電子認証プラクティスフォーラム

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(JPNIC)
セキュリティ事業担当　木村泰司

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

お話の前に・・・

- (社) 日本ネットワークインフォメーションセンター
  - 国内のISP (IPアドレス管理指定事業者) 約380社にIPアドレスの割り振りを行っている所です。
  - インターネット基盤整備事業
    - Internet Week (12月のイベント)、メールマガジン
    - 登録情報(IPアドレス)関連のセキュリティ(調査研究)

	認証局	電子証明書の種類
2005年～	指定事業者認証サービス ⇒ ユーザ認証の強化	認証用 (ICカード、https)
2007年～	経路情報の登録認可機構 ⇒ 認証と認可 (Web利用)	認証用、電子署名用 (USBトークン、S/MIME)

今日のお話

- 私たちは電子認証技術を「きちんと」使えているか
- 「プラクティス」
- ノウハウをドキュメント化しよう

私たちは電子認証技術を「きちんと」使えているか

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

様々な認証技術

- 記憶に基づくユーザ認証
  - 暗証番号、パスワード
- 生体に基づくユーザ認証
  - 指紋認証、静脈認証
- モノに基づくユーザ認証
  - ICカード

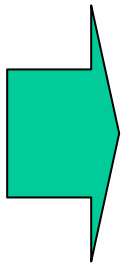
- 複合的なユーザ認証
  - 磁気カードを使った認証
  - OTP (One Time Password)

PKIはインフラ技術

使い方はシステム開発サイドに任されがち。

認証技術のリスクと“キメ”の問題

	リスク	キメが必要な部分
暗証番号、パスワード	忘却対策のリスク 偽装サイト オンライン攻撃	パスワードはつけ方は？ 新規パスワード発行の方式は？
生体認証	フォルスネガティブ 生体情報の漏洩	偽造の検知 生体情報の漏洩対策
モノに基づく認証 （IDカード類）	利用環境の問題 実装のハードル（技術情報が少ない）	モノの偽装対策



どうしたらいいの？

認証技術には技術に集約される問題と、運用上の問題の二種類がある。
運用上の問題は、対処方法はまちまちで、何をどこまでやればいいのか、わかりにくい。

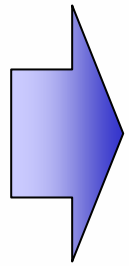
PKI　ー　いまあなたに必要なのは“標準”よりも“キメ”です

いまある課題

	リスク	キメの部分
失効検証	検証における「失効」ができない 使い勝手が悪くなる	無効化システム（認証） 電子署名の場合は..?
認証局の継続運用	技術的に継続できなくなる キーセレモニーの頻発	認証局証明書の有効期限

この先の課題

	リスク	キメの部分
証明書プロファイル	レベルの玉石混交 （EV SSLは第一歩?）	RA業務 v3拡張フィールド クリティカリティ
相互認証	抜け穴（レベルの低下）	？



深遠なる世界

ガイドライン　技術標準　要件

- **米国**
  - E-Authentication
    - **米国電子政府における認証のためのガイダンス等を公開**
  - NIST SP800 **シリーズ**
    - **米国国立標準技術研究所による政府のためのガイドライン等**

- **参照**
  - **日本**PKI**フォーラム**（PKI-J）**閲覧可能資料一覧**
    - http://www.japanpkiforum.jp/shiryou/list_shiryou.htm
  - **情報処理推進機構**（IPA）
    - http://www.ipa.go.jp/security/publications/nist/
  - E-Authentication site
    - http://www.cio.gov/eauthentication/
  - NIST Computer Security Division(CSD) Computer Security Resource Center - Publications
    - http://csrc.nist.gov/publications/

標準化活動と実装

- IETF PKIX WG's RFC
  - 2528 Key Exchange Algorithm (KEA)
  - 2560 Online Certificate Status Protocol (OCSP)
  - 3029 Data Validation and Certification Server (DVCS)
  - 3161 Time Stamp Protocol (TSP)
  - 3281 Attribute Certificate Profile
  - 3379 Delegated Path Validation and Delegated Path Discovery Protocol (DPV/DPD)
  - 3647 CP and CPS
  - 3709 Logotypes
  - 3739 Qualified Certificates (QC)
  - 3779 IP addresses and AS Identifiers
  - 3820 Proxy Certificate

標準化活動と実装 (cont'd)

