一般社団法人 日本電気計測器工業会
Japan Electric Measuring Instruments Manufacturers' Association

計測展2012 OSAKA　テクニカルセミナー

制御システムセキュリティ向上に向けた取り組み
ーセキュリティ自己評価ツールに関する取組みー

2012.11.1

SICE/JEITA/JEMIMA
セキュリティ合同WG

SICE/JEITA/JEMIMAセキュリティ合同WGのご紹介

SICE/JEITA/JEMIMAセキュリティ合同WG

- **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**を進め、会員企業、ユーザにフィードバックする。

- **設立**

  2005年4月

- **メンバー （50音順）**

  アズビル㈱、㈱東芝、富士電機 ㈱
  ㈱日立ハイテクコントロールシステムズ、㈱日立製作所
  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**

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
- **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

制御システムセキュリティ
関連団体合同委員会

JEMIMA

J-CLICS作成の経緯

制御システムセキュリティへの取り組み

- **動機： 制御システムセキュリティを向上させたい！**
  - 制御システムにおいてもセキュリティが重要になってきている
  - 既存の制御システムを保護するための施策が早急に必要
  - わかりやすく、実施しやすく、効果的なセキュリティ施策の指針がほしい
- **方法： 既存のガイドライン・評価ツールを改良して利用**
  - 対象は現場のオペレータおよびシステム技術担当者
  - 目的は制御システムセキュリティの底上げ
  - 既存のガイドライン・評価ツールを調査
  - 目的に合うものを選定して内容を調整

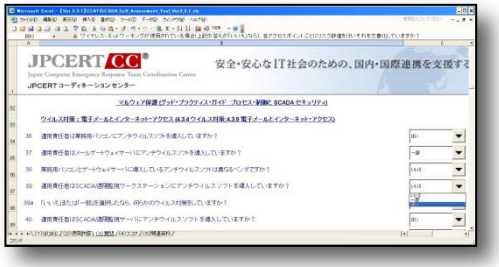
- **活動経緯**
  - **2010年度： セキュリティ自己評価ツール SSAT日本語版の調査・改良**
  - **2011年度： SSAT日本語版のさらなる改良**
  - **2012年度： SSAT日本語版をもとにJ-CLICSを作成**

2010年度の活動

セキュリティ評価ツールSSATの評価と改良

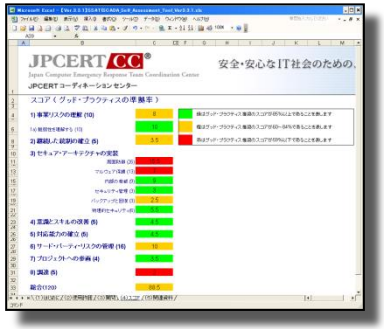
2010年度：SSATの調査・改良

- **セキュリティ自己評価ツールSSATの調査と改良を実施**
  - 既存のガイドライン・評価ツールからSSATを選定
  - SSATが生産現場で利用できるか評価
  - 問題点を抽出して改良



日本語版SSAT チェックシート

- **SSAT（SCADA Self Assessment Tool）とは**
  - **英国CPNI**が作成したSCADAシステム向けの**セキュリティ自己評価ツール**
  - **約100問の短い設問**に回答することで**セキュリティの問題点を診断**
  - **回答は択一式**（「はい」「いいえ」「ときどき」）で回答しやすい
  - **MS-Excel 形式**になっており**診断結果が即座に得られる**



SSAT診断結果例

- **SSATを選定した理由**
  - 日本語版がJPCERT/CCから入手できる
  - 他のツールや文献と比較して手頃な分量 （約100問の短い質問で構成）
  - 技術的施策から管理施策までを含むバランスの良い内容

