

# **LimeSDR GNSS Spoofer**

## **取扱説明書**

2020/04/03

Kaito Kobayashi

# 1. ハードウェア

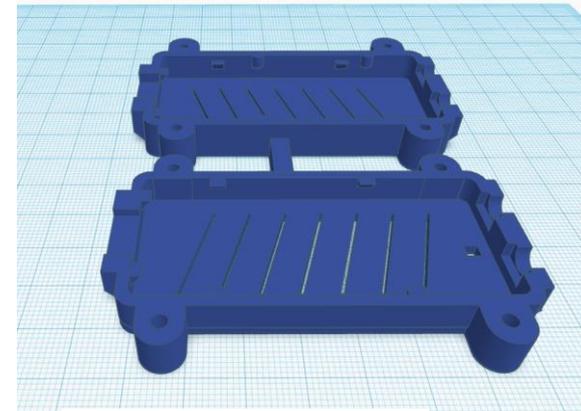
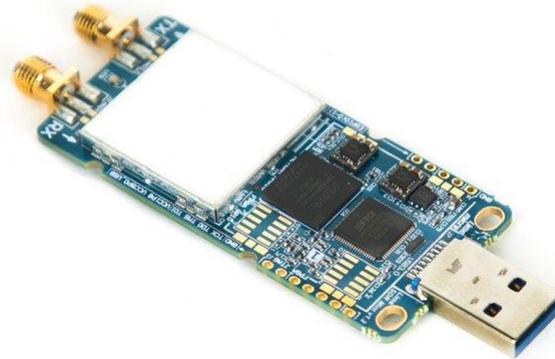
## 構成部品

- ・ LimeSDR-Mini ¥21500 (Crowd Supply)
- ・ ケース ¥1700 (DMM.make)
- ・ 再放射アンテナ ¥1000
- ・ アッテネーター(10dB\*2) ¥800

-----  
Total ¥25000

## LimeSDR-Mini 仕様

- RF送受信チップ: LMS7002M  
送信1ch, 受信1ch (10MHz-3.5GHz)
- FPGA: Altera MAX 10
- インターフェイス: USB Type-A
- サイズ: 69 mm x 31.4 mm, 20g



## 2. ソフトウェア

LimeGNSS.exe

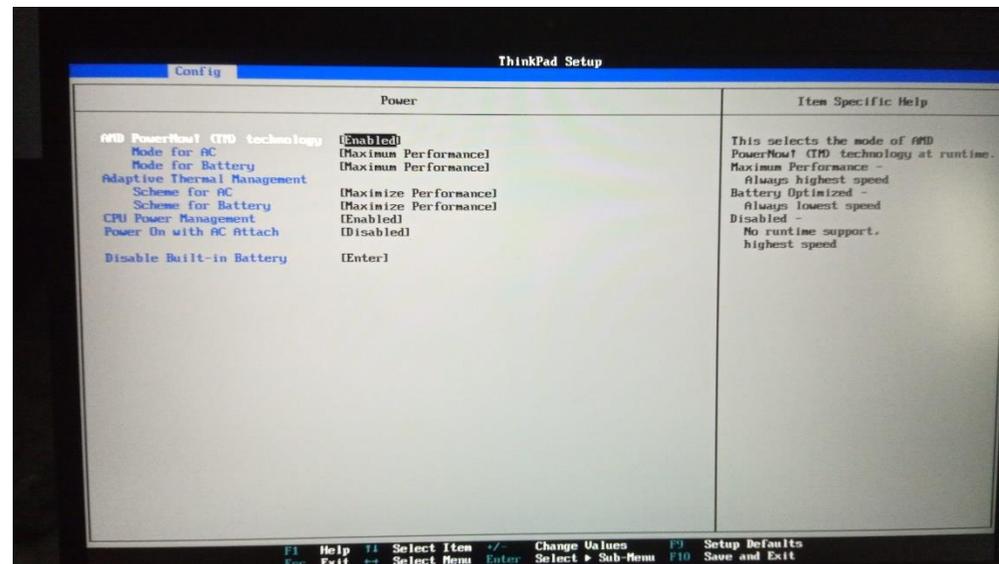
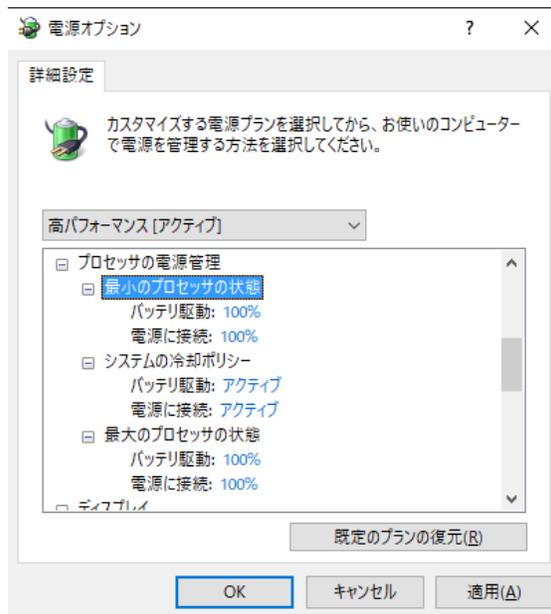
- Windows7, 8, 8.1, 10対応 (64bit)
- 推奨スペック  
CPU: intel core i7-6700, AMD ryzen5 2400G相当  
メモリ: 8GB以上
- 機能
  - GPS,QZSSのL1C/A信号の生成と放射(最大16ch)
  - 過去、リアルタイム、2時間後の範囲で信号を生成可能
  - 全地球上の位置にスプーフィング可能
  - スプーフィング位置は定点または事前に生成した軌跡データに基づくダイナミック位置
  - 速度情報のスプーフィング可能
  - 時刻情報のスプーフィング可能
  - スプーフィング継続可能時間は24時間まで

