# 東日本大震災における インターネットが果たした役割と今後の期待

財団法人インターネット協会　副理事長／シスコシステムズ合同会社　木下 剛

この度の震災で被災された全ての皆様に心よりお見舞を申し上げたい。

2011年3月11日に発生した東日本大震災は、東日本の広域に渡って甚大な被害をもたらした。通信インフラも多大なる影響を受けたが、震災発生直後から目を見張るスピードで通信インフラの復旧へ取り組み、特に移動体通信の電話やワンセグは被災者の通信手段として大きな威力が発揮された。同時に、広域に及ぶ被災地域での救援活動、災害支援活動を通じて、インターネットは、行政、医療、被災者、救援者など複数の機関／団体の連携を支えるオープンで自律分散型の情報通信基盤として、極めて高い有効性が示された。

今回の震災におけるインターネットは、被災情報、安否情報確認、支援ニーズなどリアルタイムに変化する被災地域の情報を、必要とする多数に、同時に伝達できる性質が役立ち、加えて被災地からの画像や映像といった信頼できる災害後の情報は、的確な判断を行う上で非常に有用であることが明らかになった。

このような経験から震災直後の今年4月に総務省では、「大規模災害等緊急事態における通信確保の在り方に関する検討会」を発足した際に「大規模災害時の通信インフラの確保」に加えて、今後の「インターネット利用の在り方」を検討するWGが設けられたことは注目される。また、国外に目を向けてみると、まだ記憶に新しいハイチや中国四川省における震災時の経験や、米国ハリケーンカトリーナ、インドネシア津波など大規模災害時におけるインターネットが果たした役割を踏まえ将来に備える取り組みが見られる。こうした国内外で災害支援インフラとしてのインターネット利用に向けて、今回の日本の経験を踏まえた災害発生時の救援、復旧・復興段階における迅速かつ効果的なインターネット利用環境を整備していく取り組みが期待される。

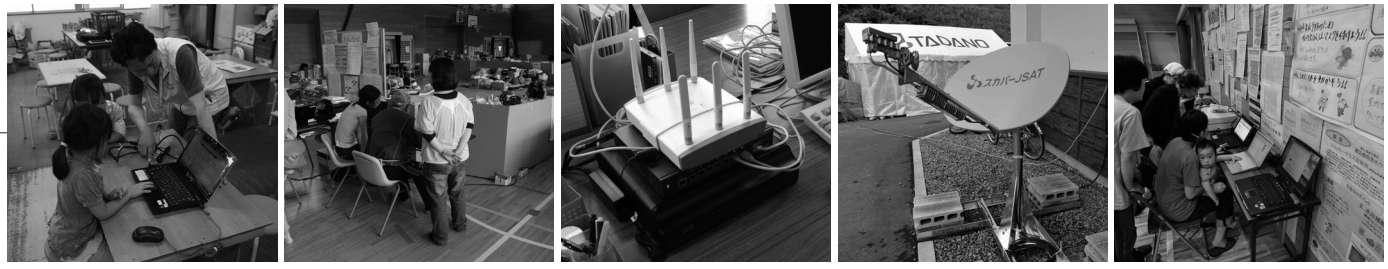
## 通信インフラの被害とインターネットが果たした役割

今回の東日本大震災では、震災直後に音声通信の利用者が急増し、総務省の調査によると、固定電話で最大80%～90%、携帯電話では最大70%～95%の発信規制が実施された。このように電話がつながりにくい一方、携帯電話におけるパケット通信では規制が最大でも30%程度で、規制期間も音声通話の規制期間にくらべると一時的であった。そのため、メールやTwitter、mixiなどのソーシャルメディアなども安否確認に利用された。また、震災後、行政機関によるTwitterなどソーシャルメディアでの情報発信が活発に行われたほか、自治体から提供された避難者名簿などの情報をウェブ上で一元的に検索できるサービスなど、さまざまな災害支援ウェブサービスが有志によって提供された。一方で、震災直後、大量の情報がやり取りされる中で、ソーシャルメディアを利用したデマなどが広がる問題も起こった。

