

侵入検知システムおよび tcpd のログ解析

長谷川 明生

名古屋大学情報連携基盤センター

概要

名古屋大学の研究教育用ネットワーク(NICE)では、2001年4月より、インターネットとの接続点に侵入検知システム(IDS)を導入して監視を行っている。このIDS以外に、センターのサブネット上で snort による監視や複数のホストでの tcpd を用いての不正アクセスの監視を行っている。インターネットでの脅威の数は、単調増加していると信じられていた。しかしながら、今回の結果は、脅威の数が必ずしも単調増加ではないことを示している。

Analysis of logs of Intrusion Detection systems and tcpd's
Akiumi HASEGAWA
Nagoya University Information Technology Center

Abstract

We have been operating an Intrusion Detection System at the boundary between the Internet and our Campus Network(NICE) since April,2001. Other than this, we are running open source SNORT IDS's on several subnets. The tcpd software has been installed on some servers for monitoring and preventing illegal accesses from the Internet. It is believed that the numbers of threats coming from the Internet are increasing monotonously. However, this result shows some discrepancies from that common belief.

はじめに

名古屋大学キャンパスネットワーク(NICE)では、2001年4月より商用の侵入検知システム(以後IDSと呼ぶ。)による不正アクセスの監視を行っている。当初の100Mbps対応の監視システムは、2001年の秋の補正予算によるNICEネットワークの再構築の際に、SuperSINET接続に対応して負荷分散機構を導入したものに更新された。この部分の構成概念図を図1に示す。

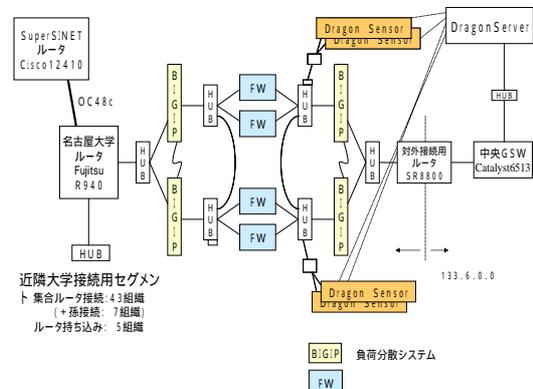


図1. IDSの構成

このIDSの他に、複数のサブネットで、オープンソースのIDSであるSNORT¹によるサブネットの監視、アクセス制限のためのソフトウェアtcpd²を複数のサーバーワークステーションに配置して不正アクセスの監視を行っている。

商用IDSの監視記録、SNORTやtcpdによる2年数ヶ月分の監視記録を、今後のセキュリティ対策の参考とするために解析した。1年程度の期間のログ解析では、ウィルスやワームによる不正トラフィックや、ツールを用いた不正アクセス数は単調増加するようになっていたが、そうでないことが判明した。

IDSおよびtcpdの配置と役割

SuperSINETとNICE間のファイアウォールおよびIDSの構成は図1に示した。Snortおよび各ホストのアクセス制御用に導入したtcpdの配置を図2に示す。近隣大学接続用セグメントには、東海地区の大学接続用のルータ群および名古屋大学と近隣大学のセカンダリネームサーバを設置している。このセグメントを以後、ファイアウォールの外部という理由で外部ネットワークと呼ぶ。サーバセグメントには、本学のネームサーバ、メールゲートウェイやポータルサーバを設置している。センターネットワークには、センターのサービス用スーパーコンピュータやメールサーバの他に、センター内の運用管理のためのホスト等を接続している。これらのサーバやホストの主なものには、アクセス制限や監視のためにtcpdを導入している。このtcpdによる制限を侵害するアクセスが発生した場合には、電子メールで管理者に通知され

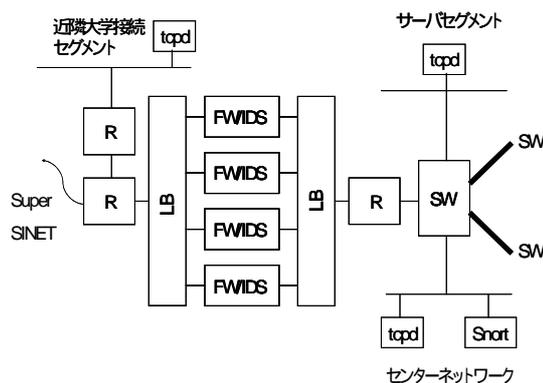


図2 . IDS および tcpd の配置

る。

センターネットワークには、オープンソースの侵入監視用ソフトウェアSnortをインストールしたホストを設置している。Snortのログは、swatchにより監視しており、ホストスキャンの発生は自動的に管理者に電子メールで通知される。

