2005 年 IPv6 移行ガイドライン

セキュリティ編

2005 年 3 月

IPv6 普及・高度化推進協議会

移行 WG　セキュリティ SWG

本ドキュメントについて

本ドキュメントは、IPv6 への移行過程において、“IPv6 技術”を起因とする変化を網羅的にとりあげ、個々の変化がセキュリティに及ぼす影響について分析し、その対策と課題について記述している。

また、各 SWG の移行ガイドラインにおけるセキュリティの記述は、本ドキュメントの当該部分を参照する形態をとっている。特に、大企業、自治体、SOHO、家庭の各 SWG で記述される BCP と IPv6 普及期のセキュリティについては、それぞれ 4 章、5 章の中で分析、評価を行っている。

目次

はじめに

目的

本SWGは、「セキュリティの考慮なくしてIPv6への移行は考えにくい」という問題意識に基づき、セキュリティに関する各種の課題と解を整理し、ガイドラインとして纏めることにより、IPv6 普及（移行促進）を図ることを目的とします。具体的には、IPv6 による影響の整理と分析、その対策の検討と提示、課題の明確化を行います。副次的には、技術手法の変化や選択肢の増加がもたらす IPv6 のメリットについても考察します。

IPv6 におけるセキュリティメリット

IPv6 のセキュリティ対策を検討する前に、IPv6 のセキュリティ上のメリットを示します。IPv6 を利用することのセキュリティ面でのメリットは、以下の通りです。

- IPsec が E2E で使用できる環境が広がる
  - 機密性（暗号化）、完全性（改竄検知）の向上
- クローズドネットワークにおいても、アドレスの一意性が保証されておりシステム管理が容易になる
  - 可用性（迅速な異常の検知）、完全性の向上（管理不整合の減少）
- 端末の特定、トレースが容易になる
  - 可用性（迅速な切り分け）、完全性（迅速な修復、復旧）の向上
- セキュリティ対策も含む Plug&Play なシステムが構築しやすい
  - 可用性（設定ミスの削減）、機密性（アクセス制御等）の両立レベルの向上

本ドキュメントの対象

本ドキュメントの対象（想定読者）と、それぞれの対象に向けた役割は以下の通りです。

SIer	IPv6 ソリューションの設計・構築・運用指針
情報システム管理者	IPv6 移行過程の運用指針

セキュリティ製品開発者　　IPv6 セキュリティ製品の開発指針

検討範囲

本ドキュメントの検討範囲は次の通りです。

- IPv6 技術を起因とする変化が及ぼすセキュリティへの影響
- 自治体・大企業、SOHO、家庭の各 SWG で議論される BCP、IPv6 普及期の利用シーンでのセキュリティ対策

セキュリティの検討項目は広範囲にわたり、その対策は「技術×意識×ポリシー」の総合的なものです。技術だけへの投資がセキュリティ向上に繋がるとは言いきれません。IPv6 が利用の「範囲」をより柔軟に広げる反面、それを利用する人の意識、ポリシーに基づいた明確な運用プロセスが、より重要になることに注意する必要があります。

なお、本ドキュメントでは、上記検討に入る前に、IPv6 技術以外の内容として、セキュリティ対策に対する考え方（次項以降）、現在（IPv4）のセキュリティ対策と傾向（第 2 章）についても、読者の理解を補う目的で記述しています。

セキュリティ対策とは

セキュリティ対策＝「技術×意識×ポリシー」の総合対策です。技術・システムだけでは対策にはなりません。すべてがきちんと運用されていなければ効果を発揮しません。「一箇所」の対策ミス、抜け穴、見落としが安全性を無効にしてしまいます。

運用を含めたセキュリティポリシーの徹底と、セキュリティ意識・モラルの向上が求められます。

セキュリティ対策技術

セキュリティ対策としては、技術・システムに頼り過ぎないことが重要です。どんなに強固なセキュリティシステムであっても、内部の人間による攻撃には対処できない場合が多いです。

対策のポイントは、物理的な隔離や遮断、そして利用者の制限・リソースアクセス管理です。

導入するセキュリティ対策手法について、何ができて何ができないかを理解しておくことが肝要です。すべてを 1 つのセキュリティ対策手法で解決しようとはしないことです。複数のポイントで手法を組み合わせることにより、全体のセキュリティレベルを高めることができます。

セキュリティ意識・リテラシー

どんなに堅牢なシステムでも、運用する人間の意識によってセキュリティレベルは低下します。したがって、セキュリティ意識の向上は重要です。

たとえば、次のような点に注意する必要があります。

- アカウントの使いまわし
- 単純なパスワードの使用や、パスワードをポストイットなどで誰でも見える位置に貼り付けている
- ソーシャルハッキング
- アカウント再発行依頼
- パスワードのリセット依頼
- サーバ利用申請

セキュリティに関しては、定期的な訓練と評価が欠かせません。セキュリティ防災訓練などを励行すべきです。

セキュリティポリシー

セキュリティポリシーについては、定義のみならず、その運用・適用が重要となってきます。いかにして利用者・機器にセキュリティポリシーを適用させてゆくかがポイントです。

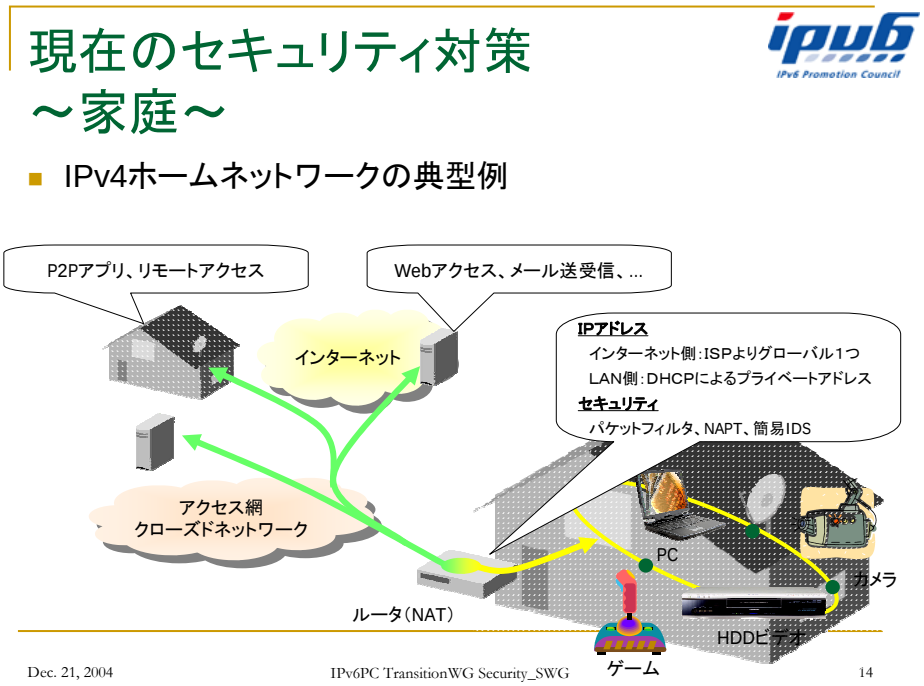
万一の損害・被害の大きさに応じて、対策にかけるコストのバランスをとることも重要です。100%安全なセキュリティ対策は存在しませんし、完全性に比例してコストは増大します。したがって、セキュリティで守るべきシステム・データの価値とコストのバランスを考慮します。軍事国家的なセキュリティは高コスト・高セキュリティです。

実際にセキュリティ対策にかかるコストや運用上の煩雑性を見極めることも忘れてはなりません。必要以上のセキュリティ対策によって、通常の業務や運用の効率が下がってしまわないか、どこまでのセキュリティ安全性を求めるか、どこまでリスクを許容できるか、を判断する必要があります。

1. 現在（IPv4）のセキュリティ対策と傾向

現在のセキュリティ対策　～家庭～

現在の IPv4 でインターネット接続されたホームネットワークは、下図のようになっています。



接続機器としては、メディアコンバータ、ルータなどのアクセス網終端装置、PC、ゲーム機、AV 機器、HDD ビデオ、ネットワーク対応カメラ、ネットワーク対応センサ、ホームゲートウェイなどがあります。

家庭内ネットワークは、有線あるいは無線（802.11a/b/g）で構成されています。

ネットワークの利用内容は、WEB、メール（クライアントの立場で利用）、メッセンジャー系（P2P 利用）、家庭内のメール・WEB サーバ（一部のスキルユーザ）、リモートからのビデオ予約など（一部サービスイン）が中心です。

セキュリティ対策は、ルータにおけるファイアウォールが基本です。パケットフィルタと NAPT 機能が中心で、一部のルータにはステートフルパケットインスペクション（SPI）機能や簡易 IDS などが搭載されています。

PC におけるパーソナル・ファイアウォール機能も使われていますが、メールのウイルスチェックが中心です。

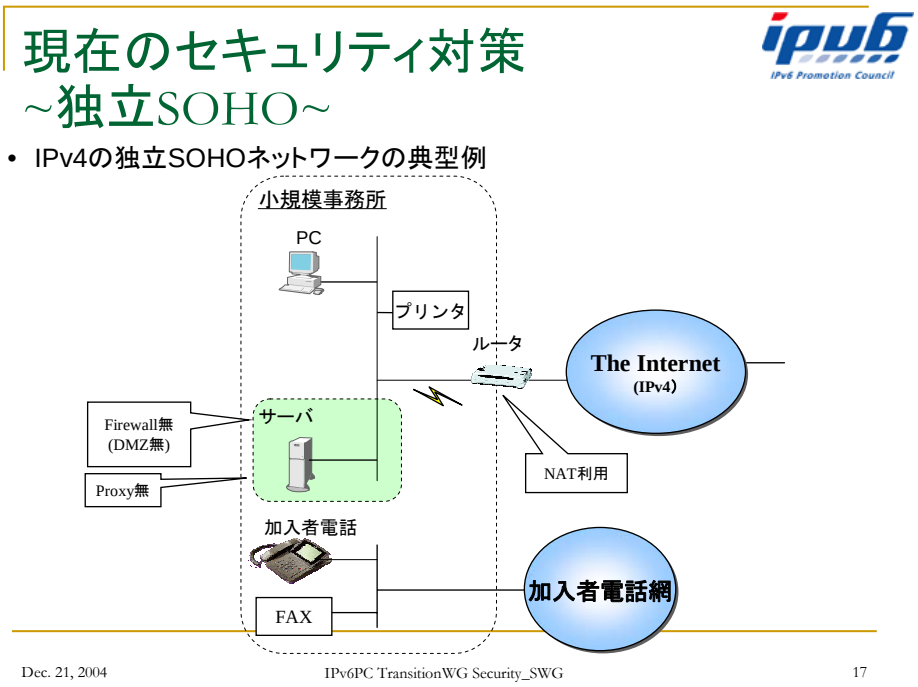
家庭ユーザ向けに、ISP や ASP から提供されているサービスとして、ウイルスチェックなどがあります。一部のスキルユーザは、ビデオ予約のための家庭内サーバへのアクセスを、Dynamic DNS＋Static NAT で実現しています。

現在のホームネットワークにおけるセキュリティを分析すると、次のようになります。

基本は NAT による incoming packet の制限で、ほとんどのユーザはデフォルト設定以上のことはまずできません。無線 AP がデフォルト設定のまま設置され、フリースポットを提供してしまうなどが発生しています。non-PC（HDD ビデオ、ネットワーク対応カメラ等）はインターネット上の特定サーバと通信（Proxy、定期的なメール Polling）することで、外部ネットワークからの脅威を防いでいますが、 PC 同等のセキュリティ機能を実装していないケースが多く、いったんホームネットワークに WORM 等の侵入を許すと、被害を受ける可能性が高まります。

現在のセキュリティ対策　~独立 SOHO~

独立 SOHO は、典型的には下図のような構成でネットワーク接続しています。



独立 SOHO においてネットワーク接続される機器は、PC、プリンタ、専用端末、業務サーバ、NAT ルータなどです。

利用内容は、社外とのメール送受信、インターネット経由での Web 閲覧、ASP 利用や自前構築による販売用 Web サイト等です。

利用アプリケーションとしては、Web ブラウジング、メール、ASP、プリンティング、リアルタイムアプリケーション、ストリーミング、アップデートツールなどがあります。

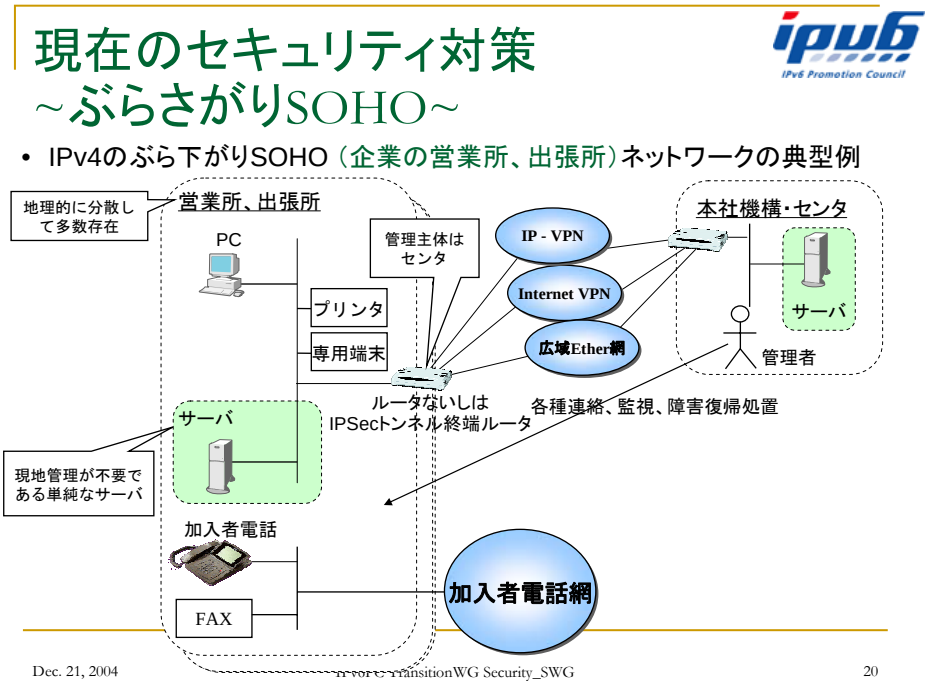
セキュリティ対策は、基本的にホームネットワークでとられている対策と同じです。

独立 SOHO におけるセキュリティを分析すると、次のようになります。

ホームネットワークに比べると運用者の技術スキルは期待できますが、中途半端な運用は、顧客情報の漏洩などを引き起こし、家庭以上の損害を与えかねません。また、自前で販売用 Web サイトを構築しているケースなどでは、NAT ルータに固定のグローバルアドレスが付与されるため、NAT ルータの処理能力から DoS には弱いといえますし、セキュリティパッチの更新が遅れると、80 番 port を通過してくる不正コード等によりで LAN 内の情報資産が漏洩する可能性があります。

現在のセキュリティ対策　~ぶらさがり SOHO~

ぶらさがり SOHO の接続構成は、下図のようになります。



ぶらさがり SOHO でネットワーク接続される機器は、PC、プリンタ、専用端末、業務サーバ、NAT ルータ(IPsec 機能搭載)などです。

ネットワークの基本的な構成は独立型 SOHO と同じですが、管理者のいる企業センタと IP-VPN、インターネット VPN、広域イーサネット網などを介して接続しています。インターネットとの接続は企業のセンタ拠点経由で行われています。

利用アプリケーションは、センタとの連携システムのほかは独立系 SOHO と同様で、Web ブラウジング、メール、ASP、プリンティング、リアルタイムアプリケーション、ストリーミング、アップデートツールなどです。

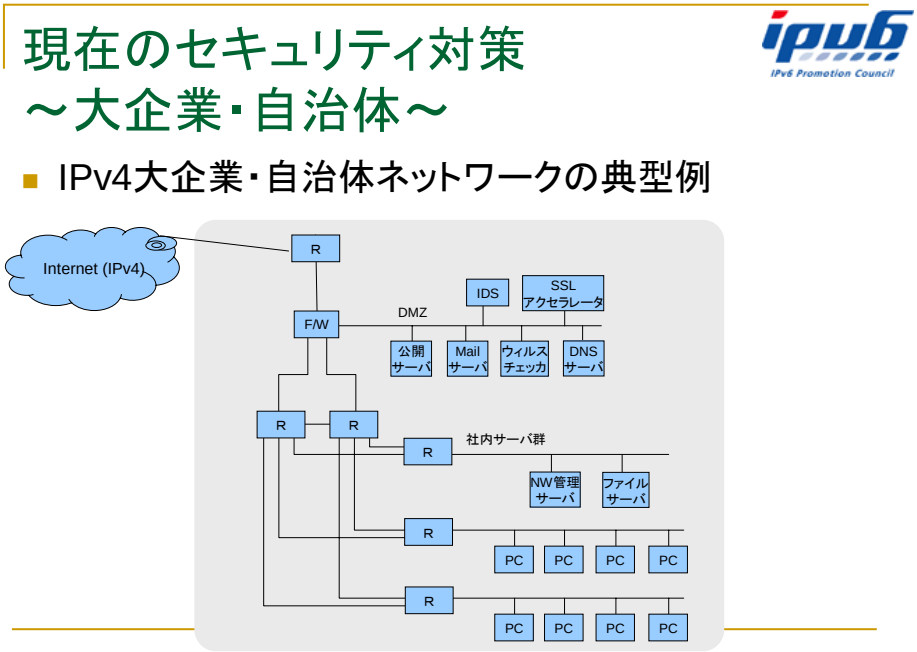
ぶらさがりSOHOでは、基本的に企業イントラネットの一部と見なせるため、イントラ内の端末、サーバと同じ対策がとられています(大企業/ 自治体セグメントを参照)。

