

沖縄ICTフォーラム2015 in 石垣島

新産業革命”Industry4.1J”が 世界を変える スマホとロボットと人間・社会

お問い合わせは、VEC (Virtual Engineering Community) のWebサイトの
<https://www.vec-community.com/ja/form/contact>
より、お願いします。

VEC事務局長兼ソリューションアドバイザー
株式会社ICS研究所
村上正志

- **1977年～1991年：日本ペーレー株式会社のシステムエンジニア**
 - － 火力発電所のボイラ自動制御装置、プラント監視制御装置のシステム設計：
広野2号、苫小牧1号、渥美3/4号、知多第二火力1/2号、東扇島1号、秋田、東新潟、川内、仙台、西名古屋、海南、新小倉、阿南、御坊、姉ヶ崎、五井、袖ヶ浦、高砂、松島、下関、玉島、尼崎、伊達、勿来、港、海外プラントなどの建設、改修などを担当
 - － 空気式制御装置⇒電子式アナログ制御装置 ⇒ DDC(16bit ⇒ 32bit⇒ 64bit)の基本設計仕様(Function Blockの基礎構造設計仕様)に関与
 - － 高速故障診断装置を企画、開発、37セット納入
- **1991年～1995年：画像処理VMEボードメーカーに従事**
 - － 大型カラー印刷機の画像処理、大蔵省印刷局の検査装置などのシステムコンサルティング
- **1995年～2015年3月：株式会社デジタル(2002年以降 Schneider Electric Group)**
 - － SCADA製品の事業戦略企画推進担当
 - － SE部長
 - － 1999年～現在 コーポレートコーディネーション／VEC事務局 General Manager
- **1999年6月～現在：Virtual Engineering Company & Virtual End-User Community 事務局長 兼 ソリューションアドバイザー**
<https://www.vec-community.com/ja/>
- **2015年5月～ 株式会社ICS研究所 代表取締役社長 兼 所長**
- **主な活動履歴**
 - － 経済産業省商務情報政策局主催「制御システムセキュリティ対策タスクフォース」委員：2011年
普及啓発ワーキング座長
 - － 制御システムセキュリティ関連団体合同委員会 委員
 - － 日本能率協会主催「計装制御技術会議」企画委員会 委員
 - － 日本OPC協議会 幹事会顧問
 - － MECHATROLINK協会会員 PLCopen Japan

Agenda

日本が抱える実状

第四次産業革命“Industry4.0”

サイバー攻撃対策＋“Industry4.1J”

今、何をしなければならないか

Agenda

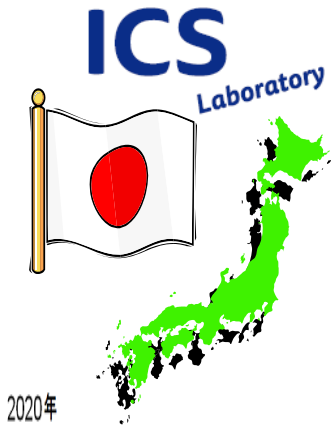
日本が抱える実状

第四次産業革命“Industry4.0”

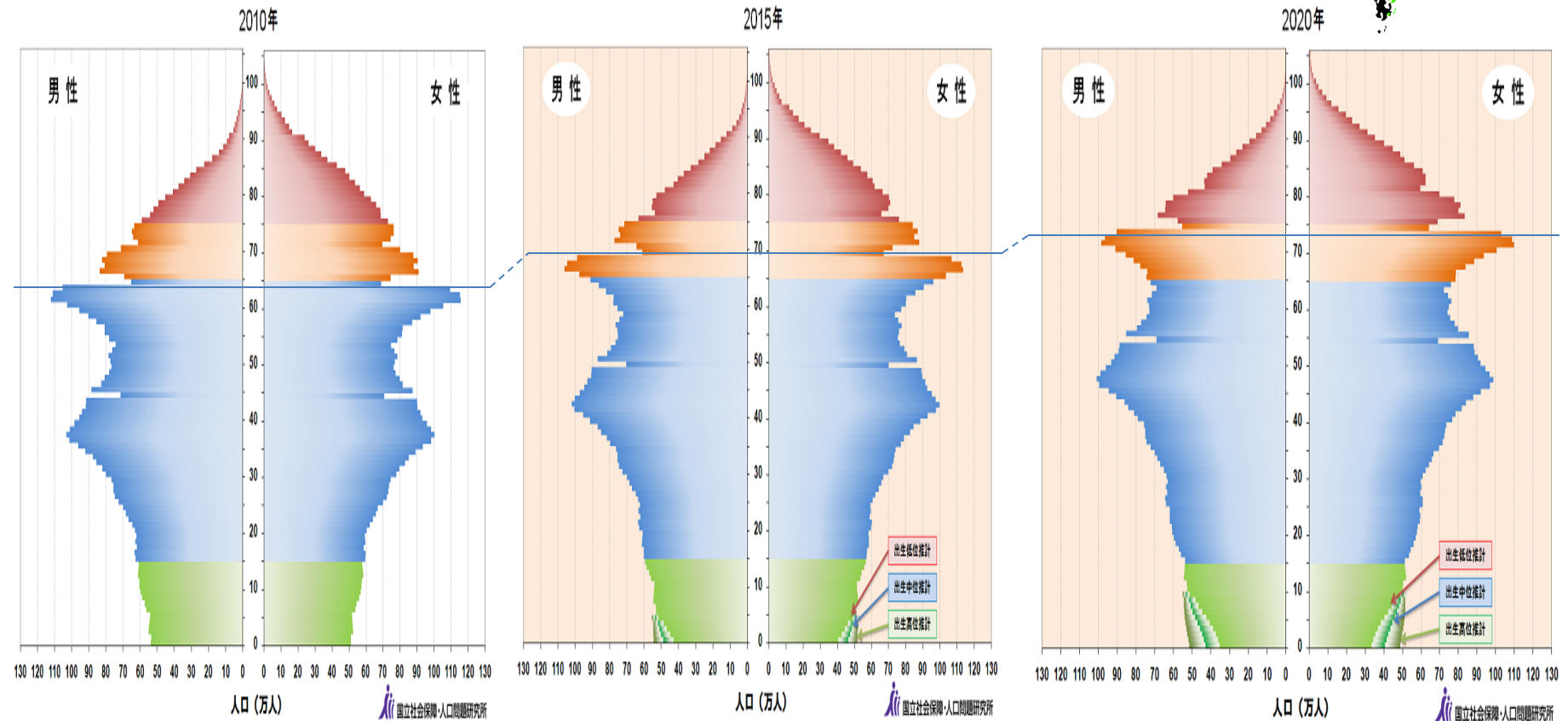
サイバー攻撃対策＋“Industry4.1J”

今、何をしなければならないか

日本が抱える実状



- 少子化、高齢化社会、若者のモノづくり離れ、労働力不足、都市集中・地方過疎化



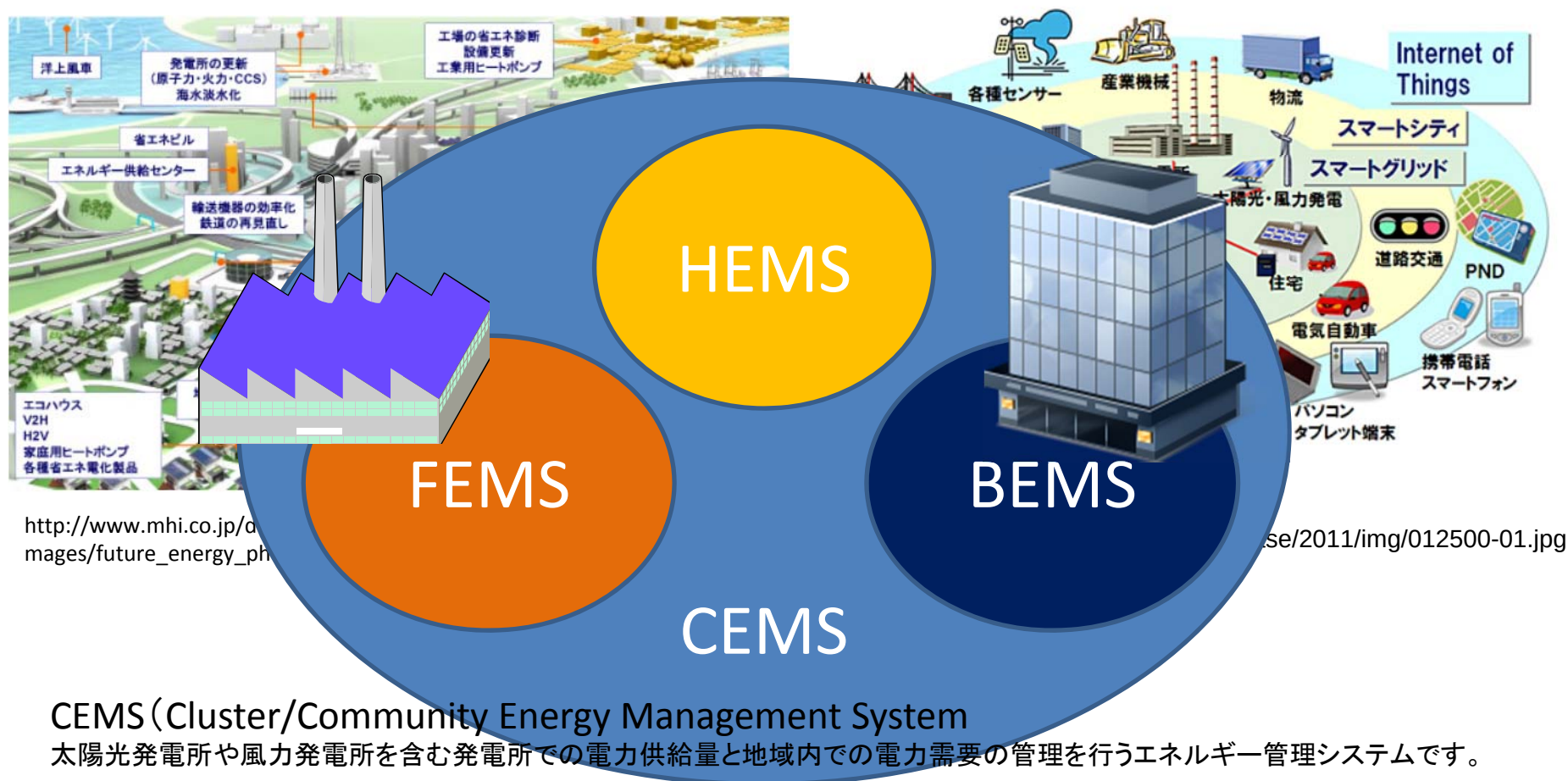
資料：1920～2010年：国勢調査、推計人口、2011年以降：「日本の将来推計人口（平成24年1月推計）」。

資料：1920～2010年：国勢調査、推計人口、2011年以降：「日本の将来推計人口（平成24年1月推計）」。

資料：1920～2010年：国勢調査、推計人口、2011年以降：「日本の将来推計人口（平成24年1月推計）」。

スマートコミュニティ

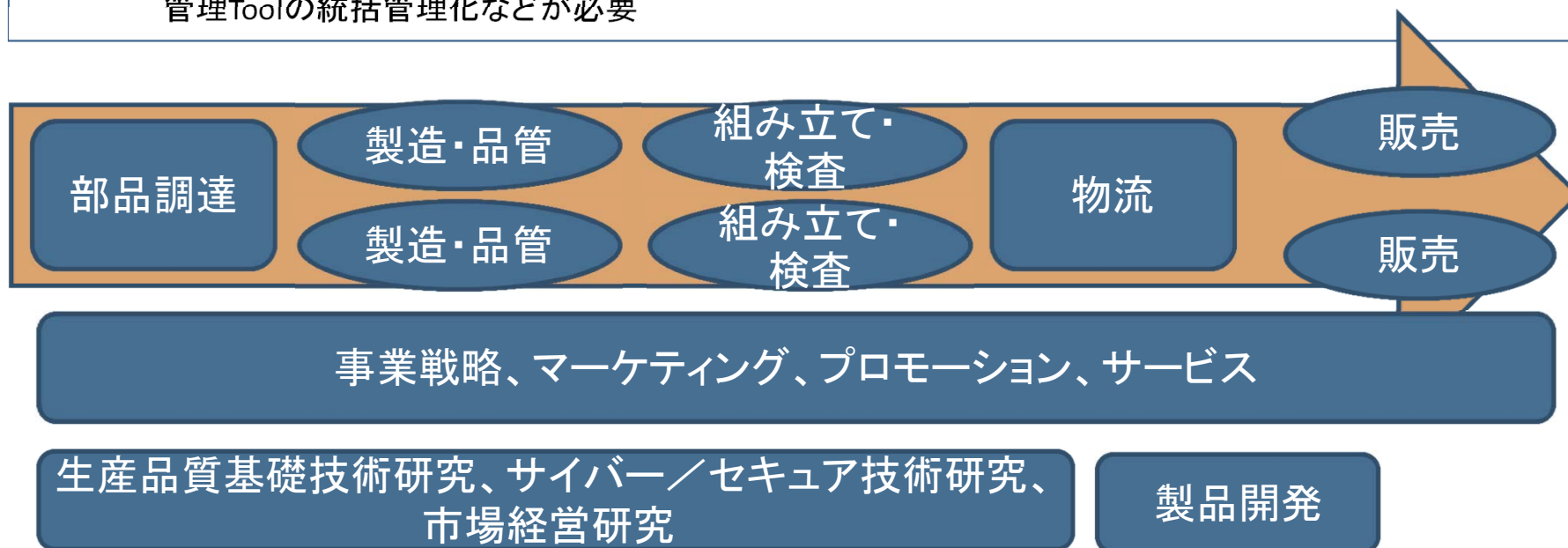
- 住民、地域を含めた「スマート化された送電網を前提としたスマートコミュニティ



<http://www.mhi.co.jp/d...>
images/future_energy_ph...

se/2011/img/012500-01.jpg

- 人の役割単位か、組織単位かは別にして、以下の構成で経営するものづくりの時代
- 統括流動管理、個別生産効率管理、市場価値と利益と投資のキャッシュフロー管理、環境評価指標管理
 - その為に、Engineering Toolの標準化、品質管理Toolの標準化、為替レート／関税／税処理／経費の管理Toolの統括管理化などが必要



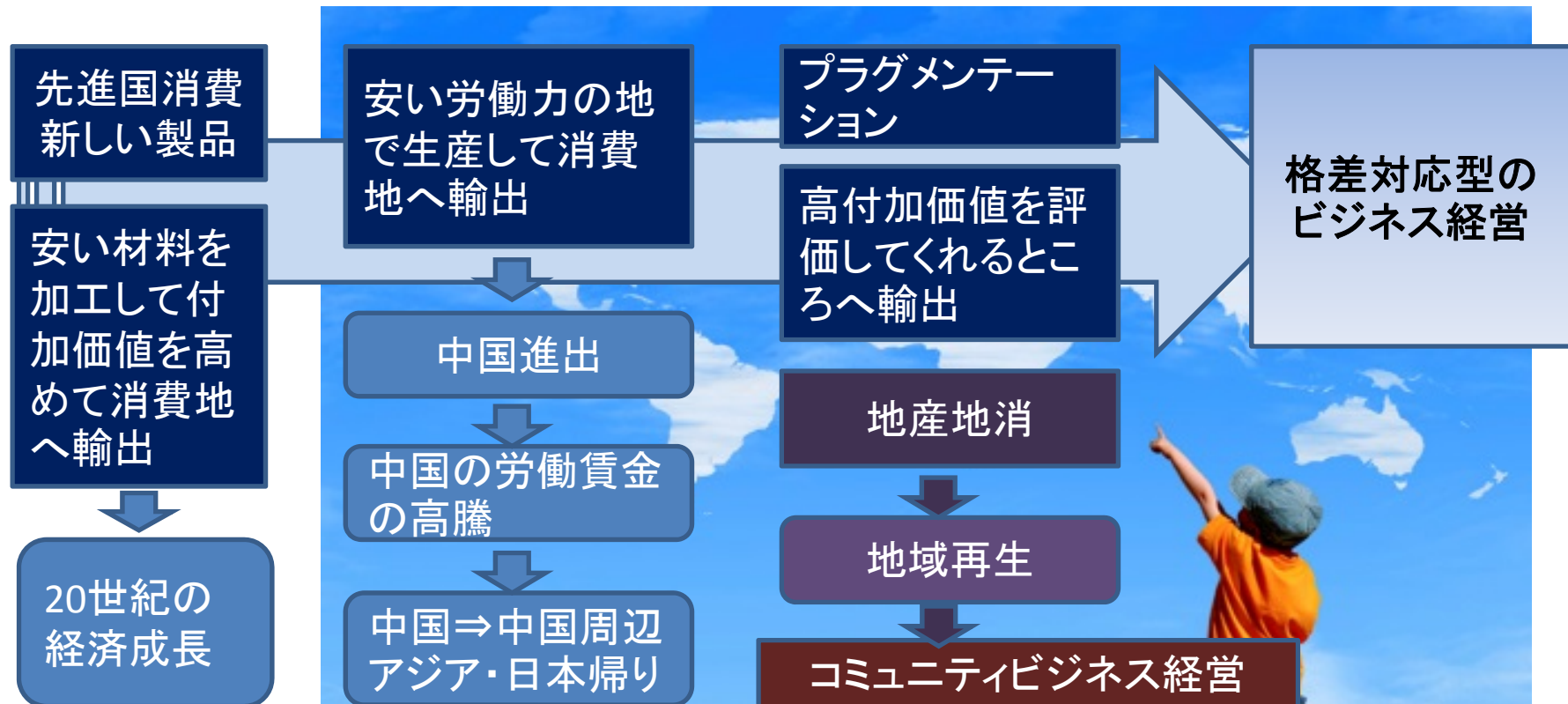
環境対策・制度・報告義務

- RoHS指令: RoHS(ローズ、ロハス、ロース、ロス)は、電子・電気機器における特定有害物質の使用制限についての欧州連合(EU)による指令である。2003年2月にWEEE指令と共に公布、2006年7月に施行された。
- RoHS2指令: CEマーク改正に伴う
- CCC: CCC制度(China Compulsory Certificate system、中国製品安全強制認証制度・中国強制製品認証制度・中国強制認証)とは、中華人民共和国国内に輸入される製品に対して国内技術の標準に適合し、輸入が認められるかを中国政府によって審査され認証が与えられる制度である。この制度は2002年5月1日から適用される。
- REACH(Registration, Evaluation, Authorization and Restriction of CHemicals、リーチ、リーチ法)は、欧州連合における人の健康や環境の保護のために化学物質とその使用を管理する欧州議会及び欧州理事会規則である。また、EU市場内での物質の自由な流通により、競争力と技術革新を強化することも目的にしている。
(REACHは化学物質とその安全な使用・取扱・用途(Use)に関する新しい欧州連合(EU)の法律である。それは、登録(Registration)、評価(Evaluation)、認可(Authorisation)、および、規制(Restriction)制度を化学物質(Chemicals)に適用するものである)
- 作業環境評価基準

グローバル事業戦略とは格差対応型のビジネス

- 「ものづくり」の言葉に酔ってはならない。
- 技術力に頼ってはならない。
- 神風に依存しない。

もし、風が吹いたら **ラッキー**



CBM (condition based maintenance)

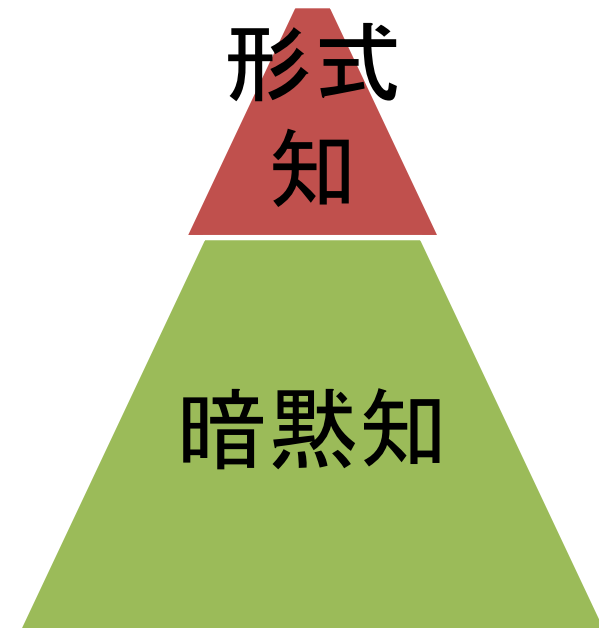
- 予知保全 (CBM: condition based maintenance)
- 過去と現在までのデータを基に、故障が起きるであろう時期を予測して、部品調達計画や在庫管理を実施していく管理手法。

赤外線カメラで撮影した映像データ例

注: センサーネットワークが予知保全や予防保全であるソリューションを出しているメーカーがあるが、品質検査や位置検査などで使用する計測センサーから取り込んだデータを予知保全の基礎データとして利用することはあるが、予知そのものを扱うには予測手法が必要。計測そのものを予知とは言わない。

技術伝承ができていない

- 伝承する相手がいない
 - 化学業界の現場の人員構成の補充不足:20年間
 - マザー工場の海外移転
 - 自動化によって緊急処理の経験機会が少ない。
 - 高度制御技術への投資(金・人)継続ができなかった。
- 
- 爆発事故多発
 - 高度制御技術使用スイッチが切られている



Agenda

日本が抱える実状

第四次産業革命“Industry4.0”

サイバー攻撃対策＋“Industry4.1J”

今、何をしなければならないか



ドイツが抱える社会問題

少子化／高齢
者社会

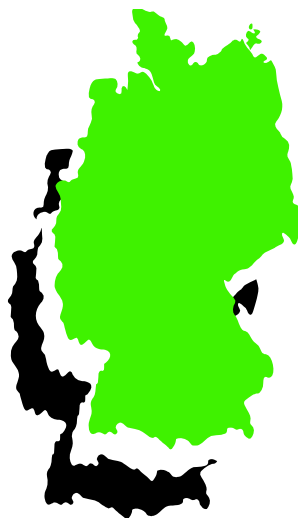
労働者希望者
が減少／若者
の製造業離れ

海外労働者受
け入れ⇒国民
権を認める
か？

少数の労働者
でできる製造
現場

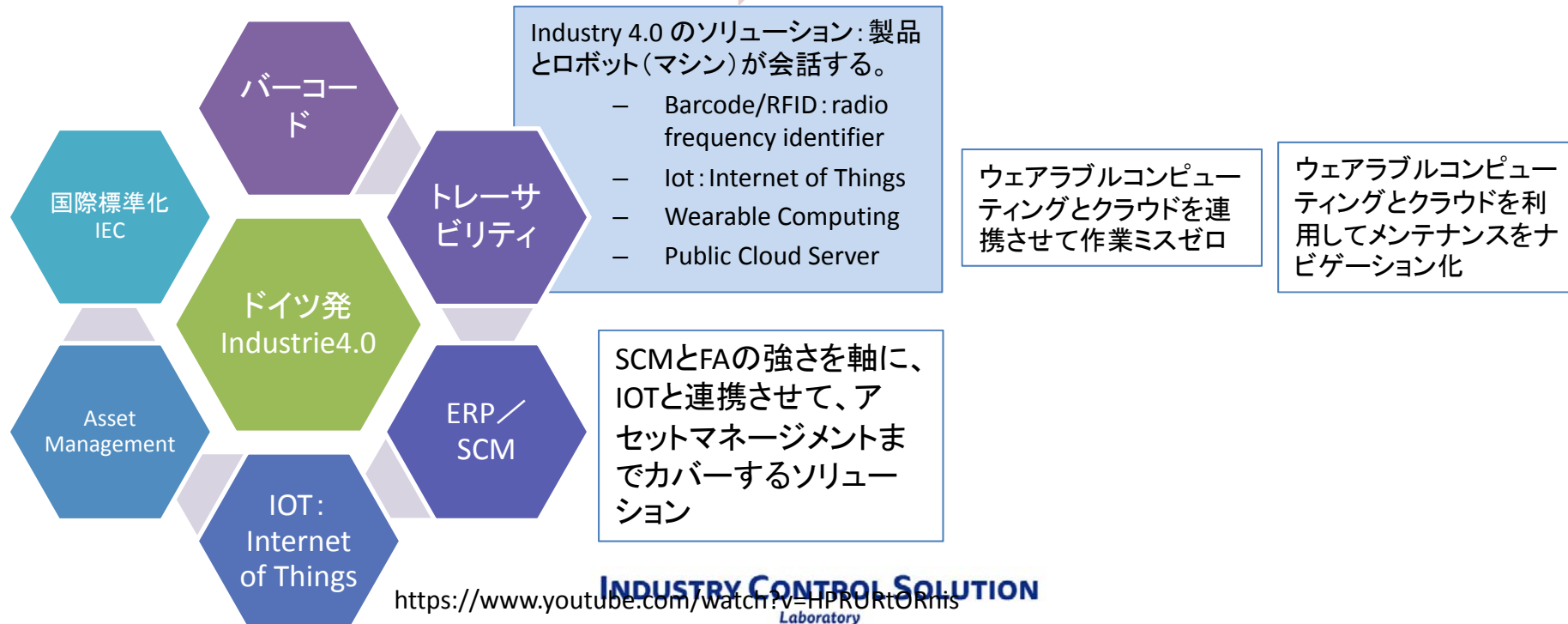
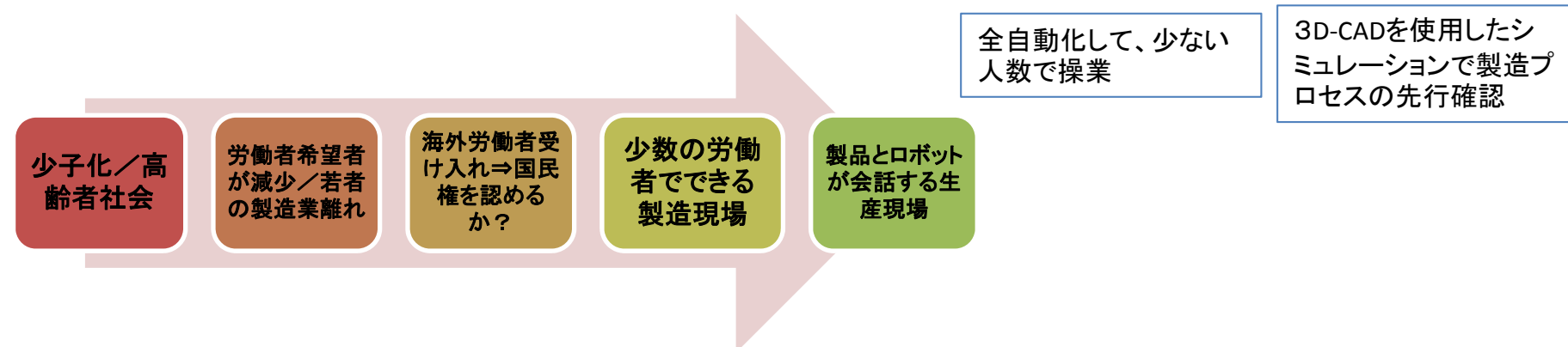
製品とロボット
が会話する生
産現場

