ユーザ企業のための
セキュリティ統括室
構築・運用キット
（統括室キット）

Part2【統括室編】

2019/9/30 ver1.0

産業横断サイバーセキュリティ人材育成検討会

セキュリティ経営戦略検討WG（旧 人材育成WG）

はじめに

- 「統括室キット」
  - 「セキュリティ統括室 構築・運用キット」（以下、「統括室キット」）は、産業横断サイバーセキュリティ人材育成検討会（CRIC CSF）において第一期より検討してきた「セキュリティ統括（室等）」を組織体として配置することを検討し、更に組織体としての配置又は、統括人材としての配置を定め、その業務運用手順を定めるものです。
  - 統括室キットは、CRIC CSFの第二期の人材育成WGの成果物として公開しています。

- 対象者
  - 本「統括室キット」は、下記の方々にお読み頂くことをして作成されています。
    1. 企業経営者
    2. CISO等
    3. セキュリティ部門責任者
    4. 情報システム部門責任者
    5. 事業部門責任者
    6. 経営企画部門責任者
    7. セキュリティ部門担当者
    8. その他、事業のリスクマネジメントを検討されている方々

- 著作権

- お問合せ先
  - 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 事務局
    office@cric-csf.jp

統括室キットの構成

- 本「統括室キット」は、以下の構成で策定されています。

1. 統括室キット Part1　概要編
   - CRIC CSFの活動経緯と共有された課題
   - 第一期 成果物「人材定義リファレンス」
   - 第二期 における検討プロセスと活動成果
   - 統括室に求められる機能・役割
   - 統括室を検討する前に確認すべき事項

2. 統括室キット Part2　統括室編
   - 統括室を設置する前に確認すべき事項
   - 統括室を設置する際に確認すべき事項
     - 統括室を組織図に記載するケース
     - 統括室を組織図に記載しないケース
   - 統括室を運用する際に必要となる考え方
   - 全社のセキュリティと部門のセキュリティ

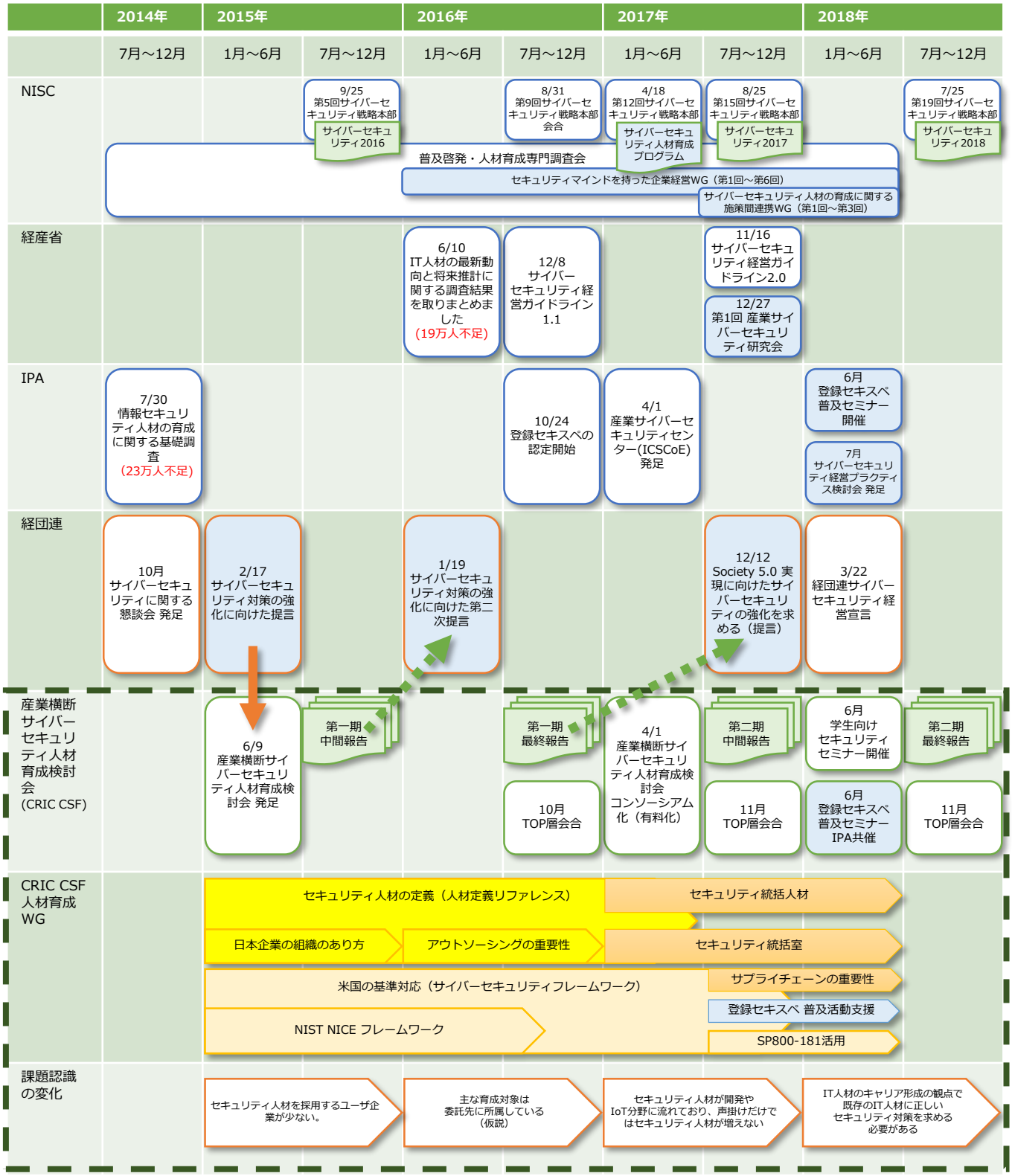
3. 統括室キット Part3　統括人材編
   - 統括室を構成する「統括人材」の定義
   - 「統括人材」に求められる役割・業務の例
   - 「統括人材」に必要とされる育成環境

目次

1.産業横断サイバーセキュリティ人材育成検討会（CRIC CSF）

1. 産業横断サイバーセキュリティ人材育成検討会の沿革

- 産業横断サイバーセキュリティ人材育成検討会の成り立ちと活動の経緯



：CRIC CSF による活動協力、情報共有・情報連携、会合参加、並びに資料等の相互参照関係を示す。

図1-1 産業横断サイバーセキュリティ人材育成検討会の沿革

1. セキュリティ統括室及び統括人材に関する解説

- 統括室キットは、自社のセキュリティ体制に関するアセスメント及び体制構築・運用改善の参考となるべく、以下の3点に配慮し、作成されています。

  1. 日本におけるIT利用は、ユーザ企業とベンダー企業の「分業体制」が前提にあるため、サイバーセキュリティに関するそれぞれの責任範囲が適切に管理されていることが望ましいです。

  2. ITを活用した事業が拡大する中で、不十分なセキュリティ対策は時に事業継続に負の影響を与えることがあり、十分な予算執行を考えるための組織化と権限の設定及び管理者の選任を検討しておくことが望ましいです。

  3. 全社リスクマネジメントの観点から、管理部門との連携を重視し、サイバーセキュリティを司る部署の例を明示することにより、今後、セキュリティ体制を検討するための情報源としてご活用ください。

- 尚、本統括室に関する検討の模様は、以下の資料も合わせてご確認ください。
  - 平成30年6月12日に開催したIPAとCRIC CSFの共催セミナー「今なすべきサイバーセキュリティ対策とそれに必要な人材とは～求められる人材像と情報処理安全確保支援士制度について～」の講演資料はIPAより公開されています。
    - 【講演資料】「サイバーセキュリティとセキュリティ統括人材像」
    - https://www.ipa.go.jp/files/000067124.pdf

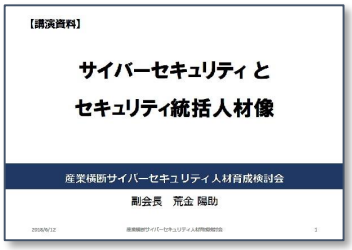


図1-2 サイバーセキュリティとセキュリティ統括人材像

  - 上記講演資料の解説は、第二期 CRIC CSF 副会長 荒金氏の講演映像を合わせてご確認ください。
    - 【講演映像】「CRIC-CSFが検討を進めているサイバーセキュリティとセキュリティ統括人材像」
    - https://www.youtube.com/watch?v=cJkSQhmS6Ic
      - IPA公式 YouTube サイト

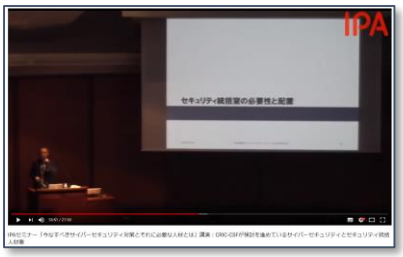


図1-3 CRIC-CSFが検討を進めているサイバーセキュリティとセキュリティ統括人材像

1. CRIC CSF 人材育成WGの取り組み

- CRIC CSF 人材育成WGにおける議論の骨子
  - CRIC CSFは、サイバーセキュリティ人材の育成に向けた様々な取り組みを討議・検証し、期毎に報告書として発表しています。
  - 人材育成WGにおける第二期のテーマは「セキュリティ統括人材」の配置と育成を中核とし、その所属組織（「セキュリティ統括室」）を、組織論及び権限・分掌、並びに人材育成の観点から整理、検証しています。
  - 日々高度化するサイバー攻撃に対応する人材及び組織を、日本の産業構造及び企業文化に対応し、現実的な解を描き出すことが、CRIC CSF 人材育成WGに課せられたミッションです。

- CRIC CSFの検討の範囲
  - CRIC CSFは、重要インフラ事業者を中核とするユーザ企業の集まりとして、事業継続及びサイバーセキュリティ対策の観点から、自社での対応だけではなく、サプライチェーン先との連携及び協業を視野に入れた、ガバナンス、リスクマネジメント、セキュリティ対策を含む幅広い業務に対応する人材育成を議論しています。

- サイバーセキュリティ人材育成に向けた環境構築
  - これまで情報セキュリティに対する取り組みは、政府、省庁、各種セキュリティ団体等を通じて広く普及啓発されてきました。今後は情報資産の保護という観点だけではなく、IT利活用の拡大及び高度化という時代の変化を踏まえ、事業活動にネガティブなインパクトを与える侵害行為（サイバー攻撃等）に迅速に対応していくための必要な取り組みを整理し「セキュリティ統括人材」および「セキュリティ統括室」の配置、運用、育成等を検討していく必要があるとの議論を進めています。

1. CRIC CSF 人材育成WGの成果物

- 「人材定義リファレンス」
  - ユーザ企業における情報システム（IT）領域に関するセキュリティ機能を定義したものです。
  - セキュリティ機能と社内の役割のマトリクスにより構成します。
  - 人材の定義だけではなく、セキュリティ対応スケジュールを定めた「カレンダー」と、アウトソーシング業務を確認するための「アウトソーシングガイド」を公開します。
  - http://cyber-risk.or.jp/sansanren/index.html

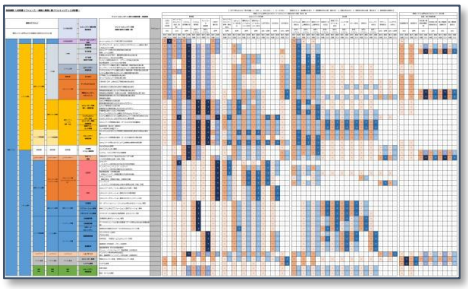


図1-4 人材定義リファレンス

- 「セキュリティ統括室および統括人材」
  - Society5.0に対応するセキュリティ人材のあり方とセキュリティ統括室の配置に関する考え方を、IPA共催セミナーにて公開します（平成30年6月12日）。
  - https://www.ipa.go.jp/siensi/report180612.html

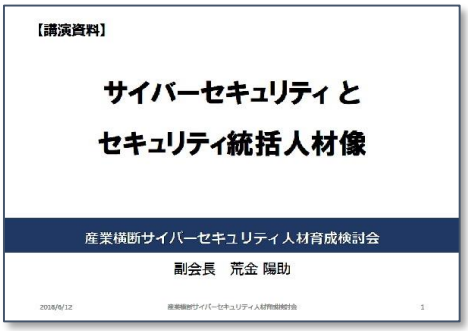


図1-5 セキュリティ統括室および統括人材

- セキュリティ人材育成 研修データベース
  - 国内のセキュリティ人材育成に関する研修情報を収集し、様々な切り口により検索できるデータベースサイトを公開し運用中です。
  - https://cs-edu.jp/

図1-6 セキュリティ人材育成 研修データベース

1. CRIC CSF 成果物の紹介・引用例

- CRIC CSF 報告書及び人材定義リファレンス等の紹介・引用は以下の通りです。

- **日本経済団体連合会**
  - 提言『**Society5.0実現に向けたサイバーセキュリティの強化を求める**』（2017年12月12日）
    - http://www.keidanren.or.jp/policy/2017/103.html
  - 提言『**サイバーセキュリティ対策の強化に向けた第二次提言**』（2016年1月19日）
    - http://www.keidanren.or.jp/policy/2016/006.html

- **内閣サイバーセキュリティセンター（NISC）**
  - 『**サイバーセキュリティ人材育成プログラム**』（2017年4月18日）
    - https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf
  - 『サイバーセキュリティ人材育成総合強化方針』（2016年3月31日）
    - http://www.nisc.go.jp/active/kihon/pdf/jinzai_kyoka_hoshin.pdf

- **金融庁**
  - 『**金融機関のサイバーセキュリティ対策における経営陣・CISO等に期待される役割・責任**』（2017年7月21日）
    - https://www.fsa.go.jp/common/about/research/20170712/20170712.html

- **公益財団法人 金融情報システムセンター**
  - 『**金融機関等におけるIT人材の確保・育成計画の策定のための手引書**』（2018年3月）
    - https://www.fisc.or.jp/publication/disp_target_detail.php?pid=368

- 諸外国において情報発信を頂いているものは以下の通りです。

- **The National Institute of Standards and Technology (NIST)**
  - **NIST Cybersecurity Risk Management Conference**
    - https://www.nist.gov/news-events/events/2018/11/nist-cybersecurity-risk-management-conference
  - **Success Story: Japanese Cross-Sector Forum**
    - https://www.nist.gov/cyberframework/success-stories/japanese-cross-sector-forum

- **NEW AMERICA**
  - **Japanese Cross-Sector Industry Forum Is Shaping Cybersecurity Talent Development Strategy**
    - https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/japanese-cross-sector-industry-forum-shaping-cybersecurity-talent-development-strategy/

- **Palo Alto Networks**
  - **How Japanese Businesses Are Cultivating Cybersecurity Professionals**
    - https://researchcenter.paloaltonetworks.com/2016/10/cso-japanese-businesses-cultivating-cybersecurity-professionals/

  - **サイバーセキュリティ人材育成に関する日本の産業界の取り組みとは**
    - https://www.paloaltonetworks.es/content/pan/ja_JP/company/in-the-news/2016/11-cso-japanese-businesses-cultivating-cybersecurity-professionals.html

1．本資料における「用語の定義」

- サイバーセキュリティ
  - サイバーセキュリティとは、電子データの漏えい・改ざん等や、期待されていた 情報システムや 制御システム等の機能が果たされないといった不具合が生じないようにすることです。
    - 参照先）サイバーセキュリティ経営ガイドライン2.0

- CISO（Chief Information Security Officer）
  - 経営陣の一員、もしくは経営トップからその役を任命された、セキュリティ対策を実施する上での責任者のことです。
    - 参照先）サイバーセキュリティ経営ガイドライン2.0

- CISO等
  - CRIC CSFでは、CISOに求められる役割を担う経営幹部がCISO以外のCRO、CIOや情報セキュリティ委員長等に割り当てられていることを踏まえ、その任にあたる人材を広く「CISO等」と示しています。

- セキュリティ統括（室等）
  - CRIC CSF の第一期「人材定義リファレンス」において定めた役割の1つです。組織図に記載される組織体として配置された場合には「セキュリティ統括室（部、課等も可）」となり、組織図に記載されないチーム体制を敷く場合は「セキュリティ統括」または「CSIRT」等の呼称を用います。

- セキュリティ統括人材
  - セキュリティ統括人材は「セキュリティ統括室」または「セキュリティ統括」を構成する人材です。
  - セキュリティに詳しい人材という意味ではなく、法人組織のリスクマネジメントの一環として、セキュリティ対策に従事する役割を与えられた人材を指しています。尚、部署横断型のセキュリティ体制を敷いている際、「セキュリティ統括室」または「セキュリティ統括」に所属していない場合でも、連携して活動するセキュリティ人材については、セキュリティ統括人材と同様の育成が求められると考えています。

２．統括室キットの活用事例

2．統括キットの活用事例：経済産業省

- 2018年11月に公開しました「統括室キット Part1 (概要編)」の考え方は、経済産業省サイバーセキュリティ課の発表資料において採用されています。

- **経済産業省 産業サイバーセキュリティ研究会**
  - https://www.meti.go.jp/press/2017/12/20171226004/20171226004.html

  - **第4回 産業サイバーセキュリティ研究会 ワーキンググループ２（経営・人材・国際）**
    - https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/004.html

  - 本ワーキンググループにおける議論の中で、CRIC CSFにおいて検証を続けている、人材定義リファレンスに定めた「セキュリティ統括（室等）」の想定業務に基づく「セキュリティ統括機能」の考え方が採用されています。

    - 資料3　事務局説明資料（PDF形式：4,757KB）
      - https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/004_03_00.pdf

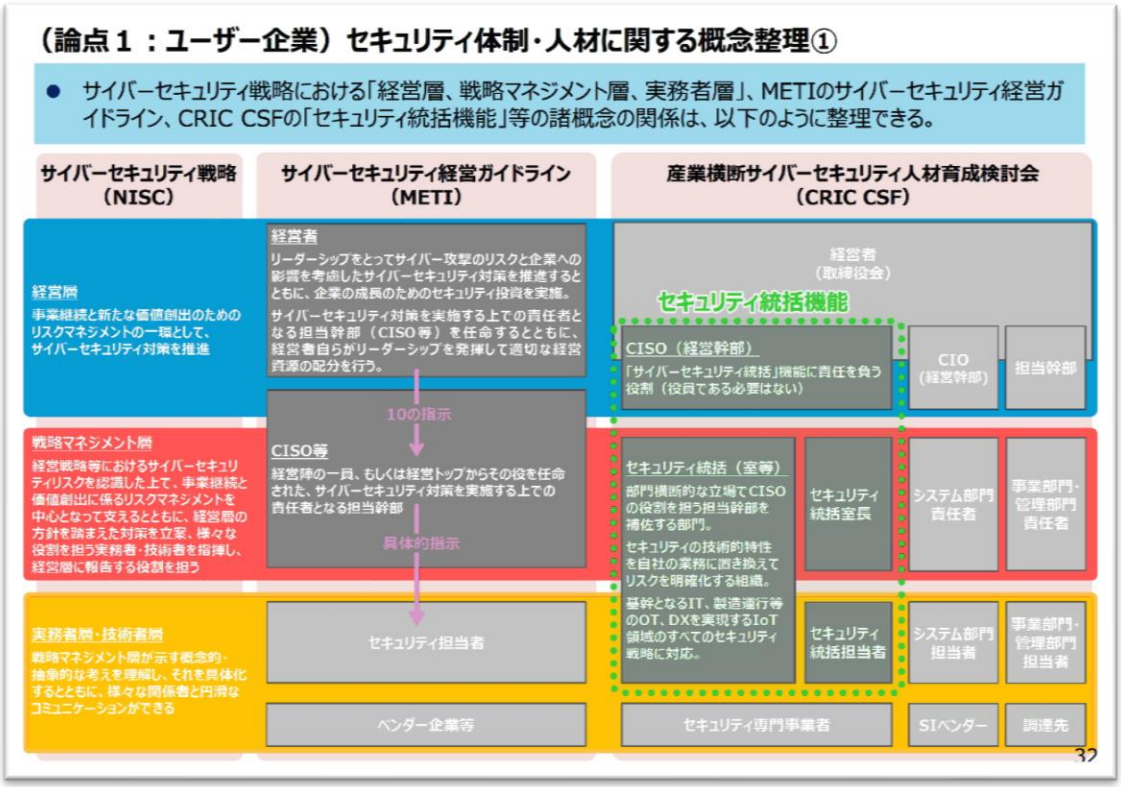


図2-1 セキュリティ体制・人材に関する概念整理①

2．統括キットの活用事例：経済産業省

- 資料3　事務局説明資料（PDF形式：4,757KB）
  - https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/004_03_00.pdf