ぶらさがり SOHO のセキュリティを分析すると、次のようになります。

基本的には企業イントラネットの内容と同じです。 ただし、インターネット VPN を利用するケースは、VPN ルータの処理能力から、WAN 側グローバルアドレスに対する DoS への耐性は低いと言えます。IPsec ポリシーの記述ミス、簡易な Preshared Key の設定が、不正者からの VPN 接続を許す危険性もあります。

現在のセキュリティ対策　～大企業・自治体～

大企業や自治体の典型的な接続構成は、下図のようになっています。



大企業・自治体ネットワークの特徴は以下の通りです。

全体ネットワークを特定の専任部門が管理している、ユーザ数が数十人以上の比較的大規模なネットワークで、組織内にイントラネットが存在しています。そして、組織内部、もしくは組織外部に対して、メール、WEBなどのアプリケーションサービスを提供しています。

こうした組織では、費用対効果が、特に強く求められます。

セキュリティポリシーは、ネットワーク部門が厳格に維持管理しています。ネットワーク設備に不具合が発生した場合、社会的・組織的に影響度が大きい（冗長構成、定期的な設備メンテナンスの必要性）という側面があります。

ネットワークに接続される機器は、PC、各種サーバ、ルータ、スイッチ、IDS、ファイアウォール、アンチウィルスゲートウェイ等です。

利用内容は、社内外とのメールの送受信、プロキシを介した社外 Web アクセス、社内業務サーバでのファイル/DB 共有、外出先からのメール／グループウェア（スケジューラ等）へのアクセスなどです。

実施されているセキュリティ対策としては、まずファイアウォールで内部ネットワークへのアクセスを遮断しています。そして、社内から社外へはサーバ（http/ftp プロキシ、メール、名前解決）を介して接続し、内部ネットの隠蔽とウイルス／コンテンツチェックを実施しています。メール/グループウェアへのリモートアクセスは、RAS へのダイヤルアップ、インターネット VPN（SSL、IPsec）が一般的で、VPN 接続認証（ID/Password が主流）によるアクセス制御が行われています。

大企業・自治体のセキュリティを分析すると、次のようになります。

現在の利用内容では必ずしも内部ネットワークと外部ネットワークが直接通信する必要はなく、上記の対策モデルが定着しています。内部もグローバルアドレスの企業イントラネットでは、http/ftp プロキシを設置しないケースもあります（ポリシー依存）。

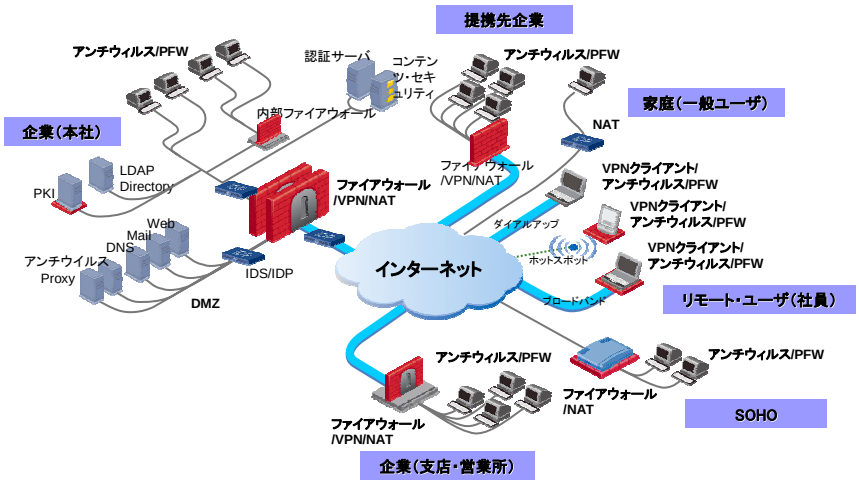
一方、上記のモデルは内部被害には脆弱であることが指摘されており、持ち出し PC による情報漏えいや、持ち込み PC による内部感染の被害に対し、ファイル自体の暗号化/操作制限、脆弱性の検疫など、事前の防御が必要となります。

現在のセキュリティテクノロジー

現在のセキュリティテクノロジーは、どのような脅威への対策になっているでしょうか。それを利用することによる副次的な効果とリスクは何でしょうか。

IPv4 のセキュリティテクノロジーには、境界ファイアウォール、PFW（Personal ファイアウォール）、プロキシ、IDS/IPS、アンチウイルス、NAT、VPN などがあります。

IPv4における利用環境



それぞれのセキュリティ技術は、次のような特徴を持っています。

IPv4のセキュリティテクノロジーのまとめ

名称	概要	主な製品名
Firewall	外部(Internet)から内部(LAN)への不正侵入を防ぐ目的で設置されるルータやサーバ等。外部からの通信を必要最低限に制限し、内部のPC等を外部の攻撃から防ぐ役割を持つ	Check Point Firewall-1 Cisco PIX
PFW	上記Firewallをクライアント PCレベルで実装した製品。クライアントPC個々への外部からの不正侵入を防ぐ目的でクライアントPC上に実装。	Trend Micro ウイルスバスターシリーズ
DMZ	Firewallの内側にあり、外部(Internet)と内部(LAN)とも切り離されたネットワークを指す。DMZ上に外部公開用のWeb Server等を設置することでDMZ上のサーバには外部からの接続を許すが、内部への接続を防ぐ機能を実現可能にする。	
Proxy server	外部への接続時、セキュリティを確保するために設置されるサーバ。Firewall内部のクライアントからアクセス要求(HTTP、FTPなど)を受け付け、クライアントの代理として外部リソースへアクセスするサーバー	Squid DeleGate
IDS/IPS	IDSとは侵入検知システムのこと。外部(Internet)や許可されていないネットワーク、ホストからの不正侵入などを検知し、管理者に警告する機能。 IPSとは、IDSの機能に加え、不正進入に対して動的に防御を実施する機能を有す。不正進入が発生した場合、検知しその不正進入を遮断する機能。	TripWire Internet Security Systems RealSecureシリーズ

IPv4のセキュリティテクノロジーのまとめ（Cont.）

名称	概要	主な製品名
アンチウィルス	コンピュータの破壊等を目的としてコンピュータの進入するコンピュータウイルスを検知・駆除するソフトウェア。	Trend Micro ウイルスバスターシリーズ Symantec Norton AntiVirusシリーズ
NAT	内部（LAN）で使用するプライベートIP Addressを外部（Internet）へ接続するためグローバルアドレスへ変換する技術。NAT配下のコンピュータに対し外部から透過的に接続することができないため、現在NATも有効なセキュリティ対策機能の1つとなっている。	BBルータ等に搭載
VPN	インターネットでは通常暗号化や認証を行わないためセキュリティレベルが高いとはいえないが、そのインターネット回線を利用し、あたかも専用線のように拠点間で相互接続をおこなうための技術。相互拠点間で取り決めた暗号化方式やユーザ認証方式を使用しインターネット上に暗号化されたパケットを流すことでセキュリティレベルを高め各拠点間で通信をおこなう。途中パケットが盗聴されても暗号化されているためセキュリティレベルが保たれることとなる。	NetScreen製、Cisco社等各社から販売されているルータ等に搭載

以下で、これらそれぞれについて、より詳しく説明します。

境界ファイアウォール

境界ファイアウォールは、内部のマシンで動作しているサービスの不正利用、侵入、攻撃を防ぐために、外部から内部への不要な通信を停止する機能を果たします。これに付帯して、DMZ 等のセグメント化や認証が行われます。

内部から外部への攻撃（SMTP エンジンを持つウイルスが外部へ流れる等）を防止することも求められ、これについても必要な通信のみを許可する機能を果たします。

副次的な効果としては、通信状況の把握が容易（集中管理）であり、マシン毎の対策に比べ低コストでの対策が可能になります。

リスクとしては、持ち込み PC による内部への被害伝播や、許可したサービスによる侵入(ワーム、ウイルス)を防ぐことができないこと、そしてトンネル化された通信の検査ができない(素通り)場合がある等が挙げられます。

PFW（Personal ファイアウォール）

パーソナル・ファイアウォールは、マシンで動作しているサービスの不正利用、侵入、攻撃を防

止するために、不要/不正な通信を停止する機能を備えています。

不正な通信の発生に関しては、無意識の攻撃者となることを防止し、外部への不正な通信停止、不正なプログラムからの通信を遮断します。

副次的な効果としては、持ち込み PC による内部からの攻撃にも対応します。

リスクは、個人によりセキュリティレベルが異なること、管理が困難であること、クライアント数に応じコスト増となること、などです。

Proxy

プロキシは、危険なサイトへの接続を防ぐため、接続先 URL、IP 等によるフィルタリングを行います。また、危険なファイルのダウンロードを防ぐため、コンテンツをチェックします。

また、内部情報の収集を防止するという点では、クライアント IP(トポロジ)の隠匿が実施できます。

副次的な効果としては、HTTP や FTP などの接続を集中管理できる、コンテンツアクセスの高速化（キャッシュ）が可能、などがあります。

リスクとしては、負荷が高いこと、そしてサービス(プロトコル)が限定されること、が挙げられます。

IDS/IPS

IDS（不正侵入検知）や IDP（不正侵入保護）は、DoS、ポートスキャン、ワーム等の不正アクセスに対する防御を提供します。不正の検出と防御には、シグネチャ（不正アクセスのパターンファイル）が使われます。IDS による防御はファイアウォールとの連携が必要です。

リスクとしては、誤検知によるサービス停止があります。また、シグネチャが出るまで対策できない、IDS/IDP を設置したセグメントのみしか対策できない、があります。

アンチウイルス

アンチウイルス製品は、ウイルス、ワーム等の感染防止を目的としています。

リスクとしては、新しいウイルスへの対策までの時間差があることと、端末によっては最新パターンへの未アップデートが発生しやすいこと、が挙げられます。

NAT

マシンで動作しているサービスの不正利用、侵入、攻撃を、内部への直接の接続性の遮断によって防止します。内部情報の漏洩（攻撃を行なうための情報として利用）を、クライアント IP アドレス(トポロジ)が隠匿できる点があげられます。

副次的な効果としては、安価なブロードバンドルータにも実装され低コストであること、ネットワークに変更を加えずに、容易に接続端末を増やすことができる（アプリケーションは制限を受ける）ことが挙げられます。

リスクとしては、持ち込み PC による内部への被害伝播や、Web、メール利用によるワーム、ウイルス感染と攻撃があります。

VPN

VPN は、盗聴、改ざん、なりすましの防止を実現します。IPSec によるインターネット VPN では IKE を用い、PKI 認証も一部で使われています。

利点は、専用線と比較し安価な WAN を利用できることで、インターネット VPN の場合、インターネット接続性さえあれば柔軟・迅速に構築できます。

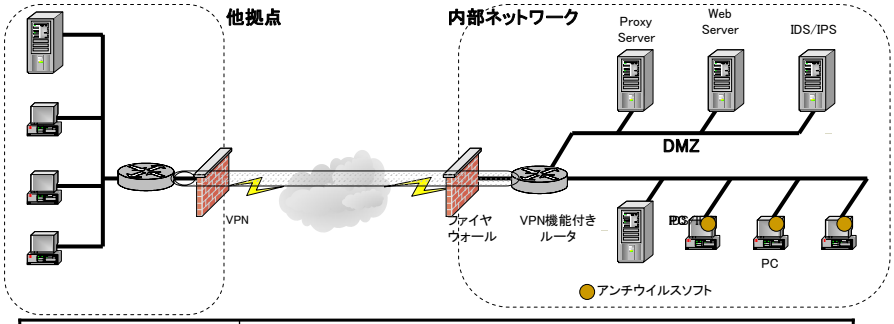
リスクは、（可能性として）暗号はやぶられるということ、そして VPN ゲートウェイが DoS に弱いといったことが挙げられます。

セキュリティテクノロジーマップ

上に説明したテクノロジーは下図のように位置づけられます。

セキュリティテクノロジーマップ

対策ポイント（レイヤ）別のセキュリティテクノロジーを以下に示す



レイヤ	セキュリティ製品
Internetレイヤ	Firewall、VPN、NAT
DMZレイヤ	Proxy、IDS/IPS
内部レイヤ	IDS/IPS、アンチウイルス、PFW

対策の傾向

以下では、セキュリティ技術の変遷と昨今の傾向につき、次の項目に分けて解説します。

- ネットワークレイヤからマルチレイヤへ
- 本人認証の高度化
- VPN の多様化
- コンテンツ・セキュリティ
- 事後から事前の防御へ
- 侵入検知の高度化
- 対策は境界から内側へ
- 分散セキュリティと管理の重要性
- 単体技術からアーキテクチャへ

ネットワークレイヤからマルチレイヤへ

これまでは、IP パケットのヘッダ情報を主な条件としたアクセス制御が実施されてきました。IP パケットの改変や偽造による攻撃や、サービス不能攻撃からネットワークを保護するというのが中心的な目的です。

現在の傾向としては、アプリケーション、OS の脆弱性を利用する攻撃の急激な増加と高度化が見られます。このため、アプリケーション層を含むマルチレイヤの認識と防御が求められるようになって来ています。つまり、パケットの検査からストリームの検査へという流れが見られます。

本人認証の高度化

認証を条件としたリモートアクセスの提供により、企業ネットワークなどに対するアクセス範囲の拡張が行われてきました。こうした認証においては、静的なパスワード、ワンタイム・パスワード、2 ファクタ、トークンなどが利用されています。

現在の傾向としては、証明書（PKI）やバイオメトリックスの利用が増加してきています。その人しか持ち得ないものとの組み合わせで認証を行うことの重要性に関する認識が高まっており、その一方で、複数システムにおける認証情報の共有（シングルサインオン）も要求されるようになって来ています。

VPN の多様化

VPN については、製品に利用される暗号化方式やアルゴリズムがベンダ固有のものであり、互換性の確保が困難であることや、鍵長による輸出（入）制限があったことなどの課題が指摘されてきました。

しかし、サイト間 VPN、リモートアクセス VPN によるイントラネットの拡張は積極的に進められてきており、IPSec の標準化は進み、相互運用性は向上しています。エクストラネットへの拡張もニーズとしてはっきりしてきています。鍵長の増大と新しい暗号化アルゴリズムの登場も見られます。

現在の傾向としては、増え続けるサイトに対する正確かつ容易な VPN の運用管理が要求されるようになってきており、VPN ルーティングも課題の 1 つとなっています。また、IPSec、SSL-VPN、拡張 SSL-VPN といった手法のなかから、個々のアクセスニーズや条件に最適なリモートアクセス実現手法を選択する必要性も高まっています。

コンテンツ・セキュリティ

コンテンツレベルでのセキュリティに関しては、おもにアンチウイルスや URL フィルタリング、迷惑メールのフィルタリング、悪意のあるプログラム（JAVA/ActiveX）からの保護が実施されてきました。

現在の傾向としては、情報漏えい防止ツール（メール内容のチェック）の利用、著作権保護技術の活用（DRM、電子透かし）、コンテンツ操作を制限する専用ビューワなどが挙げられます。

事後から事前の防御へ

これまで、攻撃が認識されたあとにシグネチャ・ベースによる防御が行われていましたが、 脆弱性の発見から攻撃までの時間が非常に短くなってきています。また、ウイルスなどでは無数の亜種が存在し、迅速な対応を困難にしています。

現在の傾向としては、脆弱性の根本的な解決による事前の防御に力を入れる傾向が強まっており、併せて根本的な解決を含むセキュリティ知識ベースの更新が必要になってきています。

侵入検知の高度化

侵入検知技術は、大きく発展してきています。ネットワーク型 IDS、ホスト型 IDS の製品の一部は、侵入検知を実施するだけでなく、不正侵入からネットワークやホストを守る IPS としての機能を強化してきています。また、不正侵入者を仮想ネットワークに誘い込む「ハニーポット」と呼ばれるツールも提供されるようになっています。

