

## eICS 講座カリキュラム

- ◆管理系および一般社員の方は、下記カリキュラム図の該当するカテゴリを受講して下さい。
- ◆制御システムについて初心者の方には、「初心者のための制御システム講座」から受講して下さい。
- ◆技術者の方は、アセットオーナーから、装置・機械・制御ベンダ及びシステムエンジニアリング会社など関係する相手の役割や機能を知っている必要がありますので、全ての講座を受講して下さい。

経営者	アセットオーナー 技術者・管理者	エンジニアリング会社 技術者・管理者	制御装置ベンダ 技術者・管理者	機械ベンダ 技術者・管理者	制御ベンダ 技術者・管理者
経営講座	アセットオーナー 技術	制御システム エンジニア技術 + システムインテグレータ	制御装置ベンダ における対策	機械ベンダ における対策	制御ベンダ講座
	制御製品開発技術				
ガイドライン 解説	サイバースクアセスメントの手引き + 制御セキュリティとシステム設計				
	セキュリティ製品講座				
	発注・受け入れ・現場立ち上げ				
	安全とセキュリティ				
	認証制度と概要				
	基礎講座 + 国際標準規格 + 初心者の為の制御システム講座				
	最新情報 / トピックス + 用語集				
Industry4.1J/ IoT/CPS					

## eICS 講座一覧 2022年3月現在 253 講座

新たに追加・更新予定の講座を青字(斜体)で記載しています。

Industry4.1J/ IoT・CPS (13 講座)	Industry4.1J/ IoT・CPS (13 講座) 続き
プログラムレス IoT プラットフォーム	サイバー・フィジカル・セキュリティ対策フレームワーク その3
Industry4.1J ソリューション その1	サイバー・フィジカル・セキュリティ対策フレームワーク その4
Industry4.1J ソリューション その2	サイバー・フィジカル・セキュリティ対策フレームワーク その5
Industry4.1J ソリューション その3	<b>最新情報 / トピックス (8 講座)</b>
Industry4.1J ソリューション その4	サイバーセキュリティ法規制の動向 国内外のサイバーセキュリティ法
Industry4.1J 「実証実験報告」	サイバーセキュリティ法規制の動向 重要インフラ
Industry4.0 解説 ドイツ編	サイバーセキュリティ法規制の動向 サイバーセキュリティ経営ガイドライン V2.0
Industry4.0 解説 米国編	産業別サイバーセキュリティの動向 2019年6月制作
サイバー・フィジカル・セキュリティ対策フレームワーク その1	制御システムセキュリティ対策の動向 2019年6月制作
サイバー・フィジカル・セキュリティ対策フレームワーク その2	サイバーセキュリティ最新情報 2022年1月制作
	IoT と制御システムセキュリティ対策
	ICS-CERT 最新情報



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

**基礎講座 (12 講座)**

制御システムセキュリティ対策の全体像と各手法 2016年11月制作  
 制御システムセキュリティ対策の全体像 2016年11月制作  
 情報システムセキュリティと制御システムセキュリティの違い  
 国際標準規格と認証機関  
 認証 CSMS 認証、SSA 認証、EDSA 認証  
 関連法規制について  
 世界の CSS 機関  
 セキュア改善  
 インシデント対応基礎  
 脆弱性情報対応基礎 その1  
 脆弱性情報対応基礎 その2  
 制御システムセキュリティゾーン設計基礎

**用語集 (12 講座)**

用語集「IEC62443 2018年1月制作」  
 用語集「DCS(Distributed Control System)」  
 用語集「インシデント (Incident)」  
 用語集「セキュア改善」  
 用語集「セグメント/ゾーン」  
 用語集「パスワード (Password)」  
 用語集「パッチ処理/オンライン・パッチ処理」  
 用語集「ホワイトリスト方式」  
 用語集「マルウェア」  
 用語集「ログ機能」  
 用語集「DMZ(DeMilitarized Zone)」  
 用語集「IDS / IPS」

