DNP

2021 年 2 月 3 日

IACS のセキュリティと 62443 シリーズ関連規格

大日本印刷株式会社
AB センター コミュニケーション開発本部
サイバーセキュリティ事業推進ユニット
主席研究員　半田 富己男, CISSP

このホワイトペーパーは，Vdoo 社のブログ[3]を翻案して作成した.

1　はじめに

1.1 IACS の変容とセキュリティ

産業用オートメーションおよび制御システム(IACS: Industrial Automation and Control System)は，古くは 1960 年代に導入された最初の PLC(プログラマブル・ロジックコントローラ)に遡り，製造工場や重要インフラの現場でリアルタイム制御とモニタリングの自動化に不可欠の存在となっている.

近年では，コンピュータと通信技術の標準化および技術進歩によりコストとサイズの両面が低下し，産業現場でも従来は切り離されていた産業用デバイスが相互に接続され, ものづくり現場の OT システムを企業の IT インフラストラクチャに統合することが可能になってきた.

接続された IACS の増加は，悪意のある攻撃者からの脅威の増加をもたらしている．IACS は，その企業にリスクをもたらす機密データを収集して送信するため，IACS が扱うデータが漏えいすると，その企業にリスクをもたらす．このため，データのセキュリティを確保する必要がある．さらに，OT システムが攻撃者に乗っ取られた場合には，物理的に甚大な被害をもたらし，重要インフラの停止や，人命の安全をも脅かす可能性があることを認識しなければならない.

IACS ベンダーには，製品を市場投入するまでの時間を短縮するために従来のデバイスをできるだけ早くネットワーク接続可能にしなければならない，というプレッシャーがある．しかし残念なことに，こうした拙速な開発はセキュリティの侵害につながることが多い. サイバー攻撃者が IACS を狙ったサイバー攻撃事案が多発するなか(表 1 参照), 規制当局は IACS 分野に許容されるサイバーセキュリティ基準認証を実施するために介入し始めている.

表 **1 IACS** を狙ったサイバー攻撃事例

	年	発生国	対象	概要	影響・被害
1	2003	米国	原子力発電所(オハイオ州 Davis Besse)	SQL サーバを狙ったワーム”Slammer”が VPN 接続を介して侵入.	SCADA システムが 5 時間停止

	年	発生国	対象	概要	影響・被害
2	2008	トルコ	石油パイプライン	監視カメラに侵入し，内部の制御システムに不正アクセス．警報機能を停止させパイプ内の圧力を異常に高めて爆発させた.	3 週間の操業停止（被害額は 50 万ドル/日と試算）
3	2010	イラン	ウラン濃縮施設	遠心分離機が USB メモリを介してマルウェア Stuxnet に感染．Stuxnet は周波数変換装置を制御する PLC に侵入し，回転数を不正操作.	約 8,400 台の遠心分離機が停止.
4	2014	ドイツ	製鉄所	標的型メールで情報システムに侵入し，製鉄所制御システムのクレデンシャルを窃取．不正操作によって溶鉱炉を正常に停止できなくした.	装置および製鉄システム（操業）に大きな損害.
5	2015	ウクライナ	送電設備	標的型メールにより情報系 PC がマルウェア BlackEnergy に感染， HMI の不正遠隔操作，マルウェア KillDisk による HMI のシステム破壊など.	6 時間の停電，22 万 5 千人に被害.
6	2017	サウジアラビア	石油化学プラント	マルウェア TRITON/TRISIS に感染し，安全計装システム(SIS)が危険な状態を許容するように改ざん.	プロセスが緊急停止
7	2019	ノルウェー	アルミニウム精錬	ランサムウェア”LockerGaga”に感染.	数ヶ月間, 生産量が低下

1.2 62443 シリーズの標準規格

IACS 分野では，“62443”という数字を冠した標準規格が最も影響力があって，よく知られており，広く利用され参照されている．異なる複数の標準化団体が“62443”を冠した標準規格を発行しており，それぞれの標準化団体が個別の標準規格セットを持っているだけでなく，これらの標準化団体の間には複雑な関係の歴史がある．異なる標準化団体から発行されている“62443”を冠した標準規格は，同じ内容で規格名称が異なるだけなのだろうか? 本稿では, “62443”を冠した様々な標準規格の背景と相互の関係性を整理し，関連する認証(certification)制度について解説する.

インターネットで“62443”を検索すると，ISA 62443，ANSI/ISA 62443，ISA/IEC 62443，IEC 62443 など，“62443”を冠した多くの種類の規格名称を見つけることができる．

たとえば, ISA/IEC 62443 と IEC 62443 は厳密には別々の 2 つの標準規格文書群である. ISA/IEC 62443 は，ISA (International Society of Automation; 国際計測制御学会)が制定した一連の標準規格である．ISA は 1945 年に設立された計測・制御に関する非営利の国際学会である．ISA/IEC 62443 は，以下に述べるように ANSI/ISA 62443 とも密接に関連している．一方，IEC 62443 は，電気及び電子の技術分野における国際標準化組織である IEC (International Electrotechnical Commission; 国際電気標準会議)が策定した規格群である.

