BBSakura Networks

トラフィックグラフはどう作られる？
～NetFlowを使ってみる～

BBSakura Networks 株式会社　外山 結月

自己紹介

- 外山 結月（とやま ゆづき）
  - 所属：BBSakura Networks株式会社 / BBIX株式会社
    ITシステム室
- 経歴
  - 2024年4月 ~ 現在：BBSakura Networks株式会社 / BBIX株式会社
    - 社内業務システムの開発
    - 新卒2年目
- JANOG参加歴
  - 初参加

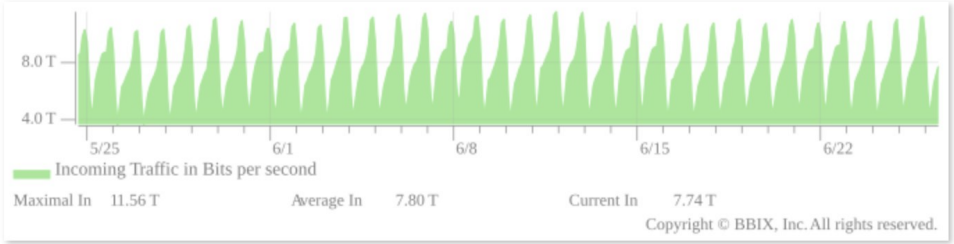
BBSakura Networks

Daily Graph (5 Minute Average)

Weekly Graph (5 Minute Average)

トラフィックグラフ

Monthly Graph (5 Minute Average)

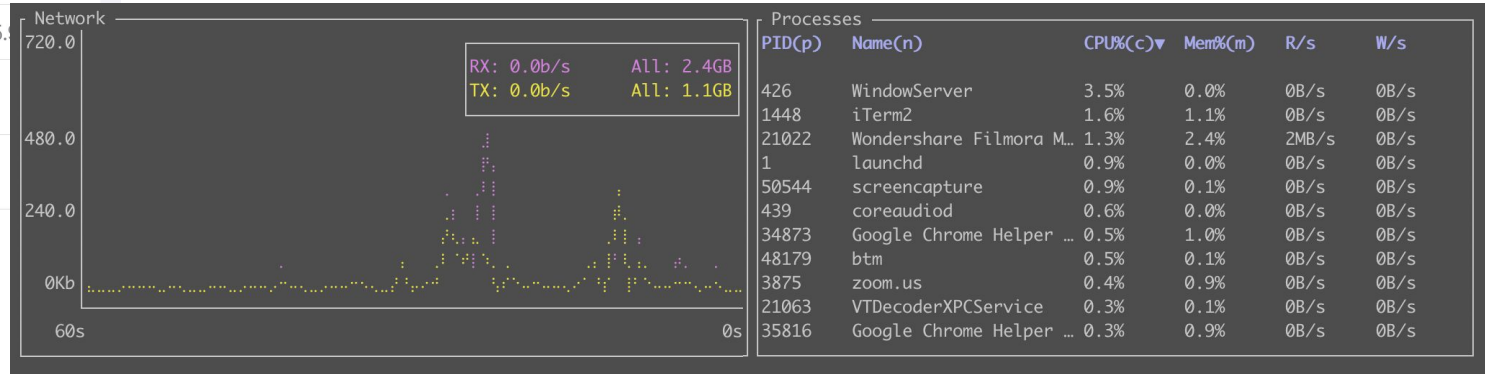


https://www.bbix.net/service/ix/traffic-graph/

トラフィックグラフとは

- 例えば、

  PCやiPhoneでのアプリごとの通信の使用状況を時間単位でグラフ化したもの！



トラフィックグラフとは

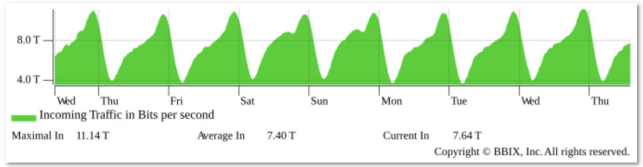
- 例えば、

  PCやiPhoneでのアプリごとの通信の使用状況を時間単位でグラフ化したもの！

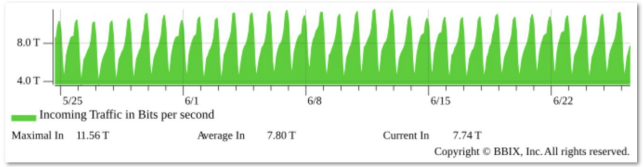
- 機器間の通信量を視覚的に把握できる
  - トラフィックの増減
  - 帯域利用状況の確認

