研修

1年に一度は最新技術を研修しましょう。

eICSは、1年間235講座以上を何度でも受講できます。

eICSの講師陣

- セキュリティベンダ
  - マカフィー株式会社　サイバー戦略室　シニア　セキュリティ　アドバイザー　佐々木弘志氏
  - 株式会社カスペルスキー　松岡正人氏
  - アズビルセキュリティフライデー株式会社　内田秀和氏
- 株式会社ICS研究所
  - 代表取締役社長　村上正志
    - 公営財団法人日本適合性認定協会JAB　制御システムセキュリティ技術専門家（技術研究組合制御システムセキュリティセンターCSSC認証ラボセンター認証機関をISA Secure認証の認定審査及び試験所審査をする技術専門家）
    - 経済産業省の産業サイバーセキュリティセンターCoEの制御システムセキュリティ技術メンター
    - 日本電気制御機器工業会NECA制御システムセキュリティ研究会顧問
    - OPC Foundation／日本OPC協議会　顧問

講座内容範囲
IEC62443、NIST Guide to Industry Control System Security、Cybersecurity Framework、ISA Secure認証、国際産業別ガイドライン、実際のインシデント対応や対策技術コンサルで得た知見や手法

企業として実現していかなければならない制御システムセキュリティ強化対策講座

実践的オンデマンドビデオ講座eICS

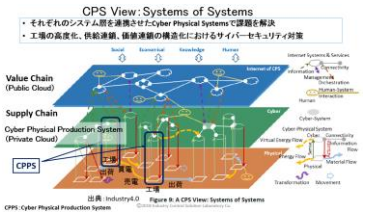
一年間全ての講座を何度も受講できるeICSと「制御システムセキュリティ最前線」の認識が得られる研修と組み合わせたセットで、お一人￥120,000（税抜き）をお勧めします。

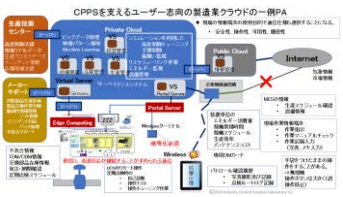
1

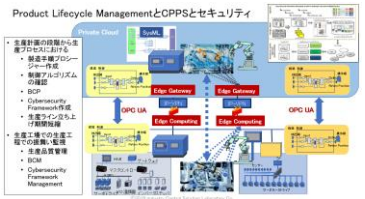
eICSの特徴

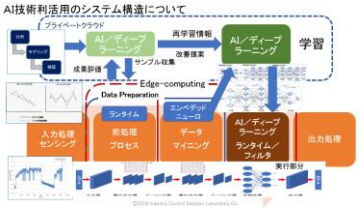
1. **制御システムセキュリティ対策を熟知した講師の徹底解説**
   様々なサイバーインシデント発生現場に呼ばれ対処してきた知見と経験、そして国際規格や産業別ガイドライン等を踏まえた上での解説が講座に反映されています。
2. **全200講座以上を何度でも繰り返し受講可能**
   あなたの仕事で必要な時に必要な講座を受講して下さい。受講期間内であれば全ての講座を何度でも繰り返し視聴可能です。
3. **新たな講座が随時 追加・更新される**
   新たなマルウェアや攻撃手法や対処法に加え、国際規格やガイドラインの情報を収集しています。eICS受講者には常にそれら最新の情報が提供され、追加・更新した講座も繰り返し視聴可能です。
4. **WebブラウザさえあればOK**
   普段お使いのPCやスマートフォン、タブレット端末のWebブラウザさえあれば、余計なソフトをインストールする必要はありません。詳しくは「視聴環境」をご確認下さい。
5. **倍速再生機能で効率よく受講可能**
   1講座あたりの所要時間は15～30分です。例え20分の講座であっても倍速再生機能を使えば、10分で見終わることが出来ます。2倍速の他にも1.75倍や1.5倍速も選択可能です。

