BLACK DUCK®

チェックリスト

EU CRA の脆弱性報告チェックリスト：2026 年 9 月からの義務

欧州連合（EU）のサイバーレジリエンス法（CRA）は、EU 域内で販売されるソフトウェアおよびハードウェア製品に対し、必須のサイバーセキュリティ要件を導入しています。これらの要件は、設計段階からのセキュリティの確保、脆弱性対応、および製品ライフサイクル全体にわたる継続的な保守義務を含みます。

2026 年 9 月 11 日、EU CRA は試行段階に入り、欧州市場に上市されるデジタル要素を備えた製品（PDE）の製造業者、輸入業者、販売業者に対し、当該 PDE に関連する悪用された脆弱性および重大なセキュリティ・インシデントについて、ENISA および指定された各国の CSIRT に通知することを義務付けました。

EU CRA の脆弱性報告義務への対応はお済みでしょうか。以下にチェックリストをまとめましたので、対応の準備にお役立てください。

対象製品

EU CRA では製品分類システムが定義されており、すべてのソフトウェアは製品の主たる機能に基づいてデフォルトのカテゴリか、またはより厳格なカテゴリのいずれかに分類されます。医療機器や EU 2019/2144（一般安全ならびに車両乗員および交通弱者の保護に関する型式認可要件）など、EU CRA とは別のサイバーセキュリティ義務が課されている製品は適用対象から除外されます。EU CRA の要件を満たさない場合、ペナルティとして（すべての不適合製品の）全世界売上高に対する一定割合の罰金、または EU 市場からの不適合製品の排除、あるいはその両方が課されます。

EU CRA の適用対象となるのは、以下の条件を満たした製品です。

- ☐ ソフトウェア、ファームウェアを含む製品、あるいはコネクテッド製品（ネットワーク接続機能を有する製品）が機能するために必要なスタンドアロン・ソフトウェア
- ☐ EU 内で商用として流通している製品（商業活動を伴わない無償のオープンソース・ソフトウェアは原則として除外）
- ☐ 他の業界規制の対象となっていない製品
- ☐ 既に欧州市場に出回っている製品も適用対象。EU CRA の要件は新しく販売される製品だけに限定されない。

報告義務と期限

報告のタイムラインは下記が含まれます。

- ☐ **24 時間：**製造業者は、PDE（デジタル要素を備えた製品）の SaaS またはクラウド・コンポーネントに影響を与える、実際に悪用されている脆弱性またはインシデントについて、ENISA が提供する単一の報告プラットフォーム（SRP）を通じて、製造業者が事象を認識してから 24 時間以内に早期警告を提出すること
- ☐ **72 時間：**製造業者は、PDE 内で悪用された脆弱性を認識してから 72 時間以内に、脆弱性の説明、その影響、講じられている対策、および顧客が講じることができる対策や、統合されたサードパーティ製コンポーネント内の脆弱性、および PDE の運用を支える SaaS またはクラウド・コンポーネントに影響を与えるアクティブな悪用によるインシデントを含む、より詳細な通知を行うこと
- ☐ **14 日：**製造業者は、対策が利用可能になってから 14 日以内に、インシデントの重大度、脆弱性の影響、得られた教訓、およびプロセス改善を網羅した最終報告書を提出しなければなりません。また、インシデント通知の提出から 1 か月以内に、PDE の SaaS またはクラウド・コンポーネントに影響を与えるインシデントについては、完全な根本原因分析を提出すること

報告が正しく行えることを 2026 年 9 月までに検証しておくこと。

SBOM の要件

ソフトウェア部品表（SBOM）は、

- ☐ 欧州市場に投入されたすべての PDE（製品のアップデートを含む）の直接的な依存関係を網羅すること
- ☐ 市場監視当局による将来の監査に備えて保管しておくこと

市場監視当局以外の第三者と SBOM を共有する義務はありません。

継続的な脆弱性監視

PDE の製造業者、流通業者、および輸入業者は、欧州脆弱性データベース（EUVD）または欧州委員会が定義するその他のデータソースを通じて伝達される、ソフトウェア・サプライチェーン・リスクの潜在的な変化を特定できる継続的な脆弱性監視プロセスを導入しなければなりません。

