Identrusとe-Japan（電子政府）のPKI技術

NPO 日本ネットワークセキュリティ協会
／セコムトラストネット株式会社
松本　泰
yas-matsumoto@secomtrust.net

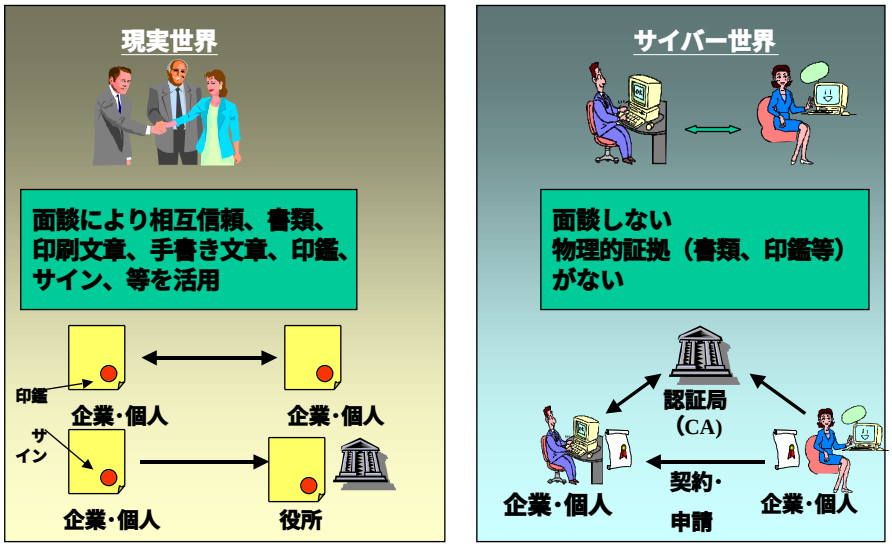
2002 年　11 月　15日

Identrusとe-Japan（電子政府）のPKI技術

- 電子社会へのパラダイムシフト
  - 政府認証基盤 (GPKI）やIdentrusに代表される認証基盤の動向
- GPKI, Identrusで要求されるPKI技術
  - PKIの信頼モデルなど
    - 階層モデルから、ブリッジモデル
- PKI相互運用技術の動向
  - GPKIやIdentrusで要求されるマルチベンダ PKI、マルチドメインPKIの鍵となるPKI相互運用技術
  - NPO JNSAのPKI相互運用技術プロジェクト
    - Challenge 2001、Challenge 2002

電子社会へのパラダイムシフト

現実世界とサイバー世界での確認比較



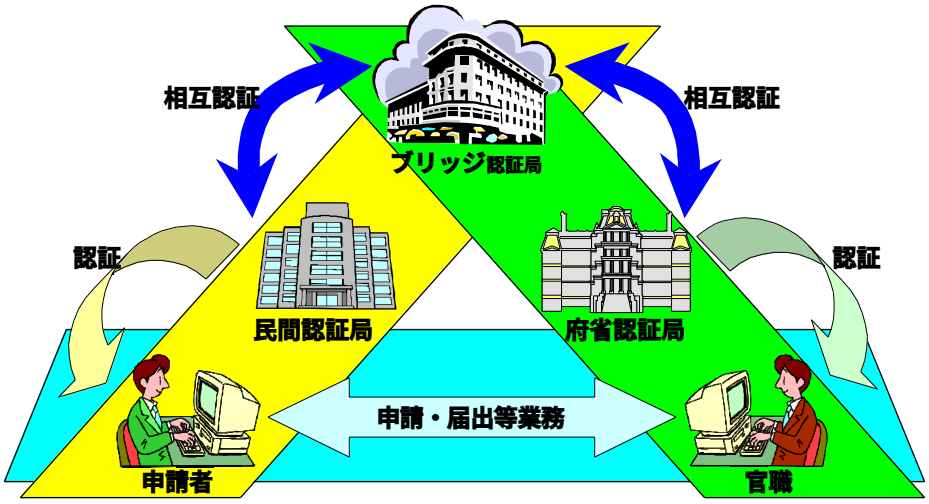
電子社会へのパラダイムシフト

電子政府とIndentrus

- 電子政府と政府認証基盤(GPKI)
  - _ 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
  - _ 全世界的な銀行を中心としたBtoBの認証基盤
  - _ 日本の４大メガバンクも参加
- GPKI、Identusなど要件
  - _ 世界で通用するセキィリティ
    - ・ファシリティ、運用、監査、PKI相互運用技術

電子社会へのパラダイムシフト

政府認証基盤ＧＰＫＩの概略



電子社会へのパラダイムシフト

政府認証基盤ＧＰＫＩの目的

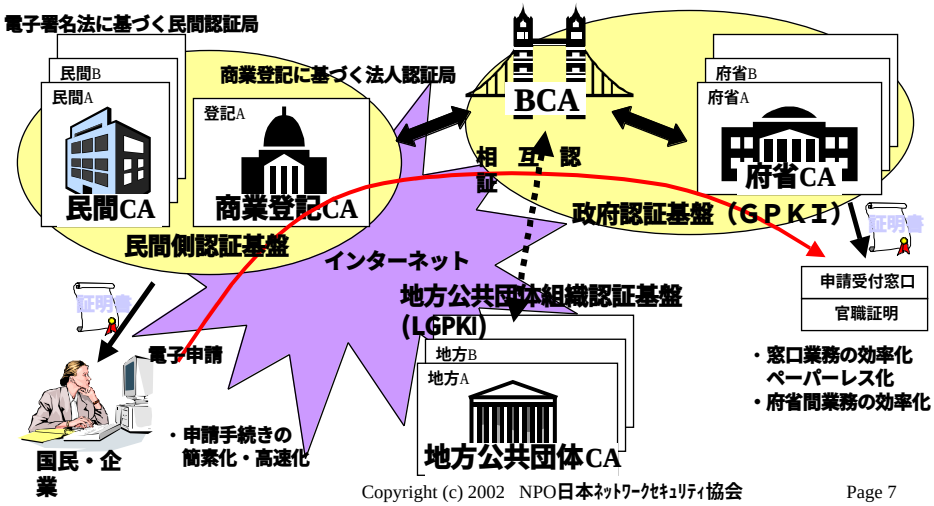
申請・届出等のオンライン化

- **オンライン化することによる脅威**
  - **申請者、処分権限者のなりすまし**
  - **通信時の盗聴**
  - **文書の改ざん**
  - **等**
- **脅威から守るためには**
  - **本人確認**
  - **データの暗号化**
  - **データの完全性**
  - **等　が必要となる**

