



制御システムセキュリティ演習から 見えてきたこと

- 早期警戒網整備とICS-CSIRT育成 -

名古屋工業大学大学院工学研究科

越島 一郎

目次

- 自己紹介
- 制御システムセキュリティBCP演習
 - 演習の構成と狙い
 - 演習におけるサイバー攻撃デモ
 - 演習結果とその分析
- 早期警戒網
 - Cyber Active Deception システム
 - 大型ハニーポット(中小企業サイズ)
 - 大規模モニタリングネットワーク





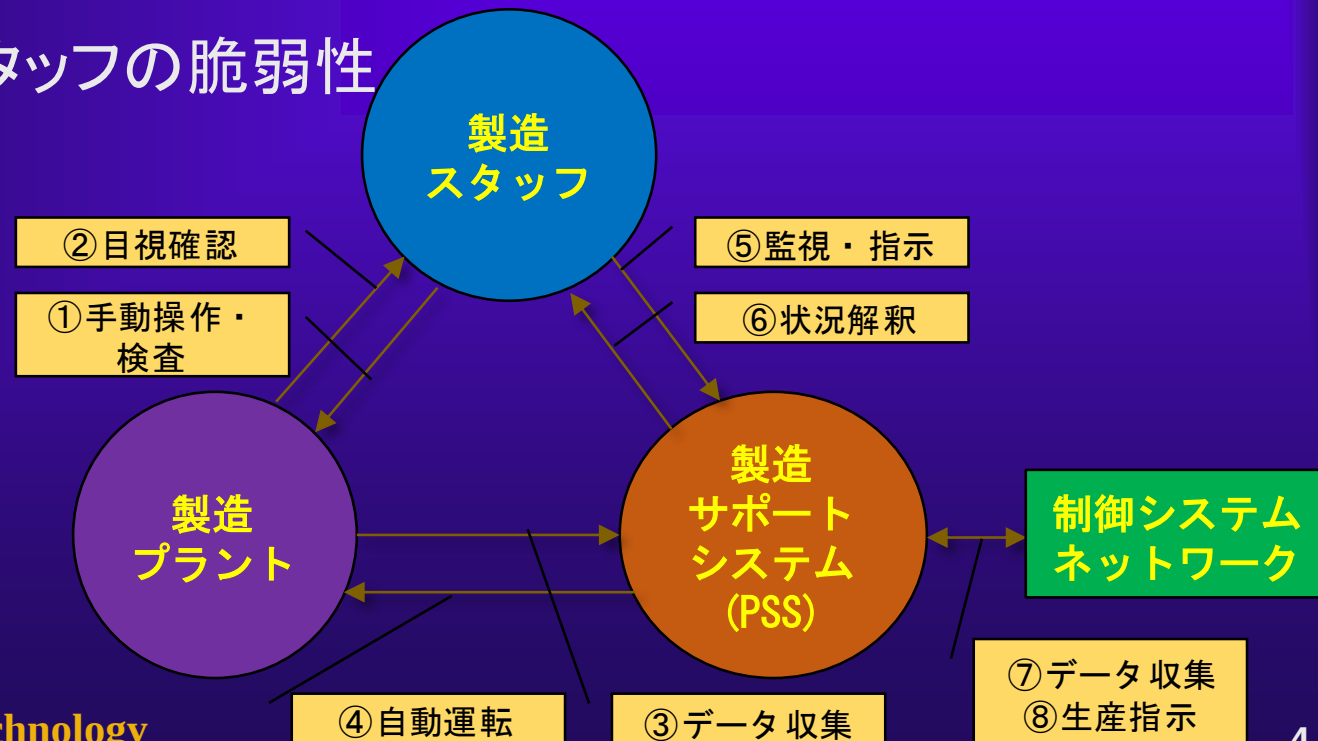
経営システム系が なぜセキュリティ問題を？

大学での私の専門は、プロジェクトマネジメントですが
化工屋としては、プラント&制御系設計、建設、運転・・・
システム屋としては、運転支援、異常診断、組み込み系・・・

更に、
制御システムのセキュリティ問題は、企業存続にも関わる時代に

プラントの構成要素

- 制御システム(ネットワーク+製造サポートシステム)の脆弱性
- 製造プラントの脆弱性
- 製造スタッフの脆弱性



制御システムセキュリティに関する 基本的な捉え方

1. サイバー攻撃は、重要インフラ防御において安全を脅かす確信的な脅威の一つとして捉えなければならない。
2. サイバー空間から操作できるのは、通信回線とCPUを持ったインテリジェント装置だけである。
3. サイバー攻撃は「悪意の誤操作、悪意の誤動作」と考えられ、従来からの安全設計であるフル・プルーフ、フェールセーフの枠組みに入るものである。しかし、悪意であるがゆえ、同時多発に発生することを検討しなければならない。
4. サイバー攻撃による大事故を防止できたとしても、**重要インフラの停止は社会活動に重大な影響を与える。安全だけでなく、事業継続も重要な課題である。**



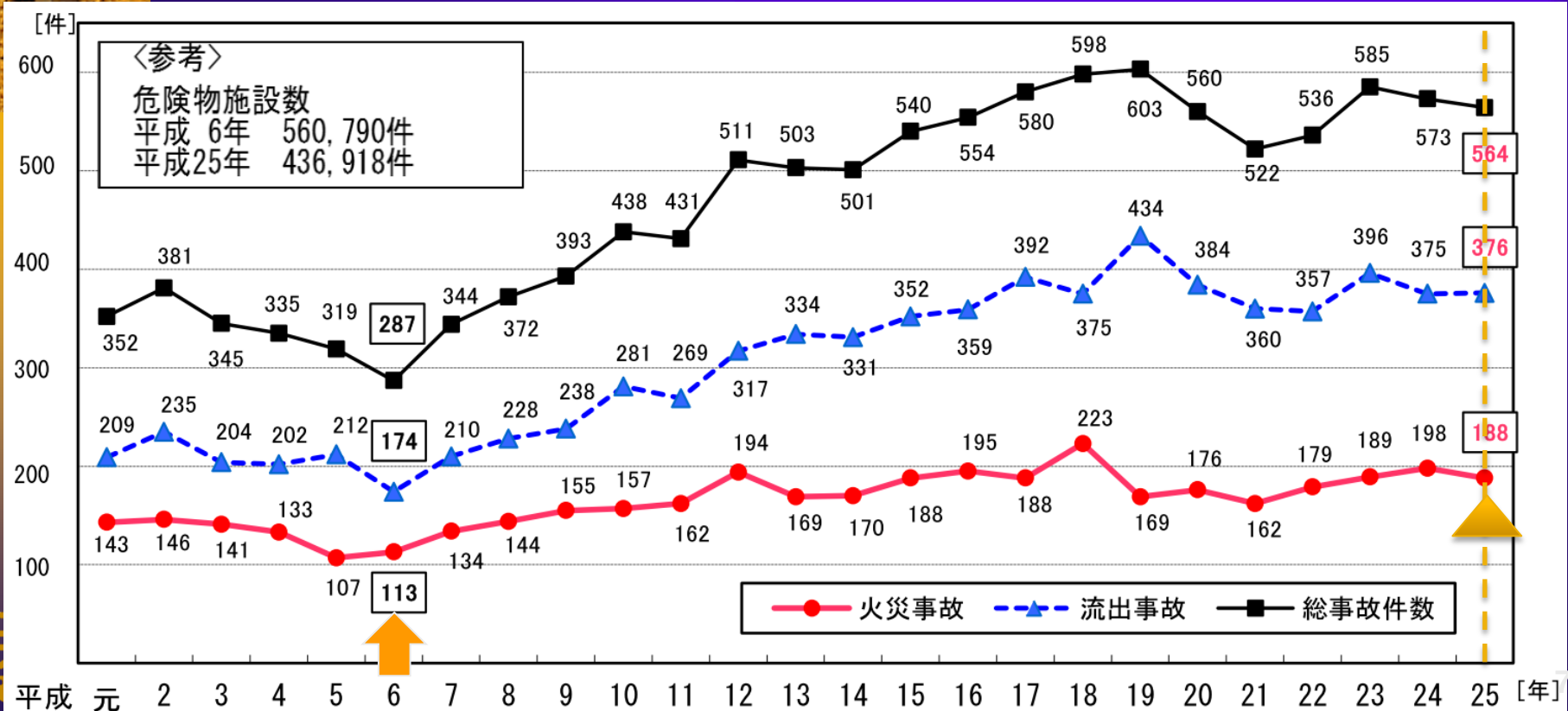
制御システムの脆弱性

- 制御システムを破綻させるのは簡単である。
 - コントローラの符号を変更するのは、一つのコマンドを送るだけである。
- コントローラの仕様はオープンである。
 - 各コントローラのコマンド群情報は無料ダウンロードできる。
- 制御ネットワークのProtocolはセキュリティが考慮されていなかった。
 - Wireshark等で、簡単にパケットキャプチャし解析できる。
- コントローラでは、ウィルス対策ソフトを稼働させない。
 - リアルタイムの制御動作の実現が最優先である。
- セキュリティパッチも、適用しない。
 - パッチが制御アプリへ影響し、不調になることを危惧する。
- ネットに繋がっていなくても、調整時にはPCを接続せざるを得ない
 - Stuxnetのように調整用PCに攻撃が潜んでいる可能性がある
- 制御システムの更新頻度は低い(15年～25年に一度?)
 - OSが自動UPDATEされていれば、古いウィルスは感染しても発症しない。
 - ウィルス対策ソフトの検索対象は、2割以下である。
 - 古いOSをアップデートせずに使用している場合、古いウィルスも脅威となる。



製造プラントの脆弱性

- 平成元年以降、事故が最も少なかった平成6年と比べると、危険物施設数は減少しているにもかかわらず、**事故発生件数は約2倍に増加**
 - 消防庁発表“平成25年中の危険物に係る事故の概要”より



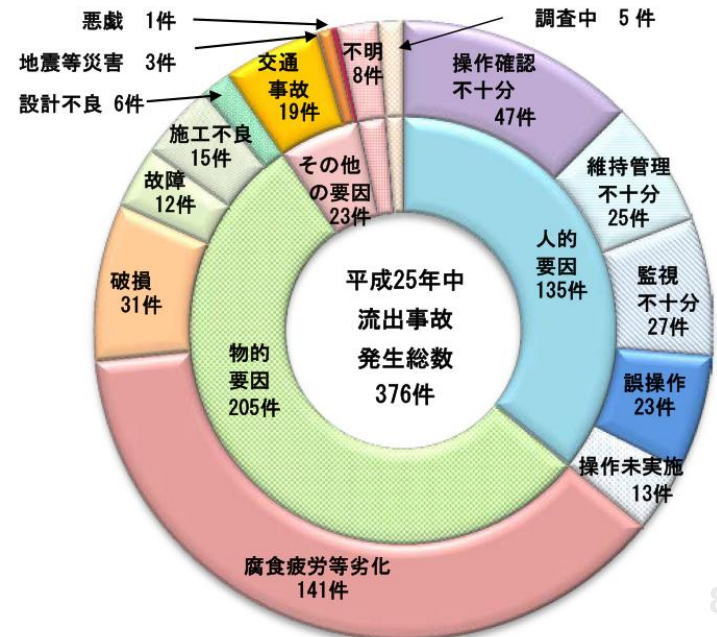
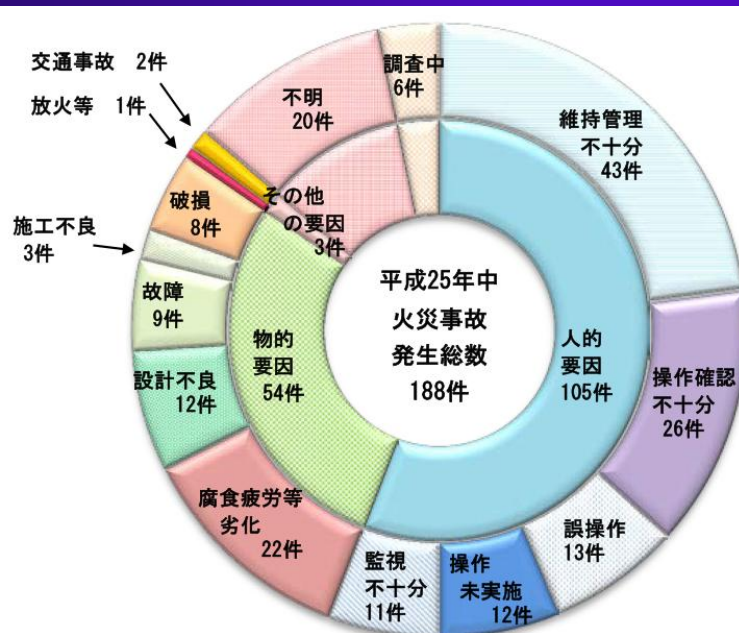
危険物施設の事故原因

流出事故発生原因

- 腐食疲労等劣化など、物的要因によるものが多くを占めています。
(流出事故発生件数376件中205件)
 - 消防庁発表“平成25年中の危険物に係る事故の概要”より

火災事故発生原因

- 維持管理や操作に当たっての不手際など、人的要因によるものが多くを占めています。(火災事故発生件数188件中105件)



製造スタッフの脆弱性

- 爆発火災事故：非定常運転時、熟練オペレータの立会下で発生
 - 2011年11月：東ソー南陽事業所（山口県周南市） 第二塩化ビニルモノマープラント
 - 稼動再開：第一VCM 2012年5月8日、第三VCM 2012年7月8日
 - <http://www.tosoh.co.jp/newsn/index.html> 参照
 - 2012年4月：三井化学岩国大竹工場（山口県和木町） レゾルシンプラント
 - 再建を断念し、本年12月末をもって事業撤退
 - http://jp.mitsui-chem.com/release/2012/2012_1225.htm 参照
 - 2012年9月：日本触媒姫路製造所（兵庫県姫路市） アクリル酸製造プラント
 - 主力製品である紙おむつ用高吸水性樹脂（SAP）や原料のアクリル酸の生産再開のめどは立っていない。
 - 2013年3月 調査報告書
 - 2013年8月6日 製造所および屋外タンク貯蔵所等5施設について、一時使用停止命令を解除
 - 2014年1月：三菱マテリアル四日市工場 高純度多結晶シリコン製造施設
 - 2014年6月14日 事故調査報告書公開 【深層原因】に言及
 - 2014年7月1日 運転再開

事故によって亡くなられた方のご冥福をお祈り致します。
また、負傷された方が早く快復されることを望みます。



高度化する設備と作業員の技能レベルが乖離

(週間ダイヤモンド Diamond Online inside Enterprise【第779回】2012年12月11日より

• <http://diamond.jp/articles/-/29207>)

- 一連の事故が起きた背景として強く問題視されたのが「現場力の低下」だ。
 - 「設備の高度化と技術継承不足で、トラブル時に臨機応変な対応が取れなくなっている」と大手化学幹部。事故の発端はそれほど甚大ではない設備のトラブルだったにもかかわらず、その後の人的な不手際が事態を悪化させたという。
- そもそも自動化が進んだからといって、人員のレベルを下げられるわけではない。
 - 1990年代以降、日本の化学各社は国内市場の縮小対応と国際競争力を高めるようと、多品種少量生産型へシフトした。
 - そのため設備は幾重にも配管でつながれ、より複雑な構造になっており、以前にも増して運転員ら現場担当者に求められる知識スキルは上がっているのだ。



