セキュリティ対応組織（SOC/CSIRT）の教科書

～ X.1060 フレームワークの活用 ～

第 3.1 版

2023 年 10 月 17 日

NPO 日本ネットワークセキュリティ協会 （JNSA）

日本セキュリティオペレーション事業者協議会 （ISOG-J）

改版履歴

2016/11/25	初版作成
2017/10/03	第２．０版作成 ・７章、８章の追加 ・別紙に「セキュリティ対応組織成熟度セルフチェックシート」を追加 ・これらに伴う、１章の修正 ・その他、軽微な修正
2018/03/30	第２．１版作成 ・「8.3. 各役割の実行レベル」における、成熟度指標（アウトソース）の改善 ・これに伴う、別紙「セキュリティ対応組織成熟度セルフチェックシート」の修正
2023/2/13	第３．０版作成 ・ITU-T 勧告 X.1060 に伴う全体的な改版
2023/10/17	第３．１版作成 ・サービススコアの説明に「As-Is」「To-Be」の追加 ・マネジメントプロセスとサービスの関連の補足説明の追加 ・5.2.1 のタイトルを「X.1060 の推奨レベルの解釈の仕方」と変更し、説明を追加 ・「8.4 セキュリティ対応組織サービスポートフォリオシート」を追加 ・付録にサービスポートフォリオシートを追加 ・その他頂いたフィードバックの反映や軽微な修正

目次

1. はじめに

企業や組織において、サイバーセキュリティへの対応は避けて通れない状況になって久しい。そのような状況の中、セキュリティ対応する組織を一般的に CSIRT や SOC というような単語で表現するが、現実には企業や組織によって組織形態や取扱う内容は異なっており、一意に定義することは難しい。しかしながら、企業や組織がどのような形であれ、根底にあるセキュリティ対応に関する考え方や、取り組むべき方向性については俯瞰的な視点に立てば共通的なものも少なくない。

本書「セキュリティ対応組織の教科書」は、2016 年に初版が発行され、当時は個別に語られることが多かったインシデント対応やセキュリティ運用、脆弱性診断など、セキュリティに関わる業務を広範に整理し、内製（インソース）か外注（アウトソース）かなども含め、組織としてどのように全体観を持ってサイバーセキュリティ対応を実現するか方向性を示した。その後 2017 年に第 2.0 版（2018 年に第 2.1 版）として改版、組織的なサイバーセキュリティ対応を継続的な営みに昇華できるように成熟度の考え方やそのセルフチェックシートなどを追加し、より体系的な整理を進めた。その結果、経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク」や、情報処理推進機構（IPA）「サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集」などの公的なガイドラインからも参照され、東京 2020 オリンピック・パラリンピック競技大会でのサイバーセキュリティ関係組織の立ち上げ・運営にも役立てられた [1][2]。

さらに、本書の内容は、ITU-T（国際電気通信連合電気通信標準化部門）においても照会され、多くのエッセンスが採用される形で 2021 年に「X.1060（Framework for the creation and operation of a cyber defence centre）」として国際標準として勧告されるに至った。その日本語版は、一般社団法人情報通信技術委員会（TTC）から「JT-X1060（サイバーディフェンスセンターを構築・運用するためのフレームワーク）」 として、国内標準としても公開されている。

X.1060/JT-X1060 は「組織において、ビジネス活動におけるサイバーセキュリティリスクを管理するためのセキュリティサービスを提供する主体」としてのサイバーディフェンスセンターを構築しマネジメントするためのフレームワークを提供している。

ISOG-J では、この国際標準化の流れを踏まえ、国際標準としての「X.1060」の新たな知見を取り込みつつも、より実践的なセキュリティ対応に繋げることができるような実用書

[1] 大西　真樹, 細田　尚史, 中西　克彦, 居林　宏明: “東京 2020 大会を支えるセキュリティオペレーション”, 電子情報通信学会論文誌, Vol. 105 No.8pp. 1035-1041 (2022-8)
[2] 武井　滋紀: “組織体制のリファレンスドキュメント活用における考察”, 電子情報通信学会論文誌, Vol. 105 No.8pp. 1054-1056 (2022-8)

とするべく「セキュリティ対応組織の教科書」を第 3.0 版として改版することとした。先ほど述べたように、企業や組織によってセキュリティ対応組織のあり方は異なるが、それが手探りにならないよう、体系的な知識をもって、より戦略的に組織を作り上げていくための教科書となれば幸いである。

自身の立場に応じて、以下観点を意識いただくと、より多くの気付きが得られる。

経営者、経営幹部

セキュリティ対応を行う上で機能の全体像を把握いただき、それらをインソースで賄うのかアウトソースすべきなのかといった経営的な判断に役立てていただければ幸いである。また、セルフアセスメントの結果から、自組織のセキュリティ対応レベルを把握し、次のセキュリティ対応戦略のヒントとしても活用いただきたい。

マネージャー

セキュリティ対応に必要となる各種サービスを理解いただき、組織内における具体的なサービスの実現や、他部門とのより効果的な連携について検討いただく材料となれば幸いである。セキュリティ専門性が高い業務領域に関しての要員数などもまとめているため、上位者の説得材料の一つとしても活用いただきたい。

現場担当者

自身の立場はそれぞれであろうが（CSIRT に所属していたり、SOC のオペレーターであったり、クラウドや NW システム運用者であったり、脆弱性診断士であったり）、その立場が「セキュリティ対応」という全体像で見たときに、どの位置にあり、どのようなミッションを負っているのかを読み取っていただきたい。今の立場のまま進むのか、将来的には別の道を目指すのかというようなキャリアプランのヒントとしても活用いただきたい。

本書が、各企業、組織におけるセキュリティ対応力の向上に寄与し、そのレベルアップに少しでも貢献できることを願ってやまない。

2. セキュリティ対応組織の存在意義

2.1. 「セキュリティ対応組織」とは

まずは「セキュリティ対応組織」というキーワードについて説明する。このワードは本書の第 1.0 版から用いられているものの、厳密な定義はなされていなかった。例えば、第 1.0 版の「はじめに」ではこのような記述となっている。

> **本書「セキュリティ対応組織の教科書」は、SOC (Security Operation Center)や CSIRT(Computer Security Incident Response Team)と言ったセキュリティ対応組織において、どのような機能や役割、人材が必要となるかについてまとめたものである。**

この記述には CSIRT や SOC を代表例として、セキュリティ業務に関連する組織全般を指し示す言葉として利用したい意図があった。

では、このニュアンスが国際標準勧告「X.1060」の中でどのように表現されているかというと、「CDC (Cyber defence centre)」というワードとして、以下のように定義されている。

> **サイバーディフェンスセンター（CDC）: 組織において、ビジネス活動におけるサイバーセキュリティリスクを管理するためのセキュリティサービスを提供する主体。**

おそらく読者にとっては直感的な理解が難しい説明となっているのではないだろうか。「X.1060/JT-X1060」の内容にもう少し踏み込み、その意味合いを掘り下げていく。「X.1060/JT-X1060」では CDC を以下の概念図[3]を用いて説明している。

[3] 一般社団法人 情報技術委員会(TTC) JT-X1060 サイバーディフェンスセンターを構築・運用するためのフレームワーク
https://www.ttc.or.jp/document_db/information/view_express_entity/1423

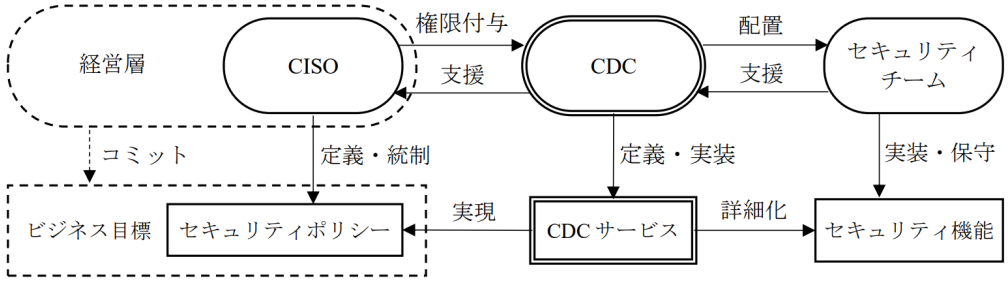


図 1　CDC の運営における関係者とその役割

CDC は CISO の命を受けて、組織のセキュリティポリシーを守ることができるよう、組織として必要な CDC サービス [4]を考え、セキュリティチーム [5]に実装していく役目を持つ存在である。そして、この図が示す重要なポイント 2 点を以下に記載する。

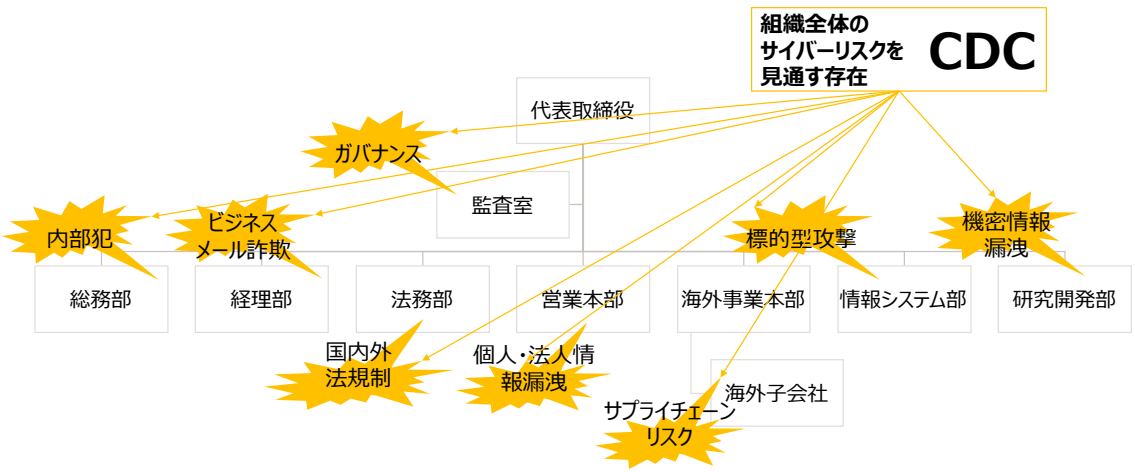


図 1 組織全体に散在するサイバーリスクと CDC

1 点目は、CDC が組織のあらゆるサイバーセキュリティの営みを統括する存在であること。図 1 のようにサイバーリスクが組織全体に散在しているため、俯瞰的な視点から捉え、対処しなければならない。

2 点目は、CDC を新たな組織として立ち上げる必要はないことである。サイバーセキュリティの対策を考え、実装する組織は、その形や規模は様々であれ既に多くの企業においては何らかの形で存在しているはずである。その代表的な例として CSIRT や SOC の存在が挙げられる。

---

[4] CDC サービスは「セキュリティに関する様々な業務」と読み替えると理解しやすい
[5]セキュリティチームは、各部門においてセキュリティに関わる実務をこなしている現場担当を指す

これらの 2 つのポイントから、CDC の概念は、組織内の各種のセキュリティ業務（CDC サービス）を実現している CSIRT や SOC も包括するような広いものを指す。つまり、定義としては本書が「セキュリティ対応組織」と言ってきたものと同等である。よって、本書では引き続き「セキュリティ対応組織」と呼称する。

「セキュリティ対応組織の教科書」は CSIRT や SOC などの業務をボトムアップ的に整理するアプローチでまとめられているのに対して、「X.1060/JT-X1060」は俯瞰的な視点からのアプローチでフレームワーク化がなされている。以降の章においては、俯瞰的な視点も加味する形で、あらためて「セキュリティ対応組織」としてその構築からマネジメントについて全体像を再整理していく。

2.2. セキュリティ対応組織の存在意義

SOC や CSIRT などを含むセキュリティ対応組織を立ち上げる動機は、企業によって異なる。例えば、情報漏えい事故を発端にしたケース、同業他社に倣ったケース、役員の一言で決まったケース、親会社や監督省庁によるプレッシャー、デジタル活用の促進など様々なケースが考えられる。またセキュリティ対応組織の位置づけも、社長直下や独立した部門、ある部門に所属する一担当など、こちらも異なる。

その理由は、各企業の事業戦略やその中のセキュリティ戦略に違いがあり、一言に「セキュリティ対応組織」と言っても様々な形態がある。それゆえ、ノウハウが集約されにくく、体系的に知識を得てセキュリティ対応を実践することが難しくなっている。

一方で、セキュリティ対応組織に共通していることもある。それは、目的が「事業におけるセキュリティリスクの低減と適切な管理」である。そのリスクが表出した事象を「インシデント」と呼ぶが、リスクの低減を実現するために、セキュリティ対応組織が叶えるべきことも、共通して概ね以下の二点になる。

- ✧ **インシデント発生の抑制**
- ✧ **インシデント発生時の被害最小化**

これらの実現があらゆるセキュリティ対応組織に共通する存在意義である。しかしながら、組織でデジタル化が促進され、守るべき対象が広がる中、極端なセキュリティ対策によって生産性や柔軟性が損なわれ、組織のパフォーマンスへの悪影響は避けなければならない。

これまで情報セキュリティでは、「CIA（confidentiality：機密性、integrity：完全性、availability：可用性）」を守るという点に主眼が置かれていたが、組織全体のセキュリティ

という意味では、ビジネスにおける「CPA（creativity：創造性、productivity：生産性、Agility：機敏性)」も守ることも必要になるだろう。

2.3. 本書でのセキュリティ対応組織の位置付け

本書では X.1060/JT-X1060 のサイバーディフェンスセンターをセキュリティ対応組織として呼ぶ。X.1060/JT-X1060 では、組織の位置付けは以下の図で示されている。

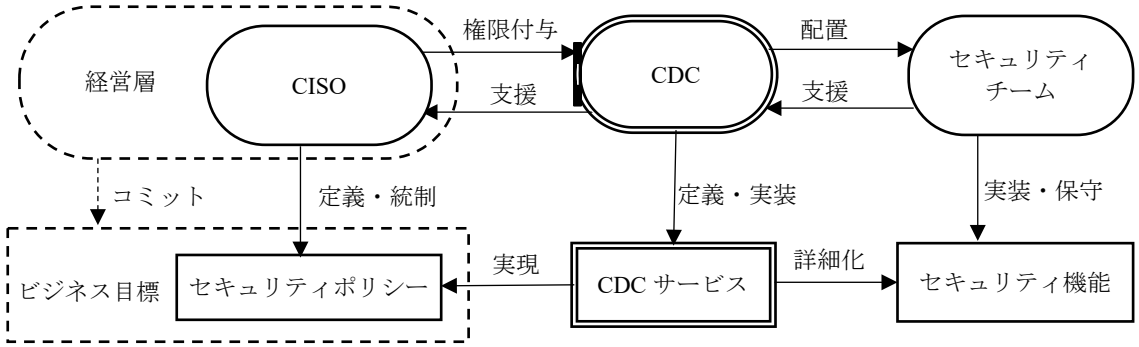


図 2 X.1060/JT-X1060 の CDC の運営における関係者とその役割 [6]

X.1060/JT-X1060 ではシンプルな組織体制を例に図の中央の CDC の構築と運用について定義をしている。

実際にセキュリティ対応組織の設立にあたっては、図の CDC の左側の経営層や CISO がビジネスリスクの一環としてサイバーセキュリティを考え、対応を判断するところから始まる。

[6] 出典：一般社団法人 情報技術委員会(TTC) JT-X1060 サイバーディフェンスセンターを構築・運用するためのフレームワーク、図 1
https://www.ttc.or.jp/document_db/information/view_express_entity/1423

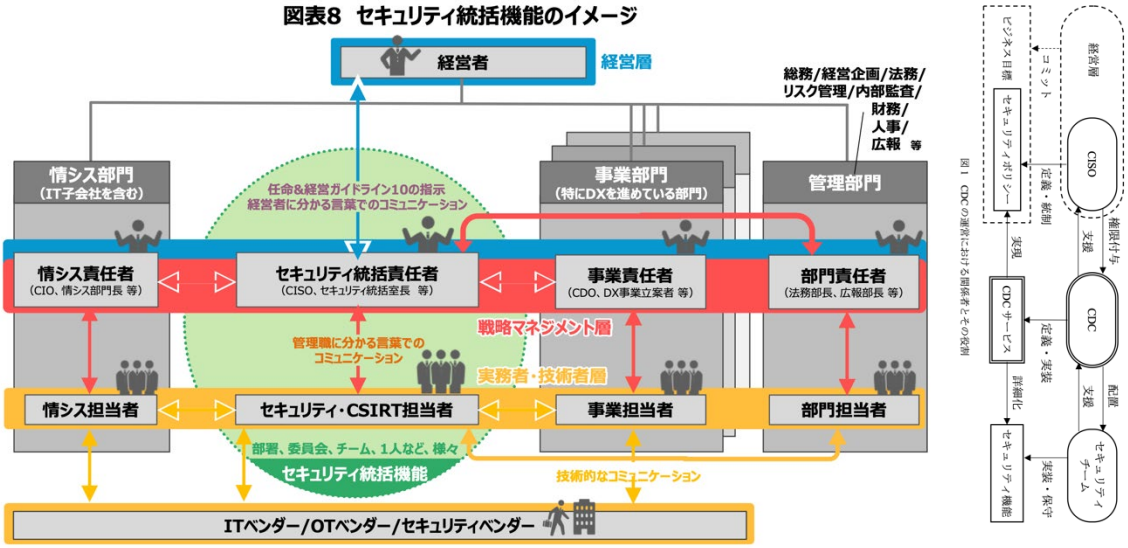


図 3 サイバーセキュリティ経営ガイドラインにおけるセキュリティ統括機能のイメージ [7]

日本における CDC の位置付けと同じように考えられる概念として、経済産業省サイバーセキュリティ経営ガイドライン Ver3.0 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 における図表 8 で示されている、セキュリティ統括(室)のセキュリティ統括機能をイメージすることができる。

経営層はビジネスのリスクの一つとしてサイバーセキュリティを考える。そのために他のリスクと合わせて優先順位を決めてセキュリティの対応を決定する。CISO はセキュリティポリシーとして対応の方針を決めて、実施するための組織としてセキュリティ対応組織を構築し、権限を委譲して各種セキュリティ対応を実施できるようにする。

経営層は、実施したセキュリティ対策がどの程度有効に働いたかを定量的に測定し、その対策が経営に寄与したかを評価する必要もある。どのように経営指標に有効であったかの示し方は JNSA CISO ハンドブックや CISO ダッシュボードが例として挙げられる。

セキュリティ対応組織の設置が決まれば、X.1060/JT-X1060 を参考にサービスを決める、割り当てるなどするが、実際の組織では親会社子会社の関係がある場合や、複数のビジネス部門に SOC や CSIRT が存在するなどのケースも存在する。本書の構築の章においては

---

7 「サイバーセキュリティ経営ガイドライン Ver3.0 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 第２版」（経済産業省）
（https://www.meti.go.jp/policy/netsecurity/mng_guide.html）を加工して作成
図の右側は TTC 標準 JT-X1060 の図１より

X.1060/JT-X1060 のシンプルな組織からスタートする。

図 2 の CDC の右側にセキュリティチームがある。セキュリティチームは CDC で定義したサービスが割り当てられ、実装や保守運用を行うチームである。セキュリティチームの実現に関して、サービスを業務として行うチームの名前を SOC や CSIRT とするのはそれぞれの組織のやり方である。セキュリティ対応組織自体を SOC や CSIRT と呼ぶこともある。

X.1060/JT-X1060 において、セキュリティチームの具体的対応手順については触れられていない。この部分はこれまでにさまざまな業務についてのガイドラインや手順書が提供されている[8]。X.1060/JT-X1060 では企業や組織全体のセキュリティとしてどのようなサービスが存在するかを定義しているだけであり、それぞれの業務や手順はこれまでのガイドラインや手順書などを参考にすることができる。すでに業務や手順を作り上げている組織では、それらを基にどのサービスをすでに実施しているかマッピングをすることができる。

2.4. 実際の例

2.4.1. 日本におけるセキュリティ対応組織の例

日本におけるセキュリティ対応組織は当初、インシデント対応のためのセキュリティ組織として CSIRT の設立や、インシデント監視のために SOC を作るところから始まった。そこから対応すべき製品や予防の観点などの業務範囲が広がってきた。

それぞれの組織や企業において SOC や CSIRT が独自で業務を定義し、それぞれに業務範囲が広がってきたため、組織ごとにそれぞれの形として存在することとなった。そのため、一口に SOC や CSIRT と言っても、何をしているかは組織ごとにバラバラである。重要なことは組織の名前がどうかではなく、何をしているかである。それぞれの企業や組織ではセキュリティ対応組織を通じて、セキュリティで行うべきサービスや業務の全体像を把握する。その上でその組織や企業のセキュリティ対応としては、何を実施し、何を実施していない（業務範囲としていない）かを認識することである。

そのために、X.1060/JT-X1060 や本書を利用することでセキュリティとして行うべきことの全体像について共通的な認識を持ち、共通的な言語として使うことが望ましい。

最近であれば、組織内や社内の業務のシステムの話だけではなく、ビジネス部門が持つビジネスのためのシステムに関しても同様に監視やインシデントの対応を行う必要も出てきた。会社によっては、子会社の吸収や M&A により突如として SOC や CSIRT の範囲が増えるなどにより、複数のセキュリティ対応組織で連携することもある。サプライチ

[8] 国内であれば JPCERT/CC や日本シーサート協議会の各種ドキュメント、海外の FIRST や NIST, ENISA などさまざまなセキュリティに関連したものがある。

ェーンについては海外の支店だけではなく、取引先の企業のセキュリティ対応組織とも連携することもある。

つまりセキュリティ対応組織が当初は組織に 1 つだけ SOC や CSIRT が存在して組織内のセキュリティの対応を行なっていた時代を経て、今では各事業部門のサービスごとに SOC や CSIRT が存在したり、親会社や子会社の関係で SOC や CSIRT が連携したり、サプライチェーンで取引先との関係で SOC や CSIRT と連携したりする必要が出てきている。

それぞれの場所に SOC や CSIRT がすでに存在している状況で、トップダウンでセキュリティを組織的に統括して、それぞれを支援する組織としての CDC、セキュリティ対応組織が必要となっている。

このように、さまざまな組織でのセキュリティのサービスや業務の範囲や組織の構造が複雑になっている。

経済産業省サイバーセキュリティ経営ガイドライン Ver3.0 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 の図表 10、図表 11 においてはどのようにセキュリティ統括機能を類型するのか、組織内への設置の類型を行なっている。[9]

