参考資料

Technical White Paper

*組込みプロセッサ サプライ チェーンにおける **CRA** の役割*

Josue Zamitiz-Ayala, Frangline Jose, and Amrit Mundra

概要

EU サイバー レジリエンス法 (CRA)、規則 (EU) 2024/2847 は、欧州連合 (EU) 市場に投入されるデジタル要素を含む製品に対してサイバーセキュリティ要件を課しています。これには、組み込み用途で製品メーカーに販売されるマイクロプロセッサなどのハードウェア部品も含まれます。CRA は、サプライ チェーン全体にわたってコンプライアンス要件を分担させています。部品サプライヤと製品メーカーは、それぞれ担う役割に応じて定められた要件を負うことになります。このホワイト ペーパーでは、TI が部品メーカーとしてシリコンおよびソフトウェア開発キット (SDK) レベルで取り組んでいる内容と、ティア 1 のボード ベンダ、システム オン モジュール (SoM) サプライヤや、OEM (Original Equipment Manufacturer) システム インテグレータなどの製品メーカーが CRA の下でどのような責任を負うことになるかを説明します。このホワイト ペーパーは法的助言を目的とするものではありません。製品ごとの具体的な対応については、各社の法務・コンプライアンス担当部門にご相談ください。

1 概要

EU サイバー レジリエンス法 (CRA) は、欧州連合市場で販売されるデジタル要素を搭載したすべてのハードウェア製品とソフトウェア製品に対して、統一的なサイバーセキュリティ要件を定める、法的拘束力のある規制枠組みです。CRA の施行は 2027 年 12 月 11 日に開始されます。脆弱性報告の要件は、2026 年 9 月 11 日に発効しました。サードパーティーの半導体部品を組み込んだコネクテッド デバイスを製造する製品メーカーにとって、CRA への対応は、シリコンやソフトウェアを個別に考えるだけでは解決できないコンプライアンス上の課題となります。これはこの規制が、デジタル要素を搭載した製品を自社名義で EU 市場に投入するサプライ チェーン上の各当事者に対して、それぞれの役割に応じた要件を課しているためです。

EU で販売される製品は、安全な設計原則に従い、最新の状態を維持するとともに、サポート期間を通じて、信頼性のある脆弱性対応プロセスを維持する必要があります。コンプライアンス上の課題は、多くの組込み製品が持つサプライ チェーン構造に起因しています。接続型 IoT ゲートウェイ、産業用コントローラ、協力ロボットを開発する OEM は通常、シリコン ベンダのマイクロプロセッサ、ティア 1 メーカーやシステム オン モジュール (SoM) ベンダのボード サポート パッケージ (ソフトウェア) を調達し、独自のアプリケーション ソフトウェアと組み合わせています。各当事者がそれぞれ部品を市場に投入しており、それぞれが CRA 上の責任を負います。

製品メーカーは、CRA の要件を満たしたサプライヤから部品を選定することで、自社に課される CRA 要件を免れることはできません。部品サプライヤが CRA に準拠していても、それによって製品メーカー自身のリスク評価、適合性の宣言 (製品が CRA のすべての要件を満たしていることを正式に表明するもの)、または製品メーカーが所在する国の CSIRT (国家サイバーセキュリティ インシデント対応チーム) および ENISA (EU のサイバーセキュリティ機関) への報告義務が満たされたことにはなりません。この 2 つの要件は並行して適用され、一方が他方に代わるものではありません。違反した場合、企業の全世界年間売上高の最大 2.5% の罰金が科される可能性があります。部品サプライヤや中間統合事業者も、この要件の対象外ではありません。

このホワイト ペーパーでは、サプライ チェーン上の責任範囲についての TI の解釈、部品メーカーとして TI が要件を満たすためにシリコンおよび SDK レベルで対応する事項、そして製品を統合する製品メーカーが完成品について対応すべき事項について説明します。コンプライアンスへの適合性の判断には、資格を有する法務・コンプライアンス専門家の助言が必要です。

