論文

ハニーポットによる学内ネットワークへの不正アクセスの観測

馬場　一輝　　梅原　英一

本研究は，学内ネットワーク，及び学外ネットワーク上にハニーポットを搭載したサーバ機を設置し，SSH 接続を介して行われる不正アクセスを観測し，その記録を分析・比較し，それを元に学内ネットワーク上にサーバ機を設置する際の留意点や行うべきセキュリティに関する設定などをまとめた．その結果，学内ネットワーク機と学外ネットワーク機への攻撃傾向には大きな差は見られず，必要なセキュリティ対策も学外ネットワーク上に設置するものと大きく変わらないという結論に至った．

キーワード：情報セキュリティ，ハニーポット，不正アクセス

1　はじめに

近年，仮想サーバ上に環境を構築する VPS サービスが手軽さ，安価，物理的保守の簡単さ，容易にスケールが変更できるといった点によって大きく流行している．これらの VPS サービスはボタン一つでサーバ上に環境を構築し，必要な機能を手軽に使用することができる．これらは便利である反面，実体を持つサーバをユーザ自身が構築していた時代と比べてユーザがサーバを運用する上で知識を持たなくても外部へのコンテンツの公開などの行為が可能となった．また，東京都市大学メディア情報学部情報システム学科では自分たちでサーバ環境の構築・運用を体験する実践的な講義が行われているが，この講義においてもセキュリティ関係の設定等に関してはセキュリティソフト任せであったり，そもそも設定を一切行わないものであったりして，講義の中で外部からアクセスが可能であるサーバのセキュリティ問題についての重要性を理解できないという問題がある．

本研究では東京都市大学のネットワーク内に設置したサーバ機及び学外ネットワークに設置したサーバ機を用いて不正アクセスの傾向を比較・検証し，それを元に大学ネットワーク内に設置するサーバに必要なセキュリティ設定，手法を考察，提案することを目的とする．

2　不正アクセスとハニーポット

2．1　不正アクセスとは

『不正アクセス行為の禁止等に関する法律』[1] による不正アクセスの定義を簡潔にまとめると，他社のコンピュータなどの ID・パスワード，その他識別子を用いて制限されている電子機器にネットワーク経由で接続し，それらの識別子をもって本来他社には制限されている機能を使用できるようにすることである．

今回の実験においては設置してあるサーバ機に対しての悪意あるログインの試行や，ログイン成功後の一連の行動を不正アクセスとして表記する．

2．1　ハニーポットとは

ハニーポットとは蜜壺という意味を持つ単語であり，クラッカーによる不正アクセスを呼び寄せる脆弱なシステム及び見かけ上脆弱に見えるシステムのことを言う俗称である．ハニーポットを用いることにより，クラッカーによる最新の攻撃手法や狙われる脆弱性，場合によっては使われているマルウェアなどのソフトウェアまで多岐に渡る項目の観測が可能となる．

ハニーポットには低対話型と高対話型と呼ばれる種類がある．低対話型ハニーポットは特定の OS やアプリケーションを模倣，エミュレートし侵入を観測する．高対話型ハニーポットは本物の OS やアプリケーションをハニーポットとして運用するものである．

前者の利点はあくまでエミュレートした範囲でしか機能が使えないため，侵入者の内部での活動による危険性はあまり大きくない．ただし，その分侵入者が実際にどのような行為を行おうとしていたのかを必ずしも全て観測することができないという問題がある．

後者の利点は本物のシステムを利用するため，侵入者が本来行おうとしていたことを殆ど全て実行でき，その分正確に侵入者の攻撃手法を知ることができる．しかし問題点として，侵入された際にそれを踏み台にされてし

BABA Kazuki
東京都市大学メディア情報学部情報システム学科
2016 年度卒業生
UMEHARA Eiichi
東京都市大学メディア情報学部情報システム学科教授

まうなどの本末転倒な状況になるといった危険性がある．

このように低対話型，高対話型双方に利点・欠点があるが，一般的に使われているハニーポットは危険性が低く比較的手軽に導入ができる低対話型ハニーポットである．

3 先行研究

3．1 最近のハニーポットの動向と倫理的問題

李ら（2012）［2］は各種ハニーポットの仕組みや最近の研究や将来の研究動向，そしてそれらに対する問題提起を行った．彼らは近年発展している仮想化技術を利用し，一台の物理マシン上に複数の仮想環境を構築し，その上で複数のハニーポットを動作させる仮想ハニーポットがコスト削減，及び不具合が生じた場合であっても素早い復旧が可能であるという利点を示した．また，ハニーポットを用いた研究上の問題点として，高対話型ハニーポットをクラッカーから逆に利用されてしまうという危険性，ハニーポットは脆弱性を持つシステムを用いて監視を行うため，最新のセキュリティ状態を保っているコンピュータと比べて安全性が低いという危険性がある，と指摘をしている．

