TLP:WHITE

FIRST CSIRT Framework

Computer Security Incident Response Team （CSIRT） Services Framework

Version 1.1

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。

目次

TLP:WHITE

はじめに

この版は、コンピューターセキュリティインシデントレスポンスチーム・サービスフレームワークの新バージョンである。複数の専門家からのフィードバックに基づいて、初版に必要な再構成と追記を行った。 特に CSIRT 内活動[1]は、CSIRT が提供する他のサービスの基礎となることが多いので、本書の主要部に移動した。

本書は、CSIRT が提供するサービスの包括的なリストを提供している。ひとつの CSIRT で全てのサービスを提供する必要はないが、少なくとも一部のサービスを提供することになるだろう。本書はプロダクトセキュリティチームの活動については記載していない。それらは本書ではなく PSIRT サービスフレームワークに記載している。

[1] 原文では、Internal Activities のこと

TLP:WHITE

本フレームワークは今後も進化していく。CSIRT は新たな脅威からステークホルダーを守り、刻々と変化する課題に対応するため、進化し続けるからである。

本書は CSIRT が CSIRT のサービスポートフォリオ[2]の選択するのを支援することを目的としている。ただし、本書は、 ケイパビリティ[3]やキャパシティ[4]についての提案や推奨は記載していない。これらのトピックについては、別のところで扱う。

最後に、草案作成、改訂とフィードバックに多くの時間を費やしてくれた多くのボランティアの助けがなければ、本書は決して実現できなかった。特に Peter Allor 氏は、CSIRT フレームワーク作成の当初から牽引しており、彼なしでは、このドキュメントの完成はなかった。

背景とスコープ

本フレームワークでは、ステークホルダー[5]への外部サービスと、運用に不可欠な内部サービスについて記述する。また、本書の全体構成と、いくつかの章が削除された理由についても記述する。

目的

CSIRT サービスフレームワークは、CSIRT が部分的にでもステークホルダーに向けて実施するのに適切なサービス、とファンクションの一覧を示している。その目的は、CSIRT の運用や、ケイパビリティの開発、教育と訓練を確立することであり、コミュニティが受け入れている用語と CSIRT が行うことのできるアプローチを利用して、これからの確立を促進することにある。

歴史

CERT/CC CSIRT サービスリストは、1980 年代後半から、CSIRT や同様のサービスについて、一貫性を持った、比較説明を行うために、さまざまな場面で使われてきた。しかし、さまざまな既存の非公式の CSIRT サービスリストの最近の評価を通して、CERT/CC のリストは、広く使われ適用されているものの、昨今の CSIRT のミッションに関する幅広い理解を得るための重要な要素が欠落していることがわかってきた。

CSIRT の世界的な発展と成熟に関心を持つ FIRST は、既存メンバーや将来のメンバーのために、共通言語での開発が重要だと認識していた。当初、本書の目的は訓練開発のための共通土台の作成であった。その過程において、本書はより広いスコープを持つようになり、CSIRT 関係者がその活動を定めるために役立つようになってきた。FIRST メンバーシップは世界規模なので、各メンバーが持つさまざまな視点から、コミュニティが集まり本書を作成した。

原則

設計原則

- 共通フレームワークモデル：PSIRT サービスフレームワークで使用するものと同等である。
- 簡潔性：フレームワークはできるだけシンプルにし、不要な複雑さや冗長性を取り除く必要がある。コミュニティにおいて受け入れられ、使用を促進するためには簡潔さが必要である。
- 包括性：フレームワークは、コミュニティの視点から CSIRT でやるべきことと合致しており、CSIRT が潜在的に提供/実施するサービスやファンクションを含んでいなければならない。ただし、ひとつの CSIRT がすべてのサービスを行うことはほとんどなく、また高い成熟度にある

[2] 提供するサービスの組み合わせのこと
[3] 実施能力のこと（質的な能力）
[4] 処理能力のこと（量的な能力）
[5] CSIRT の利害関係者という意味で使用されている Constituency（サービス対象者）よりも広い範囲で使用されている

TLP:WHITE

わけではない。

- 用語の一貫性：このフレームワークは、非英語圏の理解を促進し、相互運用性を確保するために、明確に定義された用語を一貫して使用する必要がある。
  さらに、他の正当な理由がない限り、国際標準で使用され、既に定義された用語を使用する。

標準化された、もしくは一般的に受け入れられている定義の使用

この CSIRT サービスフレームワークでは、標準化されたもしくはよく参照される文書ある既存の用語（定義）を使用している。

階層モデル

- 階層モデルは、次のように定義したレベルで構成している。
  - サービスエリア
  - サービス
  - ファンクション
- サービスエリア – 共通の特徴を持つサービスのグループ。理解を促進し、トップレベルの体系に沿ってサービスを整理するのに役立つ。（またこの領域はバージョン 2.0 でさらに発展させる予定である。）
- サービス – 特定の結果を目標として行われる、認識できる一貫性をもった一連のアクションの集合体である。これらは、インシデントレスポンスチームのステークホルダーの代わりに、またはステークホルダーのために実施される。サービスの実装にはファンクションのリストが使用される。
- ファンクション – 目的を果たす手段、もしくは特定のサービスのタスクである。タスクのリストはファンクションの一部である。

推奨定義

このフレームワークを最も効果的に使用するために、コミュニティに採用され、受け入れられている、標準の定義を使う必要がある。下記図１参照のこと。

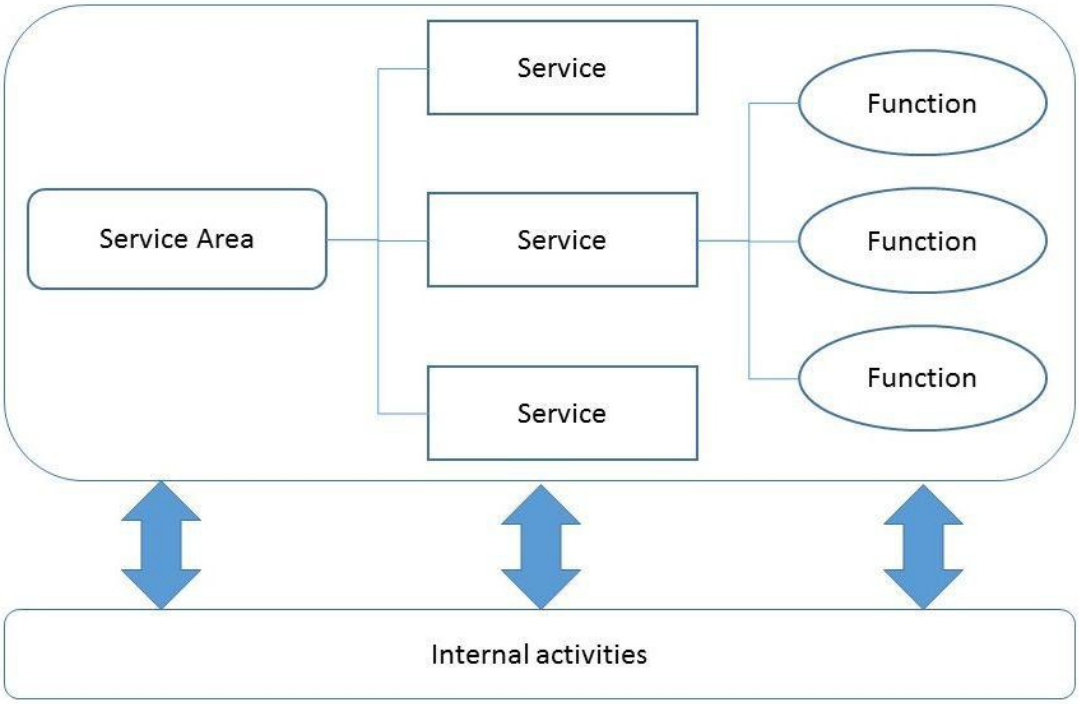

図 1:フレームワークのサービス階層

TLP:WHITE

サービスエリア – サービス – ファンクション

サービスエリア[6]

サービスエリアは共通の特徴を持つサービスをまとめたものである。トップレベルの体系に沿ってサービスを体系化するのに役立つ。各サービスエリアの仕様には、サービスエリアとサービスエリア内のサービスのリストを説明する一般的な文章からなる「説明」欄が含まれる。

サービス[7]

サービスは、サービス対象者[8]が特定のコストやリスクを伴わずに達成したい成果を得られるように、サービス対象者に価値を提供する手段である。サービスとはサービス対象者にとって価値があり、理解しやすく、すぐに利用できるものである。

CSIRT におけるサービス対象者は CSIRT のステークホルダーである。そのためサービスは特定のステークホルダーに提供される。

サービスは、次のようなひな形で明記する。

- 「説明」欄には、サービスの内容を記述する
- 「提供する価値」欄には、サービスがサービス対象者[9]にもたらす価値を記述する。価値はサービス対象者が CSIRT から得るものではなく、サービスを通じて達成するものである。

ファンクション[10]

