

IETF 85 報告 DNS, 国際化関連

藤原 和典

<fujiwara@jprs.co.jp>

株式会社日本レジストリサービス (JPRS)

IETF 85 報告会, 2012/12/21

自己紹介

- 氏名:藤原和典
- 勤務先:株式会社日本レジストリサービス(JPRS)
技術研究部
- 業務内容:DNS関連の研究・開発
- 活動
 - DNSSECの事前検討 (2002~2010)
 - DNS関係のトラフィック解析など (2005~2012)
 - IETFでの標準化活動
 - DNS関連WG(dnsex, dnsop)における議論に参加
 - enum WG: RFC 5483、RFC 6116
 - eai WG: RFC 5504, RFC 5825
draft-ietf-eai-popimap-downgrade

報告対象WG

- DNS関連
 - dnsexp* DNSプロトコル拡張
 - dnsop* DNS運用
 - dane* DNSを利用した証明書の配送・正当性検証
 - mdnsexp Bonjourの拡張 (WG前)
 - enum* DNSによる電話番号とURIの対応付け
(完了済)
 - mif Multiple Interfaces (複数の上流接続)
- 国際化関連
 - idna-update* 国際化ドメイン名 (完了済)
 - precis 国際化された識別子の事前処理と比較
 - iri 国際化リソース識別子
 - eai メールアドレスの国際化

*はIETF 85では会議なし

用語解説

- DNS: Domain Name System
 - ドメイン名 (例: isoc.jp) とIPアドレスやメールサーバ情報などを対応付ける仕組み
- DNSSEC: DNS Security Extensions
 - 暗号技術(電子署名)を用いてDNS応答が改竄されていないかを受信側で確認できるようにする仕組み
- 国際化 (Internationalization)
 - 各国語文字列を同じ仕組みで取り扱えるようにすること
 - 従来ASCIIのみであった部分に、ISO 10646 / Unicodeを扱えるようにすることで各国語文字列を同じ仕組みで扱うこと
 - 多くの場合はUTF-8エンコーディングを使用 (RFC 3629)

DNS関連WG

dnsext WG (DNS extensions)

- DNSプロトコルを拡張するWG
- dnsind WGとdnssec WGの活動を引き継ぎ、1999年12月に開始
- 2008年まで主にDNSSECプロトコルを開発
- 2010年にRootと複数のTLDがDNSSECの運用を開始し、活動がほぼ完了
- 現在の残務
 - RFCのアップデート
 - DNSSECの小規模な拡張
 - クライアント確認のプロトコル
 - (暗号やハッシュ)アルゴリズムの追加
 - DNSのRR追加方法の明確化

dnsex WGの現在の動向

- 直接は集まらず、メーリングリストで議論
- RFC発行直前
 - draft-ietf-dnsex-dnssec-bis-updates: DNSSECの明確化と実装によって得られた知見をまとめたもの (実装には必須)
 - draft-ietf-dnsex-rfc6195bis: IANA登録についてのアップデート
- 議論中
 - DNSSECの普及のために必要な拡張 (必須ではない)
 - draft-ietf-dnsex-dnssec-algo-imp-status
 - 他WGで提案されたDNSに関する提案の処理
 - draft-rafiee-intarea-cga-tsig
- 現在は、DNSSECやDNSプロトコルに問題が見つかるまで待ちの状態 (最近NSEC3の問題発見)

dnsop WG (DNS Operations)

- DNS運用のguidelinesを作るWG
 - DNSSEC運用
 - ルートサーバ、TLDの運用も含む
- 1999年6月に開始
- 現在までの主な成果
 - RFC 2870: ルートDNSサーバ運用の要求条件
 - RFC 3258: DNS Anycast
 - RFC 3901: IPv6 DNSサーバのガイドライン
 - RFC 4641: DNSSEC Operational Practices
 - RFC 5358: Reflector attackへの対策
 - RFC 6168: DNSサーバの制御のための要求仕様
 - RFC 6303: Locally Served DNS Zones (private addressの逆引きなど)

dnsop WG (2)

