EUサイバーレジリエンス法に関するFAQ

EUサイバーレジリエンス法（Cyber Resilience Act、以下CRA）は、デジタル要素を備えた製品の製造業者、輸入業者、販売業者に適用されるサイバーセキュリティに関する要件を定めた欧州連合（EU）の法規制で、ハードウェアとソフトウェアの両方が対象となります。

CRAは2024年3月に欧州議会で正式承認を受け、2024年10月10日に欧州理事会で採択されました。2024年11月20日に欧州連合官報で公告され、2024年12月10日に発効しました。その要件の大部分は、2027年12月11日から全面的に適用されます。

1. EUサイバーレジリエンス法の目的は何ですか?

EUサイバーレジリエンス法は、下記を目的としています。

・EU市場において、有線・無線を問わずインターネットに接続される製品やソフトウェの安全性を高めること
・製造業者が製品のサイバーセキュリティに関して、そのライフサイクルを通じて責任を持ち続けること
・消費者が購入・使用する製品のサイバーセキュリティに関して適切な情報を得られること

>> EU サイバーレジリエンス法に関するFAQ（よくある質問）

2. CRAの規制対象は何ですか?

CRAは製造場所にかかわらず、EU域内で市販されている「デジタル要素を備えた製品（Product Digital Elements、以下PDE）」に適用されます。スタンドアロン型ソフトウェア、デバイスまたはネットワークに直接・間接接続されるソフトウェアおよびハードウェア製品（IoTデバイスなど）、PDEに組み込まれているソフトウェアおよびハードウェアのコンポーネントがPDEに含まれます。

CRAは全ての製品に適用されるわけではありません。PDEの遠隔処理や機能をサポートしていないWebサイトやクラウドアプリケーション、商業活動以外で開発されたオープンソースソフトウェア、他のEU規制の対象となる製品（医療機器、自動車、海運/航空関連機器など）は対象外です。

PDE製造業者にはCRAが規定するPDEのサイバーセキュリティ要件の主な義務が課されています。注目すべき要件の一つは、製造業者は、さまざまなPDEリスクカテゴリーに基づいて自社製品が適切なレベルのサイバーセキュリティに準拠していることを保証する必要があることです。よりリスクレベルが高いPDEには、より厳格な適合性評価が求められます。

CRAには3つ（数え方によっては4つ）のPDEカテゴリーがあります。

重要（クラスIおよびクラスII）

重要なPDEは2つのクラスに分類されます。
クラスIおよびクラスIIに分類されるPDEは、特定の基準を満たしています。

・クラスI：主な機能が、他の製品、ネットワークまたはサービスのサイバーセキュリティにとってクリティカルである（認証とアクセスの保護、侵入の防止と検知、エンドポイントセキュリティ、ネットワーク保護など）製品
・クラスII：直接的な操作により他の多数の製品またはそのユーザーの健康、セキュリティ、安全性を混乱させたり、制御したり、損害を与える可能性が大きく、重大な悪影響をおよぼすリスクを伴う機能を実行する製品
一例として、ネットワーク管理、構成管理、仮想化、個人データの処理などの集中システム機能が挙げられる。

クリティカル

CRAのクリティカルなサイバーセキュリティカテゴリーにおけるPDEは、製品タイプに該当するサイバーセキュリティ認定制度に適合しなければなりません。クリティカルには、「重要」製品クラスに2つの評価基準が追加されます。

- 主要事業体のクリティカルな依存関係：デジタル要素を持つ製品カテゴリーについては、指令（EU）2022/2555（別名NIS2）の第3条に記載されています。簡潔に言うとこれらの製品は、EU域内で障害が発生した場合にシステム全体に影響をおよぼす可能性のある、輸送、エネルギー、医療の事業者など主要事業体を保護するものです。主要事業体（EE）の詳細はNIS2コンプライアンスガイドをご覧ください。
- サプライチェーンへの影響：PDEのインシデントや脆弱性の悪用がEU市場全体のクリティカルなサプライチェーンに深刻な混乱を引き起こす可能性がある場合、クリティカルとして認定されます。簡潔に言うと、これらの製品はサプライチェーンを保護するうえでクリティカルだということです。

デフォルトカテゴリー

デフォルトカテゴリーは、重要クラスⅠ、重要クラスⅡ、クリティカルカテゴリーのいずれにも分類されない、その他の製品に適用されます。これらは自己評価でCRAに準拠する必要があります。

3. CRAはいつから適用されますか?

CRAは2024年3月に欧州議会で、2024年10月に欧州理事会で承認されました。2024年11月20日に欧州連合官報に公告され、2024年12月10日に発効しました。36か月の移行期間を経て、2027年12月11日からほとんどの要件が全面的に適用されます。

下記の2つの例外は、36か月の期限猶予があります。

- 製造業者は、セキュリティの脆弱性とサイバーインシデントに関する報告義務を21か月以内に実施しなければならない
- 適合性評価機関を18か月以内に設立しなければならない（これは監査役にのみ適用される）

