JEMIMA

計測展2017 TOKYO 委員会セミナー

制御システムセキュリティ向上に向けた取り組み

セキュリティ自己診断ツール「J-CLICS」

2017.11.30

SICE/JEITA/JEMIMA
セキュリティ合同WG

目次

目次

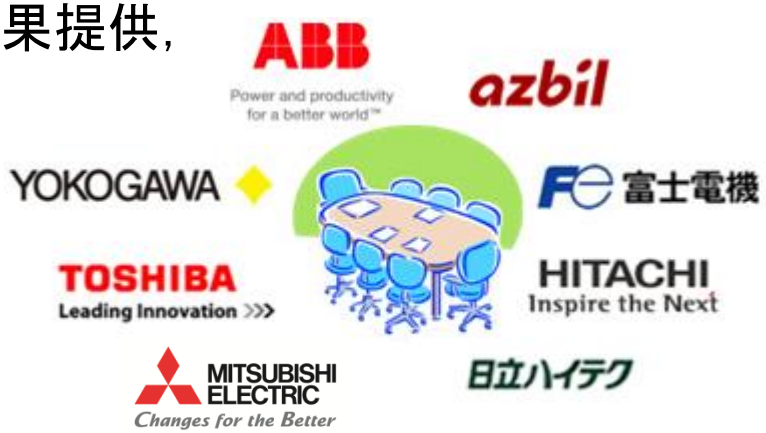
SICE/JEITA/JEMIMAセキュリティ合同WG

- **活動目的**
  製造業分野におけるセキュリティ標準化動向，技術等の調査・研究活動と会員企業・ユーザへの成果提供，展示会・各種会議での広報

- **設立**
  2005年4月

- **メンバー（50音順）**
  ABB日本ﾍﾞｰﾚｰ㈱、アズビル㈱、㈱東芝、㈱日立製作所、㈱日立ハイテクソリューションズ、富士電機㈱、三菱電機㈱、横河電機㈱

- **活動実績**
  1. ISA SP99　TR2を利用したセキュリティ対策の実践
  2. NIST SPP-ICS ver1.0を利用したセキュリティ要件の分析
  3. セキュリティ標準規格の調査
  4. CPNI グッドプラクティスの検討
  5. セキュリティ評価ツールの調査・改良
  6. **新セキュリティ評価ツール J-CLICS の作成・拡充**



JEMIMA本部
計測会館

SICE/JEITA/JEMIMAセキュリティ合同WG

- **外部団体との協力関係**
  - SICE（計測・制御ネットワーク部会）
  - JEITA（制御・エネルギー管理専門委員会）
  - JPCERT/CC
  - IPA（独立行政法人情報処理推進機構）
  - IEC/TC65/WG10 国内委員会
  - 制御システムセキュリティ関連団体合同委員会
    - NECA, JEMA, JEMIMA, JEITA, JPCERT/CC, JARA, MSTC, VEC, SICE, IPA[new !], RRI [new !]
- **広報活動**
  - 計測展委員会セミナー
  - SCF（システムコントロールフェア）シンポジウム
  - JPCERT/CC
    制御システムセキュリティカンファレンス
  - SICE Annual Conference，シンポジウム，学会誌

制御システムセキュリティ
関連団体合同委員会

目次

制御システムセキュリティの現状

- **制御システムに対するサイバー攻撃の脅威が拡大**
  - '10のStuxnet出現を契機に，制御システムのセキュリティに対する課題意識が高まっている
  - 社会インフラシステムや基幹産業を標的とした攻撃事例も発生
    - ➢ 標的分野の専門知識を悪用した攻撃手段の巧妙化
  - 制御装置／システムの脆弱性公表ペース増加
    - ➢ セキュリティ研究者・コミュニティの活動活発化

制御システムへのサイバー攻撃事例

発生年	発生地	被害設備	被害内容
2010	イラン	ウラン濃縮施設	遠心分離機が損傷し，核開発が遅延
2016	ウクライナ	送電システム	制御装置の不正操作により大規模停電

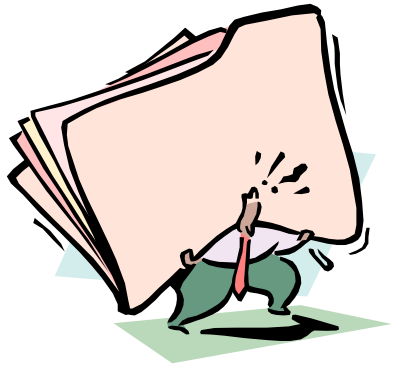
制御システムセキュリティの現状

- **制御システムセキュリティの標準化**
  - 欧米の政府や業界団体を中心に，推奨されるセキュリティ対策を標準・ガイドラインとして策定
    - 重要インフラのセキュリティを向上させるためのフレームワーク【米NIST】
    - SCADA Security Good Practice Guide【英CPNI】
  - 制御システム全般を対象とした国際標準 IEC 62443が策定中
    - 同標準に基づくシステムや装置の認証ビジネスも開始