2010年度：SSATの調査･改良

1. モデルシステムに対してSSATを試用

– 典型的な制御システムのモデルに対して WGメンバーがそれぞれSSATに回答

– 試用での「はい」回答は約20%

• 理解が難しく、回答しづらい問題が存在

→ 改良の必要があるが内容的には有用と判断

2. 試用結果をもとにWGで改良を検討

– 用語や表現を制御システム関係者向けに改良

8割のSSAT設問項目を改良

– 再評価の結果「はい」回答が55%に向上

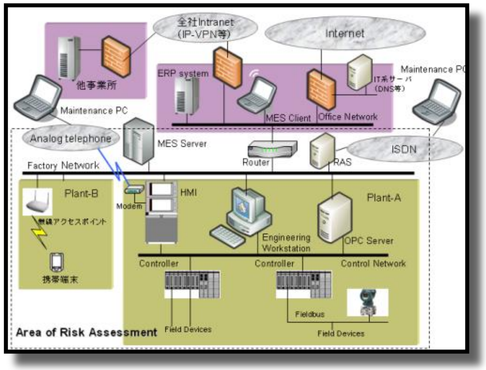
• 理解しやすくなり、回答しやすくなった

3. 検討結果をもとに改良版SSATを作成

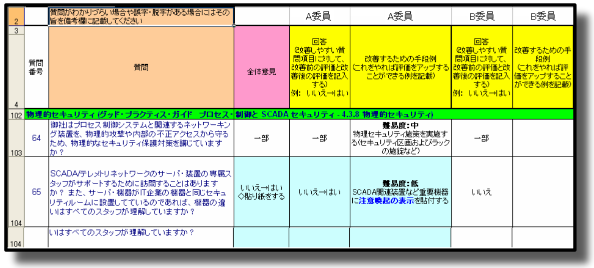
– JPCERT/CC と共同でSSATの内容を改良

→ **2011年2月に「共同監修版SSAT」を JPCERT/CC からリリース**

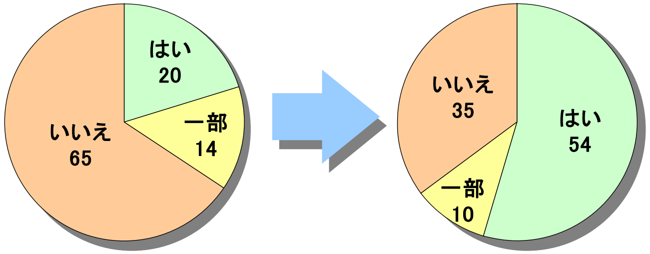
共同監修版SSAT
制御システム関係の方はJPCERT/CCから入手可能
http://www.jpcert.or.jp/ics/ssat.html



検討に用いた制御システムのモデル



試行結果の例



改良によってわかりやすくなり
「はい」回答が増加

JEMIMA

2011年度の活動

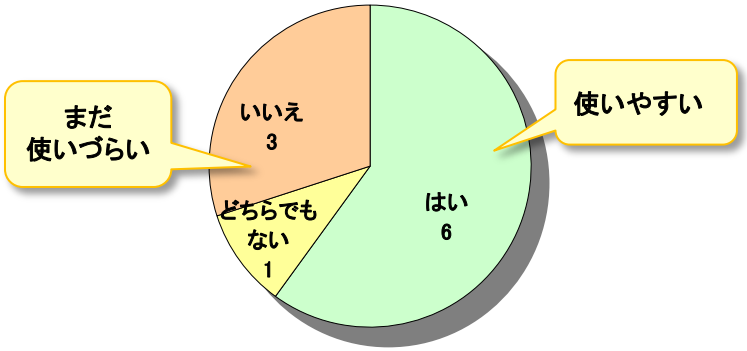
セキュリティ評価ツールSSATの
さらなる改良

2011年度：SSATのさらなる改良

1. SSAT利用者アンケートを分析

- 使いやすいという意見をいただいた
- 使いづらいという意見もいただいた
  - 設問数が多すぎる
  - まだ難解な設問が含まれている
  - 達成できない要件が含まれている

→ さらなる改良活動を行うことにした



SSAT利用者アンケート
「セキュリティ上の問題点が
手軽に抽出できましたか？」

2. ユーザの皆様に協力いただき再検討

- 制御システムユーザの皆様に協力いただき検討会を開催
  - 日本ガス協会さまにご協力いただき、制御システムユーザ企業・団体に協力を依頼
  - 主要な企業・団体のセキュリティ担当者さまに参加いただき合同検討会を開催
    - 参加団体（50音順）：**電気事業連合会　日本ガス協会　三菱化学　三井化学　森ビル**
    - 2011年11月より毎月１回のペースで検討会を開催　（現在も継続中）
  - 経産省　制御システムセキュリティ検討TFのメンバにも参加いただき連携
    - 普及啓発のツールとしての視点から意見をいただいた
- ユーザの皆様から意見をいただきながらSSAT改良を検討

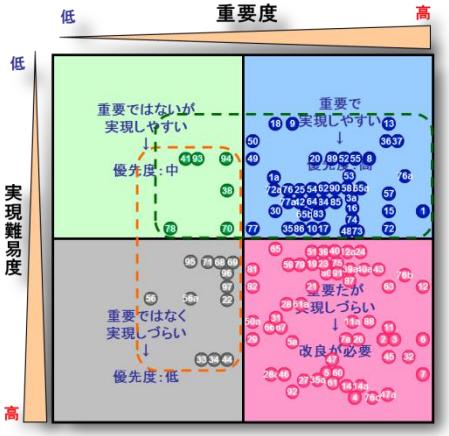
→ **SSATベースの新しいチェックツールと解説文書がまとまった**

ベンダとユーザが協力して検討

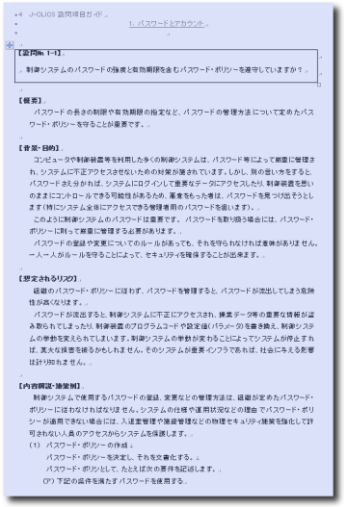
2011年度：SSATのさらなる改良

- **設問数の絞り込み**
  - 「設問数が多すぎる」という声に対応するために設問数を絞り込んだ
  - 現場視点での絞り込み　：　現場の運転・保守担当者に関する項目を抽出した
  - 重要度視点での絞り込み：　重要かつ実施難易度が低い項目を優先させた
  - 重複項目の整理・統合　：　内容が類似している項目を統合した
  - → **SSAT120項目から現場向けで重要度の高い13項目を抽出した**
- **表現・用語の改良**
  - 「わかりづらい項目がある」という声に対応するために表現・用語を見直した
  - 現場視点での表現・用語の見直し：　現場の担当者に理解いただける表現・用語に変更した
- **要件内容の改良**
  - 「実現が困難な項目がある」という声に対応するために要件の内容を改良した
  - 現場の実情に合った要件への変更：　要件の趣旨を解釈し日本の実情に合う内容に調整した
- **解説資料の作成**
  - 「どんな施策を実施すればよいのかわからない」という声に対応するため解説資料を作成した
  - 解説資料は次のような内容で作成した
    - 各項目ごとに独立した資料として作成し通読を前提としないものとした
    - 各項目ごとに　背景・目的・リスク・施策例・参考文献 を記述した
    - 普及啓発や教育にも使用することを前提に内容の検討を行った

