注意: この日本語版文書は参考資料としてご利用ください。
最新情報は必ずオリジナルの英語版をご参照願います。

MICROCHIP

AN3983

ISA/IEC 62443 とセキュア エレメントの詳細解説

はじめに

著者: Security Pattern社Matteo Giaconia氏、Microchip社Xavier Bignalet

本書は、ISA/IEC 62443 に準拠した製品を開発する際の構成要素として Microchip 社のセキュア エレメント デバイスを効果的に使う方法について説明します。

対象読者は、ISA/IEC 62443 互換または認証済み製品を提供する必要があるエンジニアとマネージャです。

本書で詳述する通り、ISA/IEC 62443 の分野では、Microchip 社のコンポーネント ATECC608 と TA100 は、同規格(特に包括的な ISA/IEC 62443 規格の一部である 62443-4-2「IACS(産業用オートメーションおよび制御システム) コンポーネントの技術的セキュリティ要件」)に基づく IACS 製品の準拠および認証取得を達成する際の技術的な実現手段として認められています。

目次

1. ISA/IEC 62443 について

ISA/IEC 62443 は、2007 年に ISA(国際自動制御学会)の IACS セキュリティ委員会(ISA99)の提案から始まり、後に IEC(国際電気標準会議)によって策定された、計約 800 ページにわたる一連の規格、技術仕様、技術報告書です。

ISA/IEC 62443 は、OT(運用技術)を利用する産業用オートメーションおよび制御システムのセキュリティ ニーズに対応する事を目的としています。これらのシステムに対するサイバー攻撃はここ数年でますます増加しています。その被害には、国家安全保障戦略上重要な資産への侵害(エネルギ供給、輸送網、医療産業の停止等)から、収益の損失(製造業等)、人命を直接的に脅かすもの(感電死、化学製品への接触、命に関わる機器の故障等)まで様々なものがあります。

これらのセキュリティ ニーズとそれがもたらす脅威は従来の IT(情報技術)システムのものとは異なります。これは IT システムに対して以下のような多くの違いがあるためです。

- 性能要件(スループット、応答時間等)
- 可用性要件(停止に対する耐性、継続運転の必要性、プラント認証等)
- 運用環境の特性(使われるオペレーティング システムの種類、技術の更新頻度、システムのアップグレード可能性等)
- リスク管理目標(耐障害性、HSE(健康、安全、環境)への悪影響の防止)

これらの特殊性により、IT 分野に適用するために当初策定された既存のセキュリティ規格(ISO 27000 シリーズの規格等)は、IACS セキュリティ要件に効率的かつ効果的に対応する上では適切ではありません。

1.1 ISA/IEC 62443 シリーズの構造と内容

ISA/IEC 62443 シリーズの規格は全 14 分冊(規格、技術仕様書、技術報告書)から構成されており、これらは以下の 4 つの階層に論理的に分類されています。

- 第 1 階層: 一般
- 第 2 階層: ポリシーと手続き
- 第 3 階層: システム
- 第 4 階層: コンポーネント

また、62443 シリーズでは以下の 3 つの役割が導入されています。

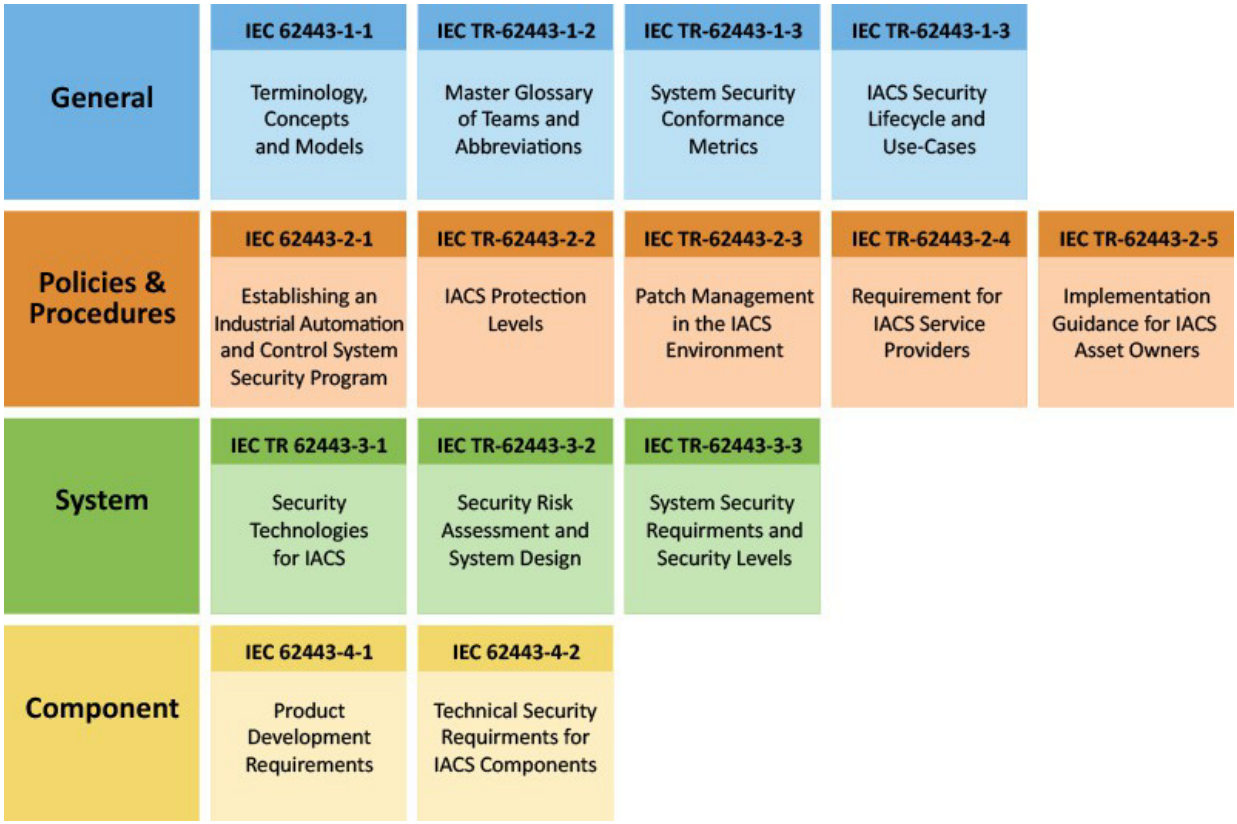
- **AO(アセットオーナー)**: 産業用オートメーション制御システムのエンドユーザーであり運用者です。
- **SI(システム インテグレータ)**: IACS を構成するサブシステムとコンポーネントの統合と構成、および目的の環境への展開を担当するエンティティです。
- **PS(製品サプライヤ)**: 産業用製品(PLC または RTU 等の組み込みデバイス、ファイアウォール等のネットワークデバイス、PC 等のホストデバイス、またはソフトウェア アプリケーション)の製造者です。

