自宅VPNのセキュリティを考え直す

神保道夫＠NISOC

2026/06/06

はじめに

- 自宅の外壁工事に伴い、ネット回線をフレッツ光+AsahiNetから、ケーブルテレビ系のNCTに変更して約1年が経ちました。
  10G回線を使える様にはなったものの、使っていくうちに、これまでとは違う使い方をする必要があり、ネットワークの課題点を改善することを検討し始めました。
- 現在進行中のため、今どのような事を検討しているか、の途中経過をお話したいと思います。

フレッツ光とNCTの回線で大きく異なる点(1)

- IPv4アドレスは、DHCPv4で取得されます。DHCPv4のアドレススペースはISP Shared Address(100.64.0.0/10)を使っており、私のエリア(旧長岡市内？) は10.127.192.0/18のアドレスブロックから割り当てがされているようです。
- IPv4アドレスは無制限に配布されるわけではないようです。
  短時間にNICを何回か取り替えると、5台くらいでIPアドレスが取得できなくなることがあり、基本的にはルータを設置する必要があります。
- 月額2,200円で固定グローバルIPv4アドレスを申し込むことも出来ますが、固定アドレスと接続したい機器の結びつけをどうやるのか、などは、申し込んでないので不明です。
- 申し込みをする事により、無料でIPv6アドレスを付与することが出来ますが、WindowsマシンにDHCPv6で/128のアドレスを払い出す仕様なので、ルータを併用する場合は、ルータがIPv6パススルー仕様に対応する必要があります。

フレッツ光とNCTの回線で大きく異なる点(2)

- これらの点を踏まえると、自宅にVPN接続をしたい場合は、
  グローバル固定IPv4アドレスを契約し、IPv4アドレスでVPN接続する、
  というのが解となります。
- 実際に私が行っている方法はちょっと違うのですが、ここはオフレコの
  話になるので、資料には掲載せず、口頭でお話します。

VPNに変わる方法を模索してみる

・「セキュリティを担保する」「費用は(なるべく)かけない」「新たな技術を検討する」というテーマで最新技術を調べてみると「Tailscale」を見つけました。

・Tailscale(https://tailscale.com/)は、Wireguardを使用しており、各クライアントPCにTailscaleのソフトを入れる事により、ルータに特別なソフトを入れなくても、クライアント同士、もしくは仮想ネットワークでのアクセスが可能となるソフトです。

・Tailscaleを使用するためには、Tailscaleに専用アカウントを作成して、自サイトの管理用コンソールを準備し、各PCでTailscaleのソフトを起動すると、各デバイス毎にTailscale内で有効な固定専用IPアドレスが割り当てられます。固定専用IPアドレスを使用することにより、PC間でのアクセスが可能となります。

・Exit-node機能を使うことにより、自宅経由でアクセスしていると見せかける機能も良く使われているようです。

Tailscaleの弱点？ 改善点？

- まいの雑記帳(https://mq1.dev/entry/j7zvrsp48lb)でバズった、「Tailscale やめたい」という内容が参考になります。
- デフォルトMTUは1280バイトとなっています。MTUをしっかり計算して使わないと、パフォーマンスが落ちる可能性があります。
- ISP Shared Addressをアクセス用のIPアドレスとして使用しています。NCTのDHCPv4アドレスとバッティングして、挙動がおかしくなる可能性がある？
  →やっぱりありました。Routedを起動しているとルーティングが混乱しそう。
- FreeBSDのpackageや、OpenBSDのpackageにはTailscaleはあります。NetBSDのpackageにはTailscaleが無い様です。Wireguardのプロトコルはあるし、githubにソースはあるので(https://github.com/tailscale/tailscale)、go言語が使えれば動きそうですが、なんかあるのですかね。

別解として、Netbirdを紹介します。

- Netbird(https://netbird.io/)は、Tailscaleとほぼ同じ機能を持っています。
  実際にはTailscaleで出来ない部分が出来るようになっています。
- デフォルトMTUの変更(引数 --mtu)や、専用固定IPアドレスを指定
  する機能(管理コンソール上で設定可能)、/etc/resolv.confの書き換えを
  行わない(引数 –disable-dns)なども実装されており、優れた部分もあります。
- FreeBSD及びNetBSDではNetbirdがpackagesで提供されています。
  OpenBSDはpackagesにありませんが、恐らくFreeBSDのportsを参考に
  すれば、package化できる可能性はありそうです。
  (https://github.com/netbirdio/netbird)

現状の目論み

- GL.iNetのWiFi6 トラベルルータ(GL-MT3000, 約¥17,000円)を購入し、OpenWrt 25.12.4を使用してNetBird(0.66.2)をインストール。
- NetBirdの動作にはそれなりのメモリが必要。お試しでやってみた、GL-AR750Sではメモリが128MBしかなく、起動したらメモリ不足で使い物にならなかった。
- 自宅LANとして、10.0.0.0/24を使用する。
- NetBirdとunboundを動かし、netbird.cloud ドメインは10.255.255.254にフォワード、それ以外はNextDNSにクエリーを出し、ローカルのDNSサーバーとして常時稼働できるようにする。
- 外部からアクセスしたい場合は、自分のPCでNetBirdを動かし、Exit-nodeとしてファイルサーバーにアクセスする。
- もう少しでいけそう、というところまでは来ているが・・・

まとめ

- NetBirdを使用して、VPNの代わりに使うことは出来そう。
- ただし、新しい技術の習得にはそれなりに時間が掛かる。
- これがうまくいくと、テスト用サーバーを自宅にいる間、
  常時動かす必要もなくなるので、なんとか動くようにしたい。