教育・研究報告

関西大学大学院総合情報学研究科における SSH アクセスの収集と分析

中田恭平 ・ 坂本　要 ・ 吉井　章 ・ 小林孝史

1. はじめに

情報通信技術の発展に伴いクラウドコンピューティングに代表されるようなコンピュータネットワークを介した形態のサービスが創出されている．そして，それらは我々にとって必要不可欠な社会基盤の一つとなっている．一方で，その社会基盤は様々な脅威に晒されており，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が発生している．情報セキュリティ白書2014によると，2012年度に引き続き2013年度も不正アクセスによる情報漏えいの被害が多数報告されている[1]．その不正アクセスの原因の一つとして，総当たり攻撃や辞書攻撃によって，認証に必要なユーザ名とパスワードが攻撃者に推測されることが挙げられる．さらに，2013年度は別の情報源から入手したユーザ名を軸に，あらかじめ用意した多数のパスワードによって認証を試行する攻撃（以下，パスワードリスト攻撃）の事例も多数確認された．これら総当たり攻撃やパスワードリスト攻撃によって，実際に不正ログインのあったサービスとその概要を表 1 に示す．不正ログインを試行した回数は，報告された事例では数万回から数千万回にわたって行われていた．また攻撃期間が短い事例では数日，長い事例では数ヶ月にわたって不正ログインが試行されていた．クラブニンテンドーの事例では，約1,500万回のログイン試行が約 1 ヶ月の期間にわたって行われた結果，約 2 万 4 千件のアカウントに対して不正アクセスが行われていた．

表 1 で挙げた事例は，主に Web サービスで発生した不正アクセスである．しかし，Web

表 1　不正ログインのあったサービスとその概要

公表日	対象サービス	攻撃期間	被害数	ログイン試行数
2013/5/17	ディノスログインページ	2013/5/4～5/8	約15,000	約1,110,000
2013/6/19	ニッセンオンライン	2013/6/18	126	11,031
2013/7/5	クラブニンテンドー	2013/6/9～7/4	23,926	15,457,485
2013/8/12	Ameba	2013/4/6～8/3	243,266	公開なし
2013/7/9	KONAMI ID ポータルサイト	2013/6/13～7/4	35,252	3,945,927
2013/9/27	バンダイナムコ ID ポータルサイト	2013/9/23～9/26	34,069	1,003,198
2013/10/23	セブンネットショッピング	2013/4/17～7/26	150,165	公開なし

1）p.17 表1-2-2 不正ログインのあったサービスとその概要より一部抜粋
出所）独立行政法人情報処理推進機構『情報セキュリティ白書2014』2014年 7 月．

サービス以外にもメールやデータベース，あるいはSSHといった他のサービスにおいても，長期間にわたるユーザ名の総当たり攻撃や，パスワードリスト攻撃によって不正アクセスが発生した事例が報告されている．

本稿では，特にSSHサービスで発生する不正アクセスに着目する．SSHサービスを提供するSSHサーバは，認証に成功すると誰でも操作することができるため，ユーザ名の総当たり攻撃やパスワードリスト攻撃によって不正アクセスが発生する恐れがある．そしてSSHサーバで不正アクセスが発生した場合は，不正アクセスを受けたユーザの情報が流出するだけではなく，イントラネット内の他のサーバに対して攻撃が実施されることや，インターネット上の他のサーバに対する攻撃の踏み台として利用されること，あるいはボットネットの一部として計算機資源が悪用されることもある．

2015年3月に国立情報学研究所で報告された事例では，研究系公開SSH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を行う踏み台として悪用されていた[2]．この事例では，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．したがって，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，日常的なログメッセージの監視が必要である．

また不正アクセスを防ぐために，侵入検知システムや侵入防止システムといった製品を導入することは有効である．あるいは，SSHサービスに限定するならば，fail2banやDenyHostsといったシステムをホストサーバに導入し，SSHに起因する不正アクセスの対策を実施することも有効である．しかし，これら不正アクセスの対策システムには誤検知や未検知の問題を切り離すことができず，状況に応じてシステムの管理者がログメッセージを手作業で調査することを求められる場合もある．ログメッセージを手作業で調査する上で，次に挙げるような問題が存在する．第一の問題は，ログメッセージが文字として提供されるため，示唆する情報を把握するためには，文字を読んで理解する必要がありその認識負荷が大きい．第二の問題は，ログメッセージに記されている情報やその記録形式は一様ではなく，ログメッセージは基本的には出力される契機があったサーバで記録されるため，ログメッセージがサーバごとに偏在している．第三の問題は，単一のログメッセージにおいても文字の量は膨大であり，調査するためには多大な時間が必要となる．

