RDPサービスへの分散型ブルートフォース攻撃

本多 聡美[1]　海野 由紀[1]　丸橋 弘治[1]　武仲 正彦[1]　鳥居 悟[1]

概要：
ネットワークセキュリティ分野において，ブルートフォース攻撃とは，ネットワークサービスの利用に必要なユーザ名とパスワードの組合せの取得を試みる攻撃を指す．侵入検知システム（IDS, Intrusion Detection System）は，このブルートフォース攻撃である可能性が高い通信を検知することができる．しかし近年では，この IDS による誤検知を装ったブルートフォース攻撃の発生も報告されるようになっている．本稿では，IDS ログを対象とした拠点間横断分析により，RDP（Remote Desktop Protocol）サービスへ向けた，複数の異なる IP アドレスから，少ない回数でのログイン試行を行うブルートフォース攻撃（分散型 BF）を検知したので報告する．我々は，攻撃元と検知された IP アドレス毎のログイン試行回数の合計に関する分布に着目することで，少ないログイン試行回数で一定期間のみブルートフォース攻撃が検知された IP アドレスを抽出することができた．また我々は使い捨て IP によるブルートフォース攻撃の発生を IDS ログから抽出する手法を提案しており，この手法を適用することで，分散型 BF を受けたホストの抽出可能性を検討した．その結果，単位時間当たりのログイン試行回数に関する回数データ列を作成する処理については手法の適用が可能であるものの，分散型 BF を受けたホストの抽出には，相関の計算による抽出に適したフィールドを選択する必要があることがわかった．

Distributed Brute Force Attacks against RDP Services

Satomi Honda[1]　Yuki Unno[1]　Koji Maruhashi[1]　Masahiko Takenaka[1]　Satoru Torii[1]

1. 背景

ネットワークセキュリティ分野において，ブルートフォース攻撃とは，ネットワークサービスの利用に必要なユーザ名とパスワードの組合せの取得を試みる攻撃を指す．例えば，ユーザ名を「root」に固定し，パスワードを「0000」から「9999」まで順番に変えながら，サービスのログインに成功する組合せが存在するかどうかを試す．辞書に収録されている単語をユーザ名あるいはパスワードの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する．さらには，他サービスから漏えいしたと考えられるユーザ名・パスワードの組合せを別のサービスのログイン試行に使用する攻撃（パスワードリスト攻撃ともいう）も報告されている [1].

侵入検知システム（IDS, Intrusion Detection System）は，ブルートフォース攻撃である可能性が高い通信を検知することができる．例えば，短時間に単一の IP アドレスからの通信で，大量のログイン失敗を伴っていたものなどである．一方で，IDS は正規通信を「攻撃」と判断することもあり得る（誤検知ともいう）．正規ユーザによる数回のログイン失敗もブルートフォース攻撃と判断されることもある．多くの場合では，ある通信が IDS によりブルートフォース攻撃と検知されても，ログイン失敗回数がある値より少ない場合は何もしない，といったように，誤検知の可能性が高い検知結果は無視するようにシステム管理者等により設定されている．しかし，近年ではこの誤検知を装ったブルートフォース攻撃の発生も報告されるようになっている．少ないログイン試行回数でのログイン試行を長期間続ける，複数の異なる IP アドレスからログイン試行を行うといった手段が各組織より報告されている．

我々は，サービスを実際に運用している複数の拠点（サーバともいう）から得られたネットワーク監視ログの分析（拠点間横断分析）を行っている．この拠点間横断分析により，我々は上述のように IDS による検知を回避する手段を伴うブルートフォース攻撃を検知した．我々は，SSH

[1] 株式会社富士通研究所

（Secure Shell）サービスへ向けた，使い捨て IP アドレスによるブルートフォース攻撃（使い捨て BF ともいう）が約半年以上発生していたことを検知し，当該事象とその対策手法を [2][3][4] にて報告している．

本稿では，IDS ログを対象とした拠点間横断分析により，RDP（Remote Desktop Protocol）サービスへ向けた，複数の異なる IP アドレスから，少ない回数でのログイン試行を行うブルートフォース攻撃（分散型 BF ともいう）を検知したので報告する．複数の異なる IP アドレスによるものや，少ないログイン試行回数でのブルートフォース攻撃の存在そのものは既知であるが，IDS ログそのものには顕著な特徴が現れないため，こうした攻撃の抽出はこれまで困難であった．我々は，攻撃元と検知された IP アドレス毎のログイン試行回数の合計に関する分布に着目することで，少ないログイン試行回数で一定期間のみブルートフォース攻撃が検知された IP アドレスを抽出することができた．抽出した IP アドレスを起点として IDS ログを分析した結果，IDS による検知を回避する手段を伴うブルートフォース攻撃が RDP サービスに向けて発生していた可能性が高いと判断できる．