図表10 セキュリティ統括機能の４類型※

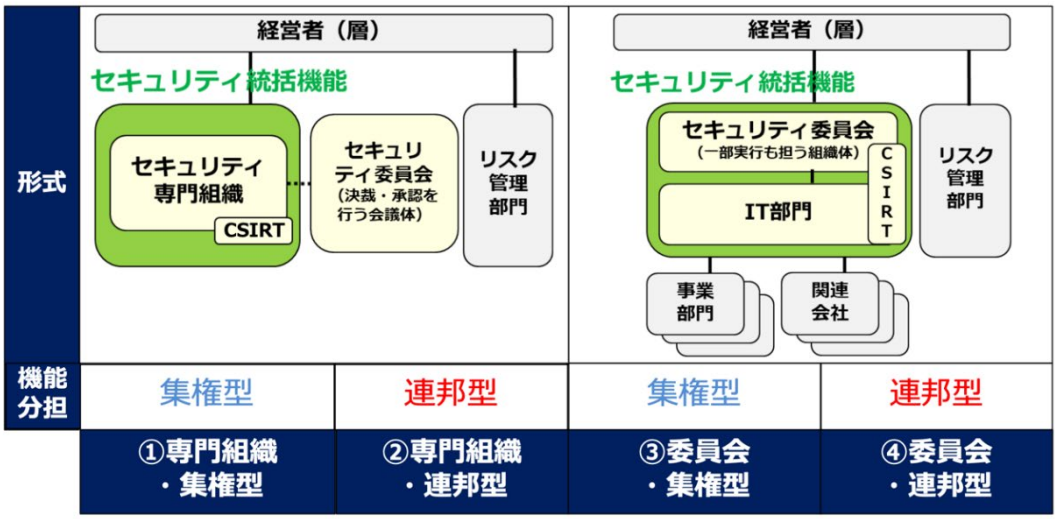


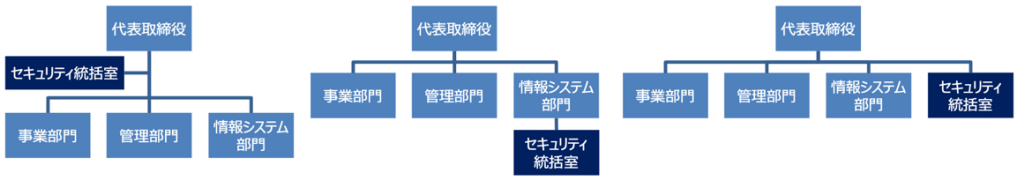
図 4 サイバーセキュリティ経営ガイドライン セキュリティ統括機能の 4 類型の図

[9] 出典：「サイバーセキュリティ経営ガイドライン Ver3.0 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 第２版」（経済産業省）、図表 10（https://www.meti.go.jp/policy/netsecurity/mng_guide.html）

ここではセキュリティ統括機能を４つの類型で整理している。専門組織型と委員会型で大きく分かれる。セキュリティ統括機能を担う適切な部署が存在しない場合は専門組織型として構築し、次の図表 11 でどのように設置をするかを示している。

すでに IT 部門などがセキュリティ統括機能を担っているような場合は委員会型でセキュリティ委員会と IT 部門でセキュリティ統括機能を分担することを示している。

図表11　組織内でのセキュリティ統括機能の位置付けに関する類型※1



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

図 5　サイバーセキュリティ経営ガイドライン　セキュリティ統括機能の位置付けの図 [10]

サイバーセキュリティ経営ガイドライン 付録 F 図表 11 では専門組織として設置する場合に、どのような位置付けにするかのいくつか類型や、それぞれの設置のタイプごとに特徴やメリット・デメリットが示されている。

CDC やセキュリティ統括機能について、どのようなサービスを選択するか、どのような組織の形にするかは組織ごとに異なることを認識し、自分の組織にあった形で構築することとなる。その際には X.1060/JT-X1060 や、サイバーセキュリティ経営ガイドライン Ver3.0 付録 F を参考にすることを推奨する。

[10] 出典：「サイバーセキュリティ経営ガイドライン Ver3.0 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 第２版」（経済産業省）、図表 11
（https://www.meti.go.jp/policy/netsecurity/mng_guide.html）

3. セキュリティ対応組織のサイクル

3.1. サイクルの全体像

企業や組織にとって、セキュリティ対応組織をどのように構築して運用を開始するか、さらにはその運用をどのように継続的に改善を続けるのか、などの課題に対してどのように実践していくのかが重要となっている。このような課題への対応として、本書では X.1060/JT-X1060 のフレームワークの考え方を活用してセキュリティ対応組織の企画、構築から運用までのサイクルを整理する。

X.1060/JT-X1060 のセキュリティ対応組織の構築と運用のフレームワークでは、大きく次の３つのプロセスが定義されている。

- ✧ **構築プロセス**
- ✧ **マネジメントプロセス**
- ✧ **評価プロセス**

これら３つの各プロセスで行うことや、プロセス間の関係を次の図に示す。

X.1060/JT-X1060 では、このように評価プロセスの結果を次の構築プロセスで活用し、継続的に改善するフレームワークを示している。

<table>
<tr><td>サービス
リスト</td><td>サービス
カタログ</td><td>サービス
プロファイル</td><td>サービス
ポートフォリオ</td></tr>
<tr><td colspan="4">構築プロセス</td></tr>
<tr><td colspan="2">評価プロセス</td><td colspan="2">マネジメントプロセス</td></tr>
<tr><td colspan="2">ギャップ分析</td><td>フェーズ</td><td>サイクル</td></tr>
<tr><td colspan="2">アセスメント</td><td>戦略マネジメント</td><td>長期サイクル</td></tr>
<tr><td colspan="2">割り当て</td><td>運用</td><td rowspan="2">短期サイクル</td></tr>
<tr><td colspan="2">推奨レベル</td><td>対応</td></tr>
</table>

図 6 サイバーディフェンスセンターを構築・運用するためのフレームワーク [11]

[11] 出典：一般社団法人 情報技術委員会(TTC) JT-X1060 サイバーディフェンスセンターを構築・運用するためのフレームワーク、図 2
https://www.ttc.or.jp/document_db/information/view_express_entity/1423

これまでの「セキュリティ対応組織の教科書」の第 2.1 版と比べると、２点大きな改版がある。１点目は構築時のプロセスとしてサービスリスト、サービスカタログ、サービスプロファイル、サービスポートフォリオといった概念が追加され、その概念が構築や評価のプロセスにおける中心的な管理項目として利用されるようになった。２点目は評価プロセスがより明示的となった。これまでは実行サイクルとして見直しがあったが、プロセスとして明示され、継続的に改善するために評価ができるようなフレームワークとなっている。

第 2.1 版で示されていた実行サイクルは、マネジメントプロセスとして X.1060/JT-X1060 に取り込まれている。

本書においては、構築プロセスに関連した記述は後述の「3.2 セキュリティ対応組織の構築」に記載する。マネジメントプロセスに関連した記述は「3.3 セキュリティ対応組織のマネジメント」に記載する。評価プロセスに関連した記述は「3.4 セキュリティ対応組織の評価」に記載する。

3.2. セキュリティ対応組織の構築

3.2.1. 構築プロセスの全体像

本書では X.1060/JT-X1060 をベースとして構築プロセスの全体像を説明する。X.1060/JT-X1060 ではセキュリティ対応組織を構築するプロセスとしては、大きく３つのフェーズで定義されている。

- ✧ **フェーズ１：サービスカタログを作成（何をするのかを決める）**
- ✧ **フェーズ２：サービスプロファイルを作成（誰がやるのかを決める）**
- ✧ **フェーズ３：サービスポートフォリオを作成（到達目標を決める）**

これらの３つのフェーズの関係を表す全体像を次の図に示す。

X.1060/JT-X1060 では一般的なサービスリストを基に各フェーズを順次実施することでセキュリティ対応組織を構築していくことを示している。

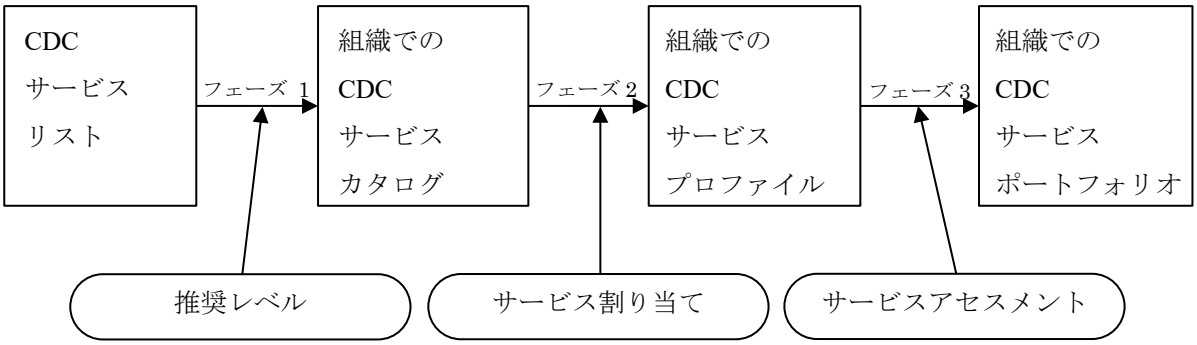


図 7 X.1060/JT-X1060 の CDC サービスの立ち上げフェーズ [12]

この３つのフェーズを実施することにより、最終的にサービスポートフォリオが作成できる。具体的なポートフォリオの例として、X.1060/JT-X1060 ではサービスポートフォリオまでを網羅したサービスマトリクスを以下のように示している。

サービス	推奨レベル	サービス 割り当て	サービススコア	
			現状 (As-Is)	あるべき姿 (To-Be)
サービス 1	ベーシック	インソース(AB 部門)	3	5
サービス 2	スタンダード	アウトソース(Z-MSSP)	2	4
サービス 3	アドバンスド	未割り当て	1	2

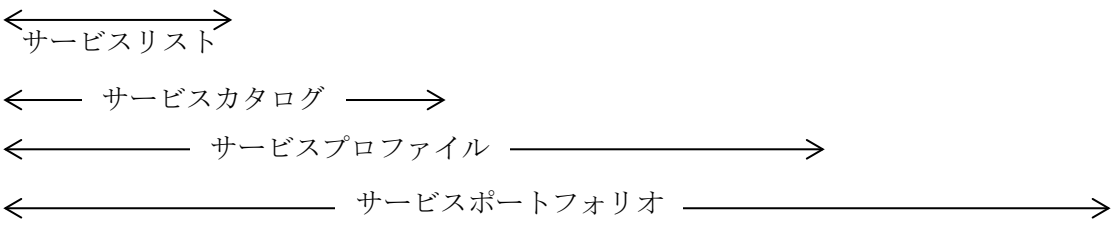


図 8 CDC のサービスマトリクス [13]

以下にそれぞれのフェーズの内容を示す。それぞれのフェーズにてサービスポートフォリオまでを網羅したサービスマトリクスに記入を行うことで、構築時のサービスポートフォリオとしてまとまった形となる。

---

[12] 出典：一般社団法人 情報技術委員会(TTC) JT-X1060 サイバーディフェンスセンターを構築・運用するためのフレームワーク、図 3
https://www.ttc.or.jp/document_db/information/view_express_entity/1423
[13] 出典：同上、図 4

3.2.2. サービスカタログの作成

構築プロセスのフェーズ 1 で作成されるサービスカタログは、後述の「5 セキュリティ対応組織のサービス」で示されるサービスリストと組織ごとに決めた推奨レベル（詳細は 5.2 サービスの推奨レベル）を用いて、どのサービスをどの程度の推奨度で実施するかを決めたものである。

第 2.1 版では 9 つの機能と 54 の役割として定義していたが、X.1060/JT-X1060 では 9 つのカテゴリーと 64 のサービスとして定義している。今後は X.1060/JT-X1060 に倣いカテゴリーとサービスと呼称する。

ベストプラクティスとして示される X.1060/JT-X1060 のサービスリストからサービスを選択するが、業種業態によっては適合するサービスが存在しないかもしれない。その場合は必要と思われるサービスを独自に定義する。

カテゴリーとサービスについては「4 セキュリティ対応組織のカテゴリー」、「5 セキュリティ対応組織のサービス」に詳細を記載する。推奨レベルの考え方や適用については後述の「5.2 サービスの推奨レベル」にて示す。

表 1 カテゴリーとサービス

9 カテゴリー	64 サービス	
A. CDC の戦略マネジメント	A1 ~ A13	13 サービス
B. 即時分析	B1 ~ B4	4 サービス
C. 深掘分析	C1 ~ C4	4 サービス
D. インシデント対応	D1 ~ D7	7 サービス
E. 診断と評価	E1 ~ E9	9 サービス
F. 脅威情報の収集および分析と評価	F1 ~ F5	5 サービス
G. CDC プラットフォームの開発・保守	G1 ~ G13	13 サービス
H. 内部不正対応支援	H1 ~ H2	2 サービス
I. 外部組織との積極的連携	I1 ~ I7	7 サービス

↓

表 2 サービスの選択（64 サービス中 22 サービスを選択した例）

9 カテゴリー	64 サービス	
A. CDC の戦略マネジメント	A1 ~ A9	9 サービス
B. 即時分析		4 サービス

C. 深掘分析	未選択(サービスを持たない)	
D. インシデント対応	D1	1 サービス
E. 診断と評価	E1 ~ E7	7 サービス
F. 脅威情報の収集および分析と評価	未選択(サービスを持たない)	
G. CDC プラットフォームの開発・保守	G1 ~ G4	4 サービス
H. 内部不正対応支援	未選択(サービスを持たない)	
I. 外部組織との積極的連携	I1 ~ I7	7 サービス

この例に基づいて選択したサービスの推奨レベルを判断して、サービスマトリクスに記入すると以下のようになる。ページの都合上、いくつかは中略してある。

表 3 サービスマトリクスへサービスカタログの記入

サービス	推奨レベル	サービス割り当て	サービススコア	
			現状 (As-Is)	あるべき姿 (To-Be)
サービス A1	必須			
(中略、A2-9)				
サービス B1	必須			
(中略、B2-4)				
サービス D1	必須			
サービス E1	推奨			
(中略、E2-7)				
サービス G1	必須			
(中略、G2-4)				
サービス I1	必須			
(中略、I2-7)				

3.2.3. サービスプロファイルの作成

構築プロセスのフェーズ 2 で作成されるサービスプロファイルは、サービスカタログで実施するとしたそれぞれのサービスについては、内部で実施するか外部で実施するか、あるいはハイブリッドで実施するかを決めたものである。それぞれのサービスがどこのチームや部署、あるいは外部委託先で実施するかを決めたものとなる。

サービスの割り当てについて、内部で実現するか外部で実現するかの考え方は第 2.1 版のものと同様である。

サービスの割り当てについては後述の「6.2 セキュリティ対応における役割分担の考え方」

にて示す。

前述の例に引き続きどの組織でサービスを実施するか判断してサービスマトリクスに記入すると以下のようになる。ページの都合上、いくつかは中略してある。

表 4 サービスマトリクスへのサービスプロファイルの記入

サービス	推奨レベル	サービス割り当て	サービススコア	
			現状 (As-Is)	あるべき姿 (To-Be)
サービス A1	必須	社内 CSIRT		
(中略、A2-9)				
サービス B1	必須	社内 SOC		
(中略、B2-4)				
サービス D1	必須	外部委託		
サービス E1	推奨	外部委託		
(中略、E2-7)				
サービス G1	必須	社内情シス部門		
(中略、G2-4)				
サービス I1	必須	社内 CSIRT		
(中略、I2-7)				

3.2.4. サービスポートフォリオの作成

構築プロセスのフェーズ 3 で作成されるサービスポートフォリオは、サービスプロファイルで割り当てられたそれぞれのサービスについて、現状どの程度のレベルで実施しているか、今後どのレベルになりたいかといったアセスメントを行ったものである。

このサービスポートフォリオは第 2.1 版では成熟度として定義していたものである。X.1060 の策定の際に、スコアの付け方が第三者の審査などによるものではなくセルフアセスメントで実施することや、スコアの扱いが内部での評価で利用するものであるため、アセスメントとして扱うこととなった。評価の軸や定義自体はそのままであるので、引き続き同様に活用されたい。

アセスメントについては後述の「8.セキュリティ対応組織のアセスメント」にて示す。また、表中のサービススコアの「現状(As-Is)」と「あるべき姿(To-Be)」のスコアの数字については「8.3 各サービスの実行レベル」にて示している。

前述の例に引き続きアセスメントの結果をマトリクスに記入すると以下のようになる。ページの都合上、いくつかは中略してある。ここまで記入をすると、どのサービスをどのような推奨レベルで選択して実施するか、どこに割り当てられたか、「現状」のスコアと目標とする「あるべき姿」のスコアが見えるようになる。

表 5 サービスマトリクスへのサービスポートフォリオの記入

サービス	推奨レベル	サービス割り当て	サービススコア	
			現状 (As-Is)	あるべき姿 (To-Be)
サービス A1	必須	社内 CSIRT	3	5
(中略、A2-9)				
サービス B1	必須	社内 SOC	2	4
(中略、B2-4)				
サービス D1	必須	外部委託	4	5
サービス E1	推奨	外部委託	4	5
(中略、E2-7)				
サービス G1	必須	社内情シス部門	3	5
(中略、G2-4)				
サービス I1	必須	社内 CSIRT	4	5
(中略、I2-7)				

3.3. セキュリティ対応組織のマネジメント

3.3.1. マネジメントプロセスの全体像

本書では X.1060/JT-X1060 をベースとしてマネジメントプロセスを説明する。

セキュリティ対応組織の詳細なカテゴリーやサービスを列挙する前に、SOC や CSIRT を含むセキュリティ対応組織を実働させる大枠の実行サイクル、マネジメントプロセスについてイメージを持っていただきたい。具体的には、大きく 3 つの工程を 2 種類のサイクルで回していく必要がある。

X.1060/JT-X1060 ではマネジメントプロセスを以下の図で示している。これまで第 2.1 版では「導入」としていた部分が「戦略マネジメント」に変化している。以後、X.1060/JT-X1060 に倣い「戦略マネジメント」と表記する。日本においては元々「戦略マネジメント層」とした言葉で定義されている部分とマッピングできるところである。

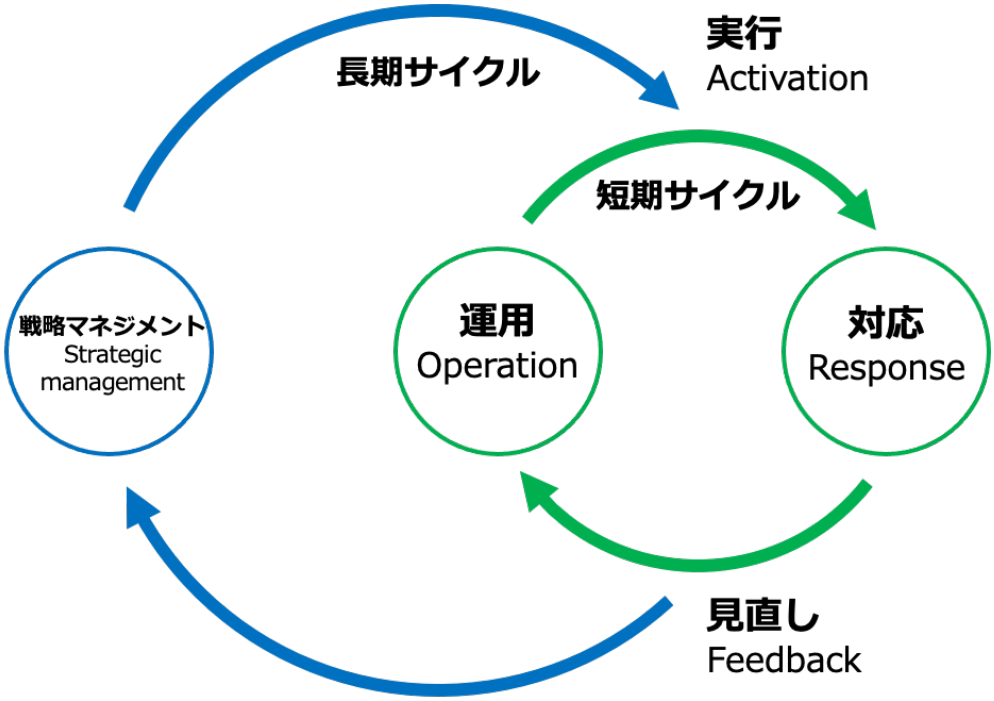


図 9 セキュリティ対応実行サイクル

3.3.2. マネジメントプロセスのフェーズとサイクル

マネジメントプロセスで示されている 3 つの工程と 2 種類のサイクルについて説明する。

- **戦略マネジメント**

X.1060/JT-X1060 では、「戦略マネジメントは、CDC の長期的な発展を保証するための定義、設計、計画、管理、認証などに関する戦略的サービスに対する責務と説明責任を有する」としている。

具体例として、セキュリティ対応の方針や短期サイクルの見直しに基づき長期サイクルで改善すべき事項、その実行に必要となる仕組み（体制、業務プロセス、システムなど）の検討、構築などを行う。

- **運用**

「運用」では、導入された仕組みの定常的な実行と維持を行う。おおむね平常時の営みがこれにあたる。インシデント検知のための分析や、セキュリティ対応システムの監視やメンテナンスなどを行う。このような分析運用を行う組織は SOC と呼ばれることが多い。

- **対応**

「対応」では、「運用」での分析で検知された事象に対し、インシデント対応を実行する。おおむね有事の営みがこれにあたる。インシデント対応を行う組織は CSIRT と呼ばれることが多い。インプットは「運用」からだけとは限らず、自組織外からの申告や、外部団体からの通達などを発端にした対応も行う。

- **短期サイクル**

「運用」と「対応」の業務が日々行われていく。その中で、業務プロセス上の問題点や、セキュリティ対応システムにおける課題が必ず発現するため、必ず見直しを行い、それらの課題に対し、導入された仕組みの中で、短いサイクルで改善を行っていく必要がある。例えば、単純業務の簡単な自動化や、分析精度向上のためのツール改善、レポート項目の見直しなどがそれにあたる。あくまで、割り当てられたリソース（人員、予算、システム）内での見直しが該当する。あえて図示はしていないが、「戦略マネジメント」「運用」「対応」それぞれの中に閉じた見直しもある。

- **長期サイクル**

「短期サイクル」の見直しにおいて、導入された仕組みの中では解決できないような課題が挙げられた場合は、長期的な視点、計画をもって対応を行う。例えば、新たなセキュリティ製品の導入や、大幅なセキュリティ対応方針の見直し、運用基盤の大規模な構成変更などがそれにあたる。新たなリソースの割り当てが必要となるような見直しが該当する。

昨今の CSIRT 構築においては、「対応」の段階を中心に組織を組み上げセキュリティ対応を行っていこうとするケースが多く見られる。しかし、そこだけを切り取り組織化するだけでは、「運用」が上手く回らずインシデントを見逃してしまったり、そもそも自組織や自社の守りたいものがはっきりしない中でセキュリティ製品を選定してしまうなど、「戦略マネジメント」の時点で失敗したりと、様々な問題に直面してしまう可能性がある。

そうならないためにも、「戦略マネジメント」「運用」「対応」という軸をおさえ、「実行」と「見直し」によるサイクルを回していくというイメージを持つことが重要である。

3.4. セキュリティ対応組織の評価

3.4.1. 評価プロセスの全体像

本書では X.1060/JT-X1060 をベースとして評価プロセスを説明する。評価プロセスは X.1060/JT-X1060 で新たに追加されたものである。評価プロセスの実施方法は、構築プロセスで行った以下の 3 つのフェーズをそれぞれ見直すことである。

- ✧ **フェーズ１：サービスカタログの推奨レベルのギャップ分析**
- ✧ **フェーズ２：サービスプロファイルのサービス割り当てのギャップ分析**
- ✧ **フェーズ３：サービスポートフォリオのサービスアセスメントのギャップ分析**

以下の図は X.1060/JT-X1060 で示される評価プロセスの概要である。

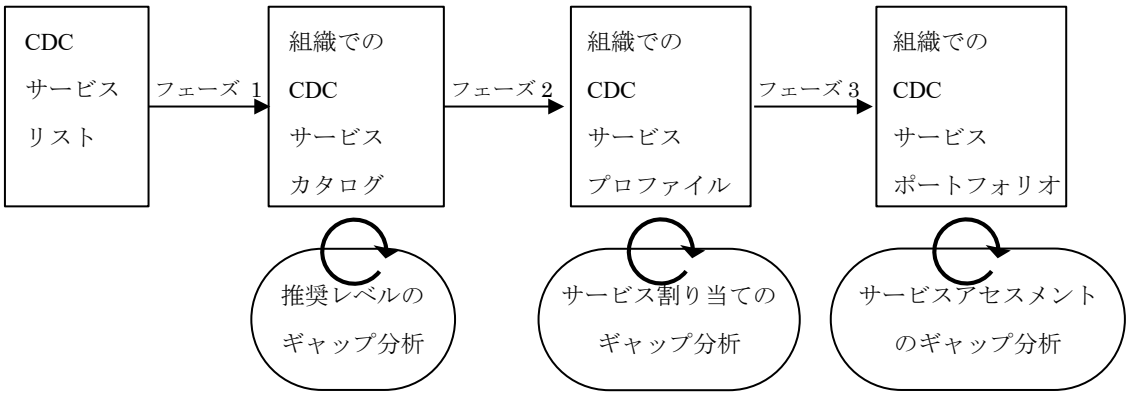


図 10 X.1060/JT-X1060 の CDC 評価プロセス [14]

