PSIRT構築と運用をサポートする日立のセキュリティソリューション

昨今のIoT機器に対するサイバー攻撃の増加を受け，機器の開発・製造企業では製品のライフサイクル全体にわたるセキュリティ対応を担うPSIRTの整備が求められているが，セキュリティの専門知識を持つ人財の不足などにより自社のみでの体制構築・運用が困難なケースが多い。
日立が提供するPSIRTソリューションは，ITベンダーとして多岐にわたるソリューションを提供してきた経験と，製造業としてセキュリティ組織構築・ガバナンス整備を行ってきた実績・ノウハウを活用し，顧客のPSIRT構築から運用までをサポートする。
本稿では，製品セキュリティの担保に向けた日立の取り組みと，対応ソリューションについて紹介する。

鈴木 篤 | Suzuki Atsushi
松井 裕介 | Matsui Yusuke

1. はじめに

インターネットにつながる家電製品やコネクテッドカーの普及に伴い，オープンソースなどを組み込むIoT（Internet of Things）機器を狙ったサイバー攻撃のリスクが増加している。

例えば，米国のある自動車メーカーではブレーキやエンジン，ドアの解錠・施錠などの遠隔操作が可能となりうる脆弱性が，医療用ペースメーカーの分野では心拍の誤作動を起こさせる脆弱性が指摘されるなど，メーカーに多大な影響を与える脆弱性が数多く見つかっている。

また，こうした背景に加えて，製品・サービスのセキュリティ確保に向けたグローバルなセキュリティ法規への対応が求められており，企業には自社の製品・サービスの脆弱性や，セキュリティインシデントについて，原因究明や対処，情報公開などを迅速に行う体制の整備が強く求められている。

そこで注目されているのがPSIRT（Product Security Incident Response Team）である。CSIRT（Computer Security Incident Response Team）がサイバー攻撃に対応する社内体制・組織であるのに対し，PSIRTは自社製品に関連したセキュリティインシデントに対応する社内体制・組織である。

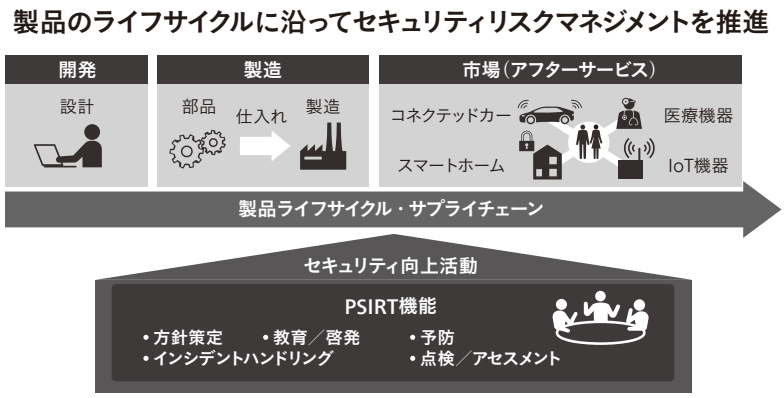
PSIRTの役割は，開発，製造，市場（アフターサービス）といった製品ライフサイクル，サプライチェーンに沿って，セキュリティリスクマネジメントを推進し，また，出荷済みの製品にインシデントが発生した場合に，被害と影響を最小限に抑えることにある（**図1**参照）。

