# xSIRT構築事例に関するヒアリング結果 [概要]

**ヒアリング対象：**電気機器、通信、IT、小売、自動車部品、デジタルサービス 等　（中小企業含む）

## 1. 機能構築の経緯

**（1）きっかけ**　●概ね①自社でのインシデント発生、②自社の新しいデジタルサービスの供用開始、③脅威動向を踏まえた対応に類別。（自動車部品では規制対応も）
●一部では、設立にあたり経営層のリーダーシップが発揮された事例も。（全社部門への位置づけ等）

**（2）参考事例**　●2017年以前は各社手探りでの対応か、外部コンサルの支援の下で設立。
●2018年以降、FIRST「PSIRT Services Framework」※が参照されている例もみられるが、初見ではハードルが高く、背景知識が必要との声も。
（自動車部品では米国AUTO-ISAC「Best Practice Guides」を参考にされるなど、業界ごとの動きもあり。）

※ FIRST(Forum of Incident Response and Security Teams) が発行する支援ガイド(2018年7月にver.1.0発行)。2019年11月にJPCERT/CC・Software ISACが共同して日本語版を作成。

## 2. 組織上の位置づけ

**（1）組織名称**　●SIRTという名称を掲げていないケース、デジタルサービスを対象としてもPSIRTと呼称するケース、PSIRTとDSIRTが並列するケースなど様々。

**（2）組織階層**　●各事業部門・製品部門ごとに設置されるケースと、全社部門に設置されるケースとに類別。
前者では、特に製造系でそうした部門の特徴や権限が色濃く、それらの品質管理部署が兼務し、事業所階層でも設置されている場合が多い。

**（3）所掌事務**　●脆弱性対処に特化しているケースと、企画・開発プロセスへの関与も含まれるケースに類別。また、こうした機能を複数の部署で分担するケースも。

※ FIRSTのFrameworkでは、脆弱性対処を中心に、Discovery / Triage / Remediation / Disclosureのプロセス別に事務を記述。

## 3. 開発プロセスへの関与にあたっての留意点・課題

●SSIRTが他サービスと連携したサービスのリスクマネジメントを行う一環として、他サービスの仕組みに踏み込んでリスク評価を行う例がみられた。

●グループ会社の新規サービスを須くホールディングスで集約してレビューする例がみられた。

●アジャイル開発の場合に、段階的に対応を依頼して最終段階ですべてが対応されるよう管理する、スプリントを分割し指摘はその次のスプリントで反映することをルール化するなど、開発側に過度な負担がかからないような工夫がみられた。

※ FIRSTのFrameworkでは、Stakeholder Managementの一部としてセキュア開発ライフサイクル(SDL)への参加を位置づけも、具体の方法論に関する記述はない。

## 4. 脆弱性対処にあたっての留意点・課題

●Discovery：脆弱性発見者に報酬を支払うバグバウンティ制度を実施している例や、定期的に外部へテストを依頼して脆弱性の発見に努めている例がみられた。

●Triage：台帳管理を廃止し、ソフトウェア構成（Software Bill of Materials：SBOM)をシステム上で管理し、自動収集した脆弱性情報とマッチングさせる例がみられた。

●Remediation：製品によってサプライチェーンの中での位置づけが異なることを踏まえ、事業部門ごとにサプライヤーと連携している例がみられた。

●Disclosure：外部テストで見つかった脆弱性について漏れなく情報公開を行う例がみられた。

## 5. その他

**（1）中小の課題** ●中小企業では追加人員確保が難しいため負荷の軽減が重要。パッケージサービス導入や取引先からの確認フォーマットの普及を進めてほしいとの声も。

**（2）求める能力** ●自社サービス仕様への理解、サービス間の相関の整理能力、脅威情報の収集能力、社内外との調整能力など様々。スキルセットの整理が必要との声も。

※ FIRSTのFrameworkでは、PSIRTに必要なトレーニングとして、脆弱性対処を念頭に技術・コミュニケーション・プロセス・タスクツールと整理。具体スキルの記述はなし。

# 1．機能構築の経緯

（凡例）●：傾向やまとめ
○：ヒアリング内容

## （1）きっかけ

●きっかけは、概ね①自社でのインシデント発生、②自社の新しいデジタルサービスの供用開始、③脅威動向を踏まえた対応（マルウェアの流行等）に類別される。なお、自動車部門では、規制対応というきっかけもみられた。

○発生した自社のインシデントについて、営業サイドから上がってくるユーザ利便性に関する要求に引っ張られ、仕様が甘いまま進んでしまった結果と分析。新たな組織を立ち上げるなど、対応を進めてきた。（小売）

○自社サイトを改ざんされたことを契機にPSIRTを設立し、その後、内部対応に特化する組織としてCSIRTを別のチームとして新設した。（デジタルサービス）

○実際に発生したインシデントを契機として組織化された。（電気機器）

○マルウェアの被害を受けたことで、社内のセクター（社内IT、開発試験、生産・製造、プロダクト＆SI、サプライチェーン等）を強化する取り組みを始めた。（電気機器）

○CSIRTの一部として、クラウドサービス商品の提供開始に伴う、開発部門内のサイバーセキュリティ対応体制として発足し、発足2年後にPSIRTの活動を開始した。（デジタルサービス）

