UPnP-IGDを応用したIPSバイパス手法の提案と実装

中島 智広[1] 水谷 正慶[1] 佐川 昭宏[2] 白畑 真[2] 南 政樹[2] 村井 純[1,2]

慶應義塾大学環境情報学部[1] 慶應義塾大学大学院政策・メディア研究科[2]

ネットワークからの脅威を防ぐ手法にIPSが挙げられる。IPSは，その性質から誤検知による正常な通信の阻害や遅延の発生と言った問題を抱えている。そのため，ある側面においてユーザの利便性を損ね，End-to-Endモデルの可能性を狭める要因ともなっている。本研究では，広く普及したプロトコルであるUPnPを用いることで，ユーザにIPSの迂回ルールを設定させる手法を提案し，実装，評価を行った。

IPS Bypass Method based on UPnP-IGD

Tomohiro Nakashima[1], Masayoshi Mizutani[1], Akihiro Sagawa[2], Shin Shirahata[2], Masaki Minami[2], Jun Murai[1,2]

[1]Faculty of Environmental Information, Keio University

[2]Graduate School of Media and Governance, Keio University

IPS(Intrusion Prevention System) is a conventional method to defend from network threats. IPS has some problems. such as "Delay", "False positive" and "Difficulty of Operation". Therefore, there is trade off between usability and is improving the security by the introduction of these equipment. In this research, it is proposed a technique that the user had a detour rule of IPS set.

1 背景

パケットフィルタ型ファイアウォールは，インターネットに接続するネットワークへの脅威に対する防御策として広く用いられている。この手法は，インターネットに接続するネットワークの間で用いられ，パケットのヘッダ情報に基づいて予め指定されたルールに則り，不必要なサービスに対する通信を識別し遮断する。しかし，ヘッダ情報に基づいて識別しているため，正常な通信を装った脅威を識別して遮断できない欠点がある。

この欠点を補う手法の一つがIPS(Intrusion Prevention System)である。一般的なIPSの手法であるミスユース型IPSは，ファイアウォールと同様にインターネットそれに接続するネットワーク間で動作し，パケットのヘッダ情報に加えてペイロード情報を識別することで，正常な通信を装った脅威を識別できる。ところが，ペイロード情報を識別するにはパケット再構成の処理が必要なことから，バッファリングによる遅延が起こる。また，予め設定されたルールに対してパターンマッチを実行していることから，しばしば誤検知が起きる。

[1],[2]Keio University Shonan Fujisawa Campus
5322, Endo, Fujisawa, Kanagawa 252, Japan
E-Mail: shima@sfc.wide.ad.jp

2 問題点

第1節で述べたIPSの構造的な問題をふまえ，実際にIPSを運用していく上でどのような問題があるかを述べる。

誤検知の対策として，IPSの設定を変更し，問題となっているノードへの正常な通信をルールから外すといった管理者の介在が不可欠であり，速やかな対応には限界がある。

遅延については，ビデオ会議やIP電話のようなストリーミングを前提としたアプリケーションを利用する際に大きな制約となる。従ってIPSを運用するネットワークでは，アプリケーションの利用が制限されることがある。

さらにこれらの限界や制約は，ユーザの立場から制御できるわけではなく，また，一般のネットワークエラーと区別することは非常に困難である。

以上の理由から，IPSの導入はネットワークの安全性を高める一方，ユーザ・管理者双方にとって問題がある。このことから，安全性を提供しつつ，管理者・ユーザ双方に利便性を提供することが必要である。

3 関連研究

安全性と利便性を提供するという目的に対する関連研究として，検疫ネットワーク [6] を挙げる。検疫ネットワークとは，エンドノードがネットワークへ接続する際に検疫を行い，その結果に応じて接続セグメントを選択する技術である。検疫ネットワークは，セキュリティ対策が施されていない無防備なエンドノードがネットワークに接続することを防ぐ。逆に，十分なセキュリティ対策が施されているエンドノードに対しては，自由な接続性を与えることもできる。

検疫ネットワークでは，エンドノードを接続しただけでは，通常のセグメントには接続されず，隔離された特別なセグメントに接続される。この特別なセグメントで検疫を行い，その結果によって接続セグメントが選択される。

