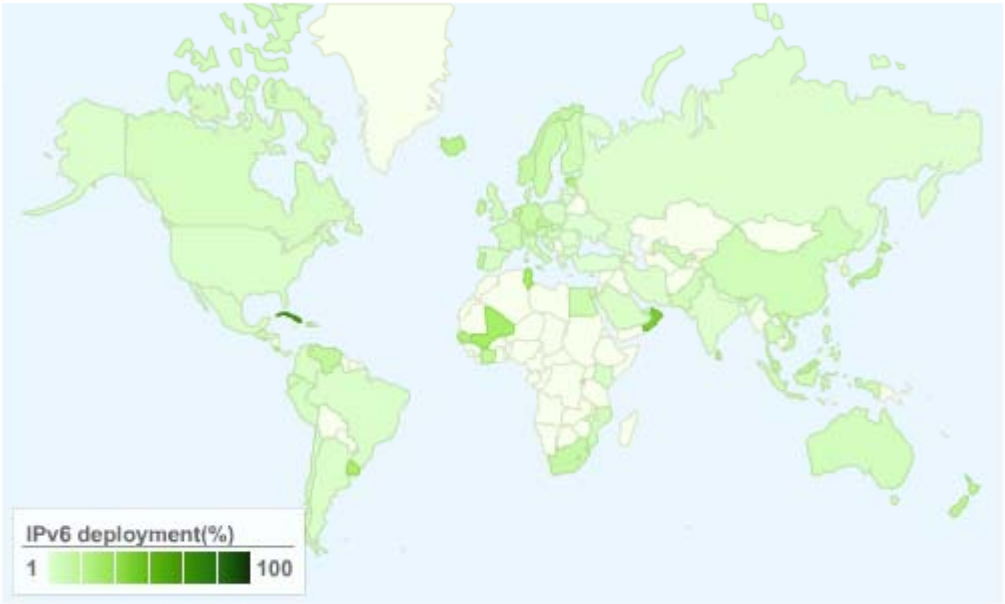
点検！セキュリティ対策製品

IPv6導入に必要とされるセキュリティ機器における課題を整理する

野々下幸治
マカフィー株式会社SE本部長

January 4, 2010

IPv6の導入状況



http://www.netknowledge.ca/index.php?option=com_content&view=article&id=57%3Aipv6-deployment-statistics&catid=38%3Anews&Itemid=58

Top10%

Country code	Country	Ipv6 deployment rate	Ipv6 network / Ipv4 networks
JE	Jersey	100%	1/1
CU	Cuba	75%	3/4
OM	Oman	50%	1/2
MC	Monaco	50%	1/2
VA	Holy See (Vatican City State)	50%	1/2
FJ	Fiji	50%	1/2
TN	Tunisia	33%	1/3
ML	Mali	33%	1/3
UY	Uruguay	31%	8/26
EE	Estonia	26%	10/39
BT	Bhutan	25%	1/4
SN	Senegal	25%	1/4
IM	Isle of Man	25%	1/4
LU	Luxembourg	24%	10/42
LK	Sri Lanka	23%	3/13
IS	Iceland	21%	6/29
EU		20%	22/109
CZ	Czech Republic	19%	34/176
NZ	New Zealand	18%	35/194
JP	Japan	17%	92/545
CI	Cote D'Ivoire	17%	1/6
NL	Netherlands	17%	85/511
MY	Malaysia	17%	13/78
MU	Mauritius	17%	1/6
VE	Venezuela	16%	6/38
PT	Portugal	15%	11/75
CR	Costa Rica	15%	2/13
TW	Taiwan, Province of China	15%	18/122
RW	Rwanda	14%	1/7
NO	Norway	14%	17/120

IPv6でもIPv4でのセキュリティの課題は同じ

- いくつかのネットワークセキュリティのため改善はこれまでのセキュリティの問題を解決？
  - IPSec -Authentication and Encryption
  - Secure Neighbor Discovery (SEND) –Layer 3 attach authentication
  - Crypto-generated Address (CGA)
  - Unique Local Addresses (ULAs)
  - Common Architecture Label IPv6 Security Option (CALIPSO)