現在の傾向は、シグネチャ・ベースの事後対応から事前の防御への進化ですが、これには同時に精度の向上も求められます。

対策は境界から内側へ

セキュリティ対策は、これまでネットワークの境界にフォーカスしてきました。これを基本として、アンチウイルスの導入や、IDS による監視が適用されてきたのが現状です。

しかし、現在の傾向としては、内部における脅威の発生や情報流出の被害が強く認識されるようになってきています。内部における被害の最小限化のためには、セグメント化の有効性も指摘されるようになって来ました。ここでは、隔離が 1 つのテーマとなっています。

分散セキュリティと管理の重要性

企業ネットワークでは、ネットワーク構成の変化に伴って、単一の境界セキュリティ・ポイントから支店など複数のセキュリティ・ポイントへの分散が見られるようになって来ています。このため、複数のセキュリティ機能とコンポーネントの運用が必要になってきています。公開セグメント、内部、エンドポイントの多段的セキュリティ展開が重要性を増しています。

現在の傾向としては、一対一の複数管理から一対多の中央集中管理への変化が見られ、ネットワーク全体をカバーするセキュリティ管理が求められています。スムーズなセキュリティ運用サイクルの必要性も増大しています。

単体技術からアーキテクチャへ

従来の対策の方法は、セキュリティ問題について対策機能を羅列していくことが基本になってきました。しかし、こうした方法では、隙間の発生を回避することが困難でした。

そこで、現在の傾向としては、脅威の内容、発生源、事前の防御、被害の最小限化、事後の対応、修復・改善を取り込んだアーキテクチャによるセキュリティ設計が進められようになってきました。

総論、総括

セキュリティ対策における最近の傾向としては、アプリケーション・レベルの脅威に対してマルチレイヤのセキュリティ対策の必要性が認識されてきていることが挙げられます。よりアプリケーション内部の検査（タグ、コマンド）や、80 番 port 上での悪意のあるコードのブロックなどが重要視されるようになりました。

先制的な事前の防御が求められるようになり、その一環として検疫による脆弱な端末の隔離も行われるようになって来ています。

境界だけでなく、内部、エンドポイントによる多段的な防御と分断も最近のセキュリティ対策のテーマであり、境界から内部セキュリティ対策に意識が広がっているほか、攻撃され感染した端末の隔離（被害の最小化）にも関心が高まっています。

一方、正確かつ迅速に対処可能な管理の重要性が説かれています。ポリシーによる集中管理と各セキュリティ・ポイントでの検知の迅速化、さらにセキュリティ運用サイクルをスムーズにする管理が求められています。

2. IPv6 のセキュリティ分析

本章の目的は、IPv6 がセキュリティに及ぼしうる影響をできるだけ網羅的に取り上げ、実際のセキュリティ対策を検討する際に、使われ方によっては、これらの影響が起こりうる可能性があることを知ってもらうために記述しています。

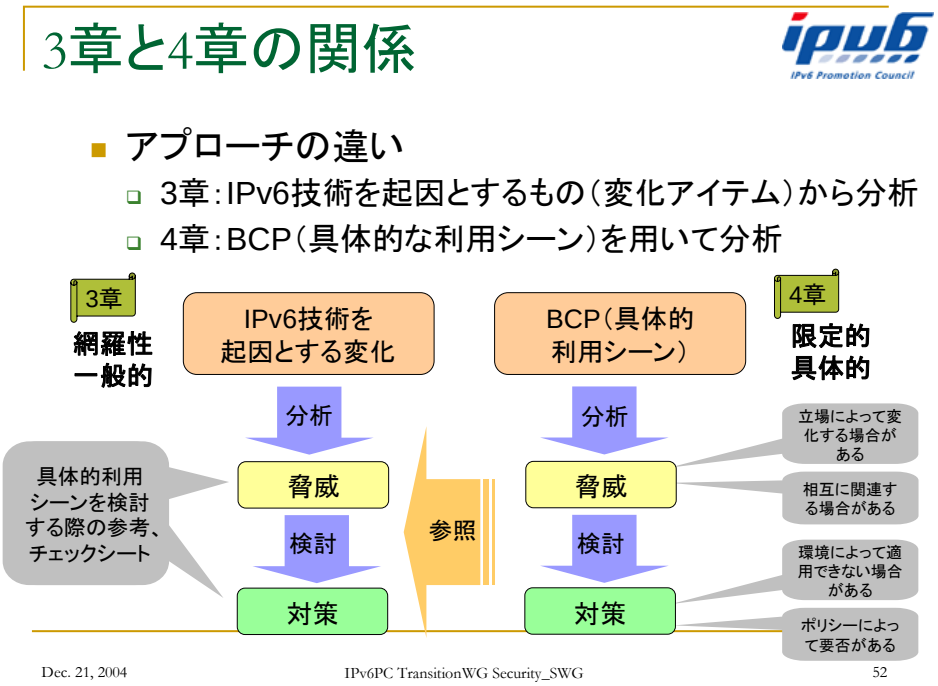
実際には、 全ての対策が求められる訳ではなく、個々の利用シーンや利用者の立場/ポリシーによって、その対策の内容/レベルは異なってきます。

個々の利用シーンでの分析・評価については 4 章を参照してください。

本章のアプローチは、IPv6 で何が変わるのか、つまり、“IPv6 技術”を起因とした変化を分析するというものです。

内容としては、個々の変化が及ぼすセキュリティへの影響（脅威）の分析、それに対する対策指針の提示、今出来る具体的な実現方法（例）の記述、IPv6 普及期への課題と提言を扱います。

この 3 章と、後に続く 4 章の違いは、アプローチにあります。3 章では、IPv6 技術を起因とするもの（変化アイテム）から分析し、4 章では、BCP（具体的な利用シーン）を用いて分析します。



IPv6 による変化

下の表は、IPv6 への移行がもたらす変化と、これによって引き起こされるセキュリティ上の脅威についてまとめたものです。それぞれの項目については、表に続いて詳細に解説します。

IPv6による変化（その１）

アイテム	変化	サブアイテム	脅威
A	グローバルアドレスにより直接の到達性が得られる	A-1	誰もがサーバ（レスポンダ）になり得るためアプリケーションの脆弱性による被害がより顕在化する
		A-2	直接の到達性が得られることからネットワーク内部までDOSを受けうる範囲が広がる
		A-3	P2Pアプリの利用環境が広がるが、通信元アドレス、受信ポートの範囲が広いためDOSを受けやすくなる
		A-4	E2Eの暗号化通信（IPsec等）が簡単になるが、経路上でパケット内を検査することは出来ないため、情報漏えい、ワーム感染を許してしまう危険性がある
B	IPアドレスそのものが持つ情報量が増える	B-1	Eui-64使用時の端末一意性により利用者の活動状況が把握されやすくなる
		B-2	IPアドレス入力時のヒューマンエラーの頻度が高まる

IPv6による変化（その２）

アイテム	変化	サブアイテム	脅威
C	固定プレフィクス環境が広がる	C-1	通信ログを紐付けることでプライバシーが漏洩する
		C-2	外部から特定される確率が高まり不正アクセスを受けやすくなる
D	匿名アドレスが利用可能になる	D-1	被管理者の管理・特定が難しくなる
E	端末が複数のプレフィクスを持ちうる	E-1	アクセス制御運用が難しく、不正アクセスを助長する
F	端末が複数のインタフェースIDを持ちうる	F-1	アクセス制御運用が難しく、不正アクセスを助長する

IPv6による変化（その3）

アイテム	変化	サブアイテム	脅威
G	E2EでのICMPv6通信	G-1	不正NDPパケットを送ることにより通信異常を引き起こすことが可能
		G-2	ICMPv6 ErrorはE2Eで疎通するため、ネットワーク管理者が管理できないbackdoorにもなりうる
		G-3	RAに認証の仕組みがないため、L2的侵入によりネットに接続され、不正アクセスの原因となりうる
H	デュアルスタック端末（トランスレータ、プロキシ含む）が増加する	H-1	当該端末が属するIPv4ネットワークとIPv6ネットワークのセキュリティレベルが異なる場合、デュアルスタック端末を踏み台とした被害が伝播する
		H-2	アンチウィルスがIPv6未対応の場合、デュアルスタック対応したアプリケーションの使用により、ワーム感染する可能性がある

IPv6による変化（その4）

アイテム	変化	サブアイテム	脅威
I	トンネルプロトコルが導入される	I-1	トンネルプロトコルにより、境界Firewallで定義したアクセス制御を素通しして、内部への到達性を与えてしまう
		I-2	トンネルサーバへのDOSによる処理能力低下
J	マルチキャストの利用環境が広がる	J-1	マルチキャスト送信による無差別攻撃
		J-2	マルチキャストへの応答を用いて端末アドレスを推定することにより、端末を狙い撃ちした攻撃が可能
		J-3	マルチキャストへの応答を用いたDDoSが可能
		J-4	大量のグループに関してマルチキャスト参加要求することにより、ルータのマルチキャスト経路表を溢れさせ、マルチキャスト通信を止めることが可能

IPv6による変化（その5）

アイテム	変化	サブアイテム	脅威
K	nonPC端末（シン・クライアント）がネットに繋がる	K-1	出荷時の実装を超える脅威に対する対処が難しい
		K-2	マシンのスペック面から十分なセキュリティ実装が難しく攻撃によるサービス停止が生じやすい
L	モバイルIPの利用環境が広がる	L-1	Care of Addressがネットワーク外部の場合、アクセス制御が難しい
M	IPアドレスに対する逆引きレコードが存在しないことが多い	M-1	逆引きによるユーザ認証が事実上不可能

以下では、上の表に示された変化と脅威を、1 つ 1 つ詳細に解説します。以下の説明は、次のような構成で行います。

概要

- 脅威の概要を記述する。
- 変化と脅威の因果関係。どこ（発生ポイント）で、どのような脅威（想定される被害）が起こりうるのか。

脅威の種類

- 脅威の種類（副次的、二次的でない直接的なもの）をキーワードで記す。複数選択 OK。
- キーワード：情報漏えい、なりすまし、盗聴、サービス停止、改ざん、踏み台、不正コード侵入（ワーム）、管理不能、検知不能など

脅威の分析

- 問題の本質（何に起因するのか、 IPv4 でも同じ脅威か）、発生頻度、被害の深刻度を記述。
- 立場や考え方の違いによりメリットにもなりうる場合は、可能な限りここでコメント。

対策の指針

・ 対策の考え方（心得）を記述。
・ それにより影響を受ける（派生する）事項がある場合は、ここでコメントする。

実現方法
・ 対策の実現性を見るために、サポートしている製品や、既存手段による解決方法を記述。

IPv6 普及期への課題と提言
・ 実現方法がない場合、課題として今後どういったものが求められるか記述。
・ また IPv6 普及期に求められる内容、提言を記す。

A-1

概要
これまで NAT 配下の端末はイニシエータにしか成りえず、不用意にサーバアプリケーションを起動していたとしても直接アクセスを受けることはありませんでしたが、IPv6 でグローバルユニキャストアドレスが各端末に割り振られた場合、各端末が簡易にレスポンダになることが可能となることから、アプリケーションの脆弱性を狙った被害がより顕在化する恐れがあります。

脅威の種類
不正コード侵入（ワーム）

脅威の分析
適切なセキュリティパッチの更新がなされているかが根本原因であり、アプリケーション・レベルでの接続は NAT 配下であろうが状況は同じといえます。
なお、アドレス範囲が広いため、第三者から特定されにくい（外部 DNS に登録しない、狙われやすいアドレス（::80 など）を使用しない）対策により、脅威は低く見積もることができます。

対策の指針
セキュリティパッチの更新による脆弱性の低減。アクセス制御による通信元の限定。
公開サーバの場合は、セグメントの分離など感染時の被害伝播を防ぐ対策が必要となります。

実現方法
セキュリティパッチの更新と、IPv6 対応 IDS、IPv6 アプリケーションに対応したファイアウォールの導入が求められます。

IPv6 普及期への課題と提言

IDS と連携したファイアウォールや IDP の IPv6 対応が必要となります。

A-2

概要

直接の到達性が得られることから、ネットワーク内部まで DoS を受けうる範囲が広がります。

脅威の種類

DoS 攻撃

脅威の分析

アドレス範囲が広大なので、DOS 攻撃前の情報収集（ポートスキャン、ブルートフォース攻撃）に時間が掛かり、効率が悪いといえます。

対策の指針

外部からのアクセスを監視し、特定パケットをブロックすることが基本となります。

実現方法

境界ルータ、ファイアウォールなどで不必要な外部からのアクセスを遮断します。外部からのトラフィックなどをロギング・監視することにより、不慮の障害時に対策を施すための情報収集・警戒を怠らないことが重要です。

IPv6 普及期への課題と提言

IDS と連携したファイアウォールや IDP の IPv6 対応が必要です。

A-3

概要

P2P アプリの利用環境が広がりますが、通信元アドレス、受信ポートの範囲が広いため DoS 攻撃を受けやすくなります。

脅威の種類

DoS 攻撃

脅威の分析

アドレス範囲が広大なので、DoS 攻撃前の情報収集（ポートスキャン、ブルートフォース攻撃）に時間が掛かり、効率が悪いという点が指摘できます。侵入を許した場合は、内部セグメントおよび通信ログの解析から他の Peer へ被害が拡大する恐れがあります。

対策の指針

外部からのアクセスを監視し、特定パケットをブロックする、外部からのアクセスを許す端末はセグメントを分ける、といった方針で対策を立てます。

実現方法

指針のとおりです。また、外部からのトラフィックなどをロギング・監視することにより、不慮の障害時に対策を施すための情報収集・警戒を怠らないことが大切です。

IPv6 普及期への課題と提言

IDS と連携したファイアウォールや IDP の IPv6 対応が必要です。また、プレゼンス管理機構とファイアウォールとの連携による Stateful なアクセス制御の仕組みも有望視されています。

A-4

概要

E2E の暗号化通信（IPsec 等）が簡単になりますが、経路上でパケット内を検査することはできないため、情報漏えい、ワーム感染を許してしまう危険性があります。

脅威の種類

情報漏えい、不正コード侵入（ワーム）

脅威の分析

IPsec が、IPv6 プロトコルスタックで標準に実装されること、そして IPv4 と違い NAT 環境での接続でないことから、IPsec の利用頻度が高まると考えられます。
IPsec では TCP/UDP ヘッダ部も暗号化されてしまうため、これらのプロトコルに対する既存のアクセスフィルタが適用できなくなります。

対策の指針

組織のセキュリティポリシーとして、外部との IPsec 通信は通信先を制限しておきます。ただし、これは E2E で IPsec を使うようなサービスの普及の阻害要因となります。

実現方法

ファイアウォールや境界ルータで、不必要な通信先との IKE、IPsec プロトコルを遮断します。

IPv6 普及期の課題と提言

IPsec を許可する端末のポリシー管理ソリューションと、エンドポイントでのコンテンツチェック機構（アンチウィルス、コンテンツフィルタ）が必要となります。

B-1

概要

インタフェース ID として使用される EUI-64 は、端末の MAC アドレスをベースに生成されますが、この EUI-64 の一意性により、利用者がいつどこで活動していたかの状況が把握されやすくなります。

脅威の種類

プライバシー漏洩

脅威の分析

複数の外出先で、 ステートレスアドレス自動設定を利用してアドレスを取得し、ネットワークに接続した場合に起こりえます。電子メールのヘッダ情報、HTTP メール表示による特定ホストへの無意識のアクセス、不特定者との P2P アプリケーション利用のログにより活動状況を解析されるケースが考えられます。

対策の指針

不必要に不特定者との通信を行わない心がけが重要です。インタフェース ID の一意性を隠蔽すること、またはアプリケーション利用ログから IP アドレス情報を削除することも有効です。

実現方法

匿名アドレスや DHCPv6 を利用します。あるいは端末アドレスを隠蔽するため、プロキシを利用します。

IPv6 普及期の課題と提言

現在のアプリケーションの実装はまちまちですが、RFC3484 では一時的アドレスより恒久的アドレスを優先するとされています。利用者のポリシーに従い、ソースアドレスを変更できる仕組みが望ましいと考えられます。

B-2

概要

ユーザインタフェースで IPv6 アドレスを手入力するシステムや機器では、IPv4 に比べ入力ミスが増える可能性があり、システムの信頼性低下や、不正アクセスの口の提供につながりかねません。

脅威の種類

システムの信頼性低下、不正侵入の口を広げる

脅威の分析

システムや機器のユーザインタフェースにもよりますが、ユーザインタフェースで IP アドレス入力を多用するシステムや機器では、アドレスの誤入力によりシステムが正常動作しないといった影響が起こりえます。ファイアウォールやルータなどでは、IP フィルタの記述ミスが不正アクセスの口を提供することになります。

対策の指針

不必要な IP アドレスの手入力をなくす必要がああります。 また、IP アドレス入力を多用するシステムでは、IP アドレスと対応付けた識別子（host name）などによりヒューマンエラーを低減するとよいと思われます。また、Neighbor Cache などの接続端末情報と突合する仕組みも有効です。

実現方法

システムや機器のユーザインタフェースに依存しますが、それほど難しいものではありません。なお、現在のパーソナル・ファイアウォールには、IPv6 アドレスを意識しない（サービスのみの制御）タイプがあります。

IPv6 普及期の課題と提言

IPv6 普及時には、IP アドレスを不必要に入力しなくてすむツールやユーザインタフェースが望まれます。

C-1

概要

一般的な ISP 接続サービスにおいても、IPv6 アドレス(prefix)が固定的に割り当てられるため、利用者のアクセス動向などが IPv6 アドレスを元に収集される危険性があります。

脅威の種類

プライバシー漏洩（アクセス動向の分析）

脅威の分析

従来までの DHCP による動的アドレス割り当てにおいても、ISP 側のセッションログをつき合わせることで IP アドレスから利用者の特定をすることは不可能ではありませんが、セッションログの開示がなければ、第三者からの利用者追跡は困難です。IPv6 サービスによってプレフィックスが利用者ごとに個別に割り当てられることによって、第三者でも利用者の特定がやりやすくなります。IPv6 アドレスのアドレス集約構造により、地域情報や上位 ISP などを容易に特定することも可能となります。また、電子メールヘッダに含まれるアドレス情報とメールアカウントの紐付け、SPAM メール内に仕掛けられた URL リンクからのアクセス誘導など複合的な手法により、固定的な IPv6 アドレスをキーとして情報の紐付けが容易になります。

外部の信頼できないサービスなどについては、匿名アドレスを用いてアクセスすることも対応策の一つとなります。しかし、企業など同一プレフィックスのネットワークセグメント内に多数の端末がある場合には、個々の端末ごとの挙動や振る舞いを隠蔽することが可能なものの、家庭や SOHO では、端末の特定を防ぐ効果はあっても、組織・家庭の挙動やネットワーク利用動向などを収集されることからの防御としては prefix 内の端末数が十分に多くないため効果がないと考えられます。

.

