プロダクト脆弱性対策・対応成熟度シート

Version 1.1

この成熟度シートは、「PSIRT Services Framework Version 1.0 日本語版」をもとに、PSIRT Services Framework の各フレームワークの目的達成過程の状態を成熟度レベル毎に示したものです。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

はじめに

プログラム開発事業やソフトウエア販売等に関わる企業において、製品の脆弱性管理は重要な課題となってきました。この成熟度シートは自社開発製品または自社販売製品に関する脆弱性管理を課題として扱い始めた組織、または製品セキュリティ・インシデント対応チーム（PSIRT）の設立を進めている組織、もしくは PSIRT 業務の品質の向上を目的に、現状評価や課題の洗い出し、施策の方向性を検討する材料として利用して頂きたいものです。
2018 年にリリースされた、PSIRT Services Framework Version 1.0 日本語版では、PSIRT のあるべき姿をサービスエリア毎に詳細に記述してありますが、組織の規模や製品販売対象範規模の違いなどで、要件としてそのまま自組織に当てはめるには難しい面も散見されます。この成熟度シートは PSIRT Services Framework の理解を助けると同時に、目標とする成熟度レベルを自ら設定し、中小規模のビジネスにおいても参考となるよう配慮しました。

利用の仕方

まずは、各フレームワークの目的を確認したうえで、外部環境や自社のビジネス状況から目標を設定してください。（※1）その後、自組織の現状把握のため、ティア 0（※2）の内容から順に上位のティアに向けて記述を読み、自組織がどのティアにも最も近いかという観点で採点してください。目的の内容が明らかに業務範囲外であればそのフレームの目標を 0 に設定してください。目標と採点結果のギャップを分析し、行動計画を策定することを推奨します。採点は定期的(半年～1 年に 1 回)、あるいは組織改革や業務改革実施後、インパクトの大きいインシデントを対処した後などが適切です。

※1 目標の設定方法は、本書 P4 を参照してください。

※2 記述の中に、サービスエリアの番号を記載しました。「PSIRT Services Framework Version 1.0 日本語版」を参考にしてください。

(https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.0_jp.pdf **)**

注意事項

・文中に「PSIRT」が主語として多く記述されていますが、「PSIRT」という組織が存在しなくても、PSIRT の一部の機能や脆弱性管理責任を持つ組織や個人が存在すれば、それを当てはめて評価してください。
・記述内容や用語が理解できない場合は、「PSIRT Services Framework Version 1.0 日本語版」の内容や用語の定義を確認してください。

ティアについて

この文書中のティアの概念は、NIST が公開している Cyber Security Framework 1.1 (※1) のインプリメンテーションティアの定義を参考に作成しています。

・ティア０　何もしていない

該当のサービスエリアについて、必要性の認識がなく、いかなる活動も実施していない状態のこと。

・ティア１　部分的である（Partial）

プロセスが定められておらず、場当たり的に事後的に対応がされている状態のこと。

脅威情報などは、一部のメンバーが確認することがあるが、ケースバイケースで流通したりしなかったりする。

・ティア２　リスク情報を活用している（Risk Informed）

リスクに対して意識が高く、プロセスが経営層などより承認されているが、全体のポリシーまで浸透しておらず、繰り返し適用可能な状態には至っていない。

脅威情報などは、非公式的に一部の層に流通しており、適切に処理はされているが繰り返し適用ができる状態までには至っていない。

・ティア３　繰り返し適用可能である（Repeatable）

プロセスがポリシーとして全体に浸透しており、繰り返し適用可能で、外部状況の変化に応じてポリシーが定期的に更新されている。

脅威情報は、手順が定められており、継続的に正確にモニタリングされている。

・ティア４　適応している（Adaptive）

プロセスが現在の状況や過去の教訓から調整され、最新のサイバーセキュリティ技術と実践に進んで順応し、高度化する脅威にタイムリーに対応している。

脅威情報は経営層に共有され、他の経営リスクと同様にモニタリングされるなどサイバーセキュリティリスクマネジメントが組織の文化となっている。

※1 IPA が公開している NIST Cyber Security Framework 日本語翻訳 (https://www.ipa.go.jp/files/000071204.pdf)

目標の設定について

どの PSIRT Services Framework のサービスエリアに、どの程度のティアを目標として定めるかは、外部環境、組織/事業の規模、提供しているサービスの形態/利用者像、組織のリスクに対する許容度などによって変わってきます。この目標設定は、経営層の判断が極めて重要です。目標の設定は PSIRT 活動を実施している担当者が設定するケースが多いと思いますが、経営層のレビューや承認プロセスを経て目標の設定をすることが望ましいです。

外部環境

外部環境とは、攻撃者の攻撃の高度化、組織の顧客が製品セキュリティに対して求める要求が高まり、外部から脆弱性報告を多く受けているか、などです。業界として攻撃ターゲットとなり攻撃が高度化し、顧客のセキュリティ要求の高まりがあれば、「脆弱性の発見」、「脆弱性の開示」、外部から脆弱性の報告を多く受けている場合は、「脆弱性情報とトリアージと分析」に関するサービスエリアのティアをあげることを推奨します。

組織/事業規模

組織/事業規模が拡大するにつれ、ステークホルダが多くなります。規模が大きくなるにつれ、「ステークホルダマネジメント」、「脆弱性情報のトリアージと分析」、「脆弱性の開示」、「トレーニングと教育」などのサービスエリアのティアをあげることを推奨します。

