TLP:WHITE

Product Security Incident Response Team (PSIRT) Maturity Document

PSIRT Maturity Levels to demonstrate Operational Capability and Maturity

製品セキュリティインシデント対応チーム（PSIRT）成熟度ドキュメント

運用能力と成熟度を示す PSIRT 成熟度レベル

https://www.first.org/standards/frameworks/psirts/psirt_maturity_document

日本語訳

日本語訳は日本シーサート協議会と Software ISAC によって翻訳された後、JPCERT/CC と Panasonic PSIRT と TOSHIBA-SIRT によってレビューされました。FIRST は関係者の協力に深く感謝します。

成熟度レベル 1（基本） - はじめが肝心

はじめに:

サイバーインシデントレスポンスへの関心は以前から存在したが、近年の様々な出来事でその関心はさらに高まっている。FIRST は 2013 年に CSIRT の運用に焦点を当てたサービスフレームワークの構築に着手した。この CSIRT Services Framework の公開後、製品セキュリティインシデントレスポンスのコミュニティが FIRST 傘下に集まり、チームが経験した固有の課題に対処するための PSIRT 中心のサービスフレームワークを作成した。CSIRT と PSIRT は大部分において共通の行動や活動があるが、前者は組織のインフラを保護することに重点を置き、後者は組織の製品の脅威や欠陥に対応することに重点を置いている。理事会は、製品セキュリティコミュニティの努力を高く評価し、すべての人を教育するためのサービスを定義したことに感謝したいと思う。

本ドキュメントでは、製品インシデントレスポンスチームが活動の一環としてある段階で選択する一連のユースケースとサービスの概要を紹介する。PSIRT 活動は、そのミッションやニーズが変化し、チームの経験が増すにつれて、時間の経過とともに進化する可能性がある。参照されているユースケースは、新しく設立された PSIRT から、プロセスを絶えず改良して機能を追加してきたより高度なインシデントレスポンスチームまで、さまざまな発達レベルをカバーしている。このような進化に伴い、チームは、プロセスの成熟度の高まりを反映して、リアクティブな運用から、よりプロアクティブな運用に移行する。本フレームワークでは、チームが同時に管理できる脆弱性とインシデントの数「キャパシティ」や、チームがどのように機能を統制し、文書化し、実行、および測定しているのかを示す SIM3 などの成熟度モデルについては扱わない。

イントロダクション:

PSIRT を作りなさいと言われてないか？もしかしたら最近までは、その場しのぎのプロセスであったり、二次的な役割として誰かが任命されたり、あるいは全く新しい組織で働く機会を得て、すべてを一から構築することになったかもしれない。いずれにしても、製品やサービスで特定された脆弱性の管理を支援するチームを編成する任務が与えられている。PSIRT にはさまざまな規模や特徴があり、まったく同じものはない。基本的には、PSIRT の中核となるのは、脆弱性レポートを受け取り、ある程度のレビューと分析を行い、適切な関係者と協力してセキュリティアップデートを作成し、最終的にはそれらのアップデートを組織の顧客やパートナーに提供することである。

このレベルでは、PSIRT が世界に旅立つ際に提供する必要がある中核的なサービスと機能を説明する。これらの教訓は、さまざまな規模、産業、分野、国の多くの組織から集められたものである。
これから皆さんが踏み出す最初の数歩は誰もが経験してきたことであり、先人がかつてつまずいた経験を皆さんの今後の活動に活かせていただきたい。ここで PSIRT Services Framework 中から、新たに活動を開始した PSIRT が最良の結果を得るための指針となるいくつかの重要なエリアを強調したい。このドキュメントで「成熟度」という用語を使用する目的は、製品セキュリティチームの概要を説明し、チームがステークホルダーに提供する能力を俯瞰的にレベルで説明することである。

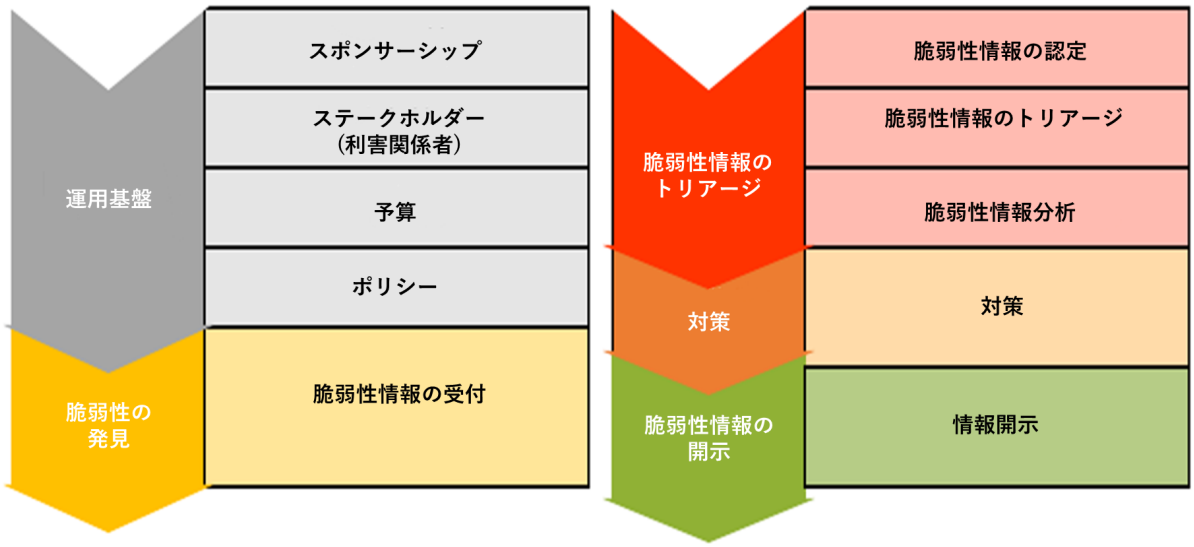

図 1:成熟度レベル 1 の望ましいサービスエリアおよびサービスの一覧

はじめに - 運用基盤

PSIRT Services Framework には「運用基盤」という概念がある。このセクションでは、運用基盤の中から組織が PSIRT を計画、構築、および効果的に運用するために必要なコアコンポーネントを特定して説明する。

ポイント-効果を上げるには、PSIRT が活動を始める前に一定の前提条件が必要である。(予算、役員からの支援、設備など)。

運用基盤とは、建物の基礎を考えるようなものである。建物の基礎(すなわちコンセプト、プロセス、及び人員)は、建物の骨組み(新しい PSIRT)を設置する前に実施または計画されなければならない。十分な機能と効果を発揮するためには、「運用基盤」の各分野に取り組む必要があるが、もし

時間や資源その他の制約がある場合、いくつかの不可欠な分野がある。PSIRT は、脆弱性の管理という複雑な問題を解決するために組織を支援する専任のスタッフを配置することが必要である。彼らが集中すればするほど、コンスティチュエンシーより良いサービスを提供できる。

