JEMIMA

計測展2018 OSAKA 委員会セミナー

IoT時代に必要な無線計装と制御システムセキュリティ

すぐできる、自分でできる
簡単セキュリティ対策J-CLICS

2018.11.08

SICE/JEITA/JEMIMA
セキュリティ合同WG

本セッションの御品書き

- 制御システムセキュリティ自己評価ツール
  J-CLICSを活用頂けるようにご用意いたしました

始 生い立ち

今 活用方法

躍 今後の展望

本セッションの御品書き

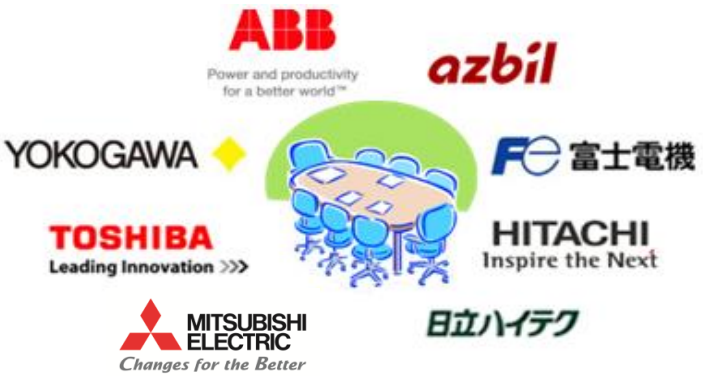
始 生い立ち

- 誰が作っているの？
- なぜJ-CLICSを開発したの？
- J-CLICSの目的は？

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
  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㈱、
  ㈱東芝ｲﾝﾌﾗｼｽﾃﾑｽﾞ、㈱日立製作所、
  ㈱日立ﾊｲﾃｸｿﾘｭｰｼｮﾝｽﾞ、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調査・改良
  6. J-CLICSの作成　国際標準との対比
  7. **J-CLICSのバージョンアップ**



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, RRI
- **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

