CRA EVIDENCE ホワイトペーパー

EUサイバーレジリエンス法：実務対応ガイド

デジタル要素を含む製品の製造業者、輸入業者、販売業者向けホワイトペーパー。

作成	CRA Evidence
バージョン	1.0
ステータス	生きた文書
根拠	EU規則2024/2847

変更履歴

本書は生きた文書です。規則、当局のガイダンス、整合規格の動向に応じて更新します。

バージョン	日付	説明
1.0	2026年5月17日	初版公開。適用範囲、分類、実質的変更、必須要件、脆弱性ハンドリング、技術文書、適合性評価ルート、AI Act / Data Act / ESPR / 製造物責任との関係を扱う。

目次

要約

60秒で要点

対象： EU市場で提供される接続型ハードウェアとソフトウェア製品です。サイバーセキュリティは任意の実務ではなく、製品コンプライアンス要件として扱われます。

発効タイミング： 第14条の報告義務は2026年9月11日に始まります。技術要件、文書、CEマーキングの主要義務は2027年12月11日から適用されます。

整備するもの： サイバーセキュリティリスク評価、ソフトウェア部品表（SBOM）、技術文書、利用者向け説明、EU適合宣言書、CEマーキング、第14条に基づくインシデント・脆弱性報告です。

誰が対応するか

中心的な責任は製造業者にあります。輸入業者と販売業者は、製品提供前に注意義務として確認を行います。

何が変わるか

サイバーセキュリティは製品コンプライアンスの一部になります。安全設計、脆弱性対応、文書、CEマーキング、上市後対応が必要です。

最初の期限

第14条の報告は、積極的に悪用されている脆弱性と重大インシデントについて**2026年9月11日**に始まります。

全面適用

技術要件は**2027年12月11日**から全面適用されます。既存製品は実質的変更後に対象となりますが、報告義務は引き続き適用されます。

証拠の中核

技術文書には、リスク評価、SBOM、サポート期間の根拠、試験証跡、利用者向け説明、適合宣言書、必須サイバーセキュリティ要件への適合証拠が必要です。

適合性評価ルート

多くの製品はモジュールAで自己評価できます。重要製品とクリティカル製品では、認証機関またはEUサイバーセキュリティ認証が必要になる場合があります。

サイバーレジリエンス法とは

サイバーレジリエンス法（CRA）、正式にはEU規則2024/2847は、EU市場に提供されるデジタル要素を含む製品について、サイバーセキュリティを拘束力のある要件にする初のEU横断的な枠組みです。根拠となる本文はEUR-Lexで確認できます。

CRAは、接続型ハードウェアとソフトウェアの製造業者、輸入業者、販売業者に適用されます。消費者向けIoT機器から産業制御システムまで、幅広い製品が対象です。実務上の変化は明確です。サイバーセキュリティを、製品コンプライアンスの一部として設計し、証跡化し、維持し、監視する体制が必要になります。

必須サイバーセキュリティ要件、または第13条と第14条の義務に違反した場合、最高1,500万ユーロまたは全世界年間売上高の2.5%（いずれか高い額）の制裁金が科される可能性があります。下位の段階も適用されます。他の特定の義務違反は最高1,000万ユーロまたは2%、認証機関や市場監視当局に対する不正確・不完全・誤解を招く情報の提供は最高500万ユーロまたは1%です。市場監視当局は、是正措置、提供制限、撤回、リコールも求めることができます。

対応計画で押さえる日付

CRAは**2024年12月10日**に発効しました。実務上の対応は、**2026年6月**の認証機関、**2026年9月**の報告、**2027年12月**の技術要件全面適用という三つの節目で進みます。

注記

欧州委員会ガイダンスの現状： 欧州委員会は2026年3月3日、CRAドラフトガイダンスを公表しました。意見募集は2026年4月13日に終了しました。最終版ではありませんが、上市、自由・オープンソースソフトウェア、サポート期間、実質的変更、製品分類、コンポーネントのデューデリジェンス、リモートデータ処理、脆弱性ハンドリング、他のEU法令との重なりを検討する際の計画材料になります。AI ActとDORAとの境界は、今後のガイダンスが必要になる可能性があります。

2024年12月10日
発効
移行期間の開始

2026年6月11日
認証機関
第IV章の適用開始

2026年9月11日
報告
第14条報告の開始

2027年12月11日
全面適用
技術要件、CEマーキング、文書、適合性評価

最初に行うこと

まず報告体制から着手します。第14条の期限は技術要件の全面適用より早く、すでにEU市場にある対象製品にも及びます。

報告は**2026年9月11日**に始まるため、まず報告体制を整える必要があります。**検知、トリアージ、利用者通知、当局報告**は、技術要件の全面適用前に機能していなければなりません。

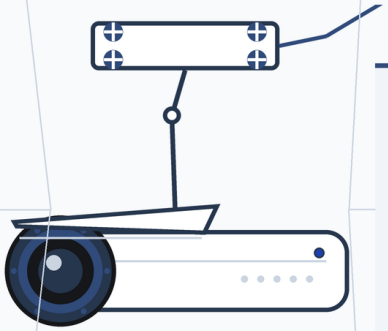
2027年12月11日より前に上市されたデジタル要素を含む製品は、同日以降に**実質的変更**を受けた場合にのみ、CRAの技術要件の対象となります。報告は別です。第14条は対象範囲のすべての製品に適用され、すでにEU市場にある製品も含まれます。

製品ライフサイクル上のCRA

ステップ 01
製品範囲を決める
適用範囲、分類、サポート期間、リスク評価

ステップ 02
安全に開発する
安全な初期設定、コード解析、SBOM、依存関係の管理

ステップ 03
検証し文書化する
セキュリティ試験、脆弱性トリアージ、技術文書、利用者向け説明



ステップ 04
市場投入する
EU適合宣言、CEマーキング、リリース判断

ステップ 05
監視し更新する
CVE、助言、悪用状況、セキュリティ更新、開示

ステップ 06
支援し協力する
第14条報告、利用者通知、当局からの要請、サポート終了

接続型IPカメラを、製品計画からCRA上の市販後サポートまで追跡

対象となる製品

適用範囲と除外

CRAは、意図された使用または合理的に予見可能な使用において、機器またはネットワークとの直接または間接のデータ接続を含むハードウェア・ソフトウェア製品に適用されます。コンピューター、スマートフォン、ネットワーク機器、IoT機器、産業制御システム、データ処理アプリケーションが含まれます。

次のカテゴリは明示的に除外されています。

- EU規則2017/745および2017/746の対象となる医療機器、体外診断用医療機器
- EU規則2019/2144の対象となる自動車システム
- EU規則2018/1139の対象となる航空機器
- 指令2014/90/EUの対象となる船舶機器
- 国家安全保障または防衛目的だけで開発された製品
- デジタル要素やネットワーク接続を持たない純粋な機械製品

明確な除外がない場合、接続型製品は対象として扱う前提で確認します。

注記

特注製品の限定的な適用除外： 個別の事業利用者向けに、書面合意に基づいて構築する製品については、二つの要件のみ別段の取り扱いができます。セキュアなデフォルト設定（ただし、安全な初期状態に戻せる手段は確保する必要があります）と、無償のセキュリティ更新（合意で異なる商業条件を定められます）の二つです。その他はすべて全面的に適用されます。脆弱性ハンドリング、その他の製品セキュリティ要件、第14条の報告、技術文書、CEマーキング、適合性評価、サポート期間は引き続き必要です。これは一般的なB2B向けの適用除外ではなく、事業者向けに販売される既製品には適用されません。

経済事業者の責任

製造業者	安全な製品を設計し、リスクを評価し、技術文書を準備し、適合性評価を行い、脆弱性を処理し、第14条事象を報告します。
輸入業者	製造業者の対応を確認し、CEマーキングと文書を検証し、宣言書を利用可能にし、既知の脆弱性に対応します。
販売業者	供給前の注意義務を確認し、必要な情報と説明を検証し、不適合製品を提供しません。

製品分類が評価ルートを決める

製品カテゴリにより、適合性の示し方が変わります。

カテゴリ	例	適合性評価
標準「未分類」	重要またはクリティカルに該当しない一般的なソフトウェアと接続型消費者向け製品	モジュールA：自己評価
重要「クラスI」	ID管理、ブラウザー、パスワード管理、ウイルス対策、VPN、ネットワーク管理、ルーター、スマートロック、セキュリティカメラなど	適用可能な整合規格、共通仕様、認証スキームを必要な形で使う場合に限りモジュールA。それ以外はモジュールB+CまたはモジュールH
重要「クラスII」	ハイパーバイザー、コンテナランタイム、ファイアウォール、IDS/IPS、耐タンパー性マイクロプロセッサー	モジュールB+C、モジュールH、または「substantial」以上の保証レベルの欧州サイバーセキュリティ認証スキーム
クリティカル製品	セキュアエレメント、スマートカード、スマートメーターゲートウェイ、ハードウェアセキュリティボックス	利用可能で必要な場合は欧州サイバーセキュリティ認証。それ以外はクラスIIルート

