IW2004 DNS Day

DNS関連技術の最新動向

2004年12月3日
米谷嘉朗 <yone@jprs.co.jp>
株式会社日本レジストリサービス

もくじ

- 概要
- IDN
- ENUM
- IPv6
- DNSSEC
- SPF/DomainKeys
- ONS
- Anycast

概要

- DNSをベースとした新しいサービスが開発・開始されている
- 開始済の新しいサービス
  - IDN、IPv6
- 新しい名前空間
  - ENUM、ONS(RFID)
- DNSの信頼性向上
  - DNSSEC
- 検討中の新しいサービス
  - SPF/DomainKeys

DNS管理者として

- 新しいDNSの機能をいち早く知ることで、自組織のサービス向上に役立てられる
  - 新しいリソースレコード
  - リソースレコードの左辺値
  - リソースレコードの右辺値
  - 上記の組み合わせ

IDN

Japan Registry Service

ドメイン名の登録サービス開始済

- アジア、ヨーロッパのTLDを中心に言語ドメイン名の登録サービスが開始されている
  - アジア
    - 日本、中国、韓国、台湾、タイ、シンガポール、他
  - ヨーロッパ
    - ポーランド、ドイツ、オーストリア、スイス、スウェーデン、他
  - gTLD
    - com/net、museum、info、biz
- IDNと「言語」を関連付ける「言語テーブル」のIANAへの登録が開始されている
  - http://www.iana.org/assignments/idn/

技術で解決できない問題

- Unicodeは多数の「似て非なる」文字を持つ
  - NI(ni)←→ＮＩ（ν ι）
  - □←→ロ←→ロ←→口
- いくつかの言語は歴史的、文化的事情により「異体」文字を持つ
  - 電気通信←→電氣通信←→电气通信
- IDNの技術仕様ではそれら文字の「混用」を避けることはできない
  - 運用上の「制約」が必要

文字、言語、用字

- 「文字」は「言語」を書き表すためのもの
  - 言語の一部だが、言語そのものではない
- 一定の規則にしたがって作られた・集められた文字の一群が「用字」
  - 平仮名、ギリシア文字、アラビア文字など
- 「用字」は複数の「言語」で使用され得る
  - 中国語、日本語、韓国語における漢字など
- IETF的定義はRFC3536の2章

ICANN Guideline

- ICANNがIDN登録を許可する条件
  - ICANNと契約関係を持つTLD(Top Level Domain)レジストリが対象
  - JET Guideline for IDNの考え方を踏襲
  - 記号の使用を原則禁止
  - 2003年6月20日にVersion 1.0が公開
    - http://www.icann.org/announcements/announcement-20jun03.htm
    - http://www.icann.org/general/idn-guidelines-20jun03.htm

JET Guideline for IDN

- IDNにおける「漢字」の扱い方について、日中韓台(JP/CN/KR/TW)のNICおよび有識者で議論し作成した、IDN登録時の制約アルゴリズム
  - DNSのゾーン管理者を対象
  - IDNを「言語」と関連付ける
  - 「言語」は「登録可能文字」と「その異体字」の集合から定義される
  - 2004年4月にRFC3743として発行
    - http://www.ietf.org/rfc/rfc3743.txt
  - 日本語の異体字テーブル
    - http://www.iana.org/assignments/idn/jp-japanese.html

適用例

日本語テーブル		
VCP	PV	CV
氣	気	氣、気
気	気	気、氣

中国語テーブル		
VCP	PV	CV
氣	氣	氣、气
气	氣	气、氣

入力		日本語	中国語	日本語＋中国語
氣	*ZV*	氣、気	氣	氣、気
	CV	―	气	气
気	*ZV*	気	×	×
	CV	氣		
气	*ZV*	×	氣、气	×
	CV		―	

VCP: Valid Code Point
PV: Preferred Variant
ZV: Zone Variants
CV: Character Variants

DNS管理者の注意点

- 自組織のドメイン名にIDNのラベルを使用する場合
  - 極力、既存の「言語テーブル」を使用する
  - 「言語テーブル」に未定義の言語のラベルを使用する際は、最初に「言語テーブル」を定義する
- DNSのゾーンにIDNのラベルを登録する場合
  - 登録する文字列中のすべての文字が、使用することにしている「言語テーブル」の使用可能文字の範囲に入っていることを確認する

利用する際の注意点

- IDN対応アプリケーションが必要
  - IEを除く主なブラウザは対応済
    - Safari、Netscape/Mozilla、Opera
    - IEはPlug-inをインストールすることで対応可能
      - http://jprs.jp/i-Nav/
  - メールはこれから
    - メールアドレス全体の国際化はまだ標準化されていない
- アクセスサイト
  - 携帯電話や、管理権限を持たずアプリケーションの更新や導入が不可能な場合に便利
    - http://jajp.jp/

