Vol.2014-DPS-160 No.4
2014/7/24

電子工作愛好者向けセキュリティゲートウェイの構築

第三報：構成要素の検討と性能評価

大野 浩之[1]　北口 善明[1]　鈴木 裕信[2]

概要：電子回路を活用したものづくりの愛好者が増加する中，2012 年に登場した手の平サイズでありながら Linux が動く “Raspberry Pi” は，電子工作の世界とインターネットの世界を近づけたが，同時に，単に電子工作を楽しみたいだけであっても作品がネットワークを介した通信を行うのであれば，情報セキュリティに関する知識と運用技術の習得が必須となった．純粋に電子工作を楽しみたいだけの者にとってこれは望んだ結果ではない．そこで著者らは，Raspberry Pi のために Raspberry Pi で作ったセキュリティゲートウェイ装置である “Raspberry Gate” と，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手法である “Raspberry Guardian” の二つを提案している．本報では，Raspberry Gate を構成する要素技術について性能評価を行い，Raspberry Pi のために Raspberry Pi で構成した Raspberry Gate が十分な性能を有することを示す．

Security Gateway for Electronics Hobbyists

(Part 3. Evaluation of Each Elements of The Rapsberry Gate)

Hiroyuki Ohno[1]　Yoshiaki Kitaguchi[1]　Hironobu Suzuki[2]

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）を趣味として楽しむ人々が増えている．電子工作は，たとえば昭和 30 年代のラジオ受信機やアマチュア無線用通信機の製作，あるいはアナログレコードの再生を主としたオーディオ機器の製作などに遡れる，以前から存在する趣味だが，パソコン上で C 言語を用いて手軽にプログラムをクロス開発できる 8bit CPU を搭載した小型のボードコンピュータ Arduino が広く普及しはじめた 2008 年ころからは，趣味の電子工作に CPU ボードを導入することはそれまで以上にありふれた事例になった．

このような流れの中で，2012 年初頭に英国で誕生したボードコンピュータ “Raspberry Pi” は，手のひらサイズでありながら Linux を始めとする UNIX 系 OS が動き，価格も 35 ドル程度と安価だったため，発売開始から 1 年半で全世界に 200 万台以上出荷するベストセラーとなった．当時，円高が進行中だった日本では 3000 円台で入手できたこともあり，日本でも多くのホビーイストが Raspberry Pi を利用するようになった [1].

小型で高機能で安価な CPU ボードの普及自体は歓迎すべきことであるが，センサやアクチュエータを接続した CPU ボードが，無防備のままインターネットにさらされれば，望まぬ事件や事故を起こしかねない．われわれはこの問題を憂慮し，既報のように Raspberry Gate [2] や Raspberry Guardian[3] を提案している．第三報である本報では，Raspberry Guardian による実証実験に入る前段階として，Raspberry Gate がわれわれが望む機能と性能を出せるかに的を絞って議論する．

2. 現状

手のひらサイズの CPU ボードでマルチユーザかつマルチタスクの現代的な OS を動かすためには，それに見合う

[1] 金沢大学 総合メディア基盤センター
Kanazawa University, Kanazawa, Ishikawa 920–1192, Japan
[2] 専修大学 ネットワーク情報学部
Senshu University, Kawasaki, Kanagawa, 214-8580, Japan

能力の 32bit CPU や数 100MB 以上のメモリが必要で，あわせて USB, HDMI, ネットワーク などの標準的なインタフェースが用意されるのが普通である．現代的な OS が動くと，利用者は新たにデバイスドライバやライブラリなどのミドルウェアやアプリケーションプログラムを新たに用意したり書き下ろすことなく，OS の基本機能としてこれらのインタフェースを利用できる．この点が，Arduino のような 8bit CPU を搭載したこれまでの CPU ボードとの決定的違いである．たとえば，複数のネットワークインタフェースを持ち，DHCP を用いて IP アドレスを取得し，DNS を用いて名前解決して，インターネット上のさまざまなリソースにアクセスしてサービスを受けつつ，自機では WEB サーバや SSH サーバを立ち上げ，自作したアプリケーションを複数同時に動かすといったことは，700MHz の CPU と 512MB のメモリを持つ Raspberry Pi のような，よい意味でありふれた Linux 機では雑作もないことである．