NIST : National Institute of Standards and Technology
CPNI : Centre for Protection of National Infrastructure

制御システムセキュリティの課題

- **既設システムなどで，十分に対策をとれていないケースも存在**
  - 具体的に誰が何をすればいいか，よくわからない
  - 対策はしたいが，工数や予算が確保できない　…etc
- **既存の標準やガイドラインだけでは対策が困難**
  - 「今，自分の組織は何をすべきか」「最低限，何をすればいいか」は具体的に書かれていない
  - リスク評価や管理体制の構築など，プロセス面の負担が重い



J-CLICS開発の動機と目的

ユーザ企業とJPCERT/CCの協力のもと，セキュリティ合同WGが**セキュリティ対策チェックツールJ-CLICS**を開発

J-CLICS：Check List for Industrial Control System of Japan

- **動機**
  - 既存の制御システムの保護にも役立つ施策が必要
  - 現場担当者から経営者までのセキュリティスキル・意識の底上げが必要

- **目的**
  - 現状の把握やセキュリティ対策の足掛かりに気軽に活用できるツールを提供する
  - 最低限必要な施策を，制御システムに関わる全ての人にわかりやすく，実施しやすい形でガイドする

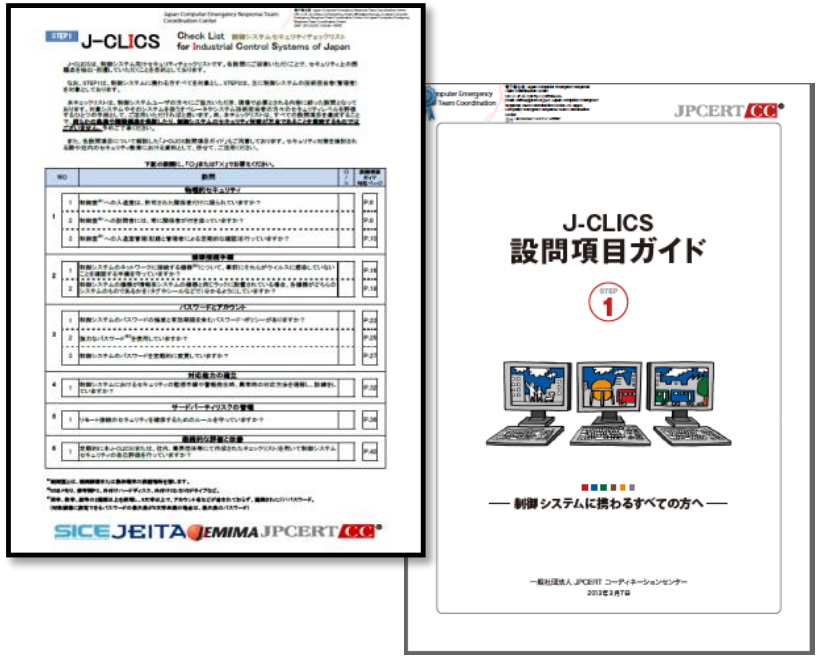
J-CLICSの開発方針

- **個々の立場に適した最低限のチェック項目を厳選する**
  - 既存の標準やガイドラインは組織全体としての要件を規定
    ⇔現場技術者，管理者などそれぞれの立場でとるべき施策がすぐにわかるようにする
- **すぐに役立つ形で提供する**
  - シンプルな設問に答えるチェックリスト形式とする
  - チェックした施策を実際のシステムにも適用できるよう，施策の内容やポイントを具体的に示す
- **教育や啓発にも活用できるようにする**
  - チェック項目や施策への理解を深め，今後のセキュリティ対策に活かせるよう，解説を加える

