再放射キットをSpooferと想定した場合の検知方法について

東京海洋大学　修士2年　長岡賢吾

目次

- 背景
- Spoofing信号の特徴
- 右旋円偏波と左旋円偏波について
- フロントエンド、SDRによる処理
- 実験概要
- 実験結果
- まとめ

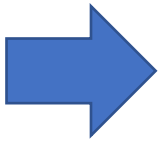
背景

- ソフトウェア受信機
  …衛星信号をAD変換するフロントエンドと
  ソフトウェアによる信号処理、測位演算

- 再放射キット
  …RF信号を取得し全く同じ信号を再送信
  …屋内で衛星信号を取得可能

背景

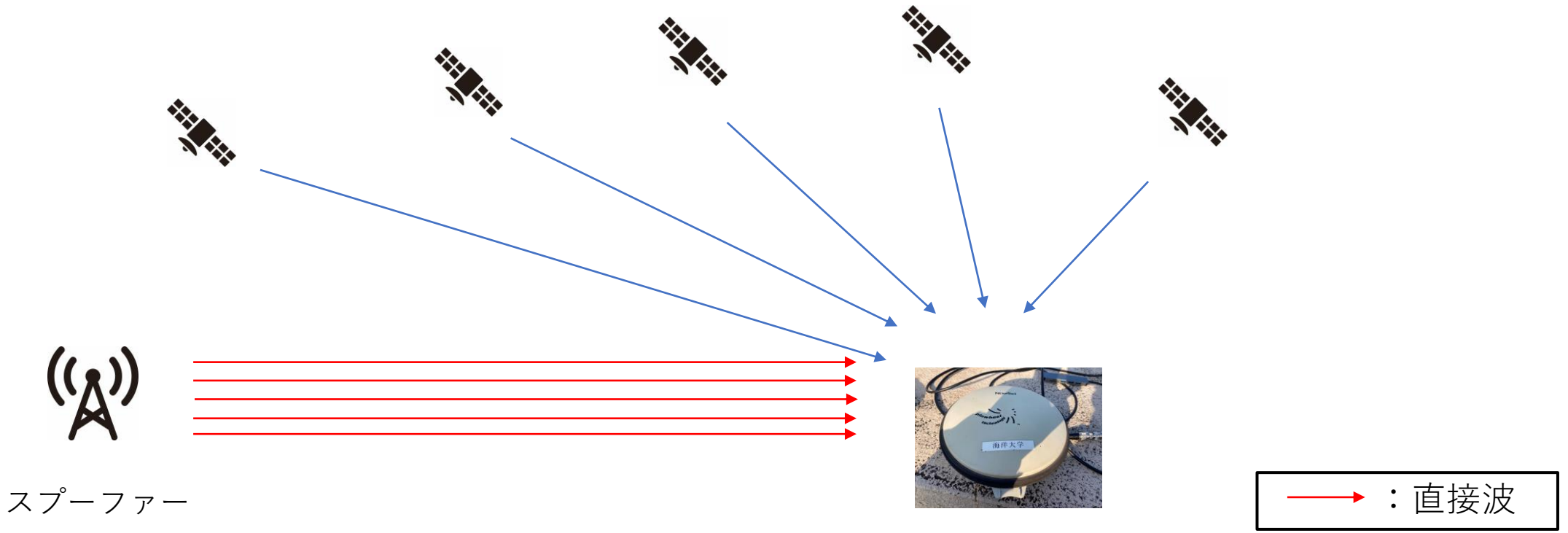
- Spoofing技術とソフトウェア受信機(SDR)の関係
  …SDRによるGNSS信号の人為的な偽造
  …今後脅威を増していくと考えられる