結論として，ハニーポットはインターネット全体の安全を向上させる目的で作られたものであるが，セキュリティを低下させた場合の責任の所在や，セキュリティを低下させないための工夫・改善をしていき，技術だけでなく倫理的問題の検討や法律の整備などの面からもバランス良く発展していく必要がある，としている．

3．2 ハニーポットを設置したダークネットのアクセス特性

曽根ら（2013）［3］は，複数のグローバル IP アドレスを変換し，一台のハニーポットで不正トラフィックを観測できるシステムを運用した．また，既存の低対話型ハニーポット Dionaea を改良し，攻撃者が本物の環境なのか，ハニーポットによって偽装構築された環境なのかを判別できないような工夫をした．

この先行研究結果から，今回の実験では初期状態から比較的クラッカーからハニーポットであることがわかりにくいような環境整備に関する検討を行い，Dionaea と比べて偽装設定などの自由度が高く，開発が比較的最近まで続けられている低対話型ハニーポット Kippo を使用することに決定した．

3．3 ハニーポットを利用した大学に対する攻撃パターン解析に関する研究

大城ら（2013）［4］は，琉球大学の公式 Web サイトを設置している Web サーバ及びミラーサーバに設置してあるネットワーク上にハニーポットを設置し，攻撃の観測を行った．この実験において，遠隔操作を目的としたアクセスが多く，Web サーバの管理者ページを狙ったアクセスにより，Web ページの改ざんや情報の窃取を狙った攻撃が多くあると考えられるという結論を出した．

4 本研究の目的と概要

4．1 本研究の目的

本研究の目的は，東京都市大学のネットワーク上に設置されたサーバ機に対する不正アクセスの実態を調査し，その対策を検討，提案することにある．

主に調査する点は本学のネットワーク上に設置されたサーバ機に対してどのようなユーザ名とパスワードを想定してアクセスを試みるのか，攻撃が無差別である場合，どのような国からの攻撃が多いのか，どのような脆弱性を狙って攻撃してくるのかといった点である．また，攻撃者が侵入に成功した場合，どのような行動を行うのかを観測し，それを元に侵入された場合，どのような対策をしておくことにより攻撃の被害を減らすことができるのかを検討することも目的とする．

4．2 本研究の概要

本研究では学内ネットワーク上及び学外ネットワーク上にそれぞれ 2 台ずつのハニーポットを搭載したサーバ機を設置し，それぞれへの不正アクセスの試行を観測，それらの内容を分析する．

実験期間は 2016 年 10 月 27 日から 11 月 27 日の 31 日間である．

本研究では学内ネットワークを利用するという点からシステムの安全性を考慮し，実際の脆弱な環境を用いる高対話型ハニーポットではなくソフトウェアにより脆弱な環境に見せかけて侵入者を騙す低対話型ハニーポットを用いることとした．

また，今回の実験において，学内に向けて行われている不正アクセスが東京都市大学に向けて行われているものなのか，それとも無作為に行われているものなのかを判別するため，学外ネットワーク上にもハニーポットを搭載したサーバ機を設置し，学内サーバ機との結果を比較し，有意な差がでるかどうかを検証する．

5 システム概要

学内ネットワークに設置するサーバ機は Ubuntu14.04 を搭載し，ハニーポットとして Kippo を使用する．また，設置は学内ファイアウォールから外れた部分に行い，学外からの攻撃を遮断しないようにした．

学外ネットワーク上に設置するサーバ機に関しては既存の VPS サービスを利用し，学内ネットワーク機と同様のシステム環境を構築した．

6　測定結果

6．1　被アクセス試行回数

外部より不正アクセス試行を受けた回数を表 1 に示す．

6．2　アクセス試行に使用されたユーザ名

学内設置サーバへのアクセス試行に使用されたユーザ名と回数を表 2 に，学外設置サーバへのアクセス試行に使用されたユーザ名と回数を表 3 に示す．試行回数は学内サーバ 2 台に向けたものと学外サーバ 2 台に向けたものをそれぞれまとめ，上位 20 件ずつを記載する．

