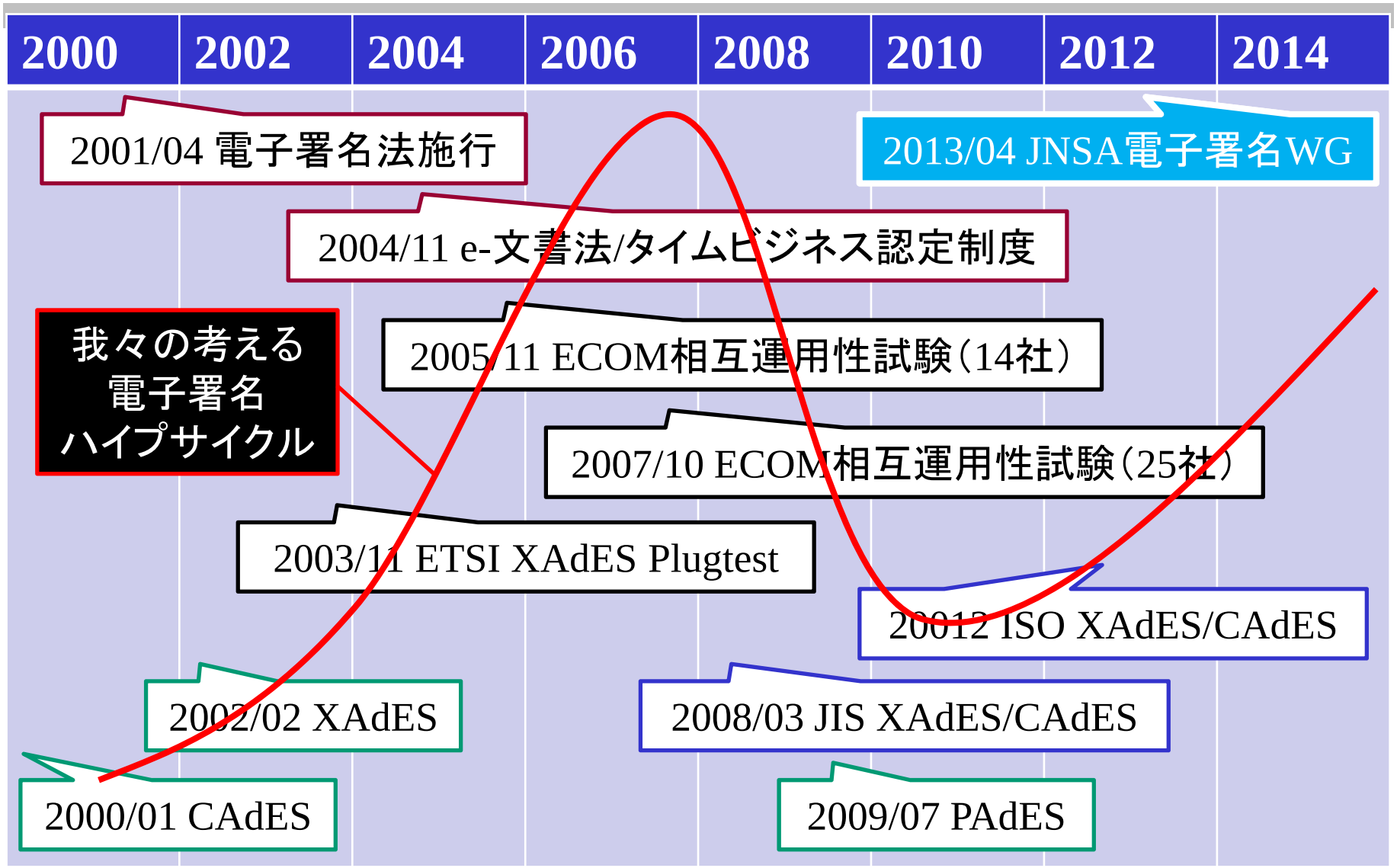
Network Security Forum 2015
電子署名ハンズオンと
PKI SandBox Project

