ユーザ企業が抱える課題や求められる対応

VEC事務局長／株式会社ICS研究所

代表取締役社長

村上正志

経済産業省の制御システムセキュリティ検討タスクフォース委員

一般財団法人日本適合性認定協会制御システムセキュリティ技術審査員

計装制御技術会議企画委員

ISA認証機関

- 米国にあるISAの国際相互認証機関が認めた機関で受ける

ISA 国際制御学会 — International Standards Association

ASCI — Automation Standards Compliance Institute

公益財団法人 日本適合性認定協会

国際的な相互認証承認

ANSI/ACLASS 認定機関

JAB 認定機関

WCI 認証推進機構

ISCI 認証推進組織

ISA Secure スキームオーナー

Test Tool

Test Tool

認定

認定

CL：認証機関

excida

CSSC

申請

申請

日本のベンダ

日本での認証ラボセンター

INDUSTRY CONTROL SOLUTION LABORATORY

ICS研究所の事業：IoT／制御システムセキュリティ対策人材育成

- 製造現場アセットオーナー
- 計装制御システムエンジニア
- 機械制御システムエンジニア
- 制御ベンダエンジニア

- eICS：E-learning教育ビデオ講座
- 実力模擬試験
- ICSセミナー
- コンサルティング

eICS ICS研究所のeラーニングサービス

INDUSTRY CONTROL SOLUTION LABORATORY

Contents

IoTのリノベーション（改革）とイノベーション（革新）

サイバーセキュリティ情報最前線

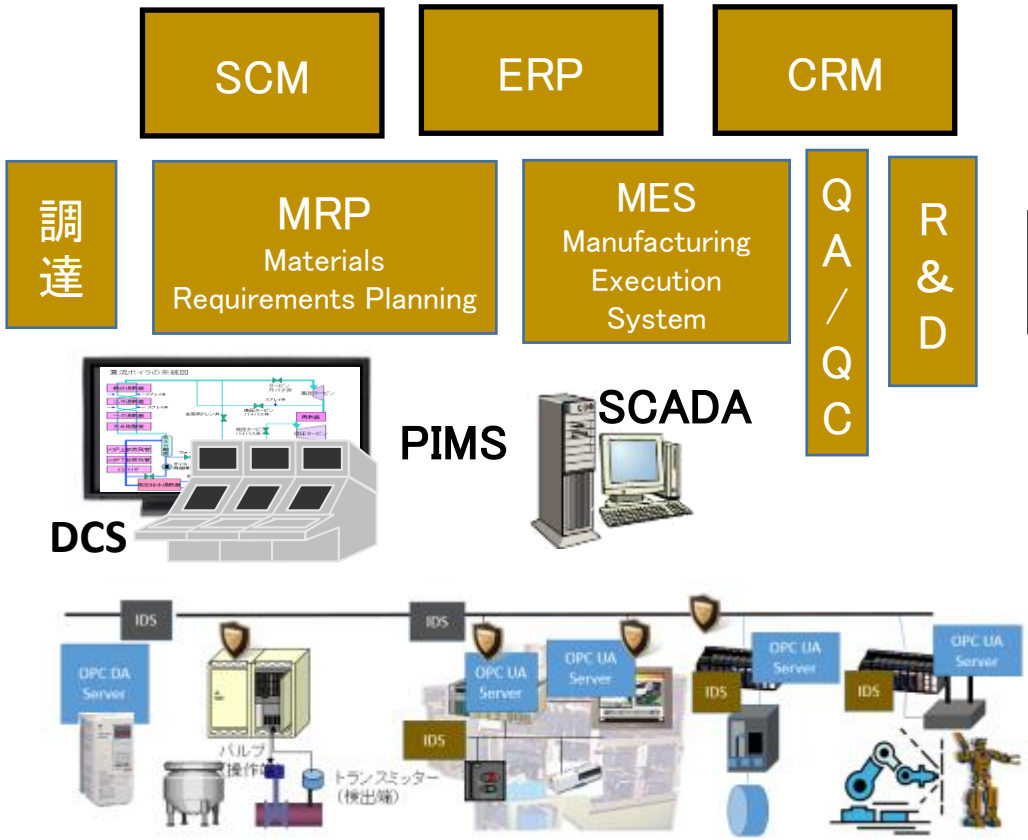
人材育成の重要性と対策

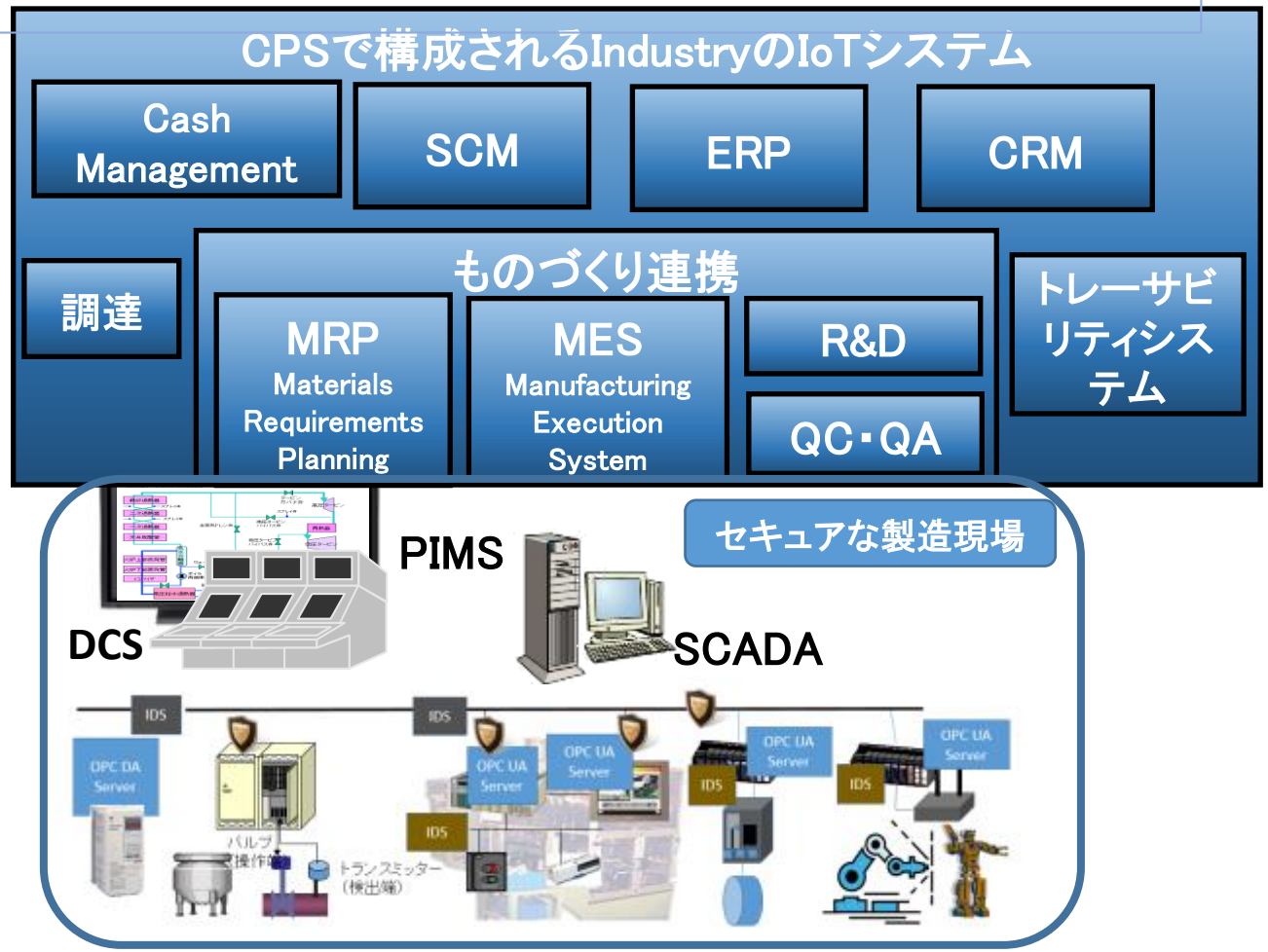
IoTのRenovation（改革）

- 第四次産業革命で企業改革を推進
- 強い企業経営体質を実現するIoT活用
- 社会を元気にするIoT活用

IoT／CPSで構成されるIndustryのIoTシステム

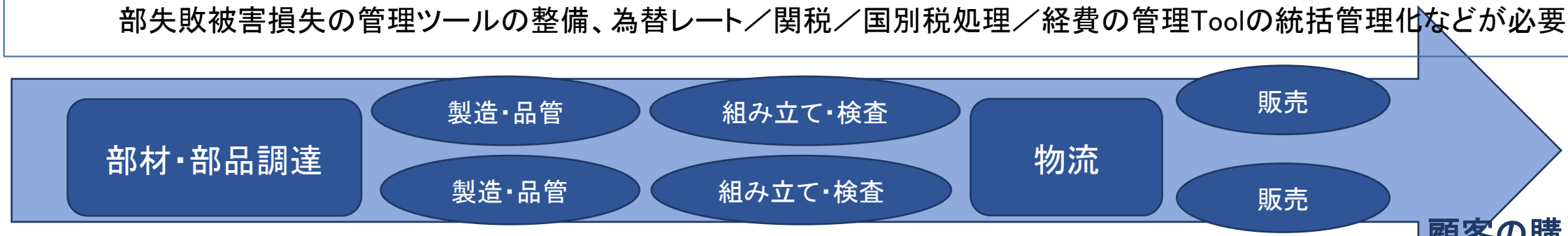
- 今まで、ITとものづくり現場の協力が無い、分断した製造形態でものづくりをしてきたことで、市場や経営上の急激な変化に対応できていなかった。
- ITとものづくり現場を連携させて統括管理できるバリューチェーンを構築し、その構造の裏で適材適所の機能を持ったMachine Learningが支えるセキュアでコンパクトなインフラを構成することで、市場や経営上の急激な変化にも対応できる企業力あるものづくり体制が実現できる。





