IoTが進まない現状と
セキュリティからみた将来

橋本 芳宏

名古屋工業大学
社会工学科経営システム分野

①ドイツが Industirie 4.0なら
　日本は Society 5.0
② そもそも IoT の革新性は
③ System から SoS へ
　(Systems of Systems)
④ IBM Watson にみる日米の
　情報力の絶望的な格差
⑤ 成功体験に甘んじたボトムアップ
　経営の結果
⑥ サイバーセキュリティからみた
　プラントの将来

化学工学会第83年会 産業セッション　　2018年3月14日関西大学千里山キャンパス

IoTが進まない現状と
セキュリティからみた将来

１．ドイツが Industirie 4.0なら
日本は Society 5.0

２．そもそも IoT の革新性は

３．System から SoS (Systems of Systems)へ

４．IBM Watson にみる日米の情報力の絶望的な格差

５．成功体験に甘んじたボトムアップ経営の結果

６．サイバーセキュリティからみたプラントの将来

IoTを推進する世界の動き

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28日

http://www.meti.go.jp/press/2016/04/20160428011/20160428011.html

① ICSサイバーセキュリティ

・ ベストプラクティスの共有、演習協力

② 国際標準化

・ アーキテクチャモデル（RAMI4.0)

③ 規制改革

④ 中小企業

⑤ 人材育成

⑥ IoT/インダストリー4.0 に関する研究開発

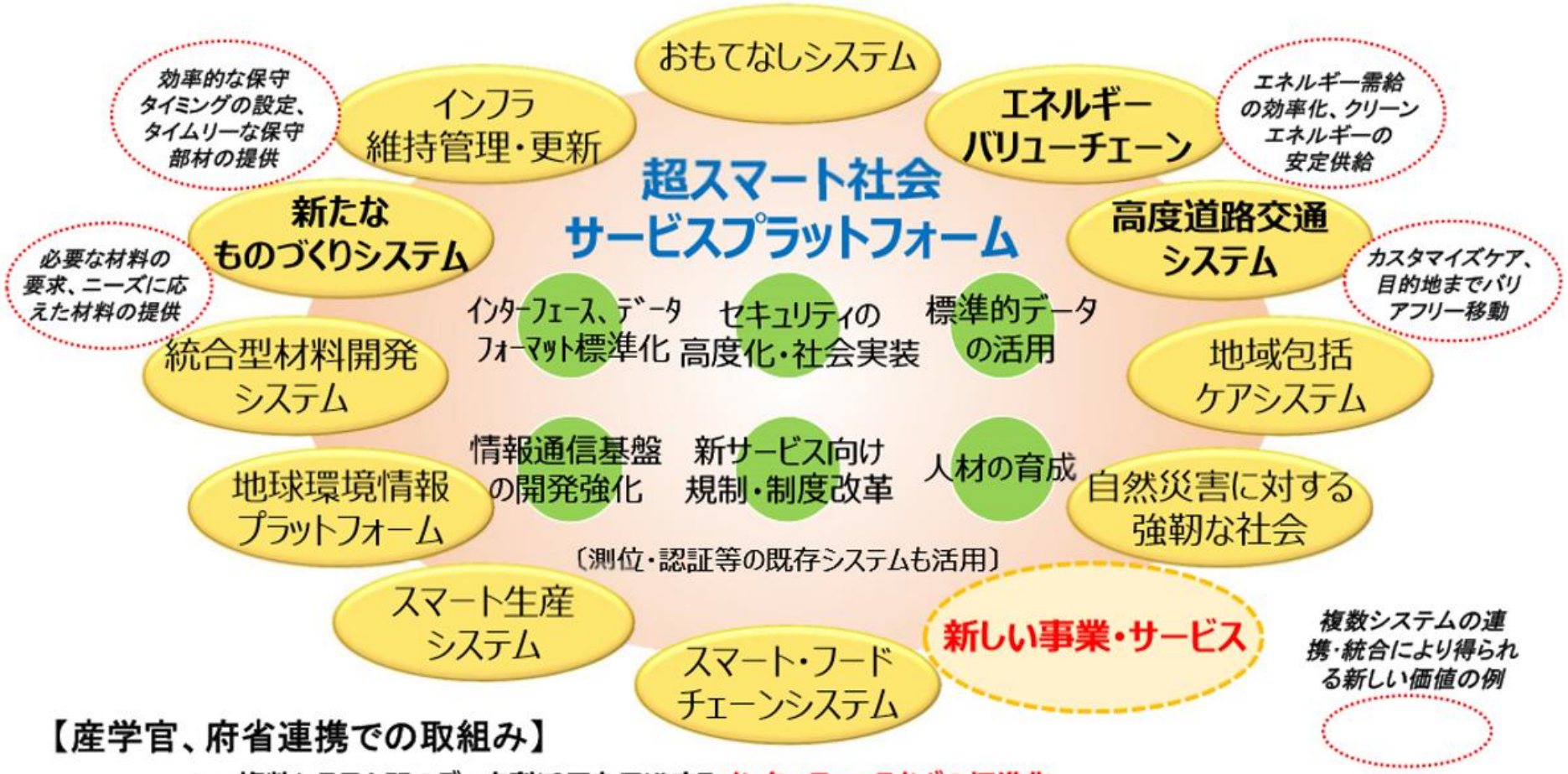
・ 産業技術総合研究所とドイツ人工知 能研究所と研究協力

⑦ プラットフォーム

・ ロボット革命イニシアティブ協議会と
ドイツのプラットフォームインダス トリー4.0

2016年10月3日IoT推進コンソーシアム（ITAC）と
Industrial Internet Consortiumで覚書

Society 5.0　（第５期科学技術基本計画 2016）



【産学官、府省連携での取組み】

- 複数システム間のデータ利活用を促進するインターフェースなどの標準化
- セキュリティ技術の高度化と社会実装、リスクマネジメント機能の構築
- 3次元地図・測位データや気象データのような共通基盤データが活用できる仕組みの整備等
- 社会実装に向けた制度・基準・規制等の改革、文理融合によるELSI（倫理・法律・社会イシュー）強化
- プラットフォーム整備及び活用に係る人材の育成

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

IoTが進まない現状と
セキュリティからみた将来

1．ドイツが Industirie 4.0なら
　日本は Society 5.0

2．そもそも IoT の革新性は

3．System から SoS (Systems of Systems)へ

4．IBM Watson にみる日米の情報力の絶望的な格差

5．成功体験に甘んじたボトムアップ経営の結果

6．サイバーセキュリティからみたプラントの将来

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

マイコン炊飯ジャーはどう変わる？

第3の革新（マイコン)の成果
職人技が、プログラムされて、
炊飯ジャーにのった.

しかし、富士山に行くと･･･

課題:

従来のアプローチ(Kaizen)
→ 圧力センサーを炊飯ジャーに加える.
→ 圧力に合わせた炊き方を実現するため
　CPUやメモリを追加する.

第4の革新（IoT）ではどう変わる？

もし、炊飯ジャーがCloud,と通信 できたら？

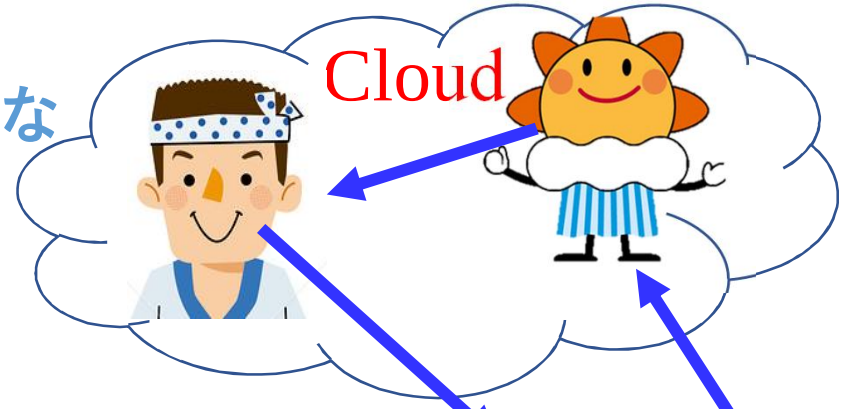
位置を特定できる.

→ 気象庁から圧力情報を獲得できる.

→ 圧力に応じた加熱パターンをCloudで算出する

→ 加熱パターンを通信で受け取り実現

Cloud では、どれだけでも豊富な計算環境を実現できる.



“Thing” が必要なのは、
通信とシンプルな機能.

Thing では、しょぼいCPU
けちくさいMemory

もし、新たな機能を炊飯ジャーに追加したかったら？

従来のアプローチ (Kaizen)

→ 炊飯ジャーに新たなボタンスイッチを追加
→ 新たな機能のプログラムを追加するため
　CPUを更新しMemoryを追加

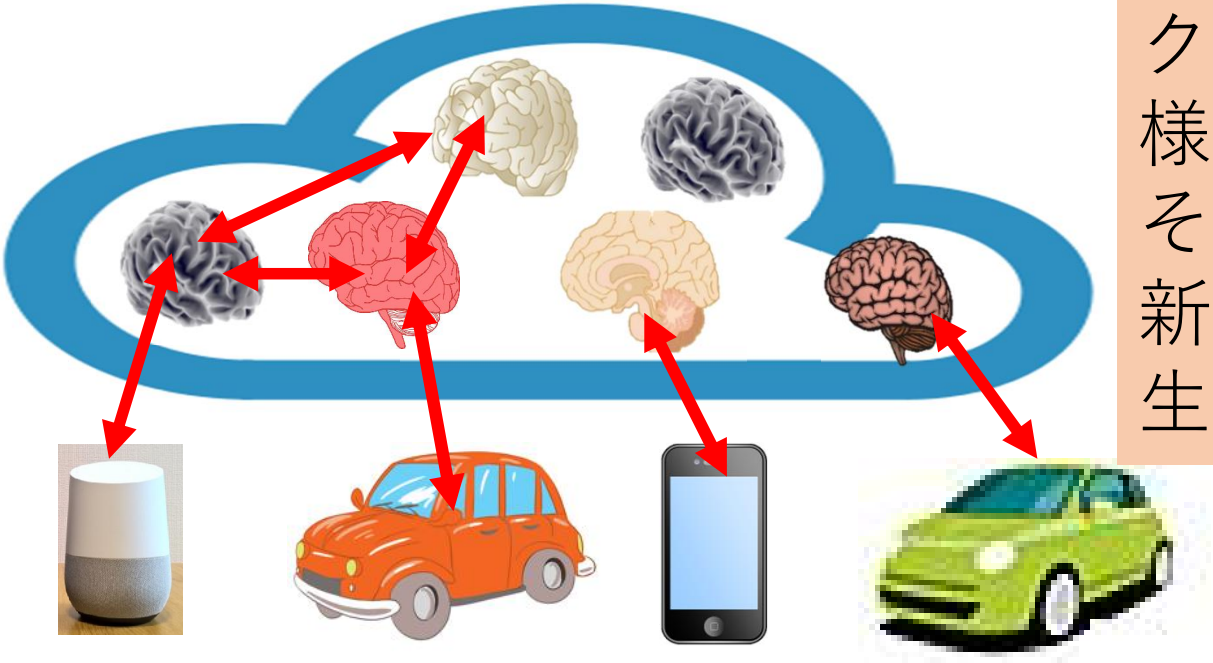
もし、Cloudにつながったら

→ 指示を得るのは
　スマホかAIスピーカーから
→ 新たな機能のための加熱法は
　Cloudで計算し、通信で送る

“Thing” には通信と
シンプルな機能があればいい.

