Vol.2015-IOT-31 No.8
Vol.2015-SPT-15 No.8
2015/9/25

関西大学におけるSSHアクセスの収集と分析

中田 恭平[1]　吉井 章[1]　坂本 要[2]　小林 孝史[2]

概要：リモートログインは遠隔地の計算機資源を有効活用するために必要不可欠になっている．リモートログインで一般的に使用されているプロトコルとしてSSHが挙げられる．しかし，一度でも認証に成功すると正規・非正規ユーザに関わらず通信が可能であることから，攻撃者の標的にもなっている．そのためSSHはセキュリティを考慮した方針に基づいて運用するとともに，日頃からログを監視する必要がある．そこで，本稿では研究室で所有する関西大学のグローバルIPアドレスを持つサーバに対して行われたSSHのログを分析する．そのログから日時，IPアドレスやその発信元の国，使用されたユーザ名などを抽出し，攻撃者の特徴を分析する．さらにSSHハニーポットを設置して，攻撃者の活動やその手法を観察する．これら関西大学宛に行われたSSHアクセスの分析結果を報告する．

キーワード：ネットワークセキュリティ，OpenSSH，SSHハニーポット

Analysis of SSH Access on Kansai University

Abstract: The remote login is essential to take advantage of computer resources deployed at remote locations. SSH is the protocol which is generally used by the remote login. But it may be targeted in attackers because who can connect to computer if only to make authentication succeed for once. Accordingly, providing SSH service should carry out with the rigorous security rules and it is always necessary to monitor access attempts logs. We analyzed attacker's features by analyzing attacker's access attempted date, IP address, hosted country and user name from access attempt log which attempted to IP address assigned to Kansai University. Moreover, we had observed attacker's activity and strategy by setting up honeypot. In this paper, we report the results of experimental and analysis.

Keywords: Network Security，OpenSSH，SSH Honeypot

1. はじめに

近年，コンピュータなどの情報通信技術の発展に伴い利便性の向上や業務の効率化が図られており，クラウドコンピューティングに代表されるような新たな形態のサービスが生み出された．しかし，利便性が向上する一方で，不正アクセスや個人情報の漏洩といったセキュリティインシデントは増加の一途を辿っている [1]．

その一つとしてSSHサーバで発生するセキュリティインシデントがある．SSHサーバで発生するインシデントは認証に成功すると誰でも計算機を操作可能という特徴によって発生する．例えば，パスワードの流出や総当たり攻撃によって正規ユーザのアカウントに対してSSHサーバへの不正アクセスが行われて，他のサーバへの攻撃の踏み台として悪用されることがある．さらにSSHサーバ自体やイントラネット内サーバの不適切な設定によって，不正アクセスによる被害がインターネットに直接公開していないサーバに対して拡大する恐れもある．2015年3月12日に国立情報学研究所で報告された事例では，研究系公開サーバに不正アクセスを許した結果，他のサーバへの辞書攻撃の踏み台とされていた [2]．この事例はSSHサーバのアクセス制御が行われておらず広範囲からアクセス可能であったこと，アカウントの管理が不十分で退職者のアカウントが不正アクセスに利用されたことが原因であった．

そのためSSHサービスはセキュリティを考慮した方針に基づいて運用するとともに，日頃からログを監視する必要がある．そこで，本研究では関西大学が保有するグローバルIPアドレスのうち，小林研究室で割り当てられたグ

[1] 関西大学大学院総合情報学研究科
[2] 関西大学総合情報学部

ローバル IP アドレスを持つ SSH サーバに対して行われたアクセスログを分析する．そのログから日時，IP アドレスやその発信元の国，使用されたユーザ名などを抽出し，攻撃者の特徴を分析する．これら関西大学宛に行われた SSH アクセスの分析結果を報告する．

2. 関連研究

佐藤らの研究 [3] では，筑波大学のネットワークで使用されていないサブネットにハニーポットを設置してアクセス情報を収集した．池部らの研究 [4] では，ダークネット宛のパケットの多くは不正な活動に起因していることに着目し，大分大学が所有する IP アドレスの中でダークネットに相当する IP アドレス空間にハニーポットを設置して通信状況を分析した．

佐藤ら，池部らの研究は組織内で使用されていないネットワークセグメントに対して，Honeyd を利用してネットワークセグメントのエミュレートを行いアクセスを収集している．本研究では使用できる IP アドレスに限りがあるため，小林研究室で実際に運用している SSH サービスの IP アドレスと SSH サービスとして提供していない IP アドレスへのアクセスを収集する．