検疫は，エンドノードで実行される検疫プログラムで行われ，その結果はサーバに送信される。検疫項目には，OS のバージョンやセキュリティパッチの適用歴，ウイルス対策ソフトやパーソナルファイヤーウォールの導入の有無，パターンファイルのバージョンなどが挙げられる。サーバに送信された検疫結果を基に，安全であると判断されたエンドノードのみが，通常のセグメントへ接続される。さらにその度合いに応じて，セグメントを選択する事も可能で，ノードによって外部からの自由にアクセス可能なセグメントを割り当てると言ったこともできる。検疫ネットワークにおいては，ユーザが問題を解決するにあたり，ネットワークの安全性を損ねないという特徴がある。

4 解決手法の提案

管理者が集中的に IPS を運用することは非常にコストが高い。一方で，あるユーザにとって IPS の存在はアプリケーションを制限する可能性があり利便性が低い。この問題に対して IPS による脅威からの防御をトレードオフとして，意識の高いユーザに対しては IPS に関してある範囲の制御権を委譲できる仕組みがあれば，全てのルールを管理者が設定の変更をしなくても利便性の高いネットワークを提供できる。

そこで，本研究ではユーザがネットワーク管理者が許可した範囲において一時的に IPS を迂回する仕組みを提供し，この利便性と安全性についての選択肢を提供する。

これを実現するために，ブロードバンドルータなどをユーザが制御するために用いられている，UPnP(Universal Plug and Play) 機能を利用し，IPS を制御する手法を提案する。

4.1 モデルの提案

本稿では，図 1 に示すモデルを提案する。本モデルでは，IPS と同一マシン上で実装を動作させパケットの流れを制御することで，IPS の迂回を実現する。ルールを設定するユーザには，管理者と通常のユーザの二種類が居る。管理者からは基本ポリシー，ユーザからは UPnP を用いて迂回ルールを受け付ける。管理者からの基本ポリシー，ユーザからの迂回ルールを照らし合わせ，基本ポリシーの枠内でユーザの設定を適用する。

4.2 UPnP の利用

UPnP は標準化され，広く普及したプロトコルである。UPnP は Intel，Microsoft，HP などが中心となって策定した機器制御技術で，情報家電及び，パーソナルコンピュータ (PC) とその周辺機器の接続を容易にし，機器の制御を目的としている。UPnP を用いたデバイスに，UPnP-IGD(Universal Plug and Play Internet Gateway Device) がある。UPnP-IGD は，複数のネットワークインターフェイスを有し，ネットワークの境界に位置するルータである IGD(Internet Gateway Device) の設定を，UPnP を用いて変更できるようにしたものである。この UPnP-IGD の手法を応用することで，IPS に対し設定を行う。

UPnP-IGD を応用する利点は，広く普及していることにある。WindowsXP では，標準で UPnP-IGD クライアントが用意されている。加えて，自動的に機器が認識されるため，ユーザが IPS についての情報をあまり知らなくとも設定を行うことができる。

ただし，UPnP はセキュリティを意識して作られたプロトコルではないため，悪意を持ったユーザがローカルネットワーク内に存在する場合，悪用される可能性がある。そこで，管理者がエンドノードから受け付ける設定を制限できるようにする。ユーザは管理者が設定したルールの枠内で IPS に対しにルールを設定できる。

5 設計

第 4 節で述べた提案を元に，以下のように設計を行った。本システムは，大きく分けて設定クライアント，設定管理機構，パケット振り分け機構の三つに分かれる。

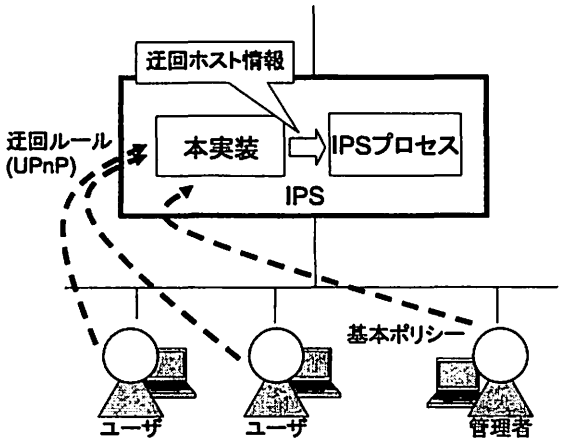

図 1: 提案モデル

5.1 設定クライアント

設定クライアントは，ユーザが利用するエンドノードから本実装に対して制御情報を送るために用いる。制御情報は，送信先ノードの「IP アドレス」「プロトコル」「ポート番号」を組み合わせて迂回ホスト情報と定義する。この迂回情報を UPnP-IGD として実装した本実装に対して送信することで，ユーザは IPS を迂回するよう制御できる。

