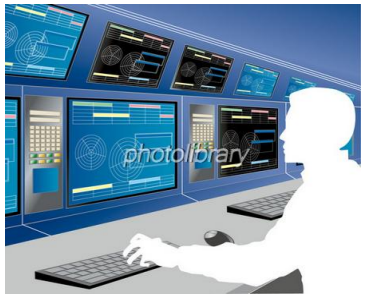
プラントオペレーションの
これまでとこれから？

橋本 芳宏

名古屋工業大学社会工学科

http://www.manage.nitech.ac.jp/Security



- 石油・化学プラント自体は、
  これまでもこれからも
  そんなには変化しないかも？
- でも計装や運転は激変するかも？
- スマート化の便利さとリスク
- さまざまな悪意にも配慮した
  これからのプラント計装と
  プラントオペレーションとは？

プラントオペレーション研究会

1979年から今年で40年

副代表と時代の主テーマ

- 中西英二（パネルからコンソール、教育訓練）
- 西谷紘一（業務革新、技術伝承）
- 橋本芳宏（？？？、大規模災害？）
- 野田賢　（情報革新, AI, IoT, セキュリティ）

気になった監督者セミナーでの発言

？？？⇒たよりつづけたベテラン層

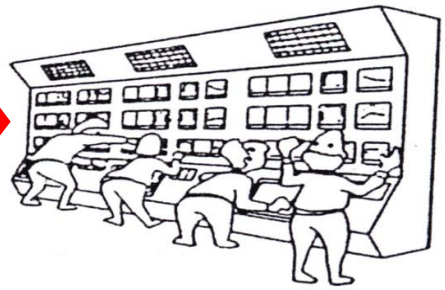
もう伝承してもらうものなんてない！？

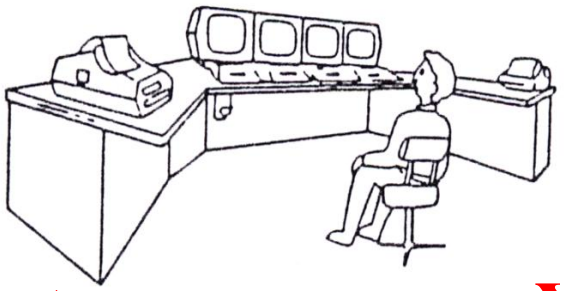
新しいものは若い者が主体で導入した

少なくとも人間の経験がたよりの異常時対応は無理！

プラント計装の変革

Manual Operation　　Analog Panel Board（～1980）　　DCS（Distributed Control System）（1980～）





NEXT (20XX)

Automation　　**Computer**　　**XXX ?**

1975年、HoneywellがTDCS2000, YOKOGAWAがCENTUMを開発

1979年 プラントオペレーション事例研究会

DCSによるConsole Operationを、ExxonMobilはHoneywellとともに推進してきた。以来、15～20年に1回、DCSの更新が行われてきたが、ExxonMobilには、いまだに初期のDCSも存在

DCSの更新に必要な費用は、莫大なものになっている。

現在、IoTやAIで変革の時代だといわれている。

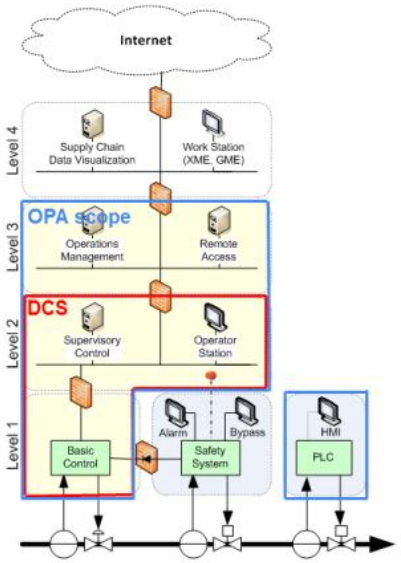
これから、プラント計装はどう変わるのか？

ExxonMobilからOpen Process Automationの提案

アビオニクス(航空電子工学)分野ではオープンシステムを活用
FACE (Future Airbone Capability Environment consortium)

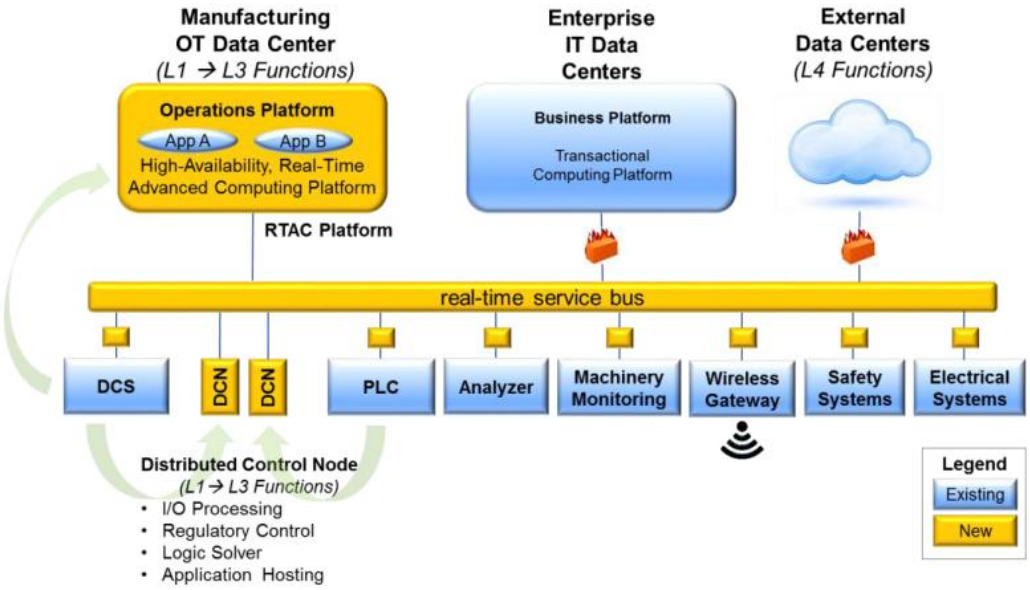
Exxon MobilはLockeed Martinと2016年1月14日にnext-generation, open and secure automation system for process industries開発のSystem Integratorとして契約

現行の DCS アーキテクチャ



- 専有ハード, インターフェース 及びネットワーク構成
- ソフトウエア利活用はベンダに依存
- 非本質的セキュリティ: ビルトインではなく追加的

OPA 参照 アーキテクチャ



- 業界標準のインターフェースとネットワーク構成
- 相互運用可能なハードウエア
- オープンなソフトウエア利活用
- 設計組込み型セキュリティ

ExxonMobil

ARC Tokyo 2018　Dung Kushnerick氏講演資料より抜粋

Open System Architectureの特徴

- **Portability -** Application software will run on multiple platforms.
- **Open Standards -** Leveraging publicly available open standards.
- **Modularity -** multi-vendor Comp Opponent Interchangeability.
- **Interoperability -** Conforming software integrated with minimal effort.

Open Architecture Standard Building Blocks Exist

OPC UA https://opcfoundation.org/

Open Controller to Controller Communications www.PLCopen.org

PLCopen XML Interchange Standard The PLCopen organization's XML standard

IEC 61131-3 Programming Standard Ladder, SFC, and the textual languages Instruction.

PLCopen Functions

Runtime Engines IEC 61131-3, PLCopen, and OPC Foundation standards.

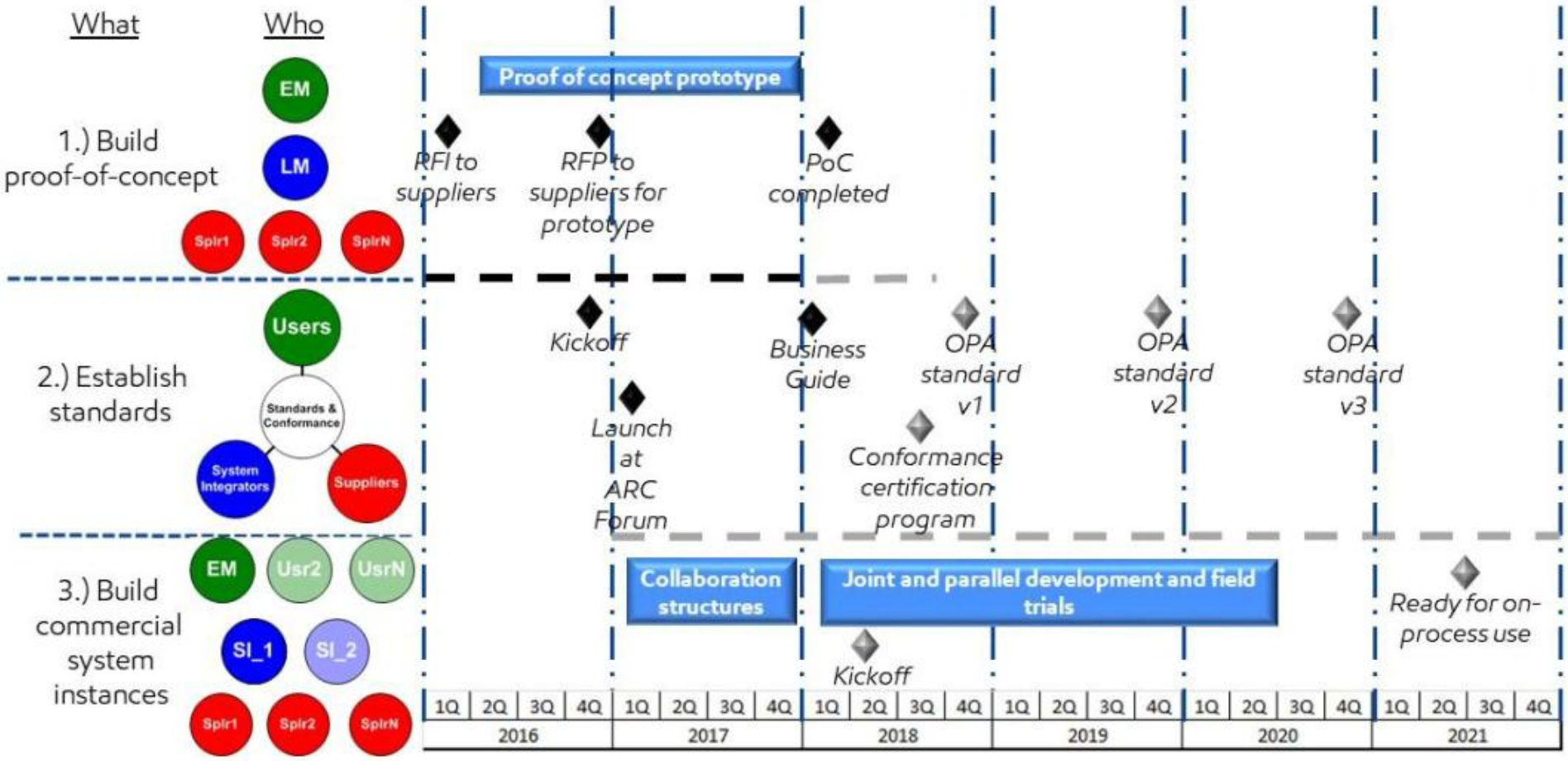
FDT http://www.fdtgroup.org/

SERCOS Sercos III FPGA or an ASIC master component. http://www.sercos.org/

http://www.automation.com/automation-news/article/exxonmobil-to-build-next-generation-multi-vendor-automation-architecture
(2016年2月16日掲載)

Open Process Automationの推進スケジュール

1) **概念実証**をロッキード・マーティンと構成
2) **業界標準**を オープン・プロセス・オートメーション・フォーラムと策定
3) 他の運用企業と協働開発および並行**プラント現場試験** (Field Trials)を実行



ExxonMobil

ARC Tokyo 2018　Dung Kushnerick氏講演資料より抜粋

業界標準: Open Process Automation Forum

- The Open Group （UNIX, Future Airborne Capability Environment, etc.） が支援
- 事業のフレームワーク+ 技術的標準+ 適合認証
- 設立 2016年11月; 現在 79 社会員
- Business Guide 発行 （2018年1月）; Requirements ホワイトペーパー 及び O-PAS 仕様 V1 （2018年6月）

オープン・プロセス・オートメーションの有利性

エンドユーザ	サプライヤ
• 制御システムアプリケーションの再利用をサポート	*売上高（top line）の成長：*
• 価値創出の増加	• 新市場と新顧客層の開拓
• 継続的技術革新を可能に	• 既存の顧客との関係性を維持
• システム統合問題を解消	• 拡大する市場向けに新製品・サービスを開発
• 安全で本質的（intrinsically）にセキュアである	*最終損益（bottom line）の成長：*
• 従業員の権能拡大	• 収益の増加
• 総所有コストの削減	• 経費削減
	• 非差別化製品の削除

[Open Process Automation™ Forum. *Business Guide: Value Proposition and Business Case*. (Jan 2018)]

ExxonMobil

オープン・プロセス・オートメーション・システム（OPAS）開発はテストベッド構築段階へ(2019/08/14)

- 従来型のDCS サプライヤの世界的大手である**横河電機**は、コンポーネントのサプライヤとしてではなく、あくまでOPA プロジェクト向けのインテグレーションソフトウエア開発者として参画する。
- 第1は、プロトタイプのコンポーネントを使用してテストベッドを立上げる段階。
  第2は、テストベッドを拡張し、新規・追加のコンポーネントを組み入れる段階。
  第3は、協働パートナー企業向けの支援を組み入れてさらに多くのコンポーネントを統合化する段階
- 横河電機が米テキサス州スプリングに開発オフィスを新設し、2019年第4四半期に第1ステージの稼働を開始する予定
- 2020年初期には協働パートナー企業向けにテストベッドの活用が開放される予定である。

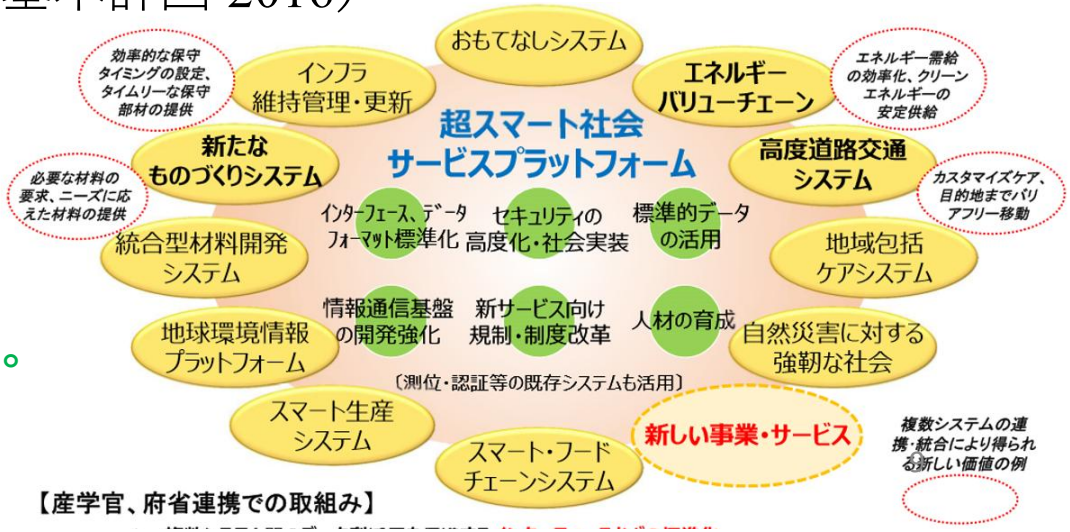
https://www.arcweb.com/ja/node/86946

IoTを推進する日本の動き

- **日独IoT/インダストリー4.0協力に係る共同声明**（2016年4月）
  http://www.meti.go.jp/press/2016/04/20160428011/20160428011.html

- IoT推進コンソーシアムと
  Industrial Internet Consortium(IIC)で覚書
  （2016年10月）
- 高圧ガス保安法［経産省］(2015年)
  スーパー認定事業所：連続運転8年許可
- **Society 5.0**（第５期科学技術基本計画 2016）
  ①狩猟社会　②農耕社会
  ③工業社会　④情報社会
  ⇒⑤**超**スマート社会

どこの会社の社員も、社長から
「なんかせなあかん」と言われている。
自分こそ、
「なんとかせなあかん」立場なのに。



スマート化と防爆

「プラント内における危険区域の 精緻な設定方法に関するガイドライン」　経産省2019年4月24日

https://www.meti.go.jp/press/2019/04/20190424001/20190424001.html

- PAの現場でスマート化が進まない大きな要因に防爆規制がある。
- スマート化をすすめたい経産省、発災時にドローンを利用したい消防庁と安全の監督官庁の厚労省とが議論し、防爆管理区域の見直しが行われた。
- ガスが停滞しない道路上などにカメラをつけ、映像で風の流れを確認できれば、その場所にも、非防爆機器を持ち込むことが可能になった。

ようやく、防爆にもクサビがさしこまれた。
これを機に、操業現場の安全なスマート化の議論を
さらに活発化させませんか？

IoTによる「もの」の革新

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）

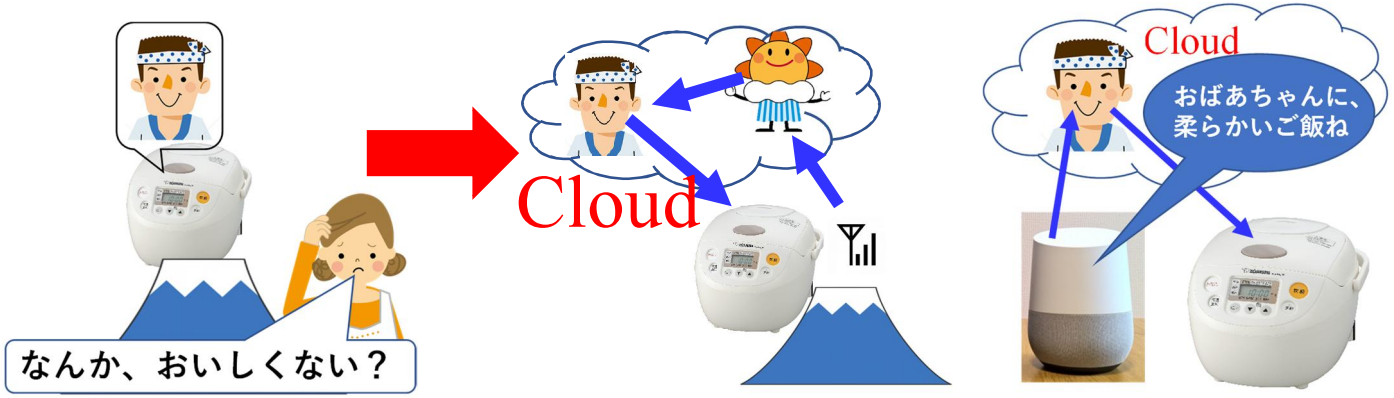
④ IoT iPhoneのSiriはクラウドにつながって作動

モノからインテリジェンスが離れる

④の革新って何？

マイコン炊飯ジャーはIoTでこう変わる

通信と単純な機能があれば、クラウドでどんどん高機能に



しょぼいCPUとけちくさいMemoryからクラウドへ

モノの進歩が物理的拘束から解放される

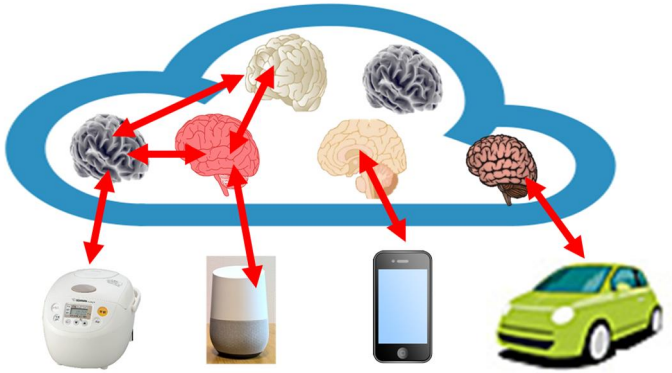
IoTの革新性

インテリジェンスがモノから離れてクラウドへ

- **物理的** (CPU, Memory, HDD, etc.)
- **空間的** (Access to all over the world)
- **時間的** (Past, Present, Predicted Future)

