社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30 (13)
2005／7／21

インシデント分析のためのホストプロファイリングの検討

大河内 一弥(*)(**) 力武 健次(*) 中尾 康二(*)(***)

(*) 独立行政法人 情報通信研究機構 〒184-8795 東京都小金井市貫井北町 4-2-1
(**) 株式会社 日立製作所 〒215-0013 神奈川県川崎市麻生区王禅寺 1099
(***) KDDI 株式会社 〒102-0072 東京都千代田区飯田橋 3-10-10

E-mail: kazuya@sdl.hitachi.co.jp, rikitake@nict.go.jp, ko-nakao@kddi.com

あらまし 既存の情報に内在する特徴を属性項目として顕在化させようと試みるプロセスをプロファイリングという．本稿では，セキュリティ攻撃のパケットキャプチャログから攻撃元ホストの IP アドレスなどの属性に基づくプロファイリングを行う際，必要な検討項目とシナリオを提案する．またこれに基づいて，DDoS 攻撃のログ分析を行った結果から攻撃に関連するウイルスの知見がどのように得られたかを報告する．

キーワード インシデント，プロファイリング，DDoS，ログ分析

A Study on Host Profiling for Incident Analysis

Kazuya Ohkouchi(*)(**) Kenji Rikitake(*) and Koji Nakao(*)(***)

(*) National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi, Koganei-city, Tokyo 184-8795, Japan
(**) Hitachi, Ltd., 1099 Ouzenji, Asao-ku, Kawasaki-city, Kanagawa, 215-0013, Japan
(***) KDDI Corporation 3-10-10 Iidabashi, Chiyoda-ku, Tokyo, 102-0072, Japan

E-mail: kazuya@sdl.hitachi.co.jp, rikitake@nict.go.jp, ko-nakao@kddi.com

Abstract Profiling is a process to disclose implicit characteristics of a pre-processed data set as the attribute columns. In this paper, we first propose the issues to resolve and applicable scenarios for profiling the implicit characteristics of a security attack based on the packet-capture logs including the IP addresses of the attacking sources. We then show a specific example of a DDoS attack analysis, which discloses implicit characteristics of the involving computer virus by applying the proposed profiling method.

Keywords Incident, Profiling, DDoS, Log Analysis

1. はじめに

ブロードバンドインターネット環境の普及に伴って，情報通信基盤がますます重要な社会インフラとなる一方，ワームやウィルスなどによるネットワークへの被害の拡散はより広範囲，かつ急速なものとなっている．

このため，ネットワークにおけるリスク状況を迅速に把握し，的確な対策に基づくリスク回避やリスクの低減を行う技術の開発が期待されており，国内外において JPCERT/CC[1]，@police[2]，DShield.org[3] などの団体や，Internet Motion Sensor[4] などのシステムにより，ネットワーク上のインシデントの監視が行われるようになってきている．

われわれのグループにおいても，インターネットリスク分析モデルに関する研究を行っており[5]，具体的なシステム化，国内ネットワークプロバイダとの連携などを進めている．

インターネットリスク分析モデルでは種々のオンライン，オフラインデータソースよりデータを収集するが，一般にこれらのデータはデータ量，データ形式の点で，そのまま分析に用いる，あるいはストレージに蓄積するには適していない．このため，収集されたデータは前処理において，データ量の削減，およびデータに内在する特徴の抽出を行うことが必要になる．

インターネットリスク分析モデルでは，上記のデータ量の削減プロセスをダイジェスト処理，特徴抽出のプロセスをプロファイリング処理と呼んでいる．これらは後段に控える種々の分析処理より有用な結果を得るために重要なプロセスである．

本稿では，これらの処理，特にプロファイリングについて，インシデントデータに適用するための検討項目，および具体的な特徴抽出について考察を述べる．また，実際の DDoS

攻撃のログデータにダイジェスト処理，プロファイリングを行った一例を述べ，攻撃に関して得られた知見を報告する．

2. インターネットリスク分析モデルにおけるプロファイリングの位置づけ

インターネットリスク分析モデルの全体図を図 1 に示す．分析モデルでは，分析のプロセスを大きく，1 次分析，2 次分析と，その前処理に分けて考えており，それぞれを以下のように定義している．