## 2. ソフトウェア

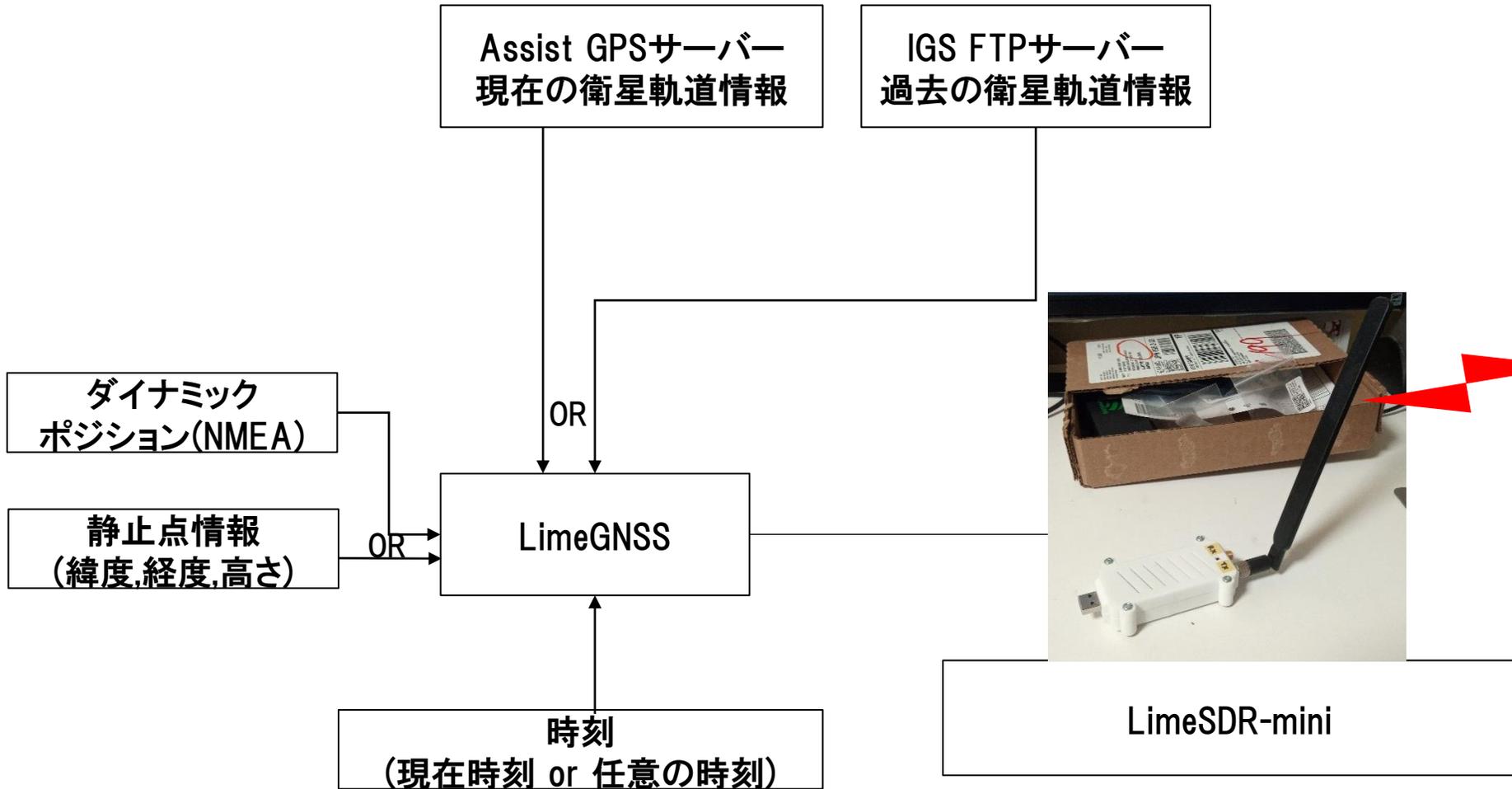
ノートPCでバッテリー駆動した場合、PCの設定によってはCPUのクロックダウンが発生し、信号生成タイミングの遅延からスプーフィング途切れることがあります。

これを避けるために以下のパフォーマンス設定を推奨します。

- コントロールパネル > 電源オプション でプロセッサを100%使用する。
- BIOSのパワーマネジメントをハイパフォーマンスに変更(PCによって「異なります」)。



# 3. システム構成



## 4. ドライバのインストール

LimeSDR用のドライバとソフトをPCにインストールします。

1. [https://wiki.myriadr.org/Installing\\_Lime\\_Suite\\_on\\_Windows](https://wiki.myriadr.org/Installing_Lime_Suite_on_Windows)  
の1の手順に従ってPothosSDRというソフトをダウンロード・インストールします。

## 5. ソフトウェア ファイル構成

BRDC00IGS_R_20200710000_01D_MN.r...	2020/03/13 10:41	GZ ファイル	879 KB	
RTCM3EPH.nav	2020/03/13 11:07	NAV ファイル	91 KB	衛星軌道情報(現在)
ECJ-HRM.nmea	2019/11/15 15:24	NMEA ファイル	728 KB	移動シナリオファイル (NMEA GGAフォーマット)
hakodate.nmea	2020/01/28 11:27	NMEA ファイル	774 KB	
TowerBridge10gs.nmea	2019/07/05 12:32	NMEA ファイル	82 KB	
LimeGNSS.pdb	2020/03/12 17:41	PDB ファイル	556 KB	
BRDC00IGS_R_20200710000_01D_MN.r...	2020/03/13 10:43	RNX ファイル	7,234 KB	衛星軌道情報(過去)
RTCM3EPH.rtc	2020/03/13 10:55	RTCM ファイル	38 KB	
run_limeGNSS_auto.bat	2019/06/17 10:11	Windows バッチ ファ...	1 KB	
run_limeGNSS_nmea.bat	2020/03/12 17:29	Windows バッチ ファ...	1 KB	実行ファイル ・移動シナリオ用 ・静止点シナリオ用
run_limeGNSS_static.bat	2020/03/12 18:44	Windows バッチ ファ...	1 KB	
LimeGNSS.exe	2020/03/12 17:41	アプリケーション	52 KB	

## 6. 衛星軌道情報の準備

最初に衛星軌道情報をインターネットからダウンロードする必要があります。

### ◆過去の軌道情報

1. スプーフィングさせたい日のDay of Yearを以下のサイト等で調べます。  
<http://navigationservices.agi.com/GNSSWeb/>

2020年3月11日は  
**2020/071**となります。

**GPS Date Calendar**

This calendar presents dates specific to the GPS community. The data for each day are as follows:

Row	Example	Definition
First	1	Calendar day of the month
Second	1485.2	Full GPS week since 1st epoch : day of week number
Third	462:172800	GPS Week since latest epoch : seconds of week at midnight for that day
Fourth	183	Julian Day Number

March 2020

February	March 2020	April				
Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
2095:0 47:0 61	2095:1 47:86400 62	2095:2 47:172800 63	2095:3 47:259200 64	2095:4 47:345600 65	2095:5 47:432000 66	2095:6 47:518400 67
8	9	10	11	12	13	14
2096:0 48:0 68	2096:1 48:86400 69	2096:2 48:172800 70	2096:3 48:259200 71	2096:4 48:345600 72	2096:5 48:432000 73	2096:6 48:518400 74
15	16	17	18	19	20	21
2097:0 49:0 75	2097:1 49:86400 76	2097:2 49:172800 77	2097:3 49:259200 78	2097:4 49:345600 79	2097:5 49:432000 80	2097:6 49:518400 81
22	23	24	25	26	27	28
2098:0 50:0 82	2098:1 50:86400 83	2098:2 50:172800 84	2098:3 50:259200 85	2098:4 50:345600 86	2098:5 50:432000 87	2098:6 50:518400 88
29	30	31				
2099:0 51:0 89	2099:1 51:86400 90	2099:2 51:172800 91				

