CRA (Cyber Resilience Act) 概要と最新動向

OSSセキュリティ技術ワークショップ(OWS)2025

October 28, 2025

自己紹介

ルネサスエレクトロニクス株式会社
余保 束

LinkedIn

- 経歴
  - ✓ 4/8bitマイコン向け組込みSWエンジニア（アセンブリ言語）
  - ✓ 16bitマイコン向け組込みSWエンジニア（C言語）
  - ✓ 組込みセキュリティエンジニア
  - ✓ PSIRT(Product Security Incident Response Team)
  - ✓ 社内OSSコミュニティ活動推進
- Linux Foundation community
  - ✓ Open SSF Japan chapter
  - ✓ OpenChain Japan WG

セキュリティの難しさ

システム全体の堅牢性はシステムの中で最も脆弱な箇所で決まる（桶理論）

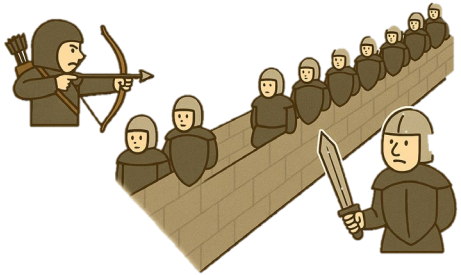
-ライフサイクル全てに渡ってセキュリティを考える必要がある。

桶の水は一番低い所
から漏れる

攻撃者はセキュリティホールを1か所見つければ良く、守る側はセキュリティホールが1か所もあってはならない（攻撃者の非対称な優位性）

-サプライチェーン全体でセキュリティを考える必要がある。

たった1か所が脆弱だと
攻め込まれてしまう



攻撃者の不均衡な優位性

Disclaimer

スピーカーは法律の専門家ではありません。

ここではスピーカーが CRA（EU Cyber Resilience Act）をウォッチし調べたことを共有しますが、誤りを含む可能性があります。

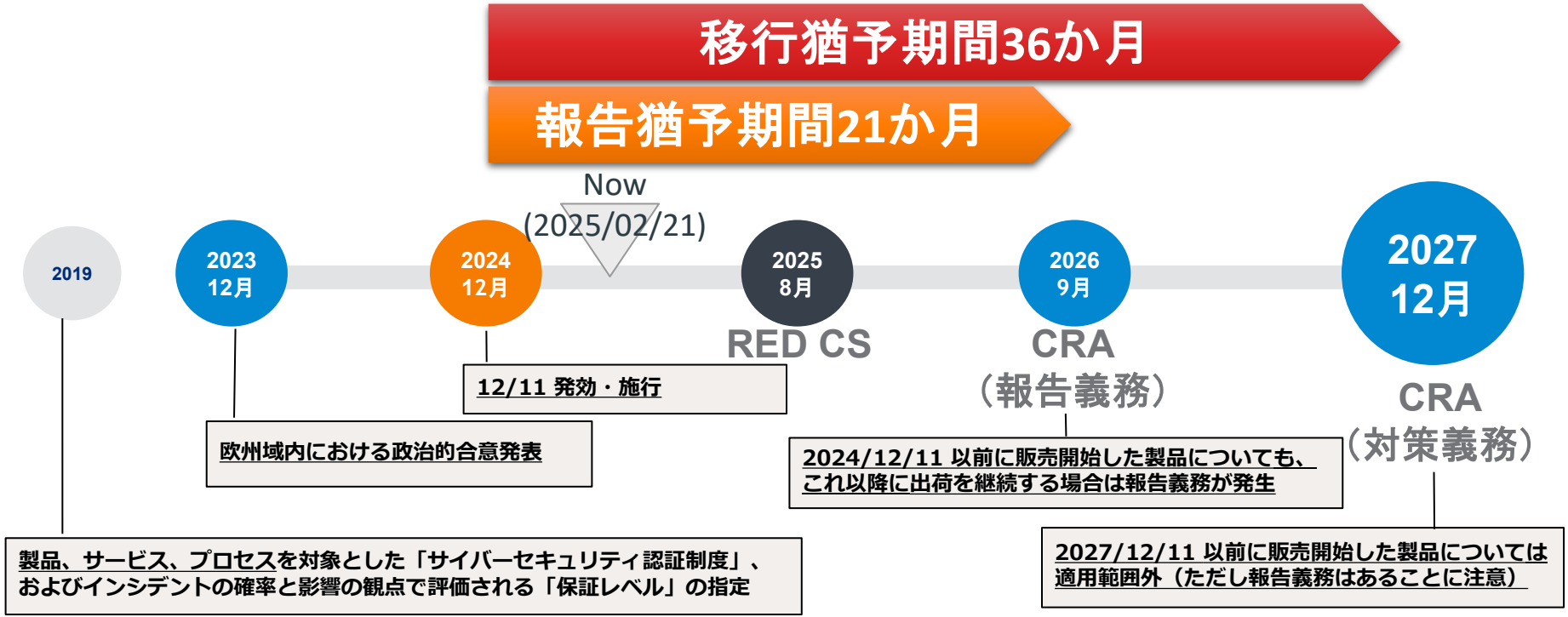
法令の正確・正式な意味・解釈は、別途専門家に確認を取ることをお勧めいたします。

Agenda

- CRAタイムライン
- CRA の全体的な構成
- 対象になる機器と分類
- 用語・概念・登場人物の整理
- CRAで求められる要件
- 主な要件の要点
- Open-source softwareとOpen-source software Steward
- Open-source software Steward(OSSスチュワード)の義務
- 最新動向
- LF Trainingの紹介

CRAタイムライン

EU CRA タイムライン



CRA の全体的な構成

CRA 全体目次-1

CHAPTER I GENERAL PROVISIONS
Article 1 Subject matter
Article 2 Scope
Article 3 Definitions
Article 4 Free movement
Article 5 Procurement or use of products with digital elements
Article 6 Requirements for products with digital elements
Article 7 Important products with digital elements
Article 8 Critical products with digital elements
Article 9 Stakeholder consultation
Article 10 Enhancing skills in a cyber resilient digital environment
Article 11 General product safety
Article 12 High-risk AI systems

