

「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

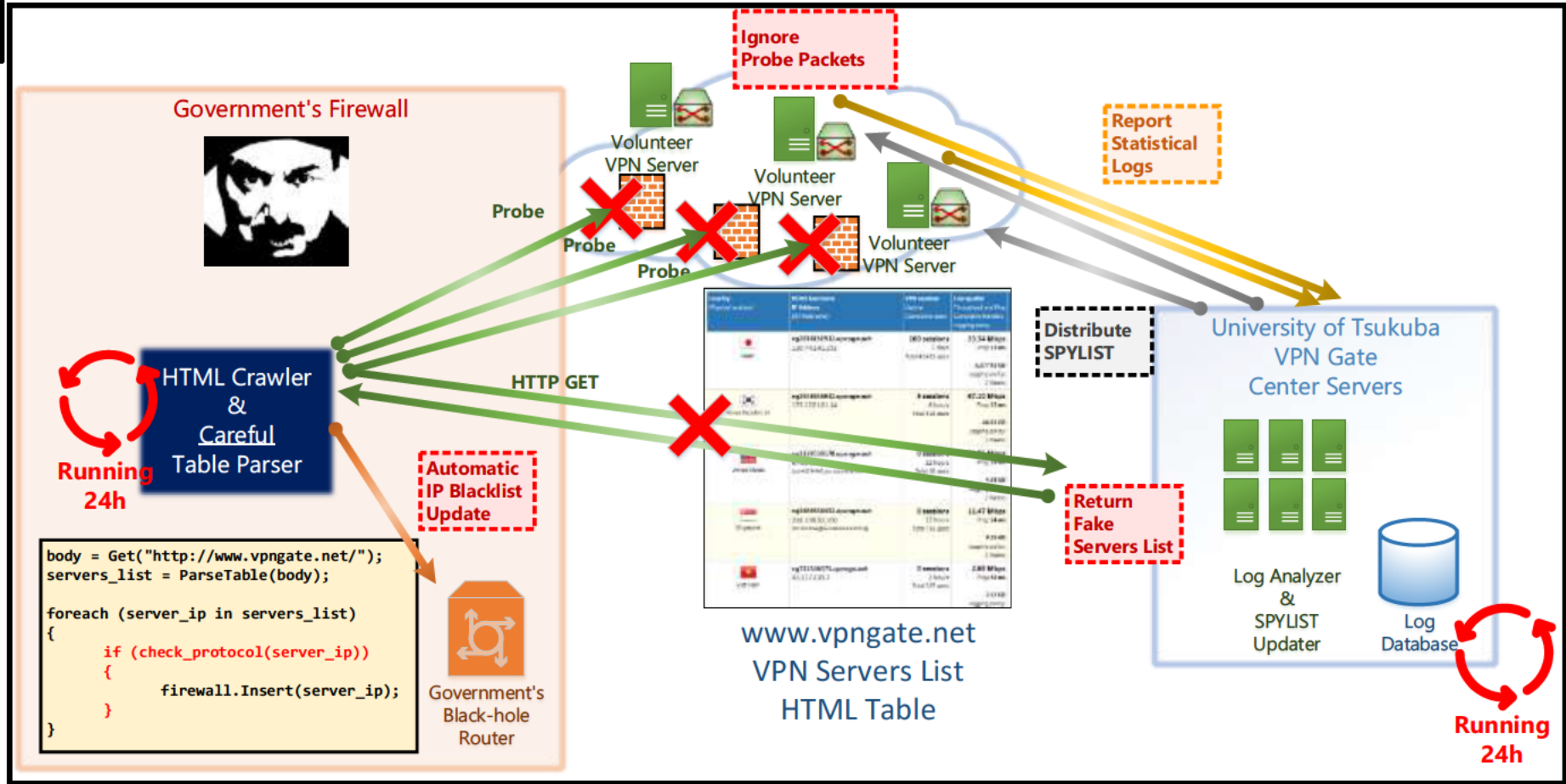
登 大遊

登大遊 自己紹介

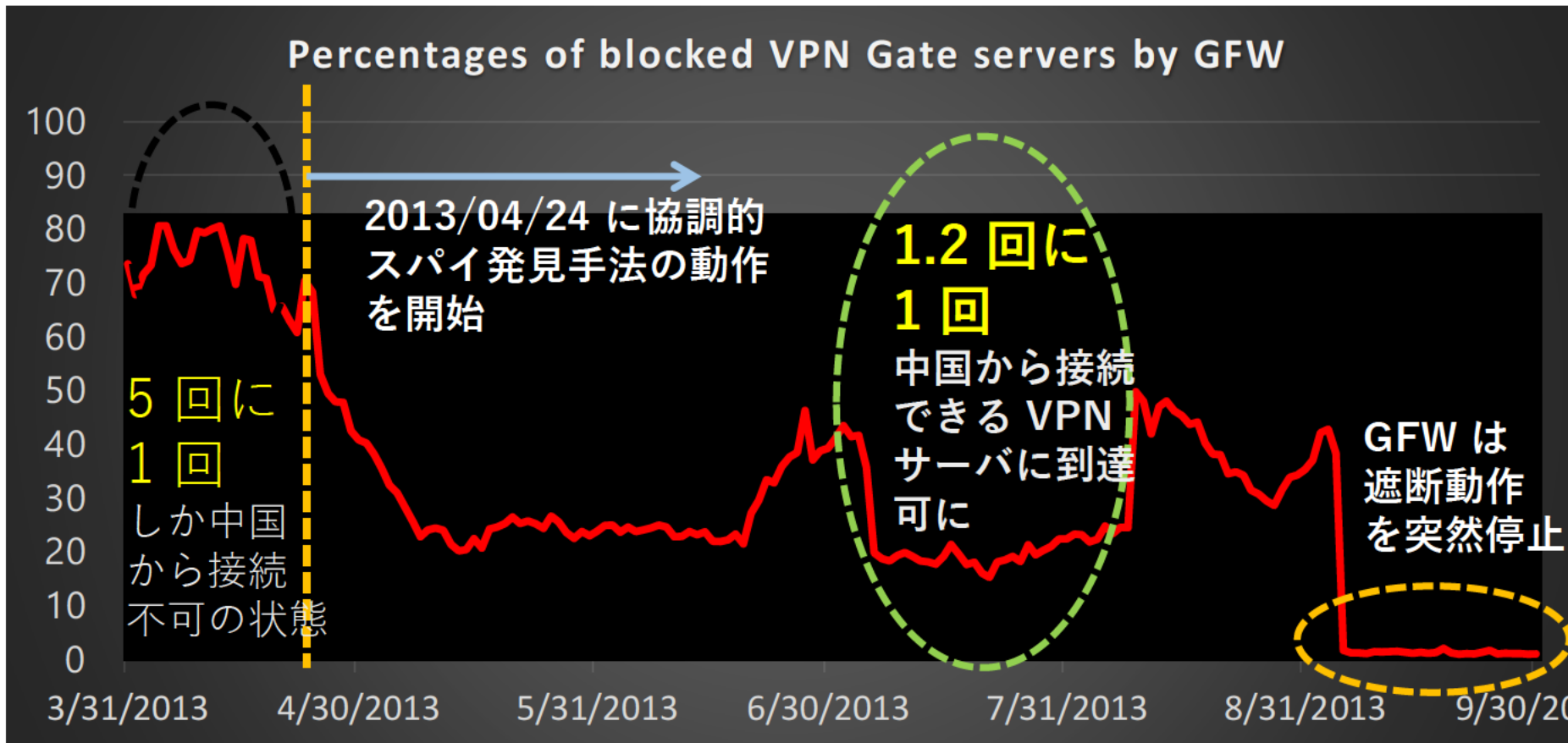


- サイバー空間の橋・トンネルを作り管理する
「SoftEther VPN」 仮想プライベートネットワーク
IPA 未踏ソフトウェア創造事業で開発 (2003.12)
全世界で 476 万の組織・個人で利用 (うち 日本 10%, 海外 90%)
「VPN Gate」 検閲回避システム
政府の検閲用ファイアウォールを回避する分散中継システム
- サイバー活動
 1. ソフトイーサ株式会社 代表取締役 (2004.4 -)
 2. 筑波大学 産学連携准教授 (2017.4 -)
 3. 独立行政法人 情報処理推進機構 (IPA)
「産業サイバーセキュリティセンター」 (2017 -) サイバー技術研究室長 (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

