使い捨てIPによる新型ブルートフォース攻撃の検出

本多　聡美†　　海野　由紀†　　丸橋 弘治†　　武仲 正彦†　　鳥居 悟†

†株式会社富士通研究所
211-8588　神奈川県川崎市中原区上小田中 4-1-1
{honda.satomi,yuki_m,maruhashi.koji,ma,torii.satoru}@jp.fujitsu.com

あらまし 近年のブルートフォース攻撃は侵入検知システム（IDS/IPS）からの検知を回避するため，その手段はますます巧妙となってきている．我々は，複数拠点のネットワーク監視ログについて，攻撃元・攻撃検知時刻に着目した可視化を行い，組織的または規則的な特徴を有するブルートフォース攻撃事例を3種類発見した．特に，毎回異なるIPアドレスから特定のIPアドレス群へ向けた組織的なブルートフォース攻撃が長期間継続して行われていた攻撃事例は報告がされていなかった新しい事例である．さらに，この攻撃事例についてその攻撃の特徴を利用することで，この攻撃を受け続ける可能性の高いIPアドレスをIDSログから早期に発見する手法を提案する．

Detection of Novel-type Brute Force Attacks used Expendable Springboard IPs as Camouflage

Satomi Honda†　　Yuki Unno†　　Koji Maruhashi†　　Masahiko Takenaka†
Satoru Torii†

†FUJITSU LABORATORIES LTD.
4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki, Kanagawa 211-8588, JAPAN
{honda.satomi,yuki_m,maruhashi.koji,ma,torii.satoru}@jp.fujitsu.com

Abstract Recently, the way of brute force attacks has become more tactical and tricky to avoid being detected by intrusion detection or prevention systems(IDS/IPS). In this paper, we show that we have detected three organized or systematic brute force attack instances from actual network monitoring logs by visualization focused on hackers and detection time. One of the instances shows that specific victims have been attacked by expendable IPs for a long time. These IPs were innumerable and appeared almost only one time. We also propose a method for detecting such victims in the earlier phase using characteristics the instance has among hackers, detection time and the number of times hackers tried to login.

1　はじめに

近年サイバー攻撃が活発化し，その被害もより深刻なものとなってきている．2013年4月には，オープンソースのブログツールであるWordPress[1]を狙った大規模攻撃が発生した[1]．この攻撃では，攻撃者は管理者ユーザ名「admin」に対し，ブルートフォース攻撃を実施しパスワードを搾取したと言われている．攻撃は，9万以上のIPアドレスから1時間当たり6000万回以上行われたと言われており，攻撃対象はWordPressを提供している全てのホスティングプロバイダであったため大きな被害となった．

[1]WordPressはWordPress Foundationの商標です．

攻撃を受けたプロバイダでは，攻撃元 IP アドレスを抽出し，そのアドレスからの通信を遮断することで防御を行ったと伝えられている．

ブルートフォース攻撃とは，考えられる全ての鍵をリストアップすることで暗号文の復号を試みる攻撃である．攻撃を効率的に実施するために，辞書に収録されている単語を候補として探す辞書攻撃や，システムに初期設定される値を使うといった手段も存在しうる [2]．さらに，他サービスから漏えいしたと考えられる大量の ID/パスワードを別のサービスへのログインに使用する攻撃 [6][7][8] も，広義のブルートフォース攻撃といえる．

近年，このブルートフォース攻撃は侵入検知システム（IDS/IPS）からの検知を回避するため，その手段はますます巧妙となってきている．IBM SOC によるレポート [3] では，SSH や FTP サービスへのブルートフォース攻撃について，複数の IP アドレスに対して 1 日に複数の異なる IP アドレスからの攻撃があったこと，単一の攻撃元 IP アドレスから行われたログイン試行が 10 回〜30 回程度であったことなどが報告されている．また SANS Internet Storm Center や Dragon Research Group による報告 [4][5] でも，多数の攻撃元 IP アドレスからの SSH を狙ったブルートフォース攻撃が発生していたことが確認され，ボットネットから分散して攻撃が仕掛けられている可能性があると述べている．

