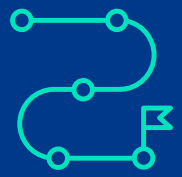
CRA は、**デジタル要素を含む製品（PDE）に対して規制による監督**を導入しており、関係者グループ全体にわたってOSS の開発に重要な影響を及ぼします。

CRA では、**OSS スチュワード**という新たな役割が定義されており、これは自ら収益化していないオープンソース技術の開発を体系的に支援する組織を指します。

CRA の下では、**OSS スチュワードはサイバーセキュリティ ポリシー、脆弱性の取り扱いや報告のためのプロセス、市場監視機関（MSA）**との連携、そして自主的な**セキュリティ宣言**に対して責任を負います。

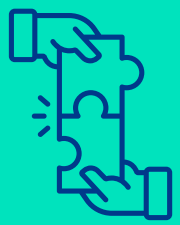


オープンソース プロジェクトは、CRA のタイムライン要件に備えるために、PSIRT チームやセキュリティ ポリシーへの投資を行いながら、**5 年間のセキュリティ ロードマップ**を策定する必要があります。

標準化されたセキュリティ ツールは CRA への準拠を加速させており、**SPDX 3.0、OpenSSF Scorecard、OpenChain** の各フレームワークが、プロジェクトによるセキュリティのベストプラクティスの実装を支援します。

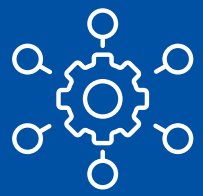
セマンティック バージョニングは、重大な変更、軽微な更新、バグ修正を明確なバージョン管理に対応させることで、製造業者が CRA への準拠状況を追跡するのに役立ちます。

SBOM はより高い粒度での情報提供が求められており、ファイルレベルでの追跡によって、製造業者にとってセキュリティの可視性、リスク評価、脆弱性対応が向上します。



オープンソースの**セキュリティには業界横断的な協力が必要**であり、製造業者、政府、プロジェクトが共同でポリシーを開発し、セキュリティに資金を提供し、長期的なソフトウェアのメンテナンスを確保します。

CRA は、セキュリティの実践、文書化、そしてエコシステム全体での協力を改善することによって、オープンソース ソフトウェアのセキュリティを強化する**機会**を提供します。



AI は新たなセキュリティ リスクをもたらし、AI 生成コードや汚染されたトレーニング データセットからの脅威を軽減するためのフレームワークが必要です。

リーダーシップはオープンソースのレジリエンスを推進します。プロジェクトのメンテナー、ディレクター、そして運営委員会のメンバーは、積極的にセキュリティ文化を構築するために、啓蒙活動や広報活動を通じて取り組まなければなりません。

Linux Foundation と **OpenSSF** は、開発者、製造業者、スチュワードがサイバーセキュリティ規制に適合できるよう、協力とベストプラクティスを通じて CRA への準備をサポートしています。