○PSIRTを持つことで、ISO 27001等とは異なった、製品に特化したセキュリティ対策を行っているという、企業として攻めのセキュリティの姿勢をアピールできると考えた。（デジタルサービス）

○宅配業者を装ったマルウェアが蔓延したことが開設のきっかけとなった。CSIRTフレームワークをベースに開設し、SSIRT活動を開始した。予防（リスクアセスメント/対策推進）、検知（不正利用等の監視/運用）、対処（インシデント対応）を行っている。（通信）

○経営を脅かす脆弱性(Code RedやNimdaといったワーム、SQLインジェクション、自社製品の脆弱性)が増加してきていた時期であり、当時は多様な製品を作って売っていたため、セキュリティ専門の組織が必要となった。自社製品や顧客システムの脆弱性を一個一個個別に管理していくことに限界を感じていたことも要因である。（電気機器）

○PSIRT構築前からセキュリティに対する漠然とした不安があった。「Software ISAC」のPSIRT協議会に参加した際にPSIRTを知り、意識し始めた。（デジタルサービス）

○米国カーメーカーからの要求及び、法令・規格（WP29、ISO21434）への対応。（自動車部品）

## （１’）経営層のリーダーシップ

●一部では、設立にあたり経営層のリーダーシップが発揮されている事例がみられた。

○有識者が経営層に必要性を訴えて設立が大きく進んだ。（電気機器）

○社長指示で組織が設立された。発足当初は事業部門に置かれていたが、他事業部門との連携強化を目的に、社長指示で現在の全社部門に移管された。（通信）

○元来、EC事業を実施していたためセキュリティに関する経営層の意識は強かったが、課題認識や具体的に何をやればいいか、といった点について認識できていなかった。（小売）

○経営層はセキュリティの重要性を理解しているが、現場に落としていく中でセキュリティへの意識や認識が薄まってしまい、現場への共有が難しいといった課題もある。（デジタルサービス）

○セキュリティはブランディングのための投資という考えについて、これまでは予算化はしていなかったが、対策として取るべきことも明確化しているし、専任を雇いたいので、今後は予算化したいと考える。（デジタルサービス）

○すでにセキュリティは経営課題となっており、事業部内のセキュリティ推進体制はセキュリティ有識者から事業部長が任命する。（電気機器）

## （２）参考事例

●2017年以前は、各社手探りでの対応か、外部コンサルの支援の下で設立した。2018年以降は、FIRST「PSIRT Services Framework」が参照されている例もみられるが、初見ではハードルが高く、背景知識が必要との声もある。なお、自動車部門では、米国AUTO-ISACが発行するベストプラクティス集「Best Practice Guides」を参考にされるなど、業界ごとの動きもあり。

○発足当時は参考にした事例はなく、手探り状態であった。現在はFIRST「PSIRT Services Framework」を活用し、不要なプロセスは実態にあわせて削除している。ただし、初見だとハードルが高いと思われ、一定の背景知識が必要と考える。（電気機器）

○組織によって理想とするPSIRT組織はそれぞれ異なるので、FIRST「PSIRT Services Framework」等のフレームワークを参考にしつつも、手段が目的とならないよう気をつけている。（デジタルサービス）

○時代に合わせて随時アップデートしている。参考にした事例等はなく、独自のやり方で進めてきた。自社の取組が他社に先駆けている状況である。製品開発のガイドラインなども社内のノウハウをまとめ、時代に合わせて更新している。（電気機器）

○FIRST「PSIRT Services Framework」や、米国AUTO-ISACのベストプラクティスを参考にしており、社外コンサルも受けている。（自動車部品）

# 2．組織上の位置づけ

## （1）組織名称

●組織の名称については、SIRTという名称を掲げていないケースや、デジタルサービスを対象とする場合にもPSIRTと呼称するケース、機密性→PSIRT／可用性→FSIRT／完全性→DSIRTと並列し、機能で役割分担しているケースなど様々。

○SSIRTはグループ会社へアウトソースしており、社内のシステムセキュリティ部門の傘下に、SOC、CSIRTと並列で属している。SSIRTはCSIRTに比べダイナミックであり、アプローチの方向性が異なるため、「CSIRTの一部」という考え方はない。インシデントレスポンスの中身が違うことを理解する必要がある。（通信）

○以前はセキュリティのポリシーと実施に関する全ての権限がシステム部門に集中していたが、現在はシステム開発を行う部門、システムの企画・要件定義におけるセキュリティ機能をレビューする部門、およびグループ統一のセキュリティポリシーを制定・運用する部門の3部門で権限を分け、三権分立のような関係になるようにした。（小売）

○グループ各社も含めた、グループ全体のPSIRTの位置づけで活動しており、グループ各社も対象としている。CSIRTとPSIRTのデマケーションについて、自社システムならCSIRT、製品ならPSIRTが対応している。CSIRTとは縦割りで別組織のため、CSIRTとの人材交流は特に行っていない。（電気機器）

