J-CLICS 推奨施策から見る国際標準 IEC 62443-3-3

2016 年 12 月 09 日

SICE / JEITA / JEMIMA セキュリティ調査・研究合同 WG

目次

本資料の作成に携わったSICE/JEITA/JEMIMAセキュリティ調査・研究合同WGメンバー

委員

新井　貴之 2)	横河電機株式会社
梅田　裕二 1) 2)	株式会社　東芝
遠藤　浩通 1)	株式会社　日立製作所
窪谷　聡 1)	アズビル株式会社
後藤　浩基 1)	ABB日本ベーレー株式会社
桜井　鐘治 2)	三菱電機株式会社
鈴木　龍一 1)	株式会社　日立ハイテクソリューションズ
高務　健二 1) 2)	富士電機株式会社
高松　家廣 1)	横河電機株式会社
中谷　昌幸	一般社団法人　JPCERTコーディネーションセンター
山田　勉 3)	株式会社　日立製作所
和田　英彦 2)	横河電機株式会社

事務局

瀧田　誠治	一般社団法人　日本電気計測器工業会
松元　敏行	一般社団法人　日本電気計測器工業会

1)【一般社団法人 日本電気計測器工業会(JEMIMA)】

日本電気計測器工業会(JEMIMA) PA・FA計測制御委員会 セキュリティ調査研究WGは、製造業分野でのセキュリティに対する今後の影響、取組みなどを調査・研究し、JEMIMA会員各社に有益となる情報のフィードバックを行う。

2)【一般社団法人 電子情報技術産業協会(JEITA)】

電子情報技術産業協会(JEITA) 制御・エネルギー管理専門委員会は、制御システムのセキュリティ対策を普及・浸透させるための課題や解決策の調査・検討を行い、安全安心な工場・プラント操業のあるべき姿を定義し、提言を行う。

3)【公益社団法人 計測自動制御学会(SICE)】

計測自動制御学会(SICE) 産業応用部門 計測制御ネットワーク部会は、制御システムにおける情報連携のために、最新のIT技術や標準化活動、制御系セキュリティ技術の産業現場への導入等の調査・研究に取り組む。

1. はじめに

SICE/JEITA/JEMIMA セキュリティ調査・研究合同 WG(以下「当 WG」)では、制御システムセキュリティに関連する動向や関連する規格・標準の調査を行っています。当 WG では 2013 年度に、制御システムユーザ向けセキュリティチェックツール J-CLICS※1を制御システムユーザや JPCERT/CC の協力のもとで作成しました。また、2015 年度からは、近年関心が高まりつつある国際標準 IEC 62443-3-3※2の調査を実施してきました。IEC 62443-3-3 では制御システムが提供することが望ましい種々のセキュリティ機能とそのレベルがシステム要件 SR※3として定義されています。また、各 SR（基本要件）の強化要件として RE※4が最大で 3 段階まで定義されています。

J-CLICS の作成と IEC 62443-3-3 の調査はそれぞれ独立した活動ですが、制御システムのセキュリティ施策に関する理解を深めるために、J-CLICS に記載されている施策例と IEC 62443-3-3 の SR を対比し、関連性がある項目を紐付けしてみることにしました。本資料はその結果をまとめたものです。

本資料の用途・期待する効果

1）J-CLICS 読者が J-CLICS の各設問項目に関連する IEC 62443-3-3 の SR 項目を参照できます。各セキュリティ施策の理解を深めるための資料となることを期待しています。

2）J-CLICS 読者が IEC 62443-3-3 の学習を始めるための資料として利用できます。
J-CLICS に関連する SR 項目から学習を開始することで IEC 62443-3-3 の理解の助けになることを期待しています。

本資料について

本資料は当 WG における調査活動のひとつとして参加委員によって作成されました。制御システムのセキュリティ施策に関する理解を深めるための参考資料となることを目的としたものであり、国際規格との対応の保証や施策の提案を目的としたものではありません。

J-CLICS は制御システムユーザが参加する J-CLICS ユーザ合同協議会の協力において当 WG が作成しました。J-CLICS チェックリストおよび J-CLICS 設問項目ガイドは一般社団法人 JPCERT/CC から無料で入手できます。

IEC 62443-3-3 は、IEC から発行されている国際規格文書です。IEC 62443-3-3 からの引用は、一般財団法人日本規格協会の了解のもとで行い、翻訳は当 WG の責で行いました。この翻訳文は参考用として提供するものであり、内容・解釈の正当性を保証するものではありません。IEC 62443-3-3 の内容については、IEC が発行する正式な原文書を参照してください。

