

計測展2016 OSAKA 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」

2016.11.10

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. J-CLICSの改良
8. まとめ

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. J-CLICSの改良
8. まとめ

SICE/JEITA/JEMIMAセキュリティ合同WG

・活動目的

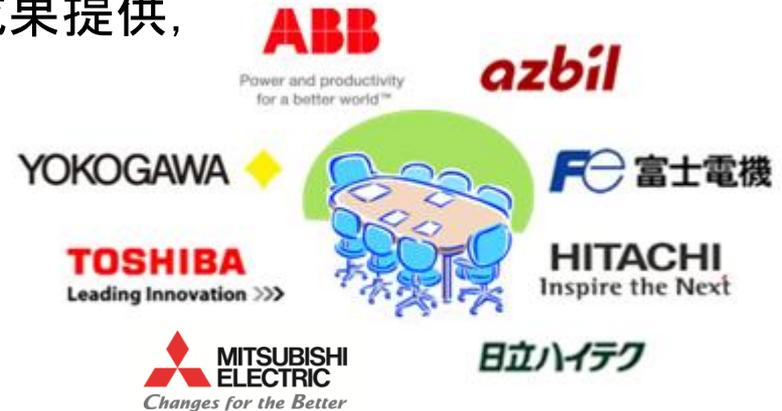
製造業分野におけるセキュリティ標準化動向，技術等の調査・研究活動と会員企業・ユーザへの成果提供，展示会・各種会議での広報

・設立

2005年4月

・メンバー（50音順）

ABB日本ベレー（株）、アズビル（株）、（株）東芝、（株）日立製作所、（株）日立ハイテクソリューションズ、富士電機（株）、三菱電機（株）、横河電機（株）



・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



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. J-CLICSの改良
8. まとめ

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 : International Society of Automation

CPNI : Centre for Protection of National Infrastructure

制御システム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
- 現場作業員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. J-CLICSの改良
8. まとめ

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: 最初の実施すべき基本の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

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
 - 現場作業員・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員や技術者。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

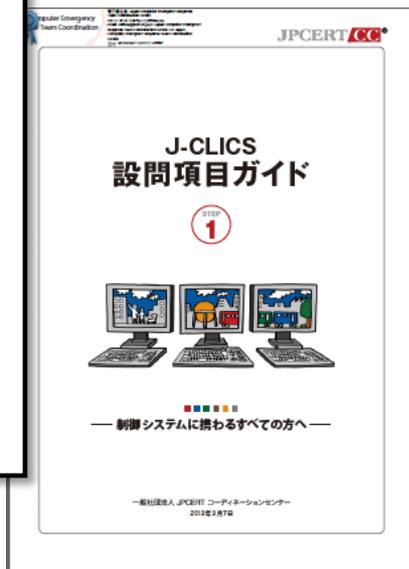
1. セキュリティ合同WGのご紹介
2. 背景と目的
3. J-CLICSの開発
- 4. J-CLICSの構成**
5. J-CLICS Step1 のご紹介
6. J-CLICS Step2 のご紹介
7. J-CLICSの改良
8. まとめ

J-CLICS の構成

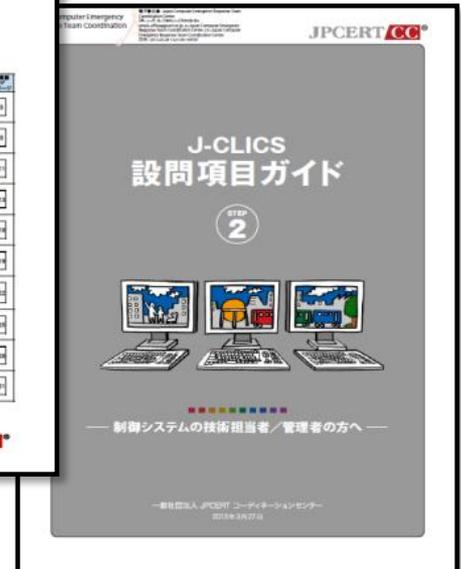
- Step1 (オペレータ・保守作業者などの現場担当者向け), Step2 (システム技術者・マネージャ向け)の2部構成
- いずれもA4のチェックリスト1枚＋設問ガイドから構成



