計測展2014 OSAKA　JEMIMA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」

2014.11.19

PA・FA計測制御委員会
SICE/JEITA/JEMIMA
セキュリティ合同WG

目次

1. セキュリティ合同WGのご紹介
2. 背景と目的
3. J-CLICSの開発
4. J-CLICSの構成
5. J-CLICS Step1 のご紹介
6. J-CLICS Step2 のご紹介
7. まとめと今後の予定

目次

SICE/JEITA/JEMIMAセキュリティ合同WG

- **活動目的**

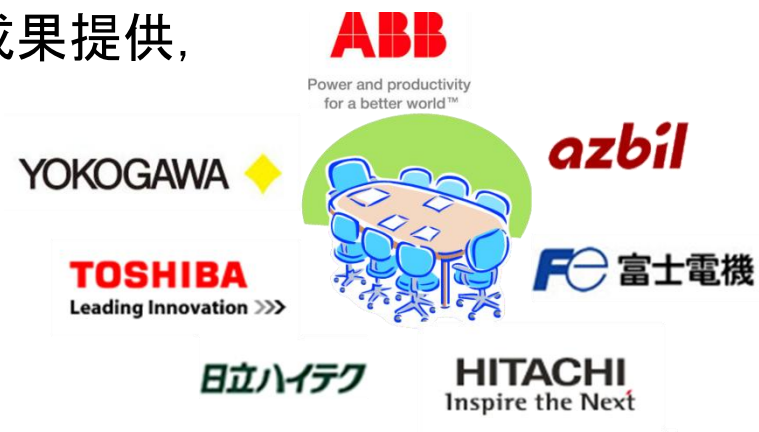
  製造業分野におけるセキュリティ標準化動向，技術等の調査・研究活動と会員企業・ユーザへの成果提供，展示会・各種会議での広報

- **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ｽﾞ、富士電機 ㈱、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
- **広報活動**
  - 計測展委員会セミナー
  - JPCERT/CC
    制御システムセキュリティカンファレンス
  - 計装制御技術会議
  - 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

1. セキュリティ合同WGのご紹介
2. 背景と目的
3. J-CLICSの開発
4. J-CLICSの構成
5. J-CLICS Step1 のご紹介
6. J-CLICS Step2 のご紹介
7. まとめと今後の予定

制御セキュリティの現状

- **制御システムに対する脅威が拡大**
  - '10のStuxnet出現以降，制御システムのセキュリティ確保が大きな課題に
    - ➢ 一般の制御システムを標的とした攻撃活動も観測
  - 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

- **セキュリティ対策の標準化**
  - 欧米の政府機関や業界団体による標準・ガイドラインが多数策定済み
    - ➢ ISA-99【米ISA】→IEC62443として国際標準化進行中
    - ➢ SCADA Security Good Practice Guide【英CPNI】

ISA : Intrernational Society of Automation
CPNI : Centre for Protection of National Infrastructure

制御セキュリティの課題

- **既存システムでは対策進まず**
  - いまだ多くのシステムが無防備 or 対策不十分なまま
    - ➢ 何をすべきかわからない，
      予算がない，・・・

- **何が問題か？**
  - 既存の標準やガイドラインは到達目標を定めたものであり，
    「いつ，誰が，何をすべきか」の具体的な提示が不十分

J-CLICS開発の動機と目的

- **動機**
  - 既存の制御システムを保護する施策が早急に必要
  - 現場作業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**
  - セキュリティ対策の足掛かりとして，制御システムの運用担当者が現状を手軽に把握できるツールを提供する
  - 制御システムに関わる全ての人が行うべき施策の例をわかりやすく，実施しやすい形で提供する

→SICE/JEITA/JEMIMAセキュリティ合同WGがユーザ企業・JPCERT/CCと協力してJ-CLICSを作成

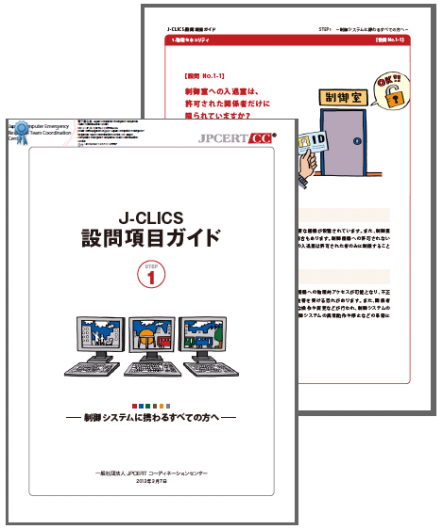
目次

1. セキュリティ合同WGのご紹介
2. 背景と目的
3. J-CLICSの開発
4. J-CLICSの構成
5. J-CLICS Step1 のご紹介
6. J-CLICS Step2 のご紹介
7. まとめと今後の予定

J-CLICSとは？

- **制御システムユーザ向けセキュリティチェックツール**
  - 制御システムのセキュリティ対策状態を手軽にチェック可能
- **重要項目を厳選した「チェックリスト」**
  - Step1：最初に実施すべき基本の11項目
  - Step2：より広い範囲を扱う追加の10項目
- **推奨施策を収録した「設問ガイド」**
  - 各項目の背景や内容の説明を記載
  - 対策に着手する際のヒントとなる施策例などを収録

J-CLICS チェックリスト

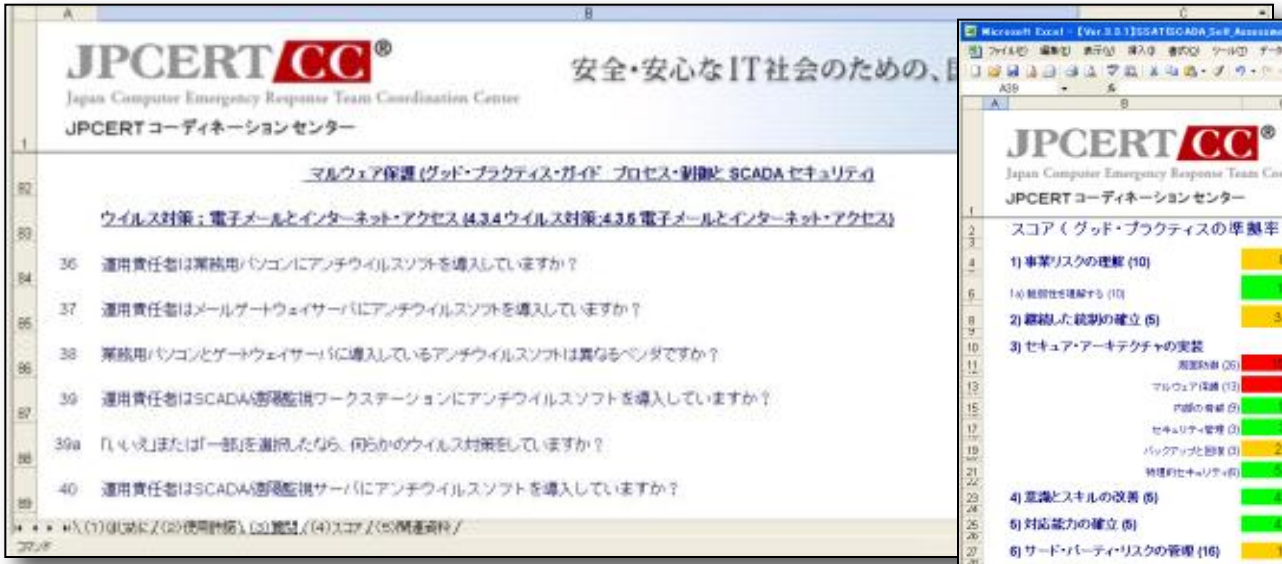


J-CLICS 設問ガイド

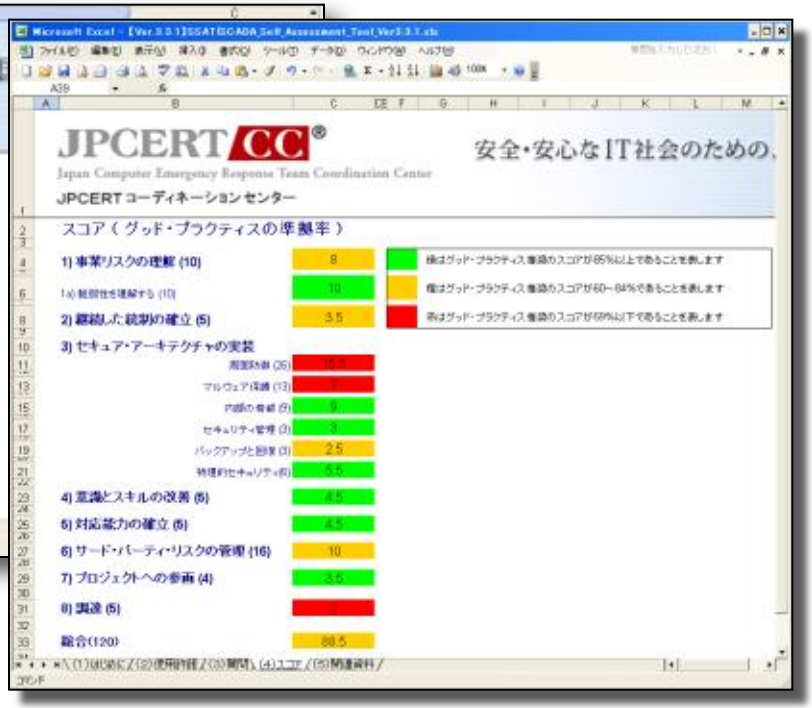
J-CLICS : Check List for Industrial Control System of Japan

