

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라이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でも受講できる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。

©2018 Industry Control Solution Laboratory Co.

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. 倍速再生機能が効率よく受講可能**
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。

ICS ジャーナル

©2018 Industry Control Solution Laboratory Co.

2

CPS View: Systems of Systems

- それぞれのシステム間を連携させたCyber Physical Systemsで課題を解決
- 工場の高次元化、供給連鎖、生産連鎖の構造化におけるサイバーセキュリティ対策

Value Chain (Public Cloud)

Supply Chain (Private Cloud)

Cyber Physical Production System (CPS)

Industry 4.0 Figure 8 A CPS View: Systems of Systems

CPPSを支えるユーザー志向の製造業クラウドの一例PA

PA: 製造現場とクラウド間の接続技術

Private Cloud

Public Cloud

Internet

AI/ディープニューラルネットワーク/ディープラーニング

クラウド(AI(人工知能))を活用

AI技術利活用のシステム構築について

Edge-computing

AI/ディープラーニング

学習

事業の将来を創造する為AIを活用したCPPSを実現する為製造/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

©2018 Industry Control Solution Laboratory Co.

3

産業別ガイドライン

重要インフラにおけるセキュリティガイドライン

電力制御システムセキュリティガイドライン(ICS/SCADA/PLC)

重要インフラにおけるサイバーセキュリティ対策推進ロードマップ(2017年7月)