これまでのブルートフォース攻撃に関する研究では，単一拠点（サーバ）に対する攻撃を分析するものがほとんどであった．しかし，上述の WordPress への攻撃等を考慮すれば，複数拠点に対するブルートフォース攻撃についての分析も必要であると考えられる．

現在我々は，複数拠点のネットワーク監視ログを対象としてセキュリティ上の新たな脅威や新しい攻撃手口の分析・抽出を行っている．この監視・分析の中でネットワークに設置した IDS から取得したログ（IDS ログ）について分析し，攻撃元・攻撃検知時刻に着目した可視化を行った．その結果，富士通が管理しているネットワークにおいて 2011〜2012 年の間に取得された 8ヶ月間の IDS ログより，SSH（22 番ポート）に対する組織的または規則的な特徴を有するブルートフォース攻撃事例を 3 種類発見した：

I) ある攻撃元 IP アドレスから複数の被攻撃先 IP アドレスに攻撃が継続して行われていた事例，II) ある攻撃元 IP アドレスから複数の被攻撃先 IP アドレスに，毎日特定の時間帯にのみ攻撃が行われていた事例，III) 毎回異なる攻撃元 IP アドレスから複数の被攻撃先 IP アドレス群へ向けた攻撃で，いずれも 1 回あたりのログイン試行回数が〜数十回程度であった事例，の 3 つである．特に，毎回異なる IP アドレスから特定の複数 IP アドレスへ向けたブルートフォース攻撃が長期間継続して行われていた事例は，我々の調査した限り報告がされていなかった新しいタイプの攻撃事例である．

タイプ III の攻撃事例で見られた攻撃（タイプ III 攻撃）は，ログイン試行回数も小さく，毎回攻撃元 IP アドレスが変化する．そのため，単一拠点での観測では攻撃か IDS の誤検知かの判断が困難である．また，従来のような攻撃元 IP アドレスを遮断するような対策は効果がないことは明らかである．そこで，ある IDS アラートがタイプ III 攻撃の一部かどうかを早期に判断し，攻撃を受けている被攻撃先 IP アドレス群を効率的に抽出する手法を提案する．被攻撃先 IP アドレス群が事前に判明し，それらに対する攻撃が開始されたことを早期に発見できれば，タイプ III 攻撃に対する効率的な対処が可能になると考える．

論文の構成は次の通りである．第 2 章でこれまでのブルートフォース攻撃事例等の報告や複数拠点のネットワーク監視・分析技術を紹介する．第 3 章で我々の行っているログ分析について説明したのち，分析したログから発見された攻撃事例とその特徴を報告する．第 4 章で，被攻撃先を早期に発見することによりタイプ III 攻撃を対策する手法を提案する．第 5 章でまとめと今後の課題とする．

なお，以下では攻撃元 IP アドレスを攻撃元，被攻撃先 IP アドレスを被攻撃先とする．

2 従来研究

2.1 ブルートフォース攻撃事例に関する報告

ブルートフォース攻撃に関する従来の報告を示す．Sperotto らは著者の所属する大学のネットワークから，scanning, brute-force, die-off の 3 種類のフェーズから構成される SSH へのブルートフォース攻撃が発生していたことを報告している [9]．Vykopal は，攻撃元数:被攻撃先数が 1:1, 1:N, N:1 の 3 種類にブルートフォース攻撃を分類し，大学のネットワーク内でそれぞれの攻撃がどの程度発生していたかを調査している [10]．IBM SOC，SANS，Dragon Research Group による報告 [3][4][5] でも，複数の被攻撃先に対して 1 日に複数の異なる攻撃元からの攻撃があったことが報告されている．