J-CLICSの前身：セキュリティ自己評価ツールSSAT

- **SCADA Self Assessment Tool（SSAT）とは？**
  - 英国政府機関CPNIが制御セキュリティガイドとともに作成した自己評価ツール
  - 約100問の短い設問で施策の達成状況や問題点を診断
  - 技術的施策から管理施策までのカテゴリをバランス良くカバー



日本語版SSAT チェックシート



SSAT診断結果例

改良版SSATの作成

- **SSATの評価・改良（'10年度）**
  - SICE/JEITA/JEMIMAセキュリティ合同WGにて利用しやすさを評価
  - 難解な設問があったため，専門知識がなくとも理解しやすい表現に改良
    →JPCERT/CCより「日本版SSAT」として公開
- **ユーザからのフィードバック**
  - アンケートや意見交換会を通じ，試用頂いたユーザ企業／団体から意見を収集
  - **「設問数が多すぎる」「わかりづらい項目がある」「項目が実現困難」「どう対策すべきかわからない」などの現場の声**

ベンダとユーザが協力して検討

J-CLICSの開発

- **生の意見からわかったSSATの問題点**
  - 一つのチェックリストで組織全体を俯瞰
    →現場作業者・技術者など個々の立場ですべきことが
    わかりにくい
  - 経営者向けの設問も多く収録
    →実際に対策するのは現場作業者や技術者。
    予算や人員が必要な施策を説いても？？

→SSATの形に拘らず，使い易さ重視のツールとすることが目標。
J-CLICS（Check List for Industrial Control System）と命名

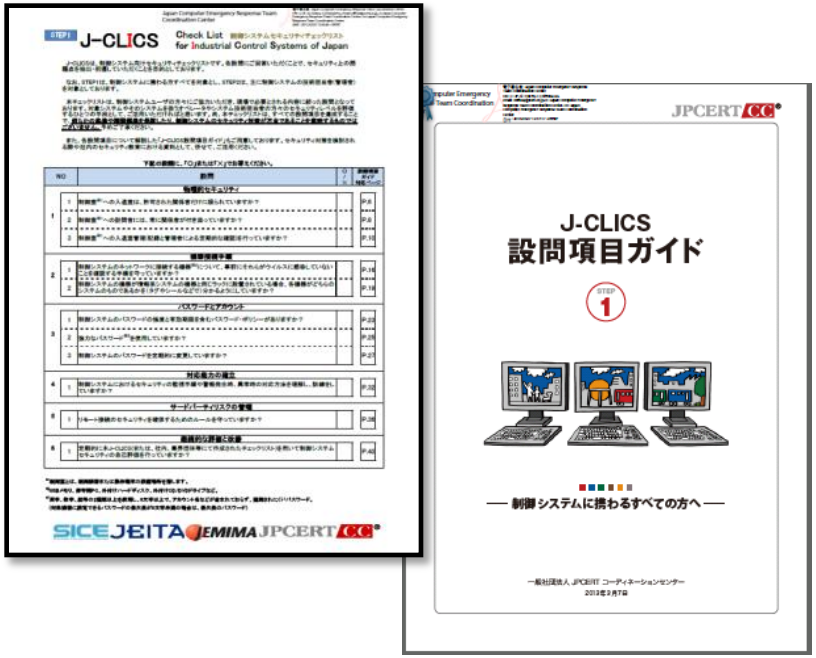
- **改良方針**
  - 現場担当者，技術者・マネージャそれぞれに最適化した設問構成
  - 各読者層の立場で最低限できる／すべき施策を厳選
  - 対策立案や教育・啓発にも活用できる各設問の解説資料

目次

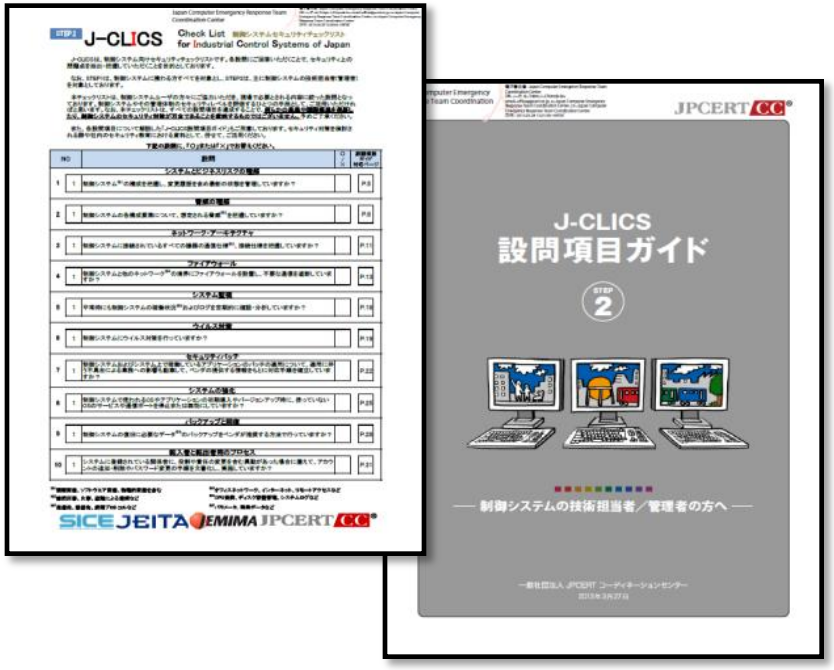
1. セキュリティ合同WGのご紹介
2. 背景と目的
3. J-CLICSの開発
4. **J-CLICSの構成**
5. J-CLICS Step1 のご紹介
6. J-CLICS Step2 のご紹介
7. まとめと今後の予定

