TTC標準
Standard

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
Framework for the creation and operation of a cyber defence centre

第 1.0 版

2022 年 2 月 24 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

本書は、一般社団法人情報通信技術委員会が著作権を保有しています。
内容の一部又は全部を一般社団法人情報通信技術委員会の許諾を得ることなく複製、転載、改変、転用及びネットワーク上での送信、配布を行うことを禁止します。

目　次

＜参考＞

1. 国際勧告などとの関連

本標準は組織レベルでの戦略的なセキュリティ対応を実現するフレームワークについて規定しており、2021 年 10 月に ITU-T SG17 において発行された ITU-T 勧告 X.1060 に準拠している。

2. 上記勧告などに対する追加項目など

2.1 オプション選択項目

なし

2.2 ナショナルマター決定項目

なし

2.3 その他

なし

2.4 原勧告との章立て構成比較表

章立てに変更なし

3. 改版の履歴

版数	発行日	改版内容
第 1 版	2022 年 2 月 24 日	制定

4. 工業所有権

本標準に関わる「工業所有権の実施の権利に係る確認書」の提出状況は、TTC ホームページでご覧になれます。

5. その他

(1) 参照している勧告、標準など

なし

6. 標準作成部門

セキュリティ専門委員会

はじめに

組織におけるサイバーセキュリティのリスクは、組織の活動全体に大きな影響を与える。組織は、社会的あるいはビジネス的な側面からの環境変化や、規制や脅威の増大による外部からの圧力といったリスクに直面している。そのため、経営幹部レベル（CxO）においては、これらのリスクや変化に対応するために組織全体を統制管理する責任がある。サイバーセキュリティにおける統制を実現するための重要な点として、ビジネス目標に沿ったセキュリティポリシーの策定と統制におけるリーダーシップが期待されており、多くの場合、最高セキュリティ責任者（CSO）または最高情報セキュリティ責任者（CISO）がそれを担っている。実際にセキュリティ対策を実現するためには、そういった CSO や CISO の活動を、組織レベルで戦略的にマネジメントしサポートする主体が必要となる。この主体を本勧告ではサイバーディフェンスセンター（CDC）と表現している。

この勧告では、CDC の構築とマネジメント、およびその有効性の評価するためのフレームワークを提供している。このフレームワークは、組織のセキュリティを実現するために、CDC がどのようにセキュリティサービスを決定し、実施すべきかを示している。このフレームワークは、組織がサイバーセキュリティのリスクに対処するのに有効である。

1. 規定範囲

この勧告は、組織がサイバーディフェンスセンター（CDC）を構築、マネジメントするとともに、その有効性を評価するためのフレームワークを提供するものである。このフレームワークは、組織のセキュリティを実現するために、CDC がどのようにセキュリティサービスを決定し、実施すべきかを示している。

この勧告は、最高セキュリティ責任者（CSO）や最高情報セキュリティ責任者（CISO）など、組織のセキュリティに責任を持つ経営幹部レベル、およびそれを補佐するセキュリティ管理者を対象としている。

2. 参考文献

以下に列挙する ITU-T 勧告及びその他の参考文献は、この本文中の参照を通して、本標準を構成する規定を含む。発行時点では、示された版は有効であった。すべての勧告及び他の参考文献は改訂の対象である。したがって、本標準の利用者は、以下に列挙する勧告及び他の参考文献の最新版を適用する可能性を調査することが推奨される。現在有効な ITU-T 勧告のリストは定期的に発行されている。本標準が文献を参照することは、その文献がそれ単体で勧告となる地位をその文献に与えるものではない。

なし

3. 定義

3.1. 他の標準等で定義されている用語

本標準は、以下の他で定義される用語を使用する。

3.1.1. アウトソーシング[b-ITU-T X.1053]: 企業が内部のプロセスや機能の 1 つまたは複数を外部の企業に委託すること。アウトソーシングは、企業のリソースを外部の企業に移すとともに、アウトソースされたプロセスとの関係性を管理する能力を保有する。

3.2. 本標準で定義する用語

3.2.1. 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。

4. 略語及び頭字語

本標準では、次の略語及び頭字語を使用する。

APT	Advanced Persistent Threat （高度サイバー攻撃）
CDC	Cyber Defence Centre（サイバーディフェンスセンター）
CISO	Chief Information Security Officer（最高情報セキュリティ責任者）
CSIRT	Computer Security Incident Response Team（コンピュータセキュリティインシデント対応チーム）
CSO	Chief Security Officer（最高セキュリティ責任者）
CxO	C-suite（経営層）
IDS	Intrusion Detection System（不正侵入検知システム）
IPS	Intrusion Prevention System（不正侵入防止システム）
IT	Information Technology（情報通信技術）
SIEM	Security Information and Event Management（セキュリティ情報およびイベント管理システム）
SLA	Service Level Agreement（サービスレベル合意書）
WAF	Web Application Firewall（ウェブアプリケーションファイアウォール）