※1 Check List for Industrial Control Systems of Japan

※2 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

※3 System Requirement

※4 Requirement Enhancement

2. J-CLICS と IEC 62443-3-3 の関連

J-CLICS の各設問に対して IEC 62443-3-3 で定義されているシステム要件 SR の関連について記載します。

2.1. J-CLICS の設問に関連する IEC 62443-3-3 の SR

J-CLICS の各設問に関連する IEC 62443-3-3 の SR を以下に示します。

2.1.1. J-CLICS Step1 の設問に関連する IEC 62443-3-3 の SR

設問カテゴリ	設問 No.	関連する SR
1. 物理的セキュリティ	1-1	－
	1-2	－
	1-3	－
2. 機器接続手順	2-1	SR3.2 SR3.3 SR3.4
	2-2	－
3. パスワードとアカウント	3-1	SR1.7
	3-2	
	3-3	
4. 対応能力の確立	4-1	SR7.3 SR7.4
5. サードパーティリスクの管理	5-1	SR1.13 SR2.6 SR4.1
6. 継続的な評価と改善	6-1	－

2.1.2. J-CLICS Step2 の設問に関連する IEC 62443-3-3 の SR

設問カテゴリ	設問 No.	関連する SR
1. システムとビジネスリスクの理解	1-1	SR7.6 SR7.8
2. 脅威の理解	2-1	－
3. ネットワーク・アーキテクチャ	3-1	－
4. ファイアウォール	4-1	SR3.2 SR5.1 SR5.2
5. システム監視	5-1	SR2.8 SR6.1 SR6.2
6. ウイルス対策	6-1	SR3.2
7. セキュリティパッチ	7-1	SR7.3 SR7.4
8. システムの強化	8-1	SR7.7
9. バックアップと回復	9-1	SR7.3 SR7.4
10. 転入者と転出者用のプロセス	10-1	－

2.2. J-CLICS と SR の関連

J-CLICS の各設問に関連する IEC 62443-3-3 の SR とその関連の考え方について以下に示します。

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。

J-CLICS Step1	3. パスワードとアカウント
設問 No.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？
設問 No.3-2	強力なパスワード※6を使用していますか？
設問 No.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？
関連する SR	SR1.7　パスワードをベースとした認証の強度
関連の考え方	設問 No.3-1：パスワード・ポリシーを設定する際に、本機能を参考にすることが有効です。 設問 No.3-2：本 SR の機能により、パスワードの強度を設定でき、強力なパスワードの使用に活用できます。 設問 No.3-3：本 SR の機能により、パスワードの変更期間を設定でき、定期的なパスワードの変更に活用できます。

J-CLICS Step1	4. 対応能力の確立
設問 No.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、異常時の対応方法を理解し、訓練をしていますか？
関連する SR	SR7.3　制御システムのバックアップ SR7.4　制御システムのリカバリと再構築
関連の考え方	本 SR の機能は、異常時対応方法として代表的な機能/能力であるシステムのバックアップ、リカバリ、再構築に活用できます。

J-CLICS Step1	5. サードパーティリスクの管理
設問 No.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？
関連する SR	SR1.13　信頼できないネットワーク経由のアクセス SR2.6　リモートセッションの終了 SR4.1　情報の機密性
関連の考え方	本 SR の機能は、リモート接続のルールの遵守に加え、不正な操作や通信の防止に有効です。

※5 USB 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。

※6 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。

J-CLICS Step2	1. システムとビジネスリスクの理解
設問 No.1-1	制御システム※7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？
関連する SR	SR7.6　ネットワークとセキュリティの設定 SR7.8　制御システムのコンポーネントの一覧
関連の考え方	本 SR の機能は、制御システムの最新の状態を把握する仕組み構築に活用できます。

J-CLICS Step2	4. ファイアウォール
設問 No.4-1	制御システムと他のネットワーク※8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？
関連する SR	SR3.2　悪意のあるコードの防御 SR5.1　ネットワーク分割 SR5.2　ゾーン境界保護
関連の考え方	本 SR の機能は、システム構築する際のネットワーク構成を検討する際に活用でき、制御ネットワークへの不必要な通信の防止に有効です。

J-CLICS Step2	5. システム監視
設問 No.5-1	平常時にも制御システムの稼働状況※9およびログを定期的に確認・分析していますか？
関連する SR	SR2.8　監査可能なイベント SR6.1　監査ログへのアクセス SR6.2　連続的な監視
関連の考え方	本 SR の機能は、稼働状況およびログを常時取得・保存し、後でそれらを閲覧するための仕組み構築に活用できます。

J-CLICS Step2	6. ウイルス対策
設問 No.6-1	制御システムにウイルス対策を行っていますか？
関連する SR	SR3.2　悪意のあるコードの防御
関連の考え方	本 SR の機能は、ウイルスの予防・検知・対処などの機能を設ける際に有効です。

