

OPC UAとUA Securityの ご紹介

The Next Generation of System Interoperability

製造業XMLフォーラム2009

2009.6.5

大田区産業プラザ(PIO)

日本OPC協議会

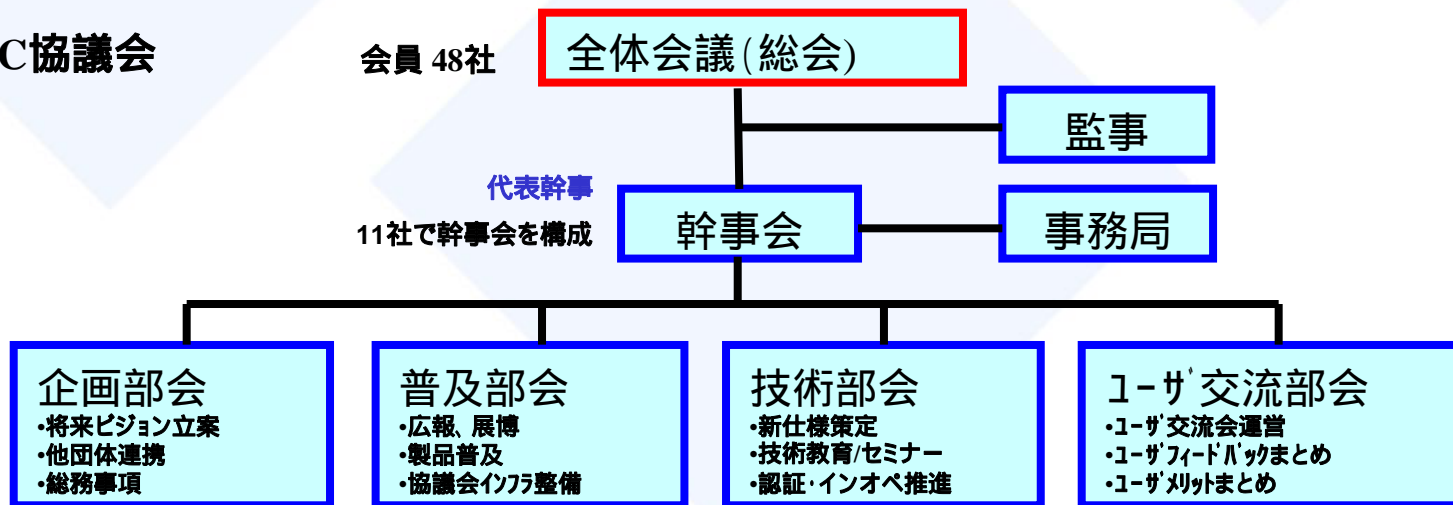
発表者: 藤井 稔久

- OPC協議会について
- OPC仕様の変遷
 - 第1世代 第2世代 第3世代(UA)
- UA仕様について
 - 特徴
 - 開発動向(広がり)
- UAセキュリティについて
 - 想定脅威
 - UAのセキュリティ機能

OPC Foundation / OPC協議会

- 国際的に組織された産業標準化団体：
 - ✓ 450+ Member Companies / 100+ end-users Members
 - ✓ 2500+ Total Companies Build OPC Products = 15000+ Products
- ビジョン：安全で信頼性のある「情報の相互運用性」を実現・提供
 - ✓ For moving information vertically from the factory floor through the enterprise of multi-vendor systems (with stops in between...)
 - ✓ For moving information horizontally between devices on different industrial networks from different vendors
 - ✓ Not just data but information.....
- 行動：
 - ✓ 情報交換のためのオープンプラットフォーム実現に向け、様々な標準化団体と協力・連携を推進

日本OPC協議会



OPC 仕様の変遷

The background features a light blue horizontal line across the top. Below it, several light blue diamonds are scattered across the page, some overlapping. The text 'OPC 仕様の変遷' is centered in a dark blue font.

第一世代： プロセスデータ交換 I/F

OPC

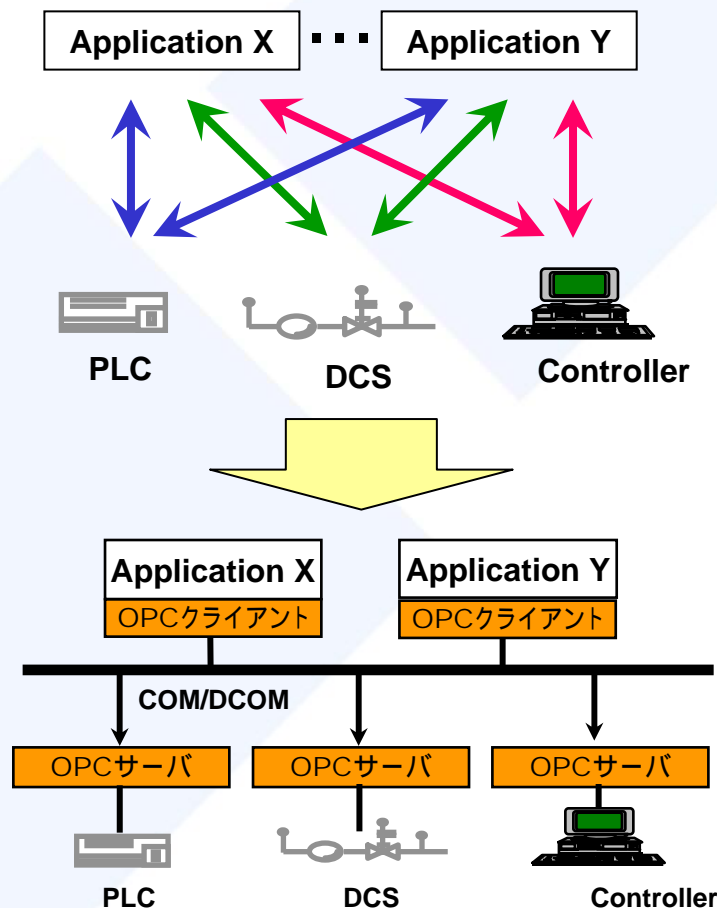
ベンダや機器に依存することなくデータ交換を行なうClient / Server システムのための標準インターフェースです。

