弁護士法人　三宅法律事務所

Miyake　& Partners

デジタル・ガバナンス／サイバーセキュリティニュース No.9

EU サイバーレジリエンス法（CRA）の実務対応

― 2026 年 9 月 11 日の「24 時間報告」から 2027 年 12 月 11 日の全面適用まで ―

平素より大変お世話になっております。

さて、今回は「EU サイバーレジリエンス法（CRA）の実務対応」をご案内いたします。CRA について、「2027 年 12 月から適用されるので対応はまだ先でよい」と理解している企業も少なくありません。しかし、製造者に直接かかる最初の大きな実務対応は、2026 年 9 月 11 日に始まります。

同日から、積極的に悪用されている脆弱性及び製品のセキュリティに影響する重大インシデントについて、原則として「認識から 24 時間以内」の速報を含む報告義務が先行適用されます。しかも、この報告義務は、2027 年 12 月 11 日より前に EU 市場へ投入された既存製品にも原則として及びます。

架空事案：1 通のメールから 24 時間時計が動く
日本の産業機械メーカーA 社は、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している。遠隔監視クラウドとファームウェア更新機能もある。 2026 年 9 月 20 日 15 時、ドイツ販売会社から本社営業部へ「顧客工場で、御社製品の脆弱性を使った攻撃の疑いがある。ログもある」とメールが届いた。 この時点で、既存製品でも Article 14 の報告義務が問題になるか、会社はいつ認識したと扱われるか、24 時間・72 時間で誰に何を報告するか、SBOM で影響製品を特定できるかが一斉に問題となる。

CRA は、単なる「EU の IT 規制」ではありません。サイバーセキュリティを、製品設計・開発・製造・販売・アップデート・脆弱性対応・サポート終了までの製品ライフサイクルに組み込み、最終的には CE マーキング（適用される EU 製品法への適合を示す表示）を通じて EU 市場へのアクセス要件とする規制です。

本号では、上記架空事案を念頭に、2026 年 9 月 11 日の報告義務と、2027 年 12 月 11 日の全面適用に分けて、日本の製造会社が準備すべき事項を整理します。

令和 8 年 8 月 17 日

弁護士法人三宅法律事務所

＊本ニュースレターに関するご質問・ご相談がありましたら、下記にご連絡ください。

弁護士法人三宅法律事務所

弁護士　渡邉雅之（執筆者）

TEL 03-5288-1021　FAX 03-5288-1025

Email: m-watanabe@miyake.gr.jp

EU サイバーレジリエンス法（CRA）の実務対応

― 2026 年 9 月 11 日の「24 時間報告」から 2027 年 12 月 11 日の全面適用まで ―

【目次】

本稿のポイントは、CRA 対応を「2026 年 9 月 11 日の事故対応」と「2027 年 12 月 11 日の製品開発・市場アクセス対応」に分けることである。最初に作るべきものは、「EU 向け対象製品台帳」と「24 時間報告フロー」である。

0 本文を読む前の用語ガイド

以下の用語は、CRA 本文を読むための前提である。すべてを暗記する必要はないが、「製品・開発」「事故対応」「EU 製品法」「隣接制度」のどの領域の言葉かを押さえると、後の条文・実務説明が読みやすくなる。

【用語ガイド A】製品・ソフトウェア・商流

用語	意味・実務上のポイント
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、制御装置、IoT 機器等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 ではライセンスだけでなく、脆弱性・依存関係も管理する。
SBOM	Software Bill of Materials。製品を構成するソフトウェア部品と依存関係の「部品表」。脆弱性が出た際に影響製品・バージョンを早く特定するための基盤。
パッチ	脆弱性・不具合を修正するための更新プログラム。原因を修正するものを指すことが多く、暫定的な回避策（workaround）とは区別して使われる。
OEM / ODM	CRA 上の法定用語ではない。一般に 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 では呼称より、誰の名で市場投入するかが重要。
SIer	通常「SIer（System Integrator）」と表記。複数の機器・ソフトを統合して顧客システムを構築する事業者。実質変更を加えて市場提供すると製造者義務の論点が生じ得る。

