(SIP)/重要インフラ等における サイバーセキュリティの確保

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

名古屋工業大学

想定外のサイバー攻撃に対してもレジリエンスの高い組織的対応を可能にするための

新たなインシデント対応演習プログラム

（IMANEシリーズ）を開発した。

産業サイバーセキュリティ人材育成

- 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
- 緊急時にできることは、遮断と手動操作（自動をあてにしない）
  - 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？
  - 遮断するためにどんな検知が必要か、遮断後の対応操作は？
  - 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

⇒どのような連携が求められるかをイメージできる演習

ITとOTの連携を理解する演習
IMANE(Incident MANagement Exercise)

IMANE-PC

PCゲーム形式で、インシデント発生時の組織間連携を
疑似体験し、実施結果で振り返る演習

様々シナリオでの考察から、レジリエンスの向上をはかる

IMANE-CARD

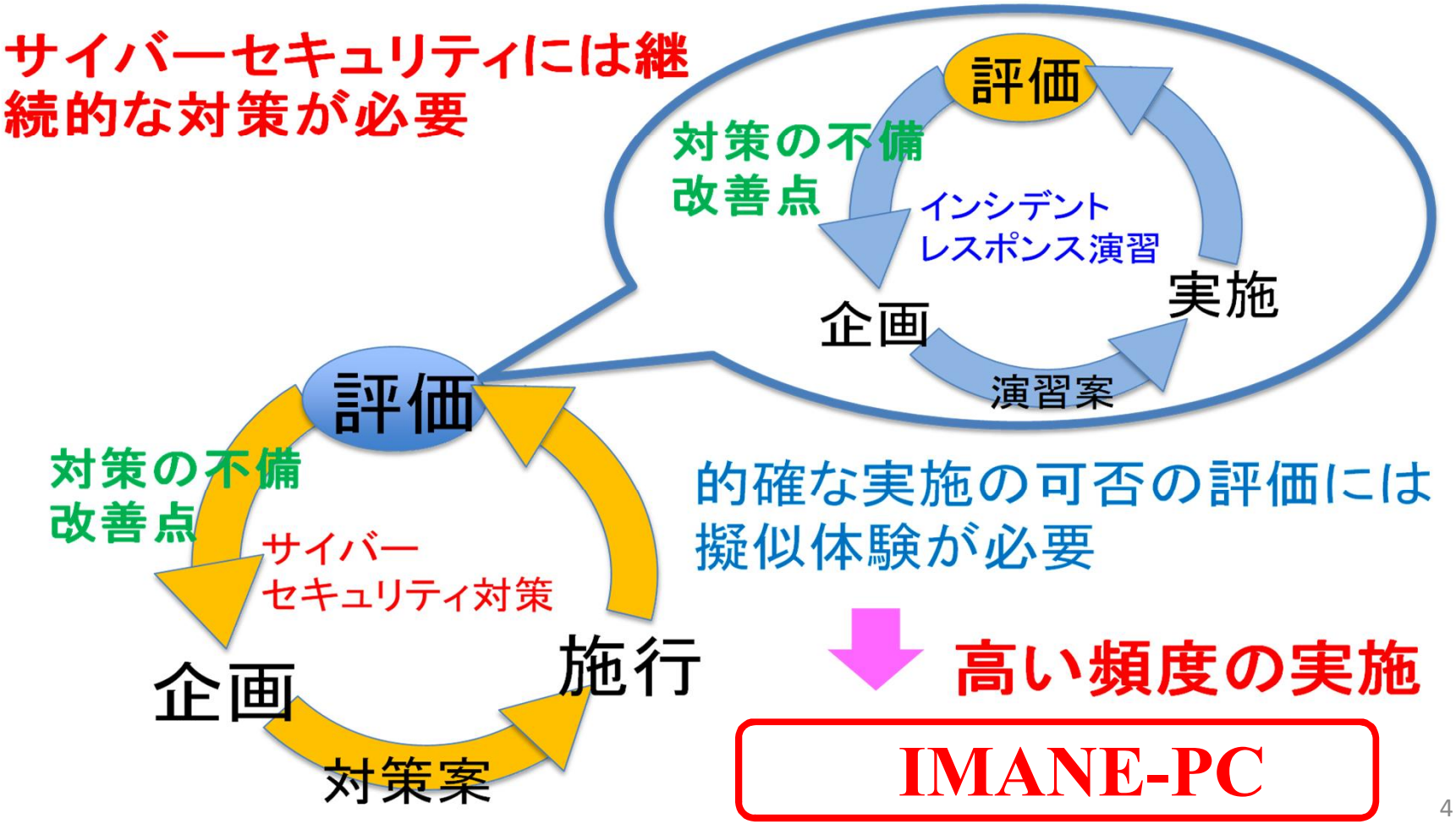
CARDを並べるグループワークで、
インシデント時に求められる組織間連係を考察する