Copyright © 2026 Texas Instruments Incorporated

2 CRA の適用範囲と部品サプライヤに関する論点

2.1 規制の対象

CRA は、「EU 市場で提供され、その意図された用途または合理的に予見可能な使用に、デバイスまたはネットワークへの直接的または間接的な論理的または物理的データ接続が含まれる」デジタル要素を含む製品に適用されます。[1] 実際には、「間接的な」接続には、USB、シリアル インターフェース、またはローカル ネットワークを介して接続可能なあらゆるデバイスが含まれます。事実上すべての組込み製品が対象となります CRA では、デジタル要素を含む製品の定義に、単体で販売されるソフトウェアまたはハードウェア部品も明示的に含めています。例えば、OEM が製品への組込みを目的として購入するマイクロプロセッサなどがこれに該当します。

TI のマイクロプロセッサおよびマイクロコントローラは、より大規模なシステムへの組込み用部品として販売されているため、デジタル要素を含む製品です。この定義において、TI と、TI のシリコンを完成品に組み込む OEM はいずれもメーカーに該当しますが、それぞれ異なる製品についてメーカーとなり、適用される要件も異なります。

CRA は、規制 (EU) 2019/2144 の対象となる自動車、規制 (EU) 2017/745 の対象となる医療機器、規制 (EU) 2018/1139 の対象となる民間航空機器など、いくつかの製品カテゴリをその適用範囲から除外しています。最終製品がこうした分野別の規制の対象となるお客様は、どのコンプライアンス対応が適用されるかについて、各社の法務部門に確認する必要があります。

2.2 CRA が TI 製品の分類方法

CRA は、製品を 4 つのリスク カテゴリに分類しています。デジタル要素を持つほとんどの製品は、デフォルト カテゴリに分類され、基準となる一連の要件が適用されます。リスクの高い製品タイプは、クラス I (Class I) またはクラス II (Class II) のいずれかに分類されます。最も機密性の高い製品はクリティカルに指定されます。

セキュリティ機能を内蔵したマイクロプロセッサまたはマイコンは、CRA 上、クラス I に該当します。クラス I は、暗号アクセラレータ、ハードウェア セキュア ブート、保護されたキー ストレージを搭載したマイクロプロセッサに適用されます。これとは別に、より厳格なクラス II のカテゴリは、物理的保護機能などのハードウェア改ざん防止機能を備えたチップに適用されます。この機能は、攻撃者がデバイスに直接物理的にアクセスした場合でも、秘密情報を抽出したり、デバイスの動作を改変したりすることを防ぐために設計された物理的保護機能を指します。改ざん防止機能のないマイクロプロセッサは、たとえこれらのマイクロプロセッサが仮想化をサポートしていたとしても、クラス I に分類されます。そのデバイス上で実行されているハイパーバイザ ソフトウェアについては、別途分類されます。

TI の Jacinto™ および Sitara™ プロセッサ ファミリはクラス I に分類されます。また、TDA54x SoC / プロセッサは、改ざん防止機能を組み込んでいるため、クラス II に分類されます。

クラス I および クラス II 製品は、EU で販売される前に、より厳格な承認プロセスを実施する必要があります。この規制では、コンプライアンスを実証する 3 つの方法が規定されています。1 つ目は、正式に認められた欧州の技術規格である整合規格に基づく自己評価プロセス (クラス I の製品にのみ適用) です (EN50765 は現在策定中)。2 つ目は、適合性評価機関 (Notified body) を利用する方法です。たとえば、EU から指定を受けたサードパーティーの機関が製品 (クラス I およびクラス II の両方を含む) を審査し、認証することができます。3 つ目の選択肢はモジュール H です。適合性評価機関は、メーカーの設計、開発、脆弱性処理プロセスを一度監査します。承認を受けた後は、メーカーは追加の審査を受けることなく、以後の製品について自ら適合性を証明できるようになります。モジュール H は、クラス I および クラス II 製品、およびクリティカル製品に適用されます。

この分類は TI の製品および TI が負う適合性に関する義務に適用されるものであり、OEM の完成品に適用されるものではありません。デフォルト カテゴリまたはクラス I/II に分類される TI 製部品をコネクテッド システムに組み込む OEM は、自社の最終製品について、別途その分類を判断する必要があります。

2.3 統合境界

TI の部品を組み込み、完成したシステムを EU 市場に投入する製品メーカーは、TI がコンポーネント レベルで満たしている適合性を、そのまま引き継ぐわけではありません。

