情報処理学会論文誌 Vol.56 No.3 911–920 (Mar. 2015)

# 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

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

受付日 2014年6月30日, 採録日 2014年9月12日

**概要**：近年，攻撃の発生をネットワークサービス管理者に知られないような手段をともなうブルートフォース攻撃がネットワーク監視組織により報告されている．我々は，実際にサービスを運用しているサーバから取得されたIDS（Intrusion Detection System）ログより，複数の攻撃元IPアドレスによる，検知時刻，ログイン試行回数について拠点間で互いに強い相関を持つブルートフォース攻撃「IP使い捨て型ブルートフォース攻撃（Brute Force Attacks with Ephemeral IPs，*EBF*）」の発生を，我々の知る限り初めて突き止めたので報告する．分析にあたり，複数の拠点から得られたIDSログに対して，拠点ごとに攻撃元として検知されたIPアドレスと検知時刻に着目した可視化を適用することで，既知のブルートフォース攻撃事象だけでなく，*EBF*の検知・分析の起点とすることができる．さらに，IDSログに残る*EBF*の挙動を分析することで，*EBF*を検知されたIPアドレスを，短期間に取得されたIDSログからでも抽出できる手法を提案する．提案手法を実際のIDSログに適用し，*EBF*被検知*DstIP*の抽出に重要なパラメタの評価を行う．

**キーワード**：ネットワーク監視，ログ分析，IDSログ，ブルートフォース攻撃，ネットワークセキュリティ

# Detecting Brute Force Attacks with Ephemeral IPs by Site-traversal Analysis and Its Extracting System

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

Received: June 30, 2014, Accepted: September 12, 2014

***Abstract:*** In recent years, some network monitoring institutes have reported brute force attacks that are hidden for network service administrators. We detect the brute force attacks, *Brute Force Attacks with Ephemeral IPs, EBF*, for the first time as long as we know. In *EBF*, there are strong correlations of multiple source IP addresses, detected date and the number of login trials among detected sites. We analyze our actual IDS log with a viewpoint of site-traversal analysis and apply a novel visualization focused on the relations among source IP addresses, destination IP addresses and detected date. With the knowledge about *EBF*, we propose the method to extract destination IP addresses with small amount of IDS log that were detected brute force attacks included *EBF*. We also evaluate the impact factors of IDS log when applying the method with our actual IDS log.

***Keywords:*** network monitoring, log analysis, IDS log, brute force attacks, network security.

## 1. はじめに

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目的として，存在するすべての組合せについて利用可能かどうかをサービスに対して試す攻撃を指す．たとえば，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．他にも辞書に収録されている単語をユーザ

1 株式会社富士通研究所
FUJITSU LABORATORIES LTD., Kawasaki, Kanagawa 211–8588, Japan
a) honda.satomi@jp.fujitsu.com

© 2015 Information Processing Society of Japan

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呼ばれている）も報告されている [6]．

近年では，攻撃の発生をネットワークサービス管理者に知られないような手段をともなうブルートフォース攻撃が報告されている．たとえば，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複数のネットワーク監視組織より報告されている．専門組織による報告だけではなく，2013 年 4 月にはコンテンツ管理システム「WordPress」が，同年の 11 月にはソースコード管理システム「GitHub」が，どちらも大規模な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．WordPress は 9 万以上のサーバから 100 万回以上のログイン試行を受けていたこと [1], [2] が，GitHub では約 4 万の異なる IP アドレスからログイン試行を受けていたこと [3] がそれぞれ報告されている．

上記のような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い．IDS は通信の挙動等から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．たとえば，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ともなっていたもの等である．一方で，IDS は正規通信を「攻撃」と判断することもありうる（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．この誤検知に対し，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サービス管理者等により設定されている場合も多い．そのため，前述のような複数 IP アドレスかつ少ログイン試行をともなうブルートフォース攻撃の発生を IDS が検知できたとしても，通信の遮断といった対策が適用されない．

本稿では，実際にサービスを運用しているサーバ（拠点ともいう）から取得された IDS ログより，複数の攻撃元 IP アドレスによる，検知時刻，ログイン試行回数について拠点間で互いに強い相関を持つブルートフォース攻撃「IP 使い捨て型ブルートフォース攻撃（Brute Force Attacks with Ephemeral IPs，*EBF*）」の発生を，我々の知る限り初めて突き止めたので報告する．単一の拠点だけでなく，複数の拠点で IDS により検知されたブルートフォース攻撃ログを横断的に分析し，攻撃元として検知された IP アドレスと検知時刻に着目した可視化を適用した．この可視化により，既知のブルートフォース攻撃事象に加えて，複数 IP アドレスが攻撃元となったブルートフォース攻撃が継続して検知されていたことが分かり，この *EBF* の分析の起点とすることができた．

さらに我々は，IDS ログに残る *EBF* の挙動を分析することで，*EBF* が検知された IP アドレスを短期間に取得された IDS ログからでも抽出できる手法を提案する．提案手法ではログイン試行回数の相関に着目し，この攻撃を受け続ける可能性の高い IP アドレスを抽出する．検知した結果を用いることで，抽出した IP アドレスに対する通信を限定して監視することや，ブルートフォース攻撃に関する注意喚起を行うことができる．

提案手法について実際の IDS ログを用いて評価実験を行った．評価の結果，検知時刻とログイン試行回数が抽出精度に大きく影響することが分かった．

本稿の貢献は主に次の 3 つである．

- 拠点横断分析により，使い捨て BF の発生を検知した．
- *EBF* が検知された IP アドレスを短期間に取得された IDS ログからでも抽出できる手法を提案・比較した．
- 我々の持つ IDS ログを手法に適用し，抽出に影響するパラメタの評価を行った．

本稿の構成は次のとおりである．2 章でこれまで報告されてきたブルートフォース攻撃事例，関連技術を紹介する．3 章で拠点横断分析について述べ，拠点間に着目した可視化を IDS ログに対して適用した結果を報告する．4 章で 3 章で検知できた *EBF* について，その特徴を分析した結果を報告する．5 章で *EBF* によるブルートフォース攻撃を検知された IP アドレスを抽出する手法を提案する．6 章で提案手法の評価実験を行った結果を報告する．7 章でまとめとする．