このような問題点から，ログメッセージの調査は時間を要する作業であるといえる．さらに手作業であるため，必要な情報の抽出に不備が発生する可能性も捨てきれない．そこで，ログメッセージに含まれる情報から疑わしい事象を検知し，関連する情報の要約と視覚化をシステムによって行う．システムによって視覚化することで，読み取るべき情報を抽象化し，人間による理解が促進されることが期待できる．ログメッセージの調査作業をシステムによって支援することで，不正アクセスの兆候を発見することが容易になる（図1）．

そこで本稿では，OpenSSHサーバに対する不正アクセスを防止する目的の日常的な監視作

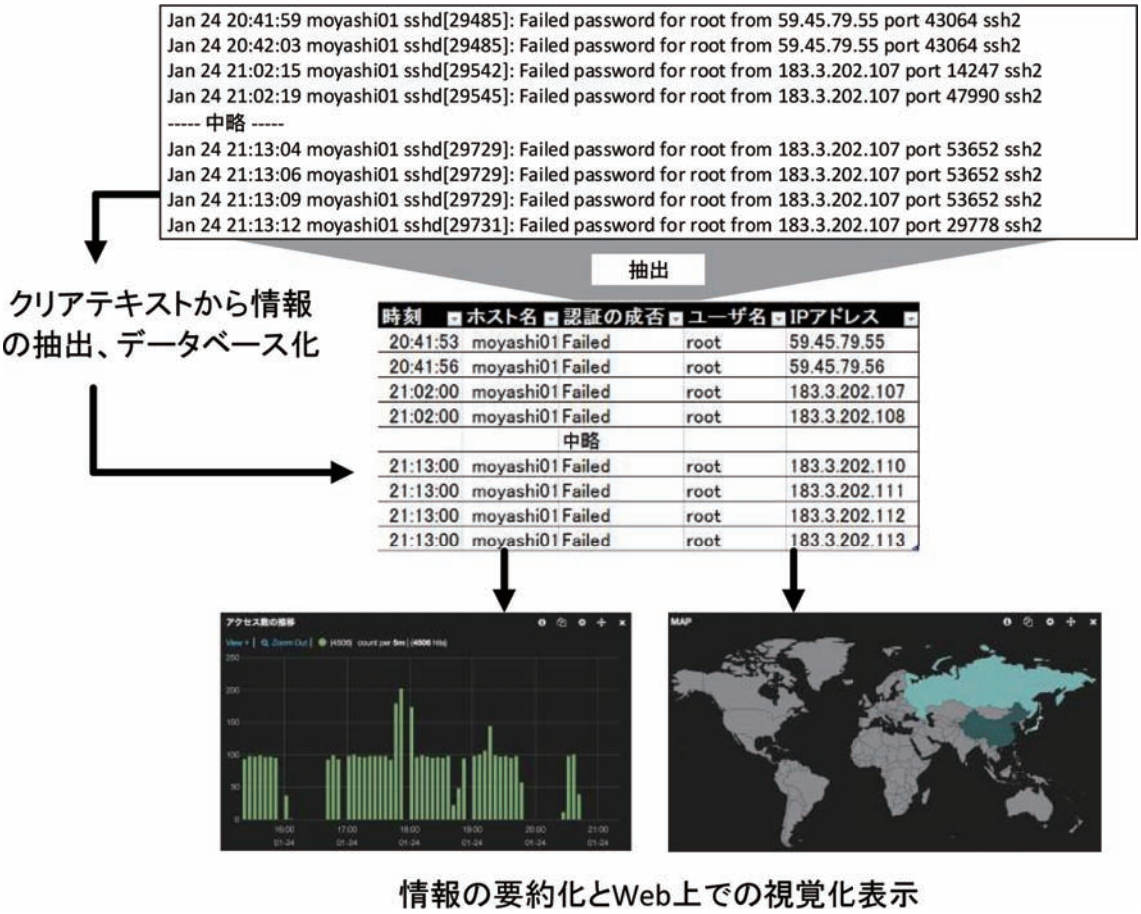


図 1　ログメッセージの抽出と情報の要約化，視覚化表示

業を支援するために，本稿で実装したシステムでログメッセージの集約と情報の要約，および視覚化表示を実施する．そして，本システムを運用して得られた知見をもとに，関西大学大学院総合情報学研究科のネットワーク宛てに行われた SSH サービスに対する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，ネットワークセグメントのエミュレートに優れた Honeyd と SSH サービスのエミュレートに優れた Kippo を組み合わせたシステムを使用して，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のアクセスを収集した．

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．そのダークネットとして，大分大学が保有する IP アドレスのうち，未使用である24ビットのネットワークセグメントを割り当てることで，クラス C 相当の通信状況の分析を可能とした．