この大規模な被災によって、多くの避難所がインターネットへの接続性を失い、情報共有の機会を奪われた。また、避難所として使用されている建物にもともとインターネットへの接続性がない場所もあった。このような避難所では支援ニーズを発信できないため、適切かつ迅速な支援を受けられないという支援格差が発生していた。このような状況に対する支援の一例として、有志によるボランティアプロジェクトである「震災復興インターネットプロジェクト」では、衛星、無線などを使用して、沿岸部で孤立した避難所などへ仮設インターネット接続を提供し、被災者の支援情報へのアクセスや、被災地の情報発信ができるようサポートが行われた。復旧段階において、被災地域における通信インフラの回復状況や避難所の開設、移動、拡張や縮小などに応じて、柔軟かつ機動的にインターネット環境を提供する必要性がある。このようなニーズに対して、衛星や無線を組み合わせたインターネット接続が有効であることが証明された。

## 経験を踏まえた総務省の取り組み

このように今回の震災後の通信インフラとしてインターネットは広く利用され、非常に重要な役割を果たした。総務省が4月から開催している「大規模災害等緊急事態における通信確保の在り方に関する検討会」において、この7月に「大規模災害等緊急事態に置ける通信確保の在り方」に




震災支援の様子

ついて中間とりまとめ(案)が公表された。この中で、通信インフラおよびインターネットがすでに社会インフラであり、今回の震災時には市民の安否確認や行政機能の維持に必要な通信手段を提供する重要な基盤としての役割を果たしたとしている。さらに、今後のインターネット利用の在り方については、①インターネット接続機能の確保、②インターネットの効果的活用、③クラウドサービスの活用、④災害発生時に備えた通信事業者の協力体制の構築の4つの分野に関して、インターネット接続機能の復旧の在り方や、情報リテラシーの涵養、関連機関との連携などの課題を提示し、政府や通信事業者などがこれから取り組むべき事項について示されている。

### 海外での取り組み

同様な災害を経験し、ICTインフラの復旧・復興利用の経験から、将来の災害時に復旧支援を行うために、平時から準備する取り組みを始めている国が日本以外にも見られる。

2004年にスマトラ島沖で起こった大地震の津波によって大きな被害を受けたインドネシアでは、国内のISPの団体であるAPJII (Asosiasi Penyelenggara Jasa Internet Indonesia) が被災地でWi-Fiによる通信の提供や、現地にあった2つのISPの復興を支援した。その後、活動を引き継ぎICTによる災害支援を行うAirputih財団を設立し、2004年の津波のほかにも国内の災害の際に被災地で同じような支援活動をすでに8回以上行っている。Airputih財団ではいつでも出動できるように機材を常に用意しており、インドネシア政府の国家災害管理局とも緊密な関係を維持し、災害後すぐに連携を取って必要な活動ができるように備えている。

同様に、2005年に米国南東部を襲い甚大な被害をもたらしたハリケーンカトリーナや、2010年に隣国ハイチで起こった地震での災害支援活動を行ってきた米国では、米国国務省国際通信情報政策諮問委員会国際災害対応小委員会が、9.11とこれらの災害時の支援活動ケーススタディを行い、6月末に国際的な災害支援について提言案をまとめている。この中では、国際的な災害において米国内の公的および私的機関、NGOが行うICT支援への米国政府の援助を強化するために、①現地のネットワークや被害などの情報、②政府やISP関係者などの窓口、③これら関係者との交流・協調の3つを国際的な災害におけるICT支援に共通な課題として上げている。この課題を解決するために、米国政府が事前に準備するべき事柄として、13か条の提案をまとめている。

### 課題と今後の展望

近年インターネットは、情報インフラとして水道や電気と同じレベルの社会基盤であると位置づけられるが、災害時に社会基盤としての貢献と責任を果たすためには、他の社会基盤と同様に災害に対する備えが必要である。今回の震災では、以下のような課題が明らかになった。まず、災害発生時に速やかに関係機関が連携してインターネット接続性を提供するための、人的支援を含めた総合的な非常時における情報インフラ利用戦略と、それに基づいた事前準備の必要性である。次に、一般市民への情報リテラシーの育成である。今後の災害発生時にインターネットを社会基盤として利用できる環境を提供してゆくためには、これらの課題を勘案し、円滑かつ効果的な利用環境を提供するフレームワーク作りが望まれる。インドネシアやアメリカの例のように国際的にも震災を経験した国々において、関連する機関／団体が平時から連携を取って非常時におけるインターネット利用を準備する取り組みが始まっている。日本からも率先して、国際的に協調し、災害に備えたあるべき連携体制の実現を目指して取り組んでゆくことが期待される。

