「インターネット上の信頼を確立する PKIの技術と運用」(基礎編)

セコム株式会社IS研究所
松本　泰
yas-matsumoto”AT”secom.co.jp

インターネット上の信頼を確立する PKIの技術と運用(基礎編)

1. PKI技術の概要
2. サブスクライバー/署名者
3. リライングパーティ/検証者
4. 認証局の信頼
5. PKIの構成
6. 証明書発行
7. 電子署名法
8. PKIの信頼性

セコムIS研究所 Intelligent Systems Laboratory

インターネット上の信頼を確立するPKIの技術と運用

PKI技術の概要

基本的な用語の理解など
ボタンの掛け違いがないように

PKI技術の概要
基本的な用語の理解　その１

セコムIS研究所 Intelligent Systems Laboratory

- **署名**(Signature)と**認証**(Authentication)
  - 自然人による**否認防止** (Non Repudiation) の**署名** (手書きの署名でも同じ)
    - 自分の意志で文書に対して内容を確認した上で署名　－自署名
    - 個人であれば、宣誓書への署名、同意書への署名
    - 医師の署名　－　カルテへの署名など
      - 医師という資格を持った人間が、その責任において文書に署名を施す。
      - 法令遵守などを示すためには、この署名文書が保存される必要がある
  - PKIで実現される機能としては **Authentication**がある。**Authentication**は署名で実現されるが**否認防止** (Non Repudiation) の**署名**との違いを理解が必要
- **Certification**と**Authentication**
  - 共に「認証」と訳されることが多いが。。違う概念
  - **Certification**
    - 証明書により何らかの権威者が何事かを証明する
    - 医療PKI(HPKI)の証明書により医師を証明する??
  - **Authentication**
    - 真正性の確認 (正当な本人であることを確認する)

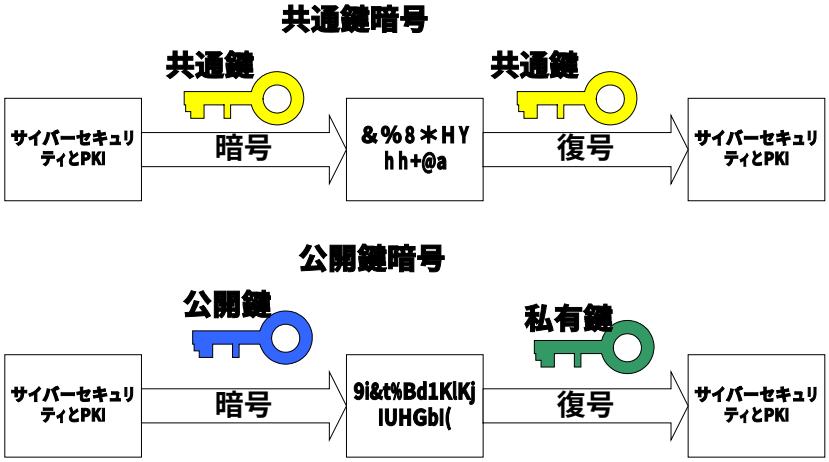
PKI技術の概要
基本的な用語の理解　その2

- 「**相互**」という言葉に要注意
  - 例：　GPKI（政府認証基盤）との**相互認証**
    - **Cross** Certification
    - 間違っても「**Mutual** Authentication」ではない
      - 双方向認証??
    - IPAでは、最近「横断認証」という言葉を使っている
  - **相互**運用　-　**interoperability**
- **Trust** という言葉が多用されるが。。。
  - Trustのニアンス
    - **信頼、信用**　　#Reliabilityの信頼ではない。IT技術者ほどこれを連想?
    - IPAでは、最近「信用点」「信用モデル」または「信頼関係モデル」という言葉を使っている
  - **信頼点**
    - Trust Point、Trust Anchor
- 信頼or信用(Trust)と認証(Certification)を理解することが重要

PKI技術の概要
基本的な用語の理解　その3

- 認証局(CA: Certificate Authority)
  - 認定局といった方がよいかもしれない。リアルな社会の証明書発行をイメージすればよい。リアルな社会で証明書を発行しえいる機関は?
- 証明書
  - リアル社会の証明書の例
    - パスポート　-　「日本国外務大臣」が発行者
    - 運転免許証、社員証、学生証、会員証　-　それぞれのAuthorityは??
    - 発行者の何らかの「印鑑」が押されている。
  - 電子証明書
    - 電子パスポート　-　発行者（日本国外務大臣??)により電子署名が施されている。
    - 運転免許証のICカード化　-　同じく電子署名が施される
- 参考
  - IPA宮川寧夫さんの「経営幹部にPKIを理解してもらうためには」
  - http://www.jnsa.org/seminar/2005/seminar_20051028/0miyakawa.pdf

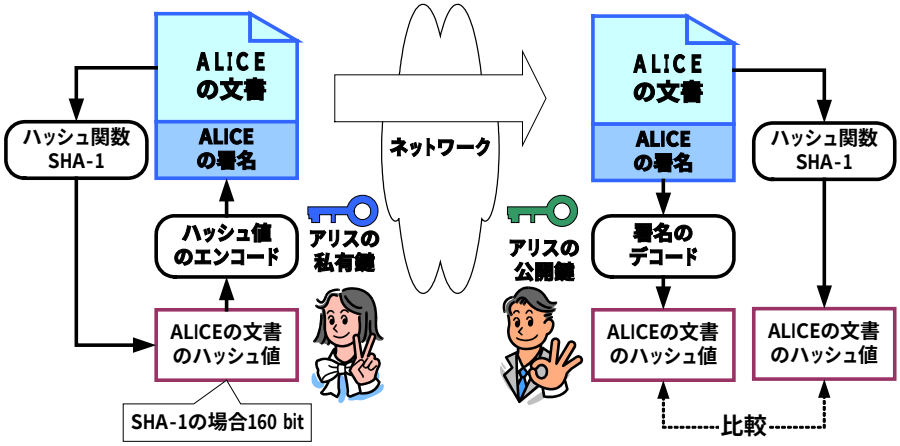
PKI技術の概要
共通鍵暗号と公開鍵暗号



公開鍵と私有鍵の組みは**鍵ペア**と呼ばれ、
その生成は、**鍵ペア生成**と呼ばれる。

7

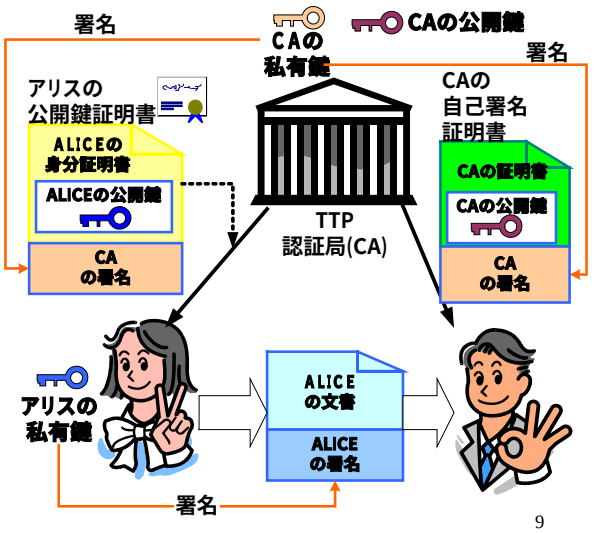
PKI技術の概要
署名の仕組み



8

PKI技術の概要
TTPよる署名（いかにアリスの公開鍵を信頼するか）

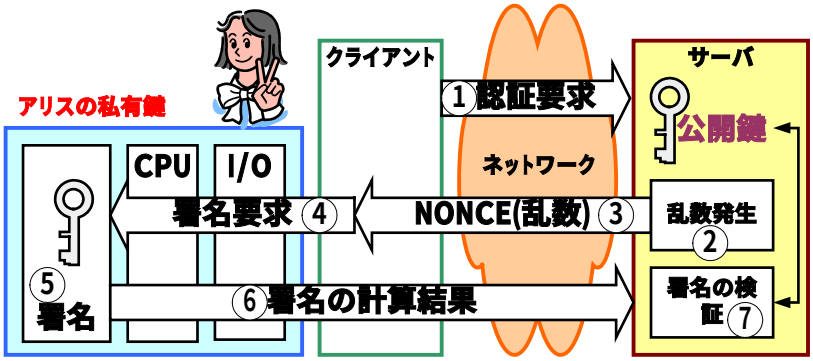
- TTP(Trusted Third Party)とは
  - 信頼できる第三者機関
  - TTPによって署名されたデータは信用できるものとする
  - 代表的な例はCA (Certificate Authority)
  - CAは印鑑証明を発行してくれる役所のイメージ
  - 公的個人認証サービスでは、都道府県CAが市民のための証明書を発行する。



9

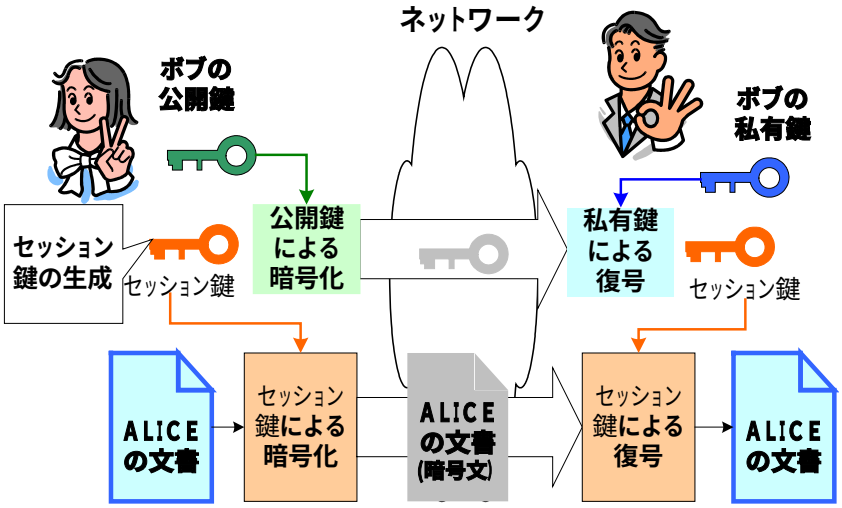
PKI技術の概要
PKIを用いた認証(Authentication)の例

- アリスの秘密情報（私有鍵）はハードウェアトークンから出ない
  - もちろんネットワークにも流れない
- アリスの秘密情報は、サーバには、格納されない
  - サーバは、アリスの秘密情報（例えばパスワード）を預かる必要がない
  - これは、アリスとっても、サーバの運用者にとってもメリット



