SSH ログインセンサによる STBF(Brute Force attacks with Single Trials) の観測

齊藤 聡美 †　　武仲 正彦 †　　鳥居 悟 †

† 株式会社富士通研究所
211-8588 川崎市中原区上小田中 4-1-1
{sa.satomi,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，IDS（侵入検知システム）だけでは効果的な対策を行うことが難しくなってきている．そのため，単純なログイン試行回数の大小ではなく，ログイン試行そのものに着目しアクセスの特徴を分析することが必要である．我々は，SSH(Secure Shell) を対象とした，ログイン試行分析を目的とするログインセンサを開発した．本センサを世界 7 拠点に設置し，6ヶ月間で約 2800 万件のログイン試行を観測した．さらに，センサに到達したログイン試行から，1 拠点に対し 1 組のユーザ名／パスワードで 1 回のみのログイン試行が断続的に発生する，新しいタイプの攻撃事象（Brute force attacks with Single Trial, STBF）を抽出することができた．

Observing STBF (Brute Force attack with Single Trials) by SSH Login Sensors

Satomi Saito†　　Masahiko Takenaka†　　Satoru Torii†

†FUJITSU LABORATORIES LTD.
1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki 211-8588, JAPAN
{sa.satomi,ma,torii.satoru}@jp.fujitsu.com

Abstract In recent years, it becomes difficult to prevent brute force attacks with only intrusion detection systems (IDS). Therefore, it is important to analyse not only the number of login trials but also habits in login trials. We develop a login sensor for SSH(Secure Shell) in order to analyse features of login trials. We operate the sensors on seven sites around the world and observe about 28 million trials within six months. Furthermore, we extract a novel type of brute force attacks instance, brute force attacks with single trials(STBF). The STBF repeats login trials from unique IP addresses and pairs of user name and passwords with only once.

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巧妙化の一途をたどり，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．これまで我々は，IDS ログの分析により，既存の検知アルゴリズムをすり抜ける意図を持ったブルートフォース攻撃事象の発生を報告してきた．[1] では，ある一定期間毎に異なる IP アドレスから特定のホスト群に向けて，ブルートフォース攻撃が断続的に発生し続ける「IP 使い捨て型

ブルートフォース攻撃」を報告している．我々の観測する限り，この攻撃事象では，攻撃元となったIPアドレスのほぼ全てが一定期間の攻撃にのみ登場した．つまり，IPアドレスを使い捨てるように一定期間にのみ攻撃に割り当てることで，単純なブラックリストによる攻撃の遮断を回避していると推測できる．また，[2] においても，一定期間毎に異なるIPアドレスから，攻撃のタイミングに規則性を有するブルートフォース攻撃の発生を報告している．いずれの攻撃事象でも，ログイン試行回数は従来報告されているものと比較すると非常に少ない回数であった．このように，攻撃元のIPアドレスを頻繁に変更し，1回の攻撃でのログイン試行回数を減少させることで既存のブルートフォース攻撃検知アルゴリズムをすり抜けるように攻撃が変化している．IDSを用いたブルートフォース攻撃の検知は限界に近づきつつある．

これに対し，アクセスそのものの特徴に着目し，実際にサービスを運用しているサーバのアクセスログやハニーポットを用いた分析に関する研究が行われている．例えば [7] では，SSHサーバのアクセスログを分析し分散型のブルートフォース攻撃を検知する手法が提案されている．しかし，この手法では大規模な攻撃の分析が中心であり，IDS等で検知が困難な攻撃の分析は行われていない．ハニーポットを用いた分析では，実際のサービスを模擬するサーバにマルウェア等をわざと侵入させ，侵入後の挙動を観測することができる．ところが，ハニーポットは侵入後の挙動分析が主な目的であるため，ログイン時に用いられたパスワードやログインのタイミングといった侵入時の挙動分析には不適切である．ホスト侵入時のアクセスに着目した分析を行うためには，ログイン試行そのものを観測できる機構が必要である．