ファンクションとは、特定のサービスの目的を達成することを目指した活動、または一連の活動である。ファンクションは、複数のサービスで使われることがある。

ファンクションは次のようなひな型で記述する。

- 「説明」欄には、ファンクションの説明を記載する。

ファンクションの一部として行うことができるタスクのリストも記載する。

CSIRT 内活動

CSIRT 内活動(Internal Activity)はサービスの提供のために必要な機能(Function)で、CSIRT に特化したもの(活動)ではない。ここでは全ての内部活動(Internal Activity)は説明せず、CSIRT に関連するものに限って説明する。

キャパシティ

一般的な用語において、キャパシティとは誰か（人もしくは組織）がある決められた期間に適切な指標を使用して、アウトプットの”量“（生産量）を生み出す能力のことである。CSIRT サービスフレームワークにおいてはある一定期間内に特定のサービスによって提供される生産量を表すのに使用され、関連する状況において、同時にサービス提供可能な利用者数や需要数の形で表示されることもある。キャパシティは提供できる「量がどれくらいか」を測定するものである。例えば、ある時間内にマルウェア検体をいくつ分析できるか、といったものを指す。

ケイパビリティ

組織の役割と責任の一部として実施される可能性のある測定可能な活動である。この CSIRT サービスフレームワークでは、ケイパビリティはより幅広い「サービス」もしくは必須な「ファンク

[6] 図 1:フレームワークのサービス階層においては、「Service Area」と記載
[7] 同　「Service」
[8] 原文では customer
[9] 原文では Subscriber だが本書では Customer と同義とし、「サービス対象者」とした
[10] 図 1:フレームワークのサービス階層においては、「Function」と記載

TLP:WHITE

ション」のどちらとも定義できる。ケイパビリティは提供されるサービスが「どれくらい質が良いか」を測定するもので、例えば、どの程度の内容や詳細さでマルウェアの検体を分析できるかといったものである。ケイパビリティはしばしば成熟度もしくは熟練度と呼ばれることがあり、本文書においては同義である。

成熟度/熟練度

CSIRT の成熟度/熟練度は、参照モデルを基準に測定されるナレッジやスキルの進歩の度合いと定義する。CSIRT は特定のサービスやファンクションの運用に望ましいと考えられるレベルに目標とする熟練のレベルを設定することになる。

サービスと CSIRT 内活動の詳細な説明

サービスエリア 1 – インシデントマネジメント

インシデントマネジメント[11]は、CSIRT が存在する理由でもある。本サービスエリアのファンクションはインシデントレスポンスの全ライフサイクルを網羅する。

1.1 サービス – インシデントハンドリング

サイバーイベント管理に関するサービスであり、サービス対象者へのアラート通知やインシデントからのレスポンス、緩和策、そして回復に関連する活動の調整作業を含む。インシデントハンドリングは、「分析」エリアで定義する分析活動にも依存する。

1.1.1 ファンクション – インシデントの検証と分類

報告されたインシデントが実際に起こったこと、関連するシステムに何らかの影響を与えたことを、CSIRT の権限範囲にあることを最終的に確認することである。

目的: イベントがセキュリティインシデントやネットワークもしくはハードウェアのエラーであるという技術的な証拠を提供し、CSIRT の管轄範囲における情報資産の機密性、可用性と/または完全性に対する潜在的なセキュリティの影響と被害を特定する。

成果[12]: 報告されたイベントが、実際に対応処理すべきインシデントなのか、または、報告が関連システムに登録され、CSIRT のさらなるアクションを必要とせずに終了するか、関連するものに引き継ぐか、を決定する。セキュリティインシデントが実際に発生したとサービス対象者が考えているイベントの詳細を引き出し、悪意があるものか、または設定誤りやハードウェア障害のような他の理由があるか、を確認する。

[11] 本来のインシデントマネジメントはインシデントレスポンスを含む、予防、是正処置まで含むが本文書ではインシデント対応のことを指している

[12] 実施した結果得られる価値または成果物そのもの。原文では outcome

TLP:WHITE

1.1.2 ファンクション – インシデントトラッキング

収集した重要な情報、実施した分析、講じた修正と緩和の手段、終了と解決など、インシデント解決に講じたアクションに関する情報を文書化すること。

1.1.3 ファンクション – 情報収集

イベントとインシデントに関する情報の取り込み、カタログ化と保存には、次の項目を含むこと。

- **インシデントレポート収集:**サービス対象者と第三者（他のセキュリティチームや商用インテリジェンスフィードのようなもの）からの悪意あるまたは疑わしいイベントに関するレポート、とインシデントのレポートを、手動、自動、もしくはコンピュータで読める形式で収集する。
- **デジタルデータ収集:**インシデント活動の理解に役立つと思われる（ただし、必ず役立つという保証はない）デジタルデータの収集とそのカタログ化（例としてディスクイメージ、ファイル、ネットワークログ/フロー）を行う。
- **その他のデータ形態（非デジタル）:** 非デジタルデータの収集とカタログ化（入館記録簿、アーキテクチャー概略図、ビジネスモデル、サイトアセスメントデータ、ポリシー、企業リスクフレームワーク、など）を行う。
- **アーティファクト[13]の収集:** 悪意のある活動の形跡と思われるアーティファクトの取得、カタログ化、保存、追跡に使用されるビジネスと技術的なプロセス。
- **証拠収集:** 法の施行において使用される可能性のある情報やデータの収集業務で、しばしば、情報源に関するメタデータの取得、収集方法、そして、所有者と保管情報を含む。

1.1.4 ファンクション – 調整と報告

CSIRT の内部・外部双方に対する情報共有とアドバイス活動である。これは主として CSIRT がインシデントの軽減に必要なアクションを実行するために、CSIRT が直接管理しない専門知識やリソースに頼る際に発生する。相互に、もしくは多角的に調整することで、現時点での攻撃者からのアクティビティの検知、防御、または修正において、能力を持ったリソースがアクションを取ることを可能にするために、または他者を助けるために、CSIRT は情報交換活動に加わる。

1.1.5 ファンクション – ニュースメディアとのコミュニケーション

インシデントで起きたことを説明するための公式発表にふさわしいやり方によるメディアとのコミュニケーションである。通常、問題を簡潔にし、機密情報を除外しながらも、状況描写の明確さは維持する。この活動はサービス対象者や CSIRT 自身のためである。CSIRT はステークホルダーのコミュニケーション部門と、事前に決められたプロセスを準備しておくことが重要である。

1.2 サービス – インシデント分析

スコープ、影響を受ける当事者、関連するシステム、時間軸（発見・発生・報告）、ステータス（進行中かは完了か）のようなイベントもしくはインシデントに関する情報の識別、と特徴づけに関連するサービスである。

1.2.1 ファンクション – 影響分析

関連するシステムによってサポートされているビジネスへの影響の識別と特徴づけを行う。

目的: インフラ、サービス、データ、部署もしくは組織の影響を受けた部分など、インシデントの規模と範囲を特定する。この分析をもとに、通常の解決のためのアプローチが行われる。

[13] マルウェア、エクスプロイト、スパム、ログ、設定ファイルなどのこと

TLP:WHITE

成果: インシデントがもたらした、もしくはもたらすかもしれない（潜在的）被害を特定する。技術的な面だけではなく、マスコミ報道、信用や信頼性の失墜と風評被害を特定する。

1.2.2 ファンクション – 緩和策の分析

セキュリティホールを塞ぐ、あるいは悪意あるプロセスを停止するといった進行している問題を止める対策を見つける、といったことを指す。

1.2.3 ファンクション – 回復方法の分析

当初のセキュリティ問題を再発させることなく、影響を受けた業務を完全に回復させるための計画を立てる。

1.3 サービス – インシデントの緩和と回復

インシデントによる影響の軽減とステークホルダー間のビジネス機能回復に関連するサービスである。

- 封じ込め：短期の戦術的アクションによって緊急性のある被害と、悪意ある活動の拡大を阻止し（例：トラフィックの遮断もしくはフィルタリング）、場合によっては、システムの制御権の奪回を伴う。
- 緩和策：インシデントの根絶、回避策の実施による徹底した包括的封じ込め戦略の実施を通じて、さらなる被害を防止する。
- 修正：同一の被害の再発防止のために、影響を受けたドメイン、インフラ、またはネットワークを変更する。これには、ポリシーの変更や、さらなる訓練教育訓練による、組織的な防御態勢や運用における即応体制の強化も含まれる。
- 回復：影響を受けたシステムの完全性を回復させ、影響を受けたデータ、システム、ネットワークをデグレードされてない運用可能な状態に復旧する。

1.3.1 ファンクション – 封じ込め

目的: インシデントの拡大を止めること。

成果: インシデントがこれ以上拡大しないため対策する。例：その時点で影響を受けたドメインの範囲内に留める。

1.3.2 ファンクション – 機密性・完全性・可用性の回復

目的: 全てのシステムを完全に復元すること。

成果: サービスを完全に復元する措置とインシデントの原因である検知された脆弱性[14]を塞ぐ措置。

サービスエリア 2 – 分析

CSIRT はインシデント対応において、検知したアーティファクトを分析しなければならない。さまざまなアーティファクトがあり、それぞれ異なった処置を必要とする。すべてのチームが、すべてのアーティファクトを処理するわけではない。

