

ユビキタスネットワーク時代のPKI  
安全安心なネットワークへの技術的裏づけと応用  
(応用編)

富士ゼロックス株式会社  
稲田 龍

<Ryu.Inada@fujixerox.co.jp>

Copyright © 2004 富士ゼロックス株式会社

ユビキタス時代に必要なもの?

- 確実な認証
  - どこでも、いつでも、ある程度、確実な認証
  - 孤立した環境でも動けることが出来ればbetter
- 安全な通信
  - 経路上で盗聴が出来ない
    - RFIDの様に無線環境にも適応できること
  - 経路上で改竄されない
    - 最低限、改竄の検出が出来ること
- 情報の漏洩を最小限にしたい

Copyright © 2004 富士ゼロックス株式会社

## 続き



- 端末上でのリスク
- 端末間通信に対するリスク
- サーバ/端末間に置けるリスク
- サーバ上でのリスク
  
- パスワードからバイオメトリックス?
- 知識での認証からデバイスでの認証へ?
- クレデンシャルの内容の変異
  - 単なるパスワードからより強度のあるものへ

Copyright © 2004 富士ゼロックス株式会社

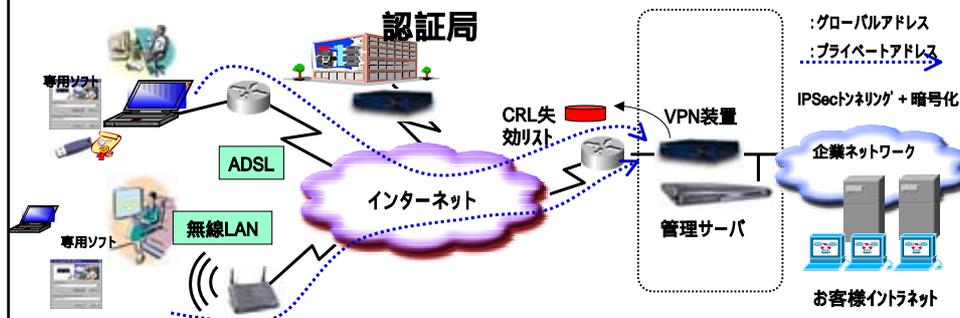
## PKIの必要性



- インターネットで要求される便利で安全な認証
  - 安心、安全なインターネット環境(PKI空間)のために、様々な用途の認証、様々なレベルの認証、広いドメインでの認証を実現したい
  - 広く採用するには、標準化された技術を採用したい
- 電子政府と政府認証基盤(GPKI)など動向
  - GtoBのための認証基盤 - > GPKI
  - 3300の地方自治体のための認証基盤 -> LGPKI
  - GtoCのための認証基盤 -> 公的個人認証基盤
- Identrusのような国を超えたB2Bの認証基盤
  - サイバー世界では国境がない。
  - 世界に通用するセキュリティが必要
- GPKI、IdentrusのPKIの技術的要件
  - 否認防止が可能な署名

Copyright © 2004 富士ゼロックス株式会社

## 例えばInternet-VPNサービス



Anywhere, Anytime, Anyplace モバイルオフィスを実現するためには、確実な認証が必要

Copyright © 2004 富士ゼロックス株式会社

## T-Engine Forumでの動向



- uIDタグにクラス分け
  - Class0-Class8まで
    - Class 0: Visible ID(2次元バーコードなど)
    - Class 1: Low Level RFID
    - Class 2: High Level RFID
    - Class 3: Low Level Smart Card
    - Class 4: High Level Smart Card
    - Class 5: Low Level Active Tag
    - Class 6: High Level Active Tag
    - Class 7: Secure Box
    - Class 8: Secure Server
- エア・プロトコルにてClass 4以上では重要な有価値情報の取り扱いのためにPKIを使用

Copyright © 2004 富士ゼロックス株式会社

## UPnP Forumでの動向



- シナリオと要件
  - 2001年初頭に定義 Security
- セキュリティ作業委員会
  - 2001年8月に設置
- Version 0.8の仕様書完成
  - 2002年3月
- 試験的実装と 3<sup>rd</sup> plugfest
  - 2003年10月

Copyright © 2004 富士ゼロックス株式会社

## PKIはどう使われているのか?



- 現行ではHTTPSのホスト認証が主流
    - 伝送路の安全性の確保
    - ホストの正当性の保証
- 判りやすく、利用者に負担をかけてない
- 利用者に対して効果(伝送路の暗号化)がわかりやすい
  - HTTPSに対応したブラウザがあれば、利用者は何も意識せずに使える

Copyright © 2004 富士ゼロックス株式会社

## PKIはどう使われているのか?



- 一方で、クライアント認証はほとんど行なわれていない
  - 金融系で一部使われている

利用者の負担が大きい?

- パスワードに比較して効能に差が見えにくい
- 利用者の利便性がない?
- 費用がかかる?