5. 規則

なし

6. 本勧告の構成

本勧告では、CDC の概念を 7 章で説明する。8 章では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の概要を説明する。フレームワークの詳細については後の章で次の通り、CDC 構築プロセス（9 章）、CDC マネジメントプロセス（10 章）、CDC 評価プロセス（11 章）で述べる。12 章では、CDC により提供されるサービスの全体像をベストプラクティスとして提示し、各サービスについては付属資料 A でさらに詳細に説明している。

7. サイバーディフェンスセンターの概要

組織はビジネスを成功に導くために活動する。CISO はその事業活動のリスクを管理するために、特にサイバーセキュリティの観点からセキュリティポリシーを策定する。CDC は、セキュリティポリシーを具体的な形として、セキュリティ担当チームの活動で構成される CDC サービスとして実装していく主体である。CDC サービスは、セキュリティ関連プ

ロセスを実行するシステムとしてのセキュリティ機能を明確にする。図 1 は、CDC の運営における関係者とその役割を示したものである。

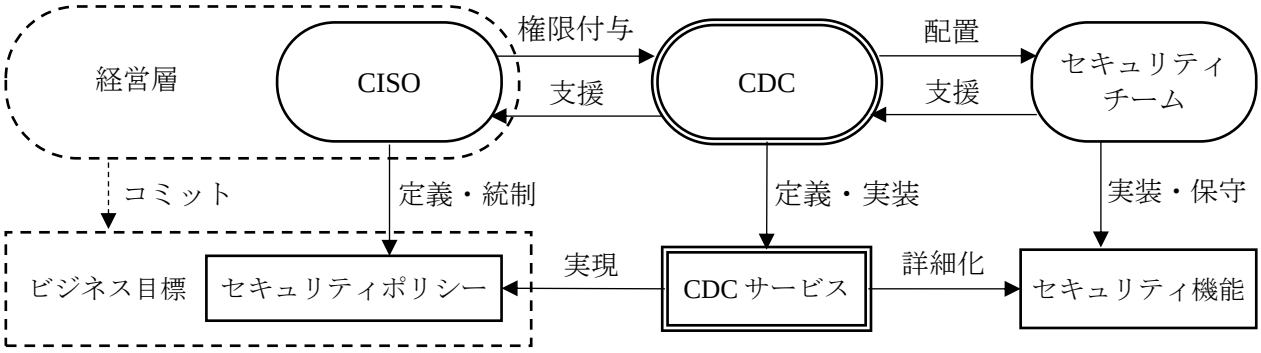

図 1　CDC の運営における関係者とその役割

組織の規模や種類によって、CDC は独立した部門となったり、委員会となったり、小さなチームとなったりするだろう。CDC はその形態がいずれであっても、組織を安全にするためのセキュリティサービスを実現する権限とリソースを持った主体として組織内に存在すべきである。セキュリティサービスはセキュリティポリシーに沿ったものでなければならず、またセキュリティ活動の品質も担保しなければならない。各サービスのレベルは、サービスレベル合意書（SLA）などの文書化された取り決めによって明示的に合意されなければならない。CDC のセキュリティサービスの全体的な品質は、9.4 節で示された方法によって評価される。

8.　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 は、CDC を構築・運用するためのフレームワークを示している。このフレームワークには、構築、マネジメント、評価の 3 つのプロセスが含まれている。組織の安全性を確保するためには、CDC を構築し、適切にマネジメントする必要がある。また、適時あるいは定期的に評価を行い、継続的に改善していく必要もある。このフレームワークにより、組織はセキュリティ活動を保ち続けることが可能となる。

構築プロセスでは、組織内のセキュリティ活動を検討する。CDC セキュリティサービスのベストプラクティスを付属文書 A に示す。組織は、そのリストからサービスを選択し、必要に応じて組織に固有のサービスを追加することで、自身のサービスカタログを作成することが可能となる。また、カタログ内の各サービスは、主管、役割と責任、サービス割り当て（インソース、アウトソース、あるいはその組み合わせ）を付加し、プロファイルとして定める。サービスプロファイルを確立したあとは、評価プロセス用に、各 CDC サービスの現在のスコアと目標スコアを決める必要がある。

マネジメントプロセスには、3 つのフェーズと 2 つのサイクルがある。戦略マネジメントフェーズでは CDC の活動全体を、運用フェーズでは監視や分析などの定常業務を、対応フェーズでは緊急時の対応をマネジメントする。これらのフェーズは、短期サイクルと長期サイクルの両輪でマネジメントされる。運用フェーズと対応フェーズでは、短期サイクルでのタイムリーな解決が求められる。一方、戦略マネジメントフェーズでは、長い期間かけて改善すべきものを、短期サイクルから溢れたものと合わせ、長期サイクルの中で熟考する必要がある。長期的な改善においては、新たな投資やシステムアーキテクチャの刷新などの意思決定が必要になる。

評価プロセスは、CDC サービスのカタログ、プロファイル、ポートフォリオを評価するものであり（図 4 参照）、適宜、客観的に評価されるべきである。

評価結果はレビューを通し、CDC の 3 つのプロセスすべてに反映されるべきである。セキュリティ活動を改善するための構築・マネジメント・評価プロセスの反復的なサイクルを組織内で確立し、それを維持し続けるべきである。

