2017 年 11 月 29 日

株式会社 ICS 研究所
NTT コミュニケーションズ株式会社
NTT セキュリティ・ジャパン株式会社

ICS 研究所・NTT Com・NTT セキュリティの 3 社が、サイバー攻撃に備えた実践的な IoT セキュリティ対策の体験学習プログラムを開始

～セキュリティ関連技術を保有するベンダー企業の協力により新たなハンズオン環境を実現～

株式会社 ICS 研究所(以下 ICS 研究所)、NTT コミュニケーションズ株式会社(以下 NTT Com) および NTT セキュリティ・ジャパン株式会社(以下 NTT セキュリティ) の 3 社は、製造業やシステムエンジニアリング企業などの、製造／制御システム※1 や各装置の設計・構築・運用を行う技術者を対象に、サイバー攻撃に備えた実践的な IoT セキュリティ体験学習プログラムを 2018 年 2 月 1 日より開始します。なお、本プログラムの受講者と、さらなるベンダー企業の募集を 2017 年 11 月 29 日より開始します。

1. 背景・目的

IoT (Internet of Things) の普及に伴い、企業の基幹業務システムや工場の制御システムなど、重要なインフラ基盤がサイバー攻撃の標的となっています。これにより企業は、システム設計の初期段階からサイバー攻撃に強いシステム構築や、OT(Operation Technology)※2 領域におけるセキュリティ対策が必要です。

しかし、Industry4.0※3 を提唱したドイツなど製造業の IoT 化を推進する主要国と比べ、日本ではセキュアな OT 環境の実現に向けた研究や人材育成の取り組みが遅れていることから、ICS 研究所、NTT Com、NTT セキュリティ の 3 社は、実践的な IoT セキュリティ技術を保有する人材の育成を目指し、「講義形式の学習」と「ハンズオン※4（体験型学習）環境の実習」を同時に受講できるプログラムを、協力ベンダー企業とともに提供します。

2. プログラム概要

製造／制御システムや各装置の設計・構築・運用を行う技術者が日頃抱えている課題を解決するとともに、実践的な IoT セキュリティ人材を育成することを目的に 2 つのプログラムを提供します。

なお、本プログラムは、複数企業のセキュリティ対策製品・技術などを 1 つのハンズオン環境内に実装しており、業界的にも新しい取り組みです。

（1）学習プログラム（有料）※5

E ラーニングおよび講義形式で、サイバー攻撃の脅威を十分に理解するとともに、被害を防ぐためのシステム設計構築方法やインシデント対処方法などを学習できるプログラムです。

（2）技術検証プログラム（無料）

学習プログラムで習得したセキュリティ技術や知識をもとに、実際に業務で利用する製造／制御システムや各装置の一部を用いたハンズオン環境を構築し、今後導入を検討している複数社のセキュリティ対策製品の技術検証や、日頃の課題解決についての体験学習ができるプログラムです。

3．各社の主な役割

・ICS 研究所　　：重要インフラ※6 や工場などで導入されている製造／制御システムの実用的なセキュリティ対策技術、および教育コンテンツなどを提供します。
・NTT Com　　：ハンズオン環境の基盤となるネットワーク・クラウドサービスを提供します。
・NTT セキュリティ：Security Operation Center※7 運営などで培った IT 領域のサイバーセキュリティ対策技術やノウハウ、試験用ツールなどを提供します。

※ハンズオン環境は、3 社で協力して構築します。

4．協力ベンダー企業

セキュリティ対策製品、製造／制御システムを構成する各装置、および試験用ツールなどの提供に協力いただきます。

【現時点での参加予定企業】

・株式会社カスペルスキー
・日本シノプシス合同会社
・アズビル セキュリティフライデー株式会社
・トレンドマイクロ株式会社
・マカフィー株式会社

※さらなる参加をお待ちしております。協力いただけるベンダー企業のみなさまは iot-testbed@ntt.com までご連絡ください。

5．プログラムの開始日程・受講対象者・受講方法

応募開始日程　：2017 年 11 月 29 日
受講開始日程　：2018 年 2 月 1 日（予定）
受講対象者　　：製造／制御システムや各装置の設計・運用・保守に携わる技術者
受講方法　　：以下どちらかより応募ください。
①メール：iot-testbed@ntt.com
②Web　：ICS 研究所 e ラーニング eICS サイト内の「お問合せ」フォーム

6．今後の展開

ICS 研究所、NTT Com、NTT セキュリティの 3 社 は、本プログラムで得た成果・ノウハウを、各社のセキュリティサービス開発・改良に活かしていきます。あわせて、あらゆる業界の企業・団体にも展開することで、共同検討・共同実験などを推進し、ICT を活用した新しいセキュリティソリューションや新サービスの創出を支援するとともに、安心・安全な産業制御システム※8 の実現に貢献していきます。

