Version 2.1

TLP:WHITE

2019 年 11 月

Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1.0

日本語抄訳

日本語抄訳は日本シーサート協議会によって翻訳された後、JPCERT/CC と NTT-CERT によってレビューされました。FIRST は関係者の協力に深く感謝します。

Notice: This document describes what the Forum of Incident Response and Security Teams, Inc. (FIRST.Org) believes are best practices. These descriptions are for informational purposes only. FIRST.Org is not liable for any damages of any nature incurred as a result of or in connection with the use of this information.

【参考訳】

注意: 本文書は法人である Forum of Incident Response and Security Teams (FIRST.Org) がベストプラクティスと考えているものを記載している。記載内容は情報提供のみを目的としている。FIRST.Org はこの情報を使用した結果として、または関連して被った如何なる性質の如何なる損害についても責任を負わないものとする。

目次

CSIRT サービス・フレームワーク

1 目的

Computer Security Incident Response Team (CSIRT[1])サービス・フレームワークは、C-S-I-R-T およびインシデントマネジメント関連サービスを提供する他のチームが提供する可能性のある、一連のサイバーセキュリティサービスおよび関連する機能を、構造化された方法で収集して記述するハイレベルな[2]文書である。このフレームワークは、Task Force CSIRT (TF-CSIRT)[3] コミュニティと国際電気通信連合 (ITU: International Telecommunications Union) からの強力なサポートを受けた FIRST コミュニティの著名な専門家によって作成されている。

CSIRT サービス・フレームワークのミッションと目的は、特にサービスポートフォリオを選択、拡張、または改善する過程にある支援チームにおいて、CSIRT 運営の確立と改善を容易にすることである。記載しているサービスは、CSIRT が提供し得る可能性があるものであるが、すべてのサービスを提供することは期待されていない。各チームは、任務として掲げている自らのミッションとコンスティチュエンシー[4]をサポートするサービスを選ぶ必要がある。

本フレームワークは、サービスのコアカテゴリとそのサブコンポーネントを特定して定義することにより、チームを支援する。これには、各サービス、サブサービス、機能、および必要に応じてサブ機能のタイトルと説明が含まれている。また、コミュニティ全体で使用される用語と定義の標準セットを特定する一貫性のあるサービス・フレームワークを提供するための出発点である。ただし、この文書は CSIRT またはそれに相当するチームを構築または改善する方法を説明するものではないことに注意され

[1] 訳注:「シーサート」と発音する。

[2] 訳注: ここでは「概観的」「おおまかな」の意味。

[3] 訳注: TF-CSIRT はヨーロッパの CSIRT のコミュニティである。https://tf-csirt.org/

[4] 訳注: ANNEX 2「用語と定義」を参照。「サービス対象」と訳されることもある。

たい。このような情報は他の文書にも記載されており、その一部は付属文書「ANNEX 1」[5]に関係資料として掲載している。

本 CSIRT サービス・フレームワークは、以前の全バージョンを置き換えるものである。CSIRT サービス・フレームワークは、特定のタイプの CSIRT の能力 (ケイパビリティとキャパシティ)[6]、成熟度、品質についての提案やアドバイスをしない。このようなテーマは、すべての CSIRT がコンスティチュエンシーに提供する価値として重要であるが、意図的にこのフレームワークには含めていない。また、実装を検討したり、特定のサービスを実装するための特定の方法を提案したりすることもない。これらのサービスは、コンスティチュエンシーや利害関係者[7]の妥当な期待を満たすことを保証しつつ、多くの異なる方法で実施可能であることを理解することが重要である。

2　イントロダクションおよび背景

Computer Security Incident Response Team (CSIRT) は、ミッションに応じて、コンピュータセキュリティインシデントの防止、検知、処理 (ハンドリング)、および対応のためのサービスと決められたコンスティチュエンシーへのサポートを提供する組織の単位(仮想の場合もある)、または能力 (ケイパビリティ[8])である。

適切に配備されている CSIRT には、明確な任務、ガバナンスモデル、適合したサービス・フレームワークと技術、そして、定義したサービスを提供、評価し、継続的に改善するためのプロセスがある。

CSIRT コミュニティの様々なエンティティ[9]が、長年にわたって独自のサービスリストやフレームワークを開発してきたが、技術、ツール、プロセスが変化するにつれて、コミュニティは既存のリストから漏れているトピックや活動があることを感じるようになった。FIRST は CSIRT の世界的な発展と成熟を可能にすることに関心を持っており、すべての CSIRT や、CSIRT と協働する他のエンティティのための共通言語を

[5] 訳注: ANNEX 3 の誤り。

[6] 訳注: ANNEX 2「用語と定義」を参照。

[7] 訳注: ANNEX 2「用語と定義」を参照。

[8] 訳注: ANNEX 2「用語と定義」」を参照。

[9] 訳注: 個人や組織体などの存在を意味する。

開発する上でこれが重要であると分かった。FIRST メンバーの地理的および機能的な広がりを考慮すると、このコミュニティこそが、CSIRT が提供するサービスの明確な理解と表現のための適切な情報源となりうると判断した。この見解に基づいて、CSIRT サービス・フレームワークの改良版を開発するためのコミュニティ主導のアプローチが開始され、最初のバージョンが 2017 年に出版された。

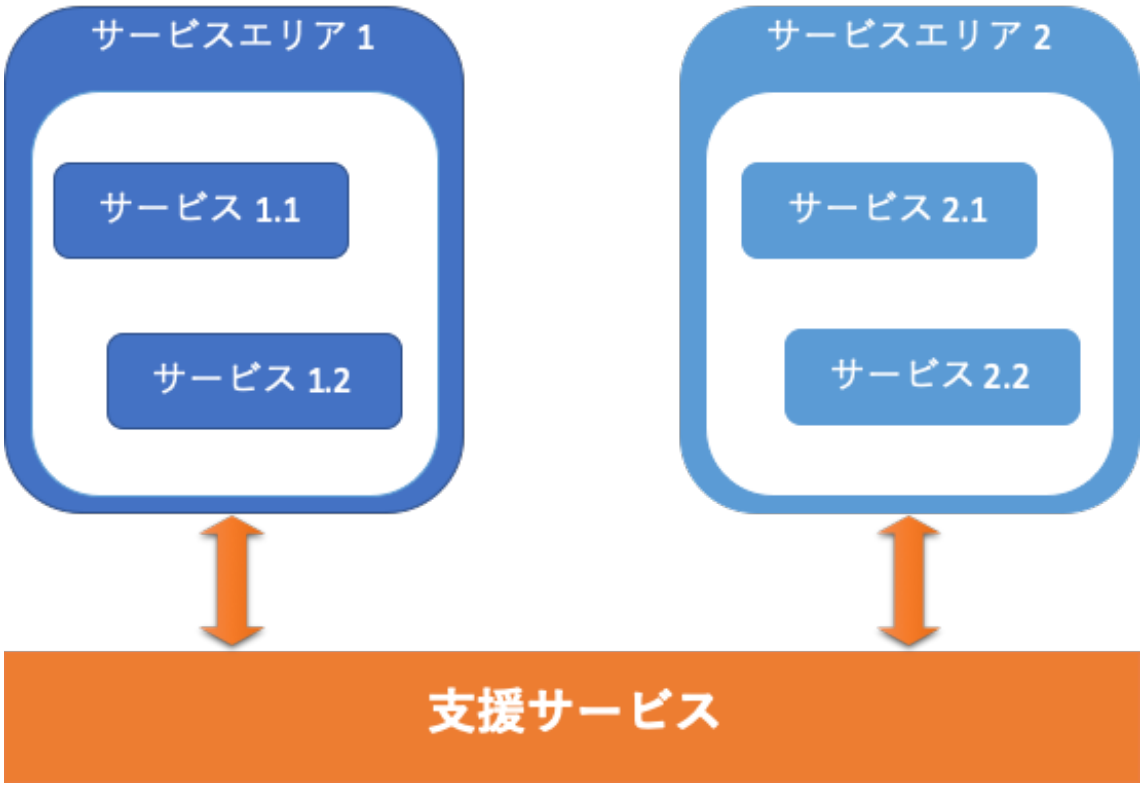
それ以来、Product Security Incident Response Teams (PSIRT)サービス・フレームワークを開発するために、サービスおよび対応する活動の組み合わせとして CSIRT とは異なるものを必要とする運用面が多くあることを認識した上で、同様のアプローチを取ってきた。すべてのサービス・フレームワークは、FIRST の Web サイトに掲載されている[10]。

本文書は、CSIRT サービス・フレームワーク第 2 版の改良版である。第 1 版における複数の専門家からのフィードバックに基づいて、必要に応じて第 2 版を再構成および拡張した。特に、内部の活動はコンスティチュエンシーへのサービス提供を構成するものではないとして削除されている。特定のサービス提供のライフサイクル全体を支援している内部および外部の活動はコンスティチュエンシーに提供されるように設計されたサービスと同様にサービスと機能にまとめることができる。それらのサービスと機能は主に支援サービスとして知られている。例としてスタッフの管理と採用、旅費の精算、または研修イベントの開催等の管理業務が挙げられる[11]。

我々の知る限り、そのような支援サービスを提供するには多くの異なる方法があり、そのほとんどは CSIRT または関連したサービス提供をホストしている組織に依存している。例えば、スタッフの採用と管理は CSIRT を支援する上で確かに必要であるが、それは典型的な組織的支援タスクであり、CSIRT 固有のものではないと考えられる。

[10] CSIRT 関連の資料 https://www.first.org/standards/frameworks/csirts/

[11] 内部支援サービスおよび他のサービスとの関係の議論ついては [Kossakowski 2001] を参照。



内部のサービスと機能はどんなチームまたは組織構成単位にとってもそのミッションの遂行を支えるものであるが、そのようなサービスは FIRST サービス・フレームワークの取り扱う範囲には含まれないと考えられ、したがってこれ以上の詳細または議論は掲載しない。

CSIRT は、新たに出現した脅威に対してコンスティチュエンシーを守るために絶えず変化する課題に直面し続けるので、本フレームワークで取り扱うサービスは、将来のバージョンで必要に応じて、レビュー、審査、および拡張または修正されるであろう[12]。

3 CSIRT と PSIRT の違い

ある組織の CSIRT と、PSIRT のような同じ組織内で代表される他のセキュリティチームとを差別化する主な要因は、提供するサービスに加え、CSIRT はそのコンスティチュエンシーに焦点を当てていることにある。一般的に、PSIRT と他のセキュリティ

[12] FIRST Special Interest Group (SIG) が「CSIRT Framework Development」を運営するために設置されている。

チーム（組織内の CSIRT も含むがこれに限定されない）とを差別化する主な要因は、PSIRT はその組織のプロダクトに焦点を当てていることにある。

組織内では、Enterprise CSIRT[13]は、組織のインフラストラクチャを構成するコンピュータシステムとネットワークのセキュリティに焦点をあてる。大きな組織の中に、複数のセキュリティチームと CSIRT がある場合、それらのうちの 1 つは、調整役として、そして外部関係者への一元化された PoC（Point of Contact）として機能するだろう。このようなチームは Coordinating CSIRT [14]と呼ばれる。

Coordinating CSIRT は、コンスティチュエンシーとして知られる、特定の個人の集まりや組織にサービスを提供する独立したエンティティとして設置されることもある。特定のコンスティチュエンシーに属する組織は、いくつかの共通の特徴(国家研究ネットワークの一部である、特定の国に属している、のような)を有している。
Coordinating CSIRT は、グループ全体の一元化された PoC として機能し、これらの組織の全体的なセキュリティの様相に焦点を当てている。

今日、National CSIRT[15] は、特殊な Coordinating CSIRT として設置され、自国の CSIRT の活動を促進および調整することが多く、また自国民や重要インフラ事業者の特定の部門などを対象に限定されたサービスを提供することもある。

CSIRT と PSIRT の間には重要な違いがあるが、2 つのエンティティの間にも相乗効果があることを認識することが重要である。注意すべき重要な点は、CSIRT と PSIRT の双方が互いに独立して活動しないことである。例えば、多くの CSIRT は、セキュリティ脆弱性をコンスティチュエンシーに警告するが、このようなアラートは、ほとんどの場合、ベンダーの PSIRT が提供する情報に基づいている。

4　CSIRT サービス・フレームワークの構造

CSIRT サービスのためのフレームワークは、4 つの主要な要素の関係に基づいている。

[13] 訳注: 企業内の CSIRT。

[14] 訳注: 主に組織内や国などの調整役として活動する CSIRT

[15] 訳注: 国や地域を代表する CSIRT のこと

「サービスエリア」 → 「サービス」 → 「機能」 → 「サブ機能」

これらの要素を以下のように定義する。

「サービスエリア」

サービスエリアとは、性質の共通した関連サービスをグループ化したものである。これらは、理解とコミュニケーションを容易にするために、トップレベルのカテゴリに沿ってサービスを編成するのに役立つ。各サービスエリアの仕様は、サービスエリアおよびサービスエリア内のサービスのリストを記述する一般的で大まかな説明文からなる「説明」フィールドを含む。

「サービス」

サービスとは、特定の成果を出すための、認識可能で一貫性のある一連の機能である。そのような成果は、コンスティチュエンシーによって、またはエンティティの利害関係者のため、もしくはその利害関係者を代表して、期待または要求されることがある。

サービスは、以下のテンプレートで詳述される。

- サービスの性質を記述する「説明」フィールド。
- サービスの趣旨を記述する「目的」フィールド。
- サービスの測定可能な成果を記述する「成果」フィールド。

「機能」

機能とは、特定のサービスの目的を達成することを目標とした活動、または一連の活動である。どの機能も、複数のサービスのコンテキストで共有および使用される可能性がある。

機能は、以下のテンプレートで説明される。

- 機能の説明を記述する「説明」フィールド。
- 機能の趣旨を記述する「目的」フィールド。
- 機能の測定可能な成果を記述する「成果」フィールド。

- 機能の一部として実行される可能性のあるサブ機能のリスト。

「サブ機能」

サブ機能とは、特定の機能の目的を達成することを目指す活動、または一連の活動である。どのサブ機能も、複数の機能やサービスのコンテキストで共有され、使用される可能性がある。サブ機能は、これらの機能やサービスのいずれかに対して任意に実行されるか、または要求されることがある。

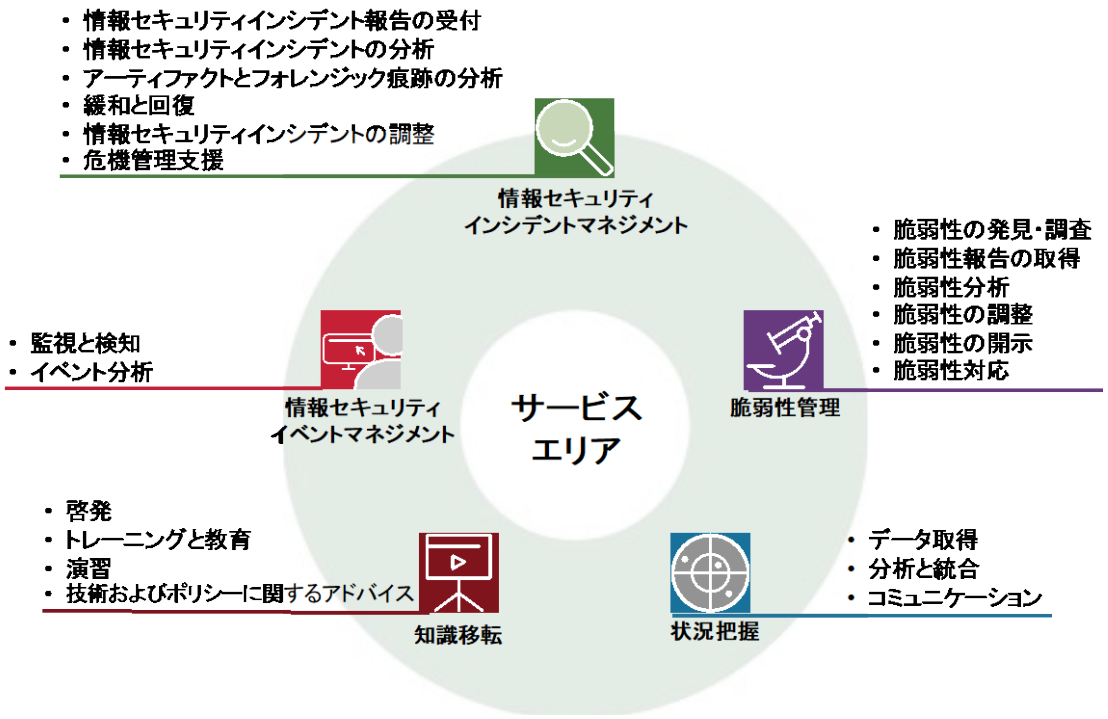
サブ機能は、以下のテンプレートでも説明される。

- サブ機能の説明を記述する「説明」フィールド。
- サブ機能の趣旨を記述する「目的」フィールド。
- サブ機能の測定可能な成果を記述する「成果」フィールド。

CSIRT サービス・フレームワークにおいては、サブ機能は完全に記述されておらず、簡単な特徴だけを述べている。

次の図 (次のページ) は CSIRT サービス・フレームワークのサービスエリアとサービスを示している。サービスエリア、サービスおよび機能のすべてを含めた表は Appendix 4[16]を参照。

[16] 訳注: ANNEX 4 の間違い。


• 情報セキュリティインシデント報告の受付
• 情報セキュリティインシデントの分析
• アーティファクトとフォレンジック痕跡の分析
• 緩和と回復
• 情報セキュリティインシデントの調整
• 危機管理支援
情報セキュリティ
インシデントマネジメント
• 脆弱性の発見・調査
• 脆弱性報告の取得
• 脆弱性分析
• 脆弱性の調整
• 脆弱性の開示
• 脆弱性対応
脆弱性管理
• 監視と検知
• イベント分析
情報セキュリティ
イベントマネジメント
サービス
エリア
• 啓発
• トレーニングと教育
• 演習
• 技術およびポリシーに関するアドバイス
知識移転
• データ取得
• 分析と統合
• コミュニケーション
状況把握

5　サービスエリア:情報セキュリティイベントマネジメント

情報セキュリティイベントマネジメントは、多種多様なイベントやそのコンテキストから得られるデータソースによるセキュリティイベントの相関関係と分析に基づいて、情報セキュリティインシデントを特定することを目的としている。大規模な組織では、このサービスエリアの全体または一部をセキュリティオペレーションセンター(SOC)に割り当てている場合がある。SOC は、被害の緩和やセキュリティコントロールの調整への着手など、第一レベル、ときには第二レベルの情報セキュリティインシデントマネジメントまでも実行する場合がある。すべての情報セキュリティインシデントマネジメントサービスは、情報セキュリティイベントに関する適格で正確なデータに依存するため、SOC と担当 CSIRT の間の連絡が重要である[17]。

以下のサービスはこのサービスエリアで提供されるものと見なされる:

- 監視と検知
- イベント分析

5.1　サービス:監視と検知

目的: 攻撃、侵入、データ侵害、セキュリティポリシー違反などの潜在的な情報セキュリティインシデントを特定するために、多種多様な情報セキュリティイベントソースとコンテキストデータを継続的に処理する自動化された仕組みを実装する。

