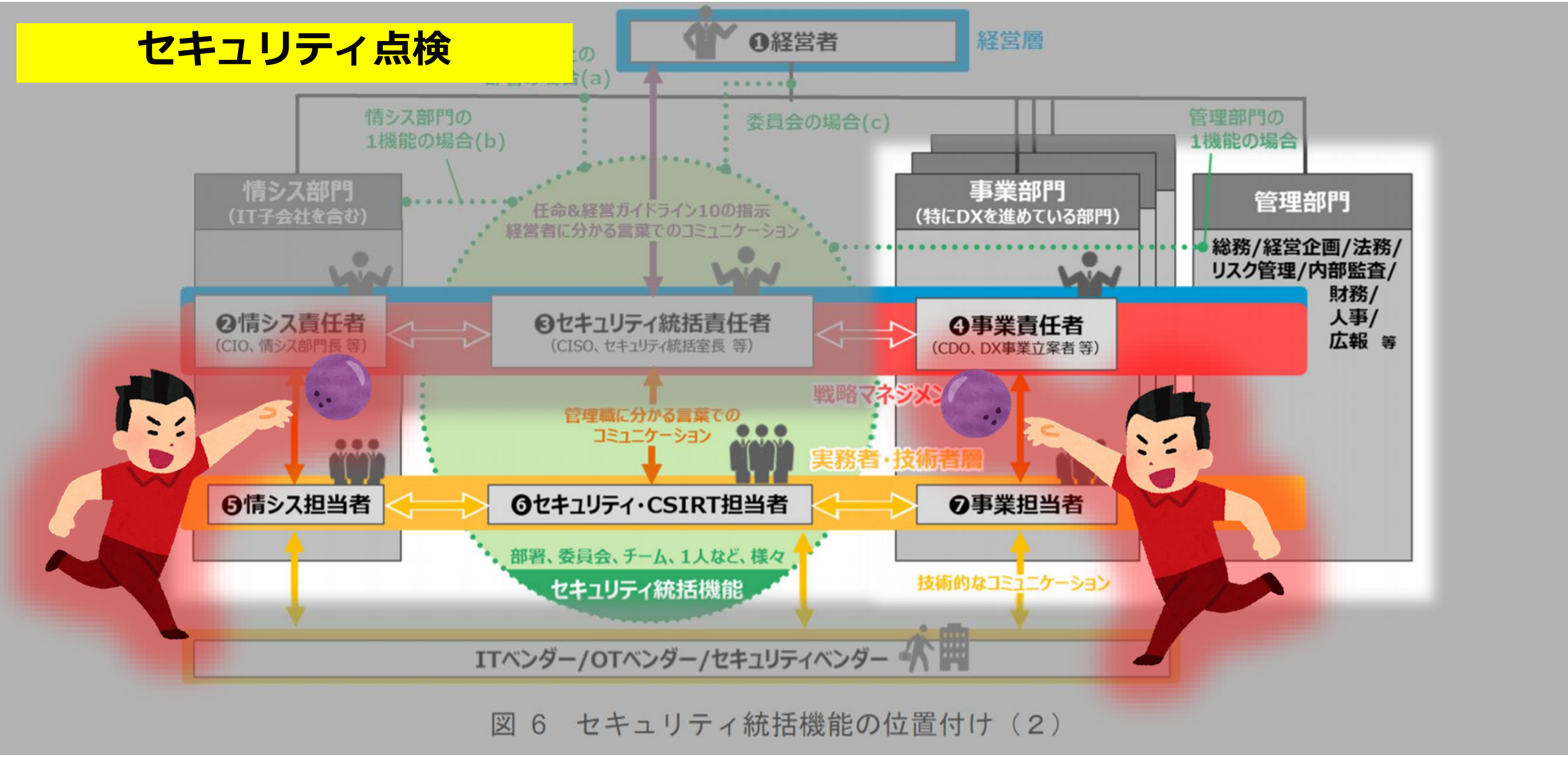


図 6　セキュリティ統括機能の位置付け（2）

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

セキュリティ点検

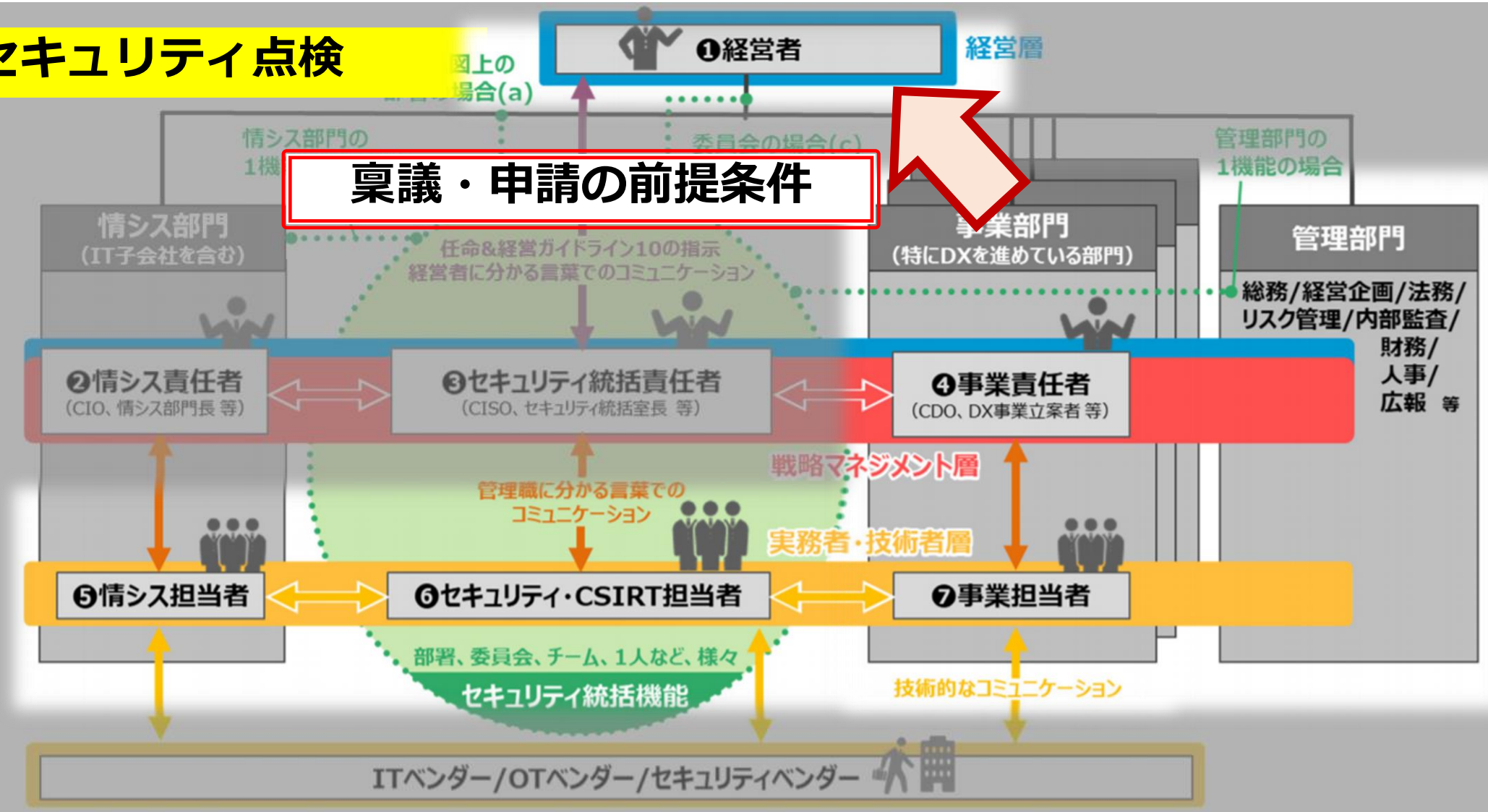


図 6　セキュリティ統括機能の位置付け（2）

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

RISSであることの価値

（対外的な価値）

- インシデント対応や、ルール策定に頼られる存在
- （ある程度）自信をもって、お墨付きを与えられる
- 「あ、RISSなんだ。だから詳しいんだね。」と思われる。。。
  ようには、まだまだなっていない（知名度をUP）

（自分自身）

- 勉強することのきっかけとなる
  コミュニティ参加、資格維持
  スライド作成のための各種ドキュメントの読み込み

RISSであることの価値

JP-RISSA
情報処理安全確保支援士会

JP-RISSA会員から

- 異業種交流会、勉強会に講師としてお声がけ頂くようになった
(セキュリティプレゼンターとしても登録)
- 自社のセキュリティ対策としてのアピールになる
- マネジメント指導業務にて中小企業支援できた
- 信頼できる基盤（コミュニティ）での情報交換のメリット
- 企画などからセキュリティの専門家として参画
- 社内における製品、ルール作り、教育担当等に
- 企業CSR、地域活動として貢献(PTAなど)

TLP：WHITE

RISSやセキュリティ人材への期待

JP-RISSA
情報処理安全確保支援士会

（課題から見えるもの）

- 「セキュリティ点検」を担う人材の圧倒的な不足
  単に「RISS」だからとクリアできる問題ではない。
  知識をインプットし続け、実践を積む必要がある
  →セキュリティ専門人材？
- 『プラス・セキュリティ』人材の必要性
  そもそも点検しなくても良いレベルへの底上げを。
  IT部門だけでなく、事業部門も。