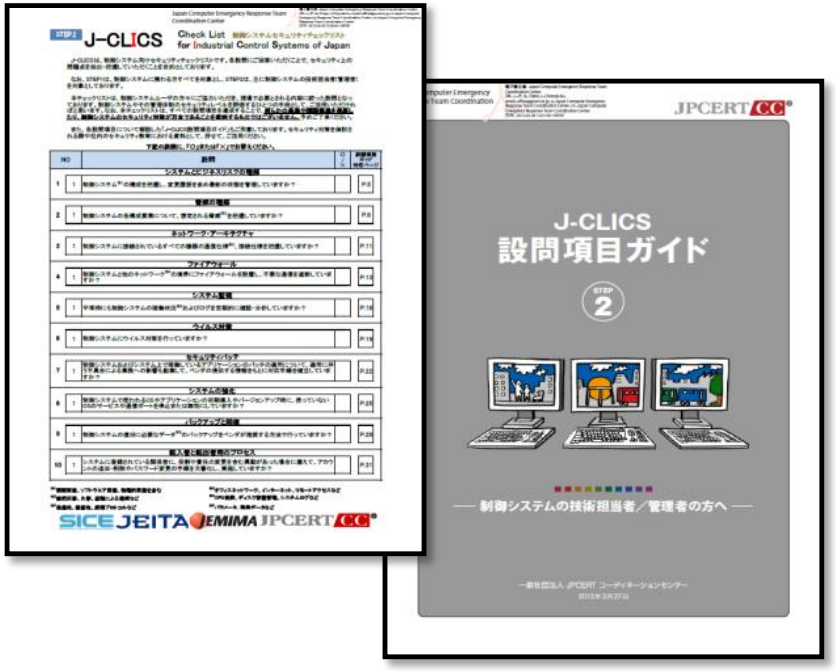
目次

J-CLICS の構成

- Step1（オペレータ・保守作業者などの現場担当者向け），
  Step2（システム技術者・マネージャ向け）の2部構成
- いずれもA4のチェックリスト1枚＋設問ガイドから構成



J-CLICS Step 1



J-CLICS Step 2

J-CLICS の構成

- 施策の実施状況を〇×式で回答

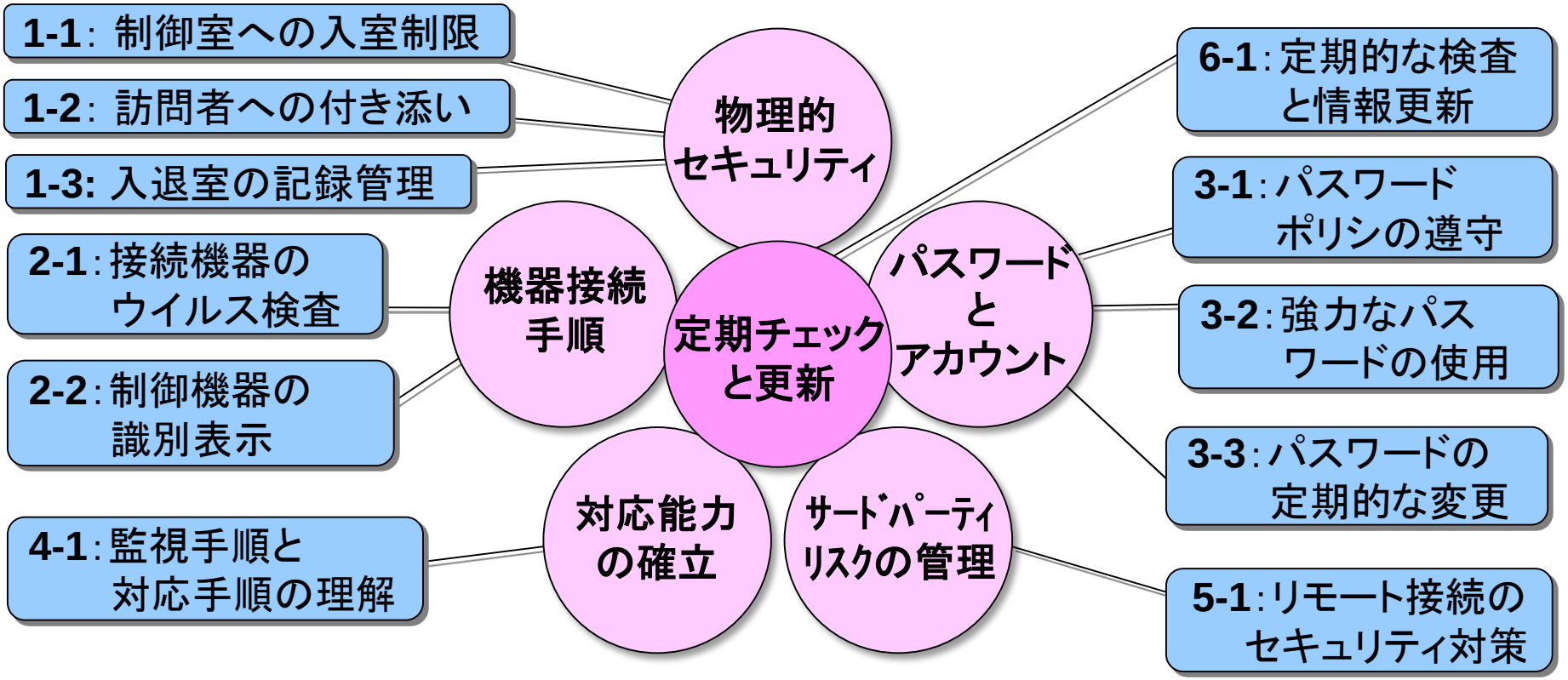
下記の設問に、「〇」または「×」でお答えください。

NO		設問	〇／×	設問項目ガイド対応ページ
		物理的セキュリティ		
1	1	制御室※1への入退室は、許可された関係者だけに限られていますか？		P.6
	2	制御室※1への訪問者には、常に関係者が付き添っていますか？		P.8
	3	制御室※1への入退室管理(記録と管理者による定期的な確認)を行っていますか？		P.10
		機器接続手順		
2	1	制御システムのネットワークに接続する機器※2について、事前にそれらがウイルスに感染していないことを確認する手順を守っていますか？		P.16
	2	制御システムの機器が情報系システムの機器と同じラックに設置されている場合、各機器がどちらのシステムのものであるかを(タグやシールなどで)分かるようにしていますか？		P.19