Copyright © 2004 富士ゼロックス株式会社

## 今後どう使われていくのか?



- インターネット = ユビキタスネットワーク?
  - とはいえ、多くの状況ではインターネットを経由するであろう
  - 認証すべきものが増えてゆく?
    - サーバのみならずPDA/携帯電話/家電……
    - いわゆる**機器認証**が増えてゆく?
      - RFIDなどの情報の交換にもPKIはついて回る?
  - 「**認証**」に重きが行くのではないか?

Copyright © 2004 富士ゼロックス株式会社

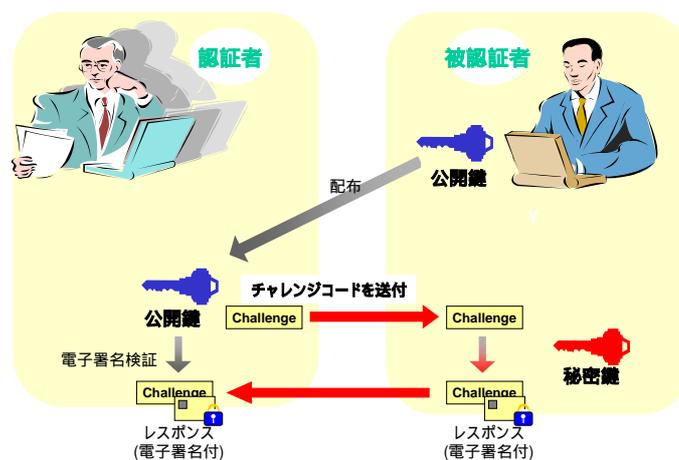
## 認証への応用



- 基本はChallenge & Response
- PKIの利点
  - 認証サーバを必要としない
    - 孤立したネットワークでの利用が可能
    - 複数の拠点間での移動ノードに適している
- PKIの欠点
  - 演算が遅い
  - 厳密な失効確認をすると大変

Copyright © 2004 富士ゼロックス株式会社

## 認証への応用の概念



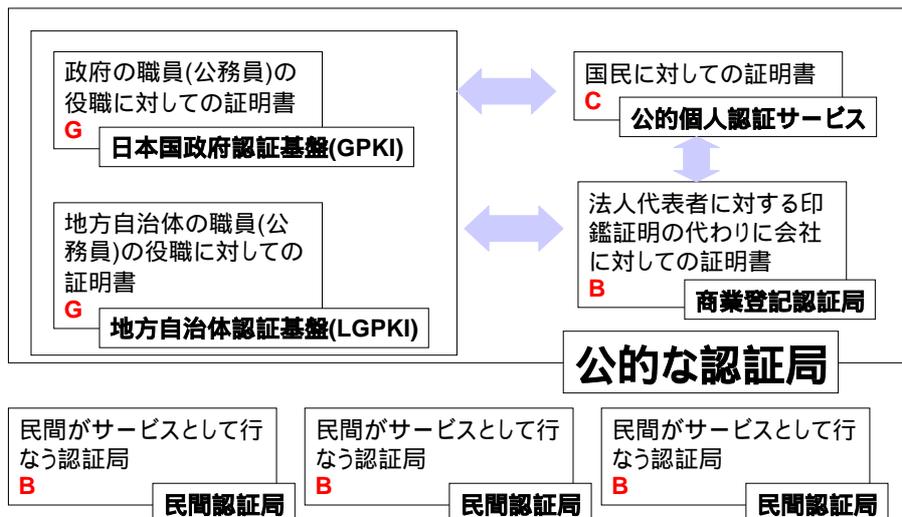
Copyright © 2004 富士ゼロックス株式会社

## 実社会での流れ

- 法的な環境の整備
  - いわゆる「電子署名法」 否認防止
  - e文書法
- 政府での利用
  - GPKI(政府)
  - LGPKI(地方自治体)
  - 公的個人認証サービス(国民)
- 公的機関において使われる **認証システム** にPKIが採用されている

Copyright © 2004 富士ゼロックス株式会社

## 日本における認証局



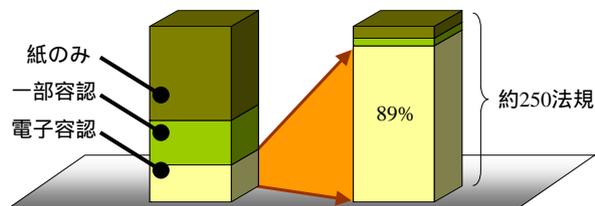
Copyright © 2004 富士ゼロックス株式会社

## e-文書法とは?

Copyright © 2004 富士ゼロックス株式会社

## e-文書法の概要

- 保存が義務付けられた文書の電子化を容認する統一的な法律
  - あらゆる法律への適用
  - 警備業法、保険業法、 などなど
- 電子化の操作者による電子署名とタイムスタンプ付与が要件化
  - 海外事例: カナダ、オーストラリア、韓国、ドイツ(Scan to File)
- スケジュール
  - 秋の臨時国会へ提出 2005年4月に施行予定



