ITU IPv6グループの設立経緯と現況について

現在ITU(International Telecommunication Union: 国際電気通信連合)には、「ITUを通じてIPv6アドレスを分配するスキーム」に関する議論を行う、ITU IPv6グループが設立されています。本稿ではこのグループに関して、これまでの動きを整理してお伝えします。

◆問題のあらまし

ITU IPv6グループの設立は、2009年9月のITU理事会に電気通信標準化局(TSB)局長から提出された「寄書29」[※1]で提案されましたが、ここに至る経緯はITU内部の会議体の決議文によってたどることができ、2005年に開かれた世界情報社会サミット(WSIS)のチュニスアジェンダまで遡ることができます。

なお、ITU内部での詳細な経緯については、JPNIC News & Viewsのバックナンバー[※2]をご参照ください。また、ITU内部の会議体や組織名称、全体の組織構造が分からないと理解しにくい面もあるかと思いますので、財団法人日本ITU協会提供のITU組織図[※3]もあわせてご参照ください。

◆CIRスキームとはどういうものか

前述のTSB局長による報告書[※1]において、CIR(Country-based Internet Registry)スキームという考え方が出てきていますが、要約すると以下のようになります。

1. 現在の五つのRIRに加え、ITUがRIR同様にIANAからIPv6アドレスの割り振りを受ける。
2. ITUレジストリから、国ごとに設置されるCIRにIPv6アドレスが再分配される。
3. CIRから分配されるアドレスに関しては、各国の事情を配慮して制定された細やかなポリシーがCIRによって制定される。また、このことがインターネットのルーティングを破壊する危険性は無い。
4. 現RIRによる独占状態には問題があり、競争環境が必要である。

このCIRスキームに対しては、IPv6グループ会合の直前に開催されたAPNIC29ミーティングにおいてAPNICコミュニティ全体から異議を唱えられ、「IPv6グループ会合に対する寄書」として声明文が出されています。[※4]

◆IPv6グループ会合

2010年3月15日～16日に、スイスのジュネーブでIPv6グループの第1回会合が開催され、ITUの会員国以外にも、セクターメンバーであるAPNIC、RIPE NCCなどのほか、ARINも技術専門家として参加しました。議事録案初版によると、発言した10ヶ国の会員のうちCIRスキームを支持したのは2ヶ国でした。支持理由として、インターネット用国際専用線の費用負担におけるアンバランス等、IPアドレス分配に直接関係の無いものを挙げる国もあり、正しい理解に基づいて支持を主張しているのか、論理的にも疑わしく感じられました。

一方、現行のRIRスキームへの支持を打ち出している国も数ヶ国あり、またRIR陣営も、全RIRに対して同一サイズのIPv6ブロックが既に分配済みであること等を理由に「現行スキームでニーズは満たしている」と考えており、CIR導入の必要性を明確化すべきとの指摘が相次ぎました。

第1回会合の結果、連絡部会や、ITU-T、ITU-Dの研究部会へのリエゾンが設置され、2010年9月1日～2日に第2回会合が開催されることになりましたが、JPNICが掴んでいる範囲では、第2回会合まで特に大きな動きはないようです。

◆考察

当初、このようなITUの動きはRIR関係者の中で大いなる懸念とともに議論され、JPNICも情報把握に努めてきましたが、今回のIPv6グループ会合の様子から、すぐに大きな動きにつながるものでなさそうだということが分かりました。

しかし、IPv6グループはITUの意志決定機構の枠外にあり、意志決定権を保持していません。セクターメンバーや技術専門家など、ITU会員国以外の幅広い人たちにより議論されるIPv6グループと違い、ITUとしての意志決定はITU理事会をはじめとする、ITU会員国のみが関われる会議等で行われるため、今後大きな動きが起こる可能性もないとは限りません。

2003年のWSISではICANN体制が大きな議論となりましたが、今後のITUの動きがIPアドレス管理体制やインターネットガバナンス全体に関する大きな動きを再び巻き起こす可能性もあり、JPNICでは今後とも状況を注視してまいります。

(JPNIC インターネット推進部 前村昌紀)

※1 ITU理事会に報告されたTSB局長による報告書「寄書29」
http://www.itu.int/dms_pub/itu-t/oth/3B/02/T3B020000020002PDFE.pdf

※2 JPNIC News & Views vol.746 ITU IPv6グループの設立経緯と現況について
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2010/vol746.html

※3 国際電気通信連合(ITU)組織図
http://www.ituaj.jp/03_pl/itu/sosikizu.pdf

※4 JPNIC News & Views vol.731 APNIC29ミーティング報告 [第1弾] 全体報告
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2010/vol731.html

2010.6.10▸6.11

Google IPv6 Implementors Conference 2010報告

2010年6月10日、11日の2日間、米国カリフォルニア州マウンテンビューにあるGoogle本社にて、「Google IPv6 Implementors Conference 2010」が開催されました。

本カンファレンスは、IPv6導入（製品への実装だけではなくネットワークやサービスへの導入も含む）経験を共有することを目的に、Google社が主催して2008年から毎年行われています。今年はVint Cerf氏からのビデオメッセージで幕開けとなりました。

◇　　◇　　◇

参加者は約170名、うち米国からが8割程度、ヨーロッパからが2割弱、日本からは10名強でした。また東日本電信電話株式会社（NTT東日本） 水越一郎氏、株式会社インターネットイニシアティブ（IIJ）松崎吉伸氏、NECビッグローブ株式会社 川村聖一氏、筆者の4名が発表を行いました。

過去2回のカンファレンスでは、IPv6実装技術全般および欧米アクセス系ISPにおけるIPv6への取り組み紹介がメインでしたが、今年は、

(1) コンテンツプロバイダーやCDN（Contents Delivery Network）におけるIPv6導入状況
(2) 携帯電話におけるIPv6実装状況
(3) CPE&ホームネットワークにおけるIPv6実装状況

が紹介されたことが大きな特徴です。本稿では上記3点に、

(4) アクセス系ISPにおけるIPv6導入状況

を加えた4点について、簡単ですがご紹介させていただきたいと思います。

(1) コンテンツプロバイダーやCDNにおけるIPv6導入状況

Google社、Yahoo!社、Facebook社、Limelight Networks社から発表があり、次の内容が紹介されました。

(a) 既知の問題（パフォーマンス、コスト、レイヤ4ポート番号の不足、abuse対応）に加えて、Geo-location（クライアント側IPアドレスなどを元に位置情報を特定する技術）の精度が低下することもCGN（Carrier Grade NAT）の大きな問題であること