→ **現場向けで重要度の高い11項目からなるチェックリストと**
それぞれの項目を解説する資料のセットがまとまった



重要度分析結果


解説資料ページ例

2012年度の活動

セキュリティ評価ツールJ-CLICSの作成と評価

2012年度：J-CLICSの作成

- **これまでの検討結果を集約してセキュリティ自己評価ツールを作成**
  - J-CLICS (Check List for Industrial Control System) と命名
  - 現場向けの新しい自己評価ツールとして広く利用していただけることを目標
  - 制御システムセキュリティの底上げが主目的
  - 想定利用者は制御システムの現場で運用・保守を担当される方
  - 想定利用目的はセキュリティ評価・セキュリティ教育・啓蒙活動

J-CLICS チェックリスト

1. より広いユーザの方に見ていただき意見をいただいた

- アンケートを実施して、内容に関する意見をいただいた
  - 75%の方から「全体的に満足」との評価をいただいた
  - 用語・表現 については90%の方から「適切」との評価をいただいた
  - 分量については40%の方から「少ない」との意見をいただいた

2. アンケート結果を分析してリリースに向けた改良を実施

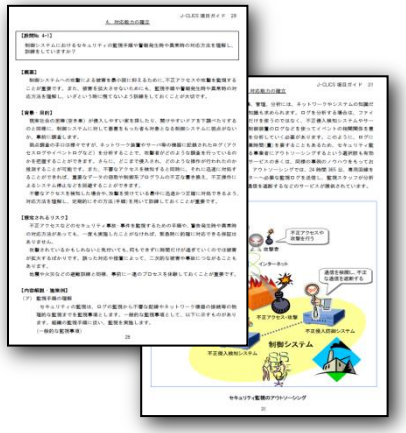
- トライアル版に対する意見をもとにリリースに向けた改良・調整を行う

3. リリースに向けた準備・調整を実施

- 利用許諾条件の検討と文書作成
- 配布形態の検討

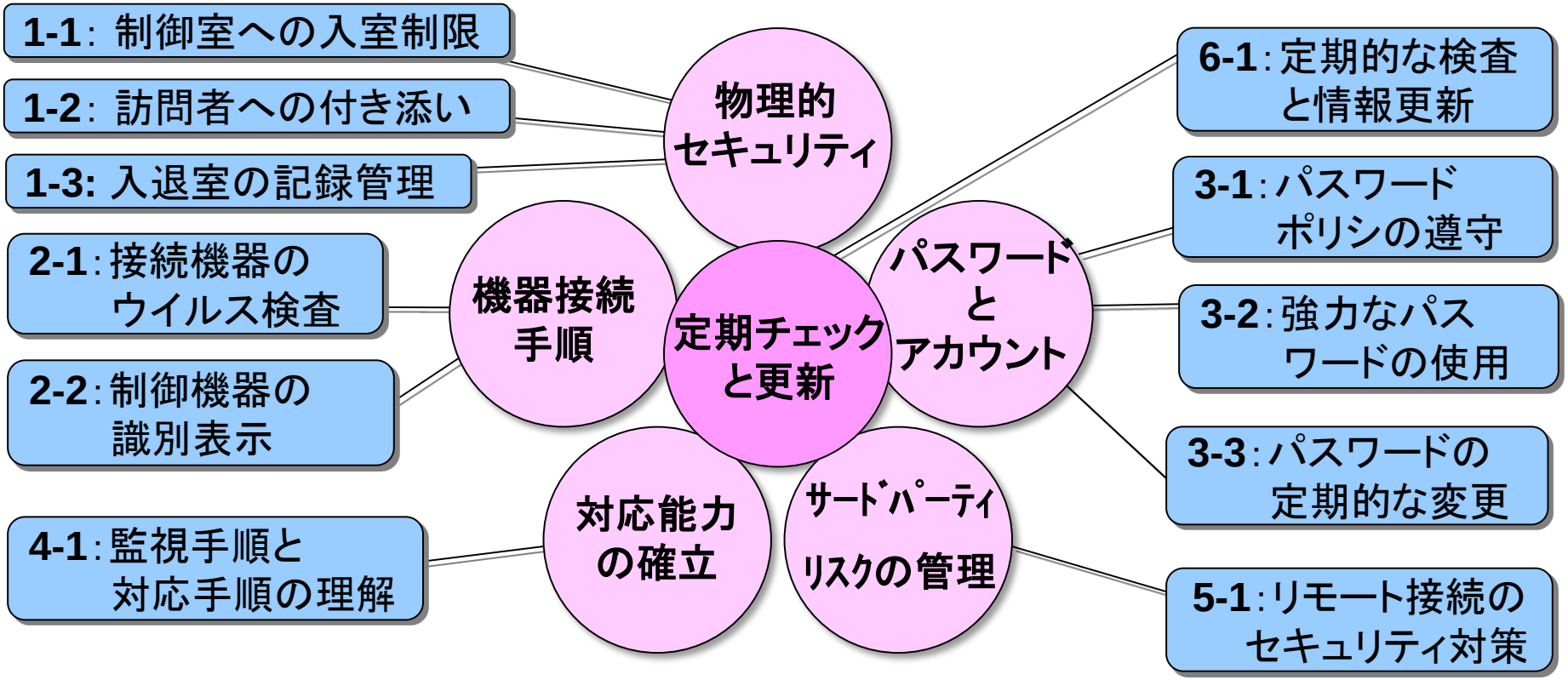
4. より広範囲な内容を含むJ-CLICSの拡張を検討

- システム技術担当者やシステム構築担当者向けの拡張項目(Step2)を検討中
- 対策分野の網羅性を考慮して項目を選定中


J-CLICS 検知項目ガイド

J-CLICSに含まれる項目

J-CLICS　Step1項目
優先度の高い 6分野 11項目



J-CLICS 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

J-CLICSは、制御システム向けセキュリティチェックリストです。
制御システムユーザを対象とし、各設問にご回答いただくことで、セキュリティ上の問題点を抽出・把握していただくことを目的としております。

