

DNS, URI, ENUM, SIP Routing, NAT traversal

N+I 2005 W03

2004年6月6日

株式会社日本レジストリサービス

藤原和典 <fujiwara@jprs.co.jp>

目次

- **SIP/H.323 URI**
 - ドメイン名とDNS概要
 - SIP URI
 - H.323 URI
 - SIP URIによるVoIP通信
- **ENUM**
- **将来への展望**
 - DNSSEC
 - ENUMによるVoIPキャリア間接続
- **NAT Traversal**
- **小規模なSIP/ENUM環境の構築**
 - APRICOT2005で行ったENUM/SIPデモンストレーション

ドメイン名とDNS概要

ドメイン名

- ピリオドで区切られた文字列
- インターネットで一意的な識別子
- URI, メールアドレスなどの構成要素
 - info@jprs.jp
 - http://jpdirect.jp/co/flow/
 - telnet host.jprs.co.jp

→ドメイン名を使わないと、

- http://192.168.100.1/ telnet
2001:0DB8:1234:5678:9abc:def0:fdb9:7531
- IPアドレスなどの情報を抽象化するもの
- 対応する情報
 - IPアドレス(IPv4, IPv6)
 - Webサーバ, ホスト
 - サービス
 - 電子メール, SIP, H.323など

DNS

- **Domain Name System**

- ドメイン名と対応する情報の対応づけを行うインターネット上の分散データベース
 - 階層的に管理
- 基本機能: ドメイン名から対応するIPアドレスを検索
- `www.jprs.co.jp` -> `61.120.151.80`

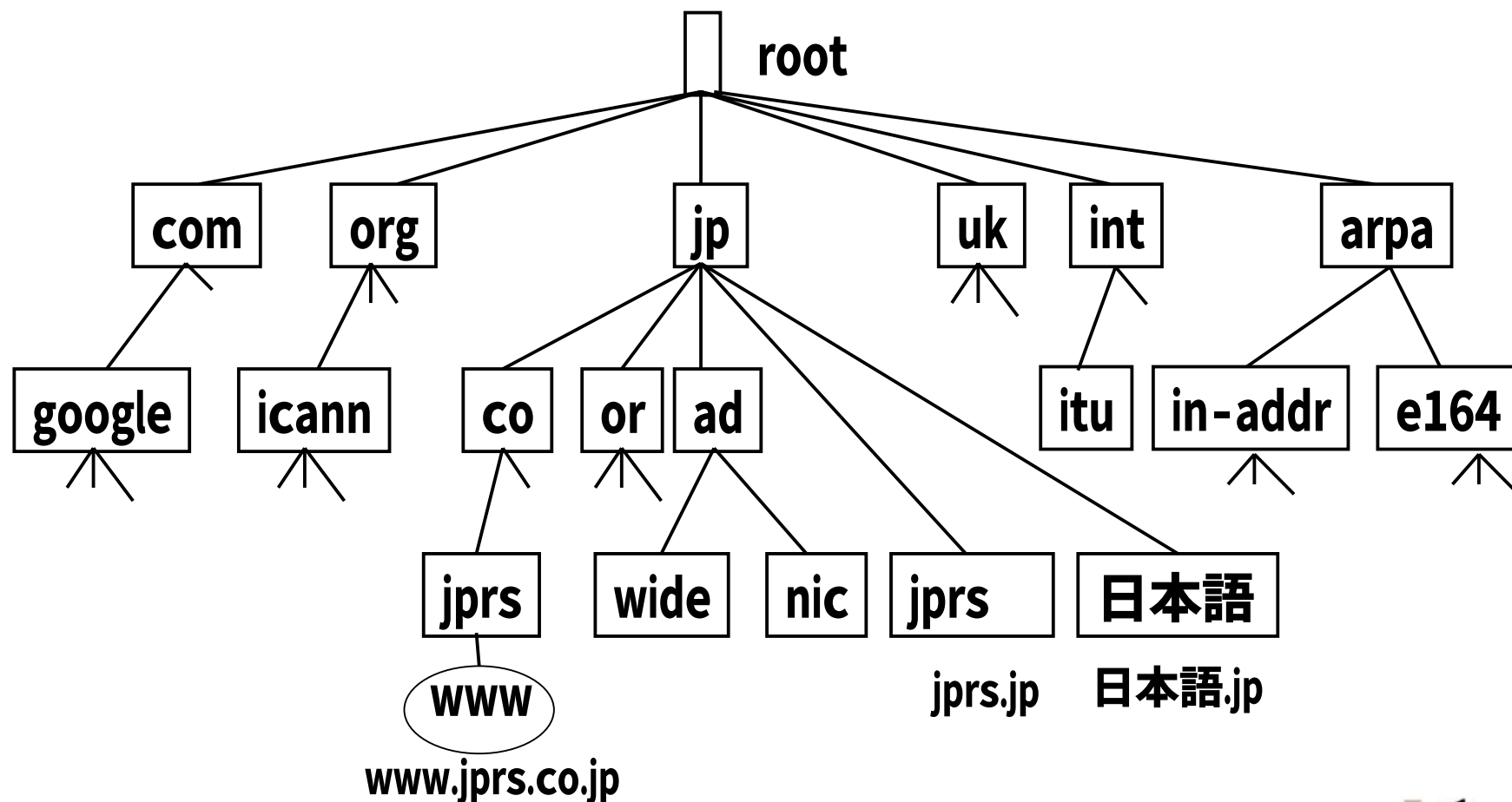
- **前DNS時代**

- 対応表のファイル(HOSTS.TXT)をダウンロード
- 更新はファイル管理者(SRI-NIC)にメールで通知
- ホスト増加で破綻
- 1985年3月, 最初のDNS登録

委任(delegation)

- 各階層は直下の階層の名前の管理を委任
- 委任された側(下位)
 - その階層の名前の登録管理
 - さらに直下への委任
- 委任する側(上位)
 - 委任した階層のネームサーバを登録
- ピリオド区切りごとに委任可能

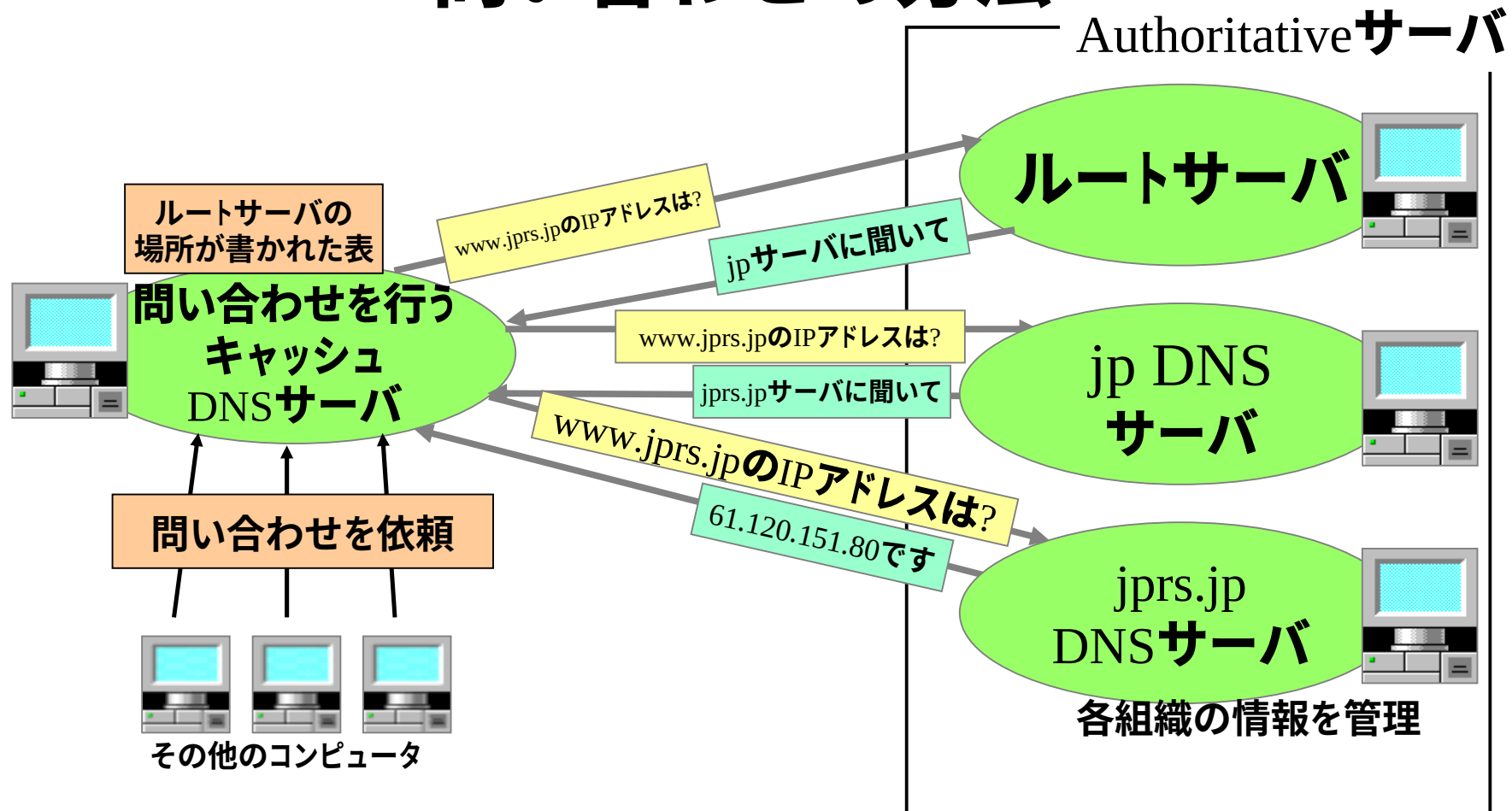
DNSツリー



DNSサーバ(ネームサーバ)

- DNSのクエリ(問い合わせ)を受けるサーバ
 - プライマリサーバ
 - データのマスタを管理
 - セカンダリサーバ
 - プライマリサーバのコピー
 - キャッシュサーバ
 - 他のサーバへ問い合わせを伝達
 - 答えを一時的に保持
 - 同じ問い合わせに対して保持した情報を利用
- セカンダリサーバをもつことで
 - 耐故障性をもつ
- キャッシュサーバをもつことで
 - 問い合わせの回数を減らすことができる
 - 問い合わせにかかる時間を短縮できる

問い合わせの方法



リソースレコード

- **DNSサーバに登録する情報**

- **管理情報**

- Authority情報(SOA)
 - ネームサーバー情報(NS)

- **IPアドレス(A, AAAA)**

- http://www.example.jp/
 - telnet www.example.jp

www.example.jp. IN A 192.168.100.1

www.example.jp. IN AAAA 2001:0DB8:1234:5678:9abc:def0:fdb9:7531

- **user@example.jpのメールサーバー(MX)**

example.jp. IN MX 100 mail-server.example.jp

- **sip:info@jprs.co.jp情報(NAPTR, SRV)**

jprs.co.jp. IN NAPTR 0 0 "s" "SIP+D2U" "" _sip._udp.jprs.co.jp.

_sip._udp.jprs.co.jp. IN SRV 0 0 5060 sip-server.jprs.co.jp.

SIP URI H.323 URI

URI

- Uniform Resource Identifier
- RFC2396として定義されていたが、RFC 3986で更新された
- インターネットに存在するリソースを一意に表現するもの
- URLを一般化し、URIとした
- URIを国際化したIRI(Internationalized Resource Identifier)も定義(RFC3987)
- EMAIL URI
 - mailto:ユーザ名@ドメイン名
 - @ドメイン名はメールサーバを指定
- SIP URI
 - sip:ユーザ名@ドメイン名, sips:ユーザ名@ドメイン名
 - @ドメイン名はSIPサーバを指定
- H.323 URI
 - h323:ユーザ名@ドメイン名
 - @ドメイン名はH.323サーバを指定
- @の右側のドメイン名は、多くの場合ISPや組織をあらわす

Email URI

- Email URI: mailto:ユーザ名@ドメイン名
- メールアドレス ユーザ名@ドメイン名
- ドメイン名をもとにメールサーバをDNS検索
- DNS登録内容
ドメイン名. IN MX preference メールサーバ名.

例. example.jp. IN MX 10 mx.example.jp.
 mx.example.jp. IN A 192.168.1.100

SIP URI

- SIPによる通信相手を特定する文字列
- RFC 3263
 - Session Initiation Protocol (SIP): Locating SIP Servers
- sip:localpart@domainpart 例: sip:info@jprs.co.jp
 - sip:localpart
 - sip:domainpart
 - domainpart
 - ドメイン名: ISPや組織(会社など)
 - domainpartをもとに、SIPサーバへの接続方法をDNS検索
 - IPアドレス、トランスポート、ポート番号
 - localpart
 - SIPサーバが管理する名前
 - 組織内のユーザ名、ISP内の電話番号など
 - ロケーションサーバにて解決

SIP URI:DNS設定

- **example.jpのSIPサーバを示すDNS設定**

- SIP URI sip:ユーザ名@example.jp
- SIPサーバのポート番号 UDP, port 5060
- SIPサーバのホスト名(IPアドレス) sip.example.jp[192.168.101.2]

```
example.jp.  IN  NAPTR  0  0  "s"  "SIP+D2U"  ""  _sip._udp.example.jp.
_sip._udp.example.jp.  IN      SRV      0  0      5060 sip.example.jp
sip.example.jp.        IN      A         192.168.101.2
```

- **NAPTRとSRV, A/AAAAを組み合わせて指定する**

SIP URI:ドメイン名解決

sip:localpart@domainpart

1. domainpartがIPアドレスの場合

- sip:の場合、そのアドレス, udp port 5060
- sips:,TLSの場合、そのアドレス, tcp port 5061

2. domainpartがドメイン名の場合:NAPTR RRを検索

- example.jpの場合、サービスフィールドSIP+D2UであるのでUDPトランスポートのSIPに対応
- _sip._udp.example.jpのSRVが、サービスを示す
- ホスト名 sip.example.jp ポート 5060
- sip.example.jpのアドレスが 192.168.101.2

3. RFC 2543との互換性

- domainpartに_sip._udpを前置してSRV検索
- _sip._udp.example.jpのSRV

4. domainpartのA, AAAAを検索

SIP補足

- **SIPS標準ポート**
 - TCP 5061
 - SIP over TLS over TCPも同様
- **SIP標準ポートは5060 UDP/TCP/SCTP**
- **SIP要素はTCP/UDPの両方をサポートしなければならない(MUST)**
- **UDPのみの相手に1300octet以上のSIP request**
 - RFC2543準拠の場合
 - そのままUDPで送る。送れなければエラー。

NAPTRリソースレコード(SIP)

SIPではNAPTRのサービスとして“SIP”を規定

- NAPTR RRはRFC 3401-3404で規定

SIP NAPTR RRの形式(RFC 3263)

label IN NAPTR *order* *pref* *flags* “SIP+*sipproto*” “” *replacement*.

