

サイバー・レジリエンス法（CRA）への準拠

CRA要件を満たすための徹底ガイド

目次

はじめに 3
CRA不適合のリスクとは 3
サイバー・レジリエンス法に関する誤った認識 4
CRAの基礎 5
CRA準拠までのカウントダウン 5
主な適合性要件（付属書I） 5
主な義務（第13条および第14条） 7
CRA第13条：製造業者の義務 7
製造業者の報告義務（第14条） 9
適合性および製品ライフサイクルに関する重要事項 10
技術文書要件 10
適合性評価手順（第32条） 11
準拠に向けた連携 12
NXPとDigiの連携 – 次世代のプロセッサおよびSOMソリューションを構築 12
NXPのセキュリティ態勢：CRA対応 12
スケーラブルなセキュリティ・アーキテクチャとCRA要件のマッピング 12
CRA準拠のアプリケーションに向けたNXPのセキュリティ・ソリューション 12
Digiによる、CRA準拠のためのエンド・ツー・エンドのサポート 13
Digiによる、準拠重視のエコシステム 13
Digi TrustFence 13
Digi ConnectCoreセキュリティ・サービス 14
Digi ConnectCoreクラウド・サービス 14
Digiワイヤレス・デザイン・サービス 14
Digi Embedded Yocto (DEY) 14
CRAへの準拠：Digiセキュリティ・ビルディング・ブロックの活用 15
CRAへの準拠：Digiセキュリティ・ビルディング・ブロックの活用 (I) 16
CRAへの準拠：Digiセキュリティ・ビルディング・ブロックの活用 (II) 17
Digiエコシステム：CRA準拠の統合 18
おわりに 18

はじめに

サイバー・レジリエンス法（Cyber Resilience Act：CRA）は、サイバーセキュリティに関する厳格な義務をCE (Conformité Européenne) マーキングの枠組みに組み込むことで、世界で販売される製品の適合性のあり方を大きく変革するものです。その要件は、原産地にかかわらず、EU域内で販売されるあらゆるOEM製品に影響を与える可能性があります。公式には規則 (EU) 2024/2847として知られるCRAは、デジタル要素を備えたあらゆる製品のうち、その意図された目的または予見可能な使用の一環として、ネットワークまたはデバイスへの直接的または間接的なデータ接続（論理/物理を問わず）を含むものに適用されます。DigiとNXPが提供するこのハンズオン・ガイドでは、それらの要件および準拠に向けた対応について解説します。

この規則に基づいて、デバイスまたはネットワークに接続可能なすべての製品は、CEマーキングを取得するために規定のサイバーセキュリティ要件を満たす必要があります。これは、EU域内で製品を販売するための法的な前提条件となっています。不適合の製品はEU市場に流通させることはできません。

CRAの核心にあるのは、恒常的に存在するサイバーセキュリティ上の弱点への対応です。セキュリティ対応が謳われた製品は数多く存在していますが、消費者や企業にとって、その主張について確かめたり、継続的な保護を確保したりするための信頼できる手段はほとんどありません。CRAは、製品のライフサイクル全体にわたるサイバーセキュリティ対策のための統一された強制的枠組みを提供します。

そのために、この規則では以下が確立されています。

- すべての製造業者にとっての一貫した開始点となる、デジタル要素を備えた製品またはソフトウェアの市場投入に関する共通要件
- 接続可能な製品の計画、設計、開発、保守のための単一のサイバーセキュリティの枠組み
- 販売時のみならず、製品のライフサイクル全体を通じて適用される注意義務

この枠組みは、完成品の製造業者だけではなく、ハードウェアおよびソフトウェア・コンポーネントの供給業者による準拠も促進することを目的としています。

これまでのEU法と同様に、他の国々も既にCRAにならった取り組みを進めています。たとえば、米国では、**2024年9月にU.S. Cyber Trust Markを導入**しました。米国連邦通信委員会（Federal Communications Commission：FCC）が運営するこの自主的ラベリング・プログラムは、よりセキュアなコネクテッド製品の開発を奨励することを意図しています。

CRAの要件に準拠することには、自社の製品と各国で展開されているセキュリティ対策との整合性を図れるという利点があります。さらに重要なことに、企業にとってCRAを理解することは、高い代償を伴う手直しや市場からの製品の回収といった事態を回避するのに役立ちます。

CRA不適合のリスクとは

CRAへの準拠は必須要件です。この規則の対象製品でCEマーキングを取得できていない場合は、EU域内で合法的に販売することはできません。規制当局は不適合製品を市場から撤退させる権利を有しており、それにより市場における企業のプレゼンスが損なわれるおそれがあります。

また、規制当局は不適合に対して罰金を科す場合があります。CRAの違反に対しては、1件につき最大1,500万ユーロまたは企業の全世界年間売上高の2.5%のいずれか高い方の制裁金が科される可能性があります。

こういった厳しい結果が伴うにもかかわらず、CRAに関する誤った認識が今もなお蔓延しています。よくある誤解は、タイムラインについてです。多くの企業でこの規則は2027年まで施行されないと認識されているようですが、CRAは既に発効しています。主な対応期限は間近に迫っています。詳細については、**5ページの「CRA準拠までのカウントダウン」**を参照してください。

> 多くの企業でこの規則は2027年まで施行されないと認識されているようですが、CRAは既に発効しています。
>
> 詳細については、5ページの「CRA準拠までのカウントダウン」を参照してください。

この規則の適用範囲、とりわけ対象製品、責任の所在、および適合性の維持に必要な手順についても、いまだに混乱が見られます。最も差し迫った問題の一部について、**4ページの「サイバー・レジリエンス法に関する誤った認識」**で取り上げています。製造業者や調達管理者、開発チームにとって、これらの詳細を把握することは極めて重要です。

より広く言えば、企業、サプライ・チェーン、製品開発におけるこの重要な規則への準拠を維持するためには、CRAの基礎を徹底的に振り返ることが不可欠です。

免責事項：本記事は情報提供のみを目的としており、法的助言を提供するものではありません。読者は、専門家に相談することなく、本記事で提供されている情報に依拠した措置を講じてはなりません。固有の状況または適用法の解釈に関する助言については、資格を有する法律家にご相談ください。

サイバー・レジリエンス法に関する誤った認識

誤った認識	実際の要件
CRAは欧州を本拠地とする企業のみに適用される。	**欧州市場に製品を流通させるすべての製造業者、輸入業者、流通業者は、本社の所在地にかかわらずCRAに準拠する必要があります。**
CRAの全面適用時において既に市場に流通している製品は、適用除外である。	**レガシー製品であるか否かにかかわらず、2027年12月11日以降に大幅な変更が加えられた製品はいずれも、CRAの要件を満たすことが必要となります。** **製造業者は、第69条「経過規定」にある例外も念頭に置く必要があります。第14条「製造業者の報告義務」に規定された義務については、2027年12月11日よりも前に市場に流通している、この規則の適用範囲内にあるすべての製品に適用されます。**
CRAに準拠する責任があるのはOEMだけである。	**CRAは、製造業者から輸入業者、流通業者、供給業者に至るまでのサプライ・チェーン全体に適用され、そのすべての当事者が準拠に対する責任を負います。この規則は、最終製品またはコンポーネントのいずれの形態のハードウェアおよびソフトウェア製品にも適用されます。これらのグループおよび個人を以下「責任当事者」といいます。この文書では、製造業者の責任のみを取り上げている点にご注意ください。**
ITデバイスや通信デバイスのみがCRAの適用対象である。	**CRAの適用範囲は、IoTデバイスから産業用制御システムまで、デジタル要素を備えた大多数の市販製品に及びます。** **ただし、他の規則が既に適用されている一部の製品については、CRAの適合性要件の適用除外となっています。たとえば、以下がそれらに該当します。** **● 医療機器** **● 自動車のシステムおよびコンポーネント** **● 航空関連機器** **● 船舶機器** **● デジタル要素を備えた製品内の同一のコンポーネントを置き換えるためのスペア・パーツ** **● 防衛や国家安全保障に関する製品、または国家機密情報の処理を目的とした製品**
オープンソースの製品はCRAの適用除外である。	**製品がCRAへの準拠を必要とする場合、オープンソースのコンポーネントが含まれているかどうかは関係ありません。**
CRAはソフトウェアが組み込まれた製品にのみ適用される。	**商用製品でその中核機能の一部としてクラウド・プラットフォームまたはリモートでのデータ処理が必要である場合は、CRAの適用対象となります。**
ほとんどの時間オフラインで使用される製品は、CRAに適合する必要はない。	**デジタル要素を備えたコンポーネントは、デバイスやネットワークにデータ接続できる機能を備えていれば、CRAに適合する必要があります。**
製品の試験や認証は一度のみでよい。	**CRAでは、市場に投入された時のみならず、製品ライフサイクル全体を通じた継続的な保守、適合、および遵守が要求されます。**

CRAの基礎

従来の規制とは異なり、CRAでは具体的な技術要件、明確な義務、および定義された対応期限が規定されており、サプライ・チェーン全体で義務を果たすことが求められます。これらの新しい規則は、6つの柱を基盤として策定されています。

