サイバーセキュリティー規格IEC 62443-4に対する取り組み

Approaches to Certification of Skelios OS in Accordance with IEC 62443-4 Cybersecurity Standards

林　和宏 HAYASHI Kazuhiro　ディネッシュ　クマー Dinesh KUMAR　田中　明良 TANAKA Akira

近年，サイバーセキュリティーに対する脅威がますます高まり，産業用オートメーション及び制御システム（IACS：Industrial Automation and Control System）でも，脆弱（ぜいじゃく）性への攻撃が急速に増加している。IEC 62443-4（国際電気標準会議規格62443-4）は，IACSのセキュリティーを確保する国際標準規格であり，特に機器・コンポーネントのセキュリティー要求事項を定義している。

東芝は，東芝グループ製品向けOS（基本ソフトウェア）である東芝Linux®ディストリビューション“Skelios”において，IEC 62443-4に対応するため，OSS（オープンソースソフトウェア）コミュニティと共同で，具体的な技術とプロセスを導入して組み込み機器のセキュリティー強化に取り組み，IEC 62443-4-1規格の第三者機関による適合確認を取得した。

Growing cybersecurity threats in recent years have been accompanied by the rapid increase in cyberattacks targeting vulnerabilities in industrial automation and control systems (IACS). To ensure IACS security, IEC (International Electrotechnical Commission) 62443-4, which is part of a series of standards that define security requirements for equipment and components used in IACS, has been specified.

Toshiba Corporation is making efforts to further enhance the cybersecurity of Skelios, a Linux® distribution developed as an operating system (OS) for Toshiba Group's products to prepare it for IEC 62443-4. We have obtained third-party verification of conformance with the IEC 62443-4-1 standard by introducing specific technologies and processes to enhance the security of embedded devices in collaboration with the open-source community.

1. まえがき

サイバーセキュリティーの重要性がますます高まる現代では，IACSのセキュリティーを確保するための国際標準規格であるIEC 62443-4は重要な役割を果たしている。東芝は，東芝Linux®ディストリビューションSkeliosがこの規格に対応するため，OSSコミュニティにおいて，規格の要件を満たす具体的な技術とプロセスを導入した。この取り組みによりOSSコミュニティは，IEC 62443-4-1規格の第三者認証機関による適合確認を取得し，現在IEC 62443-4-2の最終評価が進行中である。これにより，OSSコミュニティの成果をそのまま利用するSkeliosは，セキュリティー開発ライフサイクルと技術的セキュリティー要求事項の適合性を確認可能になる。更に，Skeliosの導入により，セキュリティー対応コストの削減と長期運用のサポートが実現され，効果的な製品のセキュリティー認証取得に寄与している。

ここでは，この規格に関する背景と概要，当社の取り組みとその効果，規格への対応がもたらす利点について述べる。

2. サイバーセキュリティー対策の重要性と効果

2.1 セキュリティーインシデントの増加

近年，セキュリティーインシデントの数は急激に増加している。例えば，2024年7月には，セキュアなリモートアクセスツールであるOpenSSHの脆弱性により，glibc（注1）ベースのLinux®システムでリモートから認証なしにコードを実行してシステムを乗っ取れることが報告された[1]。このような脆弱性情報（CVE：Common Vulnerabilities and Exposures）（注2）の報告数は年々増加し，2024年には40,077件に達した（**図1**）[2]。これらのセキュリティーインシデントは，製品やシステムの信頼性を損なう要因となり，企業にとって重大なリスクである。

2.2 各国のセキュリティーに関する法規制・整備の状況

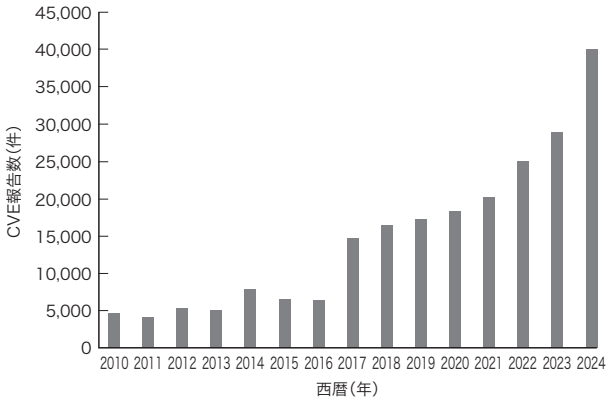
セキュリティーインシデントの増加に伴い，各国ではセキュリティーに関する法規制・整備が進められている。例えば，我が国では，総務省が「サイバーセキュリティ基本法」を制定し，サイバーセキュリティーに関する基本的な枠組みを提供している。欧州連合（EU）では，2023年にCRA