- エンドノード間のセキュリティ構築を容易にする
  - 広いアドレスレンジはNATを不要に
  - セキュリティ拡張ヘッダ(AH、ESP)を備えたIPSecが標準
- 広いアドレスレンジはワームのスキャンを難しくするかも
- 広いアドレスレンジとAHはAnonymousでの攻撃や成りすましを難しくするかも

しかし
多くのIPv4のセキュリティの問題はIPv6でも同様

CIOが直面している5つのIPv6の脅威

- Rogue IPv6通信
  - 知らない間にIPv6通信が行なわれる危険性

FirewallやIPSでIPv6の通信をブロックするべき

- IPv6トンネル
  - Teredo、6to4、ISATAP（Intra-Site Automatic Tunnel Addressing Protocol）でIPv6の通信がIPv4にカプセル化

FirewallやIDS/IPSでトラフィックを監視

- Rogue IPv6デバイス
  - 知らない間に設定されるIPv6マシン

IPv6が不要であれば、無効にしておく

- Type 0 Routing ヘッダー
  - 既知のIPv6のDoSの脆弱性

Type 0 Routingは無効にしておく

- IPv6のICMPとマルチキャスト
  - ICMPv6によるDoS攻撃、マルチキャストによるアドレスリスト取得の危険性

ルータでフィルタリングする

http://www.networkworld.com/news/2009/071309-ipv6-network-threat.html

確かにIPv6固有の脅威かもしれないが.....
対策技術についてはIPv4と同様

IPv6のセキュリティには
製品の調査と中深い計画が必要（2004年の調査）

Department of Defense
High Performance Computing Modernization Program – *Defense Research and Engineering Network*
(A Deputy Under Secretary of Defense [Science and Technology] Program)

environment, as the TAP knew from experience. Products to support DHCPv6 in an IPv6-only environment existed in the 2003-2004 timeframe, but the IPv6 pilot team was unable to find a combination of products and configurations that would support secure, automatic registration of both IPv4 and IPv6 public addresses. Consequently, while the IPv6 pilot used stateless IPv6 address auto-configuration (SLAAC), the resulting IPv6 addresses were manually rather than automatically registered in DNS. This worked well, although on systems running Microsoft Windows it was necessary to disable temporary global IPv6 address generation (which is on by default). The IPv6 pilot team is continuing to search for products that can meet their requirements.

Network Security Products. During the IPv6 pilot implementation security products with IPv6 capabilities, including Intrusion Detection (ID), firewalls, Intrusion Prevention, virus scanners, and port scanners were not as mature nor as widely available as they were for IPv4. The situation has improved since then, but adequate IPv6 security still requires some product research and careful planning. To maintain security on an IPv6-enabled network can require the use of products that are new or may be unfamiliar to security managers, who are already struggling to maintain security on their existing IPv4 networks. In 2003 the IPv6 pilot was able to find the necessary products, although often they were open source or still under development, in all categories save one: ID. To perform inspection of IPv6 packets, the IPv6 pilot had to add IPv6 support to the source code for the ID software already deployed on the DREN called the Joint ID System, or JIDS. JIDS is a DoD version of the Network ID software from Lawrence Livermore National Laboratory. The IPv6 pilot also had to add IPv6 packet analysis support to SNORT, an ancillary tool used by the JIDS. One highly skilled network engineer worked for almost three months to make the necessary changes in JIDS and SNORT. This work was completed in 2003, and the HPC CERT deployed the IPv6-enabled JIDS across the DREN WAN in 2003-2004. The HPC CERT has since deployed additional ID

市場のFirewallの31%しかIPv6に対応できていない

DAVID PISCITELLO

are commercial firewalls ready for IP version 6?