(b) サーバ側のコードすべてをIPv6対応にすることが困難な場合には、まず負荷分散装置、リバースプロキシー、CDNなどのフロントエンドをIPv6対応させる手法も有効であること

(c) Google社およびYahoo!社ではIPv6への対応が不十分なユーザーへの対策としてDNS Whitelistingを使っていること

またNECビッグローブ社の川村氏からも、同社ポータルサイトおよびホスティングサービスにおけるIPv6導入時の経験について発表があり、ルータ、負荷分散装置、監視ソフトの間で仕様整合性が一部取れていないこと、クライアントソフトやクライアント側ネットワークに依然として問題が隠れていること、運用ツール（監視ソフトや各種解析ツール）でのIPv6対応が遅れていることが指摘されました。

■ 米国カリフォルニア州マウンテンビューにあるGoogle本社

この中で特筆すべきは、「DNS Whitelisting」の採用です。一般にクライアントとサーバがIPv6を使って通信するかどうかは、クライアントがDNSのAAAAレコードに対する問い合わせを行い、かつサーバ側のDNSがそのAAAAレコードにIPv6アドレスを返すかどうかで決まります。しかしこのDNS問い合わせは現時点では、IPv6ではなくIPv4パケットを使って行われているため、実際にはIPv6での到達性が無かったり、不十分なクライアントであったりしてもAAAAレコードに対する回答を得ることができます。そのようなクライアントが、一つのFQDNにIPv4/IPv6双方のアドレスを持っているサーバにアクセスすると、IPv4に通信がフォールバックするまで数分待たされたり、タイムアウトしてアクセスできなくなったりする問題が起きます。

Google社やYahoo!社での実測値によると、この問題は約0.05～0.1%のユーザーに発生しているようです。DNS Whitelistingはこの問題を防止するための手法で、IPv6対応を行っていると確認できたISPのDNSサーバからAAAAレコード問い合わせを受けた場合のみ、サーバのIPv6アドレスを返すようサーバ側DNSを設定します。本手法は確かに有効ではありますが、「IPv6に伴う諸問題を先送りにしているに過ぎない」「原因はホームネットワーク内にあることも多く、ISPがIPv6に対応してもそれらは問題として残る」「ISPがIPv6対応したときに、DNS Whitelistingを採用しているコンテンツプロバイダーすべてに連絡することは運用上困難」との議論も行われました。なおIPv6対応したISPからコンテンツプロバイダーへの連絡に関しては、DNSの逆引きのTXTレコードに特定文字列を登録するという手法が、Google社から提案されました。

またIIJ社の松崎氏からは、IPv6インターネットへの到達性が不十分なクライアントの一例として、IPv4の場合と同様にPath MTU Discoveryがうまく働いていないケースが紹介され、対策としては

(a) CPE（Customer Premises Equipment）からRA（Router Advertisement）を使ってMTU（Maximum Transmission Unit）サイズを各ホストに通知すること

(b) IPv4の場合と同様、CPEにMSS（Maximum Segment Size）hackを実装すること

のいずれかが有効であることが述べられました。

(2) 携帯電話におけるIPv6実装状況

Nokia Siemens Networks社、T-Mobile社、Verizon Wireless社、go6.si、Ericsson社から、携帯電話におけるIPv6への移行動機および現在の実装状況について発表がありました。

IPv6への移行動機については、次の内容が挙げられていました。

(a) 携帯電話事業者においては以前からNAT44の利用が一般的であるが、NAT内部のプライベートアドレスが不足するため、プライベートネットワークを複数に分割するようになっており（Verizon Wireless社の場合、40以上に分割）その運用負荷が大きいこと

(b) データ通信の利用率向上やプッシュ型アプリケーションの普及によりNAT44を使ってもIPv4グローバルアドレスが不足しそうなこと

(c) プッシュ型アプリケーションではNAT対策としてTCPセッションを長時間保持することが行われているが、これが端末の電池を浪費する原因になっていること

次に現在の実装状況については、3GPP（Third Generation Partnership Project）での標準化状況や各社製品の実装状況の紹介に加えて、go6.siおよびEricsson社から米国の携帯事業者網（=IPv6未対応）にローミングしている携帯端末に、ホーム網側からIPv6アドレスを割り当て、通信を行うという大変興味深いデモも行われました。

(3) CPE&ホームネットワークにおけるIPv6実装状況

Cisco社、Arris社、Iskatel社、D-Link社から標準化動向、各社製品の実装状況が紹介されました。その中でも、ホームネットワークに対して複数アップストリームがある構成（マルチホーム）や複数プリフィクスが割り当てられる構成（マルチプリフィクス）における、CPEに求められる機能について多くの時間が割かれ、「各アップストリームから到達できるサービスや機能に基づいて、アップストリームやプリフィクスを使い分ける機能が必要」「セキュリティポリシーとの連動も必要」「追加機能を実装していないCPEとの互換性確保も重要」との指摘がありました。日本でもフレッツ光ネクスト上でのIPv6インターネット接続は、まさに上記の構成にあたるため、非常に興味深い議論でした。

また携帯電話端末がホームネットワークのゲートウェイとしても機能している構成が、他の発表を含めて何度か紹介され、ホームネットワークの典型的な構成例の一つとなっていくであろうことを予感させました。

(4) アクセス系ISPにおけるIPv6導入状況

Comcast社、AT&T社、NTT東日本、ソフトバンクBB株式会社からIPv6の導入状況および今後のロードマップについて紹介がありました。

Comcast社からは、今年1月から6rd（IPv6 rapid deployment）、デュアルスタック、DS-Liteを使ったトライアルを開始し、5,400人のボランティアが参加していること、デュアルスタックは地域限定だが、他のソリューションの場合は地域に対する制限は無いとのことでした。

またAT&T社からは、6rdを使ってIPv6サービスを提供予定であること、ネットワークアドレスを固定で割り当てる企業向けサービスと組み合わせるためには、現在の6rdの仕様では足りないこと、6rdを実装できないCPEを交換する費用やVoIPやIPTVなどのサービスをIPv6対応させていくためのコスト捻出が難しいこと、が紹介されました。

NTT東日本の水越氏からは、フレッツ光ネクストの概要、その上でのIPv6インターネット接続サービス形態として案2（トンネル方式）と案4（ネイティブ方式）が進められていること、フレッツ光ネクスト上ではIPTVサービスにIPv6を使っており、ピーク時にはトラフィックが50Gbpsに達していることが紹介されました。