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

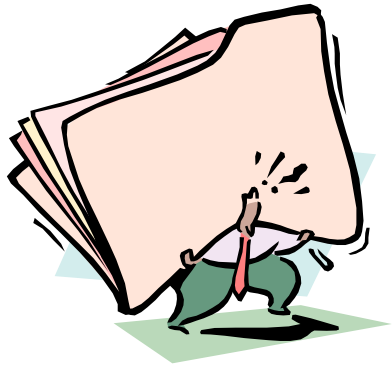
制御システムセキュリティの現状

- **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

本セッションの御品書き

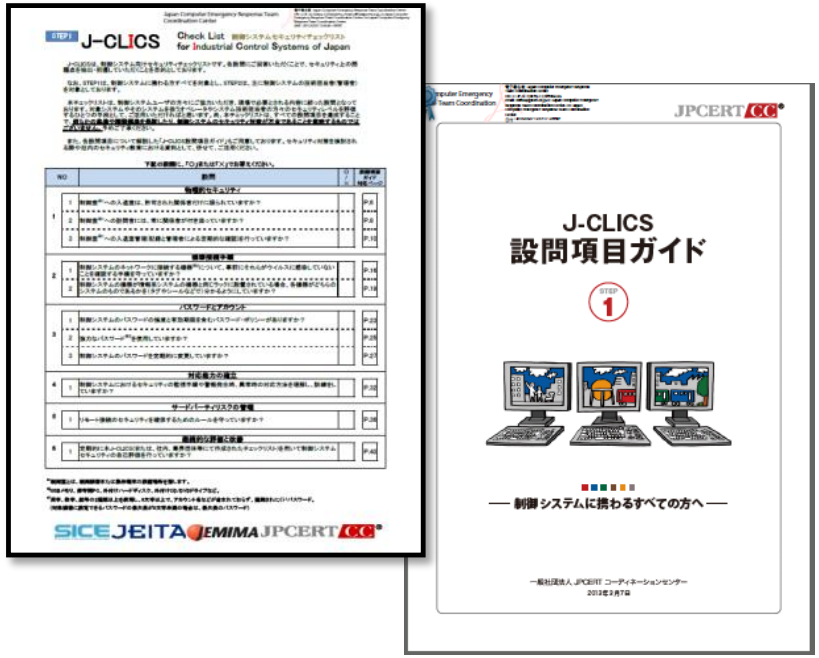
今

活用方法

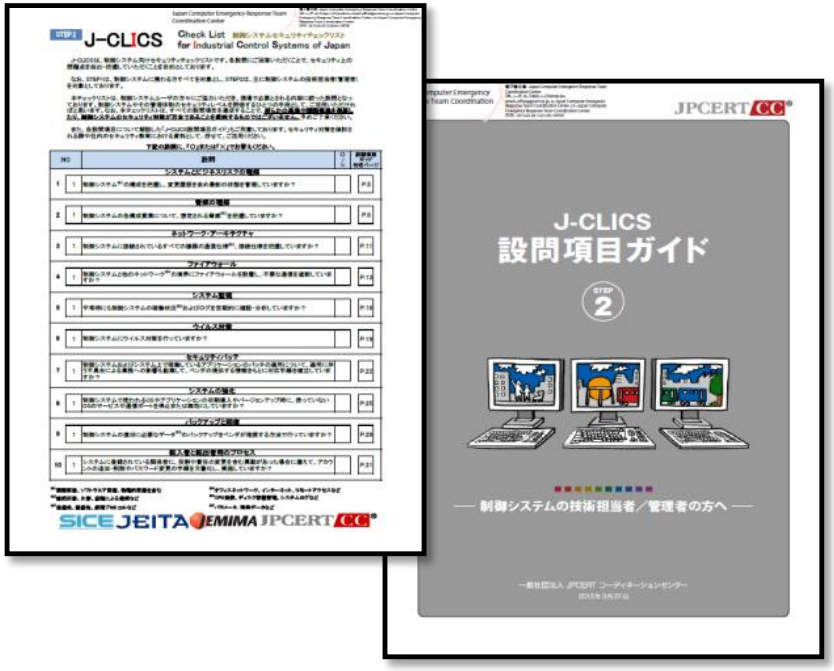
- J-CLICSはどんなもの？