■参考

総務省 大規模災害等緊急事態における通信確保の在り方に関する検討会
*http://www.soumu.go.jp/main_sosiki/kenkyu/saigai/index.html*

Airputih財団
*http://airputih.or.id*

# 急速に普及するスマートフォン ソーシャル連携や広告など広がる可能性

ケータイジャーナリスト　石川 温

スマートフォン市場が盛り上がりを見せている。2011年度末までに、NTTドコモは600万台、KDDIも400万台というスマートフォンの販売計画を見込んでいる。NTTドコモでは、2011年7月末までに200万台を突破。「最終的には今年度末には700万台達成もあり得るかも知れない」（NTTドコモ、山田隆司社長）と鼻息が荒い。今年の夏商戦では海外メーカーだけでなく、日本メーカーも本格的にスマートフォンを投入し始め、おサイフケータイ、ワンセグ、赤外線通信といった日本特有機能を搭載したモデルが相次いで登場し、ケータイからの機種変更も抵抗なく行えるようになったことが大きい。

昨今のスマートフォンは、高機能モデルでは画面サイズは4インチ以上で、チップセットも一昔のパソコンとほぼ同等レベルに達していると言っていい。アプリを追加することで、さまざまな機能が増えていく。もはやスマートフォンは電話機ではなく「手のひらに乗るパソコン」なのだ。

スマートフォン市場において、これまではアップル・iPhoneが一人勝ちを続けていたが、最近になって急成長してきたのがグーグルがプラットフォームを提供しているAndroidだ。各キャリア、メーカーが相次いで採用し、日本特有機能も載せられることから急激に増えている。世界的に見ても、すでに1億3500万台が出荷され、毎日約55万台が増え続けているのだという。

グーグルでは、「Mobile,First」（エリック・シュミット同社エグゼクティブチェアマン）として、スマートフォン向けプラットフォームの開発を重視している。パソコンはどんなに普及しても子供から年配者まですべての人が1台というのは考えにくい。しかし、ケータイであれば1人1台というのは現実味を帯びた世界だ。そのケータイがスマートフォンに置き換わっていくのは時間の問題だろう。

スマートフォンといえば、大きな画面のタッチパネル端末というのが一般的なイメージだ。しかし、シャープが発売した新製品では、ケータイのような折りたたみ型やスライド型にもかかわらず、中身はAndroidを搭載し、アプリやインターネットを楽しめる端末も登場している。「家電量販店でケータイに機種変更したはずが中身はスマートフォンと一緒だった」という世界がもう来ているのだ。予想以上にスマートフォンが急速に普及していく可能性は十分にある。

## 拓かれる新たな可能性

グーグルがAndroidプラットフォームに力を入れる背景には「リアルのインターネットをスマートフォンで実現させたい」という狙いがある。パソコンではなく、誰もが手にしているスマートフォンで、パソコンに匹敵するインターネットの利便性を提供したいというわけだ。現在、パソコン向けのサイトも、スマートフォンでそのままのデザインで閲覧できるが、スマートフォンであれば、新たな可能性も秘めている。

スマートフォンにはGPSやカメラが内蔵され、今後はNFCといった非接触ICチップなどが埋め込まれようとしている。これらのデバイスを活用することで、これまでのインターネットビジネスではできなかったサービスが実現しようとしている。グーグルはそのあたりを見据えており、アメリカではNFCを使った決済やクーポン配信サービスをスタートさせている。

「非接触ICを使った決済と言えば、日本ではおサイフケータイがあり、珍しいものではないかも知れない。しかし、世界ではまだこれからの市場だといえる」（グーグルでAndroidのグローバルパートナーシップディレクターを担当するジョン・ラーゲリン氏）。スマートフォンを使う際のアカウントで誰かを特定し、GPSで場所を把握、NFCで何を買ったのかを購入履歴がわかる。しかも、スマートフォンはケータイとは違い、オープンな世界で参入障壁はかなり低い。幅広いインターネットプレイヤーが参入し、スマートフォンでビジネスを成功させる素地は整っていると言えるだろう。

