[ポスター発表] 研究報告

IoT機器向けホストベース不正通信検知の実装

池部 実[1,a)]　吉田 和幸[2,b)]

Implementation of Host-based anomaly detection system for IoT devices

1. はじめに

我々の研究グループでは，周産期医療において，出産年齢の高齢化に伴うハイリスク出産を見守る新たなスマート技術として，IoT (Internet of Things) 機器を用いた妊産婦向けの生体音の計測・分析・見える化による周産期見守りシステムの研究開発に取り組んでいる．IoT による低コストで携帯可能な計測機器を試作し，妊産婦自身が常時装着しながら，診断が必要な状態を検出すると妊産婦の携帯機器に通知する見守りシステムの開発を進めている (図 1)．家庭内において，装着して計測するモバイル計測子機，家庭内でモバイル計測子機からデータを収集するモバイル見守り装置 (親機) からなる．FPGA を搭載した親機において，胎児の心音などを分析し，正常・異常を判断する．あるいは，親機からクラウド環境やオンプレミス環境に設置しているサーバ機へデータを暗号化して送信する．異常時には，かかりつけの産科の医師に連絡する．

見守りシステムの IoT 機器では，個人の生体データを取り扱うため，データ流出や IoT 機器の乗っ取りなどを防ぐ必要がある．

本研究では，見守りシステムを構成する IoT 機器に対するスキャン攻撃，DoS/DDoS 攻撃，telnet や ssh 宛のパスワードクラッキング攻撃などの不正通信を検知することを目標とする．我々は，不正通信を検出するために，IoT 機器自体に検知プログラムを組み込み，ホストベースでの IoT 機器向け検知システム開発に取り組んでいる．本発表ではユーザランドでの検知方法と Linux カーネルモジュールでの検知方法とそれらの予備調査の結果について報告する．

2. 不正通信検知システムの設計

2.1 機能要件

本研究で提案する IoT 機器向けの不正通信検知システムが備えるべき要件を以下に示す．

- IPv4，IPv6 どちらでも対応可能な不正通信検知システムであること
- モバイル見守り装置はバッテリー駆動であり，省電力な検知システムであること

IPv4，IPv6 の両方に対応することについて，家庭内，工場内などでは IoT 機器にグローバル IPv4 アドレスを割り当てることは考えられにくく，プライベート IPv4 アドレスを割り当て NAT/NAPT による運用が一般的と考えられる．一方で，IPv6 については，NAT/NAPT の役割をもつブロードバンドルータをパススルーして，ISP 側が配布している RA を IoT 機器が受け取り，意図せずインターネットから直接 IoT 機器へ接続することが可能となってしまう可能性がある．さらに，IPv6 アドレス空間においてのスキャン活動については，RFC 7707[1] で探索方法について述べられている．このような理由から IPv4，IPv6 の両方に対応した不正通信検知システムを目標とする．

次に，妊産婦が常時携帯するモバイル計測子機は，バッテリーで稼働であり，検知システムがモバイル計測子機が稼働する IoT 機器の電力消費に大きく影響を与えないことが求められる。

2.2 設計方針

攻撃者は，telnet や ssh などのパスワードクラッキング，Web アプリケーションへの攻撃の前に，TCP スキャンや SYN スキャンなどのスキャン攻撃を仕掛けてくる。このとき，自身の IP アドレス以外から TCP SYN セグメントが多く到達することを検知に利用する。そこで，我々は IoT 機器上で稼働している Linux が保持する TCP の接続状態

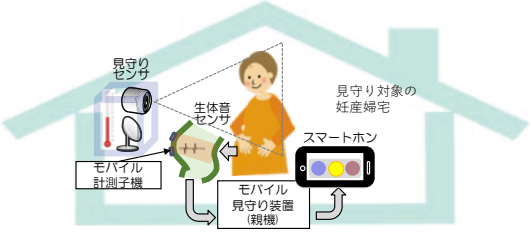

図 1　周産期見守りシステムの概要

1　大分大学理工学部共創理工学科知能情報システムコース
2　大分大学学術情報拠点情報基盤センター
a)　minoru@oita-u.ac.jp
b)　yoshida@oita-u.ac.jp

```
書式) sl: local_address rem_address st tx_queue:rx_queue
tr:tm->when retrnsmit uid timeout inode
例) 3: 0100007F:0277 0100007F:AFBA 01 00000000:00000000
00:00000000 00000000 0 878309 1 0000000000000000
```

