VLC Security

JNSA WG2
OTサイバーセキュリティ トレーニング　ご紹介

OTサイバーセキュリティ

GoBeyond!

サイバーセキュリティが未来を加速する

"Accelerate the Future with Cyber."

本日のセミナーで理解していただきたいこと

◆ サイバーセキュリティ教育 ➡ 継続的な安全操業を行うための教育

BCP：事業継続計画

単なるITセキュリティの知識の延長では防ぎきれない　工場・発電所・インフラなどの**制御システムを安全かつ安定して稼働させるために、関係者が必要な知識・判断力・行動力を身につける**。

製造現場・OTエンジニアが目の当たりにするインシデントは、**「物理的な機器・装置、作業の安全、周りの環境へ直接的な影響を与える」**ことを理解した上での教育が必要

「工場・プラントなどの生産システム」を守るためには、**実践型トレーニング**で判断力を育てる必要がある。

本講演のゴール：OT攻撃のリアルを理解し、教育の必要性に納得いただく

なぜOTサイバーセキュリティ教育が必要か：
➡ 攻撃が「操業」に直結するため

停止困難

24時間365日稼働、パッチ適用困難、レガシーOS・専用機器が残る。

物理影響

PLC / DCS / SCADAへの攻撃が、停止・品質異常・安全リスクに直結。

即時判断

故障・誤操作・攻撃を短時間で切り分け、対応へ移る必要がある。

部門連携

IT、OT、現場、管理者が共通言語で動く必要がある。

OTでは「監視できたか」だけでなく、操業をどう守るかまでが教育対象になります。

関係者ごとに異なる“守りたいもの”

- 「サイバーセキュリティ」への入り口は、立場によって違う

※関心度は、IPA制御システム関連資料、経済産業省「サイバーセキュリティ経営ガイドライン」、NIST SP 800-82 Rev.3の記述を参考に、研修説明用に整理したもの。

立場	サイバーへの関心	BCP/操業継続への関心	キーワード
IT部門	★★★★★	★★★☆☆	侵入検知・脆弱性
OTエンジニア・保全・生産技術	★★★☆☆	★★★★★	設備の停止・災害復旧
製造現場オペレータ	★★☆☆☆	★★★★☆	操業停止・安全作業
製造管理者	★★★☆☆	★★★★★	納期・採算確保
工場長・経営層	★★★★★	★★★★★	損失・信頼停止

いいかにして、教育を実施させ、操業を維持するか

立場によって、キーワード・行動は異なる

入り口は異なっても、向かうべき全体の目標は同じベクトル

関係者ごとに異なる“守りたいもの”