産学官の連携でなしえんと考えた政策



Industry 4.0

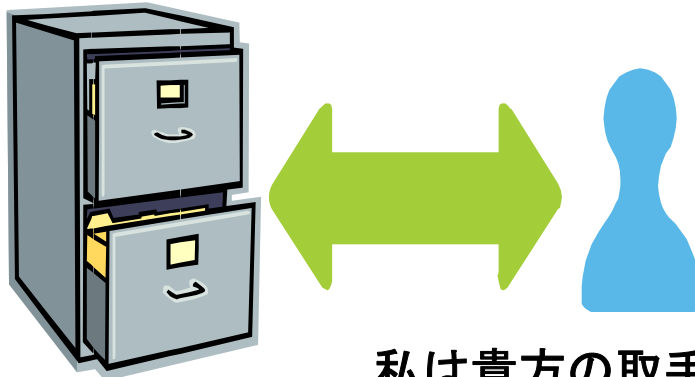
ドイツ国内の課題解決と中小企業現場のオートメーション化推進を目的に推進力を発揮。大企業と中小企業の連携強化。



アフォーダンス (affordance)

- 動物(人)と物の間に存在する行為についての関係性そのもの

私は引き出しです。



私は貴方の取手をつかんで引き出して中のものを見ることができる。

ISO/IEC14443 (10cm以下の近接型情報伝達用途)

ISO/IEC15693 (70cm以下の近接型情報伝達用途)

EPC (Electronic Product Code)

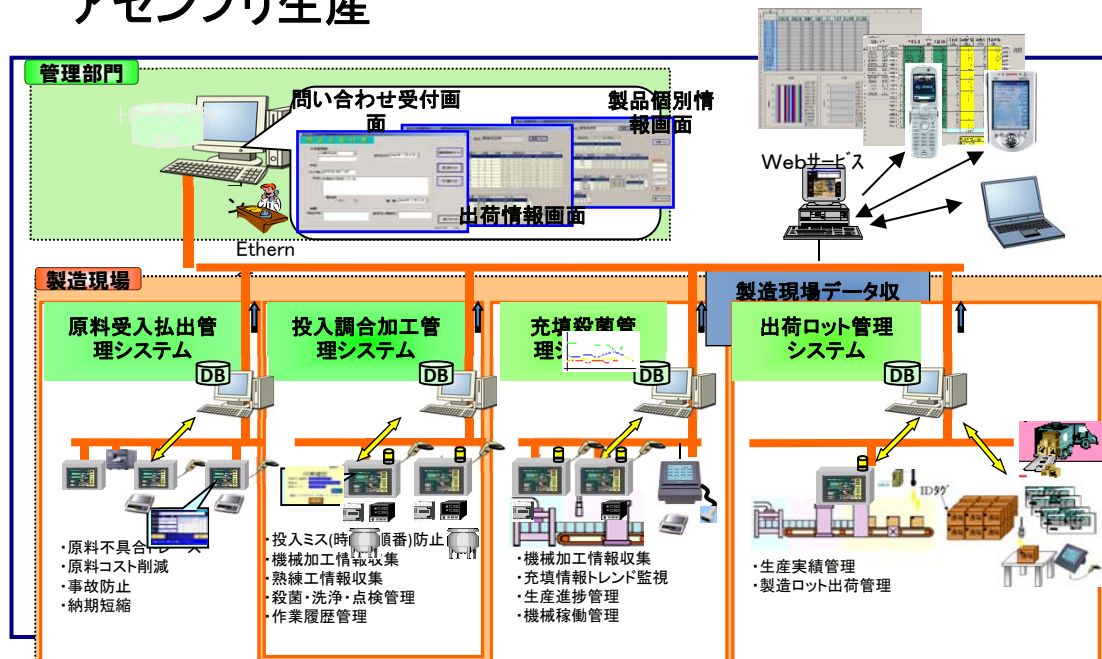
EPCは、GS1傘下のEPC globalで標準化された電子タグに書き込むための識別コードの総称であり、GTIN等のGS1が定める標準識別コードが基礎となっています。そのため、既存のバーコードシステムとの整合性を確保しながら、電子タグシステムを構築することが可能です。

	GS1識別コード	EPC
モノ・製品	GTIN Global Trade Item Number ≡ JANコード	SGTIN Serialized GTIN
場所	GLN Global Location Number	SGLN
輸送・梱包	SSCC Serial Shipping Container Code	SSCC
資産	GRAI Global Returnable Asset Identifier	GRAI
	GIAI Global Individual Asset Identifier	GIAI
サービス	GSRN Global Service Relation Number	GSRN
ドキュメント	GDTI Global Document Type Identifier	GDTI

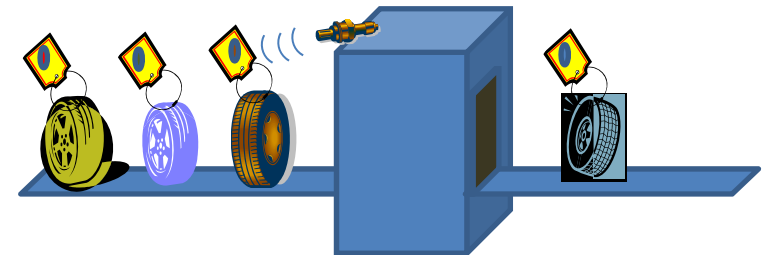
製品の情報を読み取り加工して次へ流す

- RFIDの情報を読み取って、次の生産プロセス加工段階を読み取り、その製品に合った加工をして排出する。

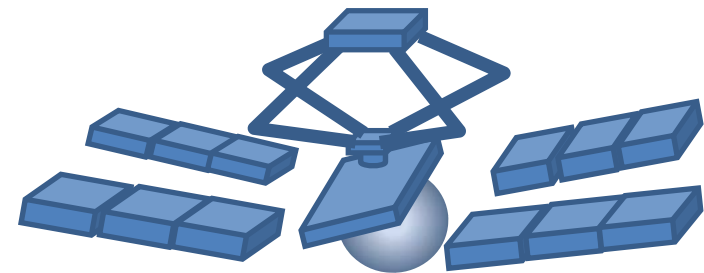
アセンブリ生産



タイヤの刻み加工

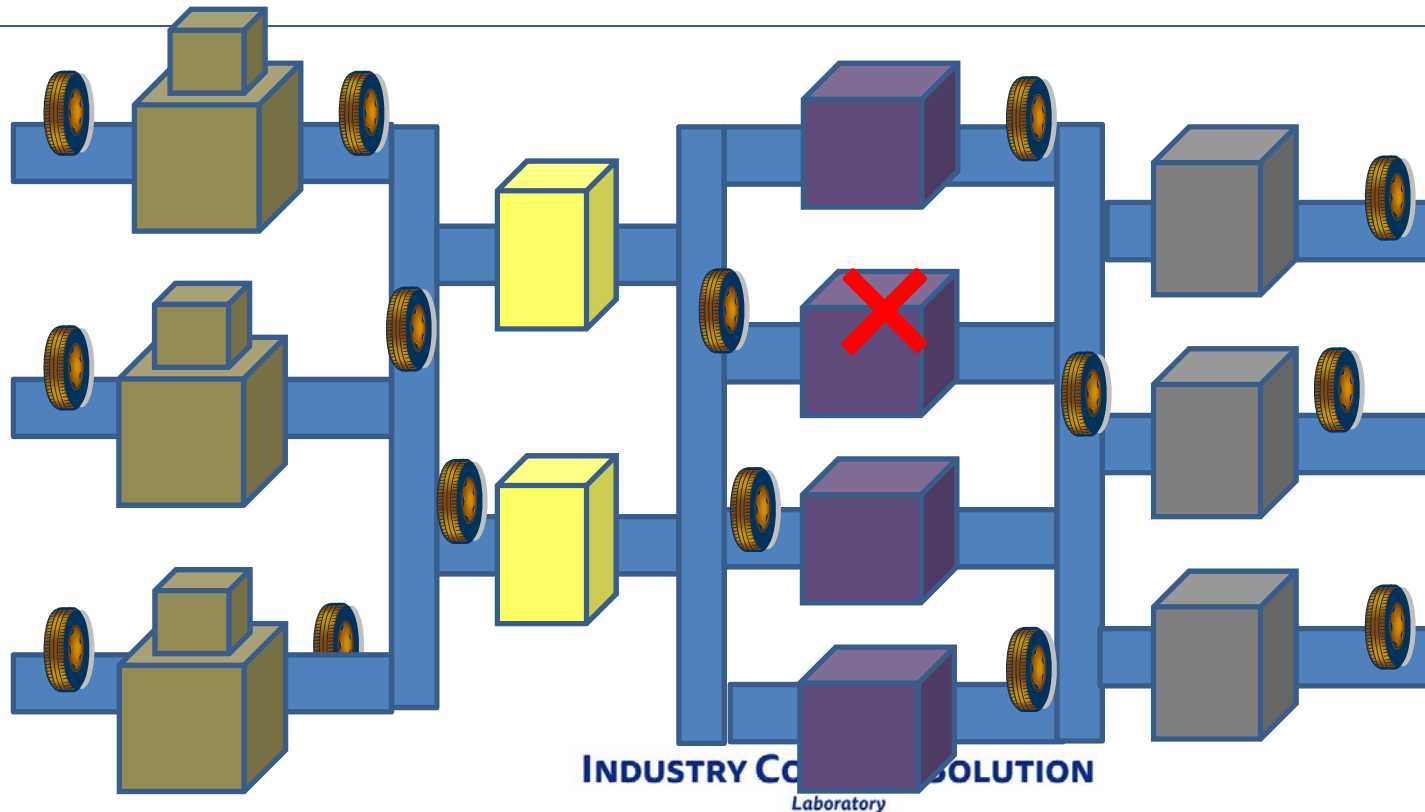


ロボットセル組み立て



アフォーダンス利用の生産ラインの特徴

- 生産プロセスラインの加工装置の故障でラインを変更しても生産継続できる。
- 生産製品の流れが管理できる。
- 予測による適応制御を利用した生産管理ができる。



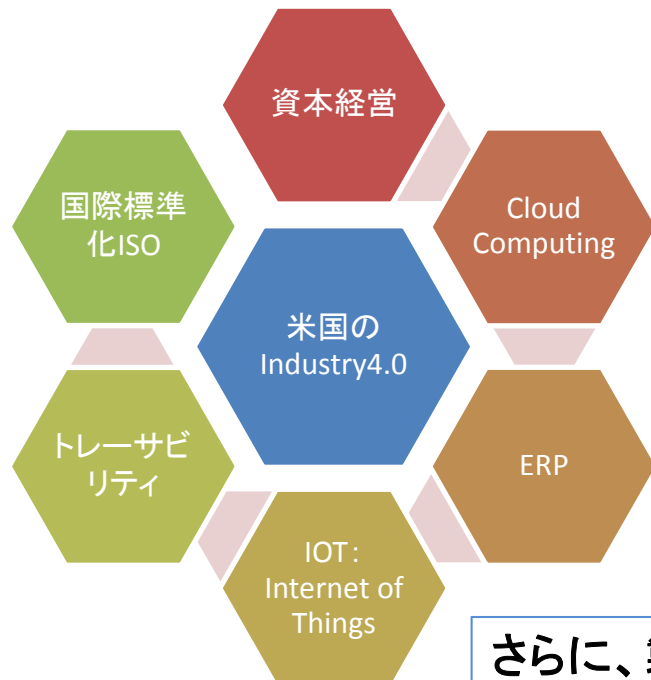
米国のIndustry4.0の特徴：資本経営誘導型

経済回復基調の追い風に、Industry4.0 INDUSTRIAL INTERNETを提唱

- ◆ 金融の健全化：リーマンショック対策
- ◆ 経済対策：金融緩和
- ◆ シェールガス開発（コスト高い）
- ◆ 国内消費回復
- ◆ 自動車向けサブプライムローン
- ◆ サイバー攻撃に強い制御システムへ

製造業をおさえないと雇用のみならずR&Dやデザインやサービスも新興国にとられてしまう危機感

特に、Industry4.0の推進でサイバー攻撃に強い現場づくり設備投資を促す経済効果が期待できる。



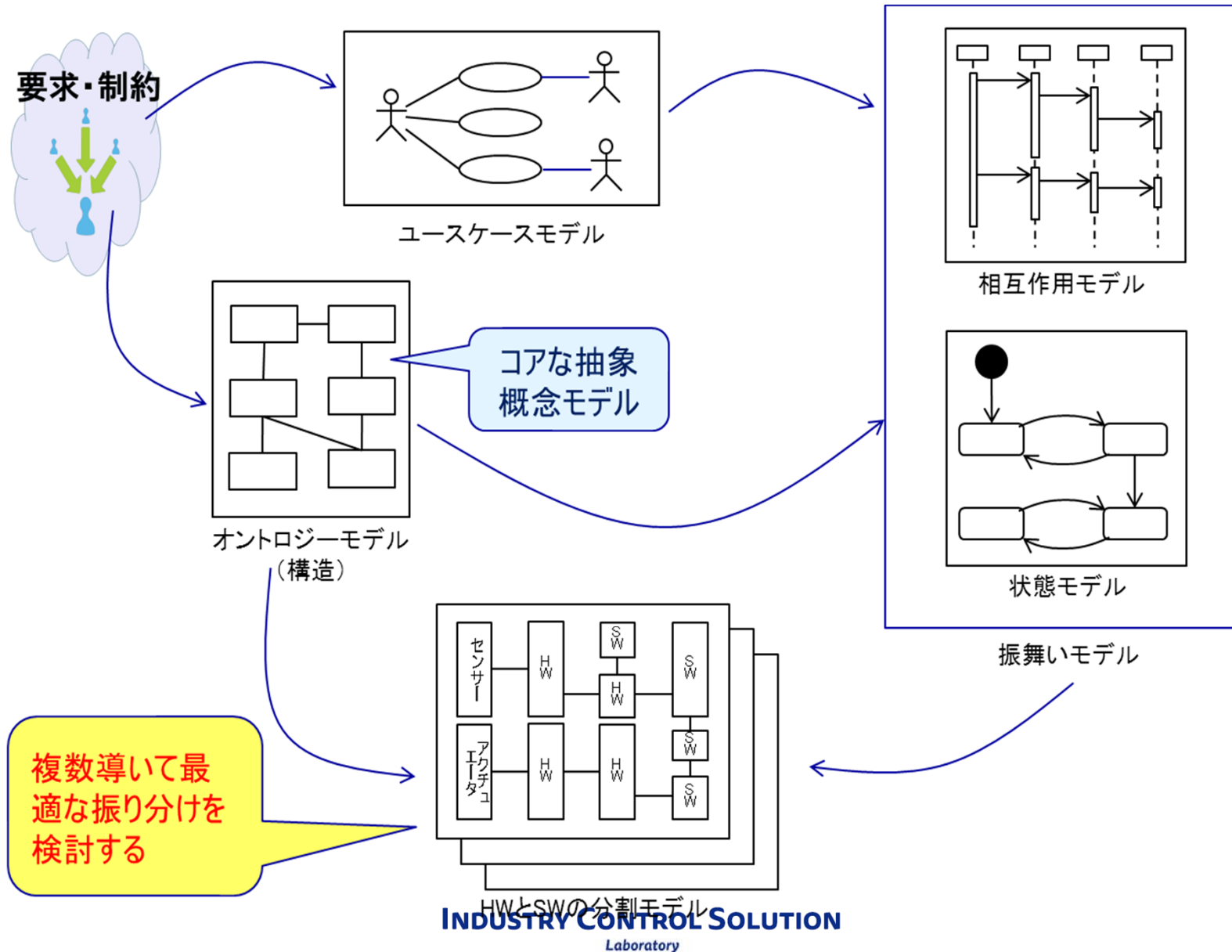
天然ガスのシェールガス生産地となったことで地産地消が低価格で可能となったことや法人税減税や中国経済成長による人件費高騰などで、中国やインドなどにシフトしていた一部の工場が米国内へ回帰した。

オペレーションのオブジェクトをシンボリック化して認識操作重視のオペレーションへ

国内の雇用を確保する

さらに、製造研究機関への支援及び研究開発投資を加速

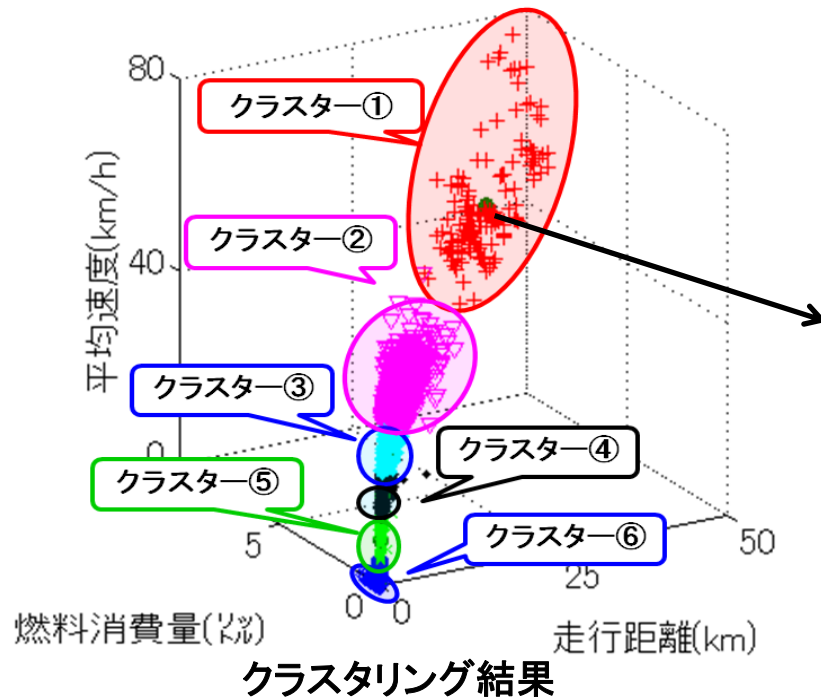
MBSE (Model Based Systems Engineering)



ビッグデータをどう活かすか？

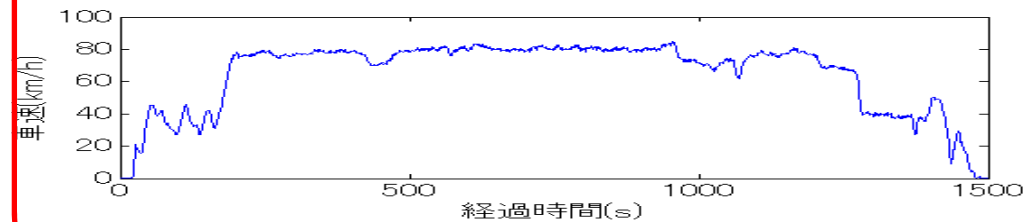
- 制御システム設計の基本は、「余計なことをしない。」。
 - 余計なことは不具合の原因となり、リスクが高くなる。⇒必要なことしかしない。
- ビッグデータで何ができるか？
 - トレーサビリティ
 - 大量の製品の品質情報をクラスタ単位にユビキタス化（消費者・使用者向けの情報公開）
 - アセットマネジメント
 - 部品メーカーが求める交換部品の消耗情報
 - 部品故障の予知保全⇒部品に係る複合データの時間経過を含めた動作傾向の妥当性（AIを使用した予知保全）
 - 製品開発の改善
 - 個別のソフトウェアの実用経歴の見える化⇒無駄なソフト検証
 - 人や車の集合動きに合わせた制御
 - ビル管理や駐車場管理におけるエネルギー制御
 - 交通監視制御でのダイヤ運行計画とリアル対応
 - オリンピックパラリンピックでの人の移動情報管理
 - 振る舞い監視
 - 制御の振る舞い監視
 - 装置の振る舞い監視
 - プラントの振る舞い監視

クラスター(Cluster) : 集合データの特徴を代表するデータ



クラスター①

- 走行距離が長く、平均速度が速い
- 高速道路走行を利用する走行パターン



クラスター①の代表走行パターン

表. 各代表走行パターンのデータ.

	クラスター①	クラスター②	クラスター③	クラスター④	クラスター⑤	クラスター⑥
テスト時間(s)	1500	391	192	116	91	53
テスト距離(km)	26.9	4.23	1.48	0.606	0.243	0.022
燃費(km/ℓ)	6.23	7.72	6.55	4.8	4.37	1.05
各クラスターのデータ数	163	1354	3240	3634	2994	6390

ART (Augmented Reality Technology)

- ART (Augmented Reality Technology) 拡張現実感をもたらす技術
- ユビキタスコンピューティング、ヘッドマウントディスプレイ、センサー情報、画像認識、音声認識、無線通信、クラウドコンピューティング、ユーザーエクスペリエンスなどに、ウェアラブルコンピューティングの技術や3Dホログラム技術が加わり、現実感をもたらしながら、深層部分のコミュニケーションを引き出す技術として注目されている。

用途例

技術伝承

暗黙知を引き出して、暗黙知情報としてデータベース化することで既知情報として再利用できるように整理・分析・整頓して、さらに暗黙知を深化／創造していく技術。

- ARTのRealityとVirtuallyの融合

AHT (Augmented Human Technology)

- 人間の脳が拡張して、脳とコンピュータ／機械が連動した各超現実を造り出す技術
 - 人間の体の一部を機械で補う。(脳からの指令を受ける腕／足)
 - 人間が行けない場所で脳の指示でロボットが作業をする。

人工知能AI

- IBMのワトソンWatson: 質問応答システム、意思決定支援システム
- Microsoftのコルタナ: 支援ツール
- Appleのsiri
- Googleのナウ
- NTTコミュニケーションズのSOINN

Agenda

日本が抱える実状

第四次産業革命“Industry4.0”

サイバー攻撃対策＋“Industry4.1J”

今、何をしなければならないか

Industry4.0は、なぜ、広がらないのか？

- 重要インフラ事業者の制御システムは、インターネットにつながっていない。
 - なぜ、インターネットにつないでいないのか？
 - 制御システムを標的にしたサイバー攻撃が急増 ⇒ 安全のリスクが高くなっている。
- でも、重要インフラ事業者の情報セキュリティ／制御システムセキュリティに対する認識が弱い。
- パーフェクトなモデリング設計を求めたがる。(UNIX的発想)⇒発想が固すぎる。

インターネット経由で制御システムをサイバー攻撃する攻撃者がいる限り、脅威リスクは無くならない。



米国では、制御製品の脆弱性情報管理をするだけでなく、実際に発生したインシデント対応で現場の要請に対応している。

ICS-CERTでまとめた脆弱性情報 “RECAP OF VULNERABILITIES IN 2013”

インシデント報告

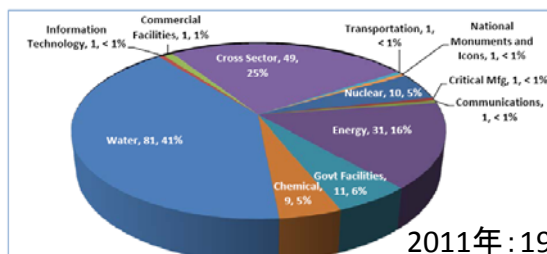


Figure 4. Incident reports by sector (2011).