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．IDS ログは IDS レコードの集合から構成される．1 つの IDS レコードは，ある時刻にある *srcIP* からある *dstIP* に対して攻撃の可能性が高い通信を IDS が検知したことを示すデータの集合を示す．IDS レコードは，*srcIP*，*dstIP*，検知時刻，通信先ポート番号，検知した攻撃，検知回数から構成される．IDS がブルートフォース攻撃を検知した場合，IDS レコードの検知回数は IDS がブルートフォース攻撃と判断したログイン試行回数を示す．なお，ブルートフォース攻撃の検知とそのとき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. 関連報告・技術

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発生は，各組織より論文や監視レポート等により報告されている．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

© 2015 Information Processing Society of Japan

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 [7]．Vykopalは，*srcIP*数 : *dstIP*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 [8]．Javedらは文献 [9] で，実際のSSH（Secure Shell）サーバアクセスログを分析し，異なる*srcIP*による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．IBM SOC，SANS，Dragon Research Groupによる監視レポート [10], [11], [12], [13] により，1日に複数の異なる*srcIP*からのブルートフォース攻撃を検知したことが報告されている．また，ブルートフォース攻撃を行う挙動を含むワームの存在も確認されている．Widnowsワークステーションやサーバを狙ったワーム「Morto」は，その挙動にブルートフォース攻撃が含まれることが報告されている [14]．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（Remote Desktop Protocol）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 [15] 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，各組織によりネットワークの監視が行われており，ブルートフォース攻撃事象も報告されている．これらの報告に基づく分析は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ものが主であった．

こうしたブルートフォース攻撃に該当する通信は，短時間に単一のIPアドレスからの通信が大量に発生したり，あるIPアドレスからの通信が長時間続いていたりすることが多い．このような挙動を検知することでブルートフォース攻撃の発生を検知することが可能である．Lazarevicらは，文献 [32] でPoint Anomalies，Contextual Anomalies，Collective Anomalliesの3種類について異常検知技術をあげ，IDSへの適用例を紹介している．ネットワーク監視ログからログの傾向変化を抽出するための分析手法も文献 [16] や [17] 等により提案されている．また，通信元のIPアドレスそのものが攻撃者により用意されたものであるかを判断し，該当するIPアドレスからの通信を遮断する手段も考えられる．現行のIPS製品には，IPアドレスのレピュテーション（評価）機能が搭載されているものも多く（文献 [30], [31] 等），この機能では，たとえば通信元IPアドレスの国情報や各ベンダーが独自にネットワークを監視した結果等から，その通信が不正であるか否かを判断する．しかし，複数のIPアドレスから分散してログイン試行を行ったり，1つのIPアドレスからの長時間続いた通信であっても少ない試行回数でのログイン試行を行うようなブルートフォース攻撃の場合，こうした技術では攻撃の発生を検知することが難しく，また検知できたとしても，誤検知であると判断されることも多い．

複数の拠点での監視・分析の実施例として，NICTのnicter [21] によるダークネットトラフィックの観測や警察庁の@plice [23]，JPCERT/CCのTSUBAME [22] 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．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しDNSサーバを悪用する不正活動の観測・分析を行っている [24], [25]．他にも，ネットワークトラフィック監視・分析に関する研究（文献 [26], [27], [28], [29] 等）も多数発表されている．最近では，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が武仲らにより報告されている [18], [19], [20]．特に文献 [19] 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の発生が報告されている．

そこで複数の拠点で得られたIDSログを分析の対象とすることで，単一の拠点から得られたログや，ネットワークトラフィックだけでは検知することが難しかった攻撃事象の発生を検知することができると考えられる．

## 3. IDSログの拠点横断分析

本章では，ネットワークサービスを実際に運用している複数の拠点から得られたIDSログに対して拠点横断分析に基づく可視化を適用した結果を報告する．拠点横断分析では，次の2項目を満たすような分析方法を適用することが必要である．まず，複数の拠点間でいつ，どのような攻撃が，どの攻撃元から検知されたのかを把握できることが必要である．拠点ごとに分析するのではなく，各拠点で発生した事象を俯瞰することで，分析対象としているネットワーク全体の攻撃傾向を検知することができる．次に，IDSログを構成する項目（フィールド）について，着目すべきフィールドを限定することも必要である．IDSログには複数種類のフィールドが含まれる．顕著に現れる必要最低限のフィールドを分析の対象とすることで，より迅速かつ明確に攻撃事象を検知することができる．

### 3.1 拠点横断分析に基づく可視化

我々は，*srcIP*，*dstIP*，攻撃検知時刻に着目した散布図による可視化をIDSログに対して適用した．*dstIP*を縦軸，検知時刻を横軸として，ブルートフォース攻撃の検知レコードをドットとして描画する．*srcIP*によりドットの色・形が異なる．この散布図により，*srcIP*ごとに，どの*dstIP*に対して，いつ攻撃が検知されたかのかを把握することができる．*srcIP*ごとにドットの色・形を変化させることで，同一あるいは異なる*srcIP*からの攻撃であったのかを区別することができる．

