Vol.2016-DPS-168 No.10
Vol.2016-SPT-21 No.10
Vol.2016-EIP-74 No.10
2016/11/18

# 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，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て．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，組込みシステムに対する情報の定義および適切な管理体制について考察するため，CSMS と ISMS の比較を行った．

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

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

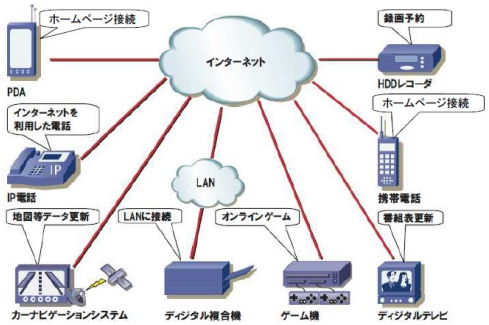
TAKUYA SHIMATANI[†1]　YONOSUKE HARADA[†1]

***Abstract***: Industrial equipment and appliances are increasingly high performance, multi-functionality, a wide variety of embedded systems is connected to the network. As a result, as well as the personal computer, there is a growing possibility that the third party of the attack target. Since the value of the information handled by the built-in system has been improved, security measures for embedded systems, it can be said that the urgent issue to be addressed by society. However, it is still vague for the definition and management system of information to be managed as an asset. In this paper, we compare CSMS with ISMS in order to discuss the definition and the appropriate management system of information for the embedded system.

***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り，パソコンと同様に，第三者の攻撃ターゲットになる可能性が高まっている．（図 1）




**多種多様な組込み機器が N/W 化されたことにより**
**セキュリティ対策を実施する範囲も拡大**

図 1：組込み機器のネットワーク化の例[1]

加えて，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も向上している．そのため，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．（図 2）

しかし，組込みシステムの開発現場では，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，セキュリティへの対策が疎かにされやすい．特に，社会インフラである重要インフラに用いられている組込み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り，組込みシステムに関するセキュリティ対策の実施は，開発元のみならず，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．

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り，資産として管理すべき情報の定義と管理体制（誰がどの範囲を管理するか）が重要となる．本研究では，特に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について考察するために CSMS と ISMS の比較を行った．

Vol.2016-DPS-168 No.10
Vol.2016-SPT-21 No.10
Vol.2016-EIP-74 No.10
2016/11/18

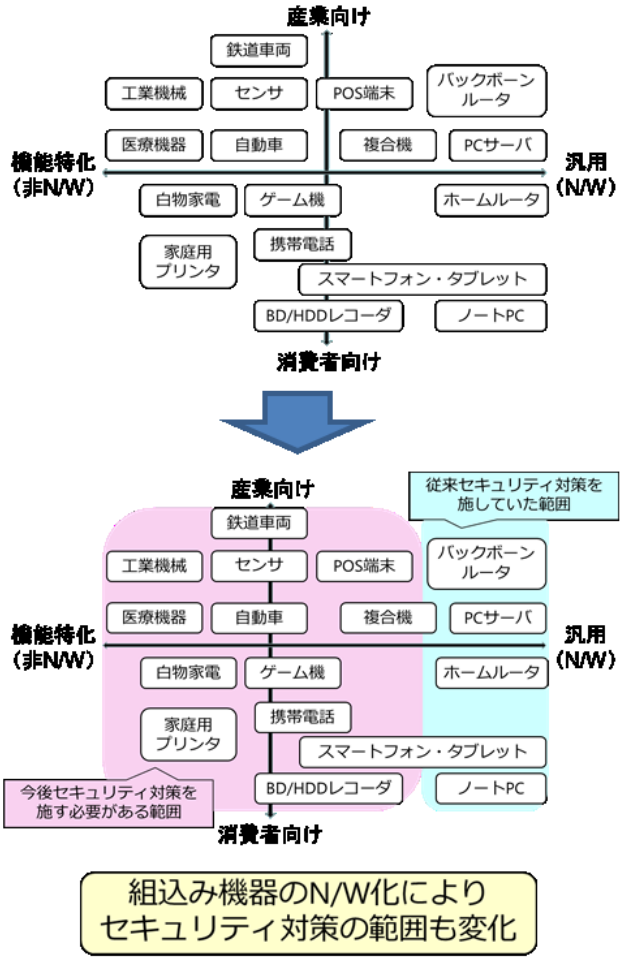



図 2：セキュリティ対策に関する位置づけ[2]

