OPC UAの効能
～OPC UA技術のおさらい～

2023年12月7日

日本OPC協議会 技術部会長
樋口 毅(三菱電機(株))

OPC の 理念 を実現する 3 + 1 の コンセプト

Utilized
活用する

情報を価値に変える

Connected
つなげる

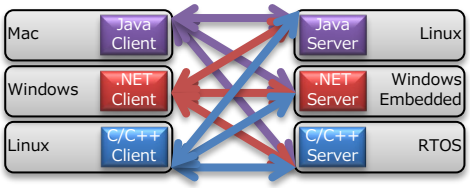
データを確実（堅牢性、信頼性）に伝送する

Communicated
伝える

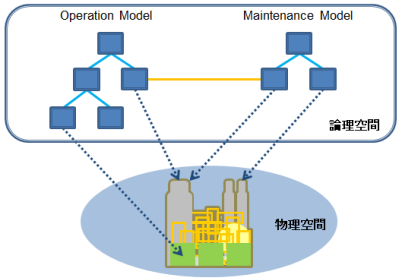
情報を正確（表現、解釈）に伝達する

Secured
安全に

データ/情報の完全性及び、機密性を保証する



プラットフォーム非依存



情報モデル

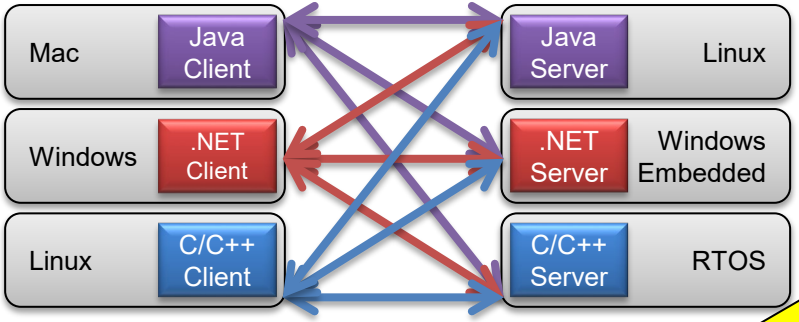
セキュリティ

Agenda

- つなげる
- 安全に
- 伝える

プラットフォーム非依存と二つの通信モデル

プラットフォーム非依存

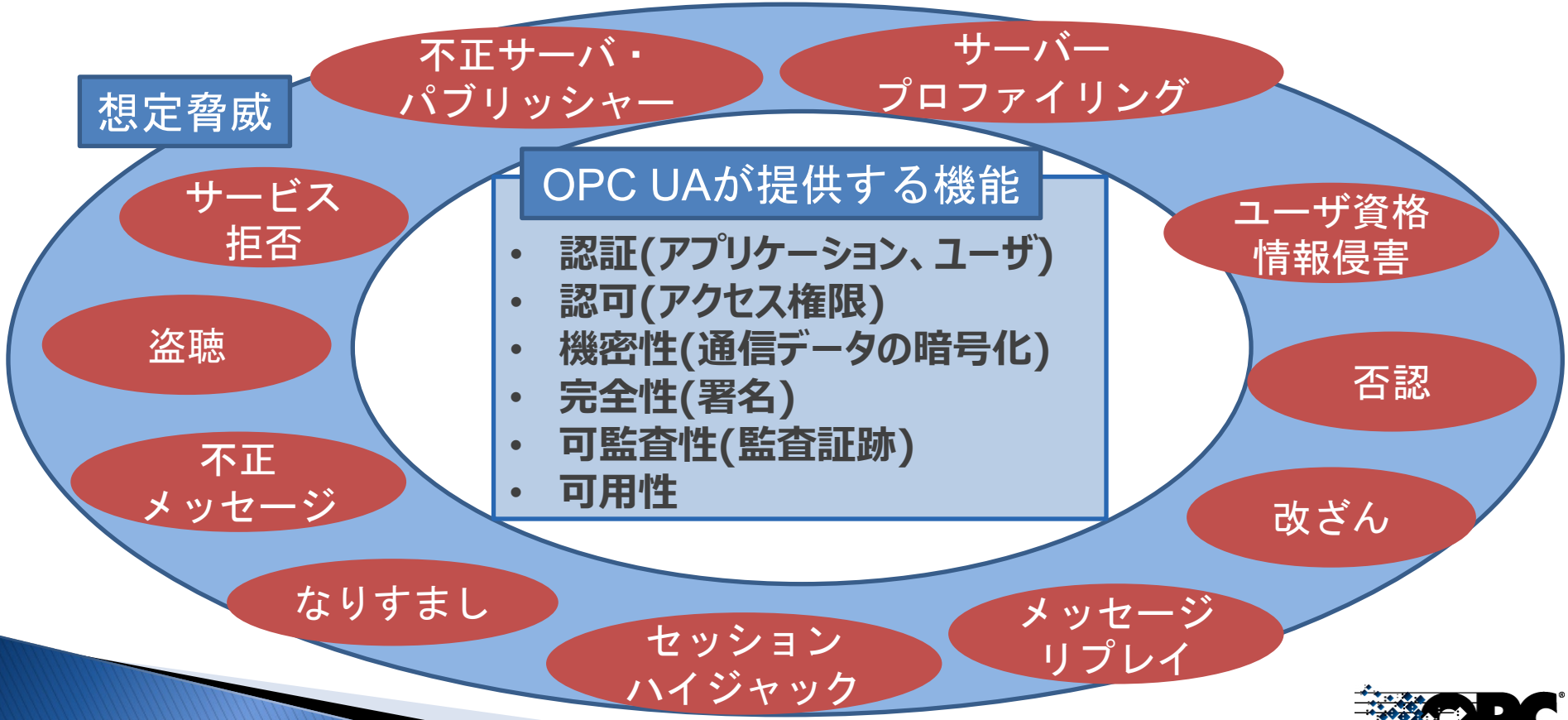


二つの通信モデル

Agenda

- つなげる
- 安全に
- 伝える

想定脅威と提供機能


想定脅威
不正サーバ・
パブリッシャー
サーバー
プロファイリング
サービス
拒否
ユーザ資格
情報侵害
盗聴
否認
不正