4つの製品カテゴリ

上の表は例示です。製品のコア機能を比較する完全な参照は、以下のとおりです。

標準製品

ほとんどの製品はここに該当します。デジタル要素を含む製品のうち、コア機能が下記の重要またはクリティカルのリストに該当しないものは、すべて標準として扱います。適合性評価はモジュールAの自己評価です。

代表例：

- スマートTV、ストリーミング機器
- ネットワークプリンター、複合事務機
- Bluetoothスピーカー、消費者向け音響製品
- メディアプレーヤーアプリケーション
- ゲーム機、電子書籍リーダー、その他の家電
- セキュリティ機能のないスマートオーブン、冷蔵庫、食洗機などのスマート家電
- セキュリティ機能のないスマート電球、接続照明
- ヘルスモニタリング目的を持たないフィットネストラッカー
- ブラウザー、パスワード管理、VPNアプリではない汎用モバイルアプリ
- ワープロや表計算ソフトなどのオフィス用ソフトウェア

上記は例示です。下記の重要およびクリティカルのリストは網羅的です。

重要製品（クラスI）

第三者評価が必須です。ただし、適用可能な整合規格、共通仕様、認証スキームを必要な形で使う場合は除きます。

1. ID管理および特権アクセス管理のソフトウェア・ハードウェア。認証とアクセス制御のリーダー（生体認証を含む）を含みます。
2. スタンドアロン型および組み込み型のブラウザー。
3. パスワード管理。
4. 悪意あるソフトウェアを検索、削除、隔離するソフトウェア。
5. VPN製品。
6. ネットワーク管理システム。
7. セキュリティ情報イベント管理（SIEM）システム。
8. ブートマネージャー。
9. 公開鍵基盤と電子証明書発行のソフトウェア。
10. 物理および仮想ネットワークインターフェース。
11. オペレーティングシステム。
12. ルーター、インターネット接続用モデム、スイッチ。
13. セキュリティ関連機能を持つマイクロプロセッサー。
14. セキュリティ関連機能を持つマイクロコントローラー。

15. セキュリティ関連機能を持つASICとFPGA。
16. スマートホームの汎用バーチャルアシスタント。
17. セキュリティ機能を持つスマートホーム製品（スマートドアロック、セキュリティカメラ、ベビーモニター、警報システム）。
18. インタラクティブ機能を持つインターネット接続玩具（発話、撮影、位置追跡）。
19. ヘルスモニタリング目的のパーソナルウェアラブル（EU規則2017/745または2017/746が適用されない場合）、または子供向けに意図されたウェアラブル。

重要製品（クラスII）

第三者評価が必須です。整合規格が存在する場合でも自己評価は使えません。

1. オペレーティングシステムなどの仮想化実行を支援するハイパーバイザーと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・防止システム。
3. 耐タンパー性マイクロプロセッサー。
4. 耐タンパー性マイクロコントローラー。

クリティカル製品

スキームが利用可能な場合は欧州サイバーセキュリティ認証が必須です。それ以外はクラスIIルートが適用されます。

1. セキュリティボックス付きハードウェア機器。
2. 指令（EU）2019/944 第2条第23号で定義されるスマートメーターシステムにおけるスマートメーターゲートウェイ、その他、安全な暗号処理を含む高度なセキュリティ目的の機器。
3. スマートカードと同種の機器、セキュアエレメントを含みます。

製品のコア機能が重要またはクリティカルのリストに該当する場合、そのクラスに分類されます。製品がリスト掲載の製品をコンポーネントとして統合していても、製品自体のコア機能が別である場合、統合してもクラスは変わりません。

分類の考え方：コア機能で見る、統合では見ない

上記のリストはカテゴリを示します。リストを自社製品に当てはめる方法までは示していません。CRAの答えは一つの用語に集約されます。**コア機能**です。

クラスは、製品が統合するコンポーネントではなく、製品のコア機能によって決まります。コア機能を重要リストと突き合わせて該当すれば重要（クラスIまたはII）、クリティカルリストと突き合わせて該当すればクリティカル、いずれにも該当しなければ標準です。これがテストのすべてです。

実務上の安全装置は、第7条第1項の第2文にあります。重要なコンポーネントを統合しても、統合する製品が重要クラスに格上げされるわけではありません。スマートホームハブにファイアウォールライブラリを組み込んでも、ハブがファイアウォールになるわけではありません。前文第45項が平易に述べています。ファイアウォールと侵入検知システムは重要クラスIIですが、それらを統合する他の製品は重要にはなりません。

自己分類は次の順序で進めます。

1. **製品のコア機能を一文で表現します。** これができない場合、以降の分析は成り立ちません。製品がそれなしには機能しないものに焦点を当てます。
2. **上記の重要リストを確認します。** クラスIまたはIIに該当すれば、製品は重要です。
3. **上記のクリティカルリストを確認します。** 該当すれば、製品はクリティカルです。スキームが利用可能な場合は欧州サイバーセキュリティ認証ルート、そうでない場合はクラスIIルートが適用されます。
4. **どちらにも該当しない場合。** 製品は標準で、モジュールAの自己評価が経路です。
5. **判断の根拠を文書化します。** コア機能の宣言、リスト確認、選択した経路を記した1ページのメモを技術文書に含めます。

具体例を2件示します。

パスワード管理を組み込んだスマートホームハブ。 コア機能は、家庭内の消費者向けIoT機器を横断してルーチンを統括することです。パスワード管理コンポーネントは、製造業者から別途販売される、それ自体が重要クラスI製品です。ハブのコア機能はホームオートメーションであり、認証情報管理ではありません。ハブは標準のままです。

機能セットで判断するオペレーティングシステム。 ある製品はスマートホーム家電として販売されていますが、主な機能はハードウェアと周辺機器の初期化、プロセススケジューリング、メモリ管理、システムコールインターフェースです。これはオペレーティングシステムのコア機能です。オペレーティングシステムは重要クラスI製品です。マーケティング上の位置付けに関わらず、製品は重要クラスIです。

分類結果がチームの想定と大きくかい離する場合、出荷前にコア機能の宣言を再検討する必要があります。

クラウドが製品の一部に含まれる場合

デジタル要素を含む製品の多くは、機器外の何かに依存します。クラウドバックエンド、モバイルコンパニオンアプリ、OTA更新サーバー、認証ポータル、機器管理システムなどです。CRAはこれらすべてを製品の一部として扱うわけではありません。製品の一部として扱われるのは、次の**両方**が成り立つ場合だけです。

- そのソフトウェアが、**自社チームまたは自社の責任のもとで**設計・開発されている。
- それなしでは、**製品がその機能のいずれかを実行できない**。

どちらかが満たされない場合、その遠隔サービスはCRAの製品境界の外側にあります。製品が通信していても、自社が所有していない第三者SaaSは製品の一部ではありません。製品を宣伝するが製品の機能を支えないWebサイトも、製品の一部ではありません。

遠隔コンポーネントが対象範囲内にある場合、それは**製品の一部として**対象になります。技術文書、適合性評価、適合宣言書、脆弱性ハンドリング、第14条の報告タイムラインのすべてが、機器とともにクラウドコンポーネントもカバーします。

次のマトリクスで判断を素早く行います。

コンポーネント	製品の一部として対象範囲内か
機器とペアリングするモバイルコンパニオンアプリ	**はい。** 自社が設計しており、機器のセットアップや利用に必要です。
機器のデータを保存・処理するクラウドバックエンド	**はい。** 自社が設計しており、ダッシュボードや主要機能に必要です。
OTA更新サーバー	**はい。** 自社が設計しており、機器がセキュリティ更新を受け取るために必要です。
機器へのアクセスを制御する認証ポータル	**はい。** 自社が設計しており、利用者のログインに必要です。
製品のマーケティングサイト	**いいえ。** 製品機能を支えていません。
製品が連携する第三者SaaS（自社所有ではない）	**いいえ。** 自社が設計していません。第三者プロバイダーがNIS 2のもとで独自の義務を負います。
サービスを動かす汎用クラウド基盤（IaaSまたはPaaS）	**いいえ。** 自社が設計していません。基盤プロバイダーはNIS 2の対象です。