経営層の支援

まず第一に、あなたはなぜこのドキュメントを読んでいるのだろうか？なぜ PSIRT についてもっと知りたいのか?ある時点で、会社に PSIRT が必要だと経営層が判断したからである。経営の支援/信任を得ることは、その後の進め方に関わる極めて重要なことである。PSIRT におけるあなたの役割は、セキュリティ上の重要な問題に対処するために、通常は行わないことを依頼したり、あなたからの依頼を自分自身の業務よりも優先してもらったりすることだ。この役割を果たす権限を(書面で)与えられることが重要である。ここでは簡潔にするため 2 つの概念を組み合わせているが(大規模な組織では微妙な違いがあるが)どちらの概念も組織のリーダーが PSIRT の取り組みをサポートすることを意味している。

PSIRT の明確な憲章と組織のリーダーの支援が重要であることは、いくら強調してもしすぎることはない。始めたばかりのころは大変だと思うが、PSIRT の仕事は、組織のリーダーの理解、サポート、支援によって飛躍的に簡素化される。

ステークホルダー

自分自身に問いかけなさい、誰のために働いているのか？ステークホルダーとは、あなたと一緒に働く人たちや、あなたの仕事の結果を享受する人たちのことである。それぞれのステークホルダーは、あなたから見た場合と同様に、あなたとの間に異なる要望やニーズを持っている。
PSIRT は主なステークホルダーを文書化することから始めるとよい。ステークホルダーについては FIRST PSIRT Services Framework に詳しく記載されている。これらのグループが誰であるか、そして彼らの要求が何であるかを理解することによって、PSIRT は彼らの要求と義務を満たすように自らを適合させることができる。PSIRT が成熟し、発展するにつれて、各ステークホルダーグループの独自性と、それぞれに対する報告やコミュニケーションをカスタマイズする必要性を理解することだろう。

予算

PSIRT はリーダーシップとステークホルダーの関与と密に連携し、スタッフや活動の準備のための予算を確保する必要がある。PSIRT が持つ予算やリソースの規模は PSIRT コミュニティのなかでも大きく異なるが、最終的には、PSIRT は組織のビジネス目標を満たすのに十分な資金を持つべきである。チームとサービスが成長するにつれて必要となる資金と人員も増加することに留意すべきである。

ポリシーと手順

企業の経営層から絶大な支持を得ることができた。次に何をすべきか？PSIRT の活動において遵守する一連のルールの文書化である。始めたばかりの段階では、1 つか 2 つのポリシーしかないかもしれないが、組織がより多くの経験を積むにつれ、リストが増える可能性がある。また、始めたばかりの段階では、多くの手順のまだ文書化されていないことが予想される。文書化とプロセスが整備されていない段階では、事後対応に一貫性がなくなる可能性がある。PSIRT が手順作成に取り組み始める際に重要なことは、PSIRT がどのように行動し、与えられた状況でどのように対応するかを把握することである。社内のプロジェクト/プログラム管理、エンジニアリング、または自社内のサポートから既存の成功事例を借用するとよいだろう。
PSIRT を立ち上げる際(またはギャップを埋めたい人)に役立つかもしれない。国際的に認められた標準の例として、ISO/IEC 29147 Information technology--Security techniques--Vulnerability Disclosure と ISO/IEC 30111 Information technology--Security techniques--Vulnerability Handling Processes がある。これらの国際標準を確認することに加えて、以下のようなポリシーを策定することもできる。

■脆弱性管理に関する方針（ISO/IEC30111 で取り扱われている）
■情報取扱方針（ISO/IEC 29147 で扱われている)
■脆弱性のスコアリングと優先順位付けに関するポリシー
■修復サービスレベル合意書
■脆弱性情報開示ポリシー (通常は公開文書)

PSIRT エントリポイント - 脆弱性の発見

誰も脆弱性について知らない場合、そこに脆弱性が存在すると言えるか？運用基盤を整え、問題を解決するための最初の段階は、問題の存在を知ることである。PSIRT Services Framework には、「脆弱性の発見」というサービスエリアに該当する。

ポイント- 一定のプロセスと人員を確保できたら、実施すべき事柄を見つける必要がある。

この機能を持つことで、PSIRT はレポートを受付けその後のアクションにつなげることが可能になる。

脆弱性情報報告の受付

セキュリティの欠陥を修正する作業を始めるには、PSIRT はまず脆弱性の存在を認識する必要がある。おそらく、まだあなたは脆弱性やそのようなレポートを積極的に探してはいないだろう。そこで、他の人(社内外)がセキュリティ上の問題をみつけたときに、どのようにあなたに連絡するのかを知ってもらう必要がある(例：電子メールアドレスの公開）。電子メールアドレスの公開に加え、脆弱性レポートを受取るための PGP 鍵を提供することもお勧めする。また、報告を受け付ける Web フォームを設定することも一般的である。

PSIRT 立ち上げてたばかりの頃は、サードパーティの研究者や社内で報告された脆弱性のみを対象にするのもよいだろう。あなたは、これらの相手と緊密に連携し、より効率的にコミュニケーションを行ったり、問題を適切なチームに迅速に転送できるようになりたいと思うはずだ。そして PSIRT として成熟するに従い、より多くの(たとえば顧客、サポート、営業組織など)異なるタイプの発見者とやりとりをするようになるのだ。

次の段階 - 脆弱性のトリアージと分析

脆弱性情報の受付とトリアージにより、 PSIRT の事案管理が開始する。運用の順序はどの PSIRT でも非常に似ているが、「事案」が作成されるタイミングや、事案の処理中に違う役割を実行する担当者など、さまざま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る組織では、事案として作成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かもしれない。逆に、脆弱性レポートの量が少ない組織では、トリアージの前に事案として作成するかもしれない。いずれにせよ、PSIRT の最終目標は、効率的で定義されたプロセスを構築することである。

どのような製品および/またはサービスがあるか、そしてこれらがどのような技術で構成されるかによって、この段階は PSIRT 間で大きく異なる可能性がある。ハードウェアベンダは、「ブーン」という音をたてたり電気的または機械的なエンジニアリング手法を活用したりする複雑なマシンを必要とするかもしれない。一方、ソフトウェアを開発およびリリースする企業は、問題をよりよく理解するために、一連のスキャナーを駆使したり、手動のコードレビューをしたりするかもしれない。

ポイント-問題の大きさは? それほど大きくない問題? それは本当にあなたに影響はある?

脆弱性の認定

レポートを受け取ったら、その内容が適切なものであることを確認する必要がある。報告者は発見を間違えていないか？レポートは実際の機能を誤って解釈していないか？PSIRT は、報告された内容を確認して理解し、その問題をセキュリティ上の脆弱性として受け入れるのか、それとも判定基準に基づいて拒否するのかを決定できなければならない。時には、PSIRT だけでは判断できず、製品エンジニアリングチームによる確認が必要な場合もあるだろう。理想的には、これらすべての作業について、前もって役割と責任を明確に文書化し、すべての関係者がそれを理解している状態にしておきたい。

手間を減らすためには、レポートを授与した最初から主要な脆弱性情報の要点を把握すること。レポートを機械読み取り可能なフォーマットや主要な技術情報を明記させるようなフォーマットにすることで、記述されている内容を理解して意思決定を行うことに役立ち、冗長性を回避し、処理時間を短縮できる。

脆弱性の文書化やコミュニケーションに役立つ主なリソースは、次のとおりである。

■Common Vulnerability Reporting Framework (CVRF)
■Common Security Advisory Framework (CSAF)
■Vulnerability Description Ontology (VDO)
■Vulnerability Handling Process ISO 30111
■Common Vulnerability Enumeration (CVE)

