

目次

SORACOM Arc を使う	1
1. インターネット接続設定	1
2. バーチャルSIM/Subscriber の作成	1
3. WireGuard PublicKey をコピーする	1
4. コピーした WireGuard PublicKey を登録する	2
5. MA の設定に必要な各種情報を取得する	3
6. MA に WireGuard VPN の設定をする	4
7. ステータス確認	6
参考▯CLI 設定	7
参考▯SORACOM Napter を利用してのログイン	7
補足▯DNS 設定	8

SORACOM Arc を使う

WireGuard VPN 機能を使用して[SORACOM Arc](#) の利用が可能です。

WireGuard VPN は Web UI 設定画面から設定できます。

1. インターネット接続設定

MA を有線もしくは LTE でインターネット接続できるように設定します。それぞれの設定方法は下記を参照して下さい。

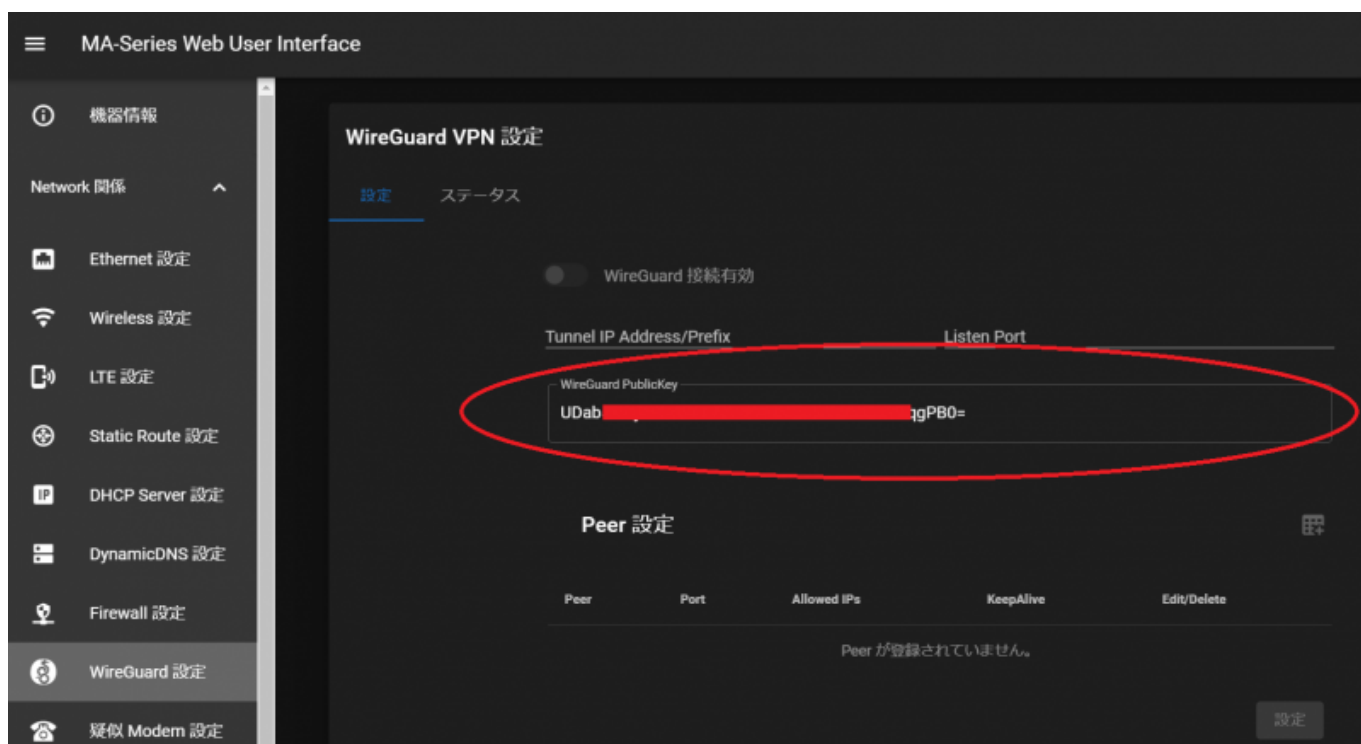
- [有線設定](#)
- [LTE 設定](#)