対策の指針

不必要に IP アドレスを外部に漏洩しないようにします。

実現方法

メールサーバの設定で、メールヘッダの Received 行で、クライアントの IP アドレスが表示されないようにします。また、メールクライアントの設定で、メールヘッダの Message-ID 行で、クライアントの IP アドレスが表示されないようにします。あるいはアプリケーションプロキシを利用することによって、外部へアクセスする際の IP アドレスを制限します。

IPv6 普及期の課題と提言

IPv6 の普及によって、攻撃者が IPv6 アドレスの収集や攻撃対象として選択する機会が増大します。IPv6 の移行期と IPv6 普及期で、脅威の内容や対策に関する変化はありません。

C-2

概要

固定プレフィックス宛にパケットを投げることにより、攻撃することが可能です。

脅威の種類

不正侵入、DoS(DDoS)

脅威の分析

<Prefix>::1 といったような、慣例的によく使われるアドレスに対して、DoS 攻撃を受ける危険性があります。また、IPv6 アドレスの収集などを組織的に行うことによって対象リスト（128 ビットアドレス）を作成して攻撃することが可能です。ブルートフォース攻撃は、端末に到達する可能性は低いものの、SOHO ルータにおける NDP 解決自体の負荷をもたらすため、DoS になりえます。

IPv4 環境では固定的なグローバルアドレスは各種サーバに限定されていましたが、こうした攻撃の対象となるノード数が IPv6 では増大します。それにもかかわらず、正しくセキュリティ対策をされていない脆弱なノードがネットワーク上に多く存在するようになることが予想されます。これらの端末を踏み台にした DDoS 攻撃など、より大規模な分散攻撃の発生が起こる危険性があります。

.

対策の指針

外部からの到達性のある固定アドレスを持つ端末に対しては、ファイアウォールなど十分なセキュリティ対策と管理を行う必要があります。

同時に E2E 通信を行う利用する場合には、境界内部の端末への外部の不特定多数からの通信を許可しなければなりません。対応策としては、パケット監視などにより、E2E 通信のセッション確立・認証シークエンスを監視することによって、動的に一時的に内部への通信を許可するなど、動的に境界ファイアウォールのルールを制御するような仕組みが必要となります。また匿名アドレスと併用することによって、外部から特定の端末に対する DoS や攻撃などの危険性をある程度防ぐことが可能となります。

実現方法

境界ルータ、ファイアウォールなどで不必要な外部からのアクセスを遮断します。E2E 通信サービスを利用する場合には、不特定多数から直接境界内部の機器へ通信が行われることを考慮し、端末側にセキュリティ対策を施します（ホストベースのファイアウォールなど）。外部からのトラフィックなどをロギング・監視することにより、不慮の障害時に対策を施すための情報収集・警戒を怠らないようにします。

組織外部へのアクセスについては、攻撃を受ける危険性を軽減する手法として、匿名アドレスを利用することも検討できますが、この問題を完全に解決するものではありません。また、E2E 通信を指向するアプリケーションサービスでは、匿名アドレスが障害となることが考えられます（匿名アドレスの変更のたびに、自身のアドレスを再登録するなどの処理が必要となる）。

IPv6 普及期の課題と提言

IPv6の普及によって、攻撃者がIPv6アドレスを収集したり、攻撃対象として選択する機会が増大します。IPv6 の移行期と IPv6 普及期で、脅威の内容や対策に関する変化はありません。

D-1

概要

企業内ユーザが匿名アドレスを利用すると、IPv4 のネットワーク管理で実施してしてきた「各種アクセスログからユーザを特定する」ことが困難になります。

脅威の種類

管理不能

脅威の分析

匿名アドレスは、ホストがアドレスの下位 64 ビットを、乱数を用いて生成し、ある一定間隔で変更することで、ホストのトラッキングをしにくくする方式です。企業内における利用を想定した場合、社外との通信でユーザが特定されない一方で、不正アクセス等の問題発生時にユーザの特定が難しくなるという課題が生じます。例えば、以下の2つのケースが考えられます。

⑴企業内サーバへ、社内からの不正なアクセスを試みた形跡が発見された場合
⑵社外のサーバにて不正アクセスが発生し、アクセス元のアドレスプレフィックスが自社の割り当て範囲である場合

対策の指針

匿名アドレスを使用した場合でも、ユーザを特定できるしくみを導入します。もしくは、企業内では、匿名アドレスを使用しないルールとします。匿名アドレスは、WindowsXP に標準ですが、設定により利用しないことも可能です。

実現方法

既存のユーザ管理ソフトウェアに、IPv6 匿名アドレスを管理する機能を追加し、アクセスログからユーザを特定することを可能とします。企業内でのみ IPv6 を用いる場合、匿名アドレスを使用禁止とします。

IPv6 普及期への課題と提言

匿名アドレスを使用しないルールとした場合でも、ユーザによる設定変更を徹底する必要があります。いずれにしても、厳密な運用を行うためには、企業内の IPv6 端末を管理する何らかのしくみ

が必要となるでしょう。

E-1

概要

端末が複数のプレフィックスを持つようになることで、アクセス制御運用が難しくなり、不正アクセスを助長することが考えられます。

脅威の種類

設定煩雑化によるオペレーションミス、不正経路情報注入、パケット盗聴、改ざん、侵入・攻撃準備、コネクション・ハイジャッキング、DoS 攻撃

脅威の分析

IPv4 で多くの組織にみられるような、外部アクセス用に一つ、内部にプライベートアドレス空間というアドレス運用形態から、複数の IP アドレスの割り当てによる運用が可能になり、取り扱うアドレスプリフィックスが増えます。各アドレスプリフィックスについて、IPv4 での運用と同等もしくはそれ以上の、機器設定、経路情報交換、経路制御、フィルタリングなどが適切に行われないと、不正アクセスなど各種のセキュリティホールになります。

設定の煩雑化による設定ミスや、オペレーションミスが高まる可能性も高くなります。

マルチホーム環境では、第三者へのリダイレクトなどによりパケット盗聴、改ざん、コネクション・ハイジャッキングをはじめ、侵入路を利用する追跡困難な flooding などの DoS 攻撃の脅威にさらされやすくなります。

管理がずさんな組織では、renumber/reassign が容易になると、不正経路の注入などと連動して、内部から外部への攻撃を助長する可能性があります。

対策の指針

ハンドリングする IP アドレスが増えることにより、IDS や IPS といったセキュリティ装置やアプリケーションとの連携上など、統合的な管理を目指す必要が出てきます。

事前のシステムアプローチができないと大規模なセキュリティホールとなることを踏まえ、問題発生時の分析、対処措置への人的およびシステム運用コストなどの影響予測と対処に関する方法を確立しておきます。

経路に関してポリシー制御がうまく行われない場合は、踏み台になったり、それ自体への DoS 攻撃の対象となったりする危険性が高いため、監視も重要です。

マルチプレフィックス、マルチホーム環境になることにより、既存にはなく、技術の想定外の新しいタイプの攻撃が登場する可能性が高く、各種最新動向調査をしておくべきです。

実現方法

プレフィックスについて網羅的な管理をする必要があります。内外への経路制御を確実に把握した上でアドレス、ルーティング設計をします。端末とその端末が持つプレフィックス毎のアクセス管理と、動的フィルタなどの防御機構の導入も求められます。

IPv6 普及期の課題と提言

今後、以下のような対策の実現が必要と思われます。

- 経路更新時や、コネクション確立時の適切な認証の導入
- 悪い RA 送信などの管理と遮断方法の導入
- locator/identifier の適切なマッピングと管理
- renumber/reassign 時の設定管理、認証の導入
- 十分に評価されたアプリケーションの導入と利用（ソースアドレスセレクション/RFC3484 の実装など）

F-1

概要

端末が複数のインタフェース ID を持つようになることで、アクセス制御運用が難しくなり、不正アクセスを助長します。

脅威の種類

端末の管理不能、不正侵入

脅威の分析

複数の IP アドレスがついている端末インタフェースの状態監視ができない場合、実質的に端末管理が不能となります。また、フィルタが適切にされない場合、不正侵入などの侵入路となり得ます。自動設定機構を不正利用した乗っ取りなどの危険性が高まり、インタフェースを利用する全ての接続先からアクセスされる危険性もあります。

対策の指針

端末管理、IP アドレス管理をしっかりと行う必要があります。また、それに基づいた動的フィルタなどの導入など、IDS や IPS といったセキュリティ装置やアプリケーションとの連携上など、統合的な管理を目指す必要がある。

実現方法

適切なユーザ教育（端末管理、アクセス管理、アプリケーションの利用規則など）が求められます。また、端末とその端末が持つプレフィックス毎のアクセス管理と動的フィルタなどの防御機構の導入、ホップ制限の導入、privacy extension の導入、アプリケーションとプレフィックスの関係を適切に結びつけた設定や実装などが考えられます。

IPv6 普及期の課題と提言

IPv6 の普及により接続端末が増加すると、被害は拡大すると思われます。脅威の内容や対策に関する変化はありません。

G-1

概要

悪意のあるユーザが不正 ICMPv6 パケットを流すことにより、そのセグメント内の通信がねじ曲げられたり、通信不能になったりします。

脅威の種類

盗聴、サービス停止、管理不能

脅威の分析

具体的には以下のような攻撃が想定される

- セグメントのプレフィックスを有する RA を、セグメント全体へ流す
- デフォルトルータの L2 アドレスを偽称する NA を、他ユーザ端末へ流す
- ある端末からの NS パケットの L2 アドレス部だけを偽称した NS パケットを、ルータへ流す
- DAD 用の NS パケットに応答する NA パケットを、他ユーザ端末へ返す
- NUD 用の NS パケットに応答する NA パケットを、他ユーザ端末へ返す
- デフォルトルータの lifetime が 0 な RA パケットを、他ユーザ端末へ流す
- 不正な nexthop への Redirect パケットを、他ユーザ端末へ流す
- 異なるプレフィックスを含んだ RA を、セグメント全体へ流す
- RA の各種パラメータ(e.g. hoplimit)のみを偽称した RA を、セグメント全体へ流す

こうした攻撃は、本質的に IPv4 の ARP/ICMPv4/DHCPv4 spoofing と同じです。ICMPv6 パケットはリンクローカル・マルチキャストアドレス宛にブロードキャストされることが多い分、悪意を持ったユーザは攻撃に必要なパラメータを得やすいと考えられます。

ただし、問題が発生するのは、ユーザがルータなどを経由せず直接通信しあえるイーサネット・セグメント内のみです。また、プライベートな VLAN, PPPoE などで、L2 的にユーザ間直接通信を制

限する場合にはこの問題は発生しません。

対策の指針

端末からの ICMPv6 パケットが他ユーザの端末へ流れることを防止します。あるいは端末からの ICMPv6 パケットを認証する仕組みを導入します。

実現方法

L2 装置での ICMPv6 パケットフィルタリングを実施します。つまり、端末収容ポート間の ICMPv6 パケットを廃棄(L3-4) 、あるいは Private VLAN(L2)を利用します。グローバルアドレスを用いた端末間通信を行わせるためには、端末収容ルータで、「NDP proxy 機能を使う」 あるいは「ICMPv6 Redirect off かつ広告する RA の on-link フラグ off」とする必要があります。リンクローカル・アドレスでの端末間通信はできなくなります。

端末間の ICMPv6 パケットをすべて廃棄すると、正当な DAD の正常動作を妨げるため、アドレスの重複を検出できなくなる危険性があります。ただし、DAD の正常動作にかかわらず、アドレス重複発生時は通信ができないことが多いと考えられます(DAD 失敗後アドレス再生成をしない実装が多いため)。そのため、実用上の問題は少ないと思われます(ネットワーク管理者がアドレス重複を検知できれば十分)。

IPv6 普及期の時代への提言

SEND(SEcuring Neighbor Discovery)の導入も考える必要があります。また、DHCPv6 を使ったアドレス配布による、アドレス重複の防止対策が望まれます

G-2

概要

IPv6 では、パケットのフラグメント処理や到達不能エラーなどに対する処理を端末が行います。その制御のために必要な ICMPv6 Error パケットは、任意の通信先から端末へ到達可能でなければなりません。到達可能性を保証するため、ネットワーク管理者が ICMPv6 Error パケットに対するフィルタリング処理を一切行わないと、ICMPv6 Error パケット自体が管理者の管理できないバックドアになりえます(例. ICMPv6 Error メッセージのペイロードに機密情報をエンコード、ICMPv6 Error メッセージを用いた外部から内部へのアタック)。

脅威の種類

情報漏洩、サービス停止

脅威の分析

これはIPv6固有の問題です。ただし攻撃者がICMPv6 Errorを攻撃先へ到達させるためには、攻撃者は攻撃先の IP アドレスを知る必要があるため、外部から内部への攻撃は困難です（C-2）。

対策の指針

攻撃者に攻撃対象のIPアドレスを推定されないようにする必要があります。呼応する通信がないICMPv6 Errorがネットワーク境界を行き来しないようにします。

実現方法

端末から直接通信可能な範囲を限定します（IPアドレス, port番号, IPsecポリシー, Proxy経由で外部通信）

端末から外部通信するときには匿名アドレスを使用、さらに EUI64 ベースのアドレスに対するACLをパーソナル・ファイアウォールで指定します。

IPv6普及期の時代への提言

境界ルータでステートフルインスペクションを実施する場合は、 ICMPv6 Error パケットのペイロード部に含まれているError発生源のパケットもチェックする必要があります。

G-3

概要

L2 的侵入によりIPv6グローバルアドレスやリンクローカル・アドレスを取得できるので、L2 的に侵入されることが、即不正アクセスにつながります。

脅威の種類

不正アクセス

脅威の分析

認証なしDHCPv4アドレス配布, IPv4リンクローカル・アドレスによる不正アクセスの危険性と同じです。L2 的に潜入されることが本質的な問題となります。L3 アドレスがまったく入手できなかったとしても、盗聴や不良Ether Frameによる攻撃は可能です。

対策の指針

対策としては、L2 のアクセス認証を行い、仮に侵入されても不正アクセスされないようにする必要があります。

実現方法

物理的なガードや IEEE802.1x などにより、L2 セキュリティを強化します。端末上のパーソナル・ファイアウォールで、外部端末から許可するアクセスを必要最小限に限定します。