- ✓ **厳格なサイバーセキュリティ**：CRAでは、設計、開発、保守、およびアフターマーケット・サポートに関する高度なセキュリティ要件が定められています。製造業者は、製品の脆弱性の監視、脆弱性に対する積極的な対応、定期的なアップデートの提供を実施する必要があります。
- ✓ **適合性評価**：製品は、EU市場に投入される前に必須サイバーセキュリティ要件に適合していることを確認するために、細部にわたって評価される必要があります。
- ✓ **脆弱性およびインシデントの早期報告**：実際に悪用された脆弱性や重大インシデントについては、迅速な対応を可能にするために、認識してから24時間以内に指定当局へ報告する義務があります。
- ✓ **製品分類**：製品は、サイバーセキュリティのリスクに応じて、一般製品、重要な製品、クリティカルな製品のカテゴリに分類されており、釣り合いの取れたセキュリティ評価を確保するために、それぞれに固有の適合性評価手順が定められています。
- ✓ **監視と監査**：適合性は、上市時のみならず製品ライフサイクル全体を通じて、積極的な監視と監査によって維持される必要があります。
- ✓ **透明性と情報伝達**：OEMは、製品のセキュリティ特性、脆弱性、および是正措置に関する明確な最新の情報をユーザーおよび当局に提供する必要があります。

第13条第19項：「製造業者は、第8項に定めるサポート期間の終了日（少なくとも年と月を含む）を、製品の購入時において明確に認識できる方法で明示しなければならない。さらに、適用可能な場合、デジタル要素を備えた製品またはそのパッケージ上、あるいはデジタル手段によってそれを表示しなければならない。

デジタル要素を備えた製品の性質上技術的に実現可能な場合、製造業者はデジタル要素を備えた製品にそのサポート期間が終了した旨の通知を表示しなければならない」

これらの柱を組み合わせることで、サイバーセキュリティへの標準化されたアプローチを創出し、エンド・ユーザーが入手する前ならびに製品ライフサイクル全体にわたって、接続可能な製品を必須サイバーセキュリティ要件に適合させることが可能になります。

製造業者は規定のタイムライン内に確実に準拠できるよう、今すぐ対策を始める必要があります。

CRA準拠までのカウントダウン

CRAは、2020年に発表されたEUサイバーセキュリティ戦略の一環であり、**NIS2指令の枠組み**を補完することを目的としていました。この規則は、2024年10月23日に欧州議会および欧州連合協議会によって正式に署名され、**2024年11月20日に官報に掲載**されました。

2024年12月10日
全面適用までの猶予期間を設けたうえで、CRAが正式にEU法として採択されました。

2026年6月11日
第IV章第35～51条に記載されているとおり、CRAの適合性評価の確認を担う適合性評価機関が業務を開始します。

企業は適合性評価手順への習熟を進め、自社の製品のカテゴリにおいて適合性評価機関との正式な関わりが必要であるか、または2027年の全面適用前の準拠に向けた取り組みをサポートする自主的な協力関係が適切であるかを判断する必要があります。

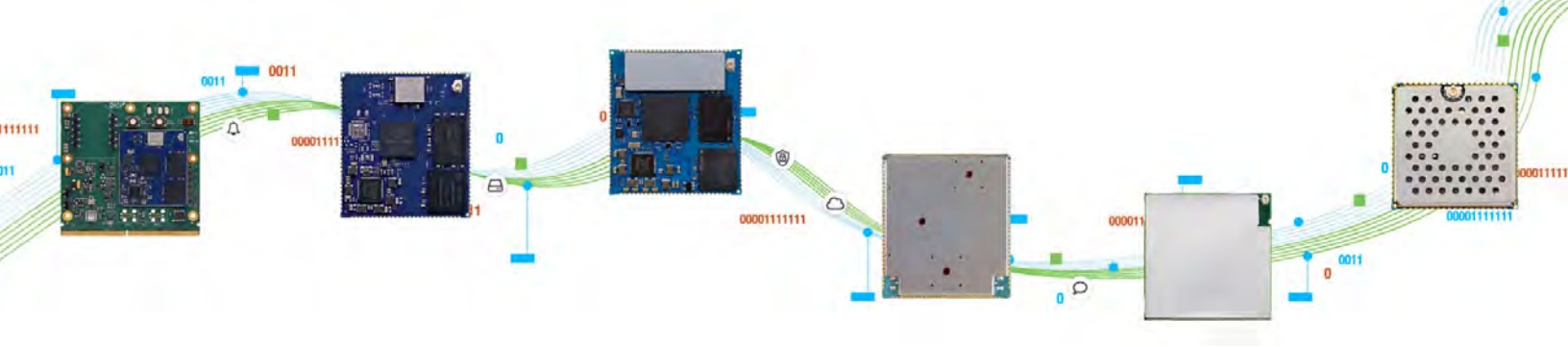
2026年9月11日
第14条に記載されているとおり、製造業者は、当該製品における実際に悪用された脆弱性および重大インシデントについて、発見から24時間以内に、「コーディネーターとして指定された」コンピュータ・セキュリティ・インシデント対応チーム（Computer Security Incident Response Team：CSIRT）および欧州連合サイバーセキュリティ庁（European Union Agency for Cybersecurity：ENISA）に同時に報告することが義務付けられます。

2027年12月11日
サイバー・レジリエンス法の全面適用。この日以降、すべての対象製品について、EUでの販売が認められるにはCEマーキングを取得していることが必要になります。

主な適合性要件（付属書I）

CRAでは、「ゆりかごから墓場まで」のサイバーセキュリティの適合性を義務付けており、セキュアな製品設計と製品ライフサイクル全体を通じた継続的な保護の両方が求められます。これは、サイバーセキュリティは、最も初期の開発段階で対応されなければならず、製品の発売以降も十分に保守される必要があることを意味します。
（**詳細については、7ページの「サポート期間」のセクションを参照してください**。）

この目的をサポートするために、CRAの付属書Iには、サイバーセキュリティ要件の2つのカテゴリ、パートIとIIについて記載されています。パートIではデジタル要素を備えた製品の特性に焦点を当てており、パートIIでは脆弱性への対応およびライフサイクル管理について規定しています。



パートI：製品関連のサイバーセキュリティ要件

企業は、設計段階において徹底したサイバーセキュリティ・リスク評価を実施し、潜在的リスクに基づいた適切なレベルのサイバーセキュリティを確立することが求められます（付属書I、パートI、第1項）。これ以降、デジタル要素を備えた製品は以下の要件を満たしている必要があります。

- リリース時において、悪用可能な既知の脆弱性がないこと（付属書I、パートI、第2項 (a)）
- 「セキュア・バイ・デフォルト」の設定で出荷されること（付属書I、パートI、第2項 (b)）
- 自動またはデフォルトでの有効化によるセキュリティ・アップデートを通じて、脆弱性に確実に対応できるようにすること（付属書I、パートI、第2項 (c)）
- 適切な認証、識別、またはアクセス管理システムにより、不正アクセスから保護すること（付属書I、パートI、第2項 (d)）
- 最先端の仕組みを用いて保存中や伝送中のデータを暗号化することなどにより、データの秘匿性を保護すること（付属書I、パートI、第2項 (e)）
- 保存、伝送、または処理されるデータ、コマンド、プログラム、構成の完全性をあらゆる不正な改ざんから保護するとともに、データ破損について報告すること（付属書I、パートI、第2項 (f)）
- 意図された使用と厳密に関連するデータのみを処理すること（付属書I、パートI、第2項 (g)）
- 重要な機能をDoS (Denial-of-Service) 攻撃から保護すること（付属書I、パートI、第2項 (h)）
- 製品自体または接続されたデバイスが、他のデバイスまたはネットワークによって提供されるサービスに及ぼす潜在的影響を最小限に抑えること（付属書I、パートI、第2項 (i)）
- 攻撃対象領域（外部のインターフェースを含む）を限定すること（付属書I、パートI、第2項 (j)）
- 攻撃緩和メカニズムを組み込み、セキュリティ・インシデントの影響を軽減すること（付属書I、パートI、第2項 (k)）
- 内部の活動（データ、サービス、または機能へのアクセスや修正など）を監視および記録することにより、セキュリティ関連の情報を提供すること。なお、ユーザーがオプトアウトできる仕組みを提供しなければならない（付属書I、パートI、第2項 (l)）
- すべてのデータおよび設定は、ユーザーによる要求に応じて、安全に削除または別の製品に移行できるようにすること（付属書I、パートI、第2項 (m)）

パートII脆弱性対応要件

セキュアな設計だけでは不十分です。CRAでは、脆弱性を管理および修正するための複数の要件が策定されています。製造業者は、それぞれの製品に含まれるすべての脆弱性およびコンポーネントを特定し、文書化する必要があります。これには、少なくとも製品の最上位レベルの依存関係が分類されたソフトウェア部品表（Software Bill of Materials：SBOM）を、最新かつ機械で読み取り可能な状態で保持することが含まれます（付属書I、パートII、第1項）さらに、製造業者は以下の要件を満たしている必要があります。

