IoTの革新性と制御システムの将来像

橋本　芳宏
名古屋工業大学 社会工学科
hashimoto@nitech.ac.jp

Internet of ThingsはBuzzwordとして、
ここでは、その定義は問題とせず、
IoTがもつ革新性についてまず触れる

さらに、その革新性を活かすための重要な課題のひとつであるサイバーセキュリティを考慮したうえで、
コントロールシステムの将来像について論じる

産業戦略の議論に対して、なんらかの参考になる情報となることを祈る

IoT(Internet of Things)

「もの」が「共通の場」に「つながる」ことに
どのような革新性があるのか？

IoTの推進技術

通信技術の進歩
・移動体通信

1G (アナログ)	1979～
2G (28.8KBPS)	1993～
3G (14MBPS)	2000～
LTE (110MBPS)	2006～
4G (100~200MPS)	2012～
5G(10～50GBPS)	2020～

・4Gでは、フル尺の映画ファイルを
ダウンロードするのに8分以上かかるが、
5Gでは5秒以下
・消費電力も低下している。
RFIDタグは、電池不要

光通信、インターネットの普及
IPv4(32bits　43**億)から**
IPv6(128bits=3.4×10^38)
すべてのものに固有番号を付加しうる

クラウド
・膨大なサーバー数、データ数
・容易なデータ利用アプリ
・AWS、Azure、i-Bress、ThingWorkなど

スマートデバイス、各種センサの
小型・安価化
・RaspberryPi等

デジタルカメラの高解像度、高速化
画像処理技術の進歩
(顔認識、動体追従など)

3Dプリンタ
樹脂だけでなく、金属加工

IoTによる「もの」の革新

⓪ 手動、風力、馬車

① 蒸気機関による大量生産運輸　**産業革命**

② 電動（コンパクト、強力、コントロール容易）

③ プログラム（マイコン制御、オートメーション）

④ インテリジェントが、もの自身からクラウドへ

つながることの革新性

（機能、CPU,メモリ、センサの制限がなくなる）

④って何？

例）iPhoneのSiriは
つながって作動

「もの」からインテリジェントが離れると？①

マイコンジャーの場合

(課題)　富士山の頂上では、うまく炊けない

革新前のカイゼン

→気圧計をマイコンジャーに追加

→マイコンのCPUを更新し、メモリを追加

革新後

→クラウドに通信し、ジャーの場所を特定

→場所の情報から、気圧を推定

(他人のセンサーや気象庁情報から)

→クライドで、気圧に応じた加熱条件を算出

→ジャーでローカルな温度制御を実現

通信とシンプルな機能があれば
ジャーにセンサーを追加することも
CPUやメモリの強化も必要ない

「もの」からインテリジェントが離れると？②

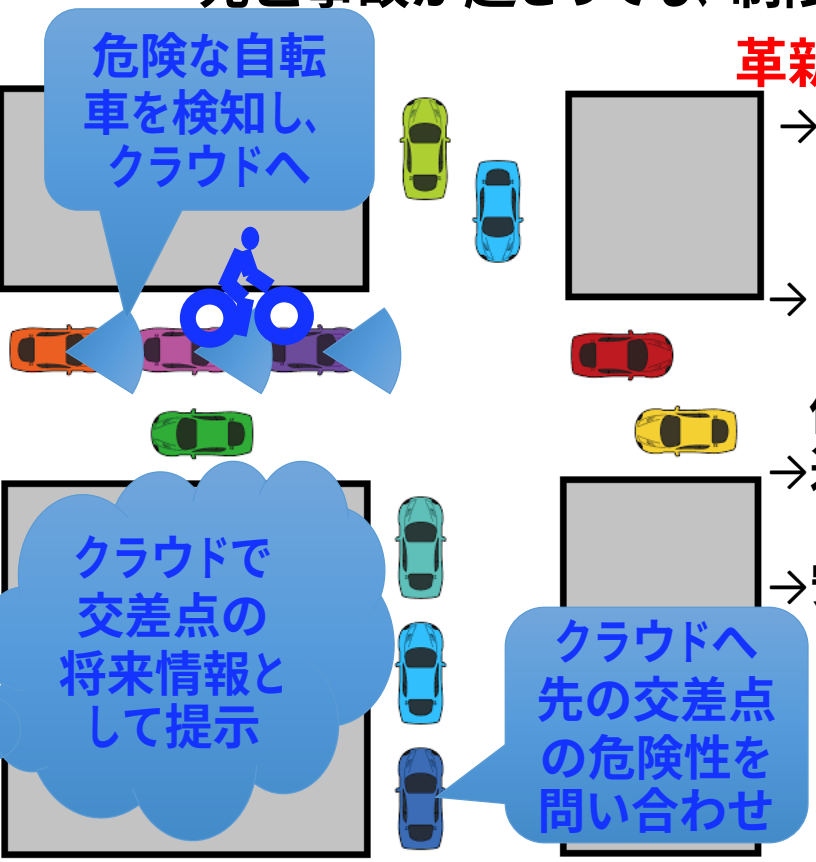
自動運転の場合

(課題)　ビルの陰から暴走自転車は出てこないか？

自動車ではなく、自転車がミソ？

革新前？

→事故は、どうせ人間でも避けられない。
　死亡事故が起こっても、制限速度を守っていれば、こちらは悪くない？



革新後

→先行車両だけでなく、他の走行中車両から走行先の交差点での情報を**予測**し、危険の予知を行う

→自車両のブレーキ等の操作を情報をもとに実施するとともに、クライドに通信し、他車両への情報も提供する

→道路情報、地図の更新を車両から得る
　Google Mapは渋滞情報をリアルタイム表示

→安全向上だけでなく、燃費向上などさまざまな効果が期待できる

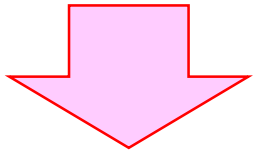
車両に最低限の安全保持機能は必要だが
クラウドからの情報は、将来予測も含めて
自車両への投資と無関係にリッチになりうる

IoTの革新性

クラウドにインテリジェントが移ると

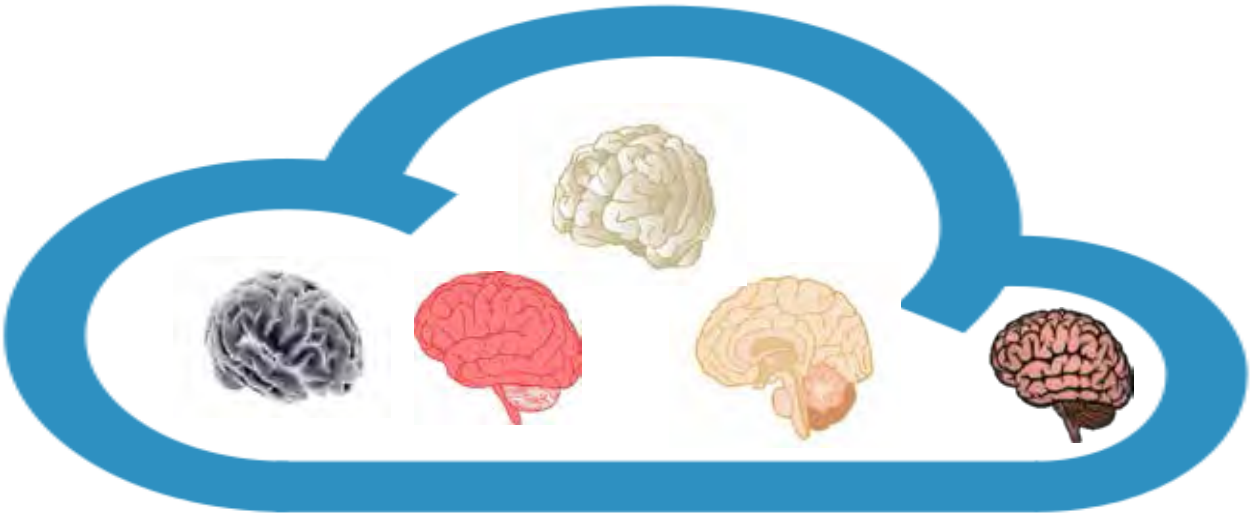
- 物理的
  (CPU,メモリ、HDDなど)
- 空間的
  (世界中のデータにアクセス)
- 時間的
  (現在、過去だけでなく、将来の予測・提案も)