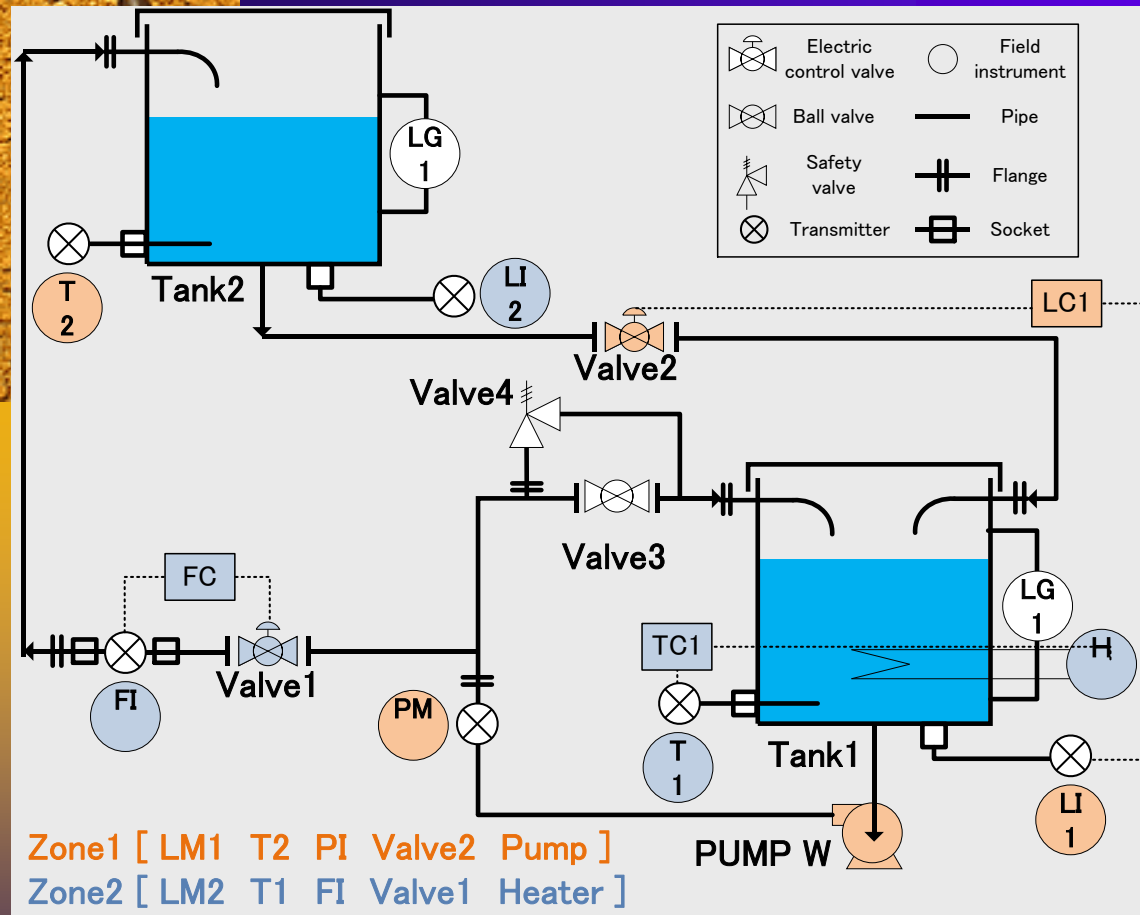


名古屋工業大学テストベッドにおける サイバー攻撃デモンストレーション

侵入・探索→攻撃→隠蔽



テストベッド概要



テストベッド概要



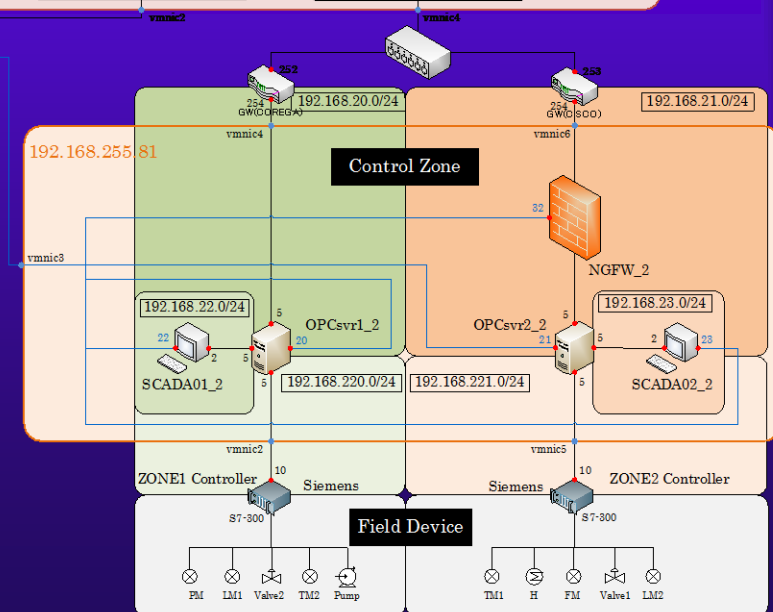
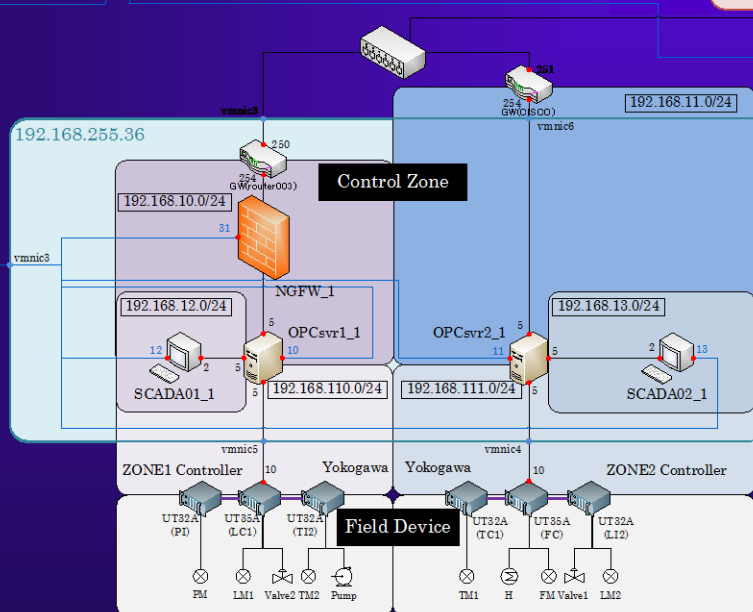
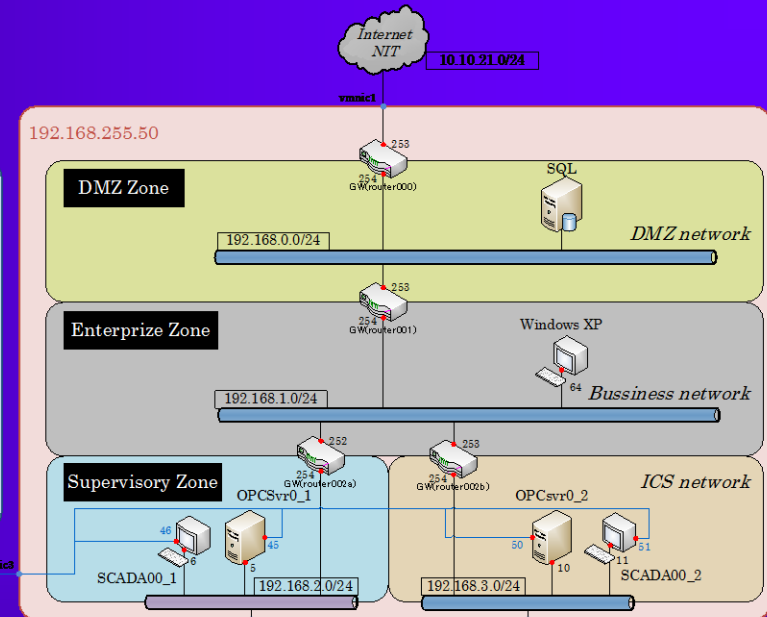
横河電機
シングルループ
コントローラ
UT35A, UT32A



SIEMENS
PLC
SIMATIC S7-300



ネットワーク構成



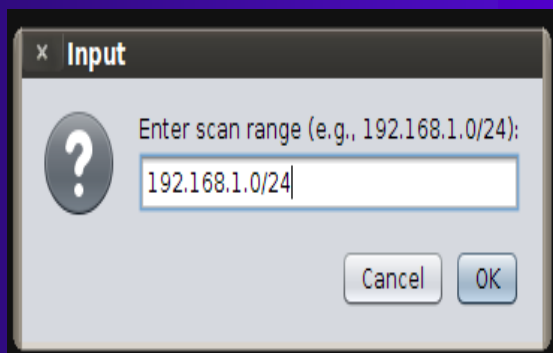
サイバー攻撃手順

1. Nmapを使って、ネットワーク内の端末をスキャン
2. 踏み台となるPCを乗っ取り、下位ネットワークへ侵入
3. 再びネットワークをスキャン
4. 目標の対象を見つけて攻撃
 - ファイル送信, VNC, ウイルス起動 等

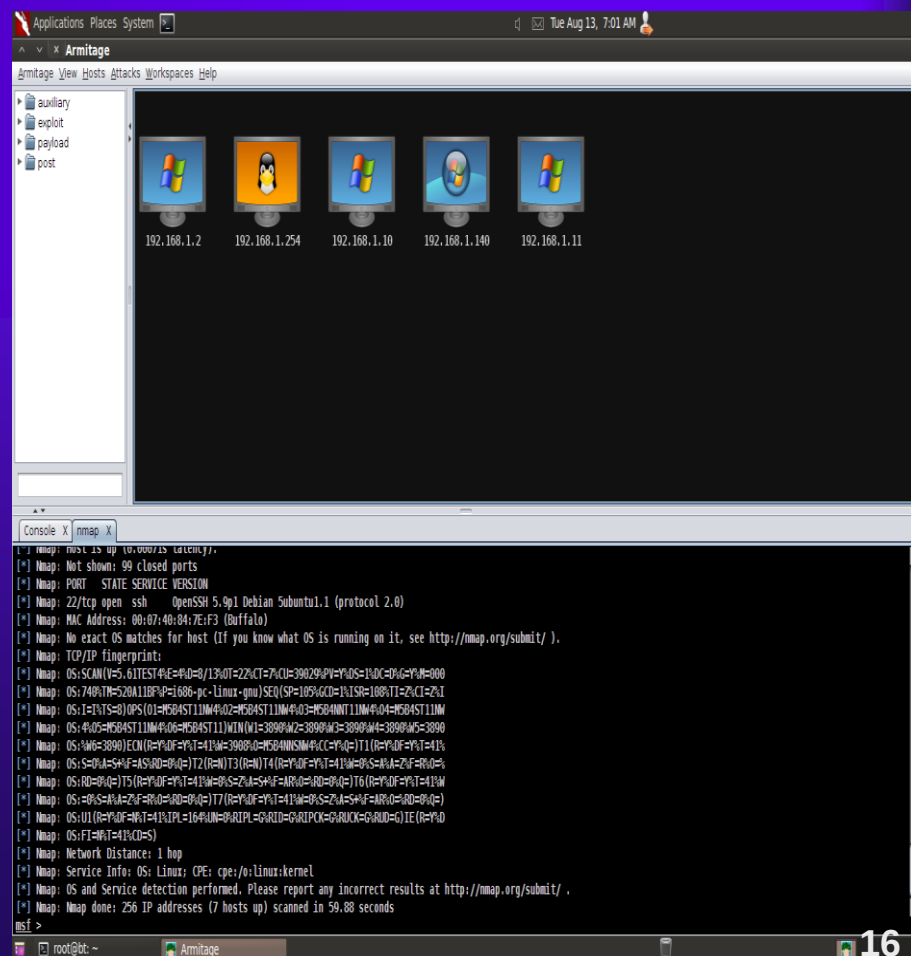


1. ネットワーク内のスキャン

- 探索したいネットワークを入力し, Nmapスキャン

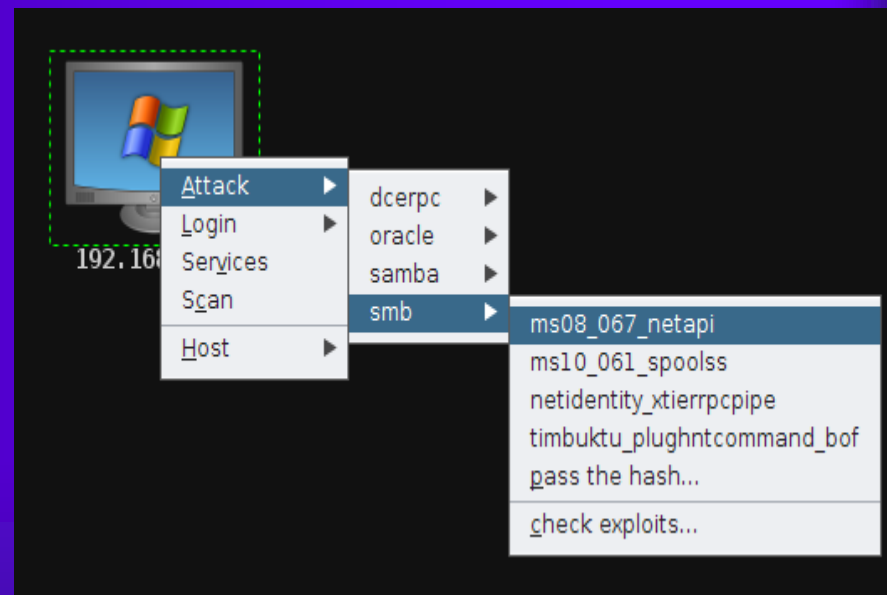


- ネットワーク内の
探索結果→



2. 踏み台となるPCの乗っ取り

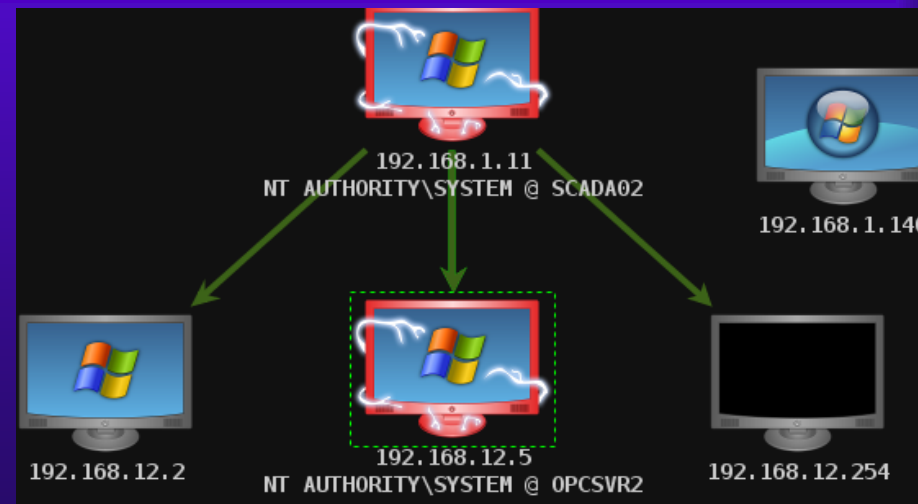
- 踏み台となるPCに対してms08_067_netapiの脆弱性をエクスプロイト



3. 下位ネットワークへ侵入

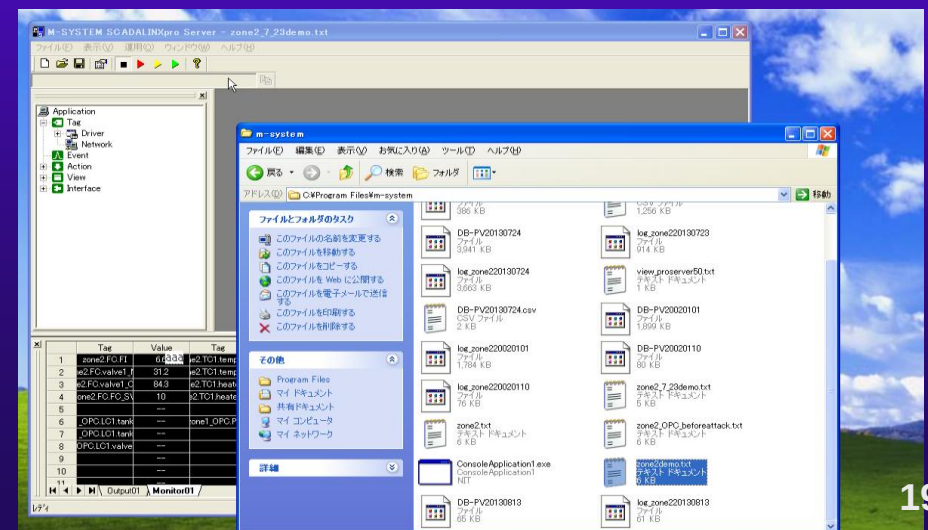
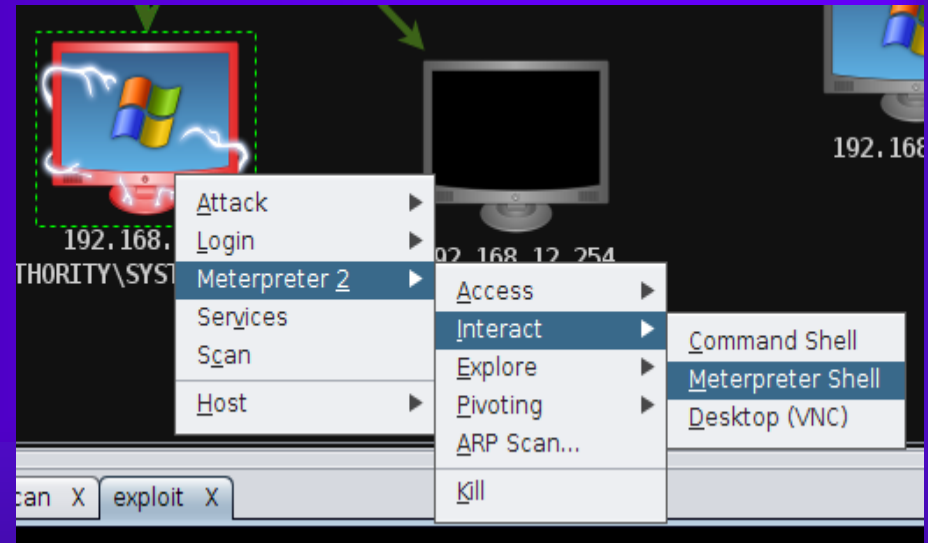
- ARP Scanによって下位のネットワークを調査
- Pivotingによって下位のネットワークに侵入
- 再びNmapにより下位のネットワーク内の探索, さらに攻撃

```
SESSION => 1
msf post(arp_scanner) > set RHOSTS 192.168.12.0/24
RHOSTS => 192.168.12.0/24
msf post(arp_scanner) > run -j
[*] Post module running as background job
[*] Running module against SCADA02
[*] ARP Scanning 192.168.12.0/24
[*] IP: 192.168.12.2 MAC 00:1d:09:76:90:72 (Dell Inc)
[*] IP: 192.168.12.5 MAC 00:18:f3:26:fb:d7 (ASUSTek COMPUTER INC.)
```



