2020 年度成果報告書

戦略的イノベーション創造プログラム（ＳＩＰ）第２期／ＩｏＴ社会に対応したサイバー・フィジカル・セキュリティ/ＩｏＴ社会に対応したサイバー・フィジカル・セキュリティに係るＯＳＳの技術検証、ＣＳＩＲＴ・ＰＳＩＲＴ連携等に関する調査

2021 年 3 月

国立研究開発法人新エネルギー・産業技術総合開発機構

委託先　　日本シノプシス合同会社

目次

参照文献

CISCO. (2020 年 7 月). Cisco Security Advisories. 参照先: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ro-path-KJuQhB86

FIRST. (2019 年 11 月). PSIRT Services Framework Version 1.0 日本語版. 参照先: https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.0_jp.pdf

imec. (2020 年 11 月). Belgian security researchers from KU Leuven and imec demonstrate serious flaws in Tesla Model X keyless entry system. 参照先: https://www.imec-int.com/en/press/belgian-security-researchers-ku-leuven-and-imec-demonstrate-serious-flaws-tesla-model-x

The Linux　foundation. (2011 年 8 月). Software Package Data Exchange® 標準フォーマット:1.0 公開版 更新内容と解説. 参照先: http://www.static.linuxfound.org/sites/mainjp/files/JP_spdx_1_0.pdf

Threatpost. (2020 年 8 月). Black Hat 2020: Mercedes-Benz E-Series Rife with 19 Bugs. 参照先: https://threatpost.com/black-hat-19-flaws-connected-mercedes-benz-vehicles/158144/

Threatpost. (2020 年 9 月). CEOs Could Be Held Personally Liable for Cyberattacks that Kill. 参照先: https://threatpost.com/ceos-personally-liable-cyberattacks-kill/158990/

Trustwave. (2020 年 11 月). Attacking SCADA Part II: Vulnerabilities in Schneider Electric EcoStruxure Machine Expert and M221 PLC. 参照先: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/attacking-scada-part-ii-vulnerabilities-in-schneider-electric-ecostruxure-machine-expert-and-m221-plc/

ZDnet. (2020 年 10 月). Over 100 irrigation systems left exposed online without a password. 参照先: https://www.zdnet.com/article/over-100-irrigation-systems-left-exposed-online-without-a-password/

Zurich）スイス連邦工科大チューリッヒ校（ETH. (2020 年 8 月). The EMV Standard: Break, Fix, Verify. 参照先: https://emvrace.github.io/

トヨタ自動車株式会社. (2019 年 12 月). OpenChain Project における OSS の Transparency 向上への取組. 参照先: https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_04_00.pdf

一般社団法人 JPCERT コーディネーションセンター. (2018 年 12 月). 2017 年度 CSIRT 構築および運用における実態調査. 参照先: https://www.jpcert.or.jp/research/20181218_CSIRT-survey2017.pdf

株式会社エヌ・ティ・ティ・データ経営研究所. (2019 年 3 月). 平成 30 年度サイバーセキュリティ経済基盤構築事業調査報告書（ソフトウェアの利活用に関わるセキュリティ確保に向けた課題に関する調査）. 参照先: https://www.meti.go.jp/meti_lib/report/H30FY/000454.pdf

鎌田 敬介 (著), 今泉 宣親 (その他). (2017). サイバーセキュリティマネジメント入門.

経済産業省商務情報政策局サイバーセキュリティ課. (2019 年 9 月). サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性. 参照先: https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/001_04_00.pdf

経済産業省商務情報政策局サイバーセキュリティ課. (2019 年 3 月). 第 4 回 産業サイバーセキュリティ研究会 ワーキンググループ 2（経営・人材・国際） 事務局説明資料. 参照先: https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/004_03_00.pdf

情報処理推進機構（ＩＰＡ）. (2020 年 10 月). ITSS+「セキュリティ領域」改訂版. 参照先: https://www.ipa.go.jp/files/000058688.xlsx

情報処理推進機構（ＩＰＡ）. (2020 年 9 月). サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き. 参照先: https://www.meti.go.jp/press/2020/09/20200930004/20200930004-1.pdf

情報処理推進機構（ＩＰＡ）. (2020 年 3 月). 制御システム関連のサイバーインシデント事例４. 参照先: https://www.ipa.go.jp/files/000080701.pdf

日本コンピュータセキュリティインシデント対応チーム協議会. (2016). CSIRT:構築から運用まで .

日本コンピュータセキュリティインシデント対応チーム協議会. (2017 年 3 月). CSIRT 人材の定義と確保(Ver.1.5). 参照先: https://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf

日立製作所. (2016 年 10 月). HIRT パンフレット. 参照先: https://www.hitachi.co.jp/hirt/publications/brochure/hirt_brochure2016.pdf

1. 研究開発の成果と達成状況

1.1. 要約

(1) 和文要約

サプライチェーンのセキュリティ確保の取り組みについて、文献調査を行った結果、プロセスと検証活動によるセキュリティ確保の取り組みが行われていることが分かりました。検証活動としては、脅威分析、静的解析、コード・レビュー、ファジング・テスト、ならびにペネトレーション・テストがあげられています。
これらの実施状況についてヒアリング調査を行ったところ、医療や産業、自動車等の社会の影響度が高い業界、ライフクリティカルな業界では、ソフトウェア・セキュリティまたは製品セキュリティに関する規制が存在し、広範囲に検証活動が実施されていることがわかりました。また、検証活動で品質やセキュリティの問題を発見した場合、自社で修正するよりも、動作を分析してソースコードの修正箇所、修正方法などを OSS コミュニティにフィードバックして改善に貢献する方法を取る傾向が高いということもわかりました。一方、その他の IoT 業界については、現時点では包括的な規制は存在せず、カリフォルニア州 IoT セキュリティ法等のローカルな規制が取り決められている段階であり、検証活動を OSS コミュニティに依存する傾向が見て取れました。
サイバー・フィジカル・セキュリティを考えるうえで重要となると想定される、自社の情報システムにおけるセキュリティ・インシデントへの対応を主導する CSIRT と、開発・製造している製品等の脆弱性に起因するインシデントへの対応を主導する PSIRT との連携方法について、文献を調査し有識者にヒアリングした結果、脅威脆弱性情報の収集配信、インシデント対応、および平常時における連携強化の 3 点において次の取り組みが重要だという結論に至りました。
1. 脅威脆弱性情報の収集配信においては、CSIRT と PSIRT で連携して実施することが効果的であり、情報のハンドリング人材を配置すること、および構成管理を一元化し取得した脆弱性情報の組織全体への影響を確認できるようにすることが望ましい。
2. インシデント対応における連携は、共通して使用するクラウド等の外部サービスでインシデントが発生した場合、あるいは情報システムへの攻撃からラテラルムーブメントにより製品の開発環境に影響が広がる場合においては実施が求められる。
3. 平常時における連携強化は、合同のサイバー演習により機能や連携の改善を図り、チームメンバー同士がお互いのスキルを把握しスキルや技術を補完し合える関係性を構築することが望ましい。
これらは OSS に特化した話ではありませんが、OSS に関わるインシデント対応や脆弱性情報の連携においても重要です。また、CSIRT・PSIRT の主体性については、連携

する機能においてより習熟したチームが主導することが効果的であり、連携する機能ごとに適切な主導者を定めることが重要となります。
脅威脆弱性情報の収集配信およびインシデント対応における CSIRT・PSIRT 連携での情報のやりとりにおいては、必ずしも固定のフォーマットを必要とするわけではないですが、少なくとも次の情報が含まれている必要があります。
・脅威脆弱性情報の収集配信の際には、判明した脆弱性の情報（CVSS、リスク、背景等)、関連する SBOM 等構成管理情報および設定情報、各 SIRT の関心度合を示す情報
・インシデント対応の際には、インシデントの情報ならびに関連する SBOM 等構成管理情報および設定情報
ただし、実際のインシデント対応においては、対応状況を管理するツール等を用いてリアルタイムに情報を共有することが重要です。
技術検証を担う人材の育成案については、上記の結果を踏まえた上で、「サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き」に基づいて分類し、整理しました。ここで求められる人材には、脅威分析や静的解析といった技術検証のスキルだけでなく、インシデント対応で重要となる回避策の検討や全体的にバランスよくセキュリティを考える能力、組織内外との連携に必要なコミュニケーション能力、海外の OSS コミュニティとのやり取りに必要な英語力等についても必要となります。

(2) 英文要約

A literature search on supply chain security efforts revealed that security efforts are based on processes and verification/validation activities. The validation/validation activities include threat analysis, static analysis, code review, fuzzing testing, and penetration testing.
An interview from experts about these activities revealed that regulations related to software security or product security are defined and verification/validation activities are conducted extensively in high social impact and life-critical industries such as Medical, Industrial, and Automotive.
It also revealed that when these industries found quality or security issues during verification /validation activities, rather than fixing those by themselves, they tend to contribute to improvement by providing feedback to the OSS community. On the other hand, for IoT industries, there is no comprehensive regulation at this time, and local regulations such as the California Internet of Things Security Law are still under discussion, therefore IoT industries tend to rely on the OSS community for verification /validation activities.

CSIRT is responsible for security incidents in the company's computer systems, and PSIRT is the responsible for security incidents in the company’s product and manufacturing. A literature search and interview from experts about collaboration activities between CSIRT and PSIRT revealed that the following three approaches are important: collection and distribution of threat vulnerability information, incident response, and strengthening collaboration activities in no incident status.

1. In the collection and distribution of threat vulnerability information, it is effective to collaborate with CSIRT and PSIRT and it is desirable to assign personnel to handle the information and to centralize configuration management so that the impact of acquired vulnerability information on the entire organization can be confirmed.
2. Collaboration in incident response is required when an incident occurs in an external service such as a shared “cloud” services, or when an attack on an computer system effects to the product development environment by Lateral Movement.
3. To strengthen collaboration in no incident status, it is desirable to improve functional through joint cyber security exercises, and to build a relationship in which team members can understand each other's skills and complement each other's skills and techniques.
These are not specific to OSS, but they are also important in incident response and vulnerability information collaboration related to OSS. In addition, as for the initiative of CSIRT and PSIRT, it is effective to be initiative by more proficient leader in the collaborated functions, and it is important to determine an appropriate leader for each collaborated

function.
The exchange of information between CSIRTs and PSIRTs in the collection and distribution of threat vulnerability information and incident response does not necessarily require a fixed format, but it is desirable at least include the following information

・In collecting and distributing threat vulnerability information, identified vulnerabilities (CVSS, risks, background, etc.), related configuration management such as SBOMs and configuration information, and the level of interest of each SIRT
・In an incident response, the incident information and related configuration management (SBOM) and oconfiguration information
However, at the moment of an actual incident, it is important to share information and response status in real time by using intelligent tools
The proposed development of human resources responsible for technical verification/validation was categorized based on the "Cybersecurity Management Guidelines Ver2.0 Appendix F: Guidance for Establishing a Cyber Security System and Human Resources" based on the above results. The human resources required here include not only technical verification/validation skills such as threat analysis and static analysis, but also the ability to consider workarounds and well-balanced security, which are important for incident response, communication skills necessary for cooperation with inside and outside the organization, and English skills necessary for communication with overseas OSS communities.

1.2. 本文

1.2.1　調査の目的

「戦略的イノベーション創造プログラム(SIP)第 2 期/IoT 社会に対応したサイバー・フィジカル・セキュリティ」においては、セキュアな Society5.0 の実現に向け、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、IoT システム・サービス及び中小企業を含む大規模サプライチェーン全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証に取り組んでいる。

近年ソフトウェアの重要性が増し、企業においても Open Source Software（以下「OSS」という。）の活用が進む中、安全な OSS の選定や、利活用するソフトウェアの脆弱性管理など、ソフトウェアの利活用に起因するサプライチェーン・セキュリティリスク対策の必要性が顕在化してきている。

本調査では、OSS のセキュリティ確保に関する技術検証項目の事例を調査すること、及び、インシデント発生時に CSIRT と PSIRT が迅速に機能するために連携すべき技術情報について、その課題・方法を分析・提言すること、その技術検証を担う人材育成案を作成することを目的とする。

1.2.2　セキュリティ確保に関する OSS の技術検証項目

1.2.2.1　サプライチェーンにおけるセキュリティ確保の取り組み

サプライチェーンのセキュリティ確保の取り組みについて、文献調査を行った結果、プロセスと検証活動によるセキュリティ確保の取り組みが行われていることが分かりました。
産業用制御システムにおけるサプライチェーンのセキュリティ標準文書である IEC62443 シリーズや自動車業界におけるサプライチェーンのセキュリティを含む ISO/SAE 21434（以下 ISO 21434 という）においては、プロセスや検証活動によって、システム全体の品質やセキュリティの向上を目指すアプローチが採用されていますが、ISO21434 や IEC62443 シリーズにおいては、OSS などのコンポーネント管理に関する、具体的な言及はありません。
欧州連合サイバーセキュリティ機関（ENISA）は、Guidelines for Securing the Internet of Things[1]（以下 ENISA IOT セキュリティ・ガイドラインという） を公開して IoT のサプライチェーンを保護するための推奨事項を定義しています。このガイドラインにおいても、検証活動に関する項目が存在します。
これらの検証活動は OSS に特化した規定ではありませんが、ソフトウェア製品の品質およびセキュリティを担保するための取り組みがそのまま OSS にも適用できます。

表 1 に、OSS 利用に適用可能な検証活動のまとめを示します。

[1] https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things(2021/3 月時点で確認済み)

表 1 OSS 利用に適用可能な検証活動のまとめ

○：検証活動の記載あり、印なし：検証活動の記載なし

検証活動	ISO21434	IEC62443-4-1	ENISA IOT ガイドライン
脅威モデリング、 脅威分析	○	○	○
静的解析	○	○	○
コード・レビュー	○	○	○
ペネトレーション・テスト	○	○	○
ファジング・テスト	○	○	

1.2.2.1.1 ISO21434

自動車業界におけるサイバーセキュリティに対応するプロセス構築・運営するために作成された規格であり、要求管理、設計、実装、検証、配布の製品ライフサイクル全般にわたり、あるべき姿を規定しています。この規格はまだドラフトの段階ですが、その内容はほぼ最終版に近いと考えられています。その中で、検証活動に関する項目は以下の通りです。

コード・レビュー

レビューは、関係者が特定の目的および基準に照らしてドキュメントまたは作業成果物をチェックする検証方法です。

OSS はソースコードが提供されているので、対象となる OSS のソースコード・レビューを行うことが可能です。特に OSS コミュニティの「健全度」が低く、継続的なメンテナンスを期待できない場合には、コード・レビューを行い、詳細なソースコードの分析を行う選択肢があります。(検証項目：コード・レビュー)

既存のコンポーネントの再利用分析

既存のアイテムまたはコンポーネントの再利用分析では、既存の脅威の分析とリスク評価を行います。たとえば、既存のアイテムまたはコンポーネントが開発されたときと比較して、新しい資産の脅威シナリオまたはリスクについて検討します。

OSS に関しては、OSS コンポーネントの既知の脆弱性を入り口とする、脅威シナリオの分析が挙げられます。(検証項目：脅威モデリング、脅威分析)

静的解析

静的解析ツールを使用して、固有の弱点、人為的エラー、既知および目に見えるシステムの欠陥、およびサイバーセキュリティ要件の仕様に関する全体的な一貫性、正確性、完全性をチェックすることができます。静的解析ツールの例としては、MISRA-C および CERT-C のルールに対してチェックする静的ソフトウェア・コード分析ツールが挙げられます。

OSS はソースコードが提供されているので、対象となる OSS に対して、それらのツールを使用することができます。静的解析ツールを使用することにより、「バッファー・オーバー・フロー」や「クロスサイト・スクリプティング」などの脆弱性を検出することが可能です。 (検証項目：静的解析)

ペネトレーション・テスト

ペネトレーション・テストは、システムに存在する脆弱性を見つけるために使用される一連のテスト方法であり、攻撃者が制御を奪ったり、特権アクセスを取得したり、特権データを公開したり、単にシステムの誤動作を引き起こしたりする可能性を検査します。
ペネトレーション・テストでは、実際の攻撃者が使用するのと同じツールと手法を使用して、実際のシステムとデータに攻撃を仕掛けます。

OSS に関しては、OSS の脆弱性を入り口としてシステムに侵入するテストが考えられます。ペンテスト・ツールや SCA ツールなどを使い OSS コンポーネントを特定し、そのコンポーネントに既知の脆弱性を入り口とした攻撃を行います。(検証項目：ペネトレーション・テスト)

ファジング・テスト

ファジング・テストは、システムへの入力として大量の予測不能なデータが（通常は自動または半自動の方法で）提供され、弱点や脆弱性（障害やコーディングエラーなど）を探すタイプのテストです。 システムがクラッシュするか、通常の定義された動作から逸脱すると、出力はエラー

として報告されます。 ファジング・テストは、システム・レベルまたはインターフェイス・レベルで実行できます。テスト対象のソフトウェアのすべての変数を一覧表示し、コード内の各ソフトウェア変数のランダム値をファジングすることで、より広範囲に実行することができます。ファジング・テストは、侵入テストの手法として使用できます。

OSS コンポーネントに対して、ファジングを行い、脆弱性を発見することができます。(検証項目：ファジング・テスト)

1.2.2.1.2 IEC 62443 シリーズ

サプライチェーンのセキュリティに対処するための、ガイドラインが標準として定義されています。

産業用制御システムのセキュリティ確保のための規定が定義されており、セキュリティ技術仕様を定義した文書群が提供されています。

IEC62443-4-1 は 制御システムを構成する個々のコントローラの開発要件を規定した国際標準（IS）です。セキュアなコンポーネントを開発するための方法を規定しており、ソフトウェア開発のライフサイクルのセキュリティに関する要求事項を記載しています。

この文書の中で、セキュリティの検証項目として以下が挙げられています。検証活動の内容は ISO21434 と同様です。

脅威分析

脆弱性データベースを参照して脅威モデリングの改良を行うことができます。例えば、TLS プロトコルをトランスポートセキュリティとして使用した場合、TLS の既知の脆弱性をチェックし、そのセキュリティ対策を行います。

コード・レビュー

セキュリティに関する問題の分析にコード・レビューを行います。

静的コード解析

セキュア・コーディング標準のチェックに静的解析ツールなどの自動化ツールを使用します。

ファジング・テスト、脆弱性テスト

脆弱性テストの一つとして、ファジング・テストを行うことが可能です。

ペネトレーション・テスト

ペネトレーション・テストを行うことによって、例えば認証機能のバイパス、管理者権限などの特権モードの奪取などを行うことができるかどうかを確認することができます。

1.2.2.1.3 ENISA IOT セキュリティ・ガイドライン

ENISA は IOT セキュリティ・ガイドラインを公開して IoT のサプライチェーンを保護するためのガイドラインを定義しています。

IoT メーカー、開発者、インテグレーター、および IoT のサプライチェーンに関与するすべての利害関係者が、IoT テクノロジーを構築、展開、または評価する際のセキュリティに関する意思決定を改善するのに役立つようにガイドラインが開発されています。