## ソーシャル連携

もうひとつ、スマートフォンを語る上で欠かせないのが、ソーシャルとの連携だ。カメラがあり、SNSでいつでもどこでも近況をつぶやくのにスマートフォンは適している。その流れを組んでか、最近ではアドレス帳にFacebookやTwitterなどの機能を融合させたスマートフォンも増えてきた。アドレス帳を開けば、友人が何をしているの

か、どこにいるのか、何を面白いと思っているのかがすぐに把握できるのだ。

ソニー・エリクソン製「Xpeira acro」では、友人が面白いと他人に共有した動画ファイルがまとめて閲覧できるようになっている。同社では「コミュニケーションエンターテイメント」を標榜し、商品開発を続けている。さまざまなサービスが登場してくる中、友達とのコミュニケーションこそが最も楽しいエンターテイメントとして位置づけているわけだ。

インターネットに向けてサービスを展開していく場合、ソーシャルにおける「友達に教えたい」という欲求を最大限に生かす必要がある。パソコン向けにおいてもバイラルマーケティングが注目されていたが、スマートフォンが普及し、リアルインターネットで24時間持ち歩く消費者が増えていく中、いかに「ユーザーが他人と共有したいか」という仕掛け作りを準備していく必要があると言える。

このユーザー動向を見て、キャリア側も動き始めている。KDDIはスマートフォン時代において、これまでのケータイ時代におけるEZwebといったポータルサイトに注力するのではなく、さまざまなSNSとの提携に注力する。世界で7億人のユーザーがいるFacebookを筆頭に、ゲームSNS「GREE」や、位置情報との組み合わせで人気の「コロプラ」、ユーザー同士が天気情報を投稿しあうウェザーニュース社「ソラテナ」などとパートナーになった。複数のSNSと提携して、ユーザーを回遊させつつ、キャリアとしては課金回収代行で稼ぐというビジネスモデルに転換しつつある。そのため、KDDIでは「auかんたん決済」という電話料金とともに回収できる仕組みを提供しつつ、オンライン上での支払いに便利な「WebMoney」を子会社化しようとし、楽天とは「Edy」で提携。リアルの世界の決済も強化しつつある。

また、スマートフォンの普及により、注目を浴びているのが広告だ。大画面により、動画などを組み合わせた広告を消費者にリーチさせることができる。さらに、GPSや個人認証を組み合わせることで、より深いターゲティングをした上でのプロモーションが可能となる。Facebookは、本名であり、自分の学歴や職歴、趣味など個人情報を幅広く登録しているのが特長だ。いまのところ、Facebookは位置情報を組み合わせたクーポン程度しか日本では展開していないが、将来的には位置情報と個人情報を組みあわせた広告モデルを投入することも考えられる。

手のひらにリアルインターネットが載り、ソーシャルと組み合わさることで、無限のビジネスチャンスが広がろうとしている。

### トラフィック問題

スマートフォンユーザーの急増に伴って、各キャリアが頭を痛めているのが「トラフィック」だ。スマートフォンの大画面化により、ウェブ閲覧やYouTubeといった動画視聴や撮影した静止画や動画を大量にアップするユーザーが続出、既存のネットワークだけでは、莫大なデータトラフィックを処理し切れなくなってきた。

そこで、各キャリアは「オフロード（回避）」として、無線LANスポットの活用に乗り出しつつある。

iPhoneを取り扱い始めて、いち早くオフロードの重要性に気がついたソフトバンクは、他社に先駆けて無線LANスポットを構築、無料化することで、ユーザーが使いやすいようにした。同社は3Gネットワーク回線が他社に比べると貧弱ということもあり、公衆無線LANスポットの拡充は重要なミッションとなっている。

一方、KDDIは、高速モバイル回線であるモバイルWiMAX網（KDDI傘下のUQコミュニケーションズ）を活用。同ネットワークに対応したスマートフォンを増やしつつある。また同時に、公衆無線LANスポットを2012年春までに全国に10万局設置する計画を明らかにした。

NTTドコモは、2010年末からサービスを提供している高速モバイル回線「Xi」（規格名：LTE）に対応したスマートフォンを2011年末から投入する予定。莫大に増えるとされるトラフィックをLTEでさばく考えであったが、予想以上にスマートフォンユーザーが増えていることから「公衆無線LANスポットを拡充させていく。他社に対応するため、無料化も検討している」（NTTドコモ・山田隆司社長）という。