さらに，IDS ログから分散型 BF を受けたホストを抽出するため，使い捨て BF を検知した IP アドレスを抽出する手法の適用を検討し，適用時の課題を述べる．

本稿の構成は次の通りである．第 2 章で関連技術および検知事例を紹介する．第 3 章で我々が検知した RDP サービスへの分散型 BF を報告し，第 4 章で使い捨て BF を検知した IP アドレスを抽出する手法の適用を検討する．第 5 章でまとめと今後の課題とする．

なお，以下では IDS により攻撃元，被攻撃先と検知された 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. 関連事例・技術

2.1 関連事例の報告

ブルートフォース攻撃はネットワークサービスにおける脅威の一つである．[5] によると，クラウド環境を狙ったブルートフォース攻撃が 2013 年には増加傾向であったことが報告されている．さらに，IDS による検知の回避を意図したブルートフォース攻撃の発生も各組織により報告されている．ネットワークの監視を行う組織により，2010〜2011 年に SSH サービスへ向けたブルートフォース攻撃の発生が報告されている（[6][8] など）．[6] では，長期間収集した SSH サーバへのアクセスログの分析結果からアクセス元となったホストの異なり数の増加が報告され，著者らはこれらのホストに関する分析の結果として，ボットネットによる攻撃である可能性が高いと考察している．[8] においても，異なる複数の IP アドレスによる辞書順でのユーザ名におけるログイン試行の発生が報告されている．これらの報告より，攻撃者はブルートフォース攻撃を実行するために，複数の IP アドレスを用意していたことがわかる．また，IBM SOC(Security Operation Center) からは，1 IP アドレス当たりのログイン試行回数が 10〜30 回程度の通常のブルートフォース攻撃と比べて少ない回数であった旨も併せて報告されている [7]．さらに 2013 年には，コンテンツ管理システムを狙った大規模なブルートフォース攻撃が発生した [9][10]．この事例においても，やはり複数の異なる IP アドレスによるログイン試行であったことも報告されている．このように，ブルートフォース攻撃の検知・対策には，複数の異なる IP アドレスによるログイン試行を行う形態にも備えることも必要となってきている．

一方で，RDP サービスへの攻撃に関する大きな事例として，Widnows ワークステーションやサーバを狙ったワーム「Morto」が挙げられる [11]．あるマシンが Morto に感染すると，Morto はローカルネットワークをスキャンし RDP が有効になっている他のマシンをスキャンする．そして RDP が有効になっているサーバを発見すると，ユーザ名を「Administrator」として，「server」「1234qwer」「admin123」等のパスワードでのログインを試みる．文献 [12] においても，著者の所属する組織のネットワーク監視ログに Morto によるログイン試行が記録されていたことが報告されている．

このように，IDS による検知の回避を意図したブルートフォース攻撃の発生は多く報告されているものの，RDP サービスに向けたブルートフォース攻撃の発生はその報告が少ないのが現状である．しかし，RDP サービスに対しても IDS 検知回避を意図したブルートフォース攻撃が発生していることを考慮した分析が必要である．

2.2 関連技術

ネットワーク上に発生した脅威を検知するため，NICT による nicter[13] や JPCERTCC による TSUBAME[14] 等では，インターネット上のトラフィックの観測が行われている．この観測により，新たなワームの活動や，DoS 攻撃の兆候などを検知することができる．また実際に運用しているネットワークサービスへの攻撃を検知するために，サービス運用拠点に設置した IDS より取得した IDS ログを分析する技術も提案されている（[15] など）．さらに，分析対象とする期間を長期間に設定したり，対象拠点を複数に増やすことで，単一拠点では検知することのできなかった攻撃を検知することができる．実際に，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 [16] や，ブルートフォース攻撃のタイミングが *dstIP* 間で同期していたこと [2] を検知できることが既にわかっている．

3. RDP サービスへの分散型ブルートフォース攻撃（分散型 BF）

本章では，RDP サービスへ向けたブルートフォース攻撃検知ログを分析し，複数の異なる *srcIP* 群から，少ない回数でのログイン試行を行うブルートフォース攻撃（分散型 BF）を検知した結果を報告する．まず *srcIP* 毎のログイン試行回数について分析を行い，分散型 BF に該当する可能性の高い *srcIP* 群を抽出する．抽出した *srcIP* 群について，*srcIP* 毎の検知時刻や国情報に関連した分析を行う．なお，分析対象としたログは 2011 年から 2012 年の 8 ヶ月間に取得されたログである．

3.1 RDP サービスへ向けたブルートフォース攻撃検知ログにおける時間変化

まず，RDP サービスへ向けたブルートフォース攻撃検知ログについて，1 分当たりのログイン試行回数，*srcIP*，*dstIP* について時間変化を分析した結果を示す．