© 2015 Information Processing Society of Japan

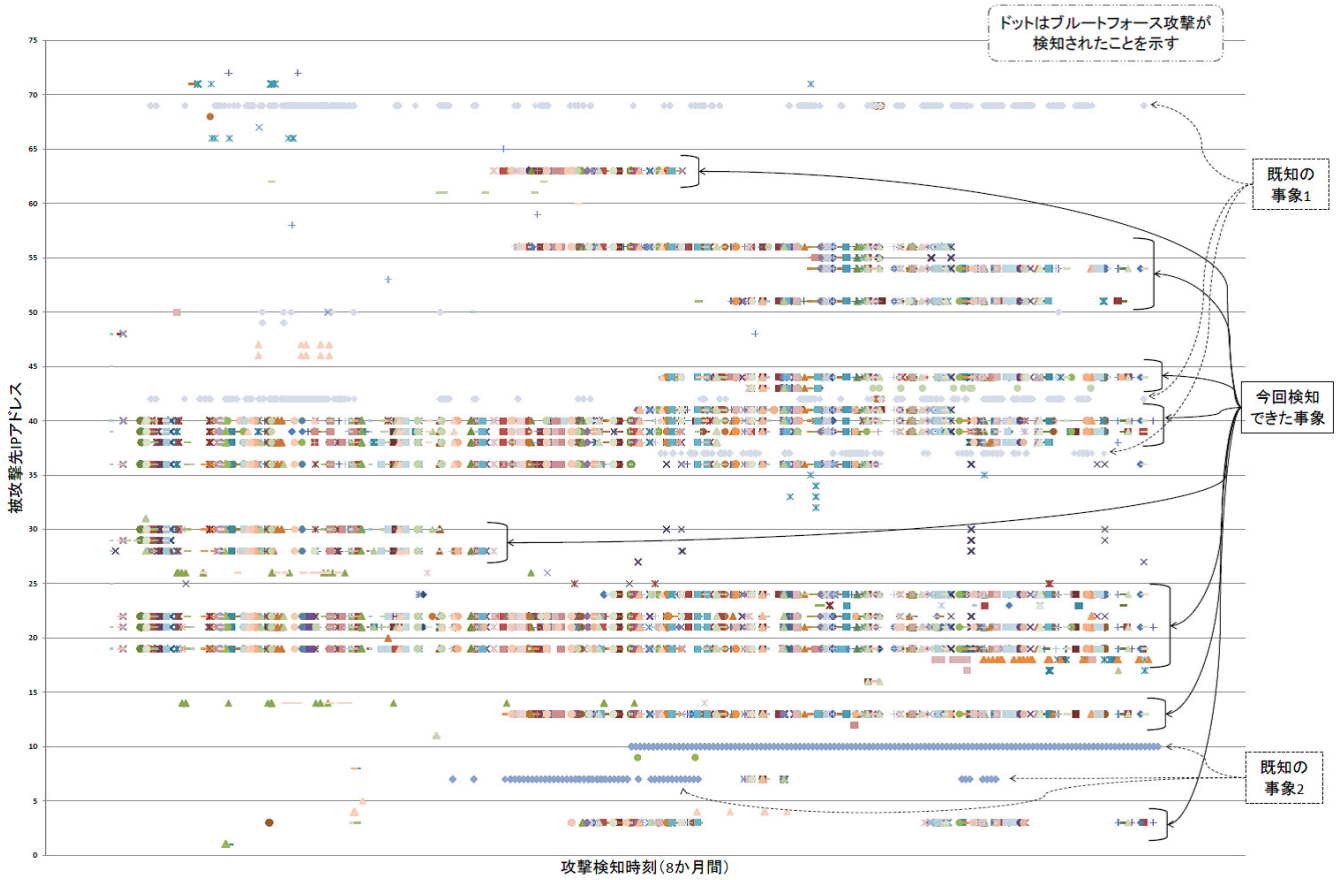



図 1　22 番ポートログの可視化結果
**Fig. 1**　Distribution map in brute force log against port 22.

### 3.2　IDS ログ可視化適用結果

3.1 節で述べた散布図を，2011～2012 年の間に取得された 8 カ月間の IDS ログの，ブルートフォース攻撃を検知した IDS ログに適用した．22 番ポートに対する SSH サービスへ向けたブルートフォース攻撃を検知した IDS ログ（22 番ポートログ）に適用した結果を**図 1** に示す．図 1 から，大きく 3 種類のブルートフォース攻撃検知事象が確認できた．次節で検知事象の詳細を述べる．

### 3.3　確認できたブルートフォース攻撃検知事象

3.1 節で述べた表現を 22 番ポートログに適用した結果，大きく 3 種類のブルートフォース攻撃検知事象が確認できた．1 種類目は，ある 1 つの *srcIP* から複数の *dstIP* 群に対してブルートフォース攻撃が継続して検知されていた事象である．2 種類目も，ある 1 つの *srcIP* から複数の *dstIP* 群に対してブルートフォース攻撃が継続して検知されていた事象であるが，描画されたドットに規則性があり，検知時刻に規則性を持っていた．これら 2 種類のブルートフォース攻撃検知事象は従来知られているブルートフォース攻撃事象である．

3 種類目は，複数の *srcIP* 群から，複数の *dstIP* 群に対してブルートフォース攻撃が継続して検知されていた事象である．しかも，同じ色・形のドットが縦の列に並んで描画されていた特徴から，ある検知時刻におけるブルートフォース攻撃は 1 つの *srcIP* から複数の *dstIP* 群に同時に検知されていたことが分かる．同一の *srcIP* が検知されていない特徴から，この事象を「使い捨て IP によるブルートフォース攻撃（Ephemeral Brute Force Attacks，*EBF*）」と呼ぶ．

## 4.　使い捨て IP によるブルートフォース攻撃（*EBF*）

*EBF* を検知した *dstIP* の集合を *DstIP*，*DstIP* に対する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．*SrcIP* に含まれるある $srcIP_1$ が一定期間 *DstIP* に対してブルートフォース攻撃を検知され続けたとき，検知が開始された時刻を $t_{start}$，検知された最後の時刻を $t_{fin}$ とする．*SrcIP* に含まれる *srcIP* である $srcIP_1$ は，時刻 $t_{start}$ から $t_{fin}$ の間 IDS によりブルートフォース攻撃が検知されていたと表現できる．

### 4.1　*EBF* に関する統計の計測

22 番ポートログから *EBF* に該当するレコードを抽出し，*SrcIP*，ログイン試行回数，検知時刻に関する統計を計測

© 2015 Information Processing Society of Japan

表 1　ログに登場した日数
**Table 1**　Unique *srcIP*s appeared in log (days).

| 登場日数 | *srcIP* 数 |
|---|---|
| 1 | 304(0) |
| 2 | 53(14) |
| 3 | 15(1) |
| 4 | 4(3) |
| 5 | 1(0) |
| 8 | 1(0) |

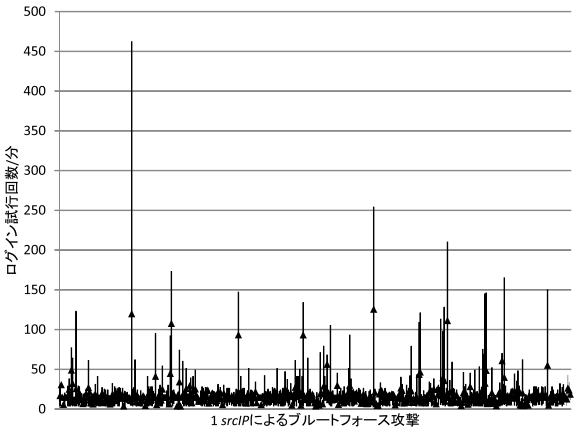



図 2　*srcIP* ごとのログイン試行回数
**Fig. 2**　Number of login trials per *srcIP*.

