ネットワークサービスに対するブルートフォース攻撃の傾向比較

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，ネットワークサービスに対するブルートフォース攻撃は，侵入検知システムだけでは効果的な対策を適用することも難しくなってきている．我々は，実際にサービスを運用している複数のサーバから取得された IDS ログを対象として拠点横断分析を行い，IP 使い捨て型ブルートフォース攻撃，ログイン統御型ブルートフォース攻撃を報告している．本稿では，これらのブルートフォース攻撃の分析の結果得られた抽出手法や分析の観点を他のネットワークサービスのログに対しても適用し，攻撃傾向を分析した．分析の結果，他のネットワークサービスに対しても我々が報告したブルートフォース攻撃と類似した傾向があることがわかった．また，攻撃元に着目してそれぞれの傾向を精査すると，各ネットワークサービスに対するブルートフォース攻撃には，ネットワークサービス毎に固有の特徴を備えていることが明らかになった．

Investigation of Brute Force Attacks for Common Network Services

Satomi Honda　Yuki Unno　Koji Maruhashi　Masahiko Takenaka
Satoru Torii

FUJITSU LABORATORIES LTD.
4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki, Kanagawa 211-8588, JAPAN

Abstract In recent years, preventing brute force attacks for network services become difficult with only intrusion detection systems(IDS). We have been analyzing IDS logs from the sites that are providing network services travarsaly. We have reported the several kinds of distributed and stealthy brute force attacks, the brute force attacks with ephemeral IP addresses and the attacks with the regular cycles in login trials. In this paper, we apply our extracting methods and viewpoints of analyses to the IDS logs for the other commonly-used network services. We investigate and compare the trends of brute force attacks among them. As a result, we grasp the similar brute force attacks that we had reported. Furthermore, the structure of brute force attack is unique to each network service.

1　はじめに

近年，ネットワークサービスに対するブルートフォース攻撃は，侵入検知システム（Intrusion Detection System, IDS）だけでは攻撃の発生を検知することも，効果的な対策を適用することも難しくなってきている [1][2][3]．複数の IP アドレスによるログイン試行であったり，一般に攻撃と判断される回数よりも少ない回数でのログ

イン試行であったりする場合，ブルートフォース攻撃の発生そのものをIDSが検知できたとしても，通信の遮断といった対策を適用することが難しい．また，RDP(Remote Desktop Protocol)サービスに対するブルートフォース攻撃の増加がアンチウィルスソフトベンダーより報告されたり [4]，ネットワーク監視レポートにブルートフォース攻撃が近年再び取り上げられるようになったり [5] と，ブルートフォース攻撃は依然として注意すべき攻撃のひとつである．

我々は，実際にサービスを運用している複数のサーバ（拠点ともいう）から取得された約8か月分のIDSログを対象として拠点横断分析を行い，22番ポートに対するIP使い捨て型ブルートフォース攻撃，3389番ポートに対するログイン統御型ブルートフォース攻撃を検知し，IDSログに残った挙動についてそれぞれ報告している [6][7][8]．これらの攻撃は，単一の拠点あるいは短期間に取得されたIDSログからでは検知することが難しいものであった．

しかし，ブルートフォース攻撃の対象となり得るネットワークサービスは22番，3389番ポートの他にも存在する．これらのポート番号に対するブルートフォース攻撃もIDSログに記録されていたものの，IPアドレスの種類が非常に多い，レコード件数が少ない等の理由でこれまで分析を進めることが難しく，攻撃傾向の把握ができなかった．

そこで本稿では，IP 使い捨て型ブルートフォース攻撃の分析の結果得られた抽出手法や分析の観点を他のネットワークサービスに対するブルートフォース攻撃検知ログに適用し，ブルートフォース攻撃傾向を分析する．分析の結果，3389 番ポートに対するブルートフォース攻撃検知ログからIP 使い捨て型ブルートフォース攻撃と類似した傾向があることがわかった．さらに，攻撃元に着目して各ネットワークサービスに対するブルートフォース攻撃の傾向を精査したところ，ネットワークサービス毎に攻撃元が分業化されていること，攻撃対象の種類数や，ログイン試行回数にそれぞれ特徴を備えていることがわかった．

