F/K LEGAL × ORIENT

EU サイバー・レジリエンス法

日本企業の製造業者、輸出業者および企業間取引向け部品サプライヤーのための経営層向けコンプライアンス体制ガイド

経営上の結論　整合規格がすべて整うまで待つことは、法的に安全な戦略ではありません。日本企業は、文書化されたリスクベースのコンプライアンス体制を直ちに整備すべきです。まず、製品範囲の特定、EU における役割の整理、および 2026 年 9 月 11 日から適用される報告ワークフローの構築から着手する必要があります。

対象読者

取締役会、法務・コンプライアンス部門、最高情報セキュリティ責任者（CISO）、製品セキュリティ部門、エンジニアリング責任者、購買部門、ならびに日本企業グループの欧州子会社、輸入業者および販売業者。

目的

本レポートは、欧州連合（EU）のサイバー・レジリエンス法（CRA）を、経営および実装のための枠組みに落とし込むものです。すべての整合規格が利用可能になる前に実施できる、委任できない公法上の義務、実務上の管理策、契約上の保護、および証拠を明確にします。

主要日程

日付	法的効果
2026 年 6 月 11 日	通知機関（適合性評価機関）に関する規則が適用されます。
2026 年 9 月 11 日	積極的に悪用されている脆弱性および重大インシデントの義務的報告が開始されます。
2027 年 12 月 11 日	製品要件、適合性評価および CE マーキングを含め、CRA が全面的に適用されます。

法的通知

本ガイドは一般的な情報を提供するものです。製品ごとの適用範囲、分類、適用される分野別法令、契約構造および執行リスクについては、別途評価する必要があります。

01 | エグゼクティブ・オーバービュー

CRA が日本企業にもたらす変化

デジタル要素を有する製品に関する横断的なサイバーセキュリティ要件を定める、2024 年 10 月 23 日の欧州議会および理事会規則（EU）2024/2847（サイバー・レジリエンス法）は、製品サイバーセキュリティを、従来の主として任意の取組みから、EU 市場へのアクセス条件へと転換するものです。同法は、製造業者の国籍ではなく、市場投入先に基づいて適用されます。

実務上の影響　日本企業がコネクテッド製品または単体ソフトウェアを開発し、EU で利用可能にする場合、EU 子会社、輸入業者または販売業者が現地販売活動を行っている場合であっても、CRA 上は当該日本企業が製造業者に該当し続けることが一般的です。

経営上の 5 つの優先事項

1. 適用範囲と役割の整理。各デジタル要素製品（PDE）、法的な製造業者、輸入業者、販売業者、認定代理人、およびリブランディングまたは実質的変更により製造業者となり得る主体を特定します。
2. 第 14 条への備え。24 時間以内の早期警告、72 時間以内の通知、調査または是正後の最終報告という三段階の報告プロセスを運用します。
3. 製品証拠。各製品ファミリーについて、サイバーセキュリティ・リスク評価、要件マトリクス、ソフトウェア部品表（SBOM）、脆弱性対応の証拠、試験報告書、利用者向け情報および技術文書を整備します。
4. サプライチェーン管理。上流サプライヤーに対し、製造業者が自らの公法上の期限を満たせるよう、十分早期に情報および支援を提供することを求めます。
5. 取締役会による監督。意思決定、リソース、未解決のギャップ、受容された残余リスク、責任者および完了期限を記録します。意思決定ログは説明責任を支えるものですが、実質的なコンプライアンス体制に代わるものではありません。

法的基準は「最善努力」ではなくコンプライアンスである

CRA は、一般的な最善努力の抗弁を設けていません。それでも、合理的で文書化された措置は法的に重要です。それらは、ガバナンスの証拠となり、技術文書を支え、当局による事情評価に影響し、執行の比例性に関係し得ます。しかし、2027 年 12 月 11 日以降、市場に投入される製品は、適用される基本的サイバーセキュリティ要件を満たしていなければなりません。

法的根拠：CRA 第 6 条、第 13 条第 1 項～第 14 項、第 31 条および第 64 条第 4 項、附属書 I、前文第 1～10 項、第 54 項、第 79 項および第 87～91 項。

早期対応が期待される理由

欧州委員会の影響評価および立法提案は、安全性の低い製品、不統一なセキュリティ更新、利用者情報の不足を市場の失敗として特定しました。最終的な前文は、ライフサイクル上の責任とサプライチェーンへの波及を、規制の中核的な理由として位置付けています。BusinessEurope は調和を支持しつつ、より明確な定義、国際的整合性および十分な実施期間を求めました。欧州人民党グループは、統一的な要件と継続的な製品更新を支持しました。これらの資料は、不確実性はリスクベースの実装によって管理されるべきものであり、何もしない理由として用いられるべきではないことを示しています。

