JPNICからの報告[II]
国際化ドメイン名(IDN)とDNSの適切な設定に向けて

2002年12月20日

小島育夫　kojima@nic.ad.jp
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

国際化ドメイン名
(Internationalized Domain Name)

国際化ドメイン名と日本語ドメイン名

- 国際化ドメイン名（IDN)とは
  - IETFで標準化作業が進められているプロトコル
  - ドメイン名を表現するのに使用できる文字を非ASCII文字に拡張したもの
- 日本語ドメイン名とは
  - 国際化ドメイン名の技術を使用し、日本語で使われる文字で表現されるドメイン名
  - レジストリのサービス仕様

IDNの例

华人.公司.cn　　華人.商業.tw

高島屋.jp

삼성.회사.kr　　三星.회사.kr

الاهرام.م

viagénie.qc.ca

ישראל.קום

ทีเอชนิค.พาณิชย์.ไทย

現代.com　　ヤフー.com

出典 http://www.jdna.jp/activities/event/jdn-tutorial/IDNSDK.pdf

国際化ドメイン名標準化状況

- 技術仕様が確定し、2002/10/24にRFC化が決定

1. IDNA
   - IDNの処理方式を規定
2. NAMEPREP
   - 正規化方式を規定
3. Punycode
   - プロトコル要素中でのエンコーディング方式を規定

IDNA
(draft-ietf-idn-idna-14.txt)

- IDNの処理はアプリケーションプログラムで行うというアーキテクチャで、その具体的な処理方式を規定
  - IDNを処理する際の文字コードはUnicode3.2
  - ユーザインターフェース層での入出力は特に規定しない
  - ネットワーク層で、プロトコル要素としてIDNを使用する場合の正規化方式とエンコーディング/デコーディング方式を規定

NAMEPREP
(draft-ietf-idn-nameprep-11.txt)

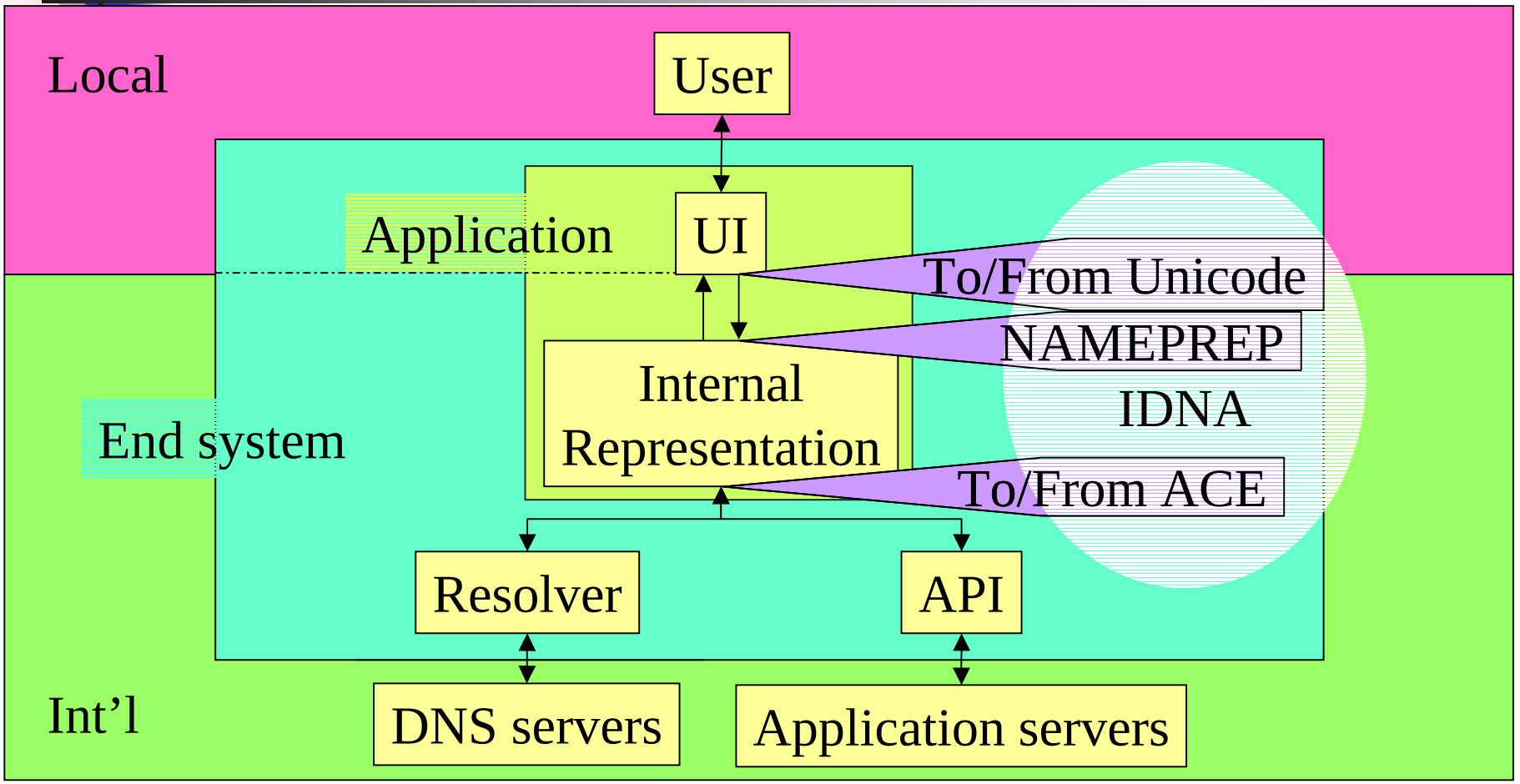
- Unicodeの文字コードで表現された文字列(IDN)の正規化処理を規定
  - STRINGPREP(draft-hoffman-stringprep-07.txt)のprofile定義
    - インターネットのプロトコルで「国際化された」文字列の比較を行う場合に、事前に意味的・表示的に同一の文字列の表現形式を統一するためのフレームワーク
  - 処理手順
    1. map: 文字種(大文字・小文字)の統一
       - A→a
    2. normalize: 合成記号の合成、互換文字の統一
       - u¨→ü
       - ｶﾞ→ガ
    3. Prohibit: 使用禁止文字のチェック
       - 空白文字など

Punycode
(draft-ietf-idn-punycode-03.txt)

