一般社団法人コンピュータソフトウェア協会
セキュリティ委員会
制度 WG

プロダクト脆弱性対策・対応成熟度シート

Version 1.0

この成熟度シートは、「PSIRT Service Framework Version 1.0 Draft 日本語抄訳」をもとに、PSIRT Service 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。

2019 年 4 月

PSIRT Services Framework Ver 1.0 Draft 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ェ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 Service Framework Version 1.0 Draft 日本語抄訳では、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 Service 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、レベル 0 の内容から順に上位レベルに向けて記述を読み、自組織がどのレベルに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は除外してください。当面はフレームワークの平均が 2.5～3.0 となるように、各フレームワークの要件を満たすための施策や計画を検討し実施してください。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。

※レベル記述文中に、フレームワークのナンバーを付与しましたので、「PSIRT Service Framework Version 1.0 Draft 日本語抄訳」と照らし合わせて参考としてください。

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、レベル 0～2 に関しては「PSIRT」という組織が存在せずとも、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 Service Framework Version 1.0 Draft 日本語抄訳」の内容や用語の定義を確認してください。

PSIRT Services Framework Ver 1.0 Draft 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：　脆弱性管理に関わる内部のステークホルダによるエコシステムマネジメントを確立するため、PSIRT と内部のステークホルダとの関わり合いや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について PSIRT の役割を明確に伝え、インシデント時の対応力を向上させる。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
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を提供していない。	一部の担当者は脆弱性管理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。 製品の脆弱性に関しては CDL への移行がセキュリティライフサイクルの要点であることには気が付いていない。	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、広報・CC、法務部、開発部門、営業が定義されている。 [1.1.3.1]インシデント事後対応プロセスの構築は成熟しているが、開発の不具合をレビューするプロセスまでは確立していない。	PSIRT の機能と内部のステークホルダのマネジメントについて向上させるには、[1.1.1.3]社内ビジネスユニット・ラインとの交流、[1.1.1.4]内部開発・エンジニアリングとの交流、[1.1.1.5]ステークホルダに対応するサポートチームとの交流、[1.1.1.6]内部ワーキンググループへ参加が必要であると認識され始めた。	以下のような SDL のメンテナンスに繋がる具体的な活動が充実してきた。 ・[1.1.3.2]プロセスの不具合を追跡し教訓を招請し重要なステークホルダの問題を定期的にレビューする。 ・[1.1.3.4]人目をひくインシデントの対応から組織としての教訓を整理し報告データを提供する。 ・[1.1.3.5]事後対応プロセスで特定された内部プロセスの再調整を支援し改善の進捗状況を追跡する。

PSIRT Services Framework Ver 1.0 Draft 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：　学者、開発専門家、プロフェッショナルセキュリティ発見者、または愛好家などの脆弱性発見者には、独自の視点があり、彼らのコミュニティとの交流が製品セキュリティ・インシデント対応に対する先を見越したアプローチとして確立させる。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
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[1.2.1.1]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、[1.2.1.2]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、[1.2.1.3]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ている。	発見者との交流に関しては、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。	[1.2.1.1]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、[1.2.1.2]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、[1.2.1.3]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、関連する部門毎でその目的とともに文書化され周知されている。	[1.2.1.1]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、[1.2.1.2]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、[1.2.1.3]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、セキュリティ・インシデント対応の品質や効率に繋がることをレポートとして記録されている。	発見者のコミュニティとの交流に関するレポートを基に、コミュニティを維持するためのコストが予算として組み込まれている。

PSIRT Services Framework Ver 1.0 Draft 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。それは「視点の異なる多くの目」となり、脆弱性修復におけるベストプラクティスを共有しやすくなるためである。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
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、当該製品の担当者が、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が必要だと感じている。	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。	[1.3.2.2]組織間の責任ある開示のためのパラメータを定義し、以下の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。 ・[1.3.2.1]ピア PSIRT ・[1.3.5.1]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	[1.3.2.3]コミュニティチャネルの活動は安全な情報共有チャネルとなり、脆弱性修復におけるベストプラクティスが整理されている。	脆弱性修復におけるベストプラクティスは、エコシステム構築に関する予算策定に適切に利用されている。