課題

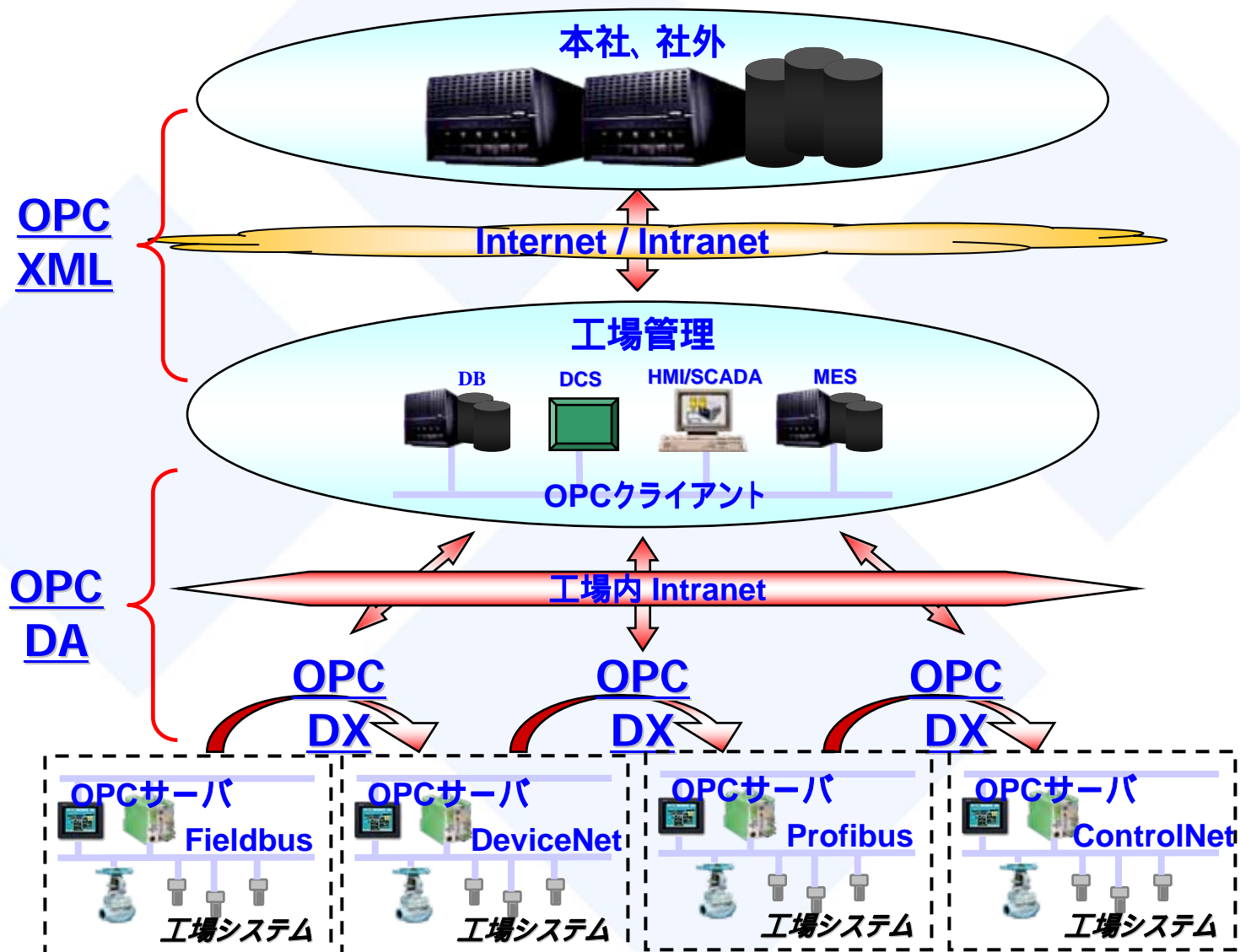
- ✓ 多数のベンダー製品
- ✓ カスタムメイドのソリューション
- ✓ プロプラエタリな技術
- ✓ 1対1結合による統合
- ✓ 限られたリアルタイム情報
- ✓ 保守の悪夢
- ✓ 散逸した責任

解決策

- ✓ OPC !

