Internet Week 2014／IP Meeting 2014 開催報告

～あらためて“みんなの”インターネットを考えよう～

Internet Week 2014 ～あらためて“みんなの”インターネットを考えよう～ 開催報告

2014年11月18日（火）から21日（金）まで、JPNICは毎年恒例のInternet Weekを開催しました。本稿ではその模様を簡単に振り返ります。

2013年をさらに超えたプログラム数

今年の総プログラム数は、42（有料プログラム26、無料プログラム10、懇親会1、同時開催イベント5）となりました。会場を横浜から東京に移して以降、最多だった昨年2013年を一つ上回り、わずかではありますが、またしても最多記録を更新しました。

最終的な参加者数は、Internet Week 2013と同水準の約2,650名（延べ人数、同時開催イベントの参加者数を含む）となりました。今年もたくさんの方にご参加いただいたことに、この場を借りて御礼申し上げます。

あらためてインターネットを考える場に

「あらためて“みんなの”インターネットを考えよう」。これが今年のInternet Weekのテーマでした。

実行委員会でテーマを考えていたのは2014年4月上旬。ちょうどOpenSSLの脆弱性が発覚した直後で、今年のInternet Weekは間違いなくセキュリティの話題が中心になるだろうと話していたものです。技術的な話題以外にも、その前月の3月中旬に米国政府がDNSの管理権限を移管する意向を明らかにするなど※1、インターネットガバナンスの分野でも大きな動きがありました。ちょうどこの時期、多くの人の関心を集めていた二つのトピックのどちらにも当てはまるのではないかということで、近年まれに見る早さで決まったのがこのテーマです。

今年の2本柱：セキュリティとインターネットガバナンス

前述のテーマの下、検討されたのがInternet Week 2014のプログラム※2です。

最近ではすっかりInternet Weekの常連となった、各種サイバー攻撃の現状と対策を紹介するプログラムはもちろん、SOC（Security Operation Center）とCSIRT（Computer Security Incident Response Team）の相互理解を促進してより良いインシデント解決をめざすプログラム、最近のセキュリティ人材育成の取り組みを紹介するプログラムなどの新顔も。毎年恒例のDNS DAYでもセキュリティの対応に大きく時間を割くなど、ほぼ毎時間帯、どこかのプログラムでセキュリティの話題が取り上げられていた、と言っても過言ではないかもしれません。

もう一つの柱であるインターネットガバナンスは、「第4回日本インターネットガバナンス会議（IGCJ）」と、「IP Meeting 2014」で取り上げました。2014年6月に発足したIGCJは、Internet Weekまでに3回の会合を重ねてきました。今回は単独開催時よりも幅広い方にご参加いただき、有意義な情報提供と議論を行うことができたのではないでしょうか。「IP Meeting 2014」では、「ビジネスの観点から見たインターネットガバナンス」と題したパネルディスカッションを行いました（内容については「IP Meeting」のところで後述しています）。遠い世界の難しいことに思えてしまう「ガバナンス」ですが、実際にそれを意識してビジネスをしている方の具体的なお話を聴き、ガバナンスの話題をこれまでより身近なもの、今後注意を払っておいた方がいいものだと感じていただけていれば幸いです。

有料プログラムを検討する場であるプログラム委員会ですが、今年は少しメンバーが替わり、若手メンバーが増えました。JPNICのメールマガジンをお読みの方の中にはお気づきの方もいらっしゃるかもしれませんが、9月より毎月、定期号に掲載されるコラムの執筆を、若手メンバーの一部にお願いしていました※3。Internetに対する熱い想いや、他のプログラム委員のアドバイスを受けながらプログラム企画に取り組む姿などが、コラムからもうかがい知ることができるのではないでしょうか。若手に刺激され、ベテランのプログラム委員もこれまで以上に活動した、例年以上に活気のある、近年で最多数のプログラムを生み出したプログラム委員会でした。

※1 米国商務省電気通信情報局がインターネットDNS機能の管理権限を移管する意向を表明
https://www.nic.ad.jp/ja/topics/2014/20140317-02.html

※2 Internet Week 2014 プログラム
https://internetweek.jp/program/

※3 News & Views Colum
https://www.nic.ad.jp/ja/mailmagazine/backnumber/column/

※4 Internet Week 2013 アンケート集計結果
https://www.nic.ad.jp/iw2013/enq/

学割導入!