### 参考

e-文書保存法: <http://www.kantei.go.jp/jp/singi/it2/kettei/040206honbun.html>

e-文書イニシアチブについて: <http://www.kantei.go.jp/jp/singi/it2/dai26/26siryou4.pdf>

内閣官房IT担当室: 民間保存文書の電子的保存に関する対応の方向性について,平成16年4月5日

Copyright © 2004 富士ゼロックス株式会社

## e-文書法の概要(続き)

- 通則法と整備法
  - 通則法
  - 電子保存容認のための共通事項を定める
  - 対象法令は約250本
  - 税務関係書類も、原則的に全ての電子保存を容認
  - 一部の文書は適用対象外(関連法令50本)
    - 緊急時に即座の確認が必要(船舶の安全手引き書など)
    - 現物性がきわめて高いもの(免許証、許可証など)
    - 適正公平な課税のために容認できないもの
  
- 整備法
  - 通則法のみでは手当が完全でない場合の規定整備
  - (NPO促進法など)

Copyright © 2004 富士ゼロックス株式会社

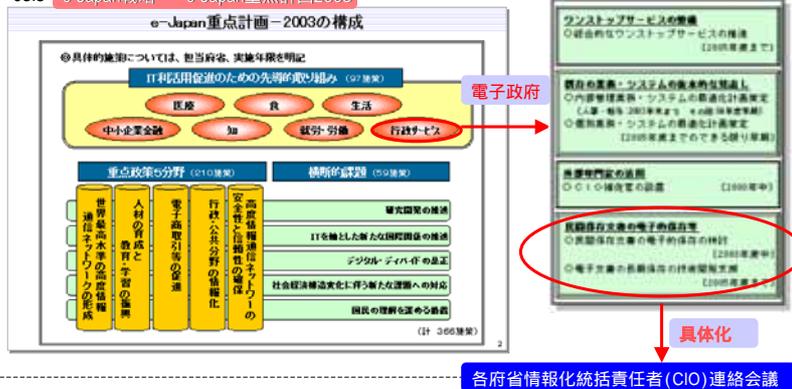
## IT戦略・電子政府戦略の全体像

**経済財政諮問会議** 内閣府に設置。経済財政運営及び経済社会の構造改革に関する基本方針を諮問。

03.7 経済財政運営と構造改革に関する基本方針2003 e-Japan戦略 に基づき、第2期IT革命を推進する。

**IT戦略本部** 内閣に設置。高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進。

03.8 e-Japan戦略・e-Japan重点計画2003



Copyright © 2004 富士ゼロックス株式会社

電子政府構築計画

## e-Japan戦略 加速化パッケージ



### 04.2 e-Japan戦略 加速化パッケージ

1	アジア等IT分野の国際戦略
2	セキュリティ(安全・安心)政策の強化
3	コンテンツ政策の推進
4	IT規制改革の推進
5	評価
6	電子政府・電子自治体の推進

e-文書イニシアティブ: 民間で保存義務のある財務関係書類、税務関係書類等の文書・帳票のうち、電子的な保存が認められていないものについて、文書・帳票の内容、性格に応じた真実性・可視性等を確保しつつ、原則としてこれらの文書・帳票の電子保存が可能となるようにすることを、統一的な法律(通称「e-文書法」)の制定等により行う。電子保存の容認の要件、対象範囲等について早急にとりまとめ、2004年6月頃を目途に法案を早期に国会に提出する。(内閣官房及び関係府省)

#### 04.3.1 経団連(情報通信委員会)が税務書類の電子保存範囲の拡大を改めて要望。(2000年以降毎年要望)

##### 税務書類の電子保存に関する報告書

1. 紙と同程度の表現力の確保 ……解像度200～300dpi、TIFF又はPDF(望ましい)
2. 改ざんの防止 ……入力操作者の識別・認証、入力操作者の電子署名、時刻認証
3. 閲覧性・検索性の確保 ……OCRにより電子化文書に年月日等の索引を付与

経済界における税務書類の紙による保存コスト試算: 年間約3,000億円

ユーザ企業のコスト試算: 紙保存コスト約70億円/7年間 電子化保存で20～30億円削減/7年間

Copyright © 2004 富士ゼロックス株式会社

## 参考:e-Japan重点計画-2004(案)



04.5.21 内閣官房IT担当室が、「e-Japan重点計画-2004(案)」に関するパブリック・コメントの募集

04.5.31 経団連(情報通信委員会 情報化部会)がパブリックコメント

##### 「e-Japan重点計画-2004(案)」に関する意見

「e-文書法」の立案方針や法案の策定においては、原則として、民間に保存が義務付けられている全ての書類を電子保存の対象とするともに、具体的な要件の設定や運用にあたっては、より多くの企業が活用できるような制度とすべきである。