説明: ログ、NetFlow データ、IDS アラート、センサーネットワーク、外部ソースまたは他の有効な情報セキュリティイベントデータに基づいて、シンプルなロジックまたはパターンマッチング規則や、統計モデル、または機械学習の適用といった様々な方法が潜在的なインシデントを特定するために利用される。これには大量のデータが含まれることがあるが、通常は Security Information and Event Management（SIEM)やビッグデータプラットフォームなどの特殊なツールを必ずしも必要としない。継続的な改善の重要な目的は、 分析サービスの一部として分析する必要がある誤認警報の量を最小限に抑えることである。

[17] このサービス・フレームワークは、SOC のサービス・フレームワークを定義することを目的としていないが、SOC サービスを定義する際には、情報セキュリティイベントマネジメント・サービスエリアとインシデントマネジメント・サービスエリア、双方のサービスが有用であり、そのまま適用できることが確かに期待される。

成果: 分析サービスの一部として潜在的なセキュリティインシデントが特定され、分析される。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- ログとセンサーの管理
- 検知ユースケース管理
- コンテキストデータ管理

5.1.1 機能:ログとセンサーの管理

目的: ログソースとセンサーを管理する。

説明: センサーとログソースは、そのライフサイクルを通して運用管理する必要がある。それらは配置、搭載、撤去される必要があり、機能停止やデータの品質と範囲(スコープ)、および構成(設定)の問題を特定し、解決する必要がある。パターン定義のような何らかの形の設定を有するセンサーは、効果を持続させるためにその設定をメンテナンスする必要がある。また、センサーには、検知ユースケースの基礎となる場合には、外部の検知サービスまたはオープンソース・インテリジェンス(OSINT)の情報源を含めることもできる。

成果: 検知ユースケースのインプットとして関連する情報セキュリティイベントの信頼できる傾向が得られる。

5.1.2 機能:検知ユースケース管理

目的: 検知ユースケースのポートフォリオを、ライフサイクル全体を通して管理する。

説明: 新しい検知アプローチを開発、試験、改善し、最終的に実環境の検知ユースケースに組み込む。アナリストによるトリアージ、適格性や相関分析に関する指示を、プレイブックや標準業務手順書(SOP)のような形式で作成する必要がある。十分に機能しないユースケース、すなわち好ましくない費用対効果を持つユースケースは、改善や再定義をするか、もしくは廃止する必要がある。検知ユースケースのポートフォリオは、リスク指向な方法で予防的コントロールと協調して拡張されるべきである。

成果: コンスティチュエンシーに関連する効果的な検知ユースケースのポートフォリオが開発される。

5.1.3 機能:コンテキストデータ管理

目的: 検知および強化のためのコンテキストデータソースを管理する。

説明: 検知と強化に関与する様々なコンテキストデータソースは、ライフサイクルを通して管理する必要がある。これらは、構成管理データベース(CMDB)、ID およびアクセス管理 (IAM)、脅威インテリジェンスシステムなどの他の IT システムとの間でライブ API をやり取りする場合もあれば、完全に独立したデータセットを手動で管理しなければならない場合もある。後者は、誤検知を抑制するためのインジケータリスト、ウォッチリスト、ホワイトリストの場合である。

成果: 検知および強化のための最新のコンテキストデータが得られる。

5.2 サービス:イベント分析

目的: 検知された潜在的な情報セキュリティインシデントとその適格性をトリアージし、情報セキュリティインシデントとして情報セキュリティインシデントマネジメント・サービスエリアへエスカレーションするか、または誤認警報とするかを認定する。

説明: 検知された潜在的な情報セキュリティインシデントの流れは、手動または自動の分析、あるいはその両方を用いてトリアージされ、それぞれが情報セキュリティインシデント(真陽性)または誤検知(偽陽性)として認定される必要がある。検知ユースケースによっては、追加情報の手動または自動収集が必要になる場合がある。最も重要なものにタイムリーに対応するために、より重要である可能性の高い情報セキュリティインシデントの分析が優先されるべきである。検知された潜在的な情報セキュリティインシデントの適格性確認が構造化されることで、品質に問題のある検知ユースケース、データソース、またはプロセスを特定し、指示された方法で効果的な継続的改善が可能になる。

成果: 適格で相関性のある情報セキュリティインシデントは、情報セキュリティインシデントマネジメント・サービスエリアへ報告でき、誤検知は継続的な改善のために有用である。

以下の機能はこのサービスにおいて実装されるものの一部とみなされる:

- 関連付け
- 適格性確認

5.2.1 機能:関連付け

目的: 他の潜在的または進行中のセキュリティインシデントに直接関連するイベントを特定する。

説明: 同じ資産(例：システム、サービス、顧客)または ID(例：ユーザー)に関連する可能性のある情報セキュリティインシデント、または他の情報セキュリティインシデントに直接関連する可能性のあるインシデントは、重複作業を避けるために、グループ化し、単一の情報セキュリティインシデントとしてエスカレーションする。進行中の情報セキュリティインシデントに直接関連する可能性のある新しい情報セキュリティインシデントは、新たに別のものとして扱うのではなく、その進行中の情報セキュリティインシデントに割り当てる。

成果: 関連する潜在的な情報セキュリティインシデントを、合わせて適格性を確認するためにグループ化する。または、情報セキュリティインシデントマネジメント・サービスエリアで既にハンドリングされている既存の情報セキュリティインシデントにアップデートする。

5.2.2 機能:適格性確認

目的: 真陽性の検知を特定、分類し、優先順位付けするために、検知された潜在的な情報セキュリティインシデントをトリアージして適格性を確認する。

説明: 潜在的な情報セキュリティインシデントは、トリアージされ、それぞれを情報セキュリティインシデント(真陽性)であるか、誤検知(偽陽性)であるか確認する必要がある。アナリストが分析できる潜在的な情報セキュリティインシデントの数は限られているため、そしてアラート疲れを回避するためには、自動化が重要である。成熟したツール化は、コンテキスト情報を充実させ、影響を受ける資産と ID の重要度に基づいてリスクスコアを割り当て、関連する情報セキュリティイベントを自動的に識別することにより、効果的なトリアージを容易にする。自動化可能な何度も繰り返されているようなケースについては特定し、自動化すべきである。重要度のより高い情報セキュリティインシデントは、重要度のより低いものよりも先に分析すべきである。

真または偽陽性を判定する適格性確認に加えて、よりきめ細かな適格性確認は、ログソース、センサーおよびコンテキストデータソースの管理と同様に、検知ユースケースの継続的改善のための重要なインプットである。また、このサービスエリアの成功を測定するためのより質の高い KPI の定義もサポートする。

成果: 適格性が確認された潜在的な情報セキュリティインシデントを、情報セキュリティインシデントマネジメント・サービスエリアの一部としてハンドリングできるようになる。

6　サービスエリア:情報セキュリティインシデントマネジメント

このサービスエリアは、どのような CSIRT にとってもその心臓部にあたり、攻撃またはインシデントの発生中に、コンスティチュエンシーを援助するのに不可欠なサービスで構成される。CSIRT は援助や支援の準備をしなければならない。この独自の立場と専門知識によって、CSIRT は情報セキュリティインシデント報告を収集し評価するだけでなく、関連データを分析したり、インシデント自体や使用されたアーティファクトの詳細な技術的分析を行ったりすることができる。

この分析により、緩和策およびインシデントから回復するための手順を推奨することができ、コンスティチュエンシーはその推奨事項を適用する際にサポートを受けることができる。また、すべての局面に対処し、これから発生する攻撃の成功率を低減するためには、関連する他の CSIRT やセキュリティ専門家、ベンダーや PSIRT のような外部のエンティティとの連携も必要である。

CSIRT が提供できる特別な専門知識は、(情報セキュリティ)危機に対処する上でも重要である。多くの場合、CSIRT は危機管理を行わないが、そのような活動をサポートすることがある。例えば、CSIRT のもつ関係先との繋がりを利用可能にすることにより、必要な緩和手順またはより良い保護メカニズムの適用を大幅に改善できる。

情報セキュリティインシデントマネジメント全体を向上させるためには、知識と利用可能なインフラストラクチャを活用してコンスティチュエンシーをサポートすることが鍵となる。

以下のサービスはこのサービスエリアにおいて提供され得るサービスと見なされる。

- 情報セキュリティインシデント報告の受付
- 情報セキュリティインシデントの分析
- アーティファクトとフォレンジック痕跡の分析
- 緩和と回復
- 情報セキュリティインシデントの調整
- 危機管理支援

6.1 サービス:情報セキュリティインシデント報告の受付

目的: コンスティチュエンシー、情報セキュリティイベントマネジメントサービスまたは第三者から、潜在的な情報セキュリティインシデントの報告を受けて処理する。

説明: CSIRT にとって、最も重要なタスクは、コンスティチュエンシー内のネットワーク、デバイス、コンポーネント、ユーザー、組織、またはインフラストラクチャ、すなわち「ターゲット」に影響を及ぼす情報セキュリティイベントおよび潜在的な情報セキュリティインシデントに関する報告の受付である。CSIRT は、潜在的な情報セキュリティインシデントが、人手を介して、あるいは自動的に、様々な情報源から様々な形式で報告される可能性があることを想定しておく必要がある。

コンスティチュエンシーがより効果的に情報セキュリティインシデントの報告ができるよう、CSIRT は、情報セキュリティインシデントを安全に報告するために、何をどのように報告するかについてのガイダンスや指示だけでなく、1 つ以上の報告手段を提供する必要がある。報告手段には、電子メール、ウェブサイト、情報セキュリティインシデント報告専用フォームまたはポータル、または安全かつ確実に提出することを可能にする他の適切な方法などがある。報告ガイダンスが、情報セキュリティインシデント報告フォームの一部として含まれていない場合は、別の文書またはウェブページで提供されるべきであり、報告に含めることが望ましい特定の情報を列挙するべきである。

情報セキュリティイベントマネジメントサービスを介して検知され、自動的にエスカレーションされる情報セキュリティインシデントが多数発生する可能性があるため、そのようなインターフェースを採用、またはコンスティチュエンシーに使用を許可する前に、この点を計画に含めておかなければならない[18]。

成果: 情報セキュリティインシデント報告は、各々の報告を専門的かつ一貫した考え方で受け入れられ、初期の検証と分類が行われる。

[18] 情報およびデータの取得に関連したすべてのサービスに対して期待されるものとして、多くの類似点がある。それゆえ、いくつかのサービスエリアからそのようなサービスを 1 つのサービス/機能に組み合わせることはよくある。これは必須ではなく、サービスエリアを組み合わせたものはないので、CSIRT サービス・フレームワーク内ではそのようなサービスを分けたままにしておくことにした。もちろん、各チームは自身に最も合った組織モデルを自由に選択して良い。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 情報セキュリティインシデント報告の受理
- 情報セキュリティインシデントのトリアージと処理

6.1.1 機能:情報セキュリティインシデント報告の受理

目的: コンスティチュエンシーまたは第三者から報告された、情報セキュリティインシデントに関する情報を受付または受理する。

説明: 情報セキュリティインシデント報告を効果的に入手するには、コンスティチュエンシー、利害関係者、および第三者(発見者、研究者、ISAC、他の CSIRT など)から報告を受け取るメカニズムとプロセスが必要である。インシデント報告には、影響を受けるデバイス、ネットワーク、ユーザー、組織といったものや、悪用された脆弱性のようにすでに特定された状況、技術レベルとビジネスレベルの両方での影響、および是正措置や緩和措置を開始するために取られたアクション、および潜在的な解決策が含まれることがある。まれに、情報セキュリティインシデントの情報が、他のサービス、特に「脆弱性報告の入手」に対するインプットの一部として一緒に受信されることがある(例えば、脆弱性報告の分析中に特定された情報セキュリティインシデントが報告された場合など)。自動的に提出された報告は、実装されたインターフェースやプロトコルの選択によっては、受理される場合とされない場合がある。

成果: コンスティチュエンシーまたは第三者からの情報セキュリティインシデント報告が適切にハンドリングされる (報告の文書化または追跡の開始を含む)

以下のサブ機能はこの機能の一部と見なされる:

- 定期的にコミュニケーション手段を監視し、通知された CSIRT への連絡手段が機能しているかどうか、および報告を送信できるかどうかをチェックする。
- 情報セキュリティインシデント報告の提出者に初期の受信報告をし、必要に応じて追加情報の提供を求め、報告者とともに見通しを設定する。

6.1.2 機能:情報セキュリティインシデントのトリアージと処理

目的: 報告された情報セキュリティインシデントについて、初めにレビュー、分類、優先順位付け、および処理を行う。

説明: 情報セキュリティインシデント報告は、問題となっている情報セキュリティインシデントの最初の理解を得るためにレビューされてトリアージされる。特に重要なのは、ターゲットに実際に情報セキュリティに関する影響を与え、且つ情報資産またはその他の資産の機密性、可用性、完全性、そして信頼性のすべてまたはいずれかに損害を与える可能性があるか(またはすでに与えているか)どうかである。最初の報告で提供される情報の詳細度と品質によって、実際のインシデントが発生したかどうか、または設定ミスやハードウェア障害などの別の理由があるかどうかが明らかでない場合がある。次のステップは、事前評価に基づいて決定される(例えば、更なる分析のために報告を処理する;報告者または他の情報源からの追加情報を求める;報告がこれ以上の処置を必要としないか、または誤警報であると決定する)。

攻撃は、CSIRT のコンスティチュエンシー内から始まったり、コンスティチュエンシーを標的にしたり、あるいは、コンスティチュエンシーが攻撃の副次的効果によってのみ影響を受けたりする可能性がある。その特定されたターゲットに対して CSIRT が情報セキュリティ管理サービスを提供しない場合、報告は、影響を受ける組織や CSIRT などの外部グループに安全に転送されてハンドリングされる必要がある。

情報セキュリティインシデント報告を拒否する理由があるか、または報告が別のハンドリングを担当するエンティティに転送されていない限りは、その報告を脆弱性分析サービスに渡して、さらにレビュー、分析、およびハンドリングを行う必要がある。

成果: 報告された事項が本当に情報セキュリティインシデントであり、CSIRT によってハンドリングされるか、または関連するエンティティに渡される必要があるかどうかを決定することができる。

以下のサブ機能はこのサービスにおいて実装されるものの一部と見なされる:

- 作業環境の完全性を保護し、そのような手段による CSIRT への攻撃を回避するために、報告および提出されたデータ(アーティファクトまたはマテリアルを含む)を分離した環境で処理する。
- 有効な分類または優先順位付けの結果に基づいて、さらなるステップに関するフィードバックを提供することで報告の承認をアップデートする。

- 一貫した分析と処理を可能にするために、すでにハンドリングされた情報セキュリティインシデントに関する新しい情報を、利用可能なデータへと集約する。

6.2 サービス:情報セキュリティインシデントの分析

目的: 確認された情報セキュリティインシデントを分析して把握する。

説明: このサービスは、攻撃、侵害、または不正使用の成功を許してしまった背後に潜む問題、脆弱性、または弱点(根本原因)を特定するために、情報セキュリティインシデントとその実際および潜在的な影響を把握するための機能で構成されている。

多くの場合、詳細な分析は複雑で時間がかかってしまうものである。 その目的は、その情報セキュリティインシデントの影響に関する現時点での理解から必要とされ、または正当化される範囲において、その情報セキュリティインシデントをできる限り詳細に特定し、その特性を明らかにすることである。情報セキュリティインシデントは、スコープ、影響を受けるエンティティ、使用されたツールまたは攻撃手法、タイムラインなどによって特徴づけることができる。このサービスは、情報セキュリティインシデントの調整サービスおよび機能が実施されている間、または緩和/復旧措置が取られている間、並行して継続実施される場合がある。

CSIRT は、何が起こったのか、そして損失や損害を修復するためにどのようなステップを取るべきかをよりよく理解するために、他の情報や独自の分析（いくつかのオプションについては以下を参照）またはベンダーや製品セキュリティチームあるいはセキュリティ研究者から入手可能な知識を使用することもある。

成果: 情報セキュリティインシデントの重要な詳細(例: 説明(記述)、影響、範囲(スコープ)、攻撃や悪用の手法、修復方法など)に関する知識が増加する。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 情報セキュリティインシデントのトリアージ(優先順位付けと分類)
- 情報収集
- 詳細分析の調整
- 情報セキュリティインシデントの根本原因分析

- クロスインシデント相関

6.2.1 機能:情報セキュリティインシデントのトリアージ(優先順位付けと分類)

目的: 情報セキュリティインシデントを分類し、優先順位を付け、初期評価を行う。

説明: 情報セキュリティインシデントの分析サービスは、情報セキュリティインシデントが CSIRT の任務に関わるシステムに与える影響を分類、優先順位付け、および評価する目的で使用可能な情報をレビューすることから始まる。情報セキュリティインシデントがコンスティチュエンシーまたは第三者によって CSIRT に報告された場合、その一部は、情報セキュリティインシデント報告のトリアージおよび処理機能(情報セキュリティインシデント報告受付サービスに含まれる)の中で既に文書化されている可能性がある。

事前のトリアージがまだ完了していない場合、その情報セキュリティインシデントは、関係するシステムに何らかの影響を与え、且つ CSIRT の任務に関連している(すなわち、ネットワークまたはシステムに対して潜在的にセキュリティ上の影響を及ぼし、CSIRT の任務として関わる情報資産の機密性、可用性、または完全性を結果として損なう可能性がある)ことを技術的に確認できる対象分野の専門家に委ねられることがある。

成果: 情報セキュリティインシデントの情報記録が分類され、優先順位が付けられて、更新される。

6.2.2 機能:情報収集

目的: 情報セキュリティインシデントおよびその一部とみなされるすべての情報セキュリティイベントに関連する情報を取得し、カタログを作成し、保存および追跡する。

説明: すべての価値ある情報の収集を可能にして、コンテキストの最適な理解を得ることで、情報の出所と内容を適切に評価してタグ付けし、その後の処理に使用できるようにする。

情報を収集する際に、どのようなデータをどのようなコンテキストで、どのような形式の処理で使用するかについて合意した共有ポリシーと制限を受け入れ、遵守する必要がある。また、収集の仕組みと手順においては、後に妥当性や真正性とともに出所

を検証するために、情報源の適切な表示と属性が用いられるようにしなければならない。

成果: 収集されたデジタルおよび非デジタルのデータまたはメタデータに関する構造化された情報が利用可能であり、追跡情報およびハンドリングと保存の両方の完全性を管理するポイントが含まれる。その結果が将来の(非公式の)分析に使用されるか、法執行活動に使用されるかによって、後のいずれかの段階で、法廷で弁護できる正式な管理過程の確立に関して異なる要件が存在する。

以下のサブ機能はこの機能において実装されるものの一部と見なされる:

- データおよび情報を提供する情報源の評価および妥当性確認
- 手動、自動または機械読み取り可能な形式の如何を問わず、悪意のあるまたは疑わしいイベントや、情報セキュリティイベント、エスカレーションされた潜在的な情報セキュリティインシデント、関係者および第三者(他のセキュリティチームや商用の情報提供など)からの情報セキュリティインシデント報告の収集
- インシデント活動の理解に役に立つという保証はないがその可能性があるデジタルデータ(例えば、ディスクイメージやメモリイメージ、メタデータを含むファイル、またはチェックサム、ネットワークアーキテクチャ特性、ログなど)の収集とカタログ化 (これには、敵対活動の形跡と考えられるアーティファクトが含まれるが、これに限定されない)
- 非デジタルデータ(例えば、物理的なサインインシート、アーキテクチャ図、ビジネスモデル、サイト評価データ、ポリシー、エンタープライズリスクフレームワークなど)の収集とカタログ化
- ソース、収集の方法、データまたはオブジェクトを扱った人物、所有者および保管情報に関するメタデータの収集とカタログ化(特に、後にフォレンジック分析または法執行活動の証拠と見なされる場合があるため)

