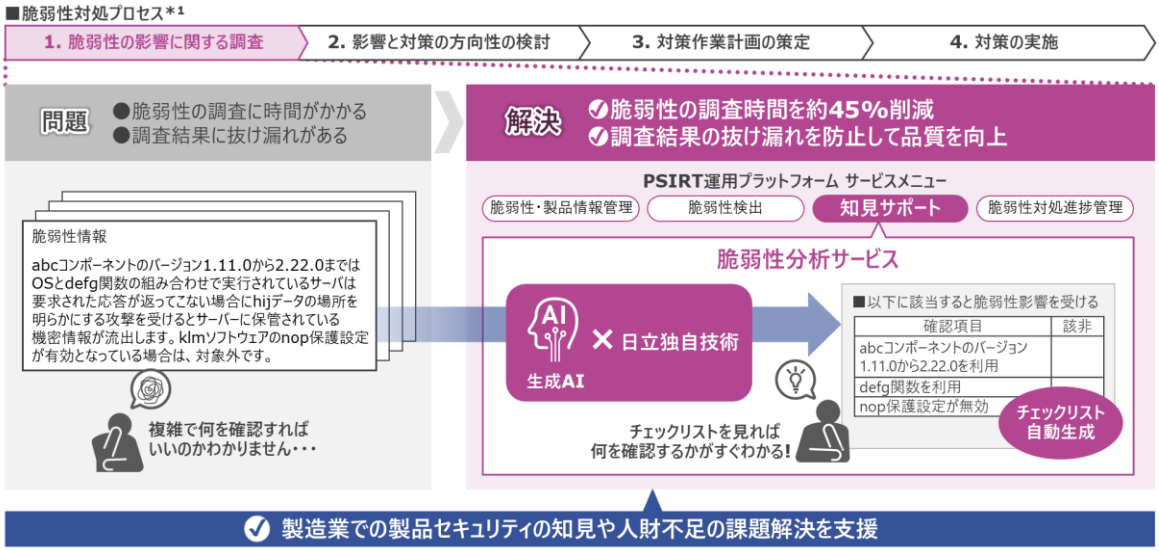
お知らせ

2025 年 3 月 5 日

IoT 製品・システムの脆弱性対処に必要なセキュリティの知見を補う、生成 AI を活用した「脆弱性分析サービス」を販売開始し、PSIRT ソリューションを強化

脆弱性の調査時間を約 45%削減し、セキュリティの知見や人財不足の課題を解決



「脆弱性分析サービス」の概要

株式会社日立製作所(以下、日立)は、IoT 製品・システムなどの製品セキュリティにおける脆弱性対処に必要な知見を補う、生成 AI を活用した「脆弱性分析サービス」(以下：本サービス)を、2025 年 3 月 5 日から販売開始し、PSIRT ソリューション*2,3 を強化します。本サービスは、サイバーレジリエンス法(CRA*4)などの法規への対応を背景に、製品セキュリティの強化や PSIRT の設置・取り組みを検討している製造業のお客さまを中心に提供します。

本サービスは、生成 AI を活用して、理解にセキュリティの専門的知見が必要な脆弱性情報を解析し、製品が脆弱性の影響を受ける条件だけをチェックリストとして提供します*5。これにより、製品の設計書やソースコードから製品が脆弱性の影響を受けるかどうかを調査するために必要な知見を補い、製品セキュリティの知見や人財不足の課題解決を支援します。

本サービスの活用により、従来時間がかかっていた人手による脆弱性の影響を受ける条件の整理が不要となり、調査にかかる時間を、約 45%削減*6 できます。チェックリストは自動で生成されるため、製品担当者の知見に左右されない調査ができ、脆弱性対処の品質向上も可能です。

近年、IoT 製品の脆弱性を狙ったサイバー攻撃の増加や関連する法規の整備により、製造業各社は自社の製品やサービスに含まれる脆弱性に迅速かつ確実に対処することが一層求められています。脆弱性対処において、製品担当者が、脆弱性情報から製品が脆弱性の影響を受ける条件を整理し、製品の設計書やソースコードをもとに、自社製品がそれらの条件に当てはまるかを確認するといった、脆弱性の影響に関する調査が必要です。しかし、多くの製造業では、製品セキュリティの知見や人財の不足が顕著であり、調