1 次分析処理：自動化されており，ほぼリアルタイムで分析結果が出るものを指す．1 次分析の結果はオペレータが確認して，リスク判定や意思決定の支援とする．つまり，1 次分析は全体としては完全自動化された無人の分析ではなく，オペレータのスキルやノウハウも必要になりうる分析のフェイズである．

2 次分析処理：1 次分析処理では発見できないような高精度の分析を実施することで，微細な変化点や特徴点の変化を捉え，インターネットのリスク状況をきめ細かく探求することである．高度な統計分析手法やデータマイニングの手法を用いる想定しており，現在，特徴ルール生成[6]や変化点検出など[7][8]の技術を適用することを検討している．

また、分析の前処理となるプロセスの役割は，

(1) データの軽量化と，1 次分析の前処理を担うダイジェスト化．

(2) 各 2 次分析の前処理．

である．

インターネットリスク分析モデルにおいて，データに前処理の目的は，大きく分けて次の 2 点であると言える．

(1) データ量の削減

(2) データからの特徴抽出

全体図にもある「ダイジェスト処理」の目的は，分析に必要なデータ項目を欠落することなく，不要なデータを削除し，データを軽量化することであり，上記(1)の目的を主とする処理である．一方で本稿で述べる「プロファイリング」は，データに内在する特徴を属性項目化し，明らかにしようとする，(2)の特徴抽出を目的とするプロセスである．

本稿ではプロファイリングを以下のような定義で用いる．

プロファイリング：既存のデータから，そのデータに内在する特徴を，属性項目として顕在化させようと試みるプロセス．

以下の章では，インターネットリスク分析モデルにおけるプロファイリングのプロセスについて検討を行う．

3. ホストプロファイリングの検討

プロファイリングを行うにあたっては，まず基本となる単位レコードの定義を検討する必要がある．

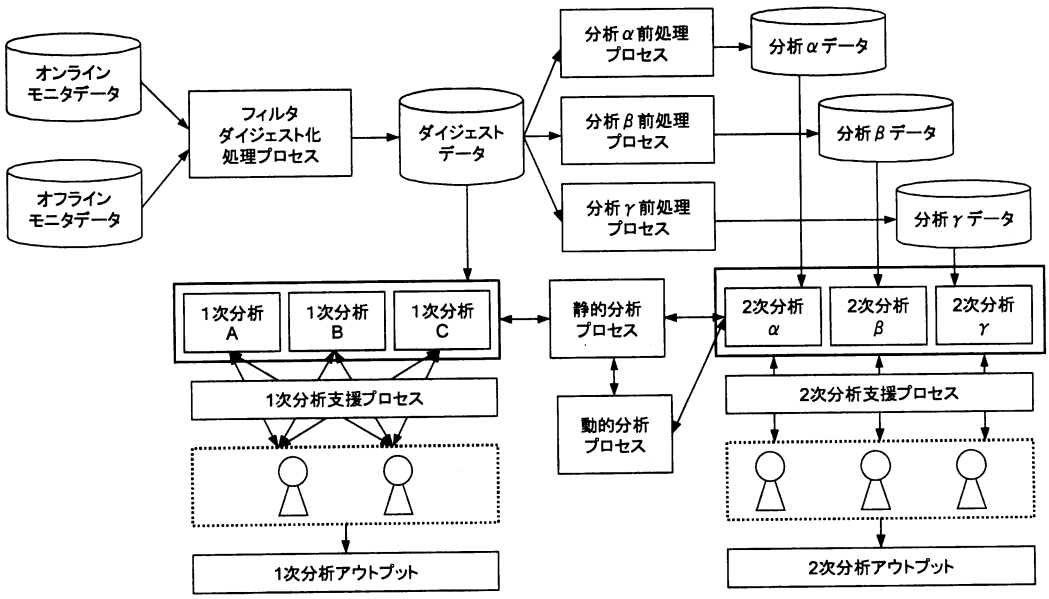

図 1 インターネットリスク分析モデルの全体図

本稿では，ホスト(IP アドレス)を単位レコードと定義してプロファイリングを行うことにした．これは，(a)インターネットリスク分析モデルにおいては，インシデントはホスト単位で検知される事，(b)分析後のアクションはホスト単位で取ることが可能であること，などの理由による．