Daily Graph (5 Minute Average)

Weekly Graph (5 Minute Average)

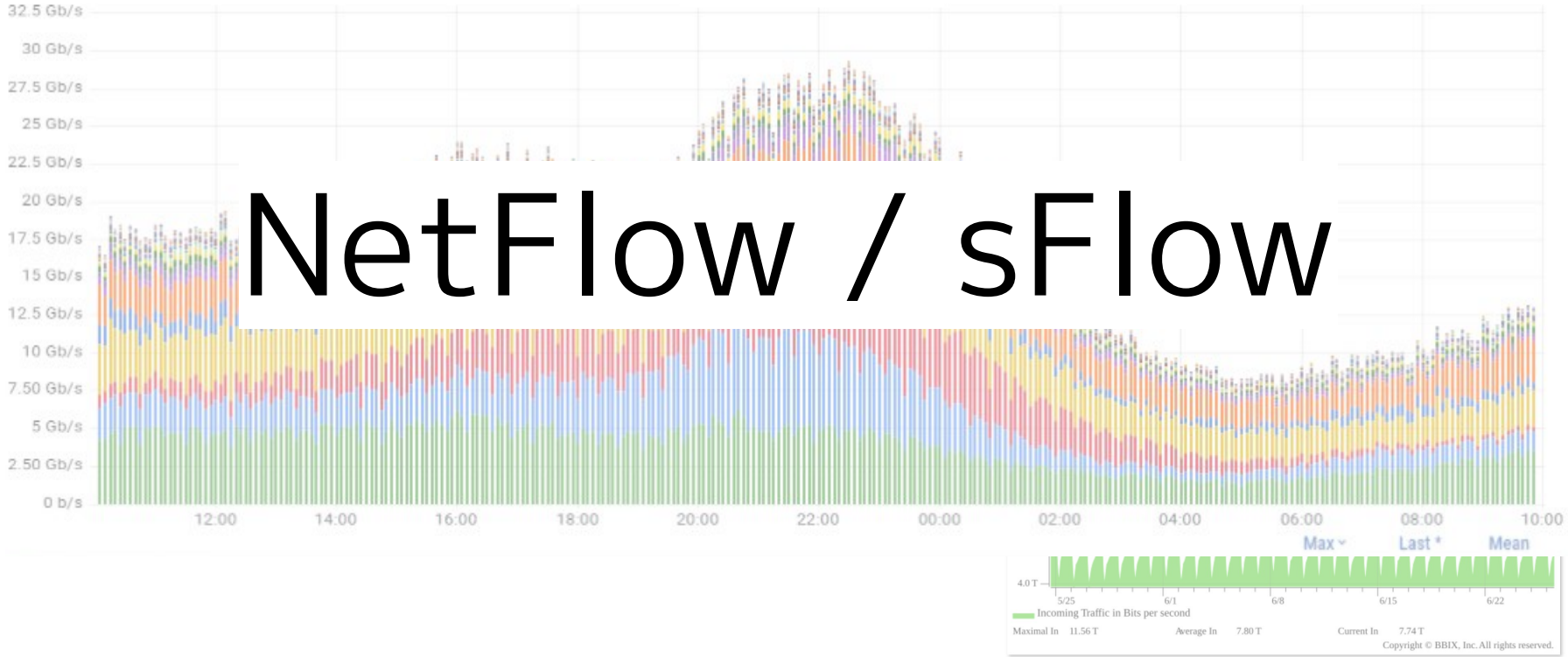


Monthly Graph (5 Minute Average)