昨年度の参加者アンケート※4を眺めると、40歳以上の参加者の割合がついに全体の3割を突破しました。チュートリアルプログラムを強化した近年は20代の参加者が増えてきてはいるのですが、それでもまだ年齢層の偏りも見られます。

これからのインターネットを担う若手が参加しやすくなる仕組みはないか、昨年度参加者などに事前アンケートを行い、まずは今年、学割を導入してみようということになりました。対象は25歳以下の学生の方、割引率は事前登録料金より9割引でした。社会人となった後、上司や先輩の勧めなどで参加するのではなく、学生のうちからInternet Weekに興味を持っている方がいるだろうかという不安はありましたが、想定より多くの方に利用されていたようです。Internet Weekのプログラムに参加し、大学の講義とはまた一味違った体験をして、何かを持ち帰っていただけたとしたらうれしい限りです。

Internet Week 2014 開催概要

【正式名称】Internet Week 2014
【テーマ】「あらためて“みんなの”インターネットを考えよう」
【開催地】富士ソフトアキバプラザ
東京都千代田区神田練塀町3 富士ソフト秋葉原ビル
http://www.fsi.co.jp/akibaplaza/cont/info/access.html
【開催日程】2014年11月18日（火）から21日（金）の4日間
［同時開催イベント］
ION TOKYO
IPv6 Summit in TOKYO 2014
第27回JPNICオープンポリシーミーティング
第41回ICANN報告会
第4回日本インターネットガバナンス会議
【開催目的】1. インターネットの発展を推進する
2. インターネットに関する議論の場・交流の場を提供する
3. セミナー開催によるインターネット基盤技術の普及を図る
【対象者】インターネットの技術者および
インターネット技術と社会動向に興味のある方
【内容】インターネットに関するチュートリアル、
最新動向セミナー、ランチセミナー、BoF等
【主催】一般社団法人日本ネットワークインフォメーションセンター（JPNIC）
【協賛】
株式会社日本レジストリサービス
TATA COMMUNICATIONS
株式会社DMM.comラボ
NTTコミュニケーションズ株式会社
Asia Pacific Network Information Centre（APNIC）
株式会社SRA
日本インターネットエクスチェンジ株式会社
Internet Corporation For Assigned Names and Numbers（ICANN）
【後援】
総務省/文部科学省/経済産業省
ICT教育推進協議会（ICTEPC）
IPv6普及・高度化推進協議会（v6pc）
一般財団法人インターネット協会（IAjapan）
Internet Society Japan Chapter（ISOC-JP）
仮想化インフラストラクチャ・オペレーターズグループ（VIOPS）
一般社団法人クラウド利用促進機構（CUPA）
一般社団法人コンピュータソフトウェア協会（CSAJ）
一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）
一般社団法人情報サービス産業協会（JISA）
独立行政法人情報通信研究機構（NICT）
一般社団法人電子情報技術産業協会（JEITA）
一般社団法人日本インターネットプロバイダー協会（JAIPA）
日本シーサート協議会（NCA）
日本セキュリティオペレーション事業者協議会（ISOG-J）
日本DNSオペレーターズグループ（DNSOPS.JP）
一般財団法人日本データ通信協会（Telecom-ISAC Japan）
日本ネットワーク・オペレーターズ・グループ（JANOG）
特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）
日本UNIXユーザ会（jus）
フィッシング対策協議会
WIDEプロジェクト（WIDE）
【URL】https://internetweek.jp/

Facebook https://www.facebook.com/InternetWeek
Twitter https://twitter.com/InternetWeek_jp
ハッシュタグ #iw2014jp

最後に

Internet Week 2014の講演資料、参加者アンケート結果、BoF開催報告書などは、公式Webサイトにて公開しています。

またInternet Week 2015は11月中旬に開催予定です。

2015年は、2月にAPRICOT-APAN 2015が福岡で、11月は94th IETFが横浜で開催されるなど、大きな国際会議が日本にやってくる年でもあります。最新の国際動向に触れ、また国際舞台で日本の技術をアピールし、パワーアップした参加者のみなさま、講演者のみなさまと2015年のInternet Weekを迎えられると思うと、今から楽しみです。

APRICOT-APAN 2015 Webサイト
http://www.apricot-apan.asia/

（JPNIC インターネット推進部 坂口康子）

IP Meeting 2014 ～あらためて“みんなの”インターネットを考えよう～ 開催報告

IP Meetingは、その年のインターネット状況を総括し、今後に向けた議論を行う会合として機能してきました。昨今はInternet Weekのメインプログラムとして、プレナリのような位置づけにもなっています。

今回も、午前中には「Internet Today!」と題し、インターネットの運用にかかる今年のホットトピックを総括しました。そして午後の部は未来を見据えるものとして「ビジネスの観点から見たインターネットガバナンス」と「あらためて“みんなのインターネット”を考える～震災から3年、東京オリンピック・パラリンピックに向け、みんなで作る未来のインフラ～」という二つのパネルディスカッションを実施しました。また合間には、Internet Week 2014の最新動向セッションを紹介するライトニングトーク大会も実施しました。本稿では、午後の部の二つのパネルディスカッションの模様について簡単に報告します。

パネルディスカッション1：ビジネスの観点から見たインターネットガバナンス

2014年は、「インターネットの資源管理体制のあり方」という話題をきっかけに「インターネットガバナンス」が大きく取りざたされた年でした。しかしどうにも、この「インターネットガバナンス」は、多くの技術者にとって遠い世界の話にも映るようです。

「技術者は『統治（ガバナンス）でなくて協調（コオペレーション）』『投票でなくてコンセンサス』を旨としてインターネットの運営をしており、それを『流儀』としているが」とモデレータから前置きがあった上で、今回のセッションでは、「ビジネスサイドから見たインターネットの流儀」という観点から、「実ビジネスへのインパクト」「流儀への疑問」などが議論されました。以降に、パネリストの代表的な発言をまとめます。

