オレオレIP電話網を大きくしたら Tailscaleの~~不具合~~を踏み抜いて発狂した話 ワナ

上羽 未栞（a.k.a. KusaReMKN）

2025-05-16

東京広域電話網〈https://tkytel.github.io/〉
https://KusaReMKN.com/
Twitter: @KusaReMKN

今回のおはなし

東京広域電話網について

東京広域電話網の電話局同士の接続

網内のセキュリティ強化（素振り）

不思議な不通問題

ええい、総当たりじゃ！

考察・追実験

まとめ

みかんちゃんについて

自称・大天才美少女プログラミング初心者

「上羽(うわば) 未栞(みかん)」あるいは「KusaReMKN(くさればかん)」
　みかんちゃんって呼んでね！

実はプログラマでもエンジニアでもない
　古い計算機っぽいものが大好き
　最近は電話機などにも目がない

Twitter で思想を垂れ流すことが得意
　https://kusaremkn.com/ も見てね

東京広域電話網について

分散型の異常オレオレIP電話網

東京広域電話網（*Tokyo Wide Area Telephony Network*）
Telephone for Everyone, Connecting Heritages

2024年10月頃に発足したオレオレIP電話網
VoIPサーバを設置して相互接続・電話網を構築
黒電話やワープロなど異常な端末が数多く生息中

2月21日のエンジニア作業飲み集会でLT発表
電話局の数: 13 → 33
端末の数: 58 → 223
（2025-05-16 20:00現在）

現在の東京広域電話網の姿

交換局数

33 局

端末数

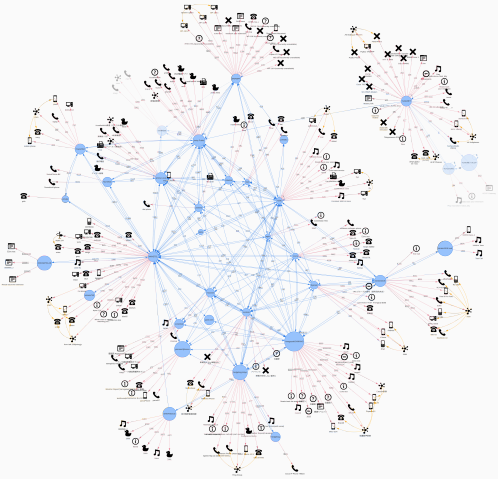
223 以上
（仮想含む）

うち黒電話

26 程度

その他

ピンク電話
ISDN や PHS



東京広域電話網コミュニティ

Website

https://tkytel.github.io/

VRChat Group

TKYTEL.6282

Discord

https://discord.com/invite/QEzAnuSy9S

GitHub Organization

https://github.com/tkytel

Mailing list

https://groups.google.com/g/tkytel

技術的なおはなし

いまさら VoIP 網

https://zenn.dev/kusaremkn/articles/abd760f9f2f450

VoIP ルータを使って黒電話を IP 電話機にする

https://zenn.dev/kusaremkn/articles/187222dc1d4f1d

ICOM VE-TA10 を使うためにパケットを書き換えたりする

https://zenn.dev/kusaremkn/articles/cb32b500fc1334

AudioCodes MP-118 VoIP Gateway を MikoPBX に収容する