筆者からは、ソフトバンクBB社ではADSLやフレッツユーザーに対しては6rdを用いてIPv6サービスを順次提供し始めていること、フレッツ光ネクストユーザーに対しては、案4を用いて2011年春から提供予定であることを説明させていただきました。

最後は主催者Google社からの「できればIPv6 Implementors Conferenceは来年で終わりにしたい（再来年にはIPv6が当たり前になっていて欲しい）」との冗談本気半々の挨拶で、2日間にわたった本カンファレンスは終了しました。

■ Google IPv6 Implementors Conferenceの様子

なお、各プレゼンテーション資料および大半のプレゼンテーションビデオが、下記URLに掲載されていますので、ご参照ください。

□Google IPv6 Implementors Conference 2010 Agenda
http://sites.google.com/site/ipv6implementors/2010/agenda

（ソフトバンクBB株式会社 山西正人）

2010.7.21

DNSSEC 2010 サマーフォーラムレポート

［関連記事］P.16「DNSSECジャパンへの参加とその活動について」

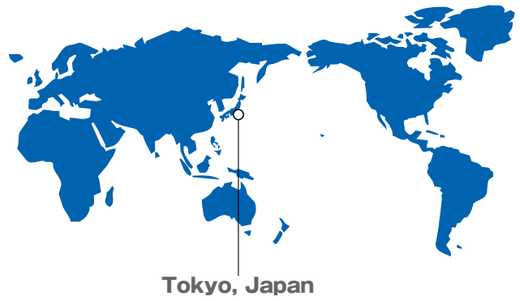
◆はじめに

2010年7月21日（水）に、DNSSECジャパンの主催によるDNSSEC 2010 サマーフォーラムが、東京・品川イーストワンタワーにて開催されました。このフォーラムは、DNSSECジャパンの活動紹介とDNSSECに関する最新情報の共有を目的としたもので、当日は130名を超える参加者が集まり大変盛況なイベントとなりました。当日のプログラムは、前半がDNSSECジャパンの紹介、後半がDNSSECに関する動向報告という大きく二つに分かれた構成でした。

筆者は普段、JPNICにおいてドメイン名全般に関する業務を担当し、その一環で各TLDにおけるポリシー動向や登録数、国際化ドメイン名などへの対応状況なども調査しています。このような背景からプログラムの後半部分で、各ccTLDとgTLDにおけるDNSSEC導入状況について、ご報告させていただくことになりました。本稿では発表者としての立場と、DNSSECに興味を持つ一参加者としての両方の立場で、プログラムの後半部分を中心に今回のサマーフォーラムをレポートさせていただきます。

◆DNSSECジャパンの紹介と活動報告について

最初に、株式会社日本レジストリサービス（JPRS）の坂口智哉氏よりDNSSECそのものについての解説が行われた後、DNSSECジャパン会長でもある日本DNSオペレーターズグループ代表幹事、日本インターネットエクスチェンジ株式会社代表取締役社長の石田慶樹氏による、DNSSECジャパンの紹介がありました。組織体制や活動内容、今後の予定などが報告された後、公募によって決定したDNSSECジャパンのロゴが紹介され、ロゴ制作者の表彰が行われました。このロゴはDNSSECジャパンのWebサイト（http://dnssec.jp/）で見ることができます。



続いて、プロトコル理解サブワーキンググループ（SWG）、運用技術SWG、技術検証ワーキンググループ（WG）の活動報告が、それぞれ株式会社インターネット総合研究所の伊藤高一氏、NRIセキュアテクノロジーズ株式会社の中島智広氏、インターネットマルチフィード株式会社の豊野剛氏より行われました。詳細についてはここでは割愛しますが、DNSSECジャパンのWebサイトにて当日の資料が公開されていますので※1、興味のある方はぜひご参照ください。

◆各ccTLDおよびgTLDにおけるDNSSEC導入状況について

筆者より、「各国ccTLD、gTLDの状況について」と題して、各TLDにおけるDNSSECの導入状況についてご報告しました。2010年7月時点で、gTLDでは約半数のTLDが対応済みもしくは対応予定となっています。一方ccTLDでは、割合だけで見れば全251TLDのうち約15%程度だけが対応済みまたは対応予定となっていますが、登録数上位20TLDに限ればその数字は75%となり、かなり対応が進んでいる状況です。gTLD、ccTLD両者とも、登録数が数万件から数十万件程度といった小・中規模のTLDだけでなく、登録数が100万件を超えるような大規模なTLDでもDNSSECが導入されており、2010年から2011年にかけて、gTLDでは.comや.net、ccTLDでは.de（ドイツ）や.uk（イギリス）、.cn（中国）などといった、登録数上位を占めるTLDがDNSSECの導入を予定しています。

ただし、ドメイン名の登録者がDNSSECを利用するためには、TLDを管理するレジストリだけでなく、登録を受け付けるレジストラなどもDNSSECに対応する必要があり、レジストリが対応したからといって、すぐにすべての登録者がDNSSECを使えるようになるわけではありません。とはいえ、多数のTLDがDNSSECへの対応を表明しており、2010年7月のルートゾーンへの署名追加を契機に、各TLDにおける対応は今後より一層進むものと思われます。

なお、各TLDにおける具体的な対応状況や導入スケジュール等については、公開されている当日の発表資料※1をご覧ください。

◆.jpへのDNSSEC導入スケジュールについて

JPRSの米谷嘉朗氏からは、.jpへのDNSSEC導入に関するスケジュールの報告が行われました。これまでは2010年中の導入予定とだけアナウンスされていましたが、この日の発表ではこれまでよりも詳細なスケジュール※2が明らかになりました。2010年7月時点の構想では、2010年10月にJPゾーンの署名を開始、2011年1月からDS登録受け付けおよびJP DNSへの反映を開始する予定とのことです。なお、10月のJPゾーン署名にあたっては、署名の2ヶ月程度前に署名パラメーターの公開を行い、署名から1ヶ月程度後にルートゾーンへDS登録をする予定とのことです。

■ 当日はUstreamでのストリーミング配信も行われました

また、米谷氏からは、.jpにおけるDNSSEC導入に関する技術検証について、6段階に分けたうち、2010年7月時点では4段階目まで進んでいるという報告と、導入時の各マイルストーンごとに、それぞれどのような影響があり、キャッシュDNSサーバなどの挙動がどう変化するのか、図を交えて詳細な説明が行われました。