よくあるパターンとして、モバイルアプリ、更新サーバー、クラウドバックエンドを伴うスマートホーム機器があります。3つすべてが製造業者の設計によるもので、機器はそれらなしでは宣伝されている機能を実行できません。3つすべてが製品の一部です。CRA義務はバンドル全体に適用されます。クラウドバックエンドが第三者の分析SaaSと通信する場合、そのSaaSは製品の一部ではありません。第三者プロバイダーはNIS 2のもとで独自の義務を負います。

CRAは、製造業者のネットワークと情報システム全体にセキュリティ対策を求めるものではありません。製品の一部である遠隔サービスについてセキュリティを求めます。境界は会社の境界ではなく、製品の境界です。

サプライチェーン：CRAのもとでの役割分担

CRAは主要な義務を製造業者に課しますが、輸入業者と販売業者も製品が市場に届くまでの過程で義務を負います。製造業者として把握しておくべき点が3つあります。

担い手	供給前に確認する事項	脆弱性発生時の対応	製造業者の義務を引き継ぐ場面
輸入業者	CEマーキング、EU適合宣言書、適切な言語の利用者向け説明、製品上または同梱の連絡先	過度の遅延なく製造業者に通知。製品が重大なサイバーセキュリティリスクを示す場合は市場監視当局に直接通知	自らの名称または商標で製品を提供する場合、または実質的に変更する場合
販売業者	CEマーキング、製造業者と輸入業者の対応完了、製品に必要書類が同梱されているか	過度の遅延なく製造業者に通知。重大なリスクがある場合は市場監視当局に直接通知。製品提供を停止することも可能	輸入業者と同じ条件

製造業者にとって、実務上の要点は3つあります。

- CEマーキング、EU適合宣言書、利用者向け説明は、販売業者が確認する時点で正確かつ適切な言語で揃っている必要があります。流通パートナーはこれらを検証する義務があり、欠落や誤りがあれば製品提供を拒否できます。
- 輸入業者と販売業者が脆弱性を報告できる、低摩擦で明確な連絡経路を用意します。実際に使われます。
- 自らの名称や商標で製品を提供する、または実質的に変更するパートナーは、そのバージョンの製造業者になります。技術文書、適合性評価、報告、サポート期間に関する義務のすべてが、そのバージョンについてその担い手に移ります。実質的変更ルールは次のセクションの「他者が製造業者になる場合」で扱います。

実質的変更：再適合が必要となる場面

製品を上市した後、CRAは後続の変更を2つの区分に分けます。多くは通常の運用で、追加対応は不要です。一部は実質的変更です。実質的変更は、CRA上、新製品を上市したものとして扱われます。これは、適合性評価の再実施、技術文書の更新、新たな適合宣言書、新バージョンへのCEマーキングを意味します。

判定は短く、実質的変更の定義に置かれています。次のいずれかが成り立つ場合、変更は実質的です。

- 必須サイバーセキュリティ要件への**適合に影響する**。
- 製品が評価された**意図された目的を改変する**。

どちらにも該当しない場合、変更は実質的ではありません。それでも判断の根拠を文書化し、ファイルに残します。この分析は証拠の一部です。

実質的に該当しないもの

実務上、適用除外が大きな役割を果たすケースが2つあります。

意図された目的を変えずにサイバーセキュリティリスクを減らすセキュリティ更新とバグ修正は、実質的ではありません。既知の脆弱性のパッチ適用、欠陥を塞ぐための入力検証の調整、CVEに対処するコンポーネントの再ビルドは、いずれもこの側に該当します。

リファービッシュ、メンテナンス、修理も自動的には実質的になりません。これらは、意図された目的を変える、または必須サイバーセキュリティ要件への適合に影響する場合に限り、実質的になります。

軽微なユーザーインターフェース作業も、安全側にあります。言語追加、アイコンセットの差し替え、画面レイアウトの調整は、それ自体では実質的変更ではありません。適切な入力検証が必要な新しい入力要素の追加は、実質的になる場合があります。

スペアパーツ

CRAはスペアパーツを限定的かつ具体的に適用除外しています。置き換える部品と同一仕様で作られた**同一スペアパーツ**は、規則の対象外です。機能的な代替品はそうではありません。

次のマトリクスで判断を素早く行います。

代替品	2027年12月11日より前に上市された本体	2027年12月11日以降に上市された本体
元コンポーネントと**同一仕様**	スペアパーツはCRA対象外。交換による義務は発生しません。	スペアパーツはCRA対象外。交換による義務は発生しません。
機能的に同等、設計や仕様が異なる	代替品自体が独立したCRA製品。本体は適用開始日より前のためCRA義務を負いません。	代替品はCRA製品。本体への組み込みが本体の実質的変更に当たるかを、上記の2段テストで評価します。

実務上の影響は2点あります。第1に、適用除外は同一仕様であることに依存します。利用者には違いが分からなくても、別のチップセットで作り直された無線モジュールは同一スペアではありません。第2に、機能的代替品を供給する製造業者は、本体を誰が作ったかに関わらず、その部品についてCRA義務を負います。

ソフトウェア更新と機能フラグ

ソフトウェアリリースは、実質的変更の判断が最も多く問われる場面です。2段テストはこの判断にも適用されます。

脆弱性を修正するパッチは実質的ではありません。製品が評価されていない機能を有効化するフィーチャートグルは実質的です。製品が新しい入力カテゴリを判断できるようにするモデル更新も同様です。一つのリリースに修正と新機能の両方が含まれる場合、新機能を評価します。

バンドルは内容ほど重要ではありません。機能更新が単独で出るか、セキュリティパッチと同じリリースに含まれるかは、判定には関係しません。

フィーチャーフラグや段階的ロールアウトを運用している場合、判定が問われるタイミングはフラグを含むバイナリの出荷時ではなく、本番環境でエンドユーザーへの有効化時です。

実務での判断

すべての変更を出荷前に、次の順序で評価します。

1. **変更は製品の意図された目的を改変するか。** 該当する場合、実質的変更。新バージョンについて適合性評価を再実施します。
2. **変更は必須サイバーセキュリティ要件への適合に影響するか。** 該当する場合、実質的変更。新バージョンについて適合性評価を再実施します。
3. **いずれにも該当しない場合：** 実質的ではありません。分析を文書化し、既存の技術文書のもとで継続します。

製品が重要またはクリティカルクラスに属し、初回に第三者評価ルートが必要だった場合、実質的変更は同じルートでの再評価を求めます。実質的になりそうな変更については、事前に第三者へ通知します。自己評価は、事後的に重要製品を再分類する裏口にはなりません。

実質的変更があった場合の結果

実質的変更は新製品の上市として扱われます。製造業者にとって、これは次を意味します。

- 変更後バージョンの技術文書を更新します。
- 製品クラスが求めるルートで適合性評価を再実施します。
- 変更後バージョンについて新しいEU適合宣言書を発行します。
- 新しい宣言書をファイルに置いたうえでCEマーキングを再付与します。
- 旧バージョンの文書は保持期間を通じて保管します。新バージョンは旧バージョンの記録を消すものではありません。

ソフトウェア製品の場合、サポート期間中のセキュリティ更新の対象を、上市された最新バージョンに限定できます。ただし、旧バージョンの利用者が無償かつ新たなハードウェアなしに最新バージョンへ移行できる場合に限ります。

旧適合のもとで既に出荷された製品は影響を受けません。義務は、変更後バージョンの提供に紐づくものであり、それ以前の同一個体には及びません。

他者が製造業者になる場合

元の製造業者でない者が実質的変更を行う場合、CRAはその者をそのバージョンの製造業者として扱います。第13条と第14条のすべての義務がその者に移ります。同じルールは、自らの名称または商標で製品を提供する場合にも適用されます。

これは、想定以上に多くの場面で発生します。

- 新機能を含む顧客固有のファームウェアビルドを出荷するシステムインテグレーター。
- 製品をホワイトラベル化し、宣伝上の意図された目的を変更する販売事業者。
- 第三者機器を自社ファームウェアでバンドルするサービスプロバイダー。

いずれの場合も、変更を加えた担い手はそのバージョンの製造業者の義務を引き継ぎます。技術文書、適合性評価、報告、脆弱性ハンドリングなどです。「輸入業者」や「販売業者」というラベルは、いずれかの線を越えた瞬間に保護機能を失います。

整備しておくべき項目

このセクションは作業用チェックリストとして使えます。要件ごとの詳細は後続セクションで扱います。

サイバーセキュリティリスク評価

製品を上市する前に、サイバーセキュリティリスク評価を技術文書に含めます。これは、製品を出荷し市場に置き続ける根拠を、自社の言葉で説明する文書です。

評価には次を含めます。

- 製品の意図された目的と、合理的に予見可能な使用ケース
- 製品が運用される条件と環境
- 保護すべきデータと機能
- 適用される脅威と、対応に使う制御策
- 製品が使われると見込まれる期間