4. マルウェアの送信・実行

- 目標となるPCにたどり着いたら、マルウェアをアップロード
- VNC(Virtual Network Computing)を使ってリモートデスクトップでOPCサーバに接続, マルウェア実行



マルウェア(モドキ)の挙動



非公開



マルウェア(モドキ)の挙動



非公開

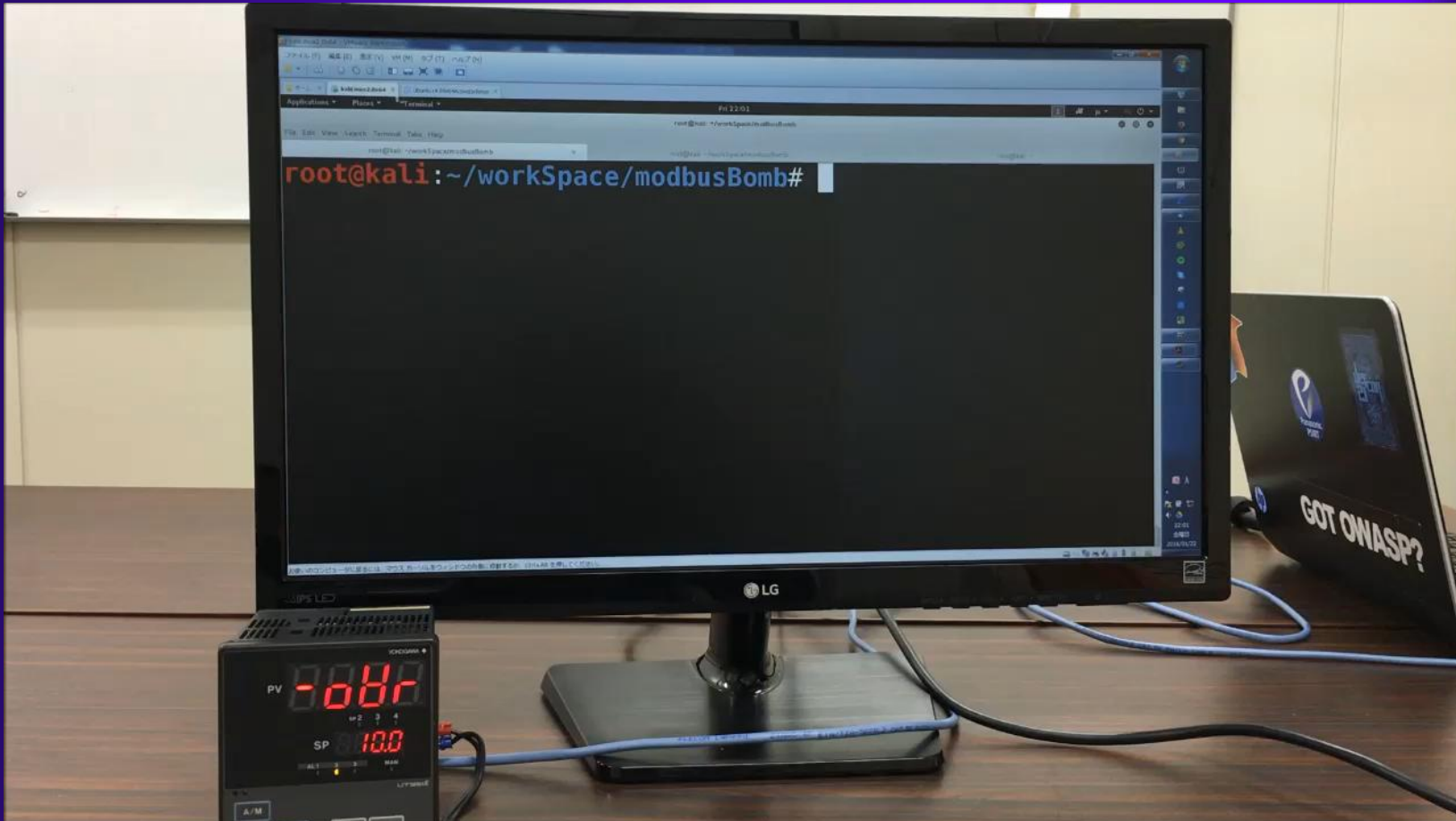




サイバー攻撃 デモンストレーション2

コントローラへの直接攻撃

Modbusプロトコルを使用した攻撃



ワンループ
コントローラ

攻撃者の画面



Nagoya Institute of Technology

pythonソースコード
ライブラリの充実で単純化

非公開





制御系セキュリティBCM演習



制御系セキュリティBCM演習の目的

なぜ制御系セキュリティBCM演習なのか？

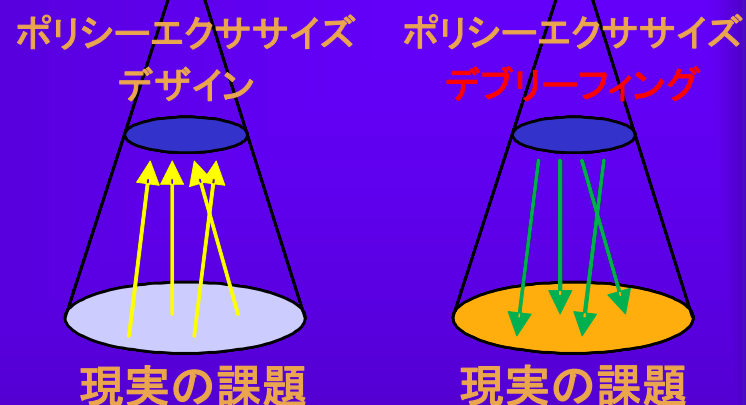
セキュリティ課題は、ツールを入れるだけでは解決しない。

- 特に、制御系システムの場合、IT部門と制御システムを運用する現場との連携が必要。
- さらに事態が深刻となった場合、マネジメント層、広報等を巻き込んで会社全体の連携が重要となる。特に、誰が責任を持って判断するのかを明確にするのが重要。



ポリシーエクササイズ

1. 参加する
2. 夢中になる
 - 心を開く
3. 体験と気づき
 - シミュレーション
 - デブリーフィング
4. 思考や行為の変革
 - 状況認知と状況対応
 - 実践への導き



© S. Tsuchiya, CIT



演習の流れ



予兆 フェーズ

- プラントの異常に対する緊急安全対応のフェーズ

緊急対応 フェーズ

- ICS-BCMとして、サイバー攻撃判定フェーズ(サイバー攻撃判定から運転停止まで)

復旧 フェーズ

- ICS対策も考慮した復旧案の作成

作成するワークフロー

対応部署

状況

9:00

- SCADA
L1 正常
L2 低下

システムメッセージ

8:30

- NGFWからのイベントで不正アクセスの検知 (SIEM)

報告事項・連絡事項

8:30

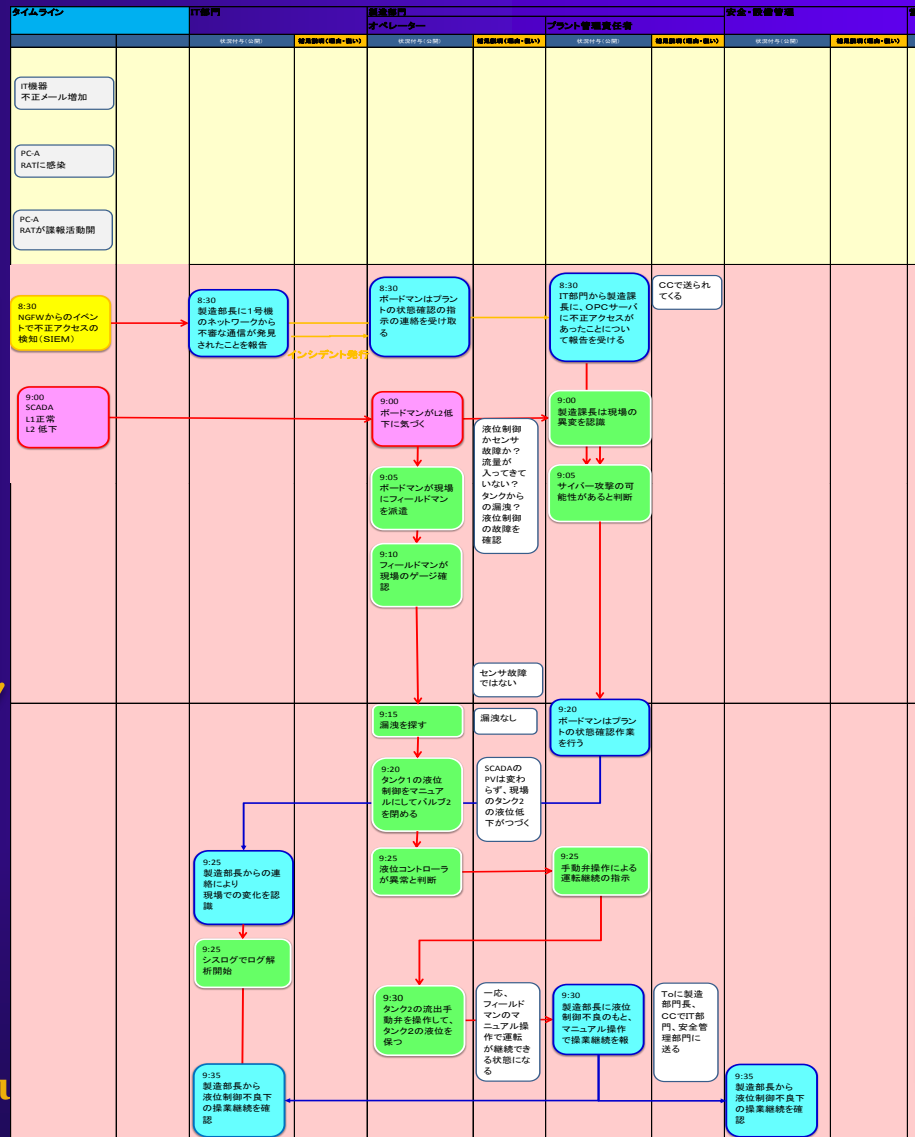
- 製造部長に1号機ネットワークから不審な通信が発見されたことを報告

行動

9:05

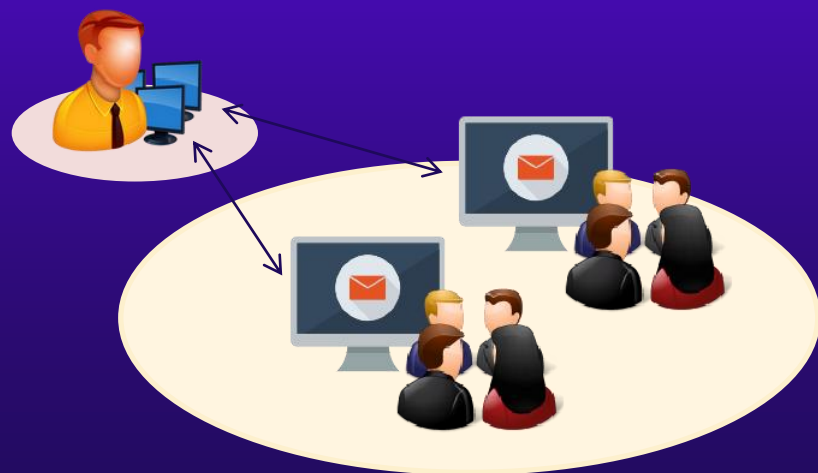
- ボードマンが現場にフィールドマンを派遣

時間経過



メールによる問い合わせの利用

- 各チームに設置されているパソコンを利用し、「橋本ケミカル」社員として、コントローラが演じる他の部署の社員にコンタクトすることができます
- 現場・他部所への情報提供依頼などに利用可能
- 指示は具体的に



メールによる問い合わせの利用

- テンプレート

宛先 : responce@nitplant.local

件名 : (指定なし)

本文 : From:

To:

(内容)



演習ファシリテーター

- アドバイザー
 - 演習会場内で、対応案のアドバイス・及びBCMに関する質問に回答します
- リプライヤー
 - 各チームからの橋本ケミカル社員への質問に回答します
- サポーター
 - 各チームのグループワークに参加します
 - サポーターから追加情報をお渡しすることはありません



本演習の留意点

- ICS-BCMの本筋を考えて頂きたい。
 - 複雑になりすぎないように、通常のBCM演習で行われるような、ストレス条件(マネージャーが居なかったら、メールが届かなかったら等)の付加については考慮しない。
- 本演習のプラントは、ICS-BCMを考えるためのリファレンスである。
 - 自社のシステムとの違いがあることを認識したうえで、想像力を働かせてほしい。
- 他チームの考え方を参考にしても構わない。
 - せっかくの演習なので、自社の経験やナレッジに基づいて、自由に発想して、自由に発言していただきたい。但し、他チームの考え方は尊重すること。
- 全体でひとつの正解を出すのが目的ではない。
 - あくまで、各社がBCMに資するアウトプットを出して、自社に持ち帰ることが目的である。この演習は、そのためのツールとして活用してほしい。





会社紹介

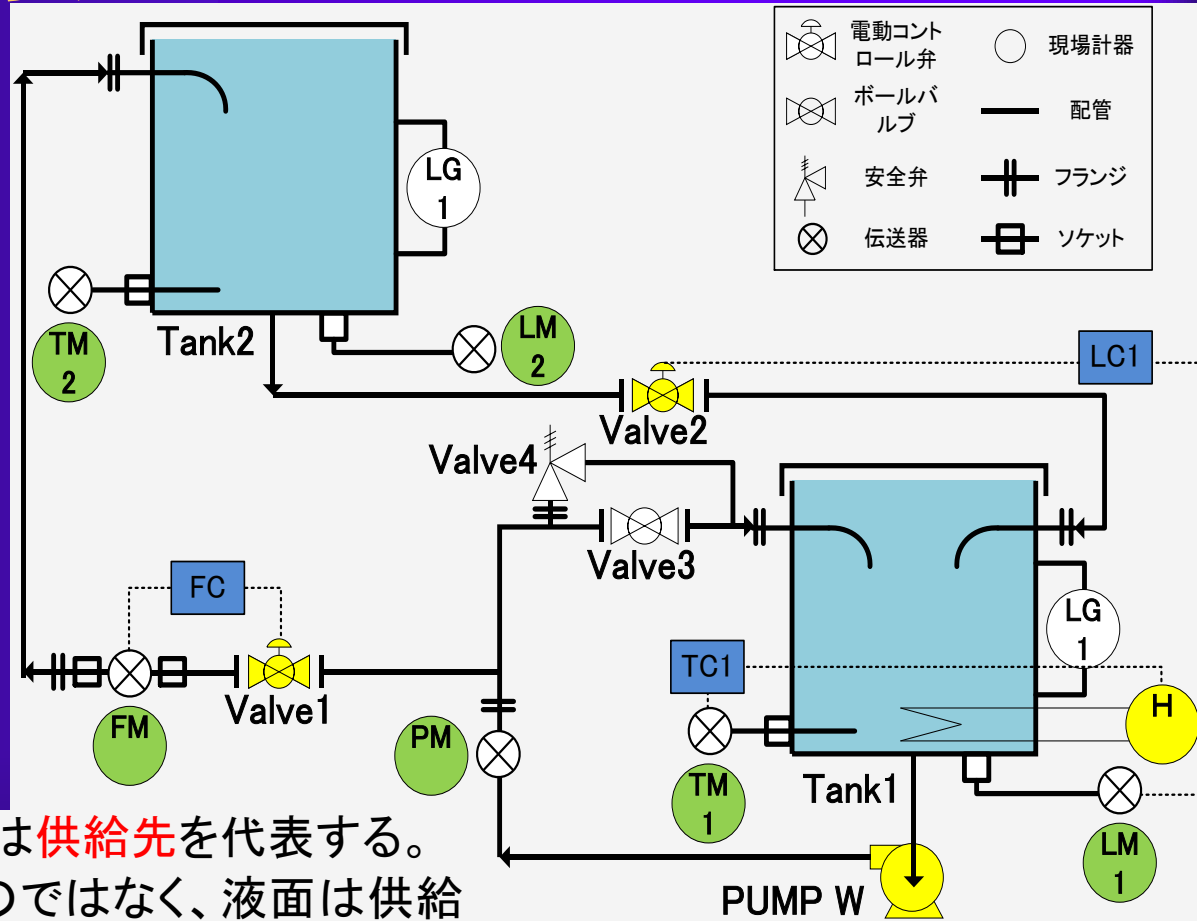
<http://www.hashichem.co.jp/>

サービス概要

- 地域冷暖房サービス会社
- プラント1は主にX市エリアに、プラント2はY市エリアに冷暖房を供給
- 主な顧客は市町村・病院・オフィスビル群・データセンターなど