2. バーチャル SIM/Subscriber の作成

SORACOM ユーザーコンソールで[バーチャル SIM/Subscriber](#) を作成します。

3. WireGuard PublicKey をコピーする


MA の GUI 設定画面にログインし、WireGuard PublicKey をコピーします。



4. コピーした WireGuard PublicKey を登録する

SORACOM ユーザーコンソールで MA からコピーした WireGuard PublicKey を登録します。

SIM 詳細

SIM ID	[REDACTED]
IMSI	[REDACTED]
名前	[REDACTED] 
グループ	<div></div>

詳細情報 通信量履歴 タグ セッション詳細 パケットキャプチャ **バーチャル SIM**

VIRTUAL SIM IMSI

 セッション  **認証情報**  高度な設定

 **認証情報** SET

クライアントピア 公開鍵	/42 [REDACTED] nBQ=
サーバーピア 公開鍵	QluOQ [REDACTED] qBh4=

▼ 公開鍵を更新

① 公開鍵を設定したり、新しい認証情報を生成すると、既存の認証情報が上書きされ、現在のセッションがリセットされます。再度接続するには、デバイスの WireGuard 設定を新しい認証情報で更新する必要があります。

WireGuard の認証情報を生成した場合は、こちらで公開鍵を登録してバーチャル SIM を更新します。

公開鍵

UDat [REDACTED] 0o>

 公開鍵を保存

バーチャル SIM の新しい公開鍵と秘密鍵を生成します。

自動生成された認証情報を使用

☐ 認証情報を生成

5. MA の設定に必要な各種情報を取得する

SORACOM ユーザーコンソールで下記の情報を取得します。このパラメータを MA に設定します。

- クライアント IP アドレス
- サーバピア公開鍵
- サーバエンドポイント
- Allowed IPs

SIM 詳細

SIM ID	
IMSI	
名前	
グループ	

詳細情報

通信量履歴

タグ

セッション詳細

パケットキャプチャ

バーチャル SIM

VIRTUAL SIM IMSI

セッション

認証情報

高度な設定

セッションステータス

ONLINE

クライアントピア IP アドレス	10.
クライアントピア 公開鍵	UDa
サーバピア 公開鍵	Qluc
サーバ エンドポイント	arc.soracom.io:11010

以下の WireGuard 接続情報をデバイスに設定してください。

```
[Interface]
PrivateKey = <YOUR_PRIVATE_KEY>
Address = 10./32

[Peer]
PublicKey = Qi
AllowedIPs = 100.127.0.0/21, 100.127.10.0/28, 100.127.10.128/25, 100.127.10.17/32, 100.127.10.18/31, 100.127.10.20/30, 100.127.10.24/29, 100.127.10.32/27, 100.127.10.64/26, 100.127.11.0/24, 100.127.12.0/22, 100.127.128.0/17, 100.127.16.0/20, 100.127.32.0/19, 100.127.64.0/18, 100.127.8.0/23, 54.250.252.67/32
Endpoint = arc.soracom.io:11010
```