このガイドラインの中では、ソフトウェア開発におけるセキュリティ検証活動が紹介されています。

セキュア・コーディングとペネトレーション・テスト

適切なセキュリティ機能を実装および検証するために、セキュリティに焦点を当てたセキュア・コーディングとテスト（ペネトレーションテストなど）の実施を IoT サプライチェーンの適切な段階に含める必要があります。

OSS に関連する検証項目としては、OSS のソースコードに対する静的解析（バッファー・オーバー・フローなどの脆弱性の発見）やペネトレーション・テストなどの検証活動が考えられます。（検証項目：静的解析、ペネトレーション・テスト）

IOT サプライチェーン向けの脅威モデルの開発

脅威モデルを作成し、重要度に応じて脅威の相対的な重要性を評価し、サプライチェーンのセキュリティを保護するためのセキュリティ対策実装するため、リスク評価方法を確立する必要があります。

OSS コンポーネントも脅威モデリングに含むことができます。（検証項目：脅威モデリング、脅威分析）

サードパーティ・ソフトウェアを特定する

OSS を含むサードパーティ・ソフトウェアの使用は、サプライチェーンのセキュリティに対する脅威をもたらします。これらのソフトウェア・コンポーネントは、その選択のために従う基準を、サプライチェーンのセキュリティ・プロセスの一部として文書化する必要があります。組織は、評価および認証プロセスに合格したものを優先し、保守計画を定める必要があります。

OSS の維持管理者や業界の利害関係者の信頼できるコミュニティを特定できない OSS のケースでは、ソースコードの包括的な分析が推奨されます。（検証項目：コード・レビュー、静的解析）

1.2.2.2　OSS 技術検証活動の事例調査

1.2.2.2.1　OSS 技術検証活動の事例調査概要

文献調査を基に抽出した OSS に対する技術検証活動が、国内のプロジェクトにおいて、どの程度行われているのかヒアリング調査を行いました。なお、この調査は業界の傾向を見ることを目的とし、個社の状況を本報告書に記載しないこと、また、聞き取りを行った内容やユースケースに関しても、業界だけ記載し、企業名を出さないことを条件に、ヒアリングの協力をいただきました。

図 1 に調査対象プロジェクトの内訳を示します。

図 1 調査対象プロジェクト

図 2 に米国電気通信情報局（以下 NTIA という）の SBOM ワーキング・グループで検討中のサプライチェーンの役割モデルを示します。

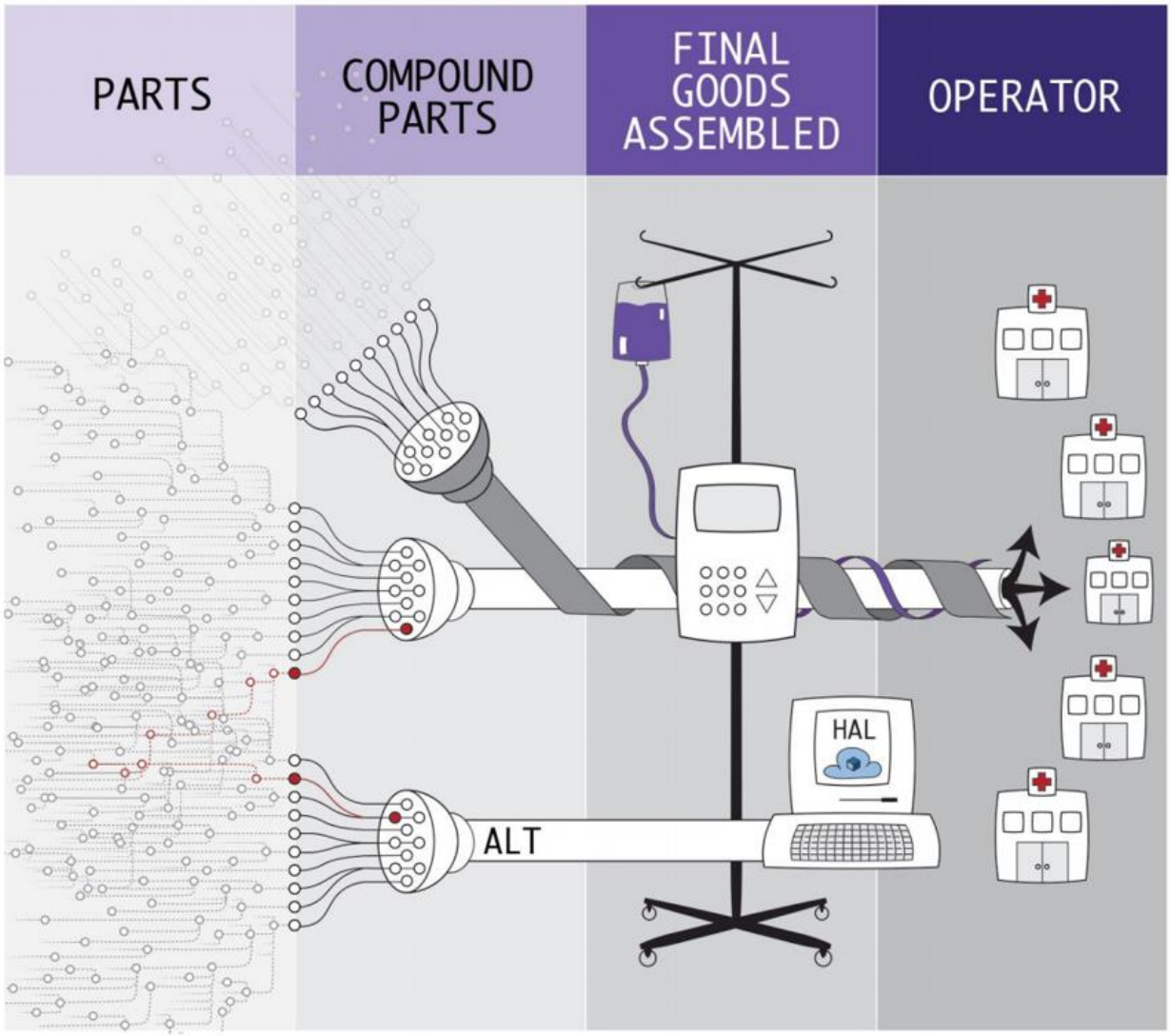

図 2　NTIA のサプライチェーンにおける役割のモデル（出典：NTIA[2]）

図 2 のモデルは、医療機器業界におけるサプライチェーンを表しています。医療機器メーカーにより、「Final Goods Assembled（最終製品）」として、複数の医療機器が「Operator（運用者）」としての病院などの組織に提供され、提供された医療機器は病院システムなどの一部として機能します。一方、最終製品は、別の組織が提供する複数の「Compound Parts(構成部品)」から構成されています。その構成部品もまた別の組織が提供する、構成部品あるいは「PARTS(部品)」から構成されています。これらの階層構造全体でサプライチェーンのエコシステムを表しています。聞き取り対象のプロジェクトは、最終製品またはその一部のソフトウェアの開発を担当するプロジェクトであり、開発されたソフトウェアを運用するプロジェクトはヒアリングの対象となりませんでした。 図 1 の「調査対象プロジェクト」における図 2 の「サプライチェーンの役割」の

[2] https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf （2021/3 月時点で確認済み）

分類を表 2 に記載します。

表 2 対象プロジェクトのサプライチェーンにおける役割

	PARTS	COMPOUND PARTS	FINAL GOODS ASSEMBLED	OPERATOR
医療			A 社（医療機器）	
IoT		E 社（IOT 機器開発）	C 社（複合機） D 社(組み込みプラットフォーム製品) F 社（IOT 関連通信機器製品）	
自動車		B 社、E 社 （自動車部品開発）		
エネルギー		B 社、E 社 （制御機器）		

品質・セキュリティ保証方法として、OSS に対しての検証活動が行われているかどうかは、各業界で異なることが予想されました。例えば、エネルギー業界では IEC62443 シリーズの EDSA 認証(Embedded Device Security Assurance)において、ファジングが検証項目として定義されており、この業界ではファジングが広く行われていることが推測されました。自動車業界で DIS となっている ISO21434 においては、脅威分析、ペネトレーション・テストなどの項目が見られます。この標準文書は、現時点でドラフトとなっていますが、最終版の内容に近いとされていますので、自動車業界のサプライヤーはこの内容に従って、プロセス構築と検証活動の準備をすすめていると推測されます。医療機器業界においては、米国食品医薬品局（FDA）で医療機器に関しての脅威分析レポートなどが義務付けられているケースがあり、これらの検証項目が行われていることが予想されました。

調査項目として、OSS に対して、以下に示すこれらの検証活動が実プロジェクトで実施されているかどうかをヒアリングしました。

OSS の既知の脆弱性を含む脅威リスク分析

OSS を含む製品やサービスにおいて、システム全体の脅威リスク分析を行う際に、OSS の既知の脆弱性を対象として取り扱っているかどうかを確認します。典型的には NVD などの公開された脆弱性の情報をもとに、システムで利用する OSS の機能の一部を使用しているかどうか、すなわち対象となる脆弱性がどのようにシステムに影響するか分析し、セキュリティの対策を決定します。

OSS に対する静的解析

使用する OSS に対して、セキュア・コーディング・ルールをチェックする静的解析ツールなどを使用して、脆弱性が存在するかどうか確認します。静的解析ツールを利用すると、ソフトウェアの品質の問題を見つけることにもつながります。組み込みソフトウェアで広く使用されている、C 言語などは、バッファー・オーバー・フローなど、影響度の高い脆弱性が入り込みやすく、メンテナンスのされなくなった、あるいはサポート力の弱い OSS コミュニティのコンポーネントを利用する場合などで、あらかじめ、静的解析ツールを実行して、品質やセキュリティに関して、調査・分析することが考えられます。

OSS のコード・レビュー

サポートされなくなった古い OSS を利用する場合、あるいは人命や影響度の高いシステムで OSS を使用する場合、使用するコンポーネントのコードをレビューすることにより、品質・セキュリティに問題がないかどうかの確認を行うことができます。

OSS に対するファジング・テスト

組み込みデバイスのプロトコルスタックや、圧縮ファイルや画像ファイルの処理に OSS が使用されているケースがあります。このようなデバイスに対して、ファジングツールなどを使用して、予測不能なデータをこれらの OSS の機能への入力として送り、動作に問題がないかどうか確認することができます。ファジング・テストはペネトレーション・テストにおけるテスト項目の一部として行われることがあります。

OSS の既知の脆弱性に対するペネトレーション・テスト

ペネトレーション・テストを実施する際、OSS の既知の脆弱性を入り口とする検証を行うことが可能です。侵入者は OSS の既知の脆弱性を起点として、実際に運用されているシステムに侵入するケースがあります。この脆弱性を利用したペネトレーション・テストを行うことにより、効率的にセキュリティに関する確認を行うことができます。

1.2.2.3　OSS 技術検証活動の事例調査分析結果まとめ

表 3 に OSS の検証活動に関するヒアリング結果のまとめを示します。

実施していることが認められる場合に、「〇：実施している」として記載しています。印がない部分は実施が認められないケースです。

表 3 品質・セキュリティの検証項目ヒアリングまとめ

〇：実施している、印なし：実施が認められない

	医療 A 社	自動車・ エネルギー B 社	IOT C 社	IOT D 社	IOT E 社	IOT F 社
OSS の脅威分析	〇	〇	〇	〇		
OSS の静的解析	〇					〇
OSS の コード・レビュー	〇					
OSS のファジング・テスト	〇	〇	〇		〇	〇
OSS のペネトレーション・テスト		〇			〇	
規制	FDA など	ISO21434 WP29 IEC62443 など			カリフォルニア州 IoT セキュリティ法など	カリフォルニア州 IoT セキュリティ法など

以下はヒアリングのまとめです。

- 社会の影響度が高い業界、ライフクリティカルな業界では、規制が存在し、広範囲に検証活動が実施されていることがわかりました。

- その他の IOT 機器の業界では、カリフォルニア州 IoT セキュリティ法など、ローカルな規制が取り決められている段階であり、各地で規制強化の動きが活発化しつつあります。しかしながら、現時点では、エネルギー業界や医療業界などで見られるような包括的な規制は存在せず、検証活動を 0SS コミュニティに依存する傾向が見て取れました。

- ヒアリングを行ったプロジェクトでは、検証活動で品質とセキュリティの問題を発見した場合、自社で修正するのではなく、動作を分析してソースコードの修正箇所、修正方法などを 0SS コミュニティにフィードバックして改善に貢献する方法がとられていることがわかりました。

1.2.3　OSS の活用に関わる CSIRT・PSIRT 連携

1.2.3.1　OSS の活用に関わる CSIRT・PSIRT 連携案

産業系システムや自動車関連でセキュリティに関するインシデントが発生すると、物理的な破壊が生じる可能性があります。懸念される脅威や脆弱性への対応として、CSIRT (Computer Security Incident Response Team) や PSIRT (Product Security Incident Response Team) が果たす役割への期待が高まっています。一般的に、CSIRT は組織が保有するシステムにおけるセキュリティ・インシデントへの対応を主導する役割を持つのに対し、PSIRT は組織が開発する製品等の脆弱性に起因するインシデントへの対応を主導する役割を持っています。

本項では、OSS の活用に関わる CSIRT・PSIRT 連携案について有識者の意見を集め、その結果を分析し、より良い連携の方法について提言をします。

1.2.3.1.1 にて OSS の活用に関わる CSIRT・PSIRT 連携案に関する提言を最初に紹介します。その提言内容を導き出すにあたって、1.2.3.1.2 にて連携方法の文献調査から仮説立案を示します。その仮説に基づき有識者インタビューから導き出した分析結果を 1.2.3.1.3 に示します。

1.2.3.1.1　CSIRT・PSIRT 連携案の提言

OSS の活用に関わる CSIRT・PSIRT 連携案に関して「脅威脆弱性情報の収集配信」と「インシデント対応」の 2 つの活動フェーズにおける提言と、平常時における連携強化に関する提言を以下に示します。脅威脆弱性情報の収集配信は、定期的な脅威脆弱性に関する情報の収集活動を想定していて、インシデント対応は、実際にインシデントが発生した際の対応活動を想定しています。これらの活動における機能・役割の違いの詳細については、「1.2.3.1.2.1　機能と連携効果の仮説立案」における検討事項として表 5 に示しています。

1.2.3.1.1.1　【提言】脅威脆弱性情報の収集配信

脅威脆弱性情報の収集は、CSIRT・PSIRT で連携して実施することが効果的です。両 SIRT 含め適材適所への情報配信を実現するため、情報のハンドリング人材を配置することが望ましいです。さらに、組織に関連する構成管理を一元的に確認できるようにし、取得した脆弱性情報の組織全体への影響を確認できることが望ましいと想定します。

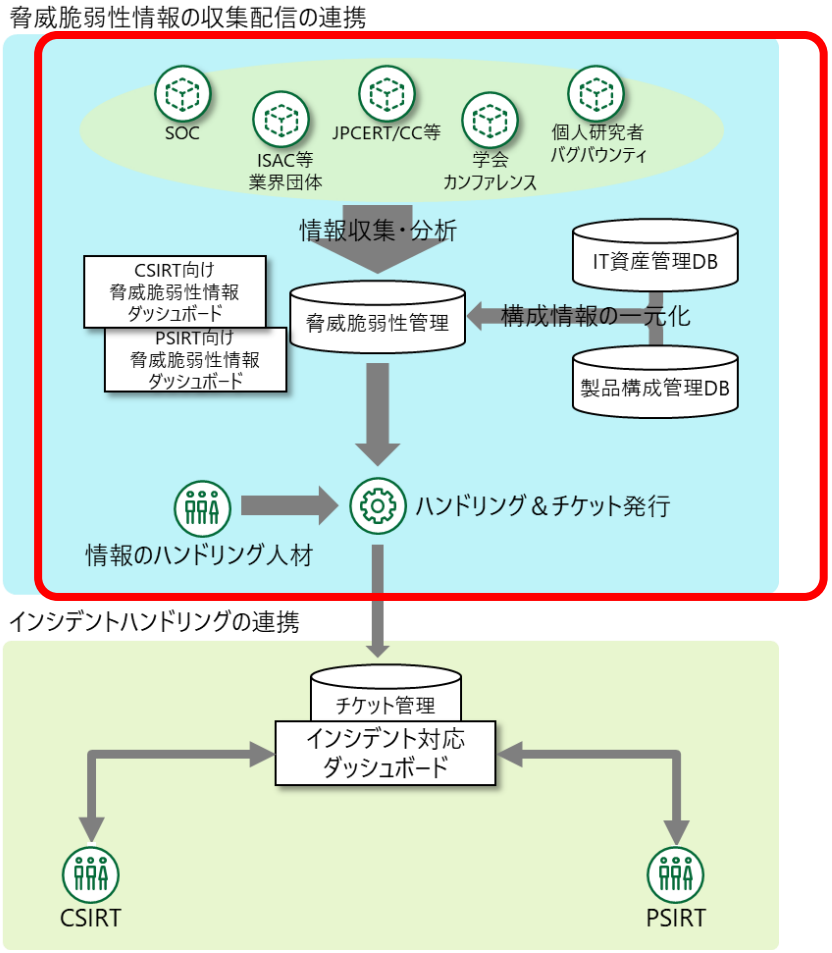

図 3　脅威脆弱性情報の収集配信の情報の流れ（イメージ）

1.2.3.1.1.2　【提言】インシデント対応

【インシデント対応おける連携案の提言】

以下のような場合のインシデントに備え、CSIRT・PSIRT で連携して対応を実施します。

- 共通して使用するクラウド等の外部サービスにインシデントが発生した場合
- 情報システムへの攻撃からラテラルムーブメントにより開発環境に影響が広がる場合

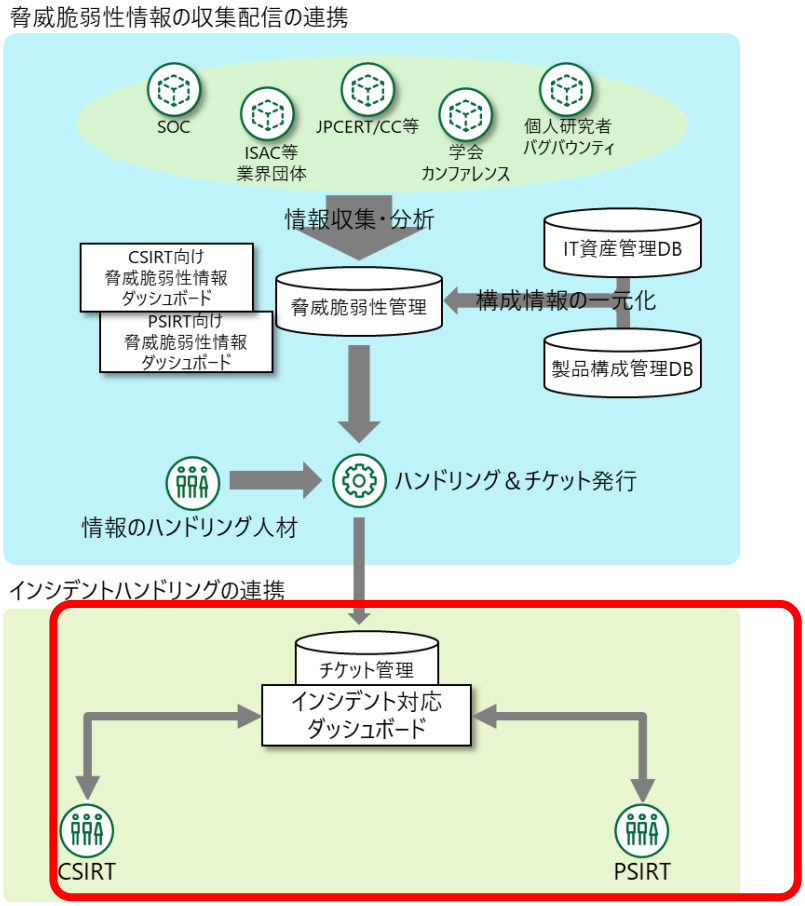

図 4　脅威脆弱性情報収集からインシデント対応連携への流れ（イメージ）

1.2.3.1.1.3　【提言】平常時の連携強化案

【サイバー演習における連携案の提言】

インシデント発生に備え、CSIRT、PSIRT を含む組織の関連部門合同で演習を実施し、各機能や連携の改善を図ります。

【チームメンバー間の意識の連携案の提言】

CSIRT・PSIRT のチームメンバーそれぞれがお互いのスキルを把握し、信頼関係がある下で、スキルや技術を相互に補完しあえる関係性を構築します。

1.2.3.1.1.4 留意事項

【連携の主導者】

CSIRT・PSIRT が連携する際、両 SIRT 以外に連携の主導者がいない場合は、連携する機能においてより習熟したチームが主導することが効果的と考えます。連携する機能によって、ケースごとに適切な主導者を定めることが重要となります。以下に連携する機能と、主導するチームの例を示します。