査の経験が浅い担当者にとっては脆弱性情報の理解自体が難しく調査に時間がかかるほか、調査結果に抜け漏れが発生し、組織全体としてリスクが高まる可能性があります。

これまで日立は、脆弱性情報と製品構成情報の一元管理など脆弱性対処を支援する機能を搭載した PSIRT 運用プラットフォームを提供していました。本サービスの追加により、特に製品セキュリティの知見・人財が不足しているお客さまに対してより効率的かつ高品質での脆弱性対処が可能になります。

日立は、本サービスによりお客さまの製品セキュリティの知見・人財不足の課題へもアプローチし、製造業各社への PSIRT 運用プラットフォームの展開を加速していきます。また、製造業のお客さまのセキュリティに関するさまざまな課題解決に向けて、IT×OT×プロダクトの知見や実績を生かしたコンサルティングや SI など、幅広いサービスも提供していきます。

*1 脆弱性対処プロセスは、IPA「セキュリティ担当者のための脆弱性対応ガイド」(2017)を参考。脆弱性の影響に関する調査はセキュリティ上の問題の有無に関する調査に該当。

*2 PSIRT：Product Security Incident Response Teamの略。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、被害と影響を最小限に抑えることが役割。

*3 PSIRTソリューション：日立が提供する、お客さまの製品セキュリティに関する課題を支援するトータルソリューション。お客さまのPSIRTの構築・構想策定や、教育、訓練などを行うコンサルティングソリューションから脅威の分析や脆弱性・サイバー攻撃監視などPSIRTの運用を支援する運用ソリューションを含む。

*4 CRA：Cyber Resilience Actのこと。欧州に事業展開する製品の製造者に対して、開発、製造、アフターサービスの製品ライフサイクル全体でセキュリティ要件の達成かつ事実上のPSIRT組成が求められる。

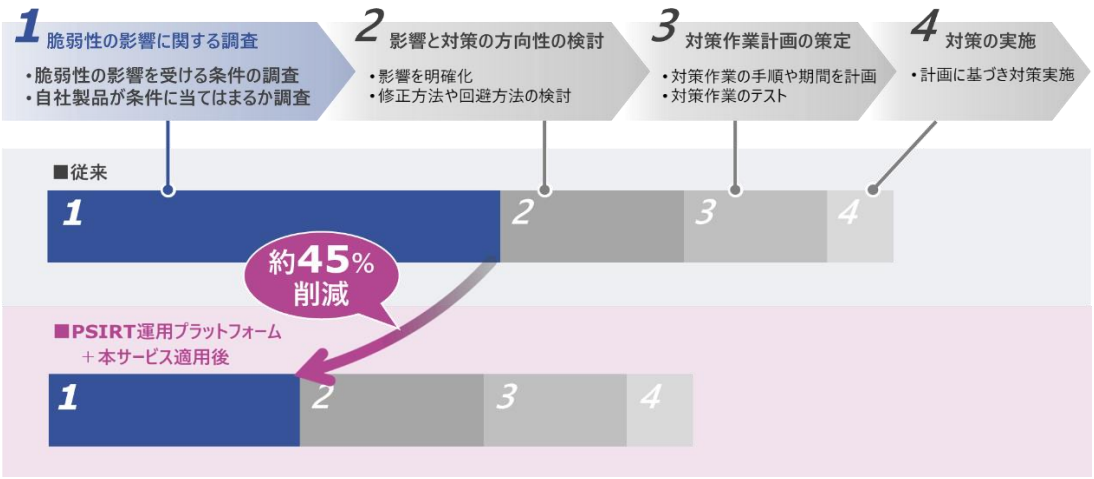
*5 特許出願中。なお、特許に関する表記は、2025年3月現在のものです。

*6 製造業の企業において脆弱性情報の収集をPSIRT部門が実施し、脆弱性対処を製品担当者が手動で実施した場合の、脆弱性の影響の調査にかかる実測時間(PSIRT運用プラットフォーム利用なし)と、当該企業にPSIRT運用プラットフォームおよび本サービスを適用した場合の当該作業時間を日立社内で見積もった値との比較。