メッセージ
改ざん
なりすまし
セッション
ハイジャック
メッセージ
リプレイ
OPC UAが提供する機能
• 認証(アプリケーション、ユーザ)
• 認可(アクセス権限)
• 機密性(通信データの暗号化)
• 完全性(署名)
• 可監査性(監査証跡)
• 可用性

セキュリティ機能

- 認証
  - アプリケーション認証、ユーザ認証の仕組みを提供
- 認可
  - ユーザ認可の仕組みを提供
- **機密性・完全性**
  - セキュリティモード、セキュリティポリシーを指定することで適用される
- 可監査性
  - セキュリティ関連の操作の監査イベントを生成
  - ただし、アプリケーションに関する情報も監査対象とする場合のイベントの生成は作りこみが必要
- **可用性**
  - 接続処理に関する可用性を考慮している

セキュリティプロファイル	設定値
セキュリティモード	None
	Sign
	SignAndEncrypt
セキュリティポリシー	署名と暗号化のアルゴリズム
	キー導出のアルゴリズム

ISA/IEC62443への考慮

- ISA/IEC62443-4-2への適用を考慮
- ISA/IEC62443-4-2 SL2(偶発的な事故や通常のサイバー攻撃に対応が可能なレベル)の要件とOPC UAが提供している機能のマッピングを明確化
- OPC UAを使うことで国際規格への対応が容易に