した．

まず *SrcIP* に関して，*SrcIP* に含まれる 1 つの *srcIP* は，一定期間ブルートフォース攻撃を検知された後は，再度同じ *srcIP* が検知されることがほとんどなかった．ブルートフォース攻撃攻撃が検知された約 1〜2 カ月に同じ *srcIP* が登場したケースはあったものの，そのような *srcIP* はごくわずかであった．

*srcIP* が IDS ログに登場した日数の集計結果を**表 1** に示す．*srcIP* 数の括弧内の数字は日付をまたいでいた *srcIP* 数を示す．約 80%の *srcIP* が約 8 カ月間の中で 1 日しか登場していなかった．5 日，8 日登場した *srcIP* について日付に規則性はなかった．

次にログイン試行回数について，1 つの *srcIP* における $t_{start}$ から $t_{fin}$ の間に検知されたブルートフォース攻撃における検知時刻におけるログイン試行回数の最小値・最大値・平均を**図 2** に示す．検知時刻の最小単位は 1 分である．横軸は 1 つの *srcIP* によるブルートフォース攻撃を，縦軸はログイン試行回数を示す．線分の上側の終端がログイン試行回数の最大値，下側の終端が最小値，三角が平均をそれぞれ示す．分析対象の IDS ログ全体のログイン試行回数の平均が約 72.18 回であったことと比較するとログイン試行回数が少ないことが分かる．

検知時刻に関して，ある 1 つの *srcIP* から *DstIP* に対してほぼ同じ時刻でブルートフォース攻撃が検知されていた．*dstIP* によっては，1 分間のみブルートフォース攻撃が検知されたものもあれば，数時間検知され続けたものもあった．*SrcIP* に含まれる *srcIP* によるブルートフォース攻撃が検知された時間の分布を**図 3** に示す．データ区間を 30 分とし，0〜1,440 分の範囲について作成した縦軸は該当する *srcIP* の数を示す．ヒストグラムの山は左側に偏っており，攻撃の約 9 割は 3 時間以内に終了していた．

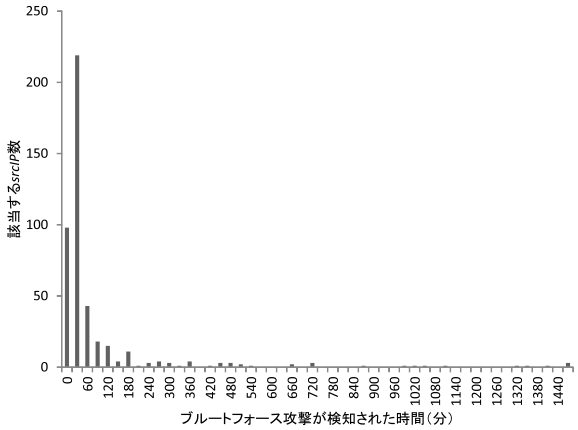



図 3　30 分ごと，0〜1,440 分における攻撃検知時間の分布
**Fig. 3**　Distribution in detected period (every 30 minutes, the range from 0 to 1,440 minutes).

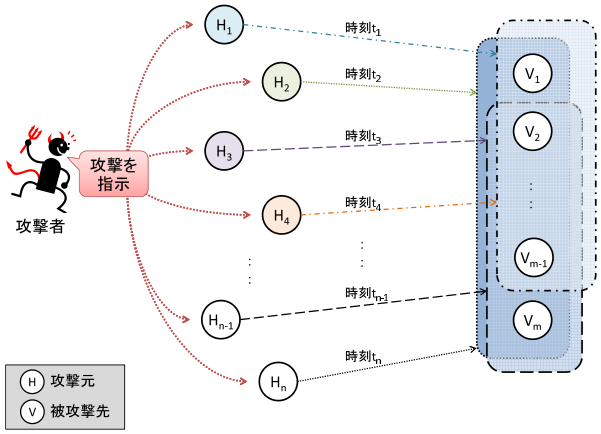



図 4　*EBF* の挙動に関する推測
**Fig. 4**　Suspected structure of *EBF* behavior.

### 4.2　*EBF* の挙動に関する推測

以上から，*EBF* の挙動に関して次の 3 点が推測できる（**図 4**）．

- ブルートフォース攻撃の発生をサービス管理者から隠ぺいするため，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．
- *DstIP* 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 *SrcIP* 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，あるいは自身の身元を隠すために，*SrcIP* に含まれる *srcIP* を使い捨てながらブルートフォース攻撃を行い続けていた．

© 2015 Information Processing Society of Japan

## 5. *EBF* 被検知 *DstIP* の抽出

本章では，*EBF* に該当するブルートフォース攻撃を検知された *dstIP* 群（*EBF* 被検知 *DstIP*）を IDS ログから抽出することで，早期に *EBF* 被検知 *DstIP* を検知する手法を検討する．*EBF* 被検知 *DstIP* は，長期間 *EBF* によるブルートフォース攻撃を検知され続けていた．早期に *dstIP* を抽出することで，抽出した *dstIP* に対する通信を限定して監視することや，ブルートフォース攻撃に関する注意喚起を行うことができる．

### 5.1 利用できる挙動と検討対象とする抽出手法

*SrcIP* に含まれる 1 つの *srcIP* によるブルートフォース攻撃の挙動を利用して IDS ログを分析することで，*DstIP* に該当する *dstIP* 群を抽出することができる．分析に利用できる挙動として，次の 3 つがあげられる．これらの挙動が IDS ログ中に存在するかを分析することで，該当するレコードから *dstIP* 群を抽出する．

a) ある 1 つの *srcIP* から複数の *dstIP* 群（*DstIP*）へブルートフォース攻撃が検知される．
b) 同じ *srcIP* からは同一の時刻にブルートフォース攻撃が検知される．
c) 同じ *srcIP*，同じ時刻に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同一である．