ものの進歩が 物理的拘束から解放される
(CPU, Memory, etc.)

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

Google Mapの渋滞情報

- Google mapのユーザーは今いる場所の地図を得たいし、経路もナビしてほしいからGPS情報をGoogleに送る
- Googleは膨大に集まるGPS情報から車の移動を推算し、地図上に表示

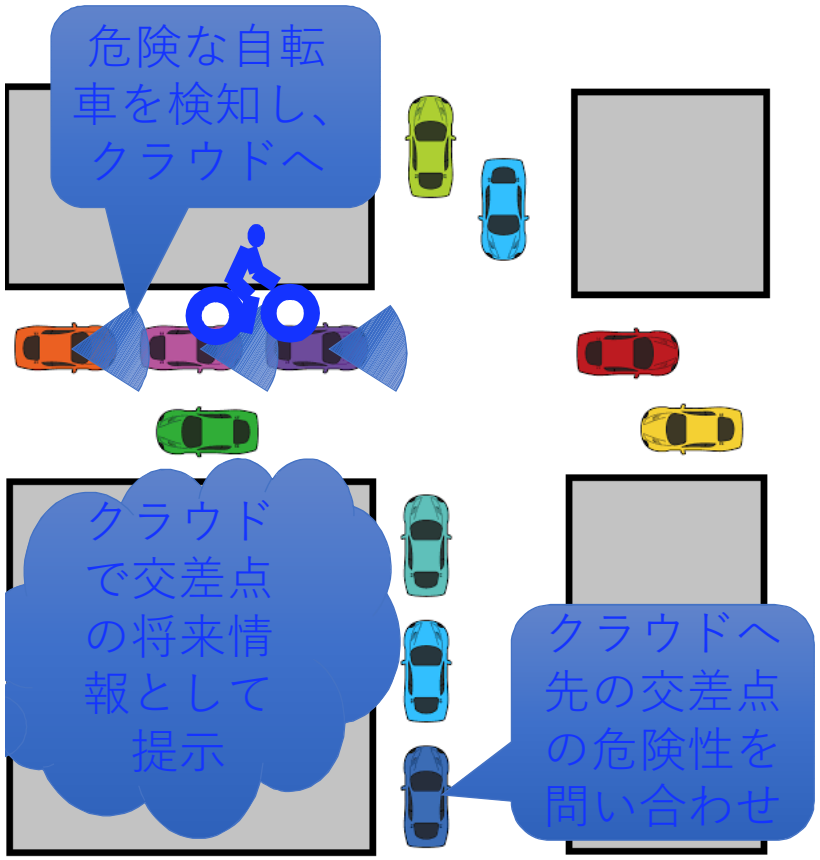
自動運転にはインフラの充実よりもIoT

（課題）ビルの陰からの暴走自転車には？

革新前？

自動車ではなく、自転車がミソ？

→交差点ごとにカメラを設置して、信号機で車に通知？



革新後

→先行車両だけでなく、
別の走行中車両からの情報で、
走行先の交差点の予測を得て、
減速するとともに、
減速することを他の車両に伝え、
危険を回避

→安全向上だけでなく、燃費向上等
な効果が期待できる

IoTとクラウドからの情報は、
インフラ投資と無関係にリッチに

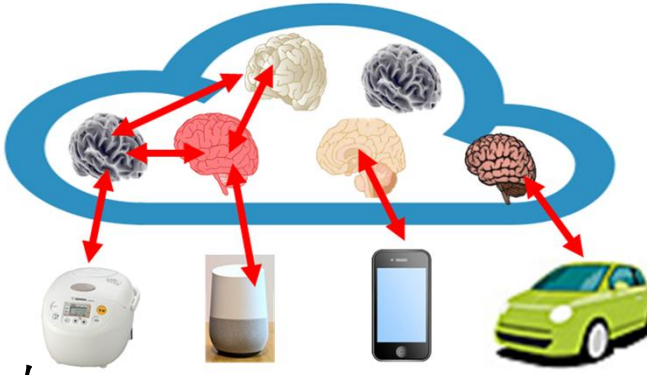
IoTの革新性

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

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

IoTが進まない現状と
セキュリティからみた将来

1．ドイツが Industirie 4.0なら
　日本は Society 5.0

2．そもそも IoT の革新性は

3．　System から SoS へ
**　(Systems of Systems)**

4．　IBM Watson にみる日米の情報力の絶望的な格差

5．　成功体験に甘んじたボトムアップ経営の結果

6．　サイバーセキュリティからみたプラントの将来

革新を進める世界観
SOS(Systems Of Systems)

Systematic Approachは当然の進め方

- 自分の目的を明確にし、必要な**情報を集める**

でも、これから重要なのは、Systems of Systems

- それぞれが、独自の目的を持ったシステムの集合
- 新たなサービスを生み出すためには、
  既存のシステムが他人が利用できるように**情報を提供**
- 共有といっても見境なく情報を公開するわけではない

日本の企業のこれまで、（これからも？）

- 他人の情報は欲しいけど、自分のものは渡さない。
- ベストプラクティスも基本データも海外から入手

情報の組み合わせでイノベーション

- 本来の目的とは異なる利用を促進するためには、
  他のユーザーでもその利用可能性を判断できる情報が必要
  設計や運転などの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

Industrie 4.0

RAMI4.0(Reference Architecture Model Industrie 4.0)と

Iustrial Internet Consortium

IIRA(Industrial Internet Reference Model)

Targets for the Reference Model

参照モデルのねらい

1. Illustrative and simple architectural model

- Structuring of all Industry 4.0 aspects into manageable partial contents for focused discussions

I4.0に関係するすべての情報の構造的な関連を理解しやすいように整理し、
個々が注目している論点の全体での位置づけを理解し、意識共有できるようにする。

2. Localization of existing norms and standards

- Identification and closing of gaps
- Identification of overlaps and establishing preferred solutions
- Identification of subsets of a norm or a standard for rapid implementation of partial contents of Industry 4.0

I4.0に関係する要素を個々に標準化し、むだやギャップをなくし、
アイデアから実装までを早く実現し、競争力を高める

3. Localization of Use Case content

- To identify and close technical gaps for the implementation of use cases
- Identification of development opportunities for the future

参照モデルでの整理から、実装までのスピードアップに対する技術的な不足を特定し、
将来のための、開発の対象を特定し、競争力を高める

以下のRAMI4.0に関するスライドは、下記の2つのpdfファイルから入手した図を利用して作成した。

http://www.omg.org/news/meetings/tc/berlin-15/special-events/mfg-presentations/adolphs.pdf

http://www.zvei.org/Downloads/Automation/5305%20Publikation%20GMA%20Status%20Report%20ZVEI%20Reference%20Architecture%20Model.pdf

設計意図も含めた様々なレベルの知識を連携させる情報構造の参照モデル

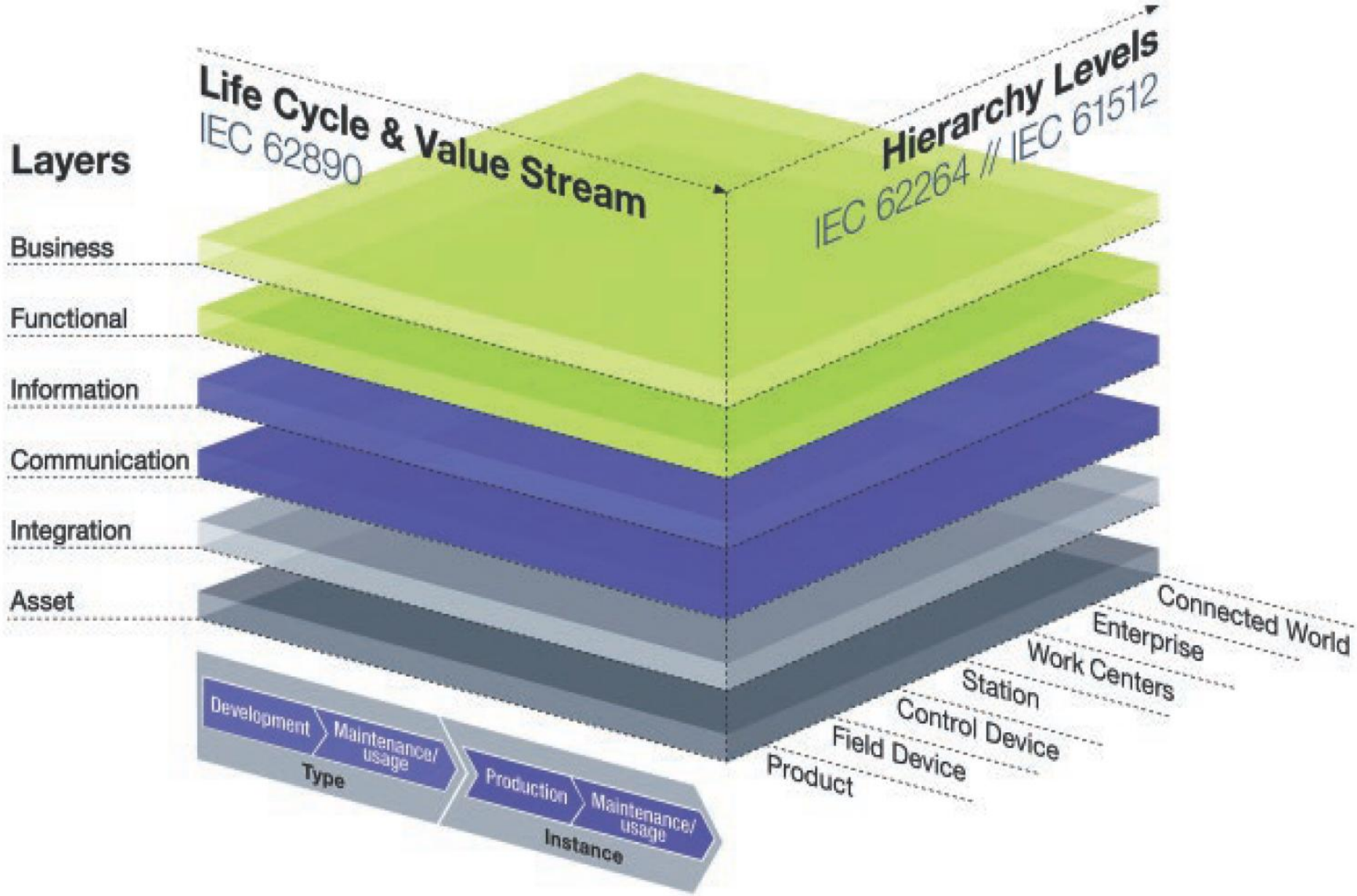


Figure 1. Reference architecture model for Industrie 4.0 (RAMI4.0)