CRA は、製品を自社名義で EU 市場に投入するすべての事業者に適用されます。OEM が TI 製プロセッサを組み込んだコネクテッド デバイスを EU 市場に投入する場合、その OEM は当該デバイスのメーカーとなり、製品全体について一連の遵守要件を負うことになります。部品メーカーとして負う TI の要件は、OEM の要件を代替するものではなく、追加的に適用されるものです。

Copyright © 2026 Texas Instruments Incorporated

TI は、製品メーカーが適合性を示すためのエビデンス パッケージ (証拠資料一式) に直接活用できる、コンプライアンス関連の資料およびハードウェア機能を提供しています。OEM の製品レベルの SBOM は、TI の SBOM に基づいて構築され、製品全体を網羅するものとなります。TI の CVE アドバイザリは、OEM の脆弱性対応プロセスにおける情報として活用されています。

3 責任分担モデル

3.1 サプライ チェーンの構成

TI のシリコンを内蔵したほとんどの組込み製品は、階層化されたサプライ チェーンを構成しています。最下層に TI のシリコンがあり、その上にファームウェアおよびソフトウェア スタックを提供する TI の SDK が位置しています。その上で、ティア 1 メーカーまたは SoM ベンダがシリコンと SDK をボードまたはモジュールに統合し、さらに OEM がその上に最終製品を構築します。サプライ チェーンの責任スタックは、このスタックをマッピングし、各階層に沿って CRA の要件を整合させます。

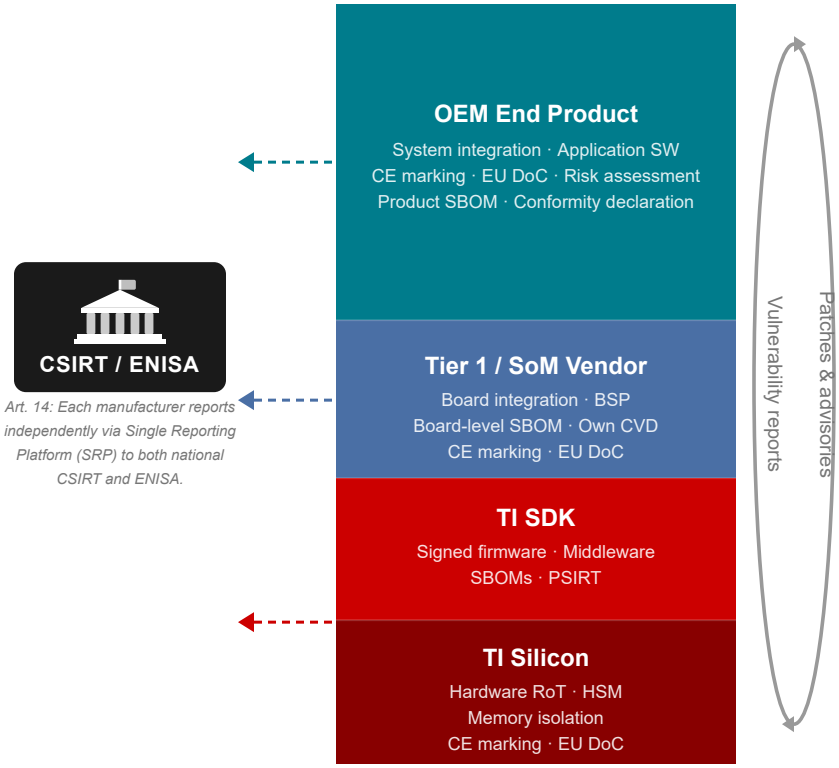


図 3-1. サプライ チェーン全体における CRA の責任の共有

セクション 3.1 に、CRA の責任がサプライ チェーン全体でどのように共有されているかを示します。TI は、ハードウェア レベルと部品レベルの要件 (下位 2 つの層) を担当します。ティア 1 サプライヤと SoM ベンダは、中間の統合に関する要件を担います。OEM は、製品レベルの適合性に関する責任を全面的に負います。パッチ、アドバイザリ、脆弱性レポートは、サプライ チェーンを循環する形で情報開示が行われるループ (右の楕円形、時計回り) を形成します。第 14 条では、サプライ チェーン内の各メーカーが、実際に悪用されている脆弱性について独立して報告することを求めています。各メーカーのレベルで、各国 CSIRT および ENISA へ同時に通知します (点線矢印)。報告期限および各層における義務については、第 14 条「メーカーの報告義務」を参照してください。これは、規制 (EU) 2024/2847 (サイバー レジリエンス法) に基づくものです。

