# 制御システムに関する サイバーセキュリティマネジメント システム（CSMS）の現状

JIPDEC（一般財団法人日本情報経済社会推進協会）
高取　敏夫

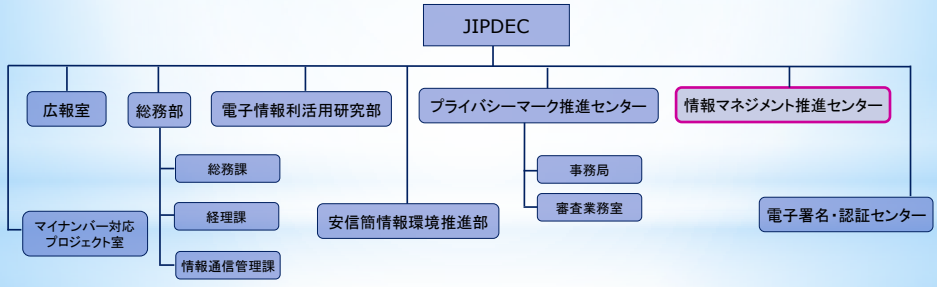
2015年5月

http://www.isms.jipdec.or.jp




# JIPDEC組織体制

- JIPDEC（一般財団法人日本情報経済社会推進協会）
- 設　　立：昭和42年12月20日
- 事業規模：25億1,610万円（平成27年度予算）
- 職　員　数：108名（平成27年4月現在）



# 情報マネジメント推進センターの主な業務内容

□情報技術に関連するマネジメントシステムの認定機関としての業務及び各制度に関連する普及業務

- ■ISMS/ITSMS/BCMS/CSMS認定システム実施に伴う諸業務
- ■ISMS/ITSMS/BCMS/CSMS認定審査の実施
- ■ISMS/ITSMS/BCMS/CSMS関連の委員会事務局業務
- ■IT資産管理（ITAM）に関する調査研究業務
- ■国際認定機関やフォーラム（IAF、PAC等）との相互連携の推進
- ■ISO/IECなど（国際規格、ガイド策定等）への積極的貢献
- ■制御システムセキュリティの普及に関する業務

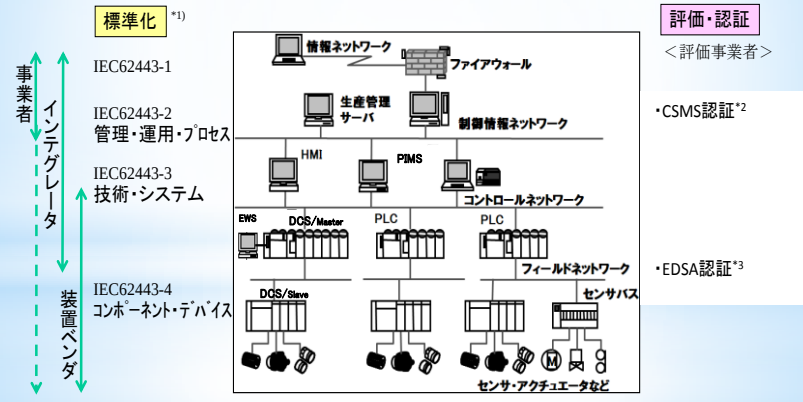



# 制御システムセキュリティを実現するための基準

制御システム分野で広く共通的な活用ができる規格であり、制御システムの利用者、装置製造者のそれぞれで広く活用できるセキュリティ規格としてIEC 62443シリーズがある。

- ・IEC 62443-1 シリーズ　：　この規格全体の用語・概念等の定義
- ・IEC 62443-2 シリーズ　：　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 シリーズ　：　システムのセキュリティ要件や技術概説
- ・IEC 62443-4 シリーズ　：　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

# 制御システムセキュリティ標準




*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

(出所:IPA「IEC62443及びCSMS/EDSA規格の詳細」に一部加筆修正)




# 制御システムの サイバーセキュリティマネジメントシステム (CSMS)

- IEC 62443-2-1:2010(Industrial Communication networks – Network and system security – Part2-1:Establishing an industrial automation and control system security program)は、IACS(Industrial Automation and Control System)をサイバー攻撃から保護するための要素を規定している。