制約から解放され、世界が広がる

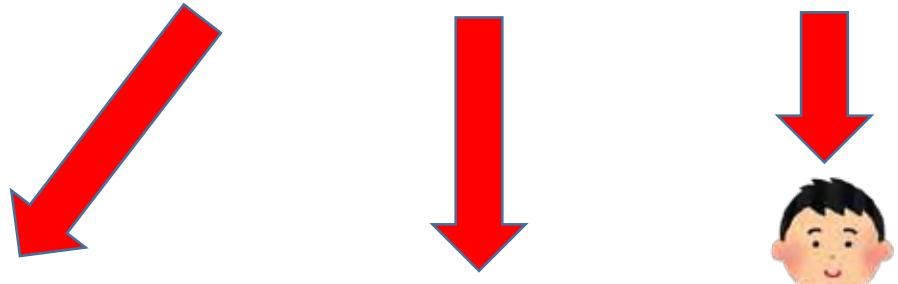


イノベーション

クラウドでのアイデア勝負



クラウドでは
さまざまな頭脳が
互いに影響して
成長するとともに
新たな発想の
頭脳が生まれる

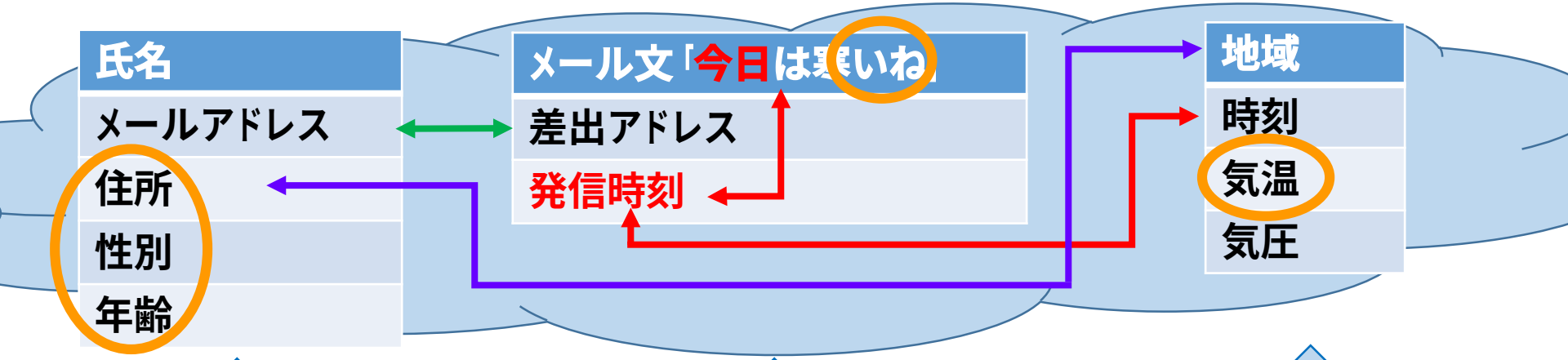


車体はトヨタ製だが
頭脳はGoogle？

IoTで情報を
アップするだけでなく
ダウンしてこそ革新

クラウドでの情報の活用

- メールから文章をたくさん集めるだけでは情報にならない。
- **リンク**をたどることで、暖房機器のマーケッティングに利用できる**情報**にもなりうる。



そもそもは、それぞれの目的で収集したデータ

個人情報保護法、プライバシー！

情報の組み合わせでイノベーション

- **システマティックなイノベーション**をめざすには、
  （場当たり的なカイゼンではなく）
  従来になかった情報の組み合わせが可能性を高める。
- 他の業務の構造的に整理された情報を**うまく選別し、有効利用する枠組みを整備**することが望まれる。
- 個々のアクティビティでのデータ構造の整理は、1990年代から
  CALS(Commerce At Light Speed)や
  STEP(Standard for the Exchange of Process model data) という
  国際的な活動があり、策定されたもの継続中のもの存在

昔との違いは、実際にこの構造で、
膨大な情報処理が急速に進んでいる。

Industrie 4.0

RAMI4.0(Reference Architecture Model Industrie 4.0)と

Iustrial Internet Consortium

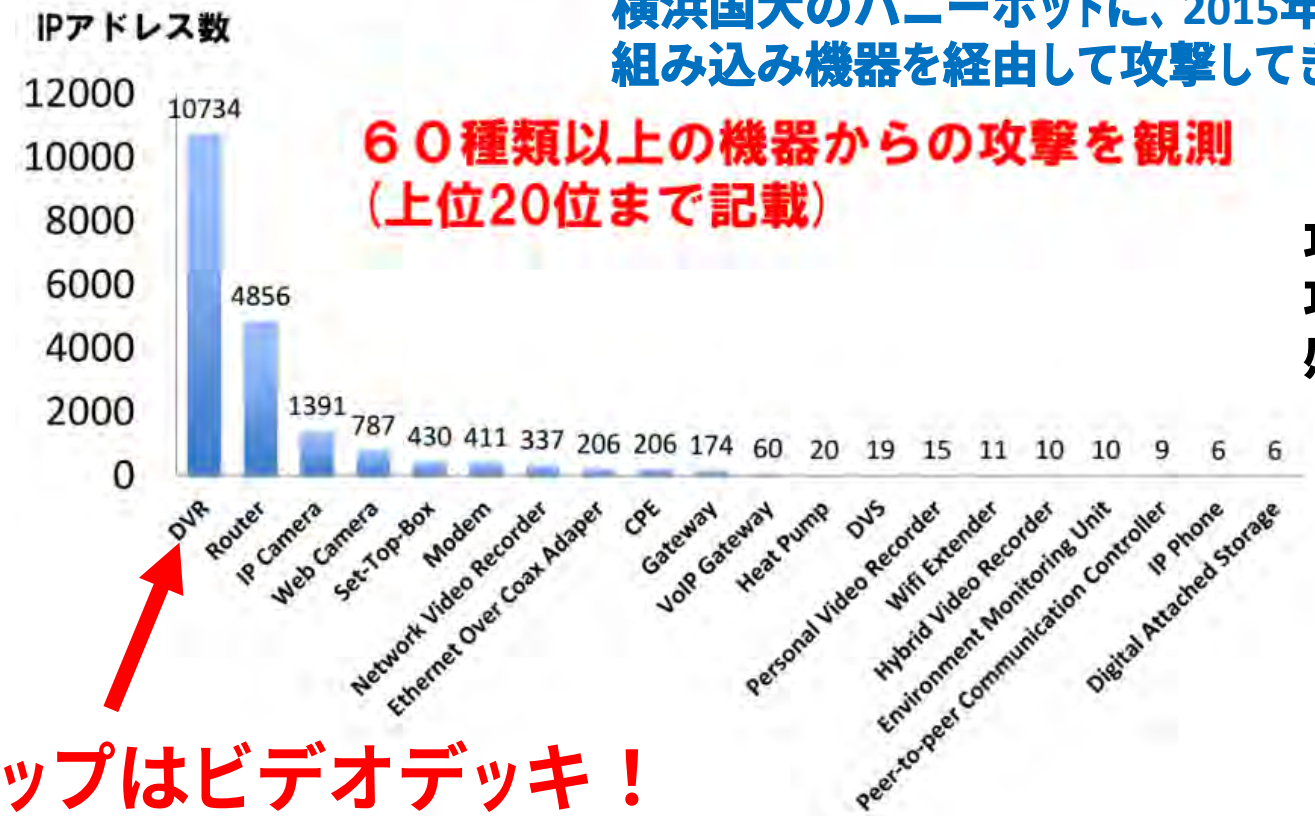
IIRA(Industrial Internet Reference Model)