トラフィックグラフとは

- 例えば



NetFlow / sFlow

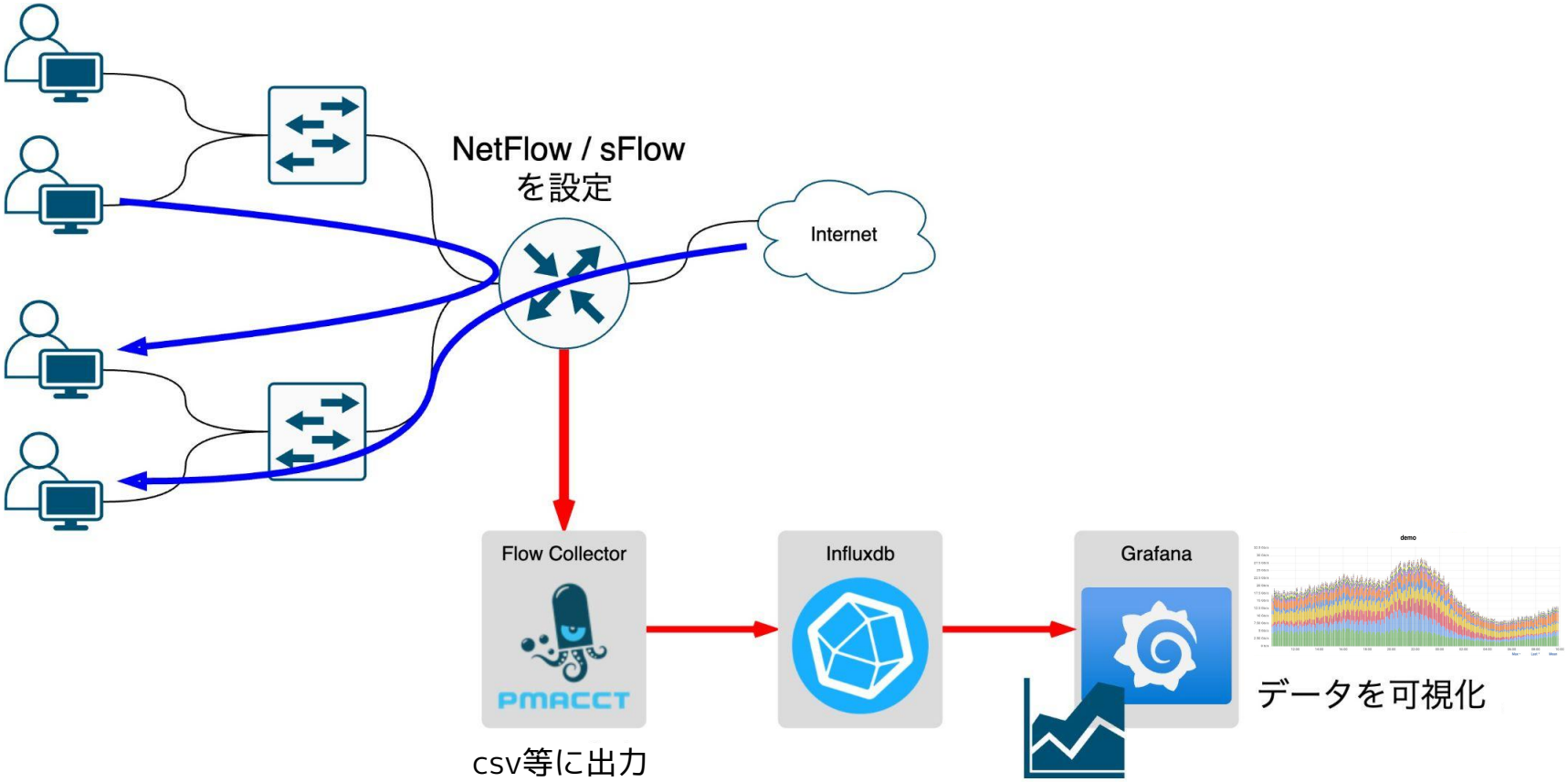
!

