

## SSH サービスに対する攻撃について

### 1 はじめに

SSH (Secure SHell) サービス<sup>1</sup>とは、ネットワークを介して別のコンピュータにログインし、遠隔操作等を可能にするサービスのことである。また、パスワードを含むすべての通信を暗号化して行なうため、盗聴等の攻撃に対しても安全な通信を確保できる(図1)。

警察庁では、SSH サービスに対するアクセスが昨年下半期と比較して約20%増加していることを認知した。そこでアクセスの中にある不正な攻撃の実態について調査するため、環境を構築して観測を行った。その結果、SSH サービスを検出し、ID・パスワードを推測して認証試行を繰り返す攻撃ツールの存在を確認することができた。攻撃者が試行したユーザ名の約50%はシステムユーザ名であり、日本人名と考えられるユーザ名を含むユーザ名辞書が実在した。攻撃者が試行したパスワードは、6文字のパスワードが全体の約25%と最も多く、4文字から8文字のパスワードが全体の約80%を占めていた。パスワードの平均文字数は6.3文字、パスワードの最大文字数は30文字であった。攻撃者が試行したパスワードには、英単語等の辞書を利用したもの、キーボードの配列パターンを利用したもの、それらのパターンを複数組み合わせ合わせたものがあった。

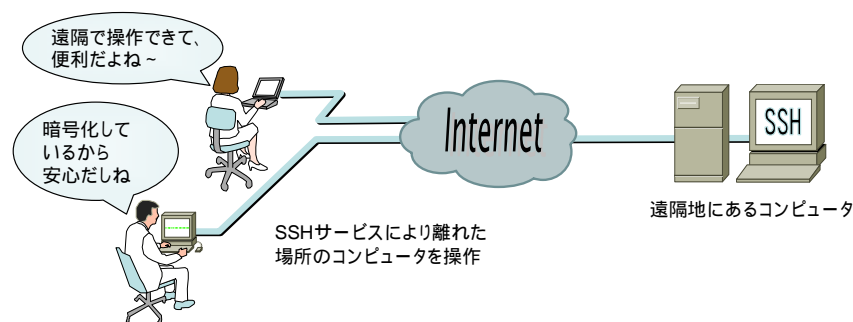


図1 SSHサービスの概要

<sup>1</sup> SSH サービスが普及する前は、Telnet サービスがよく使われていた。しかし、Telnet サービスはパスワードを含むすべての通信内容が平文のままであるため、通信内容を暗号化する SSH サービスへの移行が進んでいる。

## 2 観測結果

SSH サービスに対する攻撃状況を調査するために構築した観測環境の概要を表 1 及び図 2 に示す。観測期間は、2006 年 5 月からの 1 か月間である。

表 1 SSH サービス観測環境の概要

<ul style="list-style-type: none"> <li>・ SSH サービス用サーバ：4 台</li> <li>・ SSH サービス用グローバル IP アドレス：日本国内の連続する 4 つ</li> <li>・ リモートからのログインを許可されたユーザ：なし</li> <li>・ リモートからのパスワード認証：許可</li> </ul>
--