https://zenn.dev/pepepper/articles/b8ad94b4b6f05f

東京広域電話網の電話局同士の接続

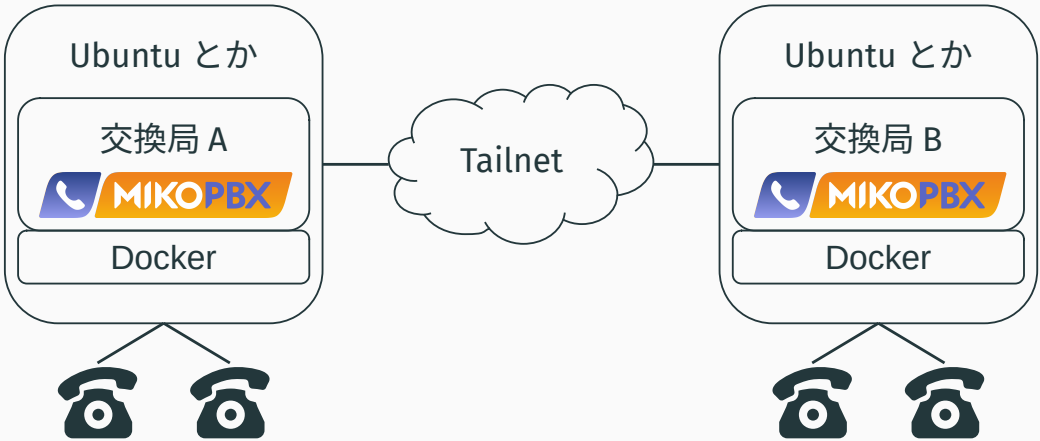
基本の構成

交換局として **MikoPBX** を用いる
　Asterisk ベースの IP PBX システム

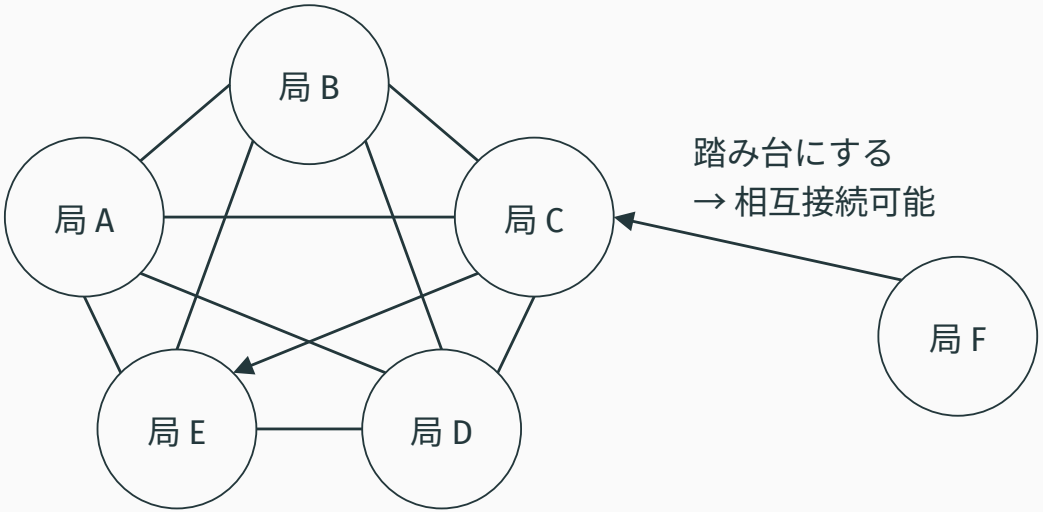
Proxmox や **Docker** を利用して
　コンテナ環境を構築

交換局同士の相互接続には
　VPN サービス **Tailscale** を用いる

システム構成図


Ubuntu とか
交換局 A
MIKOPBX
Docker
Tailnet
Ubuntu とか
交換局 B
MIKOPBX
Docker

交換局をホップするような通話にも対応



網内のセキュリティ強化（素振り）

電話網内のセキュリティを向上しよう

東京広域電話網も最初は身内向けの小規模電話網だった
　網内のユーザは全員信頼されていることが前提

時代は変わって大規模電話網になってしまった
　網内に悪意を持ったユーザが登場するおそれが出てきた
　（東京広域電話網はお前らを信じていますよ）

→ 網内のセキュリティを向上するための施策が必要

懸念事項: Tailscale でホストを共有している

電話局を相互接続するために Tailscale を利用
- 基本的には電話局のホストそれ自体を共有
- 何もしていないとそのホストの全てが見える

例えば……
- 他局の MikoPBX の設定画面（Web UI）にアクセスできる
- MikoPBX をホストしているコンテナに SSH できる
- 電話に関係のないサービスまで露出する

↑ なんかちょっと怖そう（かなり怖そう）

Tailscaleを使っているのだからTailscale ACLを使おう

Tailscale ACL（Access Control List）とは
　Tailnet上でアクセス制御をする手段

Deny by defaultからアクセス許可するルールを列挙する
　初期状態では全アクセスを許可するルールを設定済

とりあえず東京広域電話網の二大巨頭で実験

yude 局及び MikaNeTEL 局に設定して試験運用

……が、なんかうまくいかない

挙句の果てには yude-MikaNeTEL 間の通信ができなくなる

→ 交換局ホップに頼っている経路に影響

全てを元に戻してほぼ初期状態へ

MikoPBX に付属している Firewall を利用する方針へ変更

コンテナを host モードで運用しているためこれで良かった

不思議な不通問題

新規局参入 → 不通

いつものように東京広域電話網に新規局が参入
　接続確認のための自動応答番号を設置しがち
　ノウハウがぼんやりとしているのでたびたび事故が起きる

例によって今回も確認用の番号に掛けるも無音
　よくあるトラブルシューティングのノリで対応開始
　設定項目を確認するもこれといって問題点は見付からず
　どうしようもないので人対人通信で接続を確認することに

