



セキュリティ製品のIPv6対応状況

野々下幸治

マカフィー株式会社

2010年1月27日

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

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



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

- Rogue IPv6通信 FirewallやIPSでIPv6の通信をブロックすべき
 - 知らない間にIPv6通信が行なわれる危険性
- IPv6トンネル FirewallやIDS/IPSでトラフィックを監視
 - Teredo、6to4、ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) で IPv6の通信がIPv4にカプセル化
- Rogue IPv6デバイス IPv6が不要であれば、無効にしておく
 - 知らない間に設定されるIPv6マシン
- Type 0 Routing ヘッダー Type 0 Routingは無効にしておく
 - 既知のIPv6のDoSの脆弱性
- IPv6のICMPとマルチキャスト ルータでフィルタリングする
 - 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

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

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



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.

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

Category	Vender	Product	Certification	Comment
Firewall	McAfee	Sidewinder Firewall	JITC IPv6	
		UTM Firewal (Snapgear)		
	CheckPoint	Firewall-1	IPv6 Ready phase1	
	Juniper Networks	SSG5 - SSG20 Family	JITC IPv6	
		SSG320 - SSG350 Family	JITC IPv6	
		SSG520 - SSG550 Family	JITC IPv6	
		ISG1000 - ISG2000 Family	JITC IPv6	
		NS5200 - NS5400 Family	JITC IPv6	
Fortinet	FortiGate FG-400A and FG-3600 Family	JITC IPv6		
Cisco	IOS Firewall			
Network IPS	McAfee	I-2700 and M-6050	JITC IPv6	
		Securify Monitor 6.0 Family	JITC IPv6	
	TippingPoint	2500N IPS	JITC IPv6	
	IBM-ISS	Proventia		
	SourceFire	IPS		
Mail & Web Gateway	McAfee	Email and Web Security Appliance		
AntiVirus	Symantec	Norton Antivirus		Consumer
	Trend Micro	ウイルスバスター		Consumer
	McAfee	AntiVirus Plus		Consumer
		VirusScan Enterprise		Enterprise
Host IPS	McAfee	Host IPS		
Vulnerability Scan	SAINT	SAINT		
	Tenable Network Security	Nessus		
Policy Audit	McAfee	PolicyAuditor		

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
Copyright (c) 2000-2010 NPO日本ネットワークセキュリティ協会

As of 25 Dec 野々下調べ

- コンシューマー版アンチウイルスの製品側はIPv6対応が出来ているが、
 - 定義ファイルの更新用のサーバーがIPv6に対応できていない☹
- FirewallはIPv6対応になっている
 - 対応はL3以下の層までがほとんど

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。