6.2.3 機能:詳細分析の調整

目的: インシデントに関するその他の技術分析を開始して追跡する。

説明: より詳細な技術的分析が必要となる場合には、他の専門家(ホスト組織または CSIRT の内部または外部)または他の第三者(そのような分析に特化したサービスプロバイダなど)が実施することがある。これには、求められる分析を達成させるまで、そのような活動の開始から追跡する必要がある。

成果: 保留中および(情報セキュリティインシデントへの対応を調整しているインシデントハンドラの観点から)アウトソースした分析のリストが得られる。

6.2.4 機能:情報セキュリティインシデントの根本原因分析

目的: インシデントの根本原因を特定するため、悪用された脆弱性が存在したり、悪用が成功したりするのを許してしまった状況(ユーザーの行動を含むが、それに限定されない)を特定する。

説明: この機能には、システム、ネットワーク、ユーザー、組織などを、情報セキュリティインシデントのターゲットとして実行される攻撃、不正利用、または侵害等の原因になった、またはそれらの行為にさらすことになった、アーキテクチャ、使用方法、または実装上の欠陥を理解するために必要なプロセスとアクションが含まれる。また、攻撃者が最初のアクセスをもとにより多くのシステムに侵入して、さらなるアクセスを取得する可能性がある状況も考慮する。

情報セキュリティインシデントの性質によっては、CSIRT がこの機能を完全に実行することが難しい場合がある。多くの場合、特に Coordinating CSIRT の場合は、侵害されたシステムやネットワークについての詳細な技術的知識を持たないため、この機能は影響を受けた対象自身で実施するのが最適かもしれない。

成果: 情報セキュリティインシデントと、悪意のある行為者が最初にアクセスを獲得し、さらにそれを利用していく方法を理解する。その結果、根本的な原因を排除することによって将来の暴露や悪用のリスクを最小化するための是正方法や緩和方法を決定することができる。

6.2.5 機能:クロスインシデント相関

目的: 利用可能なすべての情報を使って、コンテキストを最大限に理解し、それ以外の方法では認識されなかった、または対処できなかった相互関係を検知できるようにする。

説明: この機能では、複数の情報セキュリティインシデントに関して使用可能な情報を相互に関連付け、すでにクローズされている情報セキュリティインシデントから相互関係、傾向または適用可能な緩和策を決定し、現在ハンドリングされている情報セキュリティインシデントへの対応を改善する。

成果: 個別と考えられていた情報セキュリティインシデントとの類似点や、確認された、または疑われる相互関係についての詳細な知識に基づいて、状況把握の観点から全体像が理解できる。

6.3 サービス:アーティファクトとフォレンジック痕跡の分析

目的: フォレンジックの証拠保全の必要性を考慮して、確認された情報セキュリティインシデントに関連するアーティファクトを分析し、理解する。

説明: アーティファクト(マルウェア、エクスプロイト、揮発性メモリダンプまたはディスクコピー、アプリケーションコード、ログ、文書など)の機能と目的、その伝達機構、伝播、検知、緩和、および無害化または無効化の見解に関するサービス。これは、ハードウェア、ファームウェア、メモリ、ソフトウェアなど、あらゆる形式およびソースに適用される。あらゆるアーティファクトや証拠は、変更せずに保存および収集し、隔離しておく必要がある。一部のアーティファクトおよびデータは、法執行活動の文脈において証拠となることがあるため、特定の規制または要件が適用されることがある。

このサービスでは、管理過程を維持しなくても、通常、複雑で時間のかかるタスクが伴い、専門知識、専用の監視分析環境を設定する必要がある。それは、標準の有線ネットワークまたはワイヤレスネットワーク(例えば、密閉された部屋やファラデーケージでフォレンジックを行うような場合)からの外部アクセス、活動の記録、および手順への準拠の有無にかかわらない。

情報セキュリティインシデントのハンドリングの一環として、影響を受けるシステムまたはマルウェア配布サイトにデジタル・アーティファクトが見つかる場合がある。アーティファクトは、実行可能ファイル、スクリプト、ファイル、イメージ、構成ファイル、ツール、ツール出力、ログ、使用中または使用されていないコードなど、侵入者による攻撃の残骸である場合がある。

分析は、以下の情報の一部またはすべてを見つけるために実行されるが、これは完全なリストと見なされるものではない。

- 悪意があるかどうかにかかわらず、アーティファクトが実行され、意図したタスクを実行するのに必要なコンテキスト
- アーティファクトが攻撃にどのように利用された可能性があるか（組織の環境またはコンポーネント内でアップロード、ダウンロード、コピー、実行、または作成等されたか）
- 配布とアクションをサポートするために、ローカルやリモートのどのシステムが関係しているか
- システム、ネットワーク、組織、またはインフラストラクチャへのアクセスが確立された後、侵入者[19]は何を行ったか（受動的なデータ収集から積極的なスキャンとデータ窃取目的での転送まで、または新しい活動のリクエストの収集、あるいは自身のアップデート、侵入した（ローカル）ネットワーク内での横展開等）
- ユーザーアカウントまたはユーザーデバイスが侵害された後、ユーザー、ユーザープロセス、またはユーザーシステムが何を行ったか
- ローカルネットワークまたはインターネットに接続されているか、スタンドアロンモードで動作しているかアーティファクトまたはコンポーネントと連携しているか、といったあらゆる条件の組み合わせの中で、アーティファクトまたは侵害されたシステムの動作にどのような特徴が見られるか
- アーティファクトまたは侵害されたシステムがターゲットとの接続をどのように確立するか(侵入経路、初期ターゲット、検知回避手法など)
- どのような通信アーキテクチャ(peer-to-peer, command-and-control またはその両方)が使用されているか
- 脅威の主体はどのような行動をとったか、そのネットワークとシステムのフットプリントはどのようなものか
- 侵入者やアーティファクトがどのようにして検知を逃れたか(再起動や再初期化を含むような長時間にわたるケースも考慮する)

[19] 訳注:ここでは侵入行為を行った人物だけでなく、マルウェアなどの侵入行為に用いられたツールも含まれる。

これは、以下のような様々な種類の活動を通じて達成することができる。

- メディアまたはサーフェス分析
- リバース・エンジニアリング
- ランタイムまたは動的解析
- 比較分析

各活動は、アーティファクトに関する追加情報を提供する。分析方法は、これに限定されるものではないが、アーティファクトのタイプおよび特徴の識別、既知のアーティファクトとの比較、ランタイムまたはライブ環境におけるアーティファクト実行の観察、およびバイナリ・アーティファクトの分解および解釈を含む。

分析者は、アーティファクト分析を行うにあたり、悪用された脆弱性を検知し、損害を評価し、アーティファクトに対する緩和解決策を開発し、コンスティチュエンシーや他の研究者に情報を提供することを目的に、侵入者が何をしたかを再構築して判断するよう試みる。

成果: 復元されたデジタル・アーティファクトの性質や分析されたフォレンジックの証拠を、他のアーティファクト、内部または外部のオブジェクトまたはコンポーネント、フレームワーク、ツールへの攻撃、および悪用された脆弱性との関係に沿って理解する。脅威の主体が何をしたか、およびアーティファクトがどのように動作したかについての現時点で有力な仮定または証明を行う。この知識は、損失、損害、ビジネスへの影響などを評価し、封じ込めと緩和または復旧の戦略を策定するために重要である。攻撃者または侵入者がシステムやユーザー、ネットワーク、組織、インフラストラクチャを侵害するために使用する戦術、テクニック、および手順を理解する。これには伝播、抽出、更新、変更、自身の動作やデータの偽装、自身の活動の痕跡の自動削除、悪意のある活動の追加実行等に使用される戦術、テクニック、および手順が含まれる。

このサービスにおいて実装されるものの一部と見なされる機能のリスト:

- メディアまたはサーフェス分析
- リバース・エンジニアリング
- ランタイム解析や動的解析

- 比較分析

6.3.1 機能: メディアまたはサーフェス分析

目的: アーティファクトから収集された情報を、他のパブリックおよびプライベートのアーティファクトや署名リポジトリと比較する。

説明: アーティファクトに関する基本情報とメタデータ（ファイルの種類、文字列の出力、暗号化ハッシュ、証明書、ファイルサイズ、ファイル名、ディレクトリ名を含むがこれに限らない）の特定と特性付けを行う。利用可能なすべての情報が収集され、さらに分析されることで、アーティファクトまたはその動作についてさらに知るために、パブリックでオープンな、またはプライベートでクローズドなソース情報リポジトリをレビューするのに使用することができ、このような情報は次のステップを決定するために使用することができる。

成果: デジタル・アーティファクトの特徴や署名を特定し、且つ、悪意、影響、緩和を含む、そのアーティファクトについて既に知られている情報を特定する。

6.3.2 機能:リバース・エンジニアリング

目的:アーティファクトの完全な機能を、その実行環境に関係なく断定するために、アーティファクトの詳細な静的分析を行う。

説明: マルウェアのアーティファクトをより詳細に分析し、隠しアクションや動作の引き金となるコマンドを特定する。リバース・エンジニアリングによって、アナリストは難読化やコンパイル(バイナリ)をすり抜け、ソースコードを発見するか、またはバイナリをアセンブリ言語に分解して解釈することで、マルウェアを構成するプログラム、スクリプト、またはコードを特定できる。それらさらけ出された、マシン語によって書かれていた、マルウェアが実行できるすべての機能とアクションを明らかにする。すべての機能と、マルウェアが実行できるアクションを検知する。リバース・エンジニアリングとは、サーフェス解析とランタイム解析で必要な情報がすべて提供されない場合に行う詳細な解析のことである。

成果: アーティファクトがどのように動作するか、何を引き金に動作するか、悪用され得る関連するシステムの弱点、攻撃を完全に受けた場合の影響、および潜在的な損害を理解するために、デジタル・アーティファクトの全機能を引き出す。これはアーテ

ィファクトを緩和するソリューションを開発し、適切であれば、他のサンプルと比較するための新しいシグネチャを作成することを目的としている。

以下のサブ機能はこの機能において実装されるものの一部と見なされる:

- 静的解析
- コードのリバース・エンジニアリング
- 潜在的な動作の分析と説明
- 潜在的なシグネチャのデザイン

6.3.3 機能:ランタイムまたは動的解析

目的: アーティファクトの操作に関する洞察を提供する。

説明: 実際の環境またはエミュレートされた環境(サンドボックス、仮想環境、ハードウェアまたはソフトウェアエミュレータなど)でサンプルを実行しながら、観察によってアーティファクトの機能を理解する。

シミュレート環境を使用すると、ホスト、ネットワーク・トラフィックおよび実行からの出力に対する変更を取得できる。基本的な前提として、実際の状況に可能な限り近い状態で、稼働中のアーティファクトを観察する。

成果:影響を受けるホストシステム、他のシステムのやり取り、および結果として生じるネットワーク・トラフィックへの変更を断定するために、実行中の動作の観察から、デジタル・アーティファクトの動作に対する更なる見解を得る。これはシステムの損傷と影響をよりよく理解し、新しいアーティファクト署名を作成し、緩和手順を決定することを目的として行われる。

注意: すべてのコード・セクションを動作させられない可能性もあるため、ランタイム分析からすべての機能が明らかになることはない。ランタイム分析では、マルウェアがテスト状況で何をしているかを見ることができ、できること全てを見ることができるわけではない。

以下のサブ機能はこの機能において実装されるものの一部と見なされる:

- 解析環境の準備(ライブ/制限/クローズド、エミュレート/シミュレート)

- コレクターや、センサー、プローブの準備
- 初期動作データとメタデータの収集
- 様々なコンテキストでのアーティファクトの複数回の精査
- システムやネットワークの挙動解析を短期および長期の両方で実施する。
- 収集したすべての結果とデータを評価し、様々な結果を比較し、また今回の発見に一致する既存の技術的結果を求めて利用可能なナレッジベースを調査することによって結論を導き出す。

6.3.4 機能:比較分析

目的: カタログ化されたアーティファクトのファミリー分析など、共通の機能または意図の特定に重点を置いた分析を行う。

説明: アーティファクトと他のアーティファクトとの関係を調べる。これにより、コードまたは手口、ターゲット、意図、作成者の類似性を識別できる。そのような類似性は、攻撃の範囲(つまり、より大きなターゲットがあるか、以前に同様のコードが使用されているかなど)を導き出すために使われる。

比較分析技術は、完全一致比較またはコード類似性比較を含むことができる。比較分析では、アーティファクトまたはその類似バージョンがどのように使用され、時間の経過に伴ってどのように変更されたかをより広い視野で把握できるため、マルウェアまたはその他の悪意のある種類のアーティファクトの評価を把握するのに役立つ。

成果: デジタル・アーティファクトの機能、影響、および緩和についての新たな洞察または理解を提供する可能性のある傾向、または類似点を特定するために、他のアーティファクトとの共通点または関係が導き出される。

以下のサブ機能はこの機能において実装されるものの一部と見なされる:

- 特徴および観察された行動のベースラインの定義。
- 利用可能なリポジトリやナレッジベースでの同一または類似の特性の検索。
- 新たに観察された、または以前には知られていなかった症状や、動作、研究されたアーティファクトをさらに分類するために使用できるシグネチャに関して、利用可能なリポジトリやナレッジベースを更新する。

6.4 サービス:緩和と回復

目的: インシデントによる被害者数を制限し、損失を減らし、被害から回復するために可能な限りインシデントの封じ込めを行い、また悪用された脆弱性や弱点を除去することにより更なる攻撃や損失を回避して、全体的なサイバーセキュリティを改善する。

説明: 分析によって潜在的な情報セキュリティインシデントを確認し、対応戦略を策定したら、これを対応計画に切り替える必要がある。対応計画が最終決定される前であっても、アドホックな[20]措置がとられることがある。このサービスには、情報セキュリティのインシデントがクローズされたと見なされるまで、またはさらなる分析を必要とする新しい情報が入手可能になるまでに実行されるすべての活動の開始および追跡も含まれ、これ以降、対応戦略および計画も変更される可能性がある。

成果: 情報セキュリティインシデントの緩和とサイバーセキュリティ態勢の改善。潜在的な攻撃または攻撃者の活動によって影響を受けたシステムの完全性を回復し、ネットワークおよび侵害されたシステムの保守性を回復する。可能であれば、データが失われた場合にデータを復元する。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 対応計画の策定
- 一時的な対策と封じ込め
- システムの復旧
- 他の情報セキュリティエンティティの支援

Coordinating CSIRT の場合、すべての機能を提供するわけではない。「他の情報セキュリティエンティティの支援」はそのようなチームが提供する活動であるが、「対応計画の策定」を支援することもある。

6.4.1 機能:対応計画の策定

目的: 影響を受けたシステムの完全性を回復し、影響を受けたデータ、システム、およびネットワークを劣化していない動作状態に戻し、元のセキュリティ問題が再び悪用

[20] 訳注:「その問題限定の暫定的な」の意味。

されるコンテキストを再生することなく、影響を受けたサービスを完全な機能に復元する計画を定義して実施する。

説明: ビジネスへの影響と緩和および回復の要件を十分に理解しなければ、意味のある対応を提供できない。利益相反があるか、より多くの情報を得るために攻撃を追跡するのか、さらなる損失を避けるために攻撃を封じ込めるのか、すべての利害を考慮し、既知の事実に対処し、要求された期間内に望ましい結果を提供するために妥当な対応計画を策定する必要がある。

すべての計画と同様に、新しい解析結果を得た場合は常に、新しい結果を考慮する必要があることを検討しなければならない。実際、継続的なオリエンテーションとガイダンスを提供するためには、通常、対応計画を変更する必要がある。そのような計画がなければ、外部インターフェースや他のエンティティをほとんど必要とせずに、対応を単一の小さな組織グループでハンドリングしない限り、調整不足により、効果的・効率的な活動が行われない可能性がある。

成果: 利用可能なリソースとサポートがあれば、ビジネス要件を満たす合意済みの対応計画が実行される。CSIRT による追跡と調整は、「調整」サービス[21]によって提供されるであろう。

以下のサブ機能はこの機能において実装されるものの一部と見なされる:

- 情報セキュリティインシデントによるビジネスへの影響を特定する。
- 回復を成功させるためのビジネス要件とタイムフレームを決定する。
- 意思決定のプロセスと基準の定義(ポリシーによってまだ定義されていない場合)。
- 回復する対象 (環境、システム、アプリケーション、システム、横断的な機能など) を特定する。
- 内部および外部のエンティティによる必要なサポートとアクションを特定する。

[21] 訳注:「 6.5 サービス:情報セキュリティインシデントの調整」。

- 利用可能なリソースと必要なアクションの技術的範囲に基づいて、望ましいビジネス要件とタイムフレームの中で意味のある対応を提供できる対応計画を決定する。

6.4.2 機能:一時的な対策と封じ込め

目的: 情報セキュリティインシデントがこれ以上拡大しない、すなわち、現在影響を受けているシステムやユーザー、ドメインに限定して、これ以上の損失(文書の漏えい、データベースまたはデータの変更等を含む)が発生することがないように保証する対策を実施する。

説明: 情報セキュリティインシデントが発生した場合の緊急の課題は拡散を阻止することである。システムが侵害されたり、エンドユーザーシステム上でマルウェアが活動したりしている間は、データの損失が増えるだけでなく、さらに多くの侵害が発生する。通常、攻撃の主な目的は特定のデータやシステムに到達することであり、情報セキュリティインシデントの被害を受けている組織の内外の他の組織に対する攻撃(横展開を含むが、それに限定されない)も含まれる。悪意のある活動またはそれ以上の損失を阻止する、または少なくともその範囲を制限するには、トラフィックをブロックまたはフィルタリングし、特定のサービスまたはシステムへのアクセスを遮断するなどの短期的なアクションが必要であり、重要なシステムの接続を切断することになる可能性もある。

重要な証拠となる可能性のあるデータへのアクセスを拒否することで、そのような証拠の完全な分析が可能になる。また、他のシステムやネットワークへのさらなるアクセスを拒否することは、他の組織への損害に対する自組織の責任範囲を制限することにもなる。

トラフィックのブロックやフィルタリング等の短期的な戦術的行動によって、直ちに被害を食い止め、悪意ある行為の影響範囲を制限することは、システムの制御を取り戻すことにもつながる。攻撃者またはアクティブなマルウェアがより多くのシステムまたはネットワークにアクセス可能である限り、通常のオペレーションに戻すことはできない。

成果: 発生したインシデントに関与するシステムおよびネットワークの制御の回復。攻撃者およびマルウェアによるデータ、システム、およびネットワークへのアクセスを拒否し、さらなる攻撃やシステムおよびデータの侵害を回避する。

以下のサブ機能はこの機能において実装されるものの一部である可能性がある:

- ユーザーやシステム、サービス、ネットワークのアクセスを一時的に遮断する。
- システムまたはネットワークをネットワークやシステムの中枢から一時的に切断する。
- サービスを一時的に無効化する。
- ユーザーにパスワードまたは暗号証明書の変更を要求する。
- 侵入の兆候と IoC（セキュリティ侵害インジケーター）を監視する。
- すべてのユーザーやシステム、サービス、ネットワークが影響を受けていないことを確認する。