第001975号

（経営判断の材料を）

- とにかく分かりやすく、リスクと脅威を説明できる人材が必要
  →セキュリティに限った話ではない

TLP：WHITE

セキュリティ点検

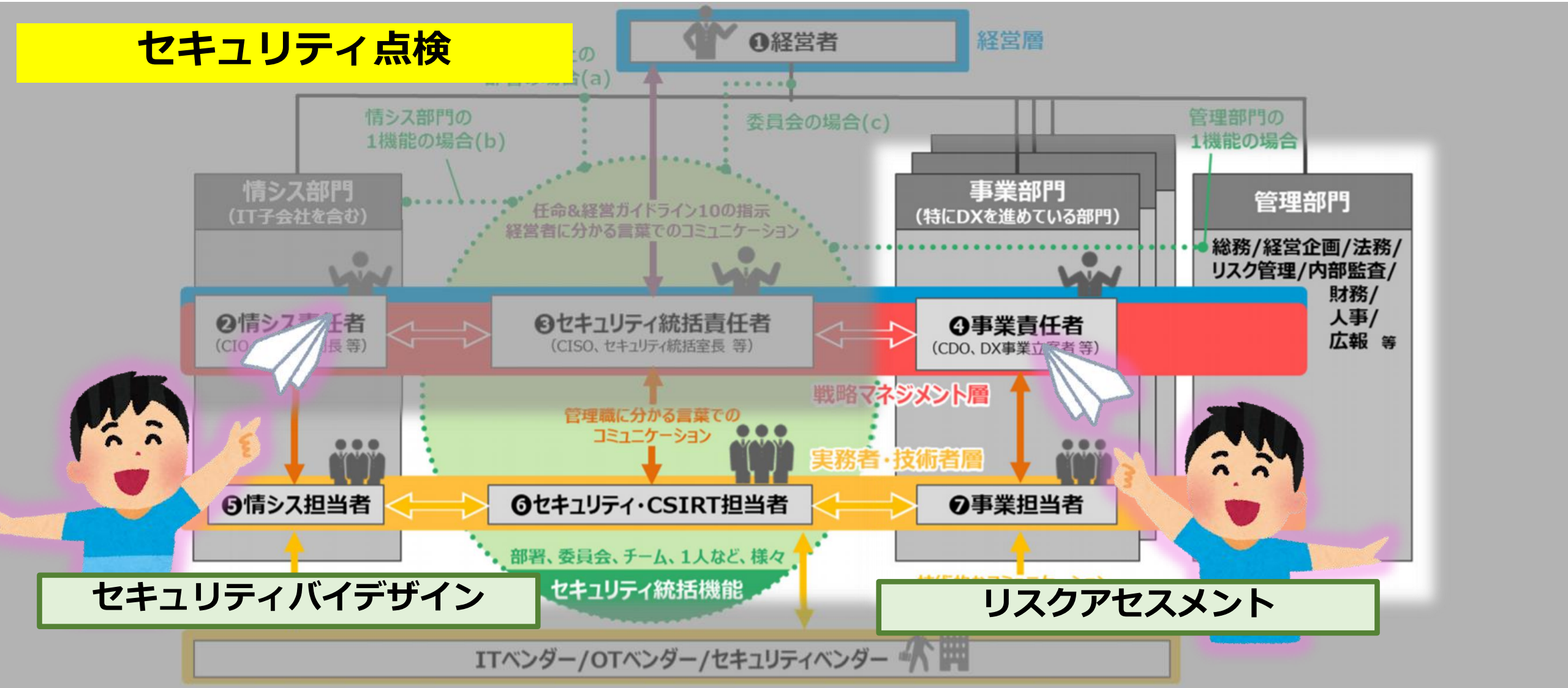


図 6　セキュリティ統括機能の位置付け（2）