図 1 に，1 日毎の 1 分当たりのログイン試行回数の時間変化を示す．横軸は 1 日単位での検知時刻を，縦軸はログイン試行回数を示す．線分はその日に記録された 1 分当たりのログイン試行回数を示し，線分の上側，下側，三角はそれぞれ 1 分当たりのログイン試行回数の最大，最小，平均を示す．この図から，別の日と比較して大きいログイン試行回数でブルートフォース攻撃が検知された日もあるものの，1 分当たりのログイン試行回数が最大でも約 20 回の範囲で検知された日が非常に多かったことがわかる．

図 2 に，1 日毎の *srcIP* および *dstIP* の異なり数の時間変化を示す．横軸は 1 日単位での検知時刻を，縦軸は *srcIP* あるいは *dstIP* の異なり数を示す．*srcIP* における異なり数は途中大きく増加した箇所も存在したものの，*dstIP* の異なり数は大きな変化はなく，常に約 10 前後の *dstIP* が攻撃を検知されていたことがわかる．

以上の結果から，RDP サービスへ向けたブルートフォース攻撃はほぼ毎日のように検知されていた．しかし，これらの単純な統計情報からは異なる複数の *srcIP* 群からのブルートフォース攻撃の検知状況を把握することは難しい．次節以降にて，*srcIP* に着目した分析を行った結果を示す．

3.2 *srcIP* 毎のログイン試行回数

RDP サービスへ向けたブルートフォース攻撃が検知された srcIP の集合を $SrcIP$ とする．つまり，$SrcIP = \{srcIP_1, srcIP_2, srcIP_3, ...\}$ である．この $SrcIP$ について，*srcIP* 毎のログイン試行回数の合計を算出した．ログイン試行回数の合計の分布を図 3 に示す．この図から，ログイン試行回数の合計が 240 回，108 回，70 回，35 回であった *srcIP* が非常に多く，それらの前後のログイン試行回数の合計についても，該当する *srcIP* 数が多かったことがわかる．こ

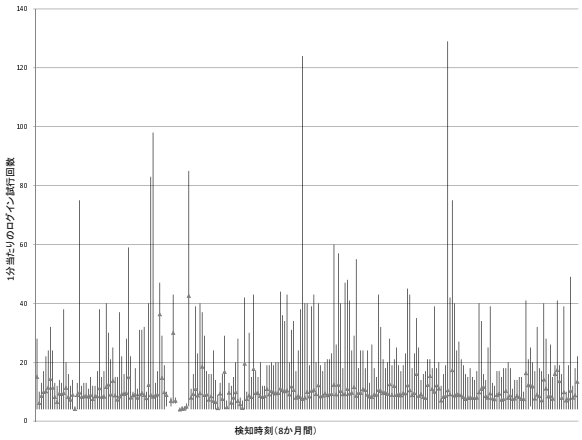

図 1 1 分当たりのログイン試行回数の時間変化

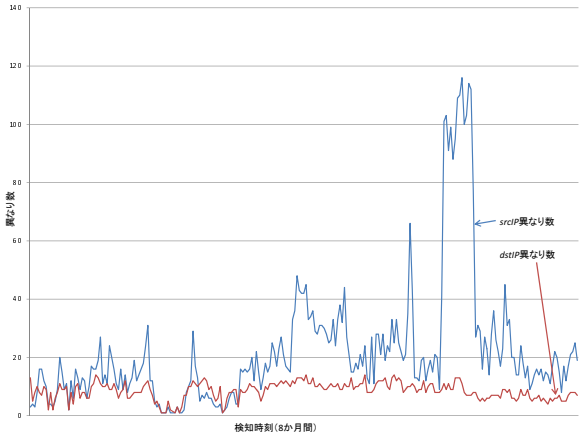

図 2 *srcIP*・*dstIP* 異なり数の時間変化

こで，ログイン試行回数の合計が 240 回，108 回，70 回，35 回であった *srcIP* の集合をそれぞれ，$SrcIP_{240}$，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ とする．つまり，$SrcIP_{240} = \{ srcIP \mid srcIP$ はログイン試行回数の合計が 240 回 $\}$，$SrcIP_{108} = \{ srcIP \mid srcIP$ はログイン試行回数の合計が 108 回 $\}$，$SrcIP_{70} = \{ srcIP \mid srcIP$ はログイン試行回数の合計が 70 回 $\}$，$SrcIP_{35} = \{ srcIP \mid srcIP$ はログイン試行回数の合計が 35 回 $\}$ である．

3.3 *srcIP* 毎の検知時刻

$SrcIP_{240}$，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ について，検知時刻と *dstIP* の関係を図 4 に示す．横軸は検知時刻を，縦軸は異なる *dstIP* を，ドットはブルートフォース攻撃が検知されたことを示す．色および形の異なるドットは，それぞれ $SrcIP_{240}$，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ に属する *srcIP* によることを示す．