規格の第 1 階層(62443-1)の「一般」には一般的な性質の分冊が含まれ、シリーズ全体で用いられる基礎的な概念、モデル、用語が紹介されています。これは以下の 4 分冊で構成されています。

- 62443-1-1: 概念とモデル
- 62443-1-2: マスター用語集および略語集
- 62443-1-3: システム セキュリティ適合性評価基準
- 62443-1-4: IACS セキュリティ ライフサイクルとユースケース

この第 1 階層は、本規格で定義されているどの役割にも同等に関連しています。

図 1-1. ISA/IEC 62443 の階層構造



第 2 階層(62443-2)の「ポリシーと手続き」は効果的なセキュリティ プログラムにおける「人」と「プロセス」の側面に焦点を当て、プラント運用に関する事項を適用範囲としています。これは以下の 5 分冊で構成されています。

- 62443-2-1: IACS アセットオーナーに対するセキュリティ プログラム要求事項
- 62443-2-2: IACS セキュリティ管理システムの実装ガイダンス
- 62443-2-3: IACS 環境におけるパッチ管理
- 62443-2-4: IACS ソリューション サプライヤに対する要求事項
- 62443-2-5: IACS アセットオーナーに対する実装ガイダンス

この第 2 階層はアセットオーナーにとって、最も重要な項目です。

第 3 階層(62443-3)の「システム」は、システムのセキュリティにおける技術関連の側面に焦点を当て、セキュリティを実現する実装と統合の指針となる原則について説明しています。これは以下の 3 分冊で構成されています。

- 62443-3-1: IACS のセキュリティ技術
- 62443-3-2: セキュリティ リスク評価とシステム設計
- 62443-3-3: システム セキュリティの要求事項とセキュリティ レベル

第 4 階層(62443-4)の「コンポーネント」は、製品およびコンポーネントの特定のセキュリティ関連要件に焦点を当て、これらの製品の技術的内容と、製品ライフサイクル全体を通じてそれらの製品を管理するために採用されるプロセスを対象としています。これは以下の 2 分冊で構成されています。

- 62443-4-1: セキュアな製品開発ライフサイクルの要求事項
- 62443-4-2: IACS コンポーネントの技術的セキュリティ要求事項

この第 4 階層は製品サプライヤが最も関わる部分です。ここで重要なのは、第 4 階層の内容は最終的な自動化プロジェクトの実装に関する詳細事項からコンポーネントとその機能を抽象化する事を目的として策定されたという点です(コンポーネントの機能に焦点を当てています)。

1.2 ISA/IEC 62443 のセキュリティへのアプローチ

ISA/IEC 62443 シリーズは産業分野のセキュリティに対する包括的なアプローチを示しており、以下の重要性を強調しています。

- プロセスと技術的機能の定義と処理に当たってリスク管理手法を適用する事。
- 統合されたフレームワークの一部としてセキュリティの全側面(物理的セキュリティ、人的セキュリティ、サイバー セキュリティ等)に対処する事。

この包括的なアプローチはエンドユーザーの懸念に対応する必要性から生じたものです(アセットオーナーの視点を中心としています)。

このアプローチの土台の 1 つとなっているのが「SL(セキュリティ レベル)」という概念です。

ISA/IEC 62443 シリーズは、SL(セキュリティ レベル)に定性的な定義を導入しており、攻撃に対する保護レベル別に分けられています。

図 1-2. ISA/IEC 62443 のセキュリティ レベル

ISA/IEC 62443 アプローチでは、アセットオーナーが実装対象の IACS を定義する際にリスク評価作業を実施する事が求められます。このリスク評価作業の結果、IACS 全体の「SL-T(目標としてのセキュリティ レベル)」が得られます。