次に，プロファイリングによって作成される属性項目であるが，属性項目の検討には以下のような点に留意する必要がある．

(1) 基礎統計量の作成と検討

プロファイリングを行う前には，データの基礎統計量を調査するなど，事前にデータの傾向を把握することが重要である．

(2) 集約する粒度の検討

1 レコードに集約するデータの粒度，時間の粒度を検討する必要がある．集約するデータの範囲が不適切である場合，ある粒度では抽出できる分析に有用なデータの特徴が抽出できなくなる場合もある．データの特徴を最もよく表す粒度を適切に選択することが重要である．

また集約する時間の粒度は後段のアクションのタイミングと密接に関係する．日ごとのアドバイザリを作成する際には，一日のデータを集約したプロファイルを使用することも可能だが，リアルタイムに近いアクションを求められる場合は，秒単位など，短い時間単位でも意味のある項目値の出る粒度にする必要があるだろう．

(3) 後段の分析，アクションへのシナリオの検討

それぞれの属性項目は，後段の分析や，分析の結果取りうるアクションへのシナリオも想定した上で検討することが望ましい．

上記に留意して考案したプロファイリングの属性項目の一例を表 1 に示す．

表 1 ではデータの粒度の観点から，ホストをキーにしてデータを集約するプロファイリングのほかに，送信元ポート，およびセッションをキーとするプロファイリングを考案した．

特に本稿では，送信元ポートに着目した属性項目を提

表 1　プロファイリングによる属性項目の例

a ホストプロファイリング

#	属性項目	説明
a-1	送信先ポート番号関連	送信元ポートプロファイリングより集約．
a-2	送信元ポート番号関連	ユニーク送信元ポート番号数など．
a-3	パケット種別別パケット数	送信元ポートプロファイリングより集約．
a-4	プロトコル別パケット数	↑
a-5	ペイロード長関連	↑
a-6	セッション関連	セッション数，継続時間，同時最多セッション数など．
a-7	HTTP メソッド関連	送信元ポートプロファイリングより集約．
a-8	アクセス間隔関連	↑

b 送信元ポートプロファイリング

#	属性項目	説明
b-1	送信先ポート番号関連	ユニークポート番号数，アクセス数(合計値・単位時間当たり)など．
b-2	パケット種別別パケット数	セッション別プロファイリングより集約．
b-3	プロトコル別パケット数	↑
b-4	ペイロード長関連	↑
b-5	セッション関連	セッション数，継続時間(平均値，最大値)など．
b-6	HTTP メソッド関連	セッション別プロファイリングより集約．
b-7	アクセス間隔関連	↑

c セッションプロファイリング

#	属性項目	説明
c-1	送信先ポート番号関連	ユニークポート番号数，アクセス数(合計値・単位時間当たり)など．
c-2	パケット種別別パケット数	SYN, ACK, FIN それぞれのパケット数(合計値・単位時間あたり)．
c-3	プロトコル別パケット数	TCP, UDP, ICMP それぞれのパケット数(合計値・単位時間あたり)．
c-4	ペイロード長関連	平均ペイロード長，最大値，分散，標準偏差など．
c-5	セッション関連	セッション開始時間，終了時間など．
c-6	HTTP メソッド関連	HTTP メソッド別アクセス数など．
c-7	アクセス間隔関連	平均アクセス間隔，分散，分布など．
c-8	アクセスのシークエンス関連	ポートのシークエンス，HTTP メソッドのシークエンスなど．

案している．これは，ウィルスによってはターゲットのマシンに複数のセッションを張って攻撃してくるものがあり，送信元ポートで集約した特徴量にウィルスの特徴がよく現れる可能性がある，という仮説に基づくものである．

以下に，それぞれの特徴量の狙いをまとめる．送信先ポートなど，従来頻繁に参照されてきた特徴量も多いが，これらについても，データの集約の粒度，時間の粒度を変更することにより，興味深い知見を得られる可能性がある．

(1) 送信先ポート関連特徴量

特定のポートを狙うウィルスや，ポートスキャンなどを検出する．ホストで集約するより，送信元ポート，あるいはセッションで特徴量を算出した方が，攻撃の特徴を鮮明に捕らえられると考えられる．

(2) 送信元ポート関連特徴量

ユニークな送信元ポート番号の数は，ウィルスが張ってくるセッション数と強い関連があることが推測される．一度に張ってくるセッション数などの情報から，攻撃の特徴を検出することを想定している．

