ライトニングトーク：

電子署名検証を10分で説明してみる

JNSA 電子署名WG秋祭り
オクトーバーフェスト

宮地（miyachi@langedge.jp）

2016年10月26日

お約束：miyachi とは？

属性：**プログラマ**（ソフトを作っている時が幸せ）

好物：**電子署名**/PKI/**PDF**/OOXML

所属：有限会社ラング・エッジ（一人開発会社w）

肩書：電子署名WG スキルアップTF リーダー
JIPDEC 客員研究員

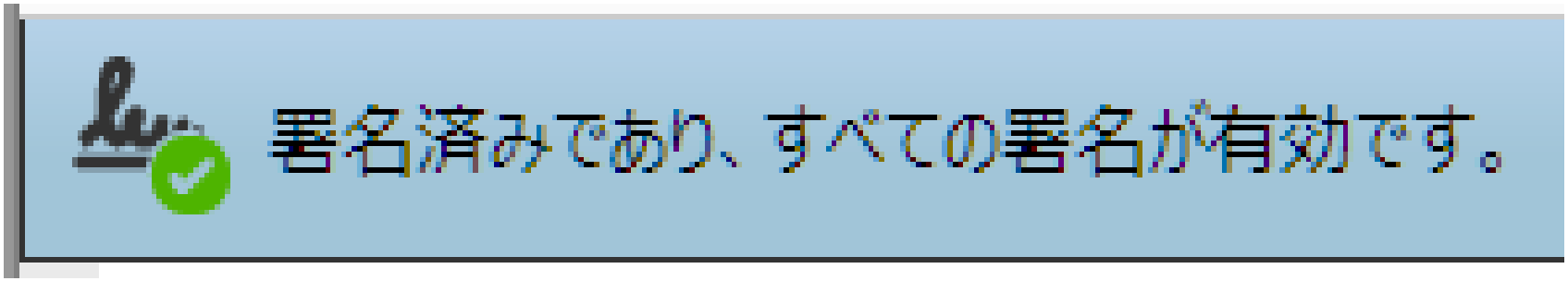
野望：オープンな**開発者コミュニティを署名業界に!**

開発：オープン系＝**FreeTSA**/**FreeXAdES**等
製品系＝LE:XAdES:Lib/LE:PAdES:Lib

電子署名の検証って？

例えば署名済みPDFを開いた時に

表示されるこれ検証だよね？



だって検証結果が正常なんだから
信頼して良いのでしょう？

じゃあ検証では何をチェックしているの？

(°Д°)ポカーン

※ 一般の人の反応「そんなの知らんがな…」

え？え？だって開発会社の人が
ちゃんとプログラミングしているから
検証OKなら**問題無い**のでしょう？

ちゃんとした検証とは？

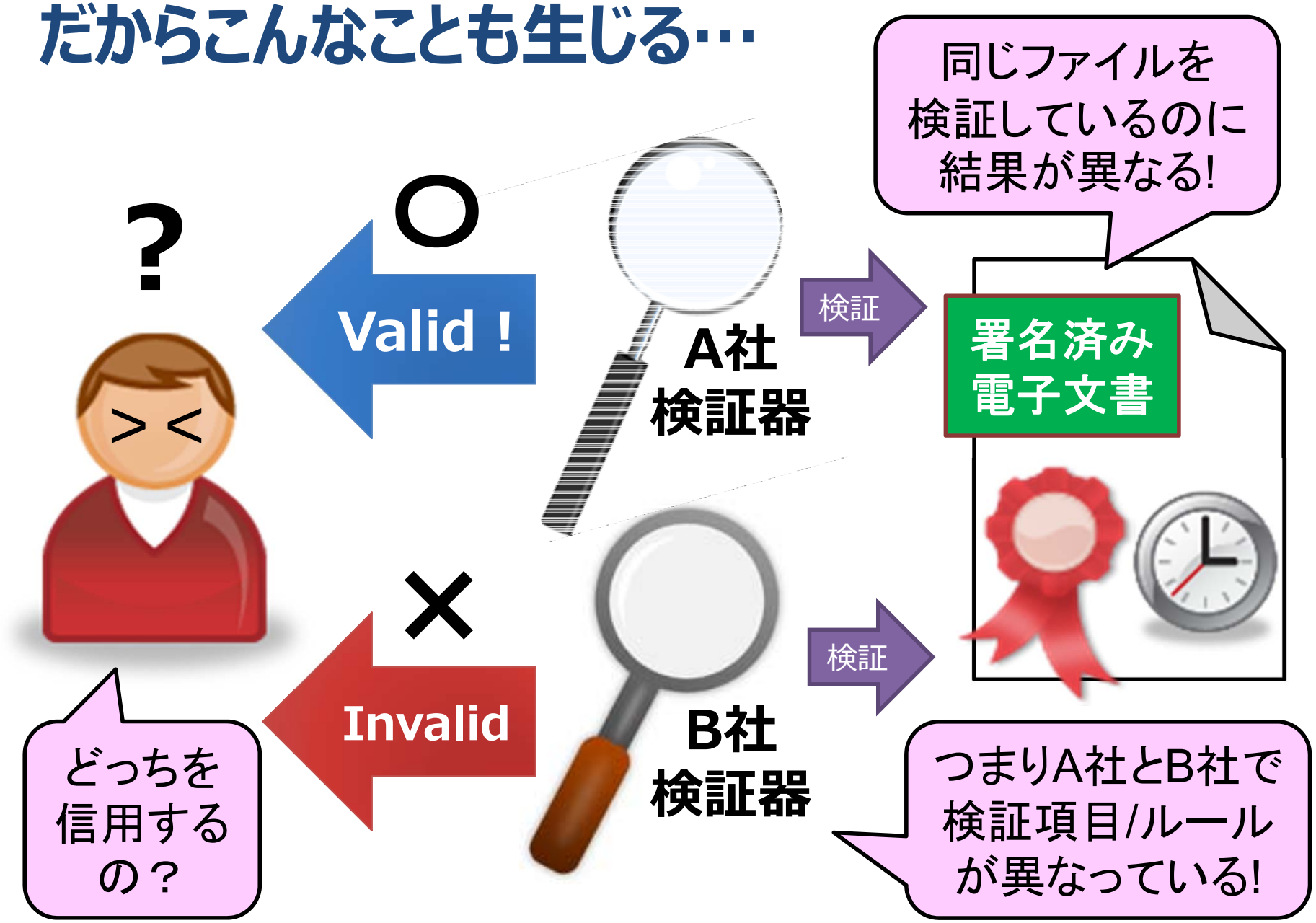
ちゃんとしているってのは、例えば標準化された仕様に従っている？

残念！

署名の生成は色々標準化されているけど、実は検証についてはまだほとんど標準化仕様は無いのです。

※ ETSIでは新たに作っているけど分かりにくいので…

だからこんなことも生じる…



今日は簡単に検証項目を勉強しましょう！

