管理サービス（SSH、FTP）に対するパスワード推測攻撃

NTT コミュニケーションズ株式会社
マネージドセキュリティサービス推進室
2013 年 12 月 25 日

NTT Communications Corporation
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo
100-8019, Japan

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

Table of Contents

1 概要

ユーザー名とパスワードが攻撃者の手に渡ってしまうと、攻撃者は正規のユーザーの権限でそのシステムやサービスを正面から利用することができる。そのためパスワードは攻撃者にとって非常に価値のある情報である。このパスワードを入手するための手段のひとつとして、パスワードとなりうる全ての候補を試すブルートフォース攻撃や、よく利用されるパスワードを試す辞書攻撃が行われる。これらの攻撃はパスワード推測攻撃と呼ばれる古典的な攻撃手法であるが、サービスを不特定多数のユーザーが利用できるよう公開している場合、日常的といっても過言でないほど攻撃者にとって攻撃の対象となるため、管理者は注意と対策が必要である。

本レポートでは、リモートから行われる SSH と FTP のパスワード推測攻撃（オンライン攻撃）について、NTTCom グループの GROC（Global Risk Operation Center）での検知状況と、サーバー管理者が行うべき対策をまとめた。

2 GROC での検知状況

2.1 SSH に対するパスワード推測攻撃

SSH（Secure SHell）はリモートのユーザーに対してコンピューターの制御機能（シェル）を提供するプロトコルおよびサービスであり、コンピューターをリモートから管理する際に利用される。SSH のアクセス権を入手すると、そのユーザーの権限でコンピューターを自由に操作することができる。

2013 年 4 月 1 日から 9 月 30 日における SSH に対するパスワード推測攻撃のアラート検知件数を表 1 と図 1 に示す。

表 1 SSH に対するパスワード推測攻撃の総計

期間	2013 年 4 月 1 日 ～ 9 月 30 日
サイト数	15 サイト
アラート検知数	5,012,600 件
アラート検知数（1 日・1 サイト換算）	1,826 件