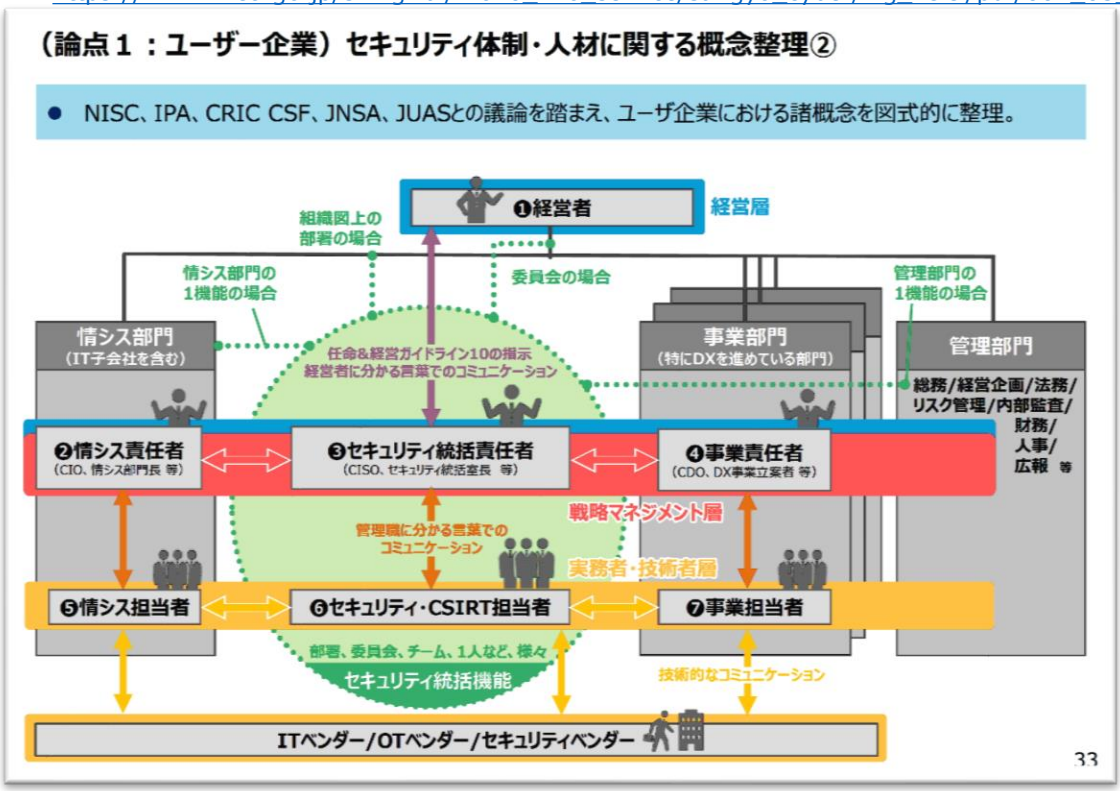


図2-2 セキュリティ体制・人材に関する概念整理②

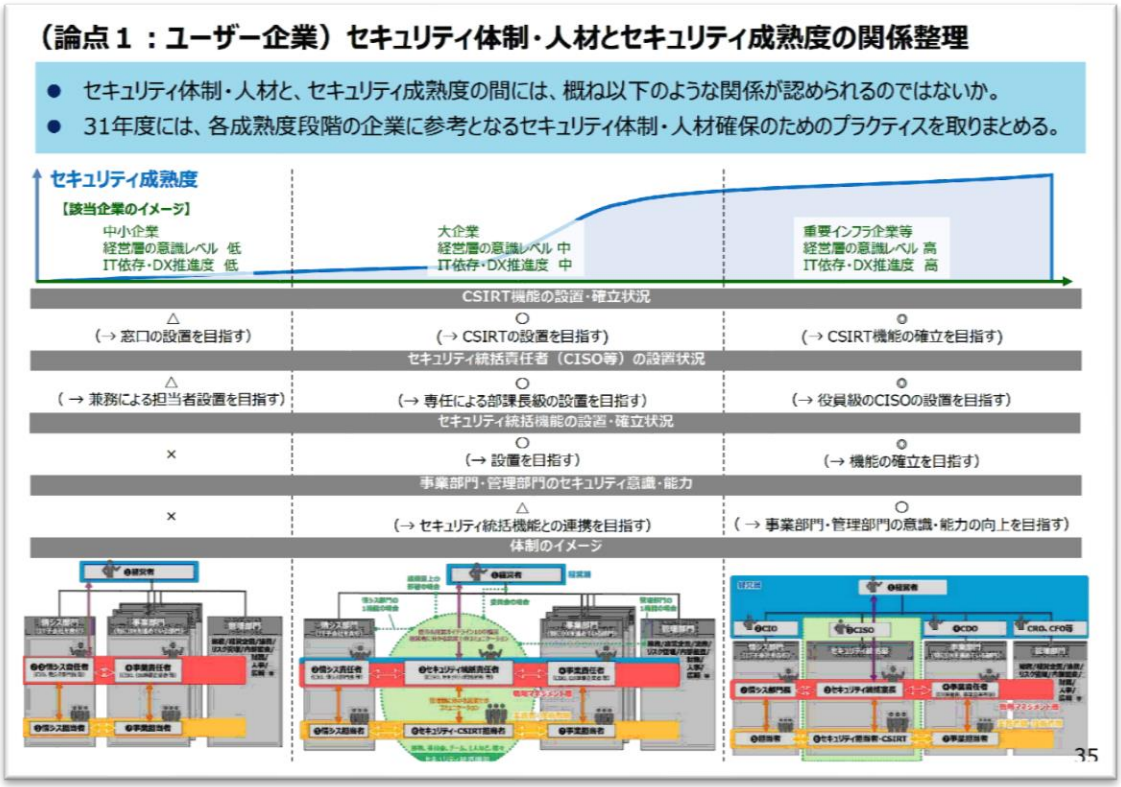


図2-3 セキュリティ体制・人材とセキュリティ成熟度の関係整理

3. セキュリティ統括室の設置を検討する前に

- セキュリティ統括室 チェックシート
  - セキュリティ統括室を配置すべきか確認するチェックシートです。

1.	取締役会や経営会議等において、IT利用及びセキュリティに関する議題が扱われている。	□
2.	グループ会社のセキュリティ対策は、事業内容や規模により、レベルを分けて適用している。	□
3.	システム監査だけではなく、セキュリティ監査が実施されている。	□
4.	営業や製造等を含む全ての業務プロセスのリスクアセスメントが継続的に実施されている。	□
5.	事業部門・部署の責任者の役割の中に、情報セキュリティの徹底が定められている。	□
6.	情報システムの「構成管理」は徹底されている。	□
7.	委託先からシステム障害等の各種インシデントに関する報告を月1回以上受けている。	□
8.	社員が利用するクラウドサービス利用状況を把握できている。	□
9.	営業進出先の各国法令・ガイドラインの更新状況を常に確認できる体制となっている。	□
10.	社外からの通報を受けた場合の対応プロセスが定められている。	□

図3-1 セキュリティ統括室 チェックシート

- チェックの数
  - 7 以上　現行体制のまま、統括するセキュリティ機能をご確認ください。
  - 4～6　組織横断型のチーム運営と、独立部署での運用のどちらでもセキュリティ運用が可能と考えられますので、初動対応と予算執行の観点から、組織作りをご確認ください。
  - 1～3　まずは責任者の配置と業務範囲を検討ください。
  - 0　0であることを、知られないように、お願いします。

3. セキュリティ統括室の設置を検討する前に

- CRIC CSFでは、総務部門を中核とした組織分化のプロセス検証から始まり、情報セキュリティ体制の構築・運用状況を検証し「セキュリティ統括室」というモデルに到達しました。

- この総務部門を起点とした、役割の細分化の検証は、昭和から平成にかけて、多くの企業が経験しているものであり、経営層が組織構造を考えるプロセスをトレースしながら、多くの日本企業で採用可能な検証モデルの1つとして活用しています。

- 2000年頃、日本国内で「コンプライアンス」という言葉が使われ始めました。企業不祥事が発覚する等により、コンプライアンスの重要性が認識され始めましたが、CSRという考え方に至る前には、倫理観や組織文化の問題として捉えられ、コンプライアンス部門という専任組織を設置するようになるのは、この数年後です。

- 更にさかのぼると、今では当然の組織体となっている「経営企画部」も、1980年代に注目され始め、徐々に普及してきました。主に、事業戦略の立案を担うための組織とされることが多いのですが、これもいくつかのパターンがありました。

  1. 総務部門から分離した経営企画部門
  2. 財務部門から分離した経営企画部門
  3. 社長直轄プロジェクトから独立した経営企画部門

- 上記、コンプライアンス部や経営企画部の成り立ちをひも解くことにより、経営に必要となる組織と機能を定義し、新たに「セキュリティ統括機能」を担う組織体を検討することができるのではないかと考えています。

■ **セキュリティ人材とはどのような業務に従事する人材なのかを、企業における事業規模の拡大と組織機能の分化の観点から検証し、セキュリティ人材像を描くこととした。**

- **第一期の検討の流れ**
  - ユーザ企業における組織分化プロセス（総務部門～情報システム部門）の検証

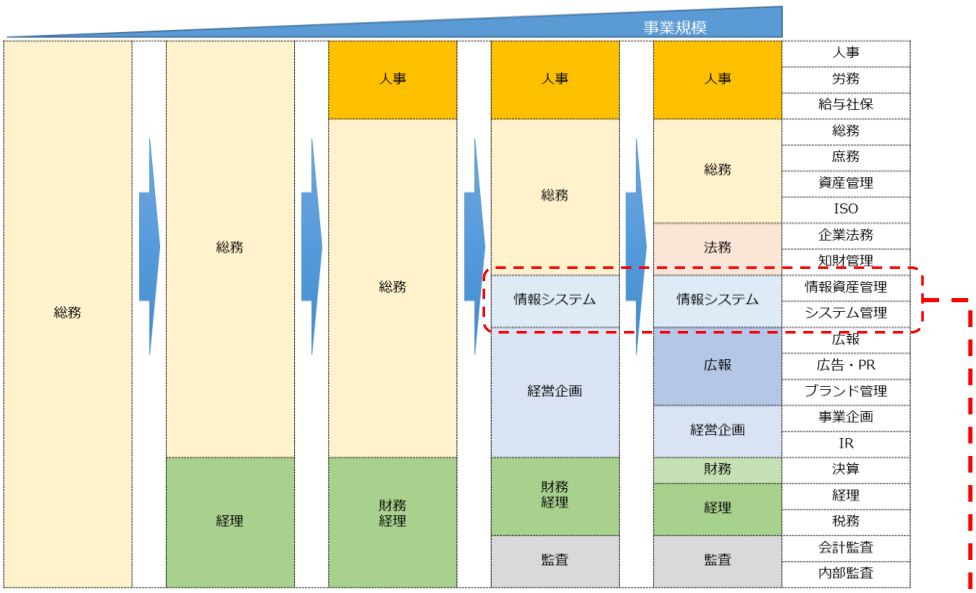


図3-2 ユーザ企業における組織分化プロセス（総務部門～情報システム部門）の検証

  - ユーザ企業における組織分化プロセス（情報システム部門の機能）の検証

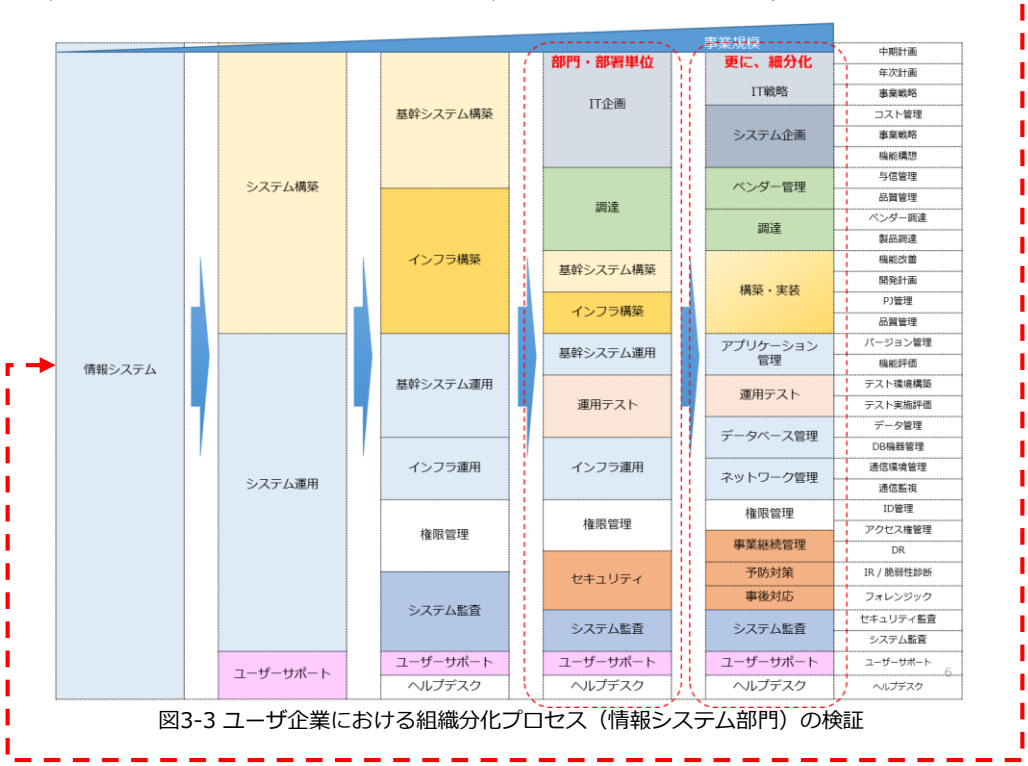


図3-3 ユーザ企業における組織分化プロセス（情報システム部門）の検証

4．セキュリティ統括室の必要性の検証

- ITに関わる意思決定と情報共有のあり方（例）
  - 業務とIT/OT/IoTが密接に関わる事業環境では、情報システム・サービスの導入・運用・更新の際のリスクアセスメントを実施する際、様々な情報を複合的に共有することになります。
  - 事業継続を支える情報システムの安定的な稼働を、ガバナンス、IT-BCP、セキュリティの観点等から情報共有していく必要に迫られています。

  - ここでは、レイヤー毎の意思決定に必要とされる情報と、情報共有の幅を図式化します。

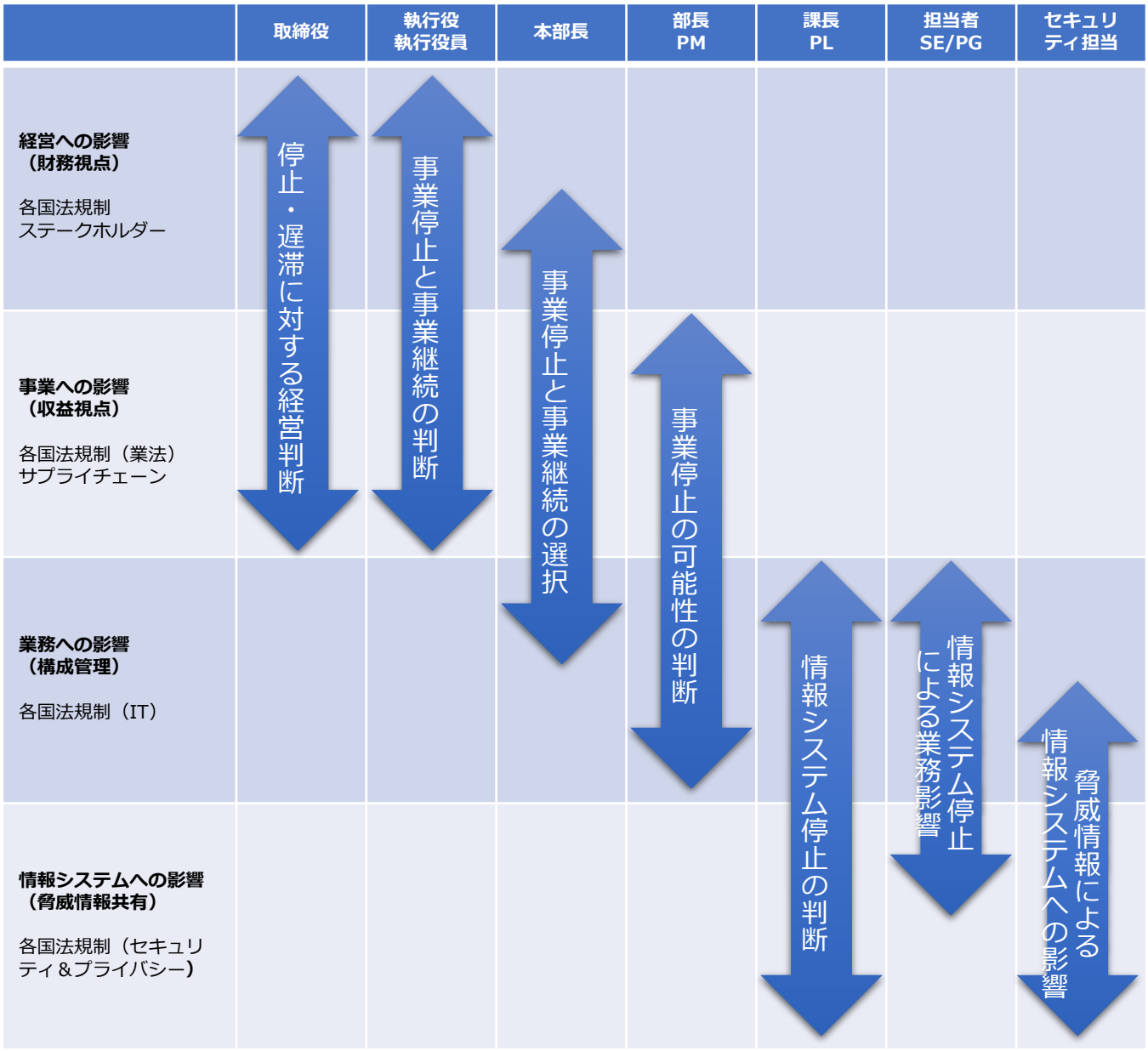


図4-1 ITに関わる意思決定モデル

- セキュリティインシデント及び事件・事故への対応（例）に基づく、情報の取り扱い
  - 本項では、セキュリティインシデント発生から事件・事故の収束に必要とされる情報の例を記します。セキュリティインシデントの疑いや通報から、原因を究明し、対策を講じ、場合によっては事業運営の改善・変更を含む意思決定を行うまでに必要と考えられる様々な情報の種類をマッピングしています。

インシデントの確認から収束までのプロセス	各組織	管理部門	セキュリティ担当組織	委員会	経営層 CEO/CISO
事業運営の復旧	◘ 復旧にかかるコスト（時間・資金）	◘ 財務的影響 ◘ 広報的影響			◘ 経営リスク
セキュリティ事件・事故対応の公表		◘ 事故報告の内容	◘ 事故報告の技術的内容	◘ 事故報告の実施に関する内容	◘ 会見等での想定問答
事業運営の変更または停止措置	◘ 変更にかかるコスト（資金） ◘ 停止した場合の損失（売上）		◘ 変更を実施するための手順 ◘ 変更した場合の影響分析	◘ 変更に伴う社内外への影響	
セキュリティ事件・事故対応の指定 報告先への対外報告	◘ 報告書の作成	◘ 監督官庁等への報告	◘ 報告書の技術的レビュー		
セキュリティ事件・事故の対処実務	◘ 事業停止または変更の影響度の測定	◘ 対外的影響度の確認および事前報告先の特定	◘ 技術的対応の実務支援 ◘ 情報収集および情報共有		
セキュリティ事件・事故の被害に関する個別連絡	◘ 損害を受けた先（があれば）への対応	◘ 損害を受けた（と確認できていない）申し出への対応			
セキュリティ事件・事故に繋がる可能性のある問合せ窓口		◘ 株主・顧客からの問合せ対応	◘ 一般の外部通報への対応		
セキュリティ事件・事故の予兆検知	◘ 現場での予兆の把握、確認		◘ 情報システム上の予兆の確認 ◘ 脅威情報からの予兆の確認		

図4-2 インシデント対応における共有情報

- この図を活用頂く際には、以下の手順で確認ください。
  1. 「インシデントの確認から収束までのプロセス」（縦軸）に従い、それぞれの段階で必要とされる情報の組み合わせを確認してください。
  2. 各組織から経営層わたる横軸において、「情報」にどのような違いがあるのかを比較します。
  3. 左下から右上に向かう流れの中で、必要とされる情報量や、纏め方を確認します。例）ログデータをどのように加工していくと経営層の意思決定に反映できるか。

4. セキュリティ統括室の必要性の検証

- セキュリティインシデント及び事件・事故への対応（例）に基づく、役割と行動の整理
  - 下図では、CSIRT活動や委員会活動における意思決定プロセスを繋げて、セキュリティインシデント発生時から事業活動への影響を確認し、対応を決定するまでの流れを模式化しています。セキュリティインシデントの疑いや通報から、原因を究明し、対策を講じ、場合によっては事業運営の変更を含む意思決定を行うまでの流れを示しています。

インシデントの確認から収束までのプロセス	各組織	管理部門	セキュリティ担当組織	委員会	経営層 CEO/CISO
事業運営の復旧	◎			報告先	◎
セキュリティ事件・事故対応の公表		◎	○	○	○
事業運営の変更または停止措置	◎		○	○	報告先
セキュリティ事件・事故対応の指定報告先への対外報告	○	◎	○	報告先	報告先
セキュリティ事件・事故の対処実務	◎	○	○	報告先	報告先
セキュリティ事件・事故の被害に関する個別連絡	○	◎	報告先		
セキュリティ事件・事故に繋がる可能性のある問合せ窓口		◎	○		
セキュリティ事件・事故の予兆検知	○		◎		

- 【凡例】 ◎：判断又は実務を行う、○：判断又は実務を支援する、報告先：報告を受ける

図4-3 インシデント対応における意思決定モデル

- 想定される課題
  1. 各段階においては、同じ事象（インシデント）に対して、共有すべき情報が異なります。
  2. 各組織においては、同じ事象（インシデント）に対して、意思決定に必要とされる情報が異なります。
  3. 1つの意思決定に対して、上記１．と２．を組み合わせた情報と判断基準が必要です。
  4. 被害の大きさや経済的インパクト、世間の関心に応じて、社内外で対応する役職（権限）が一意に定まらず、状況に合わせた意思決定が必要です。
  5. 事実・真実を管理するプロセスと、風評・リピュテーションを管理するプロセスが同時進行で行われます。
  6. ステークホルダーを分解し、それぞれに適切な説明責任を果たすことが求められます。

・セキュリティ統括室の役割分担を検討するためのイメージ（案１）：選択制

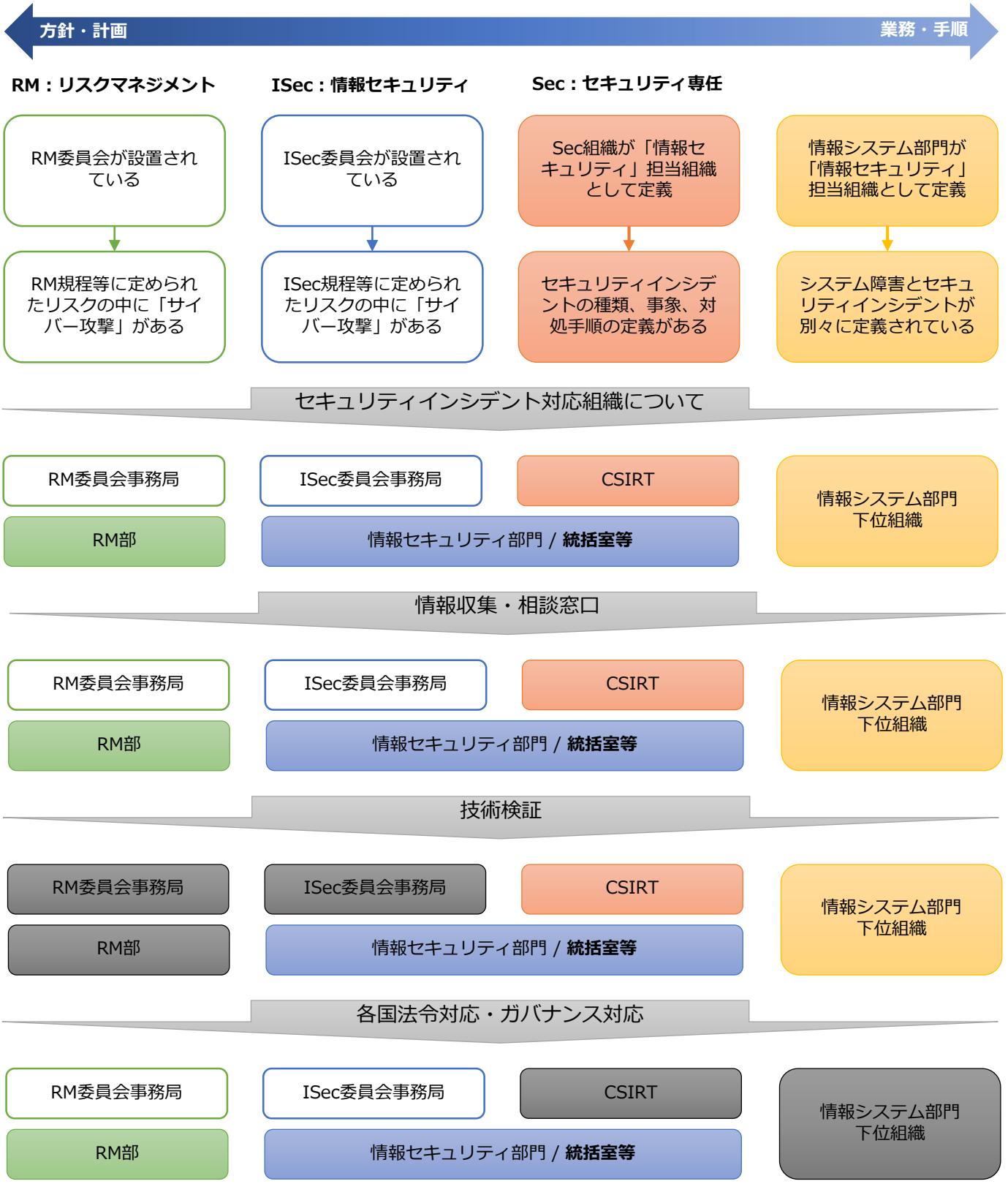


図4-4 セキュリティ組織における役割分担

5. セキュリティ統括室の配置に向けた検討

- セキュリティ統括室の機能
  - セキュリティ統括室は、ITが事業基盤として拡大するユーザ企業のためのセキュリティ対策を網羅的に統括することを目指し、その役割と機能を定義しています。
  - 特に、日本のユーザ企業では、システム構築や運用を外部委託する傾向が強いことから、適切な「分業体制」を管理することに主眼を置いています。
  - 更に、事業展開する国々の法令やガイドラインへの対応、内部統制やリスクマネジメントの観点から、事業継続上重要となるサイバーセキュリティのあり方を検討・検証する機能を重視しています。

