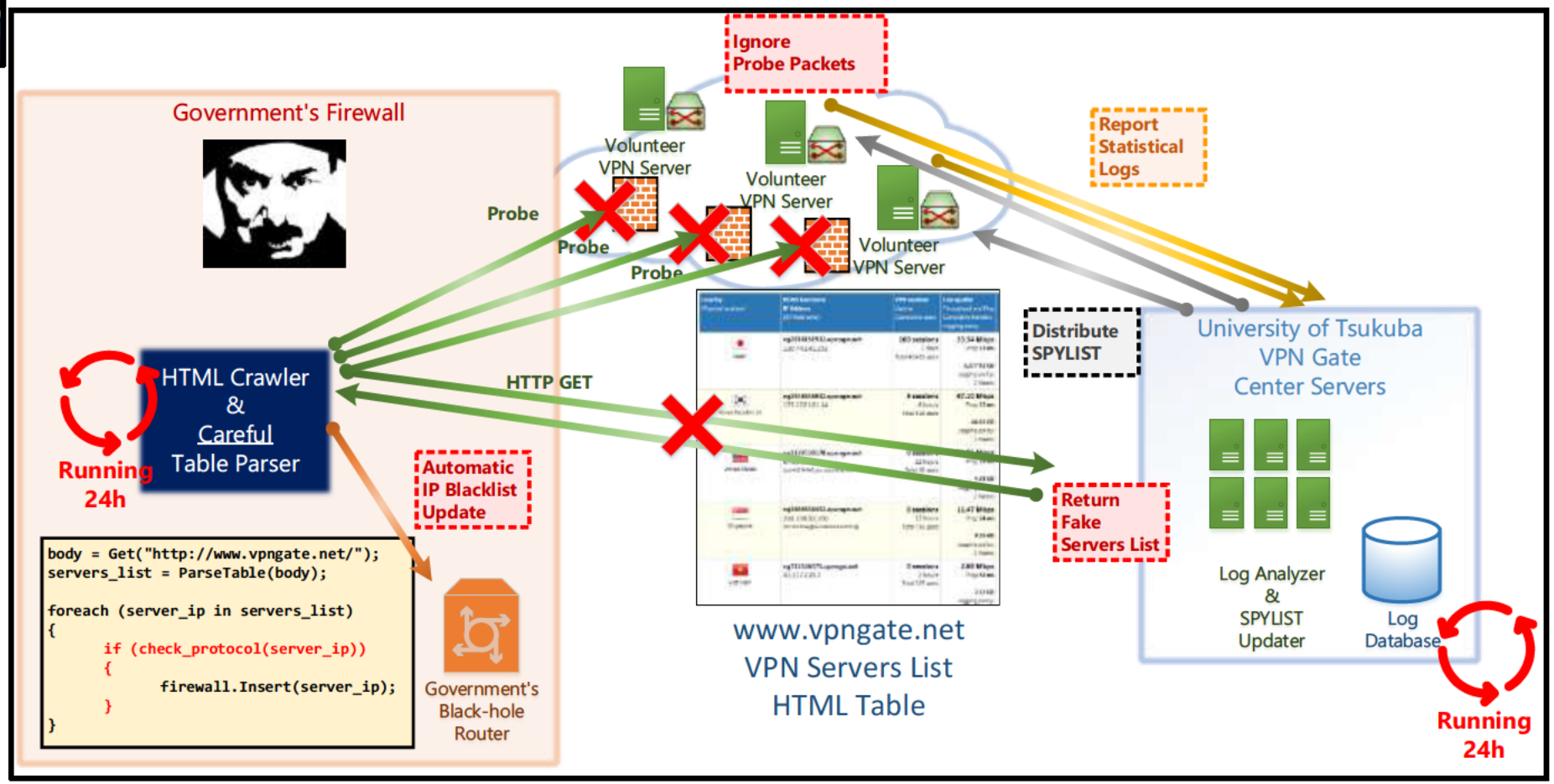
「ソフトイーサ PPPoE 実験用アクセスポイント」,「NTT 東日本-IPA シン・テレワークシステム」, etc おもしろ開発秘話

登 大遊

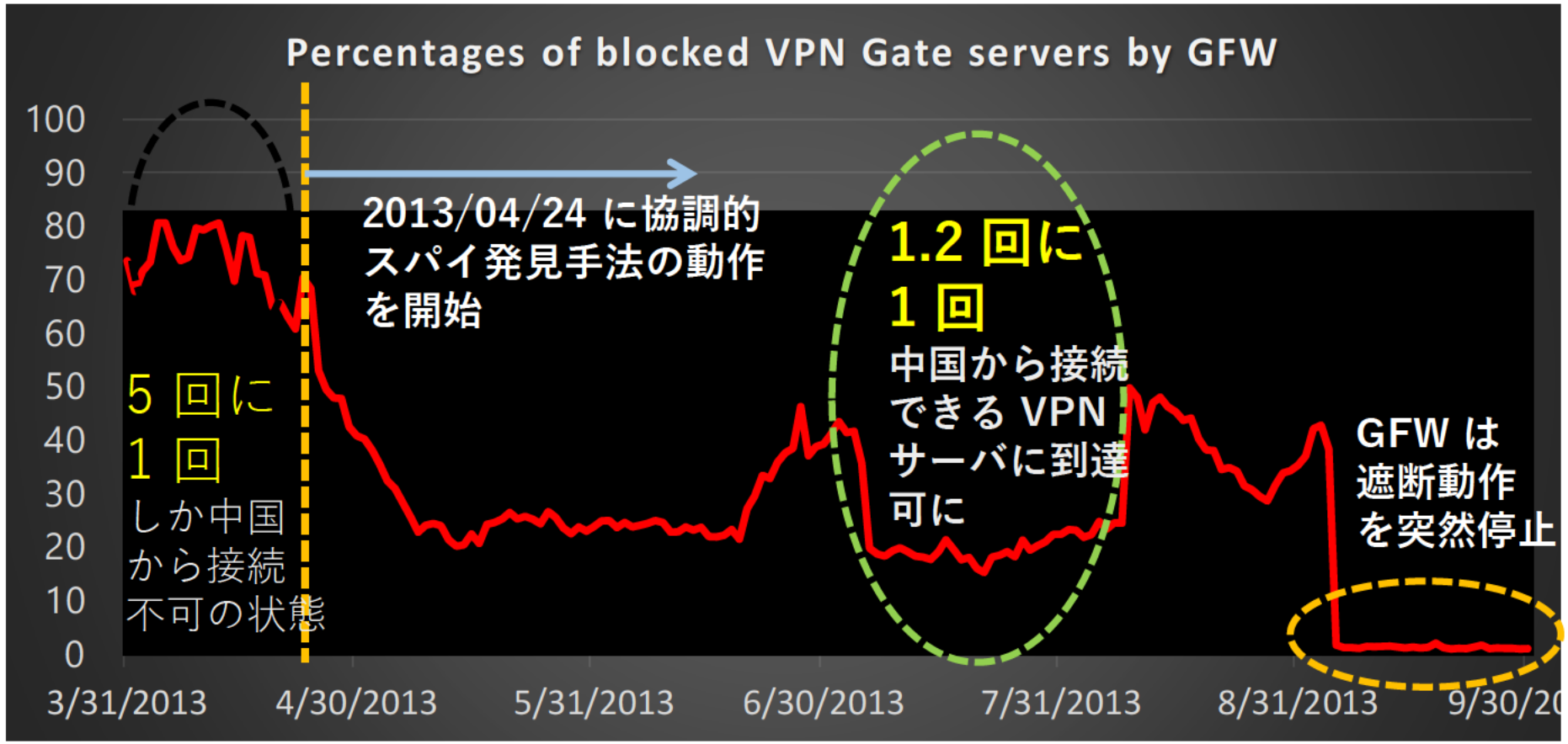
登 大遊 自己紹介

- サイバー空間の橋・トンネルを作り管理する
  「SoftEther VPN」 仮想プライベートネットワーク
  IPA 未踏ソフトウェア創造事業で開発 (2003.12)
  全世界で 476 万の組織・個人で利用 (うち 日本 10%, 海外 90%)
  「VPN Gate」 検閲回避システム
  政府の検閲用ファイアウォールを回避する分散中継システム
- サイバー活動
  1. **ソフトイーサ株式会社 代表取締役 (2004.4 -)**
  2. **筑波大学 産学連携准教授 (2017.4 -)**
  3. **独立行政法人 情報処理推進機構 (IPA)**
     「産業サイバーセキュリティセンター」 (2017 -) サイバー技術研究室長 (2018.7 -)
  4. **NTT 東日本 ビジネス開発本部第一部門 ネットワークサービス担当 社員 (2020.4 -)**
  5. **茨城県警察本部 サイバーセキュリティ対策テクニカルアドバイザー (2017.2 -)**