Table A.2 – IEC62443 to OPC UA Mapping

ISA-62443-4-2 SL2 CRs and Res	Applies to OPC UA	OPC UA Part #	OPC UA Profile/ Facet/Conformance Unit (CU)
CR 1.1: Human user identification and authentication	Y	Part 4	IssuedIdentityToken
		Part 6	JSON Web Token (JWT), JWT UserTokenPolicy
		Part 7	Security User JWT IssuedToken, Security User JWT Token Policy, OPC UA Authority Profile
RE (1): Unique identification and Authentication	Y	Part 4	IssuedIdentityToken
		Part 6	JSON Web Token (JWT), JWT UserTokenPolicy
		Part 7	Security User JWT IssuedToken, Security User JWT Token Policy, OPC UA Authority Profile
			User Token JWT Server Facet, User Token JWT Client Facet
CR 1.2: Software process and device identification and authentication	Y	Part 2	ApplicationAuthentication, X.509 v3 Security Certificates
		Part 4	ApplicationInstance Security Certificate
		Part 4	EndpointDescription.EndpointUrl, Hostname (Device)
		Part 7	Security Default ApplicationInstance Security Certificate, Global Security Certificate Management Server Facet
CR 1.3: Account management	N		
CR 1.4: Identifier management	Y	Part 4	UserIdentityToken.UserTokenPolicy
		Part 7	Security User JWT IssuedToken, Security User JWT Token Policy, OPC UA Authority Profile
			User Token JWT Server Facet, User Token JWT Client Facet
CR 1.5: Authenticator management	Y	Part 4	UserIdentityToken.UserTokenPolicy
		Part 7	Security User JWT IssuedToken, Security User JWT Token Policy, OPC UA Authority Profile
			User Token JWT Server Facet, User Token JWT Client Facet
CR 1.7: Strength of password based authentication	N		
CR 1.8: Security certificates	Y	Part 2	Security Certificates, TrustLists (CertificateStore), OPC UA

