JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

WG成果報告会
電子署名検討WG

NTTコムウェア
磐城　洋介

2004年　5月18日

第1.1版

はじめに

本WGは、電子署名の普及を促進するため、普及阻害の要因分析と、電子署名活用モデルの提案を目標に設立された。

昨年度の主な活動は、「阻害要因の分析」として、各界の有識者を交えた意見交換会の開催と、マスコミ業界関係者（雑誌記者）に対する意識調査（アンケート）、公的個人認証サービスに関する意見・情報の交換を行い、電子署名を取りまく環境の再確認を行った。

なお、活用モデルの提案は次年度以降検討とすることとなった。

活動概要

メンバー： １８名

会合： プレミーティング２回、本会９回。

オブザーバ招致＆意見交換会
　鈴木優一氏（エントラストジャパン／ＪＮＳＡ理事）
　牧野二郎氏（弁護士）
　大泉純二郎（仮名）氏（日経ＢＰ記者）

報告内容目次

1. 電子署名について
    1. 電子認証と電子署名
    2. 電子署名とは？
    3. 電子署名と印鑑
    4. 印鑑のセキュリティ
    5. 暗号について
    6. 実装形態
2. 電子署名をとりまく課題
    1. 利用者の認識
    2. 方式など技術的な課題
    3. 電子政府の実情
3. 電子署名実装アプリケーション事例 「SecureStarXML」
    1. 方式･構成
    2. 特徴
    3. 開発苦労小話

電子署名について

電子署名とは？

電子認証とは違う。
印鑑に例えられる。
電子署名法がある。
ＰＫＩより名前が知られている。
でも、利用アプリが少ない。

電子認証と電子署名 (1)

前提：「認証」と言う日本語は、英訳すると二つの意味がある
Authenticationの認証：システムなどにアクセスする際に行うパスワード投入などの本人確認のこと。例：ベーシック認証、バイオメトリクス認証
Certificationの認証：ユーザ登録などを行う際にパスワードなどを最初にその人本人であることを何らかの方法（対面とか）で確認（認証）してIDなどを渡すこと。例：認証局（CA）
これらを踏まえて「電子認証」とは、SSL端末認証などを例としたＰＫＩベースのAuthenticationのこととして、下記をしるす。