Great Firewall の検閲への耐性を有するサイバー技術「VPN Gate」を開発



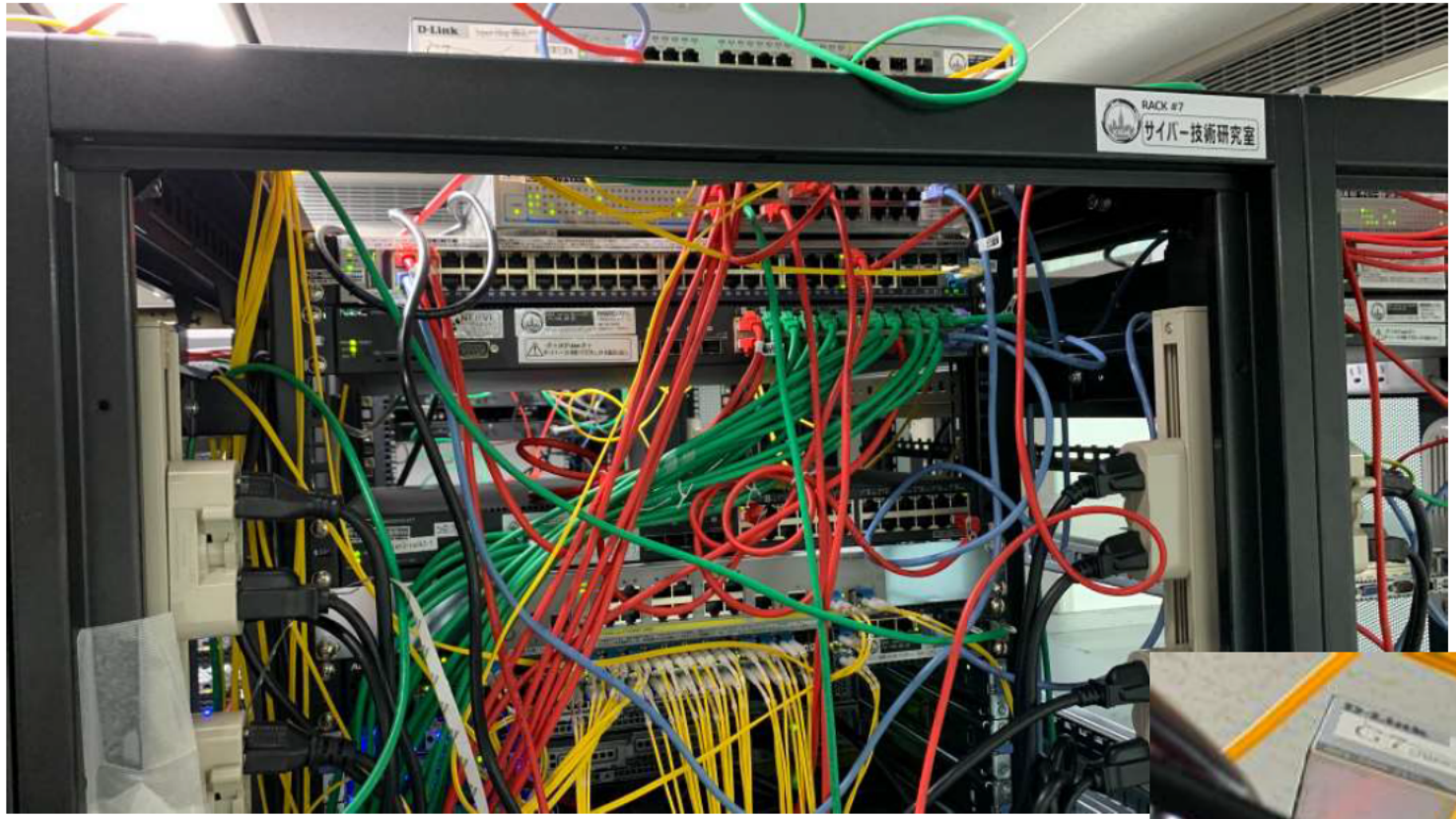
2013 年 4 月 24 日に開始した協調的スパイ発見手法の効果



超難関国際会議
USENIX NSDI 2014
Seattle
で論文発表
(筆頭著者日本人として初めて)


VPN Gate: A Volunteer-Organized Public VPN Relay System with Blocking Resistance for Bypassing Government Censorship Firewalls

最近やっている頭おかしいこと


D-Link
RACK #7
サイバー技術研究室

新型コロナ対策のためソフトイーサ社のフレッツ用 PPPoE 実験用アクセスポイントをテレワーク用に無償開放 (内部コード名: Let's PPPoE) 2020.3.6 ～

- https://www.softether.jp/7-news/2020.03.06

新型コロナ対策のためソフトイーサ社のフレッツ用 PPPoE 実験用アクセスポイントをテレワーク用に無償開放

2020 年 3 月 6 日 (金)

PPPoE へ接続

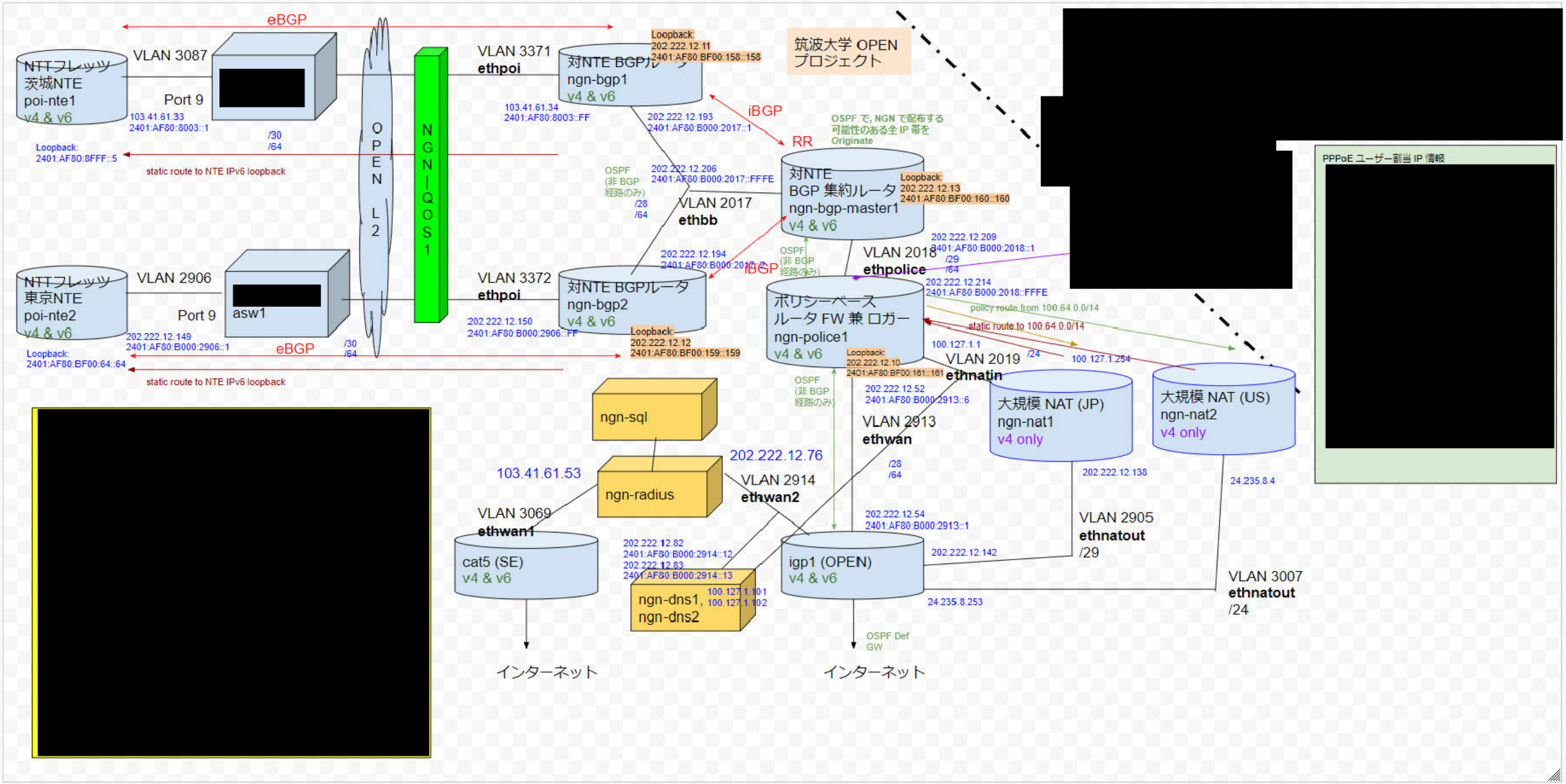
ユーザー名(U): open@open.ad.jp

パスワード(P): open

次のユーザーが接続するとき使用するために、このユーザー名とパスワードを保存する(S):

- このユーザーのみ(N)
- このコンピューターを使うすべてのユーザー(A)