【用語ガイド B】セキュリティ・監視・脆弱性対応

用語	意味・実務上のポイント
セキュア・バイ・デザイン	セキュリティを後付けせず、企画・設計段階から脅威・リスク・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。
機密性・完全性・可用性・真正性	機密性＝見せない、完全性＝変えさせない、可用性＝必要なとき使える、真正性＝相手・データ・更新等が本物だと確認できること。
DDoS 耐性	DDoS（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攻撃）を受けても、機能を維持・劣化運転・復旧できる力。主に可用性の論点。
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。サイバー事故の調査、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の受付・評価、修正、公開、顧客対応を担うチーム。
CVD	Coordinated Vulnerability Disclosure。発見者と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プロセス。
CVE	Common Vulnerabilities and Exposures。公開された脆弱性を CVE-…という共通 ID で識別する仕組み。CVE が付いたこと自体は「攻撃に悪用された」ことを意味しない。
PoC	Proof of Concept。脆弱性を技術的に再現・検証するコードや手順。PoC の存在は実攻撃での悪用確認とは別である。

【用語ガイド C】EU 製品法・標準化・報告制度

用語	意味・実務上のポイント
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メーカーが示す表示で、品質マークではない。
CEN / CENELEC / ETSI	EU が認める欧州標準化機関。CEN＝幅広い一般分野、CENELEC＝電気・電子、ETSI＝ICT・通信。CRA の整合規格策定でも重要。
RED 委任規則	RED は Radio Equipment Directive（無線機器指令）。委任規則(EU) 2022/30 が無線機器のサイバー・プライバシー等の要件を具体化し、CRA より先に対応が問題となる。
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 はより高いリスクを想定し、原則として第三者関与等が必要。
NIS2	Directive (EU) 2022/2555。重要・重要性の高いセクター等の組織にサイバーリスク管理・インシデント報告を求める EU 法。製品規制である CRA とは対象の切り口が異なる。
ENISA	European Union Agency for Cybersecurity。EU のサイバーセキュリティ機関。CRA では SRP の運用等に関与する。
SRP	Single Reporting Platform。CRA Article 14 の報告を一元的に行う単一報告基盤。メーカーは SRP から報告する。
CSIRT designated as coordinator	NIS2 に基づき加盟国が指定する「調整役 CSIRT」。CRA の報告は当該 CSIRT と ENISA へ流れる。

【用語ガイド D】小規模企業・日本／海外の隣接制度

用語	意味・実務上のポイント
零細・小規模企業	EU 定義では、micro＝従業員 10 人未満＋売上高又は貸借対照表総額 200 万ユーロ以下、small＝従業員 50 人未満＋同 1,000 万ユーロ以下。関連企業等の数値を合算する場合がある。CRA では支援・簡素化があるが、義務全体の免除ではない。
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。★の段階でセキュリティ要件への適合水準を可視化する。CRA への自動適合を意味しない。
ETSI EN 303 645	消費者向け IoT のサイバーセキュリティに関する欧州標準。パスワード、脆弱性開示、ソフトウェア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を求める。
シンガポール CLS	Cybersecurity Labelling Scheme。シンガポール CSA が運用し、消費者向け IoT 等のセキュリティ水準を 4 段階でラベル表示する制度。

制度の関係：JC-STAR と英国 PSTI は 2026 年 1 月 1 日から相互承認手続が始まり、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している。ただし、これらの制度・標準への適合が CRA 適合を自動的に意味するわけではない。

1 CRA とは何か——「サイバー版の製品安全法制」

CRA（Regulation (EU) 2024/2847）は、一定の「デジタル要素を含む製品（product with digital elements）」について、サイバーセキュリティ上の必須要件を定める EU 規則である。特徴を一言でいえば、サイバーセキュリティを EU 市場で製品を販売するための条件にすることである。

従来の企業のサイバーセキュリティは、自社ネットワーク、サーバー、個人情報、営業秘密等を守る「企業自身の情報セキュリティ」が中心であった。これに対し CRA が主に対象とするのは、会社が販売する製品そのものがサイバー攻撃に耐えられるものになっているかである。

【図表 1】CRA を一言で整理すると

場面	主な要求
市場に出す前	セキュア設計・リスク評価・技術文書・適合性評価
市場に出した後	脆弱性管理・セキュリティ更新・ユーザー通知
事故が起きたら	24 時間速報・72 時間通知・最終報告

日本法の感覚では、CRA は新しいサイバー法であると同時に、New Legislative Framework（NLF：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）を利用した「サイバー版の製品安全法制」と理解すると全体像をつかみやすい。

