Vol.2017-EIP-75 No.14
2017/2/17

製造業における情報資産の定義および管理体制に関する考察

嶋谷 拓弥[†1]　原田 要之助[†1]

概要：産業機器や家電製品はますます高機能化・多機能化が進み，内部に組み込まれている制御や監視など多種多様な組込みシステムが，インターネット等のオープンなネットワークに接続されるようになった．すなわち，パソコンと同様に，第三者による攻撃ターゲットになる可能性が高まっている．従来に比べ，組込みシステムで取り扱う情報の価値も向上しており．組込みシステムに関するセキュリティ対策は，社会全体で取り組むべき喫緊の課題と言えるが，資産として管理すべき情報の定義や管理体制については未だ曖昧なままである．本研究では，製造業における情報資産の定義および CSMS に関わる組織が実施すべき情報セキュリティ管理体制について考察を行った．

キーワード：組込みシステム，制御システム，ISMS，CSMS，ISO/IEC 27001，IEC62443

Consideration on the definition and management system of information assets in the manufacturing industry

TAKUYA SHIMATANI[†1]　YONOSUKE HARADA[†1]

Abstract: As for the Industrial equipment and the house electrical appliances are increasingly high performance and multi-functionality, but factors include that a wide variety of embedded systems is connected to the open network such as internet. As a result, as well as the personal computer, the possibility that the integration system becomes the attack target by the third party increases. The value of the information handled by the built-in system (i.e. embedded systems) has been added, security measures about the built-in systems are the urgent issue to be addressed by society. On the other hand, the definition and the management systems of the information assets for the built-in system remain still vague. In this paper, we defined the information assets in the manufacturing industry and considered the information security management system to be implemented by organizations involved in CSMS.

Keywords: control system, embedded system, ISMS, CSMS, ISO/IEC 27001, IEC62443

1. はじめに

マイクロプロセッサやメモリ等の半導体性能の向上に伴い，産業機器や家電製品は高機能化・多機能化が進んでいる．これらの機器には，制御用のコンピュータシステム（組込みシステム）が内部に組み込まれている．また，情報通信技術の進展により，多種多様な組込みシステムが，インターネット等のオープンなネットワークに接続されるようになった．（図 1.1）

この結果，個人では Web ショッピング履歴や高機能な家電製品を利用したプライバシー情報の管理，企業では工場にある産業機器の運用管理など，従来に比べ，組込みシステムで取り扱う情報の価値が向上している．

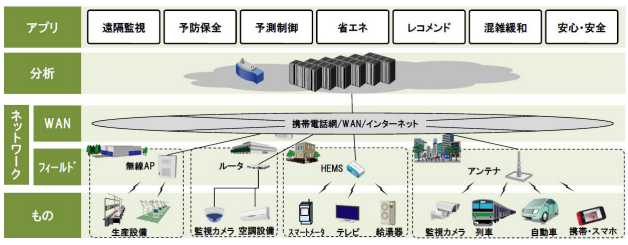

図 1.1　組込み機器のネットワーク化の例 [1]

[†1] 情報セキュリティ大学院大学
Institute of Information Security

従来のサイバー攻撃ではインターネット上でサービスを提供する情報システムが主な標的だったが，様々な組込みシステムがオープンなネットワークに接続したことで，情報システムと同様に，第三者の攻撃ターゲットになる可能性が高まっている．実際に起こったサイバー攻撃としては，図 1.2 に示す 2010 年にイラン核施設が Stuxnet と呼ばれるマルウェアに感染したことで，ウラン濃縮用遠心分離機が破壊されるという物理的実害にまで及んだ事例が有名である．[2] 従来，比較的安全だと信じられていた「インターネットに接続していない産業用制御システム」に対しても，Stuxnet は USB メモリーを介して感染・発症することから，産業用システムのセキュリティ管理のあり方を根本から考え直させた，という点で全世界に衝撃を与えた．

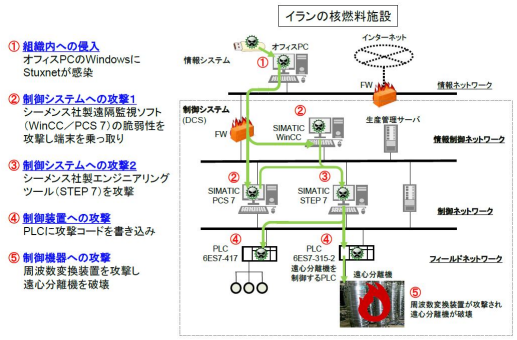

図 1.2 イラン核施設の Stuxnet（マルウェア）感染事例 [2]