6.4.3 機能:システムの復旧

目的: 影響を受けたドメインやインフラストラクチャ、ネットワークの修復および、同様の活動の再発防止に必要な変更を行う。

説明: 影響を受けたシステムの完全性を復元し、影響を受けたデータ、システム、およびネットワークを劣化のない動作状態に戻し、影響を受けたサービスを完全に機能する状態に復元する。現実のビジネスではシステムをできるだけ早く通常のオペレーションに戻す必要があるため、不正アクセスのすべての手段が正常に取り除かれていない可能性がある。したがって、解析結果が入手可能でない限り、復旧済みのシステムであっても注意深く監視し、管理しなければならない。特に、特定された脆弱性や弱点を(まだ)排除できない場合は、同一または類似の情報セキュリティインシデントを回避するために、改善された保護および検知メカニズムを適用する必要がある。

成果: システムとサービスを完全な機能と能力（キャパシティ[22]）に復元するための措置を適用する。最初の情報セキュリティインシデントの原因となった、検知された脆弱

[22] 訳注: ANNEX 2「用語と定義」を参照。

性または弱点を塞ぐための対策を適用する。分析・対応計画の推奨通り検知・対応方法を改善する。

以下のサブ機能はこの機能において実装されるものの一部と見なされる:

- 信頼できるバックアップ・メディアからユーザーやシステムのデータを復旧する。
- 信頼できるバックアップ・メディアまたは再作成されたコンテンツから設定を復旧する。
- 無効にしたサービスを有効にし、ユーザーやシステム、ネットワークへのアクセスを再確立する。
- 機能テストを実行して、インフラストラクチャとアプリケーションの両方のレベルでシステムやサービス、ネットワークの能力（キャパシティとケイパビリティ）[23]を検証する。

6.4.4 機能:他の情報セキュリティエンティティの支援

目的: 情報セキュリティインシデントを適切に緩和し、また情報セキュリティインシデントから回復するために必要な管理および技術的活動を、コンスティチュエンシーが実行できるようにする。

説明: CSIRT は、コンスティチュエンシーが損失から回復し、脆弱性を取り除くための直接的な(オンサイト)支援を提供することがある。これは先述した、オンサイトでの分析サービスの提供の直接的な延長となる場合がある。一方、CSIRT は、情報セキュリティインシデントに対応するコンスティチュエンシーのスタッフを、より詳細な説明やアドバイスなどで支援する、という選択をすることもある。

成果: コンスティチュエンシーの対応が改善され、復旧が高速化する。利用可能な知識体系に新たな知識を追加することによって、関連する活動のその後の有効性と効率性が強化される可能性がある。さらに、対応に必要な行動を実行するための詳細な技術的知識を欠いているコンスティチュエンシー内の当該エンティティを支援するのに役立つ。

[23] 訳注: ANNEX 2「用語と定義」を参照。

6.5 サービス:情報セキュリティインシデントの調整

目的: タイムリーな通知と正確な情報配信を確保する。情報の流れを維持し、情報セキュリティインシデントへの対応を任された、または要請されたエンティティの活動状況を追跡する。対応計画が実行されていることを確認し、遅延または新しい情報の両方によって生じる、計画からの逸脱を適切に管理する。

説明: 情報セキュリティインシデントに関する詳細および進行中の活動について通知を受け、また継続的に情報を与えられることは、関係するすべての利害関係者および組織にとって重要である。緩和と回復を達成するために必要な活動の中には、管理者の承認を必要とするものがあるため、情報セキュリティインシデントが効果的かつ効率的にハンドリングされる前に、適切なエスカレーションと報告の機能を確立する必要がある。CSIRT がすべての情報をそれが利用可能になり次第分析していく一方で、調整においては、通知と情報が適切な連絡先に確実に届くようにし、対応状況を追跡し、活動中のすべての関係者の報告を確実に行うことで、情報セキュリティインシデントが終了し、それ以上の調整を必要としないと見なされるまで、正確な状況把握を提供できるようになる。

利害関係者は、質問をしたり、情報セキュリティインシデントの状況をチェックしたり、問題を CSIRT に報告したりする手段を持つべきである。内部の利害関係者と連携するために、CSIRT は、情報セキュリティインシデントの修復状況を通知するための通信チャネルを提供するべきである。外部の利害関係者と連携するために、CSIRT は、アドバイスや技術サポートを提供してくれる可能性のある他の CSIRT やコミュニティとの通信チャネルを維持する必要がある。

成果: 十分に情報を与えられたエンティティによる貢献をもとに、情報セキュリティインシデントへの対応が適切に調整される。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- コミュニケーション
- 通知の配信
- 関連情報の配信
- 活動の調整

- 報告
- メディアとのコミュニケーション

6.5.1 機能:コミュニケーション

目的: 利害関係者と効果的に連携し、必要とされる機密性を提供する、適切な複数のコミュニケーションチャネルを確立する。

説明: CSIRT は、コミュニケーションの手段を用意し、使い始める際には、最も正確な受取手を考慮しておかなければならない。そしてまた、CSIRT はそのコミュニケーションに基づいて、様々なソースから入ってくるフィードバック、報告、コメント、および質問を受け取れる備えがなければならない。

セキュリティポリシーや情報共有ポリシーでは、情報の厳格な取り扱いが求められる場合があり、CSIRT は、外部と内部の両方で、信頼性があり、安全でプライベートな方法で利害関係者と情報共有ができなければならない。

機密保持契約はできるだけ事前に締結し、それに応じてコミュニケーションリソースを設定する必要がある。その延長として、「情報の禁輸措置」という概念も使用できる。したがって、これらの制約が無効になるか、情報が公開されるまで、時間などの制約に基づいて、情報の作成に使用するデータと情報自体の両方が適切に処理、共有、保存されることを保証するために、保存ポリシーも確立する必要がある。

コミュニケーションチャネルは利害関係者とコンスティチュエンシーのニーズに基づいて複数の形を取ることができる。やり取りするすべての情報には、情報共有ポリシーに従ってタグを付ける必要があり、トラフィック・ライト・プロトコル（TLP）を使用することもある。

成果: すべてのコミュニケーションチャネルが、すべての受信者および送信者のセキュリティ要件に従って使用できる。

以下のサブ機能はこの機能において実装されるものの一部と見なされる:

- 内部とのコミュニケーションチャネルを提供する
- 外部とのコミュニケーションチャネルを提供する

6.5.2 機能:通知の配信

目的: 情報セキュリティインシデントの影響を受けるエンティティ、またはインシデントへの対応に貢献できるエンティティにアラートを送る。また、これらのエンティティに対して、それぞれの役割や、期待される可能性のある協力や支援について理解してもらうのに必要な情報を提供する。

説明: 情報セキュリティインシデントは、多くの内部、および場合によっては外部のエンティティと関りがあり、システムとネットワークに関係する可能性もある。CSIRTは、潜在的な情報セキュリティインシデントの報告を受信するための中心的なポイントであるため、それらについて、認可された連絡先に通知するためのハブとしての役割も果たす。この通知は、通常、技術的詳細だけでなく、予想される対応に関する情報や、フォローアップのための連絡先も提供する。

成果: 情報セキュリティインシデントに関する情報を、対応に加わることを求められるエンティティ、およびそれについての通知を受ける必要のあるエンティティが利用可能になる。

6.5.3 機能:関連情報の配信

目的: 特定されたエンティティとのコミュニケーションを維持し、それらのエンティティが利用可能な洞察と教訓から利益を得たり、改善された対応を適用したり、新たなアドホックな措置を講じたりできるようにするために、利用可能な情報の適切な流れを提供する。

説明: 情報セキュリティインシデントへの対応が進むにつれて、潜在的であった他のセキュリティ専門家、CSIRT、または被害者によるより多くの分析結果と報告が得られる。

特に新しい攻撃やインシデントの傾向が特定された場合は、トレーニングや技術文書を改善し、適切な認識を促すために、知識伝達サービスエリア(サポートされている場合)に情報や教訓の一部を渡すことが役立つ場合がある。

成果:利用可能な情報が、インシデント対応に加わる責任がある者、または進捗状況や現在の状況を常に把握する必要のある者に配布される。

6.5.4　機能:活動の調整

目的: すべてのコミュニケーションと活動の状況を追跡する。

説明: 情報セキュリティインシデントの対応には多くのエンティティが関与する可能性があるため、すべてのコミュニケーションと活動の状況を追跡する必要がある。これには、CSIRT によって要求された行動またはさらなる情報の共有の要求、および、アーティファクトの技術的分析または危険性の指標、他の被害者についての情報共有の要求などが含まれる。これは主に、CSIRT がインシデントを緩和するための必要なアクションを実行するために、CSIRT の直接的なコントロール外の専門知識とリソースに依存しているときに起こる。しかし、それは、内部の CSIRT が緩和と回復活動を調整する、より大きな組織内でも起こる。

二国間または多国間の調整を提供することによって、CSIRT は情報交換に参加し、攻撃者による進行中の活動の検知、保護、または修復において、行動を起こす能力を備えたこれらのリソースを可能にしたり、他のリソースを支援したり、情報セキュリティインシデントを終結させたりできるようにする。

成果: 全ての活動の現在の状況や、インシデント対応に加わっているエンティティの状況についての認識が得られる。

6.5.5　機能:報告

目的:次のステップに関するさらなる決定が、その時点で可能な最良の状況把握に基づくよう、事業内のすべての関係エンティティが、確実に現在の活動状況に関する情報を持っているようにする。

説明: 情報セキュリティインシデントへの対応として要求または実行された活動の、現在の状況に関する簡潔で事実に基づいた情報を提供する。効果的な連携を可能にするためには、インシデント対応の成功のために必要とされる、進行中の連携したアクションの一部としてそのような情報がもたらされるのを待つのではなく、タイムリーな報告を行うことが重要である。

成果: 内部の利害関係者には、現在の活動の範囲、すでに完了している活動、保留中の活動が通知される。評価された遅延の影響や勧告および要請された措置についても伝

達され、選択した対応戦略および策定した計画に関する全体的な影響について理解できるようにする。

6.5.6 機能:メディアとのコミュニケーション

目的: 風評や誤解を招くような情報の流布を避けるために、進行中のイベントに関する正確で分かりやすい、事実に基づいた情報を提供できるように(公共の)メディアと連携する。

説明: 多くの場合、メディアとのコミュニケーションは利用できない。CSIRT は通常、そのような接触を避けようとするが、情報セキュリティインシデントを引き起こす、特定のタイプの進行中かつ大規模な攻撃を緩和するのにメディアが役立つこともあるのを理解することは重要である。そのためには、インシデントの原因および、ユーザーや組織への影響を説明する必要がある。場合によっては、一般公開するのに適した方法で情報を提供することを選ぶかもしれないが、その場合大抵は、すぐには習得できない、CSIRT 内部の特定のスキルを必要とする。いずれにしても、CSIRT がメディアとやり取りをする場合、技術的な問題を可能な限り単純化し、すべての機密情報を除外するように細心の注意を払わなければならない。

成果:進行中の情報セキュリティインシデントについての明確な要約を提供する、事実に基づいた情報が得られる。今後被害者となりうる者が取るべき措置についての情報や、選択された、情報セキュリティインシデントから回復するための対応戦略の概略も得られる。

6.6 サービス:危機管理支援

目的: 危機の緩和を支援するため、他のセキュリティ専門家、CSIRT、および CSIRT コミュニティに専門知識と連絡先を提供する。

説明: 今日の情報セキュリティインシデントが組織的または国家的な危機を引き起こす要素となることはまれであるが、そうなる可能性はある。しかし、危機への対応は通常、人間と社会全体の福利、あるいは少なくとも組織の存在を脅かす緊急事態と関連している。危機管理で定められているように、上層部が危機の責任を引き継ぎ、緊急時の通常の指揮系統を変更する。

システムやネットワークが緊急時の対応に貢献する可能性がある、または危機的状況に対応するために利用可能であることが要求されるので、CSIRT は通常、そのような状況を管理し、貴重な経験を提供するだけでなく、確立されたサービスや連絡先ネットワークを提供する重要なリソースともなる。

成果: 危機管理チームは、CSIRT のリソースを使用して、現在の危機のサイバーセキュリティの側面に対処できる。同時に、CSIRT のコミュニケーションリソースは、特定の支援措置や支援を要請する目的でコンスティチュエンシーや外部関係者と接触するために利用される可能性がある。また、確立された通信手段と信頼できるネットワークを使用して、信頼できる方法でコンスティチュエンシーとやり取りをするためにも使用できる。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- コンスティチュエンシーへの情報配信
- 情報セキュリティの状況報告
- 戦略的意思決定の伝達

6.6.1 機能:コンスティチュエンシーへの情報配信

目的: 危機への対処を支援するために確立されたコミュニケーションリソースを提供する。

説明: 危機への対応が進むにつれて、情報を発信し、広く知れ渡らせる必要がある。CSIRT は自身の目的のためにそのようなリソースを築き上げているため、危機管理においてそういったリソースを使うことが適切である、あるいは必要であるとされることがある。

成果: 広められた情報の正確さについて受信者が安心できるような、確立された信頼関係の恩恵を受けつつ、利用可能な情報をコンスティチュエンシーに発信する。

6.6.2 機能:情報セキュリティの状況報告

目的: 危機管理チームが、現在の情報セキュリティインシデントと既知の脆弱性の完全な概要を把握し、これを全体的な優先事項と戦略の一部として検討できるようにする。

説明: コンスティチュエンシー内のサイバーセキュリティの現状に関する簡潔かつ事実に基づく情報を提供する。危機は他の攻撃を開始するために使われる可能性もあり、また発生中の攻撃がこの危機をもたらす全体的な活動の一部であるかもしれないため、危機管理チームが完全に状況を把握することは非常に重要である。

CSIRT は、そのサービスとコンスティチュエンシーにおいてそのような状況把握を提供することができる。これは、危機の際に標準的なポリシーによって要求、または期待される可能性がある。いずれにしても、危機の最も重要な側面への対処は調整のためのリソースに依存しており、危機管理は確立された情報の流れに基づいてのみ成功するものであるため、報告はタイムリーかつ正確でなければならない。

進行中の情報セキュリティインシデントのハンドリングには、リソースが必要となるため、インシデントが発生している間は対応を中止するか(そして現在使用可能なリソースを他の領域に割り当てるか)、継続するかを決定する必要がある。合理的な意思決定は、利用可能な最良の状況把握に基づいてのみ行うことができる。

成果: 危機管理チームは、現在の活動の範囲、すでに完了している活動、および保留中の活動について知らされる。評価された遅延の影響、アドバイスおよび要請された措置についても伝達され、現在の危機に対処するために選択された戦略に関する全体的な影響を理解できるようになる。

6.6.3 機能:戦略的意思決定の伝達

目的: 現在起きている情報セキュリティインシデントに対して危機が与える影響について、他のエンティティにタイムリーに情報提供する。

説明: 現在起きている情報セキュリティインシデントに対して危機が与える影響について、他のエンティティにタイムリーに情報提供することで、危機の最中に CSIRT によってどのような支援が提供されうるか明確に理解され、また何を期待すべきかも確実に理解される。さらに、危機が優位になっていると考えている可能性のある他の当事者は CSIRT とのサポートまたはやり取りを確実に止めるようにもなる。

危機管理チームは、危機が原因で実際の情報セキュリティインシデントへの対応を延期することを決定する場合があるため、そのような決定は、現在情報の提供を受け、関与しているすべてのエンティティに伝達する必要がある。これは、CSIRT やホスト

組織に対する信頼の喪失につながる可能性のある誤解、およびさらなる問題を避けるためである。

成果: 危機がもたらす CSIRT 運営に対する影響についての情報が、進行中の情報セキュリティインシデントへの対応に関係しているコンスティチュエンシーや他のエンティティに発信される。そのようなエンティティに対する CSIRT の期待が明確に記述されており、CSIRT の情報ニーズが確実に、明確に伝達される。

7　サービスエリア:脆弱性管理

脆弱性管理サービスエリアには、情報システムにおける新たな、または報告されたセキュリティ脆弱性の発見、分析、およびハンドリングに関連するサービスが含まれる。また、既知の脆弱性が悪用されるのを防ぐための、既知の脆弱性の検知と対応に関連するサービスも含まれる。したがって、このサービスエリアには、新しい脆弱性と既知の脆弱性の両方に関連するサービスが含まれる。

「脆弱性管理」という用語は、単に既知の脆弱性が悪用されるのを防ぐ(例:「スキャンとパッチ」)プロセスを指すために使われることがあるが、この CSIRT サービス・フレームワークでは、これらの活動を、脆弱性対応と呼ばれるサービスの下に分類される機能およびサブ機能と見なす。脆弱性対応は、CSIRT が提供する可能性のあるサービスのひとつである。多くの CSIRT にとって、これらの脆弱性対応機能は、セキュリティ脆弱性をスキャンし、修正する他の役割に対して責任を負うものである。

以下のサービスはこのサービスエリアにおいて提供されるものと見なされる。

- 脆弱性の発見・調査
- 脆弱性報告の取得
- 脆弱性分析
- 脆弱性の調整
- 脆弱性の開示
- 脆弱性対応

これらのサービスのすべてを提供する CSIRT はほとんどないが、その代わり、自らの責任の範囲に該当するサービスのみを提供するであろう。例えば、ある CSIRT は、自身の提供するサービスを、公的なソース(脆弱性の発見や調査)または第三者(脆弱性報告の取得)から新しい脆弱性の情報を得ることに限定し、必要に応じて、コンスティチュエンシーにセキュリティアドバイザリを発行する(脆弱性情報の開示)かもしれない。この場合、ソリューションを開発する製品ベンダーや他のベンダーとの調整作業に必ずしも参加したり(脆弱性の調整)、修正の直接展開に関与したり(脆弱性対応)することはない。

7.1 サービス:脆弱性の発見・調査

目的: 脆弱性管理サービスエリアのメンバーによって、または他の関連する CSIRT 活動を通じて、新しい(以前は未知であった)脆弱性を発見、学習、または検索する。

説明: 新しい脆弱性の発見は、脆弱性管理ライフサイクル全体をスタートさせるために必要な最初のステップである。このサービスには、CSIRT が自身の調査または他のサービスを通して新しい脆弱性を発見するために積極的に実行する可能性のある機能と活動が含まれている。第三者から新しい脆弱性情報を受動的に受理することに関連する機能や活動については、後述の「脆弱性報告の取得」で説明する。インシデント報告の分析や調査など CSIRT が他の活動をしている際に新しい脆弱性を発見することがある。新しい脆弱性を知る他の方法としては、公開されている情報源(Web サイト、メーリングリスト[24]など)やその他の外部情報源(プレミアムサービスやサブスクリプション)を購読すること、意図的な調査(例えばファズ・テスト、リバース・エンジニアリングなど)によって積極的に脆弱性を探すことがあげられる。このような発見は、脆弱性が CSIRT によってどのように発見または知られたかにかかわらず、文書化され、組織の脆弱性ハンドリングプロセスへ渡される必要がある。

成果: このサービスにより、CSIRT に直接報告されなかった潜在的な脆弱性の発見が増加する。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- インシデント対応の脆弱性発見
- 公的情報源による脆弱性の発見
- 脆弱性調査

