3－4 組織のインシデント対応能力向上をめざす人材育成プログラム

社会実装技術

想定外が不可避のサイバーインシデントに対応できるレジリエンスの高い組織的連携を実現するための演習システムの提案

サイバーインシデント対応に求められる組織連携とは

- スーパーマンを求めるよりも、組織としての対応
- 守り切れない前提で、想定外への対応能力を向上させる
- 部分的には陥落しても、全滅を防ぐ、多重多様な安全対策
- 事業継続の破綻は、関連するAND条件すべてが原因になる（関係者が多い）
- 緊急時にできることは、通信遮断と自動システムに頼らない手動操作
  - 気づけたら、安全は確保できるように計装は構成されているはず
  - いつ、どこを遮断したら、被害を局在化し、早期復旧が図れるか？
  - 通信遮断をするためにどんな検知が必要か、遮断後の対応操作は？
  - 通信遮断して事業継続できるなら、早期遮断が可能
- 操業系のリスク管理、および現場事故対応はOT
  通信系の監視、ツール管理はITが中心になって協力

⇒求められる連携をイメージできる演習（疑似体験）を繰り返す

レジリエンス向上が重要

安全の観点での検討
- Safety-Ⅰ 事故を起こさない能力
- Safety-Ⅱ 想定外な事故でも抑え込める能力
  レジリエンス

サイバー攻撃は、安全破綻のひとつの原因
- サイバー攻撃の手口は想定しきれない
  （脆弱性も攻撃者の発明品）
- 危険源がサイバー攻撃であっても、
  起こる事故は、制御対象で決まる

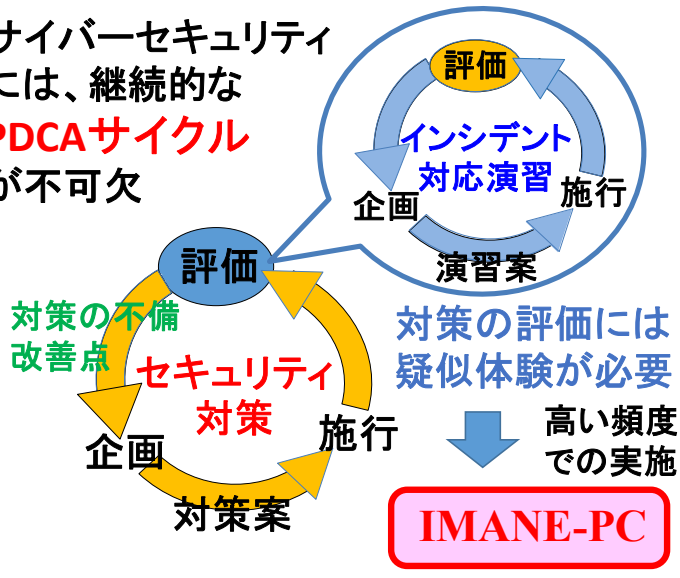
↓

予想外の攻撃にも気づける可能性のある人を配置し、
気づきを適切に対策につなげられる組織体制をつくる

↓

予想外への気づきには、想像力が重要で、
複数のシナリオでの疑似体験（演習）が有効

サイバーセキュリティには、継続的な**PDCAサイクル**が不可欠



対策の評価には疑似体験が必要

高い頻度での実施

IMANE-PC

組織連携を理解するための演習IMANE(Incident MANagement Exercise)シリーズを開発

EX-1: IMANE-DEMO　私は関係したくないという人を引き込むための演習
EX-2: IMANE-CARD　演習のための予習を必要とせず、その場で問題意識を共有するための演習
EX-3: IMANE-PC　コンピュータを利用して、組織連携を疑似体験する演習

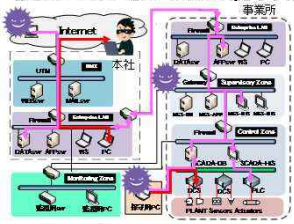
T-1: IMANE-DRAW　インシデント演習用シナリオを編集し、CARD,PC用データを合成するツール
T-2: IMANE-DB　IMANE-PCの実施用データと実施結果のデータを蓄積・検索するデータベース