OPC10000-2 OPC Unified Architecture Part2: Security Model Release 1.05.02より抜粋

Agenda

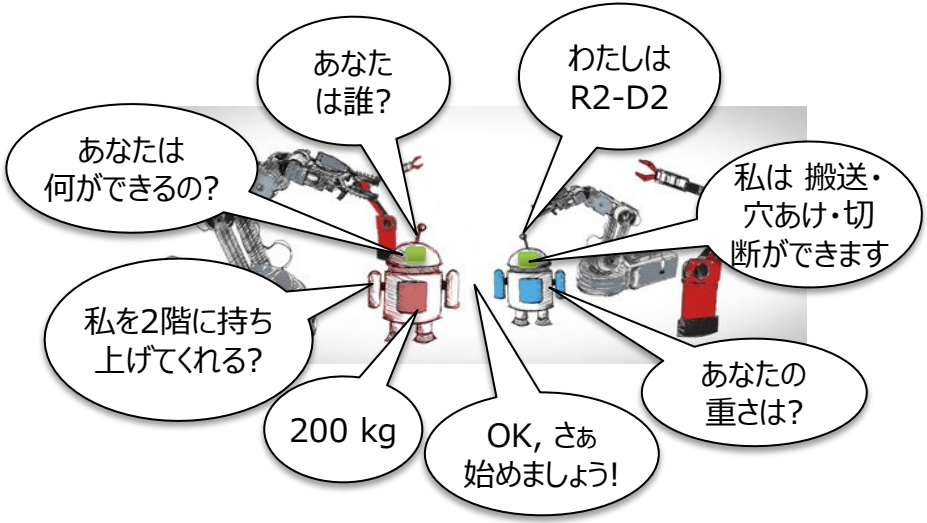
- つなげる
- 安全に
- 伝える

「伝える」とは

従来(Before)： データが交換される

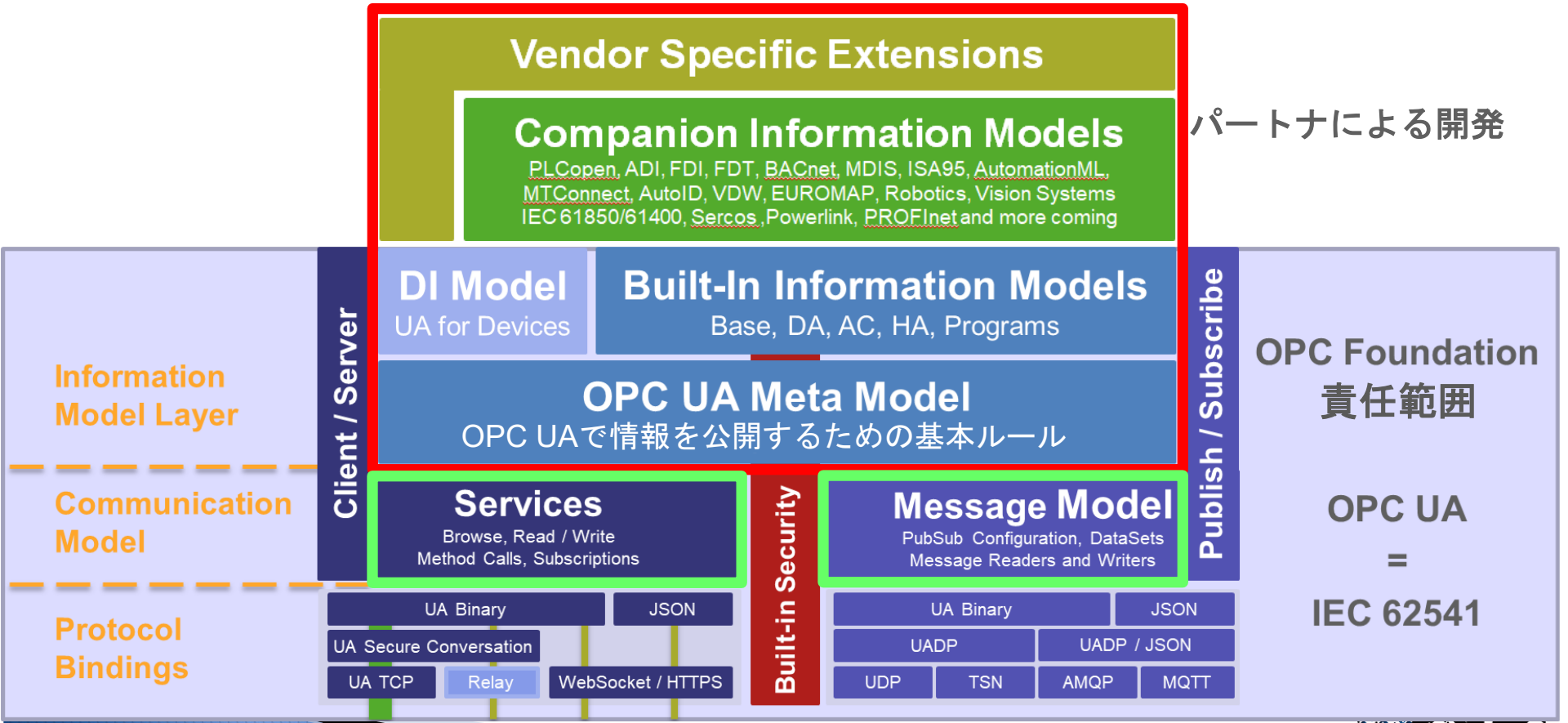
DATA TABLE 5
WORD0 = 0x5128
WORD1 = 1111000010101001
WORD2
WORD3
…
WORD255