○セキュリティチームの下にPSIRT、FSIRT、DSIRTが並列でぶら下がる構造となっており、セキュリティチームは社内SOCと連携している。外部連携については、セキュリティチームが窓口となり、FIRST、日本シーサート協議会、JPCERT/CC、サイバーセキュリティ協議会と情報共有・連携を行っている。（デジタルサービス）

## （２）組織階層

●各事業部門・製品部門ごとに設置されるケース（中には工場に設置されるケースも）と、全社部門に設置されるケースと2極に分かれる。前者では、特に製造系でそうした部門の特徴や権限が色濃く、それらの品質管理部署が兼務し、事業所階層でも設置されている場合が多い。

○情報セキュリティ統括部門のPSIRT、本社部門のPSIRT、事業所のPSIRTから構成される。本社部門のPSIRTはセキュリティ技術開発者が兼務、事業所のPSIRTは品質管理部門が兼務している。（自動車部品）

○全社的な製品セキュリティセンターが社内全体のセキュリティを対応しており、その中でバーチャル組織としてPSIRT(10名ほどで構成)がある。脆弱性対応の発生頻度から、常時専任で対応が求められるほどの作業量となっていないため、PSIRT担当者は、専任ではなく兼任となっている。（電気機器）

○事業所ごとに製品セキュリティ推進組織を設置し、PSIRTは各事業所の製品セキュリティ推進組織と、IPAやJPCERTの外部との間に入って対応している。製品セキュリティ推進組織間で連絡会を定期的に実施しており、対応情報の共有やOSSの脆弱性情報の共有などを実施している。（電気機器）

○製品セキュリティセンターには、実機の診断、脆弱性の再現性や対策の検討を行う部門、各事業部と連携し、対策時期や公開方法、発見者の情報の公開(謝辞)等を支援する部門、OSSの脆弱性などの情報の展開、方針決定、全体調整を担当する部門がある。（電気機器）

○グループ会社へのガバナンスとして、各グループ会社に情報管理委員会を設置し、情報管理統括責任者が委員長を務めている。同委員会の事務局が、本社情報管理委員会と各社の窓口となっており、半年に1回やり取りをしてホールディングスで決めたポリシーを周知・準拠してもらうという形をとっている。（小売）

## （2）組織階層（続き）

○BU（ビジネスユニット）制を採用しており、グループ・コーポレートと各BUから構成される。CSIRTはグループ・コーポレートに属しグループ全体を対象として活動しており、PSIRTはものづくり本部、D/SSIRTは品質保証本部に配置、PSIRTはBU毎に設置している。グループ全体のセキュリティを統括する情報セキュリティリスク統括本部はCISOにぶら下がった組織となっている。セキュリティセンターは、サービス＆ビジネスプラットフォーム内の事業本部に属し、脆弱性に関する情報収集・共有とインシデント対応の支援という技術的対応に特化して活動しており、ルール作り等の統制活動は品質保証・IT部門にて行っている。セキュリティセンター、その下部組織に事業部セキュリティチーム、さらにその下に開発・運用部門といった組織構造となっている。（電気機器）

○社内の体制は、サイバーセキュリティ統括部門→セキュリティ技術センター長→PSIRT責任者→各メンバーという組織構造となっている。（電気機器）

○他業務と兼務しており、PSIRT専任はいない。PSIRT主責任者は「脆弱性診断、ペンテスト、インシデントハンドリング、PJ統括」など、副責任者は「脅威動向調査、発信、技術/製品評価、海外連携」など、チームメンバーは「インシデント解析、脅威動向調査、発信、社外講師、システム開発」などを担当している。（電気機器）

○基本的には社外連携は行っていないが、問い合わせ先のMLに委託先の連絡先が含まれることはある。（デジタルサービス）

○FSIRTは、海外工場での古い機械（Windows XP組み込み機など）、USBの使用等の対応が主である。 マルウェアが多少侵入していても「止めない」ことが優先されてしまう状況があることが課題である。（デジタルサービス）

## （3）所掌事務

●脆弱性対処に特化しているケースと、企画や開発プロセスへの関与も含まれるケースに類別される。また、こうした機能を複数の部署で分担するケースもある。

○PSIRTは出荷後の脆弱性対応を担当範囲としているが、出荷前については製品セキュリティセンターとしてセキュリティ診断などの対応をしている。発生している事象の説明も製品セキュリティセンター側で行っている。事業部門の人に橋渡しを頼らなくても、製品セキュリティセンターが事業部に平易に伝わるよう、納得しやすい理由を押さえて伝えるのが役割と考えている。（電気機器）

○現在のPSIRTは、届け出相談対応、プロトコルの脆弱性等の情報収集、開発現場との調整がメインだが、今後は、より能動的に情報取得が必要と考えており、自社製品を弱い状態で公開し、どのような攻撃が来るかを確認している。（電気機器）

○現場にとって脆弱性対応の優先度が下がることも実際にはあるが、総合的なリスク判断は、最後は事業部の判断になるものであり、案件ごとの対応になる。ただし、重要性の認識や、各事業部の対応窓口の担当者との関係醸成もできてきており、対応は良くなっている。日ごろから同業他社の事例共有等もしており、必要性は理解されている。（電気機器）