2 2 つの日——2026 年 9 月 11 日と 2027 年 12 月 11 日

CRA 対応では、2026 年 9 月 11 日と 2027 年 12 月 11 日を分けて考える必要がある。求められる準備が異なるからである。

【図表 2】CRA の主な適用時期

日付	内容	企業が準備すべきこと
2024 年 12 月 10 日	CRA 発効	対象製品・社内影響の把握を開始
2026 年 6 月 11 日	適合性評価機関関係の規定が先行適用	適合性評価の外部環境を確認
2026 年 9 月 11 日	Article 14 の報告義務が先行適用	24 時間で初動できる事故・脆弱性対応体制
2027 年 12 月 11 日	主たる義務が全面適用	設計・技術文書・適合性評価・CE 表示まで整備

「2027 年 12 月まで何もしなくてよい」は誤りである。2026 年 9 月 11 日から、既存製品を含む Article 14 の法的時計が動き始める。

3 どの製品・どの企業が対象になるのか

(1) 対象製品——「デジタル要素を含む製品」

CRA の対象となる「デジタル要素を含む製品」の定義は広い。ソフトウェア、ハードウェアに加え、製品が機能を果たすために必要となる一定のリモートデータ処理も含まれる。実務では、まず次の 3 問で一次判定するとよい。

【図表 3】対象製品の一次判定

確認事項	確認のポイント
Q1 ソフトウェア又はハードウェアか	完成品だけでなく、ファームウェア・管理ソフト・部品も確認

Q2　直接又は間接にデータ接続するか	インターネットだけでなく、API・Bluetooth・USB・組込み通信・クラウド連携等も確認
Q3　EU 市場で提供されるか	EU 向けの上市・市場提供の有無を製品・バージョン単位で確認

医療機器、自動車、航空等には別の EU 法が適用され、CRA から明示的に除外される製品もある。ただし、「自動車向け部品」「医療機器向けソフト」であることのみから一律に対象外とはいえない。対象外判断も製品法務メモとして記録しておくことが望ましい。

(2) 日本企業も「製造者」になる

CRA は EU 企業だけを対象とする規制ではない。日本企業が自己の名称又は商標で CRA 対象製品を EU 市場に出せば、原則として製造者として CRA 上の義務を負う。OEM・ODM は CRA の法定類型ではなく実務用語であり、一般に 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を指す。結局は呼称ではなく、誰の名で市場投入するか等が重要である。SIer（System Integrator）が製品に実質変更を加えて市場提供する場合も「製造者」扱いの論点が生じ得る。

EU 現地法人、輸入者又は販売者に販売実務を委ねても、日本本社が製造者として負う設計・脆弱性管理等の中核的責任が当然になくなるわけではない。

4 製造者に求められる義務の全体像

CRA の製造者義務は、「製品そのもの」「製造者のプロセス」「市場対応」の 3 層で整理すると分かりやすい。

【図表 4】製造者義務の三層構造

層	主な内容	日本企業の担当部門の例
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・ログ等	製品開発、製品セキュリティ
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	開発、品質保証、PSIRT/CSIRT、法務
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・撤回・回収	品質保証、法務、EU 販売会社、経営

Article 13 及び Annex I は、計画・設計・開発・製造・提供・保守の各段階でサイバーセキュリティ・リスクを考慮することを求める。セキュア・バイ・デザイン（企画・設計段階から安全性を組み込む）とセキュア・バイ・デフォルト（初期状態から安全側の設定にする）という発想である。製品は、機密性（見せない）、完全性（変えさせない）、可用性（使える状態を保つ）、真正性（本物と確認できる）等を保護する必要がある。DDoS 耐性は、多数の端末等から大量通信を受けてもサービスを維持・復旧できる力で、主に可用性の論点である。

また、PSIRT を中心に CVD（協調的脆弱性開示）の窓口・手順を整備し、外部研究者からの報告受付、影響評価、パッチ準備、公表時期、Article 14 判断を一つのフローとして管理することが重要である。

サポート期間は、製品が使用されることが合理的に期待される期間を反映し、原則として少なくとも 5 年間とする。さらに、提供したセキュリティ更新は、原則として発行後 10 年又はサポート期間の残存期間のうち長い方の期間、入手可能な状態に置く必要がある。

5 Article 14 報告義務——24 時間時計が動く場面

2026 年 9 月 11 日から、製造者には大きく二つの事象について Article 14 の報告義務が生じる。第一は、actively exploited vulnerability、すなわち「積極的に悪用されている脆弱性」である。重要なのは、「脆弱性が見つかったらすべて 24 時間以内に報告する」わけではないことである。

