



証明書利用の現状とこれから

日本認証サービス株式会社



当社の特徴

- 富士通、日立製作所、NECの合併会社
 - ◆ 中立性
 - ◆ 信頼性
 - ◆ 標準性
- マイクロソフト認定国産ルート認証局
第一号
- 電子署名法認定認証事業者第一号



当社のサービス

■ 認証の全領域をカバー


◆1997 PaymentSign(SET/SECE)

◆1998 SecureSign(一般認証局)

◆2001 AccreditedSign(電子署名法)

◆2009春予定

SecureSignAD(WebTrust for CA)



現在のサービス体系

SecureSign(一般暗号化・署名用証明書発行)

- ・パブリックサービス

 - Webサーバ証明書、S/MIME証明書、職責証明書

 - クライアント証明書、電子署名サーバ証明書

- ・プライベートサービス(構築・運用サービス)

AccreditedSign(認定認証業務の証明書発行)

- ・パブリックサービス

- ・プライベートサービス(構築・運用サービス)



AccreditedSignパブリックサービスの利用状況

1. 申込み証明書のタイプ

基本型(氏名、住所)38%、ID型(住基4情報)8%

属性型(基本型+所属法人等)54%

2. 利用申込み時のアンケート結果(回答率48%)

1) 利用用途

特許庁インターネット出願18%、電子入札:公共工事16%

・物品9%、以下、雇用保険、労働保険、e-Tax、

特殊車両通行許可申請、定款認証・・。

2) 新規申込み60%、更新申込み40%

3) 当社選択理由

信頼性30%、料金26%、知人の薦め21%、対応9%



AccreditedSignパブリックサービスのFAQから

Q. 法人名義の電子証明書を申し込みたいが、申請に必要な書類に住民票などの個人名義の書類がなぜ必要か？

Q. 電子証明書の利用者は誰がいいのか、どのように決められているのか？

Q. 電子証明書をダウンロードしたが、実際にどう使えばいいのか？

Q. 電子証明書の記載事項に変更が生じた場合、変更の手続きはどうすればいいのか？

Q. 更新する際の手続きは？（有効期限満了案内はあるのか？、継続は出来ないのか？）


Q. 証明書の更新後、利用するシステムや手続きでは何か変更が必要か？

Q. 住民票住所に住んでいないが本人限定受取郵便は届く？



PKIの技術動向

- ◆ ベースとなる技術標準は確立済み
- ◆ 利用局面にあわせた改良が今後の課題
 - ⇒ プラットフォームの拡大
 - ⇒ 署名対象の拡大
 - ⇒ 署名検証期間の拡大
- ◆ 技術そのものの改良
 - ⇒ アルゴリズム改善
 - ⇒ 相互認証の更新



プラットフォームの拡大

- ◆ 署名／署名検証のプラットフォーム。
- ◆ 従来はほぼ Windows に限定できた。
Linux系アプリケーションの台頭
⇒ (**OpenSSL/NSS** などとの整合)

- ◆ 従来はほぼ PC に限定できた。
携帯端末、スマートフォン…
⇒ (**鍵セキュリティ条件の見直し**)



署名対象の拡大

- ◆ 単純なテキストから構造化文書へ
- ◆ PKCS#7一辺倒から署名の埋め込みへ
 - ➡ PDF, XML/SOAP, ODF/OOXML...
- ◆ 構造化文書ハンドラでの証明書管理
 - ➡ PKIをWindows CSPに任せるか
独自の鍵／証明書管理を行うか
- ◆ 署名鍵の供給方法多様化と信頼点管理



署名検証期間の拡大

- ◆ いつまで署名検証できなければならないか
 - ⇒ 従来は「署名後速やかに」だった。
 - ⇒ 「証明書有効期間切れ」と「失効」
- ◆ 電子文書の保管の議論を契機とする
署名検証可能期間の長期化
 - ⇒ 長期保管 ← 長期署名 ← タイムスタンプ



当社の取り組み状況

◆ プラットフォーム拡大

携帯端末での署名への取り組み

OpenSSL ベースシステムへの証明書発行

◆ 署名対象の拡大

ODF 署名の採用(電子更新申込み)

署名伝票の SOAP 授受(検討中)

◆ 署名検証期間の拡大

XAdES による長期保管(電子更新申込み)



いま, PKIは

- ◆ 現実の複雑さへの格闘

PKIの仕組みの美しさに比べ、現実には複雑。

- ◆ なぜ、PKIに完全を求めるのか

完全を主張し、完全を保証するか、できるのか。

- ◆ アプリケーション分野のチャレンジ不足

認証(証明)、デジタル署名、暗号と多目的なるが故に器用貧乏になっていないか。



2つの視点 その1 個人

- ◆ 個人をめぐる環境変化、今後の変化
情報爆発の時代 情報量の拡大
情報コントロールができない時代
スパム、ワンクリック詐欺、フィッシング等

インターネットに対する認識、意識が変わりつつある(不安、危険、漠然とした疎外感)

- ◆ PKIにできること
実社会の安定感、安心感をしっかりと押し出してゆくこと

2つの視点 その2 法人

◆ 内部統制時代の到来

- ・法人の管理責任、説明責任が基本に
（管理とは、何をどのように管理するか）
- ・総ての業務、総ての判断を記録する
- ・偽造・変造をゆるさないこと、そのために必要なこと

◆ PKIにできること

- ・総ての情報をコントロールすること
- ・偽造変造を防止すること
- ・監査を可能とすること





これからのPKI利用

- ◆ ネットワーク社会の高度化・複雑化につれてますます重要になる。
- ◆ シングルサインオンやワンタイムパスワード、OpenIDなどの認証技術と併用される。
- ◆ ゼロ知識証明、匿名認証など秘匿情報の取扱いや個人を特定しない仕組みが重要
Ex) 電子投票、電子抽選、・・・



これからのPKI利用(認定認証業務)

➡ 官公庁(C,B to G)から民間(B to B,C)へ

- ◆ 内部統制時代において電子署名の重要性は認知されつつある。(タイムスタンプと電子署名)
- ◆ ネットでの会員申込み・口座開設での本人確認の重要性
- ◆ 課題1. 証明書料金が高い。
 - Ex) 電子契約で利用
 - 証明書料金: 9,000円～
 - 印紙: 4,000円(継続的取引の基本となる契約書)
- ◆ 課題2. 属性情報の取扱い
 - Ex) 資格情報
 - 一級建築士、ケアマネージャー、...



日本認証サービス株式会社は、

- ・わが国におけるPKIの草分けとしての信頼に応え、
 - ・豊富な経験と人的な資源を誇りに、
 - ・大きな視点と戦略性を持って、
- 安全・安心な社会に貢献します。