OPC UAのセキュリティ機能の紹介

日本OPC協議会技術部会

目次

- OPC UAセキュリティの目的
- 脅威と対策の具体例
- セキュリティ要件
- OPC UAの対象外
- まとめ
- 証明書の運用方法

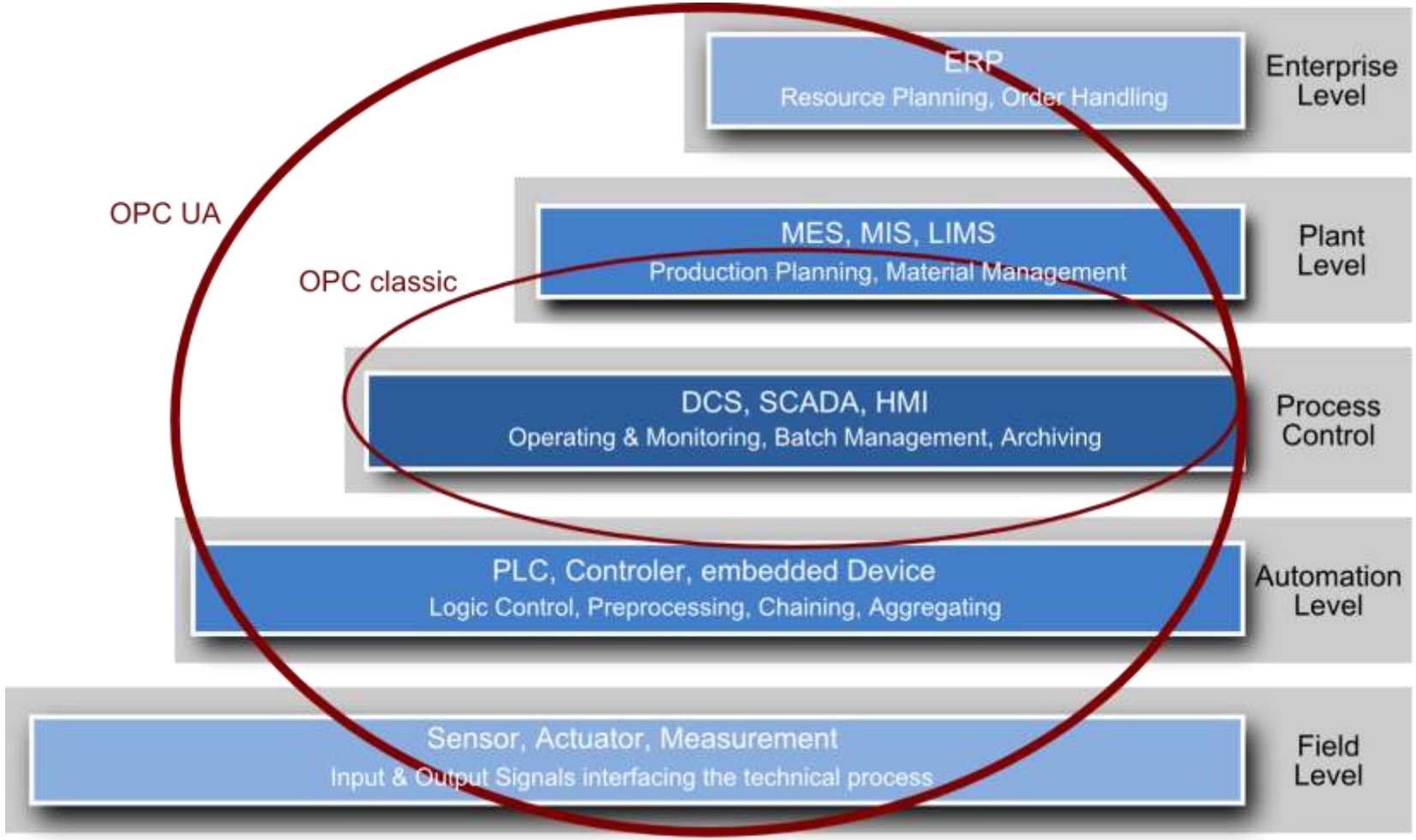
Copyright © 2016, OPC Council Japan, All Rights Reserved