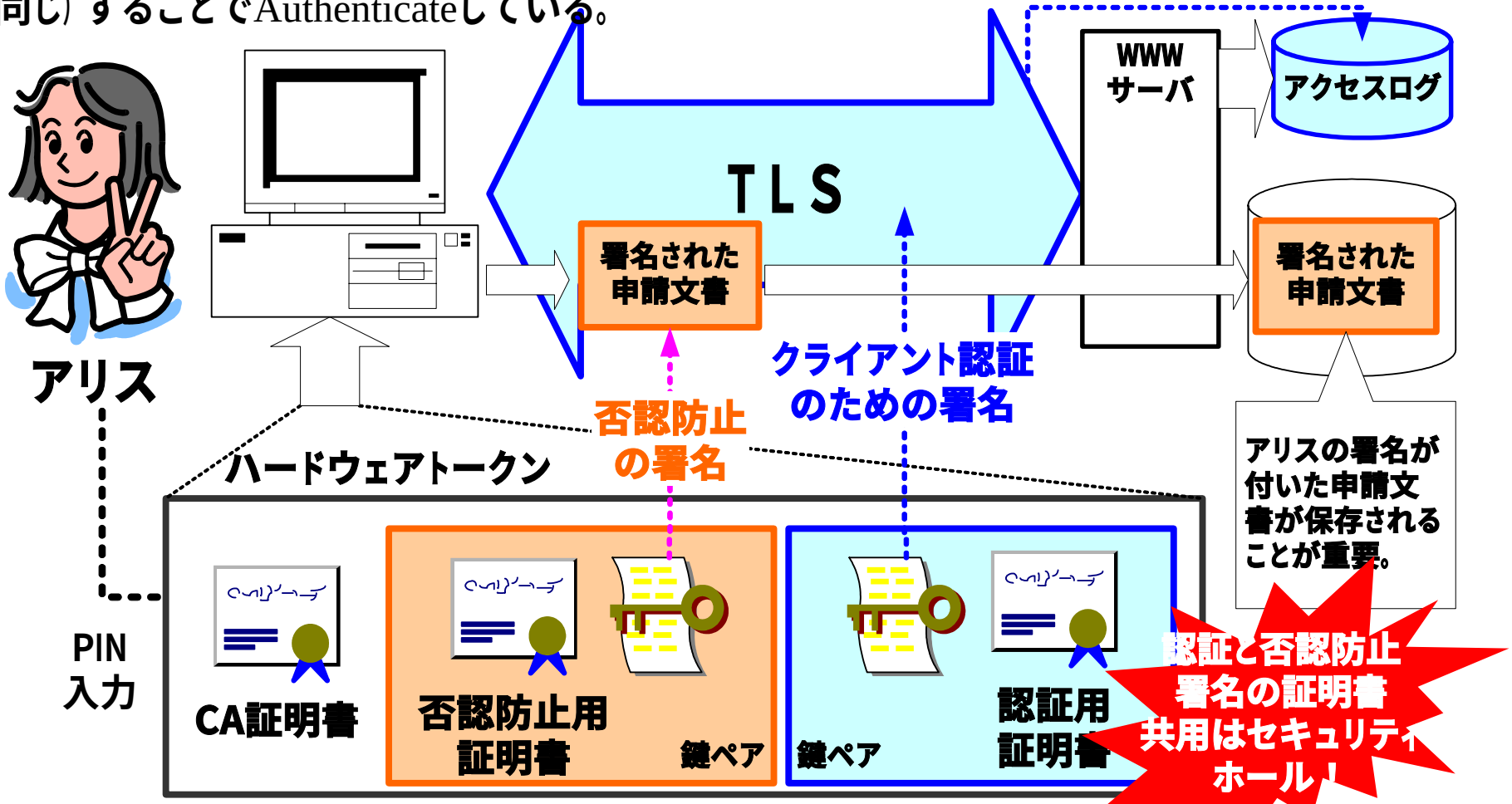
電子認証と電子署名の似てる部分と違う部分

似ている部分
・秘密鍵で暗号化する（次項）　　・電子証明書（ＰＫＩ）が必要

違う部分
・署名は暗号化したもの（電子署名）が、長く残る（残すために署名する）。
・認証は単に秘密鍵を安全に持っていさえすれば良いが、署名は対象の電子文書に記載された内容を利用者が合意したことを確認してから、秘密鍵を用いることになる。

電子認証と電子署名 (2)

クライアント認証は、サーバで任意に生成されたダイジェストを秘密鍵で暗号化 (署名と同じ) することでAuthenticateしている。



電子署名とは

電子署名は、それを実現する電子証明書の運用が、日本における「実印」「銀行印」の制度に似ている点が多いことから、よく印鑑に例えられている。

	紙の世界（アナログ世界）		電子的世界（ディジタル世界）
本人確認の道具	印鑑		秘密鍵
上記道具の作成方法	手作業による彫刻（唯一の印影）		ユニークな秘密鍵・公開鍵ペアの生成
登録機関	地方自治体	銀行	ＣＡ（認証局）
使用者登録の証明	印鑑登録証明	通帳への押印	Ｘ．５０９証明書
署名(者)の確認	(登録印影との)印影照合		署名検証
法制面での根拠	民事訴訟法第228条第4項 「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立したものと推定する。」		電子署名法第3条 「当該電磁的記録に記録された情報について本人による電子署名が行なわれているときは、真正に成立したものと推定する。」

電子署名と印鑑

学会の有識者や政府の公式文書において「印鑑」に例えられている。

- **実印にあたるのが、秘密のかぎなのでございます**

  暗号の権威「辻井先生」が平成12年5月23日第147回国会、交通・情報通信委員会で述べられた。

  http://kokkai.ndl.go.jp/SENTAKU/sangiin/147/0012/14705230012019c.html

  「(前略) これに対しまして電子の世界ではどうやるかと申しますと、実印に当たるのが公開かぎ暗号、特にその公開かぎ暗号のその中に入っておりますまた秘密のかぎなのでございますが、これをまずつくりまして、それをCA、認証機関、いろんな呼び方がありますが…(後略)」

- **電子証明書と印鑑登録証明書との類似点・相違点**

  平成14年2月28日総務省の報道資料「地方公共団体による公的個人認証サービス制度の創設について」における「参考5」に記載。

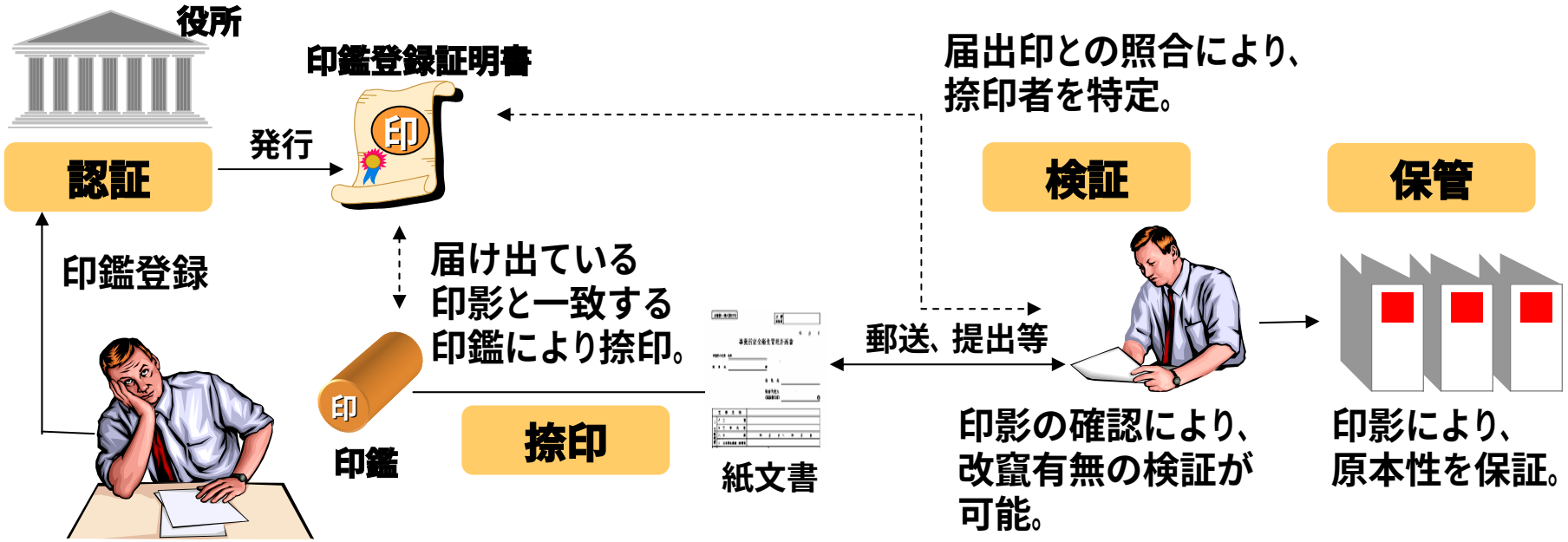
  http://www.soumu.go.jp/s-news/2002/020228_3.html