Linux を始めとする現代的な OS が動くなら，必要なソフトウェアがオープンソースソフトウェアであれば apt-get のようなパッケージ管理コマンドでダウンロードしてインストールし，テキストエディタで設定ファイルを編集し，シェルから起動を指示するだけでよい．自作プログラムも他のパソコンで開発するのではなく自機上でセルフ開発できる．OS を持たず，16MHz の 8bit CPU と，わずか 2KB のメモリで構成される Arduino では実現が困難だったことが，簡単に実現できるようになった

この高機能と手軽さゆえ，Raspberry Pi や同等のコンセプトで開発された類似機は急速に広まりつつあるが，インターネット接続ができる機器は，それに見合うセキュリティを確保しなければ，セキュリティ上の脅威に悩まされることをわれわれは Windows95 以来の 20 年弱の間に学んできた．しかし，趣味の電子工作用途の Linux 機として Raspberry Pi を考えたとき，現状は後手にまわっており，かつての Windows 機が歩んだ道を再び歩む可能性がある．これはなんとしても回避したい．

ありふれた Linux 機としての側面を持つ Raspberry Pi を趣味の電子工作に供する機材と捉えた場合，Raspberry Pi を搭載した「作品」は，セキュリティの面からいくつかの注意点がある．

(1) インターネット接続は作品の一部であり，当該 CPU ボードは作品の一部として「完成」している．よって，作者にはインターネット接続するネットデバイスには継続的なセキュリティアップデートが必要という認識がない場合が多い．
(2) 少なくとも現時点では Raspberry Pi 向けの Linux ディストリビューションでは標準では特段のセキュリティ対策は取られていない．作品の作者がシステム管理者となってセキュリティを維持する必要があるが，趣味で電子工作を楽しみたいだけの者に情報セキュリティを持続的に維持するスキルを求めるのは難しい．
(3) GPIO ポートを介してセンサーやアクチュエータが接続されていることは珍しくなく，不正アクセスを許した場合，これまではあまり発生しなかった物理的な破壊や発災に至る可能性がある．

このような状況にある中，一部の技術系雑誌では，情報セキュリティ上の危険に言及することなく RaspberryPi をインターネットに接続する解説記事を掲載するなど，危険な状態にある．

この問題に対処すべく著者らが提案している Raspberry Gate と Raspberry Guardian について改めて要するなら，Raspberry Gate は Raspberry Pi のために Raspberry Pi で作ったセキュリティゲートウェイであり，Raspberry Gate に施す「セキュリティアップデート」をソーシャルネットワークの考えに基づいて有志が作りみんなで共有しようという試みが Raspberry Guardian である．次報 [4][*1] 以降で実証実験に向けた報告を行うのに先立ち，本報では Raspberry Gate を構成する要素の性能を評価し，セキュリティゲートウェイとしての必要な性能を有することを示す．

3. RaspberryGate の性能評価

Raspberry Gate は Raspberry Pi が 1 つまたは複数 LAN に接続されている Raspberry Farm 環境と外部であるインターネット側の WAN をを区切るセキュリティ機能を持ったゲートウェイの役目を果たす．

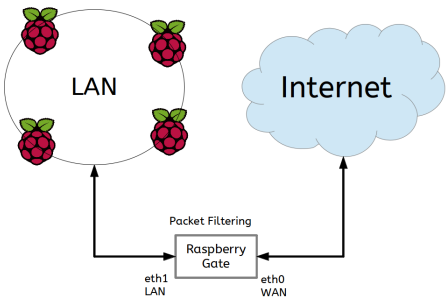

図 1 Raspberry Gate の位置づけ

Paspberry Pi の基本性能は，今日のノートパソコンやディスクトップといった一般的な PC よりハードウェア性能では劣る．OS として GNU/Linux を稼働させることが可能であり，また GNU/Linux はルータやファイアウォールとしての実績があるので，その機能を活かしセキュリ