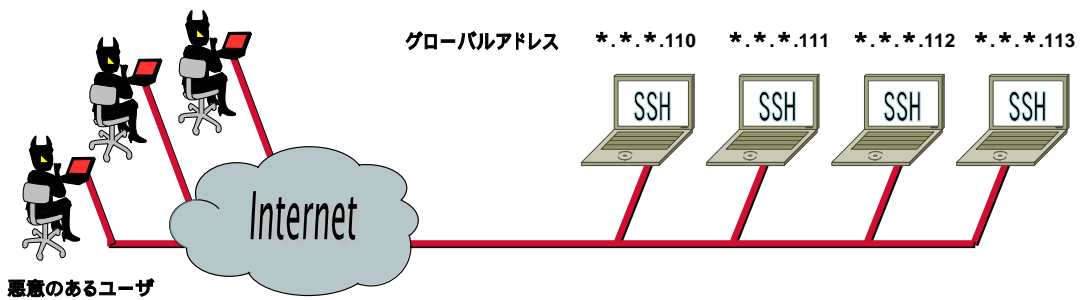


図 2 SSH サービス観測環境

### (1) アクセス状況

SSH サービスに対する接続試行は、24 の国 / 地域、合計 105 の IP アドレスから行われ、試行された認証の総数は、1 サーバあたり 41,456 回、1 日あたり 1,382 回であった。この回数は、SSH サービスが利用可能であるかどうかを確認するポートスキャン行為を除外している。認証行為が行われた発信元国 / 地域別の内訳を図 3 に示す。(発信元 IP アドレスは、攻撃者が存在する場所を確実に特定するものではない。) なお、国内を発信元とする IP アドレスは 8 件あり、試行された認証の総数は 1 サーバあたり 11,575 回、1 日あたり 386 回であった。

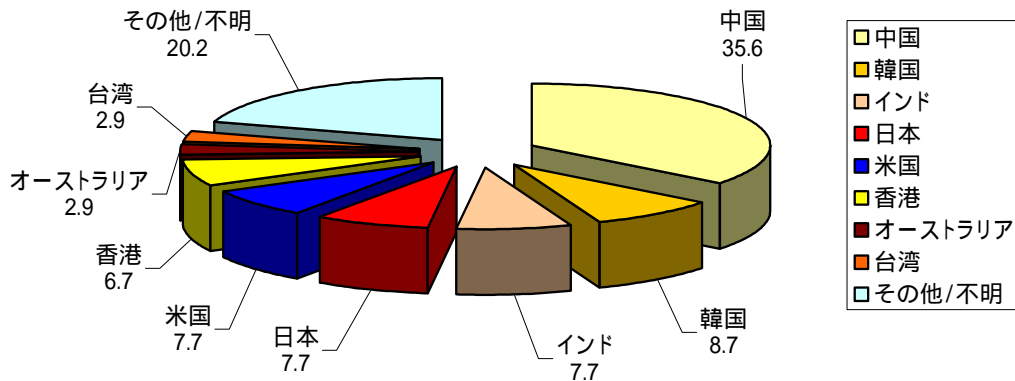


図 3 発信元 IP アドレスの国 / 地域別比率 (%)

今回観測に使用したグローバル IP アドレスは連続する 4 つであり、アクセスログの分析を行った結果は以下のとおりである。

4 つの連続するグローバル IP アドレスを設定した SSH サービスの全てに対して、1 つの発信元 IP アドレスからほぼ同時刻に認証試行を行っている例を多数確認しており、これが全体の約 80%を占めていた。これらの攻撃によって試行されたユーザ名とパスワードが全て一致することから、自動的にサービスの検出・認証試行・侵入を行う攻撃ツールが存在しているものと考えられる。(図 4、図 5)