J-CLICS Step 1

Step1（現場担当者向け）設問項目

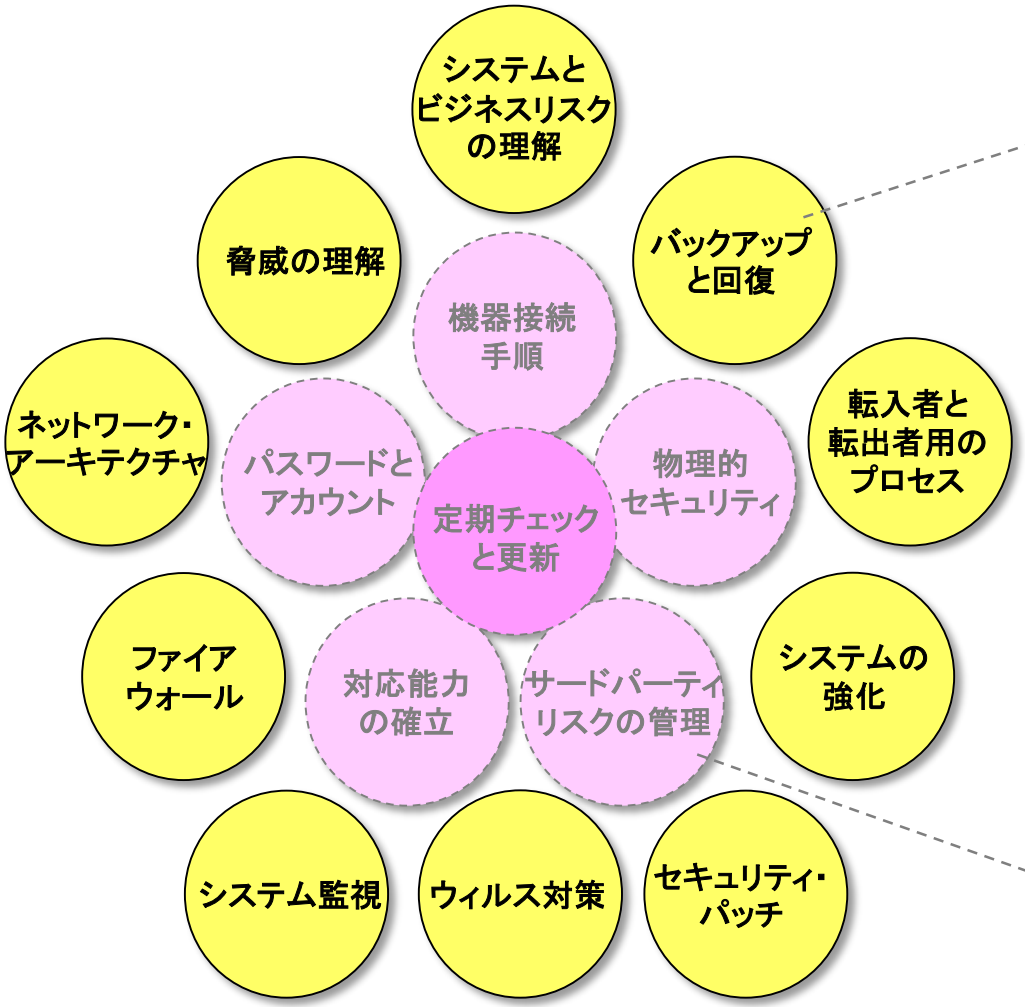
J-CLICS　Step1（現場担当者向け）
優先度の高い 6分野 11項目



Step1（現場担当者向け）チェックリスト

No.	設問
1	制御室への入退室は，許可された関係者だけに限られていますか？
2	制御室への訪問者には，常に関係者が付き添っていますか？
3	制御室への入退室管理(記録と管理者による定期的な確認)を行っていますか？
4	制御システムのネットワークに接続する機器について，事前にそれらがウイルスに感染していないことを確認する手順を守っていますか？
5	制御システムの機器が情報系システムの機器と同じラックに設置されている場合，各機器がどちらのシステムのものであるかを（タグやシールなどで）分かるようにしていますか？
6	制御システムのパスワードの強度と有効期限を含むパスワード・ポリシーがありますか？
7	強力なパスワードを使用していますか？
8	制御システムのパスワードを定期的に変更していますか？
9	制御システムにおけるセキュリティの監視手順や警報発生時，異常時の対応方法を理解し，訓練をしていますか？
10	リモート接続のセキュリティを確保するためのルールを守っていますか？
11	定期的に本J-CLICS(または，社内，業界団体等にて作成されたチェックリスト)を用いて制御システムセキュリティの自己評価を行っていますか？