IICは、世界中からの参加を求めている

- IoTによるビジネス変革のベストプラクティスを求めている
  (Energy, Healthcare, Manufacturing, Public domain,
  TransportationのCross-domain & Interoperability in IoT)
- Testbeds and Projects(提案型の実施例)
  (例1):Huawei, Haier, China Telecom and CAICT)**中国も**
  家電メーカーのManufacturing Quality Management(MQM)
  から他業種への展開（省エネルギー、環境管理も含む）
  Intelligent Manufacturing “Made in China 2025”の中核
  Manpower 55%減, Cost 27%減, Productivity 15%増
  （設備で5%,サービスで5%,End-Point需要発掘で5%）
  (例2):IBM and National Instruments(予知保全)
  Develop a new Predictive Maintenance Analytics modelling techniques:

ドイツの例も存在する。日本からの参加を募るとのアナウンスもある。
日本では、i3(industrial internet institute)というIICにエントリーする前の
中小企業、ベンチャーが参画しやすい組織もできた。(2016年8月設立）

IIC日本代表 吉野晃生（日本OMG代表理事)yoshino@omg.or.jp
Object Management Group

Architectureだけでは、情報の理解は進まないが、枠組みを定めるのは重要

- 従来より、データと情報の差違は意識されていて、
  XMLのタグなどの設計が検討されており新しい話ではない。
  「１０という数値だけでは、情報ではなく、
  それは気温でどこでいつどのように観測されたという情報もついて、
  その数値が平常か、例年になく寒いことを示すのか判断できる」

東京に出かける前に出す

- **RAMI4.0**や**IIRA**は、非常に広範囲なターゲットを設定し、
  その設計意図まで理解し、適切に流用できる構造を目指している

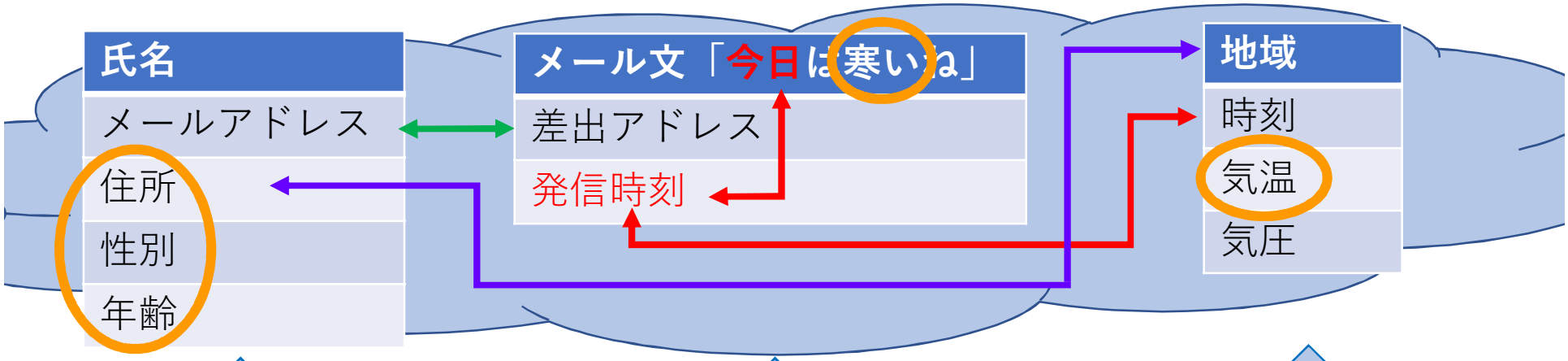
- 広範な統一規格が整備されるには、時間が必要だと考えられるが、
  少なくとも、Siemens, SAP, GE, IBMなどは、
  この構造で自社システムを展開し、情報を蓄積しつづける。
- 共有といっても、見境なく情報を開放するわけではない。
- 規格が決まるのを、手をこまねいてみていると、
  決まった時には、情報力に絶望的な差が発生してしまう

IoTが進まない現状と
セキュリティからみた将来

1．ドイツが Industirie 4.0なら
　日本は Society 5.0
2．そもそも IoT の革新性は
3．System から SoS へ
　(Systems of Systems)
4．IBM Watson にみる日米の情報力の絶望的な格差
5．成功体験に甘んじたボトムアップ経営の結果
6．サイバーセキュリティからみたプラントの将来

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。

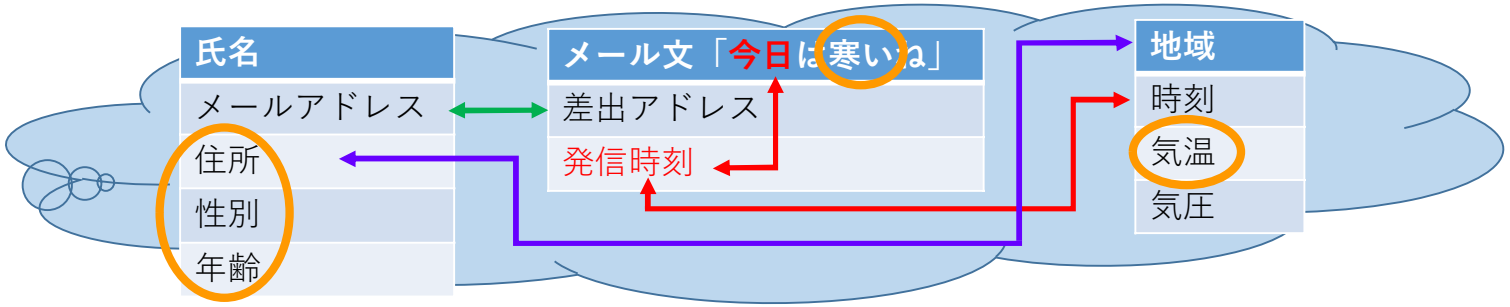


そもそもは、それぞれの目的で収集したデータ

個人情報保護法、プライバシー！

IBM Watson Explore

内部と外部の複数のサイロの構造化データと非構造化データを
接続して、コンテキストに沿ってインサイトの統一見解を提示。



データが充実するほど、新たな関連性が生まれる

でも、コンプライアンスがあるから、
データは各社で用意してね。
各社であかちゃんのWatsonを育ててね。

A社Watson

B社Watson

言語体系による違い

- IBMはCognitive Engineを言語体系ごとに提供している。
- Watsonの能力は、学習データ量に依存するが、
  IBMの各国体制に規模の差があり、赤ちゃんWatsonに格差

English Watson

アメリカでは、２％の保全コスト削減でも利益が500億円になるというように、大規模なプロジェクトがあるので、Watson導入に1億円は必要といわれても、プロジェクトが実施できるが、日本では、そのような投資にみあう規模のプロジェクトをつくれずに、赤ちゃんWatsonを育てる事例がなかなか成立しない。

Japanese Watson cannot grow up.

IoTが進まない現状と
セキュリティからみた将来

1．ドイツが Industirie 4.0なら
　日本は Society 5.0
2．そもそも IoT の革新性は
3．System から SoS へ
　(Systems of Systems)
4．IBM Watson にみる日米の情報力の絶望的な格差
5．成功体験に甘んじたボトムアップ経営の結果
6．サイバーセキュリティからみたプラントの将来

日本の深刻な問題

日本の経営者

時代はSociety5.0らしいぞ。
Big data, Deep learning, AI,うちでもなんかしろ！

日本の技術者

- GEやIBMの成功例はわかっているし、同じようなことはできないわけではない。
- ツール自体は安価に入手できるが、
  ツールが入手できればできるというわけではない。
  (Google翻訳のDeep Learningを自分で開発なんて、とても無理)
- IBMにWatsonを使いたいと言ったら、すごい額が必要になる。
- GEは予防保全でも500億円という巨額の利益を得ているが、
  うちの事業所にそんな大きな事業はないし、投資先はない。
- 他の企業の成功例の情報収集はやっているが、経産省が調べても、IoT推進協議会が募集しても、大したものは出ていない。

はたして、彼らに成功は訪れるのでしょうか？

IoTが進まない現状と
セキュリティからみた将来

1．ドイツが Industirie 4.0なら
日本は Society 5.0

2．そもそも IoT の革新性は

3．System から SoS へ
(Systems of Systems)

4．IBM Watson にみる日米の情報力の絶望的な格差

5．成功体験に甘んじたボトムアップ経営の結果

**6．サイバーセキュリティからみた
プラントの将来**

6.サイバーセキュリティからみたプラントの将来

6-1. **攻撃の脅威は現実のものになっていて、すでに日本でも被害があり爆発も起こりうる。**

6-2. インテリジェンスはセキュリティホールの源であり、クラウドで集中管理すべき。

6-3. 内部は見えないが、複数のバックアップを有し、コントロールというサービスを継続できるFogを事業所においてリアルタイム性のサービスを実現し、その他をCloudに上げ、フィールドはシンプルな機能と通信だけというデバイスで制御する構造が、プラント操業の将来像となる。