サプライ チェーンにおける責任分担の脆弱性開示チェーンでは、セキュリティ アドバイザリおよびパッチ対応の義務が、どのようにサプライ チェーンの上流から下流へ伝達されるかを示しています。

1. TI が TI-PSIRT を通じて CVE アドバイザリを発行します

Copyright © 2026 Texas Instruments Incorporated

2. ティア 1 または SoM ベンダが、このアドバイザリをボード レベルのアップデートに組み込み、OEM 顧客にそのアドバイザリを渡します
3. OEM は製品にパッチを適用し、エンド ユーザーにアップデートを提供します。この脆弱性が実際に悪用された場合、TI は第 14 条に基づき各国の CSIRT と ENISA に同時に通知します。

ティア 1 または SoM ベンダと OEM も、最終製品で実際に悪用されている脆弱性を認識した場合、それぞれ独立して同じ報告義務を負います。

CRA では、メーカーは 2 種類のセキュリティ イベントを報告する必要があり、それぞれに 3 段階の通知手順があります。最初のトラック 1 は、実際に悪用されている脆弱性に適用されます。たとえば、製品に存在する既知の脆弱性を攻撃者が実際にユーザーに対する攻撃に利用しているケースです。トラック 2 は、データや機能の可用性、真正性、完全性、機密性を保護する製品の機能に影響を与える、または影響を与える可能性のあるイベント、製品やユーザーのシステムで悪意のあるコードが導入または実行される原因となったイベント、あるいはその可能性のあるイベントなど、製品のセキュリティに影響を与える重大なインシデントに適用されます。両方のトラックにおけるすべての通知は、コーディネーターとして指定された各国 CSIRT に同時に送信され、CRA Single Reporting Platform を通じて ENISA に送信されます。

表 3-1. 第 14 条 - メーカーの報告義務

期限	報告内容 (口頭)
トラック 1：実際に悪用されている脆弱性 (第 14 条 (1) ～ (2))	
認識してから 24 時間以内	「実際に悪用されている脆弱性に関する初期警告通知。該当する場合、メーカーが、自社のデジタル要素を備えた製品が提供されていることを把握している加盟国も記載すること。」
認識してから 72 時間以内	「脆弱性通知…。入手可能な範囲で、対象となるデジタル要素を含む製品に関する一般的な情報、悪用の一般的な性質、関係する脆弱性の一般的な性質、ならびに実施済みの是正措置または軽減措置、および実施可能な是正措置または軽減措置を提供すること」
是正措置または軽減措置が利用可能になってから 14 日以内	「最終報告… 少なくとも以下を含むものとする。(i) 脆弱性の重大度と影響を含む説明、(ii) 入手可能な場合には、その脆弱性を悪用した、または現在悪用している悪意のある攻撃者に関する情報、(iii) 脆弱性を是正するために提供されたセキュリティ更新プログラムまたはその他の是正措置に関する詳細」
トラック 2：セキュリティに影響を与える重大なインシデント (第 14 条 (3) ～ (4))	
認識してから 24 時間以内	「デジタル要素を備えた製品のセキュリティに影響を及ぼす重大なインシデントに関する初期警告通知… 少なくとも、当該インシデントが違法行為または悪意ある行為によって引き起こされた疑いがあるかどうかを含めること」
認識してから 72 時間以内	「インシデント通知… 可能な場合は、インシデントの性質、インシデントの初期評価、および実施された是正措置または軽減措置、ユーザーが実行できる是正措置または軽減措置に関する一般的な情報を提供すること」
72 時間以内のインシデント通知から 1 か月以内	「最終報告… 少なくとも以下を含むものとする。(i) インシデントの重大度および影響を含む詳細な説明、(ii) インシデントの原因となる可能性のある脅威の種類または根本原因、(iii) 適用済み、かつ継続的な軽減措置」

