JPドメイン名サービスへのDNSSEC導入

◆ はじめに ～DNSの仕組みと重要性～

DNSは、ドメイン名とIPアドレスとを対応させる仕組みとして、インターネットの基盤を構成する上で必要不可欠なシステムです。ブラウザでWebサイトを閲覧したり、メールをやりとりしたりすることができるのも、裏でこのDNSが動いているからです。

IPで接続されたネットワークという意味でのインターネットが、まだ日本には存在しなかった頃、1983年に米国でDNSが開発されました。DNSは、その当時から基本的な仕組みはそのままに、現在に至るまで四半世紀以上にわたりインターネットが拡大する中で運用され続けている、世界的な分散データベースシステムなのです。

私達がインターネットを安心して利用するためには、DNSが正常に機能していることが必要です。しかし、1990年代からDNSの応答を偽装する攻撃手法の存在が指摘され、これを防止するためのセキュリティ付加技術としてDNSSEC（Domain Name System Security Extensions）※1が開発されました。

◆ DNSSEC導入への機運が、世界的に高まったきっかけ

インターネットが社会的に重要性を増し、それを支えるDNSにもさらなる安定性や安全性が求められるようになってきた中で、2008年にDNS応答を偽装させる効率的な攻撃手法が明らかになったことが、DNSSECの導入が世界的に進められる大きなきっかけになりました。

DNSは、ICANNによって管理されるルートゾーンを頂点として、「.jp」や「.com」などのTLD（トップレベルドメイン）、そしてさらにそれぞれ個別のSLD（セカンドレベルドメイン）、さらにそのサブドメイン……、という階層構造を成しています。DNSSECは、このルートゾーンから目的のドメイン名まで、すべての階層で導入されないとうまく機能しません。

とはいえ、DNSSECの導入は、インターネットの基盤を構成する上で欠かせない仕組みであるDNSに新たな機能を追加するものであり、「今動いているものに手を入れる」ことになるため、慎重に進めていかなければなりません。

導入にあたっては、インターネットに悪影響を与えることなく、また、多数の階層での対応が必要であることから、多くの関係者が協調して作業を行っていく必要があります。

DNSSECの導入は、インターネット全体、世界全体にとって、とても大きな出来事なのです。

◆ .jpにDNSSECが導入されるまでの経緯

JPドメイン名の登録管理組織（レジストリ）であるJPRSでは、2009年7月にJPドメイン名サービスへのDNSSECの導入を正式に表明し※2、準備を開始しました。.jpゾーンを管理するDNSサーバであるJP DNSサーバへDNSSECを導入する際に、万が一のことがあった場合、インターネットに大きな混乱を引き起こすことになるため、事前の準備には長い時間を必要としました。

一方、ICANNもルートゾーンへのDNSSEC導入の検討を慎重に進め、ようやく2010年の7月にルートゾーンへのDNSSEC導入が行われました※3。次はいよいよTLDへのDNSSEC導入です。

JPRSでは、2010年10月に、DNSSECで用いる鍵情報を生成する.jp DNSSECキーセレモニーを実施し※4、.jpゾーンへの署名を開始しました。そして運用に支障がないことを確認した後、2010年12月にルートゾーンのDNSSECとの関連付けを行いました※5。

DNSSECの導入に取り組む組織や個人のために、JPRSは、DNS運用に関わる事業者、機器メーカー、ソフトウェアベンダーなどとともに進めてきた技術検証の成果や、DNSSEC関連RFCの翻訳など、DNSSEC導入の中で得られたさまざまな成果やノウハウなどを、積極的にWebで公開しました。

さらに、DNSSECを適切かつ安定して運用していくためには、運用ポリシーや考え方、手順などを明確化しておく必要があります。これがDPS（DNSSEC Practice Statement）※6と呼ばれる文書で、JPRSでも「JPドメイン名におけるDNSSEC運用ステートメント（JP DPS）」として公開しました※7。

これらの準備を進めた後、2011年1月16日にJPドメイン名サービスへのDNSSEC導入を実施しました※8。これにより、個々のJPドメイン名でDNSSEC運用を行い、その鍵情報をJP DNSサーバに登録することができるようになったのです。

● キーセレモニーに参加された方々（JPRSのWebサイトより引用）

◆ DNSSECをめぐる、国内外の動き

DNSSECの導入ならびに普及には関係者間の密接な連携が必要なため、国内のコミュニティとしてDNSSECジャパンが2009年11月に設立され、2011年2月現在でJPRSも含めて36団体が会員となっています。DNSSECジャパンでは、導入・運用に関する課題の整理と検討が行われ、参加者の技術力の向上、ノウハウの共有を促進するとともに、普及のためのイベント開催や外部での講演などの活動を進めています。

世界的なDNSSECの導入動向としては、原稿執筆時点（2011年2月16日）において、62のTLDがDNSSECを導入し、ルートゾーンとDNSSECの関連付けを行っています。影響が大きいところでは、国内でも多く利用されている.comが2011年3月31日にDNSSECを導入する予定となっています。（その後、予定通り.comにDNSSECが導入されたことが、レジストリである米VeriSign社から発表されました）

◆ おわりに

DNSSECによりインターネットの安全性を向上させていくためには、DNSの管理運用に携わるすべての関係者の協力が欠かせません。また、DNSSECの普及のためには、ホスティング事業者やプロバイダー事業者の方々の、積極的な取り組みが必要です。JPRSでは今後も各方面の関係者と協力しながら、DNSSECの導入を推進していきます。

JPRS DNSSEC関連情報　http://jprs.jp/dnssec/
DNSSECジャパン　http://dnssec.jp/

（株式会社日本レジストリサービス（JPRS） システム運用部 坂口智哉）

※1 DNSSEC（Domain Name System Security Extensions）
DNSに関するセキュリティの強化を行うための拡張機能。DNSで提供する情報に電子署名を付加し、DNSを使って得られた情報と発信元にある情報との同一性を保証します。

※2 JPドメイン名サービスへのDNSSECの導入予定について
http://jprs.jp/info/notice/20090709-dnssec.html

※3 ルートゾーンへのDNSSEC署名の追加について
http://www.nic.ad.jp/ja/topics/2010/20100716-01.html

※4 .jp DNSSECキーセレモニーの実施について
http://jprs.jp/info/notice/20101015-keyceremony.html

※5 ルートゾーンへの.jpゾーンのDSレコード登録・公開に伴う影響について
http://jprs.jp/info/notice/20101210-ds-published.html

※6 DPS（DNSSEC Practice Statement）
DNSSECの運用者が作成する、運用内容を明文化し情報公開するための文書です。各章には、DNSSECにおける署名検証の考え方（DNSSEC Policy（DP））と、これを実現するための実施要領であり文書自体の名前にもなっている、DNSSECの運用ステートメント（DNSSEC Practice Statement（DPS））の二つが記述されます。

※7 JP DPSの公開について
http://jprs.jp/info/notice/20110114-jpdps.html

※8 JPRSがJPドメイン名サービスにDNSSECを導入
http://jprs.co.jp/press/2011/110117.html

APNIC 31 ミーティング報告

アドレスポリシー動向

APNIC 31ミーティングは、APRICOT-APAN 2011カンファレンスと共催の形で、2011年2月21日（月）～25日（金）の5日間、香港で開催されました。

◆ 全体概要

今回のミーティングに参加したAPNIC会員数は例年に比べ多く、約420名でした。また、APRICOT全体の参加者数は、APNICミーティングおよびAPANも併せての開催となったため、1,171名となり、昨年の参加者数733名と比べても非常に多い結果となりました。

APNICの会員数を国および地域別に見ると、香港は53ヶ国・地域中、上位5位に入りますが、APNICミーティングの開催地となったのは、今回が初めてです。会場となった、香港島北部、灣仔（Wan Chai）地区にある香港コンベンションセンターは、香港返還の式典が行われた会場でもあり、香港の中でも重要なイベントや会議、式典の多くがここで行われてきました。灣仔はオフィスビル、市場、定食屋などの地元の飲食店がすべて混在している地域で、アクセスもよく、参加者が香港の雰囲気を味わうにはよい立地の会場だったように思います。