ソフトウェア受信機セミナーで得た知識をもとに、
過去の研究室の先輩が行った研究手法を自身で検証した

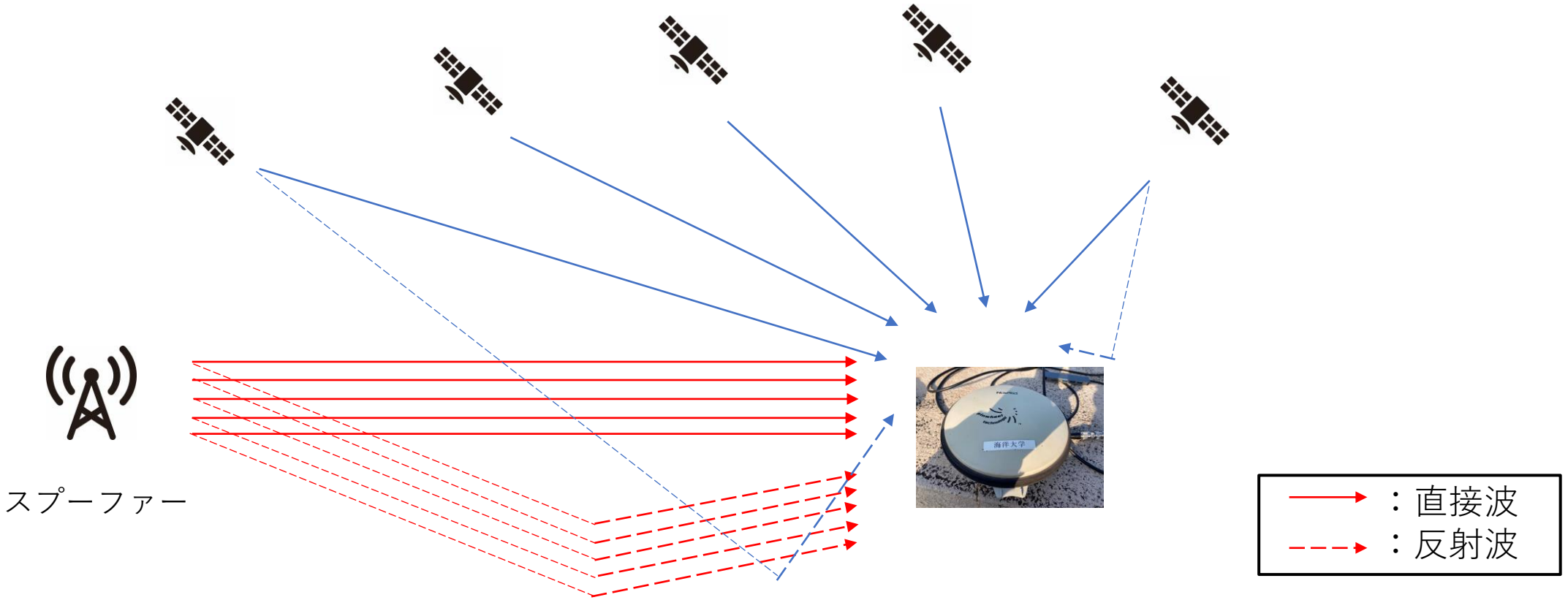
Spoofing信号の特徴

- 実際の衛星からの信号は様々な距離、角度から放射される一方で再放射キットからの信号は同一方向から放射される



Spoofing信号の特徴

- また、反射波についても類似した経路で放射される。



右旋円偏波と左旋円偏波について

- GNSSでは、RHCP(Right Hand Circular Polarization/右旋円偏波)という偏波方式を採用している。
- 一方、受信機側での電磁界は信号の反射により劣化し、LHCP(Left Hand Circular Polarization/左旋円偏波)の成分が発生する。

→　二偏波アンテナで捉える試みが行われてきた

左がLHCPアンテナ、右がRHCPアンテナ

右旋円偏波と左旋円偏波について

- 屋外環境ではリアル衛星の信号仰角がバラバラであるため、アンテナで得られる偏波に差が生じる

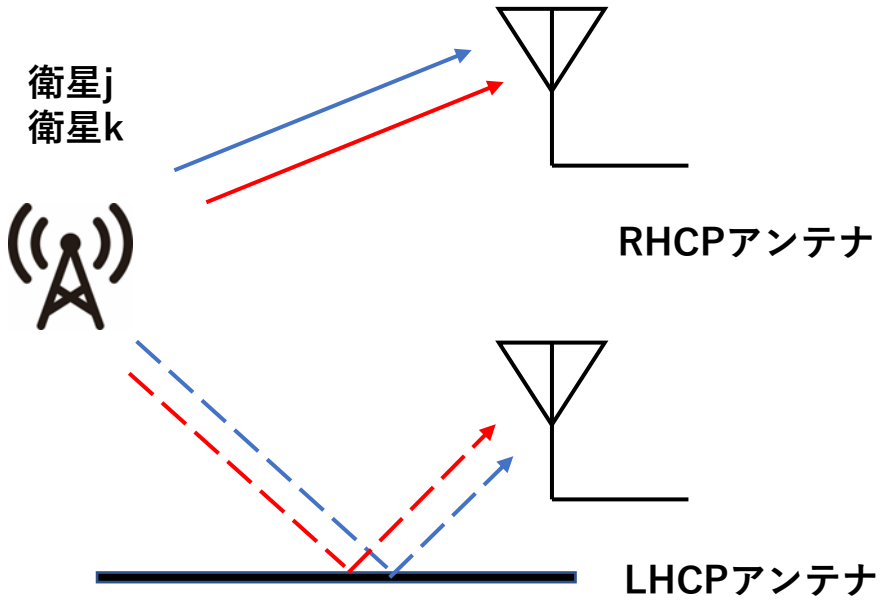
- 一方、Spooferからの信号は仰角が一定であるため、アンテナで得られる偏波は同じものになると予想される。