この SL-T に基づき、アセットオーナーが(システム インテグレータの支援を受けながら)サブシステムとコンポーネントを調達し、特定の環境に IACS を実装します。各コンポーネントおよびサブシステムは「SL-C(能力としてのセキュリティ レベル)」によって特徴付けられます。

その後、システムの実装はアセットオーナーによって評価され、「SL-A(達成できているセキュリティ レベル)」が事前に定められた要件を満たしているか(SL-A が SL-T 以上であるか)が検証されます。目標が完全に達成されるまで、システムレベルで、またはプロセスと手続きにおいて、(技術および手続きの両側面から)補正策が繰り返し適用されます。

ISA/IEC 62443 の第 4 階層の規格に準拠して開発プロセスと技術的な内容が認証されているコンポーネントを使う事で、アセットオーナーとシステム インテグレータは、実現されるシステムのセキュリティに対してより効率的に、より効果的に、また高い信頼を置いて、IACS の統合、実装、リスク管理作業を実施できるようになります。

2. 製品サプライヤのための ISA/IEC 62443

ISA/IEC 62443 に準拠して認証取得可能な製品を開発するには、製品サプライヤは規格の第 4 階層に含まれる以下の 2 つの分冊の内容を考慮する必要があります。

- 製品サプライヤのプロセスは、規格の分冊 4-1(「セキュアな製品開発ライフサイクルの要求事項」)に定められた要件を満たす必要があります。この分冊は一連の「プラクティス」を定義し、製品サプライヤのプロセスの準備状況を「成熟度レベル」の観点でランク付けするものです。
- 認証取得を目指す特定の製品は、規格の分冊 4-2(「IACS コンポーネントの技術的セキュリティ要求事項」)に定められた技術的要件を満たす必要があります。この分冊は一連の「基本要件」を定義し、製品サプライヤの製品のセキュリティ機能を「セキュリティ レベル」の観点でランク付けするものです。

本書では主に後者への対応に焦点を当てています。また、製品を規格に準拠させる上で Microchip 社のセキュア エレメントと Security Pattern 社がどのように役立つかを強調して説明する事で、本規格の 200 ページにわたる分冊 4-2 の内容を簡潔化する事を目的としています。

2.1 ISA/IEC 62443-4-2 に準拠する方法

セキュリティ レベルの定性的な定義については、1.2 ISA/IEC 62443 のセキュリティへのアプローチを参照してください。

製品に特定のレベルを割り当てるには、製品の SL-C(能力としてのセキュリティ レベル)の定量的評価を実施する必要があります。定量的評価は、CR(コンポーネント要件)と関連する RE(要件拡張)のリストに基づいています。これらの要件は FR(基本要件)と呼ばれるカテゴリにグループ化されています。

本規格では、以下の 7 つの基本要件(FR1～FR7)が定義されています。

FR1	IAC(識別および認証制御)
FR2	UC(使用制御)
FR3	SI(システムの完全性)
FR4	DC(データの機密性)
FR5	RDF(データフロー制限)
FR6	TRE(迅速なイベント対応)
FR7	RA(リソースの可用性)

各基本要件は 1 つの論理的なグループを示しているだけです。このグループは 1 つの CR(コンポーネント要件)と最終的には複数の RE(要件拡張)のセットで構成されています。

この規格では、各 SL に到達するためにどの CR/RE が必要かを示す表が提供されています。

下表は、FR1(識別および認証制御)の要件番号 7(パスワードベース認証の強度)に基づく定量的評価の例を示しています。

この CR には関連する RE が 2 つあります。表のチェックマークは、所定の SL に到達するためにその CR または RE が必要かどうかを示しています。

	SL1	SL2	SL3	SL4
CR1.7 - パスワードベース認証の強度	✔	✔	✔	✔
RE1.7.1 - 人間ユーザー向けのパスワード生成と有効期間制限				✔
RE1.7.2 - 全ユーザー向けのパスワード有効期間制限				✔

評価の例:

- コンポーネントが基本の CR を満たさない場合、その SL は 0 となります。

- コンポーネントが基本の CR のみを満たす場合、その SL は 2 となります。
- コンポーネントが基本の CR と 1 つ目の RE(1)を満たす場合、その SL は 3 となります。
- コンポーネントが基本の CR、RE(1)、RE(2)を満たす場合、その SL は 4 となります。

この評価は各 FR カテゴリに含まれる全ての CR/RE グループについて繰り返し実施する必要があります。対象製品の総合 SL は、これら全ての評価で達成された SL のうち最も低い値となります。結論として、目標とする SL(セキュリティ レベル)を達成するためには、全ての要件を満たす必要があります。

2.2 Microchip 社製品の機能

ATECC608 は、IACS 製品サプライヤが ISA/IEC 62443-4-2 によって義務付けられたコンポーネント要件を満たすための技術的な実現手段を提供します。以下に ATECC608 の暗号機能とセキュリティ保護の一覧を示します。これらの機能と ISA/IEC 62443 の仕様との対応関係については後述します。