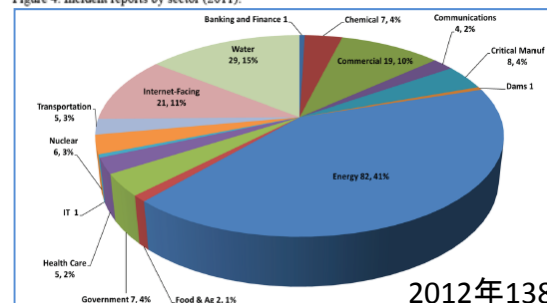
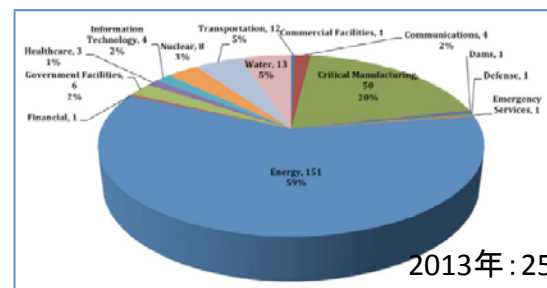


Figure 4. Incidents by Sector – Fiscal Year 2012



制御製品の脆弱性情報管理を実施
アラート: 95件
アドバイザリ: 328件
2014年12月末現在

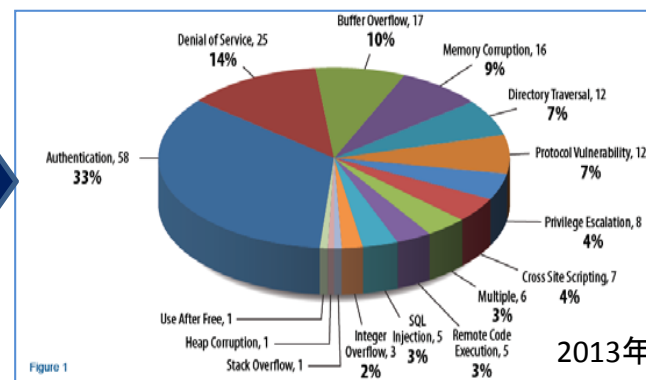


Figure 1

ICS-CERTは、2009年から2014年8月までに418件のアセスメント対応(現場対応出動)をしてきました。

カリフォルニア: 64 アイオワ: 29
フロリダ: 33 ニュージャージー: 27
テキサス: 30 ニューヨーク: 25



インシデント報告と現場出動での対応

計装制御システムエンジニアに、インシデント対応でのマルウェア分析サポートできるスタッフのチームワークで現場をサポート

現場をセキュアにしないとサイバー攻撃にやられるまま。インシデント検知だけでは、同じことの繰り返し。

制御システムのセキュア化

Report of ICS-CERT2014

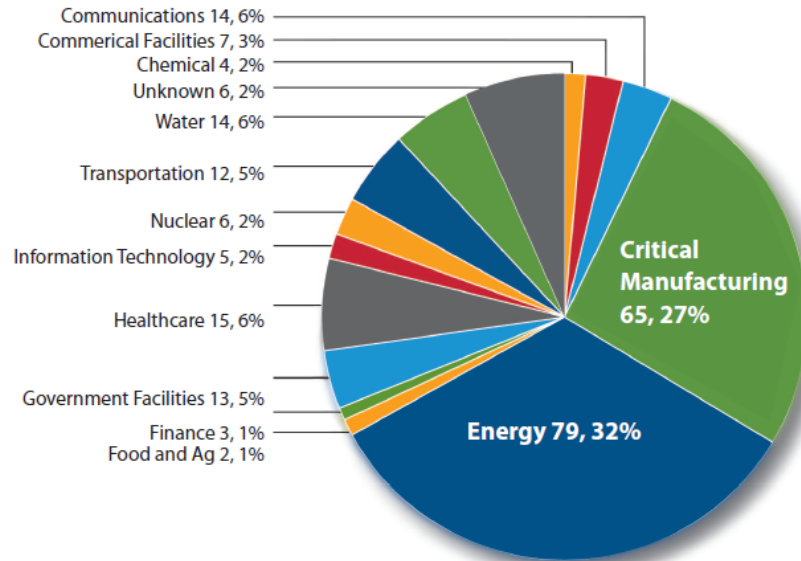


Figure 1. FY 2014 incidents reported by sector (245 total).

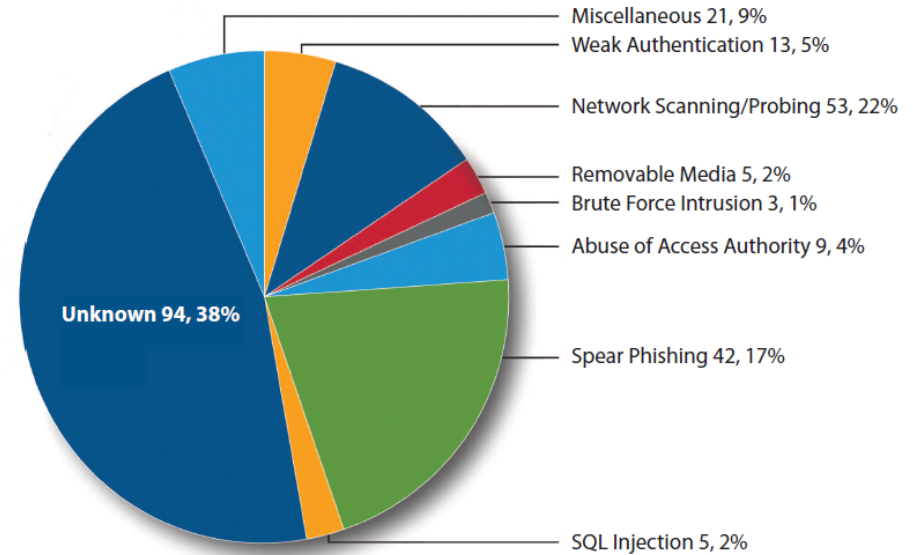


Figure 2. FY 2014 incidents reported by access vector (245 total).

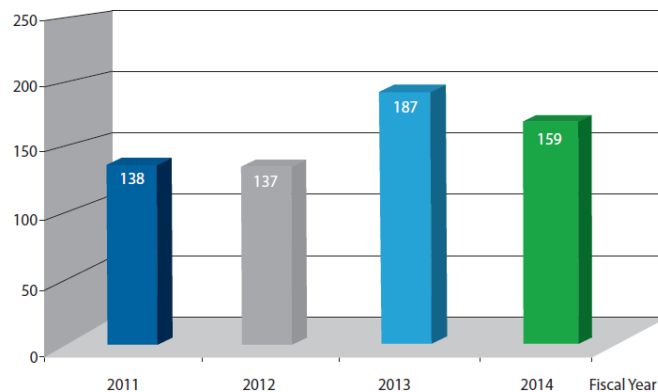


Figure 3. Vulnerability Reports, FY 2011 - 2014.

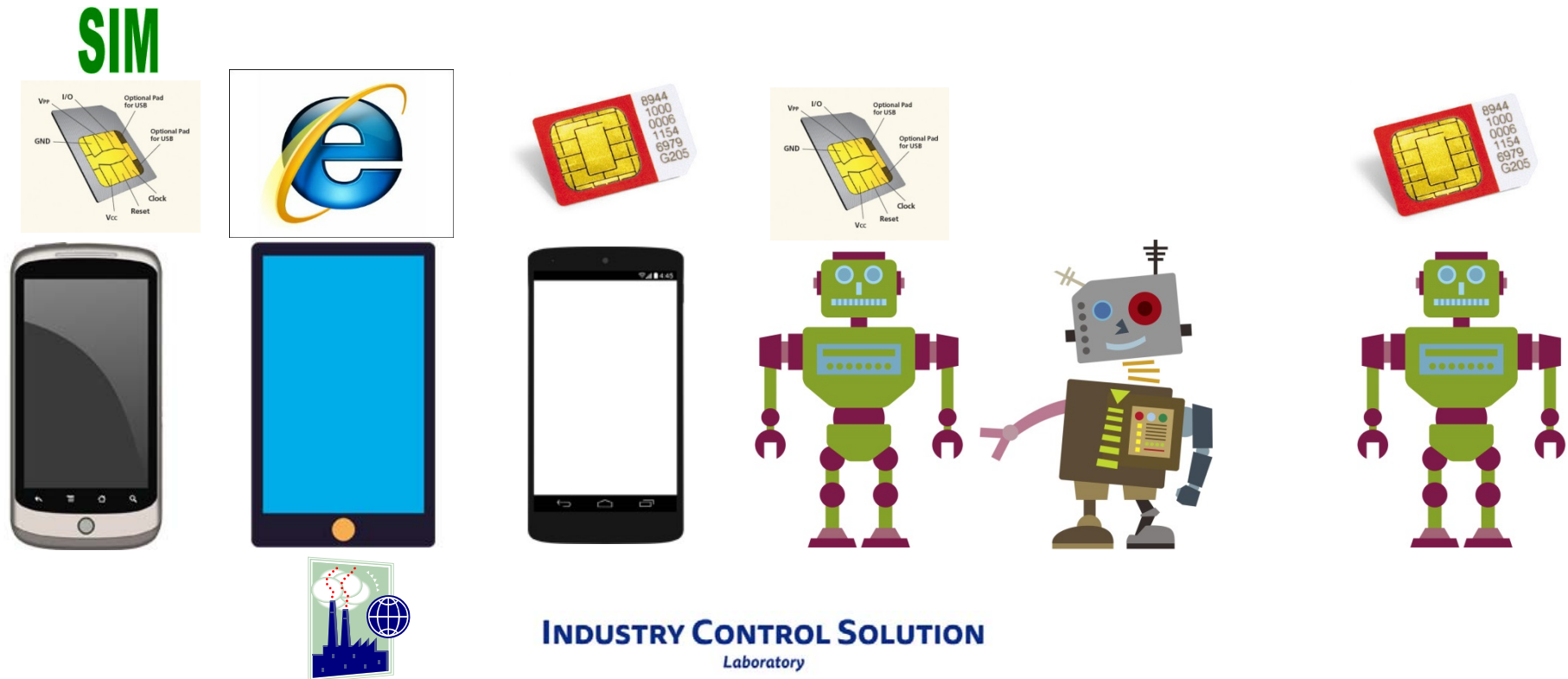
重要インフラ産業へのサイバー攻撃が増えている。
サイバー攻撃技術が高度化している。

- 攻撃手法も高度技術を使用しており、組織的サイバー攻撃武器開発をしていることは明らか。
- 対策を考えるには、攻撃対象、攻撃武器、侵入経路、攻撃内容、被害状況などの具体的情報が必要となる。

	2008	2008	2010	2014	2014
発生場所	USA	トルコ	イラン	ドイツ	韓国
攻撃対象	石油プラント	石油パイプライン	核燃料施設	製鉄所	原子力発電所
攻撃武器	不明 (中国で作られた)	不明	Stuxnet	トロイの木馬	外部操作を可能にしたマルウェア
侵入経路	インターネットから作業用PCに感染	監視カメラの通信ソフト	USBメモリ	電子メールの添付ファイル	インターネットからの侵入
攻撃内容	不明	パイプ管圧への過剰な負荷	遠心分離機への過剰な負荷	溶鉱炉の異常停止	マルウェアを使った遠隔操作
被害状況	爆発炎上	パイプライン爆発	遠心分離機を破壊	生産設備の損傷	実被害なし

スマホ／ロボットが産業スパイに変わる

- 私用のスマホから仕事のスマホへ
 - 勤務登録、業務連絡、作業レポート、行動記録など
- スマホやロボットが、産業スパイになる。
 - マルウェア侵入⇒産業スパイ／妨害・破壊工作員／殺人機
 - インシデント検知機能⇒安全ロック⇒メンテナンス・リセット⇒復旧チェック



情報セキュリティ

IT系

Internet
mobile

通信設備の電力供給システム
通信サーバールームの空調制御システム
電力、水、排気

エンタープライズ系

ERP
SCM
CRM



空調監視制御システム
電源装置
空調機
温調器

組込みシステム

電化製品
携帯電話
情報端末

JEITA
(電子情報技術産業協会)

制御システムセキュリティ

電力、石油、化学、ガス
鉄鋼、樹脂、繊維
交通
医薬品、化粧品
食品、トイレタリ
上下水道、ごみ焼却
半導体製造
自動車製造
防衛産業

JEMIMA
(日本電気計測器工業会)
JEMA
(日本電機工業会)
NECA
(日本電気制御機器工業会)
各工業会団体

重機ベンダ
制御ベンダ
制御装置ベンダ
機械ベンダ
ロボットベンダ
エンジニアリング会社
システムインテグレータ

電機組立会 (計測自動制御学会: 学術団体)

セキュリティ認識レベル目安チェックシート

アセットオーナーの制御システムセキュリティ認識チェックシート例

No.	質問	チェック
1	セキュリティポリシーに制御システムセキュリティ要素が入っていますか？	
2	セキュリティ対策オーナーを任命していますか？	
3	経営会議でセキュリティ対策報告が入っていますか？	
4	生産部門の事業方針にセキュリティ項目がありますか？（リスクアセスメント項目）	
5	生産部門に制御システムセキュリティ対策責任者を任命していますか？	
6	生産製造エリアに入退出管理システムを導入していますか？	
7	生産製造運転室・監視制御室の入退出管理システムを導入していますか？	
8	生産システムは制御システムセキュリティ対策を施していますか？	
9	制御装置や機械やロボットなどは、セキュア仕様制御システムになっていますか？	
10	制御装置や機械は、セキュアな制御製品で構成していますか？	
11	インシデント検知機能はありますか？	
12	制御システムや装置や機械にインシデント対応のログ機能はありますか？	
13	インシデント対応（検知から復旧まで）手順書はありますか？	
14	インシデント対応手順書で復旧作業トレーニングを実施していますか？	
15	インシデント分析の体制を持っていますか？	
16	セキュア改善は、実施していますか？	
17	電子媒体のセキュア管理を実施していますか？	
18	セキュリティ5S運動を実施していますか？	
19	制御装置や機械の発注先（サプライヤ）のセキュア監査を実施していますか？	
20	制御装置や機械の工場立会い試験でセキュア性能検査をしていますか？	
21	購入する制御製品のセキュア性能試験結果検査は実施していますか？	
22	コンピュータ機能を有する設備の定期点検で脆弱性検査は実施していますか？	
23	制御システムネットワークは、セグメント区分やゾーン区分していますか？	
24	スタッフの情報セキュリティ教育は実施していますか？	
25	スタッフの制御システムセキュリティ対策の人材教育を実施していますか？	

チェック項目には、
 やっていない:0
 計画している:1
 準備している:2
 実施している:3
 継続している:4
 で入力してください。

全てできているチェック
 が入って世界基準レベ
 ル(IEC62443)です。

求められるのは
 企業の回復力

セキュリティ認識レベル目安チェックシート

サプライヤの制御システムセキュリティ認識チェックシート例

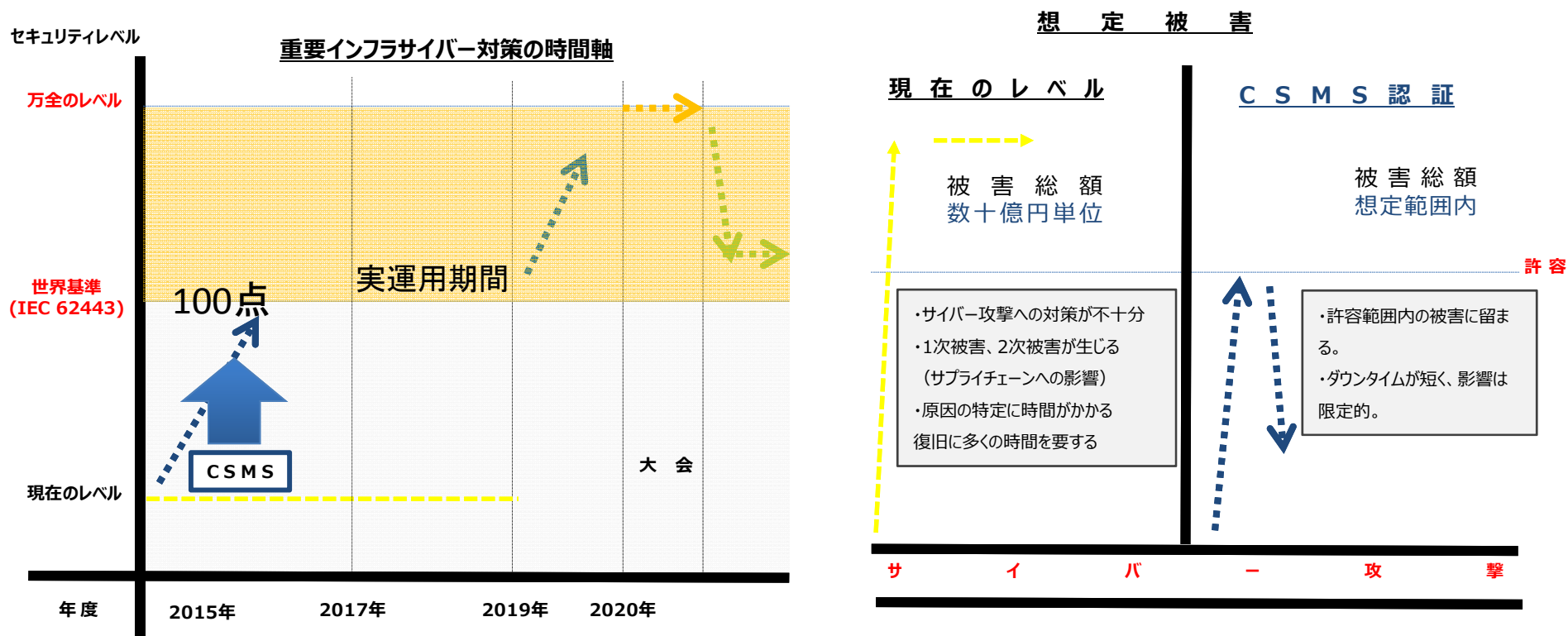
No.	質問	チェック
1	セキュリティポリシーに制御システムセキュリティ要素が入っていますか？	
2	セキュリティ対策オーナーを任命していますか？	
3	経営会議でセキュリティ対策報告が入っていますか？	
4	部門別の事業方針にセキュリティ項目がありますか？	
5	製品開発部門の制御システムセキュリティ対策責任者を任命しているか？	
6	製品開発エリアに入退出管理システムを導入していますか？	
7	製品開発環境の健全性は確保されているか？	
8	製品開発プロセスにセキュア検査があるか？	
9	セキュア試験環境はあるか？(セキュア性能試験ツールは揃っているか？)	
10	セキュア性能検査のツール管理は、できているか？	
11	製造エリアに入退出管理システムを導入していますか？	
12	脆弱性情報管理機能はあるか？	
13	脆弱性情報管理責任者はいるか？	
14	インシデント対応サポート能力は持っているか？	
15	セキュア製品開発基礎研究機能はあるか？	
16	セキュア改善は、実施していますか？	
17	電子媒体のセキュア管理を実施していますか？	
18	セキュリティ5S運動を実施していますか？	
19	部品購入先(サプライヤ)のセキュア監査は実施しているか？	
20	工場の立会試験でセキュア性能試験を実施しているか？	
21	購入するコンピュータ機能を有する部品のセキュア検査は実施しているか？	
22	コンピュータ機能を有する設備の定期点検で脆弱性検査は実施していますか？	
23	生産システムネットワークは、セグメント区分やゾーン区分していますか？	
24	スタッフの情報セキュリティ教育は実施していますか？	
25	スタッフの制御システムセキュリティ対策の人材教育を実施していますか？	

チェック項目には、
 やっていない:0
 計画している:1
 準備している:2
 実施している:3
 継続している:4
 で入力してください。

全てできているチェックが
 入って世界基準レベル
 (IEC62443)です。

求められるの
 は、世界基準
 の企業力

CSMS認証の取得により重要インフラのセキュリティレベルを世界基準まで引き上げ、その後のテストを繰り返す事により万全のレベルに到達させます。万全な状態で2020年を迎えるためには、早期の認証取得をお勧めします。



重要インフラの大半は世界基準のセキュリティレベルを満たしていない。

CSMS 認証

短時間で確実に、重要インフラのサイバー対策を世界基準のレベルまで向上させる。

2017 - 2019 年

世界基準のレベルまでセキュリティテストを繰り返し実施

大会 期間 中

万全のレベルで大会を運営

大会 後

世界基準のセキュリティレベルを維持 (安定運用)

今、事業経営者がすぐに検討すべきこととは？

- 2020年東京オリンピックパラリンピック競技大会までとその後の企業力を見据えた事業中長期経営計画の見直し
 1. セキュアで安全な事業インフラの充実
 2. 強い回復力を持った企業力を身につける
 3. これからを支える企業力を身につける為の人材教育投資計画

「標準化先行のものづくり」⇒“Industry4.0”

「セキュアなモノづくり」⇒“Industry4.1J”

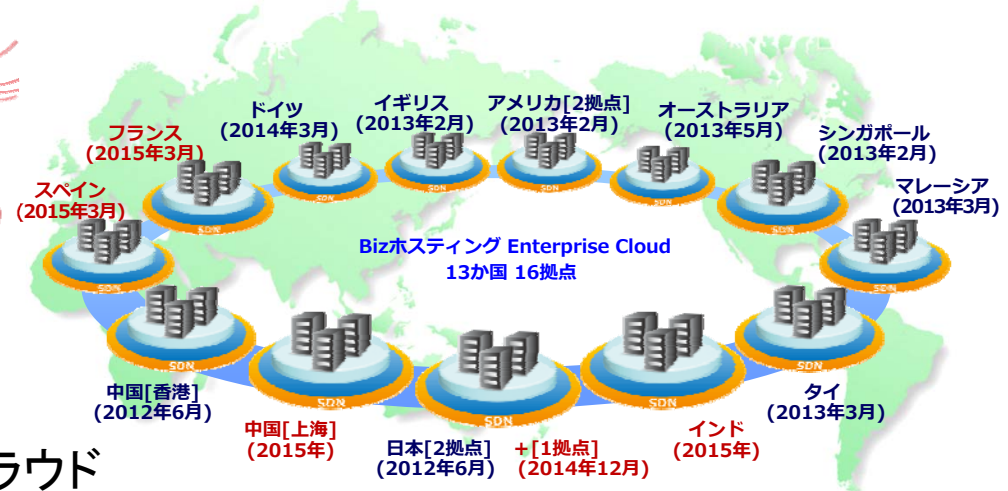
通信インフラがモノづくり世界を変える

- セキュアなモノづくり経営を実現できる条件が揃ってきた。
 - 世界中をつなぐ通信ケーブル
 - 現場に近いプライベートクラウドサーバー群
 - プライベートクラウドにつながるモバイル通信

