マルウェアの動的解析を支援するネットワークシミュレータの提案

2024/1/26

◎原 淳一郎(立命館大学情報理工学部4年)
毛利 公一, 金城 聖(立命館大学)
瀧本 栄二(立命館大学/奈良女子大学)

System Software Laboratory

はじめに(1/2)

■RATやIoTボットなど、多くのマルウェアは外部サーバと通信する
- 外部サーバ: C&Cサーバ、DNSサーバ、Webサーバ など

■外部通信をするマルウェアの動的解析において、マルウェア本来の挙動を観測するには、インターネット接続が必要である

■しかし、攻撃に加担する可能性がある

実際の外部サーバを用いない環境で
動的解析を行うことが望ましい

はじめに(2/2)

■その方法として、外部サーバを模擬した実計算機とマルウェアを通信させ、解析する方法がある

- 実機のセットアップ、ネットワーク構築、それらの設定や構成の変更は大変

■ネットワークシミュレータの柔軟性に着目した

- シミュレータのシナリオファイルを書き換えることで、ノードとネットワークを柔軟に構成できる

ネットワークシミュレータを用いた
マルウェアの動的解析を支援するシステムを提案

既存の動的解析手法と問題点

■外部通信をするマルウェアの動的解析には、以下の方法がある[1]

1. マルウェアが通信する外部サーバを模擬した、模擬サーバを用意
2. マルウェア動作環境で、マルウェアを実行
3. 動作環境から外部への通信に対し、模擬サーバが応答
4. マルウェアと模擬サーバが通信することで、マルウェアを欺瞞し解析

■実機を用いた方法の問題点

- 実機を複数台用意するコストが高い
- マルウェアに応じた環境を構築するために手間がかかる
- ネットワーク構成の変更にも手間がかかる

[1] 鉄 穎, 楊 笛, 保泉 拓哉, 中山 颯, 吉岡 克成, 松本 勉 : IoTマルウェアによるDDoS攻撃の動的解析による観測と分析, 情報処理学会論文誌, pp.1321-1333 (2018/5)