- *label* SIPドメイン名
- *order* 処理順序
- *pref* 優先度(16bit符号なし整数)
- *flags* (SIPでは”s”)
- *sipproto* SIPトランスポートプロトコル指定
D2U, D2T, D2S
- *replacement* SIPサービスを指定する名前、SRV検索を行う

SRVリソースレコード

- RFC 2782
 - A DNS RR for specifying the location of services (DNS SRV)
 - ドメイン名に対するサービスの場所を指定する
- _Service._Proto.Name IN SRV Priority Weight Port Target***
- ***Service:*** 対象とするサービス: sip, sips
 - ***Proto:*** 使用するトランスポートプロトコル: udp, tcp
 - ***Name:*** ドメイン名
 - ***Priority:*** 優先度
 - ***Weight:*** 負荷分散指定
 - ***Port:*** サービスのポート番号を指定
 - ***Target:*** サービスのホスト名を指定

H.323 URI

- H.323による通信相手を識別する文字列
- ITU-T Recommendation H.323 Annex O, 2003
 - Usage of URLs and DNS
- **h323:user@hostport;*parameter***
h323:user
h323:@hostport
 - 例: h323:info@jprs.co.jp;service=cs
 - user
 - H.323ドメイン内のユーザ名、電話番号
 - hostport
 - H.323サーバのIPアドレス、トランスポート、ポート番号を指定
 - 組織、ISPなどのH.323管理単位
 - *parameter* H.323 URL拡張パラメータ

H323 URL拡張パラメータ

- **parameter**
 - user=phone @の左側の名前が電話番号である場合に指定
 - service= H.323プロトコルのサービスを指定
 - transport= トランスポートを指定
- **service**
 - ls h323ls Location Service
 - rs h323rs Registration Service 端末をサーバへ登録
 - cs h323cs Call Signaling 発呼
 - be h323be Border Element
- **transport**
 - udp UDP
 - tcp TCP
 - sctp RFC 2960 Stream Control Transmission Protocol
信頼性のあるデータグラムプロトコル
 - h323mux

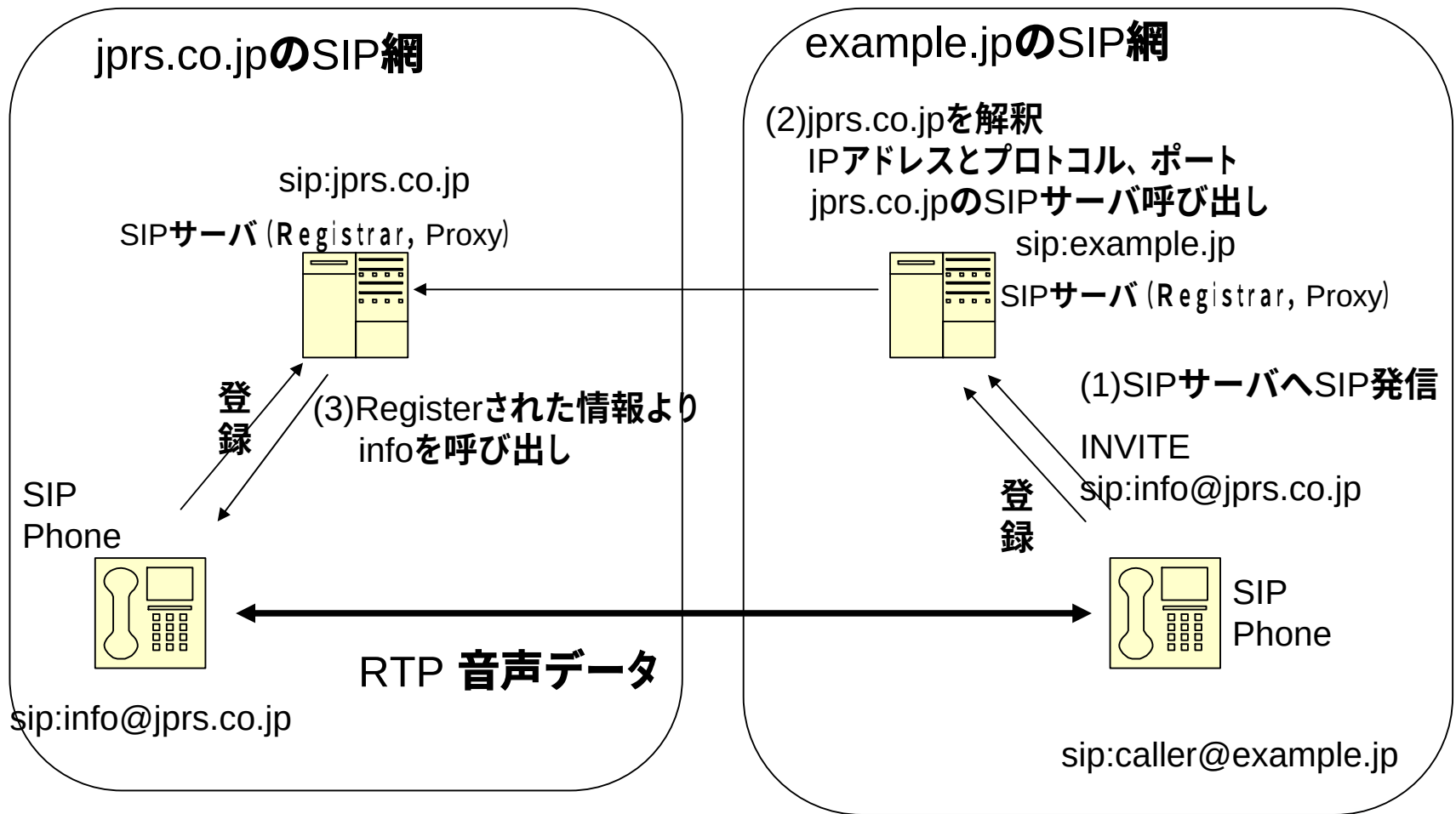
H.323 URL:アドレス解釈

h323:user@hostport;parameter hostport部は host:*port*

1. host部がIPアドレスである場合、指定IPアドレスへ接続
 - :*port*があればそのポートへ
2. hostport部がポート番号を含む場合
 - host部のA/AAAAを検索したアドレス、指定ポート番号へ接続
 - 呼び出しの場合はh323csプロトコル、tcpトランスポート
3. hostのSRVをDNS検索
 - Serviceは service parameterで指定されたもの
 - 指定がなければuser-defined: h323cs(Call Signaling)
 - Transportはservice parameterで指定されたもの
 - udp, tcp, h323mux, sctp
 - 例: h323:user@example.jp への呼び出しの場合
_h323cs._tcp.example.jpをSRV検索
→ _h323cs._tcp.example.jp. IN SRV 0 1 1720 external-gatekeeper.example.jp.
external-gatekeeper.example.jpのTCPポート1720へ接続する
4. SRVが検索できなければ、IPアドレス(A/AAAA)を検索し、標準のTCP 1720ポートへ接続

SIP URIによるVoIP通信

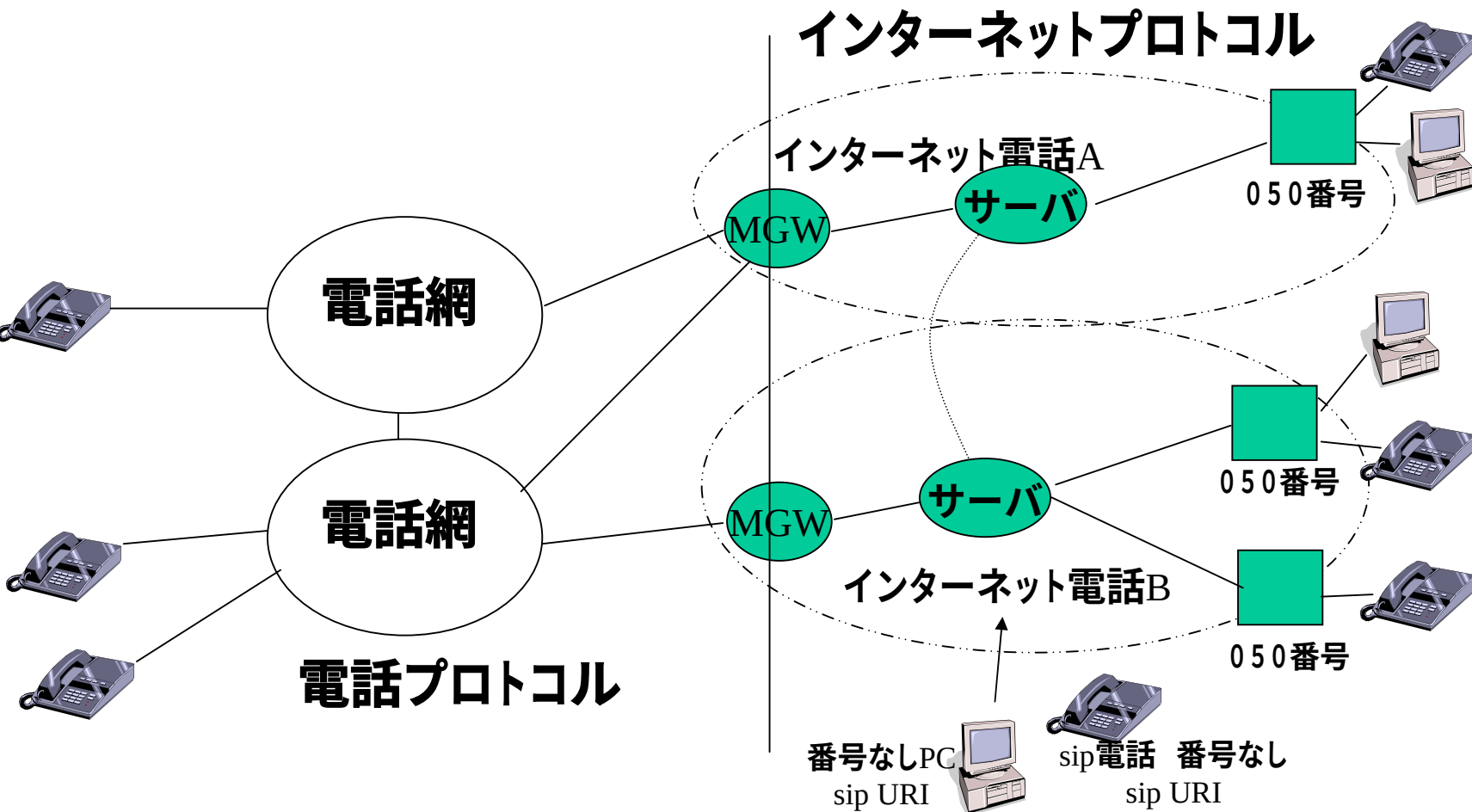
SIP URIによるVoIP通信モデル



SIP URIによるVoIP通信の特徴

- **自分で管理しているドメイン名があればSIP URIを設定、通知可能**
 - メールアドレスと同様
 - SIPサーバを用意(フリーなものあり)
 - SIPクライアントをSIPサーバに登録
- **問題点として**
 - **発信者情報確認が困難**
 - **不正なSIP callの可能性**
 - SPAM Mailと類似
 - さらに悪いことに、SIP INVITEメッセージを偽造すると、UDP packet 1つで電話が鳴る可能性あり

現在のVoIP網



現在のVoIP網 特徴

- **基本的に網内で閉じている**
 - 網外の人からは呼び出せない
 - SPAM SIPを防ぎやすい
- **SIP URIを意識させない**
 - SIP URIを使えない
 - SIP URIのうち@の左側を電話番号として経路制御
 - 050以外は固定電話網へ
 - 050xxxxはx社のSIPサーバへ
- **付加サービス**
 - 既存電話網への呼び出し

ENUM 概要

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の背景

- ・ **IP(インターネット)電話利用需要の拡大**
 - プロトコルが整備された
 - 常時かつ広帯域インターネット接続の普及 (ADSL,CATV,FTTH等)
 - 低価格化
- ・ **E.164電話番号の存在**
 - 数字だけで指定可能 ---- 言語に依存しない
 - 国際的にユニーク
 - 公衆電話網で利用されている

ENUMの可能性

利用者の視点から

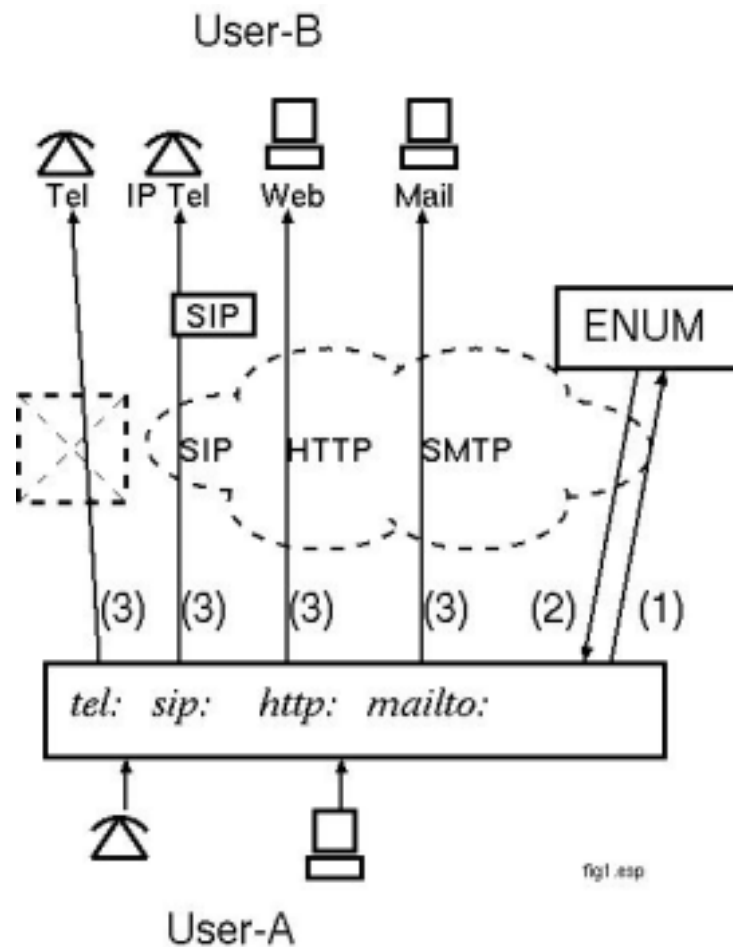
- 複数のIDを1つのE.164番号に集約できる
 - ・ 電話番号、FAX番号、メールアドレス、ホームページ、など
- 通信成立の可能性の増加
 - ・ 回線がビジーの時でも他のURIで接続を試せる

事業者の視点から

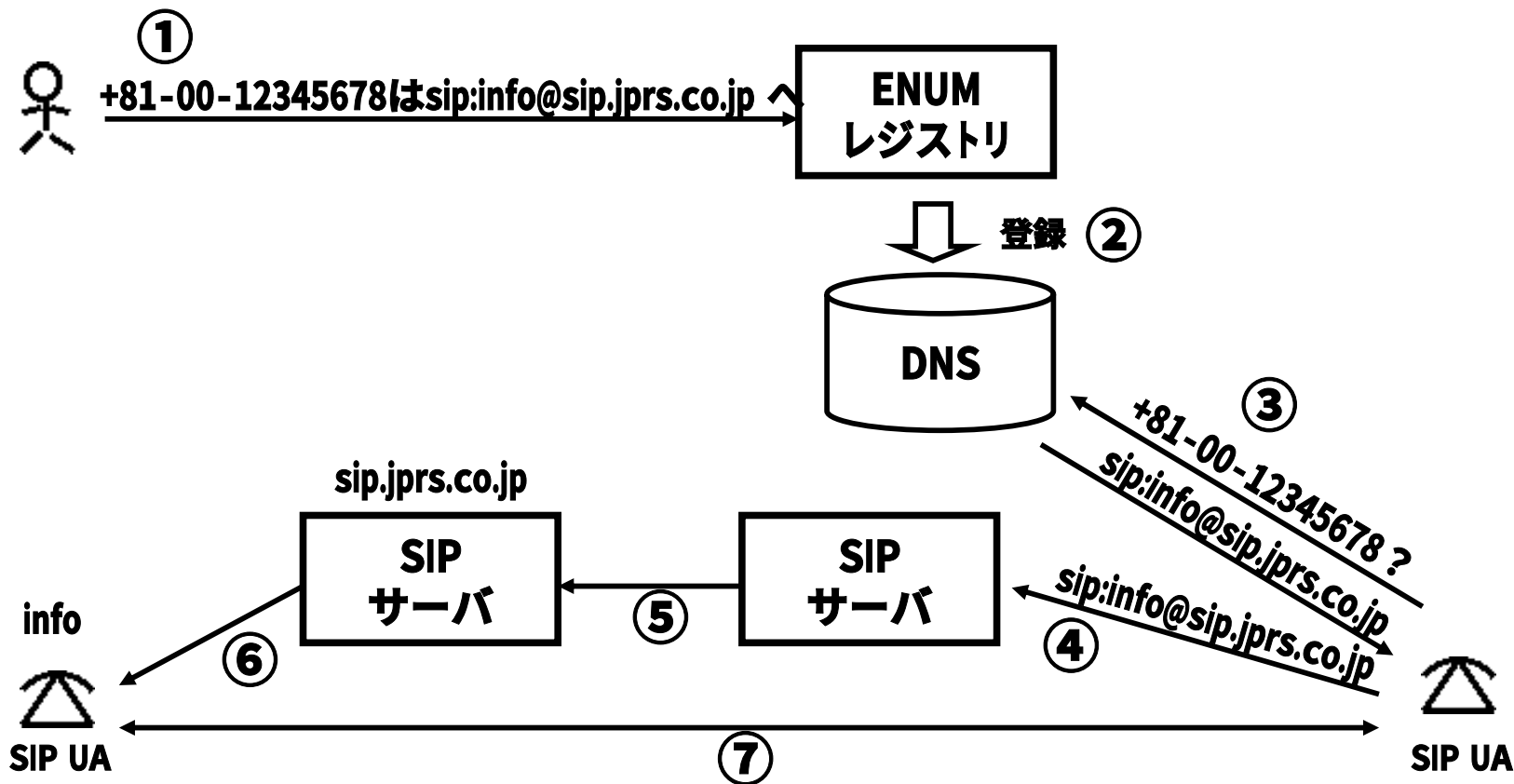
- 電話網(含むIP電話網)の番号解決手段として
 - ・ PSTNからインターネット電話
 - ・ インターネット電話からPSTN
 - ・ インターネット電話からインターネット電話
 - ・ オープンなプロトコルなので相互接続性の確保が容易