IPv6 普及期の時代への提言

DHCPv6 アドレス配布および DHCPv6 snooping ができるようになることが望まれます。リンクローカル・アドレスへの攻撃は防止できませんが、IEEE802.1x を全端末に導入するよりは簡便にアドレス取得による危険を防止することができます。

H-1

概要

IPv6(IPv4)ネットワークからデュアルスタック端末への不正侵入が行われた場合、IPv4(IPv6)ネットワークに接続される端末に対して踏み台になるなどの脅威を広げる可能性があります。また、IPv4 と IPv6 が別々のネットワークとして構築されている場合も、トランスレータ（Web プロキシ含む）の設置によりデュアルスタックでない端末も互いに踏み台になるなどの脅威を与える可能性があります。

脅威の種類

踏み台、情報漏えい

脅威の分析

IPv4、IPv6 それぞれ異なったポリシーであるものを、混在させて運用することが問題です。原因として、互いのネットワークに対する接続ポリシーの整備不足、IPv6 ready であることをユーザが知らずに使ってしまう、IPv6 ネットワークに対する技術的に未解決な部分(アンチウィルスソフトや ID など)が残っていることなどが挙げられます。また、IPv4 と IPv6 が別々のネットワークとして構築されている場合も中間にトランスレータを設置することで、そのセキュリティ対策が不十分である場合、互いに踏み台になるなどの脅威を与える可能性があります。

対策の指針

管理者は、外部との IPv6 ネットワーク境界に設置されるファイアウォール上で、双方向の適切な通信のみを許可する通信制限を行います。管理者およびエンドユーザは、デュアルスタック端末自身のセキュリティの改善として、端末ファイアウォールの適用とセキュリティパッチの早期適用の実施を行います。また、管理者は、デュアルスタックでない IPv4 と IPv6 ネットワークへの影響範囲を最小化するため、トランスレータ自身のセキュリティ管理を行う（IPv4 マップアドレスや互換アドレスの拒否）と共に、トランスレータを経由する通信を制限し、トランスレータを経由する通信ログ

の管理を適切に行う必要があります。

実現方法

定期的な外部 IPv6 と接続を行うファイアウォールでのフィルタリング設定を実施します。定期的なデュアルスタック端末へのパッチ適応・端末ファイアウォールでのフィルタリングを実施します。さらに、定常的なトランスレータのセキュリティ管理（IPv4 マップアドレスや互換アドレスの拒否）とトランスレータを経由するログ管理を実施します。

IPv6 普及期への課題と提言

端末用ファイアウォールソフトウェアで、IPv4 用(IPv6 用)で設定した内容は、IPv6(IPv4)にも自動的に適用し、必要に応じて片側のプロトコルのみ設定を変更可能にできると穴ができにくいと考えられます。

H-2

概要

現状のアンチウイルス・ソフトは、ファイル I/O に関しては IPv4/IPv6 が関係ありませんが、Web や Mail などネットワーク部分のウイルスチェックは、IPv4 ネットワークのみに対応しており、IPv6 ネットワーク経由で感染活動を行うワームには対処することができません。結果として、アンチウイルス製品の IPv6 対応が追いついていないことによって IPv6 ネットワーク経由でのワームに感染する可能性があり、さらに IPv4 ネットワークに対してもワームの活動範囲を広げる恐れがあります。

脅威の種類

不正コード侵入（ワーム）

脅威の分析

IPv6 ネットワークへのワーム対策が行われていないため、ワームの感染活動が IPv6 ネットワーク経由で行われることが想定されます。また、アンチウイルス製品の IPv6 対応が追いついていないことによって、感染したマシンから、IPv6 ネットワークに接続されている端末にワーム伝播するなどの脅威を与えるのと同時に、トランスレータなどを通じて IPv4 ネットワークに対しても影響を与えることが想定され、更なるワーム感染拡大などの脅威に繋がります。逆に IPv4 ネットワークにトランスレータ経由でアクセスし、ウイルスに感染することも考えられます。

対策の指針

管理者およびエンドユーザは、端末 OS のパッチ更新を行い、外部の IPv6 ネットワークと接続し

ているファイアウォールで適切な通信フィルタリングを行います。また、管理者は、IPv6 ネットワークに対応したアンチウイルス・ソフトが利用可能になった時点で、導入実現方法の検討を早期に行います。また、デュアルスタックでないIPv4とIPv6ネットワークへの影響範囲を最小化するため、管理者は、トランスレータ自身のセキュリティ管理を行います（IPv4 マップアドレスや互換アドレスの拒否）と共に、トランスレータを経由する通信を制限し、トランスレータを経由する通信ログの管理を適切に行う必要があります。 もちろん IPv4 対応のアンチウイルス・ソフトを端末に導入することは必須です。

実現方法

定期的なウイルス対策ソフトの更新や、外部 IPv6 と接続を行うファイアウォールでの定期的なフィルタリング設定を実施します。また、定期的な端末へのパッチ適応、端末ファイアウォールでのフィルタリングの実施、IPv4 対応アンチウイルス・ソフトの導入と最新版へのアップデートを実施します。また、定常的なトランスレータのセキュリティ管理（IPv4 マップアドレスや互換アドレスの拒否）とトランスレータを経由するログ管理を実施します。

IPv6 普及期への課題と提言

アンチウイルス・ソフトが IPv6 完全対応すれば、脅威は現状の IPv4 におけるウイルス対策と同等となります。即ち、ウイルス対策ファイルを最新版に保つようアップデートを行うこと、疑わしいサイトにアクセスしないこと、怪しい添付ファイルは開かないことなどが対策となります。

I-1

概要

トンネリングプロトコルによって、既存のネットワークトポロジー上の境界ファイアウォールなどでのアクセス制限を通過してしまう経路を簡易に作ってしまう危険性があります。

脅威の種類

設定・オペレーションに対する脅威で、外部への IPv6 接続のためのトンネル設定時に発生します。

脅威の分析

内部セグメントへ自由にアクセスできる経路を残してしまうことによって、組織内部のネットワークが外部からの攻撃にさらされます。

対策の指針

正しくネットワーク設計・管理をしていれば防ぐことができます。

実現方法

トンネルサーバ自身、または、トンネルサーバと内部セグメントの経路上でのアクセス制限やパケット検査などの対策が必要です。端末上でトンネルエンドポイントを作ることを許さない(Windows XP の Teredo など)、正しく設定したトンネルサーバ以外からのトンネルプロトコルは遮断する、トンネルサーバ自身、あるいはトンネルサーバと内部セグメントの間で不必要な外部からの通信やポリシーに反する通信をアクセスフィルタなどにおいて遮断する、といった対策が必要です。

IPv6 普及期の課題と提言

特になし

I-2

概要

トンネルサーバへ大量のパケットを送ることによって、トンネルサーバのトラフィック処理能力を低下させる脅威が考えられます。

脅威の種類

DoS

脅威の分析

IPv6 接続性が低下します。トンネル接続を使用している場合には、常にトンネルサーバが“single point of failure”になります。

トンネル接続は IPv6 移行期の一時的な利用形態であり、デュアルスタックまたはネイティブ接続への移行が望まれます。

対策の指針

トンネルサーバとクライアント間で認証を行い、許可しない端末からのトンネルサーバ利用を制限します。ただし、この場合でも、端末がワームに感染するなどした場合には、完全に防ぐことはできません。

実現方法

用いるトンネルプロトコル(DTCP)や他との併用(IPsec)によって可能になります。

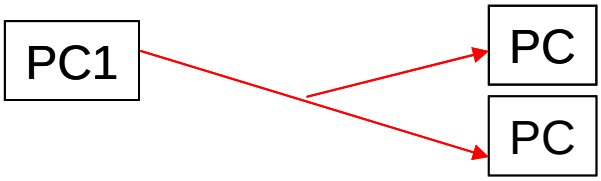
IPv6 普及期の課題と提言

特になし

J-1

概要

マルチキャストアドレス宛のパケットを送ることにより、相手のアドレスを知らなくても攻撃パケットを送ることができてしまいます。



脅威の種類

サービス停止、不正コード侵入

脅威の分析

本質的に、IPv4 マルチキャストにも同じ問題がありますが、IPv4 ではマルチキャストが普及していないために顕在化していません。

グローバル・マルチキャストの場合は攻撃範囲が広いですが、そもそもルーティングされていないことが多いですし、ルーティングされているマルチキャストアドレスを推定しにくいため、IPv4 同様に攻撃は困難です。

リンクローカル・マルチキャストの場合、攻撃範囲はセグメント内に限定されるものの、ルーティングされなくても動きます。また、よく知られたマルチキャストアドレスが多いため、攻撃は容易です(ARP storm 攻撃と同じ)。

対策の指針

マルチキャストパケットは必要最小限に流すようにすることが 1 つの対策になります。

実現方法

端末収容セグメントでの Ingress Filter により source spoofing を防止します(グローバル・マルチキャストのみ有効にする)。また、Rendezvous-Point で PIM Register ACL によるマルチキャスト送信元を限定します (PIM-SM でのグローバル・マルチキャストのみ有効にする)。

攻撃者のレイヤ 2 での侵入を防止します (グローバル、リンクローカル両方のマルチキャストに有効) (G-3 参照)。さらにレイヤ 2 スイッチでの MLD snooping (グローバル、リンクローカル両方のマルチキャストに有効)。レイヤ 2 スイッチでルータ以外のポートからの FF02::1 送信を禁止することも対策に含まれます。

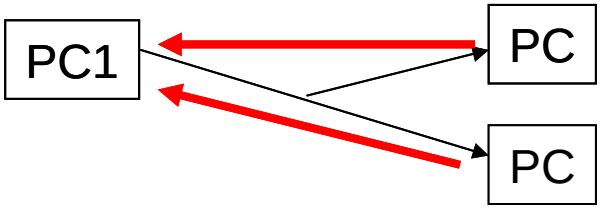
IPv6 普及期の時代への提言

特に小型スイッチの MLD snooping 対応（最低でも MLDv1，できれば MLDv2 も）が強く望まれます。

J-2

概要

マルチキャストが有効になっているネットワークでは、マルチキャストアドレス宛のパケットに対する端末のユニキャスト応答（e.g. ICMPv6 ECHO に対する ECHO-REPLY, uPnP 問い合わせに対する応答）から、端末のアドレスや属性を推測することができます。これらの情報を基に、端末を狙った攻撃が行いやすくなります。



脅威の種類

不正侵入

脅威の分析

マルチキャストへの応答が、攻撃材料の提供につながります。参加していないグループ宛のマルチキャストパケットも端末に届くことがあります（同一セグメントの他の端末が参加している場合）。そのため、リンクローカル・マルチキャストに限らず、本脅威は発生する可能性があります。IPv4 にも潜在的に同じ問題が存在します（J-1 参照）。

対策の指針

ネットワーク管理者が、マルチキャストパケットを必要最小限にしか流さないようにすることが対策となります。端末のマルチキャストグループへの参加を必要最小限にすること、端末のマルチキャストパケットへの応答を必要最小限にすることが求められます。

実現方法

J-1 で紹介した実現方法で、必要最小限なマルチキャストしかネットワークに流れないようにすることが重要です。

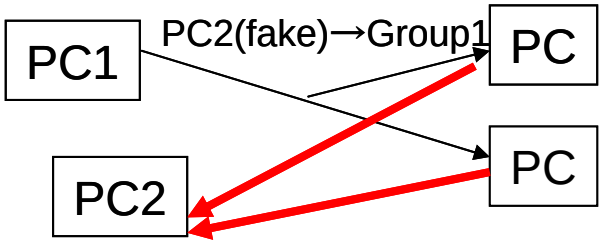
IPv6 普及期の時代への提言

端末上のパーソナル・ファイアウォールで、マルチキャストパケット、MLD Report に対する ACL を記述できるようにすべきです。

J-3

概要

マルチキャストが有効になっているネットワークでは、攻撃対象端末のアドレス(下の図では PC2)をソースに偽装したマルチキャストパケットを送ることにより、そのパケットへの応答(e.g. ICMPv6 ECHO に対する ECHO REPLY, UDP パケットに対する Port Unreachable Error)を用いた DDoS 攻撃をかけることができます。



脅威の種類

サービス停止

脅威の分析

Source Spoofing とマルチキャストへの応答を利用した攻撃です。IPv4 にも潜在的に同じ問題が存在しています(J-1 参照)。

対策の指針

Source Spoofing を防止します。また、端末はマルチキャストパケットに対して必要最小限に応答するようにします(J-2 参照)。

実現方法

端末収容セグメントでの Ingress Filter により source spoofing を防止します (グローバル・マルチキャストのみ有効)。また、J-2 に示す対策により、マルチキャストパケットへの応答を抑制します。

IPv6 普及期の時代への提言

K-2 と同じです。

J-4

概要

大量の Group へのマルチキャストグループ参加により、ルータのマルチキャスト経路表が溢れ、本来行われるべきマルチキャスト中継が行われなくなる危険性があります。

脅威の分類
サービス停止

脅威の分析
ルータのエントリ数に対する攻撃です。IPv4 マルチキャストの IGMP join 攻撃や、IPv4 の ARP storm 攻撃と同じです。

対策の指針
不要な MLD Report をルータで廃棄するか、端末で出させないようにします。

実現方法
ルータの ACL で MLD Report をグループアドレスによって廃棄します。

IPv6 普及期の時代への提言
特になし

K-1

概要
non-PC 端末（シン・クライアント）がネットに繋がると、出荷時の実装を超える脅威に対する対処が難しいという問題です。

脅威の種類
すべての可能性がありますが、non-PC プラットホームの脆弱性を悪用されるという意味では、特に踏み台、不正コード侵入（ワーム）が挙げられます。

脅威の分析
non-PC で使われる組み込みプラットホームにおいて Security Update の実施が通常行われておらず、製品出荷時に発見されていない脆弱性への対応が困難です。また、non-PC には、利用者がソフトウェアをアップデートすることを前提としたインタフェースなどがないため、リコール回収、サービス窓口への持ち込みなど、利用者に負担を強いる以外に、早急なアップデート対策を行うことができません。また、これまでの機器利用形態に慣れてしまっており、セキュリティアップデートというもの自体について、利用者がその必要性・重要度を理解することができない場合が想定さ

れるため、最新のセキュリティ対策が行われないまま利用されるケースが十分に考えられます。

対策の指針

消極的対応としては、non-PC 端末の稼動形態を解析し、もし特定サーバとの通信が確保されていればよいのであれば、それらのサーバ以外からのトラフィックを遮断したり、それらのサーバと相互認証を行って通信したりすることで問題を回避できます。さらに一般にIPsecなどによる、通信相手（サーバー）の制限・認証を行うことによって、安全性を高めることができます。

もし、non-PC が不特定な相手と通信するような動作形態の場合、ホームルータ等において、ステートフル・パケットフィルタなどで相手を特定したフィルタリングを施します。

もちろん、究極の解は、nonPC 組み込みプラットホームにおいても、OSアップデートが可能な枠組みを保証することですが、これはコスト的に厳しいでしょう。

実現方法

non-PC の通信相手を限定する、ステートフル・パケットフィルタなどで non-PC に流入するパケットを限定するなどします。

IPv6 普及期の課題と提言

組み込みプラットホームのOSアップデート機構の構築・普及が望まれます。

K-2

概要

non-PC 端末（シン・クライアント）がネットに繋がると、十分なセキュリティのサポートを提供することが難しいという問題があります。

脅威の種類

non-PC の計算力が弱いことに注目すると、（IPsec が使いにくいという意味で）なりすまし、盗聴、サービス停止、改ざんなどを受けやすいことが指摘できます。

脅威の分析

non-PC が、一般に計算能力の小さい低コストハードウェアを想定していることにより、十分なセキュリティ機能（IPSEC, TLS, SSL など）をサポートできないという問題です。

対策の指針

まずは該当する non-PC 端末において、セキュリティ機構が必須であるかどうかをベンダがどう判断するかということです。どうしてもセキュリティ機構が必要な場合、専用ハードウェアの採用、第

3者認証方式の採用など、軽量なソリューションを検討することが必要になります。

実現方法
不要と判断するなら、セキュリティ機構をサポートしないという方法、専用チップなどを採用する方法、第3者認証・鍵配布機構により、公開鍵暗号処理を回避するという方法などがあります。
リンクローカルセグメント内では、最低限のセキュリティ機能を利用し、外部との通信は、ホームルータなどの他の機器上に実装したセキュリティゲートウェイなどを利用して、より安全な暗号化通信を行います（ホームルータ・サーバ間は高度な暗号化アルゴリズムを適用するなど）。