拘束から解放される

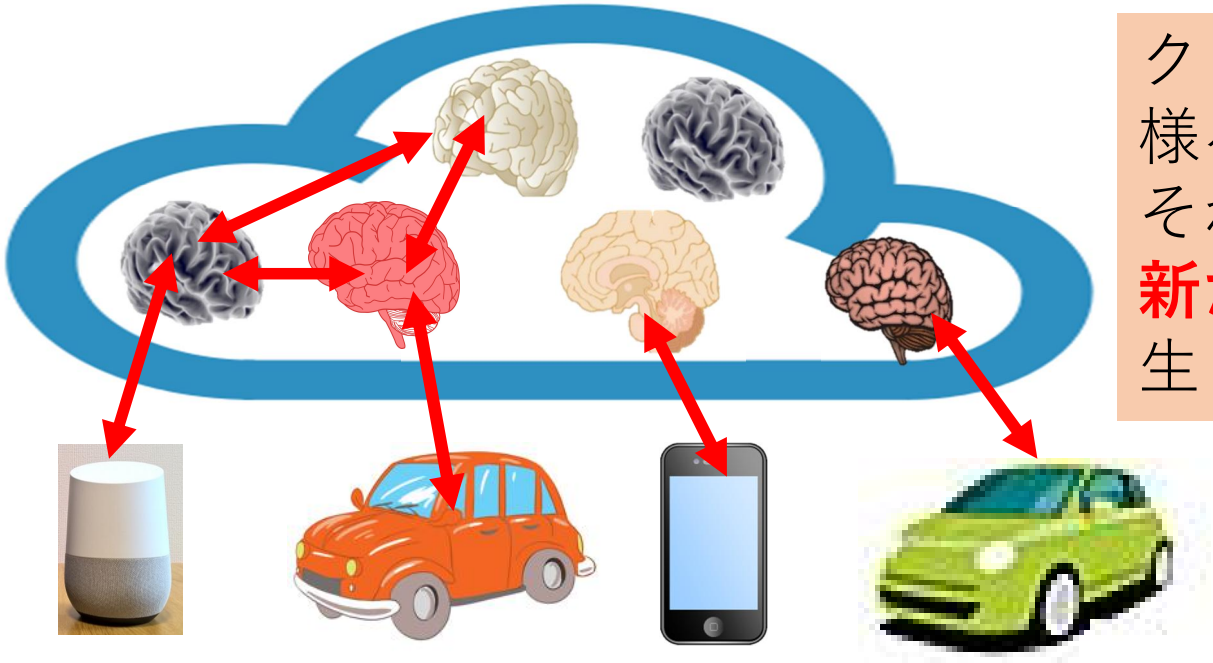
Innovation



System: 特定の**目的**で開発

System of Systems: 開発時にはなかった
新たな機能を連動して発揮

Cloudでは知能がつながって新たな知能が



クラウドには、
様々な情報が集まり、
それらをつなげると、
新たなサービスが
生まれる (改善ではない)

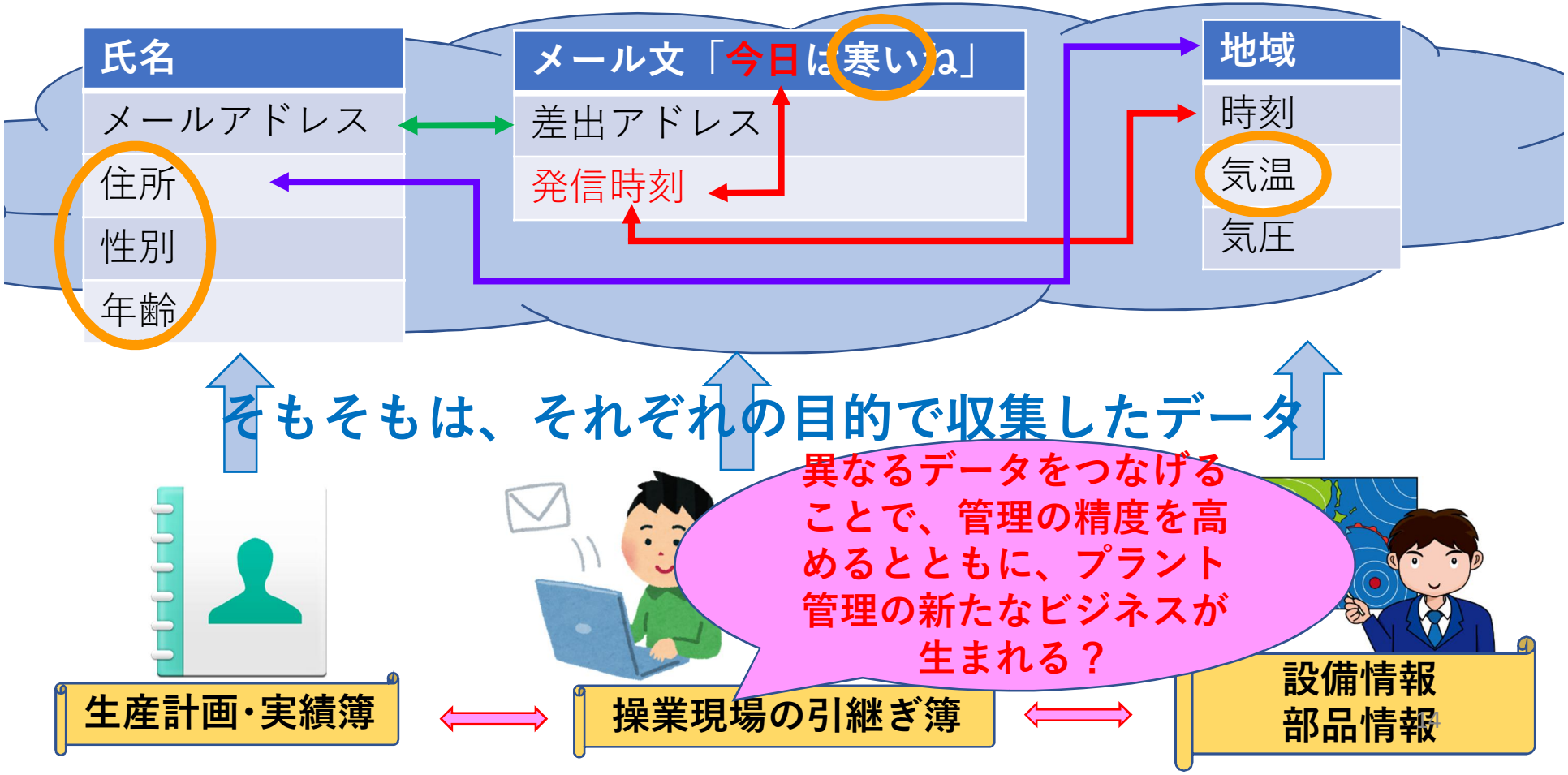
Google Mapの渋滞情報

- Google mapのユーザーは自分のためにGPS情報を送る
- Googleは集まったGPS情報から渋滞を推定
- 渋滞情報受益者はデータ提供者本人ではない

将来的には、ドライブレコーダの情報共有で、
交差点の危険予知の共有もありうる。
インフラ投資より有効で維持管理しやすい

クラウドでの情報の活用

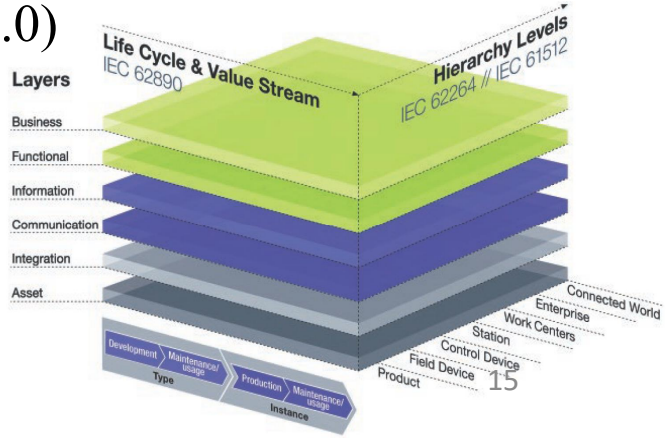
- メールから文章をたくさん集めるだけでは情報にならない。
- **リンク**をたどることで、暖房機器のマーケッティングに利用できる**情報**にもなりうる。



Big Data & AI , IoTの時代とは

- クラウドでの情報収集
  Google (検索、メール、動画、ナビによる行動情報、・・・)
  Amazon(電子書籍、ビデオ、買物情報、商品評価、・・・)
- 音声や画像の認識による情報収集
  音声認識ツール(音声情報もテキストに)
  画像認識ツール(画像認識結果も新たな情報)

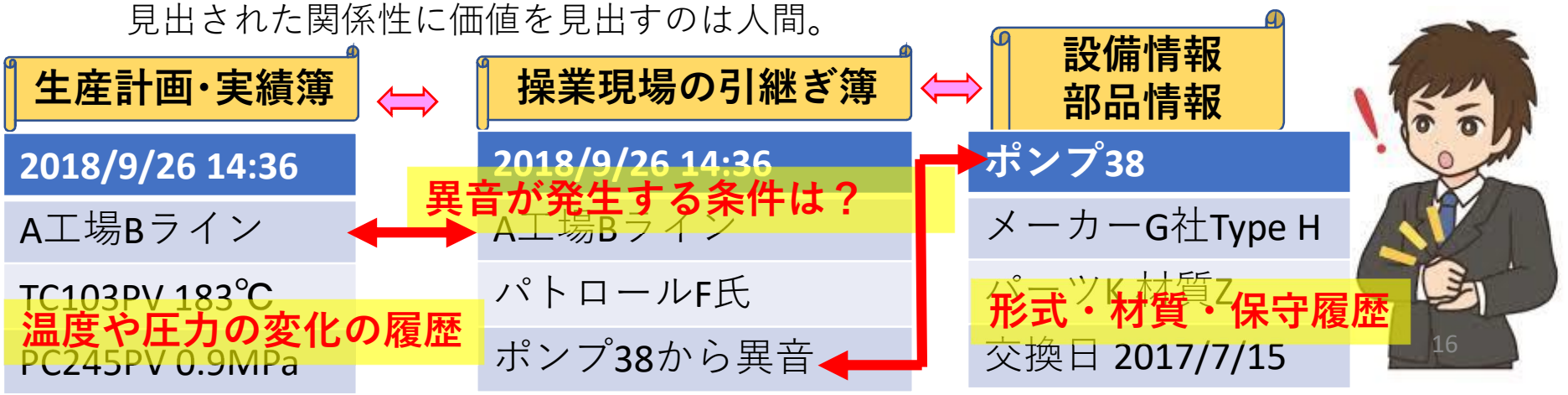
- **AIによる情報合成**
  IBM Watson(Cognitive Engineによる情報の連結)
  Alpha Go(AI同士の対戦で新たな棋譜の生成)
- 数値情報を組み合わせて有意義な情報を合成するには
  RAMI4.0(Reference Architecture Model Industrie 4.0)
  IIRA(Industrial Internet Reference Model)
  Life Cycle全般で発生するデータを活用して、
  新たなサービスを創出するのが、
  Connected world



データ構造の標準化とAI

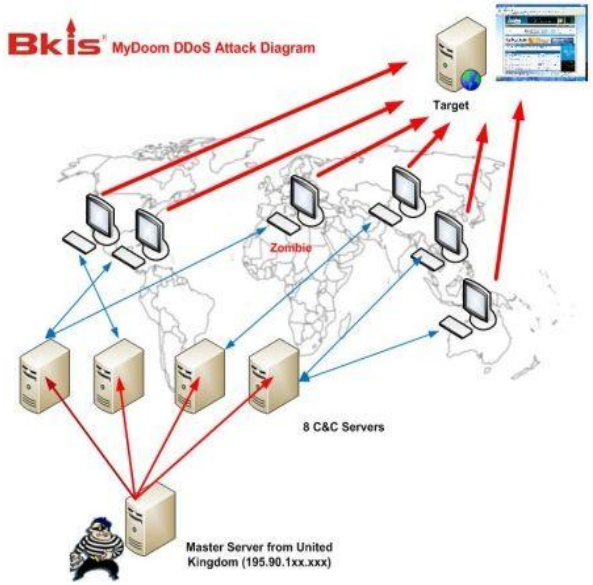
- データ構造の標準化をして、その通りにデータを格納する？
  家計簿の項目を詳細するとどの項目に入れたらいいか迷うし、
  あとでどれに入れたか探すのもたいへん
  - こういうデータベースには、こんなデータがあるはずだ。
    表現や引き出しが少しずれていても、
    自動で探してもらいたい。**⇒AIによる検索**

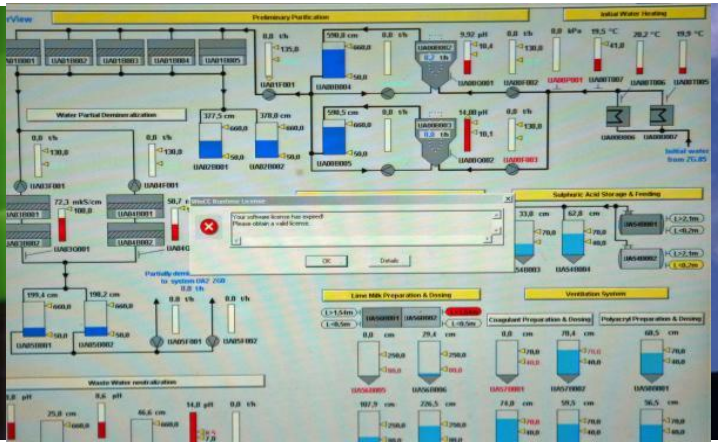
- 新たなサービスを創出するのが、**Connected world**
  - 従来、思いつかなかったほど、いろいろつなげて、おもしろい関係性を見つけたい。
    ⇒AIによる合成
  - データは玉石混交であり、信頼性の低いデータも含まれるが、
    AIは、ノイズや不整合なデータが混ざるほど、
    意味のある着眼点を見出してくれる可能性が高くなる。
  - 勝手につなげて、すばらしい発想だけが出るはずがない。
    見出された関係性に価値を見出すのは人間。



情報には改竄、隠蔽の危険性

- データからの情報の重要性は高まっていくので、
  その改竄や隠蔽の影響も大きくなっていく。
- ブロックチェーンなど、
  改竄、隠蔽を防ぐ方法は
  開発されてきている。
- ここでは、そのような情報技術だけでなく、
  ものを動かす制御技術という観点から、
  サイバーセキュリティを論じたい





プラント計装にもサイバー攻撃が？！

Stuxnet (Epoch making Malware detected in 2010)

目的な攻撃を実現する最初のサイバー兵器

developed by USA and Israel governments

標的: イランの核燃料施設の遠心分離器（シーメンスの**PLC**）

インターネットやＵＳＢを介して感染拡散し、 標的でのみ発症

発症後も攻撃を隠蔽し、長期継続

インターネットに接続されていない**PLC**が

調整用ＰＣを介して感染、プログラムが改竄された。

多くのzero-day (未発見)の脆弱性が利用されたので、

ウィルス対策ソフトは役に立たなかった。

Stuxnetの亜種 は、**愉快犯**でも作成できる。

Quantum作戦（2014年2月報道）PCメーカー協力で出荷時に発信器など

戦争ではなんでもあり （OS-Updateを悪用すればできないことはない）

中国はWindows8の導入を禁止（2014年5月）

標的型攻撃は巧妙になっているし、愉快犯による流れダマもありうる

重要インフラへのサイバー攻撃の脅威が顕在化

Black Energy 3

2015年12月　ウクライナ

30か所の変電所が同時にマルウェアに被害

コールセンターも同時に攻撃され、対応に遅れ

140万世帯が6時間にわたって停電

2017年にも新たなサイバー攻撃が

WannaCry（亜種Petya)

2017年 世界で猛威

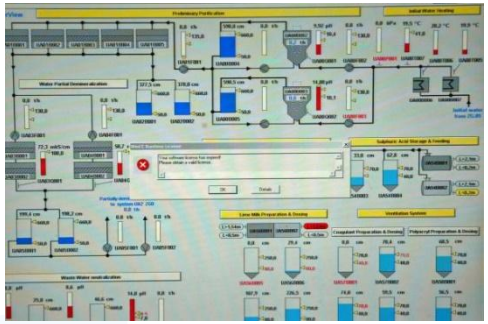
病院、電力会社、空港、公共交通機関、中央銀行などインフラ施設も
日本でも、大企業でセキュリティコンサルタントも行うH社
メールシステムが停止
サーバーのアップデートは
計画中であった
感染源はドイツの検査機器
自動車製造H社
工場ライン停止
流行の時期よりも
1カ月遅れで発生

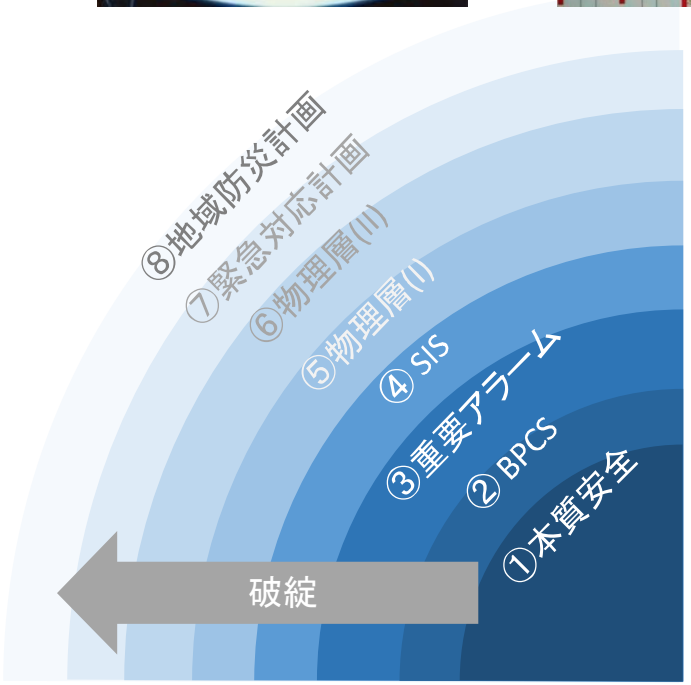
感染型の攻撃の脅威を
強く認識するようになったが、
対策は・・・

安全計装を対象にしたマルウェアも

TRITON 2017年12月 中東の重要インフラを停止

いざというときの頼みのSISもマルウェアの餌食に



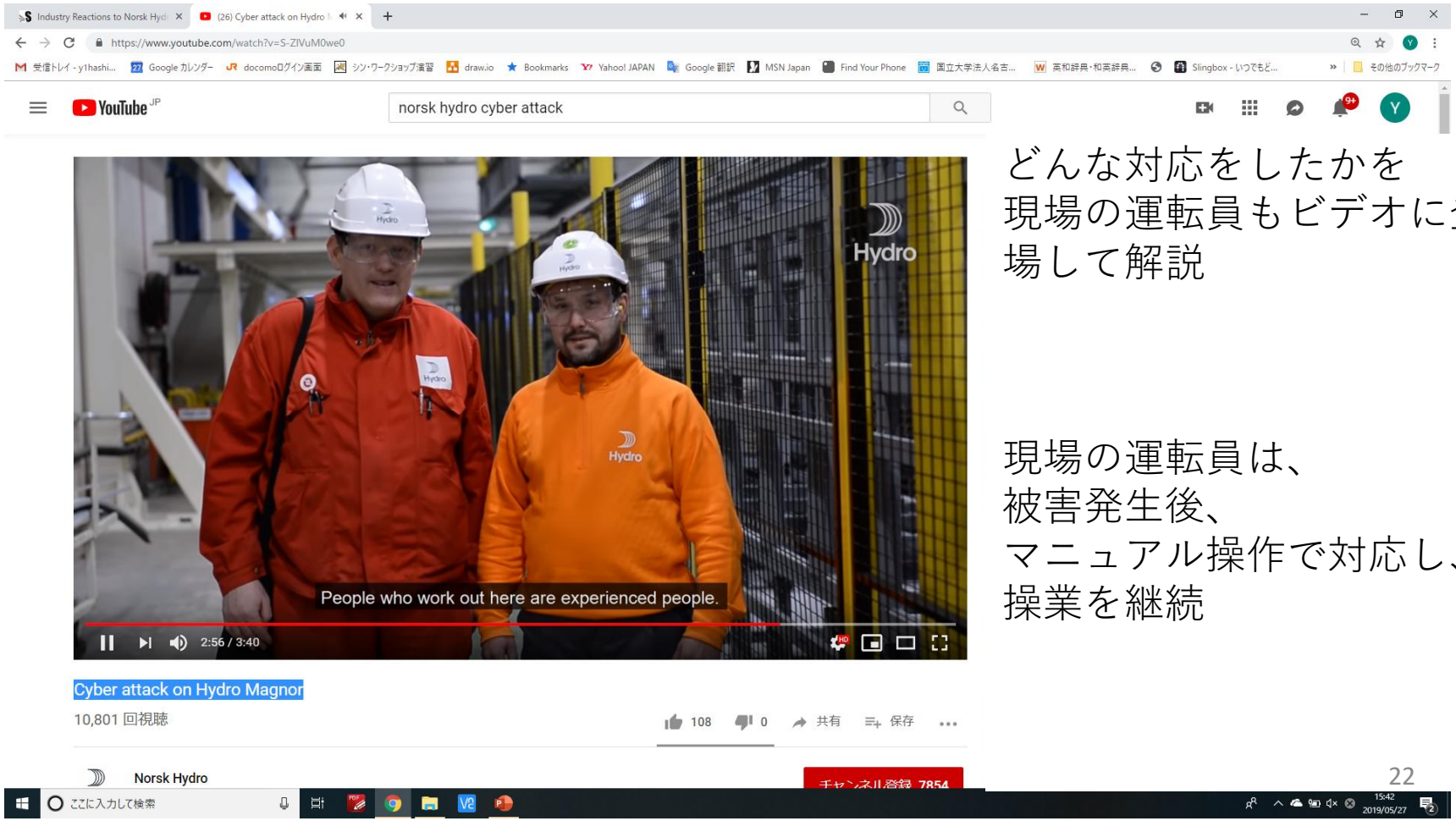


独立防護層（IPL)