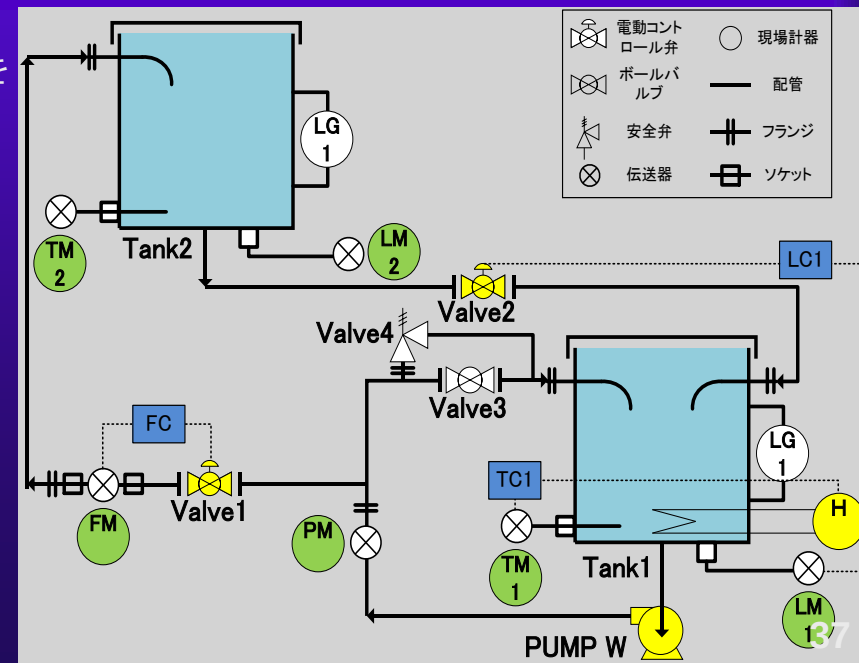
プラント概要



- タンク1は製造タンク、タンク2は供給先を代表する。
- タンク2は液面を管理するものではなく、液面は供給元だけで監視される。
- ヒータやクーラが乾くことは、火事などの事故につながり、故障であっても長期サービス停止に陥る。
- また、タンクがあふれると、周辺装置へ影響を与え、やはり事故になる。

前提条件:プラント

- プラント制御系
 - Tank1の液位をValve2でPID制御
 - Tank2の液位をモニター
 - Tank1からTank2への流量をValve1でPID制御
 - Tank1の水温をヒーターHでPID制御
 - Tank2の水温をモニター
- 施されている安全対応
 - アラーム(1号機のみ設置)
 - ポンプの吐出圧が高(H)を検知
 - アラート
 - 液位センサの高(H,HH)、低(L,LL)を検知
 - 温度センサの高(H,HH)を検知
 - ポンプの吐出圧が高(H)を検知
 - 安全弁
 - ポンプの吐出に設置
 - 手動スイッチ(1号機のみ設置)
 - ヒーターON/OFF
 - ポンプON/OFF
 - レベルゲージLG
 - Tank1、Tank2に現場設置

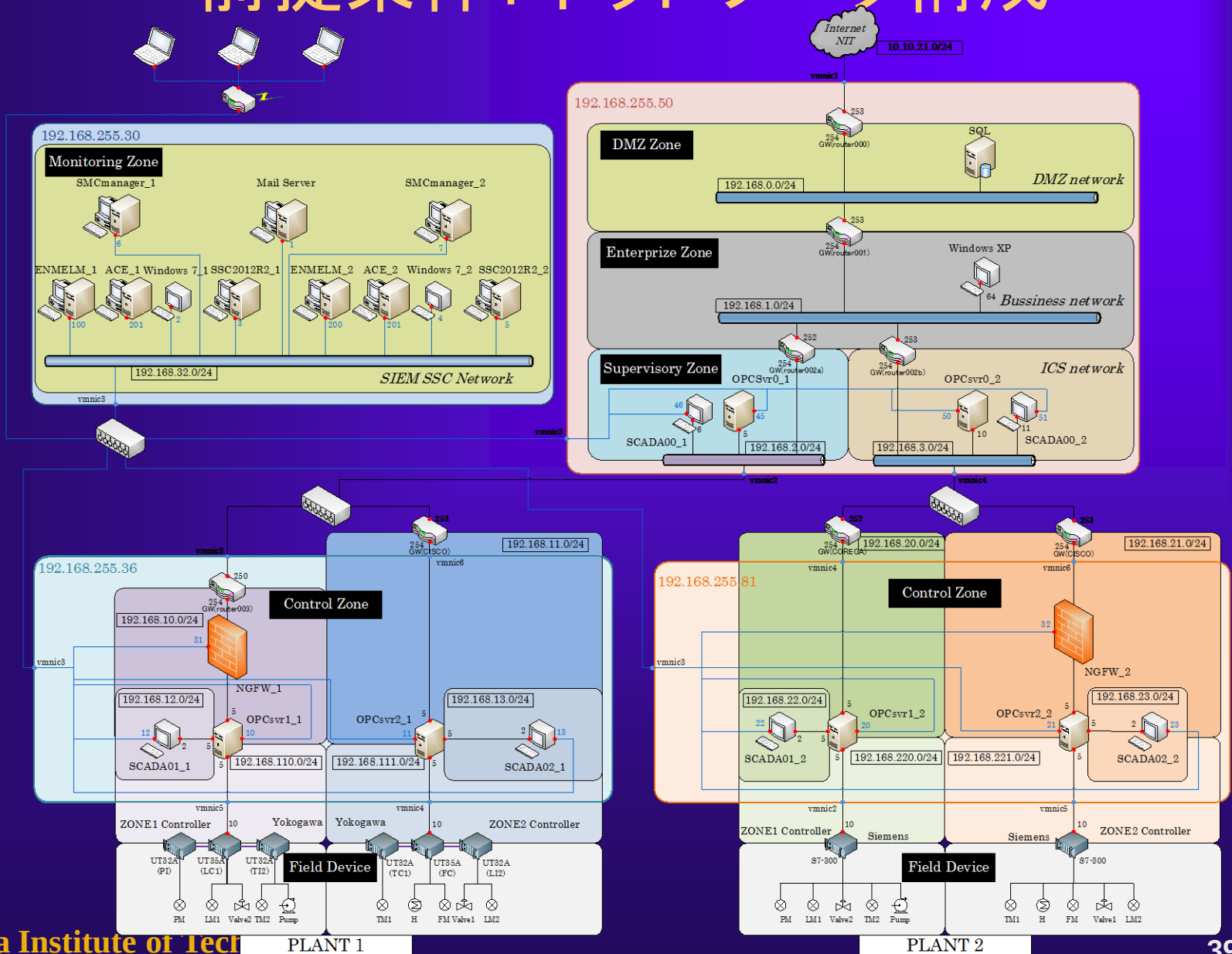


前提条件: SCADA、HMI

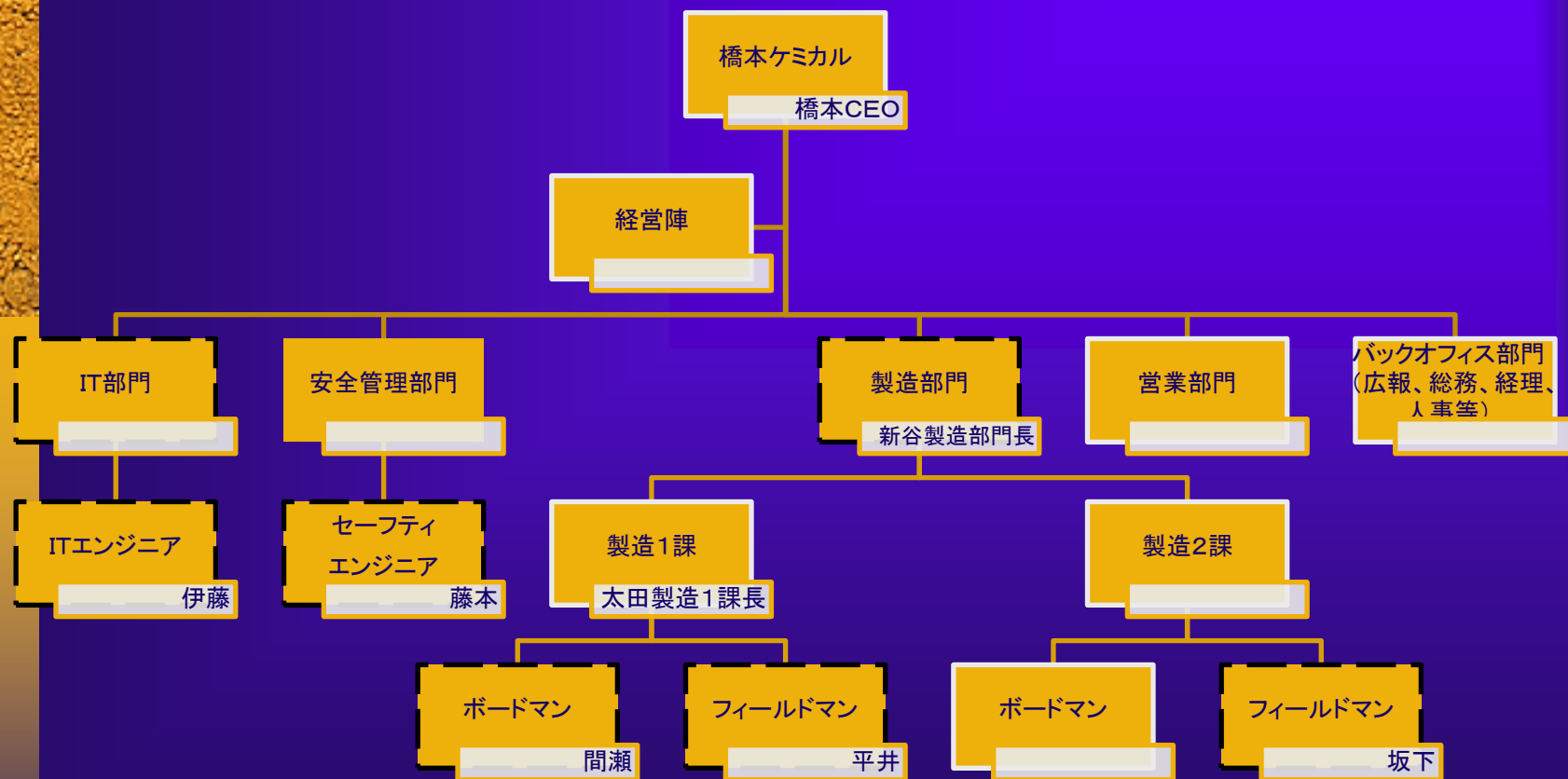
- OPCサーバを利用
 - OPC DataServer: OPC Svr0_1, OPC Svr0_2
 - Supervisory Zone に設置
 - プラント全体の監視用で操作はできない
 - コンソールは製造課長のデスクに置かれている
 - 常時監視されているわけではない
 - OPC SCADA Server: OPCsvr1_X, OPCsvr2_X (xはプラントNo.)
 - Control Zoneに設置
 - プラントXの監視と操作用に設置
 - コンソールは現場のControl Roomに設置
 - ボードマンが常時監視



前提条件: ネットワーク構成



前提条件:組織図



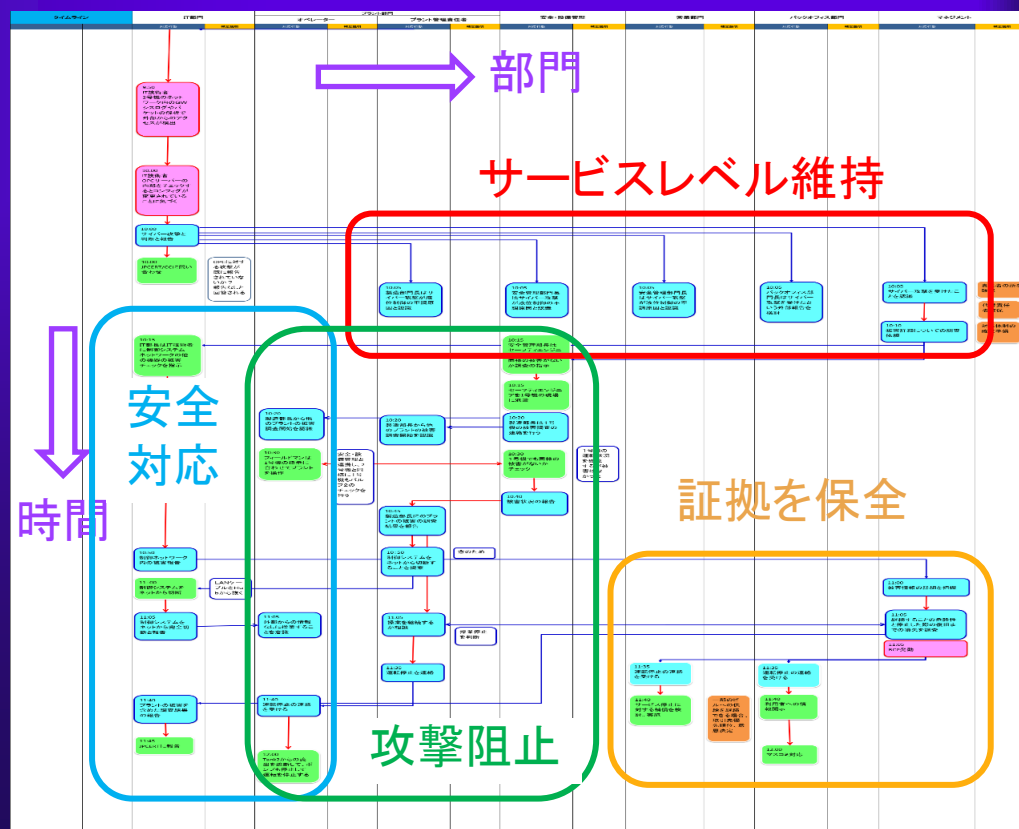
前提条件: 役割

- 製造部長
 - 他部門への連絡
 - 他部門からの情報を受けて意思決定
- 製造課長
 - 現場からの情報を受けて運転の指示
 - 上司への報告
 - 上司の指示に従い現場を指揮
- ボードマン
 - SCADAによる監視・操作
 - 現場への指示・確認
 - 異常事態発生時に上司に報告
- フィールドマン
 - 現場操作・確認
 - 現場情報をボードマンに連絡
- セーフティエンジニア
 - 安全に関わる緊急事態発生時に立ち会い
- ITエンジニア
 - ネットワーク機器の監視
 - ログの解析
 - 異常事態発生時に他部門に連絡