【図表 5】通常の脆弱性と Article 14 報告トリガー

報告対象になり得る例	直ちには Article 14 報告対象とならない例
自社製品の脆弱性が実際の攻撃に使われた信頼できる証拠がある	脆弱性を発見しただけ
顧客環境で悪用が確認された	CVE（公開脆弱性の共通 ID）が付与されたが悪用証拠はない
SOC・CSIRT 等が実運用で攻撃を確認した	PoC（再現・検証コード）が存在するだけ
信頼できる外部機関から現実の悪用情報を得た	研究者が善意で検証しただけ

第二は、製品のセキュリティに影響する重大インシデントである。会社で発生したサイバー事故すべてが CRA 対象になるわけではなく、製品が重要な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、又は損ない得るかを確認する。

・製品アップデート経路の侵害

・コード署名鍵の漏えい

・開発環境への侵入によりマルウェアが製品へ混入するおそれ

・製品又はユーザーのネットワークに悪性コードを導入・実行させた、又はその可能性がある事案

6 認識・報告先・ユーザー通知・他制度との重畳

(1) 24 時間・72 時間・最終報告

【図表 6】Article 14 の報告スケジュール

事象	24 時間以内	72 時間以内	最終報告
積極的に悪用されている脆弱性	Early Warning	Vulnerability Notification	修正・緩和措置が利用可能となった後 14 日以内
重大インシデント	Early Warning	Incident Notification	72 時間通知後 1 か月以内

最初の 24 時間は、原因調査を完了するための時間ではない。「何か重大なことが起きている」ことを速報し、その後に情報を補充する三段階の仕組みである。

(2) 最も難しいのは「いつ会社が認識したのか」

期限は、製造者が事象を「認識（becoming aware）」した時点から動く。SOC（監視・検知を担う Security Operations Centre）、CSIRT（組織のサイバー事故対応チーム）、PSIRT（自社製品の脆弱性対応チーム）等の役割分担を決め、社内ルールで PSIRT・法務への到達時を管理上の起点としても、法的な「認識」の時点を後ろ倒しできないようにする。EU 販売会社・海外子会社・販売代理店から本社への連絡期限は、「速やかに」ではなく「〇時間以内」と具体化する必要がある。

【図表 7】「認識」を社内実務に落とす

段階	確認・記録すべき事項
端緒の受領	顧客、SOC、販売店、研究者等から悪用・重大事故の兆候を受領した時刻
信頼できる情報	ログ、攻撃痕跡、製品影響等、合理的に疑える材料を得た時刻・内容
社内エスカレーション	PSIRT、法務、Article 14 責任者に到達した時刻
暫定判断	不確実性を含め、Early Warning を出すかの判断時刻・判断者・根拠

(3) SRP・ユーザー通知・重畳する時計

Article 14 の報告は、ENISA（European Union Agency for Cybersecurity：EU サイバーセキュリティ機関）が構築する SRP（Single Reporting Platform：単一報告基盤）を通じて行う。CSIRT designated as coordinator とは、NIS2 に基づき各加盟国が指定する調整役 CSIRT である。EU 域内に主たる拠点がない日本メーカーでは、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、の順で報告先となる加盟国を判断する。

当局報告だけでなく、影響を受けるユーザーへの緩和措置・是正措置の通知も必要となる。実際の事故では、SRP 報告、パッチ（脆弱性・不具合を修正する更新プログラム）の準備、ユーザー通知、Web 公表、FAQ、販売代理店説明、営業説明、広報レビューが並行して動く。

【図表 8】重畳し得る主な通知義務

制度	主なトリガー・期限の概要
CRA	製品の悪用脆弱性・重大インシデント。24 時間・72 時間・最終報告
NIS2	NIS2（EU の一定の組織・重要セクター向けサイバー規制）の対象事業者なら、重大インシデントについて 24 時間・72 時間・1 か月等
GDPR	個人データ侵害。監督機関への 72 時間報告。高リスク時は本人通知も検討
日本法	個人情報、製品安全、上場会社開示等を個別に検討
契約	顧客、販売店、クラウド、部品供給元との契約ごとに通知条件・期限が異なる

なお、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等を除き、CRA 本体の主たる製品要件の適用は限定的である。しかし Article 14 の報告義務は別であり、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。架空事案の A 社製品も、2023 年から EU で販売されていたからといって、Article 14 の検討対象から外れるわけではない。

