EU Cyber Resilience Act

日本の製造会社のための実務入門

2026年9月11日の報告義務から、2027年12月11日の全面適用まで

対象

日本の製造会社・コンプライアンス部門
日本法の知識はあるがCRAは初学者

到達点

「EU法の話」で終わらせず、
製品開発・品質保証・CSIRTへ落とす

キーワード

市場アクセス規制
セキュア・バイ・デザイン
24時間報告

弁護士法人三宅法律事務所
パートナー弁護士　渡邉 雅之

架空事案：1通のメールから24時間時計が動く

EU向け産業用IoTゲートウェイで、2026年9月20日に何が起きるか。

事案の設定

A社は日本の産業機械メーカー。

2023年からEUで、工場設備に接続するIoTゲートウェイを販売。遠隔監視クラウドとファーム更新機能がある。

2026年9月20日 15:00

ドイツ販売会社から本社営業部へメール：
「顧客工場で、御社製品の脆弱性を使った攻撃の疑い。ログもあります。」

この時点で確認すべき問い

1. 既存製品でもArticle 14の対象になるか
2. 会社はいつ「認識」したと扱われるか
3. 24時間・72時間で誰へ何を報告するか
4. SBOMで影響製品・バージョンを特定できるか
5. 顧客通知・パッチ・営業説明を同時に出せるか

本セミナーでは、この事案に戻りながら、CRAの「24時間報告」と「2027年全面適用」を分解する。

※ 架空事案。CRA Article 14、Article 69、ENISA SRP等を踏まえた検討例

最初の誤解：2027年12月まで待てばよい？

答えは「いいえ」。最初の大きな実務対応は2026年9月11日に始まる。

2027年12月11日

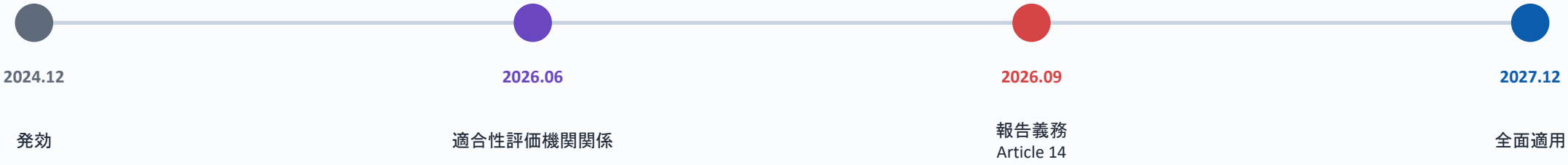
全面適用

多くの企業がここだけを見る

しかし、2026年9月11日から第14条が先行適用

「積極的に悪用されている脆弱性」と「製品セキュリティに影響する重大インシデント」の報告義務が先に動く。

既存製品にも及ぶ点が、日本メーカーの落とし穴である。



根拠：CRA Article 71、European Commission CRA summary

なぜEUは「製品のサイバーセキュリティ」を規制するのか

CRAは「事故後の対応」ではなく、製品を市場に出す前からの安全設計を求める。

1　つながる製品が増えた

ベビーモニター、スマートウォッチ、アプリ、産業機械、組込みソフト。
「ネットにつながる製品」が攻撃経路になる。

2　更新されない製品が残る

脆弱性は発見後も放置される。
ユーザーはどこまで安全か判断しにくい。

3　サプライチェーンが長い

OSS・部品・クラウド処理・販売代理店。
どこか一つの弱点が全体の弱点になる。

EUの発想

「サイバーセキュリティ」は情報システム部門だけの管理項目ではなく、製品安全・品質保証・市場アクセスの要件である。

根拠： European Commission CRA policy page; CRA Recitals and Articles 1, 6

本セミナーのゴール

ゼロから読み、明日から社内で説明できるレベルまで整理する。

1. **対象製品かを判断できる**
2. **製造者に課される義務の全体像を説明できる**
3. **2026年9月11日の報告義務に備える**
4. **2027年12月11日の全面適用に向けた社内計画を作る**

本日の読み方

日本の法務・コンプライアンス担当者にとって、CRAは「EUのIT規制」ではなく、

① 製品安全
② 品質保証
③ リコール・不具合対応
④ 取引先管理
⑤ 内部統制

がサイバーセキュリティに拡張されたものとして読むと理解しやすい。

CRAを一言でいうと

「サイバーセキュリティ」を、EU市場で販売する製品の市場アクセス要件にする規則

市場に出す前

セキュア設計・リスク評価・技術文書

市場に出した後

脆弱性管理・更新・ユーザー通知

事故が起きたら

24時間・72時間・最終報告

根拠：CRA Article 1、Article 6、Article 13、Article 14

最初に押さえる6つのEU法用語

日本法の感覚に置き換えると、条文がかなり読みやすくなる。

上市（placing on the market）

EU市場で初めて提供する行為。製品・バージョン単位で判断する。

市場提供（making available）

上市後に流通している状態。第14条の報告義務はここまで及ぶ。

経済事業者

製造者・EU代理人・輸入者・販売者の総称。役割ごとに義務が異なる。

整合規格と適合推定

規格に従えば必須要件に適合と推定される。JIS引用に近い発想。

適合性評価とノーティファイドボディ

自己評価か第三者評価か。製品分類によって手続が決まる。

市場監視当局

是正命令・販売停止・回収を命じる当局。製品安全行政に近い役割。

ポイント：New Legislative Framework（NLF）はEU製品法の共通枠組み。CRAも、経済事業者・適合性評価・市場監視・CE表示という同じ「製品法」の仕組みで読むと理解しやすい。

