



OPC UA Pub-Sub通信モデルの概要

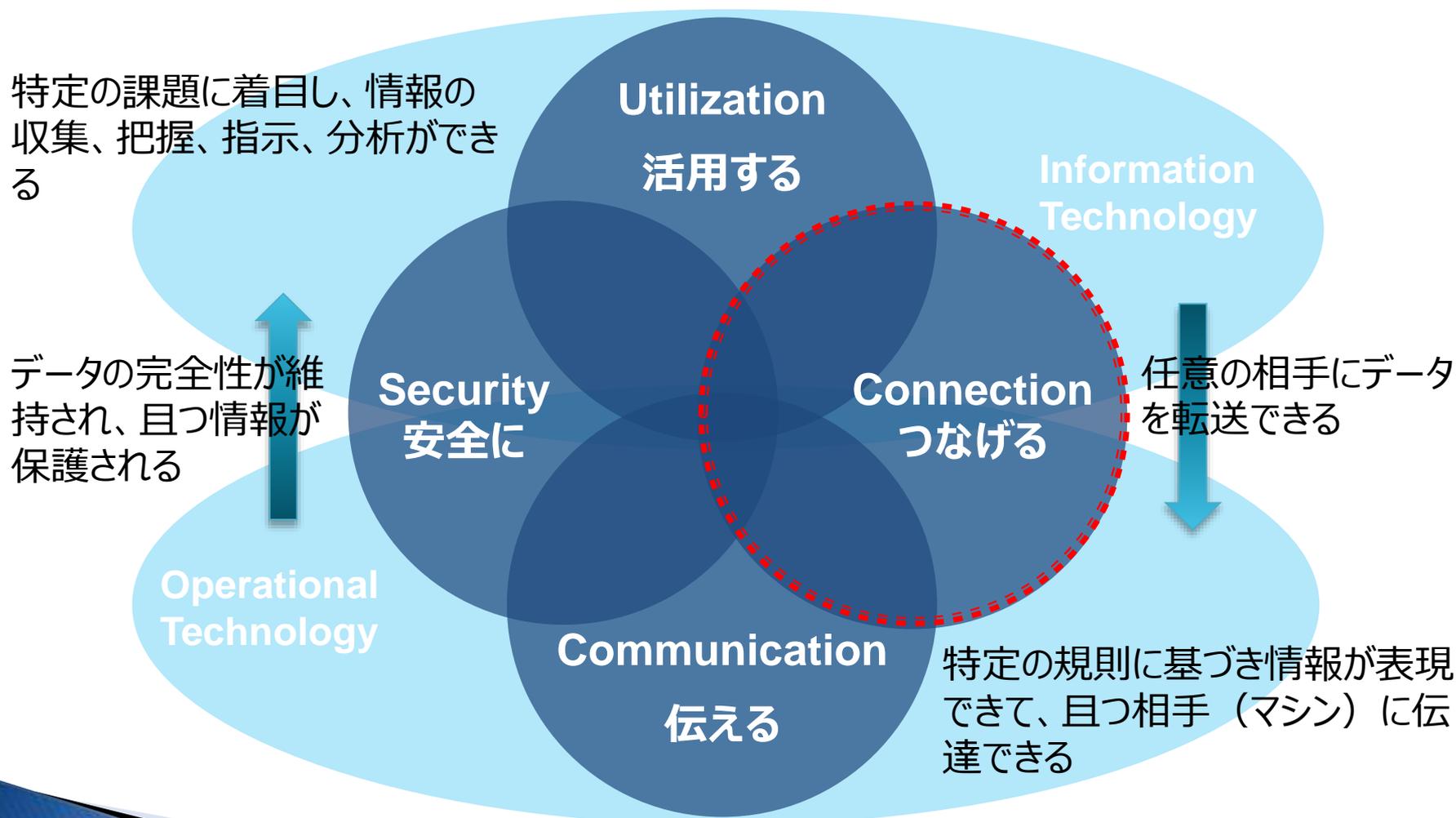
2016年12月9日

日本OPC協議会 技術部会

目次

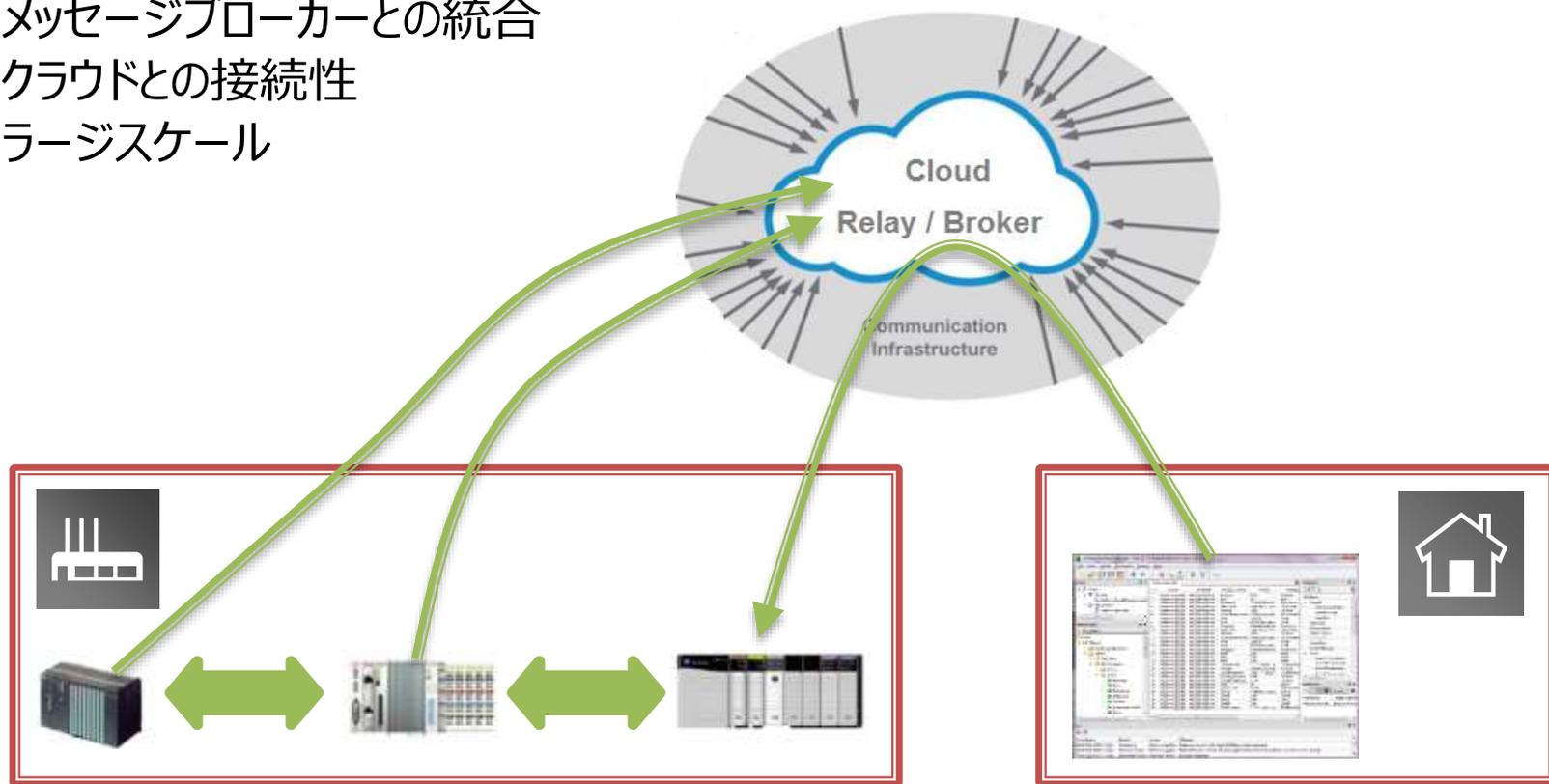
- ▶ **OPCの理念：データ活用に必要な能力**
- ▶ **Pub-Sub通信モデルの動機づけ**
- ▶ **Pub-Sub通信モデルの概要**
- ▶ **Pub-Sub通信モデルの基本情報モデル**
- ▶ **Pub-Sub通信事例：UADP (UDP/TCP)**
- ▶ **Pub-Sub通信事例：AMQP**
- ▶ **Pub-SubのコントローラM2Mへの適用**
- ▶ **Pub-Subのデモとロードマップの計画**