- IETF PKIX WG's RFC
  - 4059 Warranty Certificate Extension
  - 4043 Permanent Identifier
  - 4055 Additional Algorithms for RSA Cryptography
  - 4158 Path Building
  - 4210 Certificate Management Protocols (CMP)
  - 4211 Certificate Request Message Format (CRMF)
  - 4334 PPP and WLAN
  - 4386 Repository Locator Service
  - 4387 Certificate Store Access via HTTP
  - 4476 AC Policies Extension
  - 4491 GOST

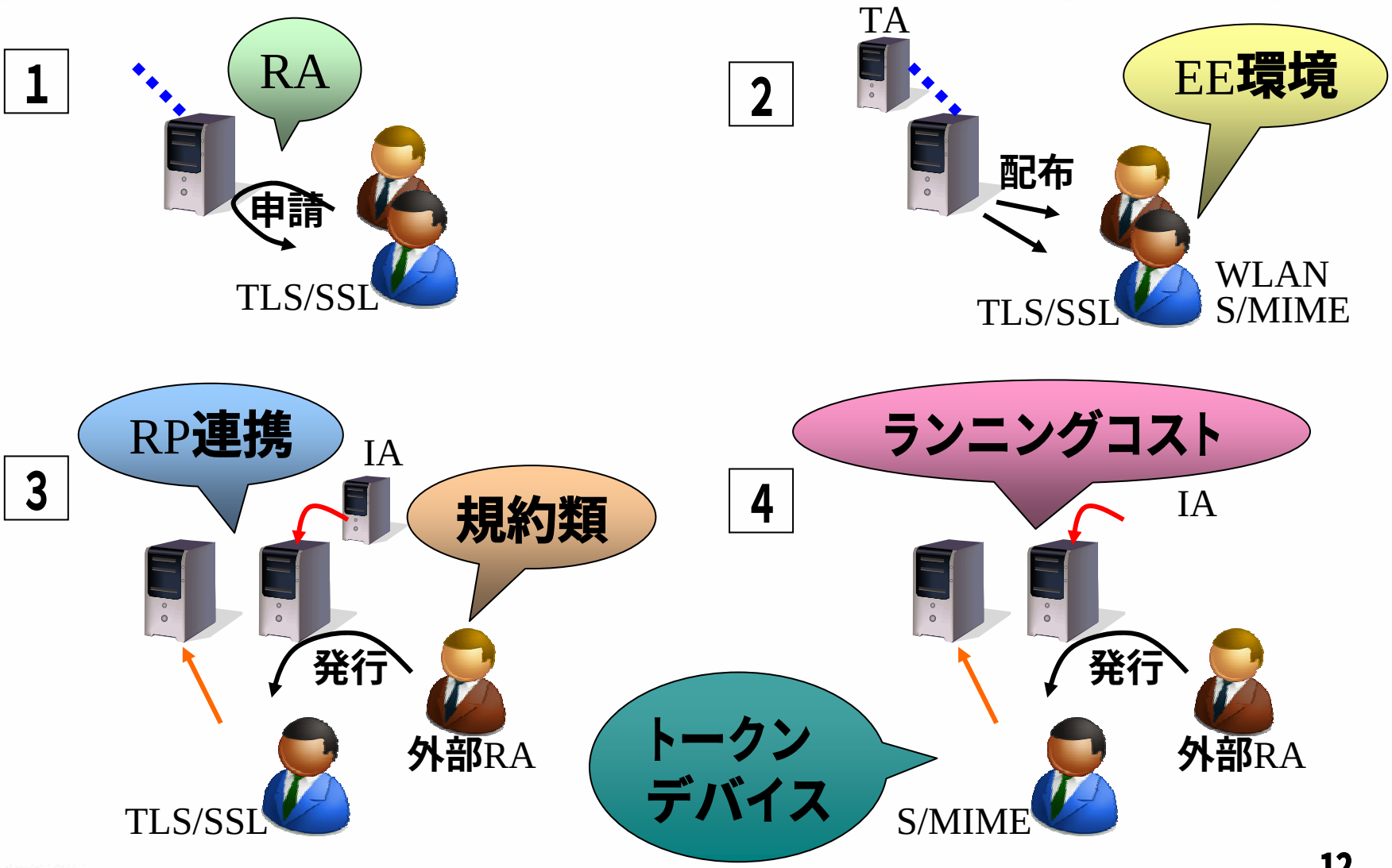
標準化活動と実装 (cont'd)