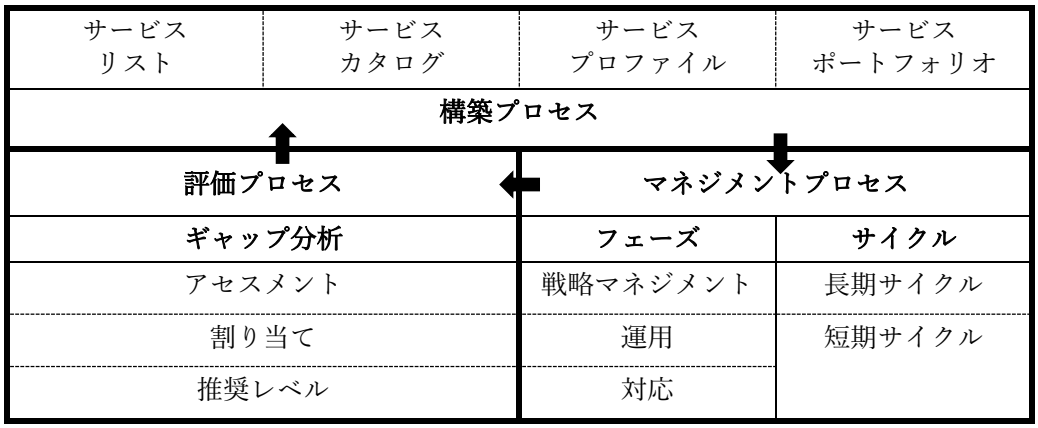

図 2　サイバーディフェンスセンターを構築・運用するためのフレームワーク

9. 構築プロセス

9.1. 概要

構築プロセスは、CDC がどのようなサービスを組織に実装すべきかを決定するプロセスである。実装するサービスの候補として、ベストプラクティスに基づく CDC サービスリストから選択することができる。CDC サービスリストは 12 章に示す。

図 3 は、CDC サービスを立ち上げるための 3 つのフェーズを示している。

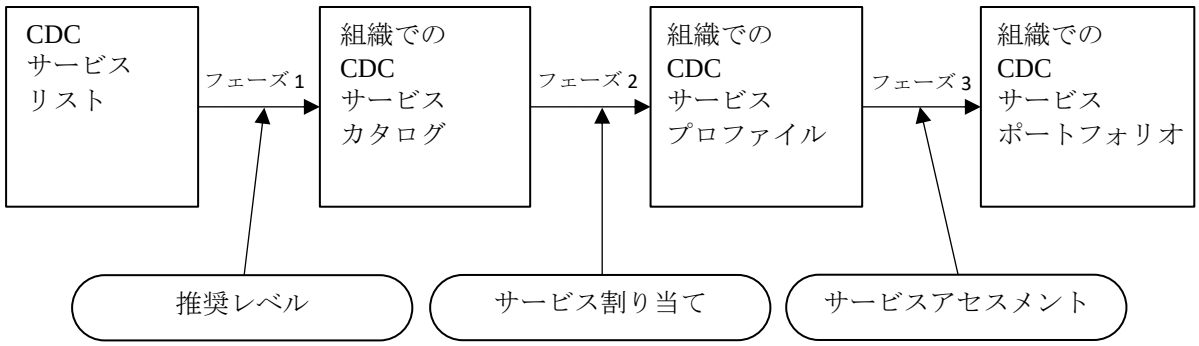

図 3　CDC サービスの立ち上げフェーズ

1)　フェーズ 1 ：CDC サービスカタログの作成

組織としてまず CDC サービスカタログを作る必要がある。

このフェーズでは一般的なサービスリストから実装の候補となるサービスを抽出する。一般的なサービスリストは 12 章に記載している。もし不足しているサービスがある場合は、そのサービスを新たに定義し、CDC サービスカタログに追加する。

2) フェーズ２：CDC サービスプロファイルの作成

CDC サービスカタログに挙げたそれぞれのサービスに対し、そのサービスを誰が実施するのか役割と責任を決定する必要がある。このフェーズでは、9.3 節に示される割り当て方針を考慮する必要がある。

このようにして、CDC サービスプロファイルを作成する。

3) フェーズ３：CDC サービスポートフォリオの作成

CDC サービスプロファイルを決定した後、組織は各サービスの現在のサービススコア（As-is：現状） を測定するとともに、中長期的な目標サービススコア（To-be：あるべき姿）を設定する。

As-is と To-be のレベルを設定することにより、CDC サービスポートフォリオを策定していく。

図 4 は、CDC サービスのマトリクスの例である。このマトリクスは、フェーズ 1 から 3 を実施することで埋められる。

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	あるべき姿
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