表内での名称	機能
SHA256	SHA-256 および HMAC ハッシュ (デバイス外部のコンテクスト退避/復元を含む)。
セキュアな鍵保存	最大 16 個の鍵、証明書、データを保存できる JIL「高」評価の保護されたストレージ。
ECDSA	ECDSA: FIPS186-3 楕円曲線デジタル署名アルゴリズム(署名/検証)。
ECDH	ECDH: FIPS SP800-56A 楕円曲線 Diffie-Hellman。
ECCP256	NIST 規格 P-256 楕円曲線をサポート。
PRF/HDKF	TLS 1.2/1.3 向けのターンキーPRF/HKDF 計算。
使い捨て鍵	使い捨て鍵の生成と SRAM 内での鍵合意。
メッセージの暗号化	完全に保護された鍵による小メッセージの暗号化。
AEC128/GCM	AES-128: 暗号化/復号、GCM のガロア体乗算。
RNG	高品質 NIST SP 800-90A/B/C RNG(乱数生成器)を内蔵。
鍵ローテーション	秘密鍵のローテーションと公開鍵の認証は利便性向上のために ATECC608 TrustFLEX にあらかじめ設定されており、効果的に実行可能。 公開鍵のローテーションも利便性向上のために ATECC608 TrustFLEX にあらかじめ設定されており、効果的に実行可能。これは後期段階の鍵のプロビジョニングにとって重要な機能。
タンパ保護	物理的耐タンパ性とサイドチャンネル攻撃保護。
セキュアな鍵 プロビジョニング	HSM ネットワークを活用した Microchip 社社内でのセキュアな鍵プロビジョニングと後期段階プロビジョニングが可能。
セキュアブート	ECC-P256 ECDSA 検証による署名検証。
鍵の無効化	セキュア エレメントは開発者によって定義された論理条件に従って鍵を無効化する機能を備える。
セキュアな鍵 プロビジョニング	Microchip 社のセキュア鍵プロビジョニング サービスを使うと、お客様は HSM(ハードウェア セキュリティ モジュール)完備の Microchip 社の工場を利用してサードパーティのメーカーの暗号化鍵を分離可能。後期段階でのプロビジョニングも可能(Microchip 社へお問い合わせください)。

ISA/IEC 62443 は「セキュアな鍵保存」、すなわち暗号鍵の保護を要求しています。これはセキュリティにおける漠然とした用語ではなく、シリコンの設計時に組み込まれた具体的な機能を指します。セキュアな鍵保存、すなわち鍵を保護する行為は、暗号演算と暗号化鍵が存在する物理的なセキュア境界を実装する事によって成り立ちます。鍵とアルゴリズムが同一のセキュア境界内に存在しない場合、トランザクション中のどこかの時点で鍵が露出してしまいます。このような場合に、ATECC608 のようなセキュア エレメントが認証取得に真価を発揮します。セキュア エレメントは、鍵保護の堅牢性をテストするため、コモン クライテリアの手法に基づく JIL (Joint Interpretation Library)の評価基準でテストされたセキュアな鍵保存デバイスです。

セキュアな鍵保存の重要性に続き、セキュアな製造プロセスに従ってこのようなデバイスの場所に鍵を格納する事が次に直面する課題です。Microchip 社は管理された HSM(ハードウェア セキュリティ モジュール) ネットワークを備えたエ場を有しており、お客様はそのセキュアな鍵プロビジョニング サービスを利用できます。このサービスでセキュア エレメントを導入する事で、管理された秘密鍵交換プロセスに従い、委託メーカー等のサードパーティに各種暗号鍵を露出させる事なく、デバイスに安全に格納された認証情報を、お客様自身または顧客のチェーンオブトラストに結び付ける事ができます。また、補完的な方法として、最終顧客がプロビジョニング プロセスの後半で暗号鍵を有効化する事を望んでいる場合、Microchip 社のセキュア エレメントで後期段階のプロビジョニングが可能です。

下表は ISA/IEC 62443-4-2 で定義されたコンポーネント要件と、ATECC608 がお客様の製品が各要件を満たすための技術的な実現手段としてどのような支援を提供できるかを示しています。表内の各 CR と暗号機能には、SL(セキュリティ レベル)が示されています。

ISA/IEC 62443 規格は、以下の 4 種類のコンポーネントに対する要件を定義しています。

- EDR(組み込みデバイス)
- SAR(ソフトウェア アプリケーション)
- HDR(ホストデバイス)
- NDR(ネットワーク デバイス)

全種類のコンポーネントに適用されるコンポーネント要件は「CR」とマークされ、その他の要件は適用されるコンポーネントの種類に応じてそれぞれ「EDR」、「SAR」、「HDR」、「NDR」とマークされています。

下表において、RE は同じ段落枠内の CR に関連している事に注意してください。例えば、「CR 1.1 RE(1) 一意の識別と認証」は「CR1.1 人間ユーザーの識別と認証」の一部です。