6-4. 想定外の攻撃からの防御には、多様性多重性が必要である。全滅を防げれば、検知や対応の可能性が生まれ、安全も確保できる。一人勝ちではなく、多様性を尊ぶ優しい世界に。

http://www.manage.nitech.ac.jp/Security/ に、
この発表に関係する既発表資料を置いている。

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

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

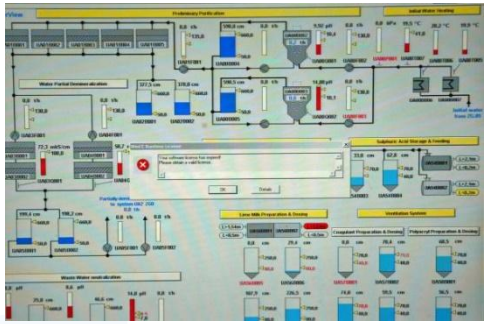
強く認識するようになったが、

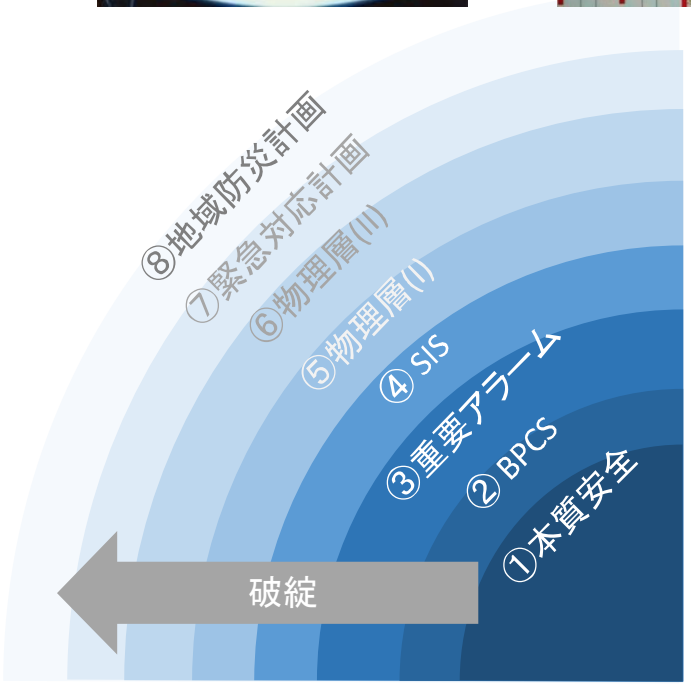
対策は・・・

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

自動車のセキュリティ

2015年 日産リーフ リコール

ＮｉｓｓａｎＣｏｎｎｅｃｔ専用車載通信ユニット（ＴＣＵ：テレマティクスコントロールユニット）交換

オーストリアからイギリスのリーフのエアコンをハッキング

便利なはずの
iphoneアプリに脆弱性

他人でも操作可能

2015年 Jeep 遠隔操作で、急ブレーキやハンドル操作も

通信の脆弱性と
車内通信のもつ
本質的脆弱性

クライスラー対象車
１４０万台超

6.サイバーセキュリティからみたプラントの将来

6-1. 攻撃の脅威は現実のものになっていて、すでに日本でも被害があり爆発も起こりうる。

6-2. **インテリジェンスはセキュリティホールの源であり、クラウドで集中管理すべき。**

6-3. 内部は見えないが、複数のバックアップを有し、コントロールというサービスを継続できるFogを事業所においてリアルタイム性のサービスを実現し、その他をCloudに上げ、フィールドはシンプルな機能と通信だけというデバイスで制御する構造が、プラント操業の将来像となる。

6-4. 想定外の攻撃からの防御には、多様性多重性が必要である。全滅を防げれば、検知や対応の可能性が生まれ、安全も確保できる。一人勝ちではなく、多様性を尊ぶ優しい世界に。

http://www.manage.nitech.ac.jp/Security/ に、
この発表に関係する既発表資料を置いている。

セキュア開発

IoTデバイスの開発

- 開発時点に、悪意のコードが潜り込んでいた可能性を
  できないトラブルがすでに発生している
- セキュアデバイス、コードの利用
- 開発時の人とコードの管理とテスト方法

IoTデバイスのメンテナンス

- OSのような共通ソフトの脆弱性について、
  そのパッチが自システムに与える影響を評価できる必要が
  ある
- 脆弱性が、共通のソフトだけで発生するわけではない。
  個別ソフトに脆弱性が存在するかというチェックと、
  開発後別のシステムで発見された脆弱性と
  自システムとの関係をチェックし、
  必要な対策を適用できる体制が必要になる。

セキュア開発は、ソフトだけでなく、ハードウェアにも注意

- 2005年11月、偽造品を追跡する国防総省・軍需企業間の機密プログラム「政府・企業間データ交換プログラム（GIDEP）」は、英航空防衛大手BAEシステムズの製品で「現場故障（兵器装置の故障）が発生」との警告を発した。BAEシステムズは原因が偽造マイクロチップにあることを突き止めた。
- 2016年にも、アメリカの兵器用に調達したチップにも、不正な回路が仕込まれているものが大量にみつかるという事件もあった。
- ハードウェアモジュールの信頼性の確保も重要な問題である。
  （安い部品を使うことの危険性も意識する必要性がある）