2









事業の将来を創造する為にAIを活用したCPPSを実現する為に製造／制御システムセキュリティ対策を実施

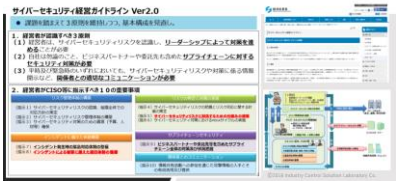
企業の将来の可能性を創り出すセキュアなCPPS

Industry4．1J／IoT・CPS講座

3

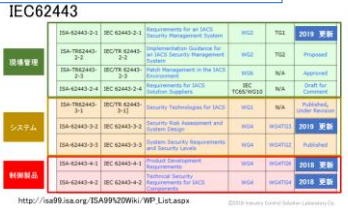
産業別ガイドライン

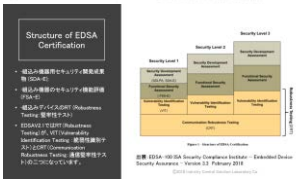
法的規制



EU一般データ保護法
中国サイバーセキュリティ法
米国サイバーセキュリティ法
日本サイバーセキュリティ基本法

国際標準規格／認証制度





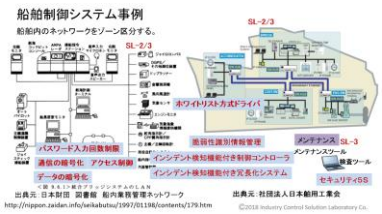
産業別ガイドライン／法規制／国際標準規格／認証制度

最新情報／基礎／国際標準規格／ガイドライン解説の各講座

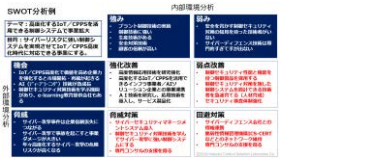
4

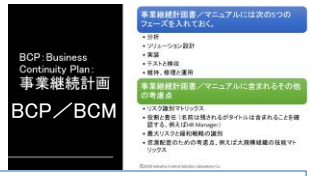
産業別ガイドライン

サイバーリスクアセスメント



マーケティングから事業戦略まで





技術からマネージメントシステムまで

広範囲の産業における制御システムセキュリティ

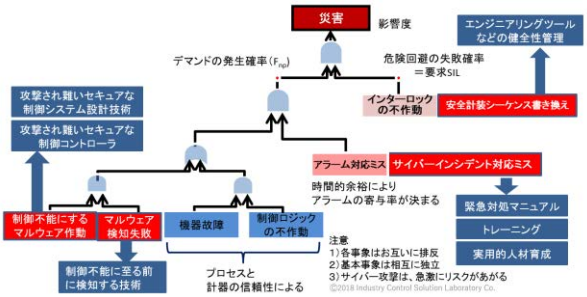
重要インフラ、製造業、航空機、船舶、列車、自動車、医療、放送、家電など

5

制御システムセキュリティリスク低減（対策）実施項目

• 広範囲で深い制御システムセキュリティ対策を体系的に整理

安全のFTA（Fault Tree Analysis）に制御システムセキュリティ・リスクを加える

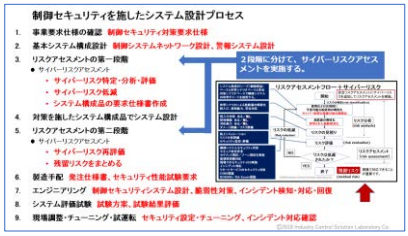


対応する国別法規制、産業別法規制やガイドラインに従って、国際標準規格や認証制度及び対策手法や対策技術の進歩によって変ってくる部分はあるものの、基本的な対策はまず押さえておくことが肝要である。

工場の制御システムセキュリティ対策の全貌

制御システムセキュリティ対策技術や管理方法は、eICSの各講座から学ぶことができる。

6



セキュリティレベルをベースにした
リスクアセスメント

リスクアセスメントIEC62443-3-2

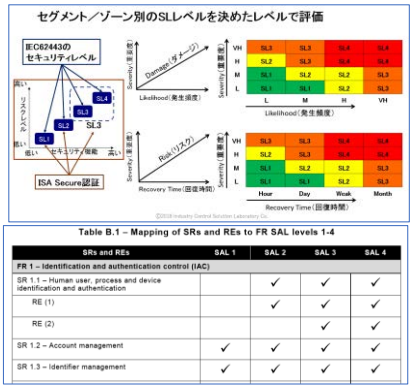


Table B.1 – Mapping of SRs and REs to FR SAL levels 1-4

SRs and REs	SAL 1	SAL 2	SAL 3	SAL 4
FR 1 – Identification and authentication control (IAC)				
SR 1.1 – Human user, process and device identification and authentication		✓	✓	✓
RE (1)		✓	✓	✓
RE (2)			✓	✓
SR 1.2 – Account management	✓	✓	✓	✓
SR 1.3 – Identifier management	✓	✓	✓	✓

