

SSH を利用した不正侵入行為

1 日常的に行われる不正侵入行為

警察庁インターネット定点観測システム¹では、本年7月中旬以降、SSH²に対するアクセスを多数検知しており、本年度第1/四半期（4月から6月の間）の検知件数が1,755件であったのに対して、第2/四半期（7月から9月の間）には8,144件と約4.6倍に増加している。

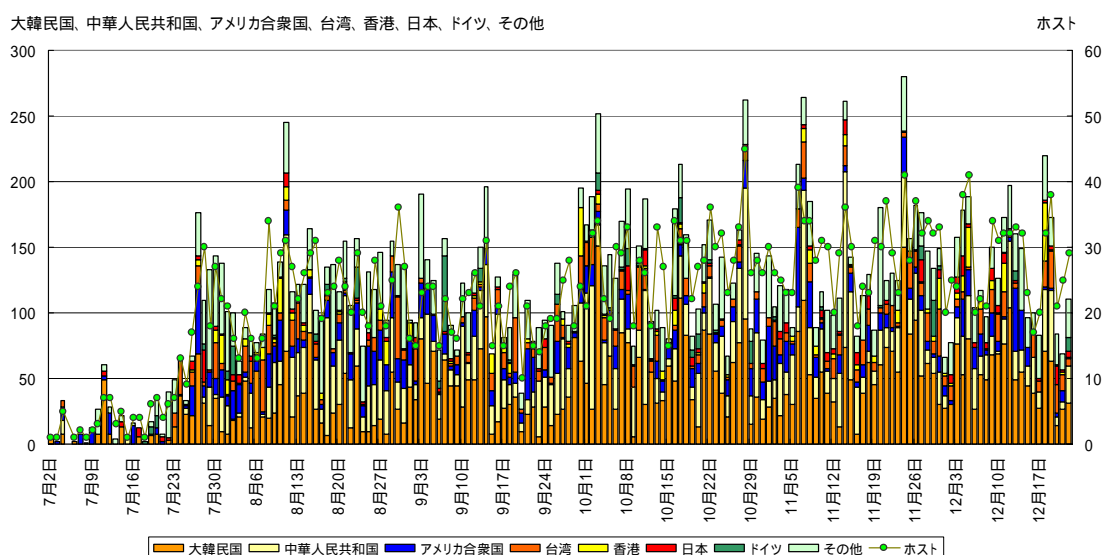


図1 SSH (22/TCP)の検知状況(7月～12月)

同時期にSSH用の辞書攻撃ツールが海外のWebサイトで公開されていることから、同ツールの利用が今回の増加の理由として考えられる。こうした不正侵入行為は以前から行われているが、特に攻撃ツールを利用することで比較的容易に実行することができ、脆弱なサーバはほとんど簡単に侵入を許して悪用されてしまう危険性がある。サーバ管理者は情報セキュリティ対策の徹底を、常に心がける必要がある。

今回、SSHに対するアクセスの詳細な情報を得るために、脆弱なサーバを1台設置して約1か月間観測したところ、合計32回の不正侵入を記録した。以下では、サイバーフォースセンターで観測した不正侵入行為の実態及びその対策について述べる。

¹ <http://www.cyberpolice.go.jp/detect/observation.html>

² SSH (Secure SHell) は主にUNIX系コンピュータで使用されるサービスであり、22/TCPポートを使用する。SSHはネットワークを介して遠隔地のマシンでコマンドを実行することができ、ネットワークを流れるデータは暗号化される。

2 観測結果

(1) 観測環境

サイバーフォースセンターでは、SSH に対して行われている活動を把握するために、専用の監視システム³を用いて観測を行った。以下の内容は、10月1日から31日までの1か月間の観測結果である。

(2) アクセス状況

SSH ポートに対する辞書攻撃は、39か所のIPアドレスから行われ、辞書攻撃に伴うアカウント及びパスワードの試行回数は、合計1,174回であった。この回数は、SSHポート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は除外している。

短時間に同じIPアドレスから数多くのアクセスが観測されており、攻撃者の多くは自動化された辞書攻撃プログラムを用いていると考えられる。発信元国別の内訳を図2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ものは無かった。

