

電子政府とGPKI

CACAnet FUKUOKA

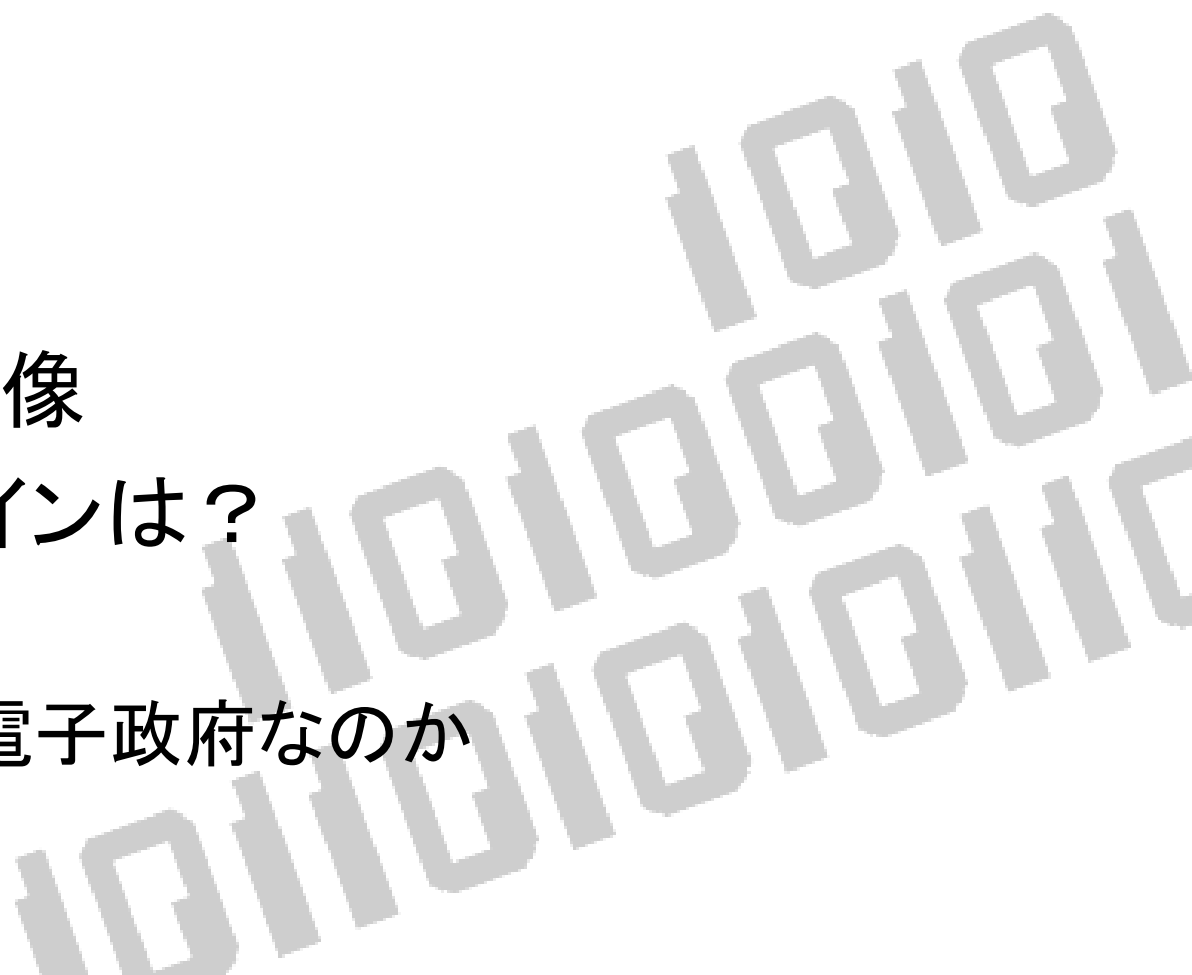
慶應義塾大学看護医療学部

宮川祥子

「電子政府」という・・・



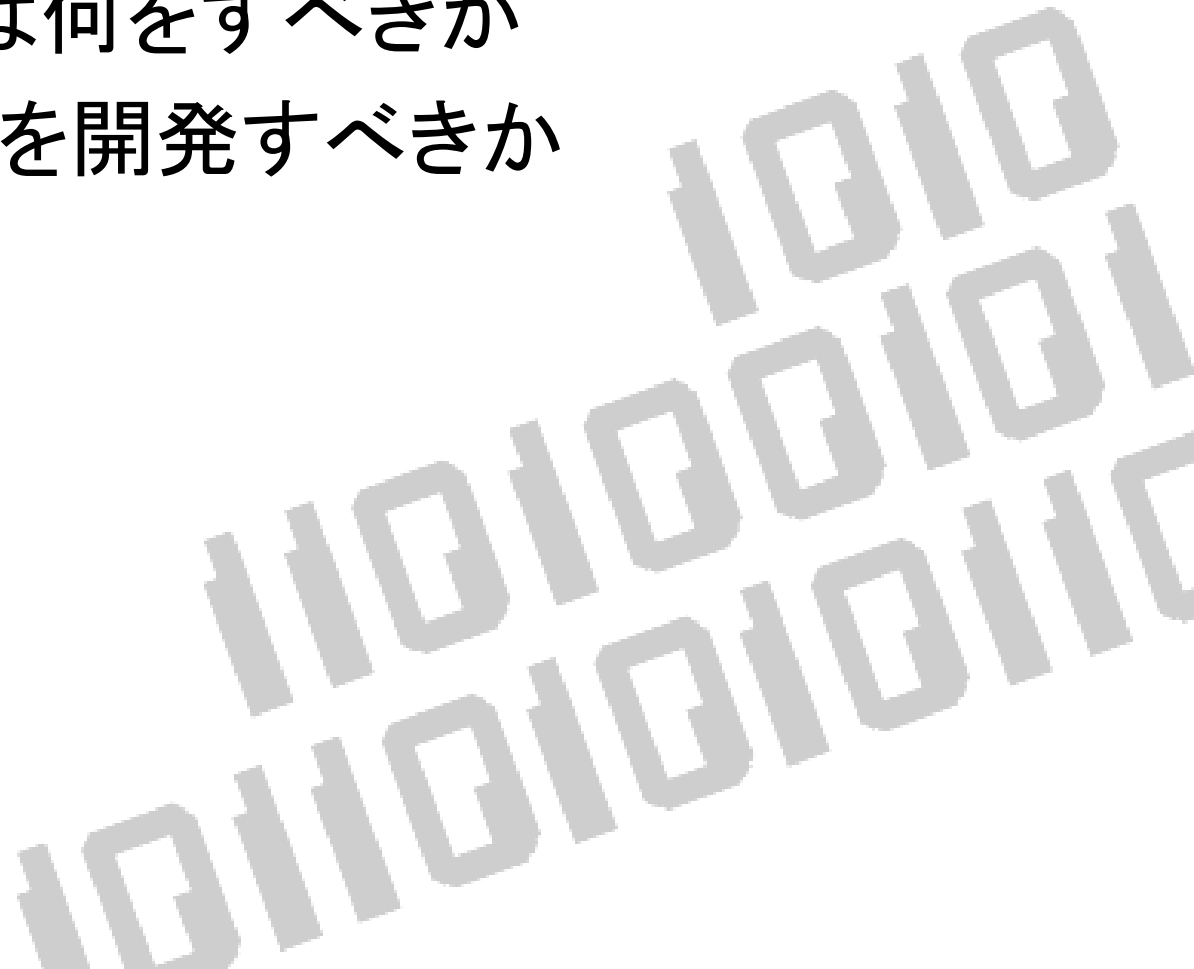
- 掛け声
- 予算
- 調達
- 見えない実態像
- グランドデザインは？
 - 誰のため
 - 何のための電子政府なのか



われわれは？



- 行政スタッフは何をすべきか
- ベンダーは何を開発すべきか
- 研究者は？
- 市民は？





- 電子政府プロジェクト
- GPKI(政府認証基盤)



