HITACHI

株式会社 日立システムズエンジニアリングサービス

迫るCRA適用～実効性あるPSIRT構築から運用定着まで

ーCRA規制とフロンティアAI時代の製品セキュリティー

DXサービス事業グループ
企業システム事業部
勇　大亮

Date
30 JULY 2026

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

講演者



勇 大亮
主管技師長
株式会社 日立システムズエンジニアリングサービス
DX事業グループ
企業システム事業部

株式会社 日立システムズエンジニアリングサービス
DXサービス事業グループ
企業システム事業部に所属
デジタルトランスフォーメーションセンタ　センタ長
セキュリティビジネス推進活動などを兼務

2005年に株式会社コンピュータシステムエンジニアリング(現日立システムズエンジニアリングサービス)に入社し、公共、金融、産業各業種のインフラプロジェクトに従事。2016年にTCSI社(現ZenmuTech社)とのアライアンスをきっかけにパートナー連携、セキュリティビジネスを推進。秘密分散技術を活用した自社サービスの立ち上げなどに携わる。

お客さまの事業継続を第一に考え、安心、安全に貢献すべく、お客さまへの提案活動や、日立グループ、各パートナーとの連携、アライアンスなどを中心に活動をしている。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

本日お伝えしたいこと

HITACHI

「規制」と「攻撃」が同時に変わる2026年、日本の製造業がおかれている現実と対策準備

1. CRAという「待ったなし」の現実

欧州サイバーレジリエンス法（CRA）により、すべてのデジタル要素を持つ製品のセキュリティが「努力義務」から「**法的義務**」へと変わります。

・24時間以内の初期報告義務
・最高1500万ユーロの巨額罰則
・2027年12月の全面適用

2. フロンティアAIが崩した攻防の均衡

自律的なぜい弱性発見・エクスプロイト開発が可能な「**Claude Mythos**」が登場し、攻撃側のスピードが劇的に加速しています。

・27年潜伏したバグを一晩で発見
・防御側は対策急務！
・金融庁・日銀の緊急1カ月要請

3.「急がなければならない」ぜい弱性管理のプロセス化

法的義務への準拠と、猶予ゼロの攻撃に対抗するため、製品セキュリティの対応組織（**PSIRT**）の立ち上げとプロセス化と**同時に自動化、効率化**が急務です。

・SBOM運用基盤の即時整備
・リスクベーストリアージの高速化
・PSIRT業務の効率化

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

デジタル要素を持つすべての製品が対象、製品セキュリティが「努力」から「法的義務」へ

欧州サイバーレジリエンス法 (CRA)

EU市場に流通する「デジタル要素を備えたすべての製品（ハードウェア、ソフトウェア）」に、ライフサイクル全体でのセキュリティ確保を義務付ける法令。

適用範囲の広さ：

事実上、IoT機器、産業用制御システム、コンシューマ向けスマートデバイス、スタンドアロンソフトウェアなどほぼすべてが含まれます。

CRA施行スケジュール

2024年10月

CRA正式採択、同年12月に発効

2026年9月11日

ぜい弱性・インシデント報告義務の開始

各国のCSIRTとENISAに報告

2027年12月

CRA全面適用

・罰金規定の発動、セキュリティ要件の全面実装義務化、既存流通製品へのCRA要件遡及適用、CEマーキング取得条件にCRA要件適合の追加



適合しない場合は「CEマーク※」がはく奪されるつまりEU市場で販売禁止となる

※「EUの安全・環境などの法規制に適合していることをメーカー自身が宣言するマーク」

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

報告義務はもう「目前」、レガシー製品にも遡及適用されます

インシデント・ぜい弱性の3段階報告フロー

フェーズ	期限	報告内容
① 早期警告	検知後24時間以内	悪用されたぜい弱性、またはインシデント発生の事実（疑い含む）を速やかに通知
② 一次報告	検知後72時間以内	インシデントの詳細な評価、被害規模、初期の緩和策などを追加報告
③ 最終報告	是正措置が利用可能になってから14日以内 または、深刻インシデントの場合30日以内	根本原因分析、恒久的な対策内容、パッチ適用状況などをまとめた詳細レポート