04.5.31 JEITA(総合企画部企画グループ)がパブリックコメント (他にJIIMA、富士通などがコメントしているが割愛)

##### 「e-Japan重点計画-2004(案)」に関する意見について

IT化の推進のためには、紙文書の電子化が必須であり、紙での保存が義務付けられている書類の電子保存範囲拡大と、イメージスキャナ等の活用による紙文書の電子化を、「e-Japan重点計画-2004」に明記していただきたい。また、民間における文書・帳票の電子的な保存を、文書・帳票の内容、性格に応じた真実性・可視性等を確保しつつ、原則として容認する統一的な法律(通称「e-文書法」)では、「電子保存を認める対象文書」と「電子化の要件」を早期に開示していただきたい。

04.6.15 IT戦略本部が、e-Japan重点計画-2004(案)概要など公表

##### e-文書イニシアティブについて

民間への紙による文書保存義務について、原則全て電子保存を容認。

「e-文書法」= 通則法(共通事項、措置する法律数250本)と整備法により構成。

2005年4月の施行を目指し、2004年度のできるだけ早期に国会提出。

\* パブリック・コメント結果もIT戦略本部が公表。PDF反対、XMLにすべきという意見あり。

Copyright © 2004 富士ゼロックス株式会社

# e-Japan重点計画-2004(案)



## e-文書イニシアティブの実現

成果目標: 法令により保存が義務付けられている文書・帳票のうち、電子的な保存が認められていないものについて、文書・帳票の内容、性格に応じた真実性・可視性等を確保しつつ、原則として民間企業等が電子保存できるようになるように、法案を早期に国会に提出し、民間企業等における文書保存コストの削減を図る。また、その他IT化が遅れている分野や現実世界の制度と整合等を図る必要がある分野においても、早期に規制改革を進めていく。

### a) e-文書イニシアティブの実現(内閣官房及び関係省)

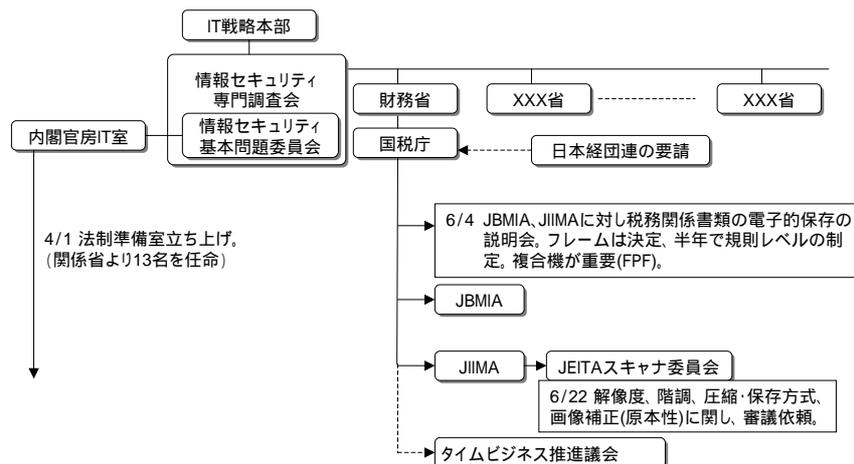
民間における文書・帳票の電子的な保存を、文書・帳票の内容、性格に応じた真実性・可視性等を確保しつつ原則として容認する統一な法律(通称「e-文書法」)の立案方針等を策定し、2004年度早期に法案を国会に提出するなど、e-Japan 戦略 加速化パッケージのe-文書イニシアティブの早期実現を図る。

### b) 電子文書の長期保存のための基礎技術の研究開発(経済産業省、総務省)

2005年度までに、暗号技術、電子署名等の技術、タイムスタンプ・プラットフォーム技術、デジタル・アナログ・ハイブリッド保存技術等、電子文書の長期保存に必要な基礎技術の研究開発を行う。

Copyright © 2004 富士ゼロックス株式会社

## 関係省庁の動き



注:JIIMA  
社団法人 日本画像情報マネジメント協会

Copyright © 2004 富士ゼロックス株式会社

## 主な要点(全体)



- 各社独自の技術に依存したのではなく、業界としての対応を要請
- 単体スキャナよりも複合機が期待
- 複合機に対する、機能・性能・セキュリティ要件が必要
- 国税庁が最も厳しい要求
  - 内閣官房IT室は、国税庁の意向を気にしている

Copyright © 2004 富士ゼロックス株式会社

## 主な要点(国税庁)



- 紙との同一性(改ざん検知)
  - モノクロ文書でも、300dpiのフルカラーを要求
- タイムスタンプを重視
  - 電子署名は、タイムスタンプとの組合せを要求
  - (コスト負担があれば、電子署名だけで可)
- イメージ化行為者の電子署名
  - 電子署名は、電子署名法に基づく、特定認証局が発行するもの
- イメージ化時点のタイムスタンプを要求
  - イメージ化されてからタイムスタンプまで人の介在を極力排除したい。
- バージョン管理
  - 利用したスキャナー情報の付与
- 画像補正の有無
- OCR処理と検索

