Japan Computer Emergency Response Team
Coordination Center



STEP2

# J-CLICS Check List for Industrial Control Systems of Japan

# 制御システムセキュリティチェックリスト

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点を抽出・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者(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。制御システムやその管理体制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。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で、**何らかの基準や国際標準を保証したり、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 | ○/× | 設問項目ガイド対応ページ |
|---|---|---|---|---|
| | | **システムとビジネスリスクの理解** | | |
| 1 | 1 | 制御システム※1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？ | | P.5 |
| | | **脅威の理解** | | |
| 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※2を把握していますか？ | | P.8 |
| | | **ネットワーク・アーキテクチャ** | | |
| 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※3、接続仕様を把握していますか？ | | P.11 |
| | | **ファイアウォール** | | |
| 4 | 1 | 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設置し、不要な通信を遮断していますか？ | | P.13 |
| | | **システム監視** | | |
| 5 | 1 | 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？ | | P.16 |
| | | **ウイルス対策** | | |
| 6 | 1 | 制御システムにウイルス対策を行っていますか？ | | P.19 |
| | | **セキュリティパッチ** | | |
| 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？ | | P.22 |
| | | **システムの強化** | | |
| 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？ | | P.25 |
| | | **バックアップと回復** | | |
| 9 | 1 | 制御システムの復旧に必要なデータ※6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？ | | P.28 |
| | | **転入者と転出者用のプロセス** | | |
| 10 | 1 | 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？ | | P.31 |

※1 情報資産、ソフトウエア資産、物理的資産を含む
※2 自然災害、火事、盗難による脅威など
※3 発信元、着信先、使用プロトコルなど
※4 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
※5 CPU負荷、ディスク容量管理、システムログなど
※6 パラメータ、操業データなど

SICE The Society of Instrument and Control Engineers JEITA JEMIMA JPCERT CC®