5.2 設定管理機構

設定管理機構は，IPS が組み込まれたマシンで動作し，前述の設定クライアントからのルール設定要求を受け取る。設定管理機構は受け取ったと管理者が設定したルールと比較し，適当な場合はパケット振り分け機構の振り分けルールに反映する。本機構はルールを管理する役割を担い，適切な運用がなされていることを監視する役割を持つ。

5.3 パケット振り分け機構

パケット振り分け機構では，設定管理機構から設定されたルールに基づき，パケットを IPS を通るもの，迂回するものに振り分ける。

6 実装

6.1 実装環境

実装環境を表 1 に示す。IPS を稼働させる OS として Debian GNU/Linux，ライブラリとして libupnp,libiptc を用いた。IPS には Snort-inline[1] を用いた。

6.2 パケット振り分け機構

本実装では，パケット振り分け機構として iptables[2] を用いた。iptables は，Linux のパケットフィルタリングを実現するネットワークモジュールである。本実装は iptables のルール管理をすることで，IPS を通過するパケット，IPS を迂回するパケットに分ける。ルールには管理者が予め定義するルールと，ユーザがエンドノードから設定するルールがある。ユーザがエンドノードから設定するための手法として，UPnP-IGD のプロトコルを用いる。本実装はエンドノードからルールの追加要求を受け取り，予め管理者が設定したルールと比較し，ルールが適当であれば，iptables のに対しルールを適用する。ルールが反映された結果，ユーザが指定されたパケットのみ IPS を迂回するようになる。

図 2 に実装概要を示す。

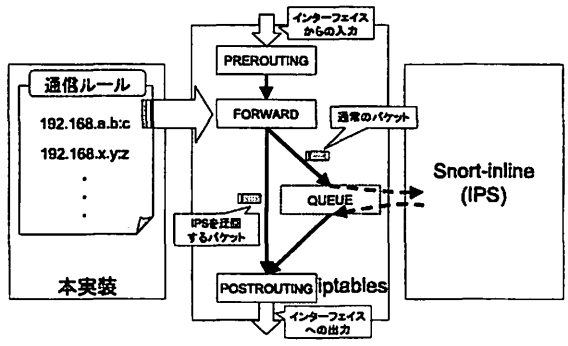

図 2: 実装概要

iptables ではインタフェースに入力されたすべてのパケットは PREROUTING チェインに入力される。パケットの中で自分以外に宛てられたものは，FORWARD チェインを経て，POSTROUTING チェインから対向インターフェイスに出力される。

今回用いた IPS である Snort-inline は，iptables の QUEUE チェインからパケットを受け取り，POSTROUTEING チェインに戻す仕様である。そのため通常は，FORWARD チェインから QUEUE チェインへ転送するルールを記述し，Snort-Inline へパケットを渡している。QUEUE チェインは，パケットをユーザ空間のプログラムやアプリケーションへキューイングするために用いられるチェインである。

そこで，FORWARD チェインから QUEUE チェインへ渡すルールに加えて，直接 POSTROUTING チェインに渡すルールを追加し，パケットを振り分ける。

7 評価

7.1 スループットの改善

本実装による遅延の改善を評価するにあたり，IPSを通した場合と，本実装を用いて迂回した場合のスループットを計測した。計測ツールにはnetperf[4]を用いた。

実験 IPSを通常動作させすべての通信を監視した場合と，本実装を用いIPSを迂回させた場合のスループットの比較

スループットを以下の条件に従い測定した.

- TCPによりホスト1からホスト2にデータを送信.
- TCPのペイロードは0の羅列によるパケット.
- パケットのサイズを60byteから1500byteまで変化させる.