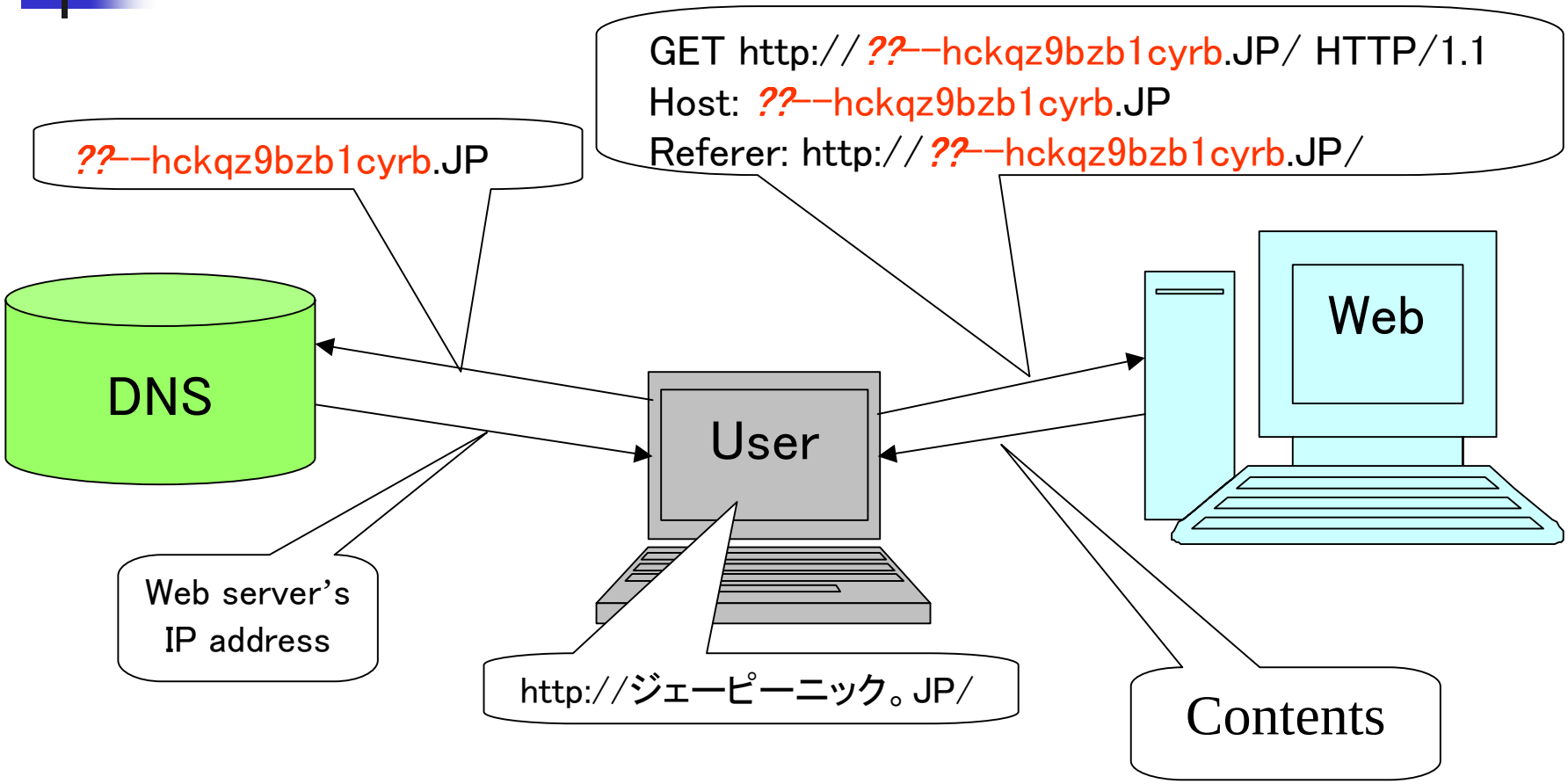
- Unicodeのエンコーディング・デコーディングアルゴリズムの一つ
  - ASCIIの英数字(a-z0-9)とハイフン(-)のみでUnicodeの文字列を表現
    - ASCII Compatible Encoding (ACE)
  - プロトコル要素でIDNを使用する場合でも下位互換性を維持
- 変換例
  - unicode文字列←→*??*--unicode-no0lo10eejx

    (※*??*の部分はIDNAのRFC発行時にIANAが割当)

IDNA


Local
User
Application
UI
To/From Unicode
NAMEPREP
Internal
Representation
IDNA
End system
To/From ACE
Resolver
API
Int'l
DNS servers
Application servers

Webサイトのブラウズ



JPNICの活動

- 1999年 5月　iDNS-TFを設置
- 2000年 2月　多言語ドメイン名に対するJPNICの取組み(案)発表
- 2000年 5月　多言語ドメイン名評価キット(mDNkit-1.x)開発開始
- 2000年10月　汎用JPドメイン名における日本語ドメイン名に関する技術方針発表
- 2000年11月　日本語ドメイン名運用試験(フェーズ1)開始
- 2001年 3月　多言語ドメイン名ツールキット(mDNkit-2.x)開発開始
- 2001年 5月　JPRSと協同で日本語ドメイン名運用試験(フェーズ2)開始
- 2002年 3月　国際化ドメイン名ツールキット(idnkit-1.x)開発開始

詳細はJPNICの「ドメイン名の国際化」のページ
http://www.nic.ad.jp/ja/idn/　を参照のこと

最終版(最新版)のリリース時期

- 2001年 2月 多言語ドメイン名評価キット最終版 (mDNkit-1.3)リリース
- 2002年 4月 多言語ドメイン名ツールキット最終版 (mDNkit-2.4)リリース
- 2002年12月 国際化ドメイン名ツールキット最新版 (idnkit-1.0pr2)リリース