- セキュリティ・アップデートを提供することにより、遅滞なく脆弱性に対応し、修正すること（付属書I、パートII、第2項）
- 製品のセキュリティについて、効果的かつ定期的なテストおよびレビューを適用すること（付属書I、パートII、第3項）
- 修正された脆弱性に関する情報を共有し、公開すること（付属書I、パートII、第4項）
- 協調的脆弱性開示に関するポリシーを導入し、実施すること（付属書I、パートII、第5項）
- 発見された脆弱性を報告するための連絡先を提供すること（付属書I、パートII、第6項）
- 脆弱性が適時に修正または軽減されるように、アップデートを安全に配布する仕組みを実装すること（付属書I、パートII、第7項）
- セキュリティ・アップデートを遅滞なく、無償にて、ユーザーに関連情報を提供するアドバイザリ・メッセージとともに配布すること（付属書I、パートII、第8項）

これらの脆弱性対応措置は、製品のサポート期間およびそれ以降にわたる協調的取り組みを通じて、製品が最初のリリース時以降も確実に保護され、適合性を維持できるようにすることを目的としています。

主な義務（第13条および第14条）

製品の設計、開発、製造、保守に関するサイバーセキュリティ要件に加えて、CRAには、製造業者に課される複数の主な義務が記載されています（一部の義務は、サプライ・チェーン全体における責任当事者に適用されます。ただし、この文書では、製造業者の責任のみに焦点を当てています）。これらの責任は、第13条の「製造業者の義務」と第14条の「製造業者の報告義務」で定義されています。
これらには、製品が付属書I、パートIおよびパートIIに定める必須サイバーセキュリティ要件を満たすようにするために遵守しなければならない、具体的な手順が記載されています。

CRA第13条：製造業者の義務

第13条は、製造業者の義務を規定しています。ここでは、製造業者の義務について、設計および開発、サポート期間、セキュリティ・アップデートの提供の3つの段階に分けて解説します。

設計および開発

最初の段階である設計および開発では、以下に示す一連の義務が規定されています。

- 製品は、付属書I、パートIに規定された必須サイバーセキュリティ要件に準拠して設計、開発、および製造されること。
- 製品に関連するサイバーセキュリティ・リスク評価を実施して文書化し、サポート期間中にアップデートを行うこと。
- サイバーセキュリティ・リスク評価は、製品の意図する目的、可能性のある使用、動作環境や資産の保護といった使用条件、およびサポート期間を考慮したものでなければなりません。サイバーセキュリティ・リスク評価は、付属書I、パートIおよびIIに規定された必須サイバーセキュリティ要件が当該製品に該当するかどうか、およびそれらの要件への実際の対応状況を示します。
- サイバーセキュリティ・リスク評価の結果は、必須サイバーセキュリティ要件の除外に該当する場合、その明確な根拠と併せて製品の技術文書に含める必要があります（第31条および付属書VII）。これらの結果は、製品の計画、設計、開発、製造、出荷、保守の各段階にわたって、決定および処置の指針となる必要があります。
- また、サード・パーティ製のコンポーネントを組み込む場合、製造業者は、それらのコンポーネントによって製品のセキュリティが損なわれることがないよう、デュー・デリジェンスを実施しなければならない点も重視する必要があります。この対象には、市販されていない無償およびオープンソースのソフトウェア・コンポーネントも含まれます。
- 製造業者は、第32条に基づいて、選択した適合性評価手順を実施するか、または実施済みでなければなりません。
- 製造業者は、付属書I、パートIおよびIIの必須サイバーセキュリティ要件に対する製品の適合性を示したうえで、第28条に従ってEU適合宣言書を作成し、第30条に従ってCEマーキングを貼付しなければなりません。

第13条第5項、第6項、第8項では、サード・パーティ製のコンポーネントを組み込む場合、それらのコンポーネントにより製品のセキュリティが損なわれることがないよう、製造業者はデュー・デリジェンスを実施しなければならない旨が定められています。この対象には、市販されていない無償およびオープンソースのソフトウェア・コンポーネントも含まれます。

サポート期間

以下では、次の段階であるサポート期間について説明します。

- 製品が市場に投入され、サポート期間が開始されると、製造業者はその期間中、付属書I、パートIIで規定されている必須サイバーセキュリティ要件に従って、製品の脆弱性に効果的に対応する義務を負います。
- 製造業者は、製品の予測される使用期間を反映してサポート期間を決定しなければなりません。この期間は、原則的に5年間以上とされています。サポート期間は、ユーザーの期待、製品の特性、製品の用途、他の製造業者によって市場に投入された類似機能を持つ製品のサポート期間、動作環境の可用性、製品に組み込まれて主な機能を提供するサード・パーティ製コンポーネントのサポート期間などを考慮して決定する必要があります。
- 製造業者は、付属書VIIに規定されている技術文書に、当該製品のサポート期間を決定した根拠となる情報を含めなければなりません。

- サポート期間は、製品が市場に投入されると同時に開始される点にご注意ください。サポート期間の終了日は、当該製品が最後に市場で販売された時点からさらに5年間とされています。そのため、たとえサポート期間が5年間となっていても、当該製品が市場で流通している限り、終了日は固定されません。事実上、サポート期間は、製品の最終バッチが販売された時点からカウントダウンされます。しかし、実際には、サポート期間は製品が寿命に達するまで、またはEU市場でお客様に最後に納品された日からさらに5年間は継続します。

- 重要なのは、サード・パーティから調達したものを含むすべてのコンポーネントについて、製造業者が脆弱性の識別、対応、および開示の全責任を負うという点です。サード・パーティ製コンポーネントの脆弱性が修復された場合、製造業者は、関連文書またはコードをコンポーネントの保守者と共有する必要があります。

- 第13条では、認識したあらゆる脆弱性やサード・パーティによって提供されたあらゆる関連情報を含め、製品のサイバーセキュリティに関する各種情報を製造業者が文書化することも要求されています。製造業者は、自社の製品のサイバーセキュリティ要素に関する包括的な記録を、各製品のリスクの性質に応じて作成された文書と併せて保持する必要があります。

- さらに、製造業者は、サード・パーティによって提出された脆弱性報告の受理、処理、および対応に関する適切なポリシーおよび手順を備える必要があります。これにより、継続的なセキュリティ強化をサポートする効果的なフィードバック・ループが生まれます。

- 製造業者は、市場監査当局の自由裁量に応じて、製品の投入から少なくとも10年間またはサポート期間のいずれか長い方の期間にわたって、技術文書およびEU適合宣言書を保存する必要があります。

- また、製造業者は、製品の市場投入から少なくとも10年間またはサポート期間のいずれか長い方の期間にわたって、ユーザーに提供した情報や指示（付属書II）をユーザーおよび市場監査当局が利用可能な状態で保管する必要があります。

- サポート期間中において、製品またはプロセスが付属書Iに定める必須サイバーセキュリティ要件に適合していないことを製造業者が認識した場合には、直ちに是正措置を講じるか、製品の回収またはリコールを行う必要があります。

- 製造業者は、市場監査当局の要請があれば、特定の製品カテゴリに対する（特に無償およびオープンソースのソフトウェア・コンポーネントについての）ソフトウェアの依存関係をEU全体で評価するために、SBOMを提出する必要があります。

製品のサポート期間は、製品が**市場に投入**された時点から始まります。

期間の終了は、当該製品がEU域内で最後に販売または納品された日に基づき、その日から5年間となります。

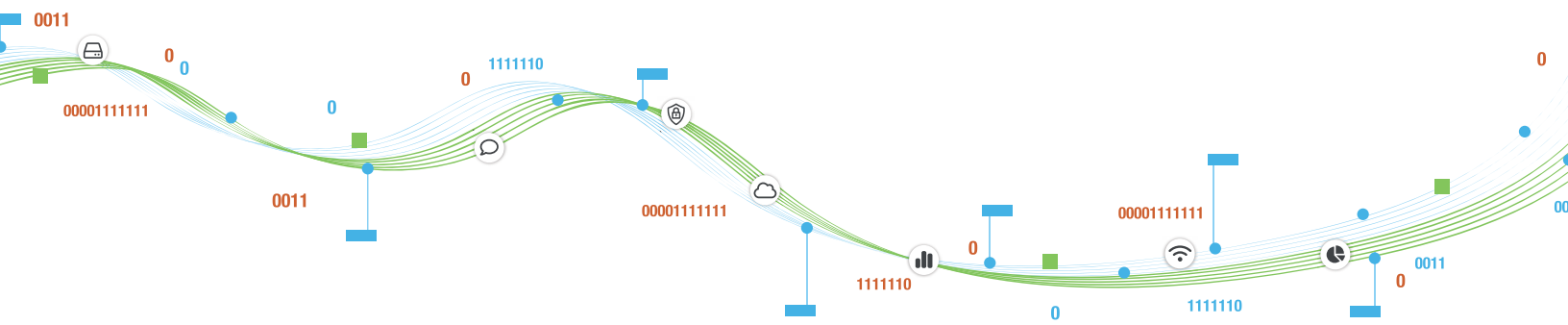
この5年間とは、製品が市場から撤退してからの期間をいい、サポート期間は販売や納品が継続している限り継続します。そのため、終了日は固定されていません。

