OPC Day Japan 2019

OPC UAセキュリティ機能のおさらい

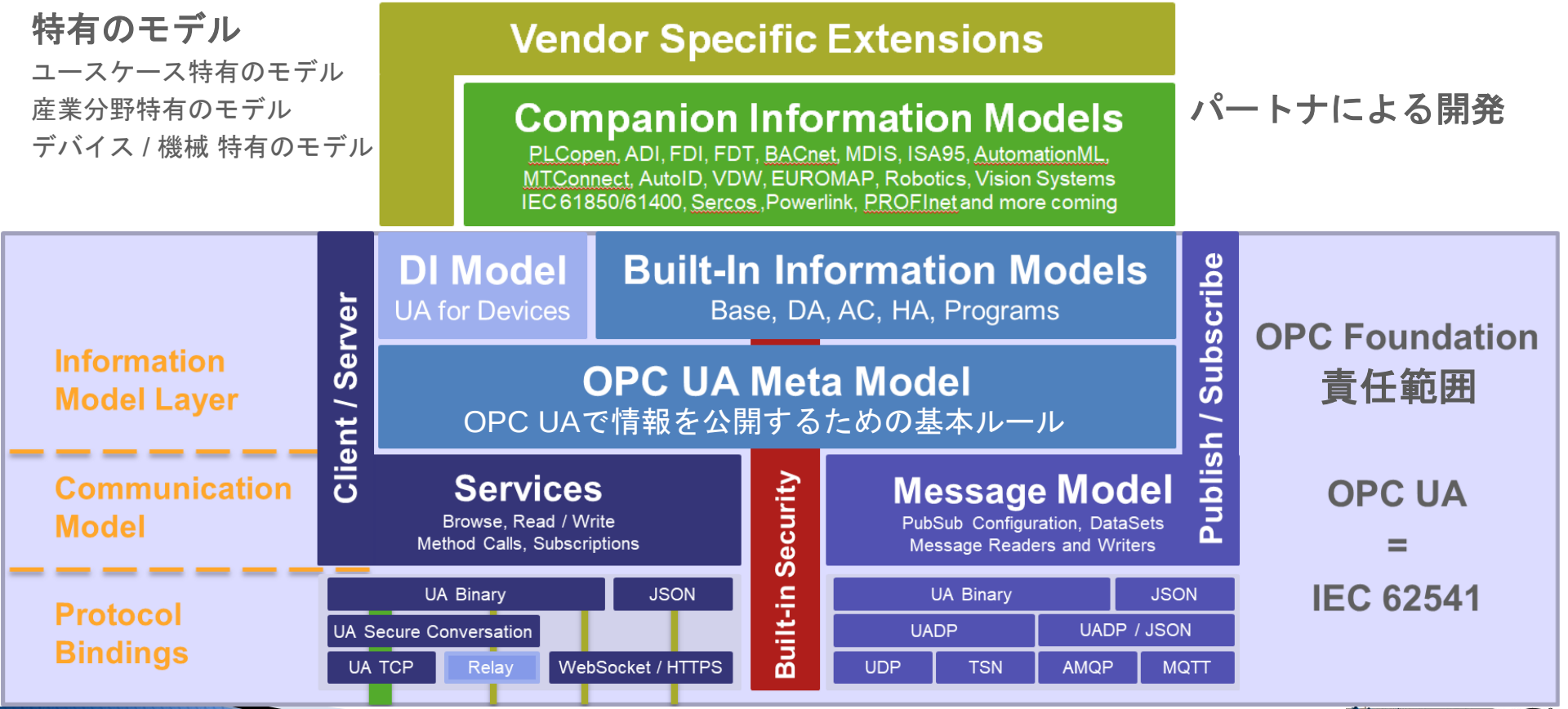
- 新たな通信モデルにも対応する Security by Design -

2019年12月12日
日本OPC協議会 技術部会
藤井 稔久(アズビル株式会社)