◆ ルートゾーンのDNSSEC署名の状況について

慶應義塾大学/WIDEプロジェクトの加藤朗氏とJPRSの民田雅人氏からは、ルートゾーンのDNSSEC署名に関する報告が行われました。加藤氏からは、ルートゾーンへのDNSSEC導入についてこれまでの経過が説明された後、ルートゾーンへの署名完了に関するアナウンスが出された2010年7月16日早朝（日本時間）以降の、ルートサーバのトラフィックが報告されました。加藤氏によると、今のところ、ルートゾーンへのDNSSEC導入に伴う顕著なトラフィック増加は認められないとのことでした。

続いて、民田氏からは「rootゾーンのKSK管理」と題して、ICANNによるルートゾーンのKSK（Key Signing Key）※3管理に関する詳細について、ICANN KSK Ceremony 2※4への参加記を中心に説明が行われました。ドメイン名空間のツリー構造において最上位に位置する、ルー

トゾーンのZSKに署名をする際に使われるKSKは、DNSSECの仕組みにおいて大変重要な役割を占めるもので、民田氏は世界中で21名いるTCR（Trusted Community Representatives;「信頼されたコミュニティの代表者の意」）の一人として、ルートゾーンのKSK管理に関わっています※5。TCRから直接話を聞く機会はやはり珍しいのか、質疑応答の時間には各参加者から興味津々の様子で多くの質問が行われていました。

KSKやZSKといったDNSSECの仕組みに関しては、JPNICニュースレター43号の「インターネット10分講座」で詳しく解説していますので、こちらを併せてご覧ください。

□JPNIC Newsletter No.43「インターネット10分講座: DNSSEC」
http://www.nic.ad.jp/ja/newsletter/No43/0800.html

◆DNSSECにおける鍵管理ポリシー

最後に、Neustar社のEdward Lewis氏より、「DNSSEC Key Management Design」と題して、DNSSECにおける鍵管理ポリシーに関する発表が行われました。当日は英語でのプレゼンテーションということで、JPNICの木村泰司が逐次通訳を行いました。Lewis氏は時折日本語の単語を使ったジョークを交えるなど軽妙な語り口で、会場を大きく盛り上げていました。

Neustar社は、登録数200万件を超えるgTLDである.bizと同時に、約170万件の登録がある米国のccTLD、.usのレジストリ業務も行っています。このような大規模TLDにおいて、DNSSECを実際に運用しているNeustar社からの報告はとても説得力のあるもので、多くの参加者の参考になったのではないかと思います。

（JPNIC インターネット推進部 是枝祐）

※1 DNSSECジャパン「DNSSEC 2010 サマーフォーラム資料」
http://dnssec.jp/?page_id=173

※2 JPRSが2011年1月に、JPドメイン名サービスにDNSSECを導入
http://jprs.co.jp/press/2010/100721.html

※3 KSK（Key Signing Key）
日本語で「鍵署名鍵」と呼ばれるもので、各ゾーンに署名する際に用いられるZSK（Zone Signing Key; ゾーン署名鍵）に署名される際に使われる鍵です。

※4 ICANN KSK Ceremony
KSKの秘密鍵と公開鍵を生成するプロセスで2010年6月16日と7月12日の2回に分けてキーセレモニーが行われました。

※5 JPRSの民田雅人がICANNのルートゾーンDNSSEC運用のTCRに選出
http://jprs.co.jp/press/2010/100617.html

2010.7.25▶7.30

第78回IETF報告

■ IPv6関連WG報告

2010年7月25日（日）から30日（金）まで、オランダのマーストリヒトにて第78回IETFミーティングが開催されました。同時期、日本は酷暑でしたが、現地は最高気温が摂氏25度程度で、カラっとした過ごしやすい陽気の中でのミーティングでした。今回の参加者は、267人の新規参加者を含み、合計1,153名でした。また、参加者の内訳は、米国からが最も多く、続いて中国、日本、ドイツ、といった様子だったようです（プレナリにおけるIETFチェア発表より）。

本稿では、会期中における、IPv6に特化した内容を議論するワーキンググループ（WG）での議論内容を中心に紹介します。

◆6man WG（IPv6 Maintenance WG）

6man WGは、IPv6のプロトコル自体のメンテナンスを実施するWGです。今回は、7月27日（火）の午後最後のコマと、28日（水）午前2コマ目の、合計2コマ開催されています。

最初にいつもの通り、6man WGで取り組み中である以下の文書について、ステータス確認が行われました。

・IPv6拡張ヘッダの統一フォーマット（WGドラフトの初版発行）
・IPv6サブネットモデル（RFC5942として発行）
・IANA経路制御ヘッダ（RFC5871として発行）
・IPv6推奨アドレス表記（RFCエディタ発行待ち）
※ミーティング後、メーリングリスト（ML）上で議論あり
・DNS RA（Router Advertisement）オプション（IESG（Internet Engineering Steering Group）評価、AD（Area Director）フォローアップ中）

今回のミーティングでは、以下のアイテム/テーマについて議論されました。

2010年7月27日（火）：
・ノード要求仕様の更新
draft-ietf-6man-node-req-bis
・IPv6アドレス選択
draft-ietf-6man-addr-select-considerations
draft-arifumi-6man-rfc3484-revise

・P2Pリンク上におけるIPv6プリフィクス長/127の利用
draft-kohno-ipv6-prefixlen-p2p

2010年7月28日（水）：
・UDPゼロチェックサムの検討
draft-ietf-6man-udpzero
・IPv6フローラベル仕様の更新
draft-carpenter-6man-flow-update
・IPv6フローラベルを用いたECMP（Equal-Cost Multi-Path）
draft-carpenter-flow-ecmp
・RPL（IPv6 Routing Protocol for Low power and Lossy Networks）でのIPv6経路制御ヘッダの利用
draft-hui-6man-rpl-routing-header
・データプレーンデータグラムでのRPL情報運搬のためのRPLオプション
draft-hui-6man-rpl-option

これらのアジェンダの中から、以下にいくつかのトピックについてご紹介します。

・ノード要求仕様の更新
IPv6ノードが実装すべき仕様（RFC）を定義する文書の更新に関する議論です。最新ドラフトでの変更点についての説明、および以下の点に関する議論が実施されました。

- 設定方法:RAとDHCP
設定方法の柔軟性を上げるために両方で同じ項目を設定できた方がよい、という意見と、両方が使用された場合に、ホストが得た情報に矛盾があった場合の対処の困難性が指摘されました。

- DNS設定
RAによるDNS設定の配布方法が標準（Standards Track）になることを受け、RAによる配布を必須とすべきかについて議論されました。RAも必須とすべきという意見が多く、MLで確認することとなっています。

