2017 年 10 月

**制御装置や機械の設計技術者／管理者対象**

# 制御装置や機械製品開発者の制御システムセキュリティ対策の能力を評価するチェックシート

**ICS研究所**

この評価項目は、IEC62443-2 と NIST の Guide to Industry Control System Security 及び NISC の第4次行動計画などを参考に作成しました。

以下の質問に対しての実施評価点数を記入し、その合計点による表の下の判定を参考にしてください。

チェック項目には、

わからない:0、 :1、 知っている:2、 一応できる:3、 自信もってできる:4

で入力してください。

制御装置／機械の制御システムセキュリティ対策能力評価評価チェックシート

| No. | 質問 | チェック |
|---|---|---|
| 1 | 情報セキュリティと制御システムセキュリティの違いを知っている(語れる)。 | |
| 2 | 制御装置／製品をサイバー攻撃する方法を知っている(語れる)。 | |
| 3 | 制御装置／製品を標的にしたサイバー事故をあげて制御セキュリティの必要性を語れる。 | |
| 4 | IEC62443 や NIST の Guide to Industry Control System Security の目的と効果を語れる。 | |
| 5 | 制御装置／製品の脅威についてサイバーリスク特定・評価ができる。 | |
| 6 | 制御装置／製品のサイバーリスク低減対策及び設計改善ができる。 | |
| 7 | 制御装置や機械の構成製品の脆弱性情報を取り寄せて改善できるかどうかを判断できる。 | |
| 8 | サイバーリスクアセスメントの残留リスクの対策を提案できる。 | |
| 9 | セキュリティ5Sを説明できる。(指導できる。) | |
| 10 | 制御装置／製品の開発プロセスに必要なセキュリティ要素をあげて対処ができる。 | |
| 11 | 開発環境のセキュリティ要求仕様作成と管理ができる。 | |
| 12 | ソフト開発及びシステム設計上の脆弱性管理方法を知っている。(できる。指導できる。) | |
| 13 | 制御装置／機械の通信のホワイトリストやマルチタスクのホワイトリストなどの仕様設計・検証ができる。 | |
| 14 | BCP／BCMをベースにしたセグメント設計・各種ゾーン設計ができる。 | |
| 15 | サイバーインシデント検知機能を制御製品に設計・検証できる。 | |
| 16 | サイバーインシデントログ機能を製品に設計・検証ができる。 | |
| 17 | サイバーインシデント対応マニュアルを作成できる。(適合性判断ができる。) | |
| 18 | サイバーインシデント対応のトレーニング計画及び指導ができる。 | |
| 19 | 制御装置／機械の脆弱性(ペネトレーション)テストの試験方案を作成できる。(適合性判断ができる。) | |
| 20 | セキュリティ性能・機能仕様を組み入れて制御製品の基本仕様書を作成できる。 | |
| 21 | 制御装置／機械のセキュリティ性能・機能確認の試験方案を作成できる。(適合性判断ができる。) | |
| 22 | 評価ツールの仕様が対象システムに適合しているかいないかの判断ができること。 | |
| 23 | 主要部品の発注先監査基準を作成し、監査ができる。 | |
| 24 | ベンダの脆弱性情報が対象システムに適応しているかどうかの判断ができる。 | |
| 25 | 人材育成のプログラムに必要となる制御セキュリティプログラムを計画できる。 | |

採点評価

90 点以上:制御セキュリティ対策を施した制御装置／機械を開発できる能力を充分持っています。

70 点以上 : eICS を受講してさらに研修でベテラン域に能力を成長させましょう。

50 点以上 : 研修＋eICS を受講してセキュアな制御装置／機械の開発ができる技術者になりましょう。

50 点未満 : eICS の基礎から始めましょう。

eICS は、産業サイバーセキュリティセンターCoE で教材として採用されている制御システムセキュリティ専門のオンデマンドビデオ講座 e-learning です。ICS 研究所が開発しました。

https://www.ics-lab.com/e