データ活用に必要な能力



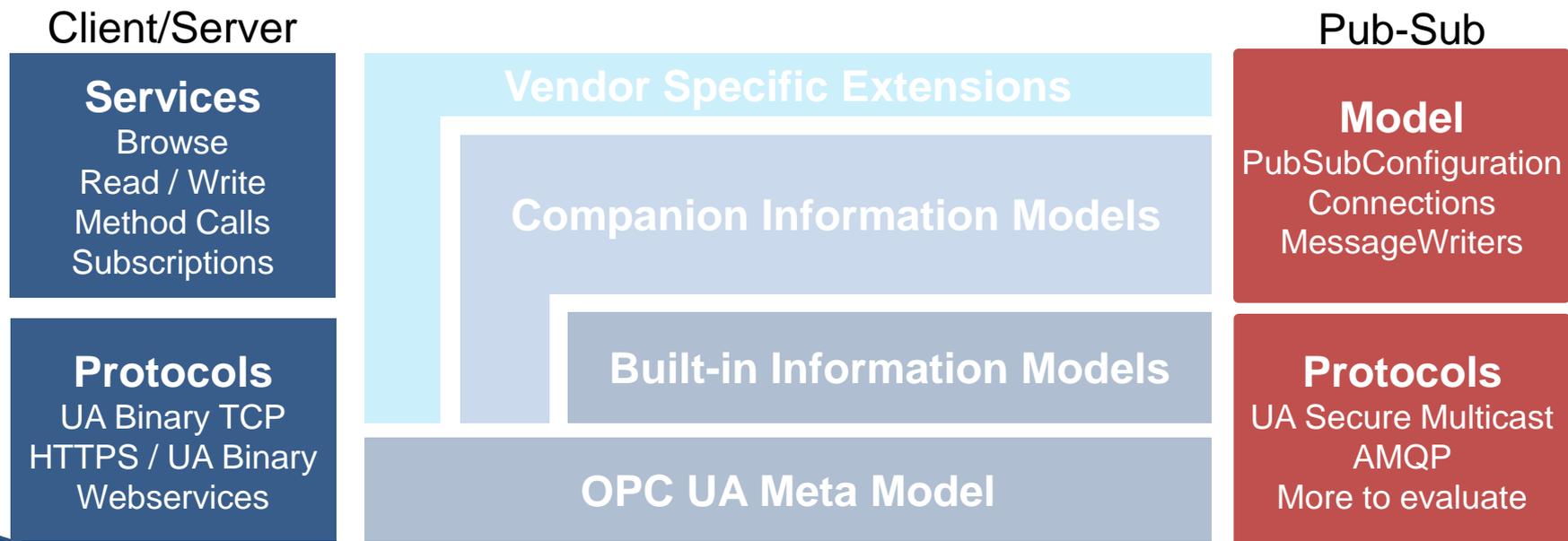
Pub-Sub通信モデルの動機づけ : 新しいユースケース

- ▶ ファイアウォールを介したクライアントとサーバー(リレー)
- ▶ コントローラー同士のコミュニケーション
- ▶ メッセージブローカーとの統合
- ▶ クラウドとの接続性
- ▶ ラージスケール