IEC は, 先に策定されていた ANSI/ISA 62443 の要求事項に基づいて IEC 62443 の規格群を策定したといわれている．IEC によると，彼らの規格は「ANSI/ISA から派生したものであり，国際的な使用のために完全に置き換えられている」という.

2　ISA/IEC 62443

2.1 ISA 99 規格から ISA/IEC 62443 へ

ISA/IEC 62443 文書は，当初は ISA99 規格として発行されていた．ISA99 は，国際計測制御学会 ISA の中で制御セキュリティの標準化を推進している委員会である．ISA99 規格文書は，2010 年から米国国家規格協会(ANSI)の文書として公開され，ANSI/ISA 62443 シリーズに規格番号が変更された．ANSI は ANSI/ISA 62443 シリーズの規格文書は ISA が作成する，としているが ANSI 規格の一部として発行している.

ISA99 委員会で作成された ISA/IEC 62443 シリーズの規格草案は ISA での投票・承認を経て，ANSI から ANSI/ISA 62443 として刊行される.

2.2 ISA/IEC 62443 シリーズと認証プログラム

この節では，ISA/IEC 62443 シリーズを構成する文書のうち，主な文書 3 つを紹介する．これらの文書は，ISASecure®認証スキーム(後述)の Web サイトに公開されている[2]．ISA は ISASecure®認証推進組織(後述の ISCI)を通じて認証スキームを提供している.

2.2.1 CSA-311

CSA-311, Component Security Assurance - Functional security assessment for components, version 1.11. この文書は，IACS を構成するコンポーネント，具体的には組み込み機器，ネットワーク・コンポーネント（ルータやファイアウォールなど），ホスト・コンポーネント（運用ネットワークに接続された PC など），およびソフトウェア・アプリケーションに対するサイバーセキュリティの技術的要求事項を示している.

2.2.2 SSA-311

SSA-311, System Security Assurance - Functional security assessment for systems, version 1.82.
この文書は，制御システムのサイバーセキュリティ要件を規定している.

2.2.3 SDLA-312

SDLA-312，Security Development Lifecycle Assurance - Security Development Lifecycle Assessment, version 5.7
この文書は，IACS で使用される製品の安全な開発のためのプロセス要件を規定している．また，安全な製品を開発し，維持するための安全な開発ライフサイクルを定義している.

2.3 ISA Global Cybersecurity Alliance

2019年にISAはISA/IEC 62443シリーズの利活用を推進するために, ISA Global Cybersecurity Allianceを設立した．[4]

3　IEC 62443

IEC62443シリーズは複数の規格文書で構成されており，そのうち下記3つの文書はセキュリティに大きな影響を与えている．

- IEC 62443-4-2，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．IACS コンポーネントの技術的セキュリティ要件．この文書は，上記のCSA-311文書と類似している．
- IEC 624433-3，産業用通信ネットワーク－ネットワークおよびシステムセキュリティ．システムセキュリティ要求事項およびセキュリティレベル．この文書は，上記のSSA-311 ISA文書と類似している．
- IEC 62443-4-1，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．安全な製品開発ライフサイクル要求事項．この文書は，上記の SDLA-312 文書と類似している．

IEC自身は, IEC 62443シリーズへのコンプライアンス認証は行っていない. TUV SUD, Tuv Rheinland, Dekraなどの，コンサルティングやコンプライアンス認証を提供する民間企業がある．

4　ISA/IEC 62443 と IEC 62443 の比較

ISA 規格と IEC 規格の内容は非常に類似している，ISA 規格は IEC の要求事項を拡張して説明とテスト情報を追加し，いくつかの条項を削除して追加し，いくつかの要求事項を追加している．最も注目すべきは，ISA SDLA-312 には構成管理のセクションがあるが，IEC62443 にはこれに対応する記述がないことである．

5　ISASecure®認証

ISA Security Compliance Institute (ISCI) は，ISASecure® 適合性認証プログラムを管理する非営利のオートメーション制御業界団体である．ISASecure®は，産業用オートメーションおよび制御（IAC）製品とシステムを独自に認証し，ネットワーク攻撃に対して堅牢で，既知の脆弱性がないことを保証する．ISASecure®プログラムは，ISA/IEC 62443 で定義された IAC セキュリティライフサイクルに基づいている．ISCI は，ISA/IEC 62443 に合わせて 4 つのセキュリティ保証レベル(SAL)を持つ 3 つの認証を提供している．