プラグメンテーション時代（情報モデルを必要とする経営には、IoTが必須）

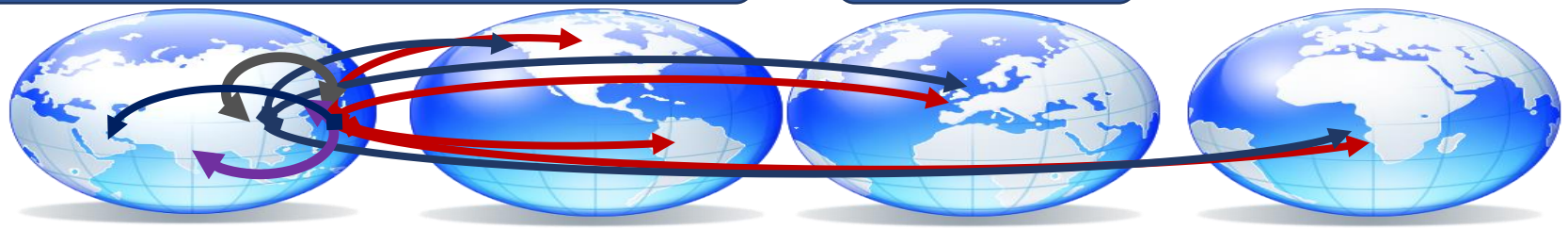
- サプライチェーンとバリューチェーンの違い
  - サプライチェーン：商品がお客様に届くまでの物の流れを管理
  - バリューチェーン：商品がお客様に届くまでの間、どこでどれだけの価値が生み出されて製品価値にして届ける管理
- 統括流動管理、個別生産効率管理、市場価値と利益と投資のキャッシュフロー管理、環境評価指標管理
  - その為に、Engineering Toolの標準化、品質管理Toolの標準化、法規制対応ツールの整備、リスク予測／評価損失と内部／外部失敗被害損失の管理ツールの整備、為替レート／関税／国別税処理／経費の管理Toolの統括管理化などが必要



事業戦略、マーケティング、プロモーション、サービス

生産品質基礎技術研究、サイバー／セキュア技術研究、
市場経営研究

製品開発



顧客の購入理由
安全安心
品質が良い
環境にやさしい
価格が適正
サービスが良い
使いやすい
健康に良い
必需品

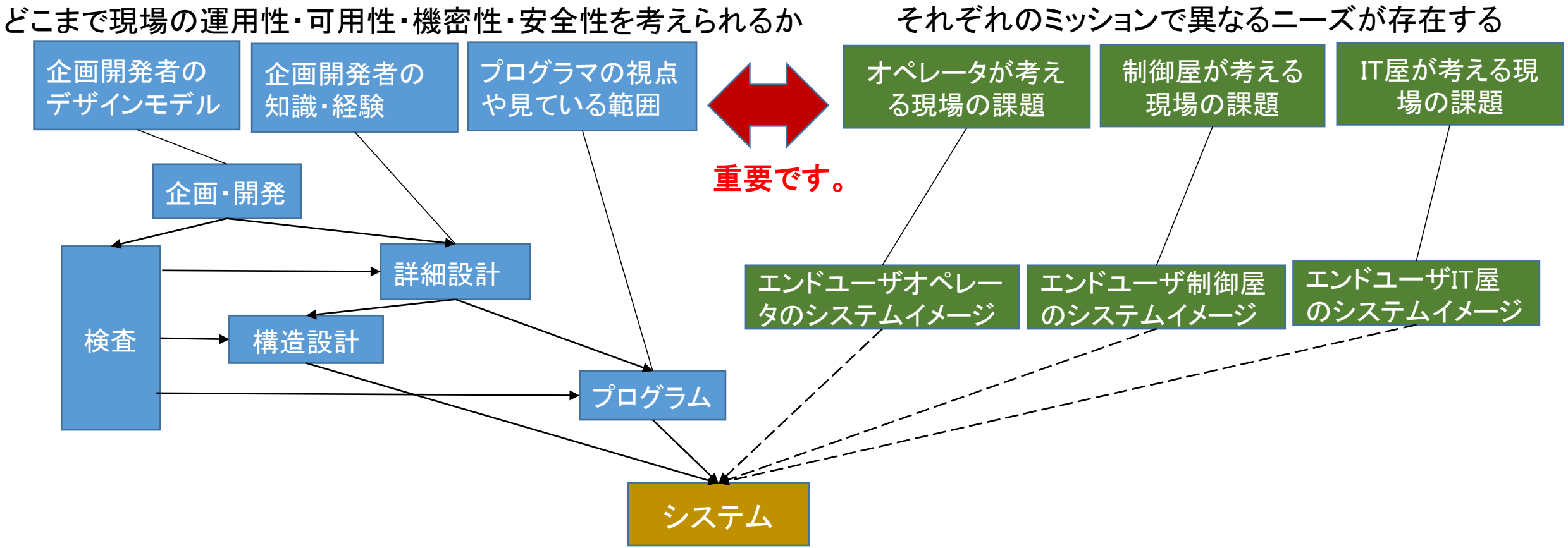
IoTのInnovation（革新）

- 企業内外のコミュニケーションを厚くする技術革新
- 社会の安全を支える技術革新
- 社会のコミュニティを向上させる技術革新

IoTの決めては、現場のイノベーションになっていること

- 現場の課題／問題解決になっているのかが重要
- 現場がシステムを使いこなせることが重要

「見える化」を失敗する原因は、この二つが欠けているからです。
失敗しないためには、現場の真の問題をしっかり理解することです。

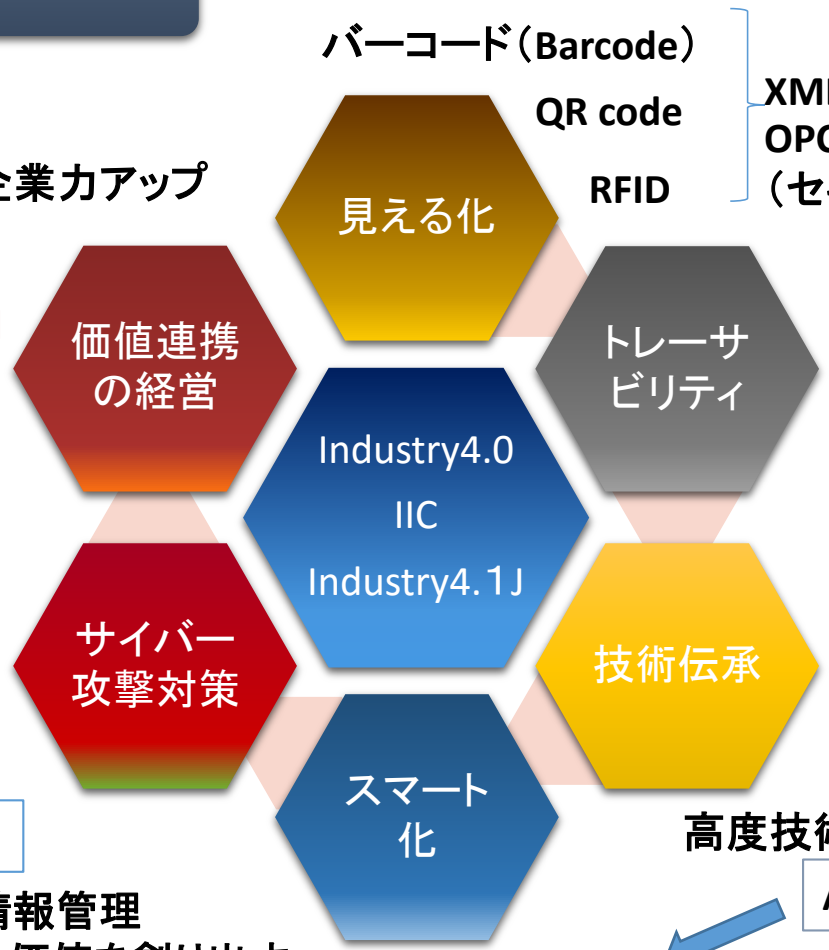


Industry4.0／IIC／“Industry4.1J”ソリューション

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
Ransonware
Havex　SHODAN



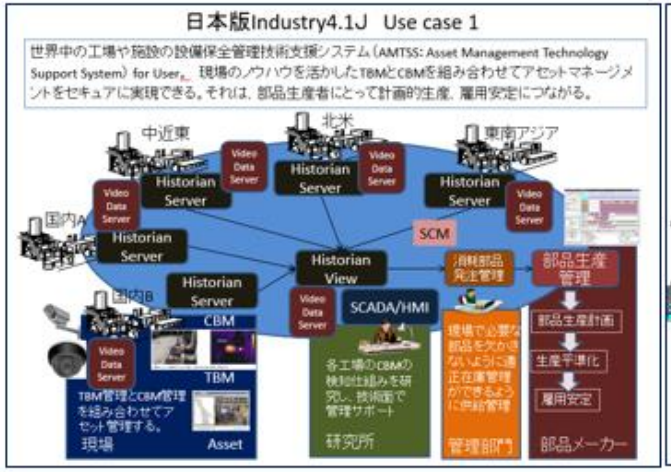
MBSE（Model Based Systems Engineering）
モデルシステム設計技術
ERP連携
SCM連携
企業力アップ
BOM連携
MES連携
社会的責任
企業資産防衛
BCP/BCM
SDLA認証
CSMS認証
EDSA認証
SSA認証
制御システムセキュリティ対策
ビデオコンテンツによるE-learning教育
人材育成
インシデント検知
サーベイランスシステム
セキュアな通信
OPC UA
Private Cloud活用
振る舞い監視
製造業における機密情報管理
ビッグデータ
AIの利用
今までにない価値を創り出す
特徴抽出技術
クラスタ制御技術（群制御）

バーコード（Barcode）
QR code
RFID
Internet of things（Public Cloud）
XMLでServerに連携
OPC UAでIOTに連携
（セキュア対応）
PLCopen
FBの差し替え技術
（レシピデータの切り替え）
SCM強化
マルチロボット技術
作業ミス撲滅
Wearable computing
セキュアなインフラ
IoTが
使えない工場
グローバルサポートされた
Private Cloudの活用
シミュレータ活用
クラウドを利用した適応制御
AIの利用
高度技術の活用
ART活用
ノウハウの蓄積
スマート・ナビゲーション
体系化
ノウハウの
抽出技術
人材育成
アセットマネージメント