NetFlow / sFlowってなに？

- **パケットを参照して、フローデータを送信するためのプロトコル**
- **インタフェースに設定を入れると、収集用サーバーにフローデータを送信する**

	NetFlow	sFlow	SNMP
標準化	Cisco社独自 →IPFIX標準（RFC7011）	RFC3176	RFC1215
監視対象	トラフィック	トラフィック	機器の状態（CPU / メモリ / インタフェース使用率）
特徴	フロー単位で集計処理 セッションごとに統計情報を生成	一部のパケットのヘッダー サンプリングされたパケットのヘッダー(+一部ペイロード)	MIBでトラフィックの総量
取得方式	Push型	Push型	Pull型

トラフィックグラフ生成のながれ



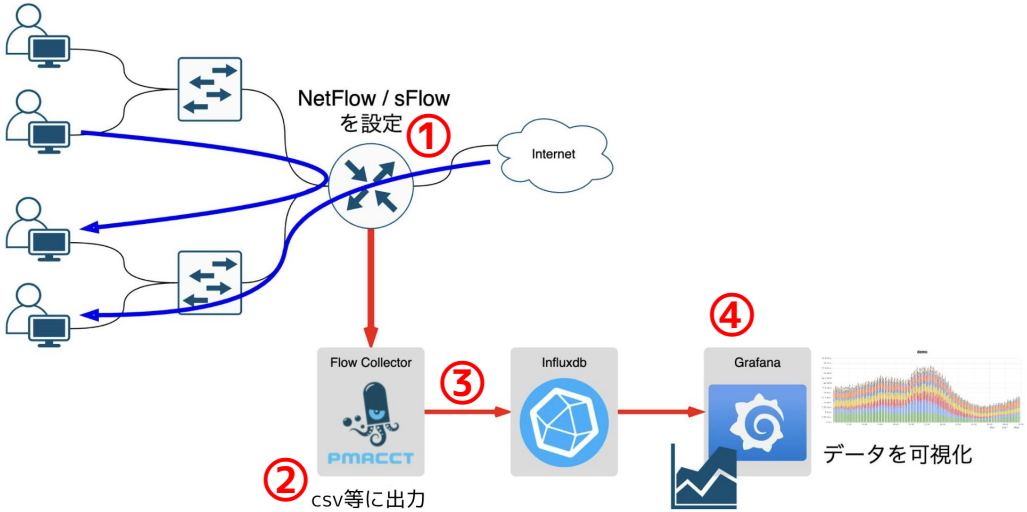
NetFlowを使ってみる

Step 1: Routerにフローデータの送信先を設定

Step 2: Flow Collectorサーバーで取得したい情報を指定

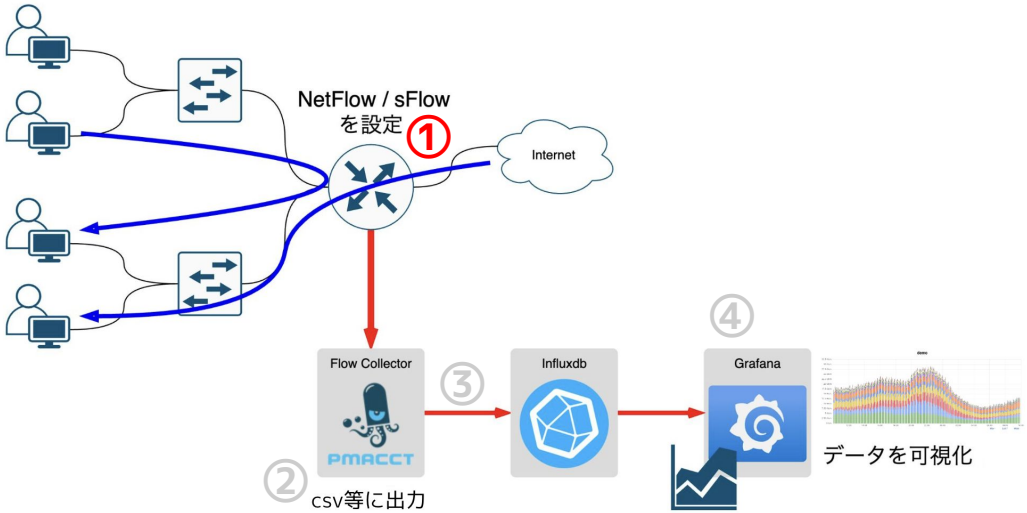
Step 3: 取得した情報を変換、InfluxDBへ挿入

Step 4: Grafanaでデータを可視化



Step 1: Routerにフローデータの送信先を設定

```
configure terminal
!
ip flow-export version 9
ip flow-export destination 192.168.1.1 2055
!
flow-sampler-map sampler
 mode random one-out-of 8000
!
interface GigabitEthernet 0/0
 ip flow ingress
