CSMS

Cyber Security Management System

サイバーセキュリティマネジメントシステム

適合性評価制度の概要

CSMS認証基準（IEC 62443-2-1：2010）対応版

CSMS

一般財団法人 日本情報経済社会推進協会

1 CSMS適合性評価制度の目的

CSMS(Cyber Security Management System)適合性評価制度(以下、CSMS制度※1という)は、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)を対象としたサイバーセキュリティマネジメントシステムに対する第三者認証制度※2である。CSMS制度は、わが国の制御システムセキュリティの向上に貢献するとともに、利害関係者からも信頼を得られるセキュリティ対策を確保し、維持することを目的としている。

※1：CSMS制度における「CSMS」とは、制御システムに関するセキュリティマネジメントシステムのことである。(2014年4月25日付経済産業省発行ニュースリリース)

※2：CSMS制度の確立については、経済産業省の平成24年度補正予算事業「グローバル認証基盤整備事業」のテーマの一つとして実施した「制御システムセキュリティ認証基盤整備事業」の成果を活用している。

2 CSMSの概要

制御システムセキュリティ対策の必要性

IACSとは、エネルギー分野(電力、ガス等)や石油・化学、鉄鋼等のプラント、鉄道等の交通インフラ、機械、食品等の生産・加工ライン、ビルの管理システムなど社会・産業基盤を支える産業用オートメーション及び制御システムである。

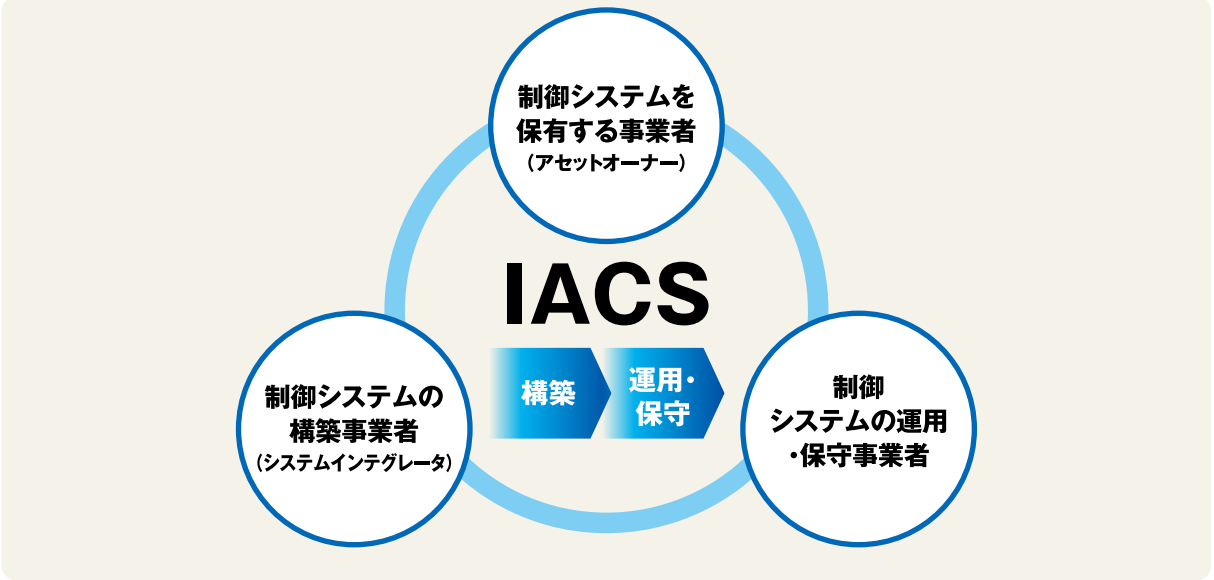
IACSは、従来、専用システムで構成され、外部ネットワークとは接続されていないことから、セキュリティ上の脅威は殆ど意識されていなかったが、近年、業務システム向けに開発された汎用技術(PCやサーバの基盤環境、TCP/IP等のプロトコル等)、ネットワーク(遠隔操作、遠隔保守等)、メディア(データ抽出、パラメータ変更)の活用が進んだ結果、IACSがサイバー攻撃の対象となりうる状況にある。