評価プロセスでは構築プロセスで行った 3 つのフェーズでそれぞれギャップ分析を行う。ギャップ分析をする順番の例としては、構築プロセスと同様にフェーズ 1 から順にそれぞれの結果が妥当であったかを見直す方法である。あるいは逆の順番で、フェーズ 3 の現在のアセスメントスコアとのギャップから、なぜそのような結果になっているのかを見直してもよい。

[14] 出典：一般社団法人 情報技術委員会(TTC) JT-X1060 サイバーディフェンスセンターを構築・運用するためのフレームワーク、図 7
https://www.ttc.or.jp/document_db/information/view_express_entity/1423

3.4.2. ギャップ分析と見直し

評価プロセスでギャップ分析を行うことで、これまで構築してきた体制の過不足が可視化される。この結果をもって、再び構築プロセスに立ち返り、より良いセキュリティ対応に繋げていくことが重要となる。組織として全体感のある改善をするためには、十分な権限をCISO やセキュリティ統括、セキュリティ対応組織に与え、一部のチーム内の改善や担当の頑張りに依存するような見直しにならないよう細心の注意を払う必要がある。

ビジネスの状況やそれを取り巻く環境は想像以上に早く進むため、一度作った体制も徐々に陳腐化してしまうことは避けられない。原則出勤して、保護されたイントラネット環境で業務をしていたような会社組織であっても、COVID-19 によって突如としてリモートワークが必須となったケースは少なくない。同時に、セキュリティ対応組織自体もリモートでの対応となった業務もあったのではないだろうか。このような外部環境の変化により、守るべき対象やセキュリティ対応組織自体の業務環境が突如として変わるケースは今後も発生するであろう。だからこそ、X.1060/JT-X1060 のフレームワークは、継続的に、構築・マネジメント・評価のプロセスを繰り返す形となっている。セキュリティ対応に関して、悪い意味での前例踏襲や硬直化を起こさないよう、評価プロセスをうまく活用し、マネジメントプロセスを意識しながら必要に応じて再構築を実現して行きたい。

4. セキュリティ対応組織のカテゴリー

4.1. カテゴリーの全体像

セキュリティ対応組織の構築時には X.1060/JT-X1060 のサービスリストを活用し、サービスカタログの作成を行った。この X.1060/JT-X1060 のサービスリストはセキュリティ対応組織が担うべき機能分野とその各分野で実施する内容として、9 つのカテゴリーと 64 のサービスで示されている。これは本書第 2.1 版が基になっており、「カテゴリー」は「機能」、「サービス」は「役割」と呼ばれていたものである。9 つのカテゴリーは同じ内容で一部名前が変更となっている。

X.1060/JT-X1060 で定義される 9 つのカテゴリーと第 2.1 版の機能との対応は以下である。

表 6 X.1060/JT-X1060 のカテゴリー第 2.1 版の機能の対応

X.1060/JT-X1060 のカテゴリー	第 2.1 版の機能
A. CDC の戦略マネジメント	A. セキュリティ対応組織運営
B. 即時分析	B. リアルタイムアナリシス（即時分析）
C. 深掘分析	C. ディープアナリシス（深堀分析）
D. インシデント対応	D. インシデント対応
E. 診断と評価	E. セキュリティ対応状況の診断と評価
F. 脅威情報の収集および分析と評価	F. 脅威情報の収集および分析と評価
G. CDC プラットフォームの開発・保守	G. セキュリティ対応システム運用・開発
H. 内部不正対応支援	H. 内部統制・内部不正対応支援
I. 外部組織との積極的連携	I. 外部組織との積極的連携

一部表現は変わっているものの、第 2.1 版と比較して数と内容もほぼ同等のものとなっている。なお、「A. CDC の戦略マネジメント」については、日本国内でいうところの「戦略マネジメント層」と用語を合わせ、マネジメントプロセスにおいても「戦略マネジメント」という用語を活用し、国内の他のドキュメントと整合性を保つ内容となっている。

それぞれのカテゴリーの詳細については「付録　カテゴリーとサービスリストの詳細」に記載する。

4.2. カテゴリーとセキュリティ対応の実行サイクル

各カテゴリーがセキュリティ対応の実行サイクルのどの時点で活用されることになるかを「図 9　セキュリティ対応実行サイクル」に当てはめると、次の図のようにまとめられる。

図中の「戦略マネジメント」、「運用」、「対応」のそれぞれの実行サイクルのどのプロセスにサービスのカテゴリーが対応するかは、図に重ねる形で記載をしている。選択したカテゴリーが実行サイクルのどのプロセスに関連するか、参考にしていただきたい。ここで、カテゴリーE、F、G は 3 つのプロセスに関係するため、幅が広くなっている。カテゴリーG は戦略マネジメントで計画された CDC プラットフォームが運用と対応のサイクルで利用されるため、プロセスの上側に重ねている。

第 2.1 版では「I. 外部組織との積極的連携」についてはどのサービスにも付随するものであるため、図に含まれていなかったが、全てのカテゴリーを明示することや X.1060/JT-X1060 作成の際に戦略マネジメントに関連が近いことから、全体の図の左側に位置するようになった。

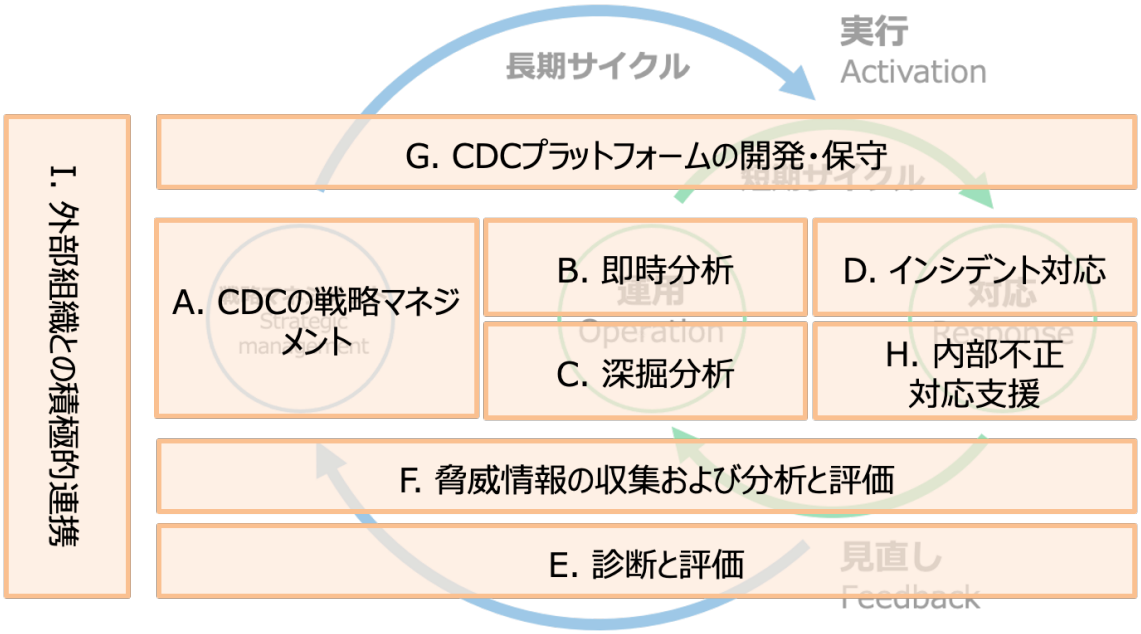


図 11 カテゴリーと実行サイクル

「A. CDC の戦略マネジメント」での決定方針に基づき、「G. CDC プラットフォームの開発・保守」において、その目的を満たすシステム実装によりセキュリティ対応を実行できるようにする。そして、そのシステムを活用しながら、「B. 即時分析」や必要に応じて「C. 深掘分析」の運用を行い、何かインシデントたるものが発見されれば「D. インシデント対応」や「H. 内部不正対応支援」を行う。

これらの運用や対応の結果も含め「F. 脅威情報の収集および分析と評価」により自組織や自社を取り巻く脅威を把握しつつ、「E. 診断と評価」により自組織や自社の守備力を評価する。その評価をもとに、すぐに実施できる改善は短期サイクルで実施し、より抜本的な見直しが必要な場合は、あらためて「A. CDC の戦略マネジメント」で決定し、次なる「G. CDC

プラットフォームの開発・保守」を実行するという長期的なサイクルを回すこととなる。

なお、必ずしも一つの組織内で全てのカテゴリーを保持し実行サイクルを回す必要はない。実情を鑑みても各カテゴリーが組織内や社内の別組織と連携しながら実行されるケースが一般的だろう。しかしながら、組織間で連携する場合には、非常に緊密な関係が維持される必要がある。

5. セキュリティ対応組織のサービス

5.1. サービスの全体像

前章でとりあげたカテゴリーと同様に、第 2.1 版で示した 54 の役割と X.1060/JT-X1060 の 64 のサービスの対応については以下となる。本書では X.1060/JT-X1060 のサービスに準拠する。呼び方も第 2.1 版までは「役割」であったが、「サービス」と呼称する。

第 2.1 版の役割から大きく変化はしておらず、新たに追加されたサービスなどがあったことからサービスの数は役割の時より増えている。それぞれのサービスの詳細については「付録　カテゴリーとサービスリストの詳細」に記載する。

表 7 X.1060/JT-X1060 と第 2.1 版の役割のサービスの対応

X.1060/JT-X1060 のサービス	対応する第 2.1 版の役割
A-1. リスクマネジメント A-2. リスクアセスメント A-3. ポリシーの企画立案 A-4. ポリシー管理 A-5. 事業継続性 A-6. 事業影響度分析	A-1. 全体方針管理
A-7. リソース管理	A-6. リソース管理 I-4. セキュリティ人材の確保
A-8. セキュリティアーキテクチャ設計	–
A-9. トリアージ基準管理	A-2. トリアージ基準管理
A-10. 対応策選定	A-3. アクション方針管理
A-11. 品質管理	A-4. 品質管理
A-12. セキュリティ監査	A-5. セキュリティ対応効果測定
A-13. 認証	–
B-1. リアルタイム監視	B-1. リアルタイム基本分析 B-2. リアルタイム高度分析 H-1. 内部統制監査データの収集と管理
B-2. イベントデータ保管	B-3. トリアージ情報収集
B-3. 通知・警告	B-4. リアルタイム分析報告
B-4. レポート問い合わせ対応	B-5. 分析結果問合受付
C-1. フォレンジック分析	C-1. ネットワークフォレンジック

X.1060/JT-X1060 のサービス	対応する第 2.1 版の役割
	C-2. デジタルフォレンジック
C-2. 検体解析	C-3. 検体解析
C-3. 追及・追跡	C-4. 攻撃全容解析
C-4. 証拠収集	C-5. 証拠保全
D-1. インシデント報告受付	D-1. インシデント受付
D-2. インシデントハンドリング	D-2. インシデント管理
D-3. インシデント分類	D-3. インシデント分析
D-4. インシデント対応・封じ込め	D-4. リモート対処 D-5. オンサイト対処
D-5. インシデント復旧	–
D-6. インシデント通知	D-6. インシデント対応内部連携 D-7. インシデント対応外部連携
D-7. インシデント対応報告	D-8. インシデント対応報告
E-1. ネットワーク情報収集	E-1. ネットワーク情報収集
E-2. 資産棚卸	E-2. アセット情報収集
E-3. 脆弱性診断	E-4. 自動脆弱性診断
E-4. パッチ管理	E-3. 脆弱性管理・対応
E-5. ペネトレーションテスト	E-5. 手動脆弱性診断
E-6. 高度サイバー攻撃耐性評価	E-6. 標的型攻撃耐性評価
E-7. サイバー攻撃対応力評価	E-7. サイバー攻撃対応力評価
E-8. ポリシー遵守	–
E-9. 堅牢化	–
F-1. 事後分析	–
F-2. 内部脅威情報の収集・分析	F-1. 内部脅威情報の整理・分析
F-3. 外部脅威情報の収集・評価	F-2. 外部脅威情報の収集・評価
F-4. 脅威情報報告	F-3. 脅威情報報告
F-5. 脅威情報の活用	F-4. 脅威情報の活用
G-1. セキュリティアーキテクチャ実装	–
G-2. ネットワークセキュリティ製品基本運用	G-1. ネットワークセキュリティ製品基本運用
G-3. ネットワークセキュリティ製品高度運用	G-2. ネットワークセキュリティ製品高度運用
G-4. エンドポイントセキュリティ製品基本運用	G-3. エンドポイントセキュリティ製品基本運用

X.1060/JT-X1060 のサービス	対応する第 2.1 版の役割
G-5. エンドポイントセキュリティ製品高度運用	G-4. エンドポイントセキュリティ製品高度運用
G-6. クラウドセキュリティ製品基本運用	–
G-7. クラウドセキュリティ製品高度運用	–
G-8. 深堀分析ツール運用	G-5. ディープアナリシス（深堀分析）ツール運用
G-9. 分析基盤基本運用	G-6. 分析基盤基本運用
G-10. 分析基盤高度運用	G-7. 分析基盤高度運用
G-11. CDC システム運用	G-10. 業務基盤運用
G-12. 既設セキュリティツール検証	G-8. 既設セキュリティ対応ツール検証
G-13. 新規セキュリティツール検証	G-9. 新規セキュリティ対応ツール調査、開発
H-1. 内部不正対応・分析支援	H-2. 内部不正対応の調査・分析支援
H-2. 内部不正検知・再発防止支援	H-3. 内部不正検知・防止支援
I-1. 意識啓発	I-1. 社員のセキュリティに対する意識啓発
I-2. 教育・トレーニング	I-2. 社内研修・勉強会の実施や支援
I-3. セキュリティコンサルティング	I-3. 社内セキュリティアドバイザーとしての活動
I-4. セキュリティベンダーとの連携	I-5. セキュリティベンダーとの連携
I-5. セキュリティ関連団体との連携	I-6. セキュリティ関連団体との連携
I-6. 技術報告	–
I-7. 幹部向けセキュリティ報告	–

サービスカテゴリーとサービスの一覧、マネジメントプロセスについては、X.1060 と JT-X1060 の「図 8 CDC サービスカテゴリー」の図中の並びにも意味付けがされている。

マネジメントプロセスの「戦略マネジメント」「運用」「対応」と縦の並びが対応している。サービスを選ぶ際に、マネジメントプロセスのどの部分で対応をすべきかについてはこの図が参考となる。

カテゴリーE,F,G はマネジメントのどのプロセスにも関わっている。しかし、それぞれのサービスについては、どのプロセスで対応するかは別である。あくまで参考であるので、この通りにしなければならないといったことはない。

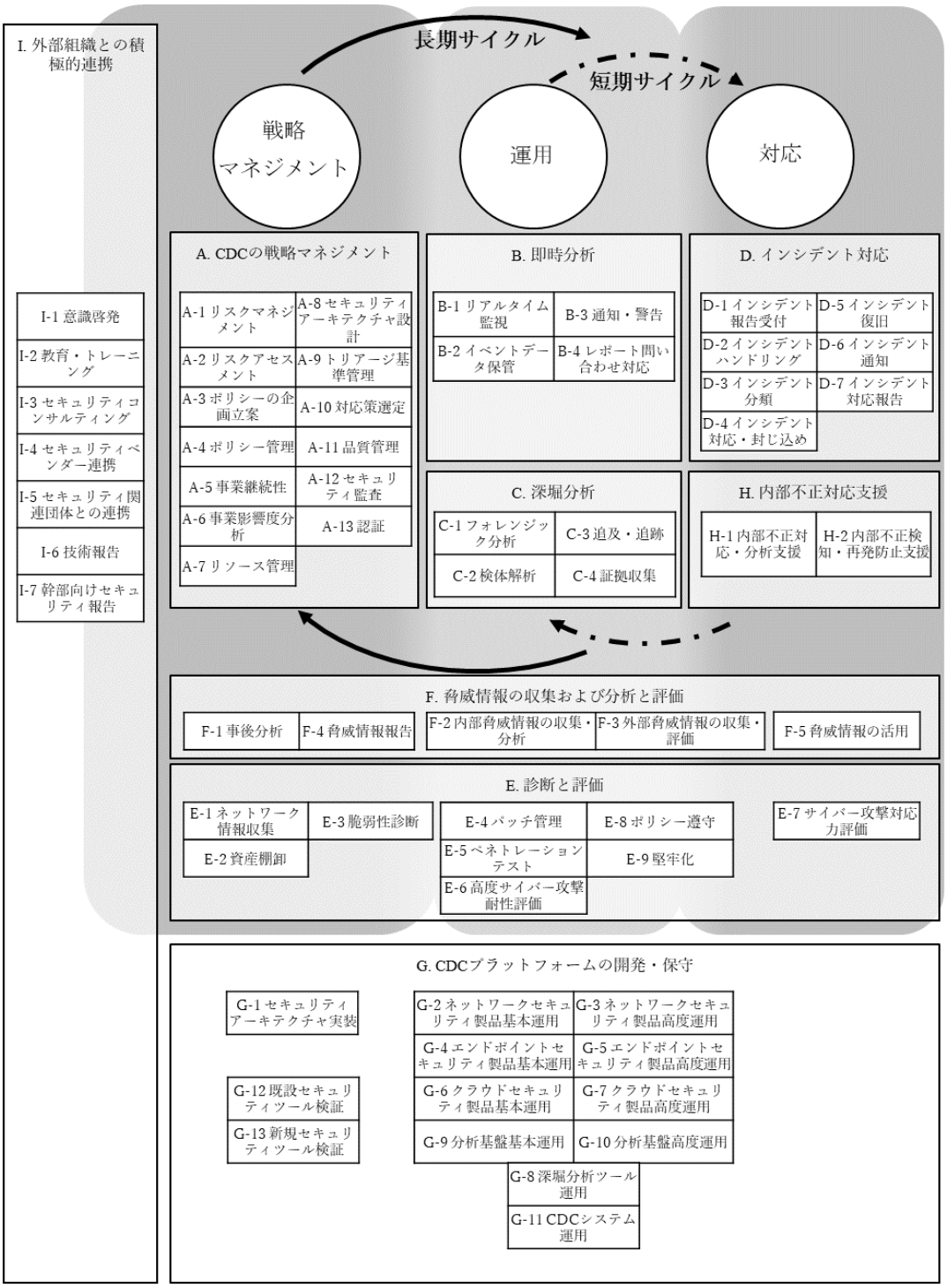


図 12 マネジメントプロセスと各サービスの関係 [15]

[15] 出典：一般社団法人 情報技術委員会(TTC) JT-X1060 サイバーディフェンスセンターを構築・運用するためのフレームワーク、図 8
https://www.ttc.or.jp/document_db/information/view_express_entity/1423

上の図における、マネジメントプロセスの「戦略マネジメント」「運用」「対応」に関連するそれぞれのカテゴリーのサービスは以下の表のように分類でき、マネジメントプロセスのどこで活用するかを参考とすることができる。

表 8「戦略マネジメント」「運用」「対応」に関連するそれぞれのカテゴリーのサービスの分類

カテゴリー	戦略マネジメント	運用	対応
A	A-1～A-13	–	–
B	–	B-1～B-4	–
C	–	C-1～C-4	–
D	–	–	D-1～D-7
E	E-1～E-3	E-4, E-5, E-6, E-8, E-9	E-7
F	F-1, F-4	F-2, F-3	F-5
G	G-1, G-12, G-13	G-2～G-11	–
H	–	–	H-1, H-2
I	I-1～I-7	–	–

5.2. サービスの推奨レベル

5.2.1. X.1060 の推奨レベルの解釈の仕方

構築プロセスの最初の段階ではサービスリストからサービスを選び、サービスカタログを作成する。その際に組織にとってそれぞれのサービスをどのレベルで実施したいかを表すものがその組織におけるサービスの推奨レベルである。

X.1060/JT-X1060 における CDC サービスの推奨レベルは、以下の表のウェイトで示す不要、ベーシック、スタンダード、アドバンスド、オプション 5 つのレベルに分けられている。

本書では X.1060/JT-X1060 のこの推奨レベルの表において、実施すべき優先度として考えるにあたり各レベルで以下の表の括弧内に示す解釈の追加を行う。

表 9 X.1060/JT-X1060 の CDC サービスの推奨レベル [16] と実施すべき優先度

ウェイト	説明
不要	不要と判断されたサービス
ベーシック （必須）	実施すべき最低限のサービス （必ずやるべき必須のサービス）
スタンダード （標準）	一般的に実装が推奨されているサービス （標準的に必要となるサービス）
アドバンスド （推奨）	高いレベルの CDC サイクルを実現する場合に要求されるサービス （よりしっかりしたセキュリティを実現するために推奨されるサービス）
オプション （任意）	想定される CDC の形態に応じて任意に選択されるサービス （任意で必要となるサービス）

構築プロセスの最初のフェーズでは、9 つのカテゴリー、64 のサービスから必要なサービスを選択する。サービスリストに必要なものがなければ、独自に追加を行う。

組織で必要なサービスを選択する時に、X.1060/JT-X1060 では「推奨レベル」の考え方が追加されている。

サービスの推奨レベルを判断する上で、まずは大きく「不要」であるかどうかである。不要な場合はなぜ不要と判断したのかを記録を残しておくことが重要である。リスクがないから不要と判断したのか、今はできないから不要と判断したのかは大きな違いがある。特に

16 出典：一般社団法人 情報技術委員会(TTC) JT-X1060 サイバーディフェンスセンターを構築・運用するためのフレームワーク、表 1
https://www.ttc.or.jp/document_db/information/view_express_entity/1423

後者の場合はその理由が、予算不足なのか、それとも人的リソースの問題か、スキル面の問題かなど明確にしておく必要があるだろう。そうすれば、評価プロセス後に再度構築プロセスを回す際の検討に活かすことができる。

次に実施すると決めたそれぞれのサービスに対して、「ベーシック、スタンダード、アドバンスド、オプション」のどのレベルを推奨レベルとするかを決める。「ベーシック」が最も優先度が高く、「オプション」が最も優先度が低い。各サービスの推奨レベルは、業界ごと、あるいは組織ごとの目標や形態、セキュリティポリシーなどによって変わってくる。そのため一律で定義することは難しく、X.1060/JT-X1060 でも、どのサービスがどのレベルにすべきかは記載されていない。

X.1060/JT-X1060 の活用が進み、ノウハウやナレッジが蓄積されれば推奨レベルの標準的なパターンが取りまとめられてくるかもしれないが、現時点では自身で決めていく必要がある。ただし、X.1060/JT-X1060 においては、この推奨レベルを決めなくとも後段のプロセスが進むようになっているため、難しい場合は必ずしも決め切る必要はない。

6. セキュリティ対応組織の役割分担と体制

6.1. これまでの日本における SOC・CSIRT とサービスの関係

セキュリティ対応組織の中で最もポピュラーなである SOC と CSIRT について、一般的に想定されている区分をおさらいする。イメージをクリアにするため、ここでは狭義の SOC（本書で言うところの、B、C のカテゴリーに限定）とする。

日本においては、インシデント対応の主体を CSIRT とした場合に、そのインシデントの発生を検知するためのセキュリティログ監視や、インシデント発生後の深掘分析（レスキューサービスあるいは緊急対応サービスと呼ばれる）を行う組織を SOC と呼称することが多い。