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．本稿では，使用可能な IP アドレスに限りがあるため，関西大学のネットワークセグメント内で小林研究室に割り当てられた 3 件の IP アドレスを観測対象として SSH アクセスを収集する．またアクセス情報を収集する手段として，OpenSSH サーバと SSH ハニーポットを併用する．これは，複数の OpenSSH サーバを運用して得た知見から，関西大学のネットワークで運用している SSH サービスに対する攻撃は単一のサーバのみに限定されず，セグメント単位で行われていると推測し，その推測に基づいて OpenSSH サーバと同一セグメントの IP アドレス上に SSH ハニーポットを設置して，SSH サービスに対する攻撃を追求するためである．そこで，OpenSSH サーバに近い IP アドレスを SSH ハニーポットの観測点として設定する．

3. 提案手法

本稿では，Syslog デーモンの一つの rsyslogd を使用した rsyslog サーバを実装し，OpenSSH サーバが出力するログメッセージを一元的に収集する．Syslog デーモンは OpenSSH サーバの OS として一般的に使用されている UNIX 系 OS，Linux 系 OS に標準として導入されているため，本稿で対象外の OpenSSH サーバを将来的にシステムの管轄下に置くことが可能である．また OpenSSH サーバの分析を補完するために，OpenSSH サーバと同一のネットワークセグメント上の IP アドレスに SSH ハニーポットを設置する．そして，その認証機構を攻撃者に使用させることで，OpenSSH が収集不能な認証時のパスワードに対する分析を実施する．さらに，rsyslog サーバで収集したログメッセージを全文検索エンジンの Elasticsearch とその視覚化ツールの Kibana で構成したログ分析システムによって，ログメッセージの調査作業を支援する．

本稿では，OpenSSH サーバのアクセス分析における指標として，三種類に分類した認証の状態を定義する．認証の状態とは，「Accepted」，「Failed」，「Invalid」と定義する．

- Accepted とは，認証に成功した状態．
- Failed とは，サーバに登録済みのユーザ名で認証に失敗した状態．
- Invalid とは，サーバに未登録のユーザ名で認証に失敗した状態．

これらの認証の状態を定義することで，OpenSSH サーバで実施された認証の結果をユーザ名の総当たり攻撃か，特定のユーザ名に対するパスワードリスト攻撃が実施されているのかを判定することできる．

4. システム概要

本稿で実装したシステムの概要を図 2 に示す．ログメッセージを収集対象とするホストサーバの SSH サービスは，OpenSSH と SSH ハニーポットの Cowrie を使用する．OpenSSH と Cowrie は，22/TCP へのアクセスを受け付ける．そのアクセスによって出力されたログメッ

セージを rsyslog サーバに転送する．OpenSSH によるログメッセージは，Syslog デーモンの rsyslogd か syslogd を用いて転送し，rsyslog サーバの rsyslogd を介して MySQL サーバに格納する．次に Cowrie によるログメッセージは，MySQL Logging Module を用いて rsyslog サーバ内の MySQL サーバに格納する．MySQL サーバに格納されたログメッセージからアクセス時刻，使用したユーザ名，アクセス元の IP アドレス，認証の成否，アクセス元 IP アドレスの国籍の分析対象とする情報を抽出し，その情報をドキュメントとしてログ分析サーバの Elasticsearch に転送する．さらに，Kibana を利用して Elasticsearch に格納されたドキュメントに対して検索と集計を実施し，その結果を Web ページ上で視覚化したレポートとして管理者に提供することで，ログメッセージの調査作業を支援する（図 3 ）．本稿で運用中の OpenSSH サーバでの正規ユーザの利用分析を実施しているレポートを図 4 に示す．正規ユーザの認証履歴を調査することで，そのユーザ名に対するパスワードリスト攻撃が行われているかといった，分析も容易にできる．