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

- 分野ごとに重要施策の実施状況を〇×式で回答

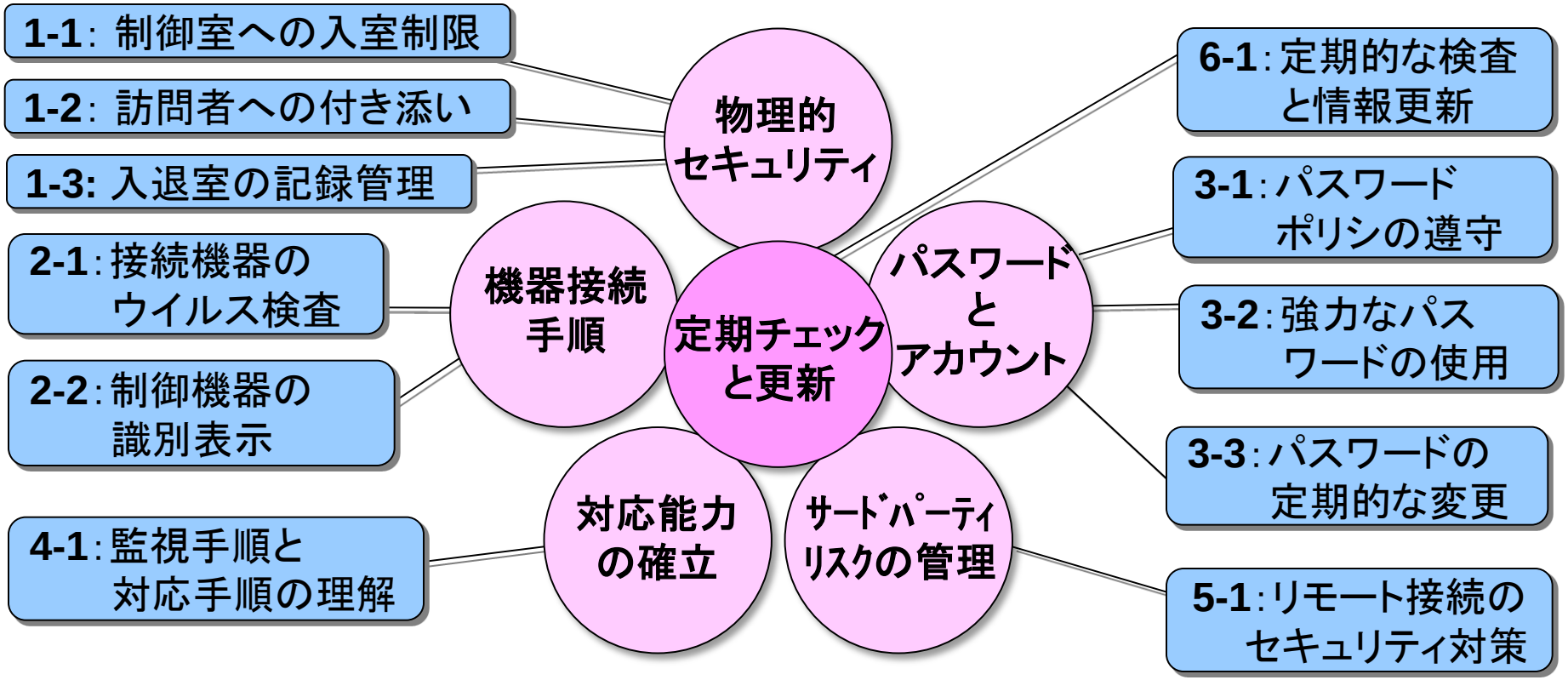
下記の設問に、「〇」または「×」でお答えください。

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

J-CLICSの設問項目（Step1）

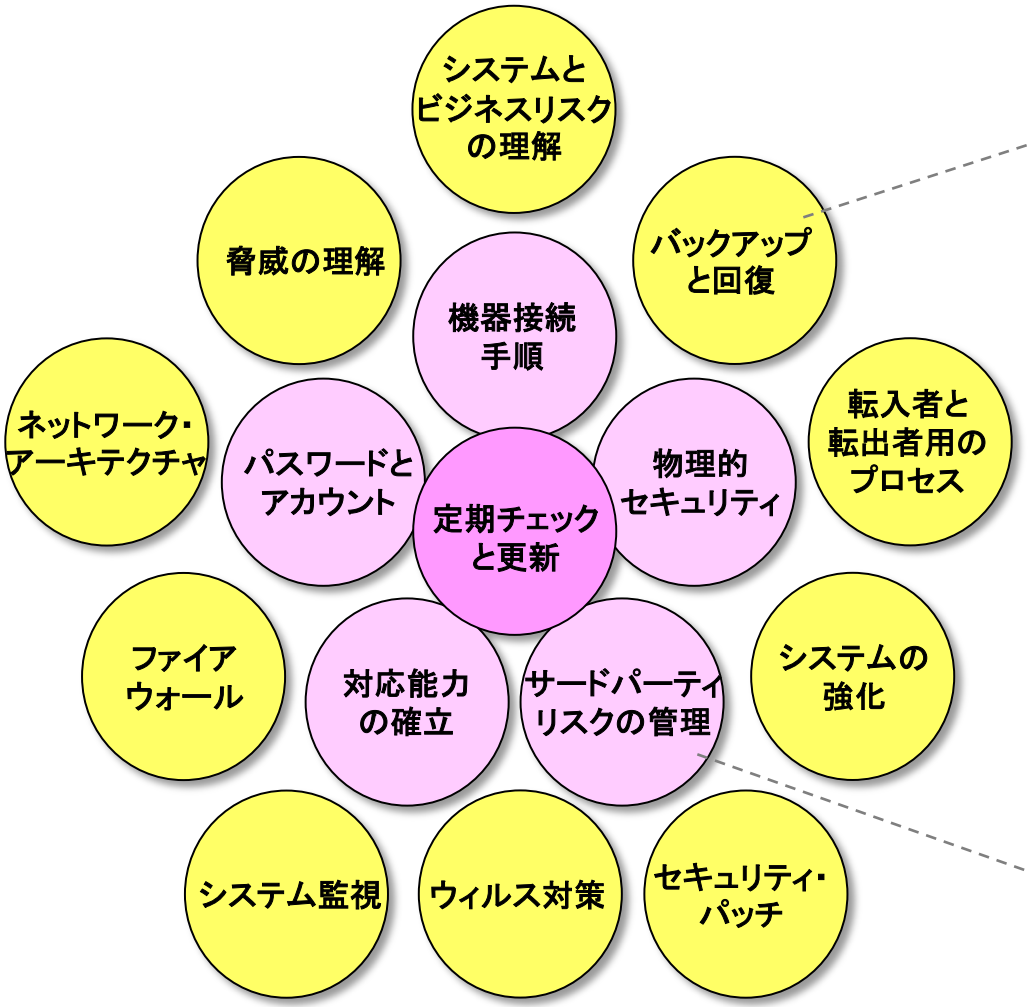
J-CLICS　Step1（現場担当者向け）
優先度の高い 6分野 11項目



J-CLICS チェックリスト（Step1）

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？

J-CLICSの設問項目（Step2）



J-CLICS Step2
（システム技術者・管理者向け）
10項目

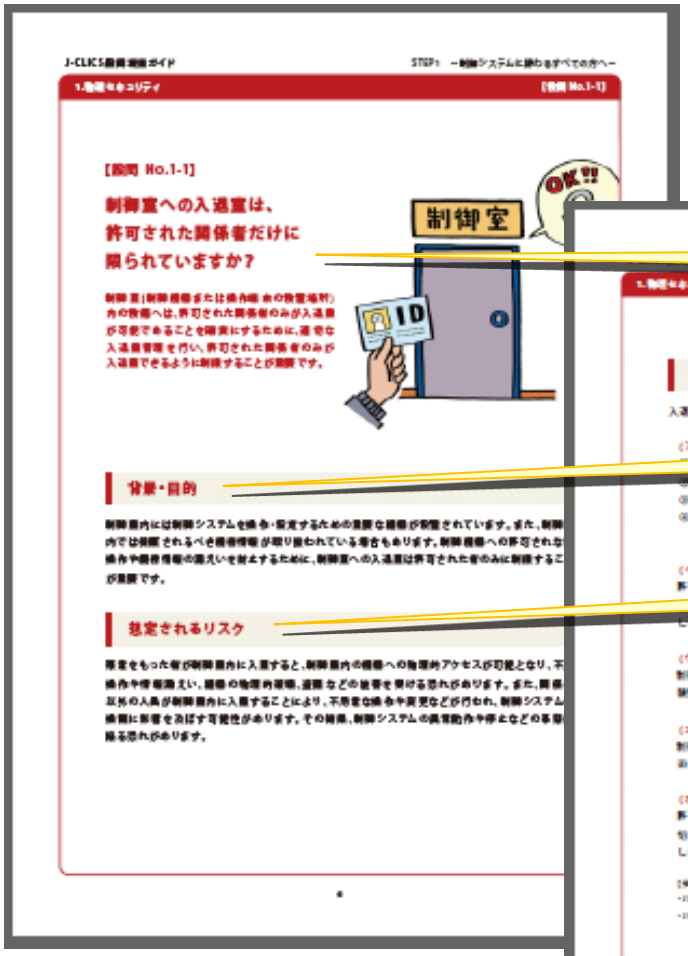
セキュリティ施策の強化に必要な，J-CLICS Step1よりもやや技術的・専門的な項目をサポート