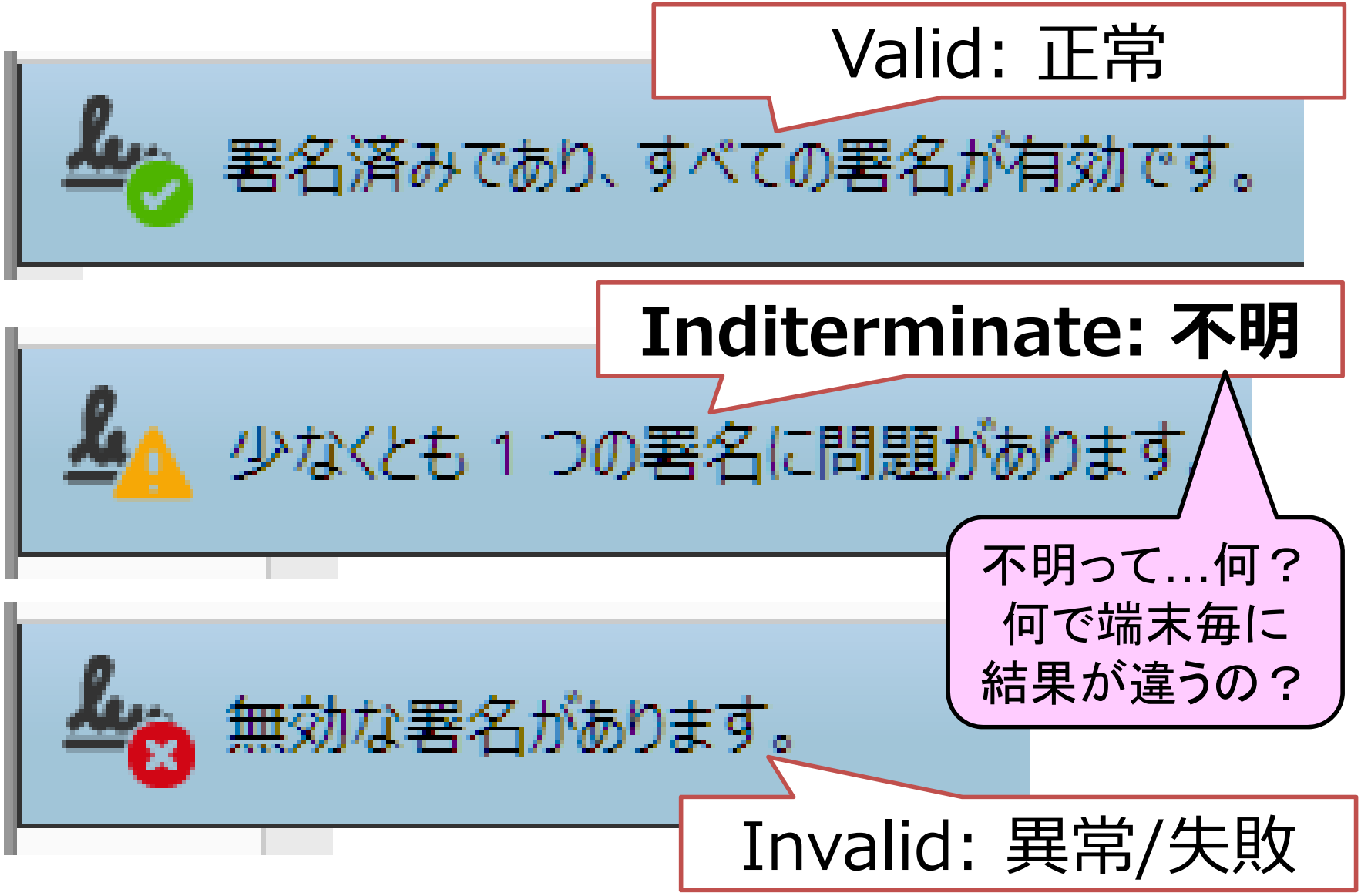
特に技術系なら

知っておいて損は無い!

(･∀･)b イイ!!

勉強しよう！

検証結果ってValid/Invalidと…



検証は大きく分けると2つの項目がある

1）ロジックで検証可能な項目

・公開鍵暗号の署名値（**改ざんの検知**）
・署名フォーマットの正しさ（標準/プロファイル）

※ ロジックなので誰がやっても同じ結果

2）PKIにより検証可能な項目

・署名証明書の認証パスと失効（**署名者確認**）
・ルート証明書の信頼性（何をトラストする？）

※ 問い合わせ等が必要で環境依存あり

外部から与える/取得する必要のあるものは？

現在時刻（通常はPC時刻） 環境依存する場合あり
中間証明書（証明書ストア等）
トラストアンカー（証明書ストア等）
失効情報（無ければネットから取得）
有効暗号リスト（今は無い…）
署名要素制約（プロファイル等）

※検証結果が異なるのはこの辺りが原因!

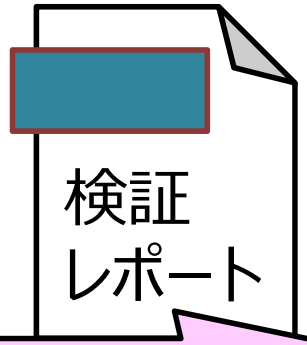
署名検証アプリケーションの例

現在時刻・中間証明書・トラストアンカー・失効情報・
有効暗号リスト・署名要素制約 等
外部から与えるパラメーター要素

これらが不足しているとPKI項目の検証が
できず **Inditerminate（不明）**になる

署名検証
アプリケーション

検証結果：
○ Valid
△ Inditerminate
✕ Invalid



検証項目がベンダー間で
一致していないと結果が
異なってしまう

レポート欲しいよね？

今、我々に必要なもの

1）標準化された検証項目リスト