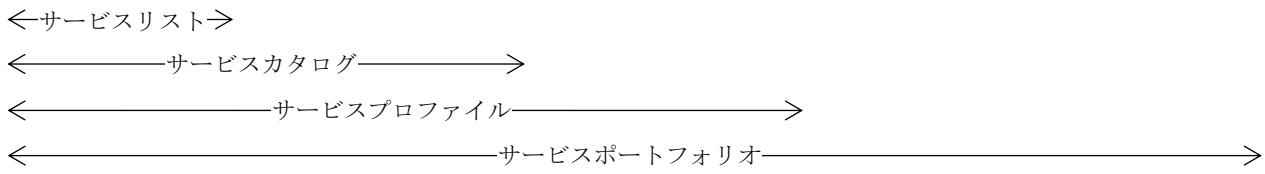

図 4　CDC のサービスマトリクス

9.2.　CDC サービスの推奨レベル

組織にとって最適な CDC サービスを実現するため、各サービスの必要性を表 1 に示す 5 つのレベルで考える。このレベルを用いることで、サービス実施の優先順位を明確にすることができる。

表 1　CDC サービスの推奨レベル

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	実装すべき最低限のサービス
スタンダード	一般的に実装が推奨されているサービス
アドバンスド	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
オプション	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

9.3. CDC サービスの割り当て

組織として CDC サービスをどのチームが実施すべきか明確にする必要がある。組織でのサービスの実施能力に応じて CDC サービスの割り当てを決定すべきであり、これにはアウトソーシングも含まれる。表 2 を参照のこと。

表 2　CDC サービスの割り当て

ウェイト	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。

アウトソースの活用においては、以下の A)と B)の観点が役に立つ。

A)　取り扱う情報の性質

取り扱う情報の性質について、組織の「内部」のものなのか「外部」のものなかを定義、区別し、はっきりとさせる必要がある。例えば、インシデントの発生時において、攻撃による被害や影響についての情報は内部的なものであり、攻撃そのものに関する情報は外部的なものであると考えるべきである。

B)　セキュリティ専門スキルの必要性

サービスの実装に当たり、セキュリティ分野の専門的なスキルが求められるかどうかを加味する必要がある。

これらの 2 つの観点により、CDC サービスは I)から IV)の象限に分類することができる。

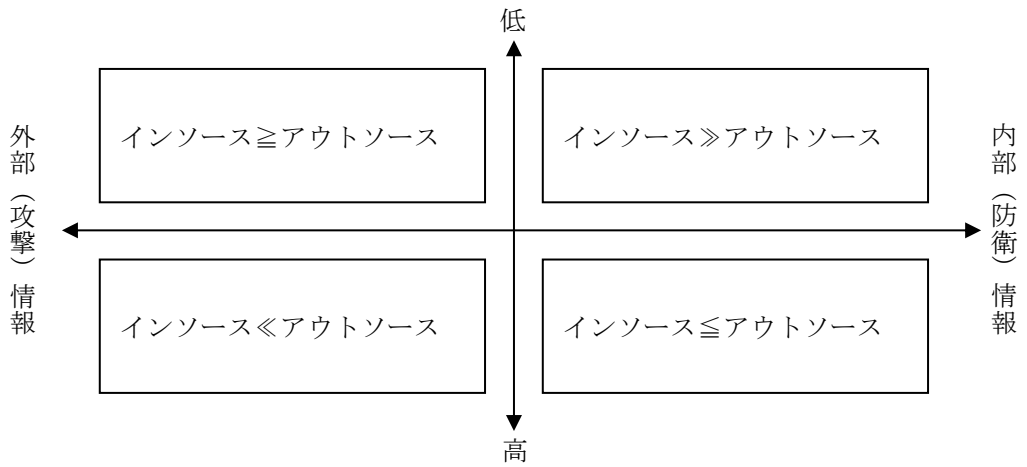

図 5　調達の象限

I)　インソース ≫ アウトソース

セキュリティの専門スキルが求められず、取り扱う情報が組織内部のものである場合は、インソースが望ましく、アウトソースは推奨されない。

II)　インソース ≧ アウトソース

取り扱う情報が組織外部のものであるが、それほど高いセキュリティ専門性が求められないのであれば、アウトソースの力を借りながら、その活動と管理の主はインソースにて実行する。

III)　インソース ≪ アウトソース

取り扱う情報が攻撃に関するものなど外部のものである場合、専門性の高いスキルを持った組織がサービスを実現すべきである（アウトソースするなどして）。特に内部に高いスキルを持つ有識者がいない場合、内製でそのサービスを実現するのは困難である。

IV)　インソース ≦ アウトソース

組織内部の情報を取り扱うものの、特別なスキルが求められる場合は、内部の組織は管理や支援をしつつも、専門性を持つ組織（アウトソースするなどして）を主に活動すべきである。

9.4.　CDC サービスのアセスメント

CDC サービスポートフォリオを作成する際には、表 3 に示すサービススコアを用いて、各サービスの実装状況として、「現状」および「あるべき姿」を評価する必要がある。なお、サービススコアを付けるにあたり、インソースとアウトソースなどサービスの形態ごとに異なる基準での評価となることに留意する。