~~3－4~~ 組織のインシデント対応能力向上をめざす人材育成プログラム

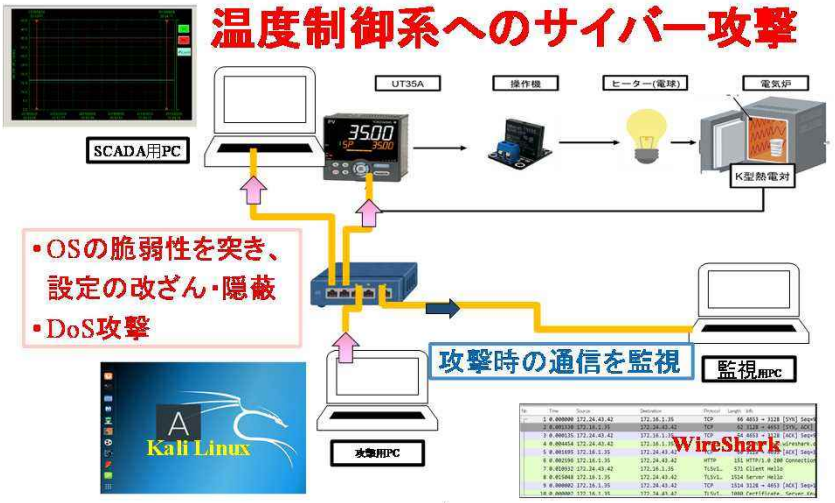
開発した演習システム IMANE (Incident MANagement Exercise)

IMANE-DEMO

- 制御系を構築することでその構造を理解
- 構築した制御系をKali Linuxで自分で攻撃
- 攻撃されている状況での通信を監視し、検知できるとした場合の防御について考える



制御ネットワークに侵入できれば SCADA, Local Controllerを操作するだけでなく、気づけない攻撃が実現できることおよび通信監視で攻撃が見えることを理解する



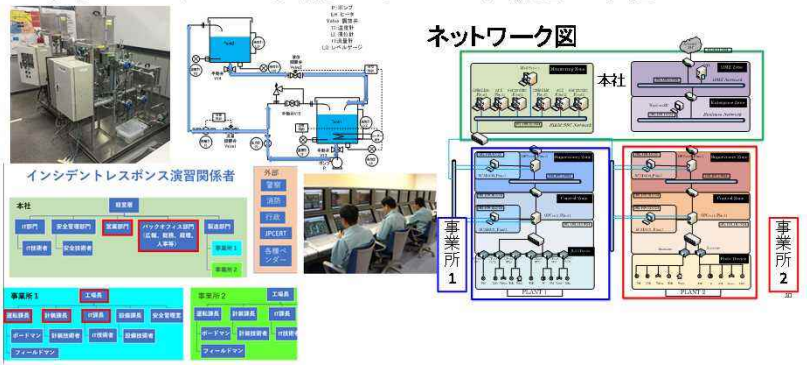
PC3台とコントローラ1台とランプ,HUBだけで実施できる。

IMANE-CARD

① 演習対象のインシデント対応体制の確認

(事業所のシナリオで参加者が役割を理解しているときには不要)

- 守るべきプラントと組織とネットワーク構造の確認



② 演習対象のインシデント対応の流れの確認

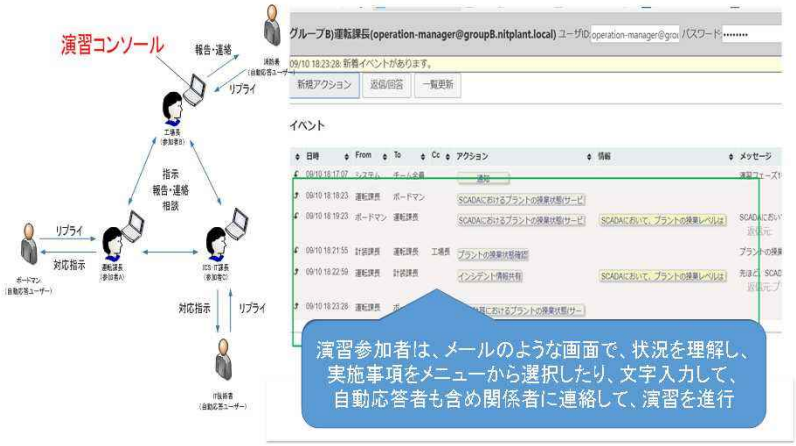
(事業所のシナリオで参加者が役割を理解しているときには不要)

どんな状況で、どんな連携が必要かをカードを並べながら議論する。

カードを正しく配置できるかではなく、カード内容を確認しながら、配置することで、インシデント発生時の状況のイメージを膨らませ、対応を検討する。

IMANE-PC

① コンピュータを利用した演習実施



演習実施風景

（直後に振り返り）

（キーボード入力だけで、会話のない静かな演習時）

ヒューマンインターフェイスはシンプルだが、だからこそ、様々な事業所やシナリオに対応しやすく、演習実施頻度を向上させやすい。そして、直後に、具体的な行動をもとにした振り返りが可能となっている。