

IoT時代のコモンセンス！知らなかったで済まされない

自宅Raspberry Piサーバを不正アクセスから守る方法

前 編　まずは不正アクセスを把握する

蕪木 岳志

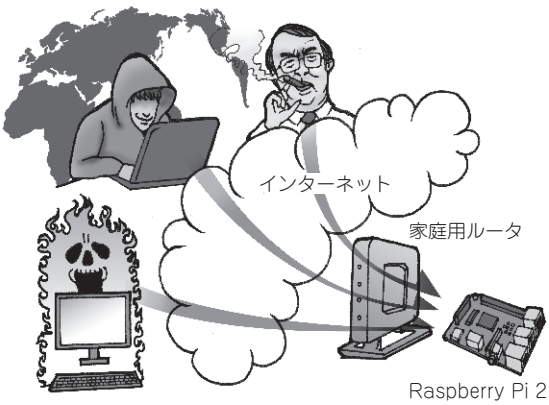

図1　インターネットに接続したRaspberry Piは常に他からの攻撃にさらされている

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ると思います．Raspberry Piのスペックなどは他の記事に譲るとして，今回はRaspberry Piサーバの管理者の皆さん，そして管理者になるかもしれない皆さんにぜひとも読んでいただきたい，セキュリティのお話です．

前編では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します．そして後編では，不正アクセスへの対策方法について解説します．

不正アクセスの実態

● まずは公開されているデータで確認

Raspberry Piを自宅の回線に接続して何らかのサーバとして運用していたり，Raspberry Piに各種IoTセンサを接続してデータをアップロードしたりするために，外部のVPSやクラウドといったサーバを運用している場合，常に気にしなければいけないのはセキュリティの問題です．インターネットに接続しているマシンは，常に他のマシンからの攻撃にさらされています（**図1**）．

表1[(1)]　カテゴリ別のコンピュータセキュリティインシデント件数
JPCERT/CC資料

インシデント	4月	5月	6月	合　計	前四半期合計
フィッシングサイト	205	201	236	642	645
Webサイト改ざん	623	186	256	1065	1268
マルウェアサイト	71	43	67	181	100
スキャン	445	576	499	1520	1654
DoS/DDoS	5	1	5	11	86
制御システム関連	6	9	0	15	11
標的型攻撃	1	9	5	15	6
その他	141	143	58	342	373

表1にJPCERT/CC[注1]カテゴリ別インシデント件数[(1)]を，**表2**に不正なアクセスをするための主な手法と目的を示します．

● Raspberry Piのログで確認

表1の中で皆さんのRaspberry Piも被害にあったり，被害を別の誰かに与える可能性のあるものは全てです．以下のような「何かに失敗した」記録を，皆さんが動かしているRaspberry Piのログで見たことはないでしょうか（**リスト1**）．

ほとんどのサービスのログは/var/log/の中にあるので，grep/zgrepコマンドなどで，failとかpassといったキーワード（大文字や小文字関係なく）や，40*とか50*といったエラーコードなどで検索してみましょう．これらはセキュリティ上問題があると思われるアクセスのほんの一部を抜粋しただけです．1番目はsshでrootとしてログインをしようとしてパスワードが異なるために接続に失敗したという記録です．また，最後はApacheというWebサーバで，

注1：「JPCERTコーディネーションセンターは，インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて，日本国内に関する報告の受け付け，対応の支援，発生状況の把握，手口の分析，再発防止のための対策の検討や助言などを，技術的な立場から行なっています」とされる．