**初心者の為の制御システム講座 (3 講座)**

制御システムの種類と規模 その1  
 制御システムの種類と規模 その2  
 業界別法規制

**国際標準規格 (13 講座)**

IEC62443-4-1  
 IEC62443-3-3 Edition1.0 2013-08 その1  
 IEC62443-3-3 Edition1.0 2013-08 その2  
 OPC Classic から OPC UA ができるまで  
 IEC62541 OPC UA の仕様について  
 OPC UA のセキュリティ機能について  
 OPC UA の Pub-Sub 機能について  
 NIST Framework 概要説明  
 【前編】IEC62443 解説 その1  
 【後編】IEC62443 解説 その1  
 【前編】IEC62443 解説 その2  
 【後編】IEC62443 解説 その2  
 IEC62443 と ISA Secure 認証と安全セキュリティ 2018年/2019年の動向

**認証制度と概要 (12 講座)**

テュフズードジャパン社 制御システムセキュリティ (IEC62443) その1  
 テュフズードジャパン社 制御システムセキュリティ (IEC62443) その2  
 認証の目的と期待効果  
 Achilles 認証  
 CSMS 認証  
 CSMS 認証「セキュリティポリシーの策定」  
 【前編】CSMS 認証「現場のセキュリティ対策項目 その1」  
 【後編】CSMS 認証「現場のセキュリティ対策項目 その1」

**認証制度と概要 (12 講座) 続き**

【前編】CSMS 認証「現場のセキュリティ対策項目 その2」  
 【後編】CSMS 認証「現場のセキュリティ対策項目 その2」  
 EDSA 認証  
 SSA 認証

**発注先管理 (3 講座)**

発注先監査  
 監査基準項目と基準  
 関連法規制

**発注・受け入れ・現場立ち上げ (4 講座)**

要求仕様書 その1  
 要求仕様書 その2  
 工場立会試験  
 受け入れ検査

**セキュリティ製品講座 (15 講座)**

アズビルセキュリティフライデー社製品「AS2000」  
 アズビルセキュリティフライデー社製品「VISUACT-V」  
 インテルセキュリティ(マカフィー)社製品  
 「ホワイトリスト製品の役割と導入時の注意事項」  
 インテルセキュリティ(マカフィー)社製品  
 「ログ解析/管理製品の役割と導入に必要な作業」  
 インテルセキュリティ(マカフィー)社製品  
 「ログ解析/管理製品の構築に必要な作業」  
 インテルセキュリティ(マカフィー)社製品  
 「ログ解析/管理製品の運用に必要な作業」  
 日本シノプシス社製品  
 制御システムの脆弱性対策「1. システムに潜む脆弱性」  
 日本シノプシス社製品  
 制御システムの脆弱性対策「2. OSS 利用時のリスク」  
 日本シノプシス社製品  
 制御システムの脆弱性対策「3.OSS 利用時のリスク対策」  
 日本シノプシス社製品  
 制御システムの脆弱性対策「4. 制御システム開発に潜むリスク」  
 日本シノプシス社製品  
 制御システムの脆弱性対策「5. 静的解析によるソースコードレビュー」  
 日本シノプシス社製品  
 制御システムの脆弱性対策「6. 未知の脆弱性」  
 日本シノプシス社製品  
 制御システムの脆弱性対策「7. ファジングテスト」  
 フォーティネットジャパン社製品「FortiGate の活用法 (概要編)」  
 フォーティネットジャパン社製品  
 「FortiGate の活用法 (実践編) ホワイトリスト式 FW の設定方法」

**制御製品開発技術 (22 講座)**

プログラム開発ツールについて 2016年12月制作  
 セキュアコーディングにおけるセキュリティ対策 2016年12月制作  
 PLC Blaster Worm とその対策  
 セキュア製品開発プロセス  
 【前編】セキュア製品開発 その1  
 【後編】セキュア製品開発 その1

**制御製品開発技術 (22 講座) 続き**

- セキュア製品開発 その2
- セキュア評価 その1
- セキュア評価 その2
- 攻撃側の視点と機密情報
- 製品仕様で対策できること その1
- 製品仕様で対策できること その2
- 製品仕様で対策できること その3
- 製品仕様で対策できること その4
- 製品仕様で対策できること その5
- 製品仕様で対策できること その6 (マシン・アーキテクチャー例)
- 製品仕様で対策できること その7 (マシン・アーキテクチャー例)
- 製品仕様で対策できること その8 (ハードウェア設計)
- 脆弱性情報管理 その1
- 脆弱性情報管理 その2
- 脆弱性情報管理 その3
- 設計環境整備と健全性管理