- RHCPアンテナとLHCPアンテナで同時取得した信号の差を見ることで、Spoofing信号の特徴(偏波方向)を捉える

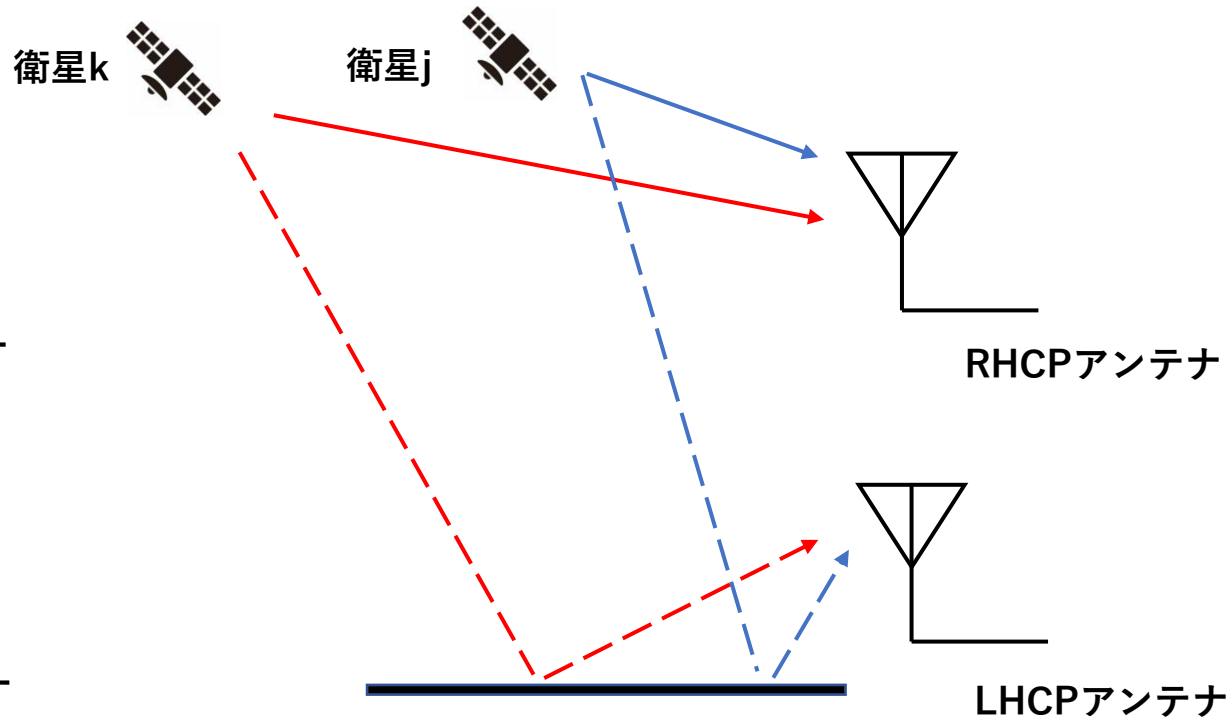
➡ RHCPアンテナのみではわからない、二偏波アンテナの理由

右旋円偏波と左旋円偏波について

- RHCPアンテナとLHCPアンテナでRHCP成分とLHCP成分を取得する



Spoofingの場合



実際の場合

：直接波
：反射波

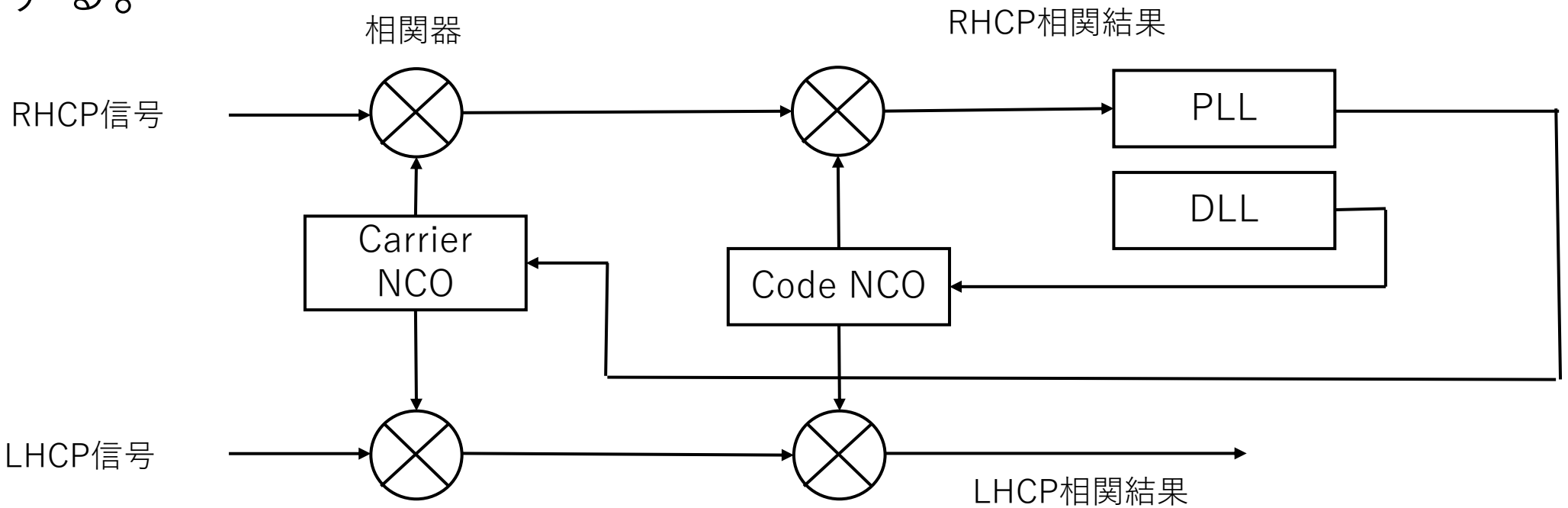
フロントエンド、SDRによる処理

- RHCP、LHCPアンテナで受信された信号は2ch入力のフロントエンドでAD変換される。

名称	メーカー	詳細
RFフロントエンド	IP Solution	中心周波数=1575.42MHz IF=4.092MHz サンプリングレート =16.368MHz 2bit、IQサンプリング 同クロックで信号取得

フロントエンド、SDRによる処理

- ソフトウェア受信機ではまずRHCP信号の信号捕捉、追尾を行う。
- ある衛星の GNSS 信号の 擬似距離コードと相関が取れた場合、相関がとれたポイントの情報を LHCP 信号の相関器に渡して 相関を取ることで同じタイミングにおける反射波の相関値 をＩ相とQ 相で計算する。



フロントエンド、SDRによる処理

- 各衛星のIp値、 Qp値から2つのパラメーターを推定する。
- 2つのパラメータを水平プロットで示す。

$$\frac{R}{L}\text{信号強度比}[dB] = 20 \cdot log10 \cdot \left|\frac{Ip(R) + i \cdot Qp(R)}{Ip(L) + i \cdot Qp(L)}\right|$$