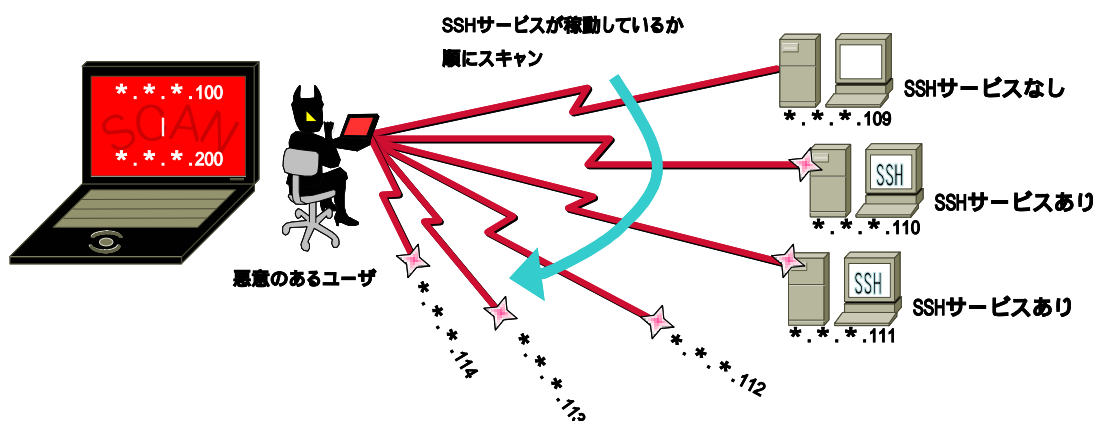


図 4 SSH サービスの検出

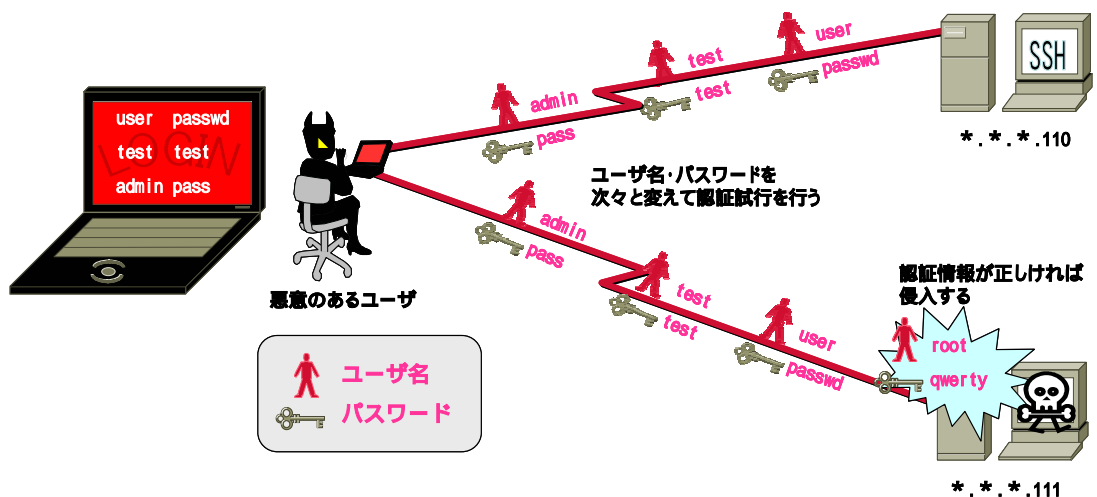


図 5 検出した SSH サービスに対する認証試行・侵入

(2) 試行された認証情報

攻撃者が認証試行に利用したユーザ名とパスワードの傾向は以下のとおりである。

ア 攻撃者が試行したユーザ名

攻撃者が試行したユーザ名の上位 10 位 (1 サーバあたり) を表 2 に示す。システムユーザ名を対象にしている場合が圧倒的に多く、全体の約 50%を占めていた。試行されたユーザ名の中には日本人名と考えられるユーザ名 (アルファベット表記) も複数含まれていた (表 3)。日本人名による試行が国内だけでなく海外からも行われていることから、日本人名を含むユーザ名辞書が海外に広まっているものと考えられる。

表 2 ユーザ名試行回数 (上位 10 位)

順位	ユーザ名	試行回数	全体に占める割合
1	root	6,872	16.576%
2	admin	425	1.025%
3	test	292	0.703%
4	mysql	139	0.334%
5	info	136	0.328%
6	oracle	127	0.305%
7	adam	125	0.302%
8	ftp	123	0.297%
9	postgres	123	0.296%
10	apache	122	0.294%

表 3 日本人名と考えられるユーザ名による試行回数 (上位 10 位)

順位	ユーザ名	試行回数	全体に占める割合
322	nakamura	12	0.028%
322	aki	12	0.028%
333	yoshida	11	0.027%
357	daisuke	10	0.024%
363	keiko	10	0.024%
363	higashi	10	0.024%
369	takashi	10	0.023%
369	koba	10	0.023%
369	ito	10	0.023%
377	takuya	9	0.022%

イ 攻撃者が試行したパスワード

攻撃者が試行したパスワードの上位 10 位（1 サーバあたり）を表 4 に示す。ただし、試行された認証の総数のうちパスワードがユーザ名と同じものが全体の 51.6%を占めた。

表 4 パスワード試行回数（上位 10 位）

順位	パスワード	試行回数	全体に占める割合
1	123456	1,928	4.65%
2	12345	743	1.79%
3	1234	702	1.69%
4	password	600	1.45%
5	test	303	0.73%
6	123	295	0.71%
7	test123	254	0.61%
8	1qaz2wsx	225	0.54%
9	passwd	222	0.54%
10	qwerty	219	0.53%
(参考)	パスワードがユーザ名と同じ	21,388	51.59%