根拠：CRA Articles 3, 27, 32, 52、Regulation (EU) 2019/1020

用語ガイド①　製品・ソフトウェア・商流

CRAでは、製品そのものだけでなく「中のソフト」と「誰の名で市場に出すか」が重要になる。

ファームウェア

機器内部に組み込まれ、ハードウェアの基本動作を制御するソフト。ルーターや制御装置ではセキュリティ更新の対象にもなる。

OSS（Open Source Software）

ソースコードが公開され、ライセンス条件の下で利用・改変・再配布できるソフト。CRAでは脆弱性と依存関係の管理が重要。

SBOM

Software Bill of Materials。製品を構成するソフトウェア部品・依存関係の「部品表」。影響製品を短時間で特定する基盤。

パッチ

脆弱性や不具合を修正するための更新プログラム。暫定的な回避策（workaround）と区別して使われることが多い。

OEM と ODM

実務用語。OEMは発注側ブランド向けの製造、ODMは設計・開発まで受託側が担う形が典型。CRAは呼称より「誰の名で市場投入するか」を見る。

SIer（System Integrator）

機器・ソフトを組み合わせ、顧客システムを構築・統合する事業者。実質変更を加えて市場提供すると「製造者」扱いの論点が生じ得る。

参考：CRA Articles 3, 13, 21, 22 / Annex I Part II

用語ガイド②　監視・事故対応・脆弱性開示

「見つける」「事故に対応する」「製品の脆弱性を直す」は、似ているが役割が違う。

SOC

Security Operations Centre。ログやアラートを継続監視し、異常の検知・分析を担う運用拠点。

CSIRT

Computer Security Incident Response Team。事故の調査、封じ込め、復旧、関係者連絡等を調整するチーム。

PSIRT

Product Security Incident Response Team。自社製品の脆弱性報告を受付・評価し、修正・公表・顧客対応を進めるチーム。

CVD

Coordinated Vulnerability Disclosure。発見者・メーカー等が連携し、修正準備と公表時期を調整して脆弱性を開示する手続。

CVE

Common Vulnerabilities and Exposures。公開脆弱性を共通ID（CVE-…）で識別する仕組み。CVE付与＝現実の悪用確認、ではない。

PoC

Proof of Concept。脆弱性が技術的に再現・悪用可能であることを示す検証コード等。PoCがある＝実攻撃で使われた、とは限らない。

参考：ENISA CSIRT/SOC・Vulnerability Disclosure / CVE Program

用語ガイド③　セキュリティの基本概念

Annex Iの要求は、専門用語を「何を守るか」に置き換えると理解しやすい。

機密性（Confidentiality）

権限のない者に情報を「見せない」。
例：暗号化、アクセス制御。

完全性（Integrity）

情報やソフトを勝手に「変えさせない」。
例：署名、改ざん検知。

可用性（Availability）

必要なときに製品・データを「使える」状態に保つ。停止や障害からの復旧も含む。

真正性（Authenticity）

データ・通信相手・更新プログラム等が「本物である」と確認できること。

セキュア・バイ・デザイン

後付けではなく、企画・設計段階から脅威と対策を製品要件に組み込む考え方。

セキュア・バイ・デフォルト

利用者が追加設定をしなくても、出荷時・初期状態から安全側の設定になっている考え方。

DDoS耐性：多数の端末等から大量通信を送り、サービスを使えなくするDDoS攻撃に対して、機能を維持・劣化運転・復旧できる力。主に「可用性」の論点。

参考：CRA Annex I / CISA Secure by Design and Default

用語ガイド④　EU製品法・標準化・適合性評価

CRAは単独のIT法ではなく、EU製品法の共通枠組みと標準化制度の上に乗っている。

New Legislative Framework / CE

NLFは経済事業者、適合性評価、市場監視、CE表示等を共通化するEU製品法の枠組み。CEは適用法令への適合を示す表示で、品質マークではない

CEN

European Committee for Standardization。
幅広い分野の欧州標準化機関。

CENELEC

European Committee for Electrotechnical Standardization
電気・電子分野の欧州標準化機関

ETSI

European Telecommunications Standards Institute。
ICT・通信分野の欧州標準化機関。CEN/CENELEC/ETSIはいずれもEUが認めるESO

RED委任規則

Radio Equipment Directive（RED）のサイバー要件を具体化する委任規則(EU) 2022/30。無線機器ではCRA前から先行対応が問題になる。

Class I / Class II

CRA Annex IIIの「重要製品」の二段階。
Class Iは条件を満たせばModule A自己評価が可能。
Class IIは原則として第三者関与が必須で、より高いリスクを想定。

参考：European Commission Blue Guide / CRA Article 32 / CEN-CENELEC-ETSI / RED

全体像：CRAは「製品ライフサイクル」規制である

設計・製造・販売・更新・終了まで、製品の一生を見ている。

企画・設計

リスク評価
セキュア・バイ・デザイン

→

開発・製造

安全な初期設定
脆弱性を作り込まない

→

市場投入

技術文書
適合性評価
CEマーキング

→

運用・更新

脆弱性対応
セキュリティ更新
ユーザー通知

→

終了

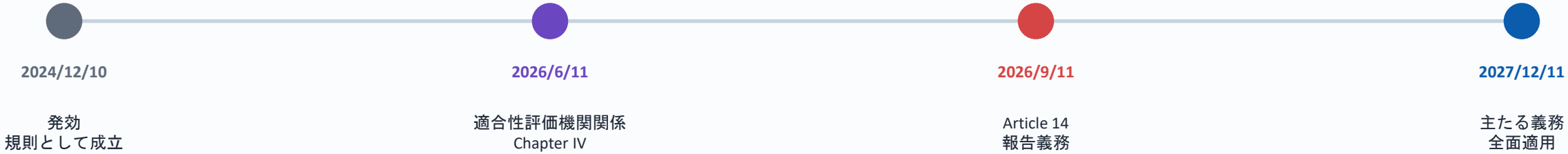
サポート終了日の表示
安全な廃止

**コンプライアンス担当者は「販売時点のチェックリスト」だけでなく、
製品開発プロセス、サポート方針、脆弱性対応フローをつなげて見る必要がある。**

根拠：CRA Article 13、Annex I、Annex II、Article 30

適用時期：2つの山場を分けて考える

2026年9月11日と2027年12月11日は、求められる準備が違う。



2026年9月11日まで

事故・脆弱性を把握した時に24時間で初動できる体制を作る。
対象は既存製品にも及ぶ。

2027年12月11日まで

新規・実質変更製品について、設計、技術文書、適合性評価、CE表示まで整備する。

根拠：CRA Article 69、Article 71、European Commission CRA policy page

誰に・何に適用されるのか

日本企業が最初に確認すべきは「自社製品が入るか」と「自社が製造者に当たるか」である。

対象製品：「デジタル要素を含む製品」

定義は広い。ソフトウェア、ハードウェア、一定のリモート処理まで含まれる。

法令上の基本形

software or hardware product
＋
remote data processing solutions
＋
別個に市場投入されるソフト・ハード部品