- IETF 85では集まらず
 - DNSSECの主な運用ドキュメントの標準化が完了したため
- RFC発行直前
 - draft-ietf-dnsop-rfc4641bis: DNSSEC Operational Practicesのアップデート
 - draft-ietf-dnsop-dnssec-dps-framework: DNSSEC Policies and Practices statements (DPS)
- 残っている話題
 - DNSSEC使用時のDNSプロバイダ引越し、key rolloverで起きる問題について
 - draft-howard-isp-ip6rdns: ISPが提供するユーザに割り当てたIPv6アドレスの逆引き

dane WG

(DNS-based Authentication of Named Entities)

- DNS(SEC)を用いてドメイン名と公開鍵証明書を対応づけるプロトコルを作る
 - DNSSECによる保護を前提に、サーバ証明書をのせてしまおうという考え方
- 2010年12月に開始(Root, TLDのDNSSEC対応後)
- 現在までの成果
 - RFC 6394: Use Cases and Requirements
 - RFC 6698: The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA
- 標準化されたプロトコルをTLSAとしている

dane WG (2)

- IETF 85では集まらず
 - コアプロトコルが完了したため
 - プロトコル拡張方法が合意されたため
 - TLS(https)での使用はコアプロトコルに含まれているため
- 現在標準化中のプロトコル
 - MUA(Mail User Agent)のTLSA対応: POP, IMAP, Submission
 - SMTPのTLSA対応
 - S/MIMEのTLSA対応
- メールングリストの議論により標準化が進む見込み
- 使うためには
 - サーバ側: 自己署名証明書の内容をTLSA RRに書く
 - クライアント側: ブラウザ・アプリケーションを拡張する!!!

mdnsexth BoF

(Extensions to the Bonjour protocol suite)

- Apple Inc.のBonjourをベースに、複数ネットワークセグメントに対応したものを標準化する
- Bonjourは、米国およびその他の国で登録されたApple Inc.の商標です。
- Bonjour
 - Apple Inc.が開発したプロトコルで、MacOS Xで実装
 - ローカルネットワークにつないだMac OS機器の名前解決、サービスディスカバリーに用いられる
 - LinuxのAvahi
 - 標準化状況
 - Apple Incの技術者がindividual submissionにて標準化中
 - RFC Editor Queueで、発行直前
 - draft-cheshire-dnsexth-dns-sd: サービスディスカバリー
 - draft-cheshire-dnsexth-multicastdns: mDNSプロトコル
 - draft-cheshire-dnsexth-special-names: ドメイン名
 - RFC 4795: Multicast Name Resolution (Author所属Microsoft)存在

mdnsex BoF (2)

- IETF 85にてBoFを開催、WG設立の方向で活動することが合意
 - チャーター提案はまだ、WG設立は次回IETF86より後
- 状況
 - 一企業が独自開発したプロトコルをそのままRFCとすることには抵抗あり
 - Bonjourで大規模なネットワークを運用しているユーザが大学とか企業を中心に増えてきた
 - 現在のBonjourはサブネット内のみ
 - Bonjourの複数ネットワーク対応をIETFで標準化することにより抵抗感が減小すると期待したひとがいた？
 - IETF 85でのBoFの結果、賛同する参加者が多かった
 - 家庭ネットワークを標準化中のhomenet WGが注目
- 今後の活動が期待される

enum WG (Telephone number mapping)

- 電話番号をドメイン名に対応づけ、電話番号に対応する情報をDNSに載せるプロトコル
 - 03-5215-8451なら、1.5.4.8.5.1.2.5.3.1.8.e164.arpa
 - もともとはIP電話やインターネットFAXの経路制御にDNSを使うことを想定していた
- 1999年に開始
- 2011年3月に必要なRFC化が完了し、2011年5月にWG完了
 - RFC 6116: ENUMプロトコル
 - RFC 6117: ENUMを使用する新規サービス登録方法
 - RFC 6118: 既存のENUM serviceの再登録

mif WG (Multiple Interfaces)