$$\frac{R}{L}\text{コード位相差}[deg] = \arctan(a, b) \quad \left(\left|\frac{Ip(R) + i \cdot Qp(R)}{Ip(L) + i \cdot Qp(L)}\right| = \mathrm{a} + \mathrm{i} \cdot \mathrm{b}\right)$$

Ip: I相相関値　Qp: Q相相関値　(R): 直接波の信号　(L): 反射波の信号

実験概要

- 2022年10月4日、東京海洋大学第四実験棟屋上での信号取得と屋内での再放射キットからの信号取得を行った。
- 2chのRFフロントエンドを用いてL1帯1周波のGNSS信号を取得。
- GNSSソフトウェア受信機でGPS,QZSS,Galileo衛星の信号捕捉、追尾を行った。
- 上記で説明した2つのパラメータを水平プロットし結果を比較する。

実験概要

実験機材

機材	メーカー/型番等	備考
アンテナ	JAVAD	L1,L2帯
RF フロントエンド	IP Solution	中心周波数：1575.42MHz IF：4.092MHz サンプリング：16.368MHz 2bitのIQサンプリング 同クロックで信号取得
SDR GNSS受信機	研究室	GPS L1C/A Galileo E1b QZSS L1C/A
再放射用送信アンテナ	L1/L2GRRKPA-T	L1,L2帯
再放射用アンプ	L1/L2GHNRRKAMP-T/5/110	+30dB
RHCP/LHCPアンテナ	小峰無線	L1帯
リファレンス用受信機	ublox F9P	L1帯マルチGNSS

