IPアドレス認証局

社団法人 日本ネットワークインフォメーションセンター
技術部／インターネット基盤企画部　セキュリティ事業担当
木村　泰司

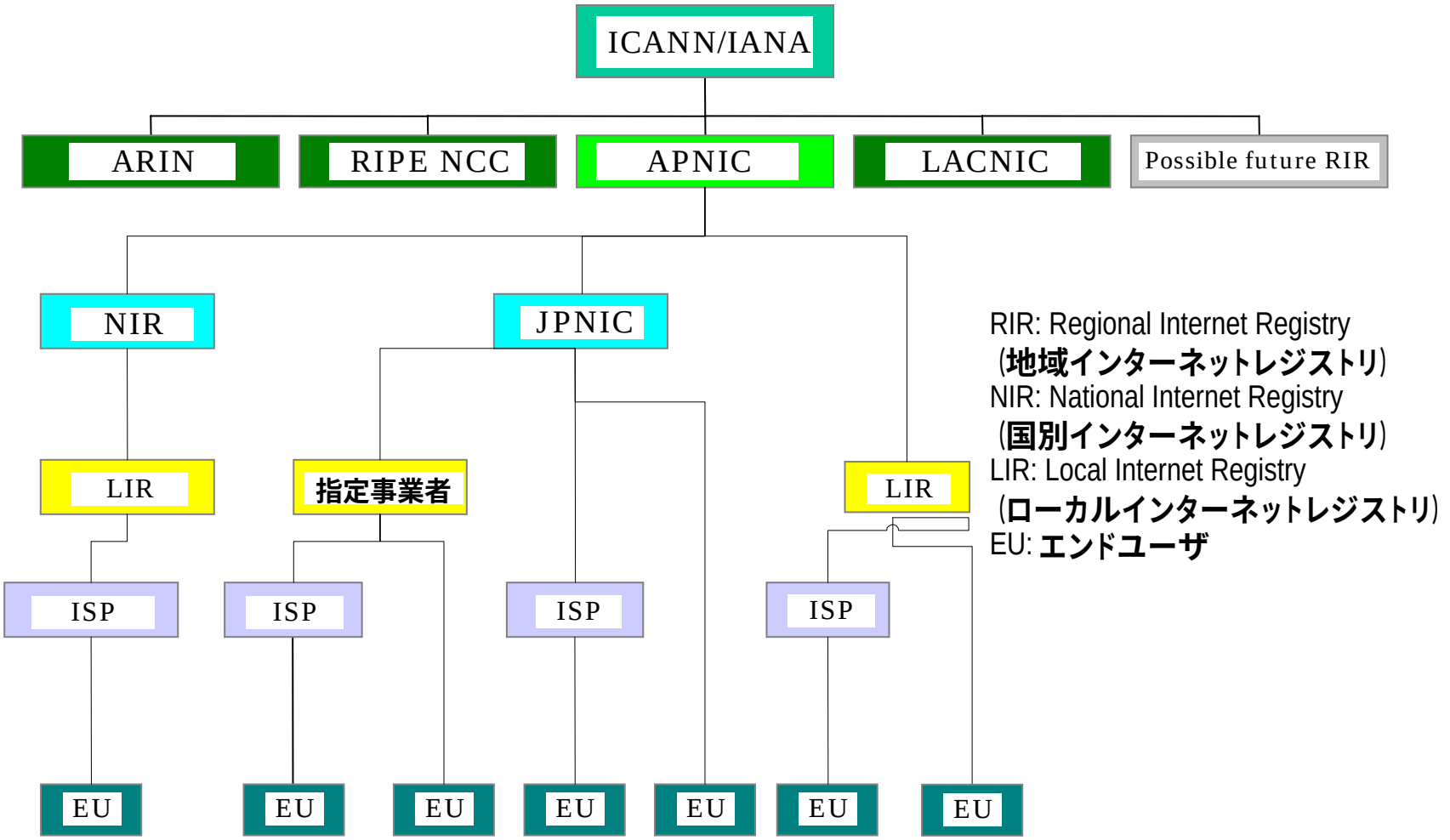
JPNICの認証局構築
事例紹介

”IPアドレス認証局　プロジェクト”

JPNIC IPアドレス認証局

- **日本におけるレジストリによる認証局**
  - IPアドレスとAS番号の管理（割り振り・割り当て）を行っているレジストリ（registry）の認証局
    - アドレス資源に関わる申請者の認証
    - IPアドレス／AS番号を用いた認証局の構築
  - 経済産業省からの受託研究として2002年度より調査研究を開始
    - 調査
      - レジストリの認証と位置づけ、CP/CPS
    - 認証業務の検討
    - CP/CPS ドラフト作成（2003年度）
    - 認証局システムの構築
  - 2005年度に実験導入開始の予定
    - IPアドレスの申請者（ISP）のクライアント認証