トラック 1 は、製品に存在する既知の脆弱性が実際に悪用されている場合に適用され、報告期限は、脆弱性の発見および是正対応を起点として設定されます。トラック 2 は、特定の脆弱性が確認されているかどうかにかかわらず、セキュリティ イベントがすでに製品またはユーザーに影響を与えている場合に適用されます。トラック 2 の報告期限の起算点は、インシデントの発生時点に紐づいています。2 つのトラックは相互に排他的ではありません。実際に悪用されている脆弱性によってセキュリティ侵害が発生した場合、両方のトラックが同時にトリガされ、各イベントには個別の通知セットが必要になります。

3.2 CRA 要件別責任分担

セクション 3.2 に、サプライ チェーンにおける各当事者に対する主な CRA の要件を示します。メーカーが EU 内に拠点を持たない場合、CRA は EU の認定担当者を任命することが求められます。この担当者は、EU 内で登録された事業者であり、規制当局からの連絡を受け取るとともに、メーカーに代わって対応する役割を担います。ここで示している責任分担は、TI が想定する一般的な組込み製品のサプライ チェーンを前提とした解釈に基づいています。特定の製品やサプライ チェーンの構成によって責任の分担が異なる場合がありますが、セクション 3.2 は、個別製品についてのコンプライアンス分析に代わるものではありません。

表 3-2. サプライ チェーン全体における CRA 義務の分担

CRA 要件	規則上の参照箇所	TI (部品メーカー)	ティア 1/SoM ベンダ	OEM 製品メーカー
サイバーセキュリティのリスク評価	第 13 条 (2)	チップ レベルの脅威モデル。セキュリティ データシート	ボード レベルのリスク評価	システム全体を対象とした製品レベルのリスク評価

Copyright © 2026 Texas Instruments Incorporated

表 3-2. サプライ チェーン全体における CRA 義務の分担 (続き)

CRA 要件	規則上の参照箇所	TI (部品メーカー)	ティア 1/SoM ベンダ	OEM 製品メーカー
SBOM - 最上位レベルの依存関係	付録 I、第 II 部、項目 1	SBOM (SPDX、CycloneDX)。MySecure を使用したセキュアな SW	ボード レベルの SBOM	すべてのサプライヤ の SBOM と自社アプリケーション ソフトウェアを統合した製品 SBOM
リリース時点で既知の悪用可能な脆弱性がないこと	付録 I、第 I 部、項目 2(a)	各リリース前に SDK をスキャン	リリース前にボード (BSP) ソフトウェアをスキャン。ベンダは SDK およびその他の SW も提供。	EU 市場に投入する前に、製品全体について既知の脆弱性をスキャン
セキュア バイ デフォルト構成	付録 I、第 I 部、項目 2(b)	ハードウェアの信頼の起点 (Hardware Root of Trust) およびセキュア ブート機能を提供。セキュリティ強化型デバイス バリアントでは ROM によって強制	ボードのデフォルト設定を構成	製品をセキュアなデフォルト状態で出荷。顧客向けの設定手順を提供。パスワードなどのデフォルト設定を変更するよう顧客に要求
セキュリティのアップデートが可能であること	付録 I、第 I 部、項目 2(c)	CI/CD パイプラインまたはセキュア フォルダを通じてファームウェア パッチを提供 (機密性に応じて)。PSIRT/PSAP がパッチの状況を追跡・連絡。	ボードのアップデート機構を提供	エンド ユーザーへの更新プログラムの配信 (無償)
不正アクセスからの保護	付録 I、第 I 部、項目 2(d)	ハードウェア アクセス制御。デバッグ ポート制御	ボード レベルの認証	製品レベルの認証とアクセス管理
完全性の保護	付録 I、第 I 部、項目 2(f)	署名付きファームウェア アーキテクチャによりブート時の完全性を確保。セキュリティ強化型デバイス バリアントでは暗号学的に強制	ボード部品向けのファームウェア署名	システム レベルの完全性の検証
攻撃対象領域を制限すること	付録 I、第 I 部、項目 2(j)	ハードウェアによる分離	ボード インターフェイス構成	製品インターフェイスの最小化と堅牢化
製品のセキュリティ試験および脆弱性対応に関するセキュリティ試験報告書	付録 I、第 I 部、付録 I 第 II 部、付録 VII(6)	部品レベルのセキュリティ機能を対象とした試験報告書。各部品レベルの脆弱性の修正に関する報告書を更新。	ボード レベルのセキュリティ統合を対象とした試験報告書。ボード レベルの脆弱性を修正するたびに報告書を更新。	最終製品のセキュリティ機能を対象とした試験報告書。製品 レベルの脆弱性を修正するたびに報告書を更新。
CE マーキング	第 29 条 ～ 30 条	EU 市場に投入する TI 製部品に必要	ティア 1 がモジュールを独立した製品として EU 市場に投入する場合に必要	最終製品に必要
EU 域内の認定担当者	第 18 条	TI は EU 域内の拠点を維持	ティア 1 が EU 域内に設立されていない場合に必要	OEM が EU 域内に設立されていない場合に必要
協調型脆弱性開示 (CVD) ポリシー	付録 I、第 II 部、項目 5	TI の PSIRT ポリシー	ティア 1 独自の CVD ポリシー	自社製品向けの OEM 独自の CVD ポリシー
脆弱性報告窓口	付録 I、第 II 部、項目 6	psirt@ti.com	ティア 1 のセキュリティ連絡先	エンド ユーザー向けに公開する OEM のセキュリティ連絡先
実際に悪用されている脆弱性の報告	第 14 条	CRA Single Reporting Platform を使用して、TI から各国の CSIRT および ENISA へ同時に通知。詳細な通知手順は第 14 条「メーカーの報告義務」を参照。	ティア 1 から各国の CSIRT および ENISA へ同時に通知。詳細な通知手順は第 14 条「メーカーの報告義務」を参照。	OEM から各国の CSIRT および ENISA へ同時に通知。詳細な通知手順は第 14 条「メーカーの報告義務」を参照。
サポート期間の明示	付録 II、項目 7	デバイス ファミリごとのライフサイクル ガイド	モジュールのサポート期間を明示	エンド ユーザー向けに製品のサポート期間を明示
技術資料	第 31 条	部品レベルの技術文書	モジュール レベルの技文書術	製品全体の技術文書