  「デジタル署名のPKIは、日本の印鑑登録制度と非常によく似ているが、両者は、まったく別の制度である。印鑑登録は、慣習に基礎を置く制度で、日本では非常に重い役割を果たしており、不動産取引をはじめ、非常に重要な取引において利用されるが、(後略)」

電子署名は、印鑑が必要な文書のデジタル化に必須の要素！

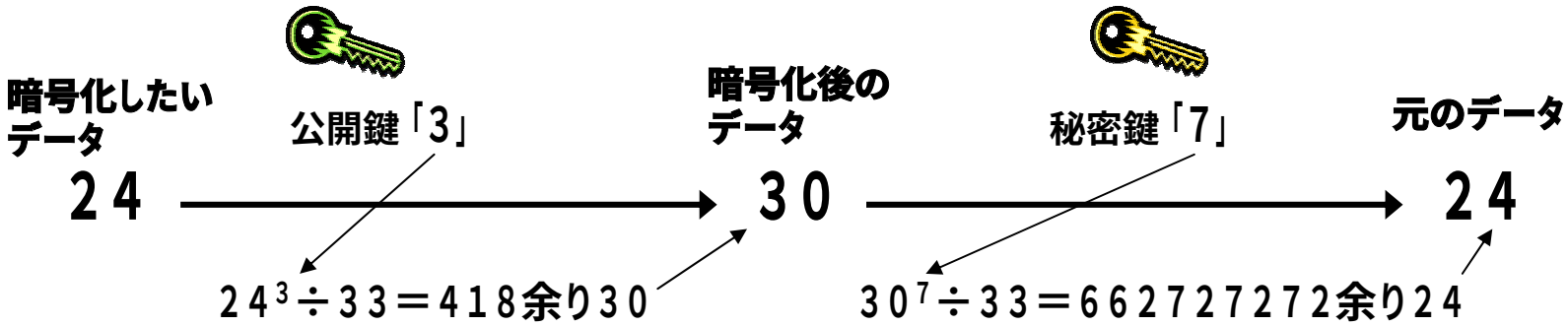
印鑑のセキュリティ

印鑑は、「印影は印鑑によってのみ生成可能である」と言う前提が、セキュリティのよりどころであり、その印鑑を所持する者の手により捺印された文書が印鑑所持者の作成や内容の合意を表すものとされてきた。ただし、昨今のIT技術革新により簡単に陰影の偽造が可能になり、問題視されている。



暗号について

電子署名は公開鍵暗号技術で、その安全性が実現されている。
公開鍵暗号（ＲＳＡ）の原理を簡単に言うと、元のデータに対して鍵となり得る「素数」で割った「余り」に変換してしまう方式である。
ここでは「ある値」に「3」「１１」を選び（この二つの数値がいわゆる「公開鍵」として証明書に含まれる）、３×１１＝３３をモジュロ（法）に計算し、図のような結果を得る。



実際には、「3」、「１１」や「7」などは非常に大きな素数を選ぶので、これらの数値がペアになっていることの推測（計算）が極めて困難である点が公開鍵暗号の安全性につながるのである。

実装形態

電子署名機能を実装した汎用ＡＰと、電子署名機能をシステムに実装する際の開発ツール（ミドルウェアなど）などがある。
なお、左記は現存する製品の一例である。

分類	製品名	開発元
S/MIME署名	Netscape Messenger	Netscape Communications
	Outlook Express	Microsoft
	Winbiff + S/GOMA	オレンジソフト
	WeMail	NEC通信システム
PDF署名（※）	Acrobat	Adobe
	SignedPDF	三菱電機
	DigitalPost	ソリトンシステムズ
ツールキット 開発ライブラリ	SecureStarXML	大日本印刷
	certMISTY	三菱電機
	SecureWare/電子署名	日本電気
	TruePass	Entrust
	BSAFE	RSA Security
その他	DocuWorks	富士ゼロックス
	WebSign	サートラスト