その他の詳細については、付録を参照。

脆弱性分析

さて、PSIRT は脆弱性報告が適切なものであることを確認した。次は、誰かが問題を掘り下げ、その欠陥がどのように動作し、どのように引き起こされるのか、どのバージョンの製品が影響を受けるのか、脆弱性が悪用されるとどのような結果が生じるのかを理解しなければならない。これらの作業は PSIRT が行うこともあるが、多くの場合、影響を受ける製品またはサービスの専門家によって、より詳細なレビューが行われる。最低限でも、PSIRT は問題の分類し、その問題を理解しレビューできる者への依頼を行う。さらに、レポートが何らかのレベルで対処されていることを確認する(リスクの是正、軽減、移転、受容が必要である)。

そして、優先順位付けとスコアリングについて話を進める前に、簡単な注意点が一つある。PSIRT は最初からスコアリングの方法を取り入れていなければならない。成功事例では、すべての受信レポートに何らかのスコアリングシステムを使用して、脆弱性かどうかを分類することを推奨している。事前に基準を文書化しておけば、対処を指示する際に役立つ。理想的には、Common Vulnerability Scoring System (CVSS) を使用すべきであるが、独自のシステムを使用することもできる。

ここでのポイントは、自分の基準となるものを選び、それを使ってすべてのものを測ることである。
CVSS を使用しない場合は、自社のスコアリングシステムが CVSS より優れていると考える理由について、顧客に適切な説明をする必要がある。

問題の修正 - 修復

わぁ！この時点で、実に多くのことを成し遂げた。発見者からレポートを受け取っている。あなたは実際にセキュリティ上の脆弱性であることを検証している。また、この問題を完全に調査して理解できるようにするための行動または支援も行っている。次の段階は、費用対効果の分析を行い、脆弱性に対処するためのオプションを評価することである。考慮すべき多くのオプションがある。たとえば、脆弱性のリスクを完全に排除するコード修正プログラムを作成したり、脆弱性のリスクを限定する一連の手順書を作成したり、もしくは修正を全く提供しないと決定することなどが考えられる。

ポイント-壊れているものが見つかったら、修正にとりかかって然るべきである。

修復

このプロセスの最も重要なアウトプットは、実際に脆弱性を解決することである。PSIRT は、製品の修復や影響の緩和によって問題が解決されるまでを追跡したり手助けしたりする。適切なチームがこの問題に対処したら、バグの発生から終了までを管理するという仕事の最終ミッションに進むことができる。

最終段階 - 脆弱性の開示

これは、セキュリティ脆弱性のライフサイクルの最終段階である。欠陥が対処された際、PSIRT は(社内外の)ステークホルダーに更新情報と関連資料を伝達する手助けをする。

ポイント-苦労して問題を解決したのだから、誰かにそのことを伝えた方がいい。

開示

これは、PSIRT が製品やサービスの顧客に通知(または責任者による通知の調整を支援)する段階である。開示にはさまざまな形態があるが、基本的に、顧客および関係者に製品またはサービスが問題の影響を受けていることを通知し、脆弱性を解決または緩和する方法に関する文書を提供する。さらに、脆弱性を発見し報告した発見者を認め、彼らに正当な評価を与える。この信頼関係と好意は今後の活動にも影響してくるだろう。

PSIRT が発行するアドバイザリの中で研究者/発見者に対して適切に謝辞を示すことは、業界全体の良い慣例となっている。謝辞は発見者のキャリアアップと評判の確立に役立ち、あなたが発見者の努力を認めることで発見者からあなたへの好意が生まれる。あなたの文章にこのような小さな投資をすることで、理想的には次に彼らが問題を発見したときに責任を持って再びあなたのところに戻ってきてくれるだろう。ISO 29147 は、脆弱性情報の開示に役立つ参考資料を提供している。

まとめ

以上が、PSIRT が実行することとその使命を果たすための核となる段階である。前述したように、これらの段階をどのように実行するかは、組織の規模や年数などによって異なってくる。これらの基本的な要素が整ったら、次はサービスの質向上と範囲拡張をどのように進めていくのかを検討するのが良い。

より多くの仕事を引き受け新しい機能を追加することを考えるより前に、これらサービスや機能を一貫して提供できることが重要である。PSIRT としてより成熟するとともに、中級 PSIRT の特徴である機能を追加していくことができるだろう。

成熟度レベル 2 (中級) -事後対応ではあるが、訓練はしっかりしている。

はじめに

いくつかのことをマスターし、いくつかの脆弱性レポートにうまく対応できるようになった後には、社内外の顧客に向けてより多くのサービスを追加することを望むようになる(または命じられる)だろう。PSIRT が提供可能なサービスの範囲は多岐にわたるが、自社のビジネスに最も利益をもたらす取り組みに集中することが重要である。製造業ではクラウドネイティブのスタートアップとは大きく異なるビジネス上の懸念とリスクを軽減しようとしており、各ビジネスの顧客も同様である。

まとめると、成熟度の中間段階にある PSIRT は、内部に焦点を当てていると考えている。物事をうまく管理し始めていて、物事を成し遂げるために誰と対話するのかを理解しているが、より広いコミュニティに拡大するための資金や人材はおそらく持っていない。これまでのすべてのサービスを適切に実施し、精査された上でサービスを提供していることが期待されている。まだ脆弱性レポートをうまく取り込むことができないのであれば、成熟度レベル#1 に戻って、記載されていることを実施する必要がある。より新しいテクニックやサービスに移る前に、そこでスキルを磨くのだ。