接続要件

意図された目的又は合理的に予見可能な使用に、

直接・間接の
論理的又は物理的な
デバイス・ネットワーク接続が含まれること

実務感覚

**「インターネットにつながるか」だけでなく、API・Bluetooth・USB・組込み通信・クラウド連携など、
製品機能の一部としてデータ接続が予定されていれば検討対象になる。**

根拠：CRA Article 2(1)、Article 3(1)〜(10)

見分け方：まずは3問で一次判定する

法務部門だけでなく、製品部門と一緒に棚卸しする。

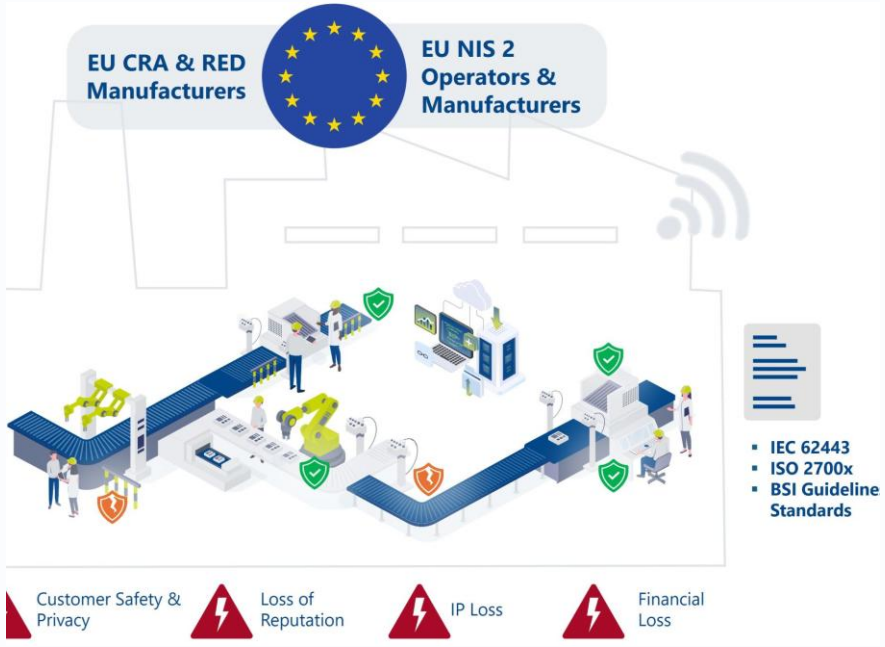
3問すべてが「はい」なら、CRA対象の可能性が高い

次に、除外規定、重要製品・クリティカル製品の該当性、製造者・輸入者・販売者の役割分担を確認する。

Reg. Arts.2,3,7,8,13,19-23

日本メーカーの典型例：どの製品が問題になるか

「完成品」だけでなく、組込み部品・ソフトウェア・更新機能も見る。



検討対象になり得る例

・ネットワーク機器、ルーター、スイッチ
・産業機械、制御装置、組込みコントローラ
・IoT家電、スマートホーム機器
・ファームウェア、アプリ、管理ソフト
・認証、VPN、セキュリティ監視製品
・クラウド側処理がなければ機能しない製品

ポイント：製品名ではなく「機能」と「接続」を見る。EUのガイダンスも、リモートデータ処理・OSS・実質変更など、境界事例への説明を重視している。

根拠：CRA Articles 2, 3、European Commission guidance（2026年7月27日）

対象外・隣接規制：除外されるから安心、とは限らない

医療機器・自動車・航空等には別のEUルールがある。

明示的除外の例

医療機器規則、IVD規則、自動車一般安全規則の対象製品、航空認証製品、船舶設備、国家安全・防衛専用製品等

セクター規制との関係

他のEUルールが同等以上にサイバーリスクを扱う場合、CRAの適用は限定・除外され得る。委任規則(EU)2025/1535による除外もある。

日本企業の実務

対象外判断は「製品法務メモ」として残す。EU代理人・輸入者・販売先にも説明できる粒度にする。

注意すべき落とし穴

「自動車向け部品」「医療機器向けソフト」だから一律対象外、とは言い切れない。
どのEU法の対象か、単体で市場投入されるか、別途ソフトウェアとして提供されるかを確認する。

根拠：CRA Article 2、委任規則(EU)2025/1535、Commission guidance

誰が義務を負うのか：経済事業者の役割分担

日本本社だけで完結しない。EU現地法人・輸入者・販売者との分担が問題になる。

製造者

開発・製造し、自己名称・商標で市場に出す者
主要義務・報告義務の中心

EU代理人

書面委任を受ける者
一定の連絡・文書対応

輸入者

EU域外からEU市場へ投入
脆弱性・重大リスクを把握したら対応

販売者

市場で提供
CE・文書確認、不適合時の販売停止

日本企業が自己ブランドでEU向け製品を出す場合、基本は「製造者」として扱われる。
EU販売会社・輸入者へ丸投げしても、設計・脆弱性・報告体制の中核責任は残る。

根拠：CRA Articles 3(12)(13)、18〜23

「製造者」になる瞬間：名称・商標・実質変更に注意

自社工場で作っていなくても製造者になる場面がある。

自己ブランド

OEM・ODMでも、自社名称・商標でEU市場に出せば製造者になり得る。

開発委託

設計・開発・製造を他社に委託しても、自己名義で市場に出す者が製造者となり得る。

実質変更

既存製品にサイバーリスクへ影響する変更を加え市場提供すると、変更者が製造者扱いになる。

実務上の意味

販売会社・SIer・顧客向けカスタマイズ部門が、意図せず「製造者義務」を負う可能性がある。
標準品、カスタム品、アップデート、EU向けラベル変更を分けて管理する。