  [ IEC 62443-2-1(Ed.2)
  Requirements for an IACS Security management system ]

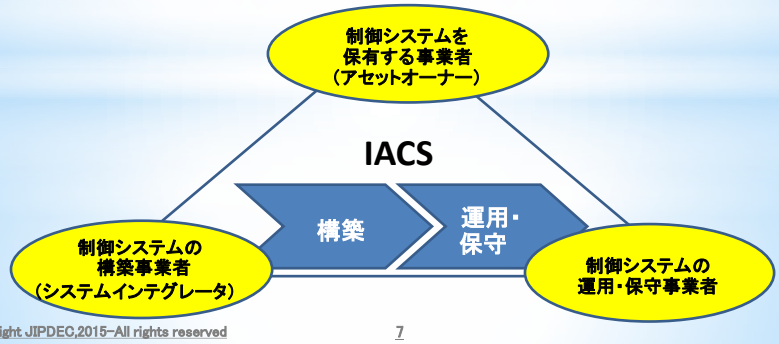
- 主要なカテゴリーは、リスク分析、CSMSによるリスクへの対処、並びにCSMSの監視及び改善の3つで構成されている。

- リスク分析をベースとしたセキュリティマネジメントシステムの構築が可能である。

# CSMSの対象者

CSMS構築の目的は、IACS（産業用オートメーション及び制御システム）のセキュリティの信頼性を確保することである。CSMS構築は、制御システムの保有事業者（アセットオーナー）及び運用・保守事業者、制御システムを構築事業者（システムインテグレーター）の三位一体で取り組むことが必要不可欠であり、各事業者が単独で取り組むのではなく、直ちに関係プレイヤーがCSMS構築に取り組む必要がある。

また、IACS自体のセキュリティを評価するのではなく、IACSの設計段階から廃棄にいたるライフサイクルの各フェーズに携わる事業者がセキュリティ上の信頼性を確保する ための要求事項に適合しているかどうかを 評価することである。その評価基準としてCSMS認証基準（IEC62443-2-1:2010）を利用する。







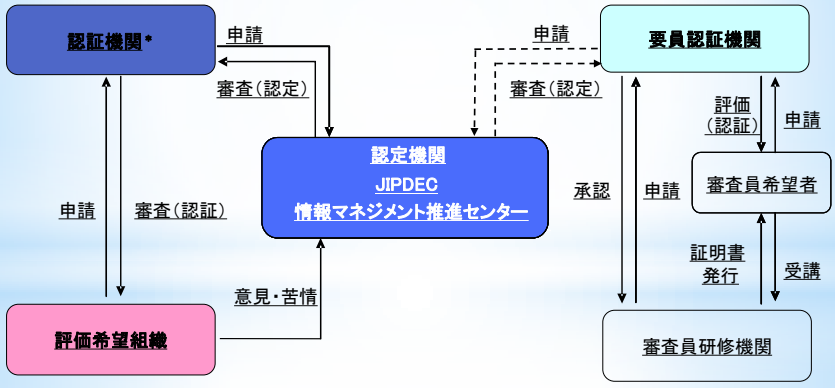
# CSMS適合性評価制度の目的

CSMS（Cyber Security Management System）適合性評価制度（以下、CSMS制度＊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。