抽出手法として，本稿では次の 3 種類の手法を検討対象とする．

#### 5.1.1 抽出手法 1：*srcIP*，*dstIP*，検知時刻，ログイン試行回数の相関を計算

挙動 a)，b)，c) *srcIP*，*dstIP*，ある時刻に検知された単位時間当たりのログイン試行回数について互いに相関が高い *dstIP* 群を抽出する．入力は *srcIP*，*dstIP*，検知時刻，ログイン試行回数をフィールドとして持つ IDS ログである．入力された IDS ログから，*srcIP*，検知時刻におけるログイン試行回数について互いに相関が高い *dstIP* 群を抽出する．

抽出された *dstIP* 群はいずれも，同じ時刻に，同じ *srcIP* から，同じログイン試行回数によるブルートフォース攻撃を検知された特徴を持つ．しかし IDS の検知アルゴリズム等により，異なる時刻やログイン試行回数で検知された場合，この抽出手法 1 では *dstIP* 群を正確に抽出できない可能性もある．

#### 5.1.2 抽出手法 2：*srcIP*，*dstIP* の相関を計算

*srcIP*，*dstIP* について互いに相関が高い *dstIP* 群を抽出する．入力は *srcIP*，*dstIP* をフィールドとして持つ IDS ログである．入力された IDS ログから，*dstIP* ごとに，各 *srcIP* からブルートフォース攻撃を検知された回数を数え上げる．各 *srcIP* からのブルートフォース攻撃を検知された回数について互いに相関が高い *dstIP* 群を抽出する．

抽出された *dstIP* 群はいずれも，同じ *srcIP* からブルートフォース攻撃を検知された特徴を持つ．しかし抽出手法 2 では，抽出された *dstIP* 群が検知されたログイン試行回数の相関を考慮することができない．

#### 5.1.3 抽出手法 3：*dstIP*，検知時刻，ログイン試行回数の相関を計算

*dstIP*，ある時刻に検知された単位時間当たりのログイン試行回数について互いに相関が高い *dstIP* 群を抽出する．入力は *dstIP*，検知時刻，ログイン試行回数をフィールドとして持つ IDS ログである．入力された IDS ログから，検知時刻におけるログイン試行回数について互いに相関が高い *dstIP* 群を抽出する．

抽出された *dstIP* 群はいずれも，同じ検知時刻に同じログイン試行回数によるブルートフォース攻撃を検知された性質を持つ．しかし抽出手法 3 では，抽出された *dstIP* 群が検知された *srcIP* が同一であったか否かを考慮することができない．

### 5.2 処理の流れ

抽出手法の処理の流れを示す．まず，入力された IDS ログから，*dstIP* を行とする 2 次元データ列を作成する．2 次元データ列の行はそれぞれ，抽出手法 1 では *srcIP* と検知時刻，抽出手法 2 では *srcIP*，抽出手法 3 では検知時刻である．データ列中の数値はそれぞれ，抽出手法 1 では *srcIP* と検知時刻におけるログイン試行回数，抽出手法 2 では *srcIP* における IDS ログ中のレコード件数，抽出手法 3 では検知時刻におけるログイン試行回数である．

次に，作成された 2 次元データ列中の各行をデータ列と見なし，相関の高低を計算することで，互いに相関が高い *dstIP* 群を計算する．互いに相関が高い *dstIP* 群を *DstIP* として出力する．

各抽出手法の処理において作成される 2 次元データ列の例を図 **5** に示す．

## 6. *EBF* 被検知 *DstIP* 抽出手法の比較

本章では，5 章で述べた *EBF* 被検知 *DstIP* 抽出手法を比較するため，我々の所持する IDS ログに対して適用し，*EBF* 被検知 *DstIP* の抽出精度を比較した．抽出精度を次の 2 点から評価した．

- **抽出正確性**：*EBF* 被検知 *DstIP* を誤検知あるいは見逃しなく正確に抽出できること．
- **抽出安定性**：手法の入力となる IDS ログに依存せずに *EBF* 被検知 *DstIP* を抽出できること．

相関係数のしきい値を変化させ抽出手法 1，抽出手法 2，抽出手法 3 を適用し，*EBF* 被検知 *DstIP* の抽出精度を比較した．

© 2015 Information Processing Society of Japan

抽出手法1

| ログイン試行回数 | | $dstIP_1$ | $dstIP_2$ | $dstIP_3$ | $dstIP_4$ | … |
|---|---|---|---|---|---|---|
| $srcIP_1$ | 1/1 0:00 | 10 | 10 | 10 | 0 | … |
| | 1/1 0:01 | 11 | 10 | 9 | 0 | … |
| | 1/1 0:02 | 13 | 12 | 12 | 0 | … |
| $srcIP_2$ | 1/1 0:00 | 0 | 0 | 5 | 5 | … |
| | 1/2 2:01 | 0 | 0 | 0 | 3 | … |
| : | : | : | : | : | : | … |

抽出手法2

| レコード件数 | $dstIP_1$ | $dstIP_2$ | $dstIP_3$ | $dstIP_4$ | … |
|---|---|---|---|---|---|
| $srcIP_1$ | 3 | 3 | 3 | 0 | … |
| $srcIP_2$ | 0 | 0 | 1 | 2 | … |
| $srcIP_3$ | 10 | 10 | 10 | 0 | … |
| $srcIP_4$ | 5 | 5 | 5 | 0 | … |
| $srcIP_5$ | 0 | 0 | 0 | 20 | … |
| : | : | : | : | : | … |

抽出手法3

| ログイン試行回数 | $dstIP_1$ | $dstIP_2$ | $dstIP_3$ | $dstIP_4$ | … |
|---|---|---|---|---|---|
| 1/1 0:00 | 10 | 10 | 15 | 5 | … |
| 1/1 0:01 | 11 | 10 | 9 | 0 | … |
| 1/1 0:02 | 13 | 12 | 12 | 0 | … |
| 1/1 0:03 | 0 | 0 | 20 | 0 | … |
| 1/1 0:04 | 0 | 0 | 0 | 3 | … |
| : | : | : | : | : | … |

**図 5** 抽出手法の処理により作成された 2 次元データ列の例
**Fig. 5** Examples tables created in *EBF* extraction.

### 6.1 比較手順

実際の運用時には 1 日に 3 回抽出手法を適用することで *EBF* 被検知 *DstIP* の有無を調査することを想定し，ある 8 時間の間に検知されたレコード（レコード集合）を各抽出手法の入力である IDS ログとした．2011〜2012 年の 8 カ月間に取得された，*EBF* が検知された 22 番ポートに対する SSH へ向けたブルートフォース攻撃検知ログに含まれるレコードから，無作為抽出により 100 のレコード集合を作成し，各抽出手法に適用した．作成されたレコード集合に含まれるレコード件数は，最小で 2 件，最大で 3,371 件，平均が 436.37 件であった．