このようなことから、IACSがサイバー攻撃を受けて停止した場合、社会インフラやビジネスの継続に深刻な影響を及ぼすだけでなく、HSE※3に対する深刻な影響が生じる可能性もある。したがって、組織のIACSをサイバー攻撃から守るためのセキュリティ対策を適切に管理する上で、CSMSの導入はもはや不可欠となっている。

※3：Health(健康)、Safety(安全) and Environment(環境)の頭文字であり、就業者及び周辺コミュニティの健康及び安全性を保護し、高い環境レベルを管理・維持する責任。(IEC 62443-2-1 3.1.16による定義)

CSMSの対象者

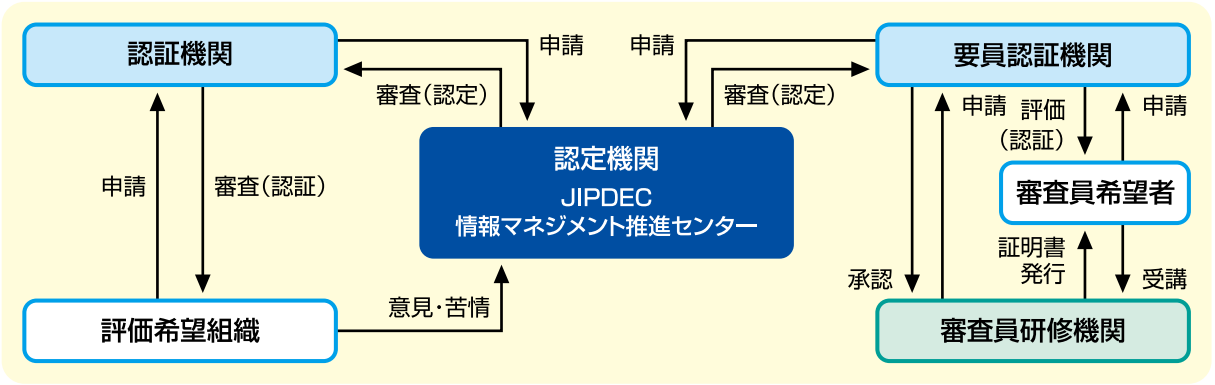
CSMSの対象者は、制御システムのライフサイクルを考慮し、制御システムのオーナーである事業者に加え、システムの構築や運用開始後のシステム改修、維持保全を分担する事業者及びシステムインテグレータとする。