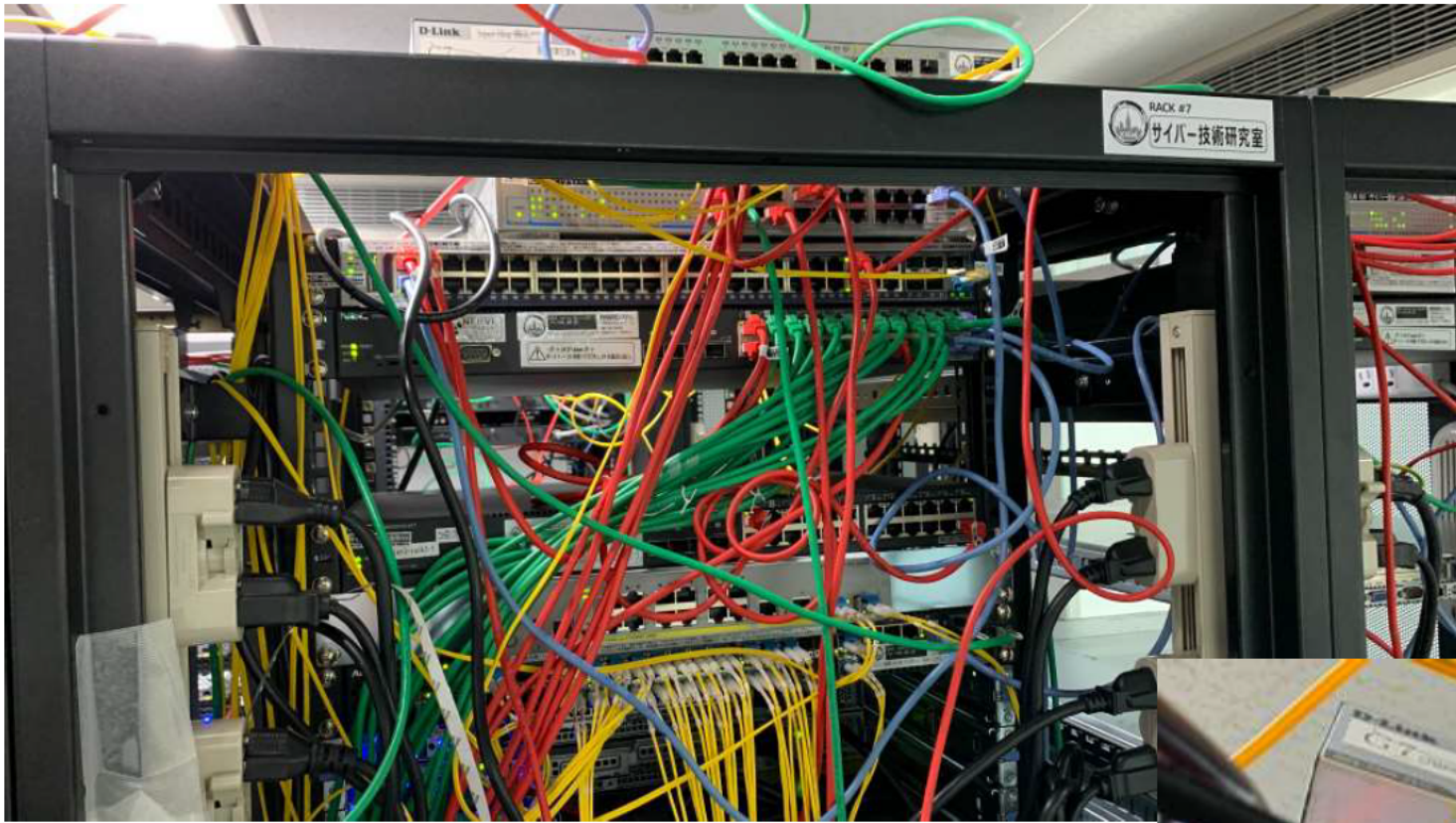
Department of Computer Science, University of Dushu, Japan

Abstract
VPN Gate is a public VPN relay service designed to achieve blocking resistance to censorship firewalls such as the Great Firewall (GFW) of China. To achieve such resistance, an operator needs to provide a VPN relay server, with many changing IP addresses. To block VPN Gate with their firewalls, censoring authorities must find the IP addresses of all the volunteers. To prevent this, we adopted two techniques to improve blocking resistance. The first technique is to make a number of volunteer IP addresses into the relay server for provided to the public. The second technique is volunteer-organizational cooperation. The volunteer servers work together to create a list of open, changing the addresses used for connecting volunteer to public the volunteer server. Using this list, each volunteer server updates its own IP address. We launched VPN Gate on March 6, 2013. By the end of August, it had about 1,000 daily volunteers using 4,000 unique IP addresses to facilitate 400,000 VPN connections. Even now, worldwide including 41,000 connections and 4,000 unique IP addresses from China. In the first VPN Gate launched about 70% of volunteer VPN servers is shut down by the GFW.

1. Introduction
Some countries in the world have censorship firewalls operated by their governments to prohibit access to users in foreign countries. For instance, the Great Firewall (GFW) of China blocks access to Twitter, Facebook, and YouTube. Internet users in countries subject to censorship often use commercial public relay servers to bypass censorship firewalls. Public proxies, VPN services, and Tor relays [1] are popular examples of such relay services. Usually, the IP addresses of relay servers are periodically available to user organizations. A censorship authority can easily block these relay servers by adding the IP addresses to its blocking blocking list. Moreover, the Chinese authority can prohibit some relay services via user-identification-based mechanisms [17]. To relay connectivity to blocked destinations [11], against such changing censorship, we have built a public VPN relay service system with blocking resistance to censorship firewalls such as the GFW. We call this system VPN Gate. To achieve blocking resistance, VPN Gate uses frequently changing IP addresses that are provided by volunteers. The current list server, called the VPN Gate List server, manages a list of IP addresses of all active VPN servers. We call this list the Server List. A user can periodically ping the Server List and connect to the IP in an active VPN server on the list. The more users connect to an active VPN server through the Server List, the more the GFW blocks all the active VPN servers in VPN Gate. It is a hard for a censorship authority to achieve blocking resistance. We adopted two techniques for blocking resistance: volunteer IP sharing and collaborative IP detection. In volunteer IP sharing, we include a number of IP addresses, which are provided to VPN Gate, in the Server List. For instance, we include widely popular services (e.g., Windows Update servers). This technique forces a censorship authority to manage a large number of IP addresses from the Server List before adding addresses to the blocking blocking list. The second technique, collaborative IP detection, uses peer-to-peer connections from censorship authority's computers, called peers. In this technique, all the volunteer VPN servers work together to create a unique IP address list of open, called the Open List, and then update peer-to-peer connections. This technique enables the volatility available to censorship authority by the IP addresses of active VPN servers and inactive IP addresses of those of inactive VPN servers. The VPN Gate system consists of instances of the VPN Gate server software, an optional application, the VPN Gate Client software, and a central List Server. The server can install itself and receive VPN Gate Service For instance, volunteers have to modify their network Address Translation (NAT) boxes to open TCP/UDP ports. Users can connect to VPN Gate Server with the VPN Gate Client (VCL) + VPN gateway by using VPN Gate Client. Users can also connect to a VPN server with the L2TP/IPsec, OpenVPN, and SSTP protocols by using the firewall. We provided VPN clients on PCs and smartphones. As for the development of the system, we search group near the VPN Gate List Server which accept organizations from volunteer servers, guarantee the Server List, and distribute it to users.