【注意】表中の商品名は、各社の登録商標です。
※： 署名対象の電子ファイルにPDFを用いているもので署名形式などは製品個々に異なります。

電子署名をとりまく課題

利用者の認識や
そもそも技術的な課題
電子政府の実情

利用者の認識（1）

JNSA

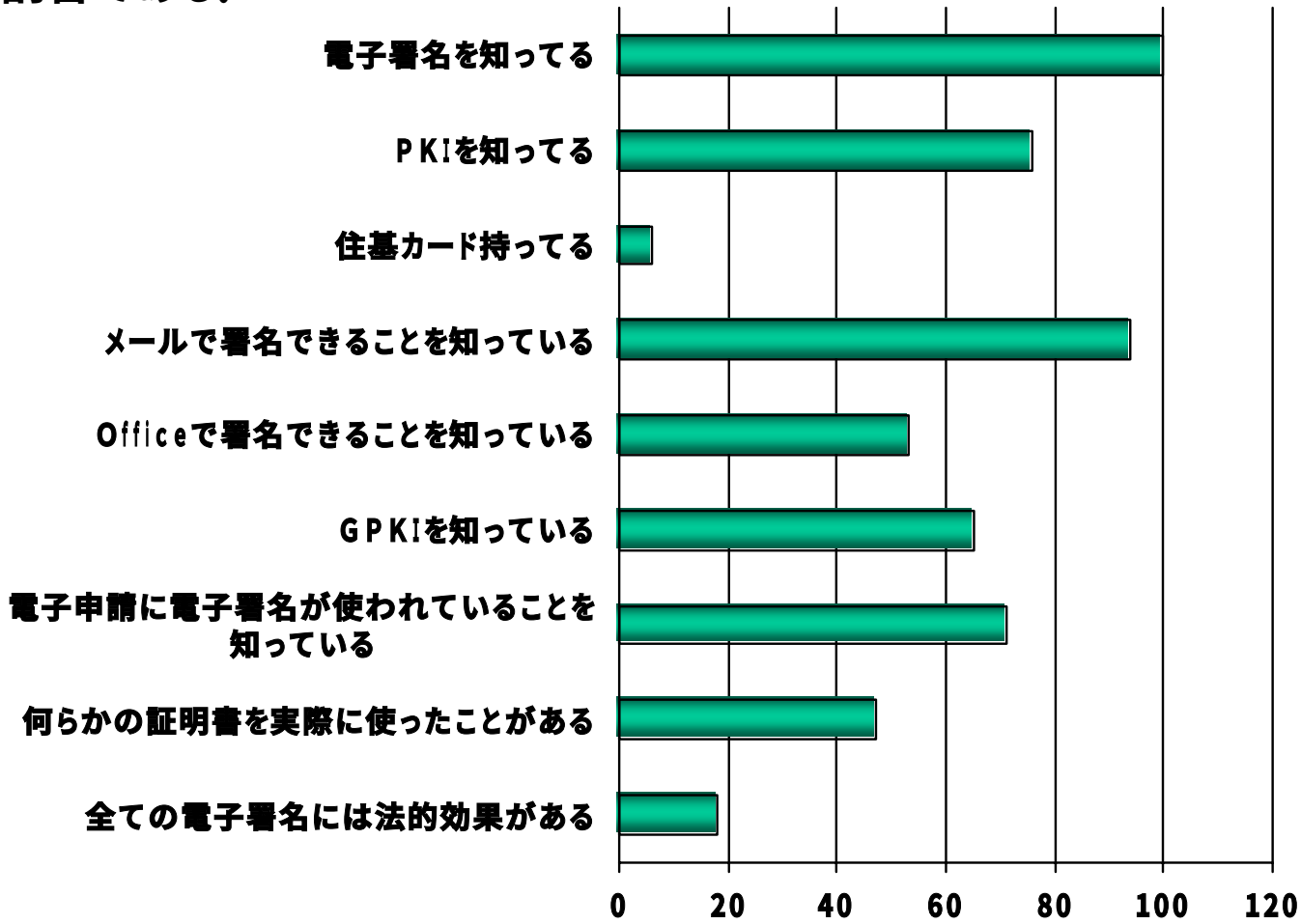
とある雑誌の記事において、「電子証明書」や「電子署名」について、「コピーできない」「改ざんできない」などの誤記があった。これを機会に、IT関連の情報発信をする立場の雑誌記者が、どの程度正しく電子署名について把握しているか調査してみた。