モデレータ：
橘 俊男 氏
（Internet Society Japan Chapter/グリー株式会社）

パネリスト：筒井 隆司 氏（ソニー株式会社 渉外部 シニアゼネラルマネージャー（当時））
水越 一郎 氏（東日本電信電話株式会社 ビジネス開発本部）
百崎 知 氏（ソネット株式会社）

日本に聞いて良かった ―そんな世界を作りたい

パネリスト：
筒井 隆司 氏
（ソニー株式会社）

ソニーに入って32年、ずっと海外営業に携わってきました。企業にはコンプライアンスが必要ですが、時代と共に見直しが必要なルールも出て参ります。このルールを適切に変えたり、そもそものルール作りにも貢献していくのが、本日お話しする「政策渉外」という仕事です。

ネットワークの政策課題は多岐に亘り、個人情報の保護や、データの国際移転をどうするか等さまざまな課題があります。個人情報にしても、活用と保護のバランスが重要なのにもかかわらず、いつの間にか保護ありきになっていたり、国境を越えた自由なデータの流通と利活用を通じてイノベーションを推進するのが本来のあるべき姿ですが、内容と目的にあった適切な保護が行われておらず、ビジネス上のリスクが非常に大きいと感じることがあります。自由に発展してきたグローバルなインターネットのイノベーションが様々な国ごとのルール作りによって阻害される懸念もあります。

こうした問題を解決しなくてはなりませんが、悩みは、インターネット関連会議は多岐に亘ることです。ITUのように一国一票制で決められるルールや論点もあれば、誰もが行って発言できるものもあります。ダボス会議のようにインターネットのことがずいぶん話されても小さい話題はあまり議論されないことがあったり、結局「外交上の問題としましょう」という結論になることもあります。

グローバルで活動するとなると「国境」の内側である特定の国のルールだけに従ってビジネスを行うということはありません。米国で商売するのであれば、そこで必要なルールに対して意見を言わなくてはいけないし、他の国でもそうです。先ほどネット中立性の話が出ましたが、米国でFCCがそれに対するパブリックコメントを募集したところ集まった件数は数百万件でした。一方、日本での個人情報保護法の綱領を変更した際のパブコメは数百件です。日本での流儀は、「ルールは誰かが決めるもので、それが決まればその下で正々堂々と勝負していく」というものなのかもしれません。しかし、これが世界で通用しないところなのではないでしょうか。もちろん、「自分がやらなくても誰かについていけばいいのでは」という話は常にあります。しかしこうした“関心が低い”というのが一番の問題なのかもしれません。

インターネットは人間が作ったものです。そのため、そこには「人の意思」があるはずです。なので、本日この場におられる皆様を含め、私たちのこうした活動のゴールが何かと問われれば、「国際的なルール形成やその論点にしっかり入って世界に貢献すること、日本に入ってもらってよかった」という状態を作れるかどうかということだと思います。日本の技術は超一流で、経済もそうです。そこは他国も認めるところです。その国がルール作りに入っておらず、後から「もう少し声を聞いておけばよかったな」という状況になってしまうのではあまりにも残念です。それができるようになるのがうれしいし、皆様にも技術のバックグラウンドを持ってやれることを、ぜひ書き出して実践していただきたいと思います。

困るよりはやってみろ、困ってから話が始まる

パネリスト：
百崎 知 氏
（ソネット株式会社）

入社以来ネットワークエンジニアとして、ISPネットワークの設計・構築・運用をやってきました。IPv4アドレスの在庫枯渇が言われ始めた2008年頃資源管理を任せられ、そこからJPOPMの議論に参加することになり、インターネットのルールがそこから見えてきました。

エンジニアから見ても、インターネットガバナンスのテーマについて、興味を惹かれるワードは多いです。インターネットの資源だけではなく、ネット中立性、迷惑メール、DoS対策、フィルタリング、サイバー犯罪などです。しかし一つ一つを深掘りしていくとわからないことも多くあります。IPv4の枯渇に関しても、売買の話もある中でCGNのような延命技術もある、そもそもIPv6の普及に対してのコストは誰が負担するのか等があります。またネット中立性に関しても、米国とFCCのようなキーワードも聞こえてはきますが、欧米と日本の違いもよくわかりません。DoSやフィルタリングというキーワードではサイバー犯罪を起こさないことが重要だと思いますが、通信の秘密の話や、オーバーフィルタリングの話にもつながります。また、国をまたがった犯罪の場合も国際連携はどうなるんだろうと思います。

ということで、いろいろ気になることはあるけれど、結局「どこで」「誰が」「何を」話し合っているのかわからず、オープンと言いながら実は閉鎖的なのではないかとか、参加する方法としても、個人としても興味を持っていても会社に言うと、短期的・中長期的なビジネスへの影響について聞かれ、卑近な政府のパブリックコメントの方に目が向きがちです。