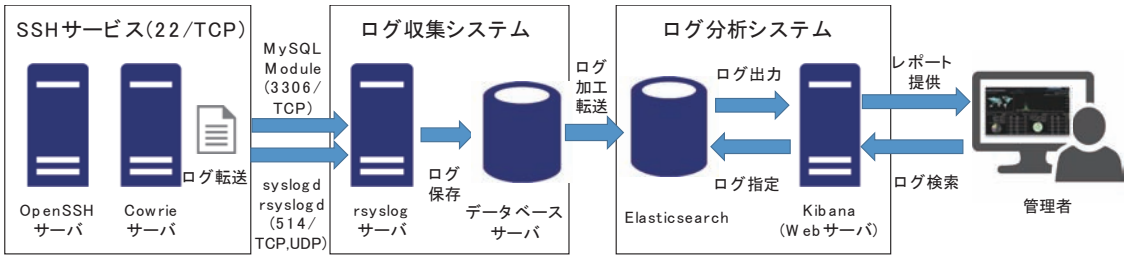


図 2　システムの概要

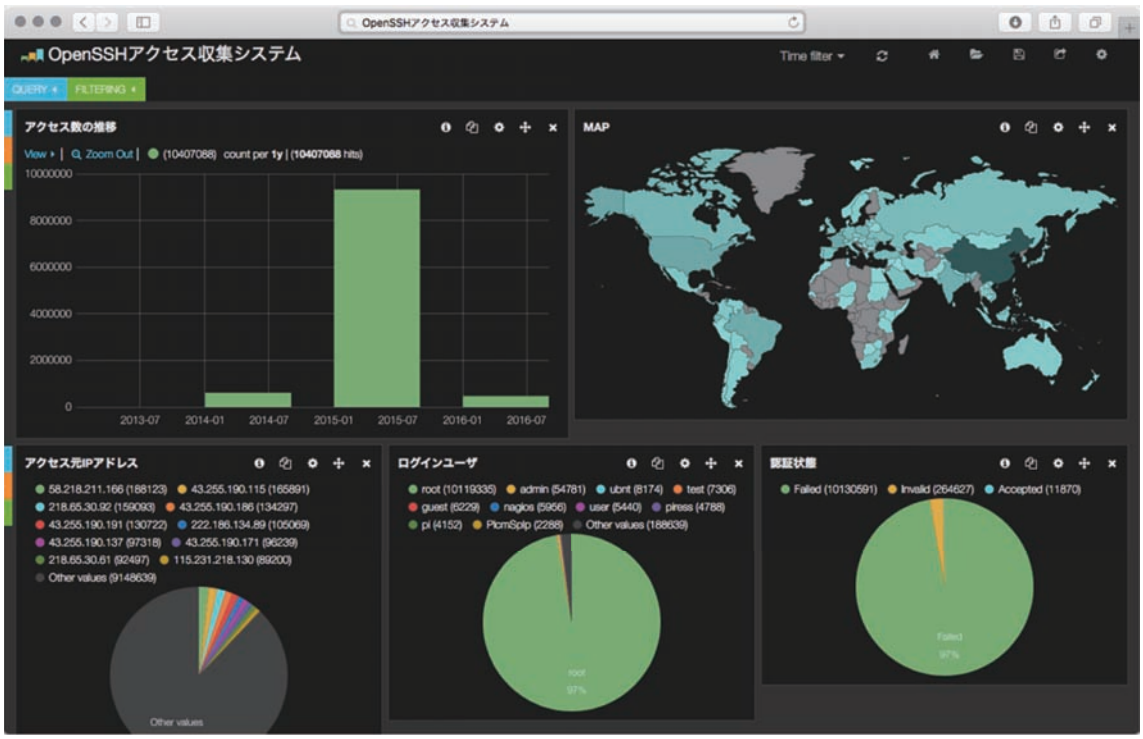


図 3　Kibana による視覚化レポート

図 4　正規ユーザのアカウントに対して実施された認証試行の視覚化レポート

5. 収集したデータの分析

本章では，3 章で論述した SSH アクセスのログ収集・分析システムを運用して得られた結果について報告する．本稿における OpenSSH サーバの「認証試行数」は，クライアントが OpenSSH サーバとセッションを構築した後に，パスワードを入力した回数と定義する．Cowrie サーバの「接続試行数」は，クライアントが Cowrie サーバにセッションを構築した回数と定義する．Cowrie サーバの「認証試行数」は，セッションの構築後に入力されたパスワードの回数と定義する．

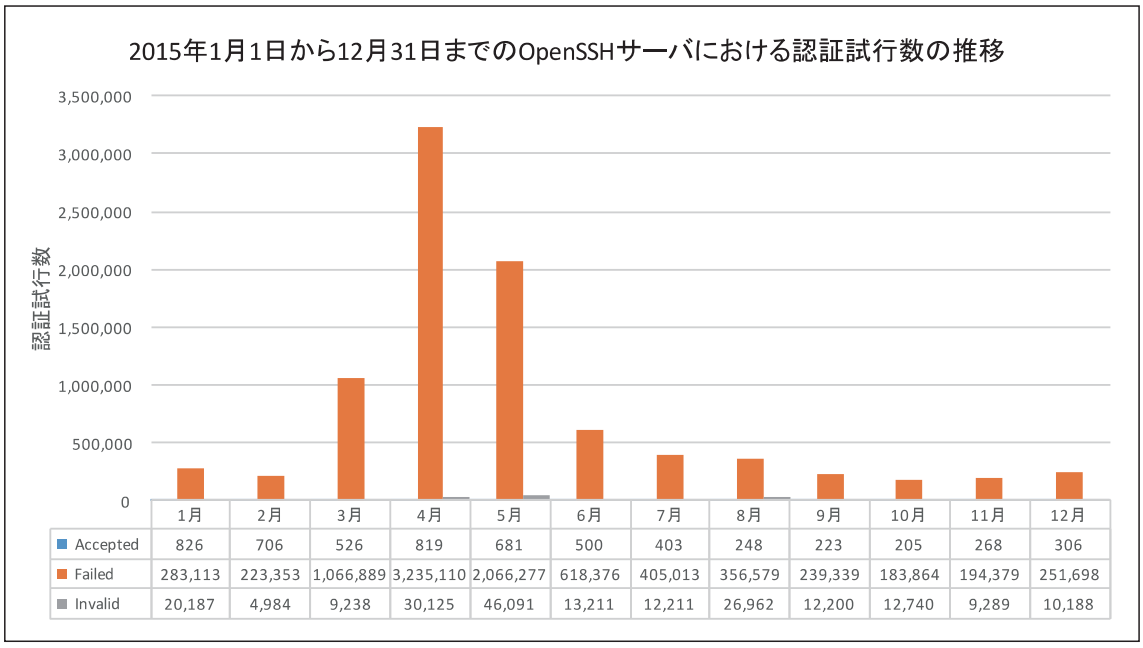
また本稿の分析対象とするネットワークは，関西大学高槻キャンパスの大学院棟（D 棟）に割り当てられた IP アドレスで，158.217.77.0/24のセグメントに相当する．そのセグメントの中から小林研究室に割り当てられた計 3 件の IP アドレスを使用し，2 件を OpenSSH サーバ，1 件を Cowrie サーバとして運用している．OpenSSH サーバに割り当てた IP アドレスにはドメイン名が付与されているが，Cowrie サーバに割り当てた IP アドレスにはドメイン名が付与されていない．