アプリケーションの選択

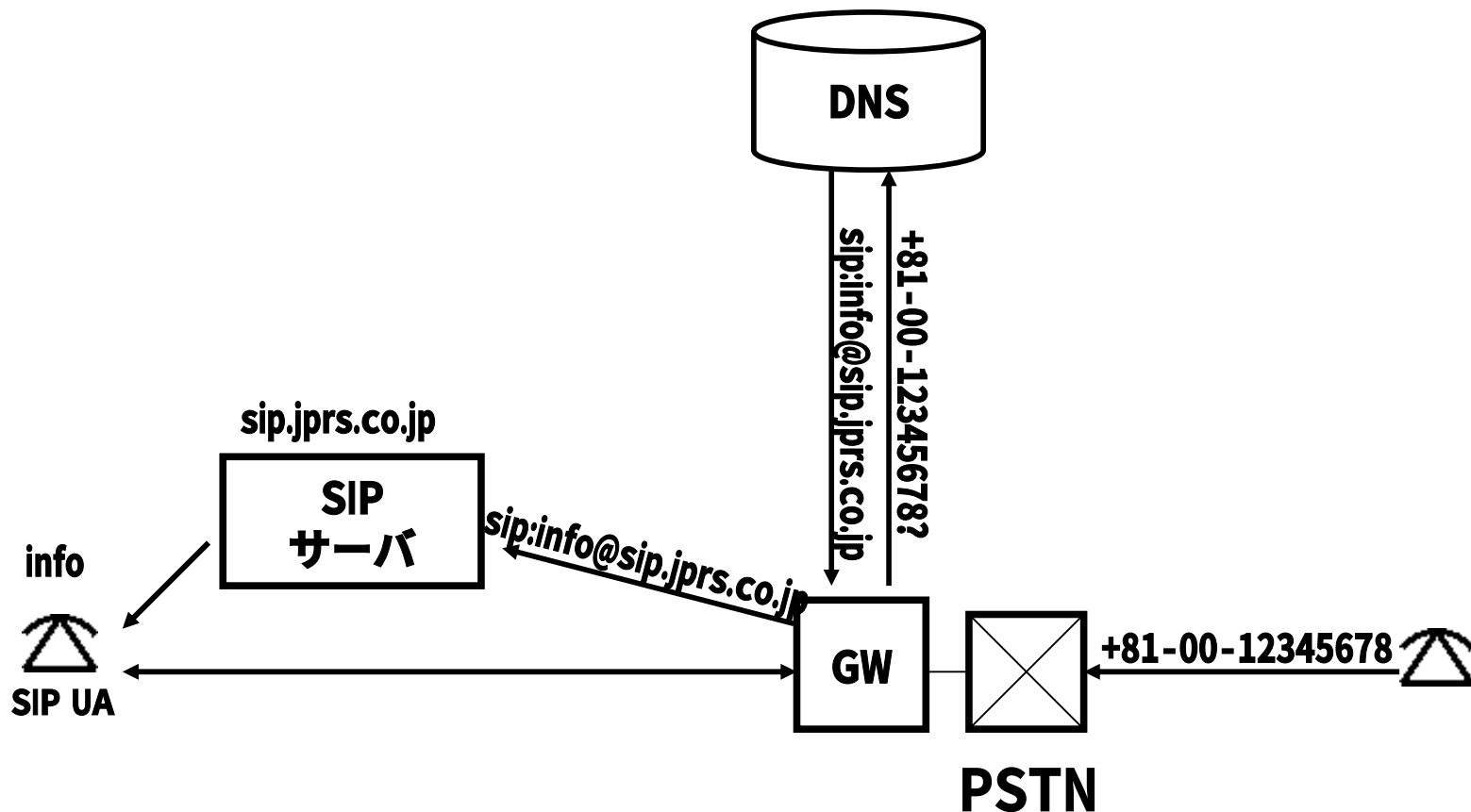
- (1) DNSを検索
- (2) 応答
- (3) アプリケーションを選択し接続



インターネット電話からインターネット電話



PSTNからインターネット電話



ENUM標準(プロトコル)

IETF ENUM WG

- 1999年に設置
- <http://www.ietf.org/html.charters/enum-charter.html>
- E.164電話番号をドメイン名として表現するためのDNSに基づくアーキテクチャとプロトコルを定める
- 目標
 - プロトコルを定める
 - ENUMを運用管理するためのドキュメント作成
 - Privacy, securityについて強く考慮する
 - DNSEXT WG, PROVREG WGと協調
 - DNSが望ましく使われるようにITU-T SG2と協調
(ITU-T SG2 = ITU-T内でのENUM標準化組織)
 - ENUMコミュニティ内の技術的な情報交換を促進する

ENUMプロトコル: RFC 3761

- ・ The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)
- ・ 2004年4月発行
- ・ E.164番号にURIを対応付ける方法を規定
 - ・ E.164番号をDNSドメイン名に対応
ENUM DNSツリーとして“e164.arpa”を規定
 - ・ NAPTRリソースレコードを用いてURIを登録(DDDS)
- ・ 2000年9月に発行されたRFC 2916を改定
 - ・ DDDS(RFC 3501-04)アプリケーションとして再定義
 - ・ 仕様の明確化

E.164番号

- ITUで標準化

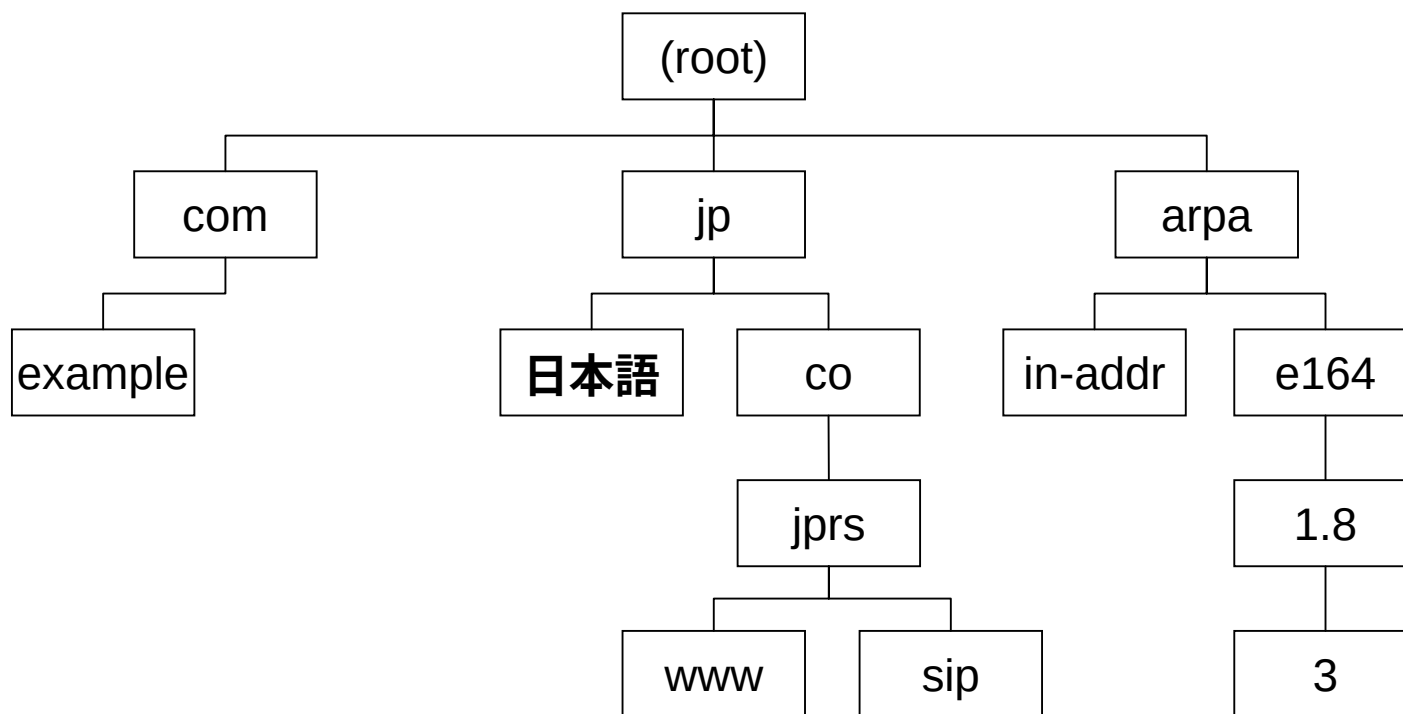
- 形式

- 先頭は‘+’
- 国コード(country code)が続く
- 国内の電話番号が続く
 - ・ 頭の0は削除
- 10-15桁の数字

- 日本の場合

- 国内 03-5297-2571
- E.164 +81-3-5297-2571

DNSツリー



E.164番号からドメイン名への変換

- RFC 3761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RFC 3401-3404で規定

ENUM NAPTR RRの形式(RFC 3761)

label IN NAPTR *order* *pref* *flags* “E2U+*enumservice*” *regexp*.

- *label* E.164番号のドメイン名形式
- *order* NAPTR RR処理順序(ENUMでは100)
- *pref* NAPTR RR優先度(16bit符号なし整数)
- *flags* NAPTR RRの動作指定(ENUMでは“u”)
- *enumservice* NAPTR RRの示すサービス/URI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.jp.rs.co.jp
H.323	3762	E2U+h323	h323:info@h323.jp.rs.co.jp
Presence	3953	E2U+pres	pres:support@im.jp.rs.co.jp
Email	msg-04	E2U+email:mailto	mailto:info@jp.rs.co.jp
WEB	4002	E2U+web:http	http://www.jp.rs.jp/
FTP	4002	E2U+ft:ftp	ftp://ftp.jp.rs.jp/
InternetFAX	*1	E2U+ifax:mailto	mailto:fax@fax.jp.rs.co.jp
会議	*2	E2U+conf-uri:sip	sip:

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

*1 draft-ietf-fax-faxservice-enum-03.txt

*2 最近議論開始、draft-johnston-enum-conf-service-00.txt

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.jp.rs.jp!” .

結果は ‘sip:info@sip.jp.rs.jp’

\$ORIGIN 8.7.6.5.4.3.2.1.0.0.1.8.e164.arpa.

IN NAPTR 100 10 “u” “E2U+msg” “!^\.*\$!mailto:info@jprs.jp!” .

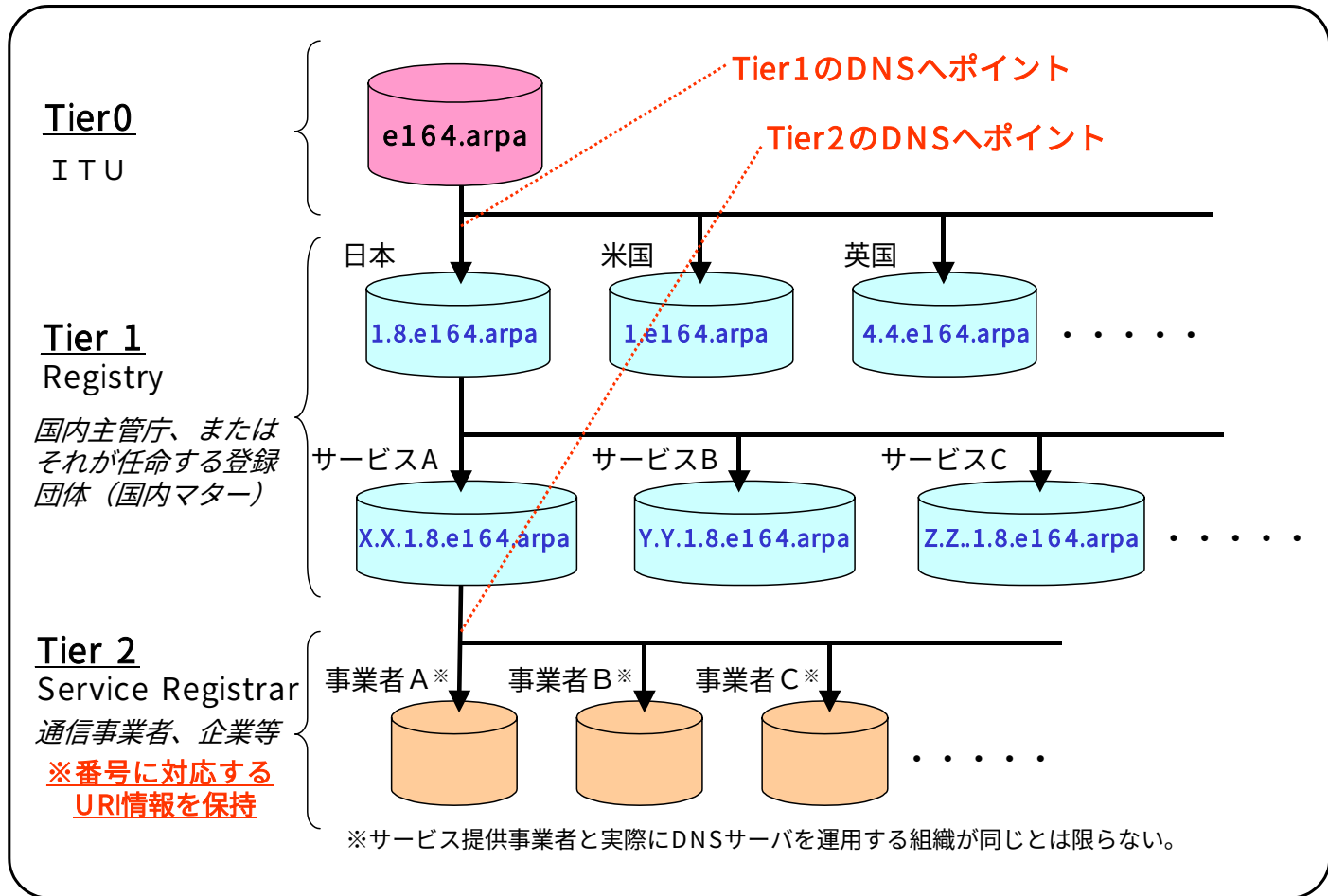
結果は ‘mailto:info@jprs.jp’

ENUMトライアルの状況

ENUMトライアル

- **実運用を前提とした試行**
- **ITUとIETF/ISOCが協調して実施**
 - RFC 3026 Liaison of IETF/ISOC on ENUM (by ITU)
- **ENUM運用に関する決定の経緯(RFC 3245)**
 - **e164.arpa ドメインの理由**
 - 一つのDNS treeである必要性
 - arpa TLDはin-addr.arpaとしてIPv4逆引きに用いられてきた
→インフラ用TLDとして再定義
Address and Routing Parameter Area(RFC 3172)
 - **E.164番号の国コードの管理はITU**
→ **国別TLDの委任の管理はITU**
 - **DNSの管理はIAB/ICANN**
 - ENUM TLDの管理をRIPE NCCに委任

ENUM DNSサーバの階層構造



総務省「IPネットワーク技術に関する研究会 報告書」2002年2月

◆ ENUMの管理・運用に関する役割分担

ドメイン	①Manager (管理責任者)	②Registry (レジストリ)	③Registrar (登録審査者)	④Registrant (登録申請者)
ENUM Tier 0 e164.TLD	IAB (現時点)	RIPE-NCC ^{注1)} (現時点)	ITU事務局 ^{注2)}	加盟国
ENUM Tier 1 <CC> .e164.TLD	加盟国	国内マター (加盟国/主管庁 もしくは、それが 任命する団体)	国内マター (通信事業者・ ISP等)	国内マター
ENUM Tier 2 <N(S)N>.<CC> .e164.TLD	国内マター	国内マター	国内マター (通信事業者・ ISP等)	国内マター (ENUM加入者)

注1: Réseaux IP Européens
Network Coordination Centre

注2: ITU-Tの事務局。国番号、国際ポイントコード等の国際番号リソースの割当・管理を実施。正式名はITU-TSB
(Telecommunications Standardization Bureau of the ITU)

総務省 平成14年度 電気通信番号に関する研究会」(第2回)

資料2-2 ENUMに関するITU-T SG2標準化動向 7ページ

http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/bango/pdf/020704_2_0247.pdf

ENUM DNS構造

- **Tier0: ENUM DNSの最上位階層**
 - e164.arpa
 - ITU-Tが管理、RIPE NCCが運用
- **Tier1: E.164国番号のENUM DNS階層**
 - 1.8.e164.arpa. (日本の場合)
 - 管理・運用は国内マター
- **Tier2: 末端(NAPTR RR)のENUM DNS階層**
 - 1.7.5.2.7.9.2.5.3.1.8.e164.arpa
 - 管理・運用は国内マター

ユーザENUM / オペレータENUM

ユーザENUM

- 利用者(E.164番号所有者)は自らの意思でNAPTRを登録可能
 - ・ いろいろなENUMサービスを選択できる
- 利用者は正当な番号所有者か要確認
 - ・ 中立な番号認証機関が必要

オペレータENUM

- 事業者(キャリア、ISPなど)が割当を受けている番号にNAPTRを設定
 - ・ ENUMサービスは制限されるかも
- 事業者間の経路制御のために利用
- ENUM DNSは事業者間に閉じる可能性
 - ・ 利用者はNAPTR RRを参照できないかも