IoTためのセキュリティ技術の重要性

「もの」をインターネットに接続するときには、
セキュリティを考慮しないと、そこから被害が発生しうる

ハニーポットで観測された感染機器の種類

横浜国大のハニーポットに、2015年4～7月の4ヶ月で、
組み込み機器を経由して攻撃してきた記録



６０種類以上の機器からの攻撃を観測
（上位20位まで記載）

攻撃してきた機種 361
攻撃元IPアドレス 15万
感染試行回数 90万回

トップはビデオデッキ！

吉岡克成先生（横浜国立大学）提供資料より

コントロールシステムのセキュリティ問題

コントロールシステムに対する
サイバー攻撃が増加

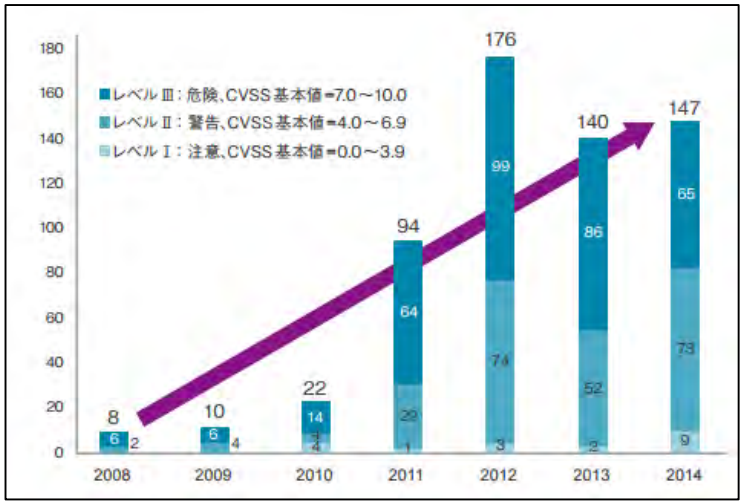
計装システムの**脆弱性**の発見も増加

しかし

情報系では常識的なアンチウィルスや
セキュリティパッチ適用も
リアルタイム処理への悪影響を恐れ、
利用しないのが通常である

システム更新は、15～20年に一度の
多額な投資で、頻繁には行われない

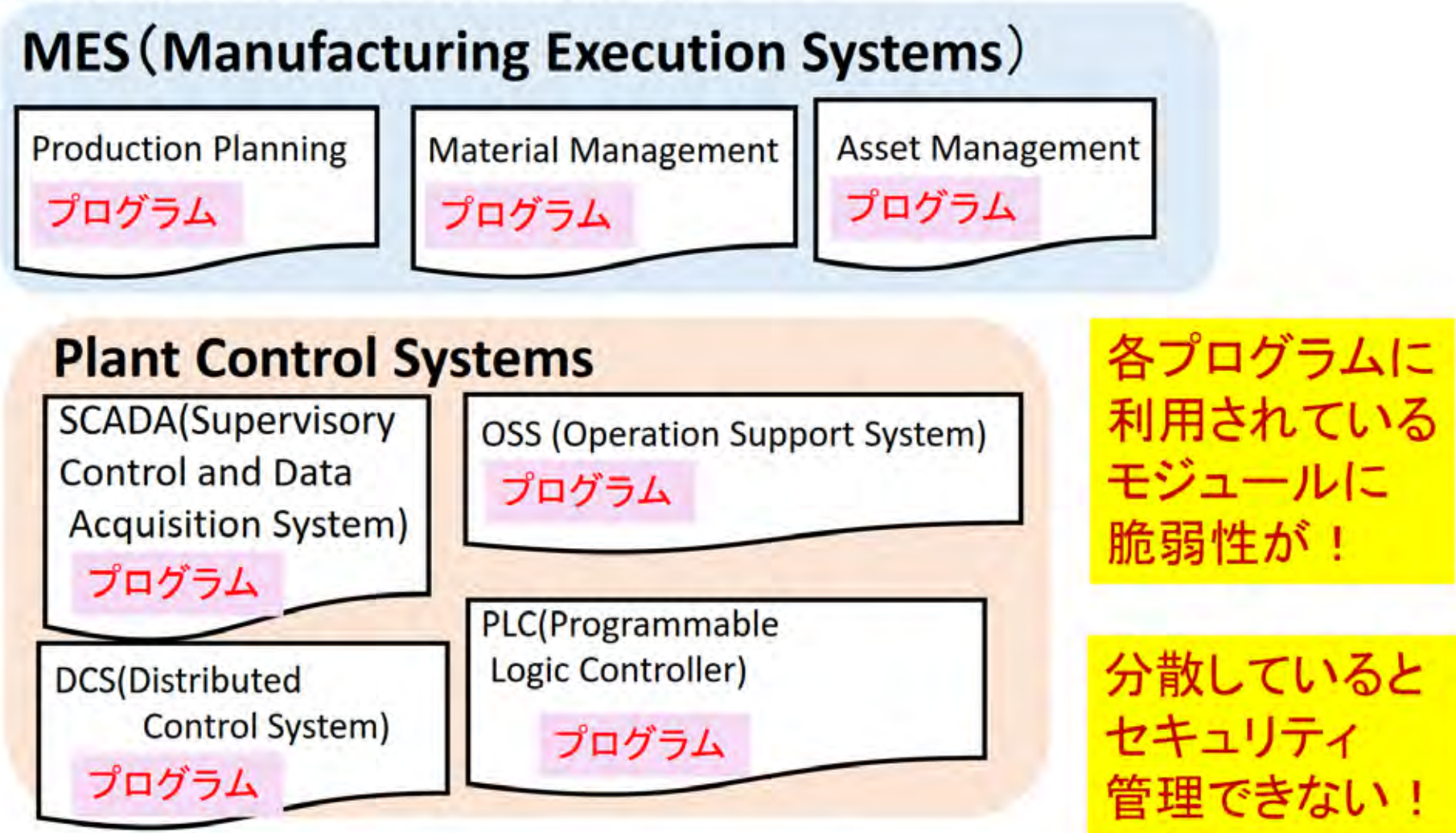
米国重要インフラへの
サイバー攻撃の発生件数の推移



ICSソフトウェアに関する
脆弱性深刻度別報告件数

インテリジェントはセキュリティ管理対象

現在、製造現場のインテリジェントは、プログラムという形で、
さまざまなモノにちらばっている。



プログラムのセキュリティ管理

検討課題例

10年前に社員が開発したプログラムに、利用されているモジュールに脆弱性が見つかったと報告を受けた。

セキュア通信のモジュールOpenSSLの脆弱性が報告されることもある。

- だれが、プログラムの修正をする？
  - その社員の現在の仕事は？
  - 他の人に頼めるプログラム修正？
- モジュールの修正版はいつ入手できるの？
- そのモジュールの修正が、リアルタイム処理に悪影響しないか、テストするには？
- そのモジュールを利用しているプログラムは社内に他にないの？