本稿の構成は次の通りである．第 2 章でIP使い捨て型ブルートフォース攻撃類似傾向の調査を行った結果を報告する．第3 章で各ネットワークサービスに対するブルートフォース攻撃検知ログに関する統計結果を示す．第4 章では，*srcIP* に着目し，その対象となった *dstIP* やログイン試行回数など，各ネットワークサービス毎の特徴を整理する．第5 章では，ネットワークサービス毎のブルートフォース攻撃の特徴を比較する．

なお，以下ではIDSにより攻撃元，被攻撃先（攻撃対象）と検知されたIPアドレスをそれぞれ *srcIP*，*dstIP* とする．ブルートフォース攻撃検知記録とそのログイン試行回数は，分析対象としたIDSログの生成元IDS製品の判断に基づく．

2　IP使い捨て型ブルートフォース攻撃類似傾向の調査

2.1　IP使い捨て型ブルートフォース攻撃

我々が [6][7] にて報告したIP使い捨て型ブルートフォース攻撃（Ephemeral Brute Force Attacks, *EBF*）は，ブルートフォース攻撃を検知した *srcIP*，*dstIP* に相関が確認できるブルートフォース攻撃である．ある一定期間毎に異なる *srcIP* から特定の *dstIP* 群に向けて，断続的にブルートフォース攻撃が検知されていた．1つの *srcIP* によるブルートフォース攻撃においては，*dstIP* 群は同時に攻撃が検知され，そのときのログイン試行回数も *dstIP* 群の間で同回数であった．

我々は，*srcIP*，*dstIP*，検知時刻に着目し22番ポートに対するブルートフォース攻撃検知ログを可視化することで，*EBF* の発生を検知することができた．*dstIP* 毎に，いつ，どの *srcIP* からの攻撃を検知したのかを一枚絵で表現することにより，異なる *dstIP* が同期し攻撃を検知された事象を見つけることができた．

この *EBF* の特徴から，*srcIP* 群を制御する攻撃者の存在が推測できる．その攻撃者は特定の *dstIP* 群を対象として，ブルートフォース攻撃を継続していたと考えられる（図1）．

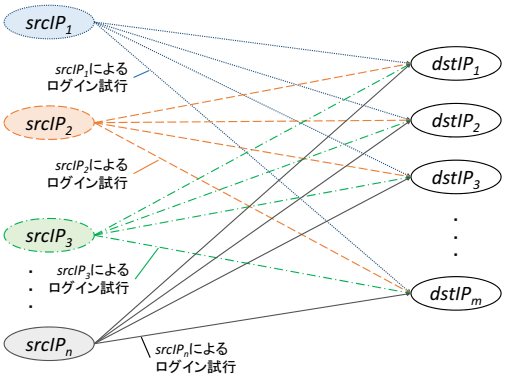

図 1: *EBF* における *srcIP*・*dstIP* 間の関係

図 2: 3389 番ポートに対する BF ログから抽出できた *EBF* に類似した事象

2.2 調査結果

前節にて述べたブルートフォース攻撃について，類似した攻撃傾向が存在しないかを調査した結果を表 2.2 に示す．調査の結果，3389 番ポートに対する BF ログから *EBF* に類似した攻撃が検知されていた．

表 1: 類似攻撃傾向の調査結果

ポート番号	*EBF* 類似傾向
21	なし
22	あり（既知）
80	なし
445	なし
3389	あり

2.3 調査手順

EBF に類似した傾向を，次の手順により調査した．

我々が [6] にて提案した，*EBF* に該当する *dstIP* 群の抽出手法を適用することで検証を行った．BF ログから *EBF* によるブルートフォース攻撃を受けた *dstIP* 群を抽出できたか否かにより，*EBF* に類似した事象の検証を行った．*EBF* に該当する *dstIP* 群の抽出手法では，次の 3 つの特徴を持つログを抽出することで，*EBF* によるブルートフォース攻撃を受けた *dstIP* 群を抽出する：i) ある 1 つの *srcIP* から複数の *dstIP* へブルートフォース攻撃が検知された，ii) ある *srcIP* から *dstIP* 群へのブルートフォース攻撃は同時刻である，iii) ある *srcIP* から *dstIP* 群へのブルートフォース攻撃におけるログイン試行が同一である．