そこで我々は，SSH(Secure Shell) を対象とした，ログイン試行の分析を目的とするログインセンサを開発した．このログインセンサは，実際のサービスを運用していないため，正規ユーザのアクセス等のノイズなしに，悪意のあるログイン試行を記録することができる．我々は，本センサを世界7拠点に配置し，ログイン試行を観測した．センサに到達したログイン試行を6か月間観測し，約2800万のログイン試行を観測した．

さらに，センサに到達したログイン試行を分析することにより，1拠点に対し1組のユーザ名／パスワードで1回のみのログイン試行が断続的に発生する新しいタイプの攻撃事象（Brute force attacks with Single Trials, STBF）を抽出することができた．この攻撃は，既存のIDS等での検知が難しいブルートフォース攻撃であり，我々の知る限り，他に類似の報告事例も存在しない．STBFは，1つの試行元IPアドレスからのログイン試行は1回のみであり，正規ユーザによるログイン試行と区別をつけることは困難である．しかし，上述のログイン試行が短期間に集中していたこと，複数拠点にて同様の事象が継続して観測されたこと，ログイン試行元となったIPアドレスの国情報や試行に用いられたユーザ名／パスワードにSTBF間で高い相関があったことから，これらは一連の攻撃であると判断できる．

本稿の貢献は，ログイン試行の分析を目的するログインセンサにより，これまで認識されなかったブルートフォース攻撃事例「STBF (Brute Force attacks wtih Single Trials)」の抽出に成功したことである．このSTBFは，既存のIDSやアクセスログの分析では抽出が難しいという特徴を持つ．そのため，現時点で運用中のサーバが本攻撃の対象となっている可能性は十分に考えられる．

本稿の構成は次の通りである．第2章で，関連技術を紹介する．第3章で，取得したログからSTBF事象を抽出した手順を述べる．第4章で，抽出できたSTBFについてその特徴を分析した結果を報告する．第5章でSTBFを実行する攻撃者について考察を行う．第6章でまとめと今後の課題とする．

2　関連技術・報告

本章では，ブルートフォース攻撃事例の報告や関連技術を紹介する．まず，ブルートフォース攻撃事例として，2013年4月にWordPress（コン

テンツ管理システム）が，同年 11 月に GitHub（ソースコード管理システム）が，どちらも数万の IP アドレスからブルートフォース攻撃を受けていた事例が挙げられる．IBM Tokyo SOC Report[6] でも，2010 年下期，2013 年上期に発行されたレポートにおいて，ブルートフォース攻撃を行う IP アドレスが多数存在することや，1IP アドレスが行うログイン試行回数が減少傾向にあることが報告されている．[7] でも，著者の SSH サーバアクセスログに大量の異なる IP アドレスからブルートフォース攻撃を受けていたことが報告されている．また，こうしたブルートフォース攻撃の激化を受け，Cisco と Level 3 Comunications は 2015 年 4 月に，ブルートフォース攻撃に悪用されているとされる IP アドレス帯に対策を講じたことが報告されている [8].

ハニーポットに関する技術を述べる．ハニーポットは，マルウェア感染などの悪意ある挙動を観測するための囮である．ハニーポットの目的としては，マルウェア検体の収集や悪性 Web サイトの検知，シグネチャ生成などが挙げられる [11][12][13]．例えば，ハニーポットを実際のサービスを模擬するサーバに見せかけ，マルウェアに侵入などさせることで，攻撃手順を観測・分析することができる．他にも [14] では，ハニーポットを内部ネットワークに設置することで内部で発生する攻撃を検知する研究がされている．[17] では，複数箇所に配置されたハニーポットで得られた傾向の比較が報告されている．また，Telnet に対する攻撃を観測するハニーポットも [15] で提案されており，実際にハニーポットに到達したユーザ名／パスワードも報告されている．

一方で，マルウェアによる大規模なスキャンといった，インターネットの傾向を把握するという観点では，ダークネット観測が挙げられる．インターネット上で使われていないホストに到達する通信を観測することで，インターネット上での流行を把握することができる [9][10][16].