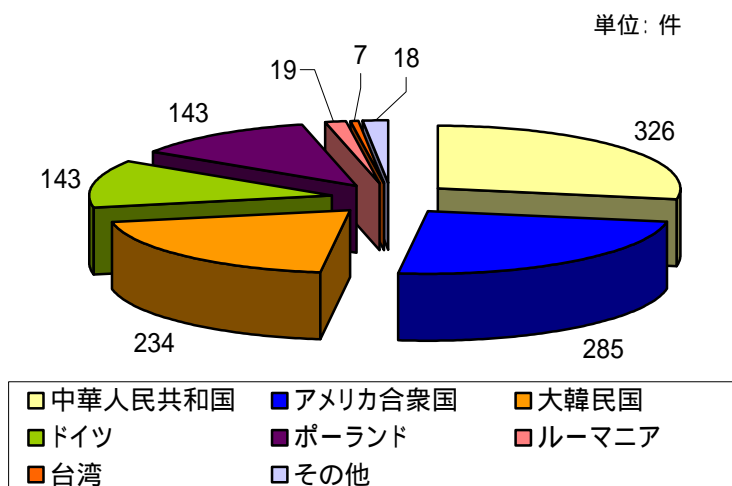


図 2 発信元 IP アドレスの国別比率

辞書攻撃が行われた回数及び発信元 IP ホスト数の推移を日毎に集計した結果を図3に示す。

³ 一般にこのようなシステムはハニーポットと呼ばれている。今回はサービスプロバイダが提供する一般的な利用者の環境(IPアドレスは1個)で観測を行った。

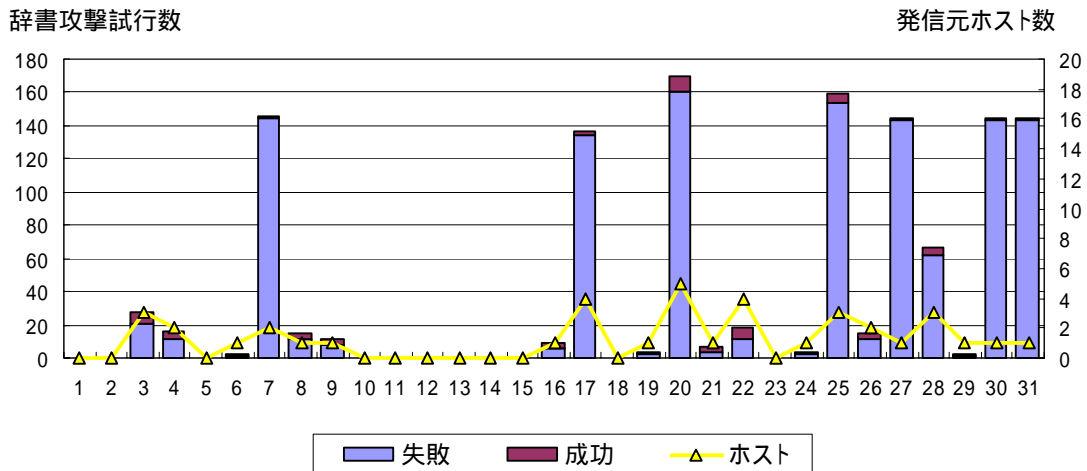


図3 辞書攻撃回数と発信元ホスト数の推移（10月1日～31日）

(3) 侵入状況

攻撃の対象となったアカウント別の割合を図4に示す。最も攻撃されたアカウントは、Unix系OSの管理者アカウントである「root」であり、全体の約4割を占める。また、図の「その他⁴」にはサーバアプリケーション等で作成されるアカウントも確認された。試行されたパスワードとしては、アカウントと同一のものや、単に「password」といった安易なものが観測されている。

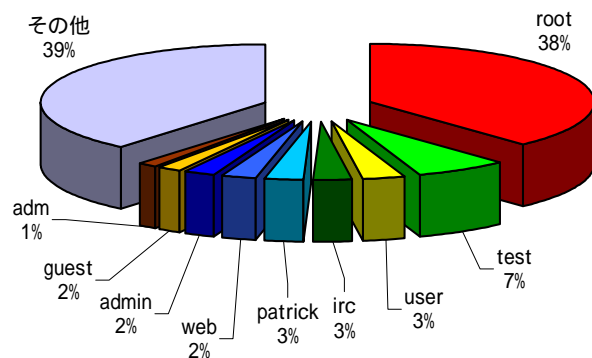


図4 アカウント別攻撃比率

今回の観測では、あらかじめアカウントとして「test」、「user」、「admin」の3つを作成し、パスワードは辞書攻撃を容易にするためにアカウントと同じものとし

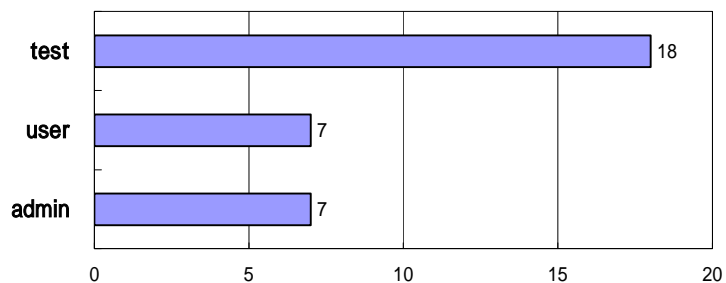


図5 アカウント別再侵入件数

⁴ その他には「adm, apache, cyrus, horde, iceuser, jane, matt, mysql, pamela, rolo, www, www-data, wwwrun, account, adam, alan, backup, cip51, cip52, cosmin, data, frank, master, noc, oracle, server, sybase, webmaster, george, henry, john, nobody, operator, tes」などが含まれる。

