Asterisk PBX 不正利用防止

不正アクセス対策環境の構築

ICTR120716-OR01A

Info Circus,Inc.

目次

第 1 章

はじめに

最近、Asterisk PBX の SIP を狙った不正アクセスが多発しています。被害の多くは、インターネット経由で Asterisk の内線端末になりすまし電話回線を乗っ取り、国際電話を大量にかけるというものです。内線端末の乗っ取りに気がつくのが遅れてしまうと、国際電話による通話料が発生したり、電話回線の不正利用など被害が発生します。

フュージョン・コミュニケーションズ株式会社 様が、不正アクセスに対しての対策[*1]を紹介されています。

また、弊社 オフィス電話/IP 電話システムでは、不正アクセスに対する対応を実装済みとなります。

このたび、Asterisk PBX をご利用のユーザー様が、不正アクセスによる同様の被害に遭われないため、弊社実装の対策スクリプトを汎用的に使用できるように変更したものを公開いたします。

本文章に記載されている内容は、作成時点で有効な文章となります。今後の不正アクセスに対しての保証はありません。

また、文章に記載の不正アクセス対策は、間違った設定を行うと IP 電話通信ができなくなる恐れがあります。対策に不安な方は十分に試験を実施するか、弊社までお問い合わせください。

[*1] http://www.asterisk-fusion.jp/illegal-access.html

第 2 章

IP-PBX 不正アクセスの概要と一般対策

近年、オープンソースソフトウェア Asterisk を使用した IP-PBX の事例が多くなりました。しかし、インターネット上で公開されている情報は、基本的な設定のみを説明しており、実運用の問題点や運用のための注意点が記載されていないことがあります。

実運用する場合には、Asterisk の設定などをよく確認し運用する必要があります。公開されている設定情報をコピー＆ペーストすることにより、動いているように見えても設定の不備により外部 (社外) から不正に電話回線を使われ、高額な通話料が請求される事例が発生しています。

本文章は、Asterisk に特化し 外部から SIP アカウントを乗っ取られないようにするための防衛スクリプトをまとめたものです。

2.1　設定ファイルのコピー＆ペーストの危険性

弊社の環境では、ここで紹介しているスクリプトを導入し、どのようなアクセスがあるかを記録しています。

外部からの不正アクセスで確認できたパターンは次のようなものです。

1000 9999 までの総当たり　SIP アカウント 1000 から始まり ９９９９ まで、単純なパスワードで認証を送りつける方法です。海外のサーバーからの不正アクセスでよく見るパターンです。

5088,100,6501 など特定番号への不正アクセス　特定の番号で認証パスワードも決めうちで不正アクセスを試みる方法です。国内の乗っ取られたと思われるサーバーなどからのアクセスが多く見られるパターンです。

特に 2 番目のパターンは、サンプルファイルにあるアカウントやインターネット上で公開されているサンプル・ファイルで指定している SIP アカウントとパスワードで攻撃をかけてきていました。

本文章のスクリプトを使用する前に、SIP アカウントが次のような状態にないかを確認してください。

- Asterisk のサンプルアカウントが残っていないかを確認する
- インターネット上のサンプルをコピー＆ペースとしたアカウントが存在しないかを確認する
- **SIP** アカウントのパスワードが十分に複雑なものであるかを確認する

第 3 章

IP-PBX 不正アクセス防止環境の構築

IP-PBX の端末を乗っ取る場合、攻撃者は最初に内線番号の走査ならびに認証処理を大量に送りつけてきます。本文章で説明する不正アクセス防止スクリプトは、この最初の内線番号の走査と不正な認証処理をアクセスログから検出し、該当の IP アドレスからの接続を拒否するのが基本動作となります。

- SIP の不正アクセスしてきた リモートホストを自動で検出
- リモートホストのアドレスからの UDP/IP の通信を遮断
- 事故防止のため、プライベート IP アドレスは接続を許可

これにより グローバル IP アドレス (社外のネットワーク) からの 不正な端末番号の走査や認証を防ぎ、不正に回線を利用されてしまう被害を食い止めます。

本対策では、一番多く使用されていると思われる CentOS での対策手順を紹介します。他の Linux ディストリビューションでも同じ方法による対策が可能ですが、それぞれの Linux ディストリビューションならびに Solaris,BSD OS などについては適時読み替えてください。

3.1 環境について

本文章での不正アクセス防止は、次の環境を前提として説明しています。

- CentOS 5.3
- perl 5.8 以上インストール済み
- iptables インストール済み
- Asterisk 1.4 系

本不正アクセス防止スクリプトでは、iptables など TCP/IP 通信に関係するコマンドを使用します。設定を間違えると通信できなくなりますので、十分に注意し試験を実施してから導入してください。