しかし，いずれの研究も単一の攻撃対象もしくは同一拠点内の複数の攻撃対象へのブルートフォース攻撃に関する研究であり，複数拠点のネットワーク監視ログからブルートフォース攻撃を分析したものではない．さらに複数の被攻撃先へ，攻撃元が連携してブルートフォース攻撃を行っていたという報告はなされていない．

2.2 複数拠点のネットワーク監視・分析に関する技術

次に，複数拠点のネットワーク監視・分析に関する従来研究を示す．武仲らは，実際のネットワーク上で，ランダムで低速なポートスキャンが発生していたことを報告している [11][12]．特に [12] では，複数の攻撃元から複数の被攻撃先に向けたランダムで低速なポートスキャンが発生していたことが報告されている．複数拠点観測に関しては，NICT の nicter[13] によるダークネットトラフィックの観測や，JPCERT/CC の TSUBAME[14] によるインターネット上のトラフィック観測がなされている．他にも，実際のネットワークトラフィック監視に関する研究（[15][16][17] など）が多数発表されている．また牧田らは，複数拠点に DNS サーバをハニーポットとして設置することで DNS サーバを悪用する不正活動の観測・分析を行っている [18]．

しかし，これらの文献で提案されている技術ではブルートフォース攻撃を検知することは検討されておらず，さらにタイプ III の攻撃のような挙動を発見することは困難である．

3 複数拠点のネットワーク監視ログの分析

現在我々は，複数拠点のネットワーク監視ログを対象としてこれまで見逃されていたセキュリティ上の新たな脅威や新しい攻撃手口の分析・抽出を行っている．分析によって得られた知見を基に，新たな攻撃手口に対する検知手法を確立することが目的である．

従来行われていた分析は，ある 1 つの拠点が受けた攻撃について，その攻撃検知件数やユニークな攻撃元数の変化を発見する，といった単一拠点に着目した分析が主流であった．そのため，複数の拠点がそれぞれ攻撃を受けたタイミングやその攻撃元の特徴などは従来の分析手法では発見することが難しかった．

3.1 攻撃元と検知時刻に着目した可視化

そこで我々は，攻撃元と攻撃検知時刻に着目したネットワーク監視ログの可視化を行った．その結果，組織的または規則的な特徴を有するブルートフォース攻撃事例を 3 種類発見できた．

具体的には，被攻撃先を縦軸，攻撃検知時刻を横軸として，攻撃元ごとにどの被攻撃先に対して，いつ攻撃が検知されたかのかを散布図として表現する．この散布図の特徴は，攻撃検知件数に着目した一般的な散布図とは異なり，攻撃元に着目している点にある．縦軸を被攻撃先として，攻撃元ごとにプロット印を変化させることで，同一あるいは異なる攻撃元からの攻撃であったのかを区別することができる．

この表現を，2011〜2012 年の間に取得された 8ヶ月間の 22 番ポートへのブルートフォース攻撃を検知した IDS ログに適用した．結果を図 1 に示す．次節にて，攻撃事例の詳細を述べる．

3.2 発見した攻撃事例

本章では，IDS ログから発見された 3 種類の攻撃事例（タイプ I〜III）を示す．なお，ログ

イン試行回数は，今回使用した IDS ログの生成元 IDS 製品の判断に基づくものである．

- タイプ I 攻撃：ある攻撃元から複数の被攻撃先に攻撃が継続して行われていた事例
- タイプ II 攻撃：ある攻撃元から複数の被攻撃先へ，毎日特定の時間帯にのみ攻撃が行われていた事例
- タイプ III 攻撃：毎回異なる攻撃元から複数の被攻撃先群へ向けて攻撃が行われていた事例（これはタイプ I，II 攻撃とは異なり，これまで報告されていなかった）