今回のAPNICミーティングは、IANA在庫枯渇後初めてのミーティングであり、また、次回8月後半のAPNICミーティングまでにAPNIC在庫も枯渇している可能性が高かったことから、枯渇に向けた最後の分配方法について、必要な対策を最終的に検討する上で、非常に重要なタイミングでのミーティングでした。

当初は提案数も多く、同じテーマで複数の提案が提出されていることから、ミーティングでの議論では意見がまとまりきらないことも懸念されていましたが、最終的には6点の提案がコンセンサスに至りました。前回のミーティングではコンセンサスが得られた提案がなかったため、対照的な結果です。

今回コンセンサスが得られた提案はすべて、その後4週間のメーリングリストでの議論期間に大きな反対もなく、APNIC理事会により承認されたことから、APNICで施行されることになりました。

また、今回は現職ECメンバーの任期満了に伴う選挙が行われ、4名のECメンバーが選出されました。

◆ アドレスポリシー提案の結果

IANA在庫枯渇後間もないというタイミングもあり、今回は最後の/8からの分配に関するテーマだけでも提案5点（うち1点は提案者によりその後取り下げ）が提出され、ミーティングでは合計11点※のポリシー提案について議論が行われました。

※ 当初は15点を予定、このうち1点は取り下げ、1点は提案者不在、2点は提案者の意思により、今回議論せず。

これらの提案は、下記テーマごとに分類した上で議論が行われました。

-「APNICにおける最後の/8在庫からの分配方法の変更」(3点)
-「IPv4アドレスの移転」(2点)
-「在庫枯渇後に返却されたIPv4アドレスの管理」(4点)
-「IPv6アドレスポリシーの変更」(2点)

以下に、テーマごとのポリシー提案の結果をご紹介します。

● APNICにおける最後の/8在庫からの分配方法の変更

<今回コンセンサスの得られた提案>

- prop-094：Removing renumbering requirement from final /8 policy
- prop-093：Reducing the minimum delegation size for the final /8

現在のポリシーでは、APNICにおける最後の/8在庫からの分配は、初回割り振りまたは追加割り振り基準を満たしていることを前提に、1組織につき、/22(1,024アドレス)1回限りの分配が認められています。

今回のミーティングでコンセンサスが得られた内容による変更点は、以下の通りです。

1)分配サイズは一律/22ではなく、最小分配単位を/24とし、最大で/22までの分配が認められます。これにより、/22を必要としない組織にはより小さな単位で分配を行うことが可能となります。

2)/24を超える分配は、必要性を証明することで1度または複数回に分けて、最大で/22までの分配が認められます。

3)クリティカルインフラへの割り当ても、最後の/8からの分配対象に含まれます。

- 現在のポリシーにおいて分配を認めている、クリティカルインフラと定義されたネットワークへのIPv4アドレス分配が、最後の/8からの分配においても認められるようになります。

4)APNICの最後の/8在庫からの分配における、リナンバ要件が撤廃されます。

- 現在の初回割り振り基準の要件では、割り振りから1年以内に、それまで上流のISPから割り当てを受けていたアドレスのリナンバを行うことが含まれています。つまり、初回割り振りを受けた際、新たに割り振られたアドレスをネットワークに付け替え、これまで利用してきたアドレスを、上流へ返却することが必要です。
- 前述のリナンバ要件に基づき、これまで利用していたアドレスを上流に返却しても、在庫枯渇前は、「これまで利用していたアドレス」と「今後必要となるアドレス」を合計したアドレスの割り振りを受けることができるため、必要アドレス数は確保できます。
- しかしながら、最後の/8からの分配においては、分配可能サイズが/22と限定されるため、リナンバ要件により、これまで利用していたアドレスを返却すると、これを充当する割り振りを受けることができず、返却した分のアドレスが不足してしまうことになるわけです。こうした事態を防ぐため、今回APNICの最後の/8在庫からの分配における、リナンバ要件が撤廃されました。

● IPv4アドレスの移転

<今回コンセンサスの得られた提案>

- prop-095：Inter-RIR IPv4 address transfer proposal
- prop-088：Distribution of IPv4 address once the final /8 period

IPv4アドレスの移転をAPNIC地域内に限定せず、APNIC地域との移転を認めるRIRとの移転が、以下の条件で認められることになります。

移転元:移転元RIRが定義する移転要件に従う
移転先:移転先RIRが定義する移転要件に従う

当初に提案されていた要件は、移転元、移転先どちらも、移転元RIRの移転要件に従うとしていましたが、「移転先で定義している移転要件とのすみ分けが難しい※」「結果として移転元、移転先の両RIRの移転要件を適用することになる」等の理由から支持されず、上記要件でコンセンサスが得られました。

※ 移転元の要件を適用するとしながらも、実質的には移転先組織は、移転先で定義している移転要件も適用されることが想定され、その場合移転元、移転先それぞれで定義している要件のすみ分けが難しい。

またこの議論では、APNICでは移転を認めても、他のRIRがAPNICとの移転を認めるのか、という点の確認も行われました。現時点でARIN地域で提案されているRIR間の移転を認めるポリシーでは、移転時にアドレスを効率的に利用しているかどうかの確認を実施していることが条件として定義されています。

この条件を前提に、ARIN地域でのRIR間の移転を認めるポリシー提案が通った場合、APNIC地域では移転時の効率的利用の確認を実施していないため、実質的には、ARIN地域とAPNIC地域間の移転は認められないことになります。

こうしたARIN地域における議論も考慮し、ARIN地域との移転が実質的に認められるよう、RIR間での移転を認める提案と併せて、APNIC地域での移転時におけるアドレス効率の確認を、APNIC在庫枯渇前と同様に在庫枯渇後も継続する提案も行われました。しかし、移転時の利用確認を条件とすることが正式な手続きを経ない移転につながり、移転結果もデータベースに反映されなくなるのではとの懸念が強かったことから支持されず、結果的には継続議論となりました。

● 在庫枯渇後に返却されたIPv4アドレスの管理

<今回コンセンサスの得られた提案>

- prop-097：Global Policy for post exhaustion IPv4 allocation mechanisms by the IANA

在庫枯渇後にIANAへ返却されたIPv4アドレスと、APNICへ返却されたIPv4アドレスの分配ポリシーについて、それぞれ提案が行われました。どちらの提案においても、再分配するのに十分なサイズのIPv4アドレスが実際に返却されることを期待しているというよりも、紛争を避けるために再分配方法をあらかじめ定義しておくことを主な目的としています。

IANAへ返却されたIPv4アドレスの分配:

- 最小単位を/24として各RIRへ分配される提案が、APNIC地域ではコンセンサスに至りました。
- この提案はIANAからの分配に関わるグローバルポリシーに該当するため、施行にあたっては今後、全RIR地域におけるコンセンサスと、ICANN理事会による承認が必要となります。

APNICへ返却されたIPv4アドレスの分配:

- 最後の/8在庫からの分配ポリシーを適用している段階で返却されたIPv4アドレスは、最後の/8ポリシーを適用することになります。その結果、APNICのIPv4アドレス在庫が/8を超えたとしても、本提案での分配ポリシーを適用するとしています。
- 返却されたIPv4アドレスは、最後の/8在庫とは別に管理し、APNIC事務局で今後再分配方法を定義することを求める提案も行われました。しかし、再分配方法が定義されていないことで紛争が生じることを避けるためにも、APNICでの在庫枯渇前に、再分配方法が明確に定義されていることの方が重視され、棄却されました。

● IPv6アドレスポリシーの変更

<今回コンセンサスの得られた提案>

- prop-083：Alternative criteria for subsequent IPv6 allocations

1組織で複数のネットワークを運用している場合、初回割り振りで分配を受けた最小割り振りサイズ(/32)を分割して、複数のネットワークで利用すると、フィルタリングされてしまうという問題があります。また、6rd技術を利用したIPv6ネットワークの運用を行う場合、実際のユーザーへのIPv6アドレス分配としてではなく、パケットに埋め込むために必要なIPv6空間を確保する必要があります。