PSIRT Services Framework Ver 1.0 Draft 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。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
自社製品のバグやセキュリティ脆弱性に関する気づきを与える社内ステークホルダとの良好な関係の構築関心がない。	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、交流のある下流のステークホルダは PSIRT 担当者にとって好意的であり、客観性に欠ける可能性がある。	組織内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。	[1.4.1.2]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、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。 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[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文書化されている。	[1.4.1.2]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、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。 [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いるが、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。	下流ステークホルダは常に製品への意見を提供し課題解決への関与と一体感が醸成されている。

PSIRT Services Framework Ver 1.0 Draft 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

目的：　PSIRT はセキュリティ・インシデントが発生した際には、組織内で脆弱性対策に関する調整を行うとともに、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中心的に機能しなければならない。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
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、機密保持対策が以下のように検討されている。 ・[1.5.2.2]安全なファイルを送信する方法を提供する ・[1.5.3.2]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。	[1.5.1.3]外部のコミュニケーションチャネル（社外コミュニケーションの有用性を確認するために活動の検証・評価することが含まれる）が提供されている。 [1.5.4.2]脆弱性の改修に関する通信、プロセス、パフォーマンスに対するフィードバックを行う方法が提供されている。	PSIRT はインシデント対応時、内部ステークホルダへの製品に対する脅威情報に関する影響の範囲やステークホルダが懸念する脆弱性・インシデント情報を明確かつタイムリーに提供できているかを把握することができる。

PSIRT Services Framework Ver 1.0 Draft 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：　製品の脆弱性の発見者との協力体制を醸成することは PSIRT の組織的な価値や評価を高める。それには発見者の協力に対する感謝を示し、互いの信頼を構築することが重要である。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
PSIRT 設置の有無に関わらず、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、組織内外に関わらず発見者に対して謝辞を示したり、なんらかの報酬が与えられるよう都度配慮したりしているが、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、[1.6.1.2]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。	組織の機能として、[1.6.2.1]脆弱性発見者への報奨プログラムが検討され、社内規定として予算が組まれている。その例として、[1.6.2.2]脆弱性報奨金制度や、[1.6.2.3]ポイント制度が開始されている。	組織の機能として、[1.6.2.1]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であることが認められてきている。	[1.6.2.1]脆弱性発見者への報奨プログラムの有効性をもとに、プログラムに対する予算バランスも最適化されている。

PSIRT Services Framework Ver 1.0 Draft 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 はその組織の有効性をステークホルダに認識させるために、PSIRT の人数、性能、提供する情報の有効性を示すための KPI を設定し、常に改善のためのフィードバックを受け、それぞれ視点の異なるステークホルダのニーズが反映されているかをモニタリングするような仕組みが必要である。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
組織は、ステークホルダが PSIRT に期待するニーズがそれぞれ異なることや、ステークホルダのそれぞれ異なる視点による気づきがフィードバックされることが重要であると気づいていない。	一部の担当者は、組織内外に関わらず PSIRT が提供する情報に関して、ステークホルダの立場により有益となったり、そうでなかったりする場合があると気づいている。また、その場合、PISRT の有効性が認識されていないため、有益な情報であるにも関わらず有益でないと判断された経験がある。	一部の担当者は、ステークホルダのニーズを知るため、ミーティングやアンケートを実施し始めているが、メトリクス（PSIRT の KPI）は設けられていない。	各ステークホルダが情報をどのように利用したいかを理解するため、以下のようなメトリクス（PSIRT の KPI）を設けミーティングやアンケートを実施し記録[1.7.2.2]している。 ・[1.7.1.1]メトリクスと成果物の内部ステークホルダ要件を収集する。 ・[1.7.1.2]メトリクスと成果物の外部ステークホルダ要件を収集する。	[1.7.3.1]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が認識できている。	[1.7.3.2]データの傾向と過去のパフォーマンスを分析できている。 [1.7.4.2]必要に応じてメトリクスデータを確認し、プロセスやサービスの提供を改善している。