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○×式で回答

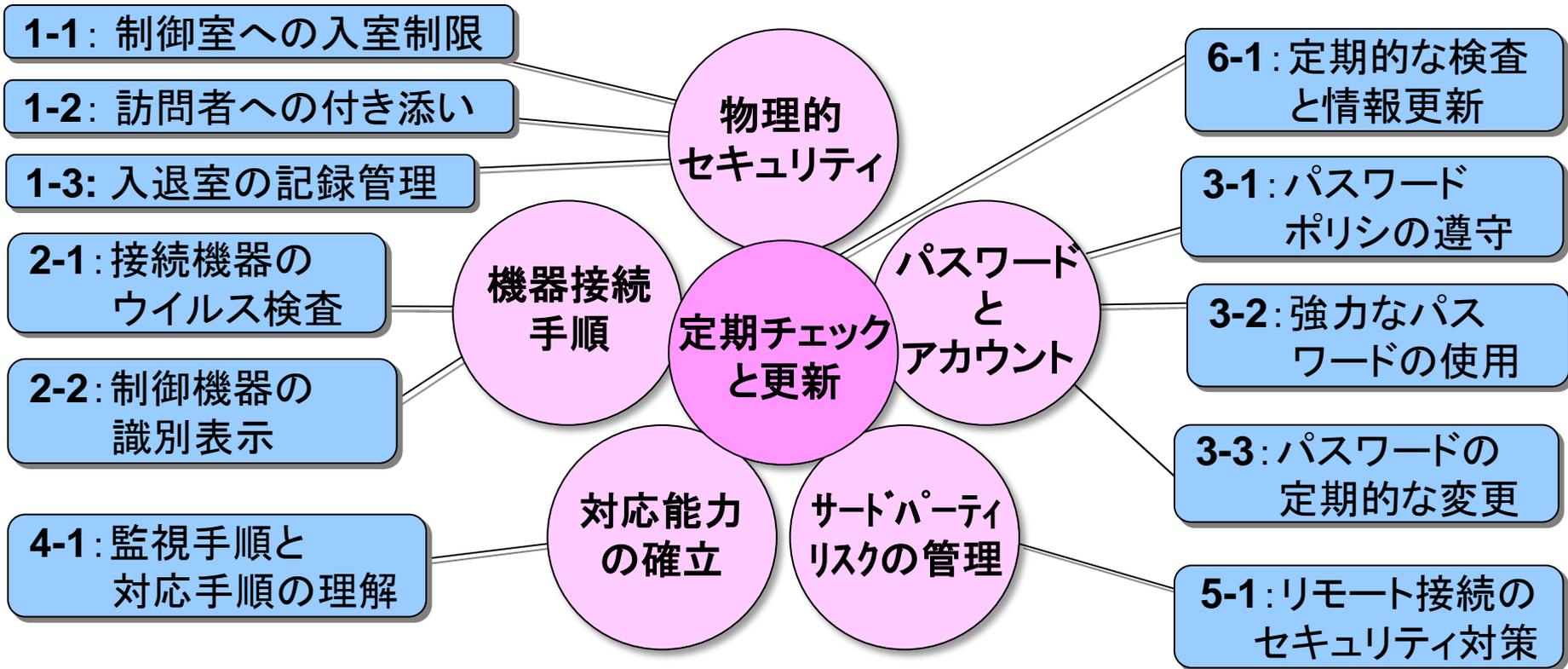
下記の設問に、「○」または「×」でお答えください。

NO	設問	○ / ×	設問項目 ガイド 対応ページ
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)