7 2027 年全面適用――CE マーキングまでサイバーが入る

2027 年 12 月 11 日の全面適用後は、CRA への適合が EU 市場アクセスの条件となる。製品のリスク評価、Annex I 必須要件への適合、技術文書、適合性評価、EU 適合宣言、CE マーキングまで一連のプロセスとして整備しなければならない。

通常製品は内部統制手続（Module A）による自己評価が原則である。Annex III の重要製品は Class I・II で手続が異なる。Class I は、整合規格・共通仕様・一定の欧州サイバーセキュリティ認証を全面適用する等の条件を満たせば Module A の自己評価が可能で、そうでなければ第三者関与が必要となる。Class II は、整合規格等を利用していても原則として第三者関与等が必要であり、より高いリスクを想定した区分である。

「CE マーキングの直前に法務が書類を確認する」対応では間に合わない。CEN（一般分野）、CENELEC（電気・電子）、ETSI（ICT・通信）は EU が認める欧州標準化機関であり、CRA の整合規格策定でも重要な役割を担う。また、無線機器では Radio Equipment Directive（RED）と、そのサイバー要件を具体化する委任規則(EU) 2022/30 が CRA に先行して問題となる。設計記録、リスク評価、SBOM、脆弱性対応等の証跡は製品開発段階から蓄積し、整合規格が出そろう前から Annex I 等を基礎にギャップ分析を開始する必要がある。

なお、CRA は Annex I の必須要件及び Articles 13・14 等への違反について、最大 1,500 万ユーロ又は前年度全世界年間売上高の 2.5%のいずれか高い額という行政制裁金の枠組みを置く（Article 64）。零細企業（micro：従業員 10 人未満で、売上高又は貸借対照表総額が 200 万ユーロ以下）・小規模企業（small：従業員 50 人未満で、売上高又は貸借対照表総額が 1,000 万ユーロ以下）については支援・簡素化があり、24 時間 Early Warning 期限違反に関する行政制裁金には限定的な例外がある。ただし、Article 14 の報告義務そのものが免除されるわけではない。

※ 零細・小規模企業の判定は EU の SME Definition による。Article 64(10)の 24 時間速報期限に関する制裁金例外は、2025 年 7 月 2 日の Corrigendum 2025/90555 を反映して理解する必要がある。

隣接制度も位置付けを整理しておきたい。JC-STAR（IPA）は日本の IoT セキュリティ・ラベリング制度、ETSI EN 303 645 は消費者向け IoT のベースライン標準、英国 PSTI 法は英国の強制的な製品セキュリティ規制、シンガポール CLS は 4 段階のラベリング制度である。相互承認や証跡の流用はあり得るが、いずれも CRA 適合を自動的に保証するものではない。

8 SBOM・OSS・実質変更——開発・調達の実務対応

CRA は、少なくともトップレベルの依存関係を含む機械可読の 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」）作成を求める。SBOM は単なる文書作成義務ではなく、脆弱性発生時に「どの製品に影響するか」を短時間で特定するための運用基盤である。製品内部のファームウェア（機器の基本動作を制御する組込みソフト）も管理対象として意識する必要がある。

OSS（Open Source Software）は、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ウェアである。従来、法務部門の OSS 審査はライセンス条件が中心であったが、CRA では脆弱性管理状況、サポート終了、SBOM への登録、修正情報、依存関係という視点が加わる。部品・OSS 供給元との契約も、悪用情報、重大インシデント疑い、顧客環境での攻撃兆候等を、何時間以内に、誰へ、どの情報とともに通知するかまで具体化することが望ましい。

また、ソフトウェア更新が CRA 上の「実質変更（substantial modification）」に当たり、変更者が製造者として義務を負う可能性がある。リリース判定時に、通信先、認証方法、アクセス権限、処理データ、新機能による脅威モデルの変化を確認する手続を組み込む必要がある。

9 ロードマップと必要最小限チェックリスト

【図表 9】日本企業の実装ロードマップ

時期・Phase	主な対応
直ちに／Phase 1	EU 向け対象候補製品の棚卸し、製品分類、Article 14 責任者・連絡網の確定
2026 年 9 月まで	24 時間報告、72 時間通知、SRP、ユーザー通知、パッチ・広報の初動フローを運用可能にする
2026 年中／Phase 2	Annex I、技術文書、SBOM、CVD、サポート期間についてギャップ分析
2027 年前半／Phase 3	開発標準、品質保証、調達契約、脆弱性対応、実質変更判定のプロセス改訂
2027 年後半／Phase 4	整合規格・第三者評価を確認し、適合性評価、EU 適合宣言、CE 表示を完了
全面適用後／Phase 5	監視、セキュリティ更新、当局対応、経営報告を継続運用