表 4 CSIRT・PSIRT 連携するケースと主導するチームの例

連携する機能	ケースと主導するチームの例
情報収集	• CSIRT のみが SOC（Security Operation Center）を所有している場合、CSIRT が主導して PSIRT と脅威脆弱性情報の収集の連携を実施します
インシデント対応	• CSIRT・PSIRT が共通して使用するクラウド等の外部サービスがあり、CSIRT のほうが高頻度で当該サービスを利用している場合、当該サービスにインシデントが発生した場合は CSIRT がインシデント対応を主導します • 情報システムと開発システムをまたぐインシデントが生じ、顧客に納入する製品への影響が懸念される場合、PSIRT が主導して顧客側にインシデント対応を行います
外部機関との連携	• CSIRT・PSIRT が共通して他社 SIRT 等、外部の機関との連携が必要な場合、従来からより交流を深めているチームが主導します

【法令順守】

IoT システムの開発、製造、保守、運用においては社内外の海外リソースを活用していることが多く、 CSIRT・PSIRT の活動においても様々な情報を海外と共有することが想定されます。どのような場合においても当該地域の法令順守が求められますが、国家をまたぐ情報

の共有については輸出管理の対象となる場合があるため[3]、法務部等への相談を含め適切な対応をとる必要があります。この留意事項を情報共有の現場担当者や管理者が把握していることが重要です。関係者に定期的な教育や注意喚起を実施して法令に関する認識を保ち、必要に応じて更新していくことが求められます。

1.2.3.1.2 CSIRT・PSIRT 連携方法の文献調査まとめ

机上調査のフェーズにおいては、まず文献調査を実施し、そして関連トピックに関する知見の収集および洗い出しを実施しました。

文献調査では、サイバー・フィジカル・セキュリティに係る様々なトピックの中から、特に OSS に関する CSIRT・PSIRT の軸で幅広いオープンソースベースの文献を収集し、関連組織やタスク等の軸で整理しました。参照例としては、サイバーセキュリティ業界や団体が出す White Paper、国内外の官公庁が出すアラートやガイドライン、カンファレンスの資料、ニュース等が含まれます（参照文献に示す）。

関連トピックの知見については、IT／OT／IoT 分野の数多くのフィジカル・セキュリティ関連案件を洗い出し、現場の現実的な「あるべき姿」論の仮説作成のための検討材料とします。

1.2.3.1.2.1 機能と連携効果の仮説立案

本項では、仮説の検討について示します。

仮説の検討は図 5 に示すフローで実施した。ここではフローの①～③について示し、1.2.3.2 で④について示します。

[3] SOFTIC, https://www.softic.or.jp/ossqa/all_180328.pdf (2021/3 月時点で確認済み)

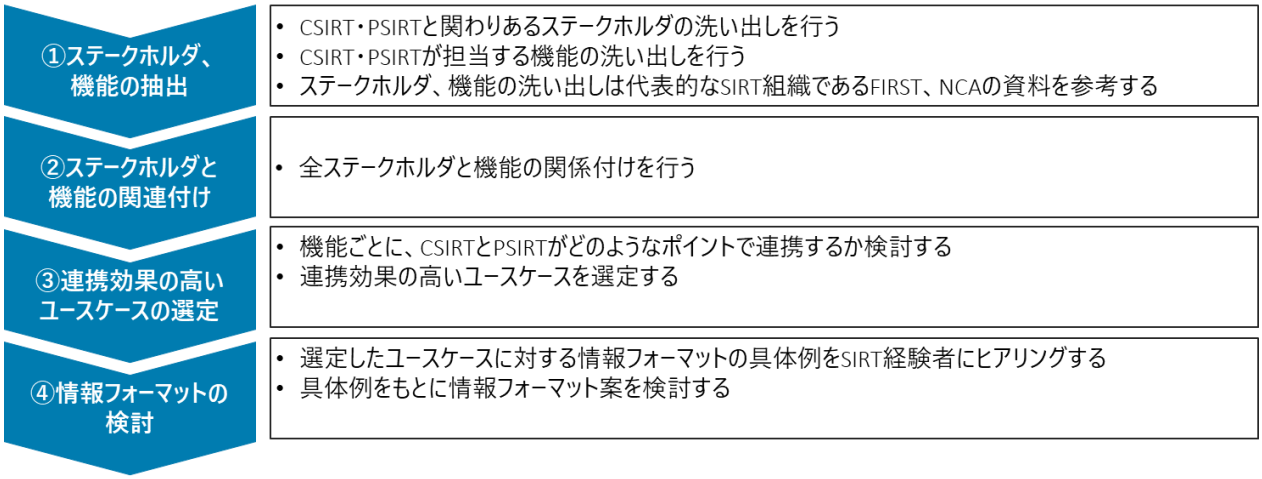

図 5　CSIRT・PSIRT の連携ユースケースおよび情報フォーマットを検討するためのフロー

① ステークホルダ、機能の抽出

日本コンピュータ・セキュリティ・インシデント対応チーム協議会（以下、「NCA」という）は、『CSIRT 人材の定義と確保(Ver.1.5)[4]』において、組織が保有すべき CSIRT の役割と機能を挙げています。その機能分類「情報共有」、「情報収集・分析」、「インシデント対応」、「組織内訓練」をベースに、FIRST（ Forum of Incident Response and Security Teams）が公開する CSIRT・PSIRT フレームワークに記載されている「運用基盤」を参照し、ステークホルダ及び機能を抽出し図 6、表 5 に整理しました。

[4] NCA, https://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf (2021/3 月時点で確認済み)

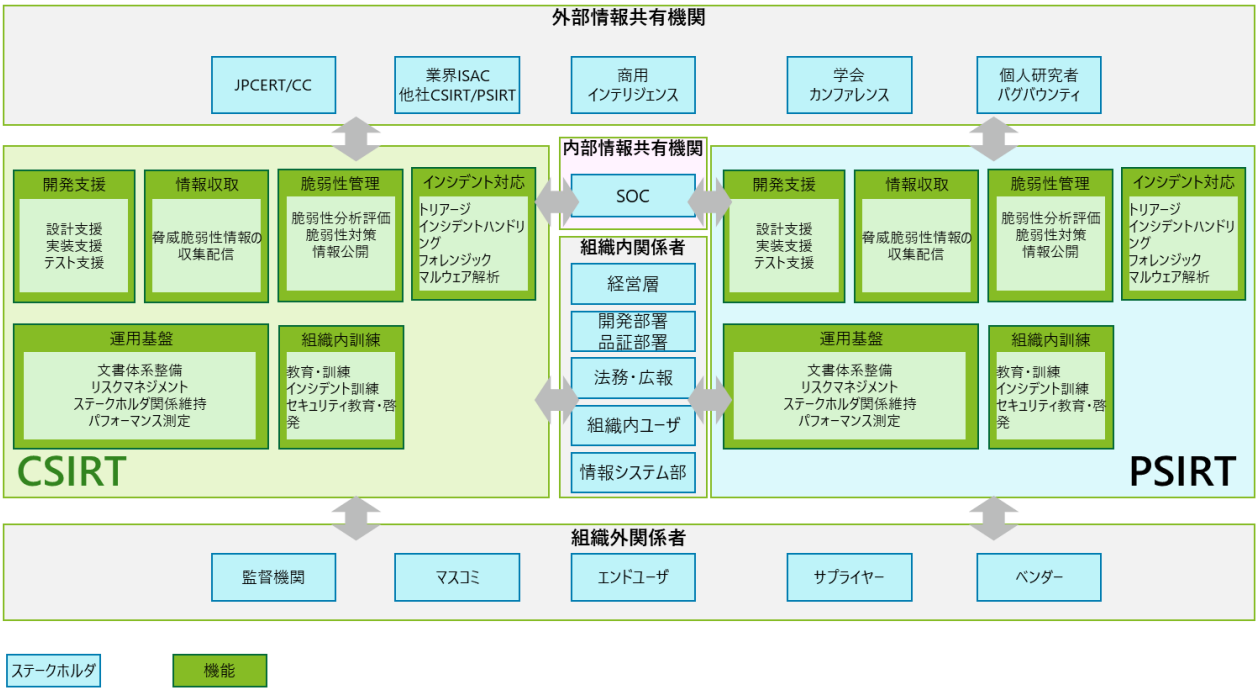

図 6　CSIRT・PSIRT のステークホルダと機能

表 5　CSIRT・PSIRT の機能と役割一覧

機能	小分類	役割
開発支援	開発支援	設計・実装フェーズにおけるセキュア設計、セキュア・コーディング等の開発支援、テストフェーズにおけるセキュリティテスト等、開発全般のセキュリティにおける支援を行います
情報収集	脅威脆弱性情報の収集配信	組織に影響しうる脅威情報や脆弱性情報を収集・整理し、内容に応じて適切な関係者に配信します
脆弱性管理	脆弱性分析	判明した脆弱性に対する自社製品や自社システムへの影響範囲や影響度を分析します
	脆弱性対策	判明した脆弱性に対する自社製品や自社システムへの暫定対策および恒久対応策を検討し必要に応じて実装します

	情報公開	ステークホルダに対する脆弱性への対応方針の告知、および修正プログラムの配布、当局への脆弱性関連情報の届け出を行います
インシデント対応	トリアージ	発生したインシデントに対する組織への影響度を判断し、復旧の優先順位を決定します
	インシデントハンドリング	発生したインシデントの対応状況を把握し、オンサイト・オフサイトによる対応支援や関係者間の調整等を行い、収束までの一連の処理を遂行します
	フォレンジック・マルウェア解析	被害を受けた機器を証拠保全し、攻撃原因、被害範囲などの詳細な調査を行います
組織内訓練	インシデント訓練	SIRT チームのインシデント対応能力の向上を図るため、インシデント対応の訓練・演習を行います
	セキュリティ教育・啓発	エンドユーザのセキュリティに対するリテラシー向上を図るため、集合型研修、e-ラーニング、メール配信等を通じて教育や啓発活動を行います
運用基盤	文書体系整備	チームの組織運営に必要な文書規定の作成およびメンテナンスを行います
	リスクマネジメント	自社ビジネスへの脅威と影響を理解するため、自社システムおよび自社製品に対するリスクを評価します
	ステークホルダ関係維持	経営層へのチームの活動状況の報告や、同業他社 SIRT チームとの交流など、ステークホルダとの関係を維持するためのコミュニケーション活動を行います
	パフォーマンス測定	経営層と合意した目標に対する進捗状況を報告するため、インシデント対応件数等の活動状況を集計し、定量化します

「運用基盤」の機能については FIRST（PSIRT）の資料のみの記載で、NCA（CSIRT）の資料には記載されていませんでした。そのため、その他の機能に含まれると想定して、以降の比較対象から除外しました。

② ステークホルダと機能の関連付け

抽出された CSIRT 及び PSIRT の機能とステークホルダについて、関連を示すユースケースを整理した結果を図 7 に示します。

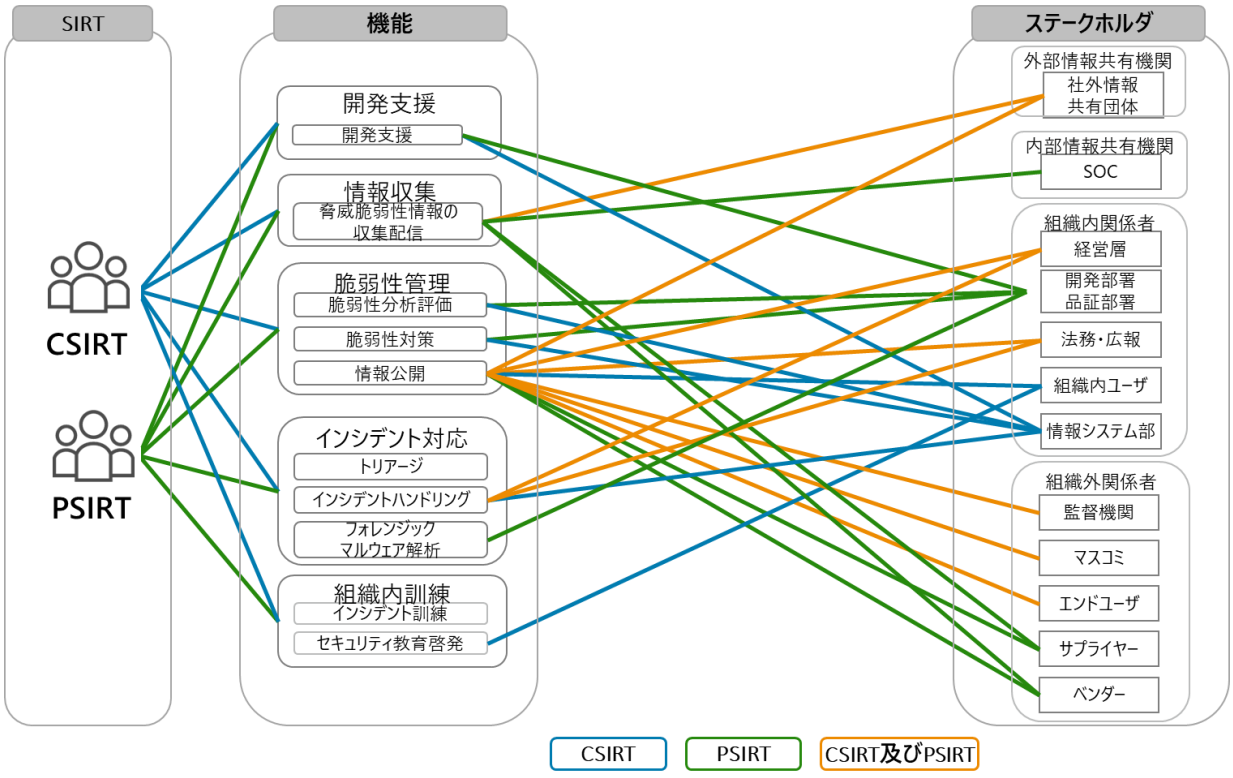

図 7　CSIRT・PSIRT ユースケース図

③ 関連効果の高いユースケース選定

図 7　CSIRT・PSIRT ユースケース図から、機能ごとに CSIRT と PSIRT の連携効果を検討した結果を表 6 に示します。

表 6　CSIRT・PSIRT の連携効果

	機能	SIRT のステークホルダ		連携が見込めるポイント	連携効果	連携効果の判断理由
		CSIRT	PSIRT			
開発支援						
(1)	開発支援	情報システム部門	開発部署	開発技法の共有	低	開発支援先となる情報システム部門と開発部署ではプロダクトの違いより開発技法も異なるため連携効果は低いです
情報収集						
(2)	脅威脆弱性情報の収集配信	外部情報共有機関 内部情報共有機関	外部情報共有機関 内部情報共有機関	脅威脆弱性情報の共有	高	互いの SIRT が持つ複数の情報ソースから提供される情報を合わせて配信することができるため連携効果は高いです
脆弱性管理						
(3)	脆弱性分析	情報システム部門	開発部署	攻撃再現方法およびツール環境の共有	高	情報システム部門と開発側では同じ OSS を利用している場合があり、調査に必要なツールや再現手順を共有することで、効率的な調査が期待できます
(4)	脆弱性対策	情報システム部門	開発部署	暫定対策および恒久対策の共有	高	情報システム部門と開発側では同じ OSS を利用している場合があり、対策策を共有することで、効率的な対応が期待できます
(5)	情報公開	組織内関係者 組織外関係者 外部情報共有機関	組織内関係者 組織外関係者 外部情報共有機関	脆弱性情報、インシデント情報の共有	低	CSIRT の場合、自社システムの情報漏洩事案、PSIRT の場合、製品不具合情報等、情報公開の目的が異なるため、インシデントの経緯や取り扱う脆弱性情報が異なることから連携効果は低いです
インシデント対応						
(6)	トリアージ	なし	なし	イベント情報の共有	低	トリアージ判断基準は情報システム、製品ごとに異なるため、連携の必要性は低いです
(7)	インシデント	組織内関係者	組織内関係者	脆弱性情報、	高	OSS を利用している場合、サイバー、

	機能	SIRT のステークホルダ		連携が見込めるポイント	連携効果	連携効果の判断理由
		CSIRT	PSIRT			
	ハンドリング			インシデント情報の共有		フィジカルの連携が必要となるインシデントケースが存在し、インシデント対応状況を共有することで、組織対応の統一を図ることができるため
(8)	フォレンジック・マルウェア解析	なし	開発部署	解析結果の共有	低	製品の場合、開発部署に解析を依頼するケースがあるが、製品と情報システムでは解析対象、解析結果は異なるため両チームの連携効果は低いです
組織内訓練						
(9)	インシデント訓練	なし	なし	訓練・演習の共同実施	低	インシデント訓練は SIRT 内部向けのユースケースです。 フローは両チームとも異なり、訓練・演習プログラムも異なることから連携効果は低いです
(10)	セキュリティ教育・啓発	組織内ユーザ	なし	セキュリティ教育の共同実施	低	組織内ユーザ向けのオフィス IT に関する教育であり、連携効果は低いです