方法は、アンケートWebサイトを用いた25問からなる質問で、うち6問は、電子署名に関する理解度をチェックできる設問を設定した。

有効回答数は「17件」と少なかったが、日経BP社の記者を対象としており、ITや特にセキュリティに興味・関心のある記者と言う点では少ない数値とは言えない。

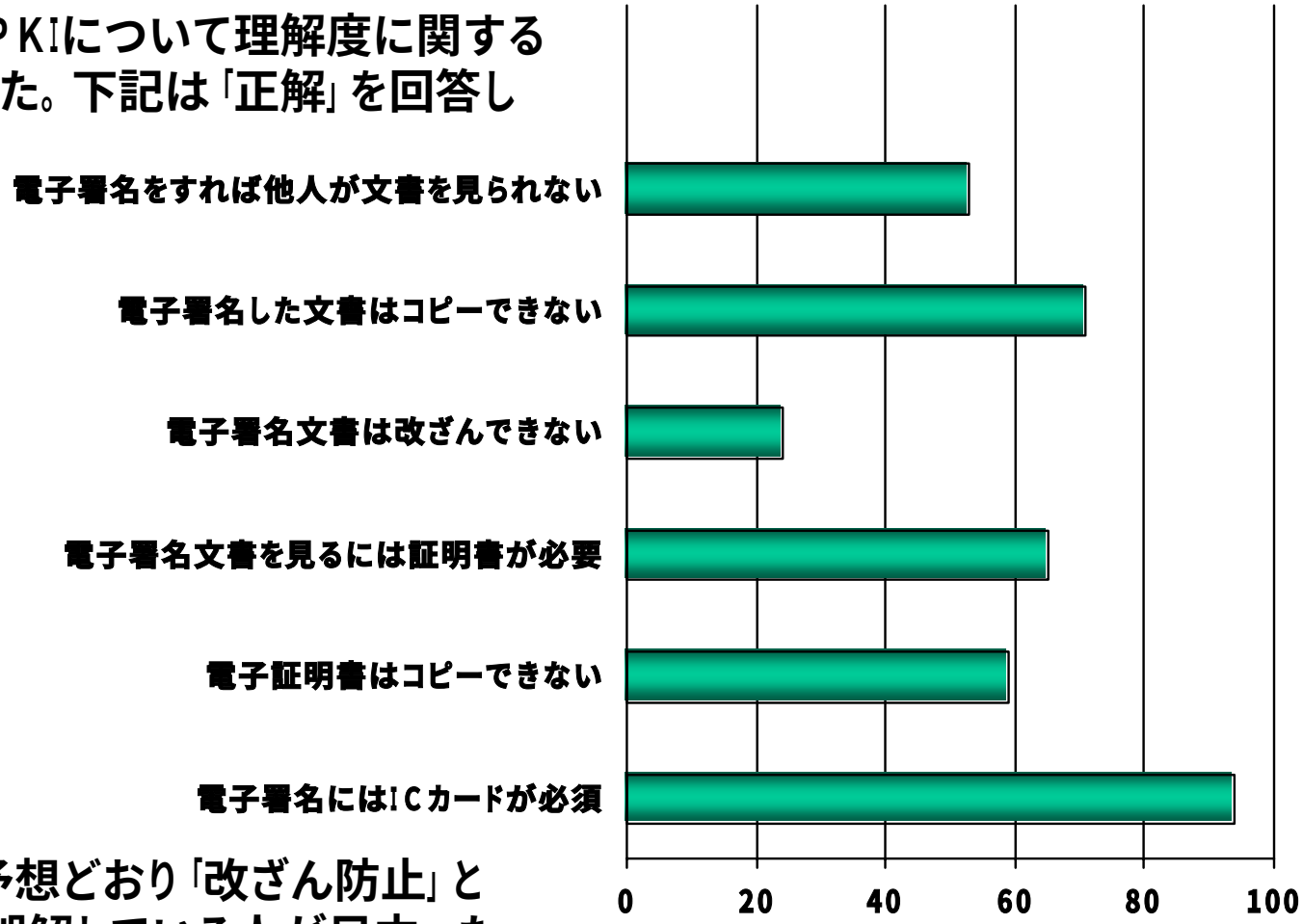
利用者の認識（2）

まず、電子署名やＰＫＩについて認知に関する質問を行った。下記は「Ｙｅｓ」と回答した人の割合である。



利用者の認識（3）

次に、電子署名やＰＫＩについて理解度に関する簡単なテストを行った。下記は「正解」を回答した人の割合である。



やはり、当初の予想どおり「改ざん防止」と「改ざん検知」を誤解している人が目立った。
最後の問題正解率の高さから、ＩＣカードへの認知や関心が高いことが推測される。

利用者の認識・まとめ

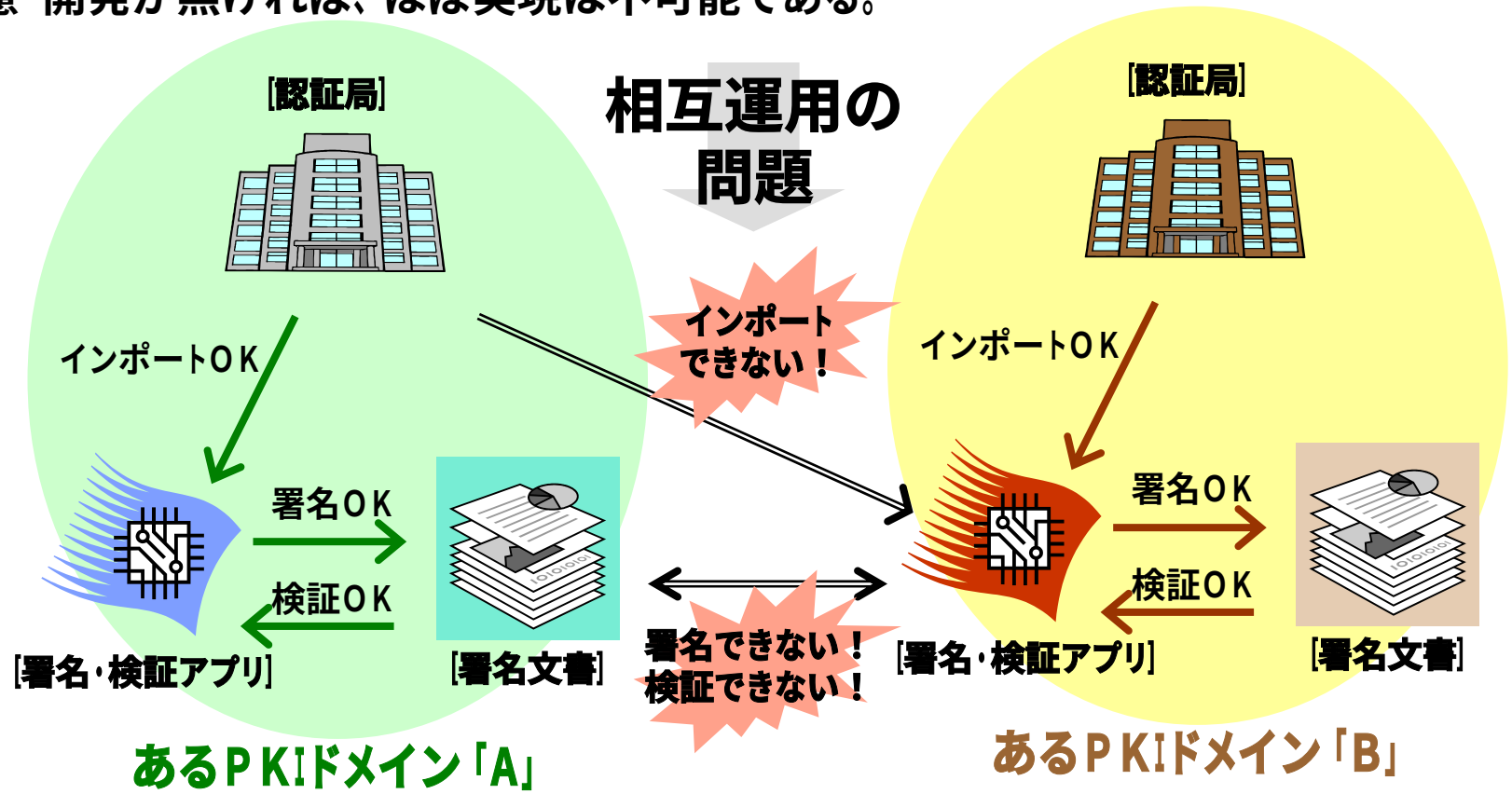
前項の設問回答者は、良く分かっている人と、そうでない人の得点差が顕著であった。

このことは、前項で述べた「印鑑」を例えに、電子署名の導入事前アセスメントが不十分だと、実際に端末を用いて署名を行う際の確認ポップアップなどの画面仕様や、署名対象の範囲、多重署名(※)の範囲などにおいて、システム開発の途中でもユーザからの仕様変更要望が炸裂することになると考えられる。

