Deloitte.
デロイト トーマツ

IT と製品でこんなに違う！

～製品に求められる SIRT 活動の勘所～

はじめに

近頃、サイバーセキュリティに関するインシデント対応を行う体制として「CSIRT」という言葉は、セキュリティに携わる部署にいれば、一般的な用語になってきたように感じる。CSIRT とは、（Computer Security Incident Response Team ）の略称であり、自組織内のコンピュータやネットワークに関するセキュリティインシデントの対処を主たる目的とした体制を指す。近年では、IoT 化の潮流もあり、CSIRT に続いて「製品 SIRT」や「PSIRT」という言葉もちらほらと耳にするようになったのではないだろうか。CSIRT がコンピュータやネットワークを対象とした組織であることに対して、製品 SIRT/PSIRT とは、自社製品に関する脆弱性への対応、製品に関するセキュリティ品質の向上等、製品が対象となる組織である。

とはいえ、現状、製品に関するセキュリティ対応に関する絶対的な指針は存在しないため、製品 SIRT を立ち上げたいが、どうしたらよいかわからないという声も併せて頻繁に耳にする。中でも、よくある誤解として、IT 領域が主体の CSIRT と混同してしまった発言の例として、ある企業のセキュリティ担当役員 A 氏の話が以下にある。

セキュリティ
担当役員 A 氏

どうやら近頃製品セキュリティへの意識が高まっているようだ。弊社でも製品 SIRT を立ち上げなければならないが、幸いなことにすでに CSIRT の整備を行っている。そのまま体制やプロセスを転用すれば十分だろう。

A 氏の考え方は正しいのであろうか。IT 領域が主体の CSIRT と、製品領域が主体の製品 SIRT では、インシデント等のセキュリティに関する事象の早期終結を目的としているという観点では同じである。では CSIRT と同じプロセス、体制で製品 SIRT を運用してみるとどのようなことが起こるのか？以下では、インシデント対応時の代表的なプロセスを例として、①インシデント等の情報の検知や、②封じ込め対処方法、③対外報告の各プロセスに対して、自動車に関する SIRT 活動を例に、CSIRT と同様の方法ではうまくいかない理由を紹介する。

IT セキュリティと製品セキュリティにおける性質の違い

① インシデント情報の検知

当然のことだが、CSIRT で検知した情報は高確率でサイバー攻撃に関する事象である。そのため、検知をしたらそのままインシデント対応のためのステップに進めばよい。

一方で、製品 SIRT において検知した情報は、一般的に製品の不具合情報などに関するものが多く、品質問題に繋がる事も多い。例えば、自動車において「車両のブレーキが作動しなかった」という情報を取得したとする。当然、インパクトの大きい事象ではあるが、製品のセキュリティが侵害されたのか、それとも製品不具合であるかを即座に判断することは難しい。また、動作不良として報告されていた事象が実はサイバー攻撃による影響によるものであったにも関わらず見過ごされた結果、対処が遅れてしまう可能性もある。

つまるところ、製品に対してサイバー攻撃であると判断するための絶対的な要素がないため、明確に切り分けを行うことは難しく、判断に時間がかかってしまうのである。

一般的に、純粋な製品不具合による問題は、社内の品質保証部門が主となり対応することが多いが、製品へのセキュリティという観点を踏まえるのであれば、不具合対処の際にも、製品セキュリティ担当部門との連携を密に行い、状況把握する等、迅速に対応を行うための情報収集が重要となる。

② 封じ込め対処方法

検知したインシデントに対して、どのように対処するべきなのか、例として、ネットワーク上のあるサーバーに対して、意図的に過剰な負荷をかけサービスを妨害する DoS 攻撃（Denial of Service Attack）が行われた場合における IT 領域と製品領域の比較をしてみる。IT 領域の場合では、ネットワークは専門の担当者が管理しており、発生源の特定、および対処が容易である。そのため、一時的なネットワークの切り分け、特定の IP からのアクセスを遮断する等、暫定対応における定石がある程度定まっている。