02｜適用範囲と法的役割

何が規制対象となり、誰が各義務を負うかを判断する

デジタル要素を有する製品（PDE）には、ソフトウェアまたはハードウェア、およびそのリモートデータ処理ソリューションが含まれ、個別に販売されるソフトウェアまたはハードウェア部品も含まれます。重要な接続は、直接的なものだけでなく間接的なものも含まれます。したがって、分析では、機器、組込みソフトウェア、アプリケーション、産業用制御部品、および製品機能に必要な該当するリモート処理を対象に含める必要があります。

法的根拠：CRA 第 2 条第 1 項、第 3 条第 1 号、第 2 号、第 3 号、第 4 号、第 6 号、第 12 号および第 13 号。

適用範囲判断の手順

確認事項	判断の証拠	完全な法的引用
直接または間接のデータ接続を有するソフトウェアまたはハードウェアが存在するか。	アーキテクチャ、インターフェース、意図された用途、製品およびサービスの説明。	CRA 第 2 条第 1 項、第 3 条第 1 号。
リモート処理が製品機能に必要か。	機能上の依存関係および開発責任。	CRA 第 3 条第 2 号。
製品が除外対象であるか、または特定の分野別法令により規律されるか。	法的適用可能性メモおよび分野別法令との同等性分析。	CRA 第 2 条第 2 項～第 8 項。
ソフトウェアが商業活動外で自由・オープンソースソフトウェア（FOSS）として提供されているか。	収益、収益化、サポートおよび開発モデル。	CRA 第 2 条第 12 項、第 3 条第 48 号、前文第 18～21 項。
製品は標準カテゴリー、重要製品クラス I、重要製品クラス II、またはクリティカル製品に該当するか。	中核機能および附属書 III／IV との対応付け。	CRA 第 7 条および第 8 条、附属書 III および IV。

経済事業者

役割	CRA 上の主な責任
製造業者	設計、開発、製造、リスク評価、脆弱性対応、適合性評価、文書化、報告、セキュリティサポートおよび是正措置。
認定代理人	書面による委任で対象とされた業務のみを行います。中核的な設計、リスクおよび製造業者の義務は移転できません。
輸入業者	適合した製品のみを EU 市場に投入し、製造業者による必要な手続、CE マーキング、文書および連絡先情報を確認し、不適合の疑いがある場合には対応します。
販売業者	相当な注意を払い、CE マーキングおよび必要情報を確認し、不適合であると考える理由がある製品を市場で利用可能にしてはなりません。
リブランダー／実質的変更者	法定要件を満たす場合、製造業者となり、製造業者の義務を負う可能性があります。

法的根拠：CRA 第 13 条、第 18 条、第 19 条、第 20 条および第 21 条。

日本企業グループに関するポイント　CRA 上の役割は、社内の事業上の呼称ではなく、法人ごと・製品ごとに割り当てる必要があります。日本の「本社」、EU 販売会社および物流会社は、製品フローごとに異なる法定上の役割を持つ可能性があります。

03 | 製品要件

附属書 I をエンジニアリング管理マトリクスへ落とし込む

デジタル要素を有する製品（PDE）は、当該製品が基本的サイバーセキュリティ要件を満たし、製造業者のプロセスが脆弱性対応要件を満たす場合に限り、市場で利用可能にすることができます。製造業者は、サイバーセキュリティ・リスク評価を実施し、文書化し、更新するとともに、それを計画、設計、開発、製造、提供および保守の全過程で用いなければなりません。

法的根拠：CRA 第 6 条(a)～(b)、第 13 条第 1 項～第 3 項、附属書 I 第 I 部および第 II 部。

基本的な製品特性

義務	必要な管理証拠	完全な法的引用
リスクに応じたサイバーセキュリティ。市場投入時点で、既知の悪用可能な脆弱性が存在しないこと。	リスク受容基準、リリースゲート、脆弱性スキャンおよび例外承認。	CRA 附属書 I 第 I 部(1)および(2)(a)。
セキュア・バイ・デフォルト設定およびリセット機能。	デフォルト設定基準、認証情報ポリシーおよび利用者によるリセット試験。	CRA 附属書 I 第 I 部(2)(b)。
適切な制御メカニズムを含む、不正アクセスからの保護。	認証、アイデンティティ、アクセス制御および権限に関するテスト証跡。	CRA 附属書 I 第 I 部(2)(c)。
保存、送信または処理されるデータの機密性および完全性。	暗号化、鍵管理、完全性保護および改ざん証跡。	CRA 附属書 I 第 I 部(2)(d)-(e)。
データ最小化；重要な機能の可用性およびレジリエンス。	データフロー分析、保持ロジック、レジリエンステストおよび復旧設計。	CRA 附属書 I 第 I 部(2)(f)-(h).
他のデバイスまたはネットワークへの悪影響の最小化；攻撃サーフェスの制限。	インターフェース一覧、ネットワーク動作テスト、ハードニングおよび公開サービスのレビュー。	CRA 附属書 I 第 I 部(2)(i)-(j).
エクスプロイトの緩和、セキュリティログ、および該当する場合の安全な削除または移転。	エクスプロイト緩和策、保護されたログ、ポータビリティ／削除機能およびテスト結果	CRA 附属書 I 第 I 部(2)(k)-(m).

