Vol.2010-IOT-11 No.9
2010/10/15

# L2/L3 スイッチを用いた動的な 透過型ファイアウォールの運用に関する一考察

土　屋　英　亮[†1]

透過型ファイアウォールは，ネットワークの論理構造を変更することなしに挿入することが可能な非常に便利なセキュリティ機器の一つである．本稿は L2/L3 スイッチの運用を工夫することで安価な動的透過型ファイア ウォールを構築する手法を説明し，その運用について解説する．

# A study of the transparent firewalls using L2/L3 switching devices

Hideaki Tsuchiya[†1]

The transparent firewalls are the useful security devices, that are capable to sit in-line without changing of the network logical topology. In this paper, L2/L3 switching devices are used as the dynamic transparent firewalls and operational results are shown.

## 1. はじめに

ファイアウォールはインターネットの商用接続が開始された 1990 年代初期頃より利用されている情報ネットワーク保護技術の一つである[1)]．基本的にはインターネットと LAN の境界に設置され，組織外から組織内あるいは組織内から組織外の通信のなかで，ポリシーに一致するものを通過させ，ポリシーに一致しないものを破棄する機能を持つ．

歴史的にはルータに搭載されたアクセスコントロールリスト（以下 ACL と書く）がファイアウォールの原点だと考えられる．その後，ファイアウォール機能に特化した専用機や，内部をソフトウェア制御ではなく専用 LSI 化してハードウェア制御にしたものや，ファイアウォール機能だけではなく通過するパケットを検査する機能やその他のセキュリティ対策を行なう複合機へと進化している．

また，クライアントコンピュータの性能向上にともない，クライアントコンピュータのネットワークインタフェースを通過する通信を監視し，ポリシーに一致しないパケットを破棄する機能を持つトラフィック監視ソフトウェアが利用されるようになった．これらをパーソナルファイアウォールと呼び、ファイアウォールに分類される．

本稿では，インターネットと組織内 LAN の対外接続部に設置するファイアウォールに注目する．著者の所属する電気通信大学（以下電通大と書く）のファイアウォール運用を概観し，セキュリティ機器運用の問題点と，L2/L3 スイッチを用いた解決策を説明する．実運用のデータを示してその有効性を検討する．最後に今後の課題を示す．

†1 電気通信大学 情報基盤センター
Information, Technology Center, The University of Electro-Cummunications

表 1　電通大で利用してきたセキュリティ機器

| 調達年 | 製品名 |
|---|---|
| 2002 年 | Nokia IP440 |
| 2002 年 | IIS RealSecure Network Sensor 6.5 |
| 2006 年 | IBM Proventia G200 |
| 2009 年 | FortiNetwork FortiGate-310B |
| 2010 年 | FortiNetwork FortiGate-620B |
| | BivioNetwork Bivio 7512 |

## 2. 電通大におけるセキュリティ機器の運用

電通大のネットワークシステムは 4 年毎に行なわれる情報基盤センターシステムリプレースにより調達される．学内 LAN と対外ネットワークである SINET との対外接続部に設置されるファイアウォールや IDS, IPS も同時にリプレースされる．電通大がこれまでに利用してきたファイアウォール, IDS, IPS 等のネットワーク対応セキュリティ機器の一覧を表 1 に示す．

このうち 2002 年の Nokia IP440, 2006 年の IBM Proventia G200, 2010 年の FortiNetwork FortiGate-620B, BivioNetwork Bivio 7512 はセンターシステムリプレースにより調達された機器であり，2002 年の IIS RealSecure Network Sensor 6.5 及び 2009 年の FortiNetwork FortiGate-310B は，それ以外の理由により調達された機器である．

これらの機器を説明すると，Nokia IP440 は静的なアクセスポリシーを設定可能なファイ

アウォールルータ，IIS RealSecure Network Sensor 6.5 は IDS, IBM Proventia G200 は IDS/IPS, FortiNetwork FortiGate-310B, FortiGate-620B は UTM, BivioNetwork Bivio 7512 はプログラマブル DPI アプリケーションプラットホームとなる．