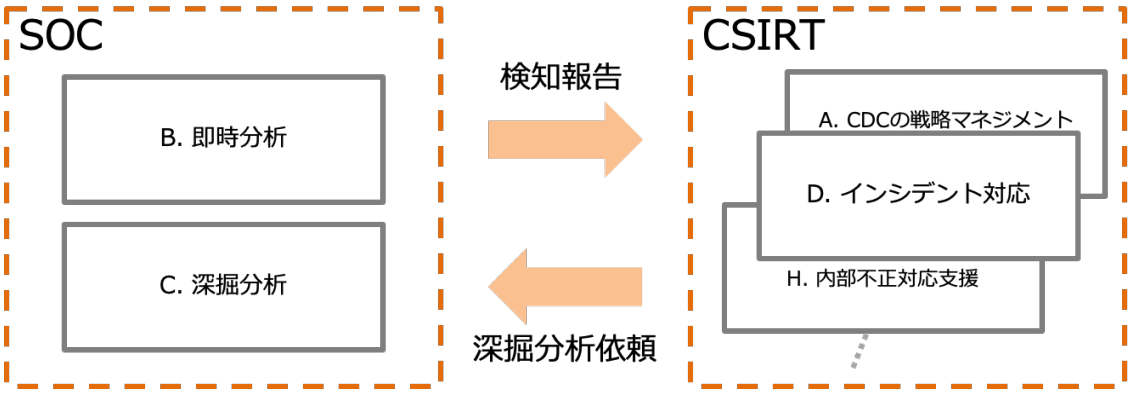


図 13　SOC と CSIRT の一般的な区分

しかし、昨今のセキュリティニーズ、意識の高まりにより、SOC はそのサービス範囲をインシデント対応の支援へ広げたり、CSIRT は基本的な分析は自身で行えるように技術レベルを上げたり、自組織内にプライベート SOC を持ったりと、その境界線は SOC 事業者や CSIRT の規模やレベルによって多様化してきている。よって、画一的な区分により、例えば「ここまでは CSIRT の役割だから自組織で、ここからは SOC の役割だから専門組織へお願いする」というような線を引くのは難しくなってきている。しかしながら、専門組織の活用等には契約行為が発生し、必然的に業務の線引きをしなければならないのも事実である。サービスをどのようにセキュリティチームへ割り当てるのか、自組織で行うのか、専門組織へお願いするのか。その「線引き」についての考え方を、次節にてまとめていく。

6.2. セキュリティ対応における役割分担の考え方

X.1060/JT-X1060 では、構築プロセスの最初のフェーズでサービスリストからサービスを選択してサービスカタログを作成する。次のフェーズでは、選択したサービスカタログからサービスを誰が実施するかの割り当てを決めたサービスプロファイルを作成する。サービスプロファイルの作成のために割り当てのタイプとして X.1060/JT-X1060 では以下の表の 4 つの分類を示している。

表 10 X.1060/JT-X1060 の CDC サービスの割り当て [17]

タイプ	説明
インソース	組織内のチームでサービスを実現する。責務を負う担当を明確にする。
アウトソース	組織外のチームでサービスを実現する。委託先を明確にする。
併用	インソースとアウトソースを併用する。責務を負う担当と委託先を明確にする。
未割り当て	組織に存在すべきサービスはあるが、割り当てられていない。

どこまでを自組織で担い（インソース）、どこから専門組織に頼るべきなのか（アウトソース）という役割分担を考えるために、以下の 2 つの指標を導入する。

① 取り扱う情報の性質

取り扱う情報が、組織内部のものなのか、組織外部のものなのか。インシデントについては、攻撃の被害・影響に関連する情報は「内部」、攻撃そのものに関連する情報は「外部」というように考える。

② セキュリティ専門スキルの必要性

サービスを実行する際に、セキュリティ分野における専門性の高いスキルがどの程度必要とされるか。「セキュリティ専門スキル」は、どのような組織においても活用可能なセキュリティ関連スキルのことを指している。ちなみに、その対となるスキルは「組織内・社内スキル」で、これは異なる組織へそのまま転用しても通用しにくいスキルを指す。

これらの指標を軸にすると 4 つの領域に分類することができる。

---

[17] 出典：一般社団法人 情報技術委員会(TTC) JT-X1060 サイバーディフェンスセンターを構築・運用するためのフレームワーク、表 2
https://www.ttc.or.jp/document_db/information/view_express_entity/1423

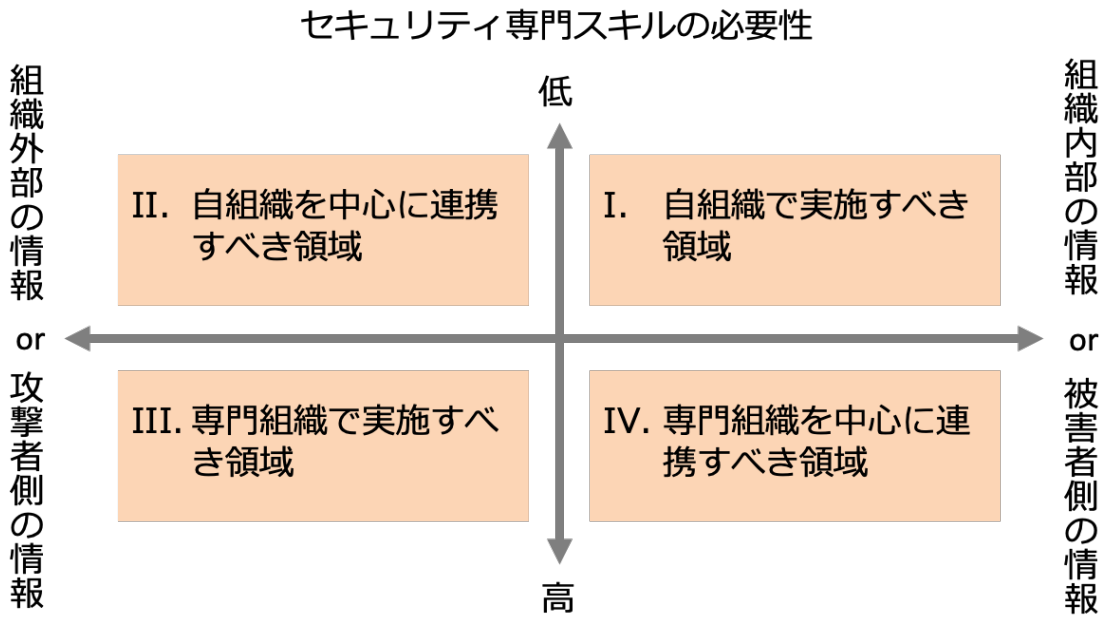


図 14　セキュリティ対応の4領域

領域I.　自組織で実施すべき領域（インソース≫アウトソース）

組織内部の情報の取り扱いにおいて、専門性がそれほど高く求められない、あるいは通用しない（裏を返せば、組織内・社内スキルが重要となる）ものは、自組織内にて実施する必要がある。外部の組織に頼ることが困難な領域。

領域II.　自組織を中心に連携すべき領域（インソース≧アウトソース）

組織外部に関する情報ではあるものの、求められる専門性がそれほど高くなく、主に組織内・社内スキルが求められる場合、実行、管理は自組織を中心に、専門組織はその支援を行う。

領域III. 専門組織で実施すべき領域（インソース≪アウトソース）

組織外部の情報、つまり攻撃に関する情報について、専門的スキルをもって対応するため、専門組織にて実施することとなる。専門的スキルを持ったメンバーが自組織内にいない限り、自組織での対応は困難な領域。

領域IV. 専門組織を中心に連携すべき領域（インソース≦アウトソース）

組織内部に関する情報ではあるものの、専門スキルが必要となるため、実行面では専門組織を中心に、自組織はその管理、支援を行う。

X.1060/JT-X1060 の構築プロセスのサービスの割り当てのフェーズでは、優先度を決めたサービスに対してそれぞれ誰が実施するかの割り当てを行う。一つのセキュリティの部門が全ての責任を持って実施するのではなく、システム部門や場合によりビジネス部門でもそれぞれのサービスを分担して実施をする。組織の全体としてセキュリティをどのように実施するかということが割り当てのフェーズの観点となる。

この割り当ての際に全て内製（インソース）できない場合もあるので、インソース、アウトソース、併用を割り当てとして考えることができる。

第 2.1 版ではインソースかアウトソースしかなかったが、X.1060/JT-X1060 では「併用」と「未割り当て」が追加されている。特に未割り当ては評価や見直しの際には活用できるものなので、割り当ての抜けや漏れがないように活用したい。本書第 2.1 版においては「アウトソース」か「インソース」か、と線引きしてしまっていたが、より現実的な選択肢として「併用」が追加され活用しやすくなっている。表の説明にもあるように、責務を行う担当がどこになるのか、誰が担うは重要であるため、このフェーズで明確にしておきたい。

6.3. セキュリティ対応の組織パターン

セキュリティ対応組織のパターンは、前節で整理した自組織での実行が必須な領域Ⅰ以外の3領域について、どこまで自組織のリソースでカバーするかで大別される。

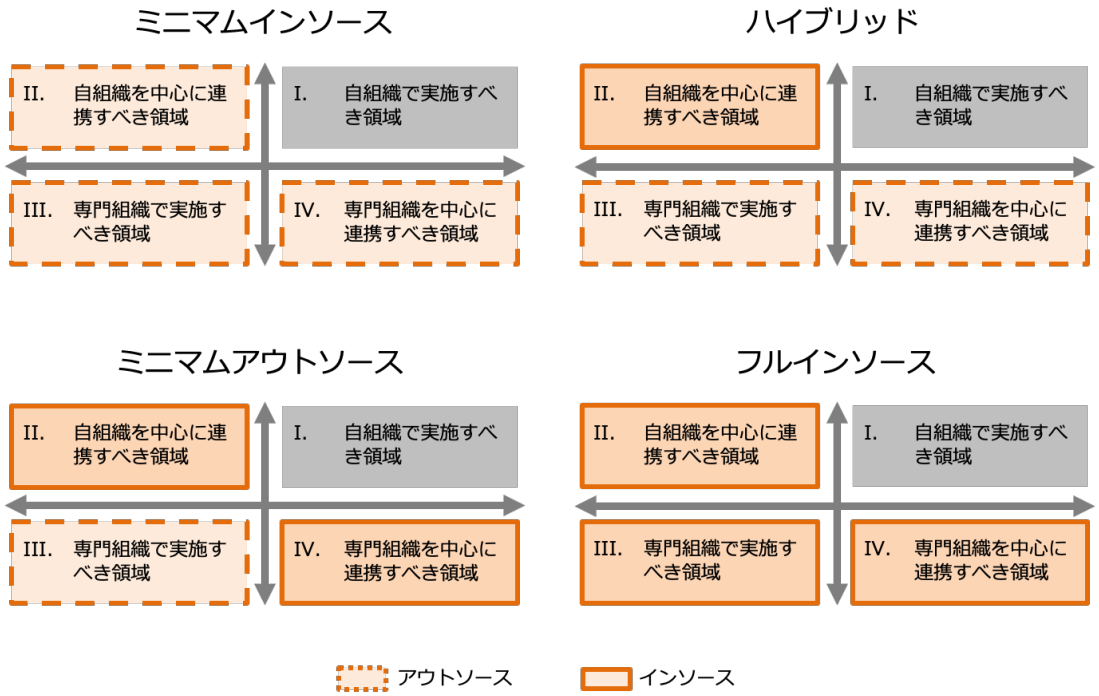


図 15 セキュリティ対応の組織パターン

パターン1. ミニマムインソース

自組織内にセキュリティ対応に関わる専門的知見がほとんどなく、領域Ⅱにおいても、外部の専門組織に大きく頼らなければならないパターン。例えば、非 IT 系のユーザー企業において総務部門等を主体にセキュリティ組織を初めて作るようなケースでは実態としてこのパターンになる。

パターン2. ハイブリッド

自組織内でセキュリティ対応に関わる知見を最低限持ち、領域Ⅱにおいても自組織が中心となって実行できるパターン。例えば、ユーザー企業やそのシステム子会社が情報システムに関する専門部門を主体として組織を作るケースではこのパターンが多く、最も一般的な形態であると言える。

パターン3. ミニマムアウトソース

自組織内でセキュリティ対応に関わる知見を持ち、領域Ⅲ以外を自組織が中心となって

実行できるパターン。例えば、IT 系の企業において情報セキュリティに関する専門部門を主体として組織を作るケースではこのパターンが多い。

パターン4.　　フルインソース

自組織内で全てのセキュリティ対応カテゴリー・サービスを担うことができるパターン。一部の IT 企業やセキュリティ専門企業あるいは、極めて高いセキュリティレベルが問われる特殊な組織においてはこのパターンが目標となる[18]。

6.4.　セキュリティ対応における役割分担

セキュリティ対応の 4 領域にサービスを割り振っていくと次の図のようにまとめられる。自組織の組織パターンを意識し、どんなサービスをアウトソースすればよいか、インソースする場合にはどのようなサービスを実現する必要があるか検討の参考としてほしい。

割り振りの考え方の例としては、「セキュリティ専門スキルの必要性」の「低」と「高」については、セキュリティの各種対策について「設計」をするのか、それに基づき「実装」や「運用」をするのかといった考え方に置き換えることもできる。例としてはカテゴリーA の「CDC の戦略マネジメント」は全体の戦略や方向性を定めて設計をするサービスが中心のため、「セキュリティ専門スキルの必要性」は「低」の領域の方向にマッピングされている。

取り扱う情報の性質の「組織内部の情報 or 被害者側の情報」と「組織外部の情報 or 攻撃者側の情報」については組織の外部からは得にくい内部の機密の情報に近いサービスか、外部の脅威情報が中心で専門性の高いスキルを中心としたサービスと考えることもできる。これらの考え方から一例として全てのサービスを割り振ったものが「図 16　セキュリティ対応の役割分担」である。ただし、「I-5. セキュリティ関連団体との連携」については全ての領域において必要であるため、各領域に設定されている。

[18]念のため断っておくが、「フルインソース」を絶対的な目標とする必要はない。自組織のスキルやリソースを鑑み、全体方針に従って必要な各カテゴリー・サービスが満たされ実行サイクルが回るのであれば、アウトソース比率が大きくても何ら問題はない。むしろ無理にインソース比率を高めてしまって実態が伴わないことの方が問題となる。

図 16 セキュリティ対応の役割分担

6.5.　セキュリティ対応組織の体制

6.5.1.　フラットな組織の例

「カテゴリー」=「体制」となっていれば議論はしやすいが、実態はそうではないため、この章で「体制」について整理する。

しかしながら実際の組織体制は各企業で千差万別であり、それらを加味しながら議論するのは非常に難しい。そのため、ここではあえて、CISO の配下に各カテゴリー、サービスがフラットな体制で配置されているという理想的な組織体制の前提でまとめていく。このような体制は「フルインソース」パターンのセキュリティ専門組織や企業などにみられる。

具体的な体制を次の表でまとめている [19]。「担当名」と「領域」のマトリックスの中に、「サービス」を列挙している。

自組織の実態とは異なるとは思うが、これまで整理してきたとおり「サービス」については明確であるため、「自組織の体制だとここは〇〇部門でやっているな、こっちは〇〇社に委託しているな」というように、頭の中でうまく当てはめていただければ幸いである。また、これからセキュリティ対応組織を作る場合には、こういった体制を念頭に、実際の体制づくりに活かしてほしい。

19

- 「領域」をⅠ・Ⅱ・Ⅳ・Ⅲの順としている。これは、専門組織への依存度が段々と高まるように並べたためである。
- 複数の担当に同じ役割が記載されているものは、共に取り組む可能性が高い業務である。実際のセキュリティ対応においてはより多くの担当が共同で対処に当たる場合ももちろんあるため、代表的な例として捉えていただきたい。なお、同一担当内の連携はあるものと考え、表が複雑化しないよう、同じサービスを複数の領域に記載することは避けている。

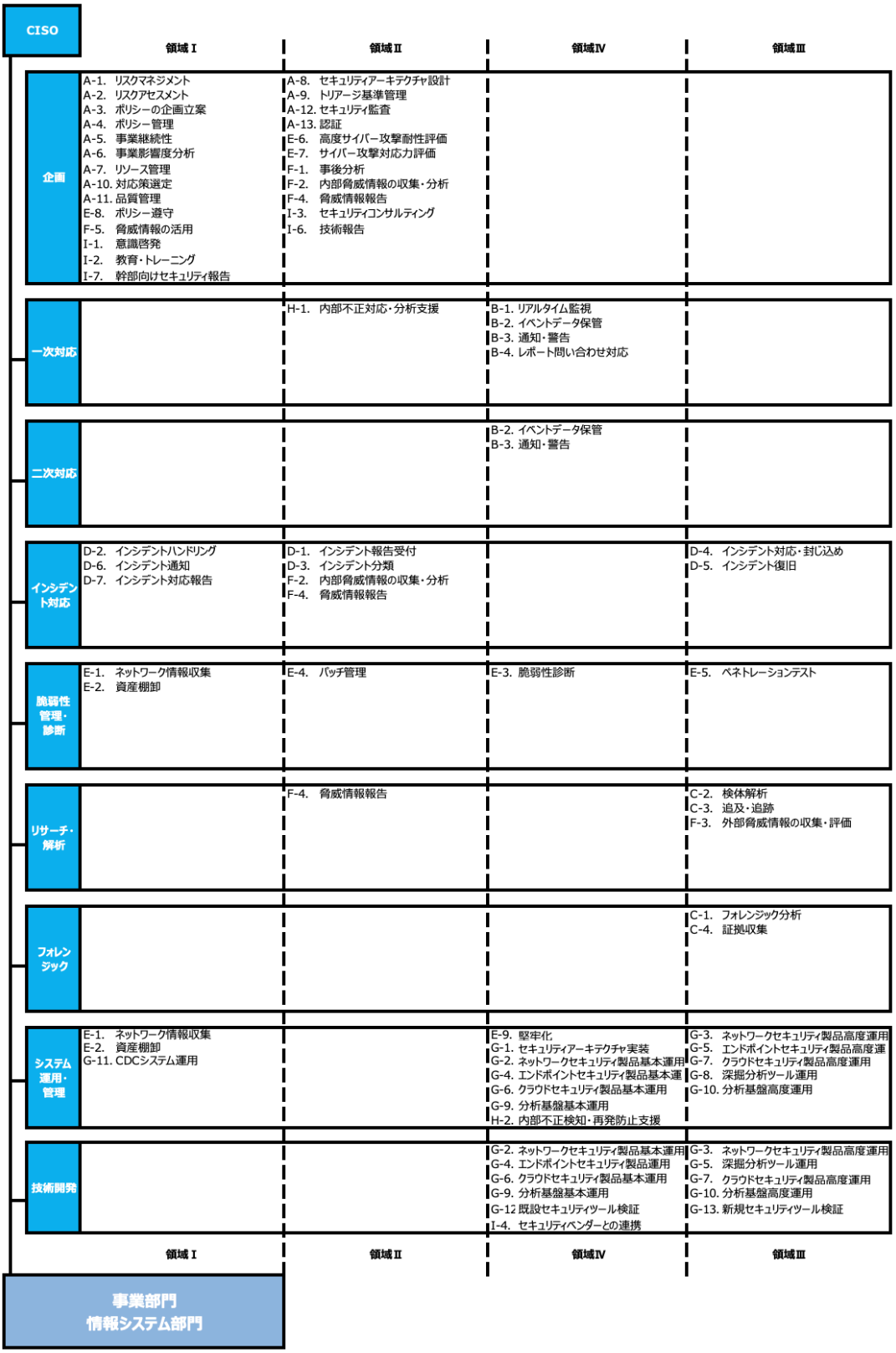


図 17　セキュリティ対応の組織体制

6.5.2. X.1060/JT-X1060 で割り当てる基本パターン例

組織体制を構築する場合、大きく 2 つのケースが考えられる。一つは新たに組織体制を作る場合、もう一つはすでにある組織体制を見直す場合である。

新たに組織体制を作る場合は、それぞれの組織の目的に合ったサービスを選択して割り当てることになる。いきなり全てのサービスを選択して割り当てることは難しく、最低限運用ができるようなカテゴリーのサービスを選択する方が良い。最低限運用ができる、というのは、マネジメントプロセスにおいて、短期サイクルと長期サイクルが実行できるような組み合わせである。

「図 11　カテゴリーと実行サイクル」を例に、実行プロセスに各カテゴリーを重ねてみると、カテゴリーA の「CDC の戦略マネジメント」、カテゴリーB の「即時分析」、カテゴリーD の「インシデント対応」の中からサービスを選択する。カテゴリーI の「外部組織との積極的連携」はどのサービスにも付随するものであるため、必要なものは選択をする。

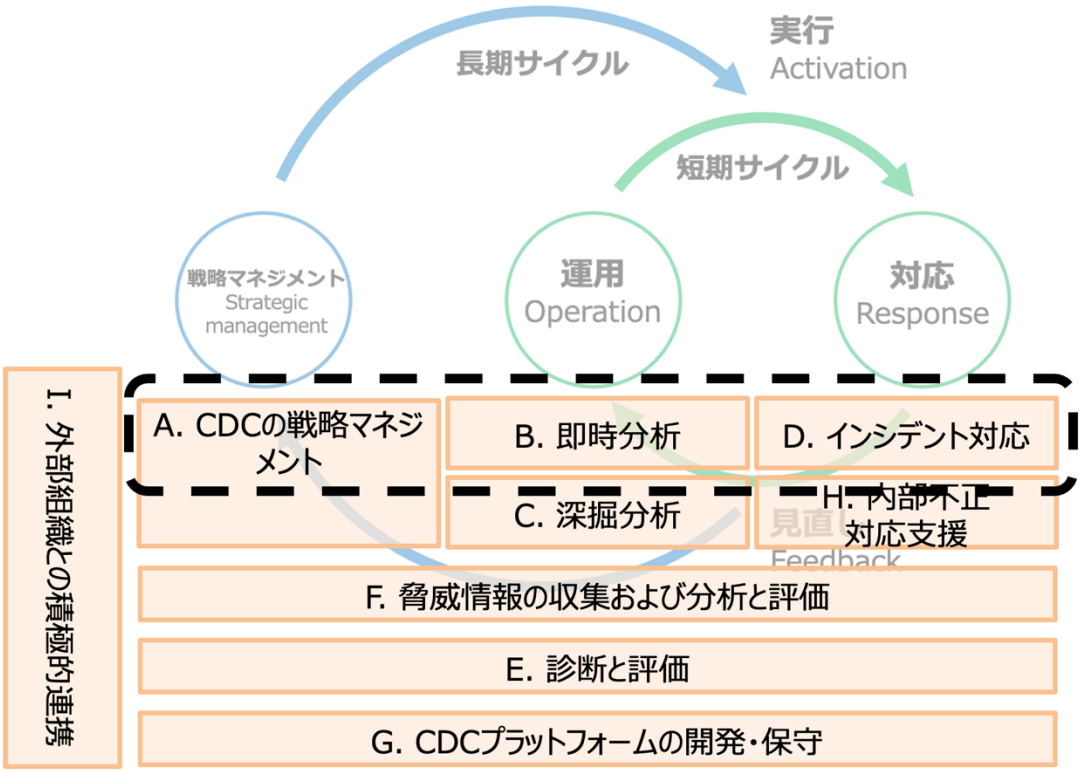


図 18 運用に向けたカテゴリー

1 から組織を形成する場合では、まずカテゴリーA, B, D の中で、それぞれの組織に必要となるサービスを、推奨レベルを含めて決定し、セキュリティチームへ割り当てる。

