TLP:WHITE

PSIRT Services Framework

Version 1.0

日本語版

日本語版は Software ISAC(一般社団法人コンピュータソフトウェア協会)と一般社団法人 JPCERT コーディネーションセンターによって翻訳された後、Panasonic PSIRT と Sony PSIRT によってレビューされました。FIRST.Org は関係者の協力に深く感謝します。

目的

CSIRT Services Framework および PSIRT Services Framework は、コンピュータインシデント対応チーム（CSIRT）および製品セキュリティインシデント対応チーム（PSIRT）が提供するサービスを想定してまとめられた高レベルのドキュメントであり、FIRST コミュニティの優れた専門家たちによって作成されている。FIRST は、国際連携 CSIRT、民間組織の CSIRT や PSIRT、その他のステークホルダを含む、すべての関係者からのフィードバックを取り込むよう努めている。これらのドキュメントは当初、新しいトレーニング資料開発の基礎を提供することを目的としていた。しかし今日では、例えば新しいチームの初期サービス内容を定義する場合など、より幅広い範囲で使用されている。

CSIRT サービスフレームワークを作成する過程で、PSIRT は CSIRT とはまったく異なるサービスを提供し、多くの場合まったく異なる環境で活動することが明らかになった。このため、PSIRT を対象とするドキュメントを別に作成することが決定された。2 つのドキュメントを並べてみれば、多くの共通点があることが分かるだろう。これらのドキュメントの開発は、Education Advisory Board によって推進されている。

CSIRT Services Framework および PSIRT Services Framework は、組織が CSIRT や PSIRT の機能を構築、維持、拡大することを支援するためのドキュメントである。これらはガイドであり、さまざまな組織モデル、機能、サービス、達成すべき成果を提示している。これらの情報をもとにして、チームは自由に独自のモデルを実装し、ステークホルダ固有のニーズを満たす機能を構築できる。これらのドキュメントは、チームの中核となる責任を明らかにし、責任を全うする能力を構築する方法に関するガイダンスを提供し、チームが組織にもたらす価値を説明する方法に関する見識を提供することにより、チームの活動を支援する。

はじめに

製品セキュリティインシデント対応チーム（PSIRT）は、組織が開発・販売する製品、ソリューション、コンポーネント、サービスなどの、脆弱性リスクの特定や評価、対処に焦点を当てた組織内のエンティティである。

適切に設置された PSIRT は、製品開発から切り離された独立したグループではなく、むし

ろ、組織におけるセキュアなエンジニアリングを推進する幅広い活動の一部として存在するものである。このような構成をとることによって、セキュリティ品質保証に関する活動を「セキュア開発ライフサイクル（SDL）」のなかに統合することができる。

製品のセキュリティインシデント対応は、多くの場合、SDL のメンテナンス段階と位置づけられている。これは、製品の脆弱性の多くが、製品やサービスが市場に提供された後に報告されるからである。しかし PSIRT の活動は、製品の構造、設計、計画、リスクモデリングフェーズの早期の要件収集の段階にも働きかけることができる。PSIRT の機能は、内部で発見されたセキュリティ問題に対応する際のガイダンスや監督機能として有用である。

サービスエリア - サービス - 機能 - サブ機能

サービスエリア

サービスエリアは、共通の特徴を持ち相互に関係する複数のサービスをまとめたものである。サービスエリアとして分類整理することにより、全体の構成を理解しやすくする。各サービスエリアは、サービスエリアの内容を概説するテキストで始まり、その後に、当該サービスエリアに分類される各サービスの説明が続く。

サービス

サービスとは、特定の結果を得るために実行される、認識可能で一貫した複数の機能の集まりのことである。サービスの内容は、次の形式で記述される。

- サービスの性質を記述する「説明」フィールド
- サービスの意図と測定可能な結果を記述する「目的」および「結果」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ための活動または一連の活動である。どの機能も、複数のサービスの文脈で共有され、使用される可能性がある。

機能は次のテンプレートで記述されている。

- 機能を説明する「説明」フィールド
- サービスの意図と測定可能な結果を記述する「目的」フィールドおよび「結果」フィールド
- 機能の一部として実行でき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ための活動である。 任意のサブ機能は、複数の機能および/またはサービスの文脈で共有され、使用される可能性がある。

PSIRT と CSIRT の違い

PSIRT が組織内 CSIRT 等と異なる点は、その活動の中心が製品のセキュリティである、ということである。一般に組織内 CSIRT の活動は、組織のインフラを構成するコンピュータシステムやネットワークのセキュリティに重きを置いている。

組織内 CSIRT と PSIRT には重要な違いがあるが、両者の間の相乗効果を認識しておくことも重要である。PSIRT も CSIRT も、組織の他の部分から独立して機能するものではない。このフレームワークでは、両者の活動において推進すべきコラボレーションと相乗効果（シナジー）に焦点を当てる。

PSIRT の組織構造

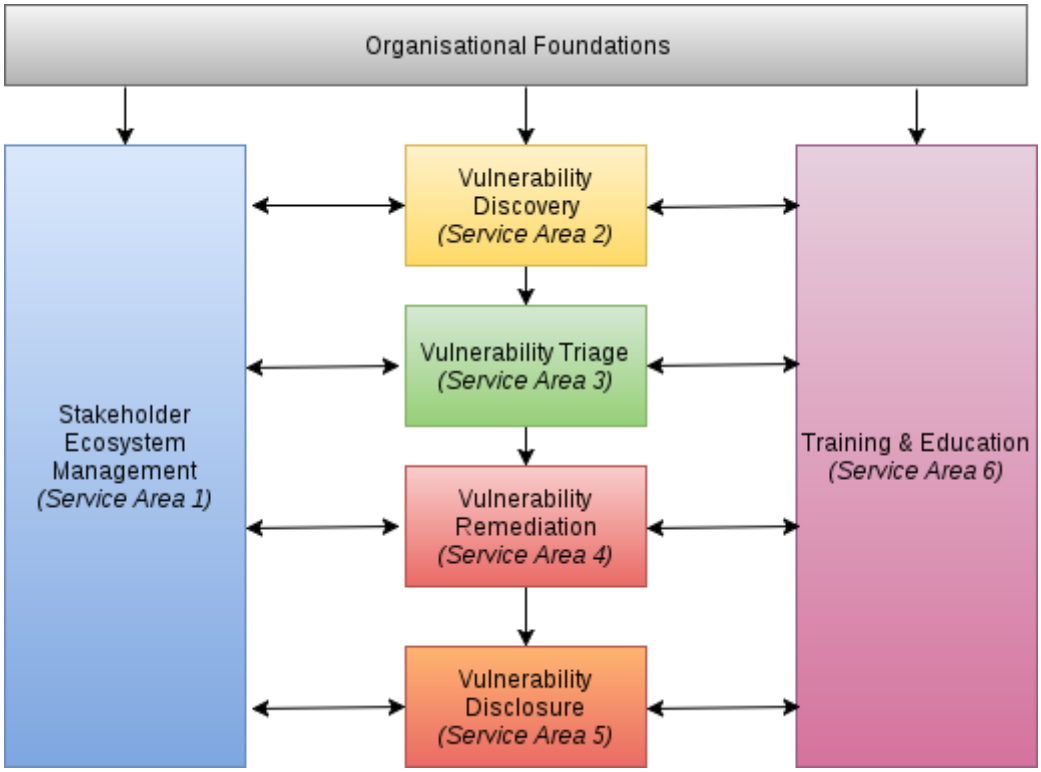


Figure 1: Organizational Structure

PSIRT の組織構造は、守る製品が多種多様であるのと同じように様々な形がある。同じ分野や同じ業界内であっても、ビジネス特性や運用モデル、製品ポートフォリオ、組織全体の構造、および製品開発戦略の違いなどがあるだろう。結果として、どんな組織にも適用できる単一の製品セキュリティインシデント対応戦略やチームテンプレートは存在しない。ただし、現在構築・運用されている PSIRT のほとんどは、分散モデル、集中モデル、ハイブリッドモデルという 3 つのモデルのいずれかにあてはまるだろう。

分散モデル

分散モデルでは、PSIRT 自体はごく小規模な組織であり、製品開発チームの代表者と協力して脆弱性に対処する。このモデルでは、PSIRT は以下のような役割を持つ:

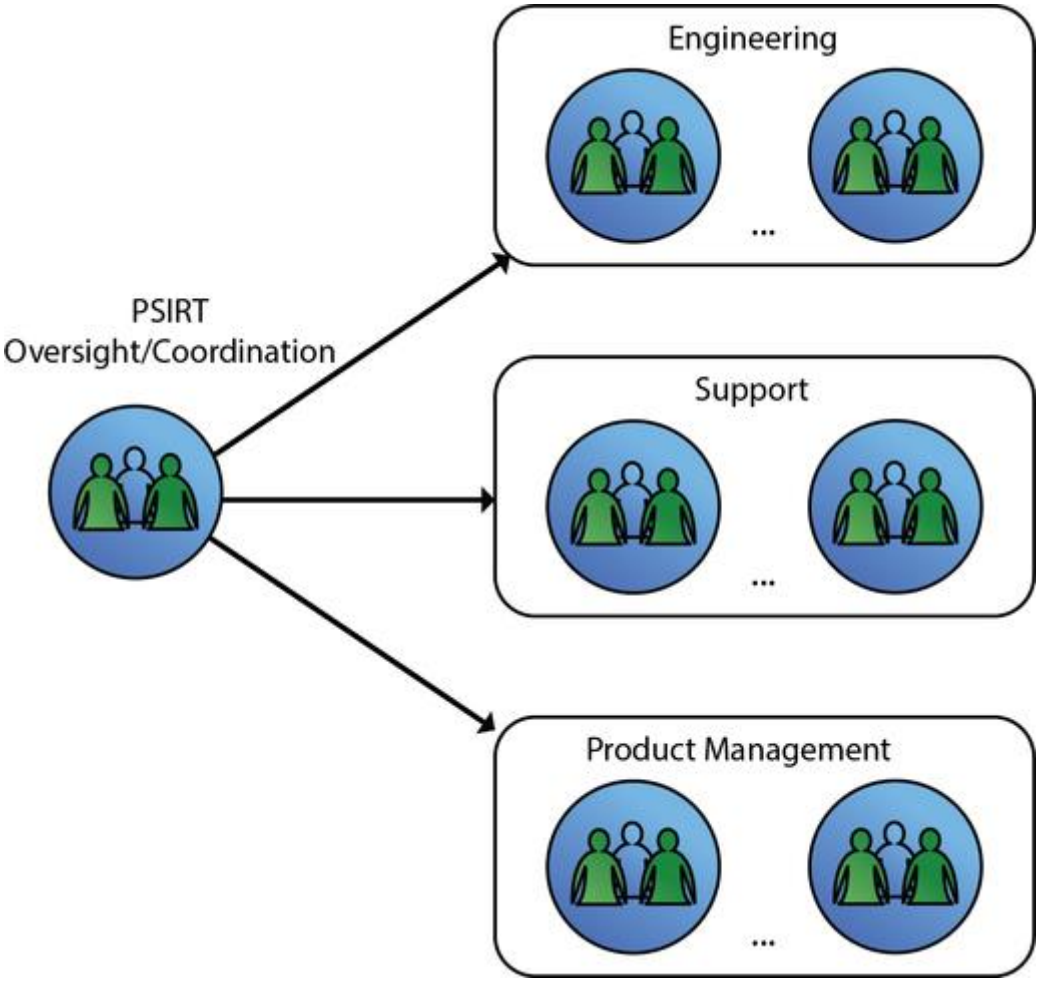


Figure 2: Distributed Model

- 脆弱性対応において、解決策・緩和策・その他アドバイザリに関する情報の取り扱いや、トリアージ・分析・対策作成・コミュニケーションなどの活動に関するポリシー・プロセス手順・ガイドラインを作成する
- 組織全体を通して、製品セキュリティエンジニアリング担当者の（階層化された）マトリクスを確立する
- 製品の脆弱性対応と潜在的なビジネスリスクについて、リーダーシップを発揮したり、助言したりする
- 組織のなかで外部から寄せられる脆弱性情報の集中管理を行う部署として機能することで、スケールメリットをもたらす
- 新しい脆弱性を製品オーナーや管理者、セキュリティエンジニアに通知し、修正対応などの計画作成を支援し、修正や緩和策の草案作成や公表を行う。さらに、インシデント管理を行う

組織の規模が大きく、多様な製品ポートフォリオを持つ組織は、PSIRT のコストが全体に分散されるため、分散モデルの恩恵を受けることができる。また、このモデルでは、製品開発チームの熟練者を PSIRT の活動に巻き込むことで、PSIRT の活動拡大に対応できる。一方、分散モデルの課題は、脆弱性のトリアージや修正プログラム提供の担当者が PSIRT の直接の管理下にないことや、PSIRT に報告を行わない可能性があることである。

集中モデル

集中モデルは多くのスタッフを抱える PSIRT のモデルであり、各部門から選抜されたスタッフが組織の製品セキュリティを担当する上級幹部に報告する。このモデルは次のような構造を持ち得る。

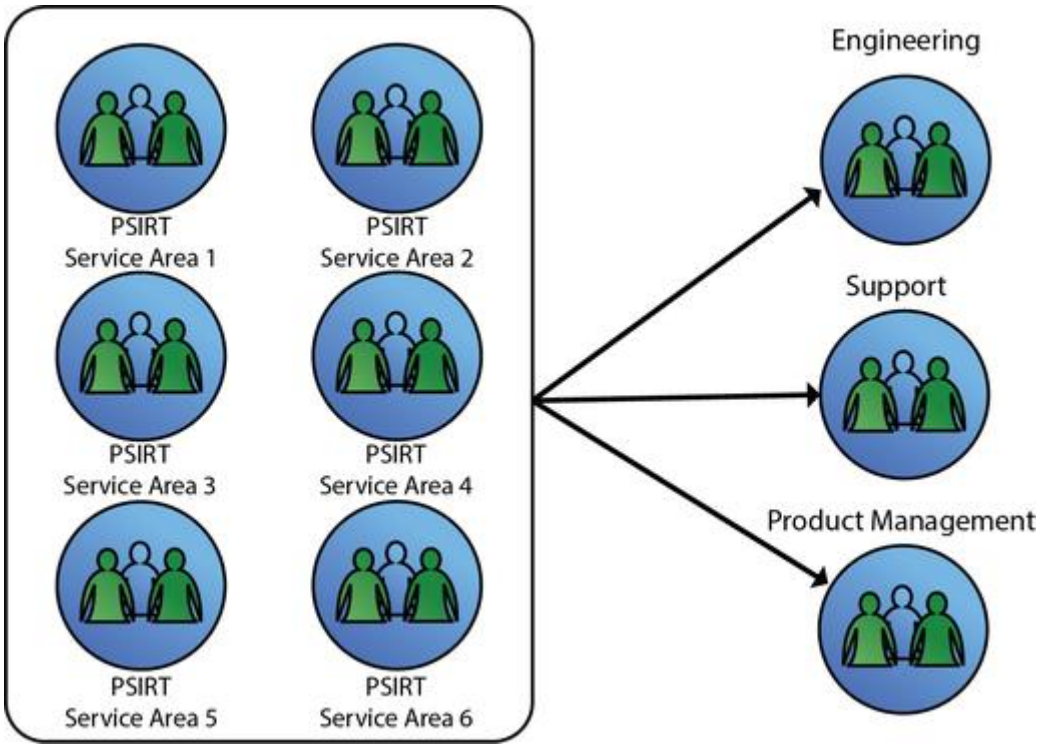


Figure 3: Centralized Model

- PSIRT プログラム管理部門: セキュリティ脆弱性のトリアージ、分析、緩和、修復、コミュニケーションのためのポリシー、プロセス手順、ガイドラインを作成する。またチケッティングシステムによる案件管理を行うとともに、PSIRT 活動全体を統括し、組織における PSIRT 活動を先導する
- セキュリティインテリジェンスとトリアージ: 脆弱性に関する様々な外部ソースを監

視する。組織の製品ポートフォリオに対する脆弱性の影響を初期評価する

- 対策とコミュニケーション: 製品のエンジニアリングチームに脆弱性に対する修正を直接提供する

このモデルは、より小さい組織や同種の製品ポートフォリオを持つ組織においてうまく機能する。また、高度なセキュリティスキルと専門知識を持った人材を 1 ヶ所に集めることで効率的に高度化を図ることができる。一方で、このモデルは集中的かつ専門的であるため、拡張性に乏しく、製品ポートフォリオが拡大したり多様化したりした場合のチーム維持にコストがかかるという課題がある。

ハイブリッドモデル

ハイブリッドモデルは、分散モデルと集中モデルの両方の特性を含むモデルである。次に挙げる要素を考慮し、双方のモデルが持つ特性や機能を選択して実装すると、ハイブリッドモデルの PSIRT を構築することになるだろう。

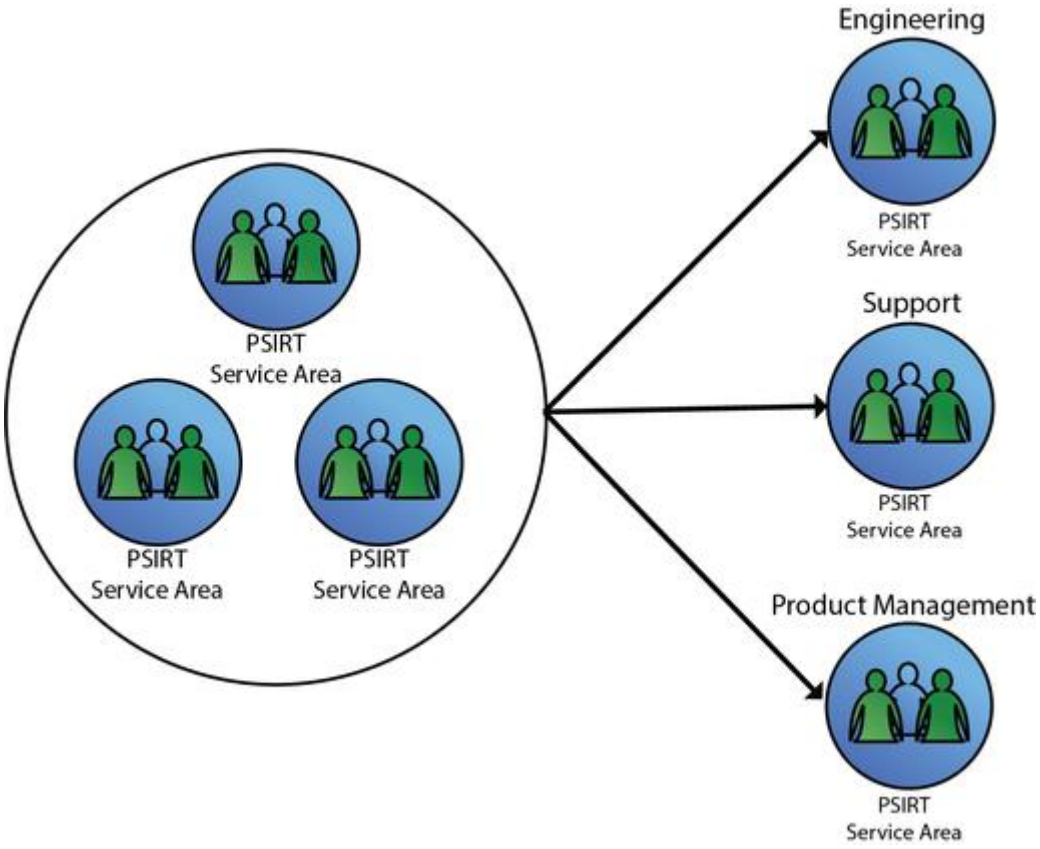


Figure 4: Hybrid Model

- 組織構造と規模
- 製品ポートフォリオの規模と多様性
- 製品開発戦略

その他の考慮事項

PSIRT は製品の脆弱性に関して独立性と客観性を備えた立場を維持するため、自律性を持つことが重要である。そのため、PSIRT の戦略や構造を検討するにあたっては、組織の報告体制を考慮し、組織としての融和を考える必要がある。また PSIRT から経営層に直接活動報告を行う形とし、PSIRT の権限を確認することが重要である。

PSIRT が成熟・拡大し、ミッションが進化するにつれて、チームの構成や報告体制が変化する可能性がある。PSIRT の変化と成熟の原動力は、主要なステークホルダの存在と、往々にして組織のステークホルダに広範にわたって影響を及ぼす深刻な脆弱性の存在である。ステークホルダは多くの場合、組織の規模や組織が採用した PSIRT のモデルから定まるものである。

ステークホルダ（利害関係者）

ステークホルダのニーズや要求を考慮することは、PSIRT の戦略と構造を定義する上で重要な要素となる。組織がどの PSIRT のモデルを採用するかによって、ステークホルダが特定され、それらが及ぼす影響力が決まる。また、ステークホルダとの良好な関係を保つことも重要である。「サービスエリア 1: ステークホルダエコシステムマネジメント」において、ステークホルダの管理方法の詳細を説明する。

最後にもうひとつ PSIRT 構築において検討すべき事項として「インフルエンサー」が挙げられる。インフルエンサーは、個人やグループとして特定されるステークホルダとは異なるものである。インフルエンサーは、業界や行政機関の基準や法令、規制、傾向のことであり、ステークホルダ以上に PSIRT の構築、戦略、活動方針や運用に影響を及ぼすことがある。

PSIRT は何をするのか？

どのようなモデルを選ぶかによって、PSIRT の活動対象や内容は決まってくるが、組織全

体として自社製品の脆弱性に対処するために取るべき行動は変わるものではない。このモデルは、組織全体における能力、取るべき行動や責任のなかで、PSIRT に直接帰する部分を明確にするものである。

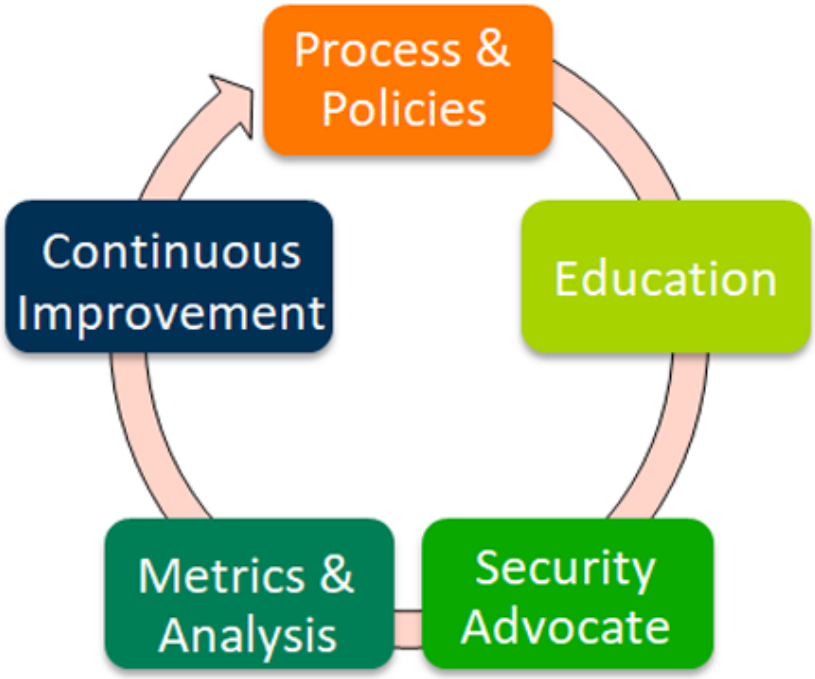


Figure 5: General PSIRT Activities

継続的なプロセスとポリシーの作成

PSIRT は製品セキュリティに関する組織の方針を確立する。PSIRT の必要性はビジネス上のニーズに依るものであって、その逆ではない。PSIRT のポリシーはその内容が実行に移される前に、組織内でレビューされ、権限を伴うかたちで組織内に浸透していなければならない。承認されたポリシーは、それに従えば組織としてそのポリシーの遵守が保証できるような行動手順が付随しなくてはならない。

ステークホルダの教育

PSIRT は製品の脆弱性への対処を効率的に実行・完了させるために、ポリシーと行動手順に沿ったワークフローおよび管理システムを構築する必要がある。そうすることにより、組織が製品セキュリティ対策を日常業務の中に取り入れることが容易になる。

PSIRT のミッションやポリシー、行動手順を組織に展開するにあたって最大の失敗となるのは、それらが自分の責任ではない、もしくは自分に要求されているものではないとみなされることである。そのため、組織内のすべての構成員に製品セキュリティの基本や各々の役割について教育することが非常に重要である。また、PSIRT のポリシー要件を満たすために、組織全体にポリシーを有効に機能させ、必要な権限付与も行わなければならない。