こうしたサイバー攻撃事例を受け，組込みシステムの開発においても，外部からの攻撃や不正なデータ複製への対策，廃棄時の機密情報の削除等を考慮した実装が求められるようになってきた．しかし，組込みシステムの開発現場においては，市場における価格競争の激化に起因するコスト削減・開発期間の短縮・生産性向上が優先されがちであり，セキュリティへの対策が疎かにされやすい．元々，組込みシステムは一定範囲内に閉じられた環境・ネットワークで活用されており，それらを制御する制御システムも機械装置の一部と見なされていたため，情報システムでは当たり前のように講じられている情報セキュリティ対策が十分に取られていない．特に，社会基盤を支える重要インフラに用いられている組込みシステム，またそれらを制御する制御システムが攻撃されると，多大な人的被害が発生する可能性があるため，開発元のみならず，運用・管理者や利用者も含めた社会全体で取り組むべき喫緊の課題と言える． [3] [4] 社会全体で，特に製造業で多く使用される組込み機器のセキュリティについて考えるにあたっては，「誰が」「どの」情報を資産として管理するかが重要になる．本研究では，製造業における資産としての情報の定義および適切な管理体制・リスクコントロール策について，考察を行った．

2. 認証・規格について

2.1 CSMS 適合性評価制度

2.1.1 背景

産業機器および制御システム（IACS：Industrial Automation and Control System）は，エネルギー分野（電力，ガス等）や石油・化学等のプラント，鉄道等の交通インフラ，機械・食品等の生産ラインなど，社会産業基盤で幅広く利用されている．従来，IACS は専用のシステム・ネットワークで構成されており，外部ネットワークとは接続されていなかったため，外部からの悪意のあるサイバー攻撃を意識したセキュリティ対策がなされていなかった．

しかし，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 といったプロトコル等），ネットワーク（遠隔操作，遠隔保守等），メディア（データ移動，パラメータ変更）が IACS に対しても活用されるようになったことから，サイバー攻撃の対象となる状況になった．（図 2.1）

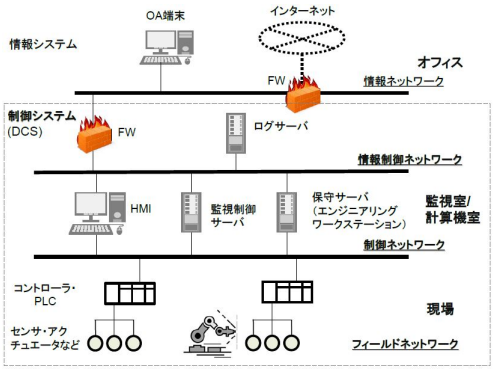

図 2.1 オフィスまでつながったプラント制御ネットワーク [7]

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だけでなく，HSE（Health Safety Environment：事業活動に伴う労働安全衛生・環境問題）に対しても深刻な影響が及ぶ可能性がある．こうした事態を受けて，IACS を構築・運用する上で，サイバーセキュリティ対策の確保を行うために，サイバーセキュリティマネジメントシステムの認証制度が検討された．[5] [6] [7]

2.1.2 目的・対象

CSMS（Cyber Security Management System：以下，CSMS という）適合性評価制度とは， IACS 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である．CSMS 適合性評価制度は制御システムセキュリティの向上に加え，組織の事業活動及び直面するリスクに対する考慮のもとで適切なリスク管理を行うことで，利害関係者からも信頼を得られるセキュリティ対策の確保・維持を目的として策定されたものである．そのため，CSMS 適合性評価制度は ISMS 適合性評価制度と同

様にリスクマネジメントプロセスを適用し、IACS のサイバーリスクに対処している．

CSMS 適合性評価制度の対象者は，図 2.2 に示すように，制御システムのライフサイクルを考慮した，保有事業者（アセットオーナー），運用・保守事業者，構築事業者（システムインテグレータ）の三者である．

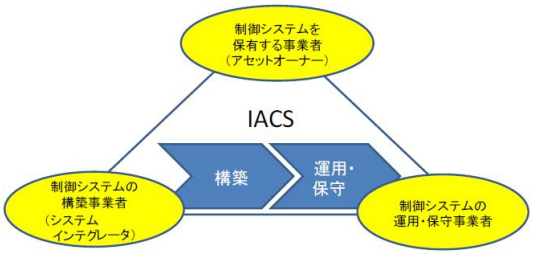

図 **2.2**　CSMS の対象者 [5] [6] [7]

2.1.3　認証基準

情報システムの管理・運用については，ISO/IEC 27001（Information Security Management System）の適用が一般的であるが，IACS については，その特徴や性質に配慮したセキュリティマネジメントの仕組みが必要である．そこで，ISMS をベースとした IACS のためのセキュリティマネジメントシステムが，IEC 62443-2-1 として規格化されている．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の認証基準として「CSMS 認証基準（IEC 62443-2-1）（JIP-CSCC100-1.0）」が策定された．IEC 62443 の構成を，表 2.1 に示す．