CHAPTER II OBLIGATIONS OF ECONOMIC OPERATORS AND PROVISIONS IN RELATION TO FREE AND OPEN-SOURCE SOFTWARE
Article 13 Obligations of manufacturers
Article 14 Reporting obligations of manufacturers
Article 15 Voluntary reporting
Article 16 Establishment of a single reporting platform
Article 17 Other provisions related to reporting
Article 18 Authorised representatives
Article 19 Obligations of importers
Article 20 Obligations of distributors
Article 21 Cases in which obligations of manufacturers apply to importers and distributors
Article 22 Other cases in which obligations of manufacturers apply
Article 23 Identification of economic operators
Article 24 Obligations of open-source software stewards
Article 25 Security attestation of free and open-source software
Article 26 Guidance

※EU官報のCRA公示へのリンク

CRA 全体目次-2

CHAPTER III Conformity of the product with digital elements
Article 27 Presumption of conformity
Article 28 EU declaration of conformity
Article 29 General principles of the CE marking
Article 30 Rules and conditions for affixing the CE marking
Article 31 Technical documentation
Article 32 Conformity assessment procedures for products with digital elements
Article 33 Support measures for microenterprises and small and medium-sized enterprises, including start-ups
Article 34 Mutual recognition agreements

CHAPTER IV NOTIFICATION OF CONFORMITY ASSESSMENT BODIES
Article 35 Notification
Article 36 Notifying authorities
Article 37 Requirements relating to notifying authorities
Article 38 Information obligation on notifying authorities
Article 39 Requirements relating to notified bodies
Article 40 Presumption of conformity of notified bodies
Article 41 Subsidiaries of and subcontracting by notified bodies
Article 42 Application for notification
Article 43 Notification procedure
Article 44 Identification numbers and lists of notified bodies
Article 45 Changes to notifications
Article 46 Challenge of the competence of notified bodies.
Article 47 Operational obligations of notified bodies
Article 48 Appeal against decisions of notified bodies
Article 49 Information obligation on notified bodies
Article 50 Exchange of experience
Article 51 Coordination of notified bodies

CRA 全体目次-3

CHAPTER V MARKET SURVEILLANCE AND ENFORCEMENT
Article 52 Market surveillance and control of products with digital elements in the Union market
Article 53 Access to data and documentation
Article 54 Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk
Article 55 Union safeguard procedure
Article 56 Procedure at Union level concerning products with digital elements presenting a significant cybersecurity risk
Article 57 Compliant products with digital elements which present a significant cybersecurity risk
Article 58 Formal non-compliance
Article 59 Joint activities of market surveillance authorities
Article 60 Sweeps

CHAPTER VI DELEGATED POWERS AND COMMITTEE PROCEDURE
Article 61 Exercise of the delegation
Article 62 Committee procedure

CHAPTER VII CONFIDENTIALITY AND PENALTIES
Article 63 Confidentiality
Article 64 Penalties
Article 65 Representative actions

CHAPTER VIII TRANSITIONAL AND FINAL PROVISIONS
Article 66 Amendment to Regulation (EU) 2019/1020
Article 67 Amendment to Directive (EU) 2020/1828
Article 68 Amendment to Regulation (EU) No 168/2013
Article 69 Transitional provisions
Article 70 Evaluation and review
Article 71 Entry into force and application

CRA Annex

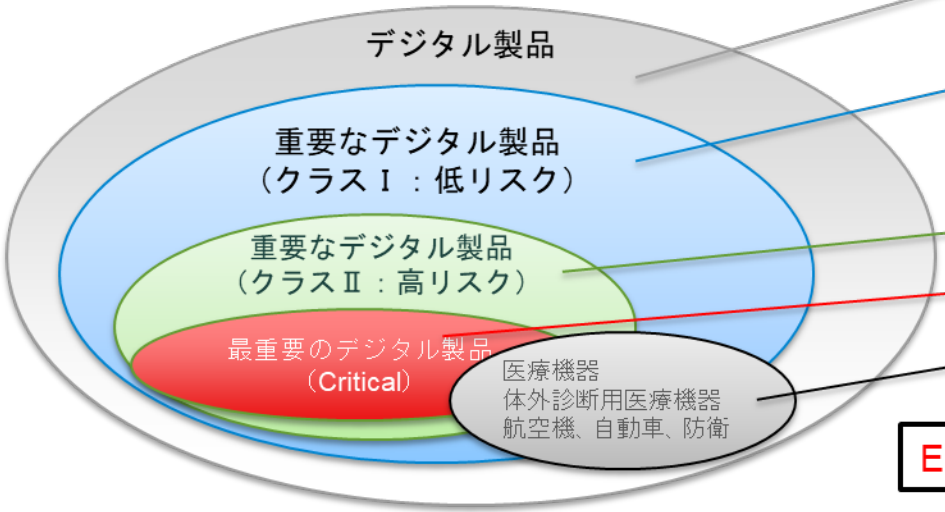
ANNEX I
ESSENTIAL CYBERSECURITY REQUIREMENTS
Part I Cybersecurity requirements relating to the properties of products with digital elements
Part II Vulnerability handling requirements
ANNEX II
INFORMATION AND INSTRUCTIONS TO THE USER
ANNEX III
IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS
Class I
Class II
ANNEX IV
CRITICAL PRODUCTS WITH DIGITAL ELEMENTS
ANNEX V
EU DECLARATION OF CONFORMITY
ANNEX VI
SIMPLIFIED EU DECLARATION OF CONFORMITY
ANNEX VII
CONTENT OF THE TECHNICAL DOCUMENTATION
ANNEX VIII
CONFORMITY ASSESSMENT PROCEDURES
Part I Conformity assessment procedure based on internal control (based on module A)
Part II EU-type examination (based on module B)
Part III Conformity to type based on internal production control (based on module C)
Part IV Conformity based on full quality assurance (based on module H)

対象になる機器と分類

CRA の対象機器範囲と求められる対応

出典：Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)
< https://eur-lex.europa.eu/eli/reg/2024/2847/ >

- 外部とデータのやり取りを行うデジタル製品全てが対象
  →何らかの半導体プロセッサと制御プログラムを有するほとんどの製品および機能の一部を実現する外部ソリューションが対象となる
- 第三者認証免除・軽減のための整合規格は検討中
  → 予想では「IEC62443」「EUCC」「ETSI EN 303 645」などが挙がっている