[*1] 本報より次報 (第四報) が 2 週間早く発表となり執筆も第四報が先行したため，本報は第四報を参照しているが，第四報は本報を参照していないというねじれが生じている

ティ機能を持ったゲートウェイ作成が可能であることは既報で説明を行った．

Raspberry Gate の利用モードは，「初期化モード」「アップデートモード」「ブリッジ動作モード」「ルータ動作モード」の 4 つある．その中でゲートウェイの役目を果たすのは，ブリッジ動作モードとルータ動作モードである．

Raspberry Pi はハードウェアとして 100Mbps の Ethernet 接続の機能を有しているが，実用的に利用するためにはブリッジ動作モードとルータ動作モードで動作した際のスループットが重要である．

ネットワーク・インタフェースであるが, Raspberry Gate の eth0 は Raspberry Pi オンボード Ethernet で、eth1 は USB ポートに接続されている Logitec 100BASE USB 2.0 Ethernet Adapter である．

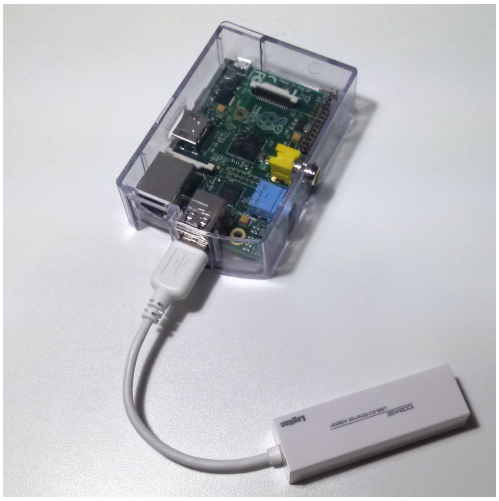

図 2 100BASE USB 2.0 Ethernet Adapter を接続

3.1 ブリッジ動作モードの性能評価

ブリッジとは，異なるネットワークのセグメントを L2 レベルで接続する機能である．Raspberry Gate のブリッジ動作モードにおけるゲートウェイとは，パケットフィルタリングを行い外部からの不正なパケットを防ぐことを目的としている．具体的には iptables を用いてフィルタリングを行う．Raspberry Gate のブリッジ動作モードでは eth0(WAN 側) と eth1(LAN 側) の他に br0(内部ブリッジ) のネットワーク・インタフェースがある．いずれのネットワーク・インタフェースに対しても INPUT/OUTPUT (インバウンド/アウトバウンド) に対してフィルタリングを設定することが可能である．

何も設定しないブリッジ動作モードの場合，そのスループットは 90Mbps 以上でありパフォーマンスに関して問題はないのは既報の通りである．ここでは iptables を設定した際のスループット変化を計測した．

まず iptables の OUTPUT チェーンにポート 1 つに対し DROP をかけるルールを設定した上で，そのスループットを計測し，次に異なる合計 202 ポートに対して DROP のルールを設定しスループットを計測した．尚，ネットワークのトラフィック計測にはコマンド iperf を用い，5 回計測し、平均を取ったものである。

コマンド例は次の通りである．

```
# iptables -A OUTPUT -p tcp \
  --dport 25 -d 0/0 -j DROP
```

結果は次の通りである．

表 1 ブリッジ動作モードのスループット

フィルタなし	92.3Mbps
フィルタルール 1 個	92.2Mbps
フィルタルール 202 個	92.2Mbps

結果はいずれも約 92Mbps となり、明白な処理の速度低下は見られなかった。

3.2 ルータ動作モードでのパフォーマンス

ルータ動作モードは，LAN 環境を NAT を用いて WAN 環境 (上位 LAN 環境) に接続するための機能である．NAT 機能を使うためには，カーネルに iptables nat モジュールをロードする．Raspberry Gate のルータ動作モードでは eth0(WAN 側) と eth1(LAN 側) のインタフェースとなる．eth0/eth1 に対して INPUT/OUTPUT (インバウンド/アウトバウンド) に対してフィルタリングを設定することが可能である．

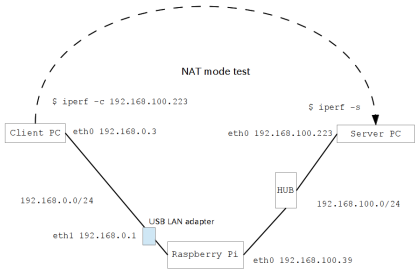

図 3 ルータ動作モードテスト環境

NAT のテストでは次のような環境を構築しテストを行った。

内部ネットワーク

- Raspberry Pi を使うネットワークセグメント (LAN 側) を想定.
- 192.168.0.0/24 のネットワークアドレスとする.
- PC を接続し 192.168.0.3 とする.