3.2.1　タイプ I 攻撃

この事例は，ある 1 つの攻撃元から複数の被攻撃先へ攻撃が継続して検知されていた事例である．これは従来知られているブルートフォース攻撃の典型例である．ただし，この攻撃は 1 回あたりのログイン試行回数が 20〜30 回程度と [3] で報告された，IDS/IPS を回避するような動作が含まれていたことが判明した．

3.2.2　タイプ II 攻撃

この事例も，ある 1 つの攻撃元から複数の被攻撃先へ攻撃が継続して検知されていた事例である．しかも，毎日 24 時前後 2 時間だけログイン試行が行われるという，攻撃検知時刻と回数に周期性があった．

3.2.3　タイプ III（新型）攻撃

この攻撃事例では，検知時刻によって毎回異なる攻撃元から特定の複数の被攻撃先群へ向けて攻撃が継続して検知されていた．例えば，時刻 t_1 では攻撃元 H_1 から被攻撃先 $V_1, V_2, \cdots, V_n$ へブルートフォース攻撃を行い，時刻 t_2 では攻撃元 H_2 から被攻撃先 $V_1, V_2, \cdots, V_n$ へブルートフォース攻撃を行うといったように，時刻によって異なる攻撃元から特定の被攻撃先群へ向けたブルートフォース攻撃が繰り返されていた．

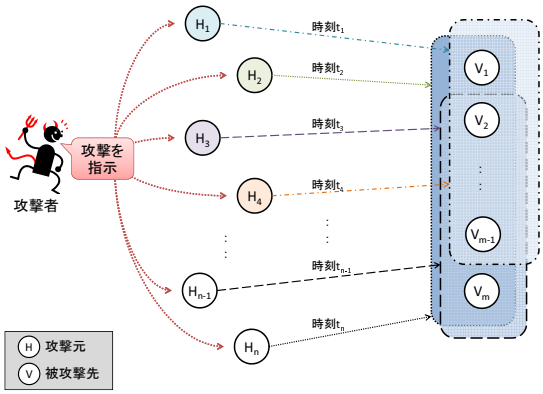

図 2: 推測されるタイプ III の全体像

3.3　タイプ III（新型）攻撃の特徴

この事例には攻撃元，被攻撃先，ログイン試行回数，攻撃検知時刻の点から次のような特徴がある．

まず攻撃元に関して，1 つの攻撃元は 1 回の攻撃においてほぼ 1 回しか登場していなかった．攻撃が検知された約 1〜2ヶ月に同じ攻撃元が登場したケースはあったものの，そのような攻撃元はごくわずかであった．

被攻撃先に関して，特定の被攻撃先群は上記のような複数の攻撃元から長期間継続して攻撃を検知し続けていた．しかし被攻撃先群の中には，他の被攻撃先群が攻撃を受けていたにもかかわらず攻撃を受けなかった被攻撃先が存在したケースも多数あった．途中から被攻撃先群に加わった被攻撃先，逆に攻撃元から攻撃を受けなくなった被攻撃先，あるいはある一定期間のみ攻撃をうけなかった被攻撃先も存在した．

ログイン試行回数は，平均が約 17.6 回であった．分析対象のログ全体のログイン試行回数の平均が約 72.18 回であったことから，比較的回数は少なかった．

攻撃検知時刻は，ある 1 つの攻撃元から被攻撃先群に対してほぼ同じ時刻で攻撃が検知されていた．しかし，被攻撃先によっては，時間的に連続して攻撃が検知されたのもあれば，そうでない被攻撃先も存在した．時間的に連続して攻撃が検知された例では，約 7 時間ほど攻撃が検知され続けたケースもあった．

以上から，次の 3 点が推測できる（図 2）．

- IDS/IPS からの検知を回避するため，少ないログイン試行回数でブルートフォース攻撃を行っていた．
- 被攻撃先へブルートフォース攻撃を試みる攻撃者が存在し，その攻撃者によって IP アドレス群が用意された．
- 攻撃者は攻撃が発生していることをカモフラージュするため，また自身の身元を隠すために，それらの IP アドレスを使い捨てながら攻撃を行い続けていた．