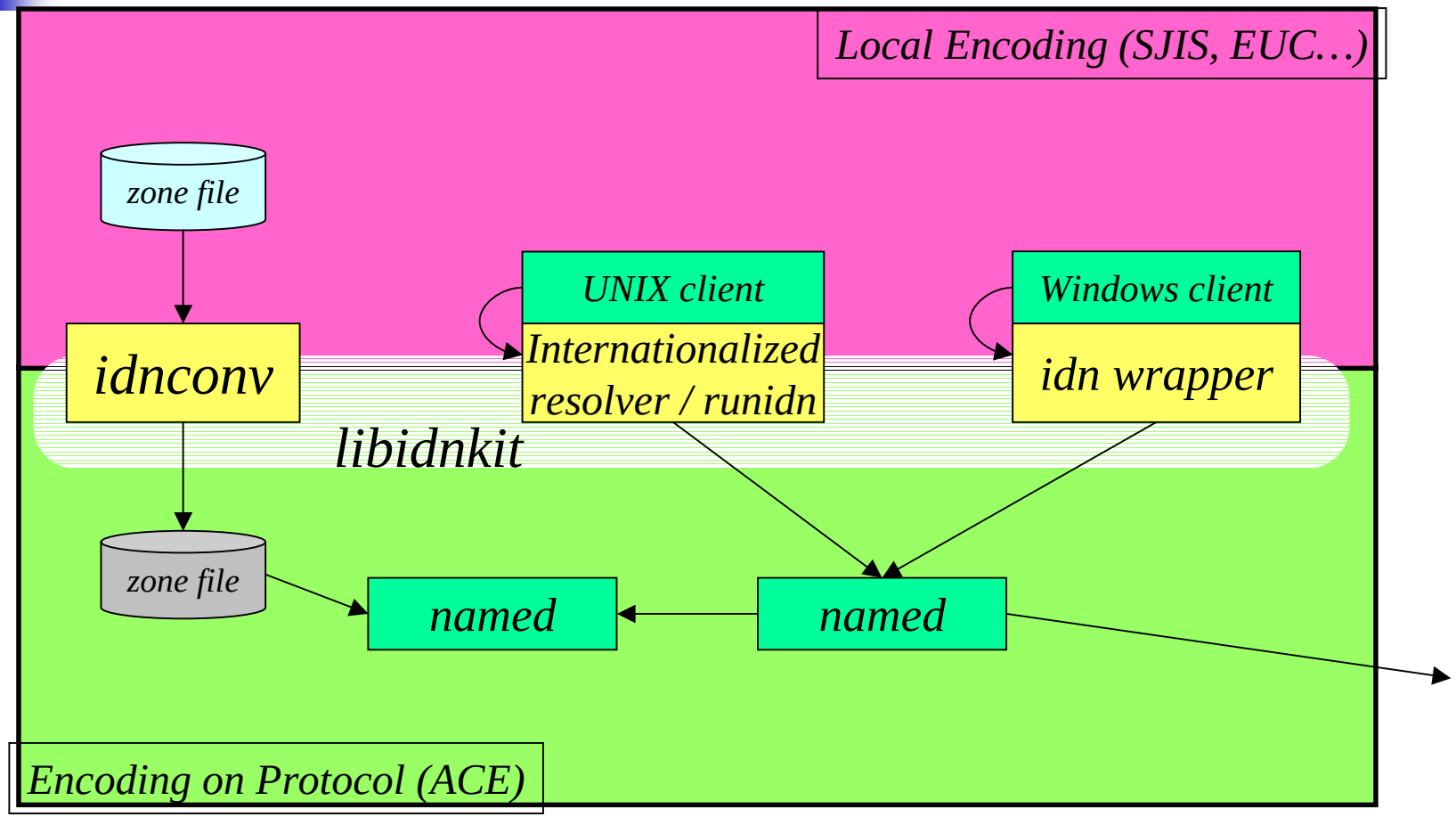
ツールキットの入手先:

http://www.nic.ad.jp/ja/idn/mdnkit/download/index.html

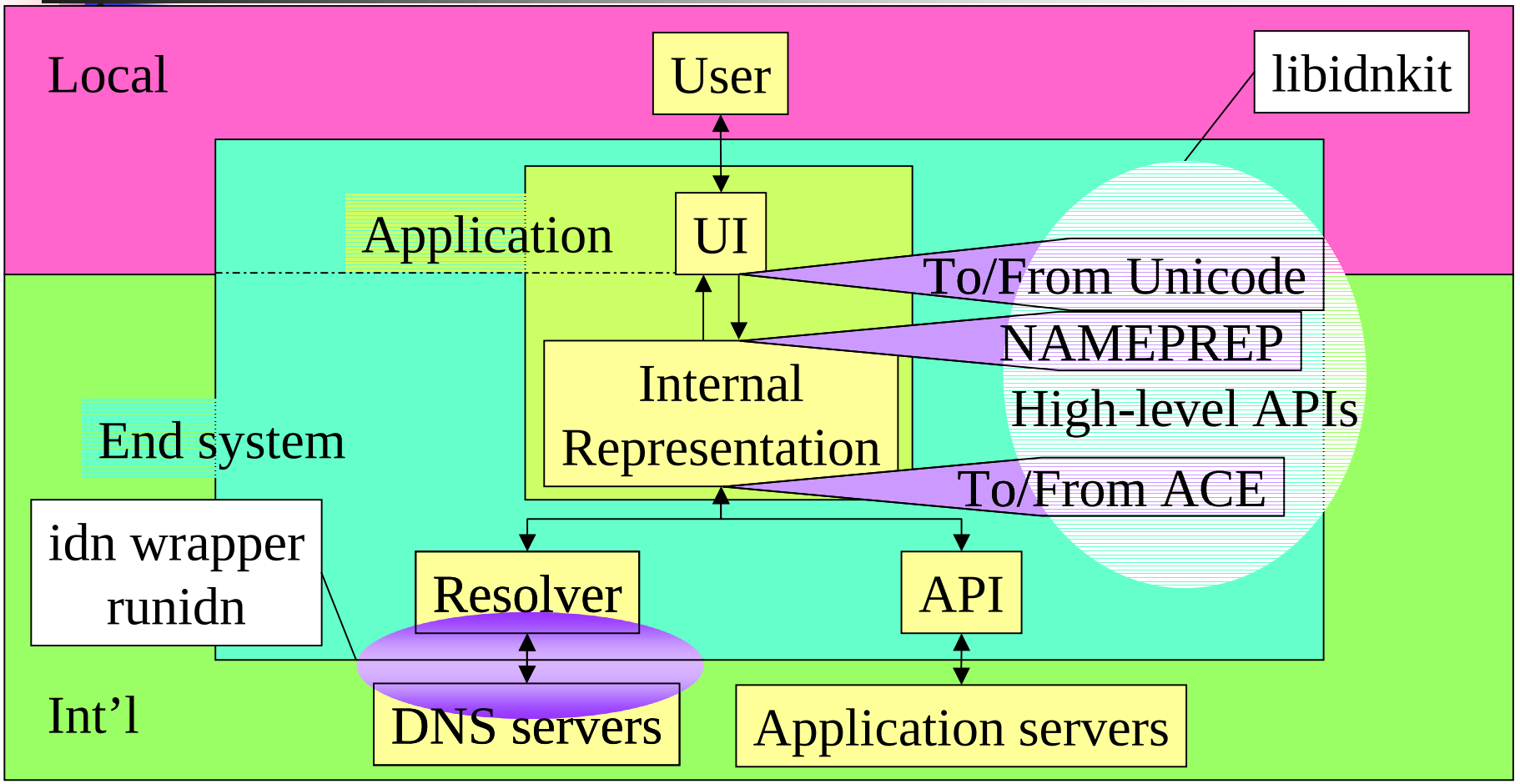
idnkit開発

- 昨年度まで開発していたmDNkitの後継
  - mDNkitは多くのIDN提案をサポートしていたがidnkitは標準化されるもののみサポート
    - 例外はRACE
- これまでのリリース履歴
  - idnkit-1.0pr1 (2002/9/27)
    - idnkit最初のリリース
    - まだRFCが発行されていないのでPreview Release
  - idnkit-1.0pr2 (2002/12/6)
    - ライセンス条項を緩和
    - MozillaのIDN対応で利用される!?

idnkitの構成


Local Encoding (SJIS, EUC…)
zone file
UNIX client
Internationalized resolver / runidn
Windows client
idn wrapper
idnconv
libidnkit
zone file
named
named
Encoding on Protocol (ACE)

idnkitの対応箇所



libidnkitの脆弱性検査

- インターネットのインフラ部分にかかる部分なので脆弱性があると大変
  - resolverのセキュリティホール(CA-2002-19)
- libidnkitにバッファオーバーフローがないか検査しようとしている
  - 検査ツールを開発中
  - 出来上がればそれもフリーソフトとして公開する予定
- TAO(通信・放送機構)の「次世代DNSに関する研究開発」の一環で実施
  - http://www.shiba.tao.go.jp/kenkyu/itakua/1438.htm

IDN-Admin Guideline

- IDNそれ自体は「言語」の概念はない(除外した)
- しかし利用者から見れば「言語」ドメイン名である
- それゆえ異なる言語のよく似た文字や、言語依存のため正規化されない等価文字の混在は利用者の混乱を招く
  - A≠Ａ
  - 机＝機
- IDN登録ガイドラインを日中韓台NICやIDN WGの有識者などと協力しながら作成中

IDN-adminとは

中国本土における繁体字（國）と簡体字（国）
→同一とみなす必要あり

日本における異体字（辺、邊、邉）

国沢、國沢、国澤、國澤を

同一文字として扱うためのメカニズム

参考URL

- JPNIC (http://ジェーピーニック.jp/)
  - ドメイン名の国際化
    http://www.nic.ad.jp/ja/idn/
  - idnkitダウンロード
    http://www.nic.ad.jp/ja/idn/mdnkit/download/
- JDNA (http://日本語ドメイン名協会.jp/)
  - IETF IDN WGの進捗状況報告
    http://www.jdna.jp/activities/survey/idn-wg/
  - 日本語ドメイン名Webサイトへのアクセス
    http://www.jdna.jp/activities/survey/browsers/
- IETF IDN WG
  - http://www.i-d-n.net/
  - http://www.ietf.org/html.charters/idn-charter.html

DNSの適切な設定に向けて

DNSの現状

一見「うまく動いている」ように見える

- しかし、実際には、DNSの運用上正しくない設定が行われている場合も多い
  - 各ホストで動いているネームサーバのエラーログを確認してみよう

正しくない設定により惹き起こされる事項

- DNSの不安定な動作
  - 本来不必要なDNSパケットの再送
  - 不必要なDNSタイムアウト待ち
  - 情報の取得が不安定

  ⇒インターネット上の各種サービスに影響を及ぼす
- DNSパケットストーム(2002年2月)
  - 特定のDNSサーバへの過大なDNSトラフィックが発生
  - 特定のBIND (8.3.0)の実装の問題+Lame delegation
  - BIND ネームサーバの更新に関するお願い(JPNIC)
    - http://www.nic.ad.jp/ja/topics/2002/20020207-01.html