ファイアウォールとともに設置している商用IDSは、各1Gbps対応のインターフェースを持つが、検出性能を高めるために1024番以上のポートは、既知のバックドアやウィルスパターンを除いて無視する仕様となっている。センターネットワーク上のSnortは、インターネット境界上のIDSの補助的役割をはたしている。

IDS等による監視で不正アクセスとみなされたホストは、ファイアウォールのフィルタリストに追加される。NICE内部からのウィルス感染による外部への攻撃等も検出次第フィルタしているが、内部からのものは、問題が解決された時点でフィルタを解除している。ファイアウォールの処理限界は、負荷分散装置の処理性能に依存しており、秒150万セッション程度である。

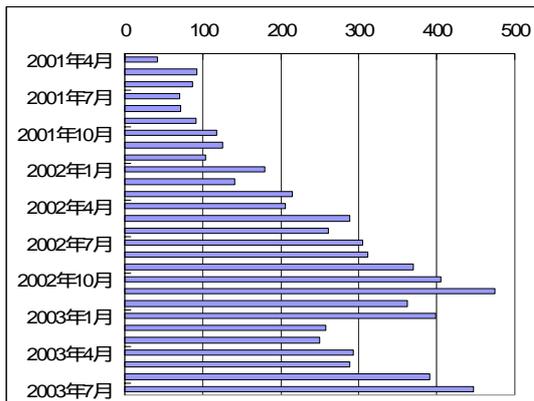


図3. ホストスキャンのインターネット境界での件数

インターネット境界でのIDS ログ

図3に、インターネット境界に置いたIDSでのホストスキャン検出件数の変化を月ごとに集計して示す。集計期間は、2001年4月から2003年7月である。検出件数は、総計6646件、月に最大約500件である。IDSの設置当初から1年程度の間は、ホストスキャン件数は単調増加のようになっていたが、2年を超えたデータをプロットしてみると単純に増加しているとはいえないことがわかる。

ホストスキャンを対象となったポートごとに分析し図4に示す。FTPの制御ポート、HTTPおよびSSHが目立っている。

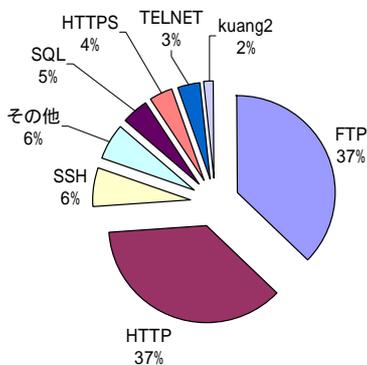


図4. 境界IDSポート別割合

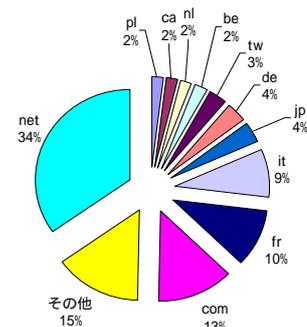


図5. ドメイン別(インターネット境界)

図5に、不正アクセスの発信元をドメイン別に解析して示す。その他は、逆引きできなかったもの、全体の2%に満たないドメインを含んでいる。ドメインnetおよびcom発が多いのは世界の大規模なISPが無国籍ドメインを利用しているからと推定されるが、本学では、frおよびitドメインからのスキャンが目立っている。

インターネットでのSnortのログ

インターネットワークに設置したSnortでPortscanとして検出された数をポート単位の積み上げグラフとして図6に示す。2001年5月から2003年7月

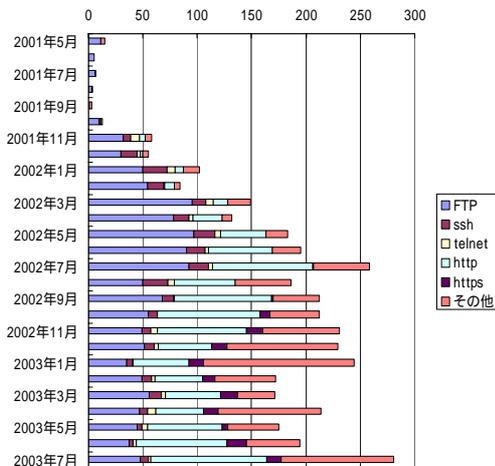


図6. Snortでのホストスキャン検出数の推移

までの総検出数は、3784 件である。月ごとの検出数の推移には、インターネット境界での検出数の推移と類似した傾向が見られる。すなわち、2003 年当初にみられるホストスキャン件数の減少である。

プロトコル別に見れば、FTP、HTTP および HTTPS が多い。2003 年 1 月に「その他」に分類される件数が多いのは、SQL slammer が原因である。SQL のポートは現在ルータでフィルタしているため、1 月以降には IDS では検出対象外となっている。2 月以降に「その他」に分類される件数が増加しているが、ポート別では、17300/tcp および 3389/tcp へのスキャンの増加が目立っている。

