IPA産業サイバーセキュリティセンター

第2回制御システム向けサイバーセキュリティ演習 in 大阪

NEW

【制御システムのセキュリティに関わる実務担当者の方】

「制御システムのセキュリティ」　備えは進んでいますか

近年は社会インフラや産業基盤に物理的なダメージを与えるサイバー攻撃のリスクが増大しています。既に海外では、サイバー攻撃により社会インフラや産業基盤の安全が脅かされる事案が発生しています。

社会インフラや産業基盤を担う制御システムの重要性は増々高まっており、サイバー攻撃への防護を強化することは喫緊の課題となっています。

大阪で初開催

日　時	2019年9月19日（木）・20日（金）
会　場	TKPガーデンシティ大阪梅田カンファレンスルーム11B 大阪府大阪市福島区福島5-4-21 TKPゲートタワービル11階 https://www.kashikaigishitsu.net/facilitys/gc-osaka-umeda/access/
受講料	1.5日間18万円（税込）
対象者	制御システムのサイバーセキュリティを担当する、又は今後担当を予定している方 （ITパスポート試験合格者相当の知識を有していることを推奨します）

制御システム向けサイバーセキュリティ演習 とは

模擬プロセス制御ネットワークを使用して、機器を不正に制御するサイバー攻撃や対応策による防御を体験でき、制御システムのセキュリティについて理解いただける実践的なコースです。
ITと制御システムのアーキテクチャ、セキュリティ脆弱性、および制御システムに固有の対策等、産業用制御システム（ICS：Industrial Control System）のセキュリティを習得いただけます。

※本演習は、2018年に実施された「ASEAN等向け日米サイバー共同演習*」の内容を改修して開催するものです。

* : https://www.meti.go.jp/press/2018/09/20180914008/20180914008.html

【お問い合わせ先】　独立行政法人情報処理推進機構　産業サイバーセキュリティセンター
Tel:03-5978-7554　E-mail: coe-promotion-info@ipa.go.jp

セミナー・スケジュール

日付	時間	予定
1日目	13:30～13:40	**オープニング** **【シラバス説明】**
	13:40～14:40	**【セッション１】ICS概要** ● ICS*におけるリスクの明確化 *：Industrial Control System ● プロセスコントロールへの脆弱性攻撃デモ
	14:50～15:20	**【セッション２】ネットワーク探索・マッピング** ● 能動的探索ツールの使用 ● 受動的探索ツールの使用
	15:30～17:30	**【セッション３】Metasploitを利用した脆弱性攻撃（ハンズオン）** ● Metasploit解説 ● Metasploit framework利用
2日目	9:30～9:40	**オープニング**
	9:40～11:20 ※途中休憩あり	**【セッション４】ネットワーク攻撃と脆弱性攻撃** ● Webハッキング技術の基礎 ● パスワードセキュリティ攻撃 ● 無線による攻撃と脆弱性攻撃
	11:20～15:00 ※途中昼食休憩あり	**【セッション５】ICSネットワークを越えた横展開** ● ピボッティングと布石 ● Pythonを利用したPLCへの攻撃
	15:10～18:00 ※途中休憩あり	**【セッション６】ネットワーク防御、発見、対応** ● 侵入検知・防御システム ● ICSネットワークにおけるインシデント対応 ● ICS環境におけるレジリエンスとBCP
		クロージング

経験者の声

✓ 演習を通し、実際の制御システムに対する攻撃のイメージを持つことができた。
✓ 演習を通してITとOTはつながっている事が分かって有益だった。
✓ 攻撃の手順についてハンズオンで学ぶ機会は対策を考える上で非常に有用だと思う。

詳細につきましては、下記URLをご参照ください。
https://www.ipa.go.jp/icscoe/program/short/icssec/index.html