## 2. 組込みシステムに関する国際規格

図 3 は組込みシステムが多用される産業システムや制御システムの各製品分野において，機能安全（セーフティ）と防衛・安全保障（セキュリティ）の 2 つの面に関し，それぞれ組織管理と機器管理の観点から国際規格を整理したものである．セキュリティ面に関して，組織の ISMS 管理体制としては ISO/IEC27001（ISMS 適合評価制度の要求事項の規格）が適用されるものの，図 3 に示すように，組織管理については，業種分野別のセキュリティ管理作が通信・医療・金融に限られており，製造業については未策定である．さらに，製品規格についても IEC62443 が開発されているものの，共通部分についてのみであり，各機器（製品）のセキュリティ標準（管理策）については未策定，もしくは現在策定中のものが多い．

国の施策としては，汎用制御システムのセキュリティに関する国際規格 IEC62443 をベースとして，CSMS 適合性評価制度がある．本研究では， この CSMS 適合性評価制度の認証基準を軸に，資産としての情報の定義や組込み機器のセキュリティ管理体制について妥当性を考察する．

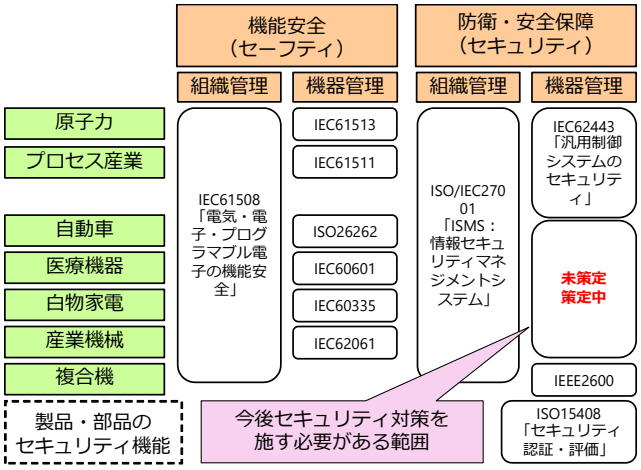



図 3：組込みシステムに関連する国際規格[3]

## 3. CSMS 適合性評価制度

### 3.1 目的・対象

CSMS（Cyber Security Management System）適合性評価制度（以下，CSMS という）とは， 産業機器および制御システム（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である．CSMS は制御システムセキュリティの向上と，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･維持することを目的として策定された．

CSMS の対象者は，制御システムのライフサイクルを考慮し，制御システムの保有者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およびシステムインテグレータである．これらの関連を図 4 に示す．

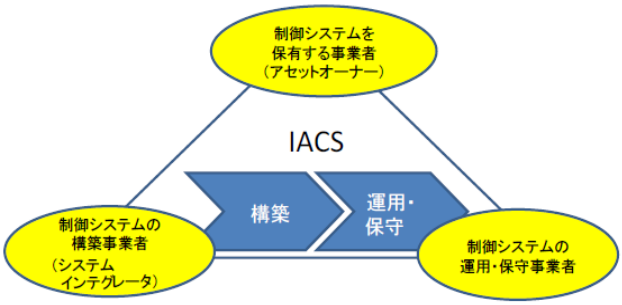



図 4：CSMS の対象者[4]

### 3.2 CSMS 認証基準

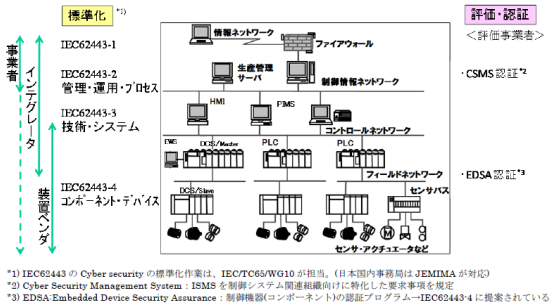
CSMS の認証基準策定については，IACS 分野のセキュリティマネジメントシリーズとして規格化されている．これを表 1 に示す．この中のマネジメントシステムである IEC62443-2-1 に基づいて策定されている．

Vol.2016-DPS-168 No.10
Vol.2016-SPT-21 No.10
Vol.2016-EIP-74 No.10
2016/11/18

表 1：IEC 62443 シリーズの構成[4]

| | |
|---|---|
| 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 IEC62443 シリーズのセキュリティ標準の全体像の例を図 5 に示す.