機能要件		関連要件																		
CR (コンポーネント要件)	コンポーネント RE(要件拡張)	SAR EDR HDR HDR 要件	SAR EDR HDR HDR 要件拡張	タイトル	NIST SP 800-90A/B/C (RNG)	ECC-P256	ECDSA P256 FIPS186-3 (署名/検証)	ECDH FIPS SP800-56A	使い捨て鍵と SRAM 内での鍵合意	TLS 1.2/1.3 向けの PRF/HKDF	SHA-256 & HMAC (逆変換/復元を含む)	AES-128: GCM、暗号化/復号	保護された鍵によるメッセージの暗号化	JIL「高」セキュア鍵保存	タンパ保護	鍵ローテーション	鍵の無効化	セキュアブート	セキュアな鍵プロビジョニング	機能と用途
CR. 1.1				人間ユーザーの識別と認証							1									ハッシュ機能とセキュアな鍵保存機能を組み合わせる事で、パスワード ファイルの完全性チェックを堅牢に管理できます。
	CR 1.1 RE (1)			一意の識別と認証							2									ハッシュ機能とセキュアな鍵保存機能を組み合わせる事で、パスワード ファイルの完全性チェックを堅牢に管理できます。
CR 1.2				ソフトウェア プロセスとデバイスの識別と認証	2	2	2	2						2	2				2	JIL「高」のセキュアな鍵保存とデジタル署名の検証および生成機能により、セキュアな識別と認証が可能です。
	CR 1.2 RE(1)			一意の識別と認証	3	3	3	3						3	3				3	JIL「高」のセキュアな鍵保存とデジタル署名の検証および生成機能により、セキュアな識別と認証が可能です。
CR 1.5				オーセンティケータ管理					1	1		1	1	1	1	1	1		1	暗号鍵の生成とセキュアな保存機能により、ハードウェアを介した鍵の強固な初期化とライフサイクル管理が可能です。
	CR 1.5 RE(1)			オーセンティケータのハードウェア セキュリティ					3	3		3	3	3	3	3	3		3	暗号鍵の生成とセキュアな保存機能により、ハードウェアを介した鍵の強固な初期化とライフサイクル管理が可能です。
CR 2.4		SAR 2.4 EDR 2.4 HDR 2.4 NDR 2.4		モバイルコード		1	1	1			1	1		1	1	1	1		1	ハッシュ機能とセキュアな保存機能により、コードとデータの完全性チェックを堅牢に管理できます。
			SAR 2.4 RE(1) EDR 2.4 RE(1) HDR 2.4 RE(1) NDR2.4 RE(1)	モバイルコードの真正性チェック	2	2	2	2						2	2	2	2		2	鍵と証明書のセキュアな保存、デジタル署名の検証および生成機能により、コードとデータの認証が可能です。
CR2.12				否認防止	1	1	1	1			1									ハッシュ機能とセキュアな保存機能により、監査情報の完全性チェックを堅牢に管理できます。鍵と証明書のセキュアな保存、デジタル署名の検証および生成機能により、監査情報の認証が可能です。
CR2.12	CR2.12 RE(1)			全ユーザーの否認防止	4	4	4	4			4									ハッシュ機能とセキュアな保存機能により、監査情報の完全性チェックを堅牢に管理できます。鍵と証明書のセキュアな保存、デジタル署名の検証および生成機能により、監査情報の認証が可能です。
CR3.1				通信の完全性							1									鍵と証明書のセキュアな保存、デジタル署名の検証および生成機能により、送信した情報の完全性と真正性を保証できます。標準的な対称鍵/非対称鍵アルゴリズムとハッシュ用の暗号化エンジンにより、一般的な通信暗号スイートをサポートできます。
インデックス値: 1 = SL1 2 = SL2 3 = SL3 4 = SL4																				

.....続き

機能要件		関連要件																		
CR (コンポーネント要件)	コンポーネント RE(要件拡張)	SAR EDR HDR HDR 要件	SAR EDR HDR HDR 要件拡張	タイトル	NIST SP 800-90A/B/C (RNG)	ECC-P256	ECDSA P256 FIPS186-3 (署名/検証)	ECDH FIPS SP800-56A	使い捨て鍵と SRAM 内での鍵合意	TLS 1.2/1.3 向けの PRF/HKDF	SHA-256 & HMAC (逐差復元を含む)	AES-128: GCM、暗号化/復号	保護された鍵によるメッセージの暗号化	JIL「高」セキュア鍵保存	タンパ保護	鍵ローテーション	鍵の無効化	セキュアブート	セキュアな鍵プロビジョニング	機能と用途
CR3.1	CR3.1 RE(1)			通信認証	2	2	2	2		2		2	2	2	2	2	2		2	ネットワーク鍵管理のサポートにより、TLS 等の標準的な暗号化通信プロトコルをサポートできます。
CR3.4				ソフトウェアと情報の完全性							1			1	1	1	1		1	ハッシュ機能とセキュアな保存機能により、コードとデータの完全性チェックを堅牢に管理できます。
CR3.4	CR3.4 RE(1)			ソフトウェアと情報の真正性		2	2	2						2	2	2	2		2	鍵と証明書のセキュアな保存、デジタル署名の検証および生成機能により、コードとデータの認証が可能です。
CR3.8				セッションの完全性	2				2	2		2	2							ネットワーク鍵管理のサポートと内部 RNG により、堅牢な一意のセッション識別子を生成する機能が提供されます。
CR3.10			EDRE3.10.1、HD RE3.10.1、ND RE3.10.1	更新の真正性と完全性		2	2	2			2	2	2	2	2	2	2	2	2	鍵と証明書のセキュアな保存、デジタル署名の検証および生成機能、非対称/対称アルゴリズムとハッシュ機能に対するハードウェア サポートにより、ソフトウェア更新の認証と完全性検証が可能になります。
CR3.12		EDR3.12 HDR3.12 NDR3.12		製品サプライヤのルートオブ トラストのプロビジョニング										2	2	2	2		2	製品サプライヤのルートオブ トラストを保護するためのセキュアなストレージ機能を利用できます。
CR3.13		EDR3.13 HDR3.13 NDR3.13		アセットオーナーのルートオブ トラストのプロビジョニング										2	2	2	2		2	アセットオーナーのルートオブ トラストを保護するためのセキュアなストレージ機能を利用できます。
CR3.14		EDR3.14 HDR3.14 NDR3.14		ブートプロセスの完全性		1	1											1		セキュアブートは、内部の署名検証メカニズムとダイジェスト/署名のセキュアな保存によりサポートされています。
CR3.14			EDRE3.14.1、HDRE3.14.1、NDRE3.14.1	ブートプロセスの真正性		2	2											2		セキュアブートは、内部の署名検証メカニズムとダイジェスト/署名のセキュアな保存によりサポートされています。
CR4.1				情報の機密性		1	1	1			1	1		1	1	1	1		1	最大 16 個の鍵、証明書、またはデータについてセキュアな暗号化ストレージが直接提供されます。さらに、対称アルゴリズムと鍵保存機能のハードウェア サポートにより、外部に保存されたデータの暗号化が可能です。
CR4.3				暗号化の使用		1	1	1			1	1								最大 16 個の鍵、証明書、またはデータについてセキュアな暗号化ストレージが直接提供されます。さらに、対称アルゴリズムと鍵保存機能のハードウェア サポートにより、外部に保存されたデータの暗号化が可能です。
CR4.3	CR7.3 RE(1)			バックアップ完全性検証							2			2	2	2	2		2	ハッシュ機能とセキュアな保存機能により、バックアップ データの完全性チェックを堅牢に管理できます。
CR7.4				制御システムのリカバリと再構成							1			1	1	1	1		1	ハッシュ機能とセキュアな保存機能により、バックアップ データの完全性チェックを堅牢に管理できます。