要は、「なんとなく興味はあるが、それは個人の興味にとどまり、誰が何をやっているのかわからなくて、わからないものを会社に説明するしようとするとよりわからない」「今の事業やビジネスに対して、いつにどのくらいの影響があるかを必ず聞かれるが、会社に経営の目線でどのように興味を持たせられるのかがわからないので、はじめられない」という状況だと思います。また日本の会社では、自身で手の届かないところ、例えば「ITUでこれが決まり、こういう影響が出る」となると「そうか、それが時代だよな。そういう時代に残っていける戦略を考えろ」と受け入れてしまう傾向があります。

本当は、困ることを回避ばかりするのは本末転倒ではないか、と思うのです。「やってみて困るというよりやってみろ、困ってから初めて話が始まる」のでは、そこから学ぶのではないかと思っています。

次々新しいテーマが出てくるインターネットは、常に変わり広がっていくものです。また、ルールは視点により捉え方も違います。僕らのような企業は、「インターネット」という商品を売っていますが、自分たちがインターネットの一部になりながら、それが思った通りのインターネットになっているなと思えると、本当のインターネットの会社になれるのではないかと思います。

日本の企業が“インターネットガバナンス”の考え方に適さない理由

パネリスト：
水越 一郎 氏
（東日本電信電話株式会社）

パソコン通信を振り出しに、ISP運用を行い、今はNTTでフレッツの開発を行っています。IPアドレスと縁があって、CIDRを導入する1998年頃、JPNIC IP-WGの主査となり、2009年にはIPv6の割り当てで関係者と議論し、最近も可能な限りJPOPMには参加しています。

そのように、IP関連のポリシーについては個人としても会社としてもその節目節目に関与してきたつもりです。しかし「インターネットガバナンス」という括りになるとジャンルが広すぎますね。ドメイン名の話も知的財産の話になると複雑ですし、ネット中立性の話もタダのり論はけしからんとは思いますが、どこで何が決まっているのか、米国の世論で決まっているのか、国内事業者としてはFCCにいくわけにもいかないし……と感じます。このように海外からの圧力は受けているはずなのに、それに対して何をするかということについては何もできていません。海外は遠いという話もあります。

そのような訳で、私自身も興味はあっても、今一つ響かないというのが実感です。分野が広すぎて興味が絞れないのと同時に、何とかなるだろうというノンポリズムやリバタリアン的な考えもあります。会社としてもドメスティックなビジネスをやっているという理由から、ほとんど響いていないように感じています。直接的な利益のにおいがしないため、スコープを定めにくく、CSR的な考え方でやっていくものなのかもしれません。

日本の会社がこうした問題に取り組むにあたって、適していないという点がいくつかあります。会社としては「ポジションを取らない」という判断をすることは、意思決定の一つです。しかしそのためにはまず「参加している」ことが必要であるし、しかも行った先でアジェンダが生まれるということもあるので、本来は行かないと何も始まらないのに、「目的と結果を持って出張に」となってしまう点です。動いている問題に対処するのは難しいのではと感じます。またこうした政策的なことは、「流れを見続けている」「相手の顔がわかる」という個人の存在感も必要になるものですが、日本の会社は「そろそろ別の人を……」となり、継続性も難しいところがあります。本来は教育のために派遣しているわけではないはずです。

こうした活動のゴールと問われれば、標準化とか文書を出すということだけではなく、文書へどれだけ貢献できたかも一つのゴールではないか、とは思います。エンドレスジャーニーではありますね。

技術の世界もビジネスの世界も、どうもこうした話題に無関心ではなさそうだというのがパネルディスカッションでわかったことです。しかし、関与方法も立場によってさまざまで、すべての領域にすべての人が関与するのはとても壮大なことだというのも見えています。そのため「関与している人を支援することも重要ではないか」「とかく継続的にやっていくことが、裾野を広げるための秘策では」とパネルディスカッションは締めくくられました。

（注：各講演者のコメントの内容は、当日の話をもとに編集を行ったものです。また、各講演者の所属は、開催当時のものです。）

パネルディスカッション2：～あらためて“みんなのインターネット”を考える

2020年のオリンピック・パラリンピックの開催地が東京に決まりました。そうした状況を受け、2012年のロンドンオリンピックでどういう現象が起こったのか、セキュリティ等はどうだったのかなどの教訓を振り返り、生かしつつこれからのネットワークインフラに期待されていること、我々が未来に向けて準備すべきことを議論するパネルディスカッションが行われました。パネリストは以下の通りです。

BTはロンドンオリンピックにおける唯一の通信プロバイダーとして、Wi-FiやCATV網、モバイルネットワークの接続なども含め、オリンピックの通信およびそのセキュリティを担当していました。そのBTのフィリップ・モリスさんからロンドンで起こったことを伺った後に、2020年に向けてのディスカッションが行われました。

モデレータ：
江崎 浩 氏
（JPNIC副理事長、東京大学）

コメンテータ：
吉田 友哉 氏
（インターネットマルチフィード株式会社）

パネリスト：**フィリップ・モリス 氏**
（BT（ブリティッシュ・テレコム））
小山 覚 氏
（NTTコミュニケーションズ株式会社 経営企画部 マネージドセキュリティサービス推進室 担当部長）
鈴木 茂樹 氏
（総務省情報通信国際戦略局長）
丸山 充 氏
（神奈川工科大学情報ネットワーク・コミュニケーション学科教授）【ビデオ出演】