第1層：プロセス設計での本質安全
第2層：基本プロセス制御BPCS
第3層：BPCSと区別された重要アラーム
第4層：安全計装SIS (緊急遮断ESD)
第5層：物理層(I) 安全弁など
第6層：物理層(II) 防液堤など
第7層：プラント内緊急対応計画
第8層：地域防災計画

Norsk Hydro社のインシデント対応
ノルウェイのアルミ工場での被害報告

YouTube: Cyber attack on Hydro Magnor
いち早く報告するとともに、説明動画も公開



どんな対応をしたかを
現場の運転員もビデオに登場して解説

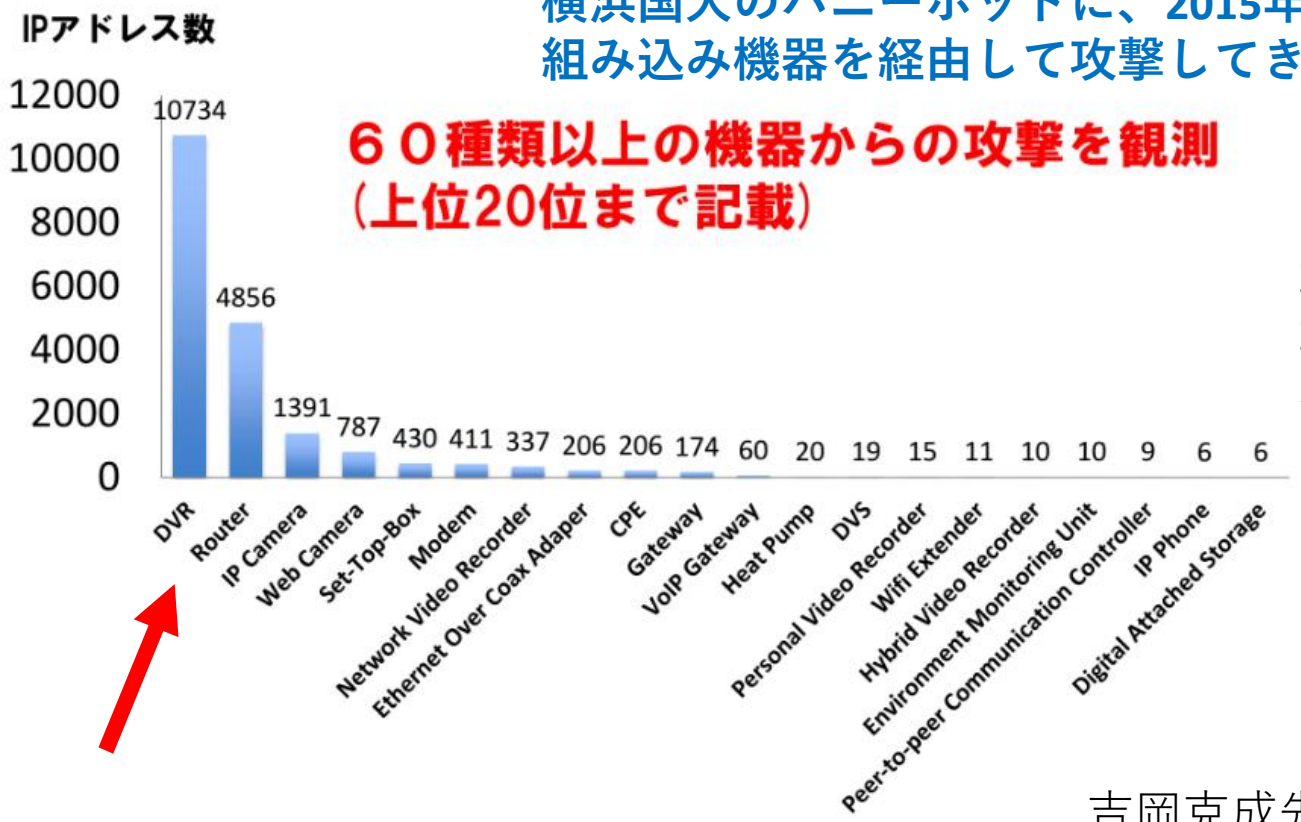
現場の運転員は、
被害発生後、
マニュアル操作で対応し、
操業を継続

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、
セキュリティを考えないと、犯罪に加担してしまう。

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

トップは防犯カメラのデッキ！

吉岡克成先生 （横浜国立大学）
提供資料より

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。

MES（Manufacturing Execution Systems）

- Production Planning
  プログラム
- Material Management
  プログラム
- Asset Management
  プログラム

Plant Control Systems

- SCADA(Supervisory Control and Data Acquisition System)
  プログラム
- OSS (Operation Support System)
  プログラム
- DCS(Distributed Control System)
  プログラム
- PLC(Programmable Logic Controller)
  プログラム

各プログラムに利用されているモジュールに脆弱性が！

分散しているとセキュリティ管理できない！

開発時はセキュアと思っても…

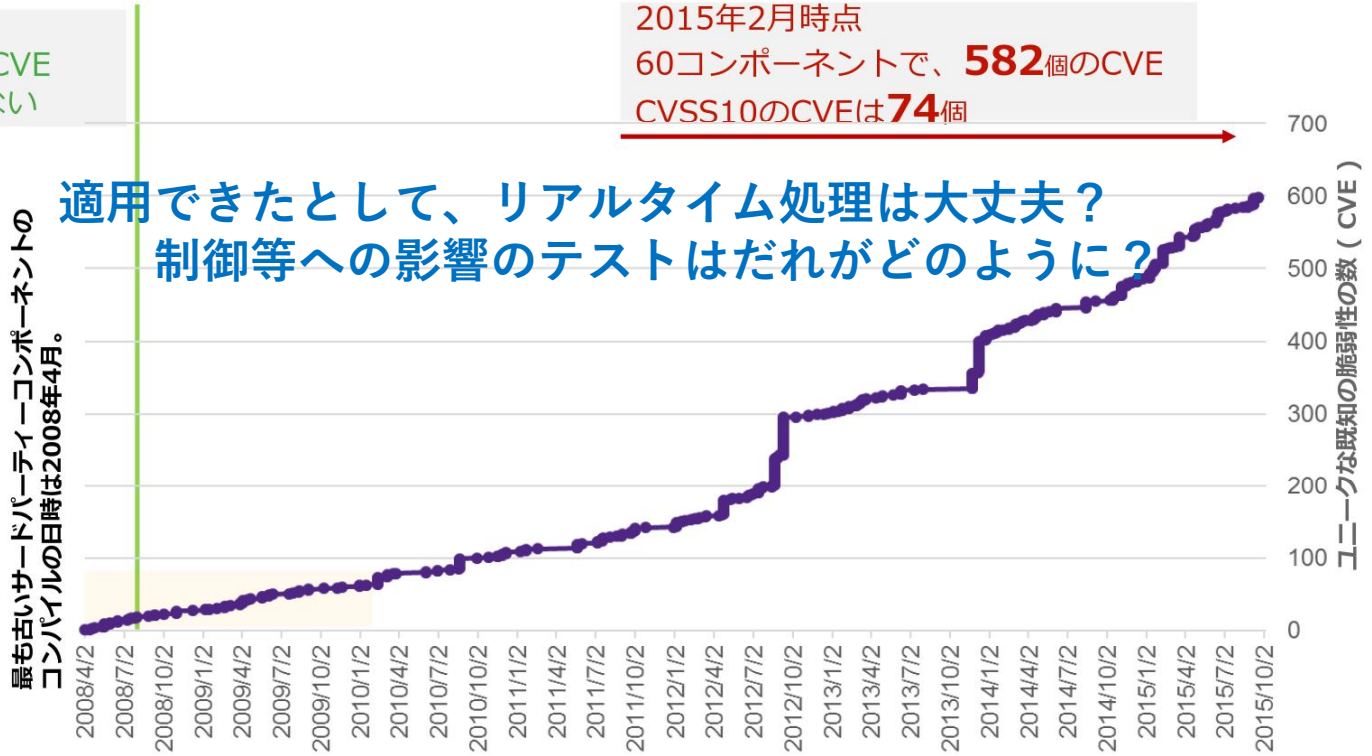
時間経過と共にシステムは相対的に脆弱になる

2008年8月にリリース
２コンポーネントで、22個のCVE
CVSS10のCVEは発生していない

2015年2月時点
60コンポーネントで、**582**個のCVE
CVSS10のCVEは**74**個

適用できたとして、リアルタイム処理は大丈夫？
制御等への影響のテストはだれがどのように？

- 商用の製品
- 81個のサードパーティーコンポーネントを利用
- リリース当時のコンポーネントは、ほぼクリーン
- 平均で5日間に1つの新しい脆弱性が製品のコンポーネントに影響
- 7年後、もはや安全に利用できる製品とは言えない



Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

CVE:公知の脆弱性情報 CVSS10は深刻なものと示す

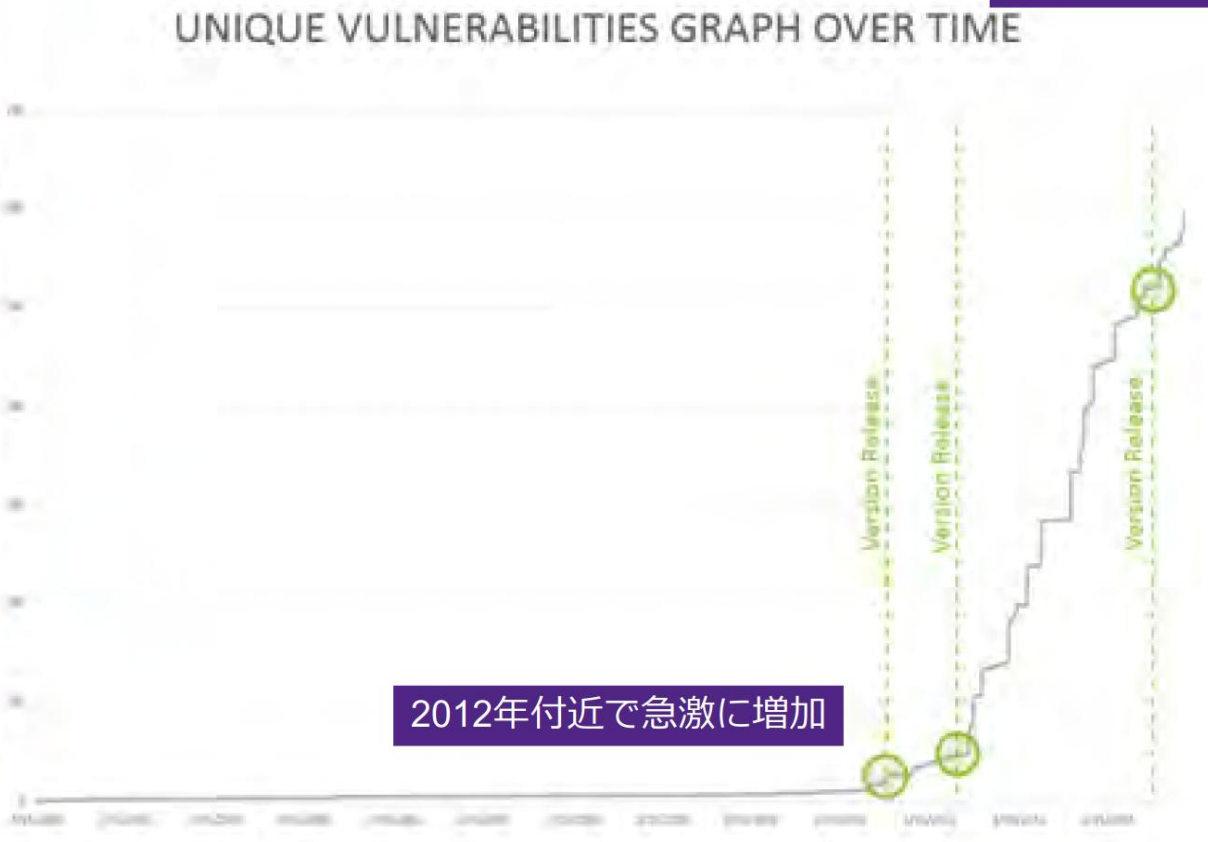
Synopsysから入手した資料より

脆弱性の報告数は激増中

脆弱性が増加し始めている

2012年～2014年の
3回の製品リリースと
脆弱性の増加の
タイミングが一致

- **Huge increase** in number of vulnerabilities entering **NIST CVE database** in the last 3 years
- **Massive spike since 2013** for common software components (such as Java, OpenSSL)
- Vulnerabilities in package: combination of increase in discovered vulnerabilities and addition of new features
- Over 1000% increase in CVEs between 2012 release and 2014 release



Synopsysから入手した資料より

プログラムのセキュリティ管理

検討課題例

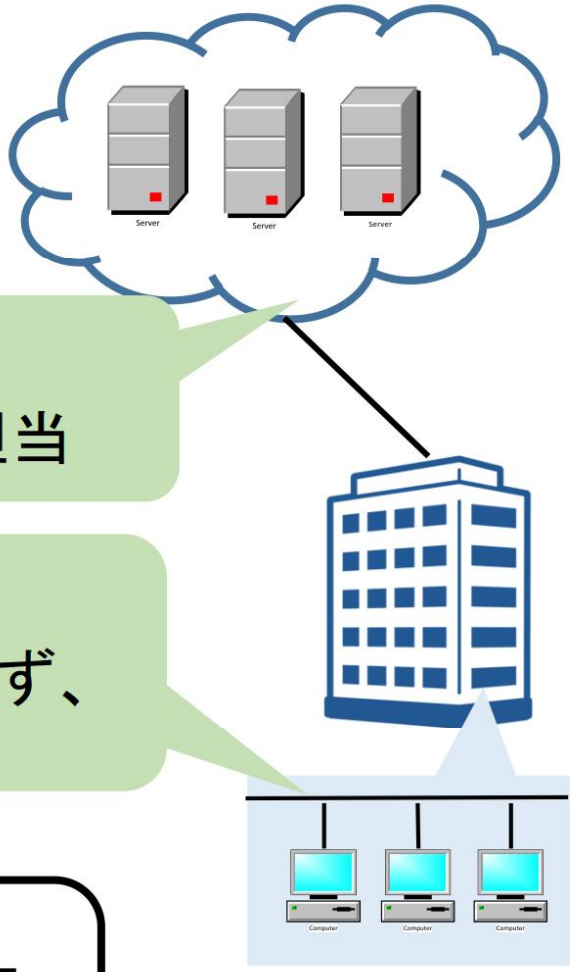
10年前に社員が開発したプログラムに、利用されている
モジュールに深刻な脆弱性が見つかったと報告を受けた。

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？
- モジュールの修正版はいつ入手できるの？
  - それまでそのプログラムは利用しつづけられるの？
- そのモジュールの修正は古いハードに適用できるの？
- 適用できたとして、リアルタイム処理は大丈夫？
  - 制御等への影響のテストはだれがどのように？
- 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

Cloudはサービスを継続しながら、内部で切り替え、セキュリティ対策

Fogによる製造現場への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

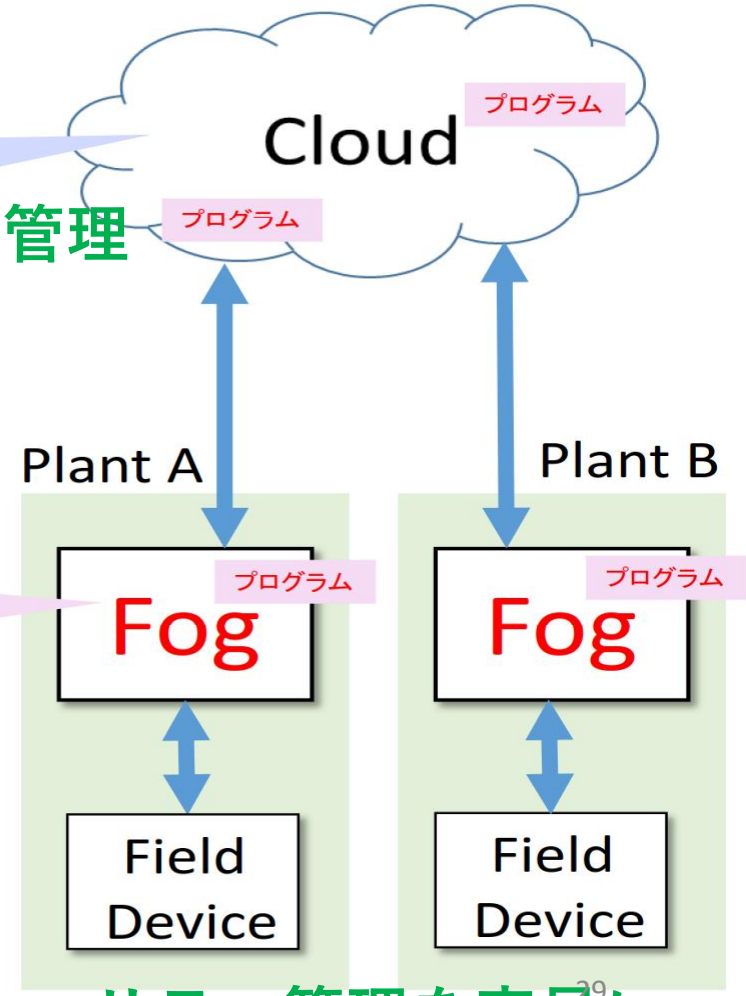
セキュリティ専門家による集中管理

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

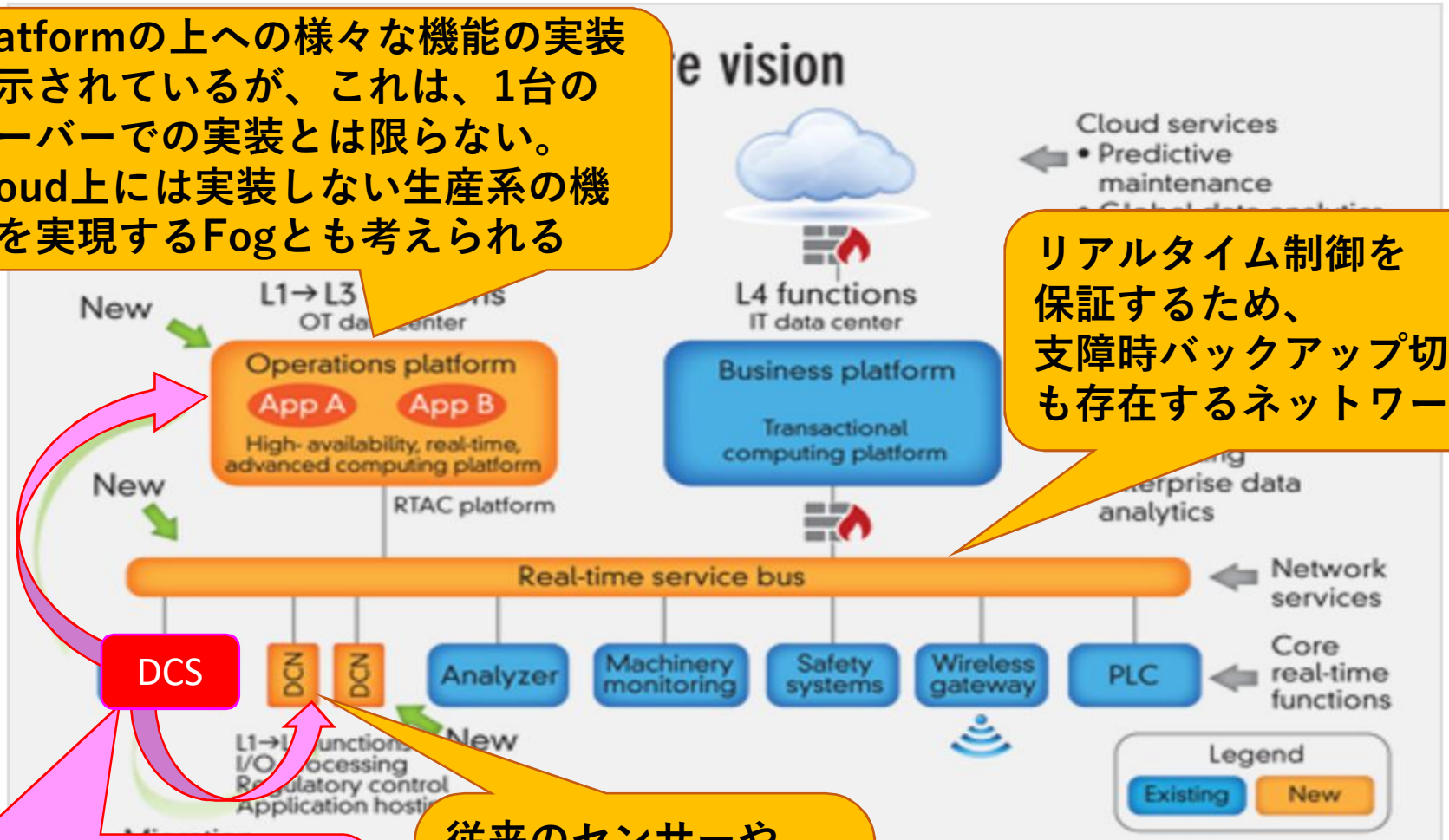
資産管理は現場だが、
セキュリティは集中管理

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



個別のデバイスはシンプルにして、セキュリティ管理を容易に

ExxonMobilが提唱する次世代制御システム



Platformの上への様々な機能の実装が示されているが、これは、1台のサーバーでの実装とは限らない。Cloud上には実装しない生産系の機能を実現するFogとも考えられる