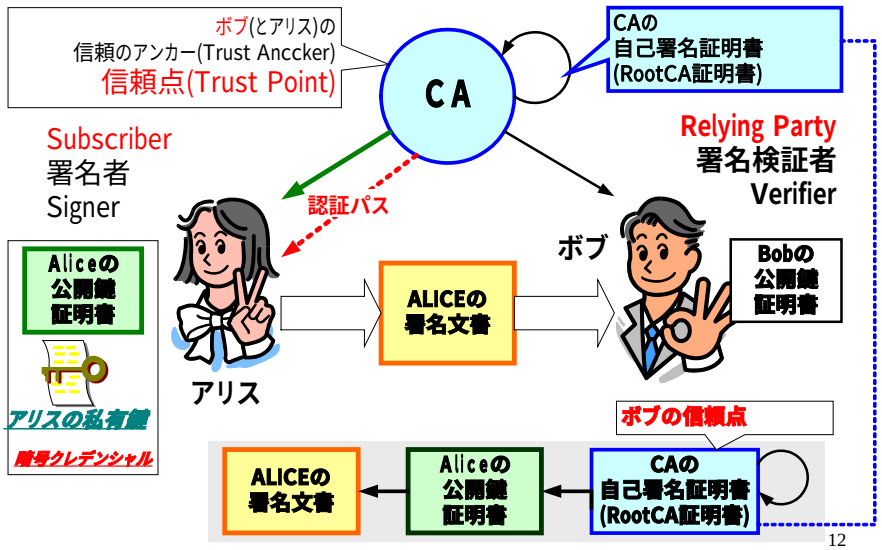
10

PKI技術の概要
PKIを用いた暗号の例（ハイブリッド暗号）



11

PKI技術の概要
PKIの基本的な信頼モデル



12

PKI技術の概要
X.509証明書

証明書バージョン番号 (V 3)
証明書シリアル番号
デジタル署名アルゴリズム識別子
発行者名の識別名
有効期間
主体者 (ユーザ) の識別名
主体者の公開鍵
　アルゴリズム識別子
　公開鍵値
V3の拡張
拡張フィールド(タイプ、フラグ、値)
拡張フィールド(タイプ、フラグ、値)
CAのデジタル署名
　アルゴリズム識別子
　署名

- 代表的な公開鍵証明書
  - 主体者(アリス)と、主体者(アリス)の公開鍵や、その他の属性をCA鍵(アリスの証明書を発行したCAの署名鍵)の署名でバインドする。
  - この時、主体者(アリス)の公開鍵に対応した私有鍵は、主体者(アリス)しか使用できないことが理想。
- 1997年版 X.509 3rd Edition
  - X.509v3証明書フォーマット
    - X.509V3証明書拡張
  - 14の標準拡張フィールド

PKI技術の概要
X.509証明書の例

Version: v3
　SerialNumber: 3a:1e:56:f9
　SignatureAlgorithm: sha1WithRSAEncryption
　Issuer: C=JP, O=ABC, OU=MedCA
　Validity:Not Before: Dec 7 13:30:00 GMT 2003 Not After: Dec 6 13:05:00 GMT 2004
　Subject: C=JP, O=ABC, OU=Person, CN=ALICE
　Subject Public Key Info:
　Public Key Algorithm: rsaEncryption
　　主体者の公開鍵値
Extensions:
　Certificate Policies: policyIdentifier: 1.2.3.4.3
Signature Algorithm: sha1WithRSAEncryption
　Signature Data:
　　CA鍵による署名

PKI技術の概要
ＣＲＬ（証明書失効リスト）

CRLバージョン番号（v2）
デジタル署名アルゴリズム識別子
発行者(CA)の識別名
今回の更新
次回の更新

証明書シリアル番号
失効日時
エントリ拡張(CRLv2の拡張)

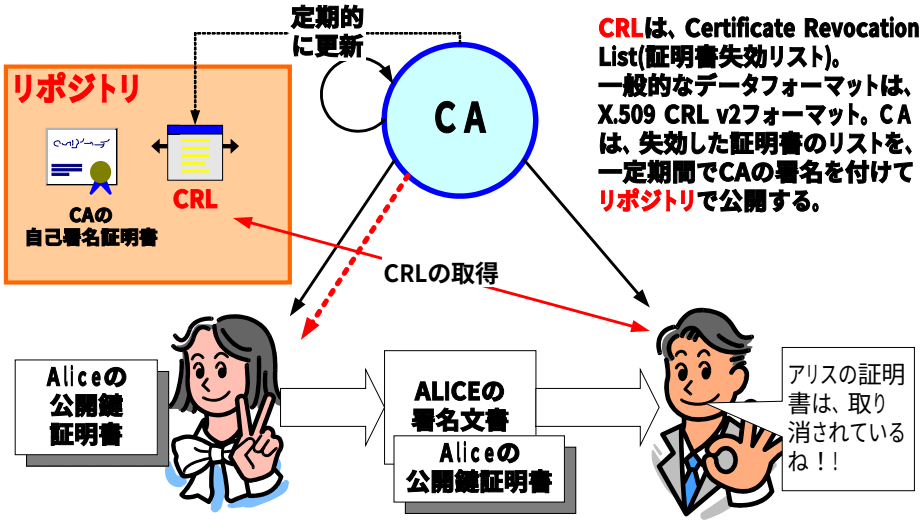
CRLv2の拡張
拡張フィールド(タイプ、フラグ、値)
拡張フィールド(タイプ、フラグ、値)

発行者（ＣＡ）のデジタル署名
アルゴリズム識別子
署名

- CRL
  - あるCAが発行した証明書の有効期限内に証明書を失効したい場合、このCRLに、失効したい証明書のシリアル番号を入れて*リポジトリ（LDAPサーバなど）*で公開する。
  - CRLは一定期間毎にCAの署名を付けて発行される。
- 1997年版 X.509 3rd Edition
  - CRLv2フォーマット
  - X.509v3証明書と同じく拡張がある

15

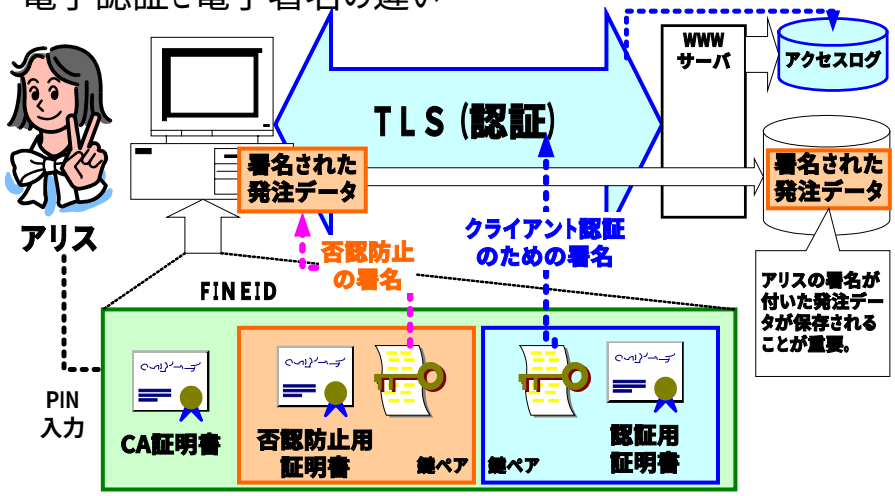
PKI技術の概要
証明書の失効



CRLは、Certificate Revocation List(証明書失効リスト)。
一般的なデータフォーマットは、X.509 CRL v2フォーマット。CAは、失効した証明書のリストを、一定期間でCAの署名を付けてリポジトリで公開する。

16

PKI技術の概要
電子認証と電子署名の違い



電子政府などでは、文書に署名され、署名された文書が保存されることが重要。欧州の市民カードは、2種類の証明書を使っている。

17

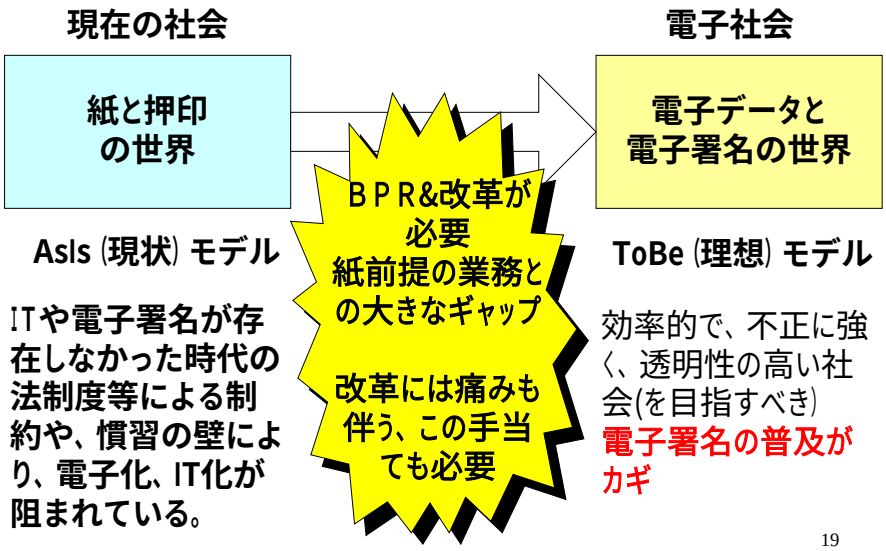
PKI技術の概要
電子認証と電子署名の違い

	電子認証(Authentication)	電子署名(Signature)
手段	現状は色々な認証のメカニズムが乱立しておりユーザからは差が分らない(クライテリアが未整備)	電子署名はPKI以外の現実的な手段はない
法制度	現状、法制度との結び付きはなく、認証のレベルもバラバラ	電子署名法、e文書法など法制度との結び付きが深い
マーケット	比較的新しい業界に需要がある。今後のユビキタスネットワーク時代のユーザ認証、機器認証の需要は測り知れない	紙に依存した比較的レガシーな業界に需要が多い。効率化するために電子化、IT化を推進したいが電子署名などの敷居の高さが壁になっている。
普及の鍵	普及には新しいビジネススキームの創造が重要	普及には業務知識、そして効率化のためのBPRが伴うことを理解する必要がある。
キーワード	ネットワーク上の安全、安心。ID管理、ID連携(Identity Federation)	e文書法対応、電子データ保存、電子契約。

同じPKIでも適用される業界、アプリケーションが大きく異なることが重要

18

PKI技術の概要
電子社会のToBeモデル



PKI技術の概要
PKIが安全であるための基本的な要件

- Subscriber側（アリス）の要件
  - セキュアな署名
    - なりすましをいかに防ぐか
    - 署名に使用する*私有鍵をいかに保護*するか??
    - セキュアなハードウェアトークン等が有効
- Relying Party側（ボブ）の要件
  - 署名検証、証明書検証をいかに行うか
    - まずは、検証者(ボブ)の**信頼点**が信頼できることが重要
    - リポジトリ(LDAPサーバ等)から必要な情報（CRLなど）を取得
    - ハードウェアトークン等に格納された**信頼点**の公開鍵からのリポジトリなどから読み出した情報を元に証明書チェーンを構築、そしてパス検証（**認証パスの検証**)を行う
- 認証局の要件
  - 認証局の運用
  - 証明書やCRLを署名する鍵の管理
  - 本人の確認方法　　Etc…

セコムIS研究所 Intelligent Systems Laboratory

インターネット上の信頼を確立するPKIの技術と運用

サブスクライバー/署名者

PKIにおける署名者の要件

アリスは、いかに自分の「鍵」を守るか？

サブスクライバー/署名者 Subscriber側（アリス）の要件

セコムIS研究所 Intelligent Systems Laboratory

- セキュアな署名
  - なりすましをいかに防ぐか
  - 署名に使用する**私有鍵をいかに保護**するか??
  - セキュアな**ハードウェアトークン**などが有効
- 私有鍵(Private Key)の保管場所
  - ハードウェアートークン
    - 耐タンパー性のあるハードウェアトークンに「鍵」を封じ込める
  - ローカルなハードディスク
    - 「鍵」をローカルなディスクに暗号化して保存
  - 外部のサーバ（ローミング）
    - 外部のサーバに「鍵(ローミング鍵)」を保管して使用時に取得する
- セキュアな署名装置のセキュリティ基準
  - 米国では、FIPS 140-2などの米国政府の調達基準
  - 欧州の電子署名では、SSCD (Secure signature creation device)としてその要件を定義

サブスクライバー/署名者
ハードウェアトークン（暗号トークン）とは??