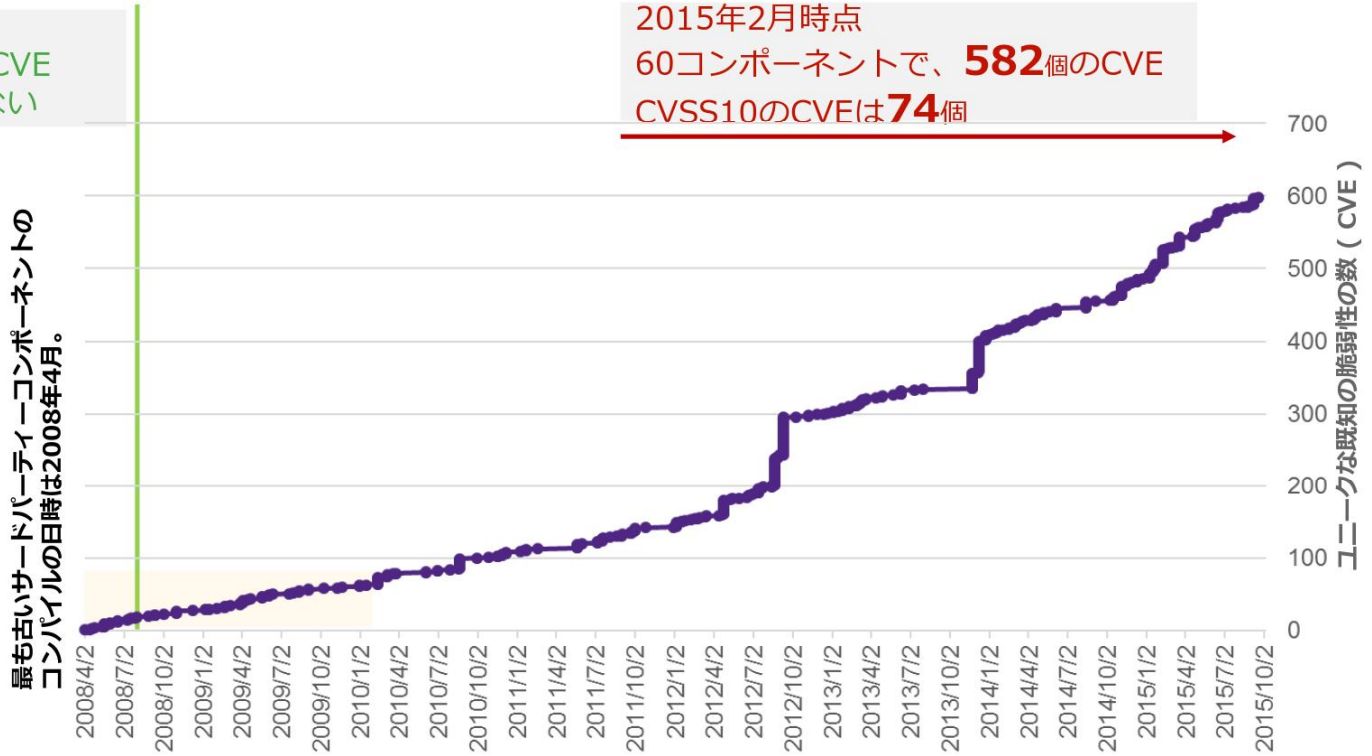
開発時はセキュアと思っても…

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

- 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



SYNOPSYS®

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

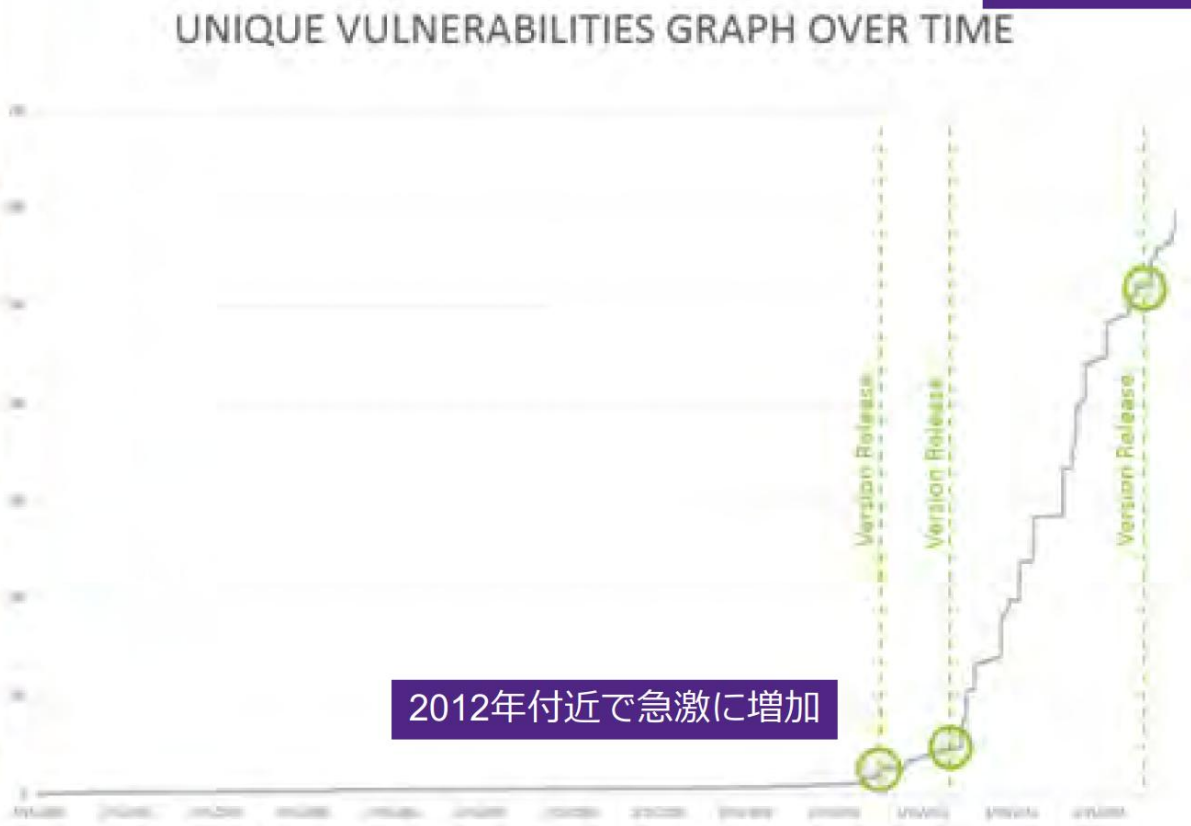
Synopsysから入手した資料より

脆弱性の報告数が激増中

脆弱性が増加し始めている

- **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

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



SYNOPSYS®

Synopsysから入手した資料より

脆弱性がわかっても対応しきれない例も

サードパーティーコンポーネントの既知の脆弱性への攻撃

サポート終了後も*1400*以上の既知の脆弱性を含んだまま利用され続けている医療機器

- ICS-CERT アドバイザリ: ICSMA-16-089-01
  - CareFusion社Pyxis Supply Station薬剤管理システムの脆弱性
- Billy RiosとMike Ahmadi(Synopsys 社)の調査
- ソフトウェアコンポジション解析(Protecode SC)により1400個 以上の既知の脆弱性を検出
  - Critical: 179個
  - Major: 606個
  - Minor: 97個
- 検出されたコンポーネントの一例
  - Microsoft Windows XP, Sybase SQL Anywhere 9, BMC Appsight 5.7, など

まずは、ソフトウェアで利用されるコンポーネントと既知の脆弱性の把握が重要

SYNOPSYS®

Synopsysから入手した資料より

コントロールシステムのセキュリティ問題

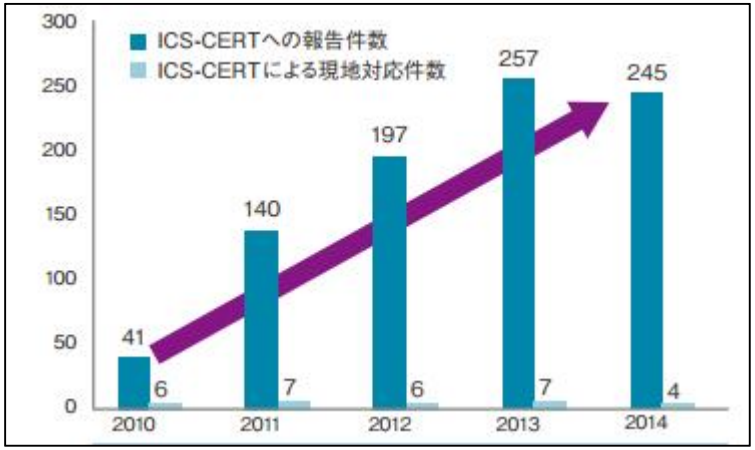
コントロールシステムに対する
サイバー攻撃が増加

計装システムの脆弱性の発見も増加

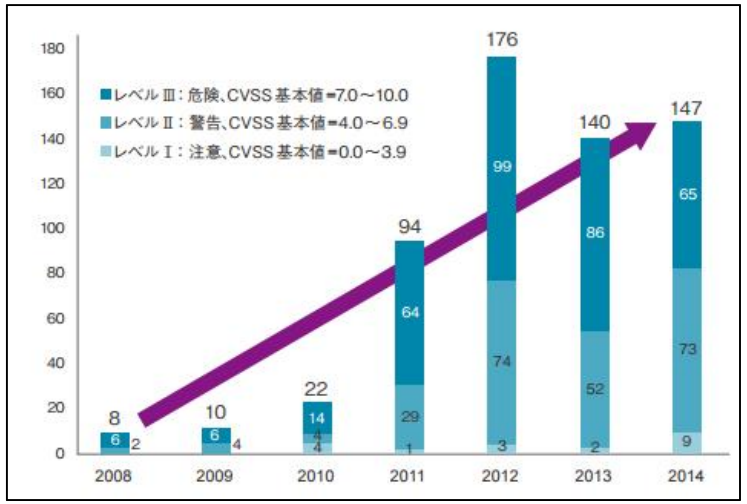
しかし

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。

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！

プログラムのセキュリティ管理

検討課題例

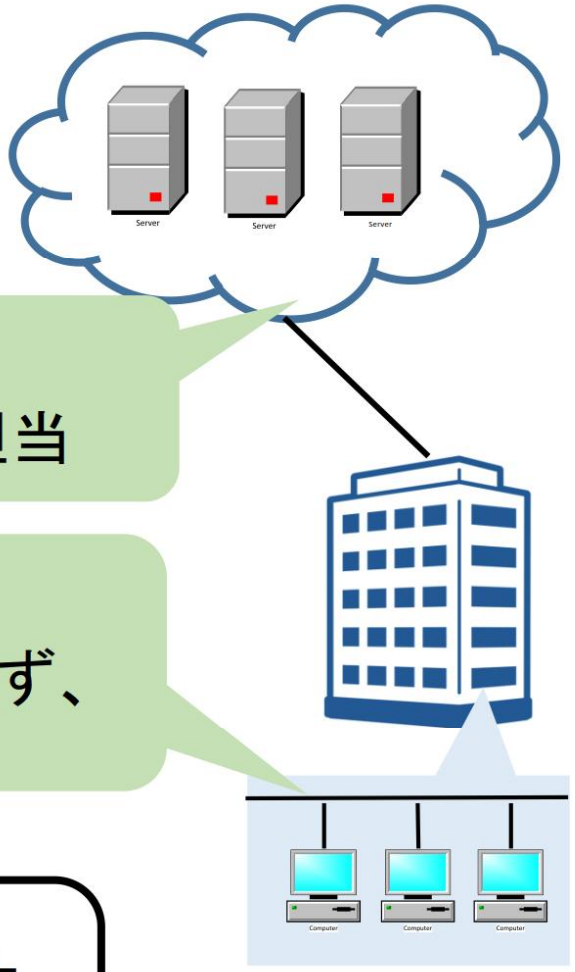
10年前に社員が開発したプログラムに、利用されているモジュールに脆弱性が見つかったと報告を受けた。

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

6.サイバーセキュリティからみたプラントの将来

6-1. 攻撃の脅威は現実のものになっていて、すでに日本でも被害があり爆発も起こりうる。

6-2. インテリジェンスはセキュリティホールの源であり、クラウドで集中管理すべき。

6-3. **内部は見えないが、複数のバックアップを有し、コントロールというサービスを継続できるFogを事業所においてリアルタイム性のサービスを実現し、その他をCloudに上げ、フィールドはシンプルな機能と通信だけというデバイスで制御する構造が、プラント操業の将来像となる。**

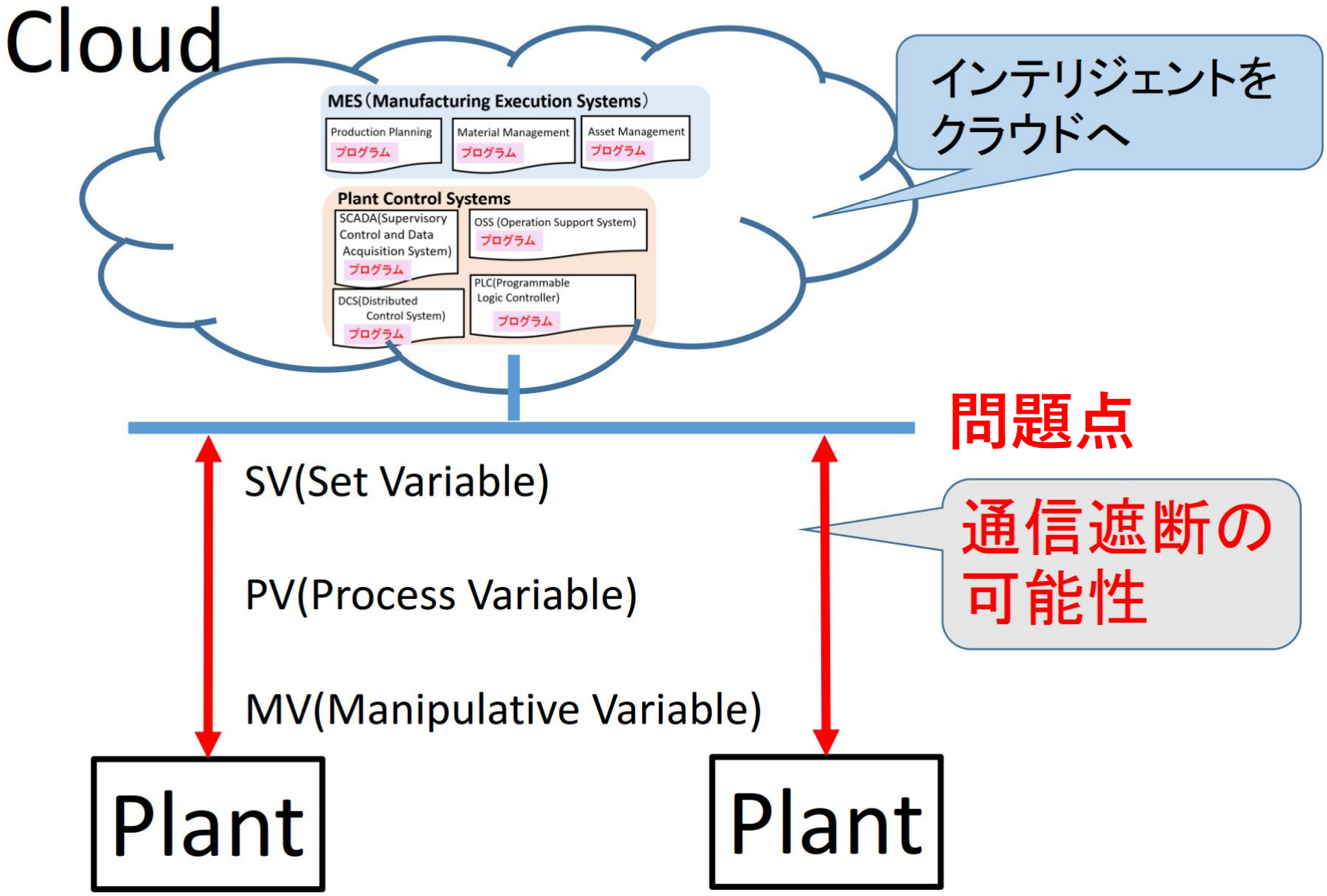
6-4. 想定外の攻撃からの防御には、多様性多重性が必要である。全滅を防げれば、検知や対応の可能性が生まれ、安全も確保できる。一人勝ちではなく、多様性を尊ぶ優しい世界に。

http://www.manage.nitech.ac.jp/Security/ に、
この発表に関係する既発表資料を置いている。

制御だって、ものから離れたい？

- 製造現場の制御システムは、ロボットのコントローラのように、装置に組み込まれているものから、DCSやPLCのように、装置からは離れて設置されているものもある。
- モデル予測制御などの高度制御や、生産管理システムも、それぞれのワークステーションをもっていて、装置とは離れている。
- 組み込み系に限らず、それぞれの機能は、ハードウェアの拘束を受けているのではなかろうか。
- それぞれを「**ハードウェアにとらわれず、サービスを継続的に提供する**」というクラウドの観点から見直すとどうなるであろうか？