## 6. 衛星軌道情報の準備

### ◆過去の軌道情報

2. IGSのFTPサイトから欲しい日の軌道情報をダウンロードします。

<ftp://igs.ensg.ign.fr/pub/igs/data/>

ファイルの詳細説明: <https://kb.igs.org/hc/en-us/articles/115003935351-Access-to-Products>

1.で調べたDay of Yearのフォルダから  
"BRDC00IGS..."というファイルをLimeGNSSフォルダ  
にダウンロードします。

ftp://igs.ensg.ign.fr/pub/igs/data/2020/071/ の一覧

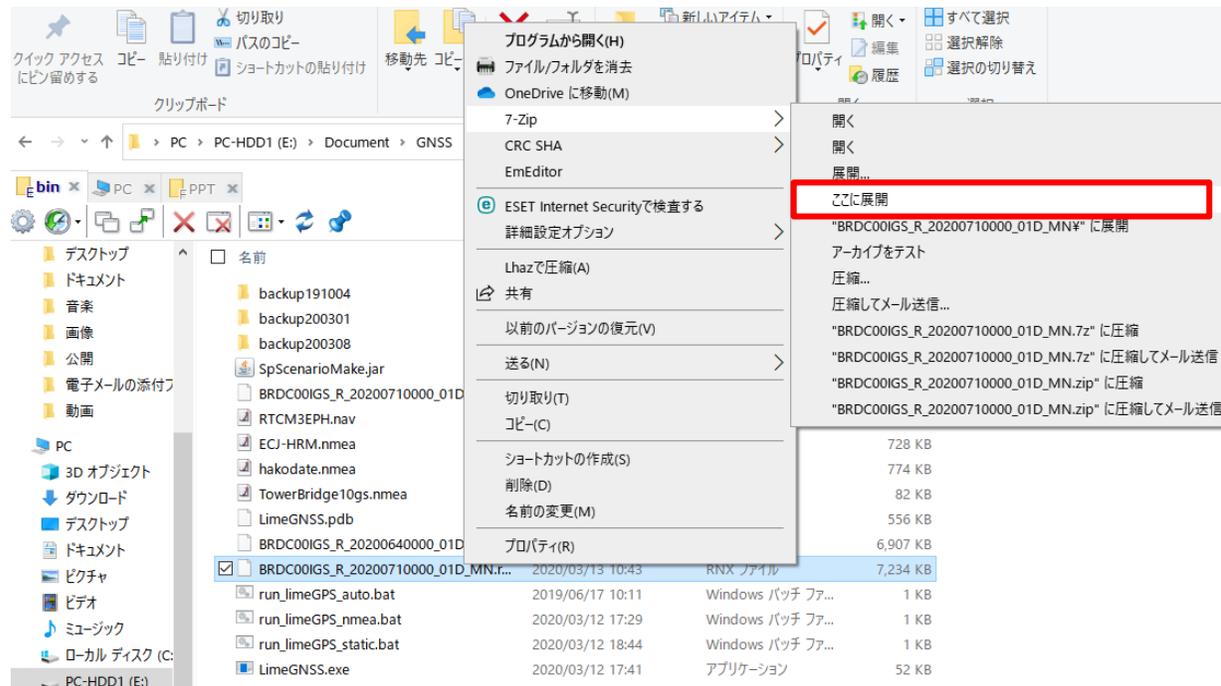
↑ 上位のディレクトリへ移動

名前	サイズ	最終更新日時
ファイル: 20071.V3status	44 KB	2020/03/13 10:22:00
ファイル: 20071.status	77 KB	2020/03/13 10:22:00
20d		2020/03/12 7:08:00
20f		2020/03/12 7:08:00
20g		2020/03/12 7:08:00
20h		2020/03/12 7:08:00
20i		2020/03/12 7:08:00
20l		2020/03/12 7:08:00
20m		2020/03/12 7:08:00
20n		2020/03/12 7:08:00
...		
...		
...		
ファイル: BOR100POL_R_20200710000_01D_SN.rnx.gz	25 KB	2020/03/12 10:26:00
ファイル: BRAZ00BRA_R_20200710000_01D_30S_MO.crx.gz	1862 KB	2020/03/13 2:14:00
ファイル: BRAZ00BRA_R_20200710000_01D_30S_MO.crx.sum.gz	3 KB	2020/03/13 2:09:00
ファイル: BRDC00IGS_R_20200710000_01D_MN.rnx.gz	879 KB	2020/03/13 2:18:00
ファイル: BRDM00DLR_S_20200710000_01D_MN.rnx.gz	1075 KB	2020/03/12 13:13:00

## 6. 衛星軌道情報の準備

### ◆過去の軌道情報

3. .gzで圧縮されているので解凍します。  
Windowsの標準ソフトでは解凍ができないため7-zipなどの解凍ソフトを利用します。
4. “BRDC...rnx”という軌道情報のファイルが生成されます。



## 6. 衛星軌道情報の準備

### ◆現在の軌道情報

現在時刻でスプーフィングさせたい場合はアシストGPSの軌道情報を利用します。

1. RTKLIBをダウンロードします。  
<http://www.rtklib.com/>



#### Download

Version	Date	Binary AP Package for Windows	Full Package with Source Programs
0.2.0	2006/12/16	-	<a href="#">rtklib_0.2.0.zip</a> (2.8MB)
1.0.0	2007/01/25	-	<a href="#">rtklib_1.0.0.zip</a> (10.5MB)
1.1.0	2007/03/20	-	<a href="#">rtklib_1.1.0.zip</a> (6.2MB)
2.1.0	2008/07/15	-	<a href="#">rtklib_2.1.0.zip</a> (22.9MB)
2.2.0	2009/01/31	<a href="#">rtklib_2.2.0_bin.zip</a> (10.7MB)	<a href="#">rtklib_2.2.0.zip</a> (23.4MB)
2.2.1	2009/05/17	<a href="#">rtklib_2.2.1_bin.zip</a> (15.3MB)	<a href="#">rtklib_2.2.1.zip</a> (30.6MB)
2.2.2	2009/09/07	<a href="#">rtklib_2.2.2_bin.zip</a> (21.4MB)	<a href="#">rtklib_2.2.2.zip</a> (33.8MB)
2.3.0	2009/12/17	<a href="#">rtklib_2.3.0_bin.zip</a> (26.7MB)	<a href="#">rtklib_2.3.0.zip</a> (35.8MB)
2.4.0	2010/08/08	<a href="#">rtklib_2.4.0_bin.zip</a> (17.4MB)	<a href="#">rtklib_2.4.0.zip</a> (26.5MB)
2.4.1	2011/06/11	<a href="#">rtklib_2.4.1_bin.zip</a> (16.5MB)	<a href="#">rtklib_2.4.1.zip</a> (26.4MB)
2.4.2	2013/04/29	<a href="#">rtklib_2.4.2_bin.zip</a> (30.4MB)	<a href="#">rtklib_2.4.2.zip</a> (55.2MB)