（注1） GNUプロジェクトが提供するC言語標準ライブラリー。
（注2） 情報セキュリティーの脆弱性・インシデントに付与した固有名・番号。

（Cyber Resilience Act）が制定され，デジタル要素を含む製品（PDEs：Product Digital Elements）に対するサイバーセキュリティー要件が規定された。CRAは，2027年までに完全な準拠を求めており，違反した場合には多額の罰金が科される可能性がある。

2.3 セキュリティー国際標準規格対応の効果

このように各国・地域において法規制・整備が行われ，対象となる製品・システムを供給する企業にとっては，この法的要求を満たすことが罰則や制裁を回避するだけでなく，製品・システムが顧客やサプライチェーンにおける納入要件となることが予想される。そのため法規制の要件をクリアする規格や認証への対応が重要となる。特に，社会インフラや産業向けのシステム・製品では，IACSを対象としたセキュリティー規格への対応が効果的である。IEC 62443シリーズは，IACSのセキュリティーを確保するための国際標準規格であり，幅広い産業分野をカバーすると同時に，IACSのライフサイクル全体を通じて安全性，信頼性，整合性，及びセキュリティーを向上させることを目的としている。また，セキュリティーリスクを体系的に管理するためのフレームワークを提供して潜在的な脅威を早期に特定し，適切な対策を講じることを可能とする。更に，顧客に対する信頼性を示すことでビジネス関係の強化が期待されると同時に国際的な標準規格に準拠してグローバル市場での競争力を高めることを可能にする。