*1) IEC62443 の Cyber security の標準化作業は，IEC/TC65/WG10 が担当.（日本国内事務局は JEMIMA が対応）
*2) Cyber Security Management System：ISMS を制御システム関連組織向けに特化した要求事項を規定
*3) EDSA:Embedded Device Security Assurance：制御機器(コンポーネント)の認証プログラム→IEC62443-4 に提案されている

図 5：制御システムにおける IEC62443 セキュリティ標準の全体像

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リスクへの対処は，表 2 および図 6 に示すカテゴリから構成される.

表 2：CSMS 認証基準の構成

| | | |
|---|---|---|
| 4.2 | リスク分析 | |
| | 4.2.2 | 事実上の根拠：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および文書化する |
| | 4.2.3 | リスクの識別，およびアセスメント：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およ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．選択した管理策およ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て管理策およ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 の監視および改善 | |
| | 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，改善および維持管理：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. |

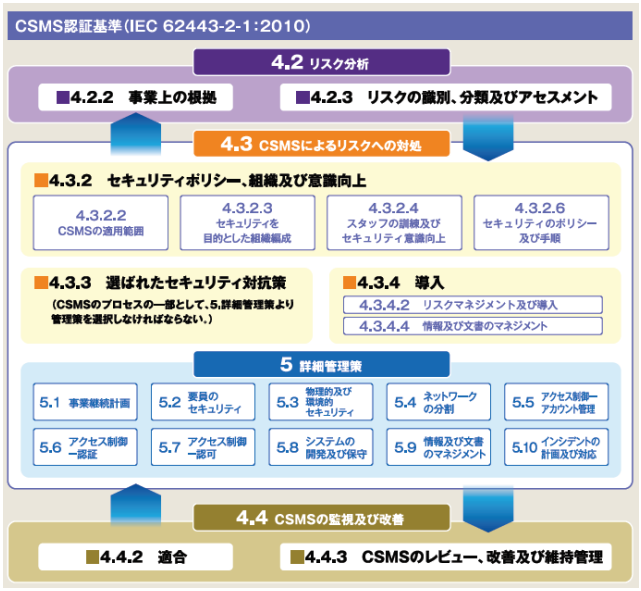



図 6：CSMS 認証基準の構成[4]

### 3.3 CSMS と ISMS の関係

CSMS 認証基準の規格である IEC62443-2-1 は，ISO/IEC27001：2005（旧 ISMS 認証基準）の要求事項を基に，制御システムをサイバー攻撃から守るための固有のセキュリティ要件を追加して作成されているため，ISMS と類似の管理要件が多数記載されている.

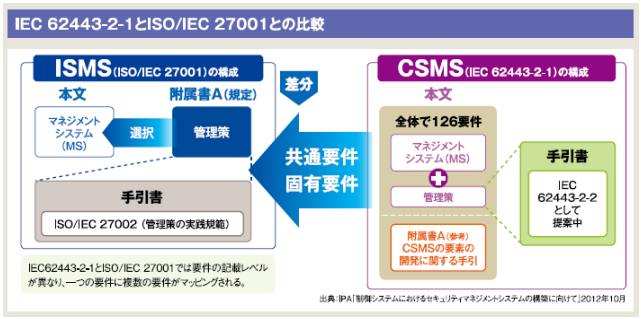



図 7：CSMS と ISMS の関係[4]

### 3.4 CSMS における課題

3.3 節で述べた通り，IEC62443-2-1 は ISO/IEC27001：2005（旧 ISMS 認証基準）を基にしており，類似の管理要件が多数あるため，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満足していると考えられる.

Vol.2016-DPS-168 No.10
Vol.2016-SPT-21 No.10
Vol.2016-EIP-74 No.10
2016/11/18

しかしながら，CSMS と ISMS では，情報セキュリティの 3 要素である「機密性」「完全性」「可用性」の優先度が異なる．ISMS では，守るべき情報の流出を問題視し，CIA（「機密性」・「完全性」「可用性」）の順で重視される場合が多い．一方で，CSMS では操業の中断を問題視するため，AIC（「可用性」・「完全性」・「機密性」）の順で重視することが多い．

すなわち，ISMS と CSMS では，守るべき資産としての情報について，優先度が異なっている．

例として，図 8 に示すプラントの運用のケースを考える．企業ゾーンとプラントの制御ゾーンはネットワークで接続されており，センサデータや運用履歴データがやり取りされる．企業ゾーン（事務所機能）では，組織の情報セキュリティ管理を行うため，ISMS が適用される．一方で，プラントの制御ゾーン（工場，オペレーション室等）では，様々な組込みシステムが使用されており，CSMS が適用されることになる．