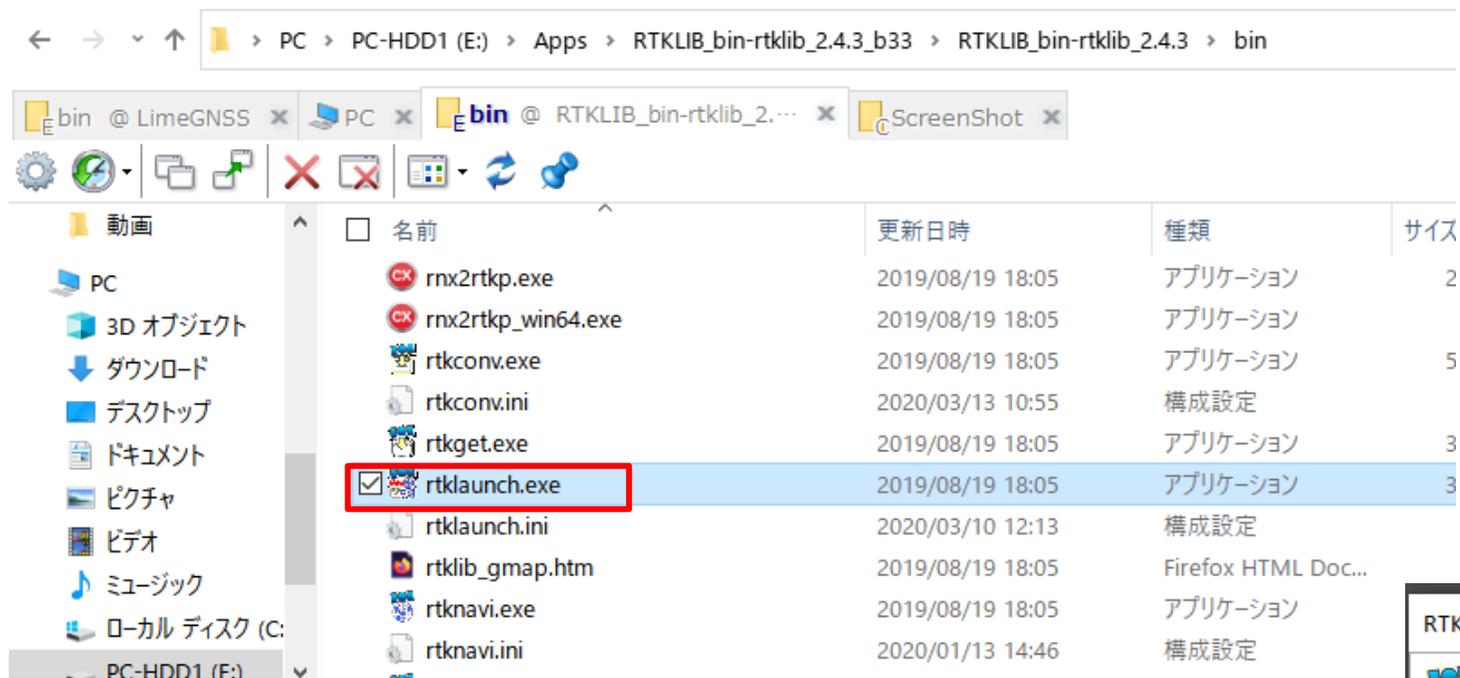
These are just old archives for recording. To download of the newest version, please visit the following GitHub links.

Version	Date	Binary APs for Windows	Source Programs and Data
2.4.2 p13	2018/01/29	<a href="#">GitHub</a>	<a href="#">GitHub</a>
2.4.3 b33	2019/08/19	<a href="#">GitHub</a>	<a href="#">GitHub</a>

## 6. 衛星軌道情報の準備

### ◆現在の軌道情報

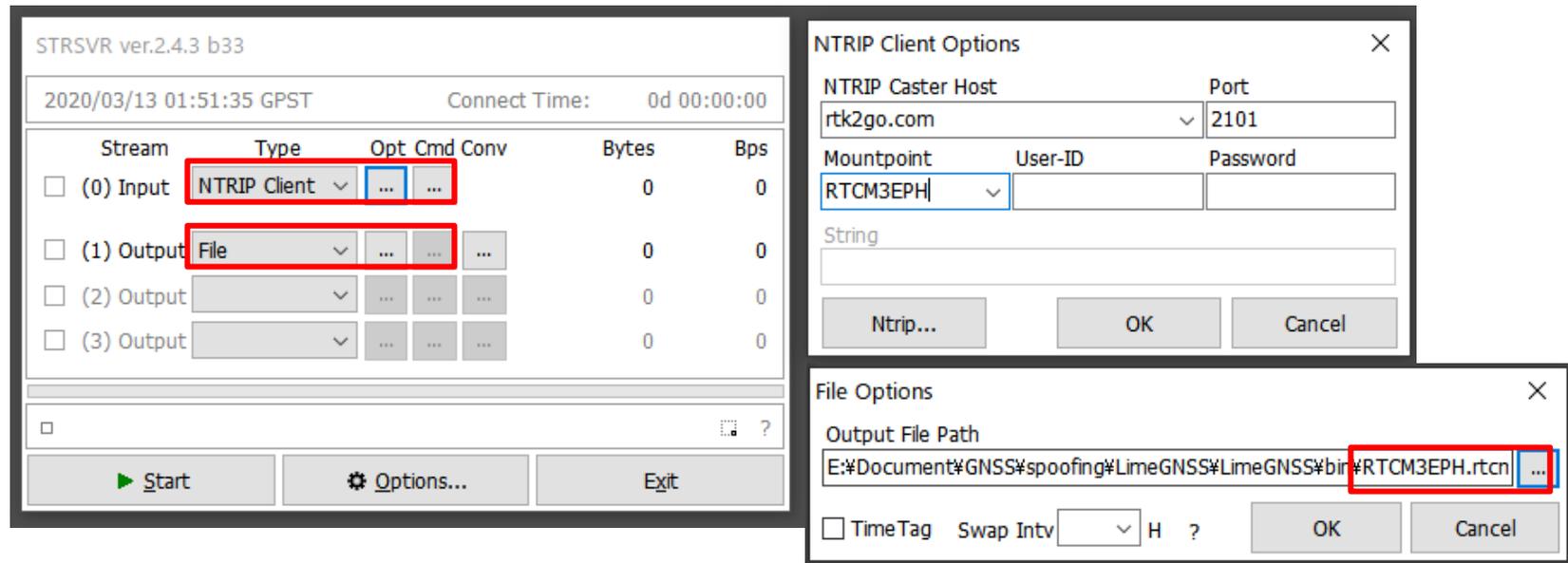
2. Binフォルダからrtklaunch.exeを起動し、STRSVRを起動します。



