



WithSecure社 セキュリティソリューションのご紹介 ～欧州CRA概要と関連サービス概要～

加賀FEI株式会社

Cyber Resilience Act 概要

・Cyber Resilience Act (以下 CRA) :

-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：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
- サイバーレジリエンス法では、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。

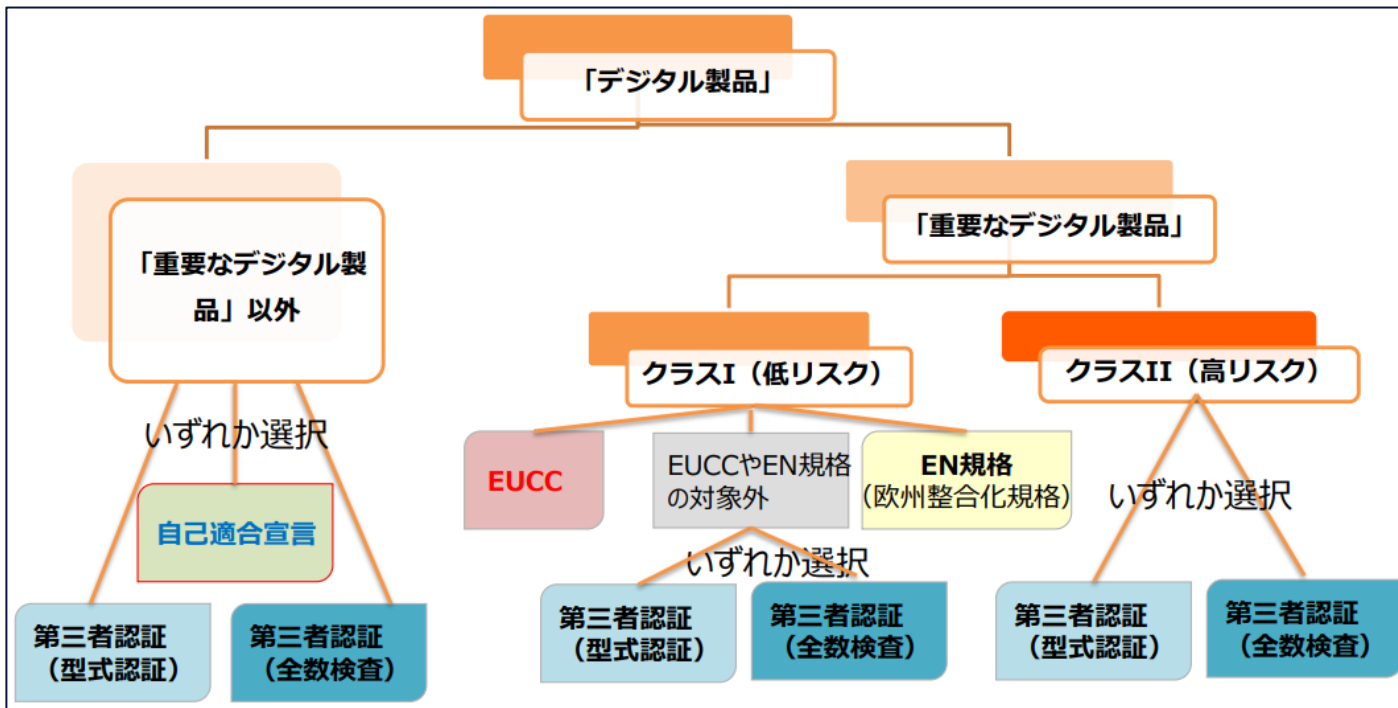
CRA対応の必要性

- EU市場に投入されるデジタル製品のセキュリティ対応を義務付け
(2022年9月 草案提出、2023年後半 発効、2025年後半 適用)
- 2025年後半の適用に向けて以下の対応が必要
 - ・**セキュリティ要件への適合**
 - ・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**

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致します。

どのような体制を構築するべきかのコンサルティングサービスを提供致します。

CRA 対象製品 適合性評価方法



出典：「EUサイバーレジリエンス法（草案概要）」 経済産業省 <https://www.meti.go.jp/policy/netsecurity/netsecurity/CRAdraft.pdf>

WithSecreでは 上記の対象となる全ての製品に対して
第三者認証を取得される際、支援となるサービス をご提供致します

重要なデジタル製品 (Class I/Class II)

Class I

1. ID管理システム、アクセス管理ソフト
2. スタンドアロン型/組込み型ブラウザ
3. パスワードマネジャー
4. マルウェア検知・削除・隔離ソフトウェア
5. VPN機能を持つ製品
6. ネットワーク管理システム
7. ネットワーク・コンフィグレーション管理ツール
8. ネットワーク・モニタリングシステム
9. ネットワーク・リソース管理
10. SEIM (セキュリティ情報イベント管理)
11. ブートマネジャーを含む更新・パッチ管理
12. アプリケーション構成管理システム
13. リモートアクセス/共有ソフトウェア
14. モバイル機器管理ソフトウェア
15. 物理ネットワークインターフェイス
16. OS (クラスII製品以外)
17. ファイアウォール、侵入検知・防止システム (産業用以外)
18. ルータ、モデム、スイッチ (産業用以外)
19. マイクロプロセッサ (クラスII製品以外)
20. マイクロコントローラ
21. NIS 2 指令の別添Iに示される目的でのASIC、FPGA
22. PLC、DCS、CNC、SCADAなどの産業用自動化制御システム (IACS) (クラスII製品以外)
23. 産業用IoT (クラスII製品以外)

Class II

1. OS : サーバ、デスクトップ、モバイル機器用のもの
2. OSや同様の環境の仮想化を実施するためのハイパバイザー及びコンテナ・ランタイム・システム
3. 公開鍵インフラ及びデジタル証明書発行
4. 産業用のファイアウォール、侵入検知・防止システム
5. 汎用マイクロプロセッサ
6. PLCやセキュアエレメントへの統合を目的としたマイクロプロセッサ
7. 産業用のルータ、モデム、スイッチ
8. セキュアエレメント
9. ハードウェア・セキュリティ・モジュール (HSMs)
10. セキュア暗号プロセッサ
11. スマートカード、スマートカードリーダー、トークン
12. 産業用のPLC、DCS、CNC、SCADAなどの産業用自動化制御システム (IACS)
13. 重要エンティティが使用する産業用IoT機器
14. ロボットセンシング/アクチュエーターコンポーネント及びロボットコントローラ
15. スマートメーター

※「高リスク」と定義されているClass II 製品のうち、日本国内製造業ユーザ様が大きく影響を受ける範囲

コンサルティングサービス (WithSecure)



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	✓	-

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



<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）



KAGA FEI