○CSIRTのRは「Response」だが、SSIRTのRは「Readiness」であり、サービス設計時から関与し、セキュリティをデザインしてサービスに組み込むことが主な役割だと理解。（通信）

○サービス連携を行う他社との組織をまたいだ連携について、グループ会社向け管理規程策定や、グループ会社へのSSIRT構築、当社で最低限のアセスメントの他社での実施を検討している。（通信）

○事業所のPSIRT内で、脆弱性対応と、脆弱性対応以外の製品セキュリティ対応で統括責任者（役職は課長級）を分けており、各統括責任者の下にセキュリティ担当者（情報/工場セキュリティ対応）、セキュリティチームリーダ（製品セキュリティ対応、主に設計）、セキュリティ実務者（製品セキュリティ対応、主に設計）が従事している。（自動車部品）

○事業所のPSIRT間で定期的に（月2回）横通し会議を実施している。各事業所内では毎週実施している。（自動車部品）

○自工会要求事項と自工会セキュリティチェックシートの配布を行っている。自工会からは取引に際して適合の要求があるが、実態は追い付いていない。（自動車部品）

○そのほか、契約内容の見直し（開発プロセスの見直し、情報提供、監査対応など）や、インシデント/脆弱性情報の提供要求、暗号鍵管理の仕組み構築要請、カーメーカー要求への対応などを行っている。（自動車部品）

## （３）所掌事務（続き）

○サプライヤとの連携は、資材部を通さず、契約している製造部が窓口になっている。（自動車部品）

○社内向けには、早期警戒情報や、インディケータ情報の発信のほか、注意喚起やレポートの発行を行っている。（電気機器）

○外部からの問合せ対応のための共通ポリシー作成、問合せ対応ガイドに基づく運用、セキュリティホワイトペーパー雛形の提供を行っている。ホワイトペーパーの内容を超える依頼等があった場合は、NDAを締結するようルール化している。（デジタルサービス）

○改正個人情報保護法/海外個人データ保護法への対応支援（データマッピング等による）を行っており、海外の法律に対する対応は専門家が欲しいところだが、現状は外部コンサルへの依頼等で対応している。（デジタルサービス）

○ISMAPやNIST SP800-171等の監査基準に基づくセキュリティ内部監査を実施している。（デジタルサービス）

○セキュリティチームメンバーのうち半数は常任メンバー。全員兼務で専任メンバーはいない。DSIRTはクラウドサービス商品の共通基盤を担当するグループに設置し、各商品グループから兼務者をアサイン、一部を除きセキュリティチームとは兼任しない。PSIRTはIoT機器のセキュリティを担っており、数名体制で運営している。グループ内で別個にCSIRTが設けられていたが、現在は統合している。（デジタルサービス）

○PSIRTは製品に関するセキュリティの強化や、製品起因のインシデント対応を行っている。開発本部に属し、メンバーのうち大半は専任、一部は情シス、現地コミュニケーターと兼務している。最近の加入メンバーはセキュリティをバックグラウンドとするものが多い。（デジタルサービス）

○CSIRTは社内ルールの策定やセキュリティ教育の実施、社内インシデント対応を行っている。社長直下の組織となっている。（デジタルサービス）

○部門間（特に、企画部署、開発運用部署におけるセキュリティ機能・担当、DSIRT/SSIRT機能を担う組織）の連携・協働について、リスクアセスメントの実施（社内規程）や個別相談受付、課題管理・定期会合主導を行っている。今後の課題として人材交流も検討している。（通信）

○他部門との調整が大変である。JPCERTからの脆弱性に関する第一報を主管部門に問い合わせると、中身がOEMだったり、さらに開発を外注しているなどのケースもある。（電気機器）

## ３．開発プロセスへの関与にあたっての留意点・課題

○従来も、新サービスのリリース前に監査を実施するルールだったため、SSIRTが関与することに対する抵抗は特になかった。また、SSIRTが決済サービスのリスクマネジメントの一環として、銀行決済の仕組みにまで踏み込んでリスク評価を行うことも考えられる。（通信）

○開発部門との連携は、法令・規格に基づいたプロセスとして、規則・手順書で整備している。（自動車部品）

○グループ会社の新規サービスに対し、企画段階、要件定義段階でセキュリティ基盤部によるレビューをかけ、リリース前にもテストを実施し、脆弱なシステムを作り出さないよう制御している。この手順等は、統一ポリシーで規定されており、ホールディングス側に集約して必要なセキュリティ対策が実施されているかレビューしている。アジャイル的な開発の場合、すべてをレビューするのは難しく、どこまでセキュリティ担保するかというのは課題。（小売）

○セキュア設計開発支援として、セキュア設計開発ガイドの策定と、設計開発を行っている。Waterfall型をベースに作成し、リスクの洗い出し・点数化や他社の脆弱性にも対応させ、内容を充実させている。アジャイル型開発の場合は、細かいサイクルでの適用になるので、開発側に過度な負荷がかからないよう完全な形ではお願いしておらず、段階的に対応を依頼し最終的にすべてが対応されるよう管理している。（デジタルサービス）

