参考資料

Technical White Paper

未来を守る:TI の Jacinto ぷロッサおよび Sitara プロセッサはサイバーレジリエンス法 (EU-CRA) に準拠しています

TEXAS INSTRUMENTS

概要

このドキュメントは、欧州連合 (EU) のサイバーレジリエンス法 (CRA) の概要を簡単に説明しています。このドキュメントではまず、EU-CRA の主要な特徴と要件について説明し、続いて TI の jacinto™ と Sitara™ プロセッサが、今後施行される EU-CRA の要件をどのように満たすのかについて説明します。

目次

1 概要

デジタル製品やサービスは、今では日常生活に不可欠なものとなっています。接続されるデバイスの数は指数関数的に増加すると予想されており、この成長に伴い、サイバー攻撃の対象となる範囲と可能性が拡大すると予想されています。2024 年、欧州議会は、欧州連合 (EU) 全体のサイバーレジリエンスを強化するために、サイバーレジリエンス法 (CRA) を採択しました。CRA は、デジタル対応製品の脆弱性を減らし、これらの製品のライフサイクル全体にわたって包括的なセキュリティを組み込むことを目的としています。CRA は、デジタル素子を含む製品に対し、ハードウェアとソフトウェアの両方を含む製品ライフサイクル全体を通して、設計段階からのセキュリティ確保という必須の原則を組み込むことを義務付けています。

このドキュメントでは、テキサス インスツルメンツのプロセッサおよびこれらのプロセッサに付随する機能が、相手先ブランド製造業者 (OEM) が CRA (消費者再投資法) に準拠する上でどのように役立つかを説明します。このドキュメントではまず、重要な Class 1 製品 (主にマイクロプロセッサ) に対する CRA の主要要件の概要を説明し、次にそれらの要件を TI のプロセッサ製品群の機能に照らし合わせて説明します。

2 CRA の範囲

EU の CRA 規則は、EU 市場で販売されるデジタル要素を含む製品および部品に適用されます。これには、他のデバイスまたはネットワークに接続されることを意図している、または想定しているデジタルデータを処理するハードウェアまたはソフトウェア製品などが含まれます。

表 2-1. 対象範囲に含まれる/除外されるプロダクトとコンポーネントの例

デジタル素子を含む製品および部品の例	以下の既存の EU 規制が適用されるデジタル素子を含む製品
• ネットワーク管理システム • スマート家電 • 携帯電話 / スマートフォン • マイクロプロセッサとマイコン • オペレーティング システム • オープン ソース ソフトウェア • ブート マネージャ	• 自動車及び自動車システム — 規則 (EU) 2019/2144 • 医療機器 — 規則 (EU) 2017/745 • 体外診断用装置 — 規則 (EU) 2017/746 • 情報技術サービス、クラウドサービス、サービスとしてのソフトウェア (SaaS) 等 — 指令 (EU) 2022/2555 • 海洋機器 — 指令 2014/90/EU • 民間航空 — 規制 (EU) 2018/1139 • 国家安全保障と防衛

3 製品の要件

CRA は、製品が適切なレベルのセキュリティを提供し、既知の脆弱性がないことを要求しています。製品のサイバーセキュリティ リスクプロファイルに基づいて、該当する保護対策にはデフォルトでセキュリティ機能が含まれている必要があります。つまり、適切なセキュリティ更新を有効にし、不正アクセスから保護します。CRA には、データの機密性と整合性に関する追加要件が含まれます。これには、次の要件が含まれます。

- コマンドとプログラム
- 保存データの最小化
- 重要な機能の可用性
- 他のデバイスへの悪影響の低減
- 攻撃対象の制限
- インシデントの影響の軽減
- セキュリティ関連イベントの記録と監視
- データと設定の永続的な消去または転送の保護

4 脆弱性処理プロセス

CRA は、製造業者に対し、すべての依存関係と脆弱性を特定して文書化し、ソフトウェア部品表 (SBOM) 供し、これらの項目を継続的に追跡するとともに、既知の脆弱性が残っていないことを確認し、新たに明らかになった依存関係と脆弱性には遅滞なく対処することを義務付けています。製造業者は、デジタル製品のセキュリティをテストし、修正された脆弱性に関する情報を公開し、連携した脆弱性開示ポリシーを維持し、潜在的な脆弱性データの共有を促進し、勧告メッセージとともにパッチを迅速かつ無償で提供しなければなりません。

5 情報とラベル付け

CRA (消費者規制法) への準拠には、製品への CE (欧州適合性) マークの表示、EU 適合宣言書の提出、認定代理人の任命、セキュリティ担当者の指定、および製品の明確な識別が求められます。CRA は、次の内容を含む技術文書も求めています。