目次

- OPC UAセキュリティの目的
- 脅威と対策の具体例
- セキュリティ要件
- OPC UAの対象外
- まとめ
- 証明書の運用方法

Copyright © 2016, OPC Council Japan, All Rights Reserved

OPC UA – 通信のスケーラビリティ

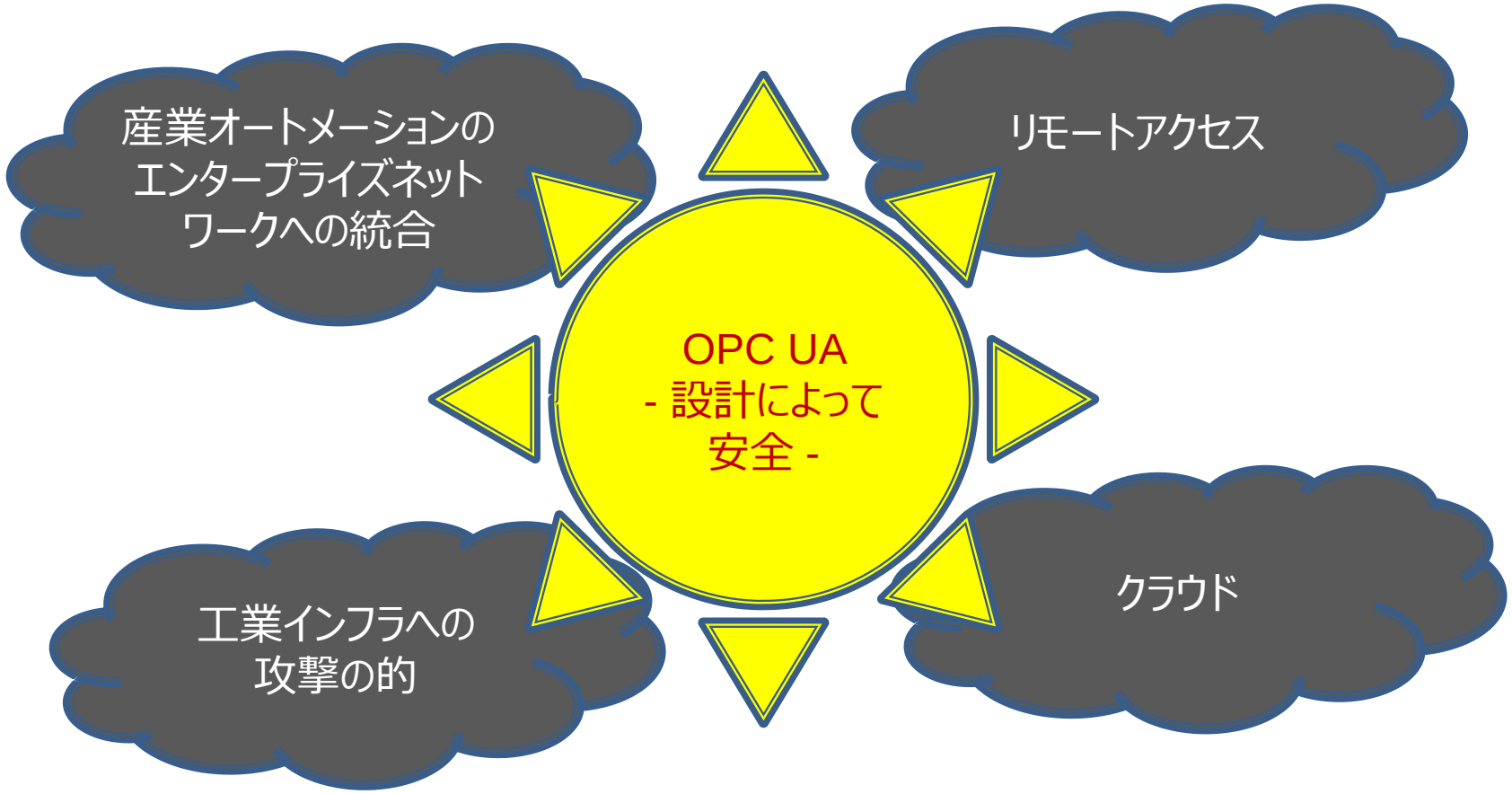


source: www.ascolab.com

Copyright © 2016, OPC Council Japan, All Rights Reserved

OPC FOUNDATION

なぜー OPC UA セキュリティ?