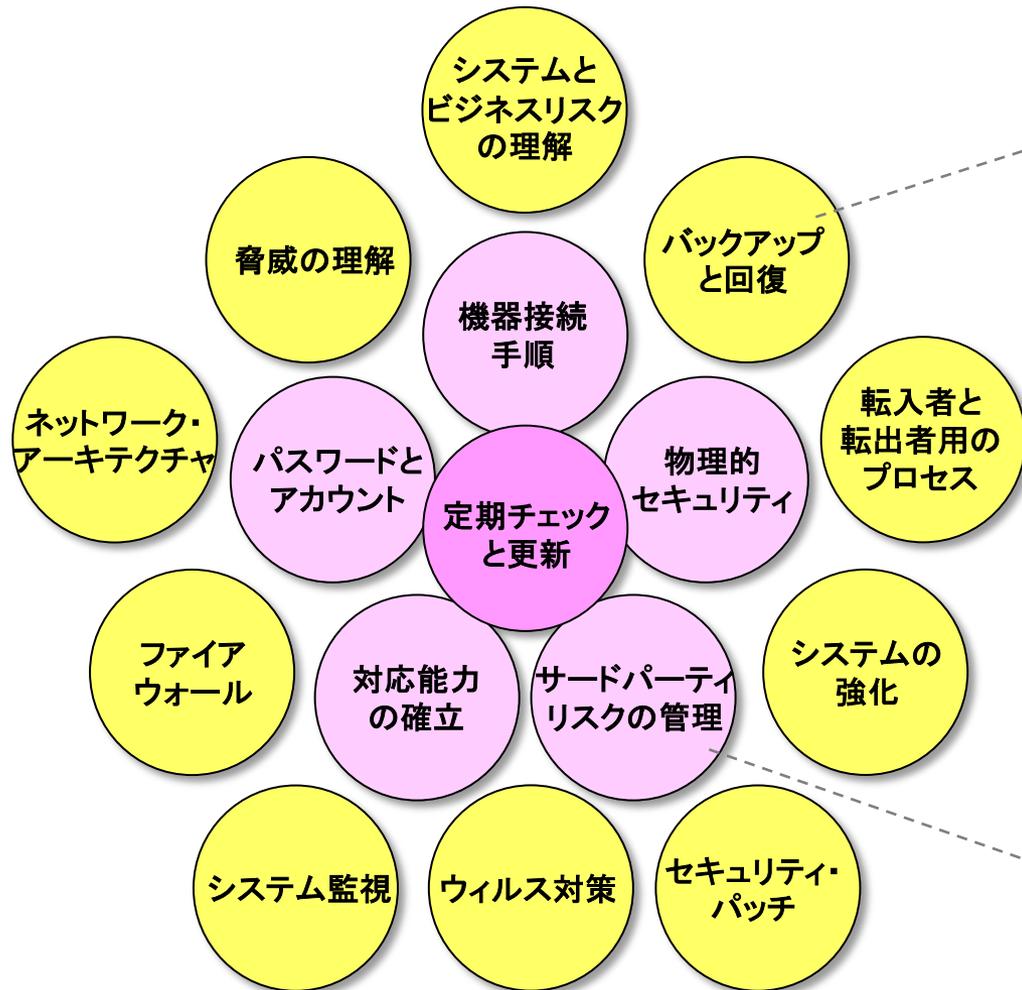
J-CLICS Step1 (現場担当者向け)
優先度の高い6分野 11項目



J-CLICS チェックリスト (Step1:現場担当者向け)

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 : システム技術者・管理者向け)

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

J-CLICS 設問項目ガイド STEP: 制御システムに接続するまでの手順へ

1. 制御室への入退室

【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？

制御室(制御室または接続領域)への入退室は、許可された関係者のみが入室が可能であることを確保するために、適切な入退室管理を行い、許可された関係者のみが入室できるように制御することが求められます。

背景・目的

制御室内には制御システムを操作・管理するための重要な機器が設置されています。また、制御室内では制御されるべき機器の稼働が取り扱われている場合もあります。制御室への許可された操作や機器稼働の誤りを防止するために、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求められます。

想定されるリスク

無許可の者が制御室内に入ると、制御室内の機器への無断アクセスが可能となり、操作や機器稼働の誤り、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、無許可の者が制御室内に入ることにより、不正な操作や変更などが行われ、制御システム稼働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被害を受ける恐れがあります。

1. 制御室への入退室

【設問 No.1-2】

内容解説・施策例

入退室管理の施策例として、次のような施策があります。

(ア) 入退室の管理

- ① 入室を許可する関係者のリストを作成し、関係者に発行する。
- ② 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。
- ③ 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。

(イ) 退室時の管理

許可された関係者はIDカードや他の入室管理システムを使用して入室許可の解除を受ける必要があります。

(ウ) 入退室記録の導入

制御室への入室は、許可された関係者のみに制限できるように、IDカードや他の入室管理システムを導入し、入室記録を導入します。

(エ) 入室の記録

制御室への入室を記録し、一定期間保存します。入室記録の保存期間は、企業ポリシーによって設定、管理します。入退室管理の施策については、【設問 No.1-2】を参照ください。

(オ) 入室許可の見直し

許可された関係者の職務などがあった場合は、直ちに入室許可の見直しを行い、適切な人員に適切な権限を付与するようにします。定期的に関係者リストの更新性を確認し、必要に応じて更新します。