上述の抽出手法を適用した結果，3389 番ポートに対する BF ログから，*EBF* に類似した事象が検知されていることがわかった．図 2 に，*EBF* に類似した事象と判断されたログを抽出し，*srcIP*，*dstIP*，検知時刻に着目した BF ログの可視化を適用した結果を示す．横軸は攻撃検知時刻を，縦軸は *dstIP* を示す．図中のドットはブルートフォース攻撃が検知されたことを示し，ドットの色や形は *srcIP* の種類に依存する．

この図から，複数の *dstIP* 群が一定期間毎に異なる *srcIP* から，同時刻に攻撃が検知されていたことが確認できた．

3 各ネットワークサービスに対するブルートフォース攻撃検知ログの比較

本章では，各ネットワークサービスに対するブルートフォース攻撃検知ログ（BF ログ）について統計を計算し，ネットワークサービス毎のブルートフォース攻撃検知状況を比較した．本

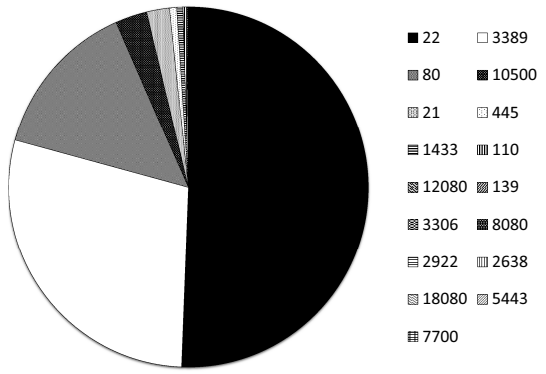

図 3: BF ログに占めるレコード件数の割合（ポート番号毎）

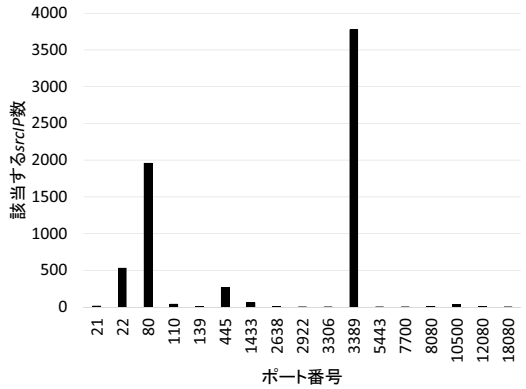

図 4: BF ログにおける *srcIP* 数（ポート番号毎）

章では BF ログに記録されたポート番号毎に統計を計算した．

まず，BF ログに占めるレコード件数のポート番号毎の割合を図 3 に示す．レコード件数の合計は 411,747 件であった．この図から，上位を占めていたのは 22 番ポート（約 50.61%），3389 番ポート（約 28.64%），80 番ポート（約 14.15%）に対する BF ログであった．

次に，BF ログに記録されたポート番号毎の *srcIP* 数，*dstIP* 数をそれぞれ図 4，図 5 に示す．この結果から，*srcIP* 数が多かった上位 3 種類のポート番号は 3389 番ポート，80 番ポート，22 番ポートであった．一方で，*dstIP* 数が多かった上位 3 種類のポート番号は 80 番ポート，22 番ポート，3389 番ポートであった．

これらの結果から，傾向を分析できるのに十分なログの量，*srcIP* 数，*dstIP* 数を持つポート番号に対する BF ログを選定する．そこで，次の 3 つの条件：条件 1) BF ログに占める割合が大きかった上位 5 種類であること，条件 2) *srcIP* 数，*dstIP* 数が 10 種類以上あること，条件 3) well-known ポートであること，の全てを満たす 5 種類のポート番号 21，22，80，445，3389 番ポートに対する BF ログを，以降の分析の対象とした．