宮地 (miyachi@langedge.jp)
電子署名WGサブリーダー/スキルアップTFリーダー
（有限会社ラング・エッジ）

2015 年 1 月 20 日

電子署名マーケットの歴史



電子署名法（電子署名及び認証業務に関する法律）

- 電子署名法は2001年4月に施行
  1. 電磁的記録の真正な成立の推定（第3条）
  2. 特定認証業務に関する認定制度（第4から16条）

- 「電子情報の信頼性」を確保する法的な裏付け

  本人による電子署名が付与された電子文書は、
  訴訟時の証拠として、紙と同等な証拠能力がある。

- 特定認証業務の認定電子認証局

  → GPKIと相互認証され電子申請等で利用可能

※ 経済産業省の管轄

タイムビジネス認定制度

- タイムビジネス認定制度は2004年11月に策定
- 「タイムビジネスに関わる指針」（総務省）
  - 「タイムスタンプビジネス」のガイドライン
    第三者が証明可能な時刻情報を付与する。
  - 日本データ通信協会による任意の認定制度
    → 技術面ではNICTやTBF（タイムビジネス協議会）と連携
  - 認定タイムスタンプ局は多くの法律の要件
    → e-文書法にも認定タイムスタンプ局の利用が明記

※ 総務省の管轄

e-文書法

- e-文書法は2005年4月に施行（内閣官房）
- 適用されるのは各府省が定める約250省令

  ※「e-文書法によって電磁的記録が可能となった規定」

  http://www.kantei.go.jp/jp/singi/it2/others/syourei.pdf
- 適用には要件（省令毎）を満たす必要がある

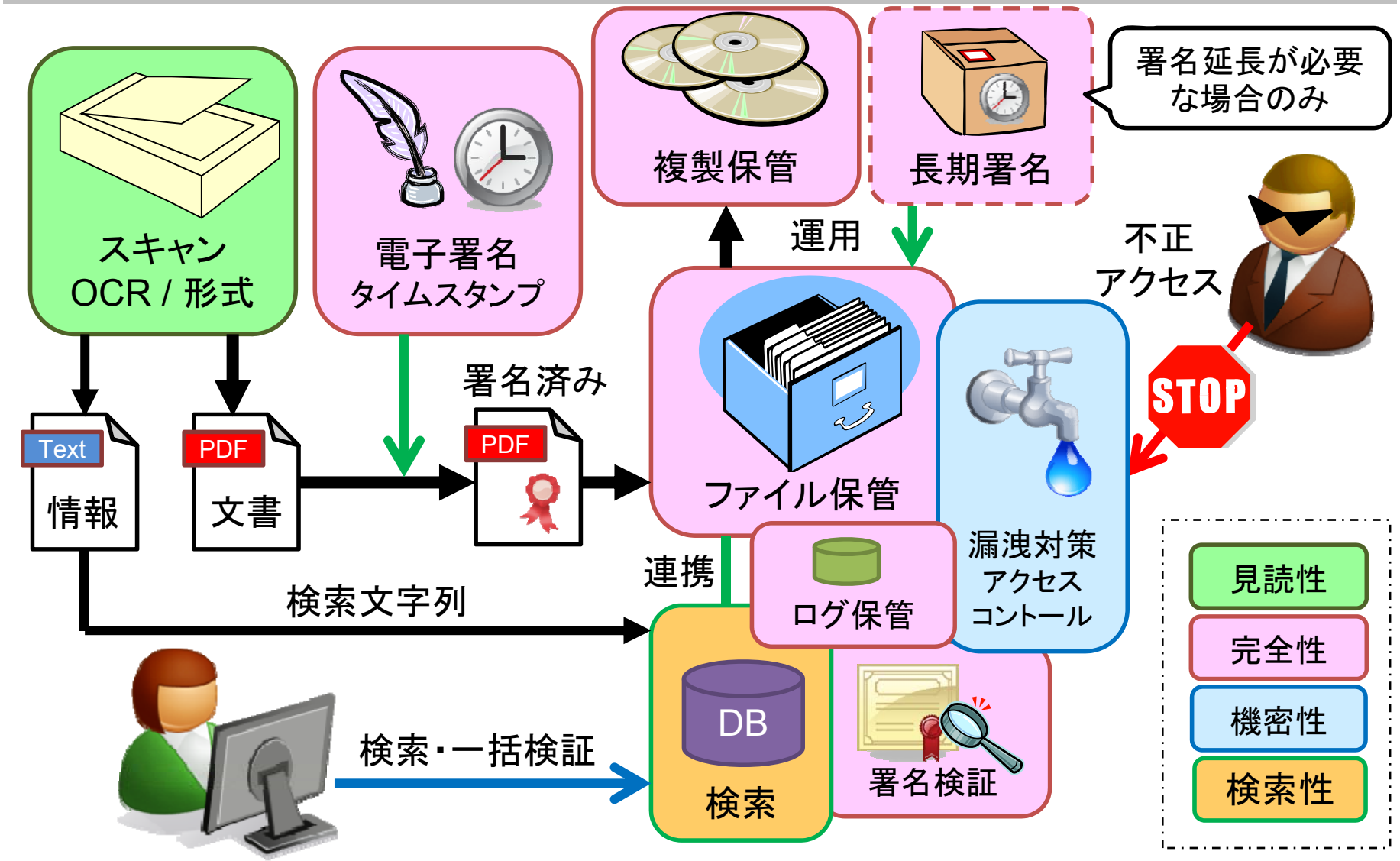
  見読性：スキャン等入力時やフォーマットの問題
  完全性：**電子署名・タイムスタンプ**や保管の問題
  機密性：漏洩対策・アクセス制御等の運用の問題
  検索性：入力時キーワードセットや検索DBの問題