図5-1 セキュリティ統括室の機能

- セキュリティ統括室の姿
  - セキュリティ統括室は「統括室」となっていますが、部門・部署として配置することだけを目指しているわけではありません。
  - セキュリティ統括人材のような1名または数名での対応体制であっても、CSIRTのような特定の活動目的を持ったチーム体制でも、本編で解説しています組織図に記載される「統括室」であっても良いと考えています。

- セキュリティ統括室の配置を考える目線
  - サイバーセキュリティに必要な取り組みは、経営レベルのものから、IT運用のセキュリティ対策やセキュリティインシデント対応まで、広範囲に把握し対応していかなければなりません。各種法令対応や事業上必要なガイドライン対応、個別事案への対応等、求められる知識や手順（ノウハウ）が異なり、常に対応チームを組んで対応していく必要があります。
  - サイバーセキュリティを統括する上では、経営レベルから現場レベルの縦方向と、 IT/OT/IoTといった事業と組み合わさった横方向を同時に考えていく必要があります。

- 右図を参考とする場合、会社がどの国で事業を展開しているのか、またその国々ではIT利用やセキュリティ対策における義務がどのように課せられているのかを確認し、実効的な対策を行う必要があります。
- その実効的な対策が、どのガイドラインを参考とし、どのようなシステム構成、運用体制で行わなければならないのかを調査、企画、導入、構築の支援を行い、また　アセスメントや監査を必要に応じて実施すること等をそれぞれ整理し、統合的に判断できることが重要です。

図5-2 セキュリティ統括室の機能

- セキュリティ統括室の機能定義の重要性
  - 「セキュリティ専任組織」を設置している場合、セキュリティ対策に必要となるコストは、組織運営に必要となるコストと、情報システムに対する実装レベルでのコストを分けて考える必要があります。
  - 特に、情報システムの構築や運用におけるセキュリティ対策では、セキュリティ要件が明確で、セキュリティ投資という観点ではなく、IT投資の中で実行される部分が少なくないことも議論されています。

  - 今後、事業がグローバルに展開され、情報システムがサイバー空間を通して国境を越えた運用をされていくこと、更にはDX（デジタルトランスフォーメーション）やIoT利用等、事業運営の中にITが積極的に活用されていく中で、ガバナンスや戦略レベルでのセキュリティと、実装レベルでのセキュリティの両方を考えていく必要があると想定されます。

  - セキュリティ統括室が担うべき機能の一覧は、専任組織にするか既存組織で分担するかも含めて、経営と事業に安全と安心を確保する1つの手段として検討いただくためのモデルとして公開しています。

  - 本「構築編」では、上記考え方に基づき、どのような検討プロセスを経ることができるのか、様々な角度から検証を行っています。

図5-3 セキュリティ統括室の機能

- 管理部門として位置付けた場合のセキュリティ統括室の役割イメージ
  - 「支援内容」の実施主体が、各管理部門にあるか統括機能が担うのかを検討ください。

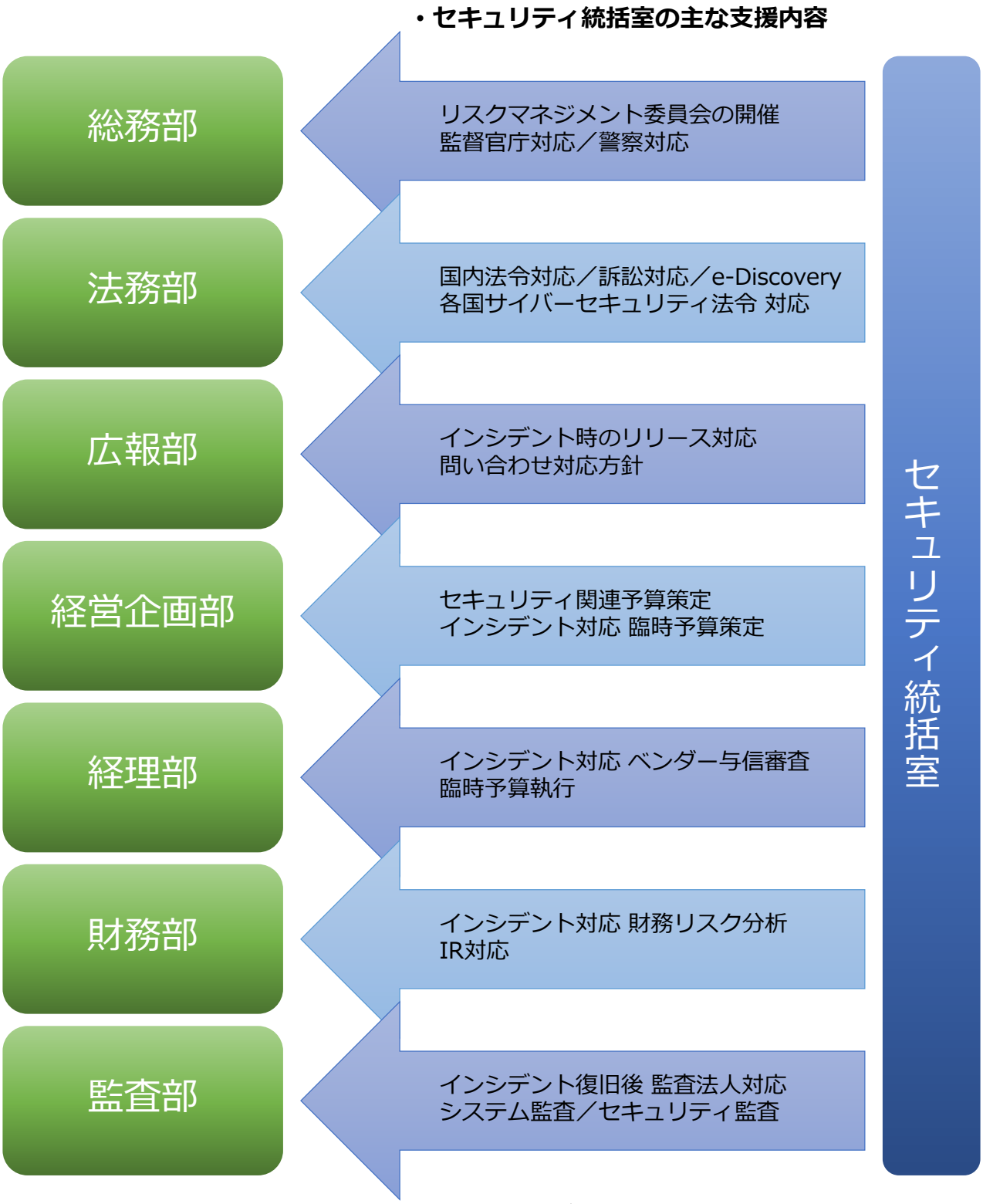


図5-4 セキュリティ統括室の主な支援内容

5.「セキュリティ統括室」配置に向けた検討

- 第一期「人材定義リファレンス」から考える役割と機能

【縦軸】
人材定義リファレンスでは、セキュリティ領域における機能の一覧を縦軸に記しています（IT領域中心）。

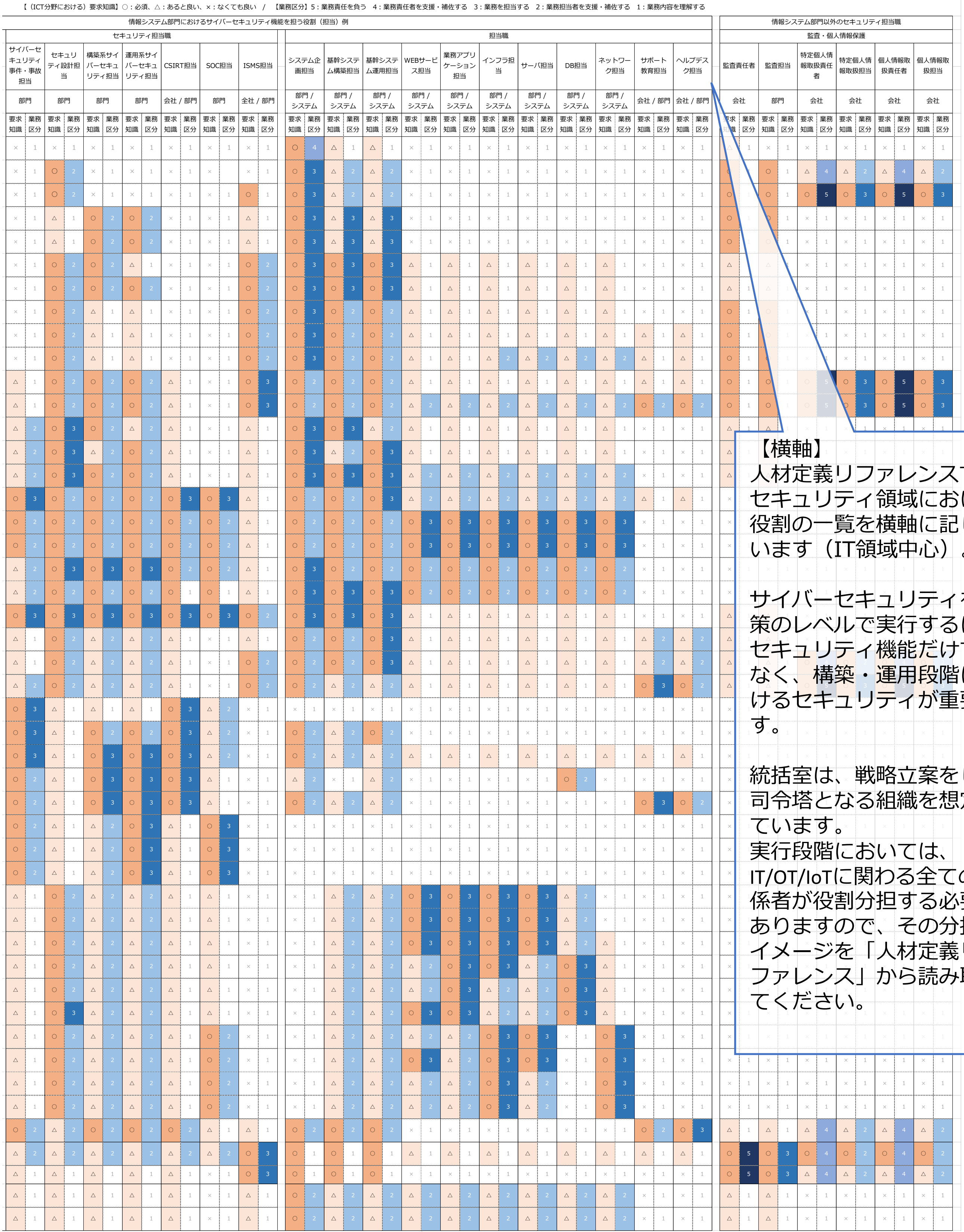
統括室を構成する機能を定義する際には、統括機能の一覧をベースに、こちらの「セキュリティ機能定義」および「サイバーセキュリティ対策 機能を実現する業務（例）」を参考に、必要とされる業務を抽出してください。

産業横断 人材定義リファレンス ～機能と業務に基づくセキュリティ人材定義～

機能分化プロセス				主な機能概要	セキュリティ機能定義 最終報告	サイバーセキュリティ対策 機能を実現する業務（例）	スキルセット	CISO CRO CIO等		サイバーセキュリティ統括（室等）		システム部門責任者		システム管理者		ネットワーク管理者		CSIRT責任者	
								全社		全社		部門		部門／システム		部門／システム		部門	
								要求知識	業務区分	要求知識	業務区分	要求知識	業務区分	要求知識	業務区分	要求知識	業務区分	要求知識	業務区分
情報システム					サイバーセキュリティ統括	サイバーセキュリティ対策に関する全社的統括		○	5	○	4	○	4	×	1	×	1	○	4
情報システム				IT戦略	事業戦略 中期計画	コンプライアンス、ガバナンス及びリスクマネジメントの観点に基づくセキュリティ対策		○	4	○	4	○	5	△	4	△	4	○	4
情報システム				IT戦略	年次計画	セキュリティ対策に係る実施計画の企画立案 規程・ルールの策定		○	4	○	4	○	5	△	4	△	4	○	4
情報システム				IT戦略	ICT企画（個別IT企画）	各事業におけるIT導入・構築運用改善計画の企画立案 ガイドライン・マニュアルの策定		○	4	○	4	○	5	△	4	△	4	△	1
情報システム				IT戦略	ICT企画（個別IT企画）	ライセンス管理を踏まえた、リプレース計画の企画立案 固定資産管理・ソフトウェア会計管理		○	4	△	1	○	5	△	4	△	4	△	1
情報システム				システム企画	セキュリティ実装計画	ユーザビリティの観点に基づく機能改善・実装計画の企画立案 エンドポイント及びLIに関するセキュリティ機能改善計画の策定		○	4	△	1	○	5	△	4	△	4	△	1
情報システム				システム企画	セキュリティ実装計画	システムセキュリティの観点に基づく機能改善・実装計画の企画立案 システム構成に関するセキュリティ機能改善計画の策定		○	4	○	4	○	5	△	4	△	4	△	1
情報システム				事業継続	IT-BCP	ICT環境における事業継続計画の策定 サイバーセキュリティ保険の導入検討		○	4	△	1	○	5	△	4	△	4	△	1
情報システム				セキュリティ対策	ディザスタリカバリ	災害対策（DR）に関するICT環境改善計画の策定		○	4	△	1	○	5	△	4	△	4	△	1
情報システム				セキュリティ対策	ディザスタリカバリ	災害対策及び災害発生時に関する稼働計画の策定		○	4	△	1	○	5	△	4	△	4	△	1
情報システム				セキュリティ対策	情報セキュリティマネジメント	情報資産保護活動におけるICT環境改善計画の策定 情報資産の保護基準・保護方法の改善、情報漏洩保険の導入検討		○	4	○	4	○	5	○	4	○	4	△	1
情報システム				セキュリティ対策	情報セキュリティマネジメント	情報資産保護活動におけるICT運用改善活動の策定 情報資産の棚卸		○	4	○	4	○	5	○	4	○	4	△	1
情報システム			基幹システム構築	基幹システム インフラ 構築・実装	セキュリティ対策 導入・開発計画	セキュア構築設計の企画立案 要件定義及び基本設計におけるセキュアデザイン		△	1	○	4	△	4	○	5	○	5	○	4
情報システム			基幹システム構築	基幹システム インフラ 構築・実装	セキュリティ対策 導入・開発計画	セキュア運用設計の企画立案 詳細設計及び運用改善におけるセキュアデザイン		△	1	○	4	△	4	○	5	○	5	○	4
情報システム			基幹システム構築	基幹システム インフラ 構築・実装	セキュリティ対策 導入・開発計画	多層防御に基づくセキュア設計管理 ネットワーク及びシステム構成に対するセキュアデザイン		△	1	○	4	△	4	○	5	○	5	○	4
情報システム			基幹システム構築	基幹システム インフラ 構築・実装	システムセキュリティ対応	システム構築及びシステム運用のセキュリティ対策分野に関するプロジェクトマネジメント及びプロジェクト運用支援		△	1	○	5	△	4	○	4	○	4	○	5
情報システム			基幹システム構築	基幹システム インフラ 構築・実装	セキュリティ製品品質管理	セキュリティ対策関連の製品・サービスに対する評価検証		△	1	○	4	△	4	○	5	○	5	△	4
情報システム			基幹システム構築	基幹システム インフラ 構築・実装	運用テスト パッチ管理	脆弱性診断（導入時・運用時） パッチ適用時の評価テスト		△	1	○	4	△	4	○	5	○	5	△	4
情報システム			インフラ環境構築	インフラ環境構築	セキュリティ機能改善	全システムに対するパッチ管理及び脆弱性診断に関する計画の企画立案		△	1	○	4	△	4	○	5	○	5	○	4
情報システム			インフラ環境構築	インフラ環境構築	セキュリティ機能改善	セキュリティ対策関連の製品・サービスの選定及び実装支援		△	1	○	4	△	4	○	5	○	5	△	4
情報システム			インフラ環境構築	インフラ環境構築	セキュリティ機能改善	セキュリティ対策におけるシステム的機能の継続的改善活動		△	1	○	4	△	4	○	5	○	5	○	4
情報システム		権限管理	権限管理	権限管理	ID管理 アクセス権管理	ActiveDirectry管理 シングルサインオン管理		×	1	△	1	○	5	○	4	△	1	×	1
情報システム		権限管理	権限管理	権限管理	ID管理 アクセス権管理	システム、フォルダ等アクセス権管理		×	1	△	1	○	5	○	4	△	1	×	1
情報システム		ユーザーサポート	ユーザーサポート	ユーザーサポート	サポート 教育	社内のICTリテラシー向上のためのユーザー支援 リスク対応教育の企画・計画・実施		×	1	○	4	○	5	○	4	△	1	○	4
情報システム	システム運用	基幹システム運用	セキュリティ対応 インシデント対応	セキュリティ対策（サイバーセキュリティ対応）	CSIRT	コマンダー インシデント発生時の全社対応及びCISO等補佐		×	1	○	5	△	1	△	1	△	1	○	5
情報システム	システム運用	基幹システム運用	セキュリティ対応 インシデント対応	セキュリティ対策（サイバーセキュリティ対応）	CSIRT	インシデントハンドリング・トリアージ インシデント発生時の初動対応及び収束対応		×	1	○	4	△	1	△	1	△	1	○	5
情報システム	システム運用	基幹システム運用	セキュリティ対応 インシデント対応	セキュリティ対策（サイバーセキュリティ対応）	CSIRT	脅威情報収集、対策情報収集 日常のインシデント情報収集及び社内共有活動		×	1	○	4	△	1	△	1	△	1	○	5
情報システム	システム運用	基幹システム運用	セキュリティ対応 インシデント対応	セキュリティ対策（サイバーセキュリティ対応）	CSIRT	フォレンジックス 機器の保全、被害拡大抑止、証跡保全活動		×	1	○	4	△	1	△	1	△	1	○	5
情報システム	システム運用	基幹システム運用	セキュリティ対応 インシデント対応	セキュリティ対策（サイバーセキュリティ対応）	CSIRT	トレーニング インシデント対応能力向上に向けた教育の企画・計画・実施		×	1	○	4	△	1	△	1	△	1	○	5
情報システム	システム運用	基幹システム運用	セキュリティ対応 インシデント対応	セキュリティ対策（サイバーセキュリティ対応）	SOC	セキュリティオペレーション業務における導入・構築		×	1	○	4	△	1	△	1	△	1	○	5
情報システム	システム運用	基幹システム運用	セキュリティ対応 インシデント対応	セキュリティ対策（サイバーセキュリティ対応）	SOC	セキュリティオペレーション業務における運用管理		×	1	○	4	△	1	△	1	△	1	○	5
情報システム	システム運用	基幹システム運用	セキュリティ対応 インシデント対応	セキュリティ対策（サイバーセキュリティ対応）	SOC	セキュリティオペレーション業務におけるインシデント対応		×	1	○	4	△	1	△	1	△	1	○	5
情報システム	システム運用	基幹システム運用	基幹システム運用	基幹システム運用	OS管理	OS・プラットフォーム・ミドルウェア等に対するバージョン管理		×	1	△	1	△	1	○	5	×	1	△	1
情報システム	システム運用	基幹システム運用	基幹システム運用	基幹システム運用	アプリケーション管理	基幹システム等のアプリケーションに関するバージョン管理		×	1	△	1	△	1	○	5	×	1	△	1
情報システム	システム運用	基幹システム運用	基幹システム運用	基幹システム運用	クラウドサービス管理	クラウドサービス選定及び利用管理、セキュリティ対策		×	1	△	1	△	1	○	5	×	1	△	1
情報システム	システム運用	インフラ環境運用	インフラ運用	データベース管理	DB機器管理	DB機器等に関するバージョン管理		×	1	△	1	△	1	○	5	×	1	△	1
情報システム	システム運用	インフラ環境運用	インフラ運用	データベース管理	DB構成管理	データマネジメントに必要なDB管理（データ特性に合わせたDB構成管理）		×	1	△	1	△	1	○	5	×	1	△	1
情報システム	システム運用	インフラ環境運用	インフラ運用	データベース管理	DBデータセキュリティ	DB設定及び格納されるデータに対するセキュリティ対策		×	1	△	1	△	1	○	5	×	1	△	1
情報システム	システム運用	インフラ環境運用	インフラ運用	ネットワーク管理	通信環境管理	ファイアウォール設定 プロキシ設定		×	1	△	1	△	1	×	1	○	5	△	1
情報システム	システム運用	インフラ環境運用	インフラ運用	ネットワーク管理	通信環境管理	WAF設定　（WEBサービスセキュリティ対策）		×	1	△	1	△	1	×	1	○	5	△	1
情報システム	システム運用	インフラ環境運用	インフラ運用	ネットワーク管理	通信監視	通信監視（死活監視・パケット監視等）		×	1	△	1	△	1	×	1	○	5	△	1
情報システム	システム運用	インフラ環境運用	インフラ運用	ネットワーク管理	通信監視	通信遮断管理（IPS/IDS機能管理） スレット・インテリジェンス（脅威情報）の対策活用		×	1	△	1	△	1	×	1	○	5	△	1
情報システム	システム運用	ヘルプデスク	ヘルプデスク	ヘルプデスク	ヘルプデスク	インシデント発生時の問合せ窓口 端末・機器異常（インシデント発生以前）の相談窓口		×	1	△	1	○	5	○	4	○	4	○	4
情報システム	システム運用	システム監査	システム監査	システム監査	セキュリティ監査	情報セキュリティ監査、物理的セキュリティ監査		○	1	○	1	○	1	○	1	○	1	○	1
情報システム	システム運用	システム監査	システム監査	システム監査	システム監査	システム監査		○	1	○	1	○	1	△	1	△	1	△	1
情報システム	システム運用	購買調達	購買調達	購買調達	セキュリティ調達管理	取引先選定		△	1	△	1	△	4	○	4	○	4	△	1
情報システム	システム運用	購買調達	購買調達	購買調達	セキュリティ調達管理	製品・サービス調達		△	1	△	1	△	4	○	4	○	4	△	1