PSIRT Services Framework Ver 1.0 Draft 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：　PSIRT にとって主要のシナリオとなる脆弱性の報告の受付における重要な要素は、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。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
ステークホルダ内外を問わず、脆弱性の報告の受付について適切な体制や運用方法に関する検討の必要性を感じていない。	組織内における脆弱性の報告窓口担当は特定の個人がイメージされる状況で、その個人の意識や業務状況によって受付業務の品質がことなる。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。	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。	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、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ている。具体的には以下のしくみが準備されている。 ・製品マニュアル ・Web サイト ・検索エンジン登録 ・主要な CSIRT/PSIRT リストの登録 ・[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。 (例) psirt@ ,incidents@, security@ 等を企業のドメインの下に確保する)	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。	[2.1.2.1]コミュニケーションチャネルの監視により、SLA の維持がなされている。

PSIRT Services Framework Ver 1.0 Draft 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：　製品開発者に直接開示されない脆弱性情報（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なチャネルを介して開示される脆弱性情報）も存在することを理解する。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
脆弱性の開示を製品に対するクレームや風評ととらえ、直接報告されない情報に対して関心がない。	一部の担当者が都度[2.2.1]攻撃情報データベースの確認を行う。	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。	製品開発者に直接開示されない情報の管理に関して、監視の対象選定や要員アサイン、利用ツール、コストなどが繰り返し見直され最適化している。

PSIRT Services Framework Ver 1.0 Draft 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モニタリング

目的：　外部コンポーネントの脆弱性は製品に影響を与える可能性があるので、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しなければならない。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
外部コンポーネントに含まれる脆弱性について関心がない。	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されはじめた。	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。	脆弱性の依存関係やパッチ情報などが開発チームに適切に通知され、次期製品リリースにおいても同様の修正を適用したり、脆弱性のトリアージにより適切に PSIRT にエスカレーションしたりすることで、PSIRT の手作業による脆弱性ハンドリングの工数が削減されている。

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 Draft 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　新しい脆弱性を特定する

目的：　製品のセキュリティ問題への対処において、外部関係の管理と調整の労力を削減するために、外部組織が発見する前に製品の脆弱性を発見する。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
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、外部関係の管理と調整の労力を削減することに気づいていない。	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いている。	[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。	[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が実施され、セキュリティテストツールの専門知識の維持向上に貢献できている。

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 Draft 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 の KPI として、PSIRT の規模、パフォーマンス、他の測定値を内外に提供することで、各ステークホルダに対し PSIRT 設置の効果や信頼性を提供する。また、ステークホルダからのフォードバックにより、PSIRT のサービスを改善できる。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
PSIRT のサービスに関する KPI は必要ない、もしくは優先順位を低く考えている。	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 が自動化され管理され始めた。	以下の項目が KPI として管理され、おおむね自動化されている。 ・[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 ・[2.5.2.1]オンタイム応答率（初動対応を SLA の時間枠で適時に行なっているか） ・[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 ・[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している。 ・[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。	以下の項目を KPI として管理し、ビジネスレポートとして開示されている。 ・[2.5.2.1]オンタイム応答率（初動対応を SLA の時間枠で適時に行なっているか） ・[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 ・[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 Draft 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：　対処したい問題の種類と範囲に関する適切な認定基準でセキュリティベースラインを設定し、セキュリティ上の「脆弱性」と「問題」を定義することで、脆弱性に関する報告を効果的にトリアージする。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
[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。 [3.1.1-3.1.2] 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）や脆弱性重大度判定（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。 [3.1.2-3.1.2.1] 脆弱性の基準は個人的な興味の範囲で改訂されるだけで、データに基づく体系的なものではない。	[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。 [3.1.1.1-3.1.1.2]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。 [3.1.2.1]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。	[3.1.1-3.1.1.1]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。セキュリティ品質レベル（品質ゲート）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、不定期に改訂がされる。 [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、セキュリティ品質レベル（品質ゲート）や脆弱性重大度判定（バグバー）の粒度が粗いため、反映に時間がかかる場合や、反映されない場合がある。	[3.1.1-3.1.1.1] 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。 脆弱性重大度判定（バグバー）は緊急、警告、重要、注意に細分化されて区別され、かつ、サービス拒否、なりすまし、改ざん、情報開示、特権昇格のマトリクスでサーバーとクライアントのそれぞれのシナリオや挙動が定義されている。セキュリティ品質レベル（品質ゲート）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、データとして管理されて、改訂のフィードバック情報となっている。	脆弱性の認定が進んだことで、製品の設計時点で脆弱性の作りこみが防止されている。セキュリティ品質レベル（品質ゲート）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おり、ファジング等で未知の脆弱性の検証も行われている。これらの情報は文書化され、開発チーム全員が関与し、共有とトレーニングがなされて、かつ、常時、柔軟に見直しがなされる。脆弱性の判定件数や脆弱性に対する見解の相違、ソフトウェアコンポーネントのバージョンなどがデータとして収集され、セキュリティ品質レベル（品質ゲート）と脆弱性重大度判定（バグバー）の改訂が最適化され、リスク管理とコスト管理も最適化されている。