- 「セキュリティ特性要件」を満たす
- 更新プログラム提供を含む「脆弱性処理要件」の遵守

→**自己適合宣言**か**第三者認証**取得

別途定める整合規格への適合、
または**第三者認証**取得
- 整合規格は未定（EUCC、EN規格が有力？）

第三者認証取得

第三者認証取得

適用範囲外（業界規則への適合）

EU適合宣言（CEマーク）取得要件に組込まれる

「重要な」デジタル製品の具体例

クラスⅠ（低リスク）*AnnexⅢ
「重要な」デジタル製品であるが、リスクが低い製品

1. 認証およびアクセス制御リーダー（生体認証リーダーを含む）を含む、アイデンティティ管理システムおよび特権アクセス管理ソフトウェアとハードウェア
2. スタンドアロンおよび組み込みブラウザ
3. パスワードマネージャー
4. 悪意のあるソフトウェアを検索、削除、または隔離するソフトウェア
5. 仮想プライベートネットワーク(VPN)機能を備えたデジタル要素を備えた製品
6. ネットワーク管理システム
7. セキュリティ情報およびイベント管理(SIEM)システム
8. ブートマネージャー
9. 公開鍵インフラストラクチャおよびデジタル証明書発行ソフトウェア
10. 物理および仮想ネットワークインターフェイス
11. オペレーティングシステム
12. インターネットへの接続を目的としたルーター、モデム、およびスイッチ
13. セキュリティ関連機能を備えたマイクロプロセッサ
14. セキュリティ関連機能を備えたマイクロコントローラ
15. セキュリティ関連機能を備えた特定用途向け集積回路（ASIC）およびフィールドプログラマブルゲートアレイ（FPGA）
16. スマートホーム汎用仮想アシスタント
17. スマートドアロック、セキュリティカメラ、ベビーモニタリングシステム、アラームシステムなどのセキュリティ機能を備えたスマートホーム製品
18. 欧州議会および理事会指令2009/48/EC（45）の対象となるインターネット接続玩具で、ソーシャルインタラクティブ機能（会話や撮影など）または位置追跡機能を備えているもの
19. 健康モニタリング（追跡など）目的があり、規則（EU）2017/745または規則（EU）2017/746が適用されない、人体に装着または装着される個人用ウェアラブル製品、または子供が使用することを目的とした個人用ウェアラブル製品。

クラスⅡ（高リスク）*AnnexⅢ
「重要な」デジタル製品のうち、リスクが高い製品

1. オペレーティングシステムおよび同様の環境の仮想実行をサポートするハイパーバイザーおよびコンテナランタイムシステム
2. ファイアウォール、侵入検知および防止システム
3. 改ざん防止マイクロプロセッサ
4. 改ざん防止マイクロコントローラ

「（最: Critical ）重要な」デジタル製品
* Annex IV

1. セキュリティボックスを備えたハードウェアデバイス
2. 欧州議会および理事会の指令(EU) 2019/944(46)の第2条(23)で定義されているスマートメーターシステム内のスマートメーターゲートウェイ、および安全な暗号処理を含む高度なセキュリティを目的としたその他のデバイス
3. セキュアエレメントを含むスマートカードまたは類似のデバイス

出典：European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) <https://data.consilium.europa.eu/doc/document/PE-100-2023-REV-1/EN/pdf>

用語・登場人物の整理

用語・登場人物の整理

用語 (第３条)

- **デジタル要素を含む製品**(product with digital elements)
  ソフトウェアまたはハードウェア製品とその遠隔データ処理ソリューションを意味し、ソフトウェアまたはハードウェアのコンポーネントが個別に市場に出回る場合も含む
- **経済事業者**(economic operator)
  製造業者、認定代理店、輸入業者、販売業者、または本規則に従ってデジタル要素を有する製品の製造またはデジタル要素を有する製品の市販に関連して義務を負うその他の自然人もしくは法人
- **製造者**(manufacturer)
  デジタル要素を有する製品を開発もしくは製造する、またはデジタル要素を有する製品を設計、開発もしくは製造させ、有償、収益化、無償を問わず、その名称または商標の下で販売する自然人または法人

用語・登場人物の整理

用語（続き）

- **輸入業者**(importer)
  EU域外に設立された自然人または法人の名称または商標が付されたデジタル要素を有する製品を市場に出す、EU域内に設立された自然人または法人
- **販売業者**(distributor)
  サプライチェーンの中で、製造業者または輸入業者以外の自然人または法人で、デジタル要素を含む製品を、その特性に影響を与えることなく連合市場で入手できるようにする者
- **フリー・オープンソースソフトウェア**(free and open-source software)
  ソースコードがオープンに共有され自由にアクセスし、使用し、改変し、再配布できるようにするすべての権利を提供するフリー・オープンソースライセンスの下で利用可能にされたソフトウェア
- **オープンソース・ソフトウェア・スチュワード**(open-source software steward)
  製造業者以外の法人でフリーかつオープンソースソフトウェアとして適格であり、商業活動を目的としたデジタル要素を含む特定の製品の開発に対して、体系的な支援を継続的に提供する目的または目標を持ち、それらの製品の実行可能性を保証するもの

用語・登場人物の整理

用語（続き）

- **サポート期間**(support period)
  デジタル要素を含む製品の脆弱性が、附属書 I の第 II 部に規定される本質的なサイバーセキュリティ要件に従って効果的に処理されることを確保するために製造者が必要とする期間
- **上市**(placing on the market)
  デジタル要素を含む製品を連合市場で最初に入手可能にすること
- **市場で入手可能にする**(making available on the market)
  商業活動の過程において、有償であるか無償であるかを問わず、連合市場において頒布または使用するためにデジタル要素を含む製品を供給すること
- **CEマーキング**(CE marking)
  製造者が、デジタル要素を有する製品およびその製造者が実施するプロセスが、附属書 I に定めるサイバーセキュリティの必須要件およびその貼付を規定する他の適用可能なEU調和法令に適合していることを示すマーキング

用語・登場人物の整理

用語（続き）

- **ソフトウェア部品表**(software bill of materials)
  デジタル要素を有する製品のソフトウェア要素に含まれるコンポーネントの詳細およびサプライチェーン関係を含む正式な記録
- **脆弱性**(vulnerability)
  サイバー脅威によって悪用される可能性のある、デジタル要素を持つ製品の弱点、感受性、欠陥
- **悪用可能な脆弱性**(exploitable vulnerability)
  実際の運用条件下で敵対者が有効に利用できる可能性を有する脆弱性
- **積極的に悪用された脆弱性**(actively exploited vulnerability)
  悪意のある行為者がシステム所有者の許可なくシステムでその脆弱性を悪用したという信頼できる証拠がある脆弱性