- J-CLICSはどうやって使うの？

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

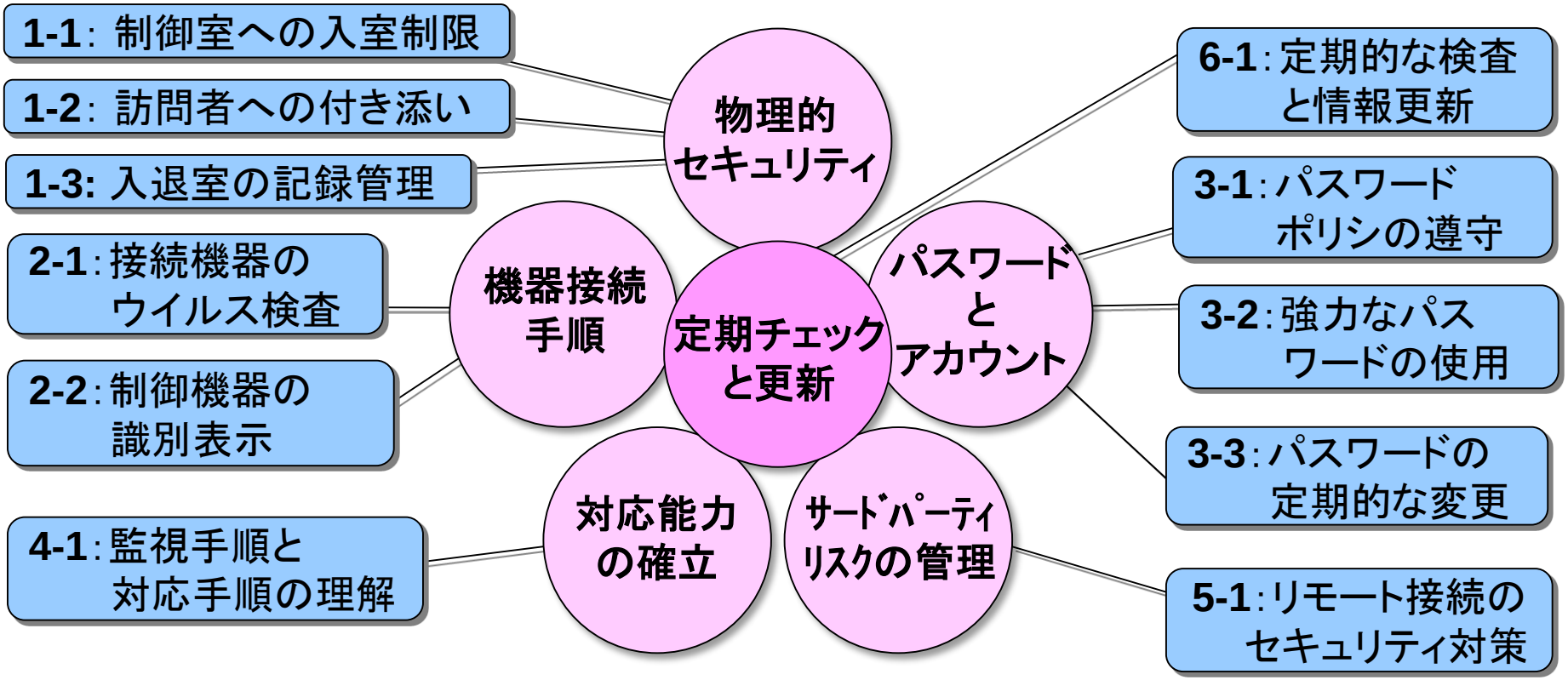
下記の設問に、「〇」または「×」でお答えください。

NO		設問	〇／×	設問項目ガイド対応ページ
1		**物理的セキュリティ**		
	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
2		**機器接続手順**		
	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