管理上の解釈

これらの要件は、目的志向かつ技術中立的です。経営陣は、エンジニアリング部門が、適用される各法的成果を製品固有の受入基準へ変換していることを確保しなければなりません。基本要件が適用されないと判断される場合、技術文書には当該製品の事実関係および理由を記録すべきであり、単に当該行を空欄にしておくべきではありません。

法的根拠：CRA 第 31 条、附属書 VII 第 3 点および第 5 点、前文第 87 項。

04 | 脆弱性対応と SBOM

製品リリース後も有効に機能するライフサイクル管理策を整備する

製造業者は、製品構成部品および脆弱性を特定し文書化し、脆弱性に遅滞なく対応し、セキュリティを試験・レビューし、セキュリティ更新を安全に配布し、協調的脆弱性開示（CVD）方針を維持しなければなりません。トップレベルの SBOM は、脆弱性対応の枠組みおよび技術文書に明示的に含まれる要素です。

法的根拠：CRA 附属書 I 第 II 部(1)～(8)、第 13 条第 5 項、第 7 項、第 8 項、第 9 項および第 12 項、附属書 VII 第 2(b)点。

運用要件

管理策	最低限の実装	完全な法的引用
構成部品の特定および SBOM	バージョン管理された構成部品台帳。少なくともトップレベルの依存関係を含め、影響を受ける製品バージョンおよびリリース記録に紐付ける。	CRA 附属書 I 第 II 部(1)、第 3 条第 39 号、附属書 VII 第 2(b)点。
脆弱性監視	サプライヤー、研究者、データベース、顧客および社内試験からの継続的な受付。トリアージ責任者および時刻記録を明確にする。	CRA 附属書 I 第 II 部(2)および(3)。
是正および更新	優先順位付けされた修正、安全な更新配布、および技術的に可能な場合にはセキュリティ更新と機能更新の分離。	CRA 附属書 I 第 II 部(2)、(6)および(8)、第 13 条第 9 項。
CVD 方針	公開連絡窓口、協調的開示手順、研究者対応および社内エスカレーション。	CRA 附属書 I 第 II 部(5)および(7)、附属書 II 第 2 点。
サポート期間	想定される使用、合理的な利用者期待、製品の性質、関連するサポート期間および構成部品の利用可能性を反映した文書化された期間。想定使用期間が短い場合を除き、通常は少なくとも 5 年。	CRA 第 13 条第 8 項、前文第 57～60 項。
無償のセキュリティ更新	限定的な法定例外を除き、セキュリティ更新を無償で提供する。	CRA 第 13 条第 9 項。

SBOM および脆弱性悪用可能性情報交換（VEX）の活用方法

SBOM は依存関係を特定するものであり、VEX は既知の脆弱性が当該製品の文脈で実際に悪用可能かどうかを記録するものです。両者を組み合わせることで、トリアージ、サプライヤーとの連絡および報告を支援できます。ただし、いずれもリスク評価、監視または是正措置の代替にはなりません。欧州連合サイバーセキュリティ機関（ENISA）の 2026 年 SBOM 関連作業および「セキュア・バイ・デザイン／デフォルト・プレイブック」は、有用な実装上の証拠となり得ますが、拘束力のある法令ではありません。

日本的な品質アプローチ　完全性を過大に表示することなく、段階的なデータ品質目標を採用します。カバレッジ、既知の盲点、補完的管理策、各ギャップの責任者、および承認された是正完了日を記録します。

05 | 2026 年 9 月からの義務的報告

24 時間／72 時間／最終報告の手順を運用する

2026 年 9 月 11 日から、製造業者は、製品セキュリティに影響を及ぼす積極的に悪用されている脆弱性および重大インシデントについて、単一報告プラットフォーム（SRP）を用いて、指定されたコンピュータセキュリティインシデント対応チーム（CSIRT）および ENISA に通知しなければなりません。期限の起算点は、完全な根本原因調査が完了した時点ではなく、製造業者が認識した時点です。

法的根拠：CRA 第 14 条第 1 項～第 7 項、第 16 条第 1 項、第 71 条第 2 項。

段階	積極的に悪用されている脆弱性	重大インシデント	完全な法的引用
早期警告	不当な遅滞なく、認識から 24 時間以内。	不当な遅滞なく、認識から 24 時間以内。不法または悪意ある行為が疑われるかを記載。	CRA 第 14 条第 2(a)号および第 14 条第 4(a)号。
通知	認識から 72 時間以内。一般情報、製品、脆弱性、悪用状況および是正措置を含める。	認識から 72 時間以内。初期評価、重大性、影響、侵害指標および軽減措置を含める。	CRA 第 14 条第 2(b)号および第 14 条第 4(b)号。
最終報告	是正措置または軽減措置が利用可能となった後、不当な遅滞なく提出する。	根本原因分析、最終的な重大性、影響、軽減措置および実施された是正措置を含める。	CRA 第 14 条第 2(c)号および第 14 条第 4(c)号。
利用者への連絡	必要に応じて、影響を受ける利用者に脆弱性、是正措置および軽減措置を通知する。	必要に応じて、影響を受ける利用者にインシデント、是正措置および軽減措置を通知する。	CRA 第 14 条第 6 項および第 7 項。