- ☐ 監視ツールは、悪用される可能性のある脆弱性を優先的に検出すべきだが、オープンソース・ライブラリと統合されたサードパーティ製コンポーネントも含める必要がある
- ☐ 製造業者は、PDE のサポート期間中、欧州市場に出荷されたすべての製品を監視しなければならない。また、サードパーティ製コンポーネントを組み込んだ製品については、当該コンポーネントに存在する悪用可能な脆弱性について、規制当局および顧客に通知しなければならない

報告基盤

製造業者は、実際に悪用された脆弱性について SRP を通じて報告し、ENISA が定める関連情報を提供しなければなりません。また、社内ポリシーおよび手順書には、製品サポート期間を含む製品ライフサイクル全体にわたる脆弱性およびインシデントの報告について規定し、詳細を記述する必要があります。

サイバーセキュリティに関するすべての意思決定は、ツールの選定、脆弱性のトリアージと対処、影響を受ける製品の範囲、および外部とのコミュニケーションを含め、文書化しなければなりません。

2026 年 9 月 11 日までに対応が必要な事項

- 脆弱性監視およびプロセス
- SBOM のサポートによる可視性
- 報告のワークフローおよび期限
- 開示および更新プロセス

2027 年に必須となる事項

- サイバーセキュリティ要件への準拠
- セキュア・バイ・デザインおよびセキュア・バイ・デフォルトの証跡を含むプロセス・ワークフロー
- アタック・サーフェスの最小化
- 適合性評価
- データ保護
- デバイスの機能を保護するための回復力対策

ブラック・ダックによる支援

ブラック・ダックは、EU CRA および関連するサイバーセキュリティ規格の厳格な要件を満たすように設計されたアプリケーション・セキュリティ・ツールを提供しています。

- Black Duck® SCA はサードパーティ・リスクを特定し、NVD、EUVD、および独自の Black Duck Security Advisories（BDSA）を継続的に監視して、新たな脆弱性やエクスプロイトの情報を把握します。このデータにより、統合されたコンポーネントのリスクを自動的に優先順位付けできるため、企業は 24 時間の報告義務の要件を満たすことができます。
- Coverity® 静的解析は、デジタル要素を備えた製品を出荷する前に適切に対処しないと、仕向け先の顧客にとってサードパーティ・リスクに発展する可能性のある、自社ソフトウェアのリスクを特定します。
- Defensics® ファジング・テストは、製品が「セキュア・バイ・デフォルト」であるかどうかテストが可能で、サイバー・フィジカル・デバイス、アセンブリ、サブアセンブリ、およびスペアパーツに関連するファーストパーティおよびサードパーティのリスクを特定します。

ブラック・ダックは、チームがオープンソースやサードパーティ製のコンポーネントを特定して脆弱性を追跡し、ソフトウェア・リスクを管理するための再現可能なプロセスを確立するのを支援することで、EU CRA の脆弱性管理および報告義務の要件を満たすために必要な基礎的な対策をサポートします。

ブラック・ダックは、御社の EU CRA への対応準備を支援します。
まずはお問い合わせください。

ブラック・ダックについて

ブラック・ダックは、True Scale Application Security によって、モダン・ソフトウェアの経営レベルのリスクに対応し、規制された、AI を活用した世界におけるソフトウェアの信頼性を保証します。ブラック・ダックのソリューションは、セキュリティ、規制、ライセンスに関するリスクを排除しつつ、組織のスピード、精度、コンプライアンスのトレードオフから解放します。クラウドでもオンプレミスでも、コードが実行されるあらゆる場所でミッション・クリティカルなソフトウェアを保護するには、ブラック・ダックこそが選択肢となるのです。ブラック・ダックを活用することで、セキュリティ・リーダーはよりスマートな意思決定を行い、自信を持ってビジネス・イノベーションを推進することができます。詳しくは、www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社
www.blackduck.com/jp

©2026 Black Duck Software, Inc. All rights reserved. Black Duck® は Black Duck Software, Inc. の米国およびその他の国における登録商標です。その他の会社名および商品名は各社の商標または登録商標です。2026 年 10 月