IoT時代のコモンセンス！知らなかったで済まされない　ご購入はこちら

自宅Raspberry Piサーバを不正アクセスから守る方法

後編　おすすめのオープンソース不正アクセス遮断ソフトBan4ip

蕪木 岳志

読者の中には自宅にあるRaspberry Piを，インターネットからアクセスできるように，つまりサーバとして動作させている方も少なからずいらっしゃると思います．前回（2017年2月号）はRaspberry Piへの不正アクセスを，ログをチェックすることで検出する方法を紹介しました．今回は不正アクセスへの対策に使えるオープンソース・ソフトウェアBan4ipを紹介します．

不正アクセス遮断（BAN）ソフトBan4ip

● 特徴…オープンソースでIPv6対応

Ban4ipは簡単なインストールと設定で，IPv4だけでなくIPv6でのパスワードクラックや不正なアクセスもBAN（禁止）してくれる便利なソフトウェアです（**図1**）．

筆者が十年以上運用しているMyDNS.JPの基本技術（!?）である，各種ログから必要データを抜粋する，という仕組みを使用していますので，実績も十分です．

記述言語はPHPで，他に主要な機能として，fail2banも使っているSQLite 3や，inotifyを利用しています．特殊な機能は使用していないので，大抵のLinuxディストリビューションで（大きな変更もなく）動作しています[注1]．

● 機能1…各種エラーを頻発するIPアドレスを遮断（BAN）

sshdなどの認証エラーを起こしている接続元IPをログで確認すると，本当に世界中からやってきます[注2]．Ban4ipはログの中にパスワードエラーを示す文字列があり，同じアクセス元IPアドレスからの接続がある一定回数を超えたかどうかをカウントします．そしてアクセス元IPアドレスがIPv4ならiptablesで，IPv6ならip6tablesで，Ban4ip用に生成したchain（パケットフィルタ定義の集まり）に遮断すべきアクセス元IPアドレスとして追加していきます．

ルーターの設定で，DMZ（外部からのパケットを全て転送する先）としてRaspberry PiのIPアドレスを設定しておけば，各種不正!?アクセスを観測できます．その際は，もちろんRaspberry Piが乗っ取られないように，デフォルトのパスワードなどは変更しておいてください．

● 機能2…正常なアクセスも度が過ぎればBAN

前述のようなFailedな記録は，明らかに不正なアクセスとして分かりやすいと思います．それに対して，例えば特定のWebページに対して短時間のうちに何百回，何千回とアクセスがあった場合はどうでしょうか．

皆さんの中にもCMS（Content Management System）の1つであるMovable TypeやWordPressを使っている方もいらっしゃると思います．これらの管理画面などへのログイン用URLに対するアクセスが，いつも自分がログインしているIPアドレスとは違うアドレスから，定期的に，もしくは短時間で大量にあった場合，確実に狙われている，もしくはすでに侵入されていると考えた方がよいでしょう．

もしくは，なんでもないURLに世界中からアクセスが殺到する場合，そのファイルにはすでに侵入者がマルウェアに感染させるためのJavaScriptを仕込んで

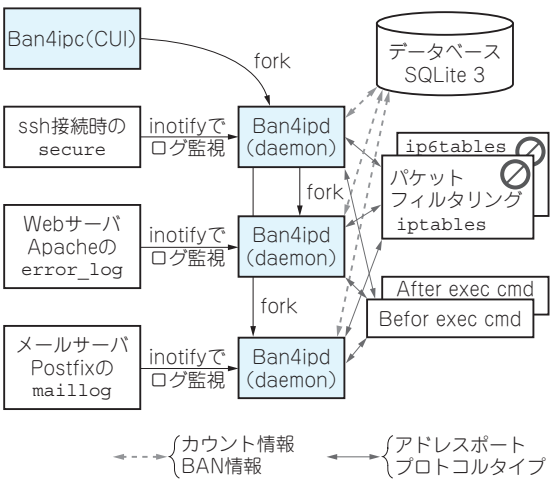

図1　オープンソース不正アクセス遮断ソフトBan4ipの動作…基本は各種ログを解析する

注1：動作確認済みのディストリビューションとしては，VineLinux 6，CentOS 6，CentOS 7，Fedora 24，Debianなど．実際にはログのパスや名前は異なる場合があるので，必要に応じて変更する（sshdの認証エラーはCentOSの場合は/var/log/secureだがDebianの場合には/var/log/auth.logなど）．