接続(C) キャンセル プロパティ(O) ヘルプ(H)


eBGP
NTTフレッツ
茨城NTE
poi-nte1
v4 & v6
VLAN 3087
Port 9
103.41.61.33
2401:AF80:8003::1
/30
/64
Loopback:
2401:AF80:8FFF::5
static route to NTE IPv6 loopback
OPEN
L2
NGN-QOS1
VLAN 3371
ethpoi
対NTE BGPルータ
ngn-bgp1
v4 & v6
Loopback:
202.222.12.11
2401:AF80:BF00:158::158
103.41.61.34
2401:AF80:8003::FF
202.222.12.193
2401:AF80:B000:2017::1
iBGP
RR
筑波大学 OPEN
プロジェクト
OSPF で, NGN で配布する
可能性のある全 IP 帯を
Originate
OSPF
(非 BGP
経路のみ)
/28
/64
202.222.12.206
2401:AF80:B000:2017::FFFE
VLAN 2017
ethbb
対NTE
BGP 集約ルータ
ngn-bgp-master1
v4 & v6
Loopback:
202.222.12.13
2401:AF80:BF00:160::160
PPPoE ユーザー割当 IP 情報
NTTフレッツ
東京NTE
poi-nte2
v4 & v6
VLAN 2906
Port 9
asw1
202.222.12.149
2401:AF80:B000:2906::1
Loopback:
2401:AF80:BF00:64::64
eBGP
/30
/64
static route to NTE IPv6 loopback
VLAN 3372
ethpoi
対NTE BGPルータ
ngn-bgp2
v4 & v6
202.222.12.150
2401:AF80:B000:2906::FF
Loopback:
202.222.12.12
2401:AF80:BF00:159::159
202.222.12.194
2401:AF80:B000:2017::2
iBGP
OSPF
(非 BGP
経路のみ)
VLAN 2018
ethpolice
202.222.12.209
2401:AF80:B000:2018::1
/29
/64
202.222.12.214
2401:AF80:B000:2018::FFFE
ポリシーベース
ルータ FW 兼 ロガー
ngn-police1
v4 & v6
Loopback:
202.222.12.10
2401:AF80:BF00:161::161
policy route from 100.64.0.0/14
static route to 100.64.0.0/14
100.127.1.1
/24
100.127.1.254
VLAN 2019
ethnatin
OSPF
(非 BGP
経路のみ)
202.222.12.52
2401:AF80:B000:2913::6
VLAN 2913
ethwan
/28
/64
大規模 NAT (JP)
ngn-nat1
v4 only
大規模 NAT (US)
ngn-nat2
v4 only
202.222.12.138
24.235.8.4
ngn-sql
202.222.12.76
103.41.61.53
ngn-radius
VLAN 2914
ethwan2
VLAN 3069
ethwan1
cat5 (SE)
v4 & v6
202.222.12.82
2401:AF80:B000:2914::12
202.222.12.83
2401:AF80:B000:2914::13
ngn-dns1,
ngn-dns2
100.127.1.101
100.127.1.102
202.222.12.54
2401:AF80:B000:2913::1
igp1 (OPEN)
v4 & v6
202.222.12.142
VLAN 2905
ethnatout
/29
24.235.8.253
VLAN 3007
ethnatout
/24
OSPF Def
GW
インターネット
インターネット

基本、全部 1 台の Linux (Ubuntu 18.04 + LXD) にまとめて仮想化 (軽量 VM)

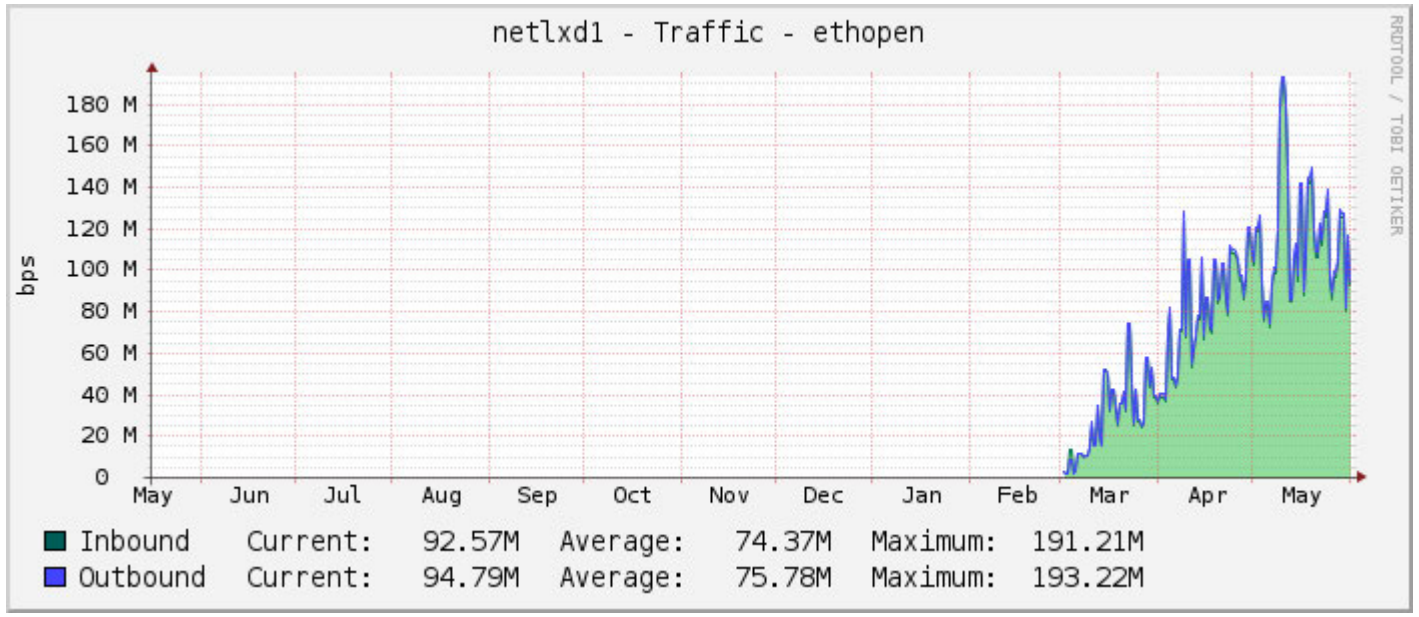
```
[root@netlxd1 ~]# lxc list
+-----------------+---------+-----------------------------+-----------------------------------------+-----------+-----------+
|      NAME       |  STATE  |          IPV4               |                  IPV6                   |   TYPE    | SNAPSHOTS |
+-----------------+---------+-----------------------------+-----------------------------------------+-----------+-----------+
| ngn-bgp-master1 | RUNNING | 202.222.12.209 (ethpolice)  | 2401:af80:b000:2018::1 (ethpolice)      | PERSISTENT | 0         |
|                 |         | 202.222.12.206 (ethbb)      | 2401:af80:b000:2017::fffe (ethbb)       |           |           |
|                 |         | 10.229.200.163 (ethmgmt)    |                                         |           |           |
+-----------------+---------+-----------------------------+-----------------------------------------+-----------+-----------+
| ngn-bgp1        | RUNNING | 202.222.12.193 (ethbb)      | 2401:af80:b000:2017::1 (ethbb)          | PERSISTENT | 0         |
|                 |         | 103.41.61.34 (ethpoi)       | 2401:af80:8003::ff (ethpoi)             |           |           |
|                 |         | 10.229.200.161 (ethmgmt)    |                                         |           |           |
+-----------------+---------+-----------------------------+-----------------------------------------+-----------+-----------+
| ngn-bgp2        | RUNNING | 202.222.12.194 (ethbb)      | 2401:af80:b000:2906::ff (ethpoi)        | PERSISTENT | 0         |
|                 |         | 202.222.12.150 (ethpoi)     | 2401:af80:b000:2017::2 (ethbb)          |           |           |
|                 |         | 10.229.200.162 (ethmgmt)    |                                         |           |           |
+-----------------+---------+-----------------------------+-----------------------------------------+-----------+-----------+
| ngn-dns1        | RUNNING | 202.222.12.82 (ethwan2)     | 2401:af80:b000:2914::12 (ethwan2)       | PERSISTENT | 0         |
|                 |         | 100.127.1.101 (ethnatin)    |                                         |           |           |
|                 |         | 10.229.200.169 (ethmgmt)    |                                         |           |           |
+-----------------+---------+-----------------------------+-----------------------------------------+-----------+-----------+
| ngn-dns2        | RUNNING | 202.222.12.83 (ethwan2)     | 2401:af80:b000:2914::13 (ethwan2)       | PERSISTENT | 0         |
|                 |         | 100.127.1.102 (ethnatin)    |                                         |           |           |
|                 |         | 10.229.200.170 (ethmgmt)    |                                         |           |           |
+-----------------+---------+-----------------------------+-----------------------------------------+-----------+-----------+
| ngn-nat1        | RUNNING | 202.222.12.138 (ethnatout)  |                                         | PERSISTENT | 0         |
|                 |         | 100.127.1.254 (ethnatin)    |                                         |           |           |
|                 |         | 10.229.200.165 (ethmgmt)    |                                         |           |           |
+-----------------+---------+-----------------------------+-----------------------------------------+-----------+-----------+
| ngn-nat2        | RUNNING | 24.235.8.4 (ethnatout)      |                                         | PERSISTENT | 0         |
|                 |         | 100.127.1.253 (ethnatin)    |                                         |           |           |
|                 |         | 10.229.200.172 (ethmgmt)    |                                         |           |           |
+-----------------+---------+-----------------------------+-----------------------------------------+-----------+-----------+
| ngn-police1     | RUNNING | 202.222.12.52 (ethwan)      | 2401:af80:b000:2913::6 (ethwan)         | PERSISTENT | 0         |
|                 |         | 202.222.12.214 (ethpolice)  | 2401:af80:b000:2018::fffe (ethpolice)   |           |           |
|                 |         | 100.127.1.1 (ethnatin)      |                                         |           |           |
|                 |         | 10.229.200.164 (ethmgmt)    |                                         |           |           |
+-----------------+---------+-----------------------------+-----------------------------------------+-----------+-----------+
| ngn-radius      | RUNNING | 202.222.12.76 (ethwan2)     |                                         | PERSISTENT | 0         |
|                 |         | 103.41.61.53 (ethwan1)      |                                         |           |           |
|                 |         | 10.229.200.166 (ethmgmt)    |                                         |           |           |
+-----------------+---------+-----------------------------+-----------------------------------------+-----------+-----------+
| ngn-sql         | RUNNING | 10.229.200.167 (ethmgmt)    |                                         | PERSISTENT | 0         |
+-----------------+---------+-----------------------------+-----------------------------------------+-----------+-----------+
[root@netlxd1 ~]#
```