4. CRAは重大インシデントと悪用可能な脆弱性の報告において、どのようなタイムラインを設けていますか?

CRAは重大インシデントを下記のように定義しています。

- 製品の可用性、真正性、完全性、機密情報の機密性を保護する能力が損なわれている
- PDEに悪意のあるコードが導入され、実行される可能性がある

CRAの定義する悪用可能な脆弱性とは、悪意のある行為者が（信頼できるエビデンスに基づいて）システム所有者の許可を得ずに悪用したシステムの脆弱性です。

CRAによれば、PDEの製造業者、輸入業者、販売業者は重大インシデントや悪用可能な脆弱性について、適切な規制当局に報告する義務があります。この場合の当局とは欧州連合サイバーセキュリティ機関（ENISA）とコンピュータセキュリティインシデント対応チーム（CSIRT）です。

- ENISAは米国政府のサイバーセキュリティ・社会基盤安全保障庁（CISA）に相当する機関です。ENISAはEUとその加盟国が情報安全保障の問題に備え、検知し、対応するのを支援します。また、EUのサイバーセキュリティ政策にも貢献しています。
- CRAの定義によれば、CSIRTはEU加盟国によってサイバーセキュリティインシデントの管理と対応する組織として指定されます。また、サイバーセキュリティの専門知識も提供します。

重大インシデントや悪用可能な深刻な脆弱性が発生した場合、PDE製造業者は下記の対応を行う必要があります。

- 事態を把握してから24時間以内に、CSIRTとENISAに早期警告通知を提供し、インシデントが悪意のある/違法な行為によって生じた疑いの有無を説明し、当該PDEが利用可能なEU加盟国を報告する。
- 事態を把握してから72時間以内に、インシデント/脆弱性の性質、初期評価、緩和策などの関連情報（まだ提供されていない場合）を含めた二度目の報告を関係機関に行う。

- 重大インシデントに際し、PDE製造業者はすべての関連情報が既に提供されている場合を除き、前回の通知から1か月以内にEUの関係機関に報告書を提出しなければならない。報告書には下記情報を記載しなければならない。
  - インシデントの説明（重大さや影響分析を含む）
  - 脅威の根本原因
  - 緩和策
- 悪用可能な深刻な脆弱性については、修正措置または緩和措置（パッチ）が利用可能になってから14日以内に作成する最終報告に、下記を記載しなければならない。
  - 脆弱性の説明（深刻度、影響分析を含む）
  - 可能であれば、脆弱性を悪用する悪意のある当事者についての情報
  - セキュリティの更新など、脆弱性の緩和策

5. CRAが対応している標準規格にはどのようなものがありますか?

ENISAは、CRA要件が複数の国際標準規格（ISO 27000シリーズ、IEC 62443など）にどう対応しているかを示したCRA要件の標準規格対応表を公開しました。この対応表には、他の基準（米国国立標準技術研究所（NIST）のサイバーセキュリティや情報セキュリティに関する特別刊行物など）と比較したギャップ分析とベストプラクティスの推奨事項が記載されています。

さらに、2023年12月には米国とEUのサイバー対話が、米国サイバートラストマークプログラムとEUのCRAの認定に関して相互承認を促進することを目的に行われました。これが承認されれば、米国の特定製品のセキュリティ基準はCRA要件を満たす可能性があります。

6. CRA規制対象品が規制に準拠していない場合、どのような罰則がありますか?

脆弱性の報告、サイバーインシデントの報告、または重大なサイバーセキュリティ要件に準拠していない場合、最高で1,500万ユーロまたは全世界での売上高の2.5%の過料が科される可能性があります。その他の義務に対しては、1,000万ユーロまたは全世界での売上高の2%の過料が科される可能性があります。

7. CRAとNIS2（EU全体のサイバーセキュリティ指令）との相互関係は?

ネットワーク情報セキュリティ（NIS2）は、EU全体のサイバーセキュリティ規制であった以前のNIS指令に代わるものです。CRAが製品のサイバーセキュリティを対象とする一方、NIS2は特定の業界の組織に対してネットワークおよび情報システムがサイバー攻撃に対応するための適切なセキュリティ対策を義務付けています。

8. ウインドリバーはどのようにCRAに対応していますか?

ウインドリバーを含む業界関係者は、CRAに準拠するための計画を進めています。

ウインドリバーはCRAの進捗状況を注意深く追跡しています。ウインドリバーは、規制準拠を確実にするとともに製品のセキュリティに対する取り組みをさらに推進するために、ウインドリバーのエッジやプラットフォーム製品にCRAをどのように適用できるかを検討しています。

ウインドリバー製品は、セキュア開発ライフサイクルに関してNISTのセキュアソフトウェア開発フレームワーク（Secure Software Development Framework、以下 SSDF）にすでに準拠しています。CRAのセキュリティ要件とNISTのSSDFには整合性があります。