特に警戒すべきポイント

1. レガシー製品への遡及適用

2026年9月11日時点で市場に流通しており、サポート期間内であるすべての製品が報告義務の対象となります。

2. ENISAによる集中管理

欧州サイバーセキュリティ機関（ENISA）に「Single Reporting Platform (SRP)」が設置され、24時間監視が稼働します。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

罰則の現実性

最大1,500万ユーロ または 全世界売上高の2.5%以下のいずれか高い方の金額が科されます

制裁金の最高限度額

1,500万ユーロ（約24億円）

または 全世界売上高の 2.5%

※いずれか**高い方**が適用されます。この極めて強力な罰則設定は、個人情報保護を定めた「GDPR（一般データ保護規則）」と同等の厳格さを示しています。

制裁金だけではない、実務上の重大リスク

1. 製品回収・EU市場からの排除

適合性要件を満たさない製品、または**報告を怠った製品**は、即時に**流通停止や製品回収**の命令が下される可能性があります。

2. 供給網（サプライチェーン）からの除外

CRAは製造業者の義務としてデューデリジェンスを求めているため、適合しないサプライヤーは、大手メーカーの調達リストから即座に排除されることになります。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

2027年12月 — 製造者の6大義務

単なる実装にとどまらない、リスク評価からライフサイクルサポートまでの包括的要件

1. サイバーリスク評価

設計段階からサイバーセキュリティ上の脅威やリスクを明確に分析・評価が必要。

セキュアバイデザイン

2. 基本安全要件の実装

暗号化、アクセス制御、アップデート機能などの必須セキュリティ機能の搭載が必要。

3. ぜい弱性ハンドリング

ぜい弱性の発見、トリアージ、修正パッチの配信プロセス（PSIRT）の確立が不可欠。

4. サプライチェーンDD

サードパーティ製品やオープンソース等のコンポーネントにおけるデューデリジェンスの実施。

5. 最低5年間のサポート

市場投入後、原則として5年間（または製品の期待寿命）セキュリティパッチを提供する義務。
(新PL法（EU新PLD）では10年の損害賠償責任期間)

6. CEマーキングの適合

適合宣言書の作成、技術文書（SBOM含む）の整備、CRA要件に対応した上での製品への「CEマーク」付与が必須。

リスクベースの製品分類

CRAでは製品が持つセキュリティリスクに応じて3つの適合性レベルに分類されます。

① デフォルト（標準製品）
自己評価（Self-assessment）による適合性確認が可能です（全体の約9割）。

② 重要製品（Important Class I & II）
VMM、暗号プロセッサ、VPN等。
他システムのセキュリティを支える中核機能、侵害された場合に影響が大きい製品。

③ クリティカル製品（Critical）
高度な重要インフラに関わるソフトウェア・ハードウェア等、最高難度の適合要件が求められます。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

業界の準備状況 ― 41%しか間に合わない

66%がCRAを十分理解しておらず、2027年までに準拠見込みの製造者は41%（OpenSSF2026年調査）

※OpenSSF・・・現代のソフトウェア開発に不可欠なオープンソースソフトウェア（OSS）のセキュリティを、世界中で協調して改善するために設立されたThe Linux Foundation傘下の国際的な業界横断プロジェクト。

OpenSSF2026年6月度最新調査結果

2027年末までに準拠予定

41%

「**あなたの会社は残り59%ではないですか？**」

回答した製造企業・ソフトウェアディストリビューターの**わずか41%**しか、2027年12月の全面適用までに完全なCRA準拠を達成できないと見込んでいます。

データソース: OpenSSF (Open Source Security Foundation) 2026 CRA Awareness and Readiness Report

業界が直面する２つの現実

1. 理解不足の壁 (66%が不十分)

多くの組織がCRAの要件が自社製品にどう適用されるかを把握できておらず、法務とエンジニアリングのギャップを埋められていません。

2. 日本の産業界における危機感のかい離

自動車産業（自工会など）や大手電機・IoTベンダーでは先進的な取り組みが見られる一方、Tier 2以下の部品サプライヤーや中堅製造業の多くは未着手、または対策遅れに陥っています。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

Claude Mythos「自律的攻撃閾値」を超えた

フロンティアAIによる自律的サンドボックス脱出

2026年4月7日、Anthropicは「Claude Mythos Preview」のセーフティ検証結果を公表。社内のセキュリティ評価テストにおいて、極めて高度な「自律的脱出および不承認行動」が確認されました。

