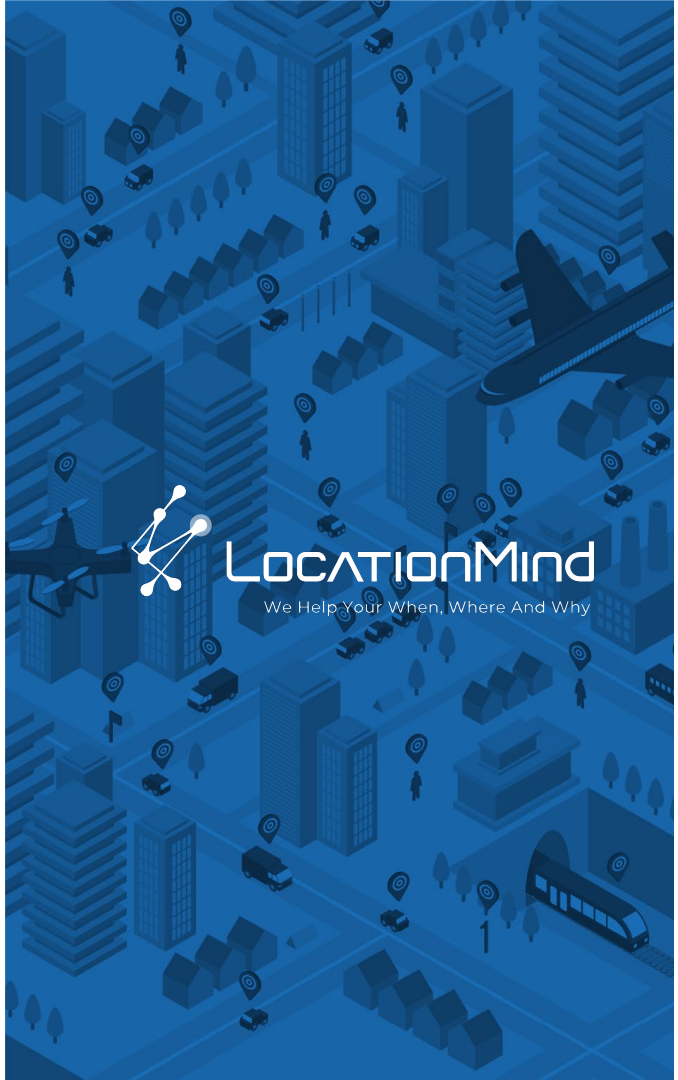
2025.9.18 第3回SBIC標準化WG

LocationMind株式会社の信号認証技術について

～日本の衛星測位の安心・安全を目指しての諸活動のご報告～

2025.9.18
LocationMind㈱
R&D Division
Senior Project Manager &
Chief PNT Strategist
千野孝一



目次

LocationMind

1. はじめに（自己紹介）

- 千野孝一
- 東京工業大学　電気電子工学科卒
- 日立製作所にてGPSの研究開発
- 東京大学・空間情報科学研究センターの研究員を兼務
- LocationMind㈱　R&D Divisionにて後進の育成を兼ねて現役中
- Senior Project Manager &
  