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

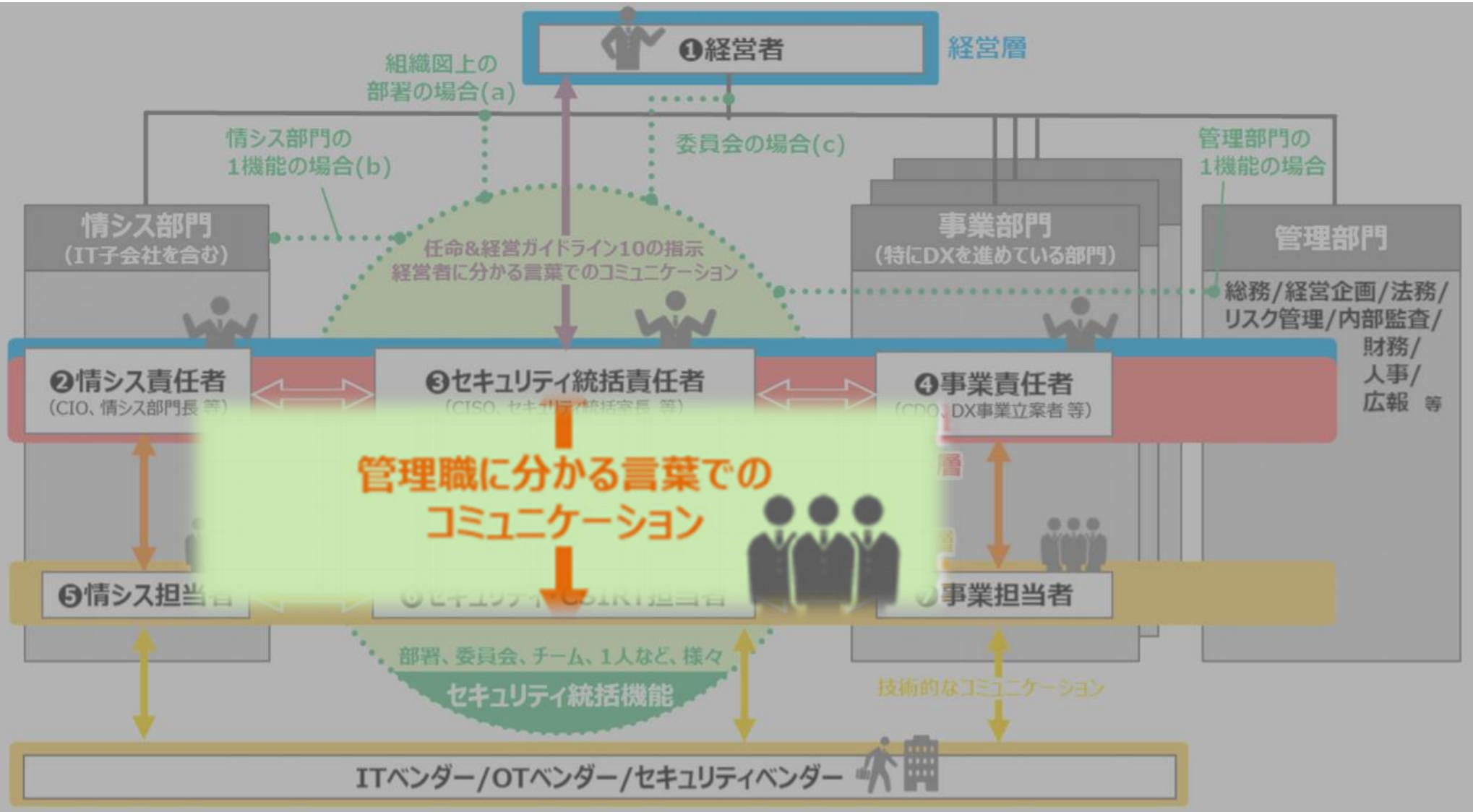
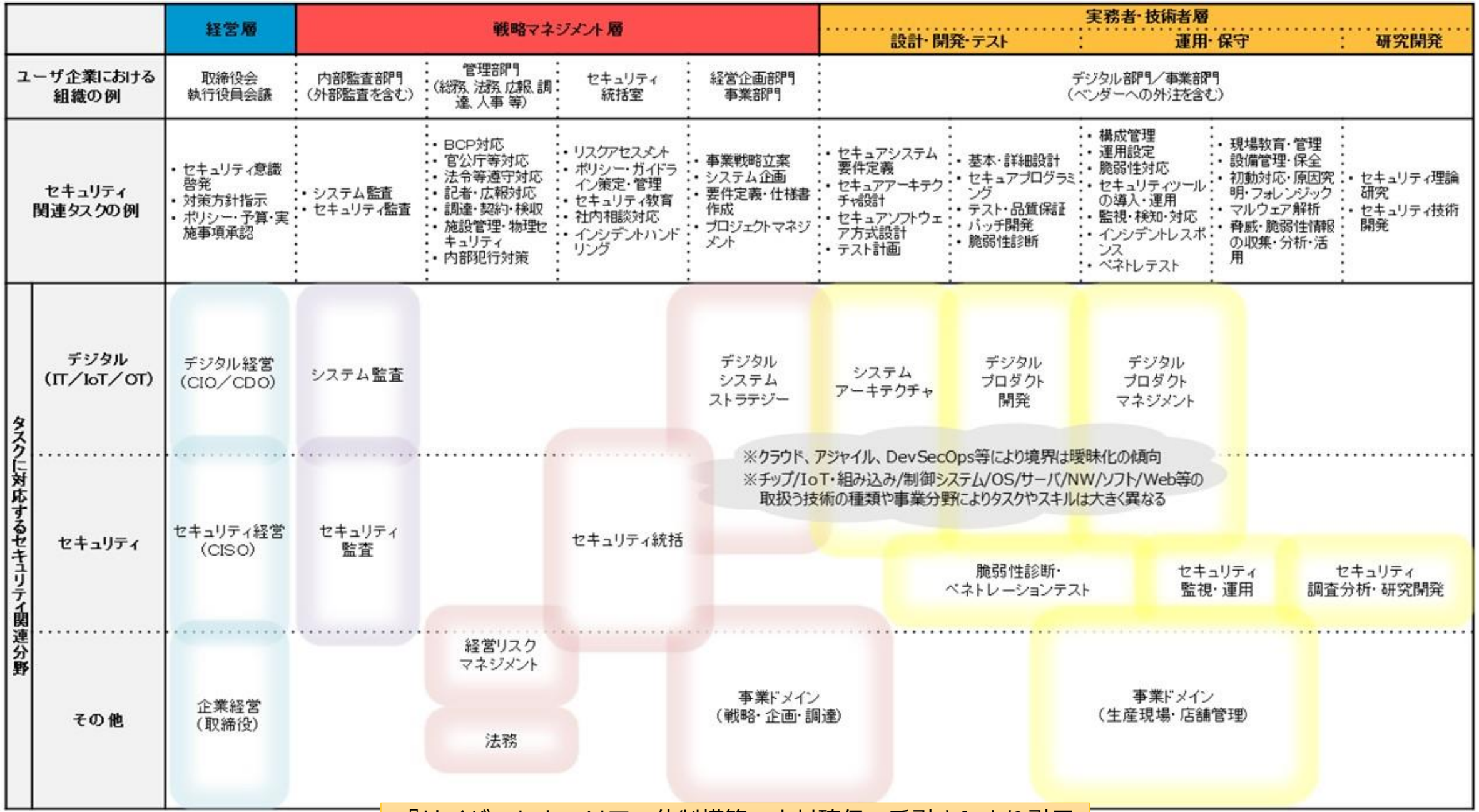


