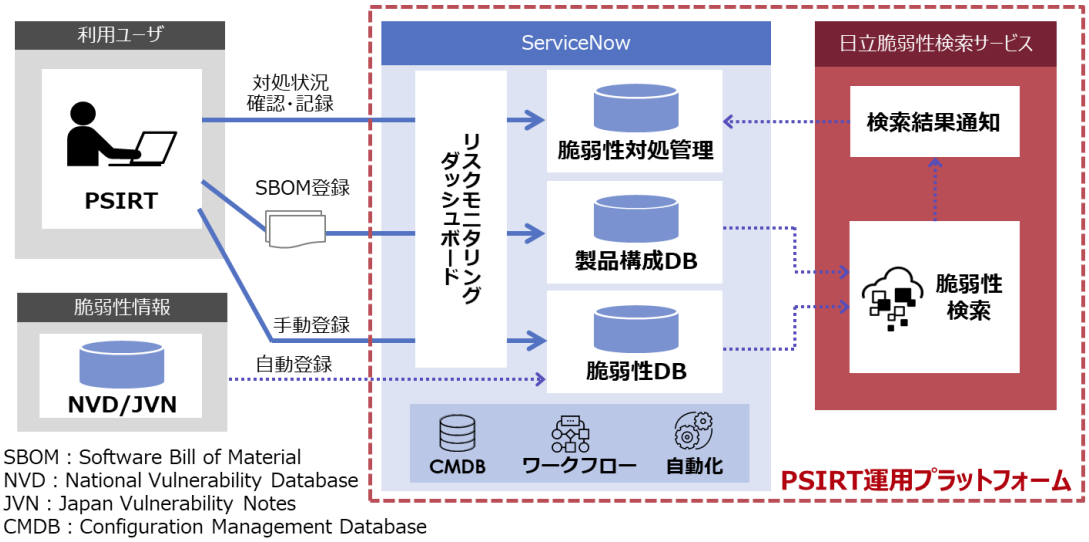
2022 年 3 月 22 日
株式会社日立製作所
ServiceNow Japan 合同会社

製造業向けサイバー攻撃や製品セキュリティの向上対策で 日立と ServiceNow Japan が協創

製品の脆弱性を早期に発見・対策を可能にする PSIRT 運用プラットフォームを提供開始



PSIRT 運用プラットフォームのイメージ

日立製作所(以下、日立)と ServiceNow Japan 合同会社(以下、ServiceNow Japan)は、製造業を中心に世界的な社会課題となっているサイバー攻撃への対策や製品セキュリティ向上に向け、PSIRT[*1] の分野で協業を開始しました。具体的には、ServiceNow の Security Operations[*2] と日立の脆弱性情報のあいまい検索[*3] を可能とする脆弱性検索サービスを組み合わせて、製造業における効率的かつ迅速な製品セキュリティ対策を可能にする PSIRT 運用プラットフォームを開発し、本日より提供開始します。

日立と ServiceNow Japan は、本発表に先立ち、大手製造業のお客さまに本プラットフォームを導入・運用開始しており、月数万件にもおよぶセキュリティインシデントの管理・対策業務の負荷を軽減し、製品出荷後だけでなく、製品の企画から開発など出荷前の段階から、迅速かつ適切な対応を行うことに貢献しています。

*1 PSIRT：Product Security Incident Response Team のこと。製品セキュリティの対応組織を指す。開発、製造、アフターサービスの製品ライフサイクルにあわせてセキュリティのリスクマネジメントを推進し、製品にインシデントが発生した場合は、被害と影響を最小限に抑えることが役割。

*2 ServiceNow の Security Operations：既存のセキュリティツールを一元管理し、脆弱性やセキュリティインシデントをリスク重大度に応じて優先順位をつけ、迅速に対応をおこなう SOAR(Security Orchestration, Automation, and Response)ソリューション

*3 あいまい検索：検索するキーワードと完全に一致していなくても、表記の異なりや同義語も含め柔軟に解釈して検索できる機能

■協業の背景について

現在、製造業において製品の IoT 化や業務プロセスのデジタル化など DX(デジタルトランスフォーメーション)に向けた取り組みが加速しています。一方で、インターネットにつながる IoT 製品を狙ったサイバー攻撃の範囲と規模は拡大しています。IoT 技術は IC チップや組み込み機器などさまざまな形態で数多くの製品に実装されているため、セキュリティインシデントが与える影響は、社会や企業経営に甚大なリスクを与えかねません。そのため、製品の企画から開発、販売、運用、保守、廃棄までの製品ライフサイクル全体を通じ、サイバーレジリエンス(セキュリティインシデントの影響を最小限に留め、迅速に元の状態に復旧する仕組み)を強化することが求められています。その実現のためには、製品のソフトウェア構成を示す SBOM(ソフトウェア部品表)や公開されている脆弱性情報などの製品セキュリティに関わる情報を一元管理し、早期かつ組織横断的に共有・対策を行うためのデータマネジメント基盤が必要です。