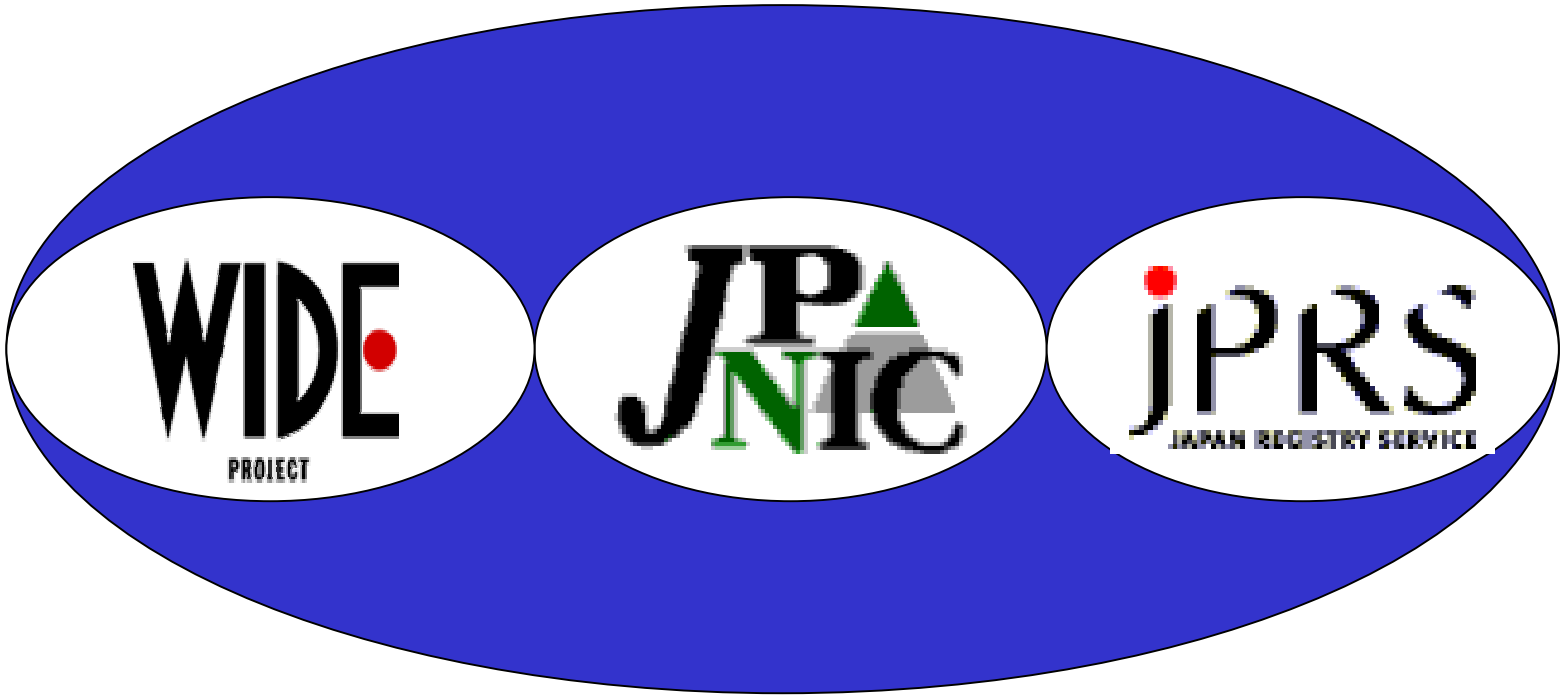
DNSの適切な設定の必要性

- DNSを基盤としたインターネットの安定運用
  - DNSへの不必要なパケットの転送を排除
  - DNSの負荷の低減
  - インターネットの見かけの不安定さを低減
- DNSの負荷を低減
  - ルートサーバやTLDのネームサーバ等の基幹となるサーバ群への不必要な問い合わせを低減
  - 現在のDNSシステムで安定的な運用を継続的に維持する

DNSの運用健全化に向けて

- 必要な活動
  - 現在のDNSの状況を観測、分析する
  - 分析した結果を公開し改善を求める
  - 自らのDNSの設定をチェックする手段を提供する
- 必要な要件
  - 商業ベースで実施することは困難
  - 国内や場合によっては海外にあるDNSサーバに対する網羅的な調査が必要
  - DNSに関する技術スキルが必要
  - DNS管理組織と(特にJPで)の連携が必要

DNS運用健全化タスクフォース (DNSQC-TF)



2002年5月、WIDE・JPRS・JPNICの共同プロジェクトとしてDNSQC-TFを設置

DNSQC-TFの活動

- 2002年度の活動内容
  - 基本的な技術(チェックツール等)の開発
  - 現状の分析
  - 判明した問題点のコミュニティへの発信
  - 自らの設定のチェック手段の提供
  - 実運用ベースでのサービス化の検討
  - 実運用に伴う個別通知に向けた環境作り

活動スケジュール

- 2002年5月
  - 設立
- 2002年7月
  - 活動開始報告(JANOG10 meeting)
- 2002年12月
  - 中間報告(Internet Week2002 / DNS Day)
  - 中間報告(Internet Week 2002 / IP meeting) ***←今日はここ***
- 2003年1月
  - 進捗報告(JANOG11 meeting)
- 2003年3月
  - 最終報告

DNSの現状調査

- [第0段階] 予備調査
  - 2002年6月
  - 加藤朗氏による第0次調査
  - IETF/JANOG-10における発表
- [第1段階] 試行調査
  - 2002年11月
  - 本報告他で発表
- [第2段階] 本格調査
  - 2003年1月～3月に調査予定
  - 管理者へのフィードバックも検討

試行調査の内容

- 2002年11月1日～11日に実施
- JP配下のドメイン
  - 属性型・地域型ドメイン
  - 汎用ドメイン
- 約38万ドメインを対象に

何がいけないのか？

- Lame Delegation（不完全委任）
- NSレコードで指定されている名前がCNAME
- MXレコードで指定されている名前がCNAME
- A/AAAAレコードにプライベートアドレス
- SOAレコードの値に不適切なものがある
- 登録されたネームサーバに到達できない
- ドット(“.”)の書き忘れ