Dave Piscitello is a Senior Security Technologist for ICANN. A 30-year Internet veteran, Dave currently serves on ICANN's Security and Stability Advisory Committee.

dave.piscitello@icann.org

THE DEPLETION RATE OF THE IP VERsion 4 (IPv4) address space has been the subject of considerable analysis and even greater speculation for nearly 15 years. However, Network Address Translation [1, 2] and classless inter-domain routing (CIDR [3]) have extended the lifespan of the IPv4 address space beyond many projected exhaustion dates. Today, many organizations still choose to dismiss experts who voice IPv4 addressing concerns as modern-day "boys who cry wolf." Whether we are perilously close to the day when ignoring the cries will prove fatal to the flock remains an open question. Assuming that exhaustion of the IPv4 address space is imminent, we consider whether the community will be able to secure networks when we are left with little choice but to deploy IPv4's successor, Internet Protocol version 6.

www.usenix.org/publications/login/2008-04/pdfs/piscitello.pdf

セキュリティ製品のIPv6対応の状況

- 対応状況を知るために参考になるサイト
  - IPv6 Ready Logo Programサイト
    - http://www.ipv6ready.org/
  - Joint Interoperability Test Commandサイト
    - http://jitc.fhu.disa.mil/apl/ipv6.html#security
  - ICSA Labs IPv6 Capable Security Productsサイト
    - http://www.icsalabs.com/technology-program/ipv6/ipv6-capable-security-products

現状の公開情報ではネットワーク製品のみで非常に不十分

セキュリティ製品のIPv6対応の状況

- Firewall
  - Juniper Netscreen, Cisco PIX, Checkpoint Firewall-1, McAfee Firewall Enterprise (Sidewinder), Fortigate Fortinet
- IPS
  - IBM-ISS Proventia, McAfee IntruShield, SourceFire, TippingPoint 2500N IPS
- 境界でのマルウェアおよび迷惑メール対策
  - McAfee Email and Web Security Appliance
- AntiVirus
  - 一般消費者向け
    - Symantec Norton, Trend Micro ウイルスバスター, McAfee Internet Security
  - 企業向け
    - McAfee ToPS
- Host IPS
  - McAfee HIPS
- 脆弱性検査
  - ネットワークベース
    - SAINT Corporation SAINT、Tenable Network Security Nesus
  - エージェントベース
    - McAfee Policy Auditor
- SIEM
  - ArcSight

ただし、IPv4のフル機能が
IPv6でサポートされているわけではない

As of 22 Oct 野々下調べ

IPv6普及・高度化推進協議会
セキュリティWGの活動の紹介

【活動目的】

IPv4アドレス枯渇時期を間近に迎え、IPv6におけるセキュリティへの関心が高まっているが、IPv6の導入によって生まれる課題とその対策や、セキュリティ製品のIPv6対応状況等の情報は、必ずしも行き渡っているとは言えない。

本WGでは、それらの情報を整理すると共に、実証実験を通じてセキュリティ製品のIPv6対応状況を検証する。加えて、IPv6固有の課題に対応するセキュリティガイドラインの検討を行う。

【2009年度活動内容】

1. IPv6インターネットに関する脅威と対応策の整理
   - IPv4時代との差異に関する分析
   - 新たに必要となるセキュリティ対策の枠組み整理

2. セキュリティ製品のIPv6対応状況の検証
   - IPv6関連セキュリティソリューションの情報収集
   - 実機を用いた機能等の検証
   - 検証結果のフィードバック及び公開

3. IPv6固有の課題に対応するセキュリティガイドラインの検討
   - IPv6でのセキュリティの方向性検討
   - セキュリティガイドラインの検討

セキュリティ製品のIPv6対応を増やすには

- システムのIPv6への対応の積極的な推進
  - 特にEnd to Endのセキュリティを担保する必要があるところはIPv6は有利
    - 最近流行のクラウドサービス、特にプライベートクラウドとか．．．
    - SCADAなど製造･制御系のシステムとか．．．
    - 他に不特定多数の接続を必要としないシステム

- IPv6普及･高度化推進協議会のセキュリティWGの活動へ協力を
  - 対応状況の整理はベンダーへのプレッシャーになります。

私のテーマについての議論


McAfee®