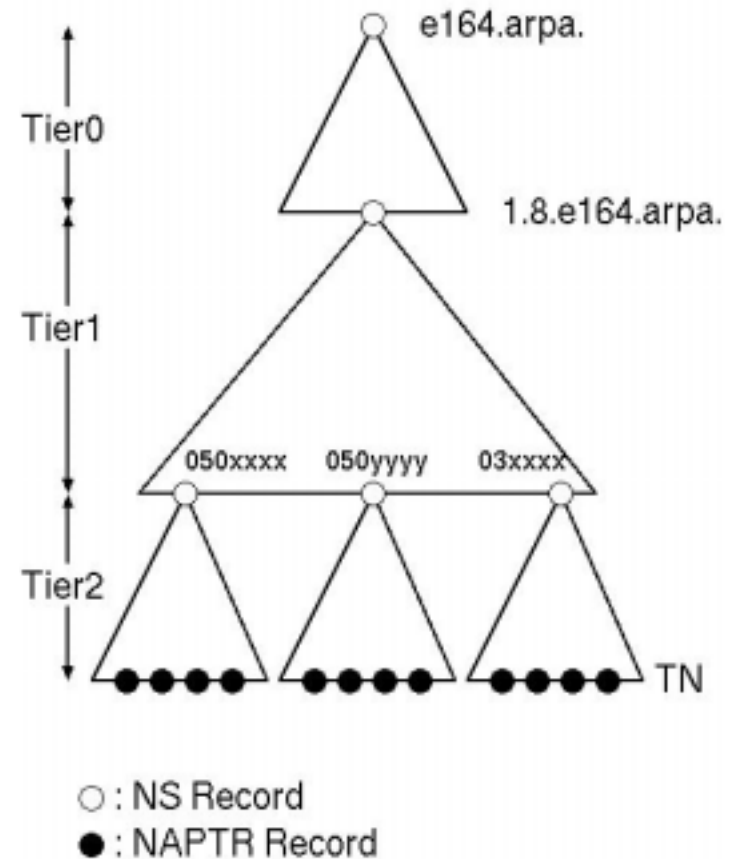
運用形態は大きく異なる

階層構造: 例1

Tier1はTier2に番号帯を委任

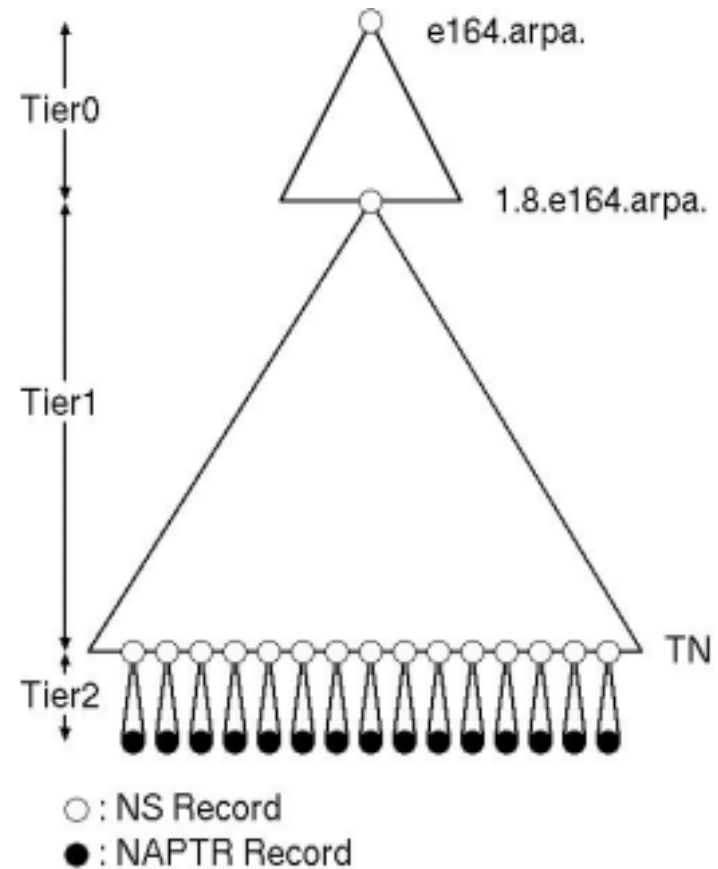
日本の場合は番号割当単位ごと

- 携帯電話は10万番号単位
- 050番号は1万番号単位



階層構造: 例2

- ・ Tier1はすべての番号を個々にTier2に委任
- ・ 番号ポータビリティを実現しやすい



各国の状況

オーストリア

- ENUM商用サービス
 - ・ 2004年12月に開始、世界最初
 - ・ 既存の固定電話、携帯電話などの番号をENUM登録
- ENUM専用番号の割り当て(2005年5月から)
 - ・ 個人番号を、first-come-first-serveで登録
 - ・ 既存電話とENUM/インターネットの両方から接続可能
 - ・ SS7 to VoIP gateway(SIP/H.323)
 - ・ インターネットユーザはENUM検索し、SIP/H.323発信
- ENUMを使ってVoIP推進

各国の状況(2)

- **CC1 ENUM LLC**

- Country Code 1 ENUM Limited Liability Company)
- Country Code 1 (北米地区)でのENUM運用を行う組織
- 各国政府からの承認を得て開始予定
- AT&T, GoDaddy.com, MCI, SBC Laboratories, Sprint, Verizon, BellSouth
- <http://www.enumllc.com/>

- **東アジア地域**

- APEET (Asia Pacific ENUM Engineering Team)を組織し、実際的なトライアルを推進
- 2005年2月に京都で開催されたAPRICOT2005で、ENUM/SIPデモを実施
- <http://www.apenum.org/>

委任状況

ITU-T SG2: E.164 country codes for which TSB has received approvals for ENUM delegations to be performed by RIPE NCC

Notes:

(a) This is a Universal Personal Telephony (UPT) code.

(b) DELETED, referred to 991 001 which is no longer assigned or delegated for ENUM.

(c) This is a temporary authorization for ENUM global TLD trial and evaluation. This delegation will end on 30 June 2005. If the ITU Interim Procedure is discontinued before then, or if the Recommendation E.A-ENUM is approved before 30 June 2005, the delegation will be turned into an objection.

(d) This is a country code and associated identification code for Networks (shared country code).

(e) This delegation will end on 31 October 2005.

出典: <http://www.itu.int/itudoc/itu-t/enum/enum/>

E.164 Country Code	Country	Delegee	Date of TSB Approval dd/mm/yy
246	Diego Garcia	Government	12/08/02
247	Ascension	Government	12/08/02
290	Saint Helena	Government	12/08/02
31	Netherlands	Ministry	23/05/02
33	France	DiGITIP (Government)	28/03/03
353	Ireland (e)	Commission for Communications Regulation	25/05/04
354	Iceland	Post and Telecom Administration	28/02/05
358	Finland	Finnish Communications Regulatory Authority	26/02/03
36	Hungary	CHIP/ISzT	15/07/02
374	Armenia	Arminco Ltd	11/07/03
40	Romania	MinCom	10/12/02
41	Switzerland	OFCOM	01/10/03
420	Czech Republic	Ministry of Informatics	24/06/03
421	Slovak Republic	Ministry of Transport, Post, and Telecommunications	04/06/03
423	Liechtenstein	SWITCH	21/10/03
43	Austria	Regulator	11/06/02
44	UK	DTI/Nominum	16/05/02
46	Sweden	NPTA	10/12/02
47	Norway	Norwegian Post and Telecommunications Authority	16/03/05
48	Poland	NASK	18/07/02
49	Germany	DENIC	16/05/02
55	Brazil	Brazilian Internet Registry	19/07/02
61	Australia	Dept of Communications, Information Technology and the Arts	17/01/05
65	Singapore	IDA (Government)	04/06/03
86	China (c)	CNNIC	02/09/02
878 10	(a)	VISIONg	16/05/02
971	United Arab Emirates	Etisalat	13/01/03
882 34	(d)	Global Networks Switzerland AG	05/03/04

日本のENUM活動

ENUM研究グループ

- **2002年9月設立**
- **目的**
 - ENUMの実現方式、運用方式、またこれらに関する検討
 - ENUMに関連する技術的課題の検討
 - ENUMの実現及び運用における制度上の課題の検討
- **研究対象**
 - ENUM技術
 - DNS、URI、DDDSなどの関連技術
- **最終報告**
 - 2003年5月発行

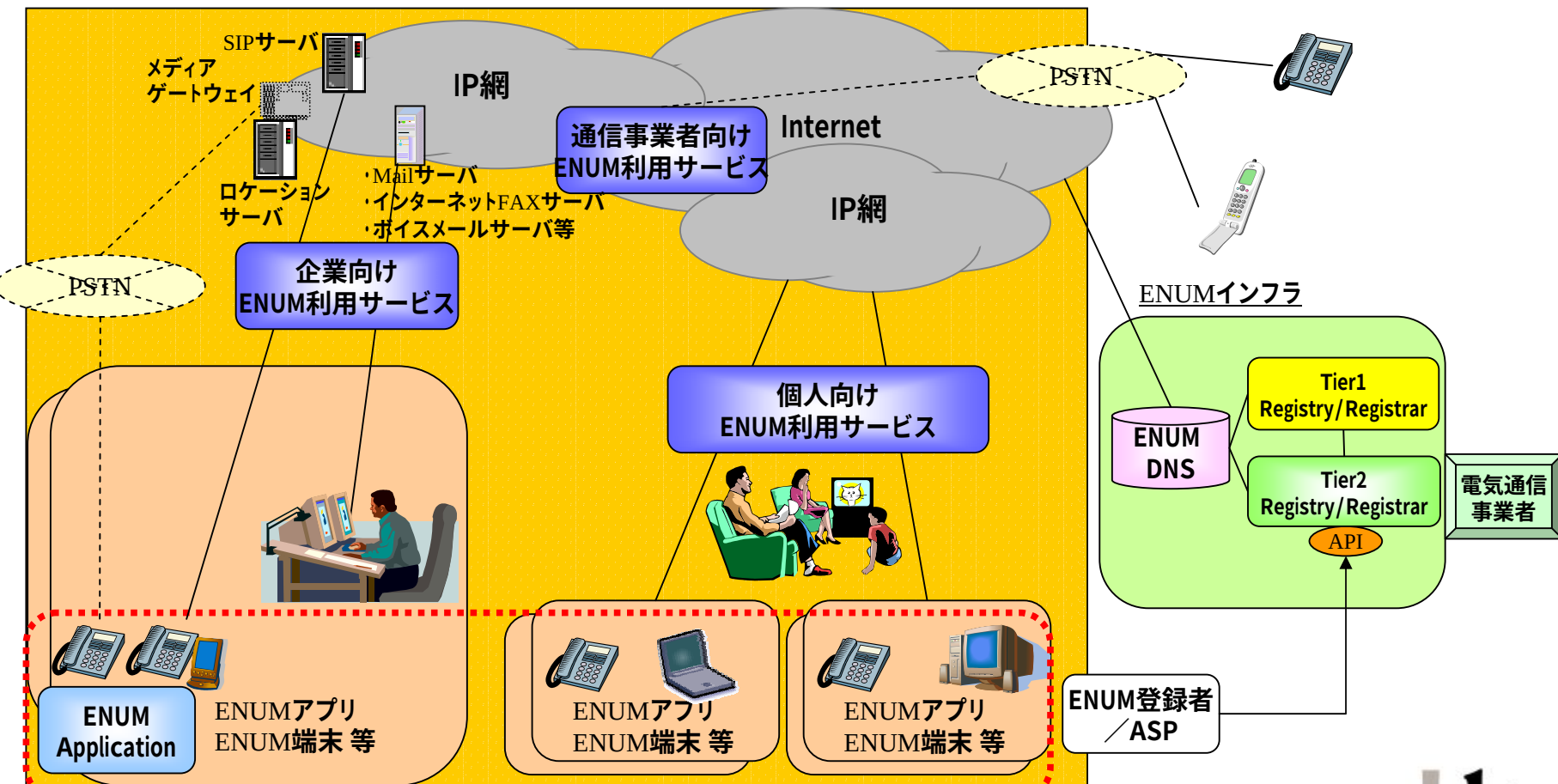
ENUMトライアルジャパン(ETJP)

- **WIDE Project, JPNIC, JPRSを中心に設立**
 - 2003年9月17日
- **ENUMに関連する技術検証の場**
 - ENUMの基盤サービス
 - アプリケーション、サービスまでを含む基本機能と実用性
 - 諸外国のトライアルと連携した国際レベルの相互接続性
- **現在42会員(個人会員を含む)**
 - 貢献できる物を持つ人は誰でも会員になることができる
- **2004年11月にENUMトライアルジャパン第2次報告書公開**
- **<http://etjp.jp/>**

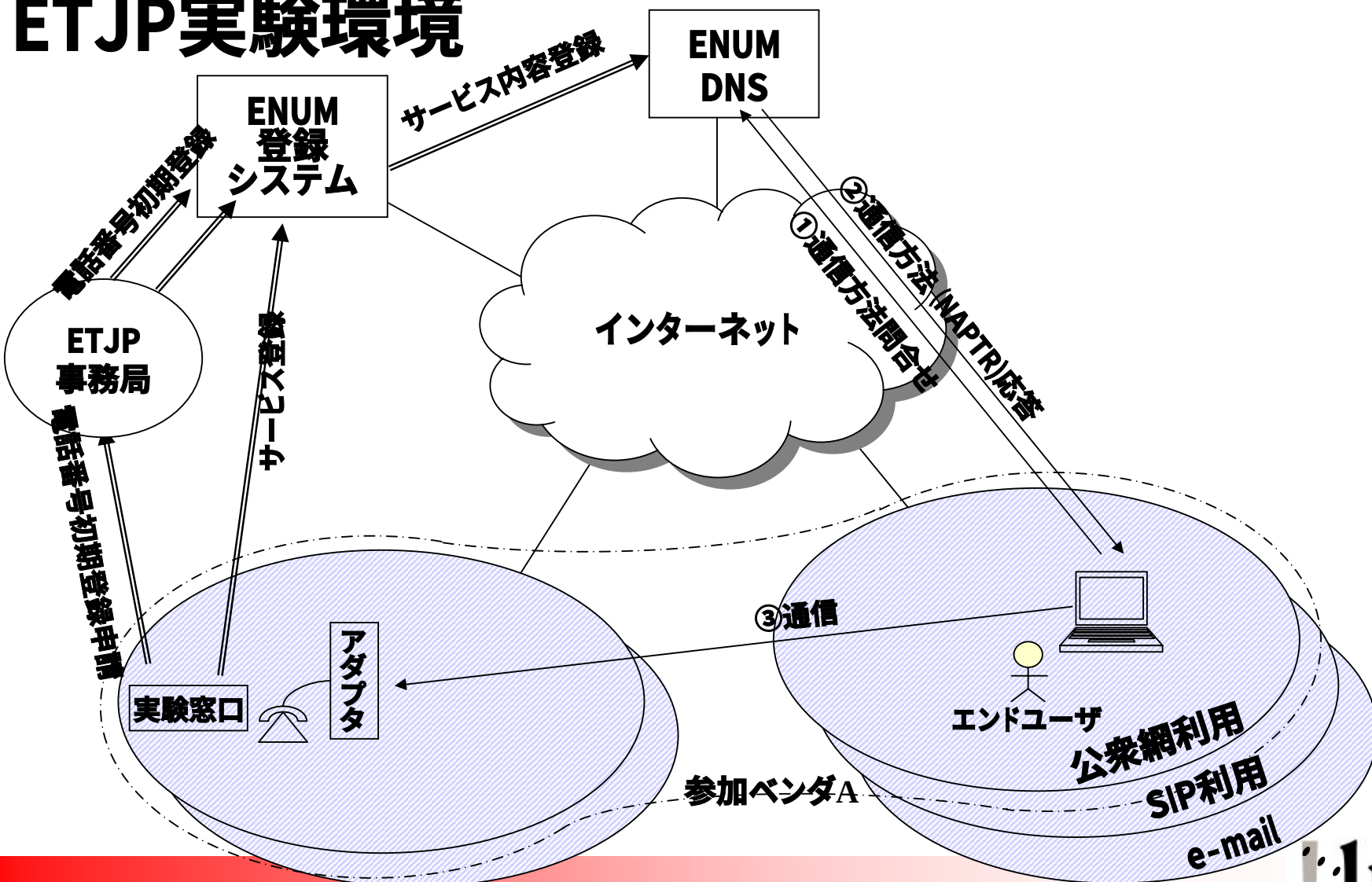
ETJP主な活動

- **ENUM実験環境構築**
 - ENUM レジストリシステム
 - ENUM DNS
- **アプリケーションの試作と動作確認**
 - ENUM対応SIPサーバ
 - ENUM対応SIP UA
 - CGIによるENUMクライアント
 - Windowsクライアント
- **ENUM応用システム試作**