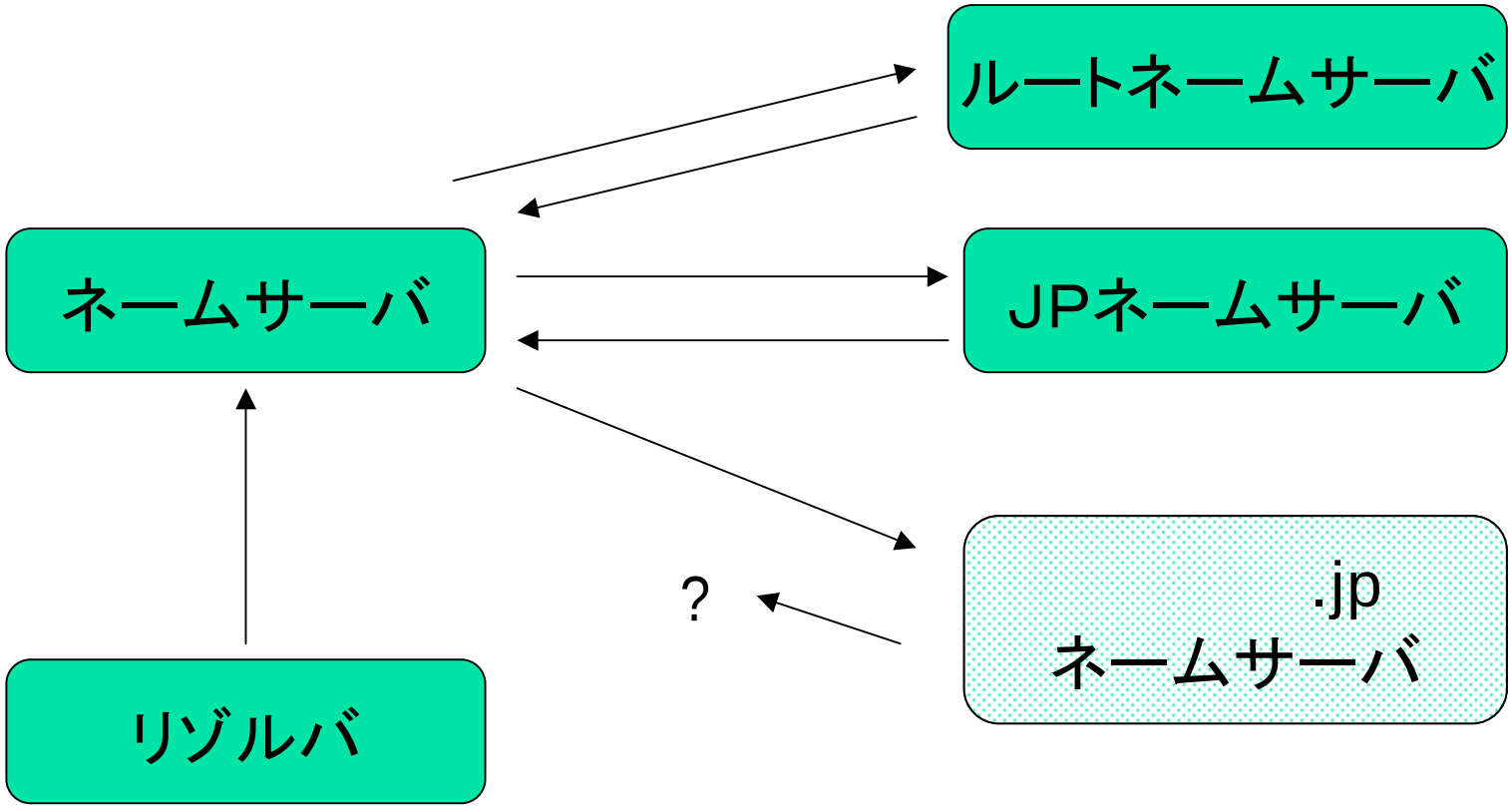
  などなど

Lame Delegation とは

- 不完全委譲(Lame Delegation)のネームサーバとは、上位ゾーンに　登録されているネームサーバが、実際にはそのゾーンの権威ある　(Authoritative)ネームサーバでない場合をいう。

  - 指定されたNSにそのゾーンの情報が発見できない
    原因:
    (1) そのNSにそのゾーンが定義されていないとき
    (2) ゾーンファイルに構文エラーがあり正しく設定されていないとき
    (3) プライマリが Lame のとき

Lame Delegation とは(2)



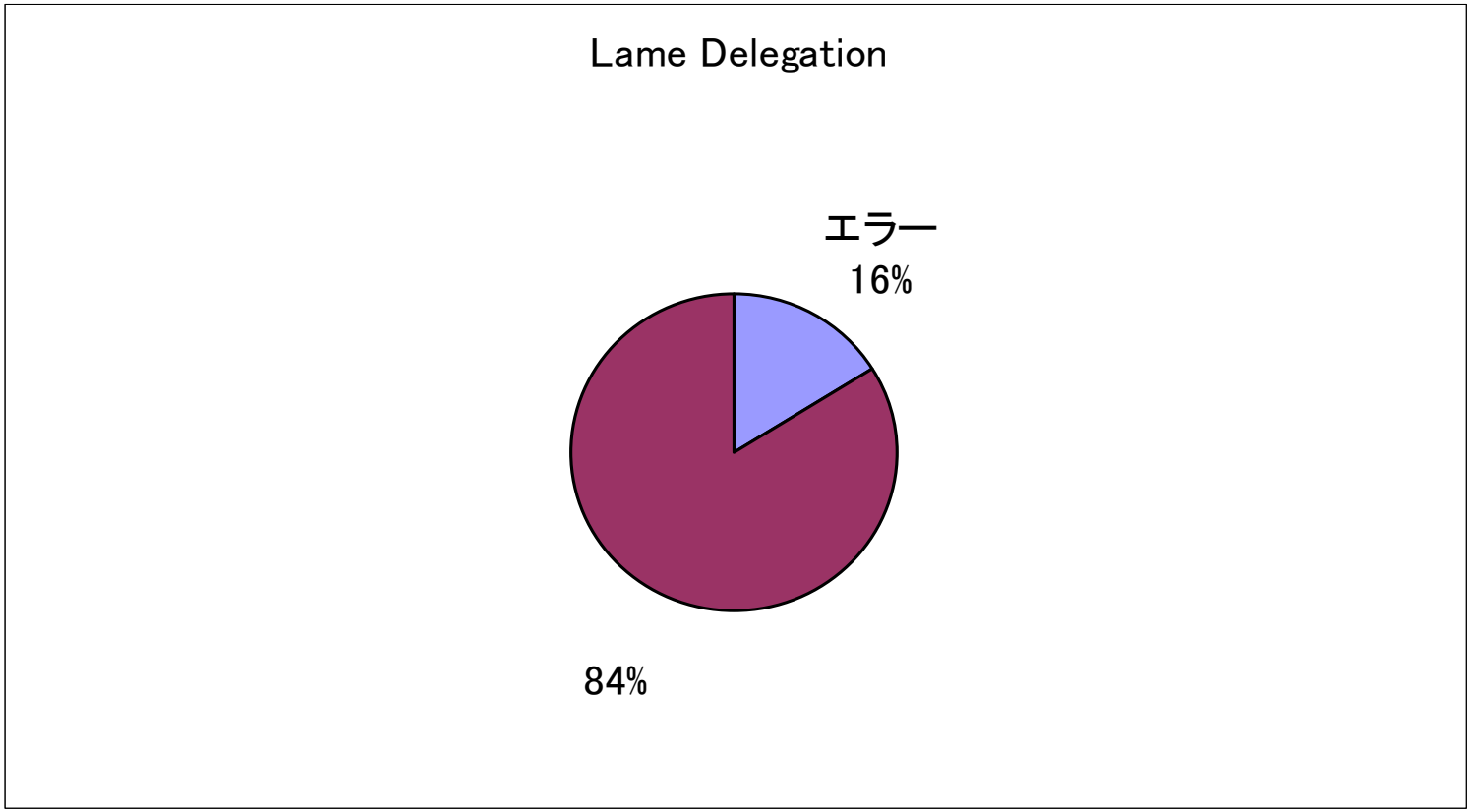
Lame Delegation による影響

発生する問題

- そのゾーンの名前が引けない.
- 検索のたびに，そのNSのネームサーバ(プライマリ，セカンダリ)に毎回問い合わせがいく
- ネガティブキャッシュが登録されないので．普通の検索でも，Lameにあたると，再問い合わせが発生する.
- むだなトラフィックが発生する

調査結果(Lame Delegation)

380953ゾーン中、61143ゾーンにエラー



NSで指定されている名前がCNAME

example.jp.	IN	NS	ns1.example.jp.
ns1	IN	CNAME	hoge.example.jp.
hoge	IN	A	1.2.3.4