5.2 節に述べた処理の流れに沿って，相関係数のしきい値を 0.1 から 0.9 まで 0.1 ずつ増加させながら 100 のレコード集合に対して 3 種類の抽出手法を適用し，*DstIP* を抽出した．なお，レコード集合における検知時刻は 2 分単位とした．なお，相関の計算には，ピアソンの相関係数を用いて，データ列 $\{x_i\}$，$\{y_i\}$ の相関係数を次式により計算した．$\overline{x}$，$\overline{y}$ はそれぞれデータ列 $\{x_i\}$，$\{y_i\}$ の平均を示す．

$$\frac{\sum_{i=1}^{n}(x_i-\overline{x})(y_i-\overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\overline{x})^2}\sqrt{\sum_{i=1}^{n}(y_i-\overline{y})^2}}$$

また，互いに相関が高い *DstIP* は最大クリークを抽出する手法（文献 [33]）を用いて抽出した．*dstIP* をノード，相関の高い *dstIP* のペアをノードどうしがエッジで結ばれていると見なし，最大クリークに該当する *dstIP* 群を抽出した．

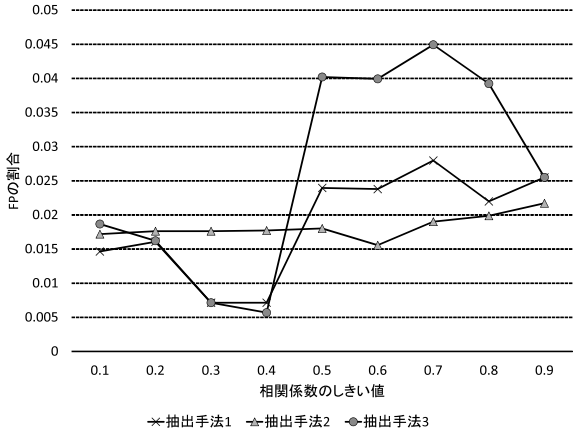



**図 6** FP 平均変化
**Fig. 6** Comparison in FP average.

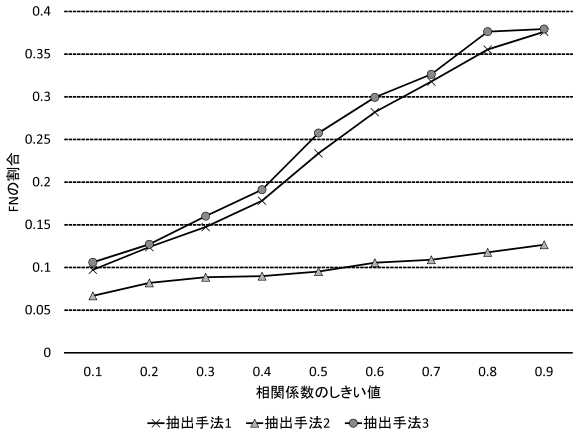



**図 7** FN 平均変化
**Fig. 7** Comparison in FN average.

5 章で統計の計測のために抽出されたレコードに基づき *EBF* 被検知 *DstIP* を作成し，各抽出手法により抽出できた *DstIP* と比較した．*DstIP* の誤検知の割合（False Positive, FP），見逃しの割合（False Negative，FN）を計算した．FP は *EBF* 被検知 *DstIP* に該当しないものの，手法により *EBF* 被検知 *DstIP* と判断された攻撃の割合を示す．FN は *EBF* 被検知 *DstIP* に該当するものの，手法により *EBF* 被検知 *DstIP* と判断されなかった攻撃の割合を示す．

### 6.2 比較結果

しきい値ごとの FP，FN の平均を折れ線グラフとしてそれぞれ**図 6**，**図 7** に示す．FP においては，抽出手法 1 はしきい値を 0.3 あるいは 0.4 に，抽出手法 2 はしきい値を 0.6 に，抽出手法 3 はしきい値を 0.4 にそれぞれ設定したとき，小さい FP で *EBF* 被検知 *DstIP* を抽出することができた．FN においては，どの抽出手法においてもしきい値を 0.1 に設定したとき，小さい FN で *EBF* 被検知 *DstIP* を抽出することができた．グラフの変化から，抽出手法 1・3 と比較し

© 2015 Information Processing Society of Japan

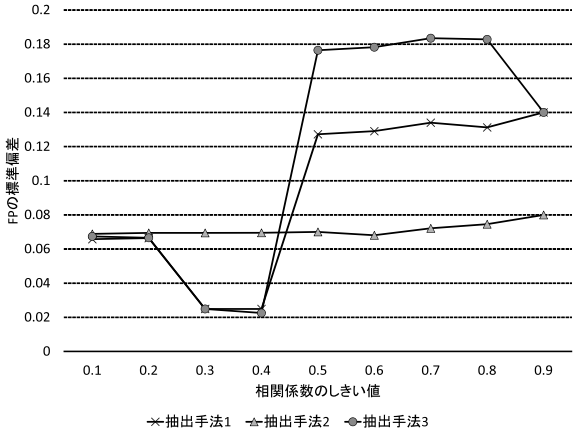



図 8 FP 標準偏差変化
**Fig. 8** Comparison in FP standard deviation.

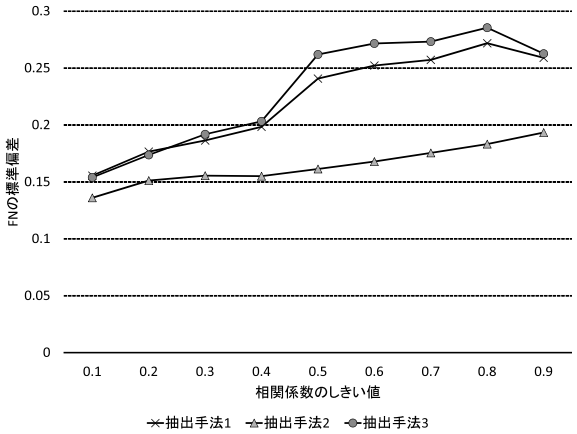



図 9 FN 標準偏差変化
**Fig. 9** Comparison in FN standard deviation.

