# Web端末型IoTプラットフォーム ia-cloudの概要

## 真のIoT・Industrie4.0を目指して

RRI第10回 IoTによる製造ビジネス変革WG会合

2016/8/5

産業オートメーションフォーラム　ia-cloudプロジェクトリーダ

@bridge consulting　橋向　博昭



## 本日お越しの皆様は？

- 講演内容のフォーカスを調整するため、お聞かせください。
  皆様のお仕事は、どれに最も近いですか。

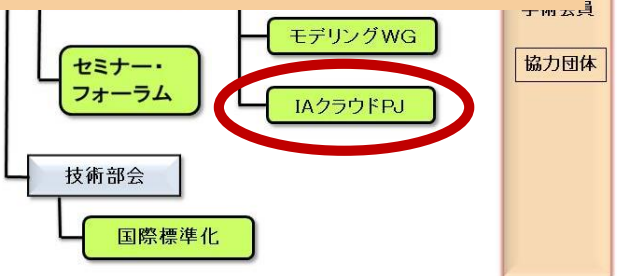
- 計測制御機器・システムベンダー
- 生産システム系SIer
- 情報系SIer
- 生産設備機器・ユーティリティ機器ベンダー
- 製造業ユーザ企業

# 産業オートメーションクラウド（ia-cloud）プロジェクト

- 製造科学技術センター
  産業オートメーション
  傘下のプロジェクト
- ia-cloud API仕様の策
- 構成
  - リーダ
    @bridgeコンサルティン
  - メンバ（五十音順）

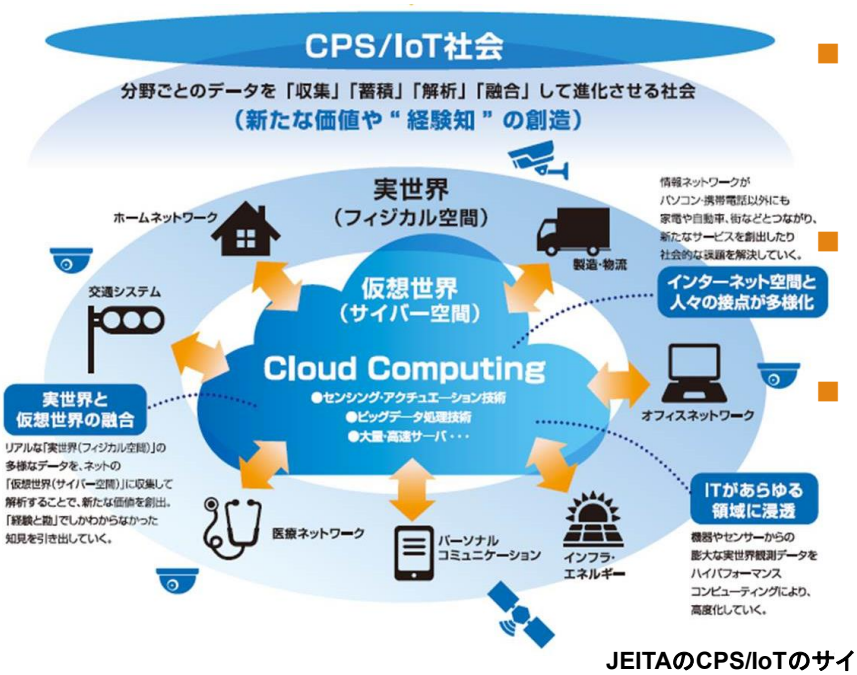
    伊藤ソフトデザイン
    エス・ジー、エムシステム
    オムロン、クオリカ
    ケー・ティー・システム
    産業インテグレーションサービス
    デジタル、日立製作所
    ものづくりAPS推進機構（CIMX、富士通）
    安川電機

- **目的**
  - 産業オートメーション（IA）分野において、様々なIA関連の設備・機器・システムが保持する情報を、クラウドサービスで利用できる共通的な仕組みを構築する。
  - IA分野におけるクラウドサービスを実現する、基本プロトコルとデータオブジェクトフォーマットを規定する規格を作成する
  - 既存のオープンで標準的な技術・規格を利用し、必要な拡張と特化を行う。






# IoT社会とはどんな社会？




JEITAのCPS/IoTのサイトから

- CPS(Cyber Physical System)社会とは、サイバー空間と実世界が繋がり、相互の密接な関係を形成し融合した社会。
- CPS/IoT社会は、実世界をサイバー空間に繋ぐことで実現する社会。
- 実世界の人々、様々な「もの」、「こと」がサイバー空間に繋がり、相互に情報交換をし、新しい価値を創造する世界。