表 3　CDC サービススコア

インソースの場合	
明文化された運用が 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、担当者のみが業務を実施できる	+2 点
実施できていない	+1 点
インソースとしては実施しないと決めた	適用外

アウトソースの場合	
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
アウトソースとしては実施しないと決めた	適用外

10. マネジメントプロセス

CDC は、図 6 に示す 3 つのフェーズと 2 つのサイクルを含む CDC マネジメントプロセスを次実装することで、組織全体としてのセキュリティ活動を可能にする。

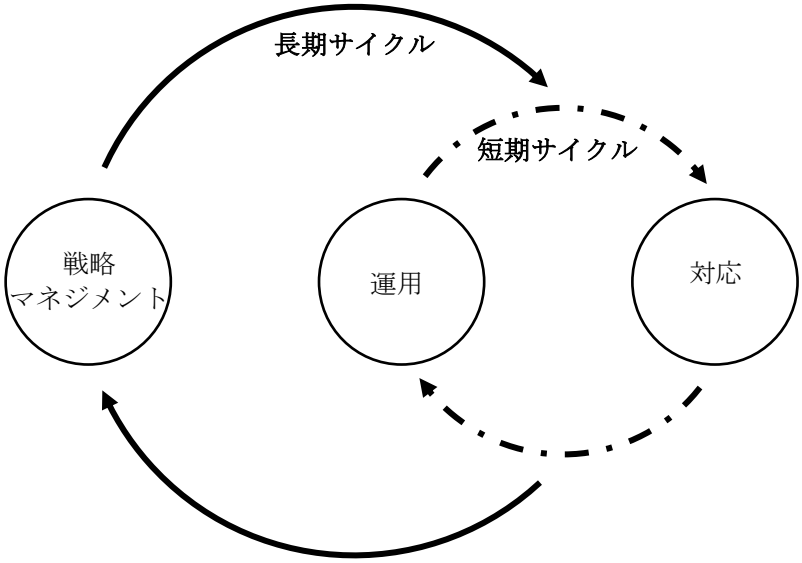

図 6　CDC マネジメントプロセス

(1)　戦略マネジメントフェーズ

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。

(2)　運用フェーズ

導入した仕組みのメンテナンスは、運用フェーズで行うことが望ましい。これは、平時、日常的に行う業務であり、一般的にはインシデント検知の分析や、セキュリティ関連システムの監視・保守などの活動が含まれる。このような業務を行うチームは、セキュリティオペレーションセンター（SOC）と呼ばれることが多い。

(3)　対応フェーズ

運用フェーズの分析によってイベントが検知された場合、インシデント対応が発動される。このフェーズは有事の対応となる。インシデントに対応する組織は、コンピュータセキュリティインシデント対応チーム（CSIRT）と呼ばれることが多い。

対応フェーズへのインプットは、運用フェーズからだけとは限らず、第三者からの報告や通知も同様に対応する必要がある。

A)　短期サイクル

運用や対応は日々行われる。それらの中で、業務プロセス上の問題やセキュリティ関連システム上の問題が必ず発生する。それらの問題を解決するために、単純作業の自動化、分析ツールの精度改善、報告項目の見直しなどの継続的な改善が必要となり、短期サイクルにおいては、すでに割り当てられたリソース（人、予算、システム）の中で実施することとなる。

B)　長期サイクル

新たなリソースの割り当てを必要とする見直しは、長期サイクルで扱われるべきである。

短期サイクルでの見直しの中で現行システムでは解決できない課題が見つかった場合には、新しいセキュリティ製品の導入、セキュリティポリシーの抜本的な見直し、セキュリティシステムの大規模な構成変更など、長期的な視点と計画に基づき対応する必要がある。

11. 評価プロセス

11.1.　概要

構築プロセスで策定された CDC サービスのカタログ、プロファイル、ポートフォリオは、随時そして定期的に評価する必要がある。図 7 は CDC サービスの評価プロセスを示したものである。