インターネットレジストリシステム



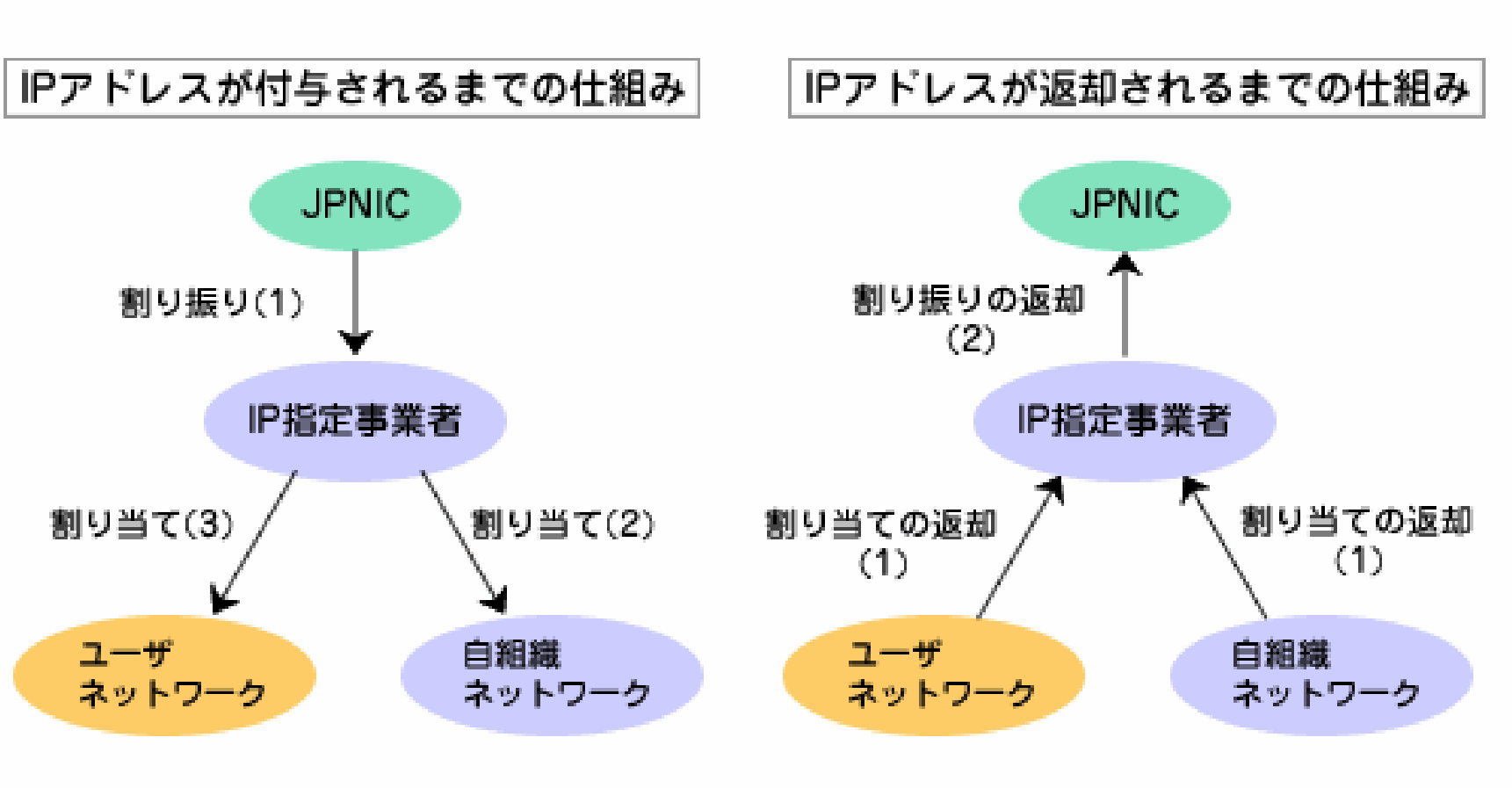
RIR: Regional Internet Registry
(**地域インターネットレジストリ**)
NIR: National Internet Registry
(**国別インターネットレジストリ**)
LIR: Local Internet Registry
(**ローカルインターネットレジストリ**)
EU: **エンドユーザ**

JPNICのIPアドレス事業

- IPv4アドレスの管理
  - 審議による効率的な利用の確認
  - APNICへの追加アドレス申請
  - データベースによる登録情報管理
- IPv6アドレスエージェントサービス
  - APNICへのIPv6申請の取り次ぎ
  - 日本語での審議問い合わせ対応
- AS番号の管理
  - 要件の審査
  - データベースによる登録情報管理
- IPアドレスレジストリシステムの提供
  - Whoisデータベース
  - 逆引きDNS
  - 申請受付･処理
- その他
  - ポリシー策定(IPv4,IPv6,AS)、統計情報の提供、ほか