図 6　セキュリティ統括機能の位置付け（2）

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE



『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

	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	・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	・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 マネジメント		
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		
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

経営層への説明も

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

3-2.
システム監査、セキュリティ監査の立場から

自己紹介

JP-RISSA
情報処理安全確保支援士会

- 大喜 康生（だいき やすお）
- 某監査法人でシステム監査部門に所属
- 経歴

  某Sierでシステムエンジニア → 監査法人（現職とは別） →
  事業会社のセキュリティ部門 → 監査法人（いまココ）
- 資格

  セキュリティスペシャリスト → 情報処理安全確保支援士

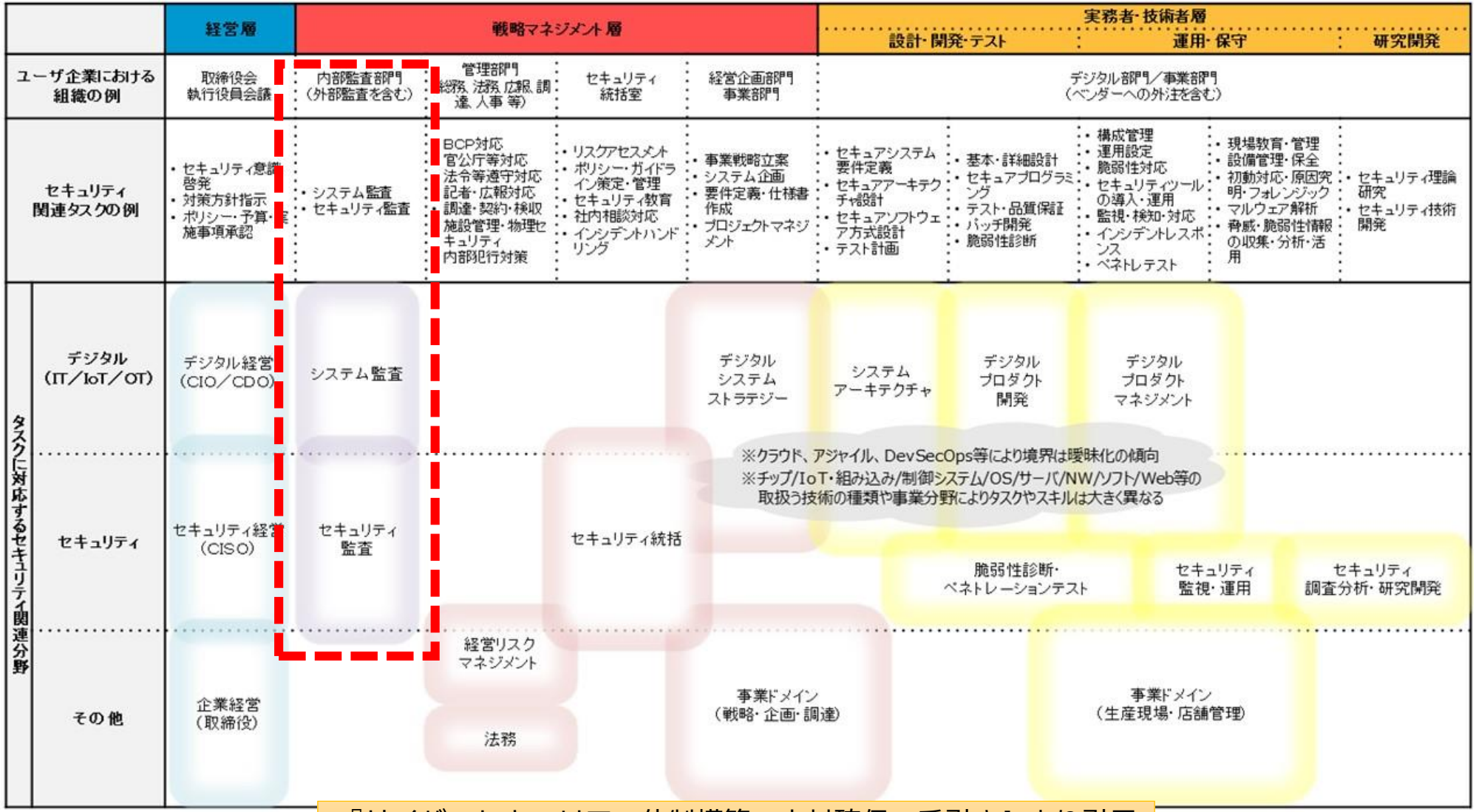
  公認情報システム監査人（CISA）

  公認情報セキュリティマネージャ（CISM）

  中小企業診断士　など　**公認会計士は持っていないです**

TLP：WHITE

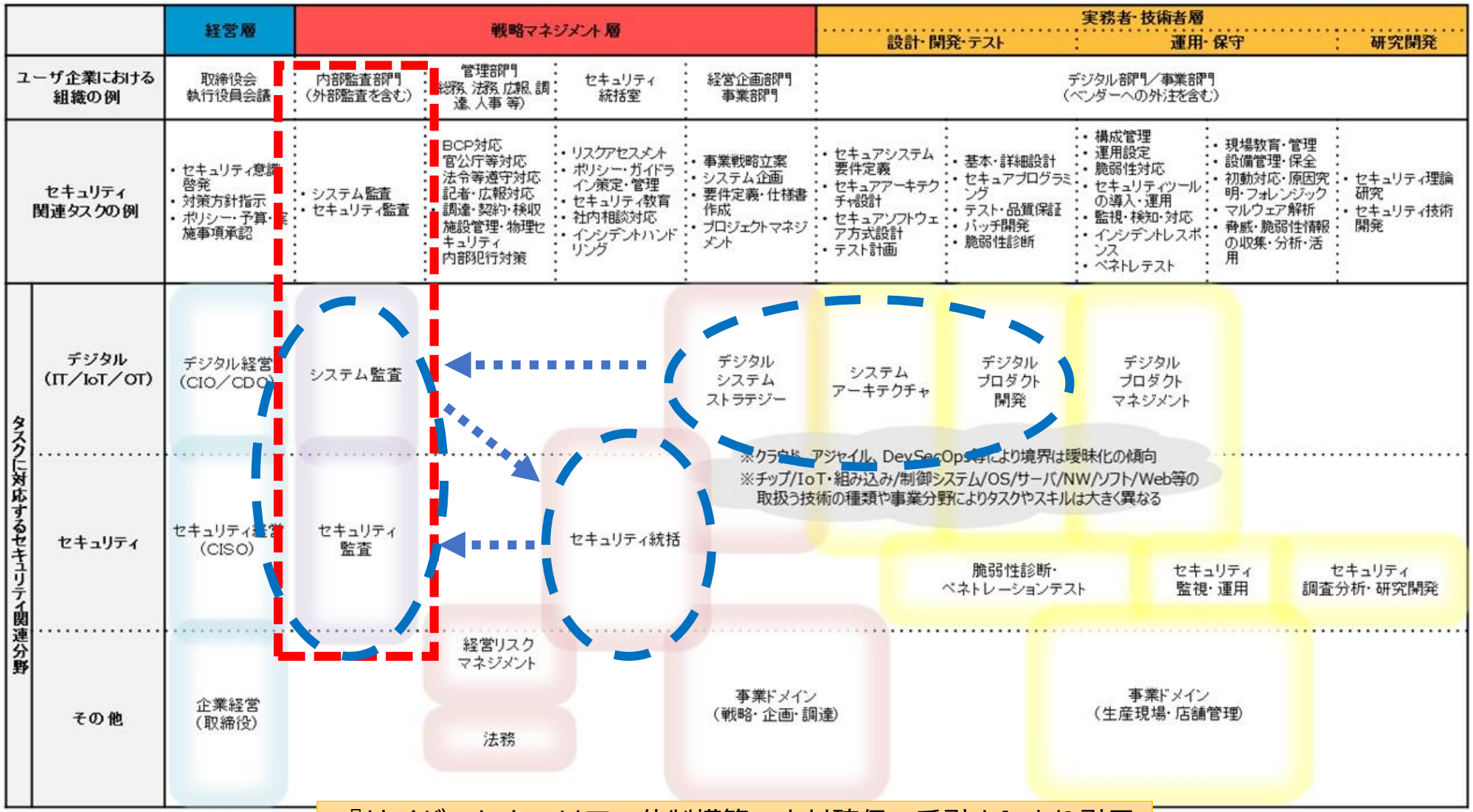
役割の位置づけ



『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

役割の位置づけ



『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

ところで監査って

- 監査ってどんなイメージ？
- 監査を受けるのは好き？
- 最近監査って厳しくなっていない？
- 監査を頼む人は誰？
- 監査って引退間際の人がやるんじゃないの？
- 監査人は指摘事項を見つけると評価されるの？