※7 情報資産、ソフトウェア資産、物理的資産を含む。
※8 オフィスネットワーク、インターネット、リモートアクセスなど。
※9 CPU 負荷、ディスク容量管理、システムログなど。

J-CLICS Step2	7. セキュリティパッチ
設問 No.7-1	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？
関連する SR	SR7.3　制御システムのバックアップ SR7.4　制御システムのリカバリと再構築
関連の考え方	本 SR の機能は、パッチ適用に伴う不具合発生に備えたバックアップ、リカバリおよび再構築に活用できます。

J-CLICS Step2	8. システムの強化
設問 No.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？
関連する SR	SR7.7　最小機能
関連の考え方	本 SR の機能は、機能、サービスや通信ポートを必要最小限に制限する上で有効です。

J-CLICS Step2	9. バックアップと回復
設問 No.9-1	制御システムの復旧に必要なデータ※10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？
関連する SR	SR7.3　制御システムのバックアップ SR7.4　制御システムのリカバリと再構築
関連の考え方	本 SR の機能は、ベンダが推奨する制御システムのバックアップ方法の実施に有効です。

※10 パラメータ、操業データなど。

2.3. SR（基本要件）/ RE（強化要件）と SL（セキュリティレベル）

各 SR はその強化要件である RE が最大で 3 段階（RE1、RE2、RE3）まで定義され、ユーザが要求するセキュリティレベル SL-C※11（1:低→4:高）に対して、どの段階の SR/RE まで対応する必要があるかが定義されています。

以下の例では、ユーザ要求のセキュリティレベル SL-C1 を満たすためには基本要件のみの対応で済みますが、SL-C2 を満たすためには、基本要件に加えて RE1 にも対応する必要があります。同様に SL-C3 は基本の要件と RE1、RE2 に対応する必要があり、SL-C4 は RE3 までの全ての要件に対応する必要があります。

（SR/RE と SL-C の対応の例）

RE	要件	SL-C			
		1	2	3	4
(SR)	*基本要件のタイトル* *基本要件の内容*	✔	✔	✔	✔
1	*強化要件 RE1 のタイトル* *強化要件 RE1 の内容*		✔	✔	✔
2	*強化要件 RE2 のタイトル* *強化要件 RE2 の内容*			✔	✔
3	*強化要件 RE3 のタイトル* *強化要件 RE3 の内容*				✔

以下に、各 SR/RE と SL の対応について記載します。また、これらの一覧表を参考として本資料の末尾に掲載しました。

2.3.1. SR1.7 パスワードをベースとした認証の強度

RE	要件	SL-C			
		1	2	3	4
(SR)	パスワードをベースとした認証の強度 パスワードをベースとした認証を利用している制御システムでは、制御システムは、最小の長さ及び文字タイプの種類をベースとした設定可能なパスワード強度を強制できる機能を備えていなければならない。	✔	✔	✔	✔
1	人間のユーザに対するパスワードの世代と有効期間の制限 制御システムは、任意の人間のユーザアカウントが設定可能な世代の数の間、パスワードを再利用することを防止できる機能を備えていなければならない。加えて、制御システムは、人間のユーザに対してパスワードの最小及び最大の有効期間の制限を強制できる機能を備えていなければならない。これらの機能は一般的に容認されたセキュリティ業界の慣行に従わなければならない。			✔	✔
2	すべてのユーザに対するパスワードの有効期間の制限 制御システムは、すべてのユーザに対してパスワードの最小及び最大の有効期間の制限を強制できる機能を備えていなければならない。				✔

※11 Capability security level

2.3.2. SR1.13 信頼できないネットワーク経由のアクセス

RE	要件	SL-C			
		1	2	3	4
(SR)	信頼できないネットワーク経由のアクセス 制御システムは、信頼できないネットワーク経由の制御システムへのすべてのアクセス方法を監視及び制御する機能を備えていなければならない。	✔	✔	✔	✔
1	明示的アクセス要求の許可 制御システムは、割り当てられた役割によって許可されない限り、信頼できないネットワーク経由のアクセス要求を拒否する機能を備えていなければならない。		✔	✔	✔

2.3.3. SR2.6 リモートセッションの終了

RE	要件	SL-C			
		1	2	3	4
(SR)	リモートセッションの終了 制御システムは、設定可能な不使用時間の経過後自動的に又はセッションを開始したユーザによる手動のいずれかで、リモートセッションを終了する機能を備えていなければならない。		✔	✔	✔