セキュリティレベル要件IEC62443-3-3

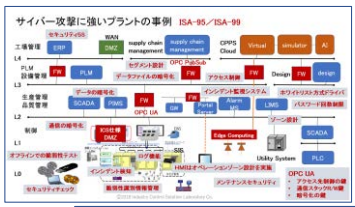
セキュリティ改善計画と管理に実用できる
Cybersecurity Framework

Cybersecurity Framework

世界に通じ、すぐできるリスクアセスメント

制御セキュリティとシステム設計「制御システム構成例とサイバーリスク分析（IEC62443）」講座

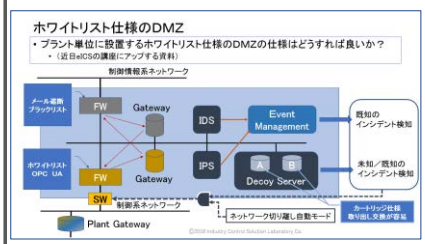
7



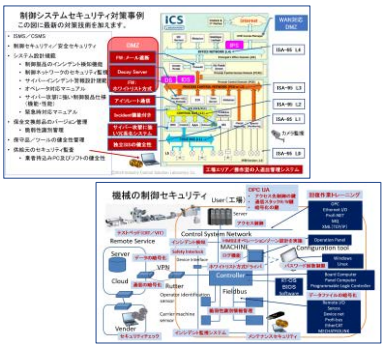
サイバー攻撃に強いISA-95／ISA-99

製造システムを守るDMZ仕様

緊急時対応マニュアル



制御系ネットワーク保護のDMZ仕様



回復時間短縮の仕組み

サイバー攻撃に強い製造システム

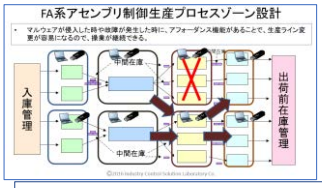
サイバーリスクアセスメントの手引き「制御システムのサイバーリスク低減」講座

8

- ホワイトリストでIDを識別することでマルウェアを排除
  - ソフトウェアにIDをつける
  - データタイプにIDをつける
  - セグメントにIDをつける
  - ゾーンにIDをつける

解析も容易になる

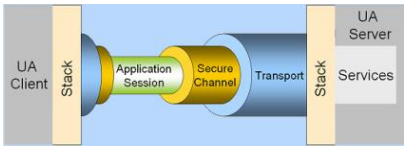
サイバー攻撃に強いアクセス制御



BCP対応セグメント／ゾーン設計

セキュリティ通信の鍵
- **アクセス制御の鍵**
- **通信スタックのR/W鍵**
- **暗号処理の鍵**

分析・監査時を考慮した通信仕様
現場確認作業を考慮した使い勝手仕様

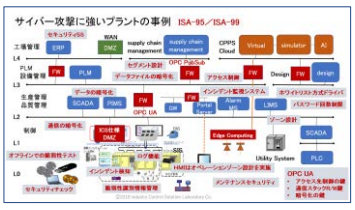


サイバー攻撃に強いOPC UA

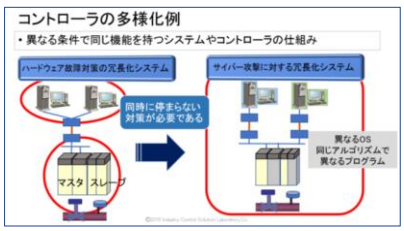
サイバー攻撃に強い製造システムネットワーク

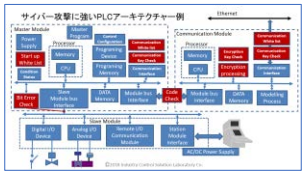
「制御エンジニアリング設計」／「制御製品開発」／国際標準規格「OPC UA」講座