ウインドリバーのプロフェッショナルサービスチームはお客様と連携し、セキュリティの評価やギャップなどを含め、コンプライアンスや認定に向けた活動をサポートしています。ウインドリバーは、OEMに対しベンダーおよびソフトウェアサプライヤーとして、NIST、ISO/IEC、DOD、FDAなどの数多くの業界標準の認証取得への対応を行ってきました。

ウインドリバーは、コンプライアンスおよび認証活動の一環として、サードパーティの評価者や認証機関に対するエビデンスとして使用される重要な文書や成果物をお客様に提供しています。こうした文書や成果物の例としては、下記のようなものが含まれます（これらに限定されるものではありません）。

- セキュア開発ライフサイクル基準マッピング www.windriver.com/resource/sdl-standards-map
- ウインドリバーの情報セキュリティ管理への取り組みと能力を裏付ける、ISO 27001情報セキュリティマネジメント www.windriver.com/resource/iso27001
- 製品セキュリティインシデント対応チーム（PSIRT）がISO/IEC 30111（ITセキュリティ技術、脆弱性ハンドリング、プロセス）とISO/IEC 29147国際規格に準拠した脆弱性開示のガイドラインを提供 www.windriver.com/japan/security#psirt

9. ウインドリバー製品はCRAの主要原則の「セキュアバイデザイン」に準拠していますか?

ウインドリバーのエッジ製品のVxWorks、Wind River Linux、Wind River Helix Virtualization Platformは、セキュアなソフトウェア開発に関する一連の要件を定めたNIST 800-218 SSDFに準拠しています。

>> 詳細はSSDFに準拠したウインドリバーのセキュア開発ライフサイクルをご覧ください。

10. ウインドリバーはCRAに関して、どのようにお客様をサポートできますか?

ウインドリバーは、40年以上にわたりエッジ製品による顧客価値につながるソリューションを提供してきました。これらのソリューションにはウインドリバーのプロフェッショナルサービスによるサポートが含まれており、セキュリティ評価、セキュリティギャップ分析、セキュリティ認証などさまざまな業界標準、フレームワーク、ガイドライン関する専門知識を提供しています。

IEC 62443は産業用オートメーションおよび制御システム（IACS）の安全な開発のためのセキュリティ標準規格であり、CRAで主要な役割を果たしています。VxWorks Cert Editionは、IEC 62443-4-2に準拠しているGE Digital Achilles Level IIの認証を受けています。IEC 62443-4-2は物理セキュリティ、ネットワーク通信セキュリティ、セキュアシステム統合などのセキュリティ要件を規定しています。VxWorks Cert Editionでは、ウインドリバーのお客様がIEC 62443-4-2規格が定める要件を満たす厳しいサイバーセキュリティテストに合格し、IACSのサイバーセキュリティの脅威から保護されていることをご確認いただけます。

11. CRAのコンプライアンス準拠の課題解決で、ウインドリバーはどのようにお客様をサポートできますか?

ウインドリバーはNISTのセキュアソフトウェア開発フレームワークに基づいて製品を開発しています。

>>詳細はウインドリバーのセキュア開発ライフサイクルをご覧ください。

NISTのSP 800-218セキュアソフトウェア開発フレームワーク（SSDF）は、セキュアなソフトウェア製品開発の基本原則を提供しています。これらのベストプラクティスは、IEC 62443などのさまざまなコンプライアンス規格に準拠し、マッピングすることができます。ウインドリバーはお客様にマッピングを提供し、セキュリティ要件のギャップをカバーするための次のステップに取り組む支援を行います。

ウインドリバーのプロフェッショナルサービスでは、セキュリティ評価の幅広い経験を活かし、お客様独特のセキュリティ要件やウインドリバー製品が明示的にカバーしていないギャップに対応する支援を行っています。

12. CRAを順守するために、ウインドリバーが提供している追加の製品・サービスはありますか?

VxWorks、Helix Virtualization Platform、Wind River Linux OSはNIST SSDFを順守しています。このフレームワークは、CRAの目的達成において主要な役割を果たしているIACS のIEC 62443などのセキュリティガイドラインに準拠しています。

CRAの要素の1つは、ソフトウェアの適切な脆弱性管理と合わせ、デジタル要素を含むソフトウェア部品表（SBOM）を生成・管理することです。ウインドリバーは、有料および無料のSBOM生成ツールと、オンラインのCVEスキャンツールを提供しています。

>>無料のオープンソースのWind River Linuxビルド用SBOM Yoctoレイヤーと、CVEスキャンツールをご覧ください。

WNDRVR

ウインドリバー株式会社
〒150-0012 東京都渋谷区広尾1-1-39 恵比寿プライムスクエアタワー
www.windriver.com/japan

ウインドリバーは、ミッションクリティカルなインテリジェントシステム向けのソフトウェアを提供する世界的なリーダーです。40年以上にわたり、イノベーターかつパイオニアとして、最高レベルのセキュリティ、安全性、信頼性を数十億台を超えるデバイスやシステムに提供しています。ウインドリバーのソフトウェアと専門性の高い包括的なポートフォリオは、あらゆる業界のデジタルトランスフォーメーションを加速させています。

Rev. 02/2025