OPC Day 2017 in Japan

OPC UAセキュリティ機能とドイツ情報技術セキュリティ担当省評価結果の紹介

日本OPC協議会　技術部会

Today

- BSIによるセキュリティ評価
- セキュリティ評価内容
- セキュリティ評価のシステム構成
- 評価結果
- OPC UA セキュリティのおさらい
- OPC UA の対象外

BSIによるセキュリティ評価

評価者: 連邦情報セキュリティ局（ドイツ政府BSI）
評価理由: OPC UAとドイツ産業の関連の為
評価内容: OPC-UAのセキュリティ評価（ 2016年3月制定 仕様の分析）

評価結果: BSI HPとOPC Foundation HPで利用可能

Bundesamt
für Sicherheit in der
Informationstechnik

Commented version available
(English + German)
www.opcfoundation.org/security

OPC FOUNDATION

セキュリティ評価内容

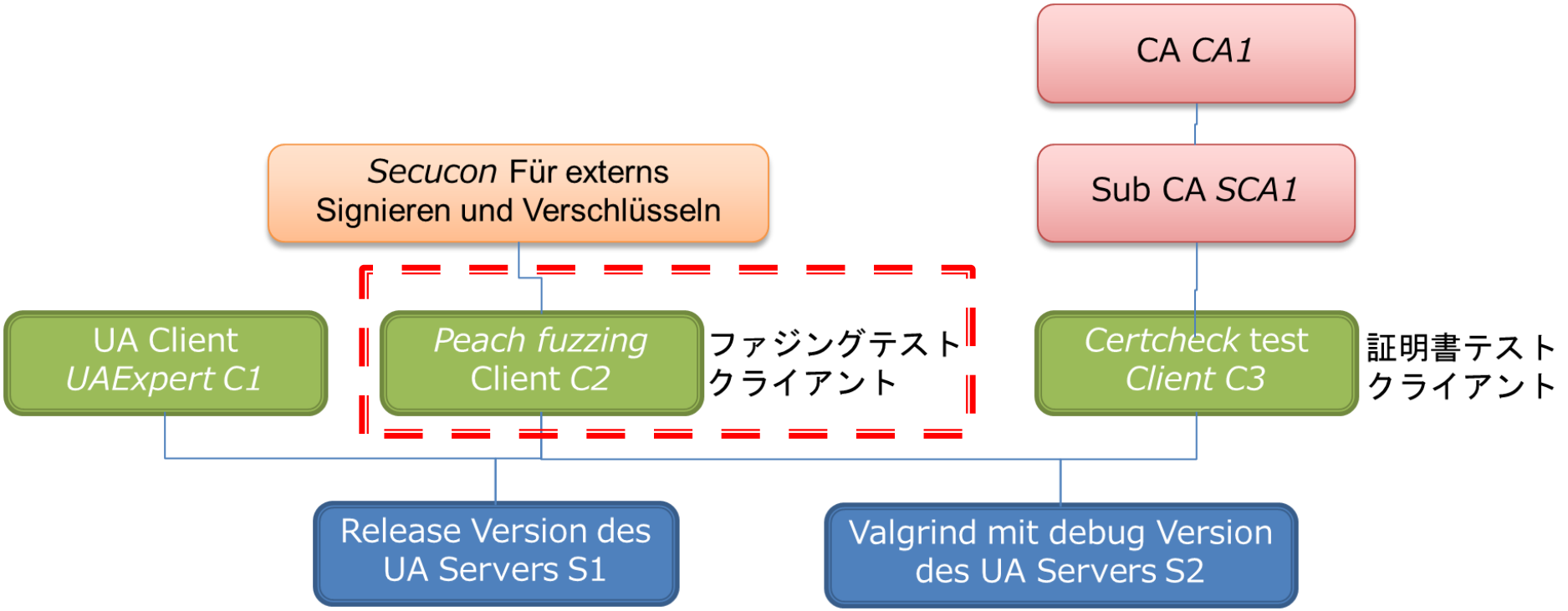
Bundesamt für Sicherheit in der Informationstechnik