## 6. 衛星軌道情報の準備

### ◆現在の軌道情報

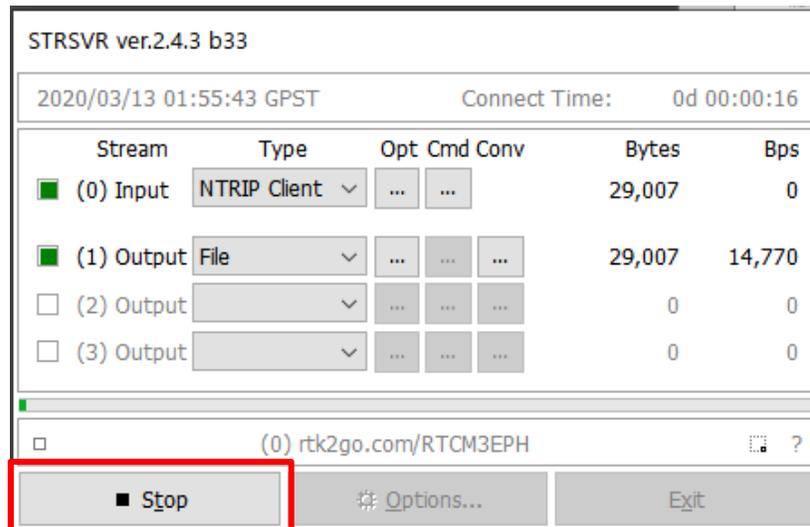
- Inputでrtk2go.comというサーバーを選択します。アシストGPS軌道情報のマウントポイントはRTCM3EPHとなります。(現在GPSのみ配信)  
登録が必要ですがmgex.igs-ip.netというサーバーのRTCM3EPH-MGEXも使用可能です。(こちらはQZSSも対応)  
登録:<https://register.rtcn-ntrip.org/cgi-bin/registration.cgi>
- Outputはファイルを選択してLimeGNSSのフォルダに保存します。



## 6. 衛星軌道情報の準備

### ◆現在の軌道情報

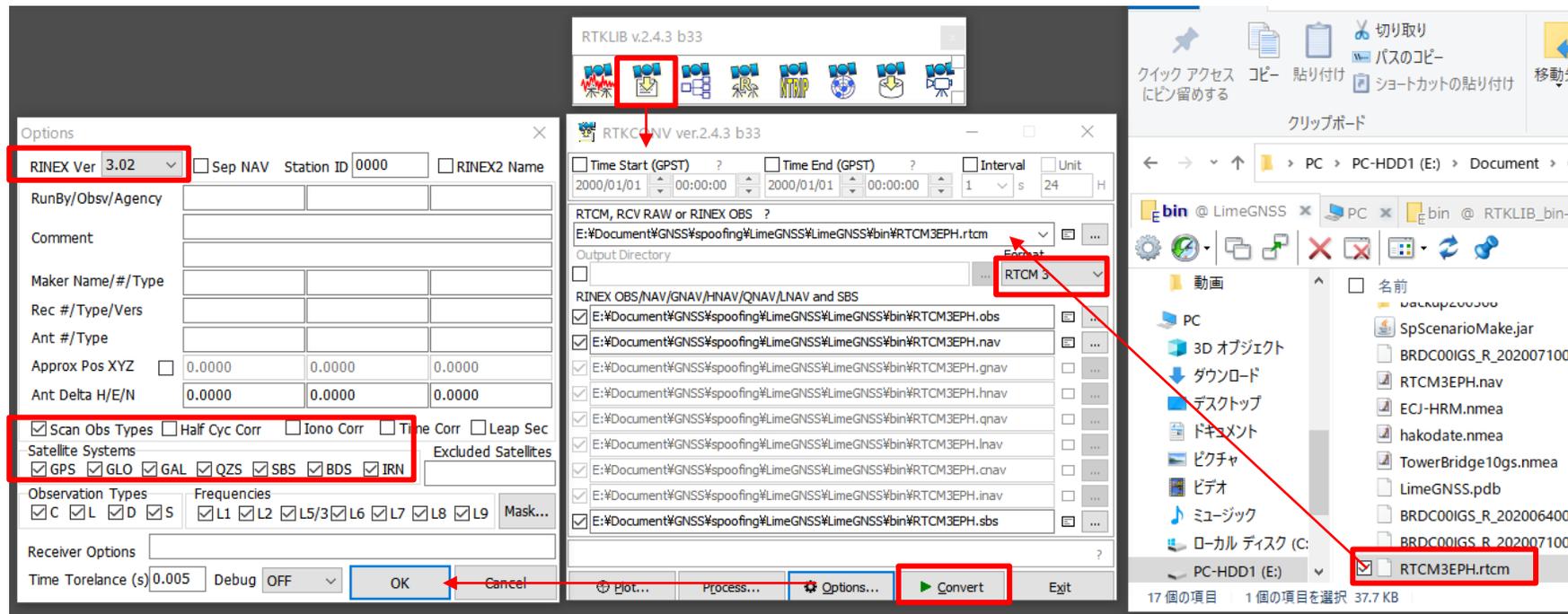
5. “Start”をクリックして30秒ほどしたら“Stop”でダウンロードを終了します。



## 6. 衛星軌道情報の準備

### ◆現在の軌道情報

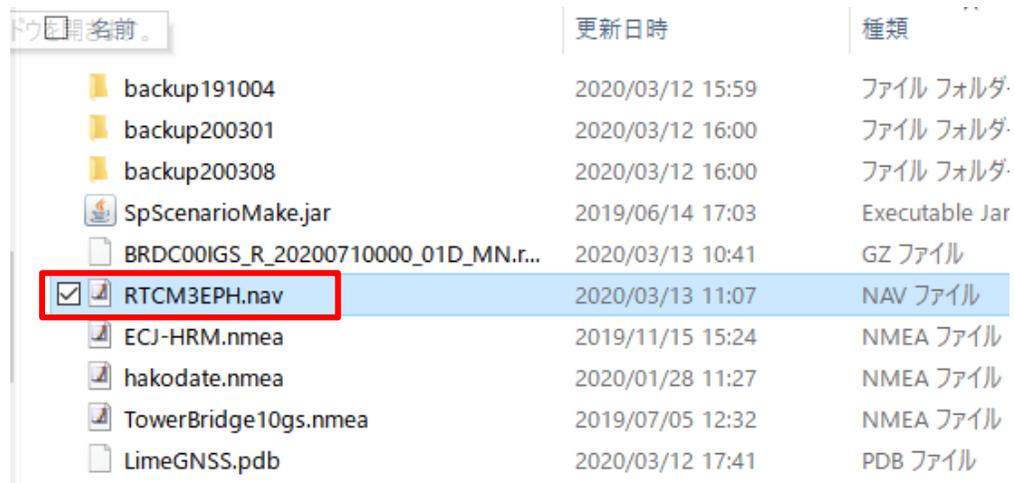
6. RTKCONVを開きます。
7. Optionを以下のように設定します。
8. ダウンロードしたファイル(ここではRTCM3EPH.rtcn)を一番上の行にドラッグアンドドロップして"Convert"をクリックします。