最近やっている頭おかしいこと





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>



The screenshot shows a news article on the SoftEther website. The article title is "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" (Free release of SoftEther's Flets PPPoE experimental access points for telework due to COVID-19 countermeasures). The date is 2020年3月6日 (Sat). The article text explains that SoftEther Corp. is providing experimental PPPoE access points for Flets users to support telework during the COVID-19 pandemic. It mentions that the service is available for users with Flets accounts and that the access points are provided for free. The article also includes a section for "ご利用の注意" (Usage Notes) and a "お問い合わせ" (Contact Us) section.

ソフトイーサ Web サイト > 報道発表資料 > 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

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 (土)

筑波大学産ベンチャー企業であるソフトイーサ株式会社（本社所在地：茨城県つくば市、以下「ソフトイーサ」といいます）は、新型コロナウイルス感染症の拡大を防止するべく在宅勤務を推奨している方々を対象として、これまで学術実験目的で試験提供してきた NTT 東日本フレッツ用 PPPoE 方式のインターネットアクセスポイント（東京・茨城）を、半日より新型コロナウイルス対策が必要な期間（以下「コロナ期間」といいます）、無償・無保証で提供いたします。テレワークで自宅のフレッツ回線をご利用の方で、テレワークの増加により普段お使いの ISP の PPPoE 通信が一時的に遅延等が原因で、實際上重要な通信が日中停滞し入らない場合は、本アクセスポイントを試してみてください。

本 PPPoE アクセスポイントは、インターネット通信が利用可能ですが、業務上重要な通信プロトコル（シンククライアント通信、テレビ会議、Webexセッションおよびメール送受信など）の速度（帯域・遅延）をできるだけ高速化し、それ以外の、遅延を許容した不急不急の通信（動画サイトの閲覧など）の優先順位を下げる特殊な処理を実験的に適用しています。これにより、コロナ期間中のテレワークに必要な重要な通信が比較的スムーズに行える可能性があります。

NTT 東日本の「フレッツ光」ユーザー（標準および特別優待サービス）の方は、共通アカウント（ID: open@open.ad.jp、パスワード: [open](#)）で、PPPoE 接続を行うことにより、本アクセスポイントを経由して、インターネットに無償・無保証でアクセスできます（図 1）。

留意事項
※1. 内部的に「コロナ」等の NTT 東日本のフレッツ光サービスを利用する各社のコロナ対応システム連携からも利用可能です。本 PPPoE アクセスポイントの利用には、事前のユーザー登録等は一切不要で、申込みも不要です。



The screenshot shows a PPPoE login window titled "PPPoE 入接続". It features a graphic of a laptop, a globe, and a desktop monitor. Below the graphic, there are input fields for "ユーザー名ID:" (Username ID) containing "open@open.ad.jp" and "パスワード:" (Password) containing "open". There are also checkboxes for "このユーザー情報を使用するときに、このユーザー名とパスワードを記憶する" (Remember this user name and password when using this user information) and "このユーザー名とパスワードを記憶する" (Remember this user name and password). At the bottom, there are buttons for "接続" (Connect), "キャンセル" (Cancel), "パスワードを再入力してください" (Please re-enter your password), and "ヘルプ" (Help).

PPPoE へ接続



ユーザー名(U):

パスワード(P):

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)

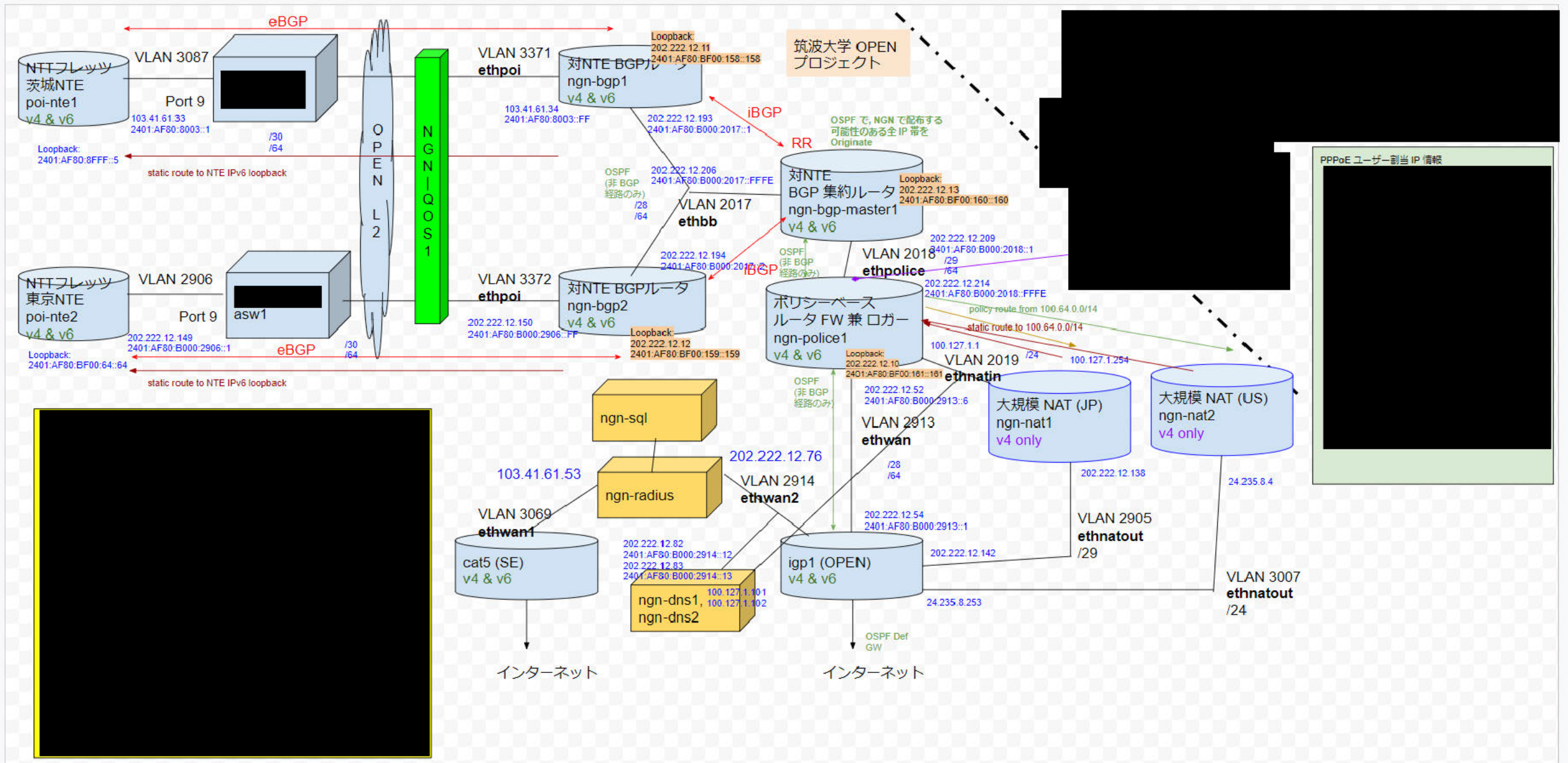
このコンピューターを使うすべてのユーザー(A)