た。観測期間中、辞書攻撃に成功した後、そのアカウントを用いて再接続してきた件数の内訳を図5に示す。実際に観測システムへ侵入した回数は32回であった。

(4) 侵入者の行動

観測システムに侵入後、入力されたコマンドの内訳を図6に示す。「wget」、「ftp」、「lynx」、「curl」といったファイル転送に用いられるコマンドが数多く占めており、外部からのツール類のダウンロードを目的とする行為が観測された。また、「cat」、「uname」、「w」、「ps」、「cd」などUNIX系OSの標準的なコマンドも実行されている。全般的な傾向として、侵入者の多くは、簡単に観測システム内の状況を確認した後、各種ツール類のダウンロードを試みている。⁵

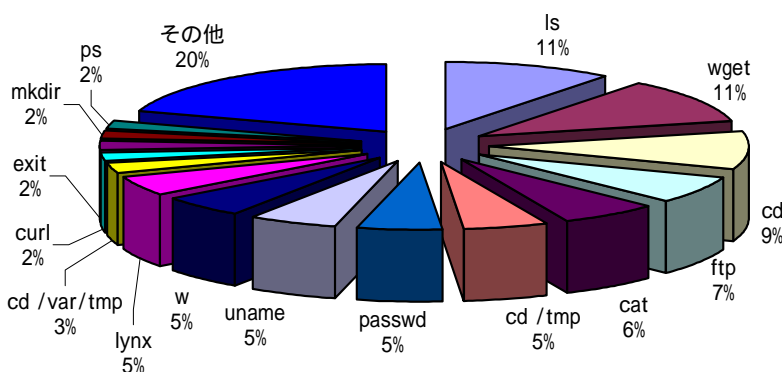


図6 侵入後に実行したコマンドの内訳

侵入者がダウンロードを試みたファイルを調査したところ、大きく次の三種類に分類できた。

- ア 管理者権限を奪取するためのツール（ルートキットを含む）
- イ SSH 辞書攻撃ツール、DDoS ツール
- ウ IRC（インターネット・リレー・チャット）に関するツール

これらのツールを観測システム侵入後に持ち込もうとした行動から、侵入者の目的をある程度推測することができる。「ア」は侵入したコンピュータを自由に操作するため、管理者権限を奪おうとするものである。「イ」は別のコンピュータを攻撃するために、侵入したコンピュータを踏み台やツール保管場所として利用するためと考えられる。「ウ」については侵入したコンピュータ上でIRC通信を中継するツール等が確認された。IRCを

⁵ 今回の観測環境では、侵入者はコンピュータを一般利用者の権限で自由に操作できるが、外部ネットワークに対するアクセスはファイアウォールで制限した。

利用する不正プログラムの1つとして Botnet⁶が世界的に広まっていることから、何らかの関連性があるものと推測され、今後動向を注視する必要がある。

3 対策

今回の事象は、アプリケーション・OSの脆弱性や欠陥を突くものではないことから、対策としては以下のことを再確認することで攻撃を防ぐことが可能である。

- (1) SSH サービスを使用していない場合は、サービスを停止する。
- (2) root によるログインを許可しない。(telnet では root ログインが不可であるのに対して、SSH では root ログインをデフォルトで許可している場合が多い。)
- (3) 安易なパスワードを設定しない。(サーバアプリケーション等が作成するアカウントを含むすべてのユーザに徹底する。)

その他、SSH 接続を許可する発信元 IP アドレスを限定することや、パスワード以外に証明書を用いた認証を行うなど、利用環境に応じて様々な対策が存在する。

4 まとめ

今回、SSH サービスを稼働した脆弱なサーバをインターネットに接続してアクセス状況の観測を行った。現在もこの観測は継続して行っており、12月下旬においても同様のアクセス傾向が確認されている。今回は特に周知のサービスを提供していない利用環境下であったが、公官庁や企業等のサーバに対してはさらに数多くのスキャン行為が行われているものと推測される。また、「重要なデータが格納されていないから」という理由で脆弱なサーバを安易にインターネットへ接続すると、悪用される危険性もあることから、サーバ管理は厳格に行う必要がある。今後、被害を防ぐためにもサーバ管理者には基本的な情報セキュリティ対策の確認を今一度お願いしたい。

サイバーフォースセンターでは引き続き同様の観測を継続し、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」にて続報を公表する予定である。

⁶ bot に感染したコンピュータは、各種脆弱性スキャン、スパム送信、DoS 攻撃等、様々な攻撃を外部から遠隔操作で実行させられてしまう。bot はコンピュータウイルスで感染する他、bot 自身にも感染機能を有するものがある。遠隔操作は主に IRC チャンネルが用いられ、bot で構築されたネットワークを Botnet と呼ぶ。bot 系のワームは、数多く存在しているが、一例として Gaobot が挙げられる。複数の脆弱性を悪用する Gaobot ワームについて(http://www.cyberpolice.go.jp/detect/pdf/report_gaobot.pdf)