＋ eBay で数万円で購入した Cisco Nexus 3064 (QoS 用)

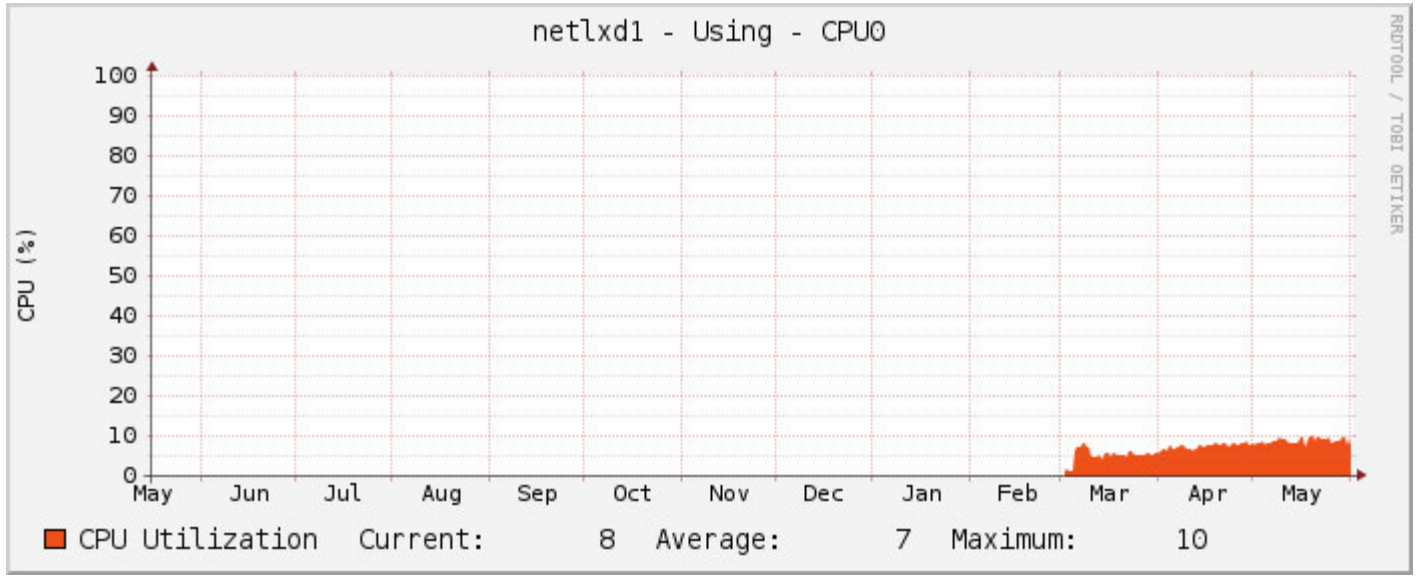
- 2009 年発売の HP ProLiant G6
- Xeon X5570 2.93GHz 8 コア
- RAM 72GB

(※ 2万円で中古で買った)
＋

- Intel 10G NIC X520-DA2 1 枚



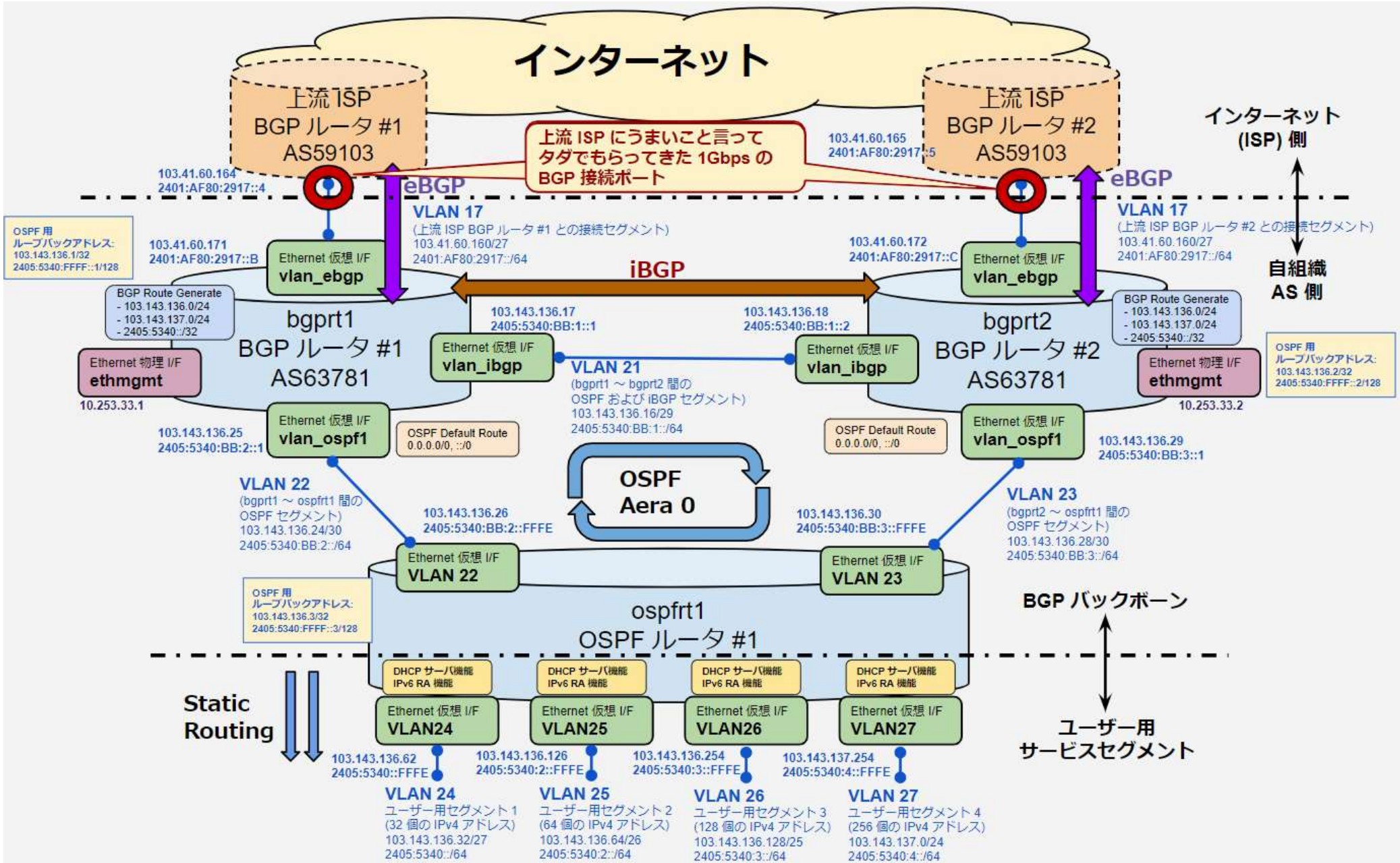
PPPoE セッション数 (東京都)



PPPoE セッション数 (茨城県)