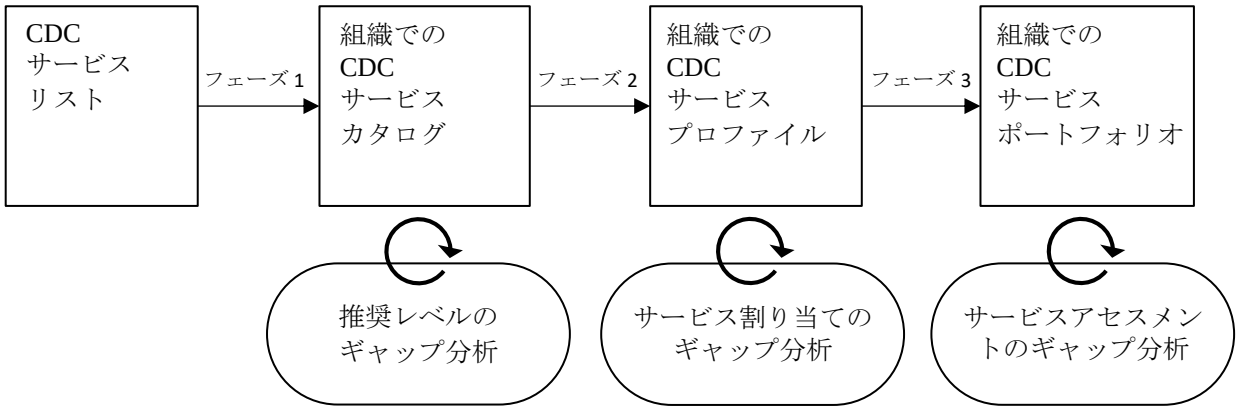

図 7　CDC 評価プロセス

11.2.　CDC サービスカタログの評価

CDC サービス推奨レベルに基づくギャップ分析を行う必要がある。環境や脅威の変化により見直しが求められ、特に「不要」としていたサービスについては再検討し、漏れがないようにする必要がある。CDC サービスカタログは、新たな事業活動を開始するなどビジネスに変化が生じる時や、新たなリスクや脅威に対応する時に合わせ、評価されるべきである。

11.3.　CDC サービスプロファイルの評価

CDC サービス割り当てに関するギャップ分析を行う必要がある。サービス割り当てを決め、「未割り当て」を解消するなどの見直しにより、組織の成熟度向上が期待できる。CDC サービスプロファイルの評価は、インソース型では社内組織の変更、アウトソース型では委託先の変更などの組織変更が発生した際に実施する必要がある。

11.4. CDC サービスポートフォリオの評価

個々のサービスにおける CDC サービススコアのギャップ分析を行う必要がある。「あるべき姿」の目標スコアと「現状」のスコアの差を明確にし、改善すべき点に焦点を当て、CDC サービススコアを再度確認し、課題を抽出する。CDC サービスポートフォリオは定期的に評価されるべきである。

12. CDC サービスカテゴリーとサービスリスト

CDC サービスカテゴリーとリストは構築とマネジメントフェーズで必要となる（9 章及び 10 章を参照のこと）。

CDC が持つ 9 つのサービスカテゴリー:

A) CDC の戦略マネジメント

B) 即時分析

C) 深堀分析

D) インシデント対応

E) 診断と評価

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

H) 内部不正対応支援

I) 外部組織との積極的連携

A. CDC の戦略マネジメント

このカテゴリーでは、CDC を含む組織全体におけるカテゴリー A)～I)に記載されたすべてのセキュリティ活動について、その安定的な運営を実現するためのポリシーやリソースの企画を担う。

B. 即時分析

このカテゴリーでは、ネットワーク機器やサーバー、セキュリティ製品など、様々なシステムのログやデータを常時監視・分析する役割を担う。リアルタイムに脅威を発見し、迅速かつ適切なインシデント対応につなげることを目的とする。

C. 深堀分析

このカテゴリーでは、影響を受けたシステムの調査、侵害されたデータの確認、攻撃に使用されたツールや手法の分析など、インシデント関わる役割を担う。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

このカテゴリーでは、リアルタイムの分析結果や脅威情報に基づいて具体的なアクションをとり、脅威を抑止、排除する役割を担う。ステークホルダーとの調整や報告など含め、システムやビジネスへの影響を最小限に抑えること目的とする。

E.　診断と評価

このカテゴリーでは、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。セキュリティレベル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

このカテゴリーでは、インター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）や、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）を取り扱う。

リアルタイム分析やインシデント対応の精度向上や、セキュリティ関連システムの改善を目的とする。

G.　CDC プラットフォームの開発・保守

このカテゴリーでは、セキュリティ対応に必要なシステム（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、新規開発を行う。