9

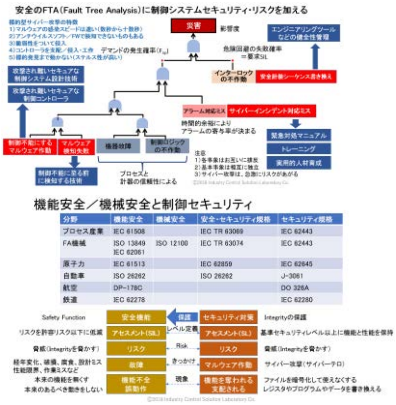


制御システムセキュリティ





制御セキュリティ

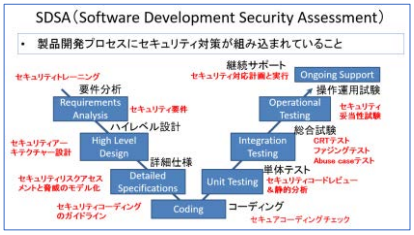


安全セキュリティ

制御セキュリティ／安全セキュリティ

制御セキュリティとシステム設計／制御製品開発技術

10



CRT：Achilles、Defensicsなど

VIT：Nessus

製品開発プロセスで脆弱性識別検証ツールでセキュリティ品質検査実施

脆弱性識別情報管理

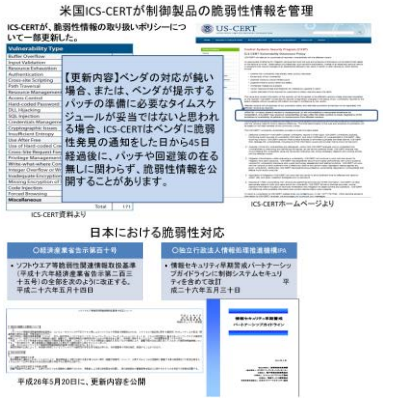
最新のCVE、CWEで検査

脆弱性識別情報管理された製品開発

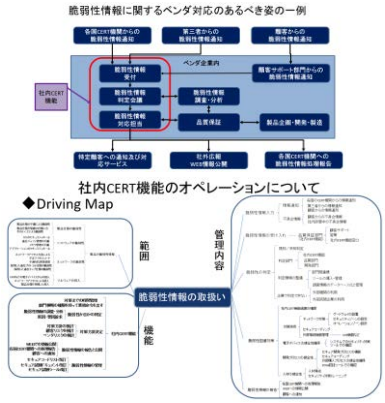
制御製品開発技術の「製品仕様で対策できること」講座

11

米国／日本ICS-CERTの脆弱性情報



脆弱性情報の対応には期限がある。

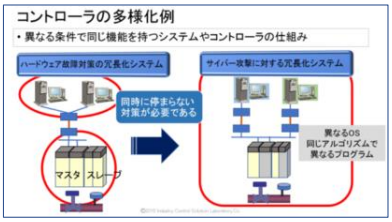


企業内の脆弱性情報の取り組み

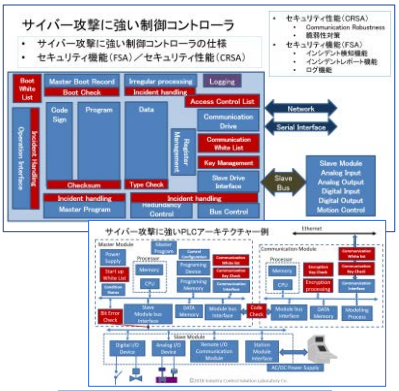
脆弱性識別情報管理

制御ベンダ、制御装置ベンダ、機械ベンダ

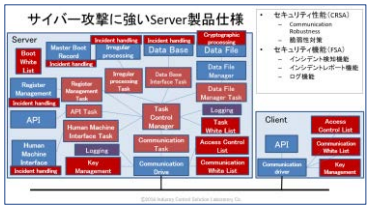
12



サイバー攻撃に強い冗長化



サイバー攻撃に強い
制御コントローラ

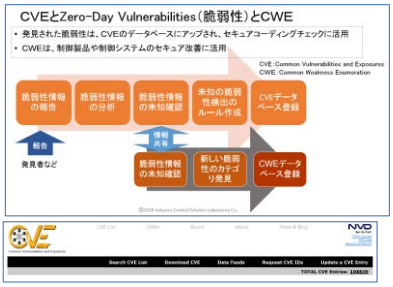


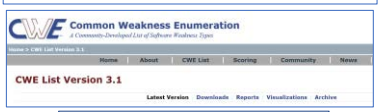
サイバー攻撃に強い
制御Server

サイバー攻撃に強い制御製品

制御製品開発技術「製品仕様で対策できること　その3」講座

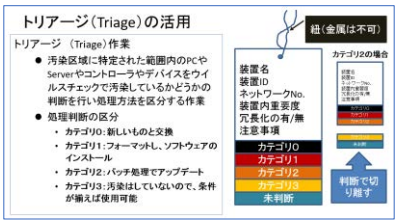
13





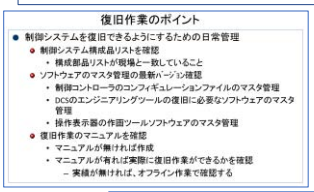
機器別脆弱性識別管理

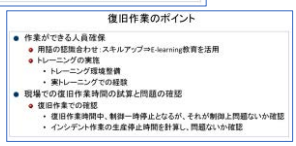
緊急時対応マニュアル



インシデント対応と復旧作業

パッチ処理はオフラインで簡単に





ハードウェア交換でアセット

サイバー攻撃に強い保全管理

「アセットオーナー技術」／「発注先管理」／発注・受け入れ・現場立ち上げ」講座

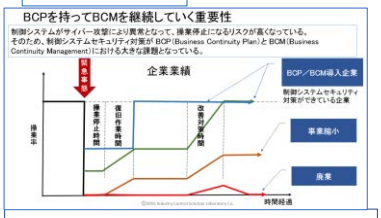
14

