

# 第129回 維持管理研究会 議事録

- 開催日時：2022年5月19日(木) 16:00~17:30
- 場所：Zoomリモート開催
- 出席者(敬称略) 21名

小田、上辻、大下、大島、熊澤、坂本、澤田、柴田、守護、日向、柳本、山下、中谷  
 地域勉強会他：萩原、柳父、中村、松本、大塚、野原、堀、加藤

## 4. 研究テーマ

今月は交通・電気・水道といった社会インフラを機能させるために必要な設備やシステムを最適に動かすための制御技術・運用技術であり、私企業においては事業活動を行う上で必要となる機器制御する技術であるOT(Operational Technology)の特徴とサイバーセキュリティについて情報提供を行い、メンバー間で情報交換を行った。

### ITとOTとは

**IT(Information Technology)**  
 コンピュータやデータ通信に関する技術の総称です。仕事や生活に役立つコンピュータやインターネットを使用した技術を指すことが多い。会社ではメール、グループウェア、経理などのコーポレート部門のシステムなどを指す。

**OT(Operational Technology)**  
 交通・電気・水道といった社会インフラを機能させるために必要な設備やシステムを最適に動かすための制御技術・運用技術。製造業においてICS(Industrial Control Systems)と呼ばれる産業用制御システムを動かす制御技術が、このOTに当たる。

(参考) 政府、22年度より重要インフラ事業者にサイバー防衛義務付け

**日本経済新聞**

重要インフラ、企業にサイバー防衛義務付け 22年度から  
 経理システムの脆弱性診断、脆弱性診断実施

政府は情報通信や電力など14分野の重要インフラ事業者にサイバー攻撃への備えを義務付ける。経理システムの脆弱性診断の義務付けも定める。サイバーセキュリティ(防衛)で使用する機器の安全確保も求める。2022年度中に必要な重要インフラ事業者に義務付ける。

### ITとの違い

- OTはITと同じセキュリティ対策が使えない。
- 現場は設備の寿命が長い=不随する制御機器(PCなど)も古い

20年モノ  
30年モノの  
設備がざらにある

OTに対するセキュリティ対策

- OTセキュリティの特徴
- ⇒ゼロトラストなど通常のネットワーク等で採用する対策が取れない
- ネットワーク上のふるまいを観察し、異常な動きを検知して対応

異常なふるまい例	従来の目的
特定機器がSearchを実施	重要データの保護
通常データを取り扱えない機器での通信が発生	他の機器への攻撃実施
大量データの発生	重要情報の窃取

### 30年前はどういう時代

- 2022年⇒1992年
- Microsoft Windows3.1、Windows NTは93年発売(それ以前はMS-DOS、もっと前だとCP/M)

「OT/IoT IDS(侵入検知システム)と呼ばれる」

OT/IoT IDSは、OT/IoTネットワークに接続するデバイス(物理または仮想)の挙動を監視し、正常な動作からの変動を検出する。人工知能を用いた機械学習技術を使用し、デバイス状態に応じたすべてのデバイスの正常な動作パターンを学習し、リアルタイムに異常な動作を検出する。資産管理、ネットワーク可視化、脆弱性評価、ICSへの異常検知、コーポレートレベルへの対応を提供する。

### OT/IoT IDS(侵入検知システム)と呼ばれる

- OT/IoT IDS(侵入検知システム)と呼ばれる
- OT機器やネットワークに影響を与えずにネットワーク構成を把握することが可能

NOZIMI NETWORKS社「Guardian」の場合

- 受動的かつ非侵入的に産業用ネットワークに接続するアプリケーション(物理または仮想)
- コントロールプレーンに接続するすべてのトラフィックを監視し、すべてのレベル(OSIレベル)を実体的に分析
- 人工知能を用いた機械学習技術を使用し、デバイス状態に応じたすべてのデバイスの正常な動作パターンを学習し、リアルタイムに異常な動作を検出する
- 資産管理、ネットワーク可視化、脆弱性評価、ICSへの異常検知、コーポレートレベルへの対応を提供

### ふるまい検知ツール導入の目的

- 目的1：OTネットワークの可視化
  - OTネットワークにふるまい検知ツールを導入し、各機器の通信を検知(ただし1週間、長い場合は1ヶ月間の場合もある)
  - 何がどのようになっているかを明確にし、リスクアセスメントに必要なOTネットワーク構成図と機器一覧表(インベントリリスト)作成のための基本情報を入力
- 目的2：異常なふるまいの検知
  - 各機器間の通信の異常なふるまいを監視
  - ⇒目的1の状況ツールに登録し、現状の通信と比較し、異常があればツールが検知
  - ※24時間365日の監視体制が必要

### ふるまい検知ツールの主な機能

- OT/IoT IDS(侵入検知システム)と呼ばれる
- OT機器やネットワークに影響を与えずにネットワーク構成を把握することが可能

NOZIMI NETWORKS社「Guardian」の場合

- 受動的かつ非侵入的に産業用ネットワークに接続するアプリケーション(物理または仮想)
- コントロールプレーンに接続するすべてのトラフィックを監視し、すべてのレベル(OSIレベル)を実体的に分析
- 人工知能を用いた機械学習技術を使用し、デバイス状態に応じたすべてのデバイスの正常な動作パターンを学習し、リアルタイムに異常な動作を検出する
- 資産管理、ネットワーク可視化、脆弱性評価、ICSへの異常検知、コーポレートレベルへの対応を提供