「電子政府」プロジェクト



- 1999年12月政府による「ミレニアム・プロジェクト」に盛り込まれる
- 省庁で扱っている各種申請・届出の電子化・インターネット化
- 政府調達の電子化・インターネット化
- スケジュール
 - 2000年度 各省庁において申請・届出についてのアクションプラン策定
 - 2003年度までにアクションプランの実施
 - 2005年度までに政府調達の電子化を実現

「電子政府」プロジェクト(続き)

各省庁ごとに実現

申請・届出の電子化

汎用的なセキュリティ
評価体系と処理シ
ステムの構築

共通基盤技術
ウイルス・不正アクセス対策
汎用申請・届出処理システム

各省庁認証基盤
の構築とブリッジ
CAを用いた連結

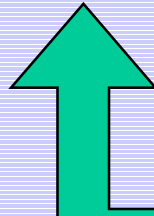
認証基盤構築
政府認証基盤(GPKI)

電子化の範囲と手法



中央官庁

パスポート
納税
年金・保険
国家試験・資格
自動車登録

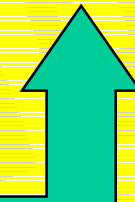


届出・申請



地方政府

住民票・印鑑証明
納税(地方税)



届出・申請



電子政府で実現されるオンライン化(1)

| | 手続数 | オンライン化 | 割合 |
|-----|------|--------|--------|
| 大蔵省 | 1329 | 1324 | 99.6% |
| 総務庁 | 53 | 52 | 98.1% |
| 法務省 | 194 | 94 | 48.5% |
| 金融庁 | 1091 | 1027 | 94.1% |
| 経企庁 | 46 | 46 | 100.0% |
| 公取委 | 20 | 18 | 90.0% |
| 防衛庁 | 40 | 36 | 90.0% |
| 外務省 | 65 | 3 | 4.6% |
| 厚生省 | 1589 | 1040 | 65.4% |
| 運輸省 | 1402 | 1332 | 95.0% |
| 農水省 | 1103 | 1062 | 96.3% |
| 合計 | 6932 | 6034 | 87.0% |

平成15年度までにオンライン化される手続

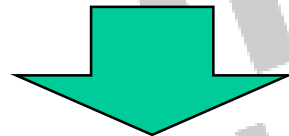
電子政府で実現されるオンライン化(2)

- ◎所得税・固定資産税・消費税等の申告
- ◎国民年金・健康保険・厚生年金保険関係の届出
- ◎医薬品・医薬部外品・化粧品又は医療用具の副作用・感染症状の報告
- ◎国家試験受験手続(一部:介護福祉士・栄養士等)
 - 医師・歯科医師・看護婦についてはシステム検討
- × 不動産登記・商業法人登記
- × 入出国・パスポート関連
- △自動車関係(平成17年度)

政府認証基盤 (GPKI)



- 政府内 (GtoG)、政府と民間 (GtoB, GtoC) での文書のやり取りをインターネット経由で行う
- 文書の真性性の確保が必要
 - 差出人が特定できること
 - 文書が改ざんされていないこと



公開鍵暗号を用いた認証基盤
と電子署名によって実現

電子署名



- 「電子署名」…電子的な文書が真正であることを証明するデータ
- 「鍵」と呼ばれる秘密データを使う…秘密鍵は盗まれてはいけない！
- 紙の文書（契約書など）
 - サイン
 - 認印
 - 実印＋印鑑証明
 - 契約の重要さによって使い分ける
- 電子署名は、電子データに対する押印

電子署名こぼれ話



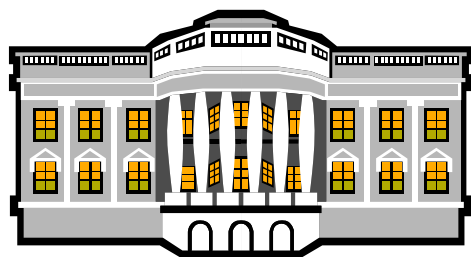
- ボルチモアテクノロジーズのビデオ
- 米国大統領とアイルランド首相が電子署名で条約に調印
- 通常では。。。そのあと握手して万年筆を交換
- ビデオでは。。。握手して秘密鍵の入ったICカードを交換