- IETF PKIX WG's RFC
  - 4683 Subject Identification Method (SIM)
  - 4985 Service Name
  - 5019 OCSP for High-Volume Environments
  - 5055 SCVP
  - 5280 Certificate and CRL Profile
  - 5274 CMS (CMC): Compliance Requirements
  - 5273 CMS (CMC): Transport Protocol
  - 5272 Messages over CMS

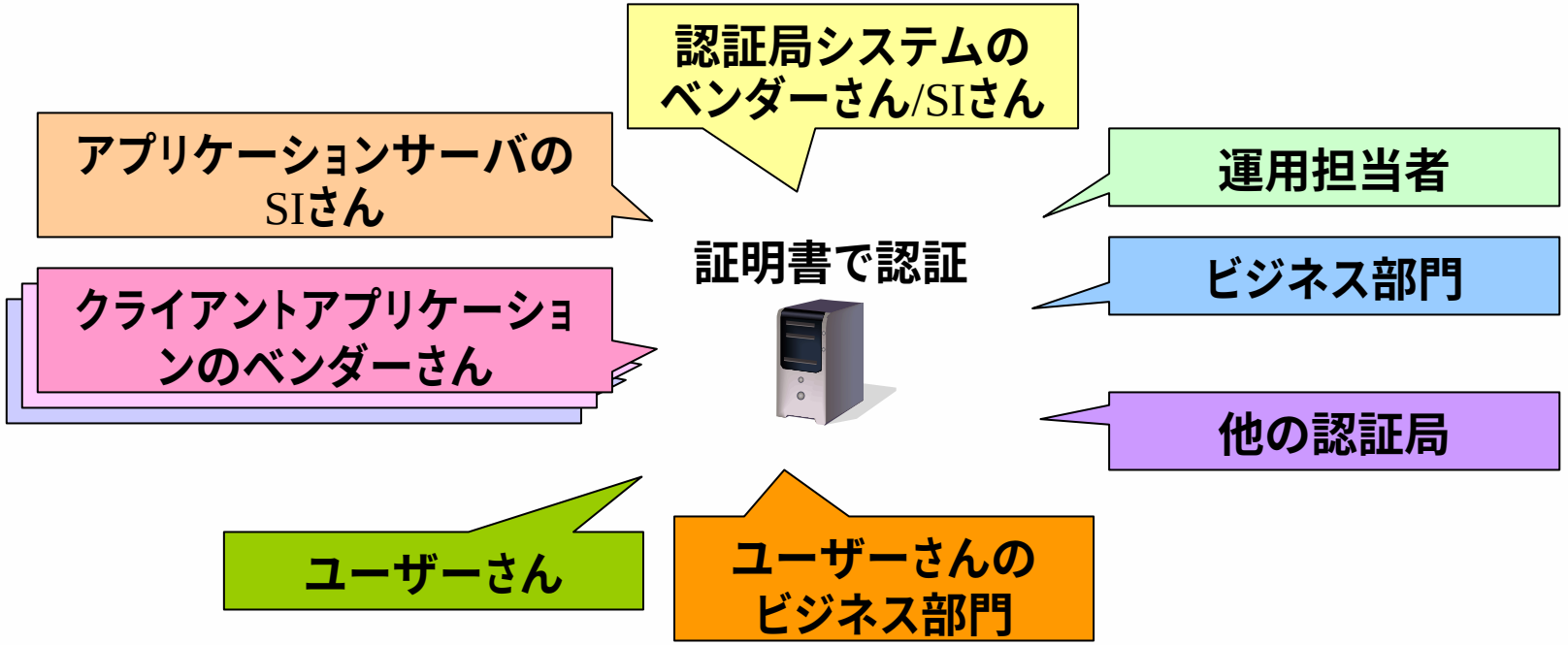
「プラクティス」

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