## 6. 衛星軌道情報の準備

### ◆現在の軌道情報

9. LimeGNSSフォルダに“RTCM3EPH.nav”という軌道情報のファイルが出力されます。



名前	更新日時	種類
backup191004	2020/03/12 15:59	ファイル フォルダ
backup200301	2020/03/12 16:00	ファイル フォルダ
backup200308	2020/03/12 16:00	ファイル フォルダ
SpScenarioMake.jar	2019/06/14 17:03	Executable Jar
BRDC00IGS_R_20200710000_01D_MN.r...	2020/03/13 10:41	GZ ファイル
<input checked="" type="checkbox"/> RTCM3EPH.nav	2020/03/13 11:07	NAV ファイル
ECJ-HRM.nmea	2019/11/15 15:24	NMEA ファイル
hakodate.nmea	2020/01/28 11:27	NMEA ファイル
TowerBridge10gs.nmea	2019/07/05 12:32	NMEA ファイル
LimeGNSS.pdb	2020/03/12 17:41	PDB ファイル

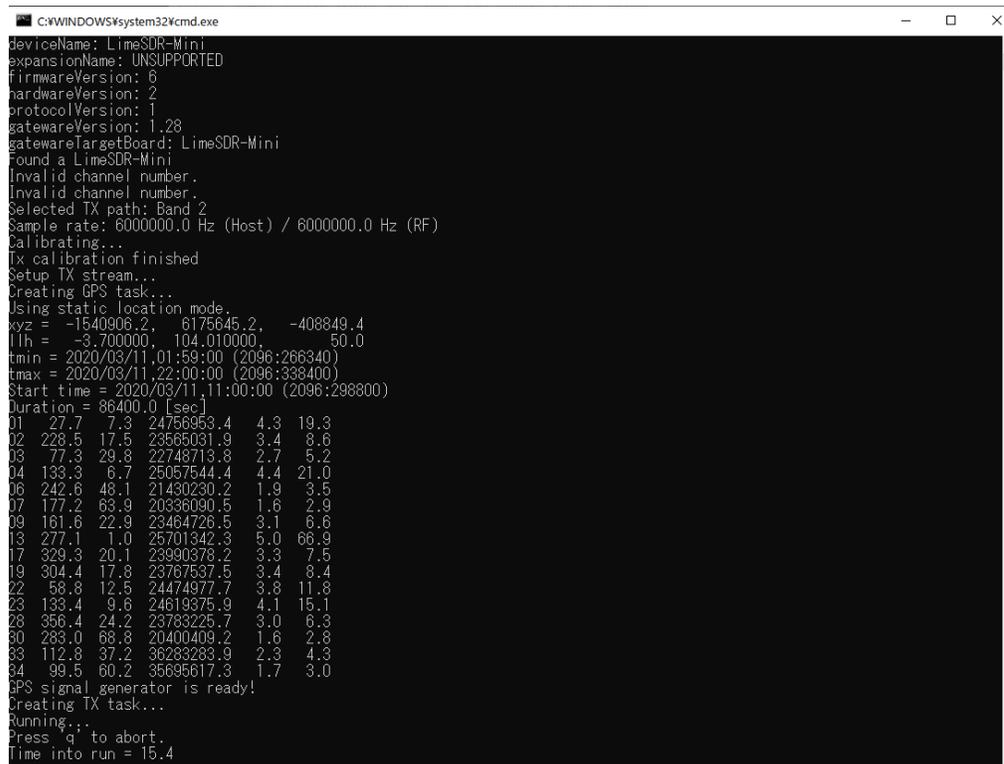
## 7. 静止点のスプーフィング

1. “run\_limeGNSS\_static.bat”というファイルを右クリック等でテキストエディターで開きます。
2. 軌道情報ファイル、緯度・経度・高さ(楕円体高)、時刻、出力を入力します。
  - ・軌道情報ファイル: “BRDC...rnx”または“RTCM3EPH.nav”
  - ・時刻: yyyy/mm/dd, hh:mm:ssフォーマット。 年を1960年以下にすると現在時刻でのスプーフィングになります。
  - ・出力: 0.3~1の範囲。屋内、5m範囲であれば0.3で十分です。
3. @remを行頭につけることでコメント扱いになります。
4. 変更後ファイルを保存します。

```
1 LimeGNSS.exe -e BRDC00IGS_R_20200710000_01D_MN.rnx -l -3.70,104.01,50 -t 2020/03/11,11:00:00 -a 0.3↓
2 @rem niru -3.444510886,104.041214891,46.562↓
3 @rem ECJ-East 35.666515095,139.792395898,59.4354↓
4 ←
```