（出典：CSMS適合性評価制度の概要）

＊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）

# CSMS適合性評価制度の運用体制

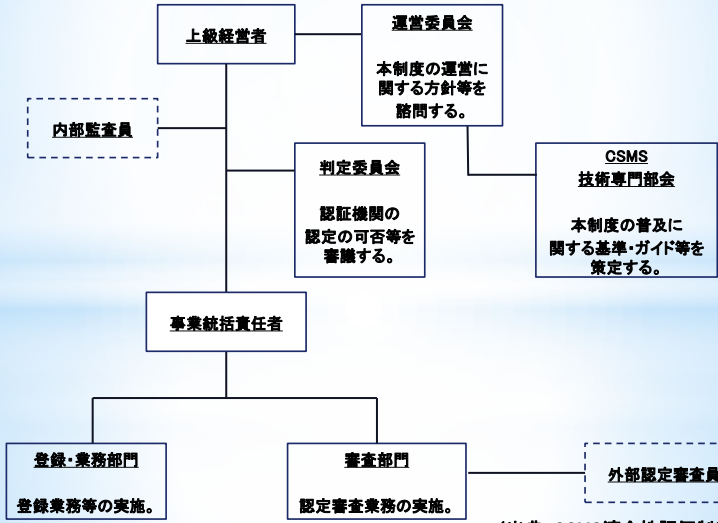



(出典:CSMS適合性評価制度の概要)

＊認証機関 ・一般財団法人日本品質保証機構(JQA) http://www.jqa.jp/
・BSIグループジャパン株式会社(BSI-J) http://www.bsigroup.com/ja-JP/




# CSMS適合性評価制度の組織運営機構




(出典:CSMS適合性評価制度の概要)

# 技術専門部会の開催状況

| 回数 | 開催日 | 主なテーマ |
|---|---|---|
| 第1回 | 2014.06.17 | ・CSMS制度運営体制の確認<br>・CSMS認証基準／ユーザーズガイド／パンフレットの検討<br>・CSMS普及啓発活動の検討 |
| 第2回 | 2014.08.07 | ・CSMSパンフレット（日本語版）の最終案の確認<br>・CSMS説明会の実施について<br>・CSMS認証基準（IEC 62443-2-1:2010）の検討 |
| 第3回 | 2014.09.26 | ・CSMS認証基準（IEC 62443-2-1:2010）とJIS Q 27001:2014のマッピング表の検討<br>・CSMS説明会（東京会場）のプログラム及びアンケート調査票（案）の検討<br>・CSMSパンフレット（英語版）（案）の検討 |
| 第4回 | 2014.11.06 | ・JIS Q 27001:2014のマッピング表の検討<br>・CSMS説明会（東京会場）プログラム及びアンケートの検討 |
| 第5回 | 2014.12.22 | ・JIS Q 27001:2014のマッピング表の最終検討<br>・CSMS説明会（東京会場）アンケート集計結果の報告<br>・CSMS説明会（大阪/東京会場）プログラム案の検討<br>・CSMS普及啓発活動の検討 |
| 第6回 | 2015.3.2 | ・JIS Q 27001:2014のマッピング表の最終確認（別紙1参照）<br>・CSMSユーザーズガイド改訂版の検討<br>・CSMS説明会（2/17東京会場）アンケート集計結果の報告<br>・今後のCSMS普及啓発活動の検討 |




# CSMSに関する説明会の開催状況

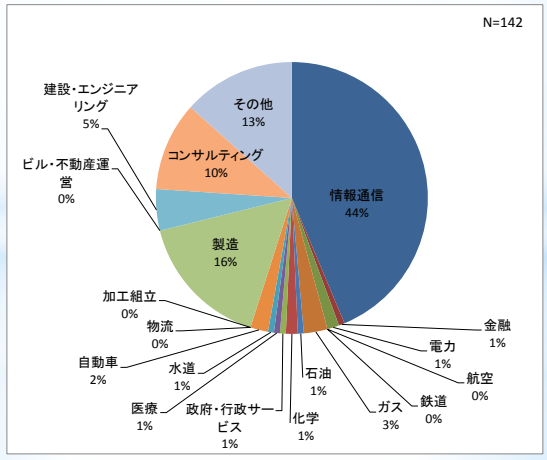
（参加者：計180名）

| 開催日 | 開催場所 | 主な講演内容 |
|---|---|---|
| 2014.11.28<br>（参加者数<br>58名） | [東京]<br>（グランパーク401ホール<br>港区芝浦3-4-1） | ・CSMSに関連する情報セキュリティ政策について<br>・サイバー攻撃対策における制御システムセキュリティの課題<br>・CSMS適合性評価制度及び認証基準の概要<br>・CSMSユーザーズガイド解説<br>・事例（2講演）－認証取得企業 |
| 2015.2.17<br>（参加者数<br>79名） | [東京]<br>（グランパーク401ホール<br>港区芝浦3-4-1） | ・生産制御に関連する情報セキュリティ政策<br>・サイバー攻撃対策における制御システムセキュリティの課題<br>・CSMS適合性評価制度及び認証基準の概要<br>・CSMSユーザーズガイド解説<br>・事例（2講演）－認証取得企業 |
| 2015.2.26<br>（参加者数<br>43名） | [大阪]<br>（大阪大学中之島センター<br>講義室703<br>大阪市北区中之島4-3-53） | |

