6D-5

# 電子工作愛好者向けセキュリティゲートウェイの構築 (第二報：運用と管理)

大野 浩之† 鈴木 裕信‡

金沢大学 総合メディア基盤センター† 専修大学 ネットワーク情報学部‡

## 1.はじめに

著者らは、Raspberry Pi や同等の機能を持つ手のひらサイズのボードコンピュータを「電子工作の愛好者が築いてきた『ものづくり』の文化と、インターネット技術者が築いてきた情報通信の世界の双方に新たな出会いと興味深い展開をもたらしたデバイス」であると捉えている。しかし同時に、インターネット接続を果たした電子工作の成果物は、当然ながらインターネット上の脅威に直接間接に晒される。そこで、まずはターゲットを Raspberry Pi に絞り、Raspberry Pi のために Raspberry Pi で作ったセキュリティゲートウェイを構築することにし、これを Raspberry Gate と名付けた。Raspberry Gate は、既存のパソコンベースのセキュリティゲートウェイと同等の構成なので、一定の安全確保が期待できるが、セキュリティデバイスの常として、デバイス単体の性能よりも、それをどのように運用し続けるかの方が重要かつ困難な問題である。この問題に対処するための組織と手法として Raspberry Guardian を提案し、脅威の低減を維持し続ける機構について考察する。

## 2. Raspberry Gate の問題点

Raspberry Gate は、Raspberry Pi で作られたネットワーク接続性を持つ作品群のために Raspberry Pi で構成したセキュリティゲートウェイで、通常は当該電子工作物と同じネットワークに，ルータかブリッジかプロキシとして設置して用いる。現状の Raspberry Pi では、Debian Linux をもとにした Raspbian というディストリビューションを始め、実用的な OS が動くので、Raspberry Gate に必要なソフトウェア群をインストールしてセキュリティゲートウェイとして運用すること自体には困難はない。もちろん、構成はできても期待する性能がでないことはあり得、そのための調整は今後も必要であるが、性能についてはここでは議論しない。

Security Gateway for Electronics Hobbyists (Part 2. Operation and Management)
† Hiroyuki Ohno, Kanazawa University
‡ Hironobu Suzuki, Senshu University

前述のように、問題は Raspberry Gate が提供するパケットフィルタリングや監視等のセキュリティゲートウェイとしての機能をいかに簡単かつ持続的に維持するかである。なぜなら、電子工作の一環として Raspberry Pi が用いられた場合、Raspberry Pi は作品の一部となるが、完成した作品に対して、永続的にセキュリティアップデートを実施するということは現状では考えにくい。そのため、電子工作の作品の一部である Raspberry Pi には手を加えず、作品が接続されたネットワークと外部のネットワークとの間に Raspberry Gate を設置し、Raspbery Gate を定期的にアップデートすることで作品の安全と安心を確保するのが次善の策となる。このアップデート作業を行うのは、ネットワーク技術者ではなく Raspberry Pi を用いた作品を作った電子工作の愛好者である場合があるので、簡単な操作で一定の安全と安心が確保できる体制の構築と運用が必要である。これを実現するのが Raspberry Guardian である。

## 3. Raspberry Guardian の構成

前報でも指摘したように、Raspberry Pi で最も多く利用されている Raspbian では、インストールすると標準ユーザ（ユーザ名 pi）が用意されるが、このユーザのパスワードは広く知られている。また、このユーザは sudo した時にパスワードを聞かれずに全コマンドの実行が可能な設定になっている。このままでは危険であることは明白であるが、実際にはこの標準設定のままで使っているユーザが多い。どうすればこの問題に対処できるのか、他にも似た問題がないかといったことは、情報セキュリティに関わる者であれば難しい問題ではないが、電子工作の愛好者ではあるがネットワークの専門家ではない者にとっては対処は必ずしも容易ではない。そこで以下の２つを提供する。

（１）何に対してどういう対処を為すべきかという情報を共有するしくみ
（２）必要な対処を自分の Raspberry Gate に簡単に反映させるしくみ

現時点では、（１）については Redmine[1]によるチケット管理で実現し、（２）については Git[2]によるソースコード管理を用いている。

3-1. Redmine

Redmine には、以下の３種類のユーザを用意した。

(1) 設定等を変更できる人(Admin)、
(2) 報告などを出せる人(Developer, Deployer)
(3) 単に閲覧するだけの人(Forum User)