2. 日立の取り組み

日立は1998年よりPSIRT活動の体制を構築し，自社製品・サービスの脆弱性への対応および製品・サービスの

図1｜PSIRTおよび製品ライフサイクル

製品の開発，製造，市場（アフターサービス）のライフサイクル全体に対してセキュリティリスクマネジメントを推進する。



注：略語説明
IoT（Internet of Things），PSIRT（Product Security Incident Response Team）

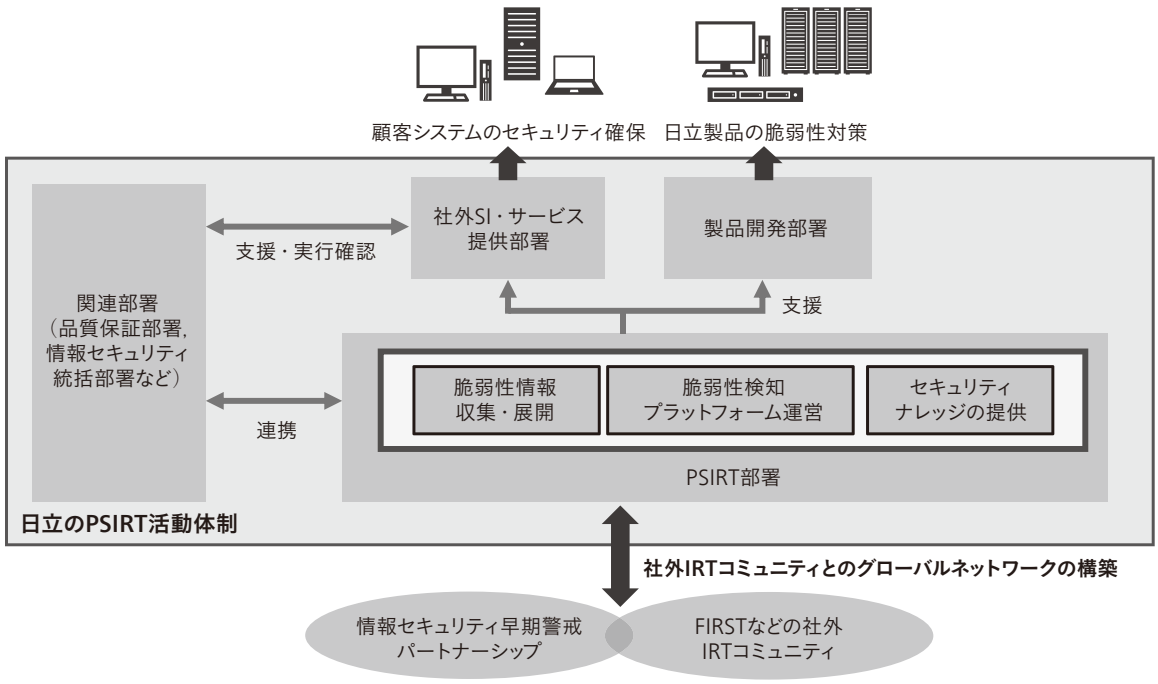
セキュリティ品質管理・向上に向けた活動を推進している。

2.1 PSIRT活動における体制

PSIRT活動は，製品・サービスを提供する製品開発部署と，顧客向けSI（System Integration）・サービス提供部署およびその活動を支援するPSIRT部署，品質保証部署，情報セキュリティ統括部署などの関連部署が連携・協力して推進している。製品開発部署とSI・サービス提供部署が製品・サービスへのセキュリティの作り込み，公開された脆弱性への対処やインシデント対応を実施する。PSIRT部署はPSIRT活動において主に技術面での活動を取りまとめ，関連部署と連携・協力してナレッジ提供や各セキュリティ強化施策などの展開を行っている（**図2**参照）。

図2｜PSIRT活動体制の概要

社外SI・サービス提供部署，製品開発部署およびPSIRT部署や関連部署が連携・協力し，PSIRT活動を推進する。



注：略語説明
FIRST（Forum of Incident Response and Security Teams），SI（System Integration），IRT（Incident Response Team）

2.2
PSIRTの活動概要

製品開発部署とSI・サービス提供部署の支援において，PSIRT部署は「セキュリティ脅威への事前対処」と「サイバー攻撃に対する耐性の強化」の二つの活動を推進している。それぞれの活動概要を以下に紹介する。