# 説明会アンケート集計分析結果(1/7)

**○業種**

**最も多い参加業種は「情報通信（44%）」で半数近くを占めており、「製造（16%）」、「コンサルティング（10%）」と続いている。今後製造業が増えることが課題である。**





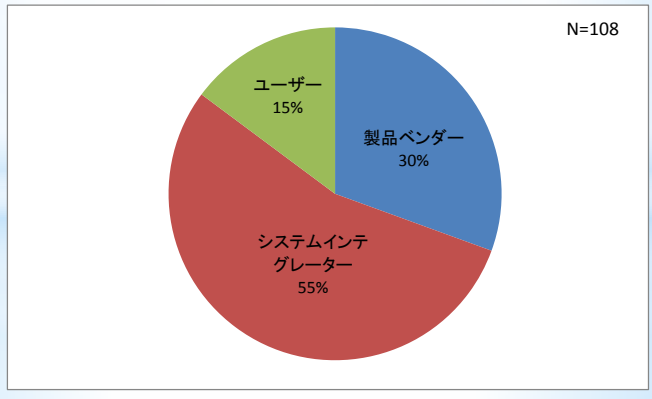



出典：平成28年度CSMS適合性評価制度に関する説明会実施報告書

# 説明会アンケート集計分析結果(2/7)

**○業態**

**業態別にみると、「システムインテグレーター（55%）」が半数以上となっており、関心が強いことがうかがわれる。**

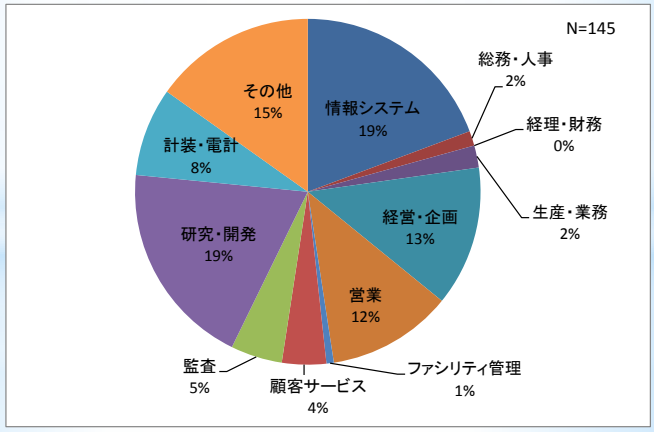



出典：平成28年度CSMS適合性評価制度に関する説明会実施報告書

# 説明会アンケート集計分析結果(3/7)

○職種

「情報システム」と「研究・開発」がともに19%で、最も多い参加職種となっている。



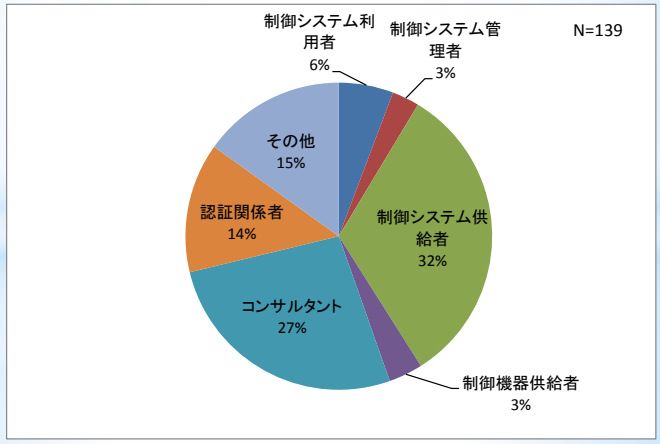

出典：平成26年度CSMS適合性評価制度に関する説明会実施報告書




# 説明会アンケート集計分析結果(4/7)

○説明会の参加の立場

説明会への参加の立場は、「制御システム供給者（32%）」、「コンサルタント（27%）」の順となっている。

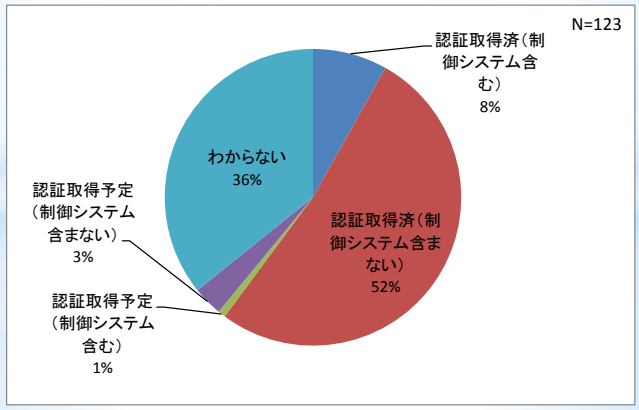



出典：平成26年度CSMS適合性評価制度に関する説明会実施報告書

# 説明会アンケート集計分析結果(5/7)

○ISMS認証取得状況

現状では、ISMS認証取得済組織が60%となっているが、ほとんどは「制御システムを含まない（52%）」となっている。



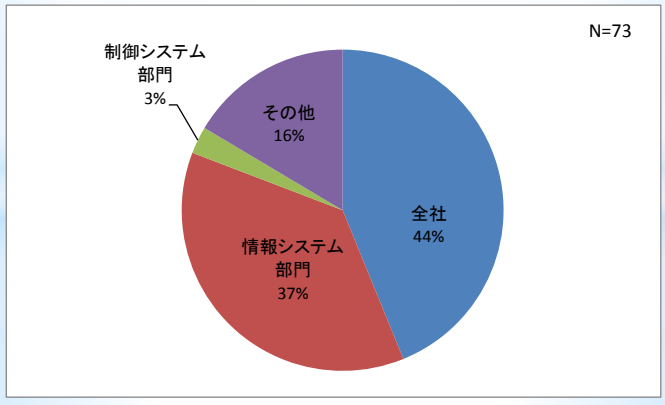

出典：平成26年度CSMS適合性評価制度に関する説明会実施報告書




# 説明会アンケート集計分析結果(6/7)

○ISMS認証取得の適用範囲

「全社」が44%、「情報システム部門」が37%で、「制御システム部門」は3%となっている。

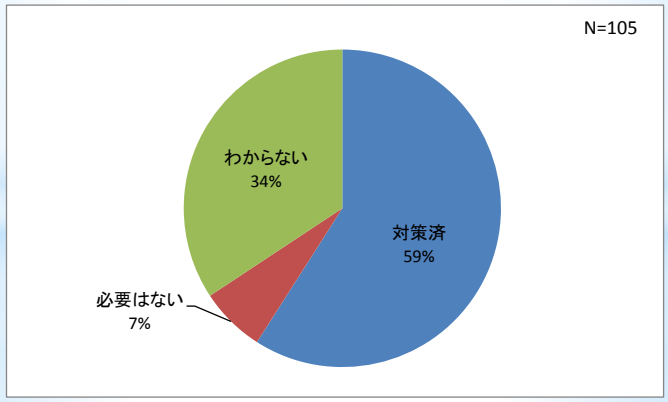



出典：平成26年度CSMS適合性評価制度に関する説明会実施報告書