【参考文献】

- JIS Q 37001 「A.6.1.2 物理セキュリティ」
- JIS Q 37001 「A.6.1.3 物理的入退室管理」

【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】

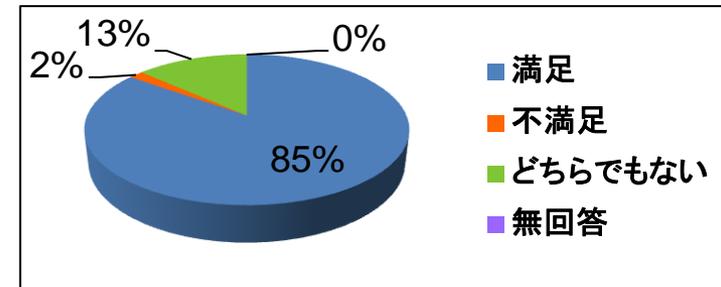
【補足】

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=180)

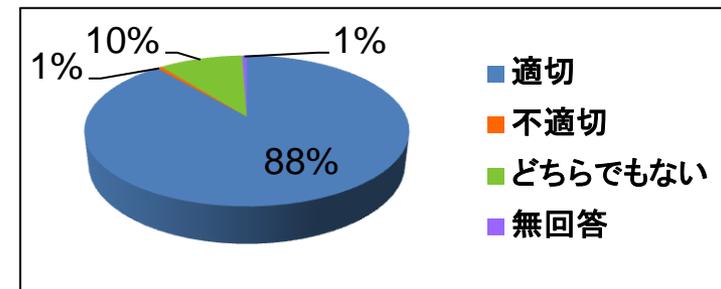
①全体的な内容はいかがでしたか。

満足	不満足	どちらでもない	無回答
153	3	24	0



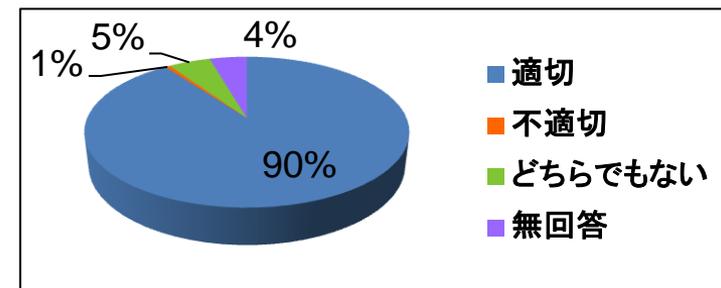
②全体的な設問の用語, 表現はいかがでしたか。

適切	不適切	どちらでもない	無回答
160	1	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
162	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. J-CLICSの改良
8. まとめ

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

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。各現場にご適用いただくことで、セキュリティ上の問題を発見・対応していただくことが目的です。

なお、STEP1は、制御システムに携わる方すべてを対象とし、STEP2は、主に制御システムの技術担当(管理者)を対象としております。

本チェックリストは、制御システムユーザの方々にご活用いただき、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。別システムや他のシステムを複数台ネットワーク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ものや、広く適用されるものとは異なります。尚、本チェックリストは、すべての制御現場をカバーすること、且つその結果を現場担当者(ユーザ)に通知することを前提として作成しております。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」も用意しております。セキュリティ対策を解説される場や社内でのセキュリティ教育に活用される資料として、併せて、ご活用ください。

下記の設問に、「○」または「×」で回答ください。

NO	設問	○ ×	解説ページ
1 制御室にセキュリティ			
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.8
2	制御室 ¹⁾ への訪問時には、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)による定期的な確認を行っていますか？		P.10
2 管理用端末			
1	制御システムネットワークに接続する管理 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定めていますか？		P.14
2	制御システムの管理が制御システムネットワークに接続されている場合、各管理がどのシステムのものであるかを(タグやシールなどで)区分することができますか？		P.14
3 パスワードとアカウント			
1	制御システムのネットワークの高度な有効権限をセキュリティが監視されますか？		P.22
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 対応者の通知			
1	制御システムにおけるセキュリティの監視や異常発生時、異常時の対応方法を通知し、訓練していますか？		P.32
5 サーバールームの管理			
1	リモート接続のセキュリティを確認するためのルール定めていますか？		P.34
6 脆弱性診断と改善			
1	定期的なJ-CLICS定例化は、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、監視室または操作室の設置場所を指し、必ずしも「室」を意味するものではありません。
2) 制御システムネットワークに接続する管理用端末は、制御システムネットワークに接続されている場合、各管理がどのシステムのものであるかを(タグやシールなどで)区分することができます。
3) 英字、数字、記号の組み合わせを使用し、8文字以上で、アポストロフなどを含めず、見出しのパスワード、(内容によって異なる)パスワードの最大長が25文字未満の場合は、最大長のパスワード