今後(After)： 意味がつたわる

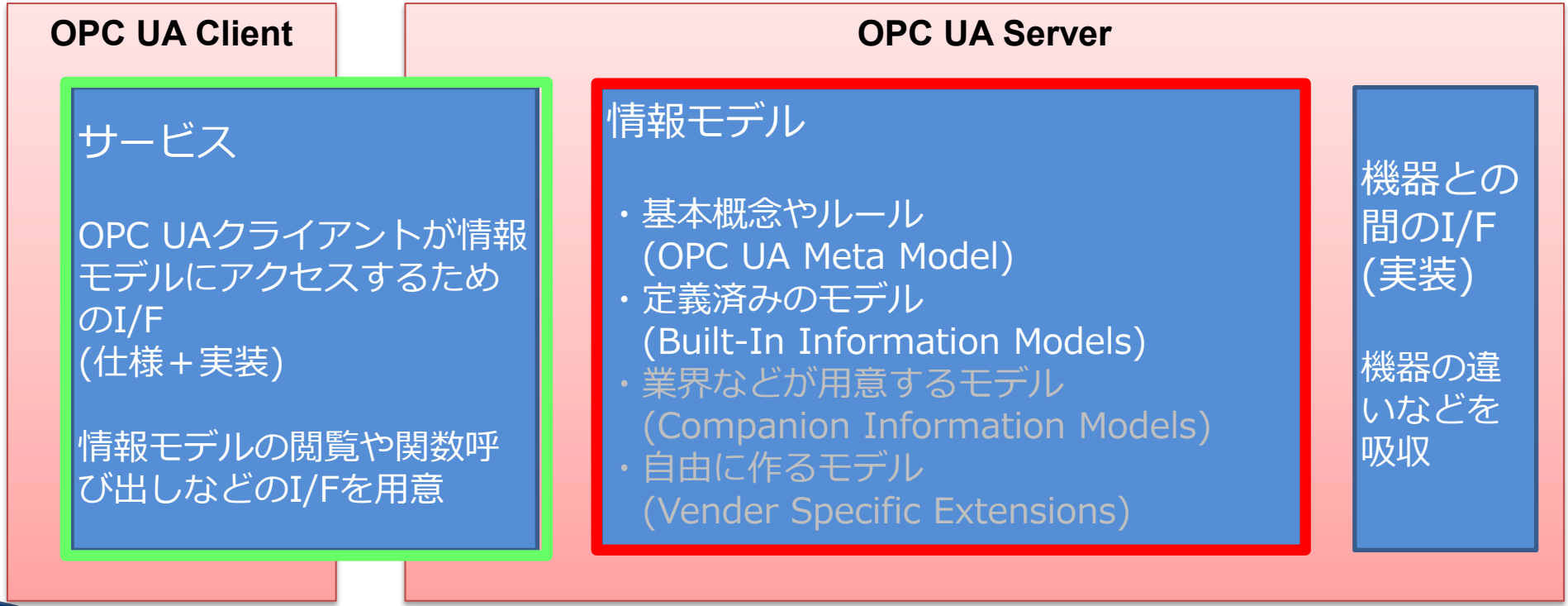


- ドキュメント化に多大な労力
- ベンダ毎にパラメータが異なる
- 人間が理解するために努力している

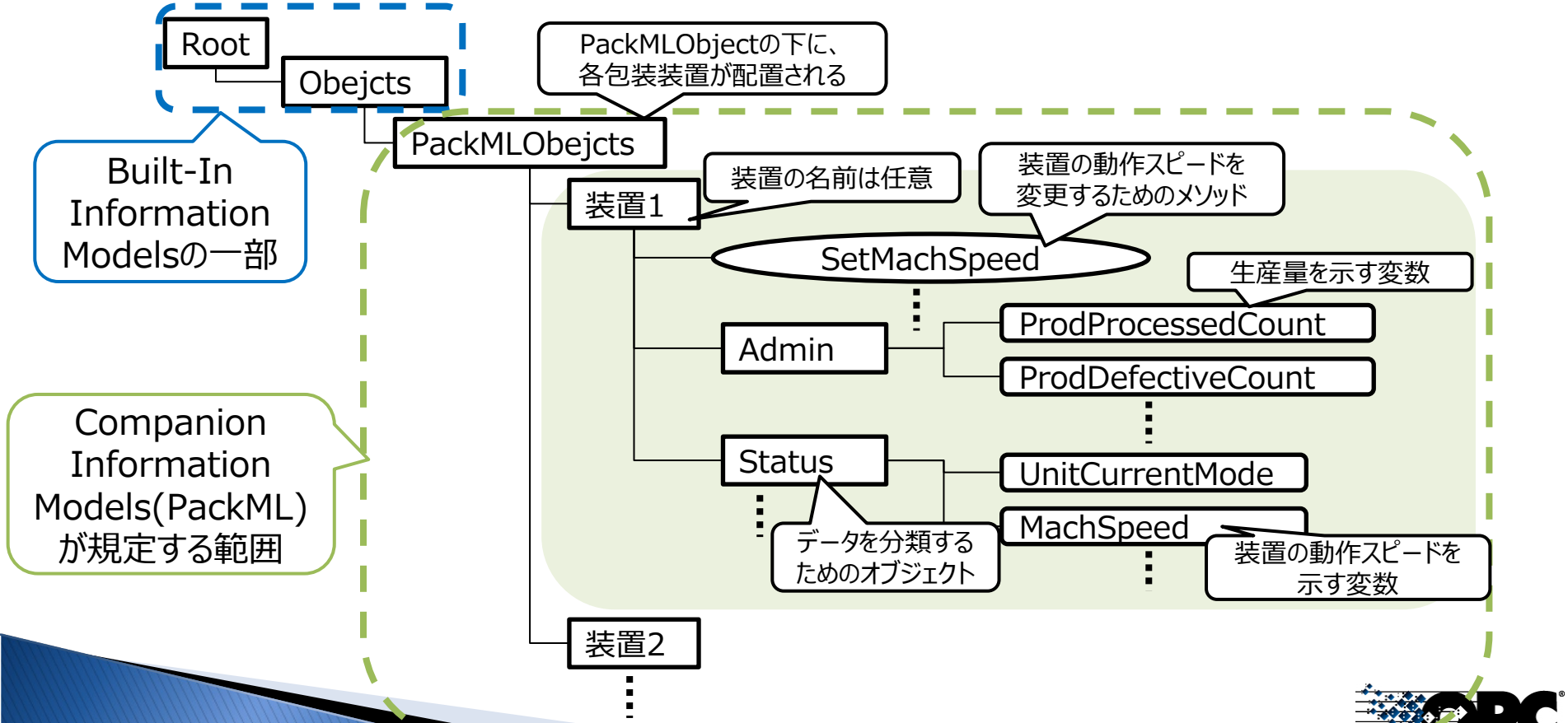
OPC UA機能モデル


Vendor Specific Extensions
Companion Information Models
PLCopen, ADI, FDI, FDT, BACnet, MDIS, ISA95, AutomationML, MTConnect, AutoID, VDW, EUROMAP, Robotics, Vision Systems IEC 61850/61400, Sercos, Powerlink, PROFInet and more coming
パートナによる開発
DI Model
UA for Devices
Built-In Information Models
Base, DA, AC, HA, Programs
OPC UA Meta Model
OPC UAで情報を公開するための基本ルール
Client / Server
Publish / Subscribe
Information Model Layer
Communication Model
Protocol Bindings
Services
Browse, Read / Write
Method Calls, Subscriptions
Message Model
PubSub Configuration, DataSets
Message Readers and Writers
Built-in Security
UA Binary
JSON
UA Secure Conversation
UA TCP
Relay
WebSocket / HTTPS
UA Binary
JSON
UADP
UADP / JSON
UDP
TSN
AMQP
MQTT
OPC Foundation 責任範囲
OPC UA = IEC 62541