Step2（システム技術者・管理者向け）設問項目



J-CLICS Step2
（システム技術者・管理者向け）
10項目

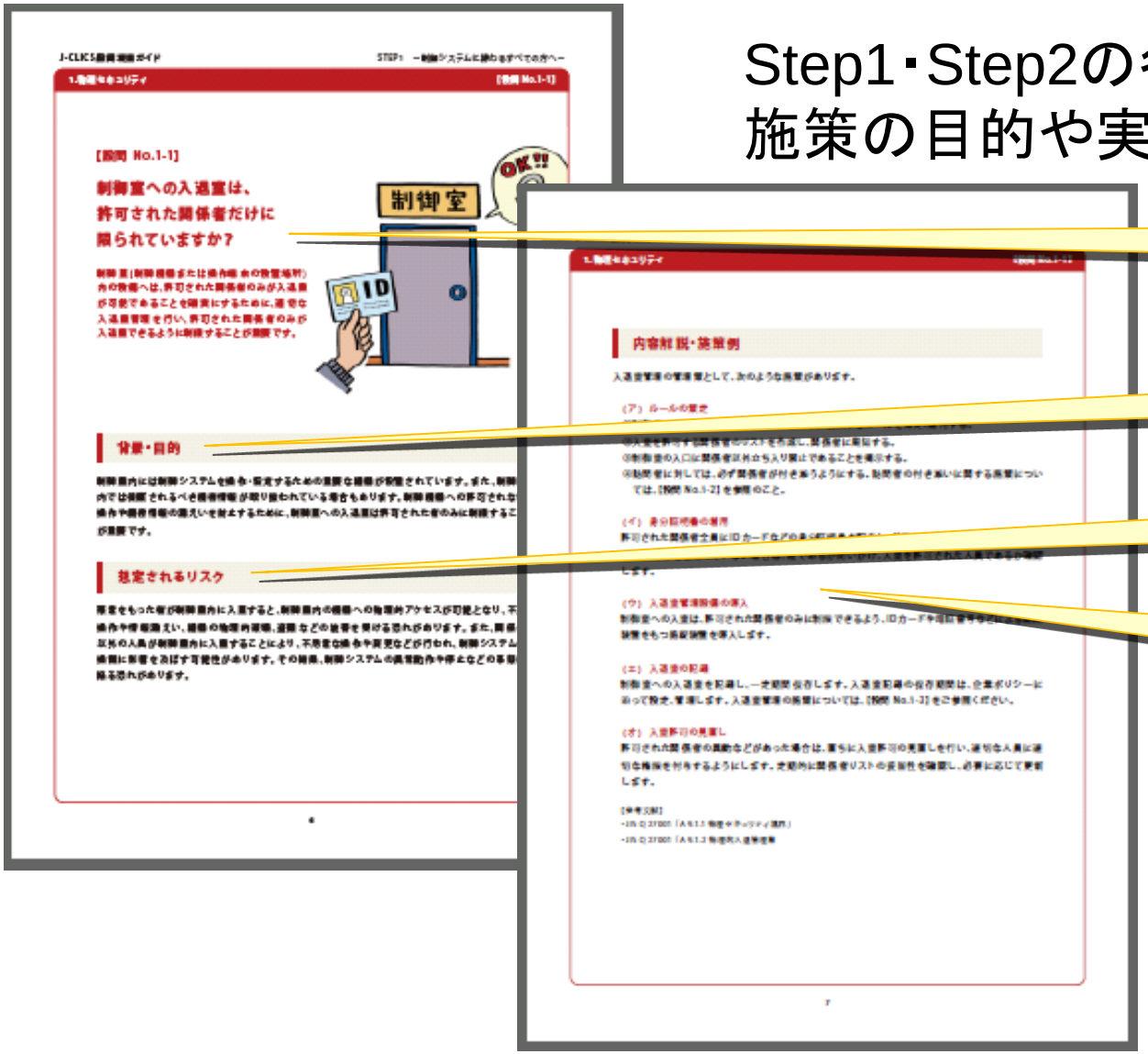
セキュリティ施策の強化に必要な，J-CLICS Step1よりもやや技術的・専門的な項目をサポート

Step1の設問分野

Step2（システム技術者・管理者向け）チェックリスト

No.	設問
1	制御システムの構成を把握し，変更履歴を含め最新の状態を管理していますか？
2	制御システムの各構成要素について，想定される脅威を把握していますか？
3	制御システムに接続されているすべての機器の通信仕様，接続仕様を把握していますか？
4	制御システムと他のネットワークの境界にファイアウォールを設置し，不要な通信を遮断していますか？
5	平常時にも制御システムの稼働状況およびログを定期的に確認・分析していますか？
6	制御システムにウイルス対策を行っていますか？
7	制御システムおよびシステム上で稼働しているアプリケーションのパッチの適用について，適用に伴う不具合による業務への影響も勘案して，ベンダの提供する情報をもとに対応手順を確立していますか？
8	制御システムで使われるOSやアプリケーションの初期導入やバージョンアップ時に，使っていないOSのサービスや通信ポートを停止または無効にしていますか？
9	制御システムの復旧に必要なデータのバックアップをベンダが推奨する方法で行っていますか？
10	システムに登録されている関係者に，役割や責任の変更を含む異動があった場合に備えて，アカウントの追加・削除やパスワード変更の手順を文書化し，実施していますか？