サイバー攻撃に脅威

法的規制

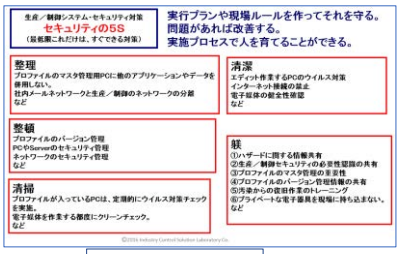
産業別ガイドライン

国際標準規格



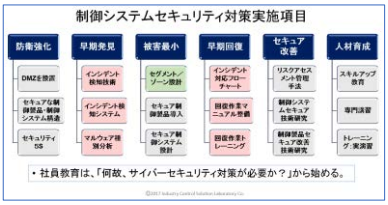
ポリシー／規範／マニュアル整備

サイバー攻撃に強い工場とは何か



セキュリティ5S

全員参加のサイバーセキュリティ



社員教育

サイバー攻撃に強いCSMS

経営講座／「セキュリティ5S」／「アセットオーナー技術」講座

15

損害金額請求範囲特定

法規制
産業別ガイドライン
企業責任

発注仕様書
受け入れ検査
検査ツール指定
立会検査
供給元監査

管理責任：ガバナンス

健康
安全
環境

リスクアセスメント
設備の機器管理リスト
ネットワークリスト
脆弱性識別情報

設備管理側責任

システムインテグレータ

供給元製造

装置ベンダ
機械ベンダ

制御ベンダ

ソフト開発会社

供給側責任

CSMS認証

SSA認証

EDSA認証

SDLA認証

第三者認証機関責任

オーナー企業は、どれをどう選ぶかは、発注側の責任になり、どう求めてどう責任を果たすかが問われる。

損害賠償請求訴訟対策

サイバー攻撃を受けた後の損害賠償請求ができるかどうかは責任範囲を明確にしているかで決まる。
供給責任は、求められたことにどこまで責任を負うかを明確に（第三者認証など）していく必要がある。

16

オンデマンドビデオ講座eICSの活用と効果

eICSを受講しながら、

- **制御システム設計及び制御システム利用における規範作成**
- **業務系ネットワークと製造系ネットワークのセグメント設計防御技術**
- **セキュリティ監視システムの構築設計（SIEMの機能・性能仕様と使い方、アイソレート仕様）**
- **緊急時対応マニュアル作成**
- **被害最小にするセグメント／ゾーン設計**
- **インシデント検知設置及びインシデント警報設計**
- **OT現場従業員セキュリティルールと教育ビデオコンテンツ（ビデオ制作はICS研究所で対応）**
- **制御コントローラに求められる機能・性能仕様、脆弱性情報管理方法**
- **装置・機械発注仕様書のセキュリティ機能・性能仕様**
- **製品開発プロセスにおける脆弱性撲滅方法**
- **試験方案作成など**
- **セキュリティ評価ツール選択基準書作成**
- **サプライヤ企業のセキュリティ監査基準書作成**

などの実務を進める時に必要な知見を取り込んで成果を出していける技術者を育てる。

17