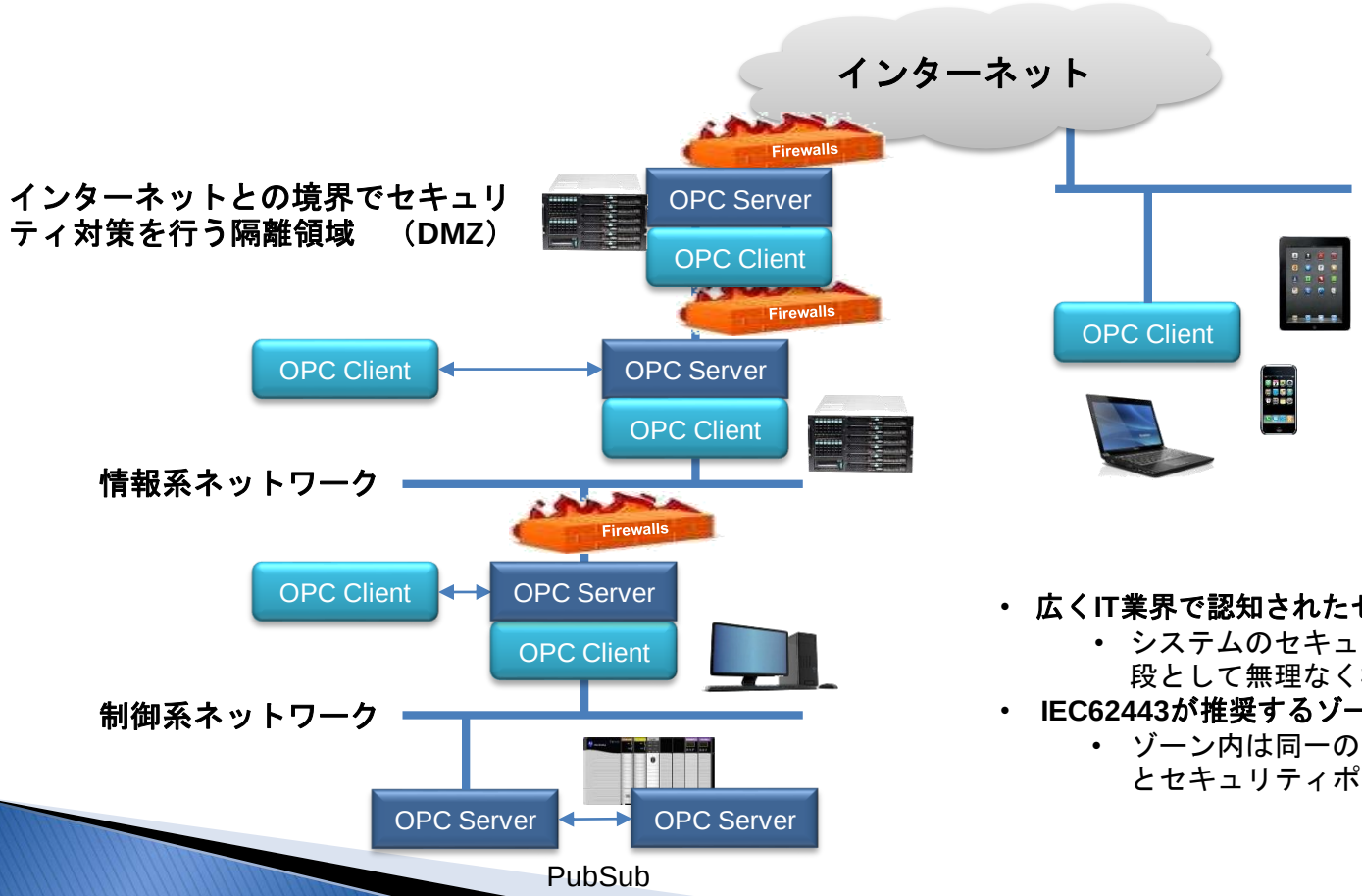
OPC UA 機能モデル

特有のモデル

ユースケース特有のモデル
産業分野特有のモデル
デバイス / 機械 特有のモデル



OPC UA　システム構成例



- **広くIT業界で認知されたセキュリティ機能**
  - システムのセキュリティポリシー対策手段として無理なく検討が可能
- **IEC62443が推奨するゾーン設計と親和性**
  - ゾーン内は同一のスタックプロファイルとセキュリティポリシーで通信。