4 タイプ III（新型）攻撃の対策手法

本章では，新型のタイプ III 攻撃を受ける被攻撃先群を早期に発見する手法を提案する．本手法により発見できた被攻撃の先群を重点的に監視することで，次の攻撃の発生を最小限に抑えることができる．

4.1 対策における要件

タイプ III 攻撃の対策における要件は，a) 被攻撃先側で対策を行う，b) 早期に対策を行う，の 2 点である．

攻撃元側に着目した対策としては，例えば攻撃元となっている IP アドレスを特定し，そのアドレスからの通信を全て遮断するといったブラックリスト方式がある．しかし，ブラックリスト方式を適用したとしても，その攻撃元は攻撃のたびに毎回異なるため，次の攻撃を防ぐことはできない．そのため，被攻撃先側で対策を行うことが必要である．

長期間収集した IDS ログに対して相関分析を行うことで被攻撃先を発見する手段もある．しかし，被攻撃先群は変動する場合もあり，この手段によって得られた被攻撃先群を対策するのでは不十分である．そのため，早期に被攻撃先を発見して対策することも必要である．

4.2 被攻撃先群の早期発見手法

4.2.1 基本アイディア

タイプ III 攻撃を今後も受け続ける可能性の高い被攻撃先群を，タイプ III 攻撃が持つ次の特徴 3 点を用いることで IDS ログを長期間収集することなく短期間に発見することができる．

- ある 1 つの攻撃元から，複数の被攻撃先へ攻撃が発生する
- 同じ攻撃元からはほぼ同一の時刻に攻撃が発生する
- 同じ時刻におけるログイン試行回数は被攻撃先間でほぼ同一である

4.2.2 処理手順

入力を IDS ログ，出力を IP アドレス群とする．IDS ログは次に示すデータ構造を持つものとする．

- 攻撃元…攻撃元と検知された IP アドレス
- 被攻撃先…被攻撃先と検知された IP アドレス
- 検知時刻…ブルートフォース攻撃を検知した時刻
- ログイン試行回数…攻撃元から被攻撃先へブルートフォース攻撃が検知された回数
- ポート番号…攻撃が検知された被攻撃先のポート番号

次の 3 手順により，被攻撃先となる IP アドレスを発見する．

1. 被攻撃先ごとに，検知時刻，攻撃元，ログイン試行回数に関するデータ列（回数データ列）を作成する．
2. 回数データ列について，相関の高い被攻撃先群が存在するかを計算する．
3. 相関の高い被攻撃先群が同一の攻撃元から攻撃を受けていたことがあるかを判断する．

手順 1. では，入力された IDS ログからポート番号ごとに，攻撃元と検知時刻を行，被攻撃先を列として，ログイン試行回数に関する 2 次元データ列（回数データ列）を作成する（図 3）．

		攻撃先				
攻撃元	検知時刻	v1	v2	v3	v4	v5
h1	11/1 0:01	0	0	0	0	50
:	:					
h2	11/1 4:00	12	12	12	0	0
h2	11/1 4:01	10	9	9	0	0
h2	11/1 4:02	3	4	4	0	0
h3	11/1 4:03	0	0	0	100	0
:	:					
h4	11/1 11:59	30	0	0	0	0

v1, v2, v3は今後もタイプIIIの攻撃を受ける可能性が高い

図 3: IDS ログから作成した回数データ列

手順 2. では，各検知時刻のログイン試行回数について相関が高い被攻撃先群を求める [2].

手順 3. では，得られた被攻撃先群が同じ攻撃元，同じ回数，同じ時刻で攻撃が検知されていたかを判断する．該当するならば，将来タイプ III の攻撃を受ける可能性が高いとして，当該被攻撃先群を出力する．

全体の処理フローを図 4 に示す.