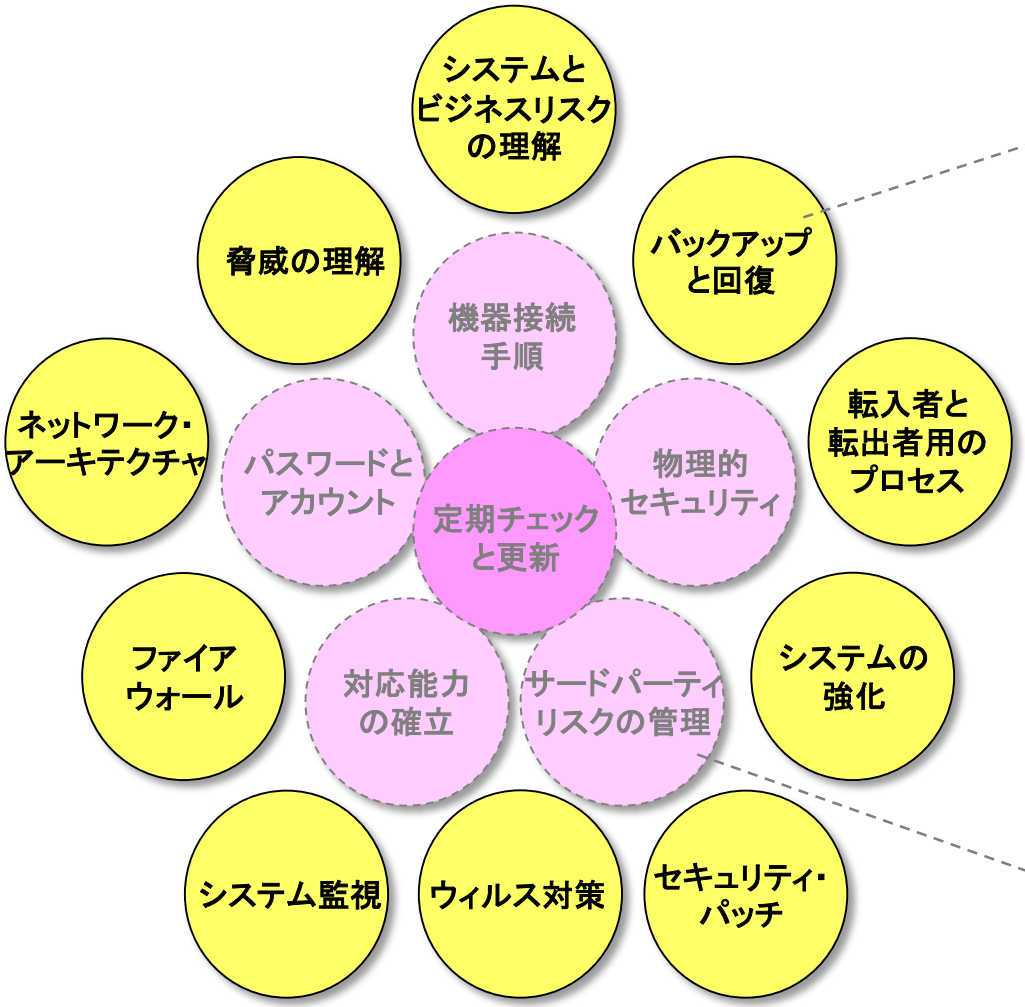
J-CLICS Step 1

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



Step2（システム技術者・管理者向け）設問項目

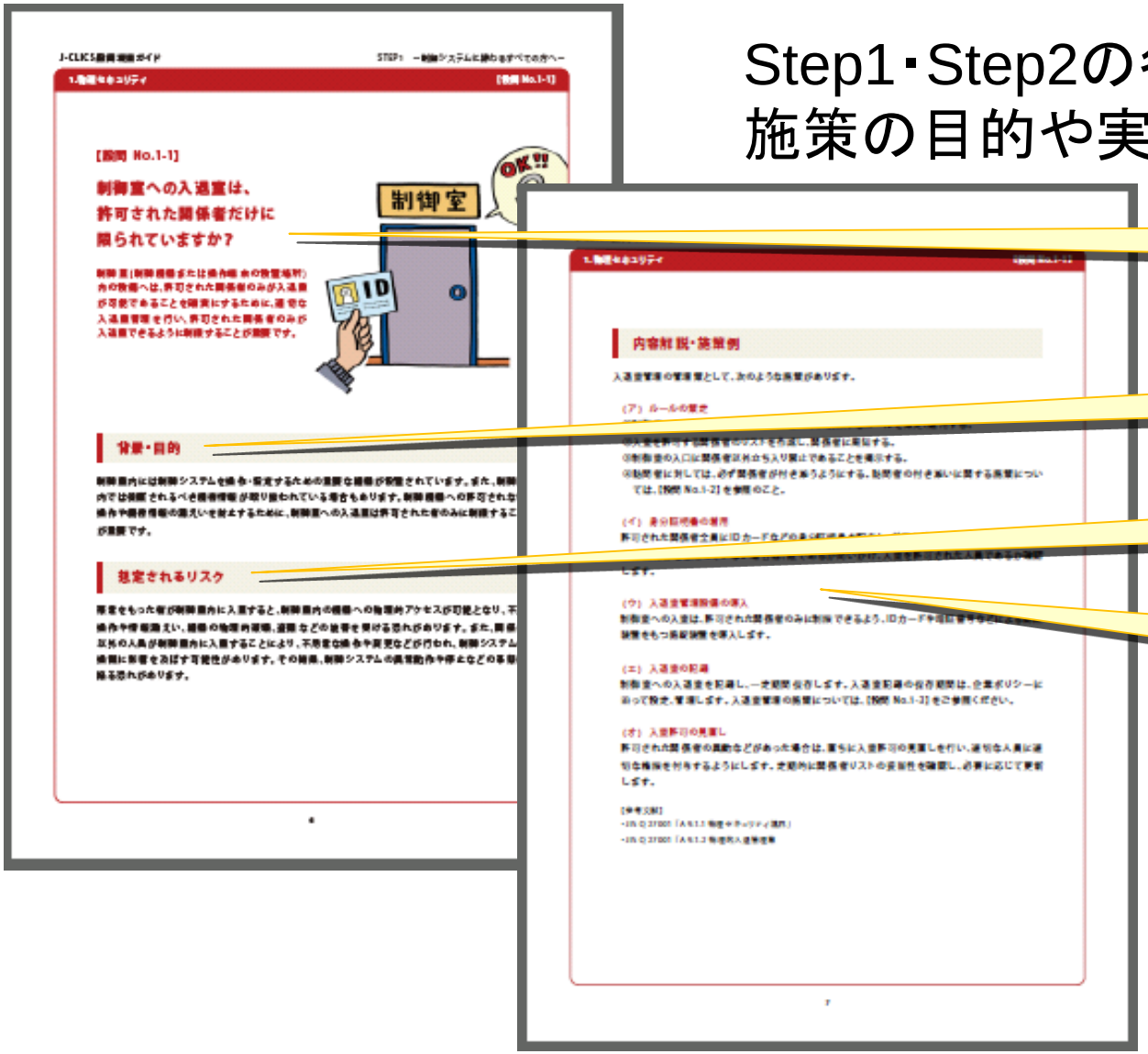


J-CLICS Step2
（システム技術者・管理者向け）
10項目

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

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】

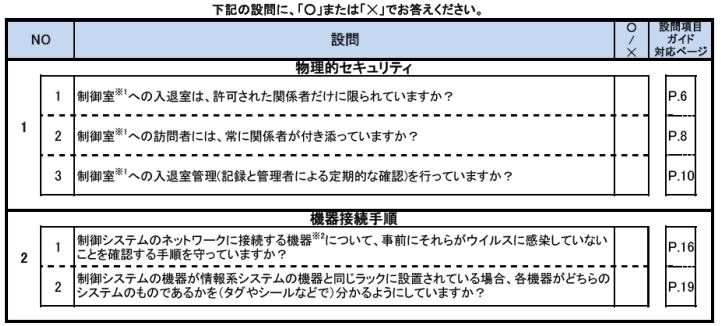
【内容解説・施策例】

【参考文献】

【補足】

J-CLICS 利用の推奨手順

- **入手する**（https://www.jpcert.or.jp/ics/jclics.html）
  - Webの検索で「J-CLICS」と入力
  - JPCERT/CCのサイトから無償でダウンロード
- **項目をチェックする**
  - 自社の現状をチェックリストに○×で反映