5.1. OpenSSH サーバの分析

本稿では，OpenSSH サーバを対象として2015年 1 月 1 日から12月31日までの期間におけるログメッセージを分析する．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

せる必要があり，ログメッセージ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メッセージを収集していない．

期間内における OpenSSH サーバの認証試行の概要を説明する．総認証試行数は，延べ9,337,127回を示した．その内訳は Accepted が5,711回，Failed が9,123,990回，Invalid が207,426回を数えた．Accepted は，期間を通して一日あたり数十回のオーダで認証試行が行われていた．Failed は，2015年 3 月上旬から一日あたりの認証試行数に上昇する傾向が見られ，3 月28日に約21万回を観測した．そして，4 月中旬から 5 月下旬にかけて，一日あたり10万回以上のオーダで認証試行が行われた．4 月30日には，期間内における Failed の最大認証試行数の325,041回を示した．その後，6 月上旬からは，一日あたり数千から数万のオーダで推移して，その後突出して認証試行が行われた形跡は観測されていない．Invalid は，期間を通して一日あたり数百から数千のオーダで認証試行があったが，Failed より突出して試行された形跡は観測されていない．また 5 月12日，7 月 5 日，8 月14日，10月17日，11月19日に Invalid に相当する認証試行が約 1 万のオーダで確認されたが，それぞれ異なる単一の IP アドレスによって，ユーザ名に対する総当たり攻撃がなされた結果であった．本稿で観測した Accepted，Failed，Invalid ごとの認証試行数の推移を図 5 に示す．認証を試行した IP アドレスの総数は4,855個，その 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14,629種類であった．



	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
Accepted	826	706	526	819	681	500	403	248	223	205	268	306
Failed	283,113	223,353	1,066,889	3,235,110	2,066,277	618,376	405,013	356,579	239,339	183,864	194,379	251,698
Invalid	20,187	4,984	9,238	30,125	46,091	13,211	12,211	26,962	12,200	12,740	9,289	10,188

図 5　OpenSSH サーバにおける認証試行数の推移

5.1.1. アクセス元 IP アドレスに対する分析

期間内において OpenSSH サーバに対して行われた認証で，認証試行数が多いアクセス元 IP アドレスのうち，上位10件を表 2 に示す．表に挙げた IP アドレスによる認証には三つの

特徴があった．第一に，全ての認証試行はユーザ名の root に対してパスワードリスト攻撃を実施していた．なおユーザ名の root は，OpenSSH サーバの OS でスーパーユーザとして存在するため Failed として分類している．第二に，アクセス元 IP アドレスの属する国が香港を含む中華人民共和国に集中していた．第三に，認証試行を一度に集中して行うだけではなく，期間を空けて継続して認証試行を行っていた．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パスワードリスト攻撃を試行していたことがわかる．

5.1.2. アクセス元 IP アドレスが属する国および地域に対する分析

期間内において OpenSSH サーバに対して行われた認証で，認証試行数が多いアクセス元 IP アドレスが属する国および地域のうち，上位10件を表 3 に示す．アクセス元 IP アドレスが属する国は，総認証試行の約61.1％を中華人民共和国，約35.0％を香港で占めていた．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中華人民共和国で，使用されたユーザ名は6,211種類であった．しかし，中華人民共和国からの認証試行は6,211種類のユーザ名が使用されていたが，認証試行の約98.52％は root による認証で占めていた．したがって，中華人民共和国からのアクセスはユーザ名の総当たり攻撃よりも root に対するパスワードリス