Copyright © 2004 富士ゼロックス株式会社

## 参考：PDFトピックス



### 標準化

- 工業標準化法に基づき(日本工業標準調査会の審議)、経済産業大臣が標準情報(TR)公表
- 日本規格協会認定が、TR X 0026:2000として認定
- ISO/IECでもPDF/X (PDF/eXchange)として国際標準化。PDFの規格全体のサブセット。

### 官公庁調達の例

- 2002.12  
国土交通省が営繕工事ならびに建設設計業務等の電子納品においてPDFファイルでの納品を指定。
- 2002.4  
法務省が商業登記規則に基づいて登記所に提出する書類の電磁記録方式にPDFの電子署名の仕様を指定。

Copyright © 2004 富士ゼロックス株式会社

## 帳簿の電子化の法的な流れ



- 電子帳簿保存法(1998-)
  - 「自己が一貫して電子計算機を使用して作成する帳簿書類」に限り、電子保存が認められる
    - 法人税・消費税、源泉所得税、所得税・消費税、その他国税全て
    - 紙で受け取る証憑書類、手書きの帳簿のスキャンは除外
  - B2C(見積・契約・注文・領収)の利用シーンに向かない
    - H13年度:7,569件
    - H14年度:8,519件
    - H15年度:30,327件(6月まで)
- 経団連
  - 「**税務書類の電子保存**」を強く要求
  - 紙の管理コスト削減が企業経営を圧迫
    - 大手企業の紙管理:2億~40億ページ/年程度(JIIMA調査)
    - 経済界全体の保存費用:3000億円(経団連試算、ヒアリング11社)

### 参考

電子帳簿保存法:電子計算機を使用して作成する国税関係帳簿書類の保存方法の特例に関する法律

経団連報告書:<http://www.keidanren.or.jp/japanese/policy/2004/018report.pdf>

Copyright © 2004 富士ゼロックス株式会社

## 経団連の動き



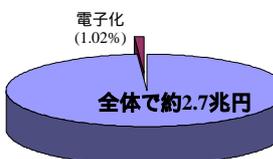
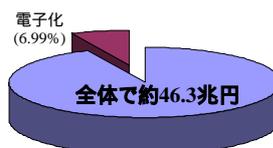
- e-Japan戦略 (2003.7)
  - 民間に保存が義務づけられている文書・帳票の電子保存を容認する方針
  - 経団連: **税務書類の電子保存**に関する打ち合わせ会(2003.5)を実施
- e-Japan重点計画 -2003(2003.8)
  - 2003年度中に、関係省庁は電子保存の容認の要件やスケジュール等の対応の方向性を明確化し、内閣官房がとりまとめる
  - 経団連:2003年度規制改革要望で**重点要望項目**として**税務書類の電子保存拡大**を挙げる(2003.10)
    - <http://www.keidanren.or.jp/japanese/policy/2003/098/kobetsu.html>
  - 東京海上の石原社長が強く発言
    - 「例えば弊社、一社でも、保管関連費用としては、年10億円程度かかっていると試算している。そういった点でいえば、日本全体では非常に大きな金額になると思う。」
    - 「紙の資料の保管コストに比べ大幅な削減と同時に、環境問題への対応としてのペーパーレス社会の推進にも寄与する」
    - <http://www.kantei.go.jp/jp/singi/it2/kaisai.html>
  - 茂木大臣の発言
    - 政府が金を掛けずに3000億円の経済効果が生まれるのなら、良いのではないかと。
- e-Japan 加速化パッケージ(2003.12素案,2004.2)
  - e-文書イニシアティブ:通称e-文書法の制定に言及
  - 経団連: **税務書類の電子保存範囲の拡大**を改めて要望(2004.3)
    - <http://www.keidanren.or.jp/japanese/policy/2004/018.html>

Copyright © 2004 富士ゼロックス株式会社

## 電子商取引の現状は?



- B2B商取引
  - 市場規模は全体で約46.3兆円
  - 電子化された取引は約6.99%
- B2C商取引
  - 市場規模は全体で約2.7兆円
  - 電子化された取引は約1.02%
  - 2007年予測でも4.5%といわれている



当分の間は、B2Cにおいて紙の証憑書類の管理が必要となる

- 作成 閲覧 流通 保管 破棄
- e-文書法が必要

Copyright © 2004 富士ゼロックス株式会社

## 電子保存のための技術要件



- 可読性 (紙と同等の表現力の確保)
  - 一定値以上のスキャン性能
    - 300dpi以上
    - 256階調(1677万色)
  - ファイル形式と圧縮
    - TIFF
    - PDF
    - 品質に影響のないデータ圧縮
  - 検索性の確保
    - OCRによる索引の入力
    - 重要項目による検索機能の確保
      - 年月日、金額など
- 真正性
  - 入力操作者の認証と電子署名
    - 権限を有する者によって申請に電子化された旨を証明
    - 特定認証局の証明書であることが前提
  - タイムスタンプの付与
    - 基準や認定について関連団体と協議