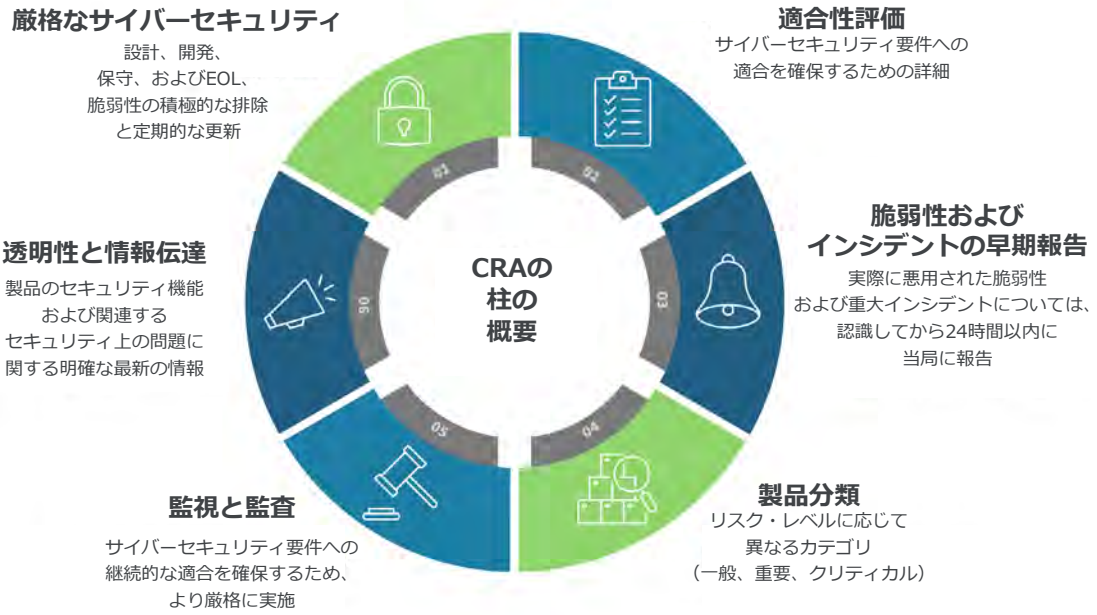
セキュリティ・アップデートの可用性

最後に、セキュリティ・アップデートの可用性について説明します。

- 製造業者は、サポート期間中にユーザーに提供された、付属書I、パートII、第8項に定められた各アップデートを、製品のリリースから10年間または残りのサポート期間のいずれか長い方の期間にわたって、ユーザーが引き続き利用できるようにする必要があります。

- 従来のバージョンのユーザーが、無償で追加の費用なく最新のバージョンにアクセスできる場合、製造業者が付属書I、パートII、第2項に定められた必須サイバーセキュリティ要件に準拠する義務を負うのは、最新のリリース済みバージョンについてのみです。





製造業者の報告義務（第14条）

製造業者は、実際に悪用された脆弱性や重大インシデントについて、**認識してから24時間以内**に報告する必要があります。実際に悪用された脆弱性とは、悪意ある攻撃者によってシステムを危殆化する目的で悪用されていることが、信頼できる証拠に基づいて判断された、既知の脆弱性をいいます。重大インシデントとは、製品、ユーザー、または接続されたシステムに深刻な影響を及ぼす可能性がある事象をいい、停止、侵入、データ漏洩などが含まれます。

どちらの場合も、各加盟国においてコーディネーターとして指定されたENISAおよびCSIRTに対して、同時に早期警告通知を行う必要があります。この通知では、製品が販売されている加盟国を明示する必要があります。重大インシデントの場合には、少なくとも、違法または悪意のある行為が原因として疑われるかどうかも含める必要があります。当該通知は、ENISAによって確立されたプラットフォームを介して提出されます（第16条）。

また、製造業者は、以下の内容を含む通知を72時間以内に発行することが義務付けられています。

- 脆弱性またはインシデントに関する一般情報
- 問題の修復または是正のために取られた処置
- 影響を軽減するためにユーザーができること
- インシデントの初期評価
- 報告された情報の機微性や秘匿性に関する、製造業者による評価

最後に、製造業者は、実際に悪用された脆弱性と重大インシデントの両方の最終報告を提出する必要があります。

実際に悪用された脆弱性の場合、是正または軽減措置が取られてから14日以内に最終報告を提出する必要があります。これには、少なくとも以下の内容が含まれていなければなりません。

- その重大度と結果を含む、脆弱性に関する説明
- 脆弱性を悪用した、または現在も悪用している、悪意ある攻撃者に関する情報
- セキュリティ・アップデートまたはその他の利用可能な是正措置に関する詳細

重大インシデントについては、インシデントに関する72時間以内の通知が行われてから1か月以内に最終報告を提出する必要があります。これには、少なくとも以下の内容が含まれていなければなりません。

- その重大度と影響を含む、インシデントに関する詳細な説明
- インシデントを発生させたと考えられる脅威または根本原因の種類
- 適用済みおよび進行中の軽減措置

適合性および製品ライフサイクルに関する重要事項

EU市場におけるすべての対象製品は、CRAの報告義務に準拠している必要があります。これには、2027年12月11日よりも前に市販された製品も含まれます。これらの要件は、CEマークが貼付されたすべての製品のライフサイクル全体に適用されます。

したがって、開発チームは、自社の製品の潜在的な脆弱性を継続的に監視および分析し、それらを適切に文書化して、ENISAおよびCSIRTに報告する必要があります。識別されたすべての脆弱性について、開発者はパッチを作成または入手し、それらを適切なタイミングで適用する必要があります。すなわち、製造業者は、接続可能なすべてのデバイスへのアクセスおよびアップデートを製品のライフサイクル全体にわたって可能にする機能を統合し、適合性を維持する必要があります。

Digiのソリューションによるこれらの要件への対応については、**13ページの「Digiによる、CRA準拠のためのエンド・ツー・エンドのサポート」**を参照してください。

技術文書要件

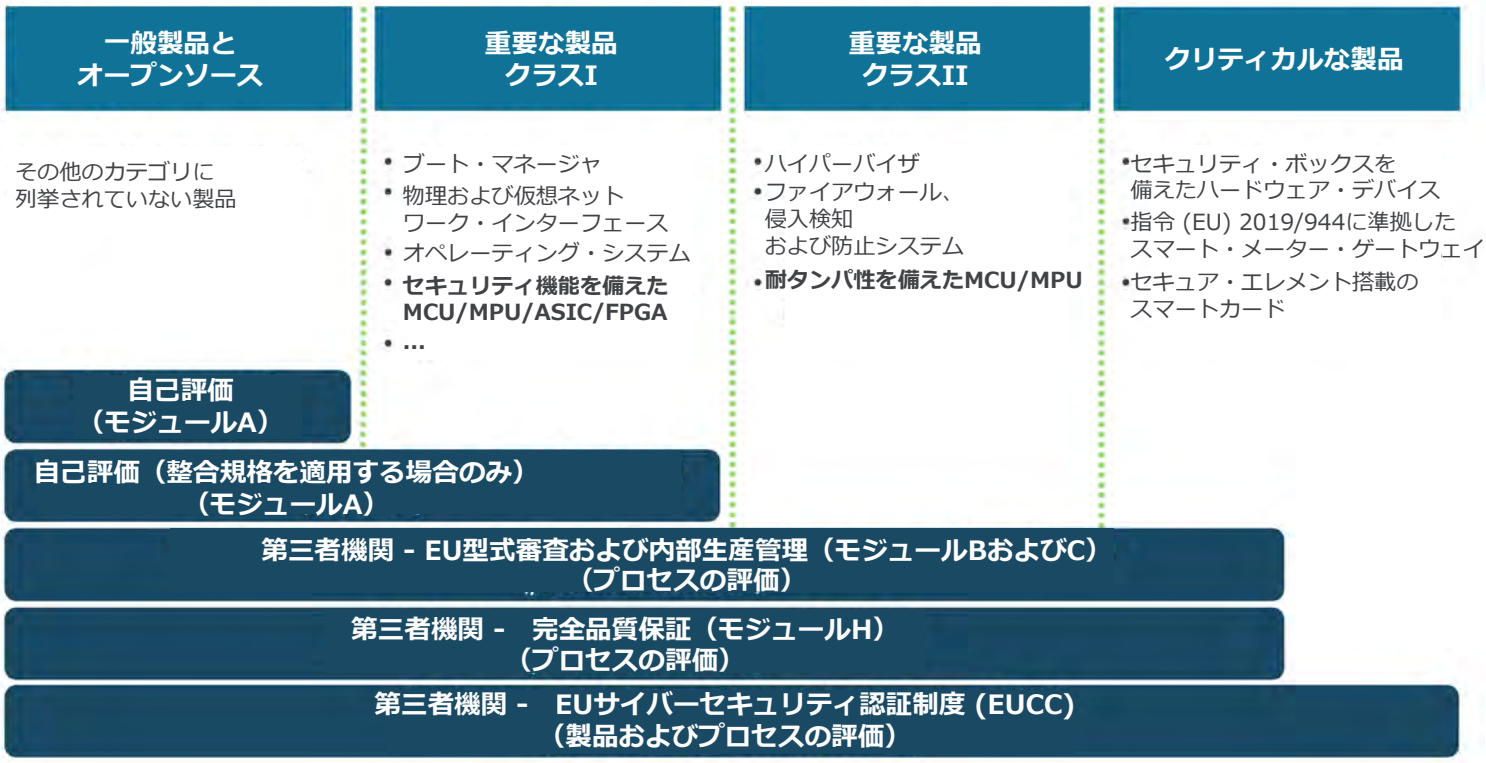
CRAの第31条で言及され、かつ付属書VIIに記載されているとおり、製造業者は以下の内容を含む文書を保管することが義務付けられています。