多くのチームが採る構成。 信用に値する手法は同じ動きに収束します。資産（製品が扱うデータ、鍵や認証情報などのセキュリティ素材、喪失が利用者に損害を与える機能）を特定し、各資産の所在や流れをマッピングし、機密性、完全性、可用性の軸で資産と環境ごとに脅威をモデリングし、影響度と発生可能性を採点し、許容する残留リスクと緩和するリスクを判断し、対策ごとに再評価します。新しい鍵、証明書、認証機能はそれ自体が新しい資産になります。

脅威モデリング。 上記の3つ目は最も技術的な動きで、確立された技法があります。STRIDEは脅威をなりすまし、改ざん、否認、情報漏えい、サービス拒否、権限昇格に分類します。広く使われており、多くの接続型製品に適合します。LINDDUNは個人データを扱う製品向けに範囲を広げ、リンク可能性、識別可能性、否認不可能性、検出可能性、情報開示、利用者の認識不足、不適合を追加します。データ保護制度がCRA義務と重なる場面で有用です。PASTAは事業目的から残留リスク受容までの7段階プロセスを実行します。攻撃像が設計を主導する複雑なシステムで有用です。いずれもCRA固有ではなく、CRAも特定の手法を求めません。製品の露出プロファイルに合うものを選びます。

実装済みの手法を探す場合。 CRAは手法を規定しません。ドイツ連邦情報セキュリティ庁（BSI）は技術ガイドラインTR-03183を公表しており、これは公開されているCRA整合のリスク評価手法として最も詳細なものです。ENISAはより広範なCRA実装ガイダンスを公表しています。

サポート期間を通じて評価を最新の状態に保ちます。脅威像、コンポーネント、利用ケースが変われば、評価もそれに合わせて更新します。

サポート期間の決定

各製品にはサポート期間の定めが必要で、購入時点でその終了日を公表する必要があります。サポート期間は、脆弱性を扱い、セキュリティ更新を提供し、技術文書を最新に保つ期間です。

期間の長さ

最低5年です。製品の使用見込みが5年未満の場合、サポート期間は想定使用期間に合わせます。5年を超えて使われる製品では、より長い使用期間を反映する必要があります。ルーター、オペレーティングシステム、産業用コントローラーなどは、5年を超える期間が妥当となるのが通常です。

考慮する要素

期間を設定する際は、適切なバランスで次を考慮します。

- 製品に対する利用者の合理的な期待
- 意図された目的を含む製品の性質
- このカテゴリに製品寿命を定める既存のEU法令
- 市場の比較可能な製品のサポート期間
- 製品が依存する運用環境の可用性
- コア機能を提供する組み込みコンポーネントのサポート期間
- 製品カテゴリに関するADCOまたは欧州委員会のガイダンス

選定した期間の根拠は技術文書に含めます。市場監視当局はその提示を求めることができます。

公表すべき内容

購入時点でサポート期間の終了日を、少なくとも月と年で、見つけやすい場所に明示します。製品にユーザーインターフェースがある場合、サポート期間の終了時に通知を表示します。

更新の保持

サポート期間中に利用者へ提供された各セキュリティ更新は、提供から少なくとも10年、またはサポート期間の残期間のいずれか長い期間にわたり、利用可能な状態を維持します。

コンポーネントのデューデリジェンス

製品はコンポーネントで構成されます。自社で書いたもの、購入したもの、オープンソースリポジトリから引いてきたものがあります。CRAは適合性について製品全体を対象とするため、コンポーネントも対象です。コンポーネントに脆弱性があれば、それは製品の脆弱性です。コンポーネントがセキュリティ更新を受けなければ、製品も受けません。

製造業者は、自由・オープンソースを含む第三者コンポーネントについてデューデリジェンスを行います。コンポーネントは製品のサイバーセキュリティを損なってはなりません。

どの程度のデューデリジェンスが十分かは、コンポーネントが持つサイバーセキュリティリスクによります。認証を扱うライブラリは、フォントレンダリングのライブラリとは異なります。次の確認のいずれか、またはリスクに見合った組み合わせを使います。

1. **コンポーネントのCEマーキングを確認します。** コンポーネント自体がCRA製品で、供給者が適合を示している場合、コンポーネントにCEマーキングが付されています。これは供給者自身のCRA対応の証拠になります。
2. **セキュリティ更新の履歴を確認します。** 定期的にセキュリティ更新を出すコンポーネントは、何年も沈黙しているものよりも良いリスクプロファイルを持ちます。リリースの頻度と最近のセキュリティアドバイザリーの記録を確認します。
3. **脆弱性データベースに対してコンポーネントを確認します。** 欧州脆弱性データベースや公開CVEデータベースは、コンポーネントに関する既知の事項を示します。パッチのない既知CVEは警告です。
4. **追加のセキュリティ試験を実行します。** 上記で不十分な場合、統合環境でコンポーネントを試験します。静的解析、動的解析、ファジング、または焦点を絞ったセキュリティレビューを使います。

供給者がまだ完全にCRA対象になっていない（CEマーキングが付与されていない）コンポーネントを組み込む場合は、他の3つの確認方法を使います。サプライチェーンの追従が遅れていることを理由に、デューデリジェンス義務が停止することはありません。

ファイルに残す証拠

技術文書では、デューデリジェンスを行ったことを主張するだけでなく、示す必要があります。次を保持します。

- 製品に含まれる第三者コンポーネントのリスト。バージョン特定が可能で、オープンソースも含めます。SBOMが自然な置き場所です。
- 確認した供給者セキュリティ文書。セキュリティポリシー、脆弱性開示プログラム、サポート期間のコミットメントなど。
- コンポーネントが製品内で安全に動作することを示す統合試験報告書。
- 商業供給者との契約またはSLAのセキュリティ条項。脆弱性通知の期限、サポート期間のコミットメント、エスカレーションルールなど。
- コンポーネントのデューデリジェンスで限界が見えた場合に、製品レベルで追加した緩和策の記録。サンドボックス化、権限制限、入力検証、ネットワーク分離など。

コンポーネントに脆弱性を発見した場合

デューデリジェンスまたは上市後監視でコンポーネントの脆弱性を見つけた場合、2つの対応が必要です。第1に、そのコンポーネントを保守する個人または組織に通知します。オープンソースであれば、それは上流プロジェクトです。第2に、自社で発見した他の脆弱性と同じタイムラインで、製品内の脆弱性を扱い、修復します。修正を開発した場合、可能であれば機械可読な形式で、コードまたは文書を保守者と共有します。

CRAは、コンポーネント保守者の対応を待ってから自社の利用者を保護することを認めていません。製品の脆弱性ハンドリングのタイムラインは、上流のものとは独立に進みます。

13の製品セキュリティ要件

デジタル要素を含む製品はすべて、上市時点で13のベースライン要件を満たし、サポート期間を通じてそれを維持する必要があります。これらはCRA上、製品としてのサイバーセキュリティの最低水準です。

13の要件は次のとおりです。

- 上市時点で既知の悪用可能な脆弱性がないこと
- セキュアなデフォルト設定
- 利用者のオプトアウトを含むセキュリティ更新（自動更新を含む）
- 不正アクセスからの保護
- 保存、送信、処理されるデータの機密性
- データ、ファームウェア、設定の完全性
- データ最小化
- サービス拒否攻撃への対策を含む可用性とレジリエンス
- 他の接続機器またはネットワークへの悪影響の最小化
- 外部インターフェースを含む攻撃面の限定
- 悪用緩和策によるインシデント影響の低減
- 利用者のオプトアウトを含むセキュリティ関連活動の記録

- 安全で恒久的なデータ削除とポータビリティ

各要件は、ガイド後段で実務上の意味と保持すべき証拠とともに詳述します。

8つの脆弱性ハンドリング要件

製造業者は、製品のサポート期間を通じて稼働する脆弱性ハンドリングプロセスも必要です。

1. 脆弱性の特定と文書化（SBOMを含む）
2. リスク管理と適時のセキュリティ更新
3. 定期的なセキュリティ試験
4. セキュリティ更新と脆弱性開示に関する通知
5. 協調的脆弱性開示（CVD）ポリシー
6. 脆弱性共有と報告窓口
7. 安全な更新配布メカニズム
8. 助言メッセージ付きの無償セキュリティ更新

第14条の報告タイムライン

これらの義務は**2026年9月11日**から適用されます。対象となるデジタル要素を含む製品の製造業者に適用され、**2027年12月11日**より前に上市された製品も含まれます。零細企業や小企業が一般に報告義務から外れるわけではありません。小規模事業者向けの制裁金上の扱いは限定的で、最初の**24時間以内の早期警告期限**だけに関係します。