これらセキュリティ機器をどのように利用してきたかを簡単に紹介する．

**Nokia IP440** 対外接続ルータとして利用していた．静的なファイアウォールとしていくつかのポリシーを設定していた．

**IIS RealSecure Network Sensor 6.5** 対外接続ルータと SINET 側のルータ間にタッピングハブを介して接続し，IDS として利用していた．

**IBM Proventia G200** IPS として利用する予定だったが，SINET へのアップリンクが 1Gbps に増速されたことと IPS での利用には制限があることが判明したため，対外接続ルータと SINET 側のルータ間にタッピングハブを介して接続し，IDS として利用した．

**FortiNetwork FortiGate-310B, FortiGate-620B** 対外接続ルータと SINET 側のルータ間にインラインで接続している．ステルスモードで IDS/IPS を稼働させている．

**BivioNetwork Bivio 7512** 実験時に対外接続ルータと SINET 側のルータ間にインラインで接続している．ステルスモードで動作させている．

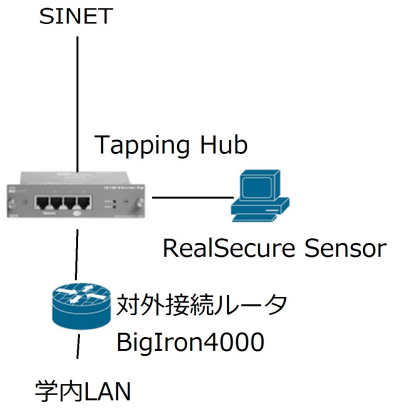


**図 1** RealSecure Network Sensor の接続図

電通大におけるセキュリティ機器は，ネットワークの帯域幅を制限しないよう，かつ，故障時にネットワーク運用を阻害しないように設置することとしている．前者は当然のこととして，後者は，セキュリティ機器を二重化する等の耐故障性を向上させる運用がコスト的に不可能なので，万が一の障害に備えて問題が発生しない設置を行なうという意味である．

これらセキュリティ機器の実運用で発生した問題を示す．Nokia IP440 はファイアウォールルータであり，運用の後半には，パケット長の短い UDP パケットを大量に送信してくる DoS 攻撃に対してサービス不能に陥ることがしばしば発生した．そのため，Nokia IP440 の利用をやめ後段に設置していたルータの ACL をファイアウォールとして用いた．この事例は，セキュリティ機器の処理能力が攻撃者のそれより低いと，セキュリティは破綻することを示していた．また，そのルータも分散 DoS 攻撃によりパケットルーティング能力の限界を越えて運用停止してしまうことがあった．このときは，ルータの対外接続部のインタフェースにて攻撃をしてくる全ての送信元 IP アドレスを遮断する ACL を設定して攻撃パケットの侵入を阻止した．この事例は攻撃者の IP アドレスをすばやく検出してそれに対応しなければならないことを示していた．

RealSecure Network Sensor 6.5 は対外接続部に接続されたタッピングハブに接続されていた．この接続方法で問題なく運用できると考えられていたが，2003 年 1 月 25 日に発生した SQL Slammer ワーム[2] の蔓延時にあまりに大量の攻撃パケットを検出したため RealSecure Network Sensor 6.5 のバックエンドのデータベースが過負荷で異常停止してしまい，SQL Slammer ワームの影響がなくなるまで，運用を再開することができなかった．これは対外接続部の配線が図 1 のようになっていたためと，適切に IDS のポリシーを変更できなかったためである．センサーが接続されているタッピングハブの上流にファイアウォールを設置して Slammer ワームの送信してくる UDP パケットを遮断すれば IDS が停止することはなかったであろうし，また，IDS の検出ポリシーより SQL Slammer からの攻撃のシグネチャを無効にすれば IDS の負荷を軽減可能だったと考えられる．

Proventia G200 は RealSecure Network Sensor 6.5 では不可能だった IPS としての運用を期待して選定された．IPS の処理能力は 200Mbps である．しかし導入の 1 年後の SINET が SINET3[3] へとアップデートする際に対外接続部のアップリングが 1Gbps に増速され IPS としての処理能力が不足することと，シグネチャファイルのアップデートする時にパケットフォワーディングが停止することがあり得ることによりステルス型 IPS としての運用を諦め，RealSecure Network Sensor 6.5 と同様にタッピングハブを介して接続し IDS と