- サイバーセキュリティのリスク評価
- セキュリティ更新プログラムの可用性に関する情報
- トップレベルの依存関係をカバーする SBOM
- サポートの定義とサポートの期間
- パブリック ソフトウェア アーカイブを通じたリビジョンへのアクセス
- ユーザー命令セット

6 CRA の要件を満たす TI のプロセッサ

jacinto™ (TDA4x および DRA8x) および Sitara™ (AM6x) プロセッサ ファミリは、デフォルトの要件でセキュリティを満たすように開発されています。これらのファミリのすべてのマイクロプロセッサは、専用の公開鍵がシリコンにハードワイヤ接続されています。ブートチェックにパスできるのは、対応する秘密キーで署名されたファームウェアだけです。このキーは、プラットフォーム上で実行されるすべてのソフトウェアの真正性と完全性を検証するハードウェア上の信頼の基点を確立し、認証されたソフトウェアのみがプロセッサ上で実行されるようにします。

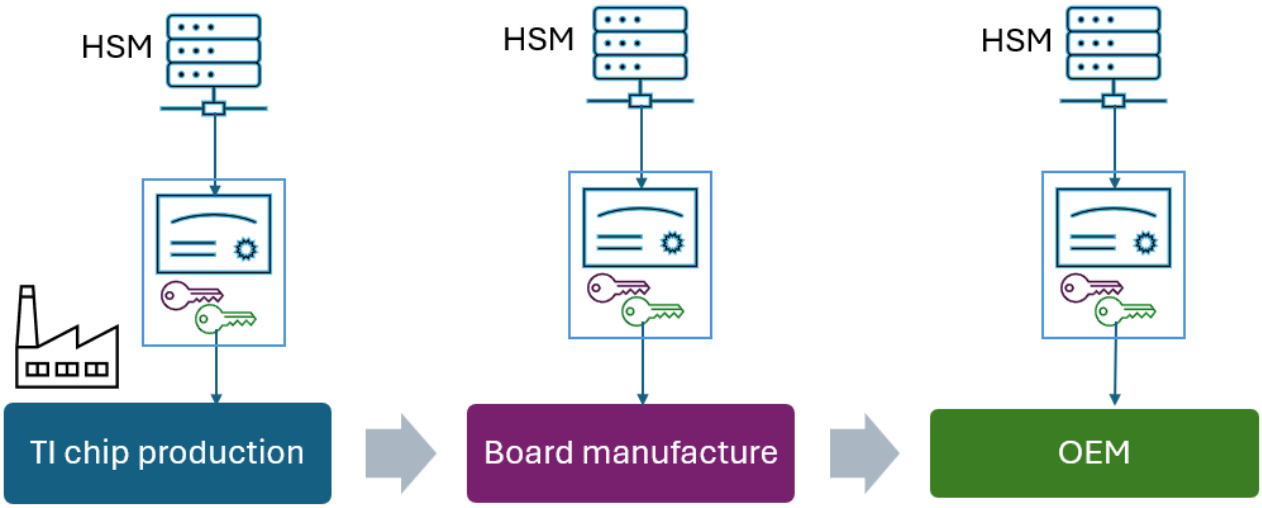

図 6-1. 信頼の基点 (RoT) キーのプロビジョニング

TI のプロセッサにはハードウェアアクセス制御機能が組み込まれており、オンチップメモリを分離したゾーンにセグメント化し、重要なメモリセクションを不正な読み取りまたは書き込み操作から保護します。このプラットフォームでは、各アプリケーション (多くの場合、同一デバイス内の別々の CPU コアで動作) に個別の保護されたコードおよびデータ領域を割り当てることで、同時ワークロードを分離できます。これにより、偶発的な漏洩や悪意のある干渉を防止できます。以上のようなメモリ保護に加えて、プロセッサにはデバッグポートを制御するアクセス用機能が用意されています。量産ユニットでは、デバッグインターフェイスを永続的に無効にすることも、署名された証明書を通して要求が認証された後にのみデバッグインターフェイスを公開することもできます。これにより、デバッグツールを悪用する一般的な攻撃ベクトルを閉じることができます。

各パッケージにはドキュメント一式が付属しています。また、TI プロセッサ向けにリリースされたファームウェアとソフトウェアは、既知の脆弱性がないか事前にスキャンされています。これらの制御機能が組み合わさることで、サイバーレジリエンス法で要求される適切なセキュリティレベルを満たしています。

TI は、既知の脆弱性を持たないソフトウェアをリリースすることを目指しています。TI は、TI の PSIRT (Product Security Incident Response Team、製品セキュリティ インシデント対応チーム) を通じて、長年にわたって積極的な脆弱性処理プロセスを実施してきました。TI における脆弱性処理プロセスには、以下のような例があります。

- SBOM の生成
- TI がプロセッサの一部として提供するさまざまなソフトウェアにわたる脆弱性を追跡
- 重大な脆弱性に対する修正プログラムの提供
- 脆弱性が修正された場合の公開