推奨される内部標準作業手順

6. 完全な本社確認を待たずに 24 時間以内の早期警告を発出できる権限を有する、欧州向け CRA 報告責任者および代理者を任命する。
7. 「認識」の定義を定め、その時刻および根拠資料を記録し、報告対象外と分類した事案については意思決定ログを保存する。
8. 日英二言語の受付フォームと、事前承認済みの最小データ早期警告テンプレートを使用する。正確性は引き続き不可欠であるが、完全性は法令上、段階的に求められる。
9. PSIRT（製品セキュリティインシデント対応チーム）、SOC（セキュリティ・オペレーション・センター）、エンジニアリング、法務、品質、広報、サプライヤーおよび EU 経済事業者を統合して運用する。
10. 該当する場合には、一般データ保護規則（GDPR）である規則（EU）2016/679 およびネットワーク・情報システム 2 指令（NIS2 指令）である指令（EU）2022/2555 に基づく並行義務も含め、週末および時差をまたぐシミュレーションを実施する。

ENISA の 2026 年 8 月の SRP ガイダンスは、段階的な入力項目を確認しています。24 時間以内の提出では小規模な中核データセットが求められ、より広範な技術情報は 72 時間段階および最終段階で提供されます。通知そのものによって、通知者の責任が増加するわけではありません。

法的根拠：CRA 第 17 条第 4 項、ENISA「SRP よくある質問」質問 7 および 16、2026 年 8 月 3 日更新。

06 | サプライチェーン責任

最終製品についての説明責任は製造業者に残る

CRA は、サプライヤーが独立して行ったすべての違反について、最終製造業者に自動的に責任を負わせるものではありません。しかし、第三者の構成部品を組み込む際には製造業者に相当な注意義務を課し、最終的なデジタル要素を有する製品（PDE）およびそのライフサイクル・プロセスが適合していることを確保することを求めています。サプライヤーの構成部品自体が PDE として市場に投入される場合、そのサプライヤーは別個に CRA 上の製造業者となる可能性があります。

法的根拠：CRA 第 13 条第 5 項～第 6 項、第 3 条第 5 号、第 6 号、第 12 号および第 13 号、前文第 9 項、第 10 項、第 36～42 項および第 54 項。

主体	公法上の位置付け	契約上の要求事項
日本の完成品製造業者（OEM）／ブランド所有者	通常は製造業者に該当し、最終製品の適合性、報告、文書化、サポートおよび是正措置について責任を負う。	上流からの即時通知、SBOM および VEX データ、パッチ適用、監査、変更管理、規制対応およびリコール協力。
Tier 1～4 サプライヤー	個別に販売される構成部品については製造業者となる可能性がある。それ以外の場合でも、契約上の約束を履行し、OEM の相当な注意義務を支援しなければならない。	OEM の 24 時間期限に十分間に合うよう、関連し得る事象を報告する。証拠を保全し、影響および軽減措置の更新情報を提供する。
EU 輸入業者	市場投入前に適合性を確認し、指定された文書を保管し、不適合の疑いに対応する。	適合宣言および技術的証拠へのアクセス、販売停止およびエスカレーション権限、費用負担の取決め。
EU 販売業者／法人顧客	相当な注意を払い、必要な表示および情報を確認し、不適合の疑いに対応する。	下流からの事象連絡チャネル、現場情報、通知・パッチ・市場からの撤回およびリコールへの協力。

優先すべき契約条項

- 確定した「データ侵害」のみではなく、信頼できる兆候および悪意ある行為の疑いを含め、CRA 上の事象に整合した定義。
- 24 時間 365 日の連絡先、時間単位の通知サービスレベル、継続的な更新、証拠保全および安全な通信チャネル。
- SBOM および VEX の形式、バージョンの正確性、脆弱性監視、更新義務ならびにセキュリティに関係する構成部品変更の承認。
- 監査権および情報請求権、ならびに適合性評価、当局からの要請、報告、利用者への連絡、パッチ、市場からの撤回およびリコールへの協力。
- 費用負担、補償および責任上限。ただし、サイバー関連義務、秘密保持、知的財産、故意、不重過失および規制当局への協力については、除外事項を慎重に交渉する。

規格の遅延は通常、不可抗力には該当しない

CRA およびその適用日は既に明らかであり、整合規格以外の方法によっても適合性を示すことができます。不可抗力条項または責任制限条項は、当事者間の経済的リスクを配分することはできますが、当局を拘束したり、公法上の義務を消滅させたり、必要な報告および協力を妨げたりすることはできません。