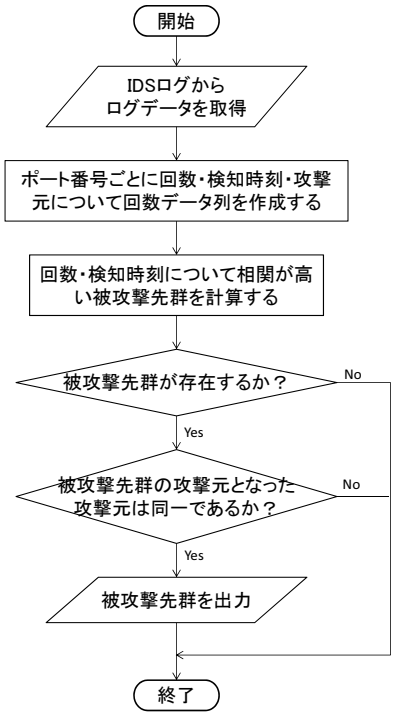

図 4: 処理フロー

4.2.3 効果

本手法により，長期間 IDS ログを収集するのに比べ，タイプ III 攻撃のような，毎回異なる IP アドレスによる攻撃を将来受ける可能性が高い被攻撃先群をより早期に発見することができる．特に提案手法では，ログイン試行回数について相関が高い被攻撃先群に対して，さらにそれらの攻撃元の情報を利用して絞りこむ．これにより，少ないログデータからでもタイプ III 攻撃を受ける被攻撃先群を抽出することができる．

なお，分析対象としたログについて，本手法により被攻撃先群を出力できることも確認した.

4.3 攻撃遮断による対策

本手法により発見できた被攻撃先群を重点的に監視する．次に一部の被攻撃先群がもしもタイプ III 攻撃を受けたとき，全ての被攻撃先群が攻撃を受ける前にその攻撃元を発見することができる．発見した攻撃元からの通信を一定期間遮断するといった対策を取ることで，攻撃を受けた一部を除く全ての被攻撃先群が攻撃を受けることを防ぐことができる．

例えば V_1, V_2, V_3 が被攻撃先群として手法により出力されたとする．次の攻撃元 IP アドレス H_2 が 1 分おきに V_1, V_2, V_3 の順で攻撃を試みようとしたとき，V_1 が H_2 から攻撃を受けたことを検知し，H_2 からの通信を一定期間遮断することで，V_2, V_3 は H_2 からの攻撃を防ぐことができる．

[2] 具体的には，まず n 個の被攻撃先群 $V_1, V_2, \cdots, V_n$ について，相関が高い被攻撃先群のペアを求める．被攻撃群をグラフ理論におけるノード，得られた被攻撃先群のペアをノード同士がエッジで結ばれているとみなす．次に相関が高い被攻撃先群のペアについて，あらゆる 2 つの頂点を繋ぐエッジが存在するノード群を見つける最大クリーク問題を適用することで，相関の高い被攻撃先群を求めることができる.

5 まとめと今後の課題

我々は，実際のネットワーク監視ログについて，攻撃元・攻撃検知時刻に着目した可視化を行い，組織的または規則的な特徴を有するブルートフォース攻撃事例を 3 種類発見した．特に，毎回異なる攻撃元から特定の被攻撃先群へ向けたブルートフォース攻撃は我々の知る限り報告がされていなかった，新しい攻撃事例である．特にこの攻撃事例は攻撃元，被攻撃先，攻撃検知時刻，ログイン試行回数の点から興味深い特徴を持っていた．これらの特徴から，攻撃者は攻撃が発生していることをカモフラージュするために IP アドレスを使い捨てながら攻撃を繰り返していたと推測することができる．

さらに，この攻撃事例について攻撃を受けた被攻撃先にはそれぞれ攻撃元，攻撃検知時刻，ログイン試行回数について強い相関がある．この特徴を利用することで，この攻撃を受けた被攻撃先を IDS ログから早期に発見する手法を提案した．提案手法により得られた被攻撃先群を監視することにより，次のタイプ III 攻撃の発生を最小限に抑えることができる．

今後の課題は，まず今回我々が発見した攻撃事例についてさらに考察を深めることである．また提案手法の適用による False Positive や False Negative の発生について評価を行うことも必要である．

参考文献

[1] SUCRI Blog, "The WordPress Brute Force Attack Timeline," http://blog.sucuri.net/2013/04/the-wordpress-brute-force-attack-timeline.html,2013.