表 **2.1**　IEC 62443 シリーズの構成 [5] [6] [7]

IEC62443-1	規格全体の用語・概念の定義
IEC62443-2	組織に対するセキュリティマネジメントシステム
IEC62443-3	システムのセキュリティ要件や技術概説
IEC62443-4	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

また，制御システムにおける IEC 62443 シリーズのセキュリティ標準の全体像の例を図 2.3 に示す．[8] [9]

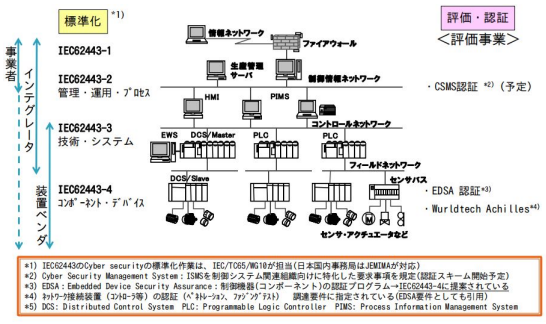

図 **2.3**　IEC 62443 シリーズのセキュリティ標準の位置付け [5] [6] [7]

CSMS 認証基準は，組織が事業活動全般および直面するリスクに対する考慮のもとで文書化した CSMS を確立し，導入・運用・監視・レビュー・維持・改善するための一般要求事項を定めている．IACS をサイバー攻撃から保護するため，CSMS に要求されるリスク分析と対処については，図 2.4 に示すカテゴリから構成される．

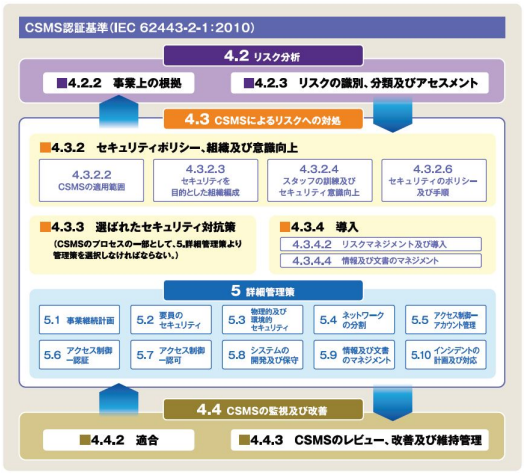

図 **2.4**　CSMS 認証基準の構成 [6]

2.2　現在の課題

CSMS 認証基準の格である IEC 62443-2-1 は，図 2.5 に示すように，ISO/IEC 27001（ISMS 認定基準）を基に，制御システムに固有の部分を追加して作成されているため，類似の管理要件が多数記載されている．そのため，既に ISMS 認証を取得している組織では，CSMS の大多数の管理要件をも満足していると考えられる．

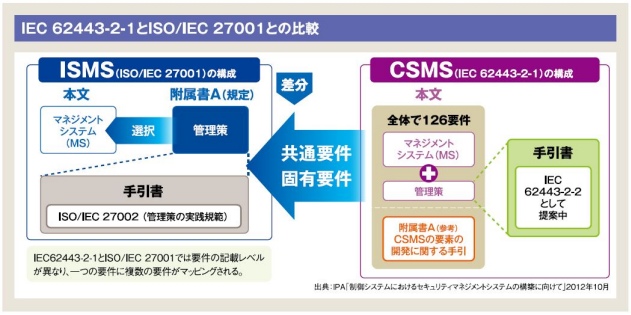

図 **2.5**　CSMS と ISMS の関係 [6]

さらに，ISO/IEC 27001 は 2013 年に改訂が行われている．CSMS の元となった IEC 62443-2-1 は ISO/IEC 27001：2005 がベースになっているため，2016 年時点では厳密に ISMS に準拠しているとは限らない．

ISMS では，情報自体を重要な資産と捉え，情報の機密性（Confidentiality），完全性（Integrity），可用性（Availability）の喪失に伴うリスクを特定し，必要に応じて効果的なリスク対策を実施することが重要と考えられている．

一方で，CSMS では，最も避けるべき事態として，「操業の中断」，そして「人命の安全」を挙げており，IACS の「可用性」の維持を重視するとともに，HSE に対するリスクを考慮することが特徴と言える．すなわち，ISMS と CSMS では，防ぐべきインシデントに関して，保護対象や情報の扱いに関して優先度が異なっていると考えられる．（表 2.2） [12]

表 2.2 CSMS と ISMS の保護対象と優先度のイメージ

保護対象	例	CSMS(Safety)	ISMS(Security)
人	命	高	小
	身体	高	小
	心	高	小
物	機械	中	中
	システム	中	中
金	金銭	中	中
情報	品質	小	高
	データ	小	高
	ソフトウェア	小	高