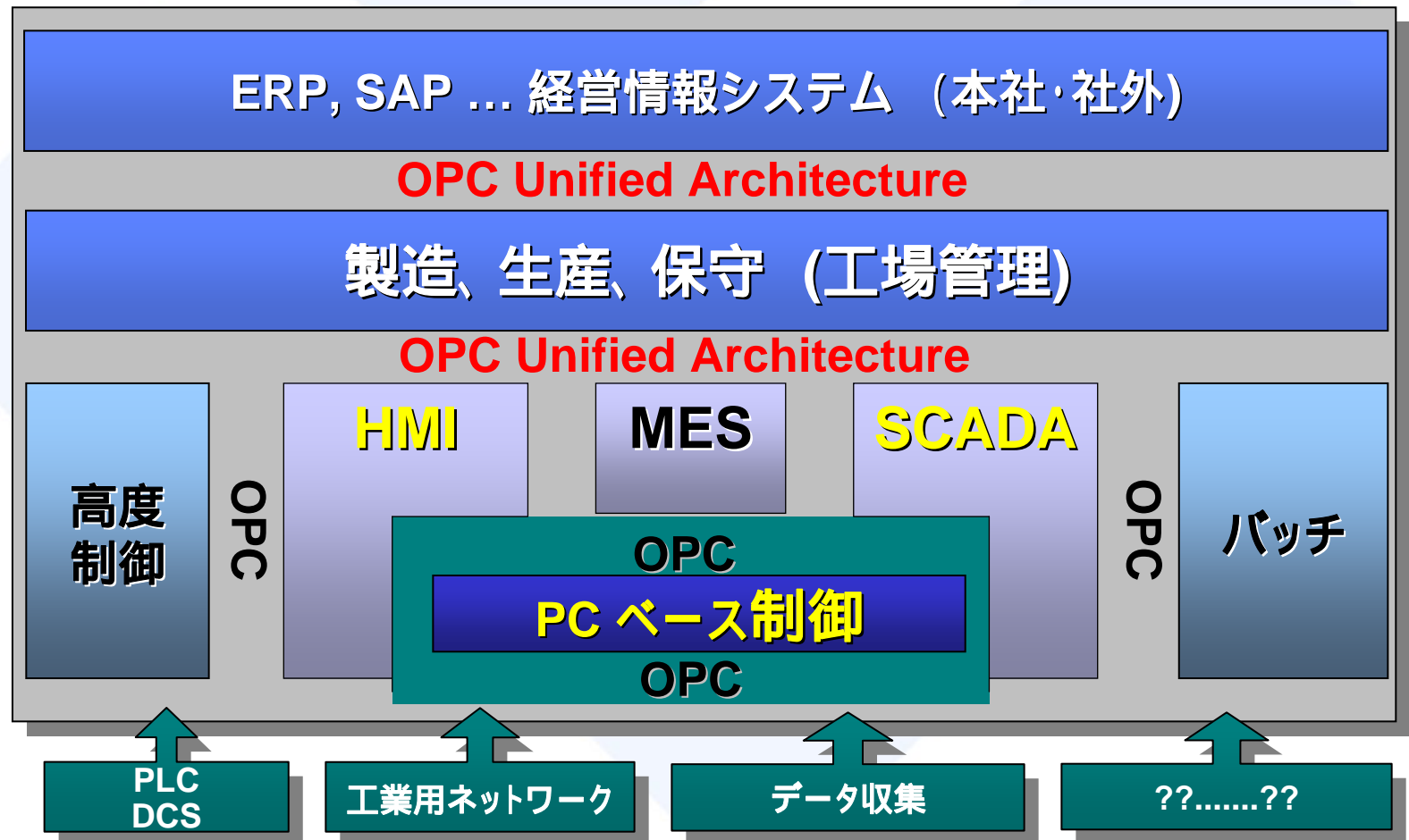


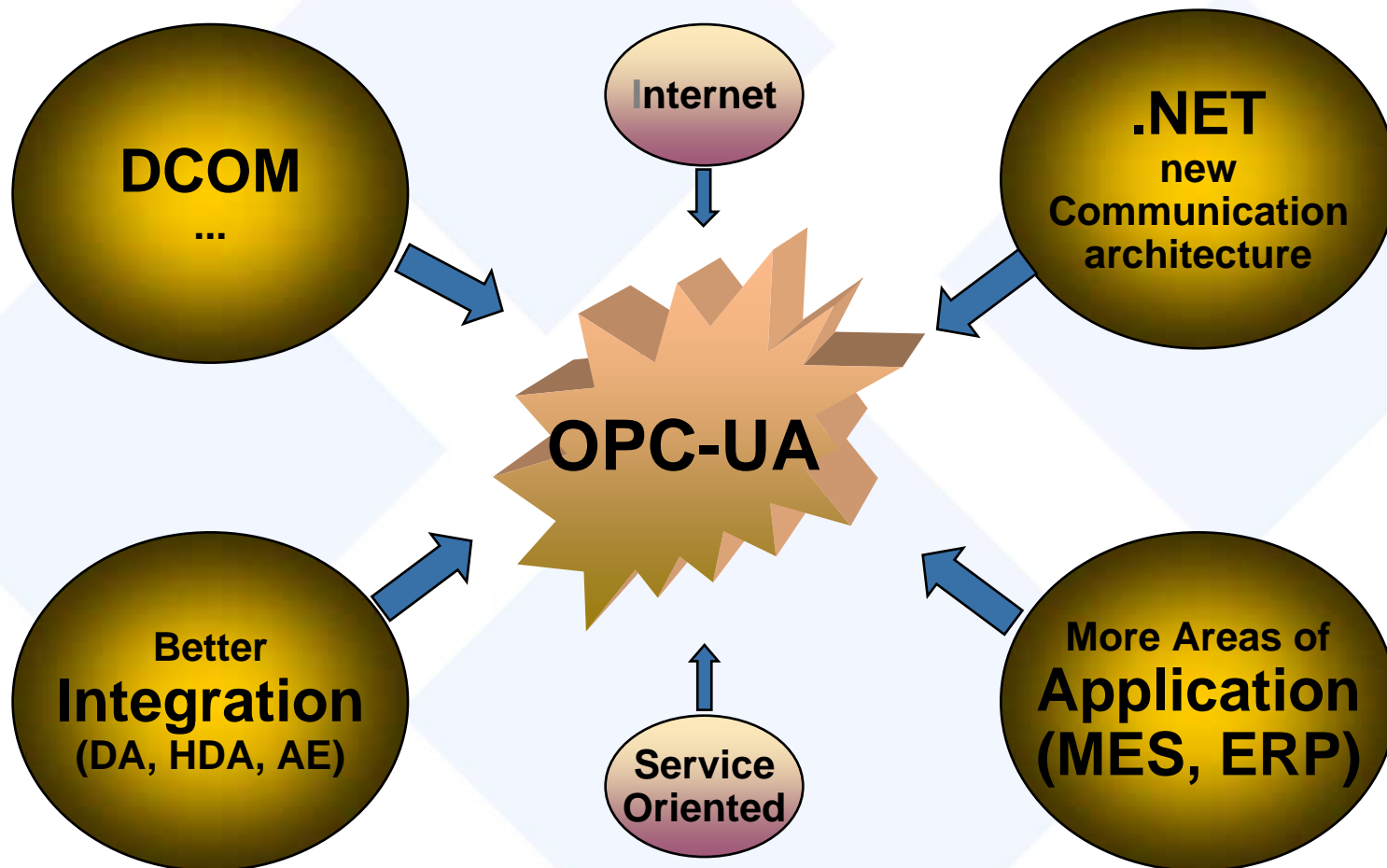
第二世代： 水平・垂直データ交換 I/F



第三世代(UA)： 製造情報データ連携 I/F