みなさんはまねをしてはいけません。

制度的に見たGPKIの必要性



省内で規定された決済手続き
(押印)
↓
GPKIを用いた認証・電子署名



政府機関
(省庁)

署名(政府認証
機関)



公文書



私文書

署名(民間認証
機関)



私文書の真正性の確保
(押印+印鑑証明)

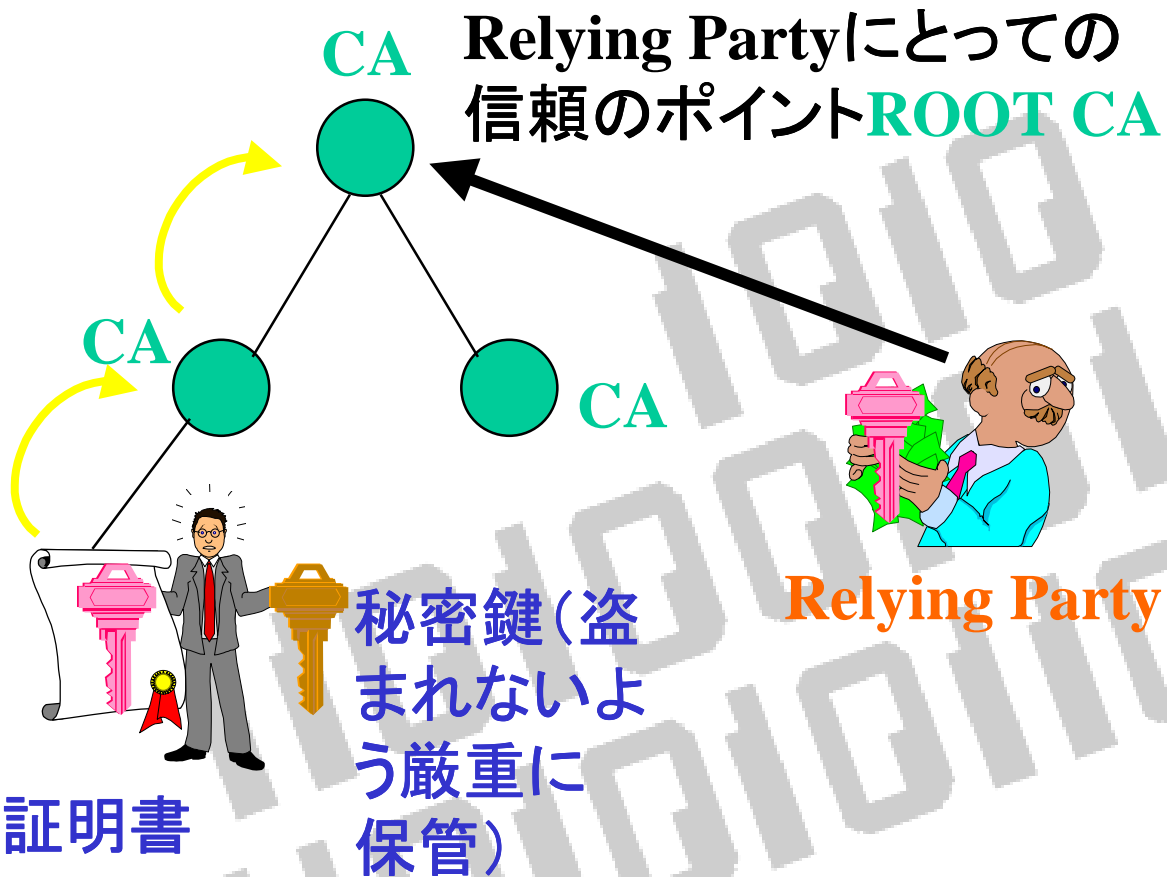
↓
基準を満たした認証機関による
認証・電子署名(電子署名法)