IMANE-DEMO

携帯できるシステムで、制御系でのサイバー攻撃を体験

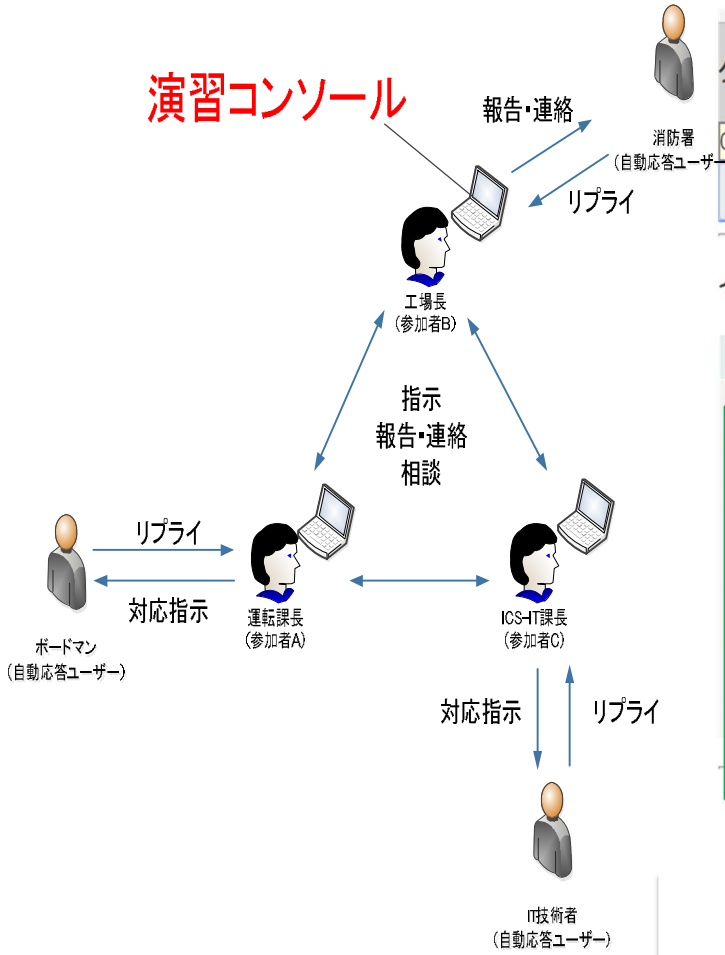
IMANE-PC ①

次なるセキュリティ対策を検討し、PDCAサイクルを促進する



IMANE-PC ②

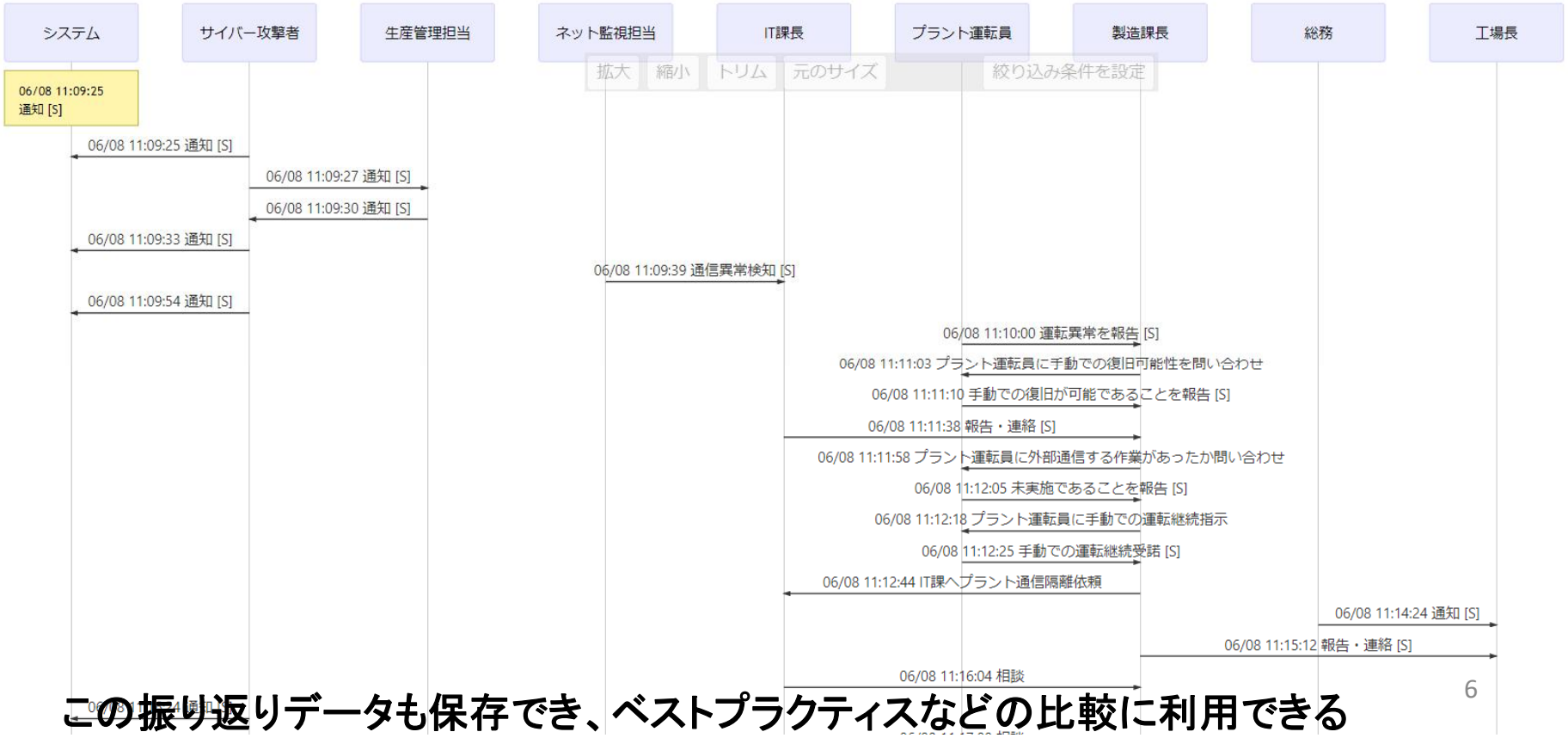
①コンピュータを利用した演習実施



IMANE-PC ③

②コンピュータ出力による演習の振り返り

参加者の行動だけでなく、サイバー攻撃者の行動等も、即座に可視化され、具体的に行動を振り返る



この振り返りデータも保存でき、ベストプラクティスなどの比較に利用できる