外部ネットワーク

- インターネット (WAN 側) を想定.
- 192.168.100.0/24 のネットワークアドレスとする.
- サーバを接続し 192.168.100.223 とする.

Raspberry Gate

- eth0(WAN 側) を 192.168.100.39 とする.
- eth1(LAN 側) を 192.168.0.1 とする.

外部ネットワークは既存のネットーワークで他のシステムも接続されている．192.168.100.0/24 側に HUB(L2 switch) が接続されているが，トラフィックピークが 100Mbps レベルの性能評価には影響を与えない．クライアント側 PC はノートパソコンで、サーバ側 PC はデスクトップパソコンである．各々性能評価に利用するにあたり十分な性能を持っている．計測はこれまでと同様に iperf を利用した．ネットワークフィルタに関しては NAT をかけた状態でブリッジモードと同じフィルタルールを使いテストを行う．

計測結果は次の通り．

表 2 ルータ動作モード (NAT) のスループット

NAT のみの	61.6Mbps
フィルタルール 1 個	62.7Mbps
フィルタルール 202 個	62.9Mbps

ルータ動作モードでは NAT を使うためスループットが低下し，ブリッジ動作モードの約 66 パーセント程度のパフォーマンスにとどまることがわかった．尚，フィルタルールの方が早く見えるが，NAT のみでの計測は $(63.1 + 63.7 + 60.1 + 60.8 + 60.6)/5 = 61.66$ となっていて、原因不明ではあるが、最後の 3 回が遅くなってしまっていた．これは 5 回計測をした中でのぶれの範囲と判断しても問題ないと思われる．

参考情報としてブリッジモードのまま，カーネルに iptables nat モジュールをロードしスループットが変わるか試してみた．NAT 機能は使わない場合でも，モジュールをロードするだけで 77.4 Mbps という値となった．

ルータ動作モード（NAT 機能）では約 62Mbps 程度のスループットとなることが明らかとなった．Web ブラウザなどで外部にアクセスするような用途に関してはスループットは問題ないと考えられる．

3.3 NAT の接続数

NAT は接続数に応じて内部でテーブルを作る．そのため内部ではメモリを消費し，その利用できるメモリ上限が接続数上限となる．

テストで利用している iperf のサーバ及びクライアントの性能の制限で Raspberry Pi の接続限界のテストまでは行えないが，テスト数値を示すことで目安としたい．

同時接続 (同時 NAT 数) に関しては同時接続数 256 で問題は発生しなかった。

この数値は今回利用していたサーバとクライアントが安定して行える同時接続テストの限界である．しかし Raspberry Gate が利用する環境では，同時接続数 256 で安定して接続していれば一応の目安となると考えられる．同時接続数 256 で処理しても，問題なく処理を行えた．この時、各接続スレッドのスループットを合計すると約 65Mbps となり予想の範囲内の値となった．

NAT でセッションを連続的に大量に生成する負荷実験も行った。iperf を使い，通信時間は 1 秒，同時接続は 256 の通信を同時に行うことを繰り返し行う．クライアント PC 側の負荷の問題で，コマンドのループのインターバルは 1 秒とした．結果は，性能に明白な劣化は見当たらず，Raspberry Gat の障害も発生しなかった．

```
while true
do
  sleep 1
  iperf -c 192.168.100.223\
    -t 1 -P 127
done
```

NAT テーブルのメモリサイズを大きくすることで NAT の接続数の上限を向上させることが可能である．netfilter faq によれば 1 コネクションあたい約 350 バイトとある．下記条件だと約 1500 コネクション弱程度を利用できることができる．

```
# echo 524288 > /proc/sys/net/\
  netfilter/nf_conntrack_max
```