して運用することとした．

この Proventia G200 も RealSecure Network Sensor 6.5 と同様に過負荷で異常終了してしまい，対外接続部の監視が不可能となることが発生した．複数のホストからサイズの小さい大量の UDP パケットを送信してくる分散型 DoS 攻撃を観測したときに，異常終了してしまうことが少なからずあった．

これらの運用経験により，IDS あるいは IPS を安全に運用するためには，それらの処理能力を超える不必要あるいは有害な観測パケットを遮断するか，常時適切にポリシーを再設定し過負荷を発生させないように調整を行なう必要がある．前者はともかくとして，後者に関しては，IDS あるいは IPS で処理すべき攻撃パケットが過負荷となる場合はそれをあえて無視するようポリシーを再設定するということは IDS や IPS の機能と矛盾する．これを避けるにはより高性能なセキュリティ機器を用意すればよいのだが，コストの問題でそれが困難なことも多い．

## 3. セキュリティ機器を保護するファイアウォールの構築とその改良

2007 年に次期ネットワークシステムの評価として運用実験を行なっていた H3C S5100-24 L2/L3 スイッチは，ギガビットに対応したイーサネット・スイッチ製品である[4]．この製品は L2 スイッチの機能のみならず基本的な L3 スイッチの機能も搭載している．ただし，この L3 スイッチ機能はベーシック L3 機能と称され，複雑なルーティングには対応しないと説明されている．

このスイッチは簡易的な L3 スイッチの機能を持つ L2 スイッチであり，IP ACL 機能も

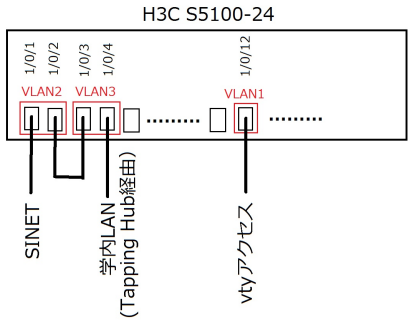


**図 2** H3C S5100-25 のインタフェース接続

有している．IP ACL 機能を実験で確認したところ，IP アドレスを割り当てた L3 スイッチとして利用されているインタフェースには当然利用可能であるが，IP アドレスを割り当てていない L2 スイッチとして利用されているインタフェースを通過するフレームに対しても IP ACL が適用されることが判明した．これはすなわち，このスイッチをステルス型のファイアウォールとして利用できるということである．IP ACL を挿入することによる通信遅延は，IP ACL がハードウェアで実行されることにより許容範囲内で収まることが予想される．

電通大では，このスイッチを対外接続部のタッピングハブと SINET ルータの間に接続し，IDS に到達する前に有害であったり不要であったりするパケットを遮断するファイアウォールとして利用することとした．調査の結果，H3C S5100 シリーズは，1 個のインタフェースに対して 200 行の ACL を挿入可能であり，ボックス全体で有効な ACL の行数は不明であった．ACL は入力トラフィックに対して適用される．定義された IP ACL のルールセットの末尾は，一般的な IP ACL で適用される暗黙の deny ではなく，全ての通信を permit する ACL が挿入される．

接続は通常の L2 スイッチと同様である．アップリンクとダウンリンクにそれぞれ IP ACL を設定することで，トラフィックの双方向に IP ACL を設定可能となる．加えて，スイッチにポート VLAN を設定しポートを分割することにより，200 行を超える ACL を設定可能となる．

配線図を図 2 に示す．H3C S5100-24 の interface GibabitEthernet 1/0/1 と 1/0/2, 1/0/3 と 1/0/4 がそれぞれ同一ポートとなるようにポート VLAN が設定してある．if GE 1/0/1 には 67 行，if GE 1/0/2 には 52 行の基本的な IP ACL を静的に設定し，不正な送信 IP アドレスのパケットや，LAN 内部でのみ利用されるプロトコル等の不要あるいは有害なパケットを遮断した．