また，近年は遠隔監視サービスのように，製造者，遠隔監視事業者，利用者が異なるケースが出てきており，同じ運用履歴データに対して誰がどのデータに，いつアクセスできるかは契約や組織のルールによる場合が多い．特に今後，運用履歴データやセンサデータをクラウドデータとして集約しつつ，ビッグデータ解析事業者に送付してリアルタイムに分析して，新たな知見・情報を生み出すソリューション等のサービス形態も想定される．そうした場合，データの提供者が，「データを提供した結果，同種の製品向上につながった」という主張をする可能性もある．そのため，データや情報を，誰がどの単位で利用・管理するかが重要になるだろう．以上のように，現行の CSMS については，資産として管理すべき情報の定義および管理体制について明確に定まっておらず，組織別にルールや契約で個別対応しているものと考えられる．

また，ISMS ではベースとなる規格が，ISO/IEC 27001 : 2005 と異なり，リスクマネジメントを行う対象が「情報資産」から「情報」へと変わったことで，より情報という資産に関する定義と管理が困難になった．例えば，発電プラント等の組込み機器を多数持つ制御システムでは，個々の機器や設備に紐付けて「情報資産」と見なして管理していたが，「情報」はリアルタイムに生成される出力値・計測値や，機器自体の設定パラメータ等があるだろう．しかし，PLC の稼働値やセンサで取得した値等のデータを情報と見なすかどうか等，どのデータを重要度に応じてどこに分類し，管理すれば良いかを明確にすることには困難が伴う．すなわち，今後，IACS 分野のセキュリティ対策を考えるに当たって，CSMS 認証基準となっている ISO/IEC 27001 : 2005 と ISMS 認証基準となっている ISO/IEC 27001 : 2013 のどちらに準拠することが妥当か考える必要がある．

3. 国際認証規格に関する調査

3.1 ISMS と CSMS の要求事項の比較

本研究の調査方法として，CSMS 認証基準である IEC62443-2-1 と，IEC62443-2-1 のベースである ISO/IEC 27001 : 2005 と，最新改訂版の ISO/IEC 27001 : 2013 の要求事項を比較する． [13]

具体的には，IEC62443-2-1 固有の要求事項を抽出することにより，ISMS と CSMS で求められている内容との整合性を確認する．また，その結果を元に，CSMS に関わる組織（特に製造業）が，管理すべき情報の定義，および実施すべき管理体制とリスクコントロール策について考察する．

3.2 CSMS と ISMS の要求事項の比較結果

要求事項の比較結果については，星取表形式でまとめた．誌面の都合上，巻末付録に結果の表を示す．

4. 情報セキュリティ調査による実態調査

4.1 情報セキュリティ調査について

原田研究室では，2010 年より「情報セキュリティ調査」を実施している．2016 年度調査では，日本国内のプライバシーマーク（以下，P マーク）取得組織，ISMS 認証取得組織，官公庁，教育機関などから選んだ 4,800 組織（送達確認できたのは 4,704 組織）を対象にアンケートを実施した．2016 年度調査では，表 4.1 に示すように，組織の IT 資産管理の実態に関する設問を盛り込んだ．本結果を基に，組織の IT 資産管理状況と，今後必要となるセキュリティ対策・方針を考察する．

表 4.1 情報セキュリティアンケートの設問（抜粋）

Q19	業務で利用している IT 資産について、どの程度管理できていると考えていますか？
Q20	業務で利用している IT 資産について、どのようなセキュリティ対策を実施していますか？
Q21	IT 資産管理・運用に関して、どのようなセキュリティ課題や懸念事項がありますか？

4.2 情報セキュリティ調査による調査結果

2016 年度調査では，544 件（送達確認できた 4,704 組織に対し 11.6 %）の回答が得られた．なお，本論文においては回答の未記入および択一問題における重複回答等の無効回答は，無回答として計上している． [10] [11]

本研究では，CSMS に馴染みの深い組織，ISMS に馴染みの深い組織でどの程度 IT 資産管理状況が異なるかを見るために，業種で各設問に対しクロス集計を実施した．

具体的には，CSMS に馴染みの深い組織の代表業種として「製造業」，ISMS に馴染みの深い組織の代表として「情報通信業」，そして「その他」の 3 区分に分けた．