4. 考察

4.1 IPv6 対応

現在の Raspberry Gate は，IPv4 での運用のみを考えて構築している．しかし，これからの時代は，特に IoT を意識するのであれば IPv6 対応は必須である．また，Raspberry Gate を構成している Linux は IPv6 に完全対応している．そこで，本節では Raspberry Gate を IPv6 対応させるための議論を行う．

4.1.1 ネットワークリソースへの配慮

IPv6 を利用する場合は，IPv6 のみにはならず，IPv4 も同時に利用するデュアルスタックとなることに注意が必要である．そのため，必要なネットワークリソースが単純に考えて二倍になる．ブリッジモードであれば，MAC アドレスを扱うだけなのでリソースの増加は気にならないが，ルータモードの場合には MAC アドレスと IP アドレスの管理テーブル（IPv4 での ARP テーブルおよび IPv6 での NDP キャッシュ）が必要なため，必要なリソースは増加する．IPv6 の場合，インターフェイスに設定されるアドレスがグローバルアドレス 1 つではなく，最低限リンク

ローカルアドレスも設定されるため2つとなる．したがって，必要なリソースも三倍以上になることを理解しておくことが重要となる．

4.1.2 ブリッジモードでの対応

IPv4 のみの場合と比較した場合，フィルタリングで扱うプロトコルタイプが増えるだけであり，大きな追加実装は不要である．フィルタリングに関しては，ルータモードでも同様な考慮が必要となるが，IPv6 では ICMP をすべて落とすと通信が成り立たなくなる点に考慮が必要となる．

4.1.3 ルータモードでの対応

ルータモードでは，ネットワークセグメントを分割する以上，Raspberry Farm セグメントに与えるアドレスが必要となる．IPv4 の場合は，NAT/NAPT 機能によりプライベートアドレスを利用する方法でよかったが，IPv6 では複数の手法が利用可能であるためそれぞれのメリット/デメリットを整理する必要がある．以下に，それぞれの手法における整理を行う．

(1) 割り当てグローバルアドレスの委譲
IPv6 は豊富なアドレス空間を持っているため，NAT/NAPT 機能によるアドレス共有をせずともすべての端末にグローバルアドレスを設定することが可能である．したがって，Raspberry Farm セグメントにグローバルプレフィックスを割り振ることが資源的に困難ではなく，end-to-end 通信を容易に実現できるメリットがある．ただし，プレフィックスを委譲するには手動設定もしくは DHCPv6-PD [5] を利用する必要がある．前者は，ユーザに経路設定を要求するため非常に敷居が高いと考えられる．後者は，Raspberry Gate を設置するネットワークにおいて PD (Prefix Delegation) 機能を持つ DHCPv6 サーバが必要となるため，現時点においてこちらも敷居の高い手法と考えられる．

(2) ULA と NPTv6 の利用
IPv4 のプライベートアドレスと似た概念のアドレスとして，IPv6 では ULA (Unique Local ipv6 unicast Address) [6] がある．このアドレスを Raspberry Farm セグメントのアドレスとして利用し，WAN 側で配られるグローバルプレフィックスにプレフィックス変換（NPTv6）[7] を用いる手法である．NPTv6 は，ステートレスにプレフィックスの変更を行う技術であり，チェックサムの修正も必要としない 1 対 1 のアドレス変換となる．そのため，個々の Raspberry Pi への end-to-end 通信は容易である．ULA のプレフィックスもルータインターフェイスの MAC アドレスを利用して生成する方式があるため，自動生成が可能である．

(3) IPv4 と同様のグローバルアドレス共有
IPv4 の場合と同様な NAT/NAPT 機能を利用することも可能である．その場合，外部から直接 Raspberry Pi への接続が IPv4 の場合と同様にポートフォワーディングなどの技術を利用する必要があり，end-to-end 接続よりは制限を受ける事になる．また，アドレス変換のステートをルータで持つ必要があるため，通信パフォーマンスも一定量損なわれる可能性がある．これは，本稿における IPv4 の性能評価と同じ結果になると想定される．