この L2/L3 スイッチによるステルス型静的ファイアウォールの運用開始により IBM Proventia G200 の異常終了は減少し監視ポリシーをデフォルトのままとして運用することができた．学内ネットワークについては同様の IP ACL をルータにて設定していたので特に変化はなかった．しかしながら，突発的に発生する DoS 攻撃等に対して IDS ひいては学内ネットワークを保護することはできなかった．そこで，IDS からの攻撃警報を利用して動的にファイアウォールを設定するスクリプトを作成し定期的に実行するよう設定した．

動的ファイアウォール設定のスクリプトは，IDS が syslog を転送するログ収集サーバ上で 10 分おきに動作し，

(1) syslog ファイルよりログ情報を収集し統計情報を作成する．

(2) 統計情報に予め設定された閾値を超える回数の攻撃を行なう攻撃元 IP アドレスがあれば遮断リストにその IP アドレスと遮断時刻を登録する．
(3) リストから予め定められた期間を経過した遮断 IP アドレスを削除する．
(4) リストより遮断 IP アドレスを発アドレスとするパケットを全て遮断する IP ACL を作成する．
(5) H3C S5100-24 に telnet セッションを行なってインタフェース GE 1/0/3 あるいは 1/0/4 に IP ACL を設定する．

なる動作を行なう．動的ファイアウォール設定スクリプトは，syslog 収集スクリプト，遮断リスト作成スクリプト，スイッチ設定スクリプトから成る．shell スクリプトと perl スクリプトによって構成され，合計 371 行のスクリプト群である．Telnet セッションによる IP ACL の設定は，CPAN Net::Telnet モジュール[5] を用いて実装した．

この動的ファイアウォール設定スクリプトは，対外接続部のアップリンクとダウンリンクの両方に設定した．インターネットから学内ネットワークへの攻撃を遮断すると同時に，不慮の事態が発生して学内ネットワークに接続したホストがインターネット上のホストあるいはネットワークを攻撃を行なったときに通信を遮断することを可能としている．

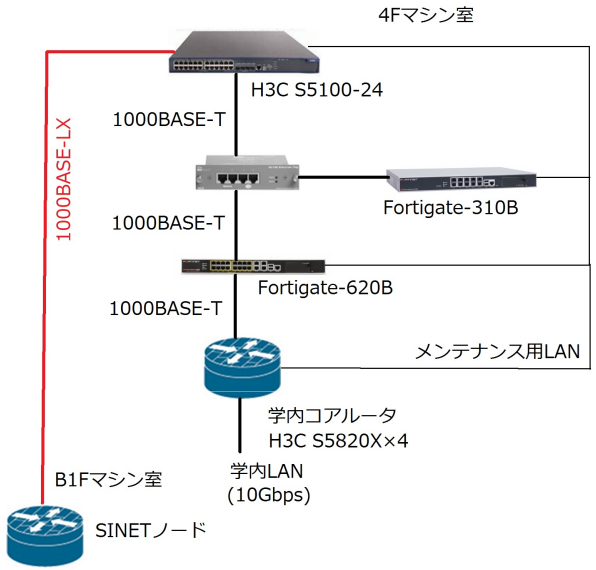


**図 3** 現在の対外接続部の接続図

遮断対象となる IDS シグネチャは，

- ssh, telnet, ftp, rdp に対するの不正ログインやブルートフォースアタック．
- TCP, UDP ポートスキャンや ping スキャン
- ボットネット等の悪質な通信．

を設定して運用した．

2009 年に IDS/IPS の Fortigate-310B が導入された．これは P2P ファイル共有ソフトウェアの活動を検出する目的で導入された．IBM Proventia 200G と併用され，Proventia 200G は一般的な攻撃を検出し，Foritgate-310B は P2P ファイル共有ソフトウェアの活動を検出した．電通大では，研究用途以外の P2P ファイル共有ソフトウェアの利用をポリシーとして禁止している．学内から学外へのアップリンクについては，これらの検出シグネチャも遮断対象とした．

2010 年 3 月の新システムより IDS/IPS は Fortigate-620B へと更新された．SINET3 に接続されている間は IPS の処理能力に問題はないため，ステルス型 IDS/IPS として利用している．対外接続部の接続は図 3 のようになっている．