- アドレス設定
現在のRFCでは、DHCPによるアドレス配布の実装は「MAY」となっています。企業等はRAよりDHCPを使うだろうという意見もあり、これを「SHOULD」とする方向になりました。

- IPsecとIKEv2に関する記述
現在のRFCでは、IPsecの実装は「MUST」となっています。IKEv2と合わせ、これを「SHOULD」とする方向になりました（会場では、"strong SHOULD"と言われていました）。

・IPv6アドレス選択
IPv6ノードが複数のアドレスを持った場合のアドレス選択手法について、6man WGではデザインチーム（DT）を構成して議論を続けてきました。今回、DTから、議論となっていたアドレス選択ポリシーの配布方法としてはDHCPが適していること、複数の矛盾するアドレス選択ポリシーを受信した場合の扱いについては、別途検討を進めるべきであること等の、議論結果の報告がありました。この報告を受け、アドレス選択手法を定義しているRFC3484の改版提案およびDHCPによるアドレス選択機構の提案について、前者はWGドラフトとして進めていくこと、後者については、さらにMLで議論を実施することとなっています。

・UDPゼロチェックサムの検討
現状「MUST」となっているIPv6のUDPにおけるチェックサム計算について、UDPをトンネルのトランスポートとして利用する場合には、これを不要とする提案です。前回のIETFにて、WGとしてこの問題に取り組むこととなり、今回、WGアイテムとして議論されました。UDPチェックサムが'0'となった場合の影響について、中間ノード（ルータ等）や、エンドノードの観点でどうなるかに関する調査の必要性や、そもそもチェックサムが'0'でよい場合かどうかの区別ができるのか、という問題が提起されており、MLで継続議論となっています。

・IPv6フローラベル仕様の更新
IPv6の特徴の一つとしてあげられることの多い、フローラベルの仕様更改に関し、前回のIETFに引き続き議論が行われています。今回は、フローラベルを経路の途中で変更可能とするかどうかが、

主な議論になりました。現在の仕様では、フローラベルは経路途中で変更してはいけないことになっていますが、これを変更可能とすることで、AS内等でローカルに利用できるようになります。しかしながら、フローラベル値は変更されたかどうか検知ができないため、情報として信用できるのか、という問題があります（IPsecでもフローラベルは保護されていません）。会場では、変更可能とすべき、という意見の方がやや多かったものの、結論は出ませんでした。

□6man WG
https://datatracker.ietf.org/wg/6man/

□第78回 IETF 6man WGのアジェンダ
http://www.ietf.org/proceedings/78/agenda/6man.html

◆savi WG（Source Address Validation Improvements WG）

savi WGは、LAN環境において、始点アドレスの詐称を防ぐ機構について検討するWGです。今回は、7月26日（月）朝一番のコマにて、開催されました。参加者は20～30名と、それほど多くない人数での議論となっています。今回は、主にsaviの解としてのステートレスアドレス自動設定（SLACC）における詐称防止（IPv6）、DHCP環境における詐称防止（IPv4/IPv6）について、議論が実施されました。ポイントとしては、

・SLACCにおける、savi機構のライフタイムの扱い
・savi装置のポートにおいて扱わなければならないIPv6アドレス数
・SLACCとDHCPv6が同時に使われた場合の扱いの問題

等が、特に時間を割いて議論されていました。

saviの機構はスイッチ、またはルータに実装されることになりますが、既に多くのベンダー（主に中国ベンダー）にて実装されており、運用実験等が進んでいる、という報告もありました。

□savi WG
https://datatracker.ietf.org/wg/savi/

□第78回 IETF savi WGのアジェンダ
http://www.ietf.org/proceedings/78/agenda/savi.txt

◆v6ops WG（IPv6 Operations WG）

v6opsは、IPv6に関するオペレーション技術や、移行技術に関する議論を実施するWGです。今回は、7月26日（月）と30日（金）に2時間ずつ、合計2コマにて議論が実施されていました。今回も、数々の新提案があり、内容も多岐にわたっていました。いくつかのトピックについて、簡単に紹介します。

・NATを用いないIPv6マルチホーミング方式
（draft-troan-multihoming-without-nat66）

従来IPv4で行われてきた、NATを用いた複数サイト帰属（マルチホーミング）を、IPv6においてNATを用いずに実現する方法について提案したものです。そもそも、家庭ユーザーなど小規模サイトでの複数サイト帰属は、複数のISPに接続するケースや、ISP接続とVPN接続の併用といった場合にNATを用いて行われています。IPv6のend-to-end原理を実現するためには、NATを使わずにこういった複数サイト帰属を実現する必要があります。その方法として、それぞれの上流ネットワークから付与されたIPv6アドレスを、サイト内の端末に付与し、その結果ユーザー端末に複数のアドレスを付与するマルチプリフィクス環境を構築し、そこで経路選択情報とDNSサーバ選択情報、アドレス選択情報の三つの情報を、ホームゲートウェイやユーザー端末に配布する必要がある、という発表がなされました。また、この提案については、BBF（BroadBand Forum）において既に必要であるという合意がなされ、今回IETFへのリエゾン文書が送付されています。

・IPv6対応ISPのリスト化についての基本ガイドライン
（draft-kawamura-ipv6-isp-listings）

ユーザーがIPv6対応のISPを選定する際に、IPv6対応をうたっていてもISPごとに対応度合いがまちまちであり、明確な基準がなくユーザーに混乱をもたらす、といった問題への対処方法として、明確なIPv6対応項目リストを提示したものです。現在のドラフトでは、既存のIPv6対応ISPリストの情報を収集し、それらのチェック項目の詳細内容についてまとめ、新たなチェックを行う場合の判断基準について提案しています。今回のセッションでは、判断基準の妥当性や、Basic、Advancedといった判断基準をクラス分けする際のネーミングについて、活発な議論が行われました。

・IPv6でのCIDRによるアドレス集約（draft-azinger-cidrv6）

IPv6における将来的な経路表爆発問題が発生するという可能性を示唆し、その対策についての提案を行ったものです。近年IPv6のDFZ（Default Free Zone）において、IPv6 PIアドレスをはじめとした小さなアドレスブロックが広告されており、それによって将来IPv6もIPv4と同様に経路表爆発の問題が発生するとし、その推移の予想などを行っています。