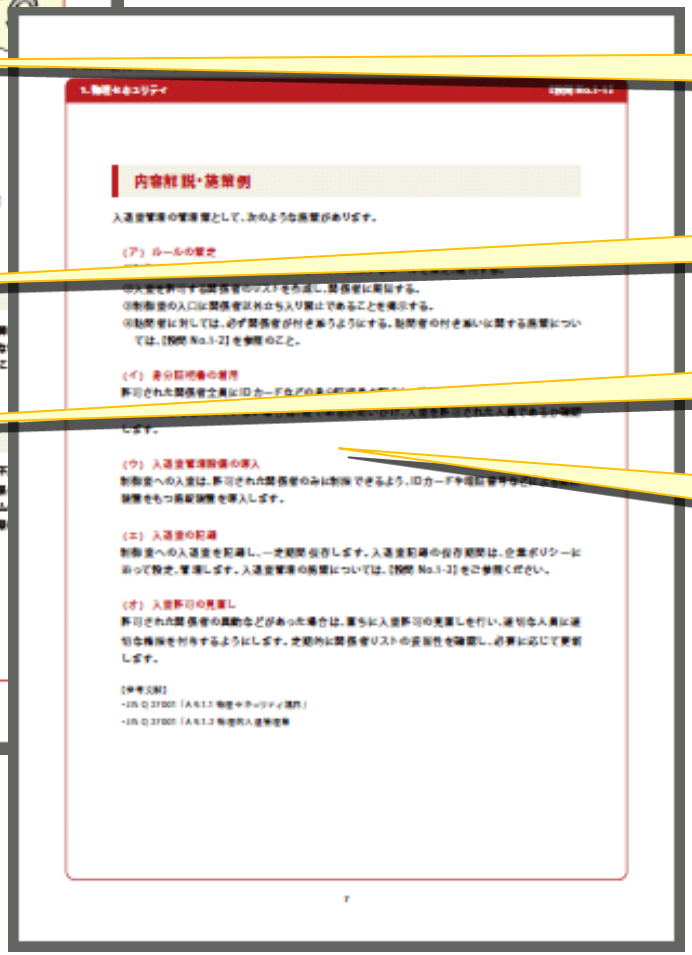
Step1の設問分野

J-CLICS チェックリスト（Step2）

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】

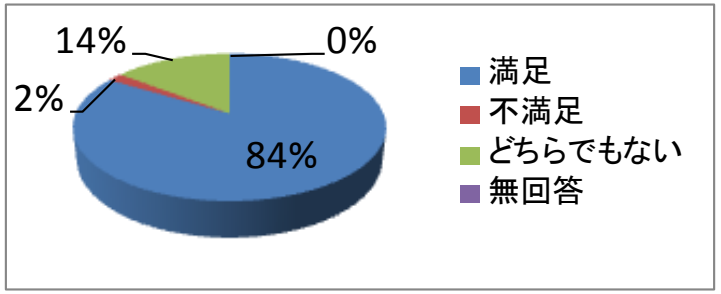
【補足】

J-CLICS に対する評価

- **ユーザ企業に試用頂き，アンケートを実施（N=165）**

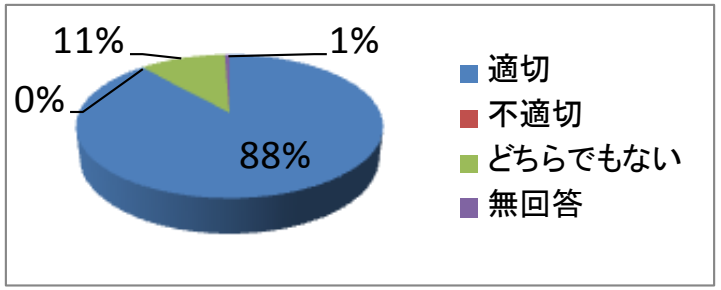
①全体的な内容はいかがでしたか。

満足	不満足	どちらでもない	無回答
138	3	24	0



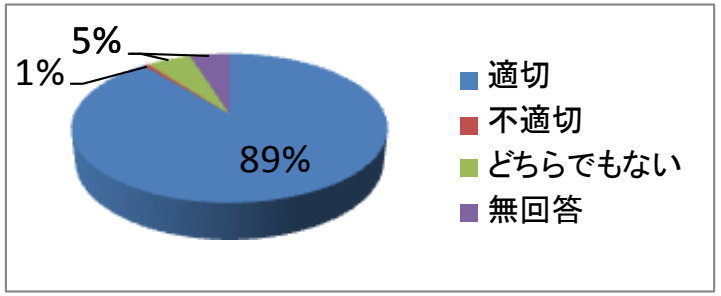
②全体的な設問の用語，表現はいかがでしたか。

適切	不適切	どちらでもない	無回答
146	0	18	1



③分量はいかがでしたか。

適切	不適切	どちらでもない	無回答
147	1	9	8



✓ **8割以上の方にご満足頂いています**

目次

1. セキュリティ合同WGのご紹介
2. 背景と目的
3. J-CLICSの開発
4. J-CLICSの構成
5. J-CLICS Step1 のご紹介
6. J-CLICS Step2 のご紹介
7. まとめと今後の予定

セキュリティチェックリスト J-CLICS Step-1

J-CLICS　Step1：6分野 11項目（現場担当者向け）

チェックリスト

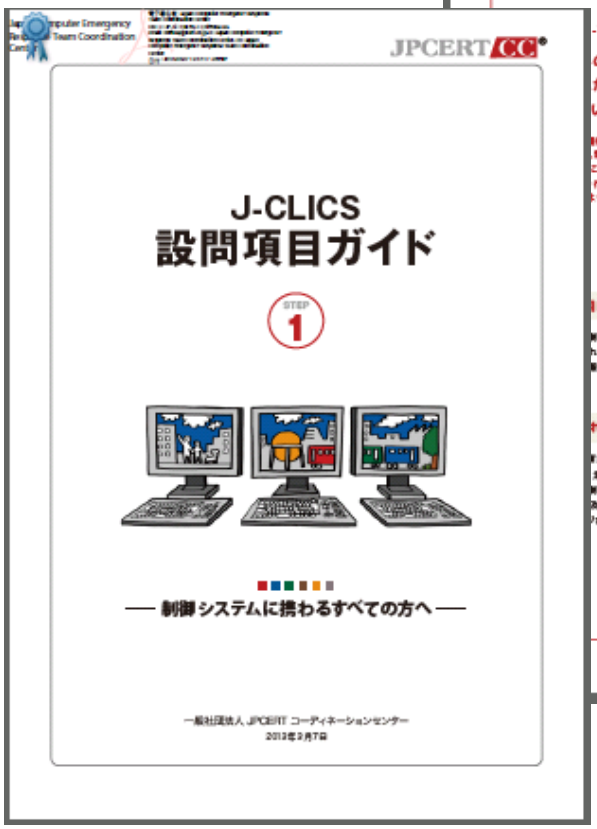
STEP1 J-CLICS Check List 制御システムセキュリティチェックリスト for Industrial Control Systems of Japan

NO		設問	○/×	解説ガイド対応ページ
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]への設置には、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		機器等調達手順		
	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.14 P.15
	2	制御システムの機器が情報系システムの機器と共に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（ラグやシールなどで）分かるようにしていますか？		
3		パスワードとアカウント		
	1	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？		P.23
	2	強力なパスワード[*3]を使用していますか？		P.25
	3	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？		P.27
4		対応能力の確立		
	1	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明確し、訓練をしていますか？		P.32
5		サードパーティリスクの管理		
	1	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？		P.38
6		継続的な評価と改善		
	1	定期的にチェックリストまたは、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？		P.40

[*1] 制御室とは、制御装置または操作端末の設置場所を指します。
[*2] USBメモリ、携帯型PC、外付けハードディスク、外付けCD/DVDドライブなど。
[*3] 英字、数字、記号の複数以上を使用し、8文字以上で、アカウント名などが含まれておらず、推測されにくいパスワード。
（対象機器に設定できるパスワードの最大桁が8文字未満の場合は、最大桁のパスワード）

SICE JEITA JEMIMA JPCERT CC

設問項目ガイド



Japan Computer Emergency Response Team Coordination Center　JPCERT CC

J-CLICS
設問項目ガイド

STEP 1

── 制御システムに携わるすべての方へ ──

一般社団法人 JPCERT コーディネーションセンター
2013年3月下旬

J-CLICS設問項目ガイド　STEP1　制御システムに携わるすべての方へ

1.物理的セキュリティ　[設問 No.1-1]