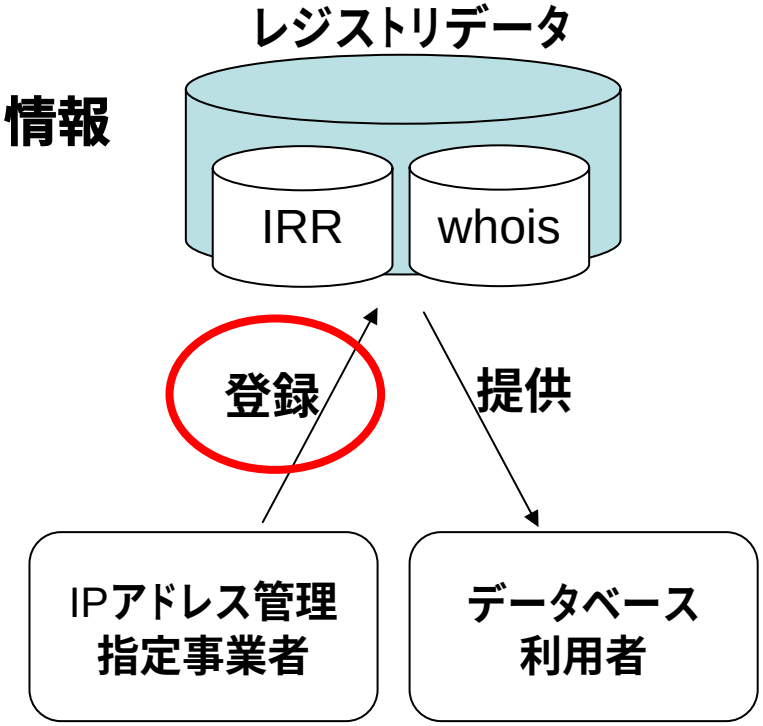
IPアドレス事業の役割
ーインターネットレジストリ
ーポリシ活動

IPアドレスの付与と返却の仕組み



アドレス資源とレジストリデータ

- レジストリデータ
  - アドレスの割り振り／割り当てに対応して登録
    - IP指定事業者への割り振り情報
    - ユーザネットワークへの割り当て情報
    - AS番号の割り当て情報
    - (連絡先、ホスト情報ほか)
  - 情報公開 (自律的な運用の為)
    - whoisを使った公開
      - whois.nic.ad.jp
      - IRR (jpirr.nic.ad.jp)



レジストリデータはアドレス資源管理の元本

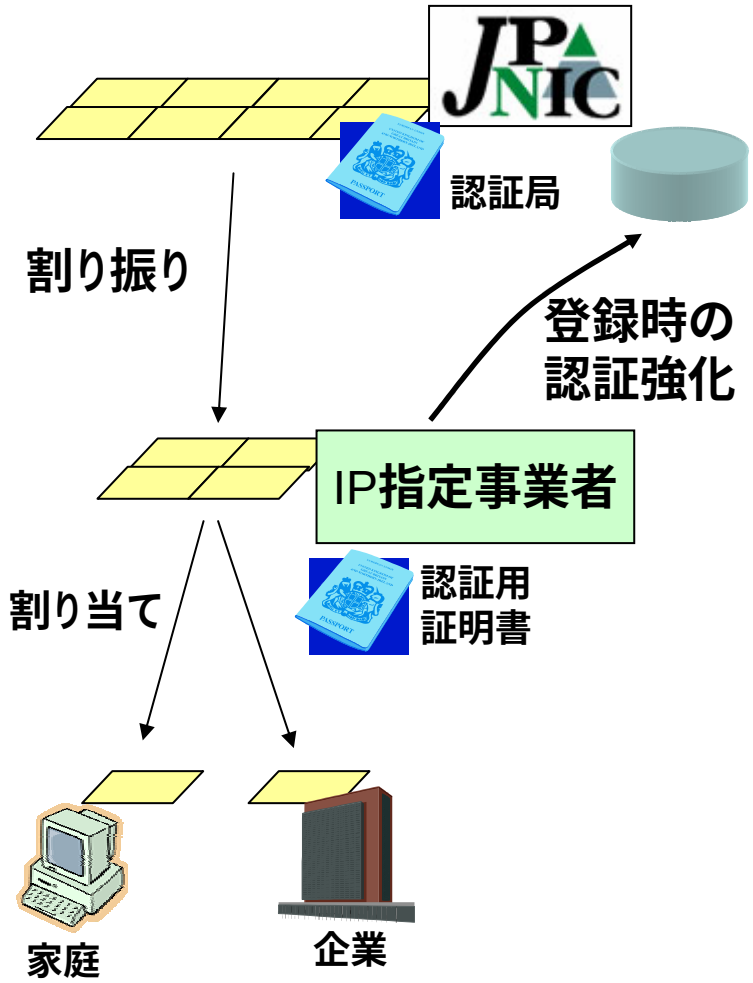
レジストリシステムの認証機能

- JPNIC
  - mail-from, ID/**パスワード**
- APNIC (**アジア太平洋地域のレジストリ**)
  - mail-from, crypto-pw, pgp-key
    ⇒ クライアント認証用の証明書
- RIPE NCC (**ヨーロッパ地域のレジストリ**)
  - mail-from, RegID/**パスワード**, crypto-pw, pgp-key, md5
    ⇒ クライアント人商用の証明書