2012年ロンドンオリンピックで起こったこと

パネリスト：
フィリップ・モリス氏
（BT（ブリティッシュ・テレコム））

オリンピックに必要なキャパシティ

まず初めに考慮すべきは、オリンピックの開催規模の巨大さです。オリンピックは国家にとって、平和時における最大のロジスティクスが要求されると言われています。そして失敗は決して許されません。通信においても放送、ネットワーク、Webと何一つ落とすわけにはいきません。ロンドンオリンピックでは、17日間に1,100万枚のチケットが売れ、多くの交通渋滞が生まれました。多くの人が複数のデバイスを持ち込んでおり、ケーブルも一から計画して敷設する必要がありました。Webとテレビの視聴者は約50億人、世界人口の5/6が見た計算になります。

オリンピックにおけるスポンサーの役割と苦労

通信の提供者としての我々に対する情報やオーダーを受け入れる体制が必要です。オーダーのピークは、大会の13ヶ月前である2011年7月でした。それらのオーダーをさばき、実現していかねばなりません。

最大の難しさは、「オリンピックでは、タイムラインに対する変更が無い」ことです。こちらの準備の度合いはまったく斟酌されず、開会式は絶対に決まった日付に行われます。ロンドンオリンピックでも、とあるスポンサーが、あるオーダーに合わせられず、軍隊の派遣で解決するようなことも発生しました。一方、タイムラインは絶対的に決まっているのに、要求は変わっていきます。例えば、スポンサー契約時には「会場は100Mbpsで接続できれば良い」とされていたものが、最終オーダーは「10Gbps」と100倍になり、400台敷設すれば良いとされていたアクセスポイントも「1,600台」と4倍になりました。そうしないとデバイスを収容できないという結論になったわけです。こうした進化のスピードは、契約書締結時には誰にも想像できませんでした。しかしスポンサーである以上、破綻させるわけにはいきません。実際、2010年にスポンサーのNortel Networks社が経営破綻し、その影響でBTも通信設備の設計をやり直す必要が出ましたが、開会まで1年未満の時間しかありませんでした。スポンサー契約になかったことも、そういう状態になればやらざるをえません。

ロンドンオリンピックにおける通信環境整備の状況

入札時の2005年初頭、いわゆるスマートフォンはまだありませんでしたが、2007年にiPhoneが生まれ、モバイルの環境が急激に変わりました。2009年には当初の計画のままではダメだと、ぎりぎりにインフラの計画を変更しました。また、携帯端末のスポンサーは他社でしたが、BTはSIMカードのスポンサーとして、その中のセキュリティも考慮しなくてはなりませんでした。これは認証も自動的に行い、ユーザーの音声を暗号化するというとても大きなプロジェクトでした。当時モバイルに関しては、2Gと3Gが主流で4Gは使われていませんでした。

Wi-Fiの敷設にも挑戦がありました。別々のWi-Fiサービスや指向性のアンテナを組み合わせて、選手用、選手の家族用、プレス用、パブリックWi-Fi等々に分けて敷設する必要があります。帯域幅も検討が必要でした。

また東京オリンピックでは、東京地区に集中して競技が行われると思いますが、ロンドンの場合は開催地が国全体に散らばっていました。そのことから5,500kmのケーブルを用意し、すべてつなぐことが必要でした。

国際オリンピック委員会の要求 ～深刻度=シビリティへの対応～

一つの鍵は、一発で成功する方法論が必要だということです。とにかく本番で成功させるために、裏でテストをしたり、冗長性や可用性を上げたり、問題が起こった際にすぐに修正できるようにしなくてはなりません。開催地によっては1年前から空いているところもあったので、早めにコンペを始め、各スポンサーが政府と協力して包括的に多くの準備を行っていきました。

また、技術のオペレーションセンターを立ち上げ、600名がオペレーションセンターに在席しました。うち180名がBTから、それ以外が他社と政府関係者です。このオペレーションセンターでの銘は、「“深刻度1”の事象は発生させない」でした。オリンピックは国際オリンピック委員会（IOC）が管理しており、IOCが開催都市に対して制定したルールに開催都市が準拠することで大会が運営されます。その一つが「（問題の）深刻度=シビリティ」であり、何か問題が起きた際にそれが競技にどの程度の深刻さを与えるかの指標です。深刻度1は、例えばタイムを取ることができない等競技自体に影響が出たり、放送が止まってしまったり、電気が落ちて感電するなどという命を脅かす事象が起こったりすることです。深刻度2は、冗長性が何か欠ける類いのもので、競技にとって必須なサービスが落ちるということではありません。この深刻度に関しIOCは、問題解決に要する時間を、以前の北京オリンピックの半分に短縮するよう求めてきました。これはとても厳しいものですが、同様の基準が、今後のリオデジャネイロや東京でも求められる可能性が高いと思います。