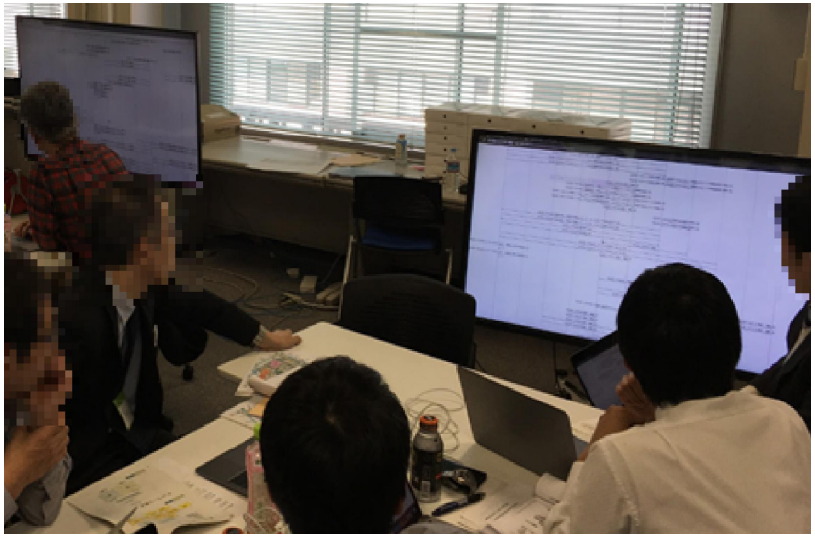
IMANE-PC ④

演習実施風景

（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。

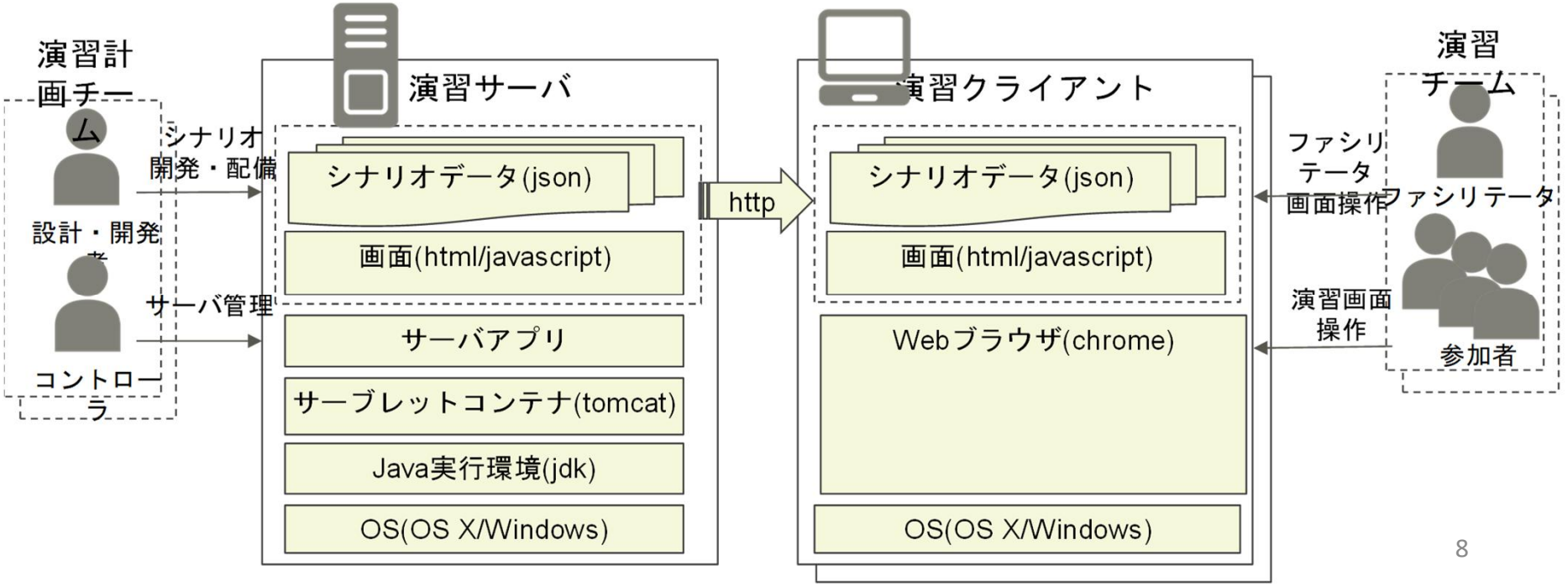
（直後に振り返り）



IMANE-PC ⑤

演習実施システムの構造

IMANE-PCの実施システムは、
サーバーと参加者分のクライアントで実現する。
サーバーはJavaとtomcatが実行できる環境であればよく
MacでもWindowsでも無料で利用できる。
クライアントはChromeでサーバーにアクセスできればよい。
SIPのプロジェクトで開発され、GIT-HUBに公開