メトリクスの重要性

製品セキュリティインシデント対応の成否を評価することは非常に重要である。メトリクスのレポーティングは要件の定義には用いることはできないが、対応プログラムの支援、必要なリソースの決定、プロセス/ツールの改善が必要な箇所の特定にも役立つ。評価指標を定めそれをトラッキングすることは、PSIRT の導入や展開に関する課題を明らかにし、PSIRT の成熟にも役立つ。「サービス 1.7 ステークホルダメトリクス」および「サービス 5.4 脆弱性情報マネジメントの評価指標」では、トラッキングする価値のある評価指標の種類について詳しく説明する。

用語の定義

本ドキュメントではいくつかの用語を定義する。サービスエリア、サービス、ファンクションは、何がなされるべきかを異なる粒度で表すものであるのに対し、タスクとアクションはそれがどのように実施されるべきかを異なる粒度で表す点に注意が必要である。タスクとアクションは、のちに付随文書の中で公開され、またより頻繁に更新され得るものである。

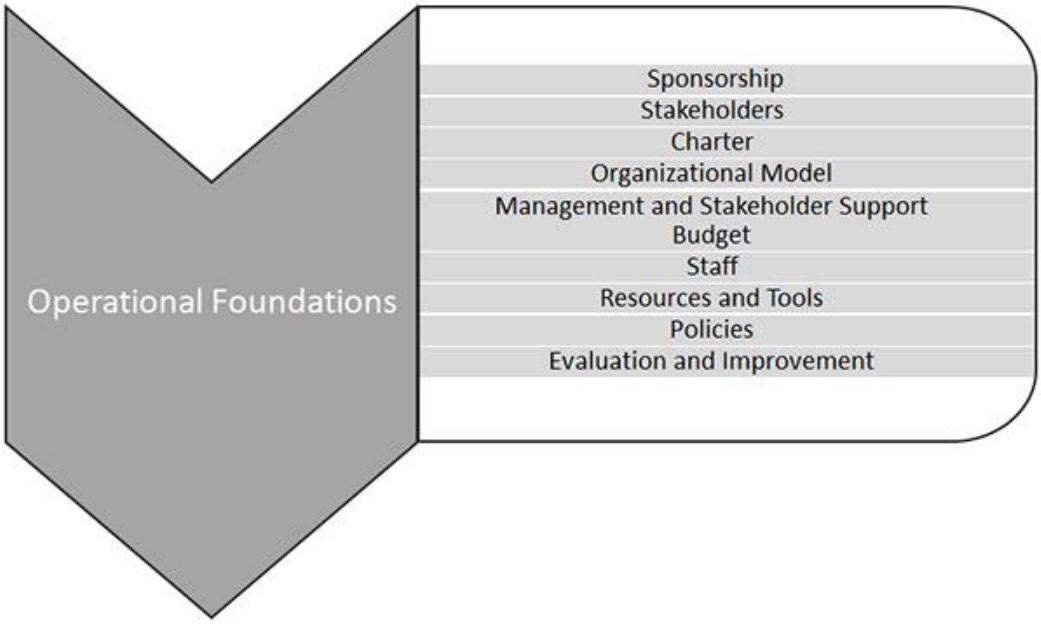
- **アドバイザリ** - 製品の脆弱性に関する通知、警告、対応に関する助言を行うための発表や速報のこと
- **Bug Bars（バグバー）** - セキュリティ上の脆弱性として分類されるバグの種類を定義する基準。これらの基準を満たすバグは脆弱性として、PSIRT の標準的な手順で対処される
- **コーディネーター（調整者）** - 脆弱性情報に関する取り扱いや開示に関してベンダと発見者の支援をする関係者のこと
- **公開の制限** - 影響を受けるベンダによりセキュリティアップデートあるいは緩和策や回避策が提供されるまで、顧客を守るために脆弱性の詳細公開を保留すること
- **発見者** - 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のこ

と。研究者、情報提供者、セキュリティ企業、ハッカー、ユーザ、政府、コーディネーターなどが含まれる

- **オープンソース** - ソースコードが公開されており、再配布およびソースコード変更が自由、使用する人や団体、使用分野を制限しない、使用に際して特定の技術に依存しない、といった条件を満たすライセンスの元に提供される製作物のこと。オープンソースソフトウェアは、多くの場合、個人や団体から構成されるコミュニティによって共同で作成し、維持される
- **パートナー** - OEM（相手先ブランドでの製造生産者）、供給者（社）、ODM（相手先ブランドでの製品設計生産者）
- **製品** - 有償販売あるいは無料提供される、実装または開発されたシステム
- **品質ゲート（クオリティゲート）** - 開発やリリースの次の段階に進む際に満たすべき基準のこと
- **修復（対策）** - 脆弱性を無くす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。修復は、通常、バイナリファイルの置換、構成の変更、またはソースコードのパッチと再コンパイルを意味する。「修復」に使用される用語には、パッチ、修正プログラム、更新プログラムおよびアップグレードが含まれる。回避策の意味で、ワークアラウンドや countermeasure といった用語も使われる
- **リスク** - 「目的に対する不確かさの影響」 ここで不確かさのなかにはイベントが生じたり生じなかったりする不確かさや、曖昧さ、情報不足によって生じる不確かさが含まれる
- **リスクの受容** - リスクを認識したうえで実際にリスクが顕在化しない限り対応を行わないとする戦略のこと
- **リスク検討記録** - リスク分析の結果やリスク対応計画の結果が記録されているドキュメント
- **セキュアな開発ライフサイクル（SDL）** - 開発コストを削減しながら、よりセキュアに製品を構築し、セキュリティコンプライアンスの要求に対処するための開発プロセスのこと
- **サービスレベルアグリーメント（SLA）** - サービスプロバイダー（内部向けまたは外部向け）とエンドユーザとの間で、期待されるサービスレベルを定義する契約
- **ステークホルダ（利害関係者）** - PSIRT のステークホルダは、製品やそのコンポーネントを開発および修正し、適切な製品コミュニケーション戦略を確実にするグループ、および製品セキュリティの恩恵を受けるグループのこと。つまり、PSIRT のステークホルダは、製品のセキュリティとインシデント対応に寄与したり、利益を得たりする関係者のこと
- **サードパーティ** - 製品またはソリューション/サービスに組み込まれるコンポーネントを提供する上流のサプライヤまたは開発者

- **ベンダ** - 製品またはサービスを開発したり保守したりする責任を負う人や組織
- **脆弱性** - 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悪用可能な欠陥

PSIRT の活動概要



このセクションでは、PSIRT の計画や確立、また効果的に運用するために必要な基本的なコンポーネントについて説明する。

> **目的**: 組織が PSIRT を確立し運用するための基本的なコンポーネントを、計画および実装できるようにする
>
> **成果:** PSIRT の運用基盤となるコンポーネントの特定/設計/実装が可能になり、製品とサービスを提供する組織の能力の維持に寄与する PSIRT の確立につながる

I. 戦略

A. 経営層の支援

組織の経営層および主要な意思決定者からの支援を獲得する。

> **目的:** 組織が PSIRT を確立し運用するための基本的なコンポーネントを、計画および実行できるようにする。PSIRT の効果的な運用を可能にするために、組織の経営層（例えば、C レベル（CxO）の役員、取締役会）または他の意思決定者に適切な情報提供を行い、彼らからの支援を得る
>
> **成果:** ビジネス指標に基づく継続的な資金提供と支援

経営層の支援を得るためには、PSIRT の重要性とその運用目的、セキュリティ脆弱性の潜在的リスク、および PSIRT 運用の利点を理解する助けとなる情報を提供する必要がある。（下記の「PSIRT 憲章」と「予算」を参照。）
関連情報については、「サービス 1.1 内部のステークホルダ管理」を参照。

B. ステークホルダ（利害関係者）

ステークホルダを特定し、彼らとの関係性を明らかにする。

> **目的:** PSIRT が誰にサービスを提供し、誰と連携するのかを理解する
>
> **成果:** 明確なステークホルダリスト

リストには、顧客、セキュリティ研究者、CSIRT、他の PSIRT のような外部のステークホルダと、ソフトウェア開発者、エンジニア、サポート、法務、広報のような内部のステークホルダの両方が含まれる。

関連情報については、「サービスエリア 1 ステークホルダエコシステムマネジメント」（特に「サービス 1.1 内部のステークホルダ管理」、「サービス 1.2 発見者のコミュニティとの交流」、「サービス 1.3 コミュニティと組織との交流」、「サービス 1.4 下流のステークホルダマネジメント」）を参照。

C. PSIRT 憲章

PSIRT 憲章あるいはその他のドキュメント（戦略計画、実施計画、運用コンセプトなど）を作成する。

目的: PSIRT が実施する業務の基本的な要素を特定、記述、文書化する

成果: PSIRT の設立理由、資金が提供された理由、および PSIRT に期待される成果を説明するドキュメントが作成される

PSIRT 憲章（または計画）では、以下を定義する必要がある。

- PSIRT のミッション（組織のミッション達成と整合性があり、それを助ける必要がある）
- 目的、役割と責任
- 製品やサービス（脆弱性報告の受け取り、修正プログラムやパッチの開発、パッチ情報の配布など）

D. 組織モデル

PSIRT の組織構造とモデルを決定し、文書化する。

目的: PSIRT が運営する組織モデルを特定、記述、文書化する

成果: 文書化された役割と責任に基づいて、明確なチーム構造を作る

文書化された組織モデルでは、PSIRT 内部の報告体制を記述し、PSIRT の活動が立脚している権限を特定する必要がある。一般的な組織モデル（分散モデル、集中モデル、ハイブリッドモデルなど）の説明については、イントロダクションの「PSIRT の組織構造」を参照。関連情報については、「サービス 1.5 組織内でのインシデントに関するコミュニケーション調整」を参照。

E. マネジメントとステークホルダの支援

組織の管理者や内部のステークホルダからのサポートの「合意」を得る。

目的: PSIRT の効果的な運用を可能にするために、他部門の経営層およびステークホルダからの支援の合意を得る

成果: ステークホルダには、継続的な支援を可能にする重要なビジネスメトリクスが示される

関連情報については、「サービス 1.1 内部のステークホルダ管理」を参照。

II. 戦術

A. 予算

PSIRT を運用するために必要なリソースを特定し、これらのリソースを賄うための適切な資金を調達する。

目的: PSIRT 運営に必要な資金が提供されるモデルを特定、記述、文書化する

成果: PSIRT の運用コスト、経費、資金供給モデルの文書化

予算には、PSIRT スタッフを雇用するための経費（給与、福利厚生、その他のコスト）、機器およびその他の経費（情報技術システム/機器、ソフトウェアライセンス）、訓練予算（旅費を含む）が含まれていなければならない。

B. スタッフ

PSIRT のサービスを提供するための人材像を特定し、熟練したスタッフを獲得する。

目的: PSIRT メンバーを確保できる組織モデルを特定、記述、文書化する

成果: PSIRT の人的リソースのニーズを文書化

個々のメンバーのスタッフのポジションや役割、責任、またそれらの役割に期待される知識、技能、能力およびその他の要件（学歴、職歴、資格など）を明記する。フルタイムの従業員、ベンダ、請負業者を、またはそれらを組み合わせたものを、PSIRT メンバーとしてのポジションや役割に割り当てることができる。

PSIRT のスタッフ配置計画の一環として（または別のドキュメントとして）、PSIRT のスタッフに対する一般的な訓練や個人の役割に基づく訓練の要件を特定し、計画する必要がある（例えば、初心者研修/自発性を促す研修、継続的な訓練、教育、意識啓発、専門的な人材育成のための高度な訓練）。

関連情報については、サービス 6.1 PSIRT トレーニングを参照。

C. リソースとツール

PSIRT 運用のために他に必要なリソースやツールを特定して取得する。

目的: PSIRT が機能するために必要なリソース、機器、ツールの特定と調達

成果: PSIRT のツールとリソースのニーズが文書化され、組織に理解される

これらのリソースとツールには以下が含まれる。

- 施設（オフィススペース）などのインフラ
- ツール/技術/機器（ハードウェア、ソフトウェア）（例: 「サービス 3.3 脆弱性の再現」を参照）
- 脆弱性報告システム/方法（例: ウェブサイト、E メール、電話）（「サービス 2.1 脆弱性報告の受付」を参照）
- 安全なコミュニケーション（例: PGP/暗号化）（「機能 1.5.2 安全なコミュニケーションの管理」を参照）
- 脆弱性データベース／トラッキングシステム（例: 「機能 1.5.3 セキュリティ欠陥のトラッキングシステムの更新」と「機能 3.2.1. 発見者データベース」を参照）

III. 運用

A. ポリシーや手順

ポリシー、プロセス、運用に関連する手順の文書化。

目的：PSIRT の運用方針と手順の特定、記述、文書化

成果: PSIRT の権限やガバナンス/オペレーションを記述する正式なポリシーと、正式に文書化された職務遂行のための手順/ガイドライン

ポリシーと手順を文書化することにより、PSIRT の全スタッフが共通の理解を持つことが

でき、PSIRT が提供する製品とサービスの一貫性と再現性を実現することができる。更には新しい PSIRT スタッフのトレーニングリソースとなる。

B. 評価と改善

改善点を特定できるようにするため、パフォーマンスおよび/または有効性を評価するための指標を定める。

> **目的:** PSIRT がどれだけうまく機能しているかを評価し、改善の必要がある領域を特定する
>
> **成果:** PSIRT は、パフォーマンスを測定し、改善が望まれる分野を理解することができる

PSIRT は、製品とサービスがどのように提供されているのかを継続的かつ/または定期的に評価し、改善が必要な分野を特定する。

評価指標および方法は、公式または非公式な方法（例えば、ステークホルダからのフィードバックの収集）で、計画に従ってまたは必要に応じて、実施することができる（例: 学んだ教訓を文書化する「機能 1.1.3 インシデント事後対応プロセス」を参照)。

このドキュメントで提供する情報を参考に、PSIRT の運用を評価する基準を検討するのもよいだろう。

サービスエリア 1

このサービスエリアは、PSIRT が社内外のステークホルダと適切に関わり、役割を果たすことができるサービスと機能を説明する。ステークホルダエコシステムマネジメントに含まれるサービスの実行は、PSIRT のインシデントライフサイクルやチームの成熟ライフサイクルに有効に機能する。このサービスエリアは、PSIRT のすべてのステークホルダに適切に情報が提供され、インシデント対応プロセスに従事することを目的としている。

PSIRT は、これらのサービスを正式に提供する前に、まずその事業に関連するステークホルダを特定する必要がある。ステークホルダには、経営層またはビジネスリーダー、社内開発チーム、外部コンポーネントの提供者または開発者、さらには組織の顧客などが含まれる。ステークホルダの製品やバージョンのマトリクスを整理しておくことは、コミュニケーションプロセスの効率化に役立つ。これらのステークホルダとのコミュニケーションに先立って、(ウェブポータル、個人的な E メール、インターネットチャット、チケットシステムなど) 彼らが望む視点や方法を理解することも有益である。この本ドキュメントでは、ステークホルダをいくつかのグループに分類している (特定のビジネス環境では、他を特定する場合がある) : ファインダー、同僚/パートナー、社内チーム、製品の顧客。

> **目的:** 連携可能なまたは連携しなければならないステークホルダと、情報共有するプロセスとメカニズムをハイライトする

成果: ステークホルダの良好な連携によって、セキュリティ脆弱性についてステークホルダに伝えなければならないときに、タイムリーかつ必要なステークホルダ／パートナーに納得のいく報告が行える

サービス 1.1　内部のステークホルダ管理

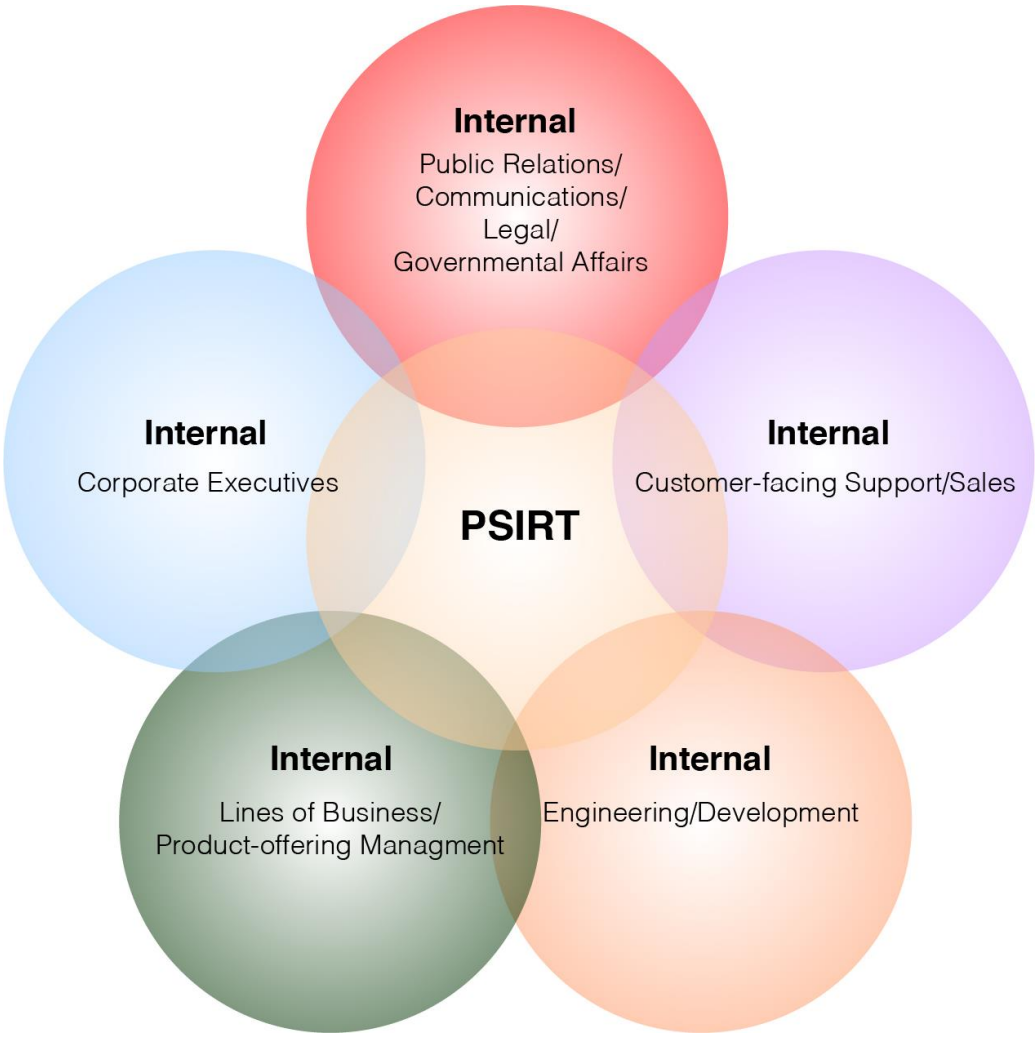


Figure 6: Internal Stakeholder Management

内部のステークホルダとの関わり合い、関連するプロセスを定義し、インシデント時の認識や支援を確実なものにする。組織内の PSIRT の役割を明確に伝え、製品チームとセキュリティアナリストとの間の連携を確立し、コミュニケーションや対応力を向上させる。

目的: 社内のステークホルダに対して PSIRT の権限と専門知識を確立し、脆弱性

の修復や製品セキュリティの円滑な調整を促進する

成果: すべての PSIRT プロセスと成果は、関与の高い内部のステークホルダと協同することで、よりスムーズに流れる。例えば、従業員によって脆弱性を発見することにより、公開時期に関する外部との調整やメディア対応などの負荷を緩和することができ、組織、利用者およびより大きなコミュニティに利益をもたらし、修正されていない脆弱性が公開されるリスクを最小限に抑えるスケジュールで問題に対処できるようになる

機能 1.1.1 内部ステークホルダとの交流

製品の開発やテスト、パッケージング、および保守に関する社内チームと活発な対話を維持する。内部ステークホルダには、エンジニアリングリソースだけではなく、テスト/品質保証、リリースエンジニアリング、ステークホルダ対応サポートチーム、セールスやマーケティング、またはその他の技術分野の専門家が含まれる。

目的: 内部のメッセージング/情報プラットフォーム上に PSIRT の存在意義が示せる体制を構築して、PSIRT の存在、プロセス、および機能について内部の関係者に通知する

成果: PSIRT が正式に文書化された内部ステークホルダリストを保持し、彼らの役割や責任を理解する

サブ機能 1.1.1.1 会社やビジネスリーダー、経営層との交流

PSIRT を有効に機能させるには、現在の組織環境を理解し、それに対応できるようになっている必要がある。ビジネスリーダーや経営層と協力することは、様々なレベルで PSIRT の支援となる。経営層の支援は PSIRT の存在を正当化することに役立つ。これによって、情報を共有し、ビジネス上の意思決定に役立つことができる。また経営層の支援は PSIRT のミッションに影響を及ぼす施策や組織の方向性の変化も捉えることができる。

サブ機能 1.1.1.2 広報/コーポレートコミュニケーション、法務部との交流

社内のコミュニケーションチームや法務部門と連携することで、ブランドやメッセージ発信ポリシー、組織が遵守しなければならない規制/法的環境にあわせた活動を行うことができる。重要なイベントやインシデント発生時に効果的な連携ができるよう、これらのステー

クホルダとは事前に連携手段を確立しておくべきである。

サブ機能 1.1.1.3 ビジネスラインとの交流

開発関係者と交流することによって、問題が適切に文書化、優先順位付け、対処される。例えば、PSIRT のエンジニアまたは承認された代理人が、欠陥のあるコードの責任を有するソフトウェアエンジニアリンググループと脆弱性修正に関する調整をする必要がある。インシデント発生時には、当事者間での連携は情報の迅速な伝達と問題の効果的かつ迅速な修復に役立つ。またステークホルダには、プログラムまたはプロダクトマネージャー、SDL 監視グループ、プロジェクトマネージャー、プロダクトオーナー、および同様のビジネス関連の責任を持つ関係者が含まれる。

サブ機能 1.1.1.4 開発／エンジニアリングとの交流

PSIRT のエンジニアは、欠陥のあるコードを担当するソフトウェアエンジニアリンググループと脆弱性の修正調整を行う必要がある。開発関係者との連携によって、問題が適切に文書化され、優先順位を付けられ、対処される。インシデント発生時には、これらのパートナーシップは情報の迅速な伝達と、問題の効果的かつ迅速な修復に役立つ。

サブ機能 1.1.1.5 顧客に対応するセールス、サポートとの交流

PSIRT のエンジニアはステークホルダのサポートチームに説明や成果物を提供する。それによって問題が起き情報が公開されても、問い合わせやサポート要求に応えることができる。「サポート」には、フロントライン（ヘルプデスク）要員、プレミアムサポートリソース（テクニカルアカウント管理、ステークホルダサクセスマネージャーなど)、社内外のセールスチーム、インフィールドリソース（コンサルティング、セールスエンジニアリングなど）が含まれる。

サブ機能 1.1.1.6 内部ワーキンググループへの参加

より成熟した組織では、PSIRT のエンジニアは、様々な社内イニシアチブやワーキンググループに参加することで、内部ステークホルダとの関係を構築し強化することができ、PSIRT の技術的専門知識を再確認/確立し、将来の取り組みのためのネットワーク/コミュニケーションチャネルを構築することができる。

機能 1.1.2 社内のセキュアな開発ライフサイクル

SDL を維持し、実施することは、組織の製品に対するステークホルダの信頼を確立するための基本である。製品のライフサイクルを通じてセキュリティ基準が継続的に適用されていることが証明できないと、組織の製品に対するステークホルダの信頼を失い、組織への厳しい要求が課せられる（証明の負担、監査の権利など）可能性がある。最終的には売上と組織に対する信頼を失うことにつながりうる。

> **目的:** 優れた SDL の実践に従う組織は、製品開発の初期段階で製品の欠陥を把握することでき、脆弱性の改修に費やすコストが少なくなる。 このライフサイクルのすべての参加者は、セキュリティ機能、全般的な機能、および製品の要件に関する期待を明確に把握し、ライフサイクル内での役割と責任を理解する
>
> **成果:** 明確な製品リリース情報を持ち、配信パフォーマンスに関するメトリクスとデータを提供することができる。成熟した組織では、過去の製品の一般的な弱点に関するデータを提供し、今後の取り組みで同様の失敗を避けることが可能である

サブ機能 1.1.2.1 SDL 活動に参加

SDL は、企業が共通の基準に準拠し、安定した再現可能なサービスを提供するのに役立つ重要なガバナンスプロセスである。 組織の SDL の作成と保守に PSIRT が参加することで、適切なセキュリティプラクティスとチェックが確実に行われるようになる。