IPv6 普及期の課題と提言
第3者認証・鍵配布機構（Trusted 3rd Party Model, KINK など）の普及が望まれます。

L-1

概要
モバイル IP の利用環境が広がると、 Care of Address がネットワーク外部の場合、アクセス制御が難しくなります。

脅威の種類
リモートアクセス系の脅威全般なので、情報漏えい、盗聴、サービス停止、改ざん、踏み台が想定されます。

脅威の分析
トンネリングに起因する脅威に関しては、項目 J と同様であり、対応も同様。MIP 特有な事情としては、次の点が挙げられます。
（1）MIPで使用する拡張オプションヘッダを解釈できるFWが存在せず、FWルールがルーズなものになる
（2）セキュリティGWが MIP aware でないと、登録パケットなどを正しくHAにフィードできず、やはりルールがルーズになりセキュリティホールとなる恐れがある。

対策の指針
移動ノード自身、または移動ノードと内部ホームエージェントへの経路上でアクセス制限やパケット検査などの対策が必要です。

実現方法
境界ファイアウォールや内部ルータにおけるMIPプロトコルパケットの正しい解釈・遮断（IP フィル

タ)を行います。

IPv6 普及期の課題と提言

MIP の適用検証に合わせた脅威の洗い出しと、それに対応するフィルタ実装(FWの IPv6 拡張オプションヘッダ対応)をベンダに要求していく必要があります。

M-1

概要

既存プロトコル実装の中には、IP アドレスの DNS 逆引きレコードとそのレコードに呼応する正引きレコードの整合性を用いて、通信相手を認証するものがあります。こうしたプロトコル実装を IPv6 実装させることは困難です。

脅威の種類

管理不能、サービス停止

脅威の分析

IPv6 固有な問題です。IPv4 ではダミーの逆引き PTR record を全部書くことにより対処します。DNS 逆引き応答が得られないことにより、ログ解析が不便になります。DNS 逆引き応答待ちにより、サービス RTT が大きくなります。

対策の指針

DNS 逆引きは元々脆弱な認証手段であり、これだけで認証を行うこと自体が問題です。認証は他の手段にて行い、DNS 逆引きはログ解析の参考程度に使うべきです。DNS 逆引き応答時間が短くなるようにし、アドレスから対応するドメインを調べるためには、whois を使うなどが考えられます。

実現方法

DNS 以外の認証手段へ移行します。また、DNS 逆引きの lame delegation を防ぎます。すなわち上流から delegate されている逆引き名前空間の NS 設定を各サイトで忘れないようにします。DNS 逆引きを無効にします。

IPv6 普及期の時代への提言

逆引きレコードを動的に自動生成する DNS サーバ実装があると、管理上便利です (IPv4 のような静的な自動生成は、DNS レコード数の激しい増加につながり望ましくない)。Whois サーバへの問い合わせ頻度が高くなることが予想されるため、whois サーバの負荷分散対策が望まれます。

まとめ

直接の到達性、デュアルスタック経由での被害伝播、IPsec 含めたトンネル技術による情報漏えい、直接の WORM 感染などは、適切な設定・オペレーションにより現時点で対策可能です。
対策の指針と方法については、IPv4 との大きな相違はありません。
執筆時点で、セキュリティ製品、ネットワーク機器の IPv6 対応は、IPv4 同等機能に達しているとは言い切れない状況です。IDS と連携したファイアウォール、IDP、アンチウイルス、レイヤ 2 装置でのレイヤ 3 パケットのフィルタリングなどで IPv6 対応が進むことが求められます。
マルチキャスト、Mobile IP 対応のファイアウォール等、使い方に応じ、セキュリティ製品の機能充実が必要になる場合があります。
non-PC は機器の特性に応じて固有の対策が必要になるだろうと思われます。

固定アドレス環境が広がることによる家庭環境のプライバシー問題については何らかの対策が必要となるかもしれません。

3. BCP のセキュリティ分析

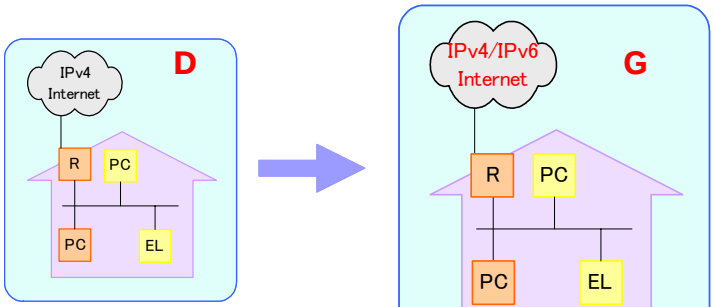
ここでは、家庭、大企業・自治体、SOHO で用いられる BCP についてセキュリティ分析と評価を行います。分析は、それぞれ次のようなシナリオに基づいて行います。

家庭	外出先から自宅サーバへのアクセス（個人ファイルのライブラリ）
大企業	イントラネットへの IP 電話の導入
自治体	庁内 LAN（自治体イントラネット）でのマルチキャスト議会中継
SOHO	営業店端末のメンテナンス

BCP のセキュリティ~家庭~

ここで想定する家庭のシナリオは、家庭 SWG の導入期モデル G です。

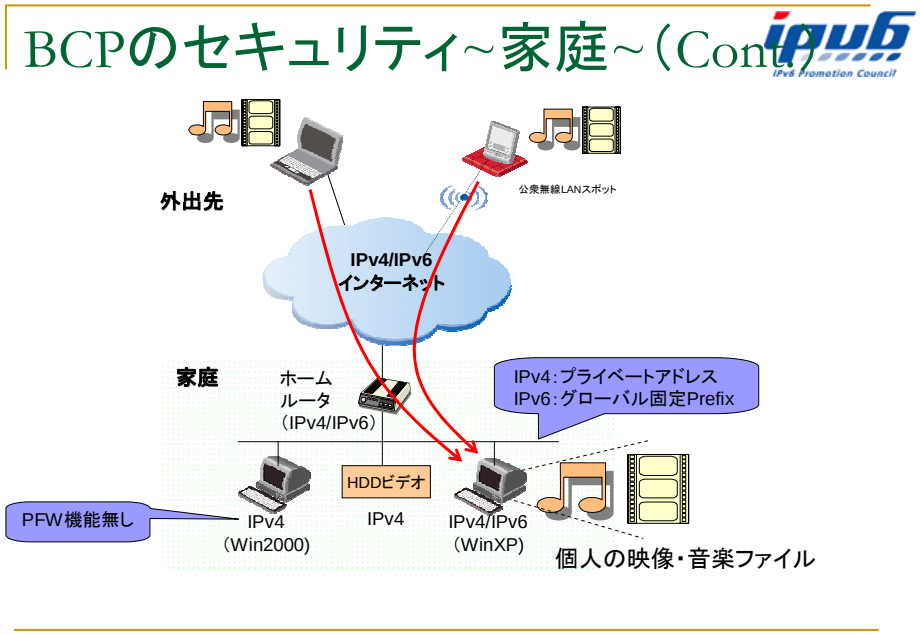
ISP の IPv6 サービスに加入しており、IPv4 の動的アドレスと IPv6 の固定アドレスで接続されています。IPv6 対応 OS の PC は既に購入しています。



モデルD　　モデルG

IPv4 は従来どおり利用可能で、IPv4 対応の PC（Windows2000）と HDD ビデオがあります。IPv6 の用途としては、外出先から自宅ファイルサーバ（IPv6PC、WebDAV）へのアクセスにより、個人の映像、音楽ライブラリを取得するなどが考えられます。

セキュリティポリシーとしては、外部からのアクセスは IPv6PC への https 接続のみに限定しています。また、アクセスできるフォルダ/ファイルは限定しています。ただし、外出先の IP アドレスは固定ではありません。



セキュリティ分析と評価

分析

(H-2) (A-2)IPv6PC へ外部から直接アクセスできることにより、IPv6PC への不正侵入やワーム感染の脅威が高まります。これにより、比較的無防備な IPv4 マシン、non-PC へ被害伝播を及ぼす可能性があり、 IPv6PC への対策が重要となります。

(A-2)利用が自分（外出先）から自分（家庭内）へのアクセスであり、経路上の情報から端末アドレスが公となり、v6 で接続されたそれぞれの機器に対して不正アクセスを受ける脅威があります。

(C-2)公衆無線 LAN スポットからのアクセスに関して、WEP 等により通信暗号化の対策がなされないと、アドレスや固定プレフィックスが公になり、v6 で接続されたそれぞれの機器に対して不正アクセスを受ける脅威があります。

Home ルータはデフォルトでは、プレフィックスが::1 のことが多く、攻撃対象とされる脅威があります。Home ルータがのっとられた場合、内部情報の収集や、脆弱なマシンへの侵入などをするための踏み台にされる可能性があります。

評価

危険度：低

以下の対策により脅威の低減が可能です。また、IPv4 での同等な使い方に比べたセキュリティ向上が期待できます。

端末での設定
・パーソナル・ファイアウォール上において、外部接続を https サービスのみに設定する。
・アプリケーション・レベルでの認証と、ファイル操作制限を実施する。

Home ルータでのアクセス制御
・IPv6PC でのアクセス制御に加え、Home ルータでアクセスを制御することにより、外部からの不正な侵入を抑止する。
・Home ルータへの接続は内部からのみとする。（耐 Home ルータのっとり）
・Home ルータでの IPv6PC へのフィルタも定義する。基本的には、外部からのアクセスは全て禁止にし、必要なもののみを個別に開ける形にする。
・Home ルータ上の SPI 機能は利用する。
・内部アクセスを Home ルーター外部端末間を VPN で接続したものに限らせる手法もある。

不用意に端末アドレスを第 3 者に流さない
・公開 DNS へ登録しない
・外出先からの名前解決は Hosts ファイルで実施
・定期的にアドレス変更する（手動設定）

3 章の関連サブアイテム

A-1,A-2,B-2,C-1,C-2,G-2,H-1,H-2

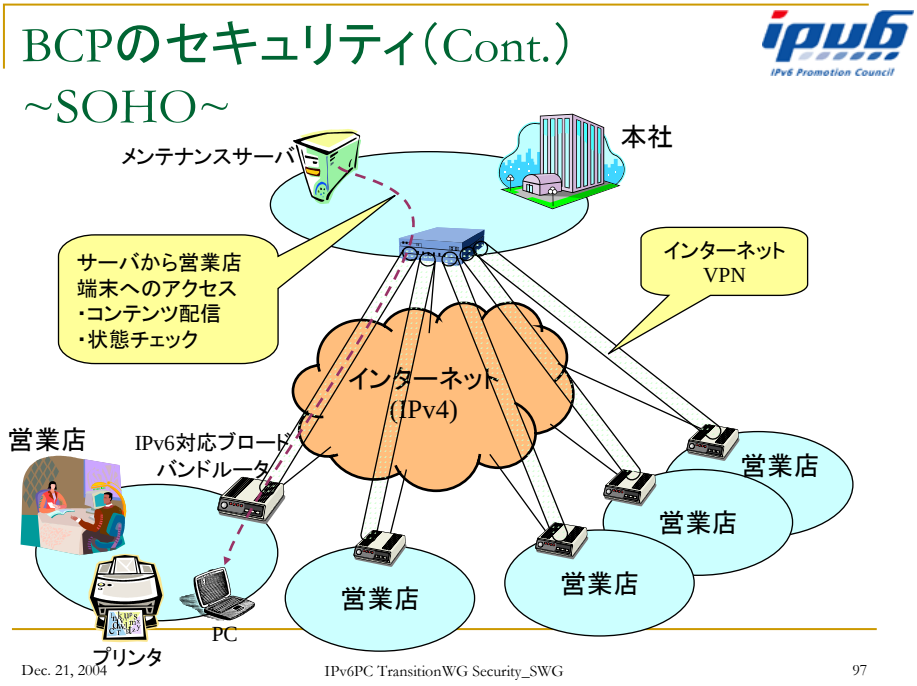
BCP のセキュリティ~SOHO~

想定シナリオは、営業店端末のメンテナンス目的で IPv6 を導入するというものです。
営業店運用の課題として、現地に IT スタッフを常駐できない、端末のメンテナンスに工

数がかかる、店舗の統廃合の運用負荷、セットアップに工数がかかる、などがあります。これを解決するため、端末の自動メンテナンスシステムを導入します。これにより、端末への直接コンテンツをプッシュ配信したい、そしてサーバから端末状態を動的に入手したいということが目的となります。

これを実現するためのシステム要件としては、サーバから直接端末を指定するため、IP アドレスの固定運用が必要になります。また、運用簡便化のため、自動アドレス付与が必要です。

セキュリティポリシーとしては、メンテナンス利用のため、クローズドな環境で利用し、IPv6 はメンテナンスにのみ用います。インターネット利用は本社経由で、IPv6 ではインターネット通信を行いません。また、メンテナンス目的での導入のため、営業店間の IPv6 通信も行いません。営業店間の IPv6 通信はフィルタリングします。あくまでも管理者による端末の設定、管理用に IPv6 通信を許可します。



セキュリティ分析と評価

分析

サーバ-端末間のセキュリティ以外は考える必要がありません。インターネットとの通信はないですし、営業所間の通信は許していないからです。ただし、営業所内は自動端末設定を利用するため、そのセキュリティは考慮する必要があります。たとえば RA に認証機構

がないという点です。これは、IPv4 と同レベルのセキュリティ上の問題です。匿名アドレスを利用した場合、リモートメンテがしにくいため、匿名アドレスは使えません。

評価

危険度：小

L2 レベルの対策を採りにくいため、ゲートウェイになんらかのセキュリティ機能が必要です。IPv4 と同レベルの危険度です。上記対策とともに、不正端末（NDP, onlink 端末）についても排除します。リモートメンテのアプリでは匿名アドレスは利用しません。

3 章の関連サブアイテム
以下項目は一般的なイントラネットでは影響しますが、本ケースでは初期前提により、無視できます。
A-1, A-2, A-4, B-1, B-2, C-1, C-2, E-1, F-1
以下の項目は、セキュリティ案件として残ります。
D-1, G-1, G-2, G-3

BCP のセキュリティ ~大企業~

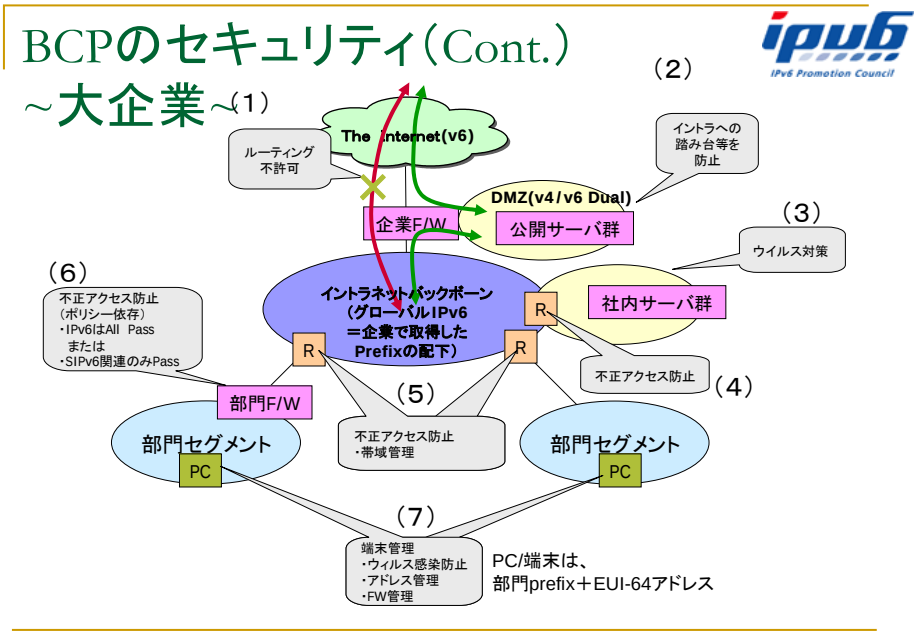
想定するシナリオは、IP 電話の導入をきっかけに IPv6 を導入し、サブネット設計の簡素化を図るというものです。

この組織では、正規のグローバルアドレスを取得しますが、当面、外部とは切り離します。NAT を介さないシームレスなイントラ VoIP 網の構築が主目的であるためです。

IP 電話でハードフォンと PC ベースのソフトフォンを導入することで、アドレスの需要が増加します。

セキュリティポリシーは、境界ルータでは、イントラ内部とインターネットとの v6 通信を遮断します。外部からの IPv6 通信は、DMZ のみ可能とします。部門ファイアウォールでは、部門管理者が 2 つのポリシーのうちどちらかを選択します。IPv6 は All Pass（イントラ内からの脅威はないと仮定）、あるいは SIP/RTP 関連ポートのみ Pass のいずれかです。

クライアントに対する適切な管理を実施します。その内容としては、検疫 VLAN 等によるウイルス対策、パーソナル・ファイアウォールの設定管理、アドレス管理（IP-MAC 対応表 : 匿名アドレス利用時の管理対策）、エージェントソフト等によるきめ細かな端末管理、などがあります。