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：　発見者との関係について、脆弱性の根本原因の分析と脆弱性の改修に係る判断基準やトリアージなどの一部のフローの省略などを含めたプロセス効率を向上させ、報告者との関係を改善する。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
[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]脆弱性レポートを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、ごく一部、含まれており、報告者によっては対応をスムーズにさせることができる。 [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。	[3.2.2]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、トリアージの効率は高い。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、報告者との対応をスムーズにさせることができる。バグバウンティプログラムによって、効率的かつ有効的な関係を維持し、専門家から見ても常に品質の高い製品供給とコストダウンが可能となる。 [3.2.4]脆弱性レポートのガイドラインが継続的に改善され、レポート完成度のばらつきがなく迅速にトリアージができる。

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：　PSIRT は脆弱性の判定基準の排外でも特段の定めがない限り、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。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
[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志に任される。 [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。 これらの業務効率向上への意識があり検討されているが、その評価は定期的でない。	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始めているが、事業計画に係るリスク管理やセキュア開発管理への要素情報としてのインプットはなされていない。	脆弱性の再現に関する手法やプロセスが定期的な評価によって常に洗練されている。 脆弱性の再現に関するアウトプットや関連する業務の品質・効率ともに、事業計画に係るリスク管理やセキュア開発管理の要素情報としては利用されている。 これらの情報は、事業計画に直結したリスク管理のモニタリングとして適切に運用され、経営者やサービスオーナーの経営戦略に生かされている。

PSIRT Services Framework Ver 1.0 Draft 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　セキュリティパッチリリースマネジメント計画

目的：　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ためのガイダンスを提供する。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
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を進めている。	[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。展開方法としては、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などがある。	[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。	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。	[4.1.1]サポート範囲またはサポート義務から外れた製品について、どのようにサポートしていくかについて脆弱性の重大さを鑑み、明確なサポートポリシーでもって、事業単位、事業ライン、ステークホルダのサポートを巻き込みながら対応していくことができる。