- 複数の上流ネットワーク接続をもつ場合に、両方を有効に使うためのプロトコルを開発
 - 3GとWiFi、フレッツのIPv6問題、VPNとの共存問題など
- 2009年ごろから開始
- 複数の上流から別々のDNSサーバ情報が配布される際のDNSの使い方を拡張する
- RFC 6731: 複数のインターフェースを持つノードでのフルリゾルバ(DNSサーバ)選択方法の拡張
 - DNSサーバごとに担当するドメイン名空間を指定するDHCPv4, DHCPv6オプションを追加
 - 例: VPN網とグローバルのフルリゾルバ(DNSサーバ)の選択
 - 閉域網とグローバルのフルリゾルバ(DNSサーバ)の選択

国際化関連WG

(Internationalized domain name update)

- 国際化ドメイン名プロトコルを更新するWG
- 2008年に開始
- 目的
 - RFC 3490, RFC 3491 (IDNA2003)をアップデートして
 - 最新のUnicode(3.2から5.2)に対応させ、
 - 今後のUnicodeの拡張に対応できるものとする
- 2010年1月に以下のRFC(IDNA2008)が発行され、2010年5月にWG完了
 - RFC 5890: 用語定義と概要
 - RFC 5891: プロトコル本体
 - RFC 5892: ドメイン名として使用可能な文字
 - RFC 5893: Bidi (右から左に書く文字への対応)
 - RFC 5894: アップデートの背景、理由など
 - RFC 5895: Mapping(文字の読み替え、対応付け)

idnabis WG (2)

- IDNA 2003からIDNA 2008への変更点
 - Unicodeのバージョン依存性をできるだけプロトコル規定外に
 - バージョン依存部を使用可能文字を示すRFC 5892とした
 - 後にUnicode 6.0に対応したRFC 6452が標準化されている
 - Mappingが標準からはずされた
 - 句点と半角仮名、全角英数字に影響あり
 - 「。」を「.」として扱う
 - 半角片仮名を全角に
 - 全角アルファベット・数字などを半角に
 - IDNA 2003互換性を保つにはRFC 5895・UTS#46を実装すること
 - 日本語ドメイン名への影響は、Mappingのみ
 - 影響が出ないように対応
- 特記事項: WG chairがVint Cerf氏
 - 積極的に標準化を推進

precis WG

(Preparation and Comparison of Internationalized Strings)

- RFC 3454で定められているstringprepの改定
 - 国際化された識別子の事前処理と比較
 - ユーザIDやパスワード、チャットのニックネーム
- 2010年設立
- 現在のステータス: 以下の標準化作業中
 - draft-ietf-precis-problem-statement: (IESGへ提出済): 問題提起
 - draft-ietf-precis-framework: 全体構成
 - draft-ietf-precis-mappings: 各種マッピング方式の定義
 - draft-ietf-precis-nickname: チャットルームでのニックネーム
 - draft-melnikov-precis-saslprepbis: ユーザ名とパスワードでの認証
- 特記事項: JPRSの米谷がCo-chair

iri WG

(Internationalized Resource Identifier)


- 国際化リソース識別子の仕様(RFC 3987, 4395)をアップデート
 - IRI: URIにUnicodeを含められるようにしたもの
 - URI (Uniform Resource Identifier): URL+URN
- 2009年に開始
- 現在のステータス
 - IETF 85にて、ワーキンググループとしての活動が停滞しているため、WGをやめ、Individual draftとしてアップデートすることが合意されつつある

eai WG

(Email Address Internationalization)