インデックス値: 1 = SL1 2 = SL2 3 = SL3 4 = SL4

3. まとめ

1. **暗号アルゴリズムの要件:** ISA/IEC 62443 は、暗号アクセラレータだけではセキュリティを確保できない事を示しています。ATECC608 製品の優れた特長は、デバイスの稼働時間の大半を占めるスリープモードで消費する電力がきわめて低い事です(30 nA)。その利点とハードウェア ベースの暗号アクセラレータを組み合わせて実行時間を短縮し、重い暗号演算を ATECC608 に任せる事で、デバイスはパワーバジェットの最適化を実現する優れたソリューションになります。
2. **JIL「高」のセキュアな鍵ストレージ:** これこそが Microchip 社のセキュア エレメントが ISA/IEC 62443 準拠達成を支援する際の強みとなっている点です。暗号アルゴリズムは単なる数学的演算に過ぎません。関連する鍵が保護されなければ、実質的にセキュリティは確保できません。本質的に、暗号アルゴリズムが必要とされる場合は常にセキュアなストレージが必須となります。ATECC608 はコモン クライテリアのセキュアな鍵ストレージに対する試験手法に従ってテストされ、JIL スケールで評価されました。ATECC608 は、セキュアな鍵ストレージにおいて最高グレードに当たる JIL「高」を取得しており、高い信頼性のもと、鍵の保護が非常に低コストで実現されます。
3. **セキュアな鍵プロビジョニング:** 同様に、セキュアな鍵ストレージとセキュアな鍵プロビジョニングの間にも同じような関係を見出す事ができます。鍵と外部変数の間の分離を可能な限り維持するには、暗号鍵をセキュアな製造プロセスに従って取り扱う事が不可欠です。これは ISA/IEC62443-4-1 規格でも強調されている点です。Microchip 社では暗号鍵をお客様に代わってロードする社内セキュア鍵プロビジョニング サービスを提供しています。Microchip 社の Trust Platform はその起点となるプラットフォームです。
4. **CryptoAuthLib ライブラリ:** マイクロコントローラまたはマイクロプロセッサの選択に柔軟性をもたらす重要な要素です(PKCS11 の使用をご検討ください)。CryptoAuthLib ライブラリは HAL(ハードウェア抽象化層)を提供します。この HAL に I^2C または SWI ドライバを実装し、セキュア エレメントをマイクロコントローラまたはマイクロプロセッサから独立した状態に保つ事ができます。

4. Microchip 社のリソースとパートナーの Security Pattern 社によるサポート

ISA/IEC 62443 規格は、セキュリティに対して包括的に取り組む必要性を強調しています。セキュリティは技術のみでは達成できません。セキュリティは確かに技術に関連しますが、人とプロセスにも関連します。

このアプローチの自然な帰結として、製品サプライヤのプロセスが ISA/IEC 62443-4-1 規格(「セキュアな製品開発ライフサイクルの要求事項」)に準拠する事が、ISA/IEC 62443-4-2 規格に基づいて CSA [1]と EDSA の製品認証を取得するための前提条件となりました。

ISA/IEC 62443-4-1 に準拠するとは、製品が製品サプライヤによって適切なセキュリティ レベルで確実に管理される事を保証する一連の堅牢なプロセスが採用されている事を意味します。そのセキュリティ レベルは、製品の技術的内容と釣り合っていて、顧客の期待に沿い、かつ製品のライフサイクル全体を通じて持続可能なものでなければなりません。これらの要件は、セキュリティに関する一般的な推奨事項とベスト プラクティスに完全に合致しています。