6．3　アクセス試行に使用されたパスワード

学内及び学外サーバに対して行われたアクセス試行で使用されたパスワードと使用回数の上位 30 件を表 4 に示す．

表 1　被アクセス試行回数

サーバ	回数
学内サーバ 1	38,512
学内サーバ 2	39,795　（合計 78,307 回）
学外サーバ 1	41,231
学外サーバ 2	43,530　（合計 84,761 回）

表 2　学内設置サーバへのアクセス試行に使用されたユーザ名上位 20 件

ユーザ名	使用回数(回)
root	57158
admin	2462
111111	1591
1234	865
123321	865
test	514
user	508
ftpuser	471
guest	435
oracle	430
git	410
ftp	357
ubnt	290
mysql	229
test1	182
info	182
postgres	170
apache	163
vyatta	158
alex	151

表 3　学外設置サーバへのアクセス試行に使用されたユーザ名上位 20 件

ユーザ名	使用回数(回)
root	70347
admin	2945
111111	1832
1234	967
pi	858
oracle	725
mysql	682
test	613
123321	576
guest	519
user	483
support	431
ftpuser	368
apache	330
git	312
test1	245
test2	203
fax	195
postgres	174
www	167

表 4　学内設置サーバ及び学外設置サーバへのアクセス試行に使用されたパスワード上位 30 件

パスワード	使用回数(回)
123456	2616
admin	1580
password	950
test	720
root	712
support	640
Unknown	640
raspberry	632
default	584
ubnt	575
guest	568
PlcmSplp	552
!@	536
user	534
vyatta	475
1234	469
12345	423
oracle	416
git	391
mysql	390
ftp	387
alpine	385
ftpuser	382
apache	381
pi	376
test1	373
alex	368
webmaster	360
postgres	352
1qaz2wsx	349

6. 4 アクセス元の IP アドレス及び発信国

学内サーバ機 2 台へのアクセスに使用されたコンピュータの IP アドレス，発信元の地域，国名を被アクセス回数が多い順に上位 30 種を表 5 に示す.

7 本学に対する不正アクセスの分析と対策の提案

7. 1 本学に対する不正アクセスの分析

(1) 攻撃傾向に関する分析

学外に設置したサーバ機と学内に設置したサーバ機で特筆するような攻撃傾向の差は見られなかった．ただし，これは先日まで一切使用されていなかった IP アドレスを使用したことが原因である可能性があり，例えば東京都市大学のホームページを公開している Web サーバに同様にハニーポットを設置した場合も同様の結果がでるかどうかは不明である.

表 5 学内設置サーバへ不正アクセスを行った IP アドレス上位 30 件

IP アドレス	地域，国名	アクセス回数
58.218.211.94	Nanjing,China	2518
116.31.116.24	Guangzhou,China	1259
116.31.116.25	Guangzhou,China	805
58.218.199.182	Nanjing,China	530
58.218.204.223	Nanjing,China	335
103.236.201.76	不明	254
110.74.141.27	Malaysia	222
123.31.34.136	Hanoi,Vietnam	199
123.31.34.137	Hanoi,Vietnam	168
123.31.41.251	Hanoi,Vietnam	163
123.31.34.148	Hanoi,Vietnam	152
123.31.34.218	Hanoi,Vietnam	152
123.31.35.218	Hanoi,Vietnam	114
123.31.41.239	Hanoi,Vietnam	114
117.3.198.11	Hanoi,Vietnam	112
121.18.238.104	Hebei,China	95
178.238.227.223	Germany	95
221.194.47.229	Hebei,China	92
221.194.44.231	Hebei,China	90
221.194.47.224	Hebei,China	89
221.194.47.249	Hebei,China	85
221.194.44.219	Hebei,China	84
121.18.238.114	Hebei,China	79
121.18.238.98	Hebei,China	79
123.31.41.237	Hanoi,Vietnam	76
221.194.47.208	Hebei,China	75
5.45.76.23	Netherlands	67
218.91.153.179	Nanjing,China	66
58.218.199.218	Nanjing,China	56
123.31.32.65	Hanoi,Vietnam	55

(2) 攻撃内容に関する分析

攻撃に使用されているユーザ名を見ると一般的に認知されている通り，管理者権限を持つことが多い root や admin といったユーザ名や 111111 や test，user といったサーバ構築・環境構築時にテストとして作成され放置されていると考えられるアカウントを狙っていると思われるものが多く見られる．これらのアカウントを残しているユーザはセキュリティ関係の設定を重視していないと考えられ標的にされていると推測できる.