3.3 ティア 1 および SoM ベンダ層

TI の多くのお客様は、TI と OEM の間で橋渡しをするティア 1 ボード メーカーまたは SoM ベンダを介して製品を提供しています。ティア 1 メーカーまたは SoM ベンダが、自社名義でボードまたはモジュールを EU 市場に投入する場合、そのベンダはメーカーとなり、CRA 上の要件を負います。ベンダが OEM の指示の下で委託メーカーとして業務を行い、自社名義で製品を市場に投入しない場合、CRA 上のメーカーとしての義務はすべて OEM が負います。同様に、チップダウン設計では、OEM はティア 1 や SoM ベンダを介さずに TI のシリコンを直接組み込むため、製品レベルの義務は OEM が単独で負います。

Copyright © 2026 Texas Instruments Incorporated

ティア 1 または SoM ベンダがメーカーとしての立場になる場合、TI の SDK の SBOM を組み込んだボード レベルの SBOM を作成し、自社の CVD (協調型脆弱性開示) ポリシーおよび脆弱性開示窓口を維持するとともに、下流の統合事業者にセキュリティ関連文書を提供する必要があります。

CRA 対応のプロセスを整備しているティア 1 メーカーからボードやモジュールを選定したとしても、OEM が完成品について製品レベルのリスク評価を実施し、製品レベルの SBOM を作成し、適合性の宣言を行う義務がなくなるわけではありません。各関係者に課される要件は、その関係者が自社名義で市場に投入する製品に対して適用されます。

4 CRA に関連する TI のセキュリティ機能

TI は、付録 I のハードウェアおよび部品レベルの要件に対応するため、セキュリティ機能を備えたデバイス ファミリを設計しています。デバイスごとの具体的な実装方法については、該当するデバイスのデータシート、セキュリティ ユーザー ガイド、『未来を守る:TI の Jacinto プロセッサおよび Sitara プロセッサにおける CRA 準拠』テクニカル ホワイト ペーパーを参照してください。