- OPC UA仕様
  - 脆弱性を見つける
  - 仕様の異なる部分の間で矛盾を見つける
  - 改善点を見つける
  - 構文エラー、不適切な画像、理解不能または曖昧な仕様を見つける
- OPC UA通信スタックの実装評価
  - 脆弱性を見つける
  - スタックの堅牢性を確認する

【具体的な評価内容】
- ファジングテスト
- 証明書テスト
- 静的コード分析
- 動的コード分析

OPC FOUNDATION

セキュリティ評価のシステム構成



評価結果：ファジングテスト

No.	評価結果	対処	バージョン
1	セキュリティモードがNoneの場合、各パラメータ(SecurityPolicyUriLength, SenderCertificate,ReceiverCertificateThumbprint)の値はNULL(-1)を期待する。	済	1.03.340
2	サーバーは、誤ったシーケンス番号を持つメッセージを受け入れる。	済	1.03.340
3	サーバーは、Helloメッセージで送信されたプロトコルバージョンと違う、OpenSecureChannel要求を受け入れる。	済	1.03.340

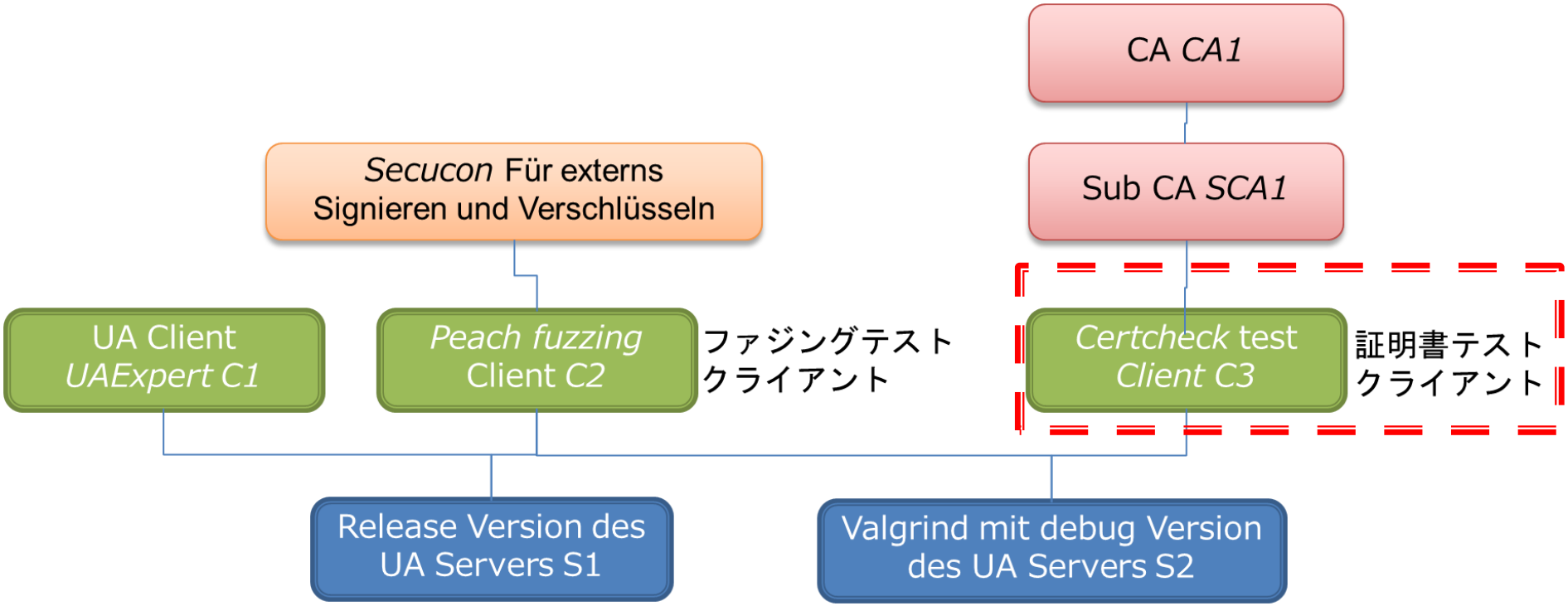
【ファジングテスト】

クラッシュは発生せず、動作は安定！！

実行回数：10万～20万回/テスト

全体の実行回数：1500万回

セキュリティ評価のシステム構成



評価結果：証明書テスト

No.	評価内容	対処	バージョン
1	不適切なStatusCodeを返す	済	1.03.340
2	正常な接続が拒否される	済	1.03.340
3	拒否すべきクライアントからの接続を許可	済	1.03.340