接続(C)

キャンセル

プロパティ(O)

ヘルプ(H)



PPPoE ユーザー割当 IP 情報

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

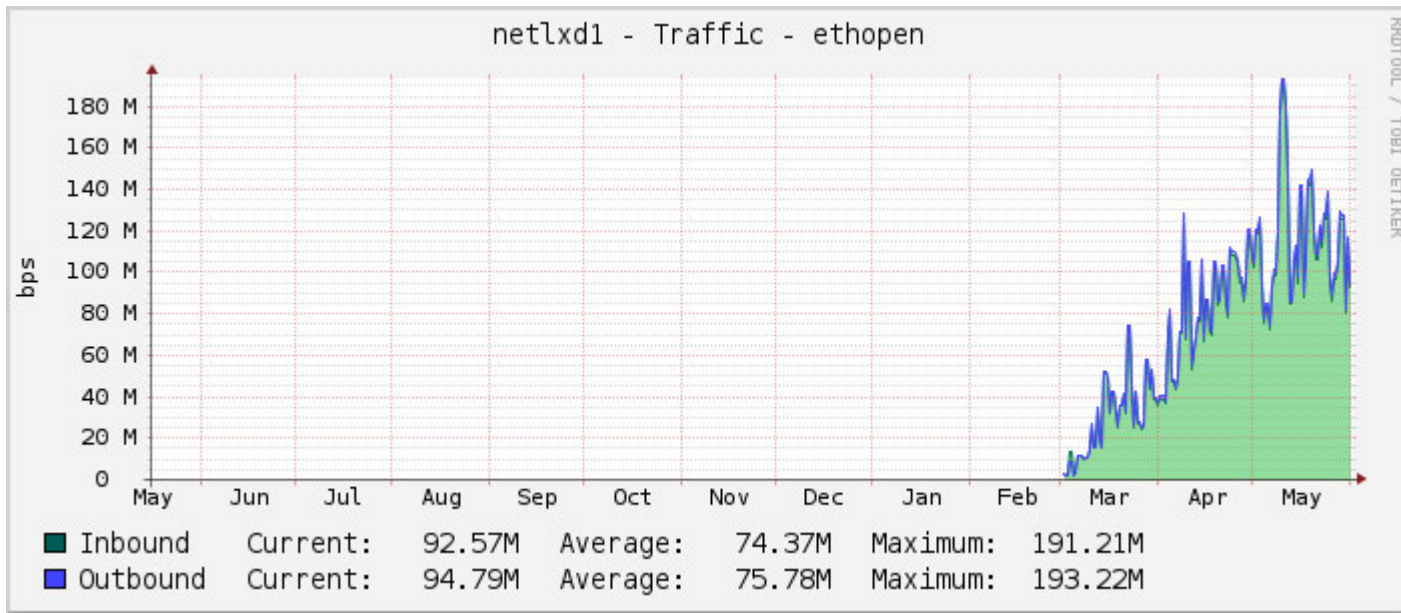
```
[root@netlxd1 ~]# lxc list
```

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

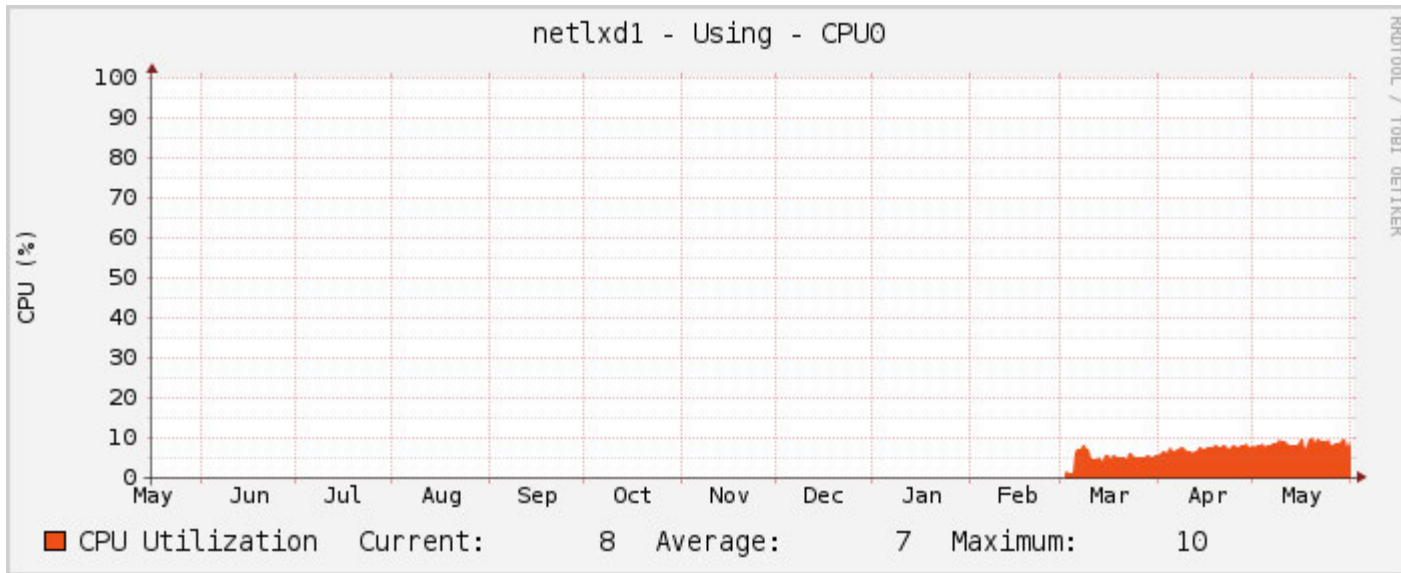
```
[root@netlxd1 ~]#
```

- 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

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



PPPoE セッション数 (東京都)