07 | 規格と適合性評価

国際規格は証拠として用い、自動的なセーフハーバーとして扱わない

整合規格の適用は任意です。その参照が欧州連合官報に掲載された場合、当該規格を正しく適用することで、その規格が対象とする CRA 要件についてのみ、適合性の推定が生じ得ます。製造業者がこれらを適用しない場合には、法的要件を満たすために用いた代替的な技術的解決策を説明しなければなりません。

法的根拠：CRA 第 27 条第 1 項、第 4 項および第 8 項、第 31 条、附属書 VII 第 5 点、前文第 79 項および第 87 項。

枠組み	現時点での価値	法的限界
国際標準化機構／国際電気標準会議 27001（ISO/IEC 27001）	情報セキュリティマネジメントシステム（ISMS）、ガバナンス、サプライヤー、インシデントおよびリスクに関する証拠を支える。	組織認証だけでは、特定の PDE が附属書 I に適合していることを証明するものではない。
国際電気標準会議 62443-4-1 および 62443-4-2（IEC 62443）	セキュア開発ライフサイクルおよび産業用コンポーネント管理の強固な基盤となる。	関連する整合規格が欧州連合官報に引用されている範囲を除き、CRA 上の適合性推定は生じない。ギャップ対応付けは引き続き必要である。
ENISA「セキュア・バイ・デザイン／デフォルト・プレイブック」	設計時点からのセキュリティ、既定設定、ライフサイクル管理、脆弱性対応および附属書 I への実務的な対応付けに役立つチェックリストを提供する。	有用な実装支援資料であるが、法令でも整合規格でもなく、網羅的または拘束的な法的セーフハーバーではない。
欧州サイバーセキュリティ認証スキーム	関連する製品カテゴリーについて、認証が利用可能な場合には適合性評価および市場信頼性を支える証拠となり得る。	対象範囲、保証レベルおよび欧州委員会の措置に依存する。認証だけで全ての CRA 義務が自動的に満たされるわけではない。

適合性評価ルート

製品カテゴリー	利用可能なルート	完全な法的引用
標準カテゴリー	内部統制（モジュール A）またはその他の認められた手続。	CRA 第 32 条第 1 項、附属書 VIII 第 I 部。
重要製品クラス I	特定の整合規格、共通仕様または認められた認証が完全に適用される場合に限り内部統制が可能。それ以外の場合は第三者評価ルート。	CRA 第 32 条第 2 項、附属書 III クラス I。
重要製品クラス II	第三者による適合性評価が必要。	CRA 第 32 条第 3 項、附属書 III クラス II。
クリティカル製品	委任行為により欧州サイバーセキュリティ認証が求められる場合がある。それ以外の場合は、適用される第三者評価を行う。	CRA 第 8 条、第 32 条第 3 項、附属書 IV。

対応事項　規格台帳を維持し、公表状況、製品への適用可能性、対象範囲、ギャップ、証拠および意思決定日を記録します。欧州委員会が整合規格、共通仕様または関連する認証措置を公表した場合には、その都度、管理策を再マッピングします。

市場監視に対応できる製品ファイルを作成する

PDE を市場に投入する前に、製造業者は、適用される適合性評価を実施し、技術文書および EU 適合宣言（EU DoC）を作成し、CE マーキングを貼付しなければなりません。EU DoC に署名することにより、製造業者は適合性について責任を負います。

法的根拠：CRA 第 13 条第 10 項～第 13 項および第 20 項、第 28 条～第 32 条、附属書 V～VIII。

技術ファイル・チェックリスト

文書／証拠	必要な内容	完全な法的引用
製品説明	意図された目的、関連するソフトウェアバージョン、該当する場合のハードウェア図、および利用者向け情報。	CRA 附属書 VII 第 1 点。
設計およびライフサイクル・プロセス	アーキテクチャおよび構成部品間の関係、脆弱性対応、SBOM、CVD、連絡窓口、安全な更新、製造および監視管理策。	CRA 附属書 VII 第 2 点。
サイバーセキュリティ・リスク評価	識別したリスク、リスク低減措置、残余リスク、適用される基本要件との対応付け、および更新履歴。	CRA 第 13 条第 2 項、附属書 I、附属書 VII 第 3 点。
サポート期間の根拠	想定使用期間、利用者の合理的期待、製品の性質、構成部品の入手可能性および例外判断の根拠。	CRA 第 13 条第 8 項、前文第 57～60 項。
規格および代替的解決策	適用した整合規格、共通仕様、認証スキーム、国際規格、または代替的な技術的解決策と、その適用範囲・ギャップ。	CRA 第 27 条、第 31 条、附属書 VII 第 5 点。
試験および正式記録	設計検証、セキュリティ試験、脆弱性スキャン、レビュー、例外承認、リリース判定および是正措置の記録。	CRA 第 13 条第 3 項、附属書 VII 第 4 点および第 5 点。