根拠：CRA Articles 3(13)、21、22

Part 2

製造者に何が求められるのか

CRA対応は「条文暗記」ではなく、製品開発プロセスの設計変更である。

義務の三層構造：製品・プロセス・市場対応

CRAの読み方は、この3層で整理すると分かりやすい。

第1層
製品そのもの

セキュア・バイ・デザイン
セキュア・バイ・デフォルト
認証・暗号・ログ・データ最小化

第2層
製造者のプロセス

リスク評価
技術文書
SBOM
脆弱性受付・修正・更新

第3層
市場対応

適合性評価
EU適合宣言
CEマーキング
報告・通知・リコール

製品部門だけ、法務だけ、CSIRTだけでは対応できない。
品質保証・開発・サポート・EU販売チャネルまでつなげる必要がある。

根拠： CRA Articles 13, 14, 28〜32、Annex I〜II

セキュア・バイ・デザイン：開発段階からリスクを織り込む

Article 13は、計画・設計・開発・製造・提供・保守の全段階でリスク評価を反映するよう求める。

計画

利用目的・利用環境・守るべき資産を定義

設計

攻撃面を減らし、認証・暗号・ログを設計

開発

第三者部品・OSSを含め脆弱性を管理

製造

既知の悪用可能な脆弱性を残さない

保守

サポート期間中、脆弱性を処理し更新を提供

日本企業では、開発プロセス規程・品質保証手順・製品安全審査・セキュリティレビューを統合することが現実的である。

根拠：CRA Article 13(1)〜(4)、Annex I Part I

製品の基本要件：Annex I Part Iを実務語に直す

「何を守るべきか」は法令がかなり具体的に示している。

既知の悪用可能な脆弱性なし

市場投入時点で既知の危険を放置しない

安全な初期設定

ユーザーが設定変更しなくても安全な状態

更新可能性

自動更新・通知・延期などを設計

不正アクセス防止

認証、ID、アクセス管理

機密性・完全性・可用性・真正性

「見せない・変えさせない・止めない・本物と確認」
暗号化、改ざん防止、DDoS耐性

データ最小化・ログ

必要なデータだけ処理し、関連活動を記録

ポイント：セキュリティ機能の有無だけでなく、「標準状態」「更新方法」「ユーザーへの説明」まで含めて評価される。

根拠：CRA Annex I Part I

脆弱性ハンドリング：発見後の運用まで法令要件になる

CRAは「出荷して終わり」ではなく、サポート期間中の脆弱性管理を要求する。

発見・受付

内部検知
外部報告
第三者部品

→

記録・評価

重大性
悪用有無
影響製品

→

修正・更新

パッチ（修正更新）
回避策
セキュリティ更新

→

報告・通知

Article 14
ユーザー通知
CVD（協調的開示）

社内論点

PSIRT（製品脆弱性対応）又はCSIRT（事故対応）が、製品部門・品質保証・法務・EU販売会社とつながっているか。外部研究者からの報告窓口、CVD、パッチ公開判断は決まっているか。

根拠：CRA Article 13(8)、Annex I Part II、Article 14

Reg. Art.13, Annex I-II, Art.14

SBOM：サプライチェーンを「見える化」するための台帳

Annex I Part IIは、少なくともトップレベル依存関係を含む機械可読のSBOM作成を求める。

なぜ必要か

一つのOSSや部品に重大脆弱性が出たとき、
「どの製品に入っているか」
「EU市場に出たものはどれか」
「ユーザー通知・パッチ対象は何か」
を短時間で特定するため。

SBOMは文書作成作業ではなく、24時間報告・パッチ・顧客通知を可能にする基盤である。

根拠：CRA Annex I Part II(1)、Article 13(24)(25)

サポート期間：最低5年が原則、表示も必要

ユーザーが「いつまで脆弱性対応・更新を受けられるか」を購入時に分かるようにする。

原則

製品が使用されると期待される期間を反映。
ただし少なくとも5年。

例外

想定使用期間が5年未満なら、その想定使用期間に対応するサポート期間。

表示

サポート終了時期を月・年まで明示。更新は発行後10年間入手可能に保つ。

実務上の難所

営業上の製品寿命、品質保証期間、部品供給期間、ソフトウェア保守期間がバラバラだとCRA対応で詰まる。
製品企画段階で「サイバーサポート期間」を決める必要がある。

根拠：CRA Article 13(8)(9)(18)(19)、Annex II(7)

リスク評価と技術文書：後から説明できることが重要

適合性は「やっている」だけでなく、文書で示せなければならない。

リスク評価に含めるべき視点

・意図された目的
・合理的に予見可能な使用
・使用環境、守るべき資産
・製品が使用される期間
・どのAnnex I要件が適用されるか
・適用しない要件の理由

技術文書の性質

・市場投入前に作成
・サポート期間中、必要に応じ更新
・適合性評価の基礎
・当局から要請された場合に提示
・製品部門だけでなく法務・品質保証も関与

日本法の「記録化」「説明責任」「内部統制」と同じく、事後的に説明できる粒度が実務の生命線になる。

根拠：CRA Article 13(2)〜(4)、Article 31、Annex VII

条文を読まないと落ちる6つの義務

設計要件と報告義務の陰に、出荷後に効く義務が並んでいる。

単一の連絡窓口

ユーザーが直接・迅速に連絡できる窓口を指定し説明書に記載。自動応答のみは不可（13条17項）。

セキュリティ更新の10年提供

提供した更新は、発行後10年又はサポート期間の残りのうち長い方の期間、入手可能に保つ（13条9項）。

技術文書の10年保管

技術文書とEU適合宣言を、上市後10年又はサポート期間の長い方の間、当局へ提示できる状態に置く（13条13項）。

是正・撤回・回収

不適合を知り又は疑う理由があれば直ちに是正し、必要なら市場からの撤回・回収を行う（13条21項）。

事業終了時の事前通知

事業終了により義務を履行できなくなる場合、事前に市場監視当局とユーザーへ通知する（13条23項）。

量産品の適合維持

シリーズ生産品が適合を維持する手続を整備し、規格改訂も反映する（13条14項）。

ポイント：いずれも「売った後」に効く義務である。サポート終了品・生産終了品・事業譲渡した製品ラインの扱いを、製品規程と契約に落とし込む必要がある。

根拠： CRA Article 13(9)(13)(14)(17)(18)(21)(23)