組織内での役割

JP-RISSA
情報処理安全確保支援士会

- 監査法人は公認会計士の集まりの組織
- 会計監査がメインのお仕事
- 会計士は持っていないのに何をやっているの？
- 主な仕事

  J-SOX監査　上場企業における情報システムの内部統制の評価
  開発プロセス・運用・セキュリティ

  セキュリティ監査　企業や自治体、大学、医療機関なども

  内部監査支援　企業の内部監査の支援 セキュリティも含む

  アドバイザリー　組織のセキュリティ態勢構築支援 など
- 情報の信頼性を提供する。セキュリティは欠かせない要素

TLP：WHITE

RISSであることの価値

JP-RISSA
情報処理安全確保支援士会

- システム監査にとってセキュリティはメインの領域
- 変化するICT環境、複雑化

  スクラッチ開発　→　既成のシステムの組み合わせ

  オンプレミス　→　クラウド化

  個別システム認証　→　統合認証

  紙の証跡、はんこ　→　電子証跡、電子署名、ログの活用
- 増加するサイバーリスク

  株価に影響、インサイダーリスク、データの改竄の可能性

  企業のセキュリティ対応態勢も会計監査で評価が必要

  米国の映画会社、Equifax情報漏洩、日本企業でも被害が増加

TLP：WHITE

結局監査って

- 監査を頼む人は誰？
  投資家・経営者・その他のステークホルダー
- 依頼者にとって欲しい答え
  厳しい評価をした結果問題のないこと
- 監査人は指摘事項を見つけると評価されるの？
  しっかりできていることを第三者の視点で保証することがお仕事
  指摘事項はない方がうれしい
- 後で問題が発覚すると責任を問われるので
  経営者のリスクを肩代わりしているとも言える
- 問題はしっかり指摘して組織を強くすることも仕事の一つ

RISSやセキュリティ人材への期待

JP-RISSA
情報処理安全確保支援士会

- 企業のデジタル化の進展
- 既存の監査手法では保証ができなくなってきている
- 監査のデジタル化も急速に進化
  データで監査する時代に
- 信頼できるデータであることの保証のため
  セキュリティの評価が必須

- 監査 ＋ セキュリティ（テクノロジー）人材の需要が急増

『 プラス・セキュリティ 』人材

TLP：WHITE

どんな人が監査人に向いている？

- リスクに敏感な人
- セキュリティを考えられる人は監査にも向いている
- 幅広い視点で物事を見られる人
- 常に新しい知識を得ることが好きな人
- 資格があることは大事
- 変化の大きな時代には過去の経験だけでは対処できない
- 経営企画部門と並んで経営幹部への登竜門となることも
- 監査視点を持って業務部門に戻って活躍する事例も増えている