この発展段階にある PSIRT は通常、次のような機能を持っている。

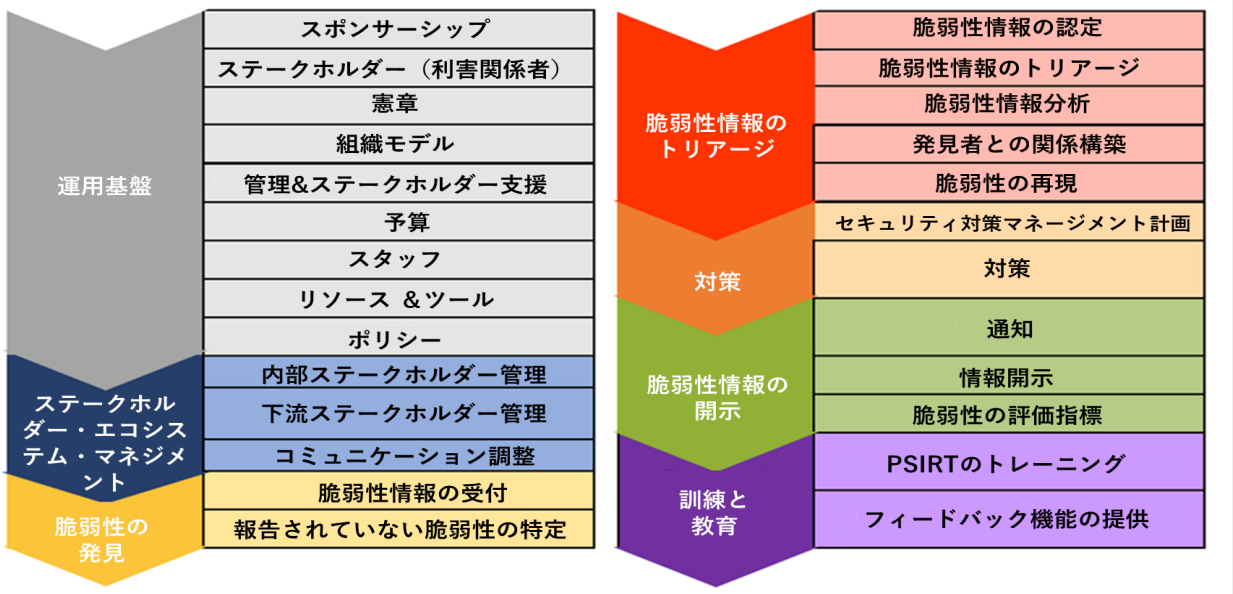

図 2：成熟度レベル 2 の望ましいサービスエリアとサービスの一覧

基本に帰る - 運用基盤

「次のレベルに進むこと」を考えているのであれば、運用基盤のすべてをある程度まで実施する必要がある。これらの基本的な活動により、PSIRT は経営層や管理者の信頼を築き上げる。またポリシー、基準、ガイドラインなどの重要な項目を文書化し、安全な運用のための資金を確保することも同様に重要である。PSIRT のスタートし、いくつかの PSIRT ではすべての項目を確立することを選択し、多少手抜きをする場合もあるが、PSIRT が成長し成熟するにつれて、継続的に運営を成功するためにはこれらの重要なことが適切に整備されていなければならない。 PSIRT Services Framework では、実施する必要のある各エリアと機能について詳しく説明している。

コミュニケーションの（断絶ではなく）詳細 - ステークホルダー・エコシステム・マネージメント

PSIRT が未熟であるかどうかは、PSIRT の運用に関わるステークホルダーの理解度によって決まるといっても過言でない。このレベルでは、これらの重要なサービスは本当に必要である。このレベルで活動している組織は、社内で誰と協力して脆弱性を確認し、対応するのか把握していることが求められている。PSIRT がいくつかの脆弱性を管理し、まだ改善の余地はあるものの一般的には PSIRT とその内部のステークホルダーは脆弱性が発生した場合に何をすべきかを知っている状態である。PSIRT は、会社の製品やサービスを誰が使用するか、また一般的には誰が組織に商品、ソースコード、またはサービスを供給するかについて基本的な理解が必要である。

この中級レベルの PSIRT は問題に対処するためのプロセスと手段を定義している。理想的には、基本的な消火活動にとどまらず、製品や顧客にとって重大な問題を認識できている。PSIRT は、このような重大な事象が発生した場合のプロセスを文書化し、適切なステークホルダーを迅速に集め、修復作業を開始する必要がある。もう一つ重要な点は、理想的にはこの段階で、PSIRT が組織のエンジニア/開発チームのメンバーから定期的に相談を受けていることである。このような交流により、ほぼリアルタイムのフィードバックグループが確保され、理想的には迅速に欠陥を特定し修正することができる。

手がかり発見！- 脆弱性の発見

組織は脆弱性に対処するプロセスを何度も経験し、PSIRT は脆弱性のレポートを取り込む方法を知っている。より成熟した PSIRT は、製品/コンポーネントの脆弱性レポートを収集するための複数の手段を持ち、問題の追跡を支援するツールを持っている。このレベルになると、PSIRT やその他の

社内エンジニアは自分自身でセキュリティの脆弱性を発見している。（いい仕事である！）これができるようになると、組織は外部で設定された期限に縛られて作業することなく、製品/コンポーネントのアップデートのリリース時期をコントロールすることができる。これは、PSIRT とそのエンジニアリングパートナーがこれらの内部的に見つかった問題を無視できるという意味ではなく、緊急事態として対処されるのではなく、組織のリリーススケジュールやその他のリソースの利用の可能性に合わせて解決策作成をスケジュールできるということである。誰もが問題を解決したいと思っているが、定時に家に帰り猫と一緒に食事できるのもよいことである。社内で発見された欠陥のリリース時期を管理する機会があれば、顧客やセキュリティ研究者から「重大な欠陥」が報告されたときに関係するすべてのチームが柔軟に対処できるようになる。

この成熟段階では、 PSIRT は時間をかけてでもリリースされた製品に含まれるすべてのコンポーネントの包括的なリストを収集することが重要である。企業によって呼び方は異なるが、通常は製品マニフェストまたは部品表 (BOM) と呼ばれる。このリストがあれば、PSIRT はどの製品に対して脆弱性を監視し、テストすべきかを知ることができる。PSIRT が成熟するにつれて、このリストは、検出された脆弱性を修正するためにどのようなサードパーティ(オープンソースプロジェクトなど)と対話する必要があるかを理解するのにも役立つ。

SDLC(Software Development Life Cycle）について

ソフトウェア開発ライフサイクル(SDLC、SDL、SSDLC）、セキュリティエンジニアリングなど、どのような名前で呼ばれていようとも SDLC プロセスに連携することは PSIRT にとって重要である。それぞれの PSIRT の役割や SDLC との関係は様々であるが、オープンなコミュニケーションラインを持ち、SDLC プロセスと連携することは、PSIRT が製品リリース前にフィードバックを提供し、セキュリティの欠陥を修正するのに役立つ(理想的である)。誰と話すべきか、いつ製品がフェーズゲート(段階の移行判断)されるか、どのように情報を提供するのが最善かを知ることは、PSIRT のミッションや発見された脆弱性への対処に役立つ。

ここでは事実のみを – 脆弱性情報のトリアージと分析

この成熟度になると既に補助輪は外れている。複数のソースから脆弱性の報告を受け、PSIRT は、その報告が本当にバグかどうか掘り下げて理解する練習をしてきている。(バグでない場合もある。インターネットで有名になりたい熱心な報告者にそのことを説明するのは楽しいことになるかもしれないが、まあ幸運を祈る！）練習をすることで、あなたはこれらのレポートを評価できるようになり、それに応じて管理できるようになっている。すべてのバグが同じように作成されるわけではないことを理解した

上で、PSIRT はこれらのレポートを評価するための定量化可能なプロセス(「バグバー」と呼ばれることもある)を持つことを考えなければならない。

ここで、PSIRT をどのように構成するかという選択が効いてくる。あなたが設計したプロセスとチーム(集中型、分散型、ハイブリッド型)の運用モデルによって、誰が脆弱性のトリアージや分析を行い、その作業をどのように管理されるのかに影響を与える。受信したレポートを誰がどのように処理しているかを理解することは、レポートを迅速に確認し、対応するために非常に重要である。各モデルには長所と短所があり、PSIRT はワークフローの中でどのような役割をはたしているのかを理解する必要がある。(積極的なコーディネーターか？調査を担当するか?問題を報告するだけか?)