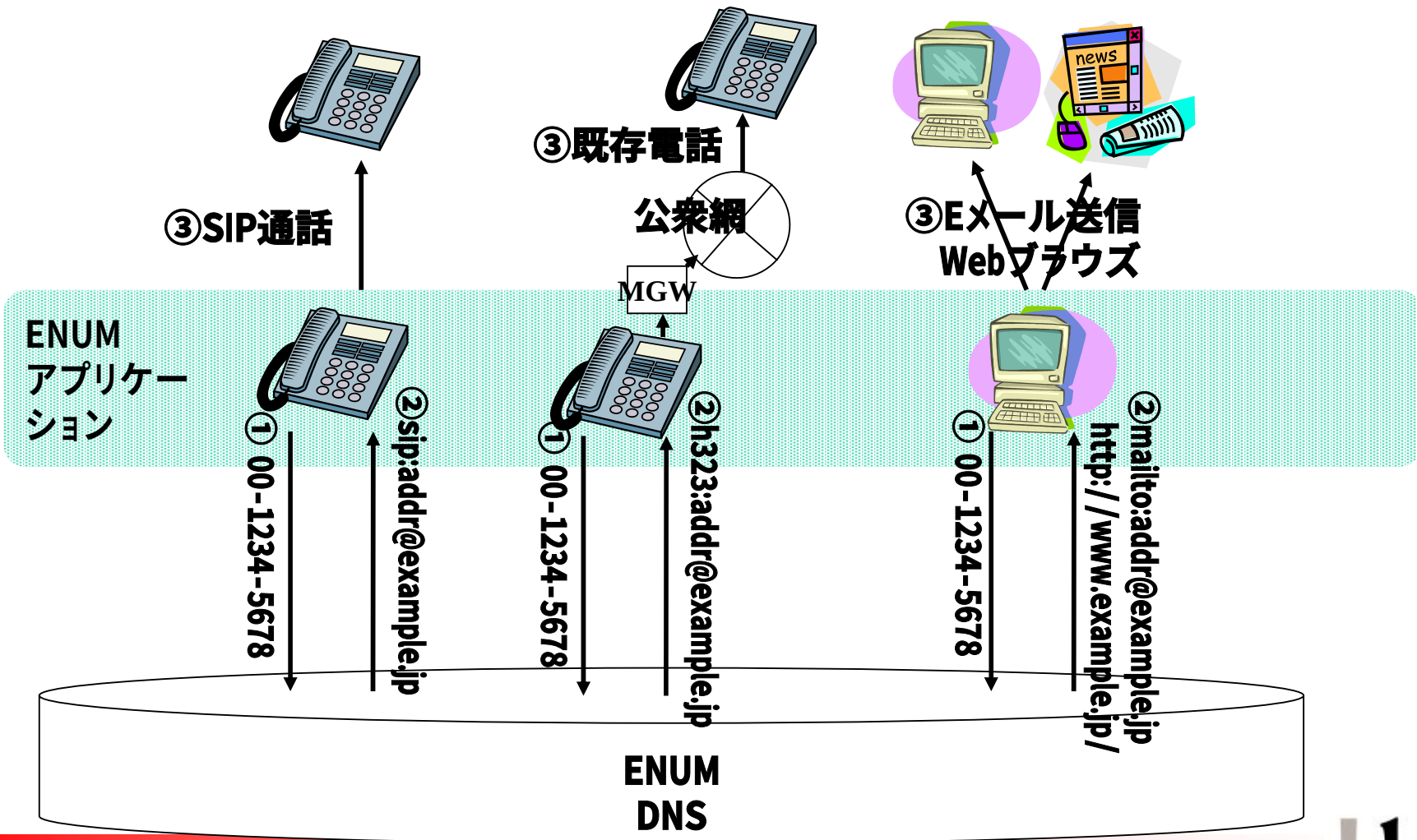
想定しているENUM世界



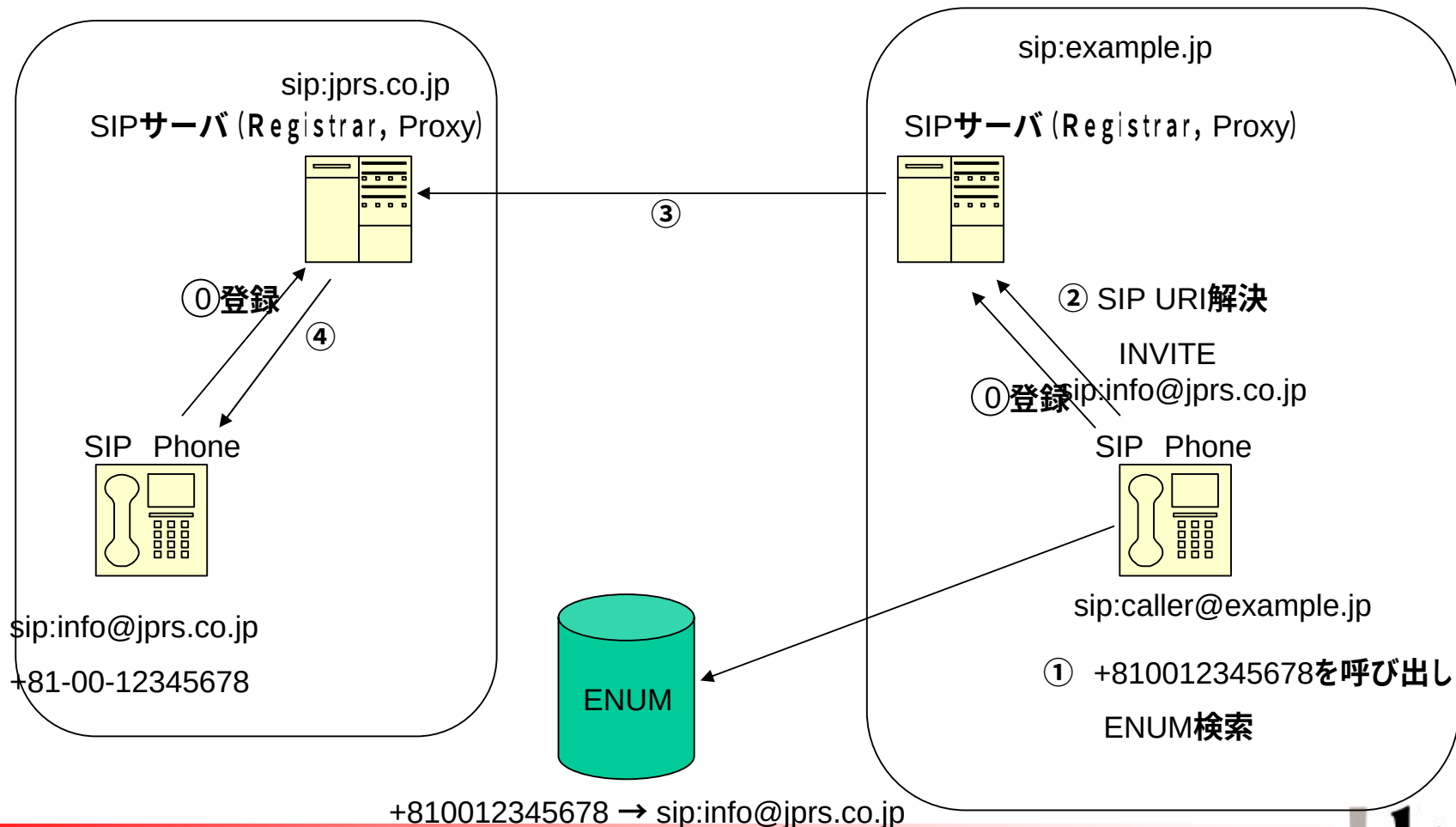
ETJP実験環境



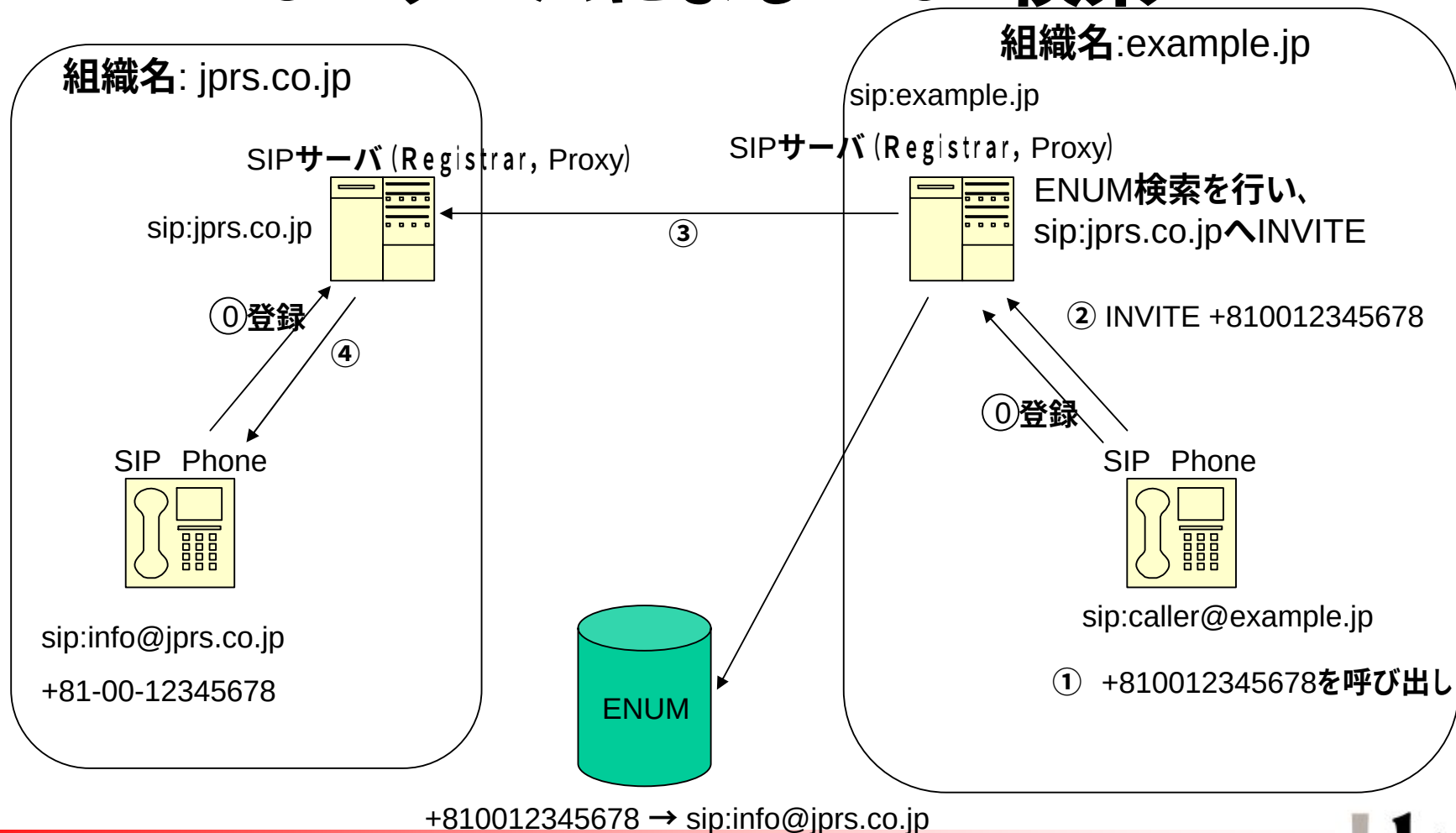
ENUMをベースとした通信のイメージ



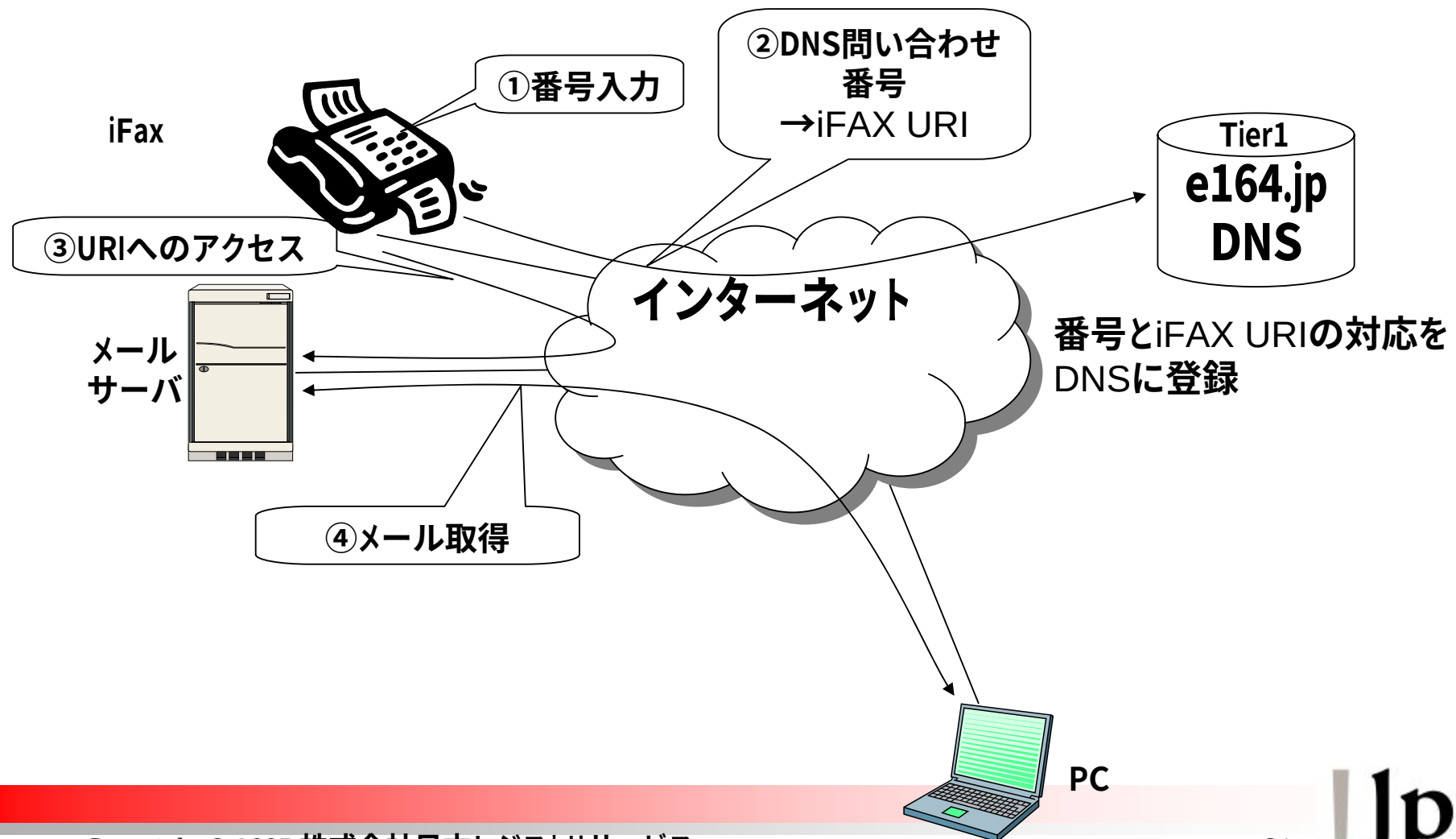
SIP UAによるENUM検索



SIPサーバによるENUM検索



iFAX



ENUMの課題

ENUMの課題(1)

利用形態、ビジネスモデル

- オペレータENUM / ユーザENUM
- 管理主体、責任
- 課金

DNS運用

- 階層(Tier)構造
- DNSサーバの配置
- NAPTR RRの登録

アプリケーション開発

- ENUMクライアント
 - ・ メール、SIP電話などを統合するENUMアプリケーション
 - ・ 携帯電話

ENUMの課題(2)

セキュリティ

- DNSデータ
- ENUMデータ
- 利用者(アプリケーション)間の通信データ

プライバシー

- 利用者情報 (whois)
- 匿名性
- 行動の追跡

制度との関係

- 特に電気通信事業法との関係
 - 「ENUMによる電話」と「音声役務」
 - 他の役務を識別するために電話番号を使ってよいか
 - どの電気通信番号を用いるか

ENUMの課題(3)

- **ENUMをSIP電話の番号解決に用いるにはSIP URIによるSIP網が必須**
 - **ENUM、SIP URIを公開すると、どの相手からのSIP INVITEにも応答する必要あり**
 - **電子メールと同様のSPAM問題が発生する可能性あり**

参考URI

- **IETF ENUM WG**
 - <http://www.ietf.org/html.charters/enum-charter.html>
- **ITU-T**
 - <http://www.itu.int/osg/spu/enum/>
- **RIPE NCC**
 - <http://www.ripe.net/enum/>
- **ETJP**
 - <http://etjp.jp/>
- **ENUM研究グループ**
 - <http://www.nic.ad.jp/ja/enum/>

将来への展望

DNSSECの導入・普及

DNSSECとVoIP

- **現在のインターネットはDNSに深く依存**
 - VoIPのサーバ名をホスト名で指定
 - SIP URI
 - H.323 URL
 - ENUM
- **DNSプロトコルのSecurity拡張 DNSSEC**

DNSSECとは

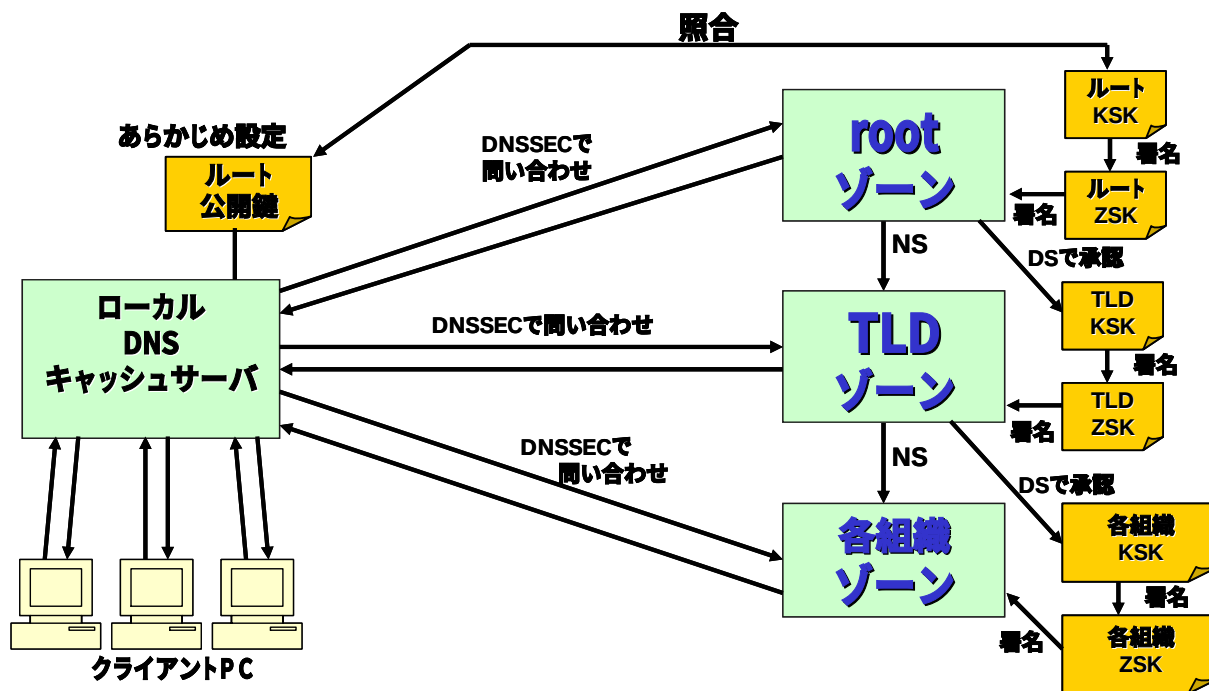
- **DNS Security Extensions**
- **DNSゾーンに権限を持つ管理者が、公開鍵暗号技術を用いて、自らのゾーン情報に秘密鍵で署名を行うDNSの運用方式**
 - **ゾーンの公開鍵で検証**
 - **そのゾーン情報の第三者による改ざん・騙りを検証することが可能となる技術**
 - **これにより、万一にも騙りを許したくないDNSレコードを守ることが可能となる**