では、製品に関する場合はどうだろうか。製品は可動性が高く、専門の人が常時管理をしているわけではないため、IT と比較して、害が発生する場所を即座に特定することが難しく、適切な対処が一様ではないということがある。

近頃では自動車の技術発展が目覚ましく、駐車サポートや、追従走行など自動運転機能をサポートする自動車が普及しつつある。高速道路で前を走る車両を追従中に、攻撃を検知した際の対処が適切でない場合、事故につながる可能性もゼロではない。そのため、製品に関するインシデントが発見された場合は、ドライバーに対する通知機能も含めてフェールセーフに対処できるよう慎重に検討しなければならない。

また、車両に搭載された実績を持つ、ある電子デバイスに対して深刻な脆弱性が ISAC（Information Share and Analysis Center の略であり、業界ごとにサイバー脅威に関する情報を収集、提供することで、各企業が迅速にサイバー脅威に対応できることを目的とした非営利団体を指す。国内では自動車、医療、金融などの分野で ISAC が設けられている。）等を通じて報告された際には、当該デバイスを搭載している車両のドライバーに対してダイレクトメールや E メールなどで通知を行う必要がある。しかし、生産、販売を行った膨大な車両の中から、車種、車種の世代、販売地域、搭載しているデバイスのソフトウェアバージョンなど、多くの情報をもとに影響を受ける車両を特定しなければならない。

実際に、セキュリティに関する世界有数のカンファレンスである Blackhat にて、2019 年に報告された BMW のインシデントレスポンスに関する報告では、上記の確認作業のために、連絡を受けてから影響を受ける車種を特定するまでに 10 日もの期間を要したとしている。

迅速に対象のユーザに通知するためにも、生産・販売した製品の情報および、製品に搭載されているソフトウェア等の来歴管理を行う、あるいは管理を行っている部門と即座に連携を取れる体制であることが望ましい。

③ 対外報告

インシデントが発生した際には、詳細調査のためにサプライヤーやセキュリティベンダーへの依頼、被害拡大防止ならびに再発防止策の検討のために IPA（Information-technology Promotion Agency, Japan：コンピュータウイルスやセキュリティに関する情報提供などを行う独立行政法人）や ISAC 組織、他社の SIRT への周知等、様々な目的で外部組織と情報連携する必要がある。

しかし、もし報告する脆弱性等が、リコールなどの品質保証問題に関わるようなものであると判断された場合、品質保証問題発生時の報告フローが優先されるため、上記の ISAC や他社 SIRT へ発生し次第即座に報告するということは難しい。

また、インシデントの詳細を調査するためにサプライヤーやセキュリティベンダーに調査を依頼する場合もあるが、外部に依頼をするということは、すなわち社内の製品情報を外部に渡すこととなるため、不用意に外部に製品情報を流出させないためにも受け渡しのルール等は契約時に定めておく必要がある。

従って、インシデント情報や脆弱性情報が提供された場合、事象がどのような状態（リコールにつながるようなものなのか、外部に提供しなければならない情報は何なのか等）を踏まえて、適切に連携する組織を判断しなければならない。

	CSIRT	製品SIRT
①インシデント情報の検知	高確率でサイバーセキュリティに関する事象であるため、判定のプロセスは不要	単純に製品の不具合である可能性もあるため、セキュリティに関連するかどうかの判定プロセスが必要
②封じ込め対処方法	暫定対処として、対象の機能やNWを一時遮断することが可能	CSIRTと同じ対処も可能だが、対象がミッションクリティカルであったり安全に関わる場合は慎重に判断
③対外報告	フローに沿って報告	インシデントの重大性によって報告すべき相手やフローが変わる

図 1：CSIRT と製品 SIRT の相違点のまとめ

社内外の組織との連携が重要

前述において、インシデント対応の際の①インシデント情報の検知、②封じ込め対処方法、③対外報告を例に、製品セキュリティで考慮しなければならないことを解説した。いずれの場合においても言えることは、製品 SIRT を効果的に機能させるためには、社内、および社外の組織との連携が非常に重要ということである。製品に関するインシデントの場合、品質保証部門、開発部門、生産部門、渉外、お客様相談窓口、サプライヤー、ソフトウェアハウスと実に多くの組織が関わっており、IT 領域と比較すると、責任の所在や役割もより複雑になってくる。