4.1 ハードウェア セキュリティ機能

セキュリティ機能を備えた TI 製プロセッサには、メインのアプリケーション プロセッサから分離されたコア上で動作する専用のセキュリティ サブシステムが搭載されており、TI が提供するファームウェア (TI Foundational Security - TIFS) によって、ハードウェアの信頼の起点 (Hardware Root of Trust) を実現します。新世代のデバイスでは、顧客の HSM ソフトウェア スタック用の 2 番目の専用セキュリティ コアを利用できるため、アプリケーション領域のソフトウェアにキー マテリアルを公開することなく暗号化サービスを実現できます。

製造時にシリコンへ恒久的に書き込まれた公開鍵が、セキュア ブートの信頼の起点となります。セキュリティ強化 (HS-SE) デバイス バリアントでは、ブート ROM が実行前にプライマリ ファームウェア イメージのデジタル署名を検証し、検証に失敗したイメージを拒否することで、電源投入時からハードウェアによって完全性および真正性が検証されます。

ハードウェア アクセス制御により、オンチップ メモリは各処理ドメインに割り当てられた複数のゾーンに分割され、異なるワークロードの境界を越えた不正な読み取りや書き込みが防止されます。

セキュリティ機能を備えたデバイス バリアントでは、量産ユニットのデバッグ インターフェイスを恒久的に無効化にすることも、署名付き証明書による認証済みのアクセス要求が行われた場合にのみアクセスを許可するよう制限することもできます。これにより、デバッグ ツールを悪用した一般的な攻撃ベクトルを閉じることができます。

各チップには、型番に加えて固有のダイ ID が付与されているため、個々のシリコンを正確に識別でき、製品識別要件への対応をサポートできます。

4.2 SDK およびソフトウェアのセキュリティ

TI は、ti.com 上で SDK の一部として公開ソース コードを提供しているすべての製品向けに、SPDX および CycloneDX 形式の SBOM を提供しています。セキュアなソフトウェア部品用の SBOM は、TI の MySecure アクセス プログラムから入手できます。

TI のプロセッサ SDK は各リリース前に、既知の脆弱性がないかスキャンされます。TI は、PSIRT を通じて脆弱性対応のライフサイクル全体を管理しています。これには、通知の受付、トリアージ、技術分析、是正対応、協調的な公開が含まれ、CVSS v3.1 による深刻度評価および CVE の割り当ても行われます。このプロセスは、ISO/IEC 30111 と ISO/IEC 29147 に準拠しています。TI は、セキュリティ パッチとアドバイザリ メッセージを無償で提供しています。

TI は、ti.com/psap にある製品セキュリティ アドバイザリ ポータル (PSAP) を通じてパッチとアドバイザリを提供しています。PSAP では、顧客が myTI アカウントを使用して体系的に脆弱性を報告したり、自社の設計で使用している TI 製品に対象を限定したアドバイザリ フィードを購読したり、CSAF v2.0 の機械可読形式で公開された情報にアクセスしたりできます。CSAF v2.0 のアドバイザリには、影響を受ける特定のソフトウェア部品が記載されており、顧客は自社の SBOM との照合を自動化し、CRA で定められた報告期限内に、自社製品への影響範囲を評価できます。

TI は、BSI TR-03183-3 と RFC 9116 に従い、ti.com/.well-known/security.txt で security.txt ファイルを公開しています。テキスト ファイルには、PSIRT 連絡先アドレス、CVD ポリシー URI、および CSAF プロバイダ メタデータが含まれています。ドイツの法域の下で事業を行っており、第 14 条に基づく報告について TI が指定する国の CSIRT は、ドイツ連邦情報セキュリティ庁 (BSI) が運営する CERT-Bund です。TI は、要求されたスケジュール内に CRA Single Reporting Platform を通じてインシデント通知を送信します。