本チェックリストは、制御システムユーザの方々にご協力いただき、現場で必要とされる内容に絞った設問となっております。対象システムやそのシステムを扱うオペレータやシステム技術担当者の方々のセキュリティレベルを評価するひとつの手段として、ご活用いただければと思います。尚、本チェックリストは、すべての設問項目を達成することで、何らかの基準や運用規準を保証したり、制御システムのセキュリティ対策が万全であることを意味するものではございません。予めご了承ください。

また、各設問項目について解説した「J-CLICS設問項目ガイド」もご用意しております。セキュリティ対策を検討される際や社内のセキュリティ教育における資料として、併せて、ご活用ください。

下記の設問に、「○」または「×」でお答えください。

NO	設問	○/×	ガイドブック対応ページ
	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.**
	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.**
	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.**
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持っていますか？		P.**
	2 制御システムの機器が…システムのものである…		
3	1 制御システムのパスワ…		
	2 強力なパスワード※3を…		
	3 制御システムのパスワ…		
4	1 制御システムにおける…ていますか？		
5	1 リモート接続のセキュリ…		
6	1 定期的に本J-CLICSを…セキュリティの自己評…		

※1制御室とは、制御装置または操作端末…
※2USBメモリ、保守用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2種類以上を使用し、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長が8文字未満の場合は、最大長のパスワード。）

SICE JEITA JEMIMA JPCERT CC®

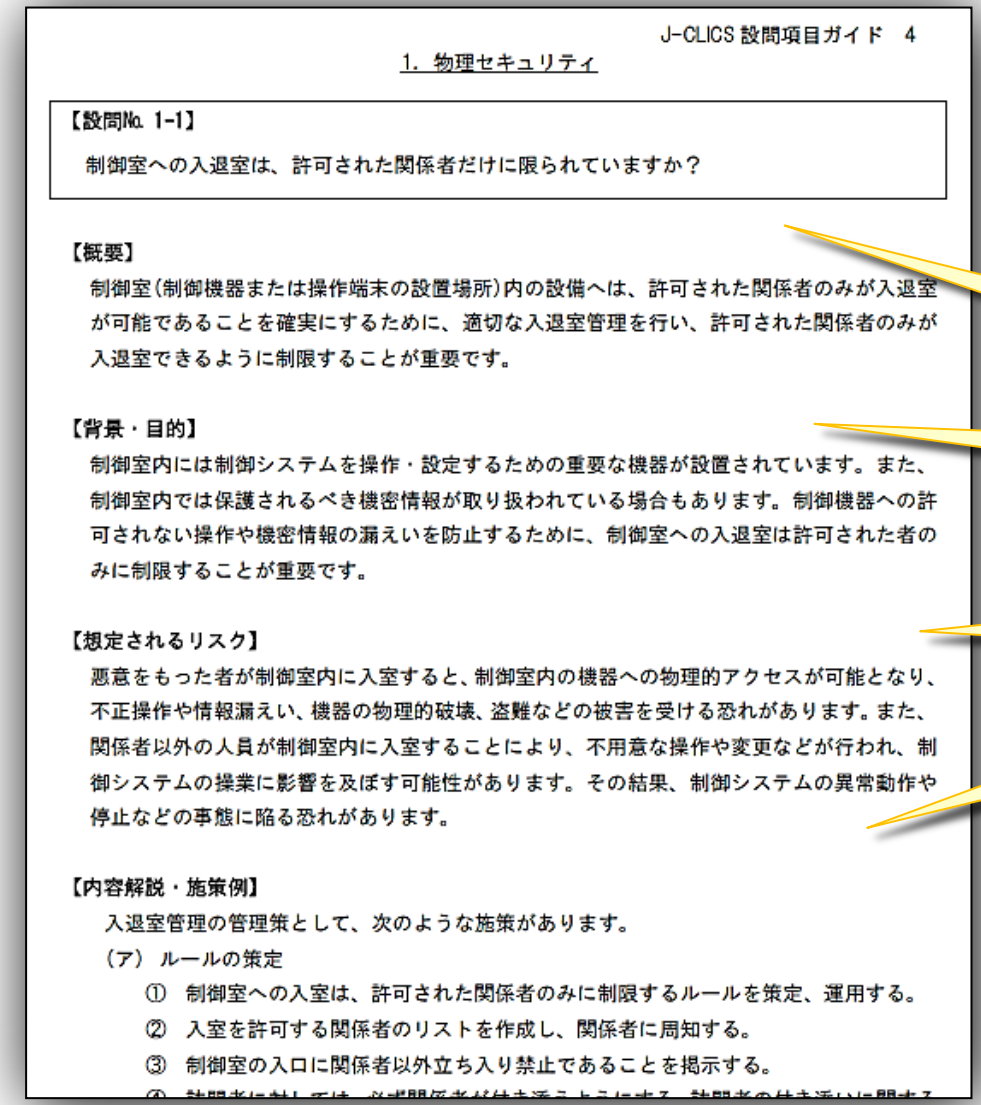
NO	設問	○/×	ガイドブック対応ページ
	物理的セキュリティ		
1	1 制御室※1への入退室は、許可された関係者だけに限られていますか？		P.**
	2 制御室※1への訪問者には、常に関係者が付き添っていますか？		P.**
	3 制御室※1への入退室管理(記録と管理者による定期的な確認)を行っていますか？		P.**