以下は、本規格が製品サプライヤに求める主な活動の一部です。

- 多層防御を含むセキュリティ バイデザイン(設計によるセキュリティ)原則の適用
- 構想から設計、実装、テスト、現場での課題管理、廃止に至るまでの、セキュリティ要件の適切な定義と追跡
- セキュア コンポーネントの設計に対するリスク管理手法の適用(脅威モデリングの活動がこのリスク中心型アプローチの不可欠な部分になっている)
- 製品の定義、開発、管理における各従業員の役割と責任の定義に従った、関連するセキュリティ分野における人材教育

Security Pattern 社は、認証済みの Microchip 社セキュリティ パートナーとして以下のサポートを提供できます。

- 重点的なコンサルティングや導入研修を通じて、産業用部品メーカーが自社製品のセキュリティ要件と ISA/IEC 62443 規格との関係を理解するためのサポートを提供します。
- セキュリティ関連の製品要件の定義と改善(プラットフォームの選択/定義を含む)をサポートします。
- 製品サプライヤが Microchip 社コンポーネントとその豊富なセキュリティ機能を適切に活用できるよう支援します。
- 製品開発段階において、製品サプライヤによるシステム定義、生産フローの合理化(サプライチェーンとサードパーティ サプライヤのセキュリティを考慮)、ソフトウェア開発を支援します。
- 公開鍵基盤の設定、デジタル証明書管理、セキュアブート等の技術とノウハウを提供します。
- ISA/IEC 62443-4-1 要件に従った製品サプライヤの内部プロセスの実装と実行を支援し、ISA/IEC 62443 規格の要件に準拠した文書構造を提供します。
- ISA/IEC 62443-4-2 コンポーネント要件に対する製品ギャップ分析を実施できます。
- 選択した ISA/IEC 62443 認証機関との技術的な討議をサポートします。
- 規格のプラクティス 1 で要求されるセキュリティ専門知識の維持と評価について、製品サプライヤの要員のニーズに合わせたトレーニング セッションを提供します。

Note:

1. www.isasecure.org/en-US/Certification/IEC-62443-CSA-Certification#tab1

5. ATECC608 と Security Pattern 社の利用を開始する

コンサルティングと設計サービスは、Microchip 社の認定セキュリティ設計パートナーである Security Pattern 社のウェブサイトをご覧ください。その他の情報については、以下の Microchip 社ウェブサイトを参照してください。

- CryptoAuthentication™向け Trust Platform の概要と Microchip 社のセキュアな鍵プロビジョニング サービスの活用の始め方
- CryptoAuthLib ライブラリの Github リポジトリ
- TLS または LoRaWan ネットワーク向けの事前プロビジョニング済み Trust&GO ISA/IEC 62443 セキュア エレメントの詳細
- 事前設定済み TrustFLEX ISA/IEC 62443 セキュア エレメントの詳細
- 完全にカスタマイズ可能な TrustCUSTOM ISA/IEC 62443 セキュア エレメントの詳細

6. 改訂履歴

リビジョン	日付	セクション	改訂内容
A	2021 年 4 月	文書全体	初版
B	2021 年 12 月	1.1 ISA/IEC 62443 シリーズの構造と内容	図 1-1 の図を修正

Microchip 社ウェブサイト

Microchip 社はウェブサイト(www.microchip.com)を通してオンライン サポートを提供しています。当ウェブサイトでは、お客様に役立つ情報やファイルを提供しています。以下を含む各種の情報をご覧になれます。

- **製品サポート** - データシートとエラッタ、アプリケーション ノートとサンプル プログラム、設計リソース、ユーザーガイドとハードウェア サポート文書、最新のソフトウェアと過去のソフトウェア
- **技術サポート** - FAQ(よく寄せられる質問)、技術サポートのご依頼、オンライン ディスカッション グループ、Microchip 社のデザイン パートナー プログラムおよびメンバーリスト
- **ご注文とお問い合わせ** - 製品セレクタと注文ガイド、最新プレスリリース、セミナー/イベントの一覧、お問い合わせ先(営業所/正規代理店)の一覧

製品変更通知サービス

Microchip 社の製品変更通知サービスは、お客様に Microchip 社製品の最新情報をお届けする配信サービスです。ご興味のある製品ファミリまたは開発ツールに関する変更、更新、リビジョン、エラッタ情報をいち早くメールにてお知らせします。

http://www.microchip.com/pcn にアクセスし、登録手続きをしてください。

お客様サポート

Microchip 社製品をお使いのお客様は、以下のチャンネルからサポートをご利用頂けます。

- 正規代理店
- 技術サポート

サポートは正規代理店にお問い合わせください。本書の最後のページに各国の営業所の一覧を記載しています。

技術サポートは以下のウェブページからもご利用頂けます。

www.microchip.com/support

Microchip 社のデバイスコード保護機能

Microchip 社製品のコード保護機能について以下の点にご注意ください。

- Microchip 社製品は、該当する Microchip 社データシートに記載の仕様を満たしています。
- Microchip 社では、通常の条件ならびに動作仕様書の仕様に従って使った場合、Microchip 社製品のセキュリティ レベルは、現在市場に流通している同種製品の中でも最も高度であると考えています。
- Microchip 社はその知的財産権を重視し、積極的に保護しています。Microchip 社製品のコード保護機能の侵害は固く禁じられており、デジタル ミレニアム著作権法に違反します。
- Microchip 社を含む全ての半導体メーカーで、自社のコードのセキュリティを完全に保証できる企業はありません。コード保護機能とは、Microchip 社が製品を「解読不能」として保証するものではありません。コード保護機能は常に進化しています。Microchip 社では、常に製品のコード保護機能の改善に取り組んでいます。