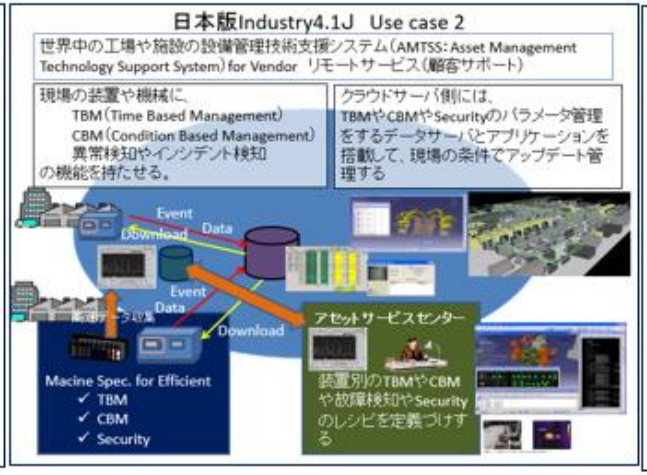
セキュアな現場の制御システムがあってのIndustryの未来

プライベートクラウドを活かした“Industry4.1J”のUse case1～16

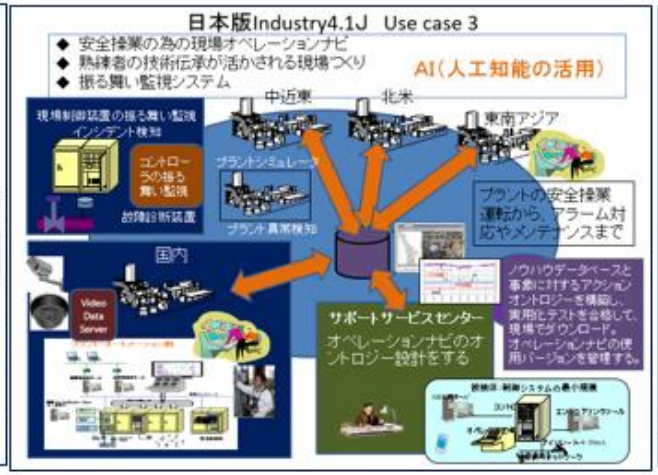
設備保全、TBM／CBM



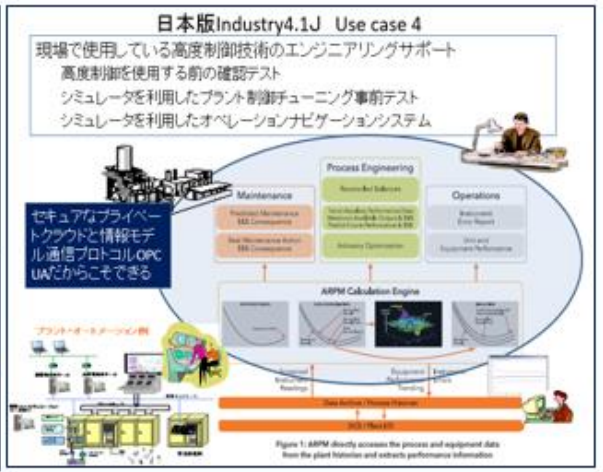
ベンダによる現場サポート



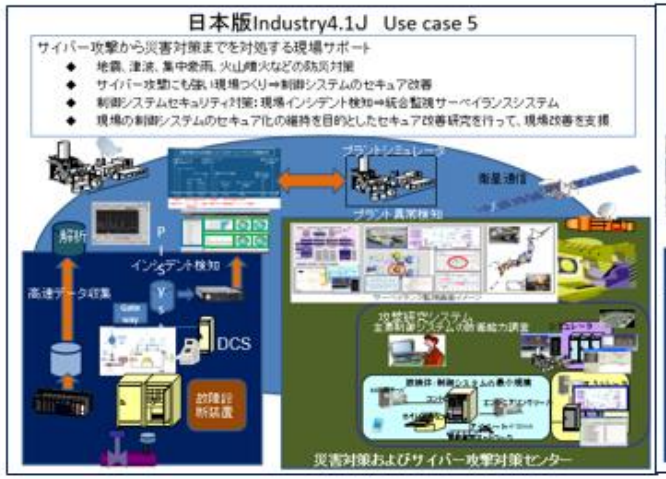
インテリジェントな現場サポート



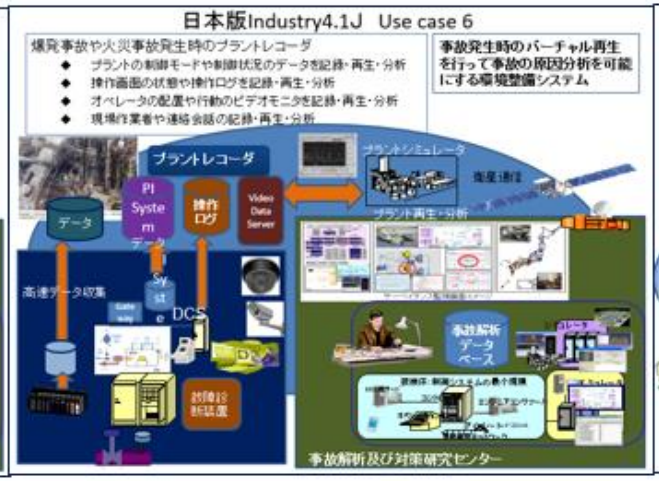
高度制御支援



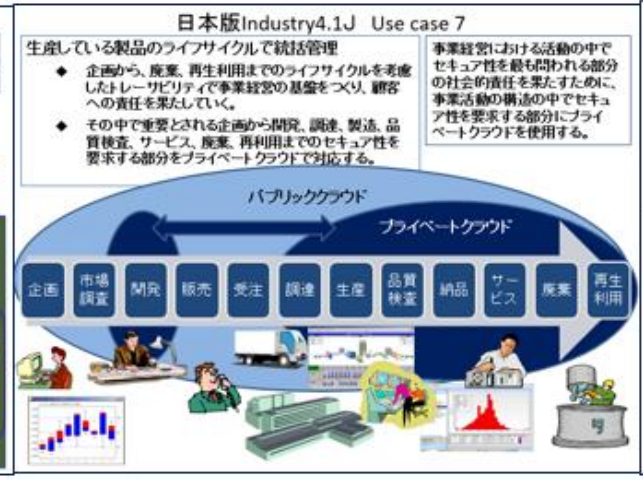
インシデント検知
インシデント対応



プラントレコーダー



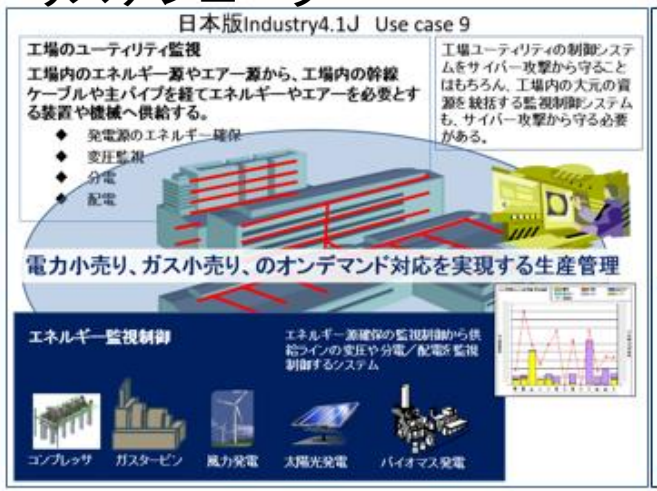
ライフサイクルサポート
トレーサビリティ



インテリジェント・ビル対応

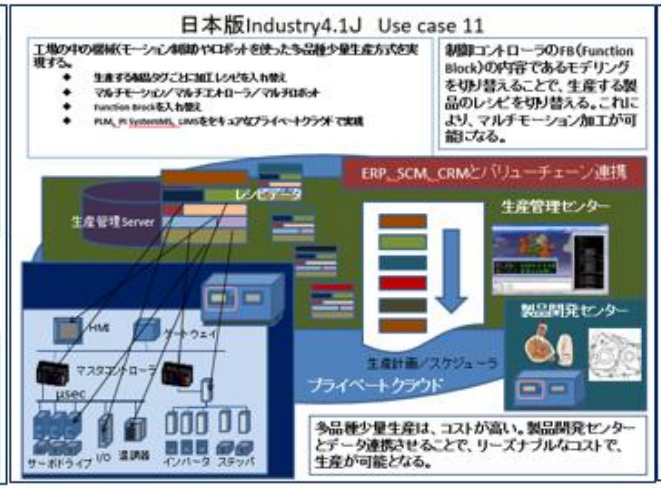
プライベートクラウドを活かした“Industry4.1J”のUse case1～16