これらのケースにおいては、現在のIPv6アドレスポリシーで定義されている分配基準を満たしていなくとも、別に定義される要件を満たしている前提で、IPv6アドレスの割り振りも認めることになりました。

◇　　◇　　◇

なお、今回のミーティング内容、およびポリシー提案の結果については、下記URLもご参考になさってください。

□ APNIC 31ミーティング
http://meetings.apnic.net/31/

□ ポリシー提案の結果
http://www.apnic.net/community/policy/proposals/

● 発表者に質問する筆者

◆ APNIC EC選挙

今回は7名の候補者の中から、以下の4名がAPNIC ECとして選出されました。なお、残り3名のECに変更はなく、現在のAPNIC ECは合計7名の、会員により選出したメンバーとAPNIC事務局長Paul Wilson氏により構成されています。

Gaurab Raj Upadhaya氏(Limelight Networks社)
James Spenceley氏(Vocus Communications Limited社)(再選)
Kenny Huang氏(TWNIC)
Wei Zhao氏(CNNIC)

候補者のプロフィールも含めた詳細は、以下のURLよりご確認ください。
http://meetings.apnic.net/31/elections/

◆ 次回のAPNICミーティング

次回のAPNICミーティングは、2011年8月29日(月)～9月2日(金)に韓国・プサンで開催される予定です。

□ APNIC 32
http://meetings.apnic.net/32/

(JPNIC IP事業部 奥谷泉)

APNICとの技術的な情報交換

◆ はじめに

APRICOTミーティングは、環太平洋地域のIPアドレスポリシーや技術動向の情報交換、技術者同士の交流を目的とし、毎年2月末から3月初頭にかけて開催されています。また、年に2回開催されるAPNICミーティングと共催となることが毎年の恒例となっています。

余談ですが、今年はアジア太平洋地域の研究・教育ネットワークを取りまとめた組織およびその会議であるAPAN（Asia-Pacific Advanced Network Consortium）とAPRICOTが合同で開催され、APRICOT-APAN 2011カンファレンスとなりました。

本稿では、筆者の参加目的の一つであった、APNICとの情報交換についてお知らせします。

◆ APNIC技術チームとの情報共有

2011年2月22日（火）の午前中、NIR SIGが開催されました。NIR SIGは毎回のAPNICミーティングで開催されており、APNICとAPNIC管理地域下のNIRとの情報共有、意見交換を目的としています。NIR SIGでは、システムに関する話題だけでなくアドレス申請やアドレスポリシーにも関わる内容が含まれますが、本稿では、筆者が特に関係するアドレス申請や、逆引きDNSシステムに関する話題を中心にお届けします。

今回のNIR SIGには、APNICの他にCNNIC、TWNIC、KRNICなどのAPNIC管理下地域の各NIRが参加しており、過去のNIR SIGでは、毎回APNIC技術チームからAPNICがその年に実施する重要なシステム開発計画などが共有され、参加したNIRとの意見交換が行われてきました。

今回のNIR SIGでは特に、APNICが管理する逆引きDNSにおけるDNSSEC対応とリソース証明書に関する対応状況やスケジュールが共有されました。また、この他にも、APNICとの個別相談の形で、JPNICからAPNICの技術担当へ、逆引きDNSに関する問題の状況確認と反映監視について情報を交換しました。

以降でこれら2点について詳細を報告します。

（1）逆引きDNSにおけるAPNICのDNSSEC対応

APNICでは、2008年度から逆引きDNSへのDNSSEC導入の検討を開始し、現在まで試験システムの開発を継続しています。前回のAPNIC北京ミーティングやAPRICOTクアラルンプールミーティングでの報告では、2010年下半期には、導入に向けたテストを開始する予定となっていました。しかしながら、開発の進捗状況や他の組織との連携が必要であり、NIRとの逆引きDNSSECに関するシステム導入テストは、2011年の6月からスタート可能であることが共有されました。

具体的には、APNICメンバーやNIRが利用するAPNIC IPアドレス申請システム「MyAPNIC」において、DNSSEC関連機能の実装と提供が2011年6月頃となり、希望するNIRやメンバーに試験提供されることが明らかとなりました。なお、補足として、NIRやAPNICメンバーの逆引きDNSに関するDNSSEC対応は任意であるとされ、APNICが強制することは、現時点ではないことも併せて明確にされました。

JPNICとしては、逆引きDNSへのDNSSEC対応については、以前から継続して検討中のステータスであり、今後の実装やシステム開発などの対応以前に、そもそも対応するかどうか自体が未定となっていますが、NIRが実施する際に必要な、APNICとNIR間向けのデータ転送システムにおけるDNSSEC対応については、MyAPNICと同様に対応可能であることはわかっています。

APNICのDNSSEC対応に伴うシステム変更は、既存のシステムへ機能を追加する形で進め、既存システムへの影響は軽微であることが何度も説明されました。APNICでは、これまで通り、逆引きDNSに関連するシステムは利用可能であり、特に新規システムへの移行なども発生しないことが分かりました。

JPNICは、JPNICが管理するIPアドレス逆引きについて、1日に数回、逆引きDNSのゾーンデータが正しくネームサーバへ反映されているかを継続してモニタリングしています。最近、APNIC技術チームの対応や改善の成果もあって、直近の半年間はかつて発生していた逆引きに関するトラブルがほとんど発生しなくなりました。DNSSEC機能追加時にも、現在の安定した状況が継続することを期待している旨をAPNIC担当者へ伝えました。今後も継続してAPNICのシステム運営に関する情報を収集し、APNICとも協力し、JPNIC管理下やその他の地域への問題が発生しない状況を維持したいと考えます。

（2）リソース証明書に関するAPNICの情報共有

近年、RIRや一部の技術者で議論が行われているリソース証明書の実装や実験についての検討状況が、APNICから共有されました。RIRであるAPNICとしては、リソース証明書については継続した研究の段階であって、今すぐにNIRやメンバーに実装を提供できる状況ではないとされました。しかしながら、準備段階として、NIRとしてRPKI（リソースPKI）導入時の業務フローや連携のフローの検討を開始してほしいとアドバイスがありました。また、RPKIシステムの実験については、ISC（Internet Systems Consortium）が開発したテストコードをAPNICからNIRへ提供することも可能、ということが発表されました。

これまでAPNICやJPNICなどIPアドレスレジストリは、ルーティング技術者との関係はIRRを提供すること等、間接的な関係であると筆者は認識しておりました。しかしながら、RPKIやROA（Route Origin Authorization）等が実装され、それがISPなどで本格的に利用される場合、これまで以上に、レジストリとしての運営責任が大きくなり、それに備えていかなければならないと感じました。

◆ 終わりに

今回新たに感じたことは、APNICはレジストリとして、ルーティング技術者へ積極的にアプローチしようと、試行を繰り返していることです。筆者が面白いと感じたことの一つは、APNICの周知活動の一環として、ルータなどで設定されたBogon FilterなどのACLの更新を促す注意喚起カードが会場において配布されていたことです。こういったことからも、APNICの「ルーティング技術者へリーチしよう」という意気込みを感じました。

JPNICでもJPIRRの運営やリソース証明書の実験などを通し、継続して情報交換・交流を継続し、今後、レジストリがルーティング技術者とどのように連携すればよいかを、考えていかなければならないと思います。

（JPNIC 技術部 岡田雅之）

● 会場で配られていたBogon FilterなどのACL更新を促す注意喚起カード

アドレス枯渇を目前に、IPv6導入やRIRのアドレス品質向上に対する取り組み

本稿では、IPv4アドレスの在庫枯渇というエポックを目前に控えた時期に開催されたAPNIC 31ミーティングにおいて、筆者が特に注目したIPv6関連の話題やRIRで行われているアドレスの品質向上に向けた取り組みについて報告します。

◆ APOPSにおけるIPv6の話題

Asia Pacific Operators Forum(APOPS)は、APNICコミュニティの中でネットワーク運用に関わる話題を扱うフォーラムです。APOPSの全体会議であるAPOPSプレナリーは、2011年2月21日(月)の16時40分から18時にかけて行われました。約240名が参加していました。