- 主体者(アリス)の公開鍵に対応した私有鍵は、主体者(アリス)しか使用できないことが理想。
- そのためには、ハードウェアトークンの使用が有効になる。
  - ハードウェアトークンは、色々なPKIアプリケーションで使用できるべき
- ハードウェアトークン
  - 所有者を識別するための暗号クレデンシャル(Cryptographic Credential)を格納することが可能で、かつ携帯性のあるデバイス
- “**暗号クレデンシャル**(Cryptographic credentials)”ってなに?
  - 鍵と証明書（群）
- ハードウェアトークンの署名者認証
  - 通常はPIN
    - 所持による認証 + 記憶による認証
  - PINに代わる、バイオメトリクス情報
    - 生体情報をカード上にしか持たない方法でのバイオメトリクス認証が盛んに研究されている。

23

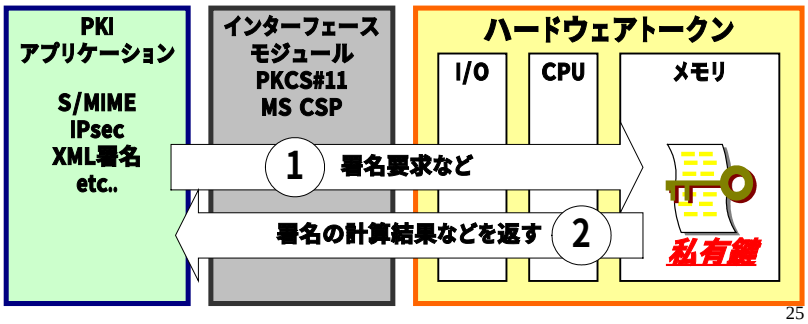
サブスクライバー/署名者
ハードウェアトークンの例

- スマートカード(ICカード)
- USB Token （Dongle）
- 生体認証と組み合わせたトークン
  - SonyのPuppy(FIU-810)など
    - http://www.sony.co.jp/Products/puppy/
- PCに内蔵されたセキュリティチップ
  - TCG（Trusted Computing Group）のTPM (Trusted Platform Module)
  - 正確にはハードウェアトークンではないかもしれないが機能的には類似
- MOPASS（ Mobile Passport ）
  - フラッシュメモリカード用のモバイルコマース拡張規格
  - SDカードなど
  - http://www.mopass.info/
- 携帯電話
  - ドコモのFOMAの証明書サービスFirstPass。携帯電話に内蔵されたUIM（User Identity Module）をパソコンから利用することも可能

24

サブスクライバー/署名者
なぜハードウェアトークン

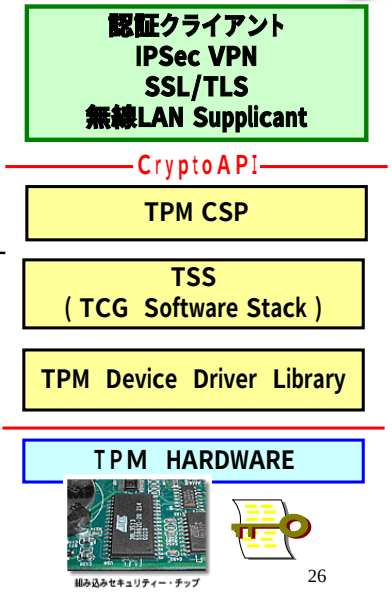
- 署名で使用する私有鍵(Private Key)を守る仕組みが可能
- 私有鍵のコピーを防ぐ。私有鍵がハードウェアートークンから外に出ない
- 私有鍵がハードウェアトークンのOSレベルで保護される
- ハードウェアトークンが盗難にあった場合を想定した耐タンパ性が重要
- PIN (Personal Identification Number)の入力や、指紋照合といった手段でハードウェアトークンにログインする。



25

サブスクライバー/署名者
TCG/TPM

- TCG(Trusted Computing Group)
  - 1999年に結成されたTCPA(Trusted Computing Platform Alliance)がTCGとして発展的に再構成
  - コンピュータデータのセキュリティを高めるための仕様を策定
- TPM (Trusted Platform Model)
  - マザーボードに組み込まれたPKI対応スマートカードのようなもの
- TPM搭載PC
  - ほとんどのPCメーカがTPM搭載のPCを出荷しつつある
- Windows VistaのTPMサポート
  - NGSCB (Next-Generation Secure Computing Base)
- プラットフォーム認証
  - TPMに格納された「鍵」を起点にからPCのOSの完全性を検証、更に構成を検証



26

セコムIS研究所 Intelligent Systems Laboratory

インターネット上の信頼を確立するPKIの技術と運用

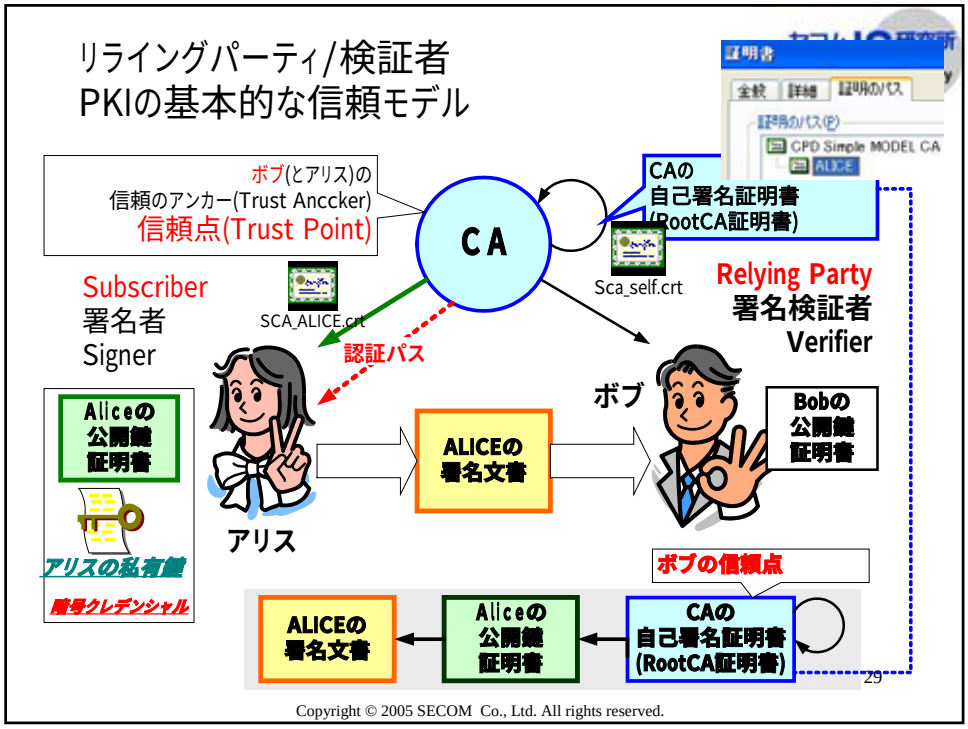
リライングパーティ/検証者

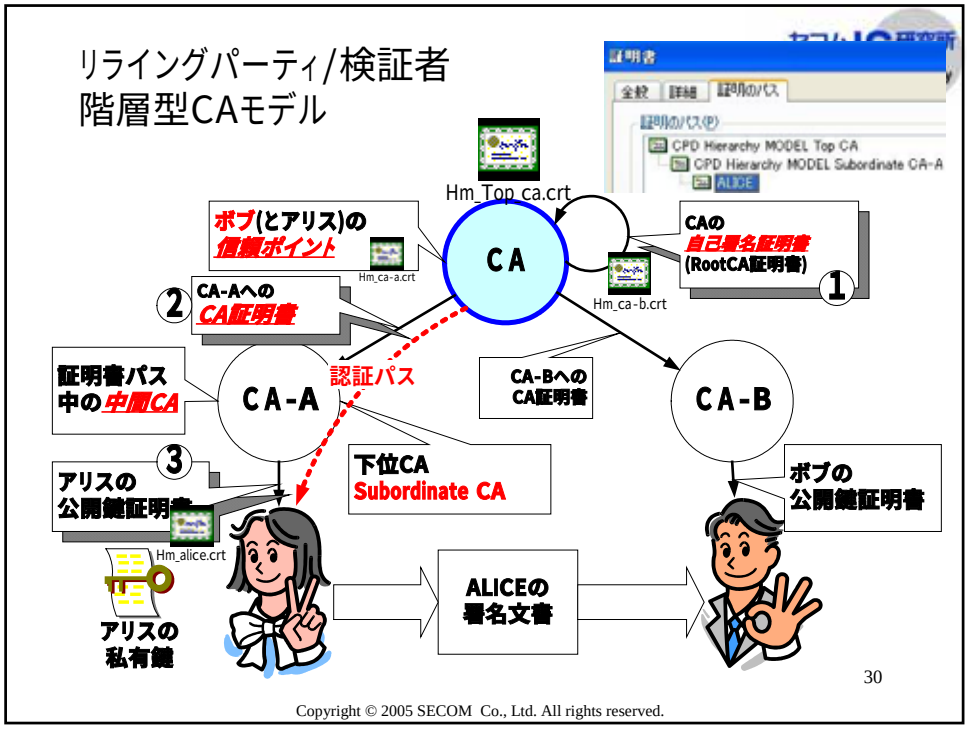
PIKの検証の考え方と、少し複雑なPKIの信頼モデルの説明。ボブは、いかにしてアリスの署名文書を信用することができるか？