### ふるまい検知ツールの機能例

NOZIMI NETWORKS社「Guardian」の場合

- 資産の可視化とネットワーク通信の可視化
- 脆弱性アセスメント
- リアルタイムモニタリング
- 異常と監視の検出(ハイブリッド自覚検知)
- DPI: パケットペイロードから通信のやり取りまで把握

### OT可視化後の対応

OT可視化後は次の4STEPでセキュリティ対応を実施(PN: 脆弱性診断システム/脆弱性診断システム/脆弱性診断システム)

**OT可視化**

- 第1STEP: システム構成とデータフローの明確化
- 第2STEP: リスク分析の各評価指標とリスク分析の結果の決定
- 第3STEP: リスク分析の実施
- 第4STEP: 対策の検討と実施の優先順位付け

常時監視の実施

### 第1STEP: システム構成とデータフローの明確化

システム構成とデータフローの明確化を行うステップ。保護すべき資産やそこで行われる処理機能やデータフロー等、リスク分析する対象を明確化して以下のアウトプットを作成

- 資産一覧(資産種別、資産の機能等、資産の取り込み)
- システム構成図(ネットワーク構成、資産配置)
- データフローマトリクス、データフロー図(プロセス値、コマンドフロー等)

### 第2STEP: リスク分析の各評価指標とリスク分析の結果の決定

第一ステップで明確化した保護対象に対して、リスク分析を行うための各評価指標と、リスク分析の結果として得られるリスク値を決定するステップ。一部の評価指標やその評価値の判断基準について、事業者自身が定義すると共に、その評価値を決定する。

- リスク値とその算定
- 資産の重要度
- 事業被害と事業被害レベル
- 脅威と脅威レベル
- 脆弱性及び脆弱性レベル、セキュリティ対策状況と対策レベル

### 第3STEP: リスク分析の実施

各保護対象に対してリスク分析を実施  
 リスク分析手法として以下の2種類がある  
 →どちらか一方を実施すればOK

- 資産ベースのリスク分析
- 事業被害ベースのリスク分析

リスク分析手法と評価指標の関係

リスク分析手法	資産の重要度	事業被害	脅威	脆弱性
資産ベースのリスク分析	○	○	○	○
事業被害ベースのリスク分析	○	○	○	○

### 資産ベースのリスク分析

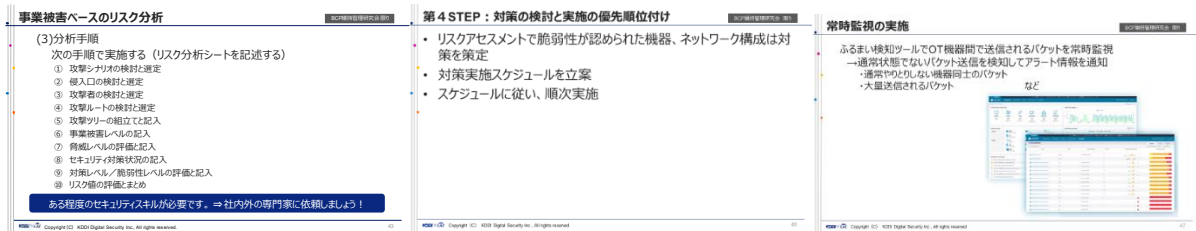
資産ベースのリスク分析は以下の手順で実施する

- 制御システムを構成する装置及び各装置を接続しているネットワーク等のシステム資産、情報資産の列挙とその重要度の決定
- 当該資産に想定される脅威(攻撃手法)とそれぞれの脅威(攻撃手法)の対策候補の記入
- 実際実施している対策状況の記入
- 対策レベル及び脆弱性レベルの評価
- 脅威、脆弱性、重要度よりリスク値の算定

### 事業被害ベースのリスク分析

事業被害ベースのリスク分析は以下の手順で実施する

- (1)分析要素と全体像
  - 攻撃手法(攻撃手法)の商業的攻撃用途「監視」、「攻撃シナリオ」、「攻撃ツール」「攻撃ツール」
  - 攻撃手法(攻撃手法)の分析要素と合わせて分析
  - 攻撃手法(攻撃手法)の分析要素と合わせて分析
  - 攻撃手法(攻撃手法)の分析要素と合わせて分析
- (2)分析対象の選定
  - 全ての分析は出来れば、攻撃手法(攻撃手法)の商業的攻撃用途が大きい、攻撃手法(攻撃手法)の商業的攻撃用途が大きい、攻撃手法(攻撃手法)の商業的攻撃用途が大きい
  - 攻撃手法(攻撃手法)の商業的攻撃用途が大きい、攻撃手法(攻撃手法)の商業的攻撃用途が大きい、攻撃手法(攻撃手法)の商業的攻撃用途が大きい



## 5. 所見

ITサイバー攻撃に関する最新情報、及び馴染みの薄い「OTセキュリティ」の基本的な考え方や対策手段について良く理解することができた。また更新不可能なPCで稼働している生産ラインの設備があることが理解できたので、今後の重要課題として社内で検討を進めたい等の意見も頂いた。

サイバー攻撃による情報システムの全面停止は、社内のみならず顧客に大きな影響を与えるので、IT部門のみに任せるのではなく、全社で訓練等を行い継続的な改善推進が必要であることに気づかされた。

なお今回は、地域勉強会とITタスクのメンバーにも参加して頂いたので、大変有意義な研究会となった。

### <次回予定>

- ・令和4年6月16日（木）16:00～17:30

以上