3 CSMS適合性評価制度の運用

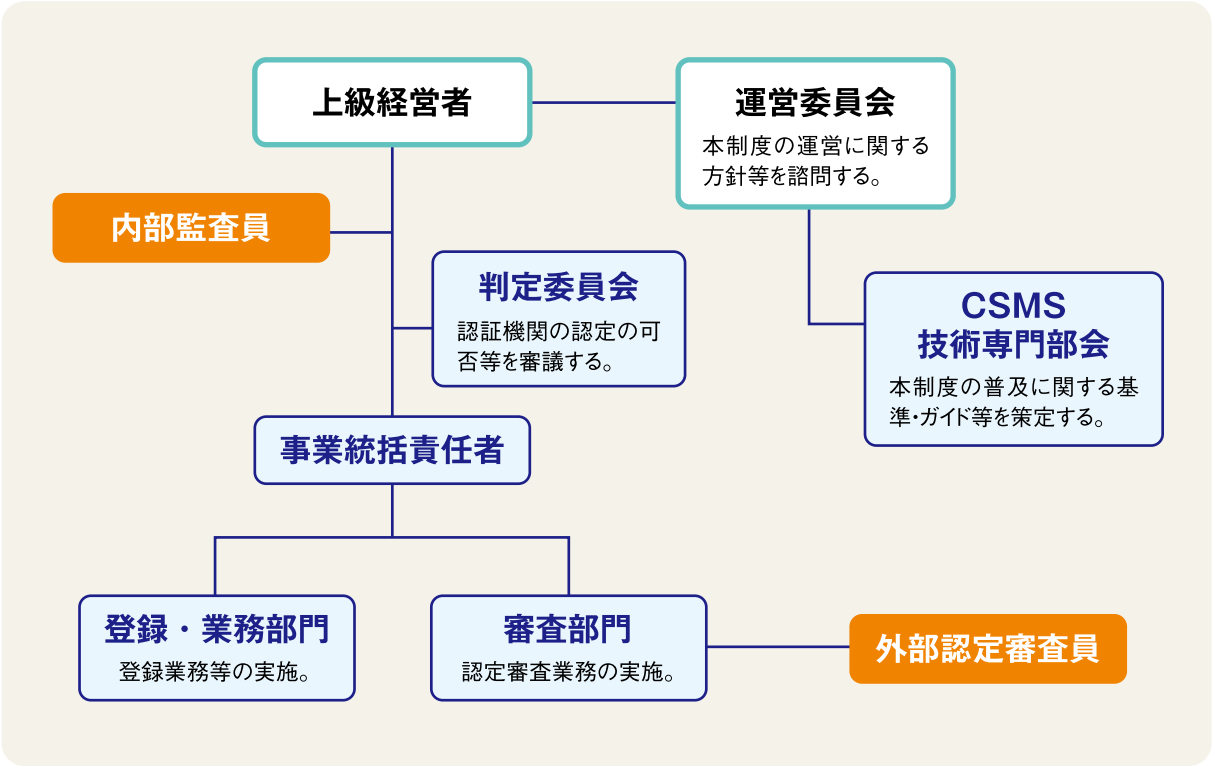
CSMS制度は、組織が構築・運用するCSMSがCSMS認証基準に適合しているか認証審査し登録する「認証機関」、審査員の資格を付与する「要員認証機関」、及びこれらの各機関がその業務を行う能力を備えているかを見る「認定機関」からなる総合的な運用の仕組みである。

適合性評価制度の運用体制



CSMS制度の公平性・透明性・客観性の確保

CSMS制度の運用については、その公平性、透明性、及び客観性を確保するために、JIPDEC組織運営機構の中に学識経験者及び業界団体の有識者等から構成される「運営委員会」、その下部組織である「技術専門部会」を設置している。また、認証機関や要員認証機関の認定の可否等を審議する有識者からなる「判定委員会」を設置している。これらの詳細は、URL:http://www.isms.jipdec.or.jp/org/index.htmlを 参照のこと。



4 CSMS構築・運用のメリット

組織が、CSMSを構築・運用することによるメリットとしては、次のようなことがあげられる。

●サイバー攻撃に対するリスクの低減

CSMSの構築・運用を通じて、社内においてリスクマネジメントに対する理解が進むとともに、セキュリティに対する目的意識の高い取組みが期待できる。また、CSMSに基づくセキュリティ対策を実施することで、サイバー攻撃に対するリスクを低減することができる。

●IACSの運用担当者に対するセキュリティ管理策の行動指針の徹底

IACSの運用担当者に対して、行動指針を徹底することで、ヒューマンエラーや組織に起因するセキュリティインシデントの発生可能性を低減することができる。また、インシデント訓練など教育カリキュラムを実施することで、セキュリティに対する意識の向上を図ることができる。

●セキュリティ対策の継続的改善が可能

CSMS構築・運用により、企業内セキュリティガイドラインの改訂とともに、企業内の各事業所の間で運用実態が明確になり、継続的な改善を行うことができる。また、制御システムセキュリティに関する提案・設計・納入・設置について信頼性や説得力を付加することができる。

5 CSMS認証取得のメリット

組織がCSMS認証を取得することによるメリットとしては、次のようなことがあげられる。

●サイバーセキュリティ管理体制の客観的な証明が可能

CSMS認証取得により、組織のサイバーセキュリティ管理体制の強化だけでなく、対外的にも事業者としての社会的責任を果たしていることの客観的な証明を得ることができる。