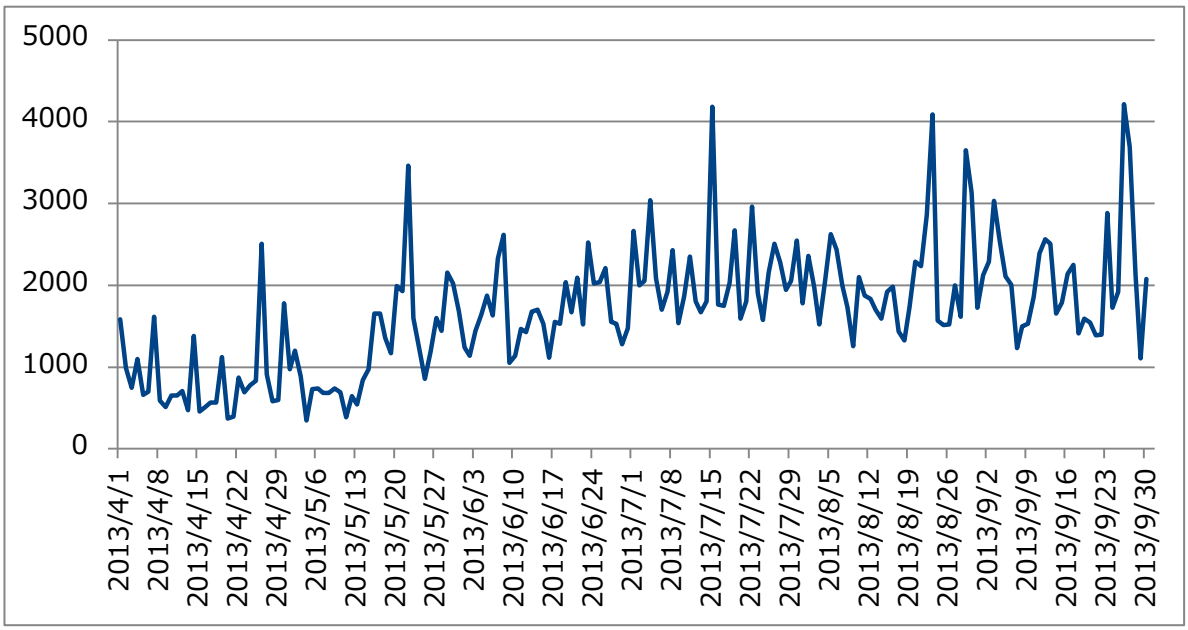

図 1 SSH に対するパスワード推測攻撃の検知数の推移

このアラート検知数は SSH サービスを不特定多数に公開している 15 サイトについての集計である。6 ヶ月間において合計 5,012,600 件の攻撃を検知しているが、これは 1 サイトあたり毎日 1,826 件の攻撃を検知していることを意味する。この結果から、不特定多数に公開している SSH サービスでは日常的にパスワード推測攻撃を受けていることが分かる。

2.2 FTP に対するパスワード推測攻撃

FTP（File Transfer Protocol）はリモートのユーザーに対してファイル転送機能を提供するプロトコルおよびサービスであり、Web サイトのコンテンツなど、コンピューター上のファイルを管理する際に利用される。FTP のアクセス権を入手すると、そのユーザーの権限でファイルにアクセスすることができる。

2013 年 4 月 1 日から 9 月 30 日における FTP に対するパスワード推測攻撃のアラート検知件数を表 2 と図 2 に示す。

表 2 FTP に対するパスワード推測攻撃の総計

期間	2013 年 4 月 1 日 ～ 9 月 30 日
サイト数	19 サイト
アラート検知数	2,170,342 件
アラート検知数（1 日・1 サイト換算）	624 件