サブ機能 1.1.2.2 SDL ガバナンスに参加

SDL は、企業が共通の基準に準拠し、安定した再現可能なサービスを提供するのに役立つ重要なガバナンスプロセスである。 PSIRT がガバナンスに参加し、組織の SDL を実施することにより、適切なセキュリティプラクティスとチェックが確実に行われ、例外が文書化され、適切に審査されるようになる。

機能 1.1.3 インシデント事後対応プロセス

PSIRT は、組織の提供製品に脆弱性が発見されると、参加するステークホルダや組織のリーダーにフィードバックを提供するため、コード、プロセス、または人事関連の問題をレビューするプロセスが必要である。深刻な脆弱性や既に広く知られている脆弱性の中には、企業がその問題にどのように対応し、解決したかについて、より詳細な分析が必要になる場合

がある。インシデント対応後には、修復やコミュニケーションの取り組みに関わるすべての社内関係者が関わる会議で、何がうまくいったのか、何がよりうまく実施できたはずなのか、そして将来のイベントに対応するためにどのような変更が必要なのかを追求し文書化する。

> **目的:** 関係するすべての関係者/チームの観点で、セキュリティインシデントを含む、脆弱性対応中に発生したイベントについて、事実に基づく明確な説明を提供する。重大な問題が発生した場合、PSIRT は、広く知られている影響の大きい問題を改善するための組織の対応を支援し、指導することができる
>
> **成果:** PSIRT は、ソフトウェアの脆弱性に対応する組織のパフォーマンスに関するデータを提供する。このデータは、今後のイベントの改善のために「教訓」として組み込まれる

サブ機能　1.1.3.1　製品脆弱性レビュープロセスを確立

問題をレビューする一貫したプロセスを確立することで、教訓を踏まえて製品が継続的に改善されるようになる。

サブ機能　1.1.3.2　プロセスとアップデートリリースのタイミングを確認し、強みのある領域、弱みのある領域をトラッキングする

サブ機能 1.1.3.3 注目を集めたインシデントのレビュー

注目を集めたインシデントに対する組織の対応、レビュー、組織の教訓をまとめ、必要に応じてビジネスデータやその他のステークホルダにレポートデータを提供する。

サービス 1.2 発見者のコミュニティとの交流

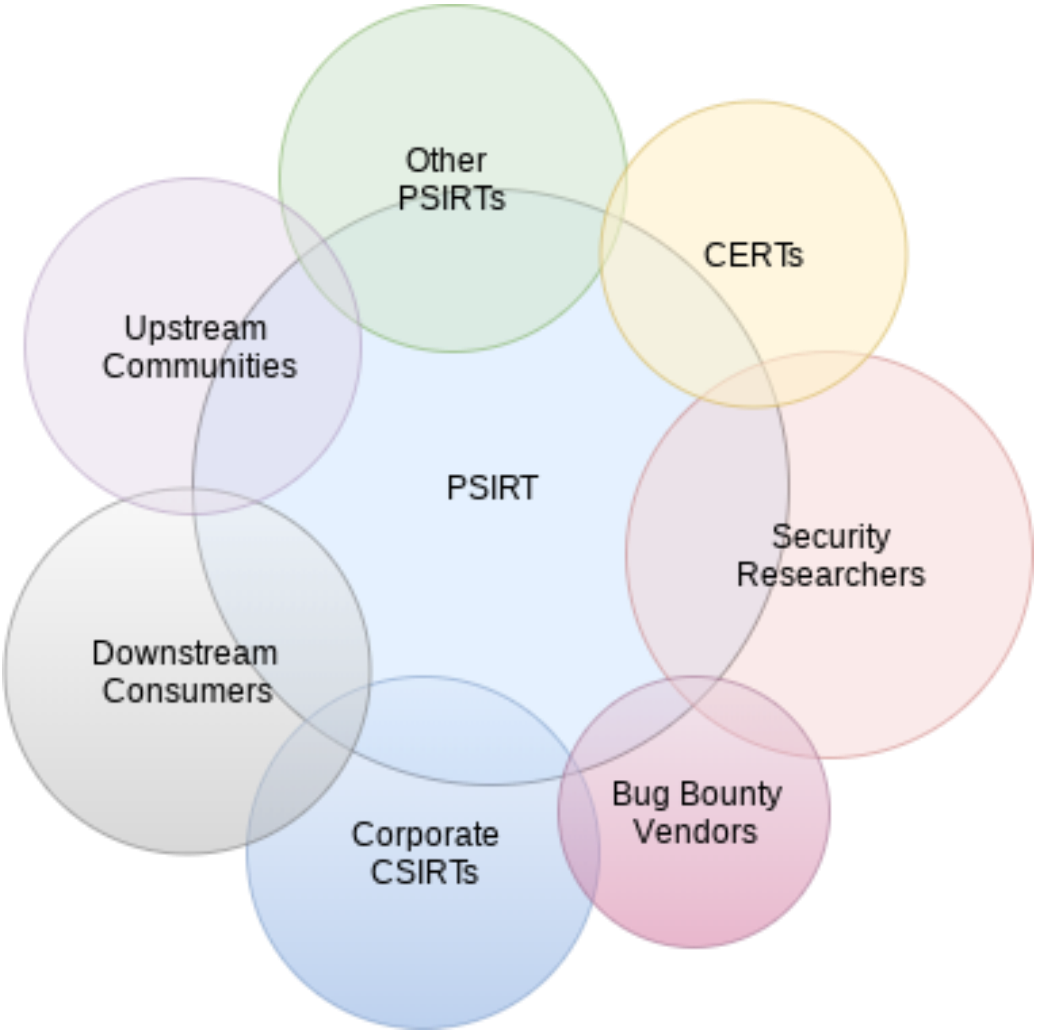


Figure 7: Example of External Stakeholders for the PSIRT

このサービスではステークホルダとしてのリサーチコミュニティとの交流について記載する。発見者には、様々な役割と独自の視点がある。例えば、学者、開発プロフェッショナル、プロフェッショナルなセキュリティ発見者、愛好家などの可能性がある。発見者は、出版や学術成果を期待して理論的な攻撃や欠陥を研究しているかもしれない。また、金銭目的あるいは業務上の目的で活動している専門のセキュリティ発見者である可能性もある。また、趣味の一環として、あるいはコミュニティから尊敬や称賛を得ることを目的として活動している人もいる。発見者コミュニティとの交流は、製品セキュリティインシデント対応における、積極的アプローチである。

> **目的:** 組織の PSIRT が研究コミュニティにも積極的に貢献し、製品セキュリティに影響を及ぼす可能性のある脅威に対する状況認識をしやすい環境を構築する。発見者との否定的または敵対的な関係は、脆弱性に対処する上で、不利益を被る可

能性のある研究の早期通知の機会損失につながり、それによって組織に対するステークホルダの感情に影響を与える可能性がある

成果: コミュニティとの交流が成功すれば、製品のセキュリティを守るために必要な組織の評判と市場の地位が強化される。さらに、発見者との積極的な交流は、組織が公開のための対応を準備する助けとなり、研究および/または脆弱性開示への早期のアクセスに繋がり、組織が情報公開のための対応を準備する助けとなる

機能 1.2.1 発見者との交流

会社の製品に関する専門知識を持ち異なるチャネルにアクセスできる発見者と積極的な対話を維持するための活動を実施する。PSIRT は、発見者コミュニティとより深く関わるために、数多くの活動を行うこともできる。これらの活動には、質の高い発見者と個別の契約を交わしたり、会議やその他のイベントに参加したり、学術研究のスポンサーになったりすることも含まれる。

目的: ソーシャルメディアサイトにプレゼンスを構築する。発見者やステークホルダが問題を見つけた可能性がある指標については、ソーシャルメディアやその他の一般的なサイト/フォーラムを監視する。発見者と会える可能性のあるセキュリティ会議に定期的に出席することを検討する

成果: PSIRT は、コミュニケーションの期待が明確に定義されているため、高い評価を得ている発見者からより高度な警告を含む質の高い報告を頻繁に受け取れる

機能 1.2.2 他の PSIRT との交流

ピア PSIRT 間の関係を育むことは、インシデントの情報共有や潜在的な相互援助、調整に役立つ。これらのピア組織と連携することで、脆弱性を改修するための重要なデータを埋めることができ、2 つのグループが問題を相談する際にピアの専門知識を組織に実質的に組み込むことができる。PSIRT は、鍵となるピア PSIRT との通信チャネル（通常とセキュアの両方）を確立する必要がある。情報の共有や両組織に影響を及ぼす問題の調整には、業界のピアとの関係を確立し育成することが不可欠である。

目的: 脆弱性情報、脅威情報、およびベストプラクティスを共有するために、組織と他の PSIRT との間のコミュニケーションチャネルを確立する

成果: ピア PSIRT のコミュニティは、ソフトウェアサプライチェーンに関連する脆弱性に対応するために有益である。より速い対応が期待できる

サブ機能 1.2.2.1 ピア PSIRT を文書化し定義する

将来の使用のために、連絡先情報とエンゲージメントプロセスを収集する。大規模な PSIRT コミュニティと連携して対話し、教訓を踏まえたベストプラクティスと洞察を共有するべきである。脆弱性が発生した場合、それらはしばしば複数グループによる共同作業により解決される。外部の協力者の情報や支援を得ることにより、PSIRT はその能力を拡げることができる。

サブ機能 1.2.2.2 協調的な開示プロセスを定義する

PSIRT は、脆弱性情報を共有する際の条件や合意事項を注意深く文書化する必要がある。PSIRT は、脆弱性発見者および/または報告組織によって設定された公開条件を尊重するべきである。

サブ機能 1.2.2.3 安全な情報共有プロセスを確立する

PSIRT は、脆弱性およびその他の機密情報を、協調的な開示に関わる当事者と安全に共有する方法を確立すべきである。これは、アウトオブバンド、非電子通信、暗号化された E メール/ポータル、またはプライベートメーリングリストなどのオプションがある。

サブ機能 1.2.2.4 業界 SIG およびワーキンググループに参加する

業界の関心のあるトピックに関する同業者との共同作業は、人脈形成を支援するだけでなく、共同で問題を解決することによって職業の専門化を促進する。

機能 1.2.3 コーディネーター（CSIRT および、その他の調整組織）との交流

政府の CSIRT と協力することで、情報共有の信頼を築き、PSIRT が評価の高い同僚の信頼と尊敬を得るのに役立つ。関連するステークホルダやコミュニティを持つ組織には、FIRST、MITRE、Open Standards for the Information Society （OASIS）、the Industry Consortium for Advancement of Security on the Internet（ICASI）、International Organization for Standardization(ISO) などの業界コンソーシアムなどがある。参加するグループは、国、企業、地域、または産業セクタに基づいて見ることができる。

目的: 組織は未知の脆弱性を使用してネットワークに侵入する攻撃の標的となることがある。早期に潜在的な脆弱性レポートを得るために、CSIRT との信頼関係と連絡手段を確立する

成果: CSIRT、およびその他の調整センター組織との良好な関係は、早期に脆弱性を認識するために重要である。より速い対応が期待できる

サブ機能 1.2.3.1 コミュニティやパートナーと交流する

PSIRT は、目的の外部のグループがどのような場で活動しているかを調査し、それらの場に参加する努力をするべきである。

機能 1.2.4 セキュリティ研究者との交流

セキュリティ研究者は、学問、愛好家、専門のセキュリティ実務家など、様々な人がいる。これらの人物は業界全体の脆弱性の主要な発見者である。研究者は製品のオーナーに連絡しようとするが、様々な理由で適切な当事者に届くとは限らない。PSIRT はこれらの個人または団体からの報告を受動的に受け取り、外部から管理された時間枠での作業を余儀なくされる。PSIRT の製品に影響を及ぼす分野の調査に携わるセキュリティ研究者に積極的なアプローチを行い、発見された問題をよりよく把握するために積極的に取り組むことが PSIRT の最大の関心事である。

サブ機能 1.2.4.1 セキュリティベンダと交流する

大規模なセキュリティベンダは、インシデント発生時にステークホルダと協力して活動し、PSIRT が平時にはアクセスできないフォレンジックデータを持つことがしばしばある。これらのベンダとの関係構築は、信頼と相互尊重の構築に役立ち、PSIRT が他の方法では利用できない可能性のある重要な脅威データへのアクセスを助ける可能性がある。

サブ機能 1.2.4.2 主要なセキュリティベンダとの交流方法の文書化

セキュリティベンダを知り、適切に関与させることで、PSIRT に問題を報告する際に、脆弱性の報告/改修に関するコミュニケーションや取り組みを加速することができる。これらのベンダがアクセスして保持するものを理解することは重要である。バグバウンティベンダとの関係は、関連するすべての関係者が、どのように行動すべきか、どのリソースにアク

セスできるか、どのようにデータを共有するか、そして誰と共有するかを理解するために、関係確立前に完全に文書化され、検証されるべきである。

サブ機能 1.2.4.3 セキュリティベンダと交流する方法の文書化

PSIRT は、目的の外部のグループがどのような場で活動しているかを調査し、それらの場に参加する努力をするべきである。

機能 1.2.5 バグバウンティベンダとの交流

コミュニケーションや脆弱性管理に関するデータ共有の取り組みを支援するために、バグバウンティベンダと関係を構築する。

> **目的:** あなたの組織がバグ発見者に報奨金を支払うベンダ/ブローカから頻繁に脆弱性の報告を受ける場合、Service Level Agreement (SLA)を確立し、その組織と直接的な関係を構築すること検討する
>
> **成果:** バグバウンティベンダとの直接的な関係を構築することにより、製品のセキュリティパッチをリリースするプロセスを連絡するための建設的な対話が可能となる。同意できる SLA 確立に加えて、このような関係は、すべてのステークホルダに有益なゼロデイ脆弱性のリスク低減に役立つ

サブ機能 1.2.5.1 バグバウンティプログラムに関連する定義および文書化

組織が提供する製品に適用されるバグバウンティベンダを定義し、文書化する。

サブ機能 1.2.5.2 バグバウンティベンダと交流する

バグバウンティベンダと活発な対話を行うためのチャネルを特定する。

機能 1.2.6 CSIRT のニーズを予測する

CSIRT は、下流のステークホルダのうち、セキュリティ問題に純粋に焦点を当てた活動を行うグループである。これらのグループとは、通常、標準的なステークホルダとの活動と顧客管理を介して交流が可能であるが、PSIRT は、PSIRT からの情報にアクセスして情報を利用するセキュリティに重点を置くこれらのグループの固有の要求と観点を理解する必要

がある。これには、開示フォーマットとタイムライン（「サービス 5.3 情報開示」を参照）と、特定の要求に対するコミュニケーションチャネルが含まれる。

サービス 1.3 コミュニティと組織の交流

PSIRT が対話する 2 つのステークホルダグループは、さらなる注意を払うに値するだろう。「上流」と「下流」と呼ばれることもあるが、コミュニティへの参加は、脆弱性を協力して改修する活動を育成したり、組織のピアグループ内の他者との相互援助を支援したりするために不可欠である。「上流」は、組織の製品のためのコンポーネントやプロジェクトの調達先となるグループまたは個人に使用される用語である。「下流」とは、組織が提供するアウトプットを、彼らの製品の一部として利用する個人、グループ、または組織を指す。下流ステークホルダとの交流は、以下のサービス 1.4「下流ステークホルダ管理」でカバーされている。

活発な上流のコミュニティは、製品ストリームへのイノベーションの促進に役立ち、複雑な脆弱性改修の負担を軽減し、しばしば組織内で不十分な重大な専門知識の欠如を補完することができる。同様に、他の組織の個人やチームとのプロフェッショナルな関係を築くことは、外部の視点、専門知識、歴史的知識へのアクセスを可能にすることによって、PSIRT の機能を拡張するのに役立つ。これは、セキュリティコミュニティをステークホルダとして積極的に関与させ、パートナーや同業者の PSIRT との関係を確立することで達成できる。

> **目的:** PSIRT は、パートナーや仲間との活発なエコシステムを構築し、維持する必要がある。これらのコミュニティとの関係は、欠陥を発見し修復するための「多くの目」のアプローチを支援するだけでなく、脆弱性修復の全体的な経験を改善するために、異なるグループ間のグッドプラクティスを共有する助けにもなる
>
> **成果:** パートナーや仲間との良好な関係や活発なエコシステムは、脅威情報とベストプラクティスの情報共有を促進する。セキュリティコミュニティで高い評価を得ている PSIRT は、重要な状況に対処するためのリソースとコラボレーションを引き寄せやすくなりうる

機能 1.3.1 上流コミュニティとパートナーの定義と交流

多くの場合、製品には、組織によって作成されていないコードやコンポーネントが含まれる。これらの素材の作成者は、サードパーティ、サプライヤ、上流のベンダ、original equipment

manufacturers(OEM)、または単にパートナーと呼ばれることがある。エコシステム内のこれらのパートナーを特定し、サードパーティのコードで脆弱性が発見された場合に、組織がどのように連絡して取り組むかを判断することは有用である。

> **目的:** 組織がコンポーネントを受け取る提供元の個人またはグループ、または組織からコンポーネントを受け取るグループと協調して活動する関係を確立する。PSIRT がそれらのステークホルダに対してどのように連絡するか、誰に連絡するのかを理解することは、PSIRT に問題が寄せられる状態を維持できるばかりではなく、PSIRT がその問題から派生する他のコンポーネントへの影響を見つけた際に誰に連絡する必要があるかを理解することになる
>
> **成果:** PSIRT は、コンポーネントが誰からおよび、どこから供給されているのかをよく理解する。これによりコンポーネントに欠陥が発見された場合、情報や修正プログラムにすばやくアクセスできる

サブ機能 1.3.1.1 上流のコミュニティとパートナーを定義し、文書化する

上流のコミュニティおよびパートナーは、組織の提供製品に組み込まれているコード、知識、および知見を提供している。PSIRT がセキュリティ脆弱性の報告を受け処理するときに、これらのサプライヤとの間で迅速かつ効果的なやりとりを行うことが重要である。こうした協力関係は非開示契約やその他の保護契約のなかで文書化されていることが理想的である。

サブ機能 1.3.1.2 コミュニティやパートナーと交流する

各上流コミュニティまたはパートナーは、ソフトウェア/製品の開発とコミュニケーションに使用する方法やツールが異なる場合がある。PSIRT は、これらの外部グループとの連携方法を理解し、PSIRT がセキュリティ問題に関して外部の協力者と協力するための適切な連絡先/方法を持つことを確実にする必要がある。

サブ機能 1.3.1.3 上流のコミュニティに参加する

上流のコミュニティやパートナーに参加することで、グループ間で貴重な信頼関係を築くことができるばかりでなく、組織の専門知識を活用して外部チームの能力を強化することもできる。

サブ機能 1.3.1.4 コミュニティや産業イベントに参加する

カンファレンスや専門組織の会議は、PSIRT がステークホルダやパートナーと対話し、組織へのフィードバックを直接得るための絶好の機会であるばかりでなく、将来の調整や、コラボレーションのために活用できる外部コミュニティの肯定的評価を得るのに最適である。

サブ機能 1.3.1.5 コミュニティのセキュリティチームと交流する

PSIRT は、上流のソフトウェア/ハードウェア/サービスプロバイダーのセキュリティチーム（PSIRT、CSIRT、セキュリティエンジニア）にどのように、また、誰に連絡するかを理解することが重要である。PSIRT とこれらのグループ間でコミュニケーションと信頼関係を確立することは、組織の危機や脆弱性の改修時の円滑なやりとりを確実にするのに役立つ。

機能 1.3.2 下流のコミュニティとパートナーの定義と交流

「下流」には多くの意味があるが、PSIRT がこれらの重要なステークホルダグループを無視すべきではない。「下流」とは、PSIRT の会社の製品を使用して、自社の目的に使用する製品、組織、個人を指す。多くの場合、提供される商品やサービスの顧客または消費者の形を取る。別の企業が PSIRT の会社の製品を使用またはライセンスし、製品として再販することも多い。また、一般的にオープンソースソフトウェアの場合、あるグループがソフトウェアを提供・メンテナンスし、これらのリソースを活用する多数のグループが存在する。

サブ機能 1.3.2.1 下流のコミュニティ、消費者、パートナーの定義と文書化

下流のコミュニティおよびパートナーは、組織の提供製品に組み込まれているコード、知識、および知見を利用している。理想的には、これらの関係は契約書に文書化され、NDA やその他の組織のための保護の対象となる。

サブ機能 1.3.2.2 下流のコミュニティとの交流

各下流のコミュニティまたはパートナーは、ソフトウェア/製品に関する開発と通信に使用する様々な方法やツールを持っている。PSIRT は、これらの外部グループとどのように交流するかを理解し、それらの外部当事者が関係するセキュリティ問題に関して協力するための適切な連絡先/方法を確保する必要がある。

サービス 1.4 下流のステークホルダマネジメント

ステークホルダとの関わり方について、PSIRT は製品セキュリティレスポンスを中心にステークホルダコミュニティと対話するためのプロセスと方法を確立する必要がある。組織の現在および将来の収益機会増加のため、ステークホルダに満足してもらうことは重要なことのひとつである。

> **目的:** PSIRT は、製品のセキュリティ脆弱性に関する情報やインシデント対応の情報を伝達するために、組織のステークホルダ基盤とのチャネルを構築し、維持する必要がある
>
> **成果:** ステークホルダとの良好な関係を築くことは、収益を確かなものとする（または場合によっては増加させる）だけでなく、ステークホルダに製品への意見を提供し、課題解決への関与と一体感を醸成する

機能 1.4.1 下流のステークホルダとの交流

あなたの製品やサービスのステークホルダは、情報や意見を共有し、組織がセキュリティ上の脆弱性をどのように処理するかについてのサポートを得る手段が必要である。組織のステークホルダと積極的に協働することは、ポジティブなブランド体験を提供し、ステークホルダロイヤリティを維持/向上させるのに役立つ。

> **目的:** 下流ステークホルダに PSIRT とのコミュニケーションを行う方法や、セキュリティ問題のサポートを受ける方法を提供する。ステークホルダの問い合わせや要求に適切に反応しなければ、否定的なコメントがよせられた結果ブランドに悪影響がおよび、契約が更新されなかったり、新しいビジネス機会を失ったりする可能性がある
>
> **成果:** 下流ステークホルダは、セキュリティ上の欠陥に関する迅速かつ明確なガイダンスを受けるべきである。これにより、製品の信頼水準が向上し、ブランドロイヤリティが向上する。下流ステークホルダは PSIRT の助けを借りて積極的な経験を積み、ステークホルダとの PSIRT 専門知識を確立する必要がある。これにより一般的には、ステークホルダのブランド全体の視点を改善する

サブ機能 1.4.1.1 明確なライフサイクルとサポートポリシーを提供する

ステークホルダがセキュリティ脆弱性の改修や製品のサポート期間に関して何を期待しているか、組織は明確かつ公的に記述する必要がある。詳細については、サービスエリア 4 を参照すること。

サブ機能 1.4.1.2 ステークホルダとの交流

組織の製品やサービスのステークホルダは、報告されたセキュリティ上の欠陥について質問をしたり、援助を必要としたり、是正処置を必要とする。PSIRT は、ステークホルダの要求に積極的に関与し、セキュリティ脆弱性に関する明確かつ正確なガイダンスを提供し、修正版がステークホルダに提供されるまでリスクの軽減策を提供する必要がある。

サービス 1.5 組織内でのインシデントに関するコミュニケーションの調整

セキュリティインシデントは、組織内の多くの社内グループや製品に影響を及ぼす可能性がある。PSIRT は、脆弱性対策に関する調整をするとともに、インシデントに関する情報を許可された内部関係者に共有するためのハブとして機能する中心的な存在である。

> **目的:** ビジネス内のすべての関係者が、セキュリティ脆弱性の対応状況に関する情報を知っていることを確認し、次のステップを妥当に判断できるようにする。コミュニケーションは様々な形（E メール、伝統的なメール、RSS フィード、ソーシャルメディアなど）で取ることができるが、最終的にはすべての情報提供が、ステークホルダが懸念する脆弱性・インシデントの情報を明確かつタイムリーかつ正確に提供する
>
> **成果:** 内部ステークホルダは、組織の提供物に対する脅威の範囲と影響を知ることになる。ステークホルダには、セキュリティ上の脆弱性が改修されたとき、軽減策が利用可能になったときに、適切な次のステップを実行できるように情報を提供する必要がある

機能 1.5.1 通信チャネル/情報提供方法を提供する

ステークホルダと効果的に関わるために、PSIRT は様々なコミュニケーションチャネルを提供しなければならない。ステークホルダごとに異なる情報の提供方法を望んでいる可能

性がある。PSIRT は、情報がリリースされるときに、できるだけ多くの関係者が閲覧できるよう考慮する必要がある。また、様々な情報源からのレポート、コメント、および質問の収集ができるようにしておくべきである。