クラウドのメンテナンスでの利点

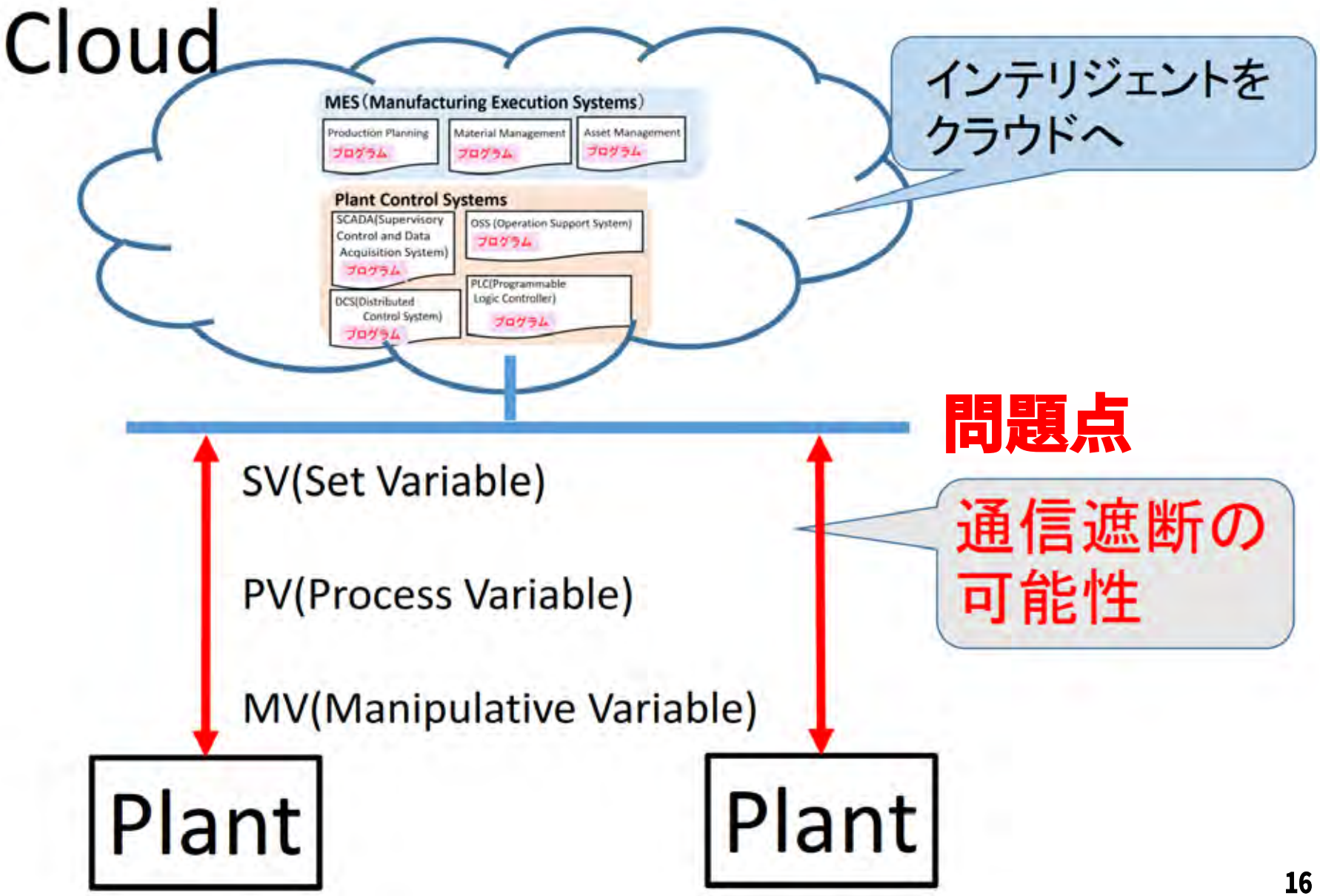
手元のコンピュータで利用していたデータやソフトウェアを、ネットワーク経由でサービスとして利用者に提供

- 企業サーバはクラウドに移行、
  セキュリティ管理はクラウド側の専門家が担当
- 企業の端末はシンクライアント化、
  端末にはアプリケーションをインストールせず、
  サーバでアプリケーション更新