この防衛手段を実現可能にするための仕組みが
GPKI（Government Public Key Infrastructure）

電子社会へのパラダイムシフト

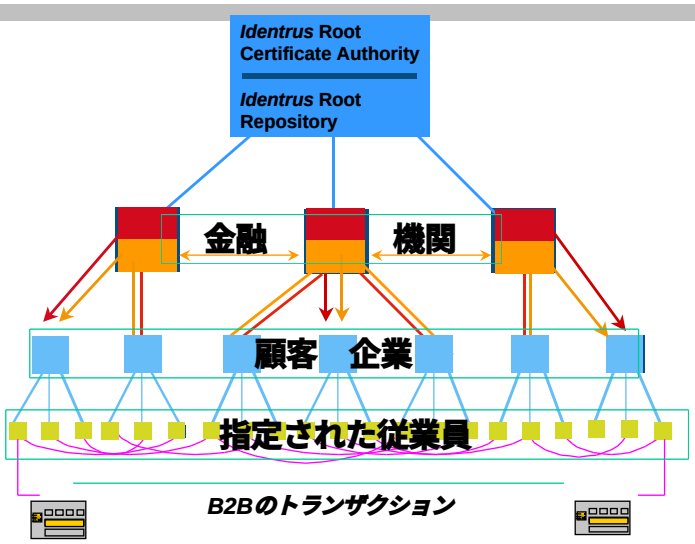
政府認証基盤ＧＰＫＩとその周辺



 Page 7

電子社会へのパラダイムシフト

Identrusのビジネスモデル－階層構造

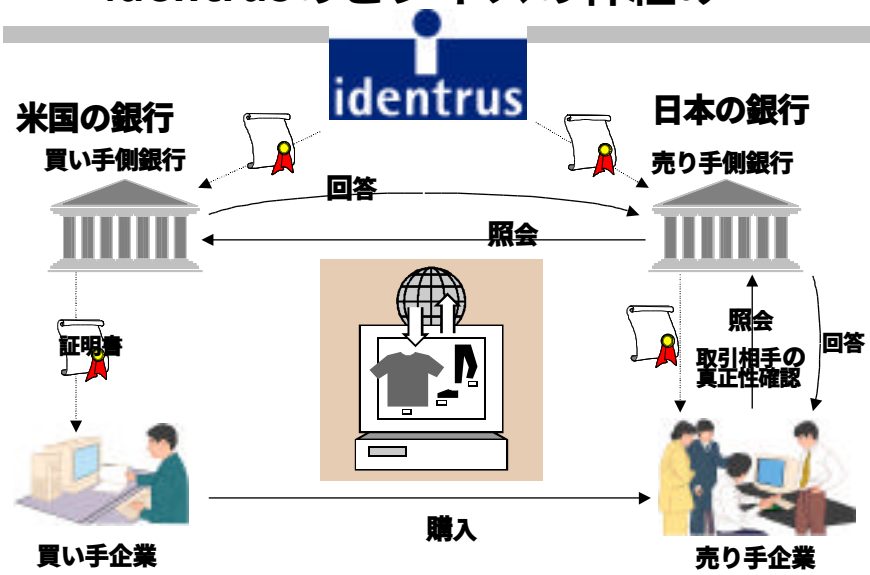


 Page 8

電子社会へのパラダイムシフト

Identrusのビジネスの枠組み

JNSA



 Page 9

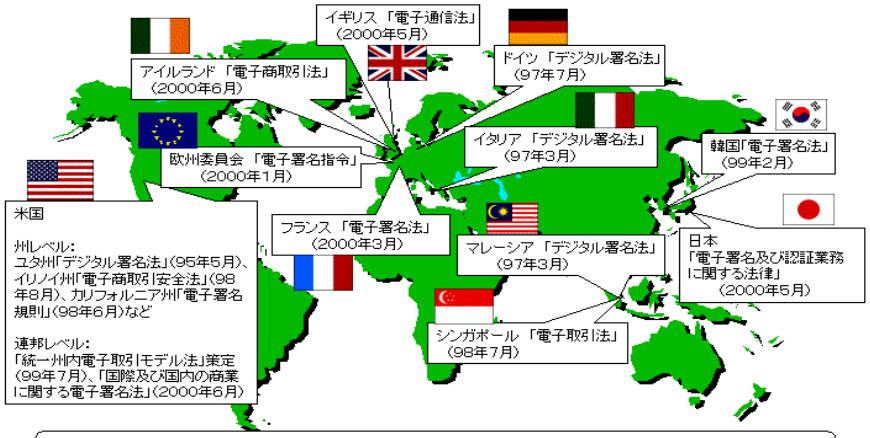
電子社会へのパラダイムシフト

■諸外国の法制度整備の動向

JNSA

諸外国の法制度整備の動向

世界各国において、電子署名／電子認証に関する法制度を策定または検討中

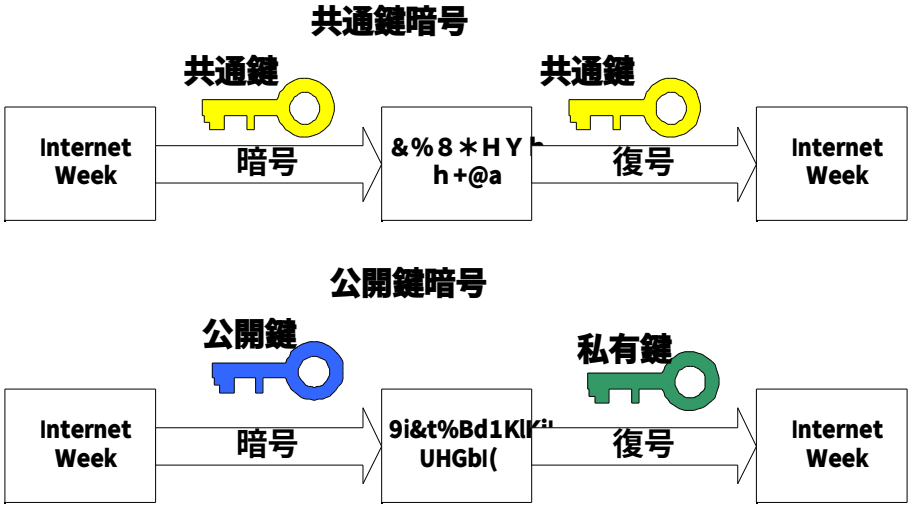


＜国際機関における検討＞
UNCITRAL(国連国際商取引法委員会):「電子商取引モデル法」(96年12月)、「電子署名に関する統一規則草案」(検討中)