表 2　OpenSSH サーバの認証試行数を軸としたアクセス元 IP アドレス上位10件

IP アドレス	Accepted	Failed	Invalid	ユーザ名数	最多ユーザ名
58.218.211.166	0	188,123	0	1	root
43.255.190.115	0	165,891	0	1	root
218.65.30.92	0	143,543	0	1	root
43.255.190.186	0	134,297	0	1	root
43.255.190.191	0	130,722	0	1	root
222.186.134.89	0	105,069	0	1	root
43.255.190.137	0	97,318	0	1	root
43.255.190.171	0	96,239	0	1	root
218.65.30.61	0	92,497	0	1	root
115.231.218.130	0	89,200	0	1	root

表 3　OpenSSH サーバの認証試行数を軸としたアクセス元 IP アドレスの国上位10件

国コード	Accepted	Failed	Invalid	ユーザ名数	最多ユーザ名	最多ユーザ名割合
CN	0	5,624,380	76,632	6,211	root	98.52%
HK	0	3,260,677	540	105	root	99.98%
FR	0	65,871	1,111	202	root	98.26%
US	1	27,250	39,131	1,454	root	35.06%
IN	0	35,422	4,242	652	root	88.96%
BR	0	16,702	13,661	3,015	root	53.25%
KR	0	16,495	2,749	240	root	84.83%
CA	0	11,506	2,753	512	root	79.24%
RO	0	10,522	670	104	root	93.89%
NL	1	2,106	8,954	208	root	18.58%

ト攻撃が行われる傾向があると言える．さらに，その root に対するパスワードリスト攻撃の傾向は，香港からの認証試行に明確に現れており，root による認証が約99.98％を占めていた．また他の国においても，全体的な認証試行の傾向は，ユーザ名に対する総当たり攻撃や特定の一般ユーザに対するパスワードリスト攻撃よりも，スーパーユーザの root や管理者を意味する「admin」や「Administrator」といったユーザ名に対するパスワードリスト攻撃が試行される傾向があった．また日本以外にもアメリカ合衆国とオランダをアクセス元とする認証試行で Accepted に分類されるものを観測したが，これは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．

5.1.3. ユーザ名に対する分析

期間内において OpenSSH サーバに対して行われた認証で，認証時に使用されたユーザ名のうち，上位10件を表 4 に示す．

最も認証に用いられたユーザ名は root で，アクセス元 IP アドレスが属する国は101の国と地域を示した．ユーザ名を root に設定された認証試行は，総認証試行の約97.6％を占めている．また root 以外にも管理者を意味する単語の「admin」や，サーバ系の OS で一般的に利用されているサービス名を表す nagios，oracle，ftp なども認証に使用されていた．このことからユーザ名の総当たり攻撃を行うリストの中に，表 4 で示したユーザ名が掲載されていると推測される．

表 4　OpenSSH サーバの認証試行数を軸としたユーザ名上位10件

ユーザ名	Accepted	Failed	Invalid	使用国数	IP アドレス数
root	0	9,113,750	0	101	3,694
admin	0	0	37,833	93	2,106
ubnt	0	0	7,562	91	1,830
test	0	0	6,269	77	991
nagios	0	0	5,556	49	315
guest	0	0	5,427	70	1,071
piress	0	0	4,788	1	1
user	0	0	4,657	63	820
pi	0	0	3,880	68	1,040
PlcmSpIp	0	0	3,330	64	809

5.2. Cowrie サーバの分析

本稿では，Cowrie サーバを対象として2015年 6 月 1 日から12月31日までの期間におけるログメッセージを分析する．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必要があり，ログメッセージを収集していない期間が存在する．

期間内における認証試行数とセッション数の概要を説明する．総認証試行数は延べ1,330,134回を示し，総接続試行数は延べ407,129回を示した．期間内における認証試行数の推移と接

続試行数の推移を図 6 に示す．認証を試行した IP アドレスの総数は2,215個，その IP アドレスが属する国の総数は93の国と地域，使用されたユーザ名の総数は13,651種類，使用されたパスワードの総数は128,623種類であった．