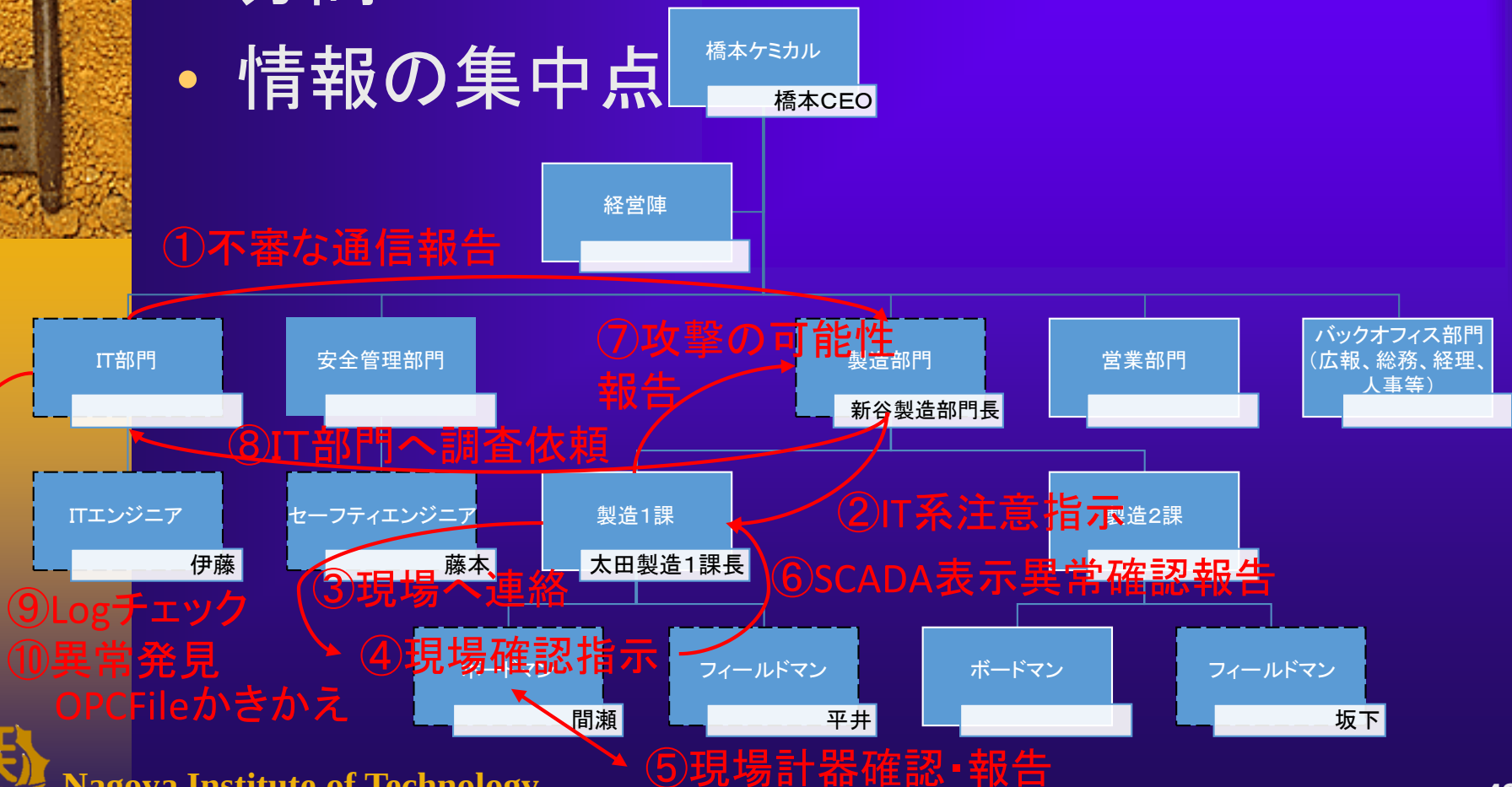
インシデント下の意思決定

- サイバーインシデント対応
 - 既存演習の分析結果から、インシデントマネジメントを重要視
- サーバー攻撃によって引き起こされた不安全状況への対応活動に以下を追加してシナリオ作成
 - ✓ 攻撃が擾乱する
安全対応を取り戻す活動
 - ✓ 攻撃で阻害される生産活動を、定められたサービスレベルを維持する活動
 - ✓ 更なる攻撃を阻止する活動
 - ✓ 攻撃の証拠を保全する活動



緊急時連絡体制

- 攻撃によってプラントが異常を示す10~30分間
- 情報の集中点



用意された演習シナリオ

予兆フェーズ

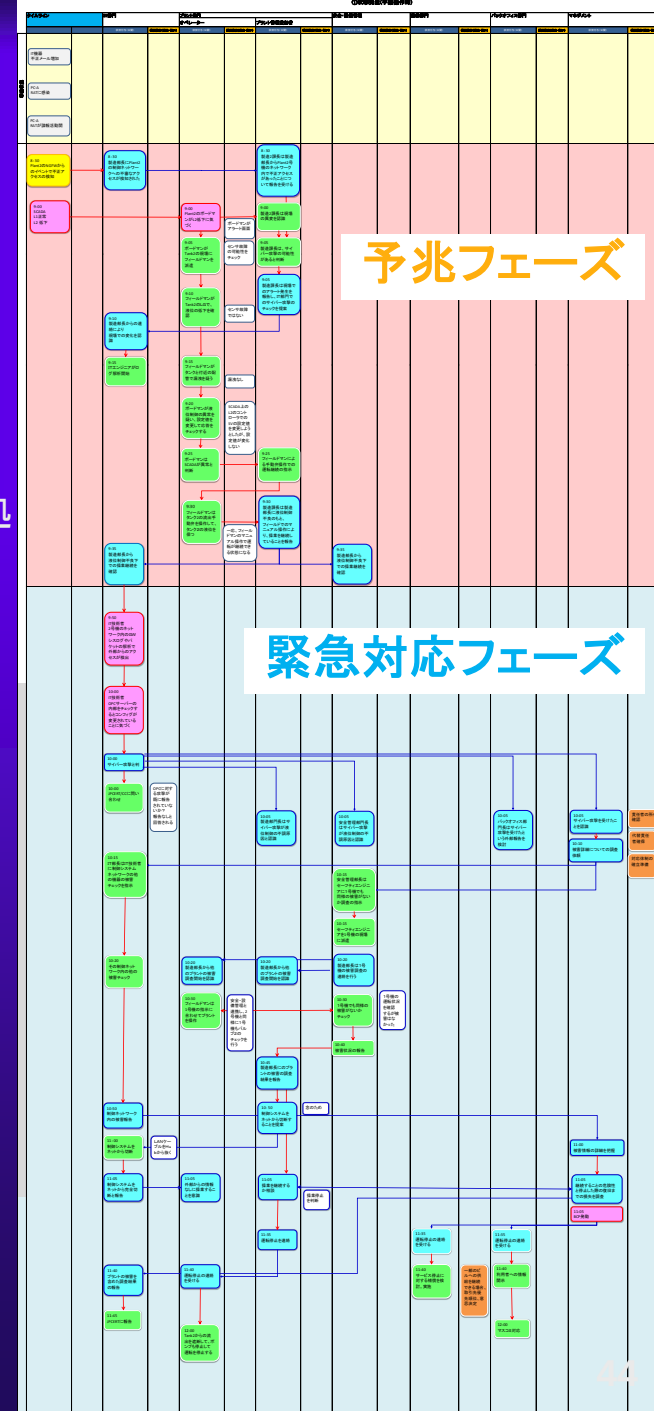
- 不正アクセスによる制御システム誤動作
 - この時点で異常の原因不明
- 運転部門
 - 誤動作によるプラント異常に対して安全対応処置を優先
 - 一応の小康を得る
- 現場IT部門
 - ログ解析開始

緊急対応フェーズ

- ログ解析により、異常原因をサイバー攻撃と特定
- 攻撃の影響把握
 - ターゲットとされたICS並びにプラント調査
 - 他プラントの保護対応
- 事業継続対応
 - 現状のサービスレベル把握(運転継続、停止)
 - ステークホルダ対応
- 証拠保全

予兆フェーズ

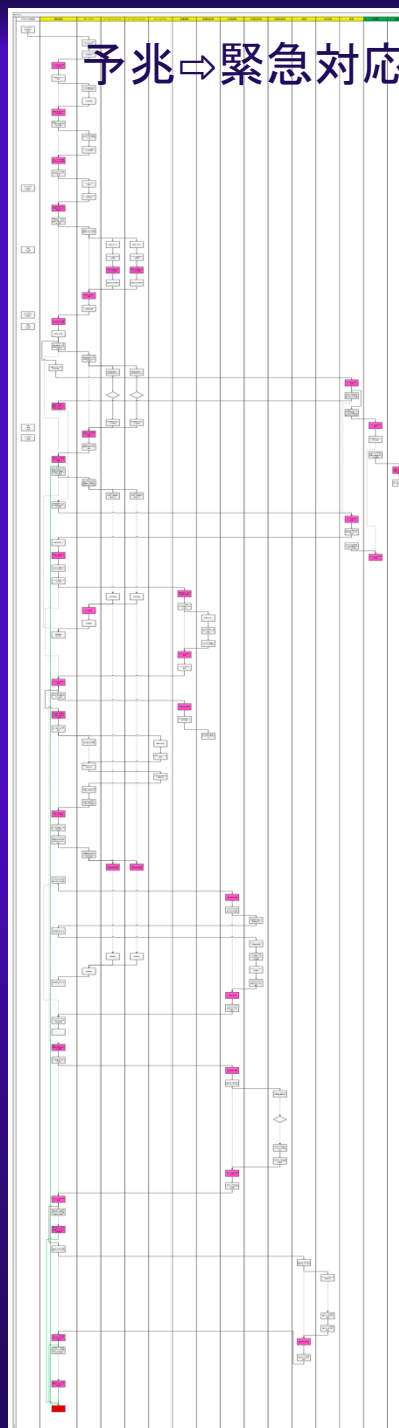
緊急対応フェーズ



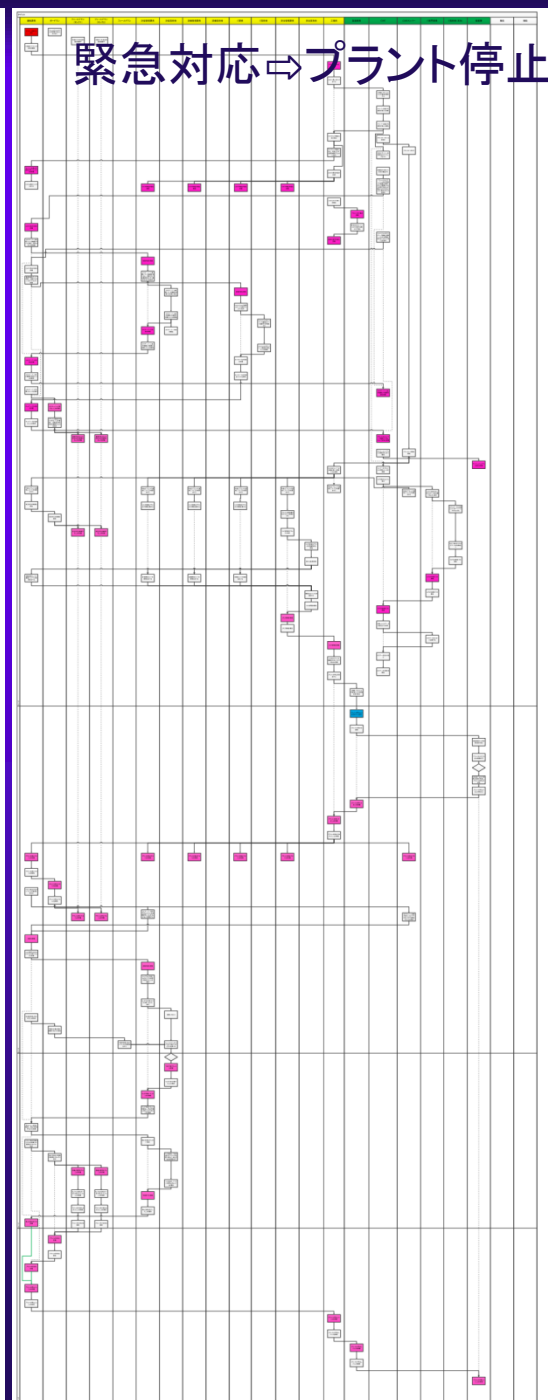
最新版 シナリオ



予兆⇒緊急対応



緊急対応⇒プラント停止





タイムライン		IT部門		プラント部門		安全・設備管理	
		オペレーター		プラント管理責任者			
		状況付与(公開)	補足説明(理由・狙い)	状況付与(公開)	補足説明(理由・狙い)	状況付与(公開)	補足説明(理由・狙い)
事前状況	IT機器 不正メール増加					予兆フェーズ	
	PC-A RATに感染						
	PC-A RATが諜報活動開始						
	8:30 Plant2のNGFWからのイベントで不正アクセスの検知						
	9:50 IT技術者 2号機のネットワーク内のGWシスログやパケットの解析で外部からのアクセスが検出					緊急対応フェーズ	
	10:00 IT技術者 OPCサーバーの内部をチェックするとコンフィグが変更されていることに気づく						

参加者が、ワークフローを作成

各フェーズの開始 インシデント対応ビデオによる初期条件の設定



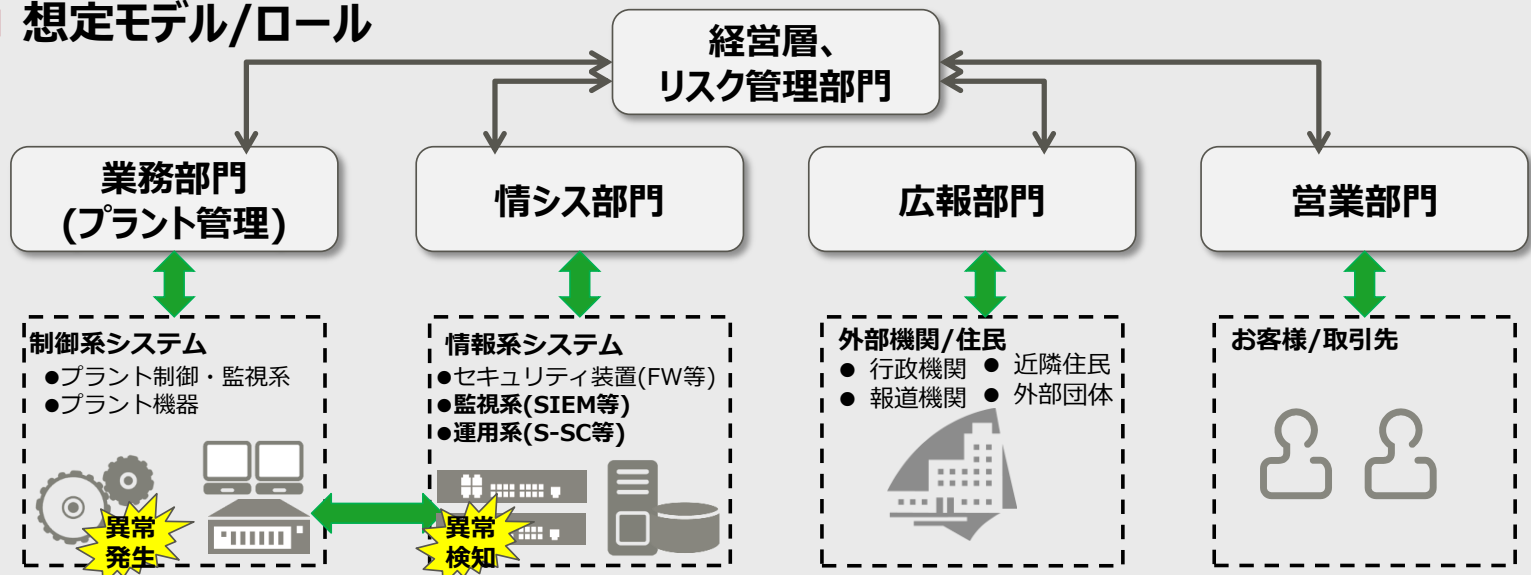
インシデントの発生から復旧
までのシナリオに合わせて、
インシデント対応フローを可
視化