DNSSEC署名

- **ゾーンごとに公開鍵・秘密鍵作成**
 - 公開鍵を公開 DNSKEYリソースレコード
- **RRsetへの署名RRSIG(name, type) = RRsetの内容のハッシュ値をゾーン秘密鍵での暗号化したもの**
 - name,typeについてのRRsetのハッシュ値 =
hash(RRSIG_RDATA|RRset(name, type)))
 - RRsetはsortして連結
 - RRSIG RDATAは、RRSIGのRDATAから署名情報を除いたもの
 - RRSIG type algorithm ラベル情報 TTL 有効期間 鍵情報 署名情報
 - RRSIGは、ラベル名、タイプ、クラス(IN)ごとに存在
 - RFC3110 RSASHA1 公開鍵暗号=RSA, hash=SHA-1
- **署名検証**
 - RRSIGの署名をゾーン公開鍵で復元したものと、RRsetの内容のハッシュ値を比較

DNSSEC:信頼の連鎖

- 鍵による信頼の連鎖 (chain of trust)を形成
- KSKとZSKの2つの鍵を使用



DNSSEC protocol

- **RFC4043,4044,4045として定義**
- **ゾーン管理者は2つの鍵を使用**
 - **KSK (Key Signing Key):親ゾーンに登録する鍵**
 - KSKで自分のZSKを署名する
 - 頻繁に更新しないため、強い鍵を用いる
- **ZSK (Zone Signing Key): 自ゾーンの署名のための鍵**
 - 比較的弱い鍵で、頻繁に更新し、署名しなおす
 - 大量に署名する場合の署名コストを減らすため
- **DS (Delegation Signer)資源レコードを使用**
 - 親ゾーンの委任ポイントに子ゾーンから登録された子ゾーンのKSK公開鍵情報を登録
 - 子ゾーンのKSKと暗号論的に等価なDS情報
 - DSにより子ゾーンのKSKの正当性を親ゾーンが承認
- **ルートの公開鍵情報を、DNSSEC検証者が持つ**
 - 主にDNSキャッシュサーバ

DNSSEC標準化(IETF)の現状

- IETFのdnsexp wgにおいて、DNSSECプロトコルを策定
 - RFC4033, 4034, 4035として2005年4月に発行
- 未解決の課題
 - ルート鍵の運用
 - dnssec-deployment wg
 - 現在の仕様では、ゾーン内のデータを網羅検索可
 - セキュリティ、プライバシー的な懸念
 - IETF dnsexp wgにて解決策を検討中

DNSSECの課題

- 普及(deployment)
 - 利用するためにはキャッシュサーバの対応が必須
 - 安全な鍵配布・鍵更新の手順が別途必要
 - アプリケーションのDNSSEC対応が必要
- 実装(implement)
 - Authoritativeサーバ
 - BIND 9.3系列からDS方式をサポート
 - BIND 9.3.1
 - NSD 2.0.0以降でDS方式によるDNSSECをサポート
 - ただしNSDはDNS authoritativeサーバ機能のみを提供
 - キャッシュサーバ
 - BIND 9.3系列のみ(9.3.1)
- ユーザーインターフェース
 - DNSSECで守られたかどうかわかりにくい

ETJP DNSSEC実験

- **ETJP ENUMテストベッドにて、DNSSEC実験中**
 - **ENUM型ドメイン名** **e164.jp**
 - 安全な、電話番号からURIへの変換
 - **通常のドメイン名空間** **dnssec.jp**
 - URIを安全に登録
- **DNSSEC対応ENUM, ドメイン名登録システム**
- **DNSSEC対応アプリケーション**

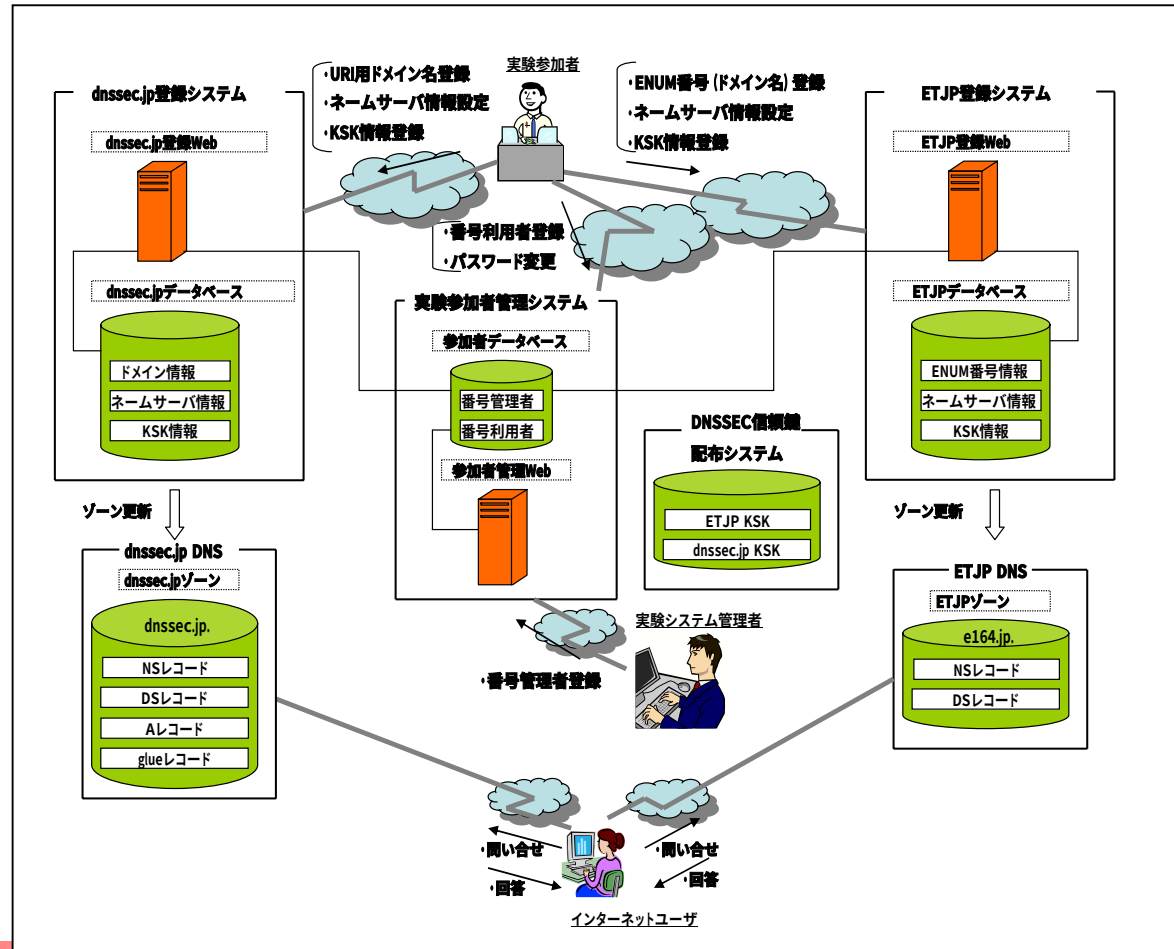
DNSSEC登録システム

- BIND 9.3を使用
- ドメイン名登録システムにKSK管理機能を追加
- 安全な信頼鍵配布システムを提供
 - httpsを使用



DNSSEC登録システムを用いたJP実証実験

- 実際のJPドメイン名配下で実施
 - 全国規模
- 実験参加者は信頼ドメイン名配下にドメイン名を登録し、ゾーンを設定
- レジストリは、
 - 実験参加者からの登録を受け付け、DNSデータを公開
 - dnssec.jpとe164.jpを信頼ドメイン名として、公開鍵を配布
- インターネットユーザは配布された鍵をもとに実験参加者のドメイン名を検証



JP実証実験全体図

クライアント側の検証

- **DNSSECへの移行促進の必須要件**
 - DNSSEC対応サーバからの応答の正当性確認
- **DNSSEC確認ツールの試作**
 - ⇒DNSSEC対応クライアントとして、ユーザに伝えるべき項目を検証

DNSSEC確認ツール試作による効果

- ユーザへの通知項目
 - 該当レコードの存在確認
 - DNSSEC対応状況
 - DNS応答の正当性
 - ⇒そのドメインを利用する前に、安全性がわかる
- DNSSECサーバ⇔クライアント間プロトコル
 - 検証失敗理由の通知
 - 通信路の安全化
 - ⇒現在の実装では不十分であることが判明



DNSSEC確認ツール 確認画面

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>
- **DNSSEC Deployment group**
 - <http://www.dnssec-deployment.org/>

ENUMによるVoIPキャリア間接続

IP電話の現状と課題

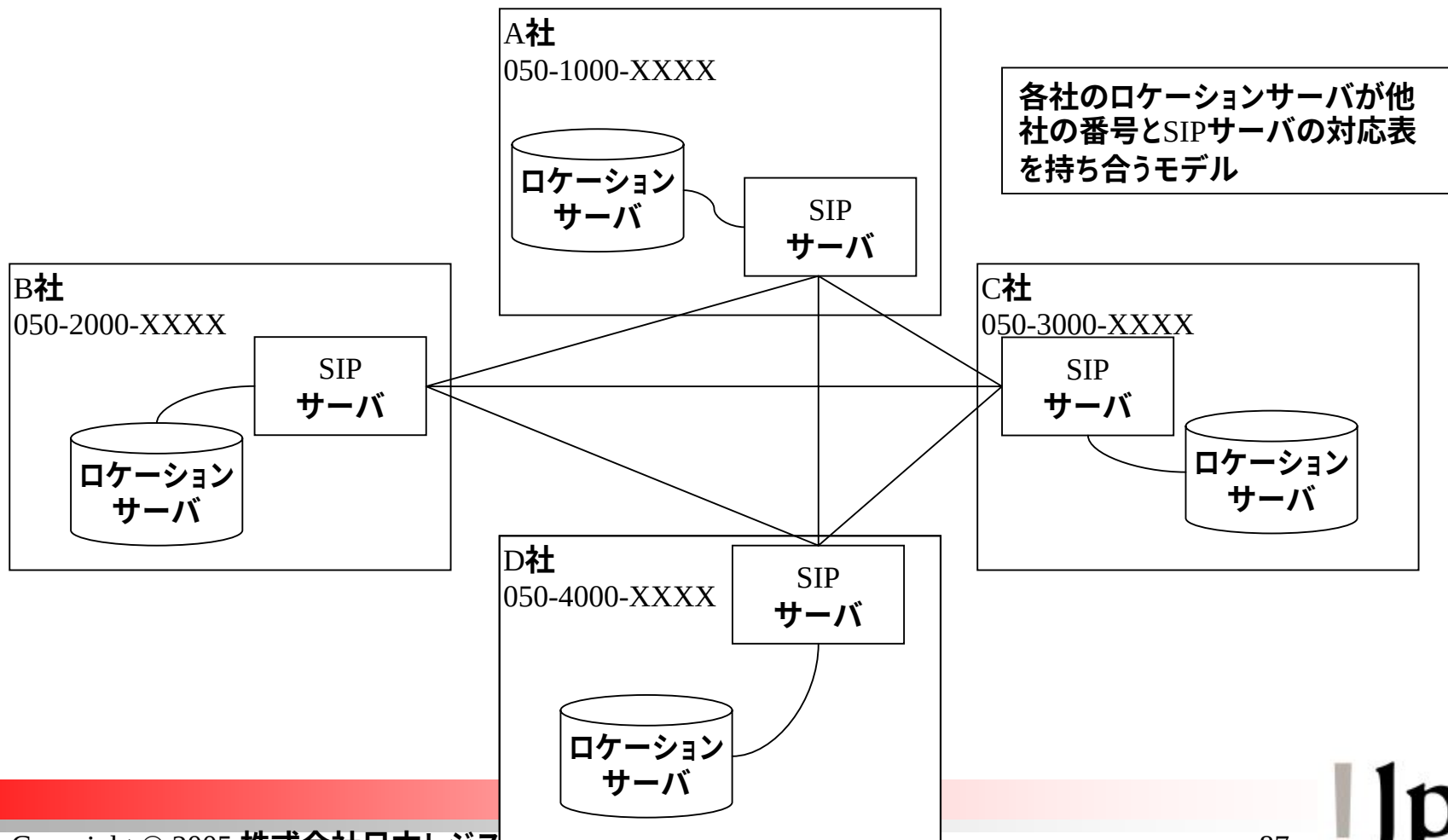
- **IP電話の現状**

- **急速に普及が進んでいる**
 - 050番号の運用開始により着信も可能に
- **電話料金が「安い」**
 - 同一ISP/キャリアグループ内なら「無料」
 - 通信コスト削減のため企業での導入も進んでいる

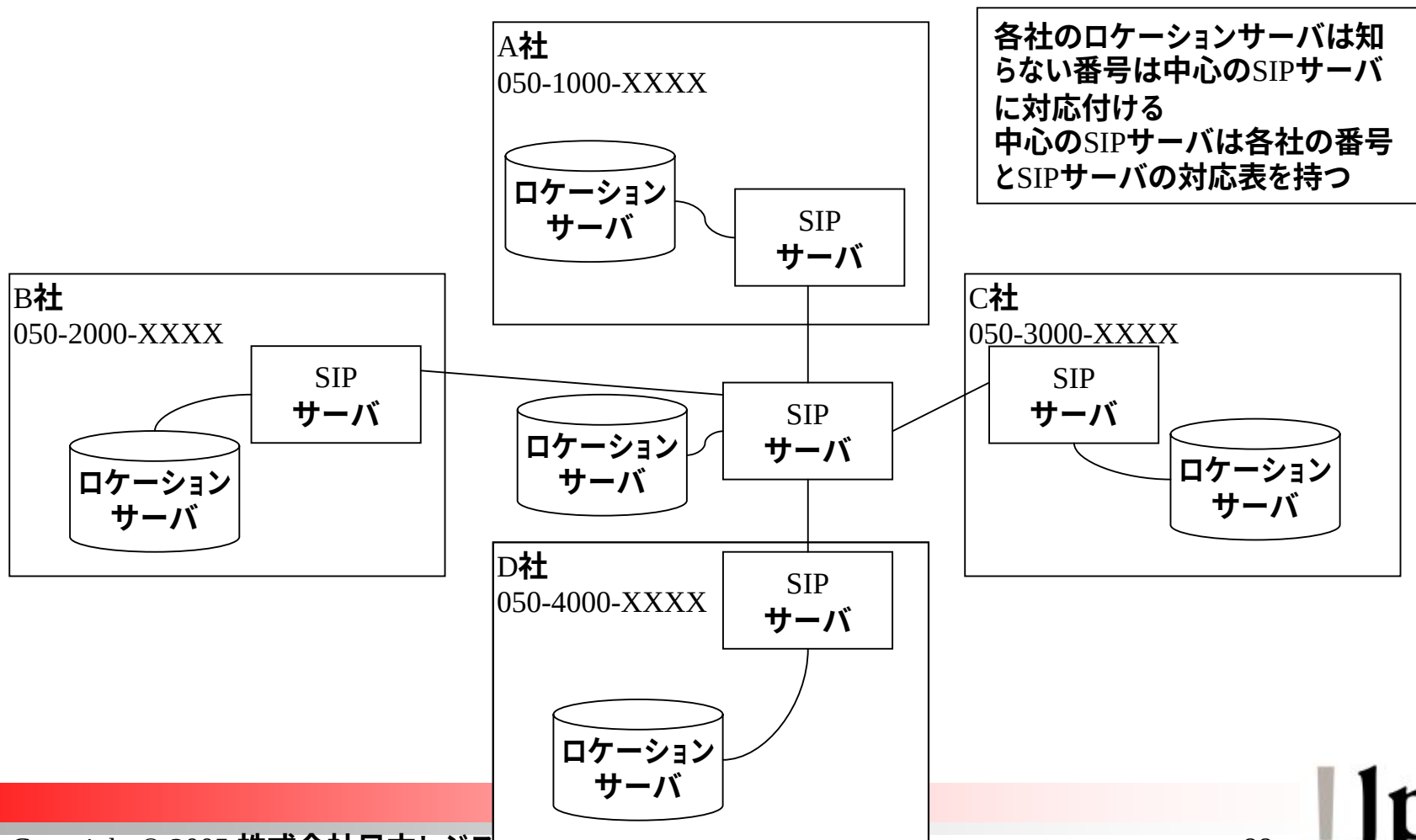
- **IP電話の課題**

- **最大の課題は異なるISP/キャリアグループ間のIP-IP相互接続**
 - IP電話利用者(050番号を持つ利用者)間でもグループが異なれば相手は「一般電話」(IP-PSTN-IP接続)
 - 相手との接続がIP-IPで可能かIP-PSTNでないと不可能かの判断・選択が容易ではない