Copyright © 2016, OPC Council Japan, All Rights Reserved

目次

- OPC UAセキュリティの目的
- 脅威と対策の具体例
- セキュリティ要件
- OPC UAの対象外
- まとめ
- 証明書の運用方法

Copyright © 2016, OPC Council Japan, All Rights Reserved

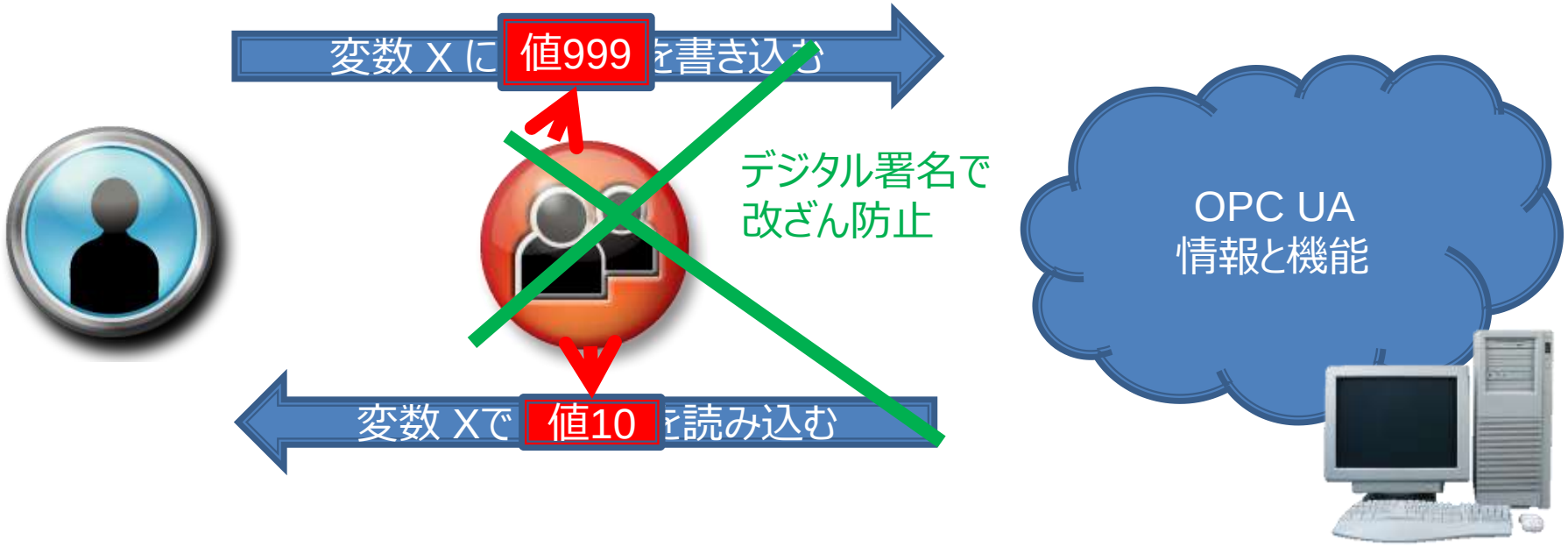
OPC UAにおけるセキュリティ対策

- **メッセージの盗聴**
  → メッセージの内容を読み取られない。

Copyright © 2016, OPC Council Japan, All Rights Reserved

OPC UAにおけるセキュリティ対策

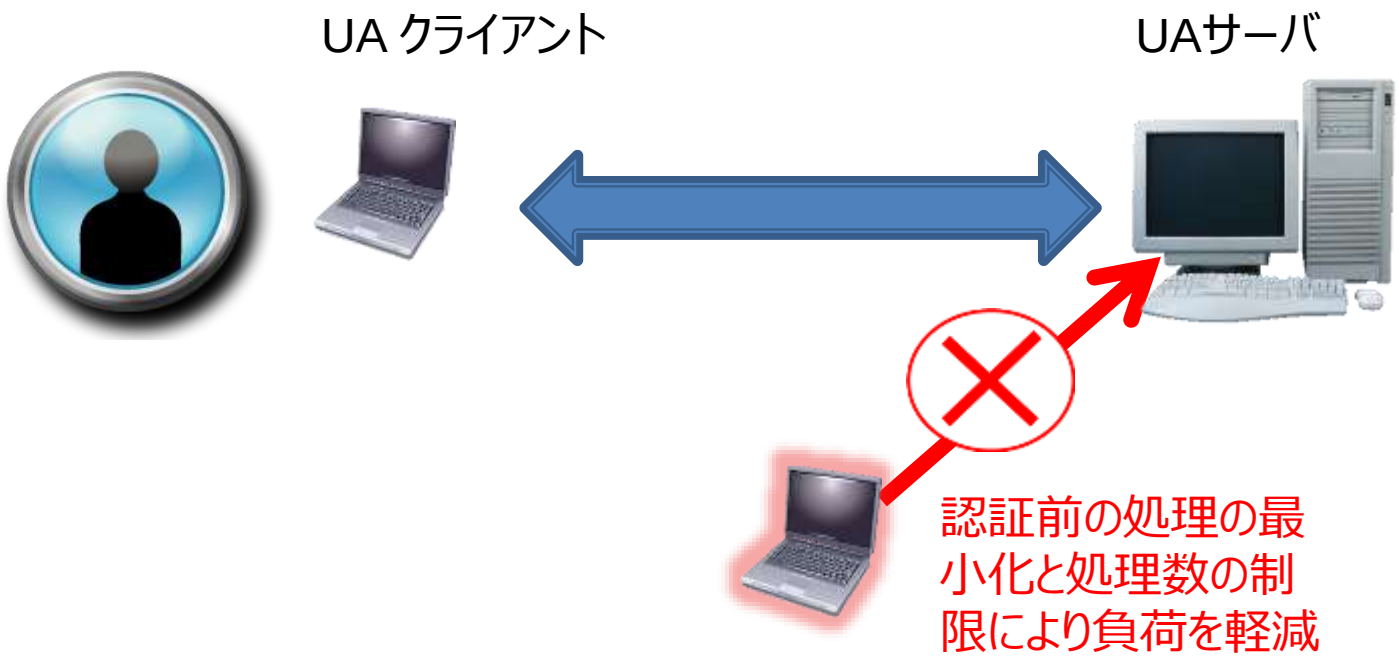
- **メッセージの改ざん**
  → メッセージの内容を書き変えられない。



Copyright © 2016, OPC Council Japan, All Rights Reserved

OPC UAにおけるセキュリティ対策

- **システム稼働率を低下させるメッセージ攻撃**
  → 攻撃によって使用されるリソースの最小化。

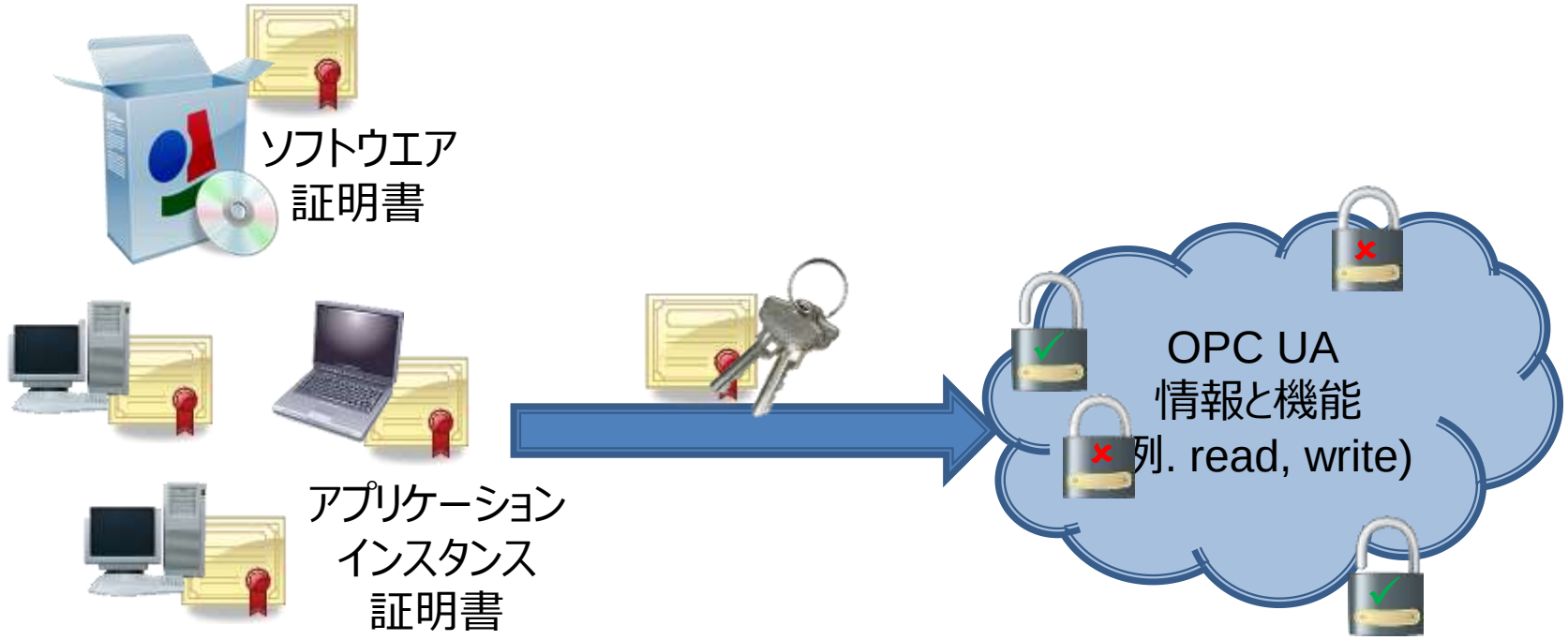


Copyright © 2016, OPC Council Japan, All Rights Reserved