-1]
の入退室は、
た関係者だけに
いますか？

制御室

ID

的

れるリスク

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。

物理的セキュリティ

＜設問 1-2＞

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？

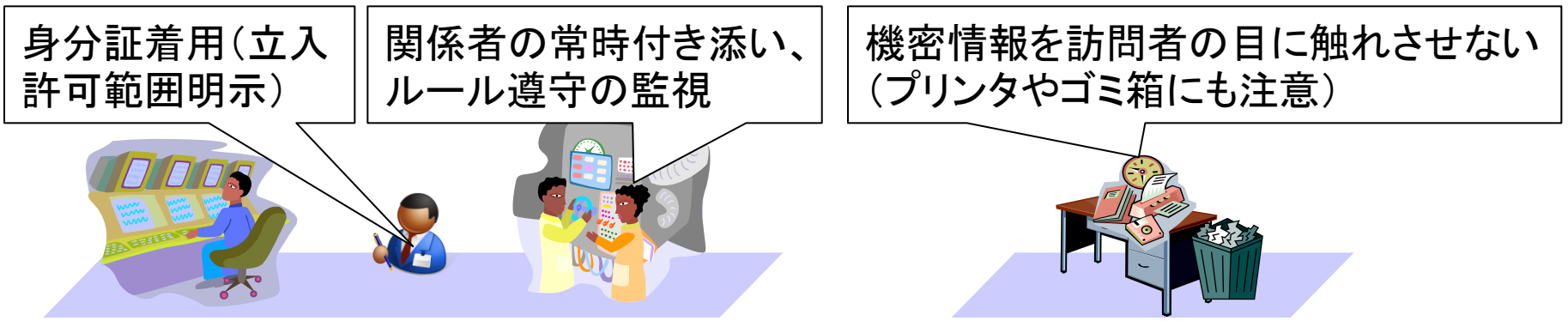
＜背景・目的・想定リスク＞

■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。

■業務上、訪問者の入室が必要な場合、関係者が常に付き添い、不用意な操作や情報の持ち出しなどを防ぐ必要があります。

＜施策例＞

①訪問者の制御室入室ルールを策定する。②機密情報へのアクセスを制限する。



物理的セキュリティ

＜設問 1-3＞

制御室への入退室管理（記録と監査）を行っていますか？

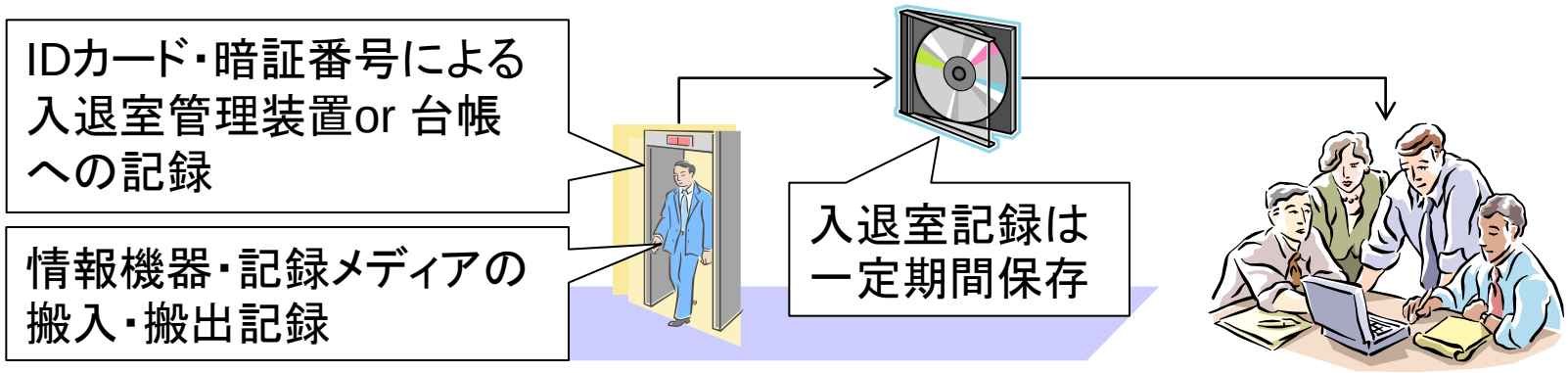
＜背景・目的・想定リスク＞

■許可された人員のみが制御室に入室していることを確実にするために、いつ、誰が、何の目的で入退室したかを記録し、定期的に確認する必要があります。

■適切な入退室記録がないと、セキュリティ事故や事件が発生した際に原因や影響範囲を特定し、適切な対応や対策が困難になる恐れがあります。

＜施策例＞

①入退室記録のルールを策定する。　　②入退室記録を定期的に監査する。



機器接続手順

＜設問 2-1＞

制御システムのネットワークに接続する機器(USBメモリを含む)について、事前にそれらがウイルスやワームに感染していないことを確認する手順を文書化して実施していますか？

＜背景・目的・想定リスク＞

■USBメモリなどのメモリデバイスやノートPC等はウイルス感染や情報漏洩の経路になる恐れがあります

■これら情報機器の持ち込み・持ち出し・設置・撤去にはルールを定め適切に管理する必要があります

＜施策例＞

〇機器接続ルールの作成

・ウイルス感染防止のための検査手順をルール化する。

・機器接続ルールの例

　・OSやソフトウェアが最新とする。必要に応じてパッチの適用する

　・事前にウイルスチェックを実施する

　・不要なサービスや通信機能が無効に設定されていることを確認する

〇備え付けUSBメモリやPCの設置

・内部でのみ使用する備え付けのUSBメモリやPCを用意して必要なデータのみを移し替えるようにすることでウイルス感染リスクの低減をはかる

機器接続手順

＜設問 2-2＞

制御システムの機器がITシステムの機器と同じラックに設置されているのであれば、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？

＜背景・目的・想定リスク＞

■多くの機器が設置されている環境では、機器やケーブルの取り違いが発生する恐れもあります

■制御システムの構成機器やネットワークケーブルなどには、ラベルなどで表示を行ない、ITシステムと誤認されないようにする必要があります

＜施策例＞

○ラベル表示

・制御システムの機器やケーブルであることをラベル表示する

○空きポート・端子の封印

・空ポートや空き端子への誤接続を防止するために、シール等で封印する

○別のラックに分載して施錠管理

・管理区分(ITシステム，制御システムなど)ごとに別の場所や別のラックに搭載し、別の鍵で施錠管理する。機器への物理アクセスを制限することで取り違い事故を防止する。

パスワードとアカウント

＜設問 3-1＞

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・ポリシーを遵守していますか？

＜背景・目的・想定リスク＞

■制御システムのパスワードが流出すると不正アクセスによる操業データの流出やシステムの不正操作・異常停止を引き起こされる可能性があります

■それらを未然に防止するためにもパスワードの管理ルール（ポリシー）を決めて正しく運用する必要があります

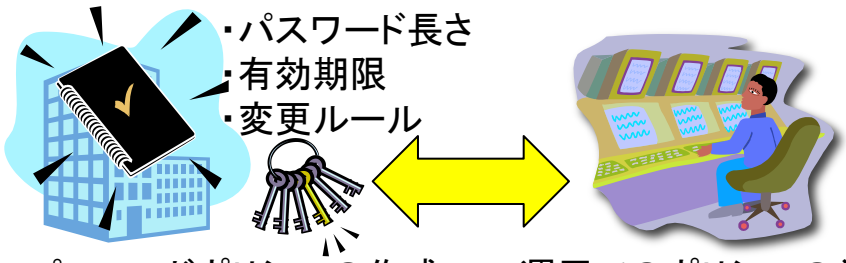
＜施策例＞

○パスワードポリシーの作成

- パスワードポリシーを作成し文書化する
- パスワードポリシーの例
  - 強力なパスワードを使用する → 設問3-2
  - パスワードを定期的に変更する → 設問3-3
  - 古いパスワードは再度使用しない
  - 他人に教えたり共有しない

○パスワードポリシーの遵守

- パスワードポリシーの内容を理解し遵守する



パスワード漏洩による事故（情報漏洩、不正操作）の防止

パスワードとアカウント

＜設問 3-2＞
強力なパスワードを使用していますか？

＜設問 3-3＞
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？

＜背景・目的・想定リスク＞

■パスワードは文字の組み合わせであるため、試せばいずれは見つけることができる

■英字や数字、大文字や小文字、記号などを使い、想定しづらいパスワードにすることにより、パスワードの漏洩を予防する

＜施策例＞

○想定しづらいパスワード

- 名前、生年月日、電話番号などを使わない
- 自分のアカウント名などが含まれない
- 辞書などに登録されている一般的な単語にしない
- 英数字記号を含む8文字以上
  （制御システムにより使える長さは異なる）

○パスフレーズを使用する

- 長い文字列を使用できるシステムの場合、単語ではなく文章をパスワードにする
- 文章の中に意図的に記号を入れて解析しづらくする

対応能力の確立

＜設問 4-1＞

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または異常時の対応方法を理解し、訓練していますか？

＜背景・目的・想定リスク＞

■被害を最小限に抑えるため、定常的に不正アクセスや攻撃の監視を行う

■監視手順や異常時の対応方法を理解し、緊急時に備え事前に訓練を行う

＜施策例＞

○主な監視事項

- FW，サーバ，IDS/IPSのアクセス記録，イベントログ
- ログイン，ログアウト時間
- パスワードの変更ログ
- 制御システムにおける各種操作ログ
- 重要な制御装置区域への入退室記録
- 配線やネットワーク機器の不正な接続
- ネットワーク負荷状況の変化
- 不正なプロセスが動作していないこと