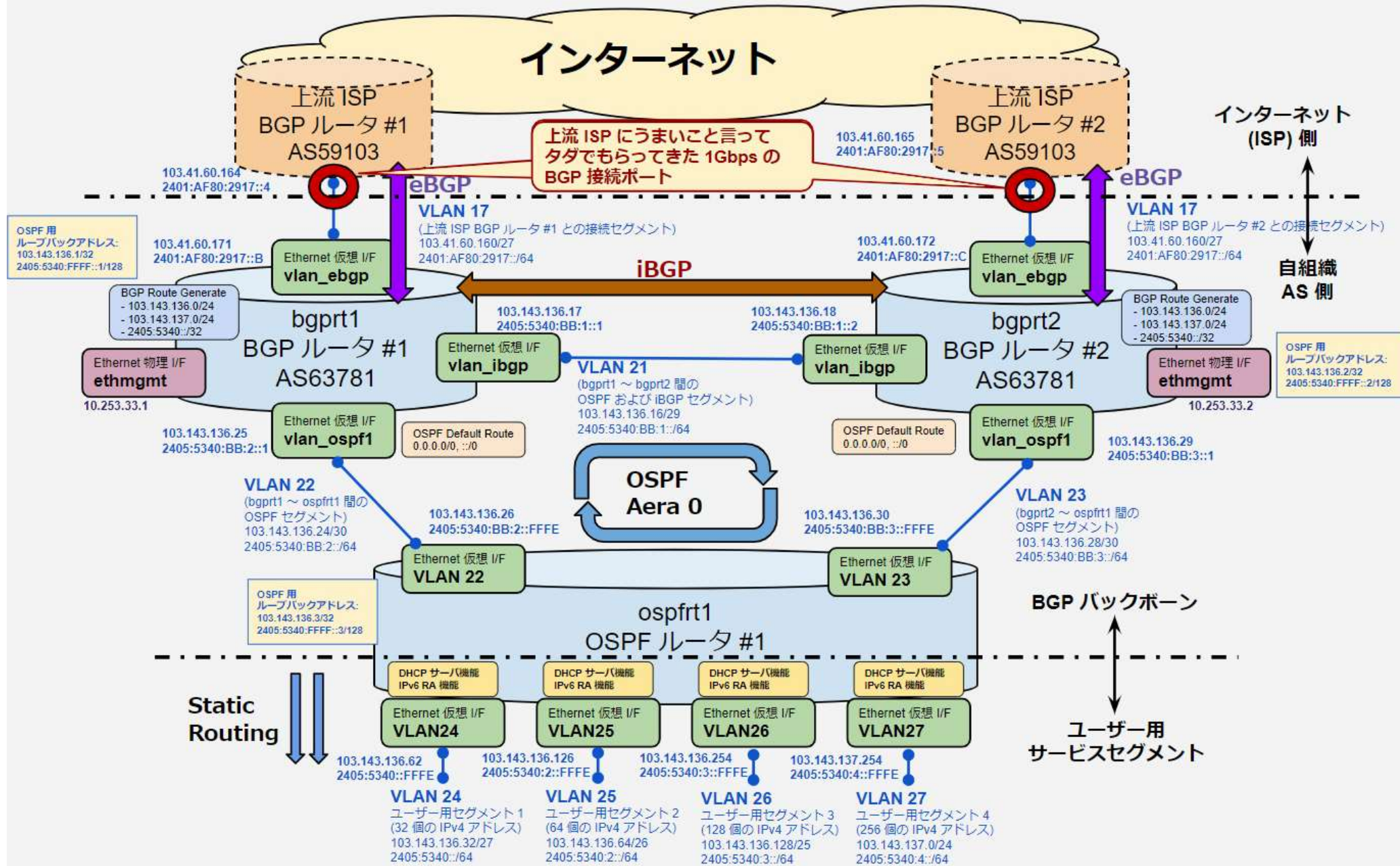
PPPoE セッション数 (茨城県)

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

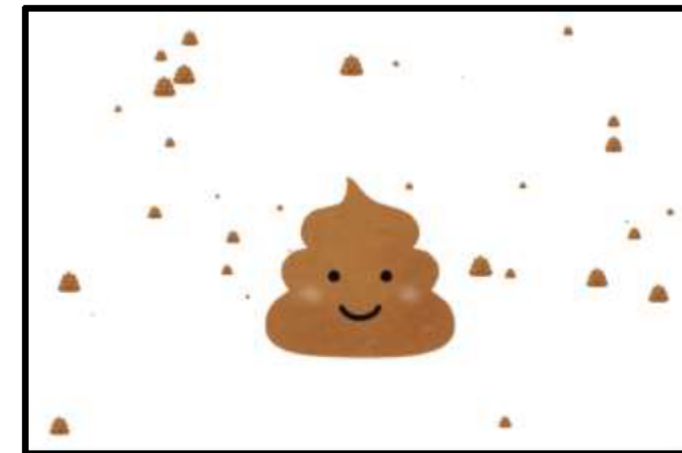
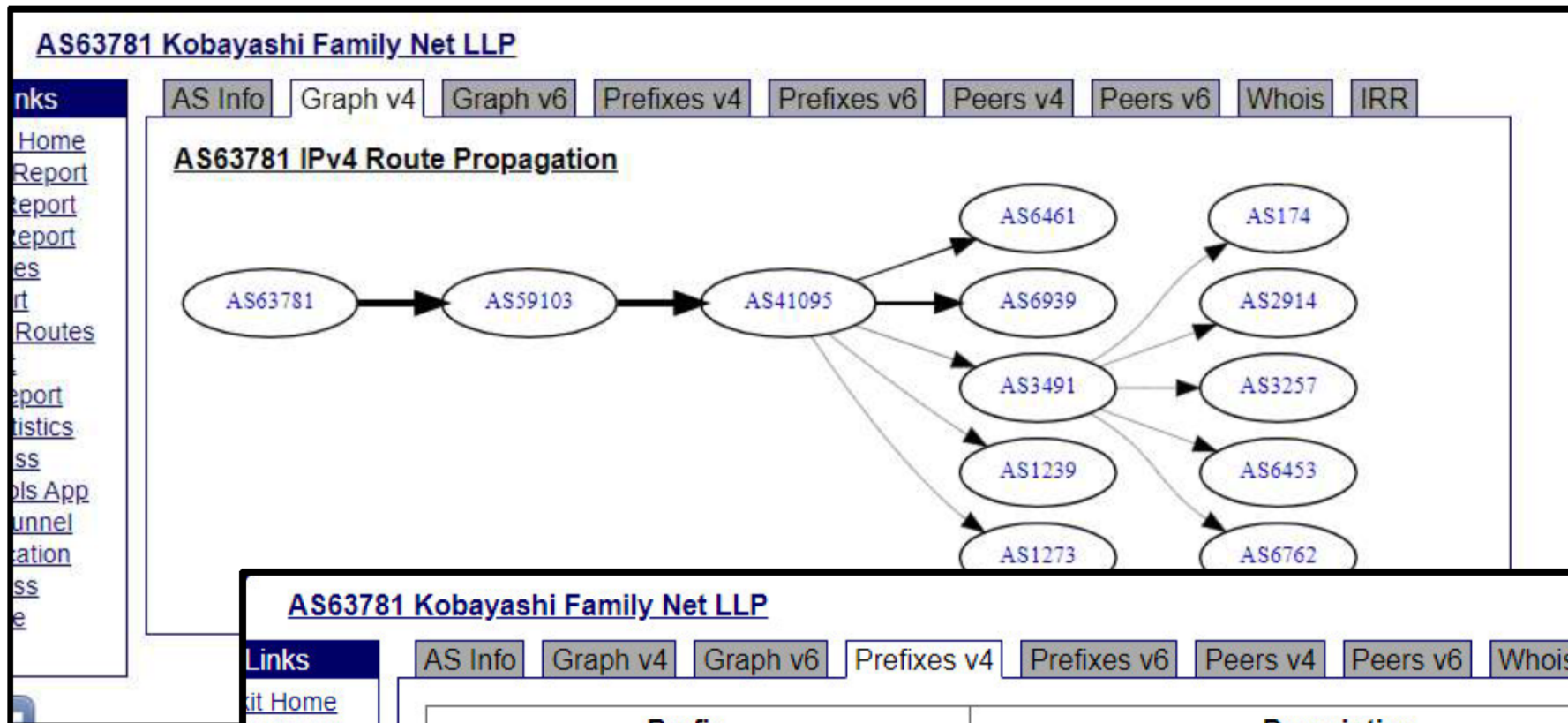


