

電子工作愛好者向けセキュリティゲートウェイの構築 (第一報：設計と実装)

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

近年、電子回路を活用したものづくり（いわゆる電子工作）を楽しむ人々が増えている。特に 2012 年初頭に登場したボードコンピュータ「Raspberry Pi」は、UNIX を OS とする手のひらサイズのコンピュータを 3000 円程度の支出で入手可能にしたため、発売開始後の 1 年間で 100 万台以上出荷するベストセラーとなった[1]。これまでも、マイクロコントローラにセンサやアクチュエータを接続してものづくりを楽しむ電子工作の世界と、インターネットが作り出した情報通信の世界を融合する方法は存在したが、Raspberry Pi によってこれが一気に普及した。しかし、このことは電子工作の世界がインターネットからセキュリティ上の脅威を直接受ける事態になったことも意味し、電子工作を楽しみたいだけの者にも、多くの場合不本意ながらインターネットに接続する情報通信機器を管理する技術者と同等の情報セキュリティに関する専門知識と運用技術を求めることになった。

そこで、情報通信分野の専門家ではない大多数の電子工作愛好者が簡単に設置して運用できる「セキュリティゲートウェイ」を提案し、情報セキュリティ上の脅威を簡単かつ持続的に低減する機構 Raspberry Guardian の提供を目指す。なお、本報での議論は、議論を簡単かつ明確にするため、Raspberry Pi のみを対象として展開しているが、その大部分は、Raspberry Pi と同様の構成の小型ボードコンピュータにも適用できる。

2. 現状の問題

Raspberry Pi 自体は、UNIX 系 OS が動作可能なボードコンピュータにすぎず、利用者が選択する OS によってその挙動は変化する。現状では Raspbian とよばれる Debian 系の Linux ディストリビューションが最も普及している。

Raspbian では、`apt-get` コマンドや `git` コマンド等を使えば第三者が作成したソフトウェアを容易に導入できて便利だが、ユーザ名とそのパスワードが既知の標準設定のままで使われていることが多く、さらにこの標準ユーザはパスワードなしで `sudo` コマンドを実行できる設定になっているという、情報セキュリティの視点からすると過度の便利さが標準になっている。このため、Raspbian を導入した Raspberry Pi をインターネットに直接接続すれば、それはセキュリティ上の大きな脅威となる。実際には、多くの Raspberry Pi はローカルアドレスが付与された NAT 内で運用されていると推測できるが、このことをもって脅威がないと言いきることはできない。Raspberry Pi が趣味の電子工作の一環で導入された場合には、完成した作品に対して定期的なセキュリティアップデートや設定変更は期待しづらいという問題もある。

3. 概念と用語

本研究では、インターネットへの接続性を有する Raspberry Pi とその周辺環境を、農場、農地、農家などに見立て、以下のように定義し、Raspberry Garden に迫る外部からの脅威を、Raspberry Gate とそれを運用する Raspberry Guardian で守るというモデルを採用した。

- Raspberry Field (比喩：畑)

Raspberry Pi が（時に無秩序に）たくさん接続されているネットワーク

- Raspberry Garden (比喩：庭園)

何らかの方針のもとに運用している Raspberry Pi の集合体

- Raspberry Farm (比喩：農園)

いくつかの Raspberry Garden とそれを見守るオフィス (Raspberry Farm House) を含む運用実体

- Raspberry Farm House (比喩：農家)

Raspberry Garden を運用する主体が滞在する場所

- Raspberry Guardian (比喩：保護者、門番)

Raspberry Farm House を拠点に Raspberry Farm に安全と安心をもたらす者

Security Gateway for Electronics Hobbyists (Part 1. Design and Implementation)

[†] Hiroyuki Ohno, Kanazawa University

[‡] Hironobu Suzuki, Senshu University

- ・Raspberry Gate (比喻：門、防火扉)