セコムIS研究所 Intelligent Systems Laboratory

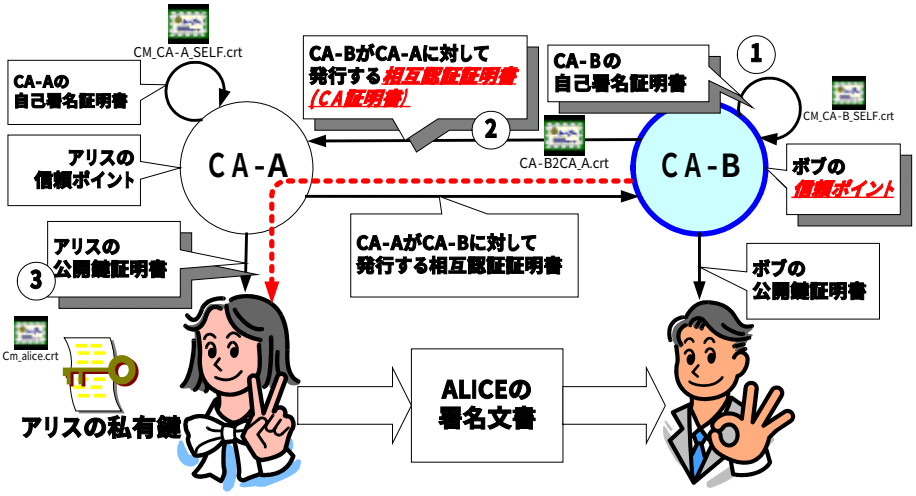
リライングパーティ/検証者 信頼モデルと証明書の検証

- Relying Party側（ボブ）の要件
  - 署名検証、証明書検証をいかに行うか
    - まずは、検証者(ボブ）の**信頼点**が信頼できることが重要
    - リポジトリ(LDAPサーバ等)から必要な情報（CRLなど）を取得
    - ハードウェアトークン等に格納された**信頼点**の公開鍵からのリポジトリなどから読み出した情報を元に証明書チェーンを構築、そしてパス検証（**認証パスの検証**)を行う
- **信頼モデル(Trust Model)**
  - CAが複数存在する場合(リアルな社会でもAuthorityは複数存在する）、CAがCAに対して証明書を発行することにより信頼関係を確立する。
    - #ここで「証明書と何か」ともう一度思い出す。。。
  - 「認証パスの検証」は、 CA証明書を含めた「信頼関係の連鎖」を検証する





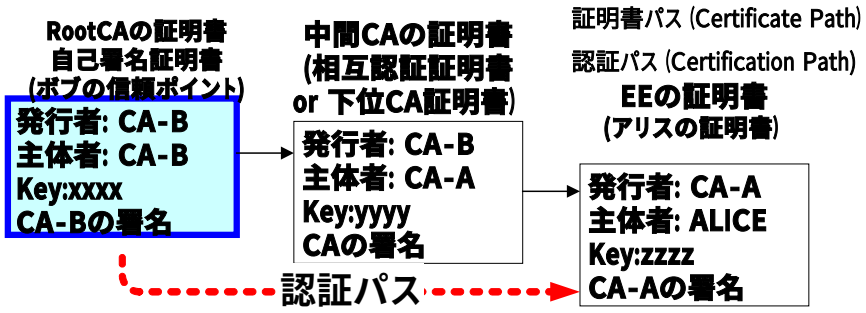
リライングパーティ/検証者
相互認証モデル（cross-certification model ）



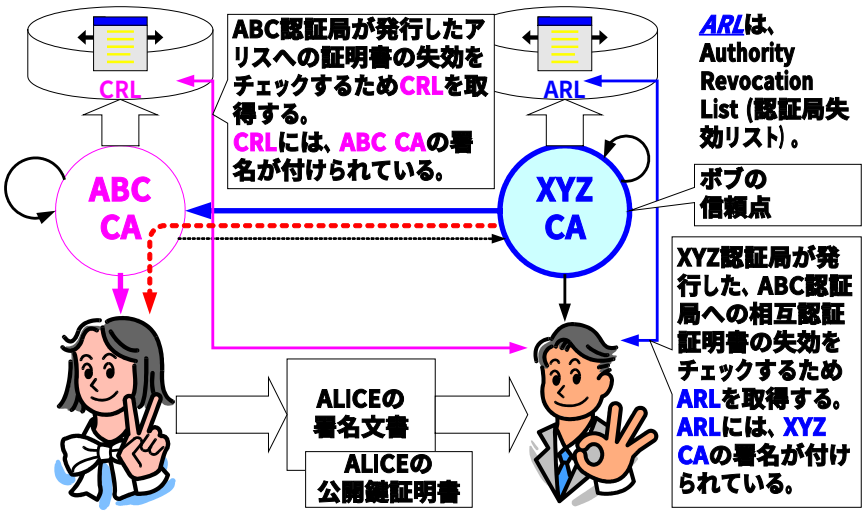
最近、IPAでは横断証明書という名称を使っている
http://www.ipa.go.jp/security/pki/083.html

リライングパーティ/検証者
認証パスとは何か？

- ボブ(RP)はアリス(SC)からのメッセージを受け取った。
- ボブは、アリスからのメッセージの署名を検証したい
- 自分(ボブ)の“*信頼点*”(ボブのRootCA)からの*認証パス*を検証する
- 検証は署名のチェーンの検証だけでなく、各証明書の失効チェック、そしてX.509証明書拡張に関する検証が行われる。

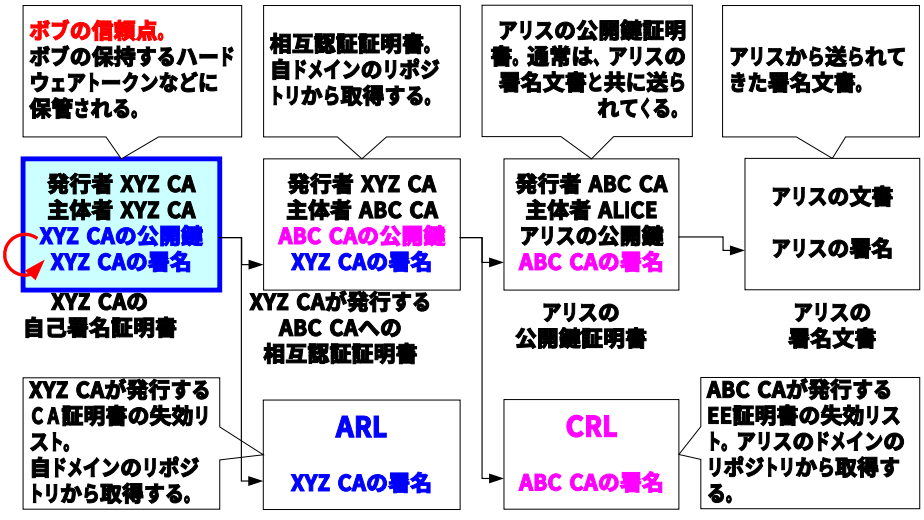


リライングパーティ/検証者
相互認証モデルでのCRL/ARLによる失効情報の取得



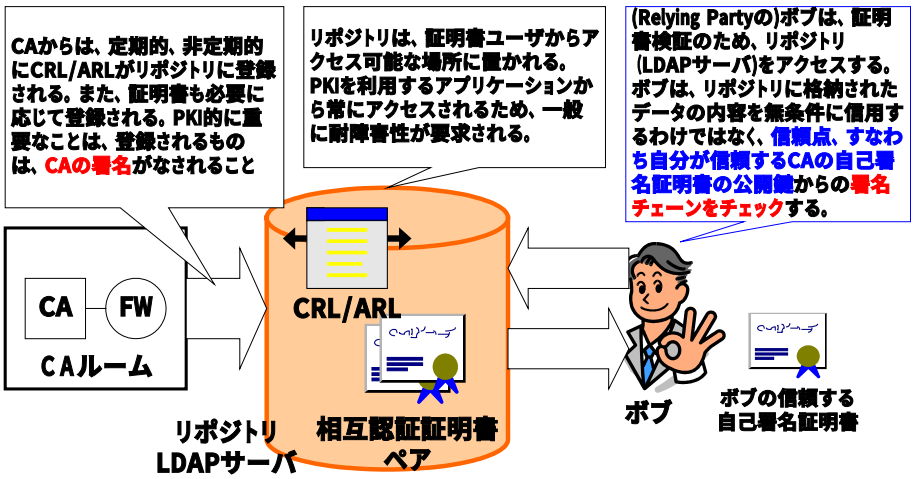
33

リライングパーティ/検証者
CRL/ARLと証明書検証



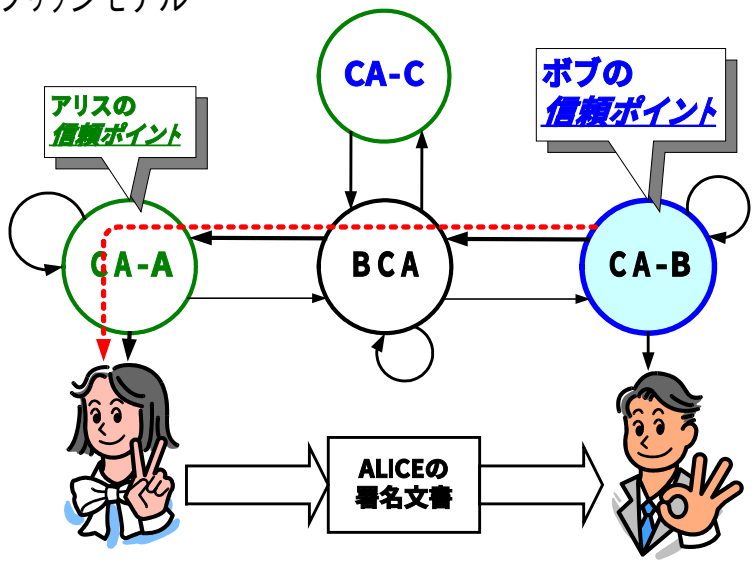
34

リライングパーティ/検証者
PKIにおけるリポジトリ



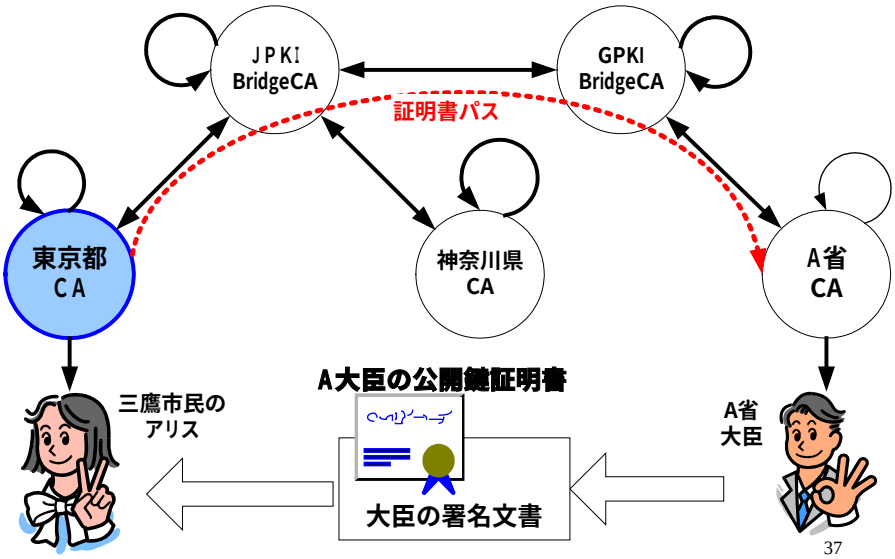
35

リライングパーティ/検証者
ブリッジモデル



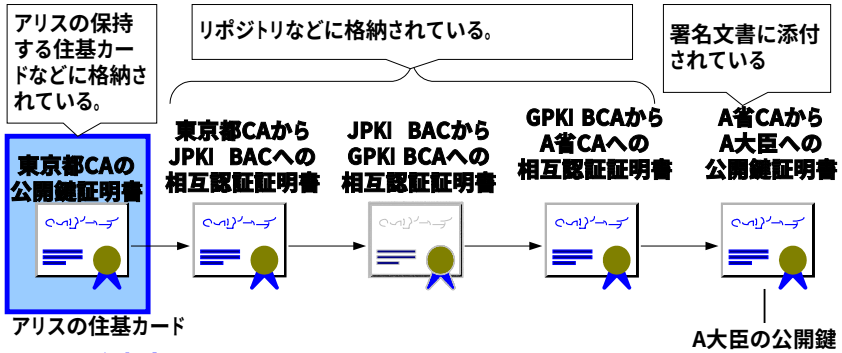
36

リライングパーティ/検証者
公的個人認証サービスにおける官職証明書の検証(1)