私が関わってきた認証局と、悩み



電子認証にかかわるプレーヤー



- **電子認証の課題には共通課題が多く、みんなで解決して共通認識を作らないと、本当の解決にならない。**

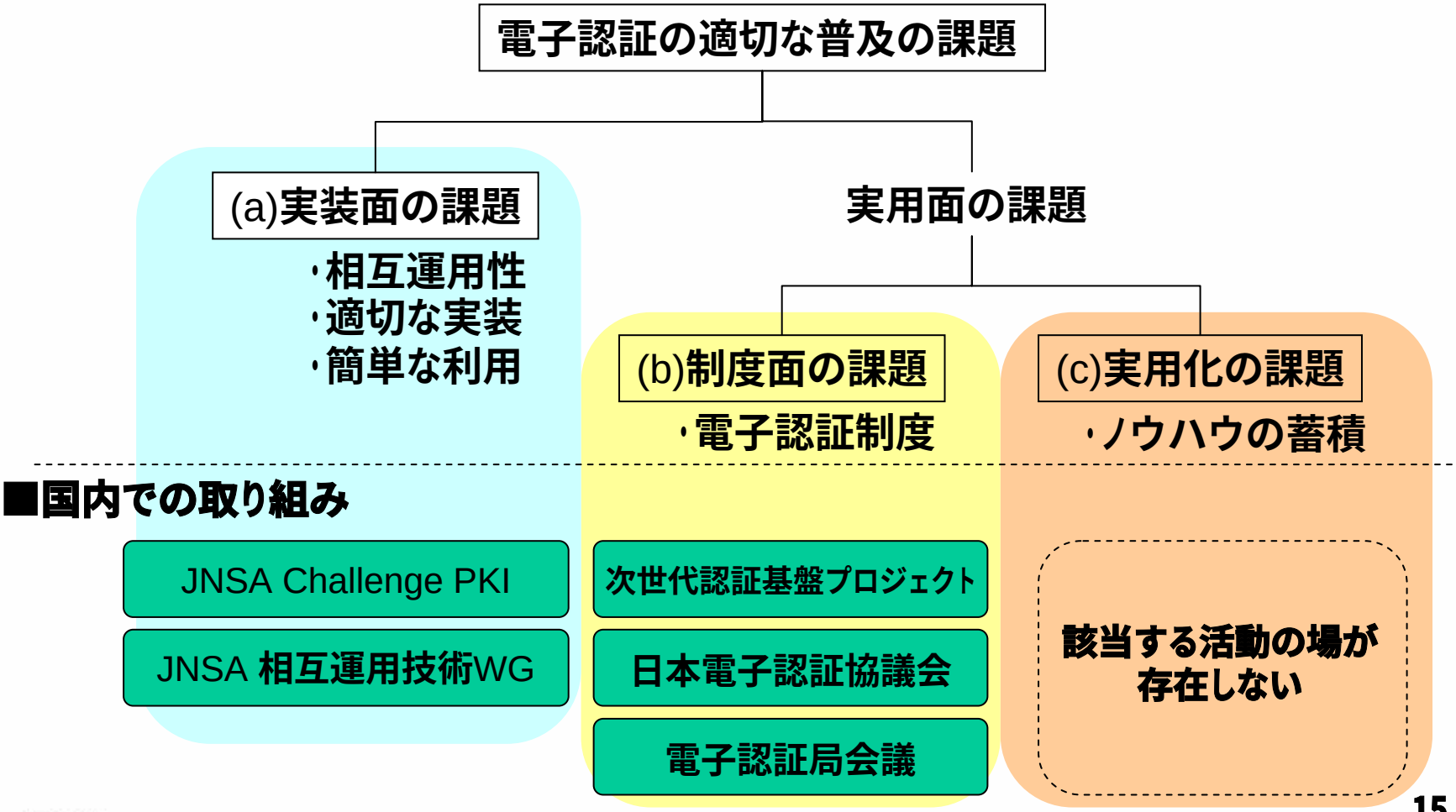
とはいっても、

- 電子認証技術の実装技術は複雑で適切な実装／適用／利用を行いにくい
  - 特に*技術的な*相互運用性の確立には大きな課題が存在

- 「パブリックなノウハウ」を蓄積する場がない
  - 電子認証技術、特にPKIについては「より高度な技術の標準化」よりも「適用や利用のノウハウ」の方が適切な普及に寄与
  - IETFにおけるBCPとも位置づけが異なる
    - IETFは「プロトコルのドキュメント化」の場