利用者に提供する情報

製品には、製造業者の名称および連絡先、固有の製品識別情報、意図された目的、関連するサイバーセキュリティ上の状況およびリスク、サポート期間または終了日、更新情報、脆弱性報告窓口、安全な導入および運用に関する説明、安全な廃止に関する情報、ならびに該当する場合には EU DoC または簡易 EU DoC を含む明確な情報を添付しなければなりません。

法的根拠：CRA 第 13 条第 15 項、第 16 項、第 18 項～第 20 項、附属書 II 第 1 点～第 15 点、附属書 VI。

保存期間および当局によるアクセス

技術文書および EU DoC は、市場投入後少なくとも 10 年間、またはサポート期間のいずれか長い期間、利用可能な状態に維持しなければなりません。当局は、設計、開発、製造および脆弱性対応を評価するために必要なデータおよび内部文書を取得することができます。

法的根拠：CRA 第 13 条第 13 項、第 18 条第 3(a)号、第 53 条、第 31 条、附属書 VII。

09 | ガバナンスと取締役会の証拠

誤った安心感を生まずに、十分な情報に基づく監督を示す

取締役会および経営陣の記録は、実質的な監督を示す場合に有用です。すなわち、対象製品群、法的役割、重要リスク、リソース、未解決のギャップ、専門家の留保、意思決定、責任者、マイルストーンおよびフォローアップが記録されていることが重要です。単に「CRA について議論した」という一般的な記載は、証拠としての価値が限られます。重大なリスクを認識しながら許容したことを詳細に記録している場合、後続の軽減措置がなければ不利に作用する可能性があります。

推奨されるガバナンスモデル

階層	説明責任	証拠
取締役会／経営会議	リスク許容度、資金配分、市場アクセスに関する意思決定、および重要な例外事項の監督。	四半期ダッシュボード、意思決定、エスカレーションおよび完了記録。
CRA ステアリング委員会	ポートフォリオ範囲、法的解釈、規格動向の監視、部門横断の優先事項および EU との調整。	意思決定ログ、役割マトリクス、製品ヒートマップおよびアクション登録簿。
製品責任者およびエンジニアリング	附属書 I の実装、リスク評価、試験、証拠およびサポート・ライフサイクル。	要件マトリクス、リリースゲート、試験報告書および技術ファイル。
PSIRT／SOC／法務	監視、認識判断、報告、利用者への連絡および当局対応。	事象登録簿、24 時間／72 時間／最終報告記録、連絡承認および教訓。
購買／サプライヤー品質	サプライヤー区分、契約上の管理策、SBOM および脆弱性情報。	契約適用範囲、サプライヤー指標、監査所見および是正措置。

四半期ごとの取締役会向け指標

- 確認済みの CRA 適用範囲および法的役割評価に対応付けられた EU 売上の割合。
- 責任者、サイバーセキュリティ・リスク評価、最新の SBOM およびサポート期間の決定を有する製品ファミリーの割合。
- 時間単位の通知条項でカバーされている重要サプライヤーの範囲、およびサプライヤーから OEM へのエスカレーション時間の中央値。
- 検知から認識判断および早期警告までの時間、シミュレーション結果、ならびに未達となった社内期限。
- 期限超過の重大ギャップ、適合性評価能力、整合規格の変更、および 2027 年に向けたポートフォリオの準備状況。

法的関連性

ガバナンスに関する証拠は、製造業者の技術文書および協力義務を支え、比例的な執行判断の文脈を提供します。ただし、不適合製品を適法化するものではなく、当局および利用者に対して負う義務を契約により免れることもできません。

法的根拠：CRA 第 13 条、第 31 条、第 53 条、第 54 条および第 64 条第 4 項。

市場アクセスを中心的なリスクとして扱う

最も重大な CRA リスクは、罰金そのものだけではありません。市場監視当局は是正措置を求めることができ、それが十分でない場合には、市場での利用可能性を禁止または制限し、市場からの撤回またはリコールを命じ、EU 全域で措置を調整することができます。CE マーキングの適格性を欠くことは、顧客の認定プロセスや調達チェーンから製品が除外される原因にもなり得ます。

法的根拠：CRA 第 54 条～第 58 条、製品の市場監視および適合性に関する欧州議会および理事会規則（EU）2019/1020。

違反	行政罰の上限	完全な法的引用
附属書 I または第 13 条および第 14 条に基づく製造業者義務への不遵守	1,500 万ユーロ（EUR）、または事業者の場合は前事業年度の全世界年間売上高の 2.5%のいずれか高い額。	CRA 第 64 条第 2 項。
代理人、輸入業者、販売業者および適合性評価関係者の特定義務への不遵守	1,000 万ユーロ、または全世界年間売上高の 2%のいずれか高い額。	CRA 第 64 条第 3 項。
要請への回答として不正確、不完全または誤解を招く情報を提供した場合	500 万ユーロ、または全世界年間売上高の 1%のいずれか高い額。	CRA 第 64 条第 4 項。