2.1 サービス – アーティファクト分析

アーティファクトのファンクション、目的の理解と、それらの配布、検出、無害化に関するサービスのことである。

[14] システムの安全性を損うセキュリティ上の欠陥のこと。ソフトウェアのバグによってできるセキュリティホールが一般的

TLP:WHITE

目的: インシデントハンドリングのプロセスにおいて、影響を受けたシステムやマルウェア配布サイトでデジタルアーティファクトが発見される場合がある。アーティファクトはスクリプト、ファイル、イメージ、設定ファイル、ツール、ツール出力、ログなどといった､侵入者による攻撃の痕跡かもしれない｡侵入者が組織のシステムやネットワークの侵入に利用するなど、どのようにアーティファクトを利用したか、また、システム内に入った後、侵入者が何をしたかを解明するためにアーティファクト分析を行う。

アーティファクト分析では、アーティファクト自体がどのように作動し、別のアーティファクトと共にどのように機能するかを解明しようとする。これには表層分析、リバースエンジニアリング、ランタイム分析、比較分析のようなさまざまな活動形態がある。それぞれの活動においてアーティファクトに関する詳細な情報が得られる。分析方法はアーティファクトの種類と特徴の識別、既に見つかっているアーティファクトとの比較、ランタイム環境におけるアーティファクトの実行の観察、バイナリ型のアーティファクトの逆アセンブルと解釈などであるがこれらに限定されない。アナリストはアーティファクトを分析して侵入者が何をしたかを再現・究明することに努める。そして被害状況を評価し、アーティファクトに対する緩和策を作成し、サービス対象者や他の研究者に情報を提供する。

成果: 復元されたデジタルアーティファクトの性質、他のアーティファクトとの関連、攻撃と悪用された脆弱性の理解。侵入者がシステムとネットワークを攻撃し、悪意ある活動を実行するのに使用した戦略・テクニック・手順を理解することで、分析したアーティファクトに対する緩和策が確認できる。

2.1.1 ファンクション－　表層分析

アーティファクトに関する基本情報とメタデータ（例：ファイルタイプ、出力文字列、暗号ハッシュ、ファイルサイズ、ファイル名）を確認し、特徴づける。また痕跡に関するあらゆる公的・私的なソース情報をレビューする。

目的: 基本的な情報収集の第一歩として、アーティファクトから得られた情報を、他の公的・私的なアーティファクトと/またはシグネチャーレポジトリ[15]と比較すること。
すべての既知の情報、すなわち潜在的な被害や機能と緩和策を収集・分析すること。実施されている分析の目的によってはさらなる分析が必要となる。

成果: デジタルアーティファクトの特徴とシグネチャーとアーティファクトについての悪質性、影響と緩和策など、すべての既知情報の確認。（確認した情報は次のステップの決定時に使用する。）

2.1.2 ファンクション－リバースエンジニアリング

実行環境に依存しない、アーティファクトの完全な機能を判定するための掘り下げた静的分析である。

目的:隠れたアクションやトリガーコマンドの特定など、マルウェアのアーティファクトについてより深い分析を提供すること。リバースエンジニアリングを行うことで、過去の（バイナリの）難読かされたソースやコンパイルを掘り下げることで、マルウェアを構成するプログラム、スクリプトやコードをアナリストは確認することができる。もしくはバイナリを逆アセンブルし、アセンブリ言語にし、それを解釈することでもそれが可能になる。すべてのマシン語を明らかにすることで、

[15] ハッシュ値のデータベース、内部で持っているもの外部で開示されているものなどを含む

TLP:WHITE

マルウェアが実行できる機能とアクションを明らかにすること。リバースエンジニアリングは、表層分析やランタイム分析で必要な情報が十分得られない時に行う、より深い分析である。

成果: デジタルアーティファクトの完全な機能を把握することで、どのように作動し、どのように誘発されるか、また攻撃されうる関連システムの弱点とその完全な影響や潜在的被害を理解できる。そしてアーティファクトに対する緩和策を準備できる。可能な場合には他の検体との比較用に新しいシグネチャーを作成する。

2.1.3 ファンクション – ランタイムもしくは動的分析

実環境またはエミュレートされた環境（例：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）において検体を実行し、観察によってアーティファクトの能力を理解する。

目的: アーティファクトの動きについて理解する手がかりを提供すること。 シミュレート環境を利用してホストやネットワークトラフィックへの変更と実行結果を保存する。大前提として実際の状況にできる限り近い環境で作動中のアーティファクトを観察すること。

成果: 感染したホストシステムの変化、他システムの相互作用とその結果のネットワークトラフィックを確認するため、実行中の動作を観察することでアーティファクトの動作についてのさらなる洞察を得て、システムへの被害と影響をより理解し、新しいアーティファクトのシグネチャーを作成し、緩和策のステップを決定する。
（注：アーティファクトのコードのすべてが実行されるわけではないので、ランタイム分析ですべての機能が明らかになるわけではない。アナリストはランタイム分析によってマルウェアがテスト環境において何をするかは確認できるが、マルウェアの全体的な能力を知ることはできない。）

2.1.4 ファンクション – 比較分析

カタログ化されたアーティファクトの系統分析など、共通の機能や意図を特定することにフォーカスした分析。

目的: ある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査すること。この調査には、コード・操作方法、標的・意図と作成者についての類似点を特定することがある。このような類似点により、大きな標的があるか、同じようなコードが以前使用されたかなど、攻撃範囲を引き出すのに利用できる。比較分析のテクニックとして完全一致比較やコード類似点比較がある。比較分析はアーティファクトや類似バージョンがどのように使用され、時間とともに変化したか、より広い視点を提供し、マルウェアの評価もしくは他の悪質なアーティファクトの理解を助ける。

成果: 他のアーティファクトとの共通点や関係を引き出し、デジタルアーティファクトの機能・影響・緩和策についてのさらなる洞察や理解を得るため、傾向や類似点を確認する。

2.2 サービス – メディア分析

「類似・関連のインシデントをどのように予防・検知と/または軽減するか」について理解を深めるため、システム、ネットワーク、デジタルストレージもしくはリムーバブルメディアからの関連データを分析することに関するサービスである。こういったサービスは法的観点、フォレンジック、コンプライアンス、もしくは他の履歴のレビューのための情報を提供することがある。

目的: ハードドライブ、モバイルデバイス、リムーバブルストレージ、クラウドストレージ、もし

TLP:WHITE

くは紙やビデオなどを含む他のフォーマットのメディアから証拠を収集し、分析すること。分析結果を法的もしくはコンプライアンス的な背景で提示する必要がある場合、情報は法的紛争・訴訟に際し利用可能な方法で収集し、証拠の一貫性[16]を維持する。証拠にはマルウェアの痕跡、例えば、ファイル、レジストリ、とその他のシステムコンポーネントの状態の変化といったアーティファクト、ネットワークトラフィックキャプチャまたは他のログファイル、メモリ内の情報を含む。ここで留意すべきはメディア分析とは、起こった出来事の証拠を見つけようと試み、必要に応じてその活動の要因を考えることである。これは 1 つのアーティファクトとその関係を見出だそうとするアーティファクト分析とは異なる。しかし、アーティファクト分析のテクニックはメディア分析のテクニックと方法の一環として使用されることがある。こういったサービスはサイバーインシデントの範疇外であっても、人事上の問題や、その他の法的もしくは組織的調査の一環として求められることがある。

成果: 分析により次の結果を提示する。１）情報資産（例：知的財産もしくは発見されたその他の機密情報）のリストを作り、２）インシデントに関連するメディア資産への追加・変更・削除を示す可能性のあるイベントのタイムラインを、可能なら「誰（何）がそのようなアクティビティをしたのか」と「すべてのエビデンスがどのように繋がっているのか」を共に提示し、インシデントの範囲と影響を説明する。

2.3 サービス – 脆弱性/悪用の分析

サイバーインシデントの要因となった、脆弱性についての理解を深めることができるサービス。

2.3.1 ファンクション – 脆弱性の悪用/パス分析

インシデント発生に利用された弱点とその弱点の悪用に使われた攻撃者のノウハウを理解する。

目的:既知の脆弱性（攻撃者共通のエントリーポイント）をステークホルダーに知らせることで、システムを最新に保ち、攻撃を監視し、ネガティブな影響を最小限にすること。

成果: システムへの侵入/攻撃を実行するための脆弱性や、悪意のある人物がその脆弱性を悪用する方法の十分な理解。

2.3.2 ファンクション – 根本原因分析

攻撃を可能にした「設計」や「実装」上の欠陥を理解する。

目的: 根本原因と攻撃ポイントを特定し、問題を完全に根絶すること。

成果: 脆弱性が存在しえた状況と結果としてどのような状況で攻撃者が攻撃できたかを十分に理解する。

2.3.3 ファンクション – 修正方法の分析

攻撃を可能にした基本的欠陥を修正し、将来の同様の攻撃を予防するのに必要なステップを理解する。

目的: 攻撃を可能にした問題を特定し、脆弱性にパッチを適用し、手順や設計を変更し、第三者によって修正方法をレビューし、そして修正の段階で作り込まれた新しい脆弱性を特定すること。

[16] 原文では、chain of custody

TLP:WHITE

成果: 特定の攻撃経路を遮断し、将来の攻撃を予防するため、プロセス・インフラ・設計の改善計画を立てる。

2.3.4 ファンクション – 緩和策分析

攻撃を招いた基本的欠陥を必ずしも修正しなくても、攻撃もしくは脆弱性によって作られたリスクを軽減（予防）する方法を見つけ出すための分析である。

サービスエリア 3 – 情報アシュアランス[17]