具体的な要件は主務省令で定める

Copyright © 2004 富士ゼロックス株式会社

## 業務プロセスへの適用



- e-文書法で考えられている方式
  - 業務サイクル対応入力方式
    - 事務処理規程でイメージ化のタイミングを定める
    - イメージ化時点のタイムスタンプを付与
  - 早期入力方式
    - 書類を取得後速やか(1週間以内)にイメージ化
    - イメージ化時点のタイムスタンプを付与
  - 一括入力方式
    - 大量に発生する書類を想定
    - 一定の事務処理規程を元に一括してイメージ化
    - コスト負担を考慮して、タイムスタンプを必須としない
- 国税関連帳簿書類への適用案
  - 業務サイクル対応入力方式
  - 早期入力方式
    - 帳簿、決算関係書類
    - 契約書、領収書などの国税関係書類
    - 取引金額が3万円未満
    - 電子公証制度による私署証書の宣誓認証
  - 一括入力方式
    - 資金やモノの流れに直結連動しない書類
    - 見積書、注文書、契約申込書

Copyright © 2004 富士ゼロックス株式会社

## 参考:法令保存文書(抜粋)



保存期間	保存を定める法律	保存対象
10年	商法36条、143条、429条 有限会社法75条①	商業帳簿等
	商法244条③	株主総会議事録
	商法260条ノ4③	取締役会議事録
7・5年	所得税法第148条及び 所得税法施行規則第63条 ならびに 法人税法第150条の2及び 法人税法施行規則第67条	仕訳帳、総勘定元帳等の帳簿、 棚卸表、貸借対照表、損益計算書、 注文書・見積書・契約書の控え
5年	商法282条	貸借対照表、損益計算書、 営業報告書等
4年	雇用保険法施行規則第143条	雇用保険に関する書類
3年	労働基準法第109条	労働者名簿、雇入、解雇、退職 に関する書類
2年	雇用保険法施行規則第143条	雇用保険被保険者に関する書類

(小谷@富士通,2003)

Copyright © 2004 富士ゼロックス株式会社

## 電子署名アプリケーション



- ファイル/データ等に対して電子署名
  - 文書などのデータに署名する
  - コード署名といわれるプログラムへの署名
- 電子署名法の施行/電子政府での採用
- 専用アプリケーション
  - 電子申請など
- 汎用アプリケーション
  - Acrobat
  - Microsoft Office XP
  - DocuWorks

Copyright © 2004 富士ゼロックス株式会社

## シリアル署名とパラレル署名

- 署名をどの部分に行うかの違い
- 用途により使い分けが必要
- Acrobat/Office XP/DocuWorksともにシリアル署名を実装

Copyright © 2004 富士ゼロックス株式会社

## シリアル署名

- 署名を「追加」していくイメージ
- 長所
  - 署名の順番がわかる
- 短所
  - オリジナルの文書に対しての署名

開発部門議事録 明日までに実装の経過報告をすること
Aさんの署名(議事録に対して署名)
Bさんの署名(議事録+Aさんの署名に対して署名)
Cさんの署名(議事録+A/Bさんの署名に対して署名)

Copyright © 2004 富士ゼロックス株式会社

## パラレル署名



- 署名対象に対してのみ署名を行う
- 順番に関係なく署名検証可能

稟議書  
甲者との締結に関する条件

Aさんの署名(稟議書に対して署名)

Bさんの署名(稟議書に対して署名)

Cさんの署名(稟議書に対して署名)

Copyright © 2004 富士ゼロックス株式会社

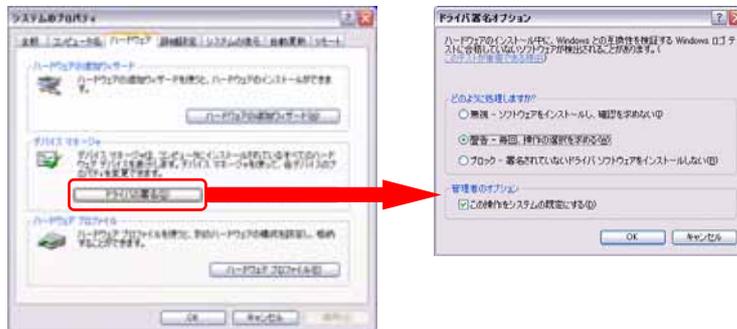
## コード署名



- ダウンロードしたプログラムが正しいかどうかをどう確認するか?
  - 悪意のあるプログラム/ウィルスの排除
  - 正当なデバイスドライバであるかどうかの確認