  システム設計時に配慮必要

  ※「文書の電子化・活用ガイド」

  http://www.meti.go.jp/policy/it_policy/e-doc/guide/e-bunshoguide.pdf

e-文書法要件対応システム例



電子契約

契約は口頭でも成立するが成立の証拠として利用する

1. スピードアップ：オンライン化で瞬時に
2. 省コスト：印紙税不要や郵送コスト削減
3. セキュリティ：改ざん防止・本人性確認

メリット

電子認証局会議が無料で配布している「電子署名活用ガイド」を読めば実務者とシステム担当向けの情報が理解可能。

電子署名の入門書としてもお奨め！
是非ダウンロードを！

http://www.c-a-c.jp/download/

現在の電子署名マーケット

何でも長期署名を付与…の時代では無くなりつつある？
用途や目的に応じて使い分ける時代に。

- タイムスタンプのみ（知財保護や電子帳簿保存法）
- 長期署名で電子契約等（本人性が必要な利用）
- デジタルエビデンス保存（米国型の起訴対策等）

クラウド署名やモバイルとの連携も注目されてきた。
顧客サイドからの「電子署名」を使いたいとの要望増。

でも電子署名ってどう使うの？

電子署名普及の課題

JNSA

- 相互運用性確保
  - 規格の標準化（とても重要！）
    特に長期署名の場合は異なるベンダー間で
    署名と検証が出来ることが必須。
  - プラグテスト（相互運用性試験）実施
    他社との互換性と自社実装の確認

セコム佐藤さん
から説明済み！

- 電子署名利用ノウハウ
  - 普及啓蒙活動
    セミナー等での発表活動
  - 勉強会やハンズオン
    現場の営業・SE・技術者向けにノウハウを提供

スキルアップTF
中心に活動中！

スキルアップTF 2014年度の活動

- 勉強会・ハンズオン（主に会員向け）
  - これまで主に会員向け勉強会を開催してきた
  - 外部（一般）向けの初めての試み！
    「電子署名ハンズオン」を３月開催予定
- 電子署名WGサーバ構築（PKI SandBox Project）
  - 実際に電子署名を体験して貰う為の公開サーバ
  - 成果はPKI SandBox Projecttとして公開して行く
  - 電子署名関連企業からの協力申し込みも順調

