Debian / Ubuntu ユーザーミートアップ in 札幌 2018.07

Debianで自宅にリモート接続 / OpenVPN編

Norimitsu Sugimoto (杉本 典充)
dictoss@live.jp

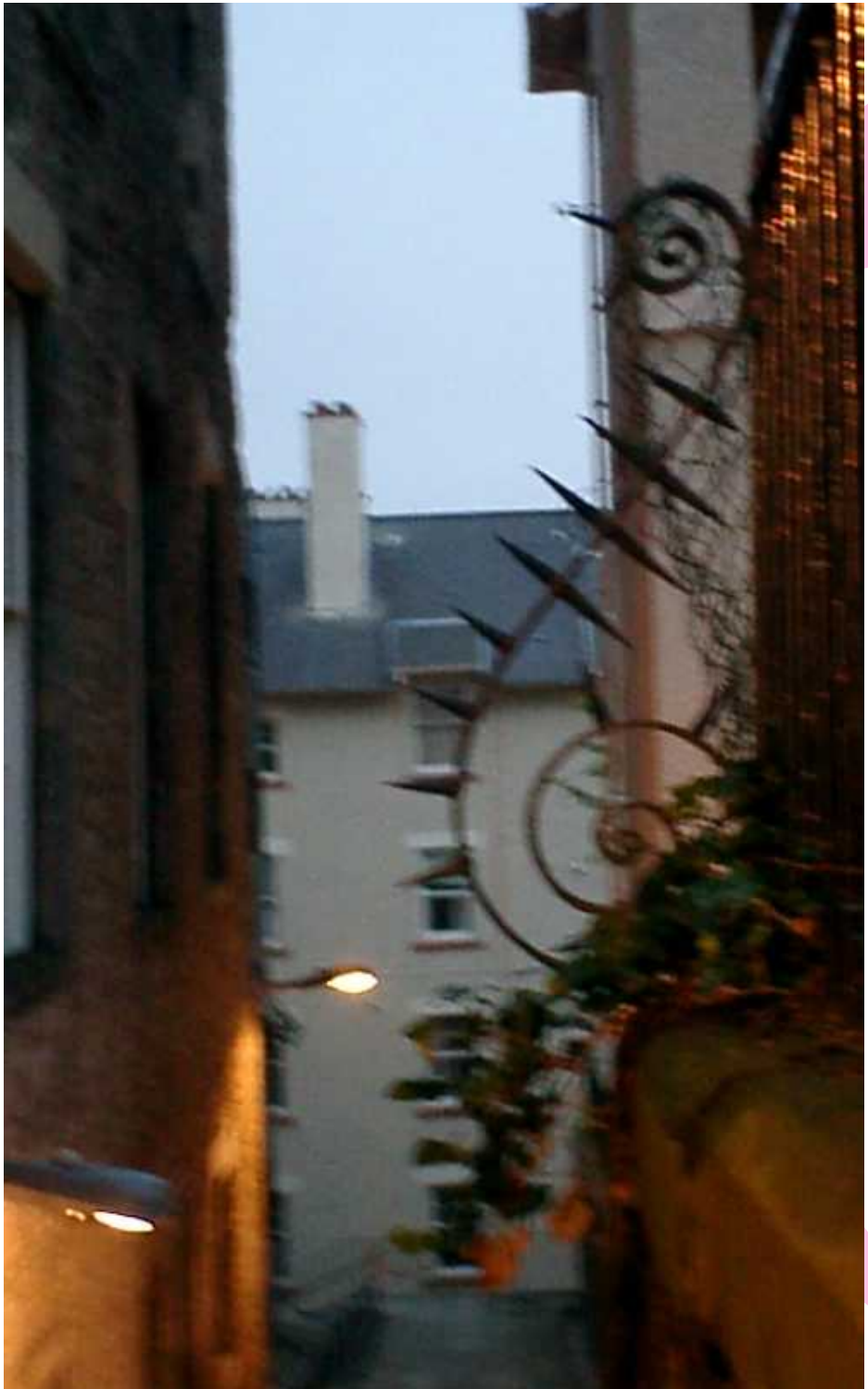
2018-07-06

アジェンダ

- 自己紹介
- VPN について
- OpenVPN の紹介
