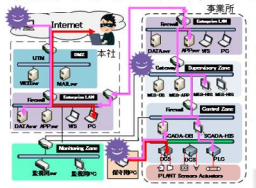
組織のインシデント対応能力向上をめざす人材育成プログラム

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

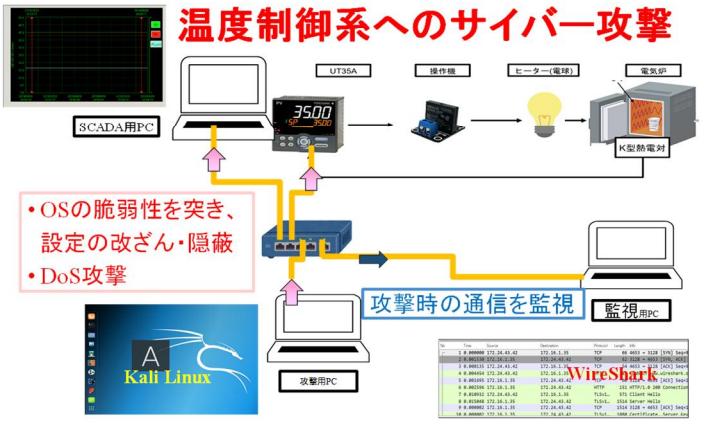
IMANE-DEMO

- 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

温度制御系へのサイバー攻撃



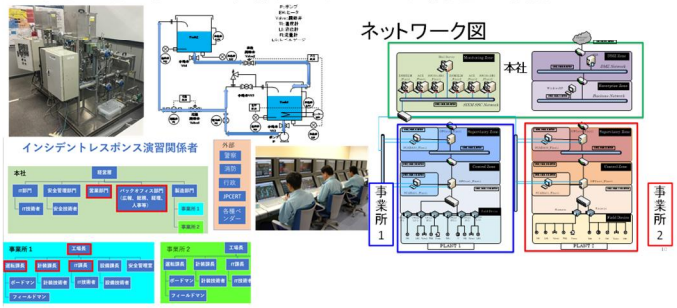
PC3台とコントローラ1台とランプ,HUBだけで実施できる。

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

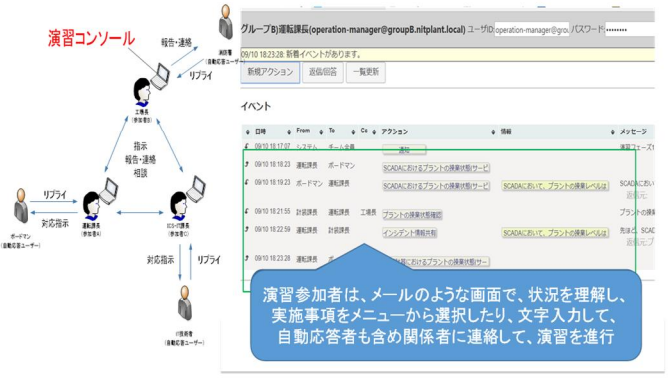
(事業所のシナリオで参加者が役割を理解しているときには不要)

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

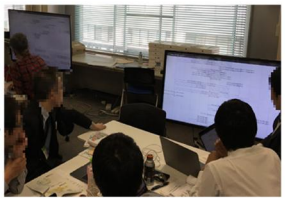
① コンピュータを利用した演習実施



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。

IMANE サポートツール

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
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

提案する演習のねらいと特徴

ここで提案している演習は、従来の取り決めた手順を基に、確実な施行をめざす演習とは趣を異にする。

- 対応手順を記憶するのでは、想定外のサイバー攻撃には到底立ち向かうことはできない。
- 従来の安全対策で検討されてきた危険源と悪意に基づくサイバー攻撃がいかに異なるかを理解し、想定外の手口であっても、変化しない共通の特性に着目して、臨機応変に対応できる組織の構築をめざす。
- サイバー攻撃が物理的変化を起こすのは、計装（コントローラ・センサ）を介してしかないということから、コントローラへの危険な指示は監視すべきであることは、演習を通じて気づいてほしい。
- 想定外が不可避のサイバー攻撃対策には、スーパーマンを求めるよりも、組織としての対応が重要である。
- 異なったシナリオでの組織連携によるインシデント対応を経験し、実行結果を議論するということを繰り返すことが、インシデント対応で共通に求められる組織連携のイメージを獲得するのには必要と考える。
- シナリオを共有し、身近なシナリオにカスタマイズするシナリオ作成環境を整備する。
- 演習結果や振り返りでの議論を共有でき、演習の普及と演習の向上をはかる環境を提供する。

演習のシナリオ作成および振り返りにおける留意点の例

提案した演習では、特にシナリオ作成と振り返りが重要である。演習における主要な観点を以下に示す。

- 東京オリンピックを標的にするようなサイバー攻撃は、多箇所で同時多重に行われる危険性が高く、物理的変化を検知してからでは遅いという危機感が必要である。
- 安全対策は、多重多層に取られており、全停電させても安全は確保できるはずではあり、SCADA がブラックアウトするというような現象が生じても、大事故が起こるわけではない。
- 多重多層の安全対策も、異常が検知されて初めて稼働するので、隠ぺい工作が行われれば、機能できない。サイバー攻撃では隠ぺいが可能であり、気づけない可能性こそが危険である。
- サイバーテロが隠蔽を含めた高度な事故の仕掛けを設置するとすれば、コントローラの情報収集が必要で、その後のサイバー兵器の設置までには、制御ネットワークでの通信が発生しているはずである。
- サイバー攻撃と特定するには時間がかかり、その間に感染や侵入は広がってしまう危険性が高い。
- 疑わしい通信検知の段階で対応するには、通信が遮断された状態での自動システムをあてにしない操業が必要。
  - 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？

  という議論を、通信系の監視、遮断後の解析は IT が中心、通信遮断後の操業対応は OT が中心で協議すべき。
- サイバー攻撃が物理的変化を起こせば、センサ以外にも、現場の表示計器など、サイバー攻撃では隠蔽しきれない検知手段があるはずである。現場パトロールや他部署でインシデントが検知される可能性を考慮すべきである。
- 重要インフラの場合、サービスの継続が重要であるので、安全が確保できても、サービス停止の範囲が広く、復旧までに時間がかかると、重大インシデントとなる。
  サービス停止の危険源は、事業所内にとどまらず、サプライチェーン全体に存在し、管理の弱いところが狙われる。
- サイバー攻撃は多重に仕掛けられている可能性があり、もし、機能が復旧できたとしても、危険源がまだ潜んでいる可能性がある。復旧も完全復旧だけでない段階的な判断が必要かもしれない。
- 異常が隠蔽され、正常でないサービスあるいは製品が外部に提供されてしまうと、現場は安全でも、重大事故となり、経済的にもコンプライアンスとしても大きな被害になることを意識すべきである。
- 特に、保守・保全の管理は重要。検査も所定の機能が実現できていることのチェックでは不十分で、所定の機能以外のことが発生しないこともチェック対象となるが、部品の回路として入り込む危険性まで考慮すると、守り切れないという前提での対策も必要

【問合先】 inquiry@manage.nitech.ac.jp 〒466-8555 名古屋市昭和区御器所町名古屋工業大学 橋本芳宏