 ip flow egress
 flow-sampler sampler
!
end
```

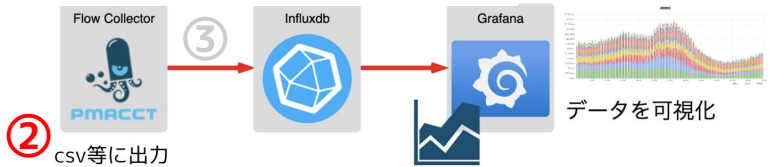


Step 2: Flow Collectorサーバーで取得したい情報を指定

```
sudo apt update
sudo apt install pmacct
sudo vim /etc/pmacct/nfacctd.conf

    nfacctd_ext_sampling_rate: 8000
    !
    aggregate: timestamp_start, in_iface, out_iface, src_net, dst_net
    !
    plugins: print
    print_output: csv
    print_output_file: /var/nfacctd/csvs/netflow.%Y%m%d-%H%M.csv
    print_output_file_append: true

sudo systemctl start nfacctd
sudo systemctl enable nfacctd
```



Step 3: 取得した情報を変換、InfluxDBへ挿入

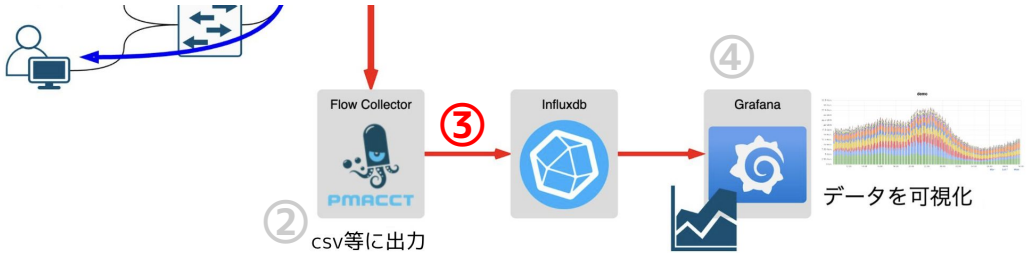
[pmacctの出力形式]

```
$ head -n 2 netflow.20250728-0000.csv
IN_IFACE,OUT_IFACE,SRC_NET,DST_NET,TIMESTAMP_START,PACKETS,BYTES
1,2,10.249.1.0,10.249.2.0,2025-07-28 00:00:00.000000,1,79
```

[InfluxDBへimportの形式]