(3) パケット種別別，プロトコル別特徴量

SYN Flood, Connection Flood などの検出を目的とする．また，不正なシークエンスのアクセスに攻撃の予兆を捉えることができる可能性がある．

(4) ペイロード長関連特徴量

バッファオーバーフローを狙う攻撃などを検出する．また上りと下りのトラフィックを監視することで，攻撃の予兆，特徴を捉えることができる可能性がある．

(5) セッション関連特徴量

送信元ポートと同様，同時に張ってくるセッション数などに攻撃の特徴が出る可能性がある．セッションに関しては，集約する時間を細かく設定してプロファイリングを行うことは無意味であろう．

(6) HTTP メソッド関連特徴量

HTTP メソッドを見ることで検出できるウィルスは過去にも CodeRed などいくつか存在している．

後述する DDoS の分析においても，HTTP メソッドに着目して算出した特徴量より，攻撃に関する新たな知見を得ることができた．

(7) アクセス間隔関連特徴量

アクセス間隔に関するプロファイル項目では，ツールによる DoS と手動の DoS を切り分けることなどが可能になると期待される．

また，ウィルスによっては，亜種によって異なるアクセス間隔でパケットを送ってくるものも知られている．

(8) アクセスシークエンス関連特徴量

アクセスするポートの組み合わせ，あるいはシークエンスより，攻撃の特徴を把握する．これも，データの粒度を変えることにより攻撃の特徴をよりはっきりと捕らえられる可能性がある．

4. DDoS 攻撃データへの適用例

以上で検討したプロファイリングの一部を，実際の DDoS 攻撃のログに対して適用し，分析を行った．分析の対象はあるワームによる攻撃のデータで，このワームは毎月 1 日より一定期間，あるサイトに DDoS 攻撃をしかけるものである．また，攻撃は毎月第一月曜日と，5 月 5 日など月数と日数が同じになる，いわゆるゾロ目の日に激しくなることが知られている．

4.1. モニタデータ

今回分析の対象とするのは時期を変えてモニタした 2 つのデータである．

データセット A は被攻撃サーバへのパケットを PCAP 形式でキャプチャしたものであり，ペイロードもすべて取得されている．データ取得月の，攻撃が始まる 1 日前(前の月の最終日)から攻撃が終了するまで，2 週間程度のデータが含まれている．

データセット B は，データセット A とは別の期間のデータである．データセット A と同様 PCAP 形式でキャプチャを行っているが，取得時の都合によりペイロードは 96 バイトで切り捨てられている．また，非常に広い帯域を用意してキャプチャを行ったため，攻撃パケットの大部分を記録していると期待される．モニタ期間は，データセット A と同様，データを取得する対象月の前月の最終日より 2 週間程度のデータが含まれている．

4.2. ダイジェストデータへの変換

モニタデータを扱いやすい形式にするため，われわれがダイジェストデータと読んでいるフォーマットに変換した．このフォーマットを表 2 に示す．

TCP, UDP, ICMP について，それぞれ後段のプロファイリング，あるいは分析の際に必要になると想定される項目を含んだ形式になっている．この形式では，それぞれのプロトコルについて，UNIXTIME，アクセス元，アクセス先の IP，IP ヘッダフラグを記録し，この以降の項目は，"T" "U" "I" の識別用の固定アルファベットを挟んで，それぞれのプロトコルで必要と思われる項目を含めた．ここで UNIXTIME とは，UNIX において用いられる 1970 年 1 月 1 日 00:00 UTC を起点としてこの時点から経過した秒数のことである．また TCP パケットの SEQ NUM, ACK NUM は，TCP ヘッダに含まれるそれぞれのシーケンス番号を記録している．また，TCP パケットにおいては，ペイロード長の後，HTTP メソッドが存在すれば記録している．

4.3. プロファイリング

まず，ダイジェストデータより，ホストごとの被攻撃サーバへ

表 2 ダイジェスト版データフォーマット

+ TCP	+ UDP	+ ICMP
- UNIXTIME	- UNIXTIME	- UNIXTIME
- アクセス元IP	- アクセス元IP	- アクセス元IP
- アクセス先IP	- アクセス先IP	- アクセス先IP
- IPヘッダフラグ	- IPヘッダフラグ	- IPヘッダフラグ
- "T"	- "U"	- "I"
- アクセス元ポート番号	- アクセス元ポート番号	- TYPE
- アクセス先ポート番号	- アクセス先ポート番号	- CODE
- SEC NUM	- ペイロード長	- ペイロード長
- ACK NUM		
- TCPフラグ		
- ペイロード長		
- HTTPメソッド (存在する場合)		