3-3.
法務、経営リスクマネジメントの立場から

自己紹介

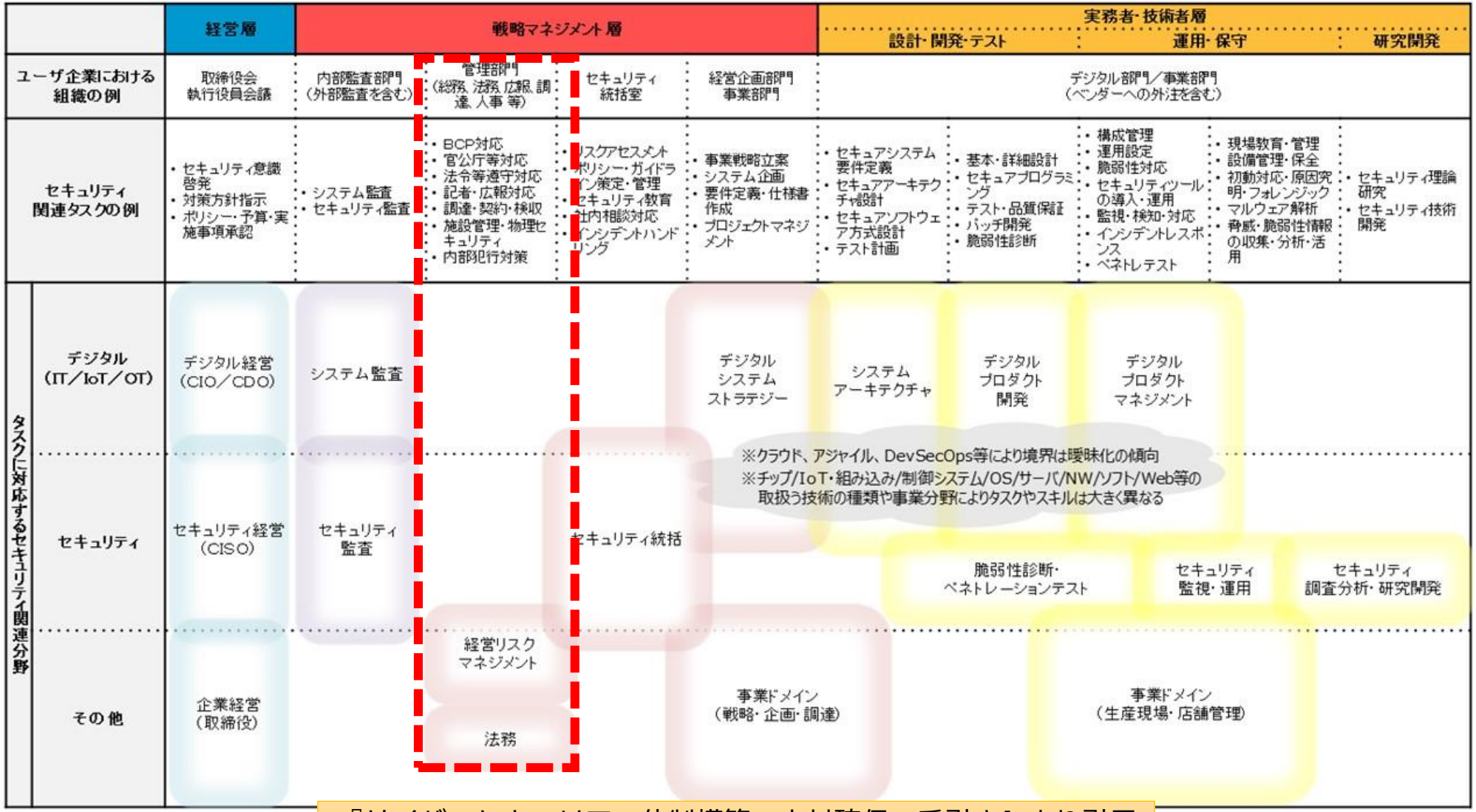
JP-RISSA
情報処理安全確保支援士会

- 足立 昌聰（あだち まさとし）
  - 弁護士、弁理士、情報処理安全確保支援士
  - MCPC IoTプロフェッショナル
  - 公認情報セキュリティ監査人補

- セキュリティ&プライバシーカウンセルというお仕事
  - データ保護（利用者の個人情報やプライバシーの保護）に特化した組織内弁護士としての仕事
  - 情報セキュリティ技術とデータ保護ルールの実装のつなぎ役を兼務

- インハウスの弁護士や弁理士の兼副業のためのプラットフォーム型法律事務所の経営

役割の位置づけ



『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

経営や法務の立場から見たセキュリティ

JP-RISSA
情報処理安全確保支援士会

- 自社が提供する製品やサービスの個人情報影響評価（PIA）
  - 個人情報保護法上の「安全管理措置」をどのように講ずるか
  - 業規制の中のセキュリティ要件をどのように担保するか
- 取引のなかで発生するリスク
  - 自社が提供するサービスが顧客のセキュリティ要件を満たすのか
  - 自社が導入するサービスのセキュリティ水準を契約上担保できるのか
- 「法務はリスクベースで考える」←→「技術手段で解決できるのはセキュリティ人材」
- お互いのことを知り、よりよい関係を維持するための「共通言語」