今回集計に使用した組織の業種と割合を，図 4.1 に示す．

次に，業務利用している IT 資産に関する管理状況の認識について，図 4.2，図 4.3 に示す．

また，業務利用している IT 資産に関するセキュリティ対策実施状況について，図 4.4 に示す．

そして，IT 資産管理・運用に関するセキュリティ課題・懸念事項について，図 4.5 に示す．

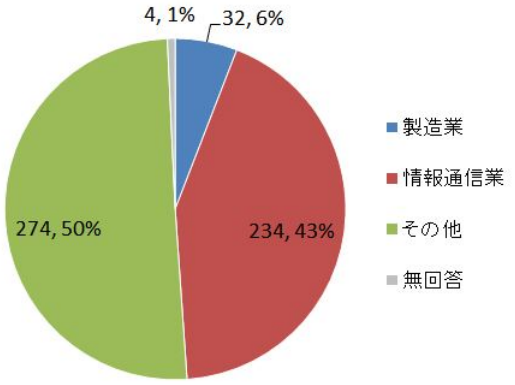

図 4.1 回答組織の業種（N=544）

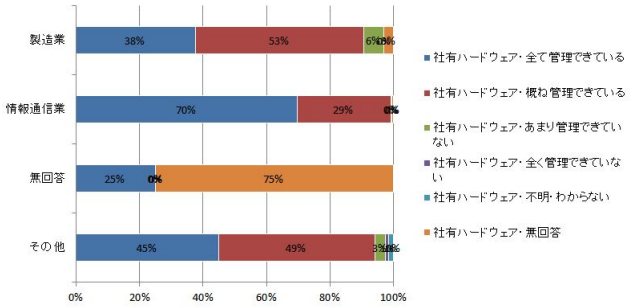

図 4.2 業種別：社有ハードウェアの管理認識（N=544）

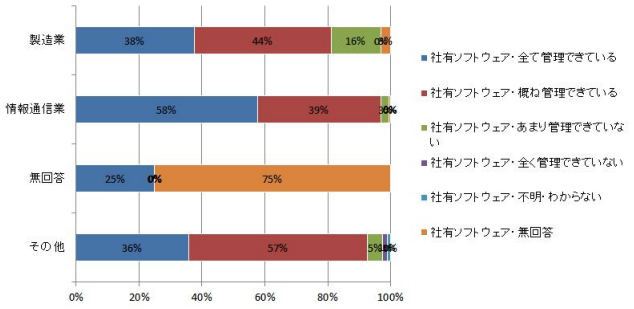

図 4.3 業種別：社有ソフトウェアの管理認識（N=544）

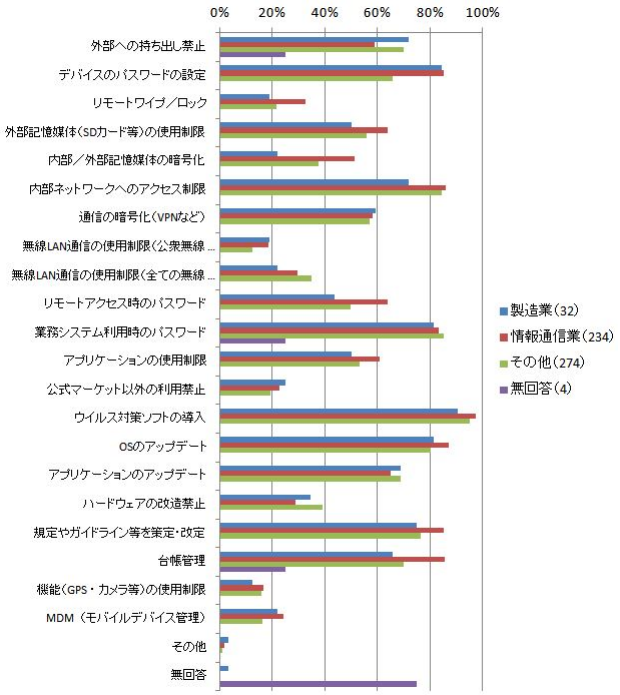

図 4.4 業種別：IT 資産のセキュリティ対策実施状況（N=544）

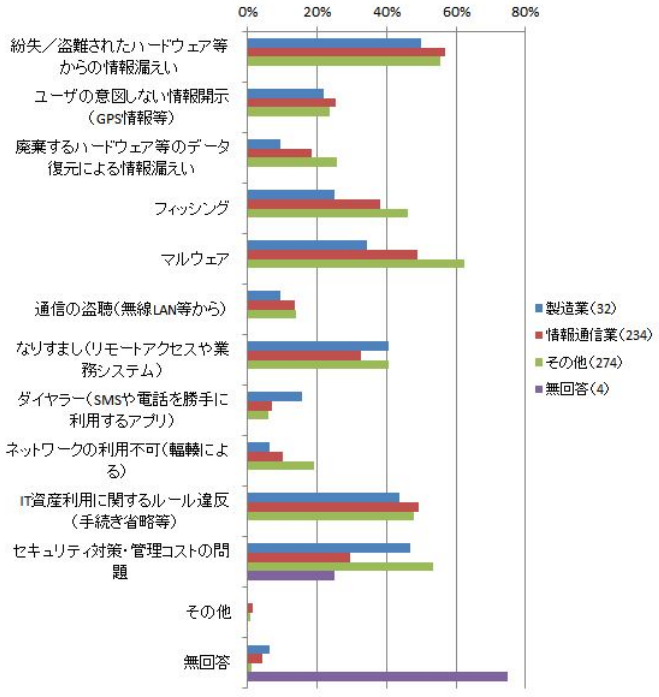

図 4.5 業種別：IT 資産管理・運用に関するセキュリティ課題・懸念事項（N=544）

5. 考察

5.1 CSMS と ISMS の要求事項の比較

CSMS と ISMS の要求事項の比較（固有要件事項の抽出）結果を見ると，固有要件としては大きく「リスクマネジメント（分析・対処・監視及び改善）」と「詳細管理策」の 2 つに大別されていると分かる．しかし，本研究の課題として挙げた「誰がどの情報を管理してよいか」については，いずれの固有要件においても触れられていなかった．正確には，詳細管理策において，要員のセキュリティやアクセス制御こそ固有要件があるものの，実際の中身としては「誰がどの情報を管理してよいか」が決定されているという前提で記述されている．リスクマネジメント（分析・対処・監視及び改善）の固有要件が，IACS 分野に限定した要求事項であるのに対し，詳細管理策は IACS 分野に限定するような書き方はほとんどされていない．つまり CSMS の要求事項では，資産としての情報の定義や管理体制については，リスクマネジメント，特にリスク分析の要求事項に包括されていると見なすべきであろう．ただし，リスクマネジメント実施後，CSMS の対象者である保有事業者（アセットオーナー），運用・保守事業者，構築事業者（システムインテグレータ）の三者で「情報の加工・取得・監視」を行う際，いかにしてセキュリティを確保するかの要件がなく，実質的には，CSMS の対象者が個別にリスクマネジメントを実施するだけに留まっている．