※： 一つの署名対象(データ)に複数の署名を付加するもの。並列多重(署名同士依存しないもの)と、直列多重(前の署名を含み署名するもの)がある。

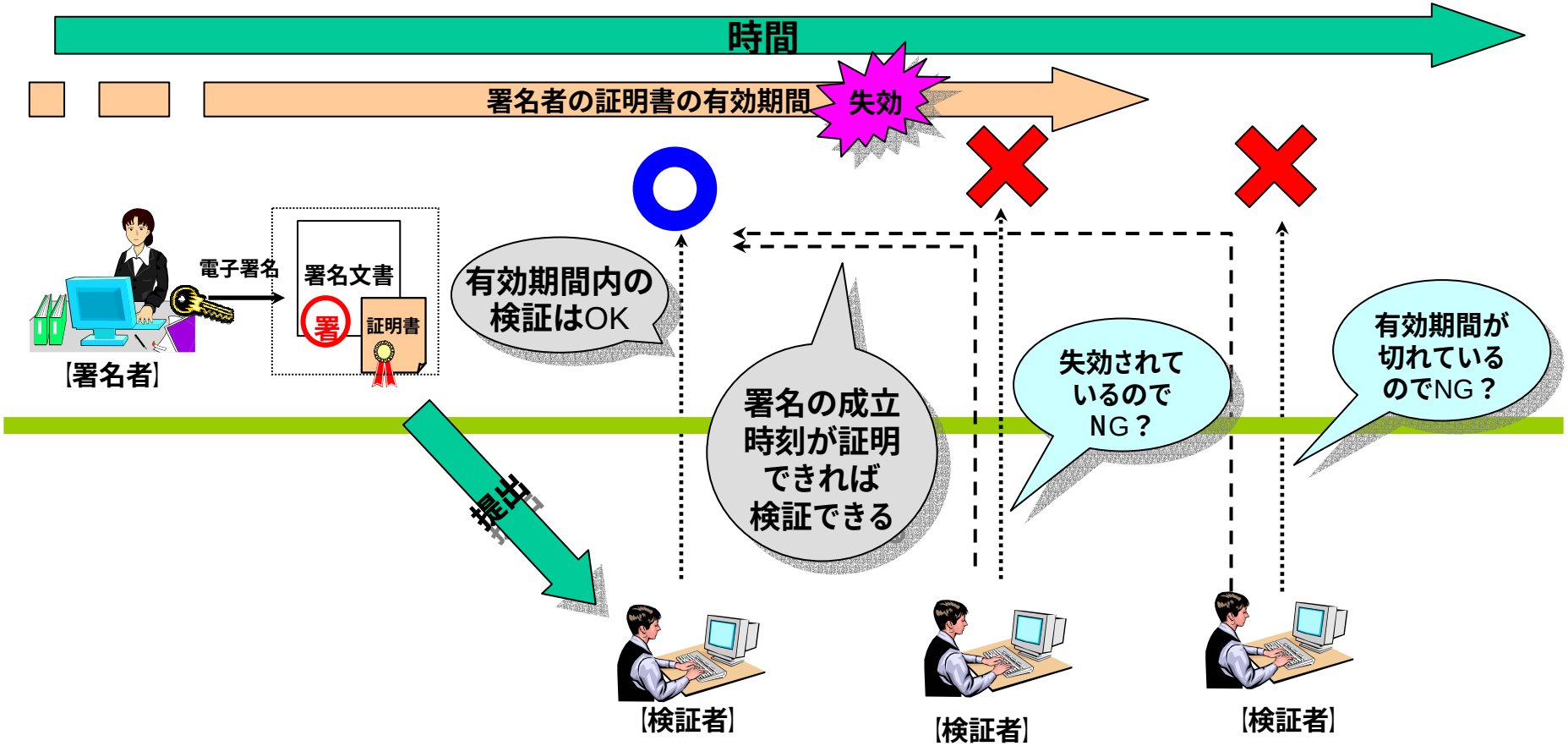
方式など技術的な課題（1）
「認証基盤や相互運用について」

相互運用とは、簡単に言うと「どんな認証局の証明書でも」「どんなアプリケーションでも」「どんなドキュメント（コンテンツ）にも」相互に署名や検証を行うことができることを言う。現状では、ほとんどの電子署名利用のシステム間において、相互運用向けの考慮・開発が無ければ、ほぼ実現は不可能である。



方式など技術的な課題（2）
「文書保管の有効期限について」

デジタル署名は、そのままでは証明書の有効期限切れにともない、署名検証も無効になってしまう。署名時刻を正確に証明できるインフラ（タイムスタンプ等）が必要。



方式など技術的な課題（3）
「その他」

JNSA

1．サーバや端末の時刻について
「ある程度厳密に同期が取れていなければならない」

証明書の有効性チェック機能は、端末や署名処理を行うサーバ上で実行されるが、その際動く「有効期間チェック機能」は、各々のコンピュータ時刻を元に処理される。古いパソコンでボードの電池切れなどを起こすと再起動の度に１９７０年1月１日などになってしまい、不要なトラブルの元になりかねない。端末も含むシステム全体の時刻同期について配慮が必要。