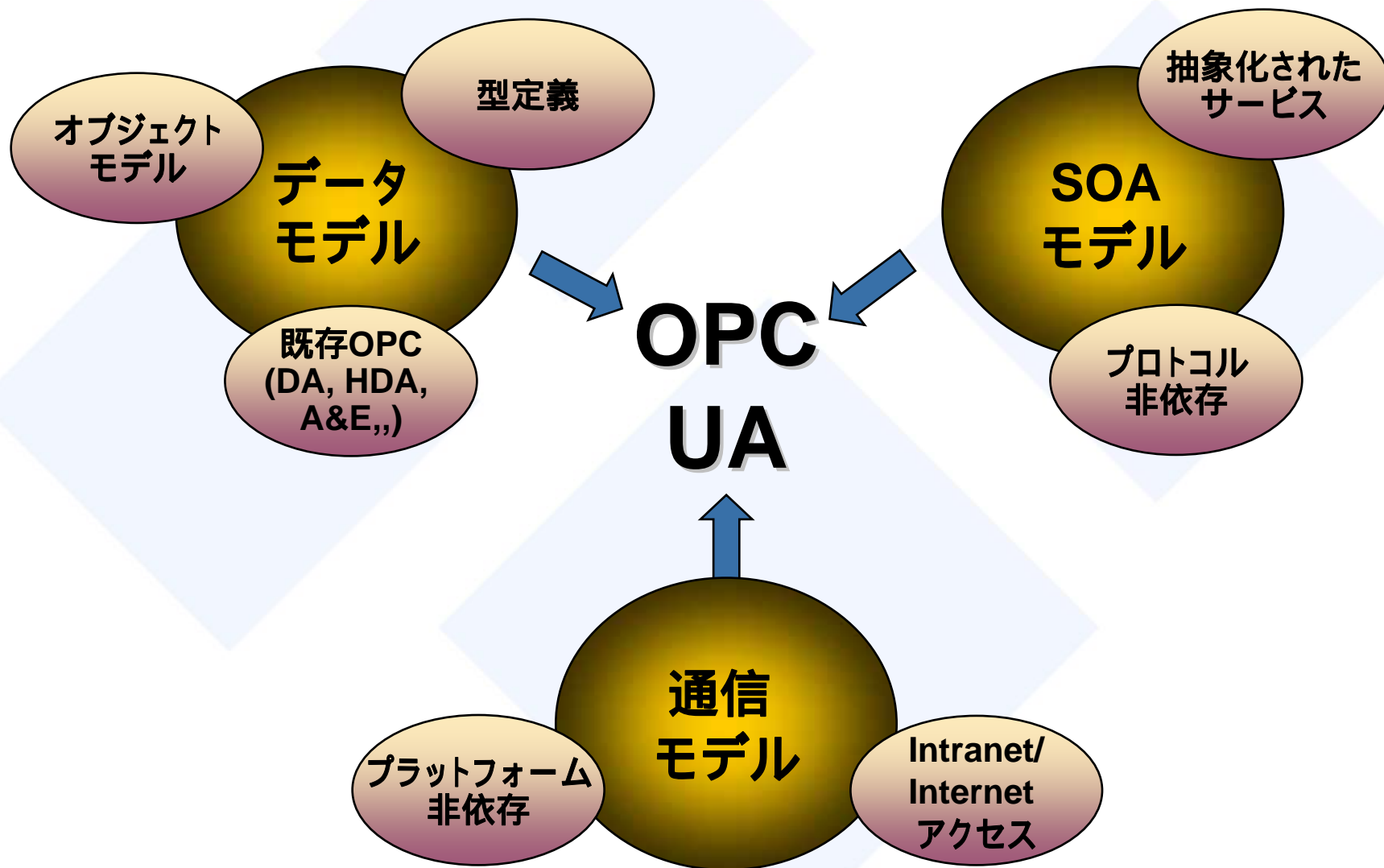
OPC UA : 業界標準の相互運用性を提供
interOperability, Productivity & Collaboration