リアルタイム制御を保証するため、支障時バックアップ切替も存在するネットワーク

DCSは更新せずSCADA機能はAppへ、コントローラはDCNへと移行

従来のセンサーやシングルループコントローラ等はコネクタを介してネットワークに接続

このような構造を実現するシステムはハネウェルや横河にも、すでに存在するが、オープンではない。

制御系セキュリティの問題点

- **きりがない**
  - 新たな悪意の攻撃がつぎつぎと現れる
  - 今日大丈夫な対策も明日はだめかも
- **不便を強いられる**
  - パスワード入力を強いたら、緊急時対応でトラブルが発生するかも
  - 正門で持物検査を厳密にしたら、行列ができて、工事も遅れるかも
- **やらないわけにはいかない**
  - 社会的責任（被害は社内にとどまらない）
- **安全だけでなく、事業継続の観点も重要**
  - アタックサーフェイスが関連するシステムすべてにセキュリティ対象が社内にとどまらない

⇒システマティックなセキュリティマネジメント

人並を志向するのもいいかもしれないけど、
いいわけのためではなく、有効でないとね

制御系サイバーセキュリティへの基本スタンス

- サイバー攻撃は所詮、情報系しか操作できない。
  プラントとの接点はコントローラ(測定端･操作端)しかない。
- **サイバー攻撃は「悪意の誤操作、悪意の誤動作」**とみなすことができ、
  誤操作、誤動作は安全解析で検討済みのはず。
- 事故の規模は攻撃の手口で決まるのではなく、制御対象で決まる。
- プラントには、制御以外に多重な安全対策がなされている。

  （全停電で、原料・熱源をFail-Close,冷却をFail-Openで安全停止）
- 気づけなかったら、制御で事故は起こせてしまうかも

  （Startupに原料・熱源全開、Shutdownに冷却全閉はありうる）
- 守るべきものからセキュリティ対策を考えたら、
  地に足の着いた議論ができるに違いない。

脆弱性は存在するし、攻略されるという前提で

- やられない対策には限界があるので、
  やられてもいう観点での対策が重要
- **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

リスクを意識した柔軟な対応能力をつける

プラント運転の立場での
サイバー攻撃への取組みとは？

- サイバー攻撃まで、自分の仕事にしたくないけど、
  事故が起こったら、命の危険にさらされるのは現場の人間
- サイバー攻撃に対する対応って、情報技術者が頑張れば
  プラントに危険は及ばないはず？
- サイバーセキュリティを勉強しろというけど、勉強したら、
  サイバー攻撃は防げるのか？
- サイバー攻撃が起こった場合、現場の人間は何ができるの？
- 現場によってリスクが異なるのだから、
  現場の人間に主体的に考えてもらわないと、
  いざというときうまく機能できないのでは？
- **起こる前に、何を考えておけばいいの?**

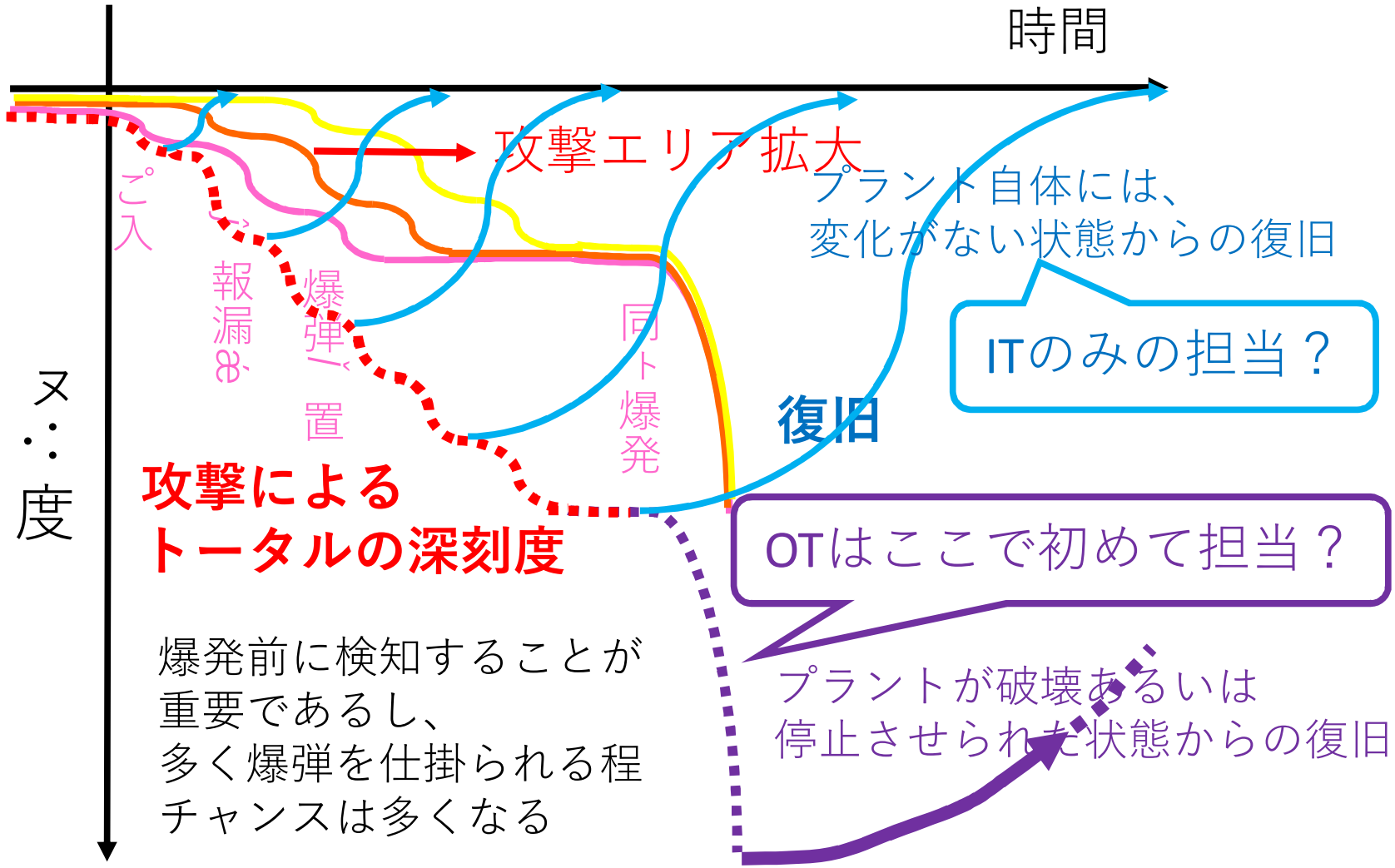
いざというときにできることは
遮断と手動操作

- サイバー攻撃で物理的変化を生じさせるには、コントローラ（センサかアクチュエータ）の操作が不可欠

  サイバー攻撃は、コントローラの悪意の誤動作・誤操作

- 安全解析で、コントローラの誤動作、誤操作のリスクは解析済みで、コントローラが壊れても事故が発生しないよう多重の対策がなされている
- 通信を遮断して、手動で操作したら、サイバー攻撃は手を出せない
- しかし、変化を隠蔽されたら、切り替えることができず、事故が発生する危険性がある。
- 気づくことが最重要であり、気づいた際に被害を局在化させ、復旧を早期化できる構造を確保することが必要である

物理的変化が起こってからでは遅い！



複数個所で同時に被害を発生させることで、被害が甚大になる
（救急車も消防車も間に合わない）被害が発生する前になんとか

コントローラは指示通り動くのが仕様

製造現場には、サイバーリスクがいっぱい！

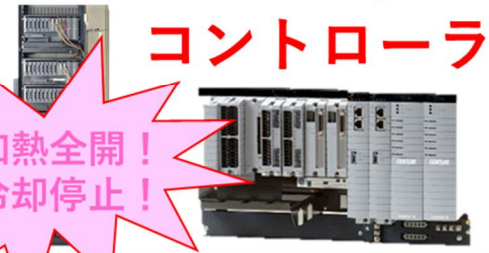
運転支援システム　高度制御システム　生産管理サーバー　設備管理サーバー

リモコンがいっぱい！

特に保守時の管理が問題

ＤＣＳに侵入しなくてもリモコンを攻略できればアクシデントを発生可能

コントローラは正常でも敵か味方はリモコン次第



コントローラ

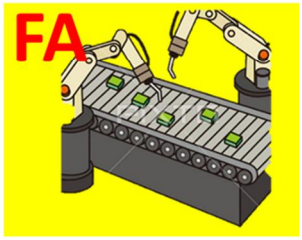
加熱全開！冷却停止！

保守PCをウィルスチェックしても、検出は2,3割に過ぎない

保守点検もサイバーで

多種の外部業者

PA



FA

保守の管理はちゃんと動くかで指定以外の動きをしないというチェックはしない

コントローラへの指示を監視しているか？

- USBの禁止など、入口への対応では、アタックサーフェイスが広く、プラントのインターフェイスであるコントローラから対応を検討すべき
- リモコンの発信元が危険な指示を発信しているかは、そのマシンのシスログをみていても検出できない
- DCSの専用BUSを監視できなくても、高度制御などとのインターフェイスは汎用ネットなので、監視できる
- コントローラごとに、監視ルールを登録すると、保守が煩雑になるかもしれない。IoTの進展とともに、ネットへの登録機器の変化が激しくなると、監視ルールの保守管理の容易さも重要になる
- 一部、操業を継続できる単位で遮断できるように、ネットワークが分割されていれば、早期復旧も図れるし、復旧までの時間の見積もりも容易になる。

ログは身の潔白を証明するためにも

- 安全をプログラムで担保しているのであれば、
  サイバー攻撃にも耐えられるのか？
- 本人は悪意を持っていなくても、
  保守点検で持ち込んでしまうかも（水飲み場攻撃）

https://www.ssaits.jp/blog/security/watering-hole-attack.html

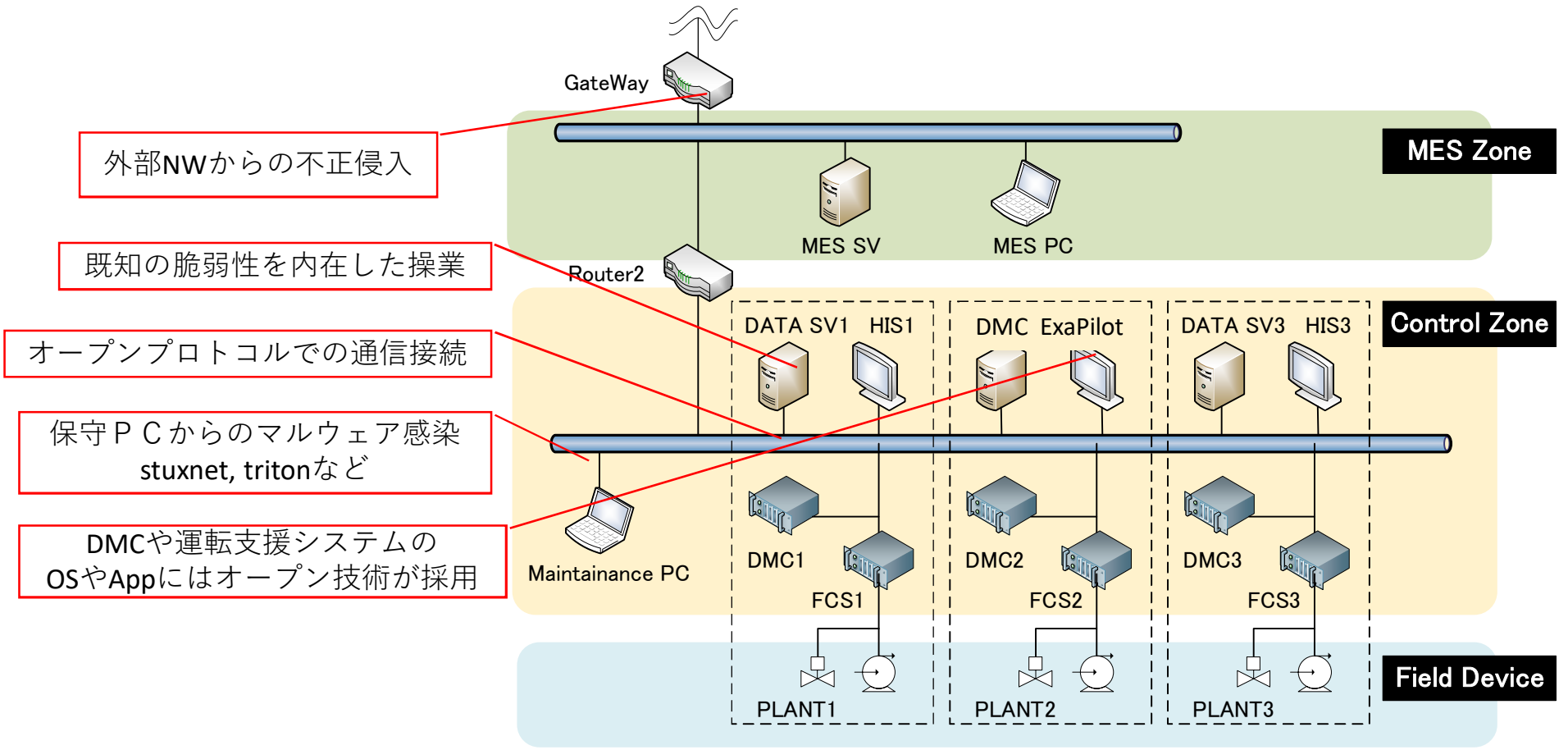
協働ロボットが人を襲う？！

現場担当者の安全対応とサイバー攻撃対応の差異

故障を対象にした対応がサイバー攻撃に対して不適な例とは？

- 変化の影響拡大は、従来の安全対応であれば、
  遮断弁で流れを止めることで防げるが、
  マルウェアの感染は、通信の遮断が必要で、
  判断が遅れると広範囲に拡散してしまう
- マルウェア感染や侵入の痕跡は、リセットすると消滅してしまう可能性が高く、事故解析のための証拠隠滅を意図せずにしてしまう危険性が高い
- 通信を遮断しても操業は可能だが、必要な情報を別の手段で確保するなど操業形態変更を事前に検討しておく必要がある
- 故障では異常原因が一つ見つかれば、その解決で検討済みにできるかもしれないが、犯罪であるセキュリティでは、同時多面な攻撃がなされている危険があり、一つ見つけて解決したとしても、残っている危険性がある。

制御システムにはサイバー攻撃の危険がたくさん



水際での対策には限界がある。
→侵入されたことを早く検知し、隔離し、
プラント操業への被害を最小限にすることが重要

制御系で通信に異常が検知された際のリスク判断は？

- 通信が異常かはＩＴ技術者の判断になるが、それがどのようなリスクにつながるかは、ＩＴ技術者だけでは判断できない
- ネットワークの中に、どのような脆弱性が存在するかはＩＴ技術者の解析対象だが、その脆弱性を利用されたら、どんな事故が発生しうるかの判断はＯＴ技術者の問題
- マルウェアの感染が疑われると、通信の遮断は即座に行うべきなので、疑わしい段階で通信を遮断しての操業モードに移行できるように、操業体制を検討するのはＯＴ技術者の問題
- どんな確認で通信を復旧できるのかはＩＴ技術者の問題
- こまめに遮断できる制御ネットワークの構成は、ＯＴ技術者とＩＴ技術者の協力で検討すべき
- 復旧までの時間の目安を算出するのも連携が必要
- ＩＴ技術者とＯＴ技術者の連携が事後にも事前にも重要

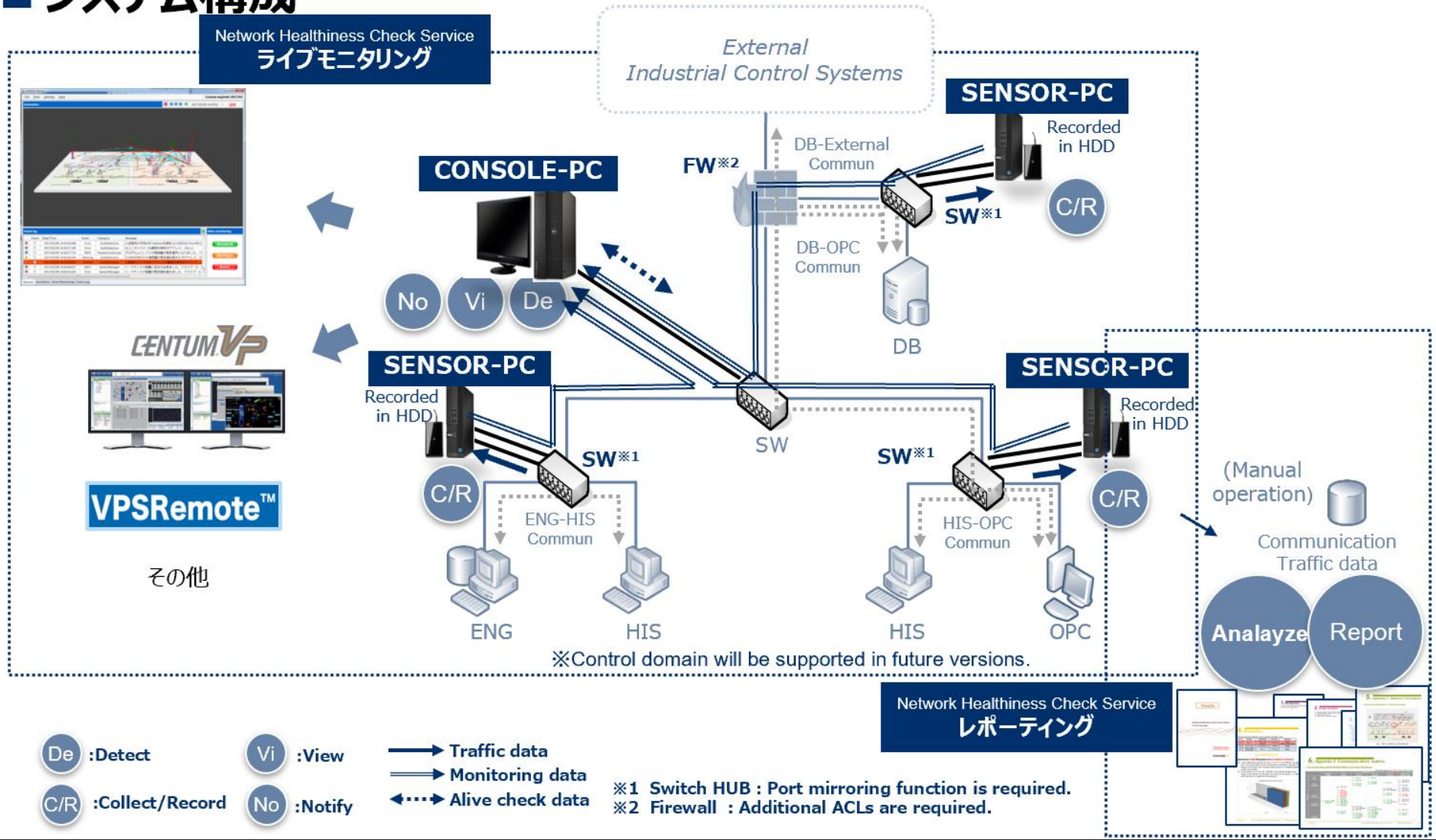
制御ネットワークの監視

- すでに、複数の監視ツールがある。
  - **ネットワーク健全性確認サービス ライブモニタリング（横河電機）**
  - KICS(Kaspersky Industrial CyberSecurity)
  - Indegy SP(東陽テクニカ）
- 監視するのは、無料のツールでも可能
  - Wireshark(パケット監視の有名ツール)
  - Scapy (Pythonモジュール)
  - Honeyd(ハニーポット)