セキュリティ機能　概要

- 認証と認可

アプリケーション認証

利用環境の妥当性

- Application Instance Certificate

ユーザ認証

利用者の妥当性

- Username & Password
- WS-Security Token
- X.509 V3

ユーザ認可

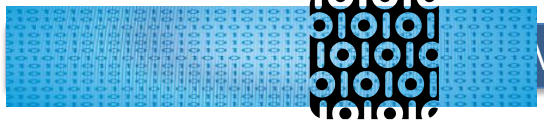
ユーザーまたはロールによるアクセス制御

- Access Level
- Write Mask
- Executable

- 完全性と機密性

メッセージ署名

FIC001.SV=50.00



暗号化

V=50.00

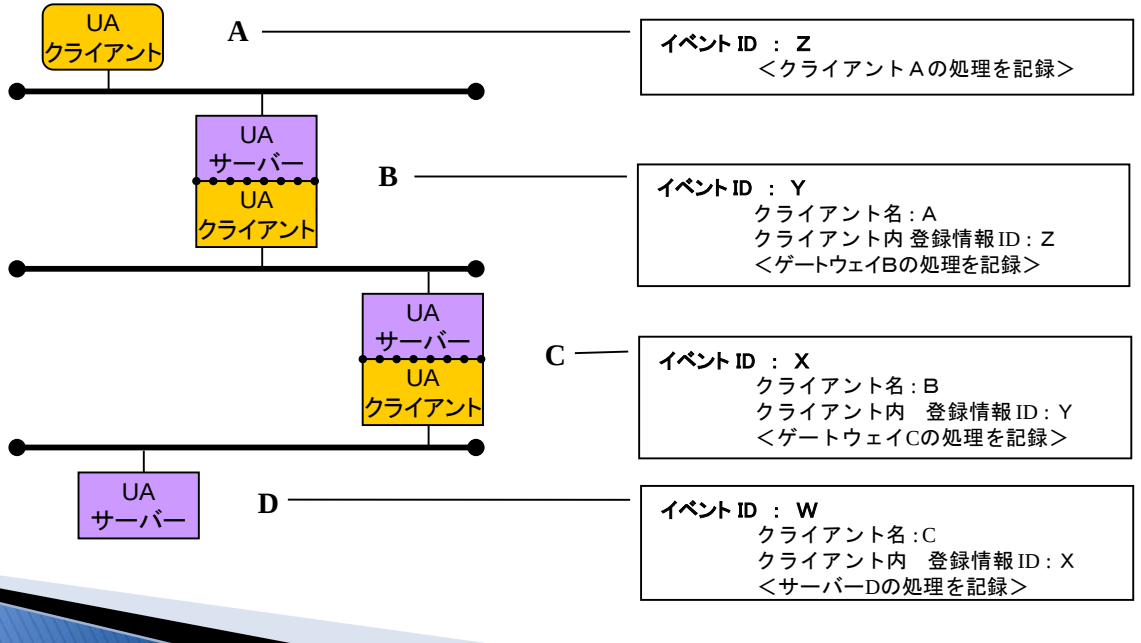
- **セキュリティモード：**
  メッセージに対するセキュリティ処理の指定
  None,Sign,SignAndEncrypt
- **セキュリティポリシー**
  次の機構の指定
  暗号化および署名のアルゴリズム
  鍵導出関数のアルゴリズム