OPC UAにおけるセキュリティ対策

- 不正なアプリケーションからの接続

→アプリケーションの認証と認可

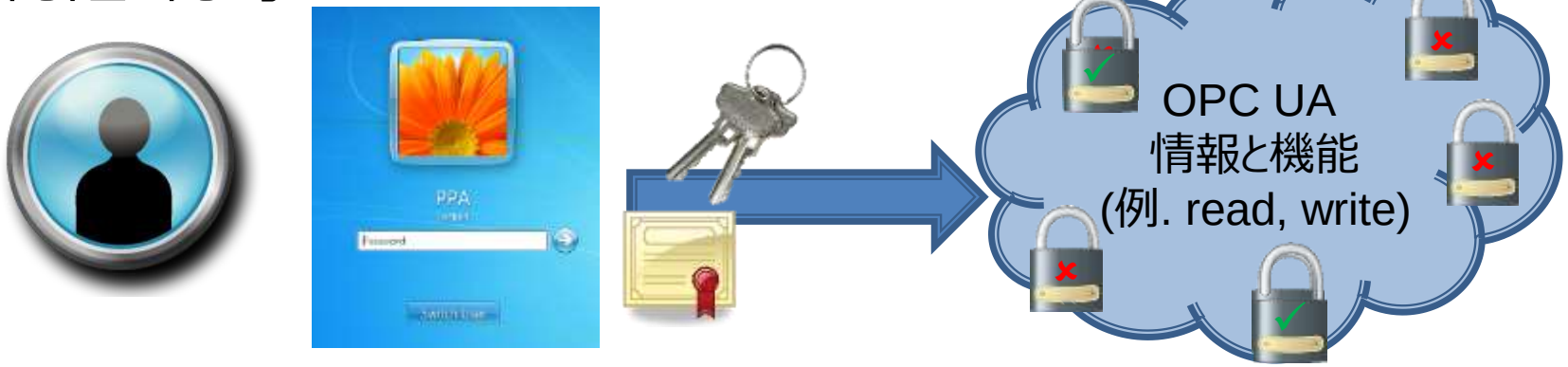


Copyright © 2016, OPC Council Japan, All Rights Reserved

OPC UAにおけるセキュリティ対策

- **権限のないユーザの接続**

→ ユーザの認証と認可



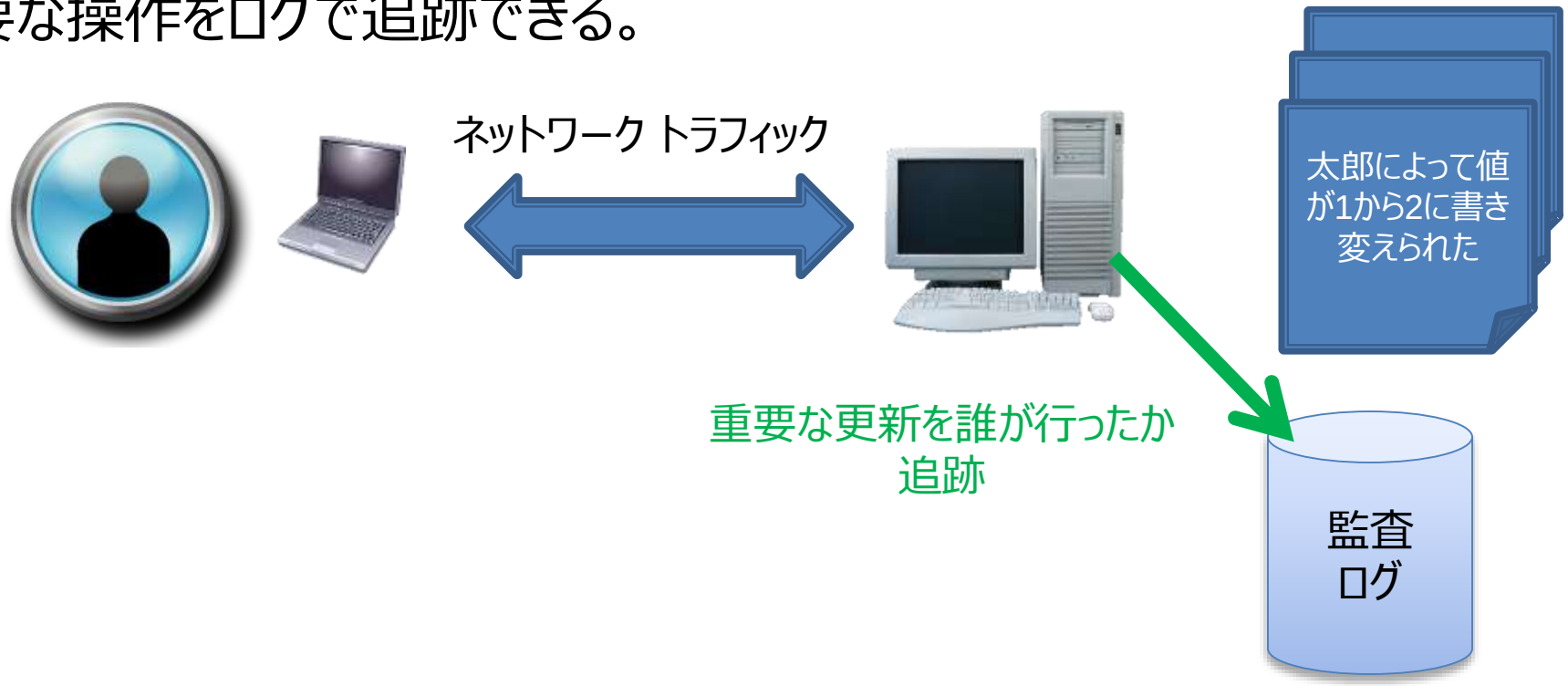
1. ユーザ認証
(例 ユーザ名とパスワード)

2. 特定の操作と情報のための認可
(例 値の書き込み)

Copyright © 2016, OPC Council Japan, All Rights Reserved

OPC UAにおけるセキュリティ対策

- **システムが安全に動作していることを証明したい。**
  →重要な操作をログで追跡できる。



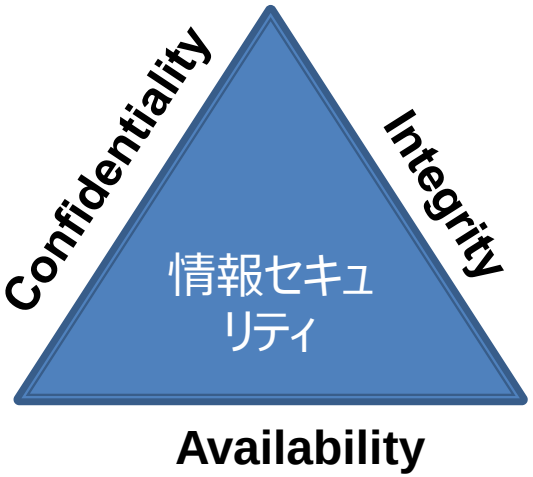
Copyright © 2016, OPC Council Japan, All Rights Reserved

目次

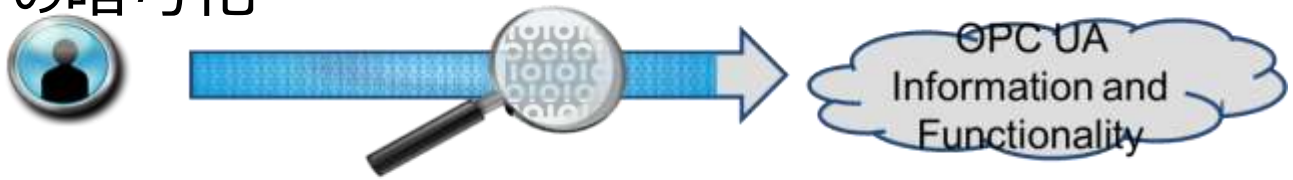
- OPC UAセキュリティの目的
- 脅威と対策の具体例
- セキュリティ要件
- OPC UAの対象外
- まとめ
- 証明書の運用方法