2.3.4. SR2.8 監査可能なイベント

RE	要件	SL-C			
		1	2	3	4
(SR)	監査可能なイベント 制御システムは、以下の部類に対してセキュリティに関連する監査用記録を生成する機能を備えていなければならない：アクセス制御、リクエストエラー、OS のイベント、制御システムのイベント、バックアップ及びリストアのイベント、設定変更、潜在的な偵察行動、監査ログに関するイベント。 各々の監査用記録は、タイムスタンプ、生成元（発生した機器、ソフトウェアプロセス又は人間のユーザアカウント）、部類、種類、イベント ID、イベントの結果を含まなければならない。	✔	✔	✔	✔
1	集中管理されたシステム全体の監査証跡 制御システムは、監査イベントを集中管理し、また、制御システム全体において複数の機器が生成した監査用記録を編集・加工してシステム全体（物理的または論理的な）において時系列的に関連付けられた監査証跡を生成する機能を備えていなければならない。 制御システムは、これらの監査用記録を、SIEM など商用のログ分析ツールで分析可能な業界標準の書式で出力する機能を備えていなければならない。			✔	✔

2.3.5. SR3.2 悪意のあるコードの防御

RE	要件	SL-C			
		1	2	3	4
(SR)	悪意のあるコードの防御 制御システムは、悪意のあるコードや許可されていないソフトウェアの影響を、防止、検出、報告及び軽減するための防御の仕組みを利用できる機能を備えていなければならない。制御システムは、防御の仕組みを更新できる機能を備えていなければならない。	✔	✔	✔	✔
1	入口と出口における悪意のあるコードの防御 制御システムは、システムのすべての入口及び出口において、悪意のあるコードの防御の仕組みを利用できる機能を備えていなければならない。		✔	✔	✔
2	悪意のあるコードの防御の集中管理とレポート 制御システムは、悪意のあるコードの防御の仕組みを管理できる機能を備えていなければならない。			✔	✔

2.3.6. SR3.3 セキュリティ機能の検証

RE	要件	SL-C			
		1	2	3	4
(SR)	セキュリティ機能の検証 制御システムは、FAT、SAT 及び計画されたメンテナンス時に、セキュリティ機能の意図した動作を検証し、異常が検出された場合にレポートできる機能を備えていなければならない。ここでのセキュリティに関する機能は、本規格で指定されたセキュリティ要求をサポートするために必要なものを全て含んでいなければならない。	✔	✔	✔	✔
1	セキュリティ機能の検証のための自動化された仕組み 制御システムは、FAT、SAT 及び計画されたメンテナンス時に、セキュリティ検証の管理をサポートする自動的な仕組みを利用できる機能を備えていなければならない。			✔	✔
2	通常運転時のセキュリティ機能の検証 制御システムは、通常運転時に、セキュリティ機能の意図された動作の検証をサポートする機能を備えていなければならない。				✔

2.3.7. SR3.4 ソフトウェアと情報の完全性

RE	要件	SL-C			
		1	2	3	4
(SR)	ソフトウェアと情報の完全性 制御システムは、ソフトウェアや保存されている情報に対する許可されていない変更を検出、報告及び防御する機能を備えていなければならない。	✔	✔	✔	✔
1	完全性に問題があった時の自動通知 制御システムは、システムの完全性をチェックしている間に問題が発見されたら、設定可能な宛先にその相違を自動的に通知するツールを使える機能を備えていなければならない。			✔	✔

2.3.8. SR4.1 情報の機密性

RE	要件	SL-C			
		1	2	3	4
(SR)	情報の機密性 制御システムは、保存状態であれ、転送中であれ、明示的な読み出しの許可がサポートされている情報の機密性を保護する機能を備えていなければならない。	✔	✔	✔	✔
1	保存情報または信頼できないネットワーク経由で転送されている情報の機密性の保護 制御システムは、保存状態にある情報及び信頼できないネットワークを通過するリモート接続セッションの情報の機密性を保護する機能を備えていなければならない。		✔	✔	✔
2	ゾーン境界での機密性の保護 制御システムは、任意のゾーン境界を通過する情報の機密性を保護する機能を備えていなければならない。				✔

2.3.9. SR5.1 ネットワーク分割

RE	要件	SL-C			
		1	2	3	4
(SR)	ネットワーク分割 制御システムは、制御システムネットワークと非制御システムネットワーク間及びクリティカルな制御システムネットワークと他の制御システムネットワーク間を論理的に分割できる機能を備えていなければならない。	✔	✔	✔	✔
1	物理的なネットワーク分割 制御システムは、制御システムネットワークと非制御システムネットワーク間及びクリティカルな制御システムネットワークと非クリティカルな制御システムネットワーク間を物理的に分割できる機能を備えていなければならない。		✔	✔	✔
2	非制御システムネットワークからの独立 制御システムは、非制御システムネットワークとの接続がなくても、制御システムネットワーク（クリティカル及び非クリティカル）へのネットワークサービスを提供できる機能を備えていなければならない。			✔	✔
3	クリティカルネットワークの論理的及び物理的な絶縁 制御システムは、クリティカルな制御システムネットワークと非クリティカルな制御システムネットワークを論理的及び物理的に絶縁できる機能を備えていなければならない。				✔