インターネット



- <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

AS63781 Kobayashi Family Net LLP

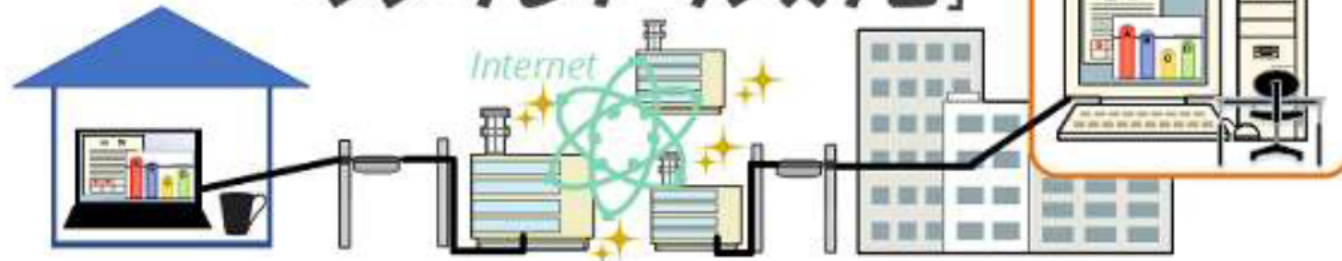
AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | IRR

Prefix	Description
103.143.136.0/24	✓ Kobayashi Family Net LLP <input type="checkbox"/>
103.143.137.0/24	✓ Kobayashi Family Net LLP <input type="checkbox"/>