- 教育の役割：部門ごとの関心を、操業継続という共通言語に変換する。

教育の役割：部門ごとの関心を、操業継続という共通言語に変換する。

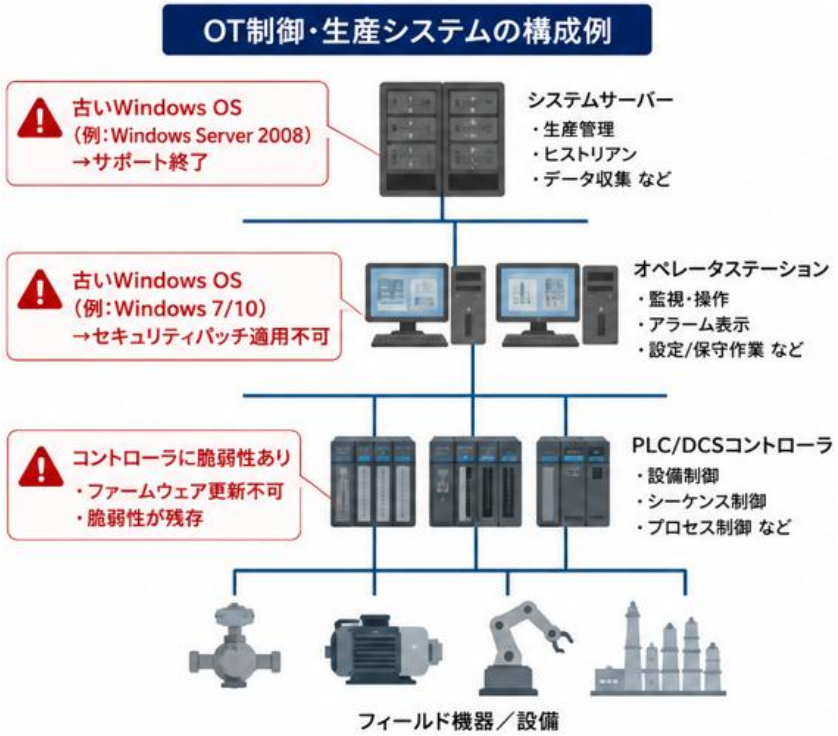
OTセキュリティとITセキュリティの違い

	OT		IT	
用途	製造現場員	製造システム エンジニア	ITシステム エンジニア	一般従業員
一般業務				
仕事環境				
取り扱う機器				

10～20年の使用。特殊な機器を扱う場合が多い　**3～5年で更新・最新OSへのアップデート**

OTシステム：レガシー環境の課題

OTシステムでは長期間の稼働が求められる。OSや機器が旧式のまま運用されています。
そのため、最新のセキュリティパッチ、AV/EDRの導入が困難な状況です。



1. 20年近く稼働する設備・システムが多い
2. Windows OSが旧式で、サポート切れ・更新が困難
3. コントローラ / PLCにも脆弱性が残存
4. セキュリティパッチを適用しにくい
5. 最新のアンチウイルス・EDRを導入しにくい

その結果

従来のITシステムに対するセキュリティ対策だけでは不十分

OTシステムでは、止めずに守るための多重防衛が重要

- 可視化
- 監視
- ネットワーク分離
- 持込機器管理
- 実践型教育・訓練

OT と IT のサイバーセキュリティ教育の違い

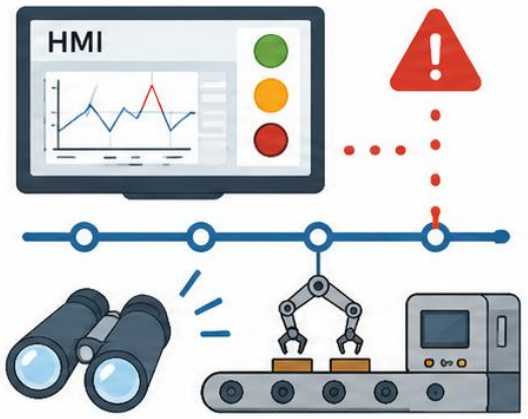
弊社トレーニングの強み

観点	OT （Operational Technology）	IT （Information Technology）
トレーニングの主目的	物理設備・操業の安全確保、停止回避	情報資産の保護、データ漏えい防止
影響範囲	**人命・設備被害・操業停止など重大**	情報漏えい・業務停止・金銭損失
重視される価値	**安全性（Safety）・可用性（Availability）**	機密性（Confidentiality）
対象者	**現場作業員**、保全担当、制御エンジニア、**製造スタッフ**	IT部門、一般社員、管理職など
教育内容の特長	**現場特性（止められない、古い機器、物理安全）を踏まえる**	最新のIT攻撃やツール活用、データ管理が中心
扱う機器	PLC、DCS、SCADA、産業用ネットワーク	PC、サーバ、ネットワーク機器、クラウド
攻撃のイメージ	**物理的破壊・ライン停止・安全装置の無効化**	ウイルス感染、情報漏えい、アカウント侵害
教育手法	**シミュレータ、現場演習、操作訓練**	e-learning、机上演習、ログ分析・技術演習
求められる意識	「操業を止めない」「安全確保が最優先」	「情報を守る」「不正アクセスを防ぐ」
インシデント対応教育	**緊急停止判断、現場での対応手順、物理的安全を伴う**	ログ分析、ネットワーク遮断、情報漏えい対策
制約条件	パッチ適用困難、長寿命機器、24/7運転	比較的頻繁な更新が可能
トレーニング頻度	現場変化が少ないため更新は緩やか（年1回等）	脅威が変化しやすく、頻度高め（定期的）