以上を踏まえると，現行の CSMS は，サイバー攻撃に対する組織内部のセキュリティマネジメントシステムとして，組織毎のセキュリティを確保するマネジメントシステムとしては使えるものの，IACS 製品に関わる組織間でのセキュリティを確保するマネジメントシステムとしては不十分と言わざるを得ない．

IACS 分野では，リアルタイムで情報が生産・加工されているが，例えば発電プラントの現場で発生したセンサ情報は，運用・保守事業者は必要であるものの，構築事業者（システムインテグレータ）にとっては必ずしも必要な情報ではなく，センサ情報を集約・加工した稼働実績情報が必要な情報である，という場合が多い．つまり，情報の生成から廃棄に至るプロセスとして，CSMS では「情報を生産する」という観点から，対象者それぞれにおける情報のリスクマネジメントを実施すべきであろう．

このことを踏まえて，筆者は CSMS のあるべき姿としては，「ISMS 適合性評価制度の認証取得」を前提とした制度に変革すべきと考える．CSMS と ISMS をつなぐこと自体は問題ないが，ISMS で組織内部での情報セキュリティマネジメントシステムが正しく構築されていることを担保し，その上で，CSMS で組織間での情報セキュリティマネジメントシステムが正しく構築されていることを担保する，という形が望ましいと考える．

実際，現場における情報のみでは，組織全体として，その情報がどれだけ重要な情報（意思決定や戦略に活用できる情報）かといったリスクを検討することは現実には難しい．そのため，CSMS では生産現場の情報そのものと，その情報を組織間で加工・活用する部分について管理し，ISMS では，センサ情報などの連続した生情報を用いずに，付加価値（工程管理情報，設備稼働情報，故障経歴情報等）を盛り込んだ情報のみを管理するというモデルが考えられるだろう．このモデルは，ISMS としては，加工された情報と付加価値情報を元に，重要度の判断やリスクマネジメントを実施することができ，現行の ISMS と大きく仕組みを変える必要がなく，CSMS ではデータの活用と組織間の情報セキュリティマネジメントに重きを置くことができ，ISMS との要求事項の重複も低減できると考えられる．

5.2 情報セキュリティアンケートによる実態調査

4.2 の結果を見ると，社有ハードウェア・ソフトウェアいずれにおいても，情報通信業（99 %・97 %）の方が製造業（91 %・82 %）に比べて「資産を管理できている・概ね管理できている」認識の組織の割合が高い．特にソフトウェアに対して，製造業は 80 %程度に留まっており，製造業の IT 資産管理はまだ十分ではない（遅れている）と言えるだろう．