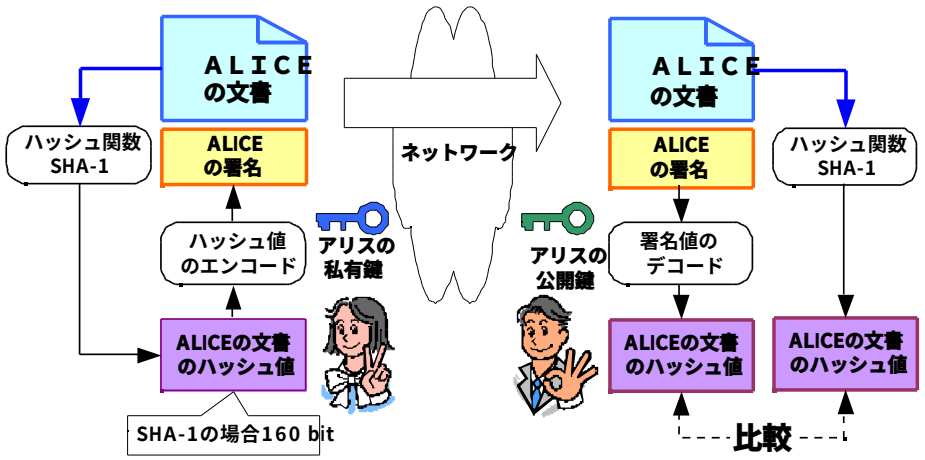
 Page 10

出典：政府委員会資料を参考に作成

共通鍵暗号と公開鍵暗号



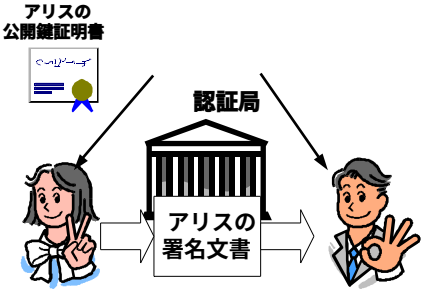
署名の仕組み



TTPよる認証 （アリスの公開鍵を信じるのか）

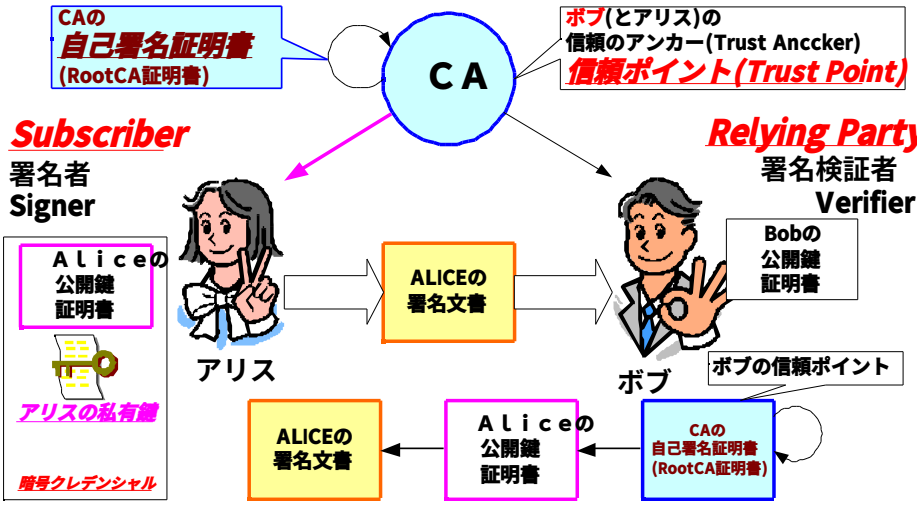
JNSA

- 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



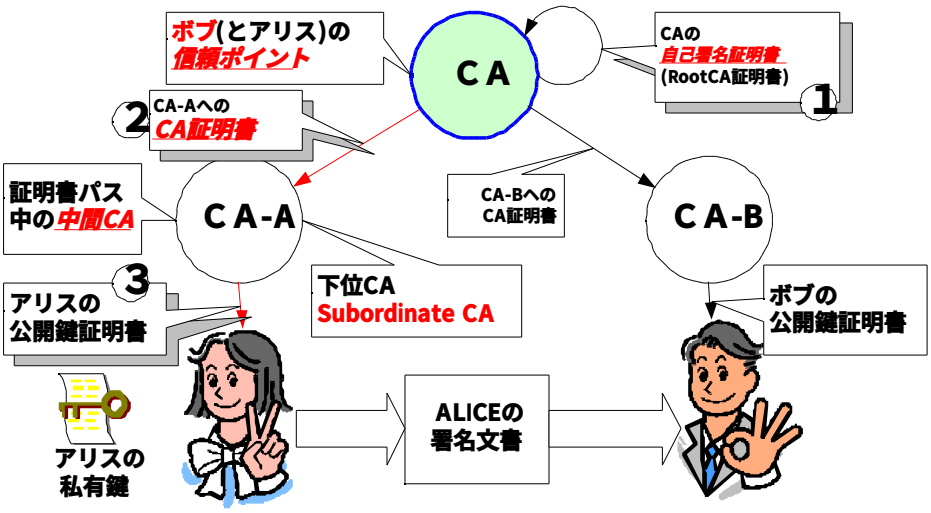
PKIの基本的な信頼モデル

JNSA



PKIの技術

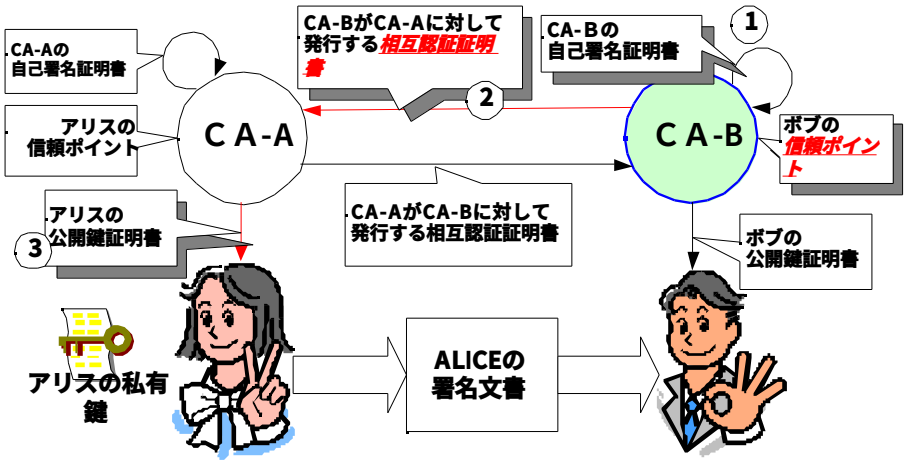
階層型CAモデル



 Page 15

PKIの技術

相互認証モデル（Cross certificate）



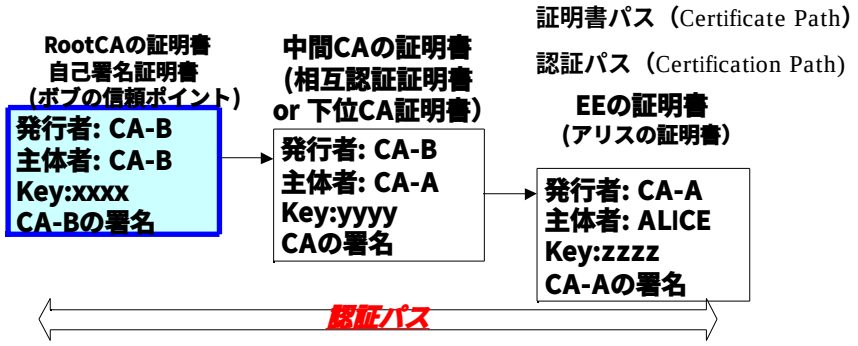
 Page 16

PKIの技術

認証パスとは何か？

JNSA

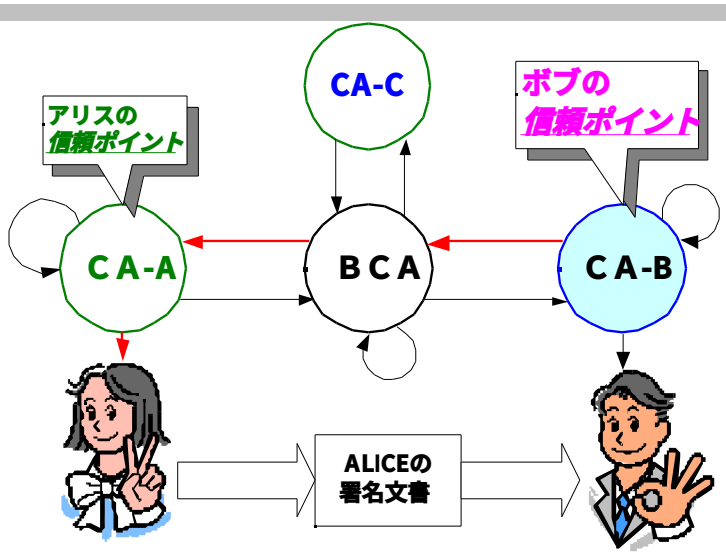
・ボブ(RP)はアリス(SC)からのメッセージを受け取った。
・ボブは、アリスからのメッセージの署名を検証したい
・自分(ボブ)の“信頼のポイント”(ボブのRootCA)からの認証パスを検証する



PKIの技術

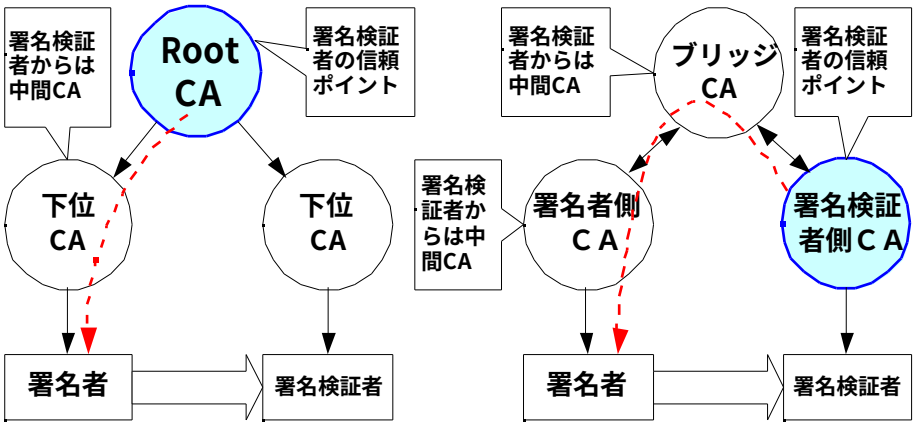
ブリッジモデル

JNSA



PKIの技術

階層モデルとブリッジモデルの認証パス



RFC3280などに記述されている認証パス検証は、信頼モデルに依存しない。しかし、ブリッジモデルでは、その性格から、 RFC3280の仕様の多くの部分の実装が要求され、高度なPKI相互運用技術が要求される。