X.1060/JT-X1060 のセキュリティ対応組織の構築と運用のフレームワークでは、マネジメントプロセスにおける工程を実施した結果を基に、定期的な改善を図るために評価プロ

セスを行うことが求められる。評価結果を基に、できることや実施すべきカテゴリーやサービスを再考する。再度構築プロセスを開始して、サービスの割り当てをすることで、セキュリティ対応組織として成長することが可能である。このように見直しを続けることで、あるべき組織の形を再構成していくことを目指したい。

すでに SOC や CSIRT などセキュリティを行う組織や部門が存在しており、それをより良くする形で見直す場合もある。

見直すためのきっかけはさまざまである。立ち上げてから数年たち、周辺の状況が大きく変化して見直すことになった、あるいはやるべきことが増えて人員などのリソースが足りなくなり、全体から見直すことになった、などである。組織によってはインシデントなどの被害が契機になることもある。

まずは 9 つのカテゴリーと 64 のサービスにすでに行なっているものをマッピングする。64 のサービスの中になければ追加してもよい。

マッピングすることで、再度会社や組織の目標やサービスの推奨レベルを考え、どんなサービスが必要であるかを確認できる。新たに行うべきサービスについては割り当てを行う。ここでも、前述のカテゴリーA, B, D によりマネジメントプロセスが実施できるような構成になっているかは注意が必要である。

スタートとしてカテゴリーA, B, D を挙げているが、それだけあれば良いということではない。各組織で必要なサービスが漏れなく実施されているかの観点が重要である。

組織を立ち上げる際に当初は人員に限りがあり、1 人から始めるといった場合もある。X.1060/JT-X1060 の構築プロセスにおいてサービスを割り当てる際には、全体を実行できるようにするため、1 人でできない部分はアウトソースを活用することやハイブリッドで割り当てることを示している。マネジメントプロセスの短期サイクルや長期サイクルにおいて日々の業務の見直しや体制の強化、スキルアップなどが実施される。評価プロセスにおいて、次の構築プロセス向けた状況として、人数が増えた、スキルが向上したなど見直すことができる。評価の結果、次の構築プロセスにおいてどのサービスにどのようにリソースを割り当てるかについては、推奨レベルやアセスメントによるスコアを参考にできる。

日々の予防に重点を置くのであれば、カテゴリーF の「脅威情報の収集および分析と評価」からサービスやカテゴリーE の「診断と評価」のサービスを選択して、情報の収集から診断の実施や訓練を強化するといった方向を考えることができる。

組織の内外や社内外との連携、要員の啓発や教育についてはカテゴリーI の「外部組織との積極的連携」からサービスを選択することになる。

このように、当初は限られたリソースによりできるところから始めることになる。見直しを続けながらできることを増やし、より良い形に改善を続けたい。

昨今では、1 つの組織の中に 1 つのセキュリティ組織だけという形ではない場合もある。組織や会社全体を所掌範囲とするもの、ビジネス組織のビジネス単位を範囲とするもの、製品を対象の範囲とするものなど、さまざまな対象のセキュリティの組織が存在する。X.1060/JT-X1060 は 1 つの組織に 1 つのセキュリティ組織があるシンプルなケースのみ例示されている。一方で経済産業省　サイバーセキュリティ経営ガイドライン　付録 F では、調査に基づく日本の組織の形態が整理されている。これらを参考に、X.1060/JT-X1060 の要素を自組織に適合していくことが望ましい。

サプライチェーンや取引関係のように、複数の組織に存在するセキュリティ組織が連携するケースも存在する。この場合はそもそも組織や企業が別であるため、それぞれのセキュリティのポリシーや考え方が異なる。その場合では X.1060/JT-X1060 を共通の言語として利用することができる。全体のセキュリティを向上させるために、お互いにどのサービスを実施している必要があるかなど検討することができる。もし、関連する組織や企業で同じサービスを共通的に実施する必要があるならば、共同のセキュリティ組織を作ることも考えることができる。情報を共有して共同で活用することや、監視運用を同じアウトソース先にして全体を一括で監視運用するというような踏み込んだ体制の作り方もできる。

6.6. セキュリティ対応組織の要員数

セキュリティ対応組織の体制の検討において、必要となる人材の数は非常に重要な観点の一つとなる。自組織が行うべき領域Ⅰ・Ⅱについては、自組織の人員や社内で既に存在する別部門の人員など、ある程度これまでの業務の延長線上で、実行するカテゴリー・サービスさえ見えてくれば想定は可能だろう。一方で、その延長線上にはなく、組織によっては全く新しいカテゴリー・サービスとなることもある領域Ⅲ・Ⅳについては人員の想定が難しい。

しかし、この領域Ⅲ・Ⅳこそが、自組織でカバーすべきかアウトソースするかという大きな判断が必要な部分であり、その判断ためにも、必要人員の算出シミュレーションを避けては通れない。

本節では、前節の体制表の領域Ⅲ・Ⅳの要員について、自組織で確保し稼働させるシミュレーションとして 4 つのモデルケースにまとめた。

このモデルケースはあくまで最低限のベースであり、実際の対象とする規模や監視するセンサーの数、組織の就業規則への対応などによってはさらに人数が増えることもあり得る。それぞれの組織での監視運用の規模と合わせて想定されたい。

表 11　セキュリティ専門性の高い役割の要員モデル

	Level 0	Level 1	Level 2	Level 3
一次対応	日勤 1 名	日勤 2 名	常時 1 名 （全 6 名）	常時 2 名 （全 12 名）
二次対応	日勤 1 名	日勤 1 名	日勤 2 名	常時 1 名 （全 6 名）
インシデント 対応	二次対応が 兼務	日勤 1 名	日勤 1 名	日勤 2 名
脆弱性 管理・診断	二次対応が 兼務	インシデント 対応が兼務	インシデント 対応が兼務	インシデント 対応が兼務
リサーチ・ 解析	しない	二次対応が 兼務	二次対応が 兼務	日勤 1 名
フォレンジック	しない	しない	二次対応が 兼務	リサーチ・ 解析が兼務
システム 運用・管理	日勤 1 名	日勤 2 名	日勤 2 名	日勤 3 名
技術開発	日勤 1 名	日勤 1 名	日勤 1 名	日勤 2 名
合計	4 名	7 名	12 名	26 名

Level 0

必要なチームを最小人数で構成し、フォレンジックやリサーチ・解析などは諦め、非常に単純な対応ルールでセキュリティ対応を行う最小モデル。立上げ最初期の試験的チーム体制の目安となる。実際にはインシデントが一つ起こっただけで対応は手いっぱいになり、セキュリティ関連システムに少しでも障害が発生すればシステム管理側も手いっぱいになるため、領域Ⅰ・Ⅱの体制で領域Ⅲ・Ⅳを支援できない限り、実行的な体制にはなりえない。

Level 1

実行的な体制として最低限の構成。24 時間 365 日の対応やフォレンジックは実施しないものの、必要最低限の対応は可能なモデル。もし別組織に NOC（ネットワークオペレーションセンター）などの 24 時間 365 日体制が存在しているのであれば、「一次対応」や「システム運用・管理」のうち手順化が容易な業務を一部委託し、補完し合うとよい。

Level 2

セキュリティ専門の 24 時間 365 日体制を持つモデル。この規模の体制を持つことができれば、一通りのセキュリティ対応を実現できる。いわゆるプライベート SOC を自組織に構えたいのであればこの体制がスタートラインとなる。なお、Level 2 および後述の Level 3 では体制の効率化のため、「システム運用・管理」における一次切り分けの機能を「一次対応」に含めるものとし、システム運用・管理における 24 時間 365 日体制を不要としている。

Level 3

1 社のセキュリティを見るというよりは、全国の支店、支社やグループ会社など、関連する複数の大組織をまとめて対象とするような SOC モデル。グローバル企業の場合は、Level 3 の規模を拡大して 1 拠点に集約するか、各リージョンの事業規模に応じて Level 1 か Level 2 の体制をブランチとして配備し、最も事業規模の大きなリージョンに設置した Level 3 の体制に、その統括もさせるような階層型になる。

7. カテゴリーおよびサービスの関連

これまで整理してきたカテゴリーおよびサービスは「図 19　セキュリティ組織を取り巻く環境」のような組織と連携してセキュリティ対応業務を行っている。ここでは、セキュリティ対応組織内のカテゴリーおよびサービスがどのように連携するのか、関係図とフローを用いて解説する。

解説は「インシデントの発生時」および「インシデントの発生していない平常時」の 2 つの場面で運用場面を整理し、2 つの場面においてカテゴリーおよびサービスがどのように動作するかを示す。

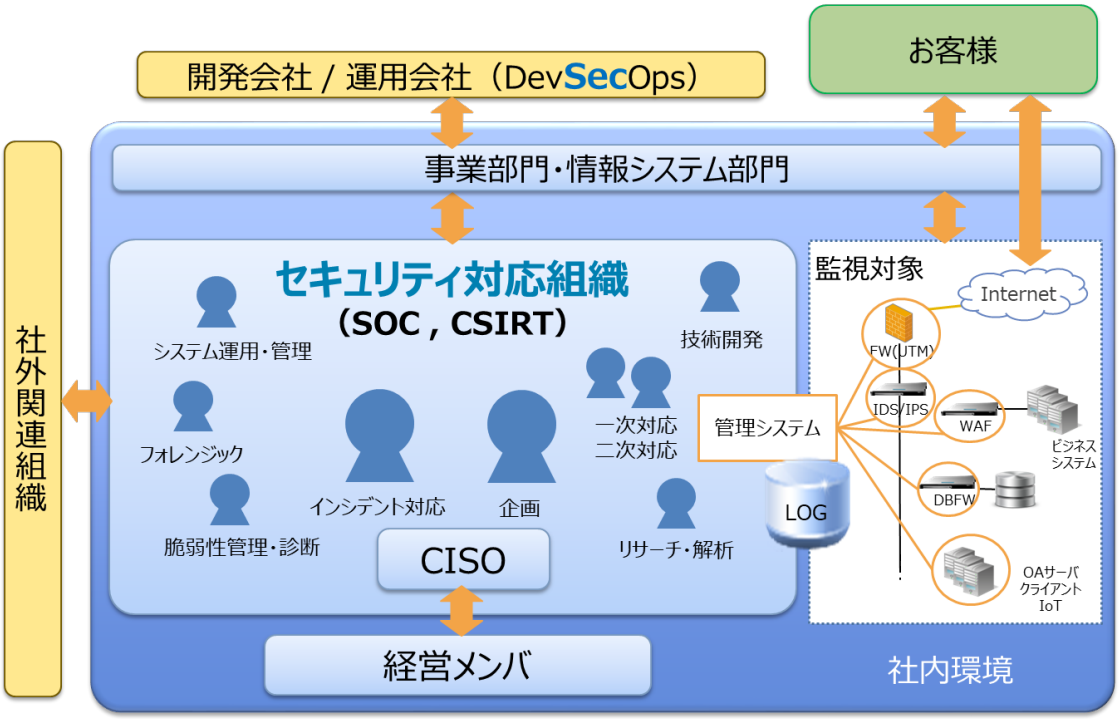


図 19　セキュリティ組織を取り巻く環境

7.1. インシデント対応フロー

インシデント発生時に大まかなフローはどのケースでもほぼ同じとなる。まずはベースとなるインシデント対応のカテゴリーおよびサービスの関係を例に示す。

ベースとなるインシデント対応のカテゴリーおよびサービスの関係を「6.5 セキュリティ対応組織の体制」で述べたカテゴリーおよびサービスで関連付け、「図 20 インシデントレスポンス時の関連」で示す。

① 普段の監視状態を維持する
② イベントをトリガにインシデントレスポンスがスタートする
- スタートは外部からの通報や監視からのアラートや公表された脆弱性についての CISO からの確認など様々である。

③ イベントが対応を要するインシデントであるか判断する
- イベントの受付からインシデントかどうかの判断はインシデント対応の領域 II、D-1,3,4 で実施する。得られた情報でインシデントであるかを判断する。

④ インシデント情報を詳細に調査する
- 状況を管理する上で影響度や情報が必要となる。専門的な情報収集を指示し、監視においての一次対応の領域 IV や専門領域である二次対応の領域 III・IV、被害がある場合にフォレンジックの領域 III や、攻撃の背景から対策を考えるのであればリサーチ・解釈の領域 III から情報を得る。

⑤ インシデントの影響度および優先度の判断を行う
- インシデントの影響度や優先度の判断は得られた情報をもとに領域 II、D-3 で実施する。

⑥ インシデント収束に向けた対処を行う
- インシデント対応の領域 I、D-2 でインシデントの状況の管理を行い、領域 II、D-4 で対処を行う。収束した後での報告を領域 I、D-6,7 で行う。

⑦ インシデント収束に伴いインシデントレスポンスの収束を宣言する
- 一連の影響や被害の調査、必要な対応を完了したところでインシデントレスポンスが収束と判断できれば、報告をして完了となる。収束しない場合継続的に情報収集や対応を繰り返し、収束するまで続く。

⑧ 報告をまとめて公表する

※領域Ⅰ/Ⅱ/Ⅲ/Ⅳについては「図 20 インシデントレスポンス時の関連」を参照

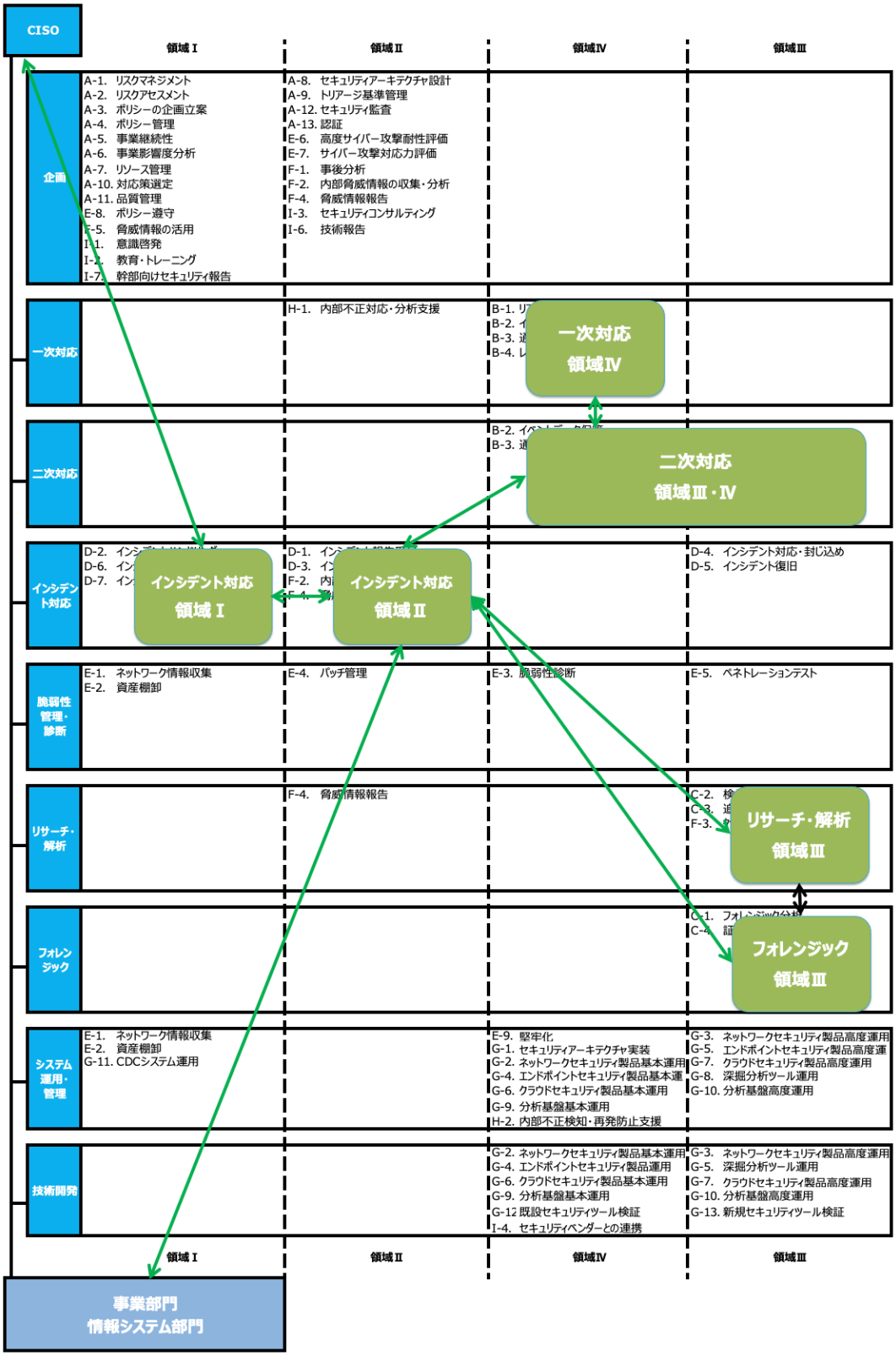


図 20 インシデントレスポンス時の関連

「図 20 インシデントレスポンス時の関連」ではカテゴリーとサービスの一覧において関連を示したが、インシデントレスポンスのフローとしてまとめると、下記「図 21 インシデントレスポンス時のフロー」のように表現できる。

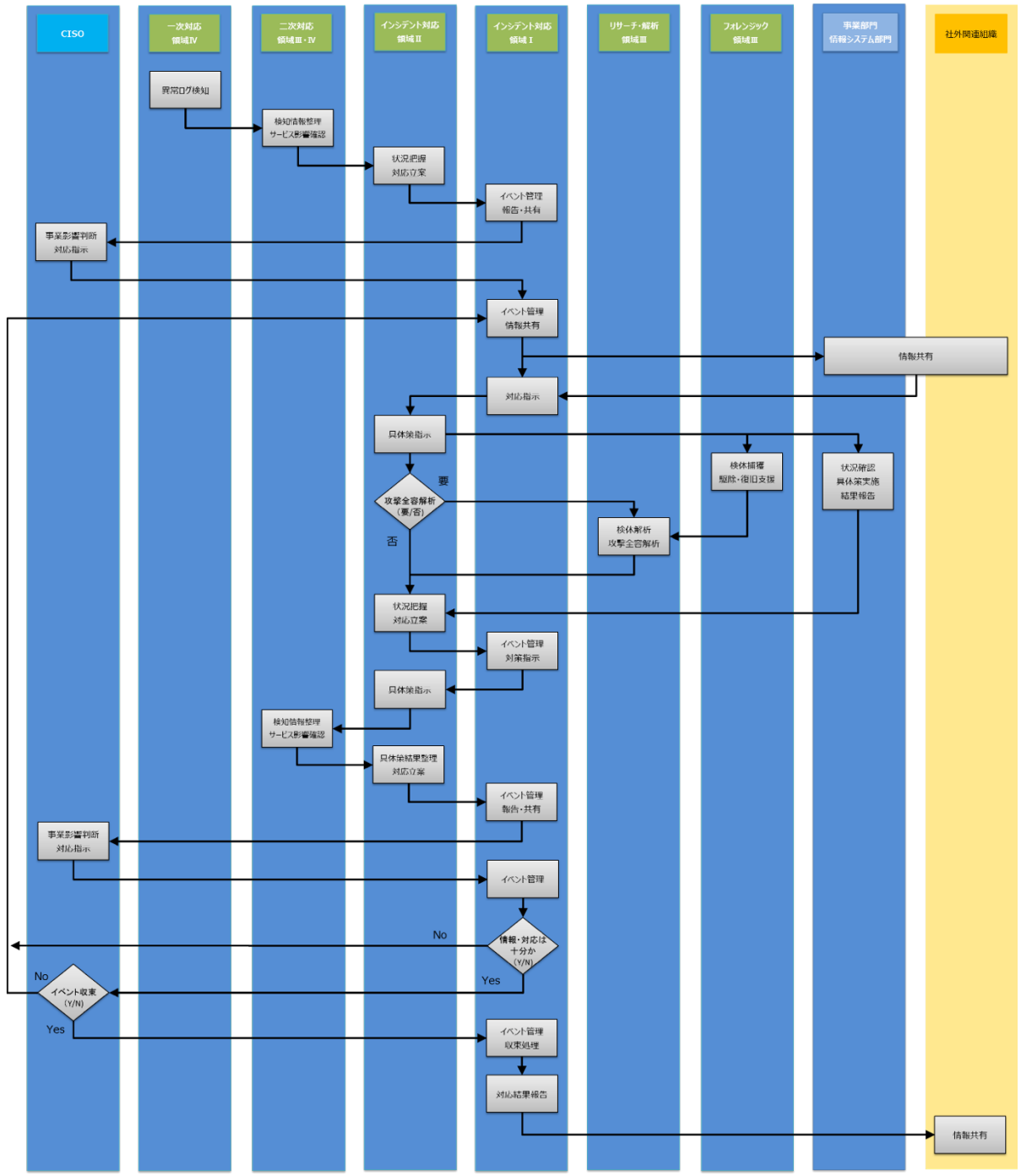


図 21 インシデントレスポンス時のフロー

インシデント対応の時のカテゴリーおよびサービスの関係である「図 20 インシデントレスポンス時の関連」や「図 21 インシデントレスポンス時のフロー」はインシデントにより細かい部分で異なるため、本書では次に述べる 2 つの例を用い図 20 や図 21 の差分を解説する。なお、例として取り上げる 2 つのインシデントは、IPA が毎年発表する 10 大脅威の組織編を参照し、以下の 2 つの脅威とした。

- クライアント端末が攻撃されたケース「ランサムウェアによる被害」
- サーバーが攻撃されたケース「ウェブサービスからの個人情報の窃取」

7.1.1. 「ランサムウェアによる被害」の例

昨今、エンドユーザーの端末のファイルを暗号化することでユーザーがファイルを利用できないようにして、もとに戻すための身代金を要求する「ランサムウェア」の攻撃が増えてきている。ここではユーザーの端末がランサムウェアに感染し、暗号化をされた場合を例にどのような関連、フローがあるか示す。

よくあるランサムウェアはメールに添付されて侵入し、ユーザーが間違えてクリックすることから感染する。かつて猛威を振るったランサムウェアとしての WannaCry はワームタイプで感染経路はネットワーク経由であったため、Windows のパッチが適用されていない端末がターゲットとなっている。平常時の対応でパッチの適用や組織内や社内のアセット管理など状況を管理できていれば防ぐことができるインシデントである。普段の取り組みによる予防が大事であるため、平常時の対応を是非実施頂きたい。平常時の対応については後述する。

- 本被害事例の特徴

ランサムウェアに感染した場合、多くは自組織の要員・社員端末やサーバーで感染が発覚し、組織内や社内からの問い合わせや報告があり、インシデント対応が進むことが想定される。このケースでは、イベントの受付から判断や管理に至る対応はベースの対応と同様である。

本ケースでは、ユーザーの端末は暗号化されて復号（暗号化の解除）ができないことが前提にあり、情報漏えいしないという部分がベースの対応と異なる部分である。

- 「カテゴリーおよびサービスの関係」・「インシデントレスポンス時のフロー」の特徴

ベースの対応を基にすると、本被害事例で特徴となる部分は「リサーチ・解析」と「フォレンジック」の実施内容である。ランサムウェアの場合では、以下の 3 点を考慮する必要がある。

- 感染経路
- ランサムウェアの動作
- 復号の可否

ランサムウェアのタイプにより情報が漏えいすることが判明した場合は、情報漏えいへの対応も考慮する必要がある。

マルウェア（例：ランサムウェア）によって図 21 からフローが変わることはない。今回のケースでは以下のカテゴリーやサービスで対応する点が特徴となる。

- 感染経路
  一次対応の領域 III や二次対応の領域 III や IV で確認する
- ランサムウェアの動作
  リサーチ・解析やフォレンジックの領域 III での確認する
- 復号の可否
  同上
  ※領域 I/II/III/IV については「図 20 インシデントレスポンス時の関連」を参照