OPC FOUNDATION

セキュリティ機能　概要

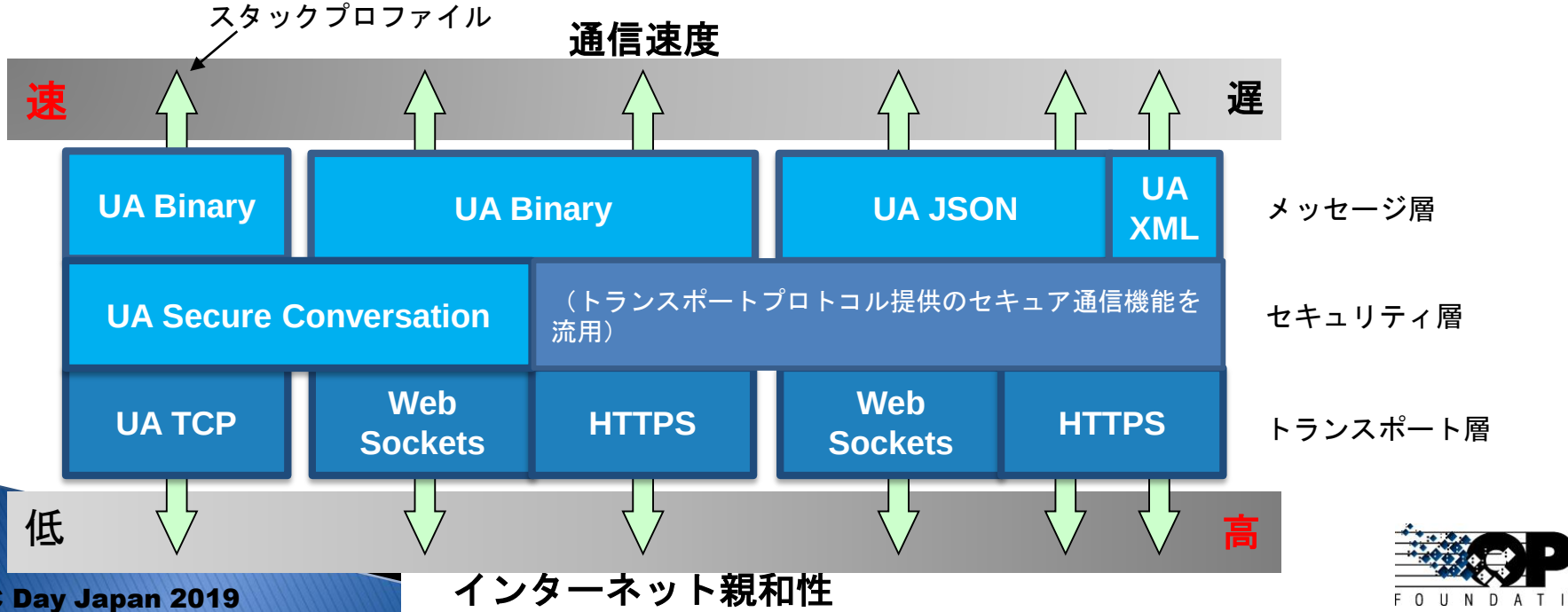
- 可用性
  - 接続処理に関する可用性はスタック内に設計済
    - 接続前の認証・検証処理は最小化し、DOS攻撃に対応
    - 不正な接続リクエストの大量受信時は処理を待機して過負荷を回避