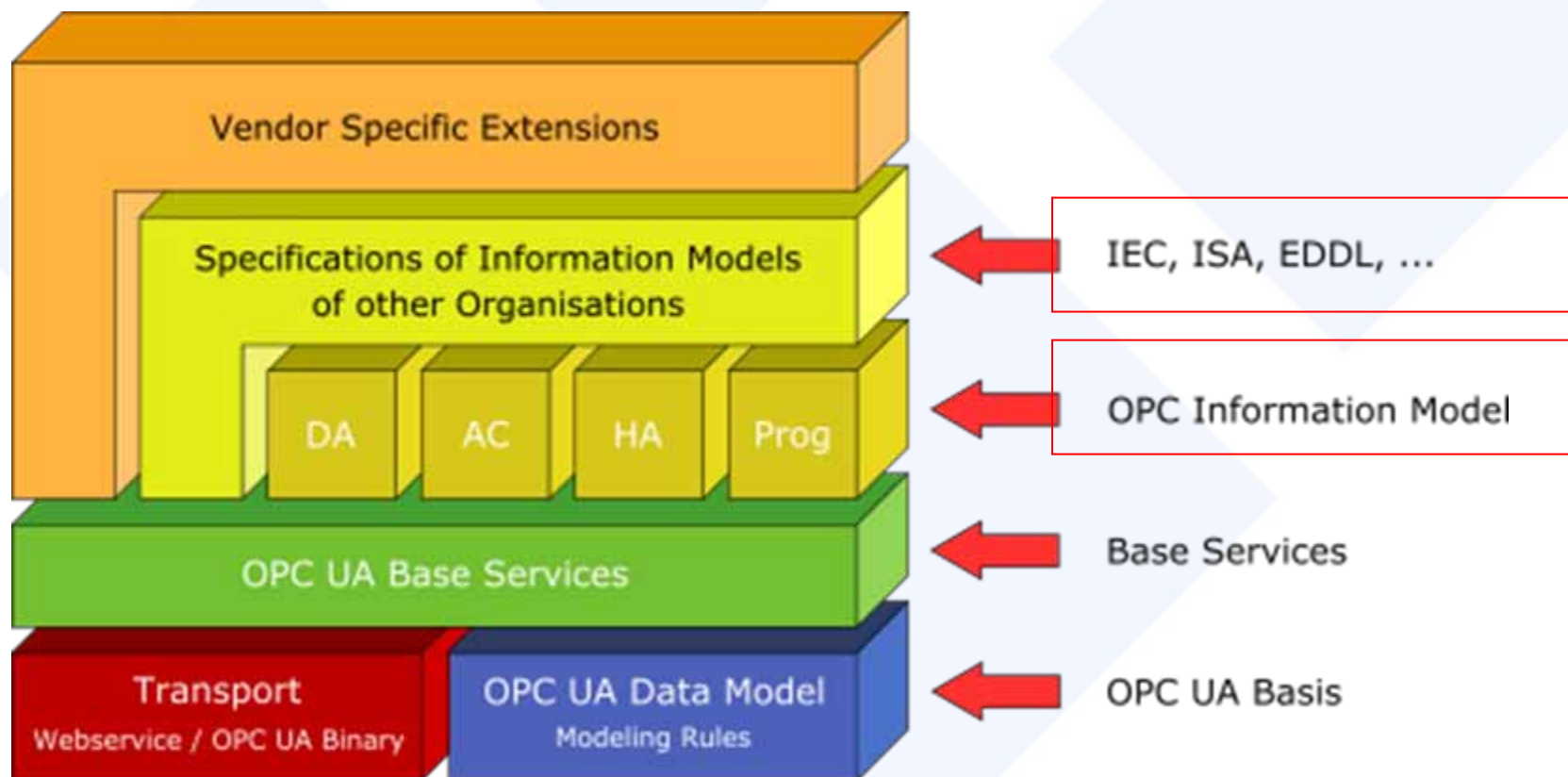


UA仕様について

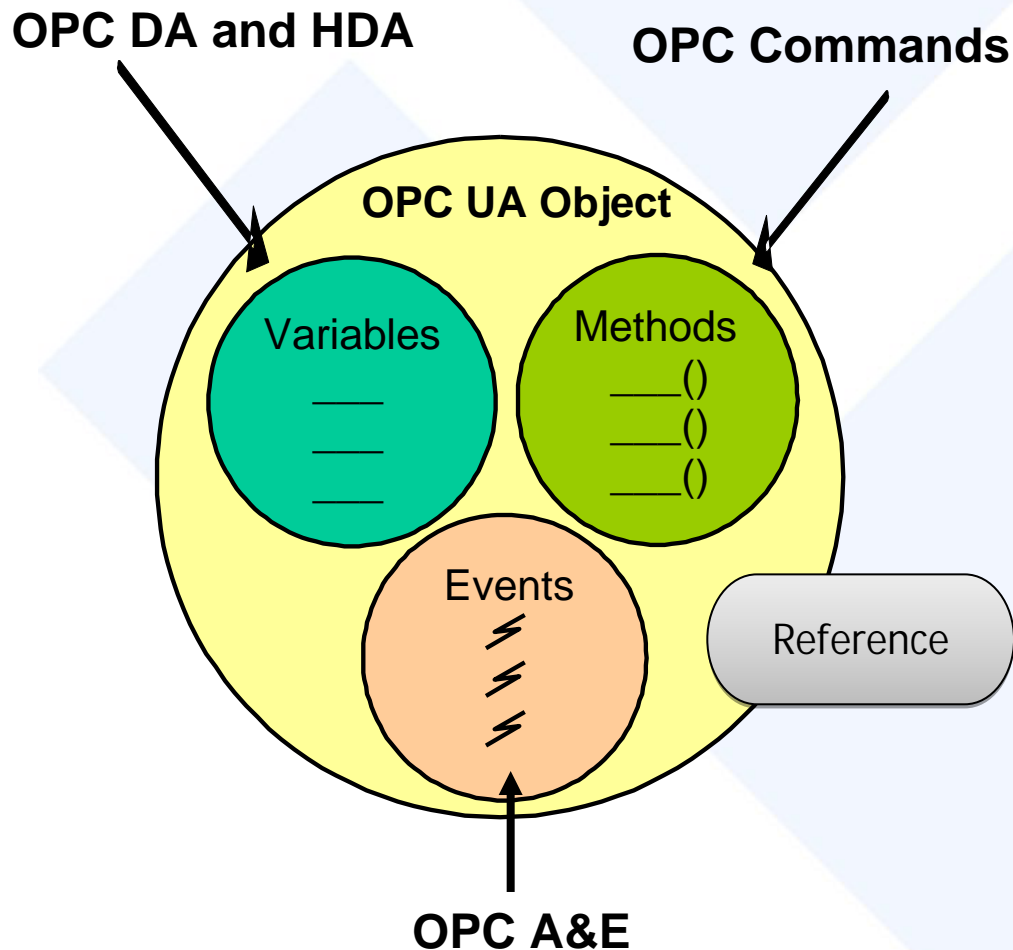
特徴: UA (Unified Architecture) とは？



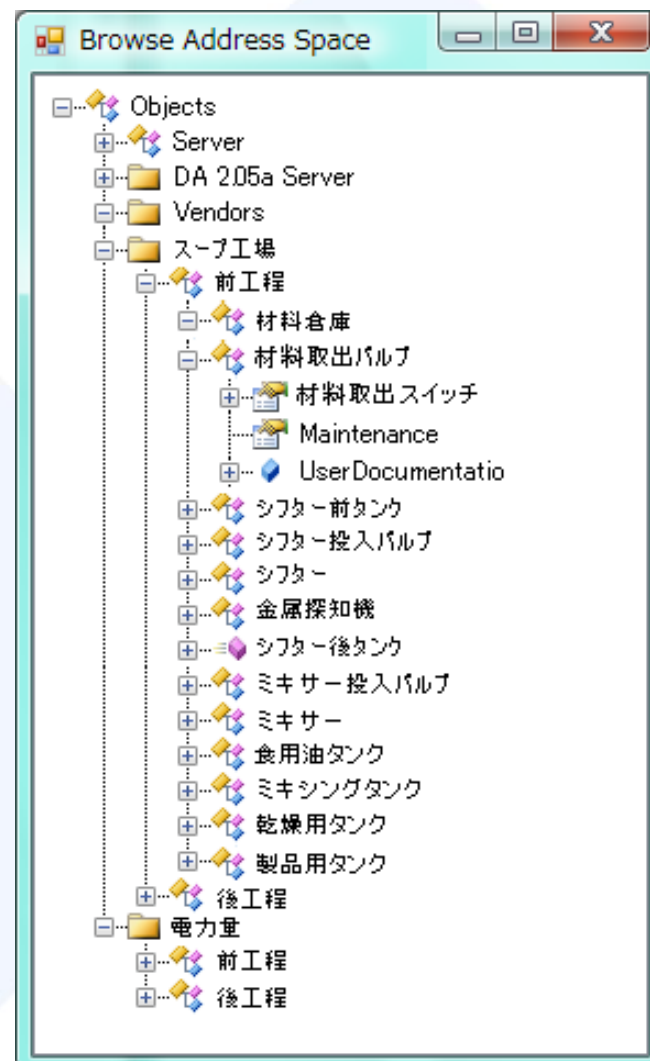
- Modeling Data – 制御対象(デバイス)に依存しないI/F
- Transport Data – 通信媒体に依存しないI/F