世界中をつなぐ通信ケーブル



現場に近いプライベートクラウドサーバー群



Internet接続SIM



プライベートクラウド
接続専用SIM

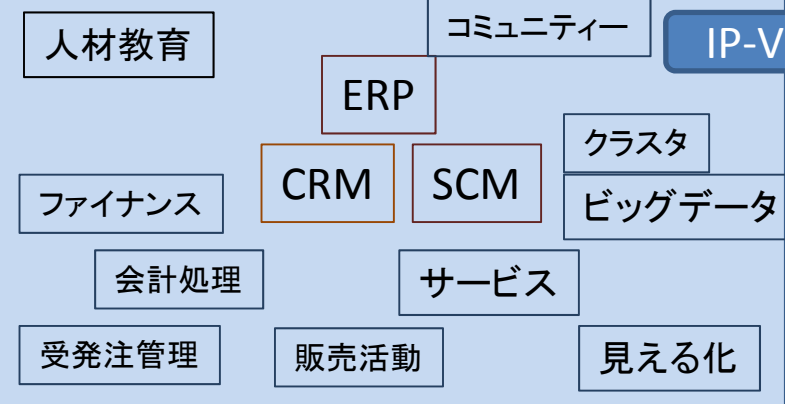


- パブリッククラウドとプライベートクラウドの違い
- OPC UAを使えばパブリッククラウドでもサイバー攻撃は心配しなくて良い訳ではない

パブリッククラウド

主なビジネスドメイン: B to C

リスク承知でインターネットを利用したビジネス



Internet-VPN

Stuxnet Worm SHODAN
Shamoon インターネット
Ransomware Havex

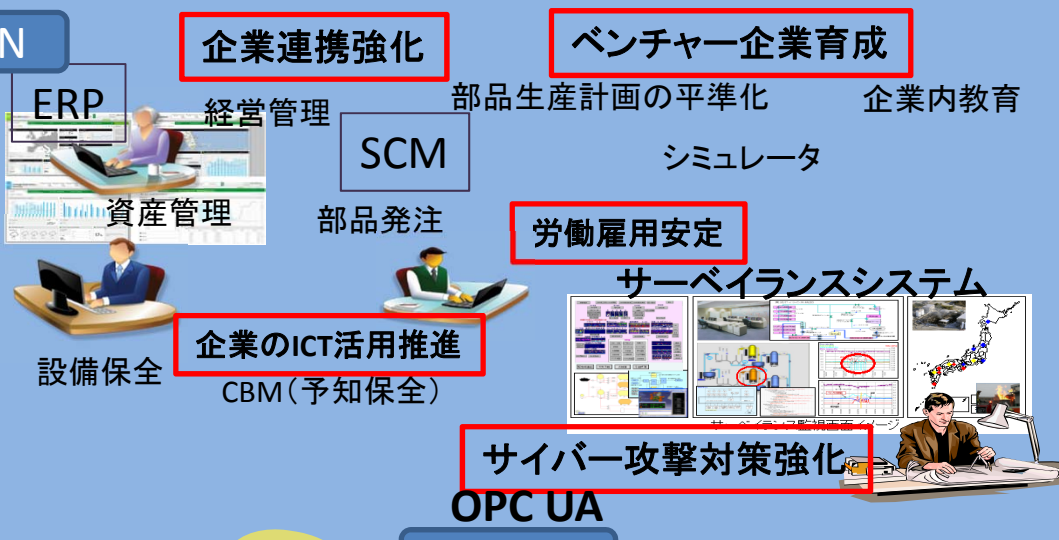
Internet-VPN



プライベートクラウド

主なビジネスドメイン: B to B モデリング連携

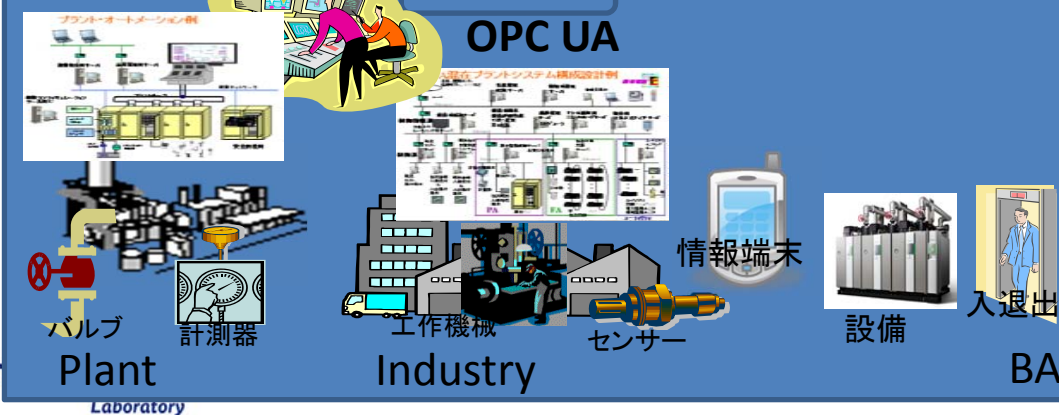
サイバー攻撃を避けてビジネスをしたい企業間ネット



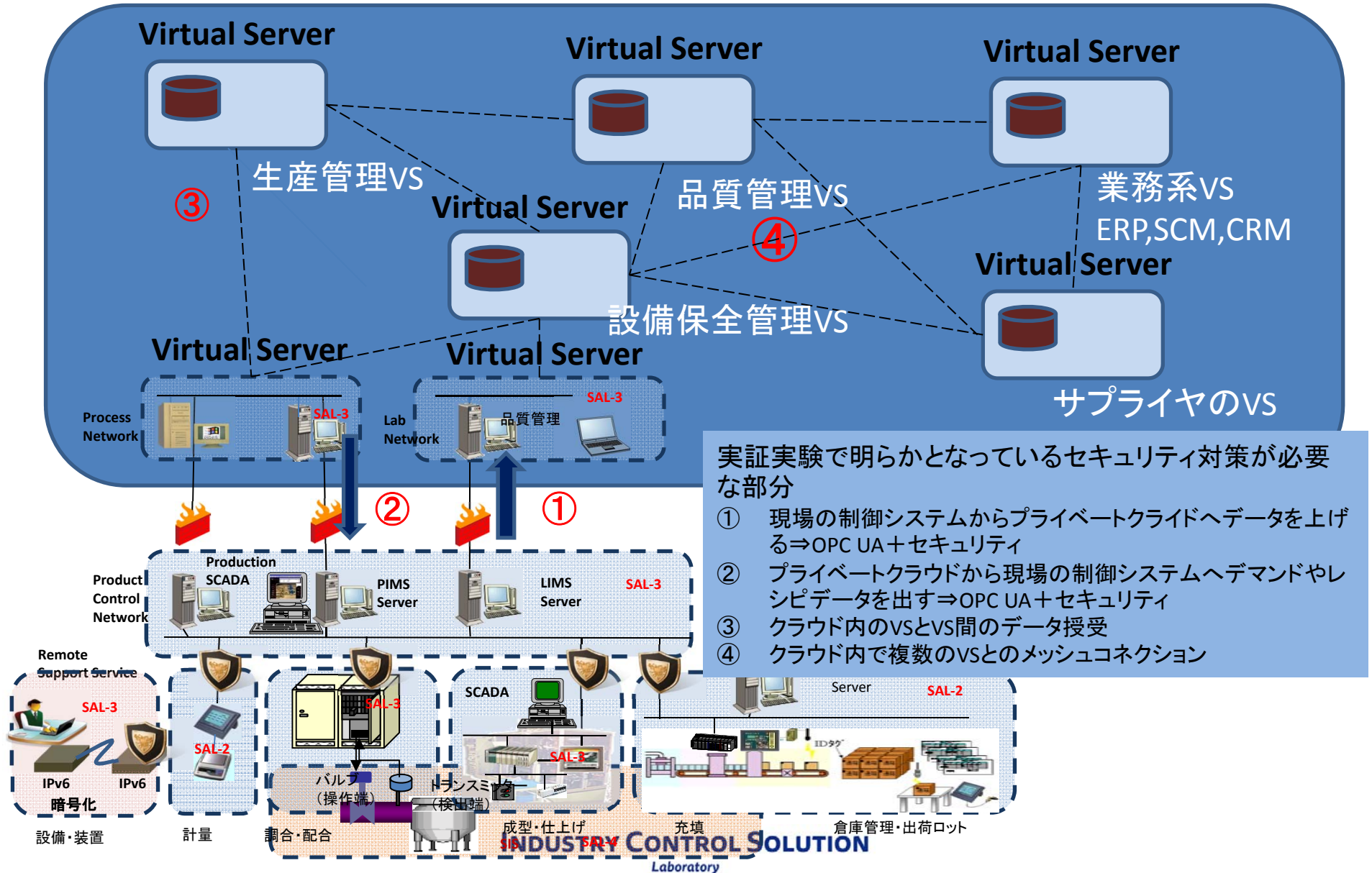
OPC UA

IP-VPN

OPC UA

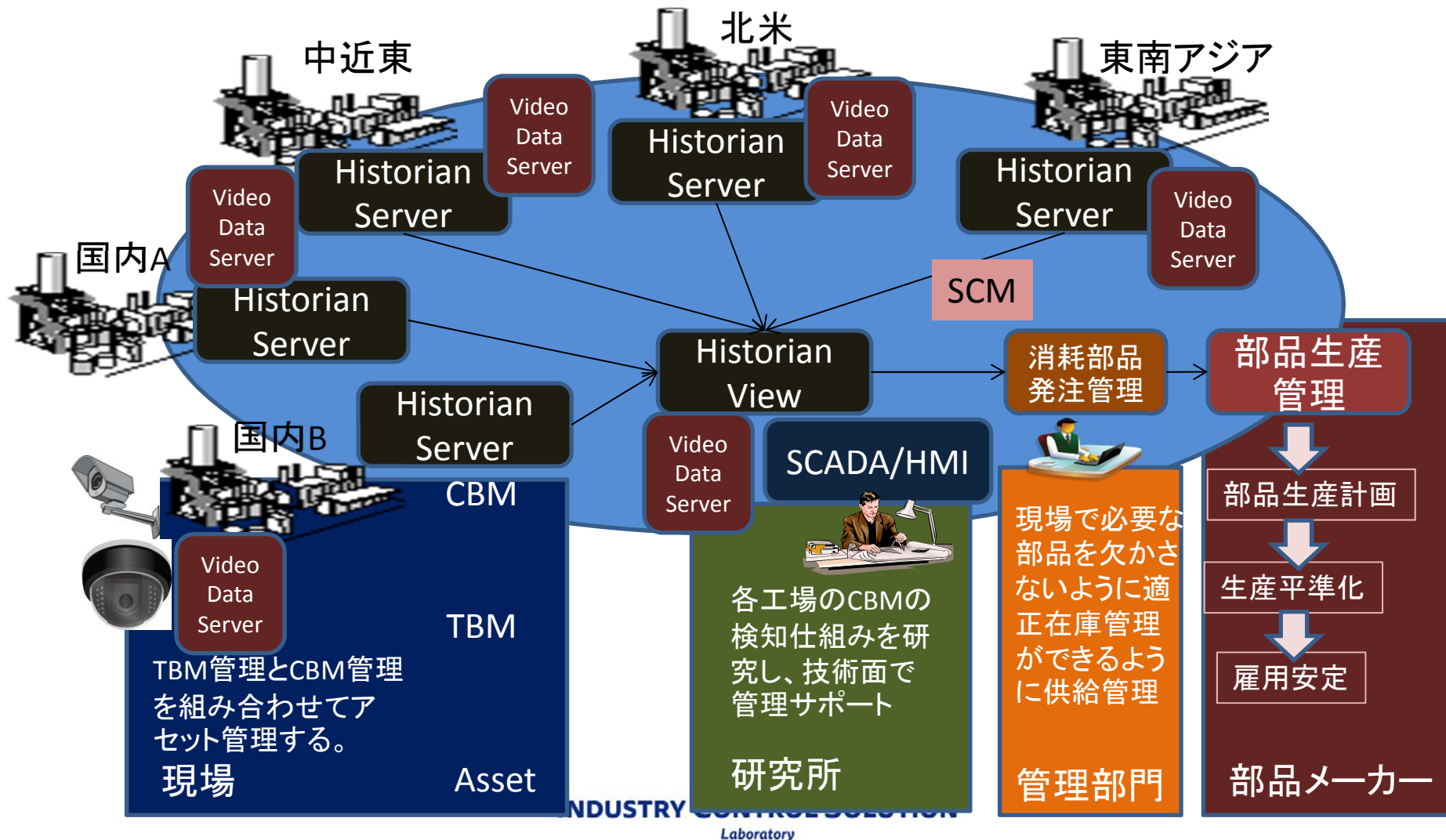


プライベートクラウド内VSのビジネスが急成長する。



世界中の工場や施設の設備保全管理技術支援システム (AMTSS: Asset Management Technology Support System) for User

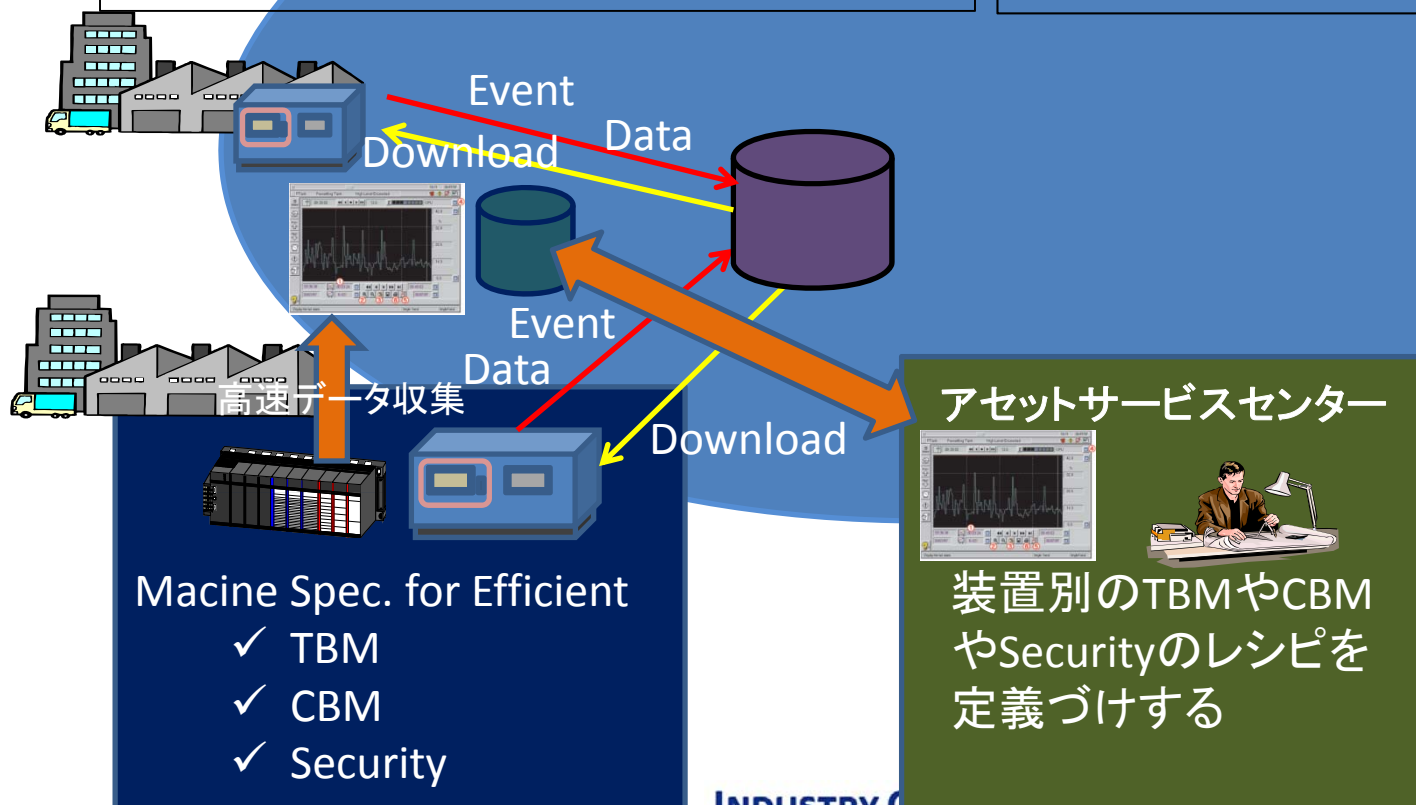
現場ノウハウを活かしたTBMとCBMを組み合わせアセットマネジメントをセキュアに実現できる。



世界中の工場や施設の設備管理技術支援システム (AMTSS: Asset Management Technology Support System) for Vendor リモートサービス (顧客サポート)

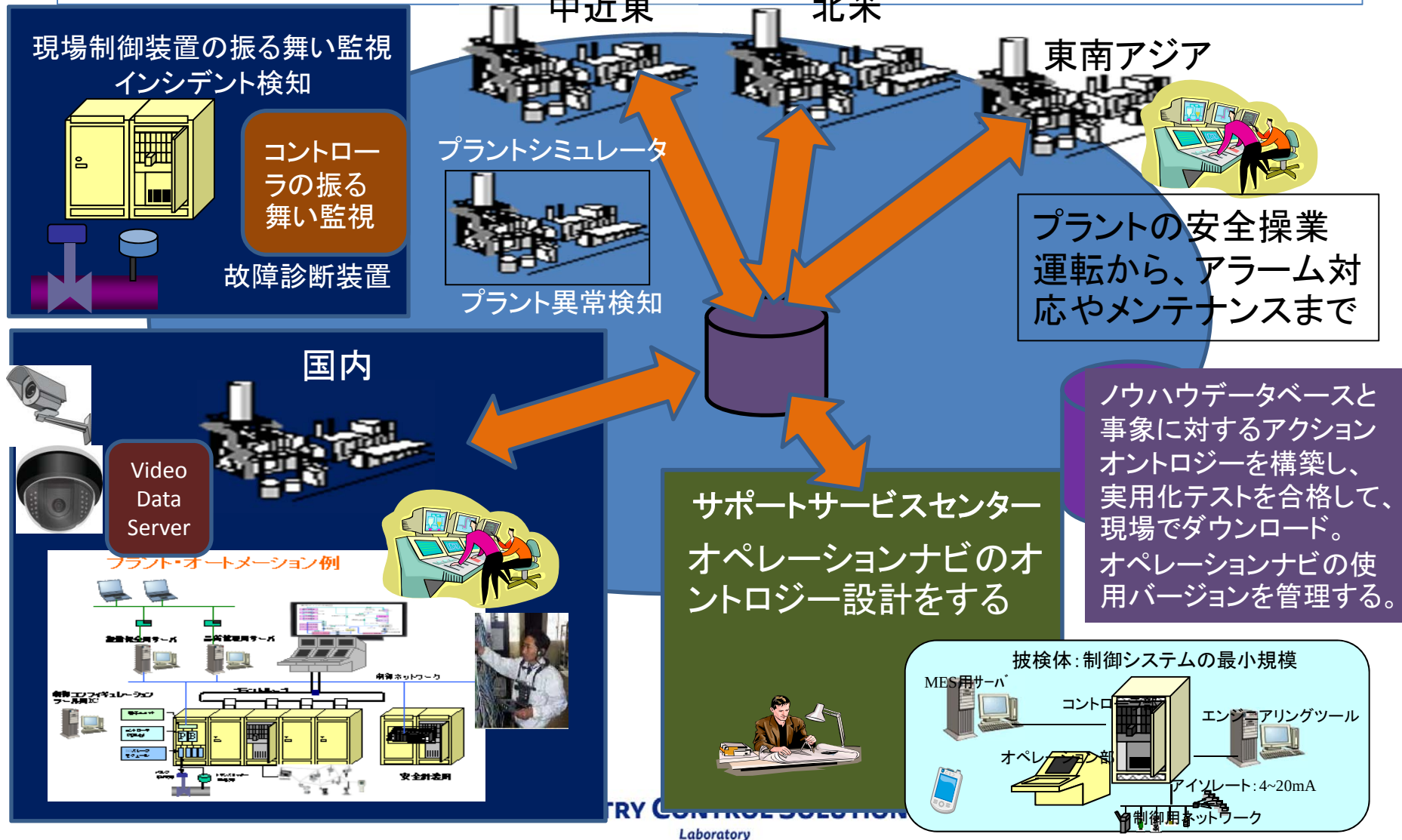
現場の装置や機械に、
TBM (Time Based Management)
CBM (Condition Based Management)
Security
の検知機能を持たせる。

クラウドサーバ側には、
TBMやCBMやSecurityのパラメータ管理
をするデータサーバとアプリケーションを
搭載して、現場の条件でアップデート管理する



- ◆ 安全操業の為の現場オペレーションナビ
- ◆ 熟練者の技術伝承が活かされる現場づくり
- ◆ 振る舞い監視システム

AI(人工知能の活用)



現場エンジニアリングサポート

高度制御を使用する前の確認テスト

シミュレータを利用したプラント制御チューニング事前テスト

シミュレータを利用したオペレーションナビゲーションシステム

セキュアなプライベートクラウドと情報モデル通信プロトコルOPC UAだからこそできる

プラント・オートメーション例

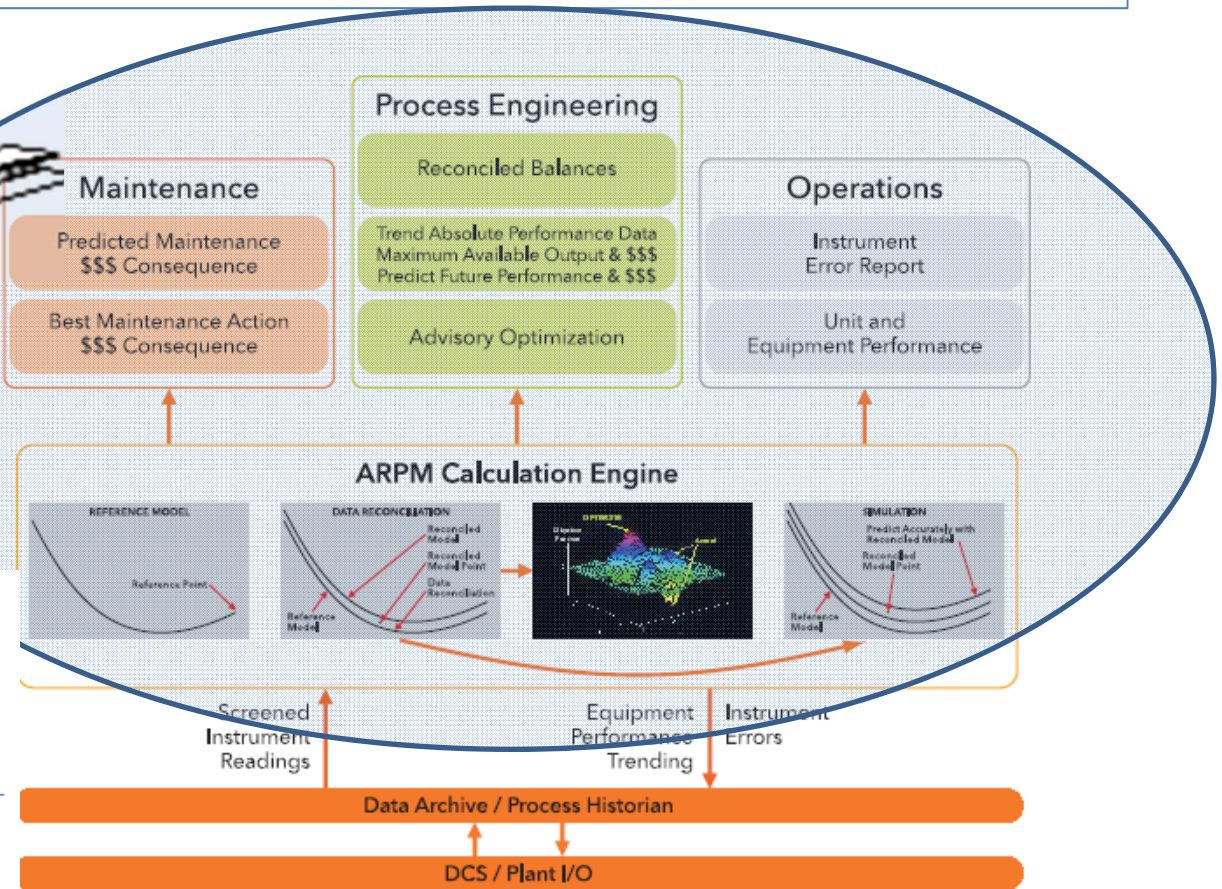
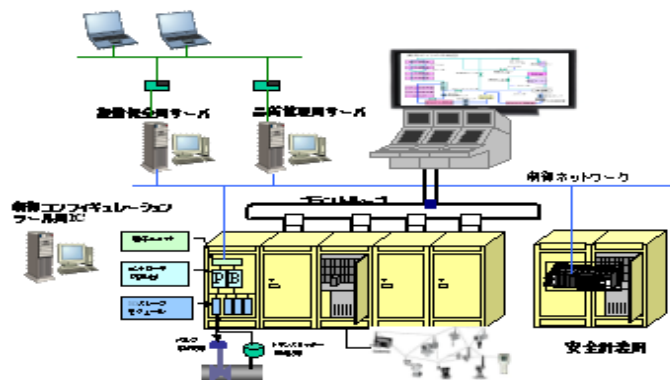
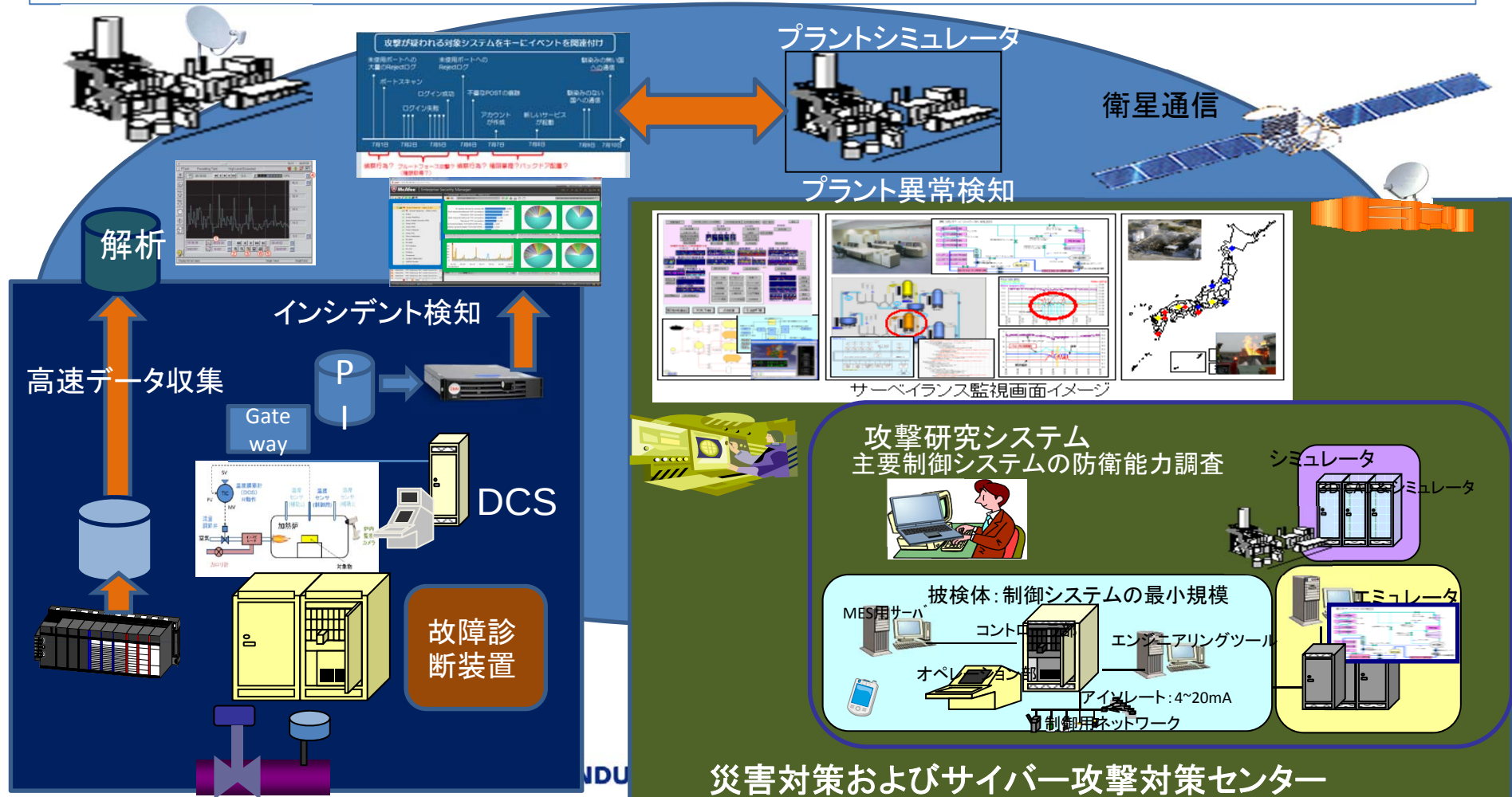