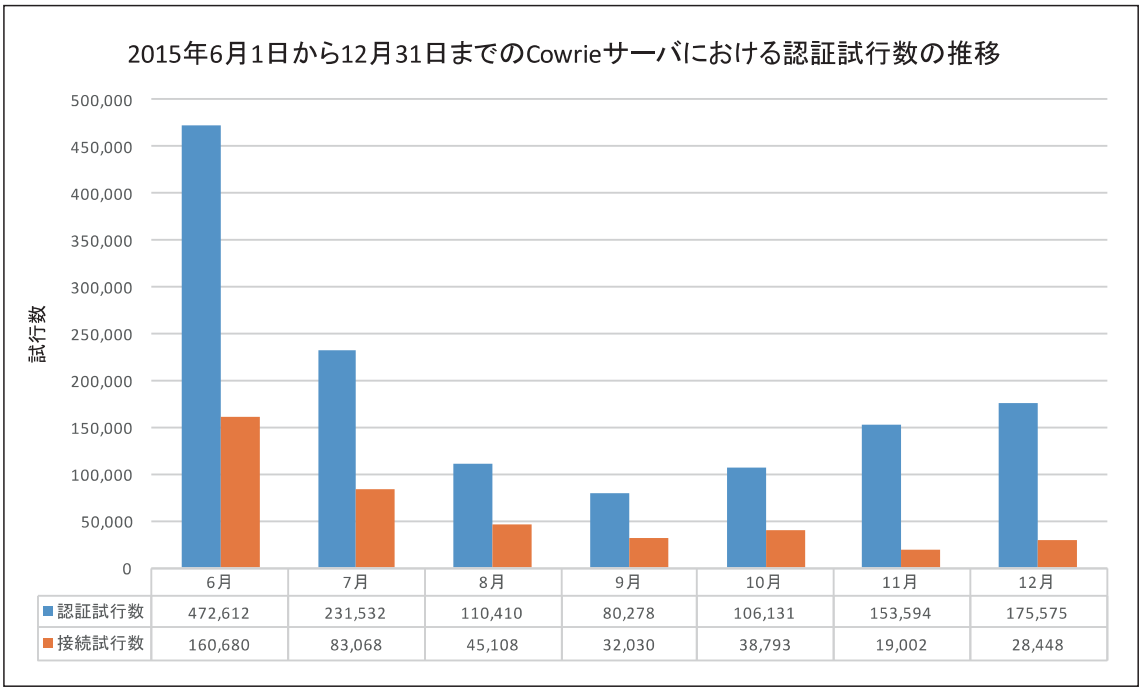


図 6　Cowrie サーバにおける認証試行数と接続試行数の推移

5.2.1. アクセス元 IP アドレスに対する分析

期間内において Cowrie サーバに対して行われた認証で，認証試行数が多いアクセス元 IP アドレスのうち，上位10件を表 5 に示す．

上位に挙げたアクセス元 IP アドレスには，三つの特徴があった．第一に，root に対するパスワードリスト攻撃を試行する傾向があった．表上では，異なるユーザ名として扱っているが，「root」の文字列に他の文字列や数字が付与されたユーザ名を観測した．例えば，「危

表 5　Cowrie サーバの認証試行数を軸としたアクセス元 IP アドレス上位10件

IP アドレス	国コード	接続数	認証試行数	ユーザ名数	パスワード数
43.255.189.44	HK	27,705	81,171	23	20,963
43.229.52.212	HK	21,355	63,776	89	24,564
58.218.211.198	CN	1,945	40,335	17	5,508
182.100.67.59	CN	2,396	37,484	17	5,508
58.218.211.38	CN	1,805	36,754	17	5,508
218.65.30.92	CN	4,603	33,902	17	5,535
113.195.145.12	CN	4,307	28,969	17	5,509
43.229.52.68	HK	8,333	24,892	39	19,739
43.229.52.167	HK	8,284	24,750	8	12,708
113.195.145.70	CN	8,168	24,430	16	5,197

険な」パスワードとされる文字列や，他のプログラム言語の記述や，あるいはファイルパスが付与されたユーザ名が見られた．この root に文字列が加えられたユーザ名の例を次に挙げる．

- root/8ik,9ol.0p;（キーボート配列と思しき文字列を付与）．
- root/1234（パスワードと思しき文字列を付与）．
- root/sshd/contrib/cygwin（ファイルパスと思しき文字列を付与）．
- avconroot（root の前に文字列を付与）．

これら文字列としての root を含有したユーザ名を378件観測した．第二に，アクセス元 IP アドレスの属する国が香港を含む中華人民共和国に集中していた．また同一のネットワークセグメントで IP アドレスを変更して，連続して認証を試行する例も見られた．第三に，香港を含む中華人民共和国以外の IP アドレスから認証は，一度の認証期間で使用された後にその IP アドレスは使用されない傾向があった．

5.2.2. アクセス元 IP アドレスが属する国および地域に対する分析

期間内において Cowrie サーバに対して行われた認証で，認証試行数が多いアクセス元 IP アドレスが属する国および地域のうち，上位10件を表 6 に示す．

香港を含む中華人民共和国からの認証試行数が，総認証試行数の約89％を占めており，セッション数においても総セッション数の約79％を占めている．香港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．特にユーザ名の root の使用率が最も高く，root を軸にパスワードを変更して認証を行うパスワードリスト攻撃を実施している傾向が見られた．