強い認証の必要性が広く認識されつつある

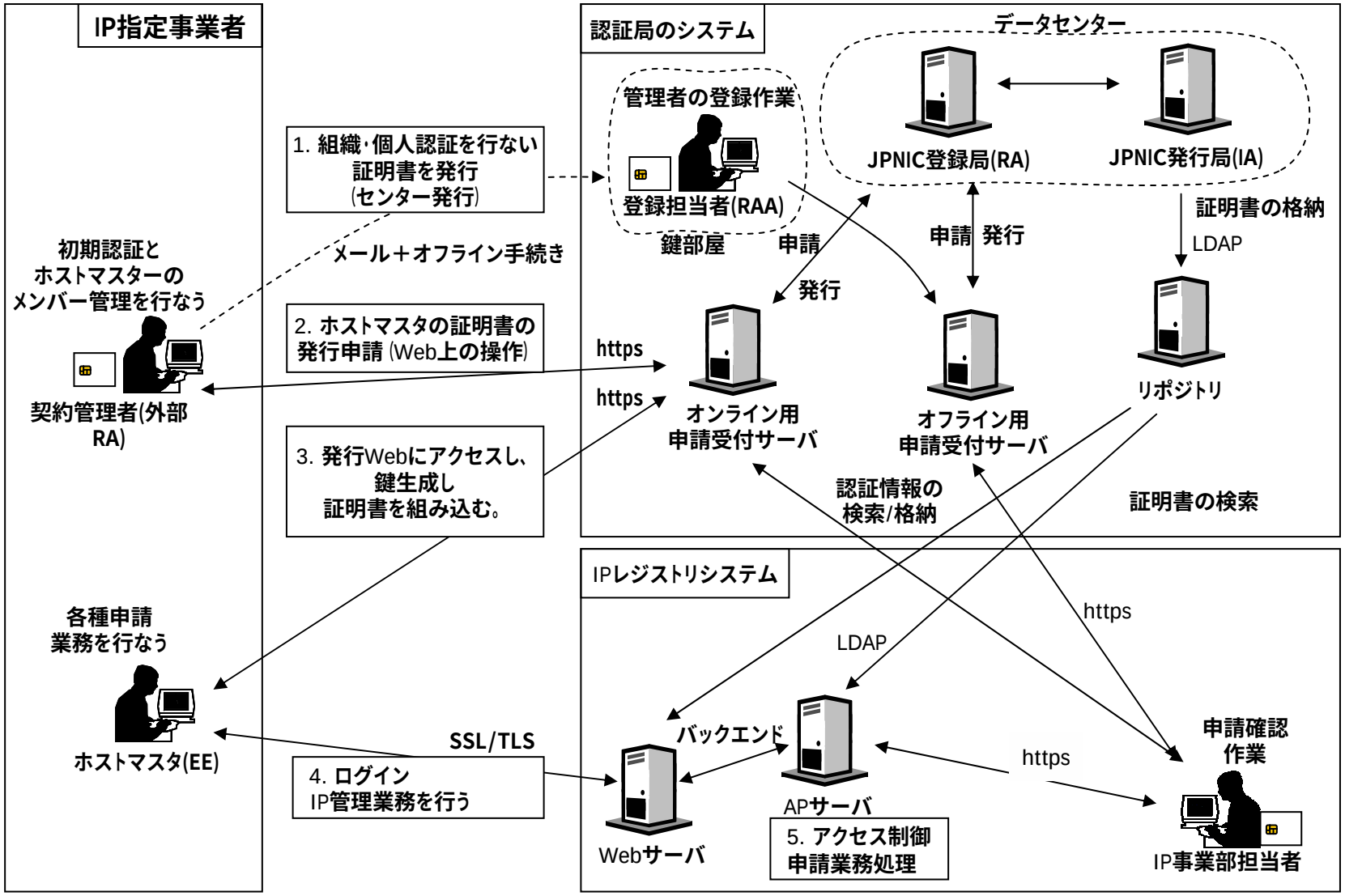
「通知アドレス／Notify」
⇒ 確認手段は存在

JPNIC の認証局 (認証用)