J-CLICS 設問項目ガイド



Step1・Step2の各設問における
施策の目的や実践例を解説

【設問】

【背景・目的】

【想定されるリスク】

【内容解説・施策例】

【参考文献】

【補足】

【設問・施策例1】物理的セキュリティ

＜設問 1-1＞

制御室への入退室は許可された関係者だけに限られていますか？

＜背景・目的・想定リスク＞

■制御室内には、制御システムを操作設定するための重要な機器や、保護されるべき機密情報があります。

■悪意を持った者が制御室に侵入すると、不正な操作によるシステムの異常動作や停止、機密情報の漏洩などの事態に陥る恐れがあります。

＜施策例＞

①入室制限ルールを策定する。　②入退室管理設備を設ける。

【設問・施策例2】システムの強化

＜設問 8-1＞

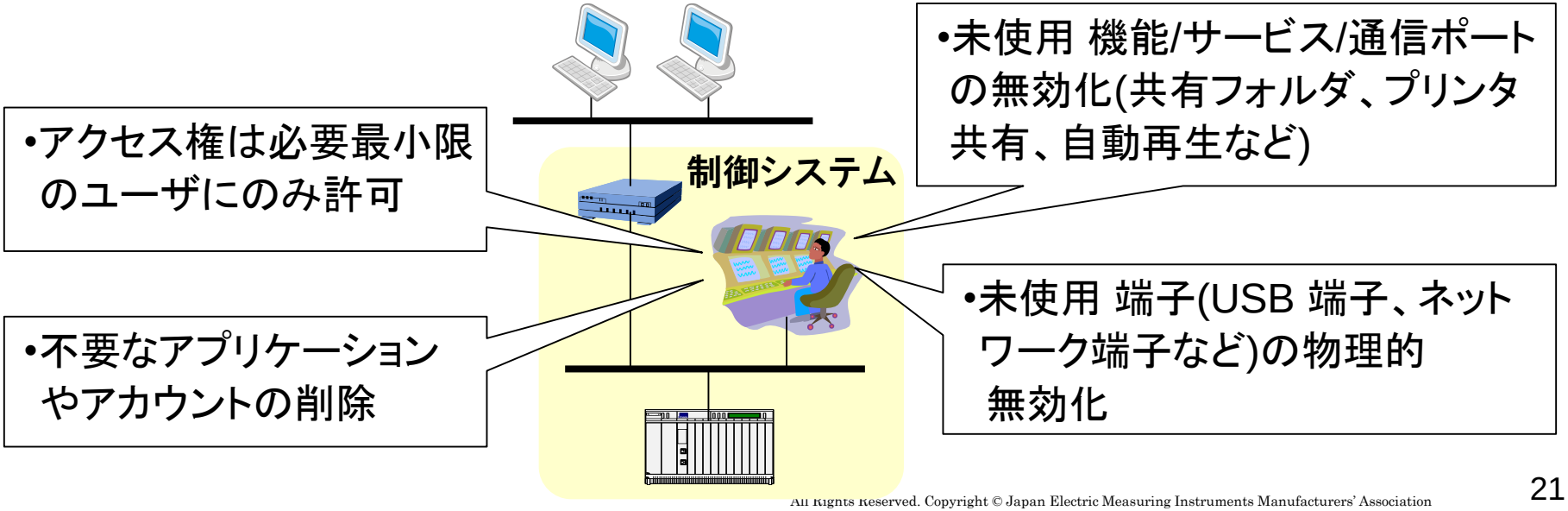
制御システムで使われるOSやアプリケーションの初期導入やバージョンアップ時に使っていないOSのサービスや通信ポートを停止または無効にしていますか？

＜背景・目的・想定リスク＞

不要なアカウントからの侵入や未使用の機能/サービス/通信ポートに関する脆弱性を使った攻撃により、異常動作や操業停止となる恐れがあります。

＜施策例＞

システムベンダのガイドに従いハードニング(要塞化)を行います。



目次

J-CLICSと国際標準の対比

- **J-CLICSの活用に対するユーザやベンダの関心**
  - ユーザ：J-CLICSの推奨施策でどのくらいの範囲が対策可能か？
  - ベンダ： J-CLICSをサポートするために，システムの構成や機能として何が必要か？
- **J-CLICSのチェック項目と国際標準 IEC 62443-3-3の項目を対比・紐付けする試みを実施（'15～'16）**