重要インフラにおける情報セキュリティガイドライン

重要インフラにおける情報セキュリティ(信頼)に係る安全管理

重要インフラにおける情報セキュリティガイドライン(第4版)の動向

重要インフラにおけるセキュリティガイドライン

法的規制

経済産業省「サイバーセキュリティ経営ガイドラインV2.0」

サイバーセキュリティ経営ガイドライン Ver2.0

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

IEC62443

製品管理	システム	制御製品
IEC 62443-2-1	IEC 62443-2-2	IEC 62443-2-3
IEC 62443-2-4	IEC 62443-2-5	IEC 62443-2-6
IEC 62443-2-7	IEC 62443-2-8	IEC 62443-2-9
IEC 62443-2-10	IEC 62443-2-11	IEC 62443-2-12
IEC 62443-2-13	IEC 62443-2-14	IEC 62443-2-15
IEC 62443-2-16	IEC 62443-2-17	IEC 62443-2-18
IEC 62443-2-19	IEC 62443-2-20	IEC 62443-2-21
IEC 62443-2-22	IEC 62443-2-23	IEC 62443-2-24
IEC 62443-2-25	IEC 62443-2-26	IEC 62443-2-27
IEC 62443-2-28	IEC 62443-2-29	IEC 62443-2-30
IEC 62443-2-31	IEC 62443-2-32	IEC 62443-2-33
IEC 62443-2-34	IEC 62443-2-35	IEC 62443-2-36
IEC 62443-2-37	IEC 62443-2-38	IEC 62443-2-39
IEC 62443-2-40	IEC 62443-2-41	IEC 62443-2-42
IEC 62443-2-43	IEC 62443-2-44	IEC 62443-2-45
IEC 62443-2-46	IEC 62443-2-47	IEC 62443-2-48
IEC 62443-2-49	IEC 62443-2-50	IEC 62443-2-51
IEC 62443-2-52	IEC 62443-2-53	IEC 62443-2-54
IEC 62443-2-55	IEC 62443-2-56	IEC 62443-2-57
IEC 62443-2-58	IEC 62443-2-59	IEC 62443-2-60
IEC 62443-2-61	IEC 62443-2-62	IEC 62443-2-63
IEC 62443-2-64	IEC 62443-2-65	IEC 62443-2-66
IEC 62443-2-67	IEC 62443-2-68	IEC 62443-2-69
IEC 62443-2-70	IEC 62443-2-71	IEC 62443-2-72
IEC 62443-2-73	IEC 62443-2-74	IEC 62443-2-75
IEC 62443-2-76	IEC 62443-2-77	IEC 62443-2-78
IEC 62443-2-79	IEC 62443-2-80	IEC 62443-2-81
IEC 62443-2-82	IEC 62443-2-83	IEC 62443-2-84
IEC 62443-2-85	IEC 62443-2-86	IEC 62443-2-87
IEC 62443-2-88	IEC 62443-2-89	IEC 62443-2-90
IEC 62443-2-91	IEC 62443-2-92	IEC 62443-2-93
IEC 62443-2-94	IEC 62443-2-95	IEC 62443-2-96
IEC 62443-2-97	IEC 62443-2-98	IEC 62443-2-99
IEC 62443-2-100	IEC 62443-2-101	IEC 62443-2-102
IEC 62443-2-103	IEC 62443-2-104	IEC 62443-2-105
IEC 62443-2-106	IEC 62443-2-107	IEC 62443-2-108
IEC 62443-2-109	IEC 62443-2-110	IEC 62443-2-111
IEC 62443-2-112	IEC 62443-2-113	IEC 62443-2-114
IEC 62443-2-115	IEC 62443-2-116	IEC 62443-2-117
IEC 62443-2-118	IEC 62443-2-119	IEC 62443-2-120
IEC 62443-2-121	IEC 62443-2-122	IEC 62443-2-123
IEC 62443-2-124	IEC 62443-2-125	IEC 62443-2-126
IEC 62443-2-127	IEC 62443-2-128	IEC 62443-2-129
IEC 62443-2-130	IEC 62443-2-131	IEC 62443-2-132
IEC 62443-2-133	IEC 62443-2-134	IEC 62443-2-135
IEC 62443-2-136	IEC 62443-2-137	IEC 62443-2-138
IEC 62443-2-139	IEC 62443-2-140	IEC 62443-2-141
IEC 62443-2-142	IEC 62443-2-143	IEC 62443-2-144
IEC 62443-2-145	IEC 62443-2-146	IEC 62443-2-147
IEC 62443-2-148	IEC 62443-2-149	IEC 62443-2-150
IEC 62443-2-151	IEC 62443-2-152	IEC 62443-2-153
IEC 62443-2-154	IEC 62443-2-155	IEC 62443-2-156
IEC 62443-2-157	IEC 62443-2-158	IEC 62443-2-159
IEC 62443-2-160	IEC 62443-2-161	IEC 62443-2-162
IEC 62443-2-163	IEC 62443-2-164	IEC 62443-2-165
IEC 62443-2-166	IEC 62443-2-167	IEC 62443-2-168
IEC 62443-2-169	IEC 62443-2-170	IEC 62443-2-171
IEC 62443-2-172	IEC 62443-2-173	IEC 62443-2-174
IEC 62443-2-175	IEC 62443-2-176	IEC 62443-2-177
IEC 62443-2-178	IEC 62443-2-179	IEC 62443-2-180
IEC 62443-2-181	IEC 62443-2-182	IEC 62443-2-183
IEC 62443-2-184	IEC 62443-2-185	IEC 62443-2-186
IEC 62443-2-187	IEC 62443-2-188	IEC 62443-2-189
IEC 62443-2-190	IEC 62443-2-191	IEC 62443-2-192
IEC 62443-2-193	IEC 62443-2-194	IEC 62443-2-195
IEC 62443-2-196	IEC 62443-2-197	IEC 62443-2-198
IEC 62443-2-199	IEC 62443-2-200	IEC 62443-2-201
IEC 62443-2-202	IEC 62443-2-203	IEC 62443-2-204
IEC 62443-2-205	IEC 62443-2-206	IEC 62443-2-207
IEC 62443-2-208	IEC 62443-2-209	IEC 62443-2-210
IEC 62443-2-211	IEC 62443-2-212	IEC 62443-2-213
IEC 62443-2-214	IEC 62443-2-215	IEC 62443-2-216
IEC 62443-2-217	IEC 62443-2-218	IEC 62443-2-219
IEC 62443-2-220	IEC 62443-2-221	IEC 62443-2-222
IEC 62443-2-223	IEC 62443-2-224	IEC 62443-2-225
IEC 62443-2-226	IEC 62443-2-227	IEC 62443-2-228
IEC 62443-2-229	IEC 62443-2-230	IEC 62443-2-231
IEC 62443-2-232	IEC 62443-2-233	IEC 62443-2-234
IEC 62443-2-235	IEC 62443-2-236	IEC 62443-2-237
IEC 62443-2-238	IEC 62443-2-239	IEC 62443-2-240
IEC 62443-2-241	IEC 62443-2-242	IEC 62443-2-243
IEC 62443-2-244	IEC 62443-2-245	IEC 62443-2-246
IEC 62443-2-247	IEC 62443-2-248	IEC 62443-2-249
IEC 62443-2-250	IEC 62443-2-251	IEC 62443-2-252
IEC 62443-2-253	IEC 62443-2-254	IEC 62443-2-255
IEC 62443-2-256	IEC 62443-2-257	IEC 62443-2-258
IEC 62443-2-259	IEC 62443-2-260	IEC 62443-2-261
IEC 62443-2-262	IEC 62443-2-263	IEC 62443-2-264
IEC 62443-2-265	IEC 62443-2-266	IEC 62443-2-267
IEC 62443-2-268	IEC 62443-2-269	IEC 62443-2-270
IEC 62443-2-271	IEC 62443-2-272	IEC 62443-2-273
IEC 62443-2-274	IEC 62443-2-275	IEC 62443-2-276
IEC 62443-2-277	IEC 62443-2-278	IEC 62443-2-279
IEC 62443-2-280	IEC 62443-2-281	IEC 62443-2-282
IEC 62443-2-283	IEC 62443-2-284	IEC 62443-2-285
IEC 62443-2-286	IEC 62443-2-287	IEC 62443-2-288
IEC 62443-2-289	IEC 62443-2-290	IEC 62443-2-291
IEC 62443-2-292	IEC 62443-2-293	IEC 62443-2-294
IEC 62443-2-295	IEC 62443-2-296	IEC 62443-2-297
IEC 62443-2-298	IEC 62443-2-299	IEC 62443-2-300