問題点を解決するための要件

問題点を解決するためには、

- 少数の実機で実現可能であること
- ネットワークを柔軟に変更できること
  - 環境を大きく変更せずとも、ある程度マルウェアが想定する通信が可能である

の2つが必要であり、以下の要件を満たすことが求められる

要件1: 1台の実計算機内で完結した環境を構築

- マルウェア動作環境
- 通信制御部
- 模擬サーバ

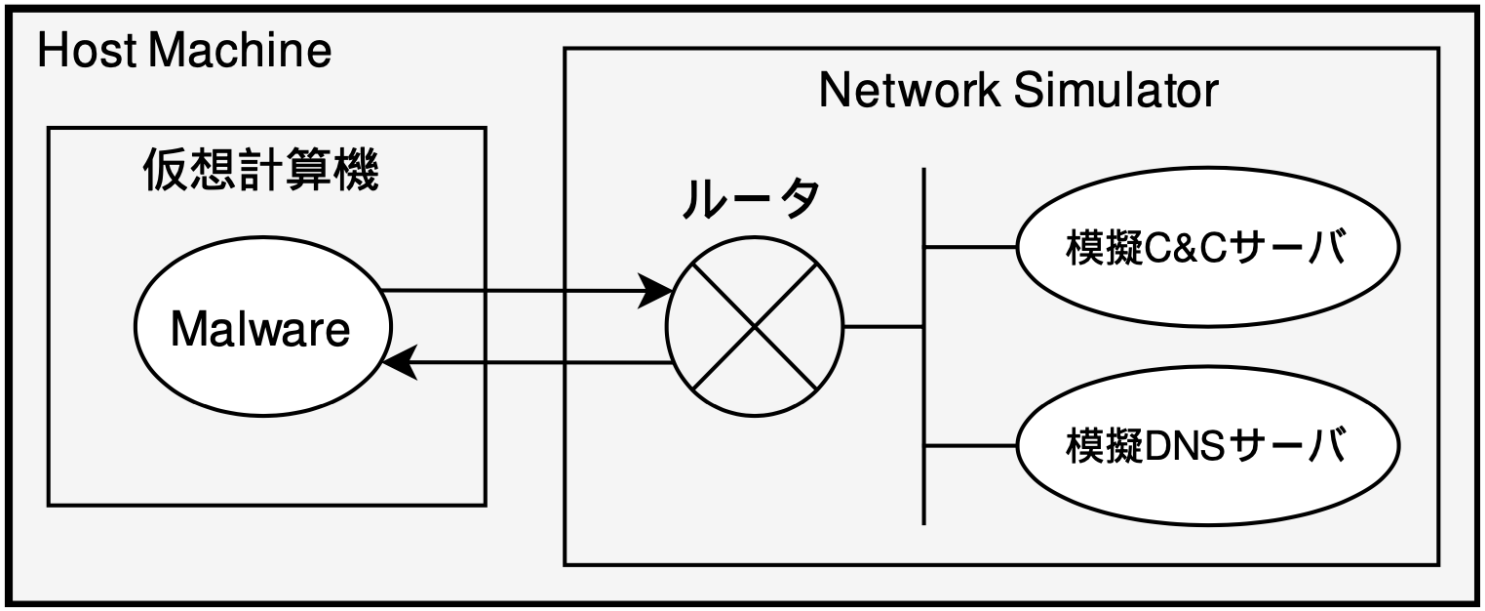
要件2: 宛先IPアドレスに関わらず通信を柔軟に確立

- マルウェアは、不特定の相手と通信

提案手法

- ネットワークシミュレータを用いて、通信制御部であるルータと、模擬サーバを構築 → ネットワークの構築・変更が容易
- ポート番号ベースのルーティングにより、IPアドレスに依存せず、適切な模擬サーバへ転送
  - その際に発生するIPアドレスの不一致には、パケットを書き換え対処