て，抽出手法 2 では相関係数のしきい値が大きくなっても FP，FN に大きな差が確認できず，どのしきい値を設定した場合においても低い FP・FN で *EBF* 被検知 *DstIP* を抽出することができた．一方で，検知時刻におけるログイン試行回数を考慮した抽出手法 1・抽出手法 3 では低い FP・FN で *EBF* 被検知 *DstIP* を抽出することが難しかった．また，抽出手法 1 と抽出手法 3 の場合における FP，FN の変化が類似しており，検知時刻におけるログイン試行回数を考慮することで FP・FN に大きな差が出ることが分かる．

次に，しきい値ごとの FP，FN の標準偏差を折れ線グラフとしてそれぞれ**図 8**，**図 9** に示す．標準偏差が大きいほど，各レコード集合における FP，FN のばらつきが大きいことを示す．グラフの変化から，抽出手法 1・3 と比較すると，抽出手法 2 ではどのしきい値を設定した場合においても，どのレコード集合に対しても変わらない FP・FN で *EBF* 被検知 *DstIP* を抽出することができた．一方で，抽出手法 1・3 を適用した場合は，設定するしきい値の値によっては FP の標準偏差の値が大きい場合もあり，FP の値のばらつきが大きかったことが分かる．

### 6.3 考察

以上の結果から，抽出正確性，抽出安定性の 2 点から 3 種類の抽出手法を評価する．相関係数のしきい値を変化させた場合において，いかなるしきい値を設定した場合でも，小さい FP 平均，FN 平均で *EBF* 被検知 *DstIP* を検知できた抽出手法を「抽出正確性を満たす」とし，いかなるしきい値を設定した場合でも，小さい FP 標準偏差，FN 標準偏差で *EBF* 被検知 *DstIP* を検知できた抽出手法を「抽出安定性を満たす」とする．図 6〜図 9 より，抽出手法 2 が相関係数のしきい値を変化させた場合において抽出正確性と抽出安定性の両方を満たす．

検知時刻，ログイン試行回数の抽出手法への影響を考察する．3 種類の抽出手法を適用した結果，抽出手法 1 と抽出手法 3 は図 6〜図 9 のいずれのグラフにおいても，グラフの変化が類似していた．これらのことから，検知時刻とログイン試行回数が FP・FN の低下に大きく影響していた．理由として，*EBF* に該当するブルートフォース攻撃であっても，検知されたログイン試行回数や検知時刻が，IDS の検知アルゴリズムや *dstIP* が割り当てられているサーバの設定によって *dstIP* ごとに異なる検知時刻・ログイン試行回数が検知された可能性が考えられる．そのため，今回の実験では，検知時刻とログイン試行回数のどちらも考慮しなかった抽出手法 2 が 3 種類の中で抽出正確性，抽出安定性を最も満たす手法であると判断された．もしも，*EBF* 被検知 *DstIP* を IDS ログより抽出するには，検知時刻とログイン試行回数について値の切り下げ・切り上げ等の処理を適用する必要がある．

## 7. まとめ

本稿では，サービスを実際に運用している複数の拠点から得られた IDS ログに対して，拠点横断分析に基づく可視化を適用した結果，既知のブルートフォース攻撃事象に加えて，複数 IP アドレスが攻撃元となり少ログイン試行回数をともなうブルートフォース攻撃事象（*EBF*）を検知することができた．*EBF* が持つ挙動を利用して IDS ログを分析することで，*EBF* が検知された *DstIP* を IDS ログから抽出することができる．評価実験の結果，検知時刻とログイン試行回数が *EBF* 被検知 *DstIP* の抽出精度に大きく影響することが分かった．

### 参考文献

[1] SUCRI Blog: Mass WordPress Brute Force Attacks?? Myth or Reality (2013), available from ⟨http://blog.sucuri.net/2013/04/mass-wordpress-brute-force-attacks-myth-or-reality.html⟩.
[2] SUCRI Blog: The WordPress Brute Force Attack Timeline (2013), available from ⟨http://blog.sucuri.net/2013/04/the-wordpress-brute-force-attack-timeline.html⟩.
[3] PCWorld: GitHub bans weak passwords after brute-

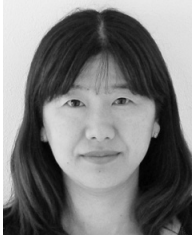
© 2015 Information Processing Society of Japan