○現在採用している製品開発サイクルは、4つのスプリントから構成され、2週間を1スプリントとして開発しているものが多い。スプリントごとに設計及び成果物に対してレビューを行い、営業やサポートから指摘があったら、次のスプリントで修正する。全スプリントが終わった時に改めてレビュー、テストを実施している。（デジタルサービス）

○複数の異なる事業部門や他の組織の提供するサービスとの連携における、セキュリティインシデントに対処する連携体制の構築について、自社のサービス総数は100を超えるが、現在SSIRTでカバーしているのは数十個。SSIRTが一時統制する体制で、必要に応じて内部統制部門へエスカレーションしている。社外については、サービス主管部門が連絡体制を構築（現状は主管を介して連絡）。（通信）

○当初は、グループ会社を中心にITインフラやシステムの構築・運用が外部ベンダーに丸投げされていることで、インターネットの出入り口がどういう構成になっているかわからないなど、社内のIT環境が十分に把握できていない状況だった。現在までに、そういった既存システムの実態把握およびアセスメントと新しく構築するシステムのセキュリティ担保を並行して行ってきた。（小売）

○EC事業をやるうえで必要な仕様を決定し、グループ全社が同じレベル感でセキュリティ対策を実施していくため、情報資産管理等のグループ全体で統一のセキュリティポリシーを昨年までに制定し、グループ全体でそのポリシーに則ったシステム構築・運用を行えるよう整備してきた。（小売）

## ３．開発プロセスへの関与にあたっての留意点・課題（続き）

○インシデント発生の際、実際にひとつの事業をやめる結果に至ったことで、全員がセキュリティの重要さを、身をもって再認識した。しかし、DXの取り組みの中でSaaS等導入しやすいものが調査不十分で上がってくることがある。依然としてセキュリティがビジネスを阻害するという意識もあるなかで、現状どういうリスクがあり、このリスクを取るかどうかの経営判断が必要であること等を、個別丁寧に説明して握っていくということをセキュリティの統括部門で進めている。（小売）

○セキュリティ投資はコストという側面があるため分野によって整備状況に差はあるが、セキュリティ対策とリスクが直結しやすいIT部門や、WP29対応に迫られた自動車部門では、先行して取組を進めてきた。他の部門の体制づくりを進めていく中で、既存の体制と矛盾しないようにしないよう整合性を取る必要がある。（電気機器）

○時代を経るにつれ、より現場でセキュリティを確保する体制へと変化していった。当初はセキュリティセンターにのみ高度セキュリティ人材がいる状況だったが、事業部セキュリティチームや開発・運用部署にもセキュリティ人材のニーズが高まっており、開発時のセキュリティ作りこみや、現場のセキュリティ確保を行っている。（電気機器）

○サイバーセキュリティ対策の実施状況の把握のため、クラウドサービス商品と基盤を対象に、DSIRT主導で各部門のレポート等を収集することで実施状況を調査し、四半期報告書を発行している。当報告書は経営層の指示によるものではない。（デジタルサービス）

○セキュリティのチェックのタイミングは、各スプリント中とリリース直前（4スプリント完了後）に設けている。スプリント中のチェックは設計レビューと、成果物に対してテストを行う。リリース直前にもテストを行う。製品開発サイクルにて、プロダクトマネジメント要件が決まったらプログラマー、品質保証エンジニア、PSIRTが連携して対応、懸念があればその時点で説明するなどしている。（デジタルサービス）

○1スプリントを2週より短くするのは厳しいが、テストはまとめて1週間ということも行っている。製品の特徴によって決めている。このサイクルも、他社を参考にしたのではなく、自社内でこうしたい、といったところが起点となっている。（デジタルサービス）

○PSIRTでは、製品のセキュリティ実装方法までは関与していない。開発チームがコーディング時にセキュリティを意識している。（デジタルサービス）

# ４．脆弱性対処にあたっての留意点・課題

○脆弱性発見者に報酬を支払うバグバウンティ制度を開始。また、年1回外部へテストを依頼し、脆弱性の発見に努めている。（デジタルサービス）

○製品セキュリティ推進組織の連絡会を定期的に実施しており、対応情報の共有やOSSの脆弱性情報の共有などを実施している。（電気機器）

○お客様からの脆弱性問い合わせの窓口対応を行っており、各開発チームへヒアリング（パッチ適用による影響有無、対応方法、セキュリティ対策状況など）し、PSIRTと連携した脆弱性情報/脅威情報の展開と対応管理を行っている。先日問題となった、プリントナイトメアのような影響が大きな脆弱性についてはセキュリティチームと連携し、全社レベルで対応している。（デジタルサービス）

○脆弱性情報収集について、従来のようなExcelシート上での台帳管理を廃止。すべてのソフトウェア構成（Software Bill of Materials：SBOM)を社内システム上で管理し、自動収集した脆弱性情報とマッチングさせている。（電気機器）

○他社製品を含む未公開脆弱性関連情報を管理するシステムと、公開済み脆弱性情報を管理するシステムを運用している。他部門との調整が大変であり、JPCERTからの脆弱性に関する第一報を主管部門に問い合わせると、中身がOEMだったり、さらに開発を外注しているなどのケースもある。後者のシステムを進化させるとSBOMになるが、どこまでソフトウェア情報を細分化するかが悩ましい課題である。（電気機器）