- 可監査性

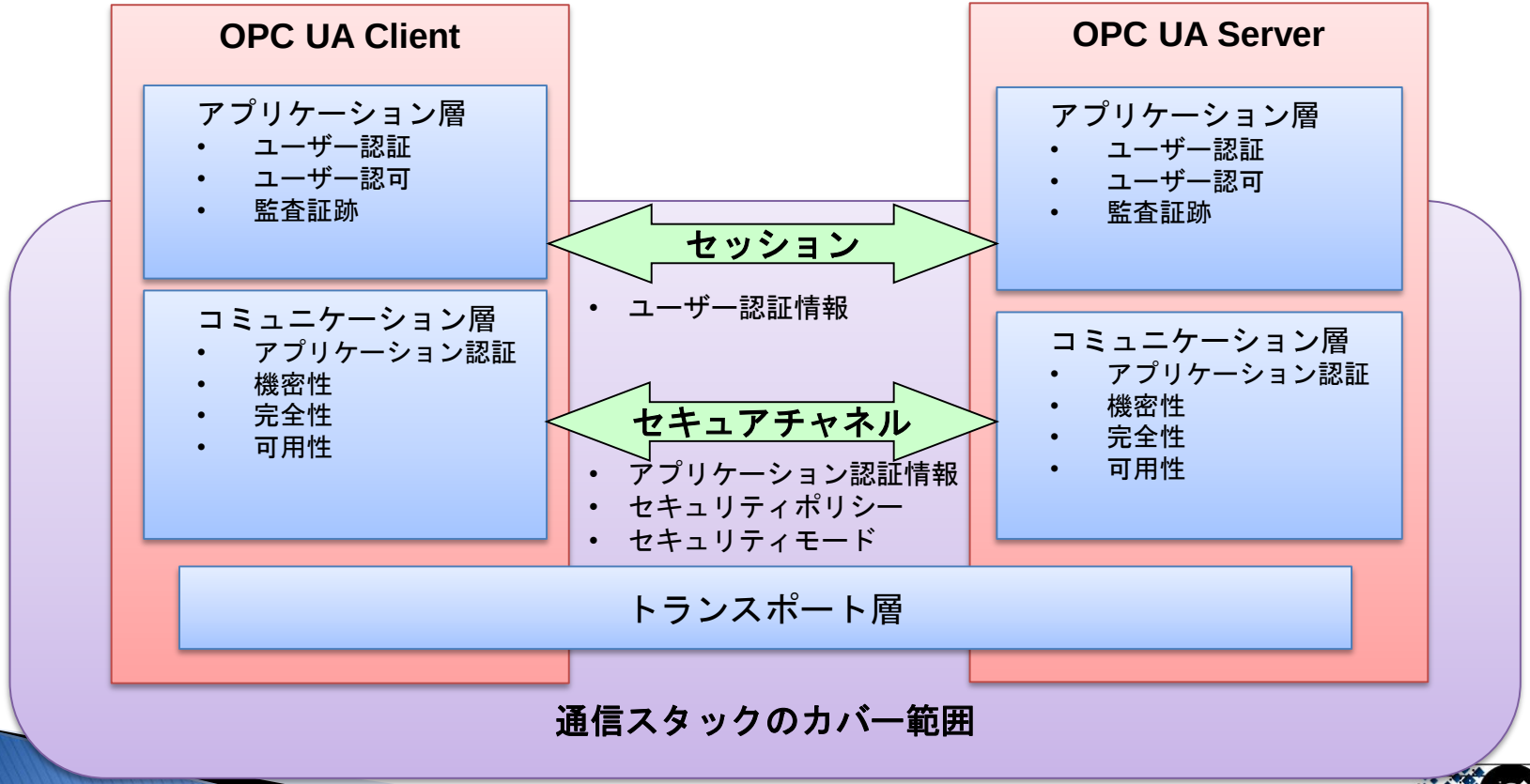


通信スタック

- OPC UA抽象IFのプラットフォーム依存部分を具現化するソフトウェア
- Client-Serverの場合は、接続時の下記指定でプロトコルを決定　（PubSubは後述）
  - エンドポイントURLの指定でスタックプロファイル（プロトコルバインディング）が確定
  - セキュリティ層は、アプリケーション認証や通信メッセージのセキュア対策など、暗号鍵を利用する処理を実装
  - サポート情報（スタックプロファイル、セキュリティモード・ポリシー、ユーザー認証手段など）はGetEndpointsで取得可能