今回は、併設のAPAN-APRICOT 2011の参加者が流れてきていて人数が多かったこともあり、プレゼンテーション(以降、プレゼン)の内容を受けて、参加者同士のディスカッションがいつもよりも活発に行われていたようです。APOPSプレナリーで行われたプレゼンを以下に紹介します。

（1） World IPv6 Day

Google社のLorenzo Colitti氏のプレゼンです。World IPv6 Dayは、Google社、Facebook社、Yahoo!社、Akamai社、Limelight Networks社などが提供するWeb上のサービスにおいて、協定世界時の2011年6月8日0時から23時59分までの間、一斉に「IPv6を優先しよう」とするイベントです。この時間帯、参加企業のDNSサーバでは、Aレコードよりも優先してAAAAレコードが返されるように設定がなされます。このようにIPv6を多くのユーザーが使う日を設定することで、IPv6の大規模な展開にあたっての課題を解決していくことを目的としています。詳しくは以下をご覧ください。

・World IPv6 Day
http://isoc.org/wp/worldipv6day/

（2） Operational Problems in IPv6: Fallback Issues

NTT情報流通プラットホーム研究所の岡田真悟氏によるプレゼンです。IPv6からIPv4にfallbackする動作において起きる遅延を、さまざまな利用環境において計測し、多くの利用環境で、ユーザーが不便を感じる程度にまでなってしまうことを指摘しています。会場でも話題になり、今後OSの実装やIETFでのディスカッションに影響すると考えられます。

（3） 6rd-Enabling IPv6 Customers on an IPv4-only Network

Cisco社のJoe Wang氏によるプレゼンです。ISPの運用者に向けて、IPv4のみのユーザーにIPv6の接続性を提供するために6rdを採用した事例を紹介しています。6to4やDS-Liteなどのトンネリング技術と比較検討されています。


● 会場の様子

◆ NIRにおけるIPv4の在庫枯渇対応やIPv6の導入促進

APNIC 31でのNIR SIGは、2011年2月22日(火)11時から12時過ぎまで行われ、30名以上が参加していました。NIR SIGでは、NIRで行われているIPv6の導入促進について活動報告が行われました。またIANA在庫枯渇時の情報共有のされ方を振り返り、RIRの在庫枯渇に関する情報共有がどうあるべきか、といったディスカッションが行われました。各NIRの報告内容は次の通りです。

- TWNIC
IPv4の在庫枯渇に関するWebページを提供するとともに、“IPv6 Directory”と呼ばれるIPv6対応機器の一覧を作成し提供しています。また、IPv6導入のガイドライン等のドキュメントも作成されています。

・IPv6 Ready Logo Program Approved List
http://v6product.ipv6.org.tw/

- KRNIC
Next Generation Internet Address (IPv6) Transition Planと称して、三つの施策を取っています。
(1)WebサービスやIPTV、3GネットワークにおけるIPv6商用サービスの促進
(2)IPv6の優先割り振りやIPv4の在庫枯渇基準日の設置
(3)IPv6 Transition Centerの設置およびその機関を通じた移行プランの周知徹底、などが行われています。

- CNNIC
CNNICからは、技術的なリサーチ活動の紹介が行われました。さまざまなプロトコルについて技術的なIPアドレスの利用形態を調査し、IPv6アドレスのフォーマットを再検討するなどの活動が行われています。なお、IANAの在庫枯渇の際には、メディア対応などが行われたとのことです。

- JPNIC
JPNICからも、2月3日のIANA在庫枯渇の際に、NRO、ICANN、ISOC、IABによる合同式典とプレスカンファレンスの中継、および同時通訳について紹介を行いました。後日、個別にNIRの方々とお話しした際に、一部のNIRの方々から、JPNICの活動を評価しており、「今後連携を図りたい」といったコメントをいただきました。

【速報】IANAからAPNICへ、二つの/8ブロックが割り振られました
http://www.nic.ad.jp/ja/topics/2011/20110201-01.html

【(IANA枯渇)続報】NROからのプレスカンファレンスの案内
http://www.nic.ad.jp/ja/topics/2011/20110201-02.html

【(IANA枯渇)第3報】NROプレスカンファレンスの日本語同時通訳ストリーミング提供のご案内
http://www.nic.ad.jp/ja/topics/2011/20110203-01.html

最後に、APNICのPaul Wilson氏やJPNICの前村昌紀がディスカッションに加わり、RIR在庫枯渇の情報共有においては、APNICとNIRが協力して進めていこうという意識共有が行われて、ミーティングが終わりました。

◆ RIRにおけるアドレス品質向上の取り組み

APNICをはじめとするRIRでは、Resource Quality Assurance (RQA)と呼ばれる活動が行われています。RQAは、ISP等によるフィルタリングや経路制御のために、インターネットにおける到達性が一部失われているようなIPアドレスを調査し、その到達性を改善する活動です。IPアドレスが返却され、そのアドレスが再割り振りされる場合を想定して、インターネットにおける到達性という意味で「品質」を保つことを目的としています。

APNIC 31では、RQAに関する「RQA BoF」が開かれました。2011年2月23日(水)の17時過ぎから19時過ぎにかけて行われ、約20名が参加しました。BoFで報告された主なRQA活動を以下にまとめます。

- RIPE NCC
これまでBogonリストに入っていたIPアドレスが、Bogonリストから外れたことを周知する“De-bogonize”の活動が行われています。IANAから/8の割り振りを受けると、多くのNOGに周知されるようになっています。

・De-Bogonising New Address Blocks
http://www.ris.ripe.net/debogon/index.shtml

- LACNIC
IPアドレスをレジストリの製品と捉え、経路の到達性という意味でよりよい品質で提供するための活動が行われています。そのために割り振りの前にテストプロセスが設けられています。

- 日本における取り組み
NTTコミュニケーションズ株式会社の吉田友哉氏による発表が行われました。JPIRRのfltr-unallocatedオブジェクトを使ったオペレーターへの通知方法紹介の後、Bogonフィルタを正しく利用しないことで著名なWebページにアクセスできなくなった事例の紹介や、到達性の確認実験「reachability test」の結果が報告されました。他に、オペレーター同士の連絡手段として、JANOGのコミュニティが紹介されるなどしました。

- Team Cymruの取り組み
インターネットにおける情報セキュリティに関して、調査や分析などを行っている非営利団体Team Cymruによるプレゼンです。Team CymruではBogonリストに関する普及啓発や、最新情報の提供を行っています。Bogonリストを使ったフィルタリングの是非から、Bogonリストを使うにあたって陥りやすい問題についての紹介が行われました。Team CyrmuのBogonに関するコンテンツは次のWebページで閲覧できます。

・The Bogon Reference
http://www.team-cymru.org/Services/Bogons/

RQAの活動は、上記のようにRIRでも取り組まれていますが、割り振ったIPアドレスの到達性を、IPアドレスのレジストリがどこまで保証すべきかという点について、共通の指標があるわけではありません。IPv4の在庫が枯渇しIPv6の普及が本格化した場合、IPアドレスのレジストリは、IPアドレスの管理業務においてどのような役割を担っていくべきなのか、という点について考えると、RQAはインターネット経路制御のセキュリティ等と同様に、重要な事項になってくるかもしれません。

◇　◇　◇

2011年に入ってから、IPv4アドレスのIANA在庫が枯渇し、RIRの在庫枯渇も近づいてきました。今後はIPv6の導入が本格化し、IPv4とIPv6の共存の際に起こる問題解決に向けた取り組みが行われていくことが考えられます。一方で、逆引きゾーンへのDNSSECの導入や、IPv6の経路制御への対応など、話題の多い年になりそうです。

(JPNIC 技術部／インターネット推進部 木村泰司)

APCERT年次総会および関連会合開催報告

◆ はじめに

2011年3月22日(火)から25日(金)にかけて、APCERT年次総会および関連会合が開催されました。APCERT年次総会は、アジア太平洋の各経済地域における最近のインターネットセキュリティ動向、インシデント対応の事例、調査・研究活動などを共有することを目的に毎年開催されています。今年は韓国のKrCERT/CC (http://www.krcert.or.kr/english_www/)がホストチームとなり韓国済州島にて開催されました。