- ISASecure® Component Security Assurance (CSA)認証 – この認証は，2019 年 8 月 28 日から開始され，従来の EDSA 認証制度を拡張して，組み込み機器も含めたコンポーネント製品に対するセキュリティ認証制度である．4 段階のセキュリティレベルを規定している．CSA 認証は以下の 3 つの観点から評価を行う．
  - ・ソフトウェア開発プロセスのセキュリティ評価（SDLPA-C 及び SDA-C）
  - ・機能的セキュリティ評価（FSA-C）
  - ・脆弱性テスト（実装時の脆弱性特定、VIT-C ）

  CSA-311 Functional Security Assessment for Components と SDLA-312 Security Development Lifecycle Assessment は，CSA 認証の基準文書の中で中心的で重要な位置を占める．

- ISASecure® System Security Assurance (SSA)認証 - この認証は，産業制御システムパッケージ製品(例：SCADA，DCS，SIS)のサイバーセキュリティを認証対象としている．機能的セキュリティ評価(FSA-S)など 3 つの観点から評価を行い，4 段階のセキュリティレベル認証を実施する． SSA-311 Functional Security Assessment for Systems と SDLA-312 Security Development Lifecycle Assessment は，SSA 認証の基準文書の中で中心的で重要な位置を占める．
- ISASecure® Security Development Lifecycle Assurance (SDLA)認証 -組み込み機器内ソフトウェアの開発とメンテナンスがセキュアなプロセスであることを認証する. SDLA 認証を取得済みのサプライヤー開発組織は，特定の製品の CSA 認証または SSA 認証の評価を受ける際に，CSA または SSA の SDLPA (Security Development Lifecycle Process Assessment)要素を満たしているものとされる．SDLA-312 Security Development Lifecycle Assessment は，SDLA 認証の基準文書の中で中心的で重要な位置を占める．

ISASecure®は，コンポーネント，システム，開発組織向けに発行した認証(certificates)のリストを保持している．ISASecure®認証スキームのスキームオーナ(scheme owner)は ISCI であり，日本では公益財団法人 日本適合性認定協会 (JAB)が認定機関(Accreditation bodies)を務めている．認証機関として JAB から認定された(Accredited)認証機関(Certification Bodies)には，技術研究組合制御システムセキュリティセンター CSSC 認証ラボラトリーがある[6][7]．この他の認証機関として，アメリカで認定された Exida 社，ドイツで認定された TÜV Rheinland 社などの企業がある[5].

6 “62443”認証とは何か?

“62443”認証を取得している，と企業がプレスリリース等で記載しているとき，それはどの標準規格の認証取得を意味しているのだろうか? これまでの説明にあるように，それはケースバイケースである．

この分野の多くの大手企業や著名企業がそうであるように，企業は 1 つの規格の認証を取得することも，両方の規格の認証を取得することもできる．企業が特定の認証を持っていると主張している場合でも，公式のプレスリリースでさえ，ある規格を別の規格と間違えることがあるため，認証書自体を確認する必要がある．例えば，Rockwell は IEC 62443 のセキュリティ認証を受けたが，プレスリリースでは ISA/IEC 62443 のセキュリティ認証を取得した，と発表していた.

7 62443 シリーズのセキュリティ要件の概観

7.1 セキュリティ要件

62443 規格のセキュリティ要件は，主に 3 つのグループに分類することができる.

- システムの構成デバイスに対する技術的なセキュリティ要件 - デバイスのハードウェアとソフトウェアの実装に対するセキュリティ要件で，識別と認証の制御，アクセス制御，システムの完全性，データの機密性，リソースの可用性，イベントへのタイムリーな応答などの基本的なセキュリティ機能を含む.
- システムの技術的なセキュリティ要件（展開，境界線，クラウド，他の外部関係者との通信など）．これまでの一連の要件とは異なり，これらの要件は，主に組織のネットワークを全体として見て，ネットワークセキュリティを扱っている．ネットワークのセグメンテーションと分離は，これらの要求事項全体に大きく関わっている.

- システムとそのコンポーネントの開発とライフサイクルのための手続き的要求事項 - これらは，手続きと文書化のための要求事項である．これらの要求事項は，安全な設計と実装，検証(verification)と妥当性確認(validation)，欠陥，インシデント，更新の管理など，製品の開発と配備の各段階におけるセキュリティ手順の実践を定義している．

多くの企業はコンポーネントや開発プロセスのみを認証取得しているが，完全な認証プロセスには 3 つのグループすべての要件が含まれる．

7.2 セキュリティレベル

コンポーネントとネットワーク要件には 4 つのセキュリティレベルがあり，各 IEC 要件には，どの部分がどのセキュリティレベルに対応しているかの説明が含まれている．ISA/IEC 要件のセキュリティレベルは，表で指定されている．