Updated 31 May 2020 03:23 PST © 2020 Hurricane Electric

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

NTT東日本-IPA「シン・テレワークシステム」

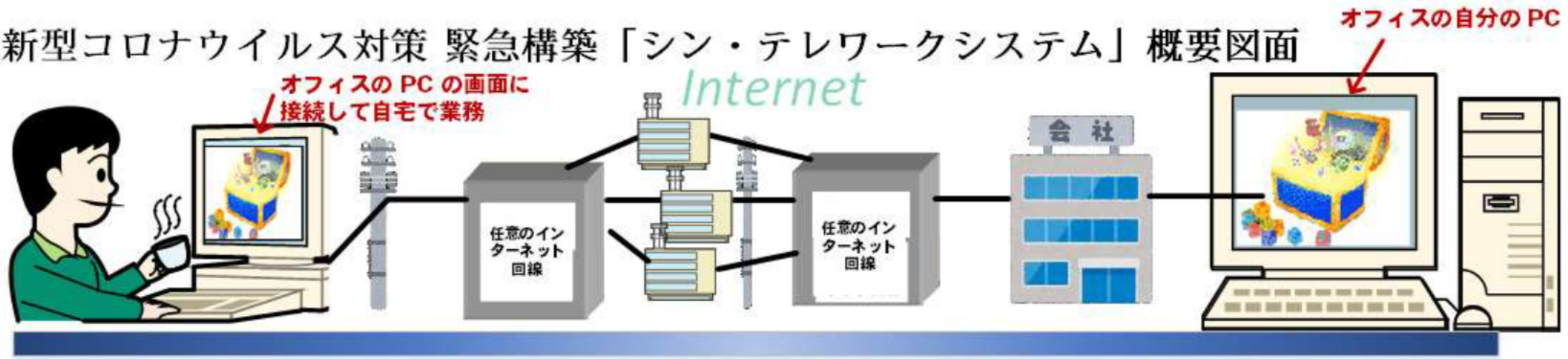


NTT東日本
IPA 独立行政法人
情報処理推進機構

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

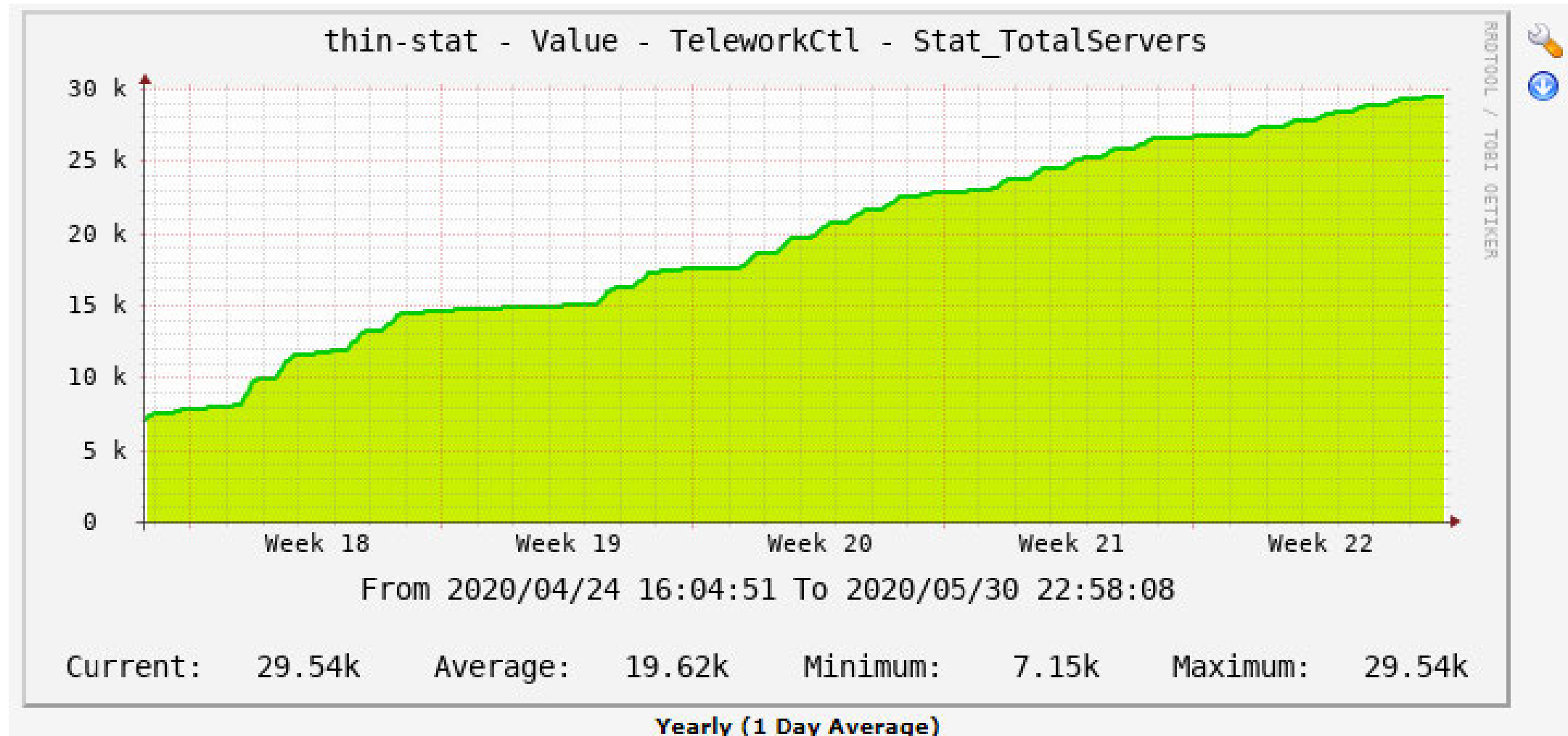
新型コロナウイルス対策 緊急構築「シン・テレワークシステム」概要図面

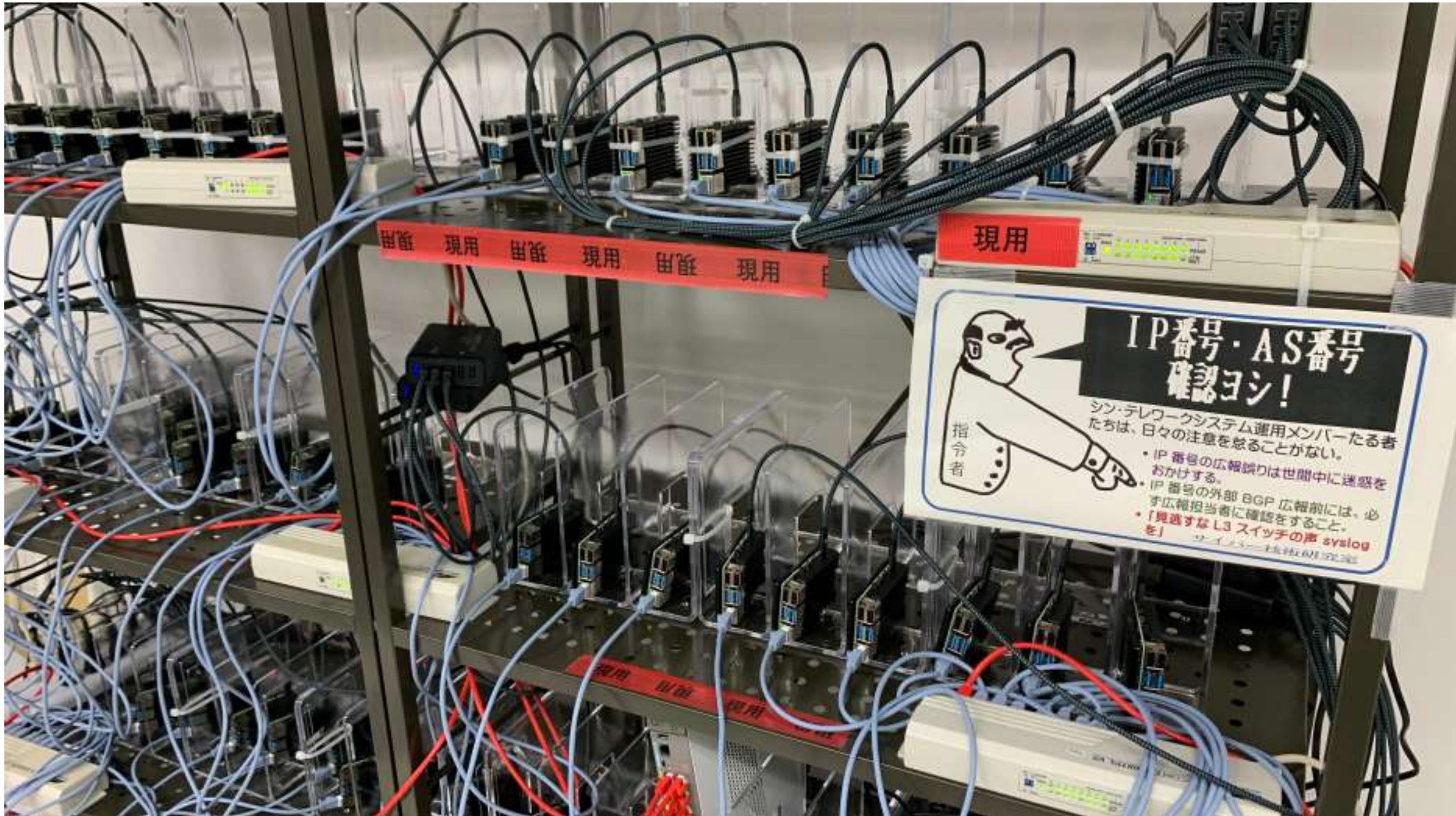


<https://telework.cyber.ipa.go.jp/>

2020/4/21 無償開放

2020/5/31 時点で約 3 万ユーザー





出番 現用 出番 現用 出番 現用

現用

IP番号・AS番号 確認ヨシ!

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。
- 「間違えなし3 スイッチの声 syslog を」