これらの機能は、CSIRT の代わりに他の個人・組織(研究者、ベンダー、PSIRT、第三者の専門家など)によってサービス(または機能)として行われることがある。

[24] 電子メールで受領した新しい脆弱性情報は、CSIRT の内部プロセスまたは脆弱性情報の流通範囲によって、脆弱性の発見サービス、公的情報源による脆弱性の発見機能、脆弱性報告の取得サービス、または脆弱性報告の受理機能の活動と考えられることがある。

7.1.1 機能:インシデント対応の脆弱性発見

目的: セキュリティインシデントの一部として悪用された脆弱性を特定する。

説明: セキュリティインシデントの分析中に、脆弱性が攻撃者によって悪用されたことを示す情報を検知する場合がある。パッチが適用されていなかった、または緩和されていなかった既知の脆弱性が悪用され、インシデントが発生する可能性がある。あるいは、新しい(ゼロデイ)脆弱性が原因である可能性もある。

インシデントの一部として脆弱性が悪用された場合、この脆弱性情報の一部を、情報セキュリティインシデントマネジメント・サービスエリア内の 1 サービスから受信する可能性がある。その後、必要に応じて、脆弱性のトリアージ機能または脆弱性分析サービスに情報を渡すことができる。

成果: インシデントの一部として悪用された疑いのある脆弱性に関する情報が、脆弱性管理サービスエリアに渡される。

7.1.2 機能:公的情報源による脆弱性の発見

目的: 公的情報源またはその他の第三者の情報源を参照して、新しい脆弱性について知る。

説明: CSIRT は、脆弱性情報を公表している様々なパブリックソースから、新しい脆弱性について初めて知る可能性がある。ソースには、ベンダーの発表、セキュリティ Web サイト、メーリングリスト、脆弱性データベース、セキュリティカンファレンス、ソーシャルメディアなどが含まれる。また、この機能は、有償サブスクリプションやプレミアムサービスなどを利用して一部のグループのみと情報共有する場合など、完全には公開されていない可能性がある他の第三者のソースから、新しい脆弱性を検知する場合もある。スタッフには、この機能を実行し、さらなるレビューと共有のために情報を収集して整理する責任を割り当てることができる。同様の脆弱性情報は、状況把握サービスエリアのサービスからも受信する可能性がある。

成果: 公的情報源またはその他の外部情報源を通じて公開された新しい脆弱性を特定する。

7.1.3 機能:脆弱性調査

目的: 意図的な活動または調査の結果として、新しい脆弱性を発見または探索する。

説明: この機能は、ファズ・テスト(fuzzing)を使用したシステムまたはソフトウェアのテストや、マルウェアのリバース・エンジニアリングなど、特定の CSIRT 活動の結果として新しい脆弱性を発見することを含む。

また、情報セキュリティインシデントマネジメント・サービスエリアまたは状況把握サービスエリアのサービスからインプットを受け取ることで、脆弱性があると疑われるものを探すためにこの機能を開始することもある。

この脆弱性調査機能の結果として新しい脆弱性が発見されると、インシデント対応サービスの脆弱性検知機能(「脆弱性スキャンおよび脆弱性ペネトレーションテスト」のサブ機能を参照)にインプットされることがある。

成果: 調査によって新しい脆弱性を特定する。

7.2 サービス:脆弱性報告の取得

目的: コンスティチュエンシーまたは第三者から報告された脆弱性情報を受理および処理する。

説明: 脆弱性情報の主要な情報源の 1 つは、CSIRT のコンスティチュエンシーまたは他の第三者から送信される報告または問合せである可能性がある。CSIRT は、これらの様々な情報源から脆弱性が報告される可能性を予測し、脆弱性報告のためのメカニズム、プロセス、およびガイダンスを提供する必要がある。報告インフラストラクチャには、電子メールまたは Web ベースの脆弱性報告フォームを含む場合がある。すべての脆弱性が、コンスティチュエンシーまたは第三者によって、規定したチャネルを通じて CSIRT に直接報告されるわけではない。支援ガイダンスには、報告のガイドライン、連絡先情報および開示方針を含むべきである。

コンスティチュエンシーがより効果的に脆弱性を報告することを可能にするために、CSIRT は、脆弱性を安全に報告するために何をどのように行うかについてのガイダンスまたは指示とともに、1 つ以上の報告手段を提供する必要がある。報告手段には、電子メールや Web サイト、専用の脆弱性報告フォームまたはポータル、その他、報告

を安全かつ確実に提出できるようにする適切な方法が含まれる。報告ガイダンスが、脆弱性報告フォーム自体に含まれていない場合、独立した文書またはウェブページを通じてガイダンスを提供し、報告に含めることが望ましい特定の情報を列挙するべきである。

成果: 個々の脆弱性報告が専門的で一貫性のある形で、初期検証と分類をともなって受領される。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 脆弱性報告の受理
- 脆弱性報告のトリアージと処理

7.2.1 機能:脆弱性報告の受理

目的: コンスティチュエンシーまたは第三者から報告された脆弱性に関する情報を受付または受理する。

説明: 脆弱性報告を効果的に入手するには、関係者、利害関係者、および第三者(発見者、研究者、ベンダー、PSIRT、他の CSIRT や脆弱性コーディネーターなど)から報告を受け取るメカニズムとプロセスが必要である。脆弱性情報には、影響を受けるデバイス、脆弱性を不正利用するために必要な条件、影響(権限昇格、データアクセスなど)、および脆弱性を解決するために実行されたアクション、修復・緩和ステップ、および解決 策が含まれることがある。場合によっては、脆弱性情報が他のサービスへのインプットの一部として受信されることがある。最も顕著なのは、インシデント報告の受信(例えば、インシデント報告の一部として脆弱性が悪用されたことが報告された場合)である。

成果: コンスティチュエンシーまたは第三者からの脆弱性報告が適切にハンドリングされる(報告の文書化または追跡の開始を含む)。

以下のサブ機能はこの機能の一部と見なされる:

- 定期的にコミュニケーションチャネルを監視し、CSIRT への連絡手段が機能しているかどうか、および報告を送信できるかどうかをチェックする。

- 脆弱性報告の提出者に受領した旨を報告し、必要に応じて追加情報を要求し、報告者の期待を設定する。

7.2.2 機能:脆弱性報告のトリアージと処理

目的: 脆弱性報告の初期レビュー、分類、優先順位付け、および処理を行う。

説明: 脆弱性報告は、問題となっている脆弱性の初期の理解を得て、次に何をすべきかを決定するためにレビューされ、評価される(例えば、更なる分析のために脆弱性を処理し、報告者または他の情報源から追加情報を求め、これ以上脆弱性対策を必要としないと判断する等)が、提供される情報の詳細度と品質によっては、新しい脆弱性が存在するかどうかが不明な場合がある。

脆弱性報告を拒否する理由がない限り、報告は脆弱性分析サービスに渡され、さらにレビュー、分析、およびハンドリングをする必要がある。CSIRT が脆弱性分析サービスを提供しない場合、報告を、影響を受けるベンダーまたは PSIRT、あるいは脆弱性コーディネーターなどの外部グループに安全に転送してハンドリングする必要がある。

成果: 次に何をすべきかを決定するために有効な情報を特定する。

以下のサブ機能はこのサービスにおいて実装されるものの一部と見なされる:

- 作業環境の完全性を保護し、そのような保護手段によって CSIRT への攻撃を防げるように、報告書および提出されたデータ (アーティファクトや資料を含む)を外部から切り離して処理する。
- 利用可能な、分類または優先順位付けの結果に基づいて、さらなるステップに関するフィードバックを提供することで、報告の認識を更新する。
- すでにハンドリングされている脆弱性に関する新しい情報と利用可能なデータを集約し、一貫した分析と処理を可能にする。

7.3 サービス:脆弱性分析

目的: 確認された脆弱性を分析し、理解する。

説明: 脆弱性分析サービスは、脆弱性とその潜在的な影響についての理解を深める機能、脆弱性の悪用を可能にする潜在的な問題または欠陥(根本原因)を特定する機能、

および脆弱性の悪用を防止する、または最小限に抑えるための修復・緩和戦略を特定する機能で構成される。

脆弱性分析サービスおよび機能は、協調的な脆弱性公開(CVD)[25]プロセスに加わっている他者と共に脆弱性調整サービスおよび機能が実行されるのと並行して継続される可能性がある。

成果: 脆弱性を理解する上で鍵となる詳細に関する知識(説明、影響、解決など)が蓄積される。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 脆弱性のトリアージ(検証と分類)
- 脆弱性の根本原因分析
- 脆弱性対策開発

7.3.1 機能:脆弱性のトリアージ(検証と分類)

目的: 脆弱性を分類し、優先順位を付け、初期評価を行う。

説明: 脆弱性分析サービスは、脆弱性の分類と優先順位付けをし、また、それが関係するシステムに何らかの影響を与えうるか、および CSIRT の任務の範囲で取り扱うのが妥当かを判断するための評価をする目的で、利用可能な情報をレビューすることから始まる。脆弱性がコンスティチュエンシーまたは第三者によって CSIRT に報告された場合、その一部は、脆弱性報告のトリアージおよび処理機能(脆弱性報告の取得サービスに含まれる)の中で既に文書化されている可能性がある。

事前のトリアージがまだ完了していない場合、その脆弱性は、関係するシステムに何らかの影響を与え、且つ CSIRT の任務に関連している(すなわち、ネットワークまたはシステムに対して潜在的にセキュリティ上の影響を及ぼし、CSIRT の任務として関わる情報資産の機密性、可用性、または完全性を結果として損なう可能性がある)ことを技術的に確認できる対象分野の専門家に委ねられることがある。

[25] 協調的な脆弱性の公開 (CVD: coordinated vulnerability disclosure) の関連情報については脆弱性の調整および脆弱性の開示サービスエリアを参照。

成果: 脆弱性の情報記録が分類され、優先順位が付けられて、更新される。

7.3.2 機能:脆弱性の根本原因分析

目的: 脆弱性の原因となった、またはその存在を顕在化する設計上または実装上の欠陥を理解する。

説明: この分析の目的は、脆弱性の根本原因を特定し、脆弱性の存在を可能にする状況、および攻撃者がその脆弱性を不正利用できる状況を特定することである。この分析はまた、インシデントを引き起こすために活用される弱点と、その弱点を活用するスパイ活動に必要な敵対的ノウハウを理解する試みが行われることもある。

脆弱性の性質によっては、CSIRT がこの機能を完全に実行することは困難かもしれない。場合によっては、この機能が脆弱性の発見者または報告者によってすでに実行されていることがある。多くの場合、この機能は、影響を受けるソフトウェアまたはシステムの製品ベンダーまたは開発者、あるいはそれぞれの PSIRT によって実行されるのが最適かもしれない。また、脆弱性が複数の製品に存在する可能性もある。この場合、影響を受けるソフトウェアまたはシステムに対し複数の分析が必要になり、複数のベンダー、PSIRT、または利害関係者との調整が必要になる。

成果: 脆弱性と、悪意のある行為者がこの脆弱性をどのように使用できるかを理解して、暴露や悪用のリスクを最小限に抑えるための修復または緩和方法を決定する。

7.3.3 機能:脆弱性対策開発

目的: 潜在的な脆弱性を修正(是正)するため、または脆弱性が悪用される影響を緩和(軽減)するために必要な手順を開発する。

説明: この機能は、理想的には脆弱性の是正策または修正策を特定するものである。ベンダーが提供するパッチや修正プログラムが適切なタイミングで入手できない場合は、影響を受けるソフトウェアを無効にしたり、設定を変更したりするなど、一時的な解決策や回避策が推奨されることがある。これは、脆弱性の潜在的な悪影響を最小限に抑えるためである。修復(パッチ)または緩和(回避策)の実際の適用または導入は、このフレームワークでは脆弱性対応と呼ばれる別のサービスの機能であることに注意されたい。

脆弱性分析サービスおよび脆弱性対策開発の一部として、この機能には、手順または設計の変更の検証、第三者による修復のレビュー、または修復ステップで導入された新しい脆弱性の特定など、その他のサブ機能または活動をオプションとして含めることができる。是正または緩和されていない脆弱性は、許容可能なリスクとして文書化されるべきである。

この機能は、多くの場合、影響を受ける製品のベンダーから情報またはインプットを受け取るが、他のサービスまたは機能によってハンドリングされる初期報告またはアナウンスの一部として受け取ることもある。

成果: 特定の攻撃ベクトル[26]を閉じ、脆弱性の悪用を防止するために、ソフトウェアコードの変更(パッチ適用)、回避策の実装、またはプロセス、インフラストラクチャ、設計の改善を行うための計画を策定する。

以下のサブ機能はこの機能の一部と見なされる:

- 脆弱性修正・パッチ開発
- 脆弱性緩和策開発

この機能は通常、他のエンティティ(例えば、製品ベンダーや PSIRT)によって実行される。

7.4 サービス:脆弱性の調整

目的: 協調的な脆弱性の公開(CVD)プロセスに関与する関係者と情報を交換し、活動を調整する。

説明: ほとんどの脆弱性のハンドリングでは、脆弱性の発見者・報告者、影響を受けるベンダー、開発者、PSRIT[27]、または脆弱性を分析して修正するために協力できるその他の信頼できる専門家(研究者、CSIRT、脆弱性コーディネーター)など、複数の関係者との関連情報の交換に関する通知、連携、および調整が行われる。

[26] 訳注: 一般的に「攻撃に使われる方法や経路」の意味。

[27] 訳注: PSIRT の間違い。

成果: 脆弱性を修正・緩和するための情報提供を支援できる CVD 参加者との情報共有が効果的かつタイムリーに行われる。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 脆弱性の通知・報告
- 脆弱性利害関係者の調整

7.4.1 機能:脆弱性の通知・報告

目的: その他の CVD プロセスの関係者に新しい脆弱性情報を最初に共有または報告する。

説明: ほとんどの脆弱性のハンドリングでは、影響を受けるベンダー、開発者、PSIRT、または脆弱性を分析して修正するために協力できる他の信頼できる専門家(研究者、CSIRT、脆弱性コーディネーター)など、複数の関係者との関連情報の交換に関する通知、連携、および調整が行われる。

成果: ベンダー(または他の CVD 参加者)は脆弱性について知らされ、修正または緩和策を開発するために行動できる。

7.4.2 機能:脆弱性利害関係者の調整

目的: 協調的な脆弱性の公開(CVD)の取り組みに関与する様々な利害関係者および参加者の間で継続した調整と情報共有を行う。

説明: 脆弱性の分析と修正を行い、脆弱性の開示に備えるために、協調的な脆弱性の公開(CVD)の取り組みにおいて、発見者・研究者、ベンダー、PSIRTS、およびその他の参加者間の情報交換を調整する。この調整には、開示の時期および時期の調整に関する参加者の合意も含めるべきである。

成果: 修正・緩和策を開発または発表できる関係者間で、脆弱性情報をより効果的に、タイムリーに、責任を持って共有できる。

以下のサブ機能はこの機能の一部と見なされる:

- 脆弱性の公表の発展[28]

7.5 サービス:脆弱性の開示

目的: 既知の脆弱性に関する情報をコンスティチュエンシーに周知し、コンスティチュエンシーがその情報に基づいて既知の脆弱性を予防、検知、および修正・緩和するための行動が取れるようにする。

説明: システムを最新の状態に保ち、不正利用を監視できるように、既知の脆弱性(攻撃者の潜在的な侵入ポイント)をコンスティチュエンシーに通知する。開示方法には、複数のコミュニケーションチャネル(Web サイト、電子メール、ソーシャルメディアなど)、脆弱性データベース、または他の媒体を介した情報の公表が含まれることがある。このサービスは、常にではないが、脆弱性の調整後に行われることが多い。

成果: コンスティチュエンシーに情報を提供することで、既知の脆弱性が悪用される可能性を事前に回避し、既に存在している脆弱性を検知して緩和することができる。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 脆弱性開示ポリシーとインフラストラクチャの整備
- 脆弱性の公表・連絡・周知
- 脆弱性開示後のフィードバック

7.5.1 機能:脆弱性開示ポリシーとインフラストラクチャの整備

目的: CSIRT が脆弱性をハンドリングして開示する方法、および脆弱性を開示するために使用されるメカニズムについて、フレームワークを提供し、期待値を設定するポリシーを策定し、維持する。

説明: 脆弱性報告をハンドリングする CSIRT は、脆弱性開示ポリシーを定義し、そのポリシーを自身のコンスティチュエンシー、利害関係者、CVD 参加者が利用できるようにすべきであり、可能であれば CSIRT のウェブサイトで公開することが望ましい。脆弱性の開示方針は、利害関係者[29]に透明性を提供し、適切な開示方針の推進に役立つ。ポリシーには、脆弱性に関する情報が開示されていない場合の非開示から、一部

[28] 訳注: 関係者間の調整をすることで脆弱性情報の公表を促進すること。

[29] 訳注: ANNEX 2「用語と定義」を参照。

の情報のみが公開されている場合の限定開示、概念実証のための攻撃を含むすべての情報が開示されている場合の完全開示まで、様々なものがある。開示ポリシーには、ポリシーの範囲、報告メカニズムおよびガイドラインへの言及、脆弱性の開示に予想される期間およびメカニズムなどの要因を含める必要がある。

成果: 情報開示に対する信頼、協力、管理が強化され、CVD 関係者との関係および連携が改善される。

7.5.2 機能:脆弱性の公表・連絡・周知

説明: 脆弱性を検知、修正、または緩和し、将来の脆弱性の不正利用を防止できるようにコンスティチュエンシー(または一般の人々)に情報を提供する。

説明: 定められたコンスティチュエンシーに脆弱性情報を開示する。開示は、脆弱性開示ポリシーで特定されたメカニズムのいずれかまたはすべてを通じて行うことができる。周知のメカニズムは、対象者のニーズや期待によって異なる。コミュニケーションは、電子メールまたはテキストメッセージを介して配布される告知またはセキュリティアドバイザリ、ウェブサイトまたはソーシャルメディアチャネルに投稿される発表、または必要に応じてその他のコミュニケーション形態およびチャネルの形で行うことができる。開示に含まれる内容は、予め定義されたフォーマットに従う必要がある。これには、一般的に、脆弱性の概要または説明、固有の脆弱性識別子、影響度・深刻度または CVSS スコア、解決策(是正または緩和)、および参考文献や資料などの情報が含まれる。

成果: タイムリーで高品質で効果的な情報をコンスティチュエンシー(または公衆)に提供することで、脆弱性を予防、検知、および是正・緩和する。

7.5.3 機能:脆弱性開示後のフィードバック

目的: 脆弱性の開示または文書に関する、コンスティチュエンシーからの質問または報告を受領し、回答する。

説明: 新たな脆弱性が開示された後、CSIRT は脆弱性文書について一部のコンスティチュエンシーから質問という形で、その後の連絡を受けることが期待される。質問を受けて、必要に応じて、脆弱性の開示メカニズムの明確化、改訂、または修正をする場合がある。コンスティチュエンシーからの情報は、単に脆弱性文書に対する感謝や

受領確認である場合もあれば、提案された修復・緩和策の実施における問題または困難性を報告するものである場合もある。脆弱性がすでに悪用されていると判断された場合、コンスティチュエンシーは新たに発見されたインシデントをその脆弱性開示の結果として報告している可能性がある。このような報告は、CSIRT のインシデント報告サービスの機能にインプットする必要がある。