提供しているサービスの形態/利用者像

提供しているサービスが多くの製品に組み込まれるコンポーネントなのか、1 社のみに提供しているオンプレ製品なのか、アップデートを自社で完結できるクラウドサービスなのかによって「対策」、「脆弱性の開示」などのサービスエリアの目標が変わってきます。自社のみで対策が完結するようなサービスや、特定の組織のみに提供しているサービスであれば「脆弱性の開示」のサービスエリアは最小限のティアで問題ないでしょう。多くの組織がオンプレミスで利用し、アップデートの適用に顧客またはステークホルダの協力が必要なサービスであれば「脆弱性の開示」は高いティアが求められます。

リスクに対する許容度

提供しているサービスが侵害された場合に、社会に与える影響が大きいが小さいか、レピュテーションリスクの想定、損害を補償するだけの財源が組織に確保されているかによって、全体のサービスエリアのティアに求められる要求が変わってきます。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

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

1.1 内部のステークホルダ管理

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は調整を促進する。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
脆弱性に関する管理の柱として PSIRT は必要とされていない。又は、必要と認識しながらも経営者は組織内にその機能を持つ為のリソースは提供していない。	一部の担当者は PSIRT の必要性を感じており、業務で顕在化した脆弱性情報に関して限られた相手に情報共有し、業務範囲や既存の業務分掌を超えたなかで対処している。	PSIRT と内部ステークホルダとのコミュニケーションの重要性に気がつきはじめ、インシデント対応プロセスは徐々にパターン化している。経営者とも意識を合わせ、製品は顧客が利用することで初めて価値が生み出されると感じている。	[1.1.1]PSIRT が組織として、その責任者や機能、役割が文書化され周知されている。内部ステークホルダとしては、経営層、広報・CC、法務部門、開発部門、営業部門などが定義されている。 [1.1.3]インシデント事後対応プロセスの構築が構築されており、脆弱性の対応について振り返り、課題を設定するプロセスがある。	PSIRT の存在が組織全体に共有され、製品の脆弱性に対応することが組織の文化となっており、環境の変化に応じて PSIRT のポリシーが適時見直されるなど環境に適応した組織となっている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

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

1.2 発見者のコミュニティとの交流

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Rick Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
組織外の脆弱性の発見者と積極的に交流する必要性は感じていない。また、交流活動が脆弱性公開のための対応を準備する助けとなることに気づいていない。	PSIRT は[1.2.1]特定の適切な発見者とプライベートな契約を締結することや、[1.2.4]会議やその他のイベントにおけるセキュリティ発見者との交流や、[1.2.1]セキュリティ上の欠陥やトピックスに関する学術研究を後援することが脆弱性情報公開のための対応を準備する手助けになると、担当者は気づき始め、一部のメンバーが非公式的にイベントなどに参加している。	発見者との交流、イベントへの参加に関しては、関連する部門の業務として明記されてはいないが、部門内で必要とされ適宜実施されている。	[1.2.1]特定の適切な発見者とプライベートな契約を締結することや、[1.2.4]会議やその他のイベントにおけるセキュリティ発見者との交流や、[1.2.1]セキュリティ上の欠陥やトピックスに関する学術研究を後援することなどが、ポリシーとして推奨される、もしくは予算化されるなどで公式的に交流している。	[1.2.1]特定の適切な発見者とプライベートな契約を締結することや、[1.2.4]会議やその他のイベントにおけるセキュリティ発見者との交流や、[1.2.1]セキュリティ上の欠陥やトピックスに関する学術研究を後援することなどが、公式的に実施され、必要あれば突発的なイベントの後援などの対応も実施していくことが組織文化となっている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

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

1.3　コミュニティと組織の交流

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
第三者、サプライヤ、上流のベンダ、OEM などのパートナーから調達したコードやコンポーネントの中に脆弱性が発見された際の、組織内の連携について何も検討されていない。	パートナーから調達したコードやコンポーネントの中に脆弱性が発見された際に対応が必要と考え、情報収集方法を考え、調達先のコミュニティやイベントに参加するメンバーが出てきている。	PSIRT は[1.3.1.2]他の PSIRT、セキュリティベンダやバグバウンティベンダとの交流やカンファレンスイベントなどの積極的な参加などによる活発な対話の中で、有用と思われるコミュニティやパートナーとのチャネルを見つけるようになってきており、有用な情報は組織内の役割にしたがって連携するようになっている。	[1.3.1.1]調達先から脆弱性の報告を受け処理するための NDA などが締結されている。 [1.3.1.2]有用なコミュニティチャネルでの活動に必要なリソースが予算化されている。 どのコミュニティと交流するか、情報連携方法についてポリシーが定めてあり、繰り返し実施可能な状況にある。	調達先との情報連携が頻繁行われ、過去の対応の教訓からプロセスが調整され、情報連携による対応がタイムリーに実施できる。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

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

1.4 下流のステークホルダマネジメント

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
自社製品のバグやセキュリティ脆弱性に関する情報を提供するために下流ステークホルダとの良好な関係の構築に関心がない。	PSIRT の一部の担当者は個人的に製品のバグやセキュリティ脆弱性に関して日頃から交流のある下流のステークホルダと情報の共有や対応をしている。しかし、PSIRT の担当者の対応は場当たり的であり、重要な情報が必ずしも提供されているとは限らない。	組織の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が確立され始めている。 脆弱性の改修やサポート期間については明確なポリシーはなく、都度設けられる会議によって個別に決められる。	[1.4.1.1]明確な製品ライフサイクルとサポートポリシーを確立するために、脆弱性の改修やサポート期間についてポリシーが定義され文書化されている。 [1.4.1.2]下流のステークホルダとの交流について、良好な関係を構築することが有効であると認知されている。脆弱性の関する情報やインシデント対応の情報を伝達するため、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ための運用について文書化されている。	[1.4.1.1]脆弱性の改修やサポート期間については明確なポリシーが定義されており、かつ下流ステークホルダとの適切な対応について常に検討されている。 [1.4.1.2]脆弱性の関する情報やインシデント対応の情報を伝達するため、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ための運用について改善が行われ、PSIRT と下流ステークホルダとの間に信頼関係が生まれている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

