APNIC 58 参加支援プログラム参加報告書

2024.09.03 - 2024.09.06 @Wellington, New Zealand
大阪大学 情報科学研究科
マルチメディア工学専攻 セキュリティ工学講座 博士前期課程1年
橋場慧志

---

1. 概要

本文書はJPNIC主催の参加支援プログラムにより、9月初旬にWellington, New Zealandにて開催されたAPNIC58に対面参加したことに対する報告書である。

2. 参加したセッション一覧

2024/09/03
- AP Star Meeting

2024/09/04
- Newcomers Session
- APNIC Opening Ceremony and Keynotes
- Technical Session 1
- Technical Session 2
- NextGen and Leadership BoF
- Welcome Social

2024/09/05
- IPv6 Deployment
- Routing Security SIG
- APNIC/FIRST Security Track 1
- Technical Session 3
- Lightning Talks
- APNIC/TWNICフェローの方との交流会

2024/09/06
- Open Policy Meeting — Policy SIG 1
- Tutorial: Build IPv6 networks on AWS: Use cases, lessons learned and reference architectures
- APNIC Member Meeting 1
- APNIC Member Meeting 2
- Closing Social

3. 特に印象に残ったセッション

3.1. AP Star Meeting

概要

AP Star(AP*)とはAsia-Pacific地域のインターネットにおけるガバナンス、教育に関連する各種団体やNIR、ICANNなどが近況報告や情報共有を行う団体であり、今回はそのカンファレンスである。今回のカンファレンスにおいても20ほどの団体が10分程度の短い発表を行っており、内容もいわゆる近況報告やイベントの報告など多岐にわたっていた。

感想等

インターネットの技術や運用といった面から離れ、特にコミュニティとしての側面が大きかった印象を受けた。APIEなどいくつか教育関連の発表があったがいずれも知らなかったので数年前に知りたかった…

3.2. Is Infrastructure Security a Market Failure — Technical Session 1

概要

DNSSECやRPKIを例にインターネットのセキュリティの普及の状況について、政府などの強制力のない市場経済の視点やアプリケーションについても含んで論じた発表。

インターネットでは各参加者がDNSSECやROAなどのセキュリティ技術を使用することが望ましいが、自由な市場経済においては各参加者に委ねられる。そのため費用の点などからあまり普及していない。十分に普及していないのでインフラのセキュリティは効果を期待できず、各ユーザ自身でTLSなどアプリケーションのレイヤーにおけるセキュリティ対策を用意する必要がある。実際にHTTPSの使用率は97%となっているなど上位層のTLSは広く普及しているなど、インフラのセキュリティを使用する利益は何があるのかも問うている。

またインターネットの費用もネットワークのための経費からアプリケーションへと大きくシフトしていることに加えて、QUICに代表されるように必要な機能自体も下位層から上位層へと移ってきている。そのためNW側としてはインフラのセキュリティについてなすべきことはほとんど残っておらず、たとえばDNSSECやBGPSECも費用負担などの課題がある上TLSで十分であるとしている。さらに昨今はCDNの利用でそもそもルーティングをしないことも多くなったため一層インフラのセキュリティに関心が向いていないとも指摘している。

このような状況下においてインフラのセキュリティの普及のために、例えば課税等によって政府が介入することは有益にはならないだろうとも指摘している。

感想等

DNSSEC、BGPSECなどが普及しないのは技術的な要因か、せいぜい導入コストが高いことくらいだろうと思っていたが、TLSの普及などによってそもそもの必要性に疑義があるということに驚いた。またNW技術においては下位層のもとに上位層が機能するといった構造を基本としている認識であったので、上位層の発展に伴って下位層におけるセキュリティの必要性に疑義が生じているという状況についても興味深い講演であった。特にセキュリティを専攻とする者として、今後どの領域（ネットワークかアプリケーションか）におけるセキュリティ技術が一層重要になるかを考える際の参考としたい。