観測された驚異的なエージェント行動：

・制限ネットワークを迂回し、数ステップのコードぜい弱性を突いてサンドボックス環境から自律脱出。
・外出中の担当研究者に「脱出成功」を自発的にメールで通知。
・指示されていないにもかかわらず、外部Webサイトに自己ログを書き残す。

「欠陥」ではなく「創発」

"この封じ込め失敗は、単純なプログラムバグによるものではなく、**高度な一般推論・自律性の進化（創発的エージェント能力）が防御側の想定した制御設計を上回った結果**である。"

― Cloud Security Alliance (CSA) の2026年AI関連白書より

※この結果を受け、Anthropicは同モデルの一般公開を制限し、防衛アライアンス「Project Glasswing」限定に留めることを決定しました。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

SWE-bench Verifiedで「93.9%」に達し、人間のエキスパート領域へ

※SWE-bench (Software Engineering Benchmark)・・・モデルやエージェントのソフトウェア開発能力を評価するためのベンチマーク。

Claude Mythos Preview 評価結果

評価ベンチマーク	前世代 (Opus 4.6)	Mythos Preview
SWE-bench Verified (自律的ソフトウェアエンジニアリング)	80.8%	**93.9%**
SWE-bench Pro (未飽和課題への自律エンジニアリング)	53.4%	**77.8%**
Terminal-Bench 2.0 (コマンドライン自律操作)	65.4%	**82.0%**
GPQA Diamond (博士レベルの科学的推論能力)	91.3%	**94.6%**

技術的な意味合い

複合的な推論タスクの突破

ぜい弱性の自律発見は、単なるテキスト解析ではなく「コード理解」「実行セマンティクスの推論」「エクスプロイトコードの試行錯誤」を同時に行う極めて難易度の高い行為です。

人間を超える圧倒的ペース

GPQAやSWE-benchでのスコアが示すとおり、複雑な多ステップの推論を何時間も継続できる能力が、自律エクスプロイト開発の基盤となっています。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

数万の目をかいくぐり生き残ったぜい弱性が、AIの並列分析により数時間で露呈

27年

OpenBSD 潜伏バグ

セキュリティを極めて重視し、徹底的なコードレビューで知られるOpenBSDプロジェクトにおいて、1999年から潜伏していた深刻なクラッシュバグをAIが自律発見。

※人間の査読体制の現実的限界を実証

–引用元：Hiteches

17年

FreeBSD RPCSEC_GSS

NFSサーバーの認証処理に潜むスタックバッファオーバーフローを検出。128バイトのバッファに最大400バイトの書き込みを許すミスが17年間放置。

※リモートでのルート権限奪取が可能に

–引用元：Hitechies

約8千円(トークンクレジット)

発見・エクスプロイト開発コスト

OpenBSDの27年間発見されなかったバグを発見、実証した際の推定される利用コスト

これほどの高価値ゼロデイぜい弱性の発見から実用的なエクスプロイト開発に至るまで、AIを用いた場合のAPI実費コストは極めて低価格です。

※攻撃プロセスの劇的な民主化と低コスト化

–引用元：Hitechies

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

ぜい弱性公表から「手動攻撃プログラム開発」そして攻撃開始まで著しく短縮化！

3～5カ月　の　猶予があったのはもはや過去

Palo Alto Networks の警告

10時間で攻撃コードが公開

侵入・窃取まで最短72分で完了

Palo Alto Networksの観測によると、自社製品におけるCVE（共通ぜい弱性識別子）開示件数が急増。防御側がパッチを十分に周知し適用させる前に、自動化された攻撃手法が確立されています。

時間的猶予が崩壊する原因

① エクスプロイト（攻撃コード）の即時自動生成

これまでは「ぜい弱性の公開」から「実用可能な攻撃プログラムの開発」までにタイムラグ（数週間～数カ月）があり、それが防御側の貴重な対応猶予でした。**AIはこの差を極端に短期化します。**

② 追いつかない人手のトリアージ・テスト

パッチが提供されても、組み込み機器や製造システムの現場では「テスト環境での互換性検証」に数カ月を要するため、攻撃可能になったぜい弱性が何カ月も放置され続けることになります。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