関連URI

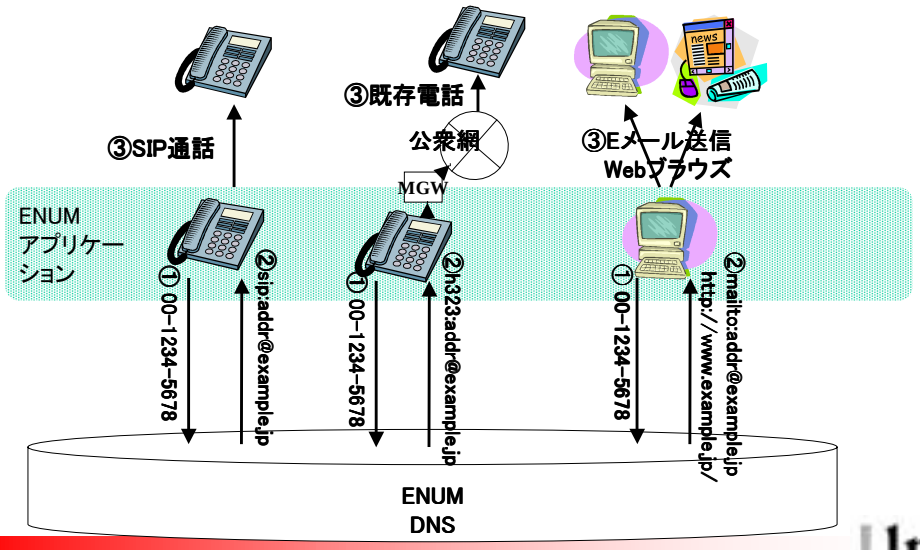
- JPRS
  - http://日本レジストリサービス.jp/ http://jprs.jp/
  - http://日本語.jp/ http://nihongojp.jp/
- JDNA
  - http://日本語ドメイン名協会.jp/ http://www.jdna.jp/
- ICANN
  - http://www.icann.org/
- IANA
  - http://www.iana.org/

ENUM

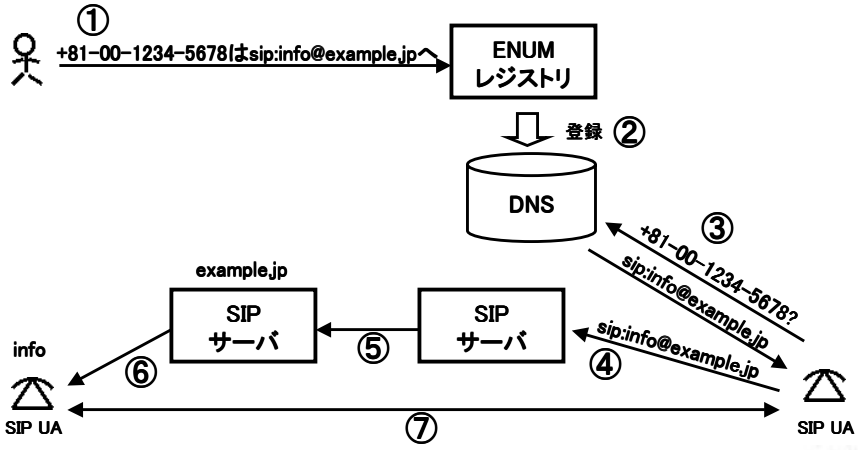
ENUMとは?

- Telephone Number Mapping
- ENUMは電話番号(E.164番号)をインターネット資源のアドレスに対応付ける機構
- インターネット資源のアドレスはURIで指定
- 対応付けはDNS(Domain Name System)で実施
  - DNSはインターネット全体をカバーする唯一の名前解決機構
- 利用者(アプリケーション)は状況に応じてURIを選択できる
- IETFとITU-Tが協同で標準化を実施

ENUMをベースとした通信のイメージ



ENUM利用の流れ



E.164番号からドメイン名への変換

- RFC3761で規定
- 先頭の'+'を除く数字以外の文字を削除
  - +810012345678
- 先頭の'+'を削除
  - 810012345678
- 数字の間にピリオド(".")を挿入
  - 8.1.0.0.1.2.3.4.5.6.7.8
- 数字の並びを逆順にする
  - 8.7.6.5.4.3.2.1.0.0.1.8
- 末尾に".e164.arpa"を追加
  - 8.7.6.5.4.3.2.1.0.0.1.8.e164.arpa