図5-5 産業横断 人材定義リファレンス①

5.「セキュリティ統括室」配置に向けた検討



【（ICT分野における）要求知識】○：必須、△：あると良い、×：なくても良い　/　【業務区分】5：業務責任を負う　4：業務責任者を支援・補佐する　3：業務を担当する　2：業務担当者を支援・補佐する　1：業務内容を理解する

図5-6 産業横断 人材定義リファレンス②

【横軸】
人材定義リファレンスでは、セキュリティ領域における役割の一覧を横軸に記しています（IT領域中心）。

サイバーセキュリティを対策のレベルで実行するにはセキュリティ機能だけではなく、構築・運用段階におけるセキュリティが重要です。

統括室は、戦略立案をし、司令塔となる組織を想定しています。
実行段階においては、IT/OT/IoTに関わる全ての関係者が役割分担する必要がありますので、その分担のイメージを「人材定義リファレンス」から読み取ってください。

5.「セキュリティ統括室」配置に向けた検討

- 第一期 産業横断 セキュリティ対策カレンダー ～セキュリティ対策AtoZ～

- セキュリティ対策カレンダーは、人材定義リファレンスに基づき、CISO等を担う方が、自社のセキュリティの取り組みの全体像を、カレンダー形式で把握するために作成しました。

- セキュリティ対策というと、事後のセキュリティインシデント対応に意識が向きがちですが、PDCAサイクルを回す情報セキュリティマネジメントの取り組みと、OODAループで回すセキュリティセキュリティインシデント対応のバランスを取るためのツールとして公開しています。

産業横断 セキュリティ対策カレンダー ～セキュリティ対策AtoZ～

		サイバーセキュリティに関する機能定義　共通項目		AtoZ 共通項目		
主な機能概要	セキュリティ機能定義 最終報告	サイバーセキュリティ対策 機能を実現する業務（例）	スキルセット	月例	定常（日次）業務	インシデント発生時
全体統括管理	サイバーセキュリティ統括	サイバーセキュリティ対策に関する全社的統括		リスクマネジメント委員会 経営会議		
IT戦略	事業戦略 中期計画	コンプライアンス、ガバナンス及びリスクマネジメントの観点に基づくセキュリティ対策		リスクマネジメント委員会 経営会議		
	年次計画	セキュリティ対策に係る実施計画の企画立案 規程・ルールの策定		経営会議	CIO/CISO支援 規程・ルール策定・改定	CIO/CISO支援
	ICT企画 （個別IT企画）	各事業に対するIT導入・構築運用改善計画の企画立案 ガイドライン・マニュアルの策定		IT戦略会議	CIO/CISO支援 ガイドライン・マニュアル改定	インシデント対応判断 （全体）
		ライセンス管理を踏まえた、リプレース計画の企画立案 固定資産管理・ソフトウェア会計管理		セキュリティ対応進捗会議	セキュリティ対応進捗評価	インシデント対応状況評価
システム企画	セキュリティ 実装計画	ユーザビリティの観点に基づく機能改善・実装計画の企画立案 エンドポイント及びUIに関するセキュリティ機能改善計画の策定			システム運用に対するセキュリティ対策評価	インシデント対応状況評価
		システムセキュリティの観点に基づく機能改善・実装計画の企画立案 システム構成に関するセキュリティ機能改善計画の策定			システム・機器等に対するセキュリティ対策評価	インシデント対応状況評価
事業継続	IT-BCP	ICT環境における事業継続計画の策定 サイバーセキュリティ保険の導入検討		リスクマネジメント委員会 CIO/CISO支援	バックアップ体制維持 システム更新対応	システム更新評価
セキュリティ対策	ディザスタリカバリ	災害対策（DR）に関するICT環境改善計画の策定		リスクマネジメント委員会 CIO/CISO支援	災害関連情報収集 災害対策ツール情報収集	
		災害対策及び災害発生時に関する稼働計画の策定				インシデント対応判断 （災害）
	情報セキュリティ マネジメント	情報資産保護活動におけるICT環境改善計画の策定 情報資産の保護基準・保護方法の改善、情報漏洩保険の導入検討		ISMS委員会		
		情報資産保護活動におけるICT運用改善活動の策定 情報資産の棚卸		教育計画策定 インシデント注意喚起		インシデント対応判断 （情報資産）
基幹システム インフラ 構築・実装	セキュリティ対策 導入・開発計画	セキュア構築設計の企画立案 要件定義及基本設計におけるセキュアデザイン		構築PJ セキュリティ対応	構築PJ セキュリティ対応	構築PJ セキュリティ対応
		セキュア運用設計の企画立案 詳細設計及び運用改善におけるセキュアデザイン			セキュリティ対策 運用状況監視	運用PJ セキュリティ対応
		多層防御に基づくセキュア設計管理 ネットワーク及びシステム構成に対するセキュアデザイン			インシデント情報収集	OSIプレイヤー整合性評価
	システムセキュリティ対応	システム構築及びシステム運用のセキュリティ対策分野に関するプロジェクトマネジメント及びプロジェクト運用支援		インシデント対応PJ運営 （緊急対応含む）	インシデント対応PJ運営 （緊急対応含む）	インシデント対応PJ運営 （緊急対応含む）
	セキュリティ製品品質管理	セキュリティ対策関連の製品・サービスに対する評価検証			セキュリティ製品評価 セキュリティサービス評価	導入システム 評価支援
	運用テスト パッチ管理	脆弱性診断（導入時・運用時） パッチ適用時の評価テスト			OS/アプリ/ファームウェアVer管理・パッチ適用、脆弱性診断	OS/アプリ/ファームウェアVer管理・パッチ適用
	セキュリティ 機能改善	全システムに対するパッチ管理及び脆弱性診断に関する計画の企画立案		IT資産管理 パッチ適用情報管理	パッチ情報収集 脆弱性診断	パッチ適用評価支援
		セキュリティ対策関連の製品・サービスの選定及び実装支援			セキュリティ製品評価	セキュリティ製品評価支援
		セキュリティ対策におけるシステム的機能の継続的改善活動			インシデント情報収集 セキュリティ製品情報収集	
権限管理	ID管理 アクセス権管理	ActiveDirectry管理 シングルサインオン管理		ID棚卸	人事異動等対応 外注先アカウント付与	設定変更
		システム、フォルダ等アクセス権管理		アクセス権棚卸	人事異動等対応 外注先アクセス権付与	設定変更
ユーザーサポート	サポート 教育	社内のICTリテラシー向上のためのユーザー支援 リスク対応教育の企画・計画・実施		インシデント注意喚起 教育計画策定	社内連絡窓口 入社社員教育/教育情報収集	レポート作成等 対応収束後研修テーマ修正
セキュリティ対策 （サイバーセキュリティ対応）	CSIRT	コマンダー インシデント発生時の全社対応及びCISO等補佐		各種委員会報告	インシデント対応PJ管理	インシデント対応判断 （サイバーリスク）
		インシデントハンドリング・トリアージ インシデント発生時の初動対応及び収束対応			インシデント対応手順改善	インシデント初動対応
		脅威情報収集、対策情報収集 日常のインシデント情報収集及び社内共有活動		月例レポート作成	情報収集・分析業務 レポート作成等	情報収集・分析業務 レポート作成等
		フォレンジックス 機器の保全、被害拡大抑止、証跡保全活動				フォレンジクス
		トレーニング インシデント対応能力向上に向けた教育の企画・計画・実施		教育計画策定 インシデント注意喚起	インシデント対応トレーニング企画実施	
	SOC	セキュリティオペレーション業務における導入・構築				
		セキュリティオペレーション業務における運用管理		月例レポート作成	監視業務 稼働状況レポート作成等	設定変更
		セキュリティオペレーション業務におけるインシデント対応				インシデント 初動対応
基幹システム運用	OS管理	OS・プラットフォーム・ミドルウェア等に対するバージョン管理		ライセンス管理	OS等Ver管理	OS等Ver管理
	アプリケーション管理	基幹システム等のアプリケーションに関するバージョン管理		ライセンス管理	アプリケーションVer管理	アプリケーションVer管理
	クラウドサービス管理	クラウドサービス選定及び利用管理、セキュリティ対策		クラウドサービス管理	クラウドサービス・サポート情報管理	サービス見直し、データ移管対応等
データベース管理	DB機器管理	DB機器等に関するバージョン管理		ライセンス管理	アプリケーションVer管理 ファームウェアVer管理	アプリケーションVer管理 ファームウェアVer管理
	DB構成管理	データマネジメントに必要なDB管理（データ特性に合わせたDB構成管理）		DB構成管理	DB構成管理	設定変更
	DBデータ セキュリティ	DB設定及び格納されるデータに対するセキュリティ対策		ログ管理	DBセキュリティ改善	設定変更
ネットワーク管理	通信環境管理	ファイアウォール設定 プロキシ設定		セキュリティ製品管理 ログ管理	監視業務 稼働状況レポート作成等	設定変更
		WAF設定　（WEBサービスセキュリティ対策）		ログ管理	監視業務 稼働状況レポート作成等	設定変更
	通信監視	通信監視（死活監視・パケット監視等）		セキュリティ製品管理 ログ管理	監視業務 稼働状況レポート作成等	設定変更
		通信遮断管理（IPS/IDS機能管理） スレット・インテリジェンス（脅威情報）の対策活用		ログ管理	監視業務 稼働状況レポート作成等	設定変更
ヘルプデスク	ヘルプデスク	インシデント発生時の問合せ窓口 端末・機器異常（インシデント発生以前）の相談窓口			社内通報窓口	レポート作成等
システム監査	セキュリティ監査	情報セキュリティ監査、物理的セキュリティ監査		監査役会支援	監査役会支援	リスクマネジメント委員会支援
	システム監査	システム監査		監査役会支援	監査役会支援	リスクマネジメント委員会支援
購買 調達	セキュリティ 調達管理	取引先選定			新規取引先審査	
		製品・サービス調達			購買申請受付対応	

図5-7 産業横断 セキュリティ対策カレンダー ～セキュリティ対策AtoZ～①

5.「セキュリティ統括室」配置に向けた検討

年間スケジュール一覧（例）

年間カレンダー

第１四半期（例：4月～6月）			第２四半期（例：7月～9月）			第３四半期（例：10月～12月）			第４四半期（例：1月～3月）		
方針発表		年次計画進捗確認			年次計画進捗確認 規程改定			年次計画進捗確認	次年度 セキュリティ対策計画	次年度 セキュリティ対策計画	次年度 セキュリティ対策計画 規程改定
		年次計画進捗確認			年次計画進捗確認 ガイドライン改定			年次計画進捗確認	次年度 セキュリティ対策計画	次年度 セキュリティ対策計画	次年度 セキュリティ対策計画 ガイドライン改定
					システム運用におけるKPI評価					システム運用におけるKPI修正	システム運用におけるKPI策定
					システム機能改善計画評価					次年度 システム機能改善計画	次年度 システム機能改善計画
						機能改善計画修正				エンドポイントセキュリティ対策計画	エンドポイントセキュリティ対策計画
方針発表			IT-BCP内部監査	IT-BCP是正措置	IT-BCP訓練計画	IT-BCP訓練			IT-BCP内部監査	IT-BCP是正措置	IT-BCP策定
					防災訓練計画		法定停電対策(例)			（防災訓練計画）	
						防災訓練		法定停電対応			（防災訓練）
方針発表			ISMS内部監査						ISMS内部監査		ISMS更新審査計画
新規入社社員教育				ISMS是正措置		新任者セキュリティ教育				ISMS是正措置	
									次年度 構築PJ 設計支援	次年度 構築PJ 設計支援	次年度 構築PJ 設計支援
運用改善 設計支援			運用改善 設計支援			運用改善 設計支援				次年度 運用PJ 設計	次年度 運用PJ 設計
			運用改善評価			運用改善評価					
		パッチ適用状況確認			パッチ適用状況確認			パッチ適用状況確認			パッチ適用状況確認
		パッチマネジメント運用状況評価		（IT機器棚卸）	パッチマネジメント運用状況評価			パッチマネジメント運用状況評価		IT機器棚卸	パッチマネジメント計画策定
					セキュリティ機能運用評価・製品評価						セキュリティ機能運用改善・製品改善
		エンドポイントセキュリティ対策評価			エンドポイントセキュリティ対策評価			エンドポイントセキュリティ対策評価			エンドポイントセキュリティ対策評価
		人事異動ID管理			人事異動ID管理			人事異動ID管理			新入社員ID管理 人事異動ID管理
		人事異動アクセス権管理			人事異動アクセス権管理			人事異動アクセス権管理			新入社員アクセス権 人事異動アクセス権
新規入社社員教育 ISMS/Pマーク研修	GW明けのマルウェア対策			お盆休み明けのマルウェア対策	稼働状況評価	新任者セキュリティ教育 ISMS/Pマーク研修			正月休み明けのマルウェア対策		次年度 体制計画
					CSIRT稼働状況評価					次年度 CSIRT体制計画	次年度 CSIRT体制計画
					インシデント対応手順改定						インシデント対応手順改定
新規入社社員教育 GW 注意喚起		インシデント対応演習		夏季休業 注意喚起	インシデント対応演習	新任者セキュリティ教育		新年 注意喚起 インシデント対応演習		サイバーセキュリティ月間-イベント	インシデント対応演習
					対象機器の棚卸						対象機器の棚卸
					ライセンス評価						ライセンス評価
					ライセンス評価						ライセンス評価
										次年度 構築PJ 設計支援	次年度 構築PJ 設計支援
					DBセキュリティ設定評価						DBセキュリティ計画
		FW 設定評価			FW 設定評価			FW 設定評価			FW 設定評価
		WAF 設定評価			WAF 設定評価			WAF 設定評価			WAF 設定評価
					稼働状況評価						次年度 体制計画
			内部監査	是正措置					内部監査	是正措置	
会計監査対応	会計監査対応		内部監査	是正措置					内部監査	是正措置	
			取引先監査						取引先監査		
									次年度 調達計画	次年度 調達計画	

図5-8 産業横断 セキュリティ対策カレンダー ～セキュリティ対策AtoZ～②

5.「セキュリティ統括室」配置に向けた検討

- 産業横断 セキュリティオペレーション アウトソーシングガイド

- セキュリティオペレーション アウトソーシングガイドは、人材定義リファレンスに基づき、社内の業務と社外へ委託可能な業務を整理するために作成しました。

- 人材定義リファレンスでは、セキュリティ業務は情報システムに関わる全ての業務において分担されるものと定めています。

- しかしながら昨今のサイバー攻撃に代表される様々なセキュリティインシデントはIT領域という可視化が難しい業務であることから、時に、外部の専門家を招聘する必要もあります。

- そこで、アウトソーシングガイドを通じて、自社で対応する範囲と社外へ委託する範囲を整理する指標として公開しています。

産業横断 セキュリティオペレーション アウトソーシングガイド

		サイバーセキュリティに関する機能定義　共通項目		AtoZ 共通項目		
主な機能概要	セキュリティ機能定義 最終報告	サイバーセキュリティ対策 機能を実現する業務（例）	スキルセット	月例	定常（日次）業務	インシデント発生時
全体統括管理	サイバーセキュリティ統括	サイバーセキュリティ対策に関する全社的統括		リスクマネジメント委員会 経営会議		
IT戦略	事業戦略 中期計画	コンプライアンス、ガバナンス及びリスクマネジメントの観点に基づくセキュリティ対策		リスクマネジメント委員会 経営会議		
	年次計画	セキュリティ対策に係る実施計画の企画立案 規程・ルールの策定		経営会議	CIO/CISO支援 規程・ルール策定・改定	CIO/CISO支援
	ICT企画 （個別IT企画）	各事業に対するIT導入・構築運用改善計画の企画立案 ガイドライン・マニュアルの策定		IT戦略会議	CIO/CISO支援 ガイドライン・マニュアル改定	インシデント対応判断 （全体）
		ライセンス管理を踏まえた、リプレース計画の企画立案 固定資産管理・ソフトウェア会計管理		セキュリティ対応進捗会議	セキュリティ対応進捗評価	インシデント対応状況評価
システム企画	セキュリティ 実装計画	ユーザビリティの観点に基づく機能改善・実装計画の企画立案 エンドポイント及びUIに関するセキュリティ機能改善計画の策定			システム運用に対するセキュリティ対策評価	インシデント対応状況評価
		システムセキュリティの観点に基づく機能改善・実装計画の企画立案 システム構成に関するセキュリティ機能改善計画の策定			システム・機器等に対するセキュリティ対策評価	インシデント対応状況評価
事業継続	IT-BCP	ICT環境における事業継続計画の策定 サイバーセキュリティ保険の導入検討		リスクマネジメント委員会 CIO/CISO支援	バックアップ体制維持 システム更新対応	システム更新評価
セキュリティ対策	ディザスタリカバリ	災害対策（DR）に関するICT環境改善計画の策定		リスクマネジメント委員会 CIO/CISO支援	災害関連情報収集 災害対策ツール情報収集	
		災害対策及び災害発生時に関する稼働計画の策定				インシデント対応判断 （災害）
	情報セキュリティ マネジメント	情報資産保護活動におけるICT環境改善計画の策定 情報資産の保護基準・保護方法の改善、情報漏洩保険の導入検討		ISMS委員会		
		情報資産保護活動におけるICT運用改善活動の策定 情報資産の棚卸		教育計画策定 インシデント注意喚起		インシデント対応判断 （情報資産）
基幹システム インフラ 構築・実装	セキュリティ対策 導入・開発計画	セキュア構築設計の企画立案 要件定義及基本設計におけるセキュアデザイン		構築PJ セキュリティ対応	構築PJ セキュリティ対応	構築PJ セキュリティ対応
		セキュア運用設計の企画立案 詳細設計及び運用改善におけるセキュアデザイン			セキュリティ対策 運用状況監視	運用PJ セキュリティ対応
		多層防御に基づくセキュア設計管理 ネットワーク及びシステム構成に対するセキュアデザイン			インシデント情報収集	OSI7レイヤー整合性評価
	システムセキュリティ対応	システム構築及びシステム運用のセキュリティ対策分野に関するプロジェクトマネジメント及びプロジェクト運用支援		インシデント対応PJ運営 （緊急対応含む）	インシデント対応PJ運営 （緊急対応含む）	インシデント対応PJ運営 （緊急対応含む）
	セキュリティ製品品質管理	セキュリティ対策関連の製品・サービスに対する評価検証			セキュリティ製品評価 セキュリティサービス評価	導入システム 評価支援
	運用テスト パッチ管理	脆弱性診断（導入時・運用時） パッチ適用時の評価テスト			OS/アプリ/ファームウェアVer管理・パッチ適用、脆弱性診断	OS/アプリ/ファームウェアVer管理・パッチ適用
	セキュリティ 機能改善	全システムに対するパッチ管理及び脆弱性診断に関する計画の企画立案		IT資産管理 パッチ適用情報管理	パッチ情報収集 脆弱性診断	パッチ適用評価支援
		セキュリティ対策関連の製品・サービスの選定及び実装支援			セキュリティ製品評価	セキュリティ製品評価支援
		セキュリティ対策におけるシステム的機能の継続的改善活動			インシデント情報収集 セキュリティ製品情報収集	
権限管理	ID管理 アクセス権管理	ActiveDirectry管理 シングルサインオン管理		ID棚卸	人事異動等対応 外注先アカウント付与	設定変更
		システム、フォルダ等アクセス権管理		アクセス権棚卸	人事異動等対応 外注先アクセス権付与	設定変更
ユーザーサポート	サポート 教育	社内のICTリテラシー向上のためのユーザー支援 リスク対応教育の企画・計画・実施		インシデント注意喚起	社内連絡窓口	レポート作成等
セキュリティ対策 （サイバーセキュリティ対応）	CSIRT	コマンダー インシデント発生時の全社対応及びCISO等補佐		各種委員会報告	インシデント対応PJ管理	インシデント対応判断 （サイバーリスク）
		インシデントハンドリング・トリアージ インシデント発生時の初動対応及び収束対応			インシデント対応改善	インシデント初動対応
		脅威情報収集、対策情報収集 日常のインシデント情報収集及び社内共有活動		月例レポート作成	情報収集・分析業務 レポート作成等	情報収集・分析業務 レポート作成等
		フォレンジックス 機器の保全、被害拡大抑止、証跡保全活動				フォレンジクス
		トレーニング インシデント対応能力向上に向けた教育の企画・計画・実施		教育計画策定 インシデント注意喚起	インシデント対応トレーニング企画実施	
	SOC	セキュリティオペレーション業務における導入・構築				
		セキュリティオペレーション業務における運用管理		月例レポート作成	監視業務 稼働状況レポート作成等	設定変更
		セキュリティオペレーション業務におけるインシデント対応				インシデント 初動対応
基幹システム運用	OS管理	OS・プラットフォーム・ミドルウェア等に対するバージョン管理		ライセンス管理	OS等Ver管理	OS等Ver管理
	アプリケーション管理	基幹システム等のアプリケーションに関するバージョン管理		ライセンス管理	アプリケーションVer管理	アプリケーションVer管理
	クラウドサービス管理	クラウドサービス選定及び利用管理、セキュリティ対策		クラウドサービス管理	クラウドサービス・サポート情報管理	サービス見直し、データ移管対応等
データベース管理	DB機器管理	DB機器等に関するバージョン管理		ライセンス管理	アプリケーションVer管理 ファームウェアVer管理	アプリケーションVer管理 ファームウェアVer管理
	DB構成管理	データマネジメントに必要なDB管理（データ特性に合わせたDB構成管理）		DB構成管理	DB構成管理	設定変更
	DBデータ セキュリティ	DB設定及び格納されるデータに対するセキュリティ対策		ログ管理	DBセキュリティ改善	設定変更
ネットワーク管理	通信環境管理	ファイアウォール設定 プロキシ設定		セキュリティ製品管理 ログ管理	監視業務 稼働状況レポート作成等	設定変更
		WAF設定　（WEBサービスセキュリティ対策）		ログ管理	監視業務 稼働状況レポート作成等	設定変更
	通信監視	通信監視（死活監視・パケット監視等）		セキュリティ製品管理 ログ管理	監視業務 稼働状況レポート作成等	設定変更
		通信遮断管理（IPS/IDS機能管理） スレット・インテリジェンス（脅威情報）の対策活用		ログ管理	監視業務 稼働状況レポート作成等	設定変更
ヘルプデスク	ヘルプデスク	インシデント発生時の問合せ窓口 端末・機器異常（インシデント発生以前）の相談窓口			社内通報窓口	レポート作成等
システム監査	セキュリティ監査	情報セキュリティ監査、物理的セキュリティ監査		監査役会支援	監査役会支援	リスクマネジメント委員会支援
	システム監査	システム監査		監査役会支援	監査役会支援	リスクマネジメント委員会支援
購買 調達	セキュリティ 調達管理	取引先選定			新規取引先審査	
		製品・サービス調達			購買申請受付対応	