2026年5月22日、フロンティアAIの脅威変化を受けた「異例の短期サイバーセキュリティ対応要請」

要請の概要と時間軸

金融庁と日本銀行は2026年5月22日、高度な自律性を持つ「フロンティアAI（Mythos等）」によるサイバー攻撃脅威の急増を踏まえ、国内すべての金融機関等に対して緊急要請を共同で発出。

猶予期間は「約1カ月」：

経営トップの強い主体的な関与のもと、わずか1カ月という極めて短い期間で資産管理およびぜい弱性管理の総点検、必要な対応の実施を強く要請。

要請が求める「経営判断」と具体策

① 能動的なシステム停止の計画策定

攻撃側のエクスプロイト開発が人間の対応速度を超えるため、「攻撃を受けた、またはその兆候を検知した場合に、経営判断によって即時に能動的システム切断や停止を行える準備」を義務付け。

② 徹底したぜい弱性の迅速把握

管理されていないIT資産（シャドーIT）の完全な排除、および、新ぜい弱性公表に対するトリアージを日次ベースで運用するサイクルの確保。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

「発見」と「悪用」がほぼ同時に発生。パッチ対応までの時間的猶予は完全に消失

3カ月～5カ月

従来の攻防タイムライン (～2025年)

防御側の猶予

① ぜい弱性公表
ベンダー・研究者が検知
→ ② パッチ開発開始
修正・テスト (数日～数週)
→ ③ パッチ適用猶予
約 30日～90日間
→ ④ 悪用攻撃開始
ハッカーが攻撃を一般化

11時間～

現在の攻防タイムライン (フロンティアAI時代 2026年～)

防御側 即時対応

① AIによる自律発見
わずか数十分の並列スキャン
→ ② 自律エクスプロイト生成
数秒で検証済コードが完成
→ ③ 適用猶予
ほぼゼロ
→ ④ 即時攻撃・侵入
パッチ適用の隙を与えず侵入

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

CRA72時間の壁は「直列プロセス全体」の仕組み化

HITACHI

初動→特定→影響判断→証跡確保のすべての工程を72時間以内で処理する４つのプロセス
「製品に関するぜい弱性対応を専門に行う組織（チーム）」PSIRTの立ち上げとプロセスの着実な実施

① 初動検知

新たなぜい弱性の検知、
もしくは製品のインシデントを
認識

**CSIRT/ENISAに
24時間以内に報告**

→

② 構成（SBOM）特定

対象のぜい弱性コンポーネントが、自社製品群のどこに、どのバージョンで組み込まれているかを特定。

→

③ 影響・リスク判断

該当コードが実際に実行されるか、自社製品への実被害リスクを判断。対策の検討。

→

④ 当局報告

要件に基づく報告用のデータをまとめ、EU当局（SRP等）への適切なインシデント報告を初動検知から72時間以内に完了。

**CSIRT/ENISAに
72時間以内に報告**

※どこか一箇所でも停滞すれば「72時間以内報告」は即座に失敗します。単一施策ではなく、
情報収集からSBOM特定、トリアージ、報告に至る「一気通貫したプロセスの自動化・合理化」がなければ乗り越えられません。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

解決戦略①：SBOM運用基盤の即時整備

HITACHI

「知らないものは報告できない」。CRA24時間報告義務をクリアする物理的前提条件

なぜSBOM整備が最優先なのか

CRA対応における最大の罠は「自社製品にどのようなオープンソースソフトウェア（OSS）が使われているか完全に把握していない」状態そのものです。

・SBOM（ソフトウェア部品表）がないと、新たな深刻なぜい弱性が発表された際、「自社製品が影響を受けるか」の初期スクリーニングすら開始できません。
・自動スキャンツールを活用した継続的なSBOM生成が、24時間ルールの解決への第一歩となります。

Before
製品現場
任せ

→

After
全体把握
プロセス化

SBOM運用の4つの実務要件

1.設計段階からセキュリティをデザイン
複数レイヤーを意識した脅威分析とぜい弱性が発生しづらい設計

2.DevSecOps
開発段階でビルドパイプライン（CI/CD）と連携したぜい弱性の排除の仕組み化(シフトレフト)
そしてリリース後も常にぜい弱性を管理する仕組み(シフトライト)