図中でドットが横軸に平行な線状の形を構成しているのは，ある *dstIP* に対するブルートフォース攻撃が検知され続けていたことを表す．この図から，特定の *dstIP* がブ

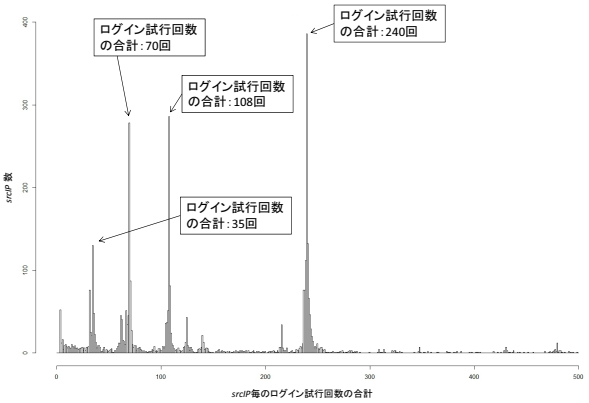

図 3 *srcIP* 毎のログイン試行回数合計の分布

ルートフォース攻撃を検知され続けていたこと，$SrcIP_{240}$，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ について検知時刻に特徴があることが確認できる．RDP サービスに向けたブルートフォース攻撃が検知された *dstIP* 数は全部で 67 であったが，その内の約 20 前後の *dstIP* が $SrcIP_{240}$，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ に属する *srcIP* によるブルートフォース攻撃を検知され続けていた．

またこの図から，$SrcIP_{240}$ に該当するドットが図中の左側にのみ登場していた，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ に該当するドットが図中に右側にのみ登場していた．これらの特徴から，*srcIP* について，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ がある時刻から検知され始めた，$srcIP_{240}$ はある時刻から検知されなくなったことがいえる．なお特定の *dstIP* 群が同時刻にブルートフォース攻撃を検知された，といった特徴は確認できなかった．

3.4 ログイン試行回数と試行時間の関係

さらに，$SrcIP_{240}$，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ に属する *srcIP* について，1 分当たりのログイン試行回数の平均と検知された時間について，該当する *srcIP* 数を算出し，3 次元ヒストグラムとして表現した．結果を図 5 に示す．x，y，z 軸はそれぞれ，1 分当たりのログイン試行回数の平均，検知された時間（分），該当する *srcIP* 数を示す．例えば，$SrcIP_{35}$ においては，1 分当たりのログイン試行回数の平均が約 7 回で検知された時間が約 5 分間であった *srcIP* 数と，1 分当たりのログイン試行回数の平均が約 8.75 回で検知された時間が約 4 分間であった *srcIP* 数が多かったことを表す．

$SrcIP_{240}$，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ について 3 次元ヒストグラムを比較する．まず 1 分当たりのログイン試行回数の平均について，いずれにおいても該当する *srcIP* は約 4〜18 回の範囲に収まっていた．分析対象としたログのブルートフォース攻撃検知記録における 1 分当たりのログイン試行回数は約 72.18 回であった．このことから，$SrcIP_{240}$，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ に該当する *srcIP* の持つ 1 分当たりのログイン試行回数平均は少ない．さらに，$SrcIP_{35}$ においてはヒストグラムの山が大きく 2 点であること，$SrcIP_{70}$ においてはヒストグラムの山が 1 箇所に集まっていることから，それぞれに該当する *srcIP* 群は，1 分当たりのログイン試行回数平均および検知された時間について，類似した挙動を記録されていたといえる．

次に検知された時間について，ログイン試行回数の合計が大きくなるにつれて検知された時間も大きくなっている．1 分当たりのログイン試行回数の平均は $SrcIP_{240}$，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ のいずれの場合も大きな差がなかったことから，各 *srcIP* の持つログイン試行回数の合計は検知された時間と大きく関連があるといえる．

3.5 *srcIP* の国情報

$SrcIP_{240}$，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ について，*srcIP* の国コード上位 5 と該当する *srcIP* 数を表 1 に示す．この表から，特に上位 3〜4 に該当する国コードの傾向が類似していることがわかる．

表 1 *srcIP* の国コード（Top 5）

$SrcIP_{240}$	国コード	US	CN	BR	DE	TR
	srcIP 数	122	71	37	25	25
$SrcIP_{108}$	国コード	US	CN	BR	TR	DE
	srcIP 数	79	68	20	19	16
$SrcIP_{70}$	国コード	CN	US	BR	RU	IN
	srcIP 数	83	79	30	20	18
$SrcIP_{35}$	国コード	CN	US	IR	BR	VN
	srcIP 数	41	31	17	11	8