情報漏えいがないケースではフォレンジックや証拠保全は重視されない。

一方で機密情報を暗号化する前に情報を漏えいさせておき、それを利用して金銭を要求するような 2 重脅迫のケースもある。暗号化によるデータが利用できなくなるケースとは分けて、次の例にて情報漏えいのケースを示す。

7.1.2. 「ウェブサービスからの個人情報の窃取」の例

サーバー側への攻撃については、最近では脆弱性が公開されてから攻撃が始まるまでの時間が短くなる傾向があり、脆弱性が公開されてから短時間で狙われて攻撃を受けて個人情報が漏えいするケースが少なくない。本ケースでは脆弱性情報が公開されて対策を打つ前に攻撃を受けて個人情報が漏えいした場合を例に、どのような関連、フローがあるかを示す。

- 本インシデント事例の特徴

事例として Apache Struts のように脆弱性情報が発表されて早いタイミングで攻撃が始まり、個人情報が漏えいするケースを想定する。

この場合のきっかけとしては脆弱性情報のニュースや情報から、あるいはすでにサイトが書き換えられて通報があった、ということが考えられる。場合により監視から攻撃コードが検知され、攻撃を受けていることが判明することもある。同時多発で各種情報が受付されることも考えらえる。いずれにせよ、各種情報を受け付けて、インシデントと判断してから管理を行う流れはベースの対応と同様である。

● 「カテゴリーおよびサービスの関係」・「インシデントレスポンス時のフロー」の特徴

今回のケースでは、攻撃を受けたことを前提に考察する。このため下記 3 点を特徴として解説する。

- どこからどのような攻撃を受けたか
- 何が漏えいしたか
- 被害最小化のために対策は何を行うか

対策方法や被害が特定されるまではサイトを停止する、という判断も必要である。CISO への報告や判断を早い段階で行い、迅速な対応が必要となる。

すでに攻撃が始まっている中での対策となるため、被害状況の特定と対策の実施を同時に進める対応となる。今回のケースでは以下のカテゴリーやサービスで対応行う点が特徴となる。

- どこからどのような攻撃を受けたか
  一次対応の領域 IV や二次対応の領域 III・IV にて情報確認する
- 何が漏えいしたか
  リサーチ・解析やフォレンジックの領域 III にて被害状況を特定の確認する
- 被害最小化のために対策は何を行うか
  リサーチ・解析やフォレンジックの領域 III にて攻撃全容を確認する
  「E 診断と評価」の脆弱性情報を参照し対策を判断する
  ※領域 I/II/III/IV については「図 20 インシデントレスポンス時の関連」を参照

攻撃の痕跡を確認した結果攻撃が失敗しており防御できる場合は対策を講じてサイトの継続した運用を行うと判断ができる。攻撃の影響や被害状況を判断しつつ、インシデントが収束するまでインシデントの管理と対応が継続される。

7.1.3. 「サプライチェーンでインシデント発生」の例

最近では、関連する組織や会社、取引先が攻撃を受けたことにより、自組織にも被害が発生する場合がある。関連する組織や会社、取引先それぞれのインシデントの対応については、前述の基本フローと同じである。

自組織においてのインシデント対応の範囲が、自組織内では閉じずに他組織へ影響がある場合に、どのように他組織と連携を行い、その後の見直しや評価により各組織および組織間でどのような対応を行うとよかったかを確認することがポイントとなる。

親会社子会社、グループ会社である場合、セキュリティ対応組織の組織構造は階層的になる。インシデント対応が自組織を超える場合は、権限が上位組織から移譲されている範囲で対応を行うが、自らの権限を超える場合は上位組織へエスカレーションを行い、対応を行うことになる。自らの権限の範囲内であれば、関連する会社や組織へ連絡を行い、インシデン

ト対応の範囲を広げることとなる。

取引先や委託先との関係については、親会社と子会社の関係やグループ会社との関連とは異なる。取引先や委託先との関係は権限のあるなしではなく、お互いの契約や取り決めの範囲でインシデント対応を行うこととなる。スムーズなインシデント対応を行うためには、お互いに情報や状況の共有を密に行うことが必要となる。後述の平常時の対応の範囲において、普段から準備としてインシデント対応の訓練や演習を行うことや、実際にインシデントが起きた際にはそれぞれの組織において対応ができるようにしておきたい。

7.2.　平常時の対応につて

これまで、インシデント時の対応フローについてどのようなカテゴリーおよびサービスに関連があるかを示してきた。一方、平常時はインシデントを予防するため、あるいはインシデント時の迅速な対応を行うために、実施する大切な業務がある。これら、平常時の業務の取り組み内容は「A. CDC の戦略マネジメント」の A-12 や「I. 外部組織との積極的連携」の I-7 でまとめ、成果物として経営層や関係各所へ報告される。

JPCERT/CC[20]によれば、平常時とインシデント時で行う業務は以下の「図 22　CSIRT の活動全般」のように整理される。

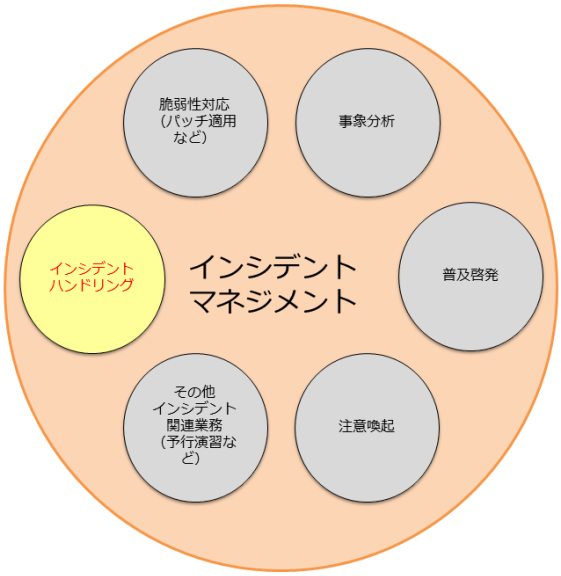


図 22　CSIRT の活動全般

この図では 6 つの業務が記載されているが、インシデント発生時の中心業務は 1 つであり、平常時に行う業務が 5 つと多く存在することがわかる。

1. 脆弱性対応（パッチ適用など）
2. 事象分析
3. 普及啓発
4. 注意喚起
5. その他インシデント関連業務（予行演習など）

これら平常時に実施する業務の実施内容と想定される成果物例を示す。

---

[20] 参考資料の図を一部改変
http://www.jpcert.or.jp/m/csirt_material/files/manual_ver1.0_20151126.pdf

7.2.1. 脆弱性対応（パッチ適用など）

普段より脆弱性情報を収集し、必要な場合はパッチの適用を各管理者に促す。
普段からどのようなサーバーが組織内や社内に存在し、どんなバージョンのソフトウェアを利用しているのか把握しておく必要がある。

ユーザーの端末側ではクライアントで利用する OS やブラウザ、プラグインソフトウェアやオフィス系の製品などの脆弱性情報に対応したかを日々チェックして、注意喚起を行う必要もある。

脆弱性の対応においては普段から状況を把握しておく必要があるため、脆弱性の情報が出て慌ててサーバーやユーザー端末の構成調査を行うということがないように日頃の準備が欠かせない。

本業務は「E. 診断と評価」のカテゴリーが主に担う。

- 成果物

例として、以下の監査結果などが挙げられる。

- 最新のシステム構成状況
- 最新のシステムパッチ適用状況
- 1 ヶ月間の脆弱性情報の注意喚起件数
- パッチ未適用システム件数

など

どの程度状況を把握しているか、どの程度迅速に脆弱性の情報を注意喚起したか、その結果どの程度最新化されたか、その結果を定量的にすることで、平常時にどの程度対応ができたか評価することができる。

7.2.2. 事象分析

日々の情報収集において、現在どのような攻撃が多いのか、どのようなテクニックが使われているのか、その他にも攻撃者の背景なども調査し、現在の脅威を分析しておく。

普段からの情報収集によりインシデントに備えとして蓄積しておくことで、過去の類似の事象から対策や対応のヒントを得ることができる。

攻撃者の背景については、国際関係での記念日や事件や政治家の発言など様々な原因が考えられるため、幅広く情報を集めることも必要ではある。普段から情報の蓄積がないと攻撃との背後関係まで思考を巡らせることが難しいため、継続した収集活動が必要である。

自組織や自社で発生したセキュリティのイベントを分析して、インシデントにはならなかったがイベント傾向からどのような攻撃が多いのか、どのような対策が効果的であるかセキュリティ対策の効果の測定の指標とすることができる。

本業務は「F. 脅威情報の収集および分析と評価」のカテゴリーが主に担う。

- 成果物

例として、定期的な脅威動向の報告を挙げることができる。

・ 自組織や自社における攻撃の検知やセキュリティイベントの件数、内容

・ 社会的に起きている攻撃の手法や傾向、その内容

現在どのような攻撃が流行しているのか、どのようなものが狙われるのか、一般的にどのような対処がされているか、後述の普及啓発にもつながる分析を行う。

7.2.3. 普及啓発

脆弱性の公表からパッチの適用や、各種攻撃の対策として何を行うべきかを普段から普及啓発を行う。

昨今はサイバー攻撃だけではなく、従業員のうっかりミスから USB メモリの紛失やノート PC の紛失、クラウドサービスの設定ミスにより、大量の個人情報漏えいなどもあり、そのようなインシデントに対応するためにも、普段からのリテラシーの向上や普及啓発が必要である。

ISMS やプライバシーマークの取得などを行なっている企業では定期的な社員教育や要員の教育の場などがあるが、そうでない企業でも IPA などで一般的に公開されているコンテンツを利用して社員の意識向上などに努めたい。

本業務は「I. 外部組織との積極的連携」の I-1, 2, 3 のサービスが主に担う。

- 成果物

どの程度の間隔で、どのような内容を、どんな社員や要員を対象にどんな普及啓発を行なったか、必要な層に必要な情報を提供できたのかを指標にし、普及啓発のパフォーマンスを示すことができる。

例えば、メールを開く必要がある職種や管理職や経営層に向けたものと、一般的な業務でメールをあまり活用していない社員や要員では普及啓発する内容が異なるはずである。同様にシステムを管理している層に対しては、パッチの管理やシステムへの攻撃の傾向やその対策が必要な情報である。

7.2.4. 注意喚起

前述の脆弱性対応や事象分析を行なっていると、今何に注意をすべきか、どう対処すべきかの注意喚起を行い、インシデントになる前に対処を行うことができる。

サーバーやシステムの管理者に向けては、公開されているサーバーに関する脆弱性への対処方法や世界的に流行している攻撃への対処方法を注意喚起することが有効である。

また、エンドユーザーに向けては、利用しているソフトウェアのアップデートの情報の提供やバラマキ型、標的型の攻撃メールなどへの注意喚起が有効である。

注意喚起については、JPCERT/CC や IPA、警察庁の注意喚起を基に行う方法もあるが、普段からの情報収集により注意喚起時にはその内容を迅速に把握して注意喚起が行えるように日々準備をしておきたい。

本業務は「E. 診断と評価」および「F. 脅威情報の収集および分析と評価」のカテゴリーで集めた情報を活用し、「I. 外部組織との積極的連携」の I-1, 2, 3 のサービスが主に担う。

- 成果物

以下を例として挙げることができる。

- 今月の注意喚起件数
- 注意喚起により対処できたシステム数、ユーザー数

注意喚起をした結果、どの程度防御に貢献できたのか、それによりインシデントを未然に防ぐことができたのかがポイントとなる。

7.2.5. その他インシデント関連業務（予行演習）

ここではそれ以外の関連業務となるが、どれにも当てはまらない予行演習や人材などのリソース管理や育成といったものが割り当てられる。

予行演習では、よく標的型メール攻撃の対処として偽メールを送信する、といったサービスを購入して実施するケースがあるが、これはエンドユーザーに向けた訓練である。

セキュリティの対応全体を訓練するためには、インシデントが起きたと仮定し、どのような対処を行うかの手順の確認や、経営層も含めたフローや判断の確認を実施する必要がある。

CSIRT 向けの演習サービスや実践的サイバー防御演習(CYDER)や、Hardening Project の競技など、全体として対応ができているかを訓練するという方法もある。

本業務は、「E. 診断と評価」の E-6, 7 や「I. 外部組織との積極的連携」の I-5 のサービスが主に担う。

その他にも、リソースの管理やセキュリティ対応に関する品質管理など含めた、全体の方針を管理していくことも必要となる。平常時にこそ「A. CDC の戦略マネジメント」の営みを計画的に実施することが重要である。

- 成果物

予行演習を例に取るならば、対象者と演習や訓練の内容により、どのケースでどの範囲までが演習や訓練できたかを指標とすることができる。

演習や訓練の範囲が足りない場合は、計画的にどこまでを対象者として行うか、どのような内容で行うかを決めて順次実施をしたい。

8. セキュリティ対応組織のアセスメント

ここではセキュリティ対応組織を客観的に評価するアセスメントについてまとめる。

8.1. アセスメントの目的

セキュリティ対応組織をアセスメントで測定することによって以下を明らかにすることが目標となる。

- 現状における、セキュリティ対応組織の「強み」と「弱み」
  - 組織の現状として、カテゴリー・サービスが充足しているもの、不十分なものを明らかにすることにより、これまでの取り組みが功を奏しているアピールポイントと、短期サイクルでの改善ポイントの洗い出しを行う。

- 将来的に達成したいセキュリティ対応組織モデル実現に必要となるポイント
  - 中長期的な目標を定めることによって、短期サイクルでの改善だけでは解決できないような、長期サイクルとしての見直しが必要となる抜本的な組織改善ポイントを可視化する。

これらが「A-12 セキュリティ監査」で測定され、「A-1 リスクマネジメント」の中で、セキュリティ対応組織運営に活用されることが重要な目的となる。

X.1060/JT-X1060 では構築プロセスの最後のフェーズで選択したサービスごとにこのアセスメントにより「現状(As-Is)」のスコアと目標とする「あるべき姿(To-Be)」のスコアを確認し、サービスポートフォリオを作成する。

本アセスメントは構築プロセスだけで利用されるのではなく、評価プロセスの中でも利用される。構築プロセスの際に目標とする「あるべき姿(To-Be)」のスコア定めて、評価プロセスの際にサービスポートフォリオの状況と比較し、次の構築プロセスでの改善に活用されるようになっている。

8.2. アセスメントの流れ

アセスメントに当たっては、下記の流れに沿って行うとスムーズである。

① 現在のセキュリティ対応組織がどの組織パターンに近いのか、「6.3 セキュリティ対応の組織パターン」を参考に決定する。組織内で意見を合わせるとよい。
② 中長期的に目指すモデルとなりうる組織パターンはどれか、「6.3 セキュリティ対応の

組織パターン」を参考に決定する。組織内で意見を合わせるとよい。

③ ①の組織パターンにおける各サービスについて、その実行レベル（後述）を評価する。各カテゴリー・サービスの中心を担う者と協力しながら評価するとよい。

④ ③の評価内容から、評価が高いカテゴリーを「強み」として、評価が低いカテゴリーを「弱み」として抽出する。

⑤ ③の評価内容と②のモデルパターンでの差分が大きいものを中長期的な改善ポイントとして抽出する。

8.3. 各サービスの実行レベル

アセスメントの客観的な指標として、各サービスの実行レベルを定義する必要がある。X.1060/JT-X1060 では、指標として下記の通り定義している。

- 自組織でそのサービスを実施する場合（インソース）
  - 明文化された運用は CISO など権限ある組織長に承認されている（+5 点）
  - 運用が明文化されており、担当者と交代して他者が業務を実施できる（+4 点）
  - 運用が明文化されておらず、担当者に代わりに他者が臨時で一部の業務を代行できる（+3 点）
  - 運用が明文化されておらず、担当者が業務を実施できる（+2 点）
  - 実施できていない（+1 点）
  - インソースでの実装を検討したものの、結果として実施しないと判断した（評価対象外）

- 専門組織でそのサービスを実施する場合（アウトソース）
  - サービス内容と得られる結果を理解でき、想定通り（+5 点）
  - サービス内容と得られる結果を理解できているが、想定未満（+4 点）
  - サービス内容、得られる結果のいずれかが理解できていない（+3 点）
  - サービス内容と得られる結果を理解できていない（+2 点）
  - 結果や報告を確認できていない（+1 点）
  - アウトソースでの実装を検討したものの、結果として実施しないと判断した（評価対象外）

ここでのアセスメントは、持続可能な組織を目指すために、現状と目標を明確にし、継続的に改善ができるようにするものである。指標値の考え方としては、自分たちで実施するインソースと、外部に委託するアウトソースの 2 つの考え方がある。

インソースにおいては、属人的ではなく組織的な対応を行えているかどうかを評価ポイントとしている。セキュリティ人材が限られている組織が多いことが想定されるが、個人に依存したセキュリティ対応は、その個人が不在時あるいは転職などによる人材喪失時に全く機能しなくなる恐れがあるため、業務を組織的に行えることが重要である。

組織の状況や目指す姿によって目標とするスコアは異なるはずである。例えば、組織として予算や人的リソースの観点から属人的な状況を許容しているのであれば、スコアが 2 点や 3 点であっても問題はない。一方で、属人からの脱却を目指しているにもかかわらず、スコアが 3 点以下で改善されない状況は問題があると言える。闇雲に全て 5 点を目指すことよりも、組織の実態にあった目標設定と、妥当な現状評価をスコアとして定め、そのギャップを可視化し、一つずつしっかりと改善していくことの方が重要である。

アウトソースにおいては、受けているサービスを理解し、使いこなせているかを重要視している。これは、いわゆる「丸投げ」の状態になっていないかチェックするためである。アウトソースに関しては、一般的に、サービス契約の締結時にはそのサービス内容等を意識できているが、時間が経つにつれ、認識が薄れたり、契約時の検討メンバーが離脱したりと、詳細不明になってしまうことがある。アウトソーサーから得られる結果を運用に生かせているうちはまだ問題はないが、それができなくなると、アウトソースしている意味が希薄化し、コストに見合わない営みとなってしまう恐れがある。

なお、インソース、アウトソースに共通している点として、組織的な判断の下、意図的に「実施しない」と決定されたカテゴリーについては成熟度の評価対象外としている。セキュリティ対応以外の形でリスクを移転、回避できるのであれば、それでも問題はない。ビジネスリスクとセキュリティ対応コストを天秤にかけ、リスクを許容する判断も現実にはあり得る。ただし、いずれの場合においても、状況の変化による見直しを柔軟に行えるよう、その判断を行った根拠とその証跡はしっかりと残しておく必要がある。

8.4. セキュリティ対応組織サービスポートフォリオシート

本書では構築プロセスにおいて、サービスポートフォリオを作成している。サービスポートフォリオのひな形のシートを付録とするため、ご活用いただきたい。

9. おわりに

本書では、セキュリティ対応組織に求められるカテゴリー、サービス、アセスメントについてまとめた。これらのカテゴリーやサービス全てを満たす組織を作り上げることは非常に難しく、現実的には段階を踏んで少しずつ形作られるものである。本書を通じて、今何ができていて何が足りないのか、これから何をすべきなのか、その把握に少しでも役立てていただければ幸いである。

自組織の「できていること、できていないこと」、あるいは「できているレベル」を認識することはセキュリティ対応能力を向上させるうえで大切なことであり、ぜひ本書を活用し、客観的な自組織の状況を把握してみてほしい。また、今後もセキュリティを取り巻く環境は変化しつづけることは容易に想像できるため、本書のアップデートも継続的に行っていきたい。

日本セキュリティオペレーション事業者協議会 （ISOG-J）は引き続き、セキュリティオペレーション事業者の連携によって生まれるノウハウやナレッジを広く提供していく。

参考文献

- Recommendation X.1060 “Framework for the creation and operation of a cyber defence centre” (ITU-T)
  - https://www.itu.int/rec/T-REC-X.1060-202106-I
- JT-X1060 「サイバーディフェンスセンターを構築・運用するためのフレームワーク」(一般社団法人　情報通信技術委員会(TTC))
  - https://www.ttc.or.jp/document_db/information/view_express_entity/1423
- サイバーセキュリティ経営ガイドライン　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(経済産業省)
  - https://www.meti.go.jp/policy/netsecurity/mng_guide.html
- SOC の役割と人材のスキル v1.0 (ISOG-J)
  - http://isog-j.org/output/2016/SOC_skill_v1.0.pdf
- Ten Strategies of a World-Class Cybersecurity Operations Center (MITRE)
  - https://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center

付録 カテゴリーとサービスリストの詳細

カテゴリー

セキュリティ対応組織の実行サイクルは、主に以下の９つのカテゴリーによって実現される。

A. CDC の戦略マネジメント

（第 2.1 版では「セキュリティ対応組織運営」）

セキュリティ対応するにあたって、取り扱うべき事象や対応範囲、トリアージ（対応優先度）基準などの、セキュリティ対応における全体方針を管理したり、必要となるリソース計画を行ったりするカテゴリーである。セキュリティ対応の安定的な運営を目的とする。

B. 即時分析

（第 2.1 版では「リアルタイムアナリシス（即時分析）」）

NW 装置やサーバー、セキュリティ製品など、各種システムからのログやデータを常時監視し、分析を行うカテゴリーである。リアルタイムに脅威を発見し、迅速で適切なインシデント対応へ繋げることを目的とする。

C. 深掘分析

（第 2.1 版では「ディープアナリシス（深堀分析）」）

被害を受けたシステムの調査や、漏えいしたデータの確認、攻撃に利用されたツールや手法の分析など、インシデントに関連するより深い分析を行うカテゴリーである。インシデントの全容解明と影響の特定を目的とする。

D. インシデント対応

（第 2.1 版と同じ）

リアルタイム分析結果や脅威情報を基に、脅威の拡散抑止、排除のための具体的な対応を行うカテゴリーである。関係者との調整、報告なども含め、システムおよびビジネスへの影響最小化を目的とする。

E. 診断と評価

（第 2.1 版では「セキュリティ対応状況の診断と評価」）

守るべきシステムに対する脆弱性診断や、インシデント対応訓練およびその評価を行うカテゴリー。セキュリティレベルの向上と共に、分析やインシデント対応の負荷削減へ繋がるよう、インシデントの予防、インシデント対応に関する練度の向上を目的とする。

F. 脅威情報の収集および分析と評価

（第 2.1 版と同じ）

ネット上に公開されている、脆弱性や攻撃に関する脅威情報（外部インテリジェンス）を収集したり、リアルタイム分析やインシデント対応時の情報（内部インテリジェンス）を取り扱ったりするカテゴリーである。リアルタイム分析の精度向上やインシデント対応、セキュリティツールの改善へ繋げることを目的とする。

G. CDC プラットフォームの開発・保守

（第 2.1 版では「セキュリティ対応システム運用・開発」）

セキュリティ対応するにあたって必要となるシステム（セキュリティ製品、ログ収集データベース、運用システムなど）の管理、改善や新規開発を行うカテゴリー。他のカテゴリーが円滑かつ持続的に活動可能な状態を実現することを目的とする。

H. 内部不正対応支援

（第 2.1 版では「内部統制・内部不正対応支援」）

内部統制の営みで必要となる監査データの収集や、内部不正に関する対応支援を行うカテゴリー。内部統制そのものや、内部不正捜査そのものは内部統制部門や法務部門が主体となって対応することが一般的であるが、ログ提供や分析によりその対応の補助し、解決の支援を行うことを目的とする。

I. 外部組織との積極的連携

（第 2.1 版と同じ）

セキュリティ対応組織ではない組織（社外、社内問わず）との連携を行うカテゴリー。波及的なセキュリティレベル向上を目指すとともに、セキュリティ対応組織の存在価値を高め、自組織のさらなる発展、強化を目的とする。