さらに近年では，インターネットに接続された機器を能動的にスキャンする事例も増加している．インターネットに接続された機器や機器上で稼働しているソフトウェア等を対象とした検索エンジン SHODAN[18]，機器の脆弱性に関する状況把握を対象としたスキャンを行う Project Sonar[19]，2012 年にインターネットスキャンを行った Carna Botnet[20] が挙げられる．

3 STBF 事象の抽出

本章では，我々が世界 7 拠点に設置したログインセンサから STBF 事象を抽出した手順を述べる．

3.1 設置したログインセンサ

我々が各拠点に設置したログインセンサは，OpenSSH[21] をベースとして開発した．ユーザ数をゼロとし，TCP22 番ポートで通信を待ち受け，到達したログイン試行を記録する．

センサが出力するログの例を表 3.1 に示す．センサに対してログイン試行が発生したとき，ログイン試行元 IP アドレス (*srcIP*)，試行先の拠点名 (*site*)，ログイン試行発生時刻 (*date*)，ログイン試行されたユーザ名 (*usr*) およびパスワード (*passwd*) を 1 つのレコードとして記録する．

表 1: ログインセンサが出力するログの例

srcIP	*site*	*date*	*usr*	*passwd*
x.x.x.x	siteA	10/21 13:00	admin	admin
y.y.y.y	siteB	10/21 14:00	Admin	12345
z.z.z.z	siteC	10/21 14:30	root	qwerty
:	:	:	:	:

3.2 抽出手順

ログインセンサから取得できたログから，次の手順により STBF 事象を抽出した．まず，1 つの *srcIP* から 1 つの *site* に対するログイン試行回数を集計し，STBF の疑いのあるレコードを抽出する．例えば，ある *srcIP* からある *site* に対して 1 回のみログイン試行が記録されたレコードなどである．

次に抽出したレコードに対し，横軸を *date*，縦軸を *user* と *passwd* の組合せとするグラフに

プロットし，ログイン試行が断続的に観測された箇所を目視により抽出し，STBF とした．

3.3 抽出結果

我々が 7 拠点（$Site_1$, $Site_2$, ..., $Site_7$）より取得したログに第 2 章 2 節で述べた手順を適用した．設置したログインセンサより取得できたログの規模を表 3.3 に示す[1]．抽出の結果，4 拠点 ($Site_1$, $Site_2$, $Site_3$, $Site_4$) から STBF 事象を抽出することができた．抽出できた STBF に該当するレコード件数はそれぞれ，$Site_1$ が 1,590 件，$Site_2$ が 621 件，$Site_3$ が 2,149 件，$Site_4$ が 1,839 件であった．

表 3.3 に示したログから抽出できた STBF 事象のグラフのプロット結果を図 1 に示す．プロットが連続し縦線のように見える箇所が STBF に該当する箇所である．これは，ログイン試行が短期間に断続的に発生していたことを示す．縦線の傾きが大きければ，断続的に発生した期間がより長かったことを示す．さらに，複数の縦線間でプロットの縦軸の並び方が共通している．これは，ログイン試行に用いられた *Usr* と *Passwd* の組合せが共通することを示す．この縦線状の箇所を 1 つの STBF が発生した箇所とする．図 1 より，$Site_1$ では 11 の STBF が，$Site_1$ では 4 の STBF が，$Site_1$ では 13 の STBF が，$Site_1$ では 11 の STBF が，それぞれ確認できた．

Site 間に着目すると，特に $Site_1$，$Site_2$，$Site_3$ の間において，いくつかの STBF が同時期に発生したことがわかる．一方で，*Usr* と *Passwd* の組合せで共通していたものは一部のみであるなど，強い相関があるとはいえない．

4 抽出できた STBF の特徴

本章では，前章にて抽出できた STBF 事象についてその特徴を分析した結果を報告する．図 1 上にプロットされたログを対象とし，*srcIP*, *Usr* と *Passwd* の組合せ (*Usr/Passwd*)，*Date* の 3 つの観点から分析を行った．