NAPTR RRの構造

- ENUMではNAPTRのサービスとして"E2U"を規定
  - NAPTR RRはRFC3403で規定
- ENUM NAPTR RRの形式

  label IN NAPTR *order pref* "u" "E2U+*enumservice*" *regexp* .
  - *label* E.164番号のドメイン名形式
  - *order* 16bit符号なし整数
  - *pref* 16bit符号なし整数(orderの方が優先される)
  - *enumservice* 利用可能なURIのタイプを指定
  - *regexp* AUSの置き換え式を指定

ENUMサービス

- RFCとして発行されIANAに登録される
- 登録済・登録が見込まれるENUMサービス・プロトコル

サービス/プロトコル	RFC/I-D	サービスフィールド	URIスキーム(例)
SIP	3764	E2U+sip	sip:info@sip.jprs.co.jp
H.323	3762	E2U+h323	h323:info@h323.jprs.co.jp
Presense	pres-01	E2U+pres	pres:support@im.jprs.co.jp
Email	msg-03	E2U+email:mailto	mailto:info@jprs.co.jp
WEB	webft-01	E2U+web:http	http://www.jprs.jp/
FTP	webft-01	E2U+ft:ftp f	tp://ftp.jprs.jp/
iFax	FAX WG	E2U+ifax:mailto	mailto:info@ifax.jprs.co.jp
VOID	void-00	E2U+void:mailto	mailto:num-drama-info@jprs.co.jp

※I-Dはdraft-ietf-enum-*XXXX-NN*.txtの部分のみ記述

ENUM NAPTRの例

E.164番号が+810012345678の場合:

$ORIGIN 8.7.6.5.4.3.2.1.0.0.1.8.e164.arpa.
IN NAPTR 100 10 “u” “E2U+sip” “!^¥+8100(.*)$!sip:¥1@sipisp.jp!” .
結果は ‘sip:12345678@sipisp.jp’

$ORIGIN 8.7.6.5.4.3.2.1.0.0.1.8.e164.arpa.
IN NAPTR 100 10 “u” “E2U+sip” “!^.*$!sip:info@sip.jprs.jp!” .
結果は ‘sip:info@sip.jprs.jp’

$ORIGIN 8.7.6.5.4.3.2.1.0.0.1.8.e164.arpa.
IN NAPTR 100 10 “u” “E2U+email:mailto” “!^.*$!mailto:info@jprs.jp!” .
結果は ‘mailto:info@jprs.jp’

SIPを使用する際の注意点

- DNSにSIPドメイン名を登録する際は、Aだけではなく別途NAPTRとSRVの設定が必要
  - 詳細はRFC3263で規定
- SIPドメイン名としてexample.jpを使用し、SIPサーバはsip.example.jpが5060/udpで提供する場合
  - SIPドメイン名のサービスをNAPTRで登録

    $ORIGIN example.jp.

    @ IN NAPTR 0 0 "s" "SIP+D2U" "" _sip._udp
  - SIPサーバをSRVで登録

    _sip._udp IN SRV 0 0 5060 sip

関連URI

- ETJP
  - http://etjp.jp/
- ENUM Info by JPRS
  - http://jprs.jp/enum/
- IETF ENUM WG
  - http://www.ietf.org/html.charters/enum-charter.html
- ITU ENUM Activities
  - http://www.itu.int/osg/spu/enum/

IPv6

TLD/RIR DNSでのIPv6対応状況

- NSのAAAA glue登録
  - gTLDでは対応し始めている
    - com/net
  - ccTLDでは対応し始めている
    - JPは2000年3月から対応している
    - 他、TW(台湾)やFR(フランス)など
- IPv6 transport
  - gTLDでは対応し始めている
    - com/netが2004年10月末に対応開始
  - ccTLDでは対応し始めている
    - JPは2001年8月から対応している
    - 他、TWやFRなど
  - RIRでも対応し始めている
    - ARIN、RIPEなど
- RSSAC(DNS Root Server System Advisory Committee)がICANN理事会にルートゾーンへのAAAA glue登録勧告(Recommendation)を提出
  - IANAで手順を検討、2004年6月にパブリックコメント
  - 2004年7月20日からルートゾーンにAAAA(IPv6アドレス) glueの登録が開始

関連URI

- RSSAC
  - http://www.rssac.org/
- IANA
  - http://www.iana.org/
- JPRS DNS関連技術情報
  - http://jprs.jp/tech/