セキュリティ重要施策チェックリスト

平易な設問文
回答は○×式
厳選された重要項目 (6分野 11項目)

セキュリティ状況を素早くチェック可能

J-CLICS 設問項目ガイド



J-CLICS 設問項目ガイド　4

1. 物理セキュリティ

【設問No. 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？

【概要】

制御室(制御機器または操作端末の設置場所)内の設備へは、許可された関係者のみが入退室が可能であることを確実にするために、適切な入退室管理を行い、許可された関係者のみが入退室できるように制限することが重要です。

【背景・目的】

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が設置されています。また、制御室内では保護されるべき機密情報が取り扱われている場合もあります。制御機器への許可されない操作や機密情報の漏えいを防止するために、制御室への入退室は許可された者のみに制限することが重要です。

【想定されるリスク】

悪意をもった者が制御室内に入室すると、制御室内の機器への物理的アクセスが可能となり、不正操作や情報漏えい、機器の物理的破壊、盗難などの被害を受ける恐れがあります。また、関係者以外の人員が制御室内に入室することにより、不用意な操作や変更などが行われ、制御システムの操業に影響を及ぼす可能性があります。その結果、制御システムの異常動作や停止などの事態に陥る恐れがあります。

【内容解説・施策例】

入退室管理の管理策として、次のような施策があります。

(ア) ルールの策定

① 制御室への入室は、許可された関係者のみに制限するルールを策定、運用する。

② 入室を許可する関係者のリストを作成し、関係者に周知する。

③ 制御室の入口に関係者以外立ち入り禁止であることを掲示する。

J-CLICS設問項目の解説文書

「何のために何をするべきか」
をわかりやすく解説

- 【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】

ここまでのまとめ

まとめ：J-CLICS を作成しました

- **これまでの検討結果を集約してセキュリティ自己評価ツールを作成**
  - 制御システムのセキュリティ底上げが目的
  - 制御システムベンダとユーザが協力して検討・開発
  - 制御システムの現場で今すぐにできる重要施策11項目を選定
  - 制御関係者にわかりやすい用語・表現を使用

- **J-CLICSチェックリスト**
  - すぐに実行できる重要セキュリティ施策 6分野11項目
  - 短くわかりやすい設問
  - 回答は〇×形式

J-CLICS チェックリスト

- **J-CLICS検知項目ガイド**
  - 各設問項目に対する説明文書
  - 各設問ごとに独立しており必要な部分だけ読める構成
  - 「何のために何をするべきか」を解説
  - 読み物や教育資料としても利用できる内容