CRA で求められる要件

CRA 第13条 製造業者の義務

1. デジタル製品を市場に出す際、附属書Iの１「セキュリティ特性要件」を遵守して設計・開発・製造 されていることを確認する。
2. サイバーセキュリティ上の**リスクアセスメントを実施**し、その結果を設計・開発・製造・配送・メンテナ ンスの際の考慮に入れる。
3. デジタル製品を市場に出す際、上記の**リスクアセスメントの結果を技術文書に含める**。
4. 第31条および付属書VIIIに従って要求される技術文書には、本条第3項で言及されるサイバーセキュリティリスク評価を含める。
5. 第三者から提供された部品を使用する際は、その部品により製品のセキュリティリスクを高めないことを保証する。
6. 特定した脆弱性を報告・対処・修復する。対処のための変更は機械可読形式でコンポーネントの製造または保守を行う個人または団体と共有する。
7. デジタル製品に関する**サイバーセキュリティ観点の情報を体系的に文書化**する。
8. **サポート期間は5年間と製品の使用期限のうち短い方とし、期間内は製造業者は脆弱性に効果的に対処する**。製造業者は脆弱性開等に適切なポリシーや手続きを有する。
9. **セキュリティアップデート公開から10年間、またはサポート期間のいずれか長い方の期間、セキュリティアップデートを利用可能とする**。
10. 大幅な変更バージョンは付属書 I、パート II、ポイント (2) の必須要件に準拠すればよい。最新バージョンへは無料でアクセスでき、旧バージョンユーザーが環境調整コストなしで適用できること。
11. ユーザーが過去のバージョンおよびサポート外ソフトウェアの使用に伴うリスク情報にアクセスできるようにする。
12. 上市前に製造業者は技術文書を作成する。対応する適合性評価手続きを行い、適合性が実証された場合はCEマーキングを貼付する。
13. 上市後10年間、技術文書と（該当する場合は）EU適合性証明書を市場監視当局が自由に使えるように保管する。
14. 一連の製造の中で、適合性を維持するための手順が整備されていることを確認する。
15. 製品の個体識別のため型番、バッチ番号、シリアル番号などを付記する。
16. 製品に製造業者の名前、商標、郵便住所、電子メールアドレスなどのデジタル連絡先、ウェブサイトなどを表示する。
17. 脆弱性報告ための単一の連絡先を附属書 II に記載されているユーザーへの情報および指示に記載する。連絡先はユーザーが通信手段を選択できるようにし、手段を自動化ツールに限定してはならない。
18. 附属書 II に定めるユーザーへの情報および説明書を**紙または電子形式で添付**する。情報および説明書は10年間とサポート期間の長い方の期間保持し、オンライン提供の場合はアクセス可能とする。
19. 購入時に、第8項のサポート期間の終了日へアクセスできるようにする。可能であれば、製造業者はサポート期間の終了をユーザーに通知する。
20. **EU適合性証明書か簡易EU適合宣言を提供する**。簡易宣言の場合は完全なEU適合宣言へのURLを提供する。
21. **サポート期間内に附属書II「セキュリティ特性要件」を遵守しない場合、直ちに必要な是正措置を講じ製品の撤回またはリコールを行う**。
22. 市場監視当局からの要求に応じて製品の適合性を証明する情報・文書を提出する。
23. 操業を停止し義務を遵守できなくなる場合、操業停止前に市場監視当局やユーザに通知する。
24. 欧州委員会は実施法の中で、SBOMの形式と要素を指定することができる。
25. ADCO は製品のフリーソフトウェアおよびオープンソースソフトウェアへの依存度評価の実施を決定できる。市場監視当局は附属書I第II部ポイント(1)のSBOM 提供を要求できる。

設計前のリスクアセスメントの実施及び設計書への反映を文書化する必要がある。
製品寿命もしくは5年間は脆弱性処理要件を満たす必要がある。（PSIRT相当の対応が必須）

CRA 第14条 製造業者の報告義務

1. **悪用されている脆弱性を認識した場合は**第7項に従い **CSIRT と ENISA に同時に通知**する。
2. 第1項の通知では以下を提出する。
   (a) 脆弱性を認識してから**24時間以内に早期警告通知**
   (b) 脆弱性を認識してから**72時間以内に**、製品の一般情報、悪用の性質、講じられた・またはユーザーが講じられる是正・緩和措置を含む**脆弱性通知**
   (c) 是正措置または緩和措置が利用可能になってから**14日以内に以下を含む最終報告書**
      (i) 脆弱性の説明（その深刻度および影響を含む）
      (ii) 入手可能な場合、脆弱性を悪用した悪意のある行為者に関する情報
      (iii) 脆弱性修正のためのセキュリティアップデートまたはその他の是正措置に関する詳細
3. 製品のセキュリティに影響を与える**重大なインシデントを認識した場合は**第7項に従い **CSIRT と ENISA に同時に通知**する
4. 第3項の通知では以下を提出する。
   (a) インシデントを認識してから**24時間以内に早期警告通知**。違法または悪意のある行為により比企侵された疑いがあるかを含む
   (b) インシデントを認識してから**72時間以内に**、インシデントに関する一般情報と初期評価、講じられた・またはユーザーが講じられる**是正・緩和措置を含むインシデント通知**
5. 以下の場合インシデントは重大とみなす。
   (a) 機密性の高いまたは重要なデータや機能の可用性、真正性、完全性、または機密性を保護する能力に悪影響を及ぼす可能性がある
   (b) ユーザーのネットワークおよび情報システムにおいて悪意のあるコードの導入または実行につながる可能性がある
6. CSIRT は現在悪用されている脆弱性や重大なインシデントに関する中間レポートの提供を製造元に要求する場合がある。
7. 第1項と第3項の通知は、第16条で規定する単一の報告プラットフォームを介して提出される。
8. 積極的に悪用されている脆弱性または重大なインシデントを認識した場合、これらについてユーザーに通知する。
9. 本法案発効日から12ヶ月以内に欧州委員会は第61条に委任行為を採択する。
10. 欧州委員会は、通知された情報の種類、形式、手順を更に指定することができる。

自社製品に対するサイバーセキュリティ・インシデントへの報告・対応・連絡を行う組織が求められる
当該義務は法律施行前に販売を開始し、施行後も出荷を継続する製品にも課せられることに注意 (第69条3)