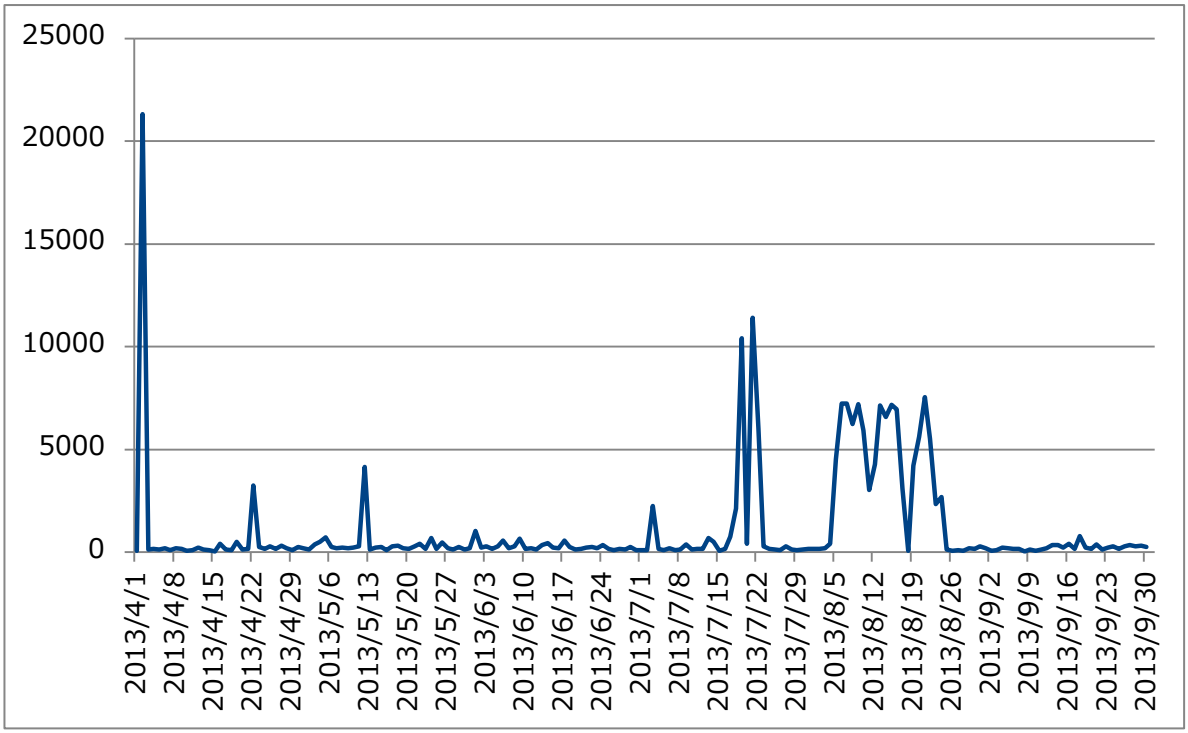

図 2 FTP に対するパスワード推測攻撃の検知数の推移

このアラート検知数は FTP サービスを不特定多数に公開している 19 サイトについての集計である。6 ヶ月間において合計 2,170,342 件の攻撃を検知しているが、これは 1 サイトあたり毎日 624 件の攻撃を検知していることを意味する。この結果から、不特定多数に公開している FTP サービスでは日常的にパスワード推測攻撃を受けていることが分かる。

また、FTP に対するパスワード推測攻撃で攻撃対象となったユーザー名のトップ 10 は表 3 のとおりであった。システム導入時に設定されるデフォルトのユーザー名などを中心に、一般的に利用される可能性の高いユーザー名が攻撃対象となりやすいことが分かる。

表 3 FTP に対する攻撃対象となったユーザー名のトップ 10

No.	アカウント名	件数
1	Administrator	188,570
2	upload	113,728
3	admin	81,458
4	user	73,229
5	webmaster	72,244
6	root	71,706
7	Guest	71,023
8	web	70,067
9	ftpuser	69,520
10	adm	67,510

3 対策

攻撃者はインターネット上の無作為に選んだホストに対して、22/tcp（SSH）や 21/tcp（FTP）などの TCP ポートにハンドシェイクを試みることで管理サービスの探索を行い、発見した管理サービスに対してパスワード推測攻撃を仕掛けることがある。管理サービスに対するパスワード推測攻撃は日常的に行われ、認証を突破された際の影響も大きいため、十分に注意する必要がある。本章では代表的な管理サービスである SSH と FTP について対策を記載するが、他の管理サービスについても考え方は同様である。

3.1 根本的対策

パスワード推測攻撃は攻撃を受けた際に対策をするのではなく、いつ攻撃を受けても問題がないように、日ごろの運用の中でチェックして対策することが重要である。パスワード推測攻撃に対する基本的な対策は、十分な強度を持ったパスワードを設定し、さらにアクセス可能なユーザーを制限することである。

根本対策 1：十分な強度を持ったパスワードを設定する

十分な強度を持ったパスワードとは、攻撃者に推測されにくいパスワードであることを意味する。大小文字、数字と記号を混在させた十分に長い文字列で、辞書に載っているものや一般的に利用される単語ではなく、さらに他のシステムで使用していないパスワードを設定する。ランダムで長い文字列をシステム毎に設定することが理想的である。

根本対策 2：アクセスする送信元 IP アドレスを制限する

加えて、特定の IP アドレスからのみ管理サービスにアクセスできるようファイアウォールや VPN（Virtual Private Network）接続などで制限をかけることで、不特定の攻撃者が管理サービスに対してパスワード推測攻撃を行うことを防ぐことが重要である。たとえパスワード推測攻撃以外の手法でパスワードが漏えいした場合であっても、送信元 IP アドレスが制限されている場合はこのパスワードを利用することができないため、パスワード推測攻

撃を含む不正ログイン全般に対して非常に有効な対策である。逆に、アクセスする送信元 IP アドレスを制限できない場合は、パスワード推測攻撃や不正ログインの対象となりうることを認識して別途対策を講じる必要がある。