○自社製品の脆弱性は、自社製品用の脆弱性対応窓口にて届出を受けている。（電気機器）

○製品により、サプライチェーンの中での位置づけが異なる。各サプライヤーの担当者との繋がりが重要なため、各事業部門ごとの各サプライヤーの担当者との繋がりを重視している。（自動車部品）

○外部テストで見つかった脆弱性の情報公開等は、経営層や営業側が懸念を持つことはあるが、漏れなく情報公開を行っている。（デジタルサービス）

○脆弱性情報は、JPCERT/CCやAuto-ISAC、J-Auto-ISACから収集している。JPCERTからの脆弱性情報への対応はコーポレートPSIRTが取りまとめて定期的に対応している。（自動車部品）

○脆弱性検査はケースバイケースで、DSIRTによる内部対応および外部への発注のいずれも行っている。（デジタルサービス）

○IPAやJPCERTが出している脅威情報や、セキュリティ会社が出しているインテリジェンス情報をとりまとめて、緊急でなければ週一程度の頻度で社内に発信している。従前はセキュリティセンターよりすべての脆弱性を随時発信し、現場でチェックする運用を行っていたが、現場の負担が大きかったため、ある程度絞ったうえで重要性が高く確実に見てほしいものを発信している。（電気機器）

## ４．脆弱性対処にあたっての留意点・課題（続き）

○社内外の連携については、脆弱性情報の入手（JPCERT/CCや外部ベンダー、個人などの外部からの入手のほか、稀に社内から届け出を受けることもある）、受け取った情報の社内システム連携、影響調査や対処方針・公開原案の調整を行っている。製品開発者、PSIRT推進責任者に対しては、脆弱性情報の確認、調査・対処（セキュリティパッチ作成など）を行っている。（電気機器）

○未公開脆弱性関連情報を管理するシステムでは一般公開前のJVNで扱われるような脆弱性を、公開済み脆弱性情報を管理するシステムでは一般公開されている脆弱性・パッチ情報を社内向けに配信している。また、製品セキュリティ情報のWebサイトにて、脆弱性情報の社外公開を行っている。（電気機器）

○社外からの脆弱性情報受付については、JPCERTとはメールで直接やり取りを行っている。それ以外は、HP上で公開している脆弱性公開ポリシーに則ってやり取りしている。（電気機器）

○PSIRTでは、社内開発・運用プロセスのテスト、出荷、運用・保守のプロセスにおいて脆弱性情報収集・対処に関する活動を行っている。セキュリティバイデザインや脆弱性診断およびその検証といった、それより前段階の要件定義や設計、実装のプロセスは、PSIRTではなく他のチームが対応している。（電気機器）

○脆弱性診断等の検証は内製でも行っているが、第三者が実施必要な場合など、お客様の要望により外注することもある。お客様の意向によるところが大きく、それによっては細かい要求までするが、手法までは指定しない。（電気機器）

○CNA（CVE Numbering Authority）に加盟しており、グループの製品に見つかった脆弱性について脆弱性番号（CVE）の割り当てが可能である。（電気機器）

○PSIRTでは、製品への脆弱性発見・報告や既知の脆弱性への対応相談を受け付けている。脆弱性対応相談においては、根拠ある「説明責任」を果たせるかを重視している。見つかった脆弱性は公開するのが当たり前の時世にあって、「対応できて褒められるのではなくやって当然」である。一つの脆弱性のずさんな対応が会社全体の不利益につながりかねない、という意識のもと、グループとして統一された脆弱性対応が必須と考える。（電気機器）

○サイバー攻撃や外部からの脆弱性指摘などのインシデントが発生した際、セキュリティチームやPSIRTと連携して対応を支援している。（デジタルサービス）

○最後のスプリントに行う検証について、脆弱性検証はPSIRT内で全バージョン検証している。組織内にもいろんなバックグラウンドの人がおり、権限周りの検出は得意だが、複合的な要因が絡んでいるものは検出が難しい、など得手不得手がある。そういったところをカバーするのが外部発注する目的である。社内と外部で片方しか検出できない場合あるので、内外双方でやることが重要である。（デジタルサービス）

## （１）中小の課題

●中小企業では追加人員確保が難しいため負荷の軽減が重要。パッケージサービス導入や取引先からの確認フォーマットの普及を進めてほしいとの声も。

○中小企業では人員確保の課題がある。専任にしないと厳しいが、即戦力の採用は難しい。特にSOC系の人材採用は難しく、募集条件にマッチする人材がなかなかいない。（デジタルサービス）

○顧客からセキュリティチェックシートの提出を求められる。セキュリティシートを用意し、Webで公開していることが自社のアピールに役立っている。チェックシートの書式がすべて異なるので、統一されたフォーマットがあると良い。コストがかかるのは承知で、ISMAPを取ろうと考えている。（デジタルサービス）