実装のイメージ

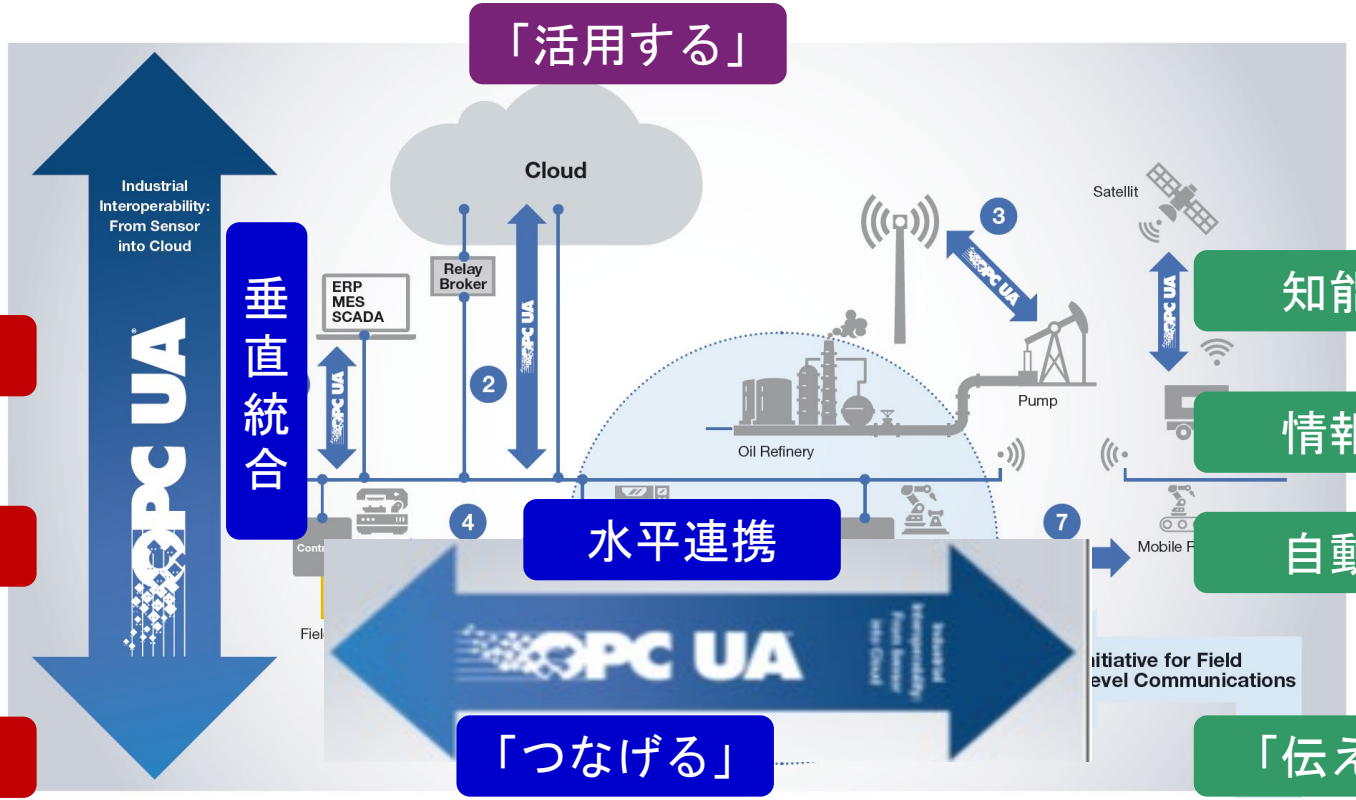

OPC UA Client
OPC UA Server
サービス
OPC UAクライアントが情報モデルにアクセスするためのI/F
(仕様＋実装)
情報モデルの閲覧や関数呼び出しなどのI/Fを用意
情報モデル
・基本概念やルール
(OPC UA Meta Model)
・定義済みのモデル
(Built-In Information Models)
・業界などが用意するモデル
(Companion Information Models)
・自由に作るモデル
(Vender Specific Extensions)
機器との間のI/F
(実装)
機器の違いなどを吸収

Companion Information Modelsの例(PackML)




AutomationML
ISA-95
PLCopen
for efficiency in automation
INTERNATIONAL DATA SPACES ASSOCIATION
DIN
OpenFog
IT
BACnet
MDIS
業界分野
THE Open GROUP
DEXPI
Data Exchange in the Process Industry
FieldComm Group
NAMUR
FDT GROUP
プロセス
オートメーション
設計
エンジニアリング
industrial internet CONSORTIUM
INDUSTRIE4.0
コンソーシアム
LNI4.0
MADE IN CHINA 中国制造 2025
IV Industrial Value Chain Initiative
W3C
OPC UA
The Industrial Interoperability Standard
60を超える業界団体と"コラボレーション"が進んでいます。
EtherCAT Technology Group
ODVA
IO-Link
CiA
PI PROFIBUS • PROFINET
ETHERNET POWERLINK Standardization Group
CLPA
sercos international
フィールド
ネットワーク
エネルギー
USE61400-25 IEC 61400-25 user group
energistics
IEC
ファクトリー
オートメーション
VDMA (17!)
ZVEI: Die Elektroindustrie
aim
CEMAFON
EUROMAP
VDW
OMAC
umati
MTConnect
OPC FOUNDATION

まとめ


「活用する」
Industrial Interoperability: From Sensor into Cloud
OPC UA
垂直統合
Cloud
ERP MES SCADA
Relay Broker
OPC UA
2
3
Satellit
Pump
Oil Refinery
4
水平連携
7
Mobile
Fiel
OPC UA
itiative for Field evel Communications
「つなげる」
Zero Trust
多層防御
「安全に」
知能化
情報化
自動化
「伝える」

ありがとうございました。

日本OPC協議会

https://jp.opcfoundation.org

日本OPC協議会
技術部会