# 説明会アンケート集計分析結果(7/7)

○制御システムにおけるセキュリティの状況

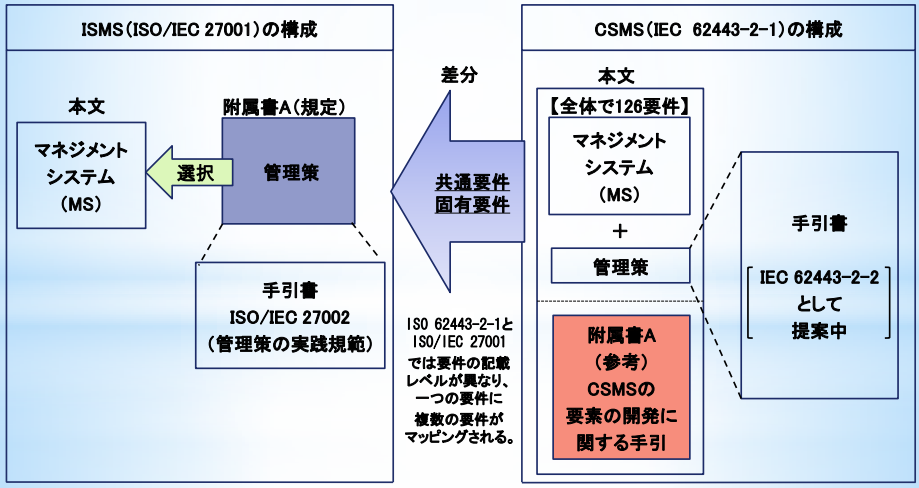
6割の組織がサイバー攻撃等に対して、何らかの対策をしていることがうかがえる。




出典:平成26年度CSMS適合性評価制度に関する説明会実施報告書




# CSMSとISMSの関係




注:CSMS固有要件は、CSMSユーザーズガイド付録2を参照されたい。

(出典:CSMS適合性評価制度の概要)

# CSMS固有の要件の概要(1/6)

| IEC 62443-2-1 | | JIS Q 270001:2014 | |
|---|---|---|---|
| 項番 | 条文 | 項番 | 条文 |
| 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、分類及びアセスメント | | |
| 4.2.3.3 | **上位レベルのリスクアセスメントの実行**<br><br>IACSの可用性，完全性又は機密性が損なわれた場合の財務的結果及びHSE(health,safety and environment)に対する結果を理解するために，上位レベルのシステムリスクアセスメントが実行されなければならない。 | 6.1.2<br>6.1.2c)<br>6.1.2d)<br>6.1.2d)1)<br>6.1.1 Para1 | **情報セキュリティリスクアセスメント**<br>組織は，次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め，適用しなければならない。 |
| 4.2.3.5 | **単純なネットワーク図の策定**<br><br>組織は，論理的に統合されたシステムのそれぞれについて，主要装置，ネットワークの種類及び機器の一般的な場所を示す単純なネットワーク図を策定しなければならない。 | 4.3 Para1 | **情報セキュリティマネジメントシステムの適用範囲の決定**<br><br>組織は，ISMSの適用範囲を定めるために，その境界及び適用可能性を決定しなければならない。 |