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 Turbo linux 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 Draft 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：　発見者に報告された脆弱性の管理に関連し、対策分析と緩和を含み、どのバージョンが改修されるかを定義し、その提供状態も考慮する。また修正プログラムが提供される前にステークホルダが適用できる回避策を検討する。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
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。	[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]脆弱性を拒否するメカニズムを決定している。	[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。	修正プログラムの開発中において、[4.2.1.8]脆弱性が改修されない例外を特定しながら、[4.2.1.7]脆弱性を軽減するために実装できる回避策があるかどうかを特定しており、 [4.2.2.2]担当の QA エンジニアまたはチームから回避策となる救済措置に関するリリースの承認を得ている。 [4.2.2.3]対策に関するリリースの承認を得るために、サードパーティの発見者または、ステークホルダと連携し、[4.2.3.1]脆弱性を公開するために優先されるメカニズムを決定している。	脆弱性対策における様々な対策コストや機会損失、投資などの[4.2.4.2]リクス管理プラティクスを定義し、[4.2.4.3]ビジネスへの脅威と影響を理解することによって、リスクを評価し定量化している。また、[4.2.4.4]リスク登記簿に定量化したリスクを記録している。[4.2.4.5]また、調査結果及び推奨事項は、リスク登記簿に記録され更新されている。	定義されたリスク管理プラクティスやビジネスへの脅威と影響を理解したうえで、プログラム開発方針の参考とする技術アーキテクチャへのフィードバックが顕著となり、リスクマネジメントとして機能している。

PSIRT Services Framework Ver 1.0 Draft 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：　PSIRT は世の中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、一般公開となった「重大な脆弱性」に対処する改修時間を早めるための仕組みを確立する。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
インシデントハンドリングを担当する者は、製品に影響する脆弱性に対処する改修時間を可能な限り早めることが必要であると感じていない。	[4.3.1.2]インシデント対応計画の一環として必要な主要のステークホルダを特定し、[4.3.3.1]情報公開（広報担当、開発者、法務担当者）が行われている。 また、[4.3.1.1]インシデントの管理に必要なリソースは特定されている。（会議室、専用回線、追加の人員）＋食料や宿泊施設など。	[4.3.2.1]インシデントに関連する情報に関して受信、カタログ化、保管がされており、[4.3.2.2]インシデント処理に必要な分析のリソースは最低限提供されている。	[4.3.2.2]インシデント処理に必要な分析のリソースは適切に提供されている。また、[4.3.2.3]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リソースが提供され、[4.3.3.2]広報活動は適切に管理され調整されている。	[4.3.2.4]収集された重要な情報、実行された分析、対策及び緩和のステップ、終了及び解決など、全てのアクションを文書化しており、[4.3.2.5]インシデント対応終了後のプロセスについて改善がなされている。これには、予防のための、プロセス、ポリシー、リソースツールの改善などが含まれる。	[4.3.3.4]PSIRT による事故後の説明会が行われた際、インシデント対応や SDL 活動を改善するフィードバックが収集されており、その都度「どのような SDL アクティビティが最初にその問題を阻止し得たか」が追及され公式に報告されている。

PSIRT Services Framework Ver 1.0 Draft 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　脆弱性メトリクス

目的：　PSIRT の評価方法を定める。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
—	—	—	—	以下の項目を例とする PSIRT 評価方法を定めている。 ・[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 また、以下を例とするステークホルダに対する SLA を定めている。 ・　[4.4.2.1]オンタイムの影響評価 ・　[4.4.2.2]オンタイムの改修計画 ・　[4.4.2.4]オンタイムの改修率	定められた評価方法による評価はインシデント毎に定期的に行われ、顕在化した課題はマネジメントレビューに報告され改善策が検討されている。 経営者はマネジメントレビューにより、PSIRT に対する投資対効果を確認することができている。

PSIRT Services Framework Ver 1.0 Draft 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：　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し、それによって、ステークホルダは計画を立てることができる。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
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いない。	[5.1.1.1]PSIRT はステークホルダからの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ことなど、タイムリーにステークホルダに情報を提供できている。	[5.1.1.4]中間ベンダによる脆弱性対策が作れない、あるいは時間がかかりすぎる場合は、ステークホルダに情報を共有することや、[5.1.1.3]全ての中間ベンダを明らかにした上で、法務部門と連携して、中間ベンダとの契約内容に脆弱対応をタイムリーに行うという条項を追記できているなど、情報提供における想定内の課題について対処が検討されている。	[5.1.2.1]様々な調整者の脆弱性情報開示ポリシーから、それぞれの違いを把握し文書化されている。[5.1.3]顧客やサードパーティの研究者などの発見者は、”Vulnerability Discovery”等に記載されている連絡手法を用いて、PSIRT に対して脆弱性の報告をおこなうことが可能となっている。	[5.1.2.2] 調整者と組み、影響を受ける全てのベンダ PSIRT が通知されたことを確認できる仕組みが構築されている。	[5.1.2.2] 調整者と組み、影響を受ける全てのベンダ PSIRT が通知されたことを確認できる仕組みが網羅的でありタイムリーであることが評価されている。