セキュリティ分析と評価

分析

（A 項）ダイレクト感染の可能性は増加します。このため、感染端末持ち込み防止を強化します（IPv4 と同じ）。しかし、ポートスキャンによる特定の可能性は低く抑えられます。
（B-1）企業網では、端末管理が容易になる分、プラスの面があります。
（B-2）オペレーションミス→この BCP では可能性が低いと考えられます。
（D-1）匿名アドレスを OFF とするか、クライアントにエージェントを導入する等の手段で端末の管理を実施します。
（G-3）レイヤ 2 認証等、IPv4 と同様の仕組みを導入します。
（H-1）BCP では、外部からのアクセスは DMZ 経由なので、H-2 の対策でカバーします。
（H-2）社内サーバ，トランスレータ等の適切な管理が必要です。
（K-2）BCP では、イントラからのアクセスのみのため、脅威の対象が内部のみです。

評価

危険度　小

3 章の関連サブアイテム

A 項：v4 と基本的に同じです。

B-1,B-2,C-2, D-1, G-3,H-1,H-2,K-2

BCP のセキュリティ ~自治体~

想定するシナリオは、開かれた行政を目指す自治体として、IT 技術を利用し、住民への情報公開や密接なコミュニケーションを重視した、自治体サービスの実現を目指すというものです。このため、内部イントラの庁内 LAN を活用して、低コストに議会中継システムを実現します。そして、マルチキャストによる議会映像配信をきっかけに IPv6 を導入します。

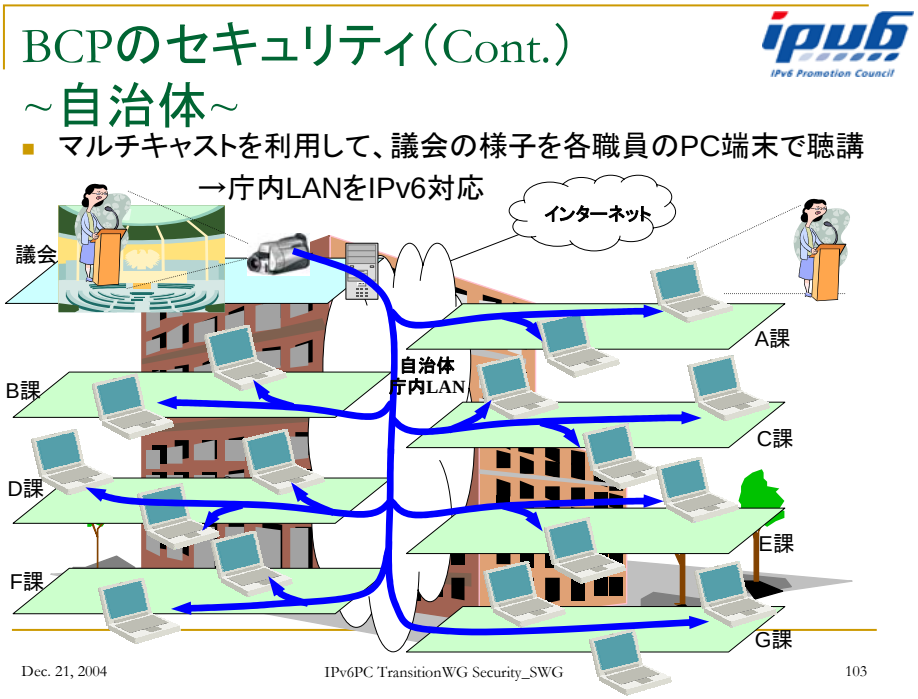
この場合のセキュリティポリシーとしては、まず配信範囲の限定があります。当面は配信範囲を庁内 LAN に限ります。自治体関連の出張所については、帯域／回線種別／機器条件時応じて配信を検討します。外部に対しては、各自治体の制約に応じて、将来的な配信を検討します。

もう 1 つは IPv6 対応アプリケーションの限定です。各端末で利用できる IPv6 サービスは、当面は目的のアプリケーション（ここでは映像配信など）に限定します。

既存サービスは、IPv4 のまま運用し、付加的なメリットが期待できる場合は IPv6 対応を検討します。

新規導入サービスについては、積極的に IPv6 活用を推進します。

オプションとしては、まず認証の適用があります。これは、ストリームデータの内容によっては、特定のユーザ/端末しか聴講できない仕組みが必要になるためです。配信範囲はネットワーク管理者が明示的に管理・限定できることが望ましく、偽配信サーバを防止できることも望まれます。



セキュリティ分析と評価

分析

IPv6 マルチキャストのみを用いた攻撃を考察対象とします。外部への IPv6 通信はサービス対象外で、境界ルータで外部からの IPv6 トラフィックを全て廃棄し、内部攻撃のみを考えればよいからです。IPv6 ユニキャストもサービス対象外です。IPv6 グローバルアドレスを端末に配布しなければよいからです。

リンク内に閉じたリンクローカル・ユニキャスト攻撃については、端末発の IPv6 パケットを MLD 以外廃棄して対応します(IPv6 端末内のパーソナル・ファイアウォールか、端末を直接収容する L2 装置にて実施)。

評価

危険度: 低

ストリームデータの認証方法

配信に関する認証では、まず DRM（ストリーミングアプリ内で認証）を利用します。また、アクセス認証として、ストリームのメタデータへの HTTP アクセス(IPv4)を認証しま

す。

意図せぬマルチキャスト・トラフィック対策

狭帯域リンク(e.g.無線 LAN)への流れ込みによる狭帯域リンク溢れという問題がありますが、(J-1) 意図せぬ流れ込みは MLD snooping で防止します。 意図した流れ込みについては、ルータを挟んでレイヤ 3 的にセグメント分けして防ぎます(そのセグメントで、マルチキャストを止める or ストリームメタデータへのアクセスを制限)。

偽配信サーバからのストリーミンの可能性については、IPv6 グローバルアドレスを端末に配布しないため、起こりえません。

マルチキャストルータに対するエントリ数攻撃対策

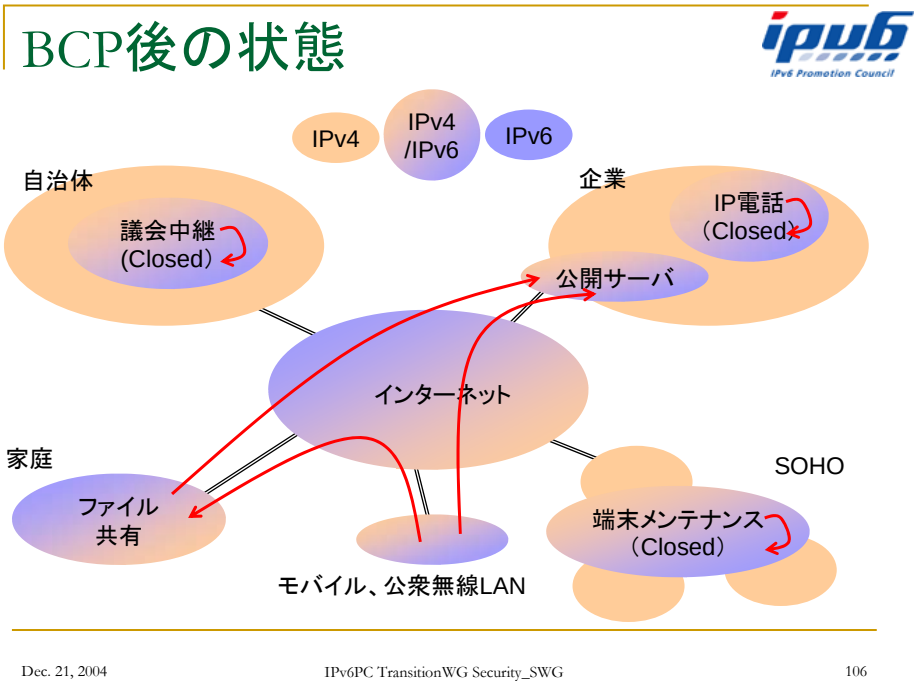
J-4 の対策参照

3 章の関連するサブアイテム

J-1, J-4

4. IPv6 普及期のセキュリティ

分析と課題



IPv6 普及期の想定

IPv6 普及期には、まず BCP 事例の導入が拡大します。閉じた IPv6 システムが拡大し、端末の増加とともに、閉じたシステム間の相互接続が進みます。そして、普及期には、デュアルスタック運用から IPv6 オンリーの運用へ移行していきます。これは、管理運用コストの削減を主な目的として行われます。アプリケーションごとの使い分けから IPv6 への統合（Web、Mail）という動きが進むと想定されます。

また、新技術との融合で IPv6 利用が拡大します。家電、携帯端末の IPv6 接続など、nonPC 向けのサービス開始や、トレーサビリティや統計情報、個人属性に応じた情報の提供のための IC タグ、センサ情報のサービス活用が進みます。

業務への IT 活用の高度化も IPv6 普及につながります。P2P アプリケーションによる業

務コラボレーションの活性化が進められ、IT 利用の目的が「業務の効率化」から「顧客の獲得」、「サービス品質の向上」に多目的化していきます。

IPv6 普及期のセキュリティ

ここでは、以下のようなシナリオに基づき、家庭、大企業・自治体、SOHO が想定する IPv6 普及期に対してセキュリティの分析と課題を示します。

家庭
IPv6 普及期のホームネットワークモデル K、L、O に基づき、外部からのアクセス（VTR 予約、宅内カメラ）を行います。

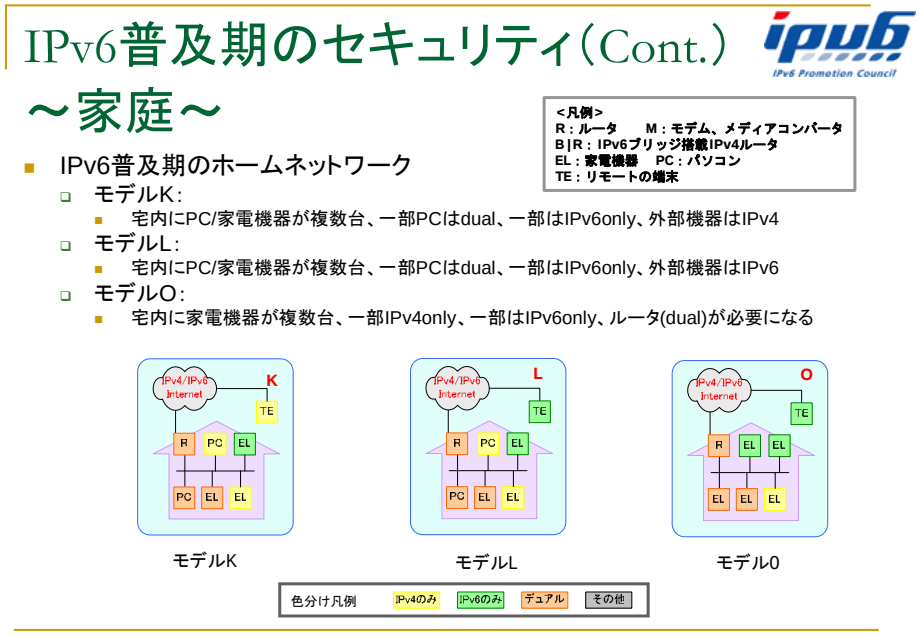
SOHO
nonPC 機器の接続と、外部連携、業務のアウトソースを行います。

大企業・自治体
全面的なデュアルスタック化を図り、業務アプリを IPv6 へシフト（P2P アプリケーション等）、さらに nonPC 含む多様な機器を接続します。マルチホーム（マルチプレフィクス）も必要となります。

以下では、関連する 3 章のサブアイテムも記述します。

IPv6 普及期のセキュリティ ～家庭～

IPv6 普及期のホームネットワークは、下図のような 3 つのモデルに類型化することができます。以下では、それぞれのモデルにおけるセキュリティを分析します。



モデル K

接続機器

PC・ゲーム機・nonPC 機器（AV・家電機器、IP カメラ、IP 電話）、IPv4 外部機器（携帯電話、PC（PDA））が接続されます。

利用アプリ

携帯からの VTR 予約、外部の機器で宅内カメラの映像を見るなどです。

セキュリティ分析

VTR や宅内カメラなどの non-PC への接続は、十分なセキュリティ機能の実装が難しいため、アクセスされる手前の段階で、十分な対策（不正アクセス対策、暗号化、ウィルス対策）がとられている必要があります。

外部からの接続は IPv4 であるため、家庭内機器が IPv6 オンリーの場合はトランスレータが必要となります。このトランスレータ及びその前後で、以上の対策がとれるかがポイ

ントになります。トランスレータが家庭内、もしくはホームルータの場合は、IPv4 での対策に依存します。

3 章の関連サブアイテム

A-1、A-2、A-3、B-2、C-1、C-2、F-1、G-2、H-1、H-2、K-1、K-2

モデル L

接続機器

PC ・ゲーム機・nonPC 機器（AV ・家電機器、IP カメラ、IP 電話），IPv6 外部機器（PC（PDA ））などです。

利用アプリ

携帯からの VTR 予約、外部の機器で宅内カメラ映像見る

セキュリティ分析

前頁のモデル K との差分は、IPv6 により直接接続が可能になる点ですが、nonPC に接続する手前で、不正アクセス対策、暗号化、ウイルス対策がとられている必要がある点は同じです。

3 章の関連サブアイテム

A-1 、A-2 、A-3 、B-2 、C-1 、C-2 、F-1 、G-2 、H-1 、H-2 、K-1 、K-2

モデル O

接続機器

ゲーム機・nonPC 機器（AV・家電機器、IP カメラ、IP 電話）です。

利用アプリ

TV とビデオが使われます。TV で宅内カメラの映像を見るなどです。

セキュリティ分析

家庭内には nonPC 機器しか存在しない場合ですが、外部 PC 等からの脅威がある以上、モデル K、L と同じです。

もしくは、 nonPC 同士が直接 P2P 通信するためには、管理サーバにより、継続的に、両者のアクセス制御ファイル、必要な通信モジュールが供給される仕組みが必要になるでしょう。

3 章の関連サブアイテム

A-1 、A-2 、A-3 、B-2 、C-1 、C-2 、F-1 、G-2 、H-1 、H-2 、K-1 、K-2

家庭におけるセキュリティ上の問題点（共通事項）

これまでケース別に紹介してきた IPv6 普及期の家庭におけるセキュリティで、共通の事項としては、次のような点が挙げられます。

ユーザオペレーション能力による問題

ユーザに対する啓蒙不足、ユーザの持つスキル不足、アドレスの打ち間違えによるフィルタ／制限適用ミスなどが問題となります。

家庭内機器のセキュリティポリシーの問題

家庭内機器間や機器提供者間で共通のセキュリティポリシーがないこと、PC、AV 機器、白物家電、センサ類など、機器の持つ能力によってそのセキュリティポリシーが変化すること、などが挙げられます。

コストの問題

家庭に導入する場合、低コストでなければならないという点も課題となります。CPE 等に低機能なものが多いのは、このためです。

セキュリティへの脅威（共通事項）

有効な対策がとられなければ、不正アクセスが容易になったり、踏み台にされる可能性が高まります。そして、迅速な対応ができず、さらに被害が広がる、といった脅威が顕著

になる可能性があります。

セキュリティ対策への課題（共通事項）

機器提供者、ネットワーク提供者、サービス提供者の間で、デフォルト設定に関するコンセンサスを得る必要があります。

使いやすい洗練された設定インタフェースの提供も課題で、パスワード変更の喚起、対話形式の GUI 等に工夫が求められます。

ツール類としては、利用目的に応じた名前解決ツール、家庭内検疫ツール等が求められます。

nonPC の利用目的にあったセキュリティ対策をサービスに組み込むことも考えられます。

IDS/IPS のような異常の検知と遮断、家庭内が踏み台になった場合の隔離、遮断など、ネットワーク側での境界サービスの提供も検討していく必要があります。

IPv6 普及期のセキュリティ ~SOHO~

IPv6 普及期の SOHO（独立 SOHO）では、次のような形になります。

まず、アドレスが豊富、自動設定が充実しているという利点から、様々なものが IPv6 で接続されていきます。PC 、プリンタ、IP 電話、PDA 、コピー機、FAX 、ホワイトボード、プロジェクタ、PC 周辺機器、防犯カメラ、タイムカードなどです。

また、外部ノードとの連携が増加していきます。その背景としては、P2P 通信に対応したセキュリティインフラの整備など、外部連携しやすい環境が整っていきます。さらに、業務のアウトソーシングが進むことも指摘できます。注文・予約システムの構築(Web ベースは現在もある)、問い合わせ・サポート受付、電話、TV 電話、コラボレーション(IPv6 化で広がる)などです。ビジネスのリアルタイム性が高くなることが IPv6 採用を促進します。