| 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**<br><br>資産のリスク全体を理解するために，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が統合されなければならない。 | 6.1.2<br>6.1.2c)<br>6.1.2d)<br>6.1.2d)1)<br>6.1.1 Para1 | **情報セキュリティリスクアセスメント**<br>組織は，次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め，適用しなければならない。 |




# CSMS固有の要件の概要(2/6)

| IEC 62443-2-1 | | JIS Q 270001:2014 | |
|---|---|---|---|
| 項番 | 条文 | 項番 | 条文 |
| 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 | | |
| 4.3.2.4.5 | **訓練プログラムの経時的な改訂**<br><br>新たな又は変化する脅威及びぜい弱性を説明するために，サイバーセキュリティの訓練プログラムが必要に応じて改訂されなければならない。 | | 該当なし |
| 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**<br><br>IACSのリスクに対処するサイバーセキュリティのポリシー及び手順は，他のリスクマネジメントシステムによって作成されたポリシーに対して一貫性があるか，又はそれらを拡張したものでなければならない。 | | 該当なし |
| 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 | | |
| 4.4.3.6 | **業界のCSMS戦略の監視及び評価**<br><br>マネジメントシステムの所有者は，リスクアセスメント及びリスク軽減のためのCSMSのベストプラクティスに関して業界を監視し，それらの適用可能性を評価しなければならない。 | | 該当なし |
| 4.4.3.8 | **セキュリティ上の提案に関する従業員のフィードバックの要求及び報告**<br><br>セキュリティ上の提案に関する従業員のフィードバックが，積極的に求められ，パフォーマンス上の欠点及び機会の点から経営幹部に必要に応じて報告が戻されなければならない。 | | 該当なし |