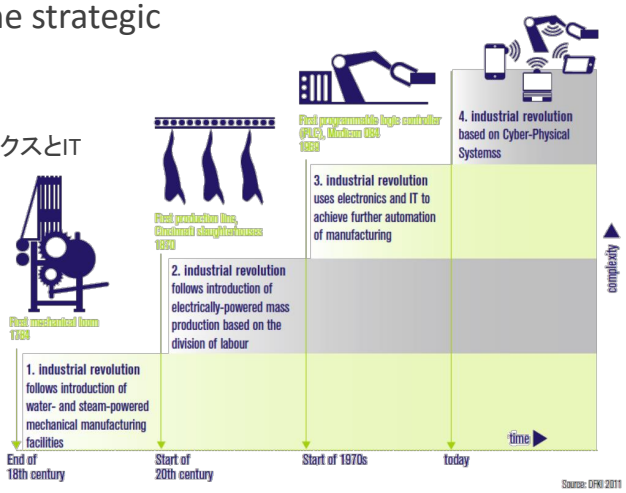
# IoTの「I」はInternetの「I」

- **Internet** of Things (IoT)
  - ◆モノやコトがインターネットに繋がること
- Industrial **Internet** of Things（IIoT）
  - ◆GEの航空機エンジンの事例はほんとにインターネットに繋がってるのか？
  - ◆コマツのKOMTRAXはインターネット、サイバー空間上にあるの？
  - ◆これらのベストプラクティスが持つ意味は極めて大きいが、サイバー空間の片隅に乗っているだけで、インターネットとは言えないのでは？
- 現在提供されているM2Mと呼ばれるデータ収集サービスのほとんどが携帯通信網でインターネット接続を実現しており、より幅広く簡便で安価な接続が期待される。
- **インターネットに繋がって初めて、IoTじゃないの？**



# Industrie 4.0は、今まで（3.x）と何が違うのか

- Recommendations for implementing the strategic initiative INDUSTRIE 4.0 によれば
  - ◆ 産業革命のドライビングフォースは
    - ✓ 1：水力・蒸気力、2：電気エネルギー、3：エレクトロニクスとIT
    - ✓ **4：Cyber-Physical Systemsに基づく革命**
- **サイバー空間に繋がることでそこで何が起こり、どう進化するのか、語っている。**
- **サイバー空間に接続できない、（CPSに基づかない）システムは、Industrie3.0の進化（3.9?）であり、4.0 ではない。**
- **サイバー空間とつながることにより、人と機械がコラボできる。**

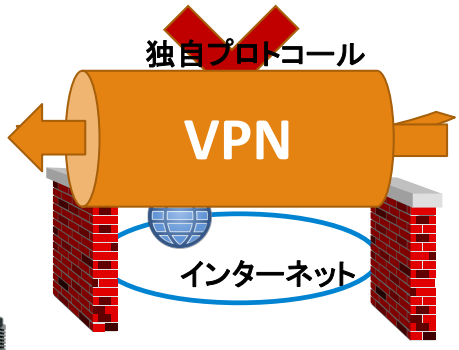


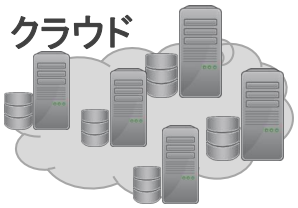

- **サプライチェーンの情報連携が可能となりマスカスタマイゼーションが可能となる。**

- **しかし、Industrie4.0の様々なドキュメント・事例も、どうやってインターネットに繋がり、どのように情報連携が可能なのかについて、多くを語っていない。**

# 設備メーカ、計測制御機器メーカが独自仕様の通信。繋がらない。

- 各メーカの独自仕様である、PLCやロボットコントローラの上位通信、NCコントローラとの通信は、ファイアーウォールの外からは使えない。
- いずれも外部からの通信コマンドを受け実行する。



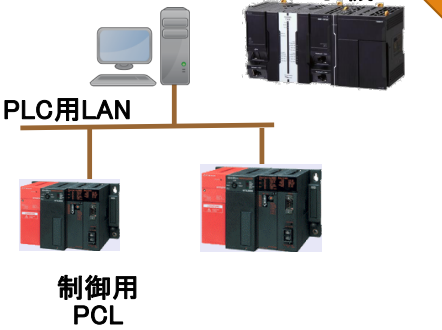

- クラウドサービスは、Webサーバから提供される。
- 使うプロトコールは、http。

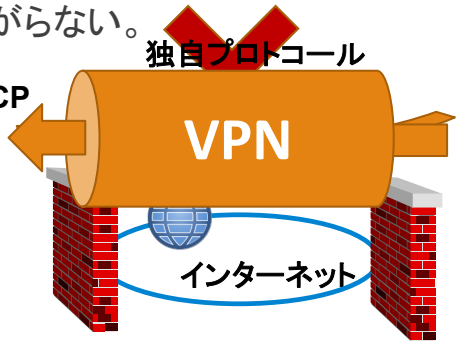
- メーカ独自の通信仕様
- シリアル通信機器も多数存在

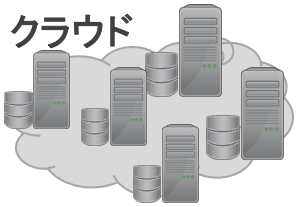


# 製造業分野にも、共通プロトコールやデファクト標準規格はある。でも・・・

- PLC通信のデファクト標準となったModbus/TCPも、上位からの通信コマンドを受けるもので、ファイアーウォールの外へは出られない。
- OPC-UAのSOAP/XMLプロトコールだけは、ファイアーウォールを外向きには通過できるが、OPC-UAサーバがファイアーウォールの内側にあるのでやっぱり繋がらない。