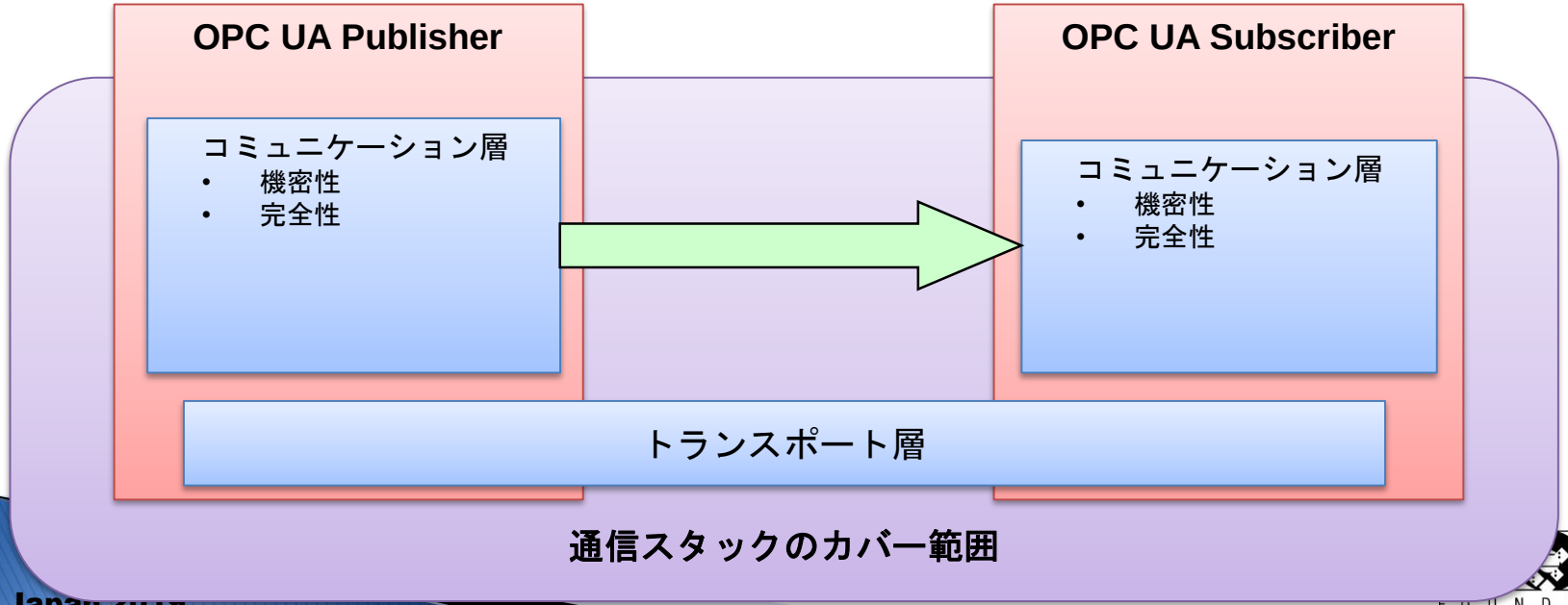


セキュリティアーキテクチャ Client-Server



セキュリティアーキテクチャ　Publisher-Subscriber

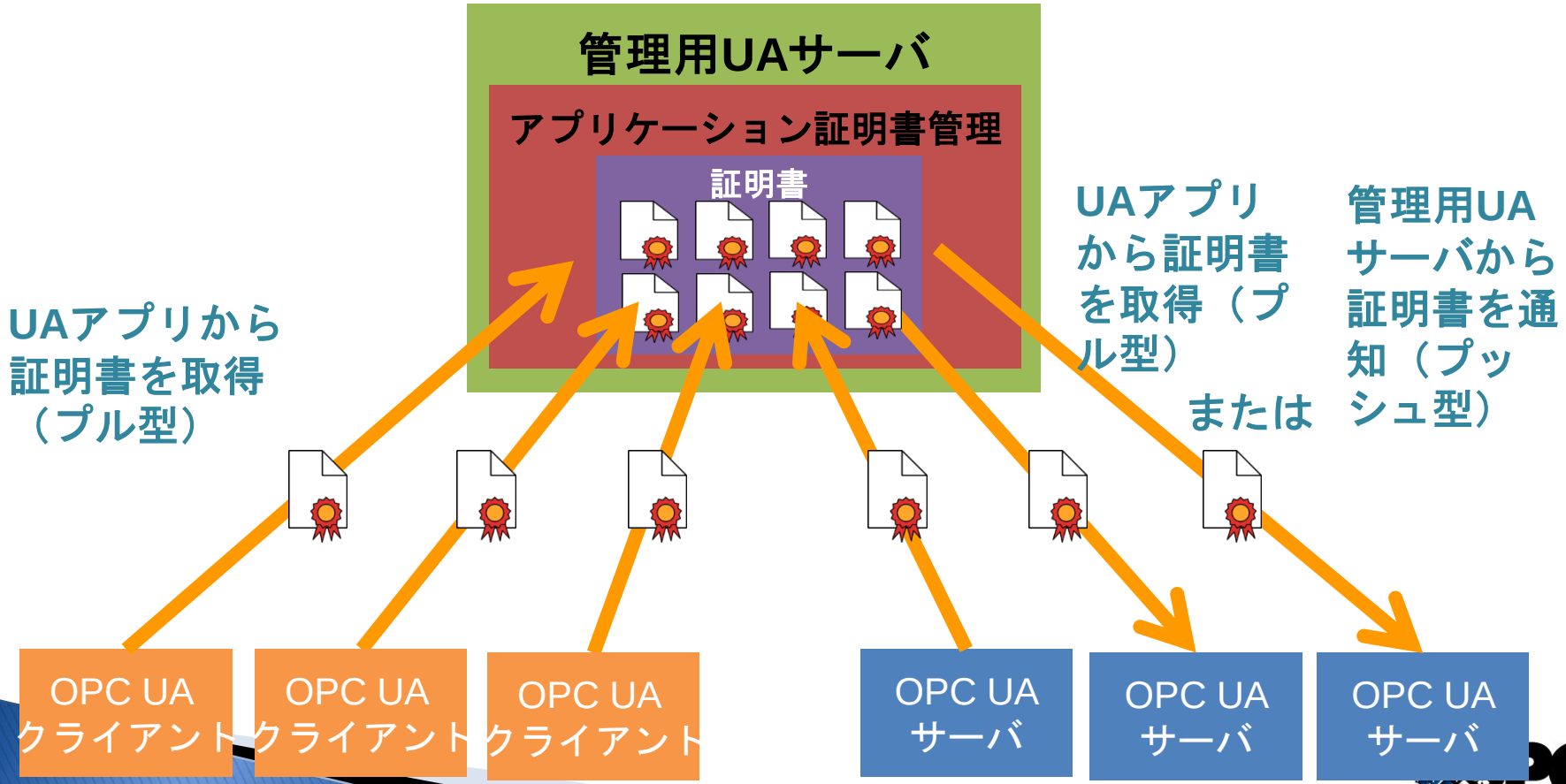
- 通信スタックはPublisherおよびSubscriber内のPubSubCoonnectionパラメータ（PubSub構成用の情報モデルの１つ）の値から、サポートする通知のエントリ毎のプラットフォームを予め設定
  - データ表現形式　（UA Binary、JSON）
  - セキュリティモード
  - 鍵管理サーバーのURIと、内部構成識別情報（セキュリティポリシー、暗号鍵などの定義）
  - トランスポートプロトコルと通知エントリのアドレス