  → 模擬サーバとの柔軟な通信を確立



提案手法による動的解析方法

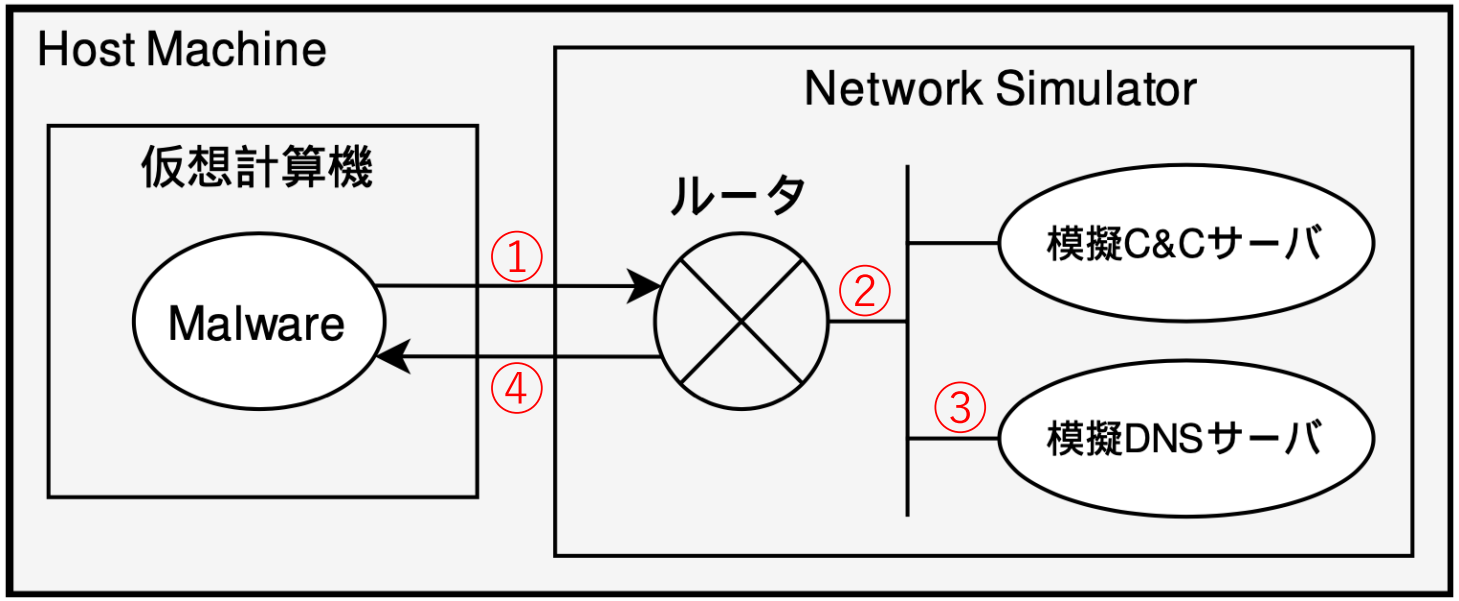
以下のように、マルウェアを欺瞞することで、動的解析を行う

① マルウェアの全通信をルータに取り込む

② ルータが、宛先ポート番号に応じて、特定の模擬サーバへ転送

③ 宛先IPアドレスを書き換え、模擬サーバがパケットを受理

④ 模擬サーバ → マルウェアは逆の経路をたどり、通信が成立



宛先ポート番号に応じたルーティング

■マルウェアは、不特定の相手と通信

→ IPアドレスではなく、通信プロトコルと宛先ポート番号に基づきルーティングを行うことで解決する

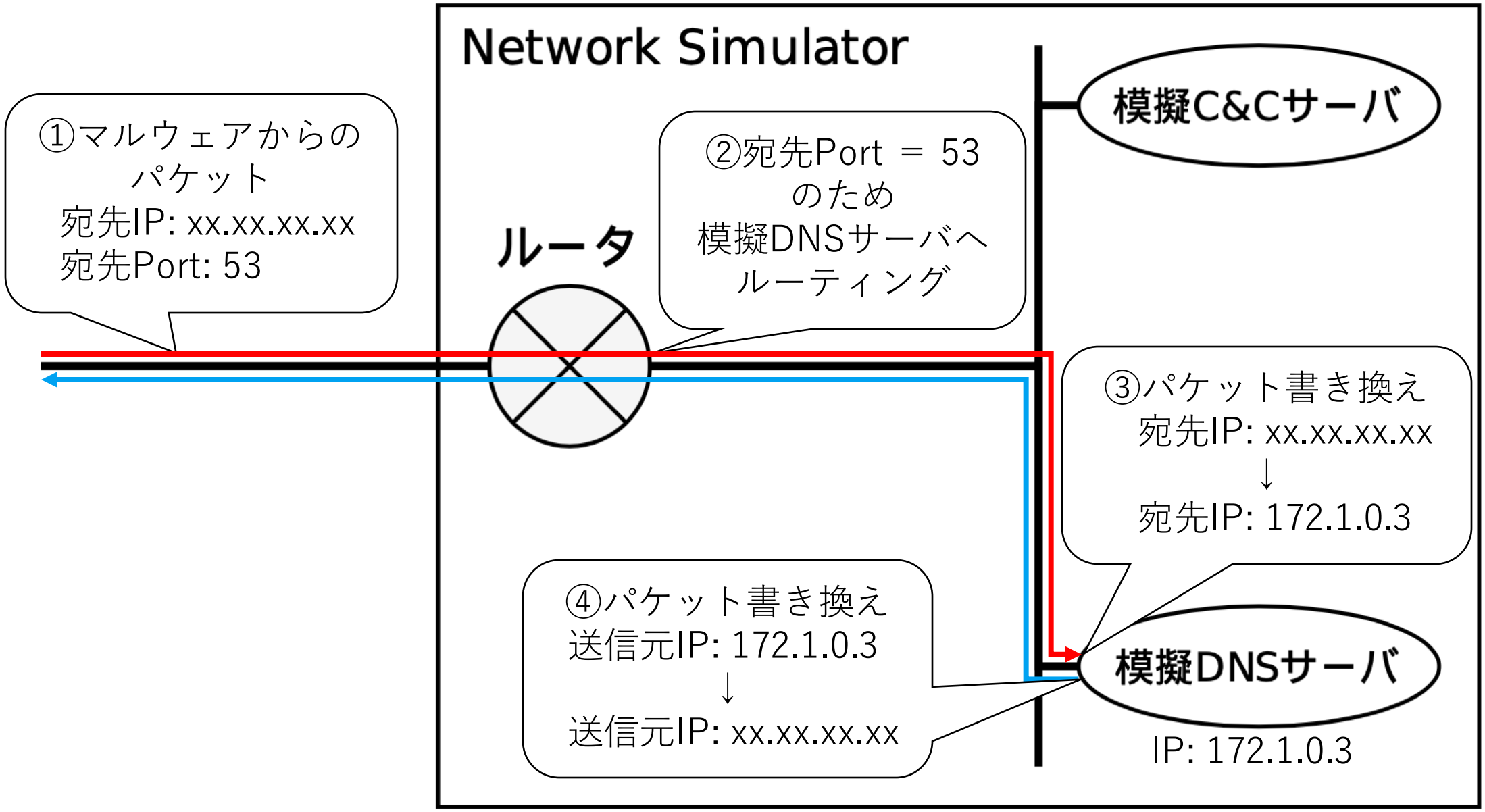
■例えば、「UDPの53番ポート宛」のパケットならば、DNSサーバ宛のパケットであると推測可能 → 模擬DNSサーバにルーティング