サービスリスト

ここでは先の９つのカテゴリーについてそれぞれどのようなサービスを持つか説明をする。

A. CDC の戦略マネジメント

A-1. リスクマネジメント

（第 2.1 版の「A-1. 全体方針管理」が詳細化された）

X.1060/JT-X1060 での概要は以下である。

「リスクマネジメント」サービスは、リスクに対して組織を方向づけ、コントロールできるよう、A-2 から A-13 を含む統括的な活動を実現する。

A-2. リスクアセスメント

（第 2.1 版の「A-1. 全体方針管理」が詳細化された）

X.1060/JT-X1060 での概要は以下である。

「リスクアセスメント」サービスは、組織の資産や脅威、セキュリティ対策の観点から、組織のリスクレベル把握を実現する。

A-3. ポリシーの企画立案

（第 2.1 版の「A-1. 全体方針管理」が詳細化された）

X.1060/JT-X1060 での概要は以下である。

「ポリシーの企画立案」サービスは、具体的なセキュリティポリシーの定義や、ガイドラインの作成に関するすべての活動を支援する。

ポリシーは CISO によって決められるものである。CDC やセキュリティ統括における本サービスではその活動を支える役割としての企画立案である。

A-4. ポリシー管理

（第 2.1 版の「A-1. 全体方針管理」が詳細化された）

X.1060/JT-X1060 での概要は以下である。

「ポリシー管理」サービスは、ポリシーや組織の規定を評価して定期的に見直しや、新たな外部要件（例えば、規制やガイドライン）への準拠を実現する。

評価プロセスにおいてサービスポートフォリオを見直す際には、経年劣化した規定類の更改も考慮をする必要がある。カテゴリーF「脅威情報の収集および分析と評価」で得られた脅威情報の整理や分析の結果から、規定類を見直すこともできる。見直した結果から、次の構築プロセスにおいて改善された形でポリシーを活用できる。

A-5. 事業継続性

（第 2.1 版の「A-1. 全体方針管理」が詳細化された）

X.1060/JT-X1060 での概要は以下である。

「事業継続性」サービスは、組織の事業継続計画の実現や実行が正しく行われるために必要な経営上の機能を支援する。

A-6. 事業影響度分析

（第 2.1 版の「A-1. 全体方針管理」が詳細化された）

X.1060/JT-X1060 での概要は以下である。

「事業影響度分析」のサービスは、様々なイベントやシナリオから起こり得る影響の体系的なアセスメントを実現する。このサービスは、発生しうる損失の規模を組織が理解するのに役立つ。直接的な金銭的損失だけでなく、利害関係者の信頼喪失や風評被害など、その他の影響も対象となる場合もある。

A-7. リソース管理

（第 2.1 版では「A-6. リソース管理」「I-4. セキュリティ人材の確保」）

X.1060/JT-X1060 での概要は以下である。

「リソース管理」サービスは、各種セキュリティ活動を支えるリソース（人、予算、システムなど）計画と、各サービスへの適切な割り当てを実現する。

セキュリティ対応するに当たり必要となるリソース（人員、予算、システムなど）の計画を行い、各カテゴリーに適切に配分する。

人事組織と連携し、セキュリティ人材の確保を行う。優秀な人材を確保するための登用制度、人材を手放さないためのキャリアパス構築、スキルアップのためのカリキュラムの見直しや新設を検討する。他部門との人材交流による全社的なセキュリティレベルの向上なども視野に入れる。

A-8. セキュリティアーキテクチャ設計

（第 3.0 版より追加）

X.1060/JT-X1060 での概要は以下である。

「セキュリティアーキテクチャ設計」サービスは、ビジネスをセキュアにするためのアーキテクチャの確立を実現する。

システムの設計やビジネスプロセスの制約（例えば、 サプライチェーン）を考慮した各種セキュリティ対策をまとめ、CDC のプラットフォーム（カテゴリーG にあるような）の開発や維持を実現する。

A-9. トリアージ基準管理

（第 2.1 版では「A-2. トリアージ基準管理」）

X.1060/JT-X1060 での概要は以下である。

「トリアージ基準管理」サービスは、全社のポリシーで合意された範囲内で発覚した事象（例えば、インシデント、脆弱性の発覚、脅威情報の発見など）へのトリアージ（対応の優先順位）基準作成を実現する。

全体方針として取り決められた対応範囲において発覚する事象への具体的なトリアージ（対応優先度）基準を取り決める。大きくは３つの基準を事前に定める必要がある。

- インシデント発生時のトリアージ基準
  想定される攻撃の種別、攻撃進行度や危険度[21]、アセットの重要度などによる分類を行う。
- 脆弱性発見時のトリアージ基準
  脆弱性を突かれた場合に想定される被害、攻撃の容易性、アセットの重要度などによる分類を行う。
- 脅威情報発見時のトリアージ基準
  組織内部で収集した、あるいは組織外部から報告された脅威情報について、攻撃の進行度や想定被害、アセットの重要度などによる分類を行う。

いずれの場合も「インシデントとしない基準」も意識して定義すると、判断のぶれを軽減できる。

A-10. 対応策選定

（第 2.1 版では「A-3. アクション方針管理」）

X.1060/JT-X1060 での概要は以下である。

「対応策選定」サービスは、A-9 のトリアージ基準に対する対応策や、各種のセキュリティ策に最も適切な技術の選定活動を支援する。

「A-9 トリアージ基準管理」に対し、それぞれの分類での具体的な対応（アクション）の方針を取り決める。トリアージ基準に相対させる形で、大きくは３つの方針を事前に定める必要がある。

- インシデント発生時のアクション

[21] 攻撃の種別のネーミングや危険度は一意に定まった定義がなく、セキュリティ製品やサービスごとに異なるため、複数の製品・サービスを導入する際は整理が必要となる。

- 脆弱性発見時のアクション
- 脅威情報発見時のアクション

ここで取り決めたアクションは、システム管理者など、実際に対処を行う関係者との共通認識とし、トリアージ基準に該当する際にただちにアクションに移れるようにしなければならない。

A-11. 品質管理

（第 2.1 版では「A-4.品質管理」）

X.1060/JT-X1060 での概要は以下である。

「品質管理」サービスは、セキュリティ活動の品質に問題がないかどうか、ビジネスに悪影響を与えていないかどうか（ユーザビリティ、生産性など）の一定期間（1 週間、1 ヶ月など）ごとの点検を実施する。

１週間あるいは１か月など、ある程度の期間において行われた各種の分析や対応について棚卸をし、対応品質に問題が無かったか確認する。対応先となった組織からのフィードバック（問い合わせ内容、意見など）も積極的に取り入れ、問題があった場合には是正しつつ、より高い品質での対応が行われるよう改善する。

それぞれのサービス単位での品質だけではなく、セキュリティ対応組織全体の対応について、事業への生産性へ悪影響を及ぼしていないか、あるいは事業を優先させるために実効的なセキュリティ活動が損なわれていないかという観点も必要である。

組織の中に複数のセキュリティ対応組織が存在している、グループ会社などでセキュリティ対応組織が階層構造になっているなどの場合も、全体の活動としてどうなっているかを考える必要がある。

本サービスでは「I-3.セキュリティコンサルティング」にて受けた相談における基準による組織的な判断や改善が必要な事項のフィードバックを受ける。

A-12. セキュリティ監査

（第 2.1 版では「A-5. セキュリティ対応効果測定」）

X.1060/JT-X1060 での概要は以下である。

「セキュリティ監査」サービスは、組織が特定の拠点や期間において、セキュリティポリシーや統制をどのように実現しているかの体系的かつ定量的な監査を実現する。CDC 関係者は、必要な情報の統制の実施状況の証拠を提供するために、監査活動に間接的に関与する。

監査に関連して、ここではセキュリティ対応がもたらす効果も測定する。インシデント対応数や、セキュリティ装置による攻撃の遮断数、脆弱性管理の結果など、各カテゴ

リーからアウトプットを収集し、成果として取りまとめる。

A-13. 認証

（第 3.0 版より追加）

X.1060/JT-X1060 での概要は以下である。

「認証」サービスは、組織がさまざまな規格や認証スキームの適合に向けた活動を支援する。

組織における「認証」については、どの範囲まで行うのか、何を取得するのか、セキュリティに関するものだけにするか、他の認証も取得するかなどについてはそれぞれの方針や決定よるものであるため、それぞれの組織次第となる。

B. 即時分析

B-1. リアルタイム監視

（第 2.1 版では「B-1.リアルタイム基本分析」「B-2. リアルタイム高度分析」「H-1. 内部統制監査データの収集と管理」）

X.1060/JT-X1060 での概要は以下である。

「リアルタイム監視」サービスは、ログやネットワークフローからシステムの状態や不審な動きを監視・分析し、インシデントやイベントに応じて必要な情報を収集し、トリアージを支援する。

主に下記のようなログを監視し、リアルタイムに分析を行う。

- ファイアウォールなどのネットワーク装置からのログやネットフロー、NDR(Network Detection and Response)などのネットワークに関するログ
- IPS/IDS,WAF(Web Application Firewall), DBFW(DataBase FireWall),CASB(Cloud Access Security Broker)などのセキュリティ装置からのログ
- Web サーバーなどのアクセスログ
- AD や DNS などの各種システムからのログ
- EDR(Endpoint Detection and Response)やアンチウイルスソフト、資産管理などのユーザー利用端末に関するログ
- XDR(Extended Detection and Response), UEBA(User and Entity Behavior Analytics)などの複合的なアクティビティに関するログ
- クラウド基盤などから取得される外部のプラットフォームのログ

多種多様なログの取り扱いが必要になるため、ログを正規化し、同一のデータベースに格納したり、SIEM を利用したりして、効率的な分析を実現する必要がある。取得可能な場合はネットフローの情報も扱う。

ログやネットフローの情報などの基本分析だけでは影響度やその内容が把握しきれない場合に、より詳細な分析を行う。例えば、専用のネットワークキャプチャ装置やセキュリティ装置に付随の機能で検知に関わるパケットキャプチャを取得したり、エンドポイントやサーバーから必要なデータを即時取得したりして、より多くの証拠を基に、正確な状況把握、影響判断を行う。

内部統制で必要となる監査データについて、収集すべきログを定義し収集する。必要に応じて、定型的なフォーマットに落とし込み、定期的なレポートとして関連組織が利用できるようにする。ここでの内部統制や監査の対象は、社内や組織全体の内部統制や監査である。そのため、CDC やセキュリティ統括、SOC や CSIRT といったセキュリティ組織の活動自体も対象となる。

B-2. イベントデータ保管

（第 2.1 版では「B-3. トリアージ情報収集」）

X.1060/JT-X1060 での概要は以下である。

「イベントデータ保管」サービスは、セキュリティ監視や分析で収集されたイベントを集約し、一元的な保管を実現する。

リアルタイム分析やパケットキャプチャ分析で収集しているデータだけでトリアージの判断を行えないケースが出てくる。その場合、「E 診断と評価」の情報を参考にしたり、普段扱っていないログソースからさらに情報を収集したりする。自組織にそのログソースへのアクセス権限が無く、他組織との調整が必要な場合は、カテゴリーD のインシデント対応のサービスとして扱われることもある。

B-3. 通知・警告

（第 2.1 版では「B-4. リアルタイム分析報告」）

X.1060/JT-X1060 での概要は以下である。

「通知・警告」サービスは、情報資産に対する潜在的なリスクがハイライトされたイベント（セキュリティ機器の警告、セキュリティ速報、脆弱性、拡散する脅威など）を、関係する内部で役目を持ったものへの通知を実現する。

リアルタイム分析によって判明した、被害端末の情報、攻撃手法、攻撃経路、情報漏えいの有無、影響度、すぐに行うべき短期的な対処策などを取りまとめ、ドキュメント化する。インシデント対応の引き金となるレポートであるため、対応に必要となる情報は最低限含まれるよう、項目は事前に取り決めておくことが望ましい。ただし、この時

点での分析で全てが明確になるわけではなく、不明なものは不明と明記し、その他のカテゴリーで補完する必要がある。

B-4. レポート問い合わせ対応

（第 2.1 版では「B-5.分析結果問合受付」）

X.1060/JT-X1060 での概要は以下である。

「レポート問い合わせ対応」サービスは、分析に関するデータやレポートに関する問い合わせ対応を実現する。

分析に関するデータや提供したレポートについての問合せ対応を行う [22]。電話やメール、ウェブサイト、チャットツールや Web 会議システムでやり取りが行われる。応対の履歴をしっかり残すため、電話に限らず Web 会議を含む音声系は録音やシステムを活用した文字起こしを行い、内容も改めてメールやウェブサイトに書き残すことが推奨される。

C. 深掘分析

C-1. フォレンジック分析

（第 2.1 版では「C-1. ネットワークフォレンジック」「C-2. デジタルフォレンジック」）

X.1060/JT-X1060 での概要は以下である。

「フォレンジック分析」サービスは、何が発生したのかの判断を促進するため、セキュリティ関連資産から収集された、あるいはイベントに関連したデジタル証跡の分析を実現する。

リアルタイム分析は即時性が求められるため、全てのネットワークログやパケットキャプチャを分析できていない場合があり、改めてそれらの分析を行う。また、リアルタイム分析の対象ではないログやパケットキャプチャがある場合には、合わせて分析対象とし、ネットワーク上で見られた挙動を明らかにする。

必要に応じて、ネットワークだけでなく、被害に遭った端末やサーバーの HDD/SSD、メモリ、外部記憶媒体などに保持されたデジタルデータ全般の分析を行う。ネットワーク上の挙動だけでは判断しにくい攻撃者が標的とした情報の特定、その漏えいの成功可否などを明らかにする。

C-2. 検体解析

（第 2.1 版では「C-3. 検体解析」）

[22]問合せ対応は集約効果が高いため、基盤運用の一時切り分けなど、他のカテゴリーにおけるフロント業務の窓口としても活用される場合も多い。

X.1060/JT-X1060 での概要は以下である。
「検体解析」サービスは、フォレンジックの過程で発見された、攻撃者によって設置されたマルウェア、プログラムやスクリプトの解析を実現する。

各フォレンジックの過程において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能を解析する。実際に動作させながら解析を行う動的解析や、リバースエンジニアリングによる静的解析などを組み合わせて実施する。

C-3. 追及・追跡

（第 2.1 版では「C-4.攻撃全容解析」）
X.1060/JT-X1060 での概要は以下である。
「追及・追跡」サービスは、環境に対するあらゆる攻撃の発生源を追及・追跡を実現するもので、これはセキュリティインシデントの抑制や分析の重要な成功要因となる。内部と外部の両方の攻撃者を追及・追跡できる能力（例えば、サイバーアトリビューション）があれば将来の攻撃を事前に防ぐことができる。

フォレンジックや検体解析の結果をもとに、攻撃活動の全容を明らかにする。分析材料が不足している場合には、公開されている脅威情報や「F-3.外部脅威情報の収集・評価」で得られた情報の活用なども参考に、仮説を組み込みながら、情報を補強していく。十分な証拠がそろっている場合には、攻撃者のプロファイル（所属組織、組織の活動目的など）の想定も試みる。

C-4. 証拠収集

（第 2.1 版では「C-5. 証拠保全」）
X.1060/JT-X1060 での概要は以下である。
「証拠収集」サービスは、扱われたインシデントに関係する電磁的証拠を収集・保全し、証拠としての妥当性の維持を実現する（証拠保全の一貫性）。

サイバー犯罪捜査や法的措置を行う可能性がある場合には、分析の各過程において電磁的証拠の保全を行う。

D. インシデント対応

D-1. インシデント報告受付

（第 2.1 版では「D-1. インシデント受付」）
X.1060/JT-X1060 での概要は以下である。

「インシデント報告受付」サービスは、運用における分析報告の受け付けを実現する。報告の受領は組織内部からだけではなく、外部の組織からの場合もある。

主には運用からの分析報告を受け付ける。

ただし、社内の別組織からの申告や社外の組織からの通報を受ける可能性がある。社内の別組織からの受付窓口としては、メールの他にはチャットツールやWeb会議システムなどいくつかの手段を確保し、周知をしておく。社内の他に社外からも受け付けられるようにするには専用のメールアドレスを準備するなどして、社内外に広く浸透させる必要がある。十分なリソースが無い場合には、「B-4 レポート問い合わせ対応」を活用してもよい。なお、外部からのインシデント受付は、WHOISデータベースに登録してあるメールアドレス等が通報先として利用されることもあるため、登録情報は常に更新し、セキュリティ対応組織へ連絡内容が届くように（別の組織が受け付けている場合は内容が共有されるように）する。

D-2. インシデントハンドリング

（第2.1版では「D-2. インシデント管理」）

X.1060/JT-X1060での概要は以下である。

「インシデントハンドリング」サービスは、受け付けたインシデントに対処し、D-3からD-7の活動の調整を実現する。

トリアージにより対応することが決まったインシデントについて、「A-9 トリアージ基準管理」での方針に従い対応されているか、インシデント分析の進捗状況など、対応状況の管理を、インシデント対応が完了するまで行う。

D-3. インシデント分類

（第2.1版では「D-3. インシデント分析」）

X.1060/JT-X1060での概要は以下である。

「インシデント分類」サービスは、発生したインシデントとその原因の種別について共通理解を促すために、インシデントの分類を実現する。

受け付けたインシデント情報を、「A-9 トリアージ基準管理」に則り、対応可否および優先度を判断する。判断の材料が少ない場合には、「B-2 イベントデータ保管」と連携する。トリアージ基準に該当しないような判断を行った場合には、「A-9 トリアージ基準管理」へフィードバックする。判断後は、インシデントの全体像、直接的なビジネスへの影響（サービス停止に伴う損失、復旧/対策に必要となったコスト）や間接的な影響（社会的信用低下、業務効率低下）を究明する。その暫定対処策、最終的な再発防

止策の検討も行う。情報の不足があり、分析が不十分な場合は「C 深掘分析」と密に連携する。

D-4. インシデント対応・封じ込め

（第 2.1 版では「D-4. リモート対処」「D-5. オンサイト対処」）

X.1060/JT-X1060 での概要は以下である。

「インシデント対応・封じ込め」サービスは、インシデントがすべてのリソースに広がるなど、被害や影響が拡大する前の封じ込めを実現する。

実際のインシデント対応に当たり、優先度の低いインシデントにおいて、電話やメール、チャットツールや Web 会議システムなどで対応を行う。厳格な証拠保全が求められない場合には、リモートアクセス（リモートデスクトップや SSH など）で対処を完了させる。対処結果については「B 即時分析」へ必ず共有し、不要な分析、インシデント化が行われないようにする。

実際のインシデント対応に当たり、リモート対処では解決できない場合、あるいは厳格な証拠保全が求められる場合は、専門員が対処の必要となるシステムが存在する物理的拠点まで出向いて対応を行う。対処結果については「B 即時分析」へ必ず共有し、不要な分析、インシデント化が行われないようにする。

D-5. インシデント復旧

（第 3.0 版より追加）

X.1060/JT-X1060 での概要は以下である。

「インシデント復旧」サービスは、対象となるシステムを通常状態へ回復することを支援する。

D-6. インシデント通知

（第 2.1 版では「D-6. インシデント対応内部連携」「D-7. インシデント対応外部連携」）

X.1060/JT-X1060 での概要は以下である。

「インシデント通知」サービスは、インシデント対応チームやその他関連するグループに対して、インシデント発生の伝達を実現する。

内部関係者との連携、調整を行う。内部関係者とは、経営層、関連する社内他部門（システム部門や法務部門など）、および社外の協力組織（開発ベンダー、サービス提供事業者など）が挙げられ、主に「インシデントの全容解明を共に行うべき関係者」を指す。インシデントに関する報告や、情報共有、分析に必要なデータの共有などの調整を行う。

外部関係者との連携、調整を行う。外部関係者とは、監督官庁、社外の取引関係組織、エンドユーザーが挙げられ、主に「インシデントによって影響を与えてしまう関係者」を指す。インシデントに関する説明や、被害状況の確認、具体的な被害内容の収集などの調整を行う。

D-7. インシデント対応報告

（第 2.1 版では「D-8. インシデント対応報告」）

X.1060/JT-X1060 での概要は以下である。

「インシデント対応報告」サービスは、対応が完了したインシデントのレポートの完成と報告を実現する（対策の試みが長期化する場合は、CDC の戦略マネジメント（カテゴリーA）に引き継がれる）。インシデント対応中に CDC 関係者が現状報告を必要とする場合は、中間報告を行う。

インシデント対応によって解明した、影響内容、発生要因、実施した対処および根本対策方針などを取りまとめ、ドキュメント化する。対策の取り組みが長期化する場合には「A-1 リスクマネジメント」に引き継いで管理を行う。

内部向け[23]の報告書と、外部向けの報告書は粒度が異なるため、それぞれ作成する。この報告書の完成・配布によって、インシデント対応としては完了（クローズ）となる。インシデント対応の報告が完了し、その後の組織における手順やツールの見直しや改善が必要な場合は「F-1.事後分析」で対応を実施する。

E. 診断と評価

E-1. ネットワーク情報収集

（第 2.1 版では「E-1. ネットワーク情報収集」）

X.1060/JT-X1060 での概要は以下である。

「ネットワーク情報収集」サービスは、保護対象となるネットワーク構成の概要の収集を実現する。

守るべき対象のネットワーク構成の概要を把握する。詳細な構成を全て完璧に理解するということではなく、各種ネットワーク装置とセキュリティ装置との位置関係やその種類、セキュリティ装置がインラインなのかそうではないのか、といったことがすぐに調べられるようにしておく。把握するにはシステム部門などの別組織との連携が必須となる。脆弱性管理だけでなく、分析やインシデント対応時の参照情報ともなる。

[23] 忘れがちなのがリアルタイムアナリシス側へのフィードバックである。リアルタイム分析が正しかったのか、何らの対処が行われたのか、それによって解決できているのかなどが把握できないと、以降のリアルタイム分析結果の精度が上がらなくなってしまう。

E-2. 資産棚卸

（第 2.1 版では「E-2. アセット情報収集」）

X.1060/JT-X1060 での概要は以下である。

「資産棚卸」サービスは、CDC の所掌範囲となるビジネスインフラ全体を構成するシステム、アセット、アプリケーションの全数調査の情報管理を実現する。

守るべき対象のサーバーや端末、ネットワーク装置などのアセット情報を収集する。ISMS などでの情報資産管理情報をベースにしつつ、さらに詳細なファームウェアのバージョンや、インストールされているアプリケーションのバージョンなどまで収集できていることが望ましい。物品やソフトウェアなどの資産を調達する際には、内部でどのような外部のライブラリやモジュール利用されているかまでチェックを行い管理が必要な場合もある。また、自社や自組織で行うビジネスやサービス・製品でも同様にどのような外部のライブラリやモジュールを利用しているか、製品の構成要素として把握をしておく必要がある場合もある。

ただし、情報収集は非常に難しいため、ISMS 関連部門と連携し社内プロセスに情報の登録を義務付けるルールを策定したり、後述する脆弱性診断時の情報を集めたりする工夫が求められる。こちらも、脆弱性管理だけでなく、分析やインシデント対応時の参照情報ともなる。

E-3. 脆弱性診断

（第 2.1 版では「E-4. 自動脆弱性診断」）

X.1060/JT-X1060 での概要は以下である。

「脆弱性診断」サービスは、ネットワーク、システム、アプリケーションの脆弱性を特定し、その脆弱性がどのように悪用されるか判断するとともに、リスクをどのように軽減できるかの提案を実現する。

守るべきシステムやネットワーク、アプリケーションに脆弱性が無いかをツールを使って確認する。プラットフォーム診断、Web アプリケーション診断、Web API 診断、スマートフォンアプリケーション診断など、目的に合わせた診断の種類を選択する。ツールでの確認であるため、精度の問題はあるものの、低コストかつ短期間で実施できるため、より多くのシステムに対する定期的な診断も行う。