2.3.10. SR5.2 ゾーン境界保護

RE	要件	SL-C			
		1	2	3	4
(SR)	ゾーン境界保護 制御システムは、リスクベースのゾーン・コンジットモデルで定義された区画を強制するため、ゾーン境界で通信を監視および制御できる機能を備えていなければならない。	✔	✔	✔	✔
1	デフォルトで拒否、例外によって許可 制御システムは、デフォルトではネットワークトラフィックを拒否し、例外としてネットワークトラフィックを許可する機能を備えていなければならない（deny all, permit by exception とも呼ばれる）。		✔	✔	✔
2	アイランドモード 制御システムは、制御システムの境界を通過する通信を防止する機能を備えていなければならない（island mode とも呼ばれる）。			✔	✔
3	フェールクローズ 制御システムは、境界を防御する機能が動作異常となった場合に制御システムの境界を通過する通信を防止する機能を備えていなければならない（fail close とも呼ばれる）。 この’フェールクローズ’機能は、SIS または他の安全関連機能の動作を干渉しないように設計されなければならない。				✔

2.3.11. SR6.1 監査ログへのアクセス

RE	要件	SL-C			
		1	2	3	4
(SR)	監査ログへのアクセス 制御システムは、権限のある要員及び/又はツールに対して読み出し専用で監査ログにアクセスさせる機能を備えていなければならない。	✔	✔	✔	✔
1	プログラムによる監査ログへのアクセス 制御システムは、アプリケーション・プログラミング・インタフェース（API）を用いてプログラムから監査ログにアクセスできる機能を備えていなければならない。			✔	✔

2.3.12. SR6.2 連続的な監査

RE	要件	SL-C			
		1	2	3	4
(SR)	連続的な監視 制御システムは、セキュリティ侵害を適時に検知、特定及び報告するため、セキュリティ業界で一般的に受け入れられている手法や推奨事項を用いて、全てのセキュリティ機能の性能を継続的に監視する機能を備えていなければならない。		✔	✔	✔

2.3.13. SR7.3 制御システムのバックアップ

RE	要件	SL-C			
		1	2	3	4
(SR)	制御システムのバックアップ 重要ファイルを識別し場所を特定する機能及びユーザレベル及びシステムレベルの情報（システム状態の情報を含む）のバックアップを実施する能力は、通常のプラント運転に影響を与えることなく制御システムによってサポートされなければならない。	✔	✔	✔	✔
1	バックアップの検証 制御システムは、バックアップの仕組みの信頼性を検証する機能を備えていなければならない。		✔	✔	✔
2	バックアップの自動化 制御システムは、頻度を設定できるバックアップ機能を自動化する機能を備えていなければならない。			✔	✔

2.3.14. SR7.4 制御システムのリカバリと再構築

RE	要件	SL-C			
		1	2	3	4
(SR)	制御システムのリカバリと再構築 制御システムは、障害や異常が発生した後、既知のセキュアな状態に回復及び再構成する機能を備えていなければならない。	✔	✔	✔	✔

2.3.15. SR7.6 ネットワークとセキュリティの設定

RE	要件	SL-C			
		1	2	3	4
(SR)	ネットワークとセキュリティの設定 制御システムは、制御システムのサプライヤが提供するガイドラインに記述される、推奨のネットワーク及びセキュリティの設定に従って設定される機能を備えていなければならない。また、制御システムは、その時点で展開されているネットワーク及びセキュリティの設定へのインタフェースを提供しなければならない。	✔	✔	✔	✔
1	現在のセキュリティ設定のマシンリーダブルな報告 制御システムは、現在のセキュリティ設定をマシンリーダブルな形式でリスト化した報告書を生成する機能を備えていなければならない。			✔	✔

2.3.16. SR7.7 最小機能

RE	要件	SL-C			
		1	2	3	4
(SR)	最小機能 制御システムは、不要な機能、ポート、プロトコル及び/又はサービスの使用を、具体的に禁止及び/又は制限する機能を備えていなければならない。	✔	✔	✔	✔