## （２）人材に求める能力

●自社サービス仕様への理解、サービス間の相関の整理能力、脅威情報の収集能力、社内外との調整能力など様々。スキルセットの整理が必要との声も。

○広範囲にわたるサービスリスク分析などは外部に委託するため、セキュリティの知識よりも問題解決能力を重視。具体的には、運用の勘どころをおさえているような精緻なサービス仕様書が必要であり、自社サービスの仕様に対する理解、各サービス間の相関・整合をロジカルに整理できる能力が重要。専門性を測る資格がないことが普及面でも課題。（通信）

○脆弱性に対する理解、世の中の動向等も含めた脅威情報の収集能力、ログ調査等のインシデント対応、といった技術的知識スキルや、社内外との調整・交渉、状況把握と判断、計画作成・実行といった管理的知識スキルが必要。（電気機器）

○求められる能力は求められる役割に依存し、設立当初と現在でも求められるものは異なる。設立当初は「脆弱性情報の一元管理」「関係者との調整（外部公表も含めて）」「脆弱性の定義」、設立中期は「検証方法のアップデート」「多角的な検証」といったことが求められてきた。また、製品ありきの企業なので、製品に対する理解/知識/興味が重要。（デジタルサービス）

○製品セキュリティセンターでは、特別に社内で説明を上手くする教育をしているのではなく説明が得意な人間が対応している。セキュリティ診断については業務として行っているため、業務の中で人材が育成されている。現状として、PSIRTの明確なスキルセットがないのが課題と感じている。（電気機器）

## （２）人材に求める能力（続き）

○全ての事業部にセキュリティへの造詣が深い人がいるわけではない。ただし、出荷前にセキュリティ診断を実施しているので、各事業部でもセキュリティについての意識はある。事業判断ができる人にセキュリティ知識があるというより、担当者が事業リスクを含めて説明している。起こり得る事象や、発生する問題(発生確率や影響度)を説明することが重要であり、事業判断する人にセキュリティ知識は必ずしもいらない。（電気機器）

○事業部門の人にセキュリティの勉強は難しいと感じている。事業部門の人にとって、製品開発の中でのセキュリティ診断の作業は、長い製品開発作業の中の一部分でしかなく、一年に1回とか触れることがないので、それでは意識づけるのも難しい。逆にセキュリティからすると、会社として事業部門が大きいので、広く製品知識を得ることは難しい。セキュリティ部門の人が、製品の知識よりも製品部門の人のことを理解して話ができることが重要と考える。サプライチェーン全体でのセキュリティ確保についても課題であると考えている。（電気機器）

○セキュリティは理解しづらい分野のため、ICTに詳しい、あるいは過去にセキュリティ業務に携わっていた人が、親和性が高いと考える。（電気機器）

○セキュア設計開発プロセス（脅威分析等）や脆弱性検査スキル、クラウド設定検査スキル、リスクマネジメント、セキュリティ関連法令知識（特に個人データ保護法関連）についての知識やスキル、経験、そのほか情報処理安全確保支援士、CISSP、CSSLP、CCSP、CISA、CISM、CRISCなどといった資格が求められると考える。脅威分析は攻撃者の身になって考えるところなので難しい。（デジタルサービス）

○組織設立当初では外部へ依頼をすることが多く、コミュニケーションのスキルも重要となる。（デジタルサービス）

## （２’）人材確保

○行政部は、各組織との調整が多いため、各組織に顔のきく経験者が担当する形が多い。逆に、総合的なとりまとめは外部人材が担当する形が多い。（電気機器）

○工場におけるPSIRT担当者は品質保証部門と併任である。セキュリティのエキスパートを雇用する動きは現状ない。脆弱性情報の分析は社内研究所に支援を受けている。外部コンサルに開発支援を頼むこともある。（自動車部品）

○インシデントを機にDX人材とセキュリティ人材を社内に揃えるべく、外部人材の募集を始めた。セキュリティ人材は取り合いであり、雇った後退職させないためにも、体制を整備し専門人材のキャリアパスを作ることが重要である。（小売）

○セキュリティ人材内製化の舵は切ったが、細かい部分まで規定できていなかった。従来、EC業界のITは内製化よりもアウトソースで賄う文化だったが、インシデントを機にDX人材とセキュリティ人材を社内に揃えるべく、募集を始めた。人材募集は今も継続している。（小売）

○セキュリティ人材は取り合いの状況と思われ、雇った後退職させないための取組も重要と考える。専門人材がセキュリティ業界の中でも細分化されてきている中、ベンダーやコンサル業界の人材は、そこで期待されている決まった仕事・役割だけをやるのではなく、いろいろできるユーザ企業で活躍したいと思う人は、実は多いと思われる。インシデントが発生した企業であれば経営層もセキュリティの重要性を理解するため、インシデントをきっかけに体制を整備し、専門人材のキャリアパスを作れたのは大きい。（小売）

○製品のセキュリティ確保のためには、品質保証部門と情報セキュリティ部門が連携した、セキュリティ技術面の対応ができる体制の構築が必要だが、技術がわかる人材、実働できる人材の確保、育成が課題となっている。（電気機器）