- クラウドサービスは、Webサーバから提供される。
- サーバから、工場内部へは接続できない

# Industrie4.0には何と書いてある？

## Today

Remote Service is enabled by the establishment of individual communication solutions between the machine supplier and the user. The technician generally connects to the machine directly via a modem. Since the advent of the Internet, VPN connections (Virtual Private Networks) have also gained in popularity, since they allow secure access to the customer's corporate network. The goal of this approach is to remotely diagnose and control the machine in order to reduce the duration of unscheduled stoppages and downtime.

従来は個別の通信手段によるリモートサービス
インターネットの登場で、VPNが普及

しかし、設定管理の仕事量が膨大

The configuration and administration of the communication links involves a significant amount of management work, since the conditions of use need to be agreed separately with each customer. Moreover, this approach can currently only be used to provide reactive services, i.e. to carry out maintenance after an incident has occurred.

## Tomorrow

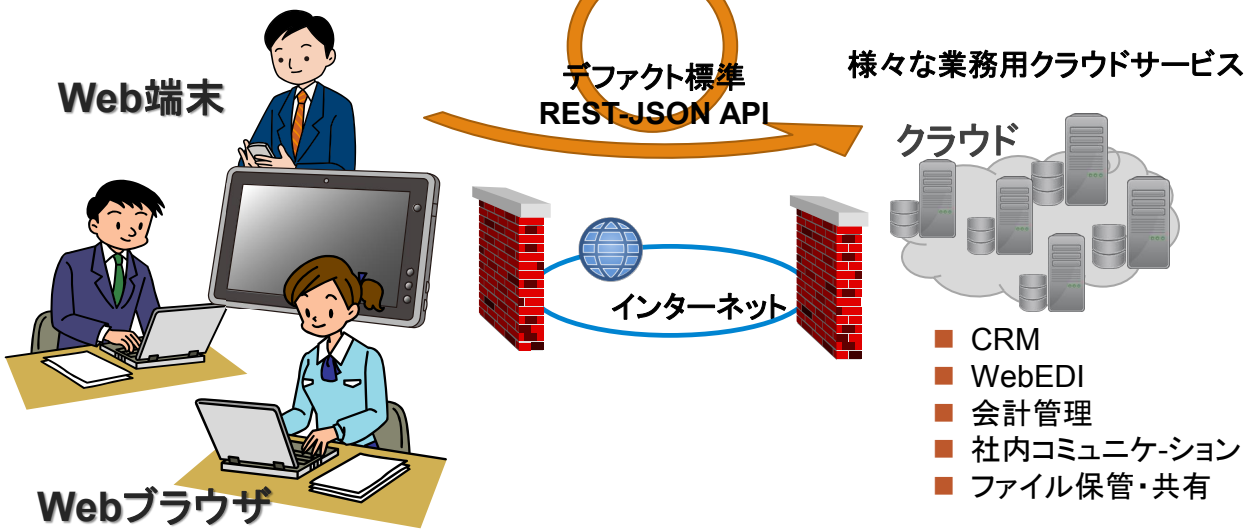
In Industrie 4.0, technicians will no longer manually connect to the machine they are servicing. Manufacturing systems will operate as "social machines" – in networks that are similar to social networks – and will automatically connect to cloud-based telepresence platforms in order to search for the appropriate experts to deal with the situation in question. The experts will then be able to use integrated knowledge platforms, videoconferencing tools and enhanced engineering methods to perform traditional remote maintenance services more efficiently via mobile devices. Moreover, machines will continuously enhance and expand their own capabilities as the situation requires by automatically updating or loading the relevant functions and data via standardised, secure communication links with the telepresence platforms.