 Page 19

PKIの技術

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

*** GPKIなどでは、X.509v3証明書フォーマットが使用されており、かつ拡張が、重要な意味を持つ。**

 Page 20

PKIの技術

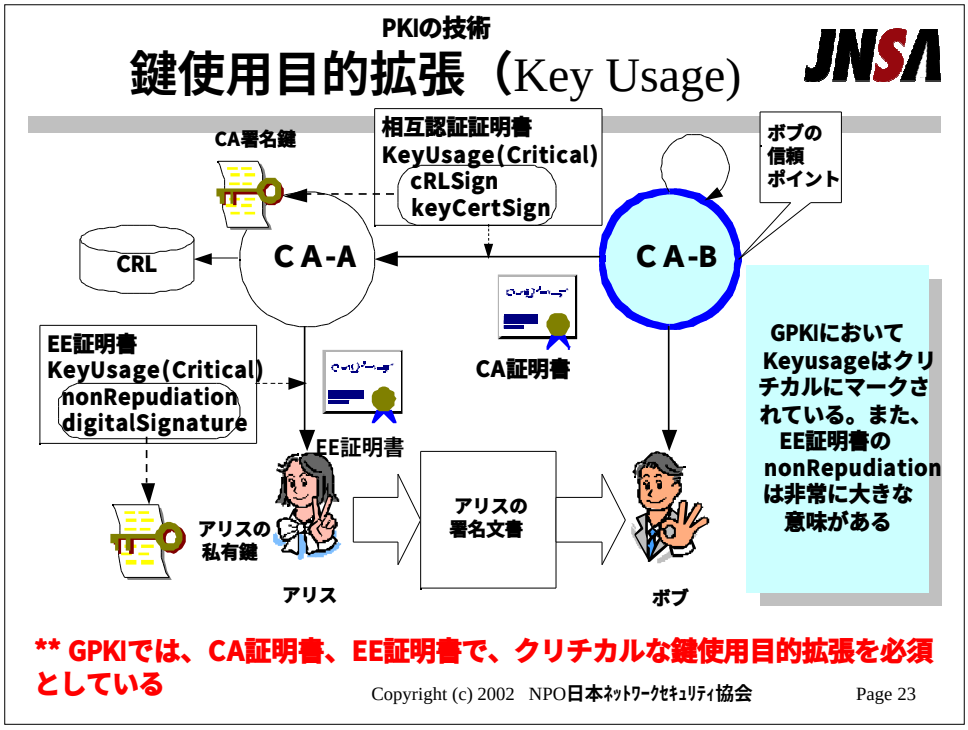
X.509証明書拡張(v3拡張)

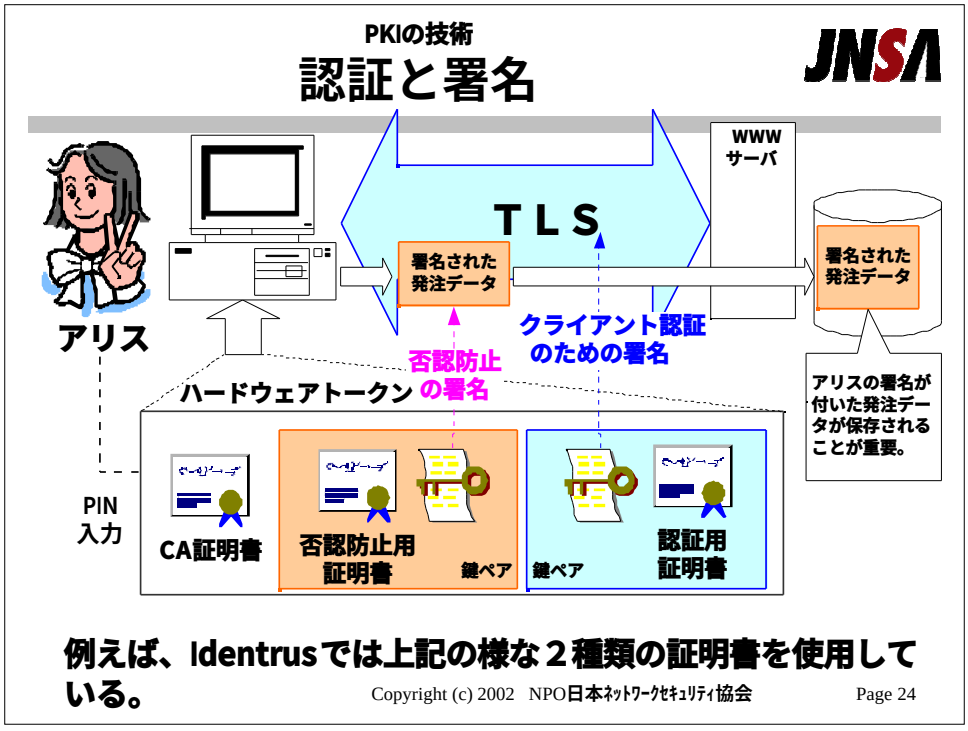
No	標準拡張(X.509v3)	説明
1	発行者鍵識別子	発行者の鍵の識別に使用されCA鍵の更新に必要
2	主体者鍵識別子	主体者の鍵の識別に使用されCA鍵の更新に必要
3	***鍵使用方法***	私有鍵の使用方法。例えば署名用鍵で、暗号化を禁止する
4	私有鍵有効期間	証明書の有効期間に対して、私有鍵の有効期間。
5	***証明書ポリシ***	証明書ポリシIDなどが格納される。ポリシによる制御などに使
6	***ポリシマッピング***	信頼ドメイン間のポリシのマッピングを行う
7	主体者別名	主体者の別名が格納される。例えばVPN装置の場合のIPaddres
8	発行者別名	発行者の別名が格納される。
9	主体者ディレクトリ属性	証明書の主体者のためのディレクトリ属性
10	***基本制約***	証明書の種類(CAorEE)。CAだった場合パス数の制限
11	名前制約	CA証明書で、相手のCAが発行する名前による制約
12	ポリシ制約	CA証明書で、相手のCAが発行するポリシ関係制約
13	拡張鍵使用方法	"鍵使用方法"以外の鍵使用方法のOIDが格納される。
14	CRL配布点	失効情報リストの配布点のDNやURLが格納される。

PKIの技術

鍵使用目的拡張（Key Usage)

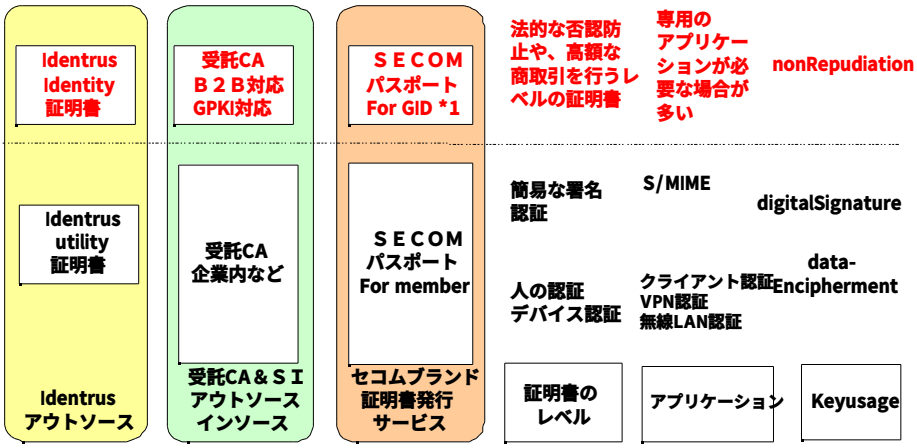
- 鍵使用目的拡張
  - _ 証明書に対応した鍵を使用してサポートする機能やサービスを識別するために(あるいは制限する) 使うビット列
- Key Usage拡張 - 署名鍵の扱い
  - _ Non Repudiation（NRビット）
    - ・文書へのデジタル署名
  - _ Digital Signature（DSビット）
    - ・Nonceへのデジタル署名
    - ・認証（Authentication)用途


