

2017年10月

システム設計及び計装制御技術者／管理者対象

## 制御システム設計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。

### 制御システム設計技術者の制御システムセキュリティ対策能力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	制御システムをサイバー攻撃する代表的な方法を知っている(語れる)。	
3	制御システムを標的にしたサイバー事故をいくつか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	制御システムの機能安全／グループ安全／サイバーリスク特定・評価ができる。	
6	制御システムの機能安全／グループ安全／サイバーリスク低減対策及び設計改善ができる。	
7	制御装置や機械の脆弱性情報を取り寄せてベンダで改善できるかどうかを判断できる。	
8	機能安全／グループ安全／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	システム設計の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	システム設計ネットワーク環境のセキュリティ要求仕様作成と設計と管理ができる。	
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	制御システムセキュリティ用のDMZ／ファイアーウォール／セキュアルータの仕様の違いを語れる。	
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システムに設計できる。	
16	サイバーインシデントログ機能装備のシステム設計ができる。	
17	サイバーインシデント対応マニュアルを作成できる。	
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	システムの脆弱性(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	制御装置や機械の発注仕様書にセキュリティ性能・機能仕様を組み入れて作成できる。	
21	制御装置や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。	
23	制御装置や機械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存在す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な制御セキュリティ要素が入った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システム設計が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できます。

50点以上:研修+eICSを受講して、制御セキュリティ対策ができるシステム設計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>