Copyright © 2016, OPC Council Japan, All Rights Reserved

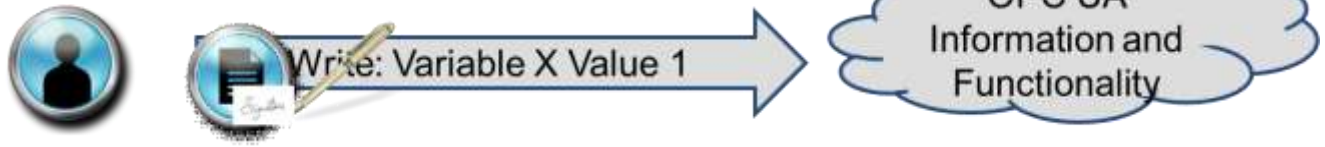
トランスポート層のセキュリティ



- **機密性**
  → メッセージの暗号化



- **完全性**
  → デジタル署名

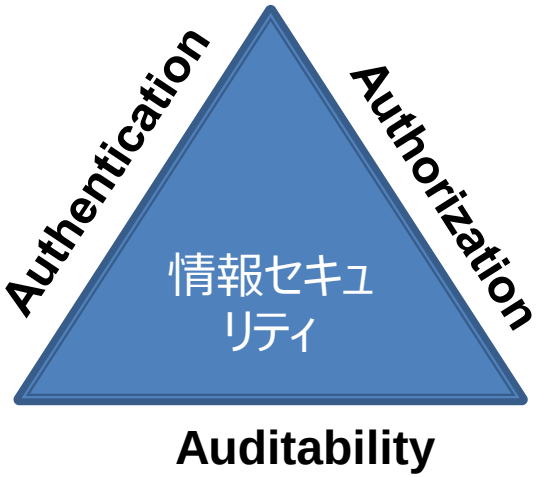


- **可用性**
  →認証前の処理を最小化
  →防御は主にサイトに依存

例:
- メッセージ長を制限する。
- セキュリティ関連のエラーコードを返さない。

Copyright © 2016, OPC Council Japan, All Rights Reserved

アプリケーション層のセキュリティ



- **ユーザの認証**
  - ユーザ名/パスワード, WS-Security トークン または X.509 証明書
  - Active Directoryのような既存の基盤
- **アプリケーションの認証**
  - アプリケーションインスタンス証明書
  - 認証局
- **認可**
  - 認可のやり方はサーバ実装依存
  - アドレス空間におけるきめ細やかな情報のアクセス制御
    - *AccessLevel* と *UserAccessLevel* – 値と履歴の読み書き
    - *WriteMask* と *UserWriteMask* – メタデータの書き込み
    - *Executable* と *UserExecutable* – メソッドの呼び出し
    - アクセスできない情報はクライアントから見えない (リファレンス、イベントなど)
- **監査**
  - セキュリティ関連の操作の監査イベントの生成

Copyright © 2016, OPC Council Japan, All Rights Reserved

目次

- OPC UAセキュリティの目的
- 脅威と対策の具体例
- セキュリティ要件
- OPC UAの対象外
- まとめ
- 証明書の運用方法

Copyright © 2016, OPC Council Japan, All Rights Reserved

OPC UA の対象外

- **ユーザ管理**
  - ユーザの追加、削除、役割への配置のようなユーザ管理のやり方は非標準。
  - ユーザの役割は非標準＞これはサーバ独自またはコンパニオンスペックで定義
- **ユーザ権限の管理**
  - アクセス権限の定義のやり方は非標準　＞これはサーバ独自またはコンパニオンスペックで定義
- **ユーザ認証の管理**
  - 生体認証のようなメカニズムは規定していないが、OPC UAのインフラストラクチャーでは利用できる。
  - パスワードのために規約はない
    - 文字の規約(最小文字数、大文字、数字、特殊文字など)
    - パスワードの有効期間
    - パスワードの保管方法
- **組織的な課題**
  - サイトに物理的なアクセス処理の仕方
  - ゾーン、セキュリティライフサイクルまたはセキュリティポリシー
  - 人材の育成
- 以上のことは次のスペックで説明されている
  - IEC 62443 (ISA 99)
  - NERC CIP
  - Regulations and Corporate Standards

Copyright © 2016, OPC Council Japan, All Rights Reserved

目次

- OPC UAセキュリティの目的
- 脅威と対策の具体例
- セキュリティ要件
- OPC UAの対象外
- まとめ
- 証明書の運用方法

Copyright © 2016, OPC Council Japan, All Rights Reserved

セキュリティ(まとめ)

- 資産ごとに適切なセキュリティ・コントロールの選択
  - 作業者の権限レベル
- 異なるレイヤーで、OPC UAセキュリティポリシーを選択
  - Basic256Sha256
  - Basic128Rsa15
  - Basic256
  - None
- OPC UA セキュリティモードを選択
  - SignAndEncrypt
  - Sign
  - None
- OPC UA の統一的な監査履歴
- OPC UAセキュリティのための特別な実装は不要。