参加者によるロールプレー

現場のインシデント対応だけでなく、部門連動のマネジメントを演習

■ 想定モデル/ロール





スタートポイント

- SIEM
 - NGFWからのイベントで不正アクセスの検知
 - SSCで検知をIT部門に連絡

演習結果：予兆フェーズ



状況

システム メッセージ

報告事項・ 連絡事項

行動

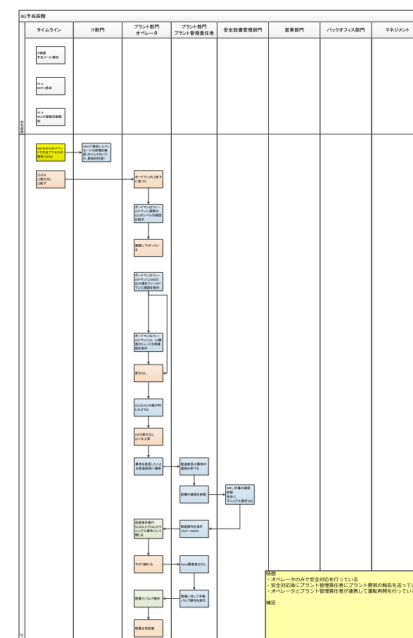
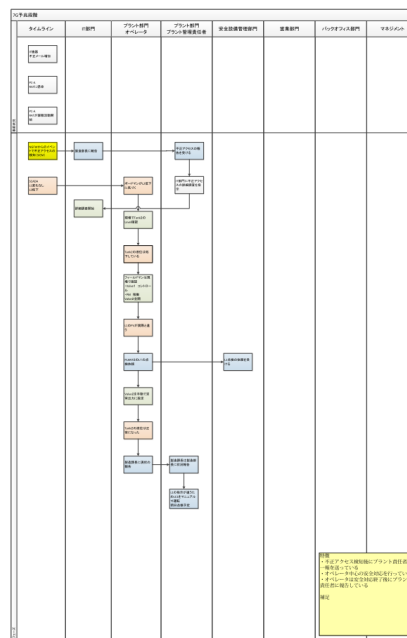
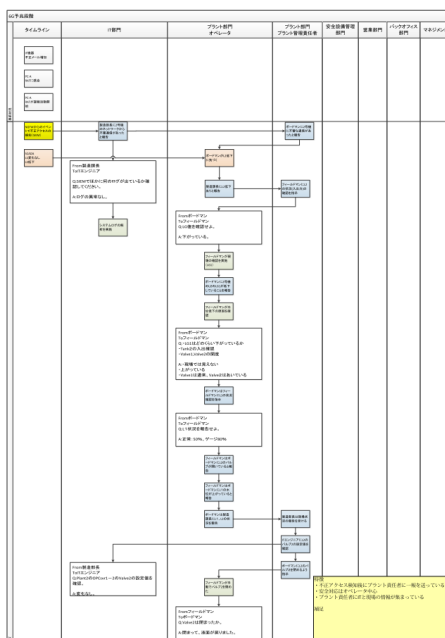
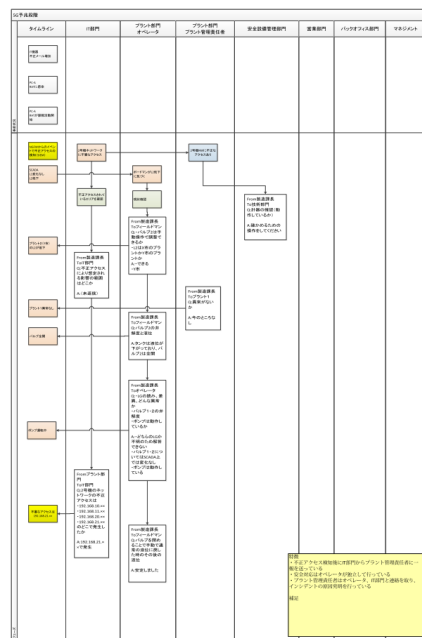
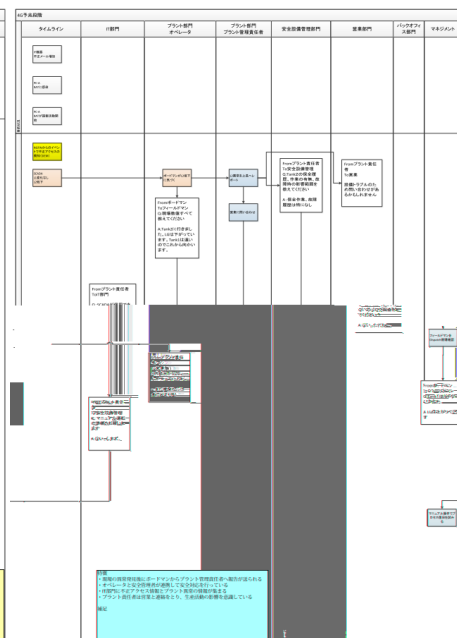
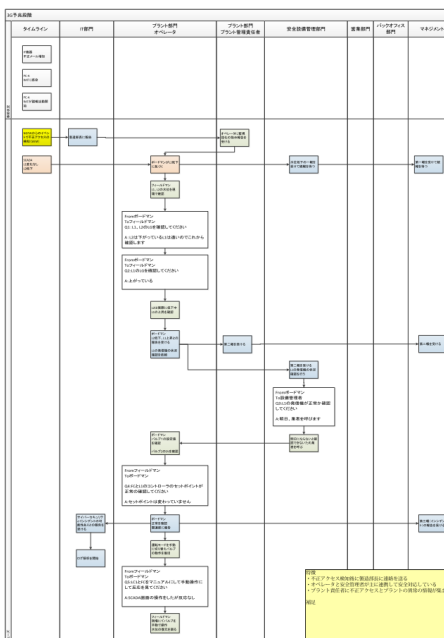
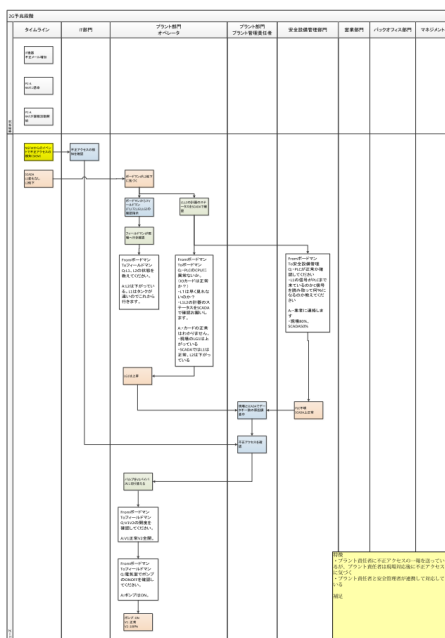
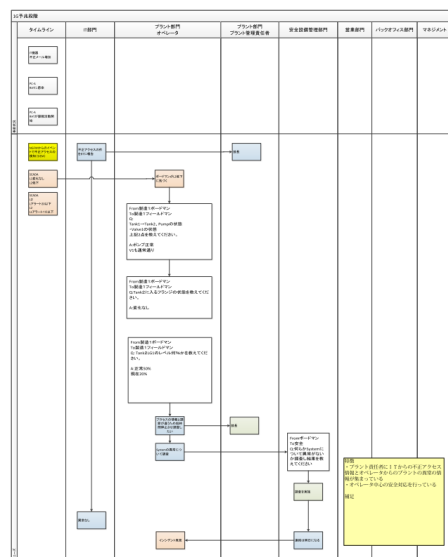
確認事項

16予選段階	タイムライン	IT部門	プラント部門 オペレータ	プラント部門 プラント管理責任者	安全設備管理部門	営業部門	バックオフィス部門	サポメント
業務内容	「I7業務 サブメール受信」							
	PCA NATO起報							
	PCA NAVIS警備活動開 始							
	NAOから出たイベント にやがてアラームも入 る(約3分後)	不正アクセスの件 を知らせる報告		調査				
	SCADA に通知なし の通り		ボーパマンの上り下 りに気づく					
	SCADA に 「アラート30秒」 あり は「アラート10分止T		From製造1ボードマン To製造1フィールドマン Q Tank1→Tank2、Pumpの状態 ・Valve1の状態 上記几点を確認してください。 A ポンプ正常 VVMも異常通り					
			From製造1ボードマン To製造1フィールドマン Q Tank2に入るフランジの状態を確認してく ださい。 A 変化なし					
			From製造1ボードマン To製造1フィールドマン Q Tank2(GL)のレベル何%かを教えてくだ さい。 A 正常50% 現在20%					
			プロセスの情報は認 知できず5分経過後 開始しようとする	調査				
			Systemの実況につ いて調査		Promボードマン To安全 Q 何かSystemに ついて異変がない か確認し結果をお返 せてください			
		異常なし。			調査と実施			
			インシデント発生		連絡先情報になり			
							付録 ・プラント責任者に1つからの不正アクセス 情報とオペレータからのプラントの異常の情報 が集まっている ・オペレータ中心の安全対応を行っている 補足	

タイムライン

[illegible]

予兆フェーズ





スタートポイント

- プラント部門オペレータ
 - 手動での運転を継続
- IT技術者
 - 2号機のネットワーク内のGWのシスログやパケット解析で外部からのアクセスが検出
 - OPCサーバの内部をチェックするとコンフィグが変更されていることに気づく

演習結果：緊急対応フェーズ



演習結果から

予兆フェーズにおけるオペレーション

- どのグループも、プラント挙動に基づいて、安全対応操作を実施
 - SCADA, 現場機器の読みのクロスチェック
 - AutoからLocalへの切り替え
 - 現場操作による対応等
- 迅速な状況確認を実施
 - 現場機器
 - SCADA、OPCサーバ

安全対応主体の行動に関しては習熟していると言える。



演習結果から

緊急対応フェーズにおけるオペレーション

- サイバー攻撃判明以降の対応がバラバラ
 - 現場指揮者
 - 直接対応部門
 - 間接対応部門との連携
 - 外部組織との連携
- 状況確認がほとんど実施出来ない
 - 把握すべき情報に対する準備不足
 - 情報取得に要するリソースに対する知識不足
 - 加速する事態に対するマネジメント能力不足



演習全体の振り返り

- 制御システムのセキュリティ対策を検討するとき、**何をどこまでやったらいいかわからない。**
 - 「脅威」⇒「対策」では、キリがない。「想定被害」⇒「対策」でバランス良い対策を。
 - 本当に必要な対策は何か？
- 「人」の判断は重要であるが、**全て「人」に頼るのは危険**である。
 - **早く検知して、早く対処する**ために、自動でできる対処は「ツール」に任せることも考慮に入れる。
 - **ツールを使えば自動でできるプロセスはどこか？**
- セキュリティ課題は、ツールを入れるだけでは解決しない。
 - 特に、制御系システムの場合、IT部門と制御システムを運用する現場との連携が必要。
 - さらに事態が深刻となった場合、マネジメント層、広報等を巻き込んで会社全体の連携が重要となる。特に、**誰が責任を持って判断するのか**を明確にするのが重要。
- 自社にとっての**制御系CSIRT**(Computer Security Incident Response Team)の必要性を検討する。
 - **どのような機能を持つCSIRTが必要か？**





- 攻撃者の心理を突く対策「Cyber Active Deception システム」
- 大型ハニーポット(中小企業サイズ)
- 大規模モニタリングシステム

早期警戒システム



対応の構図

A) 攻撃側・防御側共に活動がない状態

システムの脆弱さ、攻撃の頻発化を考慮すると、安心していられる状況ではない。したがって、脆弱性や異常にすぐ反応できる人材の訓練等、**インシデントに備える活動を継続する**必要がある。

B) 防御側にのみ活動がある状態

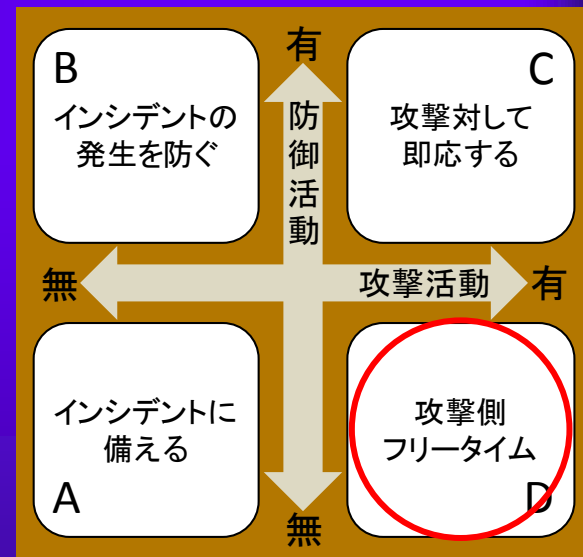
防御側が能動的に自身のシステムの脆弱性を探し、修正していくことで、**インシデントの発生を未然に防ぐ**必要がある。

C) 攻撃側・防御側共に活動がある状態

攻撃側の活動に気づき、さらに攻撃が進まない様に**相手に合わせて対応していく**必要がある。

D) 攻撃側にのみ活動がある状態

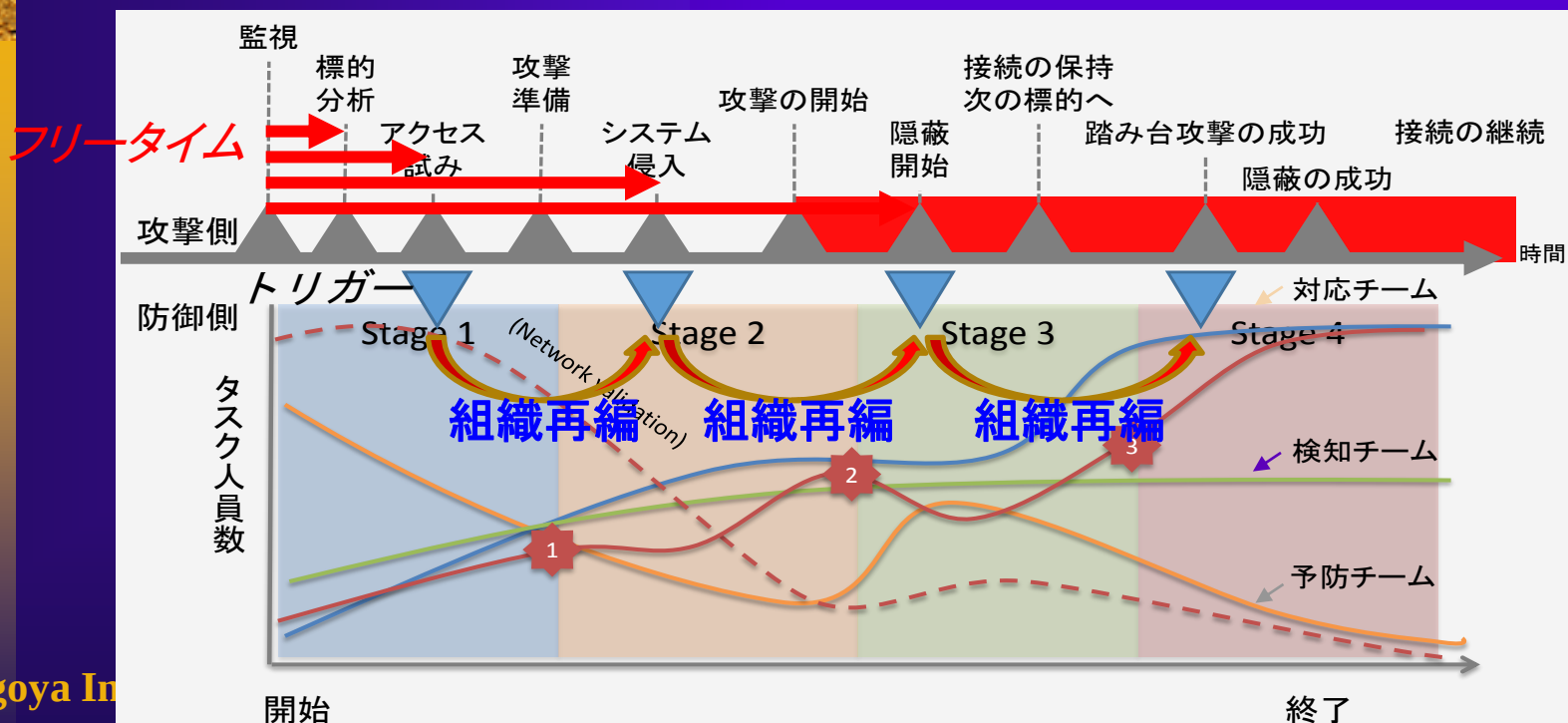
攻撃側がシステムに潜伏していることに気がついていない状態であり、**最も危険な状態**であると言える。



- 出来れば避けたい。
- なるべく、短時間に抑えたい。
- 攻撃者に無駄に時間を使わせたい。

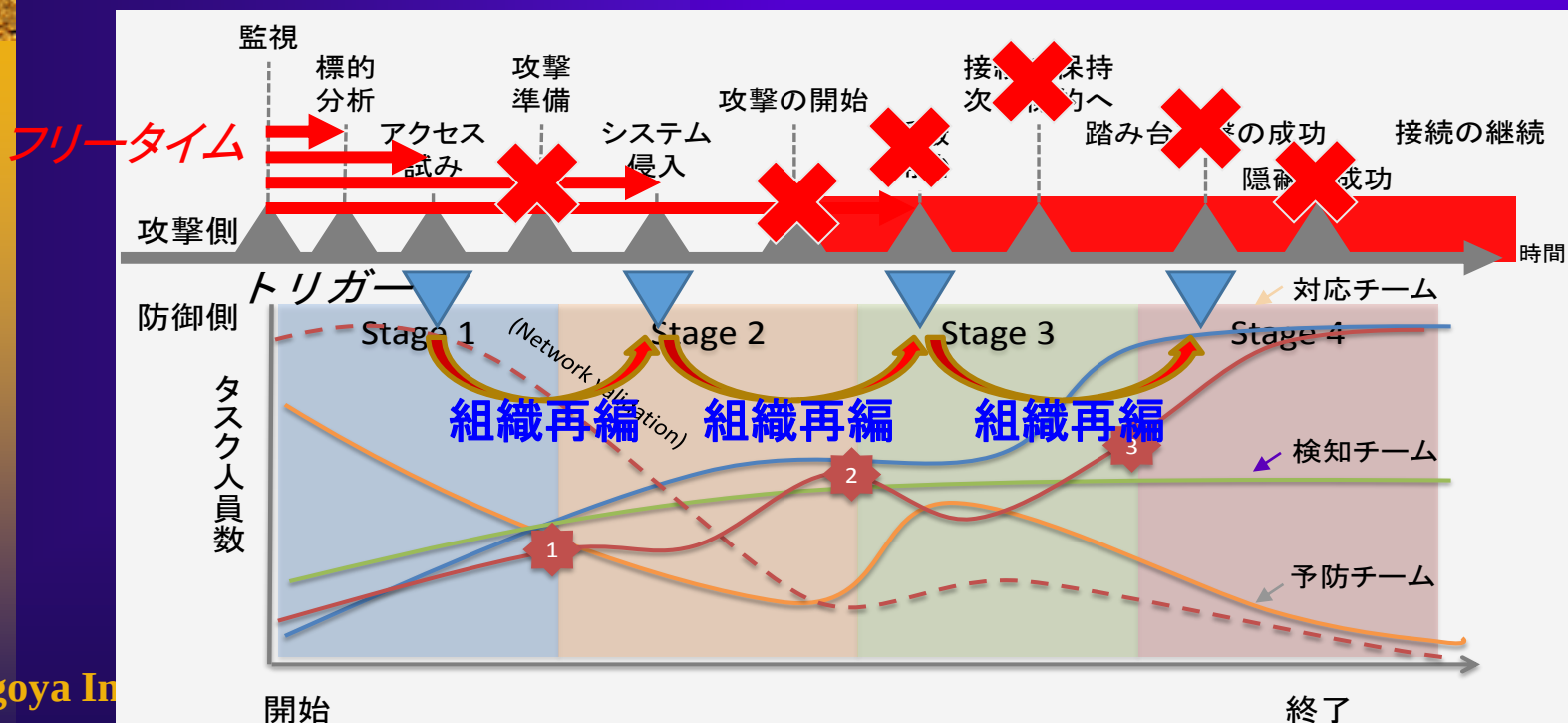
サイバー攻撃への防衛体制

- 攻撃の進捗に合わせ、体制を変更する必要がある。
 - 体制の切り替えには時間が掛かる。
- 不適切な体制では、攻撃者にフリータイムを与え、事態が急変する状況下で対応に混乱が生ずる。
 - 必要な資源の不足→対応に遅れ→攻撃者に先行を許す