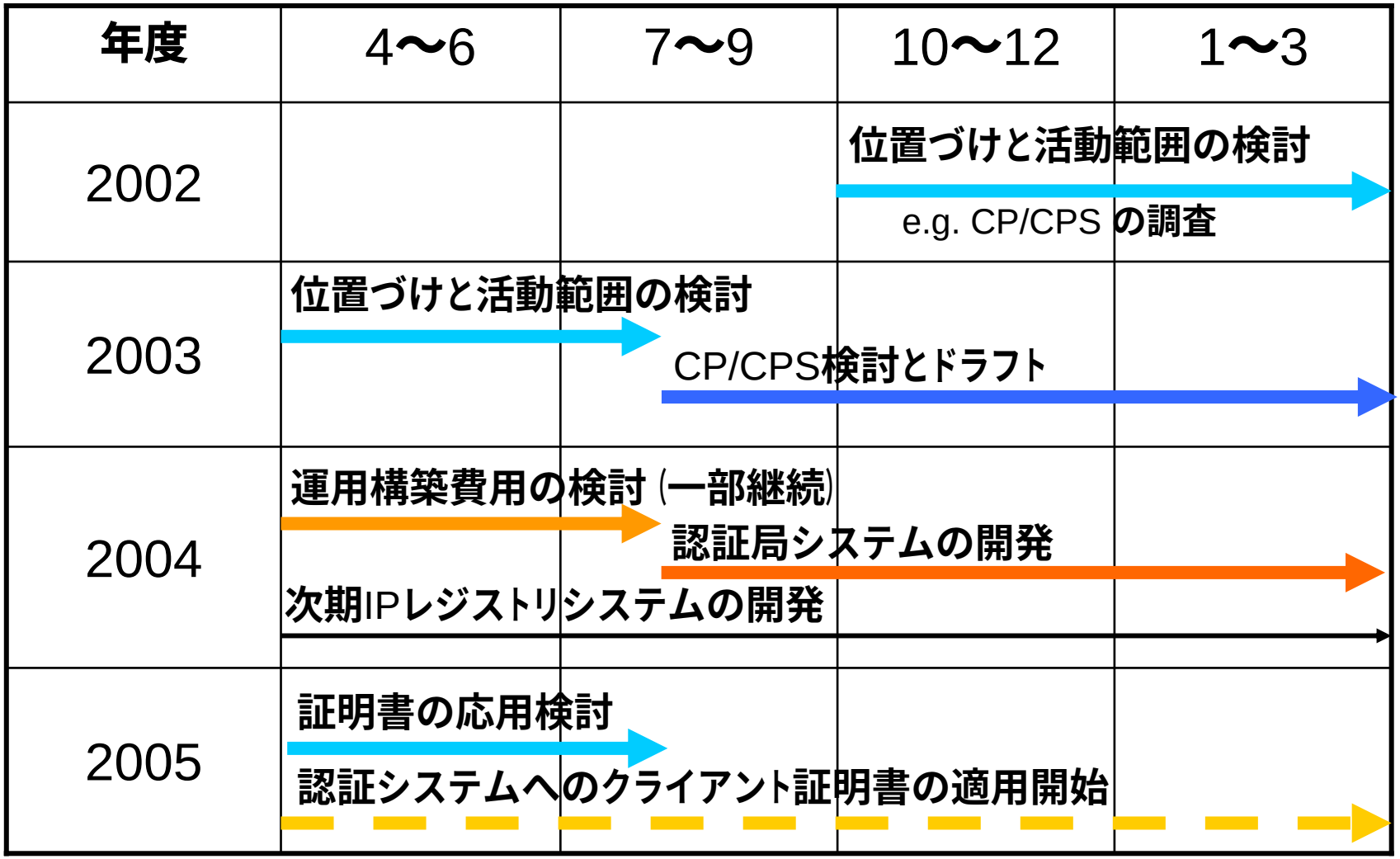


- JPNIC認証局の検討
  - IP指定事業者の申請者／業務担当者にクライアント証明書(X.509)を発行。(2005年に実験導入を予定)
  - 既存のユーザ管理方法と同様に証明書管理
- IPレジストリシステム
  - IP指定事業者向け資源管理Webインターフェース
  - サーバ認証／クライアント認証