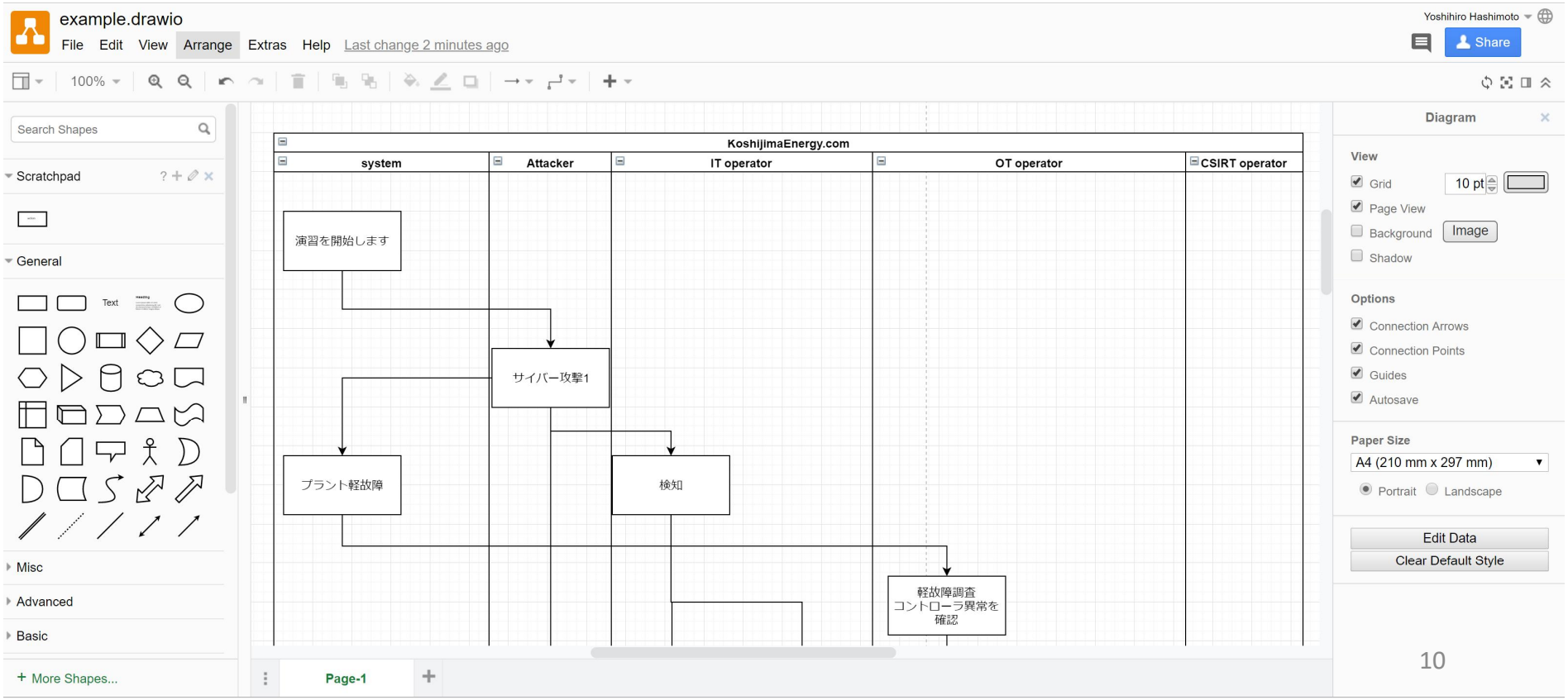
IMANE-PC演習受講生の反応から

- カスタマイズして事業所のシステムに近づけても、差異が残り、うちは違うからという受講生の反応につながるので、へたに近づけるより、アナロジーを感じることができるという対象でシナリオを展開した方が有用
- 隠ぺい工作が安全対策への大きな脅威であることを理解できた。
- OT技術者が、サイバー攻撃を意識しないと、攻撃の被害が拡大し、早期復旧を妨げる行動をしてしまう可能性があることが理解できた。
- IT技術者がフォレンジックしようとしても、情報が全く保持されていない状況がありうることが理解できた。
- 今のままではサイバー攻撃を疑えたとしても、遮断の対応をとれない。OT技術者が、通信がなく、コントローラをあてにせずに操業できれば、疑わしい時点で早期の対応がとりうることが理解できた。
- **インシデント対応演習を展開して、関係者の意識向上につなげたい**