民間(企業・個人)

一般的なPKIの構造



- 認証機関 (CA: 証明書を発行する)
- Subscriber (証明書が発行される)
- Relying Party (証明書を検証する)

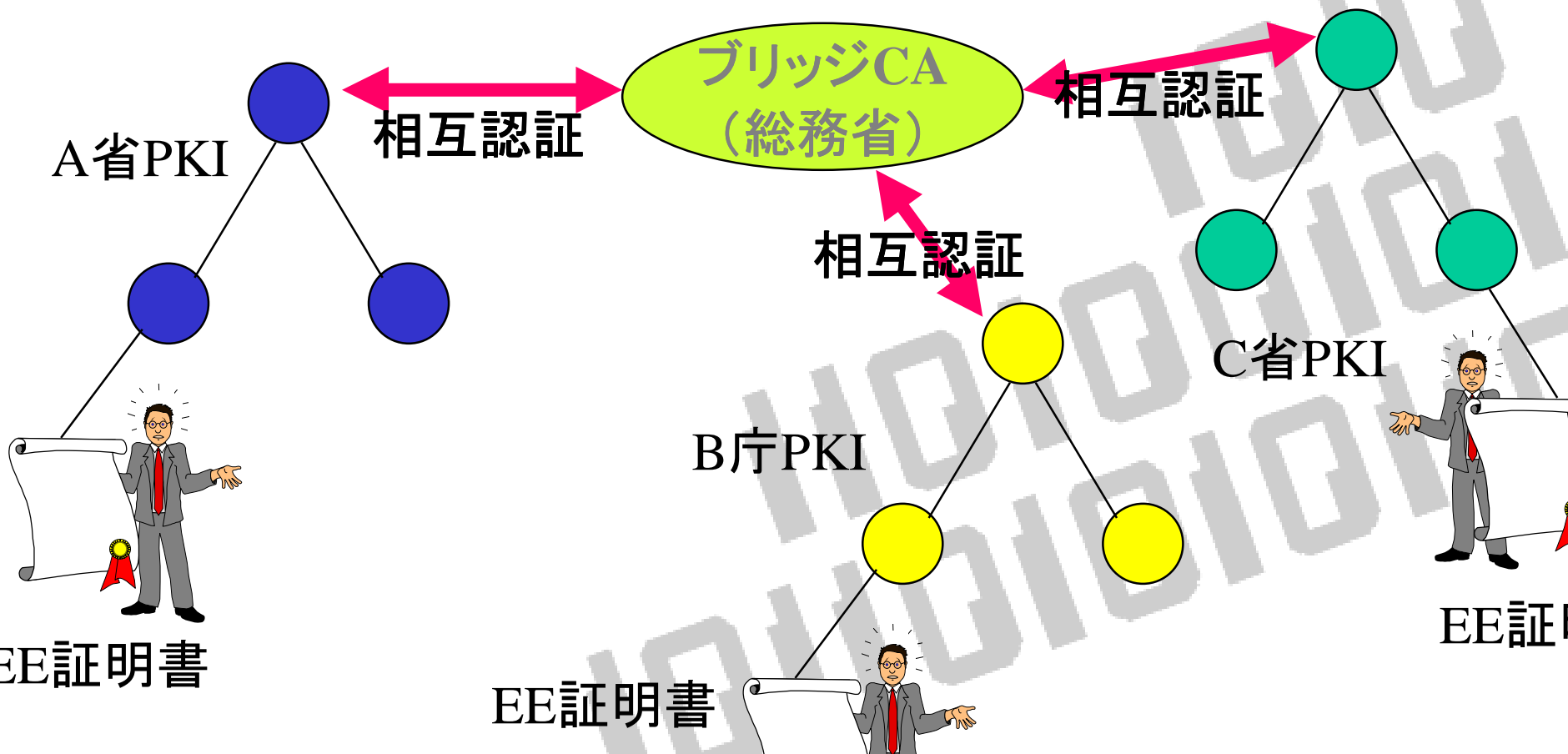


GPKIの構造



各省庁は別個にCAを構築

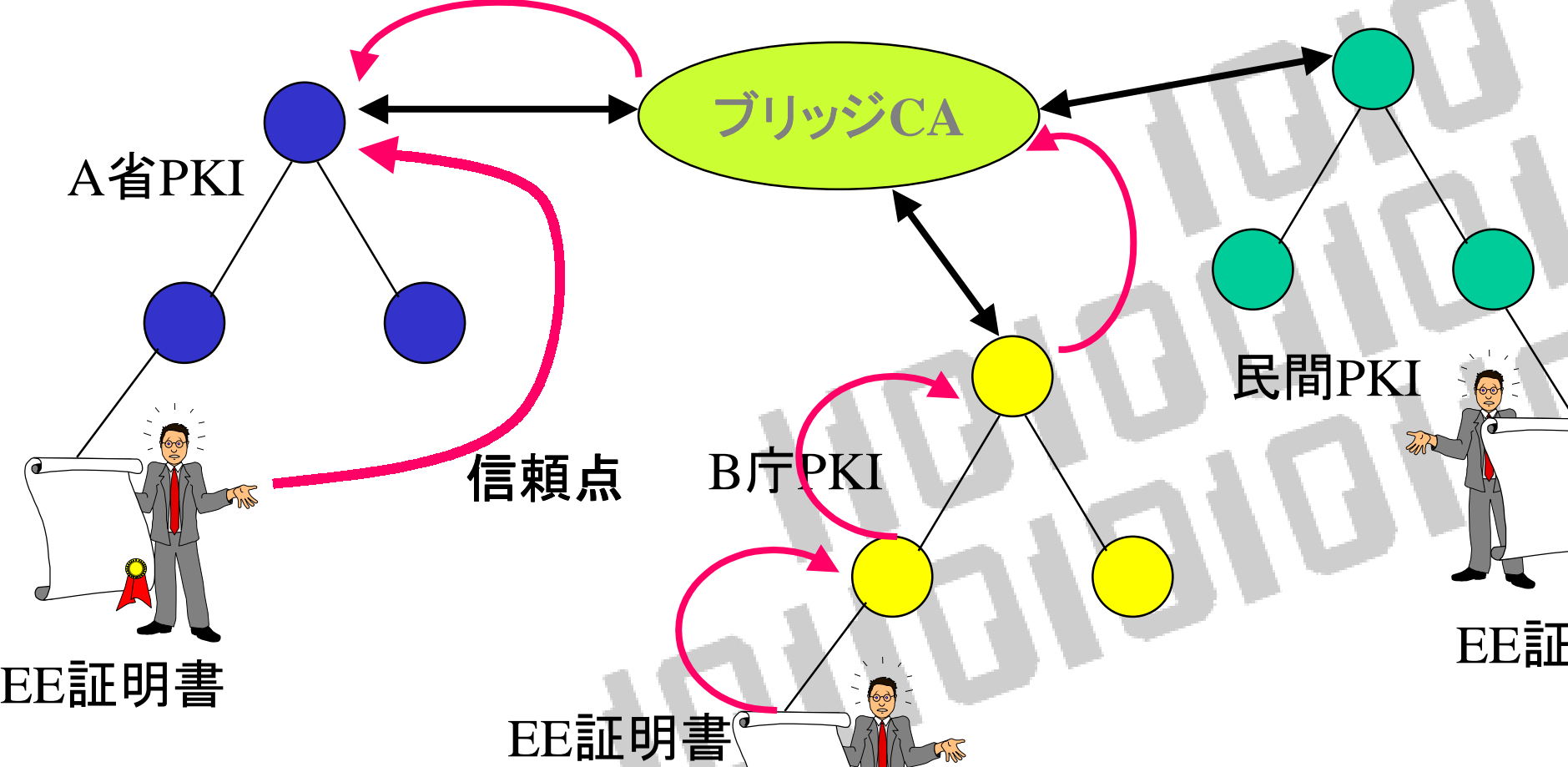
ブリッジCAを用いた省庁・民間認証機関の相互連結



GPKIの構造



各省庁が別個にCAを構築
ブリッジCAを用いた省庁・民間認証機関の相互連結



BCA——新しい技術



- 他のドメインを信じることなく証明書を検証することが可能
- BCA自体は信頼点とはならない
- 米国FPKI (Federal PKI)で採用——プロトタイプによる接続実験の段階
- 実際に利用された経験が世界中のどこにもない
- Relying Party (証明書を検証する側)のクライアント (WWWブラウザ、メールクライアント等)改造が必要

GPKIの電子証明書は「何を」 証明するか



- 官庁CAが発行する証明書は「官職証明書」
- 「本人」ではなく「官職」を証明するデータ
- たとえば・・・私は「経済産業省情報経済産業局電子政策化課長補佐1号」です。
- 役職が変わると、鍵は次の担当者に引き継がれる（鍵はICカードに格納）
- 証明書執行を少なくするための工夫