    これらの構築および使用方法は、
    名工大でサポートも可能
- 脆弱性管理とふるまい監視・通信監視を組み合わせたオペレータ支援ツールも開発

概要

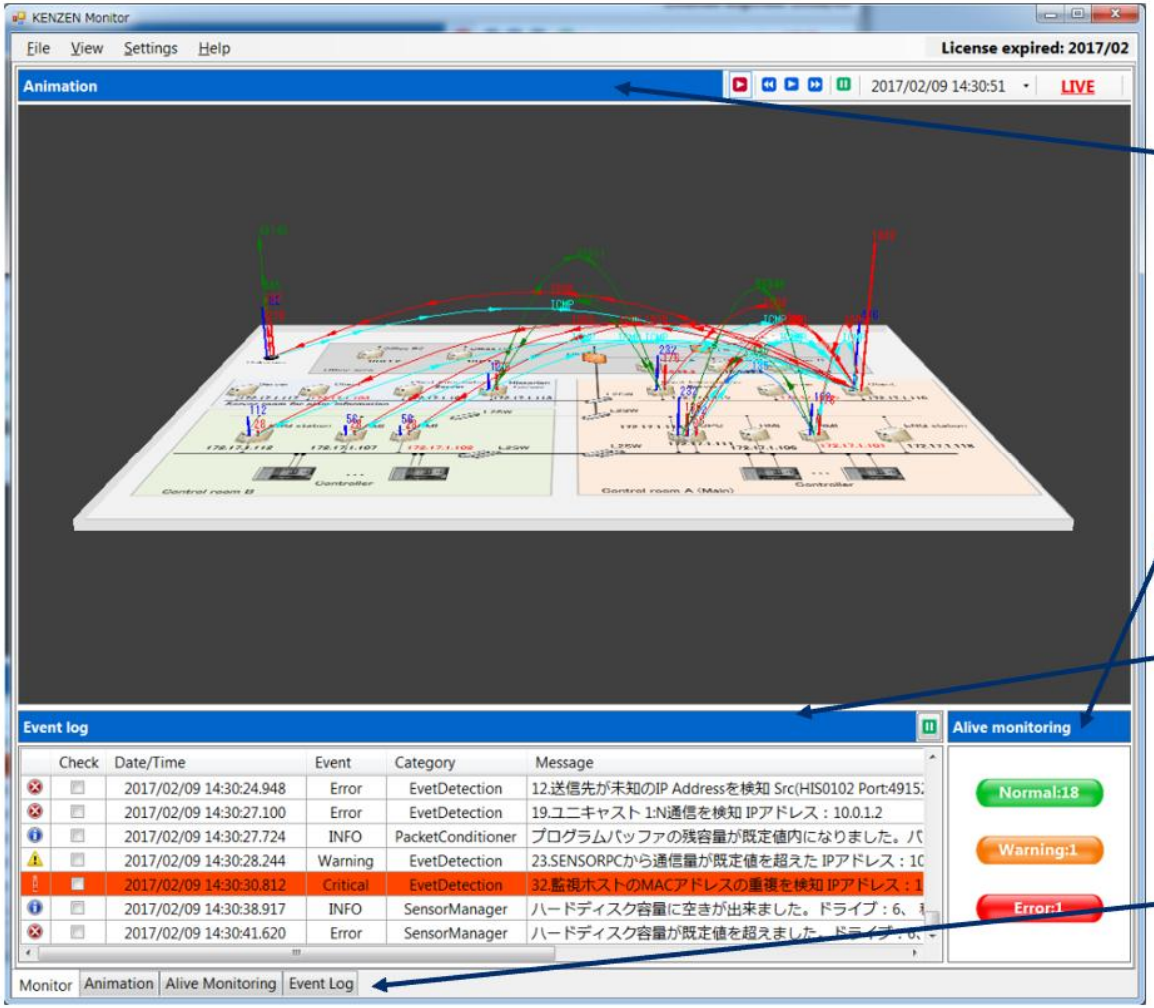
■システム構成



ソフトウェア仕様

■ Monitor画面(コンソールPC画面)

NICTのNICTERをベースにしている



アニメーション画面

- 通信発生状況を立体的にライブ表示
  通信元から通信先へ通信情報(色)：放物線
  PCの送信量/受信量：棒グラフ
- PLAYバック表示
  カレンダ指定(年/月/日　時:分:秒)
  選択したイベントログとのカレンダ指定連携

死活監視画面

- 通信応答の状態とその数(状態：数)

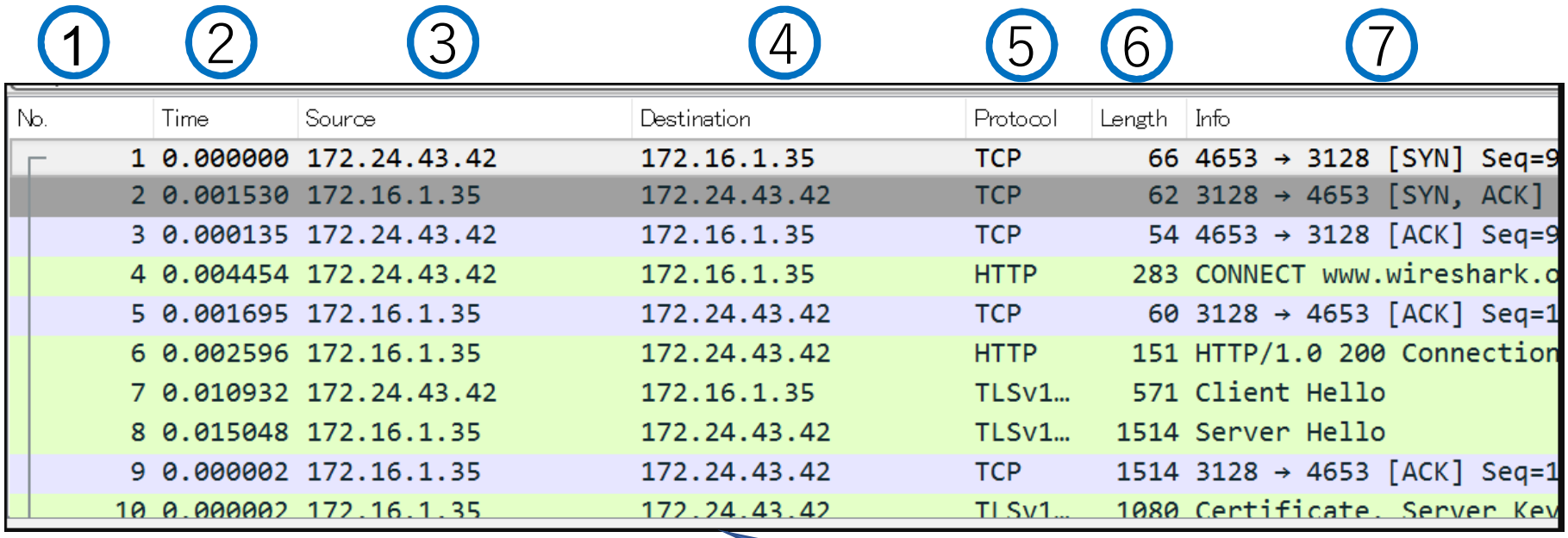
イベントログ画面

- 日付とカテゴリ(4種)およびメッセージを表示
- 最重要カテゴリ(Critical)は色反転で強調表示

画面切り替えタブ

- モニター画面(本画面)
- アニメーション全画面
- 死活監視全画面
- イベントログ全画面

Wiresharkによる通信監視



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.24.43.42	172.16.1.35	TCP	66	4653 → 3128 [SYN] Seq=9
2	0.001530	172.16.1.35	172.24.43.42	TCP	62	3128 → 4653 [SYN, ACK]
3	0.000135	172.24.43.42	172.16.1.35	TCP	54	4653 → 3128 [ACK] Seq=9
4	0.004454	172.24.43.42	172.16.1.35	HTTP	283	CONNECT www.wireshark.o
5	0.001695	172.16.1.35	172.24.43.42	TCP	60	3128 → 4653 [ACK] Seq=1
6	0.002596	172.16.1.35	172.24.43.42	HTTP	151	HTTP/1.0 200 Connection
7	0.010932	172.24.43.42	172.16.1.35	TLSv1…	571	Client Hello
8	0.015048	172.16.1.35	172.24.43.42	TLSv1…	1514	Server Hello
9	0.000002	172.16.1.35	172.24.43.42	TCP	1514	3128 → 4653 [ACK] Seq=1
10	0.000002	172.16.1.35	172.24.43.42	TLSv1…	1080	Certificate, Server Key

1. 通し番号
2. 通信が行われた時間
3. 送信元のIPアドレス
4. 受信元のIPアドレス
5. 通信に使用されているプロトコル
6. Byteで表現されたフレームの長さ
7. 通信の概略

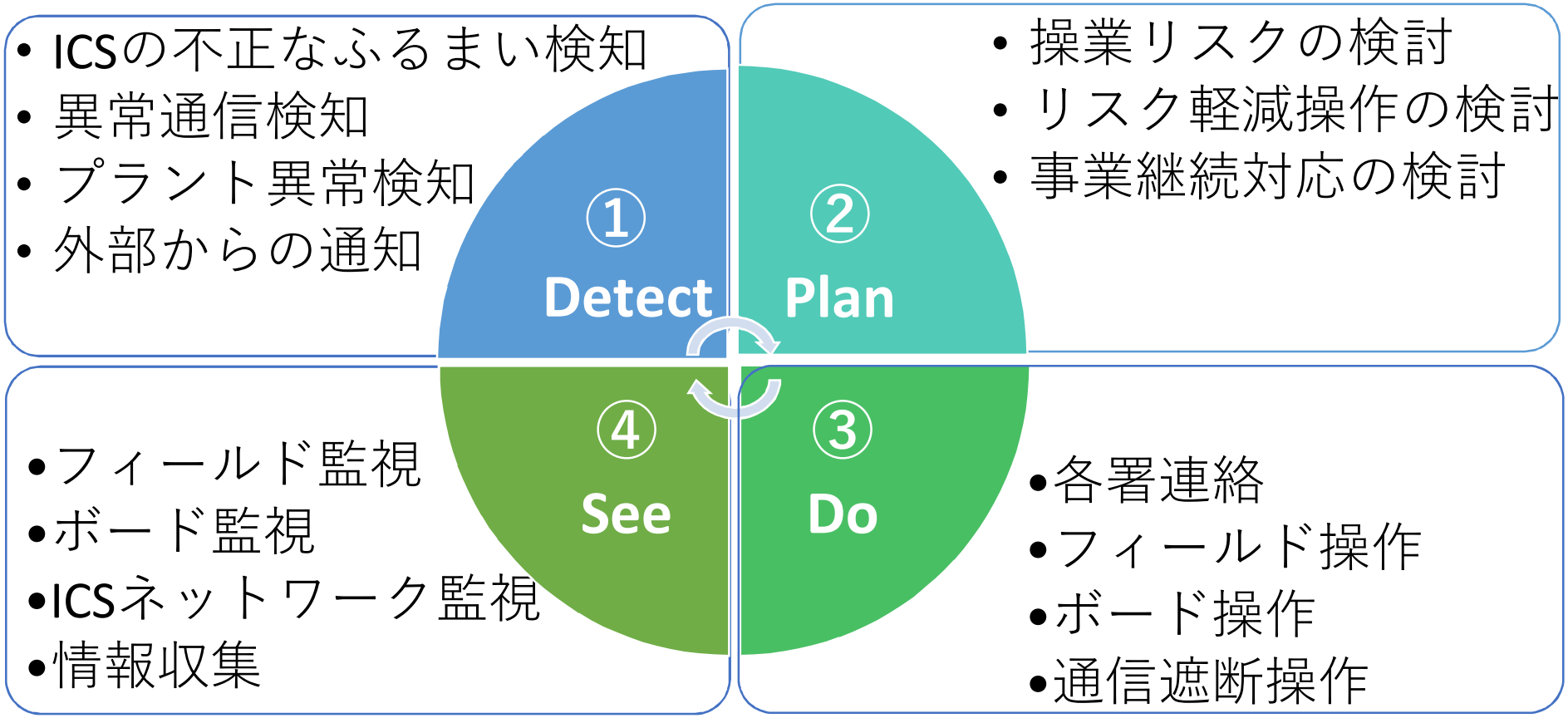
無料でも多くの情報を獲得できるが、
これをオペレータに示しても
どう利用してよいかわからない！

いかに危険な状況なのか？
どんな操作につながるのか？

いざという時にできるのは通信遮断

- どのタイミングで、どこの通信を遮断すべきか？
- 遮断して隔離したシステムは、信用できない状態だが、操業継続できるか？
- いざとなったら、手動で操業継続あるいは安全に停止できるか？
- 通信が遮断して操業を継続するとき、操業データを如何に入手して、実績管理等を行うか？
- 感染拡大の速度は速いので、疑わしい時点で遮断すべきだが、遮断した状態での操業モードへの切換は準備されているか？
- 遮断した状態から通信を復帰するためのルールが定められているか？

サイバー攻撃に対する
現場緊急オペレーションモデル



現場における意思決定シナリオ例

①Detect ②Plan ③Do ④See

① DMCから異常検知アラーム発報

（DMCは脆弱性ありand権限昇格イベント検知）

②DCSではプラントの異常は検出されていないが

DCSにも脆弱だあるので、④ DMC周りの様子見を判断

①MESでDMCからの攻撃検知アラーム発報

（MESは脆弱性なしand DMCからMESへリモートログイン失敗）

②DMCが乗っ取られていて、MESへ攻撃をしていると推定

③-1 DMCが変な挙動をしているみたいだからDMCをNWから遮断

DMCをフォレンジックにまわして、バックアップに切換

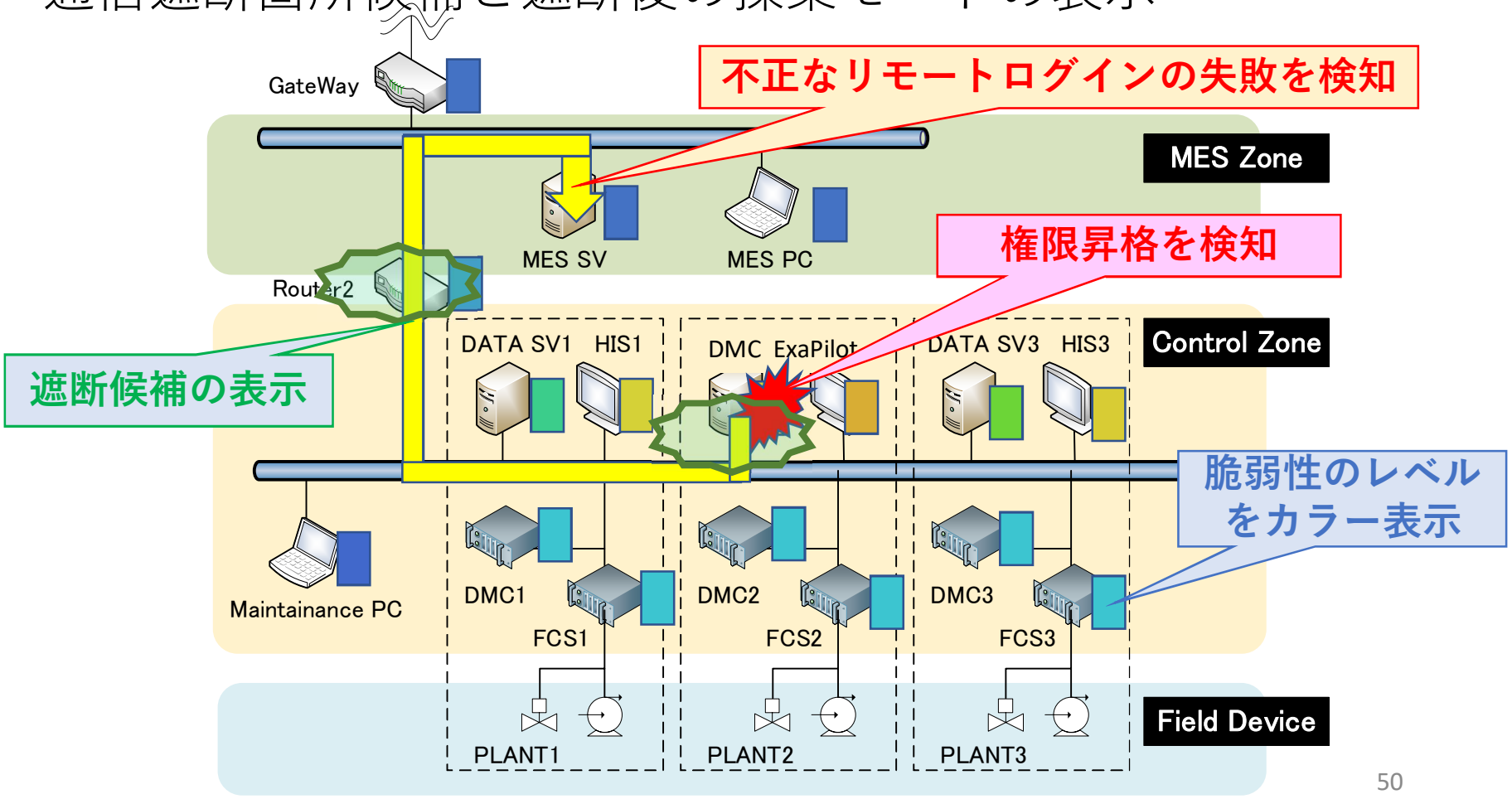
③-2 DMCからMES層へ被害が拡大する前にDCSとMESの間を遮断

実績情報などを別ルートでMESに送るなど操業モードを切換

~~④-3 今プラントへの影響は確認されていないからやっぱり様子見~~

脆弱性情報と監視情報に基づく意思決定支援

- 脆弱性情報と機器・NW監視情報を組合せたアラームの構築
- 通信遮断箇所候補と遮断後の操業モードの表示



リスク評価と操業モード切替

- 単に異常な通信を検知しただけで、プラントを停止することは考えにくい。
- サイバー攻撃により物理的な変化が発生させられる危険性はその検知された箇所により異なるし、対応も異なる。
- 制御ネットワーク内にか存在する脆弱性によっても、異常な通信の危険性が異なる。
- 例えばIEに脆弱性があると、トンネルが簡単に開くが、脆弱性がなければ同じ攻撃でもトンネルは開かない。通信やふるまいに異常が検知された場合、そのリスクは脆弱性とそこにつながるコントローラの先のプラントのリスクが関係して評価される。