- OpenVPN の設定（サーバ、クライアント）
- おわりに
- 参考資料

自己紹介

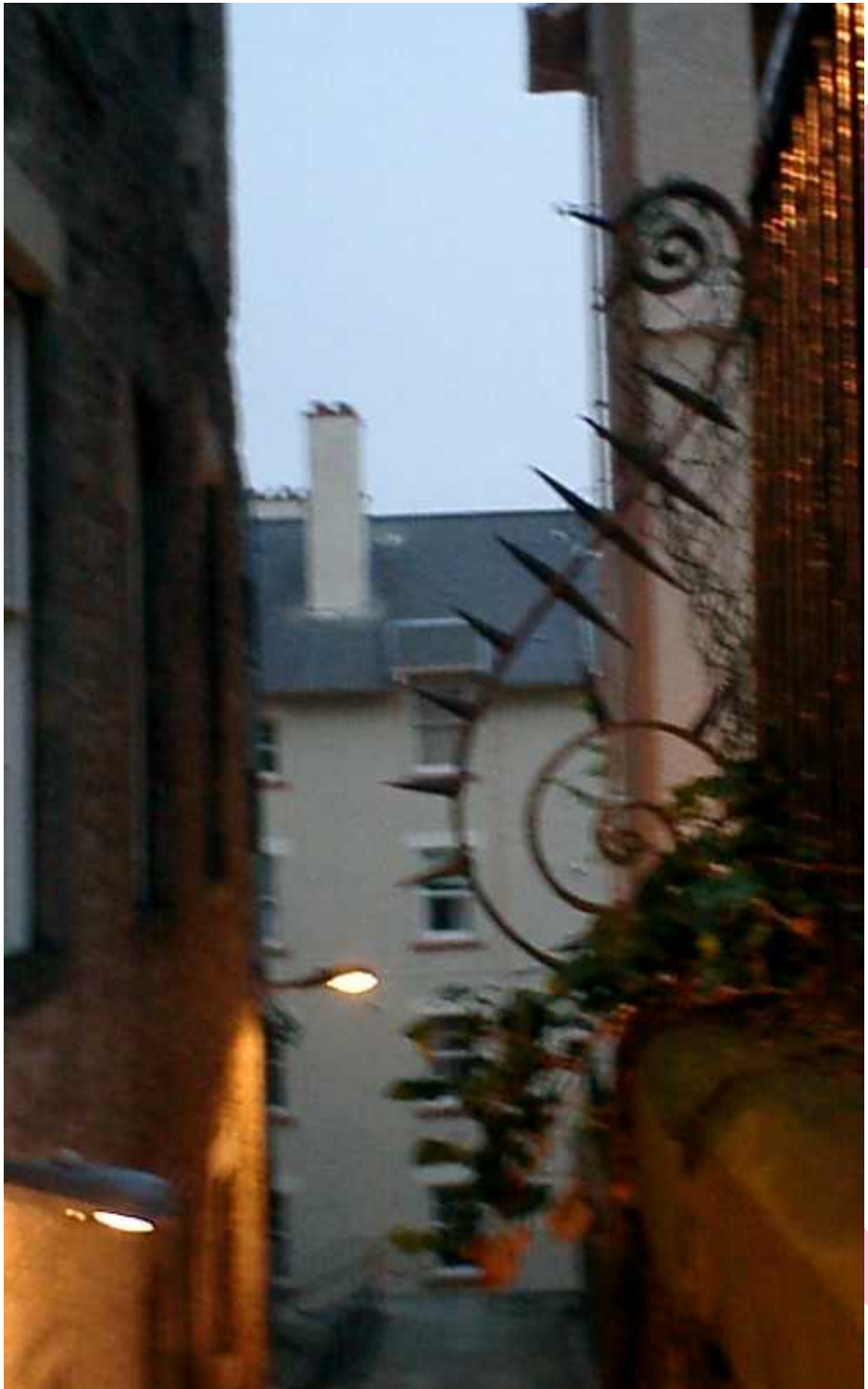
- Norimitsu Sugimoto (杉本 典充)
- dictoss@live.jp
- Twitter: @dictoss
- 大学生のときから Debian を使っています
- 仕事はソフトウェア開発者をやってます