Figure 1: ARPM directly accesses the process and equipment data from the plant historian and extracts performance information

災害対策から、サイバー攻撃までを対処する現場サポート

- ◆ 地震、津波、集中豪雨、火山噴火などの防災対策
- ◆ サイバー攻撃にも強い現場づくり⇒制御システムのセキュア改善
- ◆ 制御システムセキュリティ対策:現場インシデント検知⇒統合監視サーベイランスシステム
- ◆ 現場の制御システムのセキュア化の維持を目的としたセキュア改善研究を行って、現場改善を支援



爆発事故や火災事故発生時のプラントレコーダ

- ◆ プラントの制御モードや制御状況のデータを記録・再生・分析
- ◆ 操作画面の状態や操作ログを記録・再生・分析
- ◆ オペレータの配置や行動のビデオモニタを記録・再生・分析
- ◆ 現場作業や連絡会話の記録・再生・分析

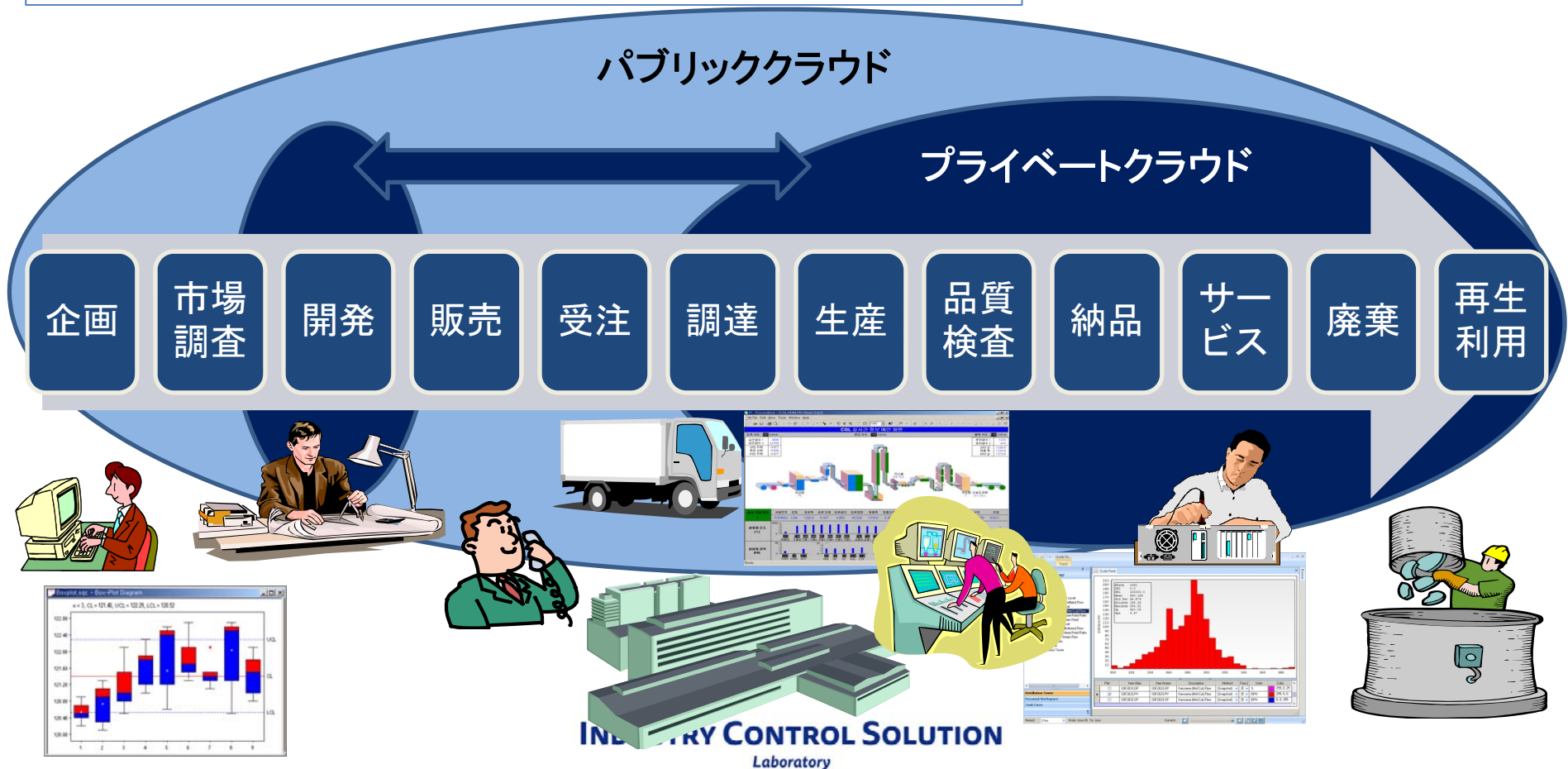
事故発生時のバーチャル再生を行って原因分析が可能な環境整備システム



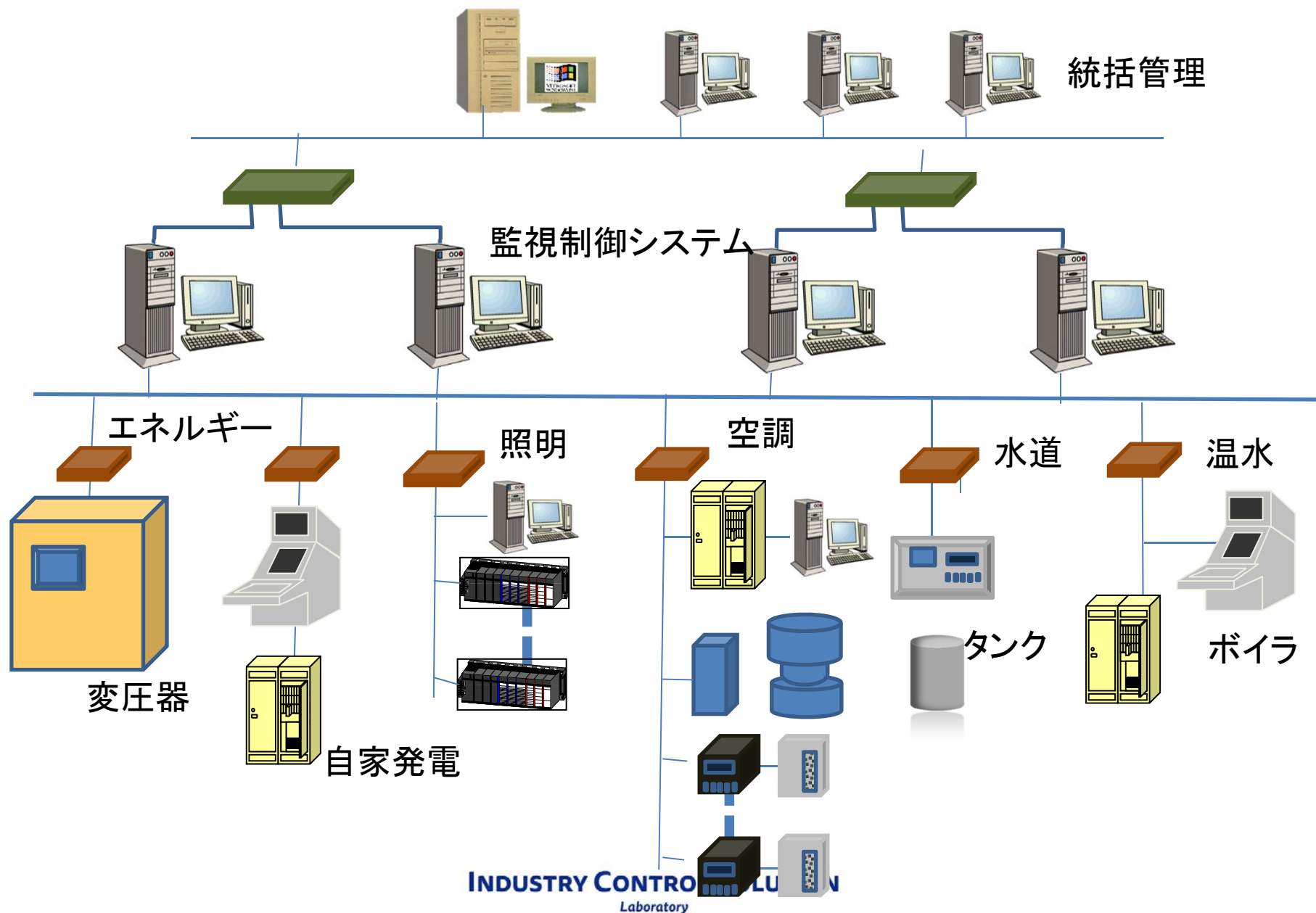
生産している製品のライフサイクルで統括管理

- ◆ 企画から、廃棄、再生利用までを連携させて、トレーサビリティを製品のライフサイクルで事業経営し、顧客への責任を果たす統合管理事業
- ◆ その中で開発から調達、製造、品質検査、サービス、廃棄、再利用までのセキュア性を要求する部分をプライベートクラウドで対応する。

事業経営における活動の中でセキュア性を最も問われる部分の社会的責任を果たすために、事業活動の構造の中でセキュア性を要求する部分にプライベートクラウドを使用する。



ビルオートメーション制御システム例



ビル設備管理では、エネルギー、照明、空調、上下水道、温水、エレベータ、防犯、防災など多項目の制御対象を個別に制御している。それらを統括監視制御で、設備の故障時の対応や火災や災害時などの緊急制御処理やサイバー攻撃を受けた時のインシデント対応を行う。

- ◆ 設備のベンダサービスをインターネットで受けずに、プライベートクラウドで受ける。
- ◆ 時間系列による情報リンク

BACnetやLon worksなどがインターネットに接続している場合は、サイバー攻撃対象になるリスクを抱える。

インシデント検知機能を装備しても、安心できるものではない。インシデント検知機能と制御データを合わせて診て対応シナリオをナビゲートする。

インターネット情報

気象情報

イベント情報

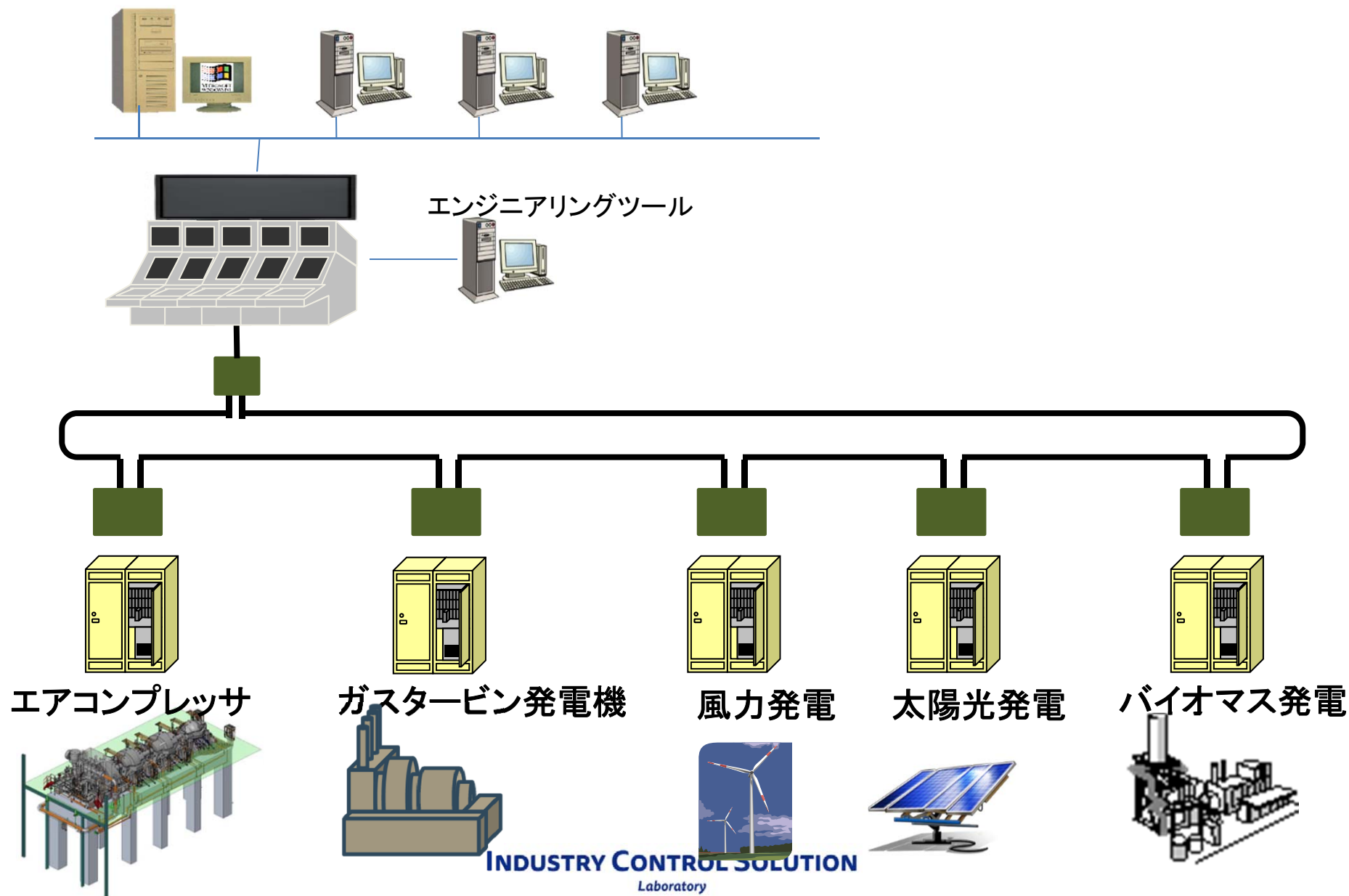
交通情報

緊急地震速報

断水情報



大規模工場ユーティリティ監視制御システム例

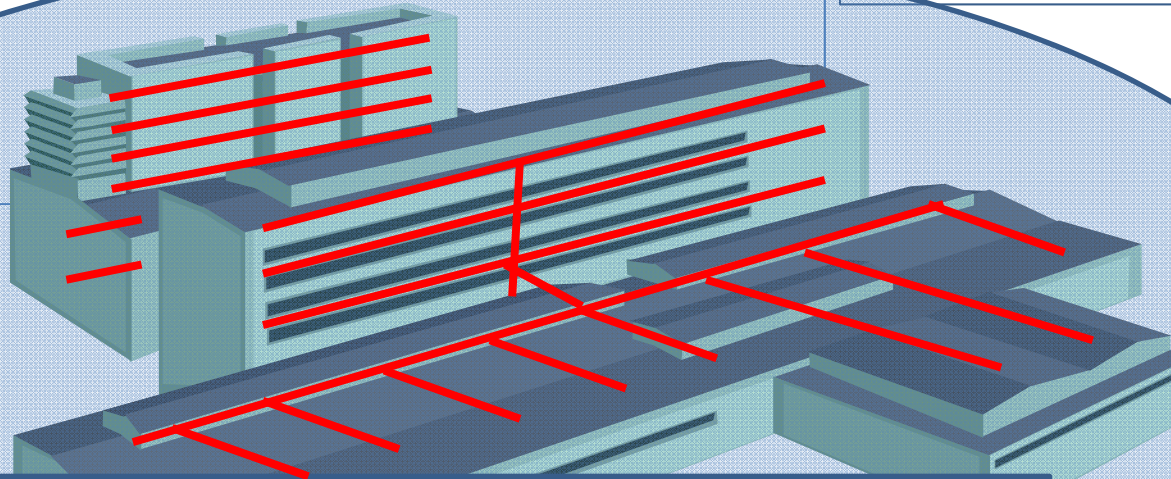


工場のユーティリティ監視

工場内のエネルギー源やエア源から、工場内の幹線ケーブルや主パイプを経てエネルギーやエアを必要とする装置や機械へ供給する。

- ◆ 発電源のエネルギー確保
- ◆ 変圧監視
- ◆ 分電
- ◆ 配電

工場ユーティリティの制御システムをサイバー攻撃から守ることはもちろん、工場内の大元の資源を統括する監視制御システムも、サイバー攻撃から守る必要がある。



エネルギー監視制御



エネルギー源確保の監視制御から供給ラインの変圧や分電／配電を監視制御するシステム



コンプレッサ



ガスタービン



風力発電



太陽光発電



バイオマス発電

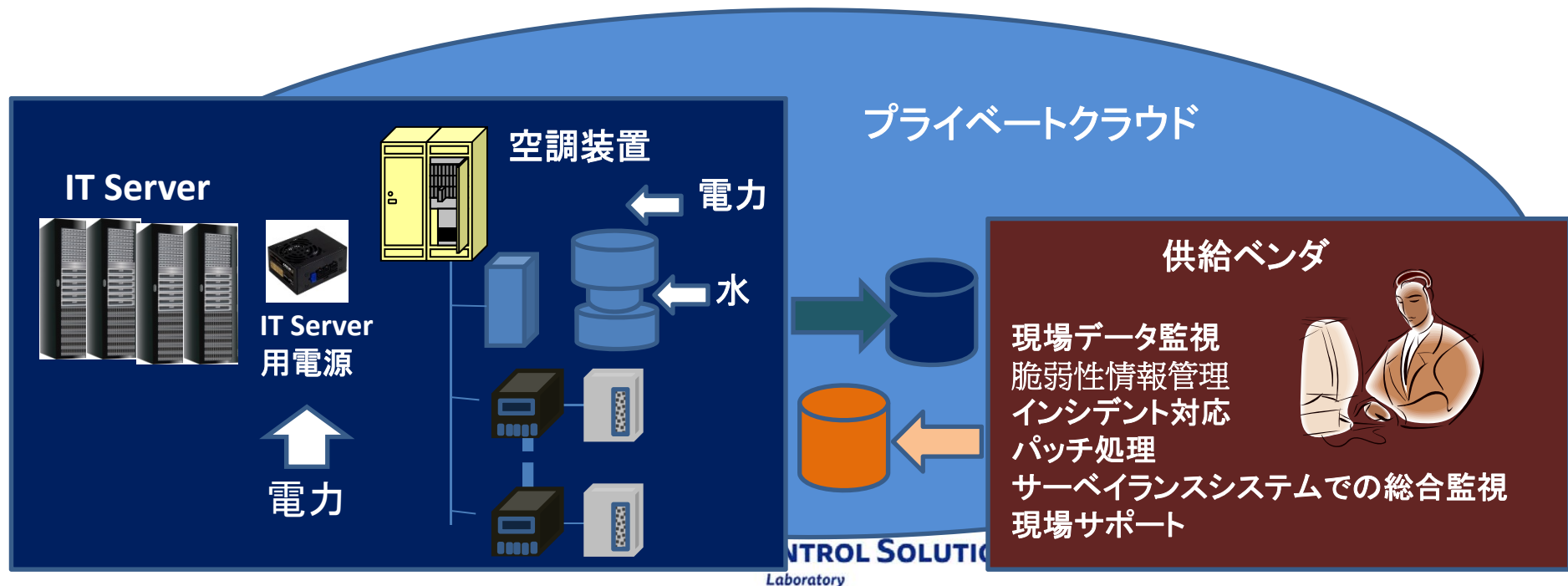
情報セキュリティ対応をしているからIT Serverは安全とは言いきれない。IT Serverをサイバー攻撃するのに、IT Serverを置いている部屋の空調設備を攻撃する方法もある。つまり、IT Serverにも、制御システムセキュリティ対策が必要である。

- ◆ 空調設備を停止させる。
- ◆ 温度設定を高くする。
- ◆ 空調設備の電源をダウンさせる。
- ◆ 空調設備の水の供給を止める。

空調装置の制御システムもセキュア仕様でインシデント検知機能を持つこと。

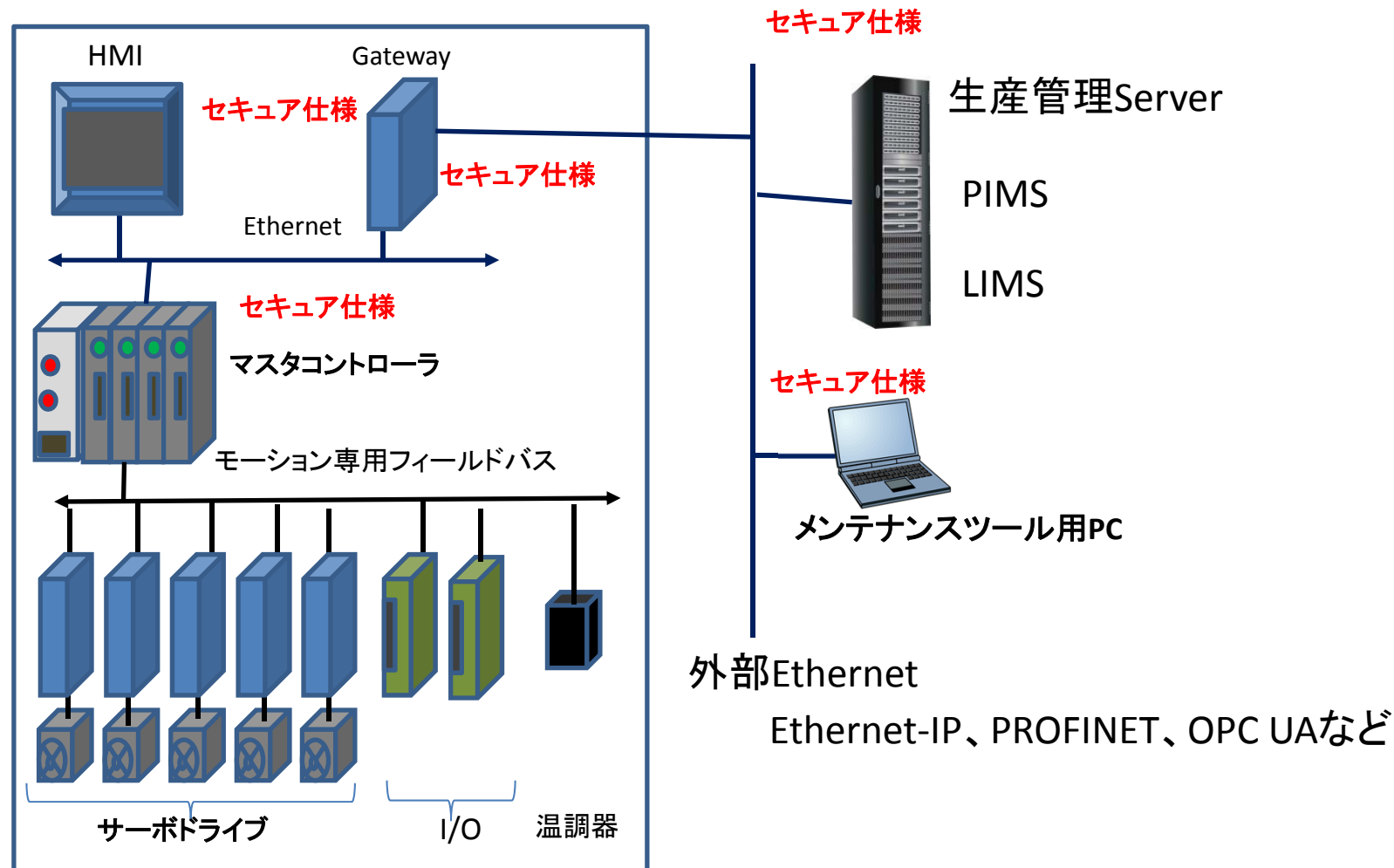
供給ベンダやメンテナンスサービス会社からのサポートは、セキュアなプライベートクラウドを利用した環境が望ましい。