制裁額の算定に関連する要素

当局は、違反の性質、重大性、期間および結果、過去の類似の制裁金、ならびに事業者の規模および市場シェアを考慮しなければなりません。そのため、迅速な是正、証拠の品質、協力姿勢およびエスカレーション管理は、商業上重要です。ただし、これらはいずれも、基礎となる法令上の義務からの免除を生じさせるものではありません。

法的根拠：CRA 第 64 条第 5 項。

責任関係との接点

CRA への適合は、契約上の保証責任、製造物責任、製品安全、データ保護、NIS2 指令、ならびに各国の民事法または刑事法と相互に関係する可能性があります。学術的な解説では、CRA が製品セキュリティに関する注意義務の水準に影響し得ると指摘されています。ただし、この見解は解釈上のものであり、法域ごとに異なります。そのため、取締役責任または刑事責任が自動的に発生するという規則として説明すべきではありません。

法的根拠：欠陥製品に対する責任に関する欧州議会および理事会指令（EU）2024/2853、規則（EU）2016/679、指令（EU）2022/2555、および適用される国内法。

11 | 90 日間の実装計画

不確実性から管理された実行へ移行する

期間	成果物	取締役会向け証拠
0〜30 日	CRA ガバナンス、EU 向け製品インベントリ、役割および適用範囲の整理、報告責任者、日英二言語の事象受付、報告標準作業手順（SOP）案。	権限付与、責任分担マトリクス（RACI）、製品登録簿、前提条件ログおよび初回机上演習記録。
31〜60 日	1〜2 つの製品ファミリーでの試行、附属書 I ギャップマップ、SBOM 成熟度レビュー、サプライヤー区分、モデル契約条項。	リスク評価、サンプル SBOM／VEX、ギャップ登録簿、契約修正案およびサプライヤー指標。
61〜90 日	24 時間／72 時間／最終報告のシミュレーション、適合性評価ルートおよび通知機関対応計画、2027 年 12 月までのポートフォリオ・ロードマップ。	演習報告書、是正計画、予算、ダッシュボードおよび適合性評価スケジュール。

日本本社が直ちに決定すべき事項

11. 単一報告プラットフォーム（SRP）のワークフローを運用する権限を有する EU 向け法人および担当者を指名するとともに、各法人が実際にどの法定上の役割を負うかを確認する。
12. 迅速かつ正確な最小限の開示と、その後の技術的な完全性確保とを区別する報告原則を承認する。
13. 各製品プログラムに対し、法的要件と技術要件を対応付けるマトリクスおよび証拠責任者を維持することを求める。
14. サプライヤー通知、SBOM 品質、セキュリティ更新サポートおよびライフサイクル記録に関するグループ方針を定める。
15. 重要製品クラス II およびクリティカル製品、ならびに適格な規格ルートを用いないクラス I 製品について、通知機関の対応能力を早期に確保する。

推奨されるクライアント支援

F/K Legal × Orient　実務的な支援として、製品影響評価、EU 上の役割整理、24 時間／72 時間／最終報告ワークショップ、SBOM ガバナンス・レビュー、附属書 I の法的要件と技術要件の対応付け、適合性評価ルートの計画、ならびにサプライヤー、輸入業者、販売業者および EU 顧客向け契約のレビューを組み合わせることができます。

最終メッセージ

最も防御可能な経営上の説明は、「指示を待っていた」というものではありません。むしろ、「当社は適用範囲と不確実性を特定し、利用可能な最善の規格を適用し、意思決定とギャップを文書化し、報告体制を実装し、サプライヤーを管理し、公式措置の進展に応じてコンプライアンス体制を継続的に更新した」という説明です。

準備作業と文献から得られる示唆

欧州委員会

2022 年の提案および影響評価は、広範な脆弱性、一貫性のないセキュリティ更新、情報の非対称性および規制の分断を特定しました。欧州委員会は、横断的な製品法の枠組み、ライフサイクル上の義務、およびリスクベースの適合性評価を選択しました。2026 年 7 月のガイダンスは拘束力を有しませんが、適用範囲、実質的変更、サポート期間、報告およびリスク評価を直接扱っています。

欧州議会、理事会および政治グループ

通常立法手続は、調和された単一市場アプローチを維持しつつ、より長い移行期間、段階的な報告アーキテクチャ、オープンソースに関する精緻化、およびより強固な運用上の仕組みを導入しました。欧州人民党グループは、最終合意を、開発者および製造業者に製品を更新し続けることを求める EU 全域で統一された規則として説明しました。また、その後のデジタル政策上の立場では、EU のサイバー関連制度間の整合性と分断回避を求めています。