OT教育で鍛えるべき力：警戒・判断・対応・報告

「技術を知っている」だけではなく、「異常時に迷わず動ける」状態を目指します。

① 警戒



通信、HMI、警報、
設備挙動から異常の
入口を見つける

② 判断

故障・誤操作・攻撃を
切り分け、止める／止めないを
判断する

③ 対応

連絡、影響範囲確認、封じ込め、
機器保護、復旧へ進む

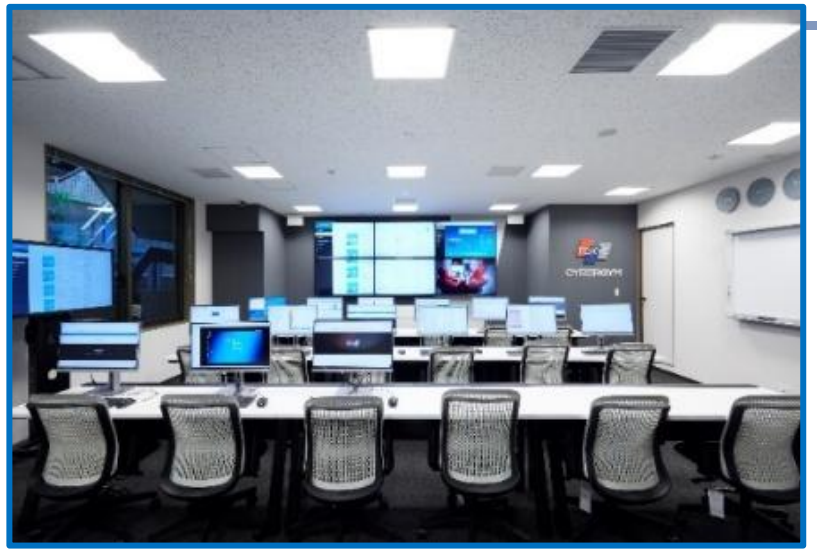
④ 報告

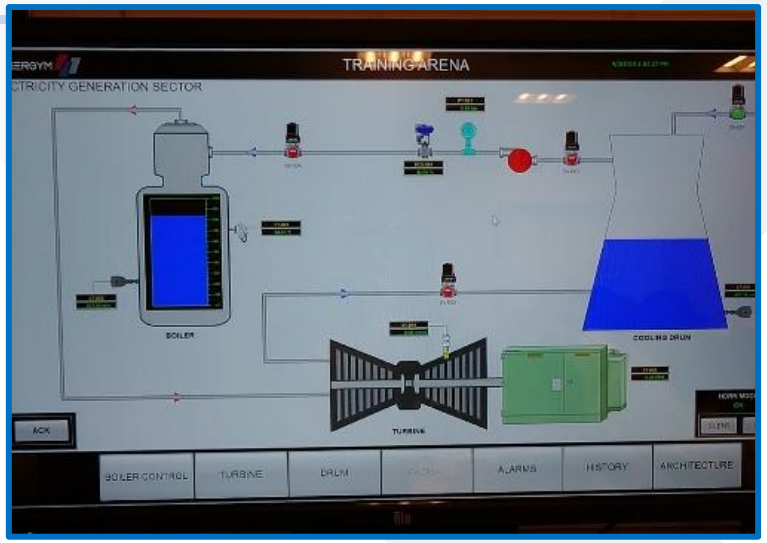
経緯、影響、根因、対処、
再発防止を説明する

最終成果：現場と管理者が共有できるインシデント報告として整理できること

VLCセキュリティアリーナの価値：安全に失敗できる実機訓練環境

- OTエンジニア・製造オペレータ・製造スタッフ・ITエンジニア向けの実践環境





本番環境では試せない

攻撃・停止・復旧を模擬プラント上で安全に再現。

影響を連続で確認できる

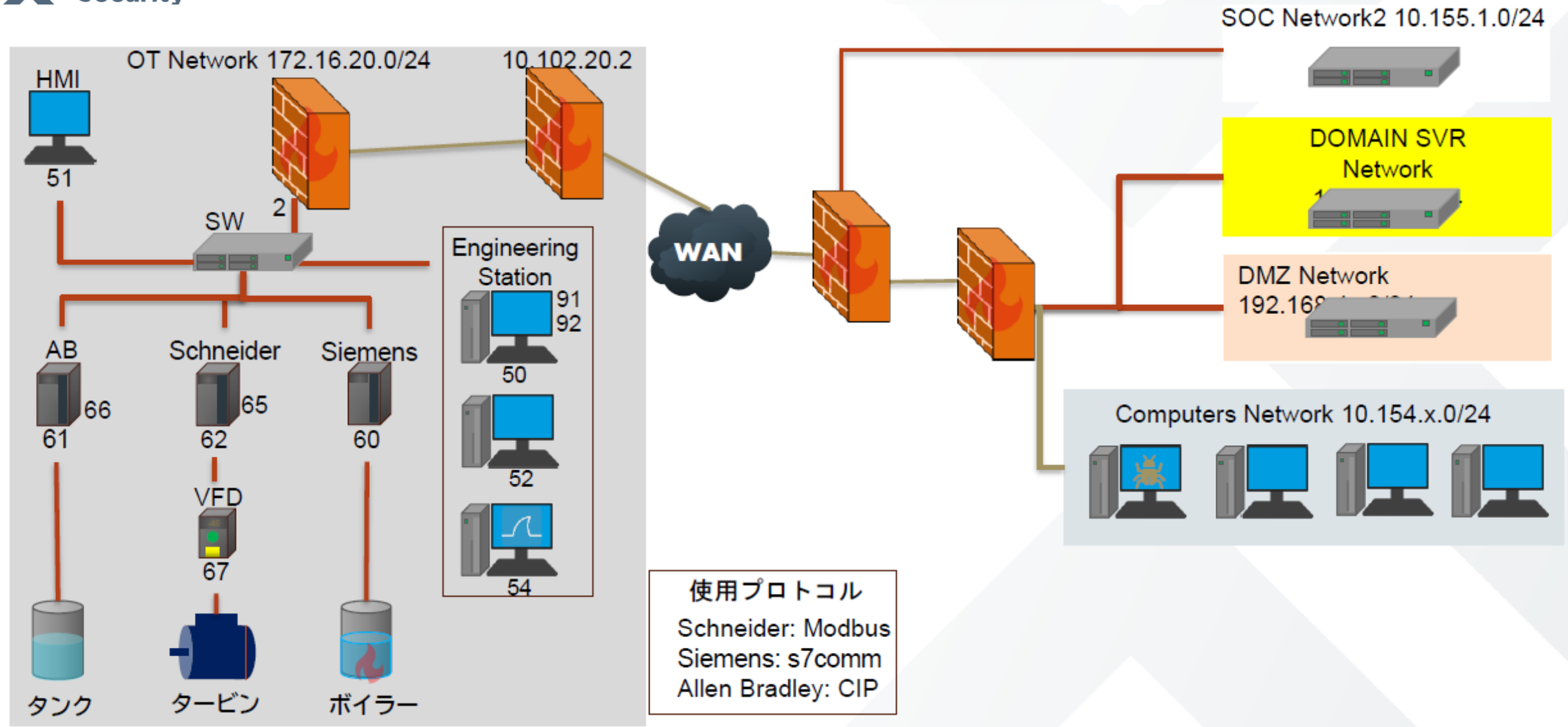
通信ログ、HMI表示、警報、PLC状態、現場装置を関連づける。

判断を反復できる

検知から初動、停止判断、報告、改善までを繰り返す。

実プラントと同じ環境での実践演習。操業に関わる重大な攻撃の体験環境の提供

プラントシステム構成図



OTトレーニング “基礎実践コース”

Day1

Time	Session	Description
10:00 - 10:15	モーニングセッション	・トレーニング確認と進め方について
10:15 - 11:00	産業制御システムの概念 	・ICS基礎やICSでのセキュリティ概要や対策などの基本的なことについて
11:10 - 12:00	**ケーススタディ** 	**・OT分野で実際に発生した脆弱性に対する攻撃や侵入インシデントに関してのケース スタディ（Colonial Pipline、Stuxnet）**
12:00 - 13:00	昼食	昼食休憩
13:00 - 13:20	**Wireshark** 	**・ネットワーク解析ツール「WireShark」の利用方法の解説**
13:20 - 15:20	**Wireshark 演習** 	**・演習用のキャプチャデータを「Wireshark」で解析するハンズオン演習**
15:30 - 16:15	**ICS 攻撃ベクトル** 	**・攻撃者が侵入するまでの流れや手法** **・使用されるプロトコル例（Modbus）**
16:15 - 17:15	**ICS 侵入テスト演習** 	**・Kali Linuxを使用してペネトレーションテスト**
17:15 - 17:30	サマリ	・1日のまとめと質疑応答