認証用認証局の外部RAモデル



活動の時期と今後

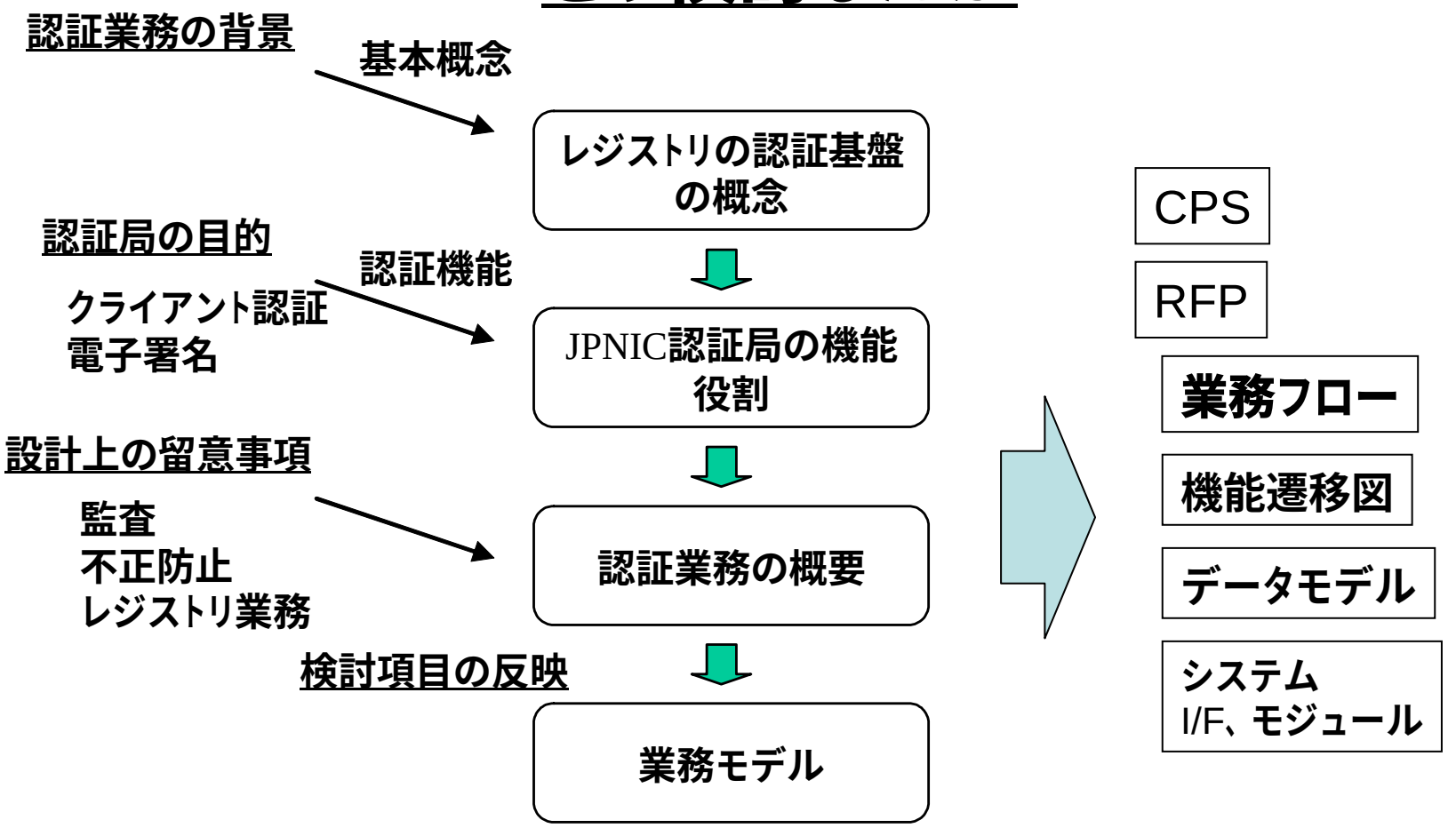

年度
4〜6
7〜9
10〜12
1〜3
2002
位置づけと活動範囲の検討
e.g. CP/CPS の調査
2003
位置づけと活動範囲の検討
CP/CPS検討とドラフト
2004
運用構築費用の検討 (一部継続)
認証局システムの開発
次期IPレジストリシステムの開発
2005
証明書の応用検討
認証システムへのクライアント証明書の適用開始

認証局構築の足掛かり

認証局構築の足掛かり(1)
留意することになった事項

1. 導入の動機を切り分けて考える
   - 認証強化か
   - PKIを使ったサービス拡充か
2. 基本は既存の「認証の意味」を踏襲する
   - 初期登録の確認手順
   - ユーザの権限範囲
3. 認証局の運用費用はピンからキリまで
   - 人件費⇒役割分担の度合い
   - 認証局システム⇒認証サービスの利用も場合によっては高額に。パッケージでライトウェイトにいれる方法もある。
     - 運用費用(人件費／ライセンス費用を含む)のシミュレートは必須

認証局構築の足掛かり（2）
どう検討したか



- 調査研究報告書　http://www.nic.ad.jp/ja/research/200404-CA/
  - 第4章　認証業務の検討
  - 第5章　CP/CPS策定に関する検討

認証というと二言目に
出てくる言葉

外部編 (1)

- 「今のままでも大丈夫なのでは？」
  - 根拠のない安心感

⇒きちんとした「認証」という概念の普及が大事

- 認証はすべてのユーザ・セッションの始まり
  - パスワードで大丈夫か (共通パスワード？)
  - アクセスできるパソコンを限定していれば大丈夫か

  ⇒ ユーザ側へのアプローチ
- 十分に問題を回避できるシステムを提供していたか

  ⇒ 提供側へのアプローチ

外部編（2）

- 「認証を（業務を）変えられるのは困る。」
  - 単なる変化に対する拒絶反応
  - 認証が弱いことはわかっている

⇒ 便利な方に変わるのは困らない ⇒ PKIを利便性に還元（本当はPKIのお陰でなくても）

⇒「方針です」（通用する状況で）

外部編（3）

- 「認証局って言うけど大丈夫なの？」
  - Good question!（困る質問！）

⇒認証局の重さと維持力の問題

- CPSを検討してみる（方針）
  - 大丈夫なレベルを明らかに
- 運用費用をシミュレート（維持）

内部編

- 「コストは誰が持つの？」
  - サービスとの兼ね合い
  - リスク計算（使えるならば）

⇒サービス（業務）部門との協力が大事

認証基盤とは何なのか

SSLブームはPKIか

認証基盤（PKI）って？

- ITU-U X.509、IETF PKIX RFC3280
  - **基本的概念はこれ**
    - **でもインターネット接続組織は必ずしもDirectoryを意識していない。認証ドメインのような「くくり」が複数存在**
  - **今後は「ドメイン同士の接続」か？**
    - **他組織との業務連携：電子文書の交換、業務Webシステム**

- PKI**は流行ってるか** → Resting
  - **"認証"は捨てられない**
  - deployment**は徐々に増えている**
    - ICカード（デュアルインターフェース・カード等）
    - VPN、今後WLAN

- **認証インフラはいるか ⇒ 今後は、いるでしょう**

"方式"か"基盤"か

- PKIを利用する仕組み
  - SSLサーバ認証、IPsec-VPN、Windowsログオン、etc…
- PKIを利用する場面
  - ○ ほか組織のサーバの認証、自組織のサーバ認証
  - △ 自組織のユーザ認証
  - × 他の組織のユーザ認証（？）

⇒「基盤」なのに今は「一つの認証方式」としか使っていない

- 方式：自分の都合で動かして使う
- 基盤：共通に動くものをそれぞれの都合で使う

「基盤」の要素

- **方式**
  - **仕組み**（X.509、RFC3280）**とアプリケーション**
    - **認証のプロトコル**（**証明書プロファイルと検証プロセス**）
    - **通信プロトコル**（SSL、IKE(IPsec)、S/MIME）
    - **ハードウェア**（**ハードウェアトークン**、HSM）