またその対策として、できる限り集約した経路を広告するなどの手法がまとめられたRFC4692を遵守することを提案し、さらにアドレスを配布するIR（Internet Registry）に対しては、/32以上の大きなアドレスブロックを極力配布し、/48などの現在IPv6 PIとして配布している小さいアドレスブロックの配布は制限するか廃止することを推奨する、としています。セッションでは、RFC4692で述べられた手法の有効性や、IETFがアドレス配布といったIRの役割について踏み込むことの是非などについて議論が行われ、今後はIRと一緒に議論すべきであるなどの提案がなされました。

・エンドサイトへのIPv6アドレス割り当て
（draft-narten-ipv6-3177bis-48boundary）

既存のRFC3177に記述された、/48をエンドサイトに割り当てるという推奨文章を更新する件について提案がなされました。現在のIRでの、エンドサイトへのアドレス配布ポリシーでは、家庭ユーザーなどのエンドサイトに対して/56を割り当てることを想定した、割り振りアドレスサイズの検討が行われており、既にRFC3177に記述された状況との乖離が発生しています。このためRFC3177をアップデートすることで、乖離の解消を目的とした提案になっており、/64から/48の間に明確な境界を設けないこと、また/128単位でのアドレス配布は推奨されないことなどが盛り込まれています。セッションでの議論としては、そもそもエンドサイトに対して複数の/64を割り当てることの必要性など、基本的な部分の議論から行われ、必要以上にアドレスを付与してもかえって有害であるだとか、IPv6版NATの必要性を排除するためにも、潤沢なアドレスを付与することが必要だといった意見が出され、継続して議論を行うことになっています。

□第78回 IETF v6ops WGのアジェンダ
http://www.ietf.org/proceedings/78/agenda/v6ops.html

□v6ops WG
http://datatracker.ietf.org/wg/v6ops/charter/

◆softwire WG（Softwires WG）

softwire WGでは、トンネルを用いてIPv4 over IPv6、またはIPv6 over IPv4通信の実現方式を検討するWGです。IPv4 over IPv6やIPv6 over IPv4の汎用的なトンネル方式以外に、昨今さまざまなISPで導入が検討されている、DS-Lite（Dual Stack Lite）や6rd（IPv6 Rapid Deployment）といった、新しいIPv4とIPv6の共存環境を構築する方式が検討されています。

6rdはつい先日RFC5969として公開されました。DS-Liteは現在ADによるレビューが行われています。

・6rd+（draft-despres-softwire-6rdplus）
・6rd over UDP（draft-lee-softwire-6rd-udp）

今回のセッションでは6rdやDS-Liteへの拡張提案が主に議論され、まず6rdの拡張方式として、6rdをUDPでカプセリングすることで、CPEなどのNAT装置が6rdに対応していない環境において、ホストが6rdを終端し、IPv6アドレスを取得して利用する方式が提案されました。しかし、IPv4ネットワークを介して、ユーザーにIPv6接続性を提供する方法としては、既にTeredoやL2TPといった複数の方式が確立されており、既存の方式でカバーされていない部分は何なのかといった部分を詰める必要がある、という議論が行われました。

・DS-Lite RADIUSアトリビュート（draft-maglione-softwire-dslite-radius-ext）
・DS-Liteでのフローラベル利用（draft-donley-softwire-dslite-flowlabel）

また、DS-Liteの拡張提案も複数議論され、DS-Liteにおけるトンネルアドレスの RADIUSアトリビュートについての提案や、DS-Liteのトンネルについ てIPv6ヘッダのフローラベルを用いたQoS制御の提案などがありました。前者の必要性については賛同者多数でしたが、後者については、やはりフローラベルの仕様変更を含む提案であり、問題提起と要件定義というフレームワークを築いた上で議論を慎重に進めるべきである、という意見が多数ありました。

□第78回 IETF softwire WGのアジェンダ
http://www.ietf.org/proceedings/78/agenda/softwire.txt

□softwire WG
http://datatracker.ietf.org/wg/softwire/charter/

（NTT情報流通プラットフォーム研究所 藤崎智宏／松本存史）

■ 会場となったMECC（マーストリヒト国際展示会場）内の様子（MECC Webサイトより引用）

■ DNS関連WG報告

◆はじめに

今回のIETF78は、オランダのマーストリヒトにて開催されました。MECCと呼ばれるカンファレンスセンターにて開催されたのですが、その周囲には大学や企業しか存在せず、商店やレストランといったものが徒歩圏内に存在しませんでした。

そのため、会場近くのホテルに滞在している参加者は、食事をするにもバスや電車を利用してマーストリヒト市街まで出向く必要がありました。この点に関して、IETF78参加者のメーリングリストでは、もっと便利な場所を選べばいいのにといった否定的な意見が出ていました。その一方で、気候が素晴らしいといった肯定的な意見も出ていました。さまざまな意見があるのは当然ですが、個人的にはもっと便利な場所で開催して欲しいと感じたIETFでした。

IETFの会合としては、"Bar BoF（Birds of a Feather）"と呼ばれる、正規の時間帯ではない時間に、空いている会場を利用して暫定的に会合を開くグループが多く見られました。Bar BoFは、同じ問題や興味を共有する人々が集まって、活発に議論を行うためには良い形式なのですが、その一方で、IETF agendaに載っている正規の会合ではないため、気付かずに参加できない人が発生したり、正規のIETF会合との差がわからなくなってしまう等の問題があるため、その開催が増えることには賛否両論ありました。今回のIETF78では、私が把握している限りで18回のBar BoFが開催されていました。

◆dnsext WG

dnsext WGは、2回の会合を開催しました。主な議題はDNS zone aliasに関するものでした。あるDNS zoneをそのまま別ドメインのDNS zone定義として利用することができるようにする仕様で、前回のIETF77においても話し合われた議題です。このzone aliasは、TLDレベルのzoneに対しても利用できるように議論されており、例えば従来の国コード別TLD zoneとIDNによる国コード別TLD zoneとのaliasに利用するといった用途も考えられているようです。

zone aliasを実現するための提案としては、

（1）BNAME RR（Resource Record）の導入
（2）CNAME+DNAMEという定義の導入

という二つの案が出され、議論が行われました。

（1）の提案は、新たに BNAMEというzone aliasのためのリソースレコードを定義し、zone中にてBNAMEを利用してzone aliasを指定するという手法です。

例えば、aliasing-test.aaaというzoneを.bbbというzoneにaliasしたい場合には、aaa zoneにて

```
aliasing-test       IN BNAME       bbb.
```

と記述します。これによって、aliasing-test.aaaというzoneに定義されている名前は、すべてbbbというTLD zoneの名前にaliasされます。つまり、www.hoge.aliasing-test.aaaという名前のA RRを問い合わせると、www.hoge.bbbという名前にaliasされ、www.hoge.bbbに対応するA RRの応答が返ります。