成果: 脆弱性の開示後、質問や支援要請があった場合にタイムリーに対応できる。

7.6 サービス:脆弱性対応[30]

目的: 既知の脆弱性に関する情報を積極的に取得し、その情報に基づいて脆弱性の防止、検知、および修正・緩和を行う。

説明: このサービスの機能は、開示された脆弱性がコンスティチュエンシーのシステムに存在するかどうかを判断することを目的としており、多くの場合、そのような脆弱性の存在を意図的に探すことによって実施される。また、パッチや回避策を導入することで、脆弱性を修正または緩和する追加アクションもこの機能に含めることもできる。

成果: 脆弱性の存在を検知し、開示された脆弱性を修正・緩和し、脆弱性の悪用を防止するために情報が処理される。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 脆弱性の検知・スキャン
- 脆弱性の修正

この脆弱性対応サービスとその関連機能は、通常、組織内の他の専門グループ (通常は CSIRT ではない) によって実行される。また、このサービスが、Coordinating CSIRT によって提供される可能性は低い。

[30] 脆弱性検知の機能およびサブ機能は「脆弱性管理」と呼ばれることがあるが、この CSIRT サービス・フレームワークでは代わりに脆弱性対応サービスの一部と呼ぶことにする。脆弱性対応サービスはこのフレームワークで脆弱性管理と名付けた、より大きなサービスエリアの一部である。

7.6.1 機能:脆弱性の検知・スキャン

目的: 設置されたシステムに既知の脆弱性が存在するかどうかの調査に積極的に取り組む。

説明: この機能の目的は、前もってパッチが適用されていない、または緩和されていないあらゆる脆弱性を、それらが悪用される、またはネットワークやデバイスに影響を与える前に検知することである。この機能は、新しい脆弱性に関する告知に応じて開始されるか、既知の脆弱性を定期的にスキャンするスケジュールの一部として実行される。脆弱性の検知を効果的に行うには、システムのインベントリを作成しておくと便利である。ソフトウェアのバージョン情報を照会できるこのようなインベントリを持つことで、組織はそのインフラストラクチャで新たに報告された脆弱性の普及率を迅速に評価できる。

この機能は、他のサービスや機能からインプットを受ける、または他のサービスや機能をきっかけに実施されることがある。

成果: 脆弱性を特定するために設計された正式なプロセスまたはツールによって、脆弱性が検知される。

以下のサブ機能はこの機能の一部と見なされる:

- 脆弱性のスキャン・探索
- 脆弱性のセキュリティ評価・ペネトレーションテスト

この機能は通常、他のエンティティ(IT サービス、SOC、第三者の専門家、システム所有者など)によって実行される。

7.6.2 機能:脆弱性の修正

目的: 脆弱性が悪用されないようにするために脆弱性を修正または緩和する。通常は、ベンダーが提供するパッチまたはその他のソリューションをタイムリーに適用する。

説明: 脆弱性の修正は、脆弱性を解決または排除することを目的としている。ソフトウェアの脆弱性の場合、これは通常、ソフトウェアの更新またはパッチの形式でベンダーが提供するソリューションの導入およびインストールによって実施される。承認されたパッチが利用または導入できない場合は、脆弱性の不正利用を防ぐ対策として、

代替の緩和策または回避策を適用できる。この機能は、多くの場合、脆弱性の検知・スキャン・探索機能の結果を受けて、脆弱性を明確に識別した後に実行される。

成果: 脆弱性が悪用される脅威にさらされるのを防止または軽減する。

以下のサブ機能はこの機能の一部と見なされる:

- 脆弱性の修正(パッチ管理)
- 脆弱性の緩和

この機能は、通常、CSIRT ではなく、他者(IT、SOC、システム所有者など)によって実行される。

8　サービスエリア:状況把握

状況把握サービスエリアは、コンスティチュエンシーの活動または任務に影響を与える可能性がある、CSIRT の責任範囲内およびその周辺で起こっていることの重要な要素を識別し、処理し、理解し、伝達する能力を含む、現在の状態を認識すること、およびその状態に対する潜在的な変化を識別または予測することも含まれる。また、様々なエリアから関連情報を収集する方法、その情報を統合する方法、およびコンスティチュエンシーがより多くの情報を得た上で意思決定を行えるようにタイムリーに情報を発信する方法の決定も含まれる。組織によっては、状況把握(のサービスエリア)を提供するために別のチームを設置することもあるが、そうでない場合、CSIRT チームは、その可視性、コンテキストの理解、技術的能力、資産へのアクセス、外部接続、およびインシデントを防ぐ使命に基づいて、この機能を提供する。状況把握は、インシデントへの対応だけに焦点を当てているのではなく、セキュリティイベントマネジメント、インシデントマネジメント、および知識伝達などの他のサービスがデータ、分析、およびアクションを確実に利用可能とするためのサービスでもある。また、他のサービス分野からの情報が適切に統合され、適切な関係者に適切なタイミングで提供することを保証する。

以下のサービスはこのサービスエリアにおいて提供されるものである。

- データ取得
- 分析と統合
- コミュニケーション

8.1　サービス:データ取得

目的: コンスティチュエンシーのセキュリティ態勢に影響を与える可能性のある内部および外部の活動が発生しているかどうかを把握するのに役立つデータを収集する。

説明: コンスティチュエンシーの情報要件を要求、収集、決定および充足することで、重要な内部および外部関連活動の状況を把握する。このサービスには、現在のイベントについてのニュースを含む関連情報の収集、将来のイベント、報告およびフィード（供給）のスケジューリング、収集された情報のフィルタリング、インシデント分析、防止、検知、またはその他の活動(計画や傾向分析など)で使用するための情報の

整理、後に使用するための情報の保存、「検索可能性」の改善などのロジスティクスが含まれる。収集されたデータは、必要な予防措置を決定し、インシデントマネジメントおよび情報保証活動に関する情報を得た上での意思決定を支援するためにも使用される。重要な環境要素に関する基本的な認識がなければ、他のサービスが誤ったイメージを形成するリスクが増大する。CSIRT はおそらくポリシーと手続きを確立する必要があり、また、情報を収集し、調査するためにテクノロジーを使うかもしれない。

成果: このサービスから生じるアーティファクトは以下のとおりである。

- 状況把握のニーズを特定し、その上で目的を満たすために収集される情報のタイプに要件をマップするデータ収集要件のセット
- コンスティチュエンシーの資産および活動の、現在および予測される将来の状況に関する情報
- 新たな技術、方法、慣行、リスク、脅威など、コンスティチュエンシーの環境や現在の環境に関する洞察を提供する外部の事象や傾向に関する情報
- 分析および検知活動のために準備した、適切にフォーマットされた情報

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- ポリシーの集約、抽出、ガイダンス
- 機能、役割、アクション、主要リスクへの資産のマッピング
- 収集
- データ処理と準備

8.1.1 機能:ポリシーの集約、抽出、ガイダンス

目的: インフラで何が起きている（と考えられる）のか把握するためにコンスティチュエンシーおよびその資産が準拠すべきコンテキストを確立する。

説明: ポリシーの収集、集約、および抽出によって、容認可能な通常の活動の基礎が確立される。最終的に得られるものは、コンスティチュエンシーとそのインフラが許容できる条件の下でどのように運営されるべきかを確立するコンテキストである。組織の CSIRT にとって、コンテキストというものは、組織が受け入れ可能なポリシー、計

画、通常の運用条件、受け入れられたリスク、およびトレードオフを理解することを含む。理解とコンテキストによって観察を評価する基礎を確立する。

成果: コンスティチュエンシーで発生している容認可能な観察の理解。この理解は、インフラと資産に対する変更または影響に焦点を当てたものである。

8.1.2 機能:機能、役割、アクション、主要リスクへの資産のマッピング

目的: 既存の資産、コンスティチュエンシー、ベースラインおよび期待される活動の知識を提供することで、異常な状況の観察を特定する分析機能を支援する。

説明: CSIRT チームは、コンスティチュエンシーの現在のサイバーセキュリティの状態を理解し、容認可能なレベルのセキュリティとは何かを十分に理解する必要があるため、以下のことを知っておく必要があると考えられる。

- 内部システム、公開システムおよびデバイスの正規ユーザー
- 認証されたデバイスとその用途
- 承認されたプロセスおよびアプリケーション、許可されている場所、およびそれらの関係者への提供方法

この情報は、潜在的にリスクのある資産の優先順位付けをするのに役立ち、インシデントマネジメント活動のコンテキストを提供する。CSIRT が入手できる情報が正確であればあるほど、セキュリティ問題を推測し、それらに対して対処することが容易になる。正確な情報とは、CSIRT が、確立されたセキュリティポリシー、現在のアクセス制御、最新のハードウェアとソフトウェアのインベントリ、および詳細なネットワーク図にアクセスできる、ということを意味する場合がある。

成果: この機能で得られるリストは以下のとおり:

- 主要な機能とそれらをサポートする資産のリスト（資産によっては、複数の機能をサポートするものもある）
- 資産について各機能を実行する役割および同等のデジタルの役割のリスト
- 各役割で一般的に許可されているアクションのリスト
- 資産と機能が直面している主なリスクのリスト

これらのリストは状況の変化に応じて変化する。

8.1.3 機能:収集

目的: 分析・解釈サービスや他の CSIRT サービスを支援するために情報を収集する。

説明: 情報およびデータの収集活動は、自動化された情報を提供する供給元となるにとどまらない。収集には、次のような有用な情報源の特定が含まれる。他のコンスティチュエンシーからのニュースを含む情報関連の外部活動、メディア、他の CSIRT またはセキュリティ組織、内部活動(組織変更等)、技術開発、外部イベント、政治的イベント、攻撃傾向、防御傾向、カンファレンス、利用可能なトレーニング等。

データ収集機能は、セキュリティイベントマネジメント、インシデントマネジメント、および知識移転などの他のサービスを支援する。また、分析、予測、対応、リスクの緩和などのサービス内の機能や活動も支援する。新たに収集された情報によって、コンスティチュエンシーに対する攻撃が起こる可能性が以前よりも高いことが明らかになる場合がある。外部イベントにより、資産に対する新たなリスクを特定する情報が一定期間暴露される、または検知活動の強化が必要になることがある。包括的な情報は、意思決定とインシデントハンドリングを支援するための実用的な情報の提供に役立つ。

成果: 分析など、他のサービスや機能が使用できる運用上または環境上のコンテキストを提供するデータおよびデータセットを収集および生成して、コンスティチュエンシーの状況を表す図を作成したり、アラートを特定したり、資産およびサポートするインフラに対するリスクの増大を緩和したりするための計画を立てる。

8.1.4 機能:データ処理と準備

目的: CSIRT 活動および分析サービスの要件をサポートできる、信頼性と一貫性のある最新のデータセットを確立する。

説明: データの処理と準備には、一連のデータの変換、処理、正規化、および検証といった工程が含まれる。サイバーセキュリティデータの情報源には、多くの誤検知があるため、情報の正確性を検証する必要がある。また、関連するデータは通常異なる形式で提供されるため、完全な分析を実行する前に新しいデータを履歴データと組み合わせる必要がある。データの種類(ニュース記事等)によっては、準備プロセスの一環として分析または処理が必要な場合がある。例えば、ニュース記事から名前、日付、

場所、技術情報、弱点、システム名などの関連するセキュリティ情報を抽出し、潜在的な影響について内部データと比較する。

一部の分析方法では、データを同じ形式で保存するか、ファイルのレコード数を同じにする必要がある。データを準備するには、複数の処理ステップが必要になる場合がある。データの増大(エンリッチメントとも呼ばれる)は、他の内部および外部ソースからの特定のデータに関連する他の利用可能な情報を含めることによって実行される。例えば、チームは自律システム識別子、国コード、または地理的位置データなどのインターネットプロトコルアドレス(IP アドレス)に関連する情報を収集することがある。内部資産情報については、チームは資産の所有者の名前、役割、他の資産に対する権限、時間の経過に伴う実際の作業場所などを使用して、資産インベントリデータを充実させることができる。

成果: 他のサービスまたは機能で即時にデータが利用可能である。

8.2 サービス:分析と統合

目的: 状況が予想と一致しない場合を評価する。例えば、特定の資産がいつ有害な事象を経験する可能性があるかを特定する。

説明: 現行のデータ、履歴および分析技法を使用して、コンスティチュエンシーの資産およびセキュリティ態勢に影響を与える可能性のあることが起きているかを判断するプロセスは、多くの場合、質問に対する回答によって決定するか、勘を働かせることによって行われる。分析によって、イベントが予想される典型的な動作と一致しない場合を明らかにする、またはイベントや動作の状況、性質、発生源に関する情報を明らかにできる。分析により、現在および将来の状況への影響が明らかになる場合がある。例えば、システムは、ユーザーID がシステムに正常にログインしたことをログに記録できるが、イベントが正規のユーザーによって実行されたかどうかは示さない。新しい情報源(ユーザーへのインタビューなど)を分析に組み込み、チームに、イベントの正当性を判断するためのより正確な状況を提供する必要がある。収集されたデータおよびそのコンスティチュエンシーへの影響を分析および解釈するために、様々な技術が使用され得る。

成果: コンスティチュエンシー内で考えられる過去、現在および将来のイベントに関する一連の結論が得られる。また、コンスティチュエンシーが直面している特定の決定に関する推奨事項も含まれる場合がある。分析は、センサーやその他の情報源から収集された観測データのような証拠や、様々な方法を介した、分析者によるその証拠の解釈によって裏付けられたものであるべきである。また、これには、結果について通知する必要があるコンスティチュエンシーと、通知する必要がある内容も含まれる場合がある。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 予測と推定
- イベント検知(アラートや探索を通じて)
- 状況的影響

8.2.1 機能:予測と推定

目的: 現在の状況の特定または将来の状況の予測を目的として、データ取得中に収集された情報を分析する。

説明: 収集されたデータの状態および関係性に基づいて、現状を推測し、可能性のある近い将来に関する予測を行うプロセス。データによっては、すぐにセキュリティの問題を示す場合がある。

成果: 状況図が、それがいつどのように変化する可能性があるかという知識を伴い更新される。

8.2.2 機能:イベント検知(アラートや探索を通じて)

目的: コンスティチュエンシーの現在の状況の詳細を断定し、確認する。

説明: 外部および内部の情報と傾向に基づいて、ネットワーク境界の内部および外部での異常な活動を体系的かつ頻繁に検索する。コンスティチュエンシーがセンサーやその他の情報源から得たデータを分析し、環境や状況に関する結論を出すのを支援する。例えば、アンチウイルスセンサーが疑わしいファイルの警告を送信した場合、チームは、システム構成、センサー構成、警告されたファイル、その時点でのユーザーの動きなどを分析して、観察結果の深刻度に関する結論を引き出すことができる。こ

の機能は、セキュリティイベントマネジメント・サービスエリアから重要なインプットを受け取ることがある。インシデントを検知するために使用するセンサーからの観測結果は、複数のサービス間で共有してもよい。

CSIRT チームは、脅威に関する特定の情報に基づいて、現在の状況を判断する必要もある。この活動は、「脅威探索（threat hunting）」と呼ばれることもある。通常、脅威探索には、特定の脅威活動を検知するための環境の準備、またはすでに存在する可能性のある特定の脅威活動の検索が含まれる。

成果: コンスティチュエンシーにおけるイベントの検知に基づいて状況図が更新される。

8.2.3 機能:情報セキュリティインシデントマネジメントの意思決定支援

目的: 被害を抑制し、将来のリスクを緩和する、あるいは新しく発生した弱点を特定するのに役立つかもしれない新しい見識をインシデント中に特定する。

説明: 明確な証拠の分析を行うことで、インシデントの解決を支援する見識を明らかにするのに役立つ。場合によっては、CSIRT は、インシデント解決のような特定の望ましい結果を支持するために、状況分析に焦点を当てることがある。インシデントに対するある種の対応は、状況の全体像に異なる影響を与える可能性があり、対応者は、選択肢の分析(影響、コスト、障害のリスクなど)を要求する可能性がある。コンスティチュエンシーの意思決定ニーズは、彼らの状況が変化するにつれて変わる可能性があり、CSIRT チームは、彼らを支援するために新しい分析プロセスを開始する可能性がある。この活動は、インシデントマネジメント・サービスエリアに関連している。インシデントマネジメント機能は状況把握によってサポートされており、インシデントマネジメントの活動に基づいて状況が変化する場合がある。

成果: 新しい観察に基づくインシデントマネジメント機能に対する状況把握が強化される。インシデントマネジメント活動に基づいて状況図が更新される。

8.2.4 機能:状況的影響

目的: 現在観察されている事象や今後観察されうる事象が状況図に与えると予想される潜在的影響を決定する。

説明: この機能は予測または推測が現在または近い将来の状況に与えるかもしれない影響を特定する。ここで言う影響には、データ損失、システムのダウンタイム、データの機密性・可用性・完全性への影響など、特定のリスクの増加または減少を含む場合がある。

成果: 推測または予測が状況に及ぼす可能性の高い影響について分析が行われる。

8.3 サービス:コミュニケーション

目的: コンスティチュエンシーやそのセキュリティコミュニティの他の人々に、状況図に応じたリスクの変化を通知する。

説明: 状況把握から得られた知識は、コンスティチュエンシーに伝達されなければならない。これにより、監視に反応し、防衛状況を改善する行動をとることができる。例えば、リスクの高い特定の供給業者のセキュリティ環境を改善することにより、第三者のリスクを低減する。

成果: 正確で、実行可能で、タイムリーな状況情報を提供することで、コンスティチュエンシーは過去をよりよく理解し、現在および将来の状況図を改善できるようになる。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 組織内外とのコミュニケーション
- 報告と推奨事項
- 実装
- 普及・統合・情報共有
- 情報共有の管理

8.3.1 機能:組織内外とのコミュニケーション

目的: 現在の状況とそれがどのように変化しているかをコンスティチュエンシー(およびその他)に知らせる。

説明: 分析と解釈の結果が完了すると、内部および外部のコミュニケーションプロセスを介して意思決定を改善するために使用できる。特定の情報は、知る必要のある者に知らされる。コミュニケーションには、配信方法と配信されるコンテンツを含む。CSIRT は、新しい情報と、それが状況図にどのように変化を及ぼすかを伝えることが

ある。この例として、インシデント中に発見された新しい悪意のある技術がコンスティチュエンシーのメンバーに対して及ぼすだろうと思われる変化を報告することが挙げられる。また、データの最も有用な情報源や、コンスティチュエンシーが自分自身の状況把握を改善するためにそれを使用できる段階などのトレンド情報を含めることともできる。

成果: コンスティチュエンシーはより良い情報を得て、セキュリティや状況を改善する行動や意識決定を行う準備ができる。

8.3.2 機能:報告と推奨事項

目的: 結果、アーティファクトまたは所見を作成し、分析中に発見または作成された重大な情報を、受取手が理解できる方法と形式で伝える。

説明: 報告と推奨事項では、コンスティチュエンシーが直面している選択と行動が明確に示され、また、その内容にはそれぞれの選択や行動から予想される結果の分析を含めるべきである。所見の伝達には、解析を支持する証拠のリストと推奨事項(作られた場合)を含めるべきである。所見を作成するために用いた方法は、提示された主張も判断できるよう、対象者に明確に説明すべきである。CSIRT は、コンスティチュエンシーが状況の全体像を理解するためのニーズをサポートするために、単一のイベント、一連のイベント、傾向、パターン、考えられるイベント等についての報告書を作成することもある。