Industrie4.0では、個別の接続は不要。
ネット上の「ソーシャル・マシン」が、SNS のように
クラウドベースのプラットフォームに繋がる。



# 各種業務システムは クラウド利用ができる。なぜ？

- CRMや会計ソフト等、多くの業務系クラウドサービスが利用できるのはなぜ？
- 今や、基幹システムさえもクラウドにおく時代、あらゆる業務システムがクラウドサービスで提供されている。



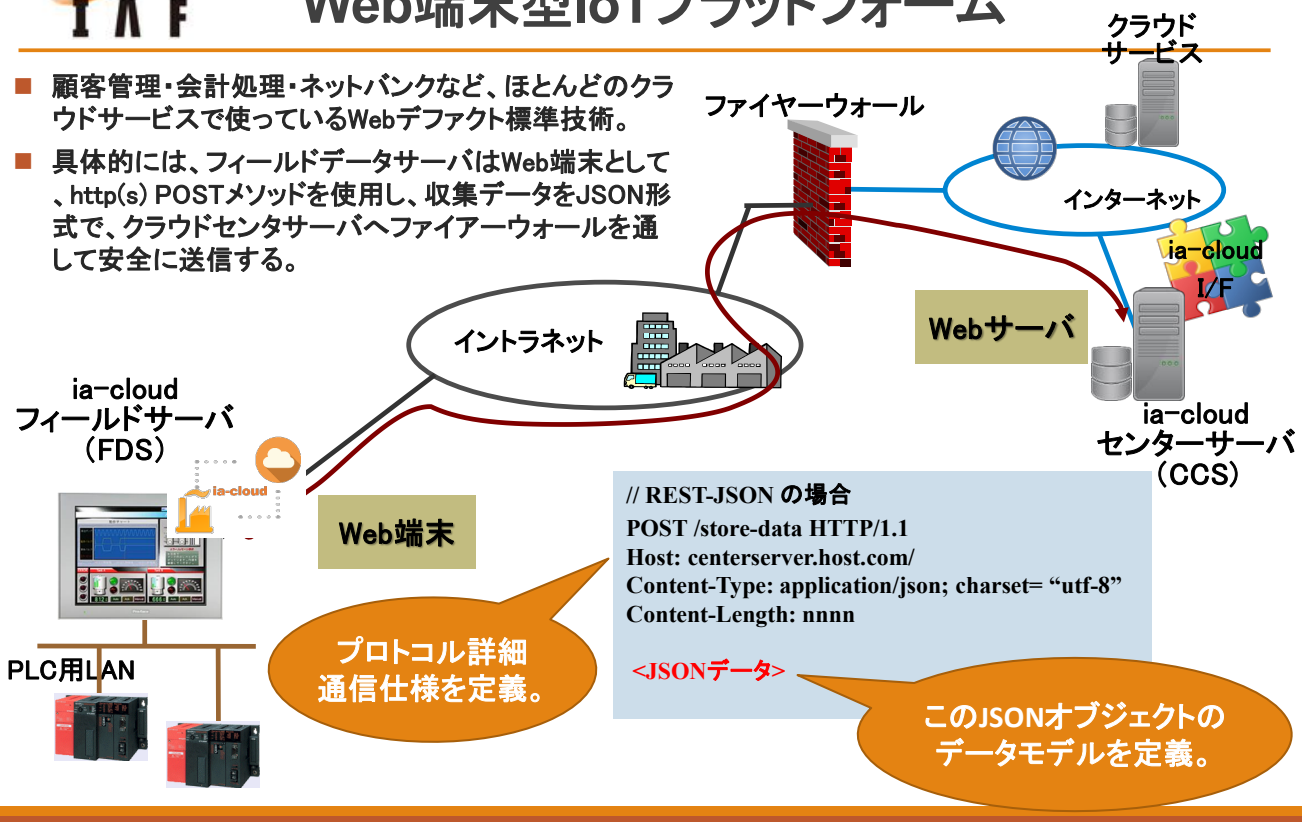

- CRM
- WebEDI
- 会計管理
- 社内コミュニケ-ション
- ファイル保管・共有

# Web端末型IoTプラットフォーム ia-cloud

- Web端末型IoTプラットフォーム、ia-cloud のAPIを実装した設備、計測制御機器、ゲートウエイで、製造業関連の様々なアプリケーションが、クラウドサービス化する。

# ia-cloudの技術的基盤 Web端末型IoTプラットフォーム

- 顧客管理・会計処理・ネットバンクなど、ほとんどのクラウドサービスで使っているWebデファクト標準技術。
- 具体的には、フィールドデータサーバはWeb端末として、http(s) POSTメソッドを使用し、収集データをJSON形式で、クラウドセンタサーバへファイアーウォールを通して安全に送信する。



# インターネット上のサイバー空間で初めて、隅々までIoTの恩恵が届く

- インターネットインフラとインターネット技術を利用することで、データの収集・蓄積・利用のビット単価が究極なまでに低減する。
- そのことによって、CPSが産業の隅々にまで普及・浸透することが可能となる（Industrie4.0）
  - ◆サプライチェーンの最上流から最下流まで
  - ◆大企業から中小企業まで
- 縦、横、深さ方向の情報連携の広がりにより、情報の価値が向上する。
- クラウド上の様々なデータ利活用技術、サービスと連携できる。