3. SSH アクセスの収集方法

本章では SSH アクセスを収集した関西大学のネットワーク環境と，OpenSSH および SSH ハニーポットによるログの収集手法について述べる．

3.1 関西大学のネットワーク環境

本研究では，小林研究室が使用している関西大学の IP アドレスが割り当てられた 3 台のサーバを対象とする．これらのサーバの中で二つを公開 SSH サービス，一つを SSH ハニーポットとして公開している．

3.2 OpenSSH によるログ収集

本研究では，インターネットから研究室のサーバへの SSH サービスを提供するために OpenSSH[5] を使用している．OpenSSH は利用環境に応じて様々な認証方式を利用できる．本研究では，認証方式を以下の二つの方法に限定している．

- パスワード認証
- 公開鍵認証

この二つの認証方式に限定することで SSH サーバとしての必要を満たし，出力されるログに類似性を持たせられる．ログに類似性を持たせることでシェルスクリプトを用いたログの整形を容易にできる．例として，図 **1** にパスワード認証，あるいは公開鍵認証を用いて認証したログの一部を示す．この形式でログを出力することで認証の成否や使用されたユーザ名，アクセス元の IP アドレスを得ることができる．また認証の成否を Accepted，Failed，Invalid の三つの状態に分類している．Accepted とは，サーバに登録されているユーザ名で認証に成功した状態と定義する．Failed とは，サーバに登録されているユーザ名で認証に失敗した状態と定義する．Invalid とは，サーバに登録されていないユーザ名で認証に失敗した状態と定義する．

```
Accepted publickey for root from 10.xx.xx.xx port 56234
Accepted password for root from 10.xx.xx.xx port 52143
Failed password for root from 10.xx.xx.xx port 35071
Failed password for invalid user a from 10.xx.xx.xx port 40961
```

図 **1** OpenSSH によるログの例

本研究では OpenSSH による認証に関してログから日時，認証の成否，使用されたユーザ名，アクセス元 IP アドレスおよびアクセス元のポート番号を抽出する．さらにアクセス元の IP アドレスは GeoIP[6] のデータベースで照合し，アクセス元の国名を取得する．これらの情報をデータベースに格納して管理する．

3.3 SSH ハニーポットによるログ収集

SSH ハニーポットは cowrie[7] を用いて構築した．cowrie はオープンソースの SSH ハニーポットである Kippo[8] を基に開発が進められている．cowrie は SSH のエミュレートに特化したハニーポットであり，認証時に入力したパスワードやユーザ名を収集することができる．特に入力したパスワードを記録することができる点が SSH アクセスを収集して分析する上で OpenSSH より優れている．さらにアクセス者に認証を成功させるとエミュレートされたシェルが提供され，そのシェル上で入力されたコマンドを記録することができる．

本研究では，外部から SSH ハニーポットに対して TCP/22 番ポートへの通信を受け取ると，NAT 機器によって cowrie を稼働させているポートに通信を転送する設定を施している．そしてエミュレートされた環境で認証の成功を許さず，アクセスを試行した者が入力したユーザ名，パスワードおよびアクセス元の IP アドレスを収集する．さらにアクセス元 IP のアドレスは GeoIP のデータベースで照合し，アクセス元の国名を求める．これらの情報をデータベースに格納して管理する．

4. ログ分析

前章で示した手法で収集した OpenSSH および SSH ハニーポットのログを分析した結果を本章で述べる．

4.1 OpenSSH のログ分析

OpenSSH で収集したログは 2014 年 10 月 1 日から 2015 年 8 月 14 日までの約 10 か月の期間を対象とする．この期間の一部で停電やメンテナンスによりサーバを停止させる

表 1　OpenSSH サーバへのアクセス元 IP アドレスの上位 15 件

IP アドレス	国名	Accepted	Failed	Invalid
58.218.211.166	China	0	180548	0
43.255.190.115	Hong Kong	0	165891	0
43.255.190.186	Hong Kong	0	134297	0
43.255.190.191	Hong Kong	0	130722	0
218.65.30.92	China	0	108306	0
222.186.134.89	China	0	105069	0
43.255.190.137	Hong Kong	0	97318	0
43.255.190.171	Hong Kong	0	96239	0
115.231.218.130	China	0	89200	0
43.255.190.189	Hong Kong	0	88445	0
43.255.190.121	Hong Kong	0	87459	0
43.229.52.188	Hong Kong	0	85410	0
218.65.30.61	China	0	85082	0
58.218.204.226	China	0	84828	0
182.100.67.112	China	0	83418	0