● 参加者による記念撮影の様子(APCERTのWebサイトより引用)

東北地方太平洋沖地震発生から約10日後の開催であったことから、JPCERTコーディネーションセンター(以下、JPCERT/CC)からの参加に関しては、物理的な移動手段の確保が可能か等の懸念もあり、直前まで予断を許さない状況でしたが、結局、参加予定者全員が無事に出席することができました。

JPCERT/CCには地震直後から海外の情報セキュリティ関連機関からのお見舞いや各種協力の申し出が多数寄せられていたところですが、APCERT年次総会においても、ホストチームからの提案により、出席者全員が被災者に対して黙祷を捧げました。

◆ アジア太平洋地域のCSIRTコミュニティ「APCERT」について

APCERT(エイピーサート、Asia Pacific Computer Emergency Response Team)は、2003年12月に発足したアジア太平洋地域に所在するCSIRT※1からなるコミュニティです。APCERTでは、アジア太平洋地域におけるCSIRT間の協力関係の構築、インシデント対応時における連携の強化、円滑な情報共有、共同研究開発の促進、インターネットセキュリティの普及啓発活動、域内のCSIRT構築支援などの活動を行っています。

APCERTの活動の対象範囲は、APNICが定義するアジア太平洋地域の範囲と同様、56の国・経済地域です。12の国・経済地域から15チームが加盟して発足しましたが、加盟国・経済地域およびチーム数は年々増加しており、2011年3月末現在、18の国・経済地域から27チームが参加しています。

アジア太平洋地域内での活動はもちろん、国際的なCSIRTのコミュニティであるFIRST (Forum of Incident Response and Security Teams)や、ヨーロッパのCSIRTコミュニティであるTF-CSIRTなどと、グローバルな連携や他の地域の関連組織との連携を図りながら活動しています。

◆ APCERT年次総会および関連会合

今年の年次総会および関連会合は、以下のスケジュールの通り実施されました。

- 2011年3月22日(火)
午前:APCERT戦略策定会議 (Strategic Planning Meeting)
午後:APCERT運営委員会(Steering Committee)

- 2011年3月23日(水)
午前:APCERT年次総会 (Annual General Meeting)
午後:APCERTカンファレンス(限定公開の講演会)

- 2011年3月24日(木)
終日:APCERTカンファレンス(一般公開の講演会)

- 2011年3月25日(金)
午前:Workshop(ワークショップ)

23日の年次総会には15の国・経済地域から19の加盟チームの代表者が出席し、活発な意見交換、情報交換が行われました。24日の一般公開の講演会には、韓国の情報セキュリティ関係者を中心に、全体で約100名が出席しました。

◆ 新ビジョンの共有

今回の年次総会では、JPCERT/CCからの提案を叩き台として討議を重ね、“APCERT will work to create a safe, clean and reliable cyber space in the Asia Pacific region through global collaboration”という組織運営の新ビジョンが採択されました。APCERTが今後目指していく方向性が、加盟チーム相互の連携構築に留まらず、アジア太平洋地域の情報セキュリティ向上への寄与にあることが、あらためて確認されたものです。この新ビジョンのもとで、今後は、新たに設置されることとなったワーキンググループによる活動や、他組織・他地域との連携強化、新規プロジェクトの実施等、さまざまな活動を実施することが確認されました。

◆ 運営委員会メンバー等の改選

APCERT年次総会にて運営委員会（Steering Committee）のメンバーの一部改選が行われ、JPCERT/CCが再選されました（任期は2013年3月まで）。また、APCERT議長チーム・副議長チームが改選され、それぞれJPCERT/CC、KrCERT/CCが選任されました（任期は2012年3月まで）。さらに、2003年2月のAPCERT発足時から担っている事務局についても、JPCERT/CCが継続して担っていくことが採択されました。JPCERT/CCは、任期中、APCERTの議長チームとしてさまざまな活動をリードすることとなりました。

◆ 情報セキュリティ動向

3月24日（木）のAPCERTカンファレンス（一般公開の講演会）にて発表された、注目すべき講演の概要をいくつか紹介します。

(1) “Cyber Risks and Collaborative Responses”（基調講演）

講演者：Mr. Greg RATTRAY, Senior Vice President of Security, BITS【米国】

米国の大手金融機関のCEOらによって設立されたThe Financial Services Roundtableのビジネス戦略・技術部門BITSに所属するGreg RATTRAY氏は、「インターネットはエコシステムである」という持論に基づき、サイバー攻撃が発生したらその都度対処するという受け身の姿勢ではなく、インターネット上の治安を積極的に維持する姿勢の重要性について言及しました。

既にこのような観点をもって、インターネットのエンドユーザーに直接働きかけてボットを駆除するプロジェクトがいくつかの国で実施されており、

- 日本のサイバークリーンセンター（CCC、https://www.ccc.go.jp/index.html）
- オーストラリアのAustralian Internet Security Initiative（AISI、http://www.acma.gov.au/WEB/STANDARD..PC/pc=PC_310317）
- 韓国のQuarantine Programs 2010
- ドイツのAnti-Botnet-Beratungszentrum（https://www.botfrei.de/en/index.html）
- フィンランドのWalled Garden

等の取り組みが紹介されました。

CSIRTコミュニティの外にいる同氏の立場から見たCSIRTの強みとは、「高い技術力」「信頼を重んじる文化」「技術面での密な連携」であり、一方弱みとは「技術への過度な依存」「目先のインシデント対応に終始」「コミュニティの外から学ぶ意識の低さ」「パートナー組織に対する用心深さ」であると言及しました。

(2) “The Response of 3.4 DDoS Attack”

講演者：Mr. Jay SEO 韓国インターネット振興院（KISA、Korea Information Security Agency）ハッキングレスポンスチーム【韓国】

韓国では、2011年3月4日に同国内の政府系サイトやポータルサイト等を対象としたDDoS攻撃が発生しました。これは世界各地に分散配置された攻撃指令サーバ（72ヶ国に748ヶ所）を用いた大規模な攻撃で、発表者の所属するKISAも攻撃対象の一つでした。韓国では、2009年夏にもDDoS攻撃が発生し、インターネットアクセス障害が起きましたが、今回起きたDDoS攻撃によるアクセス障害は限定的であるとして、その理由を二つ挙げました。

一つ目は、2009年夏のインシデントの反省から導入した「DDoS Shelter」の効果です。「DDoS Shelter」は、DNSレコードを操作し、攻撃トラフィックをあらかじめ用意したシンクホール（Sinkhole）に振り向けるシステムです。このシステムの導入によって、遠隔操作で悪用できる状態のままインターネットに接続しているゾンビパソコンから、サーバへの攻撃トラフィックを減らすことができたとの見方を示しました。

二つ目は、DDoS攻撃が確認された日から数日以内に、インターネットをはじめとするさまざまなメディアを活用し、国民に駆除ツールのインストールを呼び掛けたことの効果です。

なお、ゾンビパソコンの感染ルートについては、韓国のネットユーザーに人気のP2Pツールのダウンロード先に置かれたファイルがマルウェアに換わっており、利用者が知らずにツールをインストールした事例等が報告されました。

(3) “2010 China Internet Security Report”

講演者：Mr. Yonglin ZHOU, Director, CNCERT/CC【中国】

2010年の中国のインターネットセキュリティ概況と2011年の展望について、CNCERT/CC（National Computer network Emergency Response technical Team/ Coordination Center of China）が発表しました。2010年の中国インターネットセキュリティの主な動向については、次の通りです。

- Webサイト改ざん：35,000件（2009年比 21.5%減）
- 政府のWebサイト改ざん：4,635件（2009年比 67.6%増）
- CNCERT/CCが確認・閉鎖したフィッシングサイト数：1,597（2009年比 33%増）
- マルウェア等を配布するサーバと攻撃指令サーバの停止依頼：5,384件
- CNCERT/CCが運営するChina National Vulnerability Database（CNVD）上で公表された脆弱性情報：3,447件
- マルウェアに感染した携帯電話（Symbian OS）数：800万台