DNSSEC

DNSSECとは

- DNS Security Extension
- DNSゾーンに権限を持つ管理者が、公開鍵暗号技術を用いて、自らのゾーン情報に秘密鍵で署名を行うDNSの運用方式
  - そのゾーン情報の第三者による改ざん・騙りを検証することが可能となる技術
    - ゾーンの公開鍵で検証
  - これにより、万一にも騙りを許したくないDNSレコードを守ることが可能となる

関連URI

- ETJP DNSSECテストベッド関連資料
  - http://etjp.jp/about/wg/dnssec.html
- IETF DNSEXT WG
  - http://www.ietf.org/html.charters/dnsext-charter.html

SPF/DomainKeys

SPF/DomainKeysとは

- メール発信者の認証をDNSを使って行う
  - SPAM対策
- 考え方
  - E-mailを送る側が、From(SMTP MAIL FROM)のドメイン名とSMTP発IPアドレスの対応をDNSに登録
  - SMTP接続を受け付けたMTAは、Mail Fromのドメイン名をDNSで検索し、得られたSMTP発アドレスリストに含まれるアドレスからの接続でなければ拒否
- 複数の提案
  - 新しいRRを導入するもの
  - 既存のRR(TXT)を使用するもの
- MTA Authorization Records in DNS
  - 2004年3月にIETF Application AreaのWG化
  - 2004年9月にIPR問題によりWG終了
  - 現在、Individual Draftとして検討を継続

主な提案(概要)

- SPF(Sender Policy Framework)方式
  - example.com. IN SPF "v=spf1 +mx +a:colo.example.com/28 -all"
  - draft-lentczner-spf-00.txt
- Domainkey(Yahoo)方式
  - brisbane._domainkey IN TXT "g=; k=rsa; p=MEwwDQYJKoZIhvcNAQEB ... IDAQAB"
  - draft-delany-domainkeys-base-01.txt
- Sender ID(Microsoft)方式
  - draft-lyon-senderid-core-00.txt
  - draft-lyon-senderid-pra-00.txt
- RMX方式
  - jprs.co.jp. IN RMX host:mx1.jprs.co.jp.
  - jprs.co.jp. IN RMX ipv4:202.11.16.0/23
  - draft-danisch-dns-rr-smtp-04.txt

関連URI

- SPF
  - http://spf.pobox.com/
- Domainkeys
  - http://antispam.yahoo.com/domainkeys
- SenderID
  - http://www.microsoft.com/mscorp/twc/privacy/spam/senderid/overview.mspx
- RMX
  - http://www.danisch.de/work/security/antispam.html

ONS

ONS(Object Name Service)とは

- あるEPC(Electric Product Code) に関連する情報を提供するサービス(EPC-IS)の所在を示す、DNSベースのサービス
- 現在の最新仕様
  - Auto ID Object Name Service (ONS) 1.0
- FQDN部にシリアル番号は含まれていない
  - 36bitもあるためDNSサーバーへの負荷を懸念
  - シリアル部分はEPC-ISで解決するという考え方
  - 新しい仕様では含まれる可能性がある

ONSとは(続き)

- FQDNしたIDからNAPTR RRを提供
  - 例
    <class>.<manager>.<header>.onsroot.org. IN NAPTR 10 10 u "EPC+pml" "!^.*$!http://example.jp/cgi-bin/pmlservice!" .
    <class>: 24bitの10進数
    <manager>: 28bitの10進数
    <header>: 8bitの10進数
    ‘24.2.1.onsroot.org’のようになる
    - "onsroot.org"はONS 1.0のドキュメントにあるだけで、実際には別の名前になると思われる
- 2004/1/13 プレスリリース
  VeriSignがONSのルートサーバーを運用することが決まる
  - http://www.verisign.com/corporate/news/2004/pr_20040113a.html

関連URI

- AUTO-ID LABS JAPAN
  - http://www.auto-id.jp/index-j.html
- EPCglobal
  - http://www.epcglobalinc.org/
- ONS Specification Version 1.0
  - http://www.epcglobalinc.org/EPCglobal_ONS_1.0.pdf

IP Anycast

http://www.atmarkit.co.jp/fnetwork/dnstips/035.html

IP Anycastの効果

- 耐障害性の向上
- パフォーマンス・接続性の向上
- AS112 Projectで開始され、Rootサーバで展開中
  - http://www.as112.net/
  - http://www.root-servers.org/
    - C、F、I、J、K、M
- JPでも展開中
  - BGP Anycast (a.dns.jp)
    - 東京と大阪に展開
    - 完全二重化構成
  - IGP Anycast (d.dns.jp)
    - 日本・米国(東部・西部)に展開
    - 海外(主に米国)からの接続性の向上
  - http://www.dns.jp/index-j.html