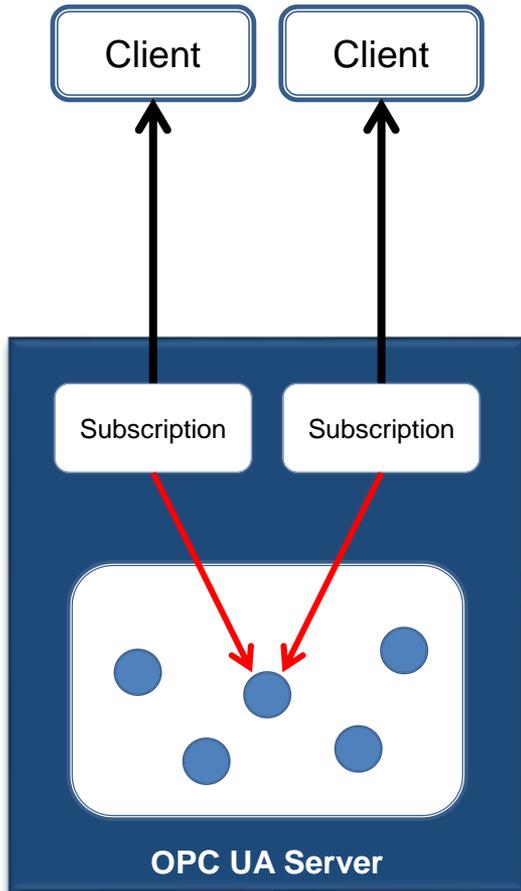


Pub-Sub通信モデルの機能拡張

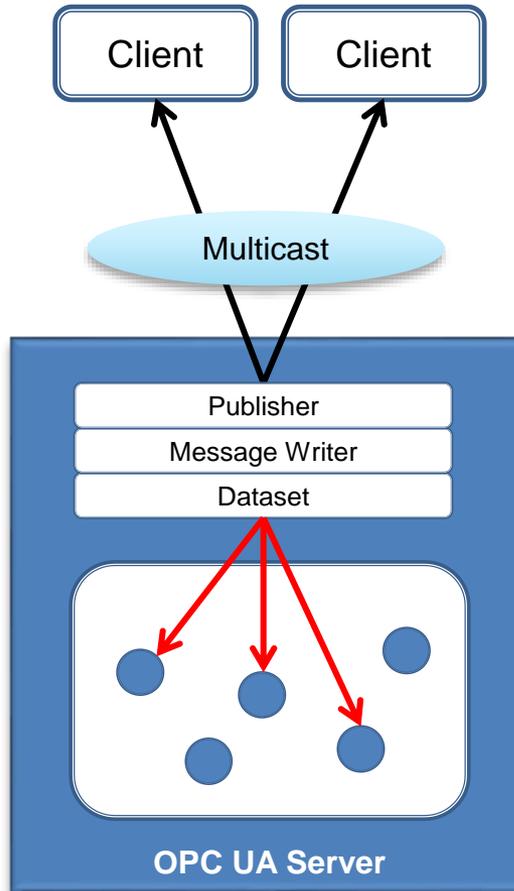
- ▶ OPC UA Publisher/Subscriber 通信モデル を機能追加
 - 汎用的な Pub-Sub情報モデル
 - 初期プロトコルの選定、他プロトコルも継続評価中