また，セキュリティ対策実施状況としては，ウイルス対策ソフトの導入等は情報通信業も製造業も殆どの組織で実施しているものの，例えばリモートワイプ・ロックや無線 LAN の使用制限，MDM（モバイルデバイス管理）等，持ち運びが容易で遠隔監視・操作を容易にするモバイル端末については，セキュリティ対策があまり施されていないことが伺える．セキュリティ対策実施状況としては，概ね情報通信業と製造業で大きく差は無いものの，ほとんどの項目で情報通信業が実施割合が高い傾向にあることも分かる．

そして，セキュリティ課題・懸念事項としては，紛失／盗難による情報漏えいやマルウェア感染，IT 資産利用によるルール違反の項目が高い傾向にある．

両者の違いの特徴的な点として，マルウェア感染については，製造業は情報通信業よりも懸念している組織の割合が低い点である．Stuxnet の事例のように，制御システムがマルウェア感染によりサイバー攻撃を受けた事例こそあるものの，製造業の現場ではセキュリティ課題に挙げられていない．むしろセキュリティ対策や管理コストの問題について，製造業は情報通信業よりも意識が高い．すなわち，製造業の情報セキュリティ担当者は，限られた予算で本当に必要なセキュリティ対策を整理・実施することに手を焼いている状況が伺える．

以上をまとめると，製造業は情報通信業に対して資産管理や情報セキュリティ対策の実施等遅れている傾向にあると考えられる．CSMS では，対象者である保有事業者（ア

セットオーナー），運用・保守事業者，構築事業者（システムインテグレータ）の三者それぞれが情報セキュリティマネジメントを実施しない限り，そこがセキュリティホールとなってサイバー攻撃・重大事故が発生しかねない．その為，製造業，特に社会基盤となる重要インフラを支える製造業に対しては，早急に，より一層の情報セキュリティ対策を実施することが望まれる．

6. 今後の展望

本稿では，現行の CSMS と ISMS に対して，固有要件を抽出し，CSMS のあるべき姿と CSMS に関わる各組織（特に製造業）が考えるべき情報セキュリティ管理体制について考察した．本研究は対象製品分野を限定した場合の一考察であるため，今後は社会基盤を支える様々な重要インフラに対して，CSMS の観点から管理すべき情報やその管理体制を考察する．また，それらの考察から，対象製品分野に依らず横断的に利用可能な，情報セキュリティリスクをコントロールするためのフレームワークを検討する．

謝辞

本論文の作成にあたり，ご指導頂いた情報セキュリティ大学院大学の教授の方々，また多くの助言をいただいた原田研究室の客員研究員及びメンバーに，感謝致します．

情報セキュリティ調査を実施するにあたり，アンケートへの回答にご協力を頂きました企業や団体，組織の皆様，調査票の封入，データ入力に多大な協力を頂いた，神奈川県立麻生養護学校元石川分教室，神奈川県立相模原養護学校，神奈川県立相模原養護学校橋本分教室，神奈川県立高津養護学校川崎北分教室，神奈川県立鶴見養護学校岸根分教室，神奈川県立中原養護学校，神奈川県立みどり養護学校新栄分教室，川崎市立田島支援学校（五十音順），並びに本学事務局の皆様に感謝致します．

参考文献

[1] 日立製作所，内閣サイバーセキュリティセンター 第 1 回会合 資料 6-3 日立製作所 説明資料「IoT のセキュリティ」，http://www.nisc.go.jp/conference/cs/kenkyu/dai01/pdf/01shiryou0603.pdf，2015/04/06（最終参照日：2017/01/09）
[2] 国家間サイバー戦争の幕開け　イラン核施設を攻撃したマルウェア「Stuxnet」（2009〜10 年），eset マルウェア情報局，https://eset-info.canon-its.jp/malware_info/trend/detail/160308.html，2016/03/08（最終参照日：2017/01/09）
[3] 独立行政法人情報処理推進機構（IPA），情報セキュリティ 10 大脅威 2016〜個人と組織で異なる脅威，立場ごとに適切な対応を〜，2016
[4] 独立行政法人情報処理推進機構（IPA），組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版），2010
[5] 一般財団法人日本情報経済社会推進協会（JIPDEC），CSMS ユーザーズガイド − CSMS 認証基準（IEC62443-2-1）対応ー，2015
[6] 一般財団法人日本情報経済社会推進協会（JIPDEC），CSMS 適合性評価制度の概要，2014
[7] 一般財団法人日本情報経済社会推進協会（JIPDEC），CSMS 認証基準（IEC62443-2-1），2014
[8] 独立行政法人情報処理推進機構（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〜IEC62443-2-1 の活用のアプローチ〜，2012
[9] 一般財団法人日本規格協会（JIS），IEC62443-22-1 国際規格 産業用通信ネットワーク -ネットワーク及びシステムセキュリティ − 第 2-1 部：産業用オートメーション及び制御システムセキュリティプログラムの確立 第 1 版，2010
[10] 副島恵子ほか，“2016 年情報セキュリティ調査から見えてくる組織（民間企業・官公庁・教育機関）における現状”，情報セキュリティ大学院大学，http://lab.iisec.ac.jp/~harada_lab/survey.html，2016/12/28（最終参照日：2017/01/09）
[11] 副島恵子ほか，“2016 年情報セキュリティ調査から見えてくる組織（民間企業・官公庁・教育機関）における現状”，2017 年 暗号と情報セキュリティシンポジウム講演予稿集，2A2-3. 2017
[12] 独立行政法人情報処理推進機構（IPA），情報セキュリティセミナー　守るべき情報資産・情報リスクの考え方，2004
[13] 嶋谷拓弥，製造業における情報資産の定義および管理体制に関する考察，情報処理学会 第 74 回電子化知的財産社会基盤研究会 (EIP)，2016