## 7. 静止点のスプーフィング

5. LimeSDRをUSBでPCに接続します。
6. “run\_limeGNSS\_static.bat”をダブルクリックすると以下のようなウィンドウが開かれスプーフィングが開始されます。

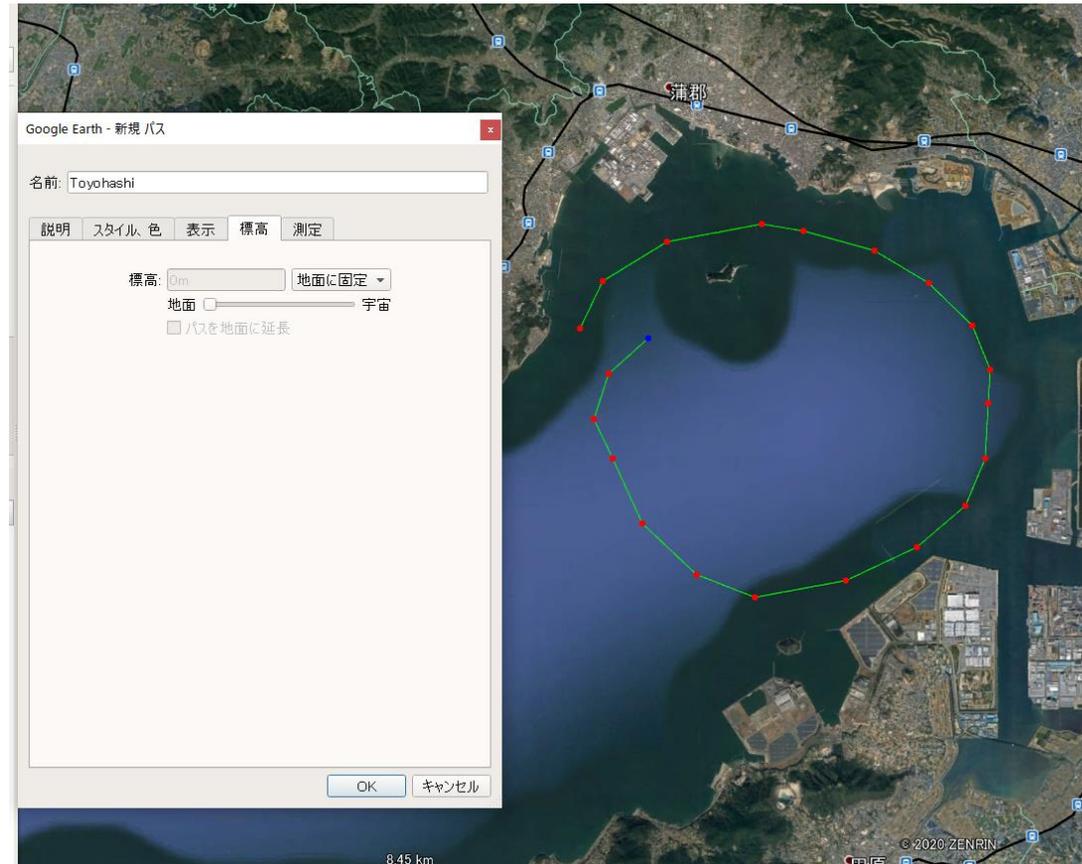


```
C:\WINDOWS\system32\cmd.exe
deviceName: LimeSDR-Mini
expansionName: UNSUPPORTED
firmwareVersion: 6
hardwareVersion: 2
protocolVersion: 1
gatewayVersion: 1.28
gatewayTargetBoard: LimeSDR-Mini
Found a LimeSDR-Mini
Invalid channel number.
Invalid channel number.
Selected TX path: Band 2
Sample rate: 6000000.0 Hz (Host) / 6000000.0 Hz (RF)
Calibrating...
TX calibration finished
Setup TX stream...
Creating GPS task...
Using static location mode.
xyz = -1540906.2, 6175645.2, -408849.4
llh = -3.700000, 104.010000, 50.0
tmin = 2020/03/11,01:59:00 (2096:266340)
tmax = 2020/03/11,22:00:00 (2096:338400)
Start time = 2020/03/11,11:00:00 (2096:298800)
Duration = 86400.0 [sec]
01 27.7 7.3 24758953.4 4.3 19.3
02 228.5 17.5 23565081.9 3.4 8.6
03 77.3 29.8 22748713.8 2.7 5.2
04 133.3 6.7 25057544.4 4.4 21.0
06 242.6 48.1 21430230.2 1.9 3.5
07 177.2 63.9 20336090.5 1.6 2.9
09 161.6 22.9 23464726.5 3.1 6.6
13 277.1 1.0 25701342.3 5.0 66.9
17 329.3 20.1 23990378.2 3.3 7.5
19 304.4 17.8 23767537.5 3.4 8.4
22 58.8 12.5 24474977.7 3.8 11.8
23 133.4 9.6 24619375.9 4.1 15.1
28 356.4 24.2 23783225.7 3.0 6.3
30 283.0 68.8 20400409.2 1.6 2.8
33 112.8 37.2 38283283.9 2.3 4.3
34 99.5 60.2 35695617.3 1.7 3.0
GPS signal generator is ready!
Creating TX task...
Running...
Press 'q' to abort.
Time into run = 15.4
```