○チームに共通して、セキュリティに関する興味と切迫感を重視している。（デジタルサービス）

## （2’’）人材育成

○法令・規格の内容、なぜセキュリティ教育が必要であるかといった基礎的な内容をベースとした社内教育を実施。必要な層には脅威分析、脆弱性分析、セキュリティテスト等、レベルに応じた教育も実施。基礎的な内容は内製のものを使用し、技術的な講座、監査や評価に関する講座は外部コンサルのものを受講しているが、世の中でも充実していない。（自動車部品）

○人材育成施策として、社内独自の情報セキュリティスペシャリストを育成する体制を開始。4段階の認定レベルを設定し、それぞれITSSのレベル7、6、5、4に相当。ランクが上から2段階目以上だとアーキテクトの権限等を持つことができるなど、社内でその地位を認めてもらえる仕組みとなっている。（電気機器）

○PSIRTとは別に全社組織がセキュリティ人材育成を担っており、内製でプログラムを持っている。（電気機器）

○情確士等の有資格者数は把握できていないが、セキュリティ以外の仕事をしている社員もおり、こうした人材の活用も重要。（デジタルサービス）

○脆弱性への知識や検証スキルについては日々アップデートしていく必要があり、尖ったスキルを持っていなくても、外部セミナー受講等でキャッチアップする姿勢が重要。（デジタルサービス）

○SSIRT登用後のキャリアパスにおいて、セキュリティにはこだわらない。サービスを俯瞰的に見ることができ、どこへ行っても役立つ人材になるよう育成することを考えている。（通信）

○製品セキュリティは、コーポレートPSIRT主導で年1回の訓練を実施している（コーポレートPSIRTから指示のあった脆弱性について調べて報告する形式）。CSIRTとの連携はない。CSIRT主導の迷惑メールの訓練は半期に1回実施。インシデント対応のシナリオはない。（自動車部品）

○脆弱性管理、パッチ適用の大事さをいかに自分事と捉えられるか、PSIRT機能構築においては当事者意識の啓発が重要と考える。（電気機器）

○クラウドサービス運用担当者向けの教育・サイバー演習として、商品開発のセキュリティに関するレクチャや、クラウドサービス運用担当者を対象にしたサイバー机上演習を実施している。（デジタルサービス）

○DSIRTへの兼務としてアサインされる方々は、一部を除きセキュリティの素養はほぼない。メーカー系企業は物を作って売るので、セキュリティはサブという位置づけとなり、社内で成果を認めてもらうのが難しく、結果として、セキュリティ人材を育てるのが難しいという課題がある。（デジタルサービス）

○教育は一部内製で行っており、前職等の経験から他の製品サービスで得た知識や自社製品サービスについての情報交換を行っている。（デジタルサービス）

○社内教育として新入社員向けにセキュリティ説明会を実施。定期的な教育はZoomで開催し、勉強会後にオンライントレーニングを提供している。標的型攻撃メール訓練も実施している。（デジタルサービス）

## （３）経営層へのインプット

○経営層を動かすに当たっては実例を伝えることがよいと思うが、インシデントについて具体的に伝えることが難しい。現場の人間が訴えるよりも、同業他社や有識者から経営層に伝搬されることが重要と考える。（電気機器）

○取締役への教育も継続的に行っている。経産省のサイバーセキュリティ経営ガイドラインなどを使用して経営会議で年に4回インプットを実施。社内の専門人材から、SOCやCSIRTの運用状況やサイバー攻撃のトレンド等、外部コンサルから、セキュリティ業界の動向や経営層として資源配分や投資にかかわる必要な判断を行うために知るべき事項をインプットしている。（小売）

○どういう施策を打たなければいけないかをセキュリティ統括部門、技術部門で検討し、経営層が意思決定できる状態までの落とし込みをしている。（小売）

○PSIRT機能構築にあたり、一番の課題は経営者がやる気になるかどうか、である。いかに経営者に危機感をもたせるかが重要であり、一人でもセキュリティ担当を部署内に配置して現場を見てもらい、インシデント報告等を上げるなど、小さいスケールから地道に始めることも大切ではないかと考える。（電気機器）

○クリティカルな脆弱性等は経営層へ報告している。社内セキュリティを統括する上組織へエスカレーションして、CISOに届くようにしている。（電気機器）

○中小企業としては、セキュリティはブランディングのため、という考えのほうが投資しやすい。セキュリティインシデントが起こらない、被害を防ぐ、だけでなく、セキュリティを「投資」として考えてもらう必要がある。（デジタルサービス）

## （４）情報開示

○会社として、有価証券報告書等での情報開示も非常に積極的である。（小売）

○PSIRTが普及するにあたっては、PSIRTの活動がどのようなものか伝わることも重要と思う。PSIRTのコミュニティ間で日ごろ情報共有もしており、そのような場があると良いのではないか。CODE BLUEなどでもPSIRT活動の情報共有しており、実際にPSIRTの活動をしている人たちが、具体的に何をしているのかを伝えることが重要ではないか。（電気機器）

○PSIRTは、必ずしも各事業部から温かい目で見てもらえているわけではないので、このようにPSIRTの活動を広めてくれることはありがたい。他社にもPSIRTがあることで対話がしやすくなる面があるため、PSIRTが広まることが望ましい。（電気機器）