●第三者の視点でセキュリティチェック

認証機関の審査員による第三者監査を通じて、セルフチェックでは見えにくい新たな気づきを得ることができる。

●組織のブランド力の強化

インテグレータとして納入するシステムが、高いセキュリティ状態で構築できることについての第三者証明を得ることになるので、組織のブランド力が強化される。

6 CSMS認証基準

IACSの構築・運用を担う組織にとって、セキュリティの根本的な向上の為には、セキュリティマネジメントシステムの仕組みが必要となる。IEC 62443シリーズでは、制御システムセキュリティ実現に活用できる基準の一つである、IACSのためのセキュリティマネジメントシステムとしてIEC 62443-2-1が規格化されている。このIEC 62443-2-1に基づき、IACS分野のセキュリティマネジメントシステム認証基準として「CSMS認証基準（IEC 62443-2-1:2010）」（以下、「CSMS認証基準」という）が策定された。

■IEC 62443シリーズ

- IEC 62443-1：この規格全体の用語・概念等の定義
- **IEC 62443-2：組織に対するセキュリティマネジメントシステム**
- IEC 62443-3：システムのセキュリティ要件や技術概説
- IEC 62443-4：部品（装置・デバイス）層におけるセキュリティ機能や開発プロセス要件

7 CSMS認証基準の構成

CSMS認証基準は、組織が事業活動全般及び直面するリスクに対する考慮のもとで文書化したCSMSを確立、導入、運用、監視、レビュー、維持及び改善するための一般要求事項を定めている。CSMSに要求される要素は、IACSをサイバー攻撃から保護するためである。それらの要素は、次のカテゴリで構成される。

■4.2　リスク分析

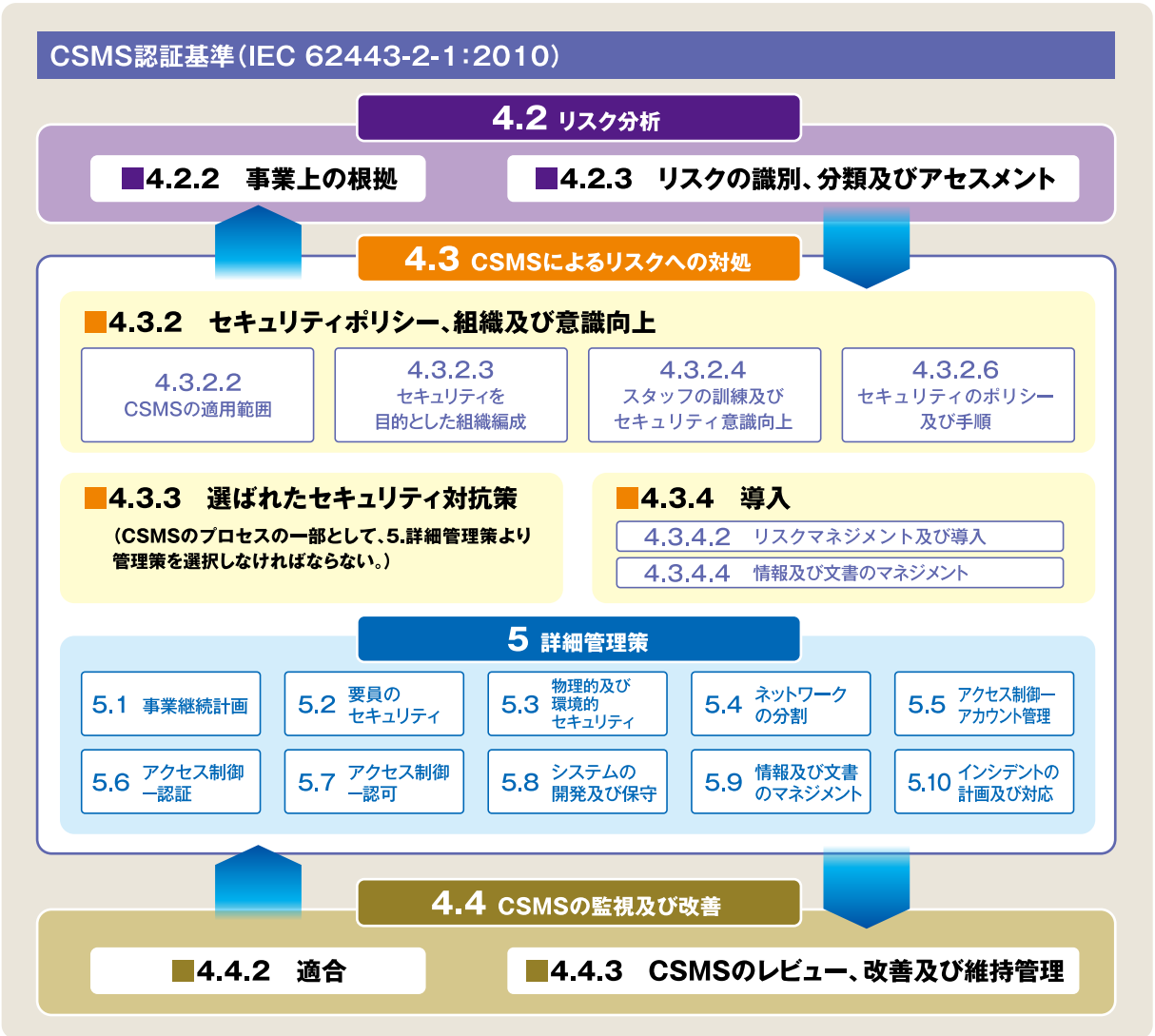
- 4.2.2　事業上の根拠：IACSのサイバーリスクに対処するため組織の固有のニーズを識別及び文書化する。
- 4.2.3　リスクの識別、分類及びアセスメント：組織が直面している一連のIACSのサイバーリスクを識別し、これらのリスクの可能性及び重大度のアセスメントを行う。