2.3.17. SR7.8 制御システムのコンポーネントの一覧

RE	要件	SL-C			
		1	2	3	4
(SR)	制御システムのコンポーネントの一覧 制御システムは、インストールされているコンポーネント及びそれらと関連するプロパティの現在のリストを報告できる機能を備えていなければならない。		✔	✔	✔

参考：J-CLICS設問と関連のある IEC 62443-3-3 で定義されているシステム要件

J-CLICS設問			J-CLICS設問と関連のある IEC 62443-3-3で定義されている システム要件（SR）		J-CLICS設問とSRの関連の考えかた	IEC 62443-3-3 SR（基本要件）/ RE（強化要件）と SL-C（セキュリティレベル） ※以下の内容は、IEC 62443-3-3原文のSR / RE の全てあるいは一部を、日本電気計測器工業会の責にて翻訳したものです。 翻訳に疑義のある場合は原文にて御確認下さい。			
						SL-C 1	SL-C 2	SL-C 3	SL-C 4
機器接続手順	S1_2-1	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？	SR3.2	悪意のあるコードの防御	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。	<SR：悪意のあるコードの防御> 制御システムは、悪意のあるコードや許可されていないソフトウェアの影響を、防止、検出、報告及び軽減するための防御の仕組みを利用できる機能を備えていなければならない。制御システムは、防御の仕組みを更新できる機能を備えていなければならない。	<RE1：入口と出口における悪意のあるコードの防御> 制御システムは、システムのすべての入口及び出口において、悪意のあるコードの防御の仕組みを利用できる機能を備えていなければならない。	<RE2：悪意のあるコードの防御の集中管理とレポート> 制御システムは、悪意のあるコードの防御の仕組みを管理できる機能を備えていなければならない。	
			SR3.3	セキュリティ機能の検証		<SR：セキュリティ機能の検証> 制御システムは、FAT、SAT及び計画されたメンテナンス時に、セキュリティ機能の意図した動作を検証し、異常が検出された場合にレポートできる機能を備えていなければならない。ここでのセキュリティに関する機能は、本規格で指定されたセキュリティ要求をサポートするために必要なものを全て含んでいなければならない。		<RE1：セキュリティ機能の検証のための自動化された仕組み> 制御システムは、FAT、SAT及び計画されたメンテナンス時に、セキュリティ検証の管理をサポートする自動的な仕組みを利用できる機能を備えていなければならない。	<RE2：通常運転時のセキュリティ機能の検証> 制御システムは、通常運転時に、セキュリティ機能の意図された動作の検証をサポートする機能を備えていなければならない。
			SR3.4	ソフトウェアと情報の完全性		<SR：ソフトウェアと情報の完全性> 制御システムは、ソフトウェアや保存されている情報に対する許可されていない変更を検出、報告及び防御する機能を備えていなければならない。		<RE1：完全性に問題があった時の自動通知> 制御システムは、システムの完全性をチェックしている間に問題が発見されたら、設定可能な宛先にその相違を自動的に通知するツールを使える機能を備えていなければならない。	
パスワードとアカウント	S1_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？	SR1.7	パスワードをベースとした認証の強度	パスワード・ポリシーを設定する際に、本機能を参考にすることが有効です。	<SR：パスワードをベースとした認証の強度> パスワードをベースとした認証を利用している制御システムでは、制御システムは、最小の長さ及び文字タイプの種類をベースとした設定可能なパスワード強度を強制できる機能を備えていなければならない。		<RE1：人間のユーザに対するパスワードの世代と有効期間の制限> 制御システムは、任意の人間のユーザアカウントが設定可能な世代の数の間、パスワードを再利用することを防止できる機能を備えていなければならない。加えて、制御システムは、人間のユーザに対してパスワードの最小及び最大の有効期間の制限を強制できる機能を備えていなければならない。これらの機能は一般的に容認されたセキュリティ業界の慣行に従わなければならない。	<RE2：すべてのユーザに対するパスワードの有効期間の制限> 制御システムは、すべてのユーザに対してパスワードの最小及び最大の有効期間の制限を強制できる機能を備えていなければならない。