図 7 にセンターネットワークで観測されたスキャン発信元のドメイン別割合を示す。図では、全件数の 2% に満たないドメインからのスキャンは、一括して「その他」に分類している。

インターネット境界での解析と比較すると、逆引きできない「不明」分類が多いことが目立つが、ここでも net および com を発信元とするスキャンが多い。それを除けば、やはり it と fr ドメインからのスキャンの多さが目立っている。

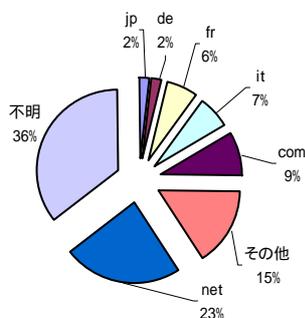


図7 センターネットワークでのドメイン別割合

tcpd ログの解析

これまでに見てきた IDS のログには、IDS がファイアウォールの内側にあるという点で、ログの内容が生の不正アクセスの実態を代表しているかどうかについて検討の余地がある。これは、不正なアクセスやネットワークワームに関連するホストからの影響がファイアウォールで取り除かれているからである。

ファイアウォールの影響の有無を判断する手段の一つとして、複数のホストに導入している TCP ラッパー tcpd の情報が利用できそうである。TCP ラッパーは、サーバネットワーク、センターネットワークおよびファイアウォールの外部にある近隣大学接続用ネットワーク等に設置されたホストの多くに導入されている。サーバネットワークには、大学全体の Web やネームサーバ、不正中継防止や電子メールに添付されたウィルスをチェックするためのゲートウェイが接続されている。これらの tcpd 導入ホストのうち、サーバネットワークと近隣大学接続用ネットワーク上のホストは、ネームサーバである。センターネットワーク上のホストは、筆者が日常的に利用しているワークステーションである。これらのホスト上では ssh も tcpd 組み込みとしてあり、不正アクセスや事故防止のために、ログイン可能な端末を極力限定している。この制限を侵害するアクセスがあった場合には、自動的に、プロトコルと発信元のアドレス情報を持った電子メールが管理者に送付されるようになっている。この警告メールは、TCP ラッパー導入以来のものが保管されており、今回は、その電子メールを解析した。

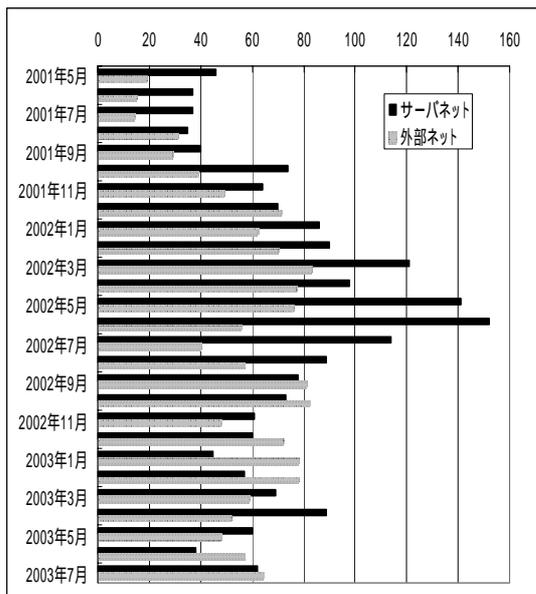


図8. ネットワーク別不正アクセス件数

図8には、煩雑さを避けるために、サーバネットワークと近隣大学接続用ネットワーク（図では、外部ネット）での検出数のみを表示している。なお、サーバネットワーク上のホストでは、観測期間中、特定の1日にsyn-fin アタックが500件を超えた日があったが、そのような異常なアクセスは無視し、前後の日の検出数の平均値を特異日の検出数として採用した。ここには示していないが、センターネットワーク上での検出数変化もほぼ図7と同様の傾向を示している。

絶対的な、不正アクセス件数では、3ネットワーク中、サーバネットワークでの検出数が多い傾向がある。その点を除けば、類似した傾向が見られており、ファイアウォールでのフィルタリングは、異常なアクセスの検出数やその変化の観測には、大きな影響を与えていないと考えてよいようである。