- **×の項目を精査する**
  - 設問ガイドで×がついた項目の対策を確認する
  - 実施方法を検討する
- **再実施する**
  - 定期的に項目のチェックを行う



下記の設問に、「○」または「×」でお答えください。

NO		設問	○／×	設問項目ガイド対応ページ
1	物理的セキュリティ			
	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
2	機器接続手順			
	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

【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？

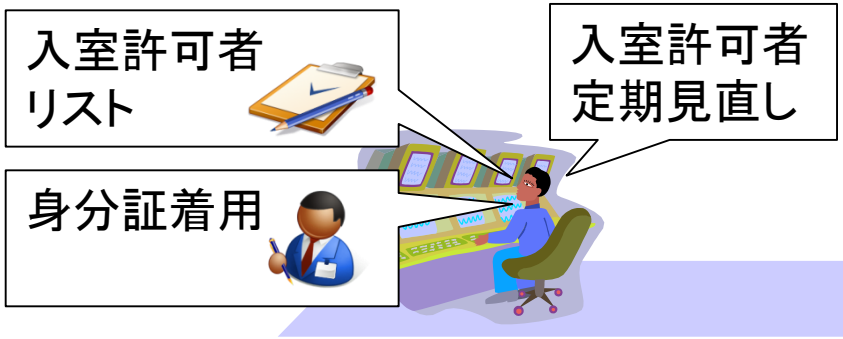
＜背景・目的・想定リスク＞

■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。

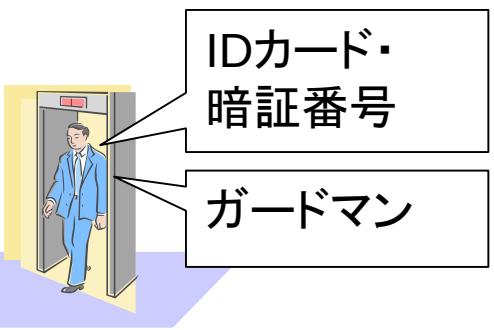
■悪意を持った者が制御室に侵入すると、不正な操作によるシステムの異常動作や停止、機密情報の漏洩などの事態に陥る恐れがあります。