CSIRT はインシデント対応の豊富な経験を持っており、巷で実際に起こっている出来事を把握している。したがって、CSIRT がナレッジセンターとして何らかのリスク管理プロセスに関わることは理に適っている。しかし CSIRT は必ずしもそのようなリスク管理プロセスを有しているわけではなく、その要素の一部を担っている。このサービスエリアではステークホルダーのリスク管理の改善を支援するサービスについて説明する。

2.4 サービス – リスクアセスメント

リスクのアセスメントやコンプライアンスアセスメント活動に関連するサービス。アセスメント結果の評価を支援することによる実際のアセスメント活動の実施に関与することも含まれる。通常、コンプライアンスの要件　（例として ISO 27XXX、COBIT など）の裏付けとして行われる。

目的: 機会と脅威の特定を改善し、対策を改善し､情報セキュリティとその他の関連機能と共に損失防止やインシデントマネジメントを改善すること。

成果: 主要な資産とデータに適用する情報リスクアセスメントと情報リスクマネジメントのための一貫したプロセス。リスクアセスメントへのインプット。インシデント管理とフォレンジック（必要に応じて）を含む適切なリスク処理方法の選択。

2.4.1 ファンクション – 重要な資産/データの台帳

組織のミッション達成に重要とされる、主要な資産やデータを特定する。これらの資産やデータは必ずしも組織が所有しているものだけに限定されず、クラウドプロバイダ、外部のデータセットもある。保存場所、所有者、情報の機密レベル、ミッション機能、現在のステータス/レベルを特定することが、このファンクションに含まれる。

目的:　関連する事業部門と連携して組織が自らのミッションの達成を可能にするためにインシデントマネジメントが必要とする資産とデータを常に特定すること。

成果:組織のリスクアセスメントに使用する、定期的に更新される主要な資産とデータのリストもしくはデータベースといった台帳。

2.4.2 ファンクション –　標準評価

経営幹部によるセキュリティレベル・ステータスの評価のため、組織のリスクポリシーと、評価項目が列挙・特定された標準を得ること。 組織のリスクマネージャーや CISO が検討できるよう、アセスメントやベンチマーキングの判断基準を示唆すること。標準の例としては、 Basel II、COBIT、ITIL、認証や認定などがあるが、これらに限定されるものではない。

目的:　組織内で使用する承認された情報リスクアセスメント手法の選択を支援し、より広い組織

[17] 脅威情報や事前情報などを把握し、リスク管理の改善につなげること

TLP:WHITE

レベルのリスクアセスメントとリスクマネジメントへのインプットを提供すること。

成果: 組織全体で使用するために選択した情報リスクアセスメント手法。選択した手法に対する、経営幹部レベルの支援と賛同。選択したリスクアセスメント手法の適切な使用を義務付ける組織的ポリシー。同意された対策、テンプレート、アウトプット。情報リスクアセスメントのための同意されたプロセスや手順。情報リスクアセスメントの結果を組織レベルのリスクマネジメントと意思決定に統合するに取り決められた仕組み。

2.4.3 ファンクション – アセスメントの実施

リスクとセキュリティ要件が満たされていること・対処していることを確認するために、レビューの実施とアセスメントへの参加を支援する。

目的: 承認された手法を使い、できる限り綿密に、選択された主要な資産・データの情報リスクアセスメントを完了すること。

成果: 主要な資産やデータに関する情報リスクアセスメントの完了。

2.4.4 ファンクション – 所見と推奨事項

所見、報告内容、推奨事項を明らかにし、提供する。（例：レポート作成、情報開示タスクの利用）

目的: リスクアセスメントの結果から得られた所見の完全な文書化を支援し、アセスメントの結果から導かれた取るべきアクションと考慮すべき推奨事項を列挙すること。

成果: 主要資産やデータ、実施したリスクアセスメントプロセス、リスクアセスメントで使用したデータ、アセスメントの結果、推奨事項、アクション、計画と目標納期について詳述した、承認され署名されたレポートの配布。

2.4.5 ファンクション – 追跡

CISO やリスクマネージャーがアセスメントとその後の推奨事項の実施状況を追跡することを支援する。

目的: すべての計画、アクション、推奨事項が遵守され、文書で示された目標納期に完了したことを確かめること。

成果: 計画と目標納期の定期的なレビュー。完了したアクションのリスト、予定どおりにアクションが完了しなかった場合の目標納期の修正。計画と目標納期に対する進捗の報告。

2.4.6 ファンクション – 診断

ペネトレーションテスト、脆弱性スキャンとアセスメント、アプリケーションテスト、監査と検証など、リスクレベルが遵守されているかどうかの積極的な診断。

目的: 選択し実施されたリスク対応が目的に適合し、正しく実施され、期待どおりのリスク軽減をもたらしたかどうかをテストする。

成果: 期待される結果を記載した文書化されたテスト計画。文書化されたテストと結果。期待され

TLP:WHITE

る結果との比較。期待される結果との差異を修正するためのアクションと目標納期。

2.4.7 ファンクション – リスクアセスメントに関するアドバイス

リスクアセスメントの標準、アプローチ、手法、リスクアセスメントの実施と結果の管理方法に関するアドバイスを提供する。

2.5 サービス – 運用ポリシーのサポート

組織の運用コンセプトやその他のポリシーを策定、維持、制度化、施行するサービス。

目的: サービス対象者や関連事業部門に対して、検討中の機会や問題、アドバイスが用いられる環境、リソース上の制約などを考慮し、公平かつ事実に基づいたアドバイスを提供し、事業継続や災害復旧に関する信頼できるアドバイザーとしての役割を担う。

成果: 事業継続や災害復旧に組み込む事業上の決定事項。信頼されるアドバイザーとしてのインシデントマネジメント;適切な時と場所で事業上の決定に関与するインシデントマネジメントチームのメンバー。

2.6 サービス – 事業継続計画と災害復旧計画のサポート

識別されたリスクに基づく組織のレジリエンス[18]活動に関与するステークホルダーに提供されるサービスである。このサービスは、実際にアセスメントを実施することから、アセスメント結果を評価し軽減するための分析サポートを提供することに至る、リスクマネジメント活動の全般を含む。

目的:検討中の機会や問題、アドバイスが用いられる環境やリソース上の制約などを考慮し、サービス対象や関連事業部門に対して公平かつ事実に基づいたアドバイスを提供し、情報セキュリティやインシデント管理に関する信頼できるアドバイザーとしての役割を担う。

成果:情報セキュリティやインシデント管理に関する経営判断。信頼されるアドバイザーとしてのインシデント管理; 時と場所に適った経営判断にかかわることのできるインシデントマネジメントチームのメンバー。

2.7 サービス – 技術的なセキュリティサポート

サービス対象者や関連事業部門に、適切なセキュリティ運用やファンクションの実行と実装について、アドバイスを提供すること。

2.8 サービス – パッチの管理

インベントリの識別、パッチ適用するシステム、パッチインストールの展開と検証に関する管理に必要とされるケイパビリティによりステークホルダーを支援すること。

目的: 製品とサービスに使用されるパッチの特定、取得、インストール、検証を支援すると共に、及インシデントマネジメントの観点から、パッチ適用の有効性と影響のアセスメントを提供すること。

成果: 必要とされるパッチに関する組織上の認識と理解。サービスプロバイダーにより適用されるパッチに関する理解。情報リスクに対するパッチの効果に関する理解。インシデント管理上の効果に関する理解。

[18] 原文では resilience。柔軟に対応して回復していく力である

TLP:WHITE

サービスエリア 4 – 状況認識

CSIRT は自身の活動にフォーカスし、リスクマネジメントに貢献するため、最新の脅威の概況を入手する必要がある。脅威の概況を十分に把握することは簡単ではなく、下記のようなさまざまなファンクションに関連する。

状況認識とは、みずからが活動する環境についての認識を組織にもたらす一連の活動を指す。状況認識は組織のミッションに影響する重要な要素を識別すること、それらの要素を監視し、その知識を用いて意思決定とその他のアクションを導く。

状況認識は、組織がタイムリーかつ安全に活動する組織能力に影響を与える、組織内外のイベントや活動について必須の認識をもたらす。

2.9 サービス – メトリック運用

調査対象となる活動を特定するためのシステムと分析方法の開発・展開・運用にフォーカスしたサービス。

目的: 組織に状況認識を提供するための情報収集基盤とプロセスを作成すること。

成果: 状況認識のための情報を提供する運用情報収集基盤（センサーなど）。

2.9.1 ファンクション – 要件の分析

ステークホルダーの要求事項を理解し、CSIRT が活動できる許可を得る。

目的: この要件開発のプロセスは、組織の状況認識の要求事項を明らかにし、それらの要件を満たすために必要な情報のタイプに対応付ける。

成果: 情報の観点から組織とそのステークホルダーが必要とする認識レベルの把握。また、組織が情報収集のために必要なすべてのポリシーや法的承認を有することの保証。

2.9.2 ファンクション – データソースの特定

要件を満たすためのデータを特定する。

目的: センサーには自動システムから人為的なのものまでさまざまな形態がある。こういった情報（データ）ソースは組織の状況認識の全体認識図を築くために利用される。「データ要件の特定」のプロセスは、状況認識の要件と潜在的な情報源（センサーなど）を対応づけること。