CRAは脆弱性の状態を3つに分けます。

- **脆弱性：** 悪用され得る弱点
- **悪用可能な脆弱性：** 実環境で利用できる弱点
- **積極的に悪用されている脆弱性：** 攻撃で使われたことが確認された弱点

時計が動き出す時点

信号が届いた瞬間に時計が動くわけではありません。時計は、初期評価を完了し、製品の脆弱性が積極的に悪用されている、または重大インシデントが製品のセキュリティを侵害したと合理的な確信を持った時点で動き出します。重点は、調査の完了を待つことではなく、迅速な初期評価にあります。顧客、研究者、当局、その他第三者から潜在的な課題が持ち込まれた場合、遅延なく評価し、その評価で合理的な確信が得られた時点で時計を動かします。

積極的に悪用されている脆弱性を検知した場合、次のタイムラインが適用されます。

期限	必要な対応	報告先
24時間以内	積極的な悪用に関する早期警告	各国CSIRT経由でENISA
72時間以内	脆弱性通知。影響を受ける製品、悪用と脆弱性の概略、緩和策、利用者が取れる是正措置、必要な機微性表示を含みます	各国CSIRT経由でENISA
是正措置または緩和策が利用可能になってから14日以内	最終報告。脆弱性の説明、深刻度、影響、攻撃者に関する利用可能な情報、セキュリティ更新またはその他の是正措置の詳細を含みます	各国CSIRT経由でENISA

製品のセキュリティに影響する**重大インシデント**を検知した場合、次のタイムラインが適用されます。

期限	必要な対応	報告先
24時間以内	早期警告。違法または悪意ある行為が原因と疑われるかも含みます	各国CSIRT経由でENISA
72時間以内	インシデント通知。インシデントの性質、初期評価、緩和策、利用者が取れる是正措置、必要な機微性表示を含みます	各国CSIRT経由でENISA
72時間通知から1か月以内	最終報告。詳細な説明、深刻度、影響、想定される脅威または根本原因、実施済みまたは進行中の緩和策を含みます	各国CSIRT経由でENISA

通知は情報が分かるにつれて更新します

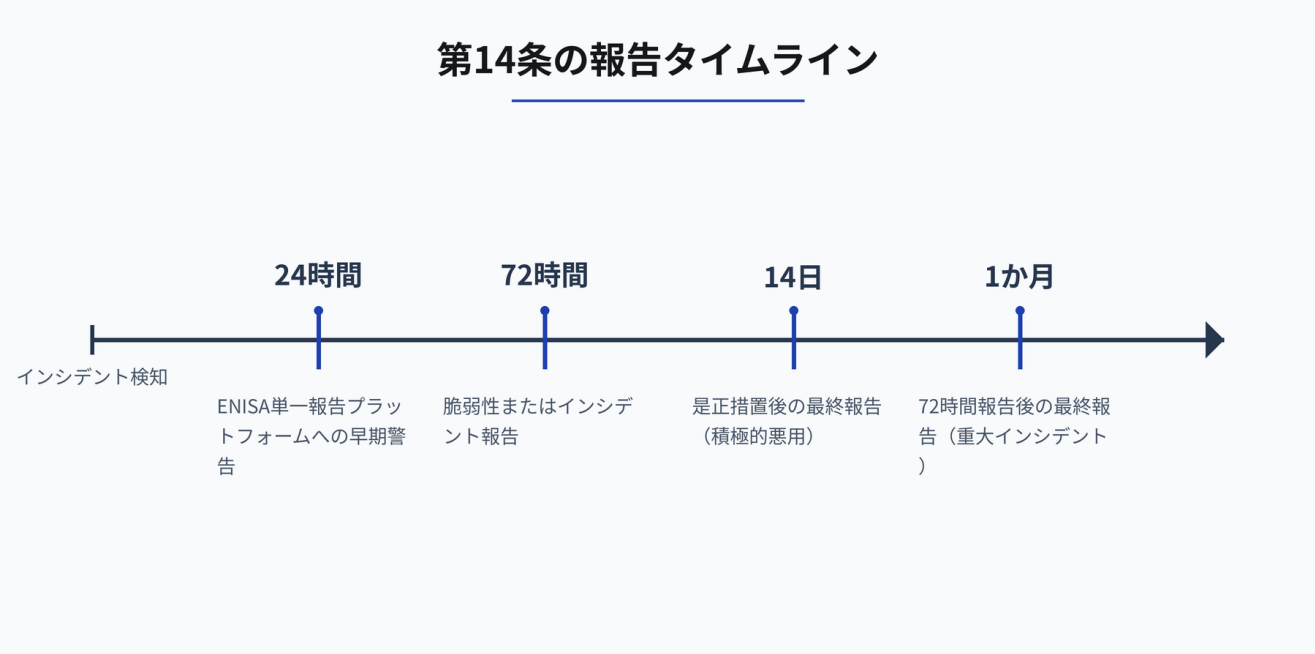
24時間、72時間、14日（または1か月）の提出は、別個の届出ではなく、同じ通知の段階です。各段階で、前段階では入手できなかった情報を追加します。コーディネーターに指定されたCSIRTは、随時、中間更新を求めることもあります。既に提供した情報を繰り返す必要はありません。

報告は**CRA単一報告プラットフォーム**で行います。製造業者の主たる加盟国のCSIRTを通じて処理され、ENISAにも同時にアクセスが与えられます。

利用者への通知

把握後、影響を受ける利用者、必要に応じて全利用者に対し、脆弱性またはインシデントと、利用者が実施できるリスク低減・是正措置を通知します。これは公開開示と同じではありません。義務は、リスクに応じて、利用者が自身を保護するために必要な情報を届けることです。機微または重要な環境で使われる製品については、脆弱性が未緩和の間、詳細な技術情報を関係する顧客に限定します。早すぎる公開詳細は悪用を容易にします。

脆弱性が修復または緩和された後は、利用者が自社製品の影響有無を確認でき、一般的な認識向上にも資するように、より広い開示が適切になる場合があります。詳細度と時期は、残留リスクに見合うものに保ちます。利用者にタイムリーに通知しない場合、CSIRTがそれを比例的かつ必要と判断するときは、CSIRT自身が情報を提供することがあります。



積極的に悪用されている脆弱性

24時間	早期警告
72時間	脆弱性通知
是正措置から14日	最終報告

重大インシデント

24時間	早期警告
72時間	インシデント通知
72時間通知から1か月	最終報告

不適合製品への是正措置

上市済みの製品、または自社プロセスがCRAの必須サイバーセキュリティ要件に適合していないと知った場合、あるいはそう疑う理由がある場合、直ちに対応します。義務は上市時点から始まり、サポート期間全体に及びます。

3つの選択肢

1. **適合状態に戻す。** 製品またはプロセスを修正します。ソフトウェア製品の場合、通常はセキュリティ更新またはプロセス変更です。対象バージョンに修正を適用します。
2. **撤回する。** 市場で製品の提供を停止します。サプライチェーンと、在庫を持つ小売、インテグレーター、リセラーから引き上げます。
3. **リコールする。** 既に利用者の手元にある製品を回収します。利用者へのサイバーセキュリティリスクが重大で、修正や撤回だけでは不十分な場合に使います。

選択はリスクに見合うもので、固定的な順序ではありません。修正が利用可能なパッチ可能な脆弱性は、通常「適合状態に戻す」を意味します。現場で安全に修正できない製品は、通常「撤回」を意味し、重大なリスクとともに実利用されている場合は「リコール」を意味します。

併せて行うこと

- 不適合が積極的に悪用されている脆弱性または重大インシデントである場合、**第14条の連鎖に基づき通知**します。タイムラインは上記に示しています。
- **利用者に通知**します。不適合と、利用者自身が適用できる是正措置を伝えます。比例性のルールは前述の「利用者への通知」を参照します。
- 市場監視当局の合理的な要請に**協力**します。技術文書を、当局が読める言語で提供することも含みます。
- **証拠を保全**します。何を見つけ、いつ見つけ、どう対処し、利用者・当局とどう連絡したかを示す記録を保持します。技術文書とEU適合宣言書は、上市から少なくとも10年、またはサポート期間全体のいずれか長い期間、利用可能な状態を維持します。

製品文書の要件

文書は、デジタル要素を含む製品が上市されてから**少なくとも10年間**、または**サポート期間全体**のいずれか長い期間にわたり保持します。サマリーレベルでは、技術文書には次の8つの証拠領域を含めます。