Copyright © 2004 富士ゼロックス株式会社

## Windowsのドライバの署名



マイクロソフトはWindowsのドライバに対して署名をすることにより、互換性の保障を行っている

Copyright © 2004 富士ゼロックス株式会社

## Active-Xのコード署名



- IEの機能拡張を行うActive-Xモジュールについてもコード署名を提供している



Copyright © 2004 富士ゼロックス株式会社

## 証明書の実効性/有効性

Copyright © 2004 富士ゼロックス株式会社

## 証明書の実効性/有効性

- 2001年の4月にいわゆる「電子署名法」が施行
  - 特定認証局が発行した電子証明書に実印と同様の権限を与えた
- 商業登記法の改正
  - 商業登記局が会社代表者に対して証明書を発行
    - 会社代表者に対しての印鑑証明に相当する
- 欧米では、バイオメトリックス情報を証明書に入れる動きもある
  - 身分証明書の代わりに使える証明書
  - 署名のイメージを入れる動きもある

Copyright © 2004 富士ゼロックス株式会社

## QC(特定証明書)とは何か?



- 通常の電子証明書に対して、より高位の「保証」をつける事を目論んでいる証明書
    - 欧州における公的個人認証の必要性から、
      - 自然人(個人)を対象
      - 法的に認められるための証明書として通用すること
- ➡
- セキュリティポリシーとそれを反映した証明書フォーマット(プロファイル)の制定が必要
  - 欧州の標準化団体により提唱された標準が、IETF で採用され RFC 3039 として規定されたものが「**クオリファイド証明書** (Qualified Certificate) (**特定証明書**)」
  - 現在はRFC 3739 として改訂版が出ている。

Copyright © 2004 富士ゼロックス株式会社

## QC(特定証明書)とは何か?



- 特定証明書の特徴
  - X.509 v3 証明書プロファイルに準拠
  - 基本領域、拡張領域への記載内容にルールを設定
  - 特定証明書に特化した拡張領域を保持
  - **「人」を対象とした証明書**
    - 必要となるポリシーを規定
- 記載内容に関するルールには、欧州電子署名指令案 (EU-directive) の指示のもと **ETSI** による標準化検討
  - 実際には欧州における法律制度・社会制度にのっとり内容についてさらに詳細な規定を加えて
- 特定証明書を定義したRFC 3739
  - 利用される国や団体の幅広い要件に対応できるように汎用的な内容

Copyright © 2004 富士ゼロックス株式会社

## 標準化動向



- 欧州における電子署名の要件を満たすために検討が進められた
  - 「電子署名についての欧州指令 (European Directive on Electronic Signature)」
    - Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
- IETFでインターネットでの適用の必要性を認め、Standard Trackとして標準化が進行中
- 911以降、米国内においてバイオメトリック認証の必要性が向上
  - 米国政府内の標準的な認証用ICカードとしてバイオメトリックス情報の利用が検討されている

Copyright © 2004 富士ゼロックス株式会社

## ETSIでの規格



- ETSI TS 101 862 V1.3.2 (2004-06)
  - Title: Qualified Certificate profile
- ETSI TS 101 456 V1.2.1 (2002-04)
  - Title: Policy requirements for certification authorities issuing qualified certificates
- ETSI TS 102 158 V1.1.1 (2003-10)
  - Title: Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates

Copyright © 2004 富士ゼロックス株式会社

## IETFでの規格



- Security Area/PKIX-WGで標準化が行なわれている
  - <http://www.ietf.org/html.charters/pkix-charter.html>
  - RFC 3739 Internet X.509 Public Key Infrastructure: unified Certificates Profile
    - 2004/3制定 RFC 3039の改訂版

Copyright © 2004 富士ゼロックス株式会社

## 日本では?



- 公的個人認証サービスなど特定証明書を適用できる/すべきものはある
  - 現状の公的個人認証サービスにおいては、個人を特定する情報としていわゆる4大基本情報(氏名、生年月日、性別、住所)を入れているが、特にバイオメトリクス情報は入れてはいない
    - 個人情報に対する扱い
  - IPA(情報処理推進機構)が、特定証明書を適用すべきではないかと画策している模様
    - 経済産業省の思惑あり?
  - 状況によっては来年度の電子署名法改正に組み込まれるかも(参考情報としては既にインプット済みの模様)
    - 2006年度変更を見据え、2005年度中に見直し
    - タイムスタンプの概念は入るとの情報あり

Copyright © 2004 富士ゼロックス株式会社

## QCの特徴 - 名前について



- 名前の一意性の保証(RFC 3739 2.4)
- 主体者ディレクトリ属性 (subjectDirectoryAttributes)をもつ場合がある
  - クリティカルフラグを立ててはならない
  - dateOfBirth/placeOfBirth/gender/countryOfCitizenship/countryOfResidenceの各属性を解釈できること