図5-9 産業横断 セキュリティオペレーション アウトソーシングガイド①

5.「セキュリティ統括室」配置に向けた検討

社内業務（例）			アウトソーシング業務（例）		
管理監督業務（インソース）			アウトソーシング		
情報システム部門（情報システム子会社を含む）		常駐者			
管理者	担当者	技術者派遣 / コンサルタント	構築・運用委託先 インテグレーター	製品・サービス ベンダー	セキュリティ専門事業者
リスクマネジメント委員会／経営会議 セキュリティ計画策定（中期計画）	NISC、IPA、JPCERT/CC等の情報収集 リスク評価・リスク分析	資料作成・調査分析　補助			リスク評価・リスク分析 セキュリティ対策計画策定
経営会議　／　CIO/CISO支援 セキュリティ計画策定（年次計画）	NISC、IPA、JPCERT/CC等の情報収集 リスク評価・リスク分析	資料作成・調査分析　補助			リスク評価・リスク分析 セキュリティ対策計画策定
IT戦略会議　／　CIO/CISO支援 システム単位 セキュリティ計画策定（年次計画）	NISC、IPA、JPCERT/CC等の情報収集 リスク評価・リスク分析	資料作成・調査分析　補助	リスク評価・リスク分析 事業・システム構成に基づく次期システム提案		リスク評価・リスク分析 セキュリティ対応計画策定
セキュリティ対応進捗会議 インシデント対応計画策定	グループ企業内　セキュリティ対策状況の情報収集 リスク評価・リスク分析	資料作成・調査分析　補助	リスク評価・リスク分析 ライセンスの切り替えに基づく次期システム提案		リスク評価・リスク分析 セキュリティ対応計画策定
システム運用プロセスに対するセキュリティ対策計画	システム運用プロセス　セキュリティ対策　要件定義	資料作成・調査分析　補助	可用性に基づくシステム改修提案		人的に起因するセキュリティインシデント対応プランの提案・情報提供
システム・機器等に対するセキュリティ対策計画	システム・機器等セキュリティ対策　要件定義	資料作成・調査分析　補助	機密性・完全性に基づくシステム改修提案		時事的なセキュリティインシデント対策プランの提案・情報提供
リスクマネジメント委員会 CIO/CISO支援	バックアップ体制維持 システム更新対応	（総務部門・経営企画部門との連携に基づく） 事業継続計画策定　補助	システム冗長化　企画立案		リスク評価・リスク分析 BCP／BCM 策定
リスクマネジメント委員会 CIO/CISO支援	災害関連情報収集 災害対策ツール情報収集		システム冗長化　構築 データセンター提供	データセンター提供	リスク評価・リスク分析 災害対策計画策定
インシデント対応判断（災害）	インシデント対応（災害）		システム冗長化　運用 データセンター運用		ディザスタリカバリー体制構築支援 データバックアップ計画策定
ISMS委員会	ISMS委員会事務局	ISMS委員会事務局（支援）	情報資産保護管理体制　構築		リスク評価・リスク分析 ISMS構築策定
教育計画策定・注意喚起 インシデント対応判断(情報資産)	インシデント対応（情報資産）	情報資産管理	情報資産の保護方法の確立	情報保管サービス提供	情報資産保護施策・保護手段の提案
構築PJ セキュリティ対応	構築PJ セキュリティ対応 要件定義、基本設計、詳細設計	設計補助	システム構築　セキュリティ対応 要件定義・基本設計・詳細設計		セキュア構築設計　レビュー
セキュリティ対策 運用状況監視	運用PJ セキュリティ対応 要件定義、基本設計、詳細設計及びレビュー	設計補助	システム運用　セキュリティ対応 要件定義・（基本設計）・詳細設計		セキュア運用設計　レビュー
NISC、IPA、JPCERT/CC等の情報収集 インシデント情報収集	OSI7レイヤー対応　整合性評価 多層防御に基づく基本設計	設計補助	多層防御に基づく詳細設計		多層防御の観点に基づく構成図レビュー
インシデント対応P)運営（緊急対応含む）	インシデント対応P)運営（緊急対応含む）		インシデント対応 構築・運用各プロジェクトへの管理・指導		インシデント対応 実務支援
セキュリティ製品評価 セキュリティサービス評価	既存システムに対する機械的適合性　評価 既存ポリシーに対する運用適合性　評価	製品・サービス評価補助	既存システムとの適合性調査 既存セキュリティポリシーとの適合性調査		
IT資産（有形・無形資産）管理 OS/ミドルウェア/アプリ/ファームウェア等　Ver管理	パッチ適用（実装） テスト環境構築、テスト実施、評価結果報告		構築・運用システム　パッチ適用	パッチ管理サービス提供	脆弱性診断サービス、テスト計画策定支援 サイバー攻撃情報提供、パッチ情報提供
IT資産管理 パッチ管理	パッチ情報収集（JVN／各ベンダー） パッチ適用情報管理	IT資産管理補助 （有形資産・無形資産・ライセンス情報等）	基幹・業務システムごとのシステム機器情報提出 パッチ対応計画の策定、進捗管理		セキュリティパッチ情報提供 セキュリティパッチ評価支援
セキュリティ製品評価	セキュリティ製品情報収集 セキュリティ製品評価		基幹・業務システムごとのセキュリティ製品適合性調査	セキュリティ製品　他社との適合性情報提供 セキュリティサービス　セキュリティ対応	セキュリティ製品評価 セキュリティサービス評価
インシデント情報収集 セキュリティ製品情報収集	インシデント情報収集（ニュース情報等） セキュリティ製品情報収集	インシデント情報管理	基幹・業務システムごとのシステム脆弱性情報収集	セキュリティ製品　脆弱性情報提供 セキュリティサービス　インシデント情報提供	インシデント対応 情報提供 インシデント対応 実務支援
ID棚卸 人事異動等対応・外注先アカウント付与	設定変更	設定変更実務	設定変更実務	シングルサインオン関連　製品・サービス情報提供 多要素認証関連　製品・サービス情報提供	認証におけるセキュリティ対策支援
アクセス権棚卸 人事異動等対応・外注先アクセス権付与	設定変更	設定変更実務	設定変更実務	アクセス権管理　製品・サービス情報提供	認証におけるセキュリティ対策支援
インシデント注意喚起 セキュリティ教育の実施	インシデント注意喚起 社内連絡窓口・レポート作成等	インシデント注意喚起 社内連絡窓口・レポート作成等	ユーザーサポート 研修企画・実施・報告	コールセンターサービス	
各種委員会報告・インシデント対応P)管理 インシデント対応判断（サイバーリスク）	各種委員会報告・インシデント対応P)管理 インシデント対応判断（サイバーリスク）				
インシデント対応改善 インシデント初動対応	インシデント初動対応	インシデント初動対応	インシデントハンドラー・インシデント管理・トリアージ ※日本シーサート協議会「CSIRT人材の定義と確保」参照		インシデントハンドラー・インシデント管理・トリアージ ※日本シーサート協議会「CSIRT人材の定義と確保」参照
月例レポート作成 情報収集・分析業務	情報収集・分析業務・レポート作成等	情報収集・分析業務・レポート作成等	セルフアセスメント・リサーチャー・キュレーター ※日本シーサート協議会「CSIRT人材の定義と確保」参照	脅威情報提供サービス	セルフアセスメント・リサーチャー・キュレーター ※日本シーサート協議会「CSIRT人材の定義と確保」参照
	フォレンジクス	インベスティゲーター	インベスティゲーター・フォレンジックス ※日本シーサート協議会「CSIRT人材の定義と確保」参照		インベスティゲーター・フォレンジックス ※日本シーサート協議会「CSIRT人材の定義と確保」参照
教育計画策定 インシデント注意喚起	インシデント対応トレーニング企画実施 インシデント注意喚起	インシデント対応トレーニング企画実施 インシデント注意喚起	教育・啓発 ※日本シーサート協議会「CSIRT人材の定義と確保」参照	インシデント対応 e-learning プログラム提供	教育・啓発 ※日本シーサート協議会「CSIRT人材の定義と確保」参照
	設計・設置・導入設定	設計・設置・導入設定	導入設計・運用設計・機器設置・ログ設定 ※日本セキュリティオペレーション事業者協議会(ISOG-J)	マネージド SOC サービス	導入設計・運用設計・機器設置・ログ設定 ※日本セキュリティオペレーション事業者協議会(ISOG-J)
監視業務・稼働状況レポート作成等 設定変更	監視業務・稼働状況レポート作成等 設定変更	監視業務・稼働状況レポート作成等 設定変更	ツールサポート、診断と評価、脅威情報収集分析 ※日本セキュリティオペレーション事業者協議会(ISOG-J)	マネージド SOC サービス	ツールサポート、診断と評価、脅威情報収集分析 ※日本セキュリティオペレーション事業者協議会(ISOG-J)
インシデント 初動対応	インシデント初動対応	インシデント初動対応	インシデント＆証拠に対する調査分析 ※日本セキュリティオペレーション事業者協議会(ISOG-J)	マネージド SOC サービス	インシデント＆証拠に対する調査分析 ※日本セキュリティオペレーション事業者協議会(ISOG-J)
ライセンス管理	OS Ver管理	OS Ver管理	OS/ミドルウェア　パッチ対応	OS／ミドルウェア　脆弱性情報　配信	ゼロデイ対応
ライセンス管理	アプリケーションVer管理	アプリケーションVer管理	アプリケーション　パッチ対応	アプリケーション　脆弱性情報　配信	ゼロデイ対応
稼働状況・セキュリティレポート確認	稼働状況・セキュリティレポート確認	稼働状況・セキュリティレポート確認		セキュリティインシデント情報　配信	
ライセンス管理	アプリケーションVer管理 ファームウェアVer管理	アプリケーションVer管理 ファームウェアVer管理	DB機器　パッチ対応	製品　脆弱性情報　配信	ゼロデイ対応
DB構成管理	DB構成管理 設定変更	DB構成管理 設定変更	DB　構成管理		DB選定・構築プラン
運用改善・ログ管理	DBセキュリティ改善 設定変更	DBセキュリティ改善 設定変更	DBセキュリティ対策　計画・実施		DBセキュリティ対策プラン
運用改善・ログ管理	監視業務・稼働状況レポート作成等 設定変更	監視業務・稼働状況レポート作成等 設定変更	ファイアウォール設置　機器監視	製品　脆弱性情報　配信	UTM（IDS/IPS）構成プラン
運用改善・ログ管理	監視業務・稼働状況レポート作成等 設定変更	監視業務・稼働状況レポート作成等 設定変更	WAF　設置、機器監視	アプリケーション　脆弱性情報　配信	UTM（IDS/IPS）設定変更・最適化プラン
運用改善・ログ管理	監視業務・稼働状況レポート作成等 設定変更	監視業務・稼働状況レポート作成等 設定変更	通信機器・通信状態の監視	製品　脆弱性情報　配信	
運用改善・ログ管理	監視業務・稼働状況レポート作成等 設定変更	監視業務・稼働状況レポート作成等 設定変更	IDS/IPSに対するチューニング SOCデータに基づく危機への反映		
	社内通報窓口・レポート作成等	社内通報窓口・レポート作成等			インシデント対応 実務支援
監査役会支援	リスクマネジメント委員会支援				セキュリティ監査　実施
監査役会支援	リスクマネジメント委員会支援				システム監査　実施
新規取引先審査		事務アシスタント		信用調査 情報提供	
購買申請受付対応		事務アシスタント			セキュリティ対策機器・サービス 情報提供

図5-10 産業横断 セキュリティオペレーション アウトソーシングガイド②

5.「セキュリティ統括室」配置に向けた検討

- 「人材定義リファレンス」
  - 第一期の成果物として公開した「産業横断 人材定義リファレンス等 セット」は、複数のシートから構成されています。また、本資料は下記URLより公開されています。
    - https://cyber-risk.or.jp/sansanren/index.html

  - 「産業横断 人材定義リファレンス等 セット」の検討および議論のプロセスについては、第一期最終報告書の別紙として、活動報告を公開しています。
    - https://cyber-risk.or.jp/sansanren/xs_20160914_02_Report_JinzaiTeigiWG_1.0.pdf

- セキュリティ統括室における業務の定義
  - CRIC CSFにおいては、先にも記述した通り、会員企業の多くが「セキュリティ専任組織」または「CSIRT組織」を持ち、サイバー空間における情報のやりとりを積極的に行っているという活動の前提がありました。

  - セキュリティ統括室またはセキュリティ統括機能を定義しようとする場合、本編では、必要とされる「機能」を中心に書いていますが、実際に定義すべきは「業務」であり、「業務」を統合した「役割」の方向での議論と、「業務」を実現するための「作業」、「作業」を担当する「人材像」および「スキル」のの方向の2系統の議論が必要です。

  - CRIC CSFでは、セキュリティ機能を実現する「作業」の重要性を理解しながらも、その「作業」の実施に向けて、社内で担当するのか、外部の専門事業者や専門家に委託するのか等、幅広い視野に立った検討が必要であると考えています。これは、リスクアセスメントを行った後のリスク対応を「移転」させるのかという議論の延長にあるものです。

  - **セキュリティ統括室の設置**または**セキュリティ統括機能の実現**を検討される場合には、まずは自社事業においてリスクとは何を指すのかを明確にした上で、セキュリティの観点から必要な取り組みについて、幅広く検証いただきたいと考えています。また、その参考資料として「産業横断 人材定義リファレンス等 セット」が一助になればと考えております。

6.セキュリティ統括室の機能に関する用語集

6.セキュリティ統括室の機能に関する用語集

- 用語について
  - 方針策定
    - サイバーセキュリティの観点から、各種方針を定めます。
  - 実務
    - サイバーセキュリティ対策の実務を担当します。
  - 支援
    - 事業上必要とされる情報システムに対するサイバーセキュリティ対策を部分的に支援します。
  - 実務支援
    - IT/OT/IoT領域におけるIT利用に対するサイバーセキュリティ対策を支援します。
    - システム企画から導入、運用、監査及び調達先管理・委託先管理におけるセキュリティ相談窓口及び対策検討支援、対策実施状況の確認等に対する実務を支援します。

  - セキュリティ戦略
    - 事業戦略、IT戦略、ITガバナンス等は他の部門部署で検討されていますので、それらをガバナンスとリスクマネジメントの観点から補強する「セキュリティ戦略」を企画・策定します。
  - セキュリティ実務
    - セキュリティ対策の中でも、組織横断的、及びグループ会社を含む会社全体でのセキュリティ対策については、統合的な運用ができる組織・チームが必要となりますので、その役割を担います。
  - セキュリティ対応
    - 事業により国別対応や事業別対応が必要になる取り組みについては、方針を受けた実務レベルでのセキュリティ対策・対応・対処を支援します。
    - また、システム企画・導入・運用等において、全てのビジネスが発注者の事業を守るものではないこともあるため、特に新規導入や法令対応等によるレギュレーション変更については、細心の注意を払い、対応するポイントを整理した上で、社内へ普及することが求められます。
  - 事業分野別セキュリティ対策
    - 大きく3つに分けた領域に対するセキュリティ対策実務を支援します。
      - この3つの分類は、ITとOTのみの2つの場合もあります。
    - 企画から運用にわたる支援は、セキュリティバイデザインの観点から、様々な基準・ガイドラインの適用を支援します。
    - 監査の支援は、監査方法が事業環境やシステム環境に応じて改定されることを支援します。
    - 調達先管理および委託先管理の支援は、調達基準の選定、委託先セキュリティ対策状況確認プロセスを効率化するためのセキュリティ要件の策定および見直し等を指します。

6.セキュリティ統括室の機能に関する用語集

- 用語について
  - 法令対応（国内法対応、各国法対応）
    - サイバーセキュリティ基本法、個人情報保護法、不正アクセス禁止法等、サイバーセキュリティに関わる国内法への対応を検討します。
    - 米国プライバシー法、国土安全保障法等、個人情報保護に関する様々な法令や、サイバーセキュリティに関する指針、EUのNIS指令およびGDPR等、中国サイバーセキュリティ法令について事業領域および展開地域を踏まえた対応を検討します。
  - セキュリティポリシー 策定
    - 法改正や各国法令対応を踏まえたセキュリティポリシーの策定および改訂を行います。
  - リスクマネジメント・事業継続管理（BCM）
    - サイバー攻撃等を含むセキュリティインシデントが事業に与える影響を分析し、リスクマネジメント体制の構築や経営幹部へのレポートラインの構築、財務リスクを踏まえた事前・事後対応を含む広範囲な対策を検討します。
  - 組織体制・業務分掌・業務分掌 策定
    - サイバーセキュリティ対策の責任と権限を明確にし、既存部門・部署の責任の明確化および新規組織による統括体制の運用方針の策定、運用改善を行います。
  - セキュリティ基準・政府等ガイドライン対応
    - 監督官庁からの政令、指針、ガイドライン等を把握し、自社事業への影響を踏まえての対応方針を策定します。

- 参照）JETRO ニューヨークだより
  - 米国等における個人情報保護と利活用に関する近況（2018年2月号）
    - https://www.ipa.go.jp/files/000064473.pdf
  - トランプ政権におけるサイバーセキュリティ政策の現状（2017年9月号）
    - https://www.ipa.go.jp/files/000061964.pdf
  - 米国における個人情報保護に関する取り組みの現状（2015年9月号）
    - https://www.ipa.go.jp/files/000048013.pdf

6.セキュリティ統括室の機能に関する用語集

- 用語について
  - 規程・社則・技術的ガイドライン策定
    - 情報セキュリティ関連規程の整備を行います。
    - システム関連規程に対するセキュリティ面での見直しを行います。
      - 法令対応及び安全管理措置、サイバー攻撃対策等に基づく対策を実装します。
    - 事業活動におけるIT利用に応じた各種ガイドラインの策定、更新を行います。
      - 尚、リスクマネジメント関連規程がある場合には、リスクの定義に、サイバー攻撃等のセキュリティインシデントを定義することも重要です。
  - 構成管理指針策定・アセスメント実施
    - 構成管理を実施するための指針・方針を策定します。
    - 構成管理状況に対するアセスメントの計画・実施・管理者へのフィードバックを行います。
    - OT/IoT領域における構成管理について検証し、指針・方針へ反映させます。
  - 情報共有・情報連携
    - 業種・業界による、セキュリティに関する情報共有活動へ参加します。
    - サプライチェーン先との情報共有体制を検証し、連絡体制・連携体制を構築します。
    - グループ企業全体での情報連携を推進します。
  - インシデント管理・CSIRT活動（SOC 含む）
    - セキュリティインシデント対応体制（CSIRT体制）を構築します。
      - まずはセキュリティインシデント対応の責任者と、PoC（Point of Contact）の配置から進めます。
    - セキュリティインシデント対応の手順を策定し、訓練を実施します。
    - セキュリティオペレーションについて、現在取り扱うログ等から対応範囲を決定します。

6.セキュリティ統括室の機能に関する用語集

- 用語について
  - 新規技術・サービス導入
    - クラウドサービスの導入の際の選定基準の策定を支援します。
    - IoT、AI、RPA等の新規技術を導入する際のリスクアセスメントを支援します。
    - オンプレミスからクラウドサービス等へ移行する際のプロセスを確認し、安全な移行手順の策定を支援します。
    - OT領域に、IT技術を導入する等の環境の変化への対応についてセキュリティ面から支援します。
    - その他、生産性向上や働き方改革等に向けた新たな製品・サービスの導入に対する検証を支援します。
  - データ管理
    - Society5.0に向けて、社内のデータがどのように扱われているかを検証するプロセスを支援します。
    - 国によって取り扱いが異なる様々なデータについて、取り扱いに関する情報収集・注意喚起・ガイドラインの運用等を支援します。
    - 個人情報の取り扱いについて、匿名化による取り扱いや、特定個人情報保護法に対応した取り扱い等の運用を支援します。
    - GDPRに代表されるプライバシー情報の取り扱いについて運用を支援します。

7.組織形態による
セキュリティ統括機能の違い

7. 組織形態によるセキュリティ統括機能の違い

- CRIC CSFにおける議論
  - CRIC CSFに議論では、会員企業の多くが「セキュリティ専任組織」を既に設置していたこともあり、担うべき役割を中心とした議論が行われました。

  - 議論の中では、事業内容により「セキュリティ専任組織」を配置する必要性が強くなく、「情報セキュリティ委員会」が取りまとめるケースや「情報システム部門」がその機能を担うケースもあり、必ずしも専任組織に拘る必要は無いという意見もありました。

  - 現実的な体制のイメージとしては、情報セキュリティ委員会（またはリスクマネジメント委員会）が経営層に対する諮問機関として配置され、情報システム部門またはその部門内にセキュリティグループやチームが配置されると考えられます。

  - CRIC CSF会員企業では、セキュリティ専任組織の配置が当然に行われていると書きましたが、この配置には様々な背景があります。

    1. 事業展開が諸外国に広がり、グローバル対応および各国対応が求められています。
    2. デジタル化を推進していく中で、経営層がセキュリティの重要性を認識しています。
    3. セキュリティインシデントへの対応を効率化・高度化するために専任部署があった方が良いと判断しています。
    4. 情報セキュリティのPDCAサイクルでは、日々の課題に対処するには時間的に制約があります。
    5. デジタルトランスフォーメーションにより、情報システム部門が社内全ての情報システムを管理することが困難になり、セキュリティに関する相談窓口を独立させるためです。
    6. 委員会組織が判断するものは、リスクの中でもクライシスに該当するものであるべきという考えからサイバーリスクへの日常的な対応を専任部署に任せることにしています。
    7. その他、各社の事業環境等による影響を鑑みたためです。

7. 組織形態によるセキュリティ統括機能の違い

- 委員会組織からCSIRT組織や専任組織（セキュリティ統括室）を検討するプロセス
  - 重大なセキュリティインシデントを経験した組織や、監督官庁発行のガイドライン等でCSIRTの必要性を認識した組織から、情報システム部門の1部署としてのCSIRT組織や、社長直轄または委員会配下に、CSIRTを設置することがあります。