- 本当にこれでいいのか？
 - 「官職」さえ証明されればいいのか
 - 属性証明書との整合性は？

電子署名法

世の中に実印と認印があるように



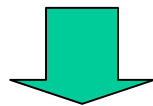
- 電子署名も千差万別
- どんな認証局が発行した鍵を使っているか
 - 実印相当の認証局
 - 十分に安全な運用
 - 認印相当の認証局
 - それなりの運用？
- 「実印」レベルの認証局を国が認定
→ 電子署名法の認定

制定までの紆余曲折



- 通産・郵政・法務の提議
- 電子商取引をスムーズにする
- 犯罪防止的視点からの検討
 - すべての認証局を登録制にしようとか
 - キーエスクローを義務付けようとか

鍵預託
信頼できる機関(公的機関)に秘密鍵を預けること

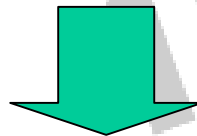


認定認証局の申請は任意
キーエスクローなし

電子署名法とGPKI



- GPKIは、政府の認証局と民間の認証局もブリッジする
- どのような民間認証局がつながるか
 - 電子署名法で認定された認証局
 - BCAに接続するための技術的な要件をクリア
 - + α



民間認証局が電子政府に対応するためには電子署名法の認定が必要(予測)

GPKIの現状



- 2001年1月～3月に相互接続実験
 - 発注仕様書には「相互接続性確保」という要件はなし
 - ベンダーの良心？