このうち、(1)は、一般的な意味での Redmine の管理者（Redmine の設定を変更できる人）と、それに加えて、次項で述べる Git の変更ができる人に分かれる。後者はごく少数となる。(1)に属する者は、ユーザ ID とパスワードで Redmine にアクセスするが、(2)に属する者は、OpenID でのアクセスに限定する方向で Redmine に手を加えている。(2)に属するものは、開発担当者（developer）と普及担当者(deployer)に分かれる。さらに閲覧するだけの(3)が存在する。これらの関係を図１に示す。

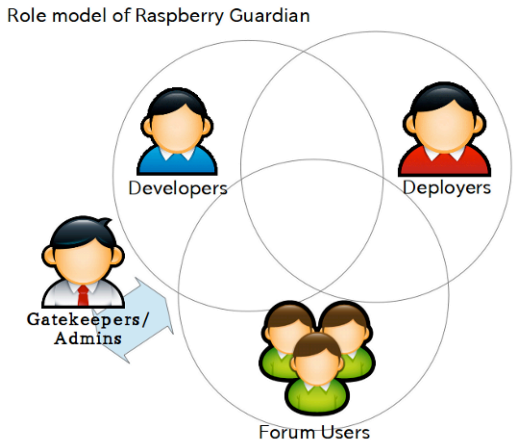


**図 1 Raspberry Guardian のための Redmine を構成するユーザ**

Redmine では、Raspberry Gate に導入するセキュリティ設定についての意見や知見を集約する。ただし、セキュリティについては、考え方や対応方法が人によって異なることが少なくない。そのため、結果的に集合知としての結論がでない場合もある。意見や知見を発散させないことは重要であり、そのための努力が管理者（上記分類の（１））には求められるが、意見に食い違いが生じ、それが Raspberry Gate の性能や運用に影響を与えるような事態になった場合の対処は現時点では未確定である。さしあたり、管理者以外を開発者、普及者、フォーラム利用者に分割したが、この理由は、各々が必用とし議論しようとしている情報のレベルや密度が異なるためである。これを同一のレベルでまとめようとするとお互いのコミュニケーションに齟齬を生じやすくなる。ことは、さまざまなソフトウェア開発の経験からよく知られているため、あらかじめ配慮した。

3-2. Git

Raspberry Guardian では、Redmine で得られた知見や知識を RaspberryPi の設定に反映させるためのスクリプトやアプリケーションプログラムを Git で管理し、ユーザ（Raspberry Gate の運用を行う者）に提供する。ユーザは、定期的に設定を自動的にダウンロードして Raspberry Gate の機能を更新する。

４．Raspberry Guardian の試験運用

著者のひとり（大野）は、石川県金沢市において、Raspberry Pi や同等のボードコンピュータを電子工作に活用する電子工作愛好者との情報交換会（木いちごの会）を主宰し、月に２度のペースで対面式の会合を行っている。Raspberry Guardian のしくみが実際に機能するかどうかは、まず木いちごの会の積極的な参加者にアルファテスタになってもらって評価することとし、現在その準備を進めている。このアルファテストの結果を受けて、著者らの勤務する大学等においてベータテストを行う予定である。

５．おわりに

Raspberry Farm に情報セキュリティ上の安全と安心をもたらすためには、Raspberry Gate の持続的かつ適切な運用が重要である。そこで、Raspberry Gate の適切設定を維持する Raspberry Guardian らは、Redmin を用いて適切な設定を決定し、Git によって決定をもとにした設定を配布する。このしくみは、Linux 等の開発に用いられている Gatekeeper Workflow であり、うまく機能しはじめれば、情報セキュリティ分野の専門ではない電子工作愛好者にとっては、簡単に自分の作品に安全と安心をもたらす重要な存在となる。

参考文献

[1] Redmine: Overview, 入手先 〈http://www.redmine.org/〉（参照日付 2014-01-14）
[2] git, 入手先 〈http://git-scm.com/〉（参照日付 2014-01-14）