1.2.3.1.2.2 CSIRT・PSIRT 連携案の仮説

1.2.3.1.2.1 の検討結果から、CSIRT・PSIRT 連携効果が高いユースケースを図 8 に示します。

A) 情報収集： 脅威脆弱性情報の収集配信

B) 脆弱性管理：脆弱性分析

C) 脆弱性管理：脆弱性対策

D) インシデント対応：インシデントハンドリング

図 8　連携効果の高いユースケース（仮説）

1.2.3.1.3　有識者インタビュー結果まとめ

1.2.3.1.2 で導き出した「あるべき姿」の仮説を検証するフェーズでは、その分析方法として有識者に対するインタビューを実施しました。その後、インタビュー結果を項目別に整理し分析することで 1.2.3.1.1 の提言としてまとめました。

1.2.3.1.3.1　インタビュー内容

インタビューでは、作成した仮説をベースにインタビューシートを作成し、その仮説の有効性や現実可能性などを以下に示す 5 名の有識者から意見を求めました。インタビューシートとインタビューの実施においては、分析・整理のフェーズで体系立てて整理できるよう、可能な限り同一シートによる同一質問アプローチを採用しました。

インタビューにご協力いただいた有識者の方々（順不同、タイトルのみ記載）
所属
パナソニック株式会社 製品セキュリティセンター 製品セキュリティグローバル戦略部 部長 兼 Head of Panasonic PSIRT
株式会社サイバーディフェンス研究所　専務理事
株式会社 Armoris 取締役専務 CTO 内閣サイバーセキュリティセンター　普及啓発・人材育成専門調査会　委員
株式会社 JVC ケンウッド 技術開発部 製品セキュリティ推進グループ・グループ長／PSIRT リーダー
金融関連製造会社　製品セキュリティ部門　マネージャ

1.2.3.1.3.2 インタビュー結果の整理

結果の整理では、インタビューシートの回答をベースに項目ごとに回答を類型化し、その結果を「あるべき姿」論の仮説と突合させることで、同分野における施策方向性の fits & gap を顕在化させ、仮説を検証しました。

1.2.3.1.2.2 から導出した CSIRT・PSIRT が連携可能な仮説について、有識者へのインタビューを実施しました。インタビューから得られた意見を表 7 に示します。

表 7　ユースケースごとの連携効果に関して有識者インタビューで得られた意見

A)	情報収集	脅威脆弱性情報の収集配信
有識者意見：○　連携の効果あり		
【連携している点、連携効果がある点】 • 各 SIRT が収集している脅威脆弱性情報を共有しています		

- サイバー攻撃事例、他社への攻撃事例、脆弱性情報、セキュリティカンファレンスで出ているような情報といった、パブリックモニタリングや OSINT（open-source intelligence）で得られる情報をみて、自分たちに何が必要か考えます

- 各 SIRT で情報収集の仕組みは共通化できると考えます
- OSS という前提であれば、各 SIRT にて脆弱性情報を収集するより、連携した方が効率的と考えます
- CSIRT からは組織内のインシデント情報など、PSIRT からは組織内規定に関連する情報を共有しています
- CSIRT が SOC 機能を持ち、そこで収集した情報を PSIRT に共有する例があります
- OSS 関連含め脆弱性情報は品質保証部門が各 SIRT へ共有しています
- 連携の枠組みはないものの、SIRT 間で個人のつながりによる情報共有を実施しています

【連携効果が期待できない点】

- 組織が縦割りであるために情報連携が期待できません
- 両 SIRT の予算や報告先が個別であり、外部への情報収集委託も個別に契約しています

【連携に向けたその他事項】

- 収集した情報のトリアージや関係者に連携できる人材の必要性
  - JPCERT/CC にて脆弱性ハンドリング業務を実施していた際には、情報収集を行う担当者がいて、毎日数百件程の情報を収集し、国内影響度等のパラメータを設定して DB に登録していました。そのうち個別の評価が必要な数十件程に絞り込み、関係者で議論しながら個々に評価を実施した。この二次フィルタリングは職人技であり、その分野に詳しい人が判断に入らないとできません
  - 組織内では、例えばあるサーバプロダクトに脆弱性があるとしても、社内でどのように利用されているかについては、運用部門に聞かないとわかりません。そこは社内での情報連携が必要で、コミュニケーションが重要な場面。機械的にやると抜け漏れが出るため、少数精鋭でトリアージするのがよくみる形です

B)	脆弱性管理	脆弱性分析

有識者意見：×　連携の効果なし

【連携している点、連携効果がある点】

- なし

【連携効果が期待できない点】

- OSS で脆弱性が報告された場合でも、CSIRT の対象となるサーバと PSIRT の対象となる製品では脆弱性の影響が異なるため、連携できる部分は少ないです
- ユーザ企業側で OSS の改修はできないため、コードレベルの深い知識を用いた PoC（Proof of Concept)再現等は不要です
- 組み込み製品が多いため、PSIRT と CSIRT のカバー範囲がほとんど重なりません
- 監視の仕組みは共通化できても、監視する対象はほとんど重複しません
- 脆弱性修正は別企業が担当しているため、コードレベルのテクニカルな分析よりも、脆弱性が発見された場合の対応や責任分解を明確に契約に含めること重要です

C)	脆弱性管理	脆弱性対策

有識者意見：×　連携の効果なし

【連携している点、連携効果がある点】

- なし

【連携効果が期待できない点】

- 製品とサーバでは脆弱性の対策方法が異なるため、連携していません
- CSIRT の対象であるサーバ、PSIRT の対象である製品に共通の OSS が使用され、そこに脆弱性が報告された場合でも、ユーザ企業側で OSS 改修は対処できないため、修正アップデートでの対応となります。回避策の検討する場合もサーバと製品により対応は異なります
- 組み込み製品が多いため、PSIRT と CSIRT のカバー範囲がほとんど重なりません

D)	インシデント対応	インシデントハンドリング

有識者意見：△　連携の効果は一部あり

【連携している点、連携効果がある点】

- CSIRT・PSIRT とも利用しているクラウドサービスに関するインシデントが発生した際は、連携して対応します
- 組織内で利用している SolarWinds のような商用製品への攻撃により、情報システムから横展開で開発システムに侵入されるケースがあります。その場合は組織内の CSIRT と PSIRT が連携して対応します。加えて当該製品の製造元の PSIRT とも連携して対応することが効果的です
- 開発中（または保守中）の製品に影響のあるインシデントが発生した場合は、PSIRT は製品納入先の PSIRT と連携して対応します

【連携効果が期待できない点】

- IoT 製品サービスに関連するサーバは PSIRT の担当範囲であるため、そこにインシデントが発生した場合も CSIRT との連携は限定的です
- 関連する部門のみに限定してインシデント情報を共有する運用となっています
- サプライチェーン上の他社の PSIRT と連携する場合、サプライチェーンの構造が多様化しており、連携を機能させることが難しくなっています

その他、仮説には含まれなかったものの有識者から得られた連携への意見

- CSIRT・PSIRT、その他関連する部門を交えて合同のサイバー演習を実施しています
  - CSIRT と PSIRT が相互に連携しており、一例として東京オリンピックに向けた演習を合同で実施しています
- メンバーの信頼関係の構築や、共通ゴールを認識して業務に取り組めるよう、組織・分野を横断したメンバーを一か所に集約してプロジェクトを遂行することで、連携が成功する例が確認されています。適切な主導者がいることも肝要となります。連携の枠組みだけ作った事例は過去に数多くあるが、それだけで成功することは難しいです
- セキュリティにおいて対応するべき状況は変化していくため、SIRT の形態を含む組織体制も状況に応じた最適化を行っていきます

1.2.3.1.3.3 有識者インタビュー結果からの分析

有識者インタビューの結果から、CSIRT・PSIRT 連携するにあたり、仮説 A～D に同意を得られた点と異論が出た点、また仮説に不足していた観点を分析し、効果的と考えられる４つの連携案を示します。

1.2.3.1.4 (A) 脅威脆弱性情報の収集配信の連携

脅威脆弱性情報の収集配信の連携は合理的であるとして、連携効果があるとの回答が多数でした。参照される情報は CSIRT・PSIRT 間での一致は少ないものの、収集プロセスについては両 SIRT で共通しており、収集した情報を両 SIRT 含む組織内の関係者が閲覧可能な状態にするまでの仕組みは共通化することが効率的という意見が得られました。

連携を実現するにあたり、必要となる要素として、「情報のハンドリング人材」、及び「構成管理の一元化」が挙げられた（「構成管理の一元化」に関する有識者インタビュー結果は 1.2.3.2.3 に記載する）。各要素の内容を以下に示します。

＜情報のハンドリング人材＞

CSIRT・PSIRT に必要となる脅威脆弱性情報を一元的に収集し、内容を評価したうえで適切な関係者に共有することができる、情報のハンドリング人材が必要になります。

情報のハンドリング人材として機能するためには、自組織の製品やシステムをよく理解していて、収集された脅威・脆弱性に関する情報がそれらに対して与える影響を評価し、適切な関係者と連携できる分析力、技術力、コミュニケーションスキルを備えた人材が求められます。

＜構成管理の一元化＞

脆弱性情報が組織に影響するか調査する際に、組織に関連する IT 資産や製品構成が一元的に確認できると、合理的な調査が実現できます。IT 資産管理 DB と製品構成管理 DB を透過的に一元化することで、収集した脆弱性をもとに自組織への影響範囲を効率的に判断可能となります。

さらに、一元的な構成管理に以下の属性を追加することにより、組織が提供する製品に影響が出るようなインシデントが発生した際に、組織を横断した CSIRT・PSIRT 間の情報共有が効率化されます。

構成管理へ追加する属性：

- 保守ベンダの、発注元、サプライヤー等のサプライチェーンに関する情報
- 納品先の詳細仕様に関する情報（製品のベース仕様から顧客ごとにカスタマイズした情報）

以上の分析結果より CSIRT・PSIRT の効果的な連携案として「1.2.3.1.1.1【提言】脅威脆弱性情報の収集配信」を示しました。

1.2.3.1.5 (B) 脆弱性分析の連携

仮説にて脆弱性を再現する PoC を CSIRT・PSIRT 間で共有することを想定していましたが、以下にまとめる意見により、連携例や連携を推奨する意見がなく提言を行いませんでした。

- 脆弱性が報告された場合でも、CSIRT の対象と PSIRT の対象で影響が異なります
- ユーザ企業側で OSS の改修はできないため、コードレベルの深い分析は不要です
- テクニカルな分析よりも、対応や責任範囲を明確に契約に含めることが重要です

1.2.3.1.6 （C) 脆弱性対策の連携

仮説にてCSIRT・PSIRT間で共通で使用するOSSの脆弱性の対策方法の共有を想定していたが、以下のような意見により、連携例や連携を推奨する意見がなく提言を行いませんでした。

- 製品とサーバでは脆弱性の対策方法が異なります

OSS に対してユーザ企業側は改修できないため、リスクに応じた適切な回避策を検討する方が重要だが、サーバと製品により対応は異なります。

1.2.3.1.7 （D) インシデントハンドリングの連携

仮説にてサーバ側等のサイバーの領域で発生した攻撃がIoT製品等のフィジカルの領域に波及する、またはその逆の場合のインシデント対応における連携を想定していたが、IoT関連サービスのサーバはPSIRTの責任範囲である等、CSIRT・PSIRTの役割分担の状況から、連携が少ないことがわかりました。

一方で、以下のまとめる場合ではCSIRT・PSIRTで連携してインシデント対応を実施している、あるいは実施することが効果的であるという意見が聞かれました。

- CSIRT・PSIRTで共通して利用する外部サービスでインシデントが発生した場合
- 組織内で広く利用している商用製品への攻撃により、情報システムから横展開で開発システムに侵入される場合は、組織内のCSIRTとPSIRTが連携し、加えて当該製品の製造元のPSIRTが連携して対応します

以上の分析結果よりCSIRT・PSIRTの効果的な連携案として「1.2.3.1.1.2　【提言】インシデント対応」を示しました。

1.2.3.1.8 （追加１) サイバー演習の連携

仮説になかった点で、大規模スポーツイベント等に付随して発生が想定されるサイバー攻撃への対応演習をCSIRT、PSIRTを含む組織の関連部門合同で実施しているとの意見が聞かれました。実際のインシデント発生を想定したシナリオを共同実施することで、連携がうまくいかないケースを洗い出し、連携強化にむけて改善することは効果的と考えられます。

以上の分析結果よりCSIRT・PSIRTの効果的な連携案として「1.2.3.1.1.3　【提言】平常時の連携強化案」に【サイバー演習における連携案の提言】を示しました。

1.2.3.1.9 （追加２）チームメンバー間の意識の連携

仮説になかった点で、すべての連携のベースに位置づけられる要素として、チームメンバー間の信頼関係の醸成が重要という指摘が聞かれました。連携を目指して枠組みだけ作った事例は過去に数多くありますが、それだけで成功することは難しく、メンバーの信頼関係の構築や、共通ゴールを認識して業務に取り組める体制や環境が整備されることが求められます。その実現にあたり、組織・分野を横断したメンバーを一か所に集約して、多様な背景のメンバーを率いる適切な主導者の下でプロジェクトを遂行することで、連携が成功する例が官民で確認されています。メンバー同士が有効に連携することで、より幅広いスキルや技術をカバーできることとなります。

以上の分析結果より CSIRT・PSIRT の効果的な連携案として「1.2.3.1.1.3 【提言】平常時の連携強化案」に【チームメンバー間の意識の連携案の提言】を示しました。

1.2.3.2 CSIRT・PSIRT 連携における情報フォーマット

本項では、「1.2.3.1 OSS の活用に関わる CSIRT・PSIRT 連携案」において、OSS に求められる情報のフォーマットについても調査を行い、その結果を分析してフォーマット案の提言をします。

1.2.3.2.1 にて CSIRT・PSIRT 連携における情報フォーマット案の提言を最初に紹介します。その提言内容を導き出すにあたって、1.2.3.2.2 にて CSIRT・PSIRT の連携を行う際に、必要となる情報フォーマットを検討した仮説立案を示します。その仮説に基づき有識者インタビューから導き出した分析結果を 1.2.3.2.3 に示します。

1.2.3.2.1 CSIRT・PSIRT 連携における情報フォーマット案の提言

1.2.3.2.1.1 【提言】脅威脆弱性情報の収集配信

【脅威脆弱性情報の収集配信を連携する際のフォーマットに記載する項目案】

- 判明した脆弱性の対応に向けた情報（CVSS、脆弱性によるリスク、背景情報等）
- SBOM 等に一元管理された構成管理情報（OSS 含む）・設定情報（収集した脆弱性情報と紐づけて合理的な脆弱性ハンドリングを実現）
- 収集した脅威脆弱性情報に、CSIRT・PSIRT の関心度合を示す情報

【脅威脆弱性情報の収集配信を連携する際のフォーマットを利用しない場合の共有案】

- インテリジェンスツールを使用し、収集・分析結果のうち CSIRT・PSIRT のそれぞれの関心事項をダッシュボードに表示します

1.2.3.2.1.2 【提言】インシデント対応

【インシデント対応の連携をする際のフォーマットに記載する項目案】

- SBOM 等に一元管理された構成管理情報・設定情報
  （インシデント影響範囲把握の特定のため）

【インシデント対応の連携をする際のフォーマットを利用しない場合の共有案】

- インシデント対応を管理するツール等を用いてリアルタイムに情報共有を行います

1.2.3.2.2 CSIRT・PSIRT 連携における情報フォーマットの文献調査まとめ

1.2.3.2.2.1 連携する情報フォーマットの仮説立案

「1.2.3.1.2.2 CSIRT・PSIRT 連携案の仮説」で CSIRT・PSIRT の連携が有効であると洗い出された以下のユースケースごとに具体的な事例を想定し、連携の際に共有する情報フォーマットに含める項目例を検討した結果を表 8 に示します。

A) 情報収集 – 脅威脆弱性情報の収集配信

B) 脆弱性管理 – 脆弱性分析

C) 脆弱性管理 – 脆弱性対策

D) インシデント対応 – インシデントハンドリング

表 8 CSIRT・PSIRT 連携の際に共有するフォーマットに記載する情報項目（仮説）

ユースケース	連携ポイント	情報フォーマット例
脅威脆弱性情報の収集配信	脅威脆弱性情報の共有	• 情報種別（脅威、脆弱性、インシデント事例等） • 情報提供者（JPCERT、バグハンター等） • 影響度 • 公開範囲（TLP） • 対策の有無

脆弱性分析	攻撃再現方法およびツール環境の共有	• ソフトウェア名、バージョン • 脆弱性管理番号 • 再現環境、再現手順
脆弱性対策	暫定対策および恒久対策の共有	• ソフトウェア名、バージョン • 脆弱性管理番号 • 応急、恒久対策
インシデントハンドリング	脆弱性情報、インシデント情報の共有	• インシデントの背景 • 利用された脆弱性の情報 • 対策の有無 • 被害の有無、被害範囲 • 外部団体（JPCERT、業界 ISAC 等）からの情報

1.2.3.2.3 有識者インタビュー結果まとめ

1.2.3.2.3.1 インタビュー内容

インタビューでは、作成した仮説をベースにインタビューシートを作成し、その仮説の有効性や現実可能性などを以下に示す 5 名の有識者から意見を求めました。インタビューシートとインタビューの実施においては、分析・整理のフェーズで体系立てて整理できるよう、可能な限り同一シートによる同一質問アプローチを採用しました。

所属
パナソニック株式会社 製品セキュリティセンター 製品セキュリティグローバル戦略部 部長 兼 Head of Panasonic PSIRT
株式会社サイバーディフェンス研究所　専務理事
株式会社 Armoris 取締役専務 CTO 内閣サイバーセキュリティセンター　普及啓発・人材育成専門調査会　委員
株式会社 JVC ケンウッド 技術開発部 製品セキュリティ推進グループ・グループ長／PSIRT リーダー
金融関連製造会社　製品セキュリティ部門　マネージャ

1.2.3.2.3.2 インタビュー結果の整理

1.2.3.2.2.1 にて検討した CSIRT・PSIRT が連携する際に共有する情報項目例について、有識者にインタビューをして把握した結果を表 9 に示します。

表 9　CSIRT・PSIRT 連携の際に共有するフォーマットに記載する情報項目（有識者インタビュー結果）

A)	情報収集	脅威脆弱性情報の収集配信	• 情報種別（脅威、脆弱性、インシデント事例等） • 情報提供者（JPCERT、バグハンター等） • 影響度 • 公開範囲（TLP） • 対策の有無
有識者意見：〇　連携の効果あり			
【連携しているフォーマット、情報項目】 • 判明した脆弱性の対応判断に関わる情報をとして、以下の項目を共有しています 　➢ CVSS 　➢ 脆弱性を適応しない場合のリスク 　➢ 脆弱性の背景情報 • SBOM を用いた構成情報、設定情報の一元管理は効率的です 　➢ 監視を連携する際、社内システムとプロダクトで SBOM フォーマットを共通化して管理する仕組みを用意し、OSS や OS の脆弱性情報の収集を自動化し、マッチしたら担当者にアラートが飛ぶ仕組みを両 SIRT で共通での実施を検討しています 　➢ ライセンス管理の目的で使用しているオープンソースをリスト化して管理していて、それを SBOM のメタデータとして取り入れることを計画しています • 収集した情報に CSIRT・PSIRT それぞれの関心度合の重み付けする項目が要ります 【情報フォーマット活用に効果が低いと感じている点】 • 連携はありますが、連絡方法や情報項目は特に定まっていません • フォーマットは利用せず、メールベースでの情報共有を行っています • フォーマットは利用せず、独自に開発した脆弱性管理システムを作って関連する事業部と共有しています • 迅速性が求められる CSIRT・PSIRT 間連携において情報フォーマットは現実的ではなく、ツールを用いてリアルタイムで観測・把握する方が効果的です		