**制御セキュリティとシステム設計 (13 講座)**

- 制御セキュリティ対策があるシステム設計 その1
- 制御セキュリティ対策があるシステム設計 その2
- 制御セキュリティ対策があるシステム設計 その3
- 制御セキュリティ対策があるシステム設計 その4
- 制御セキュリティ対策があるシステム設計 その5
- 制御セキュリティ対策があるシステム設計 その6
- 制御セキュリティ対策があるシステム設計 その7
- 制御システム構成別サイバーリスク分析  
IEC62443 セキュリティレベルベース その1
- 制御システム構成別サイバーリスク分析  
IEC62443 セキュリティレベルベース その2
- 制御装置の振舞い監視/現場工事の注意事項
- 制御システム構成別サイバーリスク分析 その1
- 制御システム構成別サイバーリスク分析 その2
- 制御システム構成別サイバーリスク分析 その3

**制御システムエンジニア技術 (20 講座)**

- セキュアな制御システム設計
- 制御システムのリスクアセスメント その1
- 制御システムのリスクアセスメント その2
- 制御システムのリスクアセスメント その3
- 【前編】セキュアエンジニアリング その1
- 【中編】セキュアエンジニアリング その1
- 【後編】セキュアエンジニアリング その1
- セキュアエンジニアリング その2
- 攻撃側の視点で見た制御システム その1
- 攻撃側の視点で見た制御システム その2
- 制御系統別ゾーン設計
- 生産プロセス別ゾーン設計
- 統括監視制御でのゾーン設計
- 無線通信ゾーン設計
- 【前編】要求仕様書から読み取る範囲
- 【後編】要求仕様書から読み取る範囲
- 見積もり設計でのセキュア仕様
- 試験評価の方法
- 試験方案でのセキュア試験
- 品質保証と顧客サポート

**制御ベンダ講座 (15 講座)**

- 制御ベンダの取り組み その1
- 制御ベンダの取り組み その2
- 脆弱性情報管理 その1
- 脆弱性情報管理 その2
- 脆弱性情報管理 その3
- 設計環境整備と健全性管理
- 【前編】セキュア製品開発 その1
- 【後編】セキュア製品開発 その1
- セキュア製品開発 その2
- セキュア製品開発プロセス
- セキュア評価 その1
- セキュア評価 その2
- 攻撃側の視点と機密情報
- 製品仕様で対策できること その1
- 製品仕様で対策できること その2

**制御装置ベンダにおける対策 (14 講座)**

- 設計仕様で対策できること
- インシデント対応設計
- セキュア製品開発プロセス
- 発注仕様書から納品まで
- セキュア設計技術 その1
- セキュア設計技術 その2
- 設計環境整備と健全化管理
- 品質保証と顧客サポート
- 攻撃側の視点と対策 機密情報
- 試験評価の方法
- リモートサービス
- 脆弱性情報管理 その1
- 脆弱性情報管理 その2
- 脆弱性情報管理 その3

**機械ベンダにおける対策 (14 講座)**

- 攻撃側の視点と対策
- 脆弱性情報管理 その1
- 脆弱性情報管理 その2
- 脆弱性情報管理 その3
- 設計環境整備と健全化管理
- 設計仕様で対策できること
- 試験評価の方法
- セキュア製品開発プロセス
- セキュア設計技術 その1
- セキュア設計技術 その2
- 発注仕様書から納品まで
- 品質保証と顧客サポート
- インシデント対応設計
- リモートサービス

システムインテグレータ (1 講座)

仕様書からの対策範囲設計範囲の読み取り

アセットオーナー技術 (16 講座)