4.1.4 IPv6 利用の利点

最後に，IPv6 を Raspberry Pi で利用する場合のメリットについて考察する．IPv6 は，128 ビットのアドレス長を持っている事から，すべての端末にグローバルアドレスを付与するだけのアドレス空間を持っている．これは，すべての端末が end-to-end で通信する事が可能であることを意味しており，IoT (Internet of Things) との親和性が高いと言える．また，同一セグメント内通信で利用できるリンクローカルアドレスが設定されるため，アドレス設定を行わずに通信する事も可能である．Raspberry Pi の ssh 接続を可能にしておけば，リンクローカルアドレスを用いて接続でき，mDNS の実装である Avahi デーモンを起動しておくことで，<hostname>.local というドメイン名の利用も可能となる．

4.2 IPv6 以外の議論

4.2.1 OnionPi

本報では，Raspberry Gate を構成する機能について性能測定を行い，セキュリティゲートウェイとして機能するに足る性能があることを示したが，Raspberry Pi で類似の機能を提供している例があれば傍証になる．Raspberry Gate は，Raspberry Guardian と連携しないのであればiptables を活用するという付加価値を持つルータあるいはブリッジである．Raspberry Gate とは方向性が異なるが，Raspberry Pi に付加価値を持たせたルータとしては，Tor (The Onion Router) Raspberry Pi で実現した Onion Pi がある．Onion Pi と Raspberry Gate とでは想定する脅威が異なるが，Onion Pi の方が開発は先行しており，その性能や有効性の議論は参考になる点が多い．

4.2.2 アプライアンス化

Raspberry Gate は，容易に起動でき，いつでも電源を切れるアプライアンスであるある．その一方で，Raspberry Guardian により適宜アップデートできる必要もある．前者の要求は，起動パーティションを読み出し専用でマウントして起動するといった方法があるが，アップデートを行うためには読み出し専用マウントでは対応できない．両者の要求を満たす実装はきわめて重要であり，現在試行錯誤を重ねている．

5. おわりに

本報では，Raspberry Gate を Raspberry Pi で構成可能かについて検討を行った．Raspberry Pi をブリッジ（第二層ゲートウェイ）あるいは NAT ルータ（第三層ゲートウェイ）として基本性能を測定したところ，Raspberry Pi のネットワークインタフェース速度を大幅に下回ることなく通信できることが明らかになった．今後はより多数のセッションを張った場合や DoS 攻撃のような不適切な IP パケットが大量に到達した場合の耐性などを調べる必要がある．次報では，今回の結果をもとに Raspberry Guardian の実現に向けた取り組みについて報告する．

謝辞

著者の一人（大野）は，電子工作愛好者が実際に集って技術的な情報交換する「木いちごの会」というハンズオンを定期的に石川県野々市市や同県金沢市で開催している．本研究は，同会における Raspberry Pi を用いた IoT デバイスの安全安心な運用についての議論がきっかけとなって始まった．それぞれ異なる技術的背景と好奇心を持って同会に集う，実行力あふれる電子工作愛好者各位に謝意を表したい．

参考文献

[1] kanai. Raspberry Pi が 200 万台を突破. `http://makezine.jp/blog/2013/11/two-million-raspberry-pis-in-the-wild.html` 2014 年 5 月 16 日閲覧.
[2] 大野浩之, 鈴木裕信. 6D-4 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). 全国大会講演論文集, Vol. 2014, No. 3, pp. 47–48, mar 2014.
[3] 大野浩之, 鈴木裕信. 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). 全国大会講演論文集, Vol. 2014, No. 3, pp. 49–50, mar 2014.
[4] 大野浩之, 鈴木裕信. 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 (第四報：Raspberry Guardian の実証実験に向けて). DICOMO2014 講演論文集, Jul 2014.
[5] O. Troan and R. Droms. *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*, December 2003. RFC 3633.
[6] R. Hinden and B. Haberman. *Unique Local IPv6 Unicast Addresses*, October 2005. RFC 4193.
[7] M. Wasserman and F. Baker. *IPv6-to-IPv6 Network Prefix Translation*, June 2011. RFC 6296.