付　　録

A.1 CSMS と ISMS の要求事項の比較結果

本文で実施した，CSMS と ISMS の要求事項の比較結果を以下に示す．

A： ISO/IEC 27001：2005 になく，IEC 62443-2-1 にだけある要求事項

B： ISO/IEC 27001：2013 になく，IEC 62443-2-1 にだけある要求事項

表 A·1: CSMS と ISMS の要求事項の比較

CSMS 認証基準 (Ver.1.2)			A	B
4		サイバーセキュリティマネジメントシステム		
	4.2	リスク分析		
		4.2.3 リスクの識別、分類およびアセスメント		
		4.2.3.2 リスクアセスメントの背景情報の提供	○	
		4.2.3.3 上位レベルのリスクマネジメントの実行		○
		4.2.3.5 単純なネットワーク図の策定	○	○
		4.2.3.11 物理的リスクのアセスメントの結果と HSE 上のリスクのアセスメントの結果とサイバーセキュリティリスクのアセスメントの結果の統合	○	○
		4.2.3.12 IACS のライフサイクル全体にわたるリスクアセスメントの実行	○	○
	4.3	CSMS によるリスクへの対処		
		4.3.2 セキュリティポリシー、組織及び意識向上		
		4.3.2.3.2 セキュリティ組織の確立	○	
		4.3.2.4.5 訓練プログラムの経時的な改訂	○	○
		4.3.2.6.3 リスクマネジメントシステム間の一貫性の維持	○	○
	4.4	CSMS の監視及び改善		
		4.4.3 CSMS のレビュー，改善及び維持管理		
		4.4.3.1 CSMS に対する変更を管理及び導入するための組織の割り当て	○	
		4.4.3.6 業界の CSMS 戦略の監視及び評価		○
		4.4.3.8 セキュリティ上の提案に対する従業員のフィードバックの要求及び報告	○	○
5		詳細管理策		
	5.2	要員のセキュリティ		
		5.2.3 要員の継続的な選別	○	○
		5.2.7 適切な抑制と均衡を維持するための職務の分離	○	
	5.3	物理的及び環境的セキュリティ		
		5.3.1 補助的な物理的セキュリティ及びサイバーセキュリティポリシーの確立	○	○
		5.3.10 重要資産の暫定的保護のための手順の確立	○	○
	5.5	アクセス制御－アカウント管理		
		5.5.5 不要なアカウントの一時停止又は削除	○	
	5.6	アクセス制御－認証		
		5.6.3 システム管理及びアプリケーション構成での強い認証方法の要求	○	
		5.6.5 適切なレベルでのすべてのリモートユーザの認証		○
		5.6.6 リモートログイン及びリモート接続のポリシーの策定		○
		5.6.7 失敗したりリモートログイン試行の後のアクセスアカウントの無効化	○	○
		5.6.8 リモートシステムの活動がなくなった後の再認証の要求		○

	5.6.9	タスク間通信での認証の採用	○	○
5.7		アクセス制御－認可		
	5.7.2	IACS 装置にアクセスするための適切な論理的及び物理的許可方法の確立	○	
	5.7.3	役割に基づくアクセスアカウントによる情報又はシステムへのアクセス制御	○	○
	5.7.4	重要な IACS に対する複数の認可方法の採用	○	○
5.8		システムの開発及び保守		
	5.8.4	システムの開発又は保守による変更に対するセキュリティポリシーの要求	○	○
	5.8.5	サイバーセキュリティ及びプロセス安全性マネジメント（PSM）の変更管理手順の統合	○	○
	5.8.6	ポリシー及び手順のレビュー及び維持管理	○	
5.9		情報及び文書のマネジメント		
	5.9.4	長期記録の取得の保証		○
	5.9.5	情報の分類の維持管理	○	
5.10		インシデントの計画及び対応		
	5.10.2	インシデント対応計画の伝達	○	○
	5.10.10	発見された問題に対する対処及び修正	○	
	5.10.11	演習の実行		○