■4.3　CSMSによるリスクへの対処

組織は、CSMSのセキュリティ対抗策として、「5.詳細管理策」より管理策を選択しなければならない。選択した管理策及びそれらを選択した理由、並びに管理策の中で適用除外とした管理策及びそれらを適用除外とすることが正当である理由を示した「適用宣言書」を作成しなければならない。

■4.4　CSMSの監視及び改善

- 4.4.2　適合：組織向けに開発されたCSMSに従っていることを確実にする。
- 4.4.3　CSMSのレビュー、改善及び維持管理：時間の経過に合わせてCSMSがその目標に合致し続けることを確実にする。

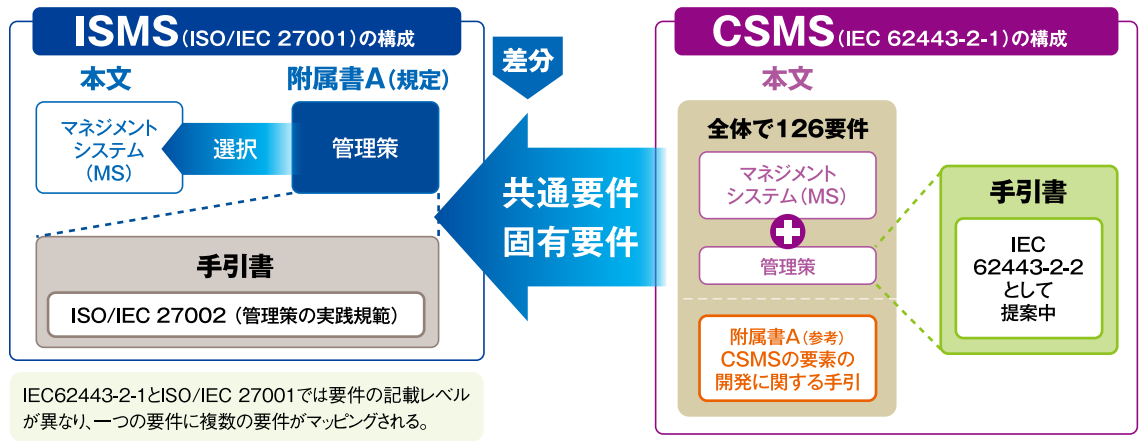


8 CSMSとISMSの関係

IEC 62443-2-1はISO/IEC 27001を参考に、制御システムに固有の部分を追加して作成されていることから、同様の要件が多数記載されている。そのため、ISMS（Information Security Management System）認証を既に取得している企業では、CSMSの大多数の要件を満足しているものと考えられる。