一般的な考え方は次のとおりです。

1）信頼しない証明書は、BadCertificateUntrustedを返す。

2）暗号サービスに問題がある場合、BadSecurityChecksFailedを返す。

3）抑制可能なエラーを検出した場合、適切なエラーコードを返す。

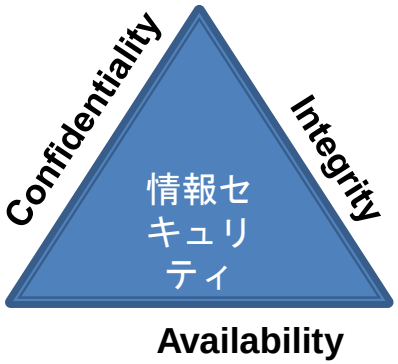
評価結果：静的コード分析

No.	評価結果	対処	バージョン
1	[エラー]Nullポインタ参照		
2	[警告]データのサイズの代わりにポインタのサイズを使用している		
3	[警告]Switch文でVariable名が使用されている		
4	防御的プログラミングの推奨		
5	If文とelse分で同じコードを使用している可能性がある		
6	使用されていない関数削除の推奨	済	1.03.340
7	再入可能な関数の使用を推奨	済	1.03.340

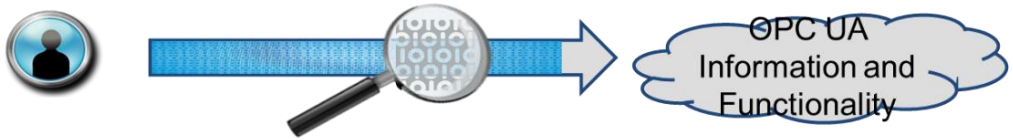
評価結果：動的コード分析 Valgrind

No.	評価結果	対処	バージョン
1	NodeIdデコードによるメモリリーク	済	1.03.340
2	証明書チェーンの解析エラー	済	1.03.340
3	予期しないリクエストボディによって引き起こされるServiceStatusの送信エラー	済	1.03.340
4	スタック変数の初期化が欠落している	済	1.03.340

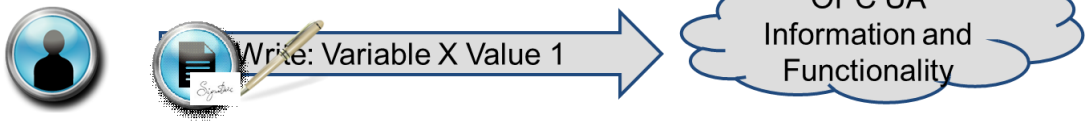
OPC UAセキュリティのおさらい
（トランスポート層のセキュリティ）



- **機密性**
  → メッセージの暗号化



- **完全性**
  → デジタル署名

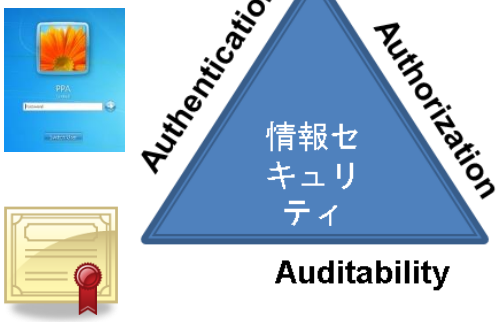


- **可用性**
  - 防御は主にサイトに依存
  - 認証前の処理を最小化

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。

OPC UAセキュリティのおさらい (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



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

OPC UA の対象外

- **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

ご清聴ありがとうございました