攻撃者が試行したパスワードの文字数の分布を図 6 に示す。6 文字のパスワードが全体の約 25%と最も多く、4 文字から 8 文字のパスワードが全体の約 80%を占めていた。パスワードの平均文字数は 6.3 文字、パスワードの最大文字数は 30 文字<sup>2</sup>であった。

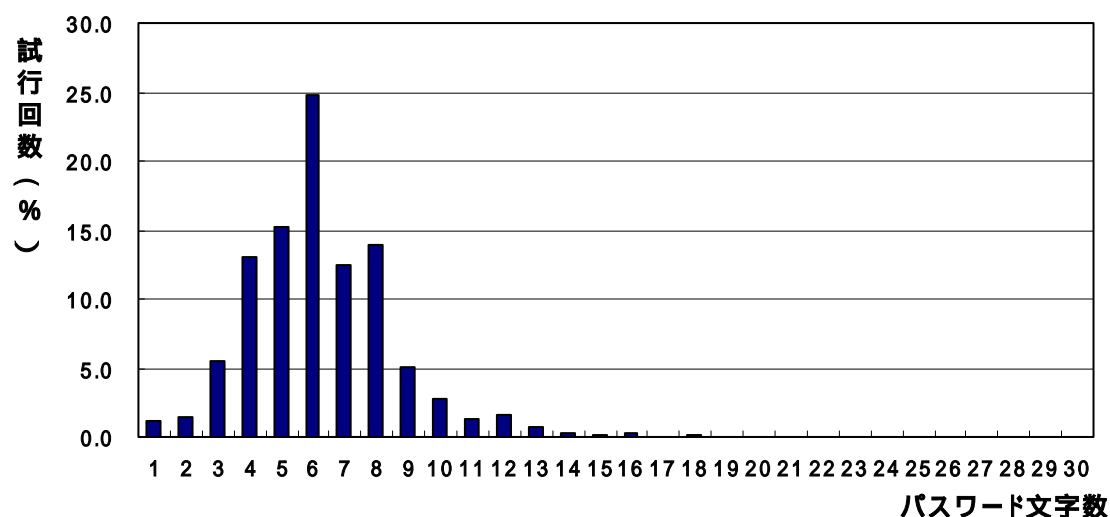


図 6 パスワード文字数の分布

<sup>2</sup> 30 文字のパスワードは”qazwsxedcrfvtgbyhnujmik,ol.p;/”であり、後述するキーボードの配列パターンを利用したものである。

攻撃者が試行したパスワードの傾向は大きく 3 種類に分別することができる。以下では、これらの特徴を述べる。

(ア) 英単語等を列挙したパスワード辞書

試行するパスワードに辞書を利用する。パスワード辞書には、利用されている可能性が高いと考えられている英単語、システムユーザ名、数字の羅列等が列挙されている。実際に攻撃に使用されたパスワード辞書の 1 例を挙げる。

例

```
root
webadmin
admin
shell
linux
test
webmaster
mysql
123456
12345678
password
master
apache
unix
redhat
login
```

(イ) キーボードの配列パターンを列挙したパスワード辞書

試行するパスワードにキーボードの配列パターンを利用する。一見すると複雑なパスワードに思われるが、記憶又は入力するのが容易であるため、実際のパスワードとして使用されている可能性が高く、これを狙ったものと考えられる。実際に攻撃に使用されたキー配列を使用したパスワードを 3 例挙げる。この 3 例とキーボードの配置状況の関係を図 7 に示す。

例 1

1q  
1q2w  
1q2w3e  
1q2w3e4r  
1q2w3e4r5t  
1q2w3e4r5t6y  
1q2w3e4r5t6y7u  
1q2w3e4r5t6y7u8i  
1q2w3e4r5t6y7u8i9o  
1q2w3e4r5t6y7u8i9o0p

例 2

qwe  
qwer  
qwert  
qwerty  
qwertyu  
qwertyui  
qwertyuio  
qwertyuiop

例 3

qaz  
qazwsx  
qazwsxedc  
qazwsxedcrfv  
qazwsxedcrfvgtb  
qazwsxedcrfvgtbyhn  
qazwsxedcrfvgtbyhnujm