スキルアップTF 2014年度勉強会

６月２６日：欧州クラウド署名Comfact社

９月２９日：IT製品の調達におけるセキュリティ要件
リストに関する認定制度の勉強会
（JIPDECあんしんかんカフェ共催）

９月３０日：SMS認証製品プレゼン ガプスモバイル社
OpenSSL/LibreSSL勉強会

１０月２日：ドイツ署名ビジネス状況の紹介 OpenLimit社
（JIPDECあんしんかんカフェ・TBF共催）

１１月５日：電子署名ハンズオン試行（前編）

１２月９日：電子署名ハンズオン試行（後編）

１２月１８日：USENIX LISA14 報告会（PKI相互運用WGとの共催）

１月１５日：Open Office XML勉強会

電子署名ハンズオンの目的

目的:

一般のプログラマ・エンジニア向けに電子署名の基本を分かりやすく説明して実際に使って貰う。電子署名利用の普及啓蒙活動として利用者の拡大を目指す。

ターゲット:

A) クラウドやサーバを構築するSIer系の技術者

B) 電子署名を理解したい企業内（PKI）技術者

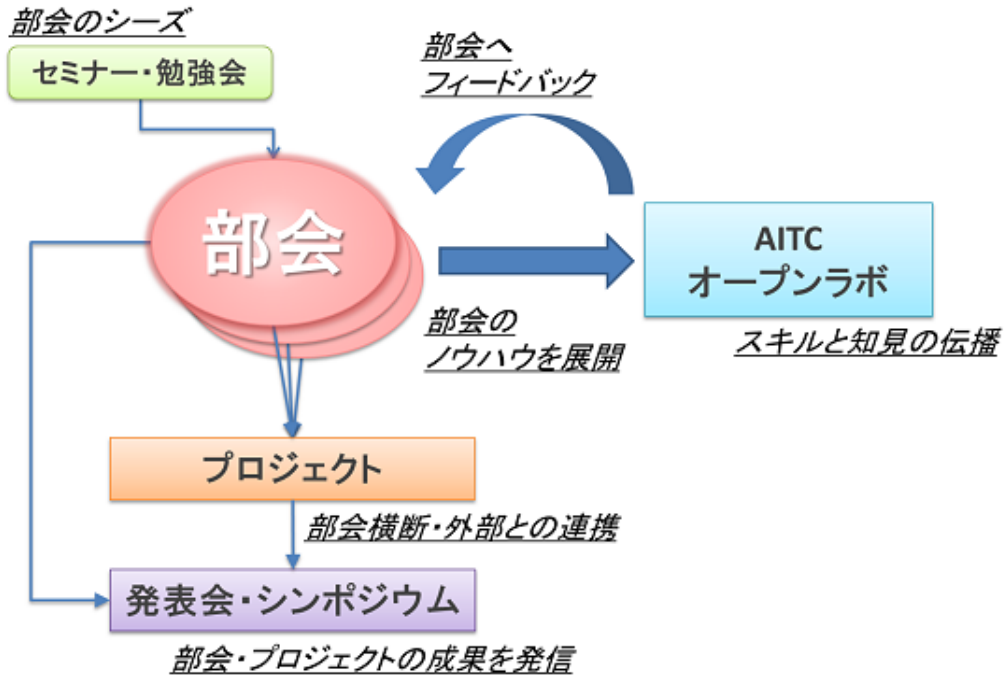
共催:

特にA)のターゲットであるクラウド系の活動をしているAITCのオープンラボとして共催し一般利用者を集客。

先端IT活用推進コンソーシアム

英名：AITC（Advanced IT Consortium to Evaluate, Apply and Drive）
由来：XMLコンソーシアムの後継団体
共催：クラウド・テクノロジー活用部会
サイト：　http://aitc.jp/

「先端IT活用推進コンソーシアム」は、企業における先端ITの活用および先端ITエキスパート技術者の育成を目指す団体です。



電子署名ハンズオン開催概要

名称：電子署名ハンズオン
(JNSA勉強会/AITCオープンラボ)
日時：2015年3月14日(土) 13:30～18:30
費用：無料（事前登録制の予定）
参加：どなたでも参加可能、PC(Win or Mac)が必要
人数：30名を想定
会場：インタセクト・コミュニケーション様 セミナールーム
住所：千代田区神田錦町3丁目14-12 神田錦町ミハマビル8階
主催：JNSA電子署名WG スキルアップTF
AITCクラウド・テクノロジー活用部会