# CSMS固有の要件の概要(3/6)

| IEC 62443-2-1 | | JIS Q 270001:2014 | |
|---|---|---|---|
| 項番 | 条文 | 項番 | 条文 |
| 4.3.3.2 | 要員のセキュリティ | | |
| 4.3.3.2.3 | **要員の継続的な選別**<br><br>要員に対しては，利害の対立又は適切な方法で職務を実行することに対する懸念を示唆する可能性がある変化を確認するために，継続的な調査も行われなければならない。 | | 該当なし |
| 4.3.3.3 | 物理的及び環境的セキュリティ | | |
| 4.3.3.3.1 | **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**<br><br>資産を保護するための物理的セキュリティとサイバーセキュリティの両方に対処するセキュリティのポリシー及び手順が確立されなければならない。 | | 該当なし |
| 4.3.3.3.10 | **重要資産の暫定的保護のための手順の確立**<br><br>例えば火災，浸水，セキュリティ侵害，中断，天災又はその他のあらゆる種類の災害が原因となって運用が中断しているときに重要なコンポーネントを確実に保護するための手順が確立されなければならない。 | | 該当なし |




# CSMS固有の要件の概要(4/6)

| IEC 62443-2-1 | | JIS Q 270001:2014 | |
|---|---|---|---|
| 項番 | 条文 | 項番 | 条文 |
| 4.3.3.6 | アクセス制御－認証 | | |
| 4.3.3.6.5 | **適切なレベルでのすべてのリモートユーザの認証**<br><br>組織は，リモート対話ユーザを明確に識別するために，適切な強度レベルの認証方式を採用しなければならない。 | 旧A.11.4.2<br>→ 削除 | **外部から接続する利用者の認証**<br><br>管理策<br>遠隔利用者のアクセスを管理するために，適切な認証方法を利用しなければならない。 |
| 4.3.3.6.6 | **リモートログイン及びリモート接続のポリシーの策定**<br><br>組織は，失敗したログイン試行及び活動のない期間に対する適切なシステム対応を定義した，ユーザによる制御システムへのリモートログイン及び／又は制御システムへのリモート接続（例えば，タスク間接続）に対処するポリシーを策定しなければならない。 | 旧A.11.4.2<br>→ 削除 | **外部から接続する利用者の認証**<br><br>管理策<br>遠隔利用者のアクセスを管理するために，適切な認証方法を利用しなければならない。 |
| 4.3.3.6.7 | **失敗した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**<br><br>リモートユーザによる一定回数の失敗したログイン試行の後に，システムがそのアクセスアカウントを一定期間無効にしなければならない。 | A.9.4.2 | **セキュリティに配慮したログオン手順**<br><br>管理策<br>アクセス制御方針で求められている場合には，システム及びアプリケーションへのアクセスは，セキュリティに配慮したログオン手順によって制御しなければならない。 |
| 4.3.3.6.8 | **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**<br><br>定義済みの，活動のない期間が経過した後は，リモートユーザがシステムに再度アクセスできるようになる前に，リモートユーザに再認証が要求されなければならない。 | A.9.4.2 | **セキュリティに配慮したログオン手順**<br><br>管理策<br>アクセス制御方針で求められている場合には，システム及びアプリケーションへのアクセスは，セキュリティに配慮したログオン手順によって制御しなければならない。 |
| 4.3.3.6.9 | **タスク間通信での認証の採用**<br><br>システムでは，アプリケーションと装置の間のタスク間通信に対する適切な認証方式が採用されなければならない。 | A.13.1.1 | **ネットワーク管理策**<br><br>管理策<br>システム及びアプリケーション内の情報を保護するために，ネットワークを管理し，制御しなければならない。 |