- メールアドレスに各国語文字を使えるようにする拡張
- 2006年にWG開始
- 2010年10月までにExperimentalでの標準化完了
- 実装、評価後、Standard Trackでの標準化開始
- 現在のステータス: ほぼ標準化完了
 - RFC 6530: 概要
 - RFC 6531: SMTPの拡張
 - RFC 6532: ヘッダフォーマットの拡張
 - RFC 6533: 配送ステータスの拡張
 - POP, IMAP, POP/IMAP downgrade: RFC Editor queue

参考: RFCの種類について

- 
- high** ➤ Standard: インターネット標準を定義するもの
Proposed Standard → Standard
- Best Current Practice: プロトコルの使い方や運用方法を提案
- 実用度**
- Informational: 情報を記録したもの
実装の記録、問題点の記録、企業の独自プロトコル
- Experimental: 実験目的に開発・実装されるプロトコル
- low** ➤ Historic: 歴史的なプロトコルとして有効でなくなったプロトコル

eai: プロトコル拡張概要

- ほとんどすべてのメールヘッダにUTF-8を許可
 - メールアドレス部 <ローカルパート@ドメイン名>
 - Display-name, (コメント), SubjectヘッダにもUTF-8 (従来はMIME)
 - Message-IDヘッダ
 - ReceivedヘッダのFOR節に書かれるメールアドレス
 - 添付ファイルのファイル名もUTF-8で直接書く (従来はMIME)
- SMTPのメールアドレス部
 - MAIL FROM, RCPT TO, VRFY, ...
- SMTPサーバがeai拡張に対応しているかどうか
 - EHLOの応答のehlo-keywordにSMTPUTF8を含むこと
 - サーバが対応してなければeai WGでの拡張を送ってはいけない
- POP, IMAPにも、サーバ・クライアントが対応していることを示すオプションUTF8を追加