Structure of IEC 62443 Certification

最新情報/基礎/国際標準規格/ガイドライン解説の各講座

©2018 Industry Control Solution Laboratory Co.

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

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

©2018 Industry Control Solution Laboratory Co.

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

防衛強化	早期発見	被害最小	早期回復	セキュア改善	人材育成
<ul style="list-style-type: none"> プラント単位にDMZを設置 セキュアな制御製品・制御システム構築 セキュリティ5S 	<ul style="list-style-type: none"> インシデント検知技術 インシデント検知システム マルウェア種別分析 	<ul style="list-style-type: none"> セグメント/ゾーン設計 セキュア制御製品導入 セキュア制御システム設計 	<ul style="list-style-type: none"> インシデント対応フローチャート 回復作業書整備 回復作業トレーニング 	<ul style="list-style-type: none"> リスクアセスメント管理手法 制御システムセキュリティ技術研究 制御製品セキュリティ改善技術研究 	<ul style="list-style-type: none"> スキルアップ教育 専門研修 トレーニング: 実演習

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わ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。

©2018 Industry Control Solution Laboratory Co.

6

制御セキュリティを指したシステム設計プロセス

- 事業要件仕様の確認 制御セキュリティ対策要求仕様の抽出
- 基本システム構成設計 制御システムネットワーク設計、制御システム設計
- リスクアセスメントの第一段階
 - サイバーリスクアセスメント
 - サイバーリスク削減
 - システム構成要件の要求仕様書作成
- 対策を施したシステム構成品でシステム設計
- リスクアセスメントの第二段階
 - サイバーリスクアセスメント
 - サイバーリスクの再評価
 - 残存リスクをまとめる
- 緊急手続 緊急応答、セキュリティ対策、性能試験要求
- エンジニアリング 制御セキュリティシステム設計、脆弱性対策、インシデント検知・対応・回復
- システム評価試験 試験方法、試験結果報告
- 現場調整・チューニング・試運転、セキュリティ設定・チューニング、インシデント対応確認

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

セグメント/ゾーン別のSLレベルを決めたレベルで評価

SRs and REs	SAL 1	SAL 2	SAL 3	SAL 4
FR 1 - Identification and authentication (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

Cybersecurity Frameworkを活用したセキュリティ改善

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

©2018 Industry Control Solution Laboratory Co.