のデータの送信バイト数など，基礎的な統計資料を作成し，検討を行った．

(1) 基礎統計量の検討

基礎統計量として検討した項目の中から，ここでは，データセットAにおいて，データの中から感染マシンが攻撃を仕掛ける際の HTTP メソッドに着目し，メソッド別のパケット数の推移を記録したグラフを示す．それぞれのグラフは X 軸を時間(1 時間単位)，Y 軸を特定の HTTP メソッドを含むパケット数として描画したものである．Y 軸は対数になっている．

われわれが注目したのは以下の 5 つの HTTP メソッドである．なお，(2) (4) の CGI のページ名は伏字としている．

(1) "GET / HTTP/1.1"

(2) "POST /.../xxx.cgi HTTP/1.1"

(3) "POST / HTTP/1.1"

(4) "POST /.../xxx.cgi HTTP/1.0"

(5) "POST / HTTP/1.0"

図 2 は観測日 A1 の前日夜 22 時以降をプロットしたものである．観測日 A1 は観測を行った月の 1 日であり，日付が変わった際に，トップページへの GET が一桁増加し，DoS 攻撃が始まっている様子が確認できる．

またこのグラフでは，1000 パケット以下の規模ではあるが，アクセス数推移の概形が類似する 2 つのページへの POST のアクセスが続いていることがわかる．

図 3 は観測日 A2 のものである．日

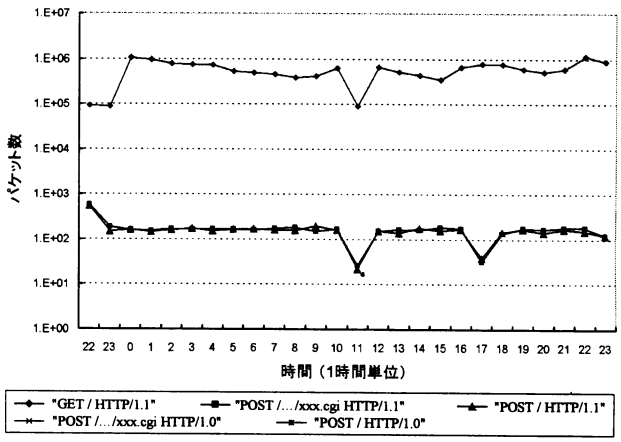

図 2 観測日 A1(観測月 1 日)の HTTP メソッド別パケット数推移

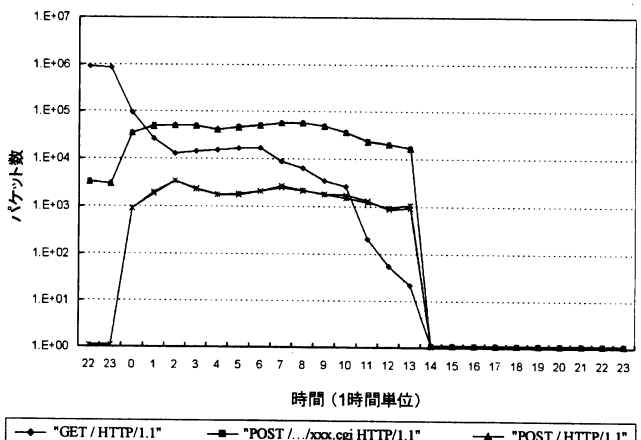

図 3 観測日 A2(ゾロ目の日)の HTTP メソッド別パケット数推移

付が変わった際にトップページと，xxx.cgi への POST による攻撃が始まっている．

前のグラフと同様，そのアクセス数の推移の概形は，ここでも類似して推移している．その際，トップページへの GET が減少しているが，これは帯域の関係などで，見かけとして攻撃パケット数が減少しているだけであろう．

グラフでは，14 時以降のデータが取得されていないのは，キャプチャサーバがダウンしたためである．

(2) ホストプロファイリング

前項における基礎統計量の検討より，HTTP メソッドに着目して検討を進める方針を決定し，各ホストを集約の単位としたプロファイリングを行ってログデータに関する考察を進めた．