[1] ログインセンサの観測期間は，2015 年内の 6ヶ月間である．

まず *srcIP* について，抽出したログ全体で *srcIP* が何回ログに記録された回数を数え上げた．出現回数を表 4 に示す．この結果は，ログ中の *srcIP* の約 90%が 1 度しかログイン試行を行わなかったことを示す．観測できた範囲においては，これらの *srcIP* は 1 度ある *site* にログイン試行を行ったきり，他の *site* にもログイン試行を行わなかった．

次に，*srcIP* が持つ国情報について，各 *site* の各 STBF が検知された *srcIP* の国情報の分布を図 2 に示す．ここで，各 STBF に対し，*site* 毎に発生時刻が早い順からラベル付けを行った．図 2 の縦軸はラベル付けした STBF を，横軸は各 STBF のレコード件数を示す．各バーの間隔は STBF の発生時刻に基づく．STBF 全体での計測結果としては，BH(バーレーン)，IN(インド)，BR(ブラジル)，IT(イタリア)，RU(ロシア) が上位 5ヶ国であった．一方，例えば $Site_1$ に着目すると，国情報の分布が 2 度変化している．まず，1-1 から 1-3 では BH, IN, BR が主であるが，1-4 では BH, BR, IT, RU に変化した．さらに，1-5 以降では IN が再び加わり BH, IN, BR, IT, RU が主な *srcIP* の国情報となった．加えて，この傾向の変化は *site* 間でも類似している．

Usr/Passwd について，ログイン試行の対象となった *Usr/Passwd* の STBF 全体での順位と，各 *site* での順位を比較した結果を表 4 に示す．例えば，全体で最も多くログイン試行に使われた *Usr/Passwd* は，$Site_1$, $Site_3$, $Site_4$ も最も多く使われ，$Site_2$ では 26 番目に多く使われていたことを示す．この表から，ログイン試行に使われた *Usr/Passwd* の多くが，$Site_1$, $Site_3$, $Site_4$ でも上位 20 位以内に入っていることが分かる．つまり，ログイン試行された *Usr/Passwd* は *site* 間で共通するといえる．このことは，図 1 にて縦線が横軸にて同じ位置にプロットされていることからもわかる．ログイン試行の対象となった *Usr/Passwd* は，ルータなどのネットワーク機器にデフォルトでログインするための組合せとなっている．

そして，*Date* について，STBF 持続時間と 1 つの STBF におけるログイン試行間の間隔を計

表 2: ログインセンサより取得できたログの規模

	レコード件数 (件)	*srcIP* 異なり数	*Usr* 異なり数	*Passwd* 異なり数
全体	28,424,677	10,905	11,272	1,110,013
$Site_1$	5,566,139	3,674	4,129	875,082
$Site_2$	3,837,898	2,174	1,115	518,155
$Site_3$	4,857,194	4,570	1,461	927,717
$Site_4$	1,921,044	3,226	6,893	127,692
$Site_5$	4,105,351	1,038	8,658	549,762
$Site_6$	4,155,833	1,058	8,265	590,398
$Site_7$	3,981,218	1,311	1,117	802,788