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

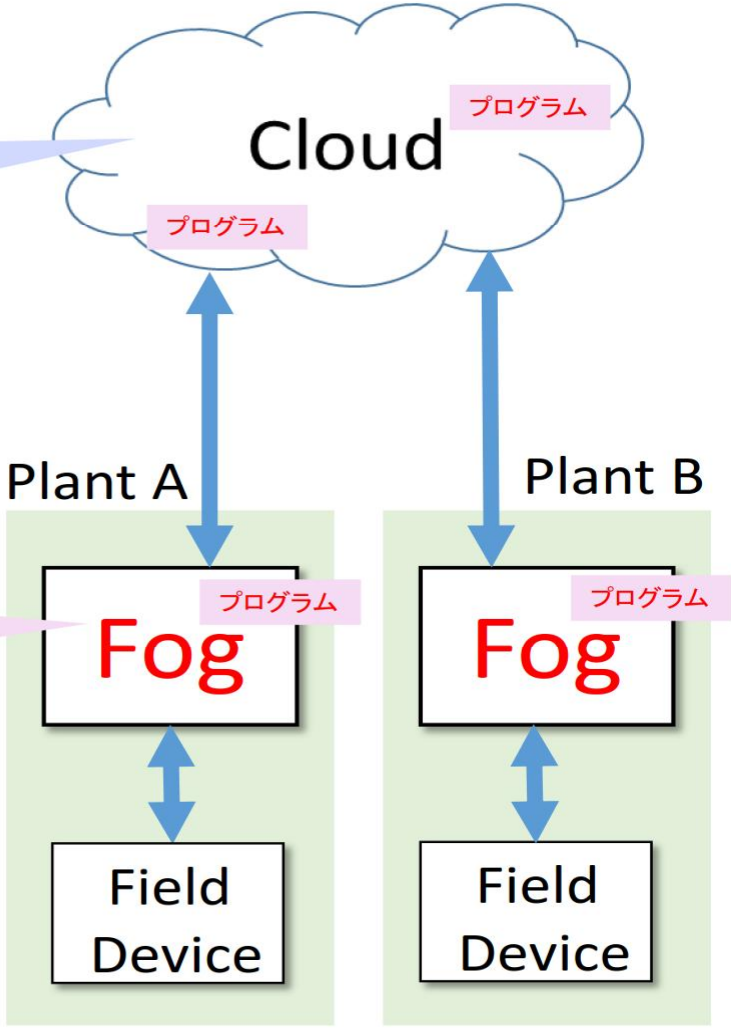
Fogによるクラウド機能の導入

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

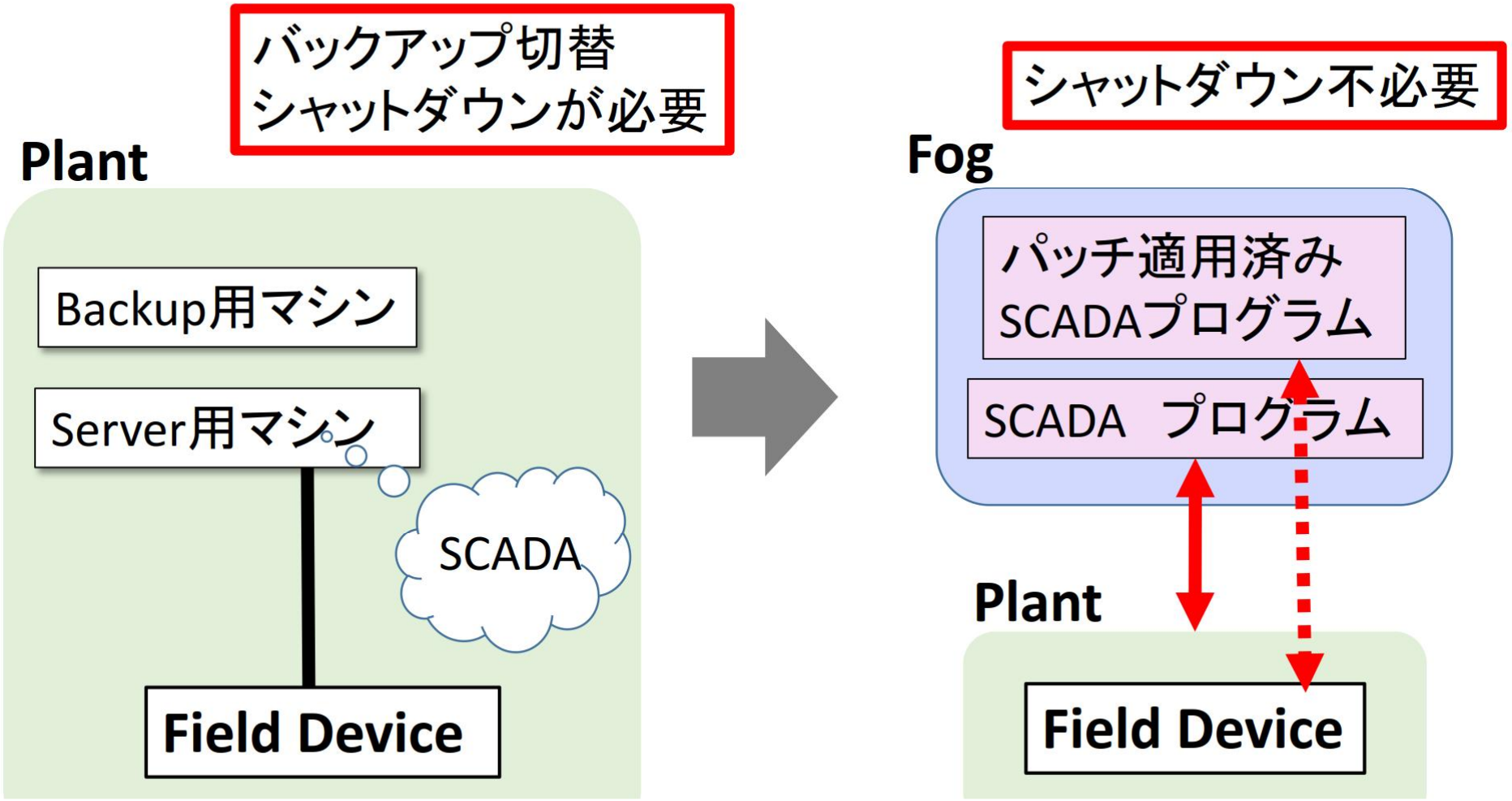
各プラント敷地内に
疑似Cloud環境（Fog）を構築

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

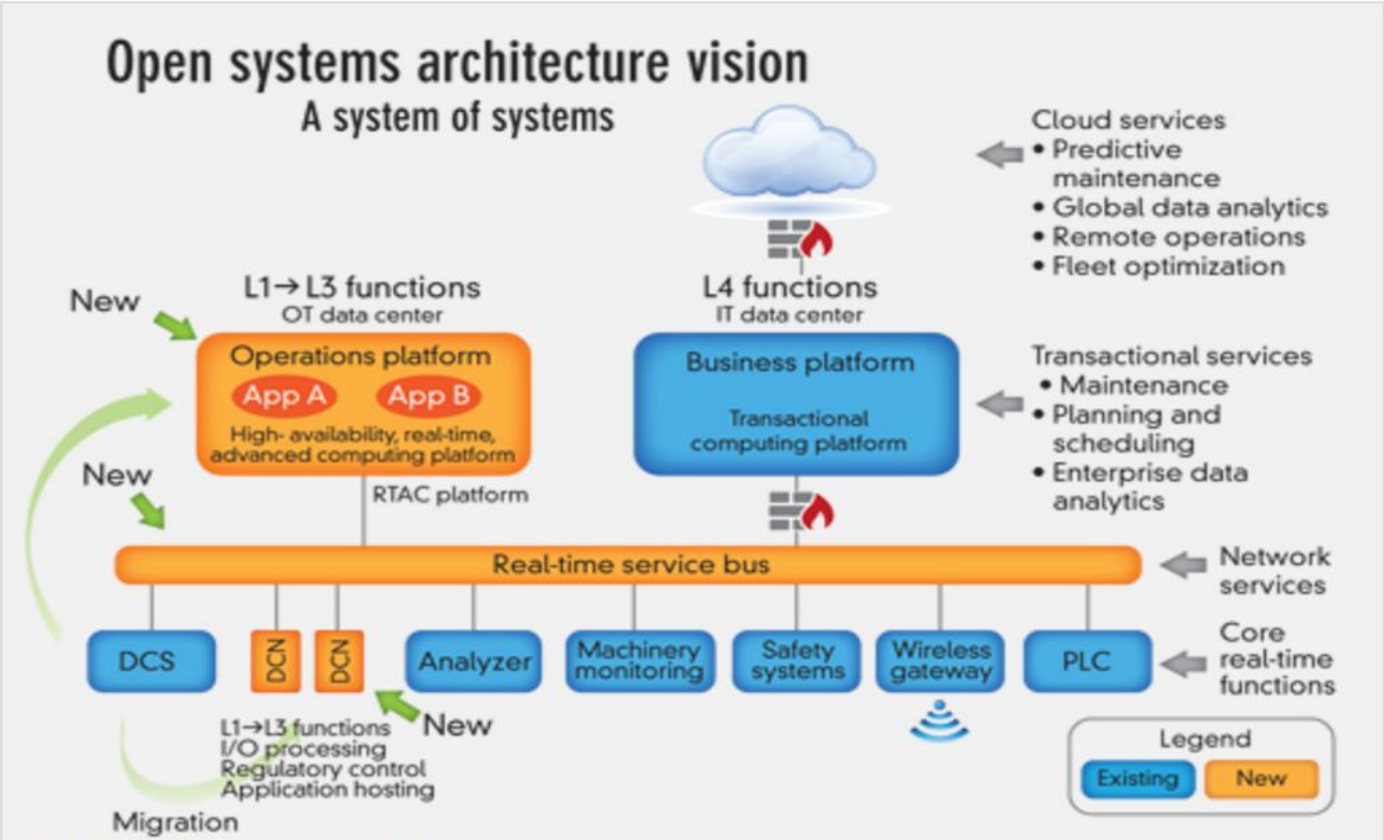


セキュリティパッチの適用やバックアップへの切り替えが容易

FogはOpenStackを利用して安価に研究室で実装済

ExxonMobil次世代生産システム

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



DCS dream taking flight

ExxonMobil envisions a new "system of systems" that will allow it to more easily adapt its operations environment to change needs and opportunities. Graphic by ExxonMobil.