SICE JEITA JEMIMA JPCERT CC

設問項目ガイド

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7月2日

J-CLICS設問項目ガイド STEP: 制御システムに携わるすべての方へ

1. 制御室セキュリティ

1-1) の入退室は、**関係者だけに**いますか？

関係室とは操作室、監視室等の設置場所、許可された関係者のみが入室することを確認するために、通常は、許可された関係者のみが入室可能とすることが原則です。

制御室

関係者

関係室とは操作室、監視室等の設置場所、許可された関係者のみが入室することを確認するために、通常は、許可された関係者のみが入室可能とすることが原則です。

関係室

関係室とは操作室、監視室等の設置場所、許可された関係者のみが入室することを確認するために、通常は、許可された関係者のみが入室可能とすることが原則です。

【例1】

セキュリティチェックリスト J-CLICS Step1 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。



【例2】

＜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＞

○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やソフトウェアを最新とする。必要に応じてパッチを適用する
 - ・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

○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



【例3】

<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作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

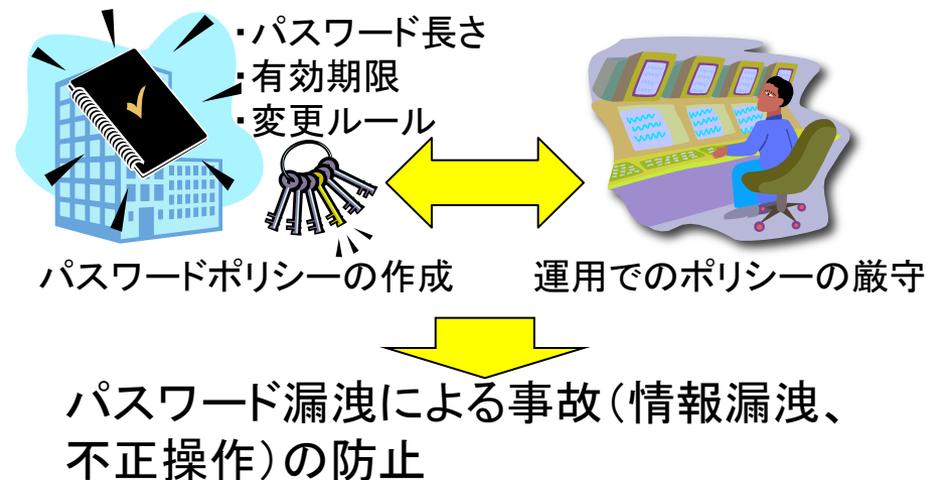
<施策例>

○ 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



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. J-CLICSの改良
8. まとめ

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

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。各設問にご回答いただくことで、セキュリティ上の問題を抽出・把握していただくことを目的としております。

なお、STEP1は、制御システムに属する方すべてを対象とし、STEP2は、主に制御システムの開発者(開発者)を対象としております。

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、理解・理解が得られる内容に絞った設問となっております。制御システム全体の管理・運用のセキュリティレベルを向上させることを目的として、ご回答いただく必要があります。なお、本チェックリストは、すべての設問項目を達成すること、最も高い評価を付与しますが、制御システム全体のセキュリティ向上に貢献するものであればご回答済み、そのこととさせていただきます。

また、各設問項目について解説したJ-CLICS設問項目ガイドを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でのセキュリティ対策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、FOまたはFCで回答してください。

NO	設問	○	△	×	設問項目 番号
システムとプロセスとの関係					
1	制御システム ^{※1} の構成を把握し、変更履歴を含めた最新の状態を管理していますか?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	P.5
管理の確保					
2	制御システム各構成要素について、想定される脅威 ^{※2} を把握していますか?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	P.5
ネットワークアーキテクチャ					
3	制御システムに接続されているすべての機器の脆弱性 ^{※3} 、接続仕様を把握していますか?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	P.11
ファイアウォール					
4	制御システムと他のネットワーク ^{※4} の境界にファイアウォールを構築し、必要な接続を確保していますか?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	P.12
システム監視					
5	平常時にも制御システムの稼働状況 ^{※5} およびログを定期的に確認・分析していますか?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	P.16
サイバー攻撃					
6	制御システムにウイルス対策を行っていますか?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	P.19
セキュリティインシデント					
7	制御システムおよびシステム上で発生しているアプリケーションのバグの使用に関して、脆弱性に付いた不具合による悪影響への影響を調査して、ベンダの提供する修補プログラムに該当する脆弱性を確認していますか?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	P.22
システムの更新					
8	制御システムで稼働するOSやアプリケーションの更新プログラムに、使っていないOSのバージョンの脆弱性 ^{※6} を発生させないよう対応していますか?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	P.25
パッチアップと復旧					
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?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	P.28
購入者と製造者間の責任の分担					
10	システムに接続されている機器等に、設置や更新作業を委託する際に適切な場合に備えて、アクセスの制限やパスワード変更の作業を実施していますか?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	P.31