通信プロトコル	宛先ポート番号	ルーティング先の模擬サーバ
TCP	23	模擬Telnetサーバ
TCP	80	模擬HTTPサーバ
UDP	53	模擬DNSサーバ
TCP, UDP	その他	sinkサーバ

模擬サーバでのパケット受理方法

- 模擬サーバが受信するパケットは、宛先IPアドレスが模擬サーバのものではない
  - ルータがポート番号によるルーティングを行うため
  - 宛先IPアドレスが自身のIPアドレスと異なる場合、TCP/IPレイヤで、パケットが破棄される
- 模擬サーバにパケット到着時、TCP/IPレイヤでパケットを書き換えることにより、受理可能
  - 宛先IPアドレスと宛先ポート番号を模擬サーバのものとする
  - sinkサーバなどでは、宛先ポート番号が模擬サーバのlistenポートと一致しない場合があるため、宛先ポート番号も書き換える
- パケット送信時は、送信元IPアドレスと送信元ポート番号を書き換える

マルウェアと模擬サーバの通信例



提案手法の実現可能性調査に向けて

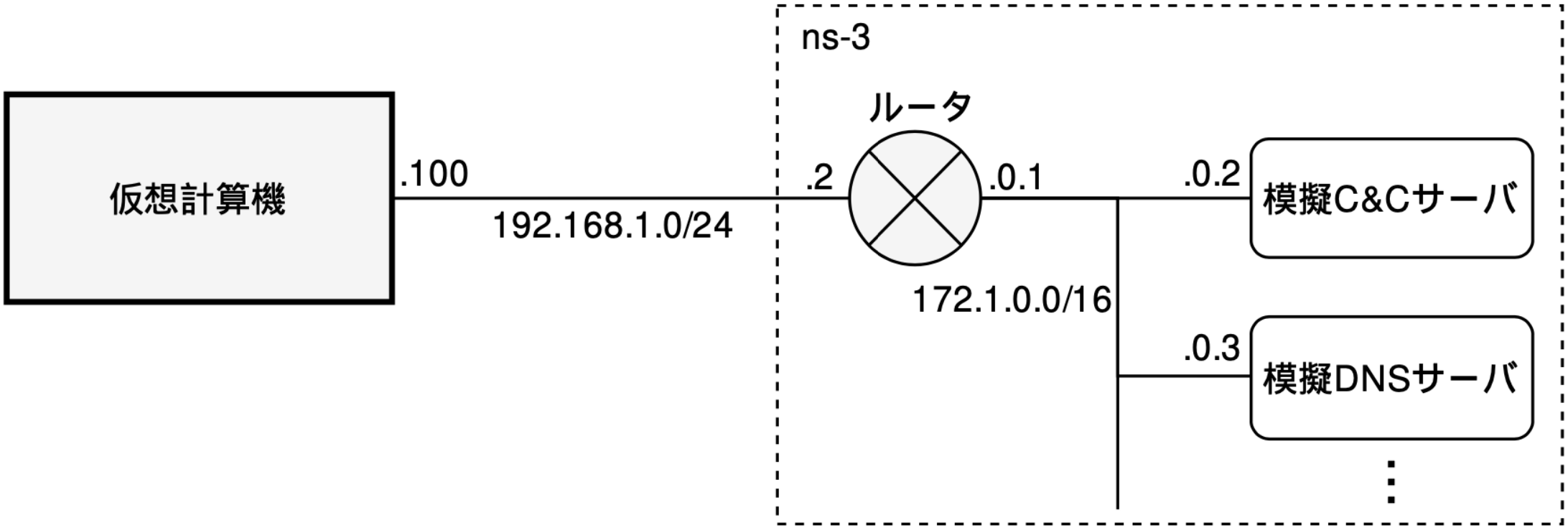
■実際に動的解析を行うことで、提案手法の実現可能性を検証

■今回は、IoTマルウェアMiraiの動的解析を行う
- IoTマルウェアは、外部サーバとの通信を前提に作成されている
  - Miraiは、C&Cサーバ、DNSサーバ、Telnetサーバなどの外部サーバと通信
- すでに解析がされていることや、ソースコード[2]が公開されているため、外部サーバの仕様を把握可能である
  - 適切な挙動をする模擬サーバを作成可能