異なるISP/キャリアグループ間の IP-IP相互接続 -- Full Mesh方式



異なるISP/キャリアグループ間の IP-IP相互接続 -- Hub SIP方式



残された課題

- **Full Mesh方式**

- Mesh間(各社間)でロケーションデータの同期が必要
- Peer相手の数が増えるとメンテナンスコストが指数的に増大

⇒スケーラビリティ

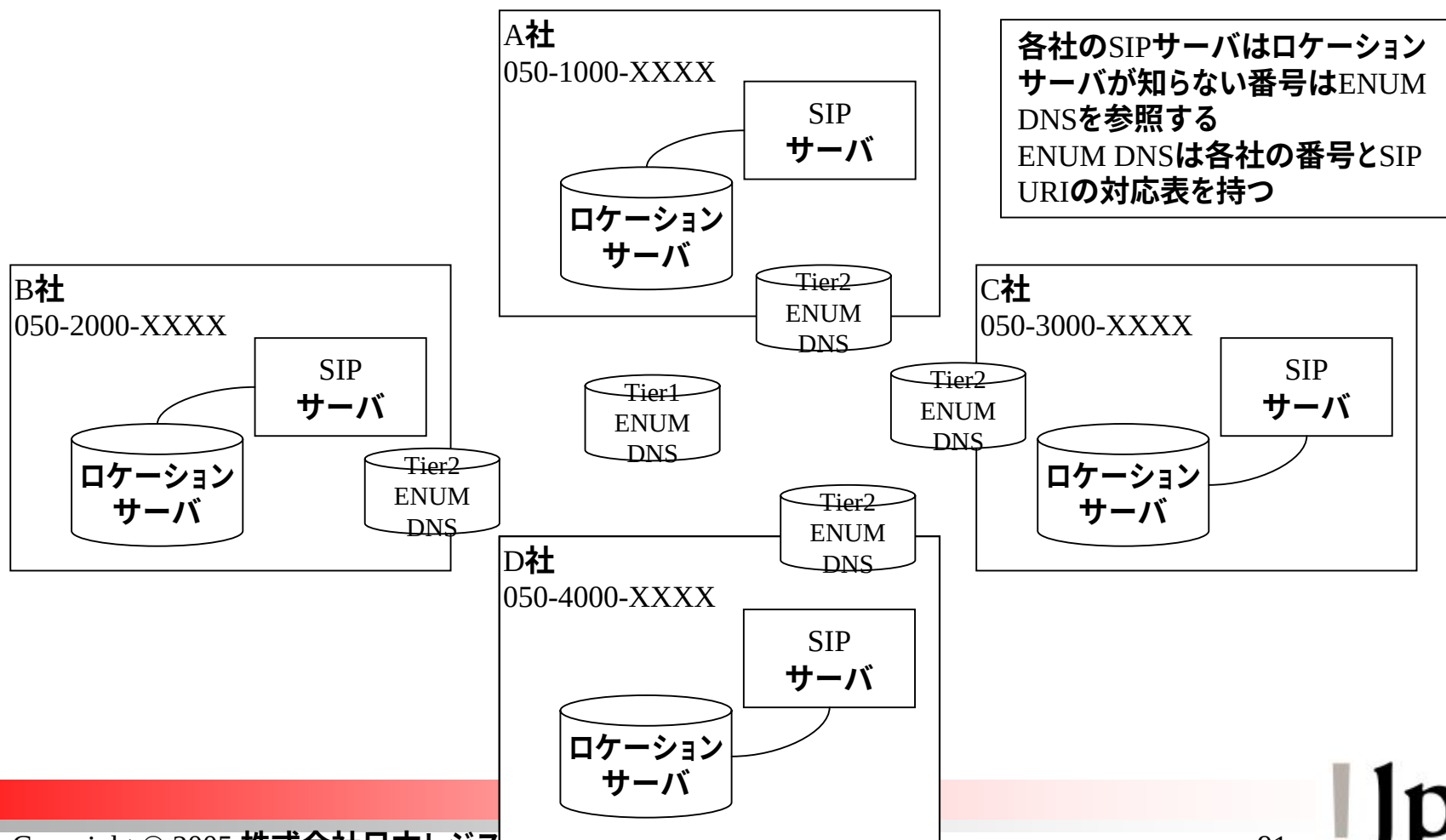
- **Hub SIP方式**

- 相手先が存在しない電話番号でもHub SIPサーバには接続に行く
- Hub SIPサーバがSingle Point of Failure

⇒リライアビリティ

ENUMによる解決

異なるISP/キャリア間のIP-IP相互接続 ENUM方式



解決される問題

- スケーラビリティ
 - 各社がTier2 ENUM DNSを持つためデータ同期は不要
 - 各社がDBを自律的に運用可能
 - Peerが増えてもメンテナンスコストは増えない
- リライアビリティ
 - 各社のSIPサーバは相互に直接接続可能
 - DNSは複数設置可能

更に...

- ナンバーポータビリティへの対応が容易
- 海外{へ、から}の接続(参照)も容易
 - グローバルスタンダード
- ENUM DNSを参照するアプリケーション

例えば

- 端末アダプタ(TA)にENUMを参照して利用者に通話が無料か有料かを通知する機能を追加
- 利用者へのアドレス一元化サービスの提供
 - 電話番号だけで電話もE-MailもHome Pageも可能

⇒利用者にとってメリットのあるサービス提供

ENUMでも解決されない問題

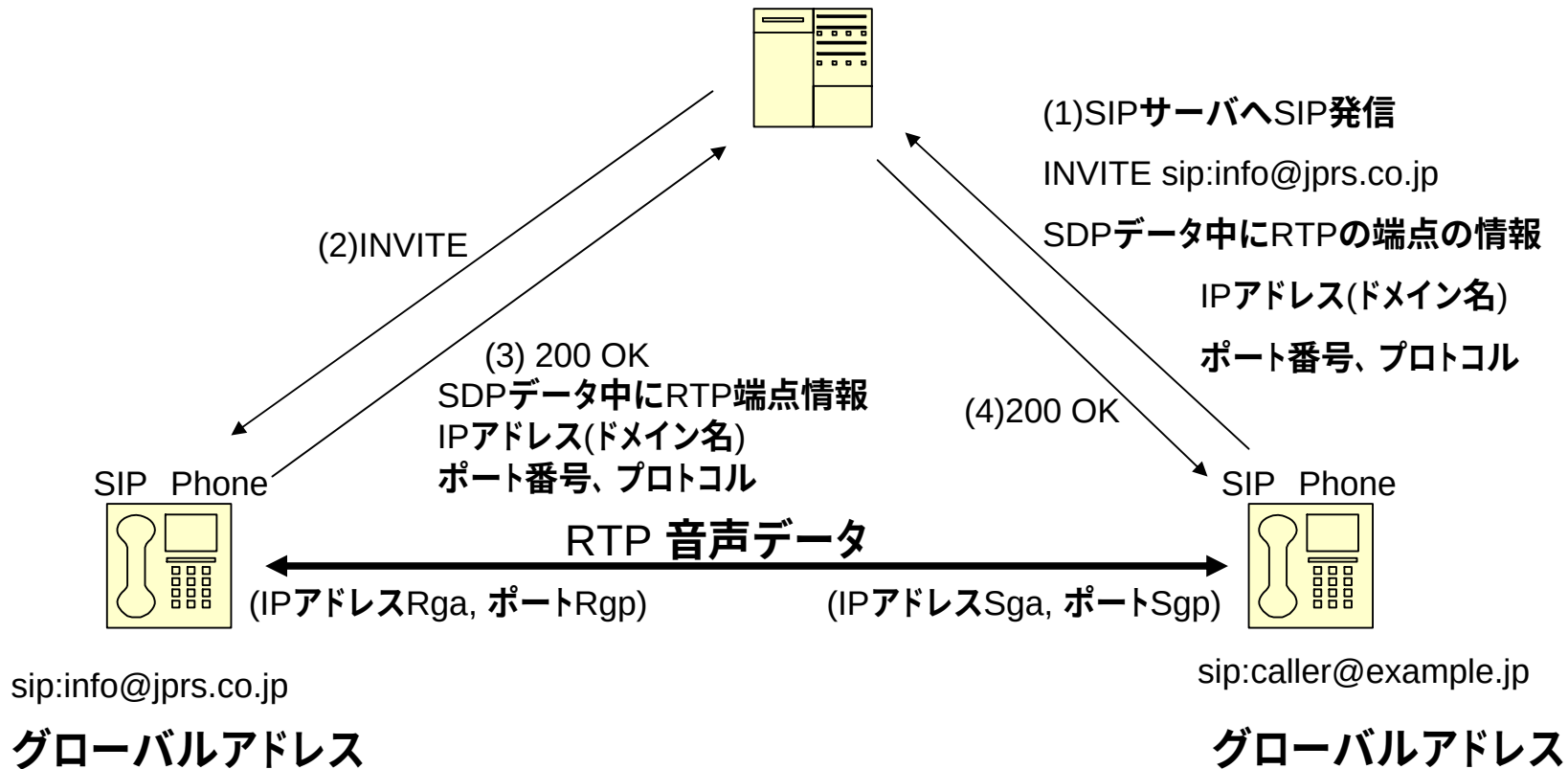
- 異なるISP/キャリアグループ間のIP-IP接続おける
 - 通話品質の保証
 - インターネットなのでBest Effortという考え方も
 - 発信者IDの認証(接続元の認証)
 - メールのSPAM対策と同様に
 - 通話課金
 - 相手先に関わらず一律?
- 利用者情報の保護
 - DNSは誰でも参照可能
 - DNS参照をVoIP事業者のみに限定する?
 - アプリケーションのレイヤで隠蔽する?

⇒ISP/キャリアグループ間の協調は依然として必要

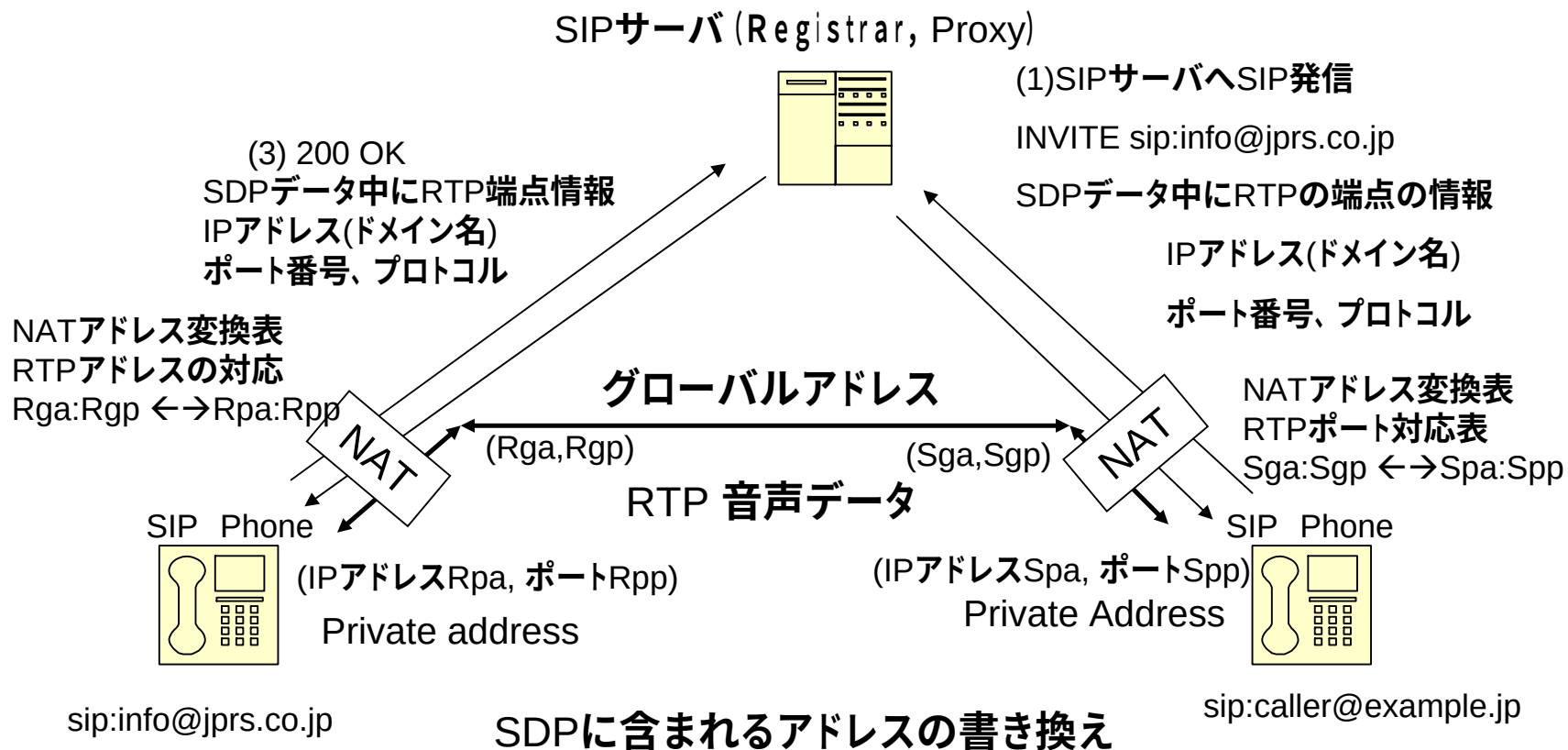
NAT traversal

SIPでの通話

SIPサーバ (Registrar, Proxy)



SIPでの通話(NATありの場合)



RTP NAT Traversal手法

- **必要条件**

- インターネットでは、SIPとRTPのIPアドレスは必ずグローバルアドレスを使用する
- SIP UAにプライベートアドレスが割り当てられている場合がある
- プライベートアドレスからグローバルアドレスへの通信をグローバルアドレス間の通信に変換するNATが存在する

- **STUN**

- NATの性質によりUDPを通す
- RFC3489

- **UPnP(Universal Plug and Play)**

- NATを制御して通す

- **Application Layer Gateway + NAT**

- SIPを理解するNAT

STUN(RFC3489)

- Simple Traversal of User Datagram Protocol
- NATでのUDPパケット通過の規則性
 - NATの内から外へ送ったパケットの戻りは、sourceとdestinationのIPアドレス・ポートの組をいれかえたものであるが、内から外へのパケット通過後しばらくは、同じアドレスパターンの外から内のパケットが通過できる
 - NATでのアドレス変換には規則性がある
- グローバルアドレスを二つ持つstunサーバが必要
 - NATでの変換後のグローバルアドレス、ポート番号を知るため
 - NATでのアドレス変換規則を推定するため
- STUN対応アプリケーションは、
 - stunサーバと何度か通信し、NATのアドレス変換後のグローバルアドレス・ポート番号を得る
 - SIPメッセージにはアドレス変換後のグローバルアドレスを記述
 - 外から入ってくるUDPパケットのために、内から外へ、同じアドレス変換を行うUDPパケットを定期的を送信する
 - たとえば、SIPポートへのUDPを受け取るために、改行のみのSIPメッセージを每秒送る

UPnP(Universal Plug and Play)

- NATの内側の機器からNATを制御する方式
- UPnP Forumが制定(業界団体)
 - <http://www.upnp.org/>
- UPnP機能
 - UPnP対応デバイス検出機能
 - LAN内の機器からのNATポートマッピング指定機能
 - LAN内の機器へのWAN側IPアドレスの通知
- UPnP機能付きNATルータとアプリケーションの対応が必要
 - Windows Messengerなどが対応
- UPnP対応アプリケーションは、
 - UPnP対応NATルータがあるか自動的に判定
 - RTPのアドレス変換をNATに指示
 - 変換後のアドレスをSIPメッセージ中のSDPに記述
 - 実際の通信はプライベートアドレスを用いて行う
- 家庭などの小規模なサイトに適している

Application Layer Gateway + NAT

- RTPストリームのアドレス変換と、SIP/SDPの管理を行うアプリケーションゲートウェイ
- メディアゲートウェイの一機能
- IPv4とIPv6の相互接続の場合にも使用される
- SIPサーバと組み合わせた大規模なものもあり