※1 監視装置、ソフトウェア装置、制御装置を含む
※2 自然災害、人災、誤操作による脅威など
※3 脆弱性、悪影響、脆弱性Patched
※4 社内ネットワーク、インターネット、リモートアクセスなど
※5 CPU負荷、メモリ使用率、ディスク使用率、ネットワーク使用率など
※6 OS更新、サービス更新、ソフトウェア更新など

SICE JEITA JEMIMA JPCERT/CC

Japan Computer Emergency Response Team Coordination Center

J-CLICS 設問項目ガイド

JPCERT/CC

J-CLICS 設問項目ガイド

STEP 2

— 制御システムの技術担当者 / 管理者の方へ —

一般社団法人 JPCERT コーディネーションセンター
2013年3月27日

J-CLICS 設問項目ガイド

STEP2 制御システムの技術担当者 / 管理者の方へ

3. ネットワーク・アーキテクチャ

されている
仕様、
いますか?

に、制御システムに接続されている
仕様を記載した管理台帳を作成
【数値No.1】で作成した管理台帳へ
項目を追加すると、より効率的です。
ことで、資産管理を簡素化できます。

3

11

【例1】

<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？

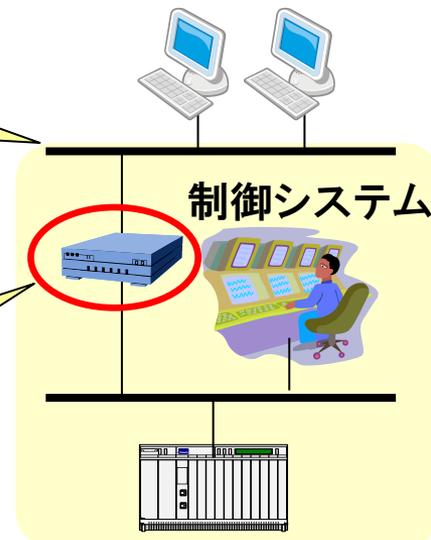
<背景・目的・想定リスク>