表 2　OpenSSH サーバへのアクセス元 IP アドレスが属する国の上位 15 件

国名	Accepted	Failed	Invalid	ユーザ名種類数
China	0	5149197	71695	4206
Hong Kong	0	3192725	539	109
France	0	80462	921	71
United States	0	16693	33526	741
India	0	32900	2920	618
South Korea	0	17933	2179	167
Ecuador	0	4261	15805	1513
Brazil	0	15341	4608	1217
Poland	0	10923	3518	441
Singapore	0	627	8404	1339
Germany	1	3738	4416	181
Netherlands	1	1390	6285	1421
Japan	3018	1423	2837	163
Turkey	0	5559	1543	88
Uganda	0	5566	865	63

必要があり，ログを収集していない期間が存在する．また認証が集中し，SSH サーバへのセッションの許容数を超えたアクセスもログを収集していない．

4.1.1　OpenSSH のログ概要

図 **2** に期間内に収集した SSH サーバへの認証試行数の推移を示す．認証試行数とは，OpenSSH サーバへ認証を試行し，図 1 で例示した形式のログが出力された回数である．期間内における総認証試行数は 8,755,808 回，Accepted は 5,677 回，Failed は 8,560,686 回，Invalid は 189,445 回であった．Accepted と Invalid の認証試行数は Failed と比較して少ないため，図 2 上では確認できない．認証を試行した IP アドレスの総数は 5,396 個，認証を試行した IP アドレスが属する国の総数は 106 の国と地域，使用されたユーザ名の総数は 11,599 種類であった．

表 3　OpenSSH サーバで使用されたユーザ名の上位 15 件

ユーザ名	Accepted	Failed	Invalid	使用した国数
root	0	8551353	0	100
admin	0	0	46293	82
ubnt	0	0	6326	83
test	0	0	5037	75
guest	0	0	5037	73
nagios	0	0	4873	44
piress	0	0	4788	1
user	0	0	4165	66
PlcmSpIp	0	0	3444	64
support	0	0	3009	71
pi	0	0	2813	67
oracle	0	0	2704	64
ftp	0	1460	1155	52
ftpuser	0	0	2229	67
xbian	0	0	1762	54

4.1.2　アクセス元 IP アドレスの分析

表 **1** に期間内で SSH サーバに対して認証を試行した IP アドレスの上位 15 件を示す．表 1 に挙げた IP アドレスによる認証試行には三つの特徴があった．第一に全てユーザ名 root に対する総当たり攻撃を行っていた．なお，ユーザ名 root は SSH サーバに存在するユーザ名であるので Failed に計数している．第二にアクセス元 IP アドレスの属する国が Hong Kong を含む China に集中していた．第三に認証試行を一度に集中して行うだけではなく，期間を空けて何日も行っていた．以上のことにより，表 1 における認証試行数が多いアクセス元 IP アドレスは管理者権限の奪取を目的とした総当たり攻撃を行っていたことがわかる．

表 **2** に期間内に SSH サーバに対して認証を試行した IP アドレスが属する国の上位 15 件を示す．認証を試行した IP アドレスが属する国の割合は約 59.6%を China，約 36.5%を Hong Kong で占めていた．ユーザ名に対する総当たり攻撃を最も試行していた国は China で，使用されたユーザ名は 4,206 種類であった．また日本国外から認証に成功したアクセスがあったが，不正アクセスではなく正規のユーザがプロキシサーバを経由して認証したものであった．以上のことにより，Hong Kong を含む China による認証試行は Invalid より Failed に分類されることが多く，ユーザ名の総当たり攻撃よりも管理者権限を有するユーザ名に対するパスワードの総当たり攻撃が多いと考えられる．

4.1.3　使用されたユーザ名の分析

表 **3** に期間内に SSH サーバで認証に使用されたユーザ名の上位 15 件を示す．最も認証に用いられたユーザ名は root で，認証を試行した IP アドレスが属する国は 100 の国と地域であった．また管理者権限を有していると考えられるユーザ名の admin やサービス名を表す nagios，oracle，ftp なども認証に使用されていた．これはユーザ名の総当