適合性評価：製品分類で手続が変わる

通常製品、重要製品、クリティカル製品で、第三者関与の程度が変わる。

通常製品

内部統制手続（Module A）
による自己評価が原則
メーカー自身が評価し、EU適合宣言を作成

重要製品

Annex III Class I / II
Class I：整合規格等を全面適用すればModule A自己評価可。それ以外は第三者関与。
Class II：整合規格利用の有無にかかわらず第三者関与等が必要。

クリティカル製品

Annex IV
委任法令により欧州サイバーセキュリティ認証（水準「相当」以上）が求められ得る

実務の順序

①対象製品か → ②製品分類 → ③使える整合規格・共通仕様・認証制度 → ④適合性評価手続 → ⑤EU適合宣言・CE表示

根拠：CRA Articles 7, 8, 27, 28, 30, 32、Annex III, IV, V, VIII

整合規格はまだ揃っていない：適合推定を当てにしない

規格が出るのを待つと、2027年12月に間に合わない。

整合規格の現状

・標準化要請M/606をCEN（一般）／CENELEC（電気・電子）／ETSI（ICT・通信）が受託
・約41規格が対象。全面適用に向け順次策定
・EU官報に引用されて初めて「適合推定」が働く
・現時点ではAnnex Iを基礎に自社で適合を立証

無線機器はRED委任規則が先行

・RED＝Radio Equipment Directive（無線機器指令）
・委任規則(EU) 2022/30がサイバー要件を具体化（2025年8月1日適用）
・EN 18031-1〜3が整合規格として引用（一部制限あり）
・CRA移行期はREDとCRAの関係を製品別に確認

実務メモ：無線を含む製品はRED対応状況を棚卸しし、CRA技術文書へ引き継ぐ前提で証跡を残す。規格が未成熟であることは、着手を遅らせる理由にはならない。

根拠：標準化要請M/606、委任規則(EU)2022/30、EN 18031、CRA Article 27

重要製品・クリティカル製品：分類が実務負担を左右する

自社製品がAnnex III / IVに入るかは、最初に確認すべき論点である。

Annex III 重要製品の例

Class I：ID/PAM、ブラウザ、パスワード管理、VPN、ネットワーク管理、SIEM、OS、ルーター・モデム・スイッチ、セキュリティ機能付きスマートホーム等

Class II：ハイパーバイザー、コンテナランタイム、Firewall、IDS/IPS、耐タンパ性MPU/MCU等

Annex IV クリティカル製品の例

Hardware Devices with Security Boxes
スマートメーターゲートウェイ等
スマートカード又は類似デバイス

今後、委任法令で追加・変更される可能性もある。

日本メーカーでは、完成品が該当しなくても、組込みモジュール・管理ソフト・セキュリティ機能部分が分類に影響することがある。

根拠：CRA Annex III、Annex IV、Articles 7, 8

製品分類は実施規則の技術的記述で確認する

Annex III / IVのカテゴリ名だけでは、自社製品の該否は判断できない。

実施規則(EU)2025/2392

2025年11月28日採択。重要製品・クリティカル製品の各カテゴリについて技術的記述を定める。

カテゴリごとに対象となる機能・用途が具体化されており、分類判断の一次資料になる。

分類実務の進め方

①製品の主要機能を書き出す
②実施規則の技術的記述と照合する
③該当・非該当の理由を文書化する

④Class Iは整合規格の利用可否を確認する

完成品ではなく、ルーター・スイッチ機能、セキュリティ機能付きスマートホーム機器、耐タンパ性MPU/MCUなどの組込み部分で分類に該当する例が多い。分類は委任法令で変わり得るため、年次で見直す。

根拠：Commission Implementing Regulation (EU) 2025/2392、CRA Articles 7, 8、Annex III, IV