■提案手法の実装の際に、Miraiが通信する外部サーバを模擬したサーバを作成した
- 模擬C&Cサーバ、模擬DNSサーバ、模擬Telnetサーバなど

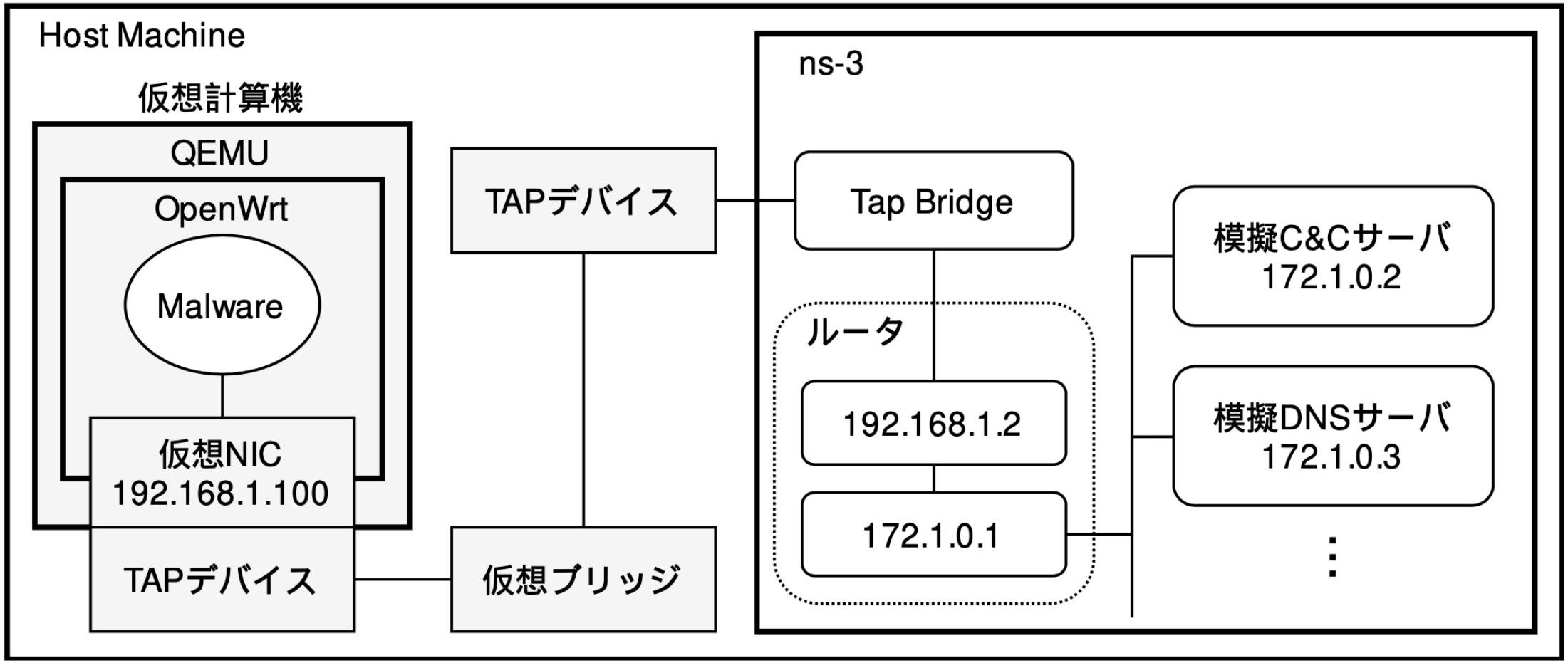
[2] Jerry Gamblin, Miraiのソースコード, https://github.com/jgamblin/Mirai-Source-Code (accessed 2024/1/16)

ネットワーク論理構成



- 仮想計算機のデフォルトゲートウェイをns-3内のルータに設定
- すべての通信がルータを通るため、ルータで、ns-3の内部と外部の通信を制御可能
- ns-3内に、Miraiと通信する模擬サーバを作成