ここでは，それぞれのホストについて，一日ごとに HTTP メソッド別の送信パケット数を集計したデータを検討した結果について述べる．

データセット B に関する検討結果のグラフの一部を図 4 以降に示す．

グラフは，X 軸に，被攻撃ホストでログに記録された特定の HTTP メソッドのパケット数が多いホストを降順にソートして並べ，Y 軸にはそのホストのパケット数を累積した値をプロットしたものである．なお，X 軸の最大値は各グラフで集計の対象となっているパケットを被攻撃サーバに送ってきたホストの数である．

図 4〜図 7 はそれぞれ，以下のパケットについてプロットしたものである．

- 図 4 観測日 B1 (観測月の 1 日)の“GET / HTTP/1.1”
- 図 5 観測日 B2 (観測月の第一月曜日)の“GET / HTTP/1.1”
- 図 6 観測日 B3 (観測月のゾロ目の日)の“GET / HTTP/1.1”
- 図 7 観測日 B3 (観測月のゾロ目の日)の“POST / HTTP/1.1”

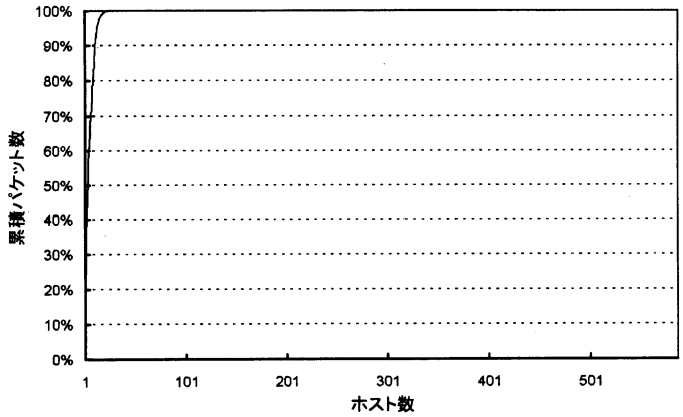

図 4　観測日 B1 (観測月の 1 日)の“GET / HTTP/1.1”

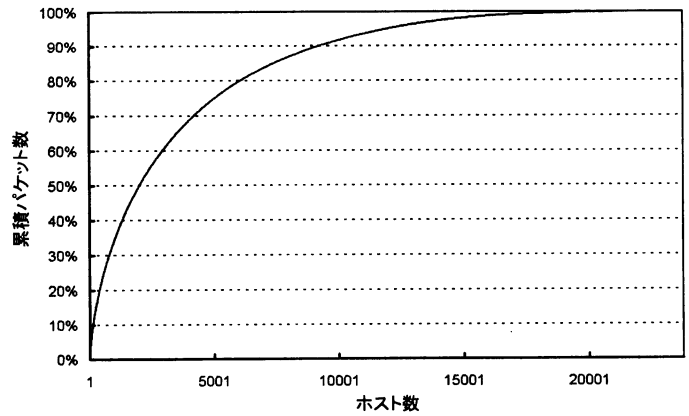

図 5　観測日 B2 (観測月の第一月曜日)の“GET / HTTP/1.1”

表 3 図 5 における累積パケット数とホスト数の関係

パケット数	ホスト数
50%のパケット	上位 2,001 ホスト
60%のパケット	上位 2,928 ホスト
70%のパケット	上位 4,184 ホスト
80%のパケット	上位 6,031 ホスト
90%のパケット	上位 9,183 ホスト
95%のパケット	上位 11,926 ホスト

表 4 図 7 における累積パケット数とホスト数の関係

パケット数	ホスト数
50%のパケット	上位 1,049 ホスト
60%のパケット	上位 1,602 ホスト
70%のパケット	上位 2,395 ホスト
80%のパケット	上位 3,588 ホスト
90%のパケット	上位 5,601 ホスト
95%のパケット	上位 7,451 ホスト

HTTP/1.1"

これを見ると，図 4，および図 6 と，図 5，図 7 では，グラフの形状が大きく異なることが確認できる．

図 4 では観測日において，被攻撃サーバは 586 のホストから GET / HTTP/1.1 のパケットと受け取っているが，その 99%以上は 20 程度のホストからのパケットであることがわかる．同様に図 6 では GET / HTTP/1.1 パケットの 99%以上を，100 程度のホストから受け取っていることがわかる．

その一方，図 5 では，95%のパケットに対応するホスト数は約 12,000，図 7 では約 7,000 程度となっており，図 4，図 6 のグラフが急激に立ち上がっているのとは対照的な形状を示している．