IMANE-DRAW

演習準備：演習シナリオの作成

サンプルシナリオは用意しているが、事業所に適したシナリオを、下図のようにシーケンス図で作製して、
演習システム用のデータを生成する

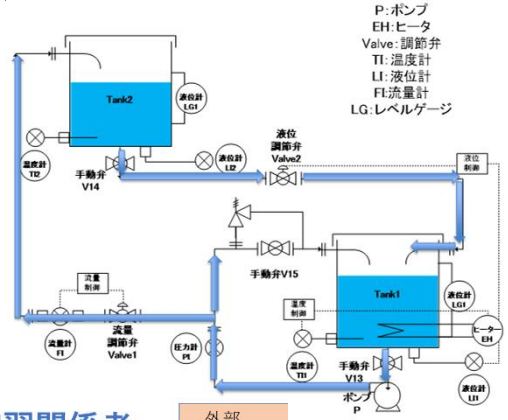


IMANE-CARD ①

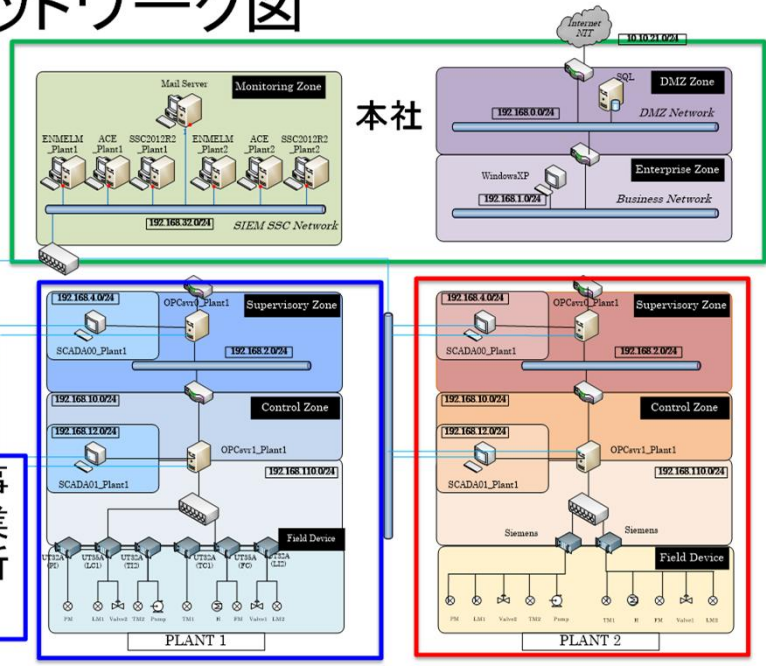
① 演習対象のインシデント対応体制の確認

(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)