CRAで求められる要件

附属書 Ⅰ の Part Ⅰ「セキュリティ特性要件」

1. リスクに基づいて適切なサイバーセキュリティを確保するよう設計・開発・生産されていること。
2. リスクベースアセスメントに基づいて、以下を満たすこと。
   - (a) 悪用可能な脆弱性が含まれないこと。
   - (b) 製品を元の状態にリセット可能である等、デフォルトで安全な設定となっていること。
   - (c) セキュリティアップデートにより脆弱性に対処できること。
   - (d) 適切な制御メカニズムにより不正アクセスからの保護が確保されていること。
   - (e) 最先端の暗号化などにより個人データ・その他のデータの機密性を保護すること。
   - (f) データやプログラムなどの完全性を許可されていない操作から保護し、破損についても報告すること。
   - (g) 必要なデータに限定して処理を行うこと。（データの最小化）
   - (h) DoS攻撃からの回復・緩和などの重要な可用性の機能を保護すること。
   - (i) 他の機器やネットワークからのサービスの可用性について自身への悪影響を最小化すること。
   - (j) 外部インターフェース等の攻撃対象領域を制限して設計・開発・製造されていること。
   - (k) インシデントの影響を軽減するように設計・開発・製造されているころ。
   - (l) アクセス、データ修正、サービス、機能などの内部活動を記録・監視し、セキュリティ情報を提供すること。
   - (m) ユーザーが全てのデータと設定を簡単に永久に削除できること。それら情報が転送可能な場合は安全に転送できること。

附属書Ⅰの Part Ⅱ「脆弱性処理要件」 ・・・製造業者が満たすべき要件

1. 製品に含まれる脆弱性とコンポーネントを特定し、文書化すること。
   - 機械可読形式で一般的に使用されるSBOM作成（少なくとも最上位レベルの依存関係含む）を行うこと。
2. セキュリティアップデートの提供など、遅滞なく脆弱性に対処・緩和すること。
3. 効果的かつ定期的なテストとレビューを行うこと。
4. 修正された脆弱性について、情報の公開を行うこと。
5. 脆弱性開示ポリシーを導入し、実施すること。
6. 製品やサードパーティコンポーネントの潜在的な脆弱性に関する情報共有を行い、連絡先を提供すること。
7. 悪用可能な脆弱性が適時に修正・緩和されるように安全にアップデートを配布するメカニズムを提供すること。
8. セキュリティパッチや更新プログラムが遅滞なく無料で配布され、ユーザーへの助言メッセージも添付すること。

主な要件の要点

要件の要点： SBOM

附属書 I Part II「脆弱性処理要件」 第1項

- 製品に含まれる脆弱性とコンポーネントを特定し、文書化すること。
- 機械可読形式で一般的に使用されるSBOM作成（少なくとも最上位レベルの依存関係含む）を行うこと。

要件の要点： 脆弱性管理

- サイバーセキュリティリスクアセスメントを行いリスクを最小限に抑えることこと(第13条2)
- サイバーセキュリティリスクアセスメントは、文書化され、適宜更新されること(第13条3)
- 脆弱性を特定した場合、脆弱性に対処し、その脆弱性を改善しなければならない(第13条6)
- セキュリティアップデートは上市してから最低10年間、またはサポート期間のどちらか長い期間提供しなければならない(第13条9)
- CSIRT及びENISAに対して製品に含まれる積極的に悪用された脆弱性を通知する(第14条1,2)
  - 積極的に攻撃された脆弱性に関する脆弱性を知った後24時間以内に早期警告通知
  - 72時間以内に是正措置又は緩和措置を含む一般的な情報を提供
  - 是正措置又は緩和措置が利用可能となった後14日以内に、最終報告書を作成する

要件の要点： アップデートの提供

第13条

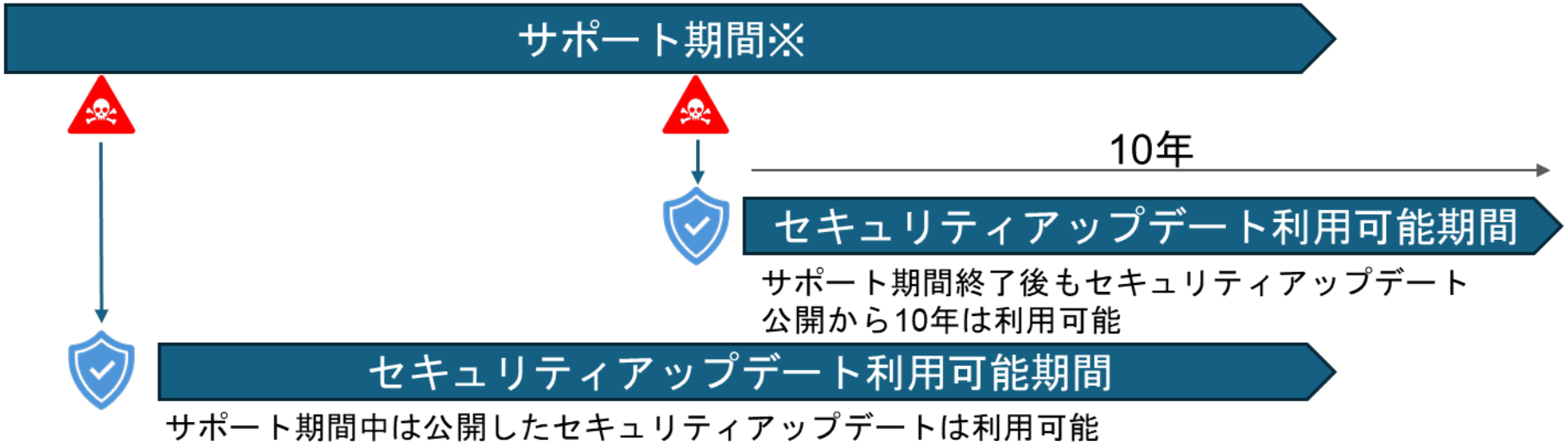
8. サポート期間は5年間と製品の使用期限のうち短い方とし、期間内は製造業者は脆弱性に効果的に対処する。製造業者は脆弱性開等に適切なポリシーや手続きを有する。

9. セキュリティアップデート公開から10年間、またはサポート期間のいずれか長い方の期間、セキュリティアップデートを利用可能とする。

10. 大幅な変更バージョンは付属書 I、パート II、ポイント (2) の必須要件に準拠すればよい。最新バージョンへは無料でアクセスでき、旧バージョンユーザーが環境調整コストなしで適用できること。

要件の要点： アップデートの提供

CRA Article13-9
Manufacturers shall ensure that each security update, as referred to in Part II, point (8), of Annex I, which has been made available to users during the support period, remains available after it has been issued for a minimum of 10 years or for the remainder of the support period, whichever is longer.