 - CA中心
 - クライアントは擬似
- 4月より、相互接続開始
 - 経済産業省
 - 国土交通省
 - 商業登記

GPKIに関する情報源



- GPKI公式ホームページ
 - <http://www.gpki.go.jp/>
 - GPKI勉強会のページ(宮川主催)
 - <http://siren.sfc.keio.ac.jp/GPKI>
- 

主な電子政府関連システムの受注実績

日経新聞より



| システム名 | 発注者 | 受注起業 | 受注額 |
|--------------|-------|----------------------|----------|
| 住民基本台帳ネットワーク | 総務省 | 富士通・NEC・NTTデータ・NTTコム | 320億円 |
| 総合行政ネットワーク | 総務省 | 富士通・NEC・NTTコム・ネットワン | 14億円 |
| 政府認証基盤 | 総務省 | NEC・セコム・日立 | 1億2000万円 |
| 電子認証システム | 総務省 | 富士通FPI | 105,000円 |
| オンライン申請システム | 国土交通省 | NTTデータ | 2億9000万円 |
| 電子認証システム | 国土交通省 | NTTデータ | 3990万円 |
| 汎用電子申請システム | 経済産業省 | NEC・三菱電機・三菱総研 | 5億5800万円 |
| 電子認証システム | 経済産業省 | NEC | 9996万円 |