また、2011年における中国でのサイバー攻撃の傾向として予想されるのは、攻撃件数のさらなる増加とその手口の巧妙化、経済的利得を目的とした攻撃の増加等であるとの見解を示しました。

さらに、重点的に対応すべきは、市場が急速に拡大しているスマートフォンのセキュリティの確保であるとの見解を示しました。加えて、このような動きに対応すべく、CNCERT/CCは、モニタリングシステムの増強、マルウェア分析の強化、モバイル・マルウェアハンドリングの強化、国際協力の強化に取り組むとの方向性を示しました。

◆ 次回のAPCERT年次総会

次回のAPCERT年次総会は、2012年3月頃にインドネシアのバリ島にて開催されることが決定しました。ホストチームはインドネシアのId-SIRTII（http://idsirtii.or.id/）です。

◆ 最後に

2011年3月22日、APCERT運営委員会（Steering Committee）にて、JPCERT/CCはAPCERT加盟チーム間の共同プロジェクトとして、アフリカにおけるCSIRT構築支援を提案しました。先述のFIRSTのWebサイト内に、FIRST加盟チームの経済地域を示す地図がありますが（http://www.first.org/members/map/）、アフリカからのFIRST加盟チームはまだ少なく、そもそもCSIRT自体がほとんど構築されてないという実態があります。JPCERT/CCでは、2009年度からアフリカにおけるCSIRT構築のための現地研修を実施しておりますが、今後はAPCERTの加盟チームと連携しながら、アフリカに対しての支援を実施していきたいと考えております。

JPCERT/CCは、変化を続ける情報セキュリティ上の脅威や、複雑化するコンピュータセキュリティインシデントに対する対応調整機関として、国内外の関係組織と連携しながら着実に対処していきます。また、APCERT内の連携強化やアフリカのCSIRT構築支援等を通じて、世界のインターネット環境の安全性向上に貢献していきたいと考えております。関係各位のご指導並びにご協力を引き続きよろしくお願いいたします。

（JPCERTコーディネーションセンター 国際部 渉外担当 梅村香織）

※1 CSIRT（シーサート、Computer Security Incident Response Team）
コンピュータセキュリティインシデントの関連情報、脆弱性情報、攻撃予兆情報等を常に収集・分析し、インシデント対応を行い、また、関係者の対応に必要な情報を提供する組織です。企業等の組織内にサービスを提供するチームもあれば、JPCERT/CCや韓国のKrCERT/CCのように、国内のインターネットユーザー全体をサービス対象とするいわゆる「National CSIRT」と呼ばれるチームもあるように、その対象とする範囲はさまざまです。

第80回IETF報告

IPv6関連WG報告

2011年3月27日（日）から4月1日（金）まで、チェコのプラハにて第80回IETFミーティングが開催されました。東欧の古都であるプラハでの開催は2007年春に続き、2回目となります。会期中のプラハは日本より暖かかったため、帰国後、日本がかなり寒く感じられました。参加人数については、49ヶ国より1,229名（新規参加173名）と発表されています。国別の参加人数内訳では、従来は日本からの参加者は人数の多い順で、2番目であることが多かったのですが、今回の震災の影響と、年度をまたがるという事情もあってか、日本からの参加者は減少し、米国、中国、ドイツに続いて日本、フランスという順番でした。

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）のうち、「6man 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、会議開始直後の3月28日（月）の朝に開催されました。

議事録担当、アジェンダ確認等の後、6man WGで取り組み中である以下の文書のステータス報告がありました。

1. P2Pリンク上におけるIPv6プリフィクス長/127の利用
   → RFCエディタによる発行順番待ち（その後、RFC6164として発行済み）

2. RPL（低電力高損失ネットワーク用のIPv6ルーティングプロトコル）用の情報伝達オプション、RPL用経路制御ヘッダ
   → Proposed Standard（標準化への提唱）に向け、IESG（Internet Engineering Steering Group）に送付

3. IPv6ノードの要求仕様改版、トンネルにおけるECMPとリンクアグリゲーションでのIPv6フローラベルの利用
   → WGラストコール終了

4. IPv6フローラベル仕様、IPv6フローラベル仕様更新理由
   → WGラストコール中（現在は終了）

また、今回議論されたアジェンダの中から、いくつかのトピックについてご紹介します。

1. フローラベル仕様の更改について
   draft-ietf-6man-flow-3697bis
   draft-ietf-6man-flow-update
   draft-ietf-6man-flow-ecmp

IPv6の特徴の一つとされているフローラベルの利用について、現在の仕様であるRFC3697を改版し、より使いやすいようにしようという提案です。IPv6トンネルを利用してECMP（Equal-Cost Multi-Path routing）やLAG（Link AGgregation）を実施する場合の、フローラベルフィールド利用方法も併せて提案しています。ドラフト中の文言の見直し、およびラストコールコメントを反映して改版をすることになりました。

2. IPv6拡張ヘッダの統一フォーマットについて
   draft-ietf-6man-exthdr

議論が続いているIPv6拡張ヘッダの標準フォーマットを決めようという提案です（6年間も議論しているという紹介もありました）。前回からの差分として、文書としてはIPv6拡張ヘッダのフォーマットに関する記述のみに特化したこと、新しい拡張ヘッダを定義する際には、終点オプション（destination option）の利用を推奨し、そうでない場合には明確な理由を必要とするという規定を加えたとの説明がありました。これは、新しい拡張ヘッダの追加は既存実装へのインパクト（特に性能面）が大きいという意見があったため、この文書は新しい拡張ヘッダ定義の追加を推奨するものではなく、既存の拡張ヘッダの枠組み内で新規機能の追加を勧めるためです。特にコメントはなく、WGラストコールを実施することとなりました。

3. RFC3484 IPv6デフォルトアドレス選択の更新について
   draft-ietf-6man-rfc3484-revise
   draft-ietf-6man-addr-select-opt

IPv6ノード、および、通信相手が複数のアドレスを持つ場合に、通信に使うアドレスペアを選択する仕様であるRFC3484に関する改版提案です。前回の議論を受けた改版の後、ULA（ユニークローカルIPv6アドレス）とプライバシー拡張の扱いが残課題となっているとの説明があり、この2点が議論になりました。プライバシー拡張を制御しようとする場合にはセキュリティに十分気をつける必要があることや、ULAのプライオリティを制御する必要性などについてのコメントがありました。コメントを反映後、WGラストコールを実施することになりました。

4. IPv6ノードの要求仕様 RFC4294の改版について
   draft-ietf-6man-node-req-bis

IPv6ノードが持つべき機能（実装が必要な機能）を定義した仕様であるRFC4294の改版です。WGラストコールを受けて修正した点の確認、MLD（Multicast Listener Discovery）に関して追加した部分に対する意見照会がありました。RFC化された文書のみ取り込むことにしていますが、現在取り組んでいるドラフトなどをどこまで取り込むかの議論がありました。しかし、ドラフトまで取り込むときりがないと判断され、現在RFC化された文書のみを取り込み、現時点で次のステップ（IESG送付、IETFラストコール）に進めることとなりました。

5. IPv6ステートレスアドレス自動設定におけるプライバシー拡張機能の管理について
   draft-gont-6man-managing-privacy-extensions

提案者が不在で、急きょ、代理人（Tim Chown氏）によるプレゼンテーションが実施されました。現在、IPv6ステートレスアドレス自動設定（SLAAC）によりノードが自動生成するアドレスがまちまち（EUI64ベース、プライバシー拡張ベース、ランダム、その他）なため、それを制御する方式についての提案です。ルータ広告（RA）を利用した制御を想定しています。コメントとして、プライバシー等のセキュリティに関連する制御を実施するのに、RAは完全には信用できないので問題であるという点や、SLACCのみの変更では不十分であること、問題の本質はどこにあるのか検討する必要があること等が挙げられました。