UA オブジェクトモデル

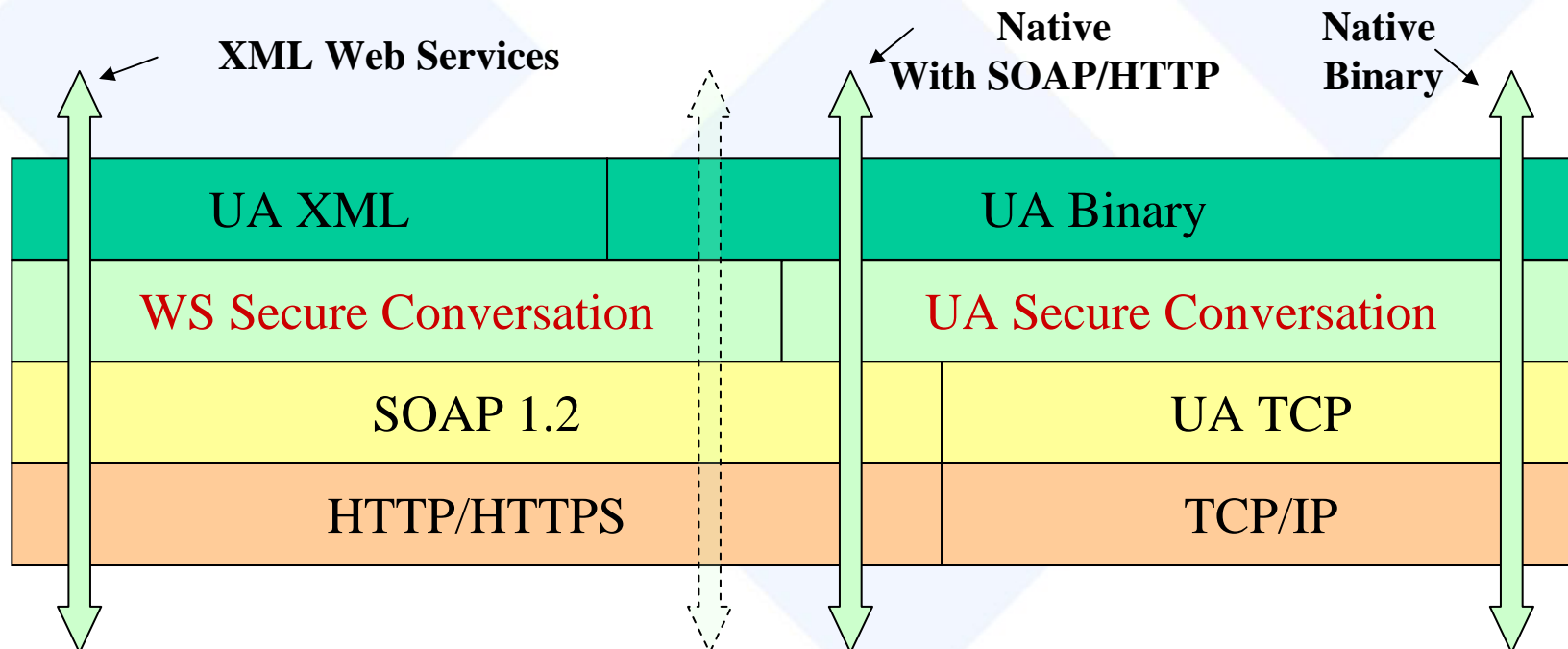


UA アドレススペース



SecurityをBuilt-inした3種類のスタックプロファイル:

- XML Web Service : ITシステムとの親和性 ERP / ビジネスApp
- Native Binary : 高速通信 組み込み / PCベース制御 / SCADA
- Native with SOAP/HTTP : MES / ERP



動向：IEC国際標準化(IEC62541)

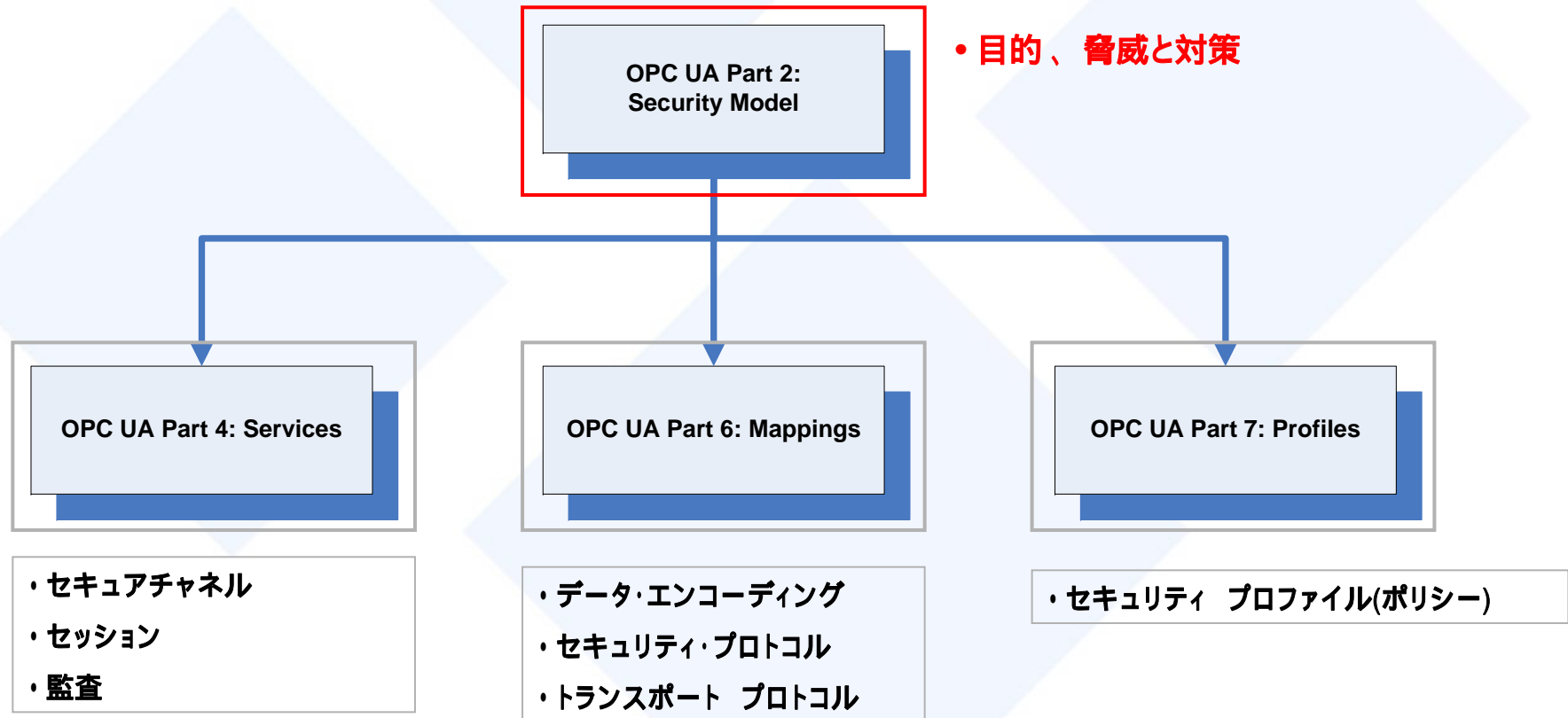
- ◆ 2007 - 05 US NCより提案 OPC-Fコンソーシアム リエーゾン
- ◆ 2007 - 05 NP(パート 1-10ドラフト含む)回送
- ◆ 2007 - 08 NP 承認
WG6設置:US、SE、FI、JP、CH、CA、FR、DE
(14名のエキスパート)
- ◆ 2007 - 09 CD1 パート 1-10 配布
- ◆ 2007 - 09 第1回WG8会議キックオフ(仏)
- ◆ 2008 - 01 第2回WG8会議 CD1のNCコメント審議
- ◆ 2008 - 04 CD1 パート 1-10 のNCコメントに対する回答
- ◆ 2008 - 06 CDV パート1-6、8配布
- ◆ 2008 - 11 第3回WG8会議 CDVコメント審議(国内)
- ◆ 2008 - 11 CD2パート7、9、10配布
- ◆ 2009 - 01 CDV パート1-6、8承認