<table>
<tr><td colspan="4">

ITU の会議で FIRST の幹部が話した内容が参考になります（Resources of CSIRT（Tools and Services of CIRT/CSIRT)[5]）。情報フォーマットは事実上紙でなく、アプリで関係者間の情報共有がされています。Collective intelligence Framework（CIF)は、CSIRT がよく利用するサービスのプロシージャーが公開されているので、そこに表示される項目を参考にするとよいです。

日本はメールも使われていますが、海外はチケット管理システムに情報を管理して関係者みんなが見られるようにしている例が多いです
情報フォーマットありきの連携は機能しない事例が多いです

</td></tr>
<tr><td>B)</td><td>脆弱性管理</td><td>脆弱性評価</td><td>• ソフトウェア名、バージョン
• 脆弱性管理番号
• 再現環境、再現手順</td></tr>
<tr><td colspan="4">有識者意見：×　連携の効果なし</td></tr>
<tr><td colspan="4">＊本調査のインタビューにおいては、連携例や連携を推奨する意見はなかったため、情報フォーマットに関する意見もありません。</td></tr>
<tr><td>C)</td><td>脆弱性管理</td><td>脆弱性対策</td><td>• ソフトウェア名、バージョン
• 脆弱性管理番号
• 応急、恒久対策</td></tr>
<tr><td colspan="4">有識者意見：×　連携の効果なし</td></tr>
<tr><td colspan="4">＊本調査のインタビューにおいては、連携例や連携を推奨する意見はなかったため、情報フォーマットに関する意見もありません。</td></tr>
<tr><td>D)</td><td>インシデント対応</td><td>インシデントハンドリング</td><td>• インシデントの背景
• 利用された脆弱性の情報
• 対策の有無
• 被害の有無、被害範囲
• 外部団体（JPCERT、業界 ISAC 等）からの情報</td></tr>
<tr><td colspan="4">有識者意見：△　連携の効果は一部あり</td></tr>
<tr><td colspan="4">【連携しているフォーマット、情報項目】
• CSIRT・PSIRT 含めた関係者間で SBOM を用いた構成管理をすることでインシデント影響範囲把握の改善が期待できます
➢ 構成管理情報だけではなく設定情報等、リスクを判断する上で必要となる情報も管理しておく必要があります</td></tr>
</table>

5 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Services.pdf (2021/3 月時点で確認済み)

- サプライヤーがどの OSS を利用しているか把握するため、サプライチェーン全体で SBOM を活用した信頼チェーンを構築します
- 構成管理情報にて異常の報告を受ける事業部側の一次振り分けの際の判断をサポートします

【情報フォーマット活用に効果が低いと感じている点】

- インシデント情報の共有はチケット管理システム等のツールを利用しています
- 迅速性が求められる CSIRT・PSIRT 間連携は情報フォーマットは現実的ではなく、ツールを用いてリアルタイムで観測・把握する方が効果的です
  - 以前は RTIR（1.2.3.2.5.1 に紹介）が使われていましたが、より手を出しやすい OTRS（1.2.3.2.5.1 に紹介）のほうが使われるようになりました。Redmine みたいなバグトラッキングシステムを使っている人もいます
  - もともと組織内で使っているのを活用しているのが操作性の習熟もあり使われています
  - チケット管理でもバグトラッカーでも、組織内において開発管理等で利用しているシステムがあればそれを利用する例は多く、操作の習熟の観点からも推奨されます
  - 有償のチケット管理システムや自社独自で頑張っている例もあるが、うまく機能しているのは OTRS を自分たちに合うようにカスタマイズしている例のように見えます。今風の言葉をつかえばアジャイルな組織です
- 情報フォーマットありきの連携は機能しない事例が多いです

その他、仮説には含まれなかったものの有識者から得られた連携への意見

- SBOM のデファクトスタンダードを望みます
- ITIL（1.2.3.2.5.1 に紹介）インシデントマネジメントの考え方が参考になります

1.2.3.2.3.3 インタビュー結果からの分析

1.2.3.1 にて CSIRT・PSIRT で効果的な連携が可能であると導出された項目 A）脅威脆弱性情報の収集配信、及び D）インシデント対応において連携する際に利用するフォーマットや情報項目について、有識者インタビューから仮説に同意を得られた点と異論が出た点、また仮説に不足していた観点を分析しました。効果的な連携において求められるフォーマット案を本項に示します。

1.2.3.2.4 （A) 脅威脆弱性情報の収集配信の連携

脅威脆弱性情報の収集配信は、仮説に挙げた情報項目をフォーマットとして用意しているという意見は聞かれませんでした。有識者から、共有している、あるいは共有するべきと検討・計画しているフォーマットや情報項目として挙げられた内容を以下に整理します。

＜連携しているフォーマット、情報項目＞

- 判明した脆弱性の対応に向けた情報（CVSS、脆弱性によるリスク、背景情報等）
- SBOM 等に一元管理された構成管理情報（OSS 含む）・設定情報（収集した脆弱性情報と紐づけて合理的な脆弱性ハンドリングを実現）
- 収集した脅威脆弱性情報に、CSIRT・PSIRT の関心度合を示す情報

脅威脆弱性情報の収集配信について連携はしているものの、フォーマットは用いていない例も複数確認されました。また、連携の際に以下のような経験則や合理性から、フォーマット自体が不要と考える意見も聞かれました。

＜情報フォーマット活用に効果が低いと感じている点＞

- 独自に開発した脆弱性管理システムを作って関連する事業部と共有しています
- 迅速性が求められる CSIRT・PSIRT 間連携は情報フォーマットは現実的ではなく、ツールのダッシュボード等を用いてリアルタイムで観測・把握する方が効果的です

インテリジェンスツール等を利用してリアルタイムに収集・分析している情報をダッシュボードにて関係者が確認する方法は既に実施され、公開されている例もあります。

このような事例を考慮し、脅威脆弱性情報の収集配信を連携する際のフォーマット案、またフォーマットを利用しない場合の共有案の提言を「1.2.3.2.1.1 【提言】脅威脆弱性情報の収集配信」に示します。

1.2.3.2.5 （D) インシデント対応の連携

インシデント対応についても、仮説に挙げた情報項目をフォーマットとして用意しているという意見は聞かれませんでした。有識者から、共有している、あるいは共有するべきと検討・計画しているフォーマットとして挙げられた内容を以下に整理します。

＜連携しているフォーマット、情報項目＞

- SBOM 等に一元管理された構成管理情報・設定情報（インシデント影響範囲把握の特定やのため）

脅威脆弱性情報収集配信の場合と同様に、連携はしているものの、フォーマットは用いていない例も複数確認されました。また、インシデント対応は迅速性が求められる場合も多いことや、過去の経験則から、フォーマット自体が不要と考える意見も聞かれました。

＜情報フォーマット活用に効果が低いと感じている点＞

- インシデント対応を管理するツールを用いてリアルタイムな情報共有を行います
- 情報フォーマットありきの連携は機能しない事例が多いです

インシデント対応の状況をリアルタイムに共有するツールの利用は既に実施されて各所にて公開されています。これらを考慮し、インシデント対応の連携する際のフォーマット案、またフォーマットを利用しない場合の共有案の提言を「1.2.3.2.1.2　【提言】インシデント対応」に示します。

1.2.3.2.5.1 ツールの紹介（参考）

脅威脆弱性情報の収集配信やインシデント対応を行う際の関係者間の情報共有に際し、有識者から例示されたツールについて紹介します。

【RTIR (Request Tracker for Incident Response)】

RTIR はオープンソースのトラッカーで、インシデント対応に利用されています。様々なソースから得られた情報の関連を検出し、根本原因の調査を支援します。チケット管理によるインシデント対応の状況をダッシュボード上にて確認できます。

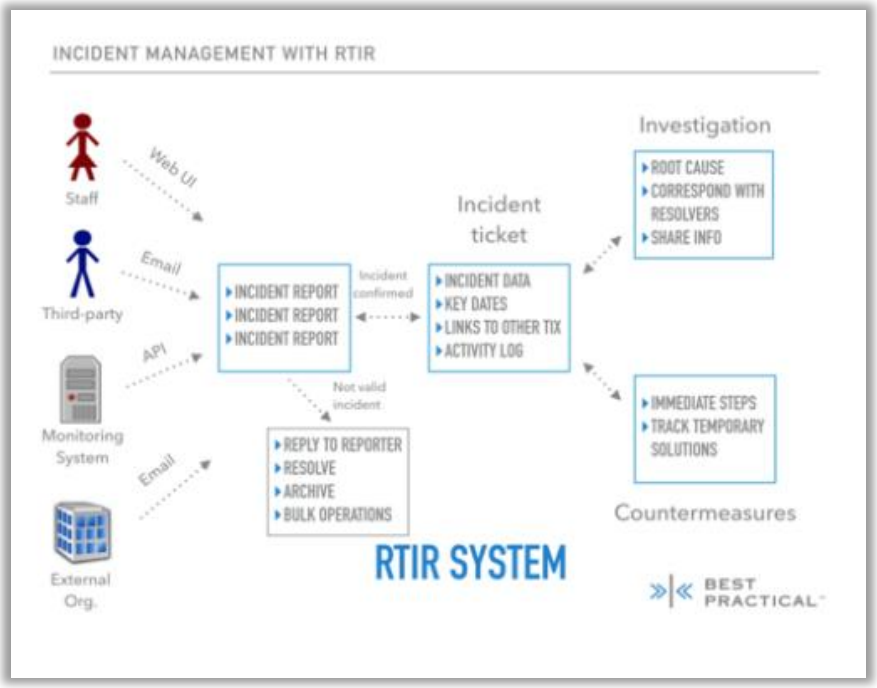

図 9　RTIR システムのワークフローのイメージ（出典：BestPractical[6]）

6 BestPractical , https://bestpractical.com/rtir (2021/3 月時点で確認済み)

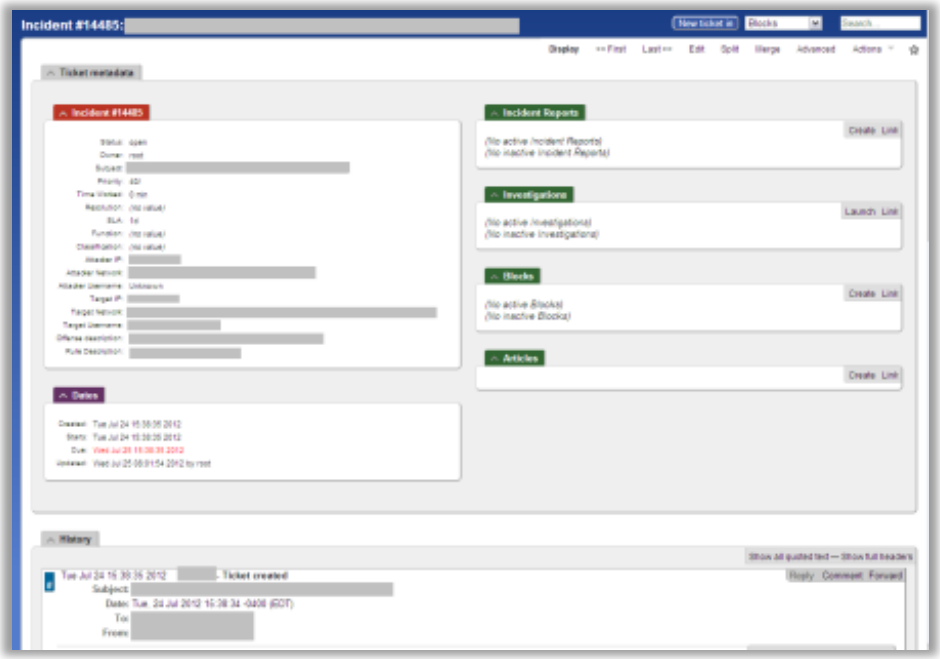

図 10　インシデントトラッキングのイメージ（出典：ITU[7]）

【OTRS（Open Technology Real Services）[8]】

OTRS はオープンソースのチケットシステムで、インシデント対応に利用されています。ITIL（Information Technology Infrastructure Library）に準拠した運用ができます。API や関連ドキュメントが整備されていて、他のツールや SIEM（Security information and event management）とのインテグレーションも可能です。

7 ITU, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Services.pdf (2021/3 月時点で確認済み)

8 OTRS, https://otrs.com/otrs-solutions/corporate-security/ (2021/3 月時点で確認済み)

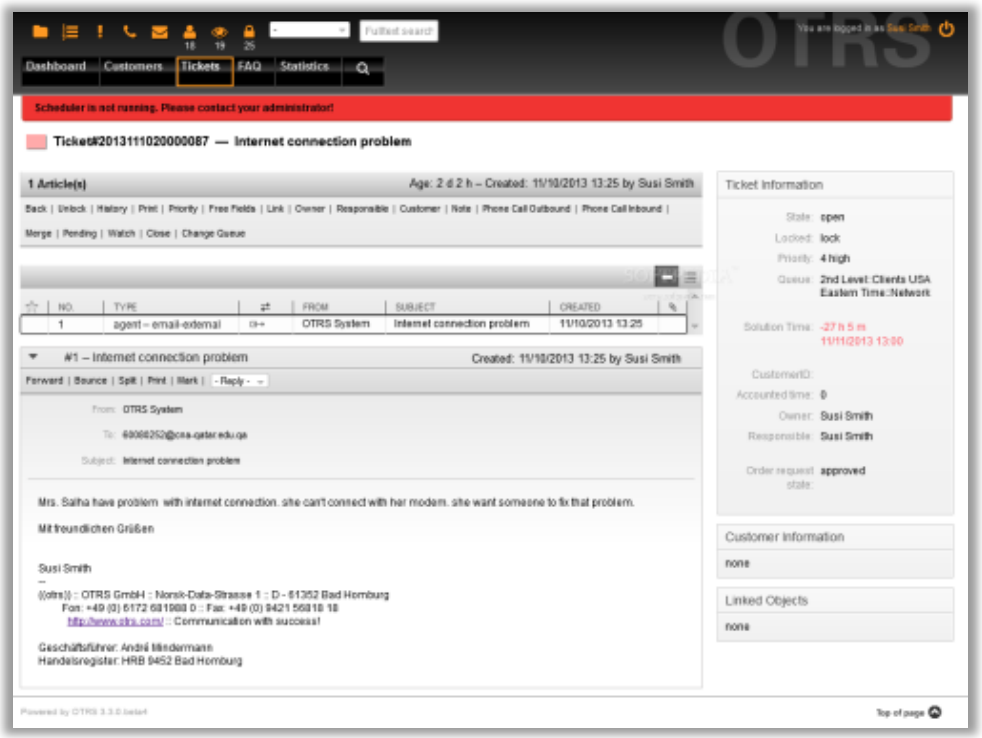

図 11　OTRS のチケットイメージ（出典：ITU[9]）

9 ITU, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Services.pdf (2021/3 月時点で確認済み)

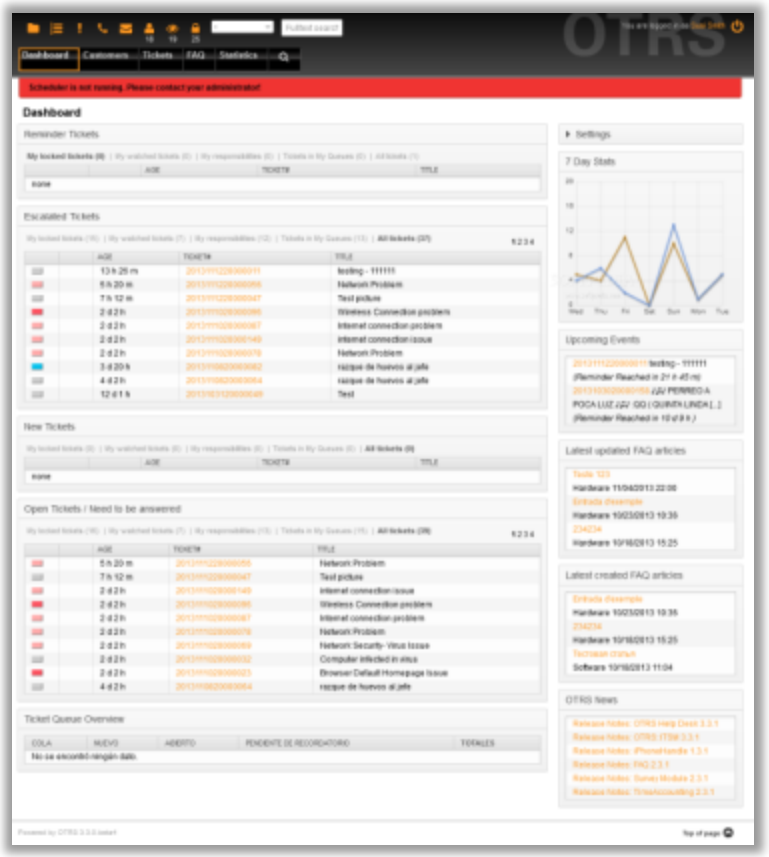

図 12　OTRS のダッシュボードイメージ（出典：ITU[10]）

【Snort + Graylog】

Snort はオープンソースの IPS（Intrusion Prevention System）で、ネットワーク上で脅威となりうる不審なパケットを検出するのに利用されます。Snort community が無償で提供する定義ファイルに加え、Cisco 社のセキュリティ専門機関 Talos[11]が同社の顧客向けに提供する定義ファイルを有償で利用できます。

Graylog はオープンソースのログ管理ソフトウェアで、ログを集約して一括管理し、検索や可視化を可能にします。

Snort のアラートのログを Graylog に取り込んで図 13 のようにダッシュボードに表示することにより、関係者間で可視化された情報を共有できる。設定の手順は Github にて公開されています。[12]