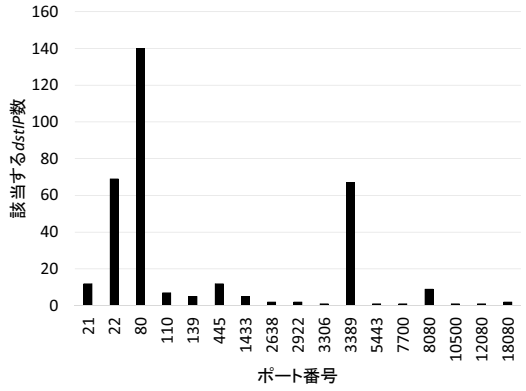

図 5: BF ログにおける *dstIP* 数（ポート番号毎）

4 *srcIP* の手口の集計

srcIP に着目して，その対象となった *dstIP* や，ログイン試行回数など，各ネットワークサービス毎の特徴を整理した．これにより，各サービスへの攻撃の特徴や，その背景にある攻撃元の意思が明らかになることが期待できる．

4.1 ブルートフォース攻撃対象のネットワークサービス

まず，*srcIP* がブルートフォース攻撃のターゲットとするネットワークサービスの種類について集計した．その結果，ほとんどの *srcIP*（約 98.5 %）は，ひとつのサービス（ポート番号）に対するブルートフォース攻撃のみを行ってい

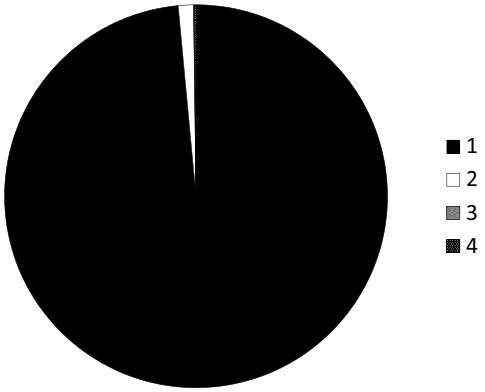

図 6: *srcIP* が攻撃先としたポート番号の種類

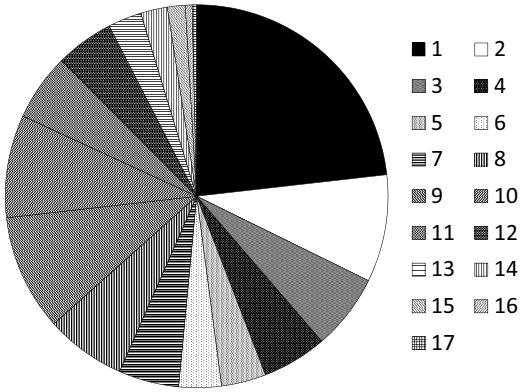

図 8: 1*srcIP* に対する *dstIP* 数 (22 番ポート)

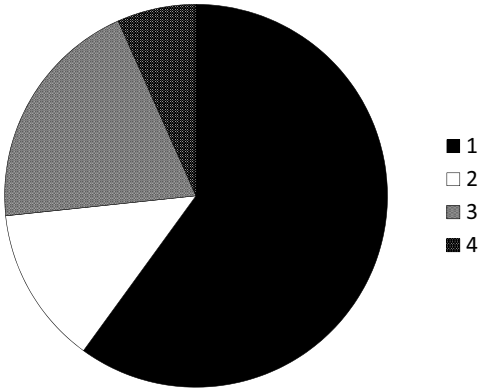

図 7: 1*srcIP* に対する *dstIP* 数 (21 番ポート)

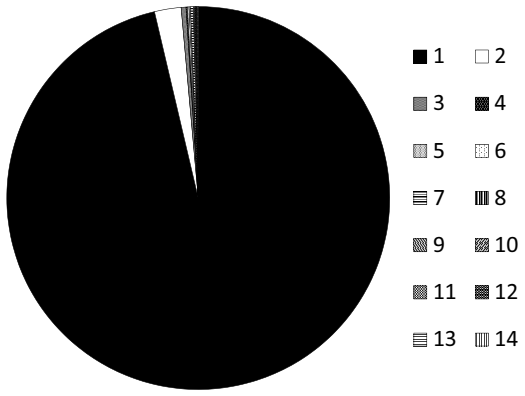

図 9: 1*srcIP* に対する *dstIP* 数 (80 番ポート)