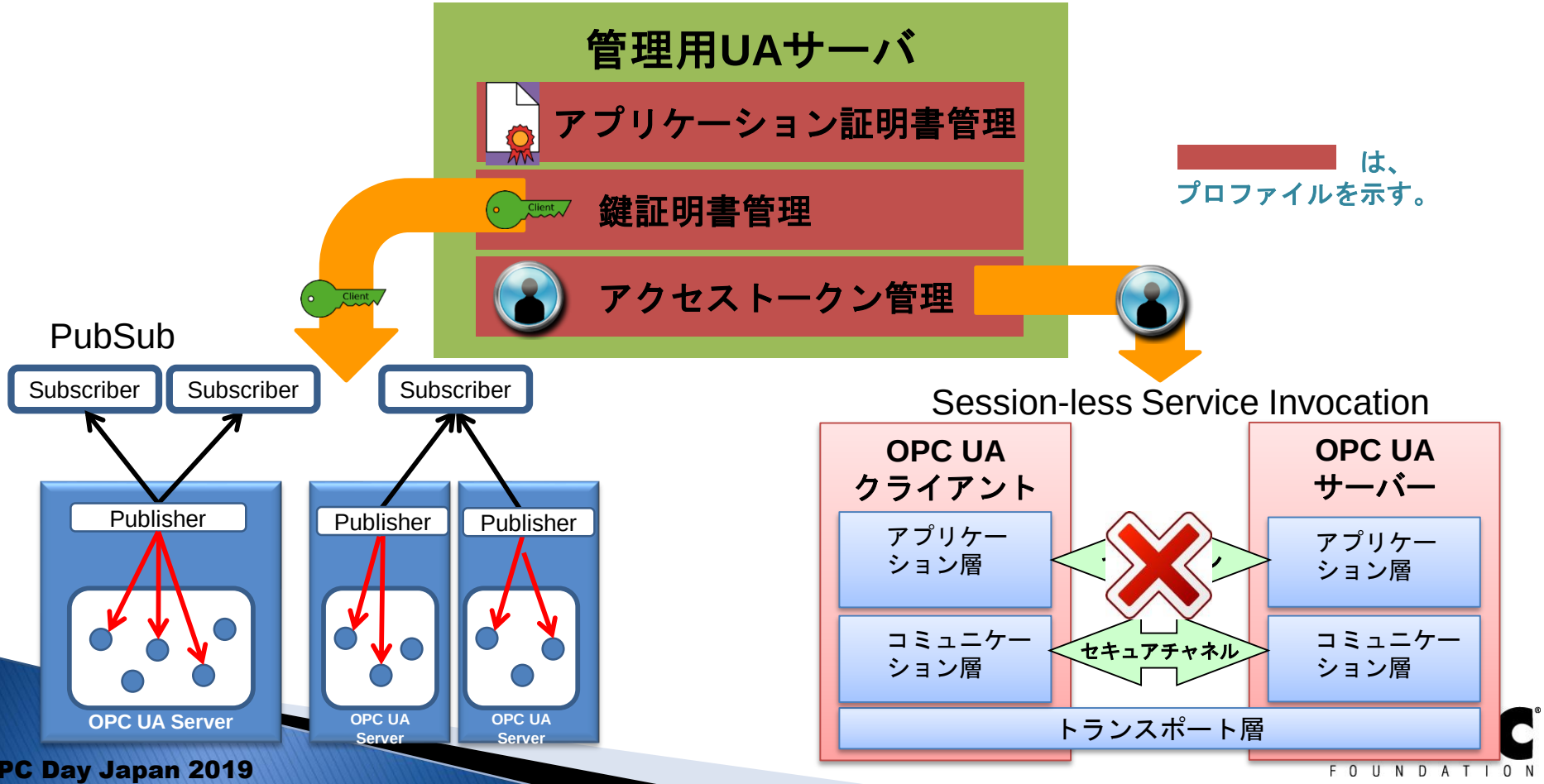
OPC UA 1.04仕様書Part 12の見直し

- タイトル変更
  - 1.03：　Discovery
  - 1.04：　Discovery and Global Services
- Glocal Serviceに関連するサーバープロファイル
  - Global Certificate Management Server Facet
  - KeyCredential Server Facet
  - Authorization Service Server Facet
- 新たなユースケースにおいてもセキュア通信を実現する手段になり得る。

アプリケーション証明書の一括管理



新たな通信モデルのセキュリティ対応



OPC UAセキュリティ機能一覧

認証	アプリケーション認証 – 電子証明書　による認証 ユーザー認証 – ユーザー名／パスワード　または　電子証明書　による認証
認可	アクセス権限 – UAノード単位での権限設定(リード、ライト、メソッド実行の可否) – ロールによる権限設定を表す情報モデルの規定
機密性	暗号化 – 暗号鍵を用いた通信メッセージの暗号化
完全性	署名 – 暗号鍵を用いた通信メッセージの署名 OPC UAメッセージヘッダの活用 – メッセージに振られたシーケンス番号の検証 – ヘッダ内の各種IDの内容の正当性チェック
可監査性	監査証跡履歴 – 監査証跡用イベントタイプの規定
可用性	アプリケーション認証前の処理への考慮 – 接続前の認証・検証処理は最小化し、DOS攻撃に対応 – 不正な接続リクエストの大量受信時は処理を待機して過負荷を回避

日本OPC協議会

URL: https://jp.opcfoundation.org