(1) セキュリティ脅威への事前対処

本活動では，主に脆弱性情報の収集・調査分析・展開を行っている。脆弱性情報の収集においては，製品ベンダーが公開した情報の収集だけでなく，情報セキュリティ早期警戒パートナーシップ※) の推進や社外IRT（Incident Response Team）コミュニティとの連携を通じ，広く自社製品・サービスに関する脆弱性情報を収集し，組織内に展開している。また，製品・サービスに含まれる脆弱性の早期検知のための仕組み（脆弱性検知プラットフォーム）を運営し，社内展開も実施している。各製品・サービスには，多くのOSS（Open Source Software）やソフトウェアが利用されている。それぞれのOSS・ソフトウェアの脆弱性情報について管理し，製品・サービスがその影響を受けるかどうかを判断することには，かなりの手間を伴う。脆弱性検知プラットフォームは，脆弱性情報と製品・サービスのOSS・ソフトウェア構成情報を一元管理するプラットフォームである。脆弱性情報とOSS・ソフトウェア構成情報をひも付けて管理し，製品・サービスを構成するソフトウェアが当該脆弱性の影響を受ける場合には，製品・サービスの担当者へ通知を行い，対処を促している。

(2) サイバー攻撃に対する耐性の強化

本活動では，製品・サービスのセキュリティを作り込むためにセキュリティナレッジの整備を行っている。クラウドネイティブ，AI（Artificial Intelligence）の普及や高度化するサイバー攻撃など事業環境が変化する中で，耐性強化を目的とし，国際基準・規格や社外ナレッジ，社内事例から得られた情報を開発担当者が活用しやすいようにガイドやチェックリストとしてまとめ，社内に展開している。

※）ソフトウェア製品やウェブアプリケーションに関する脆弱性関連情報の円滑な流通および対策の普及を図るための公的ルールに基づく官民連携体制。

3. PSIRTソリューション

本章では，ITベンダーとしてのソリューション提供の実績，および製造業としてのセキュリティ組織構築・ガバナンス整備のノウハウを活用した「日立PSIRTソリューション」について述べる。

日立PSIRTソリューションの全体像を**図3**に示す。大きく「コンサルティングソリューション」，「プラットフォーム・運用ソリューション」の2分類があり，本章では分類ごとにソリューションの概要について述べる。また，それぞれのソリューションについて顧客への適用事例も紹介する。

3.1
コンサルティングソリューション

(1) ソリューション概要

顧客企業のガバナンス強化のためのPSIRT運営を，ワンストップで支援するコンサルティングサービスを提供する。

まず「PSIRT構築・構想策定」では，迅速なPSIRT構築に向けて，現状分析，体制構築，プロセス整備，文書化の4ステップを支援する。日立のITおよび製品制御系

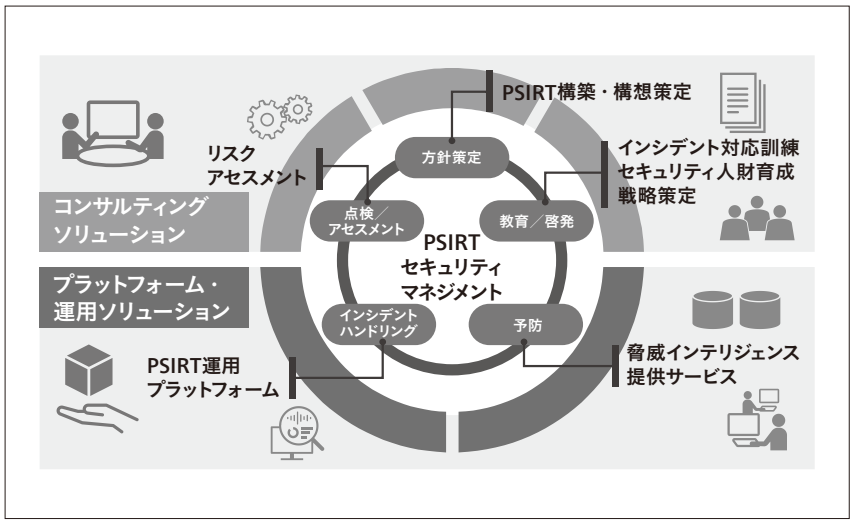


図3｜日立PSIRTソリューション概要

顧客企業のガバナンス強化を目的とした「コンサルティングソリューション」と，顧客の運用負荷軽減，インシデント対応の迅速化・属人性排除を目的とした「プラットフォーム・運用ソリューション」を提供している。