Lockeed Martin: Future Airborne Capability Environment (FACE) Consortium since 2010

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/

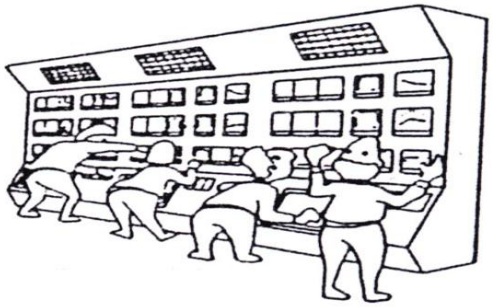
SERCOS Sercos III FPGA or an ASIC master component. http://www.sercos.org/

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

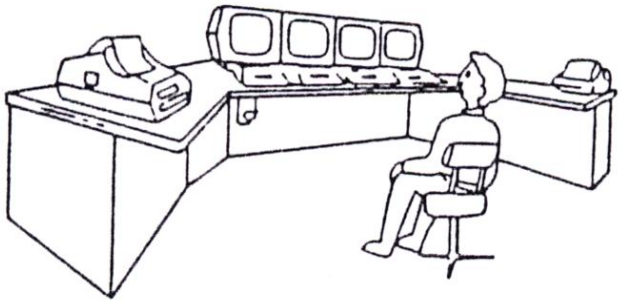
制御システムの保証はだれが？

ExxonMobilは、1975年に、パネルからDCSへの計装の革新を
ハネウェルとともに推進してきた
それ以来の事業所もあり、その保全コストも膨大になっているし、
一般には15~20年に1回のDCSの更新にも莫大な費用が必要

Analog Panel Board
（～1980）



DCS（Distributed Control System）
（1980～）



NEXT
(20XX)

DCSベンダーは、高価ながら、故障が少なく、24時間体制でのサポート体制で、高信頼性を担保してきた

オープン化でマルチベンダーになると、安全の責任は、
アセットオーナーがすべて取ることに？？

制御システムに対するセキュリティ保険

- オープンになれば、購入も保守も安価になるはず

  アセットオーナーには、
  マルチベンダーによるリスクも発生する

- その浮いた分の経費をセキュリティ保険に投資できれば、保険の大きな原資になる

- 信頼性の高い商品は、保険が安くなるという形で、セキュリティ評価がコストとリンクする

  情報漏洩などの情報セキュリティに関する保険は、現存するが、
  物理的な事故につながるサイバーセキュリティに対する保険は、
  まだ存在していない状況ではあるが

- セキュアであることを保証できない商品は、アイデアがよくても参画できないという市場になる

6.サイバーセキュリティからみたプラントの将来

6-1. 攻撃の脅威は現実のものになっていて、すでに日本でも被害があり爆発も起こりうる。

6-2. インテリジェンスはセキュリティホールの源であり、クラウドで集中管理すべき。

6-3. 内部は見えないが、複数のバックアップを有し、コントロールというサービスを継続できるFogを事業所においてリアルタイム性のサービスを実現し、その他をCloudに上げ、フィールドはシンプルな機能と通信だけというデバイスで制御する構造が、プラント操業の将来像となる。

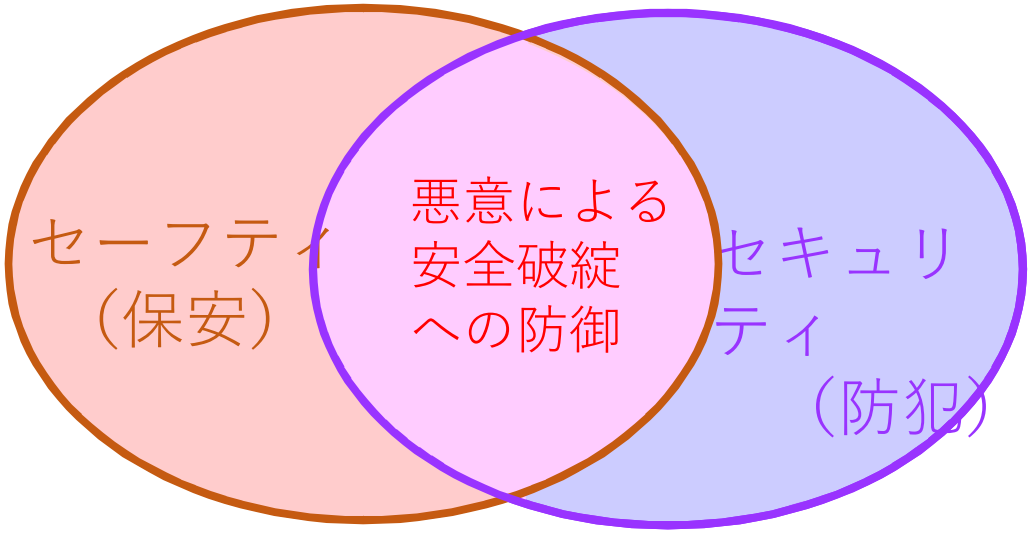
6-4. **想定外の攻撃からの防御には、多様性多重性が必要である。全滅を防げれば、検知や対応の可能性が生まれ、安全も確保できる。一人勝ちではなく、多様性を尊ぶ優しい世界に。**

http://www.manage.nitech.ac.jp/Security/ に、
この発表に関係する既発表資料を置いている。

制御システムの脆弱性

- 制御システムを破綻させるなんて簡単
  （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）
- 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というフリーソフト等で、簡単に傍受解析できる）
- コントローラでは、ウィルス対策ソフトは稼働させない。
  （リアルタイムの制御動作の実現が最優先）
- 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）
- ネットに繋がっていなくても、調整時にはPCを接続
  （Stuxnetのように調整用PCに攻撃が潜んでいる可能性がある）
- ウィルス対策ソフトの検索対象は、2割以下
  （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）
- DCS等制御システムの更新頻度は低い(15年～25年に一度?)
  （新しい錠が開発されるたびに錠を更新し続ける人はいないけど）