技術の向上

- サーバの情報量、および、処理能力の向上
- 通信の高速化、高信頼化

コントロールシステムの将来像①



コントロールシステムの将来像②

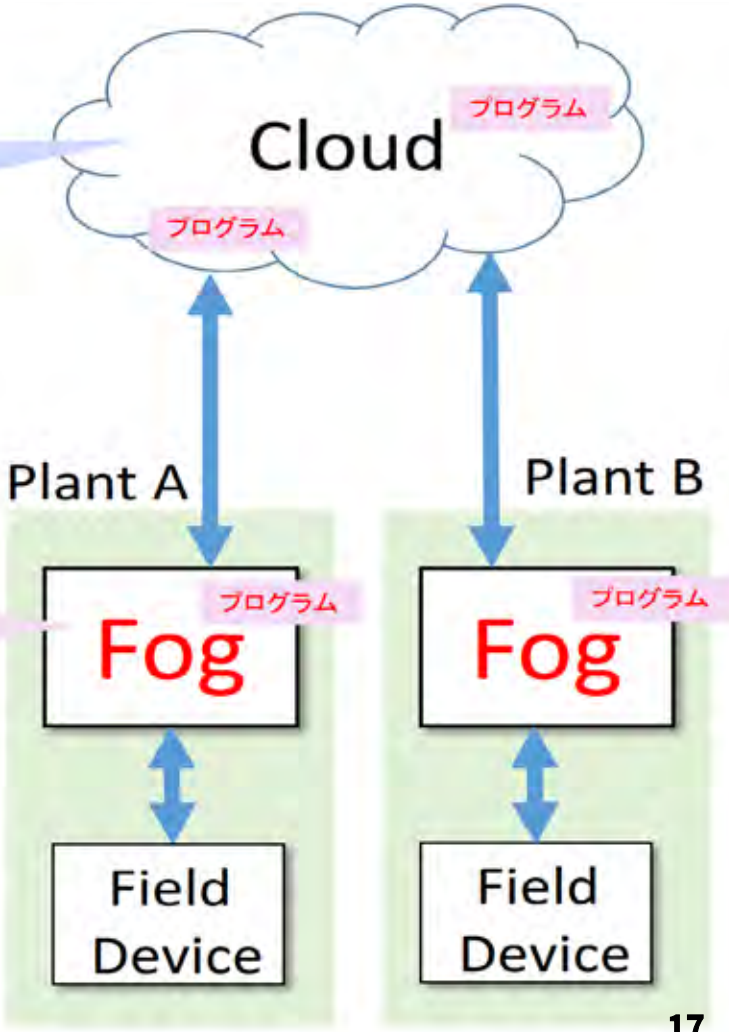
Fogによるクラウド機能の導入

リアルタイム性が低いシステムの
インテリジェントは「Cloud」に集約

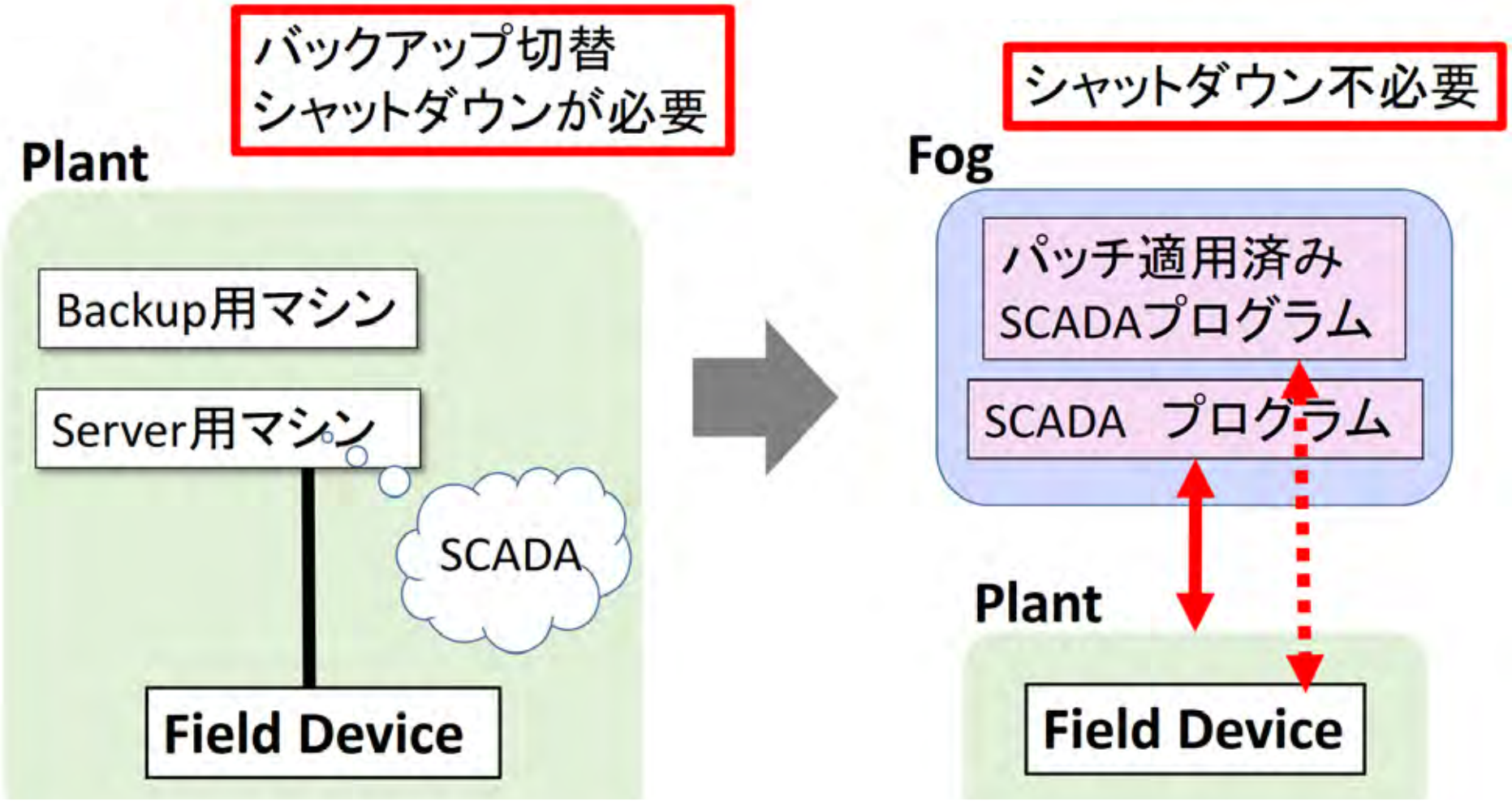
各プラント敷地内に
疑似Cloud環境（Fog）を構築

リアルタイム性が高いシステムの
インテリジェントは「Fog」に集約

インテリジェントを「Fog」と「Cloud」で管理
⇒ 柔軟なセキュリティ対策が期待できる



Fogに期待できるセキュリティ機能の向上



セキュリティパッチの適用やバックアップへの切り替えが容易

FogはOpenStackを利用して数十万円のサーバーで研究室に実装済

付録

名古屋工業大学社会工学科経営システム分野

ICSサイバーセキュリティ研究チーム

教授　越島一郎、渡辺研司、橋本芳宏

助教　浜口孝司、青山友美

セキュリティ対策研究の紹介

①異種多重多層防御

ものに基づく防御の検討

②セキュリティ人材育成

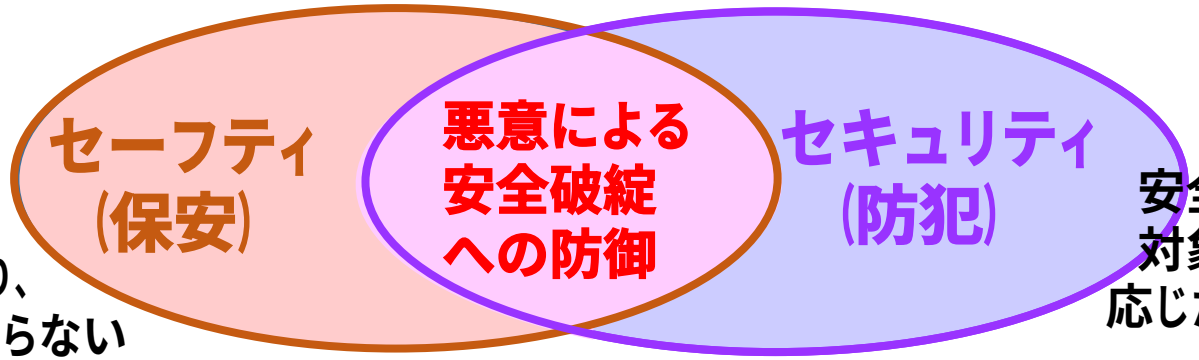
従来の安全に対するスタンスで
サイバー攻撃を受けたとき大丈夫か

名工大でのセキュリティ対策研究①

重要インフラのセキュリティ破綻

→爆発や毒劇物の漏洩、衝突事故など、**人命に影響**する重大事故

Safety & Security



危険要素は
やまのようにあり、
悪意まで手が回らない

安全な鍵の議論
対象の安全性に
応じた防犯は？