- 製品に関する一般的な説明（用途、ソフトウェア・バージョンに関する情報、外観の特長やマーキングならびに内部レイアウトを示す写真、および付属書IIに列挙されたユーザーへの情報および指示を含む）
- 設計、開発、製造、および脆弱性対応プロセスに関する詳細
- 製品の設計および開発に関する情報：図面/回路図およびシステム・アーキテクチャの説明（ソフトウェア・コンポーネントの相互運用と全体の処理への統合について説明するもの）
- 脆弱性対応プロセスの仕様（ソフトウェア部品表、協調的脆弱性開示ポリシー、脆弱性通知の連絡先、およびアップデートの安全な配布のために選択されたソリューションの説明を含む）
- 製造および監視プロセスに関する情報、および当該プロセスの検証
- 第13条に記載されているサイバーセキュリティ・リスク評価（付属書I、パートIで定める必須サイバーセキュリティ要件がどのように該当するのかを含む）
- 第13条第8項に準拠した、製造業者による製品のサポート期間の決定に関する情報
- 製品に完全または部分的に適用される、EUで発行された整合規格（サイバーセキュリティ認証制度および共通仕様を含む）
- 製品および脆弱性対応プロセスについて、該当する必須サイバーセキュリティ要件との適合性を確認するために実施されたテストのレポート
- 市場監査当局による要請があれば、製品のEU適合宣言書およびSBOM（該当する場合）のコピー

技術文書要件には、製品の説明、脆弱性プロセス、リスク評価、SBOMなどが含まれ、市場監査当局の自由裁量に応じて、文書は最低10年間保管されます。



製品カテゴリおよび適合性評価手順



適合性評価手順（第32条）

第32条に従って、CRAの対象範囲内のすべての製品は、付属書Iに記載された必須サイバーセキュリティ要件への適合を示すために、適合性評価を受ける必要があります。製造業者は、CRAの確立された適合性評価手順のうち少なくとも1つの手順を実施する必要があります。これには、製品に加えられた変更、整合規格の更新、サイバーセキュリティ認証の改訂などに関する説明も含まれます。

この評価の種類および適用範囲は、製品の分類によって異なります。現時点では、製品カテゴリについて提供されている情報はまだ完全なものではありません。第7条第4項によれば、欧州議会は2025年12月11日までに、付属書IIIに定める重要な製品のクラスIおよびII、ならびに付属書IVに列挙されているクリティカルな製品のカテゴリの技術的説明を定義する、実装法令を採択することになっています。この法令の**ドラフト**が現在策定されています。

一般

製品が重要またはクリティカルのどちらのカテゴリにも該当しない場合、製造業者は内部で適合性評価を実施することができます。対象製品の大半がこのカテゴリに属します。また、商用製品に関連する無償およびオープンソースのソフトウェアもこのカテゴリに該当します。

サービスは、製品の機能に不可欠なものでない限り、CRAの適用除外となる点にご留意ください。

重要な製品、クラスI

製造業者は、整合規格、共通仕様、または欧州サイバーセキュリティ認証制度を適用する場合に限り、内部評価を実施することができます。クラスIの製品の例には、パスワード・マネージャ、仮想プライベート・ネットワーク（Virtual Private Network：VPN）機能を有する製品、ネットワーク管理システム、スマートホーム向け汎用バーチャル・アシスタントなどが含まれます。

重要な製品、クラスII

クラスIIの製品では、必ず第三者機関による適合性評価が必要です。該当製品には、ハイパーバイザ、耐タンパ性を備えたマイクロプロセッサなどが含まれます。

クリティカル

クリティカルな製品では、規則 (EU) 2019/881の2019 EUサイバーセキュリティ法に準拠した欧州サイバーセキュリティ認証を取得するか、クラスIIの製品の場合と同様の適合性評価プロセスに従う必要があります。

製造業者は、自社製品の適合性評価を実施したうえで、製品が販売される加盟国の言語で適合宣言書を作成する必要があります。その後、製品、パッケージ、付属文書、およびウェブサイトにCEマーキングを表示できます。

準拠に向けた連携

CRAは、EUにおける製品適合性のあり方を大きく変えるものです。CRAおよびその複雑な要件への対応は、インターネット接続される可能性のあるセキュアな製品をOEMがEU市場で販売する際に直面する最も大きな課題の1つと言えます。

NXPの高度でセキュアなプロセッサとDigiの包括的ソリューションを組み合わせることで、OEMのCRA準拠を支援するセキュリティ・ビルディング・ブロックがもたらされます。

NXPとDigiの連携 — 次世代のプロセッサおおよびSOMソリューションを構築

Digi Internationalは、NXP Semiconductorsのような製造業者との連携を通じて、高度なプロセッサやセキュリティ手法を活用したビルディング・ブロックを開発者に提供しています。それにより、CRAおよびその他の規則の要件を満たすセキュア・バイ・デザイン製品を構築できるよう、OEMをサポートしています。

NXPのセキュリティ態勢：CRA対応

NXPのEdgeLock® Assuranceプログラムは、企業による成熟したセキュリティ態勢に対応するために、NXPによって生み出されました。このプログラムは、お客様がセキュリティ基準および規則を満たすための基礎となり、製品開発者によるセキュリティ・プロセスをサポートするとともに、製品にセキュリティ機能をもたらします。

このプログラムには、セキュアな開発に向けた業界のベスト・プラクティスの実施、物理的および論理的セキュリティに対応する堅牢な企業文化の確立、ならびに継続的な従業員研修が含まれます。セキュアな製品開発プロセスは、このプログラムに不可欠なものであり、ISO 21434、IEC 62443-4-1、IEC 80001-5-1といった業界標準に対して外部第三者機関による認証を取得しています。

セキュリティ機能を備えたNXP製品は、開発プロセス中に社内の脆弱性分析ラボのエキスパート・グループによって実証がなされており、最も一般的なリスクへの耐性が強化されています。さらに、NXPでは、セキュリティの保証が独立第三者機関によって裏付けられるようにしており、SESIP (EN 17927) やコモン・クライテリア (ISO 15408) などの業界標準に厳密に準拠することで、NXPのコンポーネントに最高水準の保証とレジリエンスを確保しています。独立した第三者機関が、NXP製品のセキュリティに関する言明、特定の潜在的な攻撃に対するセキュリティの実装の堅牢性、ならびに公知の脆弱性への対応について検証を行うことで、それぞれのリスク・レベルに応じた最先端のセキュリティが実現します。

スケーラブルなセキュリティ・アーキテクチャとCRA要件のマッピング

CRAへの準拠をさらに促進するために、NXP製品のセキュリティ機能をCRAの必須サイバーセキュリティ要件（製品の構成、認証、アクセス制御、データ保護、監視、脆弱性管理、インシデントへの対応など）にマッピングすることができます。NXPのセキュリティ・ソリューションは、エントリレベルから高度なものまで幅広いセキュリティ機能を備えているため、OEMがリスク・レベルに応じて保護レベルを調整することを可能にします。EdgeLockセキュア・エンクレーブ、セキュア・エレメント、EdgeLock 2GOサービスなどの主要テクノロジは、堅牢な認証情報保護、ライフサイクル・セキュリティ管理、ターンキー・プロビジョニングを提供します。

CRA準拠のアプリケーションに向けたNXPのセキュリティ・ソリューション

セキュアで堅牢なシステムを構築するには、まず第一に、システム全体の土台が確実に信頼できるものでなければなりません。セキュリティ保護がハードウェアに組み込まれているシリコンは、本質的に信頼性が高く、攻撃を受けにくくなっています。シリコンは、その上で動作するすべてのソフトウェアの基盤および基礎となります。ソフトウェアは、ファームウェア、通信スタック、OS、およびその他のアプリケーションと同様に、改変および侵害される可能性があります。しかし、シリコンは簡単には侵害されません。シリコンは、システムの信頼の基点（Root of Trust：RoT）と呼ばれています。