サイバー攻撃への対応

- 攻撃の早期警戒によって、攻撃側にフリータイムを与えないこと
- 攻撃側にフリータイムを許したとしても、重要インフラの各構成要素間で行われるやり取りを系統的に把握させないこと



攻撃者に攻撃を断念させる防御方法

- フリータイムを無駄に使わせるには
 - 攻撃者が予想したモノを提供する
 - 脆弱性を整えた、魅力的なターゲット
 - 攻撃者を混乱させる
 - 確定的・系統的な情報を与えない
 - 入手した情報の信憑性に疑問を抱かせる
- フリータイムを無駄に使わせることで
 - 攻撃を検知する時間的余裕を生み出す
 - 収集情報から攻撃のプロファイリング
 - 攻撃に対処する時間的余裕を生み出す
 - 組織的対応を可能とする



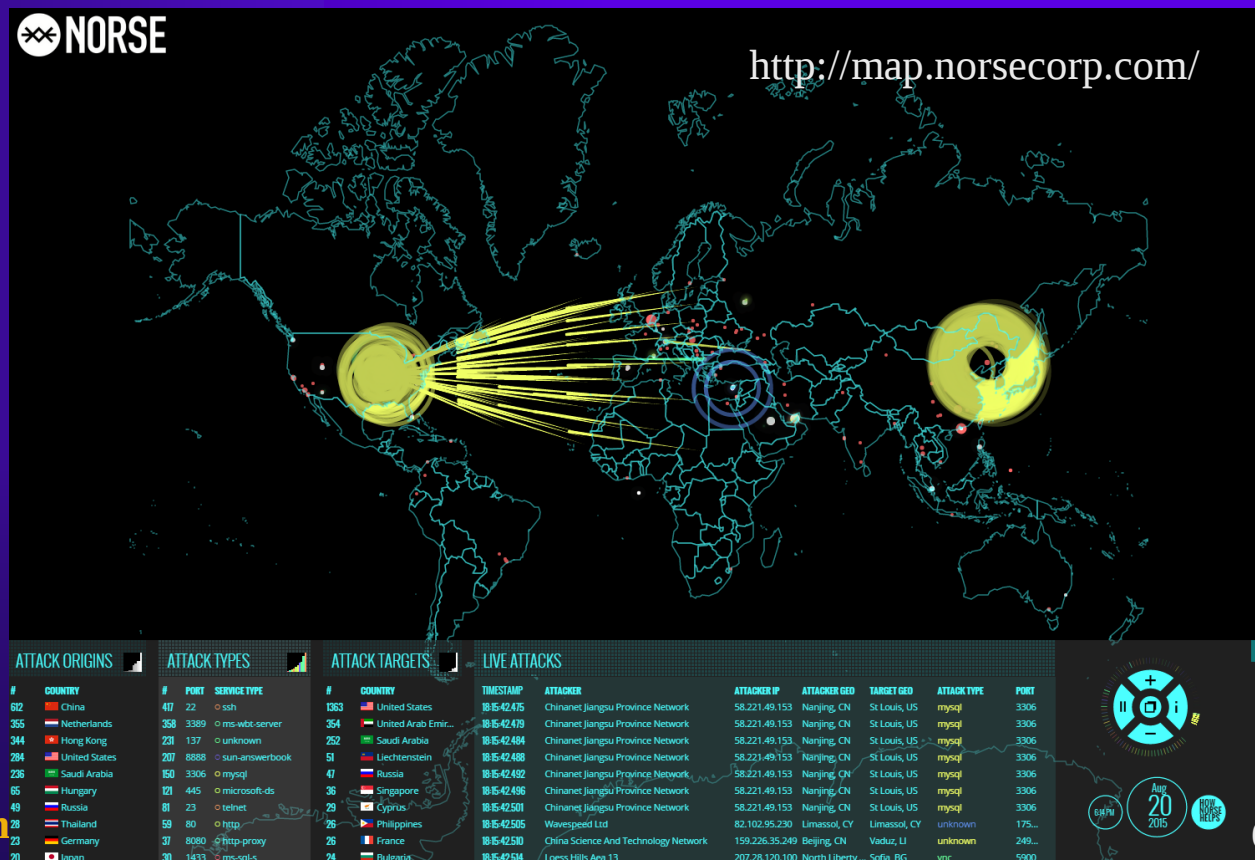
HoneyPot: 攻撃者をおびき寄せる罠

- 高対話型Honeypot
 - 意図的に脆弱性を残した、実際のコンピュータを利用
 - 実際にサービスを運用し、攻撃者の手法や侵入者の行動など、高度な情報を得る
 - ただし、侵入されたHoneypot自体が踏み台にされるなど、不正アクセスを助長させるリスクも高い
- 低対話型Honeypot
 - 特定のOSやアプリケーションをエミュレートし、監視を行う
 - エミュレートした範囲に機能が制限されるため、高対話型に比べて、比較的、安全に運用ができる
 - ただし、機能を限定しているため、情報量は落ちる



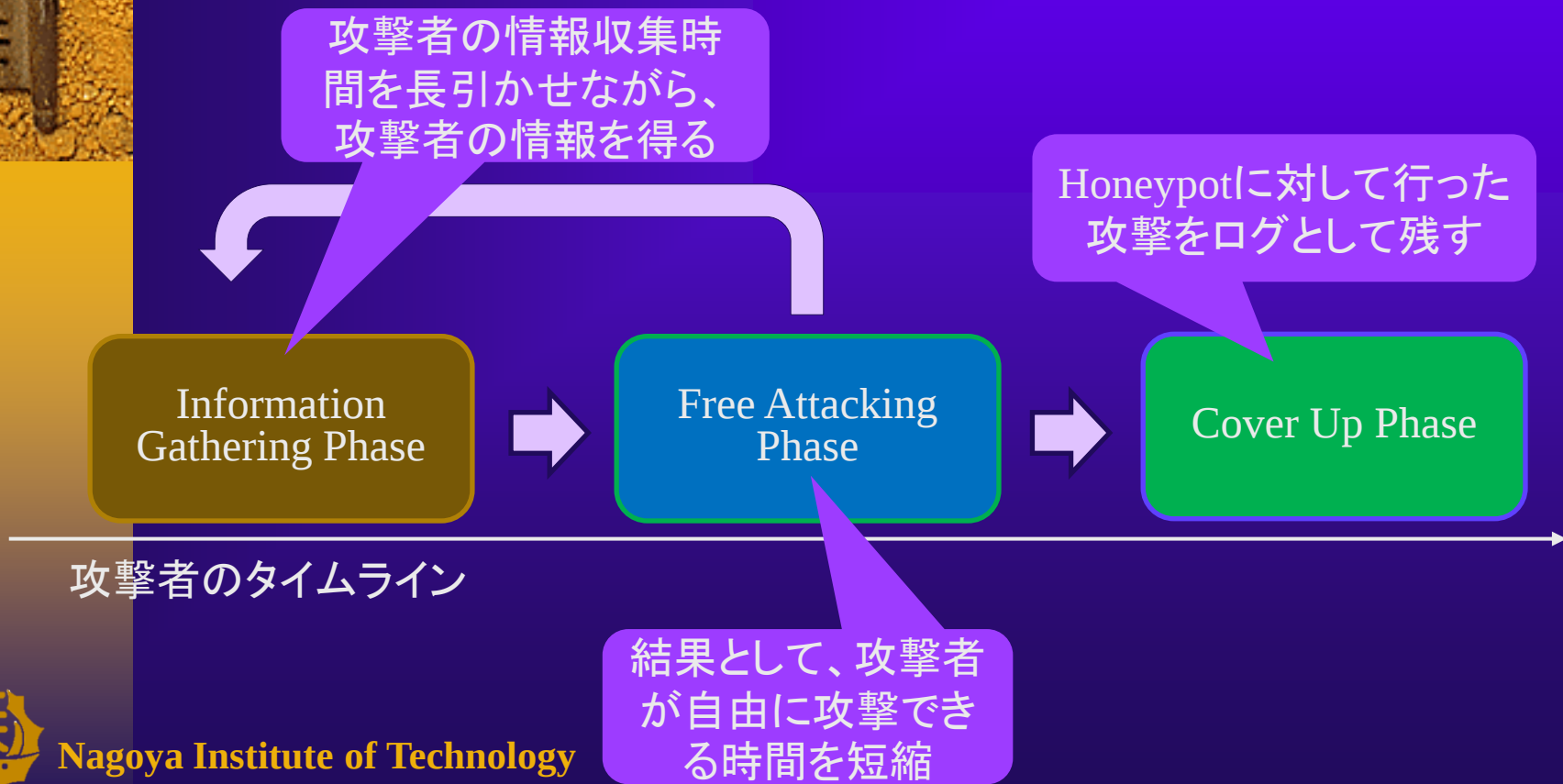
HoneyPotの活用例: Norse Attack Map

- 米国セキュリティ企業 Norse社が提供する世界のどこから、どこへ、サイバー攻撃が行われているかをHoneyPotの情報からリアルタイムで可視化するマップ



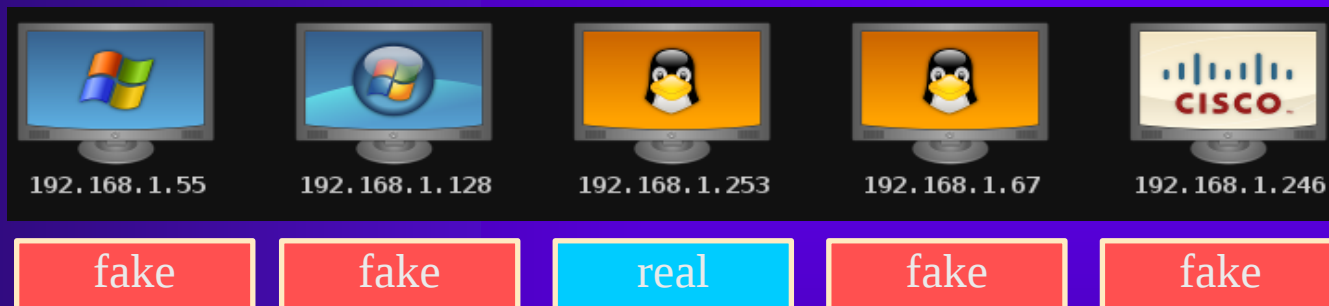
提案するCamouflageNet

- 低対話型Honeypotを使用した攻撃者錯乱ツール

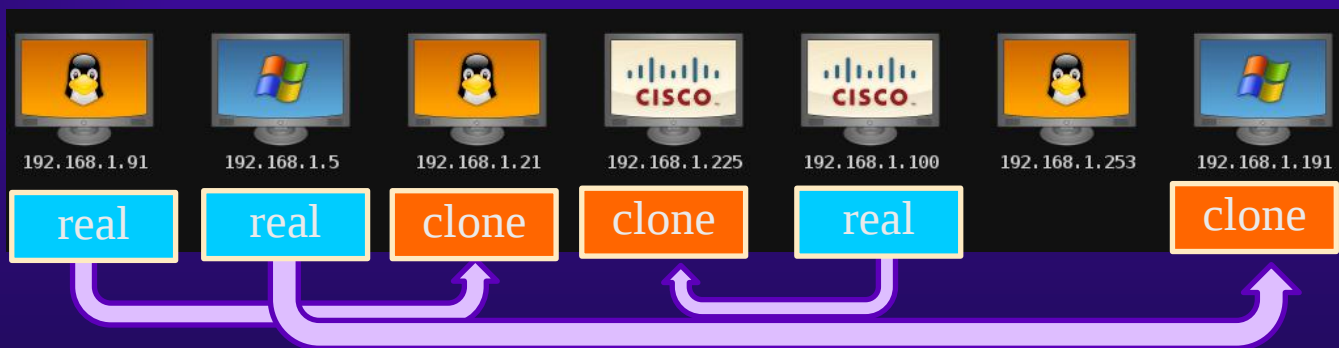


攻撃者を混乱させる機能(1)

- 実際には存在しない偽の仮想端末(fake)を生成
 - 実際のネットワークに比べて、巨大なネットワークに見せかける



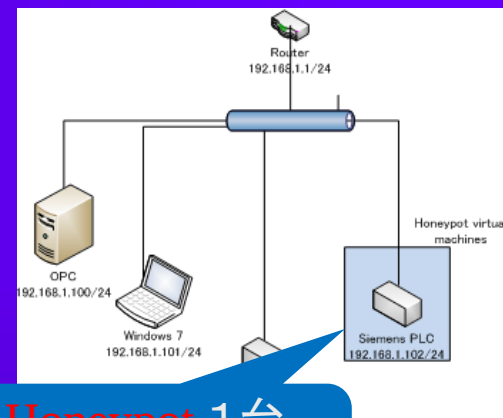
- 実際に存在する端末のプロフィールをクローンしたHoneytrapを生成
 - どの端末を攻撃すべきかを不明瞭にする



実機を模倣して配置

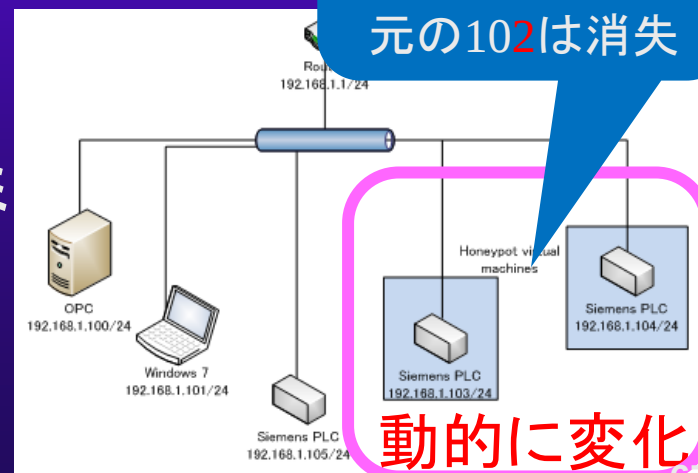
攻撃者を錯乱させる機能(2)

- ICSネットワークの動的変化
 - 攻撃検知等のトリガにより、**Honeypotの構成を変更**
 - 静的なはずのICSのネットワーク構造が、動的に変化することで攻撃者を錯乱させる
- 有効性を高めるには、
 - 動的変化を生じさせるタイミングが重要



Honeypot 1台
192.168.1.102/24

Honeypot 2台
192.168.1.103/24
192.168.1.104/24
元の102は消失



動的に変化



CamouflageNetの試作機

- ソフトウェア

- “honeyd”(+独自プログラム)
 - Low interaction honeypot
 - Emulate numerous virtual machines
 - Not to run real service
 - Define the fingerprint