（2）のCNAME+DNAME提案も、実現できることは同様です。従来のDNAMEによるzoneリダイレクションに加え、同様の定義をCNAME RRにて行うことで、同一の名前に対して、CNAMEとDNAMEで両方の定義があった場合のみ、zone aliasとして扱うようにするという提案です。CNAME+DNAMEの場合には、前述の例は、

```
aliasing-test       IN CNAME       bbb.
aliasing-test       IN DNAME       bbb.
```

と記述されます。

BNAMEは新たなRRの定義であるため、既存実装への影響が大きい一方で、既存のRR定義との混乱は起こりにくいといった意見が出されました。また、zone alias自体の賛否も含めた議論も行われ、結局どちらを標準とするかの結論は出ませんでした。その一方で、IDN TLDの導入も進んでおり、早急に仕様を決定したい、といった意見も出されました。引き続き議論が行われる模様です。

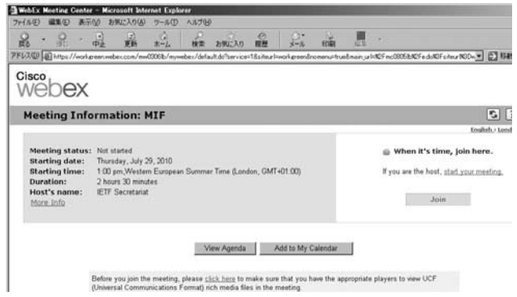
◆dnsop WG

今回のdnsop WGでは、特に中心となる大きな話題はなく、以前からあるいくつかの提案に関して報告と議論が行われました。

まずDNSSEC Operational Practicesに関する報告がありました。DNSSECの鍵管理について述べられた文章であり、RFC4641を更新するものです。DNSSECの仕様の更新に従ってRFC4641から変更されているものであり、特に議論はありませんでした。

次に、draft-mekking-dnsop-auto-cpsyncに関する発表がありました。この文章は、子ゾーンの鍵更新とともに、親ゾーンのDS RRを自動的に更新する仕組みを定義したものです。DNSのRR dynamic update機能を使い、親ゾーンのDSレコードを更新します。この提案に関しては、DSレコードのみではなく、それに付随するレジストリ的な管理情報もあるので、自動更新は適さないのではないかといった意見や、自動更新は必要だが、それはDNS dynamic update機能を利用するべきではない、といった意見が出されました。

また、draft-savolainen-mif-dns-server-selectionに関する発表がありました。これは、MIF（Multiple Interfaces） WGにて話し合われた提案をdnsop WGにて発表したものであり、複数のDNSサーバを選択するための手法を提案したものです。例えば、組織内部の名前を管理している内部用のDNSサーバと、外部の名前を解決するためのDNSサーバがあった場合に、クライアントがどう使い分けるか、という手法を定義しています。具体的には、DHCPv6に新たなオプションを定義し、クライアントはその情報を利用してDNSサーバの使い分けを行うという提案です。



■ いくつかのWGではJabberやWebExを利用した会議への遠隔参加も可能です

最後に、dnsop WGの議題ではありませんが、Root zoneのDNSSEC導入に関する報告が、同じ会場にて行われました。まず、DURZ[※1]を用いてRoot zoneの署名を行い、DURZの導入を段階的に進めていったことが報告されました。2010年7月15日に、正式な鍵を用いて署名されたRoot DNS zoneがすべてのRoot DNSサーバに導入され、いくつかのTLDのDS RRもRoot zoneに導入されたことが報告されました。

（JPNIC DNS運用健全化タスクフォースメンバー／
東京大学 情報基盤センター関谷勇司）

※1 DURZ（Deliberately Unvalidatable Root Zone）
意図的に検証不可能としたルートゾーン、またはDNSSECの検証をできないようにするため、意図的に入れられたダミーの署名データのことを指し、ルートゾーンにDNSSECを導入した場合に影響が出るかどうかの確認に利用されていました。

■ セキュリティ関連WG報告 ～IPSECME WG、TLS WGについて～

IETFには、セキュリティ関連WGが16WG存在しています。今回は、BoFとして開催されたFEDAUTHを含む、11WGがスロットを取り、12セッションが開催されました。セキュリティ関連のWGに関するこれらのミーティングは、領域および範囲が広いため、すべてのミーティング内容を把握することが困難な状況です。そこで本稿では、会期中に議論されたセキュリティ関連セッションの中から、認証やセキュア通信に特化した内容を議論するWGである、IPSECME WGおよびTLS WGの動向について報告します。

◆IPSECME WG（IP Security Maintenance and Extensions WG）

IPSECME WGは、2005年にクローズされたIPSEC WGの後継WGであり、（IPSEC WG） クローズ後に必要になった仕様拡張や既存ドキュメントの明確化などの議論を行うためのWGです。このミーティングは、2010年7月26日（月）の午前9時から1時間半程度開催されました。参加者は40人程度でした。

IPSECME WGにおいて、今回の会議までにRFCとして発行されたドキュメントやRFCとして発行される直前のドキュメントに関する状況を示します。

＜RFCとして発行されたドキュメント＞

・RFC5879 Heuristics for Detecting ESP-NULL Packets

暗号化されたESPパケットからESP-NULLパケットを識別するためのヒューリスティックについて記述したドキュメントです。なお、本RFCはInformational（情報）の種別として発行されました。詳細についてご興味のある方は、下記URLをご参照ください。

URL: http://tools.ietf.org/html/rfc5879

・RFC5930 Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol

鍵交換プロトコルであるInternet Key Exchange version 2（IKEv2）において、AES-CTRを利用できるように仕様化したドキュメントです。なお、本RFCはInformationalの種別として発行されました。詳細についてご興味のある方は、下記URLをご参照ください。

URL: http://tools.ietf.org/html/rfc5930

＜RFCとして発行される直前のドキュメント＞

・Internet Key Exchange Protocol: IKEv2
（draft-ietf-ipsecme-ikev2bis-11）

IKEv2について記述するドキュメントです。このI-D（Internet-Draft）がRFC化されると、以前発行されたRFC4306（Internet Key Exchange（IKEv2）Protocol）とRFC4718（IKEv2 Clarifications and Implementation Guidelines）のドキュメントが廃止されることになります。なお、I-Dのステータスは、RFC Editorの編集待ちリストに掲載されている状態（RFC Editor queue）です。本I-Dは、インターネット標準化過程（Standards Track）に含まれるドキュメントとして発行される予定です。