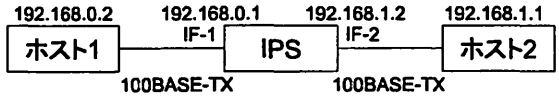

図 3: 評価実験トポロジ

表 1: 評価実験環境

	IPS	ホスト 1, ホスト 2
CPU	PentiumIII 900MHz	PentiumIII 800MHz
Memory	384MB	256MB
OS	Debian GNU/Linux	WindowsXP
Interface	100Base-TX	100Base-TX

実験結果を図4に示す。初期状態のIPSを通す設定では，スループットが40Mbps程度であったのに対し，迂回する設定ではインターフェイスの理論値に近いパフォーマンスを得ることができた。

本実装では，パケットがユーザランドに渡される前に，iptablesを用いてパケットを迂回しているため，高いスループットを実現できたと考察される。

7.2 モデルの評価

本モデルを評価するにあたり，手動設定を用いた場合と検疫ネットワークを用いた場合とで比較し，定性的評価として表2にまとめた。

まず，設定変更時の管理者負担であるが，UPnP-IGDを応用することで，設定が容易になり，ルールの設定を管理者からユーザに委譲できた。そのため，管理者の負担を減らすことができた。また，ユーザについても，WindowsXP標準のIGDクライアントを用いた設定が可能である。そのため，ユーザに対する追加負担は軽い。

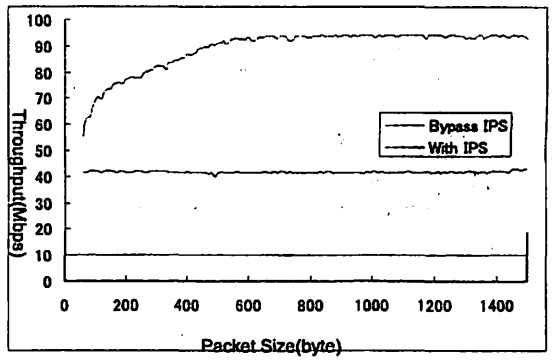

図 4: スループットの変化

また，ユーザにIPSをバイパスさせる手段を提供することで，IPSのルールを調整せずとも，IPSの抱える問題に暫定的に対処できる。そのため，管理者の手を煩わせることなく，ユーザが設定を反映することができるようになったため，即応性が高まった。

以上の二点について検疫ネットワークでは，検疫によってセグメントが選択されるため，検疫に合格している以上，そもそも何も設定をする必要がない。

安全性について本実装ではホストの安全性に対する責任を一部ユーザに委譲している。また，管理者はユーザの設定を一定の枠内に制限できるため，ユーザへ設定の強制も実現できる。このため，設定に幅を持たせることが可能となり，ユーザが十分に理解している環境であれば手動設定や検疫ネットワークと同等の安全性を確保できるといえる。

表 2: 定性的評価

	本実装	手動設定	検疫ネットワーク
管理者負担	○	×	△
設定即応性	○	×	○
安全性	○	○	○

8 今後の課題

本研究では，管理者が設定した基本ルールの枠内で，ユーザの設定を許可することで，IPSを有効活

用する手法を実現した。しかしながら，本研究の成果物では，管理者が設定した基本ルールを，ユーザに対し周知させる手段がない。本実装を有効活用していくためには，この問題を解決する必要がある。

9 まとめ

本研究では，境界防御機構の一つである IPS に焦点をあて，問題点を述べると同時に，解決手法として，広く普及したプロトコルである UPnP を用いたバイパス機構を提案し，実装・評価を行った。

本研究によりこれまでの IPS の問題であった，誤検知と遅延への対応を可能とした。

参考文献

[1] Snort-inline. http://snort-inline.sourceforge.net.

[2] Oskar Andreasson. Iptables tutorial 1.2.0, July 2005. http://iptables-tutorial.frozentux.net/iptables-tutorial.html.

[3] UPnP Forum. Internet gateway device (igd) v 1.0, December 2001. http://www.upnp.org/standardizeddcps/igd.asp.

[4] Rick Jones. Netperf. http://www.netperf.org/netperf/NetperfPage.html.

[5] Jack Weast Michael Jeronimo. *Upnp Design by Example: A Software Developer's Guide to Universal Plug and Play.* Intel Press, May 2003.

[6] 角将高, 馬場達也, 藤本浩, 稲田勉. エンドスイッチ非依存型検疫システムの検討. 電子情報通信学会大会講演論文集 Vol.2005, September 2005.

[7] 坂田史郎, 金森重友, 齋藤充, 佐野勝大. SIP/UPnP 情報家電プロトコル. 秀和システム, February 2005.