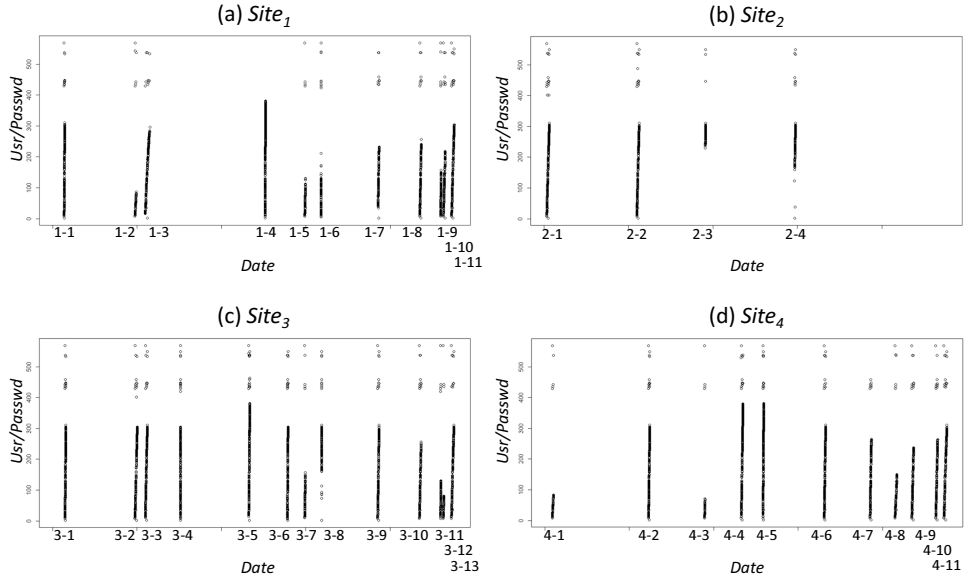

図 1: STBF 事象のグラフのプロット結果

測した．STBF 持続時間を計測した結果を表 4 に示す．持続時間の平均は約 826 分（約 13.8 時間）であるが，持続時間は *site* によって様々であり，持続時間に関して *site* 間での相関は確認できなかった．各 STBF 持続時間とレコード件数を比較した結果を図 3 に示す．この図から，持続時間は *site* のみでなく STBF によって様々であることがわかる．しかも持続時間とレコード件数の関係に着目すると，持続時間とレコード件数の間に相関も見られないことがわかる．

以上の分析結果をまとめると，STBF の特徴として次の 3 点が挙げられる．ここから，STBF は明らかに何らかの意図を持った一連の攻撃事象であるといえる．

- ***srcIP***: 1 つの *srcIP* からは 1 回のログイン試行しか行われないが，*srcIP* の持つ国情報とその遷移は *site* 間に高い相関があった．
- ***Usr/Passwd***: *Usr/Passwd* はネットワーク機器にデフォルトでログインするための組合せが対象となった．しかも各 STBF でログイン対象となった *Usr/Passwd* の多くは共通していた．
- ***Date***: STBF 持続時間は STBF によって

表 3: *srcIP* の出現頻度

出現回数 (回)	*srcIP* の割合 (%)
1	90.15
2	8.34
3	1.22
4	0.29

表 5: STBF 持続時間（分）

	最小	最大	平均
全体	27.8	2755.47	826.08
$Site_1$	27.8	2755.47	832.10
$Site_2$	273.75	1558.2	953.26
$Site_3$	91.98	1506	703.76
$Site_4$	289.47	1787	918.36