J-CLICS 検知項目ガイド

このあと内容を詳しく紹介いたします

J-CLICSのご紹介

セキュリティチェックリスト J-CLICS

J-CLICS　Step1項目：6分野 11項目

J-CLICS　チェックリスト

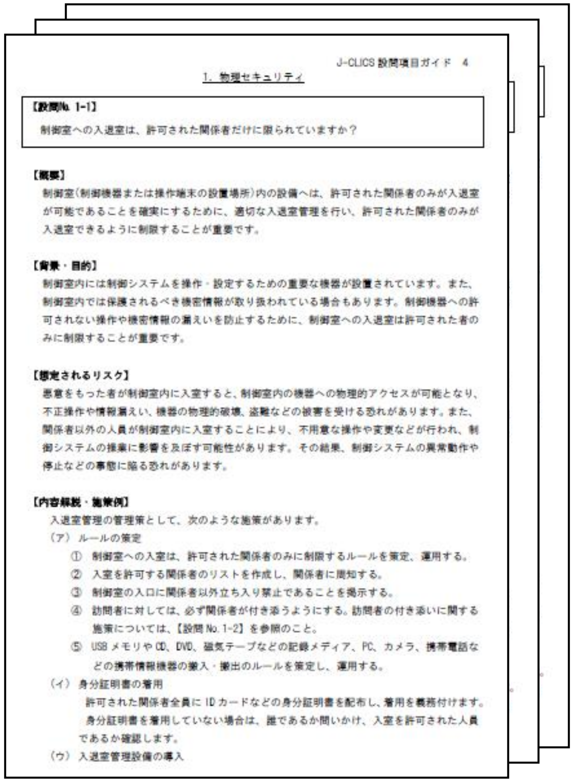
STEP1

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

下記の設問に、「○」または「×」でお答えください。

NO		設問	○／×	ガイドブック対応ページ
		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.##
	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.##
	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.##
		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.##
	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.##
		パスワードとアカウント		
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・ポリシーがありますか？		P.##
	2	強力なパスワード[※3]を使用していますか？		P.##
	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.##
		対応能力の確立		
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や異常時の対応方法を理解し、訓練をしていますか？		P.##
		サードパーティリスクの管理		
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守っていますか？		P.##
		継続的な評価と改善		
6	1	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？		P.##

J-CLICS　設問項目ガイド



J-CLICS 設問項目ガイド　4

1．物理セキュリティ

【設問No. 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？

【概要】
制御室(制御機器または操作端末の設置場所)内の設備へは、許可された関係者のみが入退室が可能であることを確実にするために、適切な入退室管理を行い、許可された関係者のみが入退室できるように制限することが重要です。

【背景・目的】
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が設置されています。また、制御室内では保護されるべき機密情報が取り扱われている場合もあります。制御機器への許可されない操作や機密情報の漏えいを防止するために、制御室への入退室は許可された者のみに制限することが重要です。

【想定されるリスク】
悪意をもった者が制御室内に入室すると、制御室内の機器への物理的アクセスが可能となり、不正操作や情報漏えい、機器の物理的破壊、盗難などの被害を受ける恐れがあります。また、関係者以外の人員が制御室内に入室することにより、不用意な操作や変更などが行われ、制御システムの操業に影響を及ぼす可能性があります。その結果、制御システムの異常動作や停止などの事態に陥る恐れがあります。

【内容解説・施策例】
入退室管理の管理策として、次のような施策があります。
（ア）ルールの策定
① 制御室への入室は、許可された関係者のみに制限するルールを策定、運用する。
② 入室を許可する関係者のリストを作成し、関係者に周知する。
③ 制御室の入口に関係者以外立ち入り禁止であることを掲示する。
④ 訪問者に対しては、必ず関係者が付き添うようにする。訪問者の付き添いに関する施策については、【設問 No. 1-2】を参照のこと。
⑤ USB メモリや CD、DVD、磁気テープなどの記録メディア、PC、カメラ、携帯電話などの携帯情報機器の搬入・搬出のルールを策定し、運用する。
（イ）身分証明書の着用
許可された関係者全員に ID カードなどの身分証明書を配布し、着用を義務付けます。身分証明書を着用していない場合は、誰であるか問いかけ、入室を許可された人員であるか確認します。
（ウ）入退室管理設備の導入