点検時に使用する情報端末やウェアラブルコンピューティングは、インターネットを使用しない無線通信を使用すると良い。



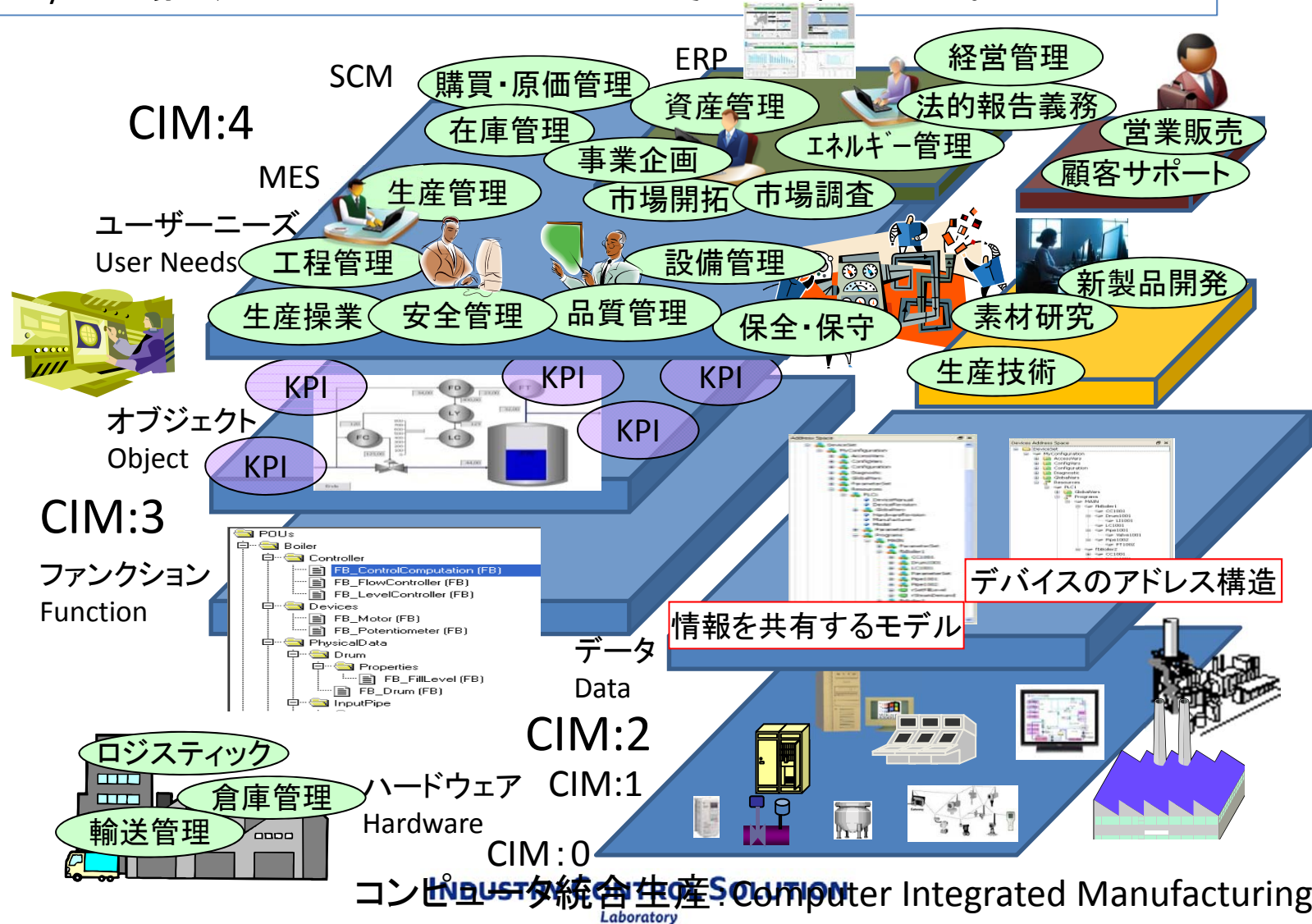
FA系でのモーション制御システム例

- モーション制御では、モーション専用フィールドバス(μsec周期の通信)の制御演算をコントローラが処理しているので、その制御部分は、セキュリティチェックは不可



企業経営情報の構図

20世紀末からは、Computer Integrated Manufacturingは言われてきた。
それをインターネットで実現しようとしてきたが、サイバー攻撃の脅威で停滞していた。
Industry4.0登場で、Common Information Modelの考えが加わってきた。



生産(プロダクション)・品質(クオリティマネジメント)・設備(アセットマネジメント):例

生産計画管理↓	生産業績管理↑	品質管理↑	設備管理↑	設備管理↓↑	エネルギー管理↓↑
生産指示	生産ロットナンバー	生産ロットナンバー	設備登録ナンバー	パッチ処理指示	消費計画電力量
生産ロットナンバー	生産製品型式	生産製品型式	操業時間数	パッチ処理対象設備登録ナンバー	消耗電力量
生産製品型式	生産数量	製品シリアルナンバー／品質管理ナンバー	通電時間数	パッチ処理対象部品ナンバー	操業スケジュール
生産数量	生産損失数量	品質検査結果	アラーム&イベント	パッチソフト登録ナンバー	操業停止指示
部品型式	生産日付	品質検査合格品数	TBM情報	パッチ処理対象ソフト照合・署名確認情報	操業開始指示
生産手順	生産効率	品質検査不合格品数	CBM情報	パッチ処理後の確認情報	操業中断時間積算
仕上げ日付		品質不合格シリアルナンバー	交換該当部品シリアルナンバー		
生産レシピデータダウンロード		品質検査合格率	交換該当部品型式・仕様		

現場の機械／ロボット管理:例

機械ウォームアップ 通信応答確認	機械操業中 モーション制御のμsecの演算処理	機械異常処理 異常原因の分析と被害範囲確認	機械定期点検 通信応答確認、正常確認
センサー正常確認	アラーム処理	修理	リフレッシュ作業
アナログ信号レンジ変換チューニング	加工レシピの指示及びレシピデータの入れ替え	修理後の正常確認	チューニング作業
自己診断結果確認と通知	品質チェック情報のアップ		通信応答確認、正常確認
インシデント検知と処理	上位ネットワークからのインシデント検知と処理		

SCM・トレーサビリティ・CRM・ERP・ファイナンス：例

プライベートクラウド

SCMサプライチェーン	トレーサビリティ	CRM(顧客サポート)	ERP資産管理	ファイナンス(投資戦略)
素材購買(素材使用条件)	製品シリアルナンバー	CRM管理ナンバー	資産管理ナンバー	資産運用種別管理情報
部品購買(調達時間)	生産ロットナンバー	製品シリアルナンバー	設備管理情報	資産評価価格情報
生産に要する時間と条件	製品シリアルナンバー／品質管理ナンバー	取扱い管理情報	資産コスト取扱い管理情報	監査管理ナンバー
ロット単位の消費期限情報	品質検査結果	顧客問い合わせ内容	設備管理ナンバー	監査結果情報
製品シリアルナンバー／ロジスティック情報管理ナンバー	CRM管理ナンバー	回答内容	減価償却種別管理情報ナンバー	管理部門情報
	素材購入元情報管理	対処内容	資産運用種別情報	ファイナンス評価情報
	販売先情報管理	販売ルート情報	エネルギー収益	

工場管理

生産(プロダクション)・品質(クオリティマネジメント)・設備(アセットマネジメント)

生産計画管理 ↓ 生産指示 生産ロットナンバー	生産業績管理 ↑ 生産ロットナンバー 生産製品型式	品質管理 ↑ 生産ロットナンバー 生産製品型式	設備管理 ↑ 設備登録ナンバー 稼働時間数	設備管理 ↓ バッチ処理指示 バッチ処理対象設備登録 ナンバー バッチ処理対象部品ナン バー バッチソフト登録ナンバー バッチ処理対象ソフト照 合・署名確認情報 バッチ処理後の確認情報
生産製品型式	生産数量	品質検査結果	通電時間数	
生産数量	生産損失数量	品質検査合格品数	アラーム & イベント	
部品型式	生産日付	品質検査不合格品数	TBM情報	
生産手順	生産効率	品質不合格シリアルナン バー	CBM情報	
仕上げ日付		品質検査合格率	交換該当部品シリアルナン バー 交換該当部品型式・仕様	

現場の機械／ロボット管理

機械ウォームアップ 通信応答確認	機械稼働中 モーション制御のμsecの 演算処理	機械異常処理 異常原因の分析と被害 範囲確認	機械定期点検 通信応答確認、正常確 認
センサー正常確認 アナログ信号レンジ変換 チューニング	アラーム処理 上位ネットワークからのイ ンシデント検知と処理	修理 修理後の正常確認	リフレッシュ作業 チューニング作業
自己診断結果確認と通知			通信応答確認、正常確 認
インシデント検知と処理			

現場の機械／ロボット管理

機械ウォームアップ 通信応答確認	機械稼働中 モーション制御のμsecの 演算処理	機械異常処理 異常原因の分析と被害 範囲確認	機械定期点検 通信応答確認、正常確 認
センサー正常確認 アナログ信号レンジ変換 チューニング	アラーム処理 上位ネットワークからのイ ンシデント検知と処理	修理 修理後の正常確認	リフレッシュ作業 チューニング作業
自己診断結果確認と通知			通信応答確認、正常確 認
インシデント検知と処理			

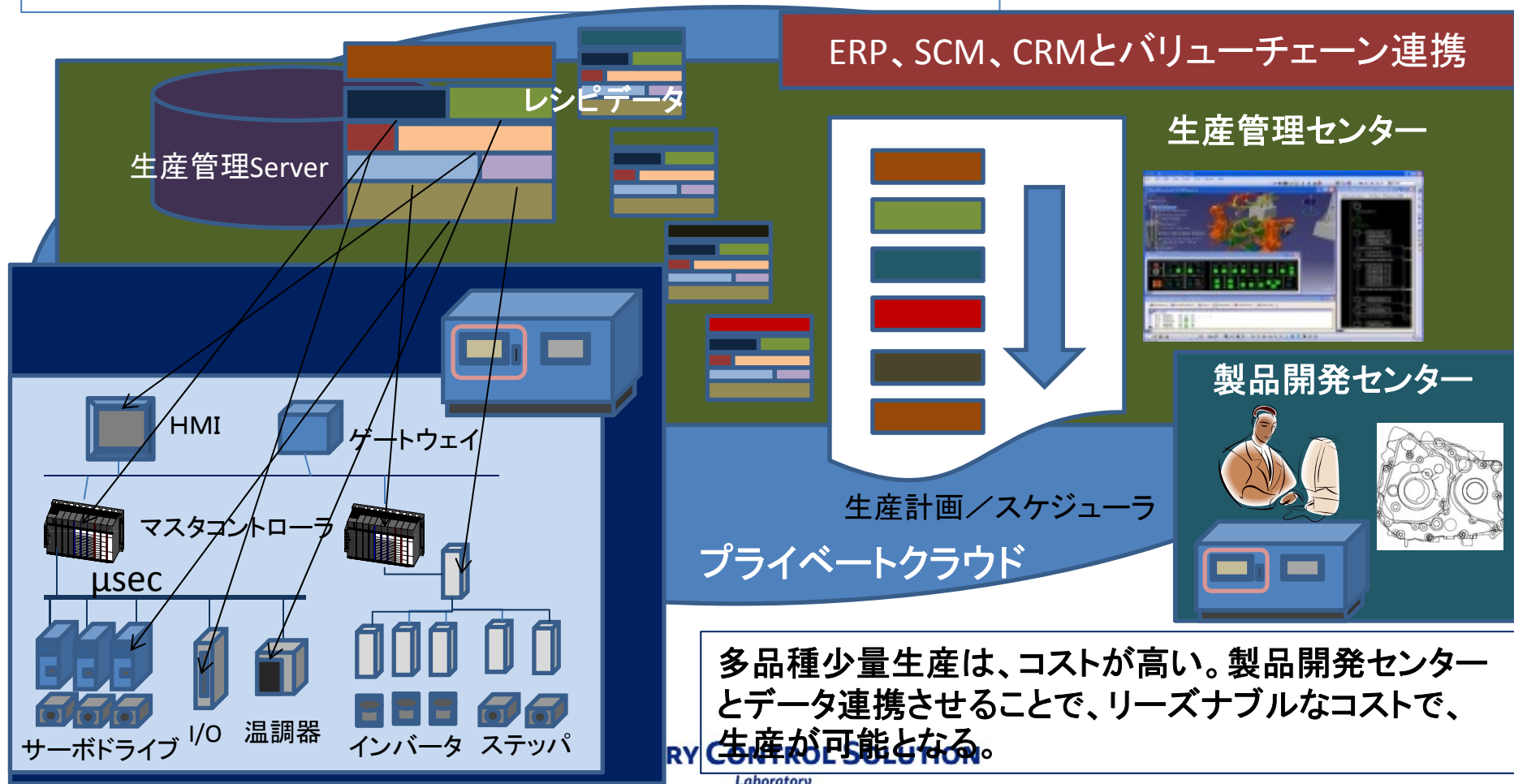
現場の機械／ロボット管理

機械ウォームアップ 通信応答確認	機械稼働中 モーション制御のμsecの 演算処理	機械異常処理 異常原因の分析と被害 範囲確認	機械定期点検 通信応答確認、正常確 認
センサー正常確認 アナログ信号レンジ変換 チューニング	アラーム処理 上位ネットワークからのイ ンシデント検知と処理	修理 修理後の正常確認	リフレッシュ作業 チューニング作業
自己診断結果確認と通知			通信応答確認、正常確 認
インシデント検知と処理			

工場の中の機械(モーション制御)やロボットを使った多品種少量生産方式を実現する。

- ◆ 生産する製品タグごとに加工レシピを入れ替え
- ◆ マルチモーション／マルチコントローラ／マルチロボット
- ◆ Function Blockを入れ替え
- ◆ PLM、PIMS、LIMSをセキュアなプライベートクラウドで実現

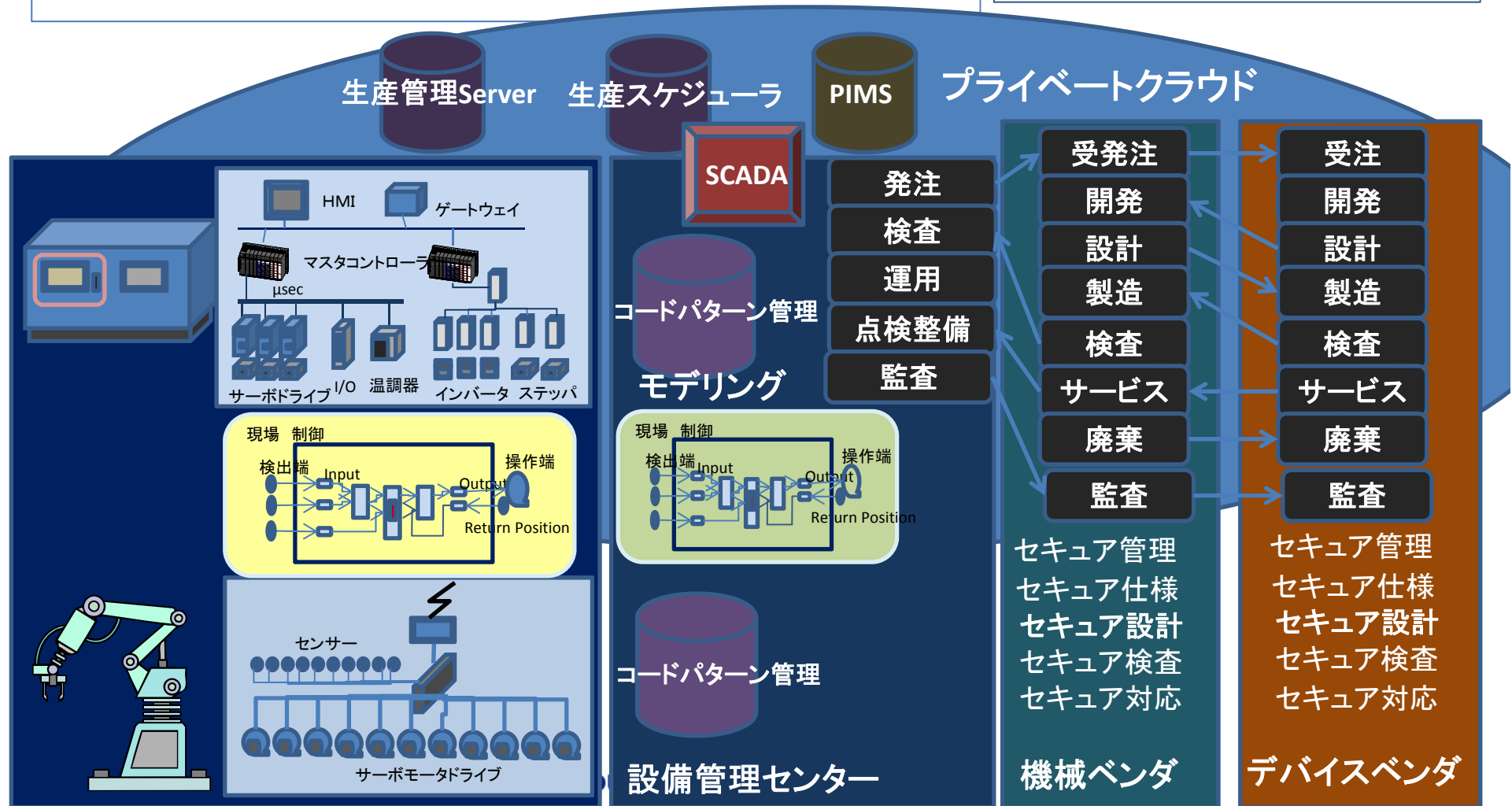
制御コントローラのFB(Function Block)の内容であるモデリングを切り替えることで、生産する製品のレシピを切り替える。これにより、マルチモーション加工が可能になる。



工場の中の機械やロボットのライフサイクルを支える機械の部品デバイスのソフト管理

- ◆ 属性モデリング定義
- ◆ セキュア五原則(管理／仕様／設計／検査／対応)

セキュア五原則を実施しながら、協業連携を構築する。
その連携環境もライフサイクルをベースとしたセキュア連携が求められる。



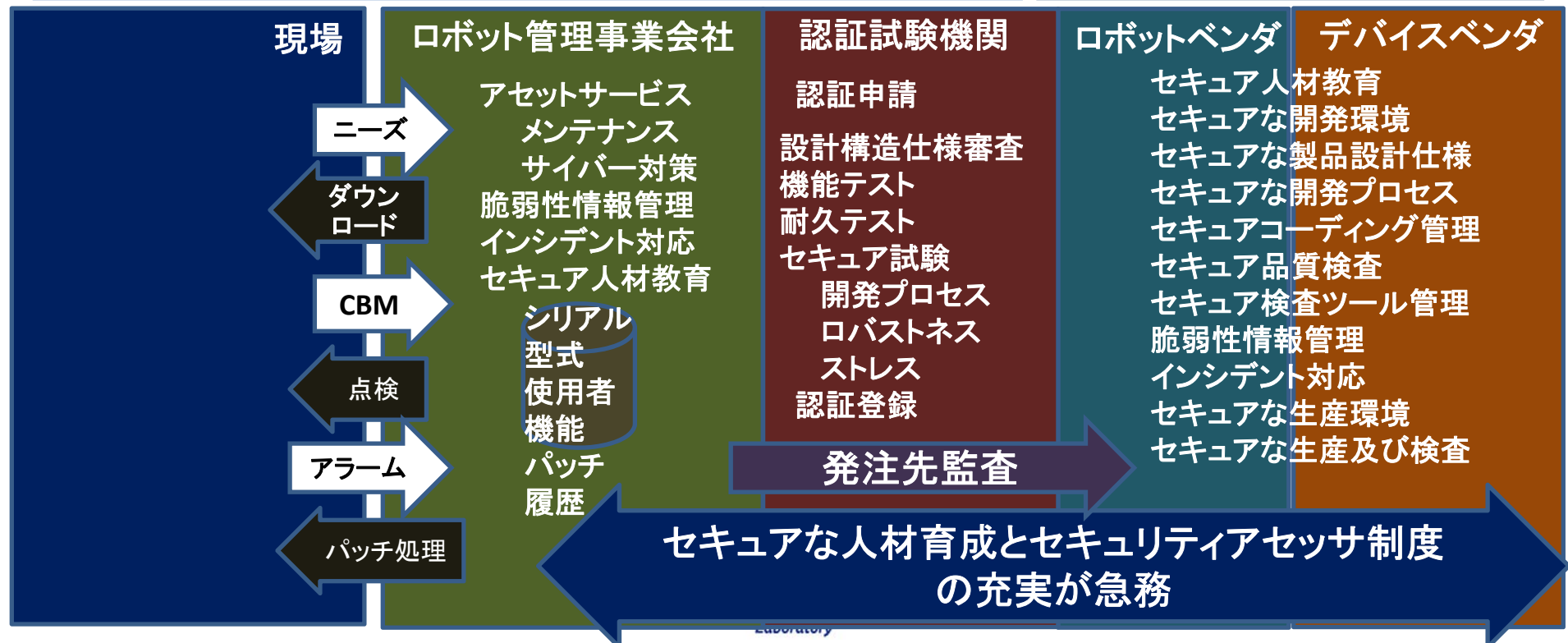
人の生活を支えるロボットのライフサイクル管理や脆弱性対策を設計段階から考慮した、セキュアで安全なロボット共存社会づくりのインフラ整備

- ◆ 使用目的: 介護、家政婦、危険作業、災害時の救助・救難・救命、パートナー(生活協同者)、癒し系、警備、防衛兵器
- ◆ 目的別の機能入れ替え／定期点検／修理／復旧
 - アセット／メンテナンス／サイバー対策