- 上記のベン図の共通部分を埋める研究が必要

やられてしまう前提でのセキュリティ対策

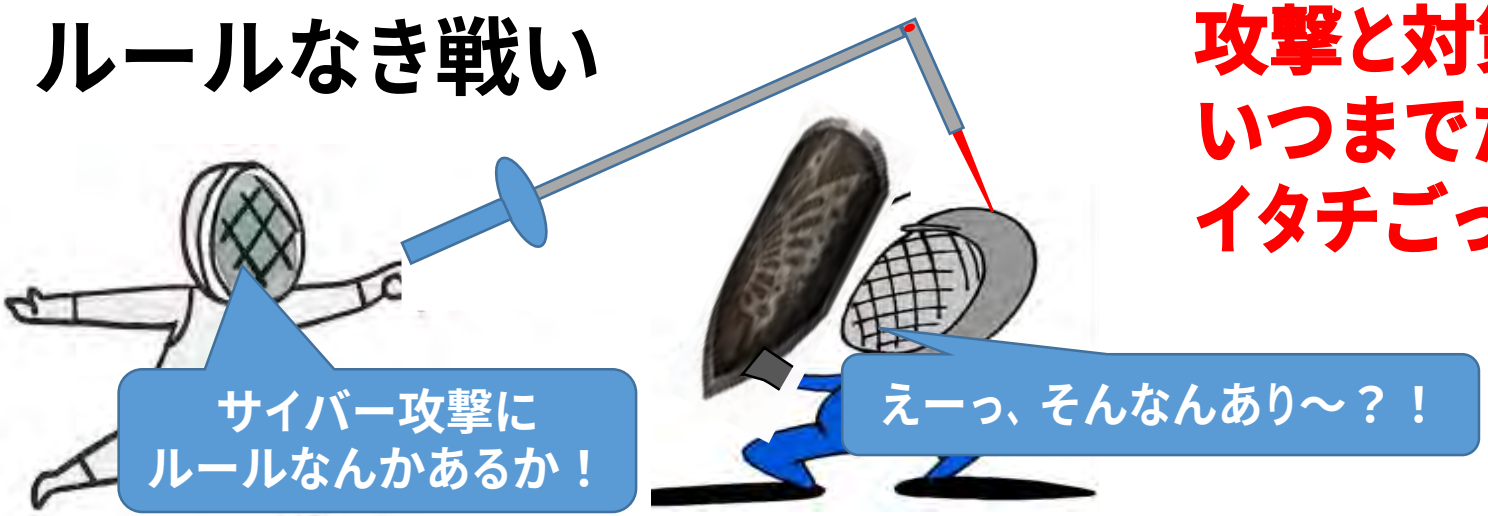
危険性は、攻撃の手口で決まるのではなく、
制御対象の特性で定まる。

→守るべきものから考えるセキュリティ対策

攻撃を想定しても、新たな攻撃は、たいてい想定外

ルールなき戦い

攻撃と対策は
いつまでたっても
イタチごっこ



サイバー攻撃対策の基本スタンス

制御系へのサイバー攻撃は、コントローラの
「悪意の誤操作、悪意の誤動作」とみなせる

サイバー攻撃では、
- 従来の安全解析で洗い出されたアクシデント以外は起こらない（危険性は攻撃手口ではなく物で決まる）
- インテリジェントのない蛇口やリレーは襲えない

従来の安全解析で不足しているのは、悪意による多重多発性

「フェールセーフ、フールプルーフ」を、
同時多重に発生するハザードに対しても徹底すれば、
サイバー攻撃からでも、安全は守れるはず

統一化ではなくバリエーションの確保

高性能、管理の効率化などで標準化、画一化

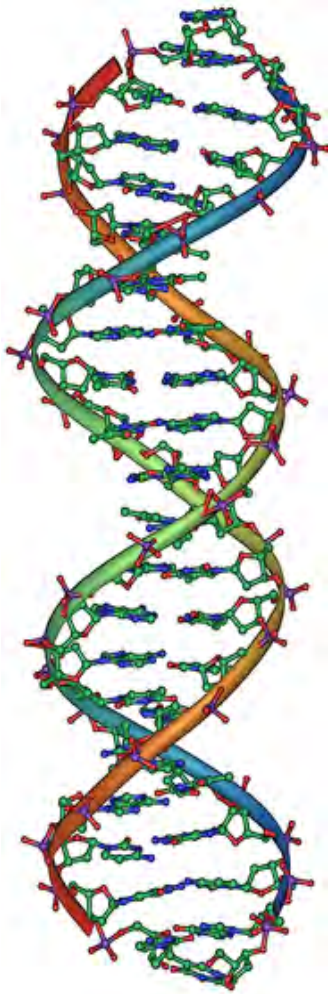
同じ攻撃で、全滅！

一つが攻略されても、生き残っている箇所で検出＆対策を実行したい

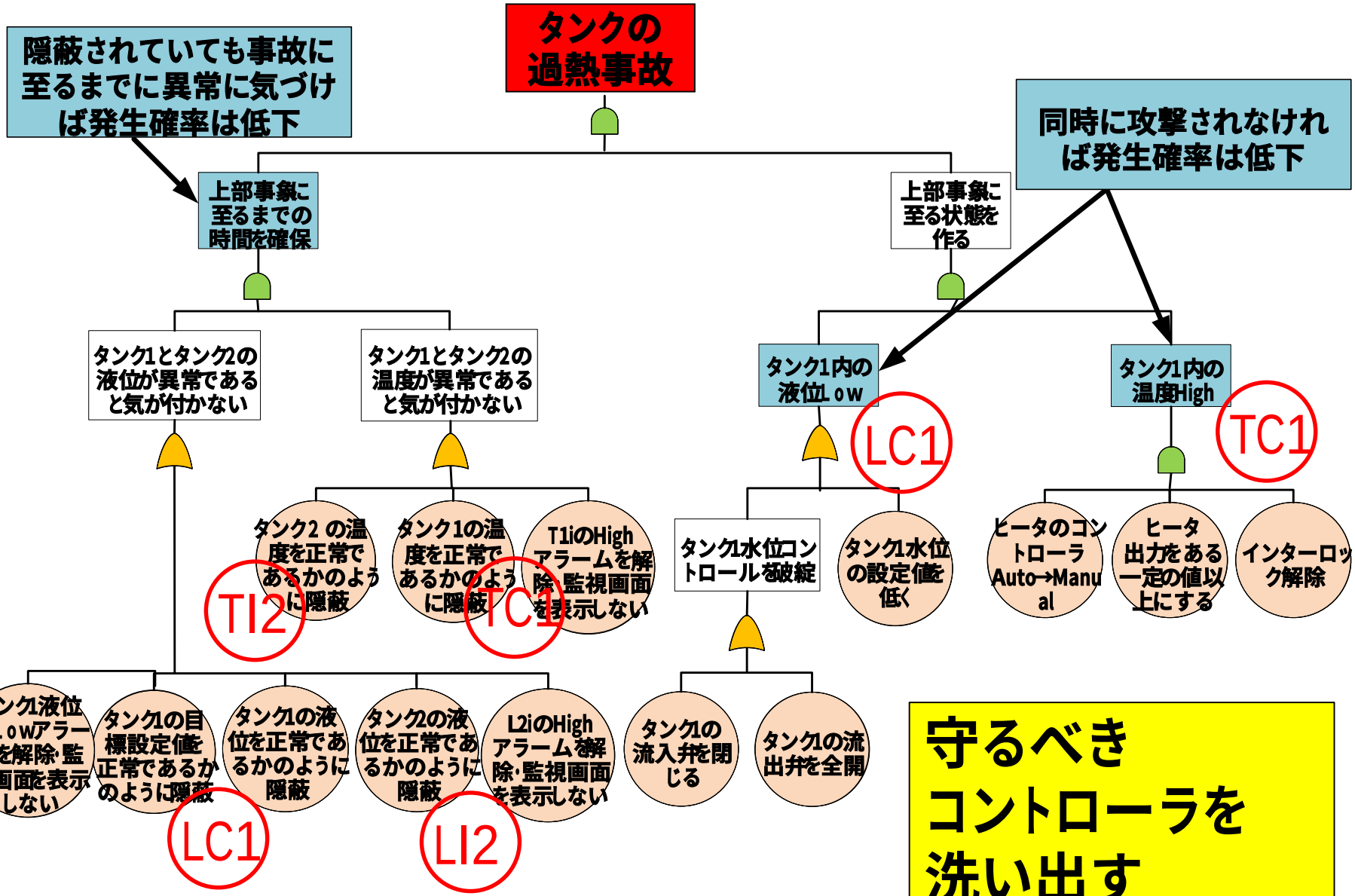
生物は生き残りをかけて、バリエーションを
（自分と遺伝子の差異が大きい人が好きになる？）

一つの機能を実現するには、多数の構成要素が存在
Application, Firewall, OS, Mother Board, CPU, Network Card
Protocol, Certification scheme**などそれぞれに脆弱性の可能性**