＊Mitre.“Published CVE Records”[2]に基づいて作成

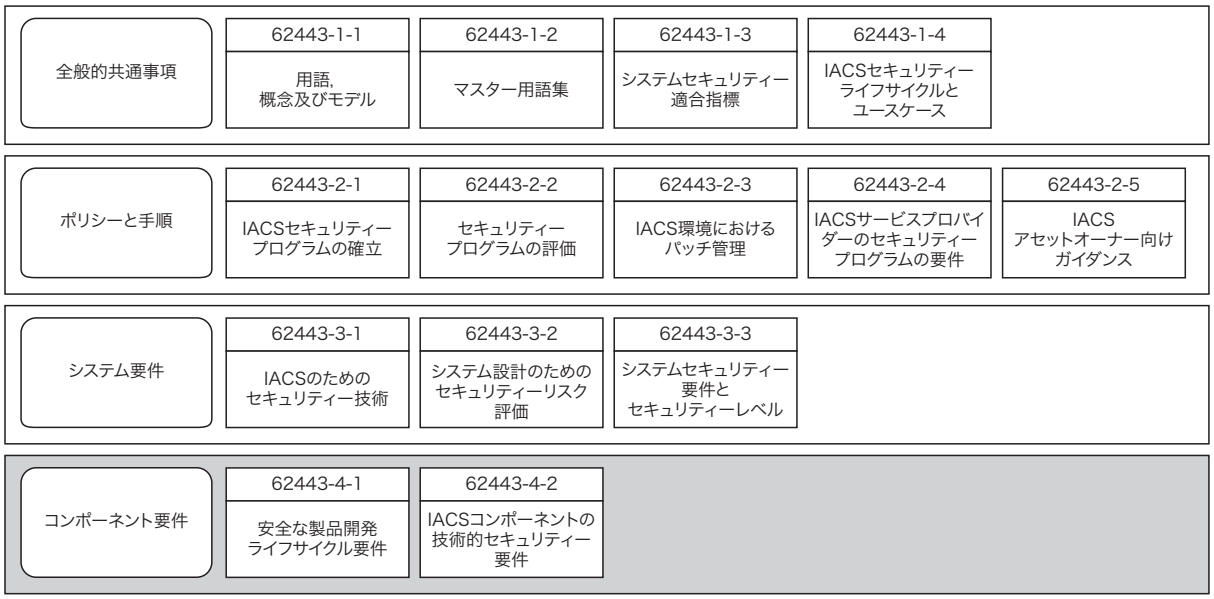
図1. CVE報告数の推移

14年前に比べて8倍以上に増加しており，セキュリティーに関するリスクが増大している。

Published number of common vulnerabilities and exposures (CVE) records by year

3. IEC 62443シリーズ国際標準規格の概要

IEC 62443シリーズは，IACSのセキュリティーを確保するための包括的な国際標準規格である。このシリーズは，IACSのセキュリティーを多面的にカバーするため，複数の分冊に分かれていて，以下の四つの主要な領域に分類される（**図2**）[3]。



＊ISAGCA. Quick Start Guide：An Overview of ISA/IEC 62443 Standards[3]に基づいて作成

図2. IEC 62443シリーズの全体構成

IEC 62443シリーズは，4項目で構成され，特に四つ目の機器（コンポーネント）要件が，製品そのものに関連した項目となる。

Overall IEC 62443 series standard system

⑴　全般的共通事項　　用語の定義やシリーズ全体に関わる共通事項を含む。

⑵　ポリシーと手順　　IACSの導入・運用における，セキュリティー管理のためのポリシーや手順を含む。

⑶　システム要件　　IACSの“システム”としてのセキュリティー水準の設計に関する標準を含む。

⑷　コンポーネント要件　　IACSのコンポーネント製品のセキュリティー保証水準に関する標準と製品開発プロセスに対する要件を含む。

この規格において，IEC 62443-4が，IACSのコンポーネントに対するセキュリティー要求事項を定義する規格であり，コンポーネントのセキュリティー開発ライフサイクルと技術的セキュリティー要求事項を対象としている。

4. CIPにおけるIEC 62443-4適合に向けた活動・成果

CIP（Civil Infrastructure Platform）(注3)は，高い安全性・信頼性が求められる社会インフラ分野で，産業グレードのOSSコンポーネントを提供するプロジェクトである。CIPは，近年高まるサイバー攻撃の脅威に対処するため，IEC 62443-4に適合したコンポーネントの提供を目指しており，当社は，この活動を主導・推進している。

CIPは，社会インフラ要件を満たすLinux®ベースの組み込みシステムを構築するために必要な共通コンポーネント（ベースレイヤー）を提供する。このレイヤーに対してIEC 62443-4の適合を取得することで，このレイヤーを拡張した様々な製品に対して認証を取得する際に，適合済みのプロセスや，機能，検証実績などを活用して認証取得までの作業効率化を実現することを目指している（**図3**）。また，ベースレイヤー自体は汎用的なコンポーネントであるため，最終的には，製品固有の要求に対して追加で適合確認を行う必要があるが，適合を受けたベースレイヤーの開発資源やプロセスを最大限流用することで認証取得の効率化と期間短縮が期待できる。

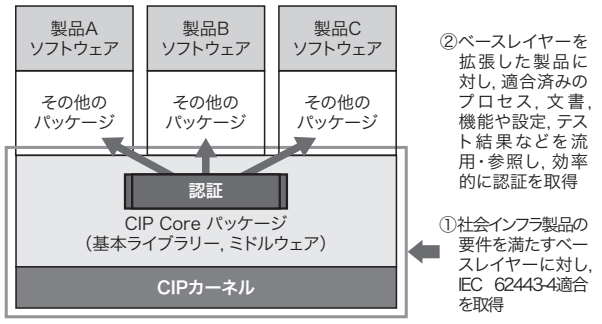


図3. CIPが提供するベースレイヤーと適合確認取得による効果

社会インフラ製品の要件を満たすベースレイヤーに対して適合確認を取得することで，このレイヤーを拡張した様々な製品に対して，適合済み成果を活用した効率的な認証取得が可能になる。

Effects of base layers provided by civil infrastructure platform (CIP) on certification acquisition

（注3）The Linux Foundationが運営する，社会インフラ向けの協業プロジェクト（https://cip-project.org/）。

4.1　IEC 62443-4-1への対応

IEC 62443-4-1は，製品開発ライフサイクルにおける企画から保守までの8段階でセキュリティーの要求事項を定めている。CIPでは，各要求項目に対し，以下の対応を実施した。