10 ITU, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Services.pdf (2021/3 月時点で確認済み)

11 Talos, https://talosintelligence.com/ (2021/3 月時点で確認済み)

12 Github – Graylog2, https://github.com/Graylog2/graylog-guide-snort (2021/3 月時点で確認済み)

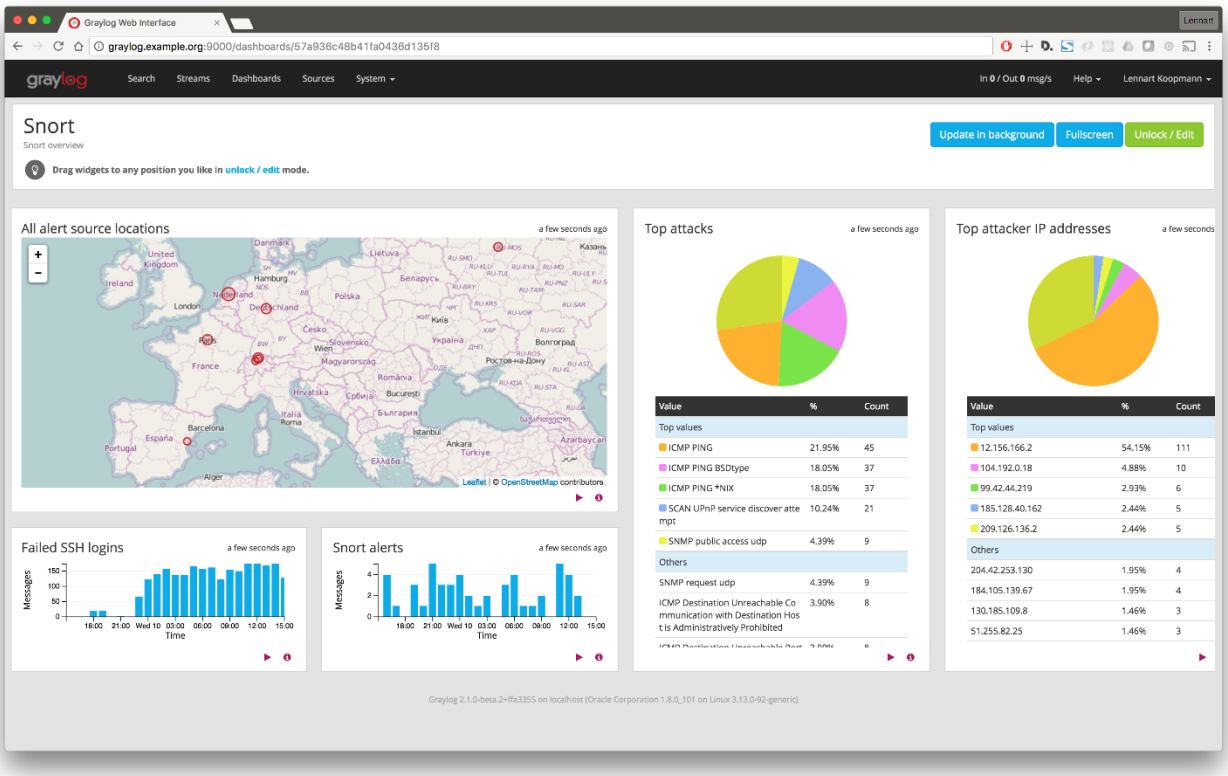

図 13　Snort アラートを Graylog のダッシュボードで表示したイメージ（出典：Github - Graylog2[13]）

13 Github – Graylog2, https://github.com/Graylog2/graylog-guide-snort (2021/3 月時点で確認済み)

1.2.3.3 OSS の品質保証や製品セキュリティ維持に関わる組織・団体

1.2.3.3.1 NIST

NIST (National Institute of Standards and Technology：米国国立標準技術研究所) は、情報セキュリティ強化ための規格としての FIPS (Federal Information Processing Standards：連邦情報処理標準) やガイドライン (SP800 シリーズ) の開発を行っています。NIST は SCAP (Security Content Automation Protocol：セキュリティ設定共通化手順) を開発し、「脆弱性管理、コンプライアンス管理の一部を機械化(自動化)することにより、情報システムに対するセキュリティ対策の負荷軽減と情報セキュリティ施策の推進の両立を目的とした仕様群」を定義しています(NIST 800-126,NIST 800-117,NISTIR 7511 rev2)。この仕様は米国の National Vulnerability Database (NVD)や JPCERT/CC と情報処理推進機構(IPA)が共同管理している、脆弱性データベースの Japan Vulnerability Notes (JVN)や JVN iPedia で使用されています。これらのデータベースには、OSS の脆弱性も含まれています。

1.2.3.3.2 MITRE Corporation

MITRE は米国政府の支援を受けている非営利団体で、CVE (Common Vulnerabilities and Exposures：共通脆弱性識別子) を管理しています。新しい脆弱性情報が公開される際に、「CVE 識別番号 (CVE-ID)」が割り振り振られます。この割り振りを行うのは CVE Numbering Authorities (CNAs) の役割です。CVE は多くのセキュリティ・ツールで使用されています

1.2.3.3.3 NTIA

米国 NTIA(電気通信情報局)において、ソフトウェアのサプライチェーンに対する可視性について議論が進められています。SBOM の仕様を作成、SBOM アプリケーション・ユースケースの検討分析、実際にヘルスケア業界などで実証実験を行うなど、業界全体のエコシステムにおける、品質およびセキュリティに関する、強靭なソフトウェアのサプライチェーンの構築を検討しています。

1.2.3.3.4 SPDX (Linux Foundation)

SPDX プロジェクトは、ソフトウェア・コンポーネントに関連するコンポーネント、ライセンス、

著作権、およびセキュリティ情報を複数のファイル形式で通信するための標準言語の仕様を取り決めています。SPDX は交換できるデータを記述するための拡張性のある言語で、ソフトウェア・パッケージおよび関連コンテンツに関する情報を簡単に収集および共有することができます。SPDX は NTIA SBOM　のワーキング・グループの議論の中で SBOM の機械可読なフォーマットの一つとして検討されています。

1.2.3.3.5　JPCERT/CC

JPCERT コーディネーションセンター（JPCERT/CC）は、インターネットを介して発生する侵入やサービス妨害等のコンピュータ・セキュリティ・インシデントについて、日本国内に関するインシデント等の報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっています。特定の政府機関や企業からは独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいます。

1.2.3.3.6　独立行政法人情報処理推進機構（IPA）

IPA では、日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的として脆弱性対策情報ポータルサイト「Japan Vulnerability Notes（JVN)」を運営しています。JVN は、JPCERT コーディネーションセンターと共同で運営されています。

(1) 脆弱性対策情報ポータルサイト「Japan Vulnerability Notes（JVN)」
JVN には、CERT/CC など海外の調整機関と連携した脆弱性情報が公表されています。

(2) 脆弱性関連情報の届出受付窓口の運営
IPA では、以下脆弱性関連情報の届出を受付けている[14]。

- ソフトウェア製品脆弱性関連情報
- ウェブアプリケーション脆弱性関連情報

[14] 独立行政法人情報処理推進機構 脆弱性関連情報の届出受付
https://www.ipa.go.jp/security/vuln/report/index.html (2021/3 月時点で確認済み)

1.2.4　OSS セキュリティの品質確保を担う人材案

1.2.2 では、OSS 活用する際に必要な技術検証項目を複数の文献の調査から導き出し、各業界に対してヒアリングすることで現状の活動状況を明らかにしました。また、1.2.3 項では OSS 活用に関して CSIRT・PSIRT が連携する上で効果が期待される連携案と情報フォーマットについて有識者のヒアリングを反映しつつ提言を行いました。

これらの状況を踏まえ、本項では、OSS のセキュリティ品質確保にむけて今後ますます重要となる技術検証を担う人材の育成案について、有識者の意見を集め、その結果を分析し、人材の育成案について提言します。

OSS のセキュリティの品質確保に関わる人材像について、また各人材像に対する効果的と考えられる育成方法を検討した仮説を 1.2.4.1.1 に示します。

そして、その仮説をベースにして有識者インタビューを実施して把握した結果を基に作成した人材像及び人材育成案の提言を 1.2.4.2.1 に示します。その提言を導き出すにあたって 1.2.4.2.2 にて仮説への有識者の意見を分析した結果を示します。

1.2.4.1　OSS セキュリティの品質確保を担う人材状況調査

1.2.4.1.1　OSS セキュリティの品質確保を担う人材状況調査まとめ

OSS のセキュリティ確保に関わる人材として求められる人材像を検討するにあたり、まずは机上調査を実施し、その結果から仮説を立案しました。本項では、仮説の検討について示します。

仮説の検討は図 14 に示すフローで実施しました。

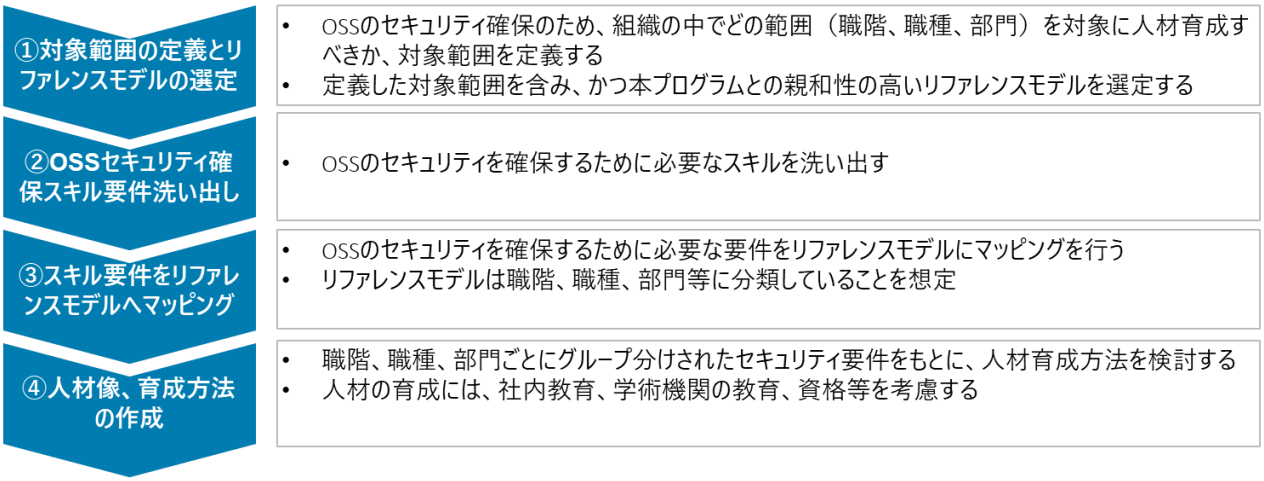

図 14　OSS のセキュリティ確保に必要となる人材像および育成案を検討するためのフロー

① 対象範囲の定義とリファレンスモデルの選定

OSS のセキュリティ確保のため、組織の中でどの範囲の職階、職種、部門を対象に人材育成すべきか、対象範囲を定めるにあたり、経済産業省の産業サイバーセキュリティ研究会ワーキング・グループ 2（経営・人材・国際）が公開する事務局説明資料[15]を参考にしました。同研究会の検討結果によると、国内企業においては、セキュリティを専業とするセキュリティ統括部門が階層に応じて横断的に全社のセキュリティ体制を統括する関係が認められるとの報告がありました。部門間の関係の概略を図 15 に整理します。部門に関わる人材として、「2020 年 IPA 発行サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き」[16]の記載された分類に従い従い、「セキュリティ人材」「プラス・セキュリティ人材」という分類で整理しました。各人材について、表 10 に概要を示します。図 15 では、情報システム部門やセキュリティ統括部門や関係部門を考慮した人材像が定義されていて 1.2.3 項で示した CSIRT・PSIRT 連携に関連する組織構成が考慮されています。

15 METI, https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/004_03_00.pdf (2021/3 月時点で確認済み)

16 METI, https://www.meti.go.jp/press/2020/09/20200930004/20200930004-1.pdf (2021/3 月時点で確認済み)

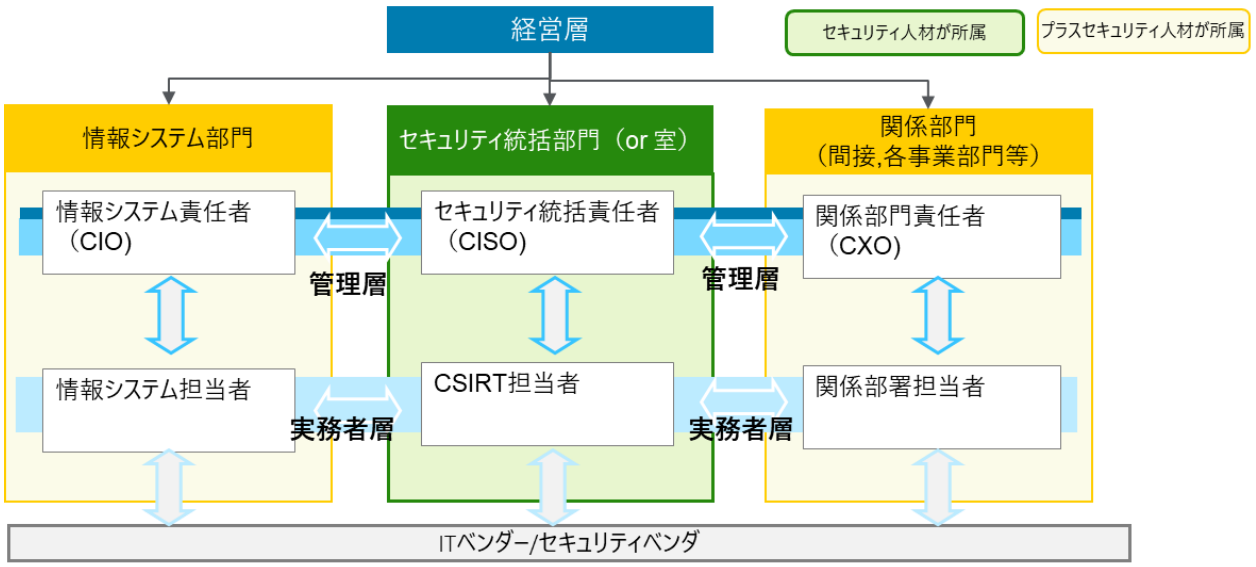

図 15　セキュリティ統括部門と関連部門との関係性

表 10　セキュリティに関わる人材の分類

人材分類	概要
セキュリティ人材	セキュリティ対策を主たる目的とする業務を担う人材。SIRT や CISO 等の経営層を補佐するセキュリティ統括部署等が該当
プラス・セキュリティ人材	デジタル部門、事業部門、管理部門等セキュリティ対策以外に主たる業務を担当しつつ、組織のセキュリティ対策を実践する人材

② OSS セキュリティ確保スキル要件洗い出し

OSS のセキュリティを確保するために必要なスキルとして、「2020 年 IPA 発行サイバーセキュリティ経営ガイドライン Ver2.0」に記載された ITSS+のタスク概要図上に、セキュリティ人材とプラス・セキュリティ人材関連する担当領域を分類しました。それぞれ異なる領域であることが確認できます。

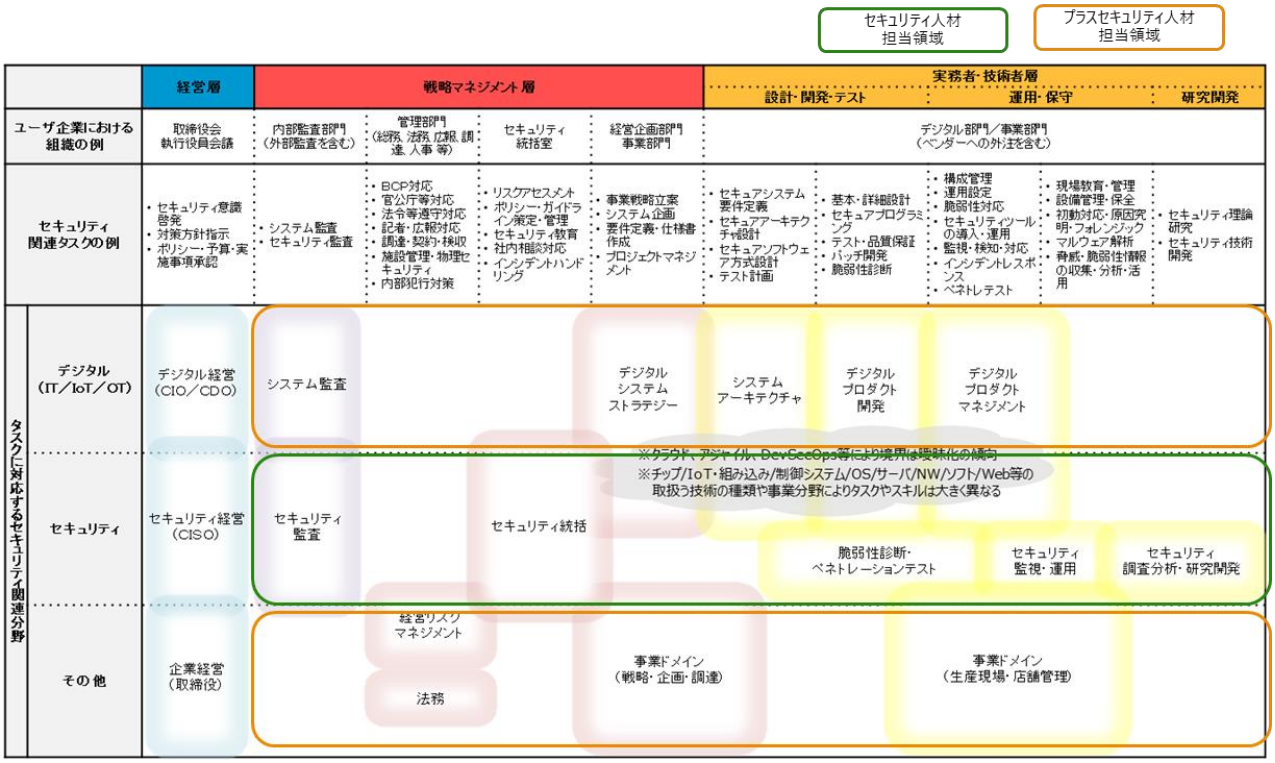

図 16　ITSS＋で定義されたセキュリティタスク[17]における人材分類ごとの担当領域

次に、必要となるスキル一覧を洗い出すにあたり、経済産業省が公開する「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性」[18]で公開する OSS 利活用における留意事項の観点に示す内容を参照し、必要となるスキルを検討しました。OSS のセキュリティ確保において必要と考えられるスキルの一覧をまとめた結果を表 11 に示します。1.2.2 で取りまとめた技術検証項目はマネジメント層にも関係しますが、主に実務者層に関連するスキルであり、表 11 の主に「リスク管理手法」「脅威脆弱性フォーマットの理解」「プログラミング能力」に関連します。各項目は表 12 の「セキュリティ関連タスクの例」に含まれることが確認できました。