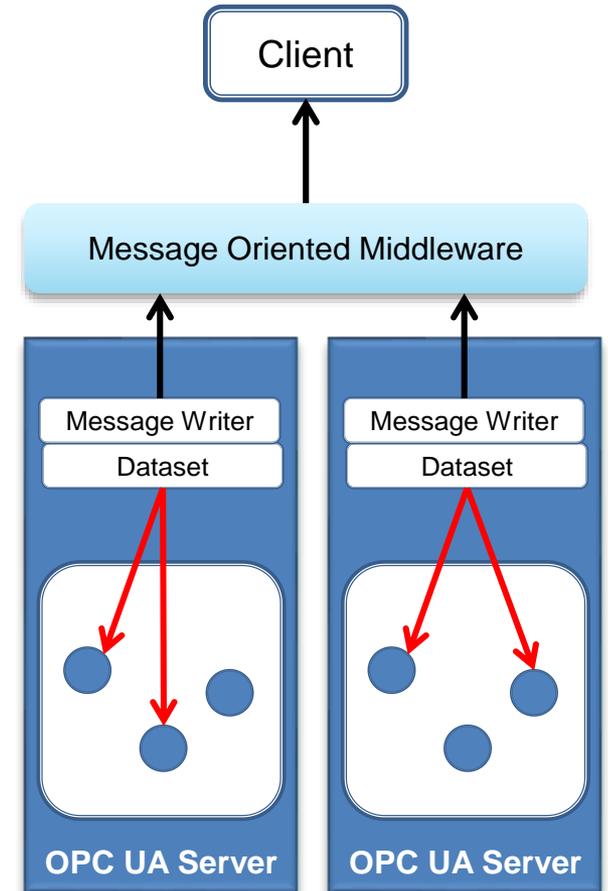
通信モデルの特徴



Client / Server

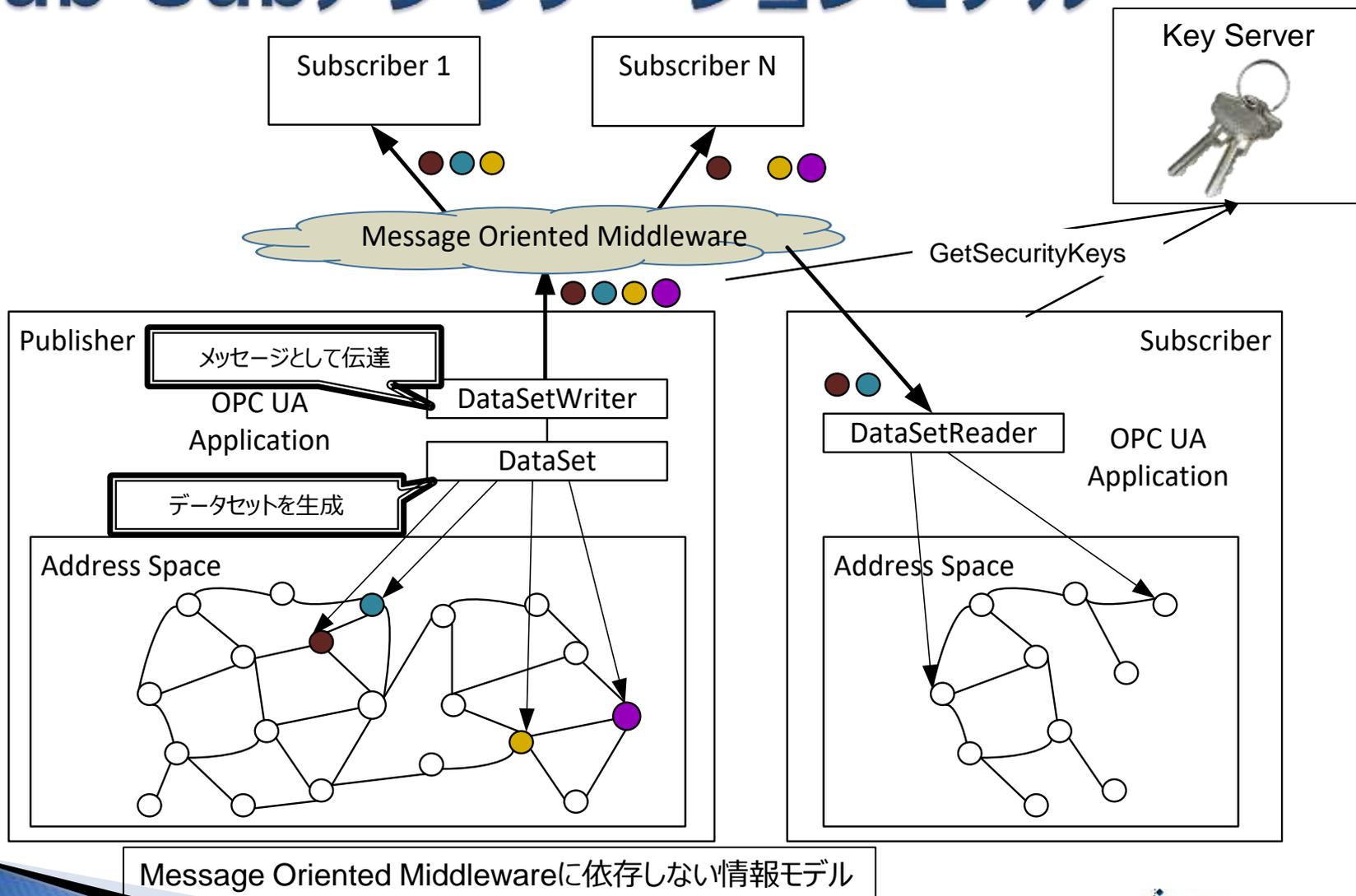


Publish / Subscriber (1:N)



Publish / Subscriber (N:1)

Pub-Subアプリケーションモデル

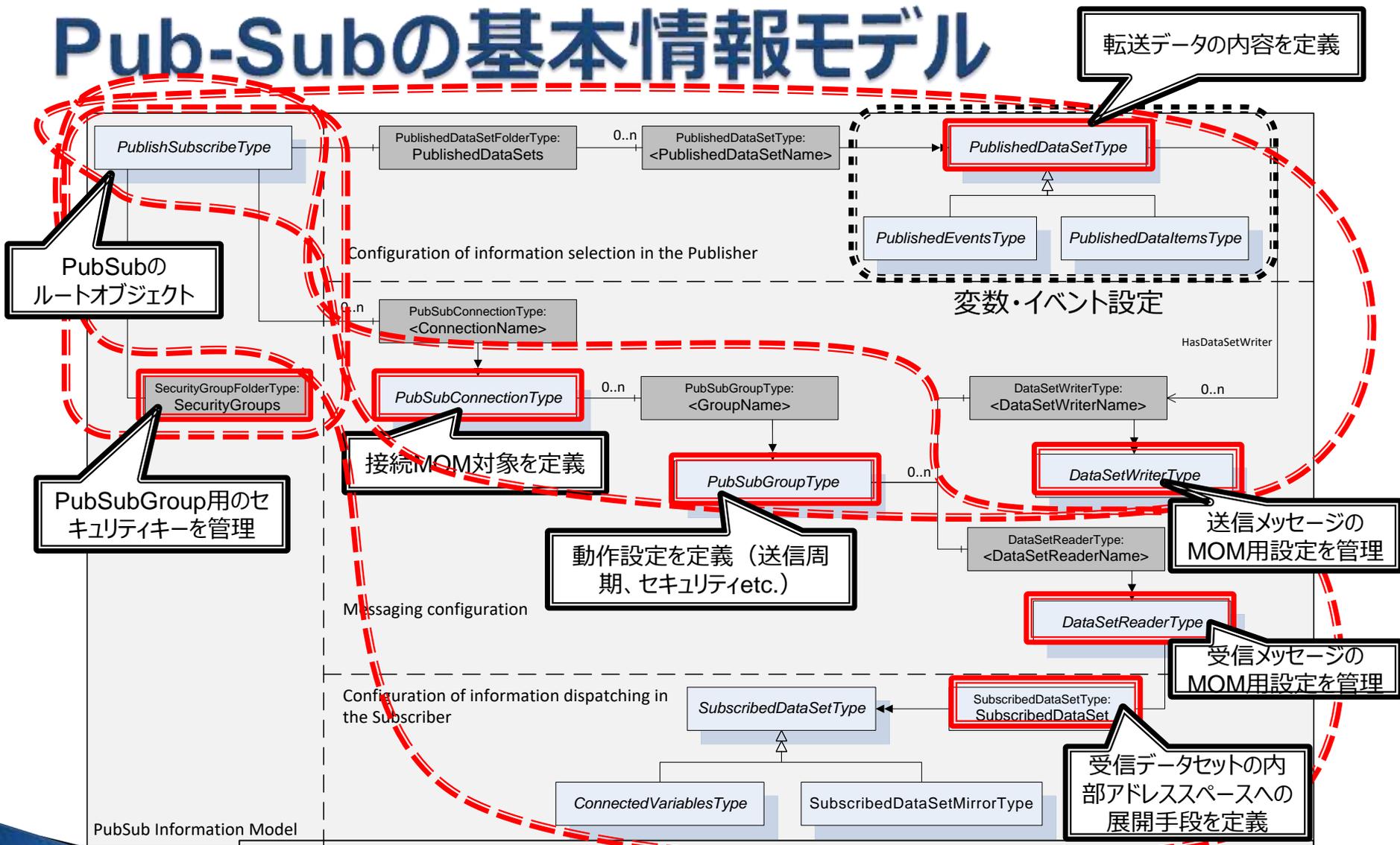


Pub-Subのアプリ種類と主な情報モデル

- ▶ **Publisher** : データセットを送信する
 - `PublishedDataSetType` : 送信データのデータセットの定義
 - `PubSubConnectionType` : 送信先MOM (Message Oriented Middleware) のエントリーポイントの定義
 - `PubSubGroupType` : データ送信の動作設定の定義
 - データセットの送信周期、KeepAliveメッセージの送信周期
 - 転送データを暗号化・署名する場合の対象セキュリティグループと、その鍵を管理するキーサーバー
 - `DataSetWriterType` : データセットの送信方式の定義
- ▶ **Subscriber** : データセットを受信する
 - `PubSubConnectionType` : (同上:ただし受信するMOMの定義)
 - `PubSubGroupType` : (同上)
 - `DataSetReaderType` : データセットの受信方式の定義
 - `SubscribedDataSetType` : 受信したデータセットの内容を自アドレススペース内のどこにマッピングするかの定義
- ▶ **キーサーバー** : 転送データを暗号化・署名する為の鍵を管理する
 - `SecurityGroupFolderType` : 管理しているセキュリティグループとその鍵などを保持