Day2

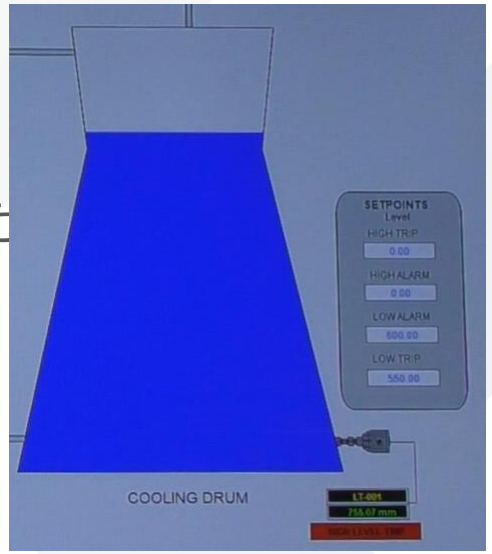
Time	Session	Description
10:00 - 10:05	モーニングセッション	・スケジュール概要
10:05 - 10:25	インシデントレスポンス（初動） 	・インシデント対応プロセスや方法について ・初動対応について
10:25 - 10:45	キックオフ	・アリーナを利用した演習について
10:45 - 11:00	アリーナ環境説明(IT) 	・ITシナリオのトレーニングで利用するアリーナのネットワーク構成やサービス、セキュリティシステム、インフラについて
11:00 - 12:00	**APT演習 (IT)** 	**・ITシナリオデモ**
12:00 - 13:00	昼食	・昼食休憩
13:00 - 14:00	アリーナ環境説明(OT) 	・OTシナリオのトレーニングで利用するOT環境の設備とワークステーションの紹介 ・事前準備時間
14:00 - 16:20	**APT演習 (OT)** 	**・OTシナリオ演習。インシデント検知から伝達、対応、報告**
16:30 - 16:50	インシデント報告 	・OT演習内で取集した方向を元にインシデントの経緯や対処内容、今後の対策などの報告
16:50 - 17:15	演習の振り返り	・OT演習の振り返り
17:15 - 17:30	サマリ	・講習全体の統括と質疑応答

トレーニング演習・実習例

クーリングタワーのレベルアラーム設定変更

- 攻撃の内容
  - クーリングタワーの上限アラーム・トリップ値が「０」に変更されたた
    - レベル異常のアラーム発生（アラーム音の発生）
    - 異常を知らせるパトライトが赤く点滅

    が発生しました。
- 対応処理
  - 以下の作業によりアラームを停止させることができました。
    - 「ACK」キーをクリックし、アラーム音を停止。
    - レベルの「High Trip」値を“850”の初期値へ変更
    - レベルの「HighAlarm」値を“820”の初期値へ変更