# CSMS固有の要件の概要(5/6)

| IEC 62443-2-1 | | JIS Q 270001:2014 | |
|---|---|---|---|
| 項番 | 条文 | 項番 | 条文 |
| 4.3.3.7 | アクセス制御－認可 | | |
| 4.3.3.7.3 | **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**<br><br>アクセスアカウントは，そのユーザの役割に対して適切な情報又はシステムへのアクセスを管理するために，役割に基づいていなければならない。役割を定義するときには，安全性に対する影響が考慮されなければならない。 | | 該当なし |
| 4.3.3.7.4 | **重要なIACSに対する複数の認可方法の採用**<br><br>重要な制御環境では，複数の認可方法を採用して，IACSへのアクセスを制限しなければならない。 | | 該当なし |



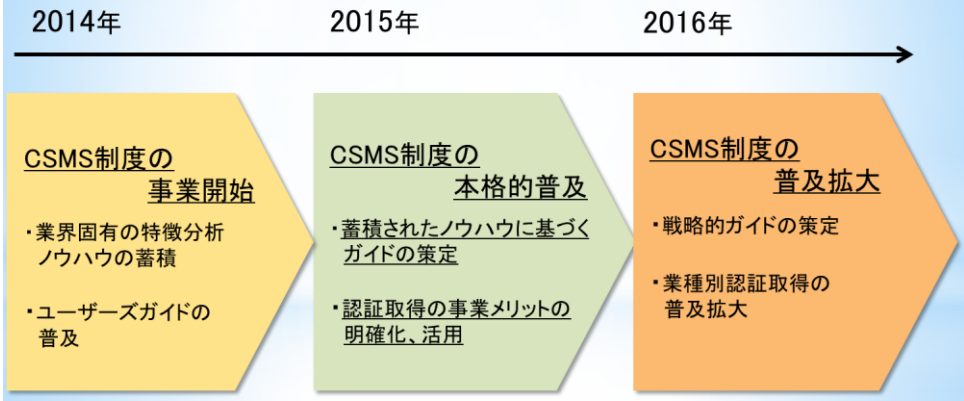

# CSMS固有の要件の概要(6/6)

| IEC 62443-2-1 | | JIS Q 270001:2014 | |
|---|---|---|---|
| 項番 | 条文 | 項番 | 条文 |
| 4.3.4.3 | システムの開発及び保守 | | |
| 4.3.4.3.4 | **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**<br><br>既存のゾーン内のIACS環境に設置される新しいシステムのセキュリティ要求事項は，そのゾーン／環境において要求されるセキュリティのポリシー及び手順に合致していなければならない。同様に，保守によるアップグレード又は変更が，そのゾーンのセキュリティ要求事項に合致していなければならない。 | A.14.2.2 | **システムの変更管理手順**<br><br>管理策<br>開発のライフサイクルにおけるシステムの変更は，正式な変更管理手順を用いて管理しなければならない。 |
| 4.3.4.3.5 | **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**<br><br>サイバーセキュリティの変更管理手順が，既存のPSMの手順に統合されなければならない。 | | 該当なし |
| 4.3.4.4 | 情報及び文書のマネジメント | | |
| 4.3.4.4.5 | **長期記録の取得の保証**<br><br>長期記録が取得できることを確実にするための適切な対策(つまり，より新しい形式へのデータの変換又はデータの読み取りが可能な旧式の機器の保持)が採用されなければならない。 | | 該当なし |
| 4.3.4.5 | インシデントの計画及び対応 | | |
| 4.3.4.5.2 | **インシデント対応計画の伝達**<br><br>すべての適切な組織に，インシデント対応計画が伝達されなければならない。 | | 該当なし |
| 4.3.4.5.11 | **演習の実行**<br><br>インシデント対応プログラムを定期的にテストするために，演習が実行されなければならない。 | | 該当なし |




の部分は、ISO/IEC 27001:2005版のCSMS固有要件

# CSMS適合性評価制度の普及




（出典：CSMS適合性評価制度の概要）




今後も、様々な活動を通じてCSMSの普及促進に努めてまいります。
皆様方のご支援、ご協力をお願いいたします。

【お問い合わせ先】
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

URL http://www.isms.jipdec.or.jp/