前回の北京では、ミーティング時間に対して議題が非常に多く、十分に議論しきれなかったのですが、今回は議題の数が少なく、予定時間よりかなり早くWGが終了しました。

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

□ 第80回 IETF 6man WGのアジェンダ
http://www.ietf.org/proceedings/80/agenda/6man.html

● 会場となったHilton Prague（ホテルの公式Webサイトより引用）

◆ v6ops WG（IPv6 Operations WG）

v6opsは、IPv6に関するオペレーション技術、および、共存・移行技術に関して議論するWGです。今回は、2011年3月31日（木）に、朝一と最終コマの2コマにて議論が行われました。

今回は、合計19件という非常に数多くの提案が挙がっていました。まず、ミーティングの冒頭でチェアより、v6ops WGのミーティングで発表時間を割り当てる議題の決め方に関する提案がありました。このところv6ops WGには非常に提案が多く、前回もコンセンサス確認をミーティング内でなく、事後にオンラインで実施する等で効率化を図り、多くの議題を扱えるようチェアが工夫をしていました。

しかし、それだけでは対処するのが困難な量の提案が継続的に挙がっているため、

- 基本的に、WG文書の議論に時間を優先的に割り当てる。
- 新規提案は、まずMLで議論し、参加者の興味度合いを確認。ミーティングの際、どの提案をプレゼンテーションしてもらうかは、議論状況によってチェアが決める。

ことで、取り扱う提案を選別し、議論時間を確保しようという提案です。賛成が多数であったため、次回からはこのポリシーで運営されると思われます。

今回議論された、いくつかのトピックについて、簡単に紹介します。

1. IPv6利用時に発生する通信問題について

今回、ミーティングの最初の時間に、'IPv6 Brokenness'に関係する項目が連続して発表され、議論も行われました。'IPv6 Brokenness'とは、IPv6を導入した際に発生する通信障害全般を指し、例えば、IPv6/IPv4デュアルスタック環境でIPv6接続性に問題があった場合に、IPv4にフォールバックするのに時間がかかる、という問題等がこれにあたります。

（1）IPv6接続性に問題がある際のホストの動作

IPv6からIPv4にフォールバックするのにかかる時間や、不正RAの影響、IPv6 Brokennessに対する解としての、Happy Eyeballs機構の有効性について報告がありました。

（2）Happy Eyeballsの実装レポート

複数のTCPセッションを同時にスタートし、最初に通信できたセッションを利用することでフォールバックを回避する機構である、Happy Eyeballsの実装レポートです。ドラフトで定義されている機構の問題点、改善提案が実施されました。

（3）デュアルスタックサービスの性能に関する実験結果

デュアルスタックWebサーバに対するユーザーアクセス統計の紹介がありました。現状、IPv6による接続性の品質はIPv4の品質に劣ることや、6to4等のトンネルからの接続失敗が多いこと、デュアルスタックにした場合に、アクセスができなくなるユーザーが存在すること等が報告されました。

（4）Happy Eyeballs:デュアルスタックホストにおいて通信を成功させるために
draft-wing-v6ops-happy-eyeballs-ipv6

Happy Eyeballsの仕様について、議論されました。前回からのアップデートとして、SRCレコードの扱いに関する記述の追加、複数インタフェース対応等を追記したこと、より多くの実装例とAPIの必要性などについて報告がありました。会場から、複数セッションを同時に張る場合のサーバ側の負荷や、TCP RSTの返答が増えることの影響、TCPセッションの数を極力少なくするための、キャッシュをはじめとした機構の必要性が意見として挙げられました。

2. NAT64アプリケーション評価について
   draft-tan-v6ops-nat64-experiences

NAT64のアプリケーションに対する影響評価の報告がありました。評価の対象はBehave WGで標準化の進んでいるNAT64（ietf-behave-v6v4-xlate-stateful）ですが、現状、実装が存在しないため、同等の動きをすると思われるNAT-PTデバイスにて多くのアプリケーションの動作を検証、問題点を整理しています。会場からのコメントとして、このような評価は重要であり引き続き実施してほしい、評価だけでなく、発見された問題点を吟味し、必要ならば解決することが重要である、NAT44との違いはどこにあるかの検討が必要である、等が挙げられています。

3. World IPv6 Day参加招集（World IPv6 Day Call to Arms）について
   draft-chown-v6ops-call-to-arms

2011年6月8日にWorld IPv6 Day※として、サービスのIPv6対応を実施しようという呼びかけが世界的に行われています。この呼びかけをさらに広めること、また、IPv6を導入した場合に発生する可能性のある問題、およびWorld IPv6 Day実施にあたって情報収集の必要性を指摘することを目的とした発表が行われました。会場からは、Webサービス提供者からのユーザーの接続性に問題が発生すると困るといった意見や、6to4は使わないようにすべき、問題が発生したという情報が収集できるのか、といったコメントが出されました。実際に、IPv6導入時の問題を検証することは重要であることは多くの人が同意するものの、現在のインターネットサービスへの影響が計り知れないことによる懸念の声も多く、World IPv6 Dayについては今後とも注視していく必要がありそうです。

4. 6to4に関する議論について

IPv6移行プロトコルとして定義されている、6to4について議論がありました。6to4は多くの実装が存在し、IPv6の接続として広く利用されていますが、品質が保証されない、パケット盗聴などのセキュリティ問題が起こりやすい、といった問題が指摘されています。IPv6をサービスとして普及させていくために、今後6to4をどうしていくべきかについて、次の3件の提案が実施されています。

(1) 6to4を利用する際のガイドライン
draft-carpenter-v6ops-6to4-teredo-advisory

6to4を利用する場合の運用、実装に対するガイドラインについての提案がありました。6to4のリレールータをしっかり管理することの必要性や、OS等で6to4を実装する場合の注意点(6to4の使用優先度をRFC3484に従うようにすべき等)について述べています。

(2) プロバイダー管理の6to4
draft-kuarsingh-v6ops-6to4-provider-managed-tunnel

NAT66と組み合わせることで、6to4の実装をそのまま利用し、プロバイダーが管理する6to4を実現する提案です。CGN(Carrier Grade NAT)と組み合わせることも想定しています。

(3) 6to4を「歴史的」ステータスに変更する提案
draft-troan-v6ops-6to4-to-historic

通信品質等、多くの問題が指摘されている6to4ですが、プロトコルとしての6to4を「歴史的」ステータスにし、利用をやめようという提案です。6to4自体の定義であるRFC3056と、6to4用のエニーキャストを定義しているRFC3068のステータスを変更することが提案されています。

ミーティングでは上記3件のプレゼンテーション終了後、6to4をどうしていくかの議論があり、結果として、(1)、(3)をWGとして継続的に議論していくことになりました。(3)がWGアイテムとして採択されたことにより、将来的に、6to4は利用されなくなると思われます。

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

□ 第80回 IETF v6ops WGのアジェンダ
http://www.ietf.org/proceedings/80/agenda/v6ops.html

(NTT情報流通プラットフォーム研究所 藤崎智宏)

※ World IPv6 Day
http://www.isoc.org/worldipv6day/

セキュリティ関連WG報告 ～TLS WG、KRB WG、暗号アルゴリズムの危殆化対応の動向について～

第80回IETFは、チェコ共和国のプラハにて、2011年3月27日から4月1日の期間に開催されました。所属組織によっては年度末から年度初めにまたがっていたため、日本からの参加者数にも影響があり、いつもより少なくなっていました。

IETFでは、インターネットに関するさまざまな議論が行われ、情報セキュリティに関する議論も行われます。また、IETFにはセキュリティ関連WGが15WG存在しています。今回のIETF会合では、15WGのうち11WGが開催され、さらに期間中にBoF (Birds of a Feather)として開催されたPLAZMA (The PoLicy Augmented S/Mime)があり、12のWG/BoFがスロットを取り、16セッションが開催されました。

セキュリティ関連のWGが扱う領域および範囲は多岐にわたりますが、今回もこれまで毎回お伝えしている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、TLS WG (Transport Layer Security WG)と、KRB WG (Kerberos WG)の動向を報告します。また、前回の北京で開催されたIETFから今回のIETF会合までに発行された、暗号アルゴリズムの危殆化対応※1(暗号アルゴリズムの世代交代)に関するRFCを本文の最後にまとめましたので、こちらもご参考になさってください。