電子認証技術の普及の課題

■電子認証の適切な普及の課題の分類



■国内での取り組み

ノウハウをドキュメント化しよう

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

電子認証プラクティスフォーラム

- 概要
  - 電子認証の適切な普及と発展を図るため、電子認証に関わるノウハウをBCP(Best Current Practice)として文書化し策定する活動
    - ノウハウを持ち寄る ⇒ 文書化して煮詰める ⇒ 認識共有 ⇒ 最善な利用／構築／運用 ⇒ 普及
    - できた文書は参照情報であり、強制力を持つものではない
    - ノウハウの利用は自己責任で行う
  - 2007年度は、経済産業省からの委託事業として実施
    - 調査研究事業(*1)の一環として実験的に行う。
      (*1)「平成１９年度電子認証フレームワークとIPアドレス認証の展開に関する調査研究に関する委託契約」

本フォーラムで扱うトピック

- 電子認証技術に関わるノウハウや考察の結果
  - 技術利用や技術理解に関わること
  - 実装の現状に関わること
  - 技術仕様や実装のあるべき姿の提案
    - 現状や実績を踏まえて

  など

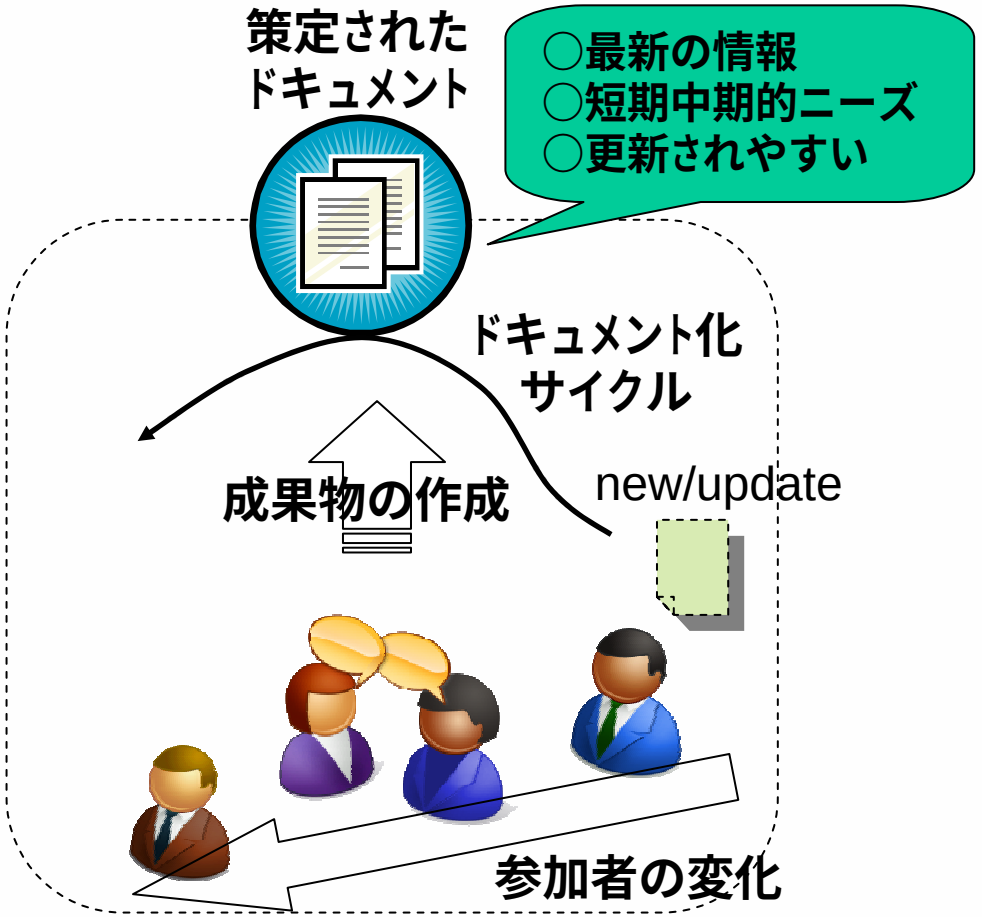
  - 特定の興味を持つグループ（SIG）の中で、議論することのコンセンサスが得られたもの

ノウハウの蓄積と公開（1）

調査活動を通じたノウハウの蓄積と公開の構造

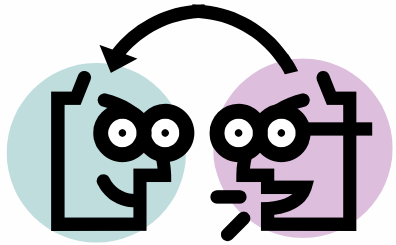
ノウハウの蓄積と公開 (2)