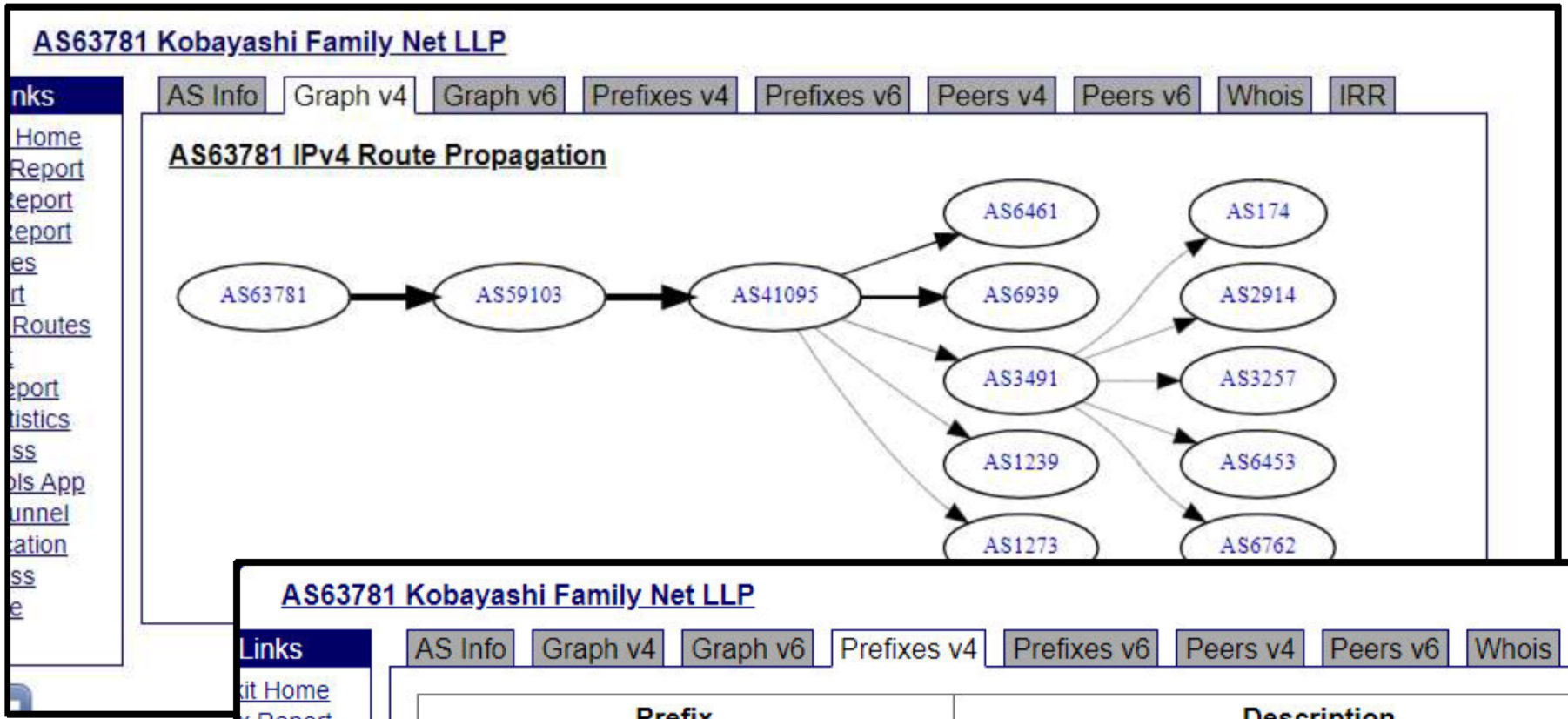
IPA Easy BGP Starter Kit 2020.3.28 ～

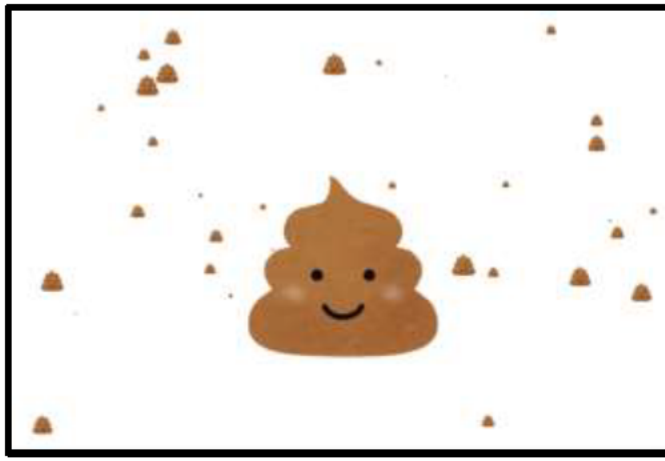
- **https://github.com/IPA-CyberLab/IPA-DN-EasyBgpStarterKit**
- 誰でも BGP フルルート (IPv4/IPv6 Dual Stack) が運用できる Raspberry Pi 4 BGP ルータ化 Ansible スクリプト集



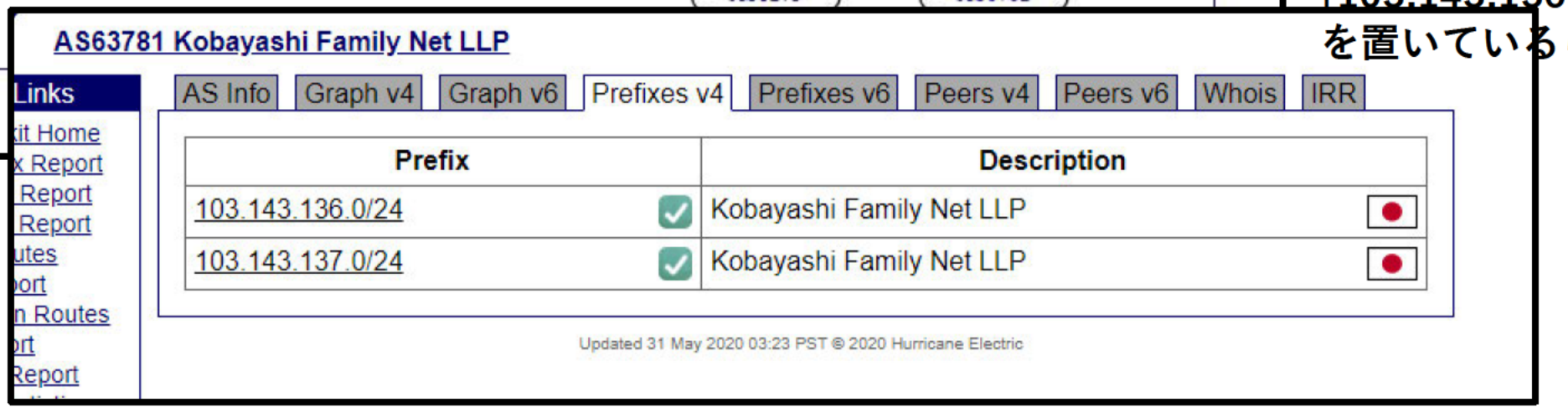
- **https://github.com/IPA-CyberLab/IPA-DN-EasyBgpStarterKit**