	S1_3-2	強力なパスワードを使用していますか？	SR1.7	パスワードをベースとした認証の強度	本SRの機能により、パスワードの強度を設定でき、強力なパスワードの使用に活用できます。				
	S1_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？	SR1.7	パスワードをベースとした認証の強度	本SRの機能により、パスワードの変更期間を設定でき、定期的なパスワードの変更に活用できます。				
対応能力の確立	S1_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？	SR7.3	制御システムのバックアップ	本SRの機能は、異常時対応方法として代表的な機能/能力であるシステムのバックアップ、リカバリ、再構築に活用できます。	<SR：制御システムのバックアップ> 重要ファイルを識別し場所を特定する機能及びユーザレベル及びシステムレベルの情報（システム状態の情報を含む）のバックアップを実施する能力は、通常のプラント運転に影響を与えることなく制御システムによってサポートされなければならない。	<RE1：バックアップの検証> 制御システムは、バックアップの仕組みの信頼性を検証する機能を備えていなければならない。	<RE2：バックアップの自動化> 制御システムは、頻度を設定できるバックアップ機能を自動化する機能を備えていなければならない。	
			SR7.4	制御システムのリカバリと再構築		<SR：制御システムのリカバリと再構築> 制御システムは、障害や異常が発生した後、既知のセキュアな状態に回復及び再構成する機能を備えていなければならない。			
サードパーティリスクの管理	S1_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？	SR1.13	信頼できないネットワーク経由のアクセス	本SRの機能は、リモート接続のルールの遵守に加え、不正な操作や通信の防止に有効です。	<SR：信頼できないネットワーク経由のアクセス> 制御システムは、信頼できないネットワーク経由の制御システムへのすべてのアクセス方法を監視及び制御する機能を備えていなければならない。	<RE1：明示的アクセス要求の許可> 制御システムは、割り当てられた役割によって許可されない限り、信頼できないネットワーク経由のアクセス要求を拒否する機能を備えていなければならない。		
			SR2.6	リモートセッションの終了			<SR：リモートセッションの終了> 制御システムは、設定可能な不使用時間の経過後自動的に又はセッションを開始したユーザによる手動のいずれかで、リモートセッションを終了する機能を備えていなければならない。		
			SR4.1	情報の機密性		<SR：情報の機密性> 制御システムは、保存状態であれ、転送中であれ、明示的な読み出しの許可がサポートされている情報の機密性を保護する機能を備えていなければならない。	<RE1：保存情報または信頼できないネットワーク経由で転送されている情報の機密性の保護> 制御システムは、保存状態にある情報及び信頼できないネットワークを通過するリモート接続セッションの情報の機密性を保護する機能を備えていなければならない。		<RE2：ゾーン境界での機密性の保護> 制御システムは、任意のゾーン境界を通過する情報の機密性を保護する機能を備えていなければならない。
システムとビジネスリスクの理解	S2_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？	SR7.6	ネットワークとセキュリティの設定	本SRの機能は、制御システムの最新の状態を把握する仕組み構築に活用できます。	<SR：ネットワークとセキュリティの設定> 制御システムは、制御システムのサプライヤが提供するガイドラインに記述される、推奨のネットワーク及びセキュリティの設定に従って設定される機能を備えていなければならない。また、制御システムは、その時点で展開されているネットワーク及びセキュリティの設定へのインタフェースを提供しなければならない。		<RE1：現在のセキュリティ設定のマシンリーダブルな報告> 制御システムは、現在のセキュリティ設定をマシンリーダブルな形式でリスト化した報告書を生成する機能を備えていなければならない。	
			SR7.8	制御システムのコンポーネントの一覧			<SR：制御システムのコンポーネントの一覧> 制御システムは、インストールされているコンポーネント及びそれらと関連するプロパティの現在のリストを報告できる機能を備えていなければならない。		