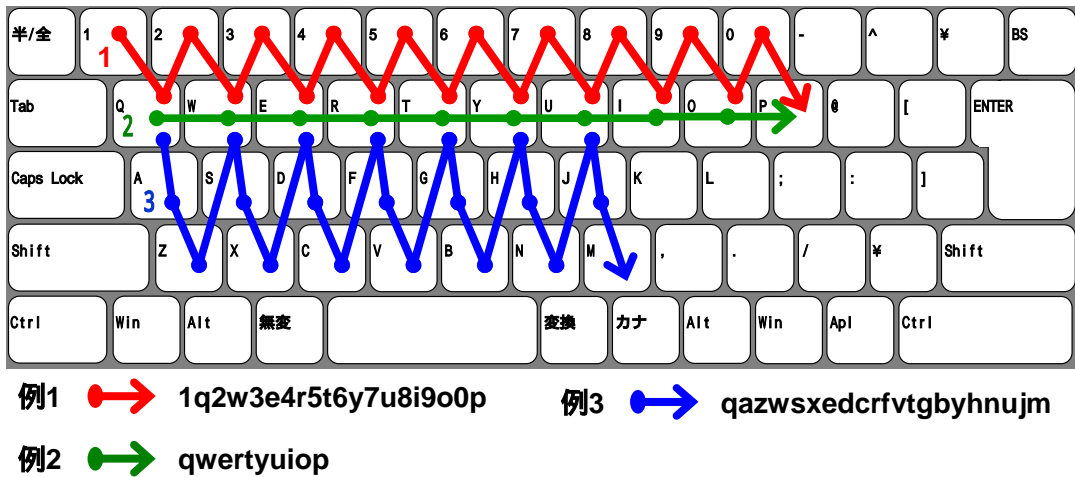


図7 パスワードとキーボードの配置状況

(ウ) 複数パターンの組み合わせ

試行するパスワードに複数のパスワードのパターンを利用する。試行するパスワードには、ユーザ名と同じパスワード、ユーザ名に数字を付加したもの、ユーザ名を逆順に並び替えたもの等がある。実際に攻撃に使用されたパスワードを1例挙げる。

例

ユーザ名 admin に対して試行されたパスワード

- admin
- 1
- 12
- 123
- 1234
- 12345
- admin1
- admin12
- admin123
- password
- passwd
- test
- test123
- nimda

ユーザ名 `guest` に対して試行されたパスワード

`guest`

`1`

`12`

`123`

`1234`

`12345`

`guest1`

`guest12`

`guest123`

`password`

`passwd`

`test`

`test123`

`tseug`

#### 4 対策

今回、調査対象とした攻撃手法は、設定の不備を攻撃するものであり、以下の対策をとることで防ぐことができる。

##### (1) サービスの停止

SSH サービスが不要な場合は、サービスを停止する。

##### (2) 推測されにくいパスワードの選択

本レポートで報告したとおり、安易なパスワードは侵入を容易にしてしまう。そのため、第三者に推測されにくい複雑なパスワードを選択する必要がある。

##### (3) 接続を許可する発信元 IP アドレスの制限

接続を許可する発信元 IP アドレスに制限を設けることで、第三者による攻撃を防ぐことができる。

##### (4) パスワード認証の無効化

パスワード認証を無効化し、公開鍵認証方式を採用することで、パスワードの総当たり攻撃を回避することができる。

## 5 まとめ

今回、SSH サービスに対する攻撃の実態について調査を行うため、環境を構築して観測を行ったところ、不正な接続が多く行われていることを確認することができた。重要なデータを保有していると予測される企業や官公庁等のサーバに対しては、これら無差別的な攻撃に加え、当該組織を狙った不正なアクセスの試みが行われている可能性も考えられる。また、不正な攻撃者に侵入された結果、踏み台等に悪用される危険性があるため、重要なデータが格納されていない等の状況であっても脆弱なサーバを安易にインターネットへ接続してはならない。サーバ管理者の皆様には基本的な情報セキュリティ対策の確認をお願いしたい。

なお、SSH サービスに限らず、パスワードによる認証を要する他のサービスについても、同様の攻撃が行われている可能性があるので注意が必要である。

サイバーフォースセンターでは引き続き観測を行い、警察庁セキュリティポータルサイト @police 「インターネット治安情勢」にて続報を公開する予定である。