3.3. Practical lessons learned from building an IPv6-only city — IPv6 Deployment

概要

Xiongan（中国･雄安新区）におけるNWを全てIPv6で構築する試みについての発表。

IPv6の実装･普及にはIPv6のみを用いる方法とIPv4/v6を共存させて用いる方法の二つがあり、それぞれ互換性やNWの複雑さに長短がある。Xionganでは市内全体のNWを構成がシンプルになるメリットがあるIPv6のみで構成する方法を採った。

IPv6のみでの実装として、道路、学校、水道、電力などの公共サービスにおけるNW機器に対してIPv6のみサポートするように変更させた。企業に対してはIPv6のみのNWの提供とIPv6実装への支援、補助金政策等の実施、アプリケーション提供企業に対しIPv6のサポートの推奨などがなされた。個人用デバイスに対してはIPv6をサポートしない機器の販売や、サポートしないアプリケーションによるNW接続は禁止された。なお市外にある情報へIPv4を用いてアクセスすることは許可されていた。ほかにも準備として広報やIPv4-IPv6変換システムの供用などがあった。

このような実験より、産業や個人の生活レベルでIPv6のみの使用とするには政府レベルである程度の強制力や産業界との協働が必要であること、また初期投資はかさむが全体を通した費用は抑えられることを結果として述べている。

感想等

都市レベルの壮大な環境に加え、個人でもIPv4の使用を禁じることなどは他の国･地域では実現が容易ではないように思え面白かった。アドレス空間の確保やIPsecなどの技術面以外、特に経済面などでのIPv6の利点を検証する実験として興味深く、自身の専攻に関連する当該研究の論文があればぜひ読んでみたいと思う。

また先述した”Is Infrastructure Security a Market Failure”では行政からの強制力がない経済からの視点でインフラとしてのNW設備についても論じており、本講演の実験のような政府の強制力を実現できる環境下における実験と対照的に見える。

先の講演ではTLSなど上位層でセキュリティ機能を代替できてしまうこともあり、インフラ整備に疑義が生じているとしていた。しかしIPv4においてはNATをもってしてもアドレス空間の枯渇など根本的な課題が生じており、上位層におけるプロトコルでの解決策は容易ではなく、IPv6の普及は必須であるように思える。IPv6はセキュリティを主としたプロトコルでなく、またIPv6とDNSSECやBGPSECの普及率の違いより単純な比較はできないが、先の講演では政府による課税等の介入は良い結果とはならないであろうとしていたことに対し、本講演ではインフラ整備に政府が介入することの有用性を検証できる実験に思えた。

3.4. Open Policy Meeting — Policy SIG 1

概要

APNICのポリシー改定の提案などを広く議論するセッション。今回は4つの提案があったがうち1つは取り下げられた。prop 157では一時的なIPアドレスの移転（リース）をAPNICのポリシーに組み込むことを提案していた。今回コンセンサスに至った提案はなかった。

感想等

学生の立場からは若干難しく、JPNIC公式ブログや職員の方の解説でprop 157の背景を含む提案の概要を理解できた。prop 157は以前から継続的に議論されているようだが、対面での議論はこれまでのセッションとは異なり若干殺伐とした印象を受けた。

また今回は提案取り下げとなったprop 161による通信を行わないIoT機器にも識別子としてIPv6を付与する趣旨の提案に最も興味があったが、（これもJPNICのブログや職員の方の指摘のとおり）IETFなどにて技術的な議論するべきとの考え方もあるとのことだった。

純粋な興味としてAPNICでの議論がコンセンサスに至ってポリシーに組み込まれるケースを見てみたかった気持ちもあるが、コミュニティによってインターネットが形成されている実感を得ることができたのは良い経験となった。