成果: 状況の全体像や結論を裏付ける証拠、実行できる行動方針とその潜在的影響に関する推奨事項について、正確で、タイムリーで、完全な報告をコンスティチュエンシーに提供する能力が改善される。

8.3.3 機能:実装

目的: 状況の変化に対してさらなる準備や対応をするためにコミュニケーションに基づいてコンスティチュエンシーの環境を調整する。

説明: 場合によっては、CSIRT チームがセキュリティインフラストラクチャの一部に対して推奨される調整を行うこともある。例えば、状況分析に基づいて特定のハニーポットのファイアウォールの設定を変更することがある。

成果: 受け取った分析や予測、推奨事項を含む情報に基づいて、コンスティチュエンシーによって行動方針の実行またはインフラストラクチャの変更がなされる。

8.3.4 機能:普及・統合・情報共有

目的: 情報を集め、標準化し、準備し、コンスティチュエンシーおよびそれ以外の人々と共有する。

説明: この機能は以下のサブ機能を含むことがある:

- 分析サービスの結果を内部および外部の計画および意思決定プロセスで活用する
- 情報を受信する適切な対象を特定する
- 解析結果を利用可能化する
- 配信の完遂を保証する
- 情報の共有に関する追跡と報告する
- さらなる利用と普及のために関連情報を知識移転サービスに送信する

成果: 状況把握分析の結果は、主要な意思決定プロセス、例えば脅威探索、インシデント分析、解決などへのインプット（内部およびコンスティチュエンシー間の両方）として使用される。また、インシデントのハンドリングまたは検知の一部として配布される。状況把握から得られた情報やデータは、知識移転サービスエリアを通じて、ベストプラクティス、報告、トレーニング、および啓発資料になることもある。

8.3.5 機能:情報共有の管理

目的: 情報の移転が成功し、使用可能であることを確実にする。

説明: この機能には以下のサブ機能が含まれることがある:

- 他のグループへ情報提供をする。
- 移転用に情報を形式化する。
- 移転プロセスとその成果の追跡をする。

成果: 適切な情報が共有され、パートナー、コンスティチュエンシー、およびその他のコミュニティ・メンバーに確実に受け取られるようにする。共有活動について報告が提供される。

8.3.6 機能: フィードバック

目的: 内部および外部の情報源から受信されるデータの品質、タイムリーさ、正確性および関連性を改善する。

説明: この機能はコンスティチュエンシー、他のサービスプロバイダまたは他の利害関係者が提供、受信および使用した情報に関するフィードバックの提供および受信を含む。フィードバックの内容としては、受信した情報の正確さ、適切さ、タイムリーさ、戦略性、新規性等はどうであったか、その情報は調査に役立ったのか、また新しい見識につながったのか、等が考えられる。これは、署名の有用性または変更、ハニーポットで分かったこと、IOC、警告、脅威情報、緩和策などについて(外部の情報源として)他の CSIRT へ情報提供することを意味する場合もある。この活動は、知識移転サービスエリアによって行われることもある。その場合は、結果を状況把握サービスエリアに戻して通知する必要がある。

成果: 得られた情報の正確性、タイムリーさ、品質および有用性を改善するために、内部および外部の情報源に対して観察結果およびフィードバックが提供される。

9　サービスエリア:知識移転

CSIRT はそのサービスの性質上、関連するデータを収集し、詳細な分析を実行し、脅威、傾向、およびリスクを特定するだけでなく、組織がセキュリティインシデントを検知し、防止し、対応するのを支援するのを目的とした、運用に関する最新のベストプラクティスを作り出す唯一の立場にある。こうした知識をコンスティチュエンシーに伝えることが、サイバーセキュリティ全体を向上させる鍵となる。

以下のサービスはこの特定のサービスエリアにおいて提供されるものと見なされる。

- 啓発
- トレーニングと教育
- 演習
- 技術およびポリシーに関するアドバイス

9.1　サービス:啓発

目的: コンスティチュエンシーのセキュリティ態勢全体を向上させ、そのメンバーがインシデントを検知し、予防し、回復できるようにするとともに、コンスティチュエンシーがインシデントに対して準備ができており、且つ教育がされていることを保証する。

説明: このサービスはコンスティチュエンシー、専門家、および信頼できるパートナーと協力して、脅威およびそれによってもたらされるリスクを防止または緩和するために取ることができる措置に対する全体的な理解を高めることを含む。

成果: コンスティチュエンシーに対して必要な以下に関する意識を提供する。

- タイムリー且つセキュアな方法で稼働する能力に影響を及ぼす可能性のあるイベント、活動および傾向
- 脅威や悪意のある活動を検知し、防止し、緩和するための手段
- セキュリティと運用のベスト・プラクティス

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 調査および情報集約
- 報告書および啓発資料の作成

- 情報の普及
- アウトリーチ

9.1.1 機能:調査および情報集約

目的: セキュリティ態勢の改善とリスクの予防・緩和のために、コンスティチュエンシーに伝えられる情報を集約、照合して、優先順位を付ける。

説明: この機能は、啓発資料と報告の作成に適した情報を調査・集約するものであり、他のサービスや機能、特にセキュリティイベントマネジメント、インシデントマネジメント、および状況把握サービスエリアの成果から得られるものを含む。

成果: 関連する傾向、進行中のインシデント、およびベストプラクティスに関する情報。これらの情報は、様々な対象者向けの報告および啓発資料の作成に使用できる。

9.1.2 機能:報告書および啓発資料の作成

目的: 異なる対象者にリーチする、または特定のコンテンツを可能な限り最善の方法で配信することを目標とし、関連性があるものとして収集・調査した情報を使用して、異なるメディアで資料を作成する。

説明: この機能では、様々な対象者向け(技術スタッフ、管理者、エンドユーザーなど)に、プレゼンテーション、ショートビデオ、漫画、小冊子、技術分析、傾向報告書、年次報告書などの様々な形態の資料を作成する。

成果: 様々な種類の効果的な配信技術とプラットフォームを利用して、コンスティチュエンシーのニーズを満たす、十分な品質の CSIRT 報告書および啓発資料が開発される。

9.1.3 機能:情報の普及

目的: セキュリティプラクティスについての認識とプラクティスの実装を改善するために、セキュリティに関連する情報を普及させる。

説明: この機能では、異なる対象者とコンテンツの特徴に基づいて、CSIRT がその報告書と啓発資料をコンスティチュエンシーに最も適切に提供できるようにするような情報発信プロセスを実装する。

成果: CSIRT のコンスティチュエンシーが、ポッドキャスト、ブログ投稿、ソーシャルメディア投稿、およびビデオ、プレスリリース、広告、キャンペーン、公的報告書などを含む様々な方法で、タイムリーで関連性のある情報にアクセスできるようになる情報発信フレームワークが実装される。

9.1.4 機能:アウトリーチ

目的: CSIRT のミッションの遂行を支援する、またはミッションに関わる可能性のある専門家または組織との関係を構築および維持する。

説明: この機能は、コンスティチュエンシーの内外でパートナーシップを構築し、協力することを促進し、主要な利害関係者を参加させるものである。その目標は、高い意識とベストプラクティスの普及、コンスティチュエンシーと外部の利害関係者が CSIRT の提供可能なサービスと便益を理解することの支援、CSIRT がコンスティチュエンシーのニーズをよりよく理解するための支援、そして CSIRT のミッションを実現可能にすることである。これには、組織間または組織横断の相互運用性の確保または協力の促進が含まれる場合がある。

成果: 主要な利害関係者との会合、業界ミーティングへの参加、会議での発表、会議の開催など、積極的で一貫性のあるアウトリーチ活動が行われる。

9.2 サービス:トレーニングと教育

目的: CSIRT のコンスティチュエンシー(これには組織のスタッフや CSIRT のスタッフも含まれる)に、サイバーセキュリティ、情報保証、およびインシデントマネジメントに関連するトピックについてトレーニングと教育を提供する。

説明: トレーニングおよび教育プログラムは、CSIRT が関係を構築し、将来のインシデントの発生を防止する能力を含めた、コンスティチュエンシーの全体的なサイバーセキュリティ態勢の改善を助けることができる。このようなプログラムでは、以下のことが可能である。

- ユーザーの高い意識を維持できるようにする。
- 変化する状況と脅威を理解できるようにする。
- CSIRT とコンスティチュエンシーの情報交換を容易にする。

- セキュリティおよびインシデントマネジメントに関連するツール、プロセス、および手順についてコンスティチュエンシーをトレーニングする。

これは、必要な知識、スキルおよび能力(KSA: Knowledge, Skills, Abilities)の文書化、教育およびトレーニング教材の開発、コンテンツの提供、指導、専門的能力と技能の開発など、様々なタイプの活動を通じて行うことができる。これらの各活動の積み重ねが、コンスティチュエンシーやチームの能力向上に繋がる。

成果: CSIRT のコンスティチュエンシーが適切に以下の内容を習得できるよう一貫したトレーニングと教育プログラムが提供される。

- 脅威を検知・防止し、それに対応する方法
- 重要な資産の保護に役立つツールと手法
- インシデントマネジメントのプロセスと支援を得る方法の理解

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 知識、スキル、能力要件の収集
- 教育およびトレーニング資料の開発
- コンテンツの配信
- メンタリング
- CSIRT スタッフの専門的能力開発

9.2.1 機能:知識、スキル、能力要件の収集

目的: 必要な KSA に関してコンスティチュエンシーのニーズを適切に評価、特定、文書化し、適切なトレーニングおよび教育資料を開発してスキルレベルを改善する。

説明: この機能は、どのようなトレーニングおよび教育を提供すべきかの決定に関する知識、スキル、能力(KSA)のニーズ、およびコンスティチュエンシーのコンピテンスを収集するものである。

成果: コンスティチュエンシーの KSA ニーズの特徴が明らかになり、文書化され、関連する教育・トレーニング資料を開発するための基礎として使用される。

9.2.2 機能:教育およびトレーニング資料の開発

目的: コンスティチュエンシーの KSA ニーズを基に、様々な対象にリーチする、または特定のコンテンツを配信する上で最善とされる配信方法に適した教育、指導、トレーニング資料を開発する。

説明: この機能は、プレゼンテーション、講義、デモンストレーション、シミュレーション、ビデオ、書籍、小冊子などの教育・トレーニング資料のコンテンツを作成または取得するものである。

成果: 多様で効果的なプレゼンテーション技術とプラットフォームを利用して、適切な品質でコンスティチュエンシーのニーズを満たす、CSIRT のトレーニングおよび教育資料が開発される。

9.2.3 機能:コンテンツの配信

目的: CSIRT が、様々な対象者とコンテンツの特性に基づいて、コンスティチュエンシーにコンテンツを最適に配信できるようになるコンテンツ配信のための正式なプロセスを開発する。

説明: この機能は、「生徒[31]」へ知識およびコンテンツを提供するものである。これは、コンピュータや Web がベースのトレーニング(CBT/WBT)、インストラクタによるもの、バーチャルで行うもの、カンファレンス、プレゼンテーション、ラボ、キャプチャ・ザ・フラッグ(CTF)コンテスト、書籍、オンラインビデオなど、様々な方法で行うことができる。

成果: 書籍、小冊子、オンラインビデオ、プレゼンテーション、ハンズオン・ラボ、CTF、CBT/WBT、対面でのトレーニングなど、あらゆる代替アプローチを使用して、コンスティチュエンシーが技術面およびソフト面でのスキルとプロセスを習得できるようにコンテンツ提供フレームワークが設計される。その結果、コンスティチュエンシーのメンバーが提供されたコンテンツを理解できるようになる。

[31] 訳注:「教育・トレーニングの対象者」の意味。

9.2.4 機能:メンタリング

目的: CSIRT スタッフ、コンスティチュエンシーまたは外部の信頼できるパートナーが、確立された関係を通じて経験豊富なスタッフから学ぶためのプログラムを開発する。

説明: メンタリングプログラムは、メンタリング対象者が自身の関わる公式の報告関係やチームの構造といったものから離れたところで、教育やスキル開発、見識、人生、キャリア経験についてメンターと共有する、公式および非公式のメカニズムを提供するのに役立つ。これには、現場訪問、ローテーション(人的交流)、シャドウイング[32]、および特定の決定と行動に対する理論的根拠の議論が含まれることがある。

成果: CSIRT チームにおける健全な意思決定を行うための維持、忠誠心、信頼、および全体的な能力を向上させる。コンスティチュエンシーのスキルレベルや CSIRT との関係性を改善する。信頼関係の構築を含む、コンスティチュエンシーと CSIRT チームメンバーの能力 (キャパシティとケイパビリティ)[33]が改善する。

9.2.5 機能:CSIRT スタッフの専門的能力開発

目的: スタッフメンバーが適切な計画を立ててキャリア形成を成功させることができるよう支援する。

説明: 適切なスキルが一旦特定されると、セキュリティ専門職、固有の職務責任、全体的なチーム環境に関連する新しい知識、スキル、および能力を確保する継続的なプロセスを促進するために、CSIRT によって専門的能力開発が行われるようになる。これにはカンファレンスへの参加、高度なトレーニング、クロストレーニング活動が特に含まれる。

成果: 必要な技術面およびソフト面でのスキルとプロセスを理解し、職務とニーズに応じて、最新の知識と能力を持つ、成熟し、訓練されたスタッフを得られる。CSIRT メンバーはチームと顧客の両方を支援しながら、日々の運用上の課題に対処する準備ができる。

[32] 訳注: インストラクターの真似をすることで身につける方法。

[33] 訳注: ANNEX 2「用語と定義」を参照。

9.3 サービス:演習

目的: サイバーセキュリティのサービス・機能の有効性と効率を評価し、改善するための演習を実施する。

説明: 個々のコンスティチュエンシーおよび利害関係者コミュニティ全体の能力（コミュニケーション能力を含む）を訓練・評価することを目的としたサイバー演習の設計・実施・評価を支援するために、組織がコンスティチュエンシーにこのサービスを提供する。以下のタイプの演習がある。

- テストポリシーと手順: インシデントを効果的に検知、対応、および緩和するための十分なポリシーと手順があるか評価する。これは一般的に、紙面上の演習または机上演習である。
- 運用準備のテスト: 適切な人員が配置されているか、ディレクトリ（連絡網）が最新であるか、手順が正しく実行されているかテストするだけでなく、タイムリーかつ順調にインシデントを検知、対応、および緩和できるインシデントマネジメント能力が組織にあるか評価する。

このサービスは、組織のニーズとコンスティチュエンシーのニーズの両方に対応する。具体的には、サイバーセキュリティベント、インシデントのシミュレーションを通じて、演習を 1 つまたは複数の目的に使用できる。

- デモンストレーション: 意識を高めるために、脆弱性、脅威、およびリスクだけでなく、サイバーセキュリティのサービスと機能を図示する。
- トレーニング: 新しいツール、手法、手順についてスタッフに教える。
    - 演習: スタッフが精通していることを期待されるツール、テクニック、手順を使う機会を提供する。演習は廃れやすい技能に必要なものであり、効率の改善と維持に役立つ。
    - 評価: スタッフの準備レベルだけでなく、サイバーセキュリティのサービスと機能の有効性と効率のレベルを分析し、理解する。
    - 検証: サイバーセキュリティのサービスと機能について、特定のレベルの有効性・効率が達成できるか判断する。

成果: サイバーセキュリティのサービスと機能の有効性と効率を改善し、さらなる改善の余地を特定する。

演習の具体的な目的によっては、サイバーセキュリティのサービスと機能を実際に内部または外部の利害関係者にもやって見せ、職員を訓練し、ツール、サービスおよび機能の効率と有効性を評価・検証することがある。また、今後の課題を改善するための教訓を特定し、経営陣またはその他の主要な利害関係者に報告書を提出することもある。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- 要件分析
- フォーマットと環境の開発
- シナリオ開発
- 演習の実行
- 演習成果レビュー

9.3.1 機能:要件分析

目的: 演習の、あらかじめ決められた範囲と焦点の特定の課題に集中することにより、確実に十分な成果を得られるようにする。

説明: 学習の目的と演習の範囲を決定する。演習で取り上げる具体的なサービス、能力(ケイパビリティ[34])、およびトピックを定義する。演習には、テストすべきプロセスだけでなく、参加者が必要とするスキルまたは望ましいスキルに関連する活動やトピックを確実に含める。

成果: 満たすべき学習目標の概要とともに、演習の目的の説明を明確化する。

9.3.2 機能:フォーマットと環境の開発

目的: 演習の実施に必要な内部および外部のリソースとインフラストラクチャを特定および決定する。

[34] 訳注: ANNEX 2「用語と定義」」を参照。

説明: 演習の目的を達成し、期待される成果を実現するために必要なフォーマットとプラットフォームを定義する。

成果: 演習の種類(机上演習、ハンズオン、シミュレーションなど)と、それを実施するために必要な内部および外部リソースを特定する。

9.3.3 機能:シナリオ開発

目的: コミュニケーションの観点を含む、模擬サイバーセキュリティイベントやインシデントのハンドリングを通して、そのサービスと機能の効率と有効性、およびそのスキル、知識、能力を改善する機会を対象者に提供する。

説明: 利害関係者の目的をサポートする演習シナリオの作成。成果物には、参加者と演習マネージャへの指示書とガイダンスも含まれる。これらの指示書には、参加者がシナリオの一部またはすべての手順を詳細に説明するために推奨されるアクションが含まれている。

成果: 多様であらゆるタイプの形式化されたインジェクションのあるメインシナリオが、演習管理チームへのタスク、役割分担と併せて開発される。

9.3.4 機能:演習の実行

目的: CSIRT チームが組織の CSIRT 計画の妥当性とその実行能力に対する信頼を高めるためにドリル・演習を実施する。

説明: この機能は、コンスティチュエンシー（生徒）に対して準備状況を試すテストを実施することで、トレーニングを適用し、且つジョブまたはタスクの機能を実行する能力をテストするものである。実際の環境や仮想環境、シミュレーション、フィールド・テスト、テーブル・トップ、モック・シナリオ、またはそれらを組み合わせた形式で実施され、構造化された方法でインジェクションが提供される。これは、チームの活動のレベルや、改善の余地があるか、あるとすればどこを改善すべきかを判断するのにも役立つ。

成果: CSIRT は準備および準備態勢について評価をし、KSA、主要なプロセス、および実行のすべてがうまく連携して機能することを保証し、そうでない場合は適応・改善しなければならない。

9.3.5 機能:演習成果レビュー

目的: 実際の観察に基づいて、演習の形式的で客観的な分析を行う。

説明: 演習から得られた教訓や知見、ベストプラクティスを含む演習後の報告を作成し、利害関係者や経営陣に評価を提供する。

成果: 組織のインシデントマネジメント能力、CSIRT のチームプロセス、コンスティチュエンシーの個々の能力、および利害関係者コミュニティ全体の能力（コミュニケーション能力と手順を含む）を改善するために、演習の成功した点、改善すべきところ、一般的な調査結果、および取るべき推奨措置を強調した成果物が作られる。

9.4 サービス:技術およびポリシーに関するアドバイス

目的: コンスティチュエンシーのポリシーおよび手順に、適切なインシデントマネジメントのために考慮すべき事項を確実に含め、最終的には、CSIRT がより効果的に機能するようにするのはもちろんのこと、コンスティチュエンシーもリスクと脅威をより良く管理できるようにする。

