欧州で適用が進められている サイバーレジリエンス法 (Cyber Resilience Act：CRA) に対応するための コンサルティングサービス

欧州委員会は、2022年9月、安全でセキュアなハードウェアとソフトウェアを開発する為の法案（Cyber Resilience Act）が提出され、いよいよ本年の後半から発効されることになっております。対象となる製品は、物理的な電子情報システムおよびその部品が対象となり、違反すると大きなペナルティが科される可能性があります。

そこで当社がご紹介するWithSecureでは、CRAに対応する為のコンサルティングサービスを提供いたします。

Cyber Resilience Act（CRA）の概要

欧州委員会で提案された、より安全でセキュアなハードウェアとソフトウェアを開発するための要件

- ハードウェアは、デジタルデータの処理、保存、送信を行うことができる物理的な電子情報システム、またはその部品が対象
- OS、アクセス管理、ブラウザなどのソフトウェア製品も対象

CRAでは、主に3つの要求項目があります。

1. 適切なセキュリティレベルの設定（「重要なデジタル製品」以外/Class I/Class II）
2. 製品出荷前の脆弱性への対応
3. 製品出荷後の継続的な脆弱性の確認と対応

組織がこの法律に従わない場合、当局は製品の発売を禁止・制限したり、全世界の売上高の2.5%を上限とする罰則を科すことができます。

医療機器、車載機器など一部を除いた デジタル製品 が適用対象！
法律に従わない場合、罰則を科される可能性がある！

CRA対応の必要性

EU市場に投入されるデジタル製品には、CRAに適合したセキュリティ対応が義務付けられることになります。

このCRAは、2022年9月 草案が提出され、2023年後半に発効、2025年後半には適用されることになりますので、あまり猶予はありません。

その為、各メーカーは、2025年後半の適用に向けて以下の対応が必要となっております。

【CRA対応について必要項目】

> セキュリティ要件への適合
→ WithSecureでは、お客様が開発製品の適合性証明を取得する際の、エビデンスとなるセキュリティ診断レポートを提供します。

> 更新プログラムの提供

> 脆弱性、インシデント発見後の報告体制構築
→ どのような体制を構築するべ か、のコンサルティングサービスを提供します。

WithSecure コンサルティングサービス

WithSecureでは、以下のコンサルティングサービスを提供いたします。

<WithSecure提供サービス>
■セキュリティガイドライン作成支援
脆弱性開示、報告およびインシデント発生時の対応などに関する社内規程の作成支援
（成果物：ガイドライン）
■ペネトレーションテスト
お客様の開発製品に対して、攻撃テストを実施し、脆弱性の有無や推奨対策案を提示
（成果物：診断レポート）

以下は、製品の開発段階に関するCRA要件（製造要件）と WithSecure提供サービスの対応を示しております。
なお適合性証明では、インシデント発見後の報告体制やSBOM作成など下記以外のCRA要件があることをご留意願います。

CRA要件	WithSecure提供サービス	
	セキュリティガイドライン作成支援	ペネトレーションテスト
製品の脆弱性とコンポーネントを文書化する	—	✓
脆弱性への対処と修復を遅滞なく行う	—	✓
自社製品のセキュリティについて、定期的なテストとレビューの実施	✓	✓
脆弱性修正に関する情報公開	—	✓
脆弱性開示ポリシーの作成と実施	✓	—
脆弱性に関する情報共有の促進、および当該報告のための連絡先の提供	✓	—

悪用可能な脆弱性を最小限に抑えるアップデートを安全に配布する仕組みを提供する	✓	—
セキュリティパッチを遅滞なく無償で配布、セキュリティパッチに関するユーザー向けの開示義務	✓	—

製品ページ　　お問合せ