  【メリット】

  J-CLICSの推奨施策がより具体的・客観的になり，利便性の向上が期待される

J-CLICSと国際標準の対比

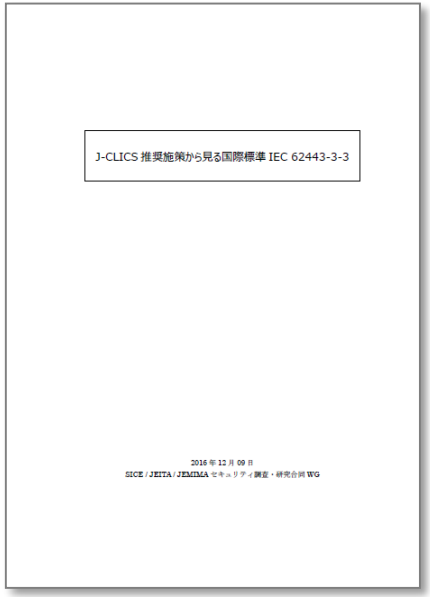
J-CLICSの設問項目ガイドに記載の推奨施策は以下の3種類に分類されます。

1）ユーザだけで実施できるもの
2）ユーザが制御システムベンダからの情報に基づいて実施できるもの
3）制御システムが機能として提供するもの、あるいは提供が望ましいもの

一方、国際標準 IEC 62443-3-3では、制御システムが備えるべきセキュリティ機能を基本要件（SR）・強化要件（RE）として挙げています。

3）に分類される推奨施策をIEC 62443-3-3のSR・REと対比し，一覧化した参考資料
「J-CLICS推奨施策から見る国際標準IEC 62443-3-3」を作成しました。
（'17/3よりJEMIMA Webサイトで公開中）

SR: System Requirement
RE: Requirement Enhancement



J-CLICS推奨施策から見る
国際標準 IEC 62443-3-3

J-CLICSと国際標準の対比

- **対比内容の記載例**
  （「J-CLICS推奨施策から見る国際標準IEC 62443-3-3」より抜粋）

J-CLICSの設問・推奨施策

J-CLICS Step1	2. 機器接続手順
設問 No.2-1	制御システムのネットワークに接続する機器※5について、事前にそれらがウイルスに感染していないことを確認する手順を守っていますか？
関連する SR	SR3.2　悪意のあるコードの防御 SR3.3　セキュリティ機能の検証 SR3.4　ソフトウェアと情報の完全性
関連の考え方	本 SR の機能は、事前のウイルスチェックに加えて、運用中や保守時のウイルスチェックやウイルス検知、ウイルス感染拡大の防止に有効です。

IEC 62443-3-3の機能要件（SR）

設問とSRとの対応の内容

- **このほか，対応するSRの内容の解説（和訳）も記載**

※IEC 62443-3-3からの引用はJSAの了解のもとで行い、翻訳はSICE/JEITA/JEMIMAセキュリティ調査・研究WGの責で実施。

目次

J-CLICSの見直しと拡充（活動中）

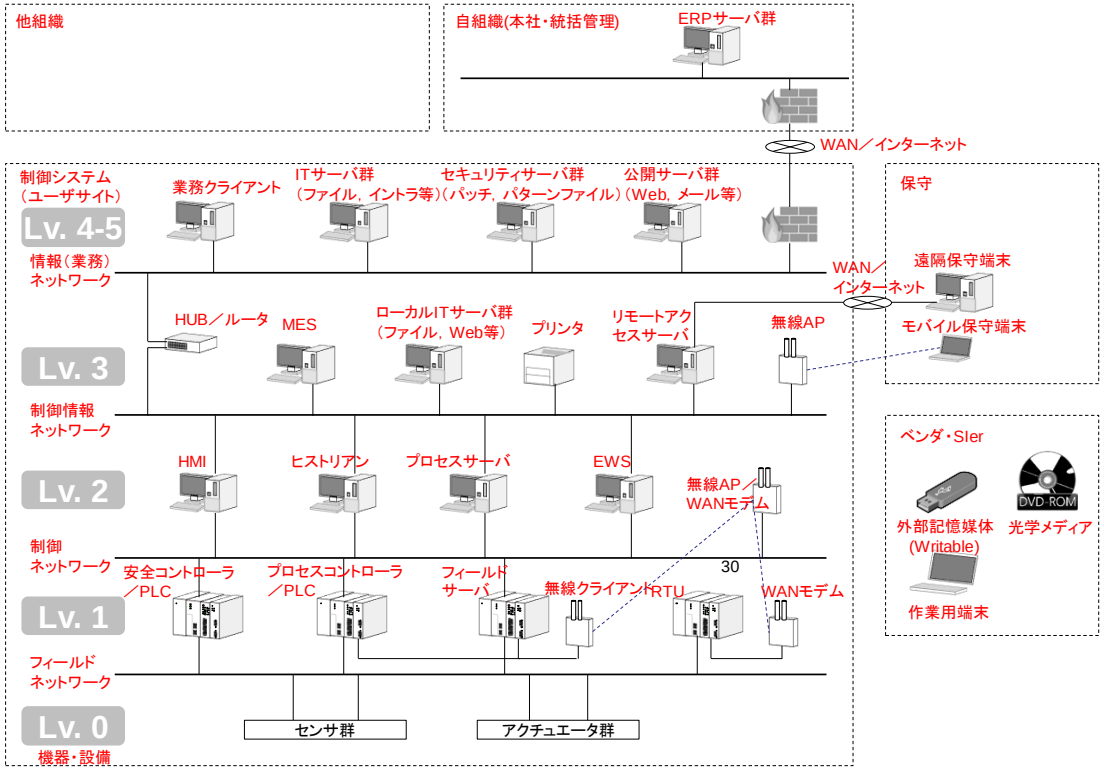
- **J-CLICSの有用性を維持するため，セキュリティ環境の変化や新しい制御システムの姿に対応していくことが必要**
  - レガシー技術の脆弱性など，分野固有の知識を悪用した攻撃手段の巧妙化
  - IoTなどを活用した制御システムへの進化
    ⇒「よりつながる」＝攻撃者からもつながりやすい？
  - 制御システム間の連携
    ⇒関連組織を踏み台にした攻撃