競技に影響がある、命が脅かされることは発生させないというのが前提でしたから、競合他社であっても、全員が協力することを学ばねばなりませんでした。結果として深刻度1の事象は無く、深刻度2は21ケースが報告されました。深刻度2の事象の大半は、半分を占める屋外の開催地に起因する、「トラックがケーブルを踏んだ」「水があふれ、光ケーブルがだめになった」等のケースでしたが、冗長化を再度取りながらクリアしました。

セキュリティ

Webセキュリティに関しても、いろいろありました。50TB以上のトラフィックがプロキシサーバに寄せられ、2億以上の悪意のあるアクセスがブロックされました。イギリスが6個の金メダルを獲得し、一番の誇らしい日であったスーパーサタデーには、1億2,800万のイベントが検知されました。また、3万人のメディアが複数のデバイスを持ち大会を取材していましたが、ほとんどの人がセキュリティに気を配っていなかったため、6割程度がマルウェアに感染し、スパムも増え、ISPの手にも負えず、プレスのネットワークは分割しなくてはなりませんでした。ブラックリスト化もできず、機器の修理にもかなり追われました。

IOCの主導で、事前に政府とともに“War Gaming”と題した大きなリハーサルやシミュレーションもしました。最初は簡単なものから、CERT（Computer Emergency Response Team）のテスト、完全な統合されたテストまで、あえてプレッシャーをかけながら、どの程度やれているか、方法論がわかっているか、本番さながらの演習をし、チェックしました。セキュリティを担保しながらシステムを見ていくのです。可用性のサービスレベルとセキュリティのサービスレベルは、大体同じくらい重要視しました。また、統合されたまったく新しい「サイバープラットフォーム」というプラットフォームを構築し、多くのデータや分析がビジュアルとしても一目でチェックできるようにもしました。

「Security by Design=計画的なセキュリティ対策」という考え方があります。必ずどんなことにもセキュリティの考えをベースに入れました。ここが一つの成功に向けた大きなドライバになったと思います。こうした教訓は、インターネット、車、ビルマネジメント、その他の公共政策にも生かせると考えています。

またセキュリティにとって重要だったポイントは、ツールや技術ではなく、人の振る舞いやスキルセットに焦点を当てたということです。行動やスキルに対する投資も、大きな注力範囲になりました。

2020年東京オリンピックに向けてのディスカッション

― 2020年に向けての現在の検討状況は?

鈴木氏

2020年にはオリンピック・パラリンピックだけでなく、「ICTによるおもてなし」で情報通信基盤をとことん利用して観光もしてもらい、日本は安心で安全で快適に過ごせるということを感じて欲しいと、今から取り組み始めています。超高速のブロードバンド、第4/5世代のワイヤレスブロードバンド、Wi-Fiの性能も上がり、放送も4K/8Kの世界となるでしょう。

いろいろな観点からどれだけのインフラを整備したら良いかを議論していきますが、問題は「セキュリティ」です。本日（2014年11月22日）解散した国会で、「セキュリティ基本法」が成立し、来年から内閣の情報セキュリティセンター（NISC）が法律に基づき設置される組織となり、体制も拡充されることになりました。通信網のネットワークだけではなく、エネルギーや運輸金融などあらゆる通信のセキュリティを考えなければならない状況になります。鉄道が止まる、金融に問題が起こる、電気が止まって街がダウンすることもあり得ます。なぜなら、重要インフラのバックボーンはすべて情報通信ネットワークだからです。ネットワークが止まったら困るものはまとめて対策する必要があります。既にオリンピックの部局として20の部局ができていますが、このうちの一つに「情報通信局」があります。また大会運営用の情報基盤をどうするか、そこのセキュリティをどうするかという意味ではセキュリティ対策室もできていると聞いているので、大会全体の基盤の整備とセキュリティ対策、情報通信基盤の運営とセキュリティを一体となって進めていくことを考えています。

ー ロンドンでは、4K放送が行われていましたか? ロンドンでは、ブロードキャスト以外のメディアもサポートしていたのでしょうか? また2020年には、4Kになると思っていいでしょうか?


モリス氏

2012年の時点で、すべてのカメラが4K対応していましたが、ユーザー側が未対応であるためHDに変換して配信していました。当時直接4Kに取り組んだのはBBCだけでしたが、2020年にはすべての映像が4Kになるでしょう。また、NetFLIXやビデオオンデマンド、またタブレットやスマートフォンで映像をダウンロードできる「オーバーザトップ」というサービスもサポートしていました。そのため、2008年の北京から2012年の間に、コアネットワークの帯域が24Gbpsから160Gbpsと750%も拡大しました。


鈴木氏

周波数は2700MHzまでに拡張する予定ですが、その理由は、2020年にはほとんどの人がスマートフォンやウェアラブル端末を持ち、その場で好きなシーンをリアルタイムに4K映像を流す時代になってくるのではないかと想定しているからです。どれだけ周波数があったら良いか明言できませんが、「出せるだけ出す」ことに決めたのが2700MHzです。