実際に運用しているヤツ

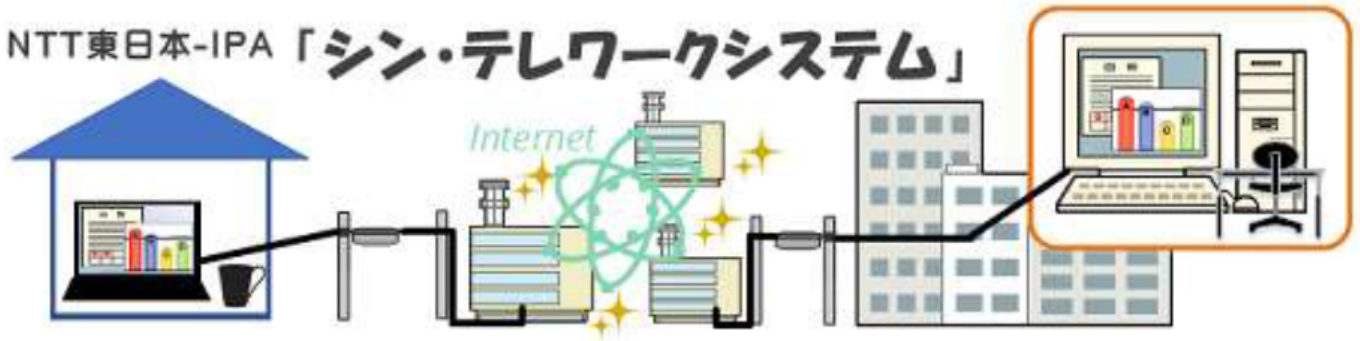




https://www.unko.co.jp /
[103.143.136.37]
を置いているらしい



- https://github.com/IPA-CyberLab/IPA-DN-EasyBgpStarterKit

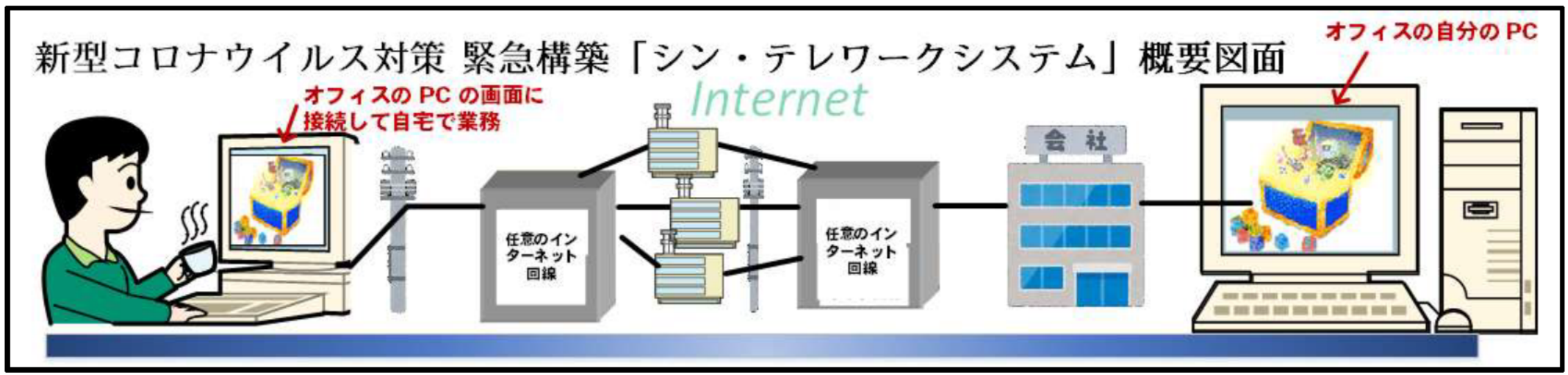


NTT東日本

IPA 独立行政法人 情報処理推進機構

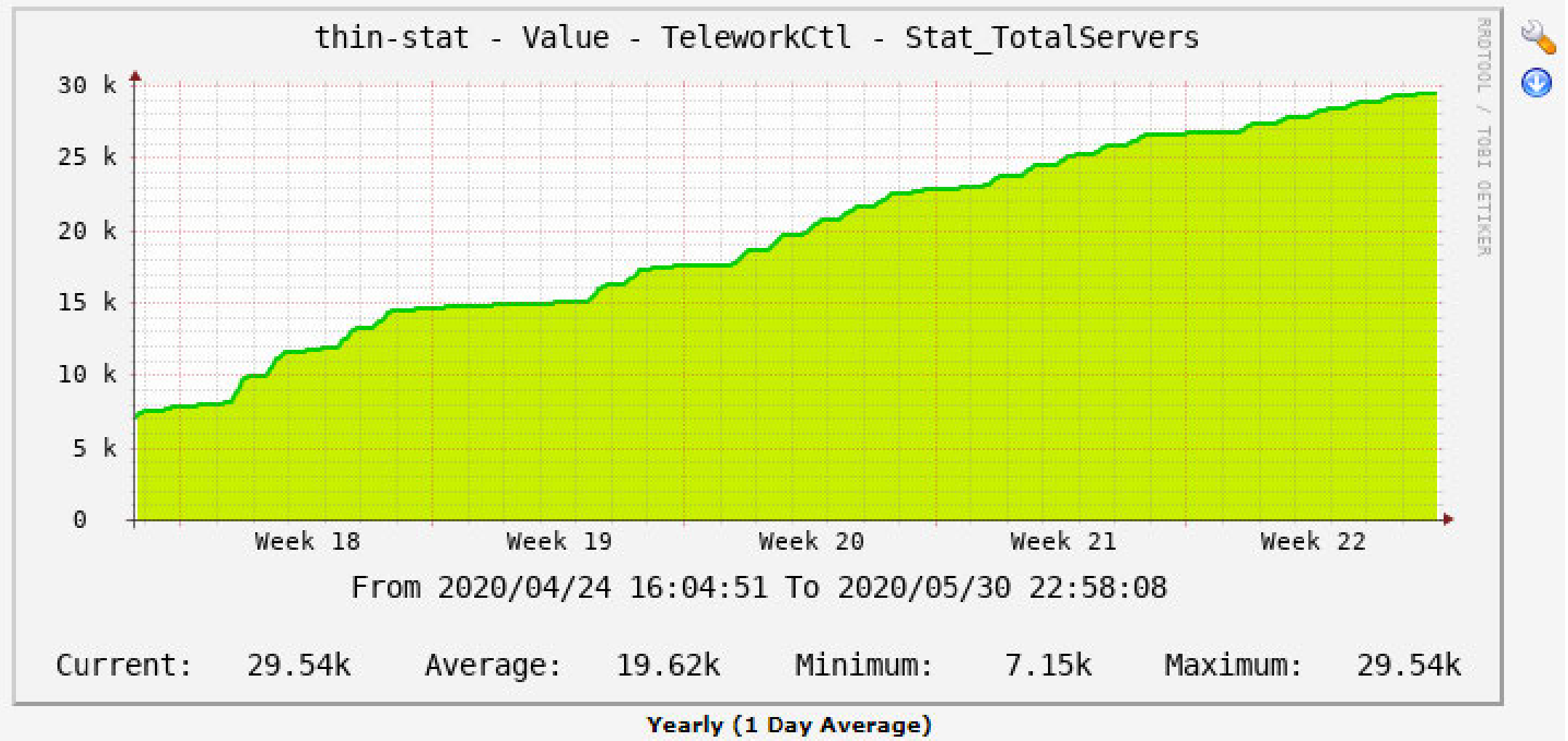
新型コロナウイルス対策 緊急構築 実証実験

NTT 東日本 - IPA「シン・テレワークシステム」　緊急構築・無償開放



https://telework.cyber.ipa.go.jp/

2020/4/21 無償開放
2020/5/31 時点で約 3 万ユーザー



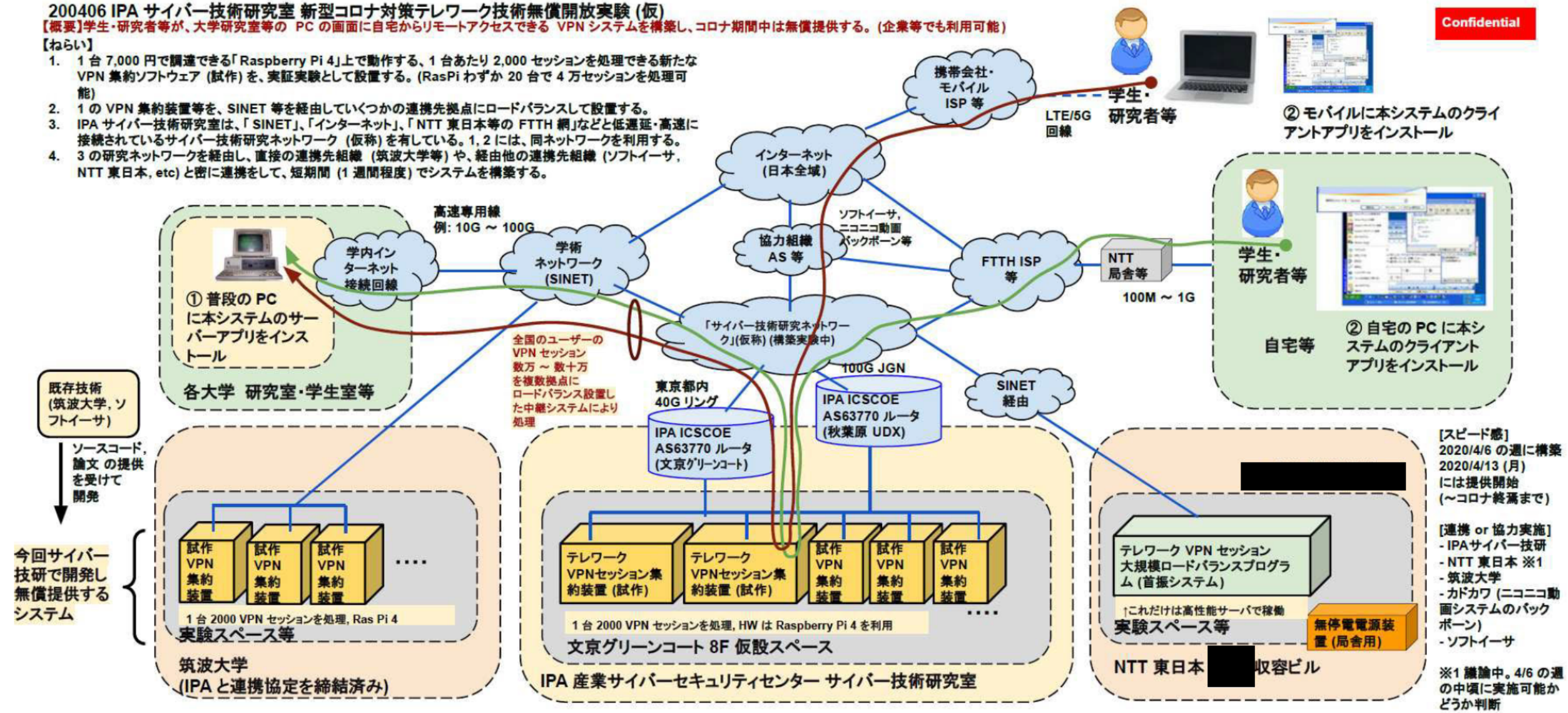
200406 IPA サイバー技術研究室 新型コロナ対策テレワーク技術無償開放実験 (仮)

【概要】学生・研究者等が、大学研究室等の PC の画面に自宅からリモートアクセスできる VPN システムを構築し、コロナ期間中は無償提供する。(企業等でも利用可能)