J-CLICS設問			J-CLICS設問と関連のある IEC 62443-3-3で定義されている システム要件（SR）		J-CLICS設問とSR の関連の考えかた	IEC 62443-3-3 SR（基本要件）/ RE（強化要件）と SL-C（セキュリティレベル） ※以下の内容は、IEC 62443-3-3原文のSR / RE の全てあるいは一部を、日本電気計測器工業会の責にて翻訳したものです。 翻訳に疑義のある場合は原文にて御確認下さい。			
						SL-C 1	SL-C 2	SL-C 3	SL-C 4
ファイア ウォール	S2_ 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？	SR3.2	悪意のあるコードの防御	本SRの機能は、システム構築する際のネットワーク構成を検討する際に活用でき、制御ネットワークへの不必要な通信の防止に有効です。	（S1_2-1）に同じ	（S1_2-1）に同じ	（S1_2-1）に同じ	
			SR5.1	ネットワーク分割		<SR：ネットワーク分割> 制御システムは、制御システムネットワークと非制御システムネットワーク間及びクリティカルな制御システムネットワークと他の制御システムネットワーク間を論理的に分割できる機能を備えていなければならない。	<RE1：物理的なネットワーク分割> 制御システムは、制御システムネットワークと非制御システムネットワーク間及びクリティカルな制御システムネットワークと非クリティカルな制御システムネットワーク間を物理的に分割できる機能を備えていなければならない。	<RE2：非制御システムネットワークからの独立> 制御システムは、非制御システムネットワークとの接続がなくても、制御システムネットワーク（クリティカル及び非クリティカル）へのネットワークサービスを提供できる機能を備えていなければならない。	<RE3：クリティカルネットワークの論理的及び物理的な絶縁> 制御システムは、クリティカルな制御システムネットワークと非クリティカルな制御システムネットワークを論理的及び物理的に絶縁できる機能を備えていなければならない。
			SR5.2	ゾーン境界保護		<SR：ゾーン境界保護> 制御システムは、リスクベースのゾーン・コンジットモデルで定義された区画を強制するため、ゾーン境界で通信を監視および制御できる機能を備えていなければならない。	<RE1：デフォルトで拒否、例外によって許可> 制御システムは、デフォルトではネットワークトラフィックを拒否し、例外としてネットワークトラフィックを許可する機能を備えていなければならない（deny all, permit by exception とも呼ばれる）。	<RE2：アイランドモード> 制御システムは、制御システムの境界を通過する通信を防止する機能を備えていなければならない（island mode とも呼ばれる）。	<RE3：フェールクローズ> 制御システムは、境界を防御する機能が動作異常となった場合に制御システムの境界を通過する通信を防止する機能を備えていなければならない（fail close とも呼ばれる）。 この’フェールクローズ’機能は、SISまたは他の安全関連機能の動作を干渉しないように設計されなければならない。
システム監視	S2_ 5-1	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？	SR2.8	監査可能なイベント	本SRの機能は、稼働状況およびログを常時取得・保存し、後でそれらを閲覧するための仕組み構築に活用できます。	<SR：監査可能なイベント> 制御システムは、以下の部類に対してセキュリティに関連する監査用記録を生成する機能を備えていなければならない：アクセス制御、リクエストエラー、OSのイベント、制御システムのイベント、バックアップ及びリストアのイベント、設定変更、潜在的な偵察行動、監査ログに関するイベント。 各々の監査用記録は、タイムスタンプ、生成元（発生した機器、ソフトウェアプロセス又は人間のユーザアカウント）、部類、種類、イベントID、イベントの結果を含まなければならない。		<RE1：集中管理されたシステム全体の監査証跡> 制御システムは、監査イベントを集中管理し、また、制御システム全体において複数の機器が生成した監査用記録を編集・加工してシステム全体（物理的または論理的な）において時系列的に関連付けられた監査証跡を生成する機能を備えていなければならない。 制御システムは、これらの監査用記録を、SIEMなど商用のログ分析ツールで分析可能な業界標準の書式で出力する機能を備えていなければならない。	
			SR6.1	監査ログへのアクセス		<SR：監査ログへのアクセス> 制御システムは、権限のある要員及び/又はツールに対して読み出し専用で監査ログにアクセスさせる機能を備えていなければならない。		<RE1：プログラムによる監査ログへのアクセス> 制御システムは、アプリケーション・プログラミング・インタフェース（API）を用いてプログラムから監査ログにアクセスできる機能を備えていなければならない。	
			SR6.2	連続的な監視			<SR：連続的な監視> 制御システムは、セキュリティ侵害を適時に検知、特定及び報告するため、セキュリティ業界で一般的に受け入れられている手法や推奨事項を用いて、全てのセキュリティ機能の性能を継続的に監視する機能を備えていなければならない。		
ウイルス対策	S2_ 6-1	制御システムにウイルス対策を行っていますか？	SR3.2	悪意のあるコードの防御	本SRの機能は、ウイルスの予防・検知・対処などの機能を設ける際に有効です。	（S1_2-1）に同じ	（S1_2-1）に同じ	（S1_2-1）に同じ	
セキュリティ パッチ	S2_ 7-1	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？	SR7.3	制御システムのバックアップ	本SRの機能は、パッチ適用に伴う不具合発生に備えたバックアップ、リカバリおよび再構築に活用できます。	（S1_4-1）に同じ	（S1_4-1）に同じ	（S1_4-1）に同じ	
			SR7.4	制御システムのリカバリと再構築		（S1_4-1）に同じ			
システムの 強化	S2_ 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？	SR7.7	最小機能	本SRの機能は、機能、サービスや通信ポートを必要最小限に制限する上で有効です。	<SR：最小機能> 制御システムは、不要な機能、ポート、プロトコル及び/又はサービスの使用を、具体的に禁止及び/又は制限する機能を備えていなければならない。			
バックアップと 回復	S2_ 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？	SR7.3	制御システムのバックアップ	本SRの機能は、ベンダが推奨する制御システムのバックアップ方法の実施に有効です。	（S1_4-1）に同じ	（S1_4-1）に同じ	（S1_4-1）に同じ	
			SR7.4	制御システムのリカバリと再構築		（S1_4-1）に同じ			