【図表 10】必要最小限チェックリスト

確認	項目	必要最小限の確認事項
☐ 1	対象製品台帳	EU 市場向け対象候補製品を、既存品・販売終了品・サポート中製品まで棚卸ししているか
☐ 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 時間以内の社内期限を決めているか
☐ 3	SRP・CSIRT	SRP 利用者、EU Login、報告先 CSIRT、EU 代理人・輸入者・販売者との情報経路を確認しているか
☐ 4	顧客通知・パッチ	ユーザー通知、緩和措置、パッチ、FAQ、営業説明、広報レビューの最低限の手順があるか
☐ 5	全面適用ギャップ	Annex I、SBOM、CVD、サポート期間、技術文書等の未整備項目を把握しているか
☐ 6	CE までの出口	重要・クリティカル製品分類、整合規格、適合性評価、EU 適合宣言、CE 表示の責任者が決まっているか

※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。そこから 2027 年 12 月 11 日の全面適用に向けて、開発・品質保証・サプライチェーン管理・適合性評価に対応する。

おわりに　サイバーセキュリティが「製品法務」になる

CRA の本質は、24 時間報告でも高額な制裁金でもない。最大の変化は、サイバーセキュリティが企業の情報システム管理の問題から、製品を EU 市場へ出すための製品法務・品質保証の問題になることである。

コンプライアンス部門の役割も、最後に契約や CE 書類を確認するだけでは足りない。製品企画、開発、品質保証、調達、脆弱性対応、販売、サポートという製品ライフサイクル全体に、「誰が判断し、誰が記録し、誰が報告するか」という統制を設計する必要がある。

まず 2026 年 9 月 11 日。次に 2027 年 12 月 11 日。この二つの期限を分けて考え、直近の 24 時間報告体制から着手することが、日本企業にとって現実的な CRA 対応の第一歩である。

〔主な参考資料〕

1　Regulation (EU) 2024/2847 of the European Parliament and of the Council (Cyber Resilience Act)
https://eur-lex.europa.eu/eli/reg/2024/2847/oj

2　European Commission, Commission guidance on the application of the Cyber Resilience Act, C(2026) 5252（2026 年 7 月 27 日）

3　European Commission, Cyber Resilience Act – Summary
https://digital-strategy.ec.europa.eu/en/policies/cra-summary

4　European Commission, Cyber Resilience Act – Reporting obligations
https://digital-strategy.ec.europa.eu/en/policies/cra-reporting

5　ENISA, Cyber Resilience Act Single Reporting Platform (SRP) / Frequently Asked Questions
https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions

6　Commission Implementing Regulation (EU) 2025/2392（重要製品・クリティカル製品の技術的記述）

7　Commission Delegated Regulation (EU) 2025/1535、Commission Delegated Regulation (EU) 2026/881、標準化要請 M/606

8　Directive (EU) 2022/2555（NIS2 Directive）Article 23、Regulation (EU) 2016/679（GDPR）Articles 33, 34

9　European Commission, The Blue Guide on the implementation of EU product rules 2022 / SME Definition

10　ENISA, How to set up CSIRT and SOC / Vulnerability Disclosure / CRA Single Reporting Platform

11　CVE Program (cve.org) / NIST CSRC Glossary (DDoS) / CISA, Secure by Design and Default

12　Regulation (EU) 2024/2847 Corrigendum 2025/90555（Article 64(10)）

13　IPA, JC-STAR（英国 PSTI・シンガポール CLS との相互承認を含む）

14　ETSI EN 303 645, Cyber Security for Consumer Internet of Things: Baseline Requirements

15　UK Government, PSTI Product Security Regime / Cyber Security Agency of Singapore, Cybersecurity Labelling Scheme (CLS)

※　本稿は、2026 年 8 月 16 日時点で公表されている法令、欧州委員会ガイダンス、ENISA 資料等を基に、CRA の概要と日本企業の実務対応を整理したものです。今後の下位法令、整合規格、当局ガイダンス等により実務上の取扱いが更新される可能性があります。また、本稿は一般的な情報提供を目的とするものであり、個別の製品又は事案に関する法的助言ではありません。