会議体におけるノウハウの蓄積と公開の構造



ドキュメント化活動の考え方

- 重視する考え方
  - ラフコンセンサスを重視
  - 現場の現状に基づいた知識
  - 議論と成果の公開



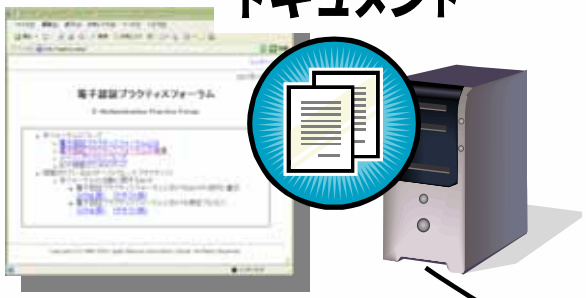
- 技術を*標準化*する活動ではない
- 参加者は所属組織を代表するものではない
- 各自の現時点で最善のノウハウを文書化し共通認識化することに最も重点を置く

電子認証プラクティスフォーラムの仕組み

1. ノウハウの蓄積

コミュニティにおける提案と議論

(コミュニティの範囲内で最良のノウハウを明確化)



ドキュメント

投稿

2. ノウハウの普及、共通認識の形成

ノウハウの利用、実装やサービスの改善、相互運用性 (整備された技術) の確保

入手

コミュニティの範囲
(ラフコンセンサスの範囲)