なお、11 月 29 日（水）から 12 月 1 日（金）に東京ビッグサイトで開催される「計測展 SCF2017」の VEC※9 ブース内にある ICS 研究所のコーナーにおいて、本プログラムを紹介します。

7. 有識者からのコメント

ＶＥＣ会長/東京農工大大学院 教授 山下善之氏

ハンズオンは、学習した知識を実際に活用できるようにするために非常に有効な方法です。今回のプログラムは、サイバーセキュリティ対策技術を製造現場に導入する際に大いに役立つはずです。このような形で、産業界に貢献できる VEC 会員企業同士のコラボレーションが広がっていくことを喜ばしく思います。

名古屋工業大学 社会工学科経営システム分野 教授　橋本芳宏氏

ハンズオンは大変良い取り組みだと思います。私の研究室でも実験装置を使ってサイバー攻撃を体験していただく演習を行っていますが、来られた方はみなさん「話としては知っていても、実際に目にすると理解が進む」と言われます。様々なセキュリティツールを実際に触り、その性能を確認しながら、セキュリティ対策の仕様を検討できるという試みは、たいへん貴重で有用であることは間違いありません。ぜひ、多くの方に体験いただきたいと思います。

株式会社ＩＣＳ研究所代表取締役社長 村上正志氏

製造システムや計装制御プラントのシステム設計の熟練者でも、サイバーリスクアセスメントをベースにシステム設計の仕事をしたことが無いのが現状です。そのため、製造／制御システムのセキュリティ対策技術は、現場の OJT で学ぶことができない対策技術とも言えます。研修や e-learning 教材で知見としては学んでいても、実際に現場の実状に合わせたシステム設計をするのは難しい。そこで今回のハンズオン（体験学習）が誕生しました。これにより、プラントや製造／制御システムのサイバーリスクアセスメントを実証実験の結果をもとに実施できるようになります。

【別紙 1】取り組み概要図
【別紙 2】ハンズオン環境の機器構成と実習内容のイメージ図

※1：製造／制御システムは、企業が、プラント・工場・重要インフラ設備などの操業を計画通りに、管理・制御することを目的に導入する装置群。
※2：OT（Operation Technology）は、システムの運用技術。近年 OT の高度化が IT の発展に欠かせないといわれている。
※3：Industry 4.0 は、ドイツ政府が 2010 年に提唱し、産官学の協力のもと製造業の高度化を推進しているプロジェクト。第四次産業革命の起点とも言われ、その後世界の主要国で、同様の取り組みが広がっている。
※4：ハンズオンは、体験型学習を意味する教育用語。本件では、実際の製造現場と類似する疑似環境において、ネットワークやシステムなどを実際に使い学習することを指す。
※5：ICS 研究所が提供するセミナー研修（講義形式）と eICS（E ラーニング）の学習プログラムセット料金。
※6：重要インフラは、国民生活および社会活動に不可欠なサービスを提供している社会基盤。情報通信/金融/航空/鉄道/電力/ガス/政府・行政サービス/医療/水道/物流の 10 分野が該当する。
※7：Security Operation Center（SOC）は、企業などにおいて、セキュリティ機器やネットワーク機器を監視し、IT システム/OT システムへ忍び寄る脅威の分析やインシデントの発見を行う組織。
※8： 産業制御システムは、重要インフラ・製造業に加え農林水産業も含む産業全体で使用する制御システム。
※9：VEC（Virtual Engineering Community）は、ユーザーニーズ、業界リーダーのシーズ、メーカーの要素技術、エンジニアリング会社の応用技術などを融合し、主に製造業・ビル・エネルギー・電力業界などを対象に、市場動向にマッチする最適なソリューションを展開している任意団体。