この頃になると「リピータ」と呼ばれる人たちがあなたに問題を報告してくれるようになる。それは素晴らしいことである。そのような人たちと仕事をすればするほど、長い目で見れば誰もが幸せになれる。脆弱性の発見者と友好な関係を保つことをお勧めする。脆弱性の報告者と上手く付き合うことができなければ、インターネット上でそれが拡散されることになり人生は悲惨なものになる。そのような無意味なことを避け、プロフェッショナルな態度で、人材、プロセス、ツールが許す限り迅速に対応する。 あなたはおそらく発見者をデータベースに登録し、彼らが誰か、何を見つけたのか、レポートの質はどうかといった基本的な情報を追跡しているだろう。

また、発見者と一緒に作業する場合、通常、不具合追跡システムやチケッティングシステムを通じて、進捗状況のアップデートを提供することも有効である。チケットデータを報告者に提供することで、あなたは報告者の懸念に適切に対応していることを示すことができ、発見者との協力関係を築くことができる。そして最終的には、発見者があなたの対応に不満に思い、合意した期日より前に欠陥を公開されてしまうリスクを減らすことができる。

この成熟度になると、すべての報告者と適切に連携し、どのようなレポートが簡単に対処できるのか、どのようなレポートが解決するまでに何度もやり取りしなくてはならないくらいめちゃめちゃなのか(誰もがイライラする） を指導することができる。覚えておいてほしいのは、やればやるほど上達し、早くできるほど他分野のスキルアップに多くの時間を使えるということである。この段階では PSIRT やエンジニアリングパートナーは何らかの形の再現能力を開発しているだろう。これら欠陥は、 隔離された環境でテストすることが重要である(ネットワーク上のすべての人の 1 日が台無しになってしまわないように)。エクスプロイトの取扱い方法、どのようにテストをするのか、どのように悪意のある人から保護するのかといったプロセスを文書化しておくこと。社内(場合によっては社外のパートナーやステークホルダーと一緒に)で安全に再現するための計画をたてておく。

PSIRT の初級者向けに CVSS スコアリングの概念を述べた。この段階では、チームはセキュリティ脆弱性の評価に習熟しており、業界標準の用語を使用してセキュリティ脆弱性を説明できるようになっているはずである。PSIRT の中には、最初のスコアリングをエンジニアリングパートナー(「セキュリティチャンピオン」とも呼ばれる)に委託し、PSIRT は必要に応じて監督や指導を行っているところもある。組織内のセキュリティ意識の高いパートナーとのネットワークを構築することは、PSIRT をより効果的に機能させるために必ず役立つ。PSIRT の中には Common Weakness Enumeration (CWE) による問題へのラベル付けをすることによって、スコアリングを強化しているものもある。また、自動スコアリングや自動記述するためのツールを作成することもある。さらに PSIRT は、組織の製品がどのように構成され、どのように導入されているかという観点から CVSS スコアや重要度ラベルの定義とともに欠陥に関する追加のコンテキストを提供することもできる。

修復

「PSIRT の実行」が上手くなれば、ツールやドキュメントが改善され、問題に対処する際の人々の安心感も向上する。パッチや修正を構築するだけでなく、現在のプロセスを活用して繰り返し実行することが可能になる。時には、通常よりも少し速く作業することもあるかもしれないが、もはや「一から作り直す」ようなことはせず、一つひとつ手作業で修正を加えていくことができる。自動化され、再現性があり、緊急事態であるが、人々はそれに対応するプロセスがあることを理解している。願わくは、このプロセスを顧客と共有し、顧客が通知を受け、最新情報を迅速に入手できるようになることを期待している。このレベルの PSIRT は、ポリシー、標準、ガイドライン、およびプロセスが文書化しているはずである。すべてが考慮されているわけではないが、環境内の最も一般的なシナリオは考慮されている。また、この時点で十分なポリシーがあり、ルールから逸脱した場合の例外プロセスが必要になる場合があるかもしれない。

私は真実を、すべての真実を話すことを約束する... - 脆弱性の開示

最初の数件はセキュリティの脆弱性は目新しく、怖かったかったかもしれないが、今はこれまでにいくつもの脆弱性に対処してきており、チームは何をすべきか訓練を受けているだろう。この段階では、単なる通知だけでなく、もっと多くのことを実施していることになる。あなたの製品のユーザはアップデートがリリースされたことを知ることができ、さらに他の人との調整も上手にできるようになっている。この調整の良い参照事例は FIRST の Multi-Party Coordination and Disclosure Guidelines に掲載されているあなたの周りを取り巻くエコシステムと同期をとることで、共有する顧客へのリスクを抑え

ることができるかもしれません。PSIRT は、開示前に顧客との事前のコミュニケーションを必要とする状況を定義している。PSIRT は、情報が開示されたときのために、電子メールによる配信や開示時の通知を導入している可能性がある。業界を超えたコミュニケーションや、営業チームやサポートチームへの情報の開示前の社内コミュニケーションも成熟している。今までに、チーム自身とセキュリティアップデートの配信を追跡する評価基準も定義されているだろう。FIRST が発行する PSIRT Services Framework には、これらの各フェーズで追跡可能な多くの評価基準が提案されている。自分のパフォーマンスを分析し、インシデントの管理方法を改善した後、これを自分のプロセスにフィードバックする。PSIRT は情報共有のためにトラフィックライトプロトコル (TLP) を考慮する場合もある。

トレーニング

経験と振り返りが、PSIRT を始めたばかりの頃とは一線を画す秘密のスパイスである。あなたは、これまであなたが学んだことを応用し、自分自身を向上させてきた。理想的には、この新しい知識を書き留めて、組織内の他の人と共有できるようにすることである。また、広報、法務、役員などの特定のステークホルダーを対象とした教育研修を実施し、自分の役割や期待されることを理解してもらうことができるだろう。新しい仲間をチームに追加する際には、一貫したトレーニングを提供することで、全員が同じ情報を理解し、自社のポリシーや実務に沿って行動できるようになる。

FIRST は、新しい PSIRT やその技術を向上させるためのトレーニングビデオを公開している。

まとめ

すべての脆弱性は PSIRT にとって学習の機会であり、そのワークフローを実行することで、実務やツールを最適化できる領域を徐々に見つけている。エンドユーザとの対話によって、PSIRT はニーズを満たすための組織全体の成果物の提供方法を学ぶきっかけができる。PSIRT がこのテクニックを一貫して実行できるようになれば、効率性が向上し、より多くの時間を状況の改善に費やすことができるようになる。十分な時間と練習と熟考を経て、PSIRT はより高度なパフォーマンスを発揮できるようになる。

成熟度レベル 3 (高度) -先手を打つ…多くの備えはできている（ほとんど）

はじめに

おめでとう！あなたは PSIRT を始めてからしばらく経ち、多くの問題を解決し、組織に根付かせている。実に素晴らしいことだ！顧客は（概ね）満足しており、影響を及ぼす問題はあなたたちが管理することによって適切に対応されている。さて、次はどうする。基本は理解できているので、ここからはエリート PSIRT のようになるための調整と改善の方法について説明していく。

このレベルに到達するには、製品のセキュリティアップデートの取得、分析、および配布のプロセスが組織内で十分に理解されている必要がある。社内の同僚はあなた方が誰で PSIRT が何をしているのかを知っており、あなた方は全員、何度も問題のサイクルを乗り越えてきたので、社内でやり取りする人にとってプロセスと要件は目新しくもなく驚くようなものでもない。また、いくつかの大きな脆弱性や「典型的な」問題よりも大きな攻撃を乗り越えてきた。このような大規模な事象は、プロセスやドキュメントに改善が必要なエリアを特定するのに役立っている。