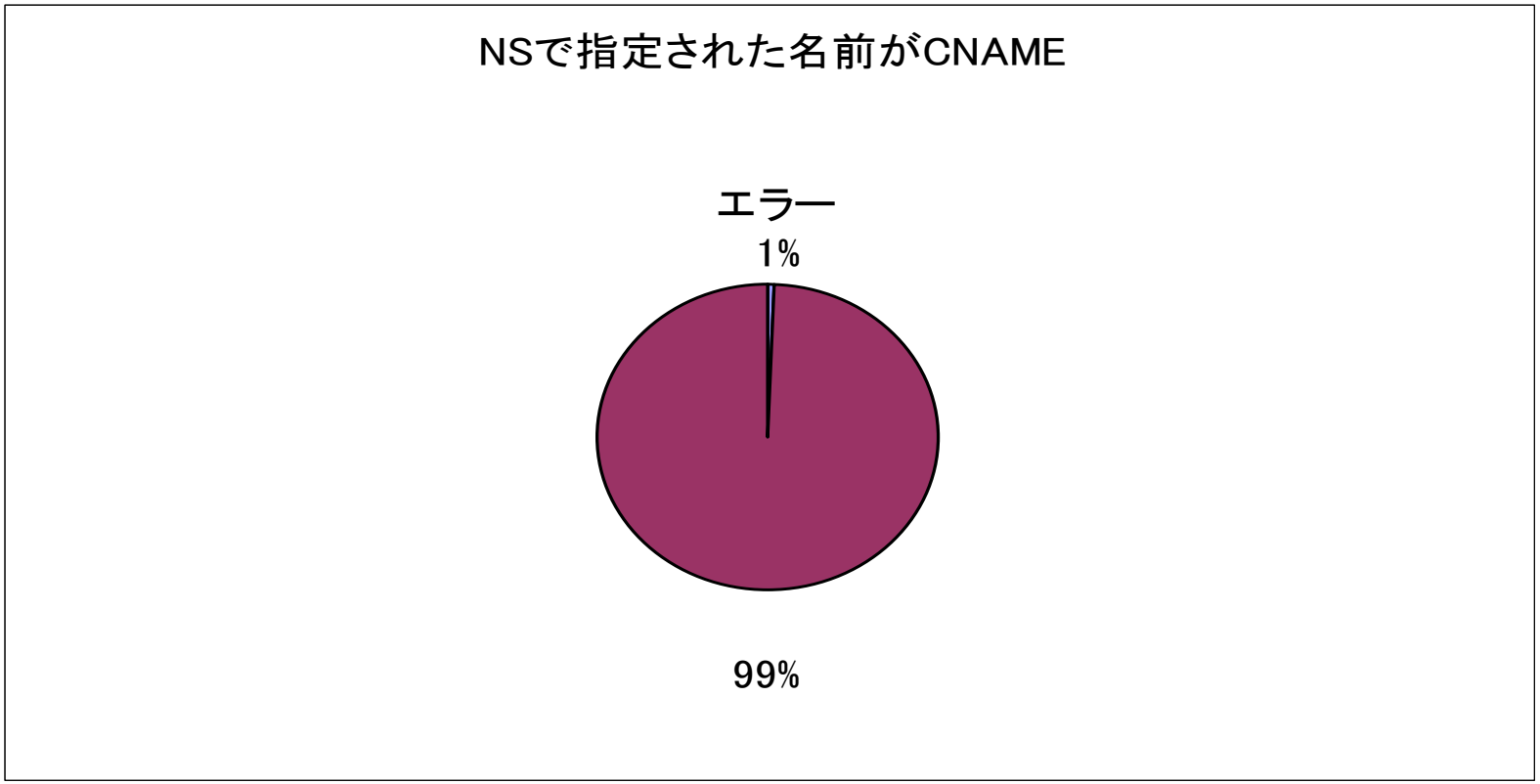
Queryの増加→ネットワークやネームサーバへの負荷

正しくは、

example.jp.	IN	NS	ns1.example.jp.
ns1	IN	A	1.2.3.4
hoge	IN	A	1.2.3.4

調査結果(NSがCNAME)

380953ゾーン中、2355ゾーンにエラー



MXで指定されている名前がCNAME

example.jp.	IN	MX	mx1.example.jp.
mx1	IN	CNAME	hoge.example.jp.
hoge	IN	A	1.2.3.4