Copyright © 2026 Texas Instruments Incorporated

第 14 条では、メーカーは、実際に悪用されている脆弱性を「認識した時点」から 24 時間以内に、適切な各国 CSIRT へ通知することが求められています。この規則では、複数の担当者が存在する組織において、具体的にいつ認識したとみなすかについては定義されていません。そのため、組織内で何を認識とみなすのかをあらかじめ定義する必要があります。たとえば、報告を受け付けた時点とするのか、担当する技術チームのメンバーが初めてその報告を確認した時点とするのか、といった基準で、これを明確に定義していないと、コンプライアンス上のリスクが生じます。24 時間の期限は、個々のエンジニアが報告を確認した時点ではなく、定義された時点から開始されます。PSAP の自動期限管理機能は、期限が到来する前に報告をエスカレーションすることで、この要件への対応を支援します。TI が把握した実際に悪用されている脆弱性については、その情報がセキュリティ研究者、顧客、または TI 内部から発見されたものであるかにかかわらず、24 時間の報告期限が適用されます。その後、72 時間以内の通知として、より詳細な評価結果を提出します。この通知は、CRA Single Reporting Platform を通じて、各国 CSIRT と ENISA の両方に同時に提出されます。

4.3 ドキュメントおよびライフサイクル関連資料

TI は、各デバイス ファミリの詳細なデータシートを公開し、ハードウェア セキュリティ機能とインターフェイスの仕様を文書化しています。専用のアップデート ポリシーでは、TI がファームウェア パッチを提供する時期と方法について説明しています。各デバイスのライフサイクル ガイドには、サポート期間と保証範囲が記載されています。

ユーザー ガイドでは、セキュア ブートの設定、デバッグ ポートの構成、HSM との統合について説明しています。

5 まとめ

デジタル要素を含むコネクテッド製品の CRA 準拠には、サプライ チェーン全体での連携した対応が必要です。各当事者には明確な要件があり、いずれも他の当事者の要件に代わるものではありません。

TI は、部品メーカーとしての役割に対応し、セキュリティ機能を備えたデバイス バリアントにおけるハードウェアの信頼の起点 (Hardware Root of Trust) とメモリの分離、署名付きファームウェア、SBOM、CRA 第 14 条の報告期限に沿った PSIRT プロセス、および CRA の情報要件を満たすデバイス レベルの文書を提供しています。製品メーカーとティア 1 ベンダは、これらの機能と成果物をコンプライアンス業務に組み込んでいます。これらの企業は、TI が代わって対応することのできない、製品レベルでのコンプライアンスについて引き続き責任を負います。

コネクテッド デバイスを EU 市場に投入する製品メーカーは、製品レベルのサイバーセキュリティ リスク評価を実施し、製品レベルの SBOM を生成し、適合性を宣言し、CE マーキングを適用し、EU 内に拠点を持たない場合には、EU の認定担当者を選任する必要があります。また、実際に悪用されている脆弱性を認識した時点から 24 時間以内に、各国の CSIRT と ENISA に同時に通知し、72 時間以内により詳細な評価を提出するためのプロセスを整備・維持する必要があります。完全な通知手順については、第 14 条「メーカーの報告義務」を参照してください。TI の PSIRT アドバイザリと SBOM は、このプロセスに活用されます。

TI のデバイス機能が CRA の要件にどのように対応しているかを評価するには、TI のセキュリティ チームに協力を依頼し、ti.com/quality-reliability/quality/ti-psirt.html で PSIRT ポリシーを確認してください。製品ごとの具体的な対応については、各社の法務・コンプライアンス担当部門にご相談ください。第 14 条に基づく脆弱性報告要件は、すでに施行されています。CRA の全面的な施行は 2027 年 12 月に開始されます。EU 市場向けにコネクテッド デバイスを製造する製品メーカーは、今のうちからコンプライアンス評価に着手しておく必要があります。

6 参考資料

1. 欧州議会および欧州連合理事会 (2024 年 11 月 20 日)。『デジタル要素を含む製品に対する水平的なサイバーセキュリティ要件に関する欧州議会および欧州連合理事会規則 (EU) 2024/2847 (サイバー レジリエンス法)。』。欧州連合官報、L シリーズ。
2. テキサス インスツルメンツ。「TI PSIRT.」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、『未来を守る：TI の Jacinto プロセッサおよび Sitara プロセッサにおける CRA 準拠』テクニカル ホワイト ペーパー
5. テキサス インスツルメンツ、『コンプライアンスの強化：サイバーセキュリティの脆弱性管理の合理化』アプリケーション ブリーフ

English Document: STDA050
Copyright © 2026 Texas Instruments Incorporated

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。

Copyright © 2026, Texas Instruments Incorporated

最終更新日：2025 年 10 月