- 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。

【例2】

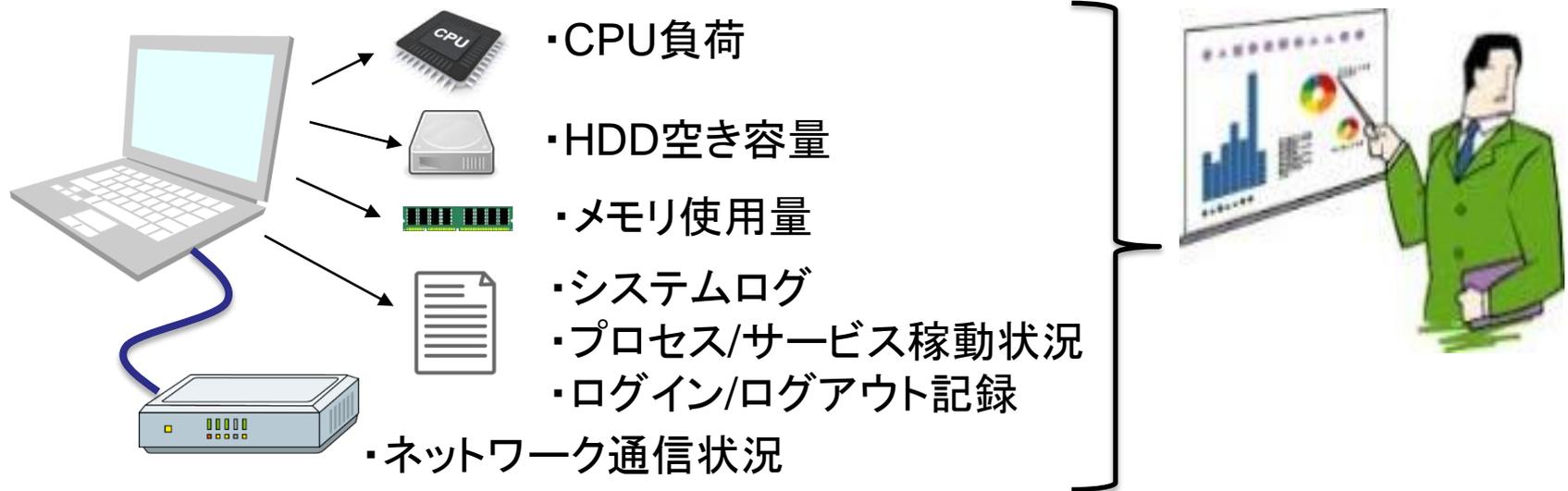
<設問 5-1>

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働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。



【例3】

<設問 8-1>

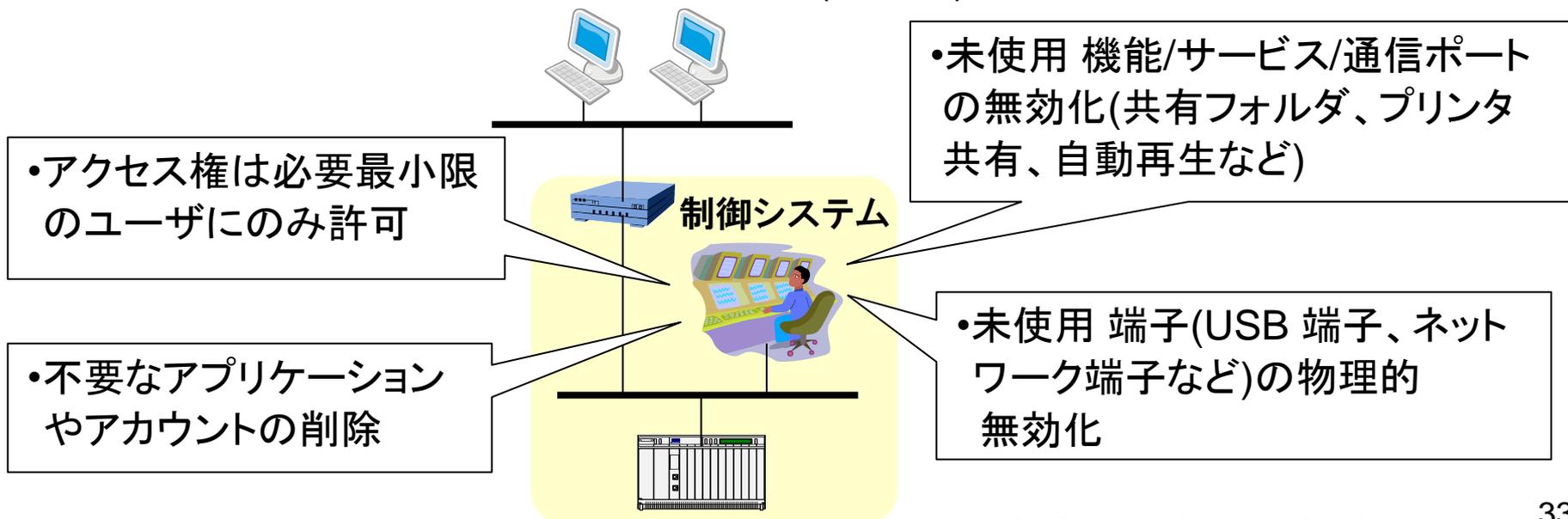
制御システムで使われるOSやアプリケーションの初期導入やバージョンアップ時に使っていないOSのサービスや通信ポートを停止または無効にしていますか？

<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

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. J-CLICSの改良**
8. まとめ

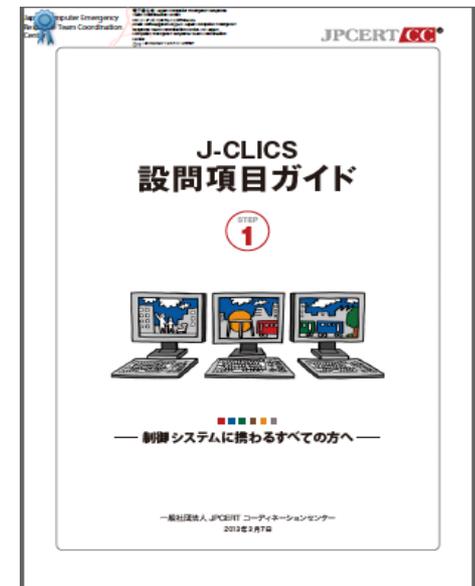
J-CLICS と IEC 62443-3-3 の関連

設問項目ガイドに記載している推奨施策は以下の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) 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