BusinessEurope および事業者関係者

BusinessEurope は、新たな立法枠組みおよび大多数の製品に対する自己評価を歓迎する一方で、適用範囲およびリスクカテゴリーの明確化、国際規格との整合、ならびに少なくとも 36 か月の実施期間を求めました。これらの懸念はプロジェクト計画には有用ですが、最終的な法的義務を変更するものではありません。

法学・学術文献

- Fabian Teichmann「The cyber resilience act as a new paradigm for product security: a compliance roadmap」International Cybersecurity Law Review、2026 年、デジタルオブジェクト識別子（DOI）10.1365/s43439-025-00162-4：CRA を任意のセキュリティから公法上の製品コンプライアンスへの転換として捉え、ライフサイクル型のロードマップを提案しています。
- Jukka Ruohonen、Kalle Hjerppe および Eun-Young Kang「A Mapping Analysis of Requirements Between the CRA and the GDPR」2025 年：機密性、完全性、可用性、最小化、追跡可能性、消去および試験との重なりを特定しつつ、CRA 固有の製品義務および脆弱性対応義務を強調しています。
- Jukka Ruohonen、Eun-Young Kang および Qusai Ramadan「An Alignment Between the CRA's Essential Requirements and the ATT&CK's Mitigations」2025 年：攻撃者の戦術、技術および共通知識の枠組み（ATT&CK）との有用な整合性を示す一方、データ最小化、消去および脆弱性調整を含むギャップを指摘しています。
- ENISA「Secure by Design and Default Playbook」第 1 版、2026 年 7 月：実務的なチェックリストおよび CRA 附属書 I への示唆的な対応付けを提供する一方で、法的または網羅的な位置付けではないことを明示しています。

コメント文献の使い方　二次文献は、設計およびガバナンス上の選択を改善するために有用です。ただし、規則（EU）2024/2847、適用される委任行為または実施行為、整合規格、共通仕様、または製品固有の法的評価の代替として引用すべきではありません。

出典 | 2026 年 8 月 27 日確認済み

法令、機関、関係者および学術文献の参照資料

拘束力のある法令

Regulation (EU) 2024/2847 (Cyber Resilience Act), Official Journal of the European Union, 20 November 2024 — https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

Regulation (EU) 2019/1020 on market surveillance and compliance of products — https://eur-lex.europa.eu/eli/reg/2019/1020/oj/eng

Directive (EU) 2022/2555 (NIS2 Directive) — https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

Regulation (EU) 2016/679 (General Data Protection Regulation) — https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Directive (EU) 2024/2853 on liability for defective products — https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng

公式ガイダンスおよび準備作業記録

European Commission, C(2026) 5252 and Annex - CRA application guidance, 27 July 2026 — https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation

ENISA, CRA Single Reporting Platform Frequently Asked Questions, updated 3 August 2026 — https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions

ENISA, Secure by Design and Default Playbook, version 1, July 2026 — https://www.enisa.europa.eu/sites/default/files/2026-07/ENISA_Secure_By_Design_and_Default_Playbook_v1.pdf

European Commission, COM(2022) 454 final - CRA proposal and explanatory memorandum — https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0454

European Commission, Commission Staff Working Document (SWD)(2022) 282 final - Impact Assessment Report — https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022SC0282

European Parliament, Legislative Observatory, ordinary legislative procedure 2022/0272(COD) — https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2022%2F0272%28COD%29

Council of the European Union, common position press release, 19 July 2023 — https://www.consilium.europa.eu/en/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/

関係者および専門家による分析

BusinessEurope, The proposal for a Cyber Resilience Act - position paper, 15 March 2023 — https://www.businesseurope.eu/publications/the-proposal-for-a-cyber-resilience-act-a-businesseurope-position-paper/

European People's Party Group, New rules to protect mobile phones and apps against cyberattacks, 1 December 2023 — https://www.eppgroup.eu/newsroom/new-rules-to-protect-cell-phones-apps-against-cyberattacks

Taylor Wessing, Cyber Resilience Act: overview for affected companies, 3 November 2025 — https://www.taylorwessing.com/en/insights-and-events/insights/2025/11/cyber-resilience-act-overview

Fabian Teichmann, International Cybersecurity Law Review, Digital Object Identifier (DOI) 10.1365/s43439-025-00162-4 — https://link.springer.com/article/10.1365/s43439-025-00162-4

Ruohonen, Hjerppe and Kang, A Mapping Analysis of Requirements Between the CRA and the GDPR — https://arxiv.org/abs/2503.01816

Ruohonen, Kang and Ramadan, An Alignment Between the CRA's Essential Requirements and the ATT&CK's Mitigations — https://arxiv.org/abs/2505.13641

出典確認に関する注記

上記の各出典について、2026 年 8 月 27 日時点で、存在、表題、発行機関または著者、および関連性を確認しています。本レポートにおける法的義務は、最終版の規則（EU）2024/2847 に基づいて引用しています。欧州委員会および ENISA のガイダンスは、拘束力を有しないものとして示しています。関係者および学術資料は、文脈および実装上の示唆を得る目的に限って使用しています。