

## North American IPv6 Summit 2004

### 概要報告 2

前回に引き続き、North American IPv6 Summit 2004参加を通じて受けた印象と北米でのIPv6動向について述べる。

#### ネットワーキング

日本ではまだIPv6ネットワーキングといえば、IPv4インターネット上でのトンネルによるIPv6接続が一般的な印象を受けるが、サミットではこの方式はあまり登場しなかった。米国防総省（以下DoD）という非常に圧倒的な実例の到来により、Pure-IPv6による本格的なネットワーキング方式とIPv4からのすみやかな移行への関心が高まっている。

IPv6ネットワークの拡大とともに、部分的に残るIPv4を暫定的にネットワーキングする必要がある。これも日本ではまだ関心が低いようだが、IPv6ネットワーク上でIPv4を通すため、各メーカーはIPv4トンネルの実装を加速しようとしている。さらに、こうした異種プロトコルを組み合わせる実装についても装置の相互接続テストメニューへ採用しようとする動きがあるなど、多少乱暴かもしれないが現場の事情を重視し実践的に取り組む姿勢が印象に残った。この点は、どちらかという標準を拠り所に緻密に積み上げてゆく日本と若干のアプローチの違いを感じた。

また、そもそもIPv6プロトコルへの移行は難しく、現実にはなかなか

かIPv4からの移行が進みにくいのではという指摘もあった。これに対して、老練な参加者からIPXからの移行時もよく似た状況であったが結局やり遂げた話が引き合いに出され、やればできるものだと反論するやりとりもあった。このように過去に試練を経験している人が多く、インターネット技術はこれまで幾多の困難を乗り越えてきたし、IPv6移行を含めこれからも乗り越えてゆけるという雰囲気支配的であった。

#### IPsec プロトコル

DoDはトランスポートモードでのIPsec利用を考えているようだが、総じて業界はやや消極的なようだ。

PKIなど周辺技術のIPv6対応を吟味し、必要に応じて標準の修正を行う必要がある。しかし、関連RFC数が膨大な上、セキュリティ技術者の非協調性というカルチャーの問題もあり、検討作業が遅々と

して進んでいないとされている。IPv6直系分野と比較して、周辺技術分野のIPv6対応の遅れは問題化しつつあるように感じた。

#### セキュリティ

IPv6セキュリティに対する関心は高く、現時点での技術的課題・問題点の認識は進みつつある。特にIPv6ではNATがなくなり、これまで以上にP2P型へ進行するであろうことから、より一層セキュリティのあり方が問われている。

トンネリング技術の発達と普及に伴い、北米でもセキュリティ脅威となる事象が顕在化しているようだ。初日のSecurity Workshopでは、ハッカーが侵入後の隠れた通信路とし



Workshop会場



サミット参加企業

てIPv6を利用する手口の紹介や、IPsecを含むトンネリング技術の前にファイアウォールはなす術がないなど、表現はやや過激だが具体的な問題点の指摘があった。ネットワーク上のファイアウォールというスタイルでセキュリティ対処するには限界があるため、今後はより『エッジ』（究極的には端末）で実施する必要があるという根本的指摘に同調する人は少なくない。

セキュリティ面のほか、総合的に見た場合のトンネルの弊害論として、IPv4上でトンネルにより端末などから直接IPv6ネットワークを張ることが、IPv6の普及と市場ニーズに根ざした適切な技術開発の妨げとなりうるとの指摘もあった。

確かに、トンネルベースのネットワーク利用が蔓延してしまえば、様々な取組みが必要とされる基本的なIPv6ネットワークでの適切な管理・エンジニアリング技術、セキュリティ技術の推進に結びつきにくい。何よりセキュリティをはじめとしたネットワーク側でのコントロールを難しくす

る。

端末からのトンネルネットワークは、便利ではあるが、失うものも少なくない。

### その他課題

他にも、DNSの実装・運用課題やアプリケーションの実装課題について

の指摘があった。また、システムレベルでの課題として、DoDはIPv6環境での認証システムの確立を求めている。具体的にはPKIベースでHost-to-Gateway型のIPsec利用時の認証とアドホックネットワーク時に必要となる相互認証利用がケースとして挙げられていた。

### サミットでのDoDの主張

サミットでのDoDの主張は、純粹技術論以外では、相互接続性の重視と、メーカー・ユーザーのIPv6への習熟推進、そのための環境整備の重視、既存アプリケーションの移行（一部はこのタイミングにあわせ作り変えられる模様）の4点にまとめられる。これらは、IPv6という新しい技術、新しい世界観に、慣れ、開拓しようという強い意識に貫かれている。

DoDは、MIL規格時代よりオープン性はさらに進み、市場の技術開発力から生まれる汎用品をよりいっそう利用する方向にある。特注品ばかり

りではなく汎用品も使う有利さを体験したDoDは、次世代の汎用技術としてIPv6の価値を信じているように見える。さらに、IPv6開発を引っ張ろうとする姿をDARPAネットワークなど現在の民生技術を生み出してきた歴史に自ら重ねて見ているようだ。DoDは過去の大きな2つの経験を今に活かしている。

DoDは単にネットワークをIPv6化するのではなく、IPv6ではじめて可能になるデザインに取り組もうとしている。すなわち仕事（ミッション）のスタイルを変えようとしているのだ。この大きな目的意識の中でIPv6を使う意義を持っている点は特筆すべきだろう。

たとえば、IPv6の最大の特長である潤沢なアドレス空間を積極的に利用し、GIG(Global Information Grid)と呼ばれる非常にたくさんのアドレスを必要とする構想を実現するという。IPv6の利点を研究し最大限に利用しようとする姿勢は、DoD関係者にかなり浸透しているように見える。また、アプリケーションのデータ・セントリック化といった直接的にはIPv6と依存関係のない話もIPv6ベースのデザインに組み込まれており、一連の変革として紹介があった。IPv6関連の取り組み紹介が中心だが、DoDのプレゼンの多くは全体としてGIGなど軍の次世代戦略システムの紹介になっていた。

もちろん、すべてIPv6ベース。彼らの言葉通り、もはや次の国防システムはIPv6抜きに考えられないことが良くわかる内容であった。