エネルギーオンデマンド
リスケジューラ

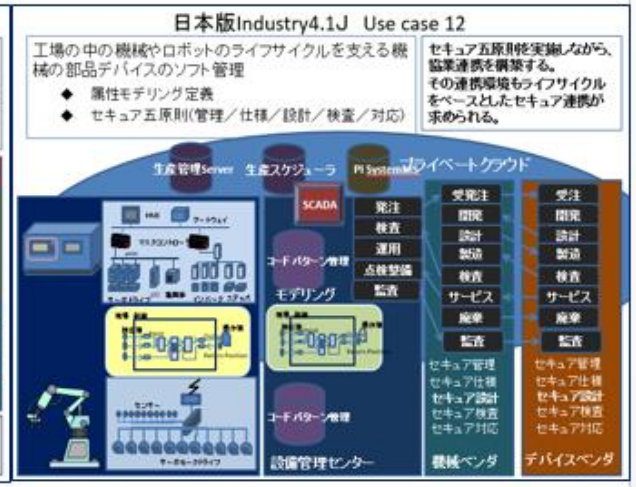


サーバールームのセキュリティ

マルチプロダクション

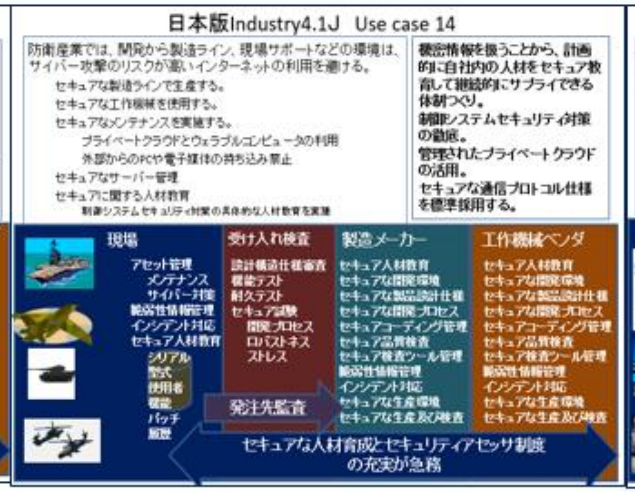


セキュアメンテナンス

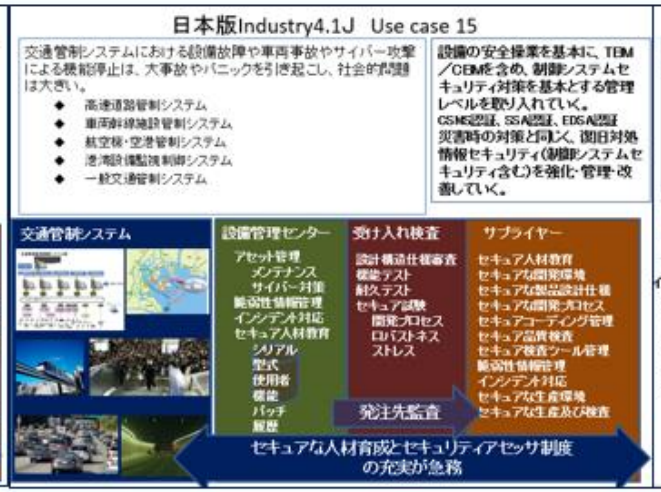


ロボットのインシデント検知
セキュアなインシデント対応

セキュアな防衛産業



安全な交通管制システム



安全な東京オリンピック・
パラリンピック大会

セキュアメンテナンス

プログラムレスでIoTが作れるプラットフォーム

プライベートクラウド内でSCADA、Historian、Simulatorが使える時代

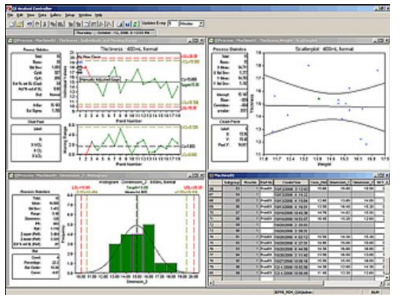
- ◆プログラマーでなくてもIoTの構築仕事ができる
- ◆短期間で「つなげる」から「分析まで」の機能を使える
- ◆産業特有の評価計算式もSCADAの中に作れる
- ◆ERPやSCMとつなげられる