PKIの技術
鍵使用目的拡張（Key Usage）
JNSA
CA署名鍵
相互認証証明書
KeyUsage(Critical)
cRLSign
keyCertSign
ボブの
信頼
ポイント
CRL
CA-A
CA-B
CA証明書
EE証明書
KeyUsage(Critical)
nonRepudiation
digitalSignature
EE証明書
アリスの
私有鍵
アリス
アリスの
署名文書
ボブ
GPKIにおいて
Keyusageはクリ
チカルにマーク
されている。また、
EE証明書の
nonRepudiation
は非常に大きな
意味がある
** GPKIでは、CA証明書、EE証明書で、クリチカルな鍵使用目的拡張を必須としている
Copyright (c) 2002 NPO日本ネットワークセキュリティ協会
Page 23


PKIの技術
認証と署名
JNSA
WWW
サーバ
TLS
署名された
発注データ
署名された
発注データ
アリス
クライアント認証
のための署名
否認防止
の署名
ハードウェアトークン
アリスの署名が
付いた発注デー
タが保存される
ことが重要。
PIN
入力
CA証明書
否認防止用
証明書
鍵ペア
鍵ペア
認証用
証明書
例えば、Identrusでは上記の様な２種類の証明書を使用している。
Copyright (c) 2002 NPO日本ネットワークセキュリティ協会
Page 24

PKIの技術

鍵使用目的拡張と証明書発行の関係
(セコムトラストネットの証明書発行サービスの例)



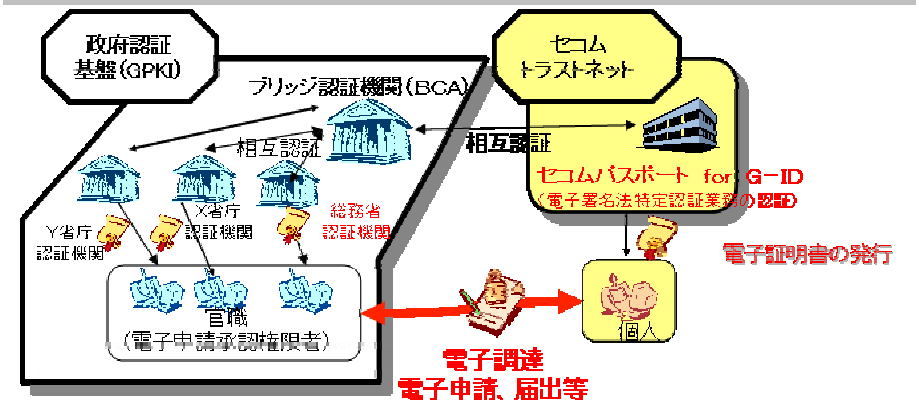
*1 SECOMパスポートfor GIDは、電子署名法特定業務認定取得済み、 GPKI相互認証を申請中

PKIの技術

認証サービスの運用基準と監査
(セコムトラストネットの証明書発行サービスの例)

認証サービス名	運用基準など	状況
Identrus Express Partner	Identrus CCAG (Identrusの運用監査基準)	認定
セコムパスポート　Ｆｏｒ GID (2002年９月現在サービス準備中)	電子署名法特定認証業務	認定
セコムパスポート　Ｆｏｒ Memb	セコムトラスネットの運用基準	ー

PKIの技術
否認防止署名のための証明書（セコムパスポート for G-ID）



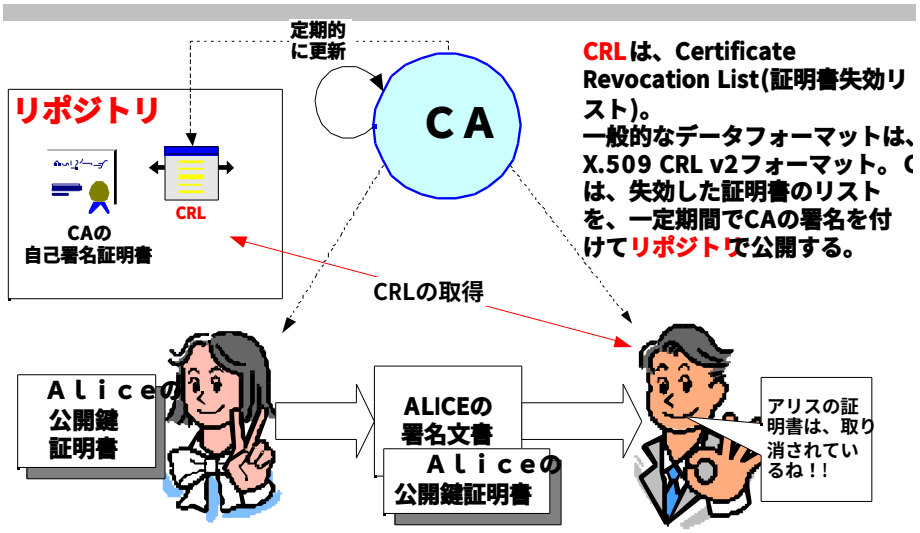
否認防止が可能な署名のための証明書

政府認証基盤のブリッジ認証局との相互認証を申請中

総務省の電子入札のための証明書などを予定している

 Page 27

PKIの技術
証明書の失効



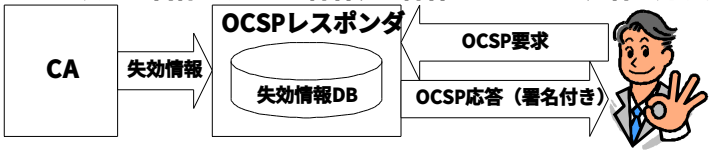
CRLは、Certificate Revocation List(証明書失効リスト)。
一般的なデータフォーマットは、X.509 CRL v2フォーマット。CRLは、失効した証明書のリストを、一定期間でCAの署名を付けてリポジトリで公開する。

 Page 28

PKIの技術

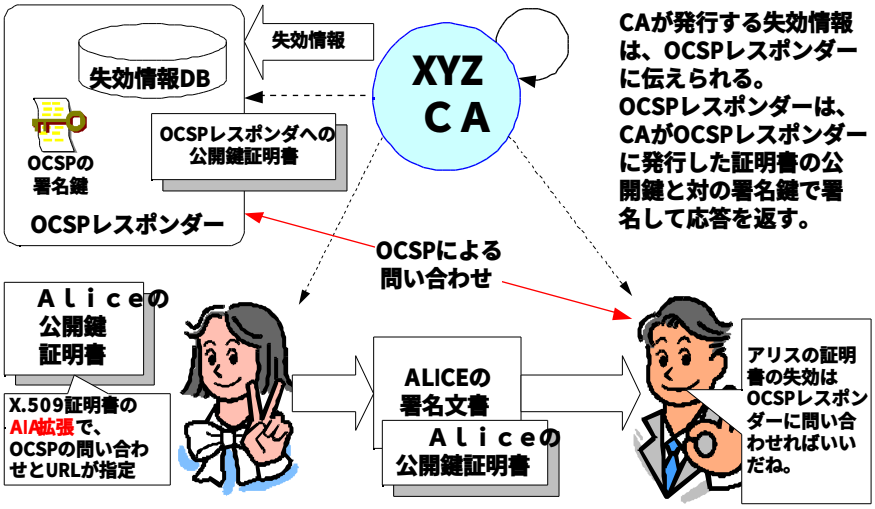
OCSP

- RFC-2560
  - Online Certificate Status Protocol - OCSP
  - RFCになったのは、 99年6月
- IdentrusでのOCSP
  - Identrusは、OCSPを利用して証明書の失効情報を取得している。
  - Identrusの4コーナモデルでかなり込入った使い方をしている。
- 商業登記CAでのOCSP
  - 商業登記CAは、CAとは別にOCSPレスポンダを用意している訳ではなく、CA自体が、CAの署名鍵で署名して OCSPの応答を返す。



PKIの技術

OCSPの仕組み



CAが発行する失効情報は、OCSPレスポンダーに伝えられる。
OCSPレスポンダーは、CAがOCSPレスポンダーに発行した証明書の公開鍵と対の署名鍵で署名して応答を返す。