他のカテゴリーの活動が円滑かつ持続的に実施されることを目的とする。

H.　内部不正対応支援

このカテゴリーでは、監査データの収集や、内部不正の対応支援を行う。

ログの提供や分析を通し、内部不正への対応や解決を支援することを目的とする。

I.　外部組織との積極的連携

このカテゴリーでは、内部の利害関係者や外部組織との調整・連携を行う。

組織のセキュリティレベル向上、セキュリティの価値向上により、組織をさらに発展・強化させることを目的とする。

図 8 ではマネジメントプロセスにサービスカテゴリーをマッピングし、表 4 に全サービスをリストアップしている。

CDC サービスリスト内の各サービスの詳細説明は付属資料 A に記載する。

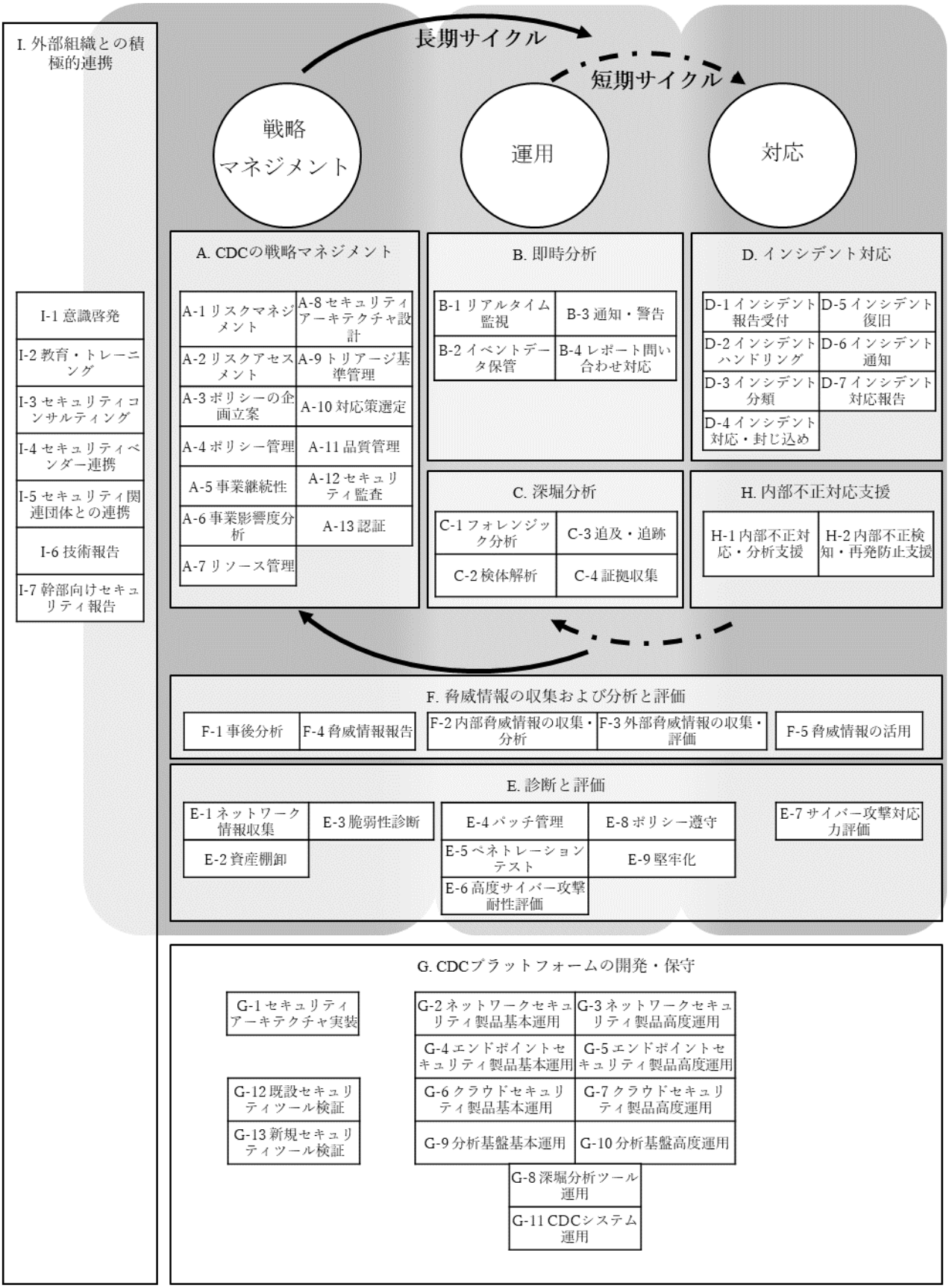

図 8　CDC サービスカテゴリー

表 4　CDC サービスリスト

A	**CDC の戦略マネジメント**
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-7	リソース管理
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-10	対応策選定
A-11	品質管理
A-12	セキュリティ監査
A-13	認証
B	**即時分析**
B-1	リアルタイム監視
B-2	イベントデータ保管
B-3	通知・警告
B-4	レポート問い合わせ対応
C	**深堀分析**
C-1	フォレンジック分析
C-2	検体解析
C-3	追及・追跡
C-4	証拠収集
D	**インシデント対応**
D-1	インシデント報告受付
D-2	インシデントハンドリング
D-3	インシデント分類
D-4	インシデント対応・封じ込め
D-5	インシデント復旧
D-6	インシデント通知
D-7	インシデント対応報告
E	**診断と評価**
E-1	ネットワーク情報収集
E-2	資産棚卸
E-3	脆弱性診断
E-4	パッチ管理
E-5	ペネトレーションテスト
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
E-8	ポリシー遵守
E-9	堅牢化

F	**脅威情報の収集および分析と評価**
F-1	事後分析
F-2	内部脅威情報の収集・分析
F-3	外部脅威情報の収集・評価
F-4	脅威情報報告
F-5	脅威情報の活用
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
G-2	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-4	エンドポイントセキュリティ製品基本運用
G-5	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-9	分析基盤基本運用
G-10	分析基盤高度運用
G-11	CDC システム運用
G-12	既設セキュリティツール検証
G-13	新規セキュリティツール検証
H	**内部不正対応支援**
H-1	内部不正対応・分析支援
H-2	内部不正検知・再発防止支援
I	**外部組織との積極的連携**
I-1	意識啓発
I-2	教育・トレーニング
I-3	セキュリティコンサルティング
I-4	セキュリティベンダー連携
I-5	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