また中華人民共和国からの認証試行は，香港からの認証試行よりもユーザ名の総当たり攻撃を観測した例が見られたが，主として root に対する認証試行を実施していた．さらに，香港や中華人民共和国以外の国からの認証試行においても，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リスト攻撃を試行する傾向が見られた．

表 6　Cowrie サーバの認証試行数を軸としたアクセス元 IP アドレスの国上位10件

国コード	接続数	認証試行数	ユーザ名数	パスワード数	最多ユーザ名	最多ユーザ名割合
CN	181,827	770,519	4,795	37,985	root	96.87%
HK	141,214	418,370	259	99,557	root	99.77%
BR	25,919	25,993	6,044	8,967	root	22.22%
NL	9,497	17,501	4,780	6,060	root	7.22%
US	6,508	11,382	351	4,314	root	77.45%
BD	3,982	7,814	2,615	2,949	root	1.06%
IN	2,715	2,716	184	742	root	68.74%
DE	1,769	1,765	122	815	root	58.47%
KR	2,021	1,618	160	578	root	48.76%
TR	859	1,359	279	591	root	48.05%

5.2.3. ユーザ名に対する分析

期間内においてCowrieサーバに対して行われた認証で，認証時に使用されたユーザ名のうち，上位10件を表7に示す．

最も認証に用いられたユーザ名はrootで，アクセス元IPアドレスが属する国は87の国と地域であった．rootによる認証試行は総認証試行の約93.9%を占めている．ユーザ名のrootとパスワードとの組合せが120,679件を観測したことから，rootに対するパスワードリスト攻撃が実施されていることが顕著に表れている．またroot以外にも，他のサービス名のmysql, postgres，ftpや他のOSを意味すると推測できるubnt, oracle, ubuntuといったユーザ名なども認証に使用されたことを確認した．

表7　Cowrieサーバにおける認証試行数を軸としたユーザ名上位10件

ユーザ名	認証試行数	使用国数	IPアドレス数	パスワード数
root	1,248,891	87	1,901	120,679
admin	10,828	84	1,149	4,565
ubnt	1,675	78	1,109	96
test	1,439	59	455	406
oracle	1,180	36	148	731
guest	962	54	385	103
pi	866	55	512	22
123456	806	18	37	697
user	805	48	253	102
mysql	788	14	31	613

5.2.4. パスワードに対する分析

期間内においてD棟割り当てのIPアドレスを有するCowrieサーバに対して行われた認証で，認証時に使用されたパスワードのうち，上位10件を表8に示す．

パスワードは，ユーザ名と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

表8　Cowrieサーバにおける認証試行数を軸とした入力されたパスワード上位10件

パスワード	認証試行数	使用割合	使用国数	IPアドレス数	ユーザ名数
root	7,356	0.55%	85	1,415	3,910
123456	4,083	0.31%	56	612	1,292
wubao	3,811	0.29%	25	204	1
ADMIN	3,539	0.27%	87	1,455	268
password	2,855	0.21%	51	597	332
1234	2,637	0.20%	58	592	582
（空白）	2,504	0.19%	25	258	250
12345	2,149	0.16%	52	584	144
jiamima	1,906	0.14%	25	190	1
ubnt	1,870	0.14%	78	1220	14

ードの wubao，jiamima はユーザ名との組合せが 1 件であるが，これは root と組合せで使用されていた．これらのパスワードを最も使用していた国は，中華人民共和国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．

6. おわりに

本稿で実装したシステムを運用して得られた知見をもとに，関西大学宛てに行われた SSH サービスに対するアクセスを分析した結果を報告した．その結果，香港を含む中華人民共和国からの認証試行が関西大学大学院総合情報学研究科に対する SSH アクセスの大部分を占めることや，管理者権限の奪取を目的としたスーパーユーザの root に対するパスワードリスト攻撃が恒常的に実施されていることが判明した．

しかし，本稿で観測する対象とした IP アドレスは，小林研究室が利用している IP アドレスに限定を余儀なくされたため，実際に関西大学大学院総合情報学研究科宛ての SSH アクセスを正確に観測しているとは言い切れない．ゆえに観測する対象として少なくとも24ビットの IP アドレス空間か，関西大学内の他のセグメント上に観測点としての IP アドレスを増加させる必要がある．ゆえに，セグメント単位の攻撃観測は今後の課題としたい．

また，本稿で実施したログメッセージの収集対象を他の総合情報学研究科の研究室で運用している OpenSSH サーバに適応することで，よりセグメント単位に対する攻撃を明らかにしたい．さらに，当該 OpenSSH サーバを運用している研究室に不正アクセスの試行状況を報告するとともに，OpenSSH サーバのセキュリティ対策を支援したい．

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 2016-02-12）．

[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.