小山氏

正直あんまり想像したくない世界ですね。1km²にいる10万人からのアップロードは、「攻撃」以外の何ものでもありません。Wi-FiやLTEでパケットを運ぶ人の気持ちも考えて、今後の利用に向けた設計していかなければいけないのではないでしょうか。また現実問題として、資金の問題も大きいように感じます。1ヶ所切れたとしても大丈夫な冗長性を備える設備の投資額は、何百億円という規模になりかねません。スポンサーになるとどこからも資金はやってこず、自分で出さねばなりません。


鈴木氏

国内のスポンサーはまだ決まっていませんが、スポンサーは資金だけではなく、さまざまなオーダーに応えなくてはならないという状況は、ある意味恐ろしいことだと思っています。ファシリティの準備をする文部科学省にも、Wi-Fiのスポットなどもたくさん置けるよう大容量の光ファイバーを依頼していますが、実際問題としてどこまでできるかは、「どれだけスポンサーが集まるか」で決まる要素と、「あと6年間のどこで見切って設備の準備を始めるのか」という要素があると思います。結構難しい問題ですね。

ー「最初の予想は裏切られる、これが学んだことだ」という話もありました。


モリス氏

絶えまない変更要求に対し、その管理をどうするか、どこでバランスを取るかについては、運営委員会とスポンサーの間だけでなく、IOCとの間でも決まることもあります。時にIOCが仲介者にもなったり、場合によっては政府も資金を調達してくれたりすることもあります。長く利用できる施設は、公的な資金できちんと整備すべきである一方、一時的な施設はそれなりに扱うというバランスを、全体的に見て決めねばなりません。

ー すべてのインフラにネットワークは関わり、物理セキュリティからサイバーに至るまでセキュリティが必要になるという話もありましたが、2020年は2012年とどういう状況が変わってくると思いますか? また、日本におけるセキュリティ議論はどう進んでいますか?


モリス氏

特にビル関係の図面などは、2DのCADデータではなく、3Dモデリングされたものとなるでしょう。パイプなどの連結情報や電源の位置など一つをとっても、テロリストや攻撃者にとって、貴重な情報になり得ます。そのため、開催地のインフラの情報に誰がアクセスできるのか、下請けも含めて把握する必要があります。それぞれのアクセス権限を管理し、漏れないようにしないとなりません。

また、チケット発行のシステムも、おそらく2020年には物理的な紙ではなく、SuicaやPASMOのようなシステムを使っていくでしょう。それの権限と複数の要素での認証が必要になります。

さらには、密度の高いところにあるビルなど、子供がフェンスを登らないようにしなくてはいけないなども含めて、どういう物理セキュリティの仕組みを引くのかという観点も必要になるでしょう。ロンドンでは、選手村も含めて、一つの大きなフェンスを作ってガードしましたが、東京の場合は、もう少しそれぞれの拠点が分散されるのではないでしょうか。川があったりお台場があったり、それぞれを守る必要があります。


鈴木氏

電力などのエネルギー網はスマートシティなどと呼ばれネットワークでコントロールされますし、鉄道もしかりです。自動車や信号も高度道路交通システム（ITS）でコントロールされているため、侵入される可能性はあります。またドローン（無人小型飛行機）などを使ってのテロも考えられるでしょう。ネットワークがあることの便利さの反面、新しいセキュリティリスクも生まれています。この対策をこれから具体的に検討していかねばなりません。また、オープンデータは悪い人にとっても使い勝手の良いデータです。その辺はNISCがこれから検討していくでしょう。

ー 日本でもサイバーの攻撃に対しては机上でシナリオを作り実機で演習していますが、ロンドンでは物理的なセキュリティも含め、チェックはどのようにされていたのでしょうか?


モリス氏

ロンドンオリンピックの準備は、Olympic Development Authority（ODA）が会場作りを担当し、これが組織委員会である、London Organising Committee of the Olympic and Paralympic Games（LOCOG）に引き継がれました。ODAでは会場作りの初めから、「Security by Design」の概念がきちんと取り入れられていました。セキュリティセンサーやモーションセンサーを入れてセキュリティを担保した後で、LOCOGやBTに運営が引き継がれましたが、引き継ぎもすべてモニターされた上で、ビックデータ分析ツールに入れられ、完全な形で行われました。作業員の認証も厳しく行われ、また人によって立ち入れる場所とそうでない場所も厳しく決められていました。また、要素認証としてバッチだけでなく生体認証を入れ、誰がどこに行ったかのトラッキングもされていました。物理的なセキュリティエキスパートもおり、爆弾やMPUが仕掛けられそうな場所の巡回をしていました。

ー 攻撃を受けている人に手を差し伸べるにはモニタリングも必要になるものですが、日本だと現時点ではこれが通信の秘密に抵触し、また情報共有も容易でありません。そういう障壁が取り除かれる状況が日本で実現するでしょうか?