1. 一般的な製品説明
2. 設計、開発、製造の詳細（SBOMを含む）
3. サイバーセキュリティリスク評価
4. サポート期間の決定
5. 適用した整合規格と仕様
6. 試験報告書
7. EU適合宣言書
8. 完全なSBOM（市場監視当局からの要請時）

適合性評価ルートのチェックリスト

上記の分類表を使ってルートを特定します。そのうえで、使用した規格、仕様、認証スキーム、または認証機関の証跡とともに、ルート判断を技術文書に残します。

具体例。同じ階層構造は、セキュリティカメラに限らず、デジタル要素を含むあらゆる製品に適用されます。

製品セキュリティ要件

a. 上市時点で既知の悪用可能な脆弱性がないこと

公知で悪用可能な脆弱性を未処理のまま出荷しない体制が必要です。既知の脆弱性は、公開データベース、サプライヤー通知、顧客報告、社内トラッカーから見つかる場合があります。

対応例：

- 各リリース前に、Common Vulnerabilities and Exposures（CVE）を含む脆弱性データベースを確認します
- ビルドパイプラインで静的・動的アプリケーションセキュリティ試験（SAST/DAST）を使います
- すべての第三者・オープンソースコンポーネントを依存関係としてスキャンします
- 特定した各課題について、リスク受容または緩和の判断を文書化します

b. セキュアなデフォルト設定

製品は初期状態で安全に使える必要があります。不要なサービスを無効にし、弱い初期認証情報を避けます。安全でない導入モードは、短時間かつ管理された形にします。セキュアなデフォルト設定の義務は、書面合意により事業利用者へ提供する特注製品については別段の取扱いができますが、製品を初期状態に戻せる手段は常に確保しておきます。

対応例：

- 初期ビルドではリモートアクセスポートとデバッグインターフェースを無効にします
- 強固な初期認証メカニズムを適用します
- 管理機能を権限のある利用者に限定します
- 利用者データを削除しつつ、設定とファームウェアを既知の安全な状態へ戻す工場出荷時リセットを実装します

c. 利用者のオプトアウトを含むセキュリティ更新（自動更新を含む）

導入後のセキュリティ課題に対応できる更新機構が必要です。自動更新が適切な場合はデフォルトで有効にし、延期またはオプトアウトの明確な手段を用意します。

対応例：

- 更新パッケージに暗号署名と完全性検証を実装します
- ロールバック防止と更新イベントの記録を用意します
- 保留中の更新を利用者に知らせる通知システムを構築します
- 明確な設定画面から自動更新を延期または無効化できるようにします

d. 不正アクセスからの保護

アクセス制御は、ローカルインターフェースとリモートインターフェースの双方を保護します。権限のない利用者が機能、データ、設定、管理面に到達しない状態を作ります。

対応例：

- パスワード複雑性ポリシーと強固な初期認証情報を適用します
- 適切な場合は多要素認証（MFA）を実装します
- ロールベースアクセス制御（RBAC）とセッションタイムアウトを適用します
- 失敗したアクセス試行を記録し、異常検知で不正な活動を把握し、その内容を点検と報告のために共有します

e. 保存、送信、処理されるデータの機密性

機密データは、保存時、送信時、処理時に保護します。

対応例：

- 標準化された暗号アルゴリズムを使います。保存データにはAES-256、送信データにはTLSなどを使います
- 安全な鍵管理を適用します
- 機密データを重要でないシステムコンポーネントから分離します
- すべてのデータアクセスイベントについて監査ログを維持します

f. データ、ファームウェア、設定の完全性

この要件は、ファームウェア、ソフトウェア、設定ファイルなどのシステム自体と、測定値、制御コマンド、利用者入力などの処理データを対象とします。

対応例：

- 信頼されたコードだけを実行するため、セキュアブートと署名済みファームウェアを実装します
- 改ざんの試みを検知・報告するランタイム検証を使います
- データ完全性を守るため、暗号ハッシュとデジタル署名を適用します
- システムまたは組織の境界を越えて暗号鍵を生成、配布、検証できる基盤を構築します

g. データ最小化

製品の意図された目的に必要なデータだけを収集・処理します。個人データと技術データの双方が対象です。

対応例：

- 不要なデータフローを特定するため、プライバシー影響評価またはデータ保護バイデザインの確認を行います
- 使っていないテレメトリ、診断、バックグラウンド収集を削除または任意化します
- 拡張的なデータ収集を状況に応じてオン・オフできる設定を用意します

h. サービス拒否攻撃への対策を含む可用性とレジリエンス

インシデントや攻撃の最中でも、主要機能は利用可能な状態を保つか、制御された形で停止する必要があります。

対応例：

- サーキットブレーカー、リトライ処理、フォールバック、ウォッチドッグタイマーを実装します
- リソース枯渇を防ぐため、リソース制限を適用します
- サービス拒否のシナリオに備え、レート制限と入力検証を使います
- 過負荷の試みを遮断するため、ネットワークレベルのフィルタリングを適用します

i. 他の接続機器またはネットワークへの悪影響の最小化

製品は同じ環境の他システムを妨げない設計にします。予測可能に動作し、共有リソースを過剰に使わない状態を保ちます。

対応例：

- トラフィックシェーピングを実装し、ブロードキャストまたはマルチキャストの利用を制限します
- 通信プロトコル仕様への適合を確認します
- ネットワークフラッディングやリソース枯渇などの妨害的な動作を検知・防止する自己監視を使います

j. 外部インターフェースを含む攻撃面の限定

侵入口と公開機能を最小化します。物理ポート、無線インターフェース、API、デバッグサービス、不要なソフトウェアコンポーネントが含まれます。

対応例：

- 本番ビルドで未使用のサービス、ポート、インターフェースを無効化します
- システムの初期値を強化し、利用者権限を制限します
- ソフトウェアアーキテクチャをモジュール化し、コンポーネント間を分離します
- 安全なソフトウェア設計原則を適用し、脅威モデリングで不要な露出を特定・除去します

k. 悪用緩和策によるインシデント影響の低減

一部の攻撃は成功する前提で設計します。製品設計は、被害が広がる範囲を限定します。

対応例：

- システムコンポーネントを分離し、サンドボックスまたはコンテナを使って隔離環境で動作させます
- 権限分離を適用し、重要機能を必要最小限の権限で実行します
- 一つのコンポーネントが侵害されても、攻撃者がシステム全体を制御できない設計にします

l. 利用者のオプトアウトを含むセキュリティ関連活動の記録

アクセス試行やデータ変更など、セキュリティに関連する活動を記録します。監視と監査に使える状態にします。CRAが求める場合は、利用者向けのオプトアウト手段も用意します。

対応例：

- タイムスタンプ付きJSONログなど、構造化ログを実装します
- ログローテーションとリモートログ転送の選択肢を持つローカル保存を用意します
- ログイン試行、設定変更、ソフトウェア更新などのイベントを異常の観点で監視します
- 許容される場合にログ記録を無効化できる、分かりやすい利用者向け手段を提供します

m. 安全で恒久的なデータ削除とポータビリティ

利用者がデータと設定を恒久的に削除できる実用的な手段を用意します。データを他製品や他システムへ移転できる場合、その移転も安全にします。

対応例：

- ストレージ領域の上書きまたは鍵の暗号学的削除により、安全な消去機能を実装します
- 移転中の露出を防ぐため、認証済みで暗号化されたチャネルを使います

脆弱性ハンドリング要件

1. 脆弱性の特定と文書化

製品にどのソフトウェアコンポーネントが含まれ、どの既知脆弱性が影響するかを把握します。SBOMは、その機械可読な棚卸しです。

対応例：

- SBOM生成をCI/CDパイプラインに直接組み込み、各ビルドで最新のコンポーネント一覧を作成します
- 相互運用性のため、CycloneDX、SPDX、SWIDなどの形式を使います
- CVEリスト、CISA KEV、ENISA EUVDなどのデータベースに対して自動脆弱性スキャンを実行します
- サポート期間を通じてSBOMを技術文書の一部として維持し、市場監視当局の要請に応じて提供します

2. リスク管理と適時のセキュリティ更新

脆弱性が見つかった場合は迅速に修正し、セキュリティ更新を届けます。可能な場合、セキュリティパッチを機能更新から分けることで、重要な修正を速やかに適用できます。

対応例：

- セキュリティ修正を全体更新なしで配布できる更新機構を設計します
- 重要コンポーネントを個別に修正できるよう、ソフトウェアとファームウェアを構成します
- 完全性チェック付きの安全なチャネルで更新を配布します
- トレーサビリティと適合性の説明に使えるよう、更新活動の記録を維持します