○警報発生や緊急時の訓練例

- 実環境と同等の訓練用環境にて確認
- 実際に行う操作手順を端末や装置前で確認

サードパーティリスクの管理

＜設問 5-1＞

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作成して実施していますか？

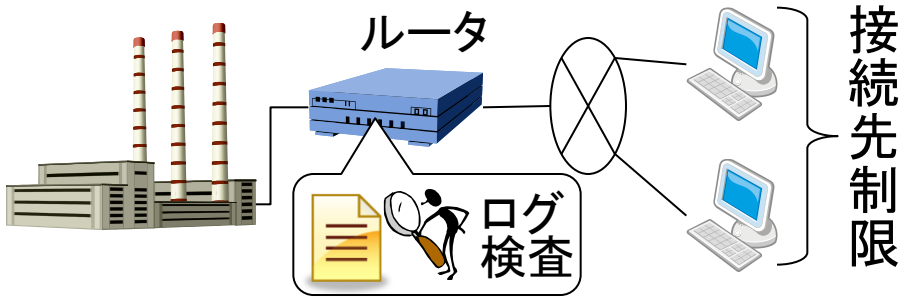
＜背景・目的・想定リスク＞

- 制御システムの外部接続は危険です。リモート接続はしないほうが安全です。
- ウイルス感染、情報漏洩、外部からの誤操作などのリスクが発生します。

＜施策例＞

① リモート接続に関するルールを周知徹底します。

② リモート接続の接続先や作業内容を最小限度に制限します。



③ 定期的にルータのログを検査し異常がないことを確認します

※リモートの接続先は「管理不能」と想定し、あらゆるリスクを検討すべきです。

継続的な評価と改善

＜設問 6-1＞

定期的に本J-CLICSを用いて制御システムセキュリティの自己評価を行い、関連する文書や施策の見直しを行っていますか？

＜背景・目的・想定リスク＞

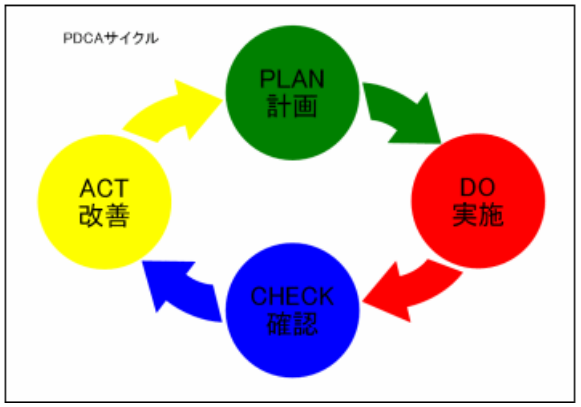
セキュリティの有効性は、業務・組織の変化、技術革新、新たな攻撃手法の登場などにより変化します。有効性を**維持**するためには**PDCA**[*1]サイクルを回すことが重要です。

実情に合わないルールや文書を放置することで、制御システムへ危険性を高めることになったり、無駄なコストの要因になったりします。

[*1] **P**lan:計画-**D**o:実行-**C**heck:点検-**A**ct:処置

＜施策例＞

- ルールの作成
- セキュリティの自己評価を実施
- セキュリティ施策の評価と見直し



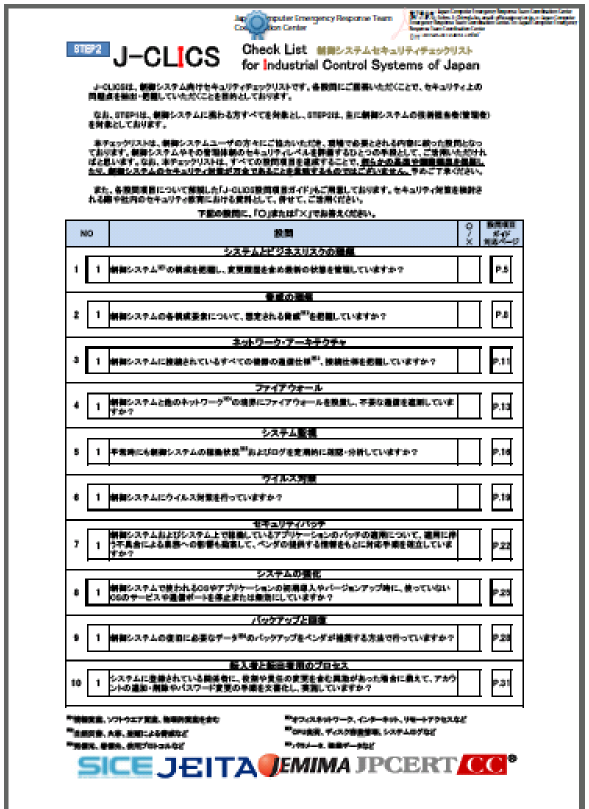
目次

1. セキュリティ合同WGのご紹介
2. 背景と目的
3. J-CLICSの開発
4. J-CLICSの構成
5. J-CLICS Step1 のご紹介
6. J-CLICS Step2 のご紹介
7. まとめと今後の予定