- **インターネットを使い、スケールアウトを起さなければ、IoT・第4次産業革命は、中小企業までは届かない。**



# インターネットを使って、セキュリティは大丈夫なのか？

| セキュリティ上の懸念 | 実際上の脅威 | 対策と効果 | 備考 |
|---|---|---|---|
| クラウド上に格納された情報の漏洩懸念 | クラウドサーバへの不正アクセスによる情報漏洩。<br>・ セキュリティホール<br>・ 成りすましによるアクセス<br>・ 情報管理権限者の不正 | クラウドサービスの提供業者を正しく選択し、クラウドサーバへの認証、アクセス制限を正しく設定することで、リスクを十分に低減できる。 | 実際の情報漏洩は、オンプレかDCのプライベートシステムで多く発生している。クラウドからの大きな情報流出インシデントはない。 |
| クラウドと接続されたIoT機器へのインターネットからの攻撃懸念 | IoT機器が直接インターネットに接続されている場合、様々な攻撃に晒される可能性大きい<br>・ IoT機器のセキュリティホール<br>・ 各種のDOS攻撃 | IoT機器をFirewallの内側へ設置し、外部からの直接アクセスを禁止。<br>携帯通信網への接続の際は、アクセス制限の可能なサービスを利用 | IoT機器は、グローバルIPを付与せず、インターネットから直接アクセスできないようにすべき。<br>IPv6での、IoT機器の直接接続は時期尚早。 |
| 生産関連システムや制御システムがインターネットから攻撃される不安 | IoT機器の接続経路からの、システムへの不正アクセスの懸念 | IoT機器をFirewallの内側へ設置し、外部からのアクセスを禁止。<br>ホワイトリストタイプのプロキシサーバ経由で、さらに強固な防御 | 社内イントラネットは、強固なFirewallの内側であるのが常識。 |

# インターネットを使って、セキュリティは大丈夫なのか？

| セキュリティ上の懸念 | 実際上の脅威 | 対策と効果 | 備考 |
|---|---|---|---|
| クラウ<br>情報 | の不正ア<br>洩。<br>るアクセス<br>情報管理権限者の不正 | クラウドサービスの提供業者を正しく選択し、クラウドサーバへの認証、アクセス制限を正しく設定することで、リスクを十分に低減できる。 | 実際の情報漏洩は、オンプレかDCのプライベートシステムで多く発生している。クラウドからの大きな情報流出インシデントはない。 |
| クラウドと接続さ<br>IoT機器へ | IoT機器が直接インターネットに接続されている場合、<br>に攻撃に晒される可能<br>リティホ | IoT機器をFirewallの内側へ設置し、外部からの直接アクセスを禁止。<br>携帯通信網への接続の際は、アクセス制限の可能なサービスを利用 | IoT機器は、グローバルIPを付与せず、インターネットから直接アクセスできないようにすべき。<br>IPv6での、IoT機器の直接接続は時期尚早。 |
| 制<br>インターネット<br>される不安 | からの、<br>不正アクセス<br>の懸念 | IoT機器をFirewallの内側へ設置し、外部からのアクセスを禁止。<br>ホワイトリストタイプのプロキシサーバ経由で、さらに強固な防御 | 社内イントラネットは、強固なFirewallの内側であるのが常識。 |