3.6 統計的特徴から推測できること

以上の統計結果から，RDP サービスへの分散型 BF について，次のような攻撃者の意図が推測できる．まず，$SrcIP_{240}$，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ のいずれにおいても 1 分当たりのログイン試行回数が少なかったことから，従来の IDS による検知を回避する意図を持った攻撃者により用意された可能性が高い．そして，攻撃者はブルートフォース攻撃制御ツールなどを用いて，単位時間当たりのログイン試行回数と 1 *srcIP* 当たりのログイン試行期間，ブルートフォース攻撃の対象とする *dstIP* を設定し，ログイン試行を長期間続けていたことも推測できる．

また，ある時刻から検知されなくなった $SrcIP_{240}$ や，ある時刻から検知され始めた $SrcIP_{70}$・$SrcIP_{35}$ は別の攻撃者により用意された可能性もあるが，同一の攻撃者が設定を変更した可能性も考えられる．例えばログイン試行回数

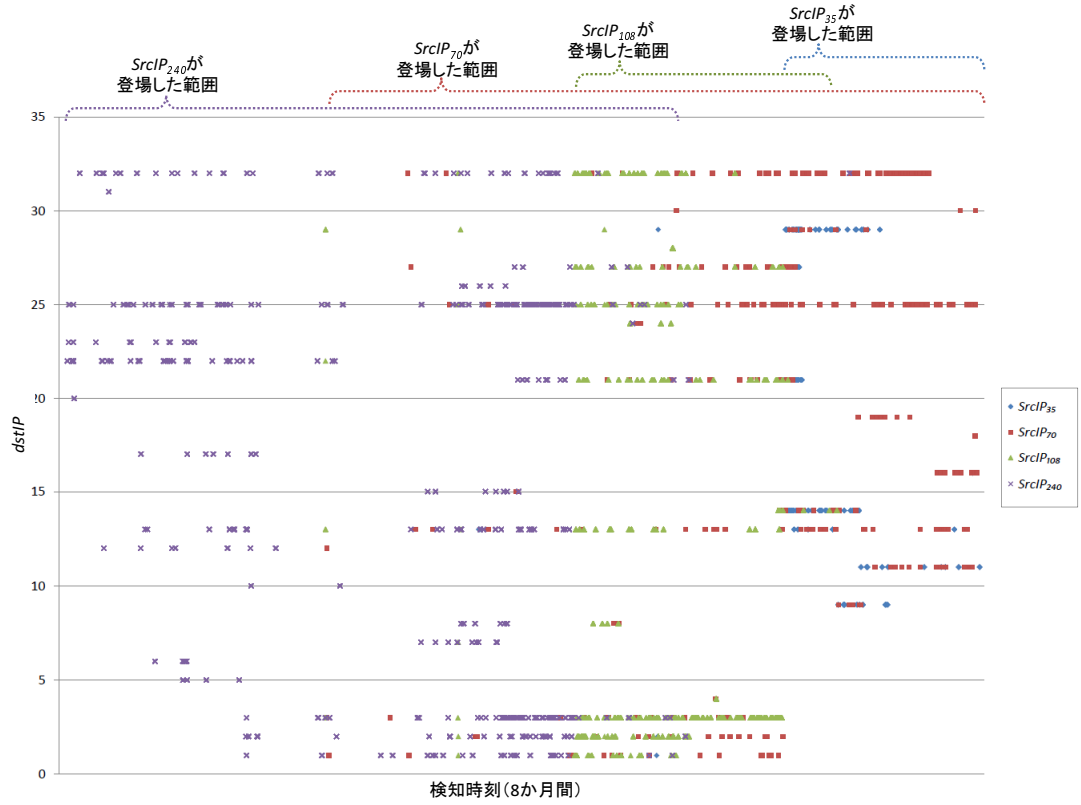

図 4　ブルートフォース攻撃検知時刻と *dstIP* の関係

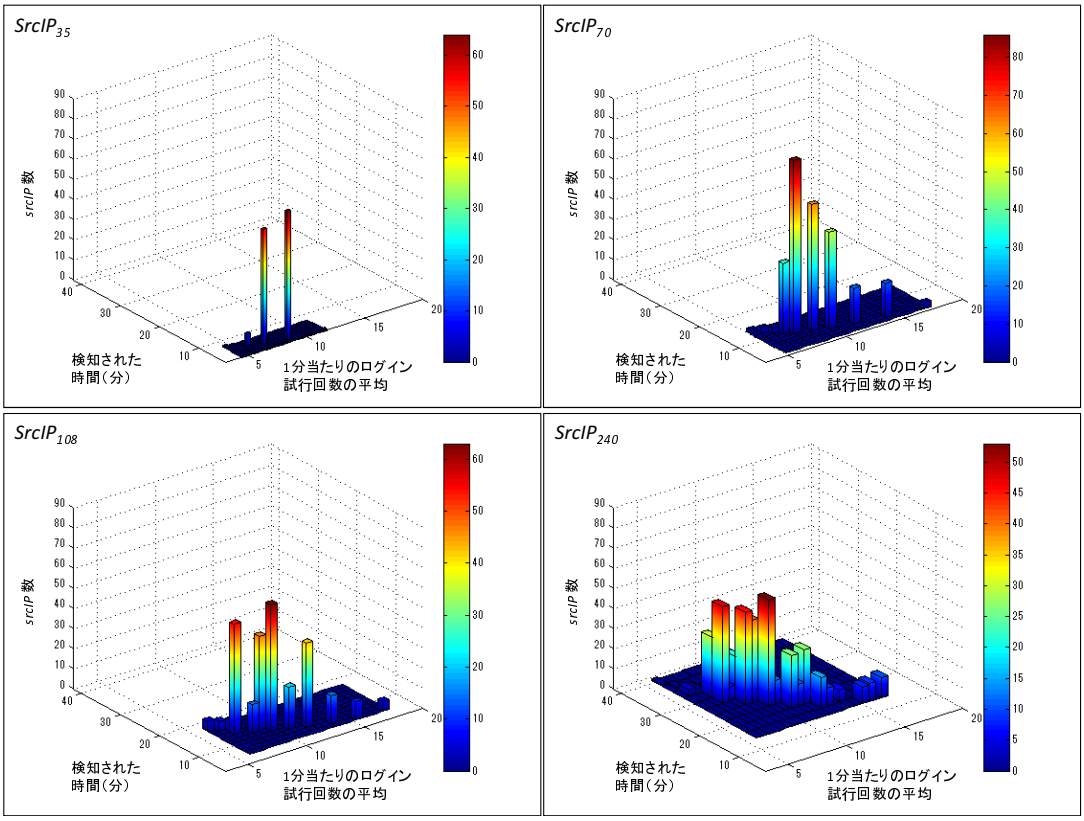

図 5　ログイン試行回数と試行時間の関係

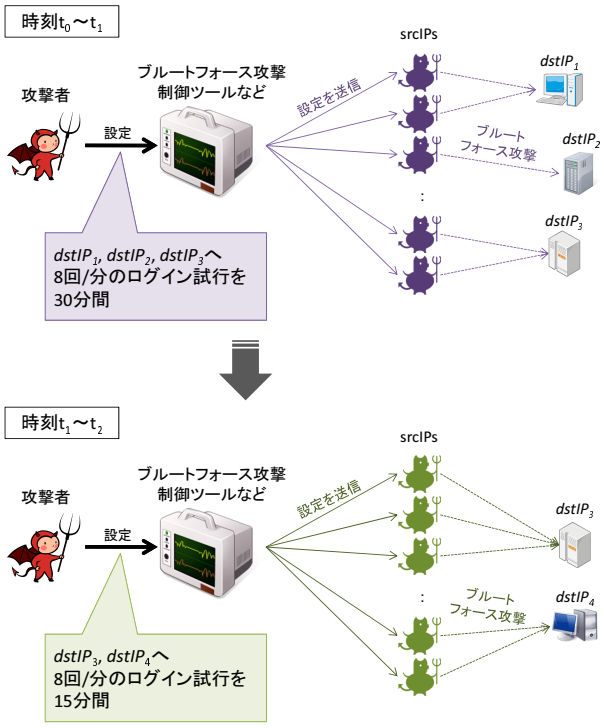