セキュリティグループ: 同じ鍵でセキュリティを確保するグループ。Pub-SubではPubSubGroupTypeのインスタンスが対象で、1つのセキュリティグループで複数のPubSubGroupTypeのインスタンスを管理できる。

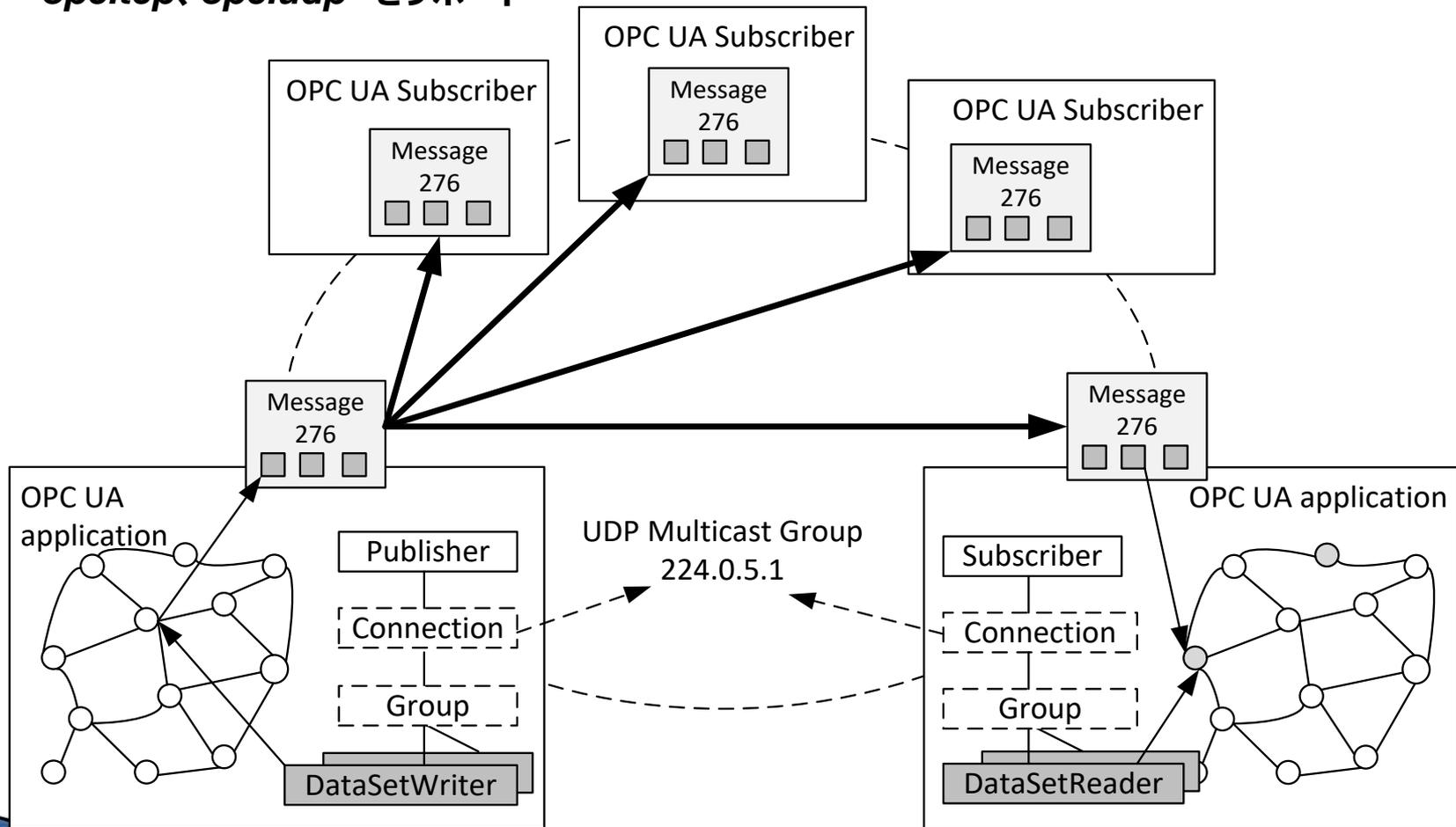
Pub-Subの基本情報モデル



※本資料は2016/8/10発行ドラフト版の内容であり、最終版はこれと異なる可能性があります。

Pub-Sub with Secure Multicast

- ▶ **UADP (UA Datagram Protocol) によるセキュアなIPマルチキャスト**
 - *opc.tcp*、*opc.udp* をサポート



Pub-Sub with Broker

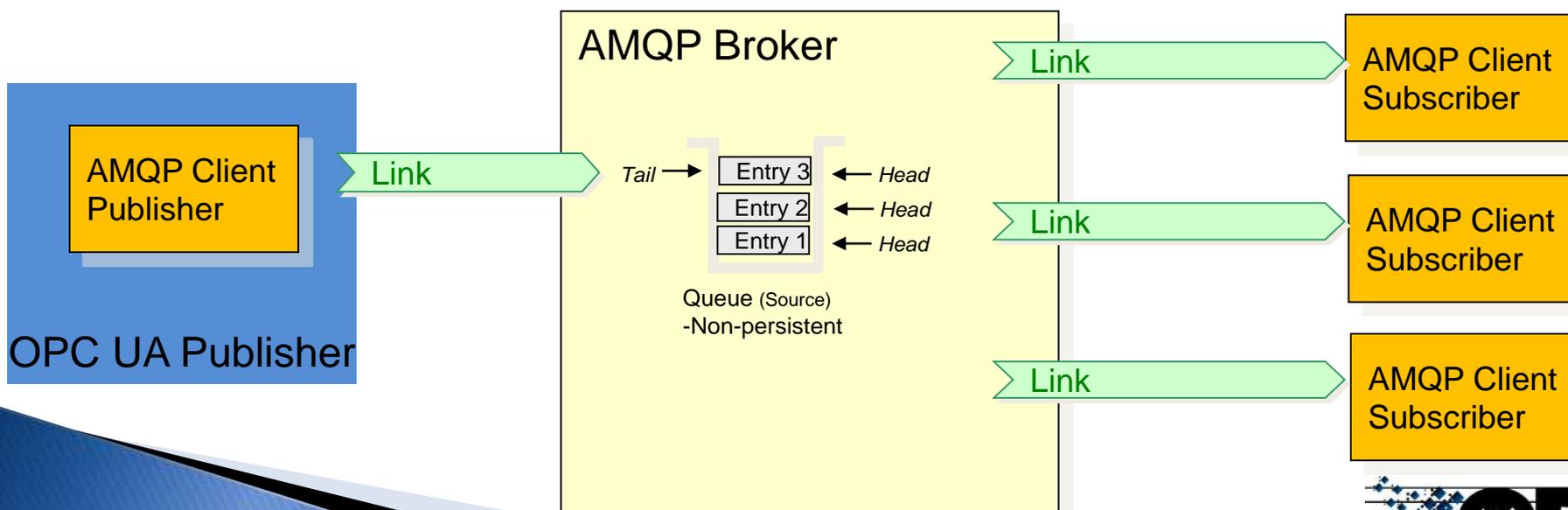
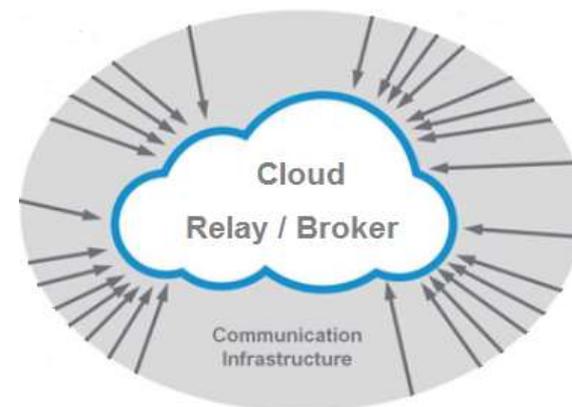
- 任意の数のクライアントとサーバー間での接続を実現