た（図 6）．このことから，サービス毎に *srcIP* が分業化されていると類推できる．

4.2 ブルートフォース攻撃の対象となった *dstIP* の種類

各ネットワークサービスに対するブルートフォース攻撃のターゲット (*dstIP*) の種類数を *srcIP* 毎に集計した．その結果を図 7 〜図 11 に示す．この結果から，多くの場合で，ひとつの *srcIP* はひとつの *dstIP* に対して（1 対 1 で）攻撃を行っている．一方で，22 番ポート (SSH) や 445 番ポート (SMB) に対しては，複数の *dstIP* に対して（1 対 n で）攻撃を行っていることが見受けられる．

4.3 ログイン試行回数

各ネットワークサービスに対するブルートフォース攻撃の試行回数を *srcIP* 毎に集計し，この試行回数の *srcIP* の数を集計した．この集計においては，ひとつの *srcIP* がひとつの *dstIP* に対して観測された試行回数を，単純に観測期間全体で合計したものとした．その結果を図 12 〜図 16 に示す．

我々は，試行回数の値そのものではなく，その頻度のばらつきに着目した．それゆえに，横軸は試行回数をその昇順で出現順に並べたものとしている．縦軸は，その試行回数に相当する *srcIP* の個数である．

この結果から，21 番ポート (FTP) は *srcIP* 毎にユニークな試行回数であり，80 番ポート

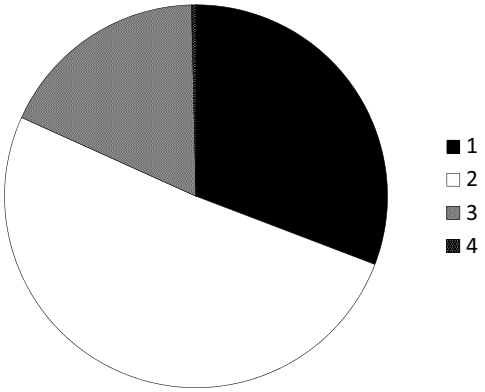

図 10: 1*srcIP* に対する *dstIP* 数 (445 番ポート)

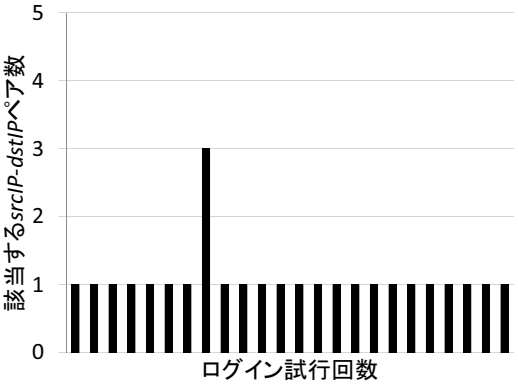

図 12: ログイン試行回数の度数分布 (21 番ポート)

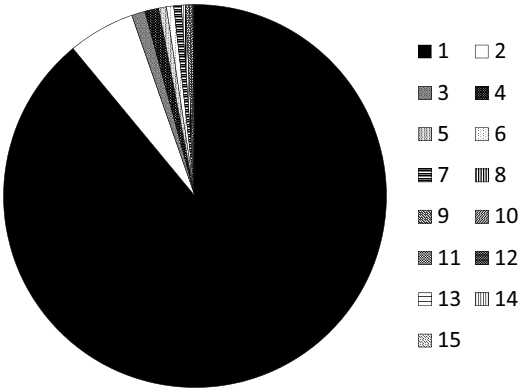

図 11: 1*srcIP* に対する *dstIP* 数 (3389 番ポート)

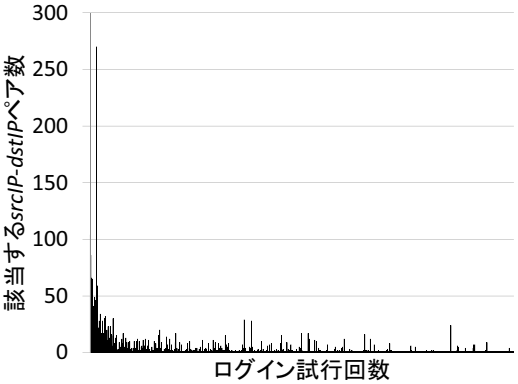

図 13: ログイン試行回数の度数分布 (22 番ポート)