eai: メールの例

From: UTF-8を直接 <藤原@日本語.dnslab.jp>

To: (コメントもUTF-8で) <fujiwara@jprs.co.jp>

Cc: <テスト@日本語.dnslab.jp>

Subject: ここもUTF-8

Message-ID: <UTF-8_ID_XX@日本語.dnslab.jp>

本文もUTF-8

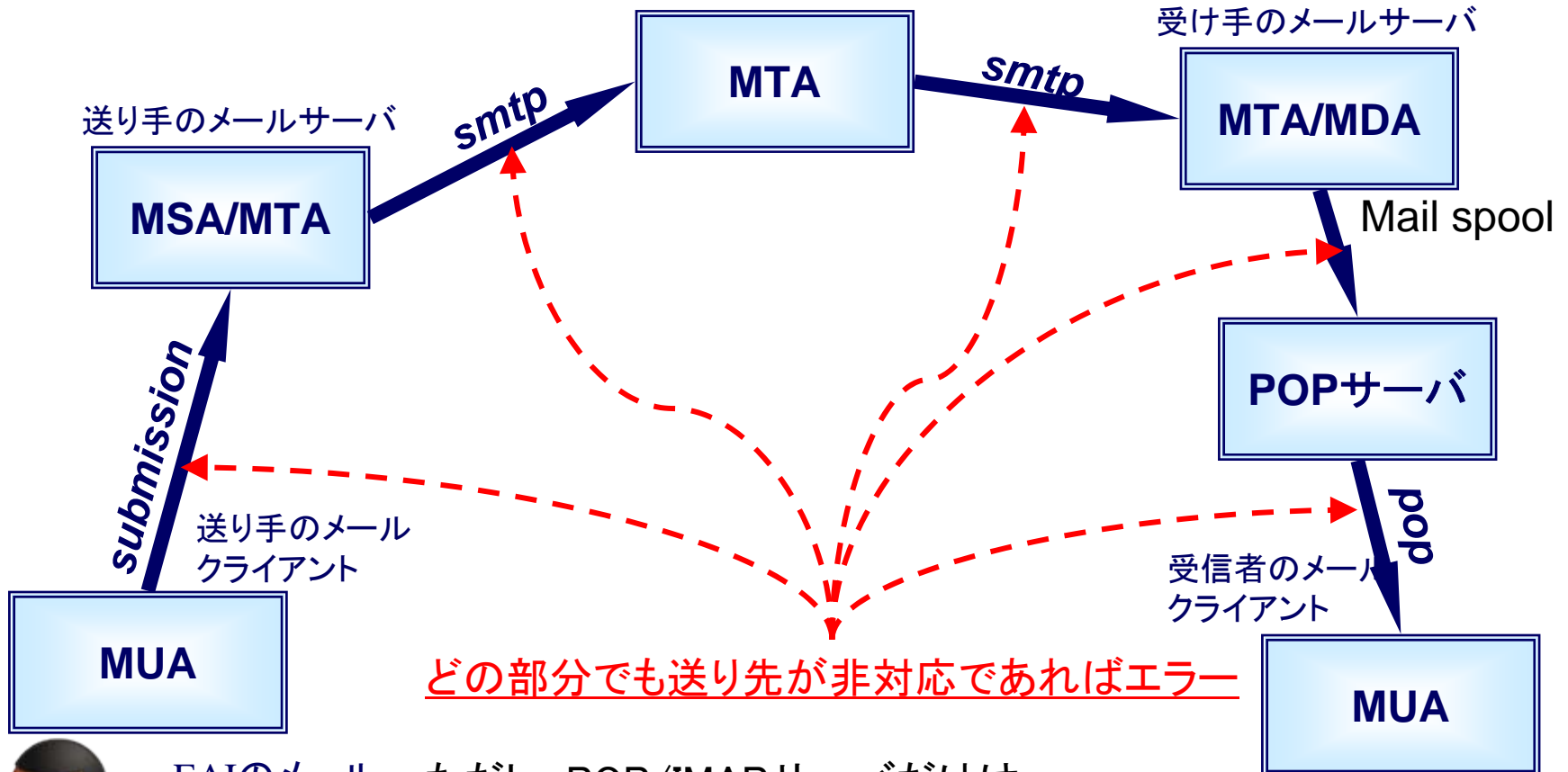
添付ファイルのファイル名もUTF-8

eai: SMTP例 (通信はUTF-8)

```
% telnet XN--WGV71A119E.dnslab.jp smtp
Server:220 XN--WGV71A119E.JP ESMTP ... DATE
Client: EHLO myname
Server:250-XN--WGV71A119E.dnslab.jp Hello, ...
Server:250-SMTPUTF8
Server:250-8BITMIME
Server:250 HELP
Client: Mail From: <藤原@日本語dnslab.jp>
Server:250 ... OK
Client: RCPT To: <テスト@日本語.dnslab.jp>
Server:250 ... OK
Client: DATA
Received: ...
From: <藤原@日本語.dnslab.jp>
...
```

以下、メッセージ

eai 通信モデル



どの部分でも送り先が非対応であればエラー

ただし、POP/IMAPサーバだけは、
受け側が非対応だと削除すらできないので、
従来のメールフォーマットに変換する拡張
あり(popimap-downgrade)



EAIのメール
作成、送信
送信者



復元機能
受信者

eai活動の今後

- 実用化について
 - 中国語圏、アラビア語圏では活発な動きがあるように見える
 - 日本では？
- その他
 - 現在も見受けられるが、ASCII以外の文字をヘッダに入れたメールが増加する可能性があるため注意

まとめ

- DNS関連のWGの活動は現在は低調
 - DNSSECが実用期に入ったため
 - 他のWGでDNSの使い方を拡張
- 新しい要求を持った人々はWGの新設へ
 - dane, mdnsex, mif
- 国際化
 - コンテンツは早くからMIMEなどを用いて国際化されていたが、ドメイン名、メールアドレス、識別子などのプロトコル要素は長らくASCIIのみだった。
 - 1999年ごろからIETFの活動で国際化が正式に行われるようになり、現在ではプロトコル要素としてもUnicodeで標準化された文字を使用可能となりつつある