セキュリティ分析

ここでは、異なるセキュリティポリシー組織と相互接続の実現性を把握する必要があります。業務のアウトソース化、提携企業との業務連携により、異なるセキュリティポリシー組織と相互接続する形態となりますが、顧客情報漏えい対策（P マーク制度など）に基づく、明確な指針と対策が求められます。

まず、業務連携先毎に情報資産の漏洩対策ができていることが要求されます。PC の持ち出し/持ち込み禁止、ネットワークセグメントの分離等、さらにはコミュニケーション（電

話/テレビ会議相当）とコラボレーション（共同開発データのやり取り等）業務の分離等が対策として考えられます。

さらに、業務提携先と同レベルのセキュリティ対策（技術、意識、ポリシー）がとれることも課題となっていきます。

しかし、一般的な SOHO の特徴からの制約があります。SOHO の規模・安定性によりますが、一般的には、対策投資に対する中期的な効果の見積もりが難しい、専門の管理者がいないといった SOHO の特性から、セキュリティ対策に対する十分な投資が難しく、限定的な導入となると考えられます。

3 章の関連サブアイテム

利用する IPv6 技術により、すべての可能性があります。

セキュリティ課題

技術面以外の課題

セキュリティポリシーの確立とドキュメントの作成、そしてセキュリティ教育による社員の意識向上が課題となります。

技術面の課題

家庭と比べ技術運用スキルへの期待は持てますが、専門の管理者がいないため、迅速な対処が難しいこと、さらに対策技術の汎用性が見積もれない（提携先毎に異なる）ことが挙げられます。

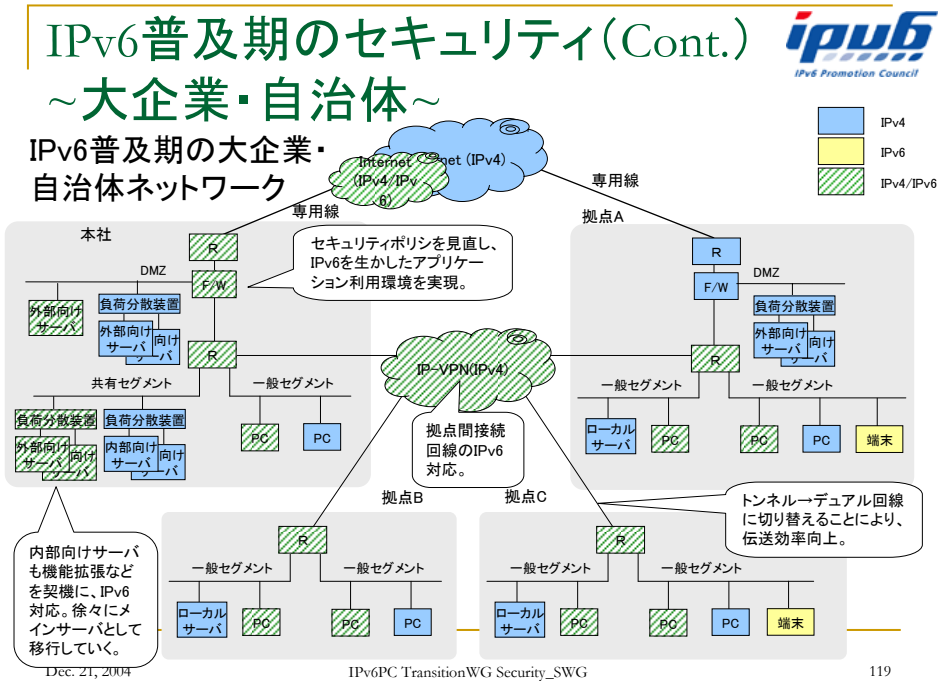
以上の課題から、第三者のセキュリティサービス（ASP 等)、提携先が構築する業務エクストラネットなど、第 3 者が提供する仕組みを利用するケースが多くなると思われます。

IPv6 普及期のセキュリティ ~大企業・自治体~

IPv6 普及期の大企業・自治体は、全面的に IPv4/IPv6 デュアルスタックネットワーク環境を導入し、IPv6 中心のアプリケーション利用環境へ順次シフトしていきます。P2P アプリケーションの業務利用（SIP ベース)や VoIP(内線、外線)、テレビ会議、ファイル共有、IM などが使われます。レガシーアプリは、トランスレータを介して接続されます。

また、多種多様な機器のネットワーク接続が想定されます。メンバ PC、プリンタ、非メンバ PC/PDA、ホワイトボード、複写機、照明、空調、センサ、監視カメラ、TV などです。

マルチホーム（外部接続の冗長化）やマルチプレフィクスも導入されます。



管理者からの RFP 例としては、次の点が挙げられます。

・Plug&Play、Secure（ユーザは端末をつなげば、設定なしに適切な相手とのみ安全に通信手段が提供される仕組みがあること）

・Traceable（管理者は、容易に端末の所有者/場所を同定できること）

・Manageable（管理者は、エンドユーザの設定を一括管理可能であること）

セキュリティ分析

RFP 例を満たす製品の登場により、P2P アプリケーションの業務利用、nonPC 機器の接続は、現在に比べ現実的になるだろうと思われます。IPv4 でも RFP 例に近い製品は登場傾向にあります。ただし、RFP 例に示されるような Centric な管理モデルは、管理ツール自体の脆弱性が顕在化した場合に被害が広がる（使用不能、管理データの漏洩等）可能性があり、被害最小化や復旧に対する代替策も必要となります。

3 章の関連サブアイテム

A-1、A-2、A-3、A-4、B-1、B-2、C-1、C-2、D-1、E-1、F-1、G-1、G-2、G-3、

H-1、H-2、K-1、K-2

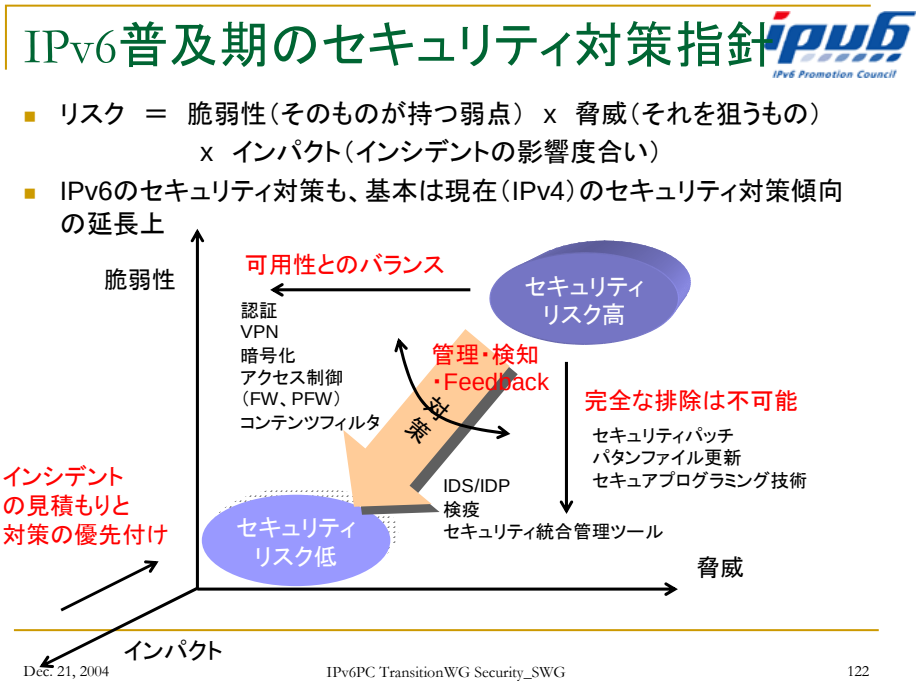
セキュリティ課題

上記の RFP 例と IPv6 普及期の状態を満足する以下のような製品の登場が課題となります。

・nonPC の特性に応じてセキュリティ GW 装置と連携したセキュリティ統合管理
・マルチプレフィクス環境におけるソースアドレス選択に対応したアクセス制御
・P2P アプリケーションの脆弱性を狙った攻撃の検知と遮断
・プレゼンス情報と連携した多段のアクセス制御

また、上記製品を用いた運用経験の蓄積も必要です。当初はセグメントを限定して運用課題を洗い出し、セキュリティ教育、運用ポリシーにフィードバックすることが必要となるでしょう。

IPv6 普及期のセキュリティ対策指針



上の図のように、リスク＝脆弱性×脅威×インパクトであることに変わりはなく、IPv6 のセキュリティ対策も、基本は現在（IPv4）のセキュリティ対策傾向の延長線上にあります。

IPv6 普及期のセキュリティの考察

セキュリティにおける 3 大要素である、情報資産の完全性（データ改竄防止、検知・復旧）、機密性（暗号管理、漏洩対策）、利便性（可用性）のバランスを高いレベルで実現するには、意識、ポリシー、技術への万遍ない投資が必要であり、IPv6 はその技術手段にすぎません。

しかし、IPv6 により P2P アプリケーション、nonPC 機器の利用が普及するにつれ、このバランスの実現レベルに変化が起こる可能性はあります。10 年前にある管理者は、「インターネットに接続するなんてとんでもない！」と発言していましたが、使ってみて初めて分かる便利さがあります。

技術的なセキュリティ対策項目は、IPv4、IPv6 で違いはありません。不正アクセス対策、暗号化、ウイルス対策などで求められるものは同じです。

IPv6 時代のファイアウォールについては、IPv6 においてもファイアウォール型の境界モデルは有効だと考えられます。ただし、通信の多様化に伴い、複数の対策ポイントでの対策と統合管理の仕組みが求められていくでしょう。

では、IPv6 でパラダイムシフトは起こるか、という点についてはどうでしょうか。

IPv6 の普及で IP 利用機器数は増加しますが IPv4 に比べ[IP 利用機器数/IP アドレス空間]は劇的に疎になります。ユーザの価値観（プライバシー、利便性、、）が多様化するとともに、モノの多様化や使われ方の多様化も進み、不正者の攻撃ターゲットは縮小（動機の低下）するかもしれません。最終的な選択権は利用者にあります。

これらのことから、セキュリティに対するパラダイムシフトが起こる可能性はあります。

Tips

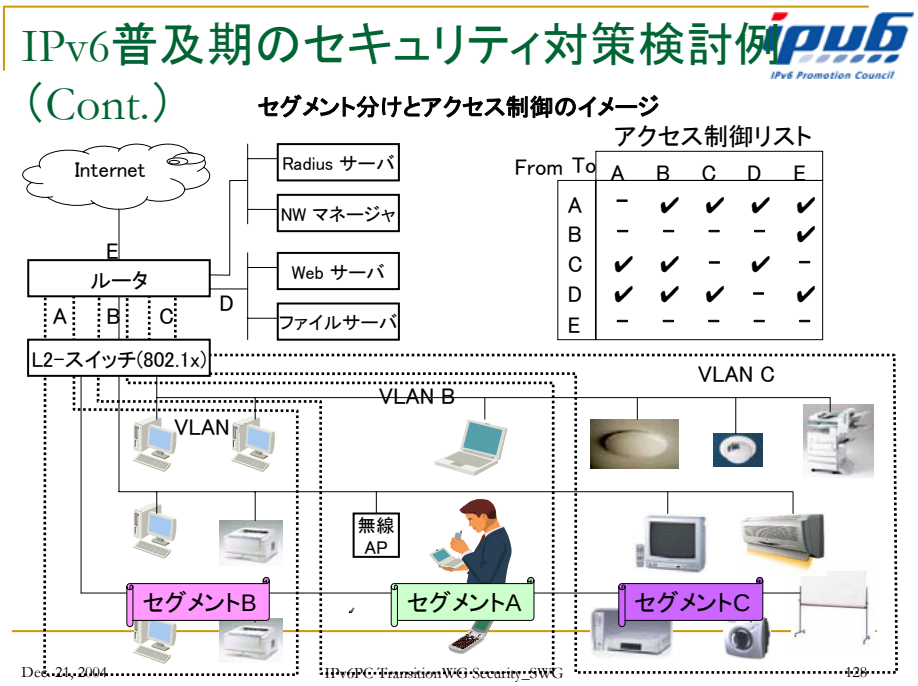
IPv6 普及期のセキュリティ対策検討例

1.　明確なセグメント分け

ネットワークにおいて、とりうる対策、脅威のレベルが異なる機器をセグメントとして明確に分けることが考えられます。

下図の例では、セグメント A が Incoming を許可する端末群、セグメント B が Outgoing のみ端末群、セグメント C が NonPC 群です。

セグメント化で期待される効用としては、インシデント発生時に被害伝播を極小化できること、混在収容した場合と比べ、トータル運用コストの低減が期待できること、があります。



2.　セグメント A での検討

アクセス元は複数の手段、対策ポイントでアクセス制御されているかを検討します。IP フィルタ、SPI などのセッション制御、アプリレベルの認証などを、境界、エンドポイント

などで実施します。
IPv6 による効用として、アドレス空間が広がることにより、総当り的な第 3 者からの攻撃による脅威の低減は期待できます。

3. セグメント B での検討

このセグメントでは、従来の IPv4 と同じ対策が有効です。従来（IPv4）と同じ利用内容（Web、Mail）の場合、このセグメントは IPv6 にしても外部ルーティングさせる必要は必ずしもありません。従来の利用（Web、Mail、DNS）では内部サーバとの通信のみで、この場合 IPv6 は内部ネットワーク通信用として利用します。

4. セグメント A、B とセグメント C の相互接続検討

目的と照らして直接接続する必要があるか、PC での脆弱性が nonPC に伝播しない策がとられているかを検討します。直接のルーティングはさせず、プロキシ、ゲートウェイ装置を介した接続に限定することが求められます。

5. セグメント A とセグメント B との相互接続

必要なければ直接のルーティングはさせません。プロキシ、GW 装置を介した接続に限定します。もしくは、検疫したうえで通信を許可します。

IETF における IPv6 セキュリティ検討状況

2004 年 12 月 13 日時点で、IETF では以下のような IPv6 セキュリティ関連の RFC やインターネットドラフトが見られます。

IPv6 Neighbor Discovery trust models and threats
RFC3756
IPv6 Transition/Co-existence Security Considerations
draft-savola-v6ops-security-overview-03.txt
IPv6 Security Problem Statement
draft-vives-v6ops-ipv6-security-ps-02.txt
Security Considerations for 6to4
RFC3964

Firewalling Considerations for IPv6
draft-savola-v6ops-firewalling-03.txt
IPv6 distributed security requirements
draft-palet-v6ops-ipv6security-01.txt
Quarantine Model Overview for IPv6 Network Security
draft-kondo-quarantine-overview-01.txt
Threats relating to IPv6 multihoming solutions
draft-nordmark-multi6-threats-02.txt
SEcure Neighbor Discovery (SEND)
draft-ietf-send-ndopt-06
Cryptographically Generated Addresses (CGA)
draft-ietf-send-cga-06.txt

IPv6 普及期のセキュリティモデルのアイデア

IPv6 普及期におけるセキュリティモデルとしては、以下のものが考えられます。

シンクライアントモデル（脆弱なものを持たない）

これは、端末がブート時に管理サーバと接続し、必要なプログラムは管理サーバから最新のものを都度入手し動作するというモデルです。脆弱性の低減に寄与します。

耐タンパーモデル（危険を察知して落ちる）

機密情報の不正持ち出し防止を目的としたモデルで、コンテンツ、プログラムは暗号化されており、必要に応じて復号化して利用します。nonPC ベースの場合、不正アクセスの検知で自己破壊するメカニズムを持ちます。

ステルスモデル（存在を隠す）

これは、管理サーバが仲介してサービスマッチングや相手アドレスの通知を行うモデルです。入手した乱数に従い、定期的に IP アドレス（インタフェース ID）を変更するなど、第 3 者からの特定のされにくさを狙います。

検討メンバ

中井（Chair、NTT コミュニケーションズ）

荒野（インテックネットコア）
石原（KDDI）
石原（東芝）
井上（東芝）
猪俣（富士通）
上杉（日立製作所）
卯城（Checkpoint）
岡（東芝ソリューション）
橘田（Checkpoint）
久保田（松下電器）
近藤（トレンドマイクロ）
近藤（NEC）
斎木（新日鉄ソリューションズ）
阪内（NEC）
佐藤（新日鉄ソリューションズ）
島田（富士通アクセス）
清水（東芝ソリューション）
鈴木（日立製作所）
高橋（トレンドマイクロ）
滝澤（富士通アクセス）
月岡（日立製作所）
橋本（三菱総合研究所）
平林（三菱総合研究所）
平山（トレンドマイクロ）
廣海（インテックネットコア）
古川（富士通アクセス）
村田（松下電器）
横田（松下電器）
吉本（Checkpoint）