- 異なるネットワークに存在するUAアプリケーションの接続
- クラウド内クライアントへのデータ転送

- AMQP 1.0を採用

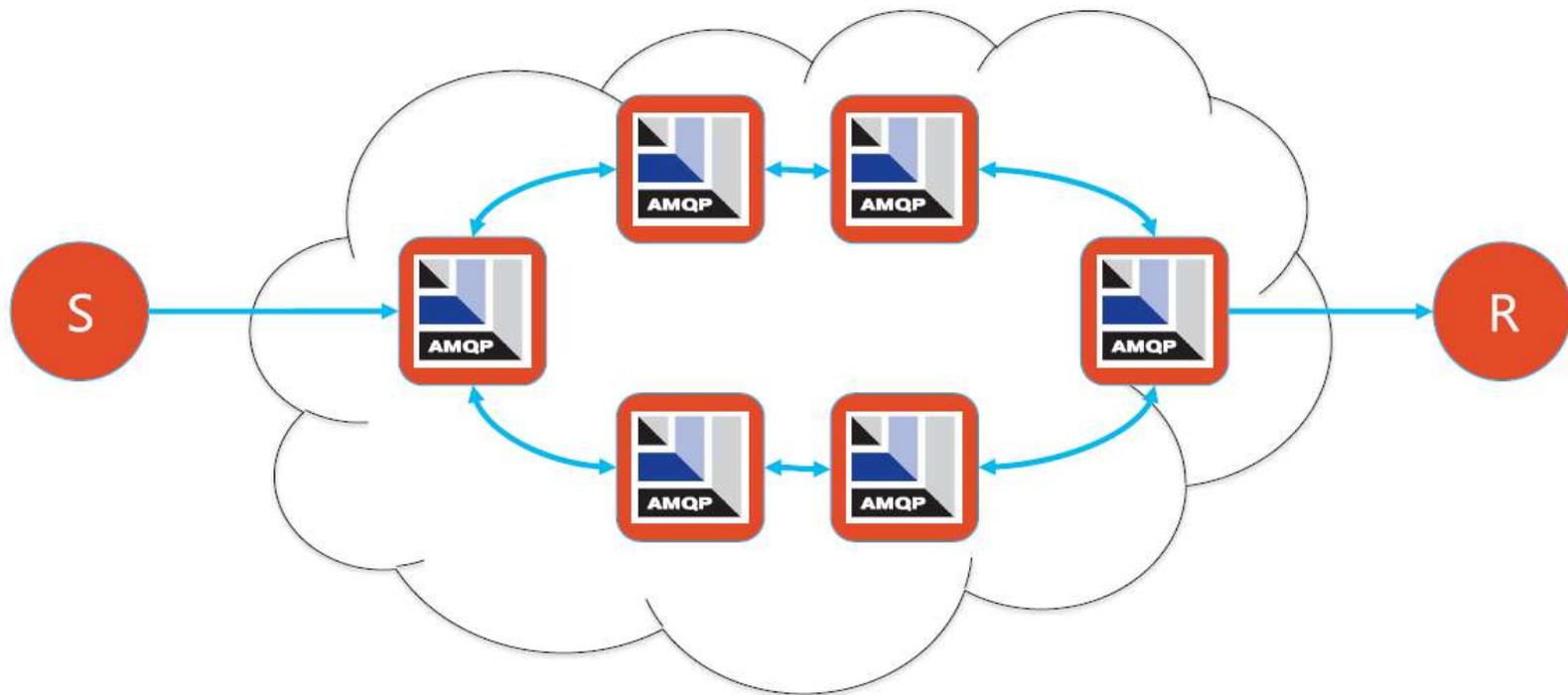
- ISO/IEC 19464:2014
- Microsoft Azure[®] などでも利用

「Microsoft Azure」は、米国 Microsoft Corporationの、米国およびその他の国における登録商標または商標です。



AMQPの概要

ISO 19464 flexible topologies



出典 : ISO 19464 Connecting Business for Value
by John O'Hara Originator of AMQP / ISO 19464