クーリングタワーのレベルアラーム設定変更　～攻撃伝文～

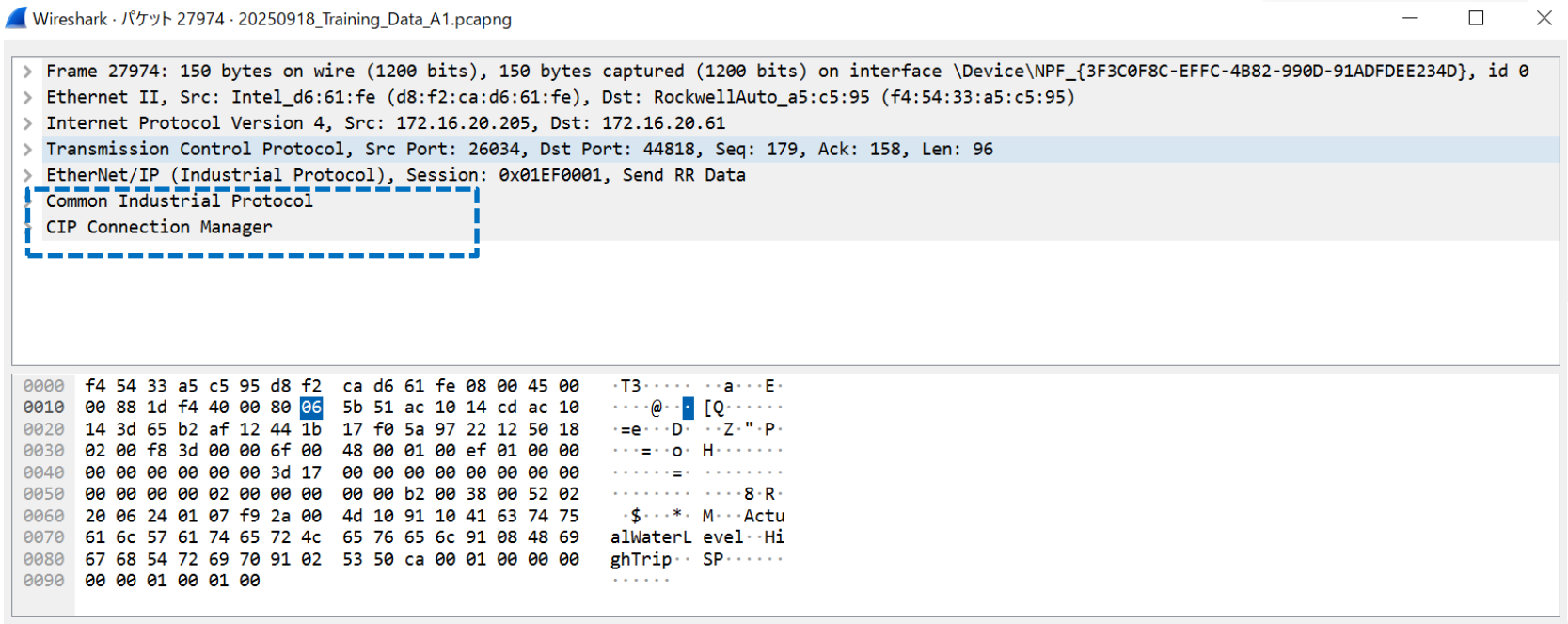
- WireShartkのキャプチャー画面
  - IPアドレス 172.16.20.205から172.16.20.61(Allen Bradley製PLC：タンク制御用)に対し状況確認とデータの書き換えが行われている。(薄緑のライン)
  - IPアドレス205は、ITにより攻撃を受けた制御システムとVPN接続された機器（前列の中畝さんが座っていた席のPCが攻撃に感染され、攻撃の仲介を行っていました。）
  - [ ]で囲まれた部分が実際にデータの書き換えを行っている部分です

Source	Destination	Protocol	Lengtl	Info
172.16.20.51	172.16.20.61	CIP CM	544	Unconnected Send: Multiple Service Packet: Service (0x4c), Service (0x4c), Service (0x4c
172.16.20.61	172.16.20.51	CIP	217	Success: Multiple Service Packet: Service (0x4c), Service (0x4c), Service (0x4c), Service
172.16.20.51	172.16.20.61	CIP CM	178	Unconnected Send: Multiple Service Packet: Service (0x4c), Service (0x4c), Service (0x4c
172.16.20.61	172.16.20.51	CIP	127	Success: Multiple Service Packet: Service (0x4c), Service (0x4c), Service (0x4c)
172.16.20.205	172.16.20.61	CIP CM	114	Unconnected Send: Identity - Get Attributes All
172.16.20.61	172.16.20.205	CIP	127	Success: Identity - Get Attributes All
172.16.20.205	172.16.20.61	CIP CM	144	Connection Manager - Forward Open (Message Router)
172.16.20.61	172.16.20.205	CIP CM	110	Connection failure: Connection Manager - Forward Open (Message Router)
172.16.20.51	172.16.20.61	CIP CM	544	Unconnected Send: Multiple Service Packet: Service (0x4c), Service (0x4c), Service (0x4c
172.16.20.61	172.16.20.51	CIP	217	Success: Multiple Service Packet: Service (0x4c), Service (0x4c), Service (0x4c), Service
172.16.20.51	172.16.20.61	CIP CM	178	Unconnected Send: Multiple Service Packet: Service (0x4c), Service (0x4c), Service (0x4c
172.16.20.61	172.16.20.51	CIP	127	Success: Multiple Service Packet: Service (0x4c), Service (0x4c), Service (0x4c)
172.16.20.205	172.16.20.61	CIP CM	150	Unconnected Send: 'ActualWaterLevel' - 'HighTrip' - 'SP' - Service (0x4d)
172.16.20.61	172.16.20.205	CIP	98	Success: 'ActualWaterLevel' - 'HighTrip' - 'SP' - Service (0x4d)
172.16.20.51	172.16.20.61	CIP CM	124	Unconnected Send: 'LogixTest' - Service (0x4c)
172.16.20.61	172.16.20.51	CIP	100	Path segment error: 'LogixTest' - Service (0x4c)
172.16.20.51	172.16.20.61	CIP CM	544	Unconnected Send: Multiple Service Packet: Service (0x4c), Service (0x4c), Service (0x4c