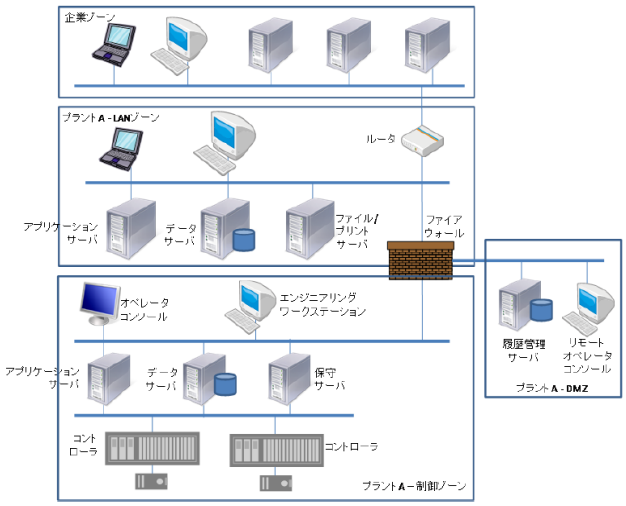



図 8：プラントにおけるネットワーク構成の例[5]

仮に制御ゾーンを含めて全組織を管理する場合は，全ての事務機器・プラントの制御機器の運用履歴データを ISMS に則って管理することになるが，運用履歴データはリアルタイムに変化するものであり，現実的な管理体制とは言えない．一方で，企業ゾーンと制御ゾーンを分割する場合，企業ゾーンにおいては ISMS 認証基準を適用できるが，制御ゾーンにおける資産としての情報をどの単位で管理するか，という問題が残る．

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するソリューションの提案を受ける，等のサービス形態も想定されるため，情報を誰がどの単位で管理するかが重要になるだろう．

以上のように，CSMS と ISMS はそれぞれがセキュリティマネジメントシステムに関する要求事項であるものの，情報セキュリティの 3 要素（CIA）の優先度や適用範囲の考え方が異なるものであるため，既に ISMS 認証を取得している組織であっても，容易に CSMS 認証も取得できるとは限らないと考えられる．特に，資産として管理すべき情報の定義（単位）および管理体制については，組織毎にルールや契約で個別対応しているものと考えられる．この例を表 3 に示す．

表 3：プラントのケースにおける資産の所有者・リスク保有者・資産の管理者の対応の例

| 標準規格 | 所有者 | リスク所有者 | 管理者 |
|---|---|---|---|
| ISMS | 利用者 | 遠隔監視事業者 | 遠隔監視事業者 |
| CSMS | 利用者 | 製造者 | 遠隔監視事業者 |

これらは契約によって決まることが多い

さらに，ISO/IEC27001 は 2013 年に改訂が行われている．CSMS は ISO/IEC27001：2005 がベースになっているため，通常であれば，ISO/IEC27001：2013 をベースにした要求事項へと改訂を行うことが妥当である．

しかし，ISO/IEC27001：2005 と比較して，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，情報という資産に関する定義が困難になった．例えば制御システムでは，個々の機器や設備を「情報資産」と見なして管理できるが，「情報」はリアルタイムに生成される出力値・計測値と機器自体の設定パラメータがあり，どのデータをどのレベルで管理すれば良いかを明確にするのは困難が伴う．

すなわち，今後制御システムのセキュリティ対策を考えるに当たって，現行の CSMS 認証基準として ISO/IEC27001：2005 と ISO/IEC27001：2013 のどちらに従うことが妥当か考える必要がある．

## 4. 調査方法

### 4.1 CSMS と ISMS の要求事項の比較

本研究では，資産として管理すべき情報の定義（単位）および管理体制について，妥当性を考察するために，

Vol.2016-DPS-168 No.10
Vol.2016-SPT-21 No.10
Vol.2016-EIP-74 No.10
2016/11/18

IEC62443-2-1 と従来の ISO/IEC27001：2005 と現行の ISO/IEC27001：2013 の要求事項（条項）を比較する．

実際には，現行の CSMS は ISO/IEC27001：2005 に準拠した内容となっているため，ISO/IEC27001：2013 を CSMS に適合させた場合の要求事項と現行の CSMS の要求事項とを比較した．今後，制御システムに適用した場合のメリット・デメリットを整理することで，妥当な定義や管理策について考察する予定である．

### 4.2 情報セキュリティアンケートによる実態調査

原田研究室では毎年プライバシーマークまたは ISMS 認証取得企業および官公庁・教育機関を対象に、情報セキュリティアンケートを実施している．2016 年度は 4800 組織を対象にアンケートを実施しており，表 4 に示す組織の資産管理の実態調査に関する設問を盛り込んだ．各組織の資産管理状況の結果とし,今後の考察の指標として活用する．