VPNについて

VPN の種類

- IPsec 系
  - L2TP/IPsec
- SSL-VPN 系
  - SSTP
  - SoftEther
  - OpenVPN
- 利用を推奨しない過去の技術
  - PPTP（セキュリティ強度が低く、突破済み）



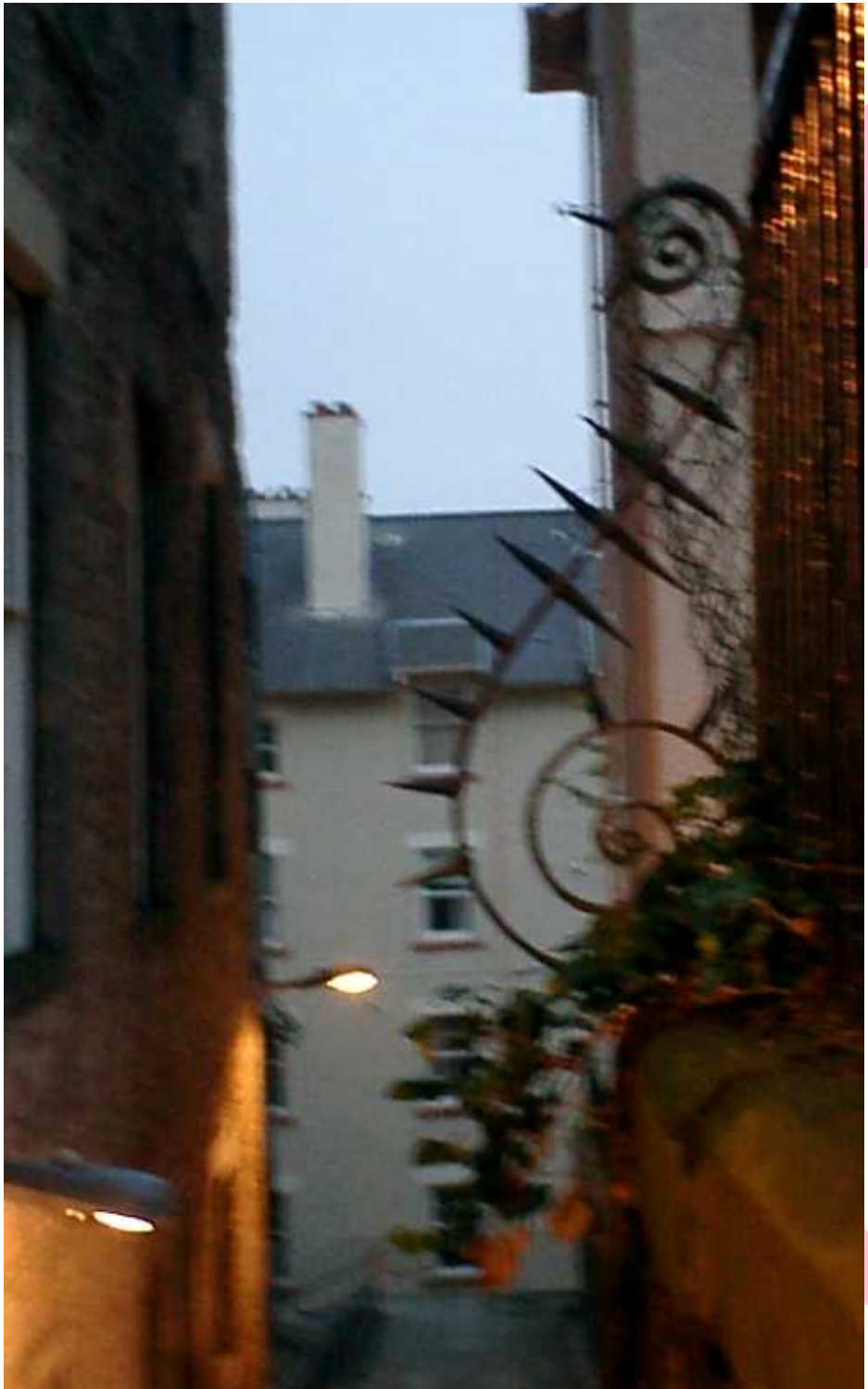
OpenVPN の紹介

OpenVPN の紹介

- SSL-VPN を使った VPN 接続を行うソフトウェア
- https://openvpn.net/
- ライセンスは GPLv2
- TLS 1.0〜TLS 1.2 による暗号通信をサポート
- サーバ側の機能とクライアント側の機能の両方をもつ
- デフォルトのポート番号は 1194/UDP で、TCP も利用可能

Debian における OpenVPN

- Debian 8
  - openvpn-2.3.4、openvpn-2.4.0（jessie-backports）
- Debian 9
  - openvpn-2.4.0、openvpn-2.4.4（stretch-backports）
- openvpn の 2.3 系と 2.4 系の違い
  - 2.3.3 から TLS 1.2 が利用可能。ただし使える暗号は TLS 1.0 由来のものに限られる（AES-CBC、RSA、DHE）
  - 2.4 から AES-GCM や、ECDHE、ECDSA など TLS-1.2 で利用可能な高度な暗号をサポート
  - サーバとクライアントで 2.3 系と 2.4 系が混在する場合、古いバージョンがサポートする設定に合わせる必要がある



OpenVPN の設定の解説

OpenVPN の設定（サーバ）

- "apt-get install openvpn" でインストール
- 証明書や鍵の生成（easy-rsa 2）
  - `https://openvpn.net/index.php/open-source/documentation/miscellaneous/77-rsa-key-management.html`
- サーバ側の設定のサンプル
  - `https://github.com/OpenVPN/openvpn/blob/master/sample/sample-config-files/server.conf`
- 設定ファイルは"/etc/openvpn/*.conf"を利用。複数の VPN 設定を同時実行するマルチインスタンスが可能。例）443/TCP と 1194/UDP の両方を listen する