現場からIoTまで使用できるプログラムレスIoTプラットフォーム

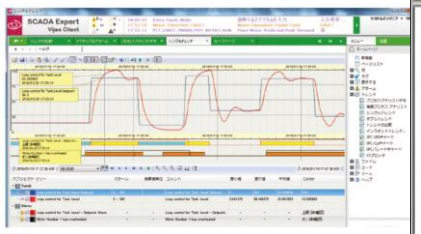
ERPとつながるSCADAやHistorian

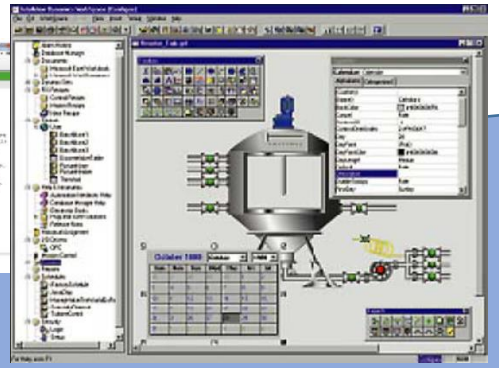
IoT SCADA Client

生産品質分析



IoT SCADA Server





Public Cloud

IP-VPN

ERP

SCM

AI

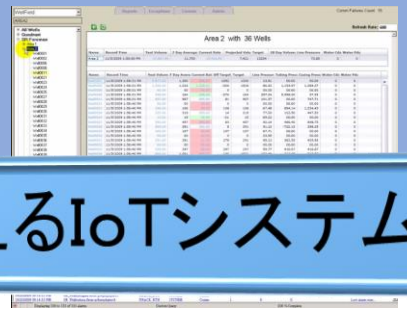
Private Cloud

AI

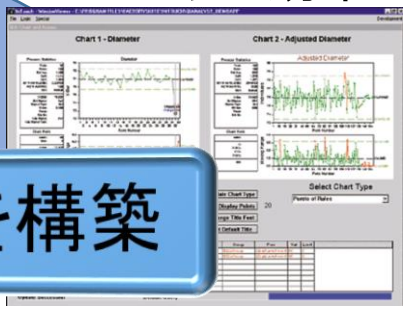
Private Cloud

IP-VPN

Historian Server

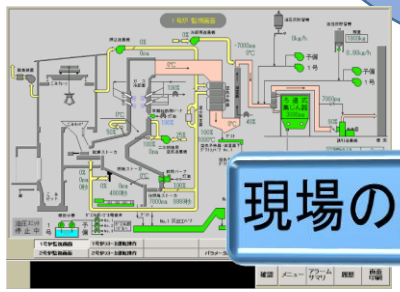


エネルギー効率



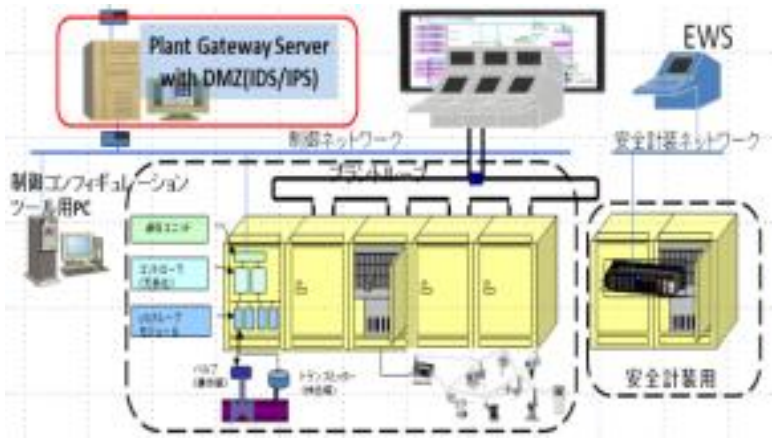
経営と現場を支えるIoTシステムを構築

DCS

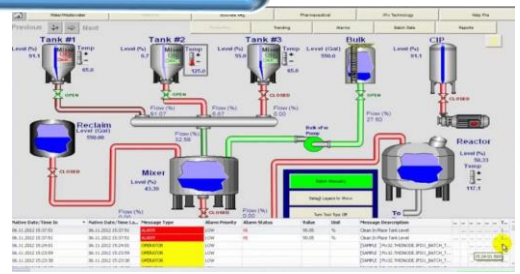


IP-VPN

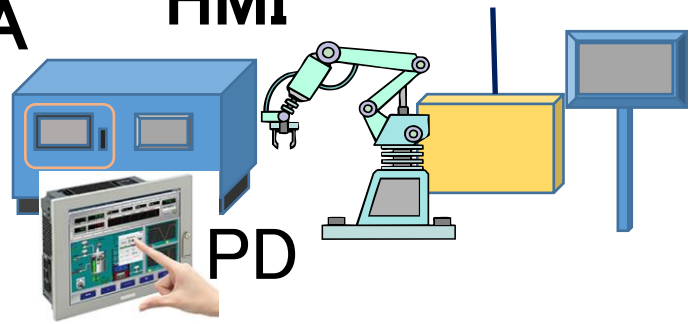
現場の安全操業は現場で守る



SCADA

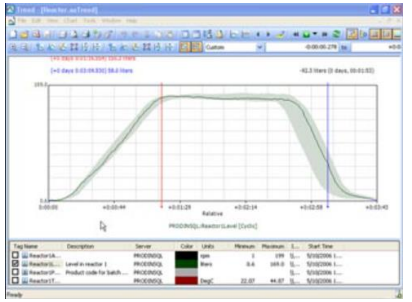


HMI

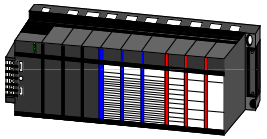


PD

生産・制御損失



PLC

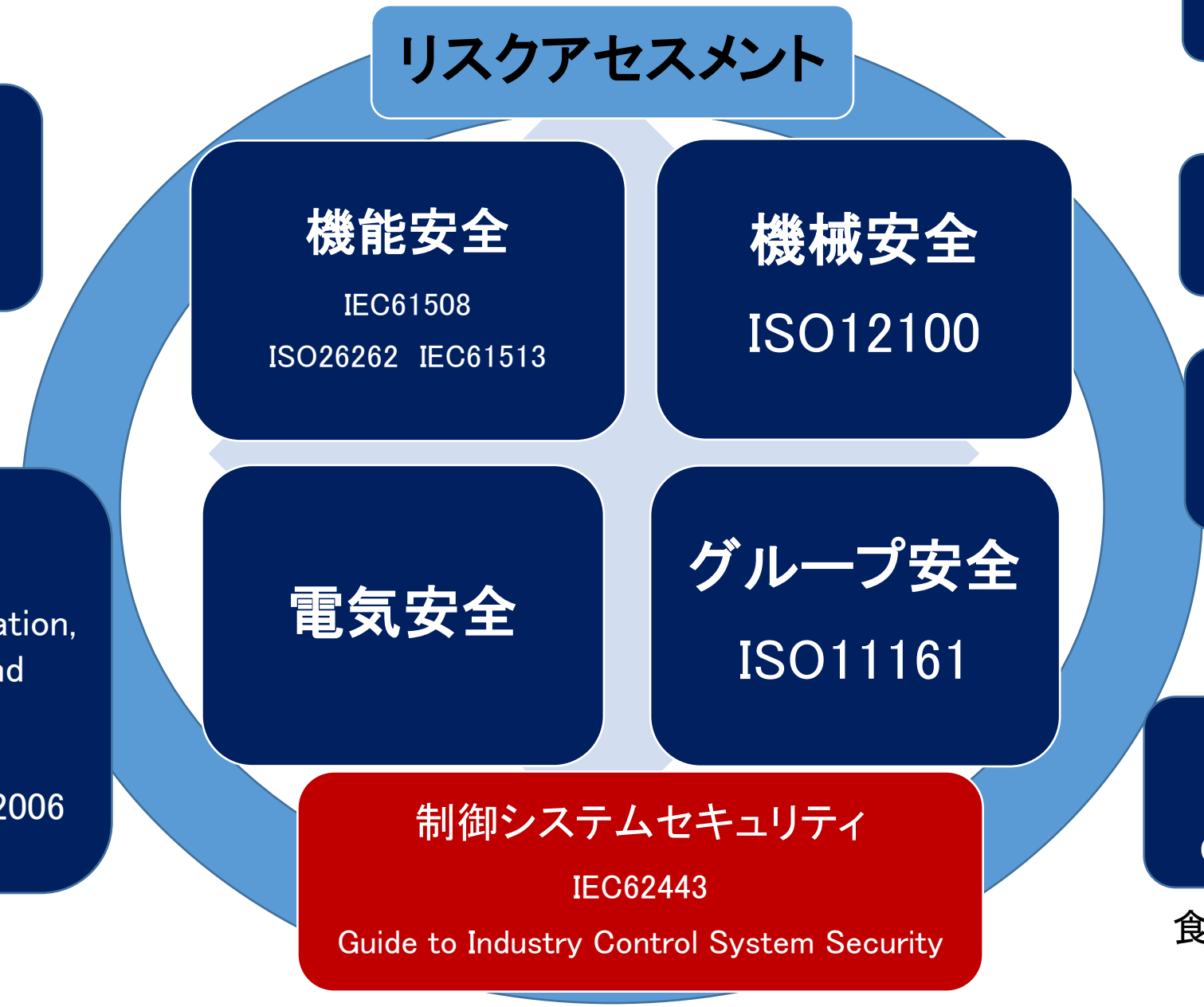


一つのプラットフォーム操作を知っているだけで現場装置からIoTのサーバーからクライアントまでの構築ができる。

サイバーセキュリティ情報最前線

- IoTシステムを進めるにはサイバーセキュリティ対策が必須
- デバイスだけでなく、コントローラにもマルウェアが侵入する
- 各産業の業界全体の問題

製造業の課題とリスクアセスメント



RoHS指令
Restriction of Hazardous Substances

危険有毒物規制

REACH
Registration, Evaluation, Authorization and Restriction of Chemicals
EC規則 No 1907/2006

有害化学物質
環境対策規制

模倣品対策

電子部品

安定供給

GMP
Good Manufacturing Practice

医薬品/医療品/化粧品/食品

HACCP
Hazard Analysis and Critical Control Point

食品/食品加工/飲料

情報セキュリティと制御システムセキュリティ

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
  - 通信ｻｰﾊﾞ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**
  - **電機組み立て**
  - **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**
    SICE
    （計測自動制御学会：学術団体）
  - 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

サイバーセキュリティ対策の重要性

国内で起きている事故

自動車工場	•現場サポート業者が持ち込んだPCから工場内ネットワークにマルウェア侵入。PC50台に感染 •10日間操業停止⇒1200台出荷できず：年間売り上げから30億円以上が無くなる
半導体製造工場	•現場装置のアップデート作業で持ち込んだデバイスから工場内ネットワークにマルウェア侵入 •1か月間操業停止⇒年間売り上げから340億円が無くなる。
石油精製工場	•MESのネットワークにマルウェアが侵入 •2週間操業停止⇒2週間分の出荷減
工作機械が並ぶ精密機械製造工場	•マルウェアが工場内ネットワークに侵入 •セキュア改善するまでは、年に数回数週間ずつ操業停止
ゴミ焼却場	•従業員が持ち込んだ携帯電話の充電中にインターネットと接続。マルウェアが侵入 •6日間操業停止
高速道路管制システム	•インターネットにつながるPCからマルウェアが侵入し、USBメモリ経由で管制システムに感染 •設備総入れ替え

サイバーインシデントが発生する都度に出てくる損失

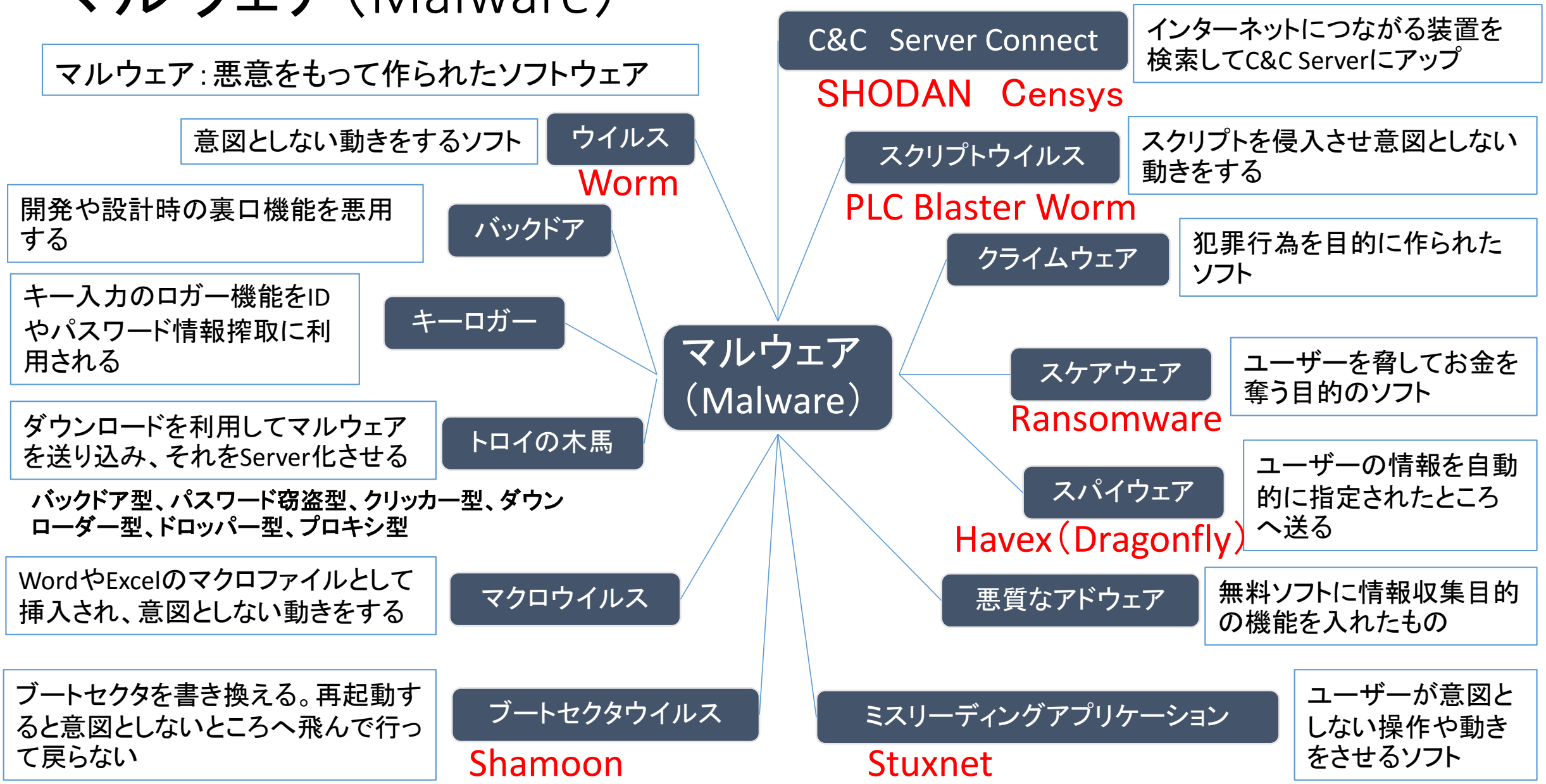
何が問題か

- 年間計画している売り上げが減る。
  - 操業停止している期間の売り上げが無くなる。
- 復旧作業の為にコスト増
  - 緊急対応コスト
    - マルウェア判定：専門家に依頼
    - 洗浄作業：
    - 回復作業：ベンダを呼びだして作業依頼
  - セキュア改善対策コスト
    - インシデント検知システム
    - セグメント設計改造
    - ゾーン設計改造
    - インシデント対応トレーニング