37

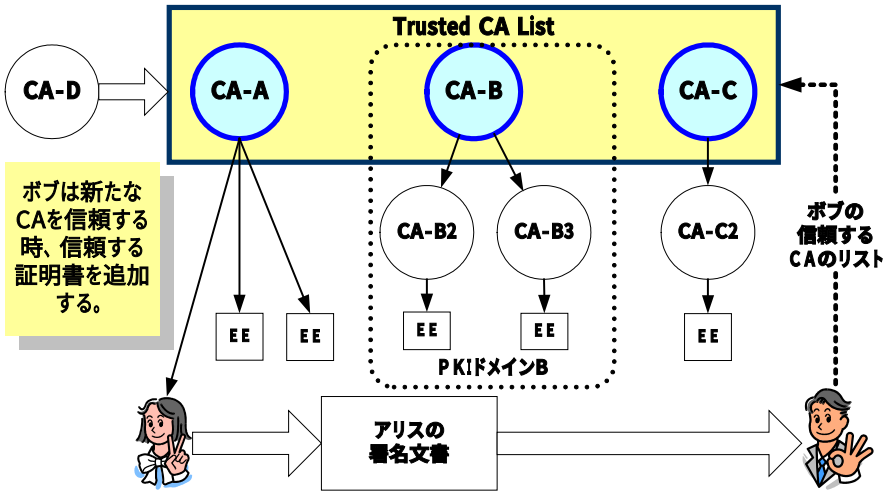
リライングパーティ/検証者
公的個人認証サービスにおける官職証明書の検証(2)



アリスの**信頼点**である東京都CAの公開鍵は、アリスに発行された公開鍵証明書や秘密鍵（私有鍵）と共に住基カードの公的個人認証サービス領域に格納される。
アリスは、この信頼点のみを信頼し証明書パスを検証し、次に、署名文書を検証する。JPKIの場合、（官職）証明書検証サーバが用意されており、実際の証明書検証はこのサーバで行うことができる。しかしこのサーバの応答の署名の検証は行う必要がある。

38

リライングパーティ/検証者
証明書信頼リストによる方法（Webモデル）



リライングパーティ/検証者
信頼点の問題

- 信頼点の問題
  - いわゆる「オレオレ証明書問題」も信頼点の問題のひとつ
  - PKIが「標準」「実装」「運用」の3要素から成り立っているとして問題だとされることの多くは信頼点の扱いであり信頼点の理解のなさが問題のある「実装」と「運用」を生んでいる。
- ではIEの証明書リストは信頼できるのか?
  - Trust file が在る世界：（例：web ブラウザの中）
    - 「これらの方々は，本人です．」と認定するリストがある世界
    - 「そのリストを作った方は，何様ですか？」
    - 「私も，そのリスト（ファイル）に載せてください．」
    - IPA宮川寧夫さんの「経営幹部にPKIを理解してもらうためには」より
    - http://www.jnsa.org/seminar/2005/seminar_20051028/0miyakawa.pdf
  - IEの証明書リストは、MSによるひとつの実装と運用の例に過ぎない(ある程度の信頼を提供しているに過ぎない)。またWebTrust for CA 監査認定を要求している「Microsoft ルート証明書プログラム」は後から決めたものに過ぎない。

セコムIS研究所 Intelligent Systems Laboratory

インターネット上の信頼を確立するPKIの技術と運用

認証局の信頼

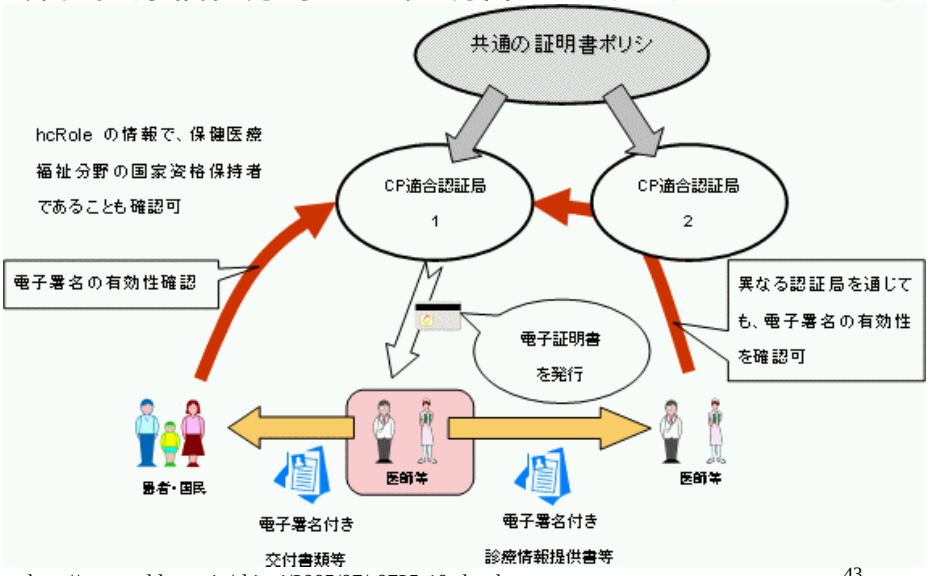
アリスとボブの証明書を発行する認証局の信頼はどうやって確保されるのか？

認証局の信頼 ＣＰとCPS

セコムIS研究所 Intelligent Systems Laboratory

- 証明書ポリシ(CP：Certificate Policy)とCPS(Certificate Practice Statement)
  - CPは、“何を(what)サポート”。CPSは、“どのよう(how)にサポート”
- 証明書ポリシ：CP (Certificate Policy)
  - 証明書には、用途がありそのことが記述される。
  - 一般的な証明書ポリシの内容
    - 認証局の発行者。署名者の義務。証明書の正しい用途や署名確認に関するリライングパティへの要求事項
  - CPに記述されたOIDが証明書に格納される
- 認証実施規定：CPS (Certification Practice Statement)
  - CPSはCPを実行するに当たって、どのような手順で (How) 行うのかを記述したものである。この中にはどのようなCAのシステムが使われているか、どのように運用されているかの詳細を記述する。

認証局の信頼
保健医療福祉分野PKIの証明書ポリシ（ＣＰ）



http://www.mhlw.go.jp/shingi/2005/07/s0725-10c.html

43

認証局の信頼
ＣＰ／ＣＰＳの記述構成　RFC 3647
インターネット X.509 PKI：証明書ポリシーと認証実施フレームワーク

RFC 3647に準拠したCP/CPS

1. はじめに
2. 公開とリポジトリーの責任
3. **識別と認証**
4. 証明書のライフサイクルに対する運用上の要件
5. 設備上、運営上、運用上の管理
6. **技術的セキュリティ管理**
7. 証明書と、証明書失効リスト及びOCSPのプロファイル
8. 準拠性監査とその他の評価
9. 他の業務上の問題及び法的問題

- RFC 3647
  - 2003年11月
  - http://www.ipa.go.jp/security/rfc/RFC3647JA.html
  - http://www.makino-law.jp/rfc2527-02/
    - 牧野弁護士事務所の若槻弁護士の翻訳。RFC 3647のドラフト時点の翻訳
  - 現時点ではRFC 3647の前バージョンであるRFC 2527に沿ったCP/CPSが多い。。

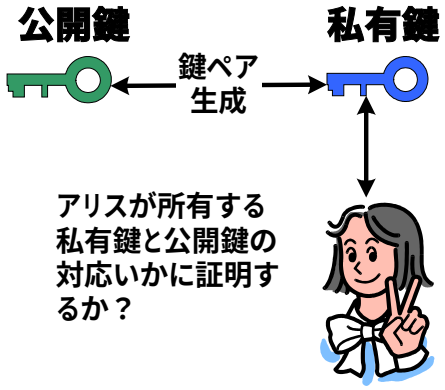
44

認証局の信頼

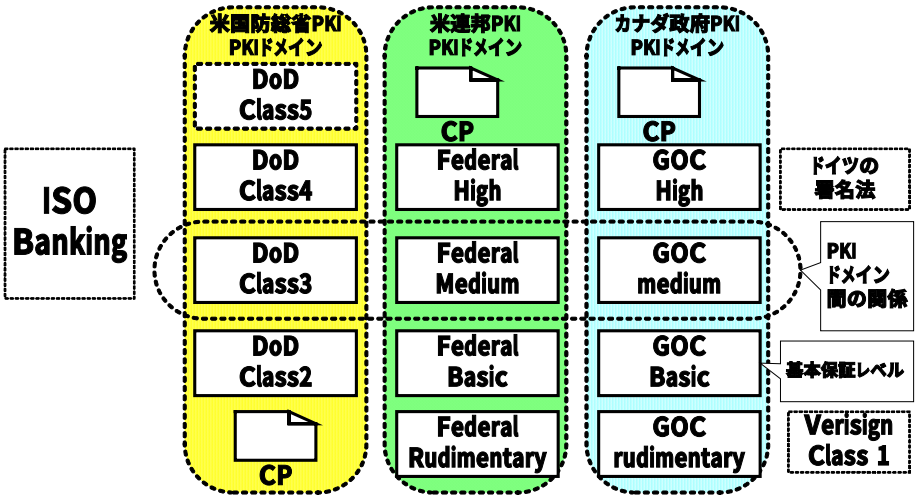
3章. 識別と認証 - IDENTIFICATION AND AUTHENTICATION