7

サイバー攻撃に強いプラントの事例 ISA-95/ISA-99

サイバー攻撃に強い工場組織を使う製造現場の事例 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

ホワイトリスト仕様のDMZ

- プラント単位に設置するホワイトリスト仕様のDMZの仕様はどうすれば良いか？
- (※目次aISの課題にアップする資料)

制御系ネットワーク保護のDMZ仕様

制御システムセキュリティ対策事例

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

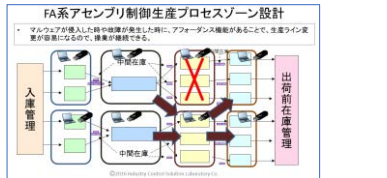
©2018 Industry Control Solution Laboratory Co.

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

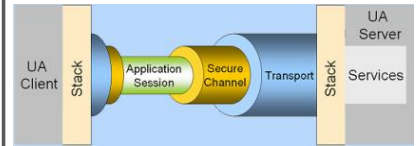
サイバー攻撃に強いアクセス制御



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



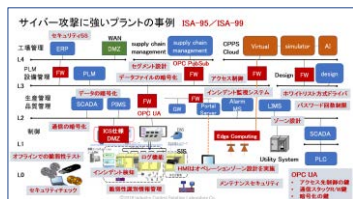
サイバー攻撃に強いOPC UA

サイバー攻撃に強い製造システムネットワーク

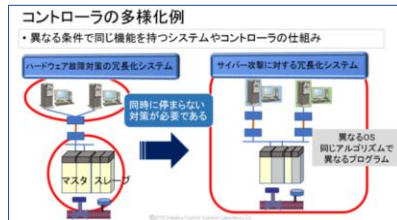
「制御エンジニアリング設計」/「制御製品開発」/国際標準規格「OPC UA」講座

©2018 Industry Control Solution Laboratory Co.

9

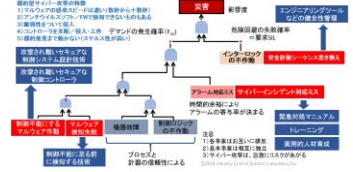


制御システムセキュリティ



制御セキュリティ

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



機能安全/機械安全と制御セキュリティ

分類	機能安全	機械安全	安全-セキュリティ規格	セキュリティ規格
プロセス産業	IEC 61508	IEC TR 63089	IEC TR 63074	IEC 62443
FM機械	ISO 13649	ISO 12108	IEC TR 63074	IEC 62443
原子力	IEC 61513	IEC 62859	ISO 26262	IEC 62443
自動車	ISO 26262	ISO 26262	ISO 26262	J-3081
航空	DO-178C	DO-178C	DO-329A	DO-329A
鉄道	IEC 62278	IEC 62278	IEC 62278	IEC 62278

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

©2018 Industry Control Solution Laboratory Co.

10

SDSA (Software Development Security Assessment)

- 製品開発プロセスにセキュリティ対策が組み込まれていること

セキュリティレビュー、要件分析、ハイレベル設計、詳細仕様、コーディング、単体テスト、統合試験、操作運用試験、脆弱性評価、脆弱性検査、脆弱性評価、脆弱性検査、脆弱性評価、脆弱性検査

制御製品の脆弱性対策

- 製品開発プロセス(モデル)における脆弱性検査を実施
- 装置や機械-ロボットのペネトレーションテスト/システムストレステストを実施

脆弱性識別情報管理

最新のCVE、CWEで検査

製品開発プロセスにおけるCVEとCWEの関係

- 製品開発の中で未知の脆弱性を発見することがある。

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

©2018 Industry Control Solution Laboratory Co.

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

©2018 Industry Control Solution Laboratory Co.