＜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＞

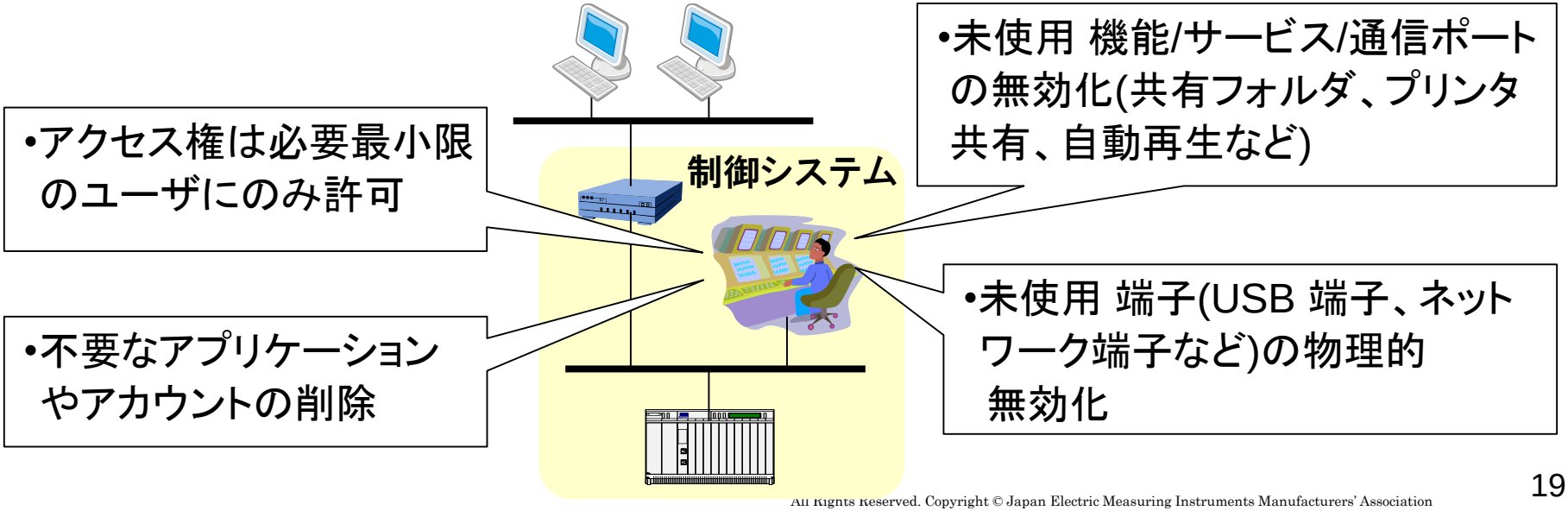
制御システムで使われるOSやアプリケーションの初期導入やバージョンアップ時に使っていないOSのサービスや通信ポートを停止または無効にしていますか？

＜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。



本セッションの御品書き

今

活用方法

- **J-CLICSはどんなもの？**
  -> 21のチェックリストと、そのガイドで構成される文書
- **J-CLICSはどうやって使うの？**
  -> 自己評価して、不十分な所への対策を検討する

本セッションの御品書き

躍 今後の展望

・J-CLICSを分析する
・J-CLICSを改定する

J-CLICSの現状と課題

- **現状**
  - J-CLICSは策定から4年が経過
  - 策定時に想定できなかったセキュリティ脅威への対策が手薄
  - 項目やガイドの拡充・見直しを含めた改良について議論中
- **主な課題**
  - J-CLICSは対策としてどこまでカバーできるのかを明らかにしたい
    → 足りないところや実態に合わないところを拡充・見直し
  - 制御システムの新しい動きにも合ったガイドラインにしたい
    → IoTや，Industrie4.0，Industrial Internetのような
    「より深くつながる 制御システム」に向けたセキュリティ対策を検討

拡充の背景：ITとOTの違い

- **IT: 防御は困難**
  - さまざまな場所・さまざまな利用者・さまざまな目的
  - 攻撃経路もさまざま
    → 攻撃経路が多いので、
    エンドポイントでの検知・緩和・回復施策で対応
- **OT: 防御が必須**
  - 限られた場所・限られた利用者・限られた目的
  - 攻撃経路が限られている
  - 攻撃で甚大な被害がでる恐れがある
    → 攻撃到達が受忍できないので、
    攻撃経路での防御施策で対応

拡充の背景:防御の要点

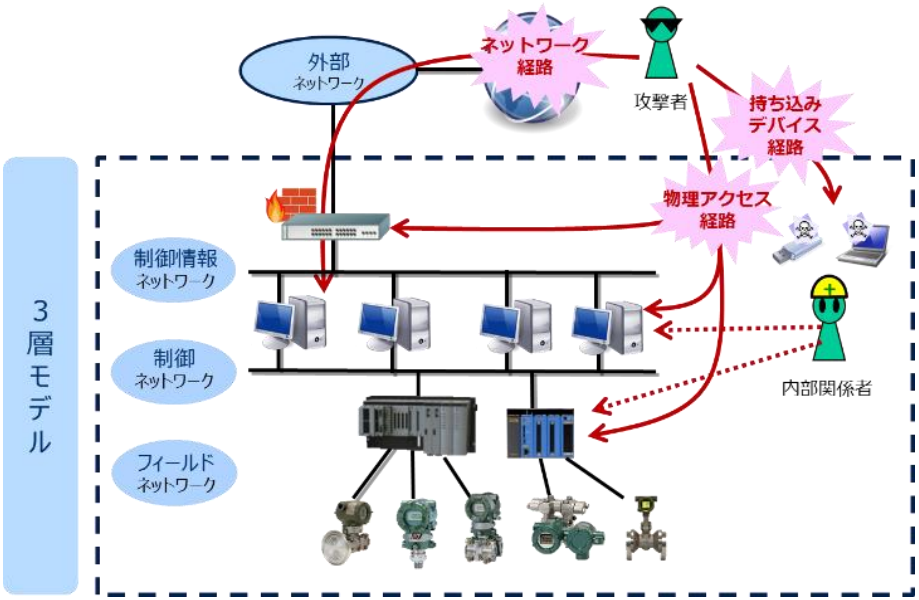
- **攻撃は外部から来る**
  - 外から中（攻撃手順）の順に対策を行う
- **弱いポイントから狙われる**
  - 全ての経路を把握する
  - 弱い経路から対策する
- **攻撃成立には条件がある**
  - 攻撃成立のための条件を把握する
  - 条件成立のタイミングを減らす
  - 条件成立時の作業は厳戒態勢で行う