あなたは、十分なツール、プロセス、人材を導入したことで、新たに発生する仕事の管理や、発生した問題のフォローアップに対応でき、日常的な「通常の業務」としての脆弱性管理の問題だけでなく、より大規模で時間のかかる問題も管理できるようになっている。

このレベルで活動している PSIRT は積極的で一貫性のある行動がとれているといえるだろう。自分の組織や製品に何かが起こるのを放っておくのではなく、問題や人を探し出すために積極的な行動をしている。あなたはこれまでの多くの経験から、今では今後の事態を予測するための手段を講じている。すごいツールを使って、過去の出来事に基づいて行動をし、何が起こるのか予測しているのではないか？もしかしたら、非常に効果的にリスクを管理し、どのような行動がビジネスに影響を与える可能性があるのか理解し、問題が発生する前にそれらの軽減に取り組んでいるのかもしれない。このレベルの PSIRT が実行する能力は、適切に管理された適応力のあるプロセスを表している。このレベルのチームが提供するサービスのリストは次のようになる。

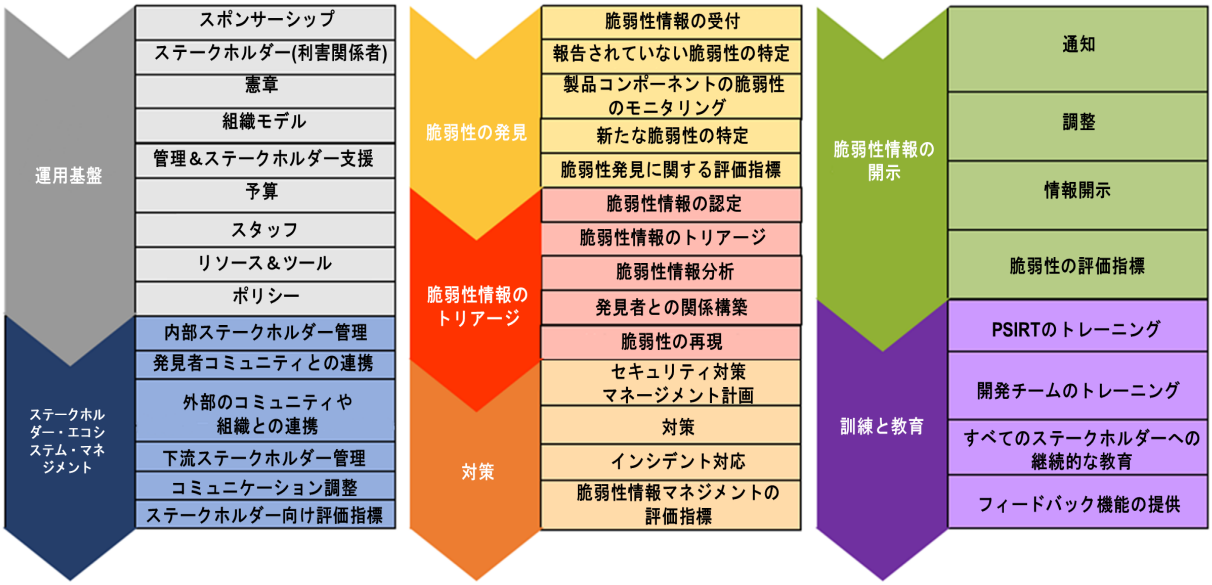

図 3：成熟度レベル 3 の望ましいサービスレベルとサービスの一覧

ここでは、熟練した PSIRT が発揮する能力について深く掘り下げていく。

揺るぎない運用基盤

自分が成熟していると考えるためには、これらのプロセスとサービスのすべてが長期にわたって確立されている必要がある。各サービスは、PSIRT の運営、資金調達、方向付けにとって不可欠である。ここで不足しているものがある場合は、一貫してできていないものや足りないものを振り返ってみなさい。それらを確立するために社内のサポートを得るべきである。この成熟度に到達するための最低限の条件である。これらをすべて完了してから、また戻って続きを読んで欲しい。

ステークホルダーにステークを入れる…うーん…

この成熟した段階の PSIRT は自信を持って活動している。この自信は組織の業の製品やプロセスに関与する人(そして外部の人も)との頻繁で活発な会話によって部分的に形成されている。この時点で、PSIRT はすべてのステークホルダー(そのリストは非常に大きい)とオープンで正直な関係を築くことに投資してきた。この段階まで進化した PSIRT は戦略集とテンプレートを活用して標準化されたコミュニケーションを構築しており、ステークホルダーはプロセスに対するフィードバックを提供したり、受け取ったりするための複数の手段を持っている。PSIRT は、組織の中核となる定期的な製品プログラムの会議に参加し、今後のリリーススケジュールに精通している必要がある。

このレベルの PSIRT が使用するフレームワークにおいては、評価基準と報告が継続的な成功の鍵となる。PSIRT とそのステークホルダーは、成功の目標と測定方法を明確に定義している。つまり、主要業績評価指標として、「顧客満足度」、「ネットプロモータースコア」、「セキュリティ脆弱性パッチの提供」、「サービスレベル目標/合意」などが適用され、運用の継続的な成功を保証するため PSIRT とそのステークホルダーによってレビューされている。これらの指標を使うことで、PSIRT はビジネス上の積極的な選択を行い、修復プロセスのすべての参加者の内部行動に影響を与えるために役立つ。

このレベルで活動している PSIRT の主な特徴は、外部のステークホルダーをしっかり理解し、関与していることである。脆弱性への対応の仕組みやプロセスの確立を支援したり、何らかの形でセキュアなソフトウェア開発ライフサイクルとの統合や監視、さらには営業組織の内部サポートに対応したりする。PSIRT が強固な基盤を持つようになった今、主に内部に焦点を当てることから、外部の関係者とより積極的に関わることにシフトしている。

PSIRT は、業界の同業者やセキュリティ研究者との連携を深めるべきであり、強力な関係を築くために、何らかの支援プログラムを作成、提供するとよい。最も有益なのは、外部の「上流」プロバイダーとの関係を構築し、彼らがセキュリティ問題にどのように対応するのかを完全に理解することである。これにより、PSIRT が管理する商品やサービスへの影響を把握することができる。このようなサードパーティコンポーネント管理には、フレームワークが詳述しているすべてのことと同様に、さまざまなやり方があるだろう。

未知なるものの発見（少なくとも最初から知られていなかった）

PSIRT がこの段階に入ると、彼らは自分たちの領域のマスターになりつつある。社内のステークホルダーとの良好な関係は、PSIRT にリリース工程へのより良い洞察を与える。今後の追加される機能/パッケージについて認識し、将来に備えたより良い準備をしているだろう。複数のソースからの脆弱性レポートの受付を管理するツールを開発または取得している。PSIRT のこの進化の段階においては、PSIRT が製品の脆弱性探しを積極的に支援していることが理想的である。この行動は、開発および保守プロセスに不可欠なものとなっている。

PSIRT は製品の開発プロセス全体を通じて、より優れた脆弱性情報スキャンと分析を行うように組織に影響を与えてきた。これにより製品の発売前により多くのセキュリティバグを検出し、エンドユーザ