キャリアもスマートフォンブームによって右往左往している状態と言えるだろう。

# 最新の脅威に備えるサイバーセキュリティ
# 整備が進むサイバーセキュリティ対策ガイドライン

IPv6普及・高度化推進協議会 セキュリティワーキンググループ / シスコシステムズ合同会社 西原 敏夫

近年、サイバーセキュリティを取り巻く環境が大きく変化している。ウィキリークスによる米国外交公電などの暴露や、大規模な個人情報漏えいとなったソニーに対するサイバー攻撃など、脅威の性質が変化し深刻化している。とりわけ、標的型攻撃（APT：Advanced Persistent Threat）と呼ばれる特定の企業・政府機関を対象とするサイバー攻撃が増加していることが、昨今の特徴としてあげられる。

このような昨今のサイバーセキュリティを取り巻く大きな環境変化へ対する取り組みの強化を計るべく、政府レベルでの動きも活発化している。米国では2011年5月に「Launching the U.S. International Strategy for Cyberspace（サイバースペースに関する国際戦略）」および「The Administration Unveils its Cybersecurity Legislative Proposal（サイバーセキュリティの法制に関する立案）」が発行された。日本においても2011年7月に経済産業省から「サイバーセキュリティと経済研究会報告書中間とりまとめ（案）」が出されたが、これらガイドラインでは、最新のサイバー攻撃手法の特徴・実例・対策などが明記されているため、是非、一度熟読されることをお奨めする。以下に簡単にサイバー攻撃の手法や対策について取り上げる。

### 進化するサイバー脅威、標的型攻撃

標的型攻撃は従来のように、マルウェアなど不特定多数の企業や個人に対し、何らかの方法で不正プログラムを配布し、システムの破壊、自己の技術力を誇示する愉快犯などの妨害行為とは一線を画している。例えば、2009年に猛威を奮った従来型の攻撃であるGumblar（ガンブラー）は、パソコンで使用している特定のアプリケーションに脆弱性が存在していれば、あるウェブサイトを閲覧するだけでウィルスに感染し、感染したパソコン内に記録されている情報に基づき、多くの企業のウェブサーバーを改ざんさせた。このように従来の攻撃が特定の情報を自動的に取得するのに対し、標的型攻撃では「個別に」「あらゆる」情報を奪取する点が、大きな相違点である。

標的型攻撃とは、まず、特定の組織・個人からの情報窃取およびそれらの弱体化を目的とし、高度な専門知識と莫大なリソースを有して、長期間、対象のシステムに潜伏し、さまざまな手法を駆使して、攻撃および情報窃取を繰り返すスパイ行為を主に行う攻撃のことである。侵入方法としては、ソーシャルエンジニアリングによるスピアフィッシングや、対象のITシステムで利用しているアプリケーションのセキュリティ上の脆弱性を突き、内部システムに侵入するなどがある。これらの手法を組み合わせて、攻撃対象システムの管理者権限などを奪取し、長期間、手動にてあらゆる情報を窃取し続けるという特徴を持っている。代表的な例としては、イランの原子力発電所の制御システムをターゲットにしたStuxnet（スタクスネット）や、Internet Explorerの脆弱性を利用し、グーグル社など30社以上の企業をターゲットにしたOperation Aurora（オペレーションオーロラ）などが挙げられる。Stuxnetウィルスに至っては、数年かけて開発を行わなければ作成できないほどのウィルスとも言われており、標的型攻撃がいかに長期的な計画のもとにスパイ攻撃・妨害攻撃を行っているかがわかる。

### 新たな攻撃手法

ソーシャルエンジニアリングとは、公共機関に携わる者、顧客、上司、退職者などになりすまし、メールや電話などで、パスワードなどの重要な情報を聞き出したり、盗聴や盗撮などで情報を盗み出したりする行為のことである。

昨今では、このソーシャルエンジニアリングが行われることが多い。例えば、対象相手に秘密裏に情報窃取するためのコードが埋めこまれている、「議事録」という名前の一般的と思える文書ファイルを添付したメールや、特定のサイトに誘導するURLが記述されたメールを送り、そのURLをクリックすることで情報窃取するプログラムが密かにダウンロードされるといった手法が行われる傾向が高い。この手法を、スピアフィッシング、またはスピア型攻撃と呼ぶ。