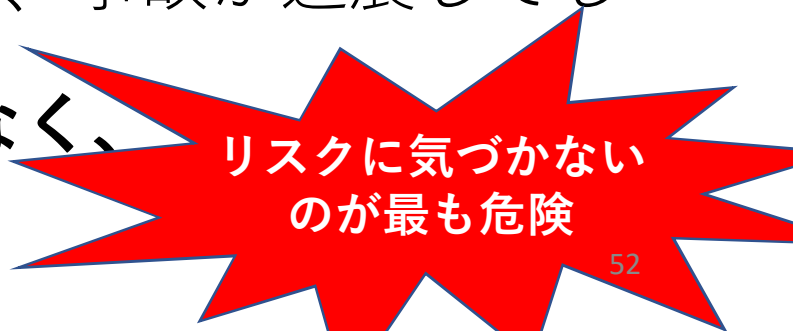
ITのプロとOTのプロの交流

- 相手から何を求めるべきで、
  自分の行動が相手にどう迷惑をかけるか
  互いに理解しあおうとすることが重要

  （OTの例）
- 通信パケットなどはわからないが、
  サイバー攻撃の可能性があるなら教えてほしい
- 電源を切ってみるとかしたら直ったと思っていたら、サイバー攻撃の証拠隠滅をしていた

  （ITの例）
- この通信がサイバー攻撃だとしたら、どれくらい危険なことになる可能性があるのだろうか
- パスワードやユーザー制限を厳密にしたら、トラブル時に、オペレータの入力が頻発して、事故が進展してしまった

互いの低いレベルの知識共有ではなく、
リスク意識の共有が重要である。



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
- 自分もプロとして、相手もプロとして敬意をもち連携できるＩＴとＯＴの技術者を育成する
- 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
- 緊急時にできることは、遮断と手動操作
  - 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
- 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

⇒どのような連携が求められるかをイメージできる演習

内閣府SIP, 経産省 ICS-CoEでの人材育成プロジェクト

制御系へのサイバー攻撃防御の基本スタンス

- サイバー攻撃で物理的変化を生じるには、コントローラ（センサかアクチュエータ）の操作が不可欠
- 安全解析で、コントローラの誤動作、誤操作のリスクは解析済みで、コントローラが壊れても事故が発生しないよう多重の対策がなされている
- 通信を遮断して、手動で操作したら、サイバー攻撃は手を出せない
- しかし、変化を隠蔽されたら、切り替えることができず、事故が発生する危険性がある。
- 気づくことが最重要であり、気づいた際に被害を局在化させ、復旧を早期化できる構造を確保することが必要である

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

↓

リスクを意識した柔軟な対応能力をつける

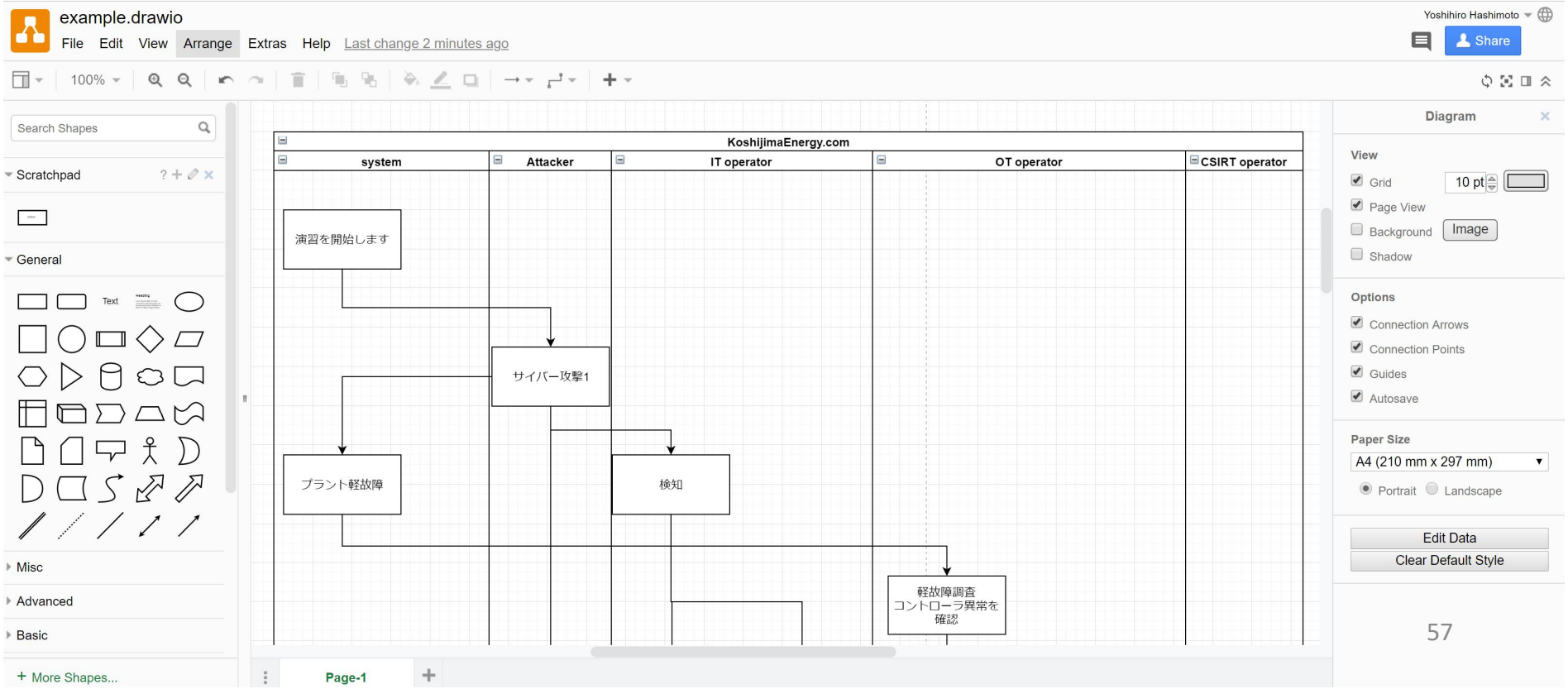
ITとOTの連携を理解する演習

- 各部署の能力向上も必要だが、インシデント対応能力向上には連係の必要性を理解することが大事
- 被害を最小にするために、遮断できるネットワーク構造の設計はＩＴ技術者だけでなく、守るべき対象をよく理解しているＯＴ技術者と相談し、どんな段階で、どこを遮断すれば、どんな操業あるいは部分的な停止で、事業を守れるかを検討して決定すべき
- 物理的変化が発生する前に、対応を始めるには、どのような検知で、どのようなアクションを取るべきかは通信の監視を理解しているＩＴ技術者とプラント操業を理解しているＯＴ技術者の連携による検討が必要
- 上位通信ネットワークからの侵入だけでなく、コントローラの保守など現場からの感染や部品や原料、あるいは配送に関わるシステムの不調での操業停止など、多方面から事業継続のリスクを解析すべきで各部署の連携も必要

Tsurumai GO!を核にした インシデント対応演習の実施①

① 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（このシステムは未完成）

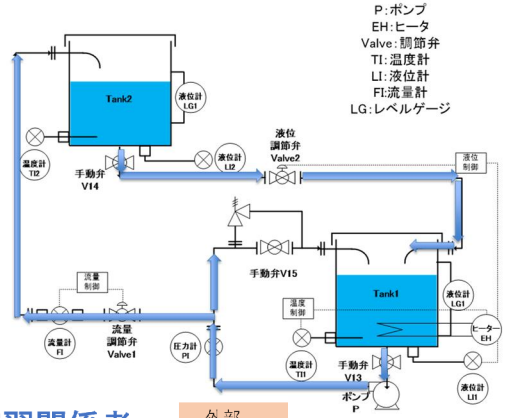


Tsurumai GO!を核にした インシデント対応演習の実施②

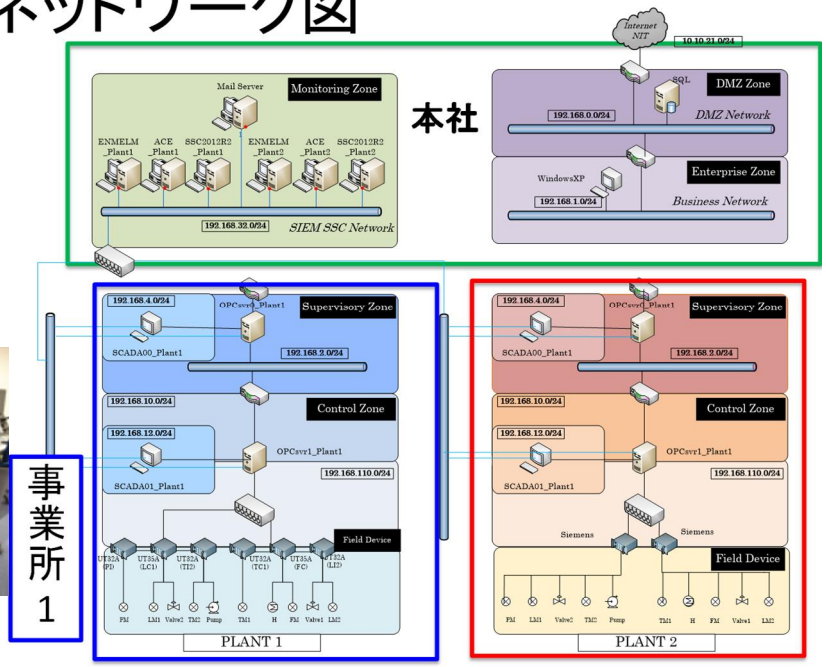
② 演習対象のインシデント対応体制の確認

(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)

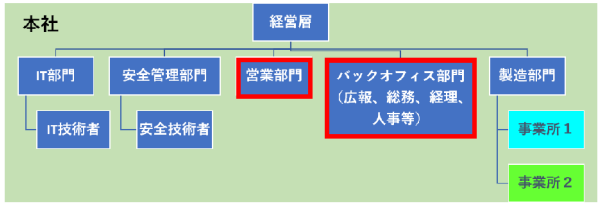
- **守るべきプラントと組織とネットワーク構造の確認**

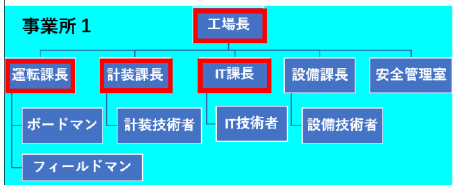


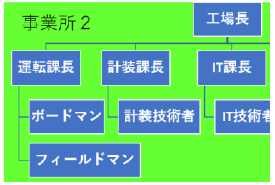
ネットワーク図



インシデントレスポンス演習関係者





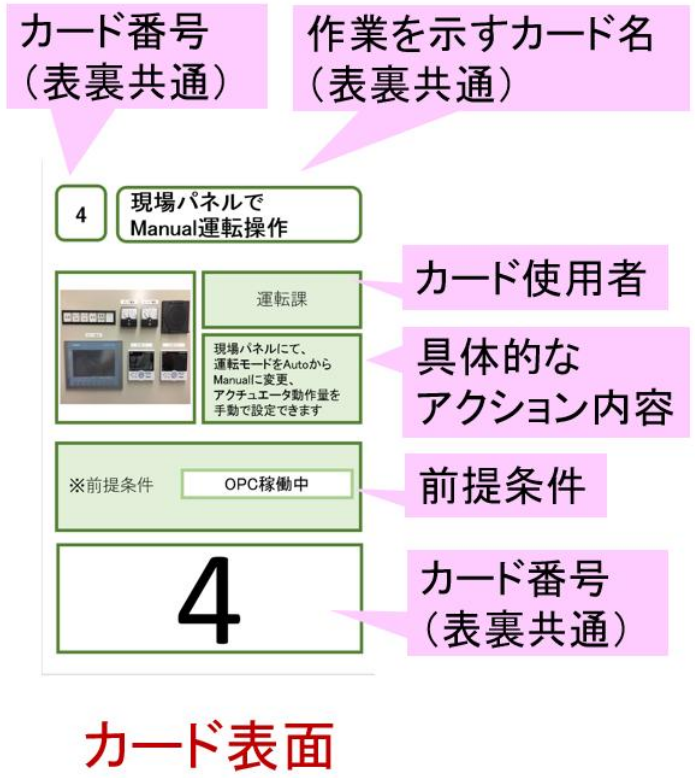


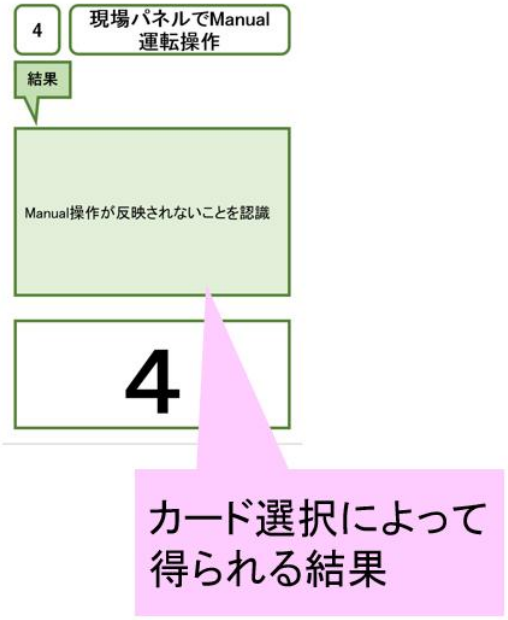
Tsurumai GO!を核にした インシデント対応演習の実施③

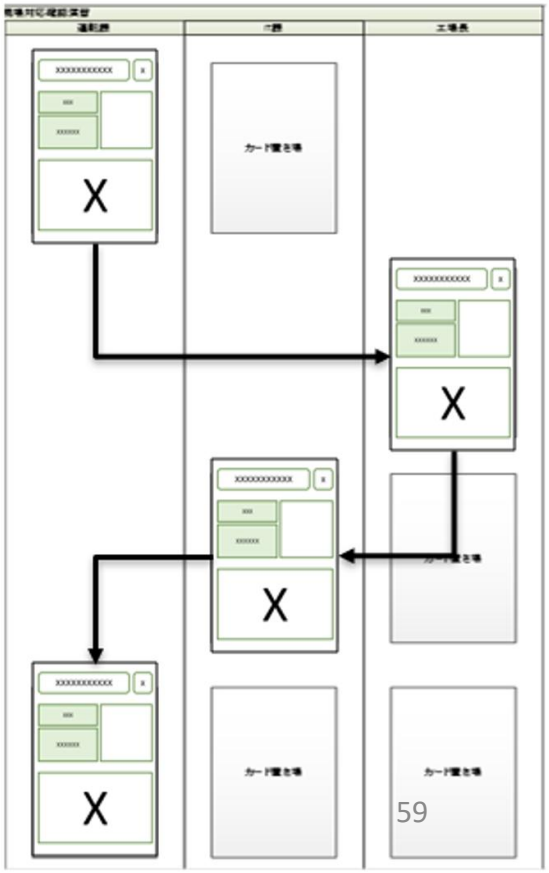
③ 演習対象のインシデント対応の流れの確認

(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**

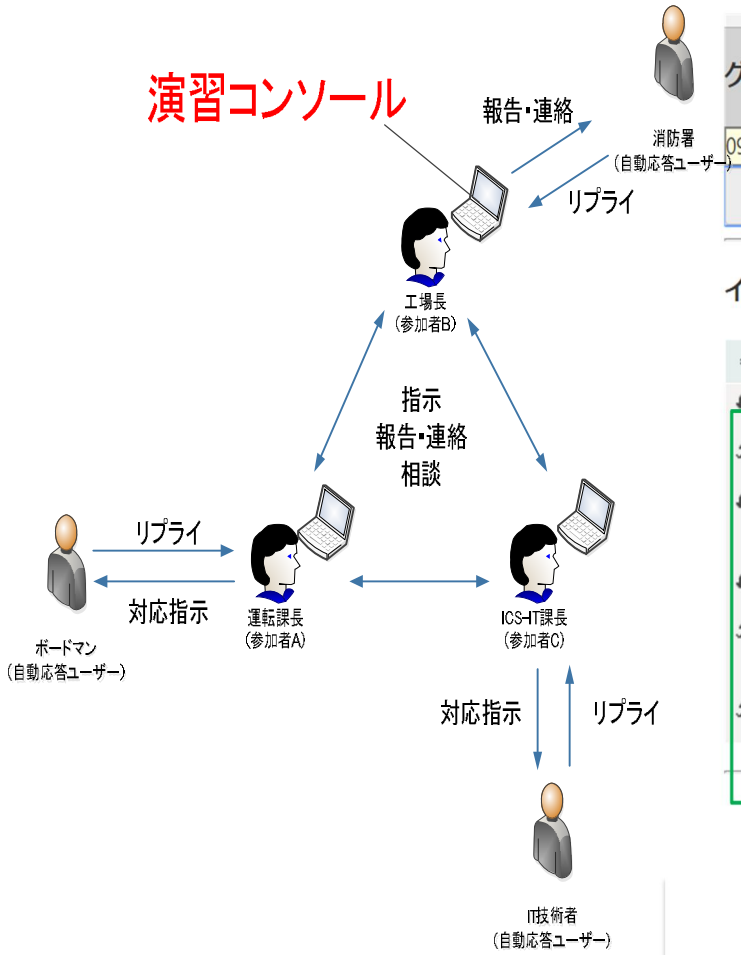






Tsurumai GO!を核にした インシデント対応演習の実施④

④ Tsurumai GO!による演習実施

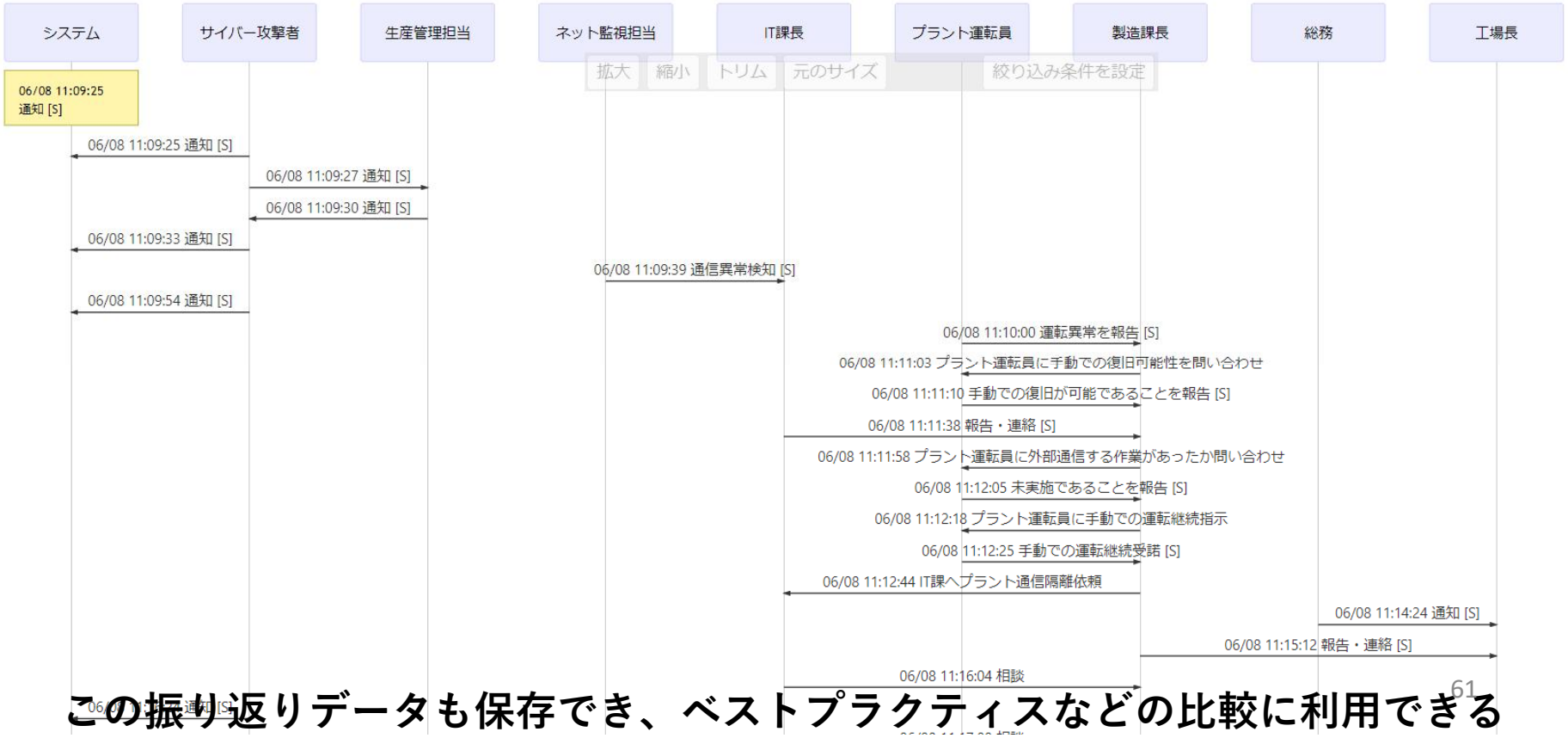


ゲーム参加者は、メールのような画面で、状況を理解し、
実施事項をメニューから選択したり、文字入力して、
自動応答者も含め関係者に連絡して、ゲームを進行

Tsurumai GO!を核にした インシデント対応演習の実施⑤

⑤ Tsurumai GO!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

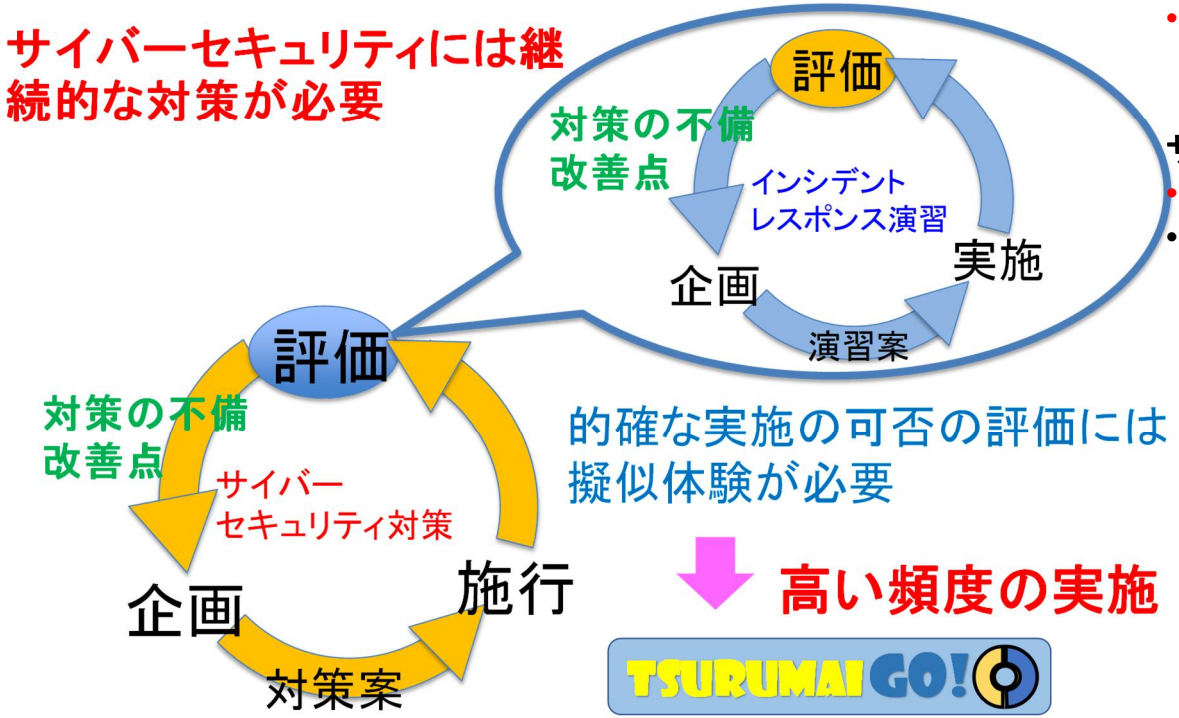


この振り返りデータも保存でき、ベストプラクティスなどの比較に利用できる

Tsurumai GO!を核にした インシデント対応演習の実施⑥

⑥ 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

サイバー攻撃対策の評価にも
インシデント疑似体験が有効



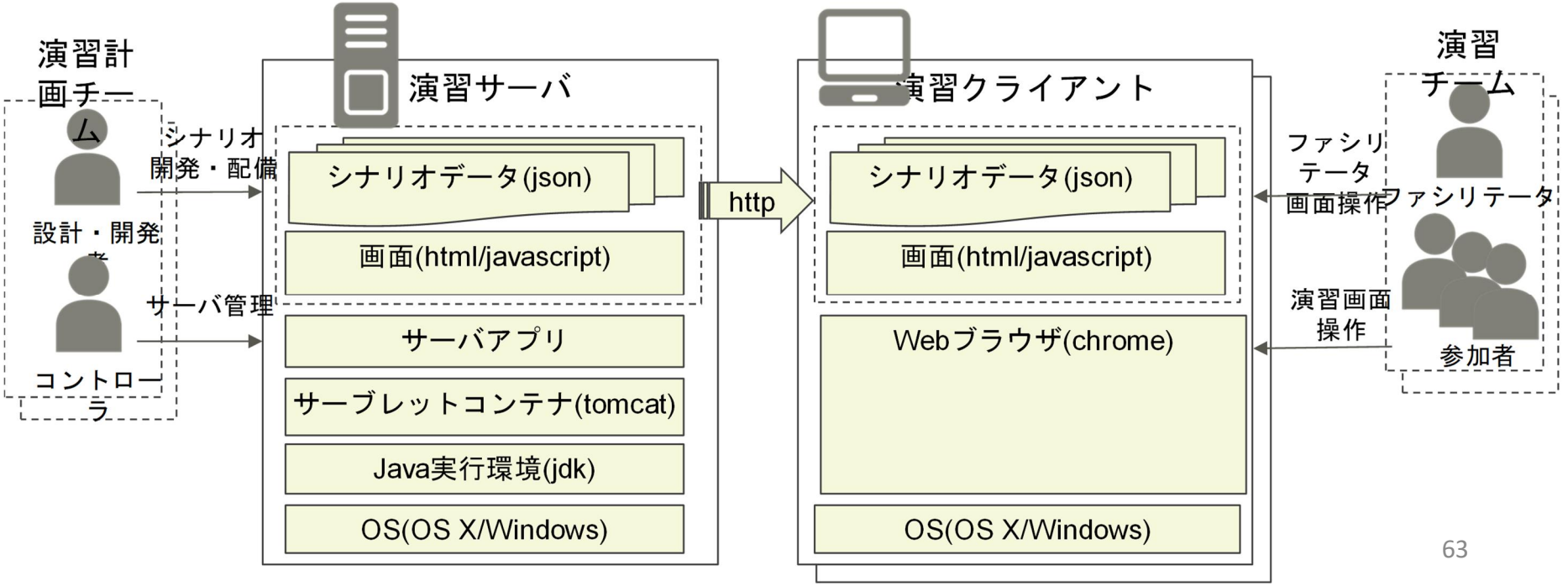
安全の観点での検討
- Safety-Ⅰ 事故を起こさない能力
- Safety-Ⅱ 想定外な事故でも抑え込める能力
  レジリエンス

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
- 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

リスクを意識した柔軟な対応能力をつける

演習実施システムの構造

Tsurumai GO!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、2019年9月に公開予定



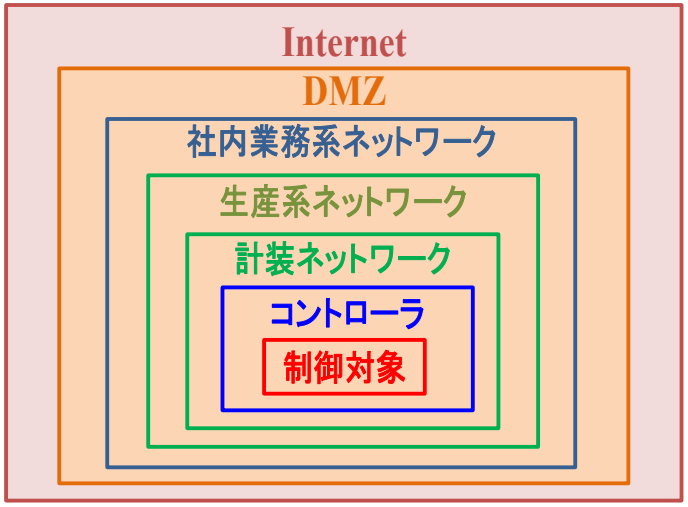
安全対応シナリオベース演習の展開

- 制御系セキュリティにとって、事業所ごとの個別性は重要であり、
  事業所ごとの開発努力は必要である。
- ゲーム形式の演習システムを開発し、
  各事業所で、入力データを作成していただくことで、
  事業所に適した個別の演習を実現する。
- 開発したデータを共有し、
  業種ごとの演習用データのブラッシュアップや、
  演習効果のベストプラクティス評価も可能にする。

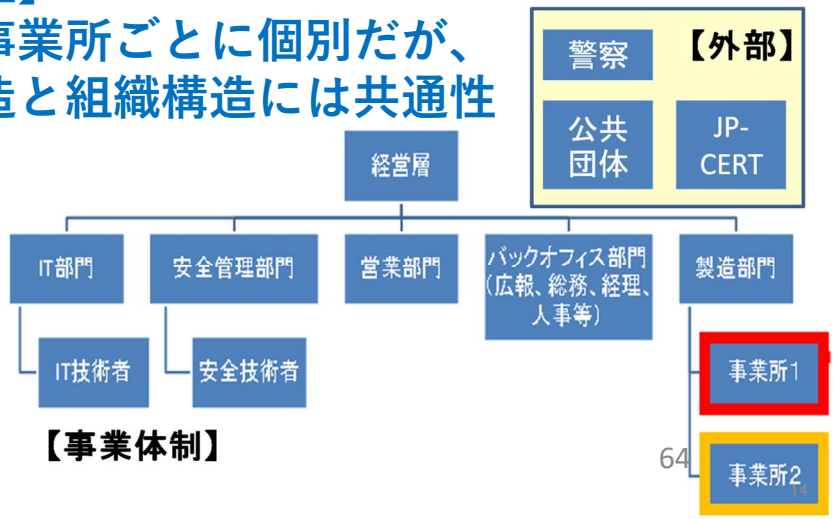
シナリオ型演習

演習

個別の努力を国全体の向上につなげる



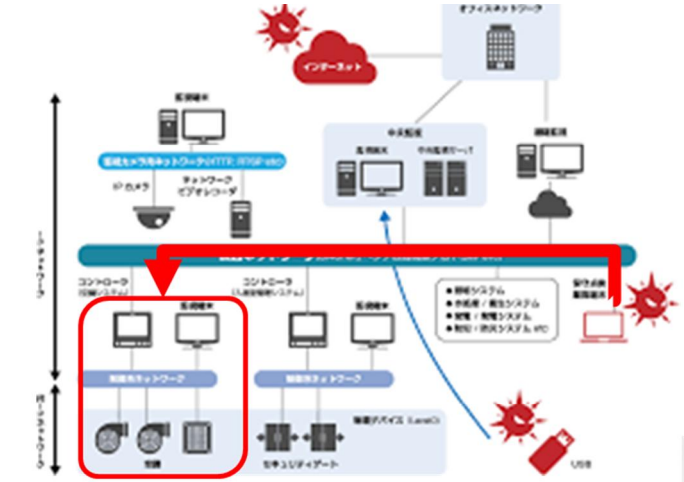
【個別性と汎用性】
アクシデントは事業所ごとに個別だが、
ネットワーク構造と組織構造には共通性



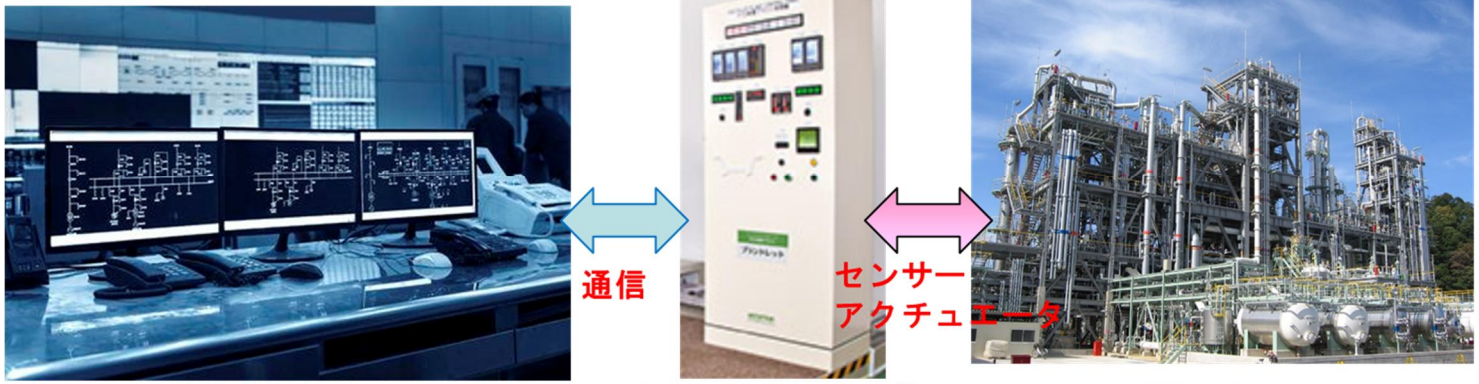
【事業体制】

制御系のサイバーリスクを体験する演習

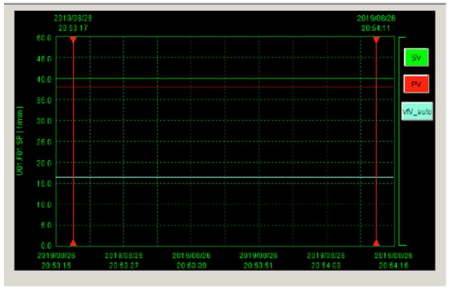
- 制御系を構築することでその構造を理解
- 構築した制御系をKali Linuxで自分で攻撃
- 攻撃されている状況での通信を監視し、検知できるとした場合の防御について考える

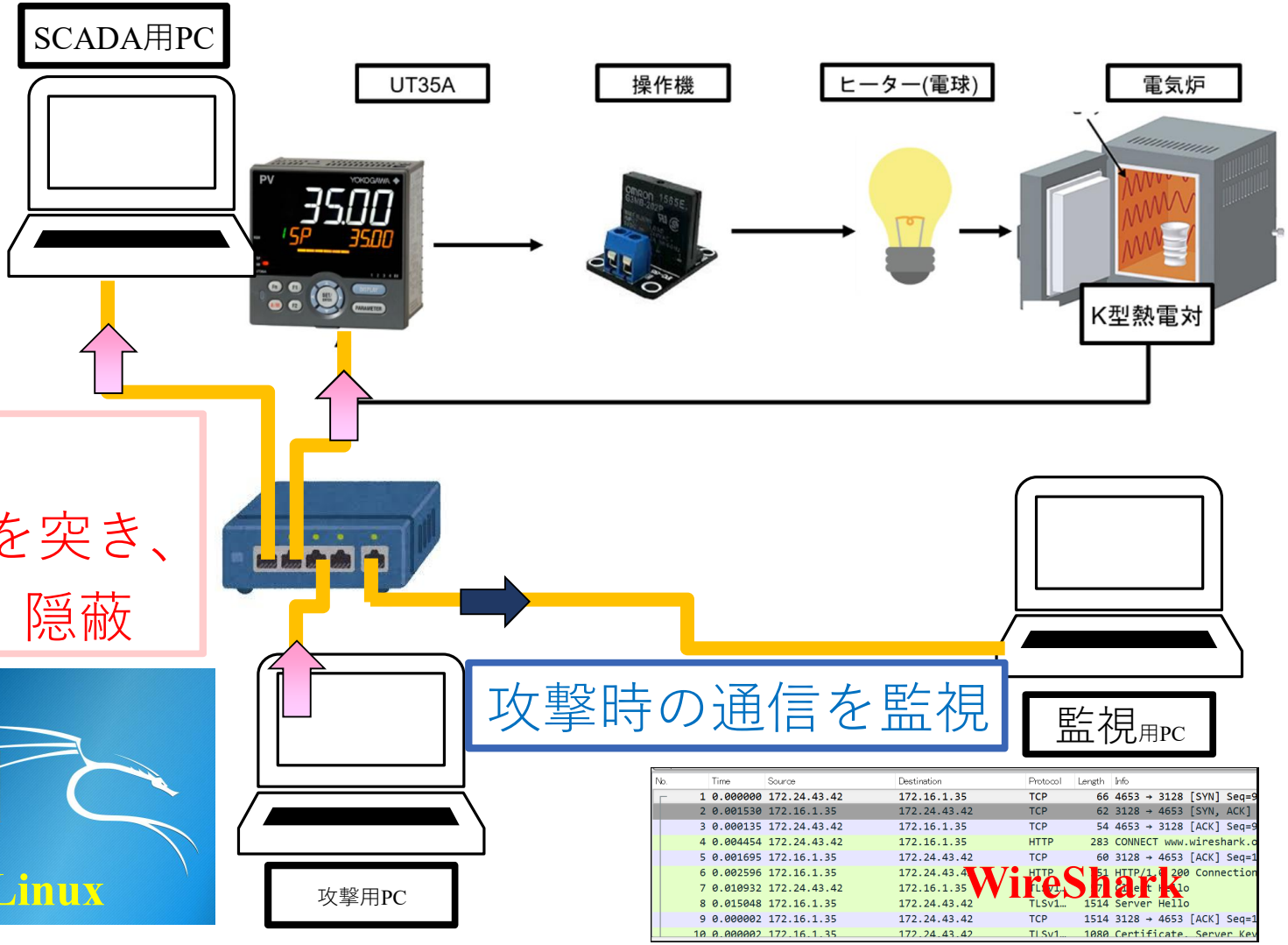


制御ネットワークに侵入できれば SCADA, Local Controllerを 操作するだけでなく、 気づけない攻撃が実現できること および通信監視で攻撃が見えるこ とを理解する



温度制御系へのサイバー攻撃





- DoS攻撃
- OSの脆弱性を突き、設定の改竄・隠蔽

PC3台とコントローラ1台とランプ,HUBだけで実施できる。

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。
- 気づくための検知システムの重要性に気づく。
- 自分のプラントを守るための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**

- 簡単な装置で実現できるので、
  各事業所で実現できる。
- **インシデント対応演習とともに、普及させたい。**

制御系セキュリティの国際標準

- 国際標準のIEC62443にも新たな動き

  セキュリティの管理レベルは従来Security Levels SL1~SL4の整理であった。

  どれだけ破られにくいかの評価に基づくが、脆弱性の発生で変化する。

  脆弱性対策など管理体制も重要である。

  Maturity Levels ML1~ML4として管理レベルを設定

  SLとMLの組み合わせで評価する。

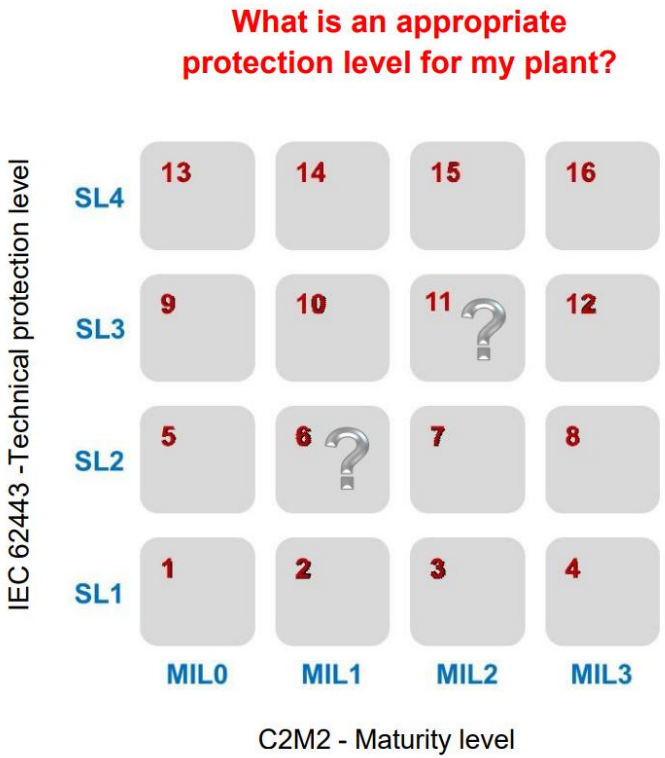
  SLは、Zone & Conduitで評価する

- NISTから重要インフラのセキュリティ対策のフレームワークが提唱されている。

  役員レベル、ビジネス／プロセスレベル、実施／運用レベルで
  アクティビティを整理し、
  対策をIdentify, Protect, Detect, React, Recoveryの観点で整理している。

  従来の情報セキュリティを基にしたConfidentiality, Integrity, Availabilityでの整理より、対策の評価として理解しやすい。

Security Level評価の世界標準 (IEC62443-3-3)



IEC 62443-3-3 – Security Levels

SL 4 – Protects against intentional security incidents using sophisticated means and having extended resources – Nation State
国家規模の大規模で高度な攻撃も防げる

SL 3 – Protects against intentional security incidents using sophisticated means – Hacktivist, Terrorist
高度な攻撃を防げる

SL 2 – Protects against intentional security incidents using simple means – Cyber Crime, Hacker
単純な攻撃は防げる

SL 1 – Protects against casual security incidents – Careless Employee or Contractor
セキュリティを気にしていない

NIST / C2M2 – Maturity Levels (As Examples)

ML 3 – Practices are managed with policies and governance from organization. Policies are reviewed and adjustments made as needed and include compliance with specified standards and/or guidelines.
標準にのっとって管理されている

ML 2 – Risk practices are approved by management and expressed as policy, policies, processes, and procedures are defined, implemented and validated. Adequate resources are provided.
手続が整理されている

ML 1 – Risk practices are performed but may be adhoc, typically by individual thus outcome may vary depending on the individual.
個人依存

ML 0 – Practices are not formalized, often case by case, and risk is managed in an ad hoc and sometimes reactive manner.
場当たり的

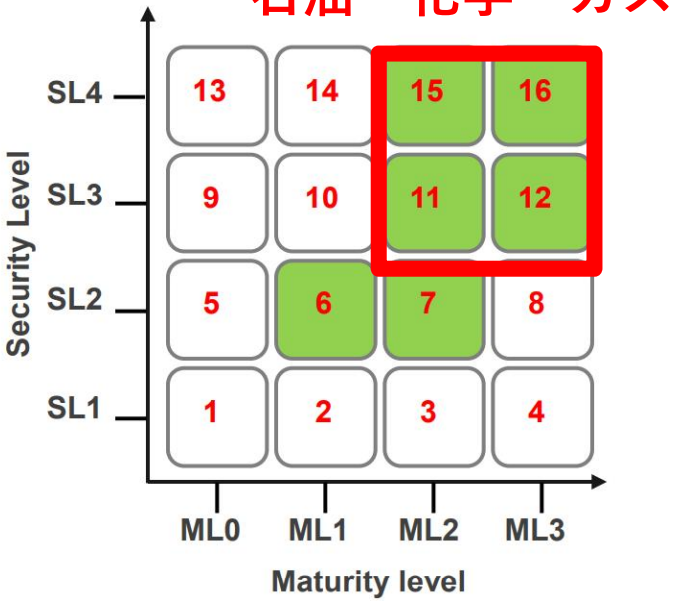
セキュリティの評価は、マネジメントも組で
初めて評価できる。
今日は安全でも明日はだめかもしれないのが脆弱性
脆弱性はハッカーの発明品
維持するマネジメント体制も重要

https://www.honeywellprocess.com/library/news-and-events/presentations/Hon-EMEA15-Spear-Industrial-Cyber-Security101.pdf

業界ごとの目標セキュリティレベル

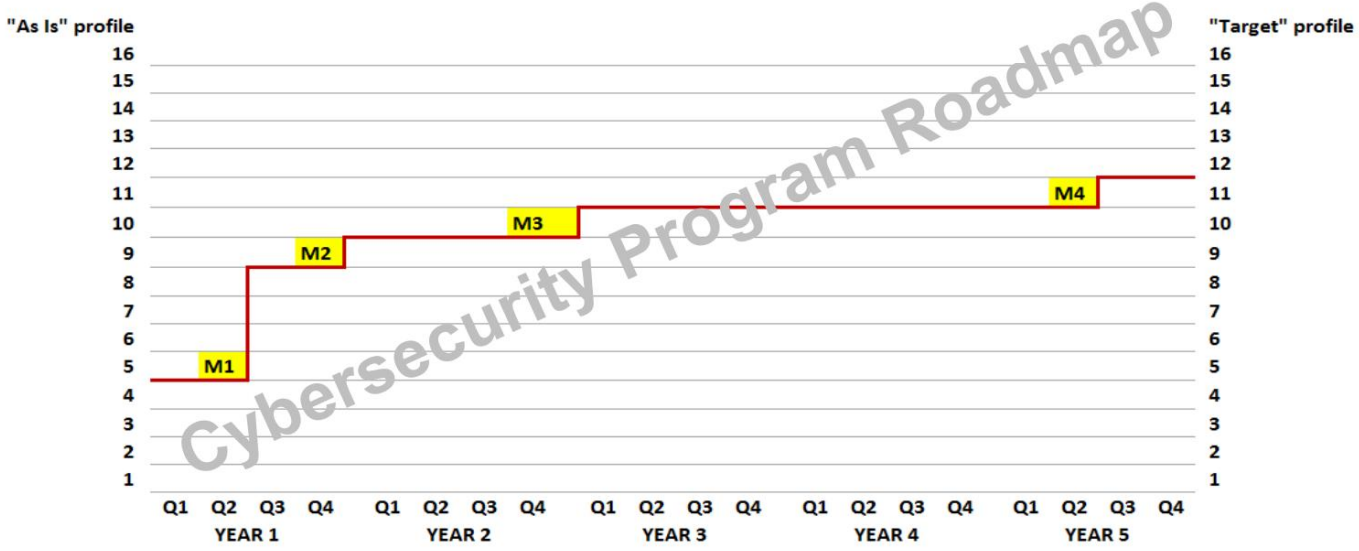
	SL 1	SL 2	SL 3	SL 4	ML 1	ML 2	ML 3	ML 4	T
1001 – Refining Process Facilities			■				■		11
1102 – O&G LNG terminals			■	■			■	■	16
1103 – O&G Processing			■				■		12
1104 – O&G Production – On-shore			■				■		11
1105 – O&G Production – Off-shore			■				■		11
1108 – O&G Marine – LNG IAS			■	■			■	■	12
1110 – Gas To Liquid			■	■			■	■	12
1112 – Production – Coal Bed M		■	■				■		11
1114 – Pipeline – Liquid			■				■		11
1115 – Pipeline – Gas			■				■		11
1201 – Pulp		■				■			6
1203 – Paper		■				■			6
1203 – CWS		■				■			6
1303 – Utility Power			■	■			■	■	16
1401 – Fertilizers		■	■				■		7
1403 – Petrochemicals			■				■		7
1404 – Plastics and Fibers		■	■				■		6
1405 – Specialty Chemicals		■	■				■		7
1406 – Biofuels			■	■			■	■	12
1501 – Alumina		■				■			7
1502 – Aluminium		■				■			7
1503 – Base materials		■	■				■		11
1504 – Cement		■				■			6
1505 – Coal & Coal Gasification		■	■			■	■		7
1506 – Iron			■			■	■		11
1509 – Precious Metals		■	■			■	■		11
1510 – Steel making			■			■	■		11
1508 – Other		■				■			6

石油・化学・ガス



https://www.honeywellprocess.com/library/news-and-events/presentations/Hon-EMEA15-Spear-Industrial-Cyber-Security101.pdf

セキュリティ向上計画

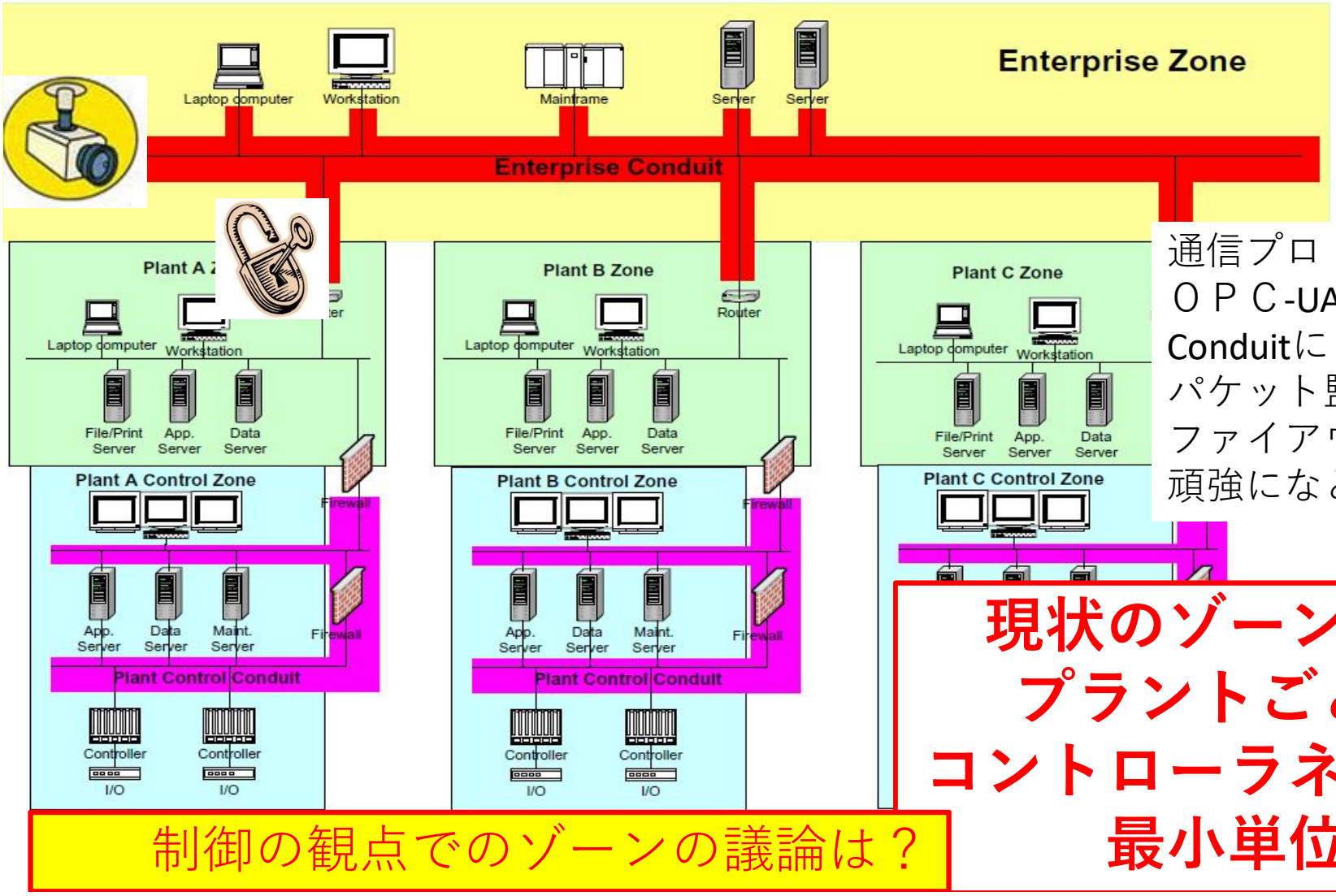


https://www.honeywellprocess.com/library/news-and-events/presentations/Hon-EMEA15-Spear-Industrial-Cyber-Security101.pdf

ISO-62443-3 Security for industrial process measurement and control

Zone & Conduit で、セキュリティ対策の設計・評価

「部屋の鍵」と「廊下の監視の頑強さ」で、やられにくさを調整

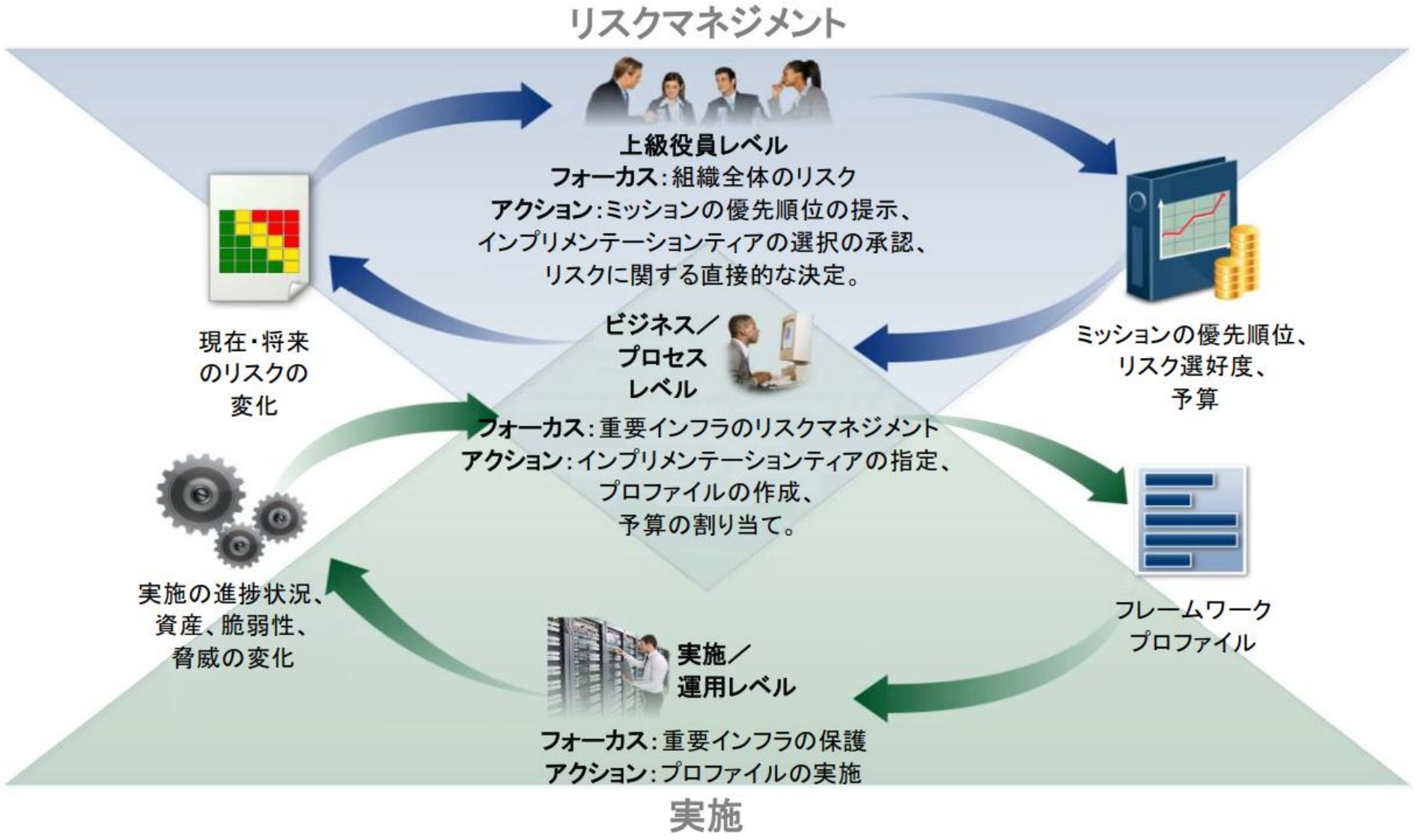


通信プロトコルに
ＯＰＣ-UAを利用し、
Conduitに
パケット監視、
ファイアウォールを
頑強になどの対策

**現状のゾーンは、
プラントごとの
コントローラネットが
最小単位**

制御の観点でのゾーンの議論は？

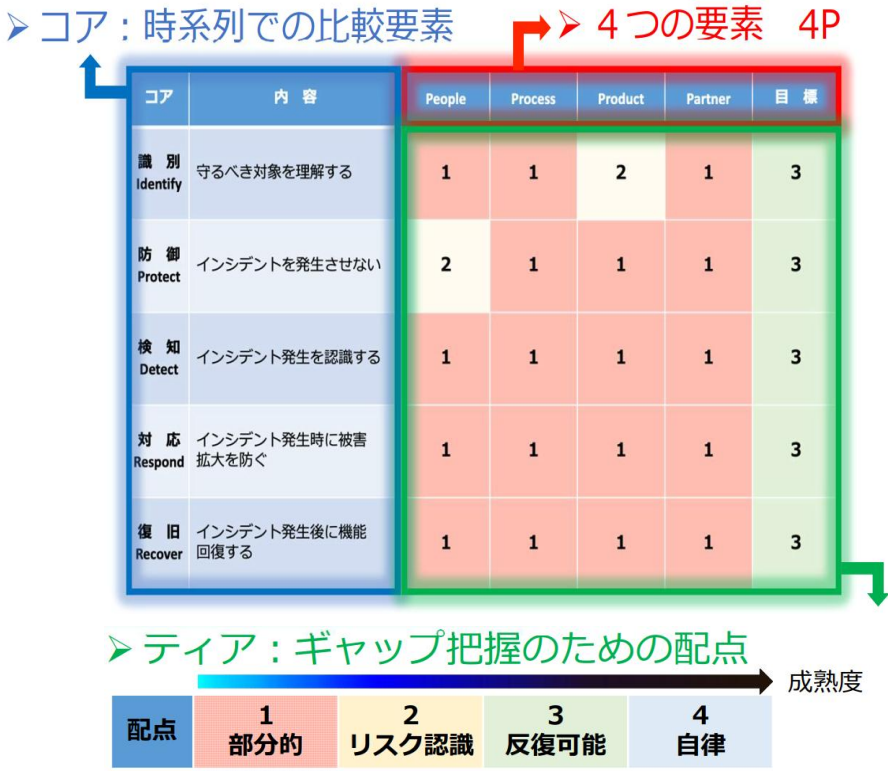
Framework for Improving Critical Infrastructure Cybersecurity
National Institute of Standards and Technology



https://www.ipa.go.jp/files/000071204.pdf

Framework for Improving Critical Infrastructure Cybersecurity
National Institute of Standards and Technology

機能の識別子	機能	カテゴリーの識別子	カテゴリー
ID	識別	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスクマネジメント戦略
		ID.SC	サプライチェーンリスクマネジメント
PR	防御	PR.AC	アイデンティティ管理とアクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術
DE	検知	DE.AE	異常とイベント
		DE.CM	セキュリティの継続的なモニタリング
		DE.DP	検知プロセス
RS	対応	RS.RP	対応計画の作成
		RS.CO	コミュニケーション
		RS.AN	分析
		RS.MI	低減
		RS.IM	改善
RC	復旧	RC.RP	復旧計画の作成
		RC.IM	改善
		RC.CO	コミュニケーション



セキュリティレベル向上のためのアプローチをフレームワークに基づいて多面的に計画

https://www.ipa.go.jp/files/000071204.pdf

Security Design Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Technical controls (Vulnerability scanning, Monitoring …)	Technical controls (Firewall, AWL, AV, IPS, DC, network segmentation, ….)	Technical controls (IPS, IDS, SIEM, Security Dashboard …)	Technical controls (IPS, Recovery CD, …)	Technical controls (Back-up Control Center, …)
Non-technical controls (Assessments, Risk management)	Non-technical controls (Security Policies & Procedures)	Non-technical controls (Security monitoring)	Non-technical controls (Security incident response, Disconnection management)	Non-technical controls (Data recovery, Disaster recovery)

設計目標

TIME TO BREACH THE PROTECTION > **TIME TO DETECT THE EVENT** + **TIME TO RESPOND TO THE EVENT**

防御を突破するのにかかる時間　検知にかかる時間　対応にかかる時間

https://www.honeywellprocess.com/library/news-and-events/presentations/Hon-EMEA15-Spear-Industrial-Cyber-

プラントオペレーションの
これまでとこれから？
まとめ

- プラント計装には、改善ではなく変革があるかもしれない
  （DCSからOPAS, 現場へのスマート機器の導入など）
- 操業現場の安全、安定操業に対するリスクの検討対象を拡大し、サイバー攻撃など悪意も考慮すべき
- ますます、人間が対象とすべき範囲は拡大し、要求される知識も広がる
- AIによる支援は考えられるであろうが、いざとなったら、頼りになるのは人間であるはず
- 手動操作で安全確保できるならあまりおそれなくてもいい
- レジリエンスを組織として高めるには、リスクに対する意識の高い専門家集団の連携が重要
- 連携の必要性を感じるシナリオによる演習の繰返しが必要
  みんなで、よいシナリオをつくって共有しよう。