

TTCセミナー

事業継続に影響を与え始めた OT (Operational Technology) セキュリティ

TTCセキュリティ専門委員会

委員長

三宅 優

Operational Technology

OTの定義とITとのセキュリティ観点からの違い

- Operational Technologyの定義 (Wikipedia)
 - 物理的な装置や工程を監視・制御するためのハードウェアとソフトウェア技術のことである。例えば、バルブやポンプなど物理的な装置・工程の変化を検出したり引き起こしたりする技術である。
- 制御システムと情報システムにおける情報セキュリティの考え方の違い

	制御システム	情報システム
セキュリティの優先順位	システムが 継続して安全に 稼働できることを重視	情報が適切に管理され、情報漏えいを防ぐことを重視
セキュリティの対象	モノ(設備、製品) サービス(連続稼働)	情報
技術のサポート期間	10年～20年	3～5年
求められる可用性	24時間365日の安定稼働 (再起動は許容されないケースが多い)	再起動は許容範囲のケースが多い
運用管理	現場技術部門	情報システム部門

(IPA産業サイバーセキュリティセンターの資料より)

制御システムの被害例

事例	被害と原因	被害企業
自動車工場 (2005年)	<ul style="list-style-type: none"> 自動車生産50分間停止等、約1,400万ドル（17億円）の損害。 ウイルス感染。外部から持ち込まれて接続されたノートPCの可能性が指摘されている 	ダイムラー
石油パイプライン (2008年)	<ul style="list-style-type: none"> サイバー攻撃により石油パイプラインが爆発した可能性が指摘されている。 監視カメラの脆弱性を利用して侵入し、監視システムと制御系を操作。 	BP (British Petroleum) 運営主体
製鉄所の操業停止	<ul style="list-style-type: none"> 電子メールに添付したマルウェアにより情報を収集してオフィスネットワークに侵入。 不正操作により溶鉱炉を正常に操作できず、生産設備が損傷した。 	ドイツの製鉄所
Stuxnet (2010年)	<ul style="list-style-type: none"> ウラン濃縮用遠心分離機が不正に操作され、8,400台が稼働不能に。 USBメモリを介して制御システムのPCに感染。 	イランの核燃料施設
大停電 (2016年)	<ul style="list-style-type: none"> 電源インフラや送電制御システムなどの重要なインフラシステムで世界的に利用されている4つの産業用通信プロトコルを悪用。 	ウクライナ

(IPA産業サイバーセキュリティセンターの資料より)

本日のセミナーのご紹介

本日のセミナーのプログラム

時間	タイトル	講演者
15:10～ 15:55	レジリエントな組織をつくる 制御システムセキュリティ教育	名古屋工業大学 社会工学専攻 助教 青山 友美 氏
15:55～ 16:40	IoTセキュリティの動向と対策を考える ～CCDS製品分野別セキュリティガイド ラインと共通ガイドラインから～	CCDS代表理事 荻野 司 氏 (CCDS：一般社団法人重 要生活機器連携セキュリ ティ協議会)
16:50～ 17:35	サイバー攻撃被害から学んだ 堅ろう化の取り組み	(株)日立製作所 情報セキュリティリスク 統括本部 サイバーセキュリティ技 術本部 本部長 村山 厚 氏
17:40～	意見交換会	