Copyright © 2004 富士ゼロックス株式会社

## QCの特徴 - 証明書ポリシー (certificatePolicies)



- **必須**
- **最小限1つのポリシーIDを持つこと**
- クリティカルでも**良い**
- 証明書発行目的が**ポリシーにより明確**になっていること
- 認証パス検証に必要なすべてのポリシー情報を含むこと

Copyright © 2004 富士ゼロックス株式会社

## QCの特徴 - バイオメトリック情報(biometric Information)



- **オプション**
- バイオメトリックテンプレートのハッシュとして格納
  - 証明書内に含まず、URIで参照しても良い
    - ナイーブな情報が含まれることに注意
    - URIは[http/https](http://)でなければならない
- 人間の検証にふさわしい情報の種類に限定することを**推奨**
- **クリティカルにはしてはならない**
- Picture/handwritten-signatureが予め登録済み

Copyright © 2004 富士ゼロックス株式会社

## 製品への対応



- RSA Security社
  - RSA Keon Certificate Authority 6.5
    - <http://www.rsasecurity.com/japan/news/data/200302181.html>
    - [http://www.rsasecurity.com/japan/products/keon/keon\\_certificate\\_authority.html](http://www.rsasecurity.com/japan/products/keon/keon_certificate_authority.html)
    - ニュースリリース内でクオリファイド証明書(QC/特定証明書のこと)に関するサポートを記述している

Copyright © 2004 富士ゼロックス株式会社

# PKI実装

Copyright © 2004 富士ゼロックス株式会社

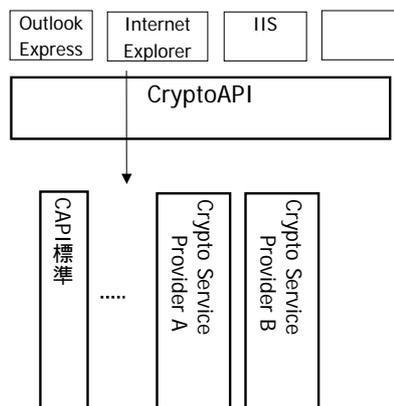
## PKI実装面

- Windows系
  - Crypto API(Microsoft)
  - OpenSSL
- JAVA系
  - JDK/JCE
- UNIX系
  - OpenSSL

Copyright © 2004 富士ゼロックス株式会社

# Windows Crypto API

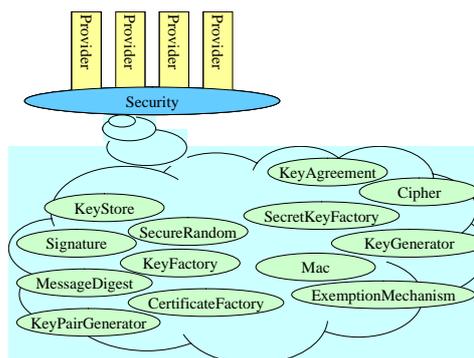
- CSP(Crypto Service Provider)モデル
- IE 4.0以降から提供
- 暗号エンジンをモジュール化
- 複数の暗号エンジンを保持
- Third Party提供のCPSを利用可能
- 証明書の検証に関しても良く考えられている
- 暗号エンジンを作る場合、[Microsoftにコード署名](#)をしてもらう必要あり



Copyright © 2004 富士ゼロックス株式会社

# JAVA/JCE

- JAVAの機能拡張モジュールとしてProviderモデルで実装されていた
  - 1.4より標準機能として実装されている
- 暗号機能/Hash機能/X509証明書操作機能を実装



Copyright © 2004 富士ゼロックス株式会社

## JDK/JCE



- java.security.cert以下に実装されている。
- クライアントとして使う面では十二分な実装
  - JDK本体で証明書の基本的なハンドリングが可能
  - JCE(Java Cryptographic Extensions)で暗号周りの機能を提供
    - Windows同様Third PartyのJCEに差し替えることが可能
    - Sunより証明書を発行してもらい、その証明書でコード署名を行う必要あり
  - JSSE(Java Secure Socket Extensions)でSSL/TLSを提供
- RFC3280の証明書検証アルゴリズム相当のメカニズムを実装
- CertPathBulder/CertPathValidator/CertStoreの3つに仮想化
  - CertPathBulder
  - CertPathValidator
  - CertStore

Copyright © 2004 富士ゼロックス株式会社

## OpenSSL



- 多くのUNIX系プラットフォームのデファクト実装
  - Linux/\*BSD\*に採用
- Windowsプラットフォームでも動作
- ApacheのSSL/TLSのエンジンとして広く使われている
  - Apache  
1.X+mod\_ssl+OpenSSL
  - Apache  
1.X+Apache\_SSL+OpenSSL
  - Apache 2.X(標準でSSL/TLSをサポート)



Copyright © 2004 富士ゼロックス株式会社