サイバーセキュリティ



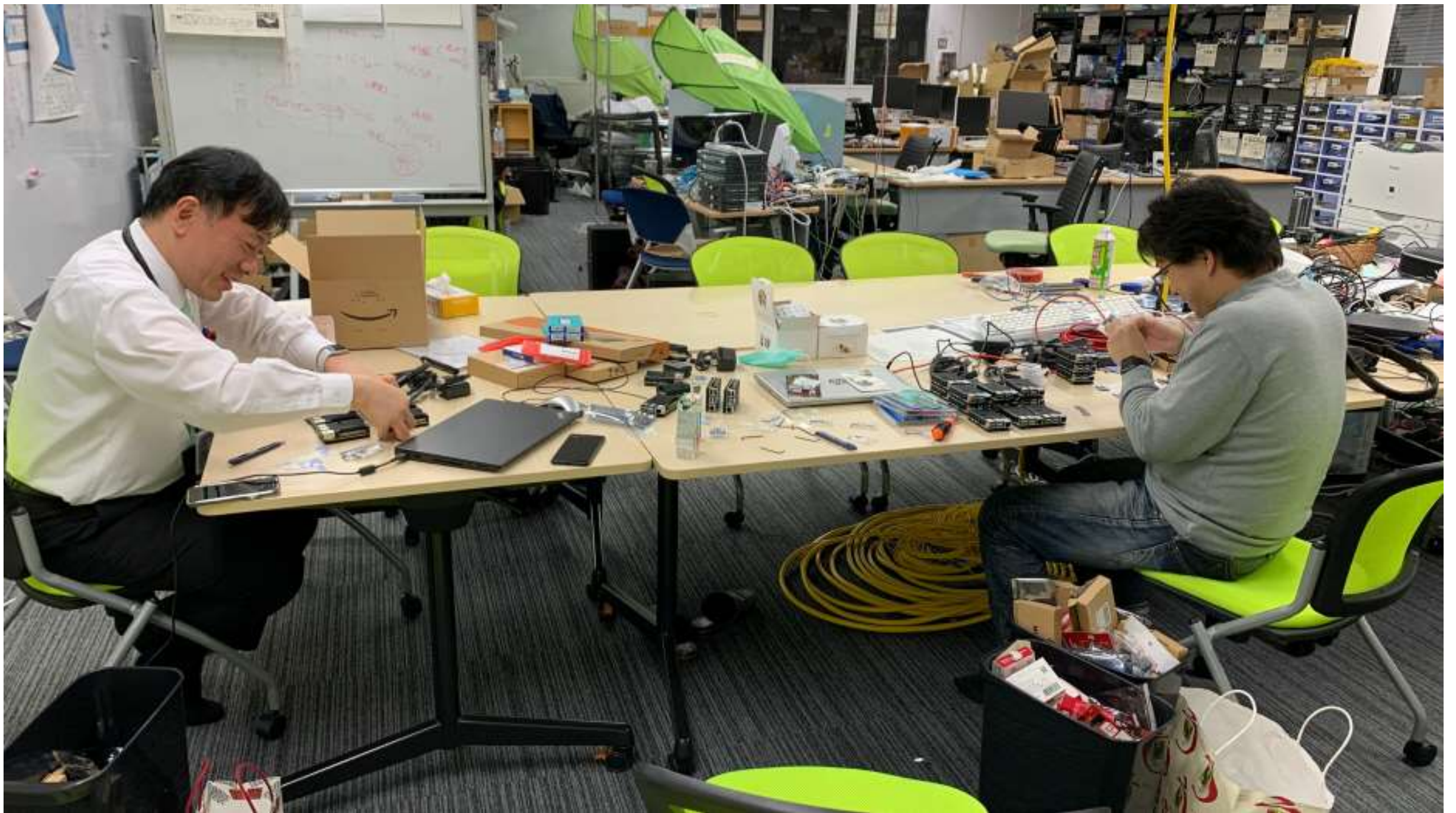
指令者

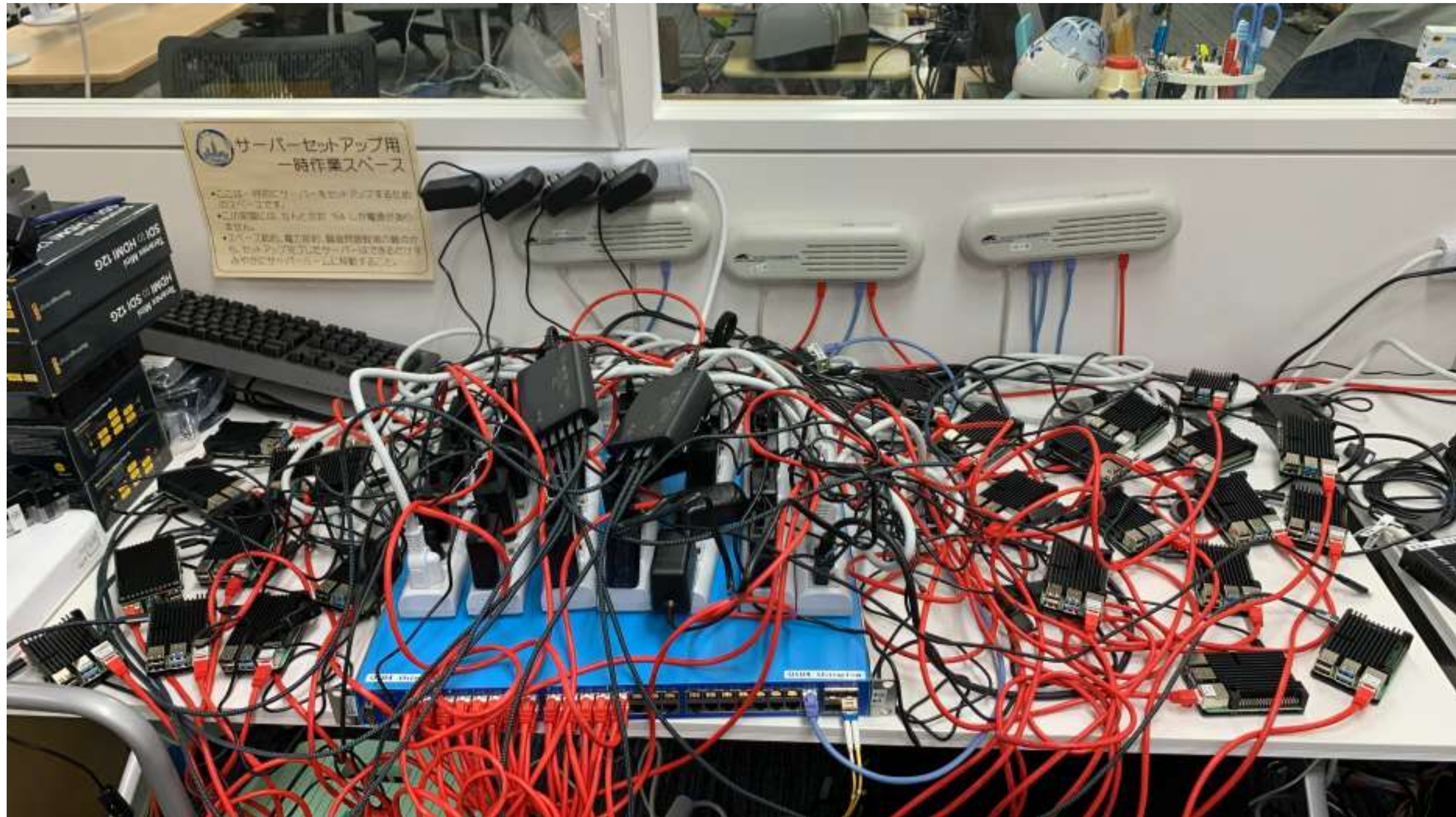
現用 出番 現用











サーバーセットアップ用
一時作業スペース

- ここは、一時的にサーバーをセットアップするための作業スペースです。
- この作業には、少なくとも1台の10Aの電源が必要となります。
- このスペースは、電力供給、騒音対策対策の観点から、セットアップされたサーバーは稼働させることができず、必ず他のサーバールームに移す必要があります。



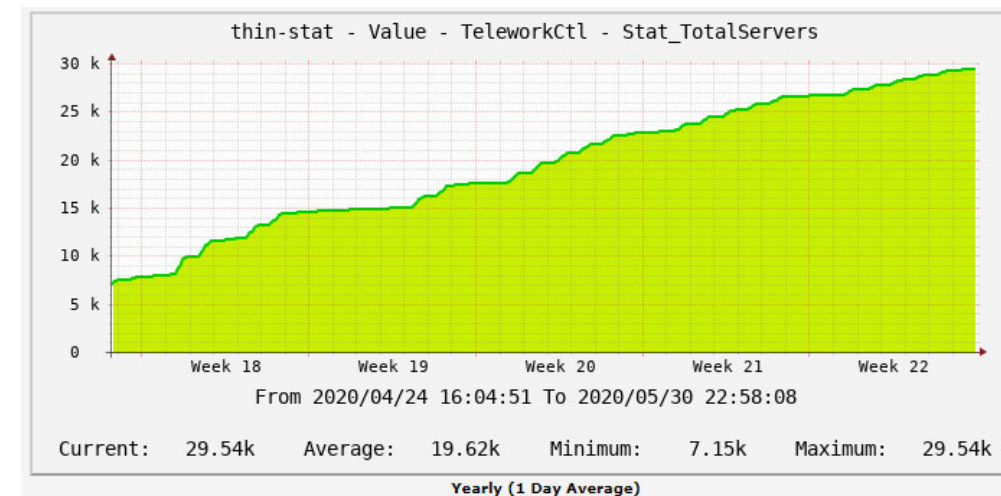
Thin Telework System 超重要ロードバランサ

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)





- 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