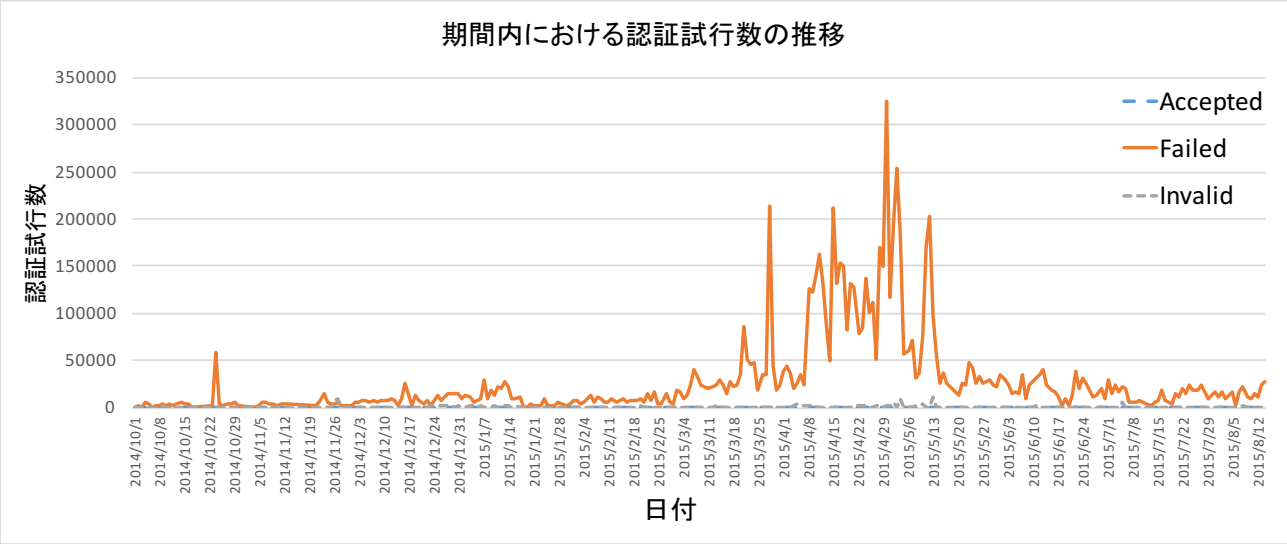

図 2　期間内における OpenSSH サーバへの認証試行数の推移

表 4　SSH ハニーポットへのアクセス元 IP アドレスの上位 15 件

IP アドレス	国	認証試行数	セッション数
43.255.189.44	Hong Kong	81171	27705
43.229.52.212	Hong Kong	63776	21355
43.229.52.167	Hong Kong	27165	9090
43.229.52.68	Hong Kong	24892	8333
113.195.145.70	China	19789	6618
218.65.30.61	China	18549	6221
43.229.52.27	Hong Kong	17395	5822
218.87.111.116	China	17018	5725
146.185.146.230	Netherlands	16128	8065
218.87.111.108	China	14805	4958
218.65.30.23	China	13259	4454
218.87.111.110	China	13150	4411
113.195.145.12	China	12768	4271
218.87.111.107	China	12663	4248
43.229.52.164	Hong Kong	12592	4219

表 6　SSH ハニーポットで使用されたユーザ名の上位 15 件

ユーザ名	認証試行数	パスワードとの組合せ数
root	1072993	138348
admin	4169	1498
ubnt	1358	36
test	799	213
guest	706	77
mysql	656	595
pi	606	6
postgres	536	231
user	471	75
support	339	38
logintest	334	333
PlcmSpIp	302	4
xbian	244	2
oracle	220	51
root/1q2w3e,.	205	6

表 7　SSH ハニーポットで使用されたパスワードの上位 15 件

パスワード	認証試行数	ユーザ名との組合せ数
wubao	2611	1
jiamima	2595	1
admin	2397	30
123456	2362	206
1234	1915	39
12345	1905	40
password	1891	86
root	1735	15
ubnt	1570	8
(入力なし)	1523	12
raspberry	1515	8
default	1452	9
12345678	1269	22
a	1214	880
1234567	1195	25

たり攻撃を行うリストの中に表 3 で示したユーザ名が掲載されていると推測される．なおユーザ名の ftp で Failed と Invalid で計数されているのは，本研究で対象とした SSH サーバのうち 1 台に ftp ユーザが存在しているためである．