いずれにしろ、やることになる投資

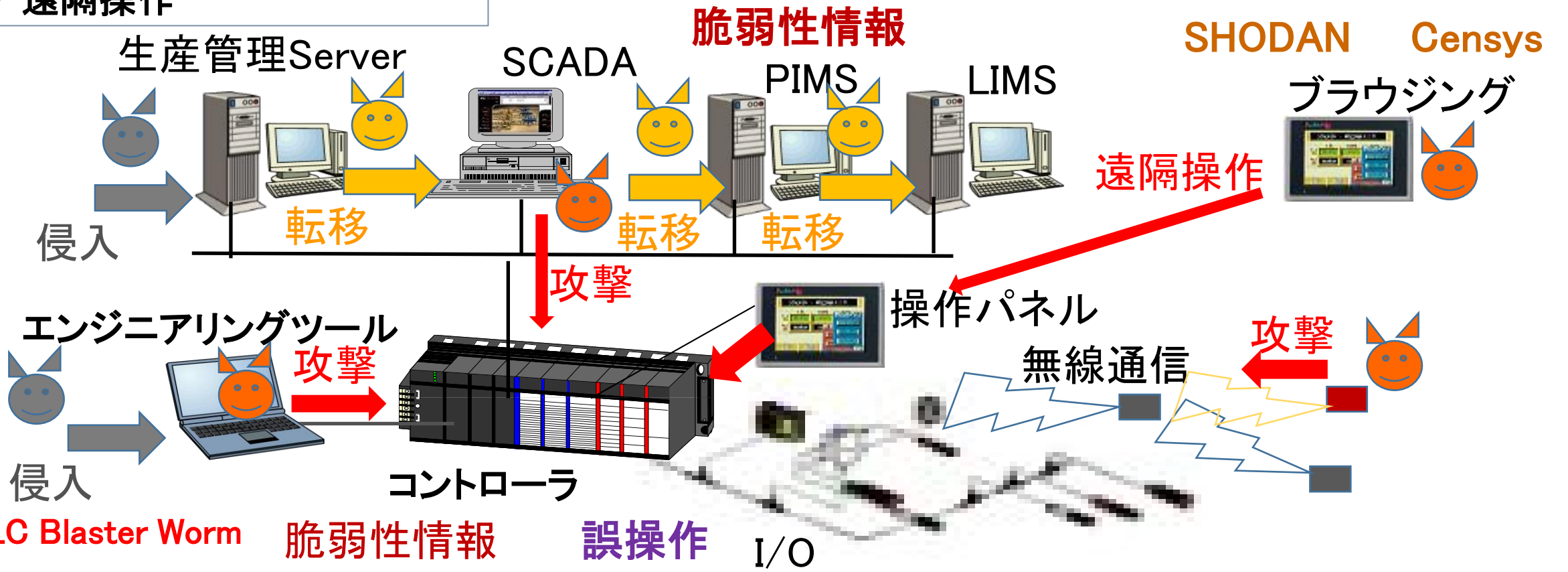
マルウェア（Malware）

マルウェア：悪意をもって作られたソフトウェア



コントローラに押し寄せる脅威

- 通信コードの差し替え
- 偽デマンド指令
- Dos攻撃
- 遠隔操作



PLC Blaster Worm：コントローラに仕込まれるマルウェア

- PLCのコンフィギュレーションツールやPLCにつながるポータルツールからWormをPLCに送り込み、PLCからPLCに感染させることもできる。PLCをネット上のC&Cサーバーの支配下におくこともできる。

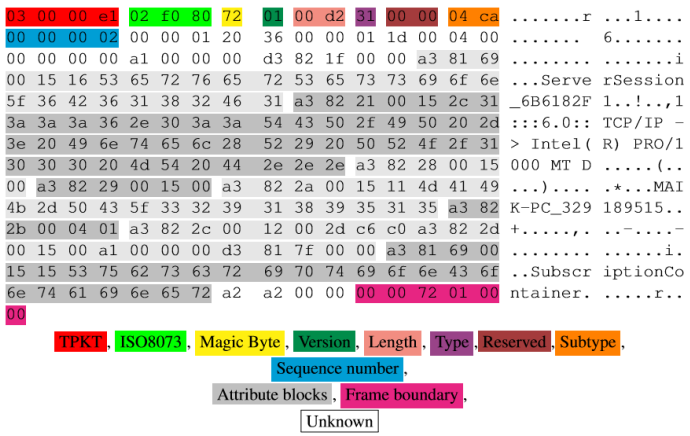


Figure 5. S7CommPlus message structure

Figure 14. TIA portal exposes the worm

資料は、Asia Black Hat 2016の発表PDFより引用

対策は、IEC62443-4-1の更新版でも検討課題。

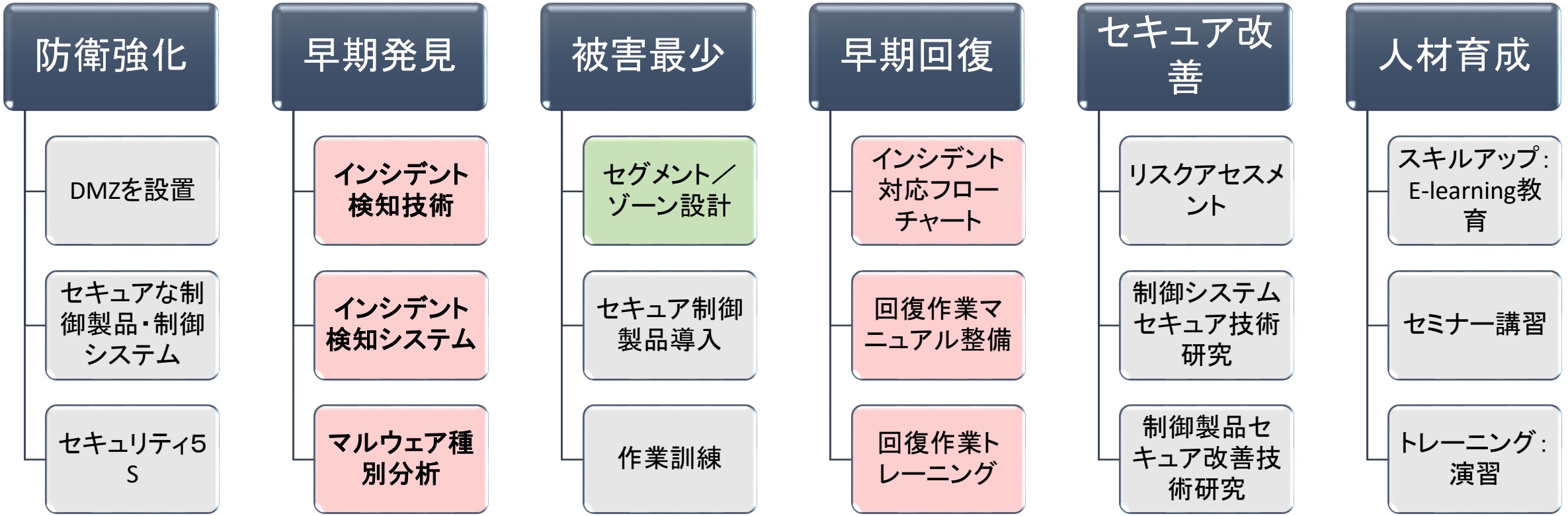
Vendor	Product	Ethernet	Transfer TCP/UDP	TCP/IP Functions
Siemens	S7-300	Ja	Ja	Ja
Siemens	S7-400	Ja	Ja	Ja
Siemens	S7-1200	Ja	Ja	Ja
Siemens	S7-1500	Ja	Ja	Ja
Mitsubishi Electric	MELSEC iQ-R	Ja	Ja	Ja
Mitsubishi Electric	MELSEC iQ-F	Ja	Ja	Ja
Mitsubishi Electric	MELSEC-Q	Ja	Ja	Ja
Mitsubishi Electric	MELSEC-L	Ja	Ja	Ja
Mitsubishi Electric	MELSEC-F	Ja	Ja	Nein
Mitsubishi Electric	MELSEC-QS/WS	Ja	Ja	Nein
Schneider Electric	Modicon Easy M	Nein	Nein	Nein
Schneider Electric	Modicon M	Ja	Ja	Nein
Schneider Electric	Modicon LM	Ja	Ja	Nein
Schneider Electric	Modicon Premium	Ja	Ja	Nein
Schneider Electric	Modicon Quantum	Ja	Ja	Nein
Schneider Electric	Preventa XPS Quantum	Ja	Ja	Nein
Rockwell Automation	ControlLogix	Ja	Ja	Ja
Rockwell Automation	CompactLogix	Ja	Ja	Ja
Rockwell Automation	MicroLogix	Ja	Ja	Ja
Rockwell Automation	SmartGuard 600	Ja	Ja	Nein
Rockwell Automation	SLC 500	Ja	Ja	Ja
Rockwell Automation	PLC-5	Ja	Ja	Ja
Rockwell Automation	GuardPLC	Ja	Ja	Nein
Rockwell Automation	Micro800	Ja	Ja	Nein

制御システムセキュリティ対策

- 制御システム構成で、セキュアでない制御製品が一つあるだけで、その制御システムは、セキュアレベルを維持できなくなります。
- 製造システムの主要な制御システムでインシデントが発生すると操業できなくなる可能性が高くなります。

制御システムセキュリティ対策

- インシデント検知機能が現場に無いと対応ができない。



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

SDLA認証：Security Development Lifecycle Assessment

- SDLPA：Security Development Lifecycle Process Assessment （セキュリティ開発ライフサイクルプロセス評価）
- SDA-S：Security Development Artifacts for System （システム設計品の開発評価）
- SDA-E：Security Development Artifacts for Embedded Devices （組み込みコンポーネント対象の開発評価）