UA Securityについて

● UAセキュリティ:仕様書(12部)のコア仕様として定義

- Part.1 :Concepts & Overview //概要
-
- **Part.2 :Security Model //コア仕様**
- **Part.3 :Address Space Model // ..**
- **Part.4 :Services // ..**
- **Part.5 :Information Model // ..**
- **Part.6 :Service Mappings // ..**
- **Part.7 :Profiles // ..**
-
- Part.8 :Data Access //OPC独自情報モデル
- Part.9 :Alarms and Conditions // ..
- Part.10 :Programs // ..
- Part.11 :Historical Access // ..
-
- Part.12 :Discovery

UA Securityの構成



- UA Security : 目的・脅威・対策

Part.2: UAに求められるクライアント/サーバシステムのSecurityアセスメント結果

目的: システムの機密性、完全性、可用性

Threat(s)	Mitigation(s)
<ul style="list-style-type: none">・メッセージ氾濫・盗聴・メッセージのなりすまし・メッセージ改ざん・メッセージリプレイ・マルフォームメッセージ・サーバプロファイリング・セッションハイジャック・...	<ul style="list-style-type: none">●ユーザ認証●アプリケーション認証●メッセージ認証●監査●侵入検知システム●侵入防止システム●...

- UA Security : アプリケーション

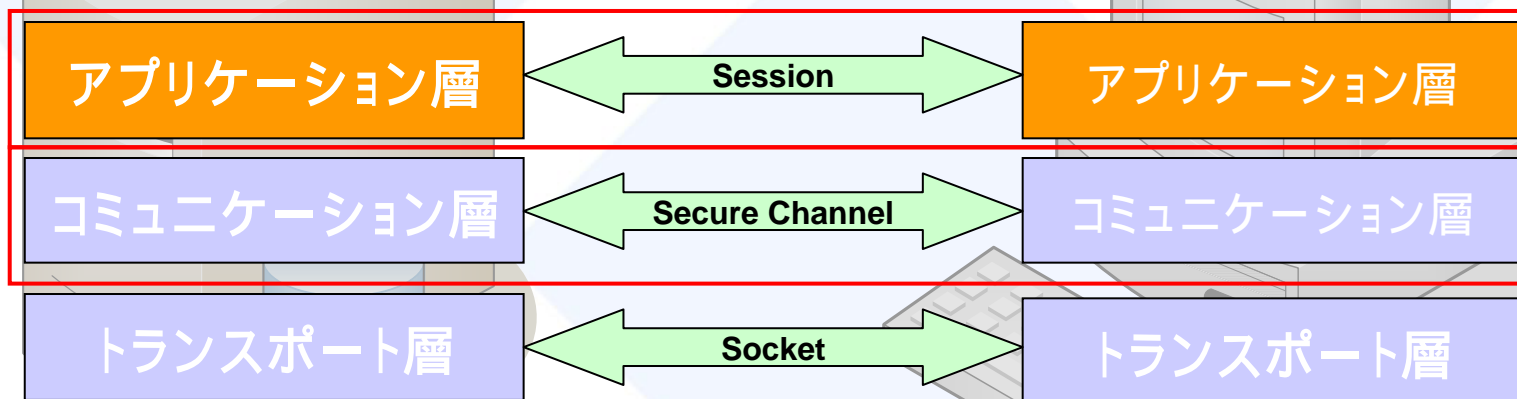
● Secure アプリケーション

安全なアーキテクチャを採用し、安全メカニズムをビルトイン

OPC UA Client

OPC UA Server

- ・アプリケーション認証
- ・ユーザ認証
- ・メッセージの完全性
- ・ユーザ権限の付与
- ・メッセージの機密性



● Security モード

- None – セキュリティなし
- Sign – メッセージに署名は付けるが、暗号化はしない。
- SignAndEncrypt – メッセージに署名は付けかつ暗号化する。

● Security ポリシー

- Basic128Rsa15 – 最低限のセキュリティ(高速応答性が必要な場合)
- Basic256 – 推奨セキュリティ
- None – 推奨できない

Security要件に応じて組合せをプロファイルに定義し、使い分けます。

● セッション管理

- UAアプリケーション層で実装
- Client/Server間のハイレベルな論理的接続機能を提供
- ユーザの認証・認可(アクセス制御)によりClientのServerアクセスを制限
- セッションの確立にはSecureチャネルの開設が必要

