JPNIC データベースへの認証機能導入について

JPNIC データベース検討部会

戸田 洋三 (千葉大学, db-wg 外部スタッフ)

発 表 概 要

- JPNIC の事業概要
  - IP アドレス割り当て
  - ドメイン割り当て
- JPNIC データベース
  - データベースの更新作業
  - 登録・情報提供業務の現状
  - 問題点と対策
- ICAT との共同研究
  - 認証機能の導入
  - JPNIC CA
  - 運用規定の検討
- 導入計画 (案)

JPNIC の事業概要

- 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
- 1993 年 3 月任意団体として設立, 1997 年 3 月社団法人化
- コンピュータネットワークの円滑な運用をはかる
- ★ ネットワーク資源の登録管理・情報提供・国際調整機能

  (ドメイン名・ IP アドレス割り当てなど)
- ネットワーク利用技術の調査研究
- ネットワーク利用に関する普及啓蒙活動
- . . . . . .

IP アドレスの割り当て

- IP アドレスはネットワークに接続するホストの識別子
- 重複しないように割り当てる
- 世界中のさまざまな組織からなる階層的管理
  (CIDR ブロックの割り当て)

$$\mathrm{IANA} \rightarrow \mathrm{RegionalNIC} \rightarrow \mathrm{NationalNIC} \rightarrow \mathrm{ISP}$$

ドメイン名の割り当て

- **人間に分かりやすいホスト名，メイルアドレス，URL などを構成する**
- **DNS ネームサーバによる分散データベースの仕組み**
- **世界中のさまざまな組織からなる階層的管理**

  (JPNIC は "jp." ゾーンのデザイン・割り当てを行なっている)

JPNIC データベース

- **ドメイン情報**
- **ネットワーク情報**
- **ホスト情報**
- **個人情報**
- **会員情報**
- **接続情報**
- **コミュニティ情報**
- **AS 情報**

(JP ゾーンのネームサーバはこれらの情報をもとに設定される*)*

```
aohakobe:yozo% whois -h whois.nic.ad.jp. icat.or.jp
[ JPNIC database provides information on network administration. Its use is   ]
[ restricted to network administration purposes. For further information, use ]
[ 'whois -h whois.nic.ad.jp help'. To suppress Japanese output, add '/e' at   ]
[ the end of command, e.g. 'whois -h whois.nic.ad.jp xxx/e'.                  ]

Domain Information: [ドメイン情報]
a. [ドメイン名]                 ICAT.OR.JP
f. [組織名]                     認証実用化実験協議会
g. [Organization]               Initiatives for Computer Authentication Technology
h. [郵便番号]                   105
i. [住所]                       港区芝公園 3-5-8(財) 日本情報処理開発協会内
j. [Address]                    3-5-8 Shibakouen,Minato-ku Tokyo 105 JAPAN
k. [組織種別]                   任意団体
l. [Organization Type]          Non-profit organization
m. [登録担当者]                 MO140JP
n. [技術連絡担当者]             MO140JP
v. [経理担当者]                 MO140JP
p. [ネームサーバ]               icat.icat.or.jp
p. [ネームサーバ]               ns1.iij.ad.jp
s. [使用 IP ネットワーク]       202.214.156.0
[状態]                          Connected
[登録年月日]                    96/03/07
[接続年月日]                    96/04/05

[最終更新]                      96/04/09 13:52:15 (JST)
                                otani@iij.ad.jp
aohakobe:yozo%
```

データベースの更新作業

申請内容の伝達

$$(\text{ユーザ}) \Longrightarrow \text{ISP} \Longrightarrow \text{JPNIC}$$

確認作業

担当者本人か?

必要なデータがはいっているか?

矛盾はないか?

エントリ更新

通知

$$(\text{ユーザ}) \Longleftarrow \text{ISP} \Longleftarrow \text{JPNIC}$$

登録業務と情報提供業務の現状

- 登録件数 (1998 年 3 月 1 日現在)

ドメイン情報	38,547
ネットワーク情報	30,051
ホスト情報	20,499
個人情報	61,540
AS 情報	138
.....	

- 申請処理件数

1997 年 12 月分:	12,208 件
1998 年 1 月分:	11,433 件
1998 年 2 月分:	11,364 件

- whois による検索件数

1997 年 12 月分:	730,490 件
1998 年 1 月分:	738,127 件
1998 年 2 月分:	678,465 件

現状の問題点と対策

- 作業量増大
- 無制限な情報公開による弊害 (個人情報の収集など)

- 機械的処理による効率化 $\Longrightarrow$ **申請者認証**
- 公開情報のアクセス制御 $\Longrightarrow$ **データベース利用者の認証**

ICAT との共同研究

- 認証技術導入に関する検討
- JPNIC CA 設立の検討
- 運用規定の検討

認証機能の導入

更新申請者がデータの担当者本人であることを確認するには?

- **JPNIC ハンドル保持者個々に鍵が必要?**
  (1998 年 3 月 1 日現在の個人情報登録件数 61,540 件)
- **鍵発行手順?**
- **アルゴリズム・形式は?**
  (楕円曲線暗号, RSA, . . . , MOSS, PGP, S/MIME, . . .)
- **どんなツールを使うの?**
  PEMCAT, PGP, NS, IE, . . .

whois データベース利用者の認証?

- **どのような制御をするのか?**
  (レコード毎・情報全体, 本人のみ・ハンドル保持者・登録制など)
- **認証手順?**

JPNIC CA

- JPNIC ハンドルと鍵との対応を証明
- JPNIC による直接証明?
  業務委任会員などを通じた間接証明?
- どの程度のパワーのマシンが必要か?
- どんな実装を使うか? (ICAP?)
- 業務委任会員との間で階層化 CA を構成?
- 認証局全体の外注の可能性?

運用規定の検討

- JPNIC 内部での鍵の扱い方
- JPNIC CA に登録してある鍵をよその用途に使ったら?
- . . . . . .

その他: 利用者への広報活動など

導入計画 (案)

- **今年度中に 試験稼働の状態にする**

  5 月: CA 立ちあげ, 計画のアナウンス, JPNIC 内部試行

  6 月: ISP から有志を募って実験をすすめる?

  9 月: 問題点の洗い出しと規模の拡大についての検討?

  . . . . . .