- ネーミングルール
  - 規約、解釈、ペンネームの可否. . .
  - ユニークであることの確保
- 識別、認証 (個人、組織)
  - 本人又は組織の真偽の確認
  - 例:各種の公的証明書
- 初期登録／更新／失効後
  - 要求方法・手続
  - 認証方法・手続
- RFC 3647 4.3. I&A (識別と認証)
  - http://www.ipa.go.jp/security/rfc/RFC3647JA.html#043

POP: proof-of-possession
所有の証明



認証局の信頼　- 3章. 識別と認証
証明書ポリシと保証レベルの例



US Federal PKIのCPの例

3. IDENTIFICATION AND AUTHENTICATION

3.1.9 Authentication of individual identity

保証レベル	Identification Requirements
Rudimentary	身元確認のために要求はない。申込者は、電子メール・アドレスを送ることによって、証明書を受け取るかもしれない
Basic	Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or comparison with trusted information in a data base of user-supplied information (obtained and/or checked electronically, through other trusted means (such as the U.S. mail), or in-person); or by attestation of a supervisor, or administrative or information security officer, or a person certified by a state or Federal Entity as being authorized to confirm identities.
Medium	Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)
High	申請者がR A に出向き、提出情報を法令に則って確認する。また、政府発行の写真付IDカード、または、ふたつの非政府発行のIDカード（ひとつは写真が必要、運転免許書など）で確認する。

出展 Federal PKI (FPKI) Policy Authority
http://www.cio.gov/fpkipa/policies.htm

47

認証局の信頼
6章 技術的セキュリティ管理

- 鍵ペア生成、鍵管理
  - CA、RA、リポジトリ、EEについて記載
  - 認証事業者側の鍵管理は最重要
  - 暗号モジュール、鍵長、Dual Control、鍵ライフサイクル管理. . .
  - CPとCPSを分けるなら. . .
    - EEの鍵管理→CP
- いわゆるコンピュータ／ネットワークセキュリティ
  - 認証業務システムの情報セキュリティ（C,I,A）
  - セキュリティ“管理”が実装されていること
- RFC 3647 4.6. 技術的セキュリティコントロール
  - http://www.ipa.go.jp/security/rfc/RFC3647JA.html#046

48

認証局の信頼
HSM(Hardware Security Modules)
セキュアなハードウェア鍵管理装置

- HSM　Hardware Security Modules
  - セキュアなハードウェア鍵管理装置
  - 鍵を守るための色々な仕組みを持つ
- FIPS 140-2
  - 米国標準技術院(NIST)によって1994年に策定された暗号モジュールの安全性に関する米国政府調達基準
  - FIPS 140-1と、見直された FIPS 140-2 (現在は FIPS 140-3 策定中)
  - 用途による複数のレベル　　Level 1　から　Level 4
  - FIPS 140-2 Level 2
    - 比較的簡易な認証局、サーバ、エンドユーザの鍵などの使用されている
  - FIPS 140-2 Level 3
    - 多くの商用の認証局で多く使用されている
- 電子署名法特定認証業務
  - FIPS 140 Level 3相当を要求

49

US Federal PKI　のCPの例
6.2　PRIVATE KEY PROTECTION
6.2.1　Standards for cryptographic module

Assurance Level	Certification Authority	Subscriber	Registration Authority
Rudimentary	FIPS 140-2 Level 1 (HW or SW)	N/A	FIPS 140-2 Level 1 (HW or SW)
Basic	FIPS 140-2 Level 2 (HW or SW)	FIPS 140-2 Level 1 (HW or SW)	FIPS 140-2 Level 1 (HW or SW)
Medium	FIPS 140-2 Level 2 (HW)	FIPS 140-2 Level 1 (HW or SW)	FIPS 140-2 Level 2 (HW)
High	FIPS 140-2 Level 3 (HW)	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (HW)

Federal PKI (FPKI) Policy Authority
http://www.cio.gov/fpkipa/policies.htm

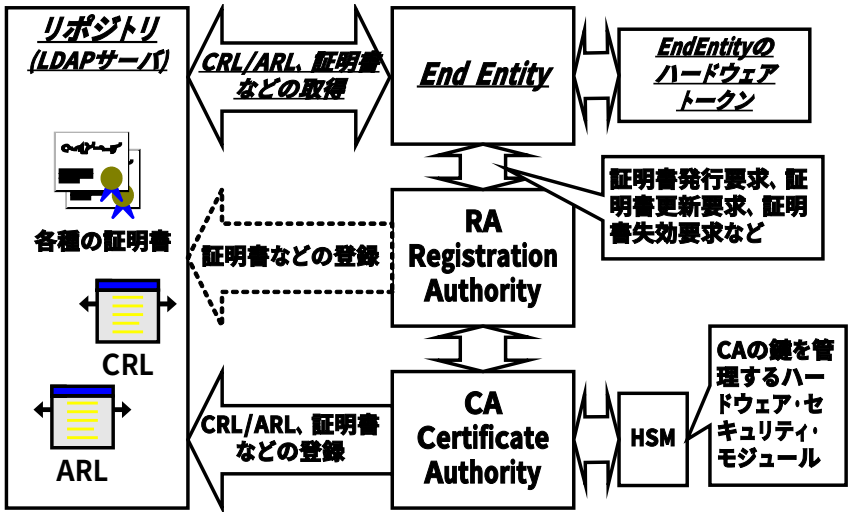
50

インターネット上の信頼を確立するPKIの技術と運用

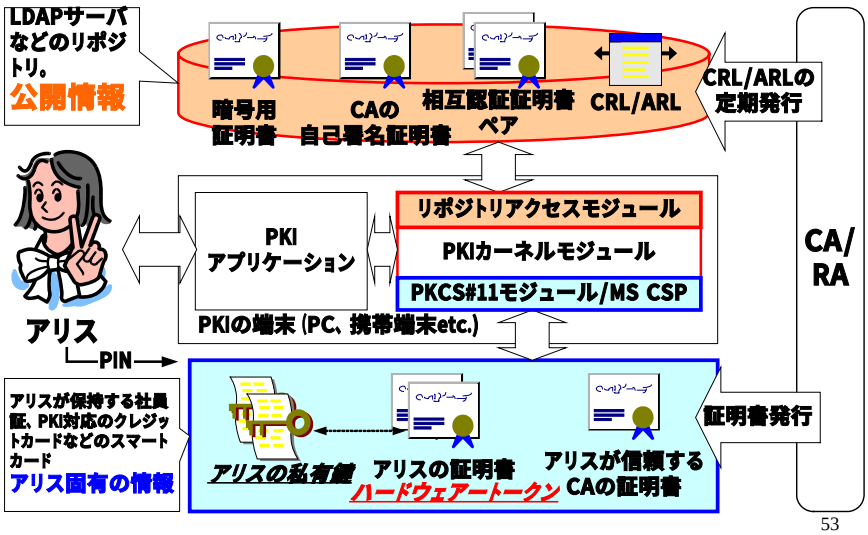
PKIの構成

ここまで説明したことを踏まえ、いくつか
の観点からPKIの構成を説明します

PKIの構成
PKIの基本コンポーネント

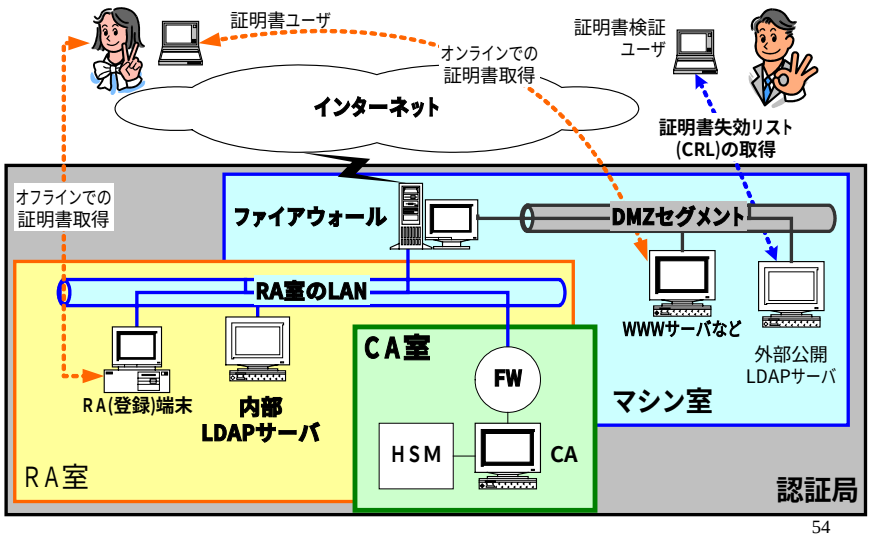


PKIの構成
PKIアプリケーションの構成例



53

認証局の信頼
認証局の構成例



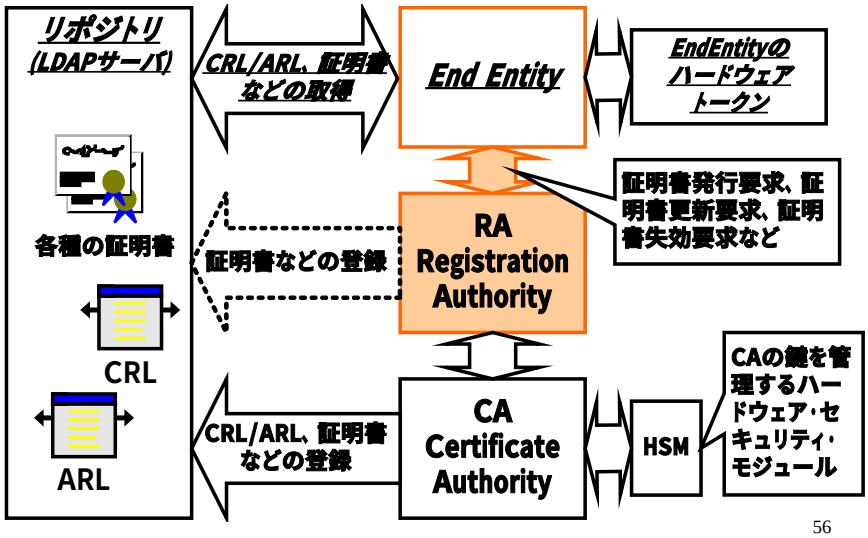
54

インターネット上の信頼を確立するPKIの技術と運用

証明書発行

アリスの証明書はどのようにして発行されるのか?