セキュリティチェックリスト J-CLICS
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。

セキュリティチェックリスト J-CLICS
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。

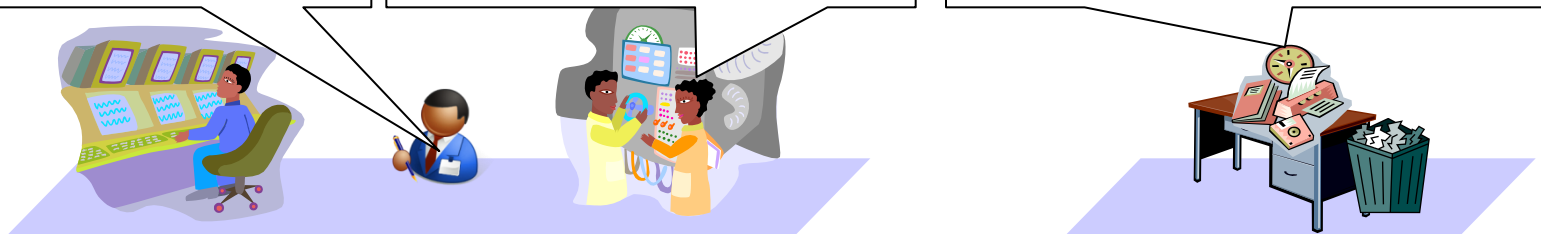
＜施策例＞

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。

身分証着用（立入許可範囲明示）

関係者の常時付き添い、ルール遵守の監視

機密情報を訪問者の目に触れさせない（プリンタやゴミ箱にも注意）



セキュリティチェックリスト J-CLICS
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？

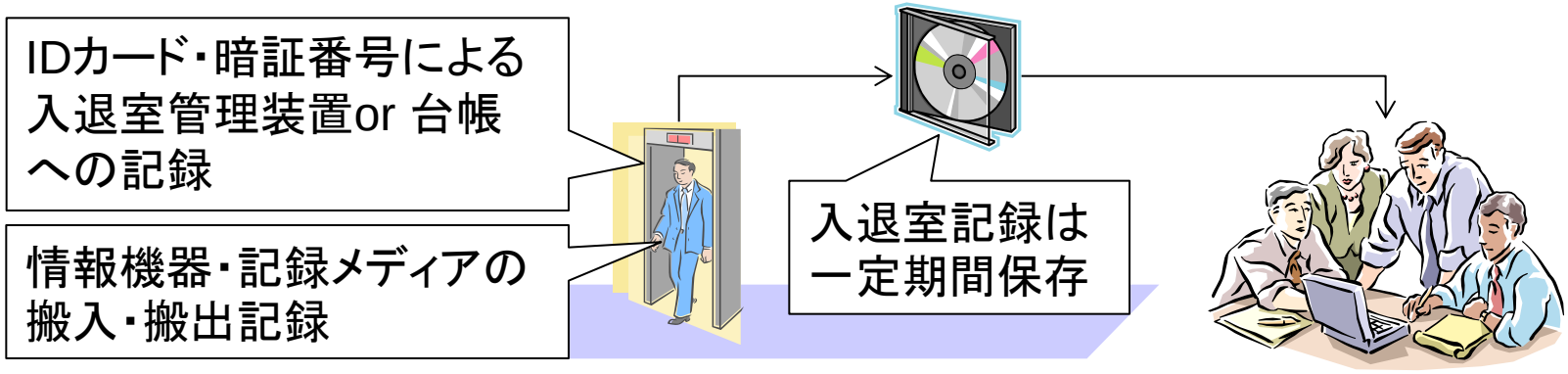
＜背景・目的・想定リスク＞

■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。



セキュリティチェックリスト J-CLICS
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＞

■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

セキュリティチェックリスト J-CLICS
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＞

■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＞

〇ラベル表示

・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

〇空きポート・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

〇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。

セキュリティチェックリスト J-CLICS
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＞

■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1-2

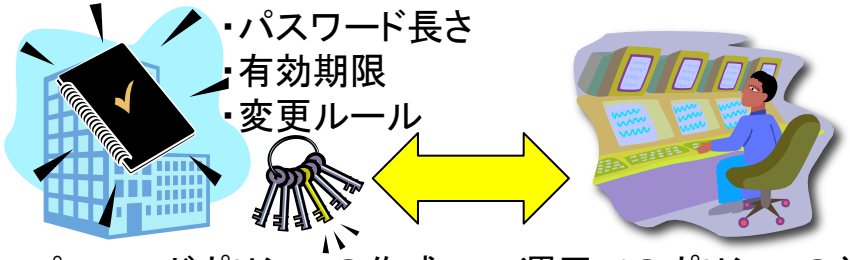
　・パスワードを定期的に変更する → 設問1-3

　・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

セキュリティチェックリスト J-CLICS
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＞

■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、想定しず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＞

○想定しずらいパスワード

- 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ずらくする

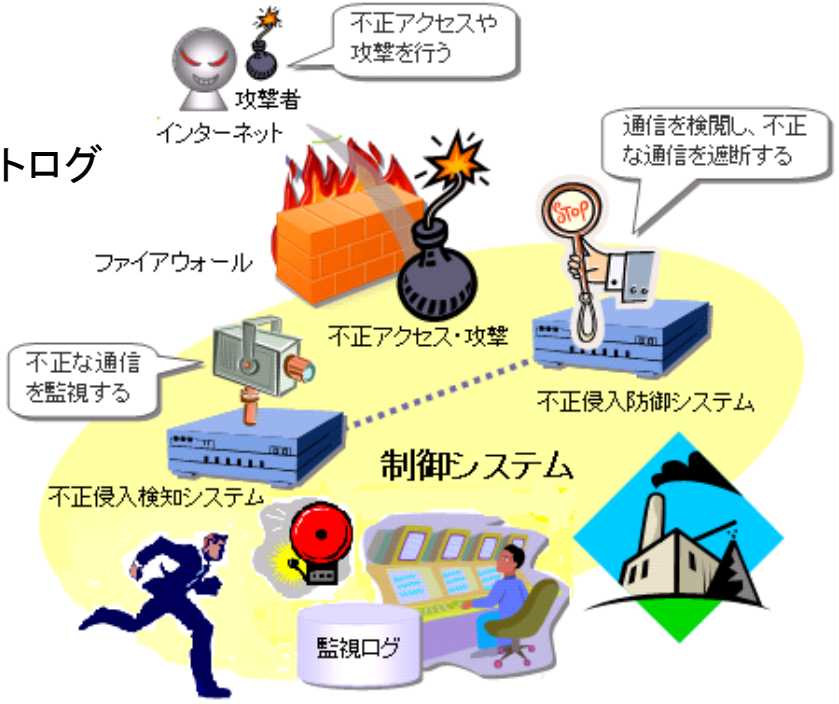
セキュリティチェックリスト J-CLICS
対応能力の確立

＜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＞
■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