成果: 組織の状況認識の要件を支援するのに必要のデータを特定。すでにデータソースが存在しているものもあるが、設計と取得が必要な場合もある。

2.9.3 ファンクション – データ収集

必要なデータの収集に使用する方法、ツール・テクニック・技術を特定する。

目的: このプロセスで集めた情報（データ）の収集・処理・保存方法を明らかにすること。

成果:情報をどのように収集・保存・処理・削除するか詳細の決定。

TLP:WHITE

2.9.4 ファンクション – 結果の管理

センサーから得た情報とメトリックスのトリアージと展開。通常、組織のさまざまなレベルごとに表示されるよう、ダッシュボード経由で提供する。

目的: ステークホルダーが結果を利用できるようにすること。

成果: 結果はダッシュボード、レポート、電子メールのウ週報などの形で対象となる利用者に提示される。

2.10 サービス – 統合と相関

複数のデータソースから取入れ、分析するサービス。ソースを問わず情報を取り込み、状況の全体像（状況認識）へ統合する。

目的: セキュリティインシデント対応や影響の緩和策を改善することができるよう、インシデント・指標・アクター間の新しい関係性を特定すること。

成果: 組織が新しい脅威情報を活用し、それを組織のナレッジリポジトリ[19]の既存情報と統合するための一貫したプロセスが可能になること。このプロセスの最終的な成果は、CSIRT がより効果的で正確な方法で意思決定が可能なよりよい情報である。

2.10.1 ファンクション – 統合アルゴリズムの決定

情報分析（統合）に利用する、方法・テクニック（アルゴリズム）もしくは技術を決める。

目的: インシデントハンドリングを担う者として、CSIRT はさまざまなソースから収集した情報について、正しい運用上の視点を維持することが重要である。情報が統合されることで、CSIRT が新たな情報を受ければ速やかに検討し、文脈に正しくあてはめ、インシデントハンドリングのプロセスに用いることを可能にする方法で管理されるようになる。情報を統合することで、CSIRT はインシデントハンドリングのプロセスにおいて、新しい情報を受け取るとともに速やかに考慮し、情報の関連付けを完全に行い使用できるようにする。

成果: インシデントの状況に応じて、新しい情報を取り入れ、既存の情報に照らし合わせて新しい情報を評価し、CSIRT が利用できる最終的な情報をうまく生成する内部プロセスが開発されること。

2.10.2 ファンクション – 統合分析

データ間の類似点と関係を明らかにするため、ナレッジ管理システムにあるデータを使い、データリソースを分析（統合）する。

目的: インシデントハンドリングの一環として、CSIRT は特定のインシデントが組織にもたらす脅威についての知見を継続的にメンテナンスする必要がある。そのためには、インシデント自体の最新の知識、敵が悪用した戦略・テクニック・手順（TTP[20]）の進化についての理解が必要である。継続的に情報を収集し、既存情報に照らして評価する必要がある。本ファンクションはファンクション 4.2.1 で選択した統合アルゴリズムを活用し、外部ソースから得た脅威情報の分析を行う。

[19] 様々な知識（情報）の蓄積のこと
[20] 原文は「Tactics, Techniques and Procedures」

TLP:WHITE

成果:　既存インシデントについて得られた新しい脅威情報の影響を理解し、攻撃者の TTP（戦略・テクニック・手順）のあらゆる変化に対し組織を備えさせ、関連するインシデントによりよく対処できるよう組織が緩和策や対応技術を常に更新できるようにすること。

2.11 サービス – セキュリティインテリジェンスの開発とキュレーション

内外のサービス対象者のために第三者のセキュリティインテリジェンス[21]の開発とキュレーションを行うサービス。セキュリティインテリジェンスは運用インテリジェンスや脅威インテリジェンスを提供するセキュリティ情報、もしくは脅威情報と定義できる。このサービスはアンチマルウェアのルールとシグネチャー、そして攻撃者の戦略・技術と手順のような脅威についての指標や検出ロジックを含むセキュリティインテリジェンスの分析・開発・分配・管理であるが、これらに限られるわけではない。これらのサービスは、サービスエリア 5「アウトリーチ/コミュニケーション」で定義されている情報交換活動に関連している。

目的:　十分なレベルの状況認識を得るのに外部からの情報は欠かせない。CSIRT はその運用に関する大量の質の高い情報を必要とするが、それを得るための費用や労力を考えると、選別された情報源に注力する必要がある。

成果:　CSIRT 運用のあらゆる側面に関する、複数の質の高いデータフィードが、主に完全自動プロセスでデータ管理システムに取り入れられること。別の成果としては、外部ソースから得た情報の流れから異常やトレンドの変化を検知するプロセスがある。

2.11.1 ファンクション – ソースの特定と保管

ナレッジ管理と分析プロセスにおける情報ソースの継続的な特定・保守・統合。

目的:　効果的なインシデンレスポンスを行うため、かつ積極的に状況認識（一般的な組織のセキュリティ体制）を向上させるために、関連する質の高い情報を外部ソースから取得すること。外部ソースはインシデントレポート、脆弱性レポート、CSIRT が運用するセンサーからのアウトプットといった内部で収集したデータを補完する。

成果:　内部、外部、オープンソースや商用ソースからの質の高いセキュリティに関連する情報の獲得。収集された情報はすべてデータ管理システムに保管される。

2.11.2 ファンクション – ソースコンテンツの収集とカタログ化

脅威情報のソースの獲得。ソースは内部、外部、オープンソースや有料サービスである。

目的: 収集した情報の質を評価すること。異常や新しいトレンドを検知するため、外部から取得したデータの特性（量を含む）の変化を観察する。

成果: ソースの品質評価を含めた文書化。外部ソースから得た情報の全般的特性の大きな変化に対する自動化もしくは半自動化されたプロセス。

2.11.3 ファンクション –　情報共有

データマークアップ（例: STIX、TAXII、IODEF、TLP）、指標[22]のデータベース、マルウェアや脆

[21] 最新の脅威を未然に検知し防御につなげるための知見
[22] 原文は Indicator（インジケーター）

TLP:WHITE

弱性カタログなどを含め、組織ナレッジを取得、開発、共有し、効果的に活用する。

目的: サービス対象者は彼らのニーズに合うサイバーセキュリティデータとナレッジを一定の品質でタイムリーに求めている。サイバーセキュリティデータはセキュリティの自動化を支援するため、システム処理を意図した情報で構成されている。サイバーセキュリティナレッジはサイバーセキュリティアナリストやオペレータ向けの情報から構成される。また、その他の CSIRT サービスやファンクションはサイバーセキュリティデータとナレッジをインプットとして必要とする。こういった情報は、複数のサービスやファンクションで再利用されるものがほとんどであり、CSIRT 全体のリソースとして最善な管理がなされる。

成果: 求められる品質のサイバーセキュリティのデータやナレッジがタイムリーにサービス対象者へ提供されること。他の CSIRT サービスとファンクションは、CSIRT 内の単一ソースから必要とするデータとナレッジを容易に獲得できること。

サービスエリア 5 – アウトリーチ/コミュニケーション

2.12 サービス – セキュリティ意識向上

直面している脅威とその脅威がもたらすリスク低減のため取り得るアクションについて、総合的な理解を深めるためにステークホルダー間で機能するサービス。

2.13 サービス – サイバーセキュリティポリシィのアドバイス

2.13.1ファンクション – ポリシーのコンサルティング

サイバーセキュリティポリシーは CSIRT が実施する具体的なタスクからとは別に、全体目標を目指して書かれることが多い。しかし究極的には CSIRT が行うサービスを規定するものでもある。

目的: サイバーセキュリティポリシーの作成と解釈は、ポリシーフレームワークから CSIRT によって実施される個々のファンクションに至るまで、サービスポートフォリオに翻訳する必要がある。

成果: CSIRT がポリシーを理解し、かつそれらの策定に積極的に貢献すること。

2.13.2ファンクション – 法的なコンサルティング

インシデントレスポンスの法的側面についてステークホルダーへのアドバイス。

目的: インシデントレスポンスはしばしば、法的に繊細な問題を扱う。例えば CSIRT スタッフは、プライバシー的に繊細な情報に触れることが多く、ある司法権の下では所有自体が違法となる資料にさえ触れることさえある。CSIRT とそのサービス対象者は、合法的に運用を確保する必要がある。このファンクションは十分な CSIRT 知識を有する外部の法律専門家によって提供されることが多い。

成果: 所定のアクションもしくはプロセスの法的アドバイスとアセスメント。

2.13.3サービス – 情報共有・開示

運用サポートの一環として組織によってサービス対象者に行われる通知など、幅広いコミュニケーションを軸としたサービス。（例：トレーニング、イベント、組織のポリシーおよび手順の通知）