(HTTP) は指数分布のような形態を示している．残りの他ポート番号では，個数に顕著な集中（スパイク）がいくつか見られる．

5 ネットワークサービス毎の攻撃の特徴

検知結果は，ブルートフォース攻撃の対象となるネットワークサービスの稼働状況に影響があると考えられる．そこで，攻撃の特徴を検討するにあたり，*dstIP* の総種類数が同程度のサービスを比較対象として考察を行う．

5.1 22 番ポートと 3389 番ポートの比較

22 番ポートと 3389 番ポートは，それぞれ，*dstIP* の種類数が同程度（約 70 個）であった．

図 8 と図 11 を比較すると，22 番ポート（SSH）はひとつの *srcIP* から複数の *dstIP* に攻撃するケースが多い．一方で，3389 番ポート（RDP）はひとつの *srcIP* からひとつの *dstIP* に攻撃するケースが多い．また，図 13 と図 16 を比較すると，22 番ポートは各 *srcIP* の試行回数の値は，ある特定の少ない試行回数の値に集中している．一方で，3389 番ポートはある特定の試行回数の値に集中しており，それが複数回に及んでいる．

これらのことから，22 番ポートでは各 *srcIP*

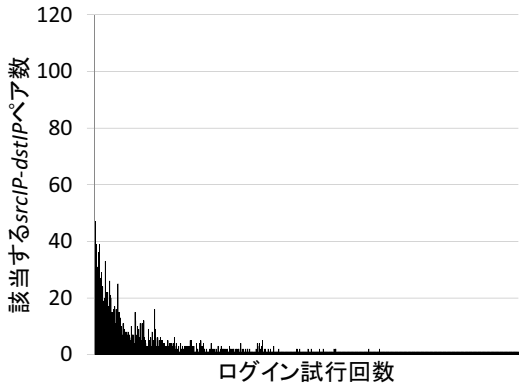

図 14: ログイン試行回数の度数分布 (80 番ポート)

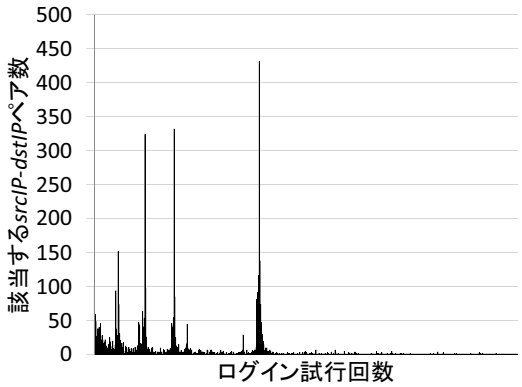

図 16: ログイン試行回数の度数分布 (3389 番ポート)

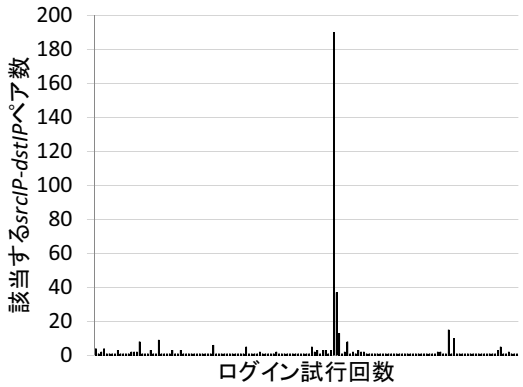

図 15: ログイン試行回数の度数分布 (445 番ポート)

は，複数の *dstIP* に対して攻撃を行い，その試行回数は異なる *srcIP* であっても同様の傾向が存在することがわかる．一方，3389 番ポートでは各 *srcIP* は，ひとつの *dstIP* に対してログイン試行を行い，その試行回数は異なる *srcIP* であっても同様の傾向が存在し，しかもその傾向は複数種類存在すると類推できる．

5.2 21 番ポートと 445 番ポートの比較

21 番ポートと 445 番ポートは，それぞれ，*dstIP* の種類数が同程度（12 個）であった．

図 7 と図 10 を比較すると，21 番ポート（FTP）はひとつの *srcIP* からひとつの *dstIP* に攻撃するケースが多い．一方で，445 番ポート（SMB）はひとつの *srcIP* から複数の *dstIP* に攻撃するケースが多い．また，図 12 と図 15 を比較すると，21 番ポートは各 *srcIP* の試行回数の値はばらついている．一方で，445 番ポートはある特定の試行回数の値に集中している．