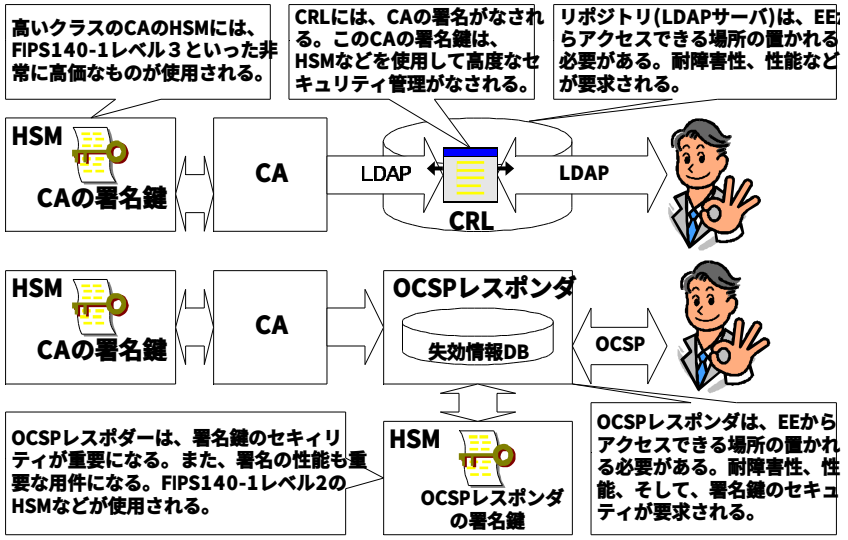
CRLとOCSPの検証の違い

OCSPレスポンダの証明書を失効の問題が面倒。OCSPでの応答にするとでは、OCSP自体の署名になってしまう。

 Page 31

PKIの技術

LDAP,CRLとOCSPの比較



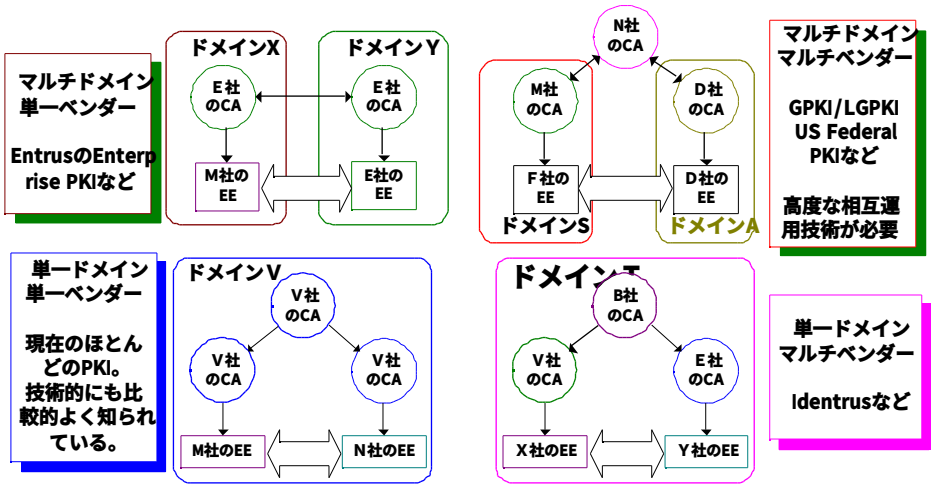
 Page 32

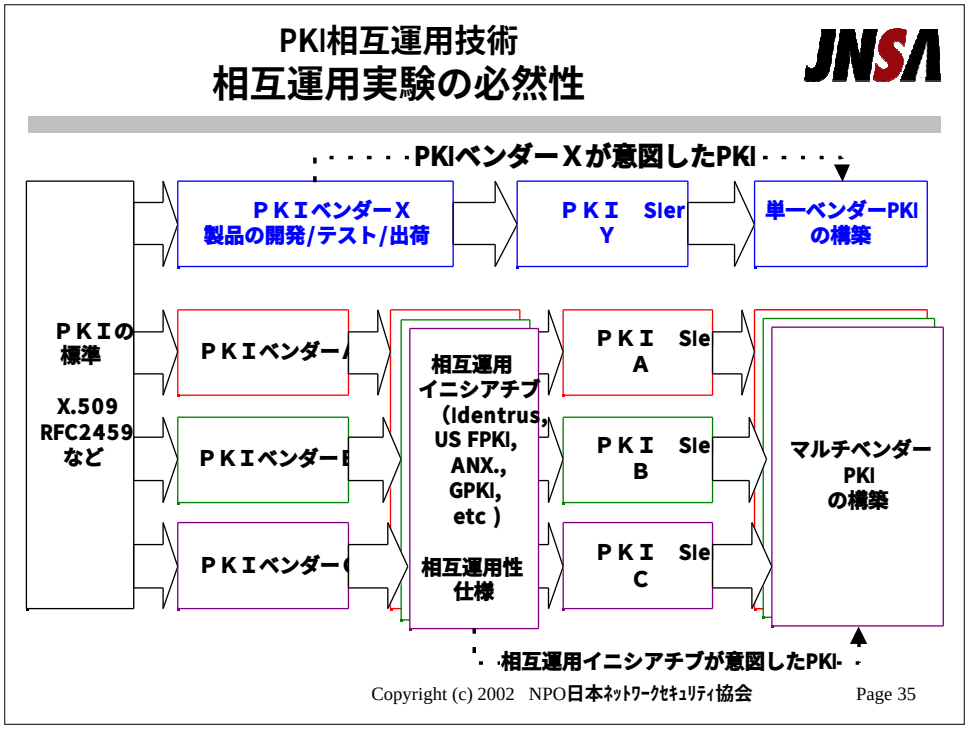
PKI相互運用技術

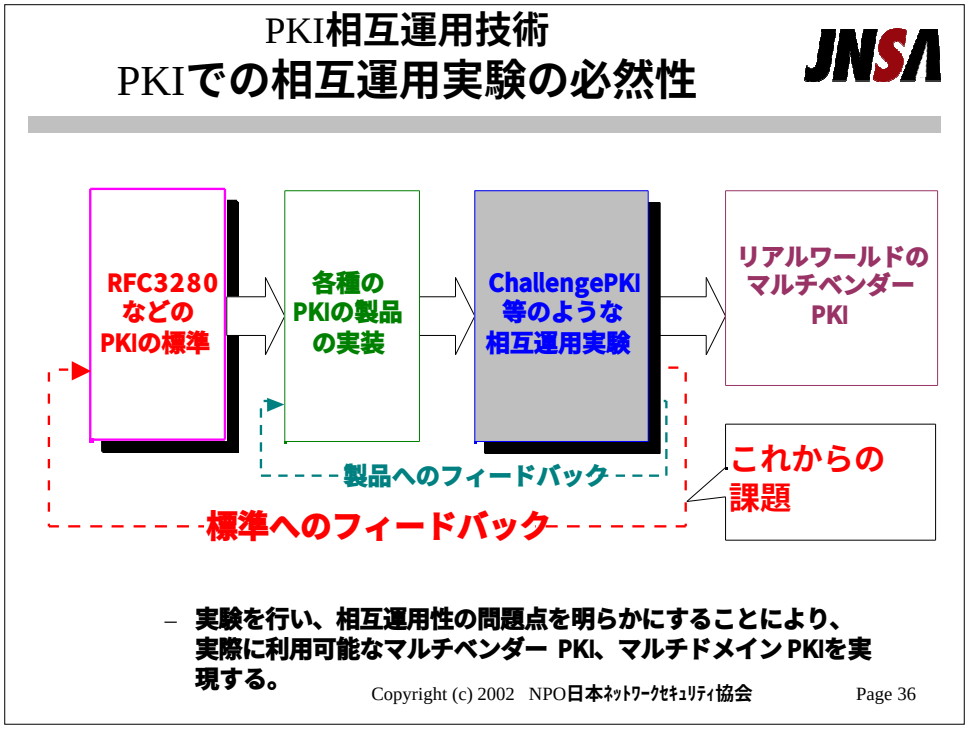
マルチドメインＰＫＩ/マルチベンダーPKIの相互運用技術

- マルチドメインＰＫＩ、マルチベンダーPKIの例は、GPKIに限ったことではない。北米やEUでは、各種の相互運用イニシアチブが積極的に活動している。
- Identrusのようなマルチベンダー PKI、GPKIのようなマルチドメインＰＫＩ、マルチベンダーPKI では、相互運用性実験の重要さが指摘されている。