TLP:WHITE

2.13.4ファンクション – 開示サービスの告知

組織、サービス対象者、業種や公共におけるセキュリティ実践の認知と実装を向上するためのセキュリティに関する情報の普及啓発。

2.13.5ファンクション – 情報の開示

- 要件の収集：どのような情報を誰にどのように、どういった時間枠（スコーピング）で広めるかを決める。
- 注意：情報の開示は限定する場合やパートナー向けなど、より詳細に開示する場合もある。
- 開発：要件を満たすフォーマットと情報製品の目的を決める。
- オーサリング：対象となる利用者が容易に理解できるよう的確に情報を取得する。（例：フォレンジック、インシデント、脆弱性とマルウェア管理に関する活動結果について提示する場合などにおいて）
- レビュー：開示する情報の明瞭性、正確性、文法、スペリング、情報の機微レベルと開示ルールの遵守をレビューし、最終承認を得る。
- 流通：必要かつ適切なチャンネルから対象となる利用者へ情報を配信する。

サービスエリア 6 – ケイパビリティの開発

2.14 サービス – 組織の評価指標

組織目標の達成状況を、識別し、体系化し、取りまとめ、分析することに焦点をあてて、効果測定するサービス。

目的: 今日、コンピュータセキュリティ対応チーム（CSIRT）やインシデント管理部門が抱える重要課題のひとつは、サイバーセキュリティインシデントの管理という CSIRT に与えられたミッションに対して、自分たちがどれくらいうまく応えられているかを見究めることである。このファンクションは、経営層、CSIRT、そしてとりわけステークホルダーが、自分たちの活動を評価し、価値を示すためには、どのような質問（情報）にこたえる必要があるかを確認することであり、必要なメトリックスを提供するものさしをあつめるメカニズムを確立すること、そこから結果を収集、分析、提示することに焦点を当てている。

成果: 「インシデント管理部門がそのミッションに対しどれだけうまく適合し実施できているかを示すのに十分な気づき、経験側的な証拠、改善すべきギャップを提供する。ここで得た情報を、意思決定の促進、パフォーマンスと説明責任能力の向上に使用できること。

2.15 サービス – 訓練・教育

ケイパビリティは CSIRT サービスにとって核となる構成要素のひとつで、サイバーセキュリティ、情報アシュアランス、インシデントレスポンスなどの各分野において、CSIRT のステークホルダー訓練・教育を提供する。キャパシティによって成熟度のレベルとしてのケイパビリティのレベルが推定できる。

目的: 教育訓練プログラムは、通常、ケイパビリティ構築に向けて踏み出す際の第一歩となる。教育訓練、必須とされる知識やスキルや能力の明文化、教育訓練用の教材の開発と配布、メンタリング、専門力開発やスキル開発、演習実施や実験室の設置などの様々な活動を通じて、このサービスは実現される。これらの各活動を総合的に実施することにより、組織やチームのケイパビリティを向上させる。

TLP:WHITE

成果: 教育訓練プログラムの全体像とともに CSIRT チームのケイパビリティ構築との関係性を理解すること。また、達成度を理解できる KPI のみならず、チームと組織の達成結果について、理解し文書化する立場になること。

2.15.1ファンクション – ナレッジ、スキル、能力に関する要件の収集[23]

ナレッジ、スキル、能力（KSA）[24]に関する要件収集: ステークホルダーに提供すべき訓練や教育の内容を決定するために必要となる知識、スキル、要求される能力、ステークホルダーの能力に関する情報を収集する。

目的: 俊敏かつ強力なチームメンバーの育成に向け、どのような KSA を CSIRT チームが必要とするかを、適切な形で評価し、特定し、明文化すること。

成果: CSIRT チームがビジネス要求に応えられるようになるための KSA とプロセスを特定する。これによりチームがどのレベルで運用されているか、改善の必要性があるかを把握できる。

2.15.2ファンクション – 教育・訓練教材の開発

プレゼンテーション、講義、デモンストレーション、シミュレーションなどの教育コンテンツや教育・訓練教材の構築や入手のこと。

目的: 教育訓練教材の開発は、ユーザーの意識を維持するのに役立つ。あわせて急速に変化する状況や脅威に対して CSIRT チームを最新化するほか、CSIRT とサービス対象者との間でのコミュニケーション促進のために役立つ。

成果: 適切な品質の CSIRT トレーニング・教育の教材。急速に変化する CSIRT を取り巻く環境からのニーズに対応し、多様でかつ効果的なプレゼンテーション技術やプラットフォームをもたらすこと。

2.15.3ファンクション – コンテンツの提供

知識やコンテンツを「生徒（受講生）」に提供すること。コンピュータを利用したオンライン訓練、講師主導型（instructor-led）訓練、仮想環境、会議、プレゼンテーション、実験室などのさまざまな方法によって実施する。

目的: コンテンツ提供のための正式な手順を作ること。これにより、CSIRT チームのメンバーが訓練を受けられる最善かつ網羅的なアプローチを確認できるようになること。

成果: テクニカルスキル、ソフトスキル、プロセスに関する講義や学習を、ハンズオン教習、遠隔 CBT[25]、個人訓練など、利用可能なすべての方法で提供できるコンテンツ提供のフレームワーク。

2.15.4ファンクション – メンタリング

現場訪問、ローテーション（交代）、シャドウイング、特定の意思決定と行動についての理論的根拠の議論などを用い、それまでに構築した関係を通じて熟練スタッフから学ぶこと。

目的: メンタリングプログラムは、メンターに対し、公式の報告関係やチームの体制の枠を越えて、

[23] 原文では、6.1.1 だが誤りのため正しい章番号 6.2.1 とした（以下章番号を繰り下げている）
[24] 原文は Knowledge, Skill, and Ability のこと。以下、KSA という
[25] CBT は Computer-Based Testing のこと

TLP:WHITE

公式にも非公式にも、メンターが教育やスキル開発、洞察力、人生/キャリア経験などをメンティーと共有するためのメカニズムの提供を支援すること。

成果: 定着率、業務への忠誠心、自信、適切な決断をおこなえる総合力を備えたCSIRTチームを得られること。

2.15.5ファンクション – プロフェッショナル育成

自分自身のキャリア計画とキャリア開発を、メンバーが適切におこなえるように支援すること。カンファレンスへの参加、応用訓練、互いに訓練することなども含む。

目的: プロフェッショナルの育成は、全体のチーム環境に関する新しいナレッジ、スキル、能力を確かなものにするための継続的なプロセスの成長を促進すること。

成果: プロフェッショナル育成の特性を引き出して、チームが自信を持つようになるだけでなく、すぐに実際の場面で活用し仕事上の役割や要求に基づいた最新のCSIRTに必須のナレッジ・スキル・能力を所持すること。

2.15.6ファンクション – スキル開発

日常の業務運用のためのツール、プロセス、手順に関する訓練を組織のスタッフに提供すること。

目的: 適切なスキルを確認したら、CSIRTは、インシデントへの備え（レディネス）の能力を見極めるための一連の活動に関与する必要がある。

成果: 必要とされるテクニカルスキル、ソフトスキル、プロセスの理解を備えた訓練されたスタッフが得られる。日々の運用上の課題やチームとサービス対象者[26]の両方のサポートについて準備万端なCSIRTメンバーを得られる。

2.16 サービス – 演習の実施

組織がサービス対象者に提供するサービスで、個々のサービス対象者やステークホルダー全体のケイパビリティの演習や評価を目的としたサイバー演習の設計・実施・評価を支援する。これらのタイプの演習には以下が用いられる：

- ポリシー&手順のテスト:チームはイベントに対処しうる十分なポリシー&手順があるかを評価する。このテストは通常、紙ベースで演習または机上演習を行う。
- 運用の準備状況（レディネス）のテスト:メンバーがイベントに対応するために適材適所で配置されているかどうか、手順が正しく実施されているかをチームが評価する。典型的なのは手順の実習である。

目的: 演習は、サイバーセキュリティに関するサービスとファンクションの有効性の確認や効率の改善を目的に実施される。本ファンクションと関連するサブ-ファンクションは、組織のニーズとサービス対象者のニーズの両方に関係する。具体的には、サイバーセキュリティのイベントやインシデントのシミュレーションを通じ、以下に示すひとつないしは複数の目的で演習を利用する。

- デモンストレーション: 意識向上のため、サイバーセキュリティに関するサービスとファンクションを、脆弱性、脅威、リスクと同様に説明する。
- 訓練: スタッフに新しいツール、技術と手順を指導する。
- 演習: 既に訓練を受けたツール、技術と手順を使用する機会をスタッフに提供する。陳腐化し

[26] 原文はCustomers

TLP:WHITE

やすいスキルには演習が必要であり、演習により、効果的にスキルを維持または改善する。

- 評価: サイバーセキュリティに関するサービスとファンクションの有効性・効率性のレベルを分析し、把握する。
- 認定: サイバーセキュリティに関するサービスとファンクションに関し、特定のレベルの有効性・効率性が達成されているかどうかを見極める。

成果: サイバーセキュリティに関するサービスとファンクションの有効性、効率性がすぐに向上し、さらなる向上のための課題を確認できること。演習の特定の目的に応じて、ステークホルダーに対してサイバーセキュリティをデモンストレーションしたり、スタッフに演習を受けさせたり、さらには、サービスとファンクションの効率性・有効性を評価・認定できること。さらに将来の演習を改善するための課題を認識できること。