Raspberry Farm と外部とを区切る門。Raspberry Farm は Raspberry Gate 以外からは外部と往来できない。

4. Raspberry Gate の基本性能

4-1 構成

Raspberry Gate には以下の3つの形態が考えられる。

- ・ルータ型

・長所：Raspberry Farm と外部のネットワークを分離できる。既存のルータによるネットワークの分離と管理の手法がそのまま利用できる。

・短所：新たなサブネットを用意する必要がある。IP アドレスの変更が必要になるが、DHCP で運用しているのであれば、大きな問題にはならない。

- ・ブリッジ型

・長所：既存のサブネットを Raspberry Farm とそれ以外に分離しその間に Raspberry Gate を挟むだけなので、IP アドレスの変更などは生じない。

・短所：既存のネットワークの一部なので、既存のネットワークの運用ポリシーの影響を受ける。

- ・プロキシ型

・長所：既存のサブネットに追加するだけでよい。

・短所：当該プロキシを見るように経路設定を変更するなどの対処が必要。この対処は個別に行う必要がある。この対処を行わない機器は Raspberry Gate の恩恵に浴せない。

4-2 基本性能の測定

Raspberry Pi には 10/100BASE-T のイーサネットが 1 つ用意されている。物理的にネットワークのセグメントを分けた上でブリッジを行うには最低 2 つのネットワークインタフェースが必要である。そこで 1000BASE-T USB 2.0 LAN アダプタ PLANEX GU-1000T を Raspberry Pi の USB ポートに接続し、iperf コマンド[2]で通信速度を測定した(図1)。

4-3 測定結果

まず、PC (インタフェース速度は 1Gbps) と 1 対 1 で通信し通信性能を確認した。Raspberry Pi は、駆動周波数を変更することが可能なので、700MHz (標準) と 1GHz の場合で測定し、以下の結果を得た(括弧内は 1GHz の場合)。

- ・内蔵イーサネット(eth0, 図1の test1)
63Mbps (100Mbps)
- ・GU-1000T(USB2.0 接続, eth1, 図1の test2)
63Mbps (92Mbps)

駆動周波数を高く設定すると CPU の処理能力が上がり iperf の計測値が良くなった。1GHz で駆

動すれば、どちらのネットワークインタフェースも 100BASE-T としては納得できる速度を出せることが確認できた。

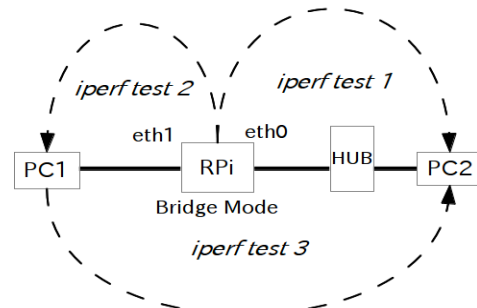


図 1 テスト環境の構成

次にブリッジを作成し PC 間で通信を行うテストを行った。この時、接続性に問題が発生した。ブリッジを構成できるが、ネットワークに負荷をかけると GU-1000T が不具合を起こし eth1 が通信不能となった。そこで、USB 2.0 を USB 1.1 (インタフェース速度は 12Mbps) に設定変更したところ、ブリッジとして通信できた。Raspberry Pi をブリッジとして PC 間で iperf を実行し性能を計測(図1の test 3)した結果は 4.77Mbps となった。なお、一連の測定は複数回実施しているが、駆動周波数を高くしたテストの際には計測データのばらつきが大きかった。

5. おわりに

現状は、Raspberry Gate の基本機能であるネットワークインタフェースの性能測定に着手した段階である。今後は、まず USB2.0 での運用を可能にしてゲートウェイとしての実用的な通信速度を確保した上で、次報で述べる運用や管理のための機構との連携を重視しつつ、通信の監視や選別などを行い、セキュリティゲートウェイとしての機能を実現する。

参考文献

- [1] Natasha Lomas: Raspberry Pi Microcomputer Racks Up 1.75M Global Sales, 1M Of Which Were Made In U.K., 入手先 <<http://techcrunch.com/2013/10/08/1-75m-raspberry-pis/>> (参照日付 2014-01-14)
- [2] Iperf - The TCP/UDP Bandwidth Measurement Tool, 入手先 <<http://iperf.fr/>> (参照日付 2014-01-14)