ネットワーク物理構成



- ns-3は、Tap Bridgeの機能により、ホストのTAPデバイスと通信が可能
- ここでは、TAPデバイスは、仮想ブリッジのインタフェースのように使用

仮想計算機と模擬サーバの通信の検証

■ルーティング機能とパケット書き換え機能を実装し、検証した

■動作例

- 仮想計算機
  ↔ 模擬DNSサーバ

```
root@OpenWrt:/# nslookup test.com 11.22.33.44
Server:         11.22.33.44
Address:        11.22.33.44#53

Name:       test.com
Address 1: 172.1.0.5
Address 2: 172.1.0.5
```

ネットワーク上に存在しない
IPアドレス

- 仮想計算機
  ↔ 模擬HTTPサーバ

```
root@OpenWrt:/# wget http://22.33.44.55/something
Downloading 'http://22.33.44.55/something'
Connecting to 22.33.44.55:80
Writing to 'something'
something             100% |************************
**********|    57   0:00:00 ETA
Download completed (57 bytes)
```

模擬サーバが
応答している

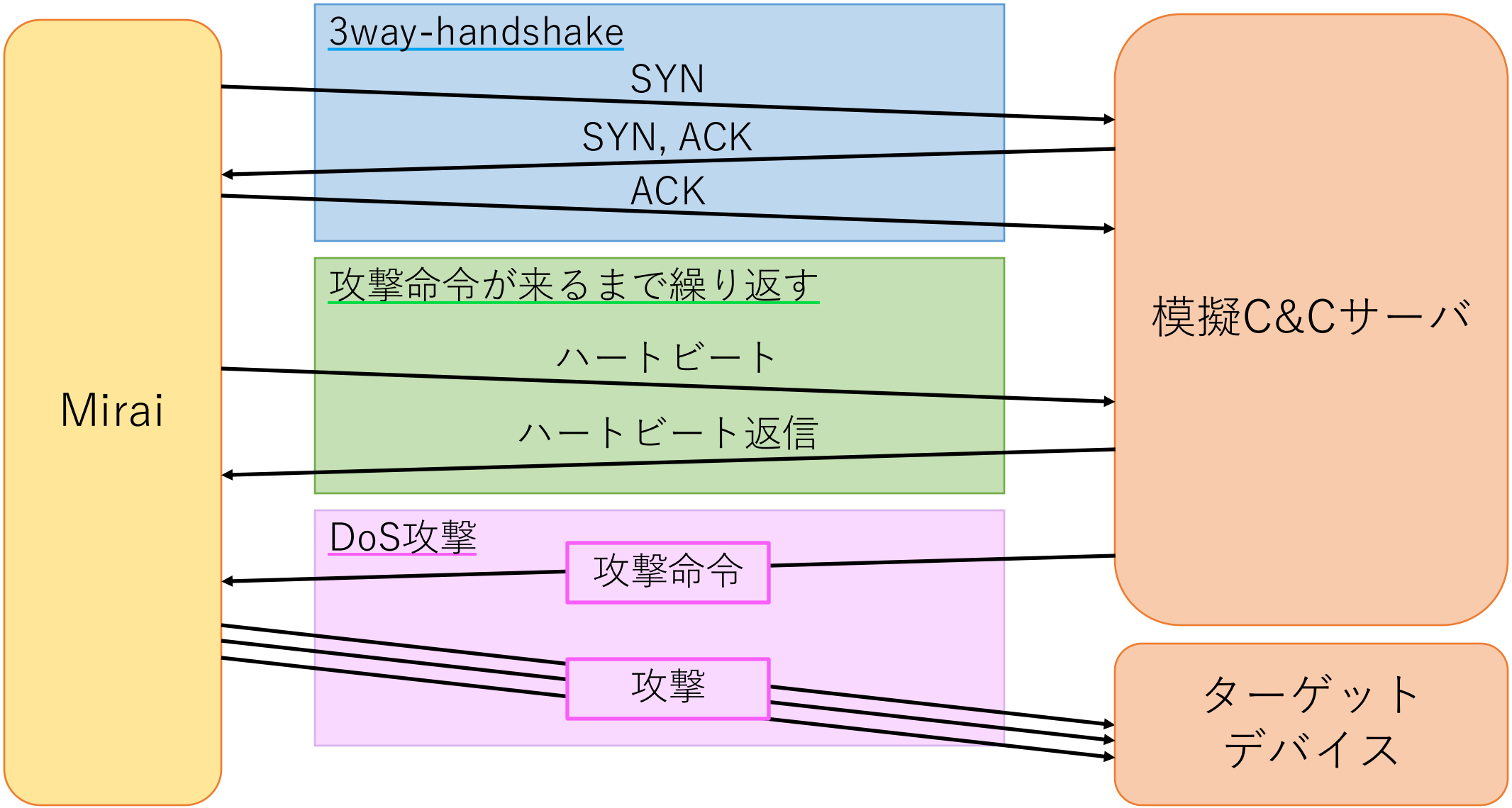
提案手法の検証

Miraiの動的解析を行う

■検証１：MiraiによるDoS攻撃の観測
- 使用する模擬サーバ
  - 模擬C&C, 模擬DNSサーバ
- 検証内容
  - Miraiが模擬C&Cサーバからの攻撃命令を理解し、DoS攻撃を行うか

■検証２：Miraiの感染拡大活動の観測
- 使用する模擬サーバ
  - 模擬DNS, 模擬Telnet, 模擬レポートサーバ
- 検証内容
  - 感染拡大活動の主要な動作である、総当たり攻撃とレポートサーバへの報告の観測

検証１：Miraiと模擬C&Cサーバの通信想定



検証１：MiraiによるDoS攻撃の観測

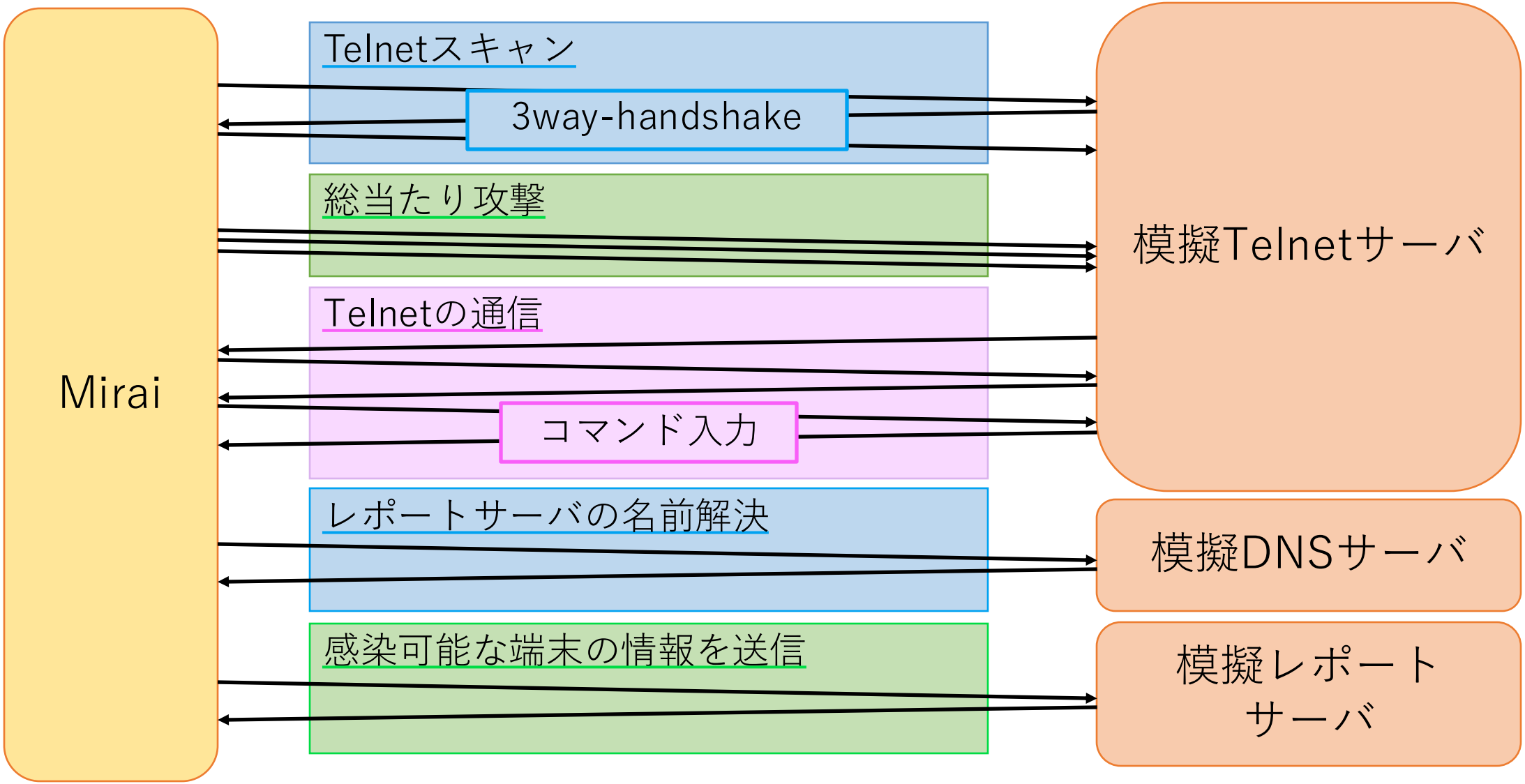
模擬C&Cサーバ: 172.1.0.2
Mirai: 192.168.1.100