CEマーキング：サイバーが市場アクセス要件になる

「品質表示」ではなく、EU市場に出すための適合表示として理解する。

CE

Cyber

CE表示までに必要な主な要素

- 製品分類の確認
- 必須サイバーセキュリティ要件への適合
- 技術文書
- 適合性評価手続
- EU適合宣言
- 表示、説明書、サポート期間の情報

コンプライアンス部門の役割は、最後にCE文書を確認するだけではなく、開発段階で必要な証跡が残るようにプロセスを設計することである。

根拠：CRA Articles 28, 30、Annex V, VI

Part 3

2026年9月11日の報告義務

全面適用より先に、事故・脆弱性を把握した瞬間から法的時計が動く。

9月11日から始まる「最初の本番」

Article 14は2026年9月11日から先行適用される。

Article 14

報告義務

対象1

積極的に悪用されている
脆弱性

対象2

製品セキュリティに影響する
重大インシデント

ポイント

脆弱性を発見したらすべて24時間報告、ではない。
しかし、悪用又は重大事故を把握した後に社内で迷っている時間はほとんどない。

根拠：CRA Article 14、Article 71、European Commission CRA reporting page

報告対象1：「積極的に悪用されている脆弱性」

通常の脆弱性管理と、法定報告のトリガーを分ける。

報告対象になり得る

・自社製品の脆弱性が攻撃に使われた信頼できる証拠
・顧客環境で悪用が確認
・攻撃コードが実運用で使われている
・CSIRT/SOC/外部研究者から悪用情報を受領

直ちには該当しない例

・脆弱性を発見しただけ
・CVE（公開脆弱性の共通ID）が付いたが悪用証拠はない
・PoC（再現・検証コード）が存在するだけ
・研究者が善意で検証しただけ

ただし、通常の脆弱性対応は必要。

実務メモ：社内分類名を「通常脆弱性」「悪用疑い」「悪用確認」に分け、Article 14の判断者とエスカレーション期限を事前に決める。

根拠：CRA Article 14(1)(2)、ENISA SRP FAQ、European Commission reporting page

報告対象2：製品セキュリティに影響する重大インシデント

「会社のIT事故」すべてではなく、製品のセキュリティへ影響する事故を見る。

重大とされる方向性

製品が重要データ又は機能の
可用性・真正性・完全性・機密性を
保護する能力を損なう、又は損ない得る場合。

典型的に問題になる例

製品又はユーザーのネットワーク・情報システムに、悪性コードを導入・実行させた、又はその可能性がある場合。

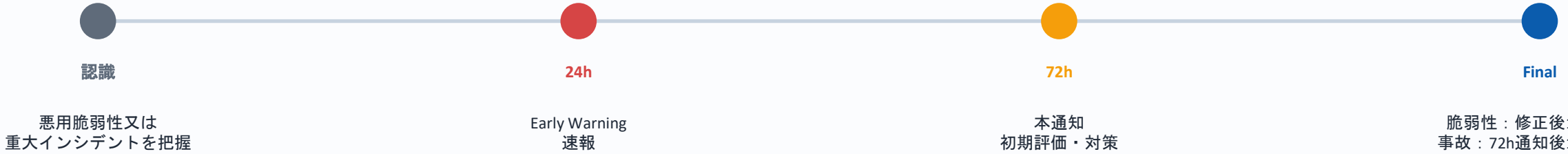
例：製品アップデート経路の侵害、署名鍵漏えい、開発環境侵害によるマルウェア混入リスク。

「個人情報漏えい」「サービス停止」「開発環境侵害」との重なりを、GDPR・NIS2・契約上の通知義務と横断して判断する必要がある。

根拠：CRA Article 14(3)〜(5)

24時間・72時間・最終報告：時計は「認識」から動く

初動判断が遅れると、法令上の報告期限に間に合わない。



社内で決めるべきこと

「誰が認識したら会社として認識か」「SOC・海外子会社・販売代理店・品質保証から何時間で本社法務/PSIRTへ上げるか」「不明なまま速報する条件」を決める。

根拠：CRA Article 14(2)(4)、European Commission reporting page

「認識」とはいつか：24時間時計の起点を社内運用へ落とす

条文上の“becoming aware”を、時刻記録・判断者・エスカレーション期限に落とす。

端緒

顧客・SOC・販売店・研究者から、悪用又は重大事故の兆候を受領。

信頼できる情報

ログ、攻撃痕跡、製品影響など、合理的に疑える材料がある。

社内到達時刻

PSIRT・法務・指定責任者への到達時刻も記録する。ただし、これによって法的な「認識」の時点を後ろ倒しできるわけではない。

不明でも速報

24時間は完全調査ではなくEarly Warning。不確実性も併記する。

時刻を記録

受領時刻、判断時刻、判断者、根拠、未確定事項を残す。

期限を逆算

海外子会社・販売代理店から本社へ「数時間以内」に上げる。

ポイント：顧客・販売会社・SOC等が信頼できる情報を得た時点から時刻を記録し、24時間時計を「法務が確定判断した時」まで遅らせない。

根拠：CRA Article 14、European Commission reporting page、ENISA SRP guidance

どこへ報告するのか：Single Reporting Platform

ENISAが構築するSRP（Single Reporting Platform）から一度報告し、調整役CSIRTとENISAへ届ける。

EUに主たる拠点がないメーカー

①当該メーカーの最も多くの製品を代理するEU代理人の所在地 → ②最も多くの製品を上市する輸入者の所在地 →
③最も多くの製品を市場提供する販売者の所在地 → ④最も多くのユーザーが所在する加盟国、の順で判断する。

根拠：CRA Articles 14(7), 16、ENISA SRP page/FAQ

当局報告だけでは終わらない：ユーザー通知もある

脆弱性・事故と、ユーザーが取れる緩和措置を知らせる必要がある。

当局報告

CSIRT designated as coordinator
＋ENISA

24時間・72時間・最終報告

→

ユーザー通知

影響を受けるユーザー
必要に応じ全ユーザー

緩和措置・是正措置

→

広報

FAQ
パッチ
顧客対応
営業説明

日本本社の実務：EU向けWeb公表、販売代理店通知、顧客サポート窓口、パッチ配布、契約上通知の整合を事前に決める。

根拠：CRA Article 14(8)

重畳する通知義務：1つの事故から複数の時計が動く

CRAだけを見ず、NIS2・GDPR・契約通知を同じ初動で仕分ける。

CRA

製品の悪用脆弱性・重大インシデント。SRP経由でCSIRT/ENISAへ24h・72h。

NIS2（EU組織向けサイバー法）

EU現地法人等が対象なら、重大インシデントについて24h・72h・1か月。

GDPR

個人データ侵害なら監督機関72h。高リスクなら本人通知も検討。

日本法

個人情報、製品安全、委託・下請、上場会社開示の観点も並走。

契約通知

顧客、販売店、クラウド、部品供給元への通知期限は契約ごとに異なる。

初動設計

受付票に「製品・個人データ・NIS2・契約」を入れ、同時起動する。

ポイント：最初の1時間で「どの通知義務が動き得るか」を横断判定する。個別部門の縦割り対応では間に合わない。

根拠：CRA Article 14、NIS2 Directive Article 23、GDPR Articles 33・34

既存製品にも注意：第14条は過去の市場投入品にも及ぶ

2027年12月前にEU市場へ出した製品についても、報告義務は原則として対象になる。

原則

2027年12月11日前に市場投入された製品は、同日以降に実質変更される場合などを除き、CRA本体要件は限定的。

例外：Article 14

報告義務は、2027年12月11日前に市場投入されたCRA対象製品にも適用される。

例　**2023年からEUで販売しているネットワーク対応機器について、2026年9月20日に現実の悪用を把握した場合、Article 14報告義務の検討対象になる。**

根拠：CRA Article 69(2)(3)、Article 71

制裁金：最大2.5%の世界売上高という枠組み

制裁金を含む第VII章の適用は2027年12月11日から。金額・手続は各加盟国法で定まる。

Articles 13・14等

最大1,500万ユーロ
又は
前年度全世界年間売上高2.5%
いずれか高い額

その他の義務

最大1,000万ユーロ
又は
前年度全世界年間売上高2%

誤情報提供

最大500万ユーロ
又は
前年度全世界年間売上高1%

実務上の読み方

零細・小規模の製造者には、24時間Early Warning期限違反に関する行政制裁金の限定的例外がある（Article 64(10)・2025年訂正反映）。詳細は次頁。