マルチベンダーPKI、マルチドメインPKI




PKI相互運用技術
相互運用実験の必然性
JNSA
PKIベンダーXが意図したPKI
ＰＫＩベンダーX
製品の開発/テスト/出荷
ＰＫＩ　SIer
Y
単一ベンダーPKI
の構築
ＰＫＩの
標準
X.509
RFC2459
など
ＰＫＩベンダー
ＰＫＩベンダー
ＰＫＩベンダー
相互運用
イニシアチブ
(Identrus,
US FPKI,
ANX.,
GPKI,
etc)
相互運用性
仕様
ＰＫＩ　SIe
A
ＰＫＩ　SIe
B
ＰＫＩ　SIe
C
マルチベンダー
PKI
の構築
相互運用イニシアチブが意図したPKI
Copyright (c) 2002　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会
Page 35


PKI相互運用技術
PKIでの相互運用実験の必然性
JNSA
RFC3280
などの
PKIの標準
各種の
PKIの製品
の実装
ChallengePKI
等のような
相互運用実験
リアルワールドの
マルチベンダー
PKI
製品へのフィードバック
これからの
課題
標準へのフィードバック
– 実験を行い、相互運用性の問題点を明らかにすることにより、
実際に利用可能なマルチベンダー PKI、マルチドメイン PKIを実
現する。
Copyright (c) 2002　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会
Page 36

PKI相互運用技術

世界のPKI相互運用実験

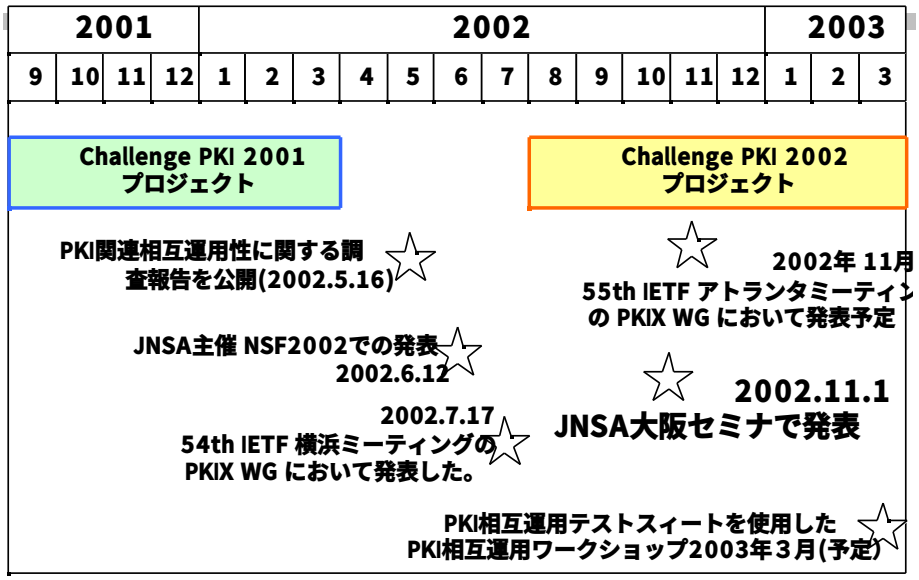
実験名	地域・主催	信頼モデル	実験アプリケーショ	その他
GPKIの実証実験	日本 総務省ほか	比較的単純なブリッジモデル	GPKIテストプログラム	BCA、３府省CA、商業登記CA、テストCA
EMA Challenge 2000	米国 EMA	階層、メッシュが混在したブリッジモデル	S/MIME	5つのCA製品。最大７つの証明書パス
BCA Technology Demonstration Phase 2	米国 NSA他	階層、メッシュが混在したブリッジモデル	S/MIME、属性証明書などの使用	６つのCA製品。複数署名アルゴリズムなど
CESG PKI相互運用テスト	英国 ＣＥＳＧ	階層モデル	S/MIME	７つのCA製品。
EEMA Pki Challenge	ＥＵ	3レベルの階層モデル 相互認証モデル	各種のPKIアプリケーションを検討中	-
３国間相互運用性実証実験	日本、韓国 シンガポール	相互認証、相互承認	-	-
ＪＮＳＡ Challenge PKI 20	*日本 JNSA/IPA*	*階層モデル、相互認証モデル、ブリッジモデル*	*SSLクライアント認証、IPsec、S/MIME*	*9つのCA製品（サービスを含む）*

NPO JNSAのPKI相互運用プロジェクト

Challenge PKI 2001とPKI2002

- Challenge PKI 2001
  - 昨年度のプロジェクト
  - 情報処理振興事業協会（IPA）の委託を受けて実施
  - ９つのCAが参加を得て行ったマルチドメイン PKI、マルチベンダーPKIのPKI相互運用実験
- Challenge PKI 2002
  - 今年度のプロジェクト
  - 情報処理振興事業協会（IPA）の委託を受けて開発
  - 相互運用テストスィートなどの開発
  - マルチドメインPKI、マルチベンダーPKIの開発を容易にする
- Challenge PKI 2001とChallenge PKI 2002の目標
  - マルチドメインPKI、マルチベンダーＰＫＩ環境

Challenge PKI 2001&2002



Challenge PKI 2001の概要

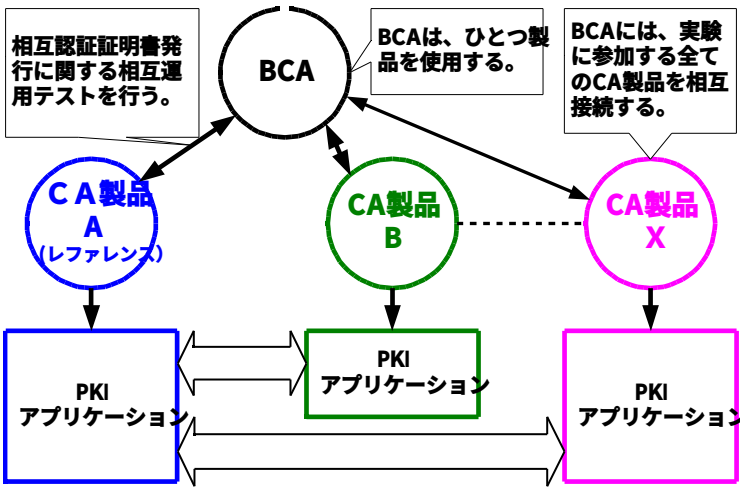
Challenge PKI 2001とは？

- Challenge PKI 2001「複数CAを使用したPKI相互運用実験」
  - NPO日本ネットワークセキュリティ協会（ JNSA）が、経済産業省のご支援の下、情報処理振興事業協会（ IPA）の 「情報セキュリティ関連の調査・開発」の一環として実施した PKI相互運用実験。
- 9団体の9CA(サービスを含む) で構成
  - マルチベンダーの PKI相互運用実験として、9 つもの異なる CAを使用する実験は世界的にも例がない。
  - 各参加団体から、多彩なメンバーが参加
  - 工学院大学などの協力
- マルチベンダーＰＫＩ／マルチドメインＰＫＩ
  - 実験では、 GPKIなどで採用されている異なる PKIドメイン間の相互運用性を取り上げる。
  - マルチベンダーＰＫＩ／マルチドメイン PKIは、PKIが真のインフラになるためには当然の流れ。
  - しかし、これらは、事例が少なく、問題点が明らかになっていない。

Challenge PKI 2001の概要 参加団体と参加CA

実験参加企業（団体）	実験参加CA
セコムトラストネット/エントラストジャパン	Entrust PKI 6.0
ＳＳＨコミュニケーションズ・セキュリティ	SSH Certifier 2.0
NECソフト	NEC Carassuit電子政府版Ver1.1
RSAセキュリティ	Keon Certificate Authority 6.
富士ゼロックス/富士ゼロックス情報システム	未発表製品
マイクロソフト プロダクトディベロップメント リミテッド	Microsoft Windows Server
日本ベリサイン	(非公開)
名古屋工業大学	Easy Cert(開発 奥野琢人氏)
ＷＩＤＥプロジェクト	ICAP v2.51（ICAT)