旧 J-CLICS と 新 J-CLICS（案）

- **旧 J-CLICS**
  - 実施しやすく効果の高い施策を記載
    - 防御・検知・緩和・回復の施策が入り混ざっている
    - 施策の優先順位がつけられていない
    - 対策後の残留リスクが明らかでない
- **新 J-CLICS（案）** 検討中
  - 攻撃経路に対する防御施策を記載
    - 防御・検知・緩和・回復の視点を明らかにする
    - リスクの高い攻撃経路の防御を優先する
    - 対策済経路、未対策経路がわかるようにする

新J-CLICSの検討　検討中

1. モデルシステムを設定
2. 攻撃経路を網羅的に列挙
3. 攻撃手順を網羅的に列挙
4. 各手順の成立条件を列挙
5. 条件を崩す対策を列挙



6. 攻撃経路・手順と対策を重要度がわかる形でマッピング

→ 各対策の対象・効果・重要度が可視化され
より効果的なセキュリティ対策が可能に

新J-CLICS イメージ　検討中

- 攻撃経路ベースのセキュリティ施策マップ

第２軸　優先度高 → 優先度低

第１軸　優先度高 → 優先度低

攻撃経路	脅威		対策			
	攻撃手順	成立条件	防御策	検知策	緩和策	回復策
経路１	手順１	条件１	防御策１	検知策１	緩和策１	回復策１
	手順２				2	回復策２
	手順３				3	回復策３
	手順４				4	回復策４
経路２	手順１				1	回復策１
	手順２	条件２	防御策２	検知策２	緩和策２	回復策２
	手順３	条件３	防御策３	検知策３	緩和策３	回復策３