> **目的:** ステークホルダに PSIRT とのコミュニケーションを可能にする方法を提供する
>
> **成果:** E メール、チャット、ウェブフォームやそれ以外のチャネルを用いることで、社内のステークホルダが PSIRT と情報を共有できるようになる

サブ機能 1.5.1.1 明確なコミュニケーションチャネルを提供する

ステークホルダには、PSIRT に対して、質問を提出し、不具合のステータスを確認し、問題を報告する手段が必要である。ステークホルダがセキュリティ上の脆弱性の影響を受けるか、またはセキュリティ上の脆弱性を発見した場合、PSIRT にレポートを作成して送信することが容易になる。

サブ機能 1.5.1.2 内部コミュニケーションチャネルを提供する

PSIRT は、内部のステークホルダとの関係を保つために、脆弱性の改修状況を告知するためのコミュニケーションチャネルを提供する必要がある。内部のステークホルダは、PSIRT に簡単にコンタクトを取ることができ、問い合わせにより何が期待できるかを理解できるべきである。

サブ機能 1.5.1.3 外部コミュニケーションチャネルを提供する

PSIRT は脆弱性の修復状況を外部のステークホルダと共有するために、コミュニケーションチャネルを提供する必要がある。また、社外のコミュニケーションの有用性およびそれらが適切に内部関係者に伝えられることを確認するために、外部とのコミュニケーションに関する活動を検証・評価することも必要である。

機能 1.5.2 安全なコミュニケーションの管理

多くの場合、PSIRT は秘密とみなされる（すなわち、公開が制限されている。）情報を処理する必要がある。PSIRT は、発見者、他の組織、または様々な内部リソースと安全かつ秘密裏にコミュニケーションできる必要がある。開示契約を遵守し、非公開でコミュニケーシ

ョンすることは、発見者からの信頼を築くのに役立つ。権限のない当事者から秘密の脆弱性情報を保護することも、公開制限の条項に従って、問題を適切かつ効果的に管理するのに役立つ。安全なチャネルは、公開されたくない発見者の正体を保護するのにも役立つ。データの使用が終了した後、データが適切に処分されるようにするための保持方針を確立する必要がある。

> **目的:** 当事者がセキュリティ脆弱性に関する情報を秘密裏にやりとりするための機能を提供する。これらのチャネルは、セキュリティ脆弱性と発見者の秘匿性を、それらが公開可能になるまでの間保護する
>
> **成果:** セキュリティ問題のサポートに関与する当事者は、その情報を知る必要がある他の関係者と秘密裡に情報を共有することができる。発見者は、彼らの懸念が組織によって守られると感じた場合、再度レポートをその組織に送ってくる可能性が高くなる

サブ機能 1.5.2.1 安全なコミュニケーションチャネルを提供する

PSIRT は、組織に影響を与える脆弱性に関わる発見者およびパートナーが情報共有できるようにするためのプライベートで安全な方法を持つようにする必要がある。

機能 1.5.3 脆弱性をトラッキングするシステムのアップデート

PSIRT は、すべての製品の脆弱性に関する記録システムにアクセスでき、トラッキングと情報共有のためのシステムを構築・使用できる必要がある。

> **目的:** セキュリティ上の欠陥を適切に記録して追跡することで、脆弱性がいつどこで対処されたかを組織が把握することができる。このシステムは、PSIRT、発見者、および問題解決に積極的に取り組むエンジニア間のコミュニケーションも可能にする
>
> **成果:** システムを使用してセキュリティ上の脆弱性が適切にトラッキングされるため、欠陥に関する情報にアクセスする必要があるすべての関係者が、履歴、進捗状況、およびコメントを確認できる

サブ機能 1.5.3.1 製品のセキュリティ上の欠陥のトラッキングを提供する

セキュリティ上の欠陥を追跡する必要がある。これらのシステムは、進捗状況を更新および追跡するために、内部および外部の関係者（該当する場合）により（最低特権モデルで）アクセス可能である必要がある。外部の発見者は、PSIRT に提出した報告書のステータスに関する適切なコミュニケーションを受ける必要がある。

サブ機能 1.5.3.2 セキュリティ上の欠陥のトラッキングプロセスを作成し、公開する

PSIRT は、組織の提供に影響を与える脆弱性に取り組んでいる脆弱性発見者およびパートナーが、情報を共有するためのプライベートで安全な方法を確保する必要がある。

機能 1.5.4 情報の共有および公開

問題が解決された後、PSIRT は、修正版が利用可能になるまで、何がセキュリティ上の脆弱性なのか、その重大度と影響の情報、悪用される可能性のあるリスク、修正の方法もしくは修正が利用可能になるまでの緩和策などについての情報を利用可能にするべきである。

> **目的:** 報告され、改修された脆弱性に関する詳細を共有する。ステークホルダは、正式な修正が提供されるまで、リスクを抑えるための回避策または代替的な緩和策を受けることができるべきである
>
> **成果:** ステークホルダに、脆弱性、その影響、修正方法が通知される。タイムリーな情報と更新情報を受け取ったステークホルダは、組織をポジティブに評価し、提供されている製品を使用し続け、将来の使用を拡大する可能性が高くなる

サブ機能 1.5.4.1 複数のコミュニケーション窓口を提供する

異なるステークホルダは、脆弱性が一般に公開される際に、様々な相互作用/通信方法を好む。PSIRT は、伝統的なアドバイザリスタイルの更新に加えて、脆弱性に関するステークホルダの関与と意識を最大限に引き出すために、他の方法を使用するようにする必要がある。脆弱性が改修された後、PSIRT は修正を告知するために複数の異なる方法を使用する必要がある

サブ機能 1.5.4.2 ステークホルダにフィードバックを提供する

フィードバックは、今後のプロセスと対応を改善するのに役立つ。PSIRT が強みとする分野を強調することができ、PSIRT がさらに発展し改善する必要がある分野での実績を継続

する必要がある。

サービス 1.6 表彰と謝辞による報酬を発見者に与える

発見者への謝辞をとおして脆弱性に関する PSIRT とのパートナーシップに対する感謝の意を表すことによって、発見者がコミュニティ内で信頼を得ることに役立つ。

> **目的:** 脆弱性の公開にむけた調整への発見者の貢献に対して謝辞を示す。これらの謝辞によって発見者は自らの専門性に関するポートフォリオを作成することができ、それにより自身の市場評価を高めることができる
>
> **成果:** 発見者と積極的に協力することで、製品のセキュリティが向上する。発見者を信認することは、内部の従業員への評判を高め、専門知識を示すうえで有益である

機能 1.6.1 謝辞の提供

脆弱性の発見をした人への謝辞は、脆弱性対応フローの中で重要な要素である。感謝の気持ちが少しでも表れれば、コミュニティ内の信頼と尊敬が得られ、組織はセキュリティ上の懸念に対応していることがわかる。

> **目的:** 製品の脆弱性の公開について責任を持って調整する努力により、発見者は信認される。発見者はこれらの謝辞に基づいて、彼らの評判を高めることができ、専門性の高いポートフォリオを構築することができる
>
> **成果:** 発見者との積極的な協力により、製品のセキュリティが向上する。発見者への謝辞は、発見者が評判を築くのに有益であり、発見者が将来の脆弱性レポートを PSIRT に送ることを奨励する

サブ機能 1.6.1.1 謝辞の提供

発見者の脆弱性の発見への取り組みと関与への謝辞は、PSIRT がこれらの個人に報酬を与える最も効果的で安価なツールである。セキュリティアドバイザリ、ソフトウェアリリースノートおよび CVE 情報に発見者への謝辞を含めることは一般的である。PSIRT は、見つかった脆弱性の社内での評価をどのように発見者に伝達するのかを理解する必要がある。

機能 1.6.2 発見者への報奨

PSIRT は報奨制度を作り拡大させることにより、ステークホルダに良い成果をもたらし、さらなる知見の共有を促すことができる。

> **目的:** 組織の製品やサービスの脆弱性を報告した人に報酬を与える。報酬は、電子/物理的な感謝状、販促品（グッズ）、金銭や金券、その他多くの形を取りうる。PSIRT は報酬に関する規則を定め、透明性をもって運用しなければならない
>
> **成果:** この活動は、PSIRT 組織にとって善意を喚起し、今後のセキュリティ問題に関する継続的な協力を奨励する

サブ機能 1.6.2.1 発見者への報奨プログラムを作る

脆弱性の発見者が PSIRT に対して好意的となるような、謝辞以上の価値を感じられる報酬プログラムを提供する。報酬は、金銭や金券、販促品などが考えられる。

サブ機能 1.6.2.2 脆弱性報奨金制度を開始する

報酬の 1 つの形式として、金銭的報酬がある。いくつかの組織は、脆弱性情報を彼らに開示する発見者に対し報酬を支払う。

サブ機能 1.6.2.3 ポイント制度を開始する

報酬の別の形態は「ポイント制度」である。これにより、脆弱性を発見して報告するリーダーを促進し、発見者が自慢するためのランキングを提供することによって、友好的な競争を促進する。

サービス 1.7 ステークホルダメトリクス

PSIRT の有効性をステークホルダに認識させるためには、PSIRT の規模や成果、その他の活動指標に関する詳細な情報を提供することが重要である。ステークホルダはそれぞれ視点が異なるため、それぞれに応じた内容やフォーマットの成果物を提供する必要がある。PSIRT は、各ステークホルダがこの情報をどのように利用したいかを理解しなければなら

ない。これらの情報は PSIRT の重要業績評価指標(KPI)になりうる。

> **目的:** PSIRT の活動指標と成果に関するデータを提供する。これは、PSIRT がどれくらい効果的にサービスを提供しているかをステークホルダが理解するのに役立つ
>
> **成果:** PSIRT メトリクスをレビューすることにより、ステークホルダは、PSIRT がサービスをどの程度効果的に提供しているかを知り、そのサービス提供を調整するためのフィードバックを提供することができる

機能 1.7.1 ステークホルダの要件を理解する

PSIRT がどのようにサービスを提供しているかを効果的に表現するための第一歩は、各ステークホルダの独自の視点を理解することである。セキュリティパッチ提供の適時性について関心を持つステークホルダもいれば、PSIRT 運用の財務的側面に重点を置くステークホルダもいる。それぞれの視点は妥当なものであり、それぞれのステークホルダが求める情報を効果的に伝達するためには、それぞれに異なる報告書を提供する必要がある。PSIRT は、どのようなやり方で情報を共有すべきか、各ステークホルダから意見を引き出す必要がある。

> **目的:** PSIRT の運営およびサービスに関してステークホルダが気にかけていることを理解する。これらの要件が収集され合意された後には、アップデートの配信方法/メディアおよび配信頻度を決定する必要がある
>
> **成果:** PSIRT を維持するために必要なステークホルダへの報告書（レポート/ビュー/ダッシュボード）要件のリストが文書化される

サブ機能 1.7.1.1 ステークホルダのメトリクス要件を収集する

ステークホルダは、他のステークホルダが関心を寄せない特定のデータセットに関心を持つことがある。例えば、このような測定基準は、拡張パッチ修復チームのパフォーマンス、コスト、および品質に関連する可能性がある。

機能 1.7.2 ステークホルダのメトリクスを収集する

すべてのステークホルダグループが要求するメトリクスを文書化することが必要なプロセ

スとアクションである。可能な限り、PSIRT が使用するツールは、PSIRT のプロセスとパフォーマンスに関する情報を収集して提供できる必要がある。理想的には、経緯的なパフォーマンスを定期的に見直すことができるように、また異なるステークホルダの意見を最小限の労力で容易に解決できるように、メトリクスは集中管理された場所（データベース、スプレッドシート、またはその他のツール）に格納する必要がある。

> **目的:** PSIRT のパフォーマンスの規模に関するステークホルダの要求を満たすために必要なデータを収集、生成、集計する。この情報は、履歴的な見直しとステークホルダによる再利用できるように一元的に保存されるべきである（すなわち、2つ以上のステークホルダグループが同じ情報を閲覧したいと考えている）
>
> **成果:** 報告書（レポート、ビュー、ダッシュボードなど）の作成のために、必要なステークホルダメトリックが収集される

サブ機能 1.7.2.1 ステークホルダのメトリクスを収集する

PSIRT は、所定の間隔（SLA / OLA）で必要なメトリックを収集するプロセスとメソッドを作成する必要がある。

サブ機能 1.7.2.2 ステークホルダのメトリクスの保管

PSIRT は、成果やその他の傾向に関するデータの履歴を分析する必要がある。そのためには、データのリポジトリを開発し継続的に利用できるようにおくとよい。

機能 1.7.3 ステークホルダのメトリクスの分析

文脈のないデータは無意味である。文脈がなければ、誤った仮定が導かれ、その結果ビジネスまたはステークホルダの要求の変化に追従するための PSIRT 活動の調整が行われない可能性がある。PSIRT が必要なデータを収集したら、そのデータを確認し、そのデータがステークホルダにとって何を意味するかという文脈を提供するべきである。

> **目的:** 収集されたデータの意味を理解し、その情報を解釈するための文脈をステークホルダに提供する。理想的には、ステークホルダは、特定の重要評価指標（KPI）がどのように遷移しているか、報告対象の期間中にどのような要因が KPI に影響を与えたか、その KPI の傾向を把握できるようにすべきである

成果: 過去のデータを保持し、現在のパフォーマンスと比較して傾向を特定する

サブ機能 1.7.3.1 メトリクスデータの分析と見直し

PSIRT は、収集されたデータをレビューし、メトリックレポートとともに文脈を提供するための時間と努力を費やす必要がある。

サブ機能 1.7.3.2 データの傾向と過去のパフォーマンスを分析する

過去のデータが収集されると、PSIRT またはそのパートナーが対応できる独自の傾向または慢性的な問題が特定される可能性がある。

サブ機能 1.7.3.3 データの文脈を提供する

ステークホルダが、彼らに提供されたものを適切に理解し、質問や懸案に対処する可能性を提供できるように、データに文脈を提供する。

機能 1.7.4 ステークホルダメトリクスの報告書を提供する

メトリクスデータが収集され分析された後、合意された形式で関係者に提供されなければならない。このフォーマットは、報告書、またはステークホルダの視点に対処するためのビューと呼ばれることがある。これらの成果物は、ウェブページ、E メール、より公式なレポート、または他の方法の形を取ることができる。

目的: ステークホルダには、サービスを提供する際の PSIRT のパフォーマンスに関する洞察と理解を提供するために、彼らが利用可能な形式でメトリクスデータを提供する必要がある。このデータは理解できるものでなければならず、ステークホルダがその業績に基づいて意思決定を行うための十分な文脈を持つべきである

成果: 合意された時間枠で適切な形式でステークホルダにメトリクスが提供される

サブ機能 1.7.4.1 ステークホルダにメトリクスの報告書を提供する

それぞれのステークホルダは、独自の視点を持っている。各視点は、いくつかの報告書の形でデータのビューで対処される必要がある。これらの報告書は、異なる視点に合わせるため

に調整する必要がある。報告書の提供方法には、E メールでの送信、またはウェブページへのポスト、ダイナミックウェブポータル、エグゼクティブブリーフ、チャート、グラフ、または他の多くのデータ配信メカニズムが含まれ得る。

サブ機能 1.7.4.2 メトリクスを見直し、教訓から学ぶ

PSIRT の最も重要な目標の 1 つは、脆弱性管理のプロセスを絶えず改善することである。パフォーマンスメトリクスとステークホルダのフィードバックを確認することで、PSIRT は特定の領域に焦点を当てたり、改善したりすることができる。

サービスエリア 2

このサービスエリアでは PSIRT による潜在的な脆弱性の発見に関する機能とサービスについて記述する。このサービスエリアでのオペレーションは、本ドキュメント中の他のセクションで記述される脆弱性情報ハンドリングのプロセスのトリガーとなる。このサービスエリアで規定されるサービスの可用性と効率性を介して、PSIRT の成熟度を測定することができる。

目的: 製品の脆弱性、脆弱なサードパーティ製品、アーキテクチャ上の弱点について、様々な情報源から情報収集するプロセスとメカニズムを確立する

成果: ステークホルダによるアクションが必要な報告や潜在的な脆弱性についての状況認識を促進する

サービス 2.1 脆弱性報告の受付

PSIRT にとっての主要なシナリオは、ステークホルダの製品に影響する報告の受付である。脆弱性報告の受付において鍵となる要素は、必要な組織構造の設置と維持、コンタクトポイントの定義と宣伝、情報を受けられる体制を定義し維持することである。

目的: ステークホルダの製品に関する脆弱性情報の報告者にとって報告しやすいプロセスとメカニズムを確立し、脆弱性報告への備えを維持する

成果: PSIRT が脆弱性報告の受付に特化した機能を備える

機能 2.1.1 到達性を確保する

PSIRT はその存在についての認知を確立し、外部組織や組織内のエスカレーションパスから常に利用可能でなければならない。明確に定義されたコミュニケーションチャネルは、発見者、パートナー、ステークホルダが PSIRT に脆弱性を報告する際の助けとなる。

目的: 脆弱性を報告しようとする者が、必要なコンタクト先と提出方法についての情報を容易に見つけることを可能にする

成果: 多数のレポートが提出された際に、PSIRT が脆弱性情報を受理できないというクレームが起こらないようにする

サブ機能 2.1.1.1 報告の提出様式を定義する

様々なチャネルから品質がバラバラな脆弱性情報が来ることが予想される。報告を処理する最善の方法を定義することが有用である。これにはウェブフォームや、公開のチケットシステム、E メールアドレス、サポートホットライン、その他の提出方法が考えられる。

サブ機能 2.1.1.2 コンタクト情報の詳細を公開する

PSIRT にとって望ましいコンタクト情報は、製品マニュアルに記述され、企業のウェブサイトで周知され、検索エンジンに登録されるべきである。また、主要な CSIRT/PSIRT のリストに登録され、CVE 発行組織（CNA）と連携しセキュリティコミュニティに周知されるべきである。

サブ機能 2.1.1.3 一般的なコンタクトポイントを登録する

PSIRT に関連する一般的な単語（psirt@、incidents@、security@ 等）を企業のドメイン名の下に確保することは、PSIRT に対する直接の連絡を受け易くするという点で役に立つ。

サブ機能 2.1.1.4 PSIRT を組織内の各部署と連携させる

ステークホルダ向けのサービス部門（ステークホルダからの要請への対応、脆弱性報告）、コミュニケーション部門（メディア対応）、製品開発部門（組織内での重要な発見のエスカレーション）に対し、PSIRT の活動とコンタクト方法についての理解を確実にする。

サブ機能 2.1.1.5 情報を受けられる体制を定義し維持する

業界またはステークホルダによって要求される要請に応じて、電話対応体制や 24 時間対応体制を敷き、重要な報告に対応するための必要な体制を維持する。

サブ機能 2.1.1.6 報告の暗号化に対応する

脆弱性報告には脆弱性が発見された製品と運用環境についての機微な情報が含まれることが多い。偶発的な情報漏洩や公開を防ぐため、S/MIME や PGP で暗号化した E メール、HTTPS を利用できるウェブフォーム等の、暗号化が可能な環境を使った報告を推奨する手段を提供すべきである。

機能 2.1.2 脆弱性報告の取り扱い

脆弱性報告は様々なソースから様々な様式で報告される。外部とのコミュニケーションチャネルを常に監視し、報告に対しタイムリーに対応することは極めて重要である。外部の発見者へのレスポンスタイムは組織内で SLA を定義するべきである。

> **目的:** ベンダ企業内の他部署、ステークホルダ、サードパーティ（発見者、他組織の PSIRT や CSIRT 等）からの脆弱性報告を受け付けるプロセスとメカニズムを提供する
>
> **成果:** サードパーティからの脆弱性報告を取り扱う専門機能

サブ機能 2.1.2.1 コミュニケーションチャネルの監視

PSIRT へのコンタクト手段として公開されている連絡手段と、他に使用可能なチャネル（一般的な E メール受信ボックスや、企業のソーシャルメディアアカウント）を常に監視する。

サブ機能 2.1.2.2 報告を独立して取り扱う

PSIRT は、脆弱性報告を検証する必要があるため、不正な報告を用いた攻撃の標的にされやすい。脆弱性報告を安全に処理する手段を提供することによって、業務環境をそうした攻撃から守るためのポリシーと技術的な手段を用意する。

サブ機能 2.1.2.3 報告者への受理連絡をタイムリーに行う

報告内容の詳細分析は複雑で時間がかかることが多い。しかし単なる報告受理連絡はすぐに実施できる。迅速な対応は、報告が真剣に取り扱われていることを示し、信頼関係を構築する助けとなる。この最初の連携が、その後の取り扱いプロセスにおけるコミュニケーションの基礎となり、また PSIRT が包括的な解決に取り組むことを示すものとなる。

サービス 2.2 報告されない脆弱性を特定する

製品開発者に直接開示された脆弱性情報、または第三者の報告機関から受け取った脆弱性情報は、そのまま処理される。しかしながら、報道機関、技術ブログ、専門のデータベース、ソーシャルメディア、技術刊行物やカンファレンス等の非公式のチャネルを介して開示される脆弱性情報があることを理解することは重要である。

> **目的:** 状況認識を維持し、ステークホルダの製品に影響する脅威を発見するための時間を減らし、フルディスクロージャの可能性を減らす
>
> **成果:** ステークホルダの製品ポートフォリオに対するセキュリティ上の脅威に関する状況認識の促進

機能 2.2.1 攻撃情報データベースを監視する

公開されている攻撃情報データベースや有料のフィードを監視し、調査が必要なゼロデイ脆弱性を発見する。完全に動作する攻撃を発見したときは、企業のステークホルダとの能動的なコミュニケーションを行う。

> **目的:** 公式のチャネルからは決して報告されない脆弱性を発見する
>
> **成果:** 市場に流通する、機能する攻撃の存在についての知識を拡大する

機能 2.2.2 カンファレンスプログラムをチェックする

セキュリティに関するカンファレンスを複数チェックし、関心のある分野に関する投稿を見つける。特定の製品や製品ブランドに関する投稿だけではなく、プロトコルの欠陥などの広範なトピックにも目を向けるべきである。PSIRT はそれらについても対応を求められる可能性がある。もしアブストラクトを見て質問すべき点を見つけた場合は、発見者と早期にコンタクトして何かアクションすべきことがないか明確にしておくと良い。さらに、カンファレンスに参加している発表者と能動的に連携しておけば、将来的に彼らの研究の中で見つかったことが PSIRT に直接連絡されることにもつながる。

> **目的:** 調整されない状態で情報公開されることを避け、さらに発見者が考慮していないステークホルダの製品への直接・間接的な影響を及ぼし得る欠陥を特定する
>
> **成果:** 公開前に発表者へ積極的にアプローチする機会を持つことにより、ステークホルダの製品への影響の有無または報告の投稿により問題が生じるかどうかを明らかにする

機能 2.2.3 高名な発見者による公開情報をチェックする

関連分野の第一人者により公開される情報や、業界あるいは特に企業の製品やサービスについての高い専門知識を持つ専門家による情報に注意を払う。彼らの科学的な研究、ブログ投稿、メーリングリストでの投稿は、注意が必要な脆弱性や弱点についてのヒントを与える。

> **目的:** ステークホルダに関係するセキュリティ上のトピックに関する科学的・技術的知識についての状況認識を維持する
>
> **成果:** 一般的な脅威、弱点、考えられる対抗策についての専門知識を得てステークホルダの製品のセキュリティ問題の解決を支援する

機能 2.2.4 マスメディアによる情報をチェックする

特に、ステークホルダの設備や人員に致命的なインシデントが発生した場合、マスメディアがまず取り上げることが多い。マスメディアの監視は、PSIRT のステークホルダが重要あるいは大口のサプライヤである場合に状況を発見するのに役立つ。

目的: 製品の脆弱性がインシデントの発生に寄与したことに反論する

成果: インシデントの原因となっていたかもしれない製品の脆弱性について、ステークホルダやメディアによる問い合わせへの対応準備の促進

サービス 2.3 製品コンポーネントの脆弱性のモニタリング

脆弱性は大雑把に次の 3 つに分類される。(1)製品固有のソースコード内の脆弱性、(2)製品開発者の組織内リソースによってメンテナンスされるコンポーネントの脆弱性、(3)製品開発者の外部リソース（サードパーティ）によってメンテナンスされるコンポーネントの脆弱性。製品の観点では、(2)と(3)は外部コンポーネントであるが、これらのコンポーネントの脆弱性は最終製品に影響を与える可能性がある。製品のオーナーは根本的な問題への対策を間接的に制御するだけであるが、ステークホルダは脆弱性の影響を受ける製品の修正に関するオーナーシップをサプライチェーン全体が何らかの形で担うと考える。これは製品に含まれる脆弱性のあるコンポーネントを、単体で修正することができない場合に当てはまる。製品に含まれるオープンソースコンポーネントはサードパーティ製コンポーネントであるとみなされる。