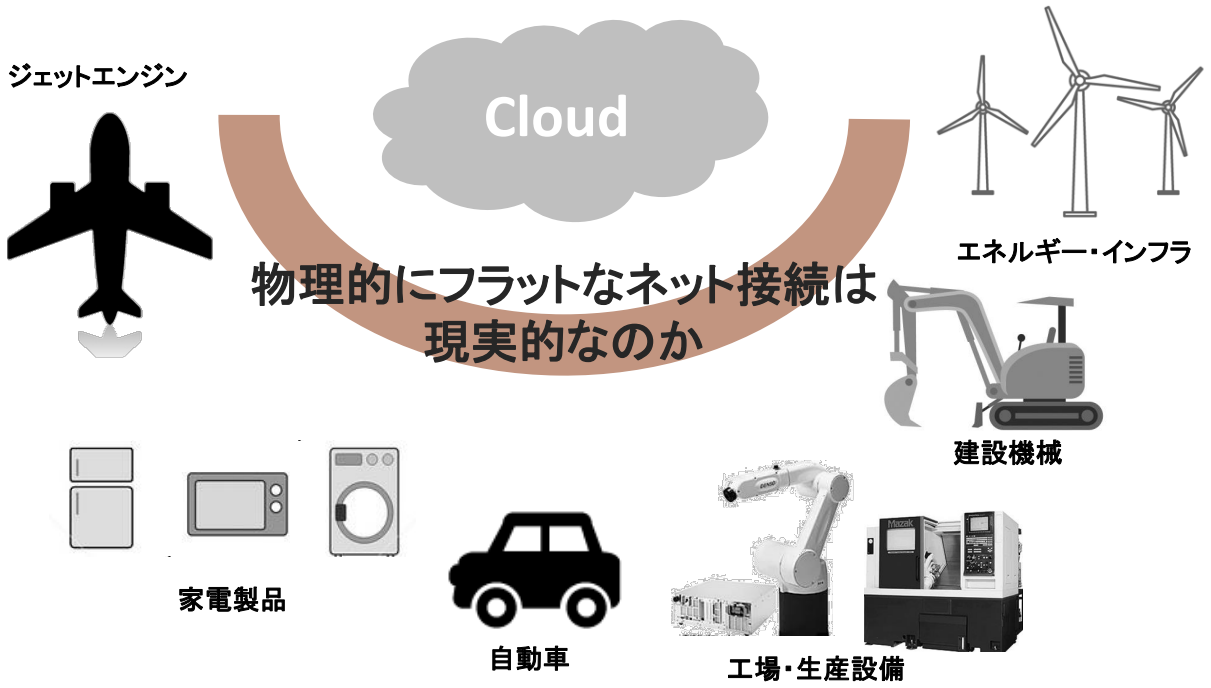
CRMや会計システムから
ERPまでもがクラウドへ

疎結合のia-cloud なら、

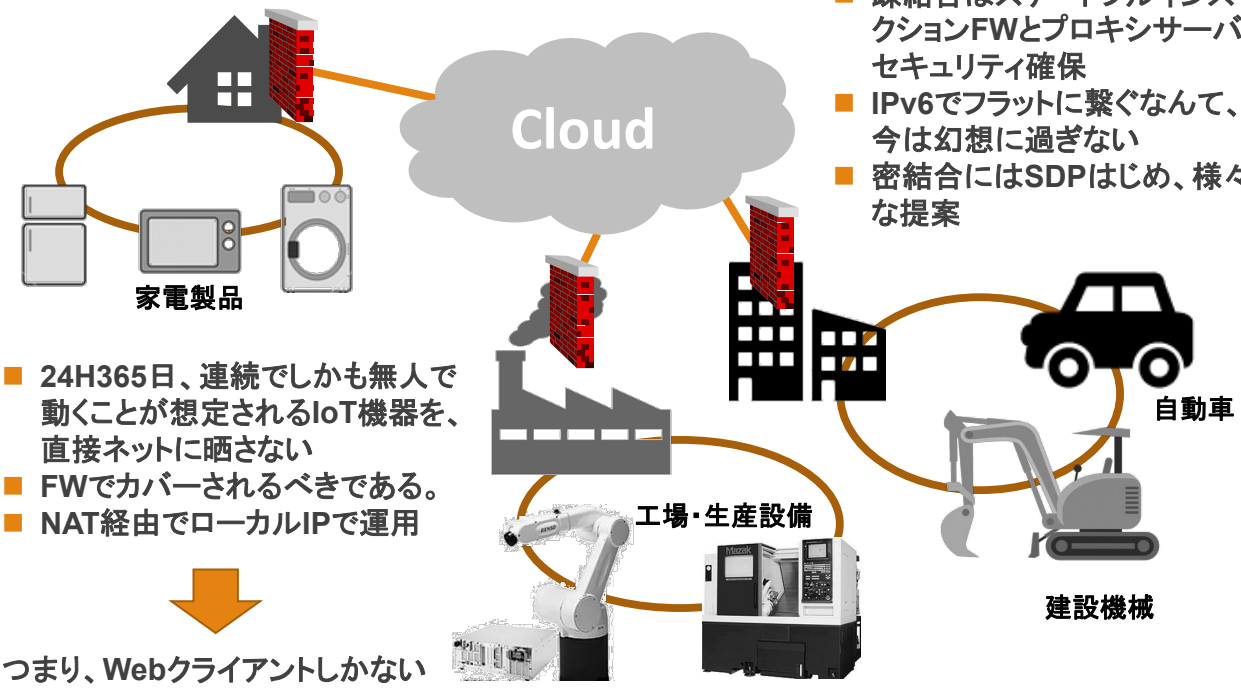
一般的なFWとProxyサーバ
に守られた内側からクラウド
接続が可能



# セキュリティを確保するためには



# セキュリティを確保するためには



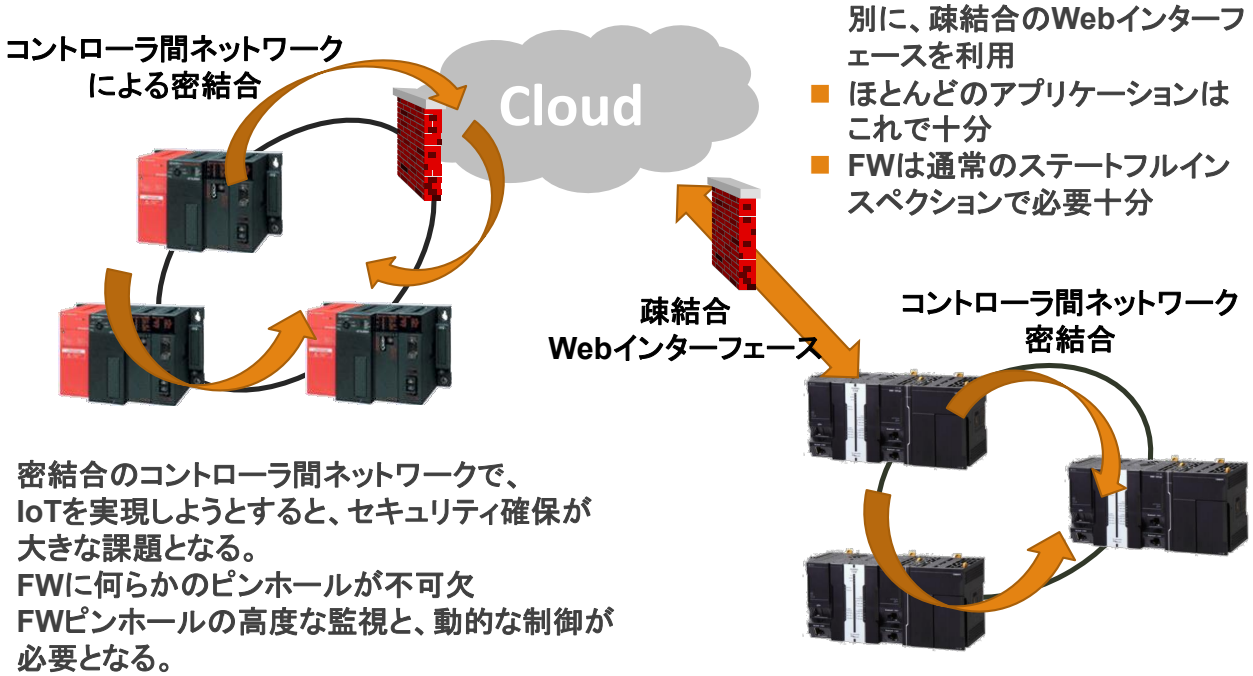

- 疎結合はステートフルインスペクションFWとプロキシサーバでセキュリティ確保
- IPv6でフラットに繋ぐなんて、今は幻想に過ぎない
- 密結合にはSDPはじめ、様々な提案

- 24H365日、連続でしかも無人で動くことが想定されるIoT機器を、直接ネットに晒さない
- FWでカバーされるべきである。
- NAT経由でローカルIPで運用

つまり、Webクライアントしかない



# 密結合と疎結合




- コントローラ間ネットワークとは別に、疎結合のWebインターフェースを利用
- ほとんどのアプリケーションはこれで十分
- FWは通常のステートフルインスペクションで必要十分

- 密結合のコントローラ間ネットワークで、IoTを実現しようとすると、セキュリティ確保が大きな課題となる。
- FWに何らかのピンホールが不可欠
- FWピンホールの高度な監視と、動的な制御が必要となる。

# 生産設備・計測制御機器が インターネットに繋がらないのは、なぜ？

- 産業オートメーションシステム・計測制御機器の多くは、各ベンダーが独自仕様のTCP/IPなどを利用した、通信仕様を搭載しており、セキュリティー上の問題で、インターネットに接続できない。
- そのほとんどが、機器のメモリイメージの直接表現であり、構造化され、意味付けされたデータ表現になっていないため、個別の知識を持った解釈評価が必要で、情報連携や共有ができない。

**だから**
**ia-cloud**

- Webクライアントの業界標準プロトコールREST-JSONで、インターネットに安全に接続
  - IoH(Internet of Human)は、Web端末型の業界標準を利用している。
  - CRMや会計処理などの業務クラウドサービスも同様の業界標準で安全にインターネットを利用
- JSONで記述された業界標準データフォーマットを定義