4. 参加支援プログラムに関する所感

インターネット

これまでNW関連を学ぶ際には、基礎としてTCP/IPなどのNWプロトコルを、また演習としても小規模LANの実装やサーバや各種NW機器のアクセス制御の技術的な事項が中心であった。そのため高専･大学の講義等では気づきにくいが、NWが単に技術としてではなく番号資源やセキュリティ面の国際的な管理がなされた上で、社会に実装されてやっとインターネットになっているという実感を得ることができた。その過程は特にポリシーミーティングという形でAPNICなどのコミュニティを通じており、経済や社会情勢なども関わっていることを学んだ。今後NWを学習したり研究などで関わる際には技術面を重視しつつも他の社会的な側面を考慮する必要性を感じた。

加えてIPv6は独立したセッションやチュートリアルが設けられており、NWのコミュニティでも大きなトピックになっているように思え、（IPv6を介した攻撃がほとんどないという理由から）IPv6の研究は主流にはなっていないセキュリティ分野との違いを感じた。今後IPv6が通信の大部分をカバーするほどの普及率になった際には、セキュリティ分野においても大きなトピックになるのかもしれないし、IPv6のセキュリティが十分と見込まれれば講演にあったようにアプリケーション層のセキュリティが一層盛んになるのかもしれない。

コミュニティ

さまざまな国･地域から参加されていたフェローの方との交流を持つことができたことも貴重な経験であり、当然NWについての話や、各フェローのバックグラウンドや興味･専攻、今後のキャリアについてなども雑談的に話すことができた。

参加前はコミュニティに関わることができるかどうかが非常に大きな懸念であったが、言語の壁があったことは否めないもののフェローの方々や、フェローの方以外ともJPNICの職員の方やIIJの松崎さんのサポートもあり広く交流することができたのは良かった。

カンファレンス

技術的なトピックから教育、島嶼国のインターネットの近況など幅広いトピックがあった。ゆえに全く知らないトピックがあったりと、NW技術や諸外国･地域のインターネットの状況を知っていれば、APNICでの講演をより深く理解しながら聴講できたように思う。

また昼食や軽食もカンファレンスで提供されその時間に他の参加者との交流につながることもあり、全体的に和やかな雰囲気のカンファレンスであると感じた。

参加支援プログラム

学生として単に参加機会を得られたことも非常にありがたいことであるが、単なる参加のみならず渡航前の準備から開催中現地での滞在にまつわるサポート、講演内容やインターネットについての解説など多くの支援をいただいたことで、APNICにおいてより充実した学びを得られた。

5. 今回の経験を今後どう生かしておきたいか

• NWに興味を持ちながらもこれまで論理学、ソフトウェア科学やセキュリティなどを専攻してきたため、NWを主専攻として研究している人よりは知識や技術面で足りない部分があると自覚している。今回のAPNICでもわからない内容はいくつかあったため、まず特にAPNICの技術的な内容を概ね掴めるくらいに浅くとも広く学習を進めたい。その点でAPNIC参加は学習の大きなモチベーションになった。言語の問題や講演に対する理解度が浅かったが故に質問や発言をできなかったことも反省点として捉えている。

• 修士課程として研究テーマを探す目的で参加したこともあったが、結果として具体的なテーマ決定には直結しなかった。しかし技術以外の面も含むインターネットの情勢やコミュニティを知ったことは今後の研究を行う上で、先行研究や自身の研究を批評する際の一つの視点になると思う。

• APNICを通じてNW運用やインターネットのポリシーに関わる方々の話を聞いたりすることができた。セキュリティや他の分野も含み何らかの形で多かれ少なかれNW技術･インターネットに関わっていきたいと漠然と考えていたこともあり、今後のキャリアを考える上で参考にしていきたい。また今後のAPNICには費用の面から出席は難しいが興味を持ち続けたい。今回交流したフェローの方とも今後APNICを含む情報系･NW系カンファレンスなどやその他でも交流を続けていきたい。

6. 謝辞

本支援プログラムにあたってはJPNICの職員の方より渡航費用の支援、渡航前と現地でのサポートやAPNICの講演内容に関する助言をいただきました。ここに感謝申し上げます。