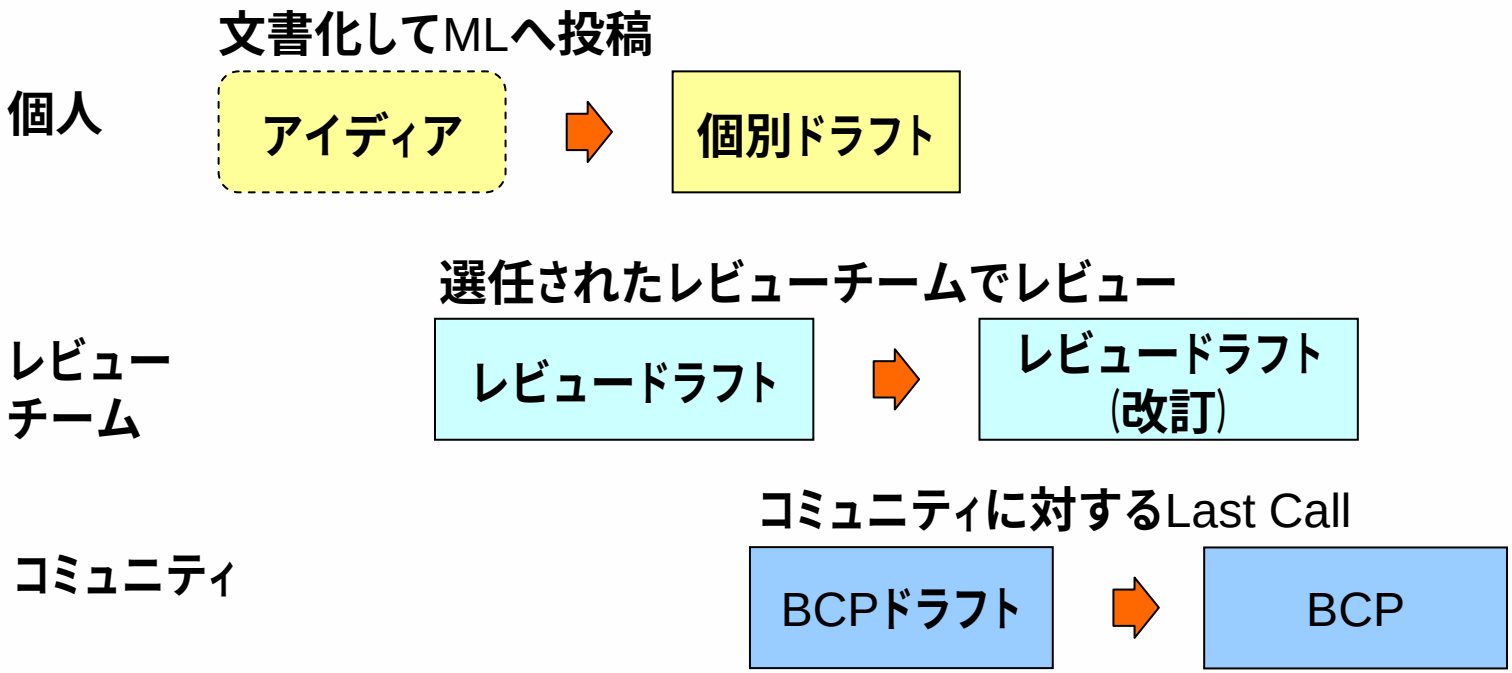
提案者

議論の参加者

フォーラム (ML) 参加者

一般ユーザ

電子認証プラクティスフォーラムにおける ドキュメンテーション・プロセス



2007年度の実験的な活動

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

電子認証フレームワーク　2007年度の活動

- 2007年11月19日 InternetWeek2007（JPNIC主催のインターネット技術者向けイベント）期間中、電子認証プラクティスフォーラムBoFを実施した。
- BCPとなるドキュメント案を収集し、ドキュメントのレビューチームを構成し活動した。

▼電子認証プラクティスフォーラムBoF 開催概要
- ー日時：2007年11月19日(月) 18:00-19:45
- ー参加者数：29名
- ー場所：秋葉原コンベンションセンター

▼アジェンダ

- ー電子認証プラクティスフォーラムの紹介
- ー電子認証技術のノウハウに関するディスカッション
  - **認証局証明書の更新が与えるユーザアプリケーションへの影響の調査**
    (富士ゼロックス 横田智文氏)
  - **PKIにおけるマルチドメイン問題**
    (セコムIS研究所 島岡政基氏)
- ー電子認証ブレインストーム
  (電子認証技術の「使いにくいところ」を洗い出す)

▼行われた議論
- ー**暗号アルゴリズムの移行問題**
- ー**PKIのICカードのあり方**
- ー**組み込み型機器のPKI**　ほか

▼アンケート結果
- ーフォーラムへの参加について
  - 是非参加したい 13%
  - 前向きに検討したい　63%
  - 参加には検討を要する　13%
- ー本フォーラムの活動について
  - **意義深く重要**　77%
  - 意義は薄く不要　0%
  - その他

▼参加者から頂いたご意見
- ーフォーラムの背景で言われている通り、ノウハウの蓄積の場が少ない。
- ー**情報のリポジトリ、情報共有の場でもあってほしい。**

BoFの様子

ドキュメント(1)

- 「中間認証局の証明書更新が与えるPKIアプリケーションへの影響」
  - 富士ゼロックス株式会社　横田智文氏
  - クライアント環境における、認証局証明書の更新の影響を調査
    - どうすれば「EE証明書が検証できない」「間違えて新証明書を消してしまった」などの問題が起こらないように更新できるか {更新時期 / DNの変更 / 鍵変更 / 旧証明書の破棄}

⇒ 答えは、ドキュメントを参照
bcp-draft-intercacertupdate-01.txt

ドキュメント(2)

- 「認証局における鍵更新のタイムチャート」
  - 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
    木村泰司
  - 認証局における鍵更新のタイミングを図示
    - いま使っている私有鍵は何年後まで使える？
    - 次のキーセレモニーは何年後までにやる必要がある？
    - EE証明書の種類を増やすときに気をつけるべきことは？

⇒ 答えは、ドキュメントを参照
bcp-draft-certchart-02-rev02.txt

ドキュメント (3)

- 保証レベルとポリシ管理機関による適切なポリシマッピングの実現
  - セコム株式会社　島岡政基氏
  - ポリシマッピングによって起こる「伝言ゲーム問題」の回避策
    - 証明書ポリシは認証局によって違う
    - 複数のマッピングをしていくと・・・レベルの低いものと「マップ」されてしまう　⇒　伝言ゲーム問題
    - どうすれば防げるの？

⇒ 答えは、ドキュメントを参照

bcp-draft-appropriate-policymapping-01.txt

今後の活動

- 2008年度　趣意書案
  - JPNICの中の活動として、趣意書を書き直した。

    - 目的：ドキュメント化　＋　情報交換
    - 活動：ミーティング　＋　ML　(2007年度と同じ)

    - 電子認証プラクティスフォーラム Webページ
      - http://eapf.nic.ad.jp/
    - EAPFメーリングリスト
      - eapf@eapf.nic.ad.jp
        - » 加入するには eapf-join@eapf.nic.ad.jp へ空メール
    - 次回のミーティング (第1回)
      - 8月中旬

ご静聴ありがとうございました。

JPNIC 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