セキュリティチェックリスト J-CLICS
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？

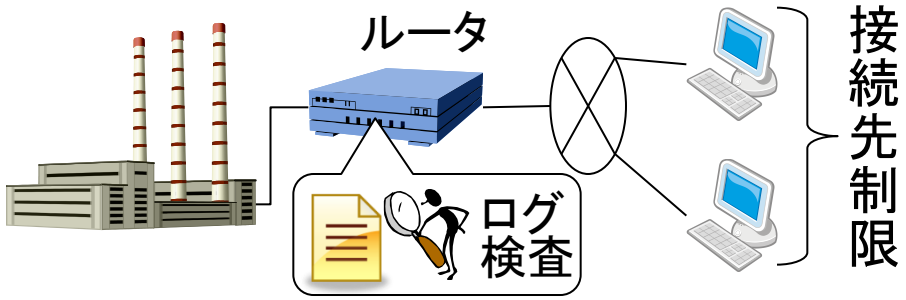
＜背景・目的・想定リスク＞

- 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。

セキュリティチェックリスト J-CLICS
継続的な評価と改善

＜設問 6-1＞

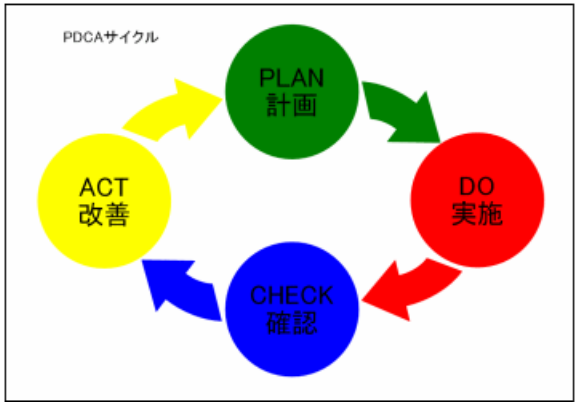
定期的に本J-CLICSを用いて制御システムセキュリティの自己評価を行い、関連する文書や施策の見直しを行っていますか？

＜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

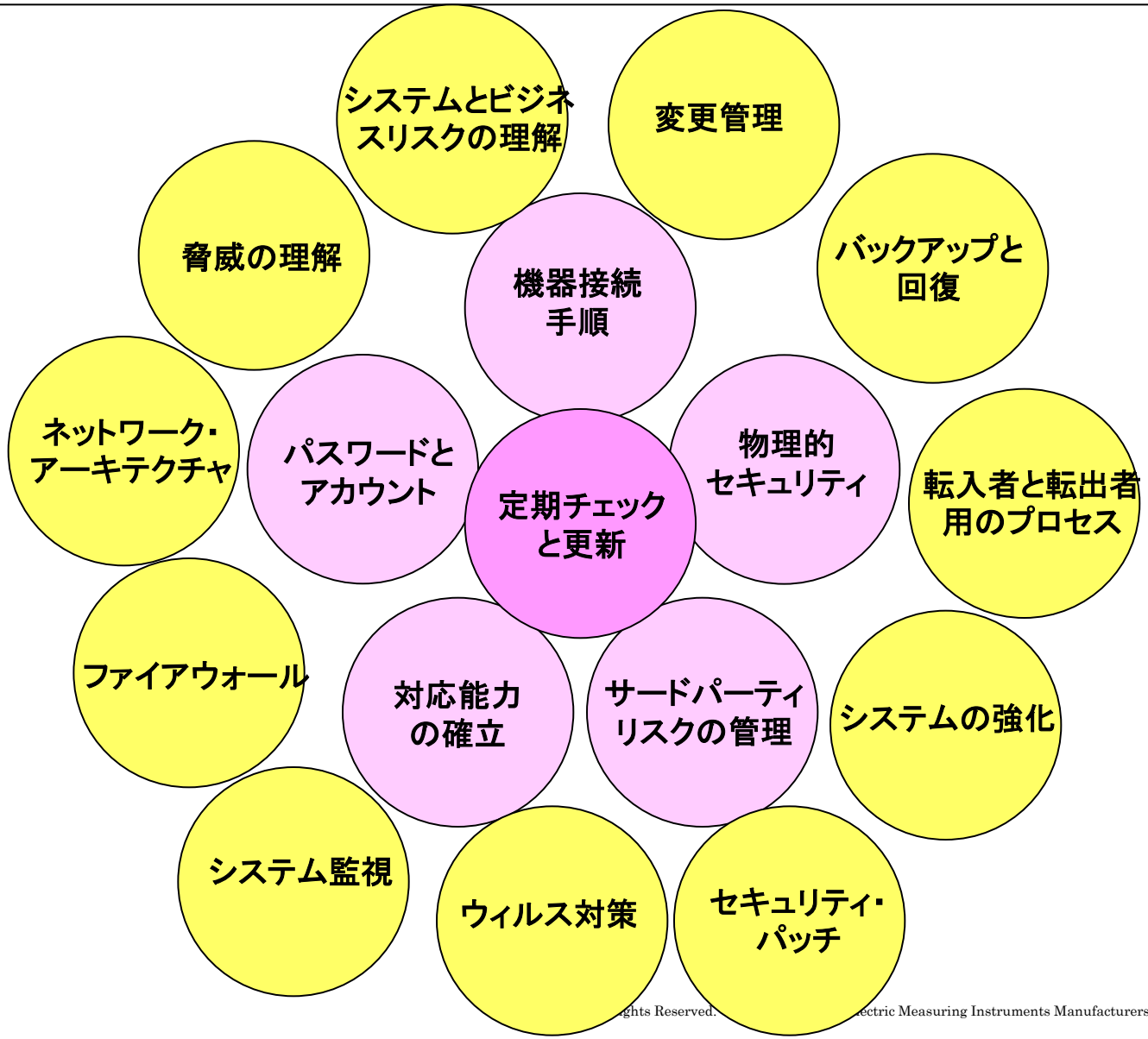


＜施策例＞

- 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

J-CLICSの拡張

J-CLICS　Step2　検討中



JEMIMA

ご静聴ありがとうございました