Japan Computer Emergency Response Team
Coordination Center

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。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。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
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
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.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
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、異常時の対応方法を理解し、訓練をしていますか？		P.32
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.36
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.40

*1制御室とは、制御機器または操作端末の設置場所を指します。

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