## 4. L2/L3 スイッチによるファイアウォールの運用実績と問題点

2010 年 2 月 1 日から 20 日まで，2010 年 7 月 1 日から 20 日までのファイアウォールによる動的な遮断件数を図 4 に示す．前者は IDS として IBM Proventia G200 と Fortigate-310B を併用していた時期のものであり，後者は IDS として Fortigate-620B を用いている時期のものである．

明らかに 2 台の IDS を利用してた時期のほうが遮断件数が多いことがわかる．これは，IDS/IPS の検出シグネチャにはベンダあるいは製品ごとに特徴があり，決して同じ検出結果を出力しないためである．傾向として IBM Proventia G200 はネットワーク全体に対する攻撃や検査をよく検出し，Fortigate-620B は個々のホストに対する個々のプロトコルに対する攻撃をよく検出する．この特徴の差異は製品が開発された時期に何が IDS として期待されていたかに因るものと思われる．

2009 年より IDS/IPS として導入された Forigate シリーズの IDS/IPS と組み合わせ動的ファイアウォールとして利用した場合，学内にて P2P ファイル共有ソフトウェアのトラフィックを遮断するのに非常に有用であった．当初は Foritgate-310B のみで P2P ファイル共有ソフトウェアのトラフィックを遮断していたが，IPS による遮断は完全ではないことが

学外からの指摘で判明した．このため検出した結果より動的ファイアウォールで通信を遮断することとした．学内での P2P ファイル共有ソフトウェアの利用をほぼ完全に遮断することに成功した．この遮断措置は継続して行なっており，遮断開始よりこれまでのところ学外より P2P ファイル共有ソフトウェアの利用を指摘されたことはない．問題としては，Fortigate シリーズでは Share や Perfect Dark のような最近開発された P2P ファイル共有ソフトウェアを検出することができず，従ってこれらの P2P ファイル共有ソフトウェアを自動遮断できないことである．

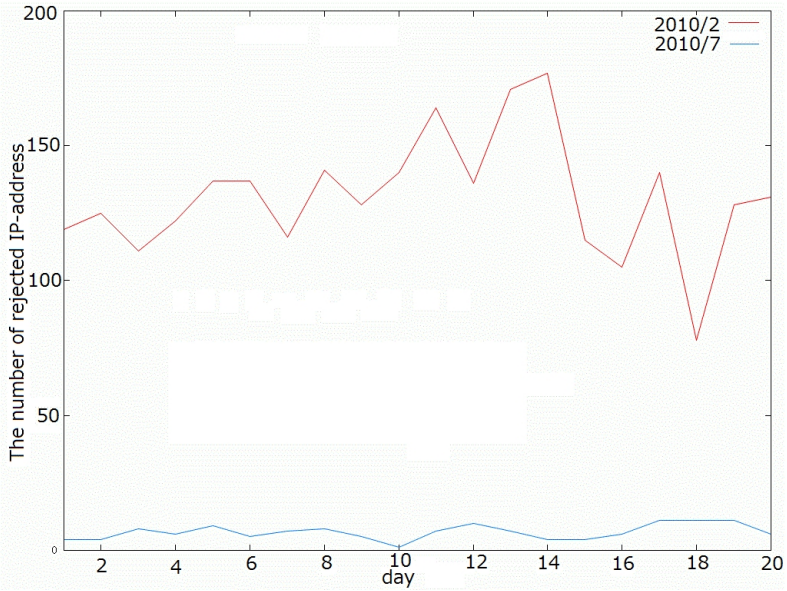


図 4　2010 年 2 月及び 7 月の遮断 IP 件数

```
Failed keyboard-interactive/pam for invalid user david from 219.93.XX.XX port 45870 ssh2
Failed keyboard-interactive/pam for invalid user david from 58.223.XX.XX port 39666 ssh2
Failed keyboard-interactive/pam for invalid user david from 62.128.XX.XX port 39984 ssh2
Failed keyboard-interactive/pam for invalid user david from 218.69.XX.XX port 36673 ssh2
Failed keyboard-interactive/pam for invalid user dan from 211.190.XX.XX port 41883 ssh2
Failed keyboard-interactive/pam for invalid user dan from 221.226.XX.XX port 34978 ssh2
```