可能性のある攻撃は極めて広範であることから、絶対的なセキュリティは存在しません。それに加えて、アプリケーションが複雑化し、攻撃対象領域が拡大しています。

結果として、Digiのようなソリューション・プロバイダを活用することが重要となります。Digiは、NXPのセキュアなプロセッサをDigi ConnectCore®システム・オン・モジュールに統合し、Digi ConnectCoreクラウド・サービスやDigi ConnectCoreセキュリティ・サービスといった包括的なセキュア・バイ・デザイン・ソリューションおよびビルディング・ブロックを提供しています。これにより、OEMはセキュアな最終製品を設計および供給できるようになるとともに、ソリューションのリモート・モニタリングおよび管理、CRAの要件への適合、さらには企業のビジネス・モデルに新たな収入源をもたらすことも可能になります。



Digiによる、CRA準拠のためのエンド・ツー・エンドのサポート

欧州に限らず世界中の企業が、CRAについて、および適合する製品を最初から設計する方法についての実用的で実行可能な指針を必要としています。

Digiは**サイバーセキュリティを極めて重視**しています。CRAについては、初めて発表されて以来準拠し続けており、セキュリティ分野での実績を活かし、自社のセキュリティ・ビルディング・ブロックをこの重要な規則の要件にマッピングしています。さらに、サービスについてもCRAの各局面に対応した独自のアプローチを取っており、実装に関する詳細なステップ・バイ・ステップ・ガイドを用意しています。

「Digiとの会話の中で、CRAに準拠するには具体的にどうすべきかを初めて耳にしました」と、あるお客様は言います。「別のベンダーが教えてくれたのは、この法律の一般的な概要のみでした」。

Digiの組込みソリューションとサービスは、お客様がCRAの要件および義務を遵守できるようにすることを意図して設計されています。また。Digiはお客様と連携し、お客様の特定のニーズに応じたサービス・パッケージを提供します。

Digiによる、準拠重視のエコシステム

Digiは、**フル・スイート**のクラウド・ツー・コネクティビティ・サービスを提供しており、これには**Digi ConnectCoreシステム・オン・モジュール** (SOM)、ソフトウェアとツール、ならびにセキュリティが組み込まれた統合エコシステムを形成する**Digi ConnectCoreセキュリティ・サービス**と**Digi ConnectCoreクラウド・サービス**が含まれます。Digiのソリューションは、積極的な脆弱性管理、セキュアなソフトウェア・アップデート、およびリモートでの設定、監視、保守機能を備え、規格に準拠したセキュア・バイ・デザインのデジタル製品の開発を促進します。

OEMは、Digiの包括的なエコシステムにより、製品のライフサイクル全体にわたり自信を持ってCRAへの適合を維持できるとともに、複雑さを軽減し、市場投入までの期間を短縮することができます。Digiの統合アプローチは、現行の要件への対応に役立つだけではなく、企業が将来の法規制の改正にシームレスに適応できるようにします。

Digiでは、特別に設計されたポートフォリオやサービスと並行して、**エンジニアがCRAの困難を克服する方法**に関する1時間のセミナーなど、いくつかの教育リソースも提供しています。



Digi TrustFence

ミッションクリティカルなアプリケーション向けに設計された**Digi TrustFence**®は、IoTデバイスに動的な適応型セキュリティを直接組み込むのに役立ちます。セキュア・ブート、セキュア・コンソール、セキュアなソフトウェア・アップデート、暗号化されたファイル・システム、保護されたハードウェアとピンなどの機能を通じて、セキュリティ・バイ・デザインとセキュアな構成の両方をサポートします。

TrustFenceは、Digiの**セルラー・ルータ**、**XBee® RFモジュールおよびセルラー・モデム**、**インフラ管理デバイス**、および**Digi ConnectCore SOM**に完全に統合されています。Digi Embedded Yocto (DEY) にもTrustFenceが組み込まれています。

Digi ConnectCoreセキュリティ・サービス

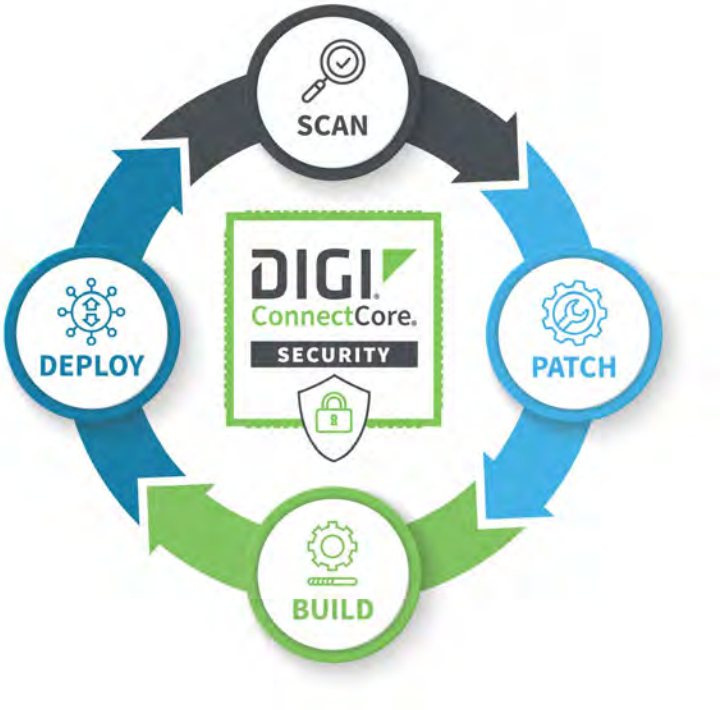
Digi ConnectCoreセキュリティ・サービスは幅広いツールを備えており、実際に悪用された脆弱性または重大インシデントについての24時間以内の報告義務など、企業がCRAの脆弱性管理および開示要件に対応するのに役立ちます。

これには、Digi ConnectCore SOMで動作してセキュリティの脆弱性に対応する、カスタムSBOMの継続的な分析および監視が含まれます。このサービスには、重大な問題の修復をサポートするために、キュレートされた脆弱性レポート、共通脆弱性を修復するパッチを備えたセキュリティ・ソフトウェア・レイヤ、さらにはエキスパートによる相談およびサポート・サービスが備わっています。

Digi ConnectCoreクラウド・サービス

Digi ConnectCoreクラウド・サービスはDigi Remote Manager® (Digi RM) プラットフォームをベースとしており、製造業者が自社のデバイスを最新に保つのに役立つとともに、広範なプロセス・オートメーション、監視、およびリモート・デバイス管理を提供します。

ConnectCoreクラウド・サービスは、実績のある商用ハードウェアとDigiの業界最先端の知識や経験を組み合わせて、多数のファームウェアおよびソフトウェアの自動化されたアップデート、双方向の通信、リアルタイム警告、デバイスの状態やネットワークの健全性に関する詳細な報告などを通じて、規格への適合性と優れた品質や使いやすさを兼ね備えたコネクテッド・デバイスを開発できるようOEMを後押しします。





Digiワイヤレス・デザイン・サービス

Digiの組込みソリューションの使用中にエンジニアリング・サポートが必要となった場合、Digiのワイヤレス・デザイン・サービス (WDS) チームがお手伝いします。WDSは、製品の設計および構築サービス、認証、ソフトウェア開発、迅速な市場投入のサポート、製品の適合性を維持するための継続的な関わりなど、あらゆるプロセスにおいて貴社の開発チームをサポートします。

このチームは、ボードの再設計や製品のレスキューを含む製品開発のあらゆる側面に精通した有能なエンジニアとプロジェクト・マネージャで構成され、エンジニアリング、テスト、および製造支援のための完全装備されたラボを有しています。

Digi Embedded Yocto (DEY)

Yocto Project™をベースとしたオープンソースのLinuxディストリビューションであるDigi Embedded Yocto (DEY) は、DigiのSOM専用に設計されています。DEYは、Digiによるソフトウェア保守、堅牢なパッチ・ポリシーに加え、Digi TrustFenceおよびDigi ConnectCoreセキュリティ/クラウド・サービスとの完全な統合により、組込み開発者がCRAの適合性要件を満たすのに役立ちます。

Digiは、自動化された脆弱性スキャン、セキュアなリモート・アップデート、製品ライフサイクル全体を通じた専門家によるコンサルティングなど、CRA準拠のための包括的なサポートを提供しています。

CRAへの準拠：Digiセキュリティ・ビルディング・ブロックの活用

Digi ConnectCoreソリューションがCRAの要件を満たすのにどのように役立つかを具体的に説明します。

パートI：製品関連のサイバーセキュリティ要件

次ページの表に、付属書I、パートIに準拠した製品特性に関する14のサイバーセキュリティ要件を示しています。ここではそれぞれの要件を、Digi TrustFence、Digi ConnectCoreセキュリティ・サービス、Digi ConnectCoreクラウド・サービス、そしてDEYオペレーティング・システムにマッピングしています。いくつかの要件について、詳しく見てみましょう。