TI は協調型の脆弱性開示 (CVD) の要件を積極的に監視し、脆弱性を開示するシステムを導入しています。

TI のプロセッサは、サイバーレジリエンス法の要件を簡潔に満たす一連のコンプライアンス関連製品です。各シリコンファミリには、詳細なデータシートを付属して出荷され、TI はファームウェアパッチがいつどのように提供されるかをお客様に通知する明確な更新ポリシーを公開しています。すべてのソフトウェアスタック (ブートローダー、SDK、ミドルウェアなど) について、SBOM はすべての最上位ライセンス、コンポーネント、および依存関係を一覧表示し、脆弱性の追跡を容易にしています。TI は、各プロセッサ向けの新しい SDK リリースの一部として、SBOM を生成し、提供しています。製品のライフサイクルガイドには、各デバイスのサポート期間、サポート終了日、保証範囲が記載されています。セキュアブートやデバッグポート制御などのセキュリティ機能を、包括的なユーザーガイドで構成する方法について説明しています。また、各チップには固有の型番とダイ ID が存在し、エンドユーザーが正確な製品バリエーションを確認できるようになっています。これらの資料、更新、SBOM、および識別子をすべて組み合わせることで、OEM は TI プロセッサの CRA 準拠を証明するために必要なエビデンスを入手できます。

7 結論

サイバーレジリエンス法 (Cyber Resilience Act) は、サイバーセキュリティ機能を搭載したマイクロプロセッサの設計、製造、サポートに関して、TI のようなベンダに指示を与えています。TI は CRA の標準化された要件に従うことで、開発プロセスの透明性を確保しています。TI のお客様は、サイバーセキュリティ対応マイクロプロセッサの設計、提供、サポートに関する TI の知識と専門知識を活用できます。TI は、お客様がサイバーセキュリティ要件に準拠できるようにする機能と規制要件を実装するために、サイバーセキュリティの全体像、CRA の開発、およびその他の同様の規格を積極的にモニタリングしています。TI は、サイバーセキュリティ イネーブラを備えたマイクロプロセッサの構築、高度なセキュリティ機能の組み込み、絶えず進化する要件や規制のサイバーセキュリティ環境において、お客様が長期的に成功するのに役立つプロセスの策定に関して、業界から高い信頼を得ています。

8 参考資料

1. 欧州委員会、サイバーレジリエンス法、Web ページ。
2. テキサス インスツルメンツ、マイコン (MCU) およびプロセッサ、Web ページ。
3. テキサス インスツルメンツ、サイバーレジリエンス法 (CRA)、Web ページ。
4. テキサス インスツルメンツ、TI PSIRT、Web ページ。

重要なお知らせと免責事項

TI は、技術データと信頼性データ (データシートを含みます)、設計リソース (リファレンス デザインを含みます)、アプリケーションや設計に関する各種アドバイス、Web ツール、安全性情報、その他のリソースを、欠陥が存在する可能性のある「現状のまま」提供しており、商品性および特定目的に対する適合性の黙示保証、第三者の知的財産権の非侵害保証を含むいかなる保証も、明示的または黙示的にかかわらず拒否します。

これらのリソースは、TI 製品を使用する設計の経験を積んだ開発者への提供を意図したものです。(1) お客様のアプリケーションに適した TI 製品の選定、(2) お客様のアプリケーションの設計、検証、試験、(3) お客様のアプリケーションに該当する各種規格や、その他のあらゆる安全性、セキュリティ、規制、または他の要件への確実な適合に関する責任を、お客様のみが単独で負うものとします。

上記の各種リソースは、予告なく変更される可能性があります。これらのリソースは、リソースで説明されている TI 製品を使用するアプリケーションの開発の目的でのみ、TI はその使用をお客様に許諾します。これらのリソースに関して、他の目的で複製することや掲載することは禁止されています。TI や第三者の知的財産権のライセンスが付与されている訳ではありません。お客様は、これらのリソースを自身で使用した結果発生するあらゆる申し立て、損害、費用、損失、責任について、TI およびその代理人を完全に補償するものとし、TI は一切の責任を拒否します。

TI の製品は、 TI の販売条件 、 TI の総合的な品質ガイドライン 、 ti.com または TI 製品などに関連して提供される他の適用条件に従い提供されます。TI がこれらのリソースを提供することは、適用される TI の保証または他の保証の放棄の拡大や変更を意味するものではありません。 TI がカスタム、またはカスタマー仕様として明示的に指定していない限り、TI の製品は標準的なカタログに掲載される汎用機器です。

お客様がいかなる追加条項または代替条項を提案する場合も、TI はそれらに異議を唱え、拒否します。

最終更新日：2025 年 10 月