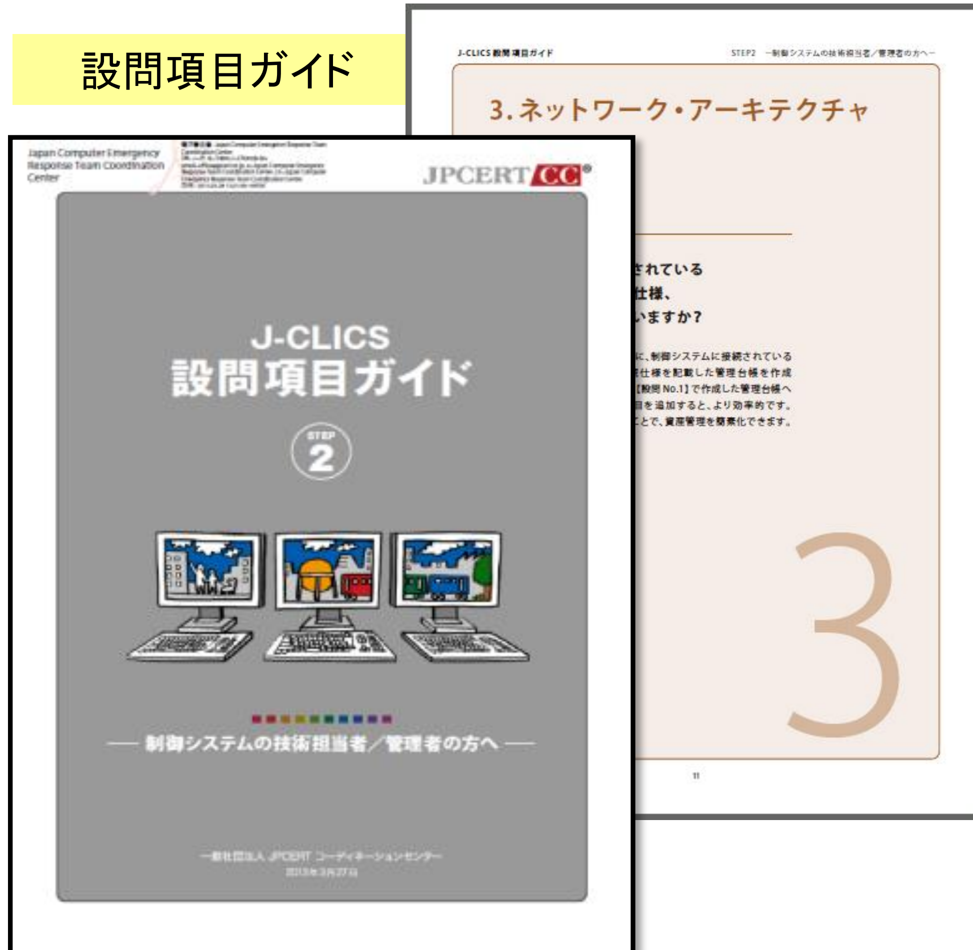
セキュリティチェックリスト J-CLICS Step-2

J-CLICS　Step2：10項目（システム技術者・管理者向け）

チェックリスト



設問項目ガイド



システムとビジネスリスクの理解

＜設問 1-1＞

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？

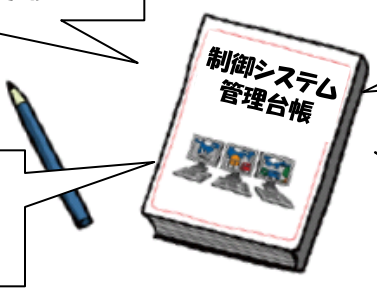
＜背景・目的・想定リスク＞

■ビジネスリスク（災害、設備暴走、秘密情報漏えい等）
　⇒　管理不足によるビジネスへの大きな影響
■リスク要因を正確に分析・評価し、発生回避／発生時に迅速に対応

＜施策例＞

管理台帳の作成、管理

機器、ソフトウェア
管理責任者、形態、
接続状況、変更履歴



復旧に必要な情報

他システムとの依存性

アカウント所有者リスト

システム構成の最新状態を把握
・変更履歴を残す
・定期的に見直す

脅威の理解

＜設問 2-1＞

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？

＜背景・目的・想定リスク＞

■システムへの脅威と脆弱性を把握し、考えられるリスクを評価し、リスク発生への対応を検討することが必要です。

■リスク対策を行わない場合、ビジネスそのものに対して大きな影響を及ぼす恐れがあります。

＜施策例＞

①どのような脅威があるか把握する。

・故意による脅威（内部関係者の情報漏えいなど）
・偶発的な脅威（入力ミス、操作ミスなど）
・環境の脅威（地震、火事など）

②脅威に対してリスク評価と対応を検討し、実施する。

・教育の実施
・二重入力、確認フローの追加
・免震床の設置、バックアップメディアの分散管理

ネットワーク・アーキテクチャ

＜設問 3-1＞

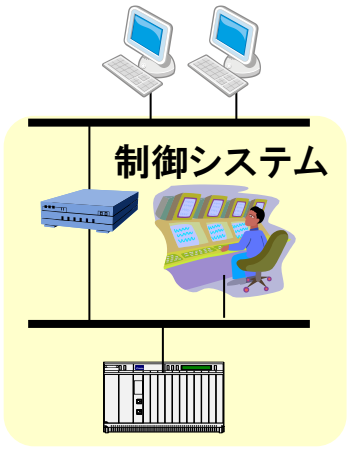
制御システムに接続されているすべての機器の通信仕様、接続仕様を把握していますか？

＜背景・目的・想定リスク＞

■ネットワークセキュリティを確保するために機器の通信仕様、接続仕様を把握することが重要です。

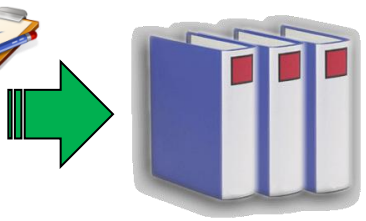
■機器の通信仕様、接続仕様を把握していないと、システムの異常の検出が十分に行えない恐れがあります。

＜施策例＞



①通信仕様、接続仕様の管理台帳を作成します。

＜通信仕様＞
・通信名称
・通信目的
・使用プロトコル
・使用ポート
など



管理台帳

②接続状況の監査やセキュリティ対策の検討に使用します。

ファイアウォール

＜設問 4-1＞

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？

＜背景・目的・想定リスク＞

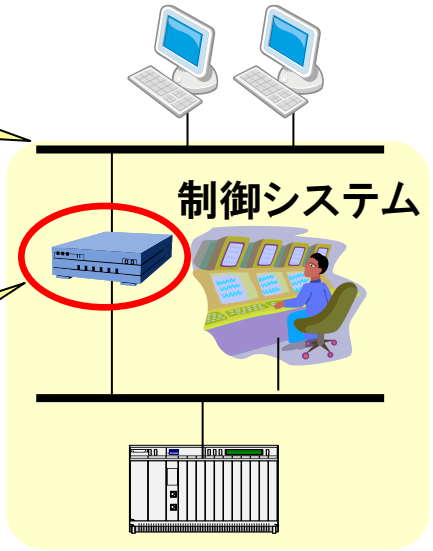
■制御システムのネットワークはインターネットなどの外部ネットワークに接続しないほうが安全です。

■制御システムのネットワークを他のネットワークに接続する場合には、ネットワークの境界にファイアウォールを設置して必要な通信のみ通過させるようにします。

＜施策例＞

•他のネットワークとの接続の必要性を精査する。

•ファイアーウォールを設置し必要な通信のみ通過させる。



ファイアウォールの設置については、
・鍵付ラックなどに格納するなどして不正アクセスから保護する。
・制御ベンダーに構成や設定を問い合わせる。

システム監視

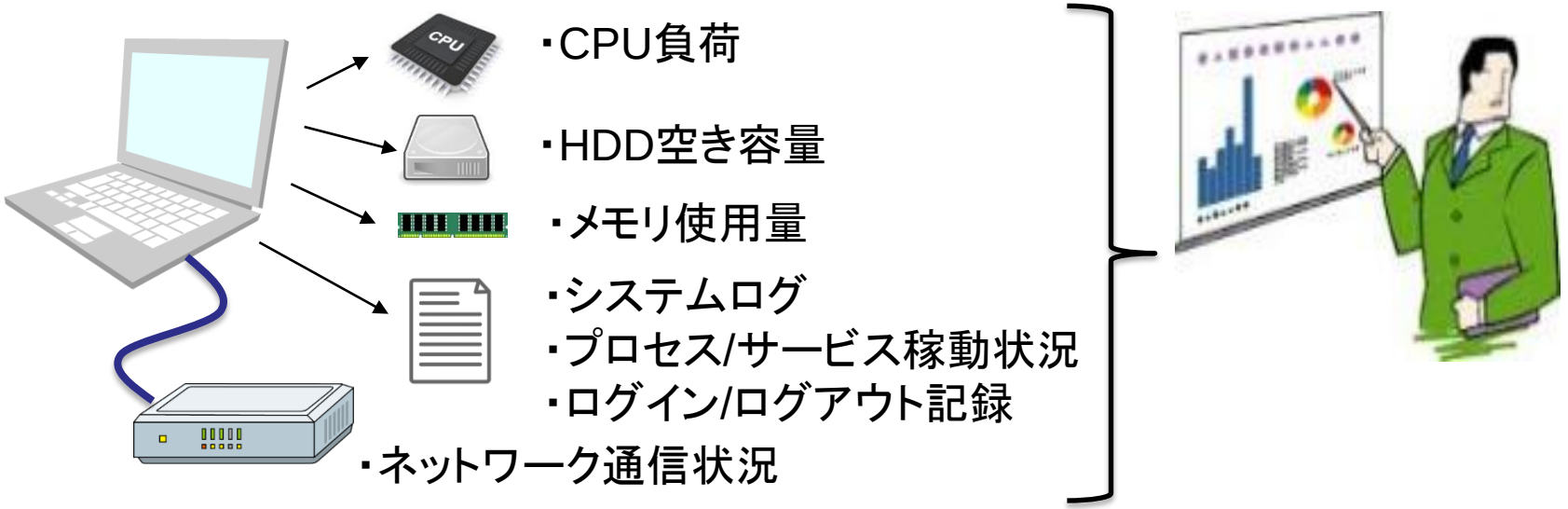
＜設問 5-1＞

平常時にも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？

＜背景・目的・想定リスク＞

■ 機器の異常に気づくには稼動状況履歴やログが有効です。
■ 定期的に確認していないと正常なのか異常なのかの判断が困難です。

＜施策例＞ 以下の項目の使用率や空き容量を確認、分析します。



ウイルス対策

＜設問 6-1＞

制御システムにウイルス対策を行っていますか？

＜背景・目的・想定リスク＞

ウイルスの侵入や感染などによる異常動作や停止で事業が大きな影響を受ける恐れがあります。

＜施策例＞

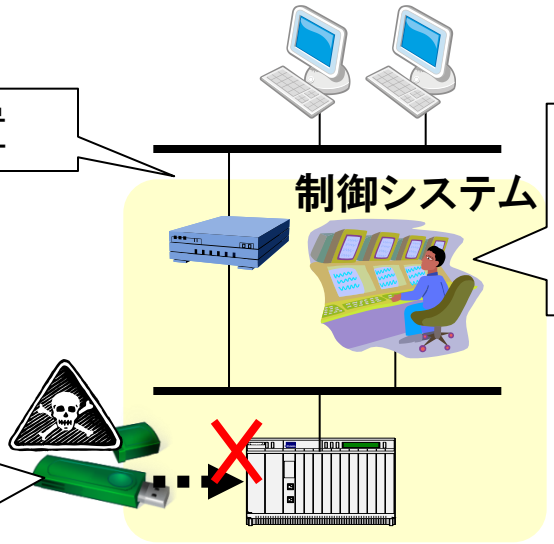
以下のようなウイルスの侵入経路に対策を施します。

①ネットワーク

- ファイアウォールの設置

②外部媒体・外部PC

- 持ち込み制限・管理
- 不要ファイルの削除
- ウイルスチェック徹底



③制御システム内PC

- 機器の施錠
- 未使用USB，LANポートの封鎖
- ウイルス対策ソフト

セキュリティパッチ

＜設問 7-1＞

制御システム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、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？