それぞれに、バリエーションを確保できれば、
様々なヘテロな構成を得ることができ、一部が陥落しても、
生き残り対策が可能になると期待出来る。



やられたら困るという視点からの防御点の選択



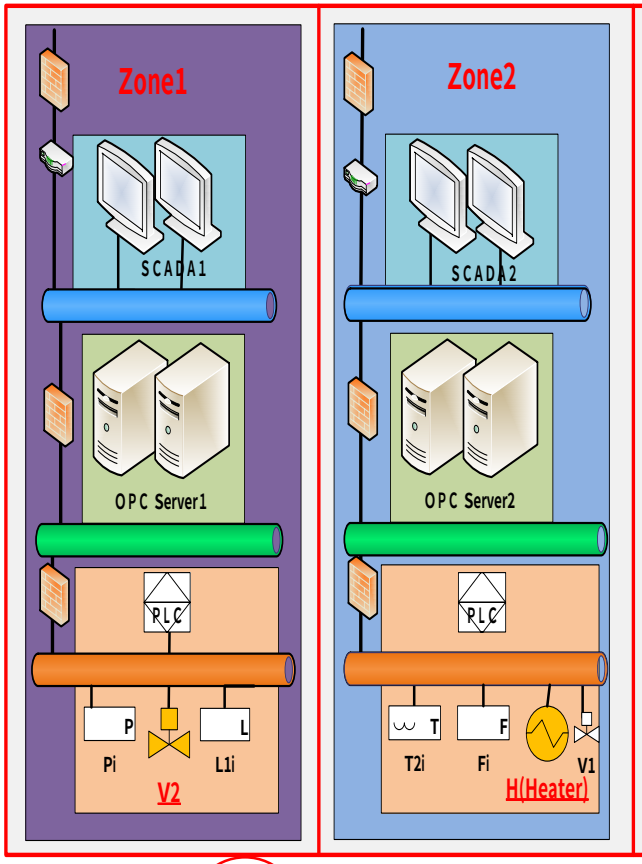
守るべきコントローラを洗い出す

同時に陥落しないゾーンに分割

制御ネットワークを複数のゾーンに分割して
ゾーンごとに異種の錠(ファイアーウォール等)を設定

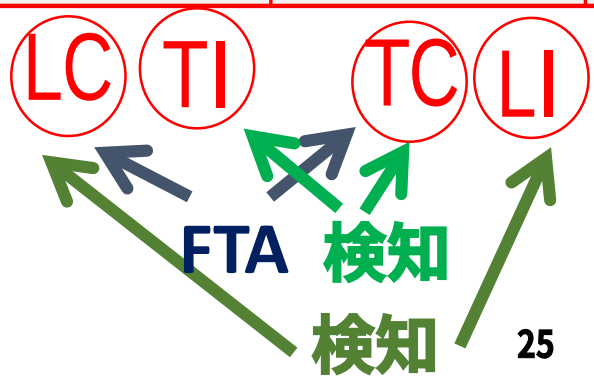
・安全のため**同時に陥落してはならないコントローラ**
　を異なるゾーンに配置することでリスクを分散

・隠蔽工作があっても**一部のゾーンが生き残れれば**、
　異常の検出が可能になる

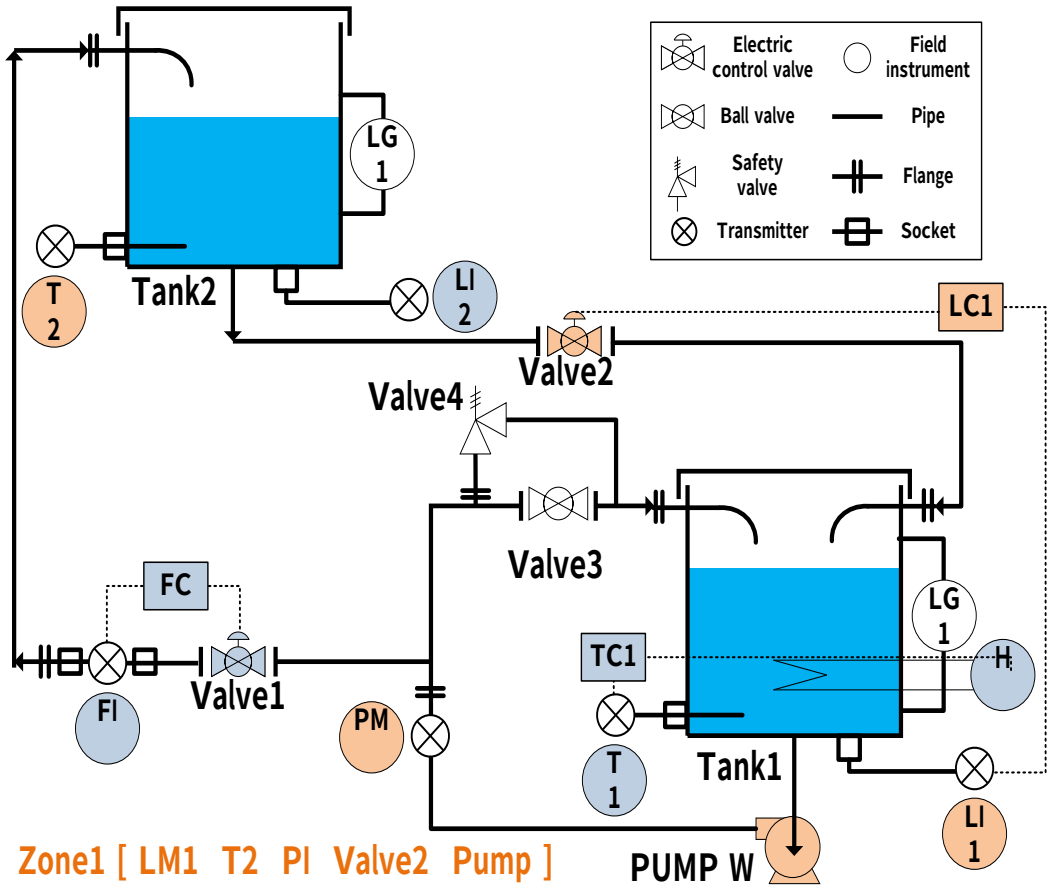


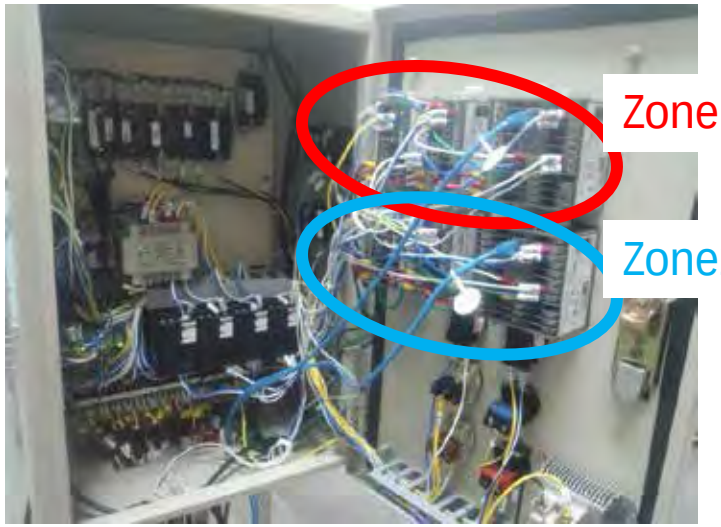
ゾーンをいくつに分割し、各ゾーンに、
どのようにセンサ、アクチュエータ、
コントローラを振り分けるかで
リスクの低減、異常検知能力の向上が変わる。