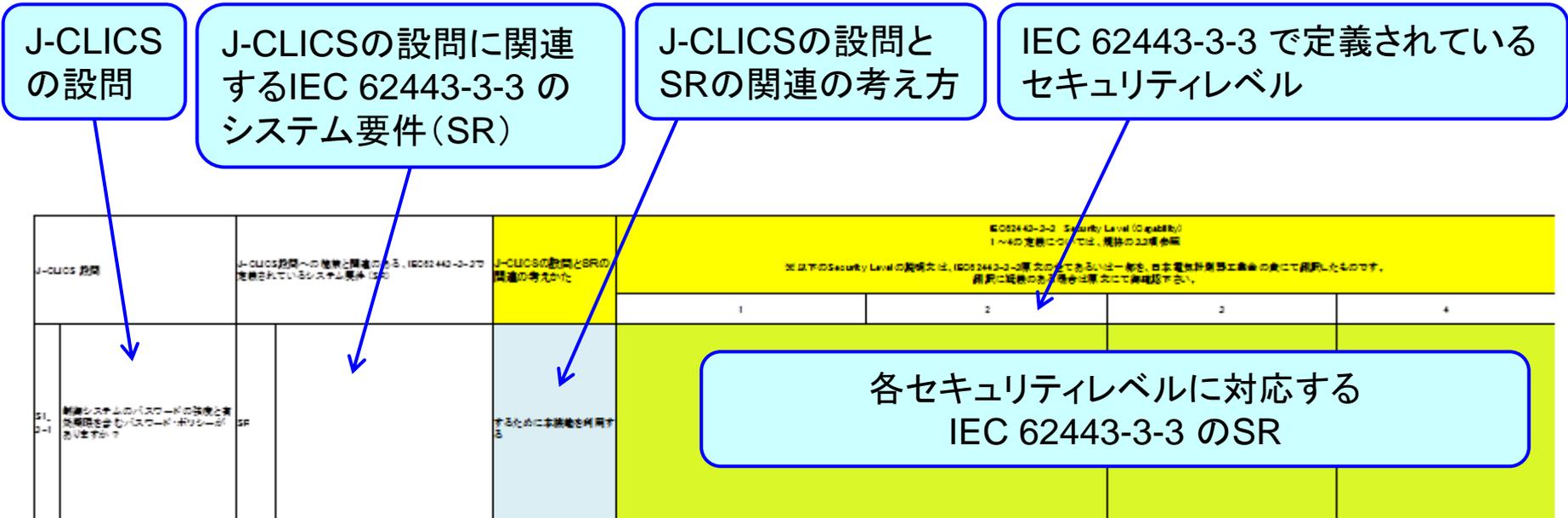
一方、国際標準である**IEC 62443-3-3**では、制御システムがセキュリティに関してどういう機能を持つべきかが**システム要件**としてまとめられています。

現在、3)に分類される推奨施策を**IEC62443-3-3**のシステム要件と対比することで、推奨施策をより具体的にするための検討作業を進めています。
これにより、J-CLICSの利便性を向上させることができると考えております。



J-CLICS と IEC 62443-3-3 の関連

- J-CLICSの各設問に関連するIEC 62443-3-3 のシステム要件 (SR) とその関連の考え方についてまとめ作業を実施中



ユーザ意見の収集

ユーザ意見の吸い上げによるJ-CLICSの改良活動を実施中です。
ユーザ企業にご協力いただき、J-CLICSについてのご意見を収集しました。

• 回答者

– 日本ガス協会の手・準大手ガス事業者10者の生産・供給部門15名

• ご意見

- セキュリティの自己点検について見直しを図っているので参考になった
- 教育資料にも活用できる
- セキュリティの初級用として分かりやすい
- 想定されるリスクだけでなく事例があると良い
- 用語の解説を充実させた方が良い
など



頂いたご意見を整理し、フィードバックを図って行きたいと考えております。

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. J-CLICSの改良
- 8. まとめ**

まとめ

• 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>

• 2016年度も改良活動を継続

- 国際標準IEC 62443-3-3との対比により、推奨施策の具体化を検討中
- 頂いたユーザ意見のフィードバックを検討中

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