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

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

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情報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さまざまな形（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にかつタイムリーかつ正確に提供する。

ティア 0	ティア 1 (Partial)	レベル 2 (Risk Informed)	レベル 3 (Repeatable)	レベル 4 (Adaptive)
PSIRT 設置の有無に関わらず、セキュリティ・インシデントに対する旗振り役がどの組織（または個人）であるか明確であることや、対応状況の把握、次のステップのための妥当な判断材料などの提供など、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に提供する必要性に誰も気づいていない。	セキュリティ・インシデント対応状況の把握、次のステップのための妥当な判断材料などの提供など、PSIRT が提供するべき基本的なインシデント対応のための仕組みが必要であることが、議事録、組織内のポータル、メーリングリストやチャット等で一部の関係者が情報を共有しているが、旗振り役は場当り的である。	インシデントオーナーは決まった組織あるいは個人によって実施され、インシデント対応時にステークホルダと十分なコミュニケーションを得るために必要な通信チャネルが検討されているが、情報の種類や整理方法、また秘密裏に運用されるよう必要最小限の共有に関する仕組みまでは検討されていない。 情報の共有に関する仕組みは、一定の方法で定着しつつあるが、利用者の選定、アクセスコントロール、認証などの運用方法が適切であるかどうかは議論されていない。	インシデント対応時にステークホルダと十分でリアルタイムにコミュニケーションを得るために必要な通信チャネル、共有のルール、機密保持対策がポリシーとして定義されている。 ・[1.5.1]コミュニケーションチャネルを提供する。 ・[1.5.2]安全なコミュニケーションの管理方法を提供する。 ・[1.5.3]脆弱性トラッキングシステムにおけるセキュリティ脆弱性の収集、分類、ルーティング、優先順位づけのプロセスの提供。	インシデントに関するコミュニケーションのポリシーが存在し運用されており、かつそのポリシーが有効に機能しているかを測定し、常に改善するサイクルが回っている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

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

1.6 表彰と謝辞による報酬を発見者に与える

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
PSIRT 設置の有無に関わらず、謝辞を示すことにより、製品の脆弱性の発見者との信頼関係を築くことが重要であることが理解されていない。	一部の担当者は、発見者に対して謝辞を示す、もしくはなんらかの報酬が与えられるよう都度配慮しているが、その方法は場当たり的であり、関係者個人により異なる。	PSIRT の慣習として、[1.6.2]パブリックセキュリティアドバイザリ、ソフトウエアリリースノート、CVE テキストで、発見者への謝辞を含めることが当たり前となっている。	組織のポリシーとして、発見者への謝辞の公開や、報奨プログラムが開始され、予算が組まれている。 ・[1.6.1.1]リリースノートなどへの記載 ・[1.6.2]発見者への報奨制度	組織の機能として、[1.6.2]脆弱性発見者への報奨プログラムは繰り返し見直しがされ、発見者との信頼関係の醸成に有効な施策となっている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

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

1.7 ステークホルダメトリクス

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
PSIRT は、組織内外のステークホルダに活動指標や成果を報告することの重要性に気付いておらず、活動していない。	一部の担当者は、組織内外のステークホルダに関わらず PSIRT 活動指標や成果を報告したりしているが、場当たり的に実施されているに留まる。	PSIRT は一部ステークホルダの要求などにより活動指標や成果を報告しているが、定期的に実施するようなポリシーまで定められていない。	各ステークホルダがどのような情報が必要かを[1.7.1]理解するため、ミーティングやアンケートを実施し記録し、[1.7.2]メトリクスを収集し、[1.7.4]メトリクスを報告するポリシーが定められている。	[1.7.3]メトリクスデータの分析と見直しにより、メトリクスデータに適切な情報（背景、経緯、環境など）を添えることが必要であることを認識し、実行している。メトリクス情報の報告からのフィードバックを得て、適宜改善されている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア2/　脆弱性の発見

２．１　脆弱性報告の受付

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
ステークホルダ内外を問わず、脆弱性の報告の受け付ける必要性を感じていない。	組織内における[2.1.1.3]脆弱性の報告窓口担当は、特定の個人が実施しており、その個人の意識や業務状況によって受付業務の品質が異なる。また受理した情報の扱いは個人の管理能力にゆだねられている。	[2.1.1.3]脆弱性の報告窓口は特定の部署や担当者がアサインされており、窓口業務として必要な組織構造の設置やコンタクトポイントの宣伝などが実施されている。 受付の効率化のため、[2.1.1.1]報告の提出方法と様式が公開されているが、受け付けた脆弱性の取り扱い方法について確立したポリシーは定まっていない。	脆弱性の報告窓口について、[2.1.1.1]報告の提出方法と様式を定義しており、[2.1.1.2]コンタクト情報の詳細を公開し、Web サイトなどで周知されている。 ・[2.1.1.3]一般的なコンタクトポイントの登録も準備され、報告の暗号化についても対策されている。 ・脆弱性方法の取扱方法が定められており、[2.1.2.3]タイムリーな受理連絡や、[2.1.2.1]連絡可能な他のチャネルの監視も実施している。	外部への発見者へのレスポンスタイムは組織内で SLA が定義されており、状況をモニタリングし、SLA に反した場合には適切にリソースの再配分などの対応がなされている。また、[2.1.2.2]不正な報告を用いた攻撃の標的にされることを想定し、業務環境は堅牢化がなされ、報告を独立して取り扱う状態にある。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア2/　脆弱性の発見