前例のない不具合: ベルは鳴れど通話はできず

相手に電話を掛けると「プルプルプル」の音が鳴る
　電話の受け側でもベルが鳴っている

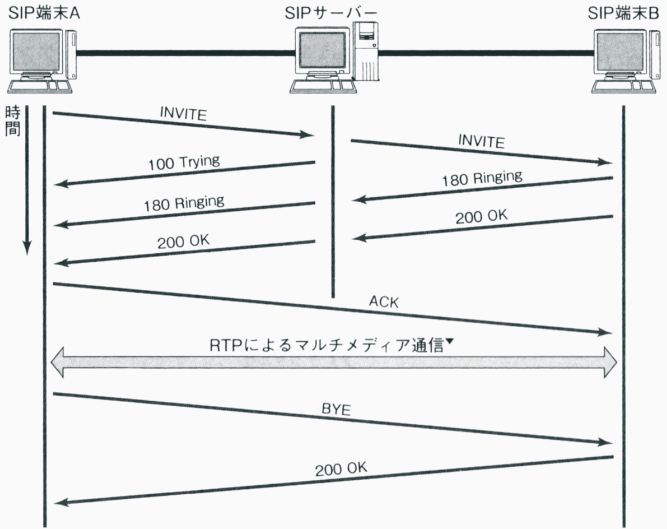
相手が受話器を上げたらしく「プルプルプル」の音が止む
　とりあえず「もしもし」してみる
　電話の受け側では「もしもし」が聞こえる
　しかし返事は聞こえない（しばらくすると通話が切れる）

IP 電話のウラ側: 呼制御の SIP と実通信の RTP

ベルが鳴っている
→ SIP は OK っぽい

声が聞こえない
→ RTP が死んでる

勝手に通話が切れる
→ だんまりだから



井上直也，村山公保，竹下隆史，荒井　透，苅田幸雄:
第 8 章 アプリケーションプロトコル，「マスタリング TCP/IP 入門編（第 6 版）」，p.331，株式会社オーム社，2021.

どうして SIP は届いて RTP は届かないのか

Firewall か何かが悪さをしていそう
- この局は Tailscale ACL や MikoPBX Firewall をいじっていた
- Tailscale ACL は yude-MikaNeTEL 間のことで嫌になっている

いったん全ての武装を解除してみる
- Tailscale ACL を all allow に
- MikoPBX Firewall を disabled に
- しかし改善せず（は？）→ 泥沼のスタート

