JPNICのセキュリティ事業について

2003年3月7日

総会講演会

㈳ 日本ネットワークインフォメーションセンター

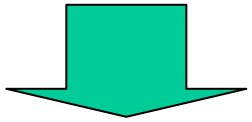
佐野　晋/山口　英

なぜセキュリティ事業か

- 2001年9月　米国同時多発テロ
- 2001年11月　ICANN年次総会(Marina del Rey)

  ㈱参考㈱ ICANN DNS Security Update #1(翻訳文)
  http://www.nic.ad.jp/ja/translation/icann/20020104.html

  – ドメインネーム及びアドレスの割り当てシステムのセキュリティが主要議題
  – 確認事項：インターネットが依存しているドメインネームとアドレスのサービスの保護を強固にしていく必要性がある



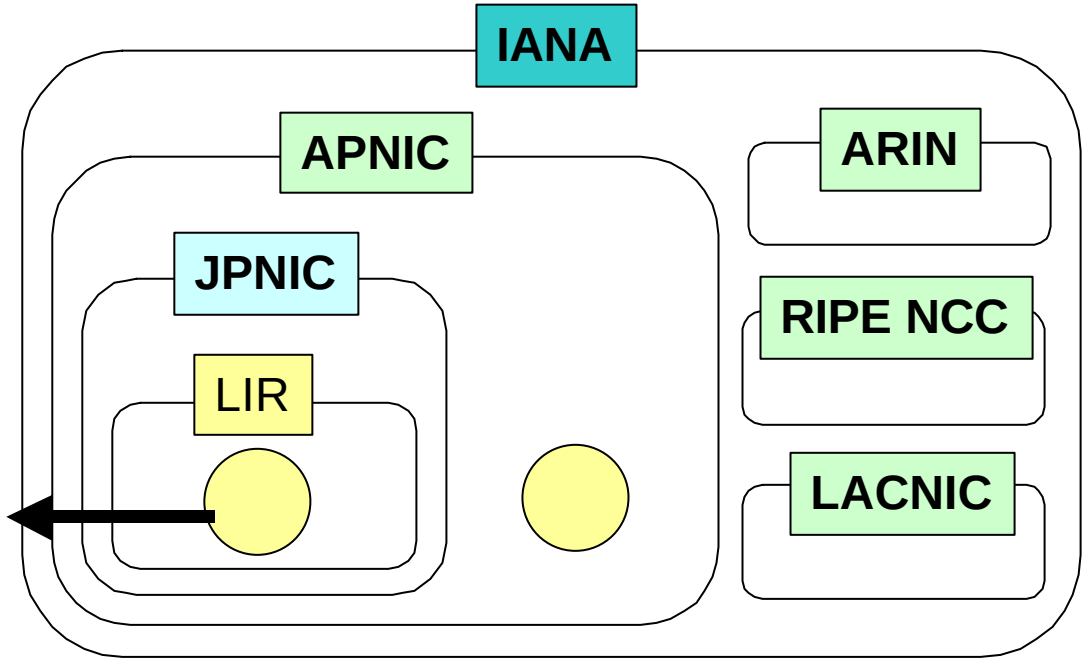
  – 各NIR (National Internet Registry)もレジストリセキュリティを高める必要がある
  – CSIRTなどとの連携が重要

レジストリデータベースのセキュリティを高めるには(1)

- 登録情報の安全性と信頼性の確立
- 堅牢な認証局の運用
- 公開鍵証明書を利用した各種認証

日本のNIR

- IPアドレスの範囲(JPNIC)
- jpドメイン(JPRS)



日本に実在する組織が割り当てられるアドレスの範囲

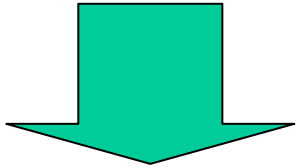
レジストリデータベースのセキュリティを高めるには(2)
～なぜNIRによる認証が必要なのか～

- 日本の組織の持つネットワークリソース（IPアドレス／ドメイン名）を証明する基盤の提供が目的
- PKIを用いたドメイン、および、IPアドレスの認証を実施する基盤が生まれつつある
  - DNSSEC
  - IPsec / IKE
- しかし現状では、アドレス或いはドメイン名と対応付けられたPKIが存在しないため、インターネットの認証基盤の成立が阻害されている(これは既存のCAサービスではカバーされていない分野である)
  - PKI　(Public-Key Infrastructure)
    - 公開鍵証明書による識別子(DN)と値(field and value)の関連付け
    - SSL, IPsec における利用が可能
  - CA　(Certification　Authority)　認証局