２．２　報告されない脆弱性を特定する

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
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を通じて開示される脆弱性があることを認識しておらず、確認していない。	一部の担当者が都度[2.2.1]攻撃情報データベースや[2.2.2]カンファレンスプログラムを確認し、自組織の製品に影響があるものを情報共有しているが、実施は場当たり的である。	製品開発者が[2.2.2]製品に関連する内容のカンファレンスプログラムに参加し、[2.2.1]攻撃情報データベースの確認についてルール化し定常的に実施している。	製品開発者やその関係者が業務として、[2.2.1]攻撃情報データベースの監視や、[2.2.2]カンファレンスプログラムの監視、[2.2.3]高名な報告者による発表の監視、[2.2.4]マスメディアの監視を実施しており、その業務は全社的に周知されている。	製品開発者やその関係者が業務として、[2.2.1]攻撃情報データベースの監視、[2.2.2]カンファレンスプログラムの監視、[2.2.3]高名な報告者による発表の監視、[2.2.4]マスメディアの監視を実施しており、各監視対象の優先順位や効率化がなされている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア2/　脆弱性の発見

２．３　製品コンポーネントの脆弱性のモニタリング

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
外部コンポーネントに含まれる脆弱性について管理し、情報収取する必要性を感じていない。	製品開発者の一部が、[2.3.1]製品コンポーネントの目録を作成し管理しはじめた。	製品開発者の一部が、[2.3.2]サードパーティのアドバイザリのモニタリングをしはじめ、[2.3.5]組織内の開発チームへの通知がされはじめた。	以下のプロセスが定義され文書化されている。 ・[2.3.1]製品コンポーネントの目録 ・[2.3.2]サードパーティのアドバイザリのモニタリング ・[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 ・[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 ・[2.3.5]組織内の開発チームへの通知	以下のプロセスが定期的に見直され改善定義されている。 ・[2.3.1]製品コンポーネントの目録 ・[2.3.2]サードパーティのアドバイザリのモニタリング ・[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 ・[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 ・[2.3.5]組織内の開発チームへの通知。

外部コンポーネント：　脆弱性は大まかに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製品開発者の外部のリソース（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②③は外部コンポーネント。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア2/　脆弱性の発見

２．４　新しい脆弱性を見つける

目的：　外部組織が発見する前に製品の脆弱性を発見する。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
外部組織が発見する前に製品の脆弱性を発見することが、製品のセキュリティ問題への対処において、工数の削減になることに気付いておらず、活動していない。	一部の担当者は、製品の脆弱性について内部で発見し対処した案件がトータルコスト面で有利であることに気づき、脆弱性発見のための活動を行っている。	[2.4.1]脆弱性アセスメント(Red Team テスト、グレーボックス／ブラックボックスセキュリティアセスメント、リバースエンジニアリングなどの幅広いツールの使用)を導入し始めた。	[2.4.1]脆弱性アセスメント(Red Team テスト、グレーボックス／ブラックボックスセキュリティアセスメント、リバースエンジニアリングなどの幅広いツールの使用)の方法や、[2.4.2]セキュリティテストツールの専門知識の維持に関する管理方法について定義され文書化されている。	[2.4.1]脆弱性アセスメント(Red Team テスト、グレーボックス／ブラックボックスセキュリティアセスメント、リバースエンジニアリングなどの幅広いツールの使用)の方法や、[2.4.2]セキュリティテストツールの専門知識の維持に関する管理方法について見直しが定期的に行われ改善している。

レッドチームテスト：　実際のサイバー攻撃への対応を経験するもの。破壊的・妨害的な活動を避けながら、一般的なサイバー攻撃や高度な攻撃による模擬攻撃によって、資産を保護するための能力を診断すること

ブラックボックスセキュリティテスト：　アプリケーションの内部動作に関する知識がほとんどないかまったくない状態で、外部の攻撃者としてアプリケーションのセキュリティ制御・防御、およびデザインを外部からテストすること

グレーボックスセキュリティアセスメント：　テスターがソースコードを除く、システム構成情報、管理者情報などを受け取り、システム内部からの長期間に渡る攻撃をシミュレートすること