● 第80回IETFのWebサイト。Twitterによる情報提供も行われています。(IETFのWebサイトより引用)

◆ 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※2の検討を行うWGです。今回のこのミーティングは、2011年3月30日の午後3時10分から1時間程度開催されました。参加者は、60人程度でした。

今回のミーティングでは、次に示すトピックスについて議論を行いました。

1) DTLS 1.2 Update (DTLS 1.2のアップデートについて)
2) Charter Revision (Charterの改正について)
3) TLS Next Protocol Negotiation (TLSの"Next Protocol Negotiation"について)
4) AES-CCM Cipher Suites (AES-CCMを利用したCipher suitesについて)
5) TLS Using EAP Authentication (EAP認証を用いたTLSについて)
6) A TLS Renegotiation coverage update (TLS Renegotiationの対処状況について)
7) Adding Multiple TLS Certificate Status Extension requests (OCSPライクな複数の証明書ステータスをサポートするための拡張について)

上記のトピックスから、今後のTLS WGの方針に関係する2)のCharter Revisionと、2009年11月に発見されたTLS Renegotiationに対するSSL/TLSサーバの対応具合を報告した6)のA TLS Renegotiation coverage updateについて、詳しく報告したいと思います。

2) Charter Revision

長年続いているTLS WGのCharterについて、現状を踏まえて見直すことになりました。大きく分けて、TLSプロトコル自体のメンテナンスを目標とした項目と、それらに付随するドキュメントの発行を目標とした項目に見直されました。メンテナンス対象として挙がっていたものとしては、TLS1.2を規定しているRFC5246や、DTLSを規定するRFC4347bisが含まれています。また、メンテナンス以外の項目としては、TLSプロトコルの利用に関する推奨や、新規Cipher suitesが含まれています。ミーティングでは概要について議論され、その結果を踏まえてChairからTLS WGのメーリングリストに、更新版のCharterが投稿されることになりました。

6) A TLS Renegotiation coverage update

この報告は、2009年11月に発見されたTLS Renegotiationに関する脆弱性対応について、対応状況の調査結果を報告することが趣旨です。しかし、Renegotiationに関する脆弱性だけではなく、SSL2.0や暗号強度的に弱い暗号アルゴリズムを利用したSSL通信についても報告していましたので、概要を取り上げたいと思います。

【サマリー】
- 2009年11月に発見されたRenegotiation脆弱性について、約50%のSSL/TLSサーバしか対応済みの実装になっていない。
- 利用の推奨がされていないSSL2.0プロトコルについて、約63%のSSL/TLSサーバにおいてサポートされてしまっている。
- 比較的攻撃可能とされている暗号強度的に弱い暗号アルゴリズムについて、約64%のSSL/TLSサーバにおいて利用可能になっている。

この報告を受けて感じたことは、Webサービスの利用者に関する秘密情報(個人情報やクレジットカード番号など)を秘匿するために利用されているSSL/TLS通信ですが、多くのサーバでの運用が不適切であり、「暗号通信を利用しているから安全である」とサービス提供者が言っているからといって、それだけでは安心できないということです。一口にSSL/TLS通信と言っても、サーバの設定などによって、その安全性は異なってしまうからです。しかしながら、サービス利用者側から見て、自分がどのような状況(接続しているCipher suiteやプロトコルバージョンなど)で暗号通信を行っているのかについては、サーバとWebブラウザなどのアプリケーションの間で決定され、ユーザーが普段それを意識することはありません。そのため、サービス提供者が確認して、安全性に対するお墨付きを与えるような仕組みが必要だと考えました。

この発表資料は、次の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。
http://www.ietf.org/proceedings/80/slides/tls-5.pdf

なお、IETFにおけるSSL2.0に関する動向として、RFC6176 "Prohibiting Secure Sockets Layer (SSL) Version 2.0"が、前回の北京での会合から今回のIETF会合の期間で発行されました。利用を推奨していないプロトコルを、世界に向けてRFCという適切な形で公開することは、プロトコル利用者として非常に有益であると思います。

次の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。
http://tools.ietf.org/rfc/rfc6176.txt

□ TLS WG
http://datatracker.ietf.org/wg/tls/charter/

□ 第80回IETF TLS WGのアジェンダ
http://www.ietf.org/proceedings/80/agenda/tls.txt

◆ KRB WG (Kerberos WG)

KRB WGは、マサチューセッツ工科大学(MIT)が考案した認証方式の一つである、Kerberosプロトコルに関する新規仕様や機能拡張について、検討を行うWGです。このミーティングは、最終日である

2011年3月29日の午後1時から2時間程度開催されました。なお、参加者は、30人程度でした。

今回のIETFより、KRB WGのChairとしてSam Hartman氏が加わりました。彼の参加により、今後のKRB WGでのRFC化が促進されると予想されます。

ミーティングの構成として、以下のような議題で進行されました。

1) ドキュメントステータスおよび確認
2) 技術的な議論
3) Rechartering

この三つの中から、二つのトピックスについて報告します。

1) ドキュメントステータスおよび確認

8本のドキュメントに関するドキュメントについて報告がありましたが、もう少しでRFCとして発行される三つのドキュメントを次に紹介します。

- Additional Kerberos Naming Constraints(RFC to-be 6111)
- Anonymity Support for Kerberos(RFC to-be 6112)
- A Generalized Framework for Kerberos Pre-Authentication (RFC to-be 6113)

また、危殆化した暗号アルゴリズムであるDESについて、Kerberosプロトコルでのサポートを停止するための仕様である"Deprecate DES support for Kerberos"は、前回の会合でWGLC (Working Group Last Call)のステータスでしたが、現在、Expireしているとのことでした。暗号の危殆化(暗号の世代交代)の観点から重要なものであるため、早くRFC化を行ってもらいたいと考えています。

3) Rechartering

WGとして議論すべき項目などが増えてきたため、Charterを見直すことになりました。今回のCharterで新規に追加されることになりそうな項目として、次のようなものがあります。

- Kerberos v5における新しいenc-typeに関する検討
- Authorization-related informationに関するGeneralized Principal Authorization Data (PAD)構造の仕様化

新しいenc-typeに関する検討については、2010年3月に開催された会合での、Camellia-CCMに代表される新しい暗号をKerberos v5で利用できるようにする活動から、今回のRecharteringの議題になりました。なお、Charterになる際には、Camelliaだけに限定せずに他の暗号アルゴリズムも検討対象になりましたので、AESなどの他の共通鍵暗号アルゴリズムのInternet-Draftが投稿される可能性もあります。

□ KRB WG
http://datatracker.ietf.org/wg/krb-wg/charter/

□ 第80回IETF KRB WGのアジェンダ
http://www.ietf.org/proceedings/80/agenda/krb-wg.txt

◆ IETFにおける暗号アルゴリズムの危殆化対応に関するRFCのまとめ

前回の北京会合から今回のIETF会合までの期間に、暗号アルゴリズムの危殆化を踏まえたRFCがいくつか発行されていましたので、どのようなドキュメントが公開されたのか、情報を整理したいと思います。暗号アルゴリズムの危殆化対応を行う必要がある際には、参考にしていただけたらと思います。

・RFC6149 MD2 to Historic Status
http://tools.ietf.org/rfc/rfc6149.txt

・RFC6150 MD4 to Historic Status
http://tools.ietf.org/rfc/rfc6150.txt

・RFC6151 Updated Security Considerations for the MD5 Message-Digest
and the HMAC-MD5 Algorithms
http://tools.ietf.org/rfc/rfc6151.txt

・RFC6176 Prohibiting Secure Sockets Layer (SSL) Version 2.0
http://tools.ietf.org/rfc/rfc6176.txt

・RFC6194 Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms
http://tools.ietf.org/rfc/rfc6194.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(きたい)化
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

※2 Cipher suite
SSL/TLSプロトコルで使用される、認証、暗号化、メッセージ認証符号のそれぞれのアルゴリズムの組み合わせです。