12

コントローラの多様化例

異なる条件で同じ機能を持つシステムやコントローラの仕組み

同時に停まらない対策が必要である

異なるOS 異なアルゴリズムで異なるプログラム

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コントローラの仕様

- サイバー攻撃に強い制御コントローラの仕様
- セキュリティ機能 (FSA) / セキュリティ性能 (CRSA)

セキュリティ性能 (CRSA)

- Communication Reliability
- 脆弱性対策
- セキュリティ機能 (FSA)
- インシデント検知機能
- インシデントレポート機能
- ログ機能

サイバー攻撃に強いServer製品仕様

サイバー攻撃に強いServer製品仕様

セキュリティ性能 (CRSA)

- Communication Reliability
- 脆弱性対策
- セキュリティ機能 (FSA)
- インシデント検知機能
- インシデントレポート機能
- ログ機能

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

©2018 Industry Control Solution Laboratory Co.

13

CVEとZero-Day Vulnerabilities (脆弱性)とCWE

CVEとZero-Day Vulnerabilities (脆弱性)とCWE

- 発見された脆弱性は、CVEのデータベースにアップされ、セキュアコーディングチェックに活用
- CWEは、制御製品や制御システムのセキュリティ改善に活用

緊急時対応マニュアル

緊急時対応マニュアル

トリアージ (Triage) の活用

トリアージ (Triage) 作業

- 汚染区域に特定された範囲内のPCやServerやコントローラやデバイスをウイルススキャンで汚染しているかどうかの判断を行い処理方法を区分する作業
- 処理判断の区分
 - カテゴリ0: 新しいものと交換
 - カテゴリ1: フォーマットし、ソフトウェアのインストール
 - カテゴリ2: バッチ処理でアップデート
 - カテゴリ3: 汚染はしていないので、条件が揃えば使用可能

紐(金風は不可)

装置名	カテゴリ0
装置ID	カテゴリ1
ネットワークNo.	カテゴリ2
装置内重要度	カテゴリ3
冗長化の有/無	未判断
注意事項	未判断

カテゴリ2の場合

利用で切り替える

パッチ処理はオフラインで簡単に

復旧作業のポイント

- 制御システムを復旧できるようにするための日常管理
 - 制御システム構成品リストを把握
 - 構成部品リストが現場と一致していること
 - ソフトウェアの管理の最新バージョン確認
 - 制御コントローラのコンフィギュレーションファイルの管理
 - ICのエンジニアリングファイルの復旧に必要なソフトウェアの管理
 - 操作表示画面の作図ソフトウェアの管理
- 復旧作業のマニュアルを確保
 - マニュアルが揃っていない作成
 - マニュアルが揃えば実際に復旧作業ができることを確認
 - 実績が揃えば、オフライン作業で確認する

復旧作業のポイント

- 作業ができる人員確保
- 用語の理解合わせ: スキルアップやE-learning教育を活用
- トレーニングの確保
- トレーニングでの確認
- 現場での復旧作業時間内の計算と問題の把握
- 復旧作業での確認
 - 復旧作業時間中、制御一時停止となるが、それが制御上問題ないか確認
 - インシデント作業の生産停止時間を計算し、問題ないか確認

機器別脆弱性識別管理

インシデント対応と復旧作業

ハードウェア交換でアセット

サイバー攻撃に強い保安全管理

「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

©2018 Industry Control Solution Laboratory Co.

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

BCPを持ってBGMを継続していく重要性

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

実行プランや現場ルールを作ってそれを守る。問題があれば改善する。実施プロセスで人を育てることができる。

セキュリティ5S

全員参加のサイバーセキュリティ

制御システムセキュリティ対策実施項目

技術強化	早期発見	被害最小	早期回復	セキュリティ改善	人材育成
DMZ構築 セキュリティ脆弱性診断 セキュリティSS	インシデント検知技術 インシデント検知システム マルウェア検出分析	セグメントゾーン設計 セキュリティ脆弱性診断導入 セキュリティ脆弱性診断	インシデント対応フローチャート 回復作業マニュアル整備 回復作業トレーニング	リスク評価 脆弱性評価 セキュリティ脆弱性評価	スキルアップ教育 専門講座 トレーニング実施

・社員教育は、「何故、サイバーセキュリティ対策が必要か？」から始める。

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

©2018 Industry Control Solution Laboratory Co.

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、求められたことにと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。

©2018 Industry Control Solution Laboratory Co.

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。

©2018 Industry Control Solution Laboratory Co.