NAT対応機器の例

- **UPnP**

- 安価なブロードバンドルータの多くがUPnP対応
- UPnP対応アプリケーション
 - Windows Messenger

- **STUN**

- SIPソフトフォン
 - Xten X-lite、Kphoneなど
- STUNサーバ
 - Vovida STUN Server

<http://www.vovida.org/applications/downloads/stun/>

小規模なSIP/ENUM環境の構築

APEET ENUM/SIP Live Trial at APRICOT2005

- APRICOT2005にて開催したENUM/SIPのデモンストラーション
 - <http://www.apenum.org/APRICOT2005>
- **主催APEET(Asia Pacific ENUM Engineering Team)**
 - <http://www.apenum.org/>
 - 2004年にCNNIC, JPRS, KRNIC, SGNIC, TWNICの技術者で組織した非公式のプロジェクトチーム
 - 複数の国でENUM共同実験をすること、SIPを含むENUM関連技術の普及推進を目的
- APRICOT
 - Asia Pacific Regional Internet Conference for Operational Technologies
 - <http://www.apricot.net/>

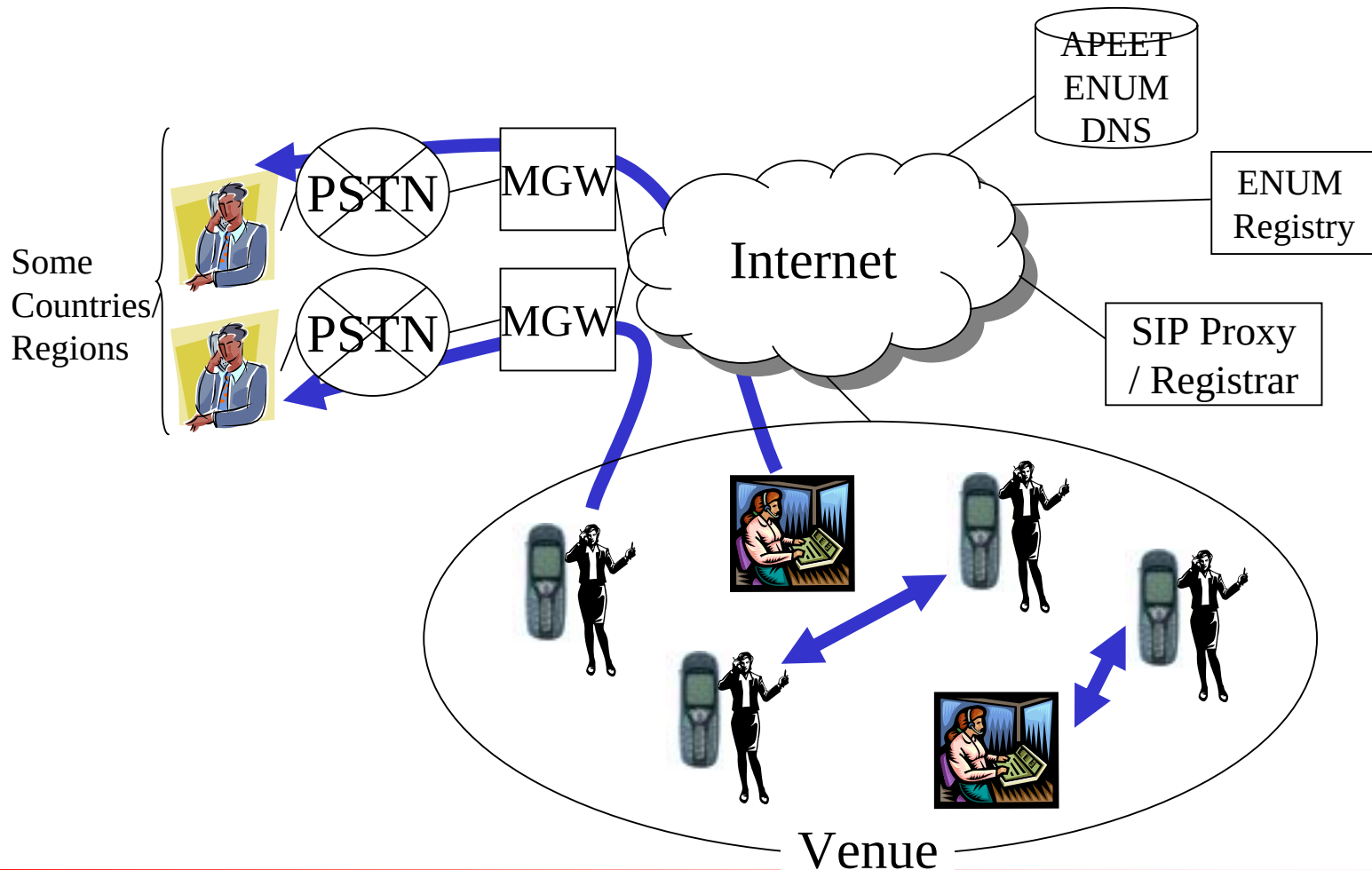
トライアルの目的

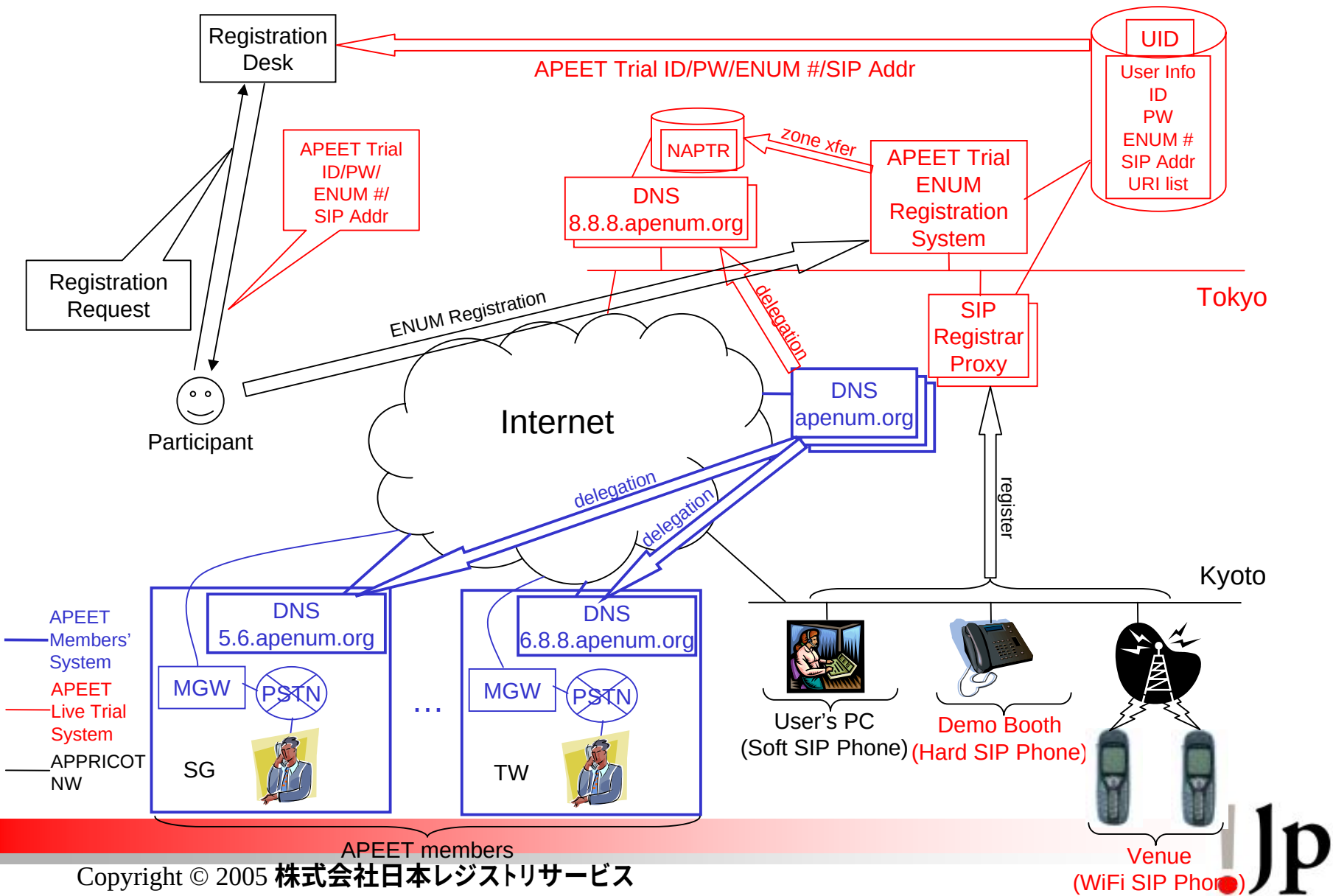
- **APRICOT2005参加者へENUM/SIP体験ができる場を提供すること**
 - ENUM
 - ENUM情報登録、ENUMでの番号解決
 - SIP
 - 参加者間の音声通話
- **電話サービスの提供ではない**
 - 無保証
 - 接続性、接続品質など
 - 独自の番号体系を使用
 - +888-2005-xxxx

トライアル参加者ができたこと

- SIP電話を持つ参加者間のSIP通信
 - 電話帳を検索し、知人の番号を得る
 - 4桁のSIPサーバ内の番号をダイヤル (ENUM検索なし)
 - 888-2005-xxxx をダイヤルするとENUM検索してSIP発信
- 海外への電話発信
 - 通信可能な国と地域は限定
 - メディアゲートウェイと回線の提供があった国・地域
 - 海外の番号を直接ダイヤル(ENUM検索し、MGWへ発信)
- ENUM情報登録
 - 参加者は自分の情報を編集可能
 - ENUM番号にURIを関連づけ
 - 電話帳(Opt-in)

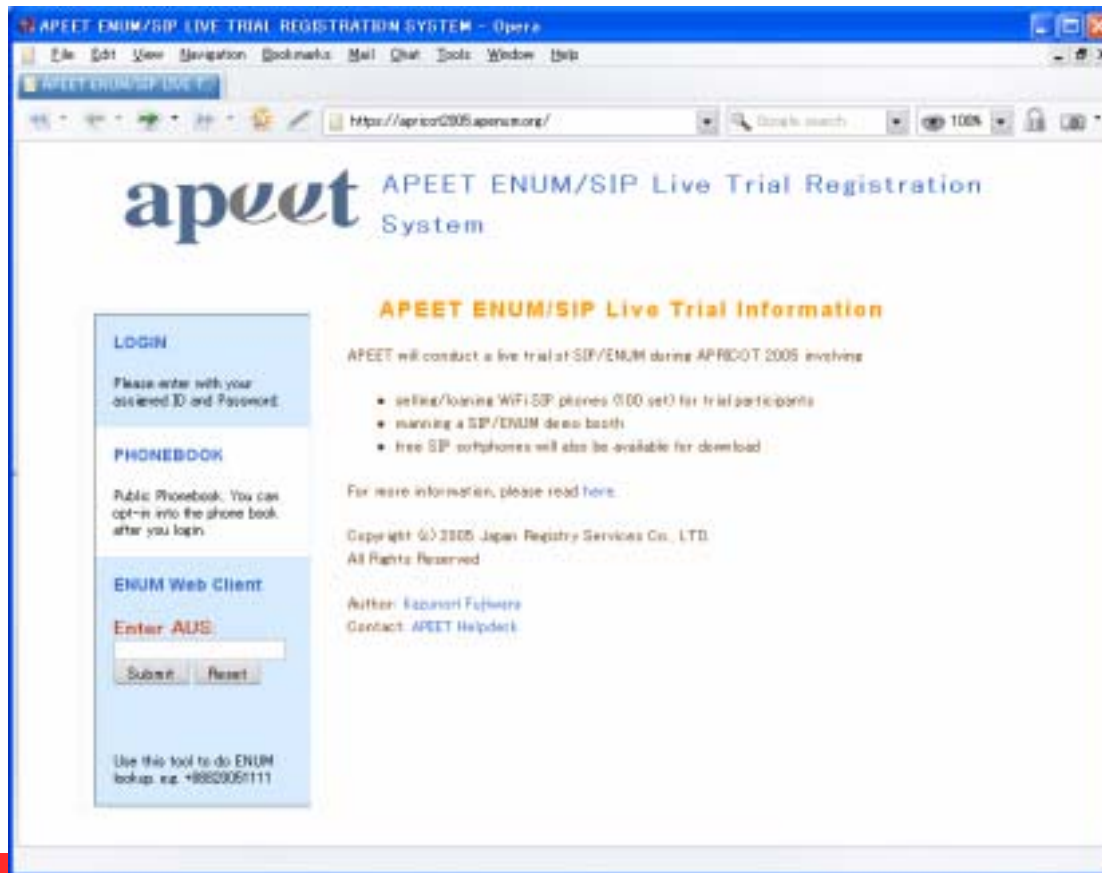
APEET Live Trial Image





ENUM Registration system

<http://apricot2005.apenum.org/>



- 100人以上が電話帳に名前を登録
- 約30人がENUM登録システムに複数の情報を登録
- ENUM登録システムのソースコードを公開

ENUM Client

http://www.apenum.org/ENUM_Client_Usage_Guide

The screenshot shows a Windows-style application window titled "ENUM Client" with a blue title bar. The window has a light beige background and contains several input fields and buttons. On the left, there are three labeled input fields: "Country" with a dropdown menu showing "Others", "Phone Number" with a dropdown menu showing "+ 888 2005", and "Domain Name" with a text box containing "5.0.0.2.8.8.8.apenum.org". On the right side of the window, there are five buttons stacked vertically: "Query", "Setup", "Phone Book", "Version", and "Close". The window also features standard Windows window controls (minimize, maximize, close) in the top right corner of the title bar.

SIP Phone

http://www.apenum.org/APRICOT2005/SIPPhone_Setup_Guide

SJPhone



X-Lite



WirelessIP-5000



トライアル結果

- Trial period
 - Feb 21 – Feb 25, 2005
- Call statistics
 - Feb 16 11:07:56 - Feb 26 00:00:00

	APRICOT	CN	SG	SE	TW	US	Total
200-OK	3227	1755	1017	2	787	1095	7883
461-CNE	43	23	7	0	88	31	192
481-Busy	62	7	35	0	0	6	110

Number of ENUM calls (8882005xxxx) from 200 - OK = 122

- Sold handsets
 - 100 sets within 5 hours

ENUM/SIPデモ システム設計(1)

- **条件**
 - **SIP端末数 1000程度**
 - WIFI Phone 115
 - 固定端末 10以下
 - 参加者数 1000以下
 - **開催期間 5日**
 - **コスト最小限**
 - **機能**
 - SIPサーバ
 - 電話帳
 - ENUM登録システム
 - アカウント作成

ENUM/SIPデモ システム設計(2)

- **決めた制限**
 - 登録システム・SIPパスワード変更なし
 - 開催期間 4日であること
 - 変更できなくても重大な問題は起きない
 - ID/パスワード/SIP URIは事前配布・機器に事前設定
 - 予備を含め、10000個のIDを事前作成、登録
- **実装案**
 - すべてフリーソフトウェアを使用
 - 登録システム・電話帳・アカウント作成ツール 書き起こし
 - SIPサーバにはSIP Express Routerを使用
 - PC 1台にすべての機能を入れ、東京に設置(会場は京都)

ENUM/SIPデモ システム

- **サーバマシン 1台**
 - インターネットに10Mbpsで接続
 - 二世代ほど前のサーバ機 P3-1266, memory 1G, 1U
 - OS: FreeBSD 5.3-RELEASE
 - SIPサーバ: SIP Express Router導入
 - ENUM登録システム向けにapache2 perl5など必要なものを導入
- **書き下ろしツール**
 - 主にperlにて数百行のものを作成
 - ENUM登録システムと電話帳
 - SIPサーバの運用だけであればほとんど不要
- **SIPアカウント、端末**
 - 日立電線 WIP-5000 100台 (+スタッフ向け15)
 - すぐ使えるところまで初期設定
 - ID、パスワード、SIP URI, SIPサーバ, 無線LAN
 - 会議参加者へID,パスワード,SIP URI配布
 - 名札に添付



SIP Express Router設定

- **FreeBSD portsほぼそのまま使用**
 - **/usr/ports/net/ser/**
 - Location databaseとして内部でmysql使用
 - enum引きはうまく動かないので独自patch作成
 - **/usr/local/etc/ser/ser.cfg**
 - コメントアウトされているmysql設定を生かす
 - コメントアウトされているdigest authenticationを生かす
 - ドメイン名などを正しく指定
 - **/usr/local/sbin/serctl**
 - 必要があれば適当に書き換える
 - **アカウント情報**
 - ランダム生成
 - 結果をserctlで登録

容易に入手可能なSIPサーバ

- ・ **SIP Express Router**
 - (ENUM対応)
 - <http://www.ipstel.org/ser/>
- ・ **Asterisk**
 - The Open Source Linux PBX
 - (ENUM対応)
 - <http://www.asterisk.org/>
- ・ **PartySIP**
 - <http://savannah.nongnu.org/projects/partysip/>
- ・ **hata sipd**
 - 国産
 - <http://hata.cc/products/default.htm>

容易に入手可能なSIP UA

- **Linphone**
 - Telephony on Linux
 - <http://www.linphone.org/>
- **KPhone**
 - KDE用SIP UA、STUN対応
 - <http://www.wirlab.net/kphone/>
- **iaxComm**
 - Asterisk PBX用のOpen Source softphone
 - Windows, MacOSX, Linuxで動作
 - <http://iaxclient.sourceforge.net/iaxcomm/>
- **Windows Messenger 5.1**
 - WindowsXP/2000で使用可能、UPnP対応
 - リアルタイム通信サービス
- **Xten X-lite**
 - 無料で使える製品 Windows/MacOSX用あり、STUN対応
 - <http://www.xten.com/>