クライアント IP アドレス

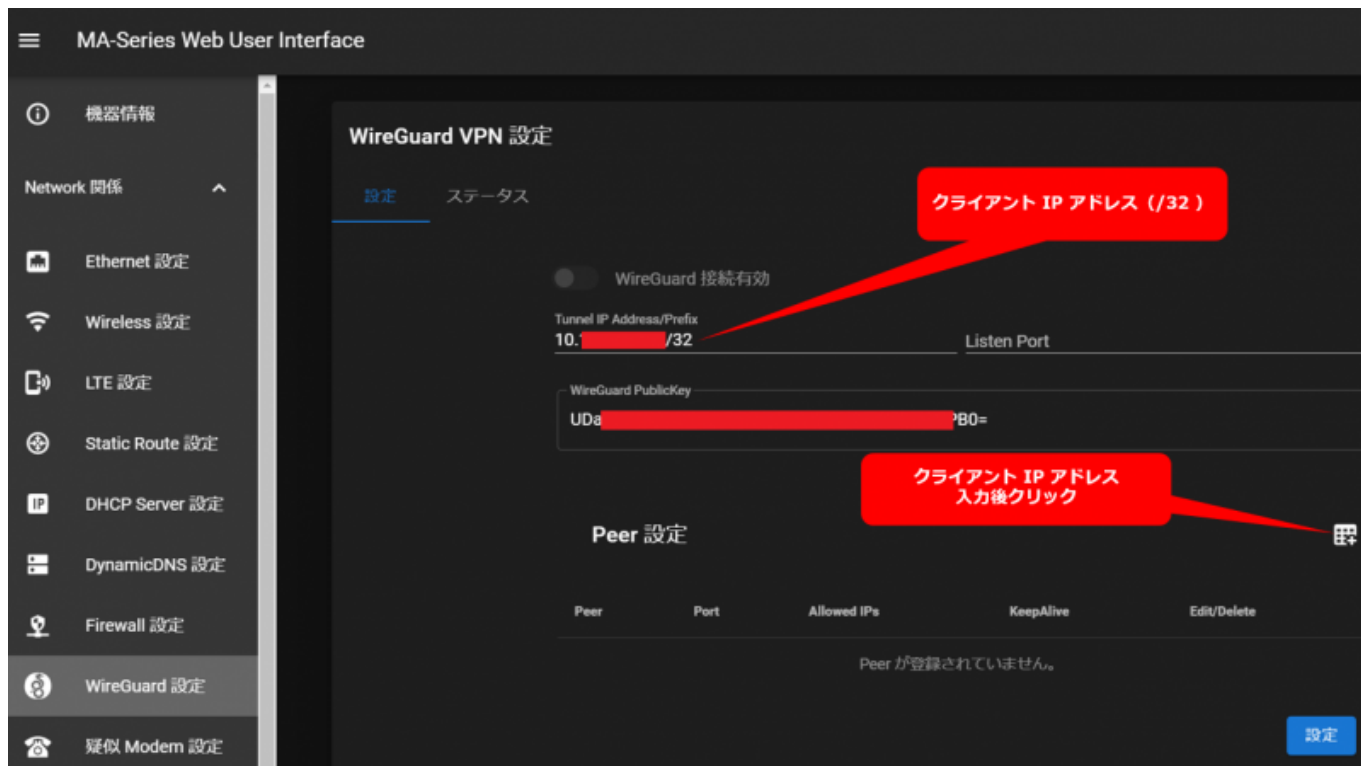
サーバピア公開鍵

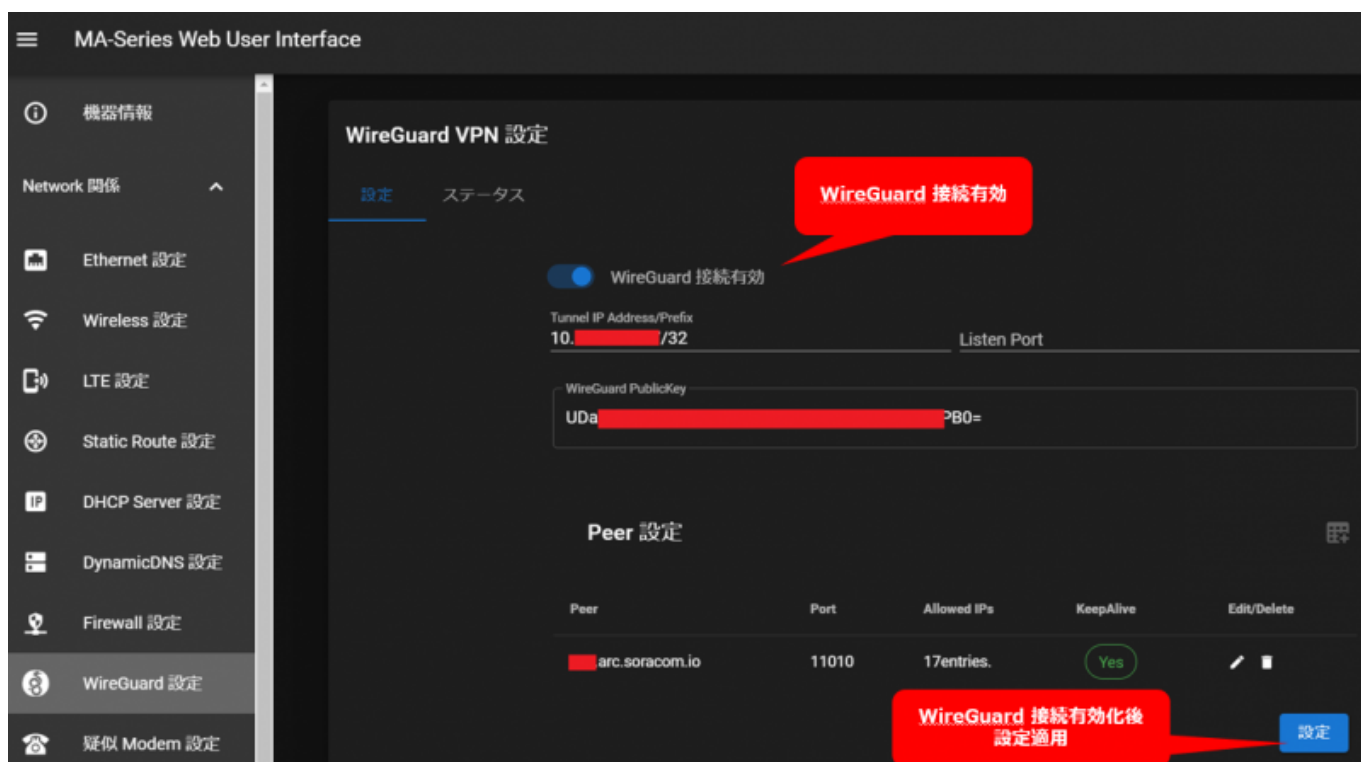
サーバエンドポイント

AllowedIPs

6. MA に WireGuard VPN の設定をする

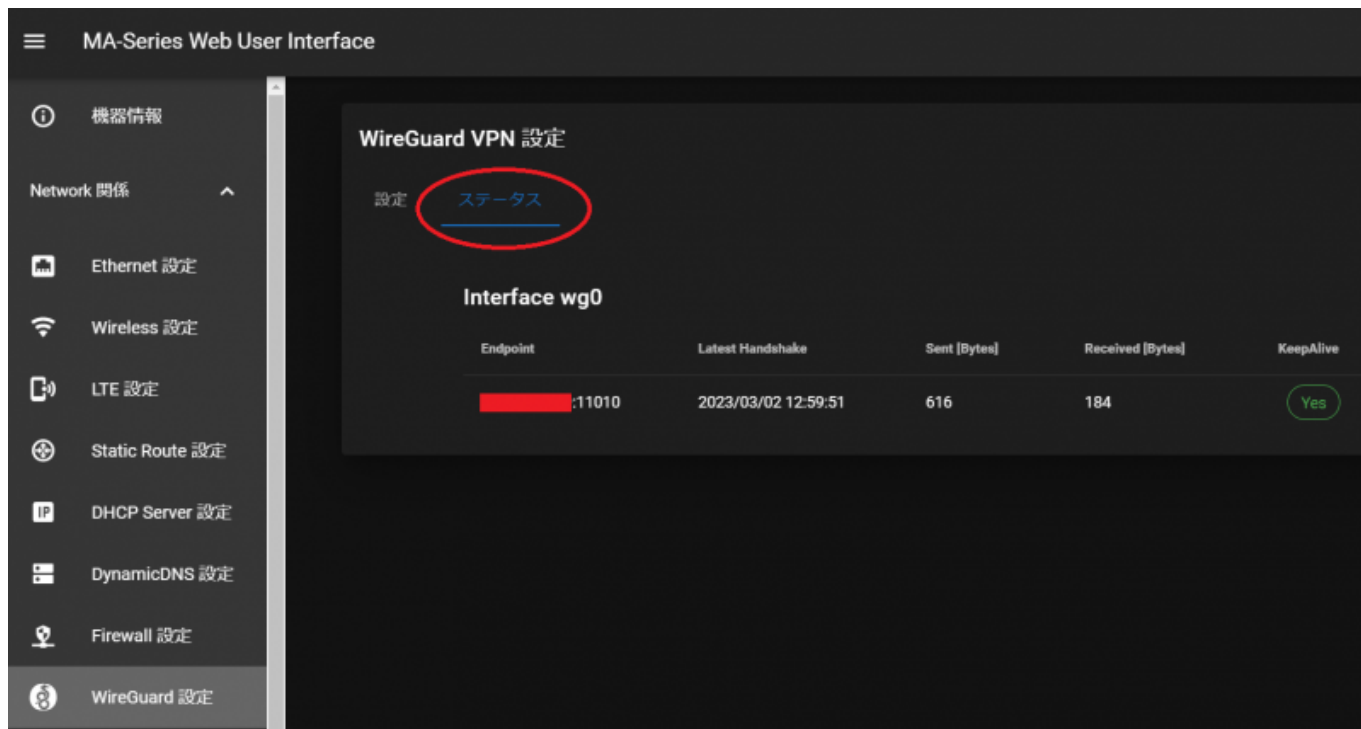
取得した情報を MA に設定します。





7. ステータス確認

WireGuard VPN のステータスを確認できます。



参考□CLI 設定

CLI 上では下記のように設定されます。

```
user1@gemini:~$ cat /etc/wireguard/wg0.conf
[Interface]
Address = 10. [REDACTED] /32
PrivateKey = sB [REDACTED] .Eg=

[Peer]
EndPoint = [REDACTED].arc.soracom.io:11010
PublicKey = QI [REDACTED] iBh4=
AllowedIPs = 100.127.0.0/21, 100.127.10.0/28, 100.127.10.128/25, 100.127.10.17/32, 100.127.10.18/31, 100.127.10.20/30, 100.127.10.24/29, 100.127.10.32/27, 