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア2/　脆弱性の発見

２．５　脆弱性発見のメトリクス

目的：　PSIRT 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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adoptive)
PSIRT のサービスに関する KPI を定め、ステークホルダの理解を得ることの重要性を理解しておらず、活動をしていない。	一部の担当者が、PSIRT サービスの向上を目的とした KPI を検討し始めたが、本務とは別に自発的に実施されている。	組織の管理する KPI が明確になってきており、一部の KPI が管理され始め、情報共有をしている。	以下の項目を KPI として管理され、ポリシーとして定義されている。 ・[2.5.1.1]発見された脆弱性と検証された脆弱性の総数 ・[2.5.1.2]サードパーティ製コンポーネント(OSS、ミドルウエア、OS 等)に落とし込まれた検証済みの脆弱性の総数 ・[2.5.1.3]CWE に落とし込まれた検証済みの脆弱性の総数 ・[2.5.1.4]脆弱性発見のアプローチ毎に細分化され発見された脆弱性の総数 ・[2.5.2.3]トリアージまでの時間 ・[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。	以下の項目を KPI として管理し、運用レポートとしてステークホルダに発行されており、継続的に見直し、改善が行われている。 ・[2.5.1.1]発見された脆弱性と検証された脆弱性の総数 ・[2.5.1.2]サードパーティ製コンポーネント(OSS、ミドルウエア、OS 等)に落とし込まれた検証済みの脆弱性の総数 ・[2.5.1.3]CWE に落とし込まれた検証済みの脆弱性の総数 ・[2.5.1.4]脆弱性発見において、細分化されたアプローチ毎に発見された脆弱性の総数。 ・[2.5.2.3]トリアージまでの時間 ・[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。

CWE: 共通脆弱性タイプ一覧 CWE（Common Weakness Enumeration） https://www.ipa.go.jp/security/vuln/CWE.html

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア3/　脆弱性情報のトリアージと分析

3.1　脆弱性の認定

目的：　組織は、対応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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
[3.1](製品の品質管理担当者)は、対処すべき問題の種類や範囲の基準を作成する必要性を感じていない。また、バグと脆弱性の違いが定義されておらず、脆弱性認定プロセスは存在していない。 [3.1.1] 最低限の許容可能なセキュリティ品質レベル（品質ゲート）や脆弱性の優先順位付け基準（バグバー）は存在していない。	[3.1]脆弱性か、そうでないかは、担当者のスキルや意思に任されており、脆弱性の性質に基づき網羅的、体系的に分類されてはいない。 [3.1.1]脆弱性の優先順位を決める取り組みが一部で実施され始めている。	[3.1]脆弱性の判定基準は存在するが、網羅的、体系的ではなく、組織の一部で共有されるにとどまっている。 [3.1.1]判定基準の文書化のフォーマットは部門ごとに異なる。また、特定の個人の知識に依存し文書化されていない場合もある。 [3.1.2]外部から寄せられた脆弱性情報をデータとして管理していない。従って、判定基準に反映されない場合がある。	[3.1]製品開発チームと品質保証部門が脆弱性の判定基準を定義している。バグバーは悪用可能な脆弱性を網羅しており、緊急とそれ以外に分類されている。品質ゲート（品質基準）は最低限許容可能なセキュリティ品質が定義されており、それに基づき製品はリリースされている。関係者は文書にとして共有されている。 [3.1.2]外部情報によって、定期的に改訂がされる。 [3.1.2.1]外部から寄せられた脆弱性情報をデータは反映されるが、バグバーや品質ゲートの粒度が粗いため、反映に時間がかかるなどや、反映されない場合がある。	[3.1] 組織として脆弱性の認定のためのセキュリティベースラインが定義されており、悪用可能な脆弱性とセキュリティ問題が区別されている。 バグバー（脆弱性定義）は緊急、警告、重要、注意に細分化されて区別され、品質ゲート（品質基準）は、最低限許容可能なセキュリティ品質が定義されており、それに基づき製品はリリースされている。 [3.1.2.1]脆弱性の報告は、データとして管理はされて、改訂のフィードバック情報とはなっている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア3/　脆弱性情報のトリアージと分析

3.2　発見者との関係構築

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
[3.2.2]特定の良質な報告者との関係維持に関心がないため、すべての報告は同一に扱われる。 [3.2.3]特定の報告者に良好な対応をする必要性を感じていないため、発見者プロファイルは作成されていない。 [3.2.4]報告者からの脆弱性レポートを迅速に評価する必要性を感じていないため、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は定義されておらず、公開もされていない。	[3.2.1]脆弱性の報告者への対応は担当者の意思に任されており、一部、良好な関係が構築される。 [3.2.3]発見者とは個人的な関係であり、最も良好な結果が得られるような対応が常時、行えるとは限らない。 [3.2.4]脆弱性レポート迅速に評価するための定義がないため、報告者と担当者との誤解、理解不足ための連絡工数が増え、トリアージが遅くなることがある。	[3.2.1]脆弱性を報告した個人及び組織に関するデータベースがあり、履歴や成果、処理事例を知ることができる。 [3.2.2]信頼性の高い報告者の存在は組織として知られているが、トリアージプロセスの効率改善にはつながっていない。 [3.2.4]脆弱性レポート迅速に評価するための定義はあるが体系化されていないため、情報不足による連絡工数が高く、トリアージに時間がかかる場合がある。	[3.2.1]脆弱性を報告した個人や組織のデータベースにより、一般公開の前に組織としての改修結果や内容が報告される。 [3.2.2]一貫性のある信頼性の高いごく一部の報告者の存在は組織として認知され、一般公開の前に組織としての改修結果や内容が報告される。 [3.2.3]報告者のプロファイルが整備され、連絡先、過去のプレゼンの成果や、手法、得意とする製品、インセンティブなどが、含まれており、報告者によるインシデント対応プロセスに違いがある。 [3.2.4]脆弱性レポートのガイドラインが定義され公開されている。	[3.2.1]脆弱性を報告した個人及び組織のデータベースがあり、履歴や成果、処理事例、やり取りの内容を知ることができる。特定の報告者のレポートに対しては、一般公開の前に組織としての改修結果や内容が報告される。 [3.2.2]一貫性のある信頼性の高い報告者の存在は組織として認知され、優先的にエスカレーションされ、トリアージの効率が高い。 [3.2.3]報告者のプロファイルが整備され、連絡先、過去のプレゼンの成果や、手法、得意とする製品、インセンティブなどが含まれており、報告者との対応をスムーズにさせることができる。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア３／　脆弱性情報のトリアージと分析