と

- **運用**（**基盤を意識した運用**）
  - **認証局の運用**
  - **サービスの運用**

両方ができて初めて「基盤」
⇒「広く利用（配布）→ 主体的利用」への移行の時期

基盤的認証局の運用

- 誰を信じるべきか ⇒ 認証ドメインと用途

種類	運用主体	用途	アプリケーション	自社用途
商用認証局	民間企業（大企業）	情報入力ほか	Web（一部業務も）	不可能
政府の認証基盤	政府／各省庁	各種申請・入札情報	Web・電子文書	不可能
契約先／取引先の認証局	契約先／取引先	業務連携	Web（業務システム） 電子文書	可能
自社認証局	自社	業務システム	Web・メール・電子文書	可能

検討を要するが、応用性が高く大きな可能性を持つ分野

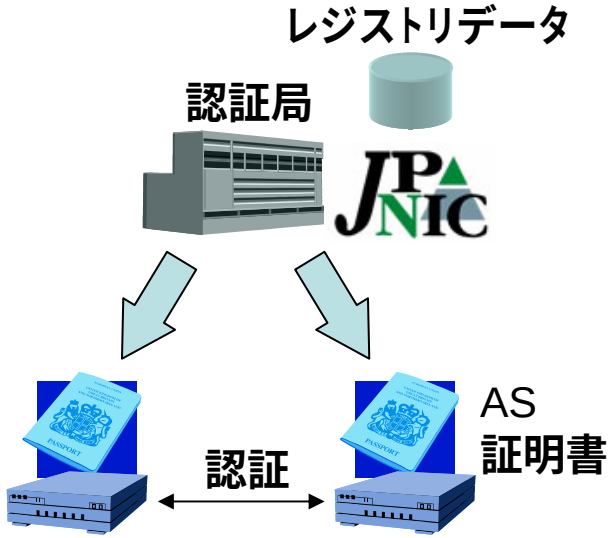
アドレスを使った認証基盤

JPNIC認証局における取り組み

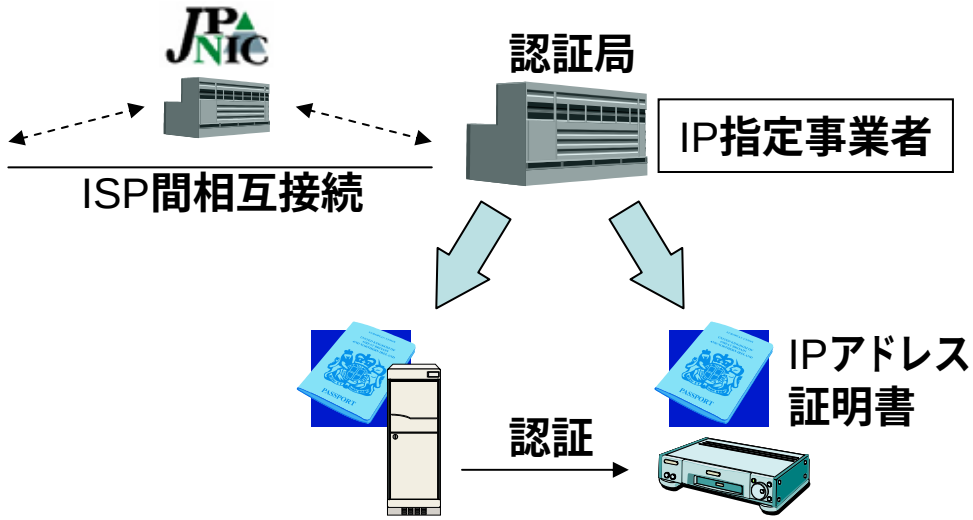
- JPNIC認証局における取り組み
  1. 認証強化の為の認証局構築
     - JPNICにおけるクライアント認証の導入検討
       ⇒ "JPNICにおける認証強化"が目標
  2. レジストリデータと電子証明書の利用検討
     - 認証基盤の調査研究（ASP/ISPによる事業化を含めて）
       ⇒ "IPの通信ノードにおける認証の導入"が目標

アドレスを使った認証基盤

- **認証基盤のアイディア**



AS情報の証明書
- origin の認証



IPアドレス証明書によるノード認証
- 通信時のISPの特定 (P2P, CDN)
- 付帯情報 (地理、運用レベル)

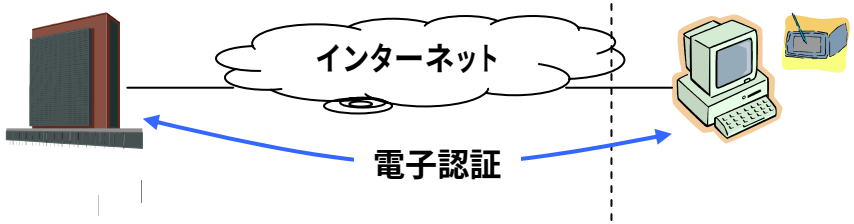
関連プロトコル
- RFC3779
- S-BGP / soBGP
- IPsec