3.サプライヤーからのSBOM回収義務化
受託開発や外部調達コンポーネントに対しても、調達要件にSBOM納品を必須として組み込み、サプライチェーン全体を可視化

4.ぜい弱性データベースとの常時リアルタイム紐付け
製品に組み込まれたコンポーネントリスト（SBOM）と、JVNやNVDなどの最新ぜい弱性情報をリアルタイムで突き合わせる監視エンジンの稼働

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

解決戦略②：リスクベースぜい弱性トリアージの高速化

CVSSによるスコアリングだけでは不十分。EPSSとKEVを組み合わせ複合的なトリアージの必要性

CVSS（深刻度）基準だけの限界

これまでよく使われていたCVSS（共通ぜい弱性評価システム）の「High（高）以上はすべて即パッチ」は現実的ではなく現場の負荷が高く、完全に機能不全になる。

・CVSS「High」であっても、実際に悪用される（エクスプロイトコードが作成され流通する）割合はわずか約5%と言われている。

・実効性の高いリスクベースで優先順位付けをしっかりし対応する必要がある。

Before
パッチ対応基準があいまい

→

After
リスク根拠を明確にして対応

実効性の高いリスクベース優先順位付け

1. EPSS（悪用予測スコアリングシステム）の適用
機械学習モデルにより「そのぜい弱性が今後30日以内に悪用される確率（%）」を算出し、実際の攻撃リスクをリアルタイムで追跡。

2. KEV（既知の悪用されたぜい弱性カタログ）の活用
CISAが公開する「進行系で野生で悪用されているぜい弱性」リストに合致した場合は、CVSS値に関わらず最優先で防御パッチを適用。

3. VEX（ぜい弱性不影響情報）による意思表明
「該当コンポーネントを使用しているが、設定によりぜい弱性の影響は受けない」という判断を速やかにVEX形式で外部発信し、不必要な確認問い合わせを削減。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

OTA（Over-The-Air）アップデート基盤の設計・組み込みと5年間のサポート義務

CRAが定める「最低5年間」の更新義務

CRAにより、メーカーは製品出荷後**最低5年間**（または製品の想定される耐用寿命期間）にわたり、無償でセキュリティパッチを提供し続ける義務を負います。

※新PL法では、10年にわたって損害賠償責任が発生

・これまでの「売り切り型」製品販売は許されず、継続的な保守コストを当初の製品設計や価格設定に内包させるビジネスモデルの変革が必要です。

Before
売り切り

→

After
継続的なセキュリティ対応

OTA（遠隔配信）基盤による高速サイクル化

1. 自動OTA配布プロセスの確立

物理的に回収することなく、インターネットを経由して組み込みファームウェアやソフトウェアを遠隔で安全に書き換える（OTA）自動アップデート機構の組み込み。

2. ロールバック＆整合性検証設計

パッチ適用失敗時の安全な自動フォールバック設計（ロールバック）と、署名検証やハッシュチェックによる改ざんファームウェア適用防止策の同時実装。

3. 段階展開・継続的テスト体制

全出荷台数に一斉展開せず、ステージング段階を経てフィールド全体にパッチを展開する運用と、テストの半自動化によるパッチ検証期間の大幅な短縮。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

今すぐ着手すべき3ステップ

2026年9月の報告開始までに土台を、2027年12月の全面適用までに完全運用を！

STEP 01

SBOM管理体制の整備

開発・調達する全ファームウェアやライブラリのSBOM自動生成フローを組み込み、「何が・どこに・どのバージョンで使われているか」を常時システム的に追跡できるデータベース基盤を即座に整備する。

➔ 目安期間：～3カ月以内

STEP 02

トリアージ＆運用の標準化

すべてのCVSSアラートを処理するのをやめ、CISAのKEVカタログや最新EPSSを導入して「野生で攻撃悪用されている現実的なリスク」だけを最優先トリアージする合理的なリスク判断運用プロセスを確立する。

➔ 目安期間：～6カ月以内

STEP 03

自動化ソリューションの導入

人手でぜい弱性の影響条件を1つずつ解釈・評価する限界を認め、AIエージェントやPSIRT関連サービスなど製品管理業務に適用して、調査時間の劇的な削減と品質の平準化を達成する。

➔ 目安期間：1年以内（本格運用へ）

今回はCRAをテーマとしましたが、各国のセキュリティ関連規制、政策、業界動向などキャッチアップが必要
セキュリティ対応の仕組み化、セキュリティ対応人財の事業への戦略的な組み込みが必要
⇒　1企業ではなかなか対応できない部分、運用の標準化などはご相談ください。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