実験概要

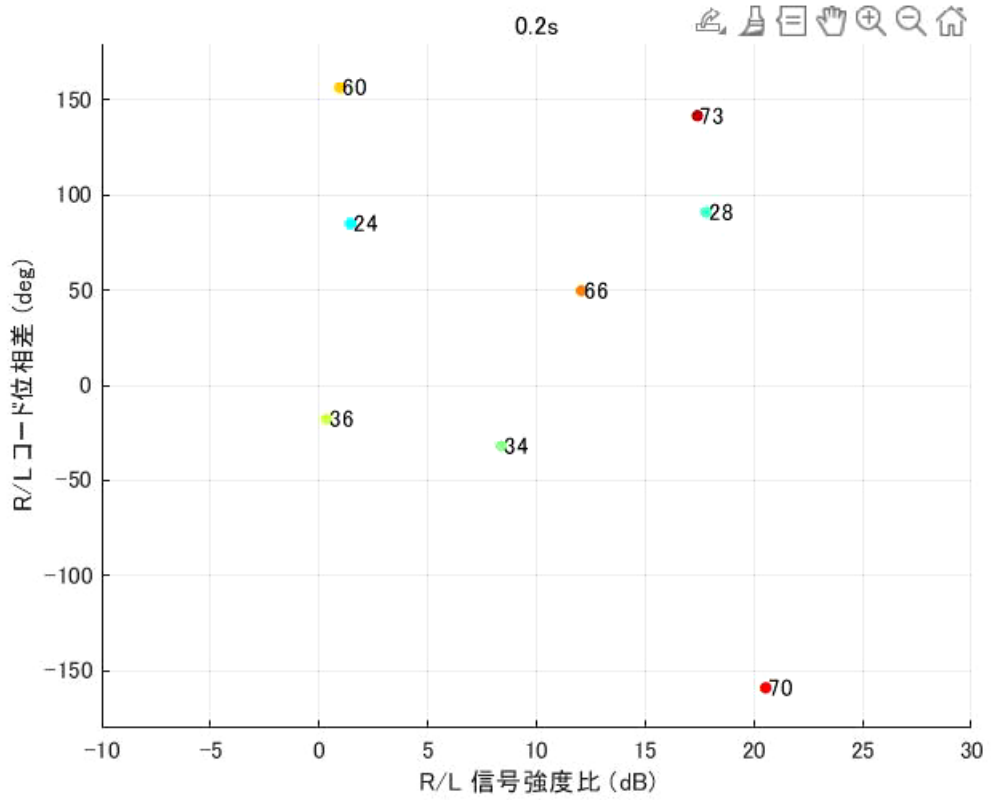
屋上での実験の様子

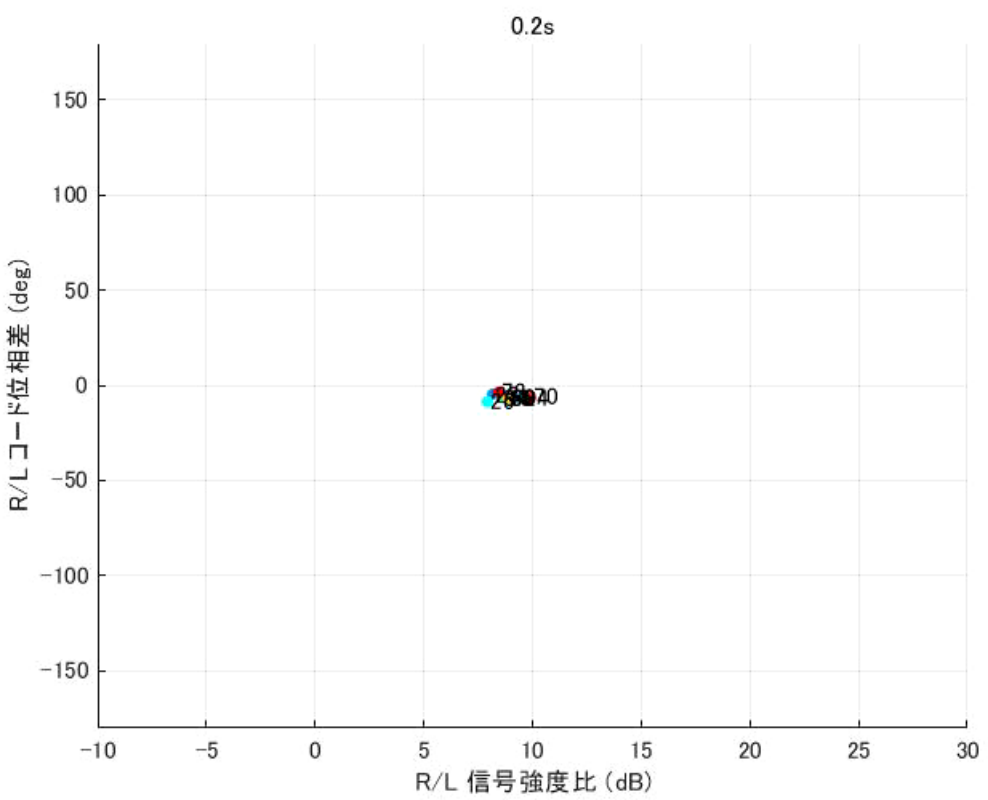
屋内での実験の様子

再放射キット

実験結果

- 左が屋上データの結果、右が屋内データの結果である





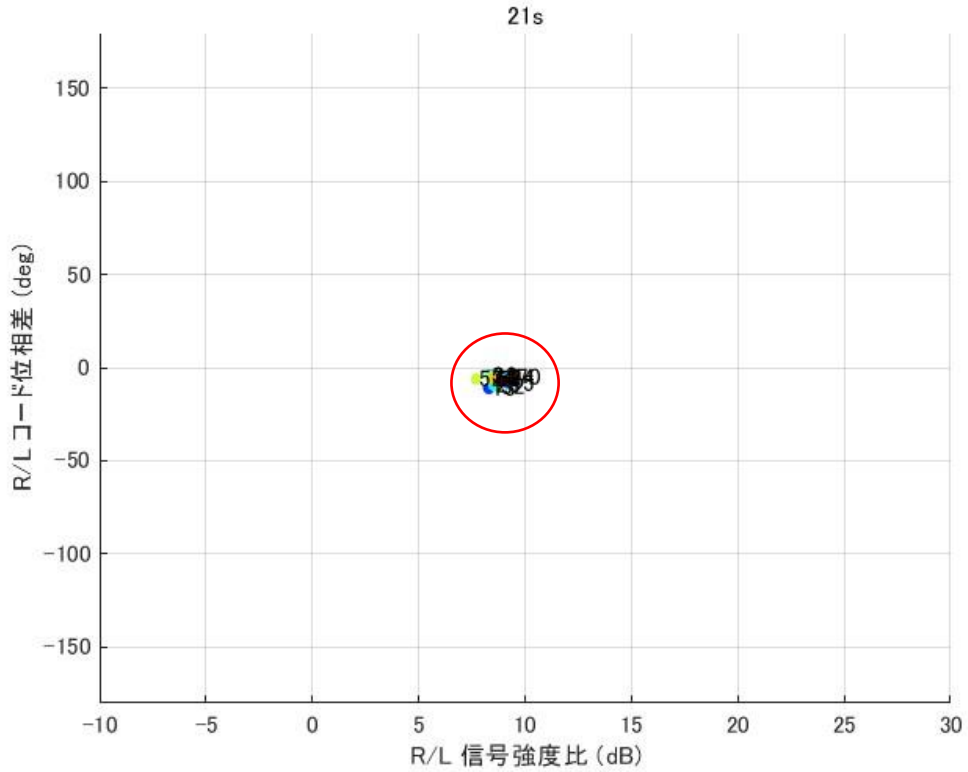
(1~32：GPS　　33~36：QZSS　　41~76：Galileo)

実験結果

- 屋上データはパラメータが散らばるのに対し、屋内Spoofingのデータは点群が形成される様子がわかる

- PLLを参照し(PLL≧0.90)、追尾できていない衛星を除いた

- 200msで各信号のI値,Q値を積分した



水平プロットのワンショット

まとめ

- Spoofing 信号における反射波のパラメーターに類似性が生じることに着目し、水平プロット図の点群形成により Spoofing 検知の評価を行った。
- 屋内 Spoofing 信号の水平プロット結果より、Spoofing 信号の性質を確認した。

- 屋内 Spoofingにより本物の衛星信号を排除した環境で実験した
- 屋外でのSpoofingで本物の信号もクラスターを形成する可能性が考えられるため今後の課題とする