・IPsec Cluster Problem Statement
（draft-ietf-ipsecme-ipsec-ha-09）

クラスタ上でのIKEやIPsecを実装するための要求条件や問題の提示および専門用語について定義し、また、異なるクラスタ間の相互運用を可能にするピアを許可するために存在している、仕様と実装のギャップを記述しているドキュメントです。なお、I-Dのステータスは、RFC Editor queueです。本I-Dは、Informationalに分類されるドキュメントとして発行される予定です。

・An Extension for EAP-Only Authentication in IKEv2
（draft-ietf-ipsecme-eap-mutual-05）

このドキュメントは、IKEv2において、拡張可能な応答者認証を提供するための相互認証（mutual authentication）や鍵合意（key agreement）を提供するEAP（Extensible Authentication Protocol）を仕様化するドキュメントです。なお、I-Dのステータスは、RFC Editor queueです。本I-Dは、Standards Trackのドキュメントとして発行される予定です。

・IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap
（draft-ietf-ipsecme-roadmap-08）

IPsecやIKEに関係するRFCが多く発行され、それぞれの関係などが複雑化しており、そのドキュメントの背景や要約を記述することで整理することを目的としたドキュメントです。なお、I-Dのステータスは、IESG Evaluationです。本I-Dは、Informationalのドキュメントとして発行される予定です。このI-DがRFC化されると、以前発行されたRFC2411（IP Security Document Roadmap）は廃止されます。

＜今回議論された検討項目＞

今回のミーティングで議論された検討項目は、以下の通りです。

- IPsec-HA Recap
- Proposed IPsec HA Cluster Protocol
- Secure Failure Detection Decision Process
- Modes of Operation for SEED for Use with IPSec
  （draft-seokung-ipsecme-seed-ipsec-modes-00）

今回のIPSECME WGミーティングでは、大きく分けるとIPsec HA関連の議論とIPsecに対して暗号アルゴリズムを追加する話題になりました。また、今回のIETF会合においては、通信の安全性を保つためのセキュアプロトコルに対して、暗号アルゴリズムを追加する提案について、セキュリティエリアに影響を及ぼす発表もありました。そこで、IPSECME WG内での話題ではありませんが、これに関連した、7月29日（木）のIETF Security Area Advisory Group（SAAG）での、セキュリティエリアディレクタSean Turner氏の発表「Cipher Suite Proliferation」について少し触れます。

Turner氏の発表では、現状におけるWGの状況を考慮して、Standards Trackとして発行するRFCを厳選することにより、RFC化に関係する人達の負荷を軽減しようという考えから、二つの選定ルールが提示されました。この発表資料は、以下のURLからご覧いただけますので、興味のある方はご参照ください。

□Sean Turner氏の発表資料:
http://www.ietf.org/proceedings/78/slides/saag-4.pdf
なお、IPSECME WGの詳細情報およびI-Dについては、以下のURLをご参照ください。

□IPSECME WG
http://www.ietf.org/dyn/wg/charter/ipsecme-charter.html

□第78回IETF IPSECME WGのアジェンダ
http://www.ietf.org/proceedings/78/agenda/ipsecme.txt

◆TLS WG（Transport Layer Security WG）

TLS WGは、インターネット上で情報を暗号化して送受信するためのプロトコルであるTLS（Transport Layer Security）について、仕様の拡張や新規Cipher suiteの検討を行うWGです。今回のミーティングは、2010年7月29日（木）の午後3時10分から1時間程度開催されました。参加者は40人程度でした。

今回のミーティングで議論された検討項目は以下の通りです。

- Transport Layer Security (TLS) Cached Information Extension
  （draft-ietf-tls-cached-info-09）
- AES-CCM ECC Cipher Suites for TLS
  （draft-mcgrew-tls-aes-ccm-ecc-00）
- Prohibiting SSL Version 3.0 and Earlier
  （draft-turner-ssl-must-not-01）
- Representation and Verification of Domain-Based Application Service Identity in Certificates Used with Transport Layer Security
  （draft-saintandre-tls-server-id-check-08）

このミーティングで、個人的に注目したい発表は、「Prohibiting SSL Version 3.0 and Earlier」です。理由としては、普段の生活の中で一般的に利用されているSSLプロトコルですが、古いバージョンのSSLプロトコルを利用してしまうと、安全性を担保するためには不十分な鍵長を使用することになってしまい、安全な通信ができない懸念があるからです。そのような状況を防ぐために、暗号アルゴリズムの危殆化※1対応（暗号アルゴリズムの世代交代）の考え方に従い、このI-Dが執筆されたと考えます。IETFにおいてセキュリティ関連を議論しているエリアなので、他のエリアに先駆けて暗号アルゴリズムの危殆化対応も行っているという印象を持ちました。このI-DがRFC化されると、RFC5246（The Transport Layer Security（TLS） Protocol Version 1.2）を更新します。

なお、TLS WGの詳細情報およびI-Dについてご興味があれば、以下のURLをご参照ください。

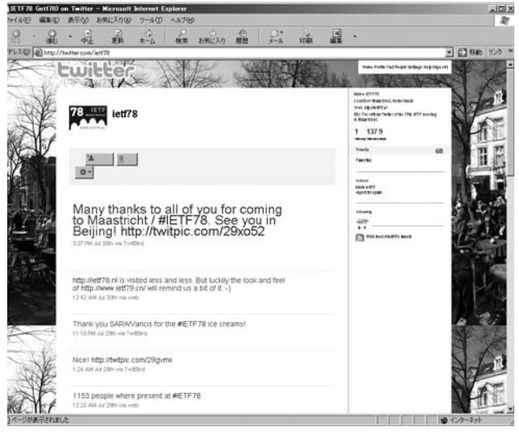
□TLS WG
http://www.ietf.org/dyn/wg/charter/tls-charter.html

□第78回IETF TLS WGのアジェンダ
http://www.ietf.org/proceedings/78/agenda/tls.txt

（NTTソフトウェア株式会社 菅野哲）

※1 暗号アルゴリズムの危殆化
簡単に言えば、暗号アルゴリズムの安全性のレベルが低下した状況、または、その影響により暗号アルゴリズムが組み込まれているシステムなどの安全性が脅かされる状況を指します。詳しくは下記のURLをご覧ください。

JPNIC Newsletter No.44「インターネット10分講座:暗号アルゴリズムの危殆化」
http://www.nic.ad.jp/ja/newsletter/No44/0800.html



■ Twitterによる情報発信も行われています