3. 定期的なセキュリティ試験

セキュリティ試験は一回限りの作業ではありません。脅威、依存関係、製品動作が変化するため、ライフサイクル全体で試験します。試験の種類と頻度はリスク評価から決めます。

対応例：

- 実際の攻撃を模擬する侵入テストを実施します
- セキュリティ上の弱点を特定するため、静的・動的コード解析を適用します
- 入力処理の欠陥を見つけるため、ファジングを使います
- 大きな設計変更や機能変更の後は、セキュリティコードレビューとアーキテクチャレビューを計画し記録します

4. 脆弱性受付、CVDポリシー、アドバイザリー

脆弱性を巡る連絡について、受付、協調的開示、修正時のアドバイザリーという3つの義務を1つのワークフローとしてまとめます。サマリーの4、5、6に該当します。

CRAは、脆弱性連絡に関する3つの要件を別個に挙げています。報告のための連絡経路、協調的開示ポリシー、修正時のアドバイザリーです。各義務の内容は次のとおりです。

受付

報告者向けに、低摩擦の明確な経路を用意します。脆弱性報告用の見つけやすい連絡手段（専用のメールアドレスまたはWebフォーム）を公開します。PGP鍵の公開などにより、安全な通信に対応します。義務は、自社製品と、製品に含まれる第三者コンポーネントに関する報告の双方を対象とします。

トリアージ

受領した報告すべてに対し、確認応答、トラッキングシステムでの記録、レビュー担当者の割り当て、定められたタイムライン内での解決を行います。報告者に確認応答とステータス更新を返します。第三者コンポーネントに起因する課題は、自社の修復と並行して上流の保守者へ連携します。

協調的脆弱性開示ポリシー

報告者とパートナー向けに、連絡方法、想定される応答時間、自社が約束する事項、報告者に求める事項といった期待値を定めたCVDポリシーを公開します。利用者を保護しつつ、報告者の貢献を認める形で開示を調整します。

修正時のアドバイザリー

修正が利用可能になった時点で、解決した課題のアドバイザリーを公表します。CVE識別子、対象製品バージョン、CVSSなどの標準的な深刻度評価、利用者が取るべき行動についての明確で分かりやすい情報を含めます。技術管理者と非技術系利用者の双方に理解できる表現で書きます。

公開開示の遅延

直ちに公開することのサイバーセキュリティリスクが便益を上回ると正当に裏付けられる理由がある場合に限り、かつ、利用者が修正を適用する機会を得るまでに限り、公開開示を遅らせることができます。判断の根拠を文書化します。

5. 安全な更新配布メカニズム

更新機構は信頼でき、改ざんに強い必要があります。自動更新が技術的に可能な場合、利用者が脆弱な状態で残る時間を短くできます。

対応例：

- 更新を安全なチャネルで送信し、デジタル署名で検証します
- 不完全または破損したインストールを防ぐ形で更新を適用します
- 差分更新またはモジュール更新により、影響を抑えつつ修正を早く届けます
- 利用者または管理者が更新状況を確認できるよう、更新ログを維持します

6. 助言メッセージ付きの無償セキュリティ更新

セキュリティ更新は速やかに、追加費用なしで提供します。特注の事業者向け製品で別合意がある場合は例外となります。各更新には、何が変わったか、利用者が何をすべきかを示す明確な助言メッセージを添えます。

対応例：

- 製品の状況に応じて、利用者へ直接通知する、または自動適用する配布システムを維持します
- 技術系利用者と非技術系利用者の双方に分かる助言メッセージを書きます
- 必要に応じて、助言メッセージに深刻度を含めます
- 利用者が取るべき行動を伝えます。更新適用、設定変更、侵害の兆候への注意などです
- 修正がすでに利用可能であるのに利用者が脆弱な状態で残されないよう、利用可能になり次第、セキュリティ更新を遅延なく配布します
- 製造業者が管理するチャネルでアドバイザリーを公表し、製品のサポートページからリンクします

無償かつ遅延なしの義務は、宣言したサポート期間の長さで継続します。特注製品の適用除外は商業条件のみを変えるもので、アドバイザリーは引き続き必要です。

技術文書に含める内容

技術文書

技術文書はCRA対応の中心的な証拠です。必須サイバーセキュリティ要件への適合のために使った、設計上、技術上、手続上の措置を示します。**上市前**に存在し、**サポート期間**を通じて最新である必要があります。

エンジニアリングワークフローに沿った技術文書の証拠

ステップ1	**範囲設定と分類**	製品目的、意図された使用、上市判断、製品分類、標準の適用ルート。
ステップ2	**アーキテクチャとリスク**	アーキテクチャ、データ接続、利用条件、リスク評価、緩和策。
ステップ3	**コンポーネントとSBOM**	機械可読SBOM、第三者コンポーネント、供給者情報、脆弱性追跡。
ステップ4	**ビルド、試験、更新**	安全な初期設定、ハードニング、試験報告、安全な更新メカニズム、助言メッセージ。
ステップ5	**リリースとサポート**	利用者向け説明、EU適合宣言書、CE証拠、サポート期間の根拠、更新記録。

技術文書には8つの必須項目があります。これらを合わせて、**製品が何であるか、どのように構築・試験されたか、どのリスクが検討されたか、どの規格が適用されたか、上市後にどう支援するか**を説明します。法的見出しをそのまま使う必要はありませんが、各トピックを扱う必要があります。

No.	項目	含める内容
1	一般的な製品説明	意図された目的と機能、関連ソフトウェアバージョン、写真または図（ハードウェアの場合）、利用者情報と説明
2	設計、開発、製造の詳細	アーキテクチャ説明（コンポーネントと相互作用）、SBOM、脆弱性ハンドリングプロセス（CVDポリシー、連絡先、安全な更新メカニズム）、検証を含む製造・監視プロセス
3	サイバーセキュリティリスク評価	製品リスクの文書化された分析、各必須サイバーセキュリティ要件の製品への適用方法、特定リスクの緩和
4	サポート期間の決定	利用者期待、比較可能な製品、法的ガイダンスなど、サポート期間を決める要素
5	適用した整合規格と仕様	適用した整合規格、共通仕様、EU認証スキームの一覧。全部適用か一部適用か。規格を使わない場合の代替策
6	試験報告書	製品と脆弱性ハンドリングプロセスの双方についての適合性証拠
7	EU適合宣言書	技術文書をCEマーキング義務に結び付ける宣言書の写し
8	完全なSBOM（要請時）	市場監視当局は適合性確認のため、完全なSBOMを求める場合があります

単一の統合技術文書で、CRAと他の適用可能なEU法令を扱うこともできます。例として、無線機器指令やESPRがあります。その場合、すべての適用義務を含めます。

EU適合宣言書

EU適合宣言書は、製品が該当するCRAサイバーセキュリティ要件を満たすという製造業者の正式な宣言です。各宣言書には次の内容を含めます。

- 製品名、型式、一意の識別子
- 製造業者の名称と住所、または認定代理人
- 提供者の単独責任に関する宣言
- 追跡可能性を確保する製品説明（必要に応じて画像を含めます）
- 関連するEU法令への適合に関する明示的な宣言
- 使用した整合規格、仕様、認証への参照
- 関与した認証機関の詳細（名称、番号、手続、証明書番号）
- 署名欄（場所、日付、氏名、役職、署名）

署名後、宣言書は法的に意味を持ち、サイバーセキュリティ適合について製造業者が全面的に責任を負うことを確認します。

包装またはマニュアルで使う簡易宣言も認められます。形式は次のとおりです。「ここに、［製造業者］は、製品［型式・名称］がEU規則2024/2847に適合していることを宣言します。EU適合宣言書の全文は、次のWebアドレスで入手できます：［Webアドレス］。」この簡易形式は透明性を維持しながら、文書負担を下げます。小規模製造業者や多品種ポートフォリオで有用です。

利用者情報と説明

利用者情報と説明は、適法な上市の条件です。製造業者は、説明を**少なくとも10年**または**サポート期間全体**にわたり利用可能にします。輸入業者と販売業者は、製品を上市または供給する前に、説明が存在し、最新で、適切なEU言語で提供されているかを確認します。

利用者向け説明には次を含めます。

- 製造業者の身元と連絡先
- 脆弱性報告の単一窓口
- 製品識別、意図された目的、安全な利用条件
- 既知または予見可能なサイバーリスク
- EU適合宣言書へのリンク
- サポート条件と明確なサポート終了日
- セットアップ、更新、安全な利用、廃棄、該当する場合の統合とSBOMアクセスに関する段階的な手順