図 6 制御ツールによる分散型 BF の例

の合計に着目すると，240 回，108 回，70 回，35 回はそれぞれ，35 の倍数である 70，105，245 に類似する．1 分当たりのログイン試行回数は $SrcIP_{240}$，$SrcIP_{108}$，$SrcIP_{70}$，$SrcIP_{35}$ の間で大きな差がなく，特定の *dstIP* 群がこれらの *srcIP* によりブルートフォース攻撃を検知され続けていた．これらから，攻撃者はログイン試行を行う期間のみを変更してログイン試行を続けていたことも推測できる．

4. 分散型 BF 被検知 *dstIP* 群の抽出

第 3 章で述べた分散型 BF について，この攻撃の対象となる *dstIP* 群（分散型 BF 被検知 *dstIP* 群ともいう）を IDS ログより抽出することを考える．この分散型 BF では特定の *dstIP* 群が長期間攻撃を検知され続けた．このことから，攻撃の対象となる *dstIP* 群を特定することで，それらの *dstIP* 群についてのみ重点的に監視・対策を行うことができる．そこで，IDS ログを長期間収集することなしに当該 *dstIP* 群を抽出したい．

本章では，[2] にて提案された使い捨て BF を検知した *dstIP* 群を抽出する手法（使い捨て BF 被検知 *dstIP* 群抽出手法ともいう）の適用により分散型 BF を検知した *dstIP* 群の抽出を検討し，適用時の課題を述べる．