大規模攻撃のスパム全体量は減少している一方、スピア型攻撃が増加している

傾向にある。スピア型攻撃に利用される特異なマルウェア事例は、2011年6月に28万7298件発見されており、この数字はシスコが2011年3月に特定した10万5536件の2倍を超える件数になる。また、標的型攻撃であっても、不特定多数を狙う攻撃であっても、侵入手段として、このソーシャルエンジニアリングやスピアフィッシングを用いることが多く、情報漏えいなどを未然に防ぐには、これらの侵入手段に対策を講じる必要がある。

また、スピアフィッシングだけでなく、脆弱性を利用するケースや、またはその両方を利用するケースが多く、複雑化するサイバー脅威に対する対策方法を次に取り上げる。

### インターネット利用と脆弱性対策

最近の一例として、ソニーの個人情報流出事件が思い起こされる。ソニーの原因調査会見において、数千万件にも及ぶ情報流出は、既知の脆弱性対策を怠っていたことが原因だと説明されている。ほとんどの脆弱性は、ソフトウェアのバグ・仕様上の欠陥であるため、発見され次第、開発側から修正パッチなどが提供される。したがって、システムの安全性を確保するには、適時、修正パッチなどを適用することが重要となる。ソニーの例では、アプリケーションサーバーの脆弱性を突かれ、侵入を許すこととなり、それを契機に、外部と通信を行うプログラムをネットワーク内に導入され、そのプログラムを経由し、個人情報を管理しているデータベースへのアクセス権を奪取された。このようなことが起こらないためにも、既知の脆弱性に対する修正パッチが作成されれば、できる限り早急に対応すべきである。

では、その修正パッチが作成・配布されていない時点、いわゆるゼロデイのタイミングで、攻撃をされることに対応するには、どうすればよいだろうか。

従来の解決策としては、IPS（侵入防止システム）の導入が考えられるが、全ての不正な通信や、ゼロデイアタックなどを完全に阻止することはできない。なぜなら、IPSの制御方法はシグネチャと呼ばれる攻撃パターンのデータベースを参照することで、不正な通信パケットを制御する。つまり、未知の不正パケットが存在した時、そのためのシグネチャが作成され、IPSのデータベースに格納し、有効化されるまでの間IPSは、その不正パケットを制御することが出来ない。

### これからのセキュリティ対策

最近は、アクセスセキュリティーとIPSがあれば安心という時代ではなくなっている。シグネチャの作成・適用が追いつかないという理由だけではない。Web2.0に代表されるように、ウェブがプラットフォームのように利用され、1つのページの中には、複数のURLや閲覧者によって表示が変わる広告、動画が存在する。メールに添付される悪意のあるコードは、「.exe」のような理解しやすいプログラムではなく、「先ほどお見せした資料を添付します」という文章と共に添付されるPDFファイルに埋め込まれている。このようなネットワーク上の振る舞いは、IPSの守備範囲を超えている。

そこで、ウェブサイトやメールの送信元を、あらゆる情報を元にスコア別に判定し、その通信を制御するレピュテーション（評価）とよばれる技術が、最新のセキュリティ対策として注目されてきている。この技術を利用することにより、脆弱性対策が不完全なセキュリティホールや、ゼロデイ対策をとることができる。

ただし、誤検知の少ないレピュテーションを行うためには、例えば、送信元のIPアドレスがブラックリストに登録されているか、参照しているウェブサイトのドメインは最近取得したものかなど、多角的、かつ膨大な情報を必要とする。また、その情報を他の組織・個人と、早い段階で提供し合う環境も必要だと考えられる。一部のセキュリティベンダーは、すでにこのような環境を整え、サービスとして展開しているが、精度・安全性を今以上に高めていくには、公共機関・組織・個人が連携するフレームワークが有効であり、繋がりによって、スパイウェア、マルウェアを止め合うような仕組みが強化されていく必要性があるのではないかと考えられる。このような環境が整うことによって、最新のサイバー脅威への対策が確立されていくことが期待される。