図 2 /proc/net/tcp の書式と記載例

を用いて不正通信を検知する方法について検討した．

3. ユーザランドでの不正通信検知プログラムの実装

まず，ユーザモードプロセスで Linux 上で TCP の状態を記録している/proc/net/tcp (IPv4)，および/proc/net/tcp6 (IPv6) から TCP の状態を読み込み，不正通信検知に利用することを試みた．/proc/net/tcp には，図 2 に示す書式で TCP の状態が保持されている．図 2 中の下線部が TCP の状態で，1 から 11 の値をとる．1 が TCP コネクションが確立した ESTABLISH の状態を表す．

/proc/net/tcp ファイルから TCP の状態を定期的に取得しながら，同一送信元からのポートスキャン攻撃，パスワードクラッキング攻撃を検出することを検討した [2]．予備調査として検出条件を導出するために Raspberry Pi に対して，セキュリティスキャナツール Nmap やブルートフォースパスワードクラッキングツール medusa を用いて検証した。このとき，Raspberry Pi 側では，Web サーバを起動して TCP80 番ポートおよび SSH サーバを起動して TCP22 番ポートを開いた状態で，Nmap で TCP コネクションスキャン，TCP SYN スキャンを実行した．Nmap のオプションとしてバージョン検出，OS 検出，オプション指定なしの 3 パターンを指定した．medusa では，SSH に対して，パスワードクラッキング攻撃を実行した．予備調査では，/proc/net/tcp を観測することでパスワードクラッキング攻撃の通信を観測できた．しかしながら，Nmap によるポートスキャンは観測できなかった．原因を調査したところ，Nmap での TCP コネクションスキャンは，TCP スリーウェイハンドシェイクの ACK を返した後に，RST,ACK を送っていた．このタイミングでは，Raspberry Pi 側の TCP の状態が ESTABLISH にならずに/proc/net/tcp には TCP コネクションの情報が書き込まれなかった．/proc/net/tcp を定期的に観測するスキャン攻撃検知は，難しいと判断した．

4. カーネルモジュールでの不正通信検知の検討

次に，netfilter[3] を用いて Linux カーネルモジュールで TCP コネクション確立要求である SYN パケットを観測する手法について検討した．まず，Raspberry Pi Desktop(x86 環境) を VirtualBox 上に構築し，netfilter を用いて TCP のコネクション要求 (SYN フラグのみ) を受信する都度，/var/log/message に送信元 IP アドレス，送信元ポート番号，宛先ポート番号を記録する Linux カーネルモジュールを作成した．試作したカーネルモジュールを組み込み，Nmap による TCP SYN スキャンを観測したところ，Nmap で指定した宛先ポート番号宛の TCP SYN をすべて観測できた (図 3)．

```
Oct 17 14:16:58 raspberry kernel: src 10.0.1.100, dst 53
Oct 17 14:16:58 raspberry kernel: src 10.0.1.100, dst 21
Oct 17 14:16:58 raspberry kernel: src 10.0.1.100, dst 8080
Oct 17 14:16:58 raspberry kernel: src 10.0.1.100, dst 25
Oct 17 14:16:58 raspberry kernel: src 10.0.1.100, dst 993
Oct 17 14:16:58 raspberry kernel: src 10.0.1.100, dst 3306
Oct 17 14:16:58 raspberry kernel: src 10.0.1.100, dst 23
Oct 17 14:16:58 raspberry kernel: src 10.0.1.100, dst 139
```

図 3 nmap で SYN スキャンした際の/var/log/message(一部)

送信元 IP アドレスごとに TCP SYN の数を数え上げる実装として，Linux カーネルが経路表を管理する際に用いる Radix Tree を利用する．本実装では，攻撃者の IP アドレスを保持するために，Radix Tree のデータ構造に，TCP SYN の数を追加し，外部 IP アドレスから TCP SYN が届く度に数え上げている。

5. おわりに

今後は，図 1 中のモバイル見守り子機，親機上で今回示したカーネルモジュールによる TCP SYN を観測する手法を動作させた場合と，させない場合における消費電力を計測する．カーネルモジュールプログラムが，省電力性について有効かどうかを検証する．携帯見守り親機として Raspberry Pi3B+，Raspberry Pi4, 子機として Raspberry Pi Zero W で実験する予定である．

謝辞 本研究開発は総務省 SCOPE(受付番号 192110002) の委託を受けたものです．

参考文献

[1] Gont, F. and Chown, T., Network Reconnaissance in IPv6 Networks, RFC7707, IETF, Mar. 2016, http://tools.ietf.org/rfc/rfc7707.txt
[2] 大谷彩人, 池部　実, 吉崎弘一, 吉田和幸, IoT 向けホストベースポートスキャン攻撃検知システムの提案, 2019 年度（第 72 回）電気・情報関係学会九州支部連合大会, 2019 年 9 月
[3] netfilter firewalling, NAT, and packet mangliing for linux, http://www.netfilter.org, アクセス日: 2020 年 11 月 9 日