レジストリデータベースのセキュリティを高めるには(3)
～なぜ独自の認証局(CA)?～

- JPNIC / JPRS のサービス提供形態から、個人および法人を対象としたPKIサービスを構成する必要がある
  - 特定認証業務事業者だけでは不十分
  - 法務省CAとの連携は現時点では実質的に不可能

- 他国のCAに依存することはJPNICにとってデメリットが多い
  - わが国のインターネットコミュニティに対するサービスが、他国のCAに依存するような構造は望ましくない



独自CAが必要

レジストリデータベースのセキュリティを高めるには(4)
～NIRと他組織との連携～

- CAのたちあげのみならず、CSIRT等の他組織との連携による情報の共有が必要
- CSIRTとは
  - Computer Security Incident Response Team の略で「コンピュータセキュリティ・インシデント」に対応する活動を行う組織体の一般名称
  - 「コンピュータセキュリティ・インシデント」とは
    - コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの（その疑いがある場合)を含む
    - 例えばリソースの不正利用、サービス妨害行為、データの破壊、意図しない情報の開示やさらにそれに至るための行為(事象)など
      - 出典：コンピュータ緊急対応センター(JPCERT/CC)　FAQ
      - http://www.jpcert.or.jp/faq.txt

JPNICのこれまでの取り組み(1)

- 2002年4月
  - インターネット推進部にセキュリティ事業準備室開設
  - 経緯： NIRとして、会員並びに指定事業者が権利を行使し、義務を履行するときの正しさの証明をする基盤をつくることが責務である

- 2002年10月～2003年3月
  - NIRにおけるルートCAの立ち上げに向けた調査研究の開始
  - Feasibility Study として

JPNICのこれまでの取り組み(2)
～NIRとしてのCAのFeasibility Studyとは～

- NIRとしてのPKIサービスの要求条件の明確化
  - 技術的要件
  - 運用条件
  - 事業化要件
- IPsec、DNSSEC等のPKIサービスを利用するアプリケーションからのCAに対する技術要件の明確化およびプロトコル標準化状況の調査
- 先行事例の調査
  - APNICのPKIパイロット・プロジェクトの調査
  - RIPE NCCの現状調査

2003年度のセキュリティ事業

1. JPNICにおけるCAサービスの開発
2. 教育・普及活動

} 2本立て

1. JPNICにおけるCAサービスの開発(1)
～CAの構成(案)～

- Root CA として構成
  - 他のCAに依存しない構造ができれば望ましい
  - 厳格なCAの運用が必要
- Internetにおける相互運用性を確保
  - X.509 profile としては他の Internet Registry が採用している profile を精査し、相互運用性を確保する
- 他の Internet Registry との相互認証について
  - 当面はCross Certificationの実施は行わない
  - ICANNなど国際調整機構のからの勧告が出た場合には追従
- 使用する技術
  - できる限り特定のベンダ等に依存しない構造を確立
  - 将来の技術変動に追従できるような体制を確保
  - ソフトウェアの独自開発を目指す
  - 国産技術へのフォーカス

1. JPNICにおけるCAサービスの開発(2)
～開発スケジュール(案)～

1. **PHASE1(2002年度): 調査・基礎研究**
2. **PHASE2(2003年度): 開発**
3. **PHASE3(2004年度): 試験運用**

1.JPNICにおけるCAサービスの開発(3)
～運用上の課題～

- 厳格な運用を伴うRoot CAを構成
  - セキュリティ面での各種条件をクリアした運用施設の確保
  - CPS(運用規定)の策定
  - 運用体制の検討
- 技術への追従性確保
  - 当面は DNSSEC, IPsec をターゲットに技術検証を実施
  - しかしながら副作用として S/MIME やサーバ認証などでも利用される可能性が高い
  - 継続的な技術調査と運用ノウハウの蓄積が必要
  - 基礎となる暗号技術についても知見蓄積が必須

2. 教育・普及活動
～セキュリティ・セミナーの開催～

- 目的
  - JPNIC会員をはじめとするインターネットコミュニティへのサービスの一環としてセミナーを開催し、情報提供をする
- 方法
  - 年3～4回程度の開催を想定
  - コンテンツ及び講師は、JPCERT/CC等のCSIRTとの連携にて調整
- 対象
  - 原則として会員
- 想定される内容案
  - ISPにおけるセキュリティマネージメント等