⑴　セキュリティ管理（SM：Security Management）
　コンポーネント開発について，開発プロセス，権限・責任，開発者のセキュリティー専門性，成果物のファイル整合性管理，レビュー方法などを明記した文書を作成した。

⑵　要求定義（SR：Specification of Security Requirement）　　前述のとおり，CIP単体では製品固有の要求を持たないため，IEC 62443-4-2の要求事項を元に複数製品で共通で必要となり得るセキュリティー要求を定義し，関連する脅威モデルを文書化した。

⑶　設計（SD：Secure by Design）　　開発・実行環境におけるインターフェースとその使用方法，関係するユーザーや権限を明確化し，脅威モデルに基づく対処方法をドキュメント化した。

⑷　実現（SI：Secure Implementation）　　セキュアコーディングに基づく実現及びセキュリティーレビューが要求されるが，この項目は，個々の製品要求に基づく対応が必要であり，CIP単体では適合対象外となった。

⑸　試験（SVV：Security Verification and Validation Testing）　　コンポーネントのエラー処理やセキュリティー対策が正しく機能する試験内容を明確化し，CIPの開発プロセスへの組み込みを行った。

⑹　不具合管理（DM：Management of Security-related Issues）　　コンポーネントを構成するLinux®カーネルや各種OSSについて，上流プロジェクトにおけるCVEの管理方法を文書化し，そのCVEをCIPで定常的に確認するプロセスを明確化・文書化した。

⑺　不具合改修（SUM：Security Update Management）
　修正の適用，更新内容に関する通知，及び更新の配布について，上流プロジェクトの情報と配布手段を最大限活用しながら，CIP開発プロセスにおける不具合改修に必要な対応を文書化した。

⑻　利用者支援（SG：Security Guidance）　　CIPの

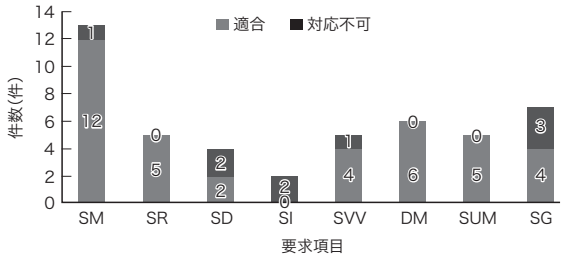


図4. CIPにおけるIEC 62443-4-1の各要求項目への対応状況

CIPではIEC 62443-4-1が定める八つの要求項目に対応し，要求事項全体の81％に対して適合確認が得られた。

Current status of CIP compliant with each requirement of IEC 62443-4-1

コンポーネントを利用するユーザー向けに，セキュリティー強化（ハードニング）に関わる開発・運用時のガイドラインを文書化した。

適合取得に向けた最終アセスメントにおいて，これら要求項目の81％に対する確認が得られた（**図4**）。そして，2024年8月に，第三者認証機関であるビューローベリタス（BV）によるIEC 62443-4-1の適合確認を取得した。

4.2 IEC 62443-4-2への対応

IEC 62443-4-2は，コンポーネント向けの技術的なセキュリティー要求事項として，七つの基礎的要件を定義している。また，四つのコンポーネントタイプが定義されており，タイプごとにコンポーネントが備えるべき機能やセキュリティー対策などの詳細なセキュリティー要件が定められている。

CIPでは，社会インフラ分野で重要度の高い“組み込み機器”と“ネットワーク機器”の2タイプを対象に，七つの基礎的要件に対し，例として以下の対応を実施した。

⑴ 識別と認証管理（IAC：Identification and Authentication Control）　アクセス者を正しく特定し，適切な権限だけを許諾する機能として，ユーザー認証，アカウント管理，多要素認証機能の設定と検証を行った。

⑵ 利用管理（UC：Use Control）　利用者の行為を許諾された内容に制限し，結果を監視する機能として，強制的な認証による権限制御，セッション制御，監査，ログ監視などの設定と検証を行った。

⑶ システムの完全性（SI：System Integrity）　想定外の状態への推移を防止する機能として，セキュアブートによるブートプロセスの完全性確保や，完全性チェックツールによるシステム改善検知などの設定と検証を行った。