4.1 使い捨て BF 被検知 *dstIP* 群抽出手法の適用

分散型 BF 被検知 *dstIP* 群を IDS ログより抽出することにおいて，基本統計量を計測するだけでは当該 *dstIP* 群を抽出することが難しいのは明らかである．また *srcIP* 毎のログイン試行回数合計の分布を計測することで分散型 BF が検知された *srcIP* を抽出し，その情報を用いて *dstIP* 群を抽出することも可能ではある．しかし，長期間収集した大量の IDS ログなしには *srcIP* を抽出することは難しい．

ここで，分散型 BF の特徴を用いることで，長期間 IDS ログを収集することなく，分散型 BF 被検知 *dstIP* 群を抽出することを考える．抽出に利用できそうな特徴として，次の 3 点が挙げられる．

- 1 つの *srcIP* から 1 つの *dstIP* に向けたブルートフォース攻撃が検知される．
- ある *srcIP* からのブルートフォース攻撃は，単位時間当たりのログイン試行回数が同一である．
- ある *srcIP* からのブルートフォース攻撃は，一定期間検知され続ける．

ところで，我々は [2][3][4] にて，使い捨て BF の対策手法を提案している．この提案手法は，IDS ログより使い捨て BF を検知した *dstIP* 群（使い捨て BF 被検知 *dstIP* 群ともいう）を抽出する手法を含む．そこで，この使い捨て BF 被検知 *dstIP* 群抽出手法の適用により，分散型 BF を検知した *dstIP* 群の抽出を検討する．使い捨て BF 被検知 *dstIP* 群抽出手法においても，検知時刻毎のログイン試行回数に着目して相関の高低を計算する処理がある．この処理は先に挙げた分散型 BF の特徴である「ある *srcIP* からのブルートフォース攻撃は単位時間当たりのログイン試行回数が同一で，しかも一定期間検知され続ける」特徴に該当するログを抽出することが可能であると考えられる．

4.2 使い捨て IP によるブルートフォース攻撃（使い捨て BF）

使い捨て IP によるブルートフォース攻撃（使い捨て BF）とは，ある一定期間ごとに異なる *srcIP* から特定の *dstIP* 群へ向けてブルートフォース攻撃が検知されていた事象である．我々は，[2] にて SSH サービスへ向けた使い捨て BF の発生を検知したことを報告している．

使い捨て BF では，例えば時刻 t_1 から t_2 の間では $srcIP_1$ から $dstIP_1$，$dstIP_2$，$dstIP_3$ へ，時刻 t_3 から t_4 の間では $srcIP_2$ から $dstIP_1$，$dstIP_2$，$dstIP_3$ へ，それぞれブルートフォース攻撃が検知される．このように，時刻によって異なる *srcIP* から特定の *dstIP* 群へ向けたブルートフォース攻撃が繰り返し検知されていた．[2][3] にて，使い捨て BF に該当する IDS ログを調査した結果，使い捨て BF に該当する *srcIP* 群の約 80%が 8 ヶ月間の IDS ログに 1 日しか検知されなかったこと，1 分当たりのログイン試行回数の平均は約 17.6 回であったことがわかっている．

4.3 使い捨て BF 被検知 *dstIP* 群抽出手法 [2]

[2] にて提案された使い捨て BF を検知した *dstIP* 群の抽

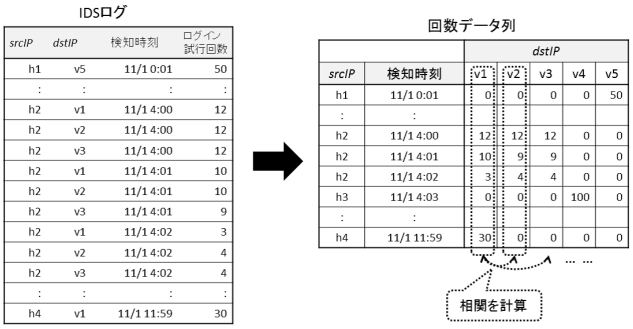

図 7 ログイン試行回数に関する相関の計算

出手法を述べる．この抽出手法では，単位時間に IDS により検知されたブルートフォース攻撃検知ログが持つ次の特徴を利用する．

- ある *srcIP* から複数の *dstIP* へ向けたブルートフォース攻撃が検知される
- 同一の *srcIP* からほぼ同時刻にブルートフォース攻撃が検知される
- 同時刻に同一の *srcIP* から検知されたブルートフォース攻撃におけるログイン試行回数は *dstIP* 間で同一である