  - CSIRTを設置し、様々なセキュリティインシデントに対応していくと、規制・法令対応や、社外活動（政府、省庁、業界団体、関係団体等）等を通じて、その活動範囲が広がっていきます。

  - CSIRT活動が拡大していくと、３つの課題が顕在化します。
    1. CSIRT活動の予算は、どの部門が負担するのか。
    2. CSIRTメンバーの業務定義や業務評価は、どのように実施するべきなのか。
    3. CSIRTが検知するセキュリティインシデントに対して、他部門はどのように連携していくべきなのか。

  - 委員会組織や情報システム部門への諮問組織として運営されるCSIRTは、その重要性が認識されると、組織の役割の見直しが必要となり、責任者の権限をどのレベルに設定すべきなのかというガバナンスの問題に向き合うことになります。

  - 尚、CRIC CSFでは、委員会組織、CSIRT組織、専任組織のメリット・デメリットを踏まえて、組織体制および事業内容に合った体制を選択し構築・運用すること討議・検証しています。

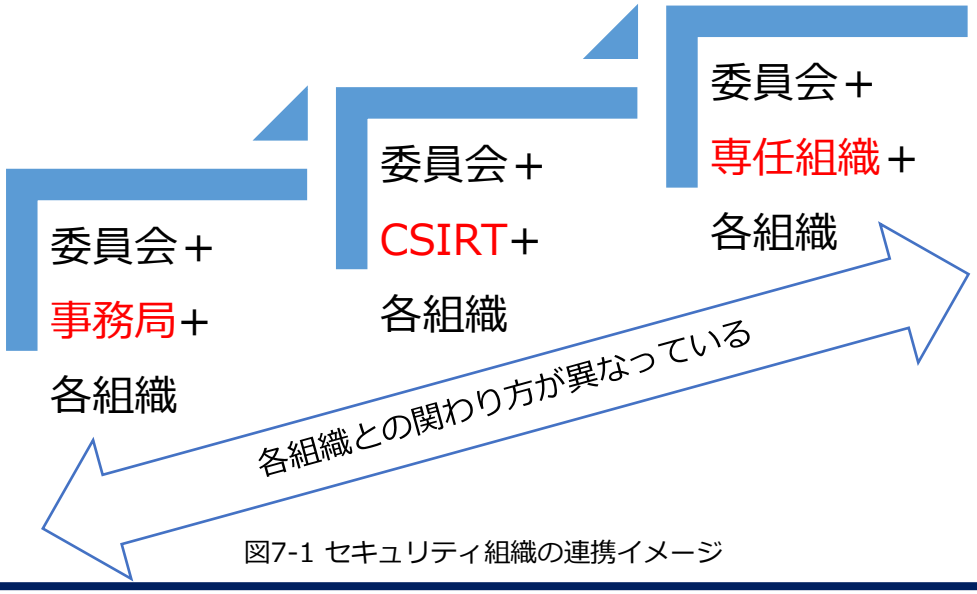


図7-1 セキュリティ組織の連携イメージ

7. 組織形態によるセキュリティ統括機能の違い

- 多くのユーザ企業では既に「リスクマネジメント委員会」や「情報セキュリティ委員会」が設置され、組織横断的なセキュリティ対策が実施されています。この前提に立ち、3つの組織のあり方について検討していきます。

A) 委員会型のリスク対応の特徴は、委員会への報告および委員長の宣言によりリスク対応プロセスが開始されることにあります。委員会メンバーも経営幹部の方々が中心になり、各現場から報告される情報に基づき、対応を審議した上で、各組織へ対応を指示するプロセスが一般的です。

B) CSIRT型のリスク対応の特徴は、サイバー空間におけるリスク対応を主な領域としており、会社の方針によって、情報システムに対するセキュリティ、諸外国動向調査、セキュリティインシデント発生時の対応等が業務に含まれてきます。ただし、多くの企業では、専任組織にしていないことから予算措置やメンバーの選任や評価（配分）等の課題を抱えています。

C) 専任組織型のリスク対応の特徴は、サイバー空間におけるリスク対応を、法令・規制、構成管理、監視・検知、外部連携等様々な活動を通じて社内における情報共有活動を行います。どの領域のセキュリティ業務を行うかは職務分掌で定められ、監査に近い立場か、相談窓口的な立場になるかは会社によって異なります。

- 組織形態に基づく特徴の整理（例）

組織形態	A) 委員会型	B) CSIRT型	C) 専任組織型
特徴	組織横断型の委員会組織として配置	IT領域を中核とした複数メンバーでのチーム体制として配置	セキュリティ対策を企画・実装する体制として配置
根拠（組織の定義）	情報セキュリティ管理方針 情報セキュリティ管理規程	経営層の宣言や指示 情報システム部門責任者の権限	組織規程 職務分掌規程 職務権限規程
組織図への記載	組織図に記載されないことが多い	組織図に記載されないことが多い	組織図に記載される
責任者	セキュリティ管掌取締役 CISO等	情報システム部門責任者 CSIRT長等	専任組織の長
メンバー構成	委員長事務局を中心とした組織横断で選任された社員	責任者より選任された社員および業務委託スタッフ	組織に所属する社員および業務委託スタッフ
予算措置	委員会は予算を持たないため委員会の諮問を踏まえて経営陣が予算措置を行う	CSIRT予算を確保している組織が措置を行う。 又は、情報システム部門の予算から費用負担	専任組織の予算計画に基づき対応

図7-2 組織形態に基づく特徴の整理

7. 組織形態によるセキュリティ統括機能の違い

- A) 委員会型の組織運営から考える「セキュリティ統括機能」
  - 委員会型では、前述の通り、経営層に対する諮問機関であるため、リスクまたはクライシスに対する対応方針を諮問（又は決定）する組織として位置付けられます。
  - よって、CRIC CSFで策定した「セキュリティ統括機能」に対しては、必要なものを取捨選択または社内の各組織の要求に基づき、検討、討議することになります。
  - 事業に影響するセキュリティインシデントが発生した場合には、その対応を進める中心組織となりますが、事業に影響する事案かどうかは、事務局が事前に検討を行うことが一般的です。
  - また、事務局機能は特定の1組織が割り当てられるため、リスク部門、総務部門、経営企画部門等の非IT部門が担当することが多く、セキュリティインシデントによる事業へのインパクトを算定するプロセスは、事務局への報告という形で、情報システム部門又はセキュリティ担当組織が対応します。
  - 企業のデジタル化に伴うIT依存度の高まりに対して、特にセキュリティインシデントによるビジネスの遅延やサイバー攻撃への対処の決定に時間がかかるプロセスを経る傾向にあります。
  - 逆に、セキュリティ戦略の策定に該当する部分については、経営層を巻き込んだ着実な議論を行うことができるため、委員会型で検討すべき範囲を特定することによって、企業全体のセキュリティ対応能力が向上することも考えられます。

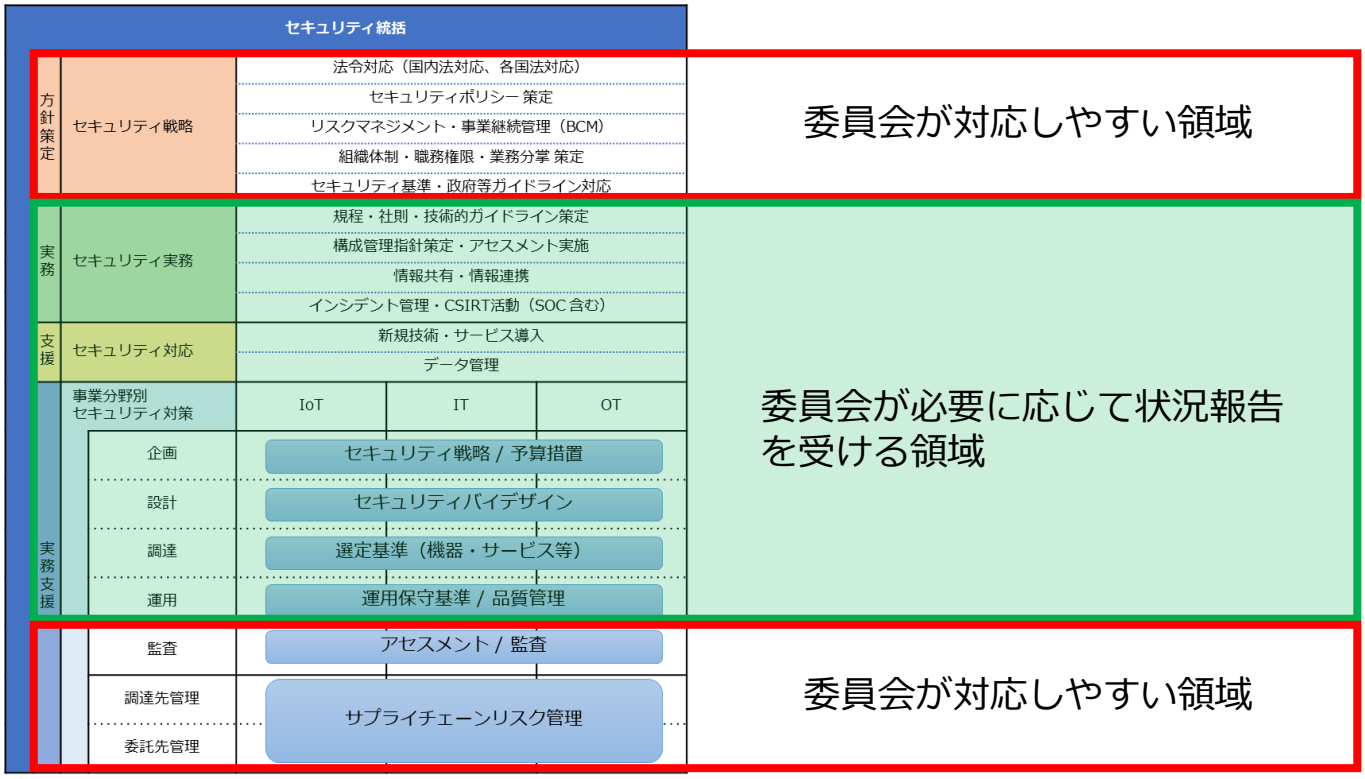


図7-3 セキュリティ統括と委員会型組織

- B) CSIRT型の組織運営から考える「セキュリティ統括機能」
  - CSIRT型では、前述の通り、サイバー空間に関するセキュリティインシデント対応組織として設置されるため、日々取り扱う情報が、自社及びグループ会社並びに取引先等に関する情報システムに関するセキュリティインシデントに集約されていきます。
  - よって、CRIC CSFで策定した「セキュリティ統括機能」に対しては、情報システムに関するもの、電磁的なデータに関するものについて対応を行うことになります。
  - 事業に影響するセキュリティインシデントが発生した場合には、その対応を進めるリスクマネジメント委員会への情報共有・情報連携を行う中心組織ですが、情報システム部門や事務局との連携に基づく事前のコミュニケーションが重要です。
  - 特に、委員会事務局に対する説明については、日常使用する用語・語彙が異なることから、セキュリティインシデント情報をいかにスムースに伝達するかは、事前の訓練等を通じて慣れておく必要があります。
  - 逆に、情報収集や対外活動を重要な役割としているCSIRTだからこそ、既知のリスク対応だけではなく、企業のデジタル化に伴う未知のリスク対応も、最新の情報をもって率先して対応を行うことができる可能性が高い組織です。
  - 課題は、CSIRTを組織体ではなくチーム編成とした場合の稼働管理と予算管理です。

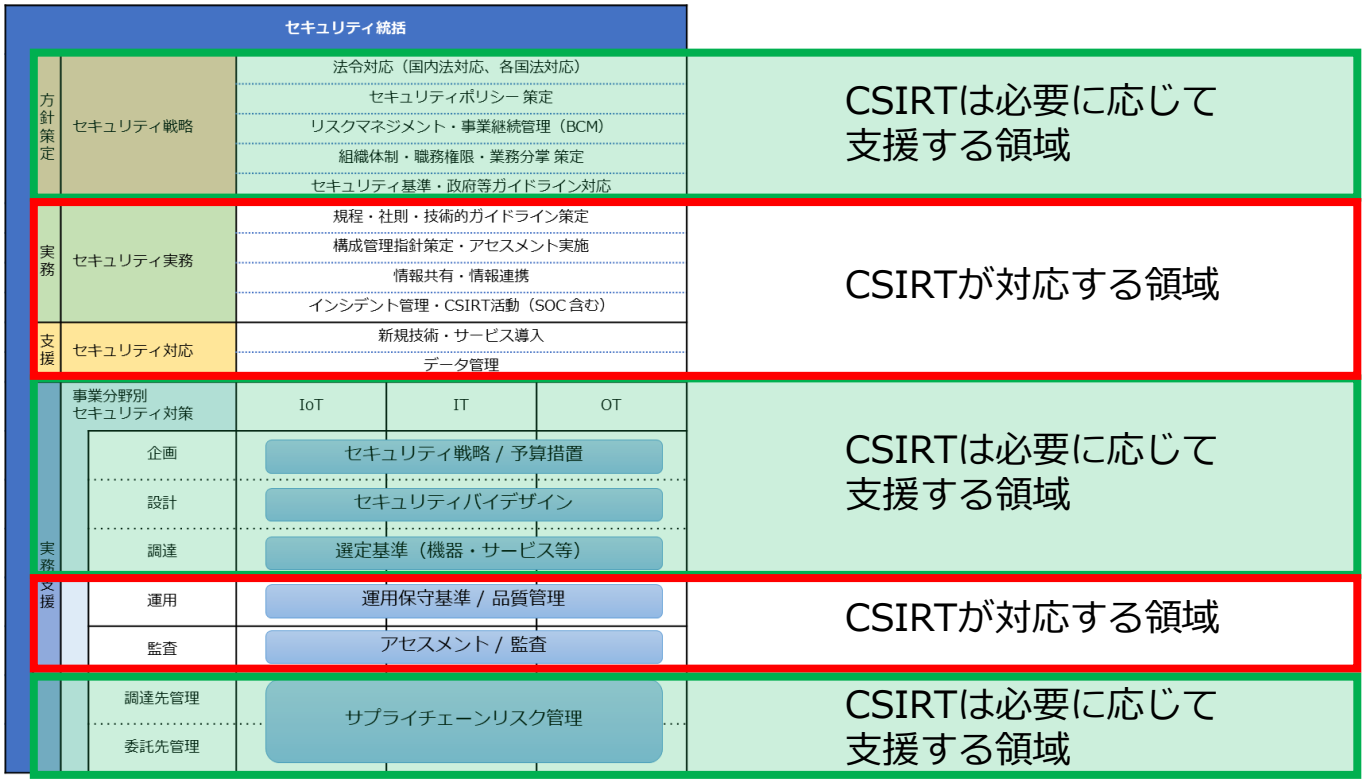


図7-4 セキュリティ統括とCSIRT型組織

- C) 専任組織型の組織運営から考える「セキュリティ統括機能」
  - 専任組織型では、委員会型やCSIRT型の運営を通じて、迅速な対応を行うための人員、スキル、外部との契約関係、予算計画策定等のニーズに基づき発足する傾向にあります。
  - 前述の通り、専任組織は、職務分掌にその役割が明記され、事業継続に必要となるセキュリティ戦略を策定し、必要な予算を確保した上で、自社内の各組織に対してセキュリティ対策の必要性を教育する役割を担います。
  - 業務のデジタル化に伴い、社内のあらゆる組織がITを活用した事業運営を行うことで発生する新たなリスクを、セキュリティインシデント発生前に予測し必要な対策を検討していくことが求められます。尚、セキュリティインシデント対応に関する組織運営プロセスはCSIRT型と変わりありませんが、組織の長として他組織への改善指導を行う点については職務権限に記載されていることもあり、実効性を高めることができます。
  - 専任組織を配置する場合、先にCISO等の任命が行われていることが多く、CISO等の片腕として経営レベルから技術レベルまでの幅広いセキュリティ戦略を考えていく必要があります。また、CSIRT組織における重要な課題であるメンバーの業務管理や評価も、組織体として役割が与えられることで、セキュリティに携わる社員一人一人が安心して業務に就くことができるというメリットが考えられます。

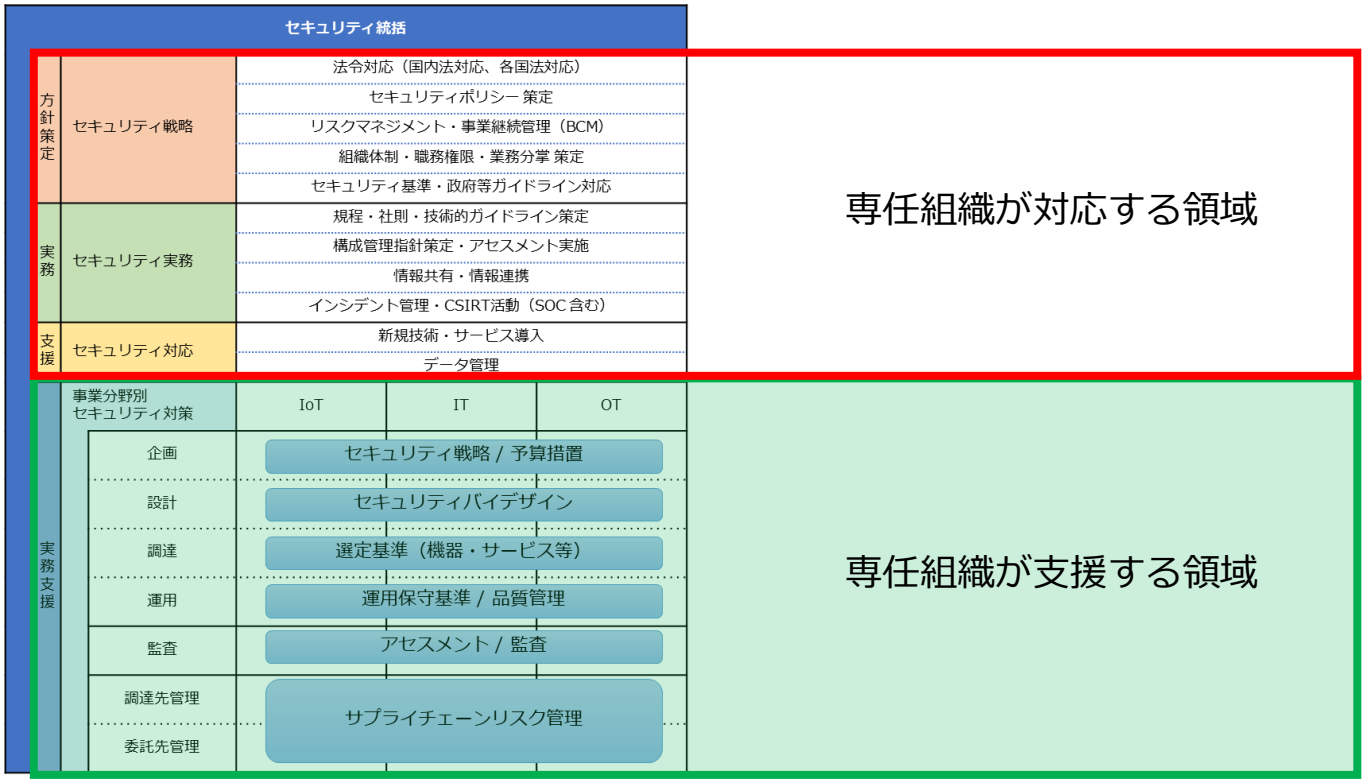


図7-5 セキュリティ統括と専任型組織

- 次に、A) 委員会型から、B) CSIRT型を経て、C) 専任組織型へ移行していく流れについて整理してみます。まずは既存の「委員会組織」の守備範囲の確認です。

1. 「リスクマネジメント委員会」の活動に関する取り決め

1. 想定しているリスクの範囲
   a. 地震・風水害・感染症等と同等のリスクとして、サイバー攻撃等（インシデント）を定義していません。
   b. 地震・風水害・感染症等と同等のリスクとして、サイバー攻撃等（インシデント）を定義しています。
2. 発足や招集のタイミング
   a. 委員会の発足や招集は、被害発生の確認の後、委員長の宣言により行われています。
   b. 委員会の発足や招集は、被害発生確認の有無によらず、セキュリティインシデントの発生（例：震度5強発生や気象予想の警報発令）に伴い、自動的に発足し、委員長の宣言により収束します。
3. 委員会事務局
   a. 委員会事務局は、総務部または経営企画部です。
   b. 委員会事務局は、リスク管理に関する専任組織です。
4. 調達部門の関わり方
   a. リスクマネジメント委員会メンバーには、調達部門又は調達部門管掌の役員はいません。
   b. リスクマネジメント委員会メンバーには、サプライチェーンの観点から参画する、調達部門又は調達部門管掌の役員がいます。

2. 「情報セキュリティ委員会」の活動に関する取り決め

1. 想定するリスク及びセキュリティインシデントの範囲
   a. 情報セキュリティに対する侵害の定義をします。
   b. サイバー攻撃等によるセキュリティインシデントは審議対象となっているか確認します。
   c. システム運用に関するトラブル（通信障害や停電等）は審議対象となっているか確認します。
2. 情報セキュリティ委員会の発足や招集のタイミング
   a. 月例開催します。
   b. 情報セキュリティに対する侵害の発生を確認した後、委員長による招集を行います。
   c. 被害発生前のセキュリティインシデント発生時に、自動的に発足し、委員長の宣言により収束します。
3. 情報セキュリティ監査に関する規定
   a. 監査基準は策定されています。
   b. 監査計画について規定されています。
   c. 監査役、監査部門および被監査部門の連携が規定されています。

7. 組織形態によるセキュリティ統括機能の違い

- 委員会の活動内容の見直し
  - サイバーセキュリティの重要性を認識するようになり、これまでのCIAを重視したセキュリティ対策・管理策の徹底に加えて、様々な攻撃に晒されることによるセキュリティインシデントのケースおよび付随するリスクを想定し、対策を更新、立案していく必要があります。

  - サイバー攻撃の面倒なところは、
    1. 攻撃者が国家レベルであると認定されると、保険会社によっては紛争・騒乱の1つとして保険料支払いを拒む可能性があります。
    2. 攻撃者が個人の場合は一般的な日本企業が損害を被った額を補償することは不可能です。
    3. 更に、攻撃者が国外に居ることが分かった場合は、逮捕・起訴・訴訟等を経て損害賠償請求までの手続きが国内に居る攻撃者によるものとは異なります。