根拠：CRA Articles 64, 71 / Corrigendum (EU) 2025/90555

小規模・零細企業：誰が該当し、何が軽減されるか

EUの企業規模定義を確認する。日本の資本金基準では判定しない。

零細企業（micro）

従業員10人未満 ＋ 年間売上高200万ユーロ以下 又は 貸借対照表総額200万ユーロ以下。
関連企業・パートナー企業の数値を合算する場合がある。

小規模企業（small）

従業員50人未満 ＋ 年間売上高1,000万ユーロ以下 又は 貸借対照表総額1,000万ユーロ以下
日本の「中小企業」区分とは別物。

CRA上の支援・簡素化

Article 33は研修・専用窓口・試験支援等を予定。零細・小規模企業には簡素化した
技術文書様式が用意され、適合性評価手数料も企業規模等に配慮。

24時間速報の注意

零細・小規模の製造者は、Article 14の24時間Early Warning期限違反について行政制裁金
の例外がある。ただし、報告義務そのものが免除されるわけではない。

重要：行政制裁金の例外は「24時間Early Warningの期限」に関する限定的なもの。脆弱性対応、ユーザー通知、72時間通知・最終報告等を含むCRA対応が不要になるわけではない。

根拠：EU SME Definition / CRA Articles 32(6), 33, 64(10)（Corrigendum 2025/90555反映）

Part 4

日本企業のコンプライアンス実装

法令知識を、社内体制・契約・製品開発・報告フローに落とす。

第三者部品・OSS：調達管理と脆弱性管理がつながる

CRAは第三者部品・OSSの統合について、製造者のデューデリジェンスを求める。

調達前

・部品・OSSのセキュリティ評価
・ライセンスだけでなく脆弱性管理状況
・サポート期間との整合

統合時

・SBOMへ反映
・トップレベル依存関係の把握
・脆弱性が製品へ与える影響評価

脆弱性発見時

・保守者への報告
・修正・回避策
・顧客通知・Article 14判断
・必要に応じコード/文書共有

法務部門はOSSライセンス審査だけでなく、SBOM、脆弱性情報、保守終了リスクを調達・開発プロセスに組み込む必要がある。

根拠：CRA Article 13(5)(6)、Annex I Part II

実質変更：アップデートが新たな義務を呼ぶ

サイバーリスクを変えるソフトウェア変更は、単なる保守では済まない場合がある。

実質変更になり得る

・意図された目的を変更するアップデート
・サイバーリスクの性質又は水準が増加
・初期リスク評価で想定していない変更
・変更後製品が市場提供される

社内手続に入れるべき問い

・この変更は機能変更か、単なる修正か
・通信先・認証・権限・データ処理は変わるか
・EU市場向けに提供されるか
・技術文書・リスク評価を更新すべきか

ソフトウェア更新を「開発部門の通常業務」として処理すると、CRA上の実質変更判定が抜け落ちる。リリース判定会議に法務・セキュリティ観点を入れる。

根拠：CRA Recitals 38〜39、Articles 21, 22、Commission guidance

EU販売チャネルとの契約：情報が24時間で流れるか

Article 14対応は、日本本社だけでは完結しない。

EU輸入者・販売者

重大リスク・脆弱性情報を本社へ即時共有
CE・適合宣言・説明書の確認責任

顧客・SIer

実質変更・カスタマイズ時の責任分担
事故時のログ・影響情報の共有

部品・OSS供給元

脆弱性情報、修正予定、サポート終了情報
SBOM更新への協力

契約条項の発想

「セキュリティ事故を通知する」では遅い。悪用情報・重大インシデント疑い・顧客環境での兆候・当局照会を何時間以内に誰へ通知するかを具体化する。

社内体制：CRAは部門横断のプロジェクトである

コンプライアンス部門は司令塔ではなく、判断基準と証跡の設計者になる。

法務・コンプラ

対象判定
義務整理
報告判断
契約条項

製品開発

リスク評価
設計要件
SBOM
技術文書

品質保証

リリース審査
適合性評価
証跡管理
サポート期間

CSIRT/PSIRT

脆弱性受付
悪用判定
24h報告
ユーザー通知

経営・取締役会への報告

対象製品数、重要製品該当、未整備項目、重大脆弱性、期限超過リスクを定例報告する。

日本の制度との対比：どこが同じで、どこが違うか

日本法の枠組みに置き換えると、社内説明が通りやすい。

日本法と似ている点

・CE表示は、EU製品法への適合をメーカーが示す市場アクセス上の表示
・技術文書の作成・保管は品質保証の記録管理と近い発想
・是正・回収は日本の製品リコール対応と共通点がある
・JC-STAR等で整備した証跡は一部流用できる

日本法と違う点

・報告先が加盟国CSIRTとENISAの二者で、期限は24時間・72時間
・個人情報保護法の漏えい報告（速報おおむね3〜5日、確報30日）より格段に短い
・報告の起点が個人データではなく「製品脆弱性の悪用」である
・サポート期間の表示自体が法定義務になる

JC-STARは★1が2025年3月開始、★2以上は2026年以降順次。英国PSTI法・シンガポールCLSとの相互承認覚書も締結されている。

実務メモ：JC-STAR、ETSI EN 303 645、英国PSTI、シンガポールCLSは次頁で整理する。相互承認・証跡流用があっても、CRA適合を自動的に意味するわけではない。

根拠：JC-STAR（IPA・経済産業省）、個人情報保護法26条・同規則、CRA Articles 13, 14

隣接制度を整理：JC-STAR・EN 303 645・PSTI・CLS

「法律」「標準」「ラベル制度」を混同しない。証跡の流用・相互承認があっても制度目的は別である。

JC-STAR（IPA）

日本のIoT製品向けセキュリティ適合評価・ラベリング制度。★の段階で要求・評価水準を可視化する。CRAへの自動適合を意味する制度ではない。

ETSI EN 303 645

消費者向けIoTのサイバーセキュリティ基準となる欧州標準。パスワード、脆弱性開示、更新等のベースラインを示す。CRAの整合規格と自動的に同一ではない。

英国PSTI法

英国の消費者向け接続製品に対する強制的な製品セキュリティ規制。パスワード、脆弱性報告窓口、最低セキュリティ更新期間の情報等が中心。

シンガポールCLS

CSAのCybersecurity Labelling Scheme。消費者向けIoT等のセキュリティ水準を4段階のラベルで可視化する制度。

関係：JC-STARと英国PSTIは2026年1月1日から相互承認手続、JC-STARとシンガポールCLSは2026年6月1日から相互承認を開始。ただし「一つを取ればCRA適合」という関係ではない。