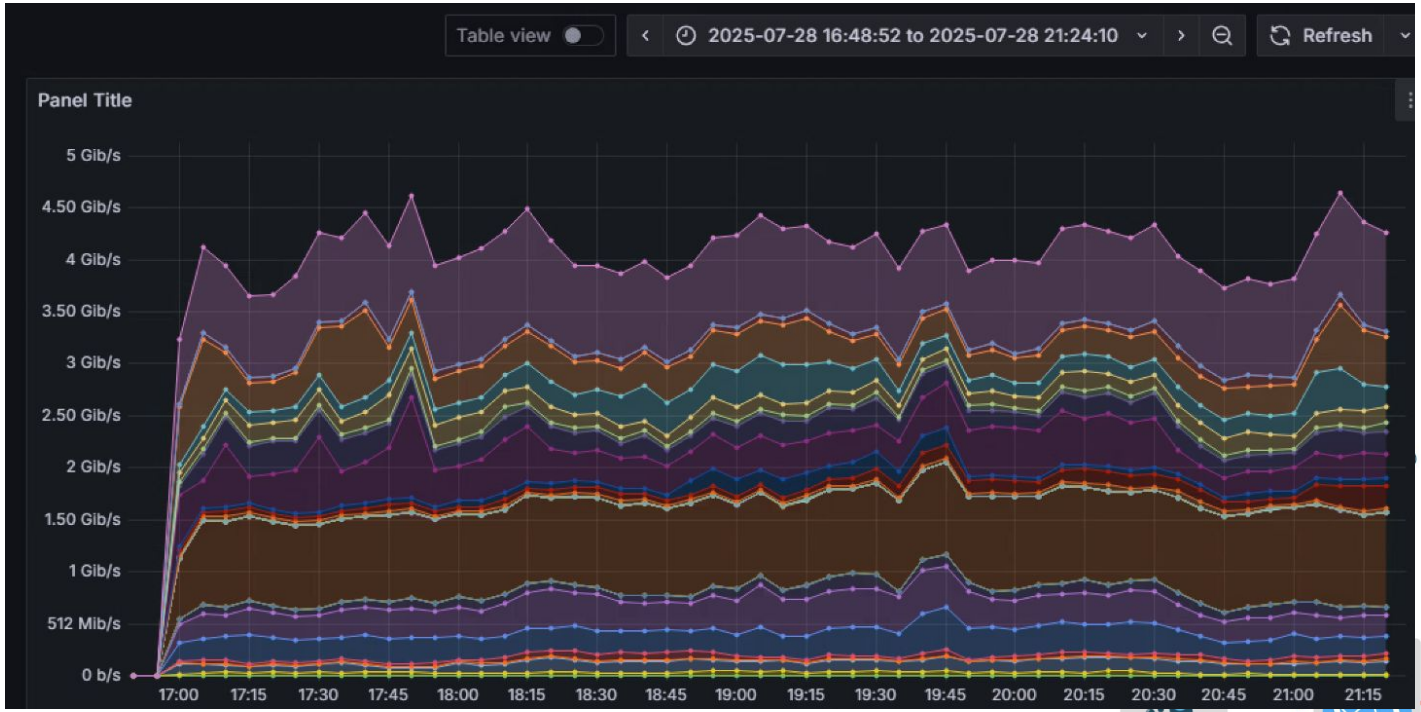
```
$ head -n 3 netflow.20250728-0000.influx
# DML
# CONTEXT-DATABASE: database
traffic,iface_in=1,iface_out=2,net_src="10.249.1.0",net_dst="10.
249.2.0" bps=10000.0 1753628400000000000
```

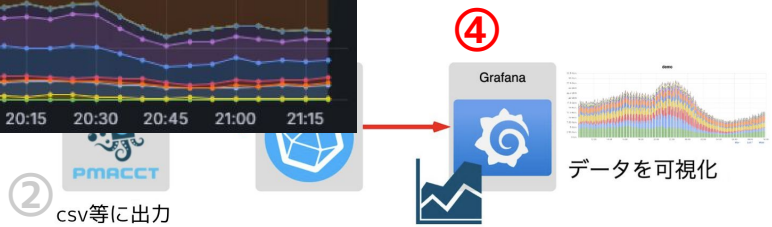
```
$ influx -import -path=./netflow.20250728-0000.influx
```



Step 4: Grafanaでデータを可視化

同一IFでのsrc_netの内訳など、詳細を確認できる！





まとめ

NetFlow, sFlowでトラフィックの詳細を可視化できる！

手順は4Step！

Enabling a Connected Future.

BBSakuraNetworks