【別紙1】取り組み概要図

■プログラム提供者

企画・運営

ICS研究所
・研修プログラムのコーディネート
・制御システムセキュリティ専門技術サポート

NTT Com
・クラウド/ネットワークの提供

NTTセキュリティ
・セキュリティ対策ノウハウの提供
・セキュリティ試験ツールの提供

ハンズオン環境の構築

共同企画

協力ベンダー

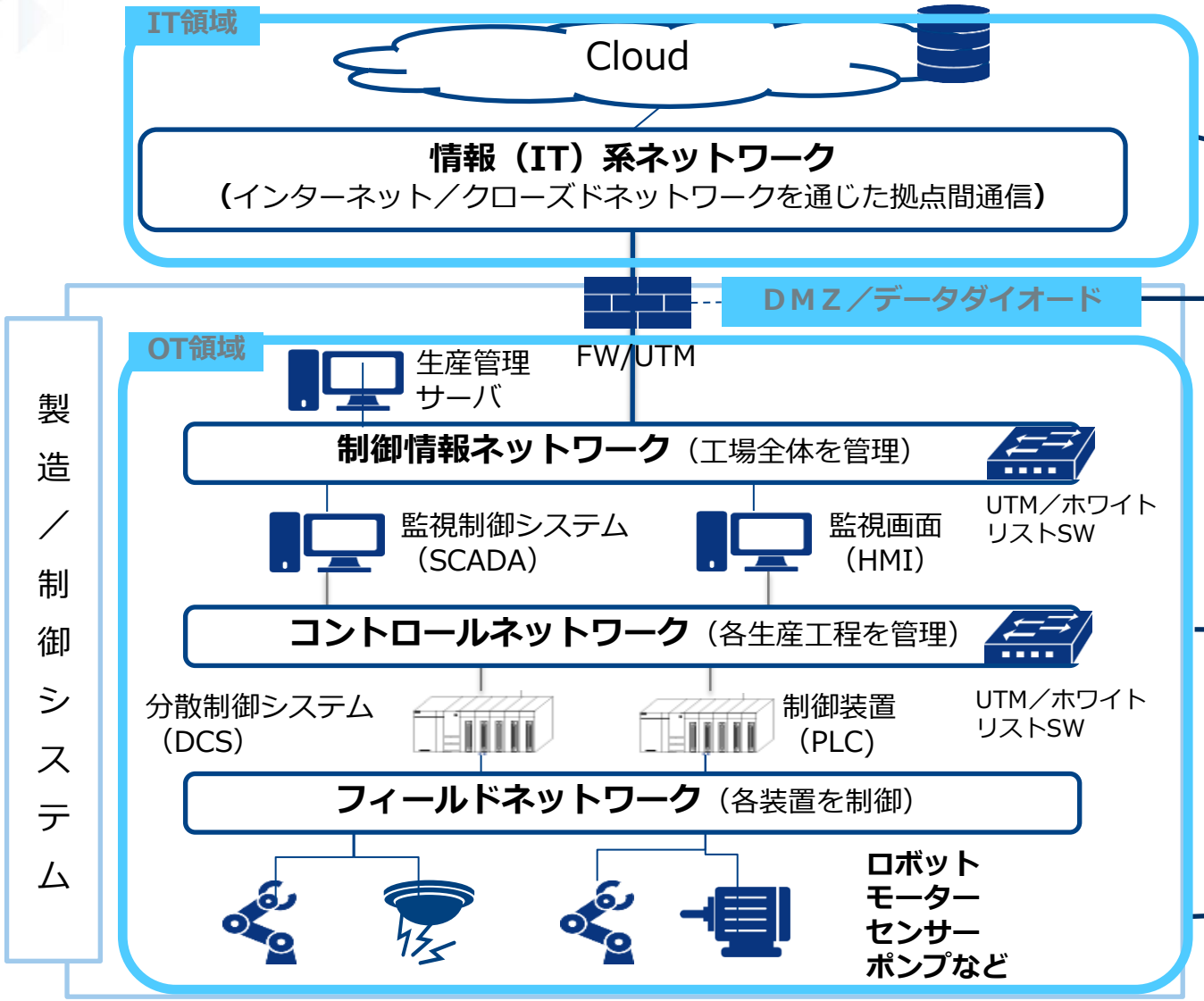
セキュリティベンダー
・セキュリティ対策製品のデモ
・専門技術サポート

計装制御ベンダー
・計装制御装置及び製品のデモ
・専門技術サポート

学習機会の提供

■プログラム受講者
・受講者の課題に応じた技術専門家による研修及びサポート
・ハンズオン（実機を用いた体験学習や実証実験）

【別紙2】
ハンズオン環境の機器構成と実習内容イメージ図



実習できる内容

複数ベンダー企業が提供するセキュリティ脆弱性テストツールを利用

セキュアなネットワーク・システム構成設計、FW/UTM端末の設定/管理方法、異常発生時の通信遮断方法を実習

1. 複数ベンダー製品の性能や操作性を比較
2. サイバー攻撃の発見/初期診断方法を実習
3. サイバー攻撃の防御方法，被災時の応急対処を訓練
4. 各装置をリモート監視

実際に業務で利用する機器を持ち込み、
サイバー攻撃発生時の脆弱性をテスト

FW：ネットワークの境界に設置され許可されていない外部からの通信を遮断する装置。　UTM：複数のセキュリティ機能を統合した装置。
DMZ：外部と内部が直接通信できないようにFWによって隔離されたエリア。　ホワイトリストスイッチ：正常な通信フローを登録しそれ以外の通信を検知する装置。
データダイオード：片方向のみの通信を物理的に許可するもの（ここでは、OT領域からIT領域のみを許可）