SSA認証：System Security Assessment Certification

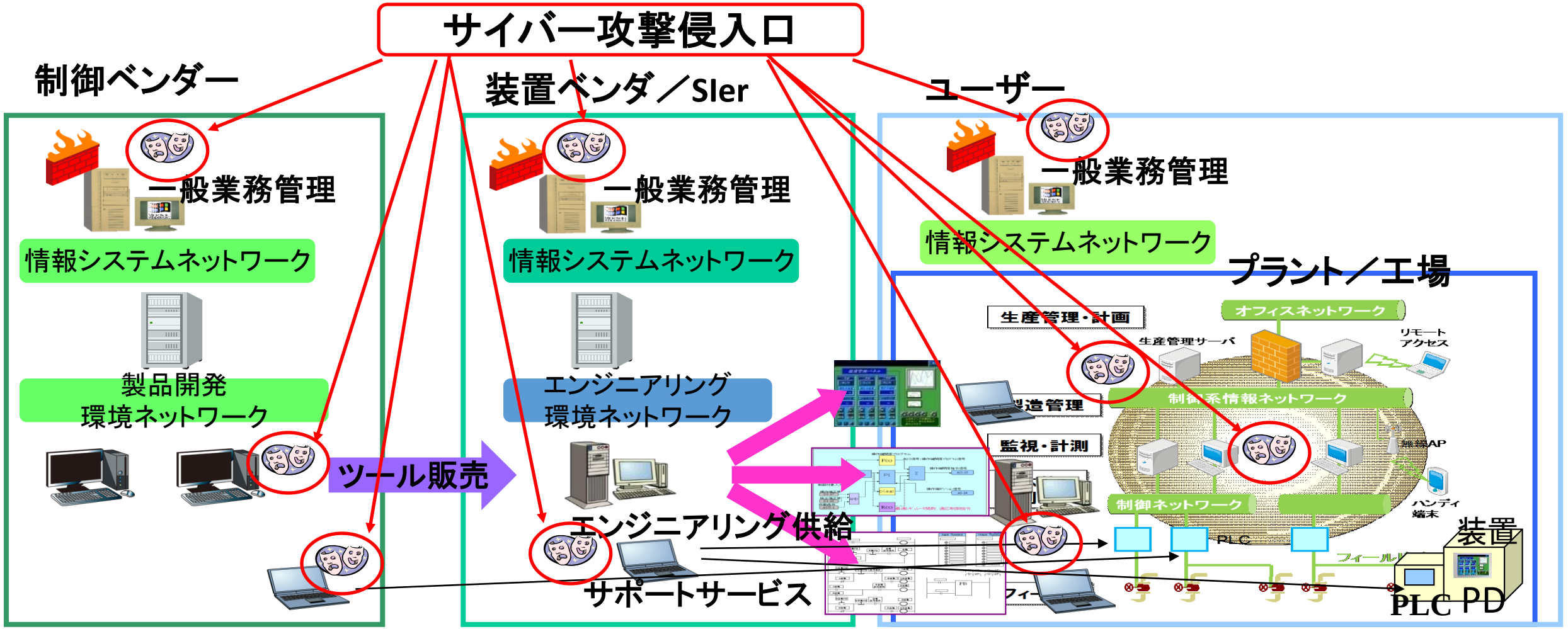
- System Security Assessment （システムセキュリティ評価）：SDLPA＋SDA-S
- FSA-S：Functional Security Assessment for System （システム対象の機能セキュリティ評価）
- FSA-E：Functional Security Assessment to Embedded Devices Components（組込みコンポーネント対象の機能セキュリティ評価）
- SRT: System Robustness Testing（システムロバストネス試験）

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）

サイバー攻撃の侵入口

- 制御ベンダの製品開発環境から、装置ベンダの開発環境、SIerエンジニアリング環境、ユーザーの現場環境と、サイバー攻撃の侵入口は、存在する。



製造業の工場をリモートサポートするIoTシステム例

- ユーザーがセキュア検証試験のセキュアカテゴリレベルを指定して、工場の実態に合ったセキュリティレベルを実現できる。

パブリッククラウド
各種人工知能サービス

パブリッククラウド
ERP、SCM、CRM
トレーサビリティ

プライベートクラウド
インシデント検知機能
MES
オペレーションナビ
高度制御
PIMS、LIMS
Gateway　DMZ

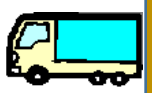
プライベートクラウド
人工知能開発
ビッグデータ処理
各種解析技術開発

大学／セキュリティベンダ
／研究所
高度制御技術研究
インシデント対応技術
インシデント検知技術
評価ツール開発

プライベートクラウド
テストベッド
第三者評価機関
DMZ

プライベートクラウド
人工知能を使った技術開発
シミュレーション技術

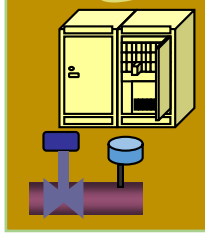
物流
センター



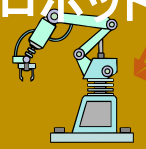
倉庫
管理

工場

装置

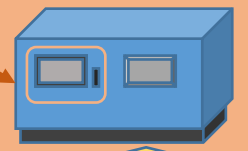


ロボット



セキュア検証試験
セキュアカテゴリ1
セキュアカテゴリ2
セキュアカテゴリ3

装置・機械ベンダ、SIer



テスト

ソフト
プロファイル

自社クラウド
ERP、SCM、CRM
技術研究
シミュレーション

生産技術
センター

製品開発
センター

プライベートクラウド
セキュアなリモートサービス
インシデント検知機能
インシデント対応、DMZ

業界企業のリモートをつなぐセキュアなクラウド

数百社から数千社

現場に制御システムセキュリティ対策がある無しで大きな差が出る

- グローバル企業は、制御システムセキュリティ対策ができているので、回復時間が短い。

ISA SecureでIEC62443の制定に参加していた欧米のグローバル企業が自社工場でやってきたこと。（2012年～2014年）

●サイバーセキュリティ対策のオーナー担当をおく

製造システムのサイバーセキュリティ対策専門チームを組織化

自社のテストベッドを設置

- インシデント検知・監視システムの実験
- セキュア検査ツールの実証実験
- 自社製品のセキュア自己認定を実施

自社製品のセキュア化対策

- 第三者セキュリティ認定を受ける製品を分類
- セキュリティ自己認定の評価基準を制定
- 品質検査にセキュア評価検査を追加

人材育成

- 部門別サイバーセキュリティ育成プログラムを決める
- TVシステムなどを利用して、各事業所でセミナーを実施
- E-learning育成コンテンツを開発し、実施（人事評価の必須項目に入れる）

自社製造システムのセキュア化

- 製造システムのセキュア改善項目とインシデント検知・監視システムの基本を決めて、各工場に実施
- 自社の製造システムのセキュア改善チームを作って、世界中の工場のセキュア改善作業を実施

サイバーインシデントは、企業経営の基盤を脅かす重大リスクである。

2010年のStuxnetが登場してから、インターネットに接続していない制御システムもサイバー攻撃できることが明らかになったことで、操業停止に至る大問題を引き起こす重大リスクであることが明らかとなった。
これにより、企業が計画している売り上げが失われ、社会的信用も損ない、企業存続の必須条件として取り組んでいかなければならない課題であることが認識された。

IoT／第4次産業革命のステップ1，2，3

制御システムセキュリティ対策は、IoT／CPSを支える基盤技術

何が見えていないかが分ればできる。

何が必要かを考えればできる。

現場の真の課題を理解すればできる。

ステップ1

- 見える化

情報セキュリティだけでは、サイバー攻撃対策は不充分

日本企業

情報セキュリティ

制御システムセキュリティ

ISO27000（ISMS）

IEC62443（CSMS）

一つのベンダ製品からデータを取り出してインターネットにアップして“見える化”する

競合しないサプライヤ仲間作り志向

ステップ2

欧米グローバル企業

- クラウドを活用したバリューチェーン

SCM、ERP、CRM

モデリング

標準化

制御システムセキュリティ

IEC62443（CSMS、SDLA、SSA、EDSA認証）

異なるベンダ製品からデータを取り出して、価値ある情報にして活用する

経営ニーズでソリューションを志向

ステップ3

Industry4.0／IICは、このレベルを目指して標準化活動している

- 現場のイノベーション

今までにない解決策

使えるAI

ビッグデータ処理

モデリング

標準化

IEC62541（OPC UA）

制御システムセキュリティ

IEC62443（CSMS、SDLA、SSA、EDSA認証）

時代に対応した現場にするべく、現場の課題を改善する技術革新

顧客の将来を考えるソリューション志向

問題は、IoT人材育成

これからのIoTシステムは、特に、広範囲で中身が深いです。

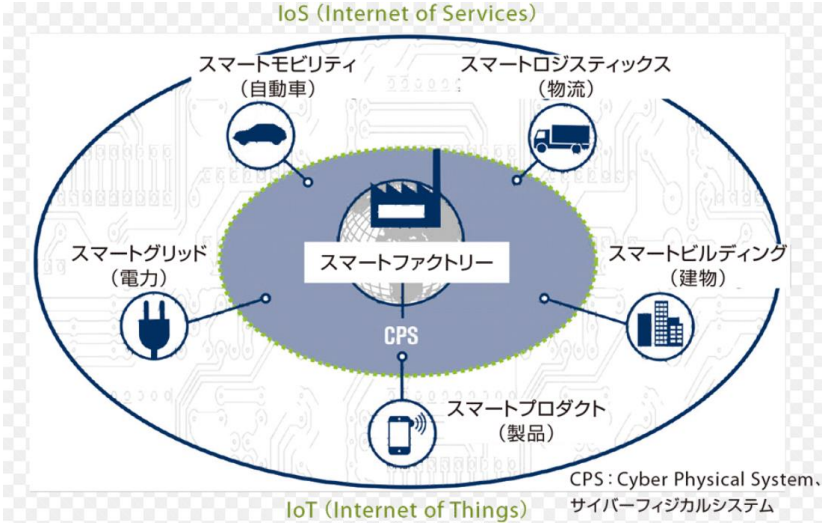
- 重要インフラから一般産業に至るまで、IoTシステムには制御システムセキュリティ対策が必要
- 特に、関連部門間をプロデュースできる人材が必要
- 当事者が制御システムセキュリティ対策を実施していくために必要な課題をこなせる実力を求められる
  - ◆ 一般社員の人材教育プログラム
  - ◆ 技術者の人材育成プログラム