3.2 アクセスログ検出の準備

アクセスログの検出として、 swatch というオープンソースソフトウェアを使用します。 swatch は、指定したシステムのログファイルを監視し、特定のパターンにマッチした場合に、コマンドを実行する機能を提供しています。

3.2.1 swatch のインストール

関係するモジュールのインストール

```
# perl -MCPAN -e shell
cpan> install Bit::Vector
cpan> install Date::Calc
cpan> install File::Tail
cpan> install Time::HiRes
cpan> install Date::Parse
cpan> exit
```

swatch のインストール

swatch の最新版は http://sourceforge.net/projects/swatch/ から取得し設置します。

```
# wget http://downloads.sourceforge.net/swatch/swatch-3.2.3.tar.gz
# tar xfvz swatch-3.2.3.tar.gz
# cd swatch-3.2.3
# perl Makefile.PL
# make
# make test
# make install
```

3.2.2 swatch の設定

```
# mkdir -p /etc/swatch/protector
# cd /etc/init.d
# wget http://www.infocircus.jp/tech/protect/swatch.txt
# mv swatch.txt swtach
# chmod +x /etc/init.d/swatch
# chkconfig --add swatch
# chkconfig swatch on
```

3.3 不正アクセス防止 スクリプトの設置

swtach の起動が確認できたら、Asterisk 不正アクセス防止のスクリプトを設置します。

```
# vi /etc/swatch/asterisk.conf
----- Begin asterisk.conf -----
# logfile /var/log/asterisk/messages
watchfor /No matching peer found/
        pipe /etc/swatch/protector/asterisk-blocker.pl

watchfor /Wrong password/
        pipe /etc/swatch/protector/asterisk-blocker.pl
----- End asterisk.conf -----
# cd protector
# wget http://www.infocircus.jp/tech/protect/asteriak-blocker.txt
# mv asterisk-blocker.txt asterisk-blocker.pl
# chmod +x asterisk-blocker.pl
```

3.4　不正アクセス防止スクリプトの起動

スクリプトの動作検証が完了したら、以下のコマンドにより swatch を起動します。

```
# /etc/init.d/swatch start
```

これにより Asterisk PBX に不正アクセスしてきた攻撃者の通信を自動でブロックし不正利用を防ぐことができるようになります。

3.5　日々の運用について

不正アクセス防止スクリプトを実行すると自動的に攻撃者の不正利用を防ぎますが、ブロックする IP アドレスが多くなるとサーバーの動作が遅くなることがあります。定期的に確認し、一定期間が過ぎたら古いアクセス制御を削除していく運用が必要です。

3.5.1　不正アクセスしてきた IP アドレスを削除して問題ないのか

不正アクセスしてきた IP アドレスを削除し通信できる状態にしても問題ないでしょうか? 攻撃者の多くは、使用するグローバル IP アドレスを頻繁に変更してアクセスしてきます。また、ウィルスに感染したコンピューターを利用してアクセスする場合もあります。

これらの攻撃は、一定期間攻撃対象のサーバー (不正アクセス対策したサーバーになります) にアクセスできないと、不正アクセスできないサーバーであると判断し攻撃対象から外し違うサーバーを攻撃します。

アクセス制御に登録して 2,3 日経過した場合には、ほとんどアクセスは無くなります。一方、不正アクセスの IP アドレスを記録した iptables のエントリが増えると、サーバーの計算量が多くなり、サーバーが遅くなっていきます。

このため、定期的なクリーニングが必要となります。もし、同じアドレスから再度攻撃を受けた場合には、

スクリプトが自動で通信を遮断しますので問題ありません。

3.6 IP-PBX 不正アクセス防止スクリプトについて

asterisk-protector.pl は、内線番号がマッチしない時と認証ができない場合に swatch から起動するスクリプトです。asterisk-protector.pl は、アクセス元のグローバル IP アドレスを確認し、iptables の実行コマンドを作成します。

実行コマンドの生成例

```
$ cat /var/log/asterisk-block.log
/sbin/iptables -A INPUT -p udp -s xxx.xxx.xxx.xxx -j DROP
```

作成する実行コマンドは、不正アクセスしてきたグローバル IP アドレスからの udp 通信すべてを拒否 (DROP) します。これにより不正アクセス元は、SIP 通信を含めたすべての UDP/IP 通信ができなくなります。

3.7 不正アクセス防止スクリプトの扱いについて

ダウンロードしたスクリプトは、自動で iptables コマンドを実行します。iptable の実行コマンド形式のログが、/var/log/block-asterisk.log に記録されます。うまく動くことが確認できるまでは 20 行目の `$exec` の行を # でコメントアウトして運用することをお勧めします。定期的に block-asterisk.log を確認し、コマンドを実行すれば 手動でブロックすることができます。