# World IPv6 Day開催報告 日本からも多数参加、IPv6は次ステップへ

インターネット協会IPv6デプロイメント委員会／インテックシステム研究所　廣海緑里

ISOC（Internet Society）主催で2011年6月8日に実施されたWorld IPv6 Dayについて報告したい。

### World IPv6 Dayの意義と目的

World IPv6 Dayは、ISOC（Internet Society）を中心に、グーグル、ヤフー、フェイスブックなどの米大手ICT／サービス提供企業が一斉にある1日（24時間）の間、自社のウェブサイトのトップページをIPv6対応にし、各種影響を全世界的に探ってみる試みで、約450の組織が参加した。

すでにIPv6に対応済みでこの実験への意義に賛同した組織も約800あり、一斉にIPv6の挙動確認が実施された。グーグルなどの研究者から、移行技術の提供品質に関する問題やIPv6の実装開発上の問題が指摘されており、そうした問題の存在を明らかにすると共に問題点の解決策を検討、実施することが目的とされた。

IPv6によるアクセスの0.5％前後がそのような問題を含んだものであると報告されている。全世界のインターネットユーザの0.5％と考えると大きなコンテンツサイトでは見過ごせない問題となる。

今後、IPv6対応のウェブサイトが増え、普及期を迎える前に、直せる部分は直し、情報共有をしておく必要がある。

### 日本におけるWorld IPv6 Day

一方日本では、3月の震災によりインターネット関連企業の多くはこうしたイベントに多くの人員を投入して対応することは難しい状況となっていた。さらに、日本ではIPv4アドレス枯渇の進展に伴った各種の移行技術が展開されたハイブリッドなインターネットサービスが提供されているため、問題がより複雑となっており、世界での予測よりも多い影響数の見積りがされた。そのため、通信サービス提供者側からは「TCPリセットの増強体制構築」、「AAAAフィルタ導入」、「IPv4優先利用」の推進体制が取られ、問題を最小限にする試みが行われた。

そうした事前対策が功を奏し、大きな混乱を与えることなく当日を過ごせたことが報告されている。IPv6に対応した通信サービスの利用者については全く問題がなく、こうしたサービスの利用者が増加することによって、懸念されている問題は解消することも確認できている。

今回実施された施策の有効性も確認できたが、現実にはそうした施策と平行して、IPv6サービスが普及展開するシナリオがこのまま進めば、ウェブサイトはクライアントの実行環境や通信環境を気にすることなく、一般的なIPv6対応をするだけでよくなる。

IPv4とIPv6の共存期は長期間におよぶと予測されているが、ウェブサイトの構築に関わる組織や担当者に何をどこまでやるべきかといった情報提供が十分に行き渡るような働き掛けが今後は必要となってきたようだ。

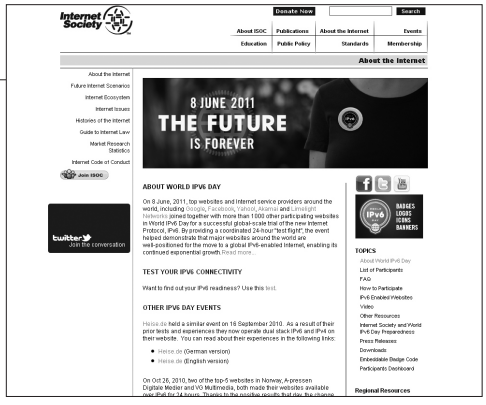
### 日本からの参加者と状況

財団法人インターネット協会、IPv6普及・高度化推進協議会、ISOC日本支部（再活性化中）、WIDEプロジェクトの4団体は、ウェブサイト提供者に対してISOCとのやり取りを日本語で受付仲介する窓口（W6D日本事務局）を開設し、先行して日本語での情報提供をしていた有志とも連携し、活動を支援した。

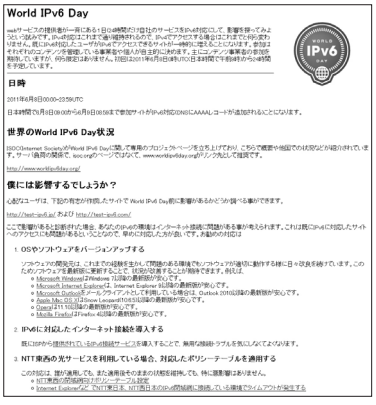
4月15日には、「World IPv6 Day国内推進キャンペーン～webサイトをIPv6に～」というキャンペーンレターを出し、広範囲に呼び掛けを行った。呼び掛けにあたっては、IPv4アドレス枯渇対応タスクフォース、JPNIC、SINETといった団体にも協力頂いた。この結果、イベント参加29組織、IPv6対応済みサイトとしての67サイトの申告を受け付け、ISOCへの登録仲介を行った。主な参加者は学術機関や業界団体だったが、なかには全国剣道連盟や歯科医院といったサイトもあった。総務省からも積極的にご参加いただいた。