SafetyとSecurity

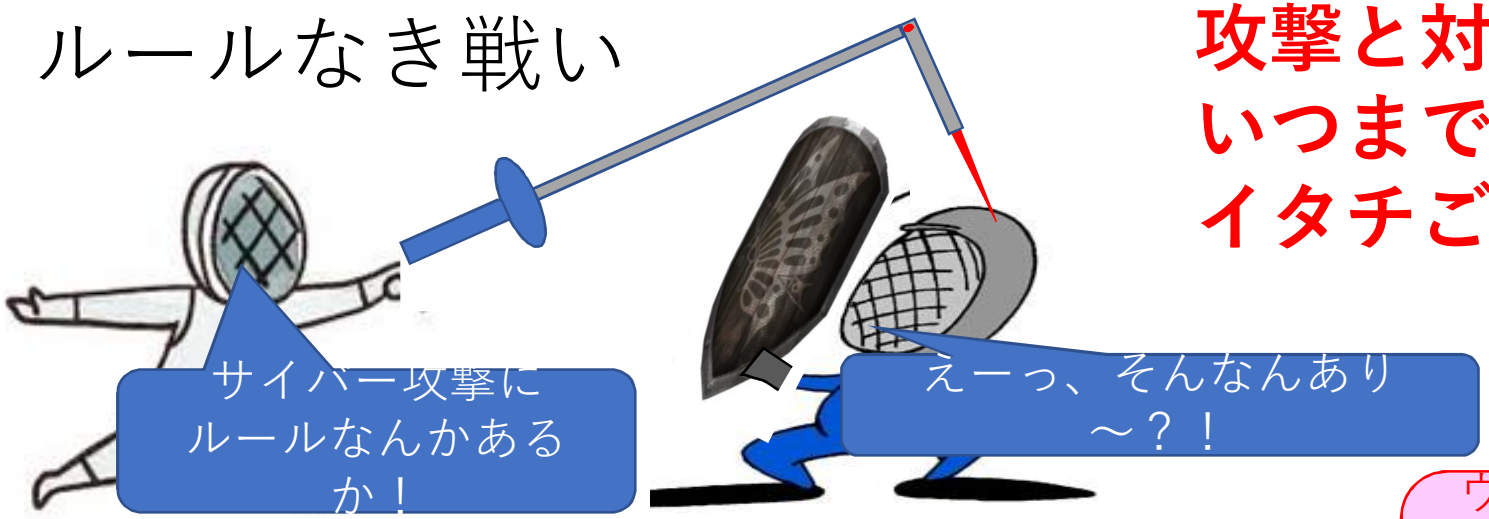


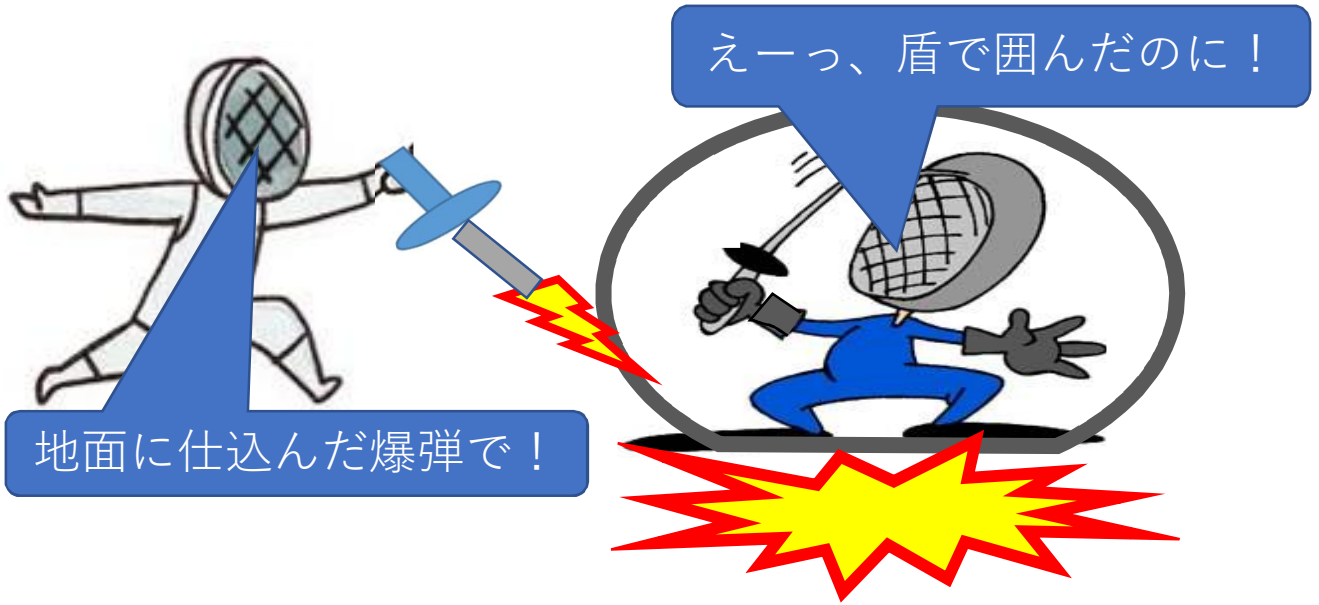
- セーフティの議論では、悪意はほとんど考慮されてこなかった
- セキュリティも守るべき対象に基づいた検討はほとんどされていない
- 制御系サイバーセキュリティに対する議論も、
  プラントのどの部分が危険というより、コントローラを自由にされたら危険であるので、コントロールシステムを守るというかたちで、
  制御対象まで検討している例はほとんどない
- 上記のベン図の共通部分が、すっぽり抜けているのでは

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





IEC62443等でのSALの議論の不十分さ

SAL(Security Assurance Level)

Zones ＆ Conduitsという視点で評価

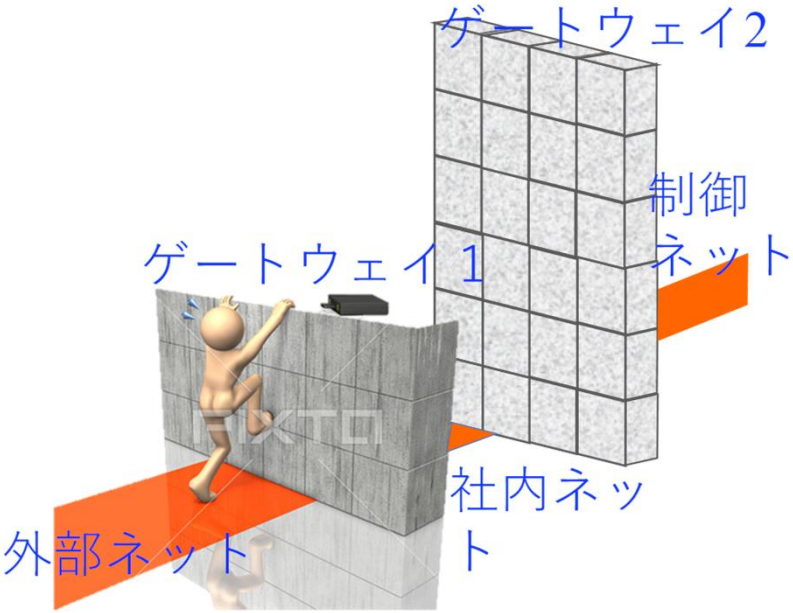
・各装置のSALは、以下の7要件で4段階の管理レベルに評価

1. Access control (AC) 2. Use control (UC) 3. Data Integrity (DI) 4. Data confidentiality (DC)
5. Restrict data flow (RDF) 6. Timely response to an event (TRE)
7. Resource availability (RA)

・ゾーンのSALはゾーン中の最弱の装置のSAL

・全体のSALは、プラントまでのパスで、
最も高い障壁のSAL

攻略のしやすさという点では
理解しやすい
しかし、制御系の安全性が
重要なときに、その評価でOK?

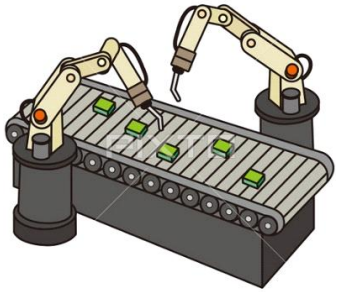


コントローラは、通信経路が攻略されなくても、リモートからの通信で危険になりうる

FirewallもWhite Listsも悪意の通信には対応できない

Cloud　　Fog　　Local Control

コントローラ　　プラント



pixta.jp - 9945344

コントローラ自体をダメにするのはすごく簡単

「攻撃手口」ではなく、守るべき「もの」を基準に対策を検討

- 重要インフラでは、安全対策が真摯に検討されている。
- しょせん、サイバー攻撃は、情報しか操作できない。
  サイバー攻撃は**「悪意の誤操作、悪意の誤動作」**
- 誤操作、誤動作は、従来から、安全解析の対象
- **Fail-Safe, Fool-Proof**として、対策も検討されている。
- 従来の安全解析とサイバー攻撃の違いは「悪意」
- **同時多重**な誤操作、誤動作を対象にすれば、
  サイバー攻撃に対するリスクアナリシスも可能

安全対策をベースに
サイバーセキュリティを検討

同時多発へのフェイル･セーフとフール･プルーフ

鍵・錠や監視カメラやパトロールは？

今は大丈夫でも、**未知の脆弱性**がどのように現れるかわからない。

- 攻撃手口を予想しても、カバーしきれないに違いない。
- 脆弱性に気づき対策を開発できても、すぐに適用できないかも

→　**一つの脆弱性で全滅しない多重の対策**

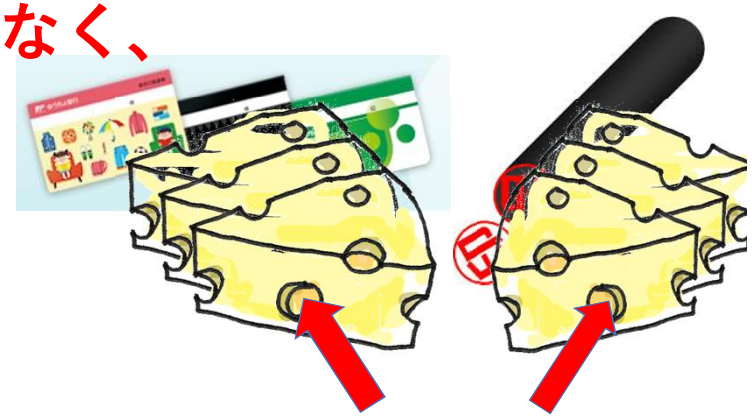
安全をベースにしたセキュリティ対策

ハザードは攻撃の手口で決まるのではなく、
制御対象の特性で決まる。

手口に関わらない対策検討とは？

安全を守る**通帳と印鑑**は？

通帳と印鑑を穴の異なる壁で防御

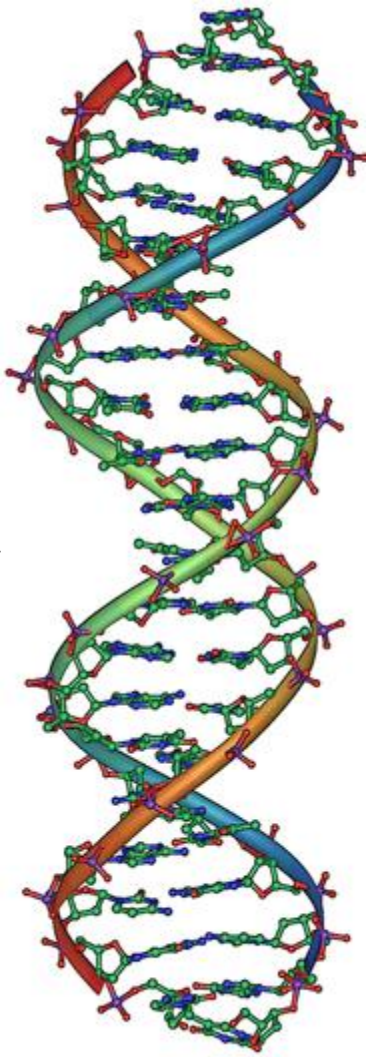


統一化ではなくバリエーションの確保

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

セキュリティから、多様性を尊ぶ優しい世界へ

講師紹介

自己紹介　橋本芳宏

名古屋工業大学 社会工学科 経営システム分野　教授

（制御系セキュリティに関して）

2011年～2012年　経済産業省
　制御システムセキュリティ検討タスクフォース
　人材育成WG 委員
2012年～2014年　IPA（情報処理推進機構）
　制御システムワーキンググループ委員
2016年～　内閣府 戦略的イノベーション創造プログラム
　重要インフラ等におけるサイバーセキュリティの確保
　セキュリティ人材育成 委員
2017年～　IPA産業サイバーセキュリティセンター講師

名古屋工業大学制御システムセキュリティWS開催
　2015年3月19,20日　13社18名参加
　2015年8月26,27日　30社74名参加
　2016年3月29,30日　26社47名参加
　2017年9月12,13日　29社47名参加
　研究室でのサイバー攻撃のデモにはのべ500名以上来訪

（プロセス制御に関して）

2010年～　計測自動制御学会 プロセス塾講師

（略歴）

1985年　京都大学化学工学専攻博士課程（単位取得退学）
1985年　名古屋工業大学 生産システム工学科 助手
2003年　名古屋工業大学 システムマネジメント学科 教授
　　学内組織再編を経て、現在にいたる