ブリッジモデルの実験と参加CAの関係



Challenge PKI 2001の概要
Challenge PKI 2001の成果

JNSA

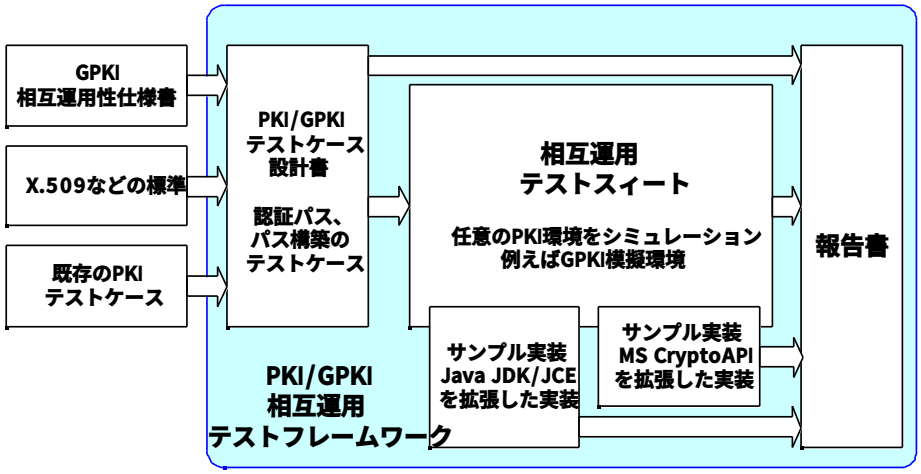
- PKI相互運用実験の実施による製品へのフィードバック
  - _ 製品などに反映されたものもある
- 報告書の作成
  - _ http://www.ipa.go.jp/security/fy13/report/pki_interop/pki_interop.pdf
  - _ PKIの相互運用性に関わる課題を解説
- IETFでの発表
  - _ 54th IETF 横浜ミーティングの PKIX WG において発表した
  - _ http://www.ietf.org/ietf/02jul/pkix.txt

Challenge 2002-プロジェクトの背景と目的

JNSA

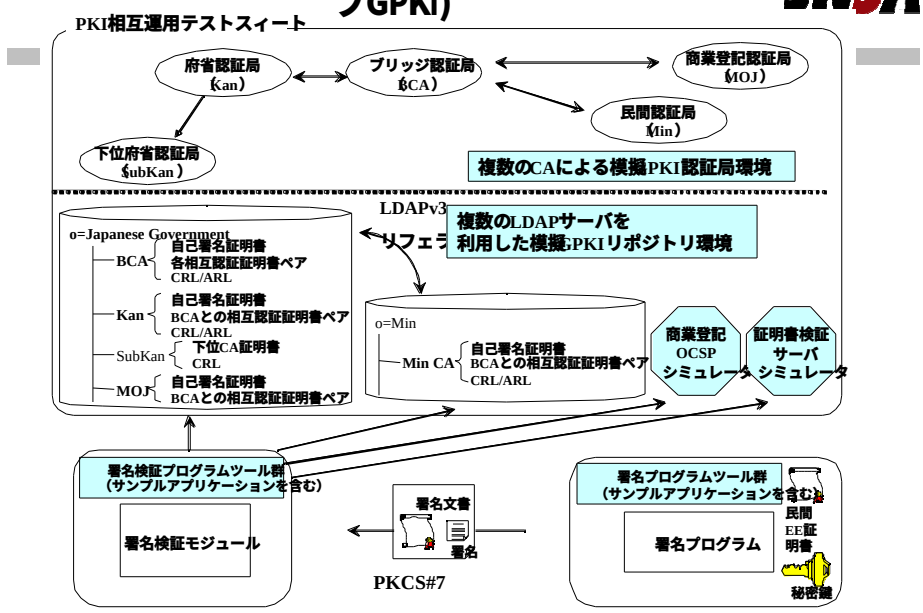
- プロジェクトの背景 - 電子政府の成功の鍵
  - _ 使いやすくセキュアなＧＰＫＩ・電子政府対応アプリケーションの流通
    - ・相互運用性が確保されたＧＰＫＩ・電子政府対応アプリケーションの流通
    - ・ＧＰＫＩ対応電子政府対応アプリケーションの開発の促進
  - _ これらは、PKIを基盤とした広範囲なセキュリティを適正なコストで実現
- プロジェクトの目的 - PKI相互運用フレームワークの提供
  - _ PKI及び、GPKI相互運用の促進のための道具を開発して提供
  - _ PKI及び、GPKIアプリケーション開発＆テスト環境の開発
    - ・GPKIは、他にはないマルチベンダー、他にはないマルチドメイン環境。
      - _ 現状、実環境以外での開発、テストは、非常に困難
  - _ PKI及び、GPKIの学習環境の提供
    - ・PKI/GPKIの啓発。
      - _ PKI/GPKIを体験できる環境を提供
      - _ GPKIサンプルアプリケーションと実装ガイド

Challenge PKI 2002
PKI/GPKI相互運用フレームワーク



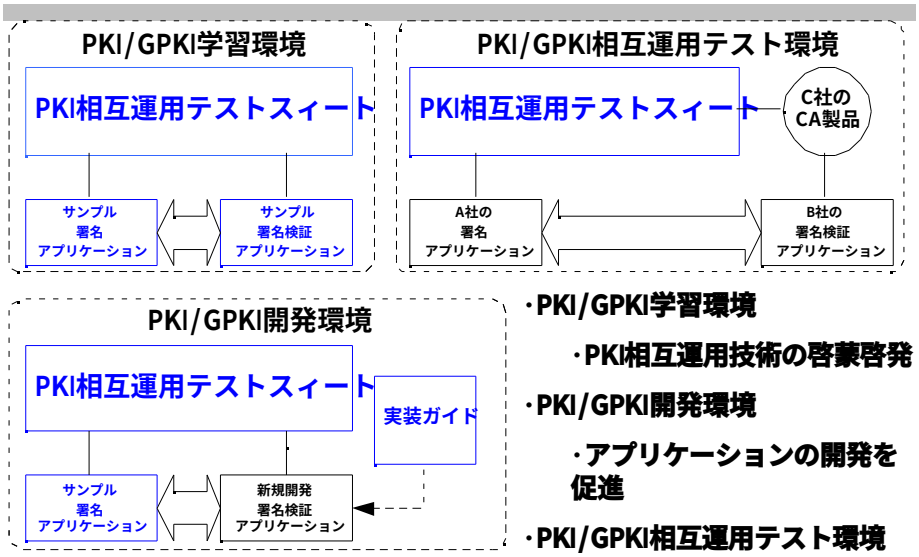
 Page 45

Challenge PKI 2002 ＧＰＫＩ模擬環境（デスクトップGPKI)



 Page 46

Challenge PKI 2002 - 成果物の利用イメージ



- PKI/GPKI学習環境
  - PKI相互運用技術の啓蒙啓発
- PKI/GPKI開発環境
  - アプリケーションの開発を促進
- PKI/GPKI相互運用テスト環境
  - PKIアプリケーションのテス

Challenge PKI 2001&2002の参考 PKI相互運用性関係の参考情報

- IPA PKI 関連相互運用性に関する調査報告
  - Challenge PKI 2001などの調査報告のページ
  - http://www.ipa.go.jp/security/fy13/report/pki_interop/pki_interop.html
  - http://www.ipa.go.jp/security/fy13/report/pki_interop/pki_interop.pdf
  - 技術的な問題点の指摘はこちらを参照
- Network Security Forum 2002でのセミナ
  - JNSAのセミナー「ＰＫＩの相互運用実験　Challenge PKI 2001」の資料
  - http://www.jnsa.org/nsf2002/r_12_b1.html
  - http://www.jnsa.org/nsf2002/pdf/B1.pdf