## 8. 移動シナリオのスーパーフィング

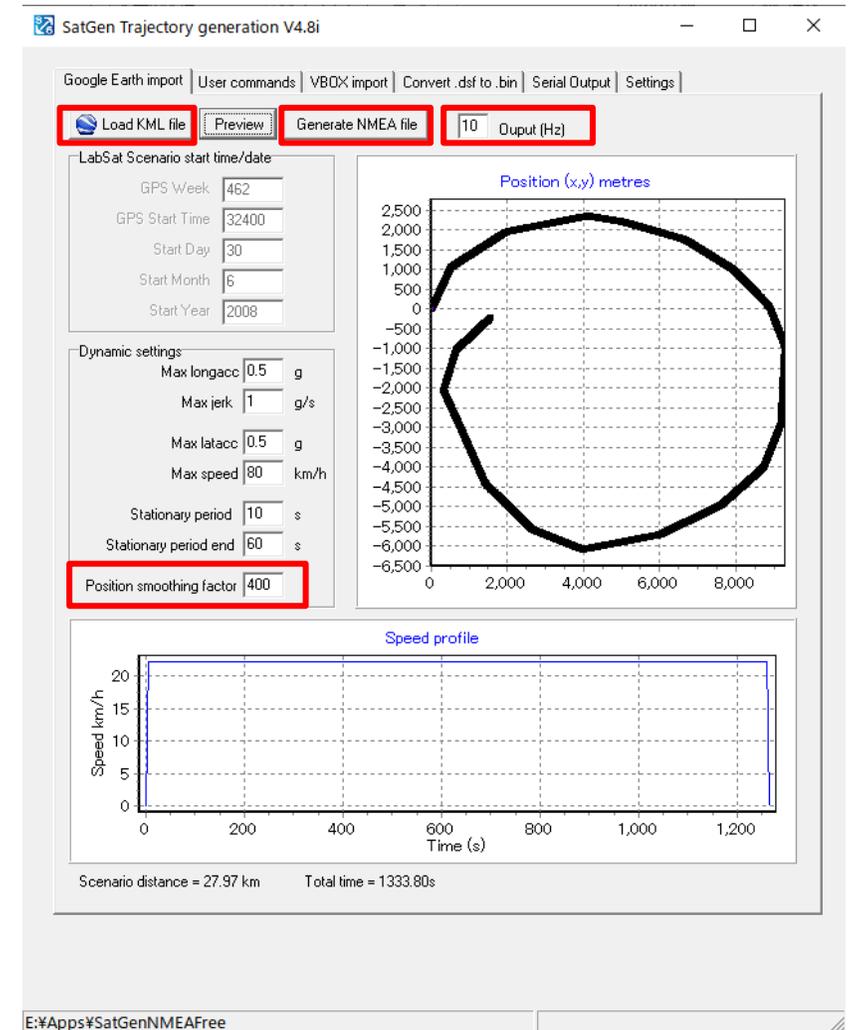
あらかじめ用意した軌跡ファイルに従ってスーパーフィングを行います。

1. Google Earthでパスを描きます。
2. パスを.kmlで保存します。



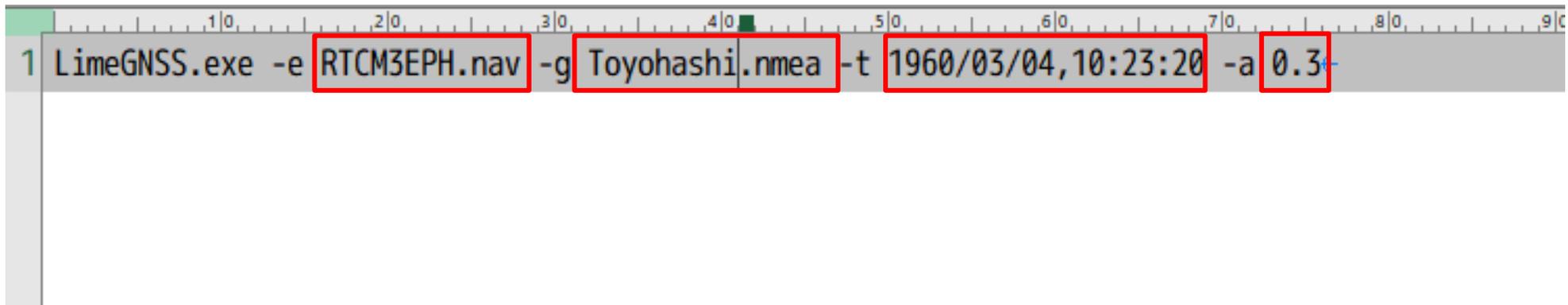
## 8. 移動シナリオのスプーフィング

3. “SatGen NMEA”というフリーソフトをダウンロード・インストールします。  
<https://www.labsat.co.uk/index.php/en/free-gps-nmea-simulator-software>
4. “Load KML file”から作成したパスのkmlファイルを開きます。
5. 速度や加速度を設定します。“Preview”で設定がグラフに反映されます。パスのポイントで減速しないようにするには“smoothing factor”を300~400に設定してください。
6. “output”を10Hzにして“Generate NMEA file”でNMEAファイルをLimeGNSSフォルダに保存します。



## 8. 移動シナリオのスプーフィング

7. "run\_limeGNSS\_nmea.bat"というファイルを右クリック等でテキストエディターで開きます。
8. 軌道情報ファイル、作成したNMEAファイル、時刻、出力を入力します。
  - ・軌道情報ファイル："BRDC...rnx"または"RTCM3EPH.nav"
  - ・時刻：yyyy/mm/dd, hh:mm:ssフォーマット。 年を1960年以下にすると現在時刻でのスプーフィングになります。
  - ・出力：0.3~1の範囲。屋内、5m範囲であれば0.3で十分です。
9. @remを行頭につけることでコメント扱いになります。
10. 変更後ファイルを保存します。



```
1 LimeGNSS.exe -e RTCM3EPH.nav -g Toyohashi.nmea -t 1960/03/04,10:23:20 -a 0.3
```

## 8. 移動シナリオのスプーフィング

5. LimeSDRをUSBでPCに接続します。
6. “run\_limeGNSS\_nmea.bat”をダブルクリックすると以下のようなウィンドウが開かれスプーフィングが開始されます。

```
C:\WINDOWS\system32\cmd.exe
Found a LimeSDR-Mini
Invalid channel number.
Invalid channel number.
Selected TX path: Band 2
Sample rate: 6000000.0 Hz (Host) / 6000000.0 Hz (RF)
Calibrating...
Tx calibration finished
Setup TX stream...
Creating GPS task...
xyz = -3848016.3, 3563605.2, 3617690.7
llh = 40.785092, -73.968285, 10.0
tmin = 2020/03/13,06:00:00 (2096:453600)
tmax = 2020/03/13,06:00:00 (2096:453600)
Start time = 2020/03/13,04:12:21 (2096:447141)
Duration = 1334.1 [sec]
03 270.7 1.9 25622638.1 4.9 53.8
04 313.0 23.9 23346766.8 3.0 6.5
14 183.1 38.4 21976373.7 2.3 4.3
16 277.8 46.9 21240862.0 2.0 3.6
21 107.2 23.4 23327192.0 3.0 6.7
23 314.3 19.2 24030008.4 3.3 8.0
25 68.2 1.2 25684025.4 4.9 65.7
26 325.5 65.5 20564395.4 1.6 2.9
27 205.5 24.4 23118966.2 3.0 6.4
29 43.0 27.3 23009781.1 2.8 5.8
31 73.3 70.8 20606679.2 1.6 2.8
32 170.7 14.8 24087232.0 3.6 10.2
GPS signal generator is ready!
Creating TX task...
Running...
Press 'q' to abort.
Time into run = 7.9popping from TX, samples popped 544/1360
Time into run = 9.0
2020/03/13,04:12:30 (2096:447150)
xyz = -3848016.3, 3563605.2, 3617690.7
```

Title	Count	Age	Current	Minimum	Maximum	Average
UTC	3822	0	04:37:54.80...	04:25:10.60...	04:37:54.80...	
GPS time	3822	0	2096:44869...	2096:44792...	2096:44869...	
ITOW	3822	0	448692.800	447928.600	448692.800	
NAV-HNR IT...	0					
TACC	3822	0	0.003000	0.003000	0.100000	0.003904
TimeStartup	3821	0	881.835	117.830	881.835	499.833
TFFF	0					0.000
TMO rising	0					0.000000000

Map - [MapView\_roadmap\_0.6061251\_2.3958111\_500]

RelPosN: 1.#Q0m  
RelPosE: 1.#Q0m  
RelPosD: 1.#Q0m  
Distance: 1.#Q0m  
AccE: 1.#Q0m  
AccD: 1.#Q0m

Longitude: 137.26982217  
Latitude: 34.72639533  
Altitude: 164.600 m  
Altitude (msl): 128.200 m  
ITFF  
Fix Mode  
3D Acc. [m] 0 1.78  
2D Acc. [m] 0 1.34  
PDOP 0 1.4  
HDOP 0 1.4  
SatellRes 0 10.8

24 tz 都市、国またはタイムゾーン  
現在の時刻 UTC  
UTC  
04:37:55  
金曜日, 3月 13, 2020

22.80 m/s = 82.1 km/h

04:37:55 UTC  
Friday 03/13/2020

NTRIP client: Not connected | u-blox M8/8 | COM4 9600 | No file open | UBX | 00:18:5 | 04:37:55

## 9. 出力電力とスプーフィング可能距離について

アンプ未装着時(実測)

- Gain=0.3: -45dBm
- Gain=0.4: -40dBm
- Gain=0.5: -35dBm
- Gain=0.6: -25dBm
- Gain=0.7: -17dBm
- Gain=0.8: -10dBm
- Gain=0.9: -8dBm
- Gain=1.0: -6dBm

+40dBアンプ装着時

- Gain=0.7: 23dBm

\*アンプが故障するためGainを0.7より大きく設定しないでください。

電波到達距離計算サイト

<https://www.circuitdesign.jp/technical/radio-wave-propagation-characteristics/>

周波数: 1575MHz

アンテナ利得: 送信2dBi、受信3dBi

で受信電力が-100dBm程度の距離がスプーフィング可能な最大距離です。

(環境によってこれより短くなります)