分野での豊富なCSIRT・PSIRT構築実績に基づいたテンプレートや，自社PSIRTの社内外ステークホルダーとの連携といった活動実績を用い，実効性のあるPSIRT組織を構築するほか，国際標準規格に基づいた定量的な評価指標CVSS（Common Vulnerability Scoring System）を活用した事象分析を支援する。

「インシデント対応訓練」では，顧客組織・製品に応じた訓練シナリオを策定し，机上でのインシデント対応訓練を実施する。関係部門担当者の意識向上，訓練対象部門が使用する既存の業務フローや手順書に対するボトルネックなどを特定し，課題抽出や改善提案・見直しなどを支援する。

「リスクアセスメントサービス」では，顧客企業の製品・サービスに対して，5W（What, Where, When, Who, Why）法やSTRIDE［Spoofing（なりすまし），Tampering（改竄），Repudiation（否認），Information disclosure（情報の漏洩），Denial of service（DoS攻撃），Elevation of privilege（権限昇格）］などの手法を活用した網羅的な脅威の抽出と定量的なリスク評価を実施する。抽出された脅威に対し，効果的なセキュリティ対策とスケジュールを決定する。

（2）提供事例

「PSIRT構築・構想策定」の提供事例を**図4**に示す。

本案件では，顧客の国際法規対応に向け，FIRST（Forum of Incident Response and Security Teams）が提供するPSIRT Frameworkを活用しPSIRT構築を支援した。顧客組織の現状を把握したうえでPSIRTの目的や役割を定義し，顧客の中でPSIRTとして行うべきミッションを明確化した。また業務フローを定義し，ステークホルダーの整理や，実行にあたって必要な体制の整備，各種手順書の整備を行った。

3.2 プラットフォーム・運用ソリューション

（1）ソリューション概要

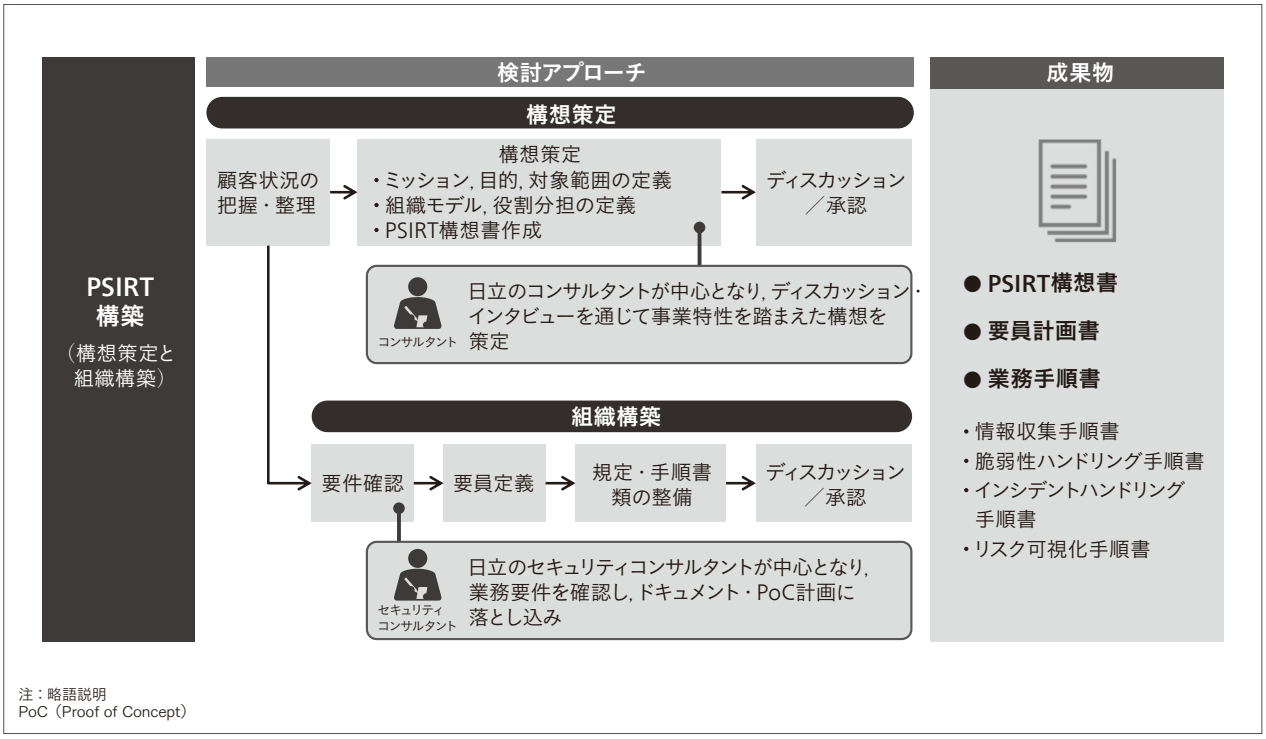
PSIRTの運用領域において，脅威・脆弱性情報の分析・一元管理の仕組みを提供する。また，顧客の運用負荷軽減，インシデント対処の迅速化・属人性排除を実現する。