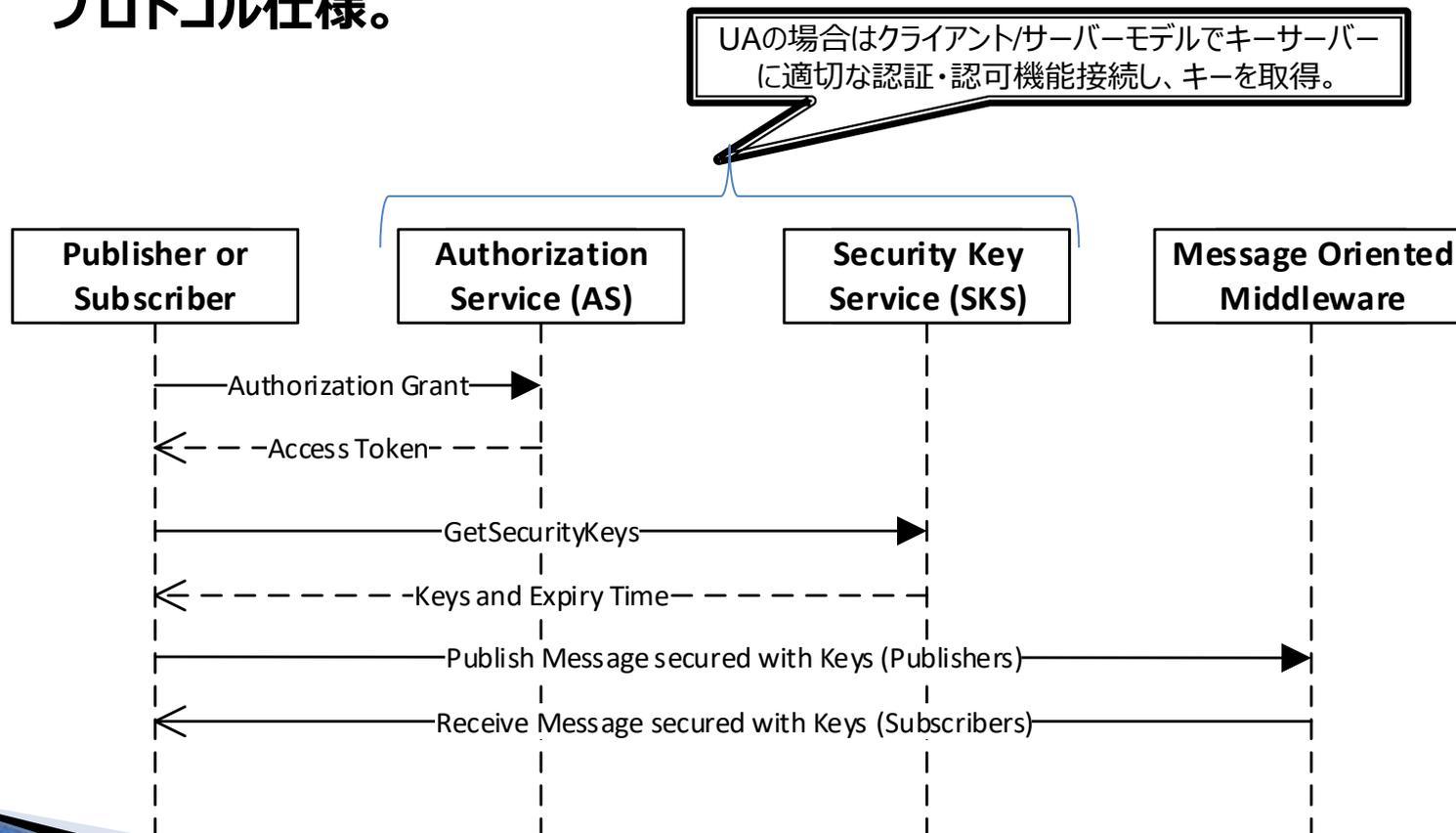
Pub-Sub セキュリティ

- ▶ クライアント/サーバー モデルのセキュリティ
 - 公開鍵基盤 (PKI) と、セッションキー交換の非対称アルゴリズム
 - セッションキーは対象アルゴリズムのコミュニケーションに利用
 - セッションキーを頻繁に更新
- ▶ PubSub モデルのセキュリティ (end to end security)
 - セッションキーはPublisherとSubscriberで共有が必要
 - セキュリティグループの為にキーを管理
 - メッセージはセキュリティグループ内で送信
 - キーは OPC UA クライアント/サーバーモデルのセキュリティでキーサーバー経由で配布
 - セキュリティグループでのアクセスにおける認証・認可はキーサーバーで実施

Pub-Sub セキュリティ

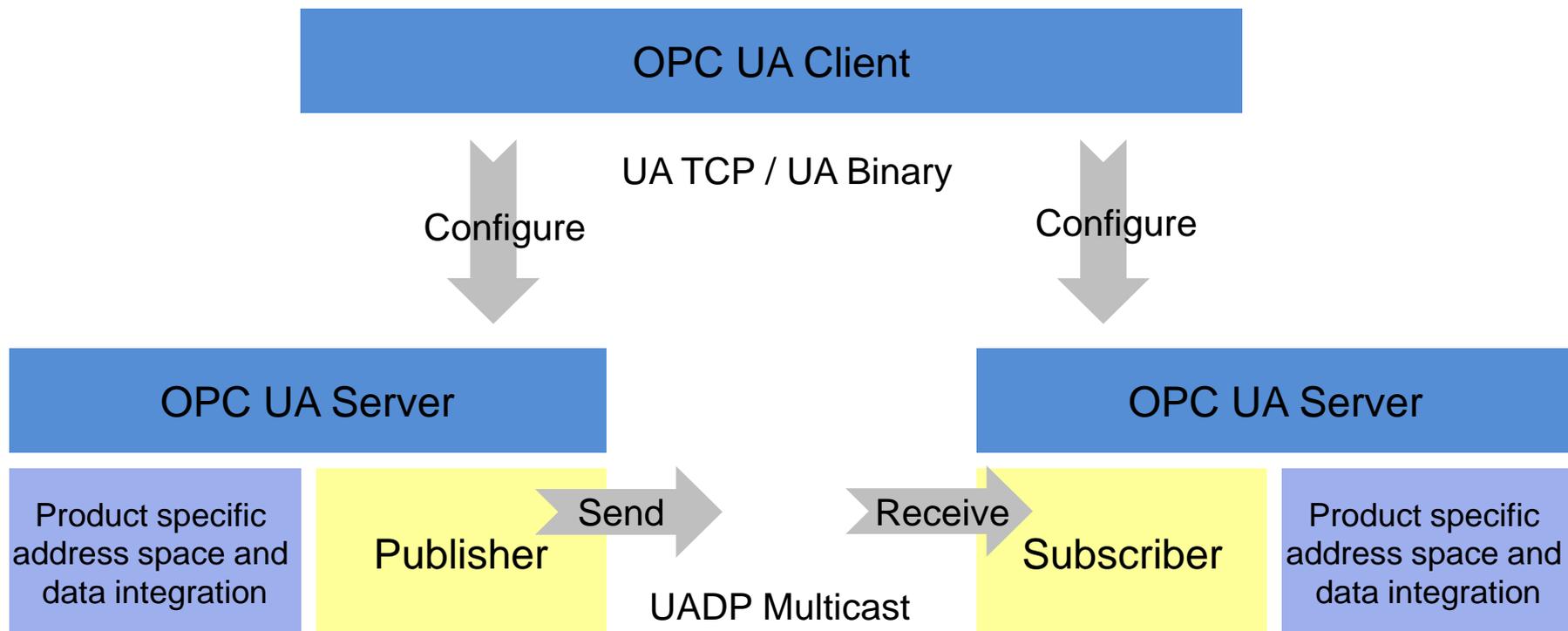
▶ OAuth2の考え方を採用

- OAuth2 : Webアプリにて、アクセス認可の判断をネットワーク越しに行うプロトコル仕様。



コントローラー M2M

- ▶ 既存OPC UAサーバーへの拡張で対応可能
- ▶ OPC UAクライアントからのPub-Subモデルのコンフィギュレーション
- ▶ UADP (UA Datagram Protocol) によるセキュアなIPマルチキャスト



リアルタイムなコントローラーM2M?