小山氏

運用については今までの10年で変わってきたと思います。当初は、電話の時代の考えしかなかったものが、インターネットの進化により少しずつでも変わっています。しかし今のままで間に合うかと言うと、現状の取り組みで足りないと感じるのがやはり情報共有です。どのオリンピックでも、軍や諜報機関の情報を使っていますが、日本ではその議論を行っておらず、攻撃が来た際に守れるのかということは通信の秘密以前の問題としての課題なのかもしれません。

ー ロンドンでは「OCCT=オリンピックサイバーコントロールチーム」というものを作ったという話がありました。その構造を簡単に説明してください。


モリス氏

BTを含む各責任省庁からの代表者がOCCTに集まり、ここでさまざまな計画内容、開発内容、脅威、攻撃者といった情報を集めることができました。事前演習のWar Gamingのシナリオの話もしましたが、このシミュレーションはOCCTが作ったシナリオに基づいて実行したものです。また重要だったのは、OCCTの代表者が内務省大臣の直属であり、この人物が、軍隊に警告をするとか、CERTを関与させるとか、分析にかけるとか、特定のシステムを切り離してオフラインにする等を判断し、決定できました。ロンドンではSuicaに似た「オイスターカード」というシステムが鉄道などで使われていますが、これがハッキングを受けるような事態が起こった場合に、鉄道のゲートがオープンモードになり、誰でも無料で交通機関に乗れるようになるというようなことまで決まっていました。


鈴木氏

ぜひ日本でもそうした仕組みを作るべきですね。実は本日の国会の解散で流れてしまったのですが、オリンピック担当大臣やスポーツ庁を置くという話も出ていました。それができると体制強化がされ、国家安全保障局もでき、NISCとの両建てにもなります。イギリスの例を参考にしたいですね。

ー オリンピックに向けて、ネットワークに関わる我々に期待されることは何でしょうか。


小山氏

日本のISPは、「通信の秘密の侵害罪」を恐れて動けなくなることを危惧しています。「オリンピックで何を守るのか」といった議論の際に「可用性だ」という声は返ってきますが、ウィルスが出回ることで例えばどこかのISPがこけたとしても開会式がきちんとできれば良い、というほどの張り詰めた中での運用が必要になると聞きます。我々ISPは2020年までに「回復力」をどれだけ持てるようになるのでしょうか。スポンサーはたくさんの要求を満たす必要があるとの話を聞きましたが、スポンサーにならない事業者、そしてISPは、「一番に自分を守ること」を真剣に考えるべきでしょう。2013年に300Gbpsの攻撃があったことを鑑みても2020年のトラフィックは膨大です。今からきれいにしておく必要があります。また、AntinnyによるDDoSで得た教訓は、「管理者不在の脆弱なネットワークやシステムもできるだけなくしたい」ということです。そのためにISPのためのガイドラインも第3版ができました。これにより、ボットネットを利用したDDoSやリフレクション攻撃に対しても、IP53B（53番ポートのブロッキング）の導入が可能になっています。

皆でできることは、IoTのセキュリティ対策に尽きるのではないでしょうか。皆がたくさんのデバイスを持っています。野良IoTをどう作らないか、素のグローバルアドレスを渡す今の状況は変えないといけないのかもしれません。IoTデバイスのハンドリングネットワークをどう作るかを皆さんと考えていきたいですね。


モリス氏

オリンピックには本当に多くのプレイヤーが関与せねばなりません。我々は通信のスポンサーとして多くのWGを立ち上げることで、Wi-Fiについても主要なオリンピックWi-Fiだけでなく、その周りの地区のホテルやファストフードの無料Wi-Fiなどのセキュリティの共有等もやりました。どこのWi-FiもSecurity by Designということです。まずは明確なビジョンが必要です。それに沿った形で人に正しい行動をしてもらえるようなインスピレーションを与え、また、適切な訓練や明確なコミュニケーションを通じて、透明性をあげ、適切な要件を見つけられるように一人一人のモチベーションをあげていくのです。「人」が大きなプロジェクトの成功の鍵になります。


鈴木氏

インフラ整備とセキュリティが必要とされる中、基本的にインフラを作るのは民間の通信事業者の皆さんです。その上でサービスを提供するのも、民間のISPやコンテンツプロバイダー、アプリケーションプロバイダーの皆さんとなります。政府やナショナルキャリアが基本の安全対策はやるかもしれませんが、個々のサービスとユーザーについてのセキュリティ意識を高めないと、オリンピック中に不具合は起きるのではないでしょうか。社会全体でセキュリティを考えていかないといけないでしょう。

最後に、以下の4点が重要なものとしてまとめられました。

(1) 超高速ブロードバンド時代がやってきそうだ
- 4K/8K も個人のワイヤレスデバイスが4K/8Kの映像を通信するような時代

(2) Security by Design（計画的なセキュリティ対策）が必要
- タイムラインに変更はないが、要求はどんどん変わっていく
- “回復力” “可用性” がすべてのインフラに求められる

(3) Olympic Cyber Control Team （OCCT）
- 規則、規制をどうしていくか
- すべてのシステム横断的なビックデータ解析、オープンデータも必要

(4) Olympic CERT
- サイバーだけではなく、すべての業界での物理的セキュリティも必要

（注：各講演者のコメントの内容は、当日の話をもとに編集を行ったものです。また、各講演者の所属は、開催当時のものです。）

（JPNIC インターネット推進部 根津智子）