証明書発行
PKIの基本コンポーネントと証明書発行



証明書発行
証明書発行と証明書の管理

- 鍵ペアの生成
  - EE(End Entity)での生成とCA/RA側での生成
- 証明書の要求
  - PKCS#10などの証明書要求のフォーマット
- 証明書の配布
  - オンラインでの配布
    - PKIX-CMP, SCEPなど
  - オフラインでの配布
    - フロッピーディスクやICカード等による配布
    - PKCS#12, PKCS#7
- その他(証明書管理)
  - 証明書の失効、証明書の更新、証明書の再発行とリカバリ

証明書発行
X.509証明書

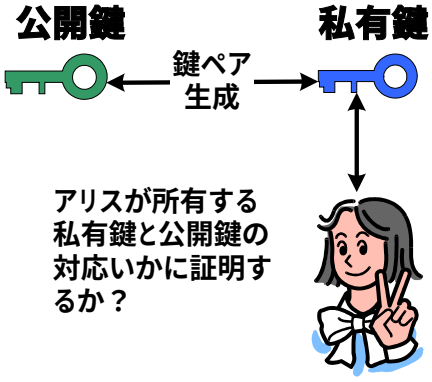
証明書バージョン番号 (V3)
証明書シリアル番号
デジタル署名アルゴリズム識別子
発行者名の識別名
有効期間
主体者 (ユーザ) の識別名
主体者の公開鍵
アルゴリズム識別子
公開鍵値
V3の拡張
拡張フィールド(タイプ、フラグ、値)
拡張フィールド(タイプ、フラグ、値)
CAのデジタル署名
アルゴリズム識別子
署名

- 代表的な公開鍵証明書
  - 主体者(アリス)と、主体者(アリス)の公開鍵や、その他の属性をCA鍵(アリスの証明書を発行したCAの署名鍵)の署名でバインドする。
  - この時、主体者(アリス)の公開鍵に対応した私有鍵は、主体者(アリス)しか使用できないことが理想。
- 1997年版 X.509 3rd Edition
  - X.509v3証明書フォーマット
    - X.509V3拡張
  - 14の標準拡張フィールド

証明書発行
CP/CPS　3章　識別と認証

- ネーミングルール
  - 規約、解釈、ペンネームの可否. . .
  - ユニークであることの確保
- 識別、認証（個人、組織）
  - 本人又は組織の真偽の確認
  - 例：各種の公的証明書
- 初期登録／更新／失効後
  - 要求方法・手続
  - 認証方法・手続

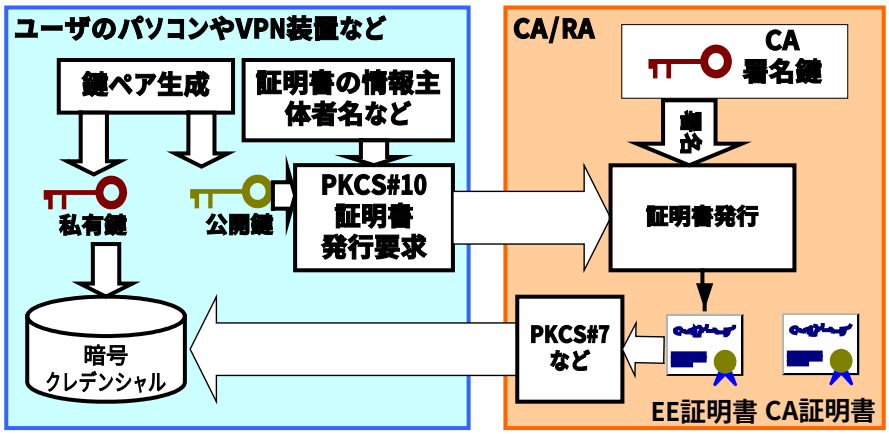
POP: proof-of-possession
所有の証明



証明書発行
鍵ペアの生成と証明書発行

- EE側での鍵ペアの生成
  - 鍵とPC上で生成
    - ハードウェアートークン内部での生成が理想的
  - PKCS#10などで証明書要求を生成
  - CAで証明書を発行
  - CAからPKCS#7などで証明書を配布
- CA/RA側での鍵ペアの生成
  - CAで鍵ペアを生成
  - PKCS#12などで私有鍵、証明書を配布
    - PINなどを別途配布（別経路が望ましい）
  - ハードウェアートークンなどに格納して発行
- NTT DoCoMo **FirstPass**の例 – FOMAのPKIサービス
  - FOMAカード(UIM：User Identity Module) に鍵ペアが出荷時に格納されている。証明書要求はオンラインで行なっている。
  - http://www.nttdocomo.co.jp/p_s/firstpass/

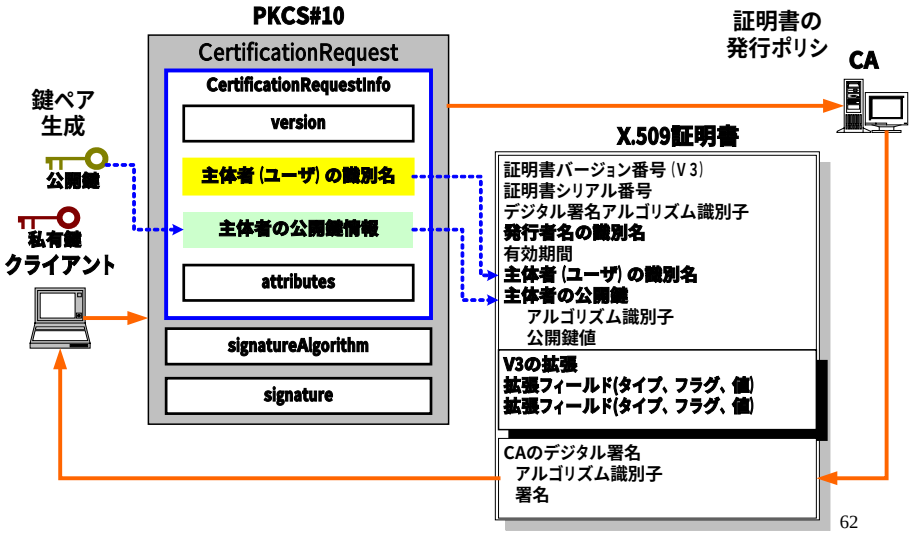
証明書発行
証明書発行 (EE側での鍵ペア生成)



人に証明書発行を行なう場合、耐タンパー性のある「ハードウェアートークン内部での鍵ペア生成が理想的。またVPN装置などの場合は、装置自体が耐タンパー性を持っていることが理想的。

61

証明書発行
PKCS#10による証明書発行要求



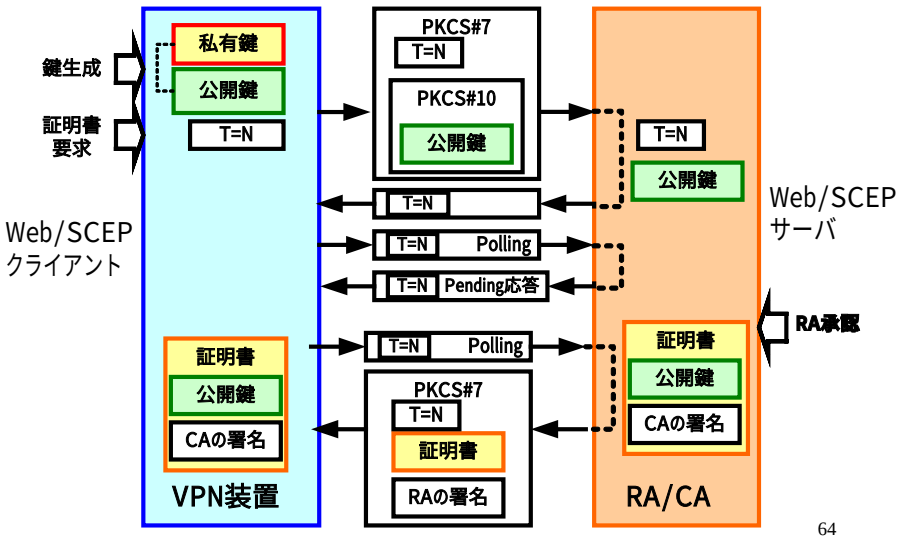
62

証明書発行
SCEP(SIMPLE Certificate Enrollment Protocol)

- SCEP
  - CISCOが仕様を作成。VPN装置などへの証明書発行が目的
  - http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm
- HTTPベース
  - SCEPデバイス側（VPN装置など)がHTTPのクライアトとして動作する
- メッセージに共通のデータ
  - メッセージには、トランザクションを一意に管理するためのTransaction IDが含まれる
- PKCS#10,PKCS#7などを使用した証明書要求
  - 通常の証明書要求であるPKCS#10をPKCS#7で暗号化して、他のメッセージも合わせて証明書要求メッセージを作っている
- 生成した証明書
  - PKCS#7でRAの署名がついてSCEPデバイスに返される