「脅威インテリジェンス提供サービス」では，情報の収集・仕分け，影響分析など，専門性の高いPSIRT業務を日立がアウトソーシングサービスとして請け負い，顧客の業界や製品，サービスに関連する脅威・脆弱性情報を選別し，製品への影響を評価する。

また「インシデント対処サービス」では，脅威・脆弱性情報と製品構成情報を一元管理するプラットフォームを提供することで一部業務の自動化を実現する。運用負荷の軽減に加え，インシデント対処の迅速化・確実性向上を支援する。

図4｜PSIRT構想策定の適用事例

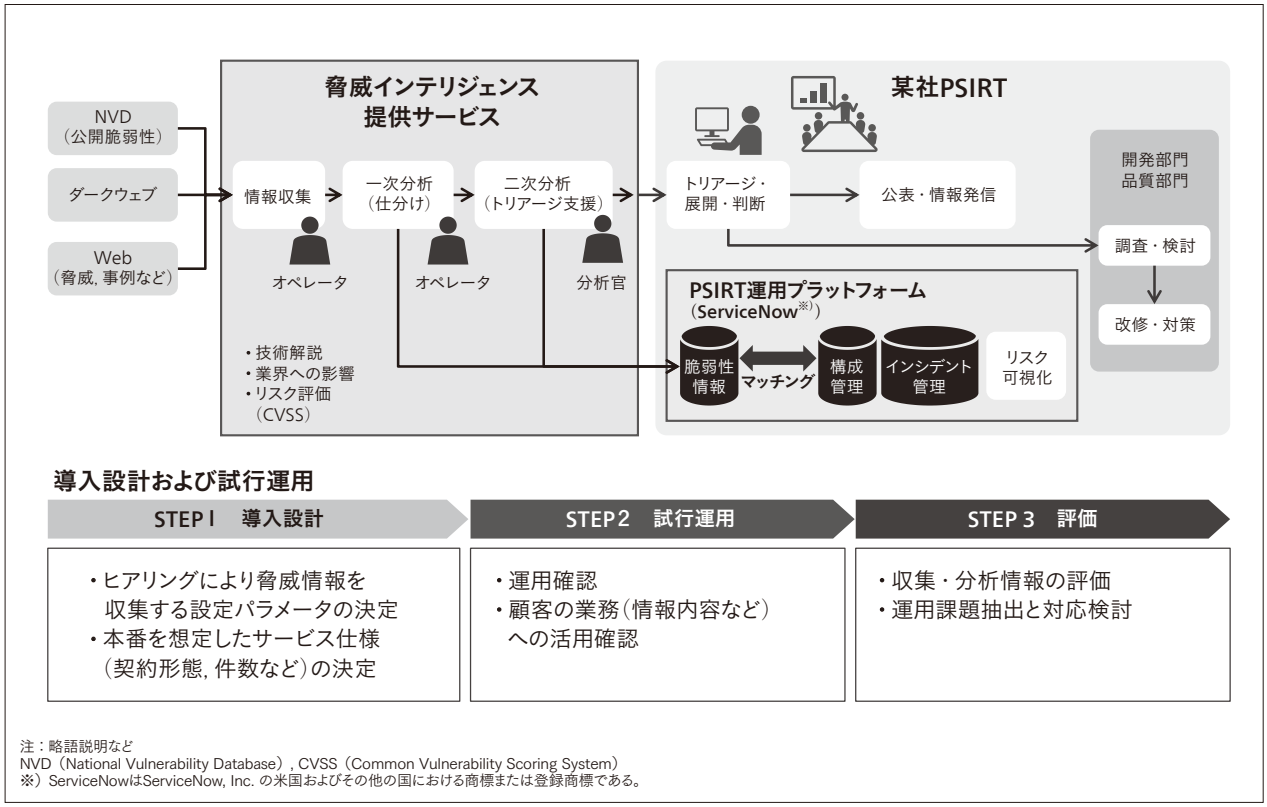
顧客のPSIRT立ち上げに向け，現状把握結果を基にあるべき姿を検討し，組織の構想書や各種業務の手順書の作成を支援する。



注：略語説明
PoC（Proof of Concept）

図5｜脅威インテリジェンス提供サービス・運用プラットフォームの適用事例

顧客のPSIRTの情報収集・仕分け業務をアウトソーシング化し，収集情報に対して技術解説などをレポートとして提供する。



注：略語説明など
NVD（National Vulnerability Database）, CVSS（Common Vulnerability Scoring System）
※）ServiceNowはServiceNow, Inc. の米国およびその他の国における商標または登録商標である。

（2）提供事例

プラットフォーム・運用ソリューションの提供事例を**図5**に示す。