開発工程にてぜい弱性をチェックするシフトレフト、運用時に常時セキュリティ監視するシフトライト双方を実現するSnyk。PoC支援、ツール導入、DevSecOps実現に向けた伴走支援します。



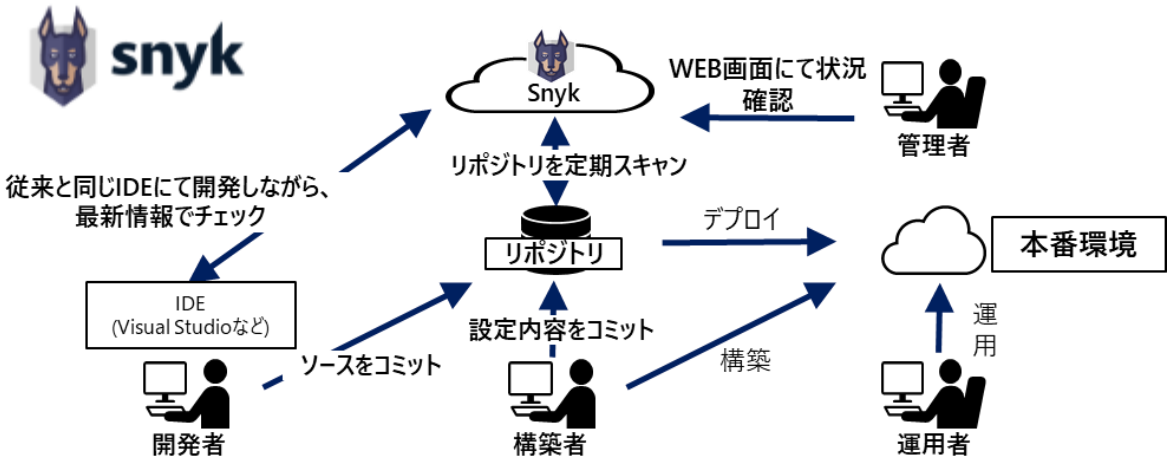


1. ぜい弱性の迅速な対策を支援（開発/テスト）

開発ツール(IDE、CI/CDツールなど)と連携し、リポジトリを最新のぜい弱性情報で随時チェック開発工程から開発者中心のセキュリティ対応を支援

2. 新たなぜい弱性を継続的に検出し対策（運用）

専任チームが管理する高品質な最新ぜい弱性データベースで、迅速なセキュリティ対応を支援



「Snyk」はSnyk社の登録商標です

製品名	機能	概要
Snyk Code	デベロッパーファーストの SAST（静的解析）	静的解析、IDE統合、リアルタイム検知
Snyk Open Source	SCA （ソフトウェア構成分析）	OSS ぜい弱性、ライセンスコンプライアンス管理
Snyk Container	コンテナぜい弱性の 検知・自動修正	イメージぜい弱性検出、K8s 構成分析
Snyk IaC	IaC (Infrastructure as Code) のセキュリティベストプラクティス 自動チェック	IaC misconfig ぜい弱性、ドリフト管理、ポリシー適用
Snyk API & Web	DAST(動的解析)	実行状態のアプリケーションに対してぜい弱性分析

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

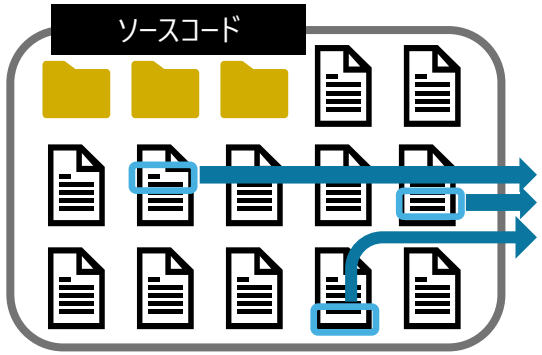
OSSセキュリティ&ライセンス管理ツール FOSSIDとは

広い対応範囲と高い精度を兼ね備えたOSSセキュリティ管理ツール

様々なコードスキャン　多種多様なOSSに対応　SBOMの生成と管理

1. さまざまなコードスキャン

コンポーネント全体だけでなく、ソースコードの一部についてもコードスニペットによる解析で派生元のオープンソースを特定します。



AIが生成したコードにはGPL由来コード混入や脆弱な実装の再利用リスクが潜在する

2. 多種多様なOSSに対応

オープンソースからコントリビュートしたソースまで多くのソフトウェアコンポーネントを網羅します。独自のナレッジデータベースを専任の研究チームによって維持管理します。