OpenVPNの設定（サーバ側を一部抜粋）

```
tls-server
tls-version-min 1.2
port 443
proto tcp
dev tun0
persist-key
persist-tun
push "dhcp-option DNS 192.168.2.1"
push "route 192.168.2.0 255.255.255.0"
client-to-client
client-config-dir /etc/openvpn/ccd
tls-auth /etc/openvpn/easy-rsa/2.0/keys/ta.key 0
  (snip)
```

OpenVPN の設定（クライアント）

- "apt-get install openvpn" でインストール
- クライアント側の設定のサンプル
  - `https://github.com/OpenVPN/openvpn/blob/master/sample/sample-config-files/client.conf`
- 設定ファイルは、"/etc/openvpn/client.conf" とすること
- systemctl start openvpn で起動

OpenVPNの設定（クライアント側を一部抜粋）

```
client
tls-client
tls-version-min 1.2
dev tun
proto tcp
remote yourserver-fqdn 443
nobind
ca /etc/openvpn/ca.crt
cert /etc/openvpn/myclient1.crt
key /etc/openvpn/myclient1.key
tls-auth /etc/openvpn/ta.key 1
log /var/log/openvpn.log
log-append /var/log/openvpn.log
```

おわりに

- Debian パッケージで提供している OpenVPN を説明しました
- サーバ側とクライアント側の設定を説明しました
- 速度重視の場合は、UDP を使ってください
- つながらない、切れやすい場合は、openvpn の設定ファイルの MTU 値を少し小さくしてみてください
- 北海道の広大な地でも、VPN 接続できればノート PC からどこでも自宅のネットワークへ接続できます

参考情報

- https://wiki.debian.org/OpenVPN
- https://openvpn.net/index.php/open-source/documentation.html