2.16.1ファンクション – 要件分析

その演習が焦点を当てるべきサービス/ケイパビリティを特定する。

目的: 特定の課題に焦点を当てることで演習の適切な効果や成果を確実にすること。

成果: 演習の目的そのもの。

2.16.2ファンクション　–　フォーマットと環境の整備

演習の形式と範囲を明らかにする。

目的: 演習実施に必要なリソースを特定し、決定する。

成果: 演習のタイプと演習の実施に必要なリソース。

2.16.3ファンクション – シナリオ開発

ステークホルダーの目的に合致する演習シナリオの開発

目的: 演習を企画する目的は、サイバーセキュティ上のシミュレートされた（模擬的な・仮想的な）イベントやインシデントのハンドリングを通じて、対象となる参加者に対して、自分たちが提供するサービスとファンクションの有効性・効率性を向上させる機会を提供すること。

成果:　ある特定の対象参加者がサービスとファンクションの有効性・効率性を向上させ、さらなる向上に向けた教訓（課題）を確認できること。また、これらの演習自体を向上させるための教訓（課題）も得られる。

2.16.4ファンクション –　演習の実施

サービス対象者（受講生）のインシデント発生に対する準備状況（レディネス）をテストして、訓練の適用能力や仕事やタスクの遂行能力を測ること。テストは、仮想環境、シミュレーション、フィールド（実地）テスト、机上訓練、模擬シナリオ、もしくはこれらを組み合わせて行う。

目的:　演習や実地訓練を行うことで、組織の CSIR(サイバーインシデントレスポンス)計画とその実施能力を検証することで CSIRT チームが自信をもつことができるようになること。

成果: チームが準備万端な状態となり、KSA の主要プロセスとすべての仕事がともにうまくまわる

TLP:WHITE

ようになること。また、これによってチームの現状の運用レベルや改善の余地があるか、あるとすればどこかを見極められるようになる。

2.16.5ファンクション – 演習成果のレビュー

演習で得られた教訓や気付きやベストプラクティスを記載した事後レポートの作成。

2.17 サービス – 技術的アドバイス

サイバーセキュリティ関連のインフラ、ツール、サービスの推奨、開発、提供、取得に焦点を当てたサービス。これらのシステムやツールは、すべて CSIRT やセキュリティに関連するものであり、メッセージ送信/アラート通知ポータルなどを除き、一般的な IT 技術に関するものではない。なお、CSIRT は、ステークホルダーに向けたサービスとして、信頼できるツールを十分に提供すべきであることに留意する必要がある。

目的: CSIRT ステークホルダーのケイパビリティを構築・強化するプロセスにおいて、インフラ、システム、ツールに関する設計、取得、管理、運用、保守を支援すること、およびステークホルダーに対する CSIRT サービスのケイパビリティ、キャパシティ、成熟度の強化を支援することに特に焦点をあてること。これがサービスレベルの成熟である。

成果: サイバーセキュリティ関連のインフラとツールに関する、ニーズ評価、要件定義、レイアウト設計、取得、コンプライアンス検証、保守とアップグレード、運用訓練、内部監査と外部監査に関する体系的なアプローチの開発ができる。

2.17.1ファンクション – インフラの設計とエンジニアリング

ステークホルダーの要求を支えるインフラの設計とエンジニアリングを支援すること。

目的: 包括的なニーズ評価とステークホルダー要件の分析に基づいた、設計手法、関連する標準や規範に関する広範な知識の提供およびインフラの設計とエンジニアリングに関するベストプラクティスの強調。

成果: 国際的なベストプラクティスに基づき、関連する標準や規範を組み込んだインフラの設計アプローチと代替手段の開発と比較の実戦的な経験を得る。

2.17.2ファンクション – インフラの調達

インフラの調達支援で、リスクフレームワークの成熟度の開発支援や契約（書）のための最低限のセキュリティ要件や基準の作成を支援する。（例えば、製品認証のような特定の標準への準拠を求めるなど）

目的: 組織、技術、運用に関する要件の観点から、インフラの調達における信用照会条件を作成するための洞察を得る。

成果: 関連する標準と規範を遵守し、さまざまな技術的手段と順守すべき契約手順を考慮した上で、インフラの調達プロセスを理解できる。

2.17.3ファンクション – ツールの評価

ステークホルダーの代わりにツールを評価すること。

TLP:WHITE

目的: ハードウェア装置、ソフトウェア、カスタムアプリケーションを含むさまざまなツールの機能や法令適合性の評価を支援する。

成果: ツールの性能と、標準、規範、現時点の信用照会条件への法令適合性を分析できる。

2.17.4ファンクション – インフラの提供

必要とされるインフラ資源の取得を支援すること。（例としてハードウェアベンダー、サービスプロバイダーなど）

目的: インフラ提供をうまく達成するための重要な要因を明らかにすること。明確な義務と責任に基づいて、ソリューションプロバイダーとベンダーとの間の持続的かつ効果的な関係を構築するメカニズムを構築すること。

成果: 効率的で効果的なインフラ提供を可能にする適切なサービスレベルアグリーメント（SLA）を示してインフラ提供のための主要業績評価指標（KPI）を導き出すこと。

2.18 サービス – 教訓

インシデント対応は常にリアクティブな要素を持っている。短時間で、初期状態が不明瞭な場合が多い。多くのインシデントは潜在的な根本原因により発生するので、後になって修正が必要になる。このサービスは、類似のインシデントを防ぎ、類似状況またはより一般的な状況に対する対応を向上させることを狙いとしている。

目的: インシデントの根本原因を特定し、推奨すべきアクションをステークホルダーへ提示すること。

成果: プロセス、手順の調整や、潜在的な根本原因の修正をステークホルダーに推奨できること。

サービスエリア 7 – 研究開発

絶え間なく進化する脅威についていくために、CSIRT は継続的に適応する必要がある。これには新規または既存のツールを継続的に研究開発することが求められる。

2.19 サービス – 脆弱性発見・分析・改善・根本原因分析方法の開発

脆弱性関連サービスを実施したり、ほかの組織や同じように見える商習慣と調整したりする新たなケイパビリティを定義・特定し、その方法を改善するのに役立つサービス。

目的: 外部ソースから脆弱性情報を取得することのみで運営する組織もあるが、脆弱性を検知・分析するための本質的なケイパビリティを必要とし、それを求める企業もある。本ファンクションは組織がどのように脆弱性研究の機能を設計するか、概括することを目的としている。

成果: 必要なときに脆弱性をより深く理解する組織が使用する方法を見極める。

2.20 サービス – セキュリティインテリジェンスの収集・統合・関連付けのためのテクノロジーとプロセスの開発

運用インテリジェンスや脅威インテリジェンスに関して、新しいケイパビリティを定義・特定し、

情報分析の実施方法や関連サービスの共有方法を向上させるサービス。

目的: うまくいくためには、どんなセキュリティインテリジェンスのファンクションでも情報収集するとともに、関連情報を第三者と共有できなければならない。この情報収集は、機密情報の共有が十分可能な信頼レベルが実現できる情報共有者間の人間関係にかかっている。アナリストはこのような人間関係を築き、共有する必要がある適切な情報群を確認し情報の自動交換や関係管理と共同調査に最も適した手順（プロトコル）を特定し、情報ソースの有効性を評価することができなければならない。

成果: 組織は情報セキュリティ資産上の脅威を示す外部ソースからの関連情報を収集・分析・統合・評価するためのプロセスや手順を有する状態になること。組織が新しいソースやパートナーを開拓する有機的（体系的）な能力をもつこと。

2.21 サービス – ツールの開発

新しいケイパビリティを開発・特定し、CSIRT 関連の新しいツールやプロセスの自動化アプローチを共有するサービス。

目的: CSIRT の特定のニーズを満たすツールを開発すること。

成果: CSIRT が開発した CSIRT 関連タスクの自動化を助けるツールが、拡張性や信頼性があり確定的な結果をだすこと。また、これを使用しても CSIRT のセキュリティ体制を低下させないこと。アナリストというリソースをルーティーンワークから解放すること。

CSIRT 内活動 1 – データとナレッジの管理

CSIRT は、構造的・技術的なものも非構造なものも両方とも多くの情報を扱っている。非構造な情報は、「あるタスクがどのように実施されているか」についてのプロセスやナレッジの形になっている。比較的最近の情報はきちんと文書化されていない場合が多い。このため、スタッフが退職した場合にはケイパビリティを喪失してしまう。一方、構造化された情報は膨大な量になるはずで、適切に保管・処理する必要がある。

規準/仕様管理

データや情報は効果的に処理できる形で保管する必要がある。これはいくつかの規準に当てはめることで行われることが多い。これらの規準は、新しいタイプのデータに対応するために十分な柔軟性を持ち、且つ、利用に耐え得るほど具体的でなければならない。

1.1.1 データ規準

目的: 過去から現在に至るまでに処理された入手可能な情報を確保すること。

成果: 所与のデータタイプを処理するための規準、とできればそのためのツール。

1.1.2 ナレッジ仕様管理

目的: 時間をかけて蓄積されたナレッジの管理方法を特定すること。

成果: 情報取り扱いに関する規準とプロセス。

TLP:WHITE

データ保管管理

CSIRT はしばしば機密性、完全性と可用性において特別な要件を伴う情報を扱う。

目的: データ保管方法を規定すること。

成果: 異なるデータタイプごとのデータ保管仕様。

データ処理管理

CSIRT はしばしば、分析のため、或いは他のチームやステークホルダーへ転送するために大きなデータを処理する必要があることが多い。このデータの効率的な使用のためには、効率的な方法で処理する必要がある。