【ねらい】

1. 1 台 7,000 円で調達できる「Raspberry Pi 4」上で動作する、1 台あたり 2,000 セッションを処理できる新たな VPN 集約ソフトウェア (試作) を、実証実験として設置する。(RasPi わずか 20 台で 4 万セッションを処理可能)
2. 1 の VPN 集約装置等を、SINET 等を経由していくつかの連携先拠点にロードバランスして設置する。
3. IPA サイバー技術研究室は、「SINET」、「インターネット」、「NTT 東日本等の FTTH 網」などと低遅延・高速に接続されているサイバー技術研究ネットワーク (仮称) を有している。1, 2 には、同ネットワークを利用する。
4. 3 の研究ネットワークを経由し、直接の連携先組織 (筑波大学等) や、経由他の連携先組織 (ソフトイーサ, NTT 東日本, etc) と密に連携をして、短期間 (1 週間程度) でシステムを構築する。

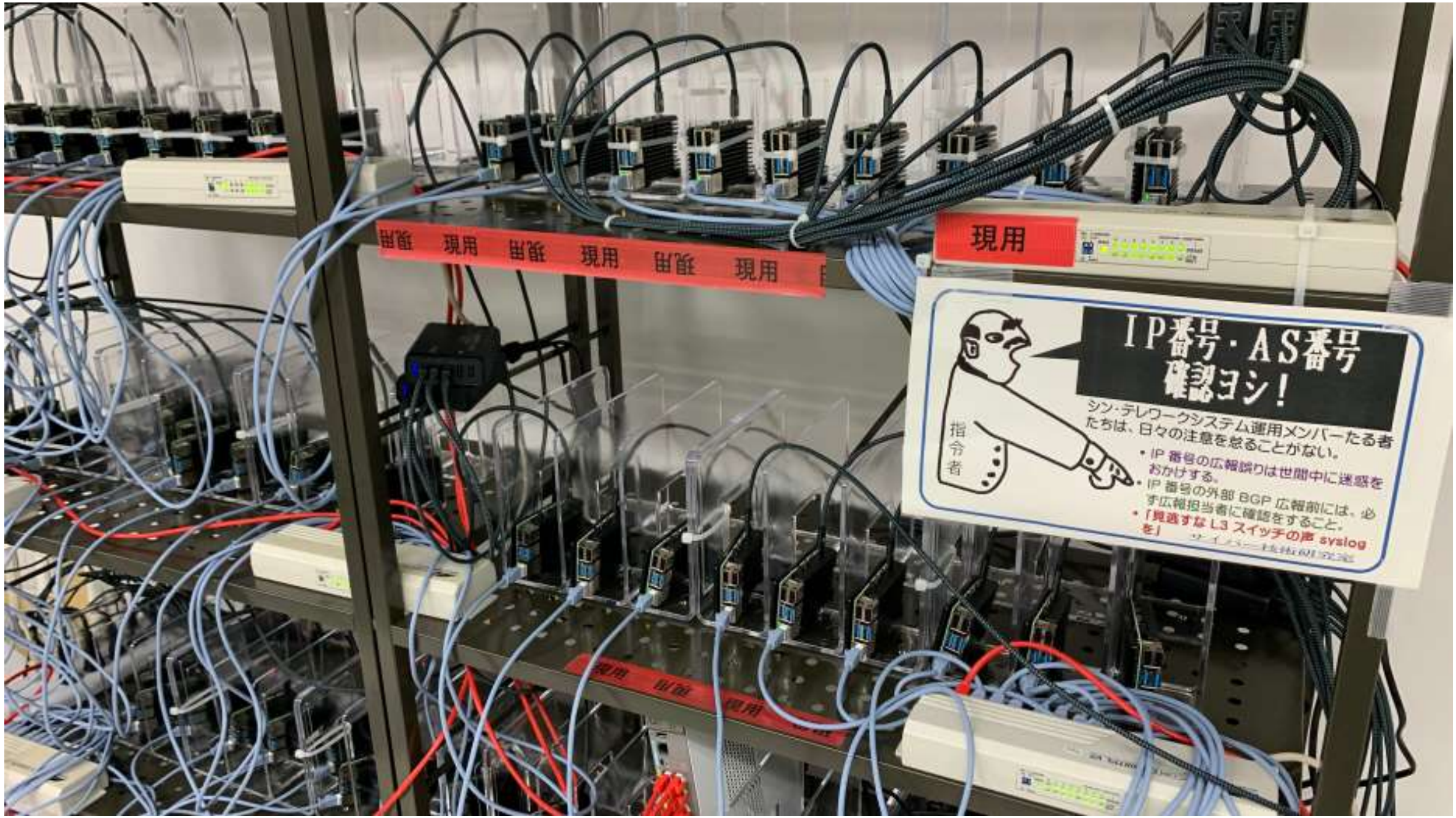
Confidential

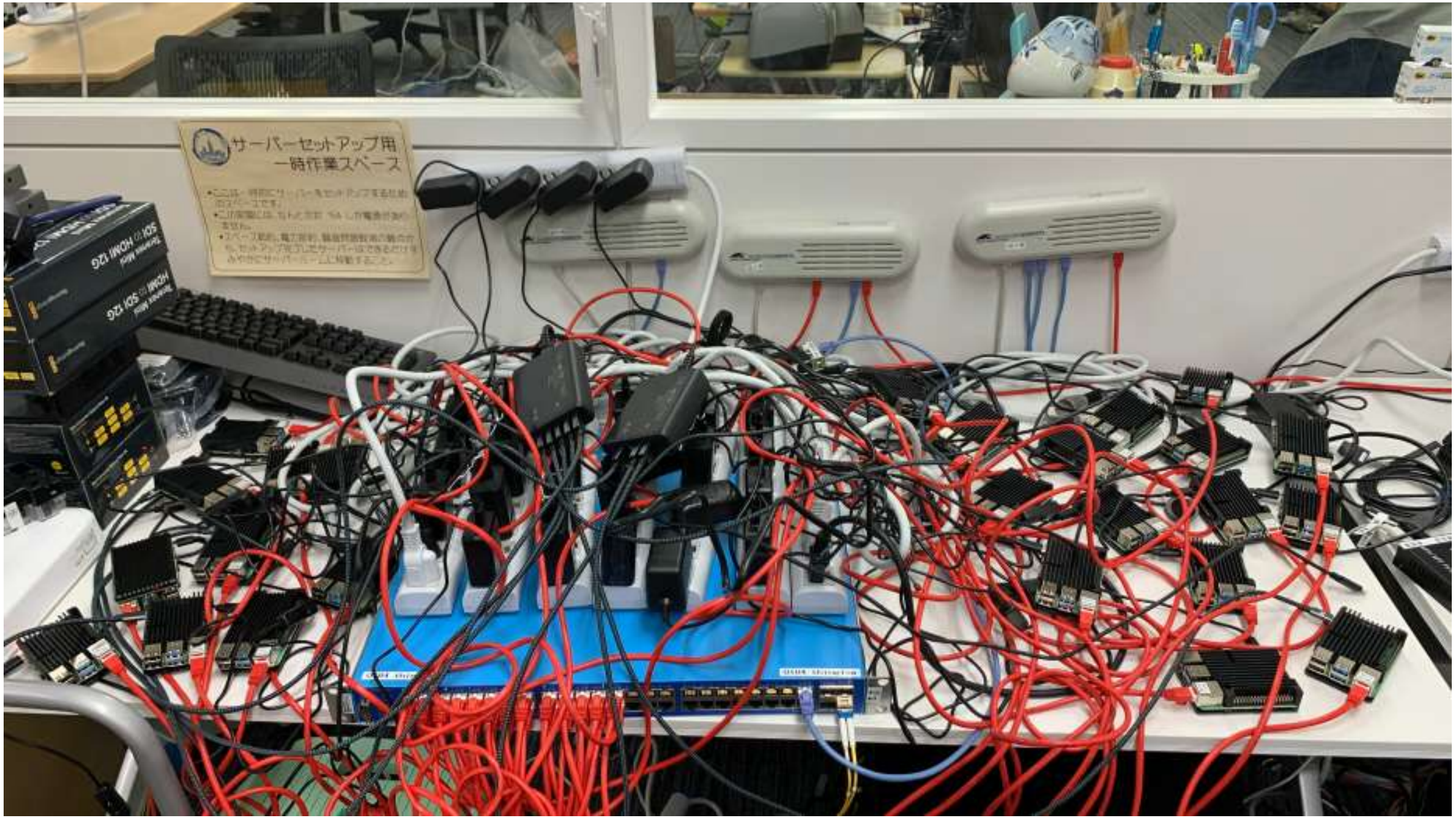


[スピード感]
2020/4/6 の週に構築
2020/4/13 (月) には提供開始
(～コロナ終焉まで)

[連携 or 協力実施]
- IPAサイバー技研
- NTT 東日本 ※1
- 筑波大学
- カドカワ (ニコニコ動画システムのバックボーン)
- ソフトイーサ

※1 議論中。4/6 の週の中頃に実施可能かどうか判断


現用
現用
現用
現用
現用
現用
IP番号・AS番号
確認ヨシ！
指令者
シン・テレワークシステム運用メンバーたる者たちは、日々の注意を怠ることがない。
• IP 番号の広報誤りは世間中に迷惑をおかけする。
• IP 番号の外部 BGP 広報前には、必ず広報担当者に確認をすること。
• 「見逃すな L3 スイッチの声 syslog を」