GPKI・電子政府のスケジュール

- 2000年度
 - ブリッジCA構築 通産・運輸・郵政で各省CA構築
 - ブリッジCAは総務省により調達
 - 2001年1月より、BCAとCAの接続実験開始
- 2001年度
 - 法整備(電子署名・認証)
 - 電子署名法は2001年4月より施行
 - BCA運用開始
 - 産業省CA,国土交通省CA,商業登記CAの相互接続
- 2003年度
 - 各省庁CA構築
 - アクションプラン実行

電子政府とセキュリティ基盤としての GPKIの課題



• 技術

- ブリッジCAを経由した証明書検証
 - テストケースの充実
 - テストセンターの整備
- スケーラビリティ

• 運用

- ブリッジCAと各省庁CAの(運用手順,セキュリティ基準)
- 秘密鍵の管理、失効手続き

• 電子化手法と評価

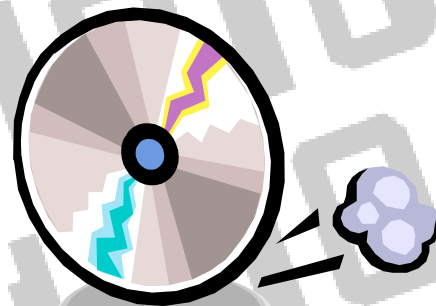
- 電子政府=既存の行政プロセスの電子化?
- 電子政府の評価軸(cost efficiency?)
- 情報公開とオープンディスカッション

PKIに関する大きな誤解(1)

- PKIアプリケーションとMS Officeの違い
- アプリケーションを買ったらPKIもついてきた
- 風呂を買ったら水道がついてきた？
- 「インフラ」という考え方



V.S.



PKI に関する大きな誤解(2)



- サーバ
- 発行

署名検証
認証パスの構築
認証パス検証
ポリシー制御
失効チェック

どっちが大変?

大変?

本人性の確認
安全な運用
失効管理

VAに聞けて?

証明書リ
ポジリは
どこ?

証明書の検証

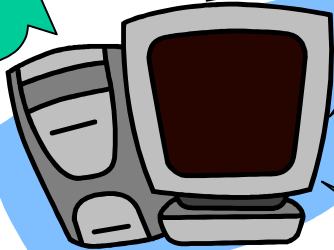
げ、昔の
署名だ!

証明書
証クライアント

ネットワー
クつながっ
てる?

CRL(証明書破棄
リスト)は最新?

証明書発行サーバ群



地方自治体の電子化



- 自治体の情報化・ネットワーク化
 - 処理の電子化
 - サービスの電子化
- 相互接続
- 総務省主導
 - GPKIは総務庁が主体
 - 地方自治体は旧自治省が主体
- 「何のための」が置き去りにされたまま仕様だけが決まっていくという現状

総合行政ネットワーク(LGWAN)

- 地方公共団体のネットワークを相互に接続
- 電子文書交換
- 横につながる意義
 - 住民票の移動？
 - どこにいても自動車免許が更新できる？
- 霞ヶ関WANとの連結がポイントか
- <http://www.home.soumu.go.jp/kokusai/index.html>

電子化する際に考えなければ いけないこと(1)



- 「電子政府」のグランドデザイン
 - 誰のために？
 - 5万人？10万人？100万人？
 - なんのために？
 - 行政の効率化？
 - 住民の利便性の向上？
 - 目標の設定とアセスメント
- サービスとしての要求と技術的な仕様にエネルギーを割かなければならない

電子化する際に考えなければ いけないこと(2)



- 仕様の継続的な見直し
 - 技術は日々進歩する
 - オープンネットワークの不確実性
 - 各国でオープンソース採用法の動き
- セキュリティの確保
 - 行政側のセキュリティ
 - 利用者(市民)側のセキュリティ
 - 秘密鍵をどこにしまえますか？
 - HSM(hardware security module)の普及
 - 体制作り

電子化する際に考えなければ いけないこと(3)



- 仕様の公開
 - 現在の情報公開で第3のベンダーが新規参入できるのか？
- テスト環境の整備
 - ベンダー固有の癖
- 人材開発
 - 技術を正しく理解した行政官がいるのか？