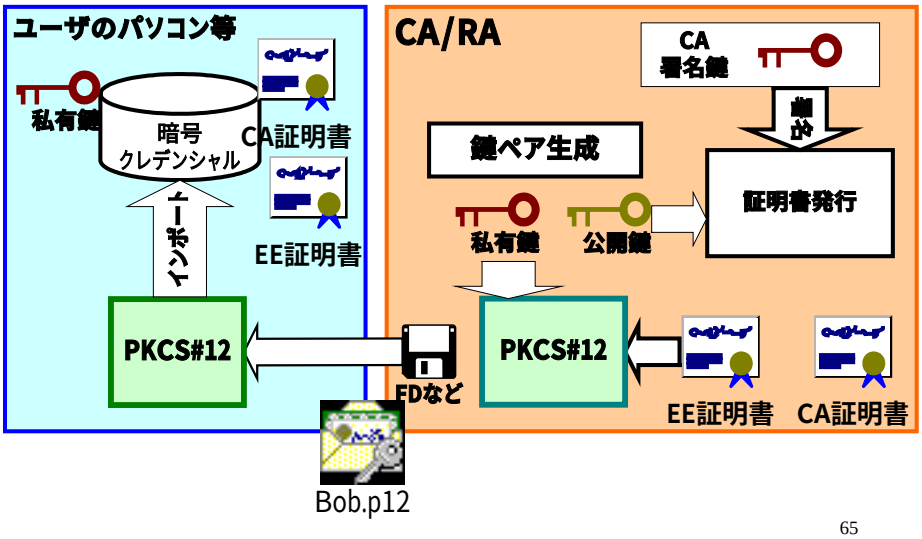
63

証明書発行
SCEPによるVPN装置への証明書発行



64

証明書発行
証明書発行（CA側の鍵ペア生成）



65

インターネット上の信頼を確立するPKIの技術と運用

電子署名法

2001年(平成12年)に施行された電子署名法

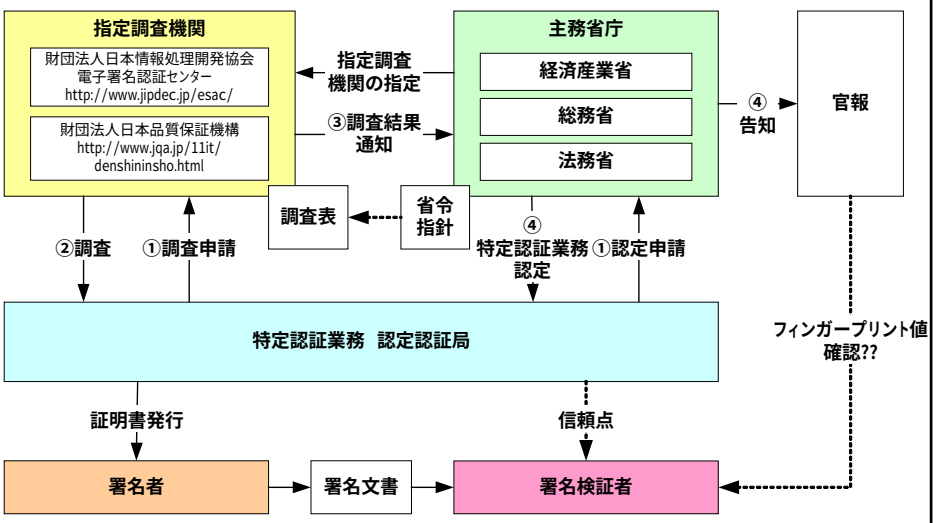
66

電子署名法

- 正式名称
  - 「電子署名及び認証業務に関する法律」
- 主な内容
  - 電磁的記録の真正な成立の推定
  - 認証業務に関する任意的認定制度の導入
    - 「特定認証業務」の認定 – 2005年10月時点で17件の認定
- 対象
  - 自然人の電子署名が対象
- 対象外
  - 法人、サーバ、エージェント。。。。の署名
  - 電子認証(Authentication)??、暗号
- 電子署名法の施行　2001年4月1日に施行　（来年で5年）
  - 政府は、この法律の施行後五年を経過した場合において、この**法律の施行の状況について検討を加え、その結果に基づいて必要な措置を講ずる**ものとする」(附 則　第三条)
    - 5年前、当初目指していた社会との齟齬はたくさんあるはず。

67

電子署名法
電子署名法特定認証業務認定のスキーム



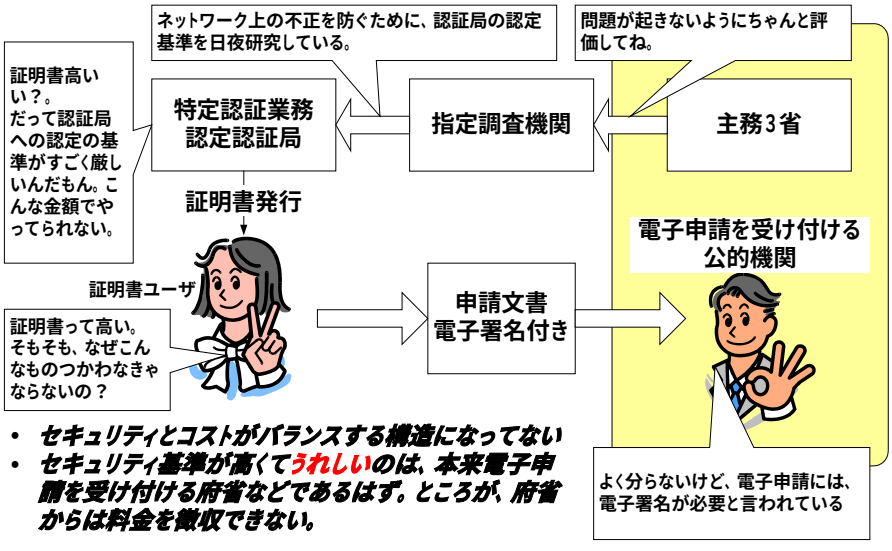
68

電子署名法
電子署名法特定認証業務認定制度の問題

- 非常に認定基準が厳しい
  - 結果、高コスト
  - 「認定基準が厳しい」ことは悪いことではない。問題は「認証事業者」以外がそのことを知らないこと。
- 非常に制約が厳しい　#技術の不理解が融通の利かない制度を作っている??
  - 結果、柔軟なPKIが構築できない
  - 自然人にしか証明書が発行できない
    - 「電子署名法」の範疇は、人と人の関係だけで、人と物、物と物の信頼関係を築けない。もしくは、人と物、物と物の信頼関係を分断しているかもしれない　-　いわゆる「オレオレ証明書」問題も関係あるかも。。。。
- 民間における電子署名法特定認証業務認定認証局の問題
  - 「非常に認定基準が厳しい」+「非常に制約が厳しい」=民間におけるビジネスの創造を阻害している可能性がある。現実に純粋に民間向けの認証局は少ないし減少傾向にある。これは本来の制度の目的を満たしていない。また、普及しないのであれば「制度」自体の意味をなさない

69

電子署名法
非常に認定基準が厳しい　- 結果、高コスト



- ***セキュリティとコストがバランスする構造になってない***
- ***セキュリティ基準が高くてうれしいのは、本来電子申請を受け付ける府省などであるはず。ところが、府省からは料金を徴収できない。***

**公的個人認証サービスは、証明書検証者からお金を取ってる。

70

電子署名法
電子署名法の課題とインターネット上の信頼

- 電子署名法の対象　ー　自然人の電子署名が対象
- 電子署名法の**対象外**
  - 法人、サーバ、エージェント、ネットワーク機器
  - 例えば、タイムスタンプは、**人（の意志）による電子署名**ではなく、（時刻監査などにより）時間が保証された**サーバによる電子署名**が施される。これは、同じ電子署名を使うが電子署名法の対象外
  - 電子認証(Authentication)??、暗号
- 問題は「電子署名法の対象外」ではなく「認定認証局への制約」
  - PKIは、証明書などの署名の連鎖により信頼関係を築く。しかし、「認定認証局」は、その制約から「電子署名法の対象外」との信頼関係を築けない。**このことは、ユビキタスネットワーク社会の様々なエンティティ間の信頼関係を築くために障害になるのではないか？**
- 電子署名法と特定認証業務認定制度の限界
  - ユビキタス・ネットワーク時代に求められるのは、人による電子署名だけではない　ー　電子署名法としては自然人は正しいかもしれないが。。。
  - 「電子署名法」の範疇は、人と人の関係だけで、人と物、物と物の信頼関係を築けない。もしくは、人と物、物と物の**信頼関係を分断**しているかもしれない

71

インターネット上の信頼を確立するPKIの技術と運用

PKIの信頼性

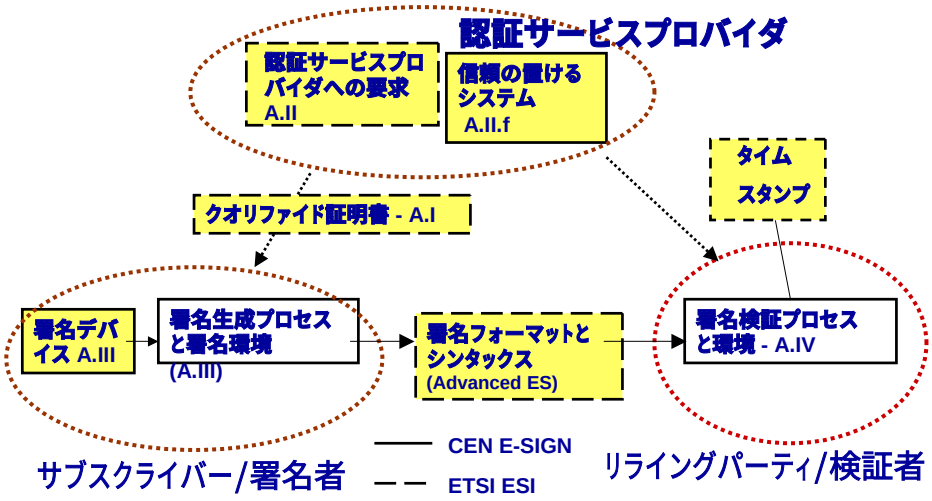
ＰＫＩは、本当に「信頼」を提供できるのか？
信頼やセキュリティを提供するための基準は本当にあるのか？

72

PKIの信頼性

- 暗号アルゴリズムの信頼性
  - 暗号アルゴリズムは十分な強度を持っているか??
- 暗号モジュールの信頼性
  - 暗号に用いる鍵は、十分に保護されているか？
    - 耐タンパー性、その他 - 認証局の鍵、署名者の鍵
- 署名者の安全性
  - 署名者の鍵は、十分に保護されているか??
- 署名検証者
  - 信頼点は十分に信用が置けるものか??
  - 署名検証、証明書検証のモジュールは十分に信頼のおけるものか??
- 認証局
  - 証明書の本人確認のポリシーとのポリシーの運用
  - 鍵の運用

PKIの信頼性
EESSIの認証フレームワーク



PKIの信頼性
関係する標準化、評価

項目	信頼性の要素	標準化、評価機関など
暗号アルゴリズムの信頼性	適切な暗号アルゴリズム、鍵長、耐用年数などの選択	CRYPTRECなど NIST、NESSIE
暗号モジュールの信頼性	評価基準	FIPS140-2
認証局	認証局のソフトウェア	ISO15408 PP
	CP/CPSのフレームワーク	RFC 3647
	認証局の認定制度	Webtrust for CA、 電子署名法特定認証業務認定
署名者の安全性	チップのセキュリティ評価	ISO15408 PP, FIPS140-2
	カードOSの評価	ISO15408 PP, FIPS140-2
	署名ソフトウェアの評価	ISO15408 PP, FIPS140-2
署名検証者	パス検証のアルゴリズム	RFC 3280
	パス検証ソフトウェアの評価	ISO 15408 PP (NIST PP draft)

インターネット上の信頼を確立するPKIの技術と運用

参考

どういった資料が参考になるか？

参考
参考図書

- PKI　公開鍵インフラストラクチャの概念、標準、展開
  - C・アダムズ、S・ロイド 著、鈴木 優一 訳
  - 2000年7月15日 初版第1刷発行
  - 出版社 ピアソン・エデュケーション
  - ISBN4-89471-248-2
  - #ちゃんと勉強したい人にお薦め
- PKI と電子社会のセキュリティ
  - 青木隆一・稲田　龍　著　　村井　純　監修
  - 発行年月日2001/10/25
  - 出版社　共立出版
  - ISBN4-320-12028-0
- 改訂　PKIハンドブック
  - 小松　文子　他 著
  - 出版社：SRC、260ページ
  - ＩＳＢＮ：4-88373-205-3

77

参考
インターネット上のリソース

- PKI 関連技術解説
  - http://www.ipa.go.jp/security/pki/
  - IPAの報告書で比較的初心者向き
- セコムIS研究所　サイバーセキュリティ読本
  - http://www.secom.co.jp/isl/j/cs_reader/index.html
  - http://www.secom.co.jp/isl/j/cs_reader/pki/index.html
- Internet WeekのPKIチュートリアル(富士ゼロックス　稲田、セコム　松本)
  - 2004年
    - http://www.soi.wide.ad.jp/class/20040031/slides/29/
  - 2003年
    - http://www.soi.wide.ad.jp/class/20030038/slides/43/
  - 2002年
    - http://www.soi.wide.ad.jp/class/20020036/slides/25/

78