今回、この社会課題の解決に向け、日立の長年のセキュリティ対策で培ってきたデジタル技術と、ServiceNow の組織横断型で情報やデータを連携するデジタルワークフローや見える化を実現するソリューションなど両社の強みを組み合わせることで、PSIRT 運用プラットフォームを開発しました。

■PSIRT 運用プラットフォームの特長について

１．増大する脆弱性情報の収集と製品情報の管理

製品セキュリティにおいて、脆弱性情報(NVD[*4] や JVN[*5] などのデータベースで公開される脆弱性情報)の収集や管理は、製品のソフトウェア構成の増大と複雑化により管理が困難となっています。特に、公開されている脆弱性情報は表記に揺らぎがあり、製品情報との照合を手作業による分析で多大な時間を要することから、結果として自社製品への影響把握に時間がかかってしまいます。

PSIRT 運用プラットフォームは、日立独自の脆弱性検索サービスのあいまい検索を用いることで表記揺れのパターンを解析するとともに、より高い精度で脆弱性情報や製品情報を照合することが可能となり、管理業務の省力化を実現します。両社で実施した PoC[*6] では、脆弱性情報収集および確認にかかる時間を約 70%削減する効果を確認しました。

２．脆弱性対応時間を短縮するワークフロー

脆弱性情報や製品情報は ServiceNow の Security Operations 上で一元管理されます。セキュリティ対策が必要な製品が検出された場合、自動的にインシデントを起票し、設計・開発・品質管理部門など関連部署に調査・対応の依頼を展開することができます。脆弱性に関わる基本情報に加え、リスクスコアがついた状態で依頼が通知されるため、担当部署では優先度に応じて効率的な調査・対策の業務を進めることができます。また、深刻な脆弱性が検出された際に対応が遅れた場合などは、催促メールの自動通知など対策を確実に進めるためのワークフローも提供されます。

3．リアルタイムで把握できるリスクモニタリングダッシュボード

セキュリティ運用にかかる脆弱性情報・インシデント情報・製品情報が PSIRT 運用プラットフォームに一元管理されることで、リアルタイムにセキュリティ運用状況を可視化し、把握することができます。時系列での脆弱性調査状況や、部署・脆弱性・製品ごとの傾向も可視化することで、ビジネスに影響するリスクの早期把握も実現することができます。

*4 NVD:National Vulnerability Database のこと。アメリカ国立標準技術研究所が管理している脆弱性情報データベース

*5 JVN: Japan Vulnerability Notes のこと。一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)と情報処理推進機構(IPA)が共同で管理している脆弱性情報データベース

*6 PoC：Proof of Concept

■今後の展開

日立と ServiceNow Japan は、PSIRT 業務の知見やノウハウを蓄積しながら、PSIRT 運用プラットフォームの強化を進め、製造業を中心に広く提供していきます。また、セキュリティ対策のノウハウや最新の業界動向などを共有しながら、それぞれの事業で、社会や企業のセキュリティ対応の課題を解決し、安全・安心な社会の実現に貢献していきます。

■価格および提供開始時期

名称	内容	価格	提供開始時期
PSIRT 運用プラットフォーム	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の提供により、 業務の効率化を実現	個別見積	2022 年 3 月

■関連リンク

日立のプロダクトセキュリティについて
https://www.hitachi.co.jp/products/it/security/solution/cyber-security/productsecurity/index.html

ServiceNow の Security Operations について
https://www.servicenow.co.jp/products/security-operations.html

■日立製作所について

日立は、データとテクノロジーで社会インフラを革新する社会イノベーション事業を通じて、人々が幸せで豊かに暮らすことができる持続可能な社会の実現に貢献します。「環境(地球環境の保全)」「レジリエンス(企業の事業継続性や社会インフラの強靭さ)」「安心・安全(一人ひとりの健康で快適な生活)」に注力しています。IT・エネルギー・インダストリー・モビリティ・ライフ・オートモティブシステムの 6 分野で、OT、IT およびプロダクトを活用する Lumada ソリューションを提供し、お客さまや社会の課題を解決します。2020 年度(2021 年 3 月期)の連結売上収益は 8 兆 7,291 億円、2021 年 3 月末時点で連結子会社は 871 社、全世界で約 35 万人の従業員を擁しています。

詳しくは、日立のウェブサイト(https://www.hitachi.co.jp/)をご覧ください。

■ServiceNow について

ServiceNow(NYSE ： NOW)は、人にしか出来ない、付加価値の高い新しい仕事を創造します。当社のクラウド型プラットフォームとソリューションは、従業員と企業双方に優れたエクスペリエンスを生み出し、生産性を高めるデジタルワークフローを提供します。

詳細はこちらをご参照ください。
https://www.servicenow.co.jp/

■商標表記

■お問い合わせ先

株式会社日立製作所 サービスプラットフォーム事業本部 IoT・クラウドサービス事業部
お問い合わせフォーム：http://www.hitachi.co.jp/it-pf/inq/NR/

以上