表 4：情報セキュリティアンケートの設問（抜粋）

| 設問番号 | 設問内容 |
|---|---|
| Q18 | 従業員の私有 IT 資産の業務利用を認めていますか？ |
| 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？ |
| Q22 | 今後、貴組織の役員・各部門へ私有 IT 資産の業務利用を認める予定はありますか？ |

## 5. 調査結果

### 5.1 CSMS と ISMS の要求事項の比較

まず，CSMS 認証基準である IEC62443-2-1 と，ISO/IEC27001：2005 の要求事項を比較し，IEC62443-2-1 だけにある要求事項（CSMS の固有要件）を表 5 に抽出した．

現在，IEC62443-2-1 と ISO/IEC27001：2013 の要求事項でも同様に CSMS の固有要件を抽出中である．今後は，2 つの抽出結果を比較し，CSMS と ISMS：2005、2013 の要求事項の違いを整理する．

表 5：ISO/IEC27001：2005 になく IEC/62443-2-1 だけにある要求事項（CSMS 固有要件）

| CSMS 認証基準 | | | |
|---|---|---|---|
| 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 |
| | | | 4.2.3.5 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 によりリスクへの対処 | |
| | | 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 |
| | | | 4.4.3.8 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 |
| | | 5.6.7 | 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 |
| | | 5.6.9 | タスク間通信での認証の採用 |
| | 5.7 | アクセス制御－認可 | |

Vol.2016-DPS-168 No.10
Vol.2016-SPT-21 No.10
Vol.2016-EIP-74 No.10
2016/11/18

| | | | |
|---|---|---|---|
| | | 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 | |
| | | 5.9.5 | 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 |

### 5.2 情報セキュリティアンケートによる実態調査

2016 年 10 月 20 日現在 544 組織から回答を得ている．現在アンケート結果を入力・集計中である．

なお，情報セキュリティアンケートの集計結果は 2016 年 12 月上旬に原田研究室 HP にて公開予定である．

## 6. 今後の研究

今後は，以下の検討を進める．

① IEC62443-2-1 と ISO/IEC27001：2013 の要求事項を比較し，CSMS 固有の要求事項を抽出する．

② 今回の調査結果と①の抽出結果を比較し，CSMS と ISMS：2005、2013 それぞれの要求事項の違いを管理策レベルまで展開して考察する．

③ 情報セキュリティアンケートの結果から，CSMS に関わる各組織（特に製造業）が実施しているセキュリティ対策傾向の分析を実施する．

④ CSMS について，今後 ISO/IEC27001：2013 に統一すべきかどうかを考察した上で，CSMS に関わる組織が実施すべき情報セキュリティ対策（リスクコントロール）に関する提案を検討する．

⑤ 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について考察・提案を行う．

## 謝辞

本論文の執筆にあたり，ご指導いただいた情報セキュリティ大学院大学の教授陣，また多くの助言をいただいた原田研究室の客員研究員およびメンバーに対し，謹んで感謝の意を表する．

## 参考文献

[1] 独立行政法人情報処理推進機構,「組込みシステムセキュリティ -情報家電-」，2007

[2] 鮫島吉喜，日本セキュリティマネジメント学会 第 4 回セキュア OS カンファレンス,「組込み系システムへのセキュア OS 応用研究」，2006

[3] 中部経済産業局,「組込みシステムのセキュリティ取組みガイドブック」，2014

[4] 一般財団法人日本情報経済社会推進協会　情報マネジメントセンター,「CSMS ユーザーズガイド -CSMS 認証基準（IEC62443-2-1）対応-」，2015

[5] 一般財団法人日本情報経済社会推進協会　情報マネジメントセンター,「CSMS 適合性評価制度の概要」，2014

[6] 一般財団法人日本情報経済社会推進協会　情報マネジメントセンター,「CSMS 認証基準（IEC62443-2-1）」，2014

[7] 一般財団法人日本情報経済社会推進協会　情報マネジメントセンター,「ISMS 適合性評価制度の概要」，2014

[8] 一般財団法人日本情報経済社会推進協会　情報マネジメントセンター,「ISMS ユーザーズガイド -JIS Q27001：2014（ISO/IEC27001：2013）対応」，2014

[9] 独立行政法人情報処理推進機構,「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

[10] 独立行政法人情報処理推進機構,「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

[11] 独立行政法人情報処理推進機構,「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

[12] 独立行政法人情報処理推進機構,「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

[13] 一般財団法人日本規格協会,「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