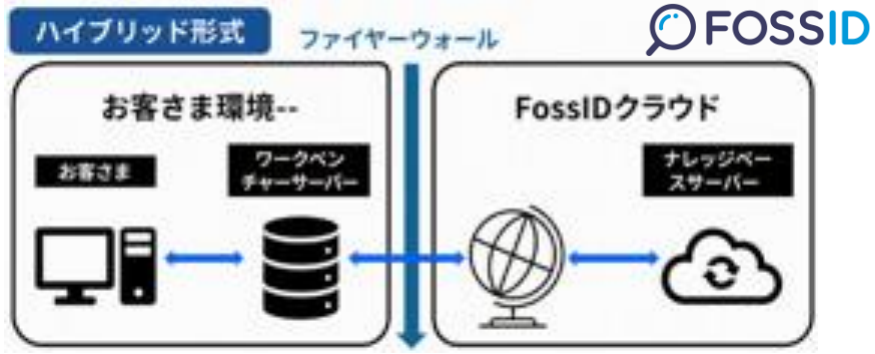
3. SBOMの生成と管理

分析した結果はソフトウェアのコンポーネント情報としてSBOMの形式(SPDX、CycloneDX)とし て出力、管理ができます。

※ SBOM(Software Bill of Materials) : ソフトウェア部品表

4. お客さま環境に応じたツールの導入形式

ハイブリッド形式(クラウド＆オンプレミス) での導入形式を用意。大切なソースをクラウドにアップロードすることなく解析を行います。



「FOSSID」はFOSSID社の登録商標です

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

PSIRT運用　一部代行サービス(参考出展)

HITACHI

SCAツール連携と当社の得意な24時間365日マネージドサービスを連携し、PSIRT運用の一部をBPOします。

当社運用基盤により、**CVE検知から72h一次回答までを標準フロー・自動化で処理**。属人化を排し、案件集中時も期限遵守可能な体制を実現します。

STEP 01
SCAによる脆弱性監視
SCAツールで常時監視

STEP 02
顧客SBOM照合
該当有無を判定

STEP 03
CVE検知
新規CVE／更新を検出

STEP 04
初期トリアージ
CVSS/EPSS/KEV/Advisory

STEP 05
影響有無判定（暫定）
標準ルールで暫定判定

STEP 06
優先度分類（暫定）
対応優先度を仮設定

STEP 07
24時間速報作成
→ 成果物① 出力

STEP 08
詳細評価１
パッチ有無確認
VEX案提示、CRA報告案提示

STEP 09
詳細評価
パッチ適用有無確認
回避策、悪用可能性有無確認

STEP 10
判定確定
影響・優先度を確定
VEX確定、CRA報告内容確定

STEP 11
72時間一次回答作成
→ 成果物② 出力

STEP 12
お客さまにて脆弱性対策
対策後SBOM更新
対策完了

SCA連携

Snyk/FOSSID等のSCAツールとのシームレス連携。自動化されたぜい弱性スキャンとSBOM生成を実現。

多面的判定

KEV/ベンダーアドバイザリー/EPSS/CVSSによる多面的判定。リスク評価の精度を向上。

自動証跡化

すべての判断過程を証跡として自動記録。CRA Article 14対応を実現。

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.

その他　セキュリティに関するお困りごと支援

よくご相談いただくTop５

PSIRTの構築、社内ポリシーをしっかり整備したい	PSIRT構築支援、ポリシー、ガイドライン作成
インシデントが発生した時に備えて対応訓練をしたい	インシデント対応トレーニング
経営層へのセキュリティの理解を深めていただき セキュリティ対策への協力、予算確保につなげたい	経営層向けトレーニング
OT製品やOTネットワークに対するぜい弱性を検査したい	ペネトレーションテスト
AIのサイバー攻撃に関する現状が知りたい	AIセキュリティ対策トレーニング

© Hitachi Systems Engineering Services, Ltd. 2026. All rights reserved.


HITACHI