17 IPA, https://www.ipa.go.jp/files/000058688.xlsx (2021/3 月時点で確認済み)

18 METI, https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/004_03_00.pdf (2021/3 月時点で確認済み)

表 11　OSS のセキュリティ確保において必要となるスキル一覧

OSS セキュリティ確保において 必要なスキル	概要
リスク管理手法	コミュニティ過疎化や分裂による予期せぬ開発終了、ライセンス違反による訴訟等、様々なリスクを識別し管理する能力
OSS 前提の商取引の理解	サプライチェーンを構成する団体で互いに必要な情報や素材（ソースコードや SBOM の提供等）の受け渡し方法等、OSS 前提とした商取引に関する理解
OSS 資産管理手法の理解	OSS の構成管理に必要な SPDX 等、SBOM の標準フォーマットに関する理解
OSS ライセンスの理解	GPL、MIT ライセンス、Apache ライセンス等、ライセンス形態ごとに利用者が配布時にすべきことの理解
OSS の事業貢献度の測定	OSS の利活用における効果を定量的に測定し、OSS 必要性を経営層に報告し、必要となるリソースを確保できる能力
OSS 選定手法の理解	OSS の品質確保に必要となる、コミュニティの活性度、誕生の経緯等、複数指標の理解
OSS コミュニティへの参加	OSS コミュニティにメンテナー、開発者、オブザーバーとして参加し、コミュニティ動向や組織内の要望をフィードバックできる能力
脅威脆弱性フォーマットの理解	NIST CSF、ATT&CK などのフレームワークを用いた攻撃手法の整理、および CVSS、STIX、OpenIOC 等を用いた脅威・脆弱性情報を示す標準フォーマットの理解
プログラミング能力	OSS を利活用するために必要なプログラミング能力
外国語能力	OSS に関する国際団体において円滑なコミュニケーションに必要となる外国語運用能力

③ スキル要件をリファレンスモデルへマッピング

表 11 に洗い出したスキルを、各セキュリティ人材の分野ごとにマッピングをした結果を表 12 に示します。「1.2.2 項　セキュリティ確保に関する OSS の技術検証項目」の表 1 で示した検証活動の各項目は、表 12 の「セキュリティ関連タスクの例」に含まれていて、該当項目については下線で示しています。

表 12　セキュリティ人材ごとに必要となるスキル

	区分	分野名	セキュリティ関連タスクの例	OSSセキュリティ確保において必要なスキル										人材分類	
				リスク管理手法	OSS前提の商取引の理解	OSS資産管理手法の理解	OSSライセンスの理解	OSSの事業貢献度の測定	OSS選定手法の理解	OSSコミュニティへの参加	脅威脆弱性フォーマットの理解	プログラミング能力	外国語能力	セキュリティ人材	＋セキュリティ人材
戦略マネジメント層	デジタル	システム監査	システム監査、脅威モデリング、脅威分析、報告・助言 等	○											○
		デジタルシステムストラテジー	デジタル事業戦略立案、システム企画、要件定義・仕様書作成、プロジェクトマネジメント 等					○							○
	セキュリティ	セキュリティ監査	セキュリティ監査、脅威モデリング、脅威分析、報告・助言 等	○										○	
	その他	セキュリティ統括	セキュリティ教育・普及啓発、セキュリティ関連の講義・講演、脅威モデリング、脅威分析、セキュリティリスクアセスメント、セキュリティポリシー・ガイドラインの策定・管理・周知、警察・官公庁等対応、社内相談対応、インシデントハンドリング 等	○		○	○	○			○		○	○	
		経営リスクマネジメント	経営リスクマネジメント、BCP／危機管理対応、脅威モデリング、脅威分析、サイバーセキュリティ保険検討、記者・広報対応、施設管理・物理セキュリティ、内部犯行対策 等	○	○										○
		法務	デジタル関連法令対応、コンプライアンス対応、契約管理 等		○	○	○								○
		事業ドメイン（戦略・企画・調達）	事業特有のリスクの洗い出し、事業特性に応じたセキュリティ対応、サプライチェーン管理 等	○	○	○	○								○
実務者・技術者層	デジタル	デジタルシステムアーキテクチャ	脅威モデリング、脅威分析、セキュアシステム要件定義、セキュアシステムアーキテクチャ設計、セキュアソフトウェア方式設計、テスト計画 等	○		○	○		○						○

	区分	分野名	セキュリティ関連タスクの例	OSS セキュリティ確保において必要なスキル										人材分類	
				リスク管理手法	OSS 前提の商取引の理解	OSS 資産管理手法の理解	OSS ライセンスの理解	OSS の事業貢献度の測定	OSS 選定手法の理解	OSS コミュニティへの参加	脅威脆弱性フォーマットの理解	プログラミング能力	外国語能力	セキュリティ人材	＋セキュリティ人材
		デジタルプロダクト開発	基本設計、詳細設計、セキュアプログラミング、静的解析、コードレビュー、ペネトレーションテスト、ファジングテスト、テスト・品質保証、パッチ開発 等				○		○	○		○			○
		デジタルプロダクト運用	構成管理、運用設定、利用者管理、サポート・ヘルプデスク、脆弱性対策・対応、インシデント対応 等			○					○				○
	セキュリティ	脆弱性診断・ペネトレーションテスト	脆弱性診断、ペネトレーションテスト、ファジングテスト 等							○	○	○		○	
	セキュリティ	セキュリティ監視・運用	セキュリティ製品・サービスの導入・運用、セキュリティ監視・検知・対応、インシデント対応、連絡受付 等			○				○	○			○	
	セキュリティ	セキュリティ調査分析・研究開発	サイバー攻撃捜査、原因究明・フォレンジック、マルウェア解析、脅威・脆弱性情報の収集・分析・活用、セキュリティ理論・技術の研究開発、セキュリティ市場動向調査 等							○	○	○	○	○	
	その他	事業ドメイン（生産現場・事業所管理）	現場教育・管理、設備管理・保全、QC 活動、初動対応 等			○					○				○

④ 人材像、育成方法の作成

以上の検討結果として、OSS セキュリティの確保に求められる人材像及び育成方法の仮説として、表 13 に整理しました。

表 13　OSS セキュリティの確保に求められる人材像、および育成方法（仮説）

分類	層別	求められる人材像例	育成方法
セキュリティ人材	A) 実務者・技術者層	• 脅威脆弱性管理の共通フォーマットを理解できる • 常に最新の攻撃手法を情報収集している • OSS コミュニティ等各業界団体に参加し、情報交換ができる • OSS のコードを理解し脆弱性を特定できる	• 業界団体への参加促進 • 産学連携の促進 • 資格取得の促進
	B) 戦略マネジメント層	• OSS 利活用する上でのリスク管理や判断ができる • ライセンスを理解し、適切な OSS の構成管理ができる • OSS 利活用における自社事業への貢献度を指標定義、評価できる • 英語を含めた海外とのコミュニケーションできる	• 業界団体への参加促進 • 産学連携の促進 • 語学力向上
プラス・セキュリティ人材	C) 実務者・技術者層	• セキュリティバイデザインに基づく設計ができる • サポート体制活性度等、複数要因から適切な OSS を選定できる • OSS のコードを理解し実装できる	• 業界団体への参加促進 • 産学連携の促進 • 資格取得の促進
	D) 戦略マネジメント層	• OSS を利活用する上でのリスク管理や判断ができる • 調達、製造、運用後も含むサプライチェーン全体を含めた OSS の構成管理、トレースができる • OSS 利活用における自社事業への貢献度を指標定義、評価できる • OSS を前提とした商取引、法規を理解し、説明できる • 英語を含めた海外とのコミュニケーションできる	• 業界団体への参加促進 • 産学連携の促進 • 語学力向上

1.2.4.2　OSS セキュリティの品質確保を担う人材育成案

1.2.4.2.1　OSS セキュリティの品質確保を担う人材案の提言

1.2.4.2.1.1 【提言】セキュリティ人材 – 実務者・技術者層

仮説に対する有識者の意見、また新たに挙げられた点を整理し、セキュリティ人材の実務者・技術者層に求められる人材像・育成案を以下に示します。

人材像案（セキュリティ人材 – 実務者・技術者層）
• 脅威脆弱性管理の共通フォーマットを理解できます • 常に最新の攻撃手法を情報収集しています • OSS コミュニティ等各業界団体に参加し、情報交換ができます • インシデント対応、ハンドリングができます • 出荷前の製品にリスクアセスメントできます • 脆弱性の修正対応ではなく、回避策を検討できます • バランスよく全体的にセキュリティを考えられます • 組織内の製品・システムの知識、および関連部門と連携可能なコミュニケーション能力があります • 情報収集・発信や人脈作りのための語学力があります
育成案（セキュリティ人材 – 実務者・技術者層）
• 業界団体への参加促進 • 資格取得の促進 • OJT によりスキル習得 • 演習による能力向上 • 外部講習の受講 • 業界団体やコミュニティへの参加 • 外部カンファレンスで発表 • 語学力向上

1.2.4.2.1.2 【提言】セキュリティ人材 – 戦略マネジメント層

仮説に対する有識者の意見、また新たに挙げられた点を整理し、セキュリティ人材の戦略マネジメント層に求められる人材像・育成案を以下に示します。

人材像案（セキュリティ人材 – 戦略マネジメント層）
• OSS 利活用する上でのリスク管理や判断ができます • ライセンスを理解し、適切な OSS の構成管理ができます • OSS 利活用における自社事業への貢献度を指標定義、評価できます • 英語を含めた海外とのコミュニケーション能力を持ちます • OSS 導入のガイドラインを策定できます • 組織リスクとコストを総合判断できます • 経営陣や技術者とコミュニケーションできるスキル • 他分野間の人材をまとめ、実務者の「意識」と「スキル」を維持できるリーダースキル • 社会人に求められるベースのスキル • 会社経営に求められることと同様のスキル
育成案（セキュリティ人材 – 戦略マネジメント層）
• 業界団体への参加促進 • 語学力向上 • OJT によりスキル習得 • 演習による能力向上 • マネジメント層向けの研修

【育成案に関する補足】

育成の前提として、採用に関する意見が有識者から挙げられました。育成の対象となる人材について、採用条件を明確化し、育成可能な条件がそろった人材を採用するスクリーニングが必要という意見で、米国 NSA が採用の要件に記載している SME（Subject Matter

Expert：内容領域専門家）が例示されました。OSS の場合は、OSS の SME を採用することが望ましいです。

また場合によっては、人材育成をできない状況も想定されるため、その場合も採用の準備や体制を整備しておくことが望ましいです。

1.2.4.2.1.3 【提言】プラス・セキュリティ人材 –実務者・技術者層

仮説に対する有識者の意見、また新たに挙げられた点を整理し、プラス・セキュリティ人材 – 実務者・技術者層に求められる人材像・育成案を以下に示します。

人材像案（プラス・セキュリティ人材 – 実務者・技術者層）
• セキュリティバイデザインに基づく設計ができます（事業部門） • サポート体制活性度等、複数要因から適切な OSS を選定できます（事業部門） • OJT で業務をこなし、バランスよくセキュリティを実装するスキルがあります（事業部門） • OSS 利用に際し定められたルールを理解し、遵守した実装・運用をするスキルがあります（事業部門） • 事業に応じた適切なリスクコントロールが実行できます（事業部門・管理部門） • エンドユーザとして最低限の IT スキルがあります（事業部門・管理部門） • 各々の業務の範囲内でできるセキュリティ対応を行います（事業部門・管理部門）
育成案（プラス・セキュリティ人材 – 実務者・技術者層）
• 業界団体への参加促進 • 資格取得の促進 • OJT によりスキル習得 • セキュリティ啓発トレーニング（組織内研修、E ラーニング） • 演習による能力向上

1.2.4.2.1.4 【提言】プラス・セキュリティ人材 -戦略マネジメント層

仮説に対する有識者の意見、また新たに挙げられた点を整理し、プラス・セキュリティ人材の戦略マネジメント層に求められる人材像・育成案を以下に示します。

人材像案（プラス・セキュリティ人材 – 戦略マネジメント層）
• OSS を利活用する上でのリスク管理や判断ができます • 調達、製造、運用後も含むサプライチェーン全体を含めた OSS の構成管理、トレースができます • OSS 利活用における自社事業への貢献度を指標定義、評価できます • OSS を前提とした商取引、法規を理解し、説明できます • 英語を含めた海外とのコミュニケーション能力を持ちます • 事業に応じた適切なリスクコントロールが実行できる人材（事業部門） • 顧客に説明し、理解させる交渉力をもった人材（事業部門） • 開発委託先のセキュリティを管理するスキルがあります（事業部門） • エンドユーザとしての最低限の IT のスキルが必要（事業部門・管理部門） • 各々の業務の範囲内でできるセキュリティ対応を行います（事業部門・管理部門） • 会社経営に求められることと同じスキルを持ちます（事業部門・管理部門）
育成案（プラス・セキュリティ人材 – 戦略マネジメント層）
• 業界団体への参加促進 • 語学力向上 • OJT によりスキル習得 • セキュリティ啓発トレーニング（組織内研修） • 演習による能力向上 • 経営層向けのマネジメントセミナー

1.2.4.2.2 有識者インタビュー結果まとめ

1.2.4.2.2.1 インタビュー結果の整理

1.2.4.1.1 にて検討した技術検証を担う人材育成案について、有識者にインタビューをして把握した結果を示します。

表 14　(A)セキュリティ人材　実務者・技術者層(識者インタビュー結果)

分類	層別	求められる人材像例	育成方法
セキュリティ人材	A) 実務者・技術者層	• 脅威脆弱性管理の共通フォーマットを理解できる • 常に最新の攻撃手法を情報収集している • OSS コミュニティ等各業界団体に参加し、情報交換ができる • OSS のコードを理解し脆弱性を特定できる	• 業界団体への参加促進 • 産学連携の促進 • 資格取得の促進

【求められる人材像】

- インシデント対応、ハンドリングができる人材
- 製品出荷前のリスクアセスメントを行える人材
  - ➢ 出荷前の企画、設計、実装、検証から、出荷後の販売・サービスと全ての段階のセキュリティをサポートしています
- 脆弱性の修正対応ではなく、回避策を検討できる人材が必要
  - ➢ OSS 自体の改修はユーザ組織側ではできないため回避策が重要
- バランスよく全体的にセキュリティを考えられる人材
  - ➢ 例えば IoT 機器はモバイル（スマフォアプリ）、サーバ、機器と三位一体で動いているので、セキュリティのトータルバランスを考えられることが大事
- 製品により、脆弱性への影響度は異なるので、判別できる人材
- 開発側のリソースは限られているので実態を総合的に確認して判断できる人材
- 脅威脆弱性に関する情報を経営者が理解できるように説明できる人材
  - ➢ 技術や対策コスト等総合的にまとめ、報告先の経営層のバックグラウンドや指向を把握して、相手に合わせた切り口で説明できます。社歴が長ければ組織を把握していることを活用し、転職者は前職における観点を含める等して各自工夫します
- 語学力（英語、中国語等）も必要（情報収集や発信、人脈づくりのため）

分類	層別	求められる人材像例	育成方法

- 大量の脆弱性情報の中から組織にとって重大な脆弱性を判別するために、その分野に詳しく内部と情報連携可能なコミュニケーション能力をもつ人材が必要

【育成方法】

- OJT による育成
  - OSS の脆弱性の回避策含めて総合的にソフトウェアを理解できる人材育成が重要
  - 机上調査力に加え、脆弱性診断等、実機で検証して理解していけるスキルを伸ばしています
  - 製品セキュリティ部門内で様々なセキュリティ業務を行っており、各機能の選りすぐりの人材 （Best of Best） が PSIRT のメンバーとなり、普段の業務と PSIRT の任務を兼業します
  - エンジニアの興味の方向性と業務を絶妙にマッチさせると成長も早いです。環境に工夫が必要（日本の管理職はそれを理解できないことが多いです）
- 演習で個々の課題を見つけ出し改善する
  - 金融 ISAC の実施する実践的な演習、サイバークエスト[19]を参照
- 資格取得や関連する外部講習受講
  - （技術系）CEH、SANS、セキュリティ企業の提供するセミナー等
  - （管理系）CISSP 等
- 業界団体やコミュニティへの参加
  - FIRST、CVE、HITB 等
  - Linux Foundation 等
  - OSS のコミュニティに積極的に関与し、浮かび上がった人材が該当します

19 ITmedia, https://mag.executive.itmedia.co.jp/executive/articles/2004/22/news022.html (2021/3 月時点で確認済み)

表 15　(B)セキュリティ人材　戦略マネジメント層(識者インタビュー結果)

分類	層別	求められる人材像例	育成方法
セキュリティ人材	B) 戦略マネジメント層	• OSS 利活用する上でのリスク管理や判断ができる • ライセンスを理解し、適切な OSS の構成管理ができる • OSS 利活用における自社事業への貢献度を指標定義、評価できる • 英語を含めた海外とのコミュニケーション能力	• 業界団体への参加促進 • 産学連携の促進 • 語学力向上

【求められる人材像】

- 組織リスクとコストを総合判断できるスキルがあります
  - ➢ パッチ検証と残存リスクを比較して考えられます
  - ➢ 最新パッチにできない場合には回避策を考えられます
- 経営陣の思考に合わせて説得交渉できる対人スキルがあります
- 事業部門や技術者とコミュニケーションできるスキルがあります
  - ➢ 旧バージョンではどのくらいのリスクがあるか等技術者と話せます
  - ➢ 事業部門や開発現場に説明する際に、背景情報、脆弱性を修正しなかった場合のリスク、二次リスク、三次リスクを説明できます
  - ➢ オープンソースは安定したもので最新版を使うように事業部門へのガイドラインを作成し提供しています
  - ➢ 事業部の理解が得られるように説得力のある説明ができます
- CSIRT・PSIRT の連携には設計、知識的背景等の価値観の異なる両者を取りまとめるリーダー役が必要
  - ➢ 実務者の「意識」と「スキル」を維持できるリーダーが必要です
- 社会人に求められるベースのスキルを持つ
  - ➢ コラボレーション、プレゼンテーション、ロジカルシンキング、クリティカルシンキングといったスキルは口頭だけでなくレポートライティングも含めたコミュニケーションスキルが必要です。この辺のスキルをまとめると、米国の情報機関がエージェントを育てる方法や、米国 OPM のリストを見ていると戦略マネジメント層のスキルと一致します
- 会社経営に求められることと同じスキルを持ちます。困難な状況において意思決定するスキルなど、会社経営者向けに実施されるカリキュラムと一致します

分類	層別	求められる人材像例	育成方法

- 管理系：組織の現状の把握（経営戦略、国内外の拠点、国内外の事業、リスク管理、等）、コミュニケーションスキル
- 技術系：CISSP 程度のセキュリティ知識、COBIT、リスク管理、内部組織の理解（CISO COMPASS[20],CISO ハンドブック[21]が参考になる）

【育成方法】

- OJT で業務をこなす
  - 一人で全てを実施するのではなく、お互いをカバーする、内部人材は外部人材から知識を学び、外部人材は内部人材から OJT で組織を学びます
  - 社歴が長ければ組織を把握していることを活用します
  - 転職者は前職における経験を活用します
  - PSIRT メンバーはインシデント対応以外にも平時からセキュリティに関する様々な業務を行っており、特段育成を必要とせずに各々の経験でうまくやっています
- 演習が効果的
  - 実践的な演習を行うのが効果的です。現在の世の中の人材育成の取り組みのほとんどが知識偏重になっていますが、いかに経験させるかが大事です。演習を通じて実戦経験を付けると自分に何が足りないか気づくことができます
- 経営層向けのマネジメントセミナー

20 Amazon, https://www.amazon.com/CISO-COMPASS-Navigating-Cybersecurity-Leadership/dp/1498740448 (2021/3 月時点で確認済み)

21 JNSA, https://www.jnsa.org/result/act_ciso/index.html (2021/3 月時点で確認済み)

表 16　(C)プラス・セキュリティ人材　実務者・技術者層(識者インタビュー結果)