説明: リスク管理と事業継続に関する活動において、CSIRT のコンスティチュエンシーと、その内外を問わず、主要な利害関係者を支援し、必要に応じて技術的アドバイスを提供し、コンスティチュエンシーのポリシーの策定と実施に貢献するとともに、CSIRT がより効果的に活動できるように影響を与えることができる。ポリシーは、CSIRT のサービスを正当化する際にも重要である。

成果: コンスティチュエンシーは、事業継続と災害復旧のベスト・プラクティスを取り入れた運用セキュリティのベスト・プラクティスに基づいて組織的な意思決定を行うことができるようになり、またインシデントマネジメントチームを、信頼できるアドバイザーとしてビジネス上の意思決定に適切に組み込む必要性も理解できるようになる。

以下の機能はこのサービスにおいて実装されるものの一部と見なされる:

- リスクマネジメント支援
- 事業継続および災害復旧計画の支援
- ポリシーの支援

- 技術アドバイス

9.4.1 機能:リスクマネジメント支援

目的: 情報セキュリティおよびその他の関連機能と連携して、機会と脅威の特定能力を改善し、統制・管理を改善し、損失防止およびインシデントマネジメントを改善する。

説明: リスクまたはコンプライアンスの評価に関連する活動への支援を行う。これには、実際の評価を実施することや、アセスメントの結果を評価するための支援を提供することを含む場合がある。

成果: コンスティチュエンシーがリスクと脅威を特定し、適切かつ効果的なインシデントマネジメント戦略やセキュリティコントロール、脅威の緩和を含む、妥当なリスクマネジメントオプションを選択できるようになる。

9.4.2 機能:事業継続および災害復旧計画の支援

目的: 事業継続と災害復旧に関する信頼されるアドバイザーとして、中立的で事実に基づいたアドバイスを提供し、そのアドバイスを使用できる環境と適用されるリソースの制約を考慮する。

説明: 特定されたリスクに基づいて、組織のレジリエンス(回復力)に関連する活動においてコンスティチュエンシーを支援する。

成果: コンスティチュエンシーがインシデントマネジメント戦略を含み、それに沿った事業継続計画や災害復旧計画を適切に実施できるようになる。

9.4.3 機能:ポリシーの支援

目的: アドバイスが利用される可能性のある環境および適用されるリソースの制約を考慮し、公平で事実に基づいたアドバイスを提供することにより、ポリシーの開発および実施について信頼されるアドバイザーとして行動する。

説明: この機能は、ポリシーの開発、保守、制度化および施行においてコンスティチュエンシーを支援し、同時にインシデントマネジメント活動を可能にして支援すること

を保証するものである。内部[35]CSIRT については、通常、情報セキュリティおよび他の運用ポリシーの支援を含む。Coordinating CSIRT と National CSIRT については、公共政策と新しい法律のための支援を含む可能性がある。

成果: コンスティチュエンシーが効果的なポリシーを策定、制度化し、効果的なインシデントマネジメント戦略が可能になる。

9.4.4 機能:技術アドバイス

目的: 効果的なインシデントハンドリング活動を可能にする一方で、コンスティチュエンシーがリスクと脅威をよりよく管理し、現在の運用とセキュリティのベストプラクティスを実装できるような技術的アドバイスを提供する。

説明: この機能では、全体的なセキュリティ体制とインシデントマネジメントの改善を目標に、コンスティチュエンシー向けのサイバーセキュリティ関連のインフラ、ツール、およびサービスの改善のための支援と推奨事項を提供する。

これには、次のようなアドバイスが含まれる可能性がある。

- 買収、コンプライアンスの検証、保守、およびアップグレードに関するセキュリティ上の考慮事項
- サイバーセキュリティ関連のインフラやツールの内外監査
- セキュアなソフトウェア開発の要件とセキュアなコーディング

成果: コンスティチュエンシーのインフラ、システム、ツールの設計、取得、管理、運用、および保守を支援するとともに、インシデントマネジメント活動の能力 (ケイパビリティとキャパシティ)[36]、および成熟度の強化を支援する。

[35] 訳注: 組織内の意味。

[36] 訳注: ANNEX 2「用語と定義」を参照。

ANNEX 1: 謝辞

CSIRT コミュニティの以下のボランティアの皆さまより、CSIRT サービス・フレームワークの本バージョンに多大な貢献をいただきました。敬称は記しておりませんが、所属、役職、および国名とともに、名字のアルファベット順でここに記します。

- Vilius Benetis, NRD CIRT (LT)
- Olivier Caleff (Service Area Coordinator), openCSIRT Foundation (FR)
- Cristine Hoepers (Service Area Coordinator), CERT.br (BR)
- Angela Horneman, CERT/CC, SEI, CMU (US)
- Allen Householder, CERT/CC, SEI, CMU (US)
- Klaus-Peter Kossakowski (Editor), Hamburg University of Applied Sciences (DE)
- Art Manion, CERT/CC, SEI, CMU (US)
- Amanda Mullens (Co-Service Area Coordinator), CISCO (US)
- Samuel Perl (Service Area Coordinator), CERT/CC, SEI, CMU (US)
- Daniel Roethlisberger (Service Area Coordinator), Swisscom (CH)
- Sigitas Rokas, NRD CIRT (LT)
- Mary Rossell, Intel (US)
- Robin M. Ruefle (Co-Service Area Coordinator), CERT/CC, SEI, CMU (US)
- Désirée Sacher, Finanz Informatik (DE)
- Krassimir T. Tzvetanov, Fastly (US)
- Mark Zajicek (Co-Service Area Coordinator), CERT/CC, SEI, CMU (US)

ANNEX 2: 用語と定義

ここでは CSIRT サービス・フレームワークで使われたいくつかの用語を定義している。

Action / アクション - 何かがどのように行われるかを、様々なレベルで詳細に説明すること。

Advisory / アドバイザリー[37] - 製品の脆弱性についての情報提供、助言、警告を目的としたアナウンスや報告書。

Capability / ケイパビリティ - 組織の役割と責任の一部として実行される可能性のある測定可能な活動。FIRST のサービス・フレームワークにおいて、ケイパビリティはより広いサービスまたは必要な機能のどちらか一方として定義されることがある。

Capacity / キャパシティ - 組織がリソースの枯渇に陥らずに実行できる特定のケイパビリティの同時プロセス発生数。

Common Vulnerability Exposures (CVE) / 共通脆弱性識別子[38] - 公に知られている脆弱性の識別番号、説明、および少なくとも 1 つの公開リファレンスを含むエントリのリスト。脆弱性を参照するための標準的な識別子として機能する。

Common Vulnerability Scoring System (CVSS) / 共通脆弱性評価システム[39] - 脆弱性の深刻度を反映して数値で表されるスコア。

Common Weakness Enumeration (CWE) / 共通脆弱性タイプ一覧[40] - アーキテクチャ、設計、コードにおけるソフトウェアセキュリティの弱点 (脆弱性) を記述するための共通言語として機能する、ソフトウェアの脆弱性の種類を列挙した公式なリスト。これらの脆弱性を対象としたソフトウェアセキュリティツールの標準的な判断の目安として機能し、また、脆弱性の特定、緩和、防止に取り組む際の共通のベースライン標準を提供する。

Constituency / コンスティチュエンシー[41] - CSIRT が提供する特定のサービスにアクセスできる特定の人々や組織。

---

[37] ISO/IEC 29147:2014 Information technology—Security techniques — Vulnerability disclosure- Terms/Definitions 3.1

[38] https://cve.mitre.org/

[39] https://www.first.org/cvss/

[40] https://cwe.mitre.org/about/index.html

[41] 訳注:「サービス対象者」と訳されることもある。

Contextual Data Source / コンテキストデータソース - データポイントにコンテキストを与えるコンテキストデータのソースで、例えばID、資産、情報セキュリティイベントなど。具体的な例としては、ユーザーデータベース、資産インベントリ、IP否認サービス、脅威インテリジェンスデータなどがある。

Coordinated vulnerability disclosure / 協調的な脆弱性の公開 - 調整を含む開示プロセスを表すために使用される用語。出典：ISO/IEC 29147:2018, Terms and definitions。

Coordinator / コーディネーター[42] - 脆弱性情報のハンドリングや開示においてベンダーや発見者を支援することができる任意の参加者。

Detection Use Case / 検知ユースケース - 情報セキュリティイベントマネジメント・サービスエリアによって検知される特定の条件。この用語はソフトウェアエンジニアリングに由来するが、現在は検知エンジニアリングで広く使用されている。

Embargo / 開示差し止め - 影響を受けるベンダーがセキュリティアップデートや緩和策、回避策を公開して顧客を保護できるようになるまで、脆弱性の詳細を公開するのを保留すること。

Finder / 発見者[43] - 製品やオンラインサービスの潜在的な脆弱性を特定する個人または組織。発見者には、研究者、報告者、セキュリティ会社、ハッカー、ユーザー、政府、またはコーディネーターが含まれることに注意してほしい。

Function / 機能 - 特定のサービスの目的を達成することを目的とした単一または一連の活動。その他の定義としては、関連するアクションのグループがあり[44]、特定のアクションまたは活動を実行し、作業し、操作する[45]。

Information Security Event / 情報セキュリティイベント - セキュリティに関連するIT環境で観察可能なイベント。例えば、ユーザーログオンやIDSアラートなど。情報セキュリティイベントは通常、監査記録やログファイルのエントリなどの何らかの証拠を生成し、情報セキュリティイベントマネジメント・サービスエリアの一部として収集および分析することができる。

[42] ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes-Terms/Definitions 3.1
[43] ISO/IEC 29147:2014 Information technology—Security techniques — Vulnerability disclosure- Terms/Definitions 3.3
[44] 出典: https://www.merriam-webster.com/dictionary/function
[45] 出典: https://www.dictionary.com/browse/function

Information Security Incident / 情報セキュリティインシデント[46] - ユーザーや、システム、組織、ネットワーク情報セキュリティの何らかの側面の侵害を示す、あらゆる有害な情報セキュリティイベント（または一連の情報セキュリティイベント）。情報セキュリティインシデントの定義は組織によって異なる場合があるが、少なくとも次のカテゴリが一般的に適用される。

- 情報の機密性の喪失
- 情報の完全性の侵害
- サービスの拒否
- サービス、システム、情報の不正利用
- システムへのダメージ

攻撃は、たとえそれが適切な保護によって失敗した場合でも、情報セキュリティインシデントと見なすことがでる。

Key Performance Indicator (KPI) / 主要業績評価指標[47] - 企業が主要なビジネス目標をどれほど効果的に達成しているかを示す測定可能な値。組織は複数のレベルで KPI を使用して、目標達成に成功したかどうかを評価する。

Maturity / 成熟度 - 組織が組織の使命と権限内で特定のケイパビリティをいかに効果的に実行しているかを示すもの。これは、特定の機能の実行、または機能やサービスの集合体のいずれかで達成される熟練度のレベルである。組織の能力は、確立されたポリシーと文書化の範囲と質、および一連のプロセスを実行する能力によって決まる。

Open Source / オープンソース - 自由に再配布および改変できるようにライセンスされている著作物。ソースコードが一般に公開され、自由に配布されていて、且つ、如何なる個人、グループ、または取り組みの分野も差別せず、技術的に中立である。オープンソースソフトウェアは、多くの場合、共同で作成および保守する個人およびエンティティのコミュニティによって保守されている。

Product / 製品[48] - 販売または無料で提供されるために実装または開発されたシステム。

[46] 「IT セキュリティ」ではなく「情報セキュリティ」を考慮することによる RFC2350 に基づく。
https://tools.ietf.org/html/rfc2350

[47] https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator

[48] ISO/IEC 29147:2014 Information technology—Security techniques—Vulnerability disclosure-Terms/Definitions 3.5

Remediation (または Remedy) / 修正[49] - 脆弱性を除去または緩和するために製品またはオンラインサービスに加えられる変更。脆弱性の修正は、通常、バイナリファイルの置き換え、設定の変更、またはソースコードのパッチと再コンパイルの形で行われる。「Remediation」に使われる様々な用語には、パッチ、修正、更新、Hotfix、およびアップグレードなどがある。緩和策 (mitigation)は、回避策 (workaround) や対策 (countermeasure) とも呼ばれる。

Responsible Disclosure / 責任ある情報開示 - 脆弱性の開示を、その是正措置（修正やパッチ）が利用可能になってから行うようにするモデルやプロセスを指す用語。この用語は、必ずしも「協調的な脆弱性の公開 (coordinated vulnerability disclosure)」と同じではない。

Risk / リスク[50] - 「目的に対する不確実性の影響」のこと。この定義では、不確実性には、(起こるかもしれないし、起こらないかもしれない) イベントと、曖昧さや情報不足によって引き起こされる不確実性が含まれる。

Risk Acceptance / リスク受容[51] - プロジェクトチームがリスクを認め、リスクが発生しない限り何も行動を起こさないことを決定するリスク対応戦略。

Risk Register / リスク登録[52] - リスク分析とリスク対応計画の結果を記録した文書。

Service / サービス - サービスとは、特定の結果に向けて、認識可能で首尾一貫した機能の集合体。そのような結果は、コンスティチュエンシーによって、またはエンティティの利害関係者やその利益のために期待されたり、要求されたりすることがある。

Service Level Agreement (SLA) / サービスレベル契約 - (内部または外部の)サービス提供者とエンドユーザーとの間の契約で、サービス提供者に期待されるサービスのレベルを定義するもの。

[49] ISO/IEC 29147:2014 Information technology—Security techniques—Vulnerability disclosure-Terms/Definitions 3.6
[50] ISO 31000:2009/ ISO Guide 73:2002 Risk management — Principles and guidelines- Terms/Definitions 2.1
[51] The Project Management Body of Knowledge (PMBOK) Guide and Standards
[52] The Project Management Body of Knowledge (PMBOK) Guide and Standards

Stakeholders / 利害関係者[53] - サービスエリアやサービスを定義・変更し、適切なサービスコミュニケーション戦略を確保する個人やグループ、および提供されるサービスの恩恵を得ることができるグループ。

Tasks / タスク - 特定の機能を完了するために実行しなければならないアクションのリスト。

Vendor / ベンダー[54] - 製品やサービスを開発した、またはその保守に責任のある個人や組織。

Vulnerability / 脆弱性[55] - 悪用される可能性のあるソフトウェア、ハードウェア、またはオンラインサービスの弱点。

[53] Architecture Content Framework

[54] ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes-Terms/Definitions 3.7

[55] ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes-Terms/Definitions 3.8

ANNEX 3: 関係資料

Alberts, David S., et.al. Understanding information age warfare. In *DOD Command and Control Research Program Publication Series*. ADA395859. Booz Allen & Hamilton, McLean, VA. 2001.
https://apps.dtic.mil/docs/citations/ADA395859

Barford P., et al. (2010) Cyber SA: Situational Awareness for Cyber Defense. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, 2010. Boston, MA. ISBN 978-1-4419-0140-8_1
https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_1

Boyd, John R. Destruction and Creation. Goal Systems International. September 3, 1976.
http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf

Cartwright, James E. Joint Concept of Operations for Global Information Grid NetOps. *United States Strategic Command*. PDF August 10, 2005. Homeland Security Digital Library. August 10, 2005.
https://www.hsdl.org/?view&did=685398

Committee on National Security Systems Instruction CNSSI 4009. *Committee on National Security Systems Website.* June 23, 2019 [accessed].
https://www.cnss.gov/cnss/

Cybersecurity Situation Awareness. *The MITRE Corporation Website.* June 25, 2019 [accessed].
https://www.mitre.org/capabilities/cybersecurity/situation-awareness

Endsley, Mica R. Toward a theory of situation awareness in dynamic systems. *Human factors* Volume 37. Number 1. March 1995 Pages 32-64.
https://journals.sagepub.com/doi/10.1518/001872095779049543

FIRST *Product Security Incident Response Team (PSIRT) Services Framework*, Version 1.0, 2018. North Carolina: First.org, 2018
https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0

FIRST Vulnerability Reporting and Data eXchange SIG (VRDX-SIG). 2013-2015. North Carolina: First.org, 2015
https://www.first.org/global/sigs/vrdx/

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, Version 1.0, 2017. North Carolina: First.org, 2017
https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0

Hawk, Robert. Situational Awareness in Cyber Security. [blog post]. *Hawk's Posts: Security Essentials from Robert Hawk.* June 11, 2015.
https://www.alienvault.com/blogs/security-essentials/situational-awareness-in-cyber-security

Householder, Allen D.; Wassermann, Garret; Manion, Art; King, Christopher. *The CERT® Guide to Coordinated Vulnerability Disclosure*. CMU/SEI-2017-SR-022. Software Engineering Institute, Carnegie Mellon University. 2017
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

Householder, Alan. Vulnerability Discovery for Emerging Networked Systems [blog post]. *Vulnerability discovery techniques*. November 20, 2014.
https://insights.sei.cmu.edu/cert/2014/11/-vulnerability-discovery-for-emerging-networked-systems.html

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability disclosure.* Second Edition. ISO/IEC 29147:2018. Geneva, Switzerland: ISO: IEC. 2018
https://www.iso.org/standard/72311.html

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability handling processes*. First Edition. ISO/IEC 30111:2013. Geneva, Switzerland: ISO: IEC. 2013
https://www.iso.org/standard/53231.html

Jajodia, Sushil, et al., (Eds.). *Cyber Situational Awareness: Issues and Research*. Part of the Advances in Information Security book series (ADIS, volume 46). 2010. ISBN 978-1-4419-0140-8
https://link.springer.com/book/10.1007/978-1-4419-0140-8

Kossakowski, Klaus-Peter. *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001. ISBN: 9783831100590.

Kossakowski; Klaus-Peter & Stikvoort, Don. *A Trusted CSIRT Introducer in Europe*. Amersfoort, Netherlands: M&I/Stelvio, February, 2000.
http://www.ti.terena.nl/process/ti-v2.pdf

Manion, Art & Householder, Alan. *Vulnerability Analysis.* CERT Coordination Center (CERT/CC). May 30, 2019.
https://vuls.cert.org/

McGuinness, B. &, Foy, L. A subjective measure of SA: The crew awareness rating scale (cars). In Kaber, D.B.; Endsley, M.R.; p. 286-291. *Proceedings of the First Human Performance, situation awareness and automation conference; user-centered design for the new millennium*. Savannah, Georgia, October 2000.

Salerno, John; Hinman, Michael & Boulware, Douglas. Situation awareness model applied to multiple domains. In *Proceedings of the Defense and Security Conference*, Orlando, FL, March 2005.
https://www.spiedigitallibrary.org/conference-proceedings-of-spie/5813/0000/A-situation-awareness-model-applied-to-multiple-domains/10.1117/12.603735.full?SSO=1

Stone, Steve. Data to Decisions for Cyberspace Operations. *The MITRE Corporation Website*. January 2016
https://www.mitre.org/publications/technical-papers/data-to-decisions-for-cyberspace-operations

Tadda G.P., Salerno J.S. (2010) Overview of Cyber Situation Awareness. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, Boston, MA. 2010. ISBN 978-1-4419-0140-8
https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_2

West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. CMU/SEI-98-HB-001. Software Engineering Institute, Carnegie Mellon University. 1998.
http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

ANNEX 4: すべての CSIRT サービスと関連機能の概要