### 参加意識に関するアンケート

W6D日本事務局では、事後調査としてウェブを用いたアンケートも実施した。参加者に対する参加動機や、ウェブサイトをIPv6対応する際の課題、イベント当日のIPv6アクセス状況、問題の有無などに関する設問を準備した。




ISOCのWorld IPv6 Dayのページ




World IPv6 Dayの日本語情報ページ

集計の途中経過から、参加者はWorld IPv6 Dayの意義に賛同し、問題解決に貢献するためという前向きな態度で参加していることが伺える。しかし、組織内での承認を得るのは難しいと感じており、継続的な参加はできないとした組織もあった。ウェブサイトのIPv6対応について困難と答えた組織の理由のトップ3は、先にあげた「組織内の承認取り付け」の次に「確認方法など運用全般」、「DNS設定」となっており、ウェブサーバーや周辺技術や通信環境の調達はスムーズに行えているようである。

逆にIPv6対応が簡単であったと回答した組織の理由をみると、圧倒的に「技術情報を持っていたから」という回答が多く、先行例などの情報を活用することで簡単にウェブサイトは構築できていることが伺える。ウェブサイトのIPv6対応は実際にやってみると1か月程度で提供開始できるほど、技術的には枯れてきていると言えそうである。

World IPv6 Day当日の状況については多くの組織がIPv6のアクセスを確認できており、IPv4との比率で、0.5%から5%のアクセスが観測された。また、問題や課題の発見については、このイベントが想定していたようなコーディネートされていない低品質な6to4を用いた通信の問題に直面した組織は極めて少なかったようだ。ルーターなどへのフィルタのIPv4同等レベルの設定方法やウェブサイト開発上の問題といった事前の準備に関する問題点やポートスキャンの観測があがっていた。もともと対応済みだったサイトからは、普段よりもIPv6での通信が減ったという報告もあった。なお、6to4の通信の日本での状況については、Tokyo6to4での観測(※1)も参考になる。

イベントの運用に関しては、「もっと一般ユーザーを巻き込んで問題点を洗い出した方がよかった」、「広報宣伝を大々的に行なえばよかった」といった広範囲な情報収集を求める声が上がっている一方で、今やインターネットは重要な通信手段となっているため、フィールドテストを行うことへの是非を問う声もあった。今回は大きな混乱や問題がなくイベントが終了したが、今後同種のイベントを実施するにあたっては、広範囲なユーザーへの説明や実施方針などについての世界的な議論が必要かもしれない。また、参加者側での観測方法や効果測定方法などの共有やHTTP以外のサービスプロトコルでの実験、1日ではなくもっと長い期間の推移をみたイベント実施といった声もあがっており、主催したISOCへはこうした日本からの声をまとめて伝え、次回イベントがある場合に役立ててもらう予定だ。

アンケートの集計結果については、インターネット協会IPv6デプロイメント委員会内のWorld IPv6 Day情報ページに掲載予定である(※2)。

## 終わりに

世界的な社会実験イベントとしては、2000年のICANN At Largeくらいに遡るのではないかと思う。当時と違うのは、グーグルやヤフーといった経済や実業に影響を持つ企業が積極的にイベントを牽引しているところで、このことから「インターネット」への関心が変わってきていることが見て取れるようだ。イベント後、IPv6対応を継続しているウェブサイトも多数ある。IPv6対応サイトが増加することで、ユーザー・OSなどの基盤技術・通信サービス・コンテンツサービスと包括的にIPv6を利用する状況が整いつつある。全体状況が整ったことからInternet of Thingsなど次世代的な利用へのステップも進むことが予測される。

（※1）*http://www.tokyo6to4.net/index.php/* トラフィック状況

（※2）*http://www.iajapan.org/ipv6/about_w6d.html*