つぎに、ネットワーク別での不正アクセス発信元のドメイン名やIP アドレス

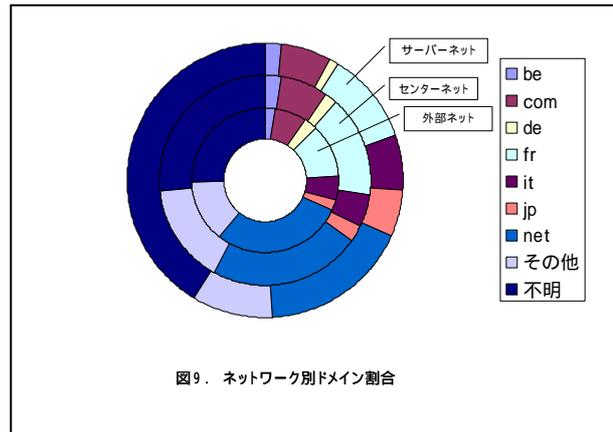


図9. ネットワーク別ドメイン割合

を解析し、トップドメインの割合を調べた。図9は、その解析結果をネットワークごとに、ドーナツグラフ化したものである。

図から、サーバネットワークで、逆引き設定されていないホストからの不正アクセスの割合が高いのが目立っている。サーバネットでのjpドメインからのアクセスは、大半が学内からのtelnetである。このホストは、インターネットに向けては、逆引きネームサーバのプライマリとして機能しているだけでなく、学内向けの正引きのプライマリサーバとして、学内のメール配送のために重要な働きをしている。このため、トラブルが発生すると、学内の管理者がtelnetを実行しがちだからである。この2点を除けば、ファイアウォールの内外には関係がない。ドメイン名的には、ほとんど匿名とみなしてもよいnetドメインおよびcomドメインからのアクセスを除外すれば、不正アクセスの発信元は、特定のトップドメインに集中する。国別トップドメインでいうとfrおよびitである。この結果は、インターネット境界のIDSのログやセンターネット上のSnortのログとも一致した傾向である。

考察

Snort 等の IDS のログの簡単な解析と不正アクセス数日々変化を調べる程度の処理で、不正アクセス件数は単調に増加しているように錯覚していた。たとえば、Snort での検出数の日変化をグラフ化すると図 10 のようになる。

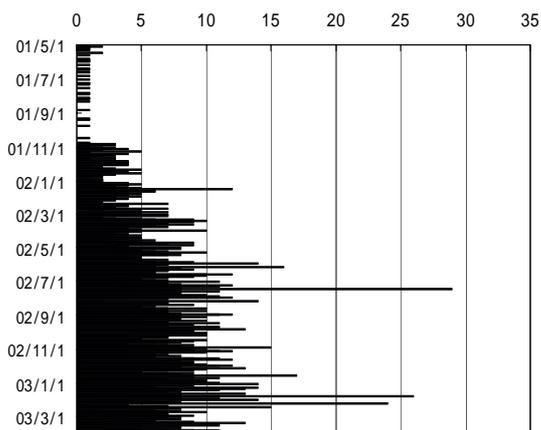


図10. Snort検出数(日計)

図 10 と図 8 を比較すると、月単位の集計を実行することにより、図 8 で示したように変化の傾向が明白に見えてくるようになる。

本論文に示した集計法以外に、時間帯別や曜日別集計も試みたが、土曜や日曜に集中するとか、深夜の時間帯に集中するといった傾向はみられなかった。

図 11 に、インターネット境界での IDS

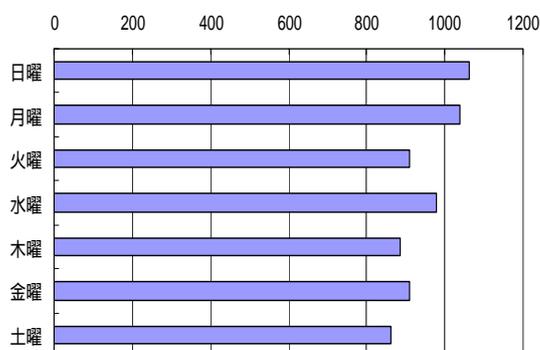


図11. 曜日別ホストスキャン数

でのホストスキャン検出数を曜日ごとに集計して示した。日曜、月曜および水曜に発生件数が多いようにも見えるが、明白な差があるとはいえない。

おわりに

2001年4月1日から2003年7月31日の間のIDSおよびtcpdのログを解析した。その結果、ホストスキャンに代表される不正アクセスの件数が必ずしも単調に増加しているわけではないことを示した。また、不正アクセス発信者のドメイン別割合やプロトコル別の割合も示した。さらに、曜日、時間帯別の解析も試み、曜日別アクセス件数については、予備的な結果を示した。

ドメイン別の割合評価が、名古屋大学に特有のものかどうかといったこと等、不正アクセスの傾向を把握するには、より長期のデータの収集と解析、曜日や時間帯別の詳細な解析が必要とされる。

参考文献

1. Roesch, M. and C. Green: Snort Users Manual, http://www.snort.org/docs/writing_rules/
2. Venema, W.Z.: TCP WRAPPER, network monitoring, access control and booby traps, UNIX Security Symposium III Proceedings (Baltimore), Sept., 1992