ISMSでは守るべき情報の流出を問題視し、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）を「CIA」の順番で重視される場合が多いが、CSMSでは最も避けるべき事態として操業の中断を挙げており、「AIC」の順番で重視するとともにHSEを考慮しているのが特徴である。

IEC 62443-2-1とISO/IEC 27001との比較



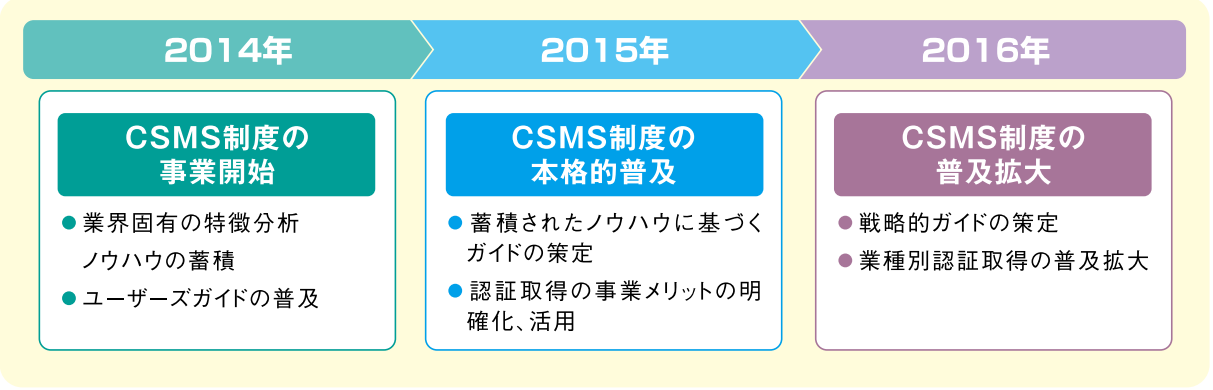
IEC62443-2-1とISO/IEC 27001では要件の記載レベルが異なり、一つの要件に複数の要件がマッピングされる。

出典：IPA「制御システムにおけるセキュリティマネジメントシステムの構築に向けて」2012年10月

9 CSMS制度の普及

マネジメントシステムの観点から、CSMSの構築・運用は制御システムに対するセキュリティ対策の実効性を継続的に向上させる効果があるため、CSMSの普及を促すことが、産業・社会基盤として重要な手段である。今後、認定された認証機関によるCSMS認証サービスを普及させることにより、制御システム事業者等が、国際的にビジネスを進める上で戦略的にCSMS認証を活用することが望まれる。

また、制御システムのオーナーや運用・保守事業者、システムインテグレータの多くの事業者がCSMS認証を取得することで、社会全体の制御システムのセキュリティ対策が持続的に向上することが期待できる。