Copyright © 2016, OPC Council Japan, All Rights Reserved

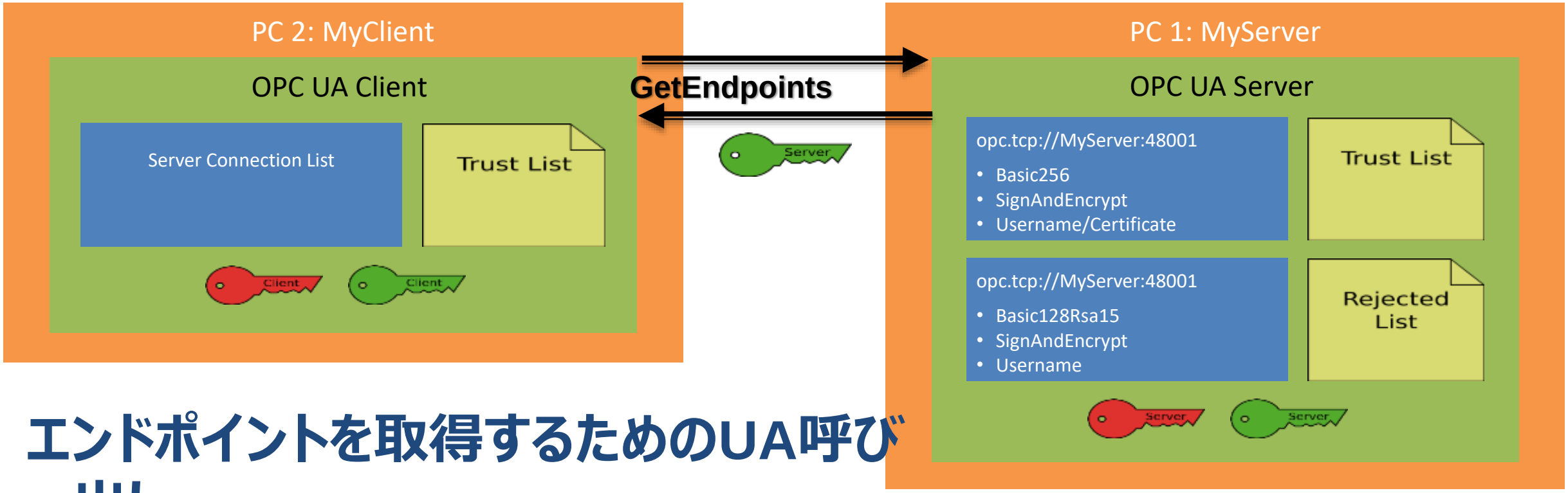
OPC FOUNDATION

目次

- OPC UAセキュリティの目的
- 脅威と対策の具体例
- セキュリティ要件
- OPC UAの対象外
- まとめ
- 証明書の運用方法

Copyright © 2016, OPC Council Japan, All Rights Reserved

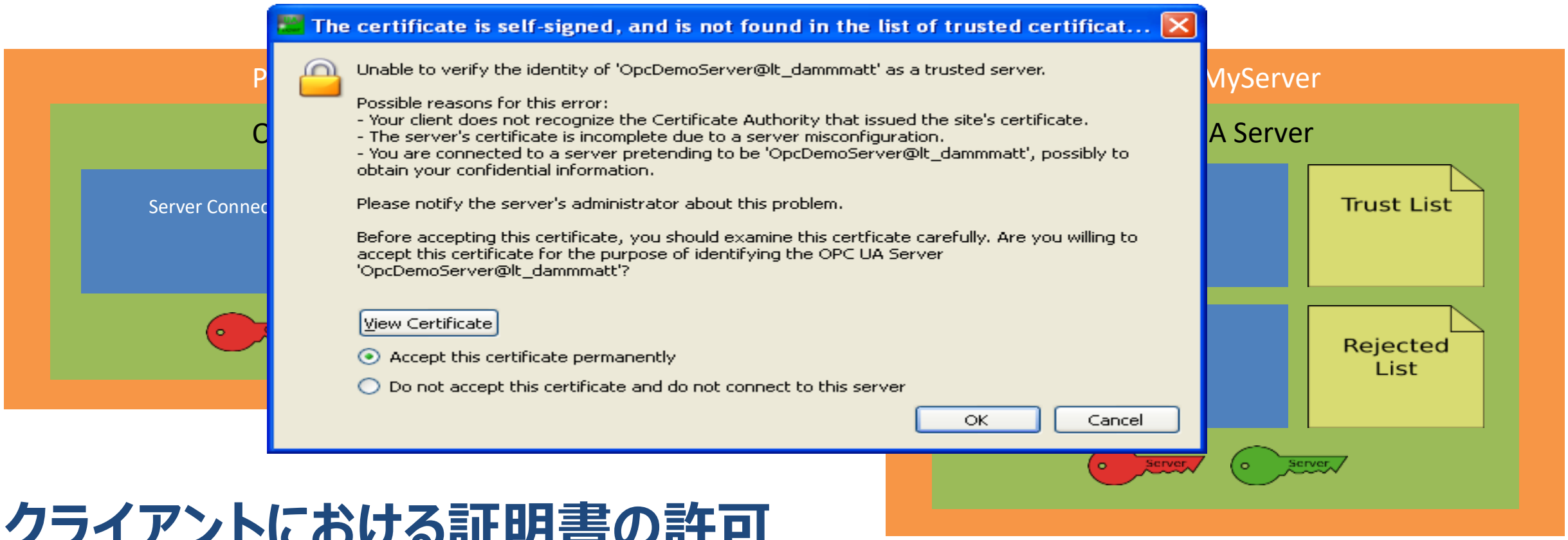
接続の流れ



エンドポイントを取得するためのUA呼び出し

Copyright © 2016, OPC Council Japan, All Rights Reserved