  - 結果として、サイバー攻撃への対処は、事後の対処だけではなく事前の策が重要となるため、上記環境の変化に対する行動を、委員会の場で共有頂く必要があります。

- セキュリティインシデント対応に必要なコミュニケーションに対する理解の醸成
  - CRIC CSF会員企業の多くは、情報セキュリティに関する取り組みに加えて、CSIRTを設置しています。これは、サイバーセキュリティにかかる情報共有活動が日常的に行われるだけではなく、必要とされる情報の取捨選択、自社の情報システム環境に対する検証、セキュリティインシデント発生時の対応等広範な役割が求められているためです。
  - 更に、企業としての説明責任を果たすための十分な情報を確保する必要があるだけではなく、サプライチェーンの重要性に基づく対外活動や調整活動が必要とされるようになっていることもその存在理由です。
  - しかしながら、セキュリティ領域においてやりとりされる情報は、IT従事者にとっても別世界のものと感じられるものであり、それが非IT部門に勤務される方々にとっては未知の領域のことに感じられることもあり、情報共有の中心を担う傍ら、通訳者として正しいコミュニケーションに基づく事業判断、経営判断をサポートする役割をCSIRTや専任組織は担っていくことになります。

7. 組織形態によるセキュリティ統括機能の違い

- セキュリティ統括機能を実現する組織形態は千差万別です
  - CRIC CSFでは、セキュリティ統括室という専任組織を1つのモデルとして提示しています。
  - しかし、これまで記述してきた通り、それぞれの組織体には得意不得意があるため、それぞれの要素を押さえた組織体の連携が重要と考えられます。

  - 委員会型では、参加メンバーが経営層であることから、これからのデジタル化へのニーズと合わせてセキュリティの必要性をインプットしていく必要があります。

  - CSIRT型では、ITおよびセキュリティの専門家組織であるという位置づけから、技術支援を重視するのか、コミュニケーションを重視するのか等、会社が必要とする役割から活動の幅を広げていくことが求められます。

  - 専任組織型では、CRIC CSFでは「セキュリティ統括室」と呼んでいますが、セキュリティに関する活動が日常的になり、組織的になり、その重要性が社内で認識されるようになるための1つの手段として、組織図に明記され、活動予算を持ち、CISOの経営判断を支える役割を与えるモデルを策定しました。

- セキュリティ統括室が無くても良いか
  - セキュリティ統括室が無くても、右図にあるような分業がそれぞれの部門で実施される場合には問題ないと考えられます。
  - 「セキュリティ統括」のモデルでは、想定される最大限の業務を規定しモデル化していますが、その機能1つ1つを、社内の別の組織が担当し、また連携して対処できれば、専任組織にすることは重要ではありません。
  - 今後普及発展するデジタル社会に、どの程度関与していくのかにより、その重要性を判断頂くのが望ましいと考えます。

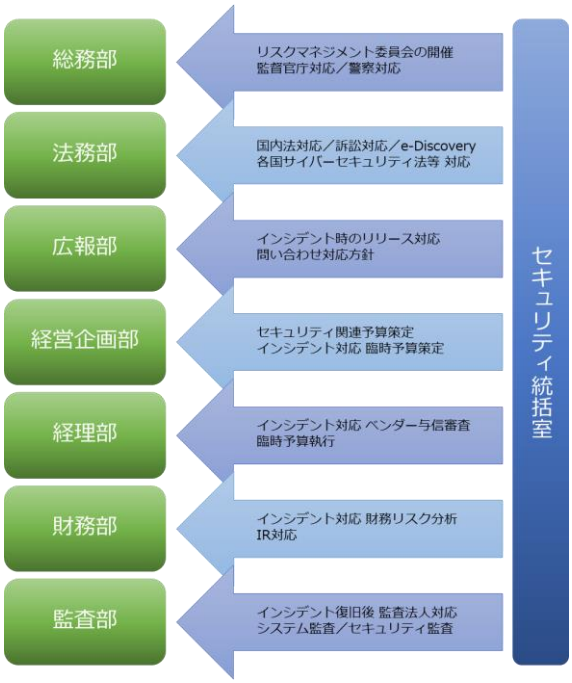


図7-6 セキュリティ統括室の主な支援内容

8.　「サイバーセキュリティは経営課題」の検証

8. 「サイバーセキュリティは経営課題」の検証

- セキュリティ統括室を検討する際に、委員会組織、CSIRT組織、専任組織等の運営形態を検討することになりますが、その前に、そもそも自社にとってのセキュリティの必要性を確認する必要があります。

- CRIC CSFでの議論において、セキュリティ人材（自社の様々な場面で、安全・保全に関わる様々な従業者の方々）の配置および処遇は重要なテーマであり、事業継続やサプライチェーンの観点から必要不可欠な人材であることは認識されていますが、その必要性をどのように定義するのかは継続的なテーマとです。

- そこで本項においては、IT利用の拡大に伴い、必然的に求められてくるセキュリティについて確認をすることとしました。

8-1. デジタルトランスフォーメーション
8-2. IT投資
8-3. 経営判断の原則
8-4. 内部統制とサイバーリスク
8-5. 経団連 サイバーセキュリティ経営宣言
8-6. サイバーセキュリティに関する諸外国における議論と関心
8-7. 各国のセキュリティ関連法令
8-8. セキュリティポリシー

8-1. デジタルトランスフォーメーション

- **デジタルトランスフォーメーションとは**
  - IDC Japan
    - 企業が第3のプラットフォーム技術を利用して、新しい製品やサービス、新しいビジネスモデル、新しい関係を通じて価値を創出し、競争上の優位性を確立することです。
      - 第1プラットフォーム：メインフレーム/端末システム
      - 第2プラットフォーム：クライアント/サーバーシステム
      - 第3プラットフォーム：クラウド・ビッグデータ/アナリティクス・ソーシャル技術・モビリティー
  - ガートナー
    - 企業内のIT利用の3段階

      1.業務プロセスを変革します。

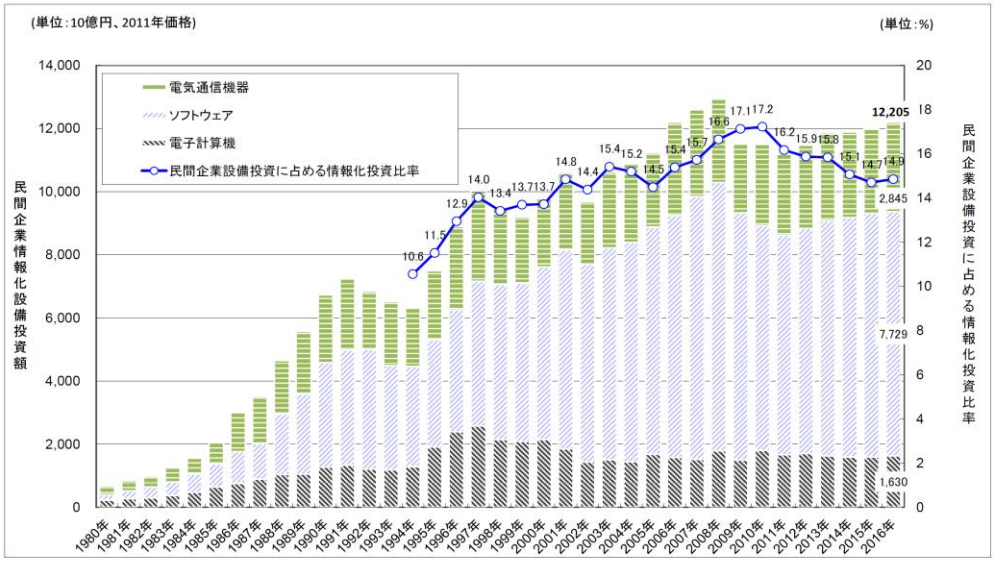
      2.ビジネスと企業、人を結び付けて統合します。

      3.人とモノと企業もしくはビジネスの結び付きが相互作用をもたらします。
    - この第３段階の状態をデジタルビジネスと呼び、デジタルビジネスへの改革プロセスを「デジタルビジネストランスフォーメーション」と定義します。

- **デジタルトランスフォーメーションに向かう組織の課題**
  - これまで閉域でのネットワーク管理に基づく情報セキュリティが実施されてきた中で、組織内の様々な組織が、独自に情報システムを導入することは、「シャドーIT」として否定されてきた経緯があります。
  - 今後、デジタルトランスフォーメーションが進展すると、情報システム部門での集中管理を維持するのか、現場に権限と採用および責任を分担してもらうべきかという議論が行われます。
- **デジタルトランスフォーメーションが普及する過程で、組織に求められる責任の例**
  - 経営層は、デジタル利用に関する**職務分掌**と**職務権限**の設定します。
  - 管理部門には、**文書管理規程**、**機密文書管理規程**、**調達・購買規程**の運用改善をします。
  - 管理職には、**不正競争防止法及び刑法並びに罰則等**に関する理解を深めてもらいます。
  - 従業員全員に、**不正アクセス禁止法および関連法令**の周知徹底します。
  - 情報システム部門には、**構成管理**の徹底と**現業部門とのIT利用の責任範囲**の確認します。
- 参考情報
  - デジタル経営改革のための評価指標（「DX推進指標」）を取りまとめました。
    - https://www.meti.go.jp/press/2019/07/20190731003/20190731003.html

- **ICTの経済分析に関する調査報告書**
  - 平成30年3月　総務省 情報通信国際戦略局 情報通信政策課 情報通信経済室
- 2. 日米の情報化投資の動向
  - 2.1.日本の情報化投資　12.2兆円

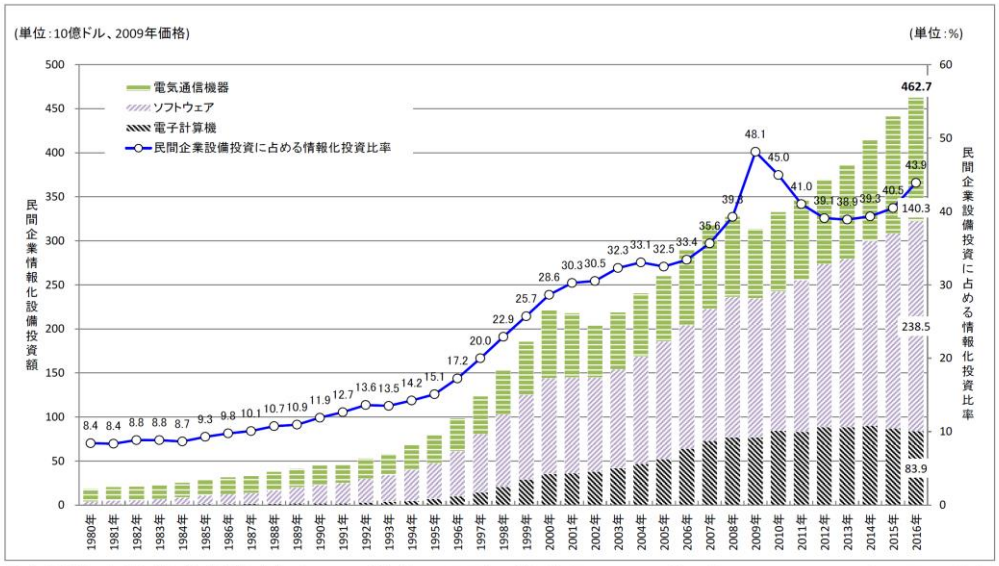
図表 1-9　日本の情報化投資の推移



注)データの詳細については、付属資料 1.情報化投資(日本)を参照されたい。

  - 2.2.米国の情報化投資　4,627億ドル

図表 1-11　米国の情報化投資の動向



注)民間企業設備投資額はこの場合、BEA 資料"Private fixed investment by Type"より"Nonresidential equipment"と"Nonresidential Software"の系列を合算した値とした。設備(Equipment)への投資は入るが、建物(Structures)への投資額は入っていない。
注)データの詳細については、付属資料 2.情報化投資(米国)を参照されたい。

- http://www.soumu.go.jp/johotsusintokei/linkdata/h29_01.pdf

8-3. 経営判断の原則

- **「サイバーセキュリティは経営課題」**
  - 企業によって経営課題が異なることは自明ですが、サイバーセキュリティに関しては、IT利用を推進する中で、共通課題も存在すると考えられています。
  - サイバー空間で事業を行うためには様々な意思決定が行われますが、取締役がリスクを取り判断することの重要性を定めている「経営判断の原則」にも触れてみます。

- **取締役の業務執行**
  - 取締役は業務執行する上で、善管注意義務を負う（民法644条準用）。
  - また、取締役は、法令及び定款並びに株主総会の決議を遵守し、株式会社のため忠実にその職務を行わなければならない（会社法355条）とされる。
  - 会社組織と取締役とは委任関係にあり（会社法330条）雇用関係ではないため、取締役は、善管注意義務違反により会社に損害が発生した場合、その損害を賠償する責任を負うと定められている（会社法423条1項）。

- **経営判断の原則**
  - 意思決定の中身と過程が適正であれば、同判断の結果会社に損害が生じたとしてもこれに対する取締役の責任は問わないとする考え方である。
    - 『新しい取締役会の運営と経営判断原則』長谷川俊明著 2015年、26ページ

- 参考文献
  - 『コーポレートガバナンス・コードの実践』武井一浩編著
  - 『判例法理 経営判断原則』近藤光男著
  - 『新しい取締役会の運営と経営判断原則』長谷川俊明著

8-4. 会社法とサイバーリスク

- **会社法が定めるリスクマネジメントとサイバーリスク**
  - リスクマネジメントの観点から、サイバーリスクへの対応の必要性を確認します。

- **損失の危険の管理（＝リスクマネジメント）**
  - リスクマネジメントに関する取り組みは、多くの企業ではリスクマネジメント規程等において想定すべきリスクが定義されていますが、その中に「サイバー攻撃（社外からのIT環境に対するネガティブなインパクトがある事象）」が定義されているか否かにより、組織の行動様式が変わります。

- **会社法施行規則（平成十八年法務省令第十二号）**（抄）

（業務の適正を確保するための体制）

第百条 法第三百六十二条第四項第六号 に規定する法務省令で定める体制は、当該株式会社における次に掲げる体制とする。

一 当該株式会社の取締役の職務の執行に係る情報の保存及び管理に関する体制

二 当該株式会社の損失の危険の管理に関する規程その他の体制

三 当該株式会社の取締役の職務の執行が効率的に行われることを確保するための体制

四 当該株式会社の使用人の職務の執行が法令及び定款に適合することを確保するための体制

五 次に掲げる体制その他の当該株式会社並びにその親会社及び子会社から成る企業集団における業務の適正を確保するための体制

イ 当該株式会社の子会社の取締役、執行役、業務を執行する社員、法第五百九十八条第一項の職務を行うべき者その他これらの者に相当する者（ハ及び二において「取締役等」という。）の職務の執行に係る事項の当該株式会社への報告に関する体制

ロ 当該株式会社の子会社の損失の危険の管理に関する規程その他の体制

ハ 当該株式会社の子会社の取締役等の職務の執行が効率的に行われることを確保するための体制

二 当該株式会社の子会社の取締役等及び使用人の職務の執行が法令及び定款に適合することを確保するための体制

8-5. 経団連 サイバーセキュリティ経営宣言

- 一般社団法人 日本経済団体連合会では、2018年3月に、サイバーセキュリティ経営宣言を発表し、経団連加盟企業の多くがその宣言に賛同しています。
  - http://www.keidanren.or.jp/policy/2018/018.html

- 経団連 サイバーセキュリティ経営宣言

1. 経営課題としての認識

- 経営者自らが最新情勢への理解を深めることを怠らず、サイバーセキュリティを投資と位置づけて積極的な経営に取り組む。
- 経営者自らが現実を直視してリスクと向き合い、経営の重要課題として認識し、経営者としてのリーダーシップを発揮しつつ、自らの責任で対策に取り組む。

2. 経営方針の策定と意思表明

- 特定・防御だけでなく、検知・対応・復旧も重視した上で、経営方針やセキュリティインシデントからの早期回復に向けたＢＣＰ（事業継続計画）の策定を行う。
- 経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じた取り組みを各種報告書に自主的に記載する等開示に努める。

3. 社内外体制の構築・対策の実施

- 予算・人員等のリソースを十分に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じる。
- 経営・企画管理・技術者・従業員の各層における人材育成と必要な教育を行う。
- 取引先や委託先、諸外国も含めたサプライチェーン対策に努める。

4. 対策を講じた製品・情報システムやサービスの社会への普及

- 製品・情報システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努める。

5. 安心・安全なエコシステムの構築への貢献

- 関係官庁・組織・団体等との連携のもと、各自の積極的な情報提供による情報共有や国内外における対話、人的ネットワーク構築を図る。
- 各種情報を踏まえた対策に関して注意喚起することによって、社会全体のサイバーセキュリティ強化に寄与する。

8-6. サイバーセキュリティに関する諸外国での議論と関心

- 経営リスクとセキュリティインシデント
  - 経営者にとってのリスクは、経営戦略や財務、事業継続やコンプライアンス、事件事故や、マネジメント体制に関するもの等多岐に渡ります。
  - ここでは、主に外的要因によるリスクについて整理してみます。

- リスクマネジメントおよびクライシスマネジメントに関する報告書の例（2018年度）
  - **「グローバルリスク報告書 2019」**
    - http://www3.weforum.org/docs/WEF_GRR2019_%E6%97%A5%E6%9C%AC%E8%AA%9E%E7%89%88.pdf
  - **「企業のリスクマネジメントおよびクライシスマネジメント実態調査」2018年**
    - https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/about-deloitte/news-releases/jp-nr-nr20190214-2.pdf
  - **「Horizon Scan Report 2018」：BCIとBSIによるリスクマネジメントレポート**
    - https://www.bsigroup.com/globalassets/documents/iso-22301/resources/bci_horizon_scan_report_2019_web.pdf
  - **「EYグローバル情報セキュリティサーベイ（GISS）2018-19」**
    - https://www.eyjapan.jp/services/advisory/giss/index.html

8-7. 各国のセキュリティ関連法令

• 代表的な国および地域におけるサイバーセキュリティ法令、プライバシー法令について

国・地域	年月	法令名称（日本語訳）
米国	• 1974年	プライバシー法（連邦行政機関を対象）制定 ※金融、通信、児童の保護、医療分野の個別法 ※民間分野は自主規制
	• 2015年	消費者プライバシー権利章典案　公表
	• 2018年6月	カリフォルニア州消費者プライバシー法　成立
	• 2020年1月	カリフォルニア州消費者プライバシー法　施行予定
EU	• 1995年	EUデータ保護指令（EU指令）採択
	• 2016年	EU一般データ保護規則（GDPR）　採択
	• 2018年5月	EU一般データ保護規則（GDPR）　適用
中国	• 2017年6月	サイバーセキュリティ法　施行
	• 2018年5月	個人情報安全規範　施行
フィリピン	• 2012年	データプライバシー法　施行
マレーシア	• 2013年	個人情報保護法　施行
シンガポール	• 2014年	個人情報保護法（Personal Data Protection Act）　施行
インドネシア	• 2016年	改正電子情報および取引法　施行
ベトナム	• 2019年1月	サイバーセキュリティ法　施行
日本	• 2003年	個人情報保護法　制定
	• 2005年	個人情報保護法　全面施行
	• 2015年	改正個人情報保護法　成立
	• 2017年5月	改正個人情報保護法　全面施行
OECD	• 1980年	プライバシーガイドライン　採択
	• 2013年	プライバシーガイドライン　改定
APEC	• 2004年	APECプライバシーフレームワーク　採択
	• 2011年	越境プライバシールール（CBPR）　採択
	• 2014年	日本のCBPRへの参加承認

図8-1 各国のセキュリティ関連法令

8-8. セキュリティポリシー

- セキュリティポリシーの必要性
  - サプライチェーンの広がりに伴い、サイバーセキュリティに関する取り組みも、サプライチェーン上にある企業間での連携が重要です。それは、攻撃者から見た場合、セキュリティの弱い企業を攻撃することにより、サプライチェーン全体にその影響を与えることが可能であることが知られているからです。
  - また、サプライチェーン上の全ての企業が、同一の情報システムを使用し、同一のセキュリティ水準を設定し維持しているわけではありません。そのような状況において、一定の水準を協力・連携しながら維持するためには、ポリシーレベルでの共有が必要となることがあります。

- 情報セキュリティポリシーの必要性の根拠の例
  - 情報セキュリティポリシーに関するガイドライン
    - 平成１２年７月１８日　情報セキュリティ対策推進会議決定
    - https://www.kantei.go.jp/jp/it/security/taisaku/guideline.html
  - ISO/IEC27001:2013
  - 経済産業省 サイバーセキュリティ経営ガイドライン
  - NIST サイバーセキュリティフレームワーク1.1
  - 総務省 地方公共団体における情報セキュリティポリシーに関するガイドライン（委託先管理）

- セキュリティポリシーの変更を検討するタイミングの例
  1. 監査法人のIT領域に対する監査スタンスの変化
  2. 証券取引所の有価証券報告書の記載に関する要求の変化
  3. 株主のセキュリティへの関心度の変化
  4. 本社、グループ会社の数、事業内容、進出国等の変化
  5. 事業進出先の国別対応と本社対応範囲の変化
  6. クラウド利用の促進等のIT環境の変化
  7. 事業におけるデータ利活用の範囲の変化
  8. その他、情報資産を取り巻く状況において、経営判断が必要になる事象が発生した場合

9. 付録：セキュリティ統括機能に求められる組織形態ごとの注意点

本付録では、セキュリティインシデントを「インシデント」と記載しています。

A-1.CSIRT活動から考える統括室

A-1.「セキュリティ統括室」を配置しない場合のインシデント対応体制の検討

- サイバーセキュリティ統括室の検討
  - サイバーセキュリティ統括室は、責任者の配置及び予算措置を目的として、組織図に記載される形態を指向する考え方です。実際には、サイバーセキュリティに関する実務をCSIRTという形で、部署横断型のチーム体制で運用しているケースも少なくありません。
  - ここでは、CSIRTを前提とする、組織図に記載されない組織体から検討します。

- サイバーセキュリティ体制の検討プロセス

1. CISO等の任命
   1. 取締役会決議により、CISO等の任命を実施します。
2. リスクマネジメント担当部署の配置
   1. CISO等を補佐する体制を検討し、専任部署とするかインシデント対応チームとするかを検討します。
3. CSIRT体制構築の検討
   1. インシデント対応チームの配置を決定した場合は、CSIRT構築プロセスに従い準備を進めます。
   2. CSIRTが配置された場合には、インシデント対応に必要となるモニタリングを開始します。
4. サイバーセキュリティ分野のリスクアセスメント
   1. リスクアセスメントを実施し、CISO等が管轄すべき業務範囲を特定します。
   2. リスク対応を検討し、アセスメント結果に対する対処案を決定します。
   3. 各対処案を管理策として定め、実施計画を策定し、対策を実施します。
5. サイバーセキュリティ分野のトレーニング
   1. CISO等及びインシデント対応チームに対する机上及び実地の訓練を実施します。
   2. インシデント発生時に関係する部署を招集し、全社での対応訓練を実施します。
6. サイバーセキュリティ分野の対策実施状況のアセスメント/監査
   1. サイバーセキュリティ対策の実施状況についてセルフモニタリングを実施します。
   2. 必要に応じて、セキュリティ監査を実施します。