サーバーセットアップ用
一時作業スペース

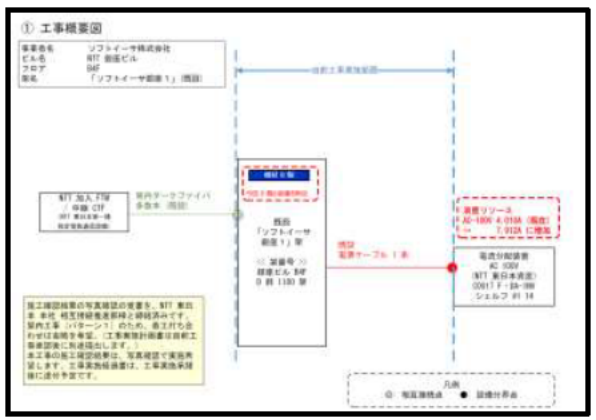

Thin Telework System
超重要ロードバランサ
重要！ 電源 抜かないこと
UPS に常時接続
みだりに再起動しないこと (WAN の NIC が調子悪く、
再起動後 30%くらいの確立でリンクアップしない)

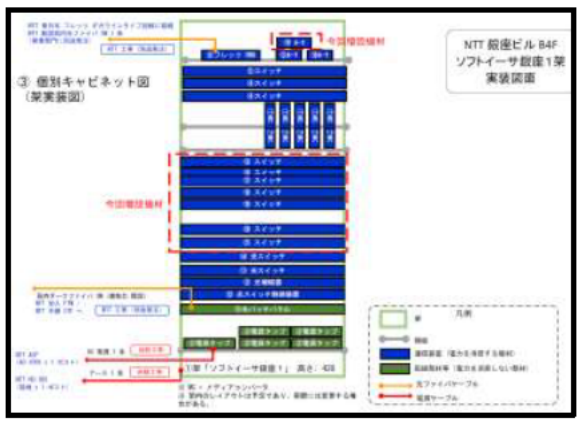

RPS
Fan Err
V2
40Gbps
NTT銀座
NTT渋谷
現用

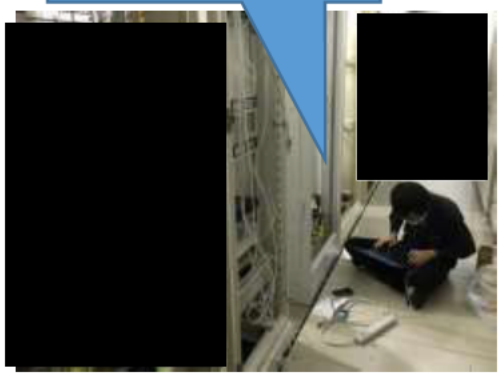
秘密の ネットワーク図

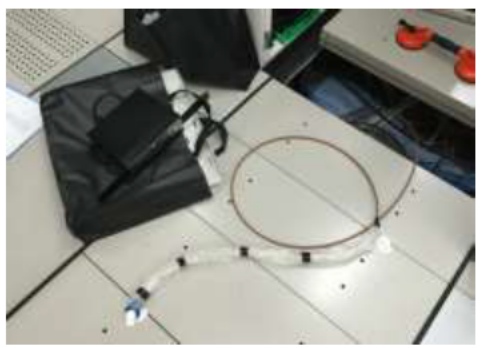
[redacted]

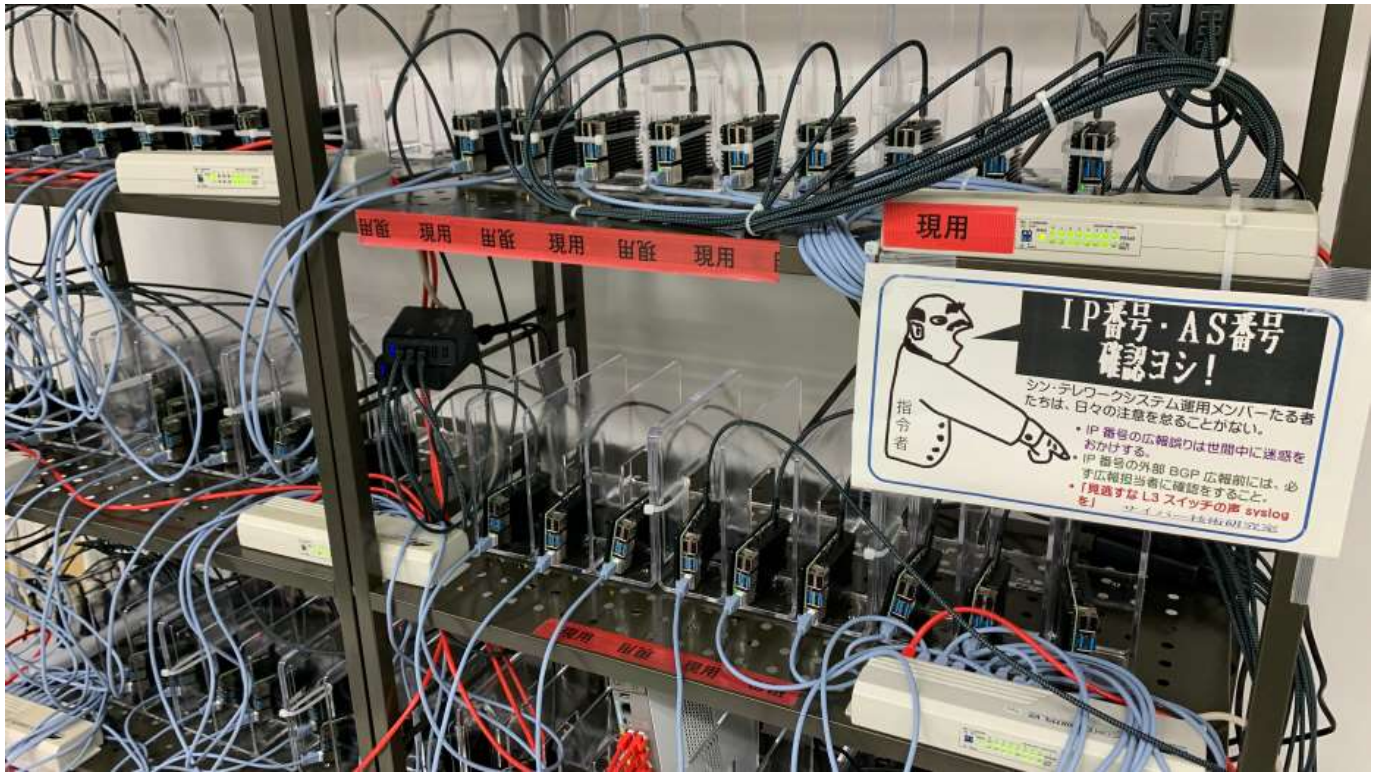
自前工事
ヨシ！

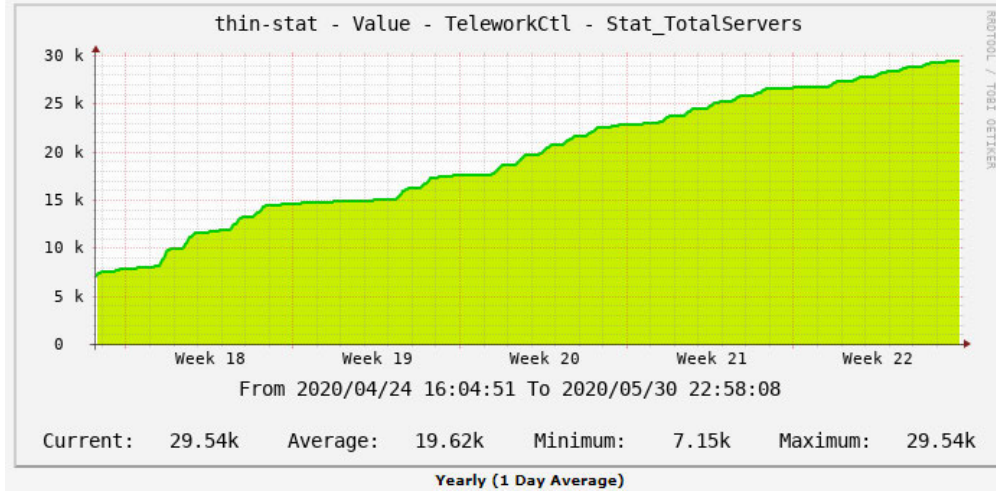












- 税金で購入した物品:
  Raspberry Pi 4 + ケース + microSD + 電源 + LAN ケーブル
  50 台 (65 万円) のみ
- 1 台あたり余裕で 1,000 セッション、最大 2,000 セッション同時処理可能
- 1 ユーザーあたり月額コスト 5 円 ～ 15 円程度を実現
  (電気代・スペース代・回線費用も含め)
- 初期設定や保守が一切不要 (壊れたら放っておけばよい)
- 不足したら Amazon で買い足せばよい。スケーラブル