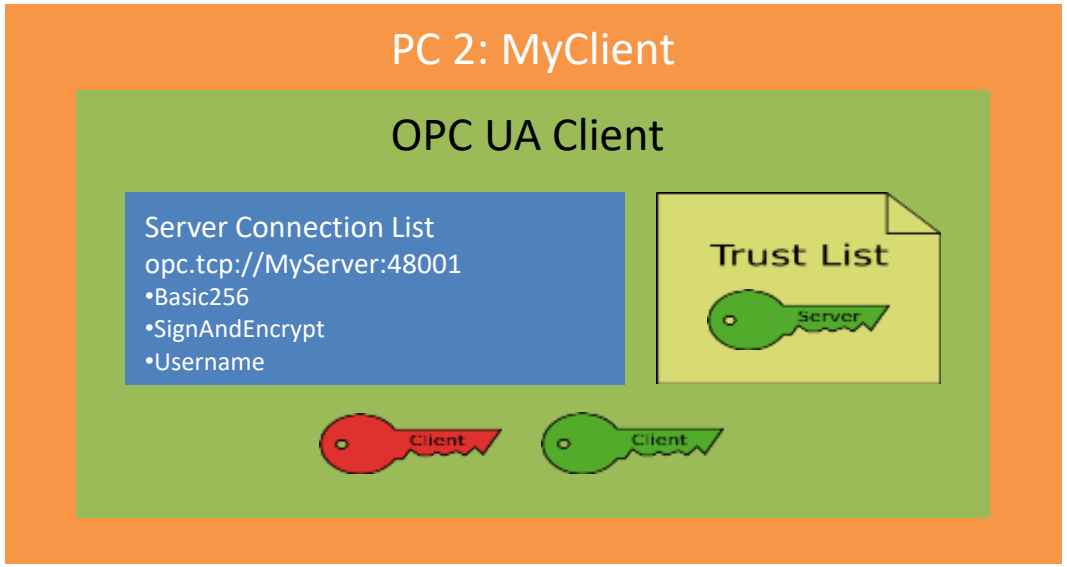
接続の流れ

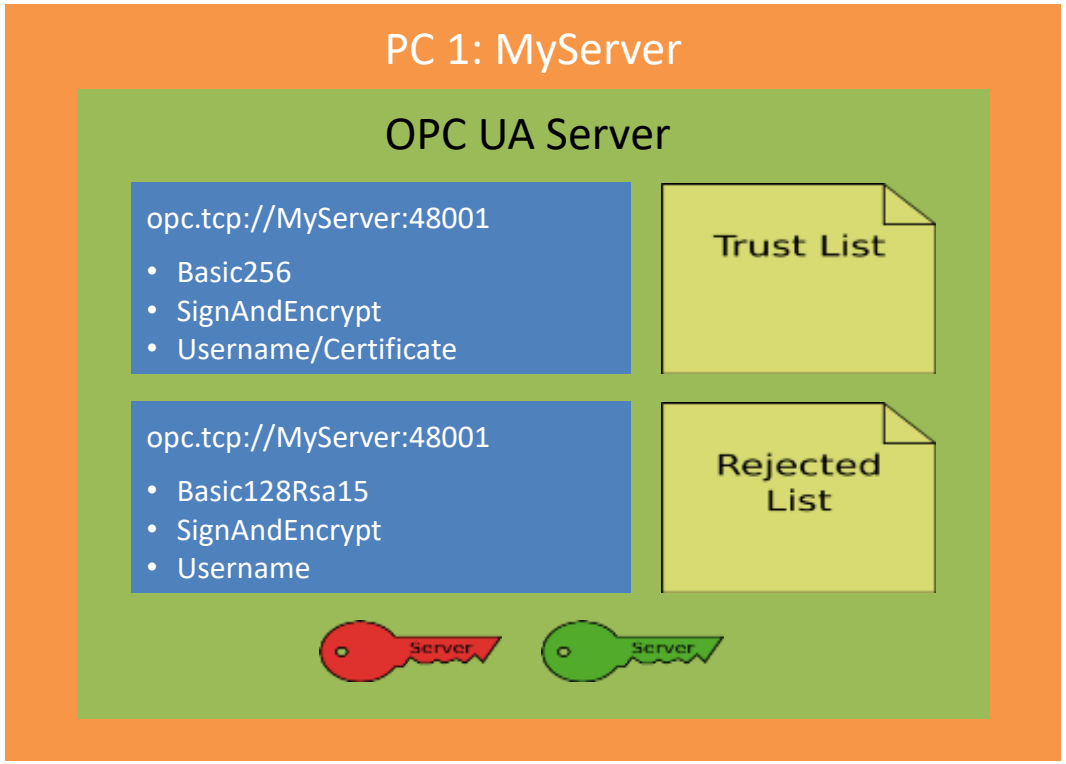


クライアントにおける証明書の許可

Copyright © 2016, OPC Council Japan, All Rights Reserved

接続の流れ

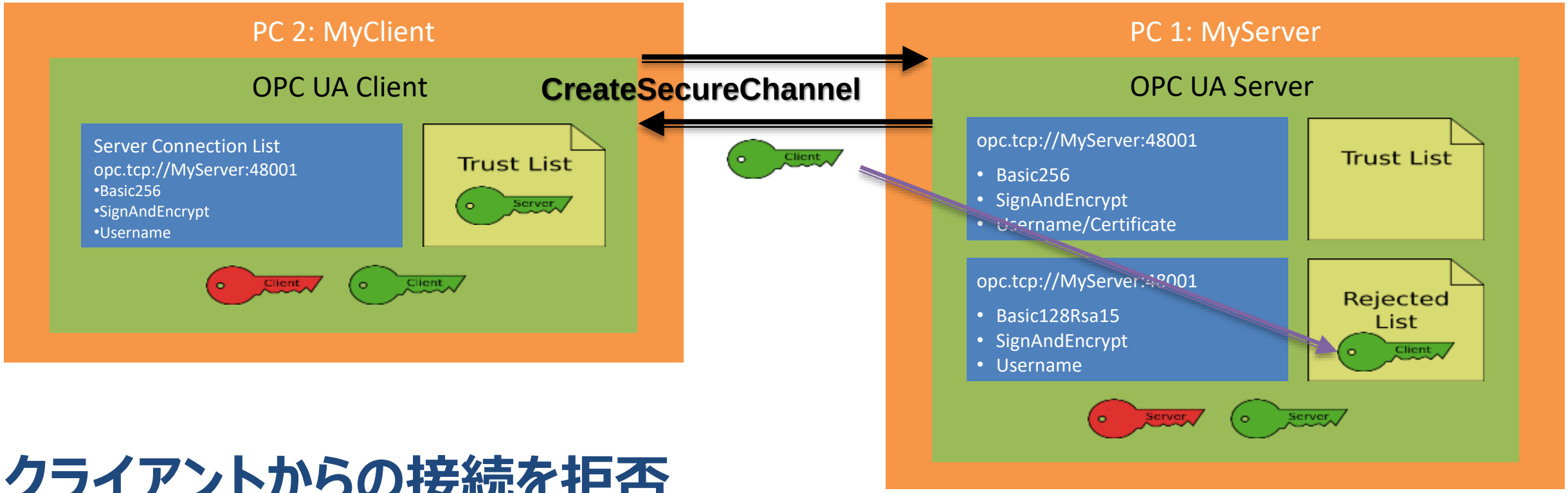




クライアント設定完了

Copyright © 2016, OPC Council Japan, All Rights Reserved

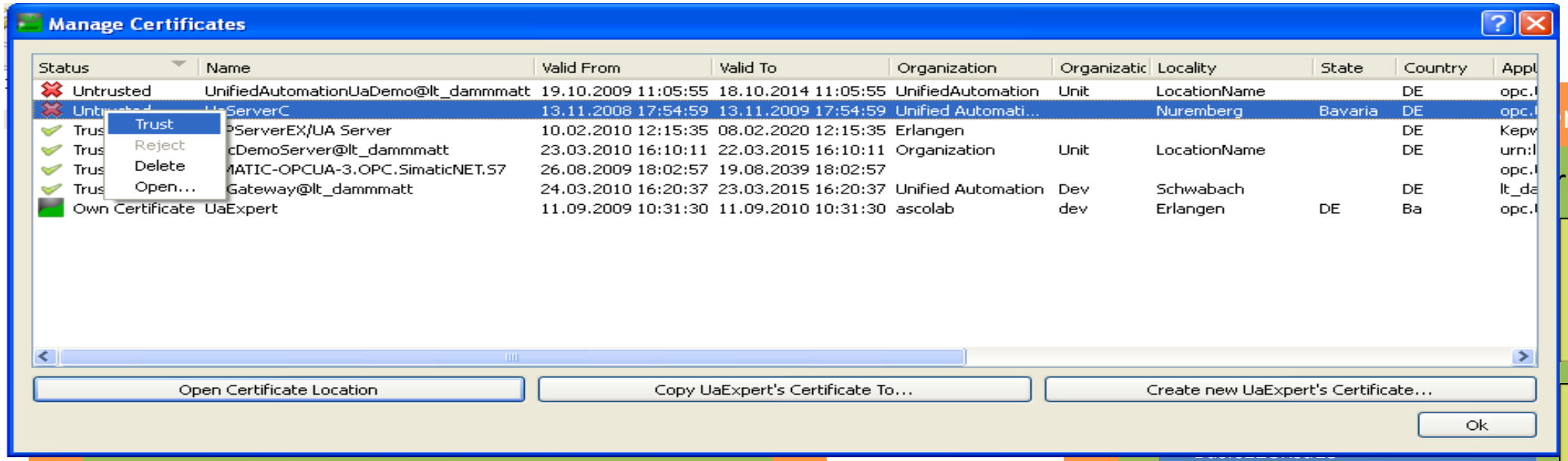
接続の流れ

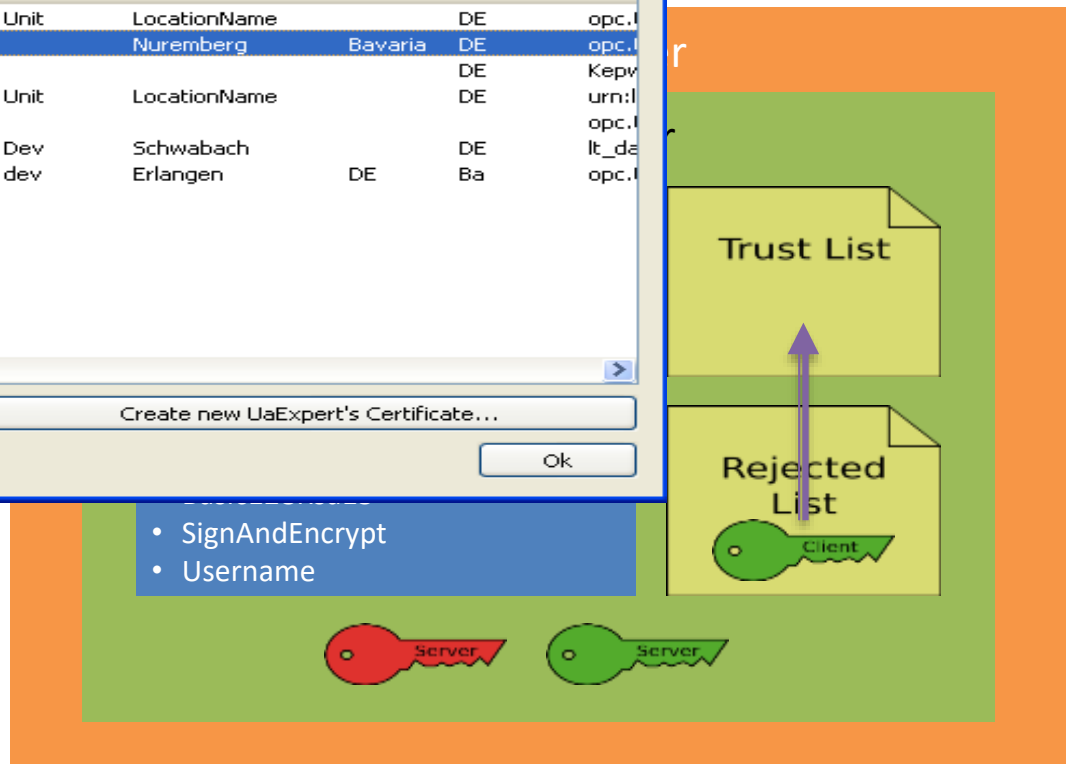


クライアントからの接続を拒否