force attack results in compromised accounts (2013), available from ⟨http://www.pcworld.com/article/2065340/github-bans-weak-passwords-after-bruteforce-attack-results-in-compromised-accounts.html⟩.
[4] US-CERT: Risks of Default Passwords on the Internet (2013), available from ⟨http://www.us-cert.gov/ncas/alerts/TA13-175A⟩.
[5] Ars Technica: Mass-login attack on Nintendo fan site hijacks 24,000 account (2013), available from ⟨http://arstechnica.com/security/2013/07/mass-login-attack-on-nintendo-fan-site-hijacks-24000-accounts/⟩.
[6] 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］(2012), available from ⟨http://www.ipa.go.jp/security/txt/2012/07outline.html⟩.
[7] Sperotto, A., Sadre, R., de Boer, P.-T. and Pras, A.: Hidden Markov Model modeling of SSH brute-force attacks, *International Workshop on Distributed Systems: Operations and Management 2009* (*DSOM 2009*): Integrated Management of Systems, Services, Processes and People in IT, pp.164–176 (2009).
[8] Vykopal, J.: A Flow-Level Taxonomy and Prevalence of Brute Force Attacks, *American Control Conference 2011* (*ACC 2011*), Part II, pp.666–675 (2011).
[9] Javed, M. and Paxson, V.: Detecting Stealthy, Distributed SSH Bruteforcing, *2013 ACM SIGSAC Conference on Computer & Communications Security*, pp.85–96 (2013).
[10] SANS Internet Storm Center: ISC Diary — Distributed SSH Brute Force Attempts on the rise again (2010), available from ⟨https://isc.sans.edu/diary/Distributed+SSH+Brute+Force+Attempts+on+the+rise+again/9031⟩.
[11] Dragon Research Group: SSH Brute Force Attack Source Insight (2011-04-29) (2011), available from ⟨http://www.dragonresearchgroup.org/2011/04/29/⟩.
[12] IBM：Tokyo SOC Report 2010 年下期 (2010)，入手先 ⟨https://www-304.ibm.com/connections/blogs/tokyo-soc/⟩.
[13] IBM：Tokyo SOC Report 2013 年上期 (2010)，入手先 ⟨https://www-304.ibm.com/connections/blogs/tokyo-soc/⟩.
[14] F-Secure: Windows Remote Desktop Worm “Morto” Spreading — F-Secure Weblog: News from the Lab, available from ⟨http://www.f-secure.com/weblog/archives/00002227.html⟩ (accessed 2014-04-08).
[15] Martin, V. and Vykopal, J.: Flow-based detection of RDP brute-force attacks, *7th International Conference on Security and Protection of Information* (*SPI 2013*) (2013).
[16] 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).
[17] 仲小路博史，寺田真敏：周波数分析に基づくインシデント傾向検知手法に関する検討，情報処理学会研究報告 2005-CSEC-30 (2005).
[18] 武仲正彦，鳥居　悟，清水　聡：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).
[19] 武仲正彦，鳥居　悟，古川和快，清水　聡：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).
[20] Furukawa, K., Shimizu, S., Takenaka, M. and Torii, S.: On detect for Scarcely Collided Super-Slow Port Scannings in IDSs' Log-Data, *International Conference on Communications and Network Security 2013* (*ICCNS 2013*) (2013).
[21] Inoue, D., Eto, M., Yoshioka, K., Baba, S., Suzuki, K., Nakazato, J., Ohtaka, K. and Nakao, K.: nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis, *WOMBAT Workshop on Information Security Threats Data Collection and Sharing*, pp.58–66 (2008).
[22] 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），入手先 ⟨http://www.jpcert.or.jp/tsubame/⟩.
[23] 警察庁セキュリティポータルサイト@police — インターネット定点観測，入手先 ⟨http://www.npa.go.jp/cyberpolice/detect/observation.html⟩.
[24] 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).
[25] 牧田大佑，吉岡克成，松本　勉，中里純二，島村隼平，井上大介：DNS アンプ攻撃の早期対策を目的とした DNS ハニーポットとダークネットの突合分析，暗号と情報セキュリティシンポジウム（SCIS2014）(2014).
[26] Zou, C.C., Gao, L., Gong, W. and Towsley, D.: Monitoring and early warning for internet worms, *ACM Conference on Computer and Communications Security* (*CCS*), pp.190–199 (2003).
[27] Yegneswaran, V., Barford, P. and Plonka, D.: On the Design and Use of Internet Sinks for Network Abuse Monitoring, *7th International Symposium on Recent Advances in Intrusion Detection*（*RAID*) (2004).
[28] Bailey, M., Cooke, E., Jahanian, F., Nazario, J. and Watson, D.: The Internet Motion Sensor: A Distributed Blackhole Monitoring System, *Network and Distributed Security Symposium* (*NDSS*) (2005).
[29] Zhou, C.V., Leckie, C. and Karunasekera, S.: A Survey of coodinated attacks and collaborative intrusion detect, *Computer & Security on ELSEVIER*, pp.124–140 (2010).
[30] McAfee: McAfee Network Security Platform, available from ⟨http://www.mcafee.com/japan/enterprise/nsp/⟩.
[31] Cisco Systems: Cisco IPS, available from ⟨http://www.cisco.com/web/JP/product/hs/security/ids4200/index.html⟩.
[32] Lazarevic, A., Banerjee, A., Chandola, V., Kumar, V., Srivastava, J.: Data Mining for Anomaly detect, *Tutorial at the European Conference on Principles and Practice of Knowledge Discovery in Databases* (2008).
[33] Makino, K. and Uno, T.; New Algorithms for Enumerating All Maximal Cliques, *9th Scandinavian Workshop on Algorithm Theory* (2004).

**本多 聡美**　（正会員）

2010 年横浜国立大学工学部電子情報工学科早期卒業．2012 年同大学大学院環境情報学府情報メディア環境学専攻情報メディア学コース博士課程前期修了．同年富士通株式会社および株式会社富士通研究所入社．現在，ソーシャルイノベーション研究所セキュアコンピューティング研究部に所属し，ネットワークセキュリティの研究に従事．2009 年度電気学会電気学術女性活動奨励賞受賞．

© 2015 Information Processing Society of Japan



**海野 由紀**　（正会員）

1999 年富士通株式会社入社．ネットワーク管理製品の企画・開発に従事．2004 年株式会社富士通研究所に異動．現在，ソーシャルイノベーション研究所，セキュアコンピューティング研究部に所属．アプリケーションセキュリティ，ネットワークセキュリティの研究開発を経て，サイバーセキュリティの研究開発に従事．

**丸橋 弘治**

1997 年京都大学理学部卒業．1999 年同大学大学院理学研究科生物科学専攻修士課程修了．同年富士通株式会社入社．2002 年株式会社富士通研究所に異動．現在，ソーシャルイノベーション研究所ナレッジプラットフォーム研究部に所属し，異常検知等のデータマイニング研究に従事．2014 年筑波大学大学院システム情報工学研究科コンピュータサイエンス専攻博士後期課程修了．博士（工学）．

**武仲 正彦**

1990 年大阪大学工学部電気工学科卒業．1992 年同大学大学院工学研究科博士前期課程修了．2009 年筑波大学大学院システム情報工学研究科博士後期課程修了．博士（工学）．1992 年より富士通株式会社および株式会社富士通研究所に勤務，現在，セキュアコンピューティング研究部長．情報セキュリティ，暗号実装の研究に従事．2005 年電気科学技術奨励賞受賞．2014 年情報処理学会喜安記念業績賞受賞．電子情報通信学会，デジタル・フォレンジック研究会各会員．

**鳥居 悟**　（正会員）

1985 年東京理科大学卒業．同年株式会社富士通研究所入社．現在，ソーシャルイノベーション研究所セキュアコンピューティング研究部主管研究員．並列処理系やオペレーティングシステムの研究開発を経て，現在，ネットワークセキュリティの研究開発に従事．情報処理学会理事（2012～2013 年度）．

© 2015 Information Processing Society of Japan