目的: 利用可能なデータの効率的使用のためのワークフローとツールを定義すること。

成果: ツールとワークフロー仕様。

データアクセス管理

目的:許可された主体にのみデータがアクセスできるようにすること。

成果: アクセス管理仕様。

自動化サポート

目的: データ、特に大量の場合は出来るだけ自動で処理すること。

成果: 自動化のためのツールおよびプロセス。

CSIRT 内活動 2　–　関係管理

POC とコミュニケーションの管理

連絡先（POC）のリストを維持し、メーリングリスト、トピックの分類法を整理し、それらをコミュニケーションチャネルに対応付けること。お知らせ、アラート、警告、データ供給とその他の開示物、またはと情報共有に使用するリストを管理すること。

電子メール、ウェブ、インスタントメッセージ或いはボイスコミュニケーションに使われる安全なコミュニケーション実施方法を管理すること。

仲間（ピア）関係の管理

CSIRT のミッションを実現するために必要な組織間連携の構築と維持管理。これには相互連携を確かなものとし、組織間、さらにはそれを越えた協力体制の促進も含まれるかもしれない。

ステークホルダーとの関係管理

ステークホルダーを特定、区別、理解、管理、追跡し、評価するのに利用する、戦術、戦略、技術の開発と実装。

会議とワークショップ

CSIRT とそのステークホルダーが脅威や直面する課題について話し合うために共に時間を過ごせるような機会を提供すること。これによって信頼関係を強め、連絡先を交換し、ベストプラクティ

スや教訓を共有することができる。

ステークホルダーとのエンゲージメントと関係性

部門間・階層間の調整含め、内外のステークホルダーとの公式な連絡先を維持すること。組織内のエグゼクティブレベルに働きかけ、組織のミッションを教育し、セキュリティ意識の理解を確かなものにする。

CSIRT 内活動 3 – ブランディング/マーケティング

CSIRT と CSIRT が提供するケイパビリティと CSIRT に要望を伝える方法について、ステークホルダーの認識を確固たるものにする活動。

CSIRT 内活動 4 – 演習参加

CSIRT にはその成熟度レベルに応じ、参加できるさまざまなレベルの演習がある。
評価: 演習の成果を評価し、フィードバックを求め、調査した演習状況に基づいた教訓を認識する。
調査: サードパーティの演習を調査する。
調整:演習を調整する。
参加：サイバー演習に参加する。参加者は演習のレベルや演習成果から参加する演習を選択できる。（例：サードパーティに参加を評価させる）

目的: 演習に参加する目的はサイバーセキュリティサービスとファンクションの有効性と効率を向上させること。参加は以下のいずれかの形で行われる。
・観察者: 演習の見学を行うが、演習を実施する参加者とはならず、課題を与えられることもパフォーマンスを評価されることもないスタッフ。直接参加せず観察することはある程度、CSIRT サービスとファンクションの有効性と効率性の向上の助けとなる。また、これからの演習の企画にも役立てられる。
・演習の参加者:参加者として演習に参加し、演習イベントの課題を与えられ、また評価も受けるスタッフ。
演習の形式次第で、スタッフは演習が行われる場所へ移動することもあれば、いつものオフィスや他の適切な場所から遠隔で参加することもできる。参加環境についても、演習固有の特別な環境が用意されることもあれば、自身のオフィスに作る研修環境や通常の業務環境から参加することもある。

成果: サイバーセキュリティサービスとファンクションの有効性と効率を向上させ、さらなる向上のための課題を確認する。演習の目的によっては、ステークホルダーへサイバーセキュリティを提示したり、スタッフへの研修を行ったり、またサービスとファンクションの効率と有効性が評価および/または認定されることがある。さらに将来の演習を改善するための課題を認識する。

CSIRT 内活動 5 – 教訓のレビュー

6.5 のサービスに似ているが、CSIRT 自体にフォーカスする。

目的: インシデントの収束後、パフォーマンスを分析することで CSIRT のケイパビリティを向上させること。

成果: 手順、プロセス、ルールもしくはインフラの変更の提言。

TLP:WHITE

TLP:WHITE

添付１　－　関連リソース

FIRST – https://www.first.org CERT/CC – http://www.cert.org
Trusted Introducer – https://www.trusted-introducer.org
TLP – https://www.us-cert.gov/tlp
IETF – https://www.ietf.org
ISO/IEC 27035 -
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379

添付２　－　用語集

- アプリケーションテスト– 検査条件下の製品やサービスの品質情報をステークホルダーに提供するために行われる調査。
- Basel II –バーゼル銀行監督委員会によって発行された、銀行法と規制についての推奨事項である Basel Accords の第二版。
- CERT/CC – Computer Emergency Response Team Coordination Centre の略。コンピュータ緊急対応チームコーディネーションセンター。
- CISO – Chief Information Security Officer の略。最高情報セキュリティ責任者。
- クラウド –インターネット接続デバイスを使用し、アプリケーションソフトウェアを稼働する、分散型コンピューティング環境。
- COBIT – Control Objectives for Information and related Technology 《米》情報システムコントロール協会
- 暗号ハッシュ – インバート、すなわちハッシュ値のみから入力データを再作成することが実質的に不可能と考えられているハッシュ機能。
- CSIRT – Computer （or Cyber） Security Incident Response Team の略。
- 外部のデータセット – サードパーティの収集データ
- FIRST – Forum of Incident Response and Security Teams の略。
- ファンクション – 目的を達成するための手段、もしくは特定のサービスのタスク。
- ファジング[27] – 時として自動化、もしくは半自動化されたソフトウェアのテスト手法で、 コンピュータプログラムの入力装置へ無効な、または予期しない、もしくはランダムなデータを入力するなどする。
- ハードウェアまたはソフトウェアエミュレータ – 1 つのコンピュータシステム（ホストと呼ばれる）が別のコンピュータシステム（ゲストと呼ばれる）のように動作することを可能にするハードウェア、もしくはソフトウェア。一般的に、ホストシステムにおいてソフトウェアを実行したり、ゲストシステム用の周辺機器を使用したりできるようにするために使用される。
- IDMEF – xxx
- IEC – International Electrotechnical Commission の略。国際電気標準会議。
- IETF – Internet Engineering Task Force の略。
- IODEF –　Incident Object Description Exchange Format（インシデントオブジェクト記述交換形式）の略。データ表現方法であり、コンピュータセキュリティインシデントについて CSIRT が一般的に交換する情報についてのフレームワークを規定する。
- ISO – International Organization for Standardization の略。国際標準化機構。
- ISO/IEC 27000-Series （ISO27k） – 情報セキュリティ管理や一般的な情報セキュリティマネジ

[27] 原文は Fuzz Testing

TLP:WHITE

メントシステム（ISMS）の中での危機管理についてベストプラクティス推奨事項を提供する、情報セキュリティの基準であり、品質管理保証基準（ISO 9000 シリーズ）と環境保護（ISO 14000 シリーズ）と似た構成となっている。

- ITIL – Information Technology Infrastructure Library（情報技術基盤ライブラリ）の略。IT サービスをビジネスのニーズと合わせることに焦点を合わせた IT サービスマネジメント（ITSM）の一連の実践集。
- オープンソース（情報） – 公開されている情報
- ペネトレーションテスト – セキュリティの弱点を見つける目的で、潜在的にコンピュータシステム、その機能とデータにアクセスし、攻撃すること。
- リバースエンジニアリング – 人工の何らかのものからナレッジ、もしくは設計情報を取り出し、そのもの自体を再生したり、その取り出した情報を元に別のものを作ったりすること。
- RID – Real-time Inter-network Defense の略。ネットワーク間におけるコミュニケーション方法で、既存の検知・追跡・ソース元の特定・軽減メカニズムを統合すると同時にインシデントハンドリングデータの共有を促進し、完成されたインシデントハンドリングソリューションを構築することを目的としている。
- サンドボックス – 実行中のプログラムを分離するセキュリティメカニズム。
- サービス – ステークホルダーの代わりに業務を行い、手助けする行為。
- STIX – Structured Threat Information eXpression （脅威情報構造化記述形式）の略。構造化されたサイバー脅威情報を示す標準言語を規定・開発するための協力的なコミュニティ主導型の取り組みである。
- 出力文字列– リテラル定数または何らかの変数として出力される結果の文字列。
- TAXII – Trusted Automated Exchange of Indicator Information（検知指標情報自動交換手順）の略。一連の各種サービスとメッセージ交換の手法であり、導入すると、企業や製品 / サービスの境界を越えた、実用的なサイバー脅威情報の共有が可能となる。
- TLP – Traffic Light Protocol（情報共有レベルの設定）の略。機密情報が適切な情報共有の範囲で使用されることを確かにするものである。
- 仮想環境 – コンピュータシステムのエミュレーション。
- 脆弱性スキャンと評価 – セキュリティ技術のひとつでコンピュータシステムにあるセキュリティ的弱点の特定に使用される。

＜以上＞

TLP:WHITE