目的: ステークホルダの製品のサプライチェーン内の脆弱性を特定、収集、監視し、製品チームに対し、製品に影響する脆弱性を通知する

成果: サプライチェーンから継承され、ステークホルダの製品に影響を与える脆弱性を早期特定するための深い洞察

機能 2.3.1 製品コンポーネントの目録

製品に含まれるコンポーネントのベンダ名、製品名、バージョンを組織内外から集めリスト化する。これは継承された脆弱性の影響を受ける製品を迅速に特定するために不可欠である。

目的: その製品自体の脆弱性に繋がる可能性のある脆弱なコンポーネントを含む製品を特定する

成果: 脆弱な製品コンポーネントを探すための、すべての製品の材料の完全なリスト

機能 2.3.2 サードパーティのアドバイザリのモニタリング

ベンダのアドバイザリの購読やサプライヤとの特定のコミュニケーションチャネルの確立により、サードパーティ製コンポーネントの脆弱性情報をタイムリーに入手する。オープンソースプロジェクトのセキュリティメーリングリストに登録する。これは脆弱性情報のプロバイダを使うことによりサポートされる。

> **目的:** ステークホルダの製品の脆弱性に繋がるサードパーティ製コンポーネントの脆弱性を特定する
>
> **成果:** 脆弱性の影響を受ける製品についての外部のレポートが出る前にハンドリングプロセスを開始できる可能性

機能 2.3.3 脆弱性に関するインテリジェンスソースのモニタリング

サードパーティ製コンポーネントのベンダのアドバイザリを購読することが常に可能であるとは限らない。これは、ベンダがアドバイザリを発行しない、ベンダが事業を終了した、コンポーネントを開発するオープンソースプロジェクトが積極的に活動していない等の場合に起こる。NVD のような情報源や商用のインテリジェンス情報源はアドバイザリの出ていない脆弱性の特定に役立つ可能性がある。

> **目的:** アドバイザリが出されていないサードパーティ製コンポーネントの脆弱性を特定する
>
> **成果:** 気づかなかった脆弱性に対するより深い洞察

機能 2.3.4 ベンダ組織内のサプライチェーンの脆弱性情報の受付手順を確立する

ベンダ組織内リソース由来の製品コンポーネントは、ほとんどの場合、解決されたセキュリティ上の問題に関する公開アドバイザリを発行しない。ベンダ内部のサプライチェーンで発見された脆弱性に関する情報を入手するために、そのようなサプライヤとの特定の通信チャネルを設定する。

> **目的:** ステークホルダの製品の脆弱性に繋がる、ベンダ内部のサプライチェーンで発見された脆弱性を特定する

成果: ベンダ内部のサプライチェーンで発見され、知らされることのなかった脆弱性に対する、より深い洞察

機能 2.3.5 組織内の開発チームへの通知

特定されたサードパーティ製品の脆弱性通知を、影響を受ける製品の開発チームに直接配布するため、自動化されたチャネルを確立する。ダウンストリーム製品の問題を解決するには、上流ベンダの指示に従うだけで十分であることが多い。優先順位付けポリシーに従って、いつ脆弱性をトリアージし PSIRT の取り扱いにエスカレーションするかを定義する。後者は、ステークホルダが安全なオペレーションのために製品の修正版を入手する行動を取る必要がある場合、特に重要となる。

目的: 脆弱性の依存関係とパッチ情報（もしあれば）について開発チームに選択的に通知し、次の製品リリースにおいて修正を適用できるようにする

成果: サードパーティからのアドバイザリ情報が開発プロセスへ直接処理されることで、PSIRT の手作業による脆弱性ハンドリングの工数を削減する

サービス 2.4 新しい脆弱性を見つける

PSIRT は、製品のセキュリティ問題への対処における外部関係の管理と調整の労力を削減するため、新しい脆弱性を組織内で発見することに積極的に取り組んでもよい。それらの活動は SDL の一部であるセキュリティ検証活動を補完するものである。PSIRT の活動には、製品セキュリティのアセスメントを製品リリース前あるいは保守フェーズに実施したり、セキュリティテストツールに関する専門知識を R&D に提供したりすることも含まれている。内部で発見されたエンドユーザに影響する脆弱性も、外部で見つかり修正、公表した脆弱性（スコアリング、レポーティングを含む）と同様に扱うべきである。

目的: 外部組織が発見する前に製品の脆弱性を発見し、修正する

成果: 組織内で製品の脆弱性を発見し、調整する労力を削減するために必要な専門知識、手順、メカニズム

機能 2.4.1 製品セキュリティアセスメント

製品セキュリティアセスメントは現在知られていない脆弱性を能動的に発見するためのプラクティスである。これには、ペネトレーションテスティング技術、脆弱性検出ツールといった幅広いテクニックやツールが含まれる。それらのグレーボックス/ブラックボックスなセキュリティアセスメントを実施することで、事前知識なしにシステムを攻撃する組織外の攻撃者の手法をシミュレートすることになる。

目的: 能動的な手法（proactive mechanisms）で脆弱性を検出する

成果: SDL のセキュリティ検証活動を補完する品質保証のステップ

サブ機能 2.4.1.1 自社製品のセキュリティアセスメント

自社製品のセキュリティコントロールに対するセキュリティアセスメントの分析結果は、製品のリリース前または修正アップデートの準備段階において、製品の状態を改善しようとする開発者にとって大きな助けになる。

サブ機能 2.4.1.2 サードパーティ製コンポーネントのセキュリティアセスメント

サードパーティから入手したコンポーネントの場合、一般的な調達管理だけではなく、より専用のセキュリティアセスメントを実施することが推奨される。重要なコンポーネントに対しては特に緻密なデューディリジェンス（due diligence）が必要である。

機能 2.4.2 セキュリティテストツールの専門知識の維持

営利企業とコミュニティの双方が、新しいセキュリティ分析と攻撃ツールを継続的に開発している。PSIRT は使用可能なツールに関する最新の知識を維持するべきである。これは製品の評価を行い、外部の発見者からの報告内容を検証し、開発チームが内部でのテスト用に適切なツールを選択する際の指針を示すのに役立つ。

目的: 良く準備されたエキスパートのチームに、複雑なツールを扱うスキルと、使用法に関するアドバイスを提供する

成果: 利用可能な最良のツールを活用する

サブ機能 2.4.2.1 PSIRT スタッフへのセキュリティテストツールのトレーニング

スタッフのトレーニングは、利用可能なセキュリティテストツールに関する最新の知識を維持するための主要な要素である。詳細は「サービス 6.3 診断チームのトレーニング」を参照せよ。

サービス 2.5 脆弱性発見のメトリクス

Figure 8: Vulnerability Discovery Metrics Process

PSIRT の規模、パフォーマンス、他の測定値を提供することは、PSIRT の有効性についてステークホルダの理解を維持するために極めて重要である（PSIRT の活動概要、III. 運用、B. 評価と改善 も参照）。ステークホルダはそれぞれ異なる独自の視点を持ち、それらは異なる形式のアーティファクト（または観点）で対処されなければならない。PSIRT は、各ステークホルダのグループが情報をどのように利用したいかを理解する必要がある。これらのメトリクスは、PSIRT の KPI となる。

> **目的:** PSIRT の測定値とパフォーマンスに関するデータを提供する。これは PSIRT が与えられた領域やサービスの提供に関してどれほど効果的であるかをステークホルダに理解させるのに役立つ
>
> **成果:** PSIRT のメトリクスをレビューすることにより、ステークホルダは PSIRT がどれだけ効果的にサービスを提供しているかを知り、フィードバックを与えて PSIRT のサービスへの修正を加えることができる

機能 2.5.1 運用レポート

運用レポートには、発見された脆弱性の種類と量に関する情報が記述される。これらのレポートは、社内のステークホルダだけでなく PSIRT 内部で定期的に発行されることもある。

目的: 一般的な報告のためのデータを定期的に収集する

成果: 分析、リソース、改善が必要な領域を決定する

サブ機能 2.5.1.1 発見された脆弱性と検証された脆弱性の総数

このデータは、リソースの観点から PSIRT が取り扱った脆弱性の量を把握する助けとなる。このデータは、ビジネスユニットレベル、製品のタイプ、特定の製品毎に細分化することができる。

サブ機能 2.5.1.2 サードパーティ製コンポーネントに落とし込まれた検証済みの脆弱性の総数

このデータは、製品に組み込まれた特定のサードパーティ製コンポーネントに関連するリスクを把握することに役立つ。

サブ機能 2.5.1.3 CWE に落とし込まれた検証済みの脆弱性の総数

このデータは、上流の SDL に供給され、トレーニングと教育に影響する。このデータはビジネスユニットレベル、製品のタイプ、特定の製品毎に細分化することができる。

サブ機能 2.5.1.4 脆弱性発見のアプローチ毎に細分化された、発見された脆弱性の総数

このデータは、簡単に発見できる脆弱性の特定に役立ち、上流の SDL に供給することができる。このデータはビジネスユニットレベル、製品のタイプ、特定の製品毎に細分化することができる。

サブ機能 2.5.1.5 情報ソース毎に細分化された、発見された脆弱性の総数

このデータは、PSIRT がどれだけ良く知られているかを説明するのに役立つ。

機能 2.5.2 ビジネスレポート

ビジネスレポートは、脆弱性のハンドリングと対応に関連について記述され、組織の脆弱性対応の健全性に関する情報を提供する。

目的: 組織の成功を定義するためのメトリクスを確立し、リスクを特定するためのマネジメント向け報告のために定期的にデータを収集する

成果: 成功と改善の機会を強調するダッシュボード

サブ機能 2.5.2.1 オンタイム応答率

このデータは、PSIRT が脆弱性報告への初動対応を、SLA の時間枠内で適時に行っているかどうかを表す。

サブ機能 2.5.2.2 PSIRT のコミュニケーションチャネルのダウンタイムの合計

このデータは、PSIRT のコミュニケーションチャネルが SLA で定義されたとおりに利用可能かどうかを表す。

サブ機能 2.5.2.3 トリアージまでの時間

これは報告を最初に受け付けてからトリアージを完了するまでの時間を計測する。このデータは PSIRT スタッフのパフォーマンスと作業負荷を示す。

サブ機能 2.5.2.4 フルディスクロージャ、外部から攻撃された脆弱性、メディアによって特定された脆弱性の数

このデータはステークホルダの製品に対するリスクを表す。

サービスエリア 3 脆弱性情報のトリアージと分析

脆弱性情報の収集やトリアージは、PSIRT における案件管理に含まれる。異なる PSIRT 間でもオペレーションの順序はほぼ同じように処理されるが、案件として管理されるタイミングや、案件の処理中に違う役割を実施する担当者がいる場合など、様々なバリエーションがある。大量の脆弱性レポートを受け取った組織では、案件として管理する前に、レポートを検証するための初期トリアージの実施を検討することがある。対照的に、脆弱性レポートの量が少ない組織では、トリアージの前に案件として管理することがある。PSIRT の最終目標は、効率的かつ明確なプロセスを作成することである。

目的: どのように脆弱性レポートがトリアージされるか定義する

成果: PSIRT と関係があるエンジニアチームとのプロセスが確立する

サービス 3.1 脆弱性の認定

組織は、対処したい問題の種類と範囲について、適切な認定基準を定義する必要がある。認定基準は、セキュリティベースラインを設定し、脆弱性の報告を効果的にトリアージするの

に役立つ。

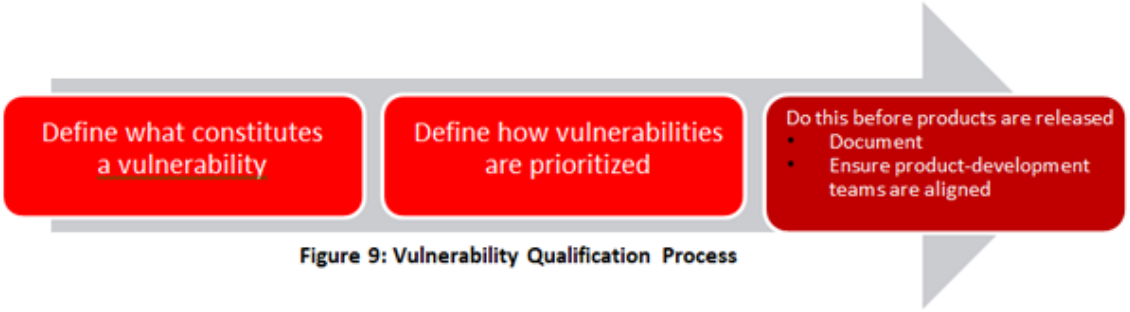


Figure 9: Vulnerability Qualification Process

機能 3.1.1 品質ゲートとバグバー

品質ゲートとバグバーは、最低限の許容可能なセキュリティ品質レベルとセキュリティ脆弱性の優先順位付け基準を確立するために使用される。製品がリリースされる前に、これらの基準を定義し PSIRT が改修すべき製品脆弱性の対象となるものを事前に決定することによって、脆弱性対応プロセスに透明性がもたらされる。

> **目的:** 内部および外部の関係者にプロセスの透明性を提供するため、明確な最小限の基準と優先順位付け基準を定義する
>
> **成果:** エンジニアと発見者に、脆弱性を構成するものについて明確な予測を提供する。さらに優先順位付けの基準は、初期トリアージからパッチの適用までの脆弱性ライフサイクル管理における混乱と争いをやわらげる

サブ機能 3.1.1.1 製品セキュリティの脆弱性の定義の文書化

品質ゲートやバグバーは、文書化し、関係者全員が閲覧可能な場所に保管し、開発者/エンジニアのための標準的なトレーニングの一部にする必要がある。

サブ機能 3.1.1.2 製品開発チームの関与

組織内に複数の製品と製品開発チームが存在する場合、脆弱性の定義の標準化を行うために関係者全員が関与することがとても重要である。

機能 3.1.2 継続的改善

成熟した PSIRT は、過去の経験、業界のベストプラクティス、製品の変更、およびステークホルダのフィードバックを反映するための判定基準の改訂に、継続的改善の考え方を適用すべきである。社内外のステークホルダに変更点を伝え、期待を管理することが重要である。

目的: 判定基準が改訂の対象であることを認識する。ステークホルダの期待や業界の動向、脆弱性の侵入など、PSIRT を取り巻くダイナミクスは、頻繁に変化することがありえる

成果: 柔軟な脆弱性の判定基準は、効率的な脆弱性判定の実践につながる

サブ機能 3.1.2.1 データの収集

受信レポートの件数、脆弱性としての判定件数、判定を受けていない報告の件数、遭遇した意見の相違など、トリアージプロセスに関するデータを収集する。

目的: データに基づいて改善を推進する

成果: 品質ゲートとバグバーの改訂がデータに基づいて行われる

サービス 3.2 発見者との関係構築

組織の PSIRT が成熟するにつれて、通常以上の件数の脆弱性を習慣的に報告する報告者グループの存在に気付くかもしれない。報告者の評判や、過去の高品質なレポートの提出を考慮して、根本原因の分析と脆弱性の改修に直接移行するため、判断基準やトリアージなどの一部のフローを省くことの検討を勧める。これは、プロセス効率を向上させ、報告者との関係を発展させていく上で役立つ。

目的: 研究コミュニティおよび、製品やサービスの脆弱性を最もよく報告する人を理解し、信頼性の高い報告者からのレポートの即時エスカレーションを検討する

成果: 精度の高い報告者への応答時間を短縮する

機能 3.2.1 発見者データベース

組織の脆弱性を報告した個人および組織のデータベースを作成し、維持して、その報告者の履歴、成果およびその他事例処理に関する考察を管理する。

> **目的:** トリアージプロセスの効率を向上させ、質の高いレポートの提出実績を持つ報告者との良好な関係を構築する
>
> **成果:** 適切な報告者からのレポートは、システムを短時間で通過する。報告者は結果および脆弱性の改修が潜在的な一般公開より前に行われることに満足する

機能 3.2.2 関係が良好な発見者の対応を加速

一部の報告者が、製品やサービスのソフトウェアバグを発見して報告する際に、多数の、もしくは一貫性のある（検査済み/信頼性の高い）報告をする可能性がある。例えば、カスタムのファジングツールを使用して、特定の詳細記述または PoC なしにクラッシュを報告することがある。報告者をよく知っており、報告する問題の大半が修正されると判断した場合は、判断/審査プロセスをすべてスキップし、脆弱性の改修フローに直接移行することを検討する。

> **目的:** トリアージプロセスの効率を向上させ、質の高いレポートの提出実績を持つ報告者との良好な関係を構築する
>
> **成果:** 適切な報告者からのレポートは、システムを短時間で通過する。報告者は結果および脆弱性の修復が潜在的な一般公開より前に行われることに満足する

機能 3.2.3 発見者プロファイル

報告者のプロファイルを作成し、脆弱性の対応をするメンバーに彼らと一緒に仕事をする最適な方法を知らせることを検討する。プロファイルには、地理的な位置、言語、彼らがプレゼンをした会議、脆弱性を発見するために使用される方法論、彼らがよく焦点を当てる製品/技術、彼らが調整された脆弱性情報の開示に従うか、彼らが見つけた脆弱性をカンファレンスで発表したいのか、脆弱性報告に対する謝礼を支払うもしくは他のインセンティブなどを提供するか、などが含まれているとよい。どの情報を収集し、どのくらいの期間保管することができるかについては、法務、またはコンプライアンスチームに相談する。

目的: 組織の製品の脆弱性を発見した人々を理解する

成果: 最も良好な結果を得られるような対応を、特定の報告者に対して行うことができる

機能 3.2.4 報告者のレポートの品質を定義する

組織は、報告書を迅速に評価するために必要な情報の種類について、報告者にガイダンスを提供するため、脆弱性レポートに最低限記載されるべき情報のガイドラインを定義し、公開することを検討することがある。ベースラインには、脆弱性に関する詳細記述、再生ステップ、テストされたプラットフォーム、および PoC が含まれるが、これに限定されない。

目的: 報告者に品質の高い脆弱性レポートのベースラインのガイドラインを提供する

成果: ベンダと報告者の間でのやりとりが最小限に抑えられ、ベンダは迅速に改修計画に集中することができる

サービス 3.3 脆弱性の再現

PSIRT は、脆弱性の判定基準の範囲外でも特段の定めがない限り、脆弱な状態になりうる条件を検証し理解するため、発見者のレポートが確実に再現可能であることを保証する必要がある。

目的: 脆弱性レポートの品質をあげるためのツールと環境を提供する

成果: 効率的で安心、安全な脆弱性レポートの検証

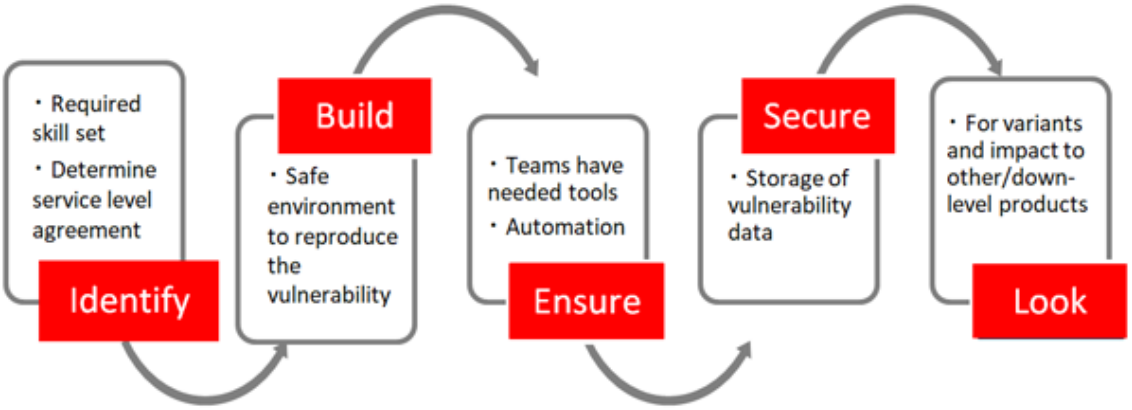


Figure 10: Vulnerability Verification/Reproduction

機能 3.3.1 脆弱性の再現に関するサービスレベルアグリーメント（SLA）の設置

PSIRT は、報告されるすべての脆弱性を再現するのに、十分な技術的専門知識を持っていない可能性がある。PSIRT は、他チームの専門性に頼ったり、相談したり、共同作業したりする必要がある可能性があるので、必要な専門知識が容易に利用可能であることを確実にするために明確な約束をしておくことが重要である。理想的には、フルタイムまたはパートタイムのリソース提供が推奨されるが、予算の都合上こういった対応が不可能である場合には、最低でも、脆弱性に関する専門知識を持つものがインシデント発生時に限られた期間の短時間で処置を行うことができるよう事前に、PSIRT のプロセスの一部に定義されるべきである。

> **目的:** PSIRT には、入ってくるすべての脆弱性を再現する技術的専門知識がないことを認識する

> **成果:** 事前の社内調整により、脆弱性の再現を援助するための短期間の専門知識の利用を、すぐに実施できるようになる

機能 3.3.2 再現テストの環境

脆弱性を再現するために、専用のテスト環境を PSIRT または専用チームに用意する必要がある。テスト環境は、悪意のあるアクティビティを回避しつつ、発見者のレポートを検証するため、隔離されている必要がある。必要に応じて、専用のネットワーク環境、シミュレーター、または仮想化技術を使用して、安全な環境を作成することができる。

> **目的:** 脆弱性の検査と再現を可能にする安全な環境を作成する

成果: 適切に準備された再現テスト環境は、脆弱性の影響をテスト環境の範囲に閉じ込めつつ、脆弱性の内容を効率的に分析するのに役立つ。

機能 3.3.3 再現ツール

報告された脆弱性を再現するチームは、これらの操作を実行するためのツールやアップデートされた製品ライセンスを持っている必要がある（デバッガなど）。

目的: 脆弱性を再現させるチームに必要なツールが提供されるようにする

成果: 報告された脆弱性の再現が可能な限り効率的であることを保証する

機能 3.3.4 脆弱性情報の保管場所

脆弱性レポートや、PoC に利用されるファイルなどの機密情報は、安全に保管し、必要とする人にのみアクセスを制限する。また、送付する際も確実に安全に行うべきことを推奨する。例として ISO 27001 を参照すること。

目的: 機密性の高い、潜在的に有害な脆弱性情報を安全に保つ

成果: 機密情報はアクセスが制限されて安全に保たれ、組織のプライマリネットワークの欠陥の影響を受けない

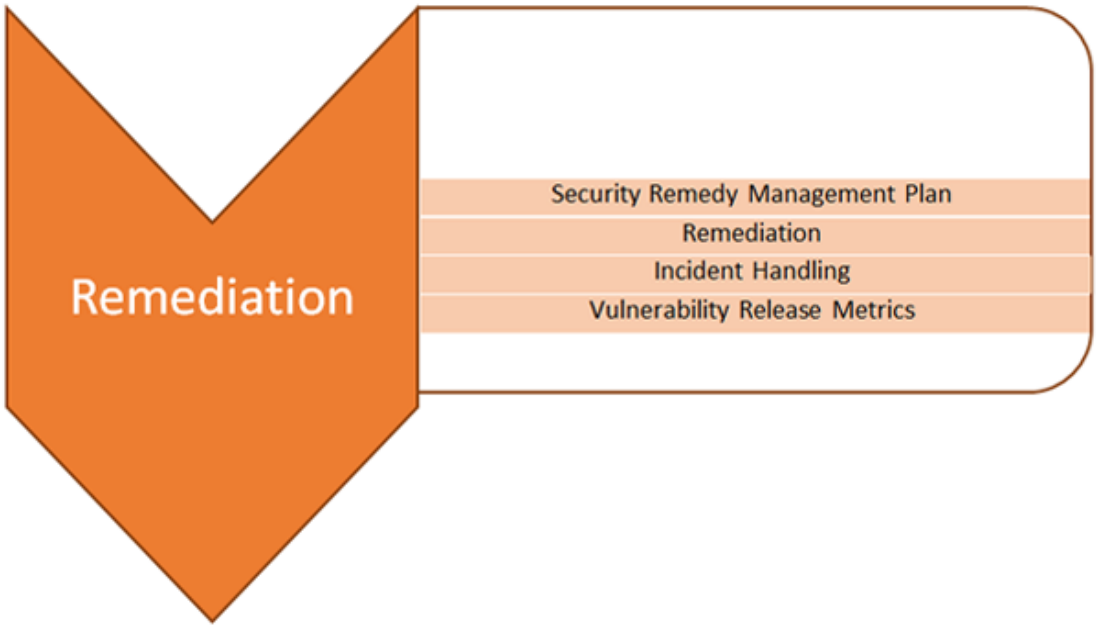
機能 3.3.5 影響を受ける製品

脆弱性の再現確認では、分析を行っているチームは、どの製品が影響を受けているか、および脆弱性の他のバリエーションが存在するかどうかを判断するために作業をする必要がある。製品ライフサイクル管理のセクション 4.1.1 も参照すること。