3.3　脆弱性の再現

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
[3.3](製品の品質管理担当者)は、脆弱性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性を感じていない。 [3.3.1]又は、再現するための技術的専門知識や再現環境の不備を理由に、再現性確認を実施していない。	[3.3.2]脆弱性を再現させるための決められた環境は無く、再現確認は必要性を感じた担当者のスキルや意に任される。[3.3.4]そのため、脆弱性レポート、PoC その他関連する情報を保護する対策は十分といえない。 [3.3.3]また、再現に必要なツールは十分でなく、作業効率は意識されていない。	[3.3.2-4]脆弱性を再現させるための環境整備や手法は一部の担当者に任され、そのプロセスはほぼ一定に進められ、脆弱性レポート、PoC を含む関連情報の保護は配慮されるが、それらのガイドラインが社内で定められ承認されてはいない。 [3.3.1]再現に不足している技術的専門知識等が顕在化し、他の部門との連携も行われるが、計画性は無い。 [3.3.5]脆弱性の再現確認において、他の製品への影響や脆弱性のバリエーションの存在を意識することがある。	[3.3.1-5]脆弱性の再現に関する責任者が定められ、必要なリソース(環境、ツール、要員、保護対策)を具備するための予算計画が承認されている。脆弱性の再現確認に関連するプロセスは文書化され管理されている。 製品ライフサイクルに基づく市場リリースの目録が管理され、脆弱性の再現確認の結果で必要な処置がとられている。	脆弱性の再現に関する責任者は、必要なリソース(環境、ツール、要員、保護対策)が適切であるか、又、関連する業務の部門間連携、その際の課題の抽出、シフトレフトへのフィードバック等の管理をしている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 4/　対策

4.1　対策リリースのマネジメント計画

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
ステークホルダがセキュリティ修正プログラムを適用するために計画を立てることを想定し、修正プログラムのリリース間隔を確立することが必要である認識がない。	[4.1.1.1]市場にリリースされている全ての製品の目録を作成することや、[4.1.1.3]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を特定するなど、修正プログラムのリリース間隔を確立するための準備が担当者レベルで進められている。	[4.1.1]一部の製品で製品ライフサイクルの管理が実施され、サポート終了時期などが明確になっている。 [4.1.2.1]RPM 等でセキュリティ修正プログラムをパッケージ化するための、様々なコンテンツタイプを理解し、[4.1.2.3]様々な製品間でセキュリティプログラムの展開方法を特定する仕組みを一部で提供し始めた。	[4.1.1]製品ライフサイクルの管理のためのプロセスが確立し、すべての製品でサポート終了時期が明確になっている。[4.1.3.1]プロダクトマネジメントチームやリリース管理と連携して、セキュリティ修正プログラムの配信時期を決定するプロセスや、[4.1.3.2]セキュリティ修正プログラムが通常の間隔で配信されない場合の例外を特定し、文書化している。	[4.1.1]製品ライフサイクルが確立、過去の経験、顧客の利用実態などから柔軟に対応ができている。[4.1.2]セキュリティパッチリリースマネジメント計画の立案、運用、評価についてステークホルダの間で継続的に調整が行われている。

RPM：　米 Red Hat 社が開発したパッケージ管理システム。アプリケーションのインストールやアンインストール、アップグレードなどの管理が簡単に行える。現在では、Vine Linux や Turbolinux などのさまざまなディストリビューションでこの RPM を利用してバイナリーパッケージやソースパッケージが作られている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 4/　対策

4.2　対策

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
発見者に報告された脆弱性に対する対策分析と緩和、修正プログラムを提供する前の回避策を検討することに必要性を感じていない。	一部担当者が[4.2.1.4]根本原因分析するために、[4.2.1.1]品質ゲートまたはバグバースに対して脆弱性報告やインシデントを検証するとともに、[4.2.1.5]脆弱性を拒否するなどの対応を行っている。	[4.2.1.2]影響を受ける製品、バージョン、ステークホルダ、および同時に修正する必要のあるバリエーションを特定し、[4.2.1.3]関連するサポート契約及びモデルを確認している。[4.2.1.6]対策分析として、ある脆弱性が原因で発生するリスクを軽減または対策する方法を特定している。また、[4.2.2.1]影響を受けた全ての製品バージョンで、報告されてすべての脆弱性が対策されていることを確認している。	[4.2.1]報告された脆弱性に対して脆弱性の認定基準、影響を受けるバージョンの調査方法、原因分析や回避方法の検討についてプロセスが定められており、安定的に対応できる。[4.2.2]対策の決定について、最終決裁者や検討プロセスが定められており、安定した運用ができる。[4.2.3]対策の公開方法が定められており、安定運用できる。	[4.2.1]報告された脆弱性に対して脆弱性の認定基準、影響を受けるバージョンの調査方法、原因分析や回避方法の検討についてプロセスが定められており、案件の対応ごとに振り返りが行われ継続的に改善されている。[4.2.2]対策の決定について、最終決裁者や検討プロセスが定められており、プロセスが継続的に改善されている。[4.2.3]対策の公開方法が定められており、継続的に改善されている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 4/　対策