電子署名ハンズオンのメニュー

- 第1部：電子署名とタイムスタンプ
  1. 電子署名とその基本技術を理解する
  2. ハンズオン1：電子署名を生成してみよう
  3. タイムスタンプ技術を理解する
  4. ハンズオン2：タイムスタンプを取得してみよう
- 第2部：署名検証と長期署名
  5. 電子署名の検証技術を理解する
  6. ハンズオン3：検証してみよう
  7. 長期署名を理解する
  8. ハンズオン4：長期署名を作ってみよう

Adobe Readerで長期署名
PAdES-Aファイルを作る

電子署名ハンズオンのレベル

- 技術者（プログラマ等）
  - ある程度具体的な情報の入手が可能です。
  - Javaでタイムスタンプ取得するノウハウもあり。
- 仕様策定者（SE等）
  - 具体的な内容はやや難しいかもしれません。
  - 電子署名・タイムスタンプの必要要件の情報あり。
- 非技術者（営業等）
  - 技術説明部はついて来れないかもしれません。
  - ただしハンズオン部はコマンド実行だけなので雰囲気は理解できると思います。

電子署名ハンズオン

開催は3月14日（土）午後です!

是非ご参加ください!!

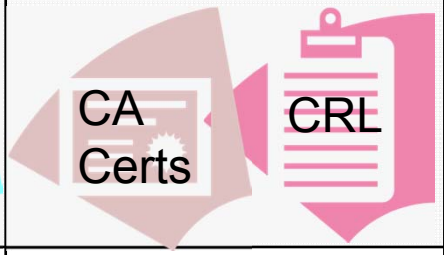
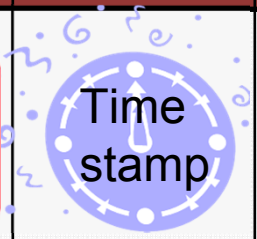
PKI SandBox Project

目的：誰でも遊べるPKI試験環境（砂場）を用意する

http://eswg.jnsa.org/sandbox/

※ 電子署名ハンズオンでも利用予定

SandBox 必要機能の一覧

CA機能			TSA機能	情報公開	署名機能	検証機能
						
証明書・鍵 サービス	リポジトリ公開 HTTP / LDAP		OCSP 発行	タイムスタンプ 発行	ソース他 公開	簡易 サービス	簡易 サービス
対話画面による発行	CA証明書は公開 CRLは定期的に更新 出来ればCSP/CP等も		証明書DB またはCRL 連動し発行	CA機能で TSA証明書 を準備	各機能実装 情報やサンプルを公開	APIを用意してクラウド的な利用方法のサンプルに	
OpenSSL のCA機能 認証連携	OpenSSLの 簡易CA機能を利用 画面は作成が必要		OpenSSL で可能？ ocspオプション利用	 準備完了 FreeTSA	Wiki, Blog GitHub 等	Ruby on Rails 等か CA機能と連携？ FreeXAdES, jsrsasign 等の利用	
証明書・秘密鍵は登録制等にして完全フリーは難しいかも。一応本人確認くらいはする？ OCSPは最初は無くても良いかもしれない。			認定TSAからの提供も 計画中	長期署名サンプル等 ノウハウも	クラウド署名の実証実験的にできるとベスト HSM等使えると面白い		
JNSAではかつて「チャレンジPKI http://www.jnsa.org/mpki/index_j.html 」があったが、今は使えない。 ベンダー様より提供頂けるサービスやソフトウェアは積極利用する。							

PKI SandBox Project の今後

- 電子署名ハンズオンの資料や内容を公開
  - 電子署名の技術的な資料蓄積場所にする
- 試験用の認証局の機能を追加
  - あくまで試験用であり実用では無い
- 協賛ベンダーのソフトウェアの組み込み
  - タイムスタンプサービスや認証局サービス
  - 電子署名ソフトの利用
- オープンソースのライブラリ開発
  - XML長期署名XAdESライブラリ(Java)開発

Enjoy Electronic Signature !

ご清聴ありがとうございました。

JNSA

電子署名WGへの参加者募集中です！

https://www.facebook.com/eswg.jnsa.org