- ハードウェア

- “RaspberryPi”
 - Linux
 - High performance
 - High mobility
 - Open I/O ports



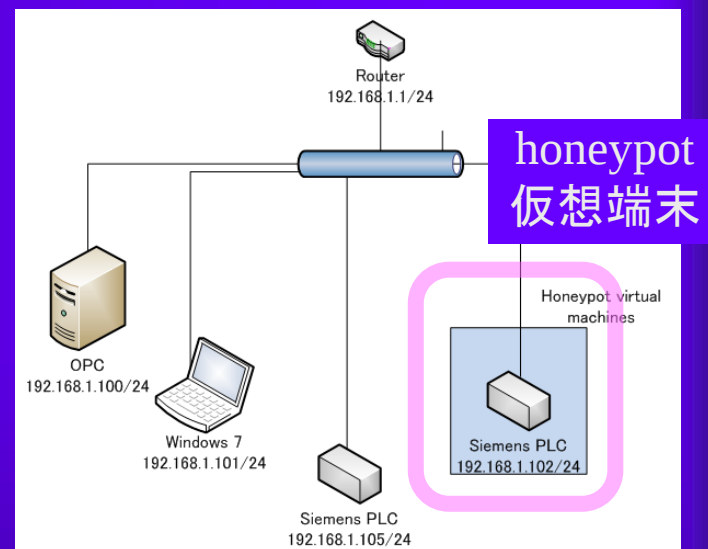
攻撃の可能性がある異常の検知機能

- 前提条件

- ICSにおいて、honeypotは、通常時は通信しない
- honeypotと通信が発生
→ 異常の発生

- 異常検知

- Honeypotに対する通信パケットを監視



timestamp

protocol

source

destination

```
2015-03-17-03:04:13.183 | honeypot log started -----
2015-03-17-03:04:41.751 | tcp(6) - 192.168.1.1 55690 192.168.1.21 554: 44 S
2015-03-17-03:04:41.769 | tcp(6) - 192.168.1.1 55690 192.168.1.191 554: 44 S
2015-03-17-03:04:41.773 | tcp(6) - 192.168.1.1 55690 192.168.1.225 554: 44 S
2015-03-17-03:04:41.775 | tcp(6) - 192.168.1.1 55690 192.168.1.21 5900: 44 S
2015-03-17-03:04:41.781 | tcp(6) - 192.168.1.1 55690 192.168.1.21 53: 44 S
2015-03-17-03:04:41.783 | tcp(6) - 192.168.1.1 55690 192.168.1.191 5900: 44 S
2015-03-17-03:04:41.788 | tcp(6) - 192.168.1.1 55690 192.168.1.225 5900: 44 S
2015-03-17-03:04:41.789 | tcp(6) - 192.168.1.1 55690 192.168.1.21 80: 44 S
2015-03-17-03:04:41.793 | tcp(6) - 192.168.1.1 55690 192.168.1.21 3389: 44 S
2015-03-17-03:04:41.802 | tcp(6) - 192.168.1.1 55690 192.168.1.191 53: 44 S
2015-03-17-03:04:41.806 | tcp(6) - 192.168.1.1 55690 192.168.1.225 53: 44 S
2015-03-17-03:04:41.808 | tcp(6) - 192.168.1.1 55690 192.168.1.21 993: 44 S
```



camouflageNet の使用例

- camouflageNetは、ICSの可用性を損なう事がなく、あらゆる箇所に設置可能で、設置障壁が低い
- 他のセキュリティツールと組み合わせる事で、さらなる効果を期待できる

Without camouflageNet

```
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .  
Nmap done: 256 IP addresses (6 hosts up) scanned in 232.59 seconds
```

43倍設置

32倍スキャンに
時間が必要

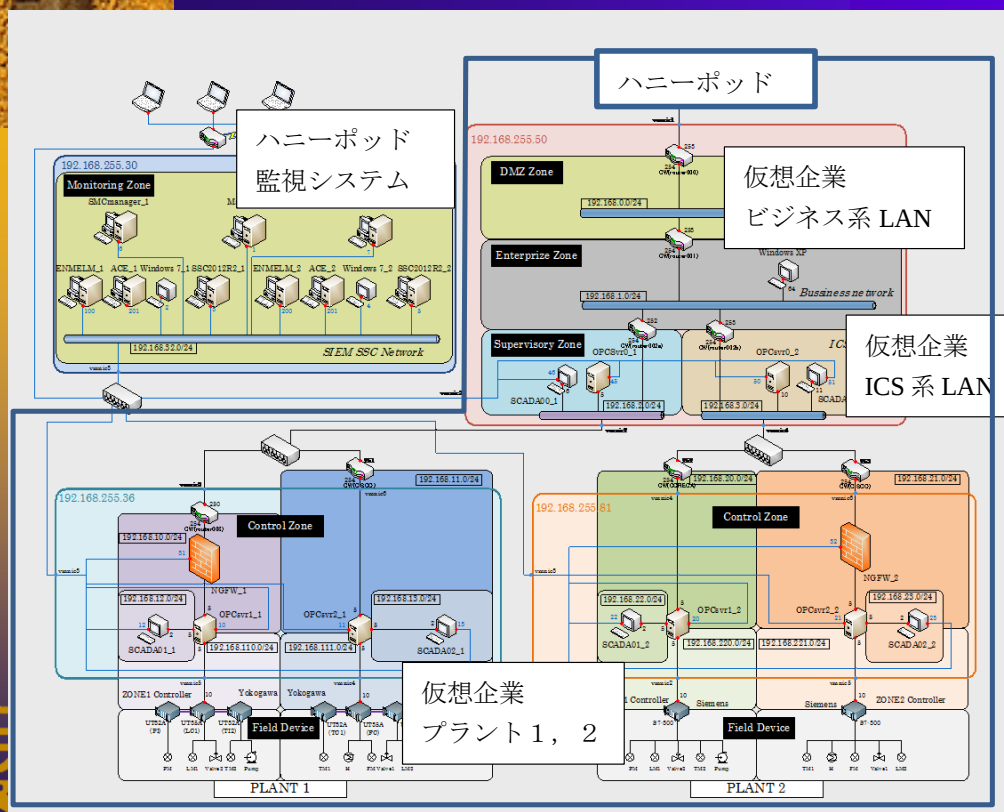
With camouflageNet

```
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .  
Nmap done: 256 IP addresses (254 hosts up) scanned in 7230.17 seconds
```



大規模ハニーポットによる攻撃者の攪乱

- 仮想環境を用いて大規模なハニーポットを構築し、仮想の事業所を攻撃させ、攻撃者の手口などの情報を得る。
- 企業においては、このハニーポットを事業所ごとに分散配置し、集中的に監視する体制をとることで、全社的な対応を迅速にとることにつながる。

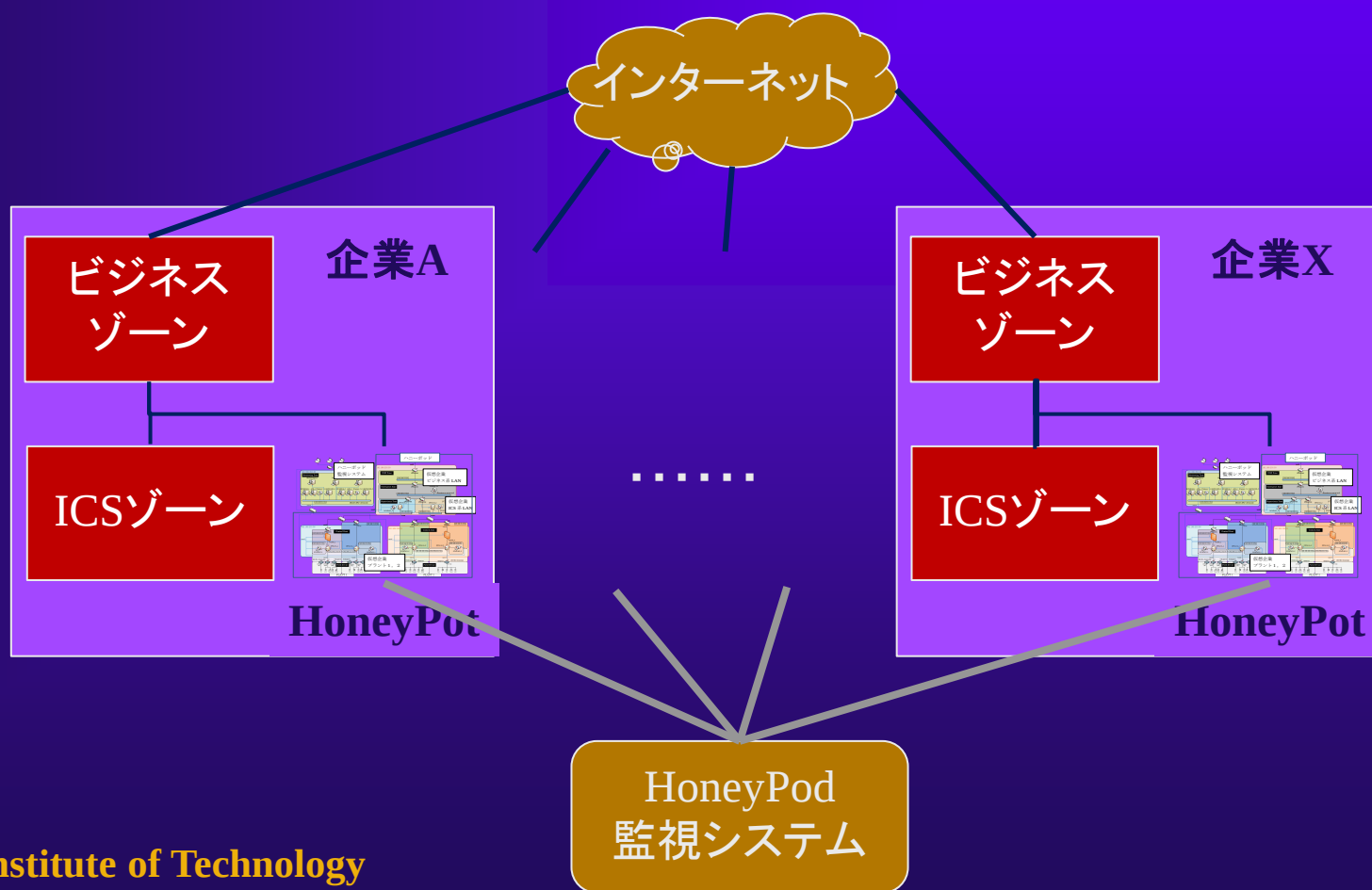


- ハニーポッドと監視システム
- を組み込んだ試作機



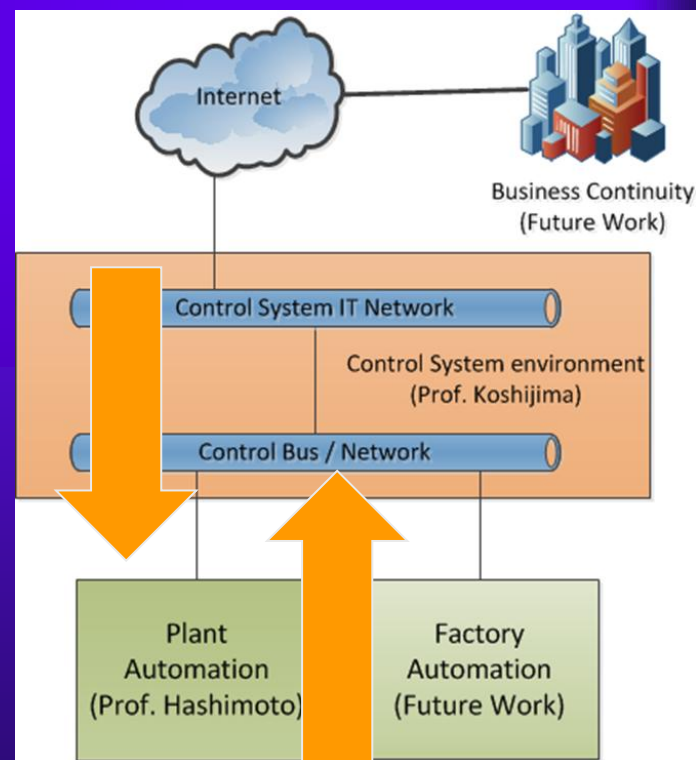
大規模モニタリングシステム

- HoneyPotを事業所ごとに分散配置し、集中的に監視することで、全体的対応を迅速にとることを可能にする。



制御システムセキュリティチーム研究では

- 攻撃者の視点で
 - サイバー攻撃を妨害・阻止するための Cyber Active Deception システムの開発
 - ICS用侵入検知システム
 - 教育プログラムの開発
 - ICS-BCP/BCM
- 防御者の視点で
 - テストベッドの構築
 - サイバー・タグアウトシステムの開発
 - 動的ゾーニングシステム
 - Software-Defined Network
 - クラウドを利用したセキュアでフレキシブルなコントローラの実現
 - 仮想環境を利用したローカルコントローラのBackup Recovery Updateサポート





利便性と安全性のトレードオフ

サイバーセキュリティの評価基準 (ISA 99.01.01)

1. Access control (AC):
システムの使用前にユーザー認証・許可を行う
2. Use control (UC):
ユーザーのリクエストを実行する前に権限を求める
3. Data Integrity (DI):
伝達・保持中のデータの不正操作を防ぎ完全を保つ
4. Data confidentiality (DC):
伝達・保持中のデータの拡散を防止し機密性を保つ
5. Restrict data flow (RDF):
データのやり取りをゾーン内に限定し、システムのセグメント分けを行う
6. Timely response to an event (TRE):
インシデント発生時に侵入を伝え、証拠を集め、即座に正しい行動をとる
7. Resource availability (RA):
システムの可用性を確保



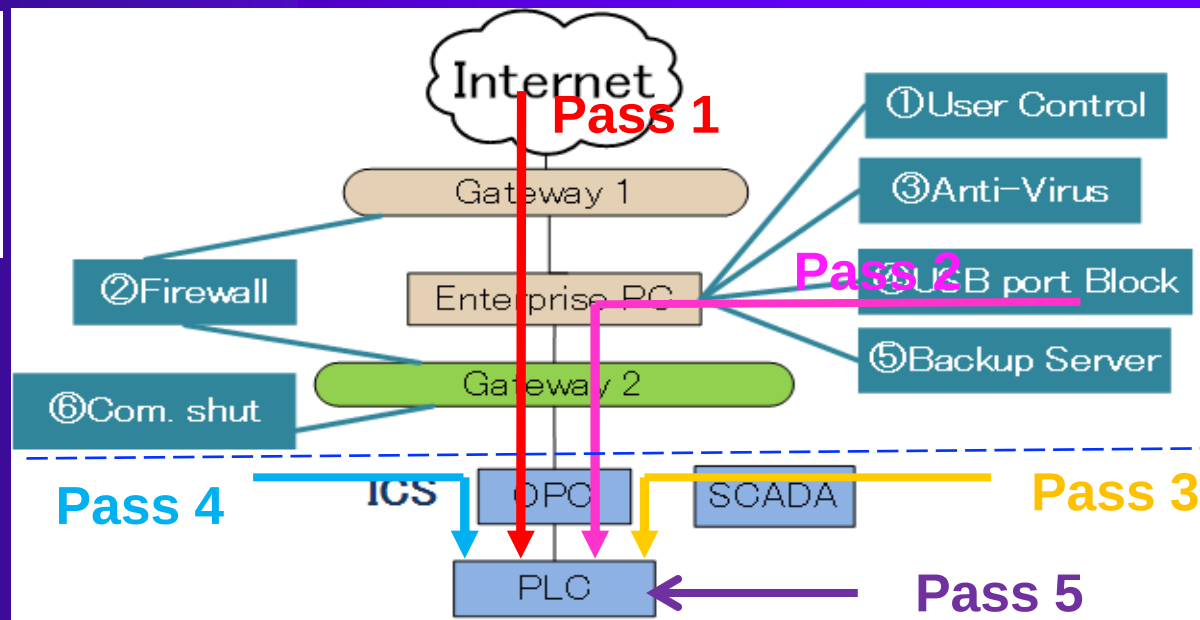
Q

対策ツールの種類と配置の選択

利便性と安全性のトレードオフ

評価ルール:

すべての侵入経路で少なくとも1つのツールが配置される(ISA99).



評価基準

	AC	UC	DI	DC	RDF	TRE	RA
Gateway 1			②	②	②		
Enterprise PC	①	①	③, ④	①, ③, ④		③, ⑤	⑤
Gateway 2			②, ⑥	②, ⑥	②, ⑥		
OPC							
SCADA							
PLC							

侵入経路

守るべきPLCに対して、経路1又は2から侵入された場合には、すべての要件が満たされるように対策を用意した。

しかし、経路3, 4と5から侵入された場合、対策は存在しない！



Nago

おわりに

- 現実
 - 攻撃を100%防ぐことはできない。
 - 組織的対応に入るまでには時間がかかる。
- 対応
 - 時間稼ぎ
 - 攻撃者にフリータイムを与えない
 - 攻撃の早期発見
 - フリータイムの浪費
 - 自動化
 - 現場での緊急対応チーム、サイバーインシデント対応チーム
BCMチームの役割分担
 - 情報の集中・展開先のコントロール
 - 命令系統のコントロール