安全確保のプライベートクラウド利用

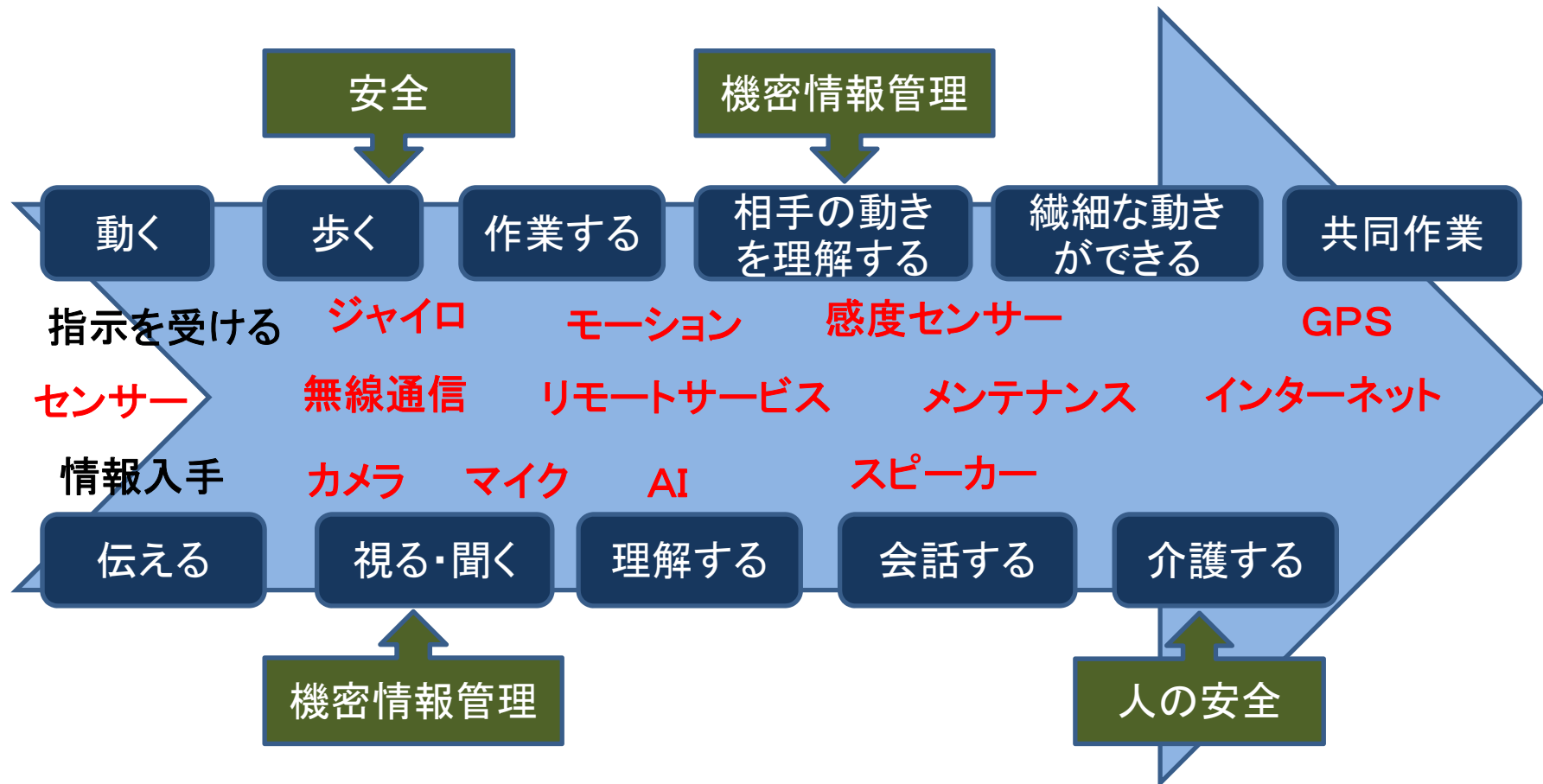
SIMカードを利用してインターネットを経由しないでプライベートクラウドに接続

制御コントローラのFB(Function Block)切り替え／参照機能が、目的別の機能入れ替えや定期点検や修理を実現し、セキュア強化を可能にする一方、機能仕様を悪用したサイバー攻撃で乗っ取りや暴走や停止ができる。人を傷つけず安全に作業。インターネットを使わないでアセットメンテナンスを実施。



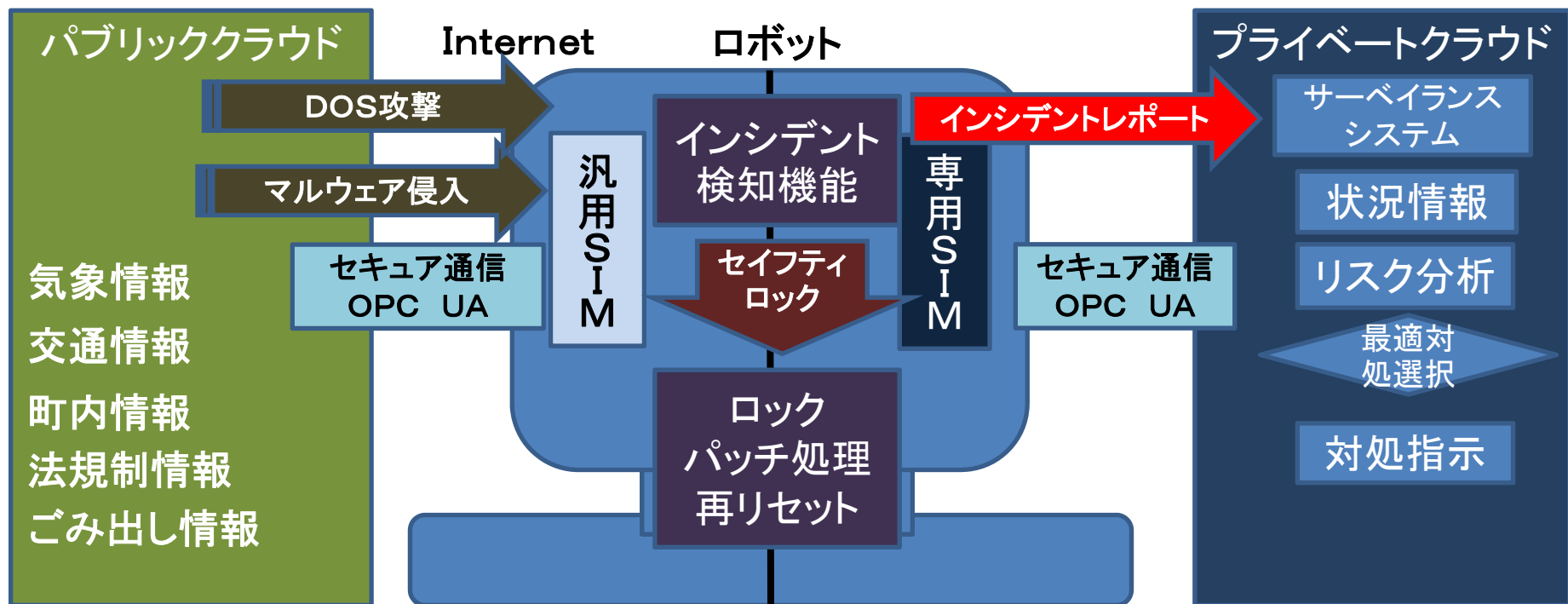
ロボットが持つサイバー脅威？

ロボットが進化することで、製品開発の企画段階から安全性とセキュア性が重要となる。アセットサービスやメンテナンスやパッチ処理を安全に実施できることが求められる。ライフサイクルレベルでセキュアで安全なロボットであることを認証することが求められる。



セキュアなロボット仕様

- インシデントが発生した場合、ロボットと周辺の状態がどのような危険状況にあるのかを確認して、その状況に合った対処方法を選択していかなければならない。
- 緊急対処(セーフティロック)はロボットの中で行う。
- 緊急対処後のアセットやメンテナンスは、対処方針や対処方法やパッチ処理や再リセット対処は、多くのデータベースやAIなどを使用する為に、セキュアなプライベートクラウドと連携で実施。



防衛産業では、開発から製造ライン、現場サポートなどの環境は、サイバー攻撃のリスクが高いインターネットの利用を避ける。

セキュアな製造ラインで生産する。

セキュアな工作機械を使用する。

セキュアなメンテナンスを実施する。

プライベートクラウドとウェアブルコンピュータの利用

外部からのPCや電子媒体の持ち込み禁止

セキュアなサーバー管理

セキュアに関する人材教育

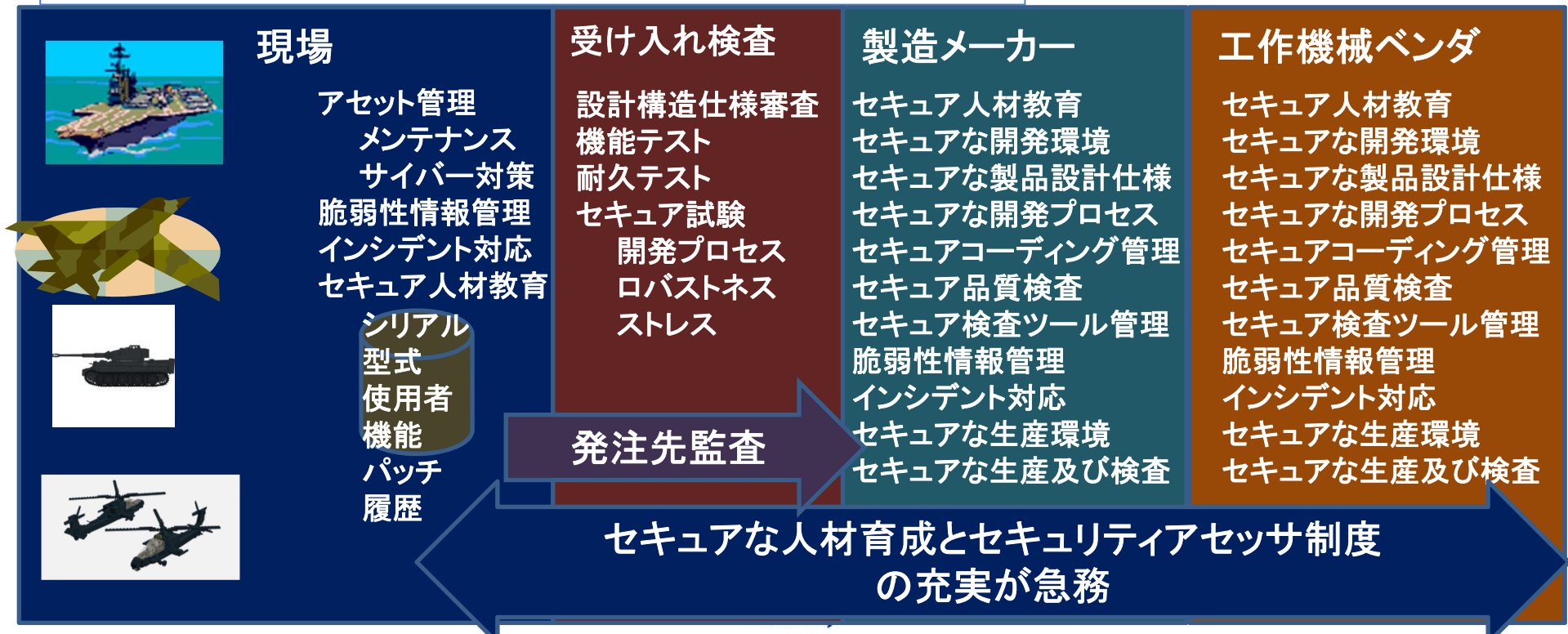
制御システムセキュリティ対策の具体的な人材教育を実施

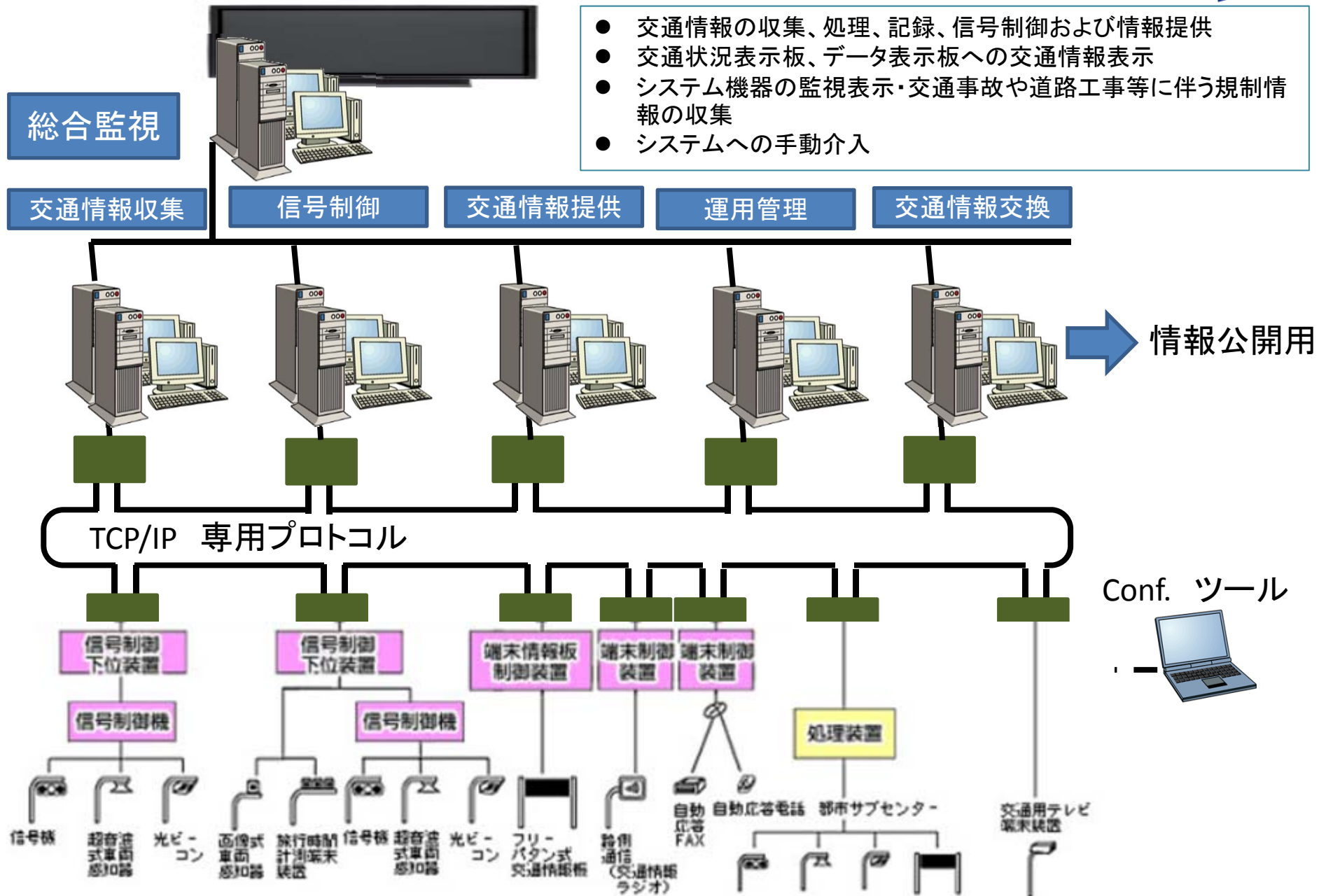
機密情報を扱うことから、計画的に自社内の人材をセキュア教育して継続的にサプライできる体制づくり。

制御システムセキュリティ対策の徹底。

管理されたプライベートクラウドの活用。

セキュアな通信プロトコル仕様を標準採用する。



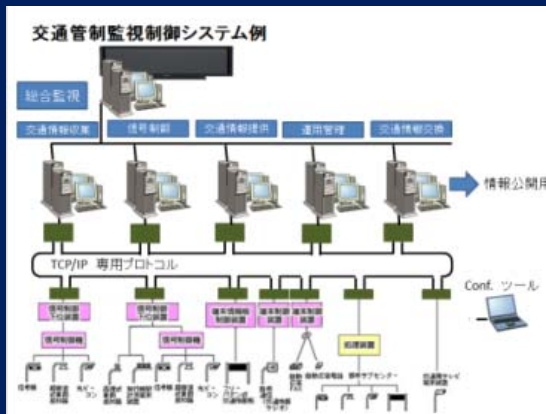


交通管制システムにおける設備故障や車両事故やサイバー攻撃による機能停止は、大事故やパニックを引き起こし、社会的問題は大きい。

- ◆ 高速道路管制システム
- ◆ 車両幹線施設管制システム
- ◆ 航空機・空港管制システム
- ◆ 港湾設備監視制御システム
- ◆ 一般交通管制システム

設備の安全操業を基本に、TBM／CBMを含め、制御システムセキュリティ対策を基本とする管理レベルを取り入れていく。
CSMS認証、SSA認証、EDSA認証
災害時の対策と同じく、復旧対処
情報セキュリティ(制御システムセキュリティ含む)を強化・管理・改善していく。

交通管制システム



設備管理センター

アセット管理
メンテナンス
サイバー対策
脆弱性情報管理
インシデント対応
セキュア人材教育

シリアル
型式
使用者
機能
パッチ
履歴

受け入れ検査

設計構造仕様審査
機能テスト
耐久テスト
セキュア試験
開発プロセス
ロバストネス
ストレス

発注先監査

サプライヤー

セキュア人材教育
セキュアな開発環境
セキュアな製品設計仕様
セキュアな開発プロセス
セキュアコーディング管理
セキュア品質検査
セキュア検査ツール管理
脆弱性情報管理
インシデント対応
セキュアな生産環境
セキュアな生産及び検査

セキュアな人材育成とセキュリティアセスメント制度
の充実が急務

イベント開催公共施設：東京オリンピックパラリンピック大会／
冬季オリンピックパラリンピック大会、スポーツイベント開催

- ◆ 入退出ゲート
- ◆ 発券システム
- ◆ 空調設備
- ◆ 照明システム
- ◆ 放送施設

重要インフラの安定供給が基本
電力、上下水道、交通、通信、物流



BACnetやLon worksなどがインター
ネットに接続している場合は、サイ
バー攻撃対象になるリスクを抱える。
設備の安全操業を基本に、TBM／
CBMを含め、制御システムセキュリ
ティ対策を基本とする管理レベルを
取り入れていく。
CSMS認証、SSA認証、EDSA認証
災害時の対策と同じく、復旧対応

インターネット情報
気象情報
イベント情報
交通情報
緊急地震速報
断水情報

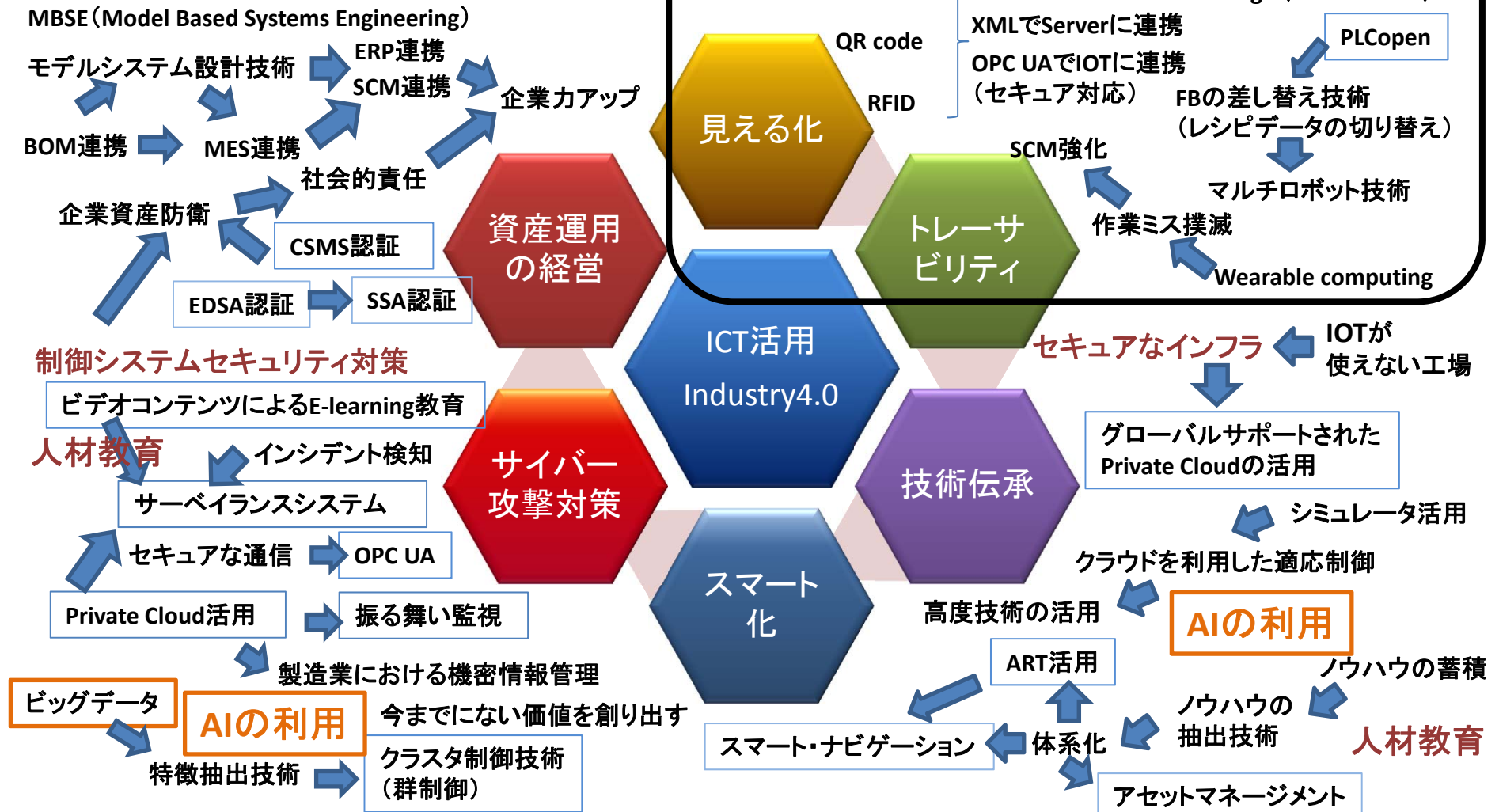


産業技術進歩から見たICT活用 Industry4.1J

制御システムセキュリティ対策無しには実現できない。

セキュアで成長するモノづくり革新

サイバー攻撃の脅威
Stuxnet Worm
Ransomware
Havex SHODAN



セキュアな現場の制御システムがあつてのIndustryの未来

Agenda

日本が抱える実状

第四次産業革命“Industry4.0”

サイバー攻撃対策＋“Industry4.1J”

今、何をしなければならないか

制御システムセキュリティ対策 e-learning教育ビデオ講座



制御システムセキュリティ対策 eラーニングサービス

ご登録されている企業従業員の
方は、こちらからログインして
ください。

パスワードをお忘れの方

ログイン

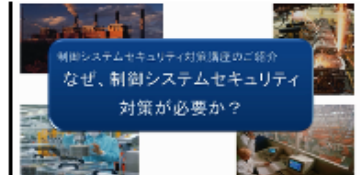


制御システムセキュリティ対策で
お悩みの方におすすめ!!