TLP：WHITE

4.ディスカッション

ディスカッションテーマ：

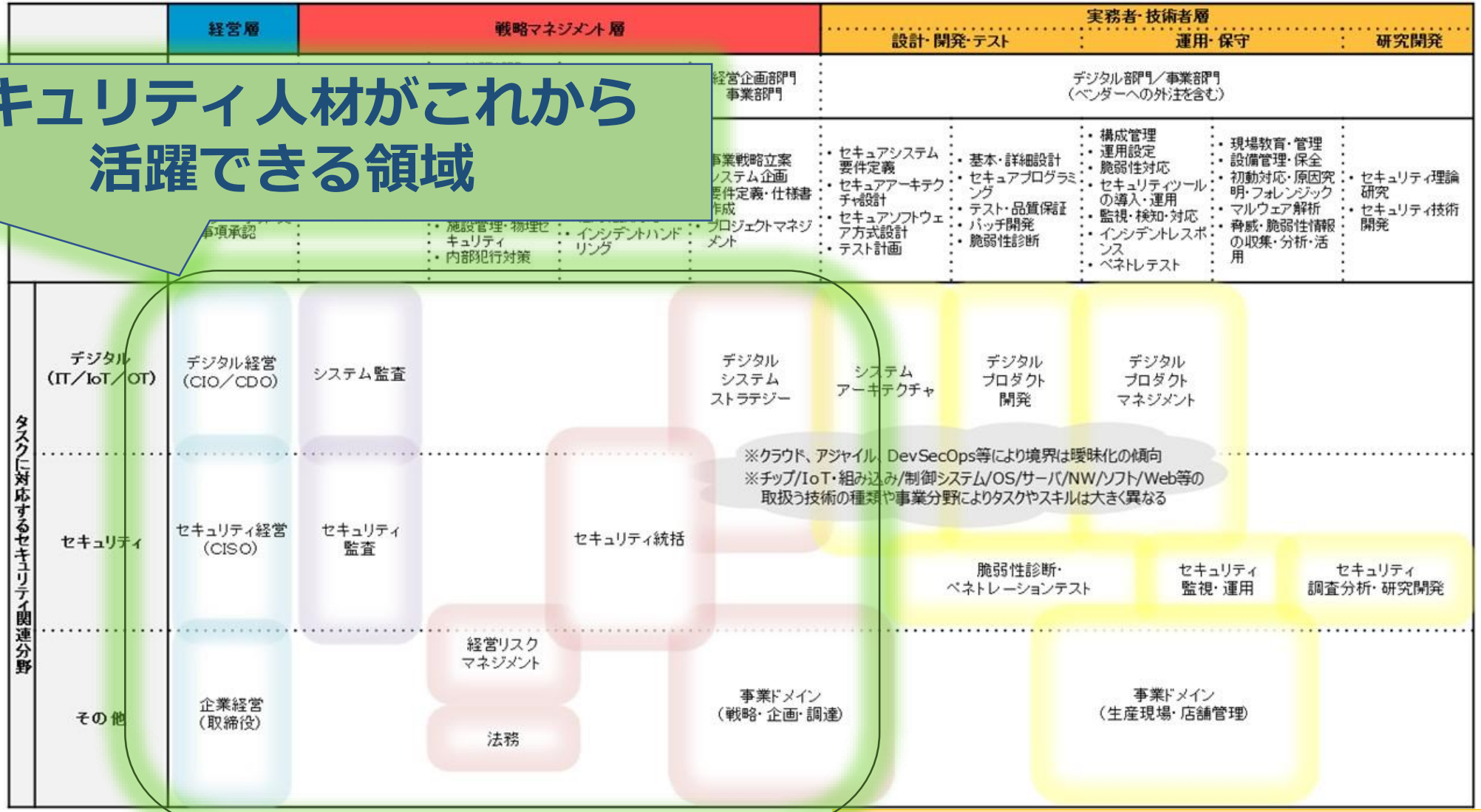
セキュリティ業務に
求められる人材像と実践事例

TLP：WHITE

まとめ

JP-RISSA
情報処理安全確保支援士会

セキュリティ人材がこれから活躍できる領域



『サイバーセキュリティ体制構築・人材確保の手引き』より引用

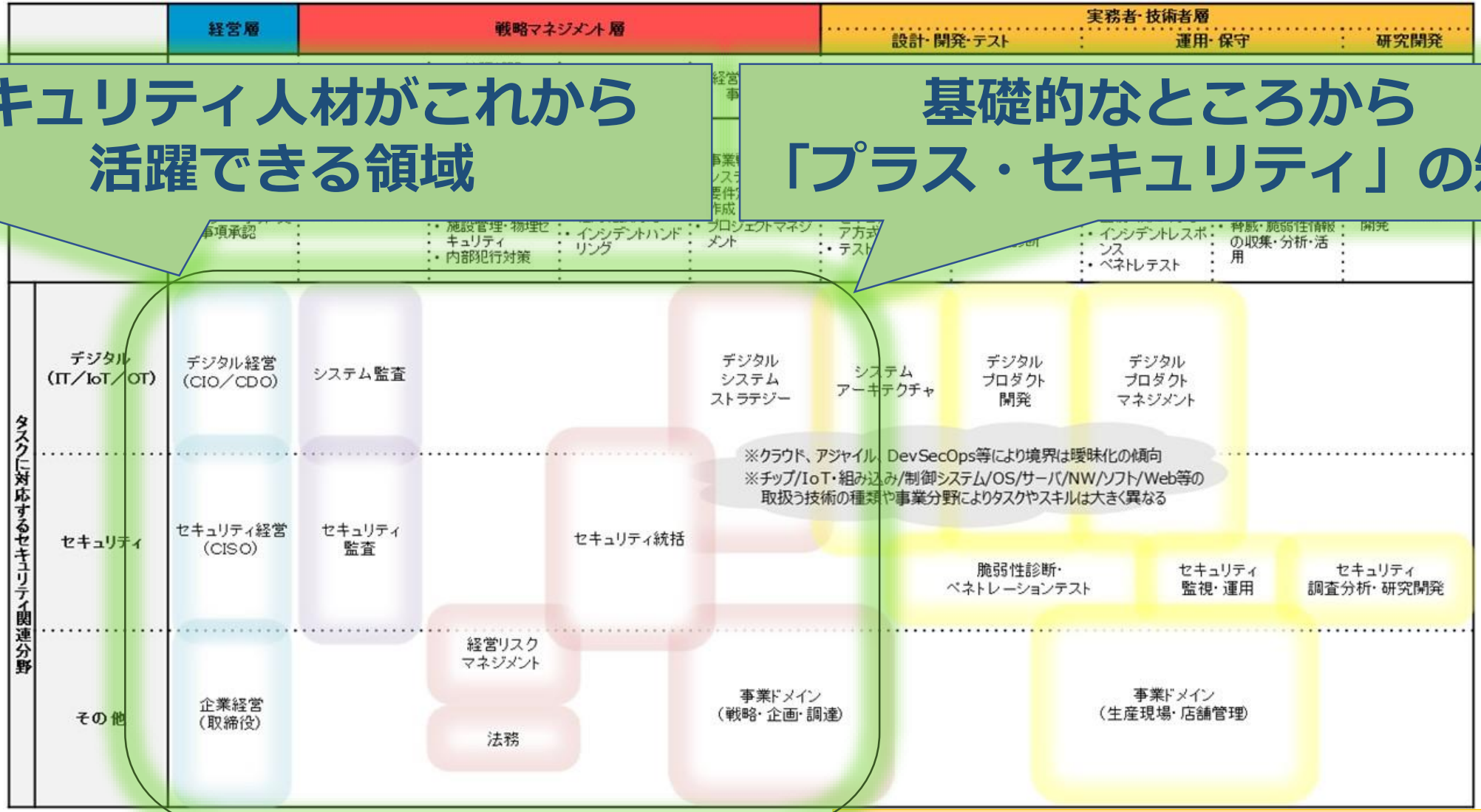
TLP：WHITE

まとめ

JP-RISSA
情報処理安全確保支援士会

セキュリティ人材がこれから活躍できる領域

基礎的なところから「プラス・セキュリティ」の知識



『サイバーセキュリティ体制構築・人材確保の手引き』より引用

TLP：WHITE

まとめ

「セキュリティ」という共通言語を使って、
ビジネスと事業を円滑に進めるために
RISSの活用を！

『サイバーセキュリティ体制構築・人材確保の手引き』より引用

(参考：アイコン、漫画素材)

https://www.irasutoya.com/
https://pixabay.com/ja/

- 本資料の著作権は一般社団法人情報処理安全確保支援士会(以下、JP-RISSA)に帰属します。
- 引用については、著作権法で引用の目的上正当な範囲内で行われることを認めます。引用部分を明確にし、出典が明記されるなどです。
- なお、引用の範囲を超えると思われる場合もJP-RISSAへご相談ください。
- 本文書に登場する会社名、製品、サービス名は、一般に各社の登録商標または商標です。®やTM、©マークは明記しておりません。
- JP-RISSAならびに執筆関係者は、このガイド文書にいかなる責任を負うものではありません。全ては自己責任にてご活用ください。

TLP：WHITE

HomePage：https://www.jp-rissa.or.jp/

お問い合わせ：contact@jp-rissa.or.jp

Twitter：@jp_rissa

JP-RISSA

情報処理安全確保支援士会