4.3　インシデントハンドリング

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
インシデント（ゼロディ攻撃、意図しない脆弱性の開示など）が発生することを想定しておらず、発生した場合の対応計画や役割分担、責任の割り当てが行われていない。	一部の担当者がインシデントの発生を想定し[4.3.2.1]インシデントに関連する情報を収集しており、[4.3.1.4]役割分担や責任の割り当てを検討している。	インシデントの発生を内部ステークホルダは認識しており[4.3.1.2]役割分担、責任の割り当てが実施されている。[4.3.1.3]インシデント対応計画は策定されているが、[4.3.1.4]インシデント発生時のトレーニングや、机上訓練などは行われていない。	[4.3.1.3]インシデント対応計画が定められており、ステークホルダに周知されている。[4.3.1.4]インシデント発生時のトレーニングや、机上訓練が実施されている。	[4.3.1.4]インシデント発生時のトレーニングや、机上訓練の結果をもとに改善が進んでいる。また、業界で発生したインシデント事例を分析し、自社で同様の事例が発生した場合のため、インシデント対応計画やトレーニング内容を改善している。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 4/　対策

4.4　脆弱性リリースメトリクス

目的：　管理レポート用に定期的にデータを収集する。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
PSIRT の運用レポートやインシデント対応能力をステークホルダに開示する必要性を認識しておらず、公開していない。	一部の担当者が PSIRT 活動に関する運用状況を分析、公開することの必要性を感じ、情報の収集と公開を実施している。	組織として PSIRT の運用状況や、インシデント対応能力を計測する必要性を感じ、一部は経営層向けに報告を行っている。	以下の項目を例とする PSIRT 評価方法を定め、定期的に報告している。 ・[4.4.1.1]報告された脆弱性数と確認された脆弱数(製品／事業単位別) ・[4.4.1.2]確認された脆弱性のサードパーティコンポーネントによる分類 ・[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） ・[4.4.2.5]インシデントの数 ・[4.4.2.3]対策状況の追跡	PSIRT の運用レポートやインシデント対応能力に関するレポートを分析、報告しステークホルダのフィードバックを受けて、レポートの改善および PSIRT の方針に反映させるなどを実施している。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 5/　脆弱性の開示

5.1　通知

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
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ことの重要性が認識されておらず、何も情報を開示していない。	一部の担当者は、ステークホルダに対する対策方法などの適切な時期に情報を開示する必要性を感じており、情報を開示するなどの対応を行っている。	製品に関する脆弱性が発見された場合に、さまざまなステークホルダへの通知が重要であることは、組織として認識しているが、対応は場当たり的に対応されており、常に実施されるとは限らない。	製品に関する脆弱性が発見された場合に、ステークホルダへの通知時期や、通知内容がポリシーとして定められており、適切に通知されている。	脆弱性が発見された場合の通知ポリシーが定められ、通知されたあとの振り返りや分析が行われ、通知方法、通知内容の改善サイクルが機能している。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 5/　脆弱性の開示

5.2　調整

目的：　修正によって取り除かれた脆弱性を説明する。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
PSIRT は潜在的な脆弱性を報告する発見者の目的、意図やスタンスを理解し、合意された日程にて責任ある情報開示を推進・促進することが重要であることを認識していない。	一部の担当者は[5.2.1.1]第三者の発見者から脆弱性レポートを受領したことを報告することや、[5.2.1.2]報告された脆弱性に関する対応状況を発見者に対して定期的に通知することなど、双方的なコミュニケーションが必要であることを認識し、活動をしている。 また、脆弱性情報の開示についてステークホルダ間の調整が必要であることを認識し、一部実施を始めている。	組織として、発見者への情報提供および、情報開示時期をステークホルダと調整することの重要性を認識し、[5.2.1.3]発見者に修正を提供し、検証を可能にすることや、[5.2.1.4]脆弱性を報告した発見者の貢献を認め、謝辞を述べること[5.2.2.2]影響を受けるベンダの特定をするなどの対応を開始している。	[5.2.1]発見者とのコミュニケーションおよび[5.2.2]複数ベンダ間の調整についてプロセスが定められており、継続して実施できる体制になっている。	[5.2.1]発見者とのコミュニケーションおよび[5.2.2]複数ベンダ間の調整について、案件の対応ごとに振り返りが行われ、常に改善しながらスピーディに対応をすることが可能となっている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 5/　脆弱性の開示

5.3　情報開示

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。

ティア 0	ティア 1 (Repeatable)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
セキュリティアップデートをリリースする際、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、適切な情報開示をすることが重要であることを認識しておらず、実施していない。	一部の担当者は、セキュリティアップデートをリリースする際に、ステークホルダに情報を開示する必要性を認識し、リリースノートやセキュリティアドバイザリ、ナレッジベースに脆弱性に関する情報を公開している。	組織として、脆弱性情報の公開の必要性を認識し、すべてのプロダクトで、リリースノートやセキュリティアドバイザリ、ナレッジベースで脆弱性情報に関する情報を公開している。 また[5.3.2.6]発見者への謝辞や、[5.3.2.5]CVE 番号の割り当てなどが一部実施されている。	脆弱性情報の開示プロセス・テンプレートが定められており、リリースノート、アドバイザリ、ナレッジベースが公開プロセスに従って公開されている。[5.3.1.3]脆弱性情報の公開には承認プロセスがあり、[5.3.2.6]発見者への謝辞、[5.3.2.5]CVE 番号の取得についてもプロセス化されている。	脆弱性情報の開示について、案件ごとに振り返りが行われるなど常に改善のためのプロセスが存在し、事案や状況に応じて適切に素早く対応できる体制となっている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 5/　脆弱性の開示