総講座数は充実の100講座以上!
場所を気にせず制御システムセキュリティ教育が可能

- ✓ 動画と解説資料で学習
- ✓ パソコン・タブレット・スマホで
いつでも・どこでも気軽に受講
- ✓ 理解度テストで研修の効果を見える化

なぜセキュリティ対策が必要か...
こちらをご覧ください▶



制御システムセキュリティ対策講座のご紹介
なぜ、制御システムセキュリティ
対策が必要か？

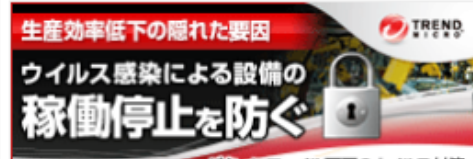


制御システム・セキュリティ
Achilles
EDSA 認証に賛して ISCI により承認を受けているツール

広告



制御システム・セキュリティ
Achilles
EDSA 認証に賛して ISCI により承認を受けているツール



生産効率低下の隠れた要因
ウイルス感染による設備の
稼働停止を防ぐ

講座紹介

ご契約プラン

ご利用料金

お申し込み方法

動作環境

利用規約

お問い合わせ

よくあるご質問

CIIE News

2015.02.19 メンテナンスのため06:00までサービス停止しました。

2015.02.05 新たなご契約プランをリリースしました。

2014.10.26 レッスンカテゴリを修正しました。

Free viewing

会員と同じ内容の講義が体験版として視聴できます。

特長

1. ビデオコンテンツで解りやすい
2. 習得スキルチェック機能
3. 職種別教育カリキュラムコースを設定
4. 経営者から技術者、品質管理者までカバー
5. スマホやタブレットやPCで受講できる
6. クラウドServerを利用
ビデオコンテンツは大容量データなのでクラウドを利用
7. 教育管理機能で人材教育管理
受講成績などの個人情報、企業内の管理者で管理

IEC62443をベースにした制御システムセキュリティ認証

CSMS認証 : Cyber Security Management System Certification

- サイバー攻撃に対するリスクアセスメントを基準にしたセキュリティ管理能力の評価

SSA認証 : System Security Assessment Certification

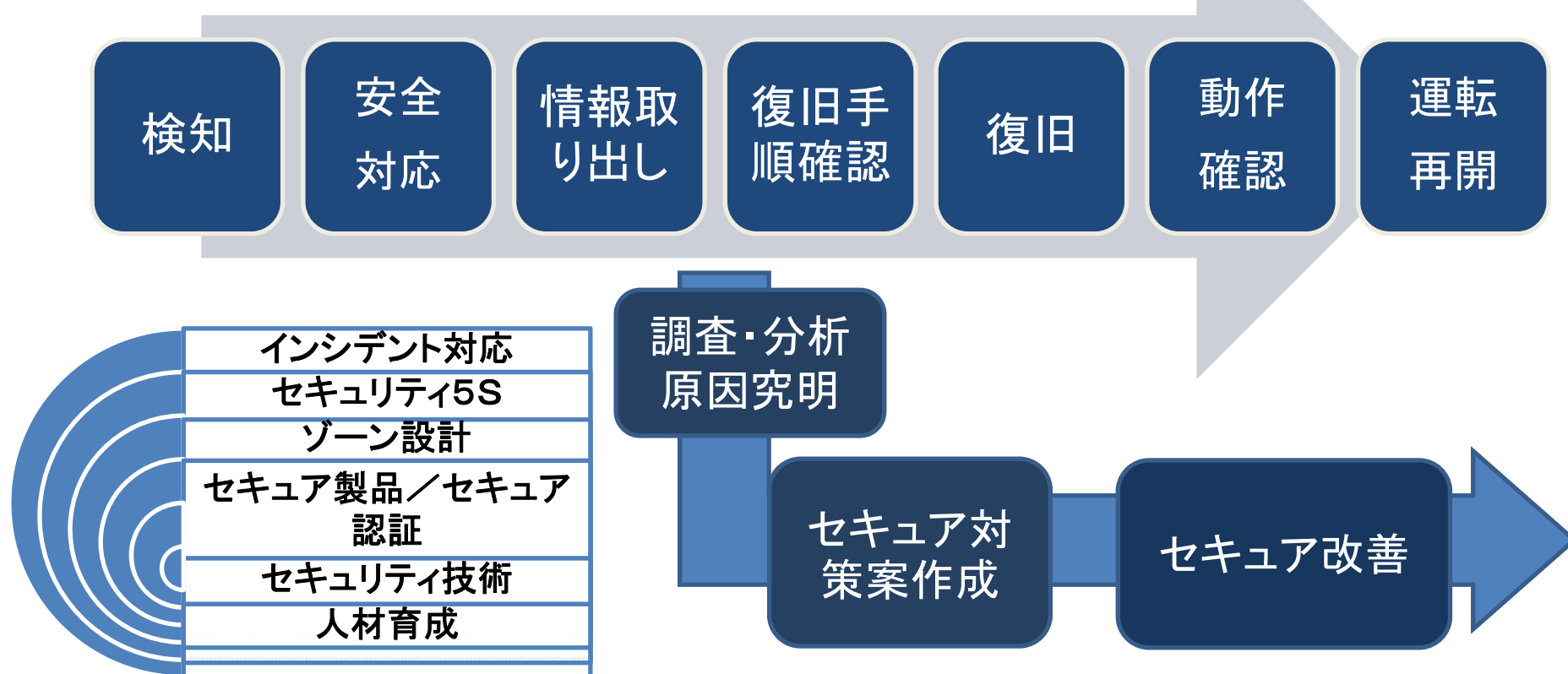
- SDLA : Security Development Lifecycle Assessment (セキュリティ開発ライフサイクル評価)
- FSA-S : Functional Security Assessment for System (システム対象の機能セキュリティ評価)
- FSA-E : Functional Security Assessment to Embedded Devices (組み込みコンポーネント対象の機能セキュリティ評価)
- SRT: System Robustness Testing (システムロバストネス試験)

EDSA認証 : Embedded Device Security Assurance Certification

- SDSA : Software Development Security Assessment (ソフトウェア開発セキュリティ評価)
- FSA : Functional Security Assessment (機能セキュリティ評価)
- CRT : Communication Robustness Testing (通信ロバストネス試験)

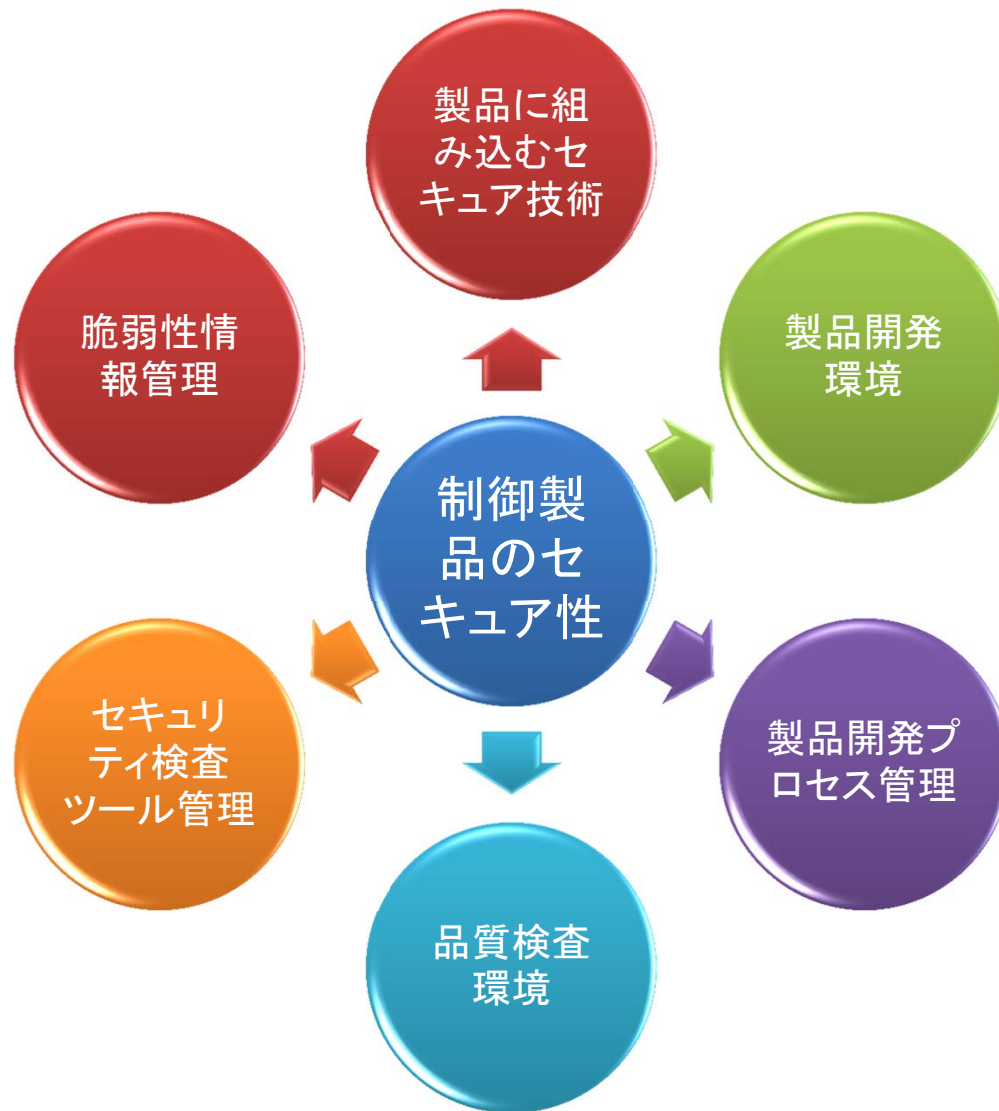
- インシデント対応は、侵入してきたマルウェアを検知してから、現場を安全に復旧させるまでの仕組みを言う。

マルウェアの特性によっては、復旧作業手順が異なる場合がある。



- [illegible]

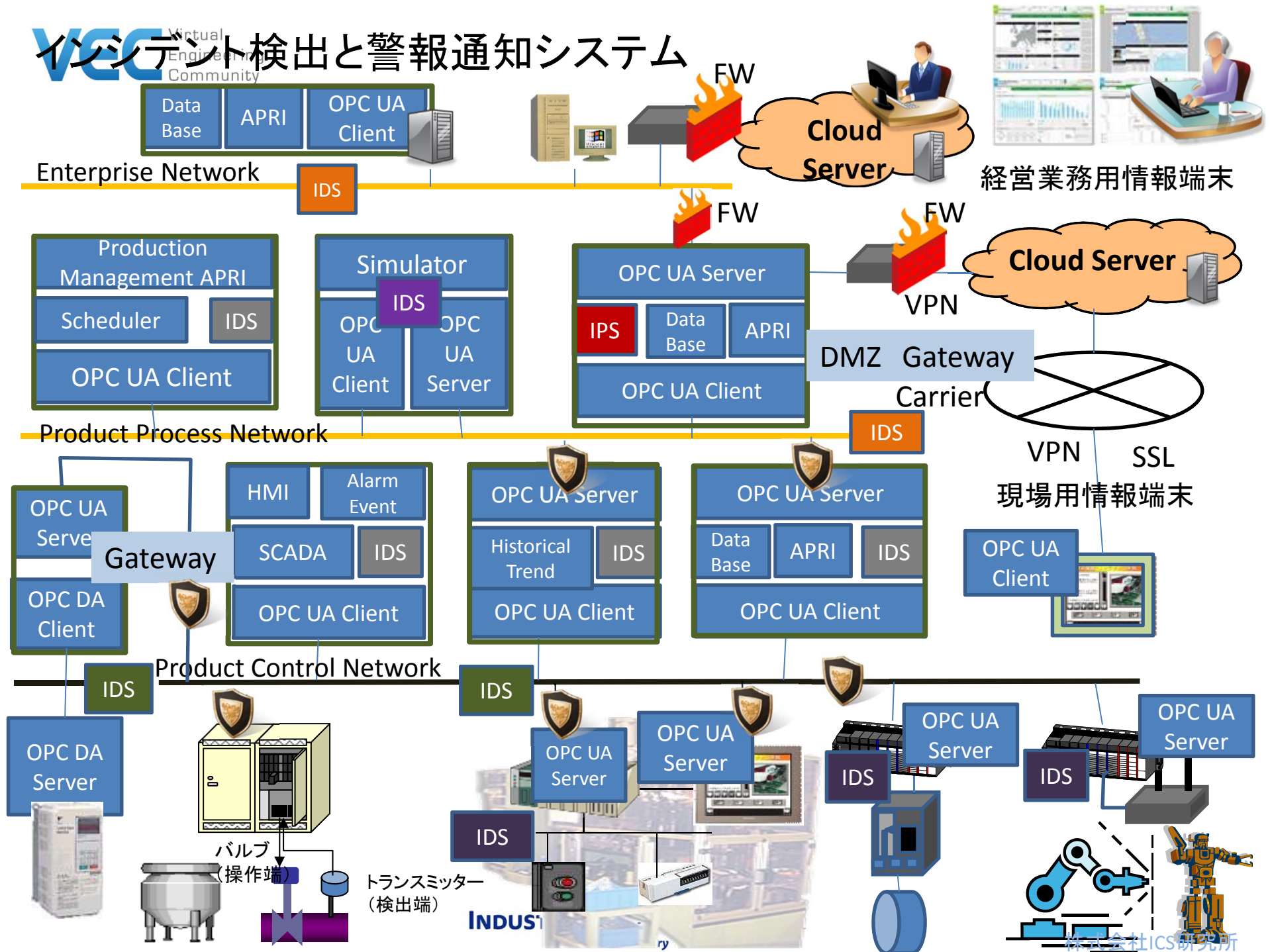
制御システムの制御製品のセキュア性を決めるもの



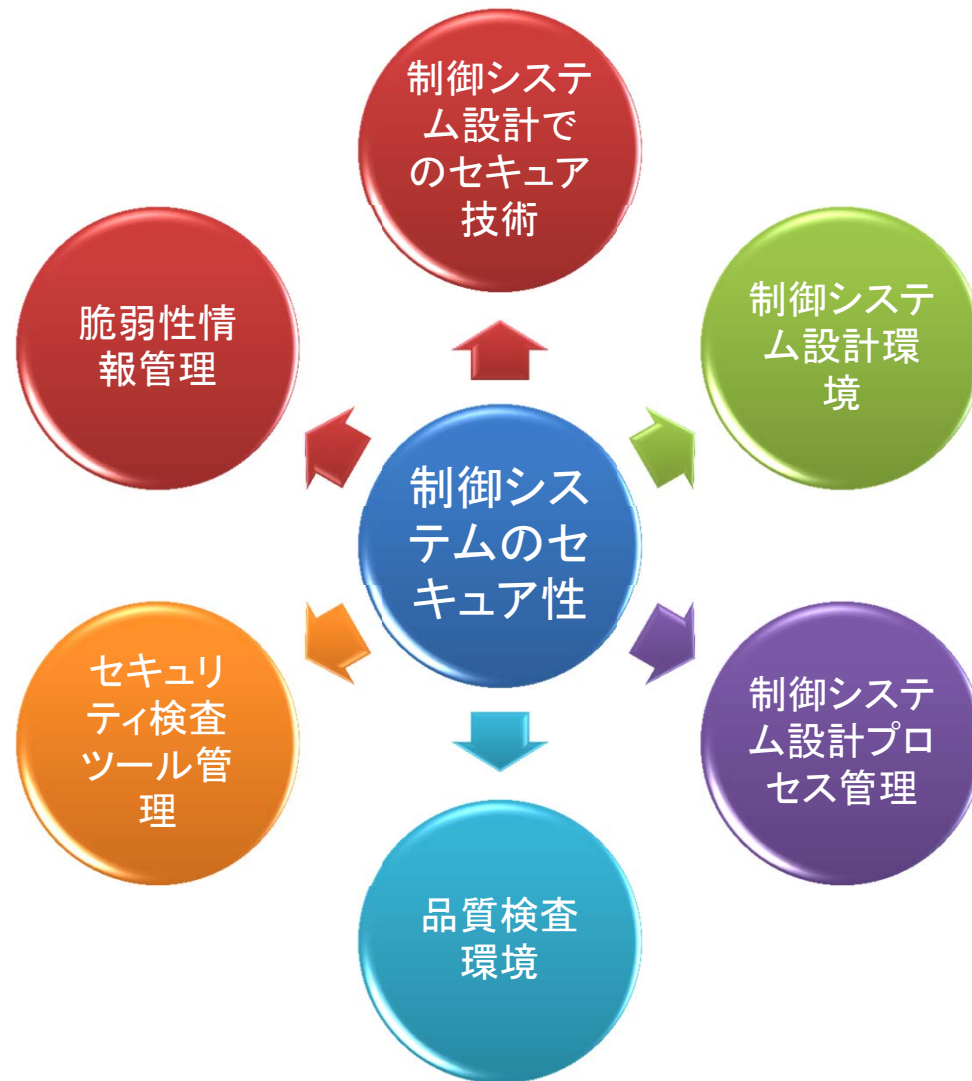
これらの対策実現に必要なことは何かを具体的に解説

環境の健全性管理
 セキュアコーディング管理
 セキュア検査技術
 ホワイトリスト技術
 ネットワーク
 フィールドバス
 無線通信
 タスク間通信
 HMIプロテクト技術
 オペレーションゾーン設計
 制御コード監視
 電子媒体認識管理
 エンジニアリングツールの健全性管理
 デザインレビューのセキュア要素
 脆弱性情報識別能力
 脆弱性情報処理・サポート

インシデント検出と警報通知システム



制御システムエンジニアリングのセキュア性を決めるもの



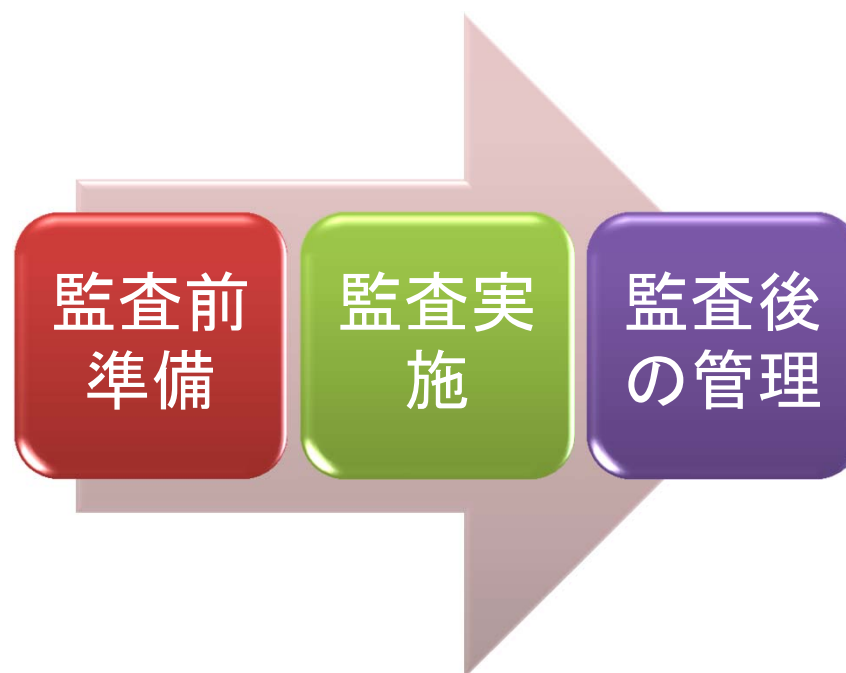
これらの対策実現に必要な
ことは何かを具体的に解説

設計環境の健全性
セキュアな設計技術
セグメント設計
ゾーン設計
DMZ・IPS・IDSの性能
ホワइटリストの技術と性能
制御製品のセキュア技術
設計プロセスでのセキュア
チェック
セキュア検査ツールの仕様と
能力
インシデント検知技術
復旧作業に必要な仕組み
復旧作業の手順
制御システムの脆弱性検査
脆弱性情報識別能力
脆弱性情報処理・サポート

発注先監査で重要なこと

発注先監査

- リスクアベースの監査
- 組織対象の監査



E-learning教育講座一覧

- 講座は、108講座以上になります。
- 内容は、制御システムセキュリティ対策の技術開発や標準規格などの更新に伴い、予告なく更新されることがあります。
- 年間全講座受講コースもあります。
- 仕事をする上で多くの知見を必要とすることから、辞書代わりに使っていただくことも想定して、VECの年会費をお支払いの会員様には、低価格で契約できるようにしております。

カテゴリ	講座名	カテゴリ	講座名
基礎	情報システムセキュリティと制御システムセキュリティの違い	発注先監査	発注先監査
	製造法設計		監査基本項目と基準
	警戒と被害その1		製造法設計
	警戒と被害その2		攻撃側の視点と対策機密情報
	警戒と被害その3		脆弱性情報管理 その1
	攻撃側の視点で見た制御システムその1		脆弱性情報管理 その2
	攻撃側の視点で見た制御システムその2		脆弱性情報管理 その3
	脆弱性情報対策基礎その1		設計環境整備と健全化管理
	脆弱性情報対策基礎その2		設計仕様で対策できること
	国際標準規格と認証機関		試験評価の方法
	世界のCSS機関		セキュア製品開発プロセス
	制御システムセキュリティゾーン設計基礎		セキュア設計技術 その1
	制御システムセキュリティ対策の全体像と各手法		セキュア設計技術 その2
	認証 CSMS認証、SSA認証、EDSA認証		発注仕様から納品まで
	インシデント対応基礎		品質保証と顧客サポート
企業経営における対策	セキュア改善	装置ベンダにおける対策	インシデント対応設計
	製造法規制について		リモートサービス
	警戒と被害と対策その1		攻撃側の視点と対策 機密情報
	警戒と被害と対策その2		脆弱性情報管理 その1
	警戒と被害と対策その3		脆弱性情報管理 その2
	警戒と被害と対策その4		脆弱性情報管理 その3
現場管理における対策	セキュリティ5Sの進め方		設計環境整備と健全化管理
	セキュリティ5Sの事例その1		設計仕様で対策できること
	セキュリティ5Sの事例その2		試験評価の方法
	現場での警戒と被害と対策		セキュア製品開発プロセス
	セキュア改善前にすること		セキュア設計技術 その1
	現場用セキュリティ製品その1		セキュア設計技術 その2
	現場用セキュリティ製品その2		発注仕様から納品まで
	現場用セキュリティ製品その3		品質保証と顧客サポート
	定期点検/修繕での作業		インシデント対応設計
	インシデント対応表紙		リモートサービス
	発注・受入・現場立ち上げ	制御ベンダ	制御ベンダの取り組みその1
	要求仕様書		制御ベンダの取り組みその2
	工場立会試験		脆弱性情報管理その1
	受け入れ検査から試験試験まで		脆弱性情報管理その2
ゾーン設計の技術	生産プロセス区分ゾーン設計		脆弱性情報管理その3
	制御系統のグループ区分ゾーン設計		設計環境整備と健全化管理
	統括管理区分ゾーン設計		【前編】セキュア製品開発その1
	SI/S区分ゾーン設計		【後編】セキュア製品開発その1
	オペレーションゾーン設計		セキュア製品開発その2
	フェイルセーフ区分ゾーン設計		セキュア製品開発プロセス
	無線通信ゾーン設計		セキュア評価その1
	現場セキュア改善手順		セキュア評価その2
	エンジニアリング		攻撃側の視点から見た機密情報
	【前編】セキュアエンジニアリングその1		製品仕様で対策できることその1
	【中編】セキュアエンジニアリングその1		製品仕様で対策できることその2
	【後編】セキュアエンジニアリングその1	認証	認証の目的と期待効果
	セキュアエンジニアリングその2		第三者認証
	オペレーション・ゾーン設計		CSMS認証
	【前編】要求仕様書から読み取る範囲		SSA認証
	【後編】要求仕様書から読み取る範囲		EDSA認証
	見積もり設計でのセキュア仕様		Achilles認証
	試験評価の方法		自己認証
	制御システムでのセキュア試験		システムインテグレータ
	品質保証と顧客サポート		セキュリティベンダ
			制御システムの種類と規模
			業界別法規制

2015年から、新しいタイプのE-learning教育が始まる。

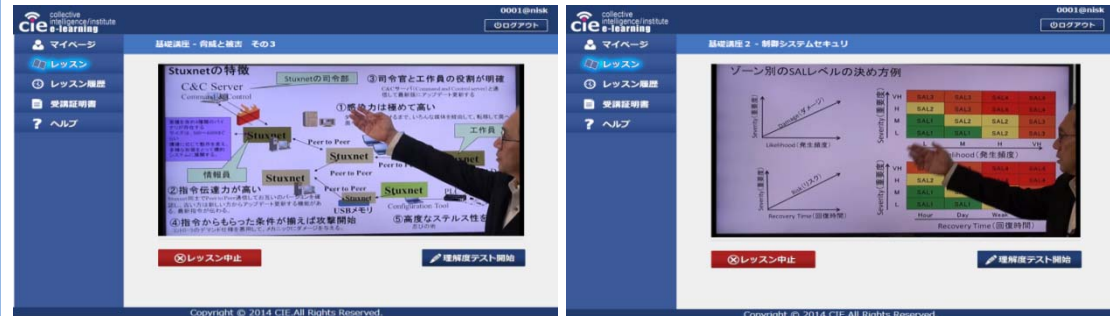
- オリエンテーション
- 基礎講座
- 企業における対策講座
- 現場管理における対策講座
- インシデント対応講座
- 発注・受け入れ・現場立ち上げ講座
- 現場セキュア改善講座
- エンジニアリング講座
- 発注先監査講座
- 装置ベンダにおける対策講座
- 機械ベンダにおける対策講座
- 制御ベンダ講座
- 認証講座
- システムインテグレータ講座
- セキュリティベンダ向け講座

延べ100講座以上

* 講座名、講座数は変わることがあります。

参考になっている情報

- NISC 公開情報
- NIST Guide to Industry Control Systems Security
- ICS-CERT情報
- IEC62443



講師陣: 制御システムエンジニアリング経験者
ソフトウェア設計経験者

今後予定している講座開発について

1. ゾーン設計エンジニアリング
2. セキュア通信仕様
 - a. OPC UA Clientの作り方講座
 - b. OPC UA Serverの作り方講座
3. セキュリティ製品の取扱い方講座
4. Industry4.1Jに関連する技術講座

まとめ

- スマホもロボットもこれからの人間社会に対応した製品仕様を見直してみよう。
- 「ものづくり」の言葉に酔うな！
- これからの日本の強みは、「セキュアなモノづくり」
- 世界に貢献できるインフラ技術を日本の強みにしよう。
- その為には、
 - 「セキュアな安全」
 - 「強い回復力」
 - 「これからを支える企業力」
- 今、やるべきは、“人材教育”。

沖縄ICTフォーラム2015 in 石垣島

新産業革命”Industry4.1J”が 世界を変える スマホとロボットと人間・社会

お問い合わせは、VEC (Virtual Engineering Community) のWebサイトの
<https://www.vec-community.com/ja/form/contact>
より、お願いします。

VEC事務局長兼ソリューションアドバイザー
株式会社ICS研究所
村上正志