様々であり，*site* や STBF で発生したログイン試行の規模との間には関係性は確認できなかった．

5 STBF を実行した攻撃者に関する推測

前章で行った分析とそこから得られた特徴に基づき，STBF の実行手順や実行した攻撃者について推測を行う．

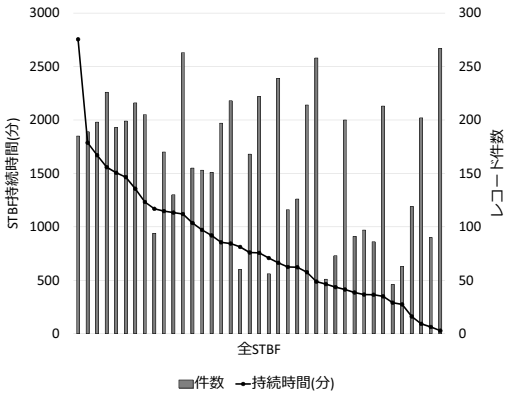

図 3: STBF 持続時間とレコード件数の比較

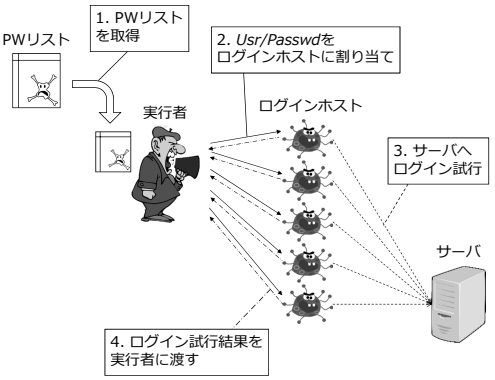

図 4: 推測できる STBF の実行手順

STBF は図 4 に示す手順で実行されると推測される．まず，STBF を実行する攻撃者 (実行者) は，ネットワーク機器のデフォルトパスワードリストといったログイン試行の対象としたい *Usr/Passwd* の組合せ（PW リスト）を取得する．次に，実際にサーバに対してログイン試行を行うためのホスト群（ログイン用ホスト）を用意し，各ログイン用ホストに対し *Usr/Passwd* を 1 組ずつ割り当てる．実行者はログイン用ホストに対し，割り当てられた *Usr/Passwd* でサーバへログイン試行するよう指令を出す．ログイン用ホストはログイン試行を行った結果を実行者に渡す．

次に，PW リストとログイン用ホストの関係について推測する．今回観測された限りでは，STBF 間で *Usr/Passwd* と *srcIP* の国情報の分布やその遷移が共通する．しかし，STBF の発生タイミングや持続時間は STBF によって様々であった．これらのことから，*Usr/Passwd* とログイン用ホストを供給するリソース（ボットネットなど）が紐付けられている可能性が推測できる．例えば何らかの機構により，実行者は PW リストからログイン試行の対象としたい *Usr/Passwd* を指定すると，リソースからランダムにログイン用ホストを取得し，*Usr/Passwd* を 1 組ずつ割り当てるといった流れが推測できる．

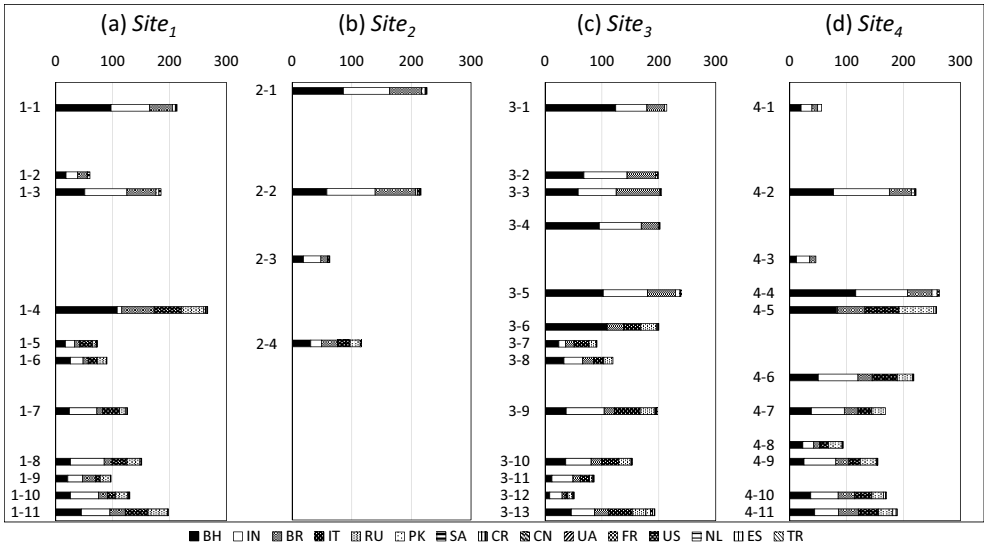

図 2: *srcIP* の国情報の分布

6 まとめ

我々は，SSH を対象に，ログイン試行の分析を目的としたログインセンサを開発し，世界 7 拠点に設置したログインセンサから，6ヶ月間で約 2800 万のログイン試行を観測した．さらに，これらのログイン試行から，1 拠点に対し 1 組のユーザ名／パスワードで 1 回のみのログイン試行が断続的に発生する攻撃事象（Brute force attacks with Single Trial, STBF）を抽出することができた．この攻撃は，我々の知る限り他に類似の報告事例も存在しない新しいタイプの攻撃事象である．しかも既存の IDS ではこの STBF を検知することが難しく，現時点で運用中のサーバが本攻撃の対象となっている可能性は十分に考えられる．