- 家電、地域的な機器の連携などが可能に？
- または相互認証の役割

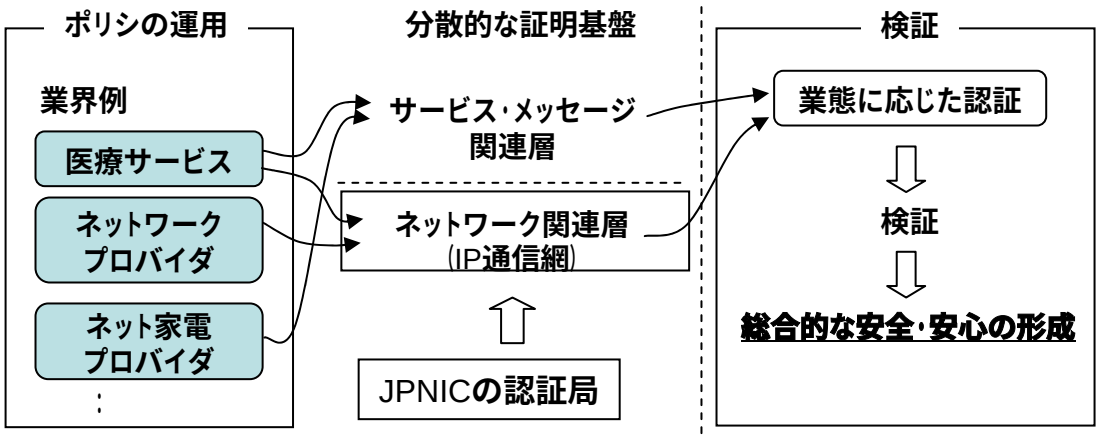
電子認証フレームワーク（アイディア）

電子認証フレームワークの概念

電子認証のイメージ



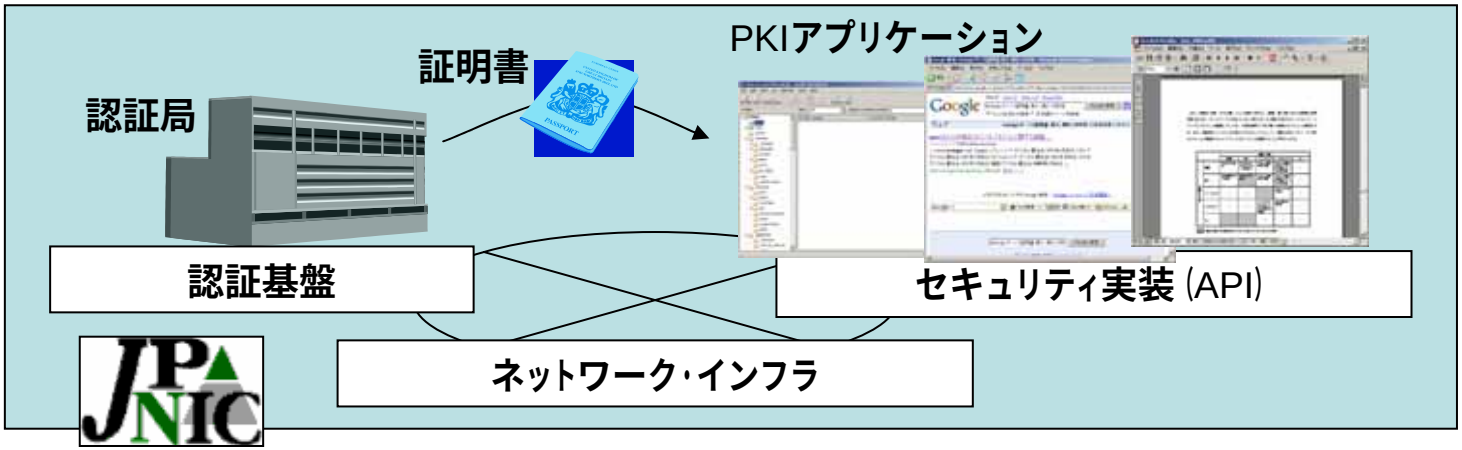
フレームワークの概念



課題

- 共通ポリシ
- 個別ポリシ
- 相互運用性の確保
- 各種属性認証の適用
- 認証基盤（PKI）の普及・啓発

フレームワークの構築イメージ



プリミティブなインフラ

カスタマイズされたインフラ

インフラと認証基盤の運用・各種実験

電子認証フレームワークコンソーシアム (アイディア)

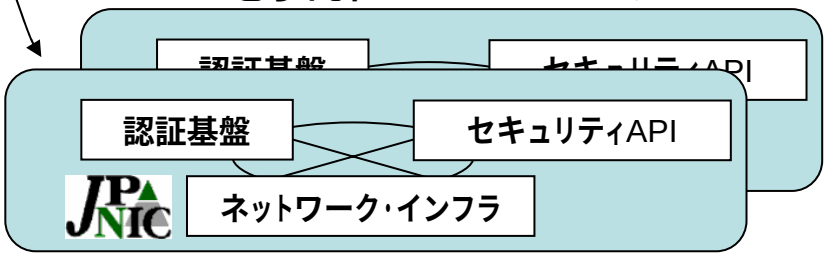
中立的かつ認証基盤の活用が可能な組織

ユーザの立場で電子認証の利用検討

Small Businesses
Companies ISP Home Users
Government

認証基盤の利用分野

電子認証フレームワーク



実装、制度面での適用、運用
利便性の高い電子認証アプリケーションの出現

まとめ

- JPNICの認証局の事例紹介
  - レジストリの認証局
  - 発行モデル、CP/CPS
- 認証基盤としてのPKI
  - アドレスを使った認証基盤
  - 電子認証フレームワークのアイディア

これからも認証はなくならない ⇒ 認証モデルを作ったものが勝者
今後の認証事業を一緒に考えてみませんか

ご清聴、ありがとうございました。

社団法人日本ネットワークインフォメーションセンター