目的: 製品をまたぐ脆弱性の完全な理解と範囲の決定

成果: 脆弱性に対する修正を、サポートされている製品全体で包括的ものにすることができる

サービスエリア 4 対策



このサービスエリアは、ステークホルダと下流ベンダの両方に対策を提供し通知するために必要な様々なサービスを示す。セキュリティ修正プログラムを配布するメカニズムは、脆弱性を悪用された場合にステークホルダに与える影響に基づいて決定されるべきである。ステークホルダと下流ベンダがこれらのセキュリティ修正プログラムのテストと展開を計画できるスケジュールで対策が提供されるようにプロセスを確立する必要がある。

目的: ステークホルダや下流ベンダに対策をリリースし通知するために必要なプロセスとメカニズムを示す

成果: ステークホルダや下流ベンダが対策のリリースに応じて計画できる

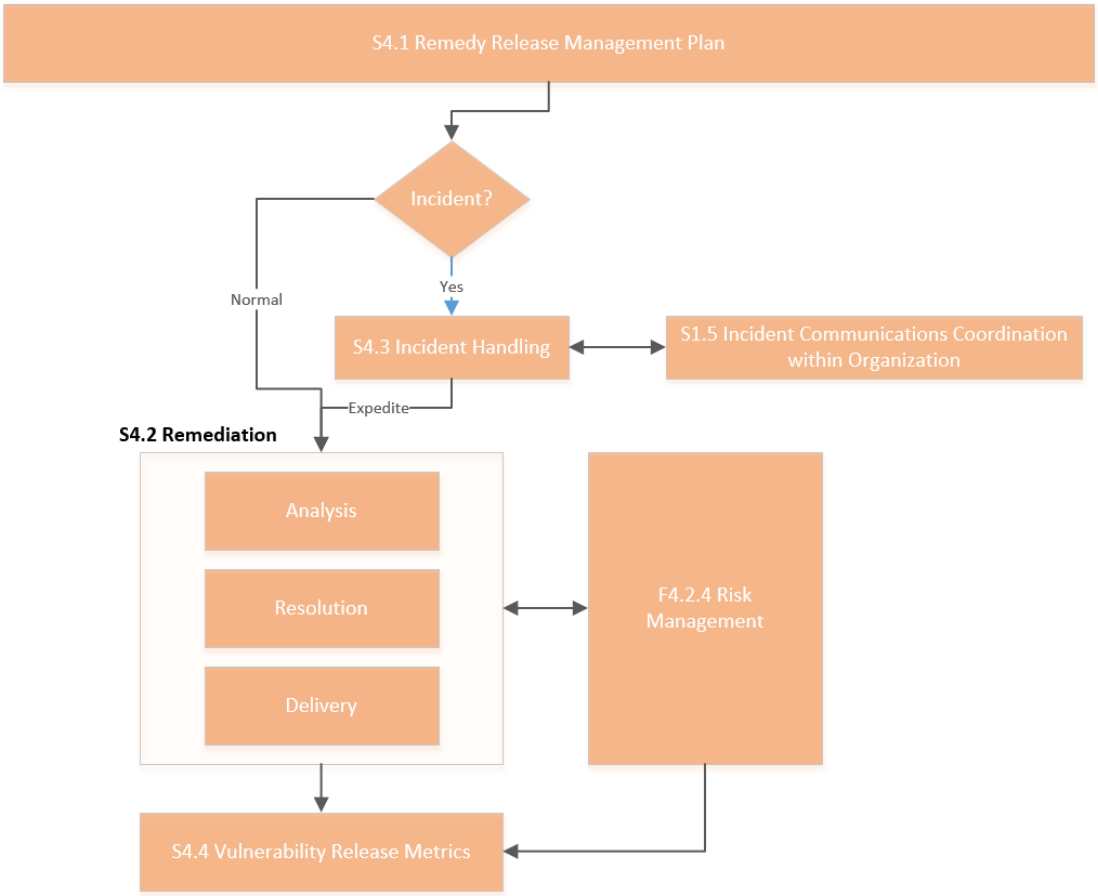


Figure 11: Example of a Core Remedy Release Process

サービス 4.1 対策リリースのマネジメント計画

このサービスは、ベンダが市場でサポートしている製品バージョンにおけるセキュリティ対策のリリース間隔を確立するためのガイダンスを提供することに重点を置いている。特にエンタープライズの領域では、ステークホルダはセキュリティ対策を適用するために計画を立てる必要がある。クラウドなどの一部の環境では、自動更新または異なるパッチ管理ポリシーが適用される場合がある。

目的: サービス対象者にどのプロダクトがサポートされるのか、対策が提供されるメカニズムおよび、提供間隔を伝えること

成果: ステークホルダは、セキュリティ修正プログラムの展開を事前に計画することができる

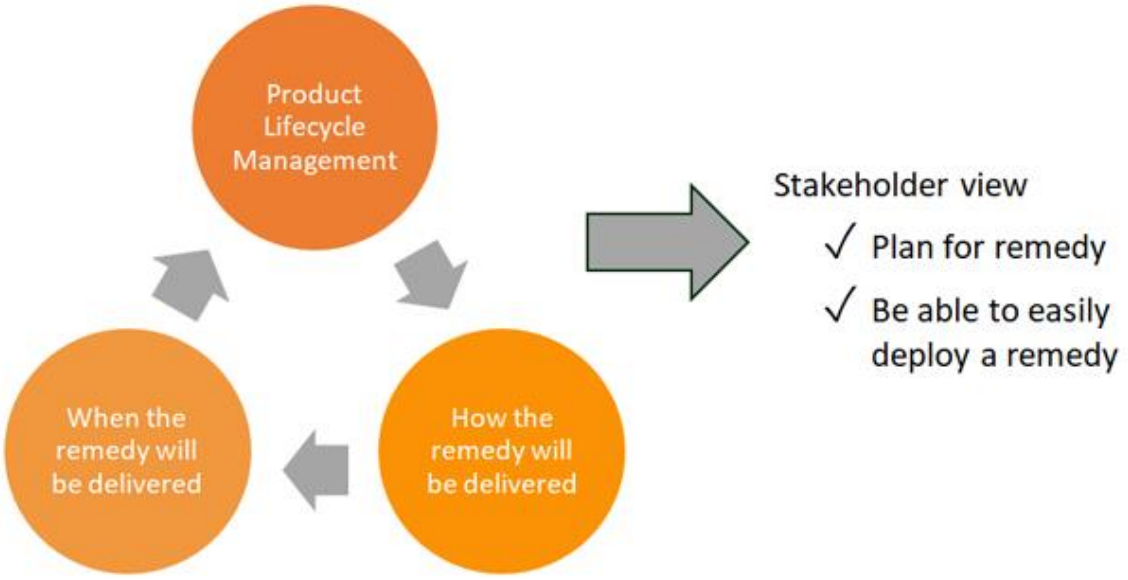


Figure 12: Setting the Foundation for Consistency

機能 4.1.1 製品ライフサイクル管理

企業はステークホルダと異なるサポートポリシーや契約を結ぶ場合がある。これらの要因に基づいて、PSIRT は事業単位、事業ラインおよび、ステークホルダサポートと協力し、サポート範囲またはサポート義務から外れた製品をどのようにサポートするかを決定することがある。これは脆弱性の重大さに依存し、事業単位、事業ライン、ステークホルダのサポートから提供される情報が関連することがある。

> **目的:** 組織が脆弱性を持つ製品をどのようにサポートするかを定めた明確なポリシーを製品チームに提供する
>
> **成果:** これらの製品への対策の提供についての事業単位や事業ラインの期待に対する明確なポリシー

サブ機能 4.1.1.1 製品インベントリ

サポートが適用されるすべての製品が評価され脆弱性が対策されていることを確認するために、市場にリリースされているすべての製品の目録を作成する。

サブ機能 4.1.1.2 サポートモデル

有料サービス、延長保証、メンテナンス契約および、特定のステークホルダとの契約など、様々な種類の製品サポートモデルを理解する。

サブ機能 4.1.1.3 製品ライフサイクル

製品ライフサイクル内で製品がいつサポートされなくなったか特定する。

機能 4.1.2 提供方法

PSIRT は対策をステークホルダへ提供する様々なオプションを特定するために、製品チームやステークホルダサポートとパートナーシップを組む可能性がある。その特定した方法を介していつ対策を提供するかを定めた基準も開発する必要がある。

> **目的:** 一連の条件に基づいて対策された脆弱性を提供するための一貫したメカニズムを維持する
>
> **成果:** ステークホルダが対策を、計画を立てて容易に適用できる

サブ機能 4.1.2.1 製品のパッケージフォーマット

対策の提供に関する様々なパッケージフォーマットについて理解すること（バイナリ実行形式、ソースコードの差分など）

サブ機能 4.1.2.2 対策の提供

ホットフィックス、パッチ、メンテナンスリリース、ファームウェアアップデートなどの対策の配布メカニズムと配布する方法について理解する

サブ機能 4.1.2.3 対策の適用

様々な製品間で対策の適用方法（リモートインストール、顧客がインストール可能、自動更新、オンサイトでの対応が必要など）を特定する。

機能 4.1.3 提供間隔

ステークホルダや下流ベンダは、彼らの環境のセキュリティを維持するために、対策を適用する計画を立てる必要がある。 対策が配信される定期的な間隔を設定することで、ステークホルダが彼らの環境を更新するために必要なリソースを計画し、予定を立てることを可能にする。

目的: ステークホルダに対策をリリースするための一貫した間隔を維持する

成果: ステークホルダが対策を、計画を立てて適用できる

サブ機能 4.1.3.1 対策の提供間隔

プロダクト管理チームやリリース管理者と協力して対策をどの程度の間隔で提供するかを決定する。いくつかの対策は機能リリースの一部として統合され、リリーススケジュールが調整されるが、アウトオブバンドリリースとみなされる緊急修正が必要になることもある。

サブ機能 4.1.3.2 例外ケースを文書化する

対策が通常の間隔で配信されない場合の例外を特定し、文書化する。

サービス 4.2 対策

このサービスは、発見者によって報告された脆弱性の管理に関連付けられ、対策分析と緩和を含んでいる。そして、このサービスはどのバージョンが修正されるかを定義し、どのように対策が提供されるかを検討する。また、対策が提供される前に、ステークホルダが直ちに適用できる回避策を検討する。

目的: 影響を受けるプロダクト、バージョンおよび、影響を受けるステークホルダに基づいて対策を提供するためのベストプラクティスとプロセスを提供する

成果: 影響を受ける製品やステークホルダへのニーズに適合する対策

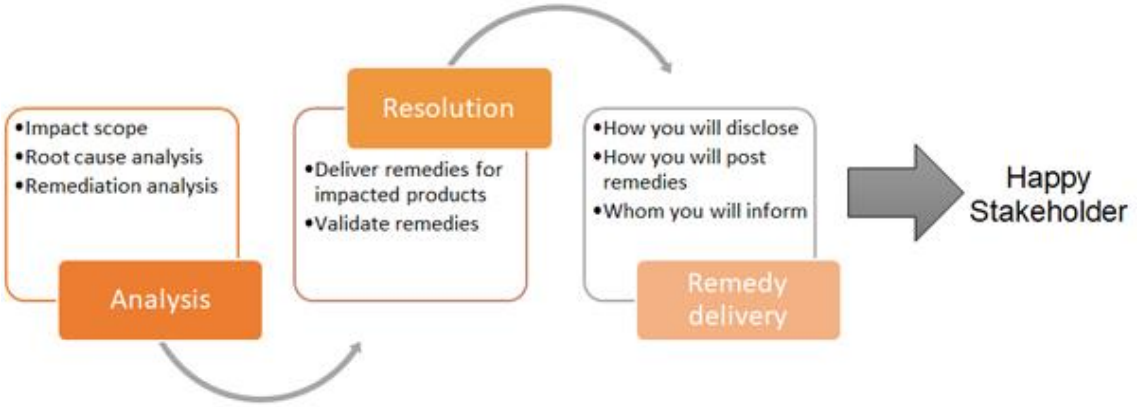


Figure 13: Remediation Process for the Reported Vulnerability

機能 4.2.1 分析

影響を受ける製品には、単一のソフトウェアアプリケーション、ファームウェア、またはソフトウェアまたはファームウェアのバージョンが異なる複数のハードウェアプログラムが含まれる。ステークホルダのニーズが満たされていることを確実にするための改修計画を立案する際には、いくつかのパラメータを考慮する必要がある。

目的: 影響を受けるプロダクト、バージョン、ステークホルダを決定する

成果: 影響を受ける製品やステークホルダのニーズに適合する修正

サブ機能 4.2.1.1 脆弱性の検証

脆弱性レポートおよびインシデントに対して、品質ゲートやバグバーを検証する。「機能 3.1.1 品質ゲートとバグバー」を参照。

サブ機能 4.2.1.2 修正すべきバージョン

影響を受ける製品、バージョン、および同時に修正する必要のある類似製品を特定する。

サブ機能 4.2.1.3 サポート契約の確認

影響を受ける製品バージョンに関するサポート契約やモデルについて確認すること。「サブ機能 4.1.1.2 サポートモデル」を参照。

サブ機能 4.2.1.4 原因分析

この脆弱性を引き起こした設計または実装上の欠陥を理解する。

サブ機能 4.2.1.5 脆弱性として取り扱わない基準を作る

例えば、ある脆弱性は偽陽性やセキュリティ設計上の欠陥となる可能性がある。

サブ機能 4.2.1.6 対策分析

ある脆弱性の結果として発生するリスクを軽減または対策する方法を決定する。

サブ機能 4.2.1.7 回避策

対策の検討中にこの脆弱性を軽減するために実行できる回避策があるかどうかを特定する。

サブ機能 4.2.1.8 例外

対策できない脆弱性を例外として識別する。「機能 4.2.4 リスクマネジメントプロセス」を参照。

機能 4.2.2 対策の決定

報告された脆弱性の対策をリリースする前に、品質保証（QA）エンジニア、セキュリティ検証、および該当する場合は脆弱性を報告した発見者によって検証されなければならない。ここでは、内部の関係者だけでなく、発見者と連携して対策を検証し承認を得るためのプロセスとメカニズムについて説明する。

> **目的:** 対策の内容について、内部で検証する、あるいは発見者と連携して検証するプロセスとメカニズムを提供する
>
> **結果:** 内部および/または外部の発見者によって、リリースする対策の内容についての承認を得る

サブ機能 4.2.2.1 対策を講じた脆弱性について検証する

影響を受けたすべての製品バージョンで、報告されたすべての脆弱性が対策されていることを確認する。

サブ機能 4.2.2.3 対策への承認を得る

担当の QA エンジニアまたはチームから対策に関するリリースの承認を得る。対策の検証は、標準的なテスト/QA プラクティスに統合されていることが必要である。

サブ機能 4.2.2.4 発見者とともに対策について検証する

対策について検証するために、第三者の発見者やステークホルダと協力関係を結ぶ。

機能 4.2.3 対策の提供

例えば、対策が利用可能になったタイミングで開示する場合や、対策が提供された後に開示を調整する場合がある。特にステークホルダとの関係（例えばパートナーや重要な団体）に基づいて開示の優先順位が決まる場合もある。それでも、発見者を含む業界全体の主要なステークホルダは公開時期について情報提供される必要がある。

> **目的:** 公開は脆弱性に合わせて計画され、ステークホルダに公開時期について情報提供する
>
> **成果:** ステークホルダへの開示とともに、対策を提供する

サブ機能 4.2.3.1 公開タイプ

脆弱性を公開するために優先されるメカニズムを決定する。深刻度または脆弱性の種類に基づいて決める場合もある。

サブ機能 4.2.3.2 必要に応じて、開示のための調整を行う

サブ機能 4.2.3.3 対策を内部のデータベースに公開する

ステークホルダサポートや他のステークホルダと協力して対策を公表する。公表の一例としてウェブポータル、ステークホルダサポートサイトまたは、RTM 版等があげられる。

サブ機能 4.2.3.4 対策の公開

報告された脆弱性を公開するためにステークホルダサポートやステークホルダと協力する。

機能 4.2.4 リスクマネジメントプロセス

ステークホルダに十分な情報を提供し、彼らのシステムや PSIRT がサポートしている製品やシステムの脆弱性から生じるシステムに対するリスクを評価できるようにするのは PSIRT の責務である。特定の期間内(SLA/SLO 単位)に脆弱性が修正されていない場合は、組織全体でリスク管理評価を実施する必要がある。この機能は、リスクを定量化するための透明化メカニズムや、組織のリスク登録簿に記載されている適切なステークホルダに報告できるようにすることを含む。

> **目的:** 内部で定められた SLA の時間要件の範囲内で対策されていない脆弱性に対する正式なリスク受容のプロセスを定義する
>
> **成果:** リスクに関する組織全体の透明性と、リスクが適切にエスカレートされ承認されていることの保証

サブ機能 4.2.4.1 権限のある役割

最高情報セキュリティ責任者（CISO)、最高セキュリティ責任者（CSO)、またはリスクマネージャのような、リスクを受け入れる権限を持つ役割を特定し、どの役割にリスクを知らせるべきかを特定する。

サブ機能 4.2.4.2 リスクマネジメントプロセスの定義

組織内のリスクを処理し対応するためのリスク管理プラクティスを定義する。これには、リスク管理プロセスのトリガーとなる条件のセットを含む。

サブ機能 4.2.4.3 リスクの評価と定量化

ビジネスへの脅威と影響を理解するため、リスクを評価し定量化する。

サブ機能 4.2.4.4 リスク登記簿にリスクを記載する

CSO、リスクマネージャ、またはその他のステークホルダによるリスク評価の状況確認や推奨事項実施の状況確認を支援する。

サブ機能 4.2.4.5 推奨事項

調査結果および推奨事項を記載し、リスク登記簿を更新する。

サービス 4.3 インシデントハンドリング

PSIRT には、世に出回っているアクティブなエクスプロイトやゼロデイ、意図しない一般公開といった「深刻な脆弱性」に対処する改修時間を早めるための仕組みが必要である。このサービスは、ステークホルダへ警告したり、脆弱性報告から対応の配信までの時間を短縮するためのインシデントの対応、緩和、復旧に関連する活動を調整するインシデントのためのガイダンスを提供したりする。

目的: 深刻な脆弱性を管理するための計画を策定し、それに対処するために必要なすべてのリソースを動員する能力を開発する

成果: 開示を控えた脆弱性や（想定外に）公開された脆弱性に対して、あるいはステークホルダがリスクに晒され迅速な対応が必要な状況に対して緊急修正プログラムを提供する

Figure 14: Incident Handling

機能 4.3.1 緊急対応室の設立

インシデント管理が必要となる場合、必要に応じて PSIRT、法律、広報、開発、ステークホルダサポート、サプライヤなどで構成される緊急対応室を設置する。すべての関係者が必要に応じて安全な方法で対応することができれば、物理的な場所でも仮想的な場所でも構わない。通常、ステークホルダが出席できるようにするには物理的および、遠隔からのオプションの双方が必要である。インシデント管理プロセスを適切にサポートするためには、事前にリソースを特定する必要がある。

> **目的:** ステークホルダが質問に答えて指示を出すことができるようにする。インシデントを管理するために適切なリソースが割り当てられていることを確認する
>
> **成果:** リソースを検証し整理できる

サブ機能 4.3.1.1 インシデント管理プラン

深刻な脆弱性を管理するための計画を策定し、それに対処するために必要なすべてのリソースを動員する能力を開発する。予想していない事態や緊急事態に対応し、それに対する準備の検証を実施するため、インシデントレスポンスの準備をするのが重要である。

サブ機能 4.3.1.2 インシデントの管理に必要なリソースを特定する

ここで言う「リソース」には、会議室、専用回線、追加の人員などが含まれることがある。インシデント対応が長期にわたる場合には、食糧と宿泊施設を考慮する必要がある。

サブ機能 4.3.1.3 ステークホルダをインシデント対応計画に含める

インシデントレスポンス計画の一環として、インシデントのハンドリングに参加することが必要なすべてのステークホルダを洗い出す。
サービス 1.1 内部のステークホルダ管理と、サービス 1.5 組織内でのインシデントに関するコミュニケーションの調整を参照。

サブ機能 4.3.1.4 インシデントを管理するための明確な役割と責任の割り当て

各担当者は、応答が必要なときに、自分の役割と操作の順序を知っていなければならない。主要な対応参加者を準備するために、トレーニングや机上訓練を実施する必要がある。

機能 4.3.2 インシデント管理

インシデントであることが宣言された後、ステークホルダとのパートナーシップにおける PSIRT の活動は、インシデントの影響を軽減し、製品とステークホルダのビジネス機能を回復することに主な焦点が置かれる。

目的: 作戦を立て、インシデントを封じ込める計画を実行する

成果: できるだけ早く製品チームとステークホルダに作業を戻す

サブ機能 4.3.2.1 情報収集

インシデントに関連する情報を受信、カタログ化、および保管する。

サブ機能 4.3.2.2 分析

インシデント処理は、分析アクティビティに依存する。分析アクティビティは「分析」セクションで定義されている。

サブ機能 4.3.2.3 対応

インシデントの影響を軽減し、サービス対象のビジネス機能を回復するためのサービスである。

サブ機能 4.3.2.4 インシデントトラッキング

収集された重要な情報、実行された分析、対策および緩和策のステップ、終了および解決を含む、インシデントを解決するために取られたアクションに関する情報を文書化する。

サブ機能 4.3.2.5 インシデント事後プロセス

将来起こる可能性がある危険を緩和および予防するために、プロセス、ポリシー、手順、リソース、およびツールの改善を確認する活動である。

機能 4.3.3 コミュニケーション計画

すべてのステークホルダと行動主体は、インシデント対応を軌道に乗せるために最新の計画と進捗状況を把握する必要がある。インシデント対応中にオープンで協調的なコミュニケーションを妨げる障壁を解消するために、必要に応じて管理者を招聘する。

目的: コミュニケーション計画を作成し、全員が最新の開発状況を把握できるようにするためのインシデントの連絡窓口を指定する

成果: コミュニケーションが整理される

サブ機能 4.3.3.1 内部ステークホルダへの情報公開

状況認識に使われる告知、アラート、データフィード、または他の情報を配布するために使用されるリストを管理する。

サブ機能 4.3.3.2 よく管理され調整された広報活動

公式の組織チャネルを通じてのみ、情報がメディアおよびステークホルダに伝わるようにする。これにはソーシャルメディアへの投稿も含まれる。

サブ機能 4.3.3.3 復旧のアクティビティの伝達

復旧のアクティビティは、内部のステークホルダ、エグゼクティブ、マネジメントチームに伝達される。

サブ機能 4.3.3.4 事故後のフィードバックを集める

PSIRT による事故後の説明会が行われ、インシデント対応や SDL 活動を改善するためのフィードバックが収集される。一例として「どのような SDL 活動が最初にその問題を阻止し得たか/すべきだったか」といったフィードバックが挙げられる。

サービス 4.4 脆弱性リリースメトリクス

収集されるデータには、問題の数、分類、修正時間、影響を受ける製品またはサービスが含まれている必要がある。収集する情報はこれらだけに限定されない。

目的: 管理レポート用に定期的にデータを収集する

成果: 分析、リソース、改善が必要な領域を決定する

Figure 15: Operational and Business Metrics

機能 4.4.1 運用レポート

運用レポートには、様々な製品やバージョンで報告されて確認されている脆弱性の種類と脆弱性数の情報が表示される。これらの報告書は、PSIRT の内部および内部のステークホルダに定期的に公表される必要がある。

目的: 一般的なレポートのために定期的にデータを収集する

成果: 分析、リソース、改善が必要な領域を決定する

サブ機能 4.4.1.1 報告された脆弱性数と確認された脆弱性数（製品/事業単位別）

このデータは、PSIRT がリソースの観点から処理できる数を把握するために役立つ。

サブ機能 4.4.1.2 サードパーティ製コンポーネント毎の脆弱性の数

このデータは、埋め込まれた特定の第三者コンポーネントに関連するリスクを把握するために役立つ。

サブ機能 4.4.1.3 確認された脆弱性の CWE による分類（製品/ 事業単位別）

このデータは、セキュリティ開発ライフサイクルの上流に供給され、トレーニングと教育に影響を与える。

機能 4.4.2 ビジネスレポート

ビジネスレポートは、組織の脆弱性対応能力の健全性に関する情報を提供する。

> **目的:** SLA で定められた稼働時間を守ることができたかどうか、組織としての達成度合いを見積もる方法を確立する
>
> **成果:** ダッシュボードを作成することで改善の機会が生まれ、成功に繋がる