7. 2 対策の提案

前項までの結果を踏まえて，以下のセキュリティ対策を提案する.

・root アカウントのアクセス禁止
・SSH 待ち受けポート番号の変更
・公開鍵暗号を用いたログイン方式の採用
・不要なアカウントの処分

8 結論と今後の課題

8. 1 結論

本研究では東京都市大学のネットワーク上に SSH ハニーポットを搭載したサーバ機を新設し，不正アクセスの分析を行い，不正アクセスを試みる攻撃者の攻撃傾向からより安全なサーバ運用方法の提案を目的とした.

SSH を通した不正アクセス傾向の観測については学外ネットワーク上に設置したサーバ機との比較を行い，学内サーバ機に対する攻撃傾向と比較したが，攻撃内容に関して大きな差は認められず，また東京都市大学のみを狙って行われていると思われるような攻撃も認められなかった．攻撃傾向が一般的に行われるものと大きく変わらないため，一般的な手法により十分に危険を排除できるであろうと考えられる.

8. 2 今後の課題

今回の研究により，SSH 経由の不正アクセスが東京都市大学を狙ったものというよりは広域的な攻撃に東京都市大学のネットワークも巻き込まれているということがわかった.

しかし，今回の研究ではいくつかの課題が見つかった.

(1) SSH 接続による不正アクセスを受け付ける際，今回は 22 番ポート並びに 2222 番ポートを利用したが，他の解放されているポートを狙った攻撃は観測できていない．なので，他のポートにも SSH を

偽装したものを割り当てるか，そもそも全てのポートを監視できるハニーポットを利用して，より多くの情報を収集する必要性がある．

(2) 使用するハニーポットにKippoを採用したが，KippoはIDとパスワードの組み合わせを自分で設定しなければいけなく，今回の実験ではインターネット上で危険とよく言われているIDとパスワードの組み合わせを事前に設定していたものの，想像以上に侵入に成功した攻撃者が少なかった．これを解消するために，次に同様の実験をする場合は一度一週間程度記録を取り，それを元に攻撃される回数の多いIDとパスワードを全て組み合わせたパターンリストを作成し使用するべきではないかと考える．

(3) 今回の実験では２つのIPアドレスを大学から割り振っていただき，その２点を観測点として実験を行った．しかし，より多くのデータを取るためにはより観測点を増やし，同一期間中に多くのデータを取る必要があると考えられる．そこで，より多くのIPアドレスを使用し，それらのIPアドレスから一台のサーバ機にアクセスを集約することで複数台のサーバ機を用意せずに多くの観測点からのデータを採取することを提案する．

また，学外ネットワークに多くの観測点を設置する際も同様にVPSサービスなどで多くのIPアドレスの使用権をレンタルし，それらから一台のサーバ機にアクセスを集約することで比較的コストを少なくデータを集めることができる．ただし，多くのサービスではIPアドレスの追加割当には別途料金がかかるため，使用可能な金額と測定期間，観測点数のバランスを考える必要がある．

(4) 観測に使用するハニーポットについて，今回の実験ではKippoを使用したが，これはあくまでSSHを偽装するものであるので，HTTPやTCPに向けられている攻撃を観測できない．よって，SSHだけではなく，そもそもポートスキャンに対する偽装を行い，攻撃者の攻撃を誘発できるような設定をする，またはそのような機能を持つハニーポットを使用する必要があるのではないかと考えられる．

参考文献

[1] “不正アクセス行為の禁止等に関する法律”, http://law.e-gov.go.jp/htmldata/H11/H11HO128.html

[2] 李超，宮田純子，木下宏揚，“最近のハニーポットの動向と倫理的問題”，電気情報通信学会技術研究報告：信学技報，Vol.112，No.343，p.13-18，2012.

[3] 曽根直人，横田凌一，大久保諒，森井昌克，“ハニーポットを設置したダークネットのアクセス特性”, 第12回情報科学技術フォーラム講演論文集, Vol.12，No.4，pp.111-123，2013.

[4] 大城佳明，“ハニーポットを利用した大学に対する攻撃パターン解析に関する研究”，http://www.jsise.org/society/presentation/doc/pdf/2013/10_okinawa/1003.pdf，2013.