本案件では，某製造業の顧客が持つPSIRTに対して脅威インテリジェンス提供サービスを実施している。本サービスの情報収集ツールを活用し，公開脆弱性情報，ダークウェブ上に出回る未公開の脅威・脆弱性に関する情報などを収集し，顧客企業や製品に関連の深い情報を提供する。日立の分析官が対象の情報に関する分析レポートを作成し，週次で提供している。

4. おわりに

本稿では，製品のIoT化・コネクテッド化に伴って増大する脅威へのセキュリティ対策について，日立自身の取り組みおよび顧客への提供ソリューションについて述べた。

今後は，PSIRT運用の高度化・自動化をキーワードに，製品への攻撃などをリアルタイムに監視・対処するPSOC（Product Security Operation Center），セキュリティインシデントの監視・意思決定などを共通プラットフォーム上で効率的に行うSOAR（Security Orchestration, Automation and Response）など提供ソリューションの拡張を進めていく。

執筆者紹介

鈴木 篤
日立製作所 サービス＆プラットフォームビジネスユニット
IoT・クラウドサービス事業部 エンジニアリングサービス第1本部
インテグレーション＆サービス第3部 所属
現在，製造業向けのセキュリティコンサルタントに従事

松井 裕介
日立製作所 サービス＆プラットフォームビジネスユニット
IoT・クラウドサービス事業部 サイバーセキュリティ技術本部
セキュリティテクニカルセンタ 所属
現在，製品・サービスのセキュリティ確保に向けた施策立案に従事