※サポート期間：新たに発見された脆弱性についてセキュリティアップデート提供が必要な期間

罰則・制約

第13条

21. サポート期間内に附属書ＩＩ「セキュリティ特性要件」を遵守しない場合、直ちに必要な是正措置を講じ製品の撤回またはリコールを行う。

第64条

2. Annex Ⅰのサイバーセキュリティ必須要件と第13条および第14条に定める義務に違反した場合、1,500万ユーロ、または違反者が企業の場合は前年会計年度の全世界売上の 2.5% のいずれか高い方を上限として罰金を課す。

3. 第18条から23条、第28条、第30条の(1)から(4)、第31条の(1)から(4)、第32条の(1)(2)(3)、第33条(5)、第39条、第41条、第47条、第49条、第53条への違反 → 1,000万ユーロ、または全世界売上の 2.0% のうち高い方の罰金

4. 不正確な情報提示 → 500万ユーロ、または全世界売上の 1.0% のうち高い方の罰金

Open-source softwareと Open-source software Steward

Open-source softwareの定義

- **フリー・オープンソースソフトウェア(free and open-source software)**
  ソースコードがオープンに共有され自由にアクセスし、使用し、改変し、再配布できるようにするすべての権利を提供するフリー・オープンソースライセンスの下で利用可能にされたソフトウェア（Article3(48)）

  製造者が商業活動の一環として収益化し提供される場合のみ、CRA の適用対象となる非営利団体による開発は、収益が非営利目的に使用される場合、商業活動とみなされない（前文(18)）

この条項は、オープンソース プロジェクトやコミュニティへの貢献がCRA の対象外であることを明確にし、既存のオープンソース プロジェクトへの貢献に対する障壁を生じさせないことを保証

Open-source software stewardの定義

- **オープンソース・ソフトウェア・スチュワード(open-source software steward)**
  製造業者以外の法人でフリーかつオープンソースソフトウェアとして適格であり、商業活動を目的としたデジタル要素を含む特定の製品の開発に対して、体系的な支援を継続的に提供する目的または目標を持ち、それらの製品の実行可能性を保証するもの（Article3(14)）

  CRAでは製造業者とオープンソース ソフトウェア スチュワードの役割を明確に区別しており、製造業者はEU市場でデジタル要素を含む製品を商業的に提供する責任がある主体で、オープンソース ソフトウェア スチュワードはオープンソース製品の開発を体系的に支援し、その実行可能性を確保する組織
  この定義は単なる個人開発者や非営利的な貢献者ではなく、OSSの品質とセキュリティを保証する役割を担う組織的存在を対象としている

無料で提供されるソフトウェアのサイバーセキュリティ機能に対して、スチュワードが責任を負うことは困難であり、
CRA はこの課題を認識し、特定の商業製品におけるオープンソース コンポーネントの目的適合性について適切なデューデリジェンス評価を行う責任を、その製品の製造業者に課している

Open-source software steward導入の目的

CRAが要求しているサイバーセキュリティ対策を全てのオープンソースソフトウェア開発に課すとオープンソース プロジェクトやコミュニティの成長を阻害する障壁となってしまうため、CRAではオープンソースソフトウェアスチュワードという新しい概念を導入し、非営利のオープンソースソフトウェア開発への影響を最小限にしつつ、オープンソースソフトウェア開発者やコミュニティと利用者（デジタル要素を含む製品の製造業者）間との責任分担の明確化と連携強化を図っている。

＜CRA義務の有無＞

区分	CRAの義務	備考
一般のOSS開発者	❌ 基本的に無し	非営利・個人開発者など
OSSスチュワード	✅ 該当する可能性あり	商用支援・配布・管理を行う場合
商用製品の製造者（OSSを含む）	✅ 義務あり	OSSを含む製品をEUで販売する場合

※参考：オープンソースにおけるサイバーセキュリティベストプラクティスへの道(Linux Foundation)

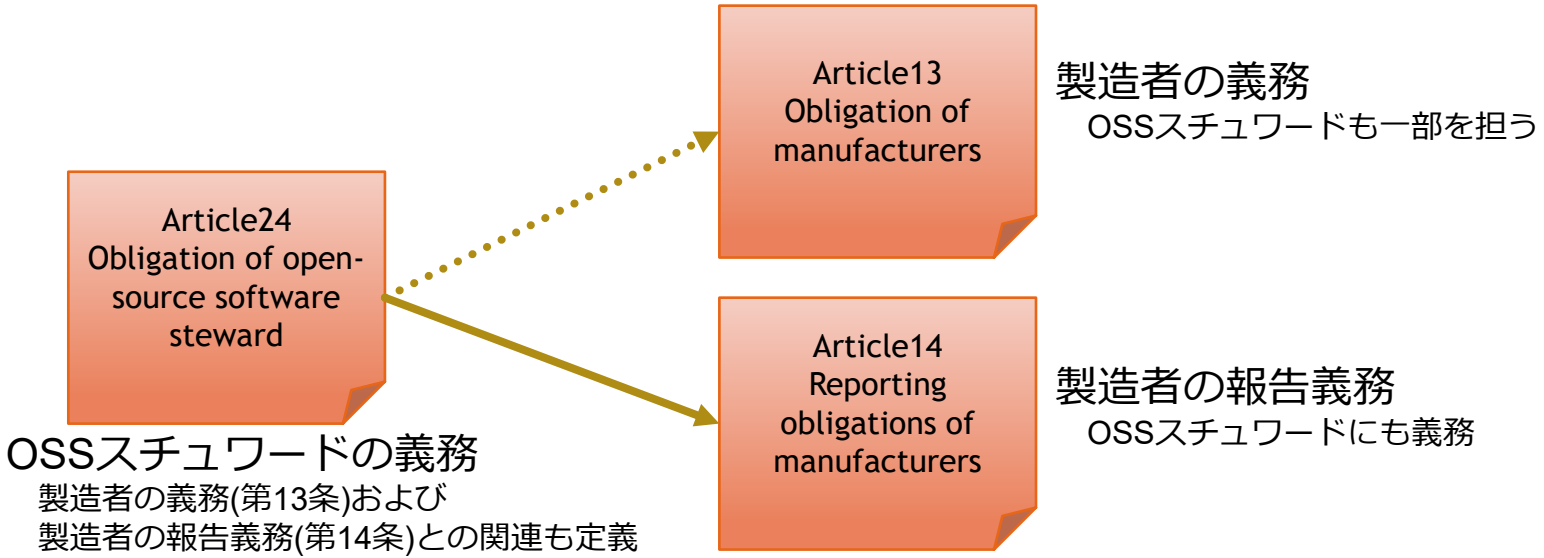
Open-source software Stewardの義務

Open-source software Stewardの義務(第24条)