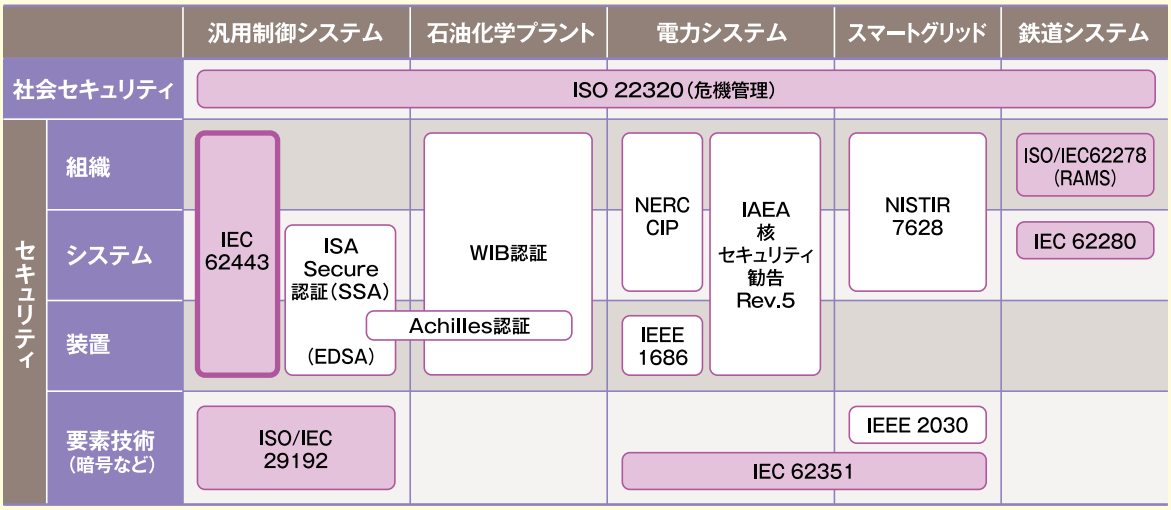


10 制御システムセキュリティ関連規格

制御システム分野では、汎用的な規格であるIEC 62443シリーズ以外にも、スマートグリッドを含めた電力やガス、上・下水道、鉄道、航空などの重要インフラ分野、あるいは制御システムの比率の高い製造業の各分野における制御システムセキュリティの業界標準がある。その中でも、CSMSは広く業界に応用可能である。

CSMS関連規格の概要

（出典：2014.3 Vol.96 No.03日立評論 ）



※略語説明：SSA(System Security Assurance),EDSA（Embedded Device Security Assurance）,NERC（North American Electric Reliability Corporation）,CIP（Critical Infrastructure Protection）,IAEA（International Atomic Energy Agency）,NISTIR（National Institute of Standards and Technology Interagency Report）,RAMS（Reliability,Availability,Maintainability and Safety）

11 IEC 62443シリーズの動向

制御システムのオーナーや運用・保守事業者、システムインテグレータの組織を対象としたのが、CSMS認証である。これに対して、製品・機器を対象としているのが、EDSA認証であり、ISA Security Compliance Institute（ISCI）が、制御システムコンポーネント（製品）認証プログラムを実施している。そのベースとなった基準をIEC 62443シリーズに反映している。

IEC 62443規格化の状況

（2014年3月現在）

区分	主対象者	規格名	原本名
共通	全体	IEC/TS 62443-1-1:2009	Terminology, concepts and models
		IEC/TR 62443-1-2	Master glossary of terms and abbreviations
		IEC 62443-1-3	System security compliance metrics
		IEC/TR 62443-1-4	IACS security life cycle and use case
セキュリティプログラム	事業・運用者	IEC 62443-2-1:2010	Establishing an industrial automation and control system security program
		IEC 62443-2-2	Operating an industrial automation and control system security program
		IEC/TR 62443-2-3	Patch management in the IACS environment
		IEC 62443-2-4	Requirements for IACS solution suppliers
システム	構築事業者	IEC/TR 62443-3-1:2009	Security technologies for industrial automation and control systems
		IEC 62443-3-2	Security levels for zones and conduits
		IEC 62443-3-3:2013	System security requirements and security levels
部品	装置ベンダ	IEC 62443-4-1	Product development requirements
		IEC 62443-4-2	Technical security requirements for IACS components

※ドラフトのタイトルについては、変更される可能性がある。

参考：独立行政法人情報処理推進機構

登録第5662324号

● CSMS制度に関する問合せ先 ●

〒106-0032　東京都港区六本木一丁目9番9号　六本木ファーストビル内
一般財団法人　日本情報経済社会推進協会　情報マネジメント推進センター
TEL　03-5860-7570　FAX　03-5573-0564
URL　http://www.isms.jipdec.or.jp/

文書番号：JIP-CSMS120-1.0

JIPDEC

一般財団法人　日本情報経済社会推進協会

〒106-0032 東京都港区六本木一丁目9番9号 六本木ファーストビル内
TEL 03-5860-7551　FAX 03-5573-0560
URL http://www.jipdec.or.jp/

April 2015