100.127.10.64/26, 100.127.11.0/24, 100.127.12.0/22, 100.127.128.0/17, 100.127.16.0/20, 100.127.32.0/19, 100.127.64.0/18, 100.127.8.0/23, 54.250.252.67/32
PersistentKeepAlive = 25
user1@gemini:~$
```

参考□SORACOM Napter を利用してのログイン

WireGuard VPN 接続後は[SORACOM Napter](#) を利用して外部から MA への Web UI ログインが可能です。

フィルタ設定等は不要です。

オンデマンドリモートアクセス

IMSI

XXXXXXXXXX

オンデマンドリモートアクセスを有効にするには、以下の項目を入力してください。

1SIMあたりの月間利用に応じて料金が発生します。

この SIM はオンデマンドリモートアクセスの月額料金が発生しています。今月は追加料金なしで有効にできます。

☐ TLS

デバイス側ポート

80

アクセス可能時間

30分

80 指定

必要に応じて設定

アクセス元IPアドレスレンジ

アクセス元IPアドレスの範囲をCIDR形式（例：12.34.56.78/30）で入力してください。カンマで区切って複数のレンジを入力することもできます。空の場合は現在アクセスしているグローバルIPアドレスが指定されます。

キャンセル

OK

補足□DNS 設定

WireGuard I/F 経由の DNS Server 設定に対応しました。

※ SORACOM Arc 経由で SORACOM Beam などにホスト名でアクセスする場合、**100.127.0.53 or 100.127.1.53** を登録する必要があります。

WireGuard VPN 設定

設定 ステータス

☐ WireGuard 接続有効

Tunnel IP Address/Prefix: 10.0.0.1/32

Listen Port: 100.127.0.53

DNS Server 1: 100.127.0.53

DNS Server 2: 100.127.1.53

WireGuard PublicKey: j79+ [REDACTED] XfiM=

Peer 設定

Peer	Port	Allowed IPs	KeepAlive	Edit/Delete
Peer が登録されていません。				

設定

From:

<https://wiki.centurysys.jp/> - MA-X/MA-S/MA-E/IP-K Developers' WiKi

Permanent link:

https://wiki.centurysys.jp/doku.php?id=mae3xx_tips:soracom:connect_soracom_arc:start

Last update: **2023/05/18 11:09**