■本サービスの特長

１．脆弱性の影響に関する調査時間を約 45％削減、効率的な脆弱性対処が可能

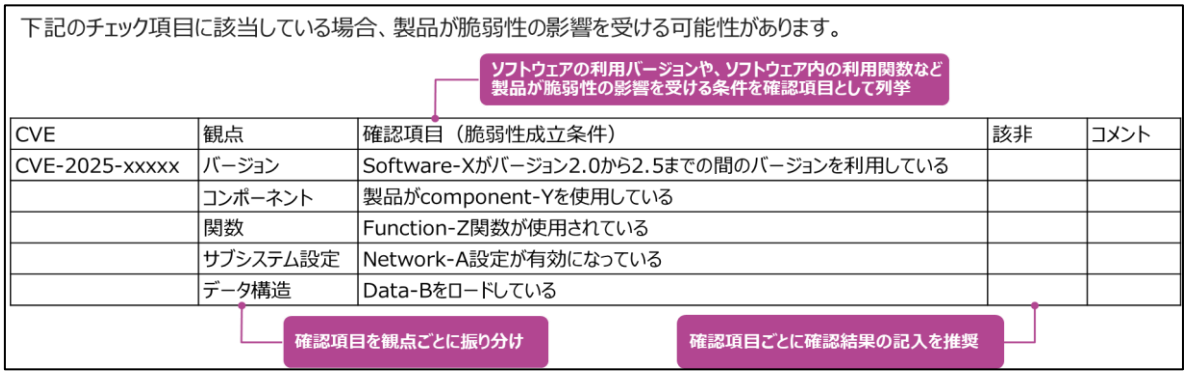
セキュリティの知見が不足している担当者が、これまで多くの作業時間を要していた製品が脆弱性の影響を受ける条件の調査を、チェックリストの確認のみで行えるため、作業時間が短縮できます。また、チェックリストに出力される条件のうち、製品に含まれるソフトウェア名やコンポーネント名、バージョン情報などは、PSIRT 運用プラットフォームで一元管理されているので、条件に当てはまるかを容易に調査できます。結果として、脆弱性の影響に関する調査にかかる時間を約 45%削減することが可能となり、担当者の知見が不足していても、効率的な脆弱性対処が実現できます。



本サービス適用による脆弱性対処にかかる時間の削減効果の例

２．チェックリストの活用により抜け漏れを防止し、脆弱性対処の品質を向上

チェックリストを活用することで、脆弱性の影響に関する調査の抜け漏れを防止し、セキュリティの知見が少ない人でも知見がある人と同等の品質での調査が可能となります。これにより、知見や人財が不足している組織でも脆弱性対処の品質の向上が図れます。また、チェックリストは調査を網羅的に行っていることを示すエビデンスとしても活用できます。



自動生成するチェックリストのイメージ

■本サービスでの生成 AI 活用効果について

脆弱性情報は、専門用語や技術的な情報が多用されており、製品が脆弱性の影響を受ける条件だけでなく、考えられる攻撃手法や悪用された際の被害、脆弱性の対象外となる条件なども混在して記述されています。本サービスは、生成 AI に日立独自のプロンプトエンジニアリング[*7]を適用することで、生成 AI が、脆弱性の影響を受ける条件だけを効率的に抽出してチェックリスト化しています。

*7　プロンプトエンジニアリング：生成AIが目的に合ったアウトプットを出力するような命令文を作成・開発する技術のこと。

■サービスの価格および提供開始時期

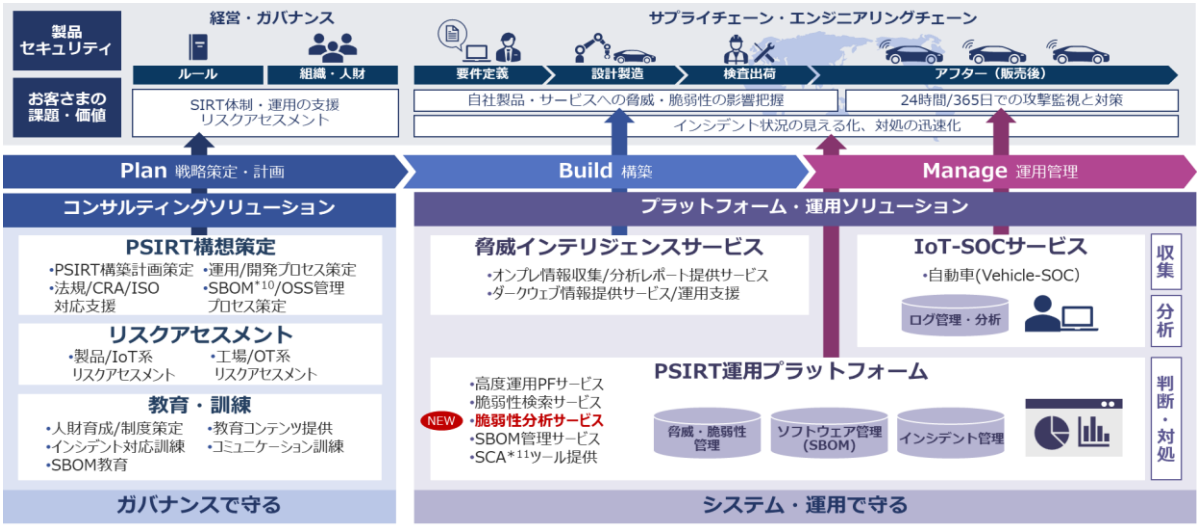
名称		概要	価格(税別)	提供開始時期
PSIRT 運用プラットフォーム		脆弱性情報と製品構成情報を一元管理するプラットフォームの提供により、業務の効率化を実現	個別見積	提供済
	脆弱性分析サービス (オプション)	公開されている脆弱性情報からお客さまの製品・システムが、脆弱性の影響を受ける条件を自動で抽出し、チェックリスト形式で提供。脆弱性対処における製品セキュリティの知見・人財不足の課題解決を支援	個別見積	2025 年 7 月*8