A-1.「セキュリティ統括室」を配置しない場合のインシデント対応体制の検討

- CSIRTは以下のように定義されています。
  - Computer Security Incident Response Team (CSIRT・シーサート) は、発生したインシデントに関する分析、対応を行うだけでなく、セキュリティ品質を向上するため の教育、監査等の活動を行う組織です。その活動の目的は、効果的なインシデント レスポンスを実践し、上記のような事業リスクを軽減することです。
    - CSIRTスタータキット（日本シーサート協議会）

  - インシデントの発生に対応するための体制のことです。
    - サイバーセキュリティ経営ガイドライン2.0（経済産業省）

  - Computer Security Incident Response Team の略称です。セキュリティ上の問題を中心として、監視対象となるネットワーク環境上で何らかの問題が起きていないかどうかを監視すると共に、問題が発生した場合にその原因解析や影響範囲の調査を行う組織です。
    - サイバー攻撃（標的型攻撃）対策防御モデルの解説（総務省）

- セキュリティ統括室の機能とCSIRTの位置づけ
  - セキュリティ統括室の機能を、CSIRT活動の拡大により実装することが、現在の日本企業においては近道と考えられます。
  - この際、CSIRTに求められる情報共有活動の範囲が、技術的なインシデント対応だけではなく、脅威情報（脅威情報と脆弱性情報）共有から、更に国内の法令及びガイドラインへの対応、事業進出先等の法令やガイドライン対応等のプロアクティブな活動に対する必要性を会社として認識する必要があります。
  - 上記、CSIRT活動範囲の拡大を検討される際は、既存のCSIRTに与えられている権限や活動範囲の定義を見直す必要があり、徐々に事業環境に応じて活動範囲を広げていく判断を行うか、全体像を担う担当者1名を配置し、機能分担として実施していくかを検討することが望まれます。
  - サイバーセキュリティが経営課題であるという認識の下、CSIRTとは別に連携するセキュリティ担当組織が経営企画部門等に在籍し、連携すること等も考えられます。

図9-1セキュリティ統括室の機能

A-1.「セキュリティ統括室」を配置しない場合のインシデント対応体制の検討

- CSIRTが取扱う情報
  - CSIRTスタータキット　別紙（１）情報収集と現状把握・問題把握すべき内容（p.22）

大項目	小項目	情報の利用目的
守るべき対策と脅威の把握	社内システム・ネットワーク －運用主管 －重要なシステム －情報資産	CSIRTが取扱うインシデントの定義の判断材料
	過去のインシデント情報 －発生した重大なインシデント －再発傾向にあるインシデント	
	既存のリスク分析結果	
既存のインシデントレスポンス体制	既存のインシデントへの事前対応 －実施主管組織/部門間連携体制/手順	既存インシデントレスポンスの機能面・体制面からの問題点・改善点の洗い出し
	既存のインシデントへの事後対応 －実施主管組織/部門間連携体制/手順	
	既存のセキュリティ向上に向けた取り組み －実施主管組織/部門間連携体制/手順	
	既存のインシデントレスポンスに関する社外組織	インシデントレスポンスに有効な社外連携体制の確立
	インシデントレスポンスに有効な社外連携体制の確立	
既存のセキュリティポリシーおよびセキュリティ関連文書	セキュリティポリシー	インシデントレスポンス時の制約の把握
	災害復旧計画・事業継続性計画	
	セキュリティに関連する制約事項や規制	
	物理セキュリティに関する制限事項	
参考情報	他のCSIRTの情報	CSIRT構築にあたっての参考情報

図9-2 CSIRTが扱う情報

- CSIRTの活動

図9-3　CSIRTの活動

- 出典：JPCERT/CC「コンピュータセキュリティインシデント対応チーム（CSIRT）のためのハンドブック」
  - https://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf

A-1.「セキュリティ統括室」を配置しない場合のインシデント対応体制の検討

- CSIRTの役割と機能
  - CSIRTはチーム構成や部署としての配置等、柔軟な運用体制を想定しています。

- CSIRTの組織体制

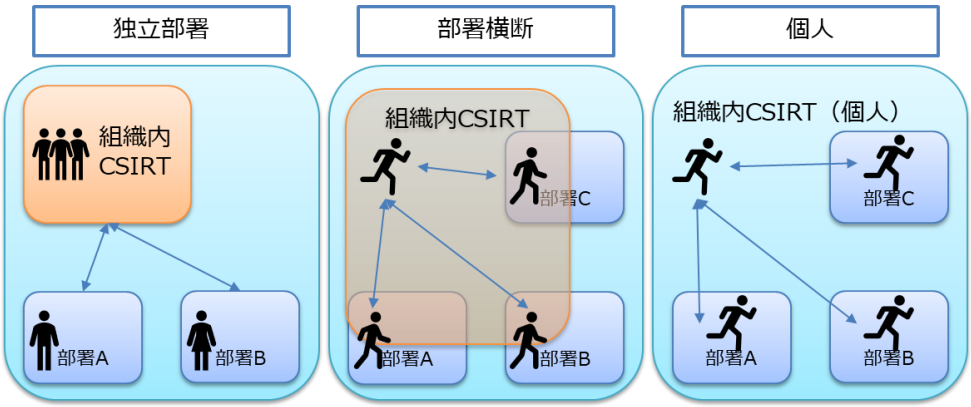


図9-4 CSIRTの組織体制

  - 出典：JPCERT/CC「CSIRTガイド」
    - https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20151126.pdf

- CSIRT活動におけるインシデントマネジメント

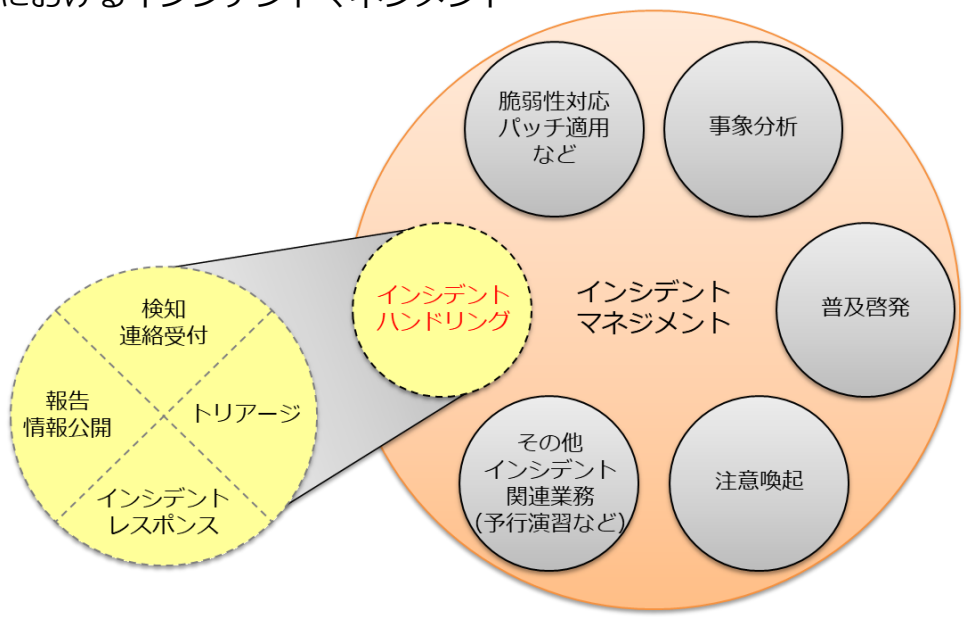


図9-5 CSIRT活動におけるインシデントマネジメント

  - 出典：JPCERT/CC「インシデントハンドリングマニュアル」
    - https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf

A-2.組織と分掌と権限から考える統括室

A-2.「セキュリティ統括室」の配置と権限・分掌

- セキュリティ統括室の配置
  - セキュリティ統括室は、全社リスクマネジメントの観点と事業運営におけるIT活用の両面からサイバーセキュリティの実装を支援するための組織として配置します。
  - サイバーセキュリティは「自衛」が基本であり、情報収集と情報共有・情報連携が重要となることから、社内の調整役と社外との連絡役の2つの役割が求められます。
  - セキュリティ統括室として、組織図に記載される組織体を目指している理由は、責任と権限を明確にし、社内からの相談を受けられる部署として配置し、更に平時と非常時の両フェーズにおいて、適切な戦略策定と予算措置がとれることを目指しています。

- サイバーセキュリティ体制の検討プロセス

1. CISO等の任命
   1. 取締役会決議により、CISO等の任命を実施します。
2. リスクマネジメント担当部署の配置
   1. CISO等を補佐する体制を検討し、専任部署とするかインシデント対応チームとするかを検討します。
3. CSIRT体制構築の検討
   1. インシデント対応チームの配置を決定した場合は、CSIRT構築プロセスに従い準備を進めます。
   2. CSIRTが配置された場合には、インシデント対応に必要となるモニタリングを開始します。
4. サイバーセキュリティ分野のリスクアセスメント
   1. リスクアセスメントを実施し、CISO等が管轄すべき業務範囲を特定します。
   2. リスク対応を検討し、アセスメント結果に対する対処案を決定します。
   3. 各対処案を管理策として定め、実施計画を策定し、対策を実施します。
5. サイバーセキュリティ分野のトレーニング
   1. CISO等及びインシデント対応チームに対する机上及び実地の訓練を実施します。
   2. インシデント発生時に関係する部署を招集し、全社での対応訓練を実施します。
6. サイバーセキュリティ分野の対策実施状況のアセスメント/監査
   1. サイバーセキュリティ対策の実施状況についてセルフモニタリングを実施します。
   2. 必要に応じて、セキュリティ監査を実施します。

- セキュリティ統括室を部門・部署として配置する際の注意点
  - 第一期の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検討は、下記「組織分化」のプロセスを確認することから始まりました。この整理は、各部門・部署が職務分掌に従い業務を遂行し、かつそれぞれのリスクマネジメントを実施していることを確認することも想定していました。
  - セキュリティ統括室を組織体として配置するためには「サイバーセキュリティは経営課題である」という認識に対して、この経営課題を対応できる部署が「分散している」又は「担当部署が無い」ことを確認することが、スタートとなります。

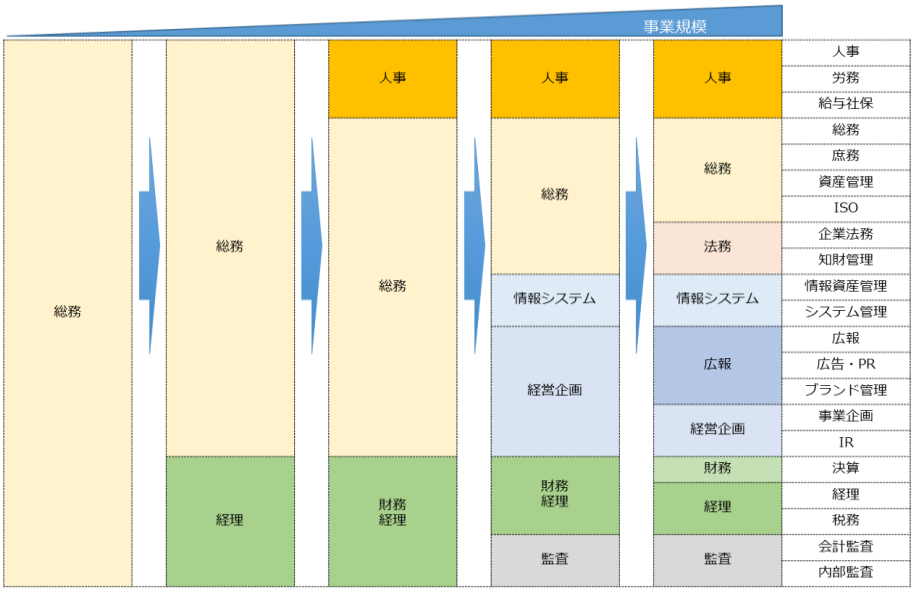


図9-6 ユーザ企業における組織分化プロセス

- セキュリティ統括室を部署として配置する場合には、組織規程に従い、組織の長を配置する必要があります。現在、セキュリティ対策を既存組織内で実施している場合や、適任者が見つからない等で兼務体制（チーム体制：CSIRT体制等）を採用している場合は、無理に組織化することなく、現体制の機能拡大も1つの選択肢となります。
- 「セキュリティ統括の機能（例）」で記載した通り、経営課題として考えた場合に、対策を統合する取り組みを検討する場合には、次ページからの組織の責任者の配置と組織の配置を検討して頂くことになります。

A-2.「セキュリティ統括室」の配置と権限・分掌

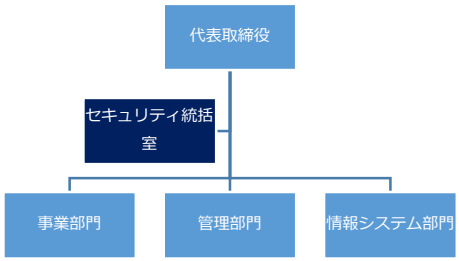
- CISO等の任命
  - セキュリティ統括室の配置と、CISO等の任命は必ずしも一緒に行うものではありません。
  - セキュリティ統括室の役割の1つが、CISO等を支援する位置づけになるため、本頁では、両面から説明しています。

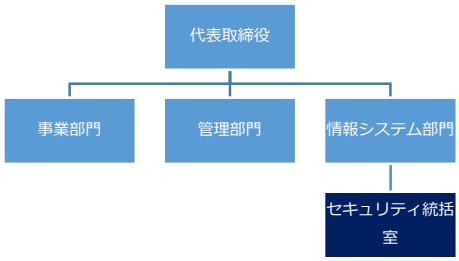
  - セキュリティ統括室長
    - セキュリティ統括室を組織図上に配置するためには、組織の長が必要です。
      - セキュリティ統括室を配置せず、機能のみを実装する場合には、既存組織の長がセキュリティ統括室長と同様の業務を担当します。
  - 管掌取締役
    - 室長のポジションを定めるための管掌取締役又は執行役員（経営幹部）を同時に決めておくことが望ましいです。
    - 全社リスクマネジメントの観点からすると、管理部門を管掌する取締役又は執行役員の方が適任と言えますが、重要情報を取り扱う事業部門の経営幹部の方が就くこともあります。
  - CISO等の役職
    - CISO等と管掌取締役が同一になるケースもありますが、CISO等については必ず取締役である必要はなく、取締役、執行役員、本部長等経営判断に資する役職の方が就任するケースがあります。

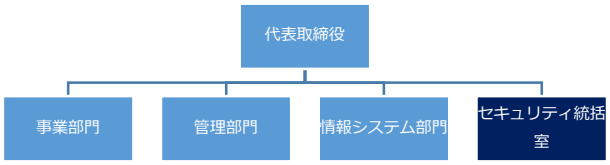
- リスクマネジメント担当部署の配置
  - セキュリティ統括室の配置を行う際には、他のリスクマネジメント機能を担う部署との役割や機能の調整が必要です。
  - 特に、既にCSIRT機能が役割として定められている場合には、CSIRTが提供するインシデント対応の機能との統合又は分離について検討を行います。

A-2.「セキュリティ統括室」の配置と権限・分掌

- セキュリティ統括室を組織図に配置する際の注意点
  - 機能の定義に加えて、会社内の組織構成において、どの位置に配置するかにより、活動の方向性や範囲、権限の持ち方が変わってきます。
  - 以下の例を参考に、位置づけを確認ください。







	特徴	メリット	デメリット
社長直轄型特命組織	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。	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。	ERM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。
情報システム部門の1機能	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。	IT予算の中で活動するため、情報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。	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。
管理部門等との同列組織	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。	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。	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。

図9-7 「セキュリティ統括室」の配置と権限・分掌

A-2.「セキュリティ統括室」の配置と権限・分掌

- セキュリティの観点
  - 経営を行う上ので、リスクをどのように認識しマネジメントしていくのかは、組織の分掌から確認していく必要があります。
  - 組織的セキュリティや物理的セキュリティは総務部門、人的セキュリティは人事部門、技術的セキュリティは情報システム部門といった分掌が定められている場合が多いです。
  - セキュリティ統括人材やセキュリティ統括室は、それらの分掌の範囲を越えて連携するのか、またはそれぞれの分掌に対応し、情報共有・情報連携を行っていくのか、事前に検討しなければなりません。

- セキュリティ統括人材が統括するもの
  - 情報セキュリティに関する活動は日々様々な局面で行われていることを前提として、統括人材の役割を、社内の専門家、社外の専門家とのハブ、経営陣と連携した全体調整役等のイメージを明確にしておく必要があります。
  - そして、統括人材が自由に動けるような環境を用意したいというニーズが生まれた場合に、権限・分掌や予算措置の必要性を認識してから、セキュリティ統括室の配置の是非を検討することが望ましいです。
  - セキュリティ統括人材が見るべき範囲は、PDCAサイクルで管理する部分と、日常的な検知・監視や情報収集に基づく即応体制（OODA）の運用まで幅広く想定していますが、1名で全てを対応することは難しいです。
  - その場合の役割分担を、人材定義リファレンスにより機能定義し、更にアウトソーシングガイドに基づき、外部連携を促進するといった取り組みが重要です。

- セキュリティ統括室と他部門との連携
  - これまでは、多くの業務に対して、IT導入による業務効率化が進められています。これは既存業務プロセスに対するITの導入と言い換えることができます。
  - 今後は、多くの業務が、IT利活用というインフラ（ITでできる事を踏まえて業務設計をするという意）に基づいて、業務効率化と合わせて展開していくことになるのでしょう。
  - このインフラ化により、ITそのもののセキュリティが業務や業績を左右することになるため、セキュリティ統括室はIT利活用（IT依存度）とのバランスを踏まえた意思決定への関与が求められます。

A-2.「セキュリティ統括室」の配置と権限・分掌

- 「調整役」としてのセキュリティ統括室

  - Society5.0の世界では、あらゆるものがインターネット上で繋がる社会を想定しています。
  - この繋がる社会においては、IPアドレスやデータ形式は共有する前提で運用されていることから、特にセキュリティが重視されていない情報システムを利用している場合は、外部からの不正なアクセスに対して、細心の注意を払い管理していく必要があります。

  - 更に、管理が不十分であった場合のリスクとして、先進国では制裁金を含むサイバーセキュリティ法令を施行しており、これまではITリスクとしてだけ考えられていたセキュリティ対策が、進出国等によっては財務リスクに変化してきていることも大きな課題です。
  - そのような事業環境の中で、サイバーセキュリティ対策を抜け漏れなく実施していくための情報を集約し、対策を企画・計画する役割を担うのが、セキュリティ統括室です。

  - 特に、ネットワークインフラは情報システム部門、事業運営上必要な業務システムは事業部門独自で開発される等社内で別々に調達された情報システムが、同一ネットワーク上で稼働している場合は、データのやり取りができているという状況においては、共同でサイバー攻撃対策を実施していく必要があります。
  - そのような状況において、安全に事業を運営していくためのセキュアな環境維持に向けた情報共有を行う取り組みが求められます。

  - 尚、各事業部門が、保有する情報資産（情報システムやデータ）に対するセキュリティ対策を個別に徹底でき、インシデント発生時に即応できる場合には、セキュリティ統括室の配置の意義はさほど強くはありません。地震や火災と同様に対処できれることが重要です。

A-2.「セキュリティ統括室」の配置と権限・分掌

- 「連絡役」としてのセキュリティ統括室

  - サイバーセキュリティ事案は、当分の間は、IT関連ニュースとして取り上げられ、またそれがネット上で共有されることにより、被害を受けた規模・範囲よりも、ネット上に残る記事による追加対応の必要性に迫られることになります。

  - 重要インフラ事業者やブランド力のある企業において、そのようなマイナスイメージの払しょくは事業価値の観点から重要であるだけではなく、サプライチェーン上で繋がるどのポイント（企業）で発生したインシデントも、全てサプライチェーン上の頂点に位置づく企業の社名で共有されていきますので、いくつかの社外連絡が必要となります。

  - ステークホルダーや連携先の例
    - お客様
    - 株主
    - 取引先
    - 監督官庁
    - 警察

  - 更に、サイバーセキュリティ事案は、その全てを検知することも難しく、中には、社外からの通報により発覚することもあります。その連絡体制の構築や、業種・業界での情報共有を行うための、正しいコミュニケーションと適切なリスクコミュニケーションを実施できる組織又は人材の配置は重要となります。

  - このサイバーセキュリティ事案に対するコミュニケーションを、関連する部門・部署で実施することは、情報を集約するという観点、また事業収益や生産性を向上させる観点からすると非効率とも考えられますので、情報の取り扱いについては（広報部が存在するように）、サイバーセキュリティに関する対外的対応を行うことが出来るセキュリティ統括室が重要と考えることもできます。

・セキュリティ統括室の配置に向けた文書体系（例）

1	組織規程 群			
	1-1	取締役会規程		・取締役会の決議事項の定義
		1-1-a.	リスクマネジメント担当取締役規程（参考）	
	1-2	組織規程		・組織体のあり方と分掌・権限の定義
		1-2-a.	組織図	・組織構成
	1-3	委員会運営規程		・委員会組織の運営
		1-3-a.	コンプライアンス委員会規程	・法令遵守
		1-3-b.	リスクマネジメント委員会規程	・リスクの定義、体制の定義
	1-4	職務権限規程		・役職者の権限の定義
		1-4-a.	職務権限一覧	・予算権限の定義
	1-5	職務分掌規程		・牽制関係の定義
		1-5-a.	職務分掌一覧	・各部門・部署の業務範囲
	1-6	監査役会規程		
		1-6-a.	内部監査規程	・内部監査における監査項目の定義
		1-6-b.	情報システム監査規程	・システム監査の実施
2	情報資産管理規程 群			
	2-1.	文書管理規程		・ 情報の定義・ 社内文書の定義
	2-2.	機密文書管理規程		・ 機密文書の定義
	2-3.	インサイダー情報取扱規程		・ インサイダー情報の定義
	2-4.	個人情報保護規程		・ 個人情報保護法対応
	2-5.	規程管理規程		・ 全規程の位置付け及び管理方法の定義
	2-6.	特定個人情報保護規程（又は、取扱い規程）		・特定個人情報の取り扱い / ・委託先管理
3	危機管理規程 群			
	3-1.	危機管理規程 / リスク管理規程		・全社リスクマネジメントの定義
		3-1-a.	事業継続計画	・復旧計画
	3-2.	情報セキュリティ管理規程		・情報セキュリティの定義
	3-3.	情報漏えい対策規程		・情報漏えいの対策の定義
		3-3-a.	個人情報管理規程	・個人情報保護法対応（2-4.と同一）
		3-3-b.	（営業）機密情報 漏えい対策規程	・不正競争防止法対応
		3-3-c.	顧客情報 漏えい対策規程	・顧客情報の漏えいに関する対策
	3-4.	法令違反防止規程		・法令違反行為の防止と処罰等
4	システム管理規程 群			
5	就業規則 群			罰則関連

図9-8 セキュリティ統括室の配置に向けた文書体系