これらの特徴を抽出するため，IDS ログから，検知時刻，*srcIP*，*dstP* について，単位時間当たりのログイン試行回数の相関を計算する（図 7）．

まず，IDS ログから，*srcIP* と検知時刻を行，*dstIP* を列とする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．次に，各検知時刻におけるログイン試行回数について，相関が高い *dstIP* 群を求める．そして，得られた *dstIP* 群について，同一の *srcIP*・検知時刻・ログイン試行回数でブルートフォース攻撃が検知されているかを判断する．当該条件に *dstIP* 群が該当するならば，それらを使い捨て BF を検知した *dstIP* 群と判断する．

4.4 使い捨て BF 被検知 *dstIP* 群抽出手法適用における課題

本節では，前節で述べた使い捨て BF 被検知 *dstIP* 群抽出手法の適用による分散型 BF を検知した *dstIP* 群の抽出を検討し，適用時の課題を述べる．

分散型 BF では，使い捨て BF と同様に *srcIP* が使い捨てであり，単位時間当たりのログイン試行回数に規則性がある．そのため，IDS ログから，単位時間当たりのログイン試行回数に関する回数データ列を作成することで，分散型 BF を検知した *dstP* 群を抽出しやすくなる．つまり，回数データ列の作成処理については手法の適用が可能であるといえる．

しかし，分散型 BF では，特定の *dstIP* 群が，同時刻に，ある *srcIP* によるブルートフォース攻撃を検知されない．ある *srcIP* は 1 つの *dstIP* に対してのみブルートフォース攻撃を検知される．つまり，各検知時刻におけるログイン試行回数について相関が高い *dstIP* 群を求めたとしても，分散型 BF では，該当する *dstIP* 群は存在しない．すなわち，分散型 BF を検知した *dstIP* 群を抽出することができない．そのため，分散型 BF を検知した *dstIP* 群を，相関の高低を計算することで抽出できるようなフィールドを IDS ログより選択する必要がある．

5. まとめと今後の課題

本稿では，IDS ログを対象とした拠点間横断分析により，RDP サービスへ向けた，複数の異なる IP アドレスによるブルートフォース攻撃（分散型 BF）を検知した．我々は *srcIP* 毎のログイン試行回数の合計の分布に着目することで，少ないログイン試行回数で一定期間ブルートフォース攻撃が検知された *srcIP* を IDS ログより抽出することができた．この分散型 BF に該当する *srcIP* はブルートフォース攻撃を試みる攻撃者により制御されていた可能性が高いことが推測できる．

また，分散型 BF を検知した *dstIP* 群を IDS ログより，長期間ログを収集せずとも抽出するため，使い捨て BF 抽出手法の適用を検討した．その結果，単位時間当たりのログイン試行回数に関する回数データ列を作成する処理については手法の適用が可能であるものの，分散型 BF を検知した *dstIP* 群の抽出には，相関の計算による抽出に適したフィールドを選択する必要がある．

今後の課題として，分散型 BF 被検知 *dstIP* 群抽出手法の確立が挙げられる．さらに抽出に必要な IDS ログの量を見積もり，*dstIP* 群の抽出精度も評価する必要がある．

参考文献

[1] IPA, ”コンピュータウィルス・不正アクセスの届け出状況［2012 年 6 月分］,” `http://www.ipa.go.jp/security/txt/2012/07outline.html`,2012.

[2] 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 2013(CSS2013), 2013.

[3] 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 2014(SCIS2014), 2014.

[4] S Honda, Y Unno, K Maruhashi, M Takenaka, S Torii, ”Detection of Novel-Type Brute Force Attacks used Ephemeral Springboard IPs as Camouflage,” International Conference on Information and Network Security (ICINS), 2014.

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

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

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

[8] 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 last visited 2013/8/27.

[9] SUCRI Blog, "Mass WordPress Brute Force Attacks?? Myth or Reality," http://blog.sucuri.net/2013/04/mass-wordpress-brute-force-attacks-myth-or-reality.html, last visited 2014/1/30.

[10] PCWorld, "GitHub bans weak passwords after brute-force attack results in compromised accounts," http://www.pcworld.com/article/2065340/github-bans-weak-passwords-after-bruteforce-attack-results-in-compromised-accounts.html, last visited 2014/1/30.

[11] F-Secure, "Windows Remote Desktop Worm "Morto" Spreading - F-Secure Weblog : News from the Lab." http://www.f-secure.com/weblog/archives/00002227.html, last visited 2014/4/8.

[12] Vizvary Martin, Jan Vykopal, Flow-based detection of RDP brute-force attacks, 7th International Conference on Security and Protection of Information (SPI 2013), 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] 竹森敬祐, 三宅優, 中尾康二, "IDS ログ分析支援システムの提案," 情報処理学会研究報告 2003-CSEC-21, 2003.

[16] Kazuyoshi Furukawa, Satoru Shimizu, Masahiko Takenaka, Satoru Torii, "On Detection for Scarcely Collided Super-Slow Port Scannings in IDSs' Log-Data," International Conference on Communications and Network Security 2013 (ICCNS 2013), 2013.