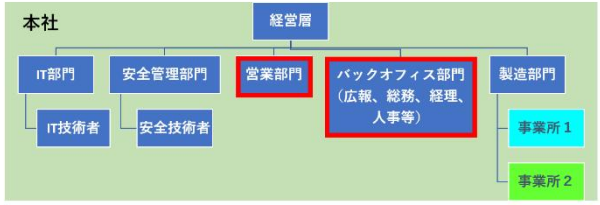
• 守るべきプラントと組織とネットワーク構造の確認



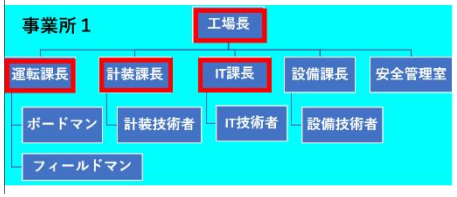
ネットワーク図

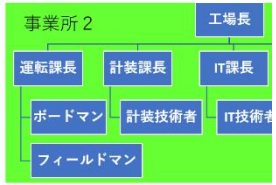


インシデントレスポンス演習関係者



外部
- 警察
- 消防
- 行政
- JPCERT
- 各種ベンダー



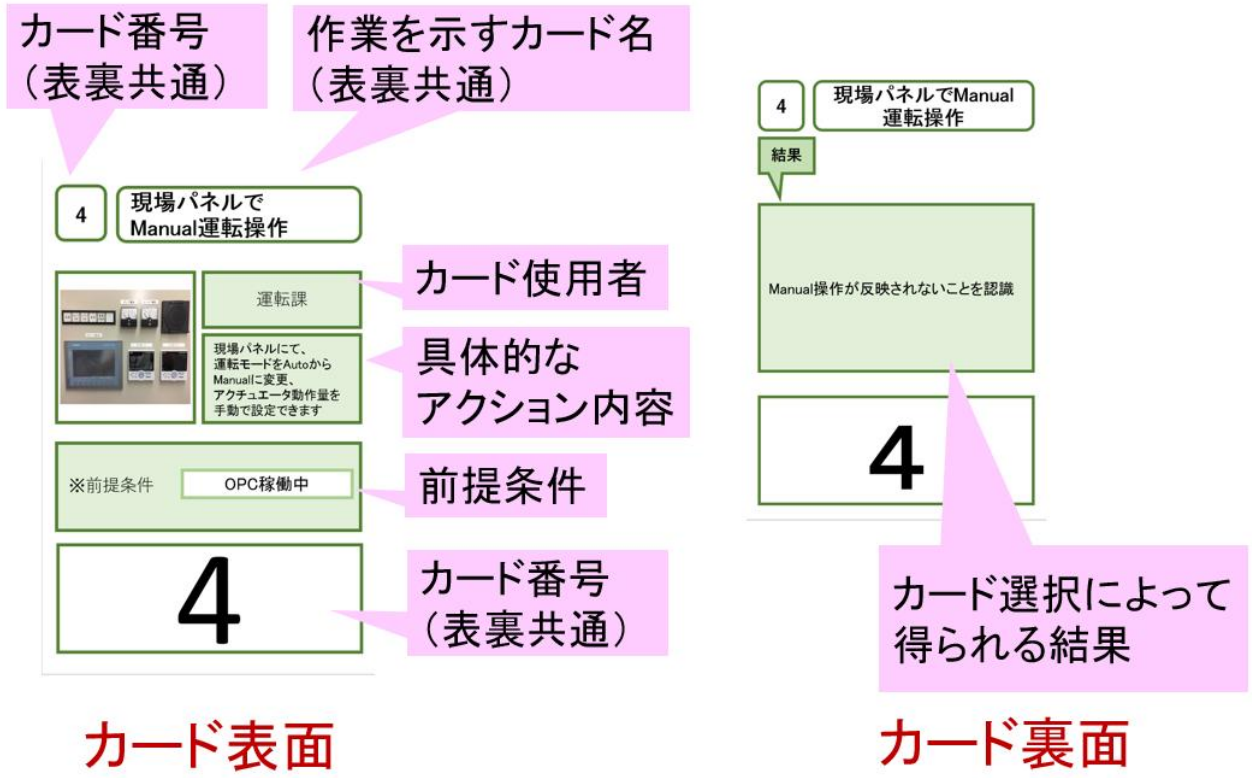


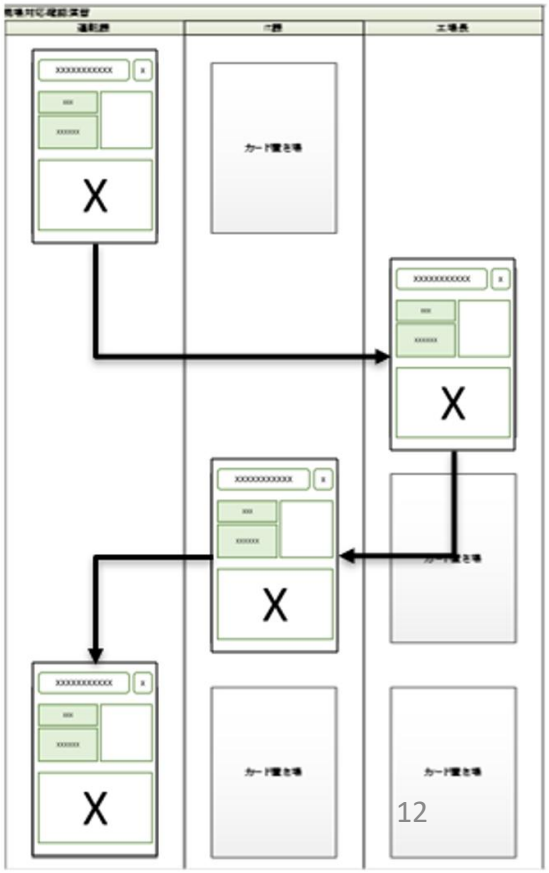
IMANE-CARD ②

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)

- **参加者で相談しながらカードを並べる**





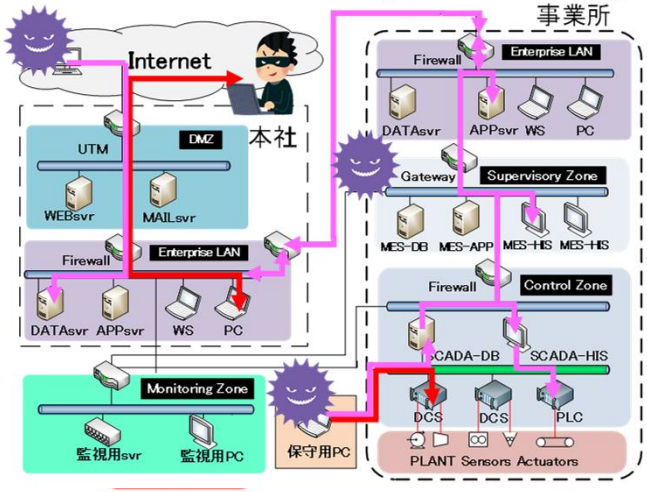
IMANE-CARD ③

演習風景

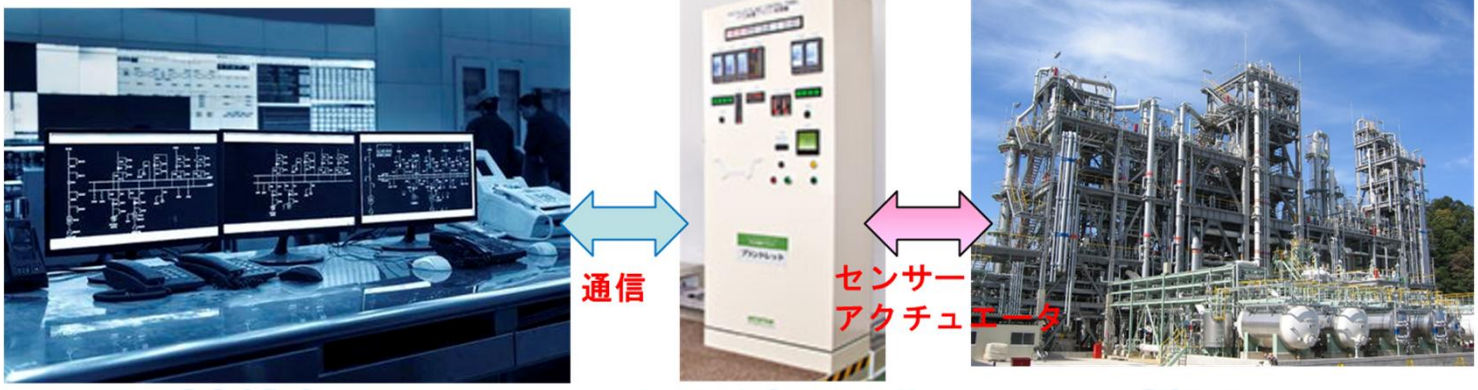
カードの配置を正しくできるかではなく、
カードというツールを使うことによって、議論を推進する。
各組織の対応行動を示すカードを確認しながら、並べることで、インシデント発生時の状況をイメージして、自分たちの部署で、発生したらというかたいで、議論を膨らませていただく。