サブ機能 4.4.2.1 オンタイムの影響評価

このメトリックは、製品チームが SLA の時間枠内でどの程度影響評価を完了できているかを示す。

サブ機能 4.4.2.2 オンタイムの改修計画の提供

このメトリックは、製品チームが指定された SLA 内でどの程度改修計画を提供できているかを示す。

サブ機能 4.4.2.3 対策状況の追跡

このメトリックは、製品チームが SLA の時間枠内でどの程度修正プログラムを提供できているかを示す。

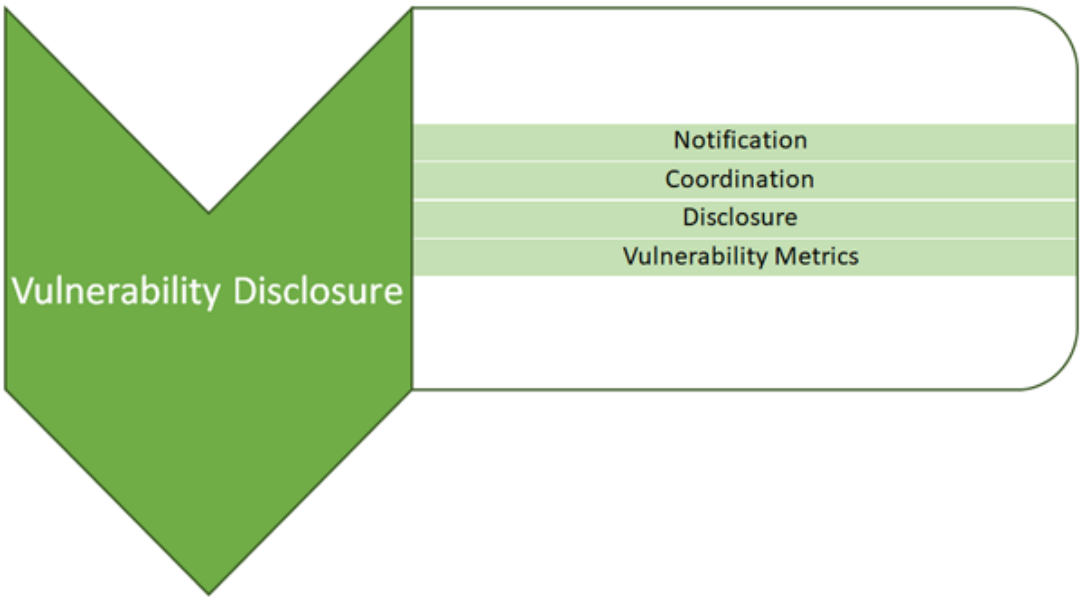
サブ機能 4.4.2.4 オンタイムでの改修率

このメトリックは、製品チームがどの程度脆弱性報告から修正プログラムの提供までの全体的な目的や合意を満たしているかを表す。これは深刻度または、脆弱性の種類（製品ライン、脆弱性の種類）によって分類できる。

サブ機能 4.4.2.5 インシデントの数

このデータは、組織のリスクを把握する。

サービスエリア 5 脆弱性の開示



脆弱性の開示を円滑に進めるためには、ベンダ、調整者、発見者が相互に、またそれぞれのステークホルダと情報を共有し、情報開示プランを相談するための透明性の高い協力的な環境を整えることが重要である。そうすることで、ステークホルダの保護や発見者との連携も含め、脆弱性を修正するという目的を実現することができる。ベンダは脆弱性情報の情報開示ポリシーを公開し、調整機関や他のベンダ、発見者などが参照できるようにすべきである。

Figure 16: Vulnerability Notification Process

目的: 脆弱性情報や対策情報を適切に開示するために発見者、調整者、下流ベンダなどとどのように連携しているかを、ステークホルダやパートナーが把握できるように透明性を確保する

成果: 関係者間の信頼関係、連携、情報開示プロセスの管理向上

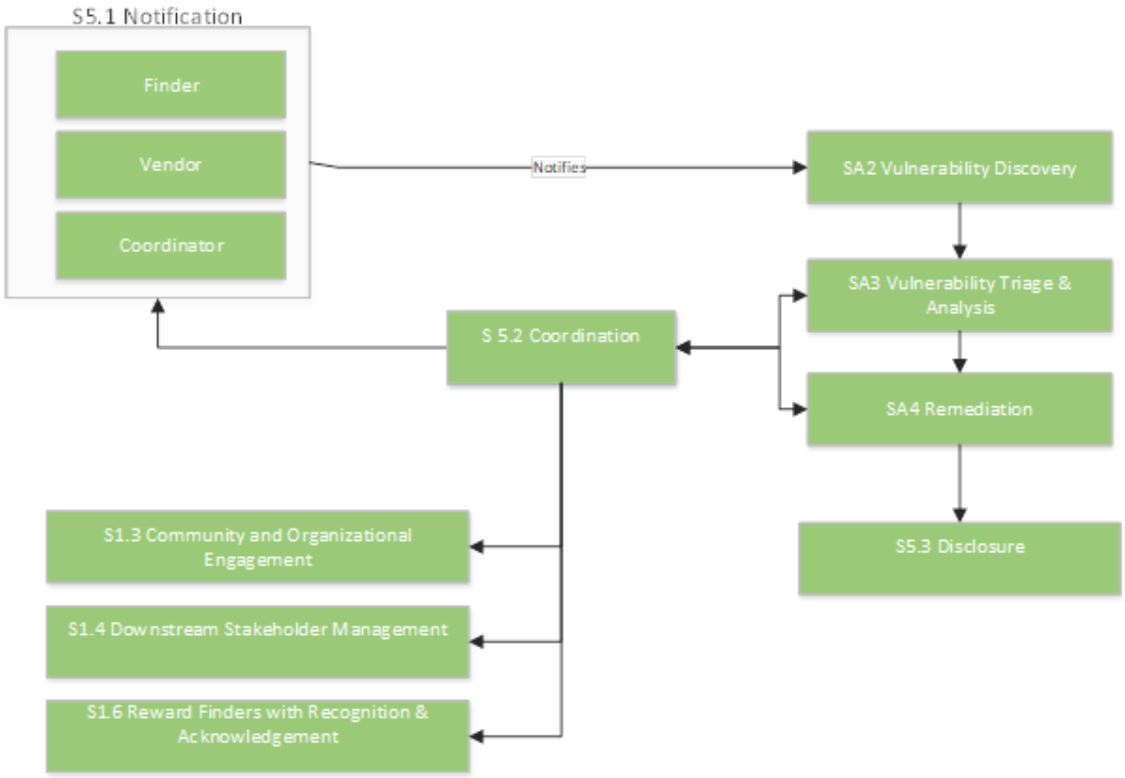


Figure 17: High-level example of Vulnerability Coordination

サービス 5.1 通知

このサービスでは、適切な通知のプロセスを決定し、対策方法、修正、回避策に関する情報をタイムリーにステークホルダに提供する。それらの情報を知ることでステークホルダは、適切な対応を計画できるようになる。上流ベンダと下流ベンダの間で、脆弱性情報の開示や既知のインシデントに関して通知を行うよう契約を結んでいることもあるだろう。通知プロセスの目的は、すべてのステークホルダとベンダが脆弱性によるリスクを把握し、管理できるようにすることにある。

目的: 連携活動を通じ、ベンダと発見者に対して透明性を確保する

成果: 発見者との信頼関係および連携の向上

機能 5.1.1 中間ベンダ（下流ベンダ）

OEM やパートナーなどの中間ベンダは、他のベンダが出荷する製品の一部を開発・作成することがある。このような場合、中間ベンダの PSIRT はベンダと脆弱性情報を共有する準備をしておくべきである。また、ベンダ毎に脆弱性ハンドリングポリシーが異なることも考慮しなければならない。互いに期待する内容を契約という形にまとめることもあるだろう。対策と情報開示にいたるタイムラインは、できるだけ早く協議するべきである。

> **目的:** OEM、パートナーおよび他ベンダとの間に連携が可能な環境を整え、期待されるものを明確にする
>
> **成果:** すべての関係者間における信頼関係、連携、情報開示プロセスの管理向上

サブ機能 5.1.1.1 PSIRT から中間ベンダへの通知

PSIRT は、ステークホルダから脆弱性の報告を受けたら、中間ベンダの PSIRT にその脆弱性を通知する。

サブ機能 5.1.1.2 中間ベンダからの通知

ベンダに対しコンポーネントやツールを提供している中間ベンダは、脆弱性の報告を直接受けることがあれば、ベンダ PSIRT にこの情報を伝える。

サブ機能 5.1.1.3 契約条項

PSIRT は、すべての中間ベンダを明らかにしたうえで、法務部門と連携して、中間ベンダとの契約内容に、脆弱性対応をタイムリーに行うという条項を追記する。

サブ機能 5.1.1.4 PSIRT からステークホルダへの通知

中間ベンダによる脆弱性の対策が作れない、あるいは時間がかかる場合、ベンダ PSIRT は、ステークホルダに情報を共有する。段階的な通知プロセスを使用して、脆弱性による影響を最も大きく受けるステークホルダに通知する、というやり方もある。

機能 5.1.2 調整者

特に複数のベンダが関わる場合、調整者は PSIRT から依頼を受け、ベンダへの通知やアドバイザリ公開のタイミングの調整を行うことがある。CERT Coordination Center (CERT/CC) やサードパーティの調整者は、脆弱性に対応するため、様々な組織に協力を呼びかけることで価値を提供する。

> **目的:** 調整者は、ベンダへの脆弱性情報通知と対応への協力呼びかけについて、PSIRT から支援の要請を受けることがある
>
> **成果:** すべての関係者間の信頼関係、連携、情報開示プロセスの管理向上

サブ機能 5.1.2.1 調整者の特徴の理解

脆弱性情報開示ポリシーから、様々な調整者の特徴を把握し文書化する。

サブ機能 5.1.2.2 調整者との連携

調整者と連携し、影響を受けるすべてのベンダ PSIRT への通知を行う。

機能 5.1.3 発見者

顧客やサードパーティの研究者などの発見者は、PSIRT に対して、「サービスエリア 2 脆弱性の発見」に記載されている連絡手法を用いて脆弱性の報告を行うことがある。

> **目的:** 発見者との連携が可能な環境を整え、発見者に期待することを明確にする
>
> **成果:** 発見者との間で信頼関係、連携、情報開示プロセスの管理向上

サービス 5.2 調整

ベンダ PSIRT は、そうすることが適切であるならば、調整者や他のベンダと脆弱性情報を共有すべきである。情報を受ける側の調整者やベンダは、情報提供元ベンダの脆弱性ハンドリングポリシーを理解しておく必要がある。対策と情報開示にいたるタイムラインは、できるだけ早く協議するべきである。

> **目的:** 修正によって取り除かれた脆弱性を説明する

成果: 修正を適用することで得られる利点と修正の取得方法の明示

機能 5.2.1 双方向の調整

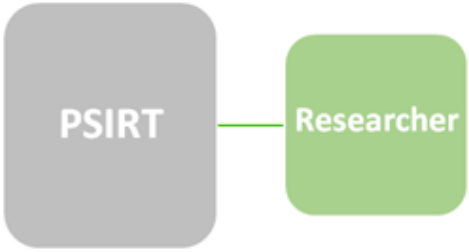


Figure 18: Bilateral Coordination

ベンダ PSIRT は、潜在的な脆弱性を報告する発見者とのコミュニケーションを維持する責任がある。一般公表日程を申し合わせ、協調して情報開示を行う活動を推進するために、発見者の目的、意図、脆弱性に対するスタンスを理解することが重要である。PSIRT は、情報開示に関して約束を守っている発見者に敬意の念を示すことを検討すべきである。

目的: 発見者が真面目に扱われていると分かるような連携のための環境を作る

成果: 発見者の努力に敬意を払い調整された情報開示プラン

サブ機能 5.2.1.1 レポートの受領

発見者から脆弱性レポートを受領したら、受領した旨を応答する。

サブ機能 5.2.1.2 定期的な状況報告

報告された脆弱性に関する対応状況を、定期的に発見者に連絡する。

サブ機能 5.2.1.3 発見者による検証

発見者に修正を提供し、発見者自身で検証できるようにする。

サブ機能 5.2.1.4 発見者への謝辞

脆弱性を報告した発見者の貢献を認め、謝辞を述べる。ただし、その内容は発見者に確認すべきである。

機能 5.2.2 複数ベンダ間の調整

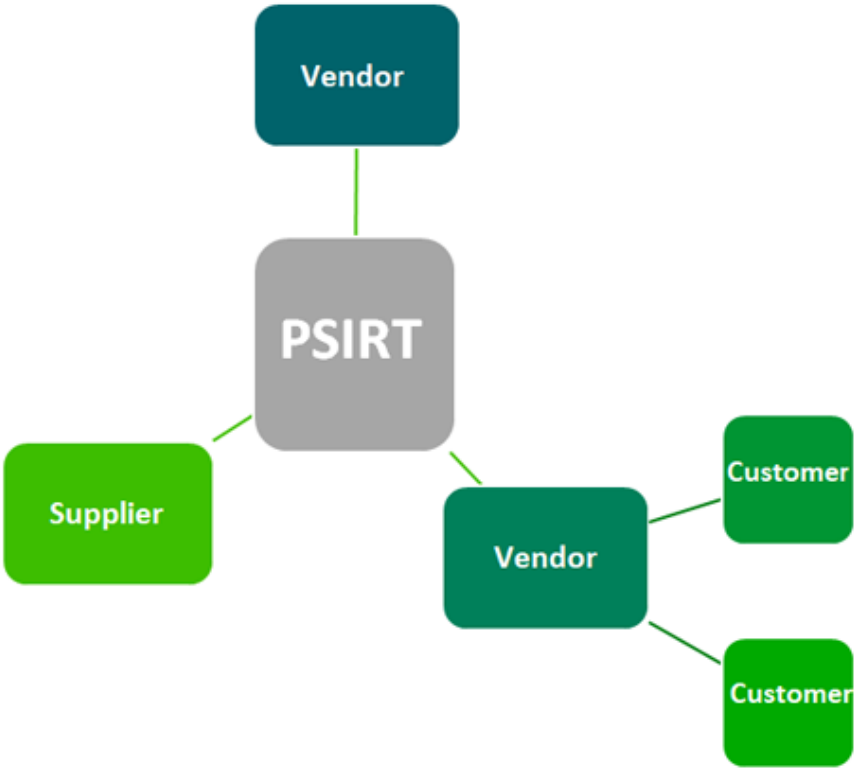


Figure 19: Multi-Vendor Coordination

ベンダ PSIRT は、そうすることが適切であるならば、調整者や他のベンダと脆弱性情報を共有すべきである。情報を受ける側の調整者やベンダは、情報提供元ベンダの脆弱性ハンドリングポリシーを理解しておく必要がある。対策と情報開示にいたるタイムラインは、できるだけ早く協議するべきである。

> **目的:** 脆弱性情報や対策情報を、責任をもって開示するために、すべての関係者との連携を通じて、ステークホルダやパートナーに対する透明性を確保する
>
> **成果:** 信頼関係、連携、情報開示プロセスの管理向上

Multi-Party Stakeholder	Relationship to Self	Stake in Coordination
Upstream Vendors	OEM supplier provides technology.	To provide a remedy it is recommended upstream vendors manage their downstream stakeholders (see Service Area 1.4).
Downstream Vendors	Receives technology from upstream vendor.	To be notified to apply the security remedy. It is recommended that downstream vendors define and engage with upstream vendors communities and partners (see Function 1.3.1).

Table 1: Example of Multi-Party Coordination

サブ機能 5.2.2.1 レポートの受領

ベンダ PSIRT は、他のベンダや調整者から脆弱性レポートを受領したら、受領した旨を応答する。

サブ機能 5.2.2.2 影響を受けるベンダの特定

ベンダ PSIRT や調整者は、報告された脆弱性の影響を受けるベンダを特定する必要がある。

サブ機能 5.2.2.3 脆弱性情報の共有

ベンダ PSIRT や調整者は、他のベンダと脆弱性情報を共有する。

サブ機能 5.2.2.4 対策情報を公開する日程の調整

ベンダ PSIRT や調整者は、情報を共有しているベンダとの間で、対策情報を公開する時期やその中身について調整する。さらに、下流ベンダがその対策情報を受け取る方法についても調整する。

サブ機能 5.2.2.5 対策情報の検証

ベンダ PSIRT や調整者はベンダとともに、対策情報が脆弱性への対処として適切であるこ

とを検証する。

サブ機能 5.2.2.6 公表の調整

ベンダ PSIRT や調整者は、脆弱性情報がどのように、またいつ開示されるのか、について、すべてのベンダとの間で協議し、合意をとる。

サービス 5.3 情報開示

セキュリティ対策をリリースする際、ステークホルダやベンダにその内容が正しく伝わるよう、適切な情報開示がなされなければならない。情報を開示する通知対象を明確に定めることが必要である（通知対象によって、異なる通知が必要になる可能性がある）。

目的: コードの変更とセキュリティ修正のリリースを記録する

成果: コードの変更内容と入手場所に関する情報の明確化

機能 5.3.1 リリースノート

リリースノート、あるいは Readme や変更履歴などにおいては、対策情報に対応する CVE 番号を記載するとともに、脆弱性がどのように対処されたかを明確に伝えるべきである。

目的: アップデートに含まれるセキュリティ関連の修正内容を提示する

成果: ステークホルダは、脆弱性が暴露されるリスクから身を守ることができる

サブ機能 5.3.1.1 リリースノートにおける開示

リリースノートで開示する脆弱性を決定する。

サブ機能 5.3.1.2 リリースノートのレビュー

リリースノートのレビュープロセスを定義する。

サブ機能 5.3.1.3 リリースノートの内容を承認する

情報開示に関するレビューと承認を行う。

機能 5.3.2 セキュリティアドバイザリ

ベンダは自身の公開ウェブサイトにセキュリティアドバイザリを掲載し、修正された脆弱性を開示する仕組みを持たなければならない。

目的: セキュリティアドバイザリの公開場所を提供する

成果: 関係者がセキュリティアドバイザリを読み、対策を取ることができる

サブ機能 5.3.2.1 アドバイザリテンプレート

セキュリティアドバイザリのテンプレートを定義する。

サブ機能 5.3.2.2 アドバイザリの提供手段

セキュリティアドバイザリを提供する仕組みを定める (例: ウェブドキュメント、RSS フィード、登録制の仕組みなど)。

サブ機能 5.3.2.3 アドバイザリの形式

ステークホルダやサービス対象者が自動化ツールを活用できるよう、Common Security Advisory Framework (CSAF) のような機械可読形式でのアドバイザリの提供を検討する。

サブ機能 5.3.2.4 アドバイザリを発行する条件

セキュリティアドバイザリを発行する条件を定義する。例えば、運用している環境に対する不正侵入が発覚し、対策を講じたことをステークホルダに通知する必要がある場合。

サブ機能 5.3.2.5 CVE 番号の割り当て

脆弱性に CVE 番号を割り当てる手順を定める。

サブ機能 5.3.2.6 発見者への謝辞

発見者が自身の名前の掲載を望むかどうか確認する。

サブ機能 5.3.2.7 開示計画

ステークホルダは誰であるか、情報をいつ開示するか、などのレビュープロセスを定義する。

サブ機能 5.3.2.8 アドバイザリのレビュー

所定のステークホルダとともにアドバイザリをレビューする。

機能 5.3.3 ナレッジベースの記事

ベンダは、ナレッジベースの記事を公開する仕組みを持っているべきである。これは、重要度が低いと判断されたアップデートについてのものであったり、ある脆弱性報告を却下した際にその理由を説明したりするために使用される。

目的: ナレッジベースの記事の公開場所を提供する

成果: 関係者がナレッジベースを読み、対策を取ることができる

サブ機能 5.3.3.1 ナレッジベース記事の公開

どのような脆弱性をナレッジベースの記事にすべきかを定義する。

サブ機能 5.3.3.2 ナレッジベース記事のレビュー

レビュープロセスを定義する。

サブ機能 5.3.3.3 ナレッジベース記事の承認

ナレッジベース記事をレビューし、公開を承認する。

機能 5.3.4 内部のステークホルダとのコミュニケーション

脆弱性情報開示の計画は経営陣に周知しておくべきである。さらに、ステークホルダと対面または電話越しに日々仕事をしている多くの従業員が存在する。彼らには、内部情報として、近く開示予定のアドバイザリの内容や FAQ について伝えておくべきである。そうすることで、アドバイザリ公開とともにステークホルダから受ける問い合わせに適切に対応するべく準備しておくことができる。

目的: 経営陣、グローバル対応の担当者、ステークホルダと接する従業員に対して、「近日中に公開される」アドバイザリと、取るべき適切な対応とを周知する

成果: 従業員はステークホルダやメディアからの質問に対し、アドバイザリが公開されたその日に回答することができる。結果として、従業員から発せられる情報を適切にコントロールすることができる

サブ機能 5.3.4.1 内部のステークホルダとの連携

内部のステークホルダと協力して、脆弱性に関して顧客から受ける質問にチームとして答える際の用語や言葉遣いを定めたりレビューしたりする。

サービス 5.4 脆弱性情報マネジメントの評価指標

収集すべきデータとしては、例えば、案件数（issue volume）、分類、修正にかかった時間、影響を受ける製品やサービス、などがある。

目的: 経営層への報告のために定期的にデータを収集する

成果: 分析、リソース、改善が必要な領域を決定する

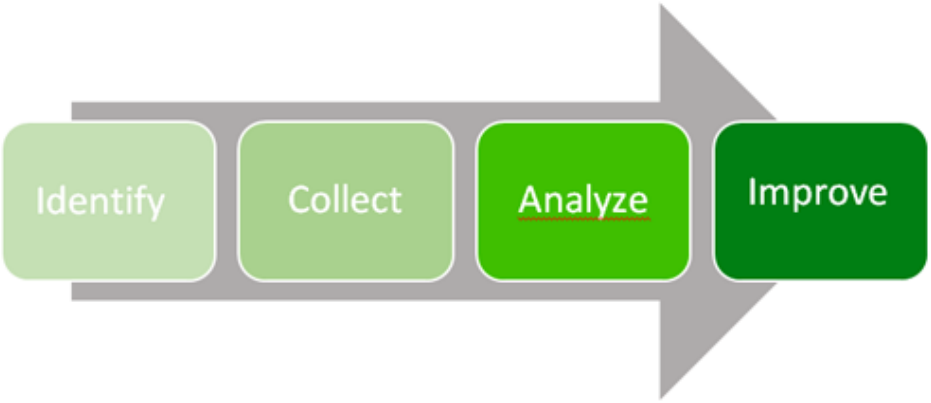


Figure 20: Vulnerability Metrics Process

機能 5.4.1 運用レポート

運用レポートには、各アドバイザリへのアクセス数だけでなく、アドバイザリの公開件数などに関する情報も含めるべきだ。PSIRT 内部でこれらのレポートを定期的に発行するとともに、内部のステークホルダ向けにも提供すべきである。

目的: 定期的にデータを収集する

成果: 分析、リソース、改善が必要な領域を決定する

サブ機能 5.4.1.1 セキュリティアドバイザリの公表数

全体の公表数だけでなく、製品ごとの公表数など。この情報は、PSIRT の技術的リソース確保の検討に役立つ。

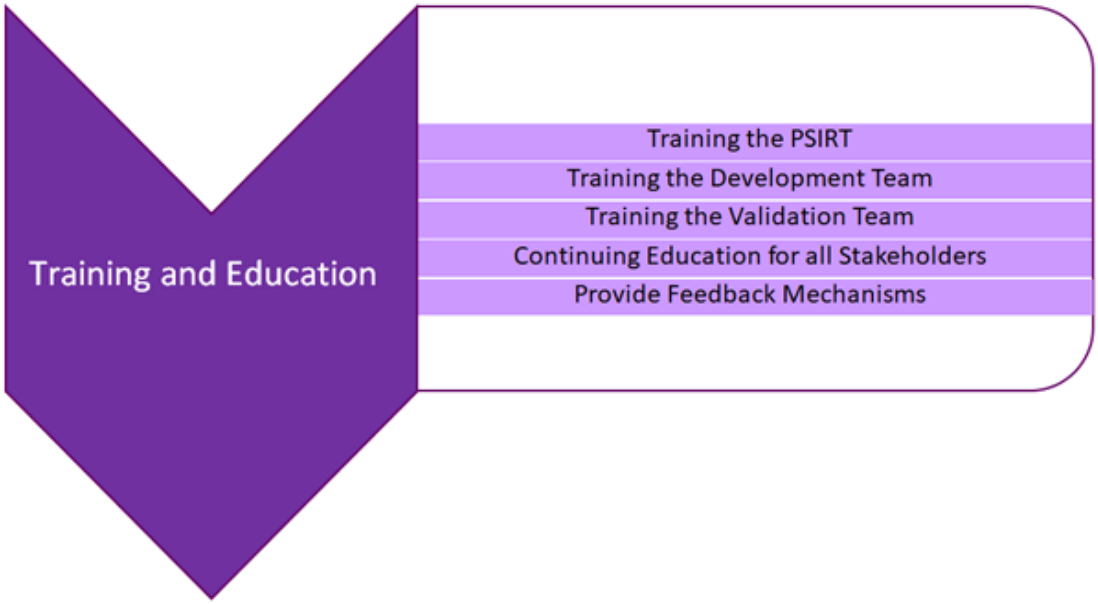
サブ機能 5.4.1.2 NVD へポストした CVE の数

CVE の割り当て状況によっては、CVE Numbering Authority（CNA）として活動することも考えられる。

サブ機能 5.4.1.3 セキュリティアドバイザリへのアクセス数

アドバイザリを参照するステークホルダの数が少ないのであれば、それらのステークホルダへの事前通知を行うことも考えられる。

サービスエリア 6



新しいテクノロジ、サービス、インテグレーションによって、製品セキュリティの世界は常に変化し、継続的なトレーニングと教育がセキュリティ専門家にとっては最重要課題となっている。私たちの生きる世界で車から冷蔵庫までもソフトウェアが浸透し、製品の安全性の確保はより重要である。今日のネットワーク化された世界で標準を満たす、複雑な製品やサービスの開発、検証、出荷について、すべてのステークホルダを教育するための強力なカリキュラムをサポートする上で PSIRT は重要な役割を果たす。