図 5　sshd への分散ブルートフォース攻撃の一例

このように動的ファイアウォールの能力は，遮断すべき通信を検出する IDS の能力に完全に依存する．どのような通信を遮断したいかにより，それに適した IDS を選定できるかが鍵となる．また，図 5 に示すようなボットネットを利用したと思われる分散型ブルートフォースアタック等は IDS で検出することも難しく，従って動的ファイアウォールを利用しても防御することは難しいと思われる．これらの攻撃を検出できるようにすることが IDS の今後の課題であろう．

## 5. おわりに

本稿にて，L2/L3 スイッチを用いた動的ファイアウォールの構築と運用を述べた．本稿で用いた H3C S5100-24 は IP ACL の処理をハードウェアで行なうためにワイヤスピードでの処理が行なわれ，理想的なファイアウォールとなっている．また，H3C S5100-24 は基本的に L2 スイッチであるので，IP ACL の末尾に追加される暗黙のルールが全ての通信を許可する，となっている．従って，動的ファイアウォール設定スクリプトによる IP ACL の書き換えが失敗したとしても全ての通信が遮断されてしまう事態にはならないことが期待される．また，スイッチに備わるポートミラー機能を利用して，ミラーポートに IDS ソフトウェアが動作する PC を接続することも考えられる（図 6）．性能は IDS を動作させる PC の性能に依存するが，安価にステレス型 IPS を構成することができる．

現在では，IP ACL を設定可能であることを特長とする L2 スイッチが販売されており，本稿で述べた静的ファイアウォールを構築するのは容易である．また，IDS の出力するログ

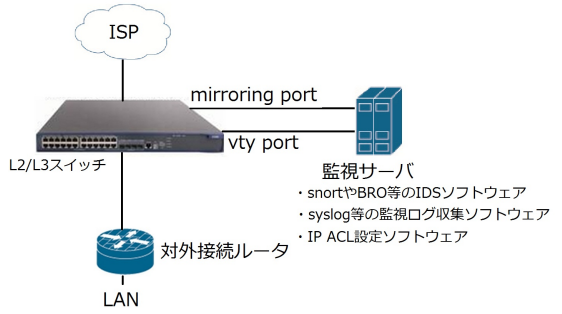


図 6　L2/L3 スイッチを用いた安価な動的ファイアウォールの構成図

Vol.2010-IOT-11 No.9
2010/10/15

を解析して IP ACL を作成し，L2 スイッチに対してその IP ACL を設定するスクリプトを作成し，それらを静的ファイアウォールにすることも容易である．

セキュリティ機器はどちらかといえば高コストな機器である．それらが監視する通信回線の帯域幅は年々増加している．具体的にいえば来年度から開始される SINET4[8] の電通大の接続は 10Gbps になる予定であり，10Gbps に対応可能なセキュリティ機器を用意できるかどうかは未定である．そのような場合に，安価に構成できる本稿のファイアウォールが効果的なのではないかと考えている．

**謝辞** 本研究に関し，電気通信大学 情報基盤センタースタッフの皆様，特に才木良治氏に深謝致します．

## 参 考 文 献

1) Ross Andersion 著 トップスタジオ訳，情報セキュリティ技術大全，p.368，日経 BP 社，2002 年．
2) SQL サーバ及び MSDE を標的とした SQL Slammer ワームに関する情報, Microsoft TechNet, http://technet.microsoft.com/ja-jp/library/dd362406.aspx．
3) 学術情報ネットワーク（SINET3:サイネット・スリー）とは，国立情報学研究所, http://www.sinet.ad.jp/about_sinet3．
4) S5100 シリーズ・スイッチ, H3C, ☒ http://www.h3c.jp/jp/Products___Solutions/Products/Switches/H3C_S5100_Series_Switches/．
5) Jay Rogers, Net::Telnet, http://search.cpan.org/jrogers/Net-Telnet-3.03/lib/Net/Telnet.pm.
6) Share, http://ja.wikipedia.org/wiki/Share_(ソフトウェア).
7) Perfect Dark, http://ja.wikipedia.org/wiki/Perfect_Dark.
8) SINET4 について, 国立情報学研究所, http://www.sinet.ad.jp/sinet4．