図 5 と図 7 におけるパケット数(%)とホスト数(上位 N ホスト)の関係を表 3 と表 4 にまとめた．

さて，以上の検討より，異なる HTTP メソッドによる攻撃の存在が明らかになったが，次に，これらの攻撃が同一のホストによってなされているのか否かを調査するため，観測日 B2 において，"GET / HTTP/1.1"，"POST / HTTP/1.1"，"POST / HTTP/1.0"を行っているホストについて，それらホストの重複を調べた．この結果を図 8 に示す．

この図より，GET を行うホストと，POST を行うホストは，一部重複して

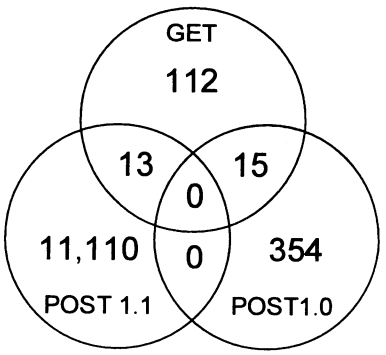

図 8 攻撃手法の重複

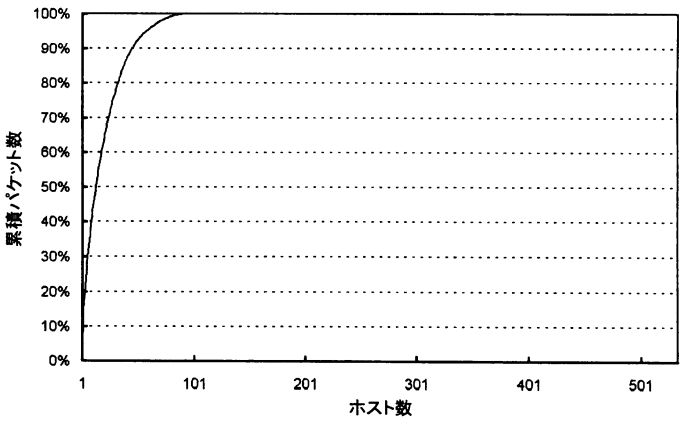

図 6 観測日 B3 (観測月のゾロ目の日)の"GET / HTTP/1.1"

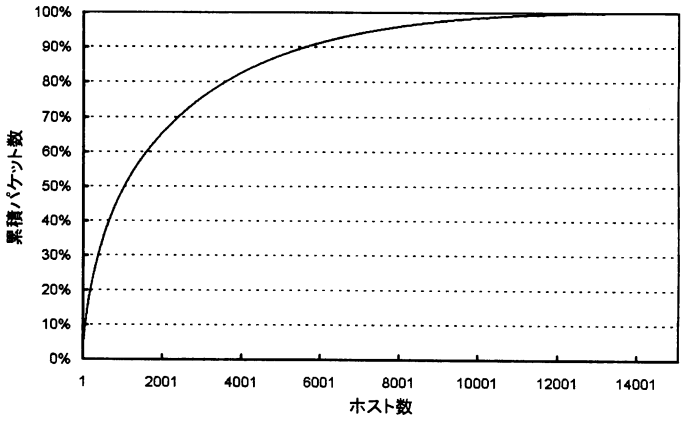

図 7 観測日 B3 (観測月のゾロ目の日)の"POST / HTTP/1.1"

いるものもあるが，基本的に別のホストが行っていることが推測される．

5. 考察

第 4 章の結果について，いくつかの観点から考察を加える．

(1) 第 4.1 節で述べた通り，データセット B が，攻撃パケットをすべて記録したと仮定すると，それぞれの攻撃を行うホスト数は，ウィルスの感染ホスト数と同等の規模になると推測される．しかし実際は，ネットワーク上にボトルネックが存在し，例えば図の上位ホストからのアクセスを遮断したとしても，別のホストからの DoS 攻撃があるものと思われる．

(2) 図 4～図 7 を見ると，第一月曜日の GET 攻撃と，

ゾロ目の日の POST 攻撃は同一のホストによってなされるのか否か，という疑問が浮かぶ．この問題は，両日が異なる日であるため，DHCP サーバによって IP アドレスが変更されている可能性があり，単純なアドレスの突き合わせはできないが，興味深い点である．