模擬C&CサーバからMiraiに、
「1.2.3.4にUDPフラッド攻撃」
を行う攻撃命令を送信

Time	Source	Destination	Protocol	Length	Info
10.043396…	172.1.0.2	192.168.1.100	TCP	80	23 → 43066 [ACK] Seq=1 Ack=8 Win=131072 Len=14
10.044804…	192.168.1.100	172.1.0.2	TCP	66	43066 → 23 [ACK] Seq=8 Ack=15 Win=29200 Len=0 T
10.057177…	192.168.1.100	1.2.3.4	UDP	554	65084 → 477 Len=512
10.059431…	192.168.1.100	1.2.3.4	UDP	554	65084 → 477 Len=512
10.060161…	192.168.1.100	1.2.3.4	UDP	554	65084 → 477 Len=512
10.060797…	192.168.1.100	1.2.3.4	UDP	554	65084 → 477 Len=512
10.061221…	192.168.1.100	1.2.3.4	UDP	554	65084 → 477 Len=512
10.061633…	192.168.1.100	1.2.3.4	UDP	554	65084 → 477 Len=512
10.062036…	192.168.1.100	1.2.3.4	UDP	554	65084 → 477 Len=512
10.062432…	192.168.1.100	1.2.3.4	UDP	554	65084 → 477 Len=512

Miraiは、短時間に、
大量のUDPパケットを1.2.3.4に送信
（1秒間におよそ8,000個のパケット）

検証２：Miraiの感染活動の通信想定



検証２：Miraiの感染拡大活動の観測

①総当たり攻撃

模擬Telnetサーバに、何度も
ユーザ名とパスワードを入力

```
Telnet-Server: -Login Information-
    UserName: root
    Password: vizxv

Telnet-Server: -Login Information-
    UserName: admin
    Password: admin
```

②コマンドの送受信

```
Telnet-Server: -Receive-
  size: 19
  str : /bin/busybox MIRAI
  hex : 2f62696e2f62757379626f78204d4952414900

Telnet-Server: -Receive-
  size: 2
  str :

  hex : 0d0a

Telnet-Server: -Send-
  size: 24
  str : MIRAI: applet not found
```

③レポートサーバへの報告

感染可能な端末の情報を
模擬レポートサーバに送信

```
Report-Server: -Receive-
  size: 16
  str : ^◆◆6root1234
  hex : 5ea6a236001704726f6f740431323334
```

5ea6a236 : IPアドレス（→ 94.166.162.54）
0017 : ポート番号 （→ 23）
04 : ユーザ名len （→ 4）
726f6f74 : ユーザ名 （→ root）
04 : パスワードlen （→ 4）
31323334 : パスワード（→ 1234）

おわりに

- 提案システムを用いた動的解析の結果、Miraiの挙動として、DoS攻撃と感染拡大活動を観測した
  - Miraiが可能な10種類の攻撃すべてを観測した
  - 感染拡大活動の一連の流れを観測した
  - 提案手法を用いてMiraiを欺瞞した動的解析が可能なことを実証した
- Miraiの亜種(MoziやTsunami)に対しても、有効な手法である
  - C&Cサーバの特定や初期動作の観測が可能

- 容易に構築でき、柔軟に変更可能な、動的解析環境の実現可能性を明らかにした
  - 1つの実計算機内で完結した環境を構築可能
  - 宛先IPアドレスに関わらず通信を柔軟に確立可能
  - 今後は、IoTマルウェア以外について検討していく