これらのことから，21 番ポートでは各 *srcIP* は独自に（バラバラに）攻撃を行っている．また 445 番ポートでは，各 *srcIP* は複数の *dstIP* をターゲットとしており，各 *srcIP* には同様の攻撃環境（攻撃ツール）が用いられていると類推できる．

5.3 80 番ポートの特徴

図 9 と図 14 から，80 番ポートは，ひとつの *srcIP* からひとつの *dstIP* に攻撃するケースが多いが，その試行回数の値はばらついている．

上記の 4 種類のポート番号への攻撃とは，また異なる傾向が見られる．1 対 1 攻撃の傾向が多くみられる点は，正直なところ，意外であった．ポート 80 番は著名な公開サービスのひとつであり，実際のところ *srcIP* の種類が多く，様々な *srcIP* が攻撃を行っているものと類推できる．

5.4 考察

3389 番ポートにおける *srcIP* の数は，他のサービスと比べて多く，おそらく 1 対 1 型攻撃の形態が主流になっているものと思われる．一方，22 番ポートに関しては，レコード件数は多いもののその *srcIP* の数は多くなく，おそらく，1 対 n 型攻撃の形態が充実しているものと思われる．

445 番ポートと 3389 番ポートにおいて，試行回数に特徴的な集中が見られる．この原因のひとつとして，流布している同様の攻撃ツールが複数で用いられていることが考えられる．あるいは，攻撃対象サービスのチェックアウト機能が影響していることも考えられる．

ひとつの *srcIP* が攻撃対象とする *dstIP* を複数とする 1 対 n とするか，ひとつとする 1 対 1 とするかは，攻撃元の環境に依存することが考えらる．すなわち，ひとつの攻撃元から，一度に複数の対象先にチャレンジできるようなサービスかどうかに影響すると考えられる．

21 番ポートや 445 番ポートにおける *dstIP* 数が少ないのは，攻撃対象としてサービスを外部に公開している対象先が限定されていることが考えられる．監視対象をさらに広げることで，あるいは，今後同様のサービスの外部公開が拡大することで，22 番ポートや 3389 番ポートと同様の傾向が見受けられる可能性もあるであろう．

6 まとめ

本稿では，各ネットワークサービスに対するブルートフォース攻撃検知ログを対象として，その攻撃傾向を分析・比較を行った．その結果，22 番ポートに対するブルートフォース攻撃検知ログから検知することができた IP 使い捨て型ブルートフォース攻撃が，3389 番ポートにおいても発生していたことが確認できた．さらに，攻撃元に着目した分析を行い，ネットワークサービス毎に *srcIP* が分業化されていること，*dstIP* の種類数や，ログイン試行回数にそれぞれ特徴を備えているという知見が得られた．

参考文献

[1] Mobin Javed, Vern Paxson, Detecting Stealthy, Distributed SSH Bruteforcing, 2013 ACM SIGSAC conference on Computer & communications security, pp85-96, 2013.

[2] Vizvary Martin, Jan Vykopal, Flow-based detection of RDP brute-force attacks, 7th International Conference on Security and Protection of Information (SPI 2013), 2013.

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

[4] http://securityaffairs.co/wordpress/26247/cyber-crime/kaspersky-lab-reveals-increase-rdp-bruteforce-attacks.html, ”Kaspersky Lab reveals an increase in RDP bruteforce attacks — Security Affairs.” last visited in 2014/7/9.

[5] Alert Logic, ”CLOUD SECURITY REPORT - SPRING 2014”, pp3-7, 2014.

[6] 本多, 海野, 丸橋, 武仲, 鳥居, ”使い捨て IP による新型ブルートフォース攻撃の検出,” コンピュータセキュリティシンポジウム (CSS2013), 2013.

[7] 本多, 海野, 丸橋, 武仲, 鳥居, ”使い捨て IP によるブルートフォース攻撃検出手法の評価,” 暗号と情報セキュリティシンポジウム (SCIS2014), 2014.

[8] 本多, 海野, 丸橋, 武仲, 鳥居, ”RDP サービスへの分散型ブルートフォース攻撃,” マルチメディア，分散，協調とモバイルシンポジウム (DICOMO2014), 2014.