Copyright © 2016, OPC Council Japan, All Rights Reserved

Connection Configuration



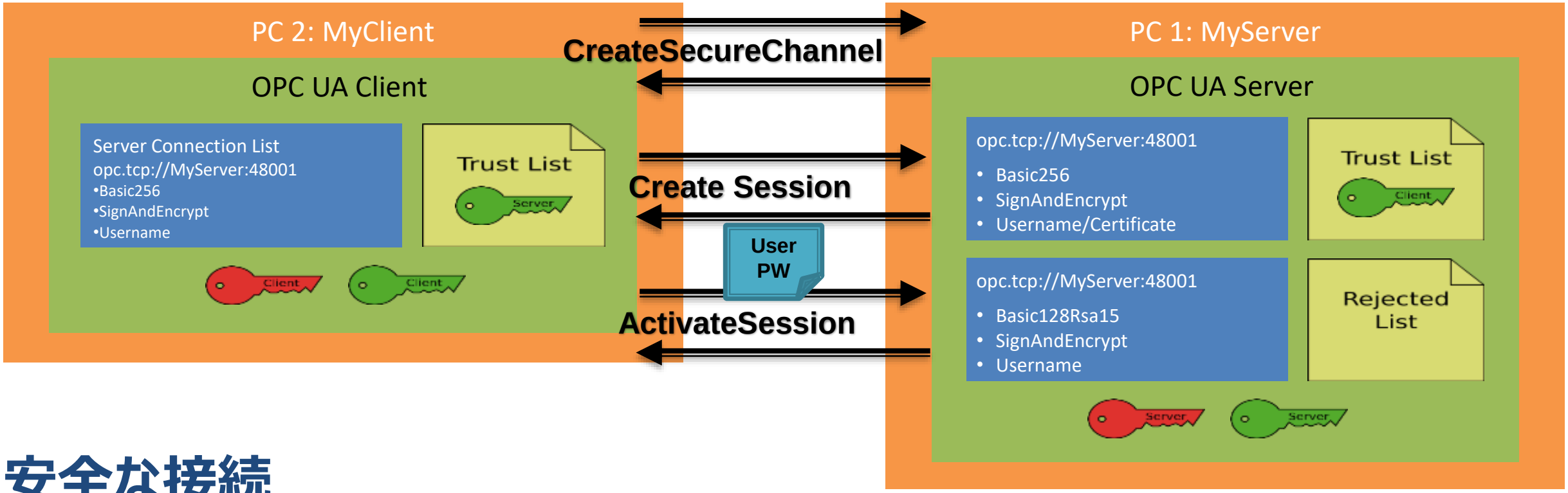


サーバにおける証明書の信頼

Copyright © 2016, OPC Council Japan, All Rights Reserved

OPC FOUNDATION

接続の流れ



安全な接続

Copyright © 2016, OPC Council Japan, All Rights Reserved

日本OPC協議会

URL: https://jp.opcfoundation.org

Copyright © 2016, OPC Council Japan, All Rights Reserved