PSIRT Services Framework Ver 1.0 Draft 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　コーディネーション

目的：　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。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。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
ベンダ 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。	[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始めている。	[5.2.1.3]発見者に修正を提供し、検証も可能にすることや、[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始めている。	以下のコーディネーションに関する業務について文書化され周知されている。 ・[5.2.2.1]他のベンダまたはコーディネータからの脆弱性レポートの受領を承認する業務 ・[5.2.2.2]報告された脆弱性の影響を受けるベンダを特定する業務 ・[5.2.2.3]様々なベンダ脆弱性情報を共有する業務 ・[5.2.2.4]様々なベンダと修正が提供される時期および下流ベンダがその修正を受ける取る方法について調整する業務 ・ [5.2.2.6]脆弱性情報がどのように、またいつ開示されるのか、ということについて、全てのベンダ間で交渉し、合意を取る業務	コーディネーションに関する業務について、脆弱性情報を共有するためのレポート様式や用語、アクションの質に差異がなくなり、実質的なマルチベンダでのコーディネーションが確立しつつある。	―

PSIRT Services Framework Ver 1.0 Draft 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：　セキュリティ更新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、適切な情報開示を実施する。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
セキュリティ更新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いない。	セキュリティ更新アップデートをリリースする際に、リリースノートの作成に関して以下のプロセスが検討されている。 ・[5.3.1.1]リリースノートにどの脆弱性を開示するかを定義する ・[5.3.1.2]レビュープロセスを定義する ・[5.3.1.3]情報開示に関するレビューと承認を行う	自身の公開 Web サイトにセキュリティアドバイザリを掲示するために以下のプロセスが検討されている。 ・[5.3.2.1]セキュリティアドバイザイリのテンプレートの定義 ・[5.3.2.2]セキュリティアドバイザリを提供する仕組	リリースノート、セキュリティアドバイザリをはじめ、以下のプロセスや定義が文書化され周知されている。 [5.3.2.4]脆弱性にCVE番号の割り当てや CVSS 評価などのプロセスを定める。 [5.3.2.5]発見者が自身の名を掲載することを望むかどうか確認する、[5.3.2.6]ステークホルダは誰であるか、いつ開示するか、などのレビュープロセスを定義する、[5.3.2.7]定義されたステークホルダと一緒にレビューする、など。	ナレッジベースの記事を公開するために、以下のプロセス・定義が周知されている。 [5.3.3.1]どのような脆弱性をナレッジベースの記事にするべきかを定義する。[5.3.3.2]レビュープロセスを定義する、[5.3.3.3]開示のレビューと承認を行う。[5.3.4]内部のステークホルダと協力して、脆弱性についての顧客からの質問にチームとして答えるための用語や言葉遣いを定めたりレビューしたりする。	—

PSIRT Services Framework Ver 1.0 Draft 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：　脆弱性情報に関するマネジメント評価指標を作成し管理する。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
—	—	—	—	脆弱性情報に関するマネジメントに関し、以下のようなインジケータを設定し定期的に評価する。 ・脆弱性情報の案件数、分類・修正にかかった時間 ・影響のある製品やサービス件数 ・[5.4.1.1]公表したセキュリティアドバイザリの数 ・[5.4.1.2]NVD へポストした CVE の数 ・[5.4.1.3]セキュリティアドバイザリへのアクセス数	評価指標による管理により、脆弱性情報の開示プロセスの透明性が高まり、ベンダ、調整者、発見者が相互に情報を共有する状態が把握できるようになっていることで、経営へのインパクトの緩和や、事業継続の安定に寄与している。 経営者は脆弱性情報マネジメントに関する現状の課題について、社外取締役や株主に具体的に説明することができ、またその改善施策について経営方針に即したアイデアを説明できる。