*8　・本サービスの利用は PSIRT 運用プラットフォームの構築が必須のため、PSIRT 運用プラットフォームの構築期間を含みます。
・PSIRT 運用プラットフォームへの個別カスタマイズは行わない前提です。

■日立 PSIRT ソリューションおよびサイバーセキュリティの取り組みについて

日立は、お客さまの PSIRT の構築・構想策定や、教育、訓練などを行うコンサルティングソリューションと、脅威の分析や脆弱性・サイバー攻撃監視といった PSIRT の運用を支援するプラットフォーム・運用ソリューションを提供しており、日々発生するセキュリティ確保のための対応をトータルに支援することが可能です。日立は、製造業として 2004 年からサイバーセキュリティ対策を行う組織として HIRT(Hitachi Incident Response Team)を立ち上げました。その活動の一つとして、同業種での脅威情報を共有する ISAC*9 の活動などで情報収集しながら、日立グループの情報システムおよび制御システム関連製品における脆弱性対策やインシデント対応を推進してきました。このような実績・ノウハウを生かし、お客さまの安全・安心な経営環境の確保および企業価値向上に貢献していきます。

*9　ISAC: Information Sharing and Analysis Center(同じ業界の民間事業者同士でサイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることをめざして活動する民間組織)



日立 PSIRT ソリューション

*10　SBOM：Software Bill of Materials のこと。ソフトウェアを構成するコンポーネントの一覧のことで、ソフトウェア部品表やソフトウェア構成表とも呼ばれる。

*11　SCA：Software Composition Analysis のこと。コードベースをスキャンし、包括的な SBOM を作成することで、コードベースに含まれる直接的および推移的(間接的)な依存関係やライセンスなどの一覧を提供する。

関連するウェブサイト

プロダクトセキュリティ

https://www.hitachi.co.jp/products/it/security/solution/cyber-security/productsecurity/index.html?pr=250305

■日立製作所について

日立は、データとテクノロジーでサステナブルな社会を実現する社会イノベーション事業を推進しています。お客さまの DX を支援する「デジタルシステム&サービス」、エネルギーや鉄道で脱炭素社会の実現に貢献する「グリーンエナジー&モビリティ」、幅広い産業でプロダクトをデジタルでつなぎソリューションを提供する「コネクティブインダストリーズ」という 3 セクターの事業体制のもと、IT や OT(制御・運用技術)、プロダクトを活用する Lumada ソリューションを通じてお客さまや社会の課題を解決します。デジタル、グリーン、イノベーションを原動力に、お客さまとの協創で成長をめざします。3 セクターの 2023 年度(2024 年 3 月期)売上収益は 8 兆 5,643 億円、2024 年 3 月末時点で連結子会社は 573 社、全世界で約 27 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。

■商標について

記載の会社名、製品名などは、それぞれの会社の登録商標もしくは商標です。

■お問い合わせ先

株式会社日立製作所

クラウドサービスプラットフォームビジネスユニット　マネージド＆プラットフォームサービス事業部

お問い合わせフォーム：https://www.hitachi.co.jp/it-pf/inq/NR/

以上