- セキュリティ 5S の事例 一般的セキュリティルール
- セキュリティ 5S の事例 製造現場のセキュリティルール
- セキュリティ 5S プレーンストーミングの進め方
- セキュリティ 5S プレーンストーミング時の参考資料
- セキュリティ 5S の重要性について
- インシデント検知機能の必要性
- セキュリティ 5S の進め方
- セキュリティ 5S の事例 その 1
- セキュリティ 5S の事例 その 2
- セキュア改善
- 現場用セキュリティ製品 その 1
- 現場用セキュリティ製品 その 2
- 現場用セキュリティ製品 その 3
- 【前編】 インシデントフローチャート作成
- 【後編】 インシデントフローチャート作成
- インシデント対応実践・復旧作業

サイバーリスクアセスメントの手引き (18 講座)

- 石油・ガスシステムにおけるサイバーリスクアセスメント事例 その 1
- 石油・ガスシステムにおけるサイバーリスクアセスメント事例 その 2
- 石油・ガスシステムにおけるサイバーリスクアセスメント事例 その 3
- 石油・ガスシステムにおけるサイバーリスクアセスメント事例 その 4
- 石油・ガスシステムにおけるサイバーリスクアセスメント事例 その 5
- 連続制御システムにおけるサイバーリスクアセスメント事例
- バッチ制御システムにおけるサイバーリスクアセスメント事例
- リモートサポートシステムにおけるサイバーリスクアセスメント事例
- 制御システムにおけるサイバーリスクアセスメントの流れ
- 制御システムのサイバーリスク低減
- DCS 制御システムにおけるサイバーリスクについて
- 電力システムにおけるサイバーリスクアセスメント事例 その 1
- 電力システムにおけるサイバーリスクアセスメント事例 その 2
- 電力システムにおけるサイバーリスクアセスメント事例 その 3
- 船舶システムにおけるサイバーリスクアセスメント事例 その 1
- 船舶システムにおけるサイバーリスクアセスメント事例 その 2
- 船舶システムにおけるサイバーリスクアセスメント事例 その 3
- 船舶システムにおけるサイバーリスクアセスメント事例 その 4

サイバーリスクアセスメントの手引き (18 講座) 続き

- Cybersecurity Framework を使ったマネジメントシステム*
- バッチ制御 (化学、醸造) システムにおけるサイバーリスクアセスメント事例*
- 管制システムにおけるサイバーリスクアセスメント事例*
- 医療品製造システムにおけるサイバーリスクアセスメント事例*
- 半導体製造システムにおけるサイバーリスクアセスメント事例*
- 原子力発電所関連におけるサイバーリスクアセスメント事例*
- 自動車製造システムにおけるサイバーリスクアセスメント事例*

安全とセキュリティ (16 講座)

- 安全と制御セキュリティ安全 その 1
- 安全と制御セキュリティ安全 その 2
- 石油・化学業界における事故原因と対策例
- 事故から学ぶ安全とセキュリティ 事故調査報告 その 1
- 事故から学ぶ安全とセキュリティ 事故調査報告 その 2
- 事故から学ぶ安全とセキュリティ 事故調査報告 その 3
- 事故から学ぶ安全とセキュリティ サイバー攻撃で事故は起こせるのか
- 機械安全と制御セキュリティ対策 その 1
- 機械安全と制御セキュリティ対策 その 2
- 機械安全と制御セキュリティ対策 その 3
- 多層防御 (Defense in Depth)
- グループ安全と制御システムセキュリティ対策 その 1
- グループ安全と制御システムセキュリティ対策 その 2
- 機能安全と制御セキュリティ対策 その 1
- 機能安全と制御セキュリティ対策 その 2
- 機能安全と制御セキュリティ対策 その 3

ガイドライン解説 (6 講座)

- IoT セキュリティガイドライン V1.0 概要
- IoT セキュリティガイドライン V1.0 方針 解説
- IoT セキュリティガイドライン V1.0 分析 解説
- IoT セキュリティガイドライン V1.0 設計 解説
- IoT セキュリティガイドライン V1.0 構築・接続 解説
- IoT セキュリティガイドライン V1.0 運用・保守 解説

経営講座 (3 講座)

- BCP / BCM とインシデント対応
- サイバー攻撃対策と操業継続対策
- BCP / BCM と制御システムセキュリティ