＜背景・目的・想定リスク＞

あらかじめ手順を確立しておかないと、システムが攻撃に屈しやすい状況になったり、セキュリティパッチ自体の不具合によってシステムが異常な状態になる恐れがあります

＜施策例＞

①セキュリティパッチの情報や手順などを確認する。

・パッチ情報の入手方法や適用手順の確認
・パッチ適用の必要性や影響の確認

②セキュリティパッチ適用時のリスク対策を検討する。

・ウイルスチェック
・パッチ適用前のバックアップ

システムの強化

＜設問 8-1＞

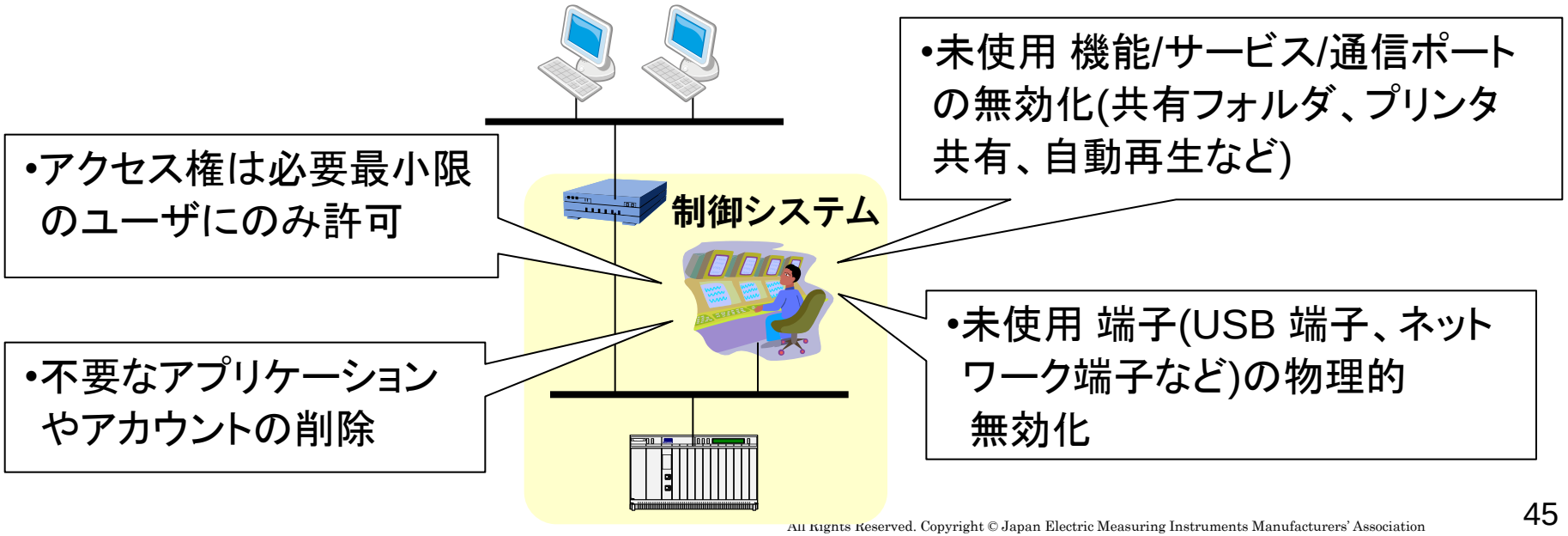
制御システムで使われるOSやアプリケーションの初期導入やバージョンアップ時に使っていないOSのサービスや通信ポートを停止または無効にしていますか？

＜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。



バックアップと回復

＜設問 9-1＞

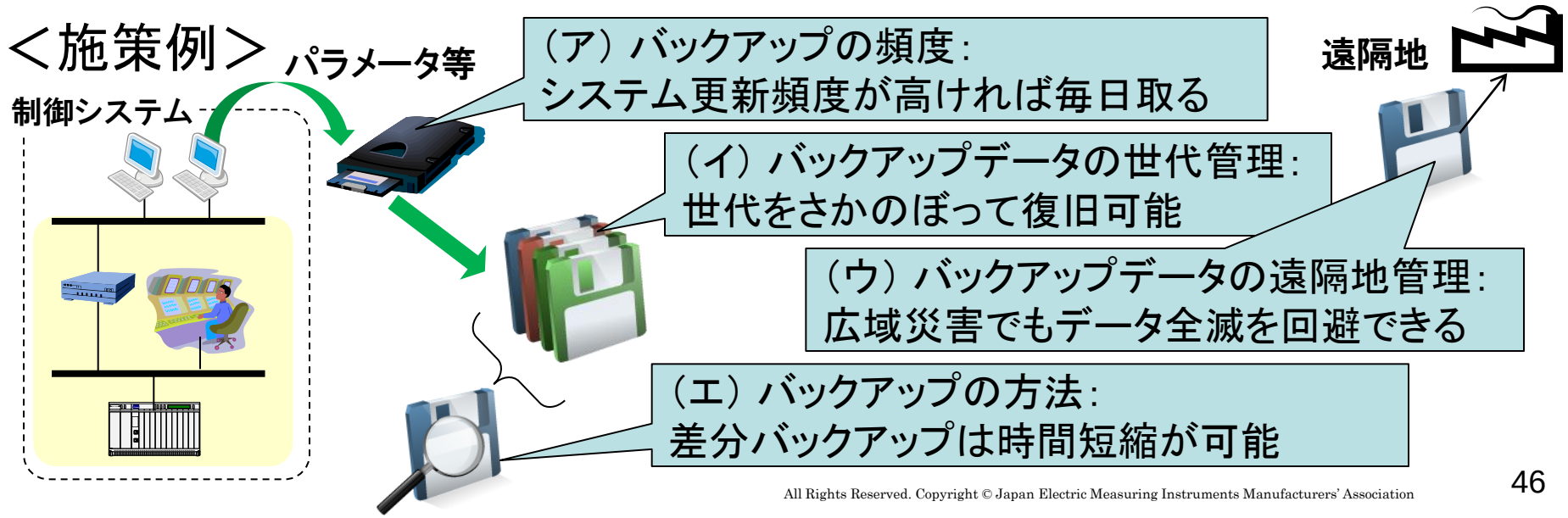
制御システムの復旧に必要なデータのバックアップをベンダが推奨する方法で行っていますか？

＜背景・目的・想定リスク＞

■システム復旧に必要なデータは、定期的なバックアップとデータ保存の確認が必要です。

■システム復旧のためには、機能不全前の直近のデータが必要です。

＜施策例＞



転入者と転出者用のプロセス

＜設問 10-1＞

システムに登録されている関係者の異動に備えて、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？

＜背景・目的・想定リスク＞

不要なアカウントや不適切な操作権限が付与された状態を放置した場合、
システムへの不正アクセスや操作が可能となり、システム停止や情報漏えい等の事態に陥る恐れがあります。

＜施策例＞

セキュリティ実施手順書等で文書化し、
定期的に適切な操作権限が付与されていることを確認する。

システムの不正操作を未然に防ぐために
・定期的なパスワード変更
・異動退職者の権限の速やかな変更
・システムログの確認
→不正アクセス・操作の早期発見に

システムの操作権限は
・必要最小限の人員に
・必要最小限の権限を

目次

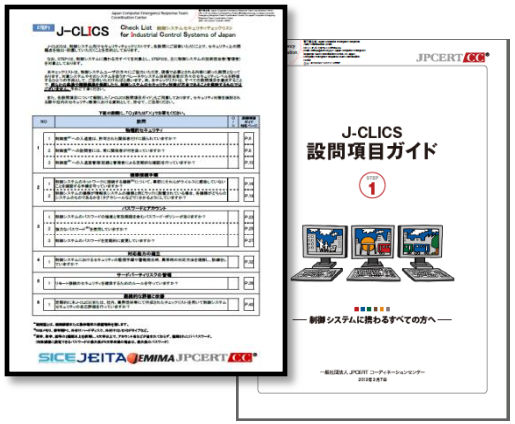
1. セキュリティ合同WGのご紹介
2. 背景と目的
3. J-CLICSの開発
4. J-CLICSの構成
5. J-CLICS Step1 のご紹介
6. J-CLICS Step2 のご紹介
7. まとめと今後の予定

まとめと今後の予定

- **J-CLICS Step 1／Step 2 を作成**
  - 制御システムのセキュリティ底上げを目的として，ユーザの意見を反映しつつ開発
  - 対策立案や教育・啓発にも使える項目ガイド付き
- **J-CLICSの無償配布**
  - 制御システム関係者を対象にJPCERT/CCから無償配布中
  - https://www.jpcert.or.jp/ics/jclics.html
- **2014年度も改良活動を継続**

  SICE/JEITA/JEMIMAセキュリティ合同WGにて利用者からのフィードバックをもとに改善継続予定

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 Step 1

J-CLICS Step 2

ご静聴ありがとうございました