

Sparrow Enterprise

EU CRA対応を支援する統合アプリケーションセキュリティ

SECURITY BY AI

開発から出荷後まで、製品のセキュリティを継続管理

SAST・DAST・SCAとSBOMを連携し、ソフトウェアの脆弱性を可視化。
CRA対応に必要なセキュリティ検証とエビデンスの整備を支援します。

CRAとは

EUサイバーレジリエンス法 (CRA) は、デジタル要素を含む製品の
サイバーセキュリティ要件や脆弱性管理に関する義務を定めた規則です。

対象：EU市場に提供する接続型ハードウェア・ソフトウェア。一部製品は個別法令により適用除外。

2024.12.10

発効

2026.09.11

報告義務の適用開始

2027.12.11

主要義務の全面適用

製造者が準備すべき主要要件

01

設計・開発段階からセキュリティを確保

リスク評価に基づいて製品を設計・開発し、既知の悪用可能な脆弱性がない状態で市場に提供します。

02

構成要素の特定とSBOMの作成

構成要素と脆弱性を文書化し、少なくとも最上位の依存関係を含む、機械可読形式のSBOMを作成します。

03

継続的な検証と迅速な修正

有効かつ定期的なセキュリティテスト・レビューを実施し、遅滞なく脆弱性を修正して更新を提供します。

04

報告体制と適合性エビデンスの整備

実際に悪用されている脆弱性や重大インシデントを報告し、技術文書・EU適合宣言の整備とCEマーキングの表示を行います。

報告義務：認知後24時間以内の早期警告、72時間以内の詳細通知

最終報告：悪用が確認された脆弱性は是正措置の提供後14日以内、重大インシデントは72時間以内の通知から1か月以内。

主要な義務違反には、最大1,500万ユーロ、または前年度の全世界年間売上高の2.5%のいずれか高い額の制裁金が科されます。

Sparrow Enterprise

EU CRA対応を支援する統合アプリケーションセキュリティ

SECURITY BY AI

CRA対応を支援する主な機能

SAST

ソースコードの脆弱性解析

開発段階でセキュリティ上の弱点を検出。解析レポートをテスト・レビューのエビデンスとして活用できます。
Java・Pythonなど25以上の言語に対応。

DAST

稼働中のWeb・APIのセキュリティ検証

稼働中のWebアプリケーションやAPIの脆弱性を検査し、静的解析を補完。
定期的なセキュリティテスト・レビューを支援します。

SCA/SBOM

OSSの特定と構成要素の可視化

ソース・バイナリ・依存関係ファイルから構成要素と既知の脆弱性を特定し、SPDX・CycloneDX形式のSBOMを生成します。

Enterprise

解析結果の統合管理

SAST・DAST・SCAの結果を単一環境で管理。CI/CDと連携した解析で、開発プロセスにおける脆弱性対応を支援します。

SecureHub

SBOMの共有と管理

SBOM管理基盤のSparrow SecureHubなどと連携。
バージョンや受領・提供履歴、サプライチェーン内での共有を管理します。

AI Package | 修正優先順位と修正ガイド

AIが修正の優先順位とコード修正案を提案します。

別途アドオンライセンスで提供し、オンプレミス環境ではプライベートLLMとの連携が必要です。

製造者が別途実施すべき業務

PSIRT運用と脆弱性の受付・開示方針 / リスク評価とサポート期間の設定

出荷後の監視とセキュリティ更新の提供 / 法令に基づく報告 / 技術文書・適合性評価・CEマーキング

Sparrowの解析結果やSBOMは、CRA対応の根拠資料として活用できます。なお、Sparrowは認証機関や適合性評価機関ではないため、製品の導入のみでCRAへの適合が保証されるものではありません。