- デジタル要素を含む安全な製品の開発およびその製品の開発者による脆弱性の効果的な取り扱いを促進するために、サイバーセキュリティポリシーを策定し検証可能な方法で文書化しなければならない
  ポリシーには脆弱性の文書化、対処および修正に関する内容を含めなければならない(第1項)
- 市場監視当局（MSA）の要請に応じサイバーセキュリティリスクの軽減を支援しなければならない
  MSAから合理的な要請があった場合には、セイバーセキュリティポリシーをMSAが容易に理解できる言語で紙または電子形式でMSAに提供しなければならない(第2項)
- .第14条第1項の義務は、デジタル要素を含む製品の開発に関与している範囲で適用される
  第14条第3項、第8項の義務は、セキュリティに影響を与える重大なインシデントが、オープンソースソフトウェアの管理者が提供するネットワークおよび情報システムに影響を与える範囲で適用される（第3項）

この条文では、商業的文脈で提供されるOSSに関与するスチュワードに対して、セキュリティ確保のための具体的な責任が明記されている

Open-source software Stewardの義務と第13条、第14条



製造者の義務
OSSスチュワードも一部を担う

製造者の報告義務
OSSスチュワードにも義務

OSSスチュワードの義務
製造者の義務(第13条)および
製造者の報告義務(第14条)との関連も定義

第24条ではOSSスチュワードの義務が定められており、第24条に従い第13条および第14条の製造者の義務の一部もOSSスチュワードの義務と扱われる

CRA 第13条 製造業者の義務

※赤字：OSSスチュワードの義務に関連がある条文

1. デジタル製品を市場に出す際、附属書Iの１「セキュリティ特性要件」を遵守して設計・開発・製造 されていることを確認する。
2. サイバーセキュリティ上のリスクアセスメントを実施し、その結果を設計・開発・製造・配送・メンテナ ンスの際の考慮に入れる。
3. デジタル製品を市場に出す際、上記のリスクアセスメントの結果を技術文書に含める。
4. 第31条および付属書VIIIに従って要求される技術文書には、本条第3項で言及されるサイバーセキュリティリスク評価を含める。
5. **第三者から提供された部品を使用する際は、その部品により製品のセキュリティリスクを高めないことを保証する。**
6. **特定した脆弱性を報告・対処・修復する。対処のための変更は機械可読形式でコンポーネントの製造または保守を行う個人または団体と共有する。**
7. デジタル製品に関するサイバーセキュリティ観点の情報を体系的に文書化する。
8. サポート期間は5年間と製品の使用期限のうち短い方とし、期間内は製造業者は脆弱性に効果的に対処する。製造業者は脆弱性開等に適切なポリシーや手続きを有する。
9. セキュリティアップデート公開から10年間、またはサポート期間のいずれか長い方の期間、セキュリティアップデートを利用可能とする。
10. 大幅な変更バージョンは付属書 I、パート II、ポイント (2) の必須要件に準拠すればよい。最新バージョンへは無料でアクセスでき、旧バージョンユーザーが環境調整コストなしで適用できること。
11. ユーザーが過去のバージョンおよびサポート外ソフトウェアの使用に伴うリスク情報にアクセスできるようにする。
12. 上市前に製造業者は技術文書を作成する。対応する適合性評価手続きを行い、適合性が実証された場合はCEマーキングを貼付する。
13. 上市後10年間、技術文書と（該当する場合は）EU適合性証明書を市場監視当局が自由に使えるように保管する。
14. 一連の製造の中で、適合性を維持するための手順が整備されていることを確認する。
15. 製品の個体識別のため型番、バッチ番号、シリアル番号などを付記する。
16. 製品に製造業者の名前、商標、郵便住所、電子メールアドレスなどのデジタル連絡先、ウェブサイトなどを表示する。
17. 脆弱性報告ための単一の連絡先を附属書 II に記載されているユーザーへの情報および指示に記載する。連絡先はユーザーが通信手段を選択できるようにし、手段を自動化ツールに限定してはならない。
18. 附属書 II に定めるユーザーへの情報および説明書を紙または電子形式で添付する。情報および説明書は10年間とサポート期間の長い方の期間保持し、オンライン提供の場合はアクセス可能とする。
19. 購入時に、第8項のサポート期間の終了日へアクセスできるようにする。可能であれば、製造業者はサポート期間の終了をユーザーに通知する。
20. EU適合性証明書か簡易EU適合宣言を提供する。簡易宣言の場合は完全なEU適合宣言へのURLを提供する。
21. サポート期間内に附属書ＩＩ「セキュリティ特性要件」を遵守しない場合、直ちに必要な是正措置を講じ製品の撤回またはリコールを行う。
22. 市場監視当局からの要求に応じて製品の適合性を証明する情報・文書を提出する。
23. 操業を停止し義務を遵守できなくなる場合、操業停止前に市場監視当局やユーザに通知する。
24. 欧州委員会は実施法の中で、SBOMの形式と要素を指定することができる。
25. ADCO は製品のフリーソフトウェアおよびオープンソースソフトウェアへの依存度評価の実施を決定できる。市場監視当局は附属書I第II部ポイント(1)のSBOM 提供を要求できる。