各攻撃経路ごとに
攻撃手順・成立条件を挙げ
防御・検知・緩和・回復策を列挙

各セキュリティ施策の 対象脅威・優先度がマップ化

→ 対策状況が可視化され、
効果的なセキュリティ施策の 計画・配置が可能になる

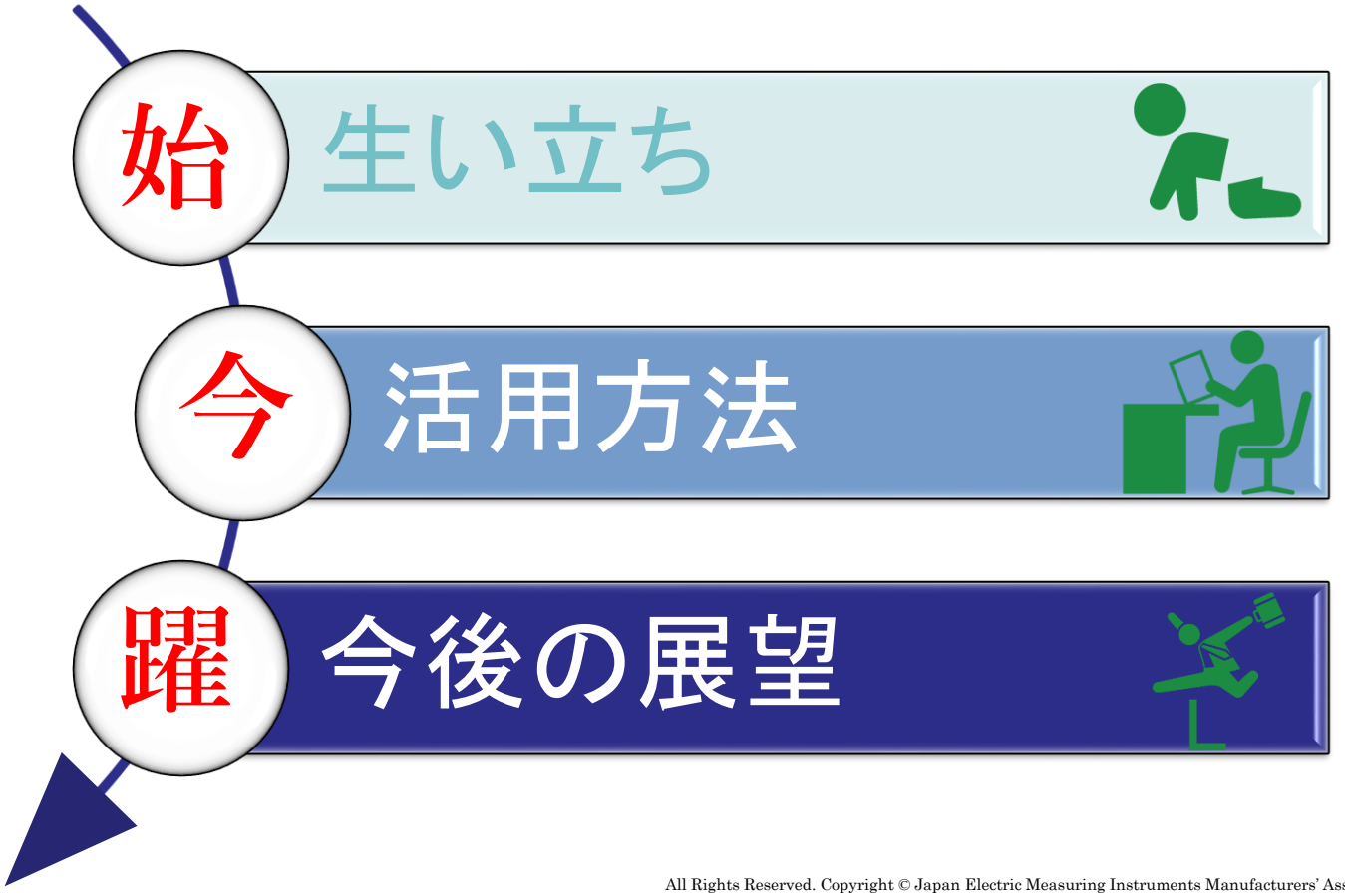
本セッションの御品書き

躍 今後の展望

- J-CLICSを分析する
  - -> 初版策定から4年が経過
  - -> カバー範囲が明らかではない
  - -> 新しい動きに追従できていない
- J-CLICSを改定する
  - -> 攻撃経路と防御施策のマップを提供する
  - -> 対策の優先順位が分かりやすいようにする

本セッションのまとめ

- 制御システムセキュリティ自己評価ツール
  J-CLICSを活用頂けるようにご用意いたしました



まとめ

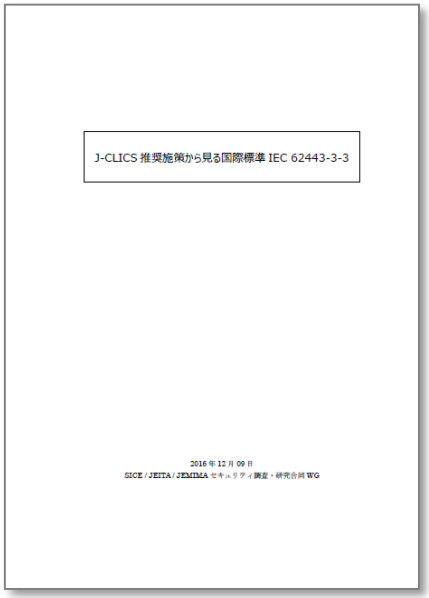
- **生い立ち**
  - SICE/JEITA/JEMIMAセキュリティ合同WGで**セキュリティ対策の足掛かりとして活用可能なチェックリストを作成した。**
- **活用方法**
  - **チェックリストとガイドを使い自己評価して セキュリティ対策が不十分なところを見つけだし検討する。**
- **今後の展望**
  - **新しい動きに追従した改訂版を提供する。**
  - **対策の優先順位が分かるような情報を提供する。**
  - **J-CLICSで対策できる部分とできない部分が分かる 攻撃経路と対策のマップを提示する。**

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

    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・公開しています
    （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

ご静聴ありがとうございました