次ページで解説

クーリングタワーのレベルアラーム設定変更　～攻撃伝文～

- WireShartkのキャプチャー画面
  - 先ほどの　　で囲まれた部分の、WireShark詳細データです。



  - 更に　　で囲まれたCIP通信の部分の詳細を見ていきます。

クーリングタワーのレベルアラーム設定変更　～攻撃伝文～

- WireShartkのキャプチャー画面
  - 先ほどの ⬚ で囲まれた部分の、詳細データ（一部分）です。

```
CIP Connection Manager
  Service: Unconnected Send (Request)
      0... .... = Request/Response: Request (0x0)
      .101 0010 = Service: Unconnected Send (0x52)

  CIP Embedded Message Request
    Common Industrial Protocol
      Service: Unknown Service (0x4d) (Request)
      Request Path Size: 16 words
      Request Path: ActualWaterLevel, HighTrip, SP
        Path Segment: 0x91 (ANSI Extended Symbol Segment)
        Path Segment: 0x91 (ANSI Extended Symbol Segment)
        Path Segment: 0x91 (ANSI Extended Symbol Segment)
    CIP Class Generic
      Command Specific Data
        Data: ca00010000000000
  Route Path Size: 1 word
  Reserved: 0x00
```

このコマンドからPCからPLCに対する要求(Request)とわかります

このCIPメッセージから
ActualWaterLevel.HighTrip.SP という **階層タグを指定(ICSではこの形式でデータの送受信を行う)

詳細

```
Request Path: ActualWaterLevel, HighTrip, SP
  Path Segment: 0x91 (ANSI Extended Symbol Segment)
      100. .... = Path Segment Type: Data Segment (4)
      ...1 0001 = Data Segment Type: ANSI Extended Symbol Segment (17)
      Data Size: 16 bytes
      ANSI Symbol: ActualWaterLevel
  Path Segment: 0x91 (ANSI Extended Symbol Segment)
      100. .... = Path Segment Type: Data Segment (4)
      ...1 0001 = Data Segment Type: ANSI Extended Symbol Segment (17)
      Data Size: 8 bytes
      ANSI Symbol: HighTrip
  Path Segment: 0x91 (ANSI Extended Symbol Segment)
      100. .... = Path Segment Type: Data Segment (4)
      ...1 0001 = Data Segment Type: ANSI Extended Symbol Segment (17)
      Data Size: 2 bytes
      ANSI Symbol: SP
```

らActualWaterLevel.HighTrip.SP への書き込み伝文。
書き込み値は”0”　ca 00 01 00 00 00 00 00：書き込み値

攻撃シナリオ

インシデント対応教育

攻撃1.OTネットワークへの侵入・内部偵察

攻撃2.アラーム設定変更攻撃

攻撃3.コントローラ攻撃

攻撃4.コントローラの強制モードへの変更

攻撃5.タービン回転数のランダム変更攻撃

プラントの操業停止判断

この段階ではOTシステムへの攻撃かどうかわからない
⇒アラームの設定値変更をミスオペレーションと思い込む

この段階で、OTシステムへの攻撃を疑い始める。
⇒ サイバー攻撃の認識し始める。F/Wからシステムの切り離しの検討

攻撃者は任務遂行(発電設備の破壊と操業停止)へ到達
OTシステム内のネットワーク上の機器からの攻撃に変更されている。
⇒ 機器の保護、早期の復旧対応のため、発電を停止し、システムの攻撃対応・攻撃者の侵入遮断