多くの組織が関連する製品セキュリティにおいて、適切に連携先を判断し、適切なプロセスで連携を行うことは容易ではない。ではこの実現に向けてどのような活動を行えばよいのだろうか。以下に長期的な視点、および短期的な視点で行える施策の例を紹介する。

連携に向けてどう取り組めばよいのか

短期的な視点での施策においては、以下の二つが挙げられる。

ひとつは、自組織における CSIRT との役割の共通点・相違点を明確にすることである。製品セキュリティと IT セキュリティの性質の違いを先述したが、社内向けの教育や啓発活動、セキュリティ関連の窓口の一本化、共通のリスク判定ポリシーを使用する等、共通化する工程には、CSIRT/製品 SIRT の兼任者を設置することでリソースやコストを節約することができる工程もある。また、兼任者を設けることは、CSIRT/製品 SIRT 間の密な情報共有を容易にするというメリットもある。このように、製品 SIRT を立ち上げる際には、CSIRT と分けるべき内容を明確にした上で、自社の既存の体制、リソースなどを鑑みて体制を検討することが望ましい。

もうひとつは、FIRST の発行する「PSIRT Services Framework」）（https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0）を参照することである。これは、国際的な CSIRT のコミュニティである FIRST が発行した、製品 SIRT に関する機能を整理したフレームワークであり、脆弱性の発見からトリアージ、分析、開示方法等、製品セキュリティについて多岐に渡る情報が公開されている。社内外の各組織との連携における目的や効果なども記載されており、連携組織を特定する際の一助とすることができる。加えて製品 SIRT 組織を立ち上げた場合、インシデント対応や社内外の組織との連携プロセスの定期的な見直し等、継続的な改善が必要となる。その際に PSIRT Services Framework は、見直し時の基準とすることや、必要な基礎知識を振り返る際にも有用となる。

また、長期的な視点での施策例は、人材育成である。製品セキュリティに関連する組織は多岐に渡るため、それらの組織と円滑にコミュニケーションをとることができるスキルは非常に有用となる。スキル向上の方法の例として、製品開発部門の人材を OJT の名目で、一定期間セキュリティ統括部門で活動してもらい、広い分野の視野を持つ人材の育成を行う、また、ISAC 等の業界横断で活動可能な組織での活動を通じて、社外のコネクションの確立や、他社との相場観の獲得等に役立てることができる。

効果的な製品 SIRT の構築に向けて

ここまで、製品 SIRT 構築において、CSIRT 組織との立ち位置の違いの理解、ならびに連携の重要性を説明した。これらを踏まえて、セキュリティ担当役員 A 氏の考えが次のようであれば、今後の製品 SIRT 構築計画においても、安心が持てる。

セキュリティ
担当役員 A 氏

製品 SIRT を立ち上げなければならないが、むやみに CSIRT と同様にするのではなく、まずは CSIRT との領域の違いを明確化した上でどのような体制やプロセスするかを検討しよう

近年の IoT 化に伴い、製品のコネクテッド化も著しい。特に、自動車業界においては、その特徴が顕著に表れており、WP29 で策定された型式認可においても、自動車製品に対するインシデント対応体制の構築が言及されている。そのため、今後 IT 領域だけでなく、製品に関するセキュリティへの対応も求められるようになることは必至となる。その際に対応を開始する前に、社内外のどの部門や組織と連携しなければならないのかを整理した上で、既存の CSIRT 等の体制も踏まえて検討をはじめることが重要である。

デロイト トーマツ サイバー合同会社
Mail　ra_info@tohmatsu.co.jp
URL　www.deloitte.com/jp/dtcy
【国内ネットワーク】　東京・名古屋・福岡

※貴社および貴社の関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス 内容がご提供できない可能性があります。詳細はお問合せください。