法律上の注意点

本書および本書に記載されている情報は、Microchip 社製品を設計、テスト、お客様のアプリケーションと統合する目的を含め、Microchip 社製品に対してのみ使う事ができます。それ以外の方法でこの情報を使う事はこれらの条項に違反します。デバイス アプリケーションの情報は、ユーザーの便宜のためにのみ提供されるものであり、更新によって変更となる事があります。お客様のアプリケーションが仕様を満たす事を保証する責任は、お客様にあります。その他のサポートは Microchip 社正規代理店にお問い合わせ頂くか、www.microchip.com/en-us/support/design-help/client-support-services をご覧ください。

商標

ISBN: 979-8-3371-0993-0

品質管理システム

Microchip 社の品質管理システムについては www.microchip.com/quality をご覧ください。

各国の営業所とサービス

南北アメリカ	アジア/太平洋	アジア/太平洋	欧州
本社 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 技術サポート: www.microchip.com/support URL: www.microchip.com **アトランタ** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **オースティン、TX** Tel: 512-257-3370 **ボストン** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **シカゴ** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **ダラス** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **デトロイト** Novi, MI Tel: 248-848-4000 **ヒューストン、TX** Tel: 281-894-5983 **インディアナポリス** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **ロサンゼルス** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **ローリー、NC** Tel: 919-844-7510 **ニューヨーク、NY** Tel: 631-435-6000 **サンノゼ、CA** Tel: 408-735-9110 Tel: 408-436-4270 **カナダ - トロント** Tel: 905-695-1980 Fax: 905-695-2078	**オーストラリア - シドニー** Tel: 61-2-9868-6733 **中国 - 北京** Tel: 86-10 -8569-7000 **中国 - 成都** Tel: 86-28-8665-5511 **中国 - 重慶** Tel: 86-23-8980-9588 **中国 - 東莞** Tel: 86-769-8702-9880 **中国 - 広州** Tel: 86-20-8755-8029 **中国 - 杭州** Tel: 86-571-8792-8115 **中国 - 香港 SAR** Tel: 852-2943-5100 **中国 - 南京** Tel: 86-25-8473-2460 **中国 - 青島** Tel: 86-532-8502-7355 **中国 - 上海** Tel: 86-21-3326-8000 **中国 - 瀋陽** Tel: 86-24-2334-2829 **中国 - 深圳** Tel: 86-755-8864-2200 **中国 - 蘇州** Tel: 86-186-6233-1526 **中国 - 武漢** Tel: 86-27-5980-5300 **中国 - 西安** Tel: 86-29-8833-7252 **中国 - 厦門** Tel: 86-592-2388138 **中国 - 珠海** Tel: 86-756-3210040	**インド - バンガロール** Tel: 91-80-3090-4444 **インド - ニューデリー** Tel: 91-11-4160-8631 **インド - プネ** Tel: 91-20-4121-0141 **日本 - 大阪** Tel: 81-6-6152-7160 **日本 - 東京** Tel: 81-3-6880-3770 **韓国 - 大邱** Tel: 82-53-744-4301 **韓国 - ソウル** Tel: 82-2-554-7200 **マレーシア - クアラルンプール** Tel: 60-3-7651-7906 **マレーシア - ペナン** Tel: 60-4-227-8870 **フィリピン - マニラ** Tel: 63-2-634-9065 **シンガポール** Tel: 65-6334-8870 **台湾 - 新竹** Tel: 886-3-577-8366 **台湾 - 高雄** Tel: 886-7-213-7830 **台湾 - 台北** Tel: 886-2-2508-8600 **タイ - バンコク** Tel: 66-2-694-1351 **ベトナム - ホーチミン** Tel: 84-28-5448-2100	**オーストリア - ヴェルス** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **デンマーク - コペンハーゲン** Tel: 45-4485-5910 Fax: 45-4485-2829 **フィンランド - エスポー** Tel: 358-9-4520-820 **フランス - パリ** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **ドイツ - ガーヒンク** Tel: 49-8931-9700 **ドイツ - ハーン** Tel: 49-2129-3766400 **ドイツ - ハイルブロン** Tel: 49-7131-72400 **ドイツ - カールスルーエ** Tel: 49-721-625370 **ドイツ - ミュンヘン** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **ドイツ - ローゼンハイム** Tel: 49-8031-354-560 **イスラエル - ホドハシャロン** Tel: 972-9-775-5100 **イタリア - ミラノ** Tel: 39-0331-742611 Fax: 39-0331-466781 **イタリア - パドヴァ** Tel: 39-049-7625286 **オランダ - ドリューネン** Tel: 31-416-690399 Fax: 31-416-690340 **ノルウェー - トロンハイム** Tel: 47-7288-4388 **ポーランド - ワルシャワ** Tel: 48-22-3325737 **ルーマニア - ブカレスト** Tel: 40-21-407-87-50 **スペイン - マドリッド** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **スウェーデン - ヨーテボリ** Tel: 46-31-704-60-40 **スウェーデン - ストックホルム** Tel: 46-8-5090-4654 **イギリス - ウォーキンガム** Tel: 44-118-921-5800 Fax: 44-118-921-5820