その他に、原始的なパスワード認証以外の認証方法を利用することも、根本対策として有効である。

根本対策 3：公開鍵認証を利用する

SSH ではパスワード認証ではなく公開鍵認証方式を利用することで、不特定多数のホストに対するパスワード推測攻撃を根本的に防ぐことができる。ただし、秘密鍵が漏えいした場合はやはり不正ログインのリスクが発生するため、秘密鍵を格納するクライアントのセキュリティや秘密鍵自体に設定するパスフレーズの強度にも気をつけなければならない。

根本対策 4：ワンタイムパスワードを利用する

ワンタイムパスワードを利用することで、パスワード推測攻撃を根本的に防ぐことができる。2 段階認証を提供するサービスと連携することで、SSH などの認証にワンタイムパスワードを簡単に導入することができるが、外部サービスに依存するためサービスの継続性が第三者に依存することがデメリットである。

[参考] google-authenticator (http://code.google.com/p/google-authenticator/)

3.2 保険的対策

根本対策以外にも、併せて実施することでさらにセキュリティを高めることができる保険的対策について紹介する。

保険的対策 1：TCP ポートをデフォルトから変更する

攻撃者は無作為に選んだホストに対して管理サービスが動作しているかチェックを行い、管理サービスの動作を確認できたホストに対してパスワード推測攻撃を行うという手順を踏む場合がある。このような攻撃者は、効率的に探索を行うために管理サービスとしてよく利用される TCP ポートのみをチェックすることがほとんどである。そこで、管理サービスの TCP ポートをデフォルトから変更することで身を隠すことができる。例えば、SSH の場合はデフォルトの 22/tcp から 50022/tcp に変更するだけでも攻撃の頻度は大幅に緩和される。ただし、特定の標的を狙いポートスキャンを行って時間をかけて調べれば、管理サービスの存在が見つかってしまうため、根本的対策とはなりえない。

さらに、ポートノッキングを利用して管理サービスが開く TCP ポートを隠ぺいすることができる。通常時は隠ぺいしたいサービスの TCP ポートを閉じておき、ユーザーがサービスを利用する際に事前に取り決めた特定の TCP もしくは UDP ポートに対するパケットを送信させることで、その直後のみ目的のサービスの TCP ポートを開くという手法である。通信を盗聴された場合にこの対策は無意味となるため過信はできないが、外部からの管理サービスの隠ぺいの手段としては強力である。

保険的対策 2：認証試行回数の制限

連続して認証試行を失敗した場合にユーザーアカウントを一時停止することも対策となりうる。ただし試行回数の制限内でパスワードを推測された場合や、別の理由でパスワードが漏えいした場合には認証を突破されてしまうため、根本的対策とはなりえない。また、正規のユーザーがパスワードを忘れて試行した場合にも一時停止されることになるため、利便性を損なうこともデメリットである。

保険的対策 3：定期的なログ確認

攻撃自体を防ぐことはできないが、定期的にログを確認することで、攻撃が成功してしまったことを事後に発見することができる。ただし、ログが改ざんされないよう別のホストでログを保管するなどの工夫が必要である。根本対策とはなりえないが、ログの確認はパスワード推測攻撃に限らずセキュリティを維持するために重要であるため、定期的にチェックすることが望ましい。

最後に、パスワード推測攻撃と直接的には関係しないが、管理サービスにはセキュアなプロトコルを利用することも重要である。例えば、FTP の通信は平文で行われ、盗聴された場合にパスワードやファイルの内容が漏えいする。アクセス先のサーバーが正しいかどうか確認するための認証機能もない。そのため、SFTP や FTPS などセキュアなプロトコルを利用することを強く推奨する。

4 本レポートについて

4.1 レポート作成者

NTT コムセキュリティ株式会社
オペレーション＆コンサルティング部
羽田 大樹

4.2 履歴

2013 年 12 月 25 日（ver1.0）：初版公開

4.3 お問い合せ

NTT コミュニケーションズ株式会社
経営企画部 マネージドセキュリティサービス推進室
E-mail: scan@ntt.com

以上