がその影響を受ける前に修正されている。問題が報告されたら、それぞれを分析して、さらに別の亜種が存在しないかどうかを確認する必要がある(研究者は頭脳明晰ではあるが、すべてを知っているわけではない)。PSIRT と製品エンジニアリングチームが持っている詳細な製品知識によって、新たな悪用方法を発見できるかもしれない。PSIRT は、サードパーティ製コンポーネントのセキュリティリスクを管理し、脆弱性レポート(ソーシャルメディア、報道機関、カンファレンスペーパーなど)のソースを積極的に監視している。これらは、将来の攻撃兆候の把握や組織によってまだ発見されていない脆弱性の分類に対する重要な早期指標となる可能性がある。

先生、診断結果は？

チームは結成されてしばらくたち、自分たちがサポートする製品の状況を理解している。PSIRT は脆弱性レポートを迅速かつ正確に評価するためのプロセスを構築しており、過去の発見者を活用したり、組織の製品がどのように悪用されるかについての理解を深めたりしている。経験とアイデアによりプロセスとツールが効率化され、チームは自分たちのパフォーマンスを継続的に振り返りサービスの改善を図ることができる。

これまで報告された欠陥に対応する中で、PSIRT はその分野のセキュリティ研究者や報告者に対する多くの見識をもっている。これらの研究者の中には、非常に有能であることを証明した者もいる。これらの研究者は、実績のない報告者であれば対応しなければならないトリアージ段階を回避して、適切に優先順位を設定してそのまま分析フェーズに移行することができるかもしれない。PSIRT は、何が「良い」レポートなのか、どの要素/データが研究者の発見をより迅速に検証(または反証)するために役立つのかに強い関心を持っているはずである。

また、攻撃や脆弱性を再現するために、PSIRT は問題を安全に再現できるシステムに展開するプロセスを持っている必要がある。これにより、チームは「もしも」のシナリオを試すことができる。

PSIRT は開発チームと協議し、よくあるコーディングミスやセキュリティ上の欠陥を避けるためのフィードバックを提供することができる。CWE のようなツールはエンジニアが過去の欠陥を確認し将来発生する問題を回避することができる。このガイダンスは、開発ライフサイクルの早い段階でフィードバックを取り入れることにより、リリース後のコストのかかる修正を回避することに役立つ。

問題の修正

理想的には、過去の問題を繰り返し修正してきたこの段階で、PSIRT とすべてのステークホルダーは矛盾なくアップデートを提供できるようになっている。すべての関係者は何をすべきかを知っており、緩和策を提供するためのスケジュールについて明確な予想を持ち、問題の修正に充てるための十分なリソースを持っている。PSIRT が技術的な問題を修正すると同時に、適切な文書化とコミュニケーションフローを進めて問題を公表することで、パートナー、仲間、顧客のすべてが問題を理解し、どのように修正されたのか、「ただのパッチ当て」以外の選択があったのかどうかを確認することができる。
アップデートの提供は日常的なプロセスであり、その場しのぎで行われるものではない。最終的なアップデートの提供は、標準化されたアップデートリリーススケジュールの形式をとるかもしれないし、自動化された更新メカニズムを介して「OTA」で配信する準備をするかもしれない。問題が関係する製品によって、問題の影響を受けるエンドユーザに緩和策を提供するために組織が利用可能なオプションが決まる。エンドユーザが脆弱性に対処するためにすべきことの準備は整っており、あとは公開を待つのみである。

聞いてくれ！知らせがある･･･壊れたモノの(もちろん、どうやって直すかも教える)

脆弱性の公開準備が整いアップデートが利用可能になったときに、PSIRT は全てのステークホルダーに警告が伝わるようにする必要がある。前述の「ステークホルダーマネージメント」の項の通り、PSIRT は情報を提供する必要があるさまざまなグループと、それぞれにどのように関与するのがベストなのかを理解している。最新情報や公式声明を発表するとき、PSIRT はどのような手段を使ってコンスティチュエンシーに適切な情報を提供するかを把握している。

PSIRT が上流またはサードパーティのプロバイダーに依存している場合、または PSIRT自身が下流に製品やサービスを提供している場合は、PSIRT がこれらの異なるグループにどのように情報を提供するのが最適かを理解していることが重要である。PSIRT が複数のベンダーが同じバグの影響を受ける大規模なエコシステムの一部に属している場合、関係する PSIRT は通常、影響を受けるすべてのお客様に同時に情報提供ができるよう相互に合意できる時間(情報を開示しない期間に)を調整している。理想的には、特定のエンドユーザグループが別のエンドユーザグループよりも不利益を受けることがないように、さまざまな更新プログラムが同時にリリースされ、悪意のある攻撃者が公開された脆弱性を利用できる時間を最小限に抑えることを目標としている。

先生教えてください。

この段階の PSIRT は、これまでに様々なレベルのトレーニングに携わってきた。製品やセキュリティ技術に関する戦術的なトレーニングを受け、標準的な運用手順を戦略集に文書化し、新しいメンバーが理解できるよう努めていたことだろう。

繰り返しになるが、このレベルの PSIRT は以前よりも積極的である。PSIRT は、自ら参加するだけではなく、社内の同僚やその他の ステークホルダーにセキュア開発トレーニング・コンテンツを提供することもできる(リソースやミッションに応じて)。また、よい事例や学びを反映させたトレーニングやドキュメントを増やすことで、仲間やパートナーが「次世代」の PSIRT を構築する支援ができる。開発者、エンジニア、および製品チームがセキュアコーディング、プライバシー、および情報セキュリティ技術を理解し、これらの原則を実行することで PSIRT は飛躍的に強力になる。

まとめ

組織の製品やサービスのセキュリティを確保することは、ゴールのない旅のようなものである。日々、脅威の状況は変化し、新しい技術が生まれ、新しい考え方が開発され、新しい脅威が発生し、古いものは停滞していく。このドキュメントの成熟度レベルが、あなたが PSIRT の旅立ちに役立つことを願っている。

「レベル 3」以上

なんだって？不可能に聞こえる？・・・いやそんなことはない！

付録 1:補足資料

サポートリソースの一覧と用語集は、FIRST PSIRT Services Framework を参照する。
https://www.first.org/education/FIRST_PSIRT_Services_Framework_v1.0.pdf

付録 2:図

付録 3:PSIRT 憲章

PSIRTs には、機能とその範囲を記述した明確な憲章が必要である。一般的な憲章には次の項目がある。:

■ミッションステートメント
ミッションステートメントはチームの目的と活動(付録 3 の例参照)を定義する。
■ステークホルダー(利害関係者)
ステークホルダー(利害関係者)とは、PSIRT がサービスを提供する相手／対象である。詳細は、「Service 1.1:Internal Stakeholders in the PSIRT Framework」を参照する。
■所属及びスポンサー組織
経営層の支援で定義されているスポンサー組織は、PSIRT の目標、アクションをサポートし、運営のためのリソースを提供している。
■スコープ
PSIRT フレームワークで述べられているように、PSIRT は、保護する製品、利害関係者、組織構造と同じくらいユニークで多様である。スコープは組織全体にわたって PSIRT に与えられた責任と影響力を表している。