参考文献

[1] 本多, 海野, 丸橋, 武仲, 鳥居, ”拠点横断分析による IP 使い捨て型ブルートフォース攻撃の検知とその抽出手法,” 情報処理学会論文誌 Vol56 No.3, 2015.

[2] S Honda, Y Unno, K Maruhashi, M Takenaka, S Torii, ”TOPASE: Detection of Brute Force Attacks used Disciplined IPs from IDS Log,” 1ST IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT), 2015.

[3] 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,2013.

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

[5] 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, 2013.

[6] IBM Security Services, ”Tokyo SOC Report,” https://www-304.ibm.com/connections/blogs/tokyo-soc/.

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

[8] Cisco Blog, ”Threat Spotlight: SSHPsychos,” http://blogs.cisco.com/security/talos/sshpsychos, 2015.

[9] Qian Wang, Zesheng Chen ; Chao Chen, ”Darknet-Based Inference of Internet Worm Temporal Characteristics,” IEEE Transactions

表 4: *Usr/Passwd* の順位比較

			順位（*site* 毎）			
順位（全体）	レコード件数	*Usr/Passwd*	$Site_1$	$Site_2$	$Site_3$	$Site_4$
1	59	cisco/cisco	1	26	1	1
2	36	administrator/administrator	6	122	6	6
3	35	barbara/barbara	19	197	11	7
4	34	mysql/mysql	15	133	2	31
5	34	emily/emily	44	191	3	15
6	34	anna/anna	17	173	10	24
7	34	nfsnobody/nfsnobody	11	147	23	8
8	33	emma/emma	63	193	12	14
9	33	rk/rk	41	187	19	10
10	33	monitor/monitor	9	127	34	27

on Information Forensics and Security, Volume6, Issue 4, 2011.

[10] 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.

[11] Christian Kreibich, Jon Crowcroft, "Honeycomb: creating intrusion detection signatures using honeypots," ACM SIGCOMM Computer Communication Review, Vol 34 Issue 1, pp51-56, 2004.

[12] Paul Baecher, Markus Koetter, Thorsten Holz, Maximillian Dornseif, Felix Freiling, "The Nepenthes Platform: An Efficient Approach to Collect Malware," 9th International Symposium on Recent Advances in Intrusion Detection (RAID), pp165-184, 2006.

[13] Akiyama Mitsuaki, Makoto Iwamura, and Yuhei Kawakoya. "Design and implementation of high interaction client honeypot for drive-by-download attacks." IEICE Transactions on Communications 93.5 (2010): 1131-1139.

[14] Spitzner, Lance. "Honeypots: Catching the insider threat." Computer Security Applications Conference, 2003. Proceedings. 19th Annual. IEEE, 2003.

[15] Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," 9th USENIX Workshop on Offensive Technologies(WOOT), 2015.

[16] Bailey M, Cooke E, Jahanian F, Nazario J, Watson D, "The Internet Motion Sensor-A Distributed Blackhole Monitoring System." 12th Network and Distributed System Security Symposium(NDSS). 2005.

[17] F. Pouget, M. Dacier, V.H. Pham, "Leurre.com: on the Advantages of Deploying a Large Scale Distributed Honeypot Platform," E-Crime and Computer Conference, 2005.

[18] SHODAN, "SHODAN - Computer Search Engine," `http://www.shodanhq.com/`.

[19] Project Sonar, "Project Sonar by Rapid7," `https://sonar.labs.rapid7.com/`.

[20] Carna Botnet, "Internet Census 2012", `http://internetcensus2012.bitbucket.org/paper.html`.

[21] OpenSSH, `http://www.openssh.com/`.