[2] US-CERT, "Risks of Default Passwords on the Internet," http://www.us-cert.gov/ncas/alerts/TA13-175A,2013.

[3] IBM, "Tokyo SOC Report 2010 年下期," https://www-304.ibm.com/connections/blogs/tokyo-soc/,2010.

[4] SANS Internet Storm Center, "ISC Diary — Distributed SSH Brute Force Attempts on the rise again," https://isc.sans.edu/diary/Distributed+SSH+Brute+Force+Attempts+on+the+rise+again/9031 ,2010.

[5] Dragon Research Group, "SSH Brute Force Attack Source Insight（2011-04-29）," http://www.dragonresearchgroup.org/2011/04/29/,2011.

[6] インターネットコム, "「gooID」不正ログイン攻撃は総当たりでなく使い回し ID/パスワード試行、全 ID をロック," http://japan.internet.com/webtech/20130411/1.html,2013.

[7] サイバーエージェント, "「Ameba」への不正ログインに関するご報告," http://www.cyberagent.co.jp/info/detail/id=7874,2013.

[8] Ars Technica, "Mass-login attack on Nintendo fan site hijacks 24,000 account," http://arstechnica.com/security/2013/07/mass-login-attack-on-nintendo-fan-site-hijacks-24000-accounts/,2013.

[9] Anna Sperotto, Ramin Sadre, Pieter-Tjerk de Boer, Aiko Pras, "Hidden Markov Model modeling of SSH brute-force attacks," DSOM2009, LNCS5841, pp164-176, 2009.

[10] J Vykopal, "A Flow-Level Taxonomy and Prevalence of Brute Force Attacks," ACC2011 Part II CCIS 191, pp666-675, 2011.

[11] 武仲, 鳥居, 清水, "ランダムで低速なポートスキャンの検知についての検討," コンピュータセキュリティシンポジウム（CSS2012）, 2012.

[12] 武仲, 鳥居, 古川, 清水, "ランダムで低速なポートスキャンの検知についての検討 2," 暗号と情報セキュリティシンポジウム（SCIS2013）, 2013.

[13] D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, and K. Nakao, "nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis," WOMBAT Workshop on Information Security Threats Data Collection and Sharing, pp58-66, 2008.

[14] JPCERT コーディネーションセンター, "TSUBAME（インターネット定点観測システム）," http://www.jpcert.or.jp/tsubame/

[15] Cliff Changchun Zou, Lixin Gao, Weibo Gong, Don Towsley, "Monitoring and early warning for internet worms," 10th ACM CCS, pp190-199, 2003.

[16] Vinos Yegneswaran, Paul Barford, Dave Plonka, "On the Design and Use of Internet Sinks for Network Abuse Monitoring," 7th International Symposium on Recent Advances in Intrusion Detection（RAID）, 2004.

[17] Michael Bailey, Evan Cooke, Farnam Jahanian, Jose Nazario, David Watson, "The Internet Motion Sensor: A Distributed Blackhole Monitoring System, " Network and Distributed Security Symposium（NDSS）, 2005.

[18] 牧田大祐, 吉岡克成, 松本勉, "DNS ハニーポッドによる不正活動観測," 情報処理学会研究報告 2013-CSEC-62, 2013.