参考：IPA JC-STAR / ETSI EN 303 645 / UK PSTI / Singapore CSA CLS

直近対応：9月11日報告義務に向けた最小セット

全面適用対応より先に、Article 14対応を独立して走らせる。

- **EU市場に出ているCRA対象候補製品の棚卸し**
- **Article 14判断責任者・代替責任者の指定**
- **悪用脆弱性／重大インシデントの社内分類基準**
- SOC・PSIRT・品質保証・海外子会社からの即時エスカレーション
- 24h速報・72h通知・最終報告テンプレート
- SRP利用者・EU Login・報告先CSIRTの確認
- 顧客通知・パッチ公開・広報レビューの手順
- 既存製品・販売終了製品のサポート責任の確認

根拠：CRA Article 14、Article 69、ENISA SRP FAQ

2027年12月11日全面適用に向けたロードマップ

1年半で「開発プロセス」まで変える必要がある。

Phase 1
棚卸し

対象製品
EU市場
分類
責任者

→

Phase 2
ギャップ分析

Annex I
技術文書
SBOM
サポート期間

→

Phase 3
制度設計

開発標準
脆弱性対応
契約
報告フロー

→

Phase 4
適合性評価

整合規格
第三者評価
EU適合宣言
CE表示

→

Phase 5
運用

監視
更新
当局対応
経営報告

2027年末の「書類作成」では間に合わない。2026年中に棚卸しとギャップ分析、2027年前半にプロセス改訂・標準化、2027年後半に適合性評価とCE対応へ進む。

Reg. Arts.13,28-32, Annexes I-VIII

ケーススタディ：EU向け産業用IoT装置

自社製品に当てはめると、CRA対応の全体像が見える。

製品

工場設備に接続するIoTゲートウェイ
遠隔監視クラウドあり
ファーム更新機能あり

CRA論点

対象製品性
遠隔データ処理
SBOM
安全な初期設定
サポート期間

事故時

顧客環境で悪用確認
24h速報
72h通知
顧客へ緩和策通知

経営

出荷停止
パッチ
EU当局
販売先説明

コンプライアンス部門が確認すべき資料

対象判定メモ、製品分類、リスク評価、技術文書、SBOM、サポート期間根拠、CVDポリシー、Article 14判断フロー、EU販売チャネル連絡網。

よくある誤解

社内説明では、最初にここを潰しておくと議論が早い。

誤解1	EU市場で製品を提供する日本企業にも問題になる
誤解2	2026年9月11日から報告義務が先行する
誤解3	報告対象は積極的に悪用されている脆弱性等
誤解4	製品開発・品質保証・法務・販売の横断課題
誤解5	設計・開発段階の証跡がないと間に合わない

本日の結論

1. CRAは、サイバーセキュリティをEU市場アクセス要件にする規則である。
2. 2026年9月11日から、悪用脆弱性・重大インシデントの報告義務が先行する。
3. 2027年12月11日の全面適用までに、設計・開発・技術文書・適合性評価・CE表示を整備する。
4. 日本メーカーは、EU販売チャネル、OSS、サポート期間、脆弱性対応を部門横断で管理する必要がある。
5. コンプライアンス部門の役割は、最後の法令確認ではなく、製品ライフサイクルの統制設計である。

次にやること：EU対象製品の棚卸しとArticle 14対応フローの整備から始める。

日本企業の必要最小限チェックリスト

まずここだけ確認する。詳細対応は、製品分類・EU販売形態・既存体制に応じて深掘りする。

□ 1　対象製品台帳

EU市場向けの対象候補製品を、既存品・販売終了品・サポート中製品まで棚卸しする。

□ 2　Article 14体制

悪用脆弱性・重大インシデントの判断責任者、代替者、24時間内の社内期限を決める。

□ 3　SRP・CSIRT

SRP利用者、EU Login、報告先CSIRT、EU代理人・輸入者・販売者の情報経路を確認する。

□ 4　顧客通知・パッチ

ユーザー通知、緩和策、パッチ、FAQ、営業説明、広報レビューの最小手順を用意する。

□ 5　全面適用ギャップ

Annex I要件、SBOM、CVD、サポート期間、技術文書10年保管の未整備項目を出す。

□ 6　CEまでの出口

重要/クリティカル分類、整合規格、適合性評価、EU適合宣言、CE表示の責任者を決める。

結論：最初に作るべきものは「対象製品台帳」と「24時間報告フロー」である。ここから2027年12月の全面適用対応へ接続する。

根拠：CRA Articles 13・14・28〜32、Annex I〜VIII

主な参考資料

本資料は2026年8月17日時点で公表されている資料を前提とする。

- Regulation (EU) 2024/2847 — Cyber Resilience Act（EUR-Lex）
- European Commission, Commission guidance on the application of the CRA（C(2026) 5252、2026年7月27日、約80頁）
- European Commission, CRA implementation FAQ / CRA reporting obligations / CRA summary
- ENISA, CRA Single Reporting Platform (SRP) / CSIRT・SOC / Vulnerability Disclosure
- Implementing Reg. (EU) 2025/2392 / RED Delegated Reg. (EU) 2022/30 / 標準化要請M/606
- NIS2 Directive / GDPR / EU SME Definition / Corrigendum (EU) 2025/90555
- CISA Secure by Design / CVE Program / NIST DDoS / IPA JC-STAR / ETSI EN 303 645 / UK PSTI / Singapore CLS

注記

本資料は一般的な情報提供であり、個別事案の法的助言ではない。具体的対応は製品・販売形態・EU域内体制に応じて確認が必要である。