IMANE-DEMO ①

- 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

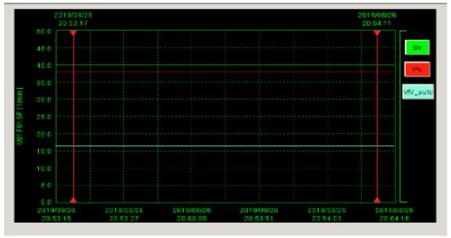


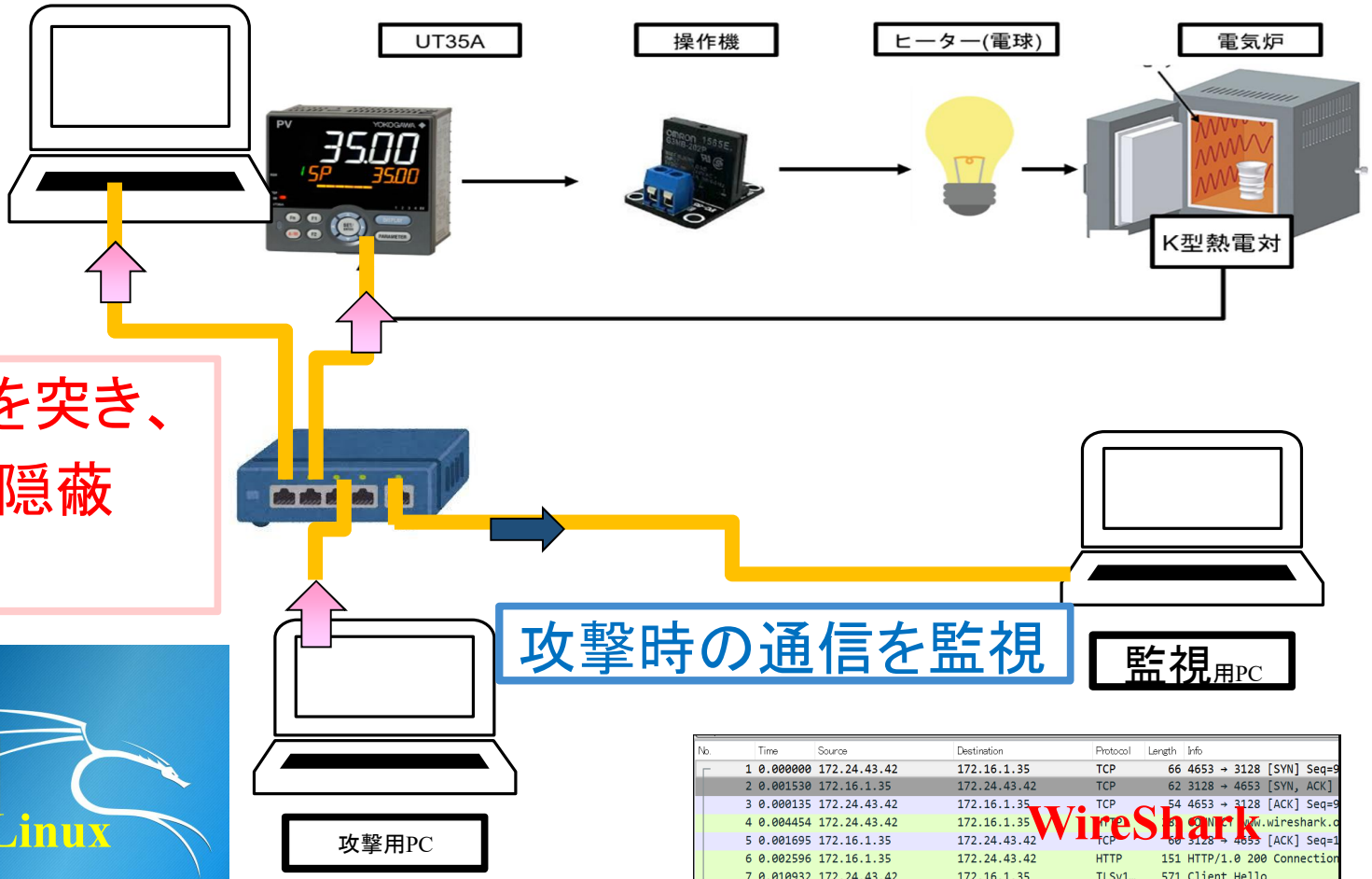
制御ネットワークに侵入できれば
SCADA, Local Controllerを
操作するだけでなく、
気づけない攻撃が実現できること
および通信監視で攻撃が見えること
を理解する



IMANE-DEMO ②

温度制御系へのサイバー攻撃





- OSの脆弱性を突き、設定の改竄・隠蔽
- DoS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-DEMOの演習受講生の反応から

- サイバー攻撃を目の当たりにすることで、
  自分のプラントにも危険性があることを実感できる。
- 気づくための制御ネットワークの通信監視システム
  の重要性に気づく。
- 自分のプラントを守るセキュリティ対策を知りたくなる。
- **サイバー攻撃には想定外がつきものなので、
  知ることよりも考える姿勢が重要と理解した。**
- 簡単な装置で実現できるので、各事業所で実現できる。

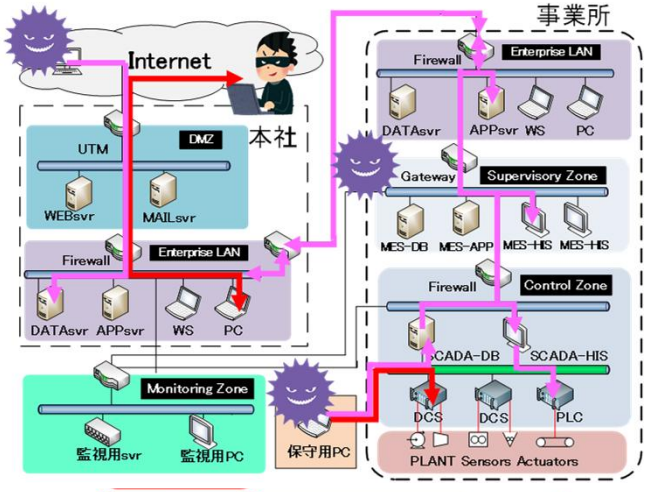
IMANEの維持管理

- 管理対象システム
  ① IMANE-PC（JavaとJava Script）
  ② IMANE-DRAW(フリーウェアのdraw.ioとPython）
- 維持管理体制
  - 開発は名古屋工業大学の研究室だが、
    維持管理は、ユーザー会を設立して継続したい。
  - ユーザー会の中心として、名古屋工業大学発のベンチャー企業である合同会社OTA (Operation Technology Associates)を設立し、制御システムセキュリティ演習の企画＆実施と演習シナリオ開発支援を有償の事業として、企業継続をはかる。
  - IMANE-PC開発当初から協力してくれていた企業社員が退社後の取組として、ユーザー会に加盟し、公開前のソースファイルの脆弱性チェックなどを担当してくれている。
  - 今後、演習体験者を中心に、ユーザー会のメンバーを勧誘し、ユーザー会としての維持管理能力を高めていきたい。