2．署名対象データのサイズについて
「現在の技術では、数百ＭＢ程度が上限」

市販のツールキットなどを利用してシステム構築する場合、署名データのサイズについて配慮が必要。なお現在では分割ハッシュなどについてのＰＫＩ関連標準が制定されていないため、必要に応じた独自規格の実装と言う形になり、電子文書の可用性を損なうことになる。

電子政府の実情(1)

1. **政府認証基盤**
   - **仕様(証明書のフォーマット、検証方式)の異なる複数の認証基盤**
   - **これら認証基盤を相互にまたがった業務の存在**

2. **情報公開**
   - **情報により公開の方法が異なる**(誰でもいつでも見られると言う状況ではない)
   - **開示の時期がまちまち**(十分な開発期間が取れないため、見切りで開発を開始し途中仕様変更が生じる)

3. **詳細仕様の策定**
   - **署名規格の規定がない**(詳しくは後述)。
   - **利用者環境**(PC)**などに関する明確なガイドラインがない**
   - **行政アプリ**(**電子申請**APなど)**との連携仕様が明確でない**

電子政府の実情 (2)

4. **公的個人認証基盤**
   - **住基カードのハンドリング方法に明確なガイドラインがない**
   - **証明書の拡張領域に個人情報が載っている (または、この事実を知らない人が多い)**

電子署名アプリケーション事例

JNSA

「SecureStarXML」

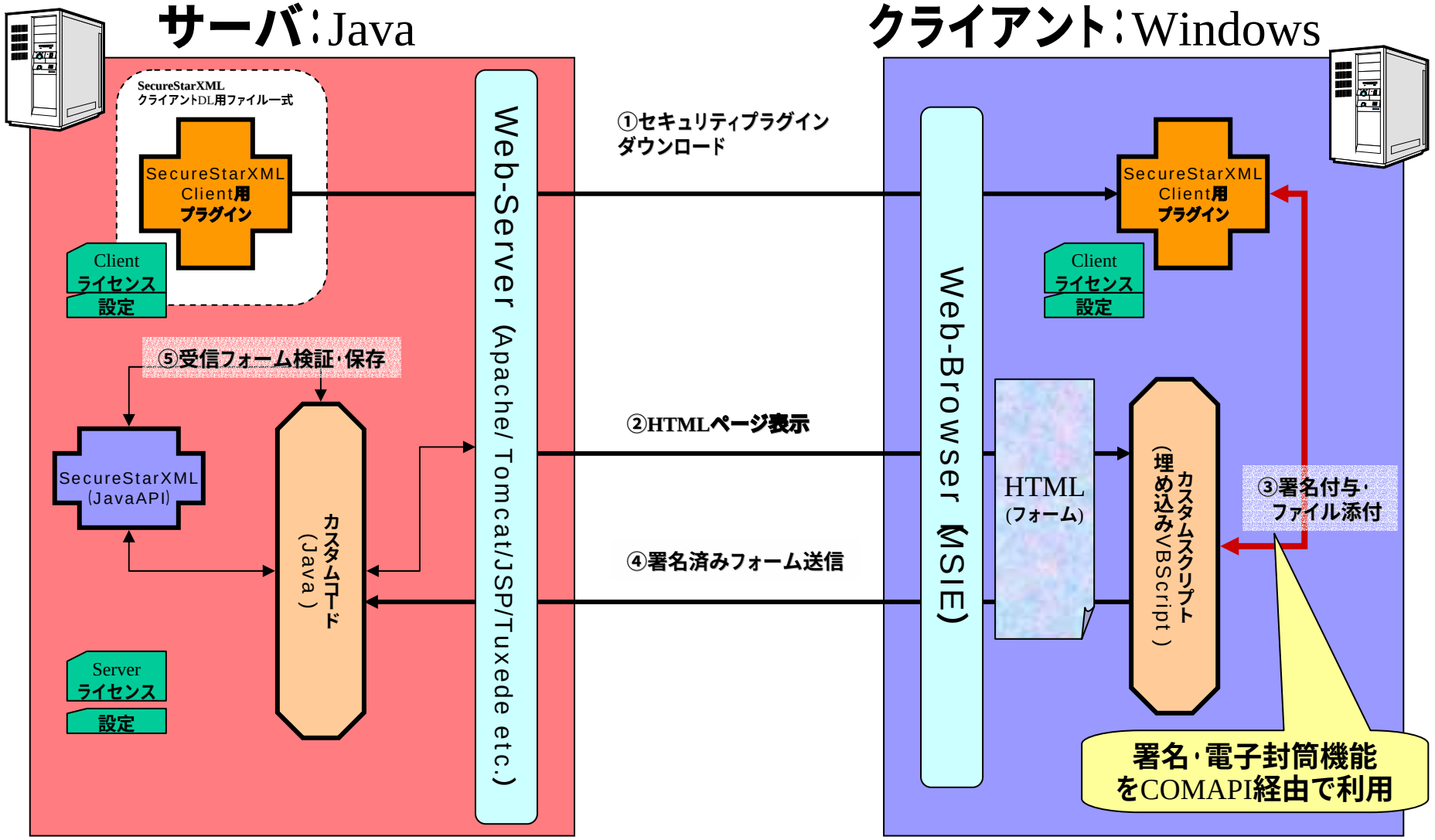
開発元： 大日本印刷

販売元： ネットマークス

http://www.netmarks.co.jp/prdct_srvc/prdct_info/solution/secure_star/index.html

方式・構成

(Hybrid Client/Server Model)