ネットワークのゾーンの設計手法が必要。

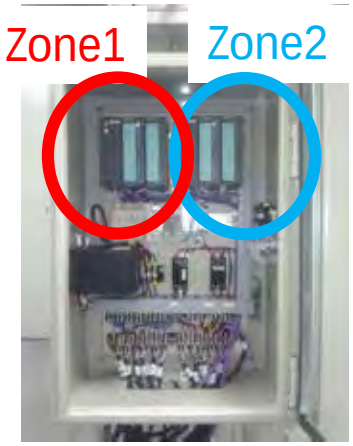


デモプラントのゾーン分割例





シングルループ･コントローラ
3台ずつをゾーンに配分



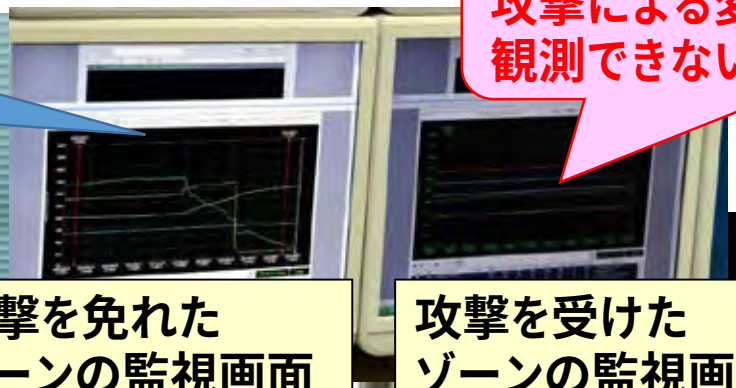
各ゾーンにPLC1台

新たな設備や現場工事を要求するものではなく、
景気室内の配線の変更ですむ工夫

名工大でのテストベッドでサイバー攻撃の手口を実演し、対策の有効性も確認

生き残ったゾーンの画面では
攻撃による変化が検知できる。

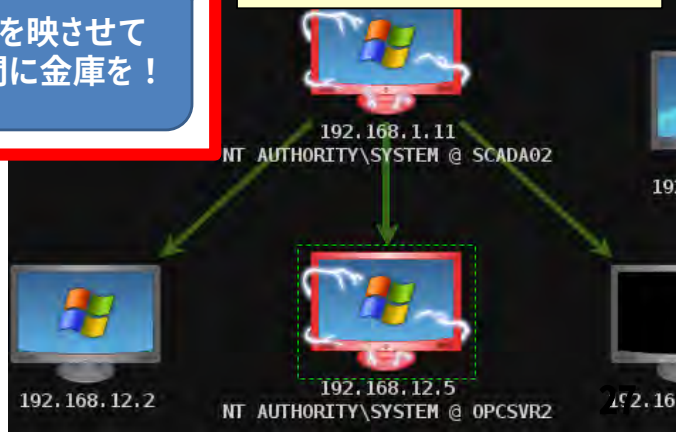
攻撃を受けたゾーンの画面では
攻撃による変化が隠蔽により
観測できない



攻撃を免れた
ゾーンの監視画面

攻撃を受けた
ゾーンの監視画面

ハッカーのPC



攻撃を受けて、
コントローラが操作され、
危険な状態に陥って、
現場計器では、
アラームが発生

攻撃を受けたパネル計器

2017年2月の時点で、のべ400名以上の来訪あり

名工大でのセキュリティ対策研究②

悪意で発生する同時多重のハザードに対して
「フェールセーフ、フールプルーフ」を徹底するには
　現場の人間の対応も重要

早期検知・早期復旧（BCM）には、現場担当者、情報技術者、計装技術者、営業など、社外も含めた多くの部署が組織的に連動して、適切に対応することが必要

想定外の攻撃に備えるためには前例に基づくのではなく、
人間の想像力を刺激し、対応力を高めるべき

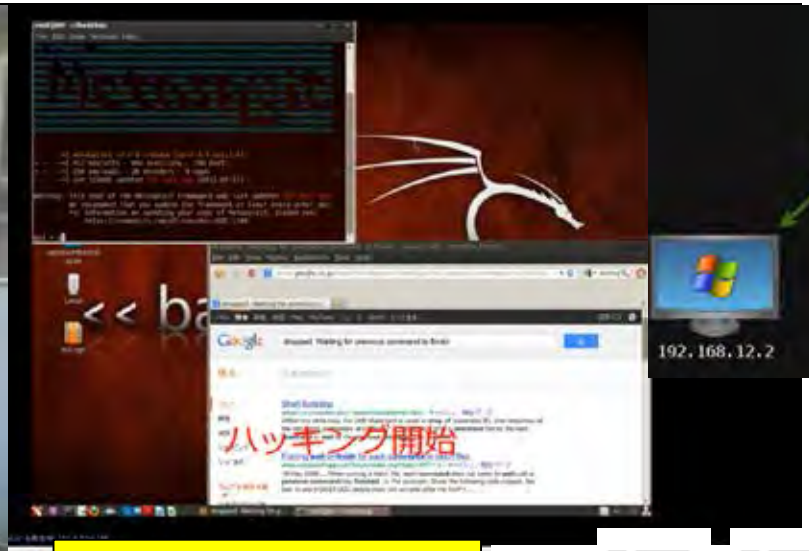
臨場感のある演習で、現在の対策を見つめ直し続ける
PDCA(Plan Do Check Action)サイクルを職場に根付かせる
　　→安全・安心な社会

名工大制御系セキュリティWS①

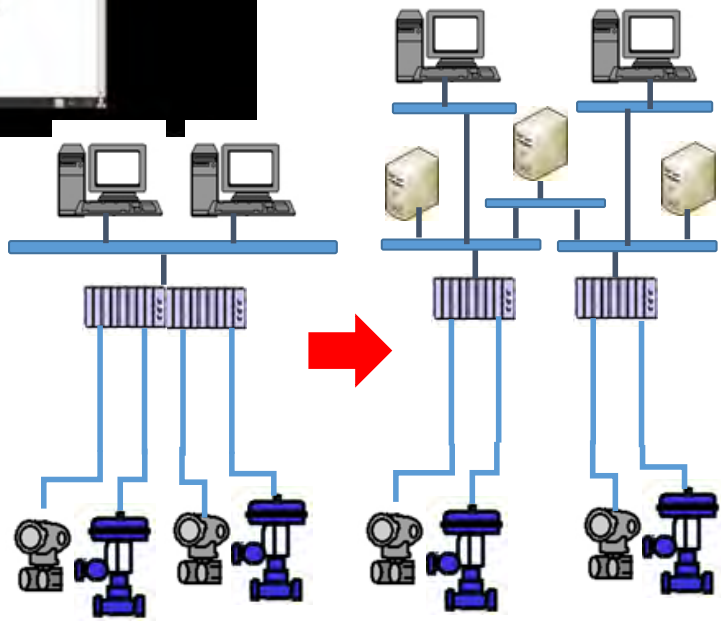
(その1) 2015年3月19,20日 13社18名参加 (その2) 2015年8月26,27日 30社74名参加
(その3) 2015年3月29,30日 26社47名参加 (その4) 2016年9月27日32社54名参加

・実際のサイバー攻撃と対策の有効性を体験する演習

すでに、のべ400名以上の
来訪者と議論 (2017年2月)



制御ネットワークの
ゾーン分割工事



名工大制御系セキュリティWS②

「やられない」だけではなく、「やられる前提」での対策

安全だけでなく事業継続(BCP/BCM)として、
組織全体としての連携ができる体制の構築と演習での準備

生産現場、計装、設備、情報、営業、総務、経営、さらに社外との連動

インシデントの発生から対応を、具体的想定で検討

実験装置を「地域冷暖房サービスの企業」と想定し、
サイバー攻撃を受けた際の、検知から復旧までを
想定ビデオを利用しながら、グループディスカッション



異常が発生しても、原因がサイバー攻撃とは、なかなか判断できない？

現在、内閣府の下記のプロジェクトに参加し、教育プログラムとして拡充を図っている。
戦略的イノベーション創造プログラム(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
(b4)セキュリティ人材育成（セキュリティ人材育成の研究開発）

名工大制御系セキュリティWS③

今の体制で、サイバー攻撃から安全を本当に確保できるのか？

演習により、全社的な議論の仕方を学び、社内での展開へ

■ 想定モデル/ロール