- **付属書I、パートI、第2項 (a)。**製品は、悪用可能な既知の脆弱性がない状態で出荷しなければなりません。Digi ConnectCoreセキュリティ・サービスは、カスタム・ソフトウェア部品表 (SBOM) スキャンにより、共通脆弱性識別子 (CVE) の優先順位付けを効率化することで、誤検出を排除し、OEMが最も重要な問題への対応に集中できるようにします。加えて、OEMは、DEY、ボード・サポート・パッケージ (BSP)、Linuxカーネルおよびブートローダ向けの統合済みセキュリティ・パッチ一式が含まれたメタDigiセキュリティ・レイヤを活用することもできます。
- **付属書I、パートI、第2項 (c)。**脆弱性は、Digi TrustFenceやDigi ConnectCoreクラウド・サービスに含まれるセキュア・ソフトウェア・アップデート機能を利用して、安全かつ確実にパッチを適用し、Over-the-Air (OTA).によりリモートで修復することができます。

徹底的かつ注意深い評価を通して、OEMのお客様が自信を持ってCRAに準拠するために利用可能なDigiのソフトウェア、ツール、機能、手順を特定することで、市場投入までの期間を短縮し、さらに重要なこととして、製品ライフサイクル全体にわたり適合性を維持できるようになります。

要件の中には、Digiのセキュリティ・ビルディング・ブロックは対象外であっても、ConnectCoreベースの最終製品は対象となるものがあります。たとえば、Digi ConnectCore SOMを使用してアプリケーションを構築したOEMは、最終製品でCRA要件を満たさなければなりません。実際、OEMのお客様の最終製品には潜在的に脆弱なハードウェアやソフトウェアが備わっていることから、CRA準拠において何を行うべきかを慎重に検討する必要があります。

パートII脆弱性対応要件

最後の表には、付属書I、パートIIで規定された8つの脆弱性対応要件を示しています。パートIと同じアプローチに従い、細部にわたってそれぞれの要件をDigiのセキュリティ・ビルディング・ブロックにマッピングしています。いくつかの要件について掘り下げてみましょう。

- **付属書I、パートII、第1項。**実績のあるDigiの手法は、DEYおよびDigi ConnectCoreセキュリティ・サービスとともに、少なくとも最上位レベルの依存関係を網羅するカスタムSBOMを作成することにより、製造業者が製品に含まれる脆弱性およびコンポーネントの識別や文書化を容易に行えるようにします。
- **付属書I、パートII、第7項。**Digi TrustFenceとDigi ConnectCoreクラウド・サービスもまた、脆弱性が必ず適時に（セキュリティ・アップデートに該当する場合は自動で）修正または軽減されるように、製品のアップデートをセキュアに配布する仕組みを提供します。Digiのクラウド・サービスは、TLS (Transport Layer Security)、証明書ベースの認証、および暗号化をサポートする、セキュアなエッジ・ツー・クラウド通信を確保します。加えて、テンプレート機能により、所定の設定に従ってOEMのデバイス・フリートを自動でスキャン、アップデート、および管理することができます。テンプレートを利用することで、OEMのお客様は設定の更新が必要な際に、時間の短縮、エラーの削減、労力の最小化、対応規模の調整を実現できると同時に、設置されたすべてのデバイスにわたる一貫性と標準化を確保することができます。

ここでのレビューの対象範囲は、Digi ConnectCoreに絞られています。DigiのSOMベースの製品を設計するOEMのお客様は、付加価値の高いDigiソリューションの利点を享受できますが、CRAの要件や義務への適合、製品発売までのマイルストーン、または既存製品の販売の継続などについては、一定の労力を費やす必要があります。

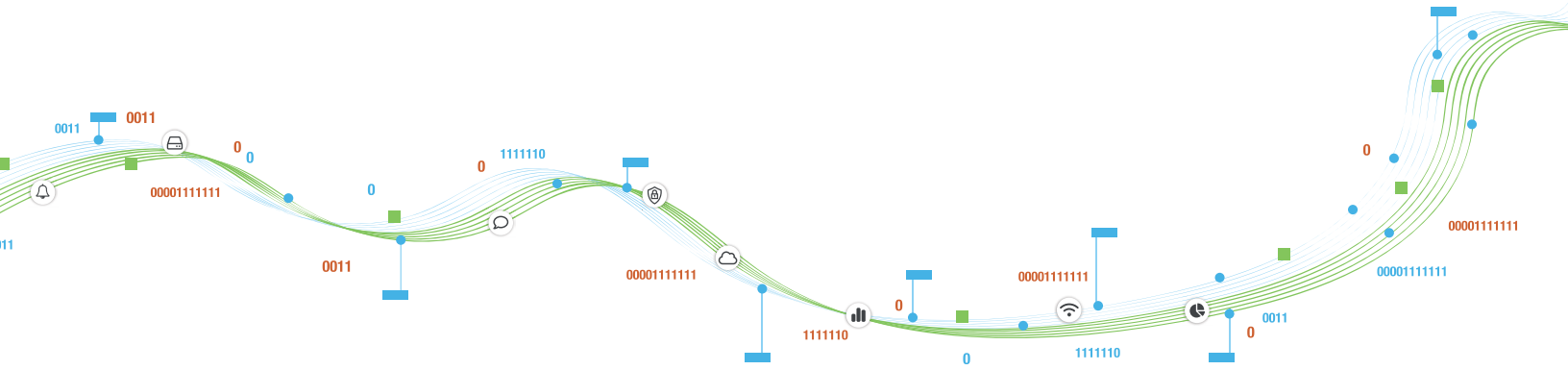
Digiでは、お客様がこれらの要件および特定のプロジェクトでのDigiセキュリティ・ビルディング・ブロックの実装方法についての理解を深めることができるよう、営業担当者との打ち合わせを手配させていただきます。

CRAへの準拠：Digiセキュリティ・ビルディング・ブロックの活用 (I)

パートI	内容	Digi TrustFence	Digi ConnectCore セキュリティ・サービス	Digi ConnectCore クラウド・サービス	Digi Embedded Yocto
(1)	製品は、リスクに応じた適切なレベルのサイバーセキュリティを確保したうえで、設計、開発、および製造しなければならない	TrustFence全体	セキュリティ・サービス全体	クラウド・サービス全体	DEY全体
(2) (a)	製品は、悪用可能な既知の脆弱性がない状態で市場に投入されなければならない	該当なし	カスタムSBOMスキャン、メタDigiセキュリティ	Digi RM脆弱性パッチ・ポリシー	Digiによるソフトウェア保守
(2) (b)	製品は、セキュア・バイ・デフォルトの構成で市販されなければならない	TrustFence全体	該当なし	該当なし	強化されたDEY
(2) (c)	製品は、セキュリティ・アップデートを通じて確実に脆弱性に対応できるようにしなければならない	セキュア・ソフトウェア・アップデート	メタDigiセキュリティ、相談とサポート	セキュアなリモートOTAソフトウェア・アップデート	セキュア・ソフトウェア・アップデート、デュアル・ブート構成
(2) (d)	製品は、不正アクセスから確実に保護されなければならない	セキュア・コンソール、セキュアJTAG	該当なし	該当なし	SSH/TLS
(2) (e)	製品は、保存、伝送、または他の方法で処理された個人またはその他のデータの秘匿性が保護されていなければならない	暗号化されたファイル・システム / ファイル（ハードウェアによる制限）	該当なし	ファイル・システムへのアクセス、TLS、証明書ベースの認証および暗号化	暗号化、WPA3、FIPS 140-2/3（追加料金）
(2) (f)	製品は、保存、伝送、または他の方法で処理された個人またはその他のデータ、コマンド、プログラム、設定の完全性が保護されていなければならない	セキュア・ブート / 認証されたファイル・システム	該当なし	ファイル・システムへのアクセス、TLS、証明書ベースの認証および暗号化	TLS、読み取り専用のファイル・システム
(2) (g)	製品は、適切で関連性があり必要なものに限定された個人またはその他のデータのみを処理するものでなければならない	該当なし	該当なし	カスタム・データ・ストリーム	該当なし
(2) (h)	製品は、DoS (Denial-of-Service) 攻撃に対して必要不可欠かつ基本的な機能の可用性を保護するものでなければならない	該当なし	該当なし	該当なし	組込みシステム・セキュリティのベスト・プラクティス
(2) (i)	製品は、製品自体または接続されたデバイスが他のデバイスまたはネットワークによって提供されるサービスの可用性に及ぼす悪影響を、最小限に抑えるものでなければならない	該当なし	該当なし	該当なし	組込みシステム・セキュリティのベスト・プラクティス
(2) (j)	製品は、外部インターフェースを含む攻撃対象領域を限定するように設計、開発、および製造されていなければならない	セキュア・ブート、セキュア・コンソール、セキュアJTAG、改ざん検知	メタDigiセキュリティ、相談とサポート	該当なし	該当なし
(2) (k)	製品は、適切な攻撃緩和メカニズムおよび技術を用いて、インシデントの影響を低減するように設計、開発、および製造されていなければならない	改ざん検知	該当なし	テンプレート	該当なし
(2) (l)	製品は、関連する内部活動を監視および記録することにより、セキュリティ関連情報が提供されなければならない	改ざん検知	該当なし	セキュリティ監視エージェント	該当なし
(2) (m)	製品は、ユーザーがすべてのデータおよび設定を安全かつ容易に永久的に削除できるものでなければならず、当該データが他の製品またはシステムに転送される可能性がある場合、これを確実に安全な方法で実施する必要がある	該当なし	該当なし	ファイル・システムへのアクセス、Digi RMデータ/設定管理	該当なし