調べてみると片方向通信になる話が出てくる

NAPT 環境下だと片方向通信になりがち
- NAPT 環境で外から内に入ってくるには
- 能動的に内から外に出る必要がある

SIP の通信はこれに該当する
- SIP サーバはリクエストがあって初めて答えてくれる

RTP の通信はこれに該当しない
- SIP 上で指定されたポートを狙って勝手に飛んでくる
- NAPT は飛んできたパケットを誰に転送するのかわからない

や、でもこれTailnet内の通信だよ？

あ、そうだったわ

その他の関係ない人たち

上流が Rakuten Turbo 5G ルータだよ？
　→ 同様の環境で疎通してる別の局がありました

無線だからか RTT めちゃくちゃデカいよ？
　→ バカ遅いリンクでも他局と通信できました（10Base2）

音声コーデック非対応なんじゃない？
　→ よく使われるものに絞ってもダメでした

ええい、総当たりじゃ！

とりあえず全局と接続テストしてみる

東京広域電話網の全ての局で片方向通信になるのか確かめてみる
　通信できる局は比較的多かった
　むしろ片方向通信や不通になる方がレア

通信できる他の局をホップしてから通信すると繋がる
　これに頼っても良いけどちょっと不便かも
　（スケールできないことを露呈していてダメ）

とはいえ、原因となるものが何もわからない

伝家の宝刀 パケットキャプチャ

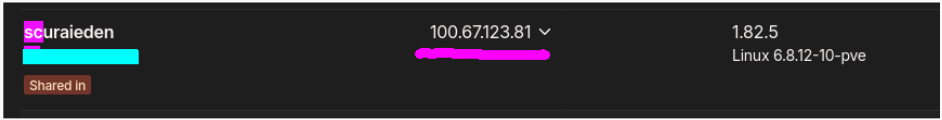
tcpdump を使ってパケットを眺めてみる
- SIP のパケットは問題なさそうに見える
- 予想通り RTP のパケットは片方しか来ていない

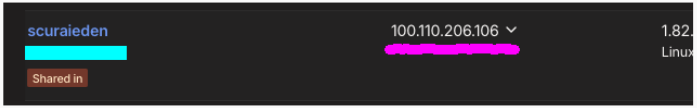
しかもなんか変な NIC に出てる
- Tailnet 上の通信は仮想 NIC（tailscale0）に流れるハズ
- 発狂している通信では物理 NIC（eth0）に流れている

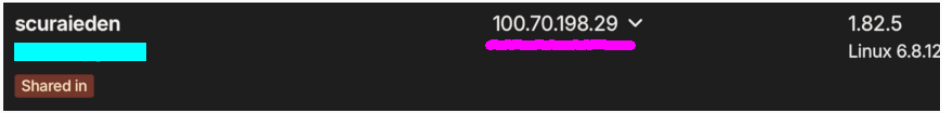
あぁ、ちゃんと100.70.198.29にパケット投げてるのに！

「え、100.70.198.29 って誰ですか」

「は？」


scuraieden
100.67.123.81
1.82.5
Linux 6.8.12-10-pve
Shared in


scuraieden
100.110.206.106
Shared in


scuraieden
100.70.198.29
1.82.5
Linux 6.8.12
Shared in


scuraieden
100.110.206.106
Shared in

TailscaleでIPv4アドレスを割り当て直すと通信可能に！

Tailscaleの機能でIPv4アドレスを再設定
　通信の両端で同じアドレスとなるように設定
　無事に通信できるようになりました

……本当か？

考察・追実験

互いに異なるIPv4アドレスが見えていたため発狂した？

お互いに見えているIPv4アドレスが異なる事象
    Tailscaleがよしなにしているなら問題ないハズ
    つまり、TailscaleがNATのように仕事をしている？

SIPで通信できたのはNAT的ふるまいのおかげ

RTPはSIPで指定されたIPアドレス・ポートを使う
    指定された場所はルーティングテーブルに存在しない
    デフォルトルートである`eth0`にパケットをぶん投げる

じゃあ追実験だ！

通信できている局間で IPv4 アドレスを変えたら発狂するのか

1. 通信できている局の対を用意する
2. 片方の IPv4 アドレスを変更してみる（発狂させる）
3. 通信が壊れる
4. IPv4 アドレスを直したら通信できるようになる

実験は失敗しました

1. 通信できている局の対を用意する
2. 片方の IPv4 アドレスを変更してみる（発狂させる）
3. ~~通信が壊れる~~ ← **壊れませんでした**
4. IPv4 アドレスを直したら通信できるようになる

そもそも異なる IPv4 アドレスが見えていたのに
　通信できていた局も存在していたのでした

つまりルーティングテーブルにないホストと通信できている
　（もう何もわからん）

まとめ

オレオレIP電話網を破壊したり発狂したりしてみた

分散形の異常オレオレIP電話網「東京広域電話網」

ベルは鳴るのに音声が届かない問題を掘り下げた

SIPとRTPとの通信の違いを確認した

Tailscaleのせいなのか何なのかよくわからない感じになった

バックボーンの通信も自分で実現すれば発狂せずに済むかもネ
　東京広域通信網に乞うご期待

東京広域電話網は

老練な
ネットワークエンジニア

を募集しています

電話屋さん、懐古厨、カーネルエンジニア、信号処理屋さん、古代のコンピュータ技術者を含む一般人・逸般人も可

おわりです

Telephone for Everyone, Connecting Heritages

このスライドについて

Written in May 2025.

Permanent ID of this document: `c8edfb391dbbafd3`.