E-4. パッチ管理

（第 2.1 版では「E-3. 脆弱性管理・対応」）

X.1060/JT-X1060 での概要は以下である。
「パッチ管理」サービスは、情報技術(IT)さービスの可用性を維持しながら、必要なセキュリティパッチのインストールを支援する。

脆弱性情報と前述のネットワークマッピングやアセット情報とを突合することで、対処が必要となるシステムを特定する。システムの管理主体へ通達を実施し、対処の進捗状況も合わせて管理していく。新たな脅威情報は「F-3 外部脅威情報の収集・評価」から受けるが、主要なソフトウェアや製品の脆弱性情報については、その提供元の Web サイトなどから随時収集する。

E-5. ペネトレーションテスト

（第 2.1 版では「E-5. 手動脆弱性診断」）
X.1060/JT-X1060 での概要は以下である。
「ペネトレーションテスト」サービスは、攻撃者に悪用される可能性のあるセキュリティの脆弱性を明らかにし、考えられる侵害方法の炙り出しを実現する。(例：脅威ベースのペネトレーションテスト)。

こちらは「自動」ではなく、専門の人員による「手動」で実施される。ツールと比較し、コストと時間はかかるものの、より精度の高い結果を得ることができる。重要度の高いシステムに対しては必ず行う必要がある。新システムの立上げ、大規模なシステム改修など、重要なマイルストーンに合わせた診断も行う。

脅威ベースのペネトレーションテスト[24](Threat-Led Penetration Test, TLPT)では、攻撃側のレッドチームや防御側のブルーチームによって実施される。その場合は本サービス以外でも後述の「E-6.高度サイバー攻撃耐性評価」、「E-7.サイバー攻撃対応力評価」と連携を行う。

E-6. 高度サイバー攻撃耐性評価

（第 2.1 版では「E-6. 標的型攻撃体制評価」）
X.1060/JT-X1060 での概要は以下である。
高度サイバー攻撃(APT)に対抗するための「高度サイバー攻撃耐性評価」サービスは、標的型メール訓練やソーシャルエンジニアリングテストを実施しながら、標的型攻撃に対する組織耐性の計測を実現する。

標的型攻撃に対する自社の耐性を測るために、標的型メール訓練やソーシャルエン

[24] 脆弱性診断士スキルマッププロジェクト　「ペネトレーションテストについて」
https://github.com/ueno1000/about_PenetrationTest

ジニアリングテストを実施する。その結果は、社員教育に生かしたり、会社に対しセキュリティ対策の必要性を訴える根拠として活用したりする。

ペネトレーションテストや TLPT においては「E-5.ペネトレーションテスト」と連携をする。

E-7. サイバー攻撃対応力評価

（第 2.1 版では「E-7. サイバー攻撃対応力評価」）

X.1060/JT-X1060 での概要は以下である。

「サイバー攻撃対応力評価」サービスは、攻撃発生を想定したシナリオに基づき、セキュリティ対応が実際に発動され、インシデントを遅滞なく終息させることができるかどうかの確認を実現する（サイバー攻撃対応演習と呼ぶ)。

攻撃が起きたことを想定したシナリオに基づき、実際のセキュリティ対応の営みを発動し、滞りなくインシデント終息までたどり着けるか確認する（サイバー攻撃対応演習と呼ばれる)。問題があった場合は、原因の分析を行い、対応力の強化につなげる。

机上演習だけではなく、ペネトレーションテストや TLPT の防御側のブルーチームであれば「E-5.ペネトレーションテスト」と連携する。対応の際の結果を利用して対応能力を評価する。

E-8. ポリシー遵守

（第 3.0 版より追加）

X.1060/JT-X1060 での概要は以下である。

「ポリシー遵守」サービスは、事前に定義されたセキュリティポリシーへの適合性と遵守の検証を支援する。

E-9. 堅牢化

（第 3.0 版より追加）

X.1060/JT-X1060 での概要は以下である。

「堅牢化」サービスは、システムに対するセキュリティ設定の見極めや評価、適用するため、および攻撃のリスクの低減や排除のための、IT コンポーネントの構成最適化を実現する。

F. 脅威情報の収集および分析と評価

F-1. 事後分析

（第 3.0 版より追加）

X.1060/JT-X1060 での概要は以下である。

「事後分析」サービスは、CDC 関係者の手順やツールの見直しや改善を実現するため、インシデントの解決法の詳述を実現する。

「D-7.インシデント対応報告」でインシデント対応が完了した際に、セキュリティ対応組織として全体的な手順やツールの見直しなどの改善を実施する。組織的な改善が必要な部分についてはカテゴリー「A. CDC の戦略マネジメント」で改善を実施する。

F-2. 内部脅威情報の収集・分析

（第 2.1 版では「F-1. 内部脅威情報の整理・分析」）

X.1060/JT-X1060 での概要は以下である。

「内部脅威情報の収集・分析」サービスは、リアルタイム分析やインシデント対応に関する情報（内部インテリジェンス）の収集を実現する。

リアルタイム分析やインシデント対応に関する情報（内部インテリジェンス）を収集する。自組織内で管理把握すべき（サプライチェーンも含む）インシデントの根本的な要因を分析し（システムの観点だけでなく、社内のルールやプロセスも含む)、中長期的な対策に繋げられるような整理を行う。合わせて、リアルタイム分析やインシデント対応そのものにおける課題点も整理することで、セキュリティ対応全体の改善へ繋げられるようにする。

F-3. 外部脅威情報の収集・評価

（第 2.1 版では「F-2. 外部脅威情報の収集・評価」）

X.1060/JT-X1060 での概要は以下である。

「外部脅威情報の収集・評価」サービスは、新たな脆弱性、攻撃の傾向、マルウェアの挙動、悪意のある IP アドレスやドメインの情報（外部情報）の収集を実現する。

公開された新たな脆弱性情報、攻撃動向、マルウェア挙動情報や悪性 IP アドレス/ドメイン情報などの情報（外部インテリジェンス）を収集する。得られた情報の信頼度、自社に与える影響などを評価し、対応すべき脆弱性を取捨選択する。脅威情報の活用は「F-5.脅威情報の活用」にて行う。必要であれば「C-3. 追及・追跡」でも外部脅威情報を利用して分析を行う。

情報ソースは逐次見直しを行い、常に鮮度の高い情報を収集する必要がある。また、本来分析において発見されるべきであった事象や、その時点で対策が困難な情報を得た場合には、必要に応じて運用の見直しを行う。

F-4. 脅威情報報告

（第 2.1 版では「F-3. 脅威情報報告」）

X.1060/JT-X1060 での概要は以下である。

「脅威情報報告」サービスは、内部と外部の脅威情報を取りまとめ、詳細も含めたドキュメント化を実現する。

収集した内部脅威情報と外部脅威情報を取りまとめ、詳細も含めドキュメント化する。月毎や四半期毎など、決まったタイミングで定点観測的に生成することが望ましいが、セキュリティを取り巻く状況の変化は目まぐるしく、あまり形にこだわり過ぎるとすぐに形骸化してしまうため、内容の見直しは必須であり、変更を恐れてはならない。また、想定される影響が甚大な脅威情報については、速報を準備する必要もある。

F-5. 脅威情報の活用

（第 2.1 版では「F-4-. 脅威情報の活用」）

X.1060/JT-X1060 での概要は以下である。

「脅威情報の活用」サービスは、あらゆるカテゴリーのセキュリティ対応のために、脅威情報の編纂と発信を実現する。

取りまとめた脅威情報は、セキュリティ対応に関わるすべてのカテゴリーに対して周知が必要である。各カテゴリーにおいて興味を持つ部分は異なってくるが、情報把握状況の偏りが無い状態にすることで、各カテゴリーのスムーズな連携が期待される。各カテゴリーへのより具体的な活用指示、あるいは逆に各カテゴリーからのフィードバックがなされるよう、セキュリティ対応方針管理の中でそのプロセスやルールを決める必要がある。その際は、特に「G CDC プラットフォームの開発」への落とし込みを意識するとよい。脆弱性やパッチに関連した情報であれば「E-4.パッチ管理」で活用されることとなる。

G. CDC プラットフォームの開発・保守

G-1. セキュリティアーキテクチャ実装

（第 3.0 版より追加）

X.1060/JT-X1060 での概要は以下である。

「セキュリティアーキテクチャ実装」サービスは、CDC の戦略マネジメント（カテゴリーA）で設計したセキュリティアーキテクチャの実装を実現する。

G-2. ネットワークセキュリティ製品基本運用

（第 2.1 版では「G-1. ネットワークセキュリティ製品基本運用」）

X.1060/JT-X1060 での概要は以下である。

「ネットワークセキュリティ製品基本運用」サービスは、ファイアウォール、不正侵入検知システム/不正侵入防止システム(IDS/IPS)、WAF、プロキシなどのネットワーク装置の運用を実現する。

ファイアウォール、IDS/IPS、WAF、プロキシ、NDR などのネットワーク装置の運用を行う。ネットワーク構成を把握したうえで、ネットワークセキュリティ製品の種類、配置場所、設置構成（インラインかタップかなど）、機器/ファームウェアバージョン、設定内容などを管理する。各製品が適切に動作しているか、死活監視や検知シグネチャの更新の監視を行う。構成変更や設定変更がネットワークへ大きな影響を与える可能性があるため、作業の手順やプロセスの策定が必須である。

G-3. ネットワークセキュリティ製品高度運用

（第 2.1 版では「G-2. ネットワークセキュリティ製品高度運用」）

X.1060/JT-X1060 での概要は以下である。

「ネットワークセキュリティ製品高度運用」サービスは、IDS/IPS や WAF などの攻撃検知機能を持った製品において、製品ベンダーの検知シグネチャでは不十分な場合に、組織独自のカスタムシグネチャ作成を実現する。

IDS/IPS や WAF に代表される攻撃検知機能を持った製品において、製品ベンダーの検知シグネチャが不十分な場合に、独自にシグネチャを作成し（カスタムシグネチャ）、適用を行う。また、過剰な検知や誤った検知による検知ログの暴発や誤遮断の発生リスクを抑えるため、各シグネチャの特性を理解したシグネチャ設定ポリシー（マスターポリシー）の策定、適用を行う。

G-4. エンドポイントセキュリティ製品基本運用

（第 2.1 版では「G-3. エンドポイントセキュリティ製品基本運用」）

X.1060/JT-X1060 での概要は以下である。

「エンドポイントセキュリティ製品基本運用」サービスは、アンチウイルスソフトのようなエンドポイントでの対策製品の運用を実現する。

アンチウイルスソフトや EDR に代表される、エンドポイントでの対策製品の運用を行う。近年ではエンドポイントでのマルウェア挙動や脆弱性を突く攻撃を検知あるいは記録する機能を有するものもある。インストール漏れが無いか、パターンアップデートが適切になされているか、スキャン機能が有効かなどを監視し、可能な限り漏れのな

い管理を行う。

エンドポイントの管理においては、資産管理やアセット管理の対策ソフトウェアを利用することもある。どんなエンドポイントの製品を利用している、どんなソフトウェアを搭載しているかなど、運用管理を行う。

G-5. エンドポイントセキュリティ製品高度運用

（第 2.1 版では「G-4. エンドポイントセキュリティ製品高度運用」）

X.1060/JT-X1060 での概要は以下である。

「エンドポイントセキュリティ製品高度運用」サービスは、エンドポイント内の不審なプログラム挙動を検出し、レジストリの状態やプロセスの実行状況などを収集・分析するエンドポイント対策製品の運用を実現する、必要に応じて、独自に IOC(Indicators of Compromise)を定義し、エンドポイントでの検知を実現する。

エンドポイント対策製品において、そのエンドポイント内での不審なプログラムの活動を検知するため、レジストリの状態やプロセスの実行状況などを収集し分析する。必要に応じて、独自に IOC（Indicators of Compromise）を定義し（カスタム IOC)、それを基にエンドポイントで検知を行えるようにする。

G-6. クラウドセキュリティ製品基本運用

（第 3.0 版より追加）

X.1060/JT-X1060 での概要は以下である。

「クラウドセキュリティ製品基本運用」サービスは、クラウドで提供されるセキュリティサービスの運用を実現する。

G-7. クラウドセキュリティ製品高度運用

（第 3.0 版より追加）

X.1060/JT-X1060 での概要は以下である。

「クラウドセキュリティ製品高度運用」サービスは、攻撃検知機能を持つクラウド上のセキュリティサービスに対して、組織独自のカスタムシグネチャ作成を実現する。ベンダーが提供するシグネチャでは不十分な場合に、そのカスタムシグネチャを適用する。

クラウドサービスの活用においては、ユーザー側での設定の不備による情報の漏えいが起こることもある。クラウドの設定不備を見つけるサービスの利用や、見つけた場合に設定を変更するようなサービスを活用する。

G-8. 深掘分析ツール運用

（第 2.1 版では「G-5. ディープアナリシス（深堀分析）ツール運用」）

X.1060/JT-X1060 での概要は以下である。

「深堀分析ツール運用」サービスは、デジタルフォレンジックや、マルウェア解析のような深堀分析に用いるツールの運用を実現する。

デジタルフォレンジックや、マルウェア解析などで用いられるツールを運用する。深掘分析においては、扱うデータの中に機密情報や個人情報が含まれていたり、マルウェアなど非常に危険なプログラムが含まれていたりするため、ツールの利用方法や手順、作業の認可プロセスなど、厳重な管理が求められる。

G-9. 分析基盤基本運用

（第 2.1 版では「G-6. 分析基盤基本運用」）

X.1060/JT-X1060 での概要は以下である。

「分析基盤基本運用」サービスは、必要なログデータを蓄積し、日常的に、主にはリアルタイム分析を行うことができる SIEM(Security Information and Event Management)のような分析基盤の運用を実現する。

分析基盤とは、主にリアルタイムアナリシスにおいて、必要となるログデータを保存し、定常的に行われる分析を実現するシステムを指す。SIEM がこれに含まれる。どのようなデータをどれだけの期間保持するか決め、分析ルールのアップデートや追加を行う。データが保存できているか、分析処理が常時行えているかなどの監視を行う。

G-10. 分析基盤高度運用

（第 2.1 版では「G-7. 分析基盤高度運用」）

X.1060/JT-X1060 での概要は以下である。

「分析基盤高度運用」サービスは、市販の SIEM では取得できないシステムログやパケットキャプチャデータを保持し、それらのデータやシステムに対して独自の分析アルゴリズムやロジックを開発し、より詳細で正確な分析を組織独自のシステムとして実現する。

市販の SIEM が取り込むことのできないシステムのログやパケットキャプチャデータなどを独自のシステムで保持し、それらを対象にした分析アルゴリズムやロジックおよびそれらが動作するシステムも独自に開発を行い、より詳細で精度の高い分析を実現する。

G-11. CDC システム運用

（第 2.1 版では「G-10. 業務基盤運用」）

X.1060/JT-X1060 での概要は以下である。

「CDC システム運用」サービスは、これまでに記した各種セキュリティ対応ツール、各種レポート作成、問い合わせ対応、脆弱性管理システムなど、セキュリティ対応業務に必要なタスクを遂行するシステムの運用を実現する。

CDC システム（第 2.1 版では業務基盤）とは、上記の各種セキュリティ対応ツール運用や各種レポートの生成、問合せ対応、脆弱性管理システムなど、セキュリティ対応業務に必要な業務を実現するシステムを指す。必要となる業務のフロー、プロセス、手順に基づき実装し、その他のシステムにおける不足機能の穴埋め、オペレーションミスの防止、作業の効率化や自動化を行う。

G-12. 既設セキュリティツール検証

（第 2.1 版では「G-8. 既設セキュリティ対応ツール検証」）

X.1060/JT-X1060 での概要は以下である。

「既設セキュリティツール検証」サービスは、既に存在するセキュリティ対応ツールのバージョンアップや設定変更時の、システムや運用への主に可用性の観点での影響検証を実現する。

既設のセキュリティ対応ツールにおいて、製品のバージョンアップや設定の変更を行う場合に、他システムや運用への、主に可用性についての影響を検証する。

G-13. 新規セキュリティツール検証

（第 2.1 版では「G-9. 新規セキュリティ対応ツール調査、開発」）

X.1060/JT-X1060 での概要は以下である。

「新規セキュリティツール検証」サービスは、セキュリティ活動において新たな対策が必要となった場合に、新規のセキュリティ資産の設計・導入を実現する。

一連のセキュリティ対応の中で新たな対策が必要となった場合、それを実現するための新たなツールの導入を検討する。市販製品の調査を行い、トライアル利用により、期待される効果を実現できるかや、現行の運用への影響度合いなどの確認を行う。要求を満たせる市販製品がなければ、独自開発を行う。

セキュリティ対応における新たな対策としては、以下の３つのケースも想定される。

- セキュリティ対応組織内の業務で使用する攻撃を解析するソリューションや製品
- セキュリティ対応組織外の業務で使用するビジネスソリューションや製品
- セキュリティ対応組織がサービスとして提供する攻撃対策ソリューションや製品

セキュリティ対応組織内の業務で使用する攻撃を解析するソリューションや製品では、規定やアーキテクチャが基準を満たしているか、という観点が必要となる。

セキュリティ対応組織外の業務で使用するビジネスソリューションや製品では、規定やアーキテクチャが基準を満たしているかだけではなく、脆弱性が発見されても十分なサポートを受けられる体制があるかどうかという観点も必要となる。

セキュリティ対応組織がサービスとして提供する攻撃対策ソリューションや製品では、脆弱性が発見されても十分なサポートを受けられる体制があるかどうかだけではなく、調査検討をしている時点で流行している攻撃を十分に対応できる機能を具備しているかという観点も必要となる。

これは、企業や組織においてセキュリティアーキテクチャとして使いたいサービスや製品に対するリスクアセスメントの分析、利用できるかどうかの判断、場合により決裁をどうするかなども合わせて検討を行う必要がある。

H. 内部不正対応支援

H-1. 内部不正対応・分析支援

（第 2.1 版では「H-2. 内部不正対応の調査・分析支援」）

X.1060/JT-X1060 での概要は以下である。

「内部不正対応・分析支援」サービスは、内部不正が発覚した場合に、セキュリティ活動で取得したログから行動内容を整理することで、組織的な対応を支援する。

内部不正が発覚した場合に、セキュリティ対応組織で収集しているログからその活動内容について整理するなど、内部不正に対応している組織の支援を行う。内部不正の対象は組織全体としており、セキュリティ対応組織の CDC やセキュリティ統括、SOC や CSIRT も対象となる。

H-2. 内部不正検知・再発防止支援

（第 2.1 版では「H-3. 内部不正検知・防止対応」）

X.1060/JT-X1060 での概要は以下である。

「内部不正検知・再発防止支援」サービスは、発見された内部不正行為の内容を分析し、ログから検知できないか検討し、可能な場合、検知ロジックとしての実装を実現する。

発覚した内部不正の活動内容について分析し、ログから検知できないか検討し、可能な場合、検知ロジックとして実装する。UEBA などを活用し、ユーザーの不審な挙動

を発見できるよう、検知ロジックに組み込むこともある。検知した場合には、内部不正に対応している組織への連絡を行い、内部不正の抑止に貢献する。内部不正の対象は組織全体としており、セキュリティ対応組織の CDC やセキュリティ統括、SOC や CSIRT も対象となる。

I. 外部組織との積極的連携

I-1. 意識啓発

（第 2.1 版では「I-1. 社員のセキュリティに対する意識啓発」）

X.1060/JT-X1060 での概要は以下である。

「意識啓発」サービスは、CDC に関わるあらゆる関係者の意識を高め、ビジネス資産を保護するための適切なツール、ベストプラクティス、ポリシー、リソースの活用促進を実現する。

実際のセキュリティ対応事例や統計的なデータを取りまとめ、身近な問題として社員に認識してもらえるよう、関連部門と連携し、ポータルサイトの作成や、ビデオ作成、ポスター配布、教材化などを通し、啓発を行う。

I-2. 教育・トレーニング

（第 2.1 版では「I-2. 社内研修・勉強会の実施や支援」）

X.1060/JT-X1060 での概要は以下である。

「教育・トレーニング」サービスは、CDC が支援する組織関係者への、セキュリティ分野に特化したトレーニングを支援する。

セキュリティ対応において得られた専門的知見について、セキュリティに関する社内研修や勉強会を行い、セキュリティ対応組織以外の部門における理解度を高めていく。

I-3. セキュリティコンサルティング

（第 2.1 版では「I-3. 社内セキュリティアドバイザーとしての活動」）

X.1060/JT-X1060 での概要は以下である。

「セキュリティコンサルティング」サービスは、ビジネスにおけるさまざまな業務で、セキュリティに関連したコンサルティングを実現する。

社内のシステム開発や、お客さま向けのサービス運営などにおいてその主体となっている部門からのセキュリティに関わる相談を受け、カテゴリー「A. CDC の戦略マネジメント」の方針や判断基準によりアドバイスを行う。必要性のある基準を超えるよう

な判断や改善する項目がある場合は「A-11.品質管理」と連携して改善や対応を行う。この活動を通して、Security By Design の浸透に貢献する。

I-4. セキュリティベンダー連携

（第 2.1 版では「I-5. セキュリティベンダーとの連携」）

X.1060/JT-X1060 での概要は以下である。

「セキュリティベンダー連携」サービスは、購入したセキュリティ製品・サービスについて、その提供元と直接対話できる関係を築き、セキュリティの対応で見つかった不具合への対応要求や、改善に向けた前向きなフィードバックを実現する。

購入したセキュリティ製品、あるいはセキュリティサービスについて、その提供元と直接対話できる関係を築く。セキュリティ対応の中で発見した不具合への対応要請や、改良すべき点についての前向きな意見交換を行う。

I-5. セキュリティ関連団体との連携

（第 2.1 版では「I-6. セキュリティ関連団体との連携」）

X.1060/JT-X1060 での概要は以下である。

「セキュリティ関連団体との連携」サービスは、外部のコミュニティへの参加を通じて、積極的な情報交換を実現する。そこで得られた情報は、セキュリティ活動に反映させることができる。

セキュリティ対応を行っている組織の集まり（NCA、各種 ISAC など）へ参加し、開示可能な範囲で積極的な情報交換を行い、情報共有、情報活用の輪を広げる。

I-6. 技術報告

（第 3.0 版より追加）

X.1060/JT-X1060 での概要は以下である。

「技術報告」サービスは、監視運用の結果についての報告を実現する。このような活動はシステムや IT インフラのセキュリティレベルの可視化に役立つ。

I-7. 幹部向けセキュリティ報告

（第 3.0 版より追加）

X.1060/JT-X1060 での概要は以下である。

幹部向けセキュリティ報告」サービスは、組織のセキュリティレベルや運用のパフォーマンスの指標を際立たせるため、幹部向けの定期的な報告や統計的な分析を実現する。

執筆

日本セキュリティオペレーション事業者協議会（ISOG-J）

セキュリティオペレーション連携 WG(WG6)

野尻 泰弘　NEC ソリューションイノベータ株式会社

早川 敦史　NEC ソリューションイノベータ株式会社

/ ISOG-J 運営サポートリーダー

武井 滋紀　NTT テクノクロス株式会社

/ ISOG-J WG6 リーダー

彦坂 孝広　NTT テクノクロス株式会社

河島 君知　NTT データ先端技術株式会社

阿部 慎司　GMO サイバーセキュリティ by イエラエ株式会社

/ ISOG-J WG4 リーダー

執筆協力

川田 孝紀　NTT セキュリティ・ジャパン株式会社

本橋 孝祐　NTT セキュリティ・ジャパン株式会社

角田 玄司　ネットワンシステムズ株式会社

竹之内　一晃　パーソルクロステクノロジー株式会社

青木　翔　株式会社日立製作所

（執筆関係者、社名五十音順）