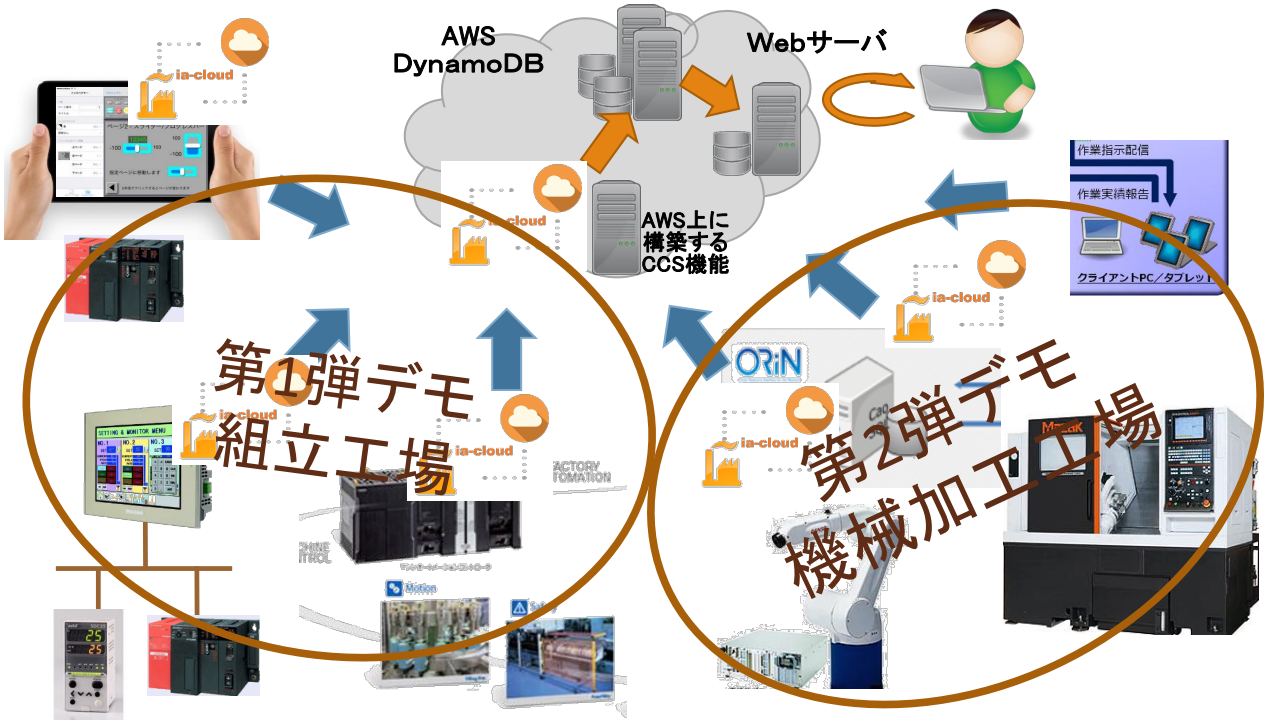
# ia-cloud REST-JSON API仕様書

- 現在のバージョンは 0.63β
- Webクライアントの業界標準プロトコール REST-JSONに基づき、通信仕様を定義
  - 認証方式とTLS1.2を必須とする
  - REST uri を定義
  - 操作コマンドのJSONを定義
- JSONで記述された業界標準データフォーマットを定義
  - オブジェクトモデル
    オブジェクトIDとタイムスタンプでインスタンスキーを構成
  - データモデル
    設備機器の状態データや稼働状況、警報状態などのデータモデルをJSONで定義
- ia-cloudメンバで共有中、2.0の策定を開始する段階で、1.0を一般公開予定。

目次


1 目的
2 概要
2.1 ia-cloud フィールドデータサーバ（FDS）
2.2 ia-cloud センターサーバ（CCS）
3 REST プロトコール
3.1 ia-cloud サービスの uri
3.2 認証と Https
3.3 サービスのリクエスト
3.3.1 接続の開始
3.3.2 データオブジェクトインスタンスの格納
3.3.3 データオブジェクトインスタンスの取得
3.3.4 状態の確認（serviceID の更新）
3.3.5 接続の終了
3.4 CCS 側からの下り通信（オプション）
3.4.1 方針
3.4.2 Web-Socket コネクションの確立
3.4.3 利用可能な Method の通知
3.4.4 CCS 側からの Method 呼び出し
3.5 Http(s)エラー処理
4 ia-cloud オブジェクト
4.1 オブジェクトモデル
4.2 オブジェクトアレイモデル
5 ia-cloud データモデル
5.1 基本データモデル
5.2 生産実績データモデル
5.3 在庫実績データモデル
5.4 品質データモデル
5.5 装置ステータスモデル
5.6 エラーステイタスモデル （エラー番号を格納）
5.7 コントロールポイントモデル
5.8 温度調節計モデル
5.9 アクチュエーターモデル
5.10 インバータモデル
5.11 ロボット ORiN データモデル
5.12 PLC レジスタモデル
5.13 USER Defined Data Model

# 生産システム見える化展デモの概要






# Web端末型IoTプラットフォーム ia-cloudの発表セミナー「実証デモ」

# 今後の計画

- 実証実験
  - ◆発表セミナーとデモ展示、6月23日、機械振興会館（完了）
  - ◆生産と設備TOKYO2016、「生産システム見える化展」に出展
    - ✓7月20日～22日　ビッグサイト（完了）
      ものづくりAPS推進機構（APSOM）の「つながる工場」PSLX3とも連携
  - ◆11月に第2弾のデモ・セミナーを予定（ORiNとの連携）
- 実証事業
  - ◆実際の製造現場等でia-cloud機器とクラウドサービスを利用し、その利用技術の開発とデータモデルの追加・仕様の拡張を行う。
- Websocketによる、API仕様の強化
  - ◆他のWeb非対応通信を、ia-cloud のWebsocketにパックすることで、クラウド利用を可能とする技術開発



# ご清聴ありがとうございました。

ご質問は、下記までいつでもお気軽にお寄せください。

consulting@hashimukai.com
http://www.atbridge-cnsltg.com
https://www.facebook.com/atbridgecnsltg