トレーニングと教育ニーズは、組織の中でも異なる可能性がある。ファームウェア開発者とソフトウェアサービスの開発者の関心は異なり、非常に特殊性の高い独自のトレーニングが必要なことがよくある。このドキュメントでは、PSIRT プロセスに関与する 4 つのステークホルダグループ、PSIRT、製品開発、製品検証、およびその他のステークホルダに関するトレーニングに分類する。

1. **PSIRT トレーニング**は法律やコミュニケーション、開発など様々なトレーニングが必要なため、とても独特である
2. **開発(内部エンジニアリングと開発)**：開発者は専門分野のトレーニングを必要としているため、焦点を絞ったトレーニングが必要である。現場で更新するのが非常に困難な 安全なファームウェアを開発することと、デスクトップアプリケーションエンジニアの要件とは大きく異なる。

3. **製品検証（内部エンジニアリングと開発）**：診断担当者は、リリース前に脆弱性を発見するため、最新のツール・ペンテスト・脆弱性スキャン・初期設計のレビューのテクニックに精通するためのトレーニングが必要である
4. **他のすべてのステークホルダ**：ステークホルダは、セキュアな製品の開発・検証・出荷に関する基礎を理解すると同時に出荷された製品に脆弱性がある場合の対応に関するトレーニングが必要である

セキュア開発のトレーニングは、PSIRT プログラムの一部としては考慮されておらず、PSIRT のプロセス外で処理される。しかし、PSIRT は、安全な製品を市場に提供するために必要な中心的な存在であり、トレーニングが適切に行われていることを確認するために、様々な開発チームと提携する必要がある。また小規模な組織の多くは、セキュアな製品開発状況を確認する独自組織は存在しないこともある。そのような場合、PSIRT はギャップを埋めることに関与する可能性があるが、本書では範囲外とする。

各セクションでは、様々なステークホルダのグループを特定し、PSIRT がステークホルダの訓練と教育について有意義な議論を行うために、重点的に実施する分野をまとめる。PSIRT は、社内のすべてのトレーニング教材を作成したり、外部の教材を使用したり、外部のトレーニングリソースを使用したりしてステークホルダを育成することが可能である。

サービス 6.1 PSIRT のトレーニング

PSIRT スタッフはセキュリティの世界で起こっていること（最新のトレンドや新たな悪用、業界活動を含むがこれに限らない）の最前線にいる必要がある。この幅広い知識は主要なセキュリティ認定で示されているように、一般的なセキュリティトピックを理解し、確固たる基礎を築き上げる必要がある。しかし、セキュリティ認定は常に更新をしていくための基礎を提供するにすぎない。例えば、セキュリティに焦点を当てたカンファレンスや業界コンソーシアムへの関与、ブログ、広報、コンソーシアムの出版物、熱心な一消費者として業界全体に対する認識を持つことなど、これらによって更新をしていく必要がある。また、PSIRT のメンバーはセキュリティとプライバシーに関する法律について、世界で絶え間なく変化していることも認識する必要がある。

機能 6.1.1 技術的なトレーニング

PSIRT のスタッフは、サポートされている製品の基本的なセキュリティの概念と知識を深く理解していることが重要である。セキュリティの状況が変化するにつれて、新しい脆弱性

に関する技術がトレーニング資料に確実に含まれるよう、トレーニング資料を定期的にレビューする必要がある。

> **目的:** 報告されている問題を理解し、修正プログラムの開発、テスト、リリースを担当するチームに引き渡す前に、最初のトリアージを適切に実行できるようにPSIRT スタッフを訓練する
>
> **成果:** PSIRT スタッフは、職務を遂行するに十分な技術訓練を受けられる

セキュリティコンセプトトレーニングは、ベンダがサポートしている製品の種類(ハードウェア、ファームウェア、ソフトウェア、ネットワーク、クラウド製品など)によって異なる。高い次元では、一般的な攻撃手法、暗号技術、機密性、完全性、可用性、認証、認可、アクセス制御モデル、マルチテナント、関連するコンプライアンス、その他の規制などの基本的なセキュリティトピックを取り扱う必要がある。このトレーニングには、ヘルスケア業界のHIPAA やクレジット決済関連ベンダや銀行向けの PCI DSS など、PSIRT の活動に影響を与える可能性のある業界固有の規制も含まれる。報告された問題を理解できるように、PSIRT のスタッフには製品に関するトレーニングもカバーする必要がある。

機能 6.1.2 コミュニケーショントレーニング

PSIRT への外部発見者からの問題報告に備えて、PSIRT スタッフは、外部の発見者や社内のステークホルダとのコミュニケーションを適切に対処する方法を含む、コミュニケーションポリシーと対人的な能力をトレーニングしておくことが重要である。

> **目的:** PSIRT のスタッフが組織のコミュニケーションポリシーに従って外部組織と対話し、不適切なコミュニケーションに起因する規制/法的な問題を排除する
>
> **成果:** PSIRT スタッフは、あいまいさを伴わない明確かつ正確なコミュニケーションが行うことができ、割り当てられた任務を遂行するのに十分なコミュニケーショントレーニングを受けられる

機能 6.1.3 プロセスのトレーニング

報告された問題がどのようにトラックされ、管理され、測定されるかを定義するプロセスガイドラインが必要である。また報告された問題の解決プロセスに関わる様々なステークホルダの役割を定義する必要がある。このプロセスでは、発見者にタイムリーに対応し、対応

しているすべての問題について定期的な更新を送信する必要がある。また、外部発見者とベンダとの間で情報を伝達する明確かつ安全な手段が必要である。

> **目的:** 製品のセキュリティインシデントを管理する際にスムーズな情報フローがあることを確認し、タイムリーに問題を解決する
>
> **成果:** PSIRT スタッフは、内部のプロセスを十分に訓練し、それぞれの任務を遂行することができる

機能 6.1.4 タスクツールのトレーニング

サブ機能 6.1.4.1 PSIRT およびエンジニアリングスタッフ用のバグトラッキング・その他の管理ツール

組織が提供するそれぞれの製品(すべての製品で同じであることが好ましい)について、正式に承認されたバグトラックツールを利用する必要がある。このツールではセキュリティバグを一様に識別し、すべてのバグを把握する必要がある。なお、必要なユーザだけが、製品の脆弱性に関する情報にアクセスできる制御をする必要がある。さらに、このツールには、手動および自動のいずれのレポート機能を備えたプログラムメトリクス要件をサポートする機能が含まれている必要がある

> **目的:** 認定されたトラッキングツール内で、案件が効果的に管理され、脆弱性情報は必要のあるもののみがアクセス、トラック、管理できるように保護されるようにする
>
> **成果:** PSIRT スタッフは、職務を遂行できるツールについて十分に訓練され、知識を有する

サブ機能 6.1.4.2 サードパーティトラッキングツール

ほとんどの製品には、製品とともに出荷される複数のサードパーティコンポーネント(オープンソースを含む)が含まれている。客は製品に含まれているサードパーティのソフトウェアについて往々にして知らないため、変更に伴う修正や情報提供はベンダに依存する。そのため、サードパーティの様々なトラッキングツールを使用し、サードパーティの様々なコンポーネントに対するベンダの製品の依存性を理解しておくことが重要である。サードパーティのコンポーネントの脆弱性と修正を追跡するために、 NVD (National Vulnerability

Database)、サードパーティベンダのセキュリティアドバイザリおよびその他の外部サイトを監視して、これらの修正プログラムを顧客に提供する必要がある。

> **目的:** 製品に組み込まれたサードパーティのコンポーネントをトラックするためのツールを特定し、これらのコンポーネントの脆弱性をトラックおよびリリースできるようにする
>
> **成果:** PSIRT スタッフは、出荷された製品内のサードパーティコンポーネントを理解し、追跡できるようになる

機能 6.1.5 すべてのトレーニングの取り組みをトラッキング

PSIRT は、様々なステークホルダが利用出来るすべてのトレーニングをトラックする必要がある。PSIRT は、セキュリティ環境の急速な変化に対応し、トレーニングやプロセスを継続的に再定義する必要がある。そのため、これらのトレーニングがすべて一定の頻度で確実に行われるようにする必要がある。

> **目的:** 様々なステークホルダのためのすべてのトレーニングがトラックされることを確認する
>
> **成果:** PSIRT スタッフは、様々なステークホルダが PSIRT プロセスでの役割について訓練されていることを知ることができる

サービス 6.2 開発チームのトレーニング

安全な開発とは、ソフトウェア関連製品やサービスに残される脆弱性の数や深刻度を低減させるための方法論や、開発プロセス全般にわたり行われるさまざまな活動をさす。強力なカリキュラムと安全な開発方法論にしたがうことで、製品リリース前に脆弱性を大幅に削減することができる。これは、製品が市場にリリースされた後の対応に比べるとはるかに安価である。

安全な開発は、製品要件とアーキテクチャから始まる。さらに、安全なデザインレビューは、製品開発が始まる前に、潜在的な脆弱性を突き止めるための鍵となる。

安全な開発プログラムに関わる多くの活動があるが、詳細は本ドキュメントの範囲外であ

る。適切にセキュアな開発ライフサイクル（SDL）の取り組みを管理するためには、別のプログラムが存在することを強く推奨する。このプログラムは、受け入れられている業界標準のプログラムモデルに従うべきである。セキュアな開発ライフサイクル（SDL）の例は、Microsoft セキュアな開発ライフサイクルモデルである。

> **目的:** セキュアなコードを記述でき、文書化されたセキュリティガイドラインを使用して開発を行い、製品のアーキテクチャと設計を作成する適切なセキュア開発ライフサイクル(SDL)プログラムを組織に奨励する
>
> **成果:** 開発チームは安全なコードを書いてより安全な製品をリリースすることができる

セキュアな開発訓練は、 PSIRT 活動の一部として常に考慮されているわけではなく、PSIRT プロセスの外で処理される可能性がある。いずれにしても、製品の安全性を気にするベンダが考慮すべき重要なステップである。

機能 6.2.1 PSIRT プロセスのトレーニング

開発プロセスの各メンバーは、PSIRT プロセスがなぜ存在するのか、どのように機能するのか、そして PSIRT プロセスを支援するための製品開発として何をする必要があるのかを理解する必要がある。製品がリリースされた後は、開発チームは異なるプロジェクトに移行し、継続的な努力は最小限に抑えられる。PSIRT が製品の脆弱性の問題に完全に対処するためには、チームをトレーニングし、製品に関する重要な情報を格納するための適切な方法を提供することが重要である。PSIRT がリスクを評価し、軽減策を開発するために最もよく知っている人に戻すことができるよう、セキュリティアーキテクト、開発責任者、テストリードなどの情報を記載する。このドキュメントには、使用されているサードパーティのコンポーネントとは何か、製品の更新プロセスとは何か、ログが存在するかどうか、セキュリティの例外が許可されたかどうか、どのようにステークホルダに知らされているかを含む必要がある。この情報は、PSIRT がセキュリティ上の脆弱性を対処するためにも重要である。また新しい開発チームのメンバーが出入りするに伴い、新人のトレーニングも重要である。

> **目的:** すべてのステークホルダが PSIRT のプロセスを理解し、どのように製品開発において役割に関係しているかを確認する
>
> **成果:** 開発者間のセキュリティ文化と脆弱性に対するより良い協力を得られる

サービス 6.3 診断チームのトレーニング

診断担当者は、ペンテスト、脆弱性スキャン、ファジング、倫理的ハッキングなどの最新ツールと技術について常に把握しておく必要がある。診断担当者のトレーニングはセキュア開発ライフサイクルの問題であるが、本ドキュメントの対象外とする。しかし、PSIRT は、組織がトレーニングについて集中的に取り組むグループを設置するよう努力するべきである。

> **目的:** 組織が、適切なセキュリティテストツールの特定を含む、適切なセキュア開発ライフサイクルプログラムを持つことを奨励する
>
> **成果:** 高品質でより安全な製品

セキュアな開発と同様に、セキュアな検証トレーニングは PSIRT 活動の一部とはみなされず、PSIRT のプロセス外で処理される。しかし、それはベンダによって製品のセキュア開発ライフサイクルの一部として、カバーされなければならない重要なステップである。

機能 6.3.1 PSIRT プロセスのトレーニング

検証チームのメンバーの中には、製品の脆弱性を修正するために必要な修正プログラムのテストに携わるものがいるかもしれない。これらのチームメンバーは、PSIRT のプロセス、仕組み、予想される時間枠とそのプロセスにおける役割について理解する必要がある。製品のライフサイクルをよく理解している必要があり、彼らは脆弱性の修正テストが必要なサポートしている製品のバージョンを知っている。回避策がある場合は、回避策もテストする必要がある。リグレッションのテスト(回帰テスト)を実施することも重要である。

> **目的:** すべてのステークホルダが PSIRT のプロセスを理解し、製品の検証におけるその役割と関係を確認する
>
> **成果:** 検証者間のセキュリティ文化と脆弱性対処におけるより良い協力が得られる

サービス 6.4 すべてのステークホルダへの継続的な教育

すべてのステークホルダは、PSIRT プログラムの一定レベルの訓練と理解が要求される。すべての PSIRT プロセスには多くのステークホルダが関わっている。従って、様々なステークホルダグループを特定し、ニーズに応じたトレーニングを開発することが重要である。

目的: すべてのステークホルダグループが、PSIRT プログラムでの役割を果たすため、必要な訓練または基本的な意識を持っていることを確認する

成果: 内部の関係者が、緊急の脆弱性問題を解決、管理する際に PSIRT とどのように連携するか、また PSIRT がそのような状況でどのようなサービスを提供するかを知っている

機能 6.4.1 経営層のマネジメントに関するトレーニング

このグループは、通常、会社のコミュニケーション、脆弱性の保護およびその他のポリシーの承認に関係している。セキュリティアドバイザリを作成するには、管理者の承認が必要な場合もある。経営層の承認はリスクの高い危機的な状況や、非常に目立つ状況や、重大な責任を伴う状況でしばしば必要となる。また、管理者は、すべての製品のセキュリティ状態に関する定期的なステータス確認が必要な場合がある。 従って、PSIRT プロセスの管理者に通知することが重要である。

目的: 管理チームが PSIRT プログラムでの役割を認識できるようにする

成果: 管理者の承認を必要とする際のタイムリーな問題解決

機能 6.4.2 法務チームの教育

法律は最初の企業ポリシー策定に関与している。発見者の報告には法的問題があることがあり、法務グループからの援助が必要な場合がある。そのため、事前に連絡先を特定することが重要である。

目的: PSIRT プログラムおよび関連するタイムラインでの役割を法務部門に認識させる

成果: 法的な承認を必要とするセキュリティ問題の適切な開示ができる

機能 6.4.3 政府関係者、コンプライアンスチームの教育

政府職員は、企業コンプライアンスの問題に関与している。従って、事前に連絡先を特定することが重要である。

目的: 政府関係者に、PSIRT プログラムにおける彼らの役割を認識させる

成果: 特定の規制基準に遵守する必要がある脆弱性のタイムリーな解決

機能 6.4.4 マーケティングチームのトレーニング

マーケティングはブランドに対するリスクがあるときにしばしば関与する。また、セキュリティアドバイザリがレビューされ、関連するマーケティング情報が一緒にリリースされる場合がある。マーケティングチームは製品のセキュリティ面にも携わっている。

目的: マーケティングチームに PSIRT プログラムにおける彼らの役割を認識させ、製品セキュリティに関して主張できることとできないことを教える

成果: PSIRT とマーケティングチームとの適切な調整によって、マーケティング資料とセキュリティアドバイザリの間に整合性のとれたセキュリティ姿勢を外部に示すことができる

機能 6.4.5 広報チームのトレーニング

広報(PR)チームは、外部のセキュリティポストやブログへの対応、または重大な製品の脆弱性に関する問い合わせ対応を行う責任がある。連絡先を特定して、外部の投稿が必要な場合には PR が関与する必要がある。

目的: 広報チームが PSIRT プログラムでの役割を認識できるようにする

成果: PSIRT と PR チームとの間の適切な調整によって、ベンダの良い外部セキュリティの姿勢が得られる

機能 6.4.6 セールスチームのトレーニング

営業チームはセキュリティのコンセプトやコミュニケーションについて訓練を受けることが可能である。また外部との共有可否について認識しておくことは重要である。営業担当者はステークホルダや潜在的顧客のセキュリティに関する懸念について、直接的に対処するのではなく、PSIRT スタッフまたはサポートスタッフに対応を求めることが推奨される。

> **目的:** 製品のセキュリティに関して主張できることとできないこと、回答できない質問をどこで対応すべきかを認識できるようにする
>
> **成果:** PSIRT と営業チームとの適切な調整によって、顧客の期待に応えることができる

機能 6.4.7 サポートチームのトレーニング

サポートチームは顧客からの脆弱性報告に対処できる訓練を受けなければならず、問題解決には PSIRT の関与が必要な場合がある。またサポートは、すべての製品の有効期間、サポートされているバージョン、およびセキュリティアドバイザリが公開されるかどうかを定義する、ポリシーを公開する必要がある。ほとんどのベンダはサポートされているバージョンのセキュリティアドバイザリのみを公開している。そのため、これらのポリシーはベンダのウェブサイトに公開して、ステークホルダが容易に参照可能にする必要がある。サポート担当者が顧客からの脆弱性報告に関する問題の種類を理解できるよう、典型的な PSIRT は彼らと緊密に連携をとる。また発見者が顧客である場合もあるので、問題への対処はサポートと PSIRT の間で移行する可能性がある。

> **目的:** サポートチームに PSIRT プロセスにおける役割を認識させる
>
> **成果:** PSIRT チームとサポートチームとの間の適切な連携によって、顧客と問い合わせ対応者の両方の期待に応えることができる

サービス 6.5 フィードバック機能の提供

インシデントの根本原因の分析中に得られた情報を使って、関係者を教育し、似たような脆弱性インシデントが発生しないように予防する。

目的: セキュリティ業界の急速な変化に対応し、維持し続けるために継続的にトレーニングを改善する

成果: より高い品質のトレーニングは、すべてのステークホルダの経験を向上させる

Annex 1: Supporting Resources

- Architecture Content Framework
- ISO 31000:2009 Risk management - Principles and guidelines
- ISO/IEC 27000/2018 Information technology - Security techniques - Information security management systems
- ISO/IEC 30111:2013 Information technology - Security techniques - Vulnerability handling processes
- ISO/IEC 29147:2014 Information technology - Security techniques - Vulnerability disclosure
- Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure
- The Project Management Body of Knowledge (PMBOK) Guide and Standards

Annex 2: Acknowledgements

- Barbara Cosgriff, MetLife
- Beverly Finch, Lenovo
- Carl Denis, Siemens
- Chris Robinson, Red Hat
- Jeff Hahn, Honeywell
- Jerry Bryant, Microsoft
- Josh Dembling, Hikvision
- Jean-Robert Hountomey, Brocade
- Kevin Ryan, NetApp
- Krassimir Tzvetanov, Fastly, Inc.
- Langley Rock, Red Hat
- Lisa Bradley, Nvidia
- Pete Allor, Honeywell
- Reshma Banerjee, Oracle
- Rupert Wimmer, Siemens
- Steve Brukbacher, Johnson Controls
- Tania Ward, Dell EMC
- Vic Chung, SAP

Annex 3: Tables and Illustrations

Annex 4: Pros and Cons of PSIRT Organizational Models

モデル	説明	メリット	デメリット
分散モデル	小規模に分散したコアPSIRTオペレーションを、さまざまな組織にPSIRT機能を持たせて活動をするモデルである。（例：サポート、エンジニアリング、プロダクトマネジメントチームがPSIRT活動を分散させて実施する。）	・大規模で多様な製品ポートフォリオを持つ大企業に最適である。 ・PSIRT設立の初期費用が少なくて済む。 ・作業負荷が異なる組織に分散される。 ・拡大するポートフォリオにおいて拡張可能なスケーラビリティを確保できる。	・PSIRTは、ポリシーと方向性を決定するなんらかの権限をもつべきであるが困難になる。 ・多くの場合、PSIRTは脆弱性に対応するリソースを直接制御せず、管理が難しくなる。 ・PSIRT活動より、別の製品に関する活動が優先される可能性がある。
集中モデル	すべてのさまざまな製品分野について、PSIRTのすべての活動（プログラム管理、トリアージ、識別、改修、コミュニケーションなど）に直接関与する、より大きなPSIRT組織である。	・小規模なポートフォリオを持つ中小企業に最適である。 ・高度に熟練した製品セキュリティ専門家による集中管理グループ。 ・PSIRT組織は、PSIRTの予算、ポリシー、およびリソースに関するすべての決定を行う。 ・PSIRTの運用活動に関するより優れたコントロールと説明責任を果たすことができる。	・ポートフォリオが拡大するにつれて機能しにくくなる。 ・他組織のマネージャーの協力または承認を得て、主要な決定を行う必要がある。 ・専門スキルを持つ集中モデルのチームを維持するのにコストがかかる。
ハイブリッドモデル	集中モデルと分散モデルの両方の特性を持ったモデルである。		

Table 2: Pros and Cons of PSIRT organizational models

Annex 5: Types of Incident Response Teams

- **国際連携 CSIRT** - 国際連携 CSIRT は、サイバーセキュリティインシデントの国家レベルの調整を実施するために国家機関によって構成されている組織を指す。その管轄には通常、政府機関や法執行機関、市民組織が含まれる。また、一般的には、他国の国際連携 CSIRT や国際的/地域的なサイバーセキュリティに関する関係者と交流する機関でもある
- **重要インフラ/セクタ別 CSIRT** - 特定のセクタ（エネルギー、電気通信、金融など）に関連するサイバーセキュリティインシデントの監視、管理、および対応を担当する
- **企業（組織）内 CSIRT** - 企業内 CSIRT は、一般的に特定の組織内の ICT インフラストラクチャとサービスに影響を及ぼすサイバーセキュリティインシデントの監視、管理、および対応を担当するチームを指す
- **地域/複数組織 CSIRT** - 地域/複数組織 CSIRT は、特定の地域または複数の組織に関連するサイバーセキュリティインシデントの監視、管理、および対応を行うチームまたは混合チームを指す
- **製品セキュリティインシデント対応チーム（PSIRT）** - 営利組織（典型例はベンダー）内のチームであり、当該組織が提供する製品やサービスに関するセキュリティ脆弱性情報の受領、調査、内部や外部への脆弱性情報の報告を管理するチームである

用語集

- **アクション** - 何かが様々なレベルの詳細さ/成熟度でどのように行われているかを示すリスト
- **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測定可能な活動。本ドキュメントにおいては、より広範なサービスと定義することも、必要な機能、タスク、アクションの集まりと定義することもできる
- **キャパシティ** - 組織がリソースの範囲内で実行できる特定のケイパビリティの同時プロセス数
- **成熟度** - 組織が組織のミッションと権限の範囲内で、あるケイパビリティをいかに効果的に実行するか。これはアクションやタスク、または機能やサービスの集合体で達成された熟練度である
- **レッドチーム** - ネットワーク/システムの脆弱性を検出し、システム/ネットワーク/データに対して攻撃者のようなアプローチを用いてセキュリティをテストするプロセス。このプロセスは、究極の目的はセキュリティを強化することであるため、「エシカルハッキング」とも呼ばれる
- **タスク** - タスクを完了するために実行する必要のあるアクションのリスト