4.2　SSH ハニーポットのログ分析

2015 年 5 月 14 日から 2015 年 8 月 14 日までの約 3 か月のログを対象とする．この期間の一部でメンテナンスによりサーバを停止させる必要があり，ログを収集していない期間が存在する．

4.2.1　SSH ハニーポットのログ概要

図 3 に期間内の SSH ハニーポットにおける認証試行数とセッション数の推移を示す．認証試行数とは，SSH ハニーポットにセッションを張り，パスワードの入力を試行した回数を表す．セッション数とは，SSH ハニーポットに接続してから通信を遮断するまでの処理の回数を表す．

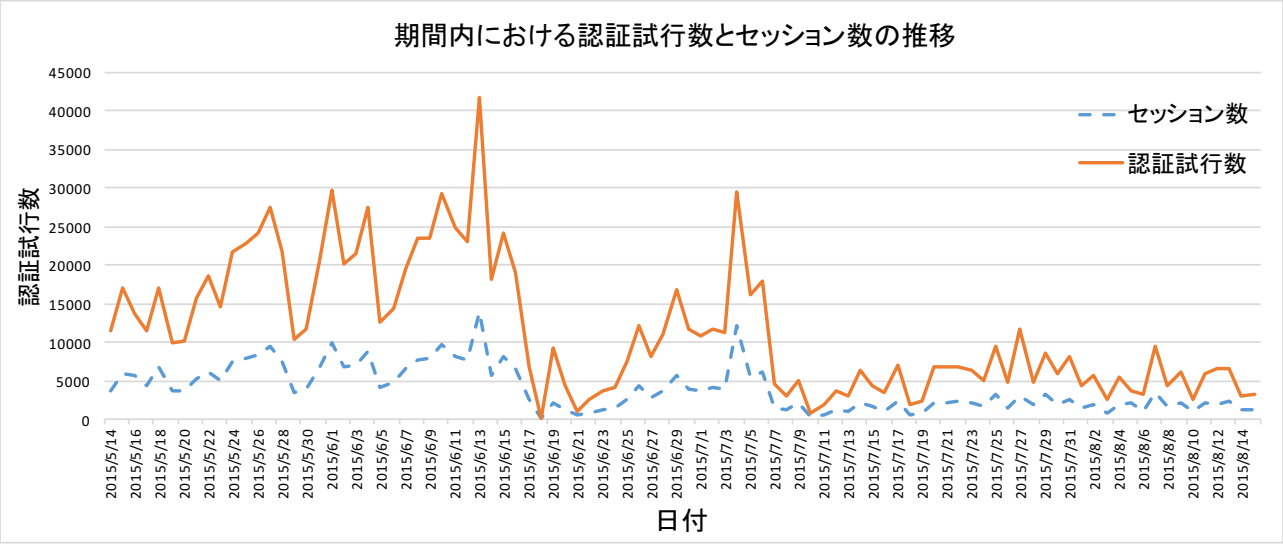

図 3　期間内における SSH ハニーポットへの認証試行数の推移

表 5　SSH ハニーポットへのアクセス元 IP アドレスが属する国の上位 15 件

国名	認証試行数	セッション数	ユーザ名種類数	パスワード種類数
Hong Kong	564837	189274	373	112819
China	507857	171425	3059	68723
Netherlands	16573	8503	4770	6022
United States	7605	4470	179	3464
India	1868	1807	85	599
Germany	1335	1307	68	732
Korea, Republic of	1322	992	98	452
Brazil	1121	961	229	391
Russian Federation	877	563	56	243
Chile	704	704	65	617
Turkey	672	344	29	307
Seychelles	641	31	3	124
Poland	477	469	20	382
Japan	469	135	21	355
Thailand	436	436	31	48

期間内における総認証試行数は 1,107,990 回，総セッション数は 385,281 回であった．使用されたユーザ名の総数は 7,474 種類，使用されたパスワードの総数は 112,055 種類，認証を試行した IP アドレスの総数は 1,715 個であった．

4.2.2　アクセス元 IP アドレスの分析

表 4 に期間内で SSH ハニーポットに認証を試行した IP アドレスの上位 15 件を示す．表 4 で挙げた IP アドレスの特徴として，期間を空けて何度も認証を試行する傾向があった．特に Hong Kong を含む China から認証を試行する IP アドレスは，数日にわたり認証を試行していた．Hong Kong を含む China 以外からの認証を試行する IP アドレスは，数日に分けて認証を試行を行うのはなく，一度だけ認証を試行して後は使用されない傾向があった．