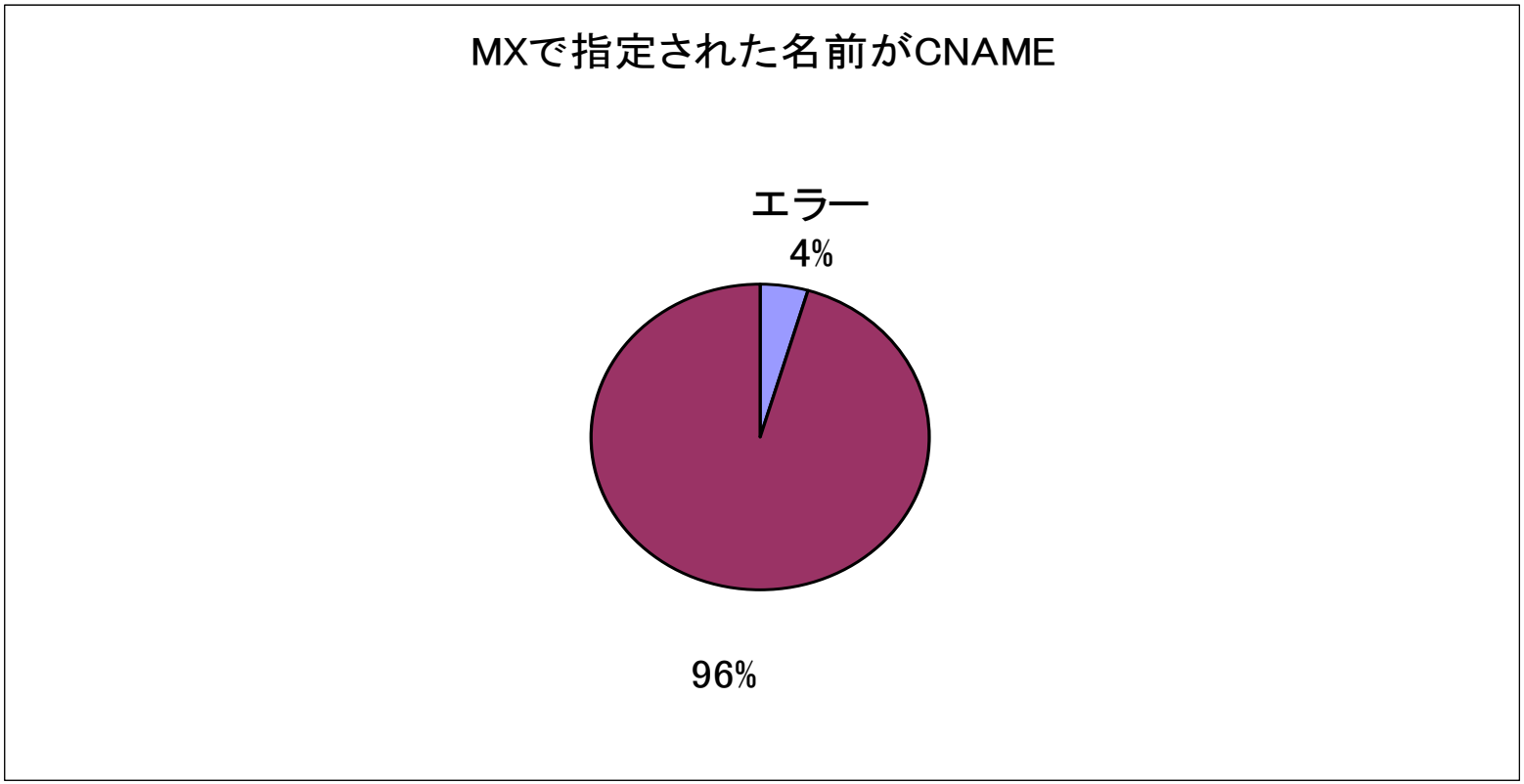
Queryの増加→ネットワークやネームサーバへの負荷

正しくは、

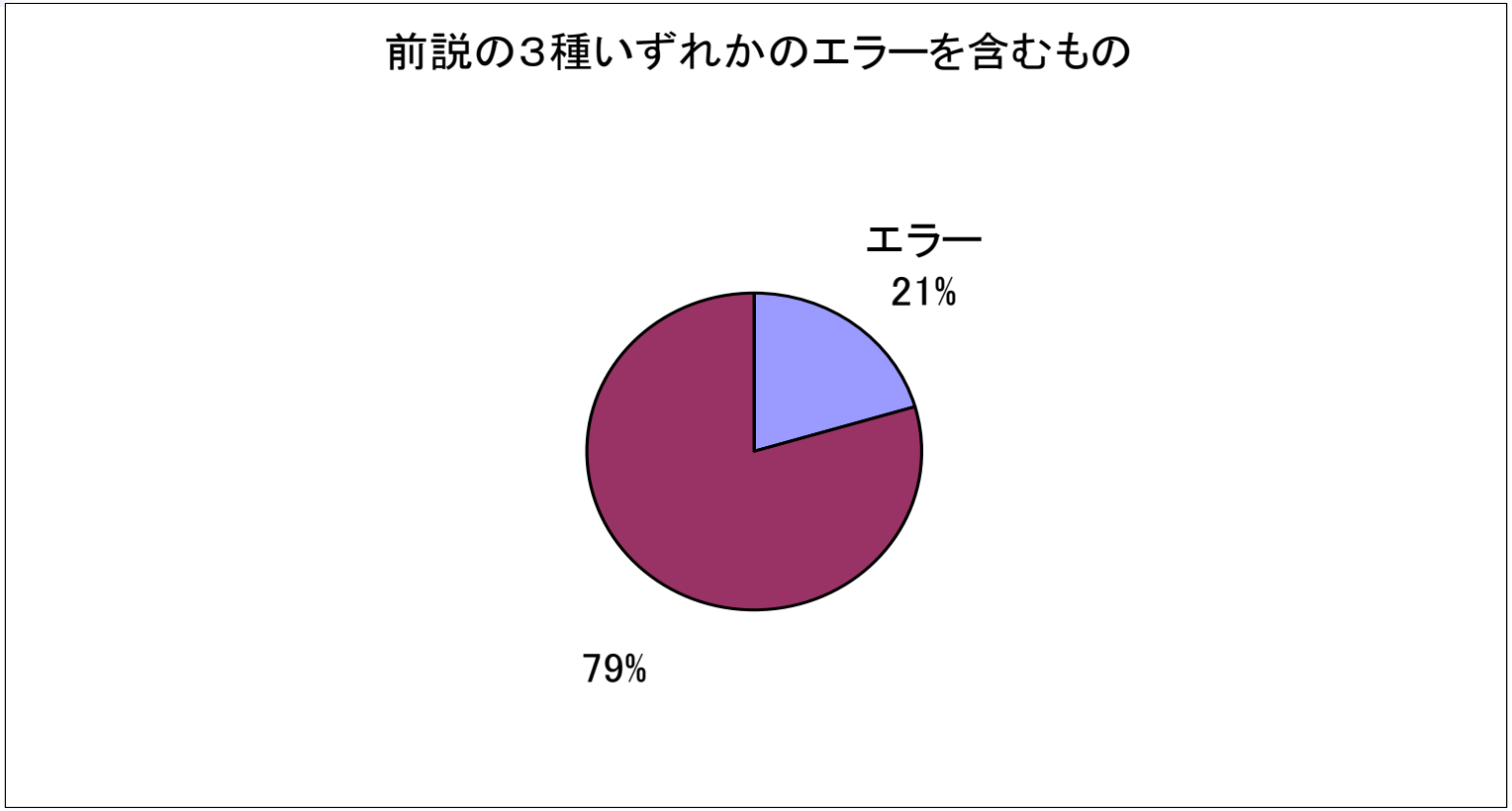
example.jp.	IN	MX	mx1.example.jp.
mx1	IN	A	1.2.3.4
hoge	IN	A	1.2.3.4

調査結果(MXがCNAME)

380953ゾーン中、17037ゾーンにエラー



調査結果(LameまたはCNAME)
380953ゾーン中、78197ゾーンにエラー



調査結果から

- 前説の３種のエラーだけでも2割を超える。

→結構危うい状態！

自社のWebサイトが閲覧できない状態に
なっているかも！？

DNSの設定再確認と
「正しい設定を行おう」という意識改革を

今後の活動

- 本格調査の実施
  - 2003年2月から3月にかけて実施予定
    （その前に修正を）
  - 最終報告書としてとりまとめる予定

- 継続的かつ定期的なチェックを検討中

最後に

- 積極的な情報発信
  - http://www.nic.ad.jp/ja/dnsqc/index.html
- DNS設定の自己確認ツールの提供
  - 上記Webページ中で提供予定
  - 2003年1月中の公開を目標