・パブリックに公開され利用可能なチェックリスト
・1つではなく国毎や分野毎にポリシーとして必要

※ 無ければ作るしかない!

2）チェックリストの適合宣言書

・どの検証項目に対応しているか各ベンダーが公開
・検証結果に標準化された検証レポートの出力

※ これによりベンダー間の差異が明確に!

実はやってました、またやります！

➢2013年頃に一度公開した

「署名検証ガイドライン」JNSAとTBFで協力し作成
http://www.dekyo.or.jp/tbf/seika/pdf/densiguideline.pdf

・英訳化してETSIに持って行ったが採用されなかった…

➢やっぱり必要だと思うんです…

「**標準原案作成TF**」で検討して行きます！
まずはガイドラインで、その先できれば標準化を目指したいと考えています。**リブート！**

※ ご興味があれば是非ご参加ください！

他にもこんなものがあると嬉しい！（特に実装者）

➢相互運用性テスト

各ベンダーが参加して行われるテストで**相互に検証**。
ETSIでは開催しており日本も過去に開催していた。
またできないか**検討中**です。

➢試験用の公開テストデータ

ただこれは難しい･･･
PKIでは時間の概念が重要ですし、期限があるので**常に更新**して行く必要がある。
相互運用性試験時に更新できると良い？

まとめ その１：

署名検証には**ロジック**と**パラメータ**が必要。
署名検証標準化には**検証項目リスト**が必要。

まとめ その２：

検証項目リストが無いなら**作るしかない**！
無いものを作ることこそオープン系の醍醐味だ！
それに勉強になること間違いなし！

興味があればご連絡ください m(_ _)m

Thank you！