CRAへの準拠：Digiセキュリティ・ビルディング・ブロックの活用 (II)

パートI	内容	Digi TrustFence	Digi ConnectCore セキュリティ・サービス	Digi ConnectCore クラウド・サービス	Digi Embedded Yocto
(1)	製造業者は、機械で読み取り可能かつ一般的に使用される形式で、ソフトウェア部品表 (BOM) を作成しなければならない	該当なし	カスタムSBOMの作成	該当なし	DEY SBOM
(2)	製造業者は、遅延なく脆弱性に対応し、修復しなければならない	該当なし	メタDigiセキュリティ、相談とサポート	セキュア・リモートOTAソフトウェア・アップデート、テンプレート	DEY定期リリース
(3)	製造業者は、製品のセキュリティについて効果的かつ定期的なテストとレビューを適用しなければならない	該当なし	カスタムSBOMスキャン	Digi RM脆弱性パッチ・ポリシー	DEYパッチ・ポリシー
(4)	製造業者は、修復された脆弱性に関する情報を共有し、公開しなければならない	該当なし	セキュリティ・サービス全体	Digiセキュリティ・センター	Digiセキュリティ・センター
(5)	製造業者は、協調的脆弱性開示に関するポリシーを導入し、実施しなければならない	該当なし	該当なし	Digi RM脆弱性パッチ・ポリシー、Digiセキュリティ・センター	DEYパッチ・ポリシー、Digi Embedded GitHub、Digiセキュリティ・センター
(6)	製造業者は、発見された脆弱性を報告するための連絡先の提供を含め、潜在的な脆弱性に関する情報の共有を促進しなければならない	該当なし	該当なし	Digiセキュリティ・フォーム	Digiセキュリティ・フォーム
(7)	製造業者は、脆弱性が必ず適時に修正または軽減されるように、アップデートをセキュアに配布する仕組みを提供しなければならない	セキュア・ソフトウェア・アップデート	該当なし	セキュア・リモートOTAソフトウェア・アップデート、テンプレート、TLS、証明書ベースの認証および暗号化	該当なし
(8)	製造業者は、セキュリティ・アップデートが利用可能である場合には、遅滞なく、ユーザーに潜在的措置などの関連情報を提供するアドバイザリ・メッセージとともに、無償で配布しなければならない	該当なし	該当なし	セキュア・リモートOTAソフトウェア・アップデート、テンプレート	DEYパッチ・ポリシー、Digi Embedded GitHub





Digiエコシステム：CRA準拠の統合

Digiのポートフォリオの強みの1つは、CRA準拠へのアプローチを統合していることです。Digiのソリューションは、セキュア・バイ・デザインであり、Digi TrustFence、Digi ConnectCoreセキュリティ・サービス、Digi ConnectCoreクラウド・サービス、およびDigi Embedded Yocto (DEY)によってサポートされています。これらは、最初からセキュリティが組み込まれた統合ハードウェアおよびソフトウェアを形成します。

Digiのエコシステムは、以下に示す主要なCRA要件を網羅しています。

- ✓ **SBOM管理：**ソフトウェア部品表 (BOM) を作成および管理するためのツール
- ✓ **脆弱性対応：**最初の製品リリース以降に生じた脆弱性の継続的スキャン
- ✓ **報告ツール：**重大な問題に焦点を当ててキュレートされた脆弱性報告を含む
- ✓ **脆弱性の修復：**共通脆弱性を修正するパッチを含むセキュリティ・ソフトウェア・レイヤ
- ✓ **セキュリティ・メンテナンス：**セキュアで信頼性の高いリモートOTAソフトウェア・アップデート
- ✓ **デバイス・フリート管理：**プロセス・オートメーション、監視、リモート・デバイス管理、コスト削減
- ✓ **エキスパートによるサポート：**パッチや修正の統合に関する相談およびサポート・サービス

DigiのSOM、ソフトウェア、ツール、サービスを含む包括的なエコシステムにより、OEMは自信を持ってこの規則への適合を加速させ、市場投入までの期間を短縮し、そして何よりも製品ライフサイクル全体を通じて適合性を維持できるようになります。この統合アプローチは、現行のCRA要件に対応するのみならず、企業が将来の法規制の変更にシームレスに適応できるようにします。

おわりに

CRAは、デジタル製品のあり方を抜本的に変革するものです。この規則は、サイバーセキュリティを製品の設計およびライフタイム管理の基盤となる確固たる要素として確立しています。

CRAは欧州で策定された規則ですが、その影響は既に世界中に広がっています。その原則に今すぐ対応することで、企業は他の地域で新たに採用され得る規制に対応できるようになります。これにより、規則への準拠はもはや単なる困難な課題ではなく、持続可能な成長や市場における長期的なリーダーシップをもたらす機会ともなります。

CRAへの準拠に向けて戦略的に取り組む企業は、法規制の遵守のその先にある好機を見出すことが可能になります。製造業者は、概念から開発、製造、展開、保守まで、製品ライフサイクル全体にわたりセキュリティを組込みことで、顧客との深い信頼関係を構築しながら、高い代償を伴うセキュリティ・インシデントを減らし、さらには長年にわたって使用可能なより強靭な製品を開発できるようになります。

1時間無料のDigiセキュリティ相談をリクエスト



Digiが選ばれる理由

Digiは、ミッションクリティカルな通信機器から設計および実装サービスまで、お客様のプロジェクトのあらゆる側面をサポートする包括的なIoTソリューション・プロバイダであり、お客様のアプリケーションを設計、インストール、テストし、セキュアかつ確実に最高のパフォーマンスで機能させます。

Digiでは、高い信頼性、優れたパフォーマンス、セキュリティ、スケーラビリティ、多機能性を実現する製品を構築しています。それによりお客様は、長期にわたる製品寿命を想定し、進化するシステム要件に迅速に適応し、さらには将来新たに出現するテクノロジをすぐに導入できるようになります。Digiの組込みモジュール、ルーター、ゲートウェイ、およびインフラ管理ソリューションは、一般企業から輸送、エネルギー、インダストリアル、スマートシティまで、業界をまたいだ最新のコネクテッド・アプリケーションをサポートします。

Digiのソリューションは、標準ベースおよび独自設計の各種機器、デバイス、センサへのコネクティビティを実現し、事実上あらゆる形態のワイヤレスまたは有線システムを介して信頼性の高い通信を実現します。Digiの統合リモート管理プラットフォームは、実装を加速するのに役立つとともに、マス・コンフィグレーションやファームウェア・アップデートといったミッションクリティカルな機能に適した効率の高いネットワーク運用、ならびにダッシュボード、アラーム、パフォーマンス指標によるシステム全体の監視を活用して、最適なセキュリティを提供します。

会社沿革

- Digiは、1985年の設立以来、デバイス、自動車、機器、資産などの「IoT (Internet of Things)」向けにコネクティビティを提供しています。
- DigiはNASDAQに上場しています（ティッカー・シンボル：DGII）。
- Digiは、ミネソタ州のツイン・シティーズに本社を置き、世界全体で800名を超える従業員を擁しており、これまでに1億を超えるデバイスの接続を実現してきました。

Digiは、IoTソリューション・プロバイダとして、実績のあるテクノロジをお客様のために活用し、お客様がネットワークに光を当てて、新たな製品を投入できるよう支援します。卓越した信頼性、セキュリティ、スケーラビリティを備え、適切に管理されたマシン・コネクティビティを、最も必要としているお客様へお届けすることが、Digiの使命です。

次のステップ

- Digiのエキスパートに相談：**お問い合わせ**
- Digiからの情報提供を希望：**ニュースレターへの登録**
- Digiのソリューションを今すぐ購入：**購入方法**

Digiのエキスパートに連絡し、今すぐ始めましょう。

電話： 877-912-3444
www.digi.com

Digi International Worldwide Headquarters
9350 Excelsior Blvd. Suite 700
Hopkins, MN 55343

/digi.international　@DigiDotCom　/digi-international

© 2025 Digi International Inc. All rights reserved. 91004734 A6/725

弊社では正確かつ完全な最新の情報を提供するよう最善を尽くしておりますが、すべての情報は「現状有姿」で提供されており、いかなる保証もいたしません。
弊社は、本情報の利用について一切の責任を負いません。すべての登録商標および商標は、それぞれの所有者に帰属します。