まとめ

- 物理的変化が起こってからでは遅いという危機感が必要
- 保守・保全やサプライチェーン等アタックサーフェスは広い
- いざというときは、通信遮断と手動操作
- 想定外が不可避であるサイバー攻撃に対抗するには、
  リスクに対する意識の高い専門家集団の連携が重要
- さまざまなシナリオで演習を繰り返すことで、
  想定外にも対応できるインシデント対応の向上をめざす。
- できるだけ、演習シナリオを組織内でも共有して、
  多くの事業所で、何回も、インシデント演習を実施して、
  レジリエンスが高い組織を実現しよう。

制御システムへのサイバー攻撃演習



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

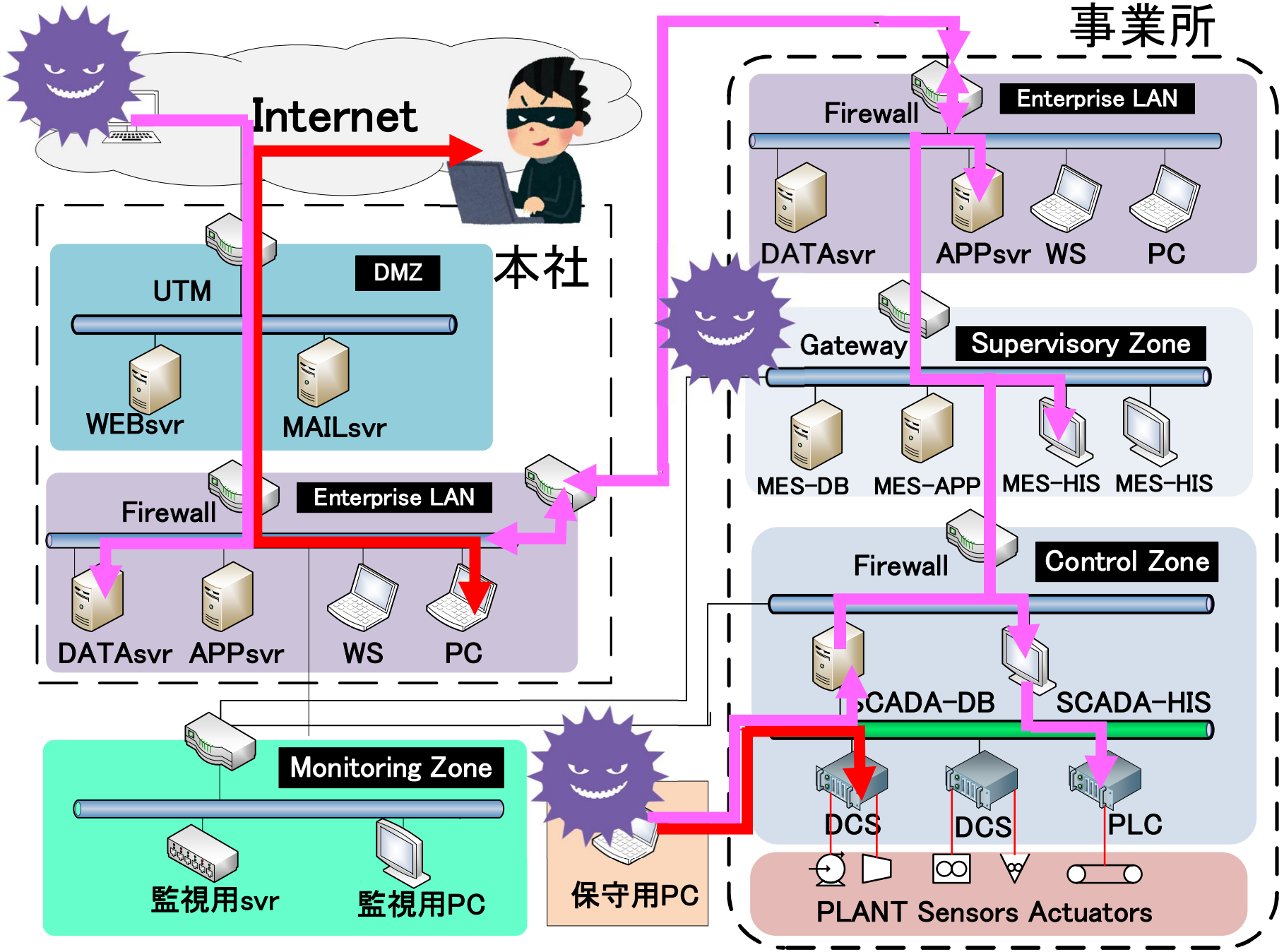
SCADA

通信

Local Controller

センサー
アクチュエータ

Plant


事業所
Internet
本社
DMZ
UTM
WEBsvr
MAILsvr
Firewall
Enterprise LAN
DATAsvr
APPsvr
WS
PC
Monitoring Zone
監視用svr
監視用PC
保守用PC
Firewall
Enterprise LAN
DATAsvr
APPsvr
WS
PC
Gateway
Supervisory Zone
MES-DB
MES-APP
MES-HIS
MES-HIS
Firewall
Control Zone
SCADA-DB
SCADA-HIS
DCS
DCS
PLC
PLANT Sensors Actuators