表 5 に SSH ハニーポットに認証を試行した IP アドレスが属する国の上位 15 件を示す．Hong Kong を含む China からの認証試行数は総認証試行数の約 96%を占めており，セッション数も総セッション数の約 94%を占めている．Hong Kong からの認証試行の特徴として，使用されたユーザ名の種類に対してパスワードの種類が多い点が挙げられる．またユーザ名の総当たり攻撃を試行するよりも，管理者権限を有しているユーザ名に対するパスワードの総当たり攻撃を試行する傾向が見られた．

4.2.3　使用されたユーザ名の分析

表 6 に期間内に SSH ハニーポットで使用されたユーザ名の上位 15 件を示す．最も使用されたユーザ名は root で 1,072,993 回計数した．これは総認証試行数のおよそ 96%を占めており，サーバに登録されているユーザ名の中で最も高い権限を有しているユーザ名が不正アクセスの標的にされていることを示唆している．

4.2.4　使用されたパスワードの分析

表 7 に期間内に SSH ハニーポットで使用されたパスワードの上位 15 件を示す．パスワードはユーザ名とは異なり

突出して使用されたものを観測していない．またパスワードの wubao，jiamima はユーザ名 root と組合せで使用されていた．これらのパスワードを Internet Storm Center[9] が公開している SSH に関する情報と照合すると，両者とも使用されていることが報告されていた．またこれらのパスワードを使用した IP アドレスが属する国は China であることから，中国語に関するフレーズとしてパスワードリストに含まれていると推測される．

5. おわりに

本研究では，関西大学の IP アドレスに対して行われた SSH アクセスについて調査した．その結果，香港を含む中華人民共和国からの認証試行が多く，管理者権限の奪取を目的とした総当たり攻撃が行われていることがわかった．

しかし，SSH アクセスを観測する対象とした IP アドレスが少ないため，実際に関西大学に対して行われた SSH アクセスを正確に観測しているとは言い切れない．そのため，取り扱う関西大学の IP アドレスを増やし，SSH アクセスを収集する観測範囲を増加させる必要がある．SSH アクセスを観測する手段として OpenSSH を使用したが，OpenSSH はセッションを張ることができないとログを出力できず，正確な認証試行数を観測したとは言えない．また，SSH ハニーポットを使用したが，エミュレートされたシェルへの接続を許さずに OpenSSH と同等の認証機構のみを利用したことにより，アクセス者の認証後の行動を記録できず，不正アクセス後の行動を観測することができていない．

今後の課題として，より SSH ハニーポットを活用して攻撃者による不正アクセスの振る舞いを観測できる SSH アクセスの収集システムを開発する必要がある．

参考文献

[1] 独立行政法人情報処理推進機構 (IPA)：情報セキュリティ白書 2014，独立行政法人情報処理推進機構 (IPA) (2014).
[2] 国立情報学研究所：研究系公開サーバへの不正アクセスについて，(オンライン)，入手先 <http://www.nii.ac.jp/news/2014/0312/> (参照 2015-08-24).
[3] 佐藤聡，小川智也，新城靖，吉田健一：筑波大学におけるハニーポットを用いた 不適切な SSH アクセスの収集とその解析，情報処理学会研究報告. IOT, [インターネットと運用技術] 2014-IOT-25(17), pp1-6, 2014-05-15.
[4] 池部実，宮崎桐果，吉田和幸：ハニーポットによる大分大学におけるダークネット宛通信の分析，情報処理学会研究報告. IOT, [インターネットと運用技術] 2015-IOT-29(17), pp1-8, 2015-05-14.
[5] OpenBSD：OpenSSH，(オンライン)，入手先 <http://www.openssh.com/> (参照 2015-08-24).
[6] MaxMind：GeoIP2 データベース，(オンライン)，入手先 <https://www.maxmind.com/ja/geoip2-databases> (参照 2015-08-24).
[7] micheloosterhof：Cowrie SSH Honeypot (based on kippo)，(オンライン)，入手先 <https://github.com/micheloosterhof/cowrie> (参照 2015-08-24).
[8] The Honeynet Project：Kippo - SSH honeypot，(オンライン)，入手先 <https://www.honeynet.org/project/Kippo> (参照 2015-08-24).
[9] SANS - Internet Storm Center：SSH Scanning Activity，(オンライン)，入手先 <https://isc.sans.edu/ssh.html> (参照 2015-08-24).