PSIRT Services Framework Ver 1.0 Draft 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 チームのトレーニング

目的：　PSIRT は常に変わる脅威環境に追従する必要があるため、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。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定期的にレビューされる必要がある。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
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、一定のトレーニングを受けることで満足している。	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。	[6.1.1]PSIRT 担当者はチームのトレーニングを受けることにより、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訓練されている。	[6.1.2]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ことができている。 [6.1.3]また、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／法的な問題を排除できている。	[6.1.4.1]PSIRT 及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が有効に使われている。 [6.1.4.2]また、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キングするツールを特定し利用している。	PSIRT チームは、さまざまなステークホルダが利用できる全てのトレーニングをトラックできており、セキュリティ環境の変化に対応しトレーニングに関する内容やプロセスを見直ししている。

PSIRT Services Framework Ver 1.0 Draft 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：　セキュアなコードで記述でき、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。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
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。	[6.2.1]開発プロセス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。	開発チームのトレーニングにより、製品に関する重要な情報を管理するための適切な方法が検討され始めている。 （例）セキュリティアーキテクト、開発責任者、テスト責任者など、リスク軽減策に最も近い人に情報を戻す方法など	PSIRTがリスクを評価し、軽減策を開発するためにもっともよく知っている人にフィードバックができるよう文書化による周知が進んでいる。 (例)サードパーティのコンポーネント、更新プロセス、ログ、セキュリティの例外が許可されたか、どのようにステークホルダに知らされているかなど。	ソフトウェア関連の製品やサービスの脆弱性数と重大度を減らすように特別に設計された開発プロセス全体で行われる方法論と手順が追及され管理されている。	—

PSIRT Services Framework Ver 1.0 Draft 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：　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。

※対象外

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
—	—	—	—	—	—

PSIRT Services Framework Ver 1.0 Draft 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　全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。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
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必要であるという認識がない。	[6.4.6]セールスチームや[6.4.7]サポートチームにおいて、PSIRT プログラム及び関連するタイムラインでの役割について一定レベルの訓練と理解が要求されることを認識している。	[6.4.2] 法務チームや[6.4.5]広報チームにおいてPSIRTプログラム及び関連するタイムラインでの役割について一定レベルの訓練と理解が要求されることを認識している。	[6.4.1]経営層や、[6.4.3]政府関係者、コンプライアンスチームにおいて PSIRT プログラム及び関連するタイムラインでの役割について一定レベルの訓練と理解が要求されることを認識している。 すべてのステークホルダは、一定レベルの訓練と理解について標準が設けられ文書化されている。	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。	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その内容が定期的に見直され、課題となったインシデントにおいてもそのフィードバックが反映され訓練の効果がみられる。その効果は、経営者がマネジメントレビューにより、PSIRT プログラムの一定レベルの訓練に対する投資対効果として確認することができている。

PSIRT Services Framework Ver 1.0 Draft 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：　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、関係者に教育し、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。

レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
PSIRT に関するトレーニングや教育について必要性が認識されていない。	PSIRT に関するトレーニングや教育について必要性が認識されているが、一部の担当者が外注もしくは内製により不定期に実施している。	PSIRT に関するトレーニングや教育のコンテンツは定期的（例えば半年毎）に見直される。見直す内容は、一部の担当者のスキルに委ねられている。	PSIRT に関するトレーニングや教育のコンテンツは定期的（例えば半年毎）見直される。見直す内容は、インシデントの根本原因の分析中に得られた情報が反映されるとは限らない。	インシデント対応中にそのインシデントの根本原因の分析内容がトレーニングのコンテンツに反映されるようなフィードバックがされている。	インシデント対応中にそのインシデントの根本原因の分析内容がトレーニングのコンテンツに反映されるようなフィードバックがされている。 トレーニングを受けたステークホルダは、似たような脆弱性インシデントが発生しにくいイメージを実感している。