付録 4:ミッションステートメントの例

■Microsoft

Microsoft Security Response Center (MSRC) は、Microsoft の顧客、ブランド、システムに影響を与えるセキュリティ問題を調整して軽減する。MSRC は外部のセキュリティ研究者と Microsoft 製品チームとの間の連絡窓口である。MSRC はセキュリティ研究者や Microsoft 製品チームと連携して、Microsoft 製品で報告されたセキュリティ脆弱性を文書化して修正するという重要なインターフェースを提供している。

■IBM

IBM Product Security Incident Response Team (PSIRT) は、IBM 製品に関連するセキュリティ脆弱性情報の受領、調査、内部調整を行うグローバル・チームである。IBM PSIRT はセキュリティ研究者、業界団体、政府機関、およびベンダーが IBM 製品の潜在的なセキュリティ脆弱性を報告するための中心的な役割を果たしている。このチームは、IBM の製品＆ソリューションチームと連携して調査を行い、必要に応じて適切な対応策を特定している。IBM 製品利用のお客様は、セキュリティ上の脆弱性の可能性を含む、関連するすべての問題を IBM テクニカルサポートに報告する必要がある。社内外のすべての関係者間のコミュニケーションを維持することは、当社の脆弱性対応プロセスの重要な要素である。

■Brocade

Brocade Product Security Incident Response Team のミッションは、製品およびサービスの機密性、完全性、または可用性に影響するセキュリティ脆弱性の受領、調査、および調整を管理することにより、組織と顧客を保護することである。

■DELL EMC

DELL は、お客様の当社製品のセキュリティ脆弱性に関連するリスクを最小限に抑えるためのサポートに努めている。私たちの目標は、脆弱性に対処するためのタイムリーな情報、ガイダンス、および軽減策をお客様に提供することである。Dell Product Security Incident Response Team (Dell PSIRT)は、デルに報告されたすべての製品の脆弱性の対応と情報開示の調整を行う責任がある。

■Red Hat Product Security

製品、サービス、プロジェクトにおける重大なセキュリティ上の懸念からお客様を保護するために、製品の安全性を確保し、脆弱性を調査し、問題を解決している。
明確、正確、タイムリーで、信頼できる情報を通じて、製品セキュリティに関する優れた品質のカスタマー・エクスペリエンスを提供する。組織の価値の確保は、サブスクリプション価値の重要な一部であると認識している。
高い成功を収め、情熱と幸福感を持ち、効果的に働き、社内外でセキュリティのリーダーと見なされる、結束力のあるチームを構築し、維持している。

■Honeywell

Honeywell Product Security Incident Response Team (PSIRT) は、同社のすべての製品、サービス、コンポーネントのセキュリティの脆弱性とインシデントを管理している。PSIRT は、製品のセキュリティインシデントおよび脆弱性に関連するリスクの特定、評価、軽減、および処理に焦点を当てている。これには、製品、ソリューション、コンポーネント、サービスが含まれている。PSIRT サービスは、安全な開発ライフサイクル (SDL) に不可欠な要素である。

付録 5:憲章テンプレート

憲章には、目的、ビジネス上の問題、背景 (オプション) 、チーム憲章、メインスポンサーを含めるべきである。たとえば、次のようになる。
製品セキュリティインシデントレスポンスチーム(PSIRT) は、会社の製品のセキュリティ関連のすべての側面において開発チームをサポートしている。これには、開発、販売、または配布したサポート対象の製品、サービス、ソリューションに影響する脆弱性の特定、軽減、および開示が含まれているが、これらに限定されない。PSIRT は[適切な経営層をここに記入]がスポンサーとなって資金を提供している。

付録 6:ポリシーテンプレート

ポリシーでは、製品セキュリティの脆弱性に関して従業員に「何を」期待するかを明確に伝える。これは、制定されたポリシーを「どのように」満たすかを説明するプロセスとは異なっている。各ポリシーまたは一連のポリシーは、企業およびセキュリティ文化に固有である。文書の主要な構成要素には、責任役員、責任部署、有効日、最終更新日、ポリシーおよびポリシーの影響を受ける人も含まれている。ポリシーに含まれる可能性のある例を次に示している。

■既知のセキュリティ上の脆弱性はすべて、Product Security Incident Response Team (PSIRT) に提出して処理および排除する必要がある。
■脆弱性は、レポートを受け取ってから [#] 日以内に評価する必要がある。最終的な結果は、サポート対象の製品と顧客への影響のステートメントになる。
■報告されたセキュリティ脆弱性に対する修正を、製品への影響に基づき、PSIRT で定義されたとおりに提供している。
■修正可能で、顧客側の対応が必要な場合にのみ、脆弱性情報を公表している。

詳細については、成熟度レベル 1 のポリシーと手順を参照する(「Vulnerability Disclosure Policy」は通常、公開文書であることに留意 - ISO/IEC 29147 より)。

付録 7:サンプルチェックリスト

成熟度レベル 1

■運用基盤
■経営層の支援の確保
■ステークホルダーの特定
■予算の確定
■ポリシーの確立
■脆弱性の発見
■脆弱性報告の受付
■PGP キーを使用した PSIRT 電子メールアドレスの設定
■脆弱性のトリアージ
■脆弱性取り込みプロセスの定義
■脆弱性の認定、優先順位付け、および分析のための内部ワークフローの確立
■修復
■修復オプションの分析
■修正または緩和策の文書化
■脆弱性の開示
■CVE/CVSS などの業界標準を採用し、脆弱性を文書化して通知/開示する方法を標準化

■連絡用のテンプレートを作成する
■ステークホルダーとのコミュニケーション
■研究者/発見者への謝辞

成熟度レベル 2

■運用基盤
■憲章の制定
■組織モデルの構築
■経営陣とステークホルダーのサポートの確保
■追加のスタッフ要件の特定
■その他のリソースとツールの特定
■ブランチ/バージョン・サポート・ポリシーとライフサイクルを理解していることの確認
■ベースライン指標の作成
■依存関係マッピングを使用した製品レジストリの確立
■ステークホルダー・エコシステム・マネジメント
■脆弱性管理の鍵となる内部利害関係者の特定
■下流のステークホルダーの特定
■インシデントコミュニケーションと調整の確立
■脆弱性の発見
■報告されていない脆弱性を発見するプロセスの確立
■脆弱性のトリアージ
■品質レポートを繰り返し提供してくれる報告者の特定
■脆弱性再現能力の開発
■修復
■セキュリティ対策管理計画の策定
■脆弱性の開示
■ステークホルダーへの周知体制の整備
■脆弱性指標の確立
■トレーニング/教育
■PSIRT チームメンバーへのトレーニングの提供
■フィードバック機構の提供

成熟度レベル 3

■運用基盤
■ポリシーの策定
■脆弱性管理コストの決定
■ステークホルダー・エコシステム・マネジメント
■発見者コミュニティとの直接的な関わりの開始
■コミュニティおよび組織への取り組み(FIRST.org などの組織に参加するなど)
■ステークホルダー指標の作成
■脆弱性の発見
■製品コンポーネントの脆弱性監視
■新しい脆弱性の特定(フィード、フォーラム、外部サイトの監視)
■脆弱性検出指標の確立
■修復
■高度なインシデント処理の定義
■脆弱性リリース指標の開発
■脆弱性の開示
■ステークホルダー/業界の調整に関するプレイブックの作成
■トレーニング/教育
■開発チームのトレーニング
■全ステークホルダーへの継続教育の定着