システムにネットワーク防御機器があったら

攻撃1.OTネットワークへの侵入・内部偵察

攻撃2.アラーム設定変更攻撃

攻撃3.コントローラ攻撃

攻撃4.コントローラの強制モードへの変更

攻撃5.タービン回転数のランダム変更攻撃

プラントの操業停止判断

NOZOMI/TXOneのようなツールを産業向け制御システムに導入したら、

- どこまでの攻撃を防げるのか
- 不審な電文を検知できるのか
- プラントへの攻撃を防げるのか

を、模擬プラントで検証したい。

受講対象者

OTトレーニングのターゲット受講者層

	経営者層（経営者・役員）	部長・課長マネージャー層	**OTエンジニア（制御システム担当者・保全技術者）**	**ITエンジニア（情報システム部門）**	**現場作業員・オペレーター**	**サプライヤー・協力会社**
目的	全社的なリスク理解と意思決定能力の向上させる	現場のセキュリティ運用と人員管理を適切に行う	設備の安全/安定運用を維持するためのセキュリティ知識を習得する	OT/ITをまたぐセキュリティ運用を理解し強化させる	日常業務の中で安全に設備を操作し、ヒューマンエラーを防ぐ	外部の出入りが多いOTでのリスク削減
教育内容	OT・IT サイバーリスクの全体像 経営責任（ガバナンス、法規制、NIST/IEC62443など） サイバー攻撃が操業・財務に与えるインパクト 投資判断（セキュリティ投資、BCP、DR対策） 重大インシデント発生時の意思決定シナリオ演習（テーブルトップ演習）	組織のセキュリティ方針と統制の理解 OT/ITのリスク管理、優先度の付け方 プロジェクト管理におけるセキュリティ要求事項の組み込み 部下のセキュリティ意識管理 インシデント発生時の指揮・連絡体制 企業全体のセキュリティ文化（Security Culture）醸成の方法	OT特有の脅威（PLC改ざん、SCADA侵入、USB感染など） 物理安全とサイバー安全の統合(Safety x Security) ネットワーク基礎（産業プロトコル：Modbus、OPC-UAなど） セキュリティパッチ管理方法とリスク評価 リモートアクセス管理 異常検知・ログ確認の基礎 **現場での判断・緊急対応訓練**	最新のIT攻撃手法（フィッシング、マルウェア、ゼロデイ） アクセス制御、ID管理（IAM/ゼロトラスト） ネットワークセグメンテーション クラウドセキュリティ（SaaS/IaaS） SOC/ログ分析、脅威ハンティング OT環境との接点における注意点	ルール遵守の重要性（USB禁止、未承認機器持ち込み禁止） 不審動作・異常の早期発見 SCADA・HMIの操作時の注意 社外業者対応（ゲート管理、立ち入り管理） 緊急時のエスカレーション手順 **実機・シミュレータによる現場訓練**	現場安全教育（Safety & Security） 持ち込み機器の管理（ウイルスチェック・承認制） VPN・リモート作業手順 作業記録・アクセスログ管理 工場での行動規範

本日のセミナーで理解していただけたでしょうか？

◆ サイバーセキュリティ教育 ➡ 継続的な安全操業を行うための教育

BCP：事業継続計画

単なるITセキュリティの知識の延長では防ぎきれない　工場・発電所・インフラなどの**制御システムを安全かつ安定して稼働させるために、関係者が必要な知識・判断力・行動力を身につける**。

製造現場・OTエンジニアが目の当たりにするインシデントは、「**物理的な機器・装置、作業の安全、周りの環境へ直接的な影響を与える**」ことを理解した上での教育が必要

「工場・プラントなどの生産システム」を守るためには、**実践型トレーニング**で判断力を育てる必要がある。

ご質問は？

株式会社VLCセキュリティ

〒105-0001
東京都港区虎ノ門 4 丁目 1-40 江戸見坂森ビル

https://vlcsecurity.com/