● Secureチャネル

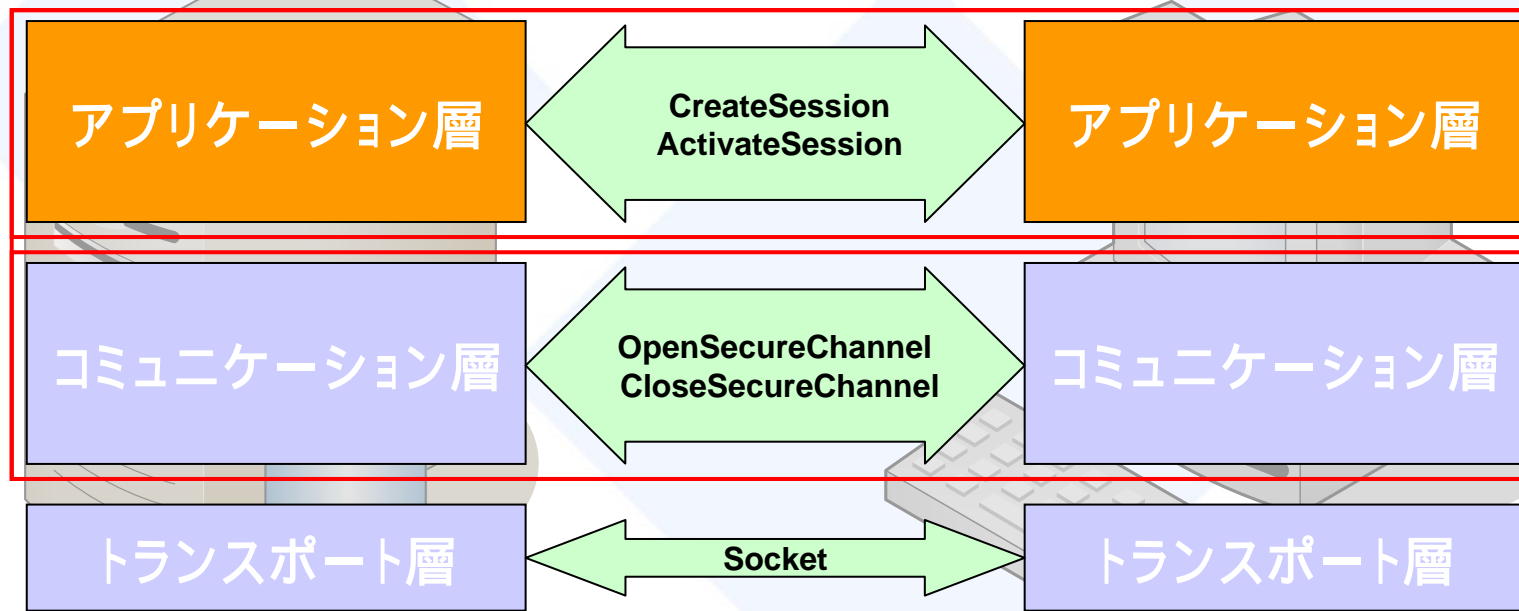
- UAコミュニケーション層(通信スタック)で実装
- Client/Server間のローレベルな論理的接続機能を提供
- アプリケーション認証のための証明書を提供
- 送信メッセージを暗号化するなど、Secureなメッセージ送信を可能に！
- 受信メッセージの署名による改ざん検査(Verify)など、Secureなメッセージ受信を可能に！

- UA Security : サービス

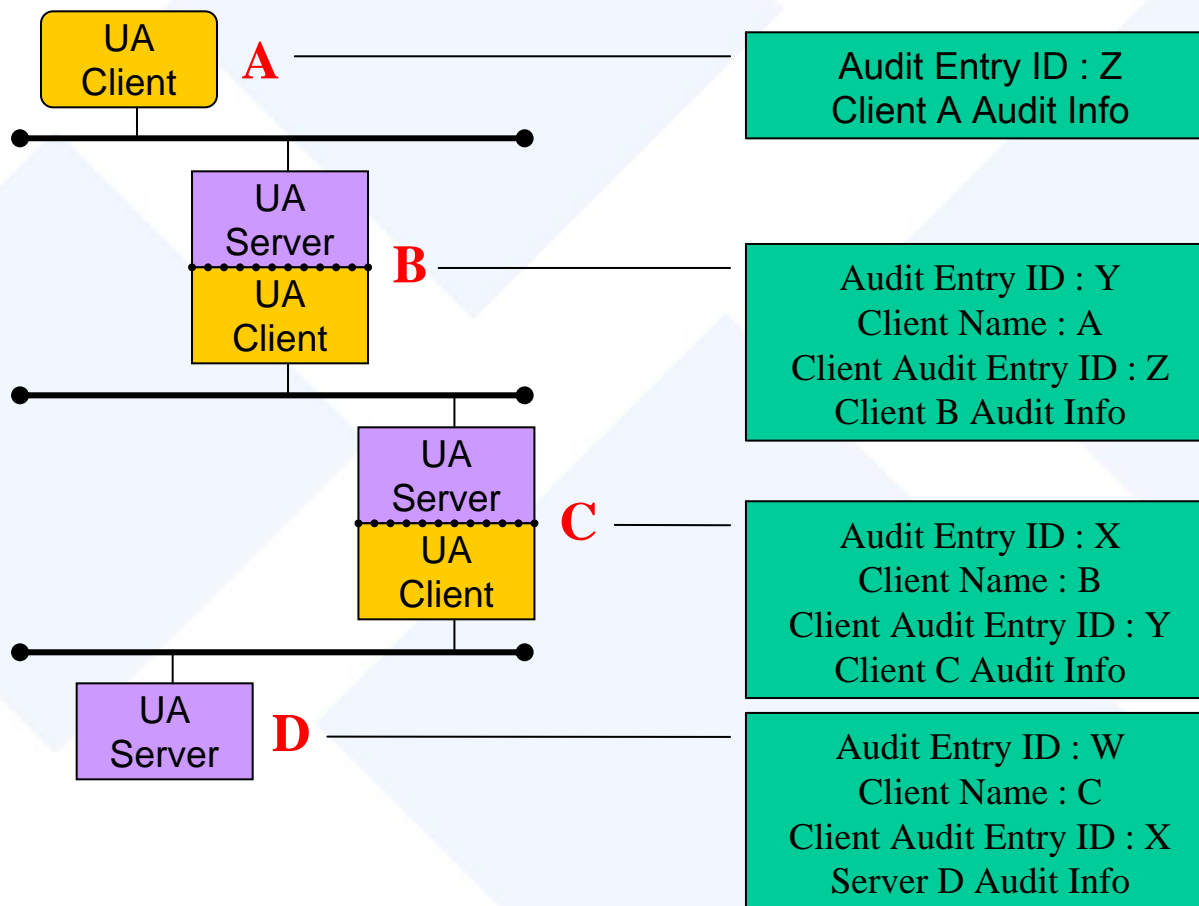
- セッション Service Set
- セキュアチャネル Service Set
- 監査

OPC UA Client

OPC UA Server



- UA Security: 監査



- UA Security : まとめ

UAセキュリティは特殊なものではありません。

ITの世界で標準的に使用されているセキュリティ対策を使用します。

UAセキュリティのための特別な実装は不要です。

スタックに実装されている機能を利用することにより
その恩恵を簡単に享受することができます。

Questions?

● 日本OPC協議会