⑷ データの秘密性（DC：Data Confidentiality）　許容されないデータ開示を防止する機能として，システムデータ暗号化の設定と検証を行った。

⑸ データの流れの制限（RDF：Restricted Data Flow）　不要なデータの流れを防止するため，システムとしてネットワークのセグメント化などが要求されるが，この項目は個々の製品要求に基づく対応が必要であり，CIP単体では適合対象外としている。

⑹ 事象に対するタイムリーな応答（TRE：Timely Response to Events）　監査ツールやシステムログの設定により，事象の常時監視と有効なログ取得が可能なことを確認した。

⑺ 資源の可用性（RA：Resource Availability）　パケットフィルタリングによるDoS（Denial of Service）攻撃に対する保護設定や，システムデータのバックアップ・復元方法などの試作・検証を実施した。

更に，CIPでは，これらの各種機能・設定が有効化されたOS環境をリファレンス実装として構築・利用可能にしており，CI（継続的インテグレーション）と自動テスト環境を用いて各種機能が正しく動作していることを定常的に確認できるようにした。

IEC 62443-4-2については，現在，適合取得に向けた最終アセスメントを実施中である。

5. Skelios導入による効果

Skeliosは，CIPのベースレイヤーを構成するカーネルや基本パッケージセットを再利用し，製品ごとのカスタマイズを加えることで，社会インフラ・産業用途向けLinux®の迅速な開発と長期運用を可能にしている。前述したCIPにおけるIEC 62443-4適合の成果は，ベースレイヤーを共有するSkeliosに対して，機能や，設定，テストなどの直接的な流用，及びCIPを上流プロジェクトとした開発プロセス・管理方法の参照が可能である。このため，Skeliosの導入により，長期的な脆弱性への修正対応，修正版ソフトウェアへ安全に更新可能な仕組みの導入，その他前述のセキュリティー要件に対するシステム設定並びに検証，開発プロセスへの対応が可能となる。そしてこの結果として，IEC 62443-4規格対応に必要な調査，検討，開発，維持管理コストを削減でき，国際的に認められたセキュリティー対策に準拠した当社製品を効率的に開発・提供することが可能になる。

6. あとがき

当社の取り組みとして，CIPの活動を主導・推進し，社会インフラ・産業向け要件を満たす基本コンポーネントに対するIEC 62443-4-1の適合取得を達成したこと，及びIEC 62443-4-2適合取得に向けた技術開発・環境整備を

推進していることについて述べた。また，各々の要件に対するこれまでの具体的成果についても併せて述べた。そして，Skeliosが，CIPの基本コンポーネントをベースにして製品への拡張と展開が可能であること，IEC 62443-4適合成果を再利用・参照して製品の効率的なセキュリティー認証取得に寄与することを示した。

当社は，今後も継続してOSSコミュニティと連携した基本コンポーネントの規格適合取得と適合状態の維持を行うとともに，Skeliosを基盤とした製品のIEC 62443-4規格対応を推進することで，IACSにおけるセキュリティー強化を図っていく。

文　献

⑴ Gigazine. “OpenSSHに重大な脅威となる脆弱性「regreSSHion」(CVE-2024-6387)が発覚、ほぼすべてのLinuxシステムに影響”. Gigazine. <https://gigazine.net/news/20240702-regresshion-cve-2024-6387/>, (参照 2025-04-22).

⑵ Mitre. "Published CVE Records". Metrics. <https://www.cve.org/About/Metrics>, (accessed 2025-04-22).

⑶ ISAGCA. Quick Start Guide: An Overview of ISA/IEC 62443 Standards. ISA, 2024, 15p. <https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023 ISA Website Redesigns/ISAGCA/PDFs/ISAGCA Quick Start Guide FINAL.pdf>, (accessed 2025-04-22).

林　　和宏　HAYASHI Kazuhiro
総合研究所 デジタルイノベーション技術センター
コンポーネント技術部
Component Technology Dept.

ディネッシュ　クマー　Dinesh KUMAR
東芝ソフトウェア・インド社
Toshiba Software (India) Pvt. Ltd.

田中　明良　TANAKA Akira
総合研究所 デジタルイノベーション技術センター
コンポーネント技術部
Component Technology Dept.