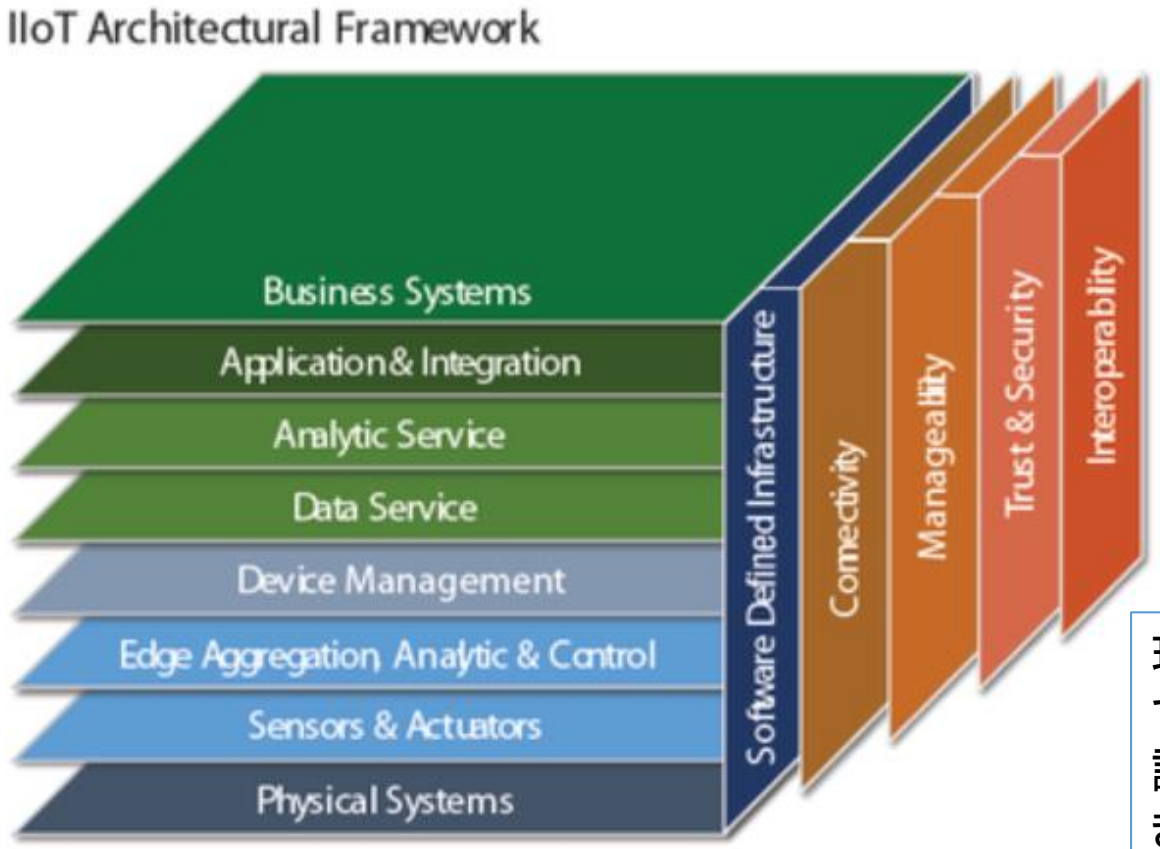
IoT人材育成対策

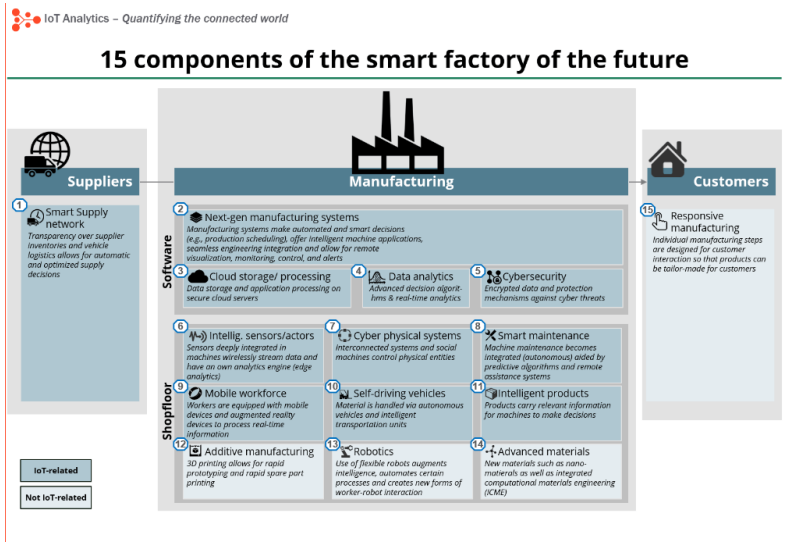
- ビジョン：どのような人材を必要となるか。その役割と素養とレベルを定義
- 課題と対策：IoT構築インフラ技術、国際標準技術、サイバーセキュリティ
- 教材と講師：コンテンツ教材、講師養成
- 実践トレーニング：テーマと成長レベルとコンセプトの定義、トレーナー養成

ユーザ企業内のIoT人材育成について
育成する人材像について

- 欧米と日本のIoTの違い
  - Industry4.0とIICに参画している企業のIoT







現場からデータや情報が上がってくればクラウドで対応できる。
課題は、現場から上げるデータや情報の中身を設計できるエンジニアが不足している。

人材育成における現状、課題と対応策

■情報技術者の教育しかなく、現場の制御システム担当者は、自分の問題と感じていないし、現場と連携してIoTを設計する人材がいない。

人材育成

現状

①日本におけるIoTイベントで発表されている内容は、「見える化」や欧米グローバル企業のソリューションを紹介しているものが多い。

②企業の中では、IoT情報収集にとどまっている企業が多い。

③パブリッククラウドとプライベートクラウドの区別が理解できていない企業人が多い。

④現場は、サイバー攻撃対策ができていないのに、インターネットやクラウドにつなげればIoTシステムができると考えている人が多い。

⑤業界特有のIoTのイノベーションが解らない。

課題

①現場とIoTの両方を理解した関連部門を連携した事業戦略を企画・推進・実現できるプロデュース人材がいない。

②IoTシステムで使用するオブジェクト対応のBDやAIを開発できるハイエンド技術人材がいない。

③IoTシステムをセキュアに構造設計できる技術者がいない。

④現場の施設や機械や装置やデバイスの制御システムセキュリティ対策ができていない。

⑤業界のIoTをけん引するイノベータがいない。

対応策

①部門を越えた技術やサービスの連携ができるプロデュース人材を育てる IoT事業戦略塾／コンサルティング

②課題を解決するためのBDやAIの構造設計ができる素養を持つ人材支援と環境整備

③IoTシステムをセキュアに構造設計できる技術を揃えた教育ツールを整備する。

④IoTシステム構造設計での制御システムセキュリティ対策教育ツール開発・検証ができるテストベッドを整備

⑤業界のIoT牽引イノベータ

要素定義と教材と講師と実践的トレーニング

- 人材育成要素：IoT構築インフラ技術、国際標準技術、サイバーセキュリティなどの要素定義
- 人材育成実施整備：教材づくり、講師養成
- 人材育成を支えるツールの開発
  - E-learning教育ビデオ講座⇒セキュアなIoTシステムを構築できる技術を習得
  - インシデント対応トレーニング（水処理、エネルギー管理など）⇒インシデント初動対応感性を育てる

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
	脅威と被害その1
	脅威と被害その2
	脅威と被害その3
	攻撃例の視点で見た制御システムその1
	攻撃例の視点で見た制御システムその2
	脆弱性情報対応基礎その1
	脆弱性情報対応基礎その2
	国際標準規格と認証機関
	世界のCSS機関
	制御システムセキュリティゾーン設計基礎
	制御システムセキュリティ対策の全体像と各手法
	認証 CSMS認証、SSA認証、EDSA認証
	インシデント対応基礎
	セキュア改善
	関連法規制について
企業経営における対策	脅威と被害と対策その1
	脅威と被害と対策その2
	脅威と被害と対策その3
	脅威と被害と対策その4
現場管理における対策	セキュリティ５Sの進め方
	セキュリティ５Sの事例その1
	セキュリティ５Sの事例その2
	現場での脅威と被害と対策
	セキュア改善前にすること
	現場用セキュリティ製品その1
	現場用セキュリティ製品その2
	現場用セキュリティ製品その3
	定期点検／修繕での作業
インシデント対応実践	インシデント対応実践
発注・受入・現場立ち上げ	要求仕様書
	工場立会試験
	受け入れ検査から試運転試験まで
ゾーン設計の技術	生産プロセス区分ゾーン設計
	制御系統のグループ区分ゾーン設計
	統括管理区分ゾーン設計
	ＳＩＳ区分ゾーン設計
	オペレーションゾーン設計
	フェイルセーフ区分ゾーン設計
	無線通信ゾーン設計
現場セキュア改善手順	現場セキュア改善手順
エンジニアリング	【前編】セキュアエンジニアリングその1
	【中編】セキュアエンジニアリングその1
	【後編】セキュアエンジニアリングその1
	セキュアエンジニアリングその2
	オペレーション・ゾーン設計
	【前編】要求仕様書から読み取る範囲
	【後編】要求仕様書から読み取る範囲
	発種もり設計でのセキュア仕様
	試験評価の方法
	試験方案でのセキュア試験
	設備保証と顧客サポート

カテゴリ	講座名
発注先監査	発注先監査
	監査基準項目と基準
	関連法規制
装置ベンダにおける対策	攻撃例の視点と対策機密情報
	脆弱性情報管理　その1
	脆弱性情報管理　その2
	脆弱性情報管理　その3
	設計環境整備と健全化管理
	設計仕様で対策できること
	試験評価の方法
	セキュア製品開発プロセス
	セキュア設計技術　その1
	セキュア設計技術　その2
	発注仕様書から納品まで
	設備保証と顧客サポート
	インシデント対応設計
	リモートサービス
機械ベンダにおける対策	攻撃例の視点と対策　機密情報
	脆弱性情報管理　その1
	脆弱性情報管理　その2
	脆弱性情報管理　その3
	設計環境整備と健全性管理
	設計仕様で対策できること
	試験評価の方法
	セキュア製品開発プロセス
	セキュア設計技術　その1
	セキュア設計技術　その2
	発注仕様書から納品まで
	設備保証と顧客サポート
	インシデント対応設計
	リモートサービス
制御ベンダ	制御ベンダの取り組みその1
	制御ベンダの取り組みその2
	脆弱性情報管理その1
	脆弱性情報管理その2
	脆弱性情報管理その3
	設計環境整備と健全性管理
	【前編】セキュア製品開発その1
	【後編】セキュア製品開発その1
	セキュア製品開発その2
	セキュア製品開発プロセス
	セキュア評価その1
	セキュア評価その2
	攻撃例の視点から見た機密情報
	製品仕様で対策できることその1
	製品仕様で対策できることその2
認証	認証の目的と期待効果
	第三者認証
	CSMS認証
	SSA認証
	EDSA認証
	Achilles認証
	自己認証
システムインテグレータ	仕様書から対策設計の範囲の読み取り
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