付属資料A　CDCサービスリストとその説明

（本付属資料は仕様の一部である。）

A.1.　カテゴリーA:　CDC の戦略マネジメント

A.1.1.　A-1.　リスクマネジメント

「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.1.2.　A-2.　リスクアセスメント

「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.1.3.　A-3.　ポリシーの企画立案

「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。

A.1.4.　A-4.　ポリシー管理

「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。

A.1.5.　A-5.　事業継続性

「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.1.6.　A-6.　事業影響度分析

「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.1.7.　A-7.　リソース管理

「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）の計画と、各サービスへの適切な割り当てを実現する。

A.1.8.　A-8.　セキュリティアーキテクチャ設計

「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.1.9. A-9. トリアージ基準管理

「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。

A.1.10. A-10. 対応策選定

「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.1.11. A-11. 品質管理

「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）ごとの点検を実現する。

A.1.12. A-12. セキュリティ監査

「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、必要な情報や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。

A.1.13. A-13. 認証

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

A.2. カテゴリーB: 即時分析

A.2.1. B-1. リアルタイム監視

「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。

A.2.2. B-2. イベントデータ保管

「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。

A.2.3. B-3. 通知・警告

「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。

A.2.4. B-4. レポート問い合わせ対応

「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。

A.3. カテゴリーC: 深堀分析

A.3.1. C-1. フォレンジック分析

「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。

A.3.2. C-2. 検体解析

「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。

A.3.3. C-3. 追及・追跡

「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止や防止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。

A.3.4. C-4. 証拠収集

「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）。

A.4. カテゴリーD: インシデント対応

A.4.1. D-1. インシデント報告受付

「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。

A.4.2. D-2. インシデントハンドリング

「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。

A.4.3. D-3. インシデント分類

「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の共通理解を促すために、インシデントの分類を実現する。

A.4.4. D-4. インシデント対応・封じ込め

「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。

A.4.5. D-5. インシデント復旧

「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。

A.4.6. D-6. インシデント通知

「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。

A.4.7. D-7. インシデント対応報告

「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。

A.5. カテゴリーE: 診断と評価

A.5.1. E-1. ネットワーク情報収集

「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。

A.5.2. E-2. 資産棚卸

「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。

A.5.3. E-3. 脆弱性診断

「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。

A.5.4. E-4. パッチ管理

「パッチ管理」サービスは、情報技術（IT）サ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。

A.5.5. E-5. ペネトレーションテスト

「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）。

A.5.6. E-6. 高度サイバー攻撃耐性評価

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。

A.5.7. E-7. サイバー攻撃対応力評価

「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）。

A.5.8. E-8. ポリシー遵守

「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。

A.5.9. E-9. 堅牢化

「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。

A.6. カテゴリーF: 脅威情報の収集および分析と評価

A.6.1. F-1. 事後分析

「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。

A.6.2. F-2. 内部脅威情報の収集・分析

「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。

A.6.3. F-3. 外部脅威情報の収集・評価

「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などの情報（外部情報）の収集を実現する。

A.6.4. F-4. 脅威情報報告

「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。

A.6.5. F-5. 脅威情報の活用

「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。

A.7. カテゴリーG: CDC プラットフォームの開発・保守

A.7.1. G-1. セキュリティアーキテクチャ実装

「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。

A.7.2. G-2. ネットワークセキュリティ製品基本運用

「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。

A.7.3. G-3. ネットワークセキュリティ製品高度運用

「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。

A.7.4. G-4. エンドポイントセキュリティ製品基本運用

「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。

A.7.5. G-5. エンドポイントセキュリティ製品高度運用

「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。

A.7.6. G-6. クラウドセキュリティ製品基本運用

「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。

A.7.7. G-7. クラウドセキュリティ製品高度運用

「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。

A.7.8. G-8. 深堀分析ツール運用

「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。

A.7.9. G-9. 分析基盤基本運用

「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に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。

A.7.10. G-10. 分析基盤高度運用

「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。

A.7.11. G-11. CDC システム運用

「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。

A.7.12. G-12. 既設セキュリティツール検証

「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。

A.7.13. G-13. 新規セキュリティツール検証

「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。

A.8. カテゴリーH: 内部不正対応支援

A.8.1. H-1. 内部不正対応・分析支援

「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収集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。

A.8.2. H-2. 内部不正検知・再発防止支援

「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。

A.9. カテゴリーI: 外部組織との積極的連携

A.9.1. I-1. 意識啓発

「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。

A.9.2. I-2. 教育・トレーニング

「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。

A.9.3. I-3. セキュリティコンサルティング

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

A.9.4. I-4. セキュリティベンダー連携

「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。

A.9.5. I-5. セキュリティ関連団体との連携

「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。

A.9.6. I-6. 技術報告

「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。

A.9.7. I-7. 幹部向けセキュリティ報告

「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。

参考文献

[b-ITU-T X.1053] Recommendation ITU-T X.1053 (2017), Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations.