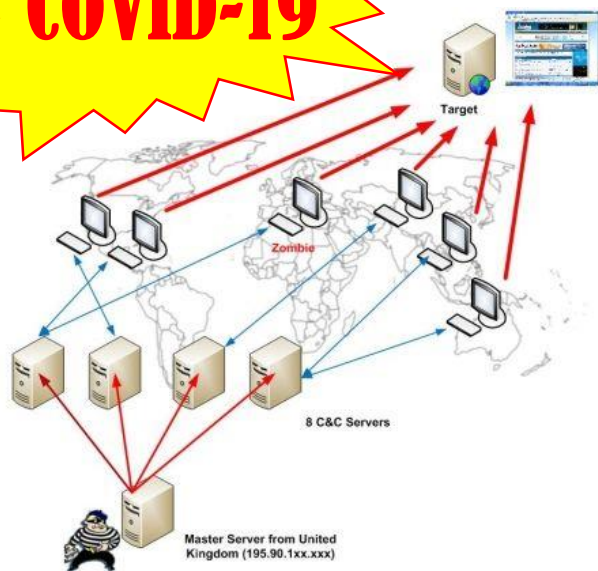


# セキュリティからみた制御の将来

橋本芳宏 (名古屋工業大学)

**COVID-19**



第69回VEC協賛セミナー 2020年9月18日(金)オンライン

# 2020年の重大トピック **COVID-19**

- 世界中でLock down
- 感染防止で移動できない
- 在宅勤務
  - 航空会社、観光業、飲食店の倒産
  - 都心のオフィス解約
  - デリバリー産業の繁盛

## ポスト・コロナ、ウィズ・コロナの社会変革

- ICS(Industrial Control Systems)の現場では？

# コロナ禍でのICSの現場は？

- 24時間操業を支える運転員の感染防止  
外部の人間との接触を回避
  - 直の引継ぎも、テレビ会議システム
  - トラブルや工事の対応は、
    - 部品が送られてきて、現場作業員がリモートからの支援で補修作業
    - 外部業者が作業するが、現場での監督や立会検査はリモートか時間差
    - 無症状者からの感染を回避するため、立入作業者の入構前1週間の生活も管理して、共同作業

リモート化の進展

# 急速なリモートワークの進展による セキュリティ問題(1)

- COVID-19問題のフィッシングサイトやマルウェアが多発

2020年第1四半期（1～3月）の脅威動向



**1月** Ursnif (ファイル名にCoronavirusを含む)

**2月** Fareit (COVID-19やCoronavirusという用語をメールへ含める)

**3月** • Emotet (検査結果や治療法に関して言及)

• Trickbot (検査組織を装う)

• COVIDをテーマにしたランサムウェア

**4月** • Azorult (偽のウイルス感染マップを悪用)

• Hancitor (保険会社を装う)

• Nanocore (予防策について言及)

• NetWalkerランサムウェア (後述)

**COVID-19を悪用するマルウェアファミリーの蔓延**  
フィッシング攻撃、偽のWebサイト、マルウェアなどが急増

[https://japan.zdnet.com/image/l/storage/35158088/storage/2020/08/13/403bad5577b9f14e45cdd4566c490257/200812\\_mcafee\\_002.jpg](https://japan.zdnet.com/image/l/storage/35158088/storage/2020/08/13/403bad5577b9f14e45cdd4566c490257/200812_mcafee_002.jpg)

# 急速なリモートワークの進展による セキュリティ問題(2)

- VPNのアクセス処理能力限界と管理不備による情報漏洩

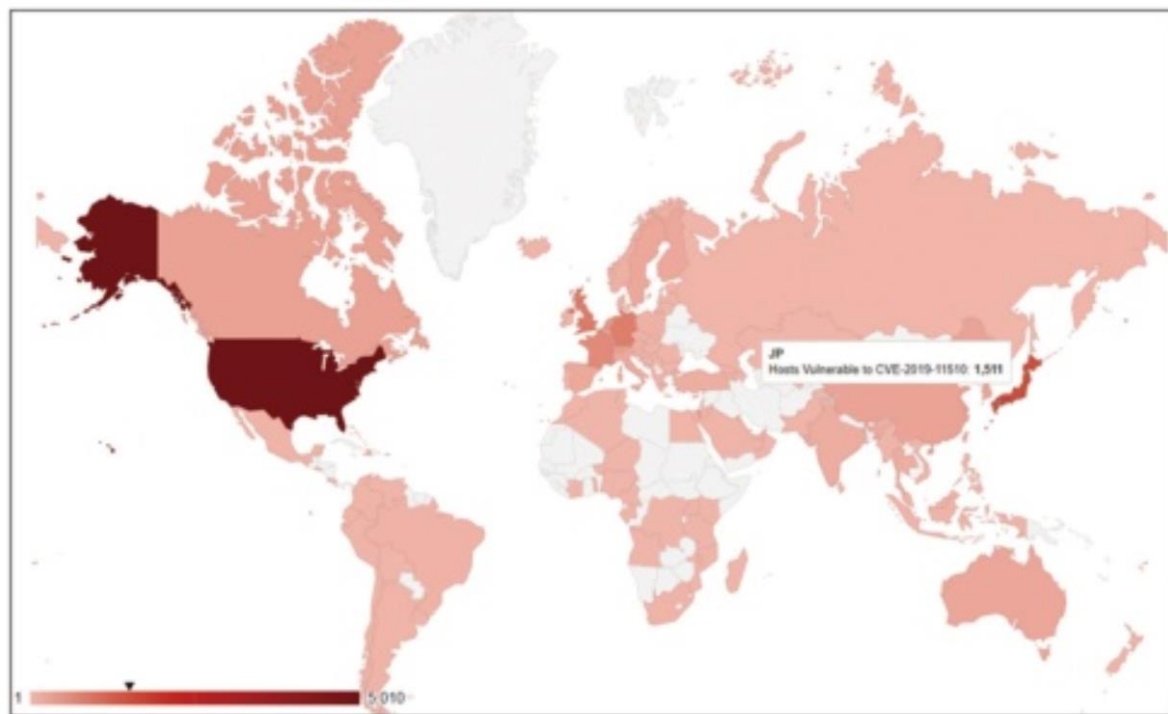


図2●脆弱性があるパルスセキュア製品を動かしているサーバーの利用状況

2019年8月25日時点のデータ。色が濃い地域ほど脆弱なVPNサーバーの数が多い。最も色が濃い米国には5010台の脆弱なサーバーがあった。日本には1511台が存在していた。（出所：米バッドパケッツ）

<https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/041800012/052000103/>

# 深層防護とTrusted Networks



正門  
警備

外界

人物  
認証

玄関鍵

監視  
カメラ

構内  
パトロール

部屋  
扉鍵

金庫

窓鍵

VPNの認証情報漏洩は  
正門の入門許可の問題

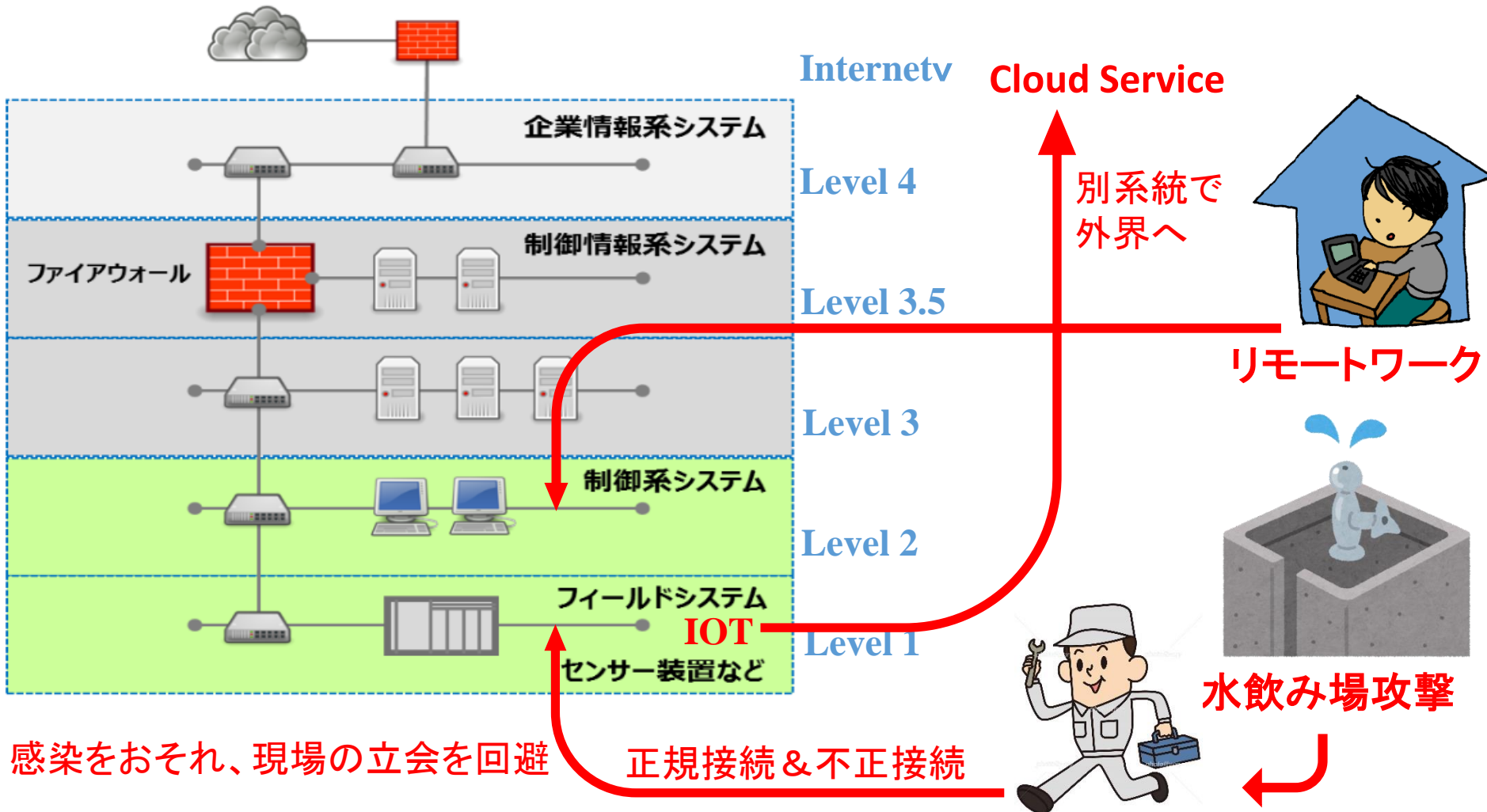
即、プラント事故発生  
というわけではない

ただ、従来は、  
金庫の前でしか  
仕事ができなかった  
のに、むりやり  
在宅勤務になった  
面がある

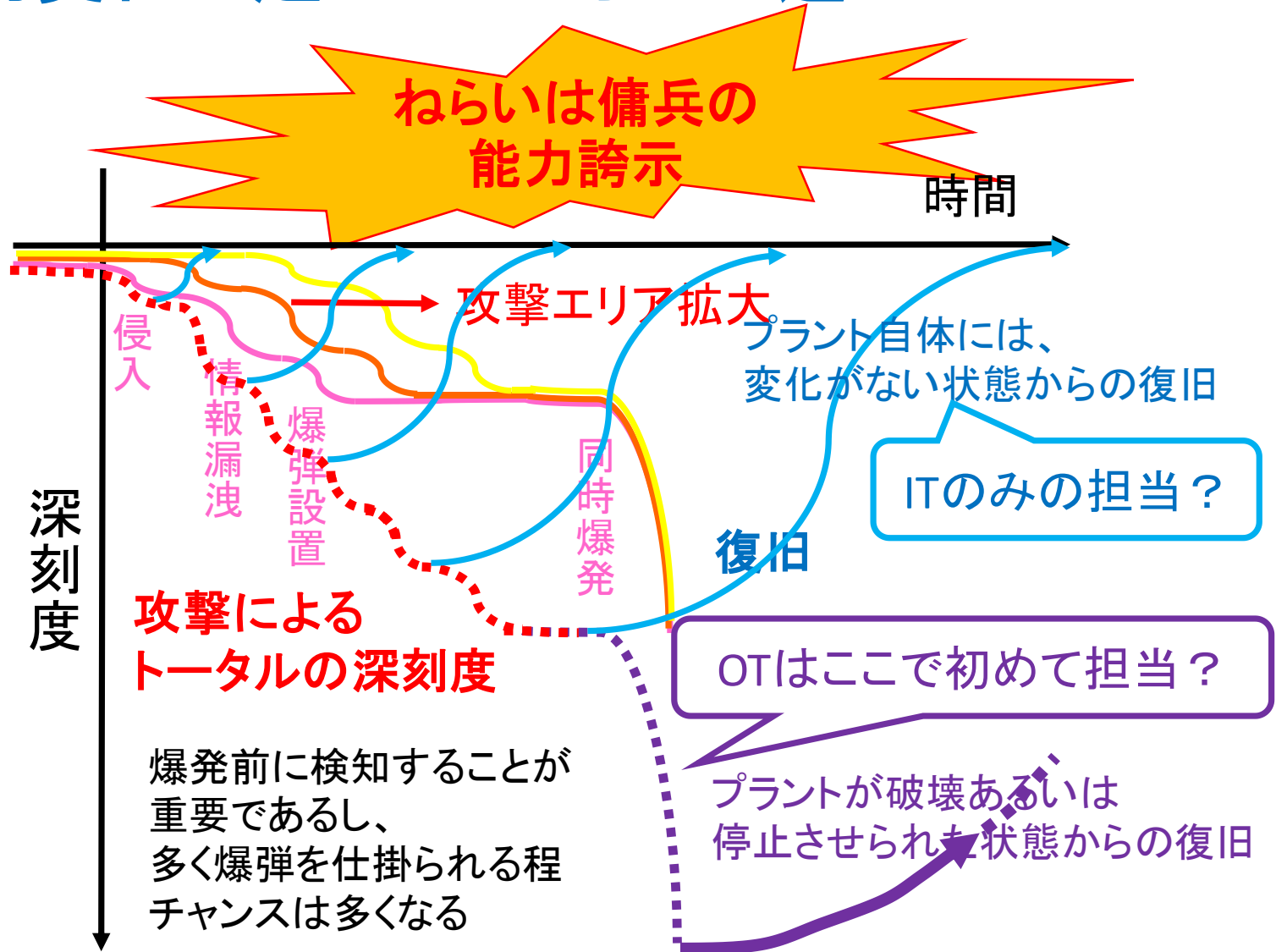
こんな  
ショートカット  
ないよね



# 外部からは階層だけど、 外からだけの想定では不足



# 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



# ゼロトラスト ネットワーク

「必要な人に必要なだけのアクセス」を原則に、  
認証、権限、脆弱性、検疫、脅威検知などの点で、  
決して信頼せず（ゼロトラスト）、  
すべてのデバイスのトラフィックの検査とログの取得を行う

急激な在宅勤務の進行で、すべての事業所で、VPNによる  
trusted networkを確保することの難しさが意識され、  
ゼロトラストでの管理に注目が集まっている。

ユーザーが、どこにいてもという「モバイルアクセス」  
高度な管理を広く適用するための「クラウド移行」  
被害拡大を防止する「独立性確保」という点は、  
ICSセキュリティにも有効なはず

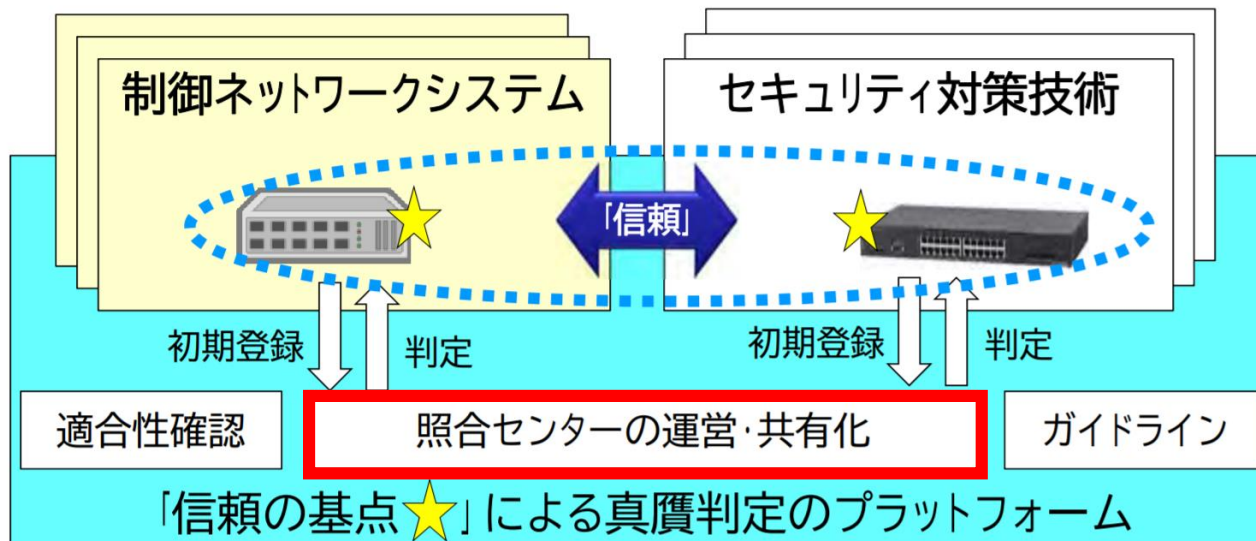
# 信頼性の確保はブロックチェーンでは？

## 第1期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』

### 真贋判定技術のプラットフォーム化

「信頼の基点」による真贋判定技術をプラットフォーム化し、国内外の優れたセキュリティ技術の受け皿に (TOPの実践)

⇒国内外の関連技術との連携インターフェースに向けた国際活動



中央集権的な  
こんな管理が、  
自由主義社会で  
成立するとは  
思えない!!

分散により、  
改竄しきれない  
ブロックチェーン  
の発想を  
導入したい

# ブロックチェーン

- ・ブロックチェーンは、ブロックと呼ばれる暗号化されたレコードが増加するリストを、ネットワーク上に分散したノードで共有し、コンセンサスをとることによって正しい情報を得る

## 【特徴】

- ・改ざんが非常に困難
- ・システムダウンが起きない
- ・取引の記録を消すことができない
- ・自律分散システム

## 【課題】

ビットコインではコンセンサスをとる計算に、全世界の消費電力の0.1%の電力を利用しているといわれている。

制御ネットワークに導入するには、分散ノードの設置とコンセンサスアルゴリズムの開発が必要

# ゼロトラストとブロックチェーンのアイデアを制御ネットワークに導入するには？

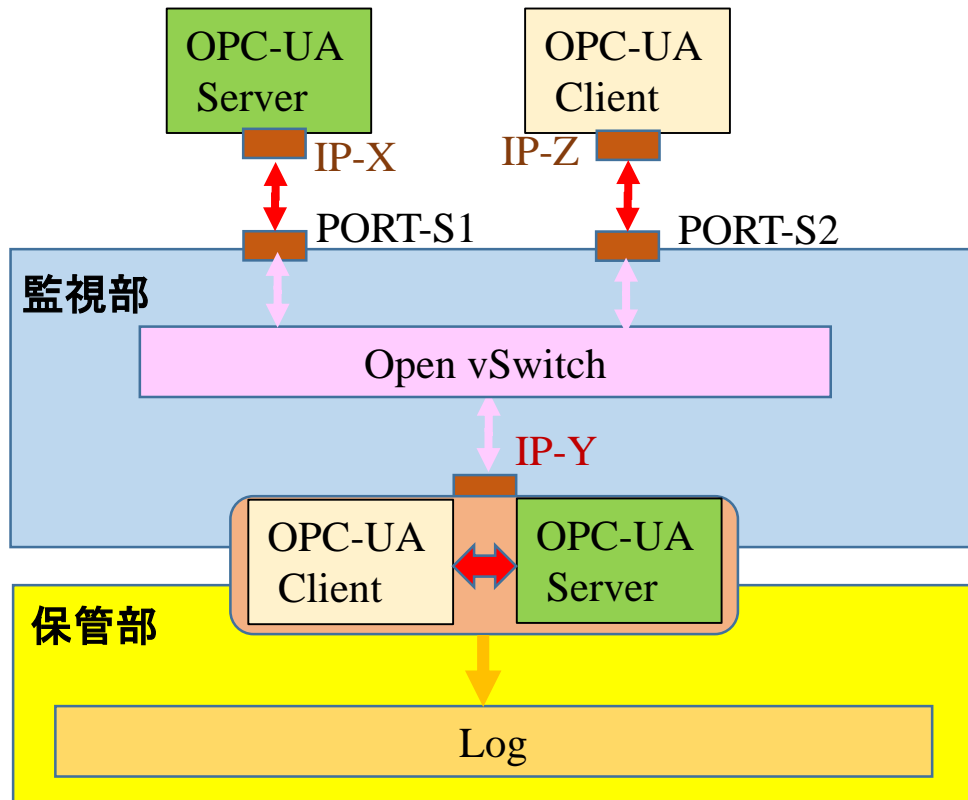
- 制御系ネットワークでのセキュアな通信を実現するには OPC-UA
- OPC-UAはセキュリティを考慮して設計された通信プロトコルで、Industrie4.0でも標準プロトコルとされている。
- OPC-UAは、秘密鍵・公開鍵による認証と、共通鍵による暗号データ通信、多ベンダーの相互接続を実現する標準、情報モデルによる構造体通信、アラームやヒストリアンなどプロセス制御に必要な機能のサポート

# OPC-UAでの暗号通信の監視は？

- コントローラの通信で怖いのは、正規のデバイスから危険な指示が出されること。
- 保守PCやSCADAのマルウェア感染や侵入による危険な指示があれば、コントローラは、内容の判断はなく、指示を受け入れるのが基本仕様
- 指示の変化の大きさや速度に制限を設定することは可能だが、スタートアップやシャットダウンも正常な操業範囲なので、操作量は、全閉から全開までを可動域としなければならない。
- 暗号化してしまうと、通信で監視できるのは、IPアドレスなどのヘッダ情報だけ。
- 情報系では、監視対象は通信から振舞いに移っているが、コントローラへの指示に関しては、そのデータ部分も監視対象としたい。

# OPC-UAの通信監視

- 2つのOPC-UA通信をする機器の間に、監視用HUBを接続
- HUB内には、OPEN FlowスイッチとOPC-UAのブローカーが存在
- IP-XとIP-Zは、Publisher, Subscriberに相当するが、ブローカーをOpenFlowで隠密化する。
- ネットワークとしては、Peer 2 Peerの暗号通信が存在する形式とする



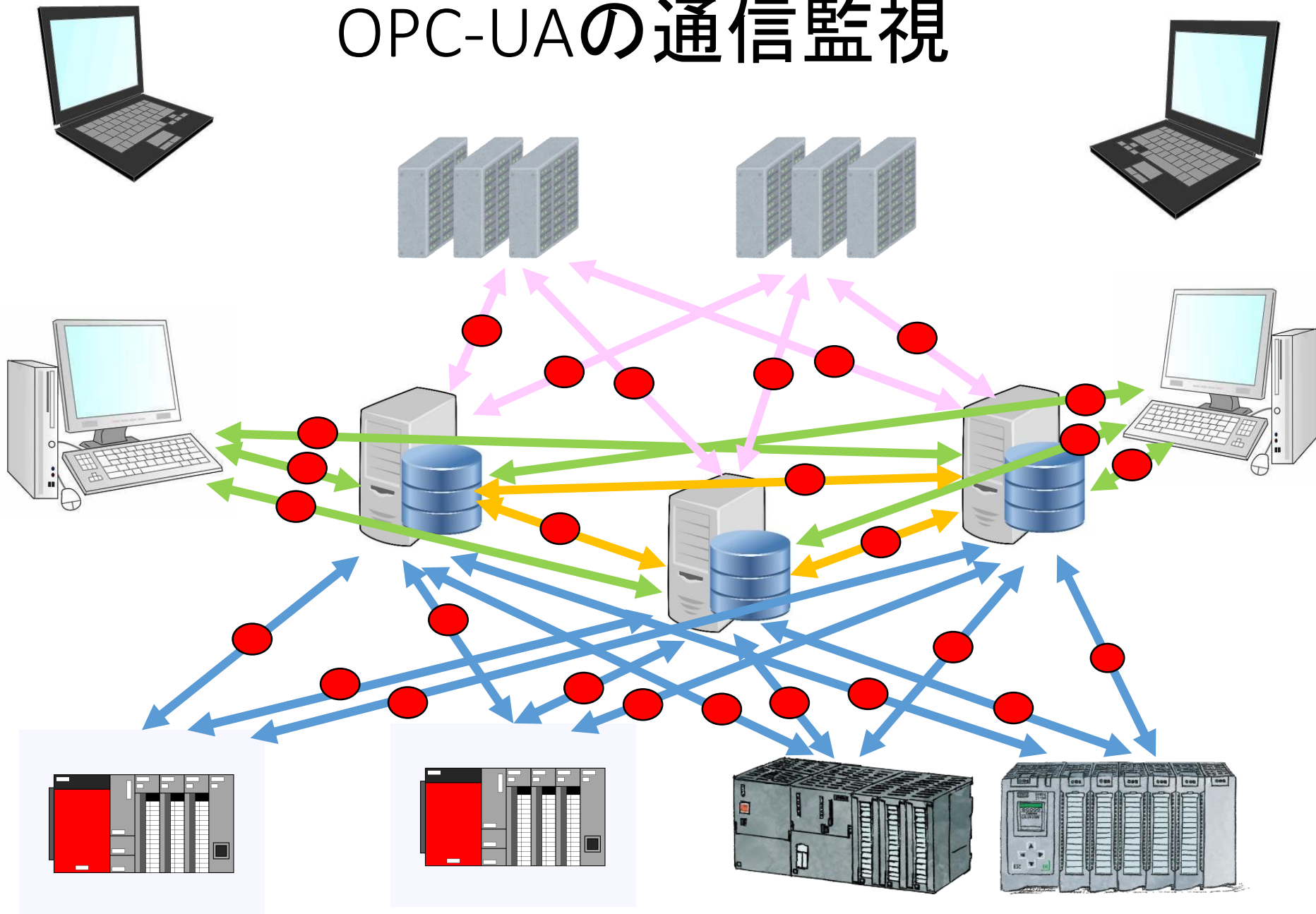
- ブローカーの情報を安全に、別のネットワークに保存する

監視機能付きHUB

HUBに接続するときには、OPC-UA通信の登録が必要

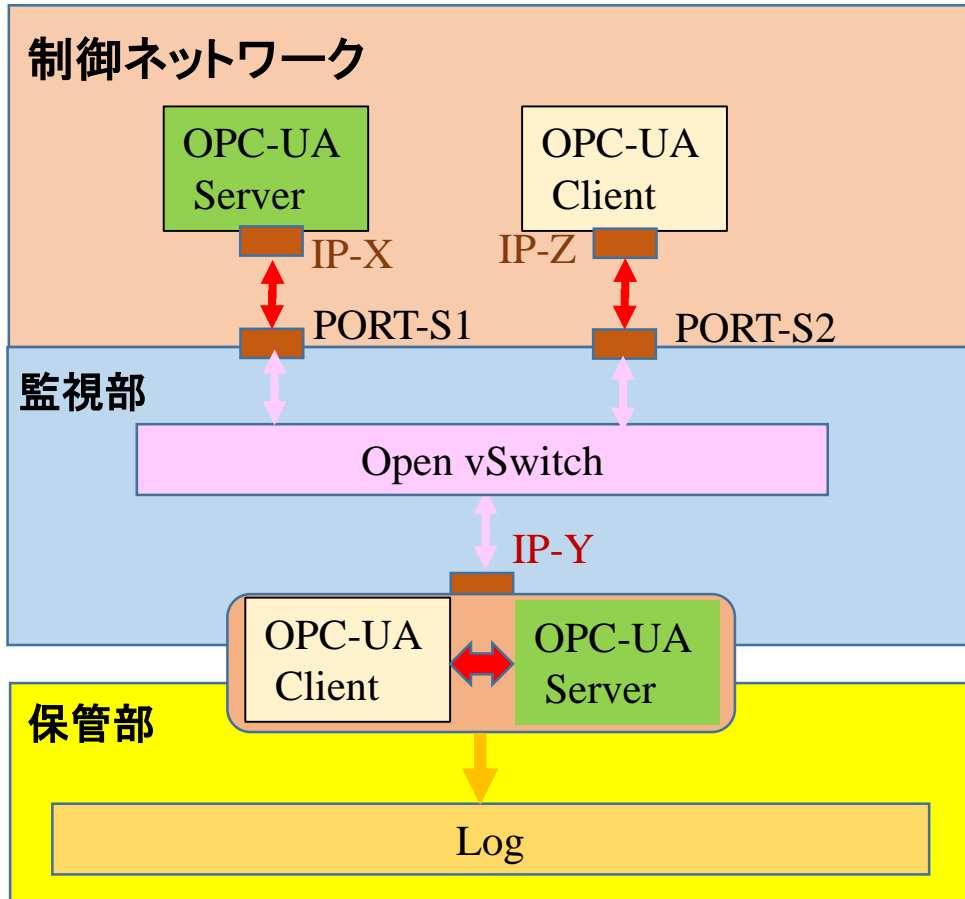
HUBのポートにはIPアドレスはない

# OPC-UAの通信監視



監視点 ● でブロックチェーンの構築が可能かも

# OPC-UAの通信監視



制御ネットワークは、Availability  
Realtime性が重要なネットワーク

監視部で、通信の異常を処理し、  
通信データを保管部に送る

保管部で、制御ネットワークと  
独立なネットワークを構成し、  
ブロックチェーンの  
コンセンサス制御  
異常を検知すると、  
制御ネットワークを制御



# セキュリティの設計性能と運用の問題

## 【コントローラが故障したときの保守】

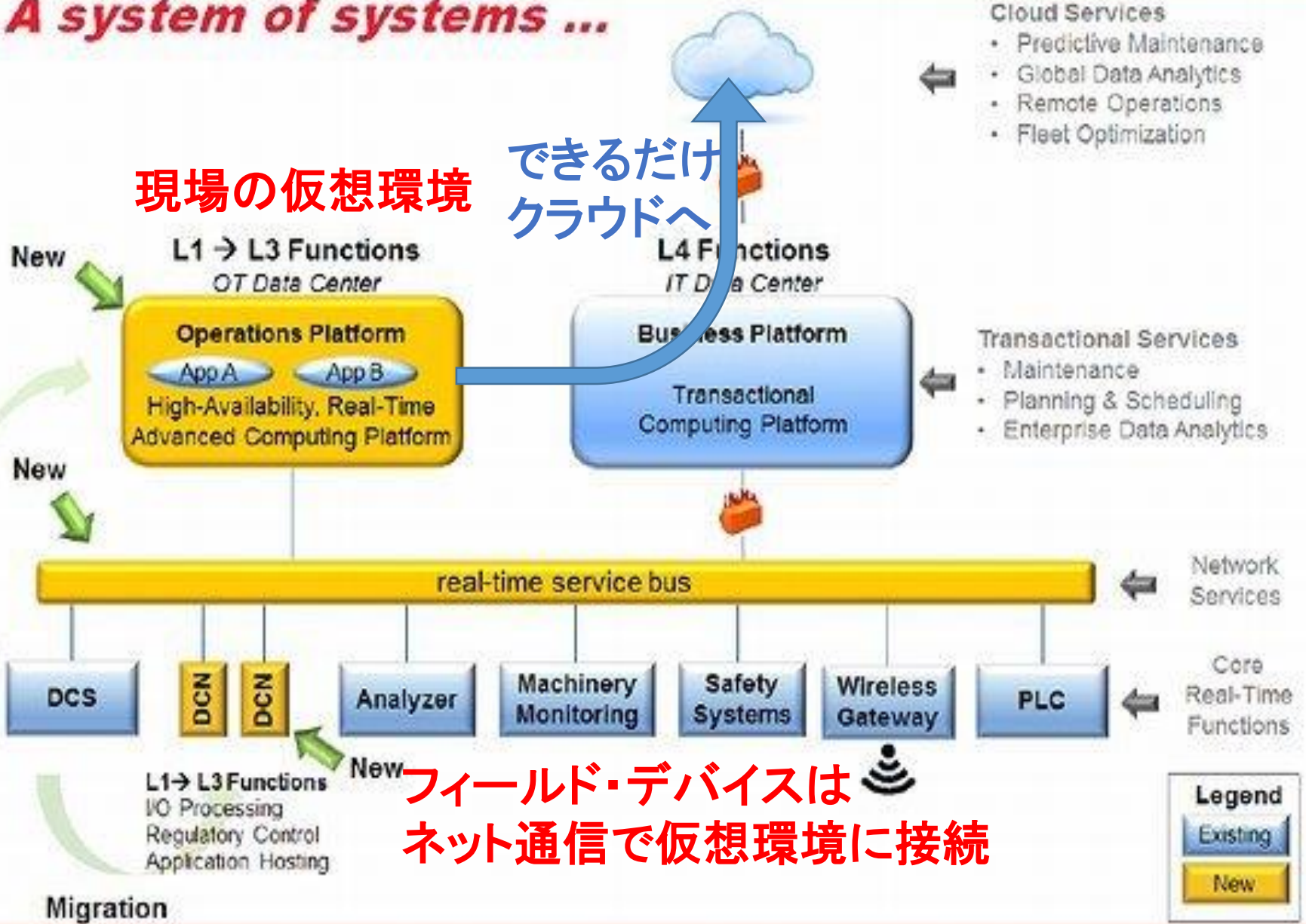
- 別のコントローラに入れ替える。
- コントローラだけでなく、サーバーとクライアントの両方のOPC-UAの設定をやり直す。
- データサーバーの作業も必要なので、現場運転員には難しいかもしれない。
- OPC-UA準拠製品には、秘密鍵をコピーできるものが存在し、コントローラの秘密鍵をコピーすれば、OPC-UAでも、コントローラを差し替えるだけで対応できる。
- セキュリティ上は問題であるが、メンテナンスを重視したこのような運用が、今後も登場すると危惧される。

# サイバーセキュリティ対策はますます高度化

- サイバーセキュリティ専門家の現場ごとの確保は困難
- 通信監視は必要だが、現場作業員の仕事ではない
- 現場でのセキュリティ対策をリモート化、自動化
- 異常を検知したときに、現場ができるのは、通信が遮断された状態での操業体制を実施すること
- トラブル時の保守も、できるだけリモート化と自動化で対応。OPC-UAの設定に現場作業が必要だとしても、簡素に
- 現場での脆弱性発生の可能性を下げるためには、現場でのプログラムはできるだけシンプルに
- リアルタイム性の低いものは、できるだけクラウドに移行

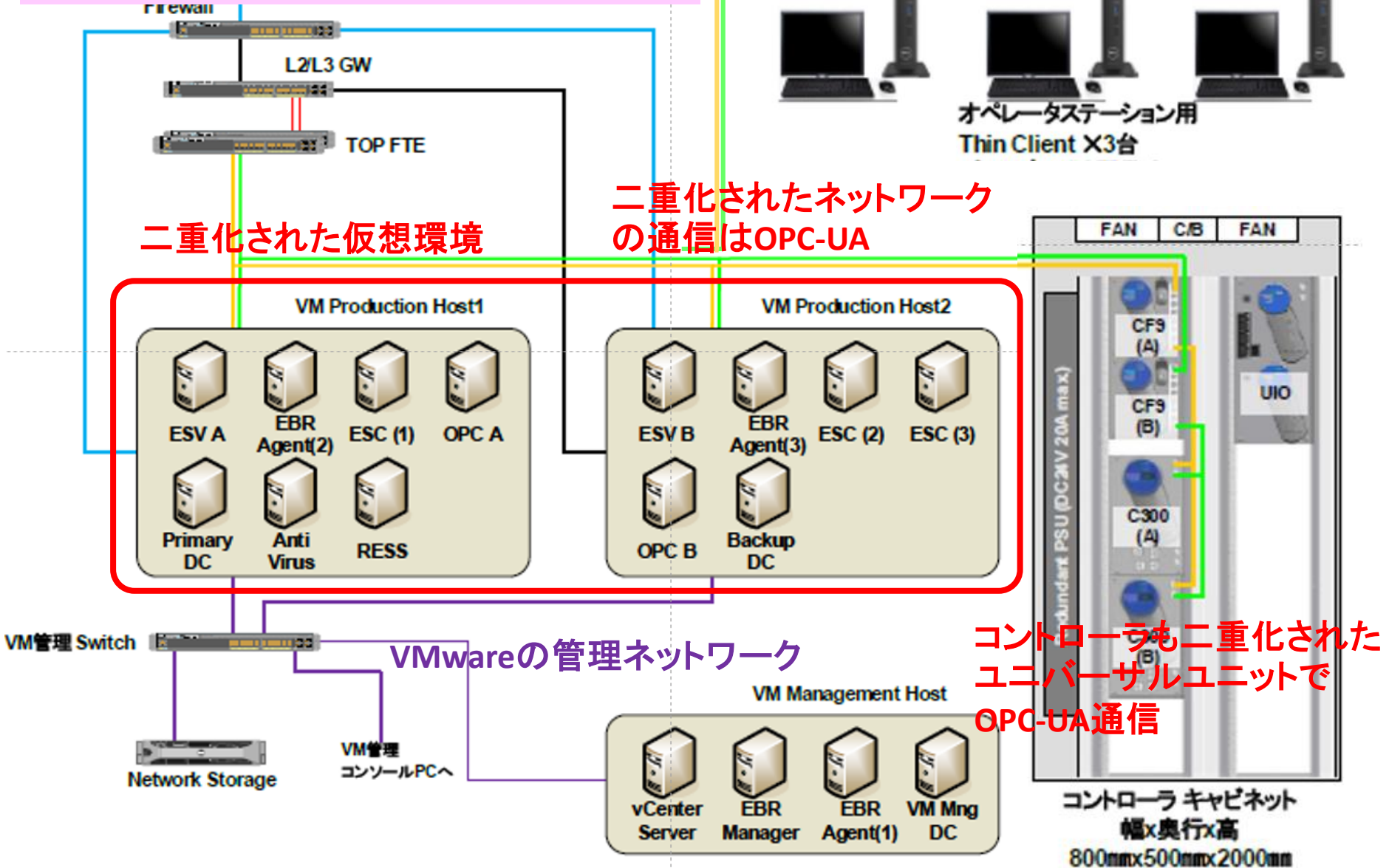
# Open Process Automation System (by Exxon)

*A system of systems ...*

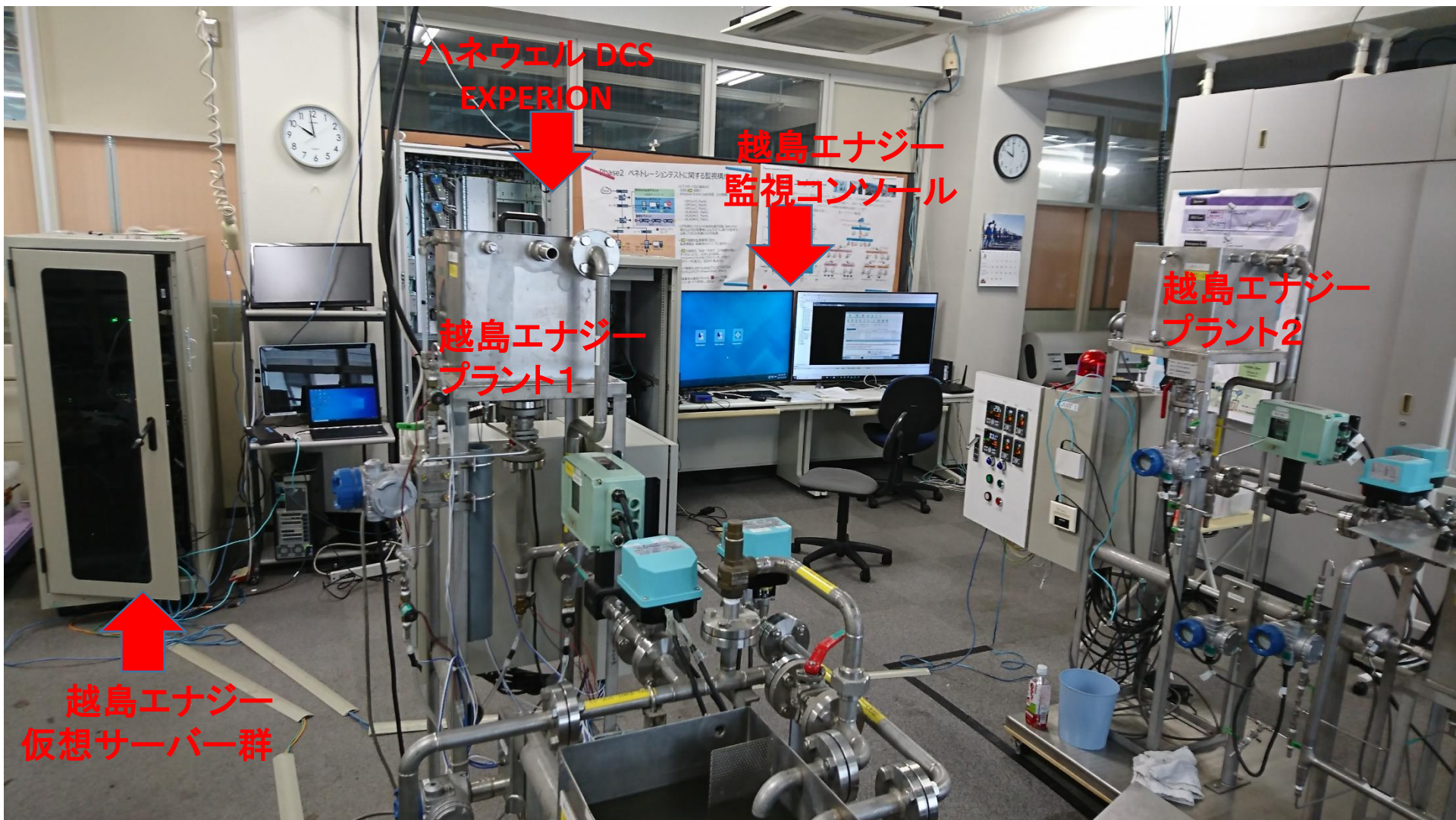



# Honeywell Experion PKS C300

ハネウェルは、世界3か所の監視センターで  
24時間リモートサービスを実施



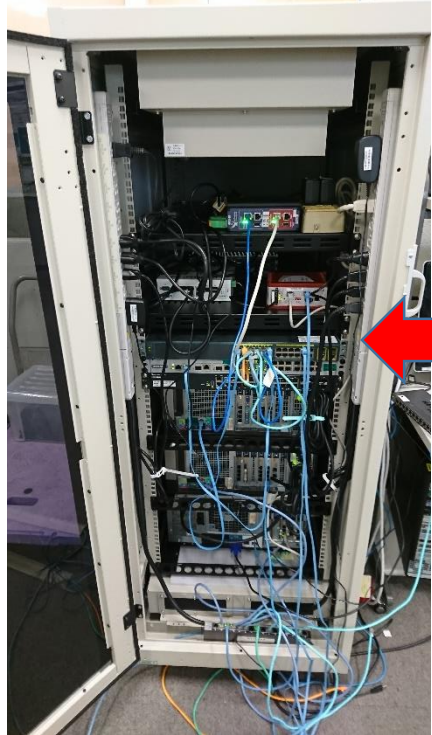
# 「つるまいプロジェクト」は、新たなPhaseへ





DCS EXPERIONの  
仮想サーバー2台  
と管理用WS  
スイッチ類


DCS EXPERION以外に  
複数のOPC-UAのPLCと  
センサー・アクチュエータ単位で  
切り替え可能  
MELSEC, SIEMENS, OMRONなど



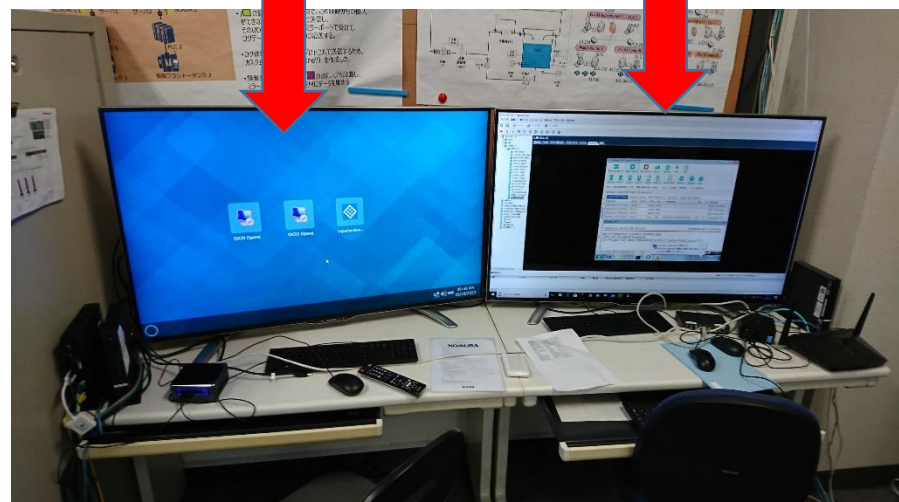
越島エナジー  
ネットワーク用  
仮想環境サーバーと  
IDS,IPS、  
ファイアーウォール  
データダイオードなど



EXPERION用  
コンソール



越島エナジー  
仮想環境用  
コンソール



# システムティックなセキュリティ対策提案

- IEC62443, NIST CyberSecurity Frameworkに準拠したアプローチを越島エナジーで例示

サイバー攻撃の危険性など  
もう聞きたくもない。  
どのように対策すべきかを  
ちゃんと提案したまえ。

多額の投資が必要といえ、  
きっとリスクは他にもあるといわれる。  
でも、中途半端では意味がない。  
どこから、どの程度の対策で  
始めればよいのだろうか？

「いいねえ、それ。  
すぐにでも始めてくれ。」

このシート  
5年前から使ってる

って言いたいけど、  
何を聞けば  
そう言えるんだろう？

って発言、  
どうやったら引き出せ  
るんだろう？



# つるまいプロジェクトへの参加を お待ちしております。

ICS研究所  
MHPSコントロールシステムズ  
NTTコミュニケーションズ  
アズビル/  
アズビルセキュリティフライデー  
アドソル日進  
シュナイダーエレクトリック  
立花エレテック

東陽テクニカ  
トレンドマイクロ  
千代田システムテクノロジーズ  
日本シノプシス  
日本ダイレックス  
日本電気  
マカフィー  
横河電機

**(Phase 1) 2017年4月24日**

**(Phase 2) 2018年1月18日**