適合性評価ルートの選択

モジュールA：自己評価

モジュールA（内部統制）は、製品が必須サイバーセキュリティ要件に適合していることを自己宣言するルートです。設計と製造の双方について、製造業者が全面的に責任を負います。標準（未分類）の製品で使えます。重要クラスI製品では、関連する整合規格、共通仕様、欧州サイバーセキュリティ認証スキームが利用可能で、CRAルールが求める形で適用される場合に限り使えます。

モジュールAでは次を行います。

- 包括的な技術文書を準備します
- 製品設計、製造プロセス、サイバーセキュリティ機構、脆弱性ハンドリング手順を詳述します
- 製品ライフサイクルを通じて継続的な適合責任を維持します
- 製品の運用期間におけるセキュリティ更新と脆弱性管理の計画を実施します
- 記録を少なくとも10年間利用可能にします

モジュールBとC：製品中心の評価

モジュールBとCは、特定の製品型式について第三者検証が必要な場合に使います。製造業者が関連する整合規格、共通仕様、認証スキームを適用していない、一部のみ適用している、または適用できない重要クラスI製品が対象です。重要クラスII製品では、モジュールB+C、モジュールH、または「substantial」以上の保証レベルを持つ欧州サイバーセキュリティ認証スキームを使います。

モジュールB（EU型式審査）： 認証機関が代表的な製品サンプルと関連する技術文書を審査します。必須サイバーセキュリティ要件への適合を確認し、製品設計がCRAの基準を満たす場合にEU型式審査証明書を発行します。

モジュールC（型式適合、生産管理）： 製造業者は、すべての生産単位がモジュールBで認証された承認済み型式に適合するようにします。製造業者はCEマーキングを付し、EU適合宣言書を発行し、記録を少なくとも10年間保持します。モジュールBとCを組み合わせることで、特定の製品モデルが技術的に適合し、各生産ロットが承認済み設計と一致することを示します。

モジュールH：プロセス中心の評価（全面的品質保証）

モジュールH（全面的品質保証）は、個別製品の試験ではなく、製造業者の内部品質システム全体に焦点を当てます。重要クラスIおよびクラスII製品で利用できます。クリティカル製品は、要件が満たされる場合に認証ルートを使います。要件が満たされない場合は、重要クラスII製品と同じルートを使います。

モジュールHでは次を行います。

- 製品カテゴリ全体について、設計、開発、製造、試験、脆弱性ハンドリングを含む品質システムを構築・維持します
- 品質システムを認証機関に提出し、評価と承認を受けます
- 継続的な適合を確認するため、認証機関による監視、監査、検査、プロセスレビューを受け入れます

承認後は、個別の製品型式ごとに認証機関の審査を繰り返さず、その品質システムで製造される製品について適合宣言書を発行できます。

ルートの違いは次のとおりです。

- モジュールB+Cは製品に焦点を当てます。代表的な製品型式が試験・認証されます。
- モジュールHはプロセスに焦点を当てます。製造業者の設計・製造システム全体が認証され、監視されます。

適合性評価ルート

A

モジュール

自己評価

標準製品、および整合規格、共通仕様、認証スキームを完全に適用した重要クラスI製品。製造業者が設計と製造の責任を負います。

B+C

モジュール

型式と生産

適用可能な規格を使えない重要クラスI製品、また重要クラスIIルートの一部として使います。認証機関が代表型式を審査し、製造業者が各生産単位の適合を確保します。

H

モジュール

全面的品質保証

重要クラスIとIIで利用できます。認証機関が、設計、開発、製造、試験、脆弱性ハンドリングのシステム全体を承認・監査します。

上市までの流れ

EU規制全体におけるCRAの位置付け

CRAは単独で存在する規制ではありません。製造業者にとっての実務的な問いは具体的です。CRAの対応は、他のEU制度のもとで作業の重複削減に使えるか、それとも別個の義務として並行して走らせる必要があるか、です。

CRA対応を再利用できる領域

- **高リスクAIシステム（AI法、規則2024/1689）。** 製品がCRA対象範囲内の高リスクAIシステムである場合、CRAの必須サイバーセキュリティ要件を満たすことは、EU適合宣言書がカバーする範囲においてAI法のサイバーセキュリティ要件を満たしたとみなされます。適合性評価手続きは原則としてAI法体系を経由しますが、重要およびクリティカルなCRA製品には適用除外があります。CRAのサイバーセキュリティリスク評価では、データポイズニングや敵対的攻撃などのAI固有のリスクも考慮する必要があります。
- **他のEU法令と統合したリスク評価。** CRAは、製品が複数の制度の対象となる場合、サイバーセキュリティリスク評価を別のEU法令で求められる広範なリスク評価の一部とすることを明示的に認めています。1つの評価成果物を、2つの規制目的で使えます。
- **複数制度を横断する1つの技術文書。** 技術文書のセクションで既述のとおり、すべての制度の義務に対応している限り、CRAと他の適用可能なEU法令を単一の統合技術文書で扱えます。同じ製品が無線機器指令、エコデザイン規則、その他の製品法のもとで既に文書を必要としている場合に有用です。
- **リファービッシュ、メンテナンス、修理の共通定義。** CRAは、これらの定義をエコデザイン規則から取り込んでいます。サービス業務が実質的変更に該当するかを分析する際の参照は、CRA固有の用語ではなく、エコデザインの定義です。

別個の義務が残る領域

- **AI法のその他すべて。** サイバーセキュリティはAI法の一部分にすぎません。リスク分類、透明性、データセットガバナンス、人による監視、AI挙動の上市後監視などはAI法の義務であり、CRAではカバーされません。CRA適合のサイバーセキュリティは、AI法全体への適合を推定するものではありません。
- **エコデザインとデジタル製品パスポートの内容。** エコデザイン規則のエネルギー効率、耐久性、修理可能性スコアリング、デジタル製品パスポートの持続可能性内容に関する要件は、CRAの対象範囲外です。CRAの証跡はエコデザイン作業と並行しますが、それを置き換えるものではありません。
- **データ法のIoTデータアクセス権。** データ法は、利用者に対し、接続製品が生成するデータへのアクセス、共有、移転の契約上の権利を与えます。CRAはそのデータのセキュリティを扱いますが、アクセス権制度は定めません。別の義務、別の証拠です。
- **欠陥製品に対する製造物責任。** 製造物責任指令（2024/2853）は、欠陥製品が引き起こす損害について、製造業者の厳格責任を維持します。CRAは、上市後セキュリティ更新の欠如が責任を引き起こす欠陥になり得ることを示しています。契約、保険、インシデント対応の手順は、CRA適合とは独立に、この露出を考慮する必要があります。

CRA Evidence のコンサルティング支援

CRA Evidence は、EUサイバーレジリエンス法の義務を検証可能な製品証跡に変換し、コンプライアンスプラットフォームと技術コンサルティングを組み合わせます。

プラットフォーム

CRA準備の根拠となる証拠を一か所で管理します。

- **SBOMとコンポーネント棚卸し：** 製品バージョンとリリースごとのCycloneDX、SPDX、HBOM記録
- **CI/CD証跡自動化：** スキャン、SBOMアップロード、リリースゲート、監査記録のCLI/APIワークフロー
- **署名付きSBOMと来歴：** バージョン管理された証跡、サプライヤー証明、デューデリジェンス記録
- **脆弱性運用：** CISA KEV、EPSS、VEX、監視、トリアージ、報告ワークフロー
- **技術文書とCE証跡：** EU適合宣言記録、保持履歴、QR連携の製品コンプライアンスパスポート

技術コンサルティング

CRA義務を、製品、アーキテクチャ、リリースプロセス、サプライヤーモデルに関するエンジニアリング判断へ落とし込みます。

- **技術準備スプリント：** 必須要件のギャップレビュー、アーキテクチャ推奨、優先順位付きアクションプラン
- **CRAプログラムリード：** 責任モデル、義務トラッキング、証跡マイルストーン、技術文書の維持
- **当局対応・インシデント対応計画：** 報告ワークフロー、照会対応手順、利用者連絡、証跡パッケージ準備
- **規制横断の整理：** CRA証跡をData Act、ESPR、AI Act、RED、業界要件と接続
- **技術ワークショップ：** 製品、開発、セキュリティ、コンプライアンス、サプライヤーチームとのリモートまたは現地セッション

ツール非依存：CRA Evidence は CycloneDX、SPDX、Grype、Trivy、CI/CDパイプライン、課題管理システムと連携します。

実務的な最初の一歩

1つの製品ファミリーを選びます。責任者、適用範囲判断、SBOM、脆弱性ワークフロー、技術文書の不足、リリース証跡を整理します。コンプライアンスを別プロジェクトにせず、具体的なCRAベースラインを作れます。

製品全体の支援範囲は craevidence.com/ja で確認できます。無料アセスメントは craevidence.com/ja/assessment から予約できます。