J-CLICSの見直しと拡充（活動中）

- J-CLICSが現在のセキュリティ環境にどの程度対応できているかを改めて検証する活動を開始しています

  - 起きうる攻撃の種類や侵入経路をモデル化し，現在の推奨施策でどこまで阻止できるかを検討

  - 新たな対応が必要になった部分について，推奨施策の見直しや拡充を検討していきます



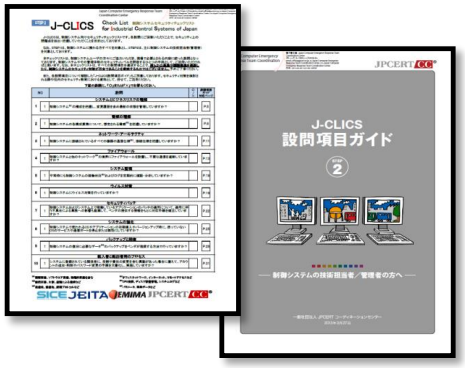
制御システムの構成モデル

目次

1. セキュリティ合同WGのご紹介
2. 背景とJ-CLICSの開発目的
3. J-CLICSの構成と推奨施策例
4. J-CLICSの発展改良
   - 4.1 国際標準との対比
   - 4.2 見直しと拡充（活動中）
5. まとめ

まとめ

- **セキュリティ対策の足掛かりとして活用可能なチェックリストJ-CLICSを開発**
  - 制御システムに携わる立場ごとに最適化した，Step1／Step2の2部構成
  - 対策立案や教育・啓発にも使える項目ガイド付き
- **国際標準との対比資料を作成**
  - セキュリティ対策への理解を深める参考情報として，J-CLICSの推奨施策と国際標準 IEC 62443-3-3を対比した資料を作成・公開
- **J-CLICSの拡充・見直し活動を開始**
  - セキュリティ環境の変化に対応するため，チェック項目や推奨施策の再検証に着手

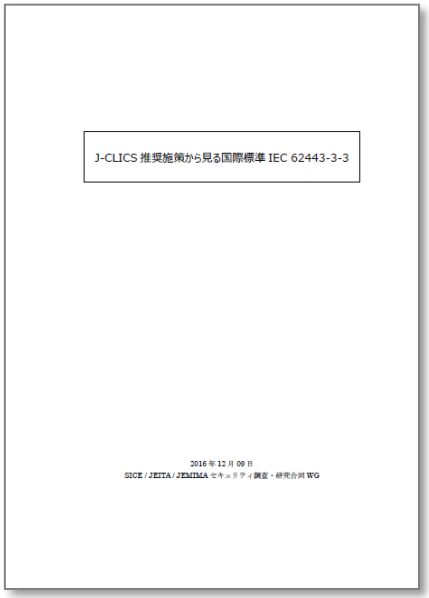


J-CLICS Step 1 & Step2

J-CLICS・対比資料の公開

- **制御システムに携わる方を対象に，J-CLICSを無償配布中**
  - JPCERT/CC様のWebサイトからダウンロード可能
    （https://www.jpcert.or.jp/ics/jclics.html）
  - 対比資料「J-CLICS 推奨施策から見る国際標準 IEC 62443-3-3」はJEMIMAより公開中
    （https://www.jemima.or.jp/activities/strategic-project/strategic-project-4/339.html）

制御システムのセキュリティ向上のため，
J-CLICSをぜひご活用ください！



J-CLICS**推奨施策から見る**
国際標準 IEC 62443-3-3

JEMIMA

ご静聴ありがとうございました