最後に，DDoS について考察を加える．

第 4.3 節の図より，このサイトへの DDoS 攻撃は，大きく 2 つの種類の攻撃によるものであることがわかる．すなわち，トップページへの GET による DoS 攻撃と，POST による 2 つのページへの DoS 攻撃である．

さらに第 4.3 節のホストプロファイリングの結果を見ると，「攻撃が激しくなる」とされている第一月曜日とゾロ目の日の攻撃ホスト数が数千～一万に上るのに対し，それ以外の日は高々100 程度のホストから，トップページに GET が来ているのに過ぎず，ホスト数に大きな違いがあることがわかる．第一月曜日の GET と，それ以外の日の GET は，まったく異なる性質のものと考えるのが自然である．

従って，われわれが，一つの DDoS 攻撃の影響であると考えている現象は，実は 3 つの種類の DDoS 攻撃，すなわち，

(1) 毎月 1 日より継続的に行われる，トップページへの GET による DoS 攻撃

(2) 毎月第一月曜日に行われる，トップページへの GET による DoS 攻撃

(3) 毎月ゾロ目の日に行われる，トップページへの POST による DoS 攻撃

が複合しているものである，と結論することができる．

また，この結果を実運用に適用することを検討すると，(1) の攻撃は(2)(3)の攻撃に比べ少数のホストについて対策することで大半のパケットを防ぐことができると考えられる．図 4，図 6 の結果を用いるならば，第一月曜日およびゾロ目の日以外の攻撃に関しては，数百程度の IP アドレスからのアクセスを拒否することで，99%以上の DoS 攻撃のパケットを防ぐことができると予想される．

6. まとめ

本稿では，インターネットリスク分析モデルの中で，分析にいたる前処理に焦点を当て，ホストプロファイリングについての考察，および具体的な特徴量の考案を行った．また，DDoS データにダイジェスト処理，プロファイリングを行った一例を述べ，ある DDoS 攻撃が，実際は 3 種類の攻撃の複合であることを明らかにした．

本稿では本質的に主張するのは，プロファイリングによって特徴抽出を行うことにより，今までに見えていなかったインシデントの特徴を捉えることができる，という点である．これに関して本稿では，第 3 章，第 4 章にて，基礎統計量の調査によるデータの傾向の調査→プロファイリングによる分析→インシデントに関する知見の発見，というインシデント分析の流れのひとつを提示した．

しかしながら，今回行ったのはプロファイリング項目をグラフとして図示し，それに考察を加える，という分析としては比較的単純なものであった．今後は複数のプロファイル項目間の関係などにも着目し，またプロファイルデータに統計分析やデータマイニングの技法を適用することにより，より深い分析を行ってゆく予定である．

謝　辞

本稿で述べた実験を担当してくださった横河電機の鈴木和也氏，馬場俊輔氏にここでお礼を申し上げます．また，実験データの取得，提供にご協力頂いた関係各社の方々についても，ここで厚くお礼を申し上げます．ありがとうございました．

文　献

[1] JPCERT/CC Internet Scan Data Acquisition System (ISDAS)
URL: http://www.jpcert.or.jp/isdas/

[2] 警察庁セキュリティポータルサイト@police
URL: http://www.cyberpolice.go.jp/

[3] DShield.org—Distributed Intrusion Detection System
URL: http://www.dshield.org/

[4] Evan Cooke, Michael Bailey, David Watson, Farnam Jahanian, and Jose Nazario "The Internet motion sensor: A distributed global scoped Internet threat monitoring system." Technical Report CSE-TR-491-04, University of Michigan, Electrical Engineering and Computer Science, July 2004.

[5] 中尾，丸山，大河内，松本，守山，武智，"インターネットリスク分析モデルに関する考察"，暗号と情報セキュリティシンポジウム SCIS 2005, pp.1531-1536, Jan. 2005.

[6] 芦田,前田,高橋，"データマイニングにおける特徴的ルール生成方式"，情報処理学会第 50 回全国大会，1995.

[7] K.Yamanishi, J.Takeuchi, "A Unifying Approach to Detecting Outliers and Change-Points from Non stationary Data" The Eighth ACM SIGKDD International Conference on Data Mining and Knowledge Discovery, ACM Press, pp.676-68, 2002.

[8] Y.Maruyama, K..Yamanishi, "Dynamic Model Selection and Its Applications to Computer Security", The IEEE Information Theory Workshop 2004.
URL: http://ee-wcl.tamu.edu/itw2004/