特徴

規模： １００KL（Windowsモデル）

特徴： 既存のAPに電子署名（XML署名）機能を付加する開発ツール。

- 電子政府各種認証基盤対応
- 世界標準電子証明書対応（X.509/RFC3280他準拠）
- Java/Windows両プラットフォーム対応
- 案件専用でなく、汎用である＝高信頼･低コスト
- 添付書類取り回し問題を解決（添付書類を完全に１つのＸＭＬでハンドリング）
- 電子申請などのネットメッセージングに必要な機能をオールインワンのＳＤＫとアプリで提供。（住基カード対応、署名/証明書処理、書類添付、ユーザナビゲーション処理等）

導入事例：

- 岐阜県、公正取引委員会、その他各都道府県及び市町村向け電子申請システム
- 某医療機関、某金融機関（予定）

動作環境

Windows版：Windows 98SE , NT4.0, 2000, XP ＋ IE 5.5SP2以上

Java版：Java仮想マシンが稼動するOS ＋ JRE 1.3

(Windows 98SE, NT4SP6, 2000, Linux RedHat 7.4上で動作確認済み)

開発苦労小話

【1】日本語対応

・WorldWideなミドルウェアは日本語非対応のため上手く適用できない。
・補助漢字対応

【2】政府認証基盤対応

・各認証基盤対応
公的個人認証基盤(JPKI)、商業登記認証基盤、政府認証基盤(GPKI)、自治体認証基盤(LGPKI)の各々に対応した機能の実装

【3】要件定義のあいまい対応

開発着手後でも要件定義があいまいな部分が多数あり、取捨選択を迫られた。

開発苦労小話
「日本語対応」

JNSA

- 海外ベンダ製SDKでは日本語対応が不十分。
  - -サーバ系プログラムでShiftJISしか使えないものがある（ASPなど）
  - -日本認証基盤仕様を満たすのが極めて困難な場合がある
    （海外SDKではまったく処理できないH社策定のX.509証明書拡張仕様など）

- JIS-X0212 補助漢字対応
  - - JIS-X0212 補助漢字保持のためのUTF-8透過性確保

    クライアントサイド、サーバサイド双方のアプリが問題をクリアする必要があった。
    しかし、Windows98、NT4.0等ではUTF-8に対応していない。 (´･ω･`)ｼｮﾎﾞｰﾝ
    → クライアントサイドのUTF-8表示部を独自実装。
    →サーバサイドでUTF-8処理可能な環境を選択した。（ASP.NET）

開発苦労小話
「政府認証基盤対応」

- 設計段階で必要な時期に認証基盤／ICカード関係に関する仕様などの技術情報取得に難儀した。
(もっと広く一般に公開されるべき内容と思われる。) ヽ<*`Д´>ノ ｺﾞﾙｧ
- 上記仕様を確認した結果、補助漢字対応問題が発覚。 (´･ω･`)ｼｮﾎﾞｰﾝ

・LDAP ? OCSP ? CVS ?

開発着手段階で、どの方式になるか未定。

→ 結局、全部実装。
- テスト環境構築に苦しむことに。(まともに組むと数億円のコストが！)
- Challenge PKI 2001のテストスィートが有用であった。

→ 各プロトコルともSSL対応が必須であることも(本番テスト直前で)発覚。

－ ('Д')ﾎﾞｶｰﾝ
- SSLサーバを立て、上記テストスィートのScriptを移植。

→ SSL対応を追加開発。 (´･ω･`)ｼｮﾎﾞｰﾝ

開発苦労小話
「要件定義のあいまい対応（1）」

- **XMLSignature vs PKCS#7 vs PDF署名**
  → PKCS＃7では、将来的な汎用性に乏しいため、XMLと親和性の良いXMLSignatureを採択。
- **XMLSignature- Detached vs Enveloping vs Enveloped 署名**
  → Detachedが他の方式の機能を全て包含するので、採択。
- **XMLSignature バージョン：何年版？**
  最新版の2002年4月版を採択すべき。
  → 開発工期の関係で2000年7月版を適用。

- **XMLSignature 推奨Transform, XPath記述は?**
  あまりに曖昧な仕様が多いため、本来は電子政府用などに軽量なサブセットが規定されるべき。
- **XMLSignature 正規化: ExclusiveC14N vs InclusiveC14N, WithComment vs None**
  自ファイル署名の場合、XML正規化処理でネームスペースへの依存度が高すぎるInclusiveC14N(最も現在普及している単純な正規化アルゴリズム)は、不適。ExclusiveC14Nを採択すべき。
  → 実際には開発工期の関係で同等効果の RFC-2803 アルゴリズムを適用。

開発苦労夜話
「要件定義のあいまい対応（2）」

- **MS-CryptAPI　vs　PKCS#11**
  - → PKCS#11は開発側の負担が大きい曖昧な規格なので、MSCAPIを採択。
  - 実際他の電子申請システムでJavaからPKCS＃11をコールするのを断念し、JNI経由でMSCAPIをコールするなど、本末転倒な実装をしているものもあった。
  - ↑無理にオープン系で実装しようとして失敗。

- **MSCAPI 証明書ストア経由カードアクセス型　vs　住基カード直接アクセス型**
  - → 住基カードのCSPを直接コールするのは汎用性に乏しいため、ストア経由方式を採択。

電子申請システム開発時のあいまい対応事例
- 形式審査時の必須確認事項
- 署名と署名対象の紐付けの運用方法
- 自治体間、省庁間等で署名文書形式、文書交換の運用スキーム
- 暗号化について：文書の暗号化についての規定がない。

おわりに

ご清聴ありあとうございました。

WGグループ一同