分類	層別	求められる人材像例	育成方法
プラス・セキュリティ人材	C) 実務者・技術者層	• セキュリティバイデザインに基づく設計ができる • サポート体制活性度等、複数要因から適切な OSS を選定できる • OSS のコードを理解し実装できる	• 業界団体への参加促進 • 産学連携の促進 • 資格取得の促進

【求められる人材像】

- 言われたことを実装するだけでなく、全体のセキュリティを俯瞰して見られる能力を持ちます
- 特定の個所に偏重せずバランスよく製品全体のセキュリティを管理できるスキルがあります
- 事務方もエンドユーザとしての最低限の IT のスキルが必要
- 組織の全員がベースとなるセキュリティの知識や意識が必要
  - ➢ セキュリティ人材を中心に組織にセキュリティを広げていくやり方をすると、セキュリティは専門家だけがやればいいと思われてしまいます。全員参加を大前提にしないと、会社のオペレーションにはまりません。それぞれのポジションでセキュリティに対して何ができるか把握し、対応しないと、組織の対応力は上がらない
  - ➢ 企画から開発だけでなく、品証、生産、外注と関係する法務や調達にもセキュリティの観点から実施すべきことを社内セミナー通じて伝えています

【育成方法】

- 外部から専門家を採用します
- 専門家に外注し協業することで内部の人材を育てます
- 組織内のトレーニングや E ラーニング
  - ➢ 年に複数回全従業員が（オンライン含め）教育を受講しています
- OJT で業務をこなします（4～5 年かかる印象）
- 演習で個々の課題を見つけ出し改善します
  - ➢ 金融 ISAC の実施する実践的な演習、サイバークエスト[22]参照

22 ITmedia, https://mag.executive.itmedia.co.jp/executive/articles/2004/22/news022.html (2021/3 月時点で確認済み)

表 17　(D)プラス・セキュリティ人材　戦略マネジメント層(識者インタビュー結果)

分類	層別	求められる人材像例	育成方法
プラス・セキュリティ人材	D) 戦略マネジメント層	• OSS を利活用する上でのリスク管理や判断ができる • 調達、製造、運用後も含むサプライチェーン全体を含めた OSS の構成管理、トレースができる • OSS 利活用における自社事業への貢献度を指標定義、評価できる • OSS を前提とした商取引、法規を理解し、説明できる • 英語を含めた海外とのコミュニケーション能力	• 業界団体への参加促進 • 産学連携の促進 • 語学力向上

【求められる人材像】

- 顧客にセキュリティの管理を説明し、理解させる交渉力をもった人材
  - 積極的にセキュリティ対策コストをかけられる顧客はあまりいないため、戦略マネジメント層がセキュリティ責任分界を顧客と明確に決めて、機器提供側のセキュリティ範囲を最小限とします。善管注意義務のような、世の中の標準的なセキュリティ対策はやっておかなければなりませんが、その範囲を明示して顧客と合意を取ります。また顧客側におけるセキュリティ対策で必要となる義務を明確に示します
  - 製品提供後に公開された脆弱性の対策に費用を掛けられないのであるならば、提供側も最初に示した範囲でしか対応できないことを顧客に伝えていく、といった交渉事をできる人材が製品提供側で必要となります
- 開発委託先のセキュリティを管理するスキルがあります
  - ソフトウェア開発は外注することもあるため、契約書にオープンソースに脆弱性があった場合に対応すること等を記載して、契約や研修にて管理します
  - 委託先に対して、脆弱性の対応については、単なる瑕疵担保でなく、保守サービスに含めるのか？有償、無償の範囲も定める必要があると思っています。OSS に限った話ではないです。
- ライセンス管理ができます
- 事業に応じた適切なリスクコントロールが実行できる人材
  - プロジェクトマネージャとして、開発して終わりではなく市場投入後のリスクも含めて事業成功できることが必要な一要素となる
  - 最新パッチか否か、旧バージョンではどのくらいのリスクがあるかといった話が技術者とできることが大事
  - パッチが出ても、IT システムと違い製品は量産するため、マスターソフトウェアの動作確認フェーズでのバージョン変更は手戻りが甚大となります。特に製品開発のリードタイムが長い製品では、OSS に限らず汎用ソフトウェアはその間に脆弱性が公開されていきます。そういう際にパッチ検証と残存リスクを比較して考えられ、最新パッチにできない場合には回避策を考えられる人材が求められます
- 事務方もエンドユーザとしての最低限の IT のスキルが必要
- 組織の全員がベースとなるセキュリティの知識や意識が必要

➢ セキュリティ人材を中心に組織にセキュリティを広げていくやり方をすると、セキュリティは専門家だけがやればいいと思われてしまいます。全員参加を大前提にしないと、会社のオペレーションにはまりません。それぞれのポジションでセキュリティに対して何ができるか把握し、対応しないと、組織の対応力は上がらないと • 会社経営に求められることと同じスキルを持つ ➢ 管理系：組織の現状の把握（経営戦略、国内外の拠点、国内外の事業、リスク管理、等）、コミュニケーションスキル ➢ 技術系：CISSP 程度のセキュリティ知識、COBIT、リスク管理、内部組織の理解 【育成方法】 • OJT で業務をこなす ➢ 技術者はアウトソースできるのに対して、戦略マネジメント層、管理層は、組織をよく把握している必要があり、内部での育成が必要 • 組織内のトレーニングや E ラーニング ➢ 年に複数回全従業員が（オンライン含め）教育を受講しています • 演習が効果的 ➢ 実践的な演習をやるのが効果的です。現在の世の中の人材育成の取り組みのほとんどが知識偏重になっていますが、いかに経験させるかが大事です。演習を通じて実戦経験を付けると自分に何が足りないか気づくことができます • 経営層向けのマネジメントセミナーを受講する

表 18　人材育成　その他の意見（識者インタビュー結果）

その他、仮説には含まれなかったものの有識者から得られた連携への意見
• 日本の伝統的組織の就業環境ではトリアージ人材の候補に上がります。ジョブ型雇用に変えたとしてもスキルの箇条書きだけでは、本人の適性やモチベーションを判断できずうまく機能しないと想定します • inference 能力を備えた OSS の SME を採用すべきです • 大学や軍では inference 能力育成のカリキュラムがあります

1.2.4.2.3　(A) セキュリティ人材 - 実務者・技術者層

セキュリティ人材の実務者・技術者層は、CSIRT・PSIRT メンバーを想定します。

【人材像の分析】

仮説に示した人材像に対する有識者の意見は以下になりました。「OSS のコードを理解し脆弱性を特定できる」人材が不要な理由として、OSS のユーザ側となる企業は、コードを改変することは想定されないため、理解する必要性は低いことがインタビューにて判明しまし

た。また、仮説には含まれなかったが実効性のある人材像として、有識者から以下が挙げられました。

仮説	有識者コメント
• 脅威脆弱性管理の共通フォーマットを理解できる	賛同
• 常に最新の攻撃手法を情報収集している	賛同
• OSS コミュニティ等各業界団体に参加し、情報交換ができる	賛同
• OSS のコードを理解し脆弱性を特定できる	賛同無し
仮説以外で有識者が挙げた人材像	
• インシデント対応、ハンドリングができる • 出荷前の製品にリスクアセスメントできる • 脆弱性の修正対応ではなく、回避策を検討できる • バランスよく全体的にセキュリティを考えられる • 組織内の製品・システムの知識、および関連部門と連携可能なコミュニケーション能力がある • 情報収集・発信や人脈作りのための語学力がある	

【育成案の分析】

仮説に示した育成案に対する有識者の意見は以下になりました。「産学連携の促進」については有識者からの賛同は無く、代替としてコミュニティへの参加や外部の講習受講といった育成案が実用的という意見が得られました。また、仮説には含まれませんでしたが実効性のある人材像として、有識者から以下が挙げられました。

仮説	有識者コメント
• 業界団体への参加促進	賛同
• 産学連携の促進	賛同無し
• 資格取得の促進	賛同

仮説	有識者コメント
仮説以外で有識者が挙げた育成案	
• OJT によりスキル習得 • 演習による能力向上 • 外部講習の受講 • 業界団体やコミュニティへの参加 • 外部カンファレンスで発表 • 語学力向上	

「上長の業務采配の工夫」については、技術者の興味の方向と業務の方向性を絶妙にマッチさせると成長が著しいとの意見が得られました。「OSS やセキュリティ関連のコミュニティへの参加」については、育成であると同時に、コミュニティ上の活動の成果が上がっていく人材を選定して組織内の業務に充てていくという意見も聞かれました。「外部カンファレンスで発表」は、Black Hat 等のセキュリティ分野で関心が高い場で発表し、人脈作りのきっかけとするという意見でした。「資格取得、外部講習」は技術寄りの CEH、SANS といったトレーニングや、CISSP 等のガバナンス面のものも聞かれました。「語学力」は、海外とのコミュニケーションや情報収集・発信の基本として英語や中国語の必要性が挙げられた。

1.2.4.2.4 (B) セキュリティ人材 - 戦略マネジメント層

【人材像の分析】

仮説に示した人材像に対する有識者の意見は以下になりました。仮説のすべての人材像について、有識者から賛同が得られました。また、仮説には含まれていませんでしたが、有識者インタビューにて実効性のある人材像として以下が挙げられました。

仮説	有識者コメント
• OSS 利活用する上でのリスク管理や判断ができる	賛同
• ライセンスを理解し、適切な OSS の構成管理ができる	賛同

仮説	有識者コメント
• OSS 利活用における自社事業への貢献度を指標定義、評価できる	賛同
• 英語を含めた海外とのコミュニケーション能力	賛同
仮説以外で有識者が挙げた人材像	
• OSS 導入のガイドラインを策定できる • 組織リスクとコストを総合判断できる • 経営陣や技術者とコミュニケーションできるスキル • 他分野間の人材をまとめ、実務者の「意識」と「スキル」を維持できるリーダースキル • 社会人に求められるベースのスキル • 会社経営に求められることと同様のスキル	

「他分野間の人材をまとめ、実務者の「意識」と「スキル」を維持できるリーダースキル」は、例としては CSIRT と PSIRT の連携時や、PSIRT と製品開発の事業部門など、従来は別の部門で業務を行うメンバー間で連携が必要になった際に、共通のゴールにむかって協業できるようまとめ上げるスキルです。形だけの連携でなく、各メンバー間のスキルを効果的に融合させるために肝要なスキルとして意見にあがりました。「会社経営に求められることと同様のスキル」は、具体的に非テクニカルな要素としてはコミュニケーションスキル、リスク管理、内部組織の理解等、テクニカルな要素としては CISSP 程度のセキュリティ知識、COBIT の理解等で、セキュリティと経営の両方を判断基準に含めて意思決定できる人材像として挙げられました。

【育成案の分析】

仮説に示した育成案に対する有識者の意見は以下でした。「産学連携の促進」については有識者からの賛同は無く、代替としてコミュニティへの参加や外部の講習受講といった育成案が実用的という意見が得られました。また、仮説には含まれませんでしたが実効性のある人材像として、有識者から以下が挙げられました。

仮説	有識者コメント
• 業界団体への参加促進	賛同

• 産学連携の促進	賛同無し
• 語学力向上	賛同
仮説以外で有識者が挙げた育成案	
• OJT によりスキル習得 • 演習による能力向上 • マネジメント層向けの研修	

「OJT」では、組織内部をよく把握した人材と、外部のセキュリティ知識家を採用ないし協業にてお互いのスキルを補完しあいながら学んでいくという意見がありました。マネジメント層向けの研修は、スキルとして会社経営と同様のことが求められることから、経営層に向けた内容を含めた研修が挙げられました。「演習」は、知識偏重ではなく実践重視型がより効果的という意見がありました。

1.2.4.2.5 (C)　プラス・セキュリティ人材 - 実務者・技術者層

プラス・セキュリティ人材の実務者・技術者層は、事業部門、管理部門を想定します。

【人材像の分析】

仮説に示した人材像に対する有識者の意見は以下でした。「OSS のコードを理解し実装できる」について、開発者が OSS のコードを理解する必要性は低いことがインタビューにて判明しました。また、仮説には含まれなかったが、有識者インタビューにて実効性のある人材像として以下が挙げられました。

仮説	有識者コメント
• **セキュリティバイデザインに基づく設計ができる（事業部門）**	賛同
• **サポート体制活性度等、複数要因から適切な OSS を選定できる（事業部門）**	賛同
• **OSS のコードを理解し実装できる（事業部門）**	賛同なし
仮説以外で有識者が挙げた人材像	

- **バランスよくセキュリティを実装するスキルがある（事業部門）**
- **OSS 利用に際し定められたルールを理解し、遵守した実装・運用をするスキルがある（事業部門）**
- **事業に応じた適切なリスクコントロールが実行できる（事業部門・管理部門）**
- **エンドユーザとして最低限の IT スキルがある（事業部門・管理部門）**
- **各々の業務の範囲内でできるセキュリティ対応を行う（事業部門・管理部門）**

【育成案の分析】

仮説に示した育成案に対する有識者の意見は以下でした。「産学連携の促進」については有識者からの賛同は無く、代替として組織内のトレーニングや E ラーニングといった育成案が実用的という意見が得られました。また、仮説には含まれませんでしたが実効性のある人材像として、有識者から以下が挙げられました。

仮説	有識者コメント
• 業界団体への参加促進	賛同
• 産学連携の促進	賛同無し
• 資格取得の促進	賛同
仮説以外で有識者が挙げた育成案	
• OJT によりスキル習得 • セキュリティ啓発トレーニング（組織内研修、E ラーニング） • 演習による能力向上	

「セキュリティ啓発トレーニング」は、組織内やグループ共通で準備されたものや、外部の E ラーニングを利用し、組織全体のセキュリティの底上げに利用するとの意見でした。

1.2.4.2.6 (D)　プラス・セキュリティ人材 - 戦略マネジメント層

【人材像の分析】

仮説に示した人材像に対する有識者の意見は以下になりました。仮説のすべての人材像について、有識者から賛同が得られました。また、仮説には含まれませんでしたが、有識者インタビューにて実効性のある人材像として以下が挙げられました。

仮説	有識者コメント
• OSS を利活用する上でのリスク管理や判断ができる	賛同
• 調達、製造、運用後も含むサプライチェーン全体を含めた OSS の構成管理、トレースができる	賛同
• OSS 利活用における自社事業への貢献度を指標定義、評価できる	賛同
• OSS を前提とした商取引、法規を理解し、説明できる	賛同
• 英語を含めた海外とのコミュニケーション能力を持つ	賛同
仮説以外で有識者が挙げた人材像	
• 事業に応じた適切なリスクコントロールが実行できる人材（事業部門） • 顧客に説明し、理解させる交渉力をもった人材（事業部門） • 開発委託先のセキュリティを管理するスキルがある（事業部門） • エンドユーザとしての最低限の IT のスキルが必要（事業部門・管理部門） • 各々の業務の範囲内でできるセキュリティ対応を行う（事業部門・管理部門） • 会社経営に求められることと同じスキルを持つ（事業部門・管理部門）	

【育成案の分析】

仮説に示した育成案に対する有識者の意見は以下になりました。「産学連携の促進」については有識者からの賛同は無く、代替としてセキュリティ啓発トレーニングといった育成案が実用的という意見が得られました。また、仮説には含まれなかったが実効性のある人材像として、有識者から以下が挙げられました。

仮説	有識者コメント
• 業界団体への参加促進	賛同
• 産学連携の促進	賛同無し

仮説	有識者コメント
• 語学力向上	賛同
仮説以外で有識者が挙げた育成案	
• OJT によりスキル習得 • セキュリティ啓発トレーニング（組織内研修） • 演習による能力向上 • 経営層向けのマネジメントセミナー	

「演習」は、実践的な意思決定を含むプログラムが効果的という意見でした。

1.2.4.2.6.1 米国連邦政府機関の人材に求められる要素の例（参考）

有識者インタビューにて、戦略マネジメント層に必要なスキルとして米国連邦政府人事管理局(OPM) が公表する “Proficiency Levels for Leadership Competencies[23]” に記載されるコンピテンシーが参考になるという意見が得られました。同書では様々な職務毎に習熟度を 5 レベルに分けて、各レベルで求められる習熟度を具体的な例示を含めて記載しています。育成する人材の現状把握や、育成プログラムのレベルを検討する際に参考になると思われるため、「テクノロジーマネジメント」人材の部分を抜粋して紹介します。

Proficiency Levels for Leadership Competencies (OPM) からの抜粋

リーダーシップ能力の熟達度レベル

テクノロジーマネジメント：技術開発の最新動向を把握する。成果向上のために技術を効果的に利用する。技術システムへのアクセスとセキュリティを確保する		
習熟度レベル	**習熟度レベルの定義**	**習熟度レベルの例示**

23 OPM, https://www.opm.gov/policy-data-oversight/assessment-and-selection/reference-materials/proficiencylevelsleadershipcomp.pdf (2021/3 月時点で確認済み)

レベル 5- Expert	• 例外的に困難な状況下でのコンピテンシーを活用する • 重要な情報源としての役割を果たし、他の人にアドバイスをする	• 政府機関の情報技術（IT）アプリケーションおよびシステムに対する投資の優先順位付けと承認を行う • IT システムの欠点を特定し、選択肢を調査し、新しいシステムを導入するためのプロセスの再設計と再構築を提唱する • IT の専門知識を活用し、スタッフと情報を共有することで、インフラの改革や革新的な IT 業務
レベル 4- Advanced	• かなり困難な状況でコンピテンシーを活用する • 一般的に指導はほとんど必要ない	• オンライン調査や関連 IT ツールを利用して、利害関係者からのデータを収集することで、政府機関の行動能力を向上させる • 既存の IT アプリケーションをクライアントやスタッフが利用できるように拡張することで、政府機関の生産性を向上させる
レベル 3- Intermediate	• 困難な状況でコンピテンシーを活用する • 時々、指導が必要	• IT システムの技術的な知識を応用して、システムへのアクセスとセキュリティを確保する • IT の知識を活用して、全国的なデータ収集プロセスを合理化し、アウトプットを増加させる • コスト計算のための自動化されたシステムの計算式を開発する • 政府機関内の新しい電子処理システムの導入を管理する
レベル 2- Basic	• 多少困難な状況でコンピテンシーを活用する • 頻繁な指導が必要	• 新しい法的義務の要件を満たすために、請負業者と協力して、IT システムの変更を実装する • 特定のプログラムのニーズを満たすために、情報技術システムを研究する • 新しい技術開発に合わせて、プロセスを適応させる
レベル 1- Awareness	• 最も単純な状況でコンピテンシーを活用する • 詳細な指導が必要	• 新技術システムの仕様を決定する • オンライントレーニングを効率化し、冗長な情報を排除する • IT セキュリティ情報を発信し、強化することで、IT セキュリティを推進する

2. 2.研究発表・講演、文献、特許等の状況

(1) 研究発表・講演

なし

(2) 論文

なし

(3) 特許等（知財）

なし

(4) 受賞実績

なし

(5) 成果普及の努力（プレス発表等）

なし

契約管理番号：	20002280-0