付録 A

設定ファイル

本文章に掲載の設定ファイルは、サンプルです。
最新の設定ファイルは、文章中のサーバーから取得してください。

A.1 /etc/swatch/protector/asterisk-blocker.pl

```
#!/usr/bin/perl
use strict;

my $log='/var/log/block-asterisk.log';

my $iptables = '/sbin/iptables';
my $input = <STDIN>;
if( $input =~ /\[.+\].+\' failed for \'(.+)\' - .*/ ){
  my $addr = $1;
  my @c =
    ( $addr =~ /^([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})$/ );
  my $dec = $c[0]*(256**3)+$c[1]*(256**2)+$c[2]*(256)+$c[3];
  if( ( 167772160 <= $dec and $dec <= 184549375 ) or
      ( 2886729728 <= $dec and $dec <= 2887778303 ) or
      ( 3232235520 <= $dec and $dec <= 3232301055 ) ){
    exit 1;
  }

  my $exec = "$iptables -A INPUT -p udp -s $addr -j DROP";
  `$exec`;
  open LOG, ">>$log";
  print LOG "$exec\n";
  close LOG;
}
```

```
exit 0;
```

A.2 /etc/init.d/swatch

```
#!/bin/bash
#
# swatch
#
# chkconfig: 2345 90 35
# description: swatch start/stop script

# Source function library.
. /etc/rc.d/init.d/functions

PATH=/sbin:/usr/local/bin:/bin:/usr/bin

mkdir -p /var/log/swatch

start() {
    # Start daemons.
    ls /var/run/swatch_*.pid > /dev/null 2>&1
    if [ $? -ne 0 ]; then
        echo -n "Starting swatch"
        pno=0
        for conf in /etc/swatch/*.conf
        do
            pno=‘expr $pno + 1‘
            WATCHLOG=‘grep "^# logfile" $conf | awk ’{ print $3 }’‘
            swatch --config-file $conf --tail-file $WATCHLOG \
            --script-dir=/tmp --awk-field-syntax --use-cpan-file-tail --daemon \
            --pid-file /var/run/swatch_$pno.pid \
            >> /var/log/swatch/swatch.log 2>&1
            RETVAL=$?
            [ $RETVAL != 0 ] && return $RETVAL
        done
        echo
        [ $RETVAL = 0 ] && touch /var/lock/subsys/swatch
        return $RETVAL
```

```
    else
        echo "swatch is already started"
    fi
}

stop() {
    # Stop daemons.
    ls /var/run/swatch_*.pid > /dev/null 2>&1
    if [ $? -eq 0 ]; then
        echo -n "Shutting down swatch"
        for pid in /var/run/swatch_*.pid
        do
           kill $(cat $pid)
           rm -f $pid
        done
        echo
        rm -f /var/lock/subsys/swatch /tmp/.swatch_script.*
    else
        echo "swatch is not running"
    fi
}

status() {
    ls /var/run/swatch_*.pid > /dev/null 2>&1
    if [ $? -eq 0 ]; then
        echo -n "swatch (pid"
        for pid in /var/run/swatch_*.pid
        do
           echo -n " `cat $pid`"
        done
        echo ") is running..."
    else
        echo "swatch is stopped"
    fi
}

case "$1" in
  start)
        start
        ;;
```

```
  stop)
        stop
        ;;
  restart)
        stop
        start
        ;;
  status)
        status
        ;;
   *)
        echo "Usage: swatch {start|stop|restart|status}"
        exit 1
esac

exit $RETVAL
```

参考文献

[1] セキュア・プログラミング講座
http://www.ipa.go.jp/security/awareness/vendor/programming/index.html IPA/セントラル・コンピュータ・サービス株式会社

[2] セキュア Web プログラミング
http://www.trusnet.com/secinfo/docs/webprog1/index.html セントラル・コンピュータ・サービス株式会社

[3] Web アプリケーションに潜む セキュリティホール
http://www.atmarkit.co.jp/fsecurity/rensai/webhole01/webhole01.html @IT

[4] JPCERT/CC
http://www.jpcert.or.jp/ 有限責任中間法人 JPCERT コーディネーションセンター

[5] 実践 ネットワークセキュリティ監査 - リスク評価と危機管理
ISBN4-87311-204-4 オライリー・ジャパン

[6] セキュリティウォリア - 敵を知り己を知れば百戦危うからず
ISBN4-87311-198-6 オライリー・ジャパン

Asterisk PBX 不正利用防止

作成者　インフォサーカス・インコーポレイテッド
住所　東京都港区海岸 1-2-3 汐留芝離宮ビルディング 21 階
文章番号　ICTR120716-OR01A

電子メールお問い合わせ先: info@infocircus.jp