5.4　脆弱性情報マネジメントの評価指標

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
脆弱性情報の公開に関する指標を取り、経営層へ報告する必要性を感じておらず、実施していない。	一部の担当者は、脆弱性情報の公開に関する指標を策定し、経営層に報告する必要性を感じており、セキュリティアドバイザリの公表数などを作成し、報告したことがある。	組織として、脆弱性情報の公開に関する指標の必要性が認識され、アドバイザリの公開数、プロダクトごとの公開された脆弱性件数や、アドバイザリの閲覧件数などが報告されている。	脆弱性情報の公開に関する指標の作成がプロセス化され、アドバイザリ公開数、プロダクトごとの公開件数、アドバイザリの閲覧状況などが定期的に報告されている。	脆弱性情報の公開に関する指標の作成がプロセス化され、アドバイザリ公開数、プロダクトごとの公開件数、アドバイザリの閲覧状況などが定期的に報告されて、経営判断に関わる指標として活用され、さまざまな指標を取得するための改善がされている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 6/　トレーニングと教育

6.1　PSIRT のトレーニング

目的：　PSIRT スタッフはセキュリティの世界で起こっていること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。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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
PSIRT が、常に変化する脅威環境に追従していく必要性を感じておらず、トレーニングは行われていない。	一部の担当者はセキュリティトピックを理解し、必要なトレーニングを受けているが、トレーニング内容や受講者について計画性はない。	組織として PSIRT 担当者のトレーニングの必要性を理解し、予算が組み込まれている。が、トレーニング内容については、ポリシーがなく、トレーニング内容がバラバラになっている。	PSIRT のトレーニングについてポリシーがあり、トレーニングメニューが決められている。トレーニングの内容には、[6.1.1.]技術的なトレーニング（攻撃手法、ツール、法規制や認証、プライバシー法など）[6.1.2]コミュニケーショントレーニング、[6.1.3]プロセスに関するトレーニング、[6.1.4]タスクツールに関するトレーニングが含まれる。	PSIRT のトレーニングポリシーが定められており、外部環境の変化（法規制や顧客の意識の変化など）に応じて、トレーニング内容が見直され、適時必要なトレーニングを実施できる体制となっている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 6/　トレーニングと教育

6.2　開発チームのトレーニング

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
開発チームは、セキュア開発が最適化すれば、自社製品がすでに市場にリリースされた後のセキュリティ対応に比べてはるかに安価であることを認識していない。	開発の一部のメンバーは、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なにをする必要があるのかを理解している。	組織として、開発メンバーが、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なにをする必要があるのかを理解している必要があると認識している。	開発チームに対し PSIRT プロセスをトレーニングすることがポリシーとして定められており、定期的にトレーニングが実施されている。	開発チームに対し PSIRT プロセスをトレーニングすることがポリシーとして定められており、トレーニングが実施され、開発チームが PSIRT プロセスに対し協力して、PSIRT 活動をスムーズに実施できる体制となっている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 6/　トレーニングと教育

6.3　診断チームのトレーニング

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
診断チームは、診断が最適化すれば、自社製品がすでに市場にリリースされた後のセキュリティ対応に比べてはるかに安価であることを認識していない。	診断チームの一部のメンバーは、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なにをする必要があるのかを理解している。	組織として、診断チームのメンバーが、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なにをする必要があるのかを理解している必要があると認識している。	診断チームに対し PSIRT プロセスをトレーニングすることがポリシーとして定められており、定期的にトレーニングが実施されている。	診断チームに対し PSIRT プロセスをトレーニングすることがポリシーとして定められており、トレーニングが実施され、開発チームが PSIRT プロセスに対し協力して、PSIRT 活動をスムーズに実施できる体制となっている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 6/　トレーニングと教育

6.4　すべてのステークホルダへの継続的な教育

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
PSIRT は、内部ステークホルダへの PSIRT プロセスのトレーニングの必要性を認識しておらず、実施されていない。	PSIRT の一部のメンバーは、内部ステークホルダへの PSIRT プロセスのトレーニングが必要であることを理解し、経営層向けへの PSIRT プロセスのトレーニングを実施している。	組織として PSIRT プロセスのトレーニングの必要を認識し、法務、リスク管理部門、マーケティング部門、広報、サポート、営業部門に対するトレーニングを実施し始めている。	内部ステークホルダへのトレーニングはポリシーとして定められ、定期的にトレーニングが行われている。	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について標準が設けられ、その内容は定期的に見直されている。

PSIRT Services Framework Ver 1.0 に基づくプロダクト脆弱性対策・対応成熟度シート

サービスエリア 6/　トレーニングと教育

6.5　フィードバック機能の提供

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。

ティア 0	ティア 1 (Partial)	ティア 2 (Risk Informed)	ティア 3 (Repeatable)	ティア 4 (Adaptive)
インシデントの根本原因の分析で得られた情報を使って、類似の脆弱性インシデントが発生しないようにする取り組みの必要性を感じておらず、対応していない。	インシデントの根本原因について、類似のインシデントが発生しないための取り組みが必要であることを一部の担当者が認識し、活動をしている。	インシデントの根本原因について、類似のインシデントが発生しないための取り組みの必要性を組織として認識し、情報共有が行われている。	インシデントの根本原因について、類似のインシデントが発生しないための取り組みがポリシーとして定められ、情報共有の方法、ツールが統一され、継続的に実施されている。	インシデントの根本原因について、類似のインシデントが発生しないための取り組みがポリシーとして定められ、取り組みの内容が日常的に改善され、情報共有することが組織の文化となっている。