CRA 第14条 製造業者の報告義務

※赤字：OSSスチュワードの義務に関連がある条文

1. **悪用されている脆弱性を認識した場合は第7項に従い CSIRT と ENISA に同時に通知する。**
2. 第1項の通知では以下を提出する。
   (a) 脆弱性を認識してから24時間以内に早期警告通知
   (b) 脆弱性を認識してから72時間以内に、製品の一般情報、悪用の性質、講じられた・またはユーザーが講じられる是正・緩和措置を含む脆弱性通知
   (c) 是正措置または緩和措置が利用可能になってから14日以内に以下を含む最終報告書
      (i) 脆弱性の説明（その深刻度および影響を含む）
      (ii) 入手可能な場合、脆弱性を悪用した悪意のある行為者に関する情報
      (iii) 脆弱性修正のためのセキュリティアップデートまたはその他の是正措置に関する詳細
3. **製品のセキュリティに影響を与える重大なインシデントを認識した場合は第7項に従い CSIRT と ENISA に同時に通知する**
4. 第3項の通知では以下を提出する。
   (a) インシデントを認識してから24時間以内に早期警告通知。違法または悪意のある行為により比企侵された疑いがあるかを含む
   (b) インシデントを認識してから72時間以内に、インシデントに関する一般情報と初期評価、講じられた・またはユーザーが講じられる是正・緩和措置を含むインシデント通知
5. 以下の場合インシデントは重大とみなす。
   (a) 機密性の高いまたは重要なデータや機能の可用性、真正性、完全性、または機密性を保護する能力に悪影響を及ぼす可能性がある
   (b) ユーザーのネットワークおよび情報システムにおいて悪意のあるコードの導入または実行につながる可能性がある
6. CSIRT は現在悪用されている脆弱性や重大なインシデントに関する中間レポートの提供を製造元に要求する場合がある。
7. 第1項と第3項の通知は、第16条で規定する単一の報告プラットフォームを介して提出される。
8. **積極的に悪用されている脆弱性または重大なインシデントを認識した場合、これらについてユーザーに通知する。**
9. 本法案発効日から12ヶ月以内に欧州委員会は第61条に委任行為を採択する。
10. 欧州委員会は、通知された情報の種類、形式、手順を更に指定することができる。

Article13 とOpen-source software Stewardの義務

- 製造業者は、第三者から調達したコンポーネントを統合する際に、当該コンポーネントが製品のサイバーセキュリティを損なわないようデューデリジェンスを実施しなければならない
  これには、商業活動の一環として市場に出されていないフリーおよびオープンソースソフトウェアのコンポーネントも含まれる（Article13(5)）
  OSSスチュワードが提供するOSSが製品に統合される場合、そのセキュリティ品質や脆弱性管理の体制が問われるため(Article24)、間接的にこの条文の対象
- 製造者は、オープンソースコンポーネントを含むデジタル要素とともに製品に組み込まれたコンポーネントの脆弱性を特定した場合、そのコンポーネントの製造者または保守者に報告し、脆弱性に対処・是正しなければならない（Article13(6)）
  OSSスチュワードはOSSの保守者として脆弱性報告の受け手となる可能性があり、報告を受けた後の対応責任が生じる

OSSスチュワードが直接的に製品を市場に出していなくても、そのOSSが製品に組み込まれることでCRAの義務の一部を担う可能性がある

Article14 とOpen-source software Stewardの義務

- 製造業者は、積極的に悪用される脆弱性を認識した場合、ENISAおよび指定されたCSIRTに対して、遅滞なく報告しなければならない（Article14(1)）
  この義務はデジタル要素を含む製品の開発に関与している範囲で適用される（Article24(3)）
- 製造者は、製品のセキュリティに影響を及ぼす重大なインシデントを認識した場合、ENISAおよび指定されたCSIRTに対して、遅滞なく報告しなければならない（Article14(3)）
  この義務はセキュリティに影響を与える重大なインシデントが、その製品の開発のためにOSSスチュワードが提供するネットワークおよび情報システムに影響を及ぼす限りにおいて適用される（Article24(3)）
- 製造業者は、積極的に悪用される脆弱性や製品のセキュリティに影響を及ぼす重大なインシデントを認識した場合、影響を受けるユーザーに通知し必要に応じリスク緩和策を提供する必要がある
  この義務はセキュリティに影響を与える重大なインシデントが、その製品の開発のためにOSSスチュワードが提供するネットワークおよび情報システムに影響を及ぼす限りにおいて適用される（Article24(3)）

これらの条文の義務は、Article24（OSSスチュワードの義務）の3項で定義された範囲で適用される

Open-source software StewardのCRA対応ガイド

1. セキュリティポリシーと開発体制の整備（第24条）
   - セキュリティポリシーを文書化・公開
2. 脆弱性管理と報告体制の構築（第13条・第24条）
   - 脆弱性報告窓口の設置
   - 脆弱性の評価・修正・公開のプロセス整備
   - ENISAや製品製造者からの報告に対応できる体制構築
3. SBOM（ソフトウェア部品表）の提供支援（第13条）
   - OSSのバージョン、依存関係、ライセンス情報等の情報を機械可読形式で提供
4. セキュリティアップデートの提供（第13条）
   - 既知の脆弱性に対するセキュリティアップデートの提供
   - 長期サポート（LTS）バージョンの提供の検討
5. 市場監視機関（MSA）との連携準備（第24条）
   - 法的通知や問い合わせに対応する責任者を明確化
   - MSAの要請に応じて技術文書やセキュリティ情報を提出できる体制を整備
6. 技術文書と証跡の整備（第13条）
   - セキュリティ設計、リスク評価、脆弱性対応履歴を記録
   - OSSがCRA附属書Ⅰの要件を満たすことを示す文書の準備

最新動向

CRA関連の最新動向

- ## Harmonized Stadards（整合規格）

  欧州委員会はデジタル製品がEU官報に掲載された整合規格に適合している場合、CRAのサイバーセキュリティ要件に適合していると推定する。欧州委員会は整合規格の策定を１つ以上の欧州標準化機関に要請する。（第27条１項）

  2025.4.3 欧州委員会からの要請をCEN/CENELEC、ETSIが正式に受理
  ・2027年12月11日の1年前までに整合規格を準備
  ・Horizontal Standards（製品カテゴリ非依存）とVertical Standards（製品カテゴリ別）の２つのクラスに分けて策定
  ・採択予定
  Horizontal Standards：2026年8月,Vertical Standards：2026年10月 Interview – convenor of CEN-CENELEC Joint TC 13 – Working Groups 6 and 9

- ## CISA 2025 SBOM minimum elements 2025 Minimum Elements for a Software Bill of Materials (SBOM)

  NTIAの役割をCISAが引き継ぎ、NTIA Minimum Elements* では脆弱性管理の観点では情報不足との判断でCISA版のMinimum Elements(Draft版)を2025年8月にリリース。（現NTIA Minimum Elementsが失効する訳ではなく、どちらを採用するかはRegulationで決まる）今年中に正式版をリリースの意向。

  *NTIA Minimum Elements:米大統領令14028の下でNTIA（National Telecommunication s and Information Administration)により発行され、米政府調達要件に採用

LF Trainingの紹介

EU CRAに関するLF Trainingコースの提供が開始されました（無料）

Understanding the EU Cyber Resilience Act(CRA)(LFEL1001)

Thank you