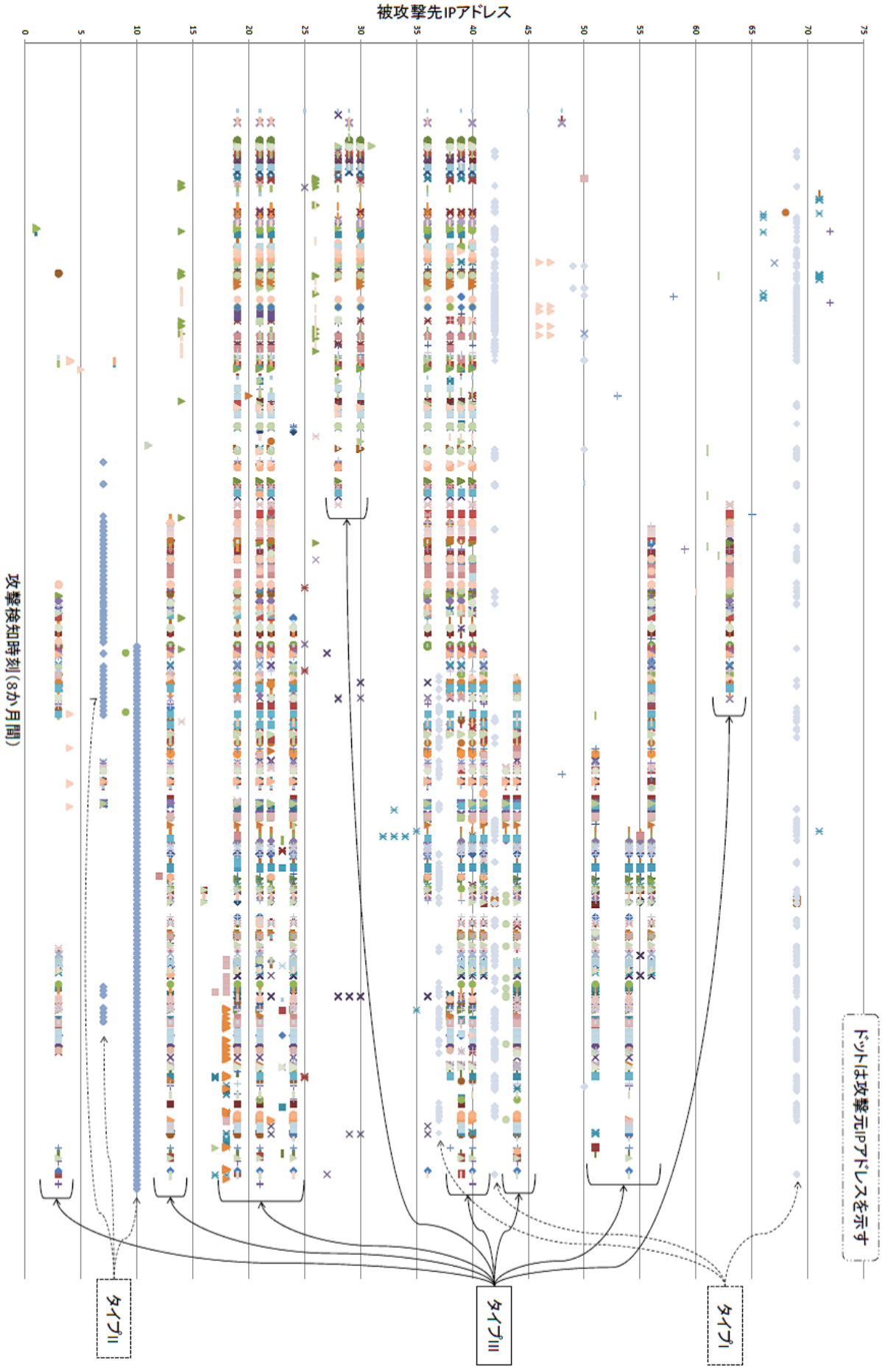

図 1: 22 番ポートへのブルートフォース攻撃可視化結果