セキュリティレベルは， 1 から 4 の順に上昇し，IACS が安全であることの信頼性を測定する．レベルが上がるごとに，より強力な認証(authentication)方法を追加したり，レベル 3 と 4 ではハードウェアセキュリティを導入したりすることで，下位のレベルよりも安全性を高めている．より高いレベルになると，より複雑なソリューションが必要となり，実装が困難な場合もある．各レベルには，下位のレベルのすべての要件が含まれている．

8　Vdoo ソリューションの貢献 [3]

Vdoo では，お客さまのデバイスセキュリティニーズを迅速かつ効率的に満たすためのお手伝いをしており，これには業界標準に準拠したコンプライアンスの達成と検証も含まれる．Vdoo プラットフォームは、複数の方法でコンプライアンスの取り組みを加速し，簡素化するのに役立つ．

まず，自動化されたデバイスセキュリティ解析機能がある．このプラットフォームは，デバイスに関連するセキュリティ問題を識別し，その解決状況を自動的にチェックする．これらの問題は，ISA/IEC および IEC 62443 規格の両方のセットを含む数十の業界標準の要件に明示的にマッピングされている．そのため，IACS コンポーネントなどの IoT 製品のファームウェア(バイナリイメージのみ，ソースコード不要)をクイックスキャンすると，これらの規格の技術的なセキュリティ要件の多くにマッピングされたセキュリティ要件への適合性に関する詳細な情報が得られる．例えば，製品がユーザ認証やアクセス制御の要件に準拠しているかどうかを確認することができる．

第二に，Vdoo は，コンプライアンスの状況を評価し，コンプライアンスを達成するために解決する必要があるセキュリティ問題を特定することを支援するだけでなく，未解決の問題を解決するための明確なガイダンスを提供している．ステップバイステップの指示により，製品のセキュリティと開発チームは，コンプライアンスのギャップに迅速に対処することができる．

第三に，Vdoo プラットフォームには，62443 シリーズなどの標準規格のセキュリティ要件に対応した複数の機能が含まれている．例えば，自動化されたセキュリティ分析レポートは，デバイスソフトウェアコンポーネント，CVE，デバイス設計上のセキュリティ上の問題点(security exposures)，潜在的なゼロデイ脆弱性，に関する詳細な情報を提供し，問題のステータスと変更の追跡をサポートする．デバイスに搭載する組み込みランタイム保護機能エージェントは，デバイスリソースの使用状況の追跡やアラートなどのランタイムセキュリティをサポートし，継続的なモニタリング機能は，脆弱性のモニタリン

グやアラート要件をサポートする.

9　結論

本稿では，62443 シリーズの主な標準化団体、標準規格と認証プログラム，及びそれらの関係をレビューした．それらの相違点と類似点，構造，セキュリティ関連の内容を分析した結果，類似性のレベルが非常に高いことがわかった．62443 規格の特定のセットとその背後にある標準化団体にかかわらず，より安全な IACS 製品を市場に投入し，将来の接続された産業環境の安全性と運用性を確保する上で，62443 シリーズの規格の重要性と影響力に疑いの余地はない.

謝辞

本稿は，Vdoo 社ブログ[3]を翻案して作成した．翻案を許諾いただいたビドゥジャパン株式会社に感謝の意を表する.

参考文献

[1] ISA/ISAGCA, “Quick Start Guide: An Overview of ISA/IEC 62443 Standards, Security of Industrial Automation and Control Systems”,
https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf (参照 2021-01-05)

[2] ISASecure®, IEC 62443 Conformance Certification
https://www.isasecure.org/en-US/Certification (参照 2021-01-05)

[3] Anna Schnaiderman, “Deconstructing the 62443 Series of Standards for Industrial Automation Control Systems”, The Vdoo Blog
https://www.vdoo.com/blog/industrial-automation-control-systems-62443-standard (参照 2021-01-05)

[4] ISA Global Cybersecurity Alliance
https://isaautomation.isa.org/cybersecurity-alliance/ (参照 2021-01-05)

[5] ISASecure®, Accredited ISASecure® Certification Bodies,
https://isasecure.org/en-US/Certification-Bodies/Accredited-ISASecure-Certification-Bodies (参照 2021-01-05)

[6] 公益財団法人 日本適合性認定協会 (JAB), 製品認証機関の認定(ISO/IEC 17065) >認定された製品認証機関 >技術研究組合制御システムセキュリティセンター CSSC 認証ラボラトリー
https://www.jab.or.jp/system/service/product/accreditation/detail/520/ (参照 2021-01-05)

[7] 公益財団法人 日本適合性認定協会 (JAB), JAB PD363:2015 第 2 版, 「認定の基準」についての分野別指針－セキュア制御製品及び開発ライフサイクル・プロセス－
https://www.jab.or.jp/service/product/bal/ (参照 2021-01-05)