- ▶ UADP マルチキャストが提供するもの
 - 最小限で効率的なプロトコルスタックによるメッセージ処理
 - サイクリックなデータ交換が可能
 - デバイス側のリアルタイム処理の基盤
- ▶ 標準イーサネットはリアルタイムではない
 - 遅延の可能性がある
- ▶ TSN (Time Sensitive Network) が解決できる
 - IEEE 802 working group – 標準イーサネットの一部になる予定
 - 時刻同期
 - 境界が保証された遅延時間 (Guaranteed bounded latency)
 - 冗長経路による信頼性
 - 低い遅延時間 (latency) – カットスルーとプリエンプション
 - Gb以上のバンド幅
 - 将来のPub-Subの採用プロトコルとして検討

Pub-Sub プロトタイプ

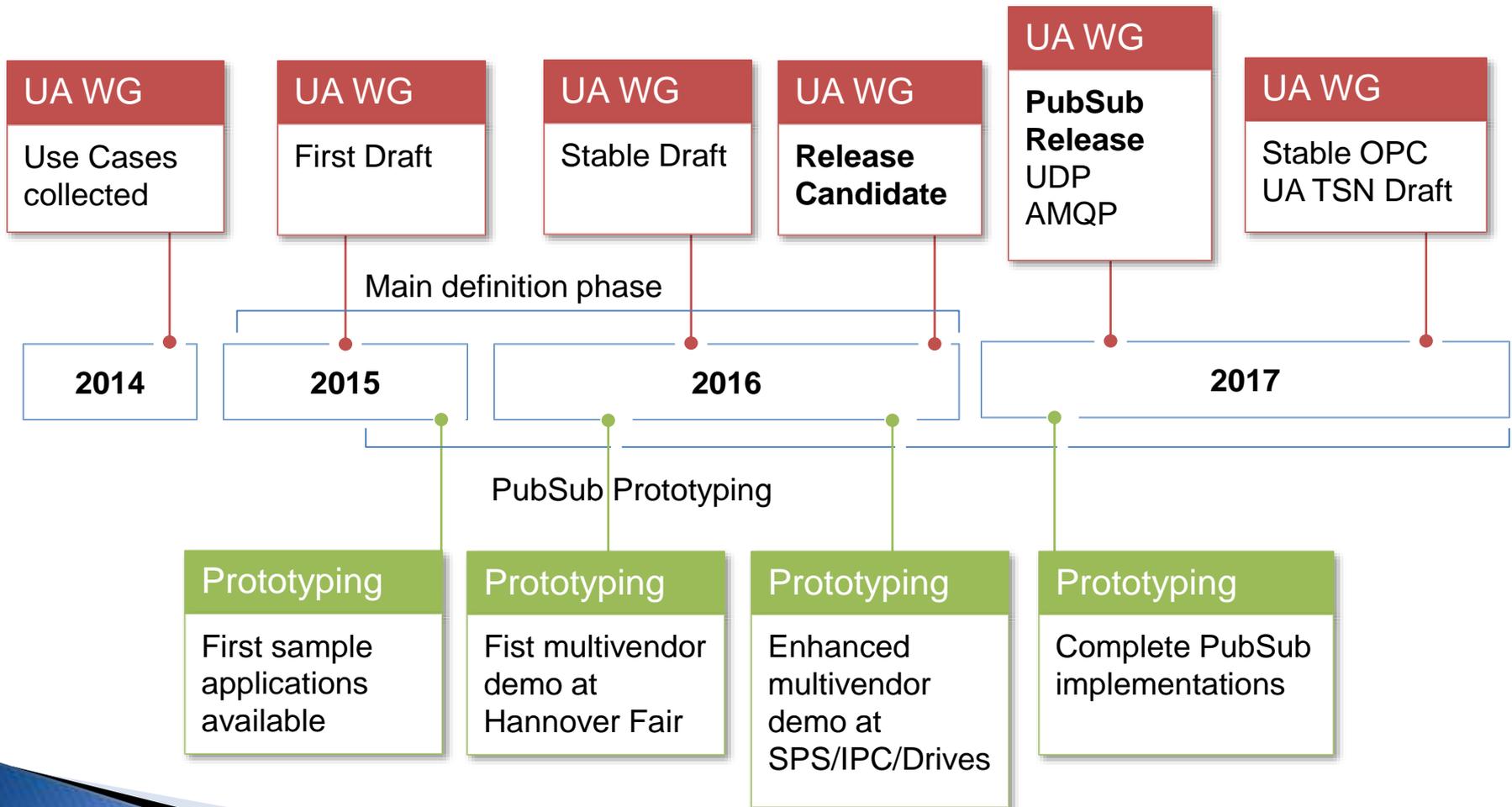
- ▶ UA WGのサブWGとして活動
- ▶ 2015/7/8にキックオフ
- ▶ 70以上のWGメンバー
- ▶ Wireshark(*) 利用可能
- ▶ 最初のデモが2016/04にハノーバーで展示

(*) オープンソースのネットワークアナライザ

Wiresharkは、Wireshark Foundation, Inc.の商標です。



OPC UA Pub-Sub ロードマップ



OPC UA Pub-Sub

- ✓ OPC UA – 情報モデルのためのコミュニケーションプラットフォーム (HOW)
- ✓ ドメインのエキスパートが情報モデルを定義 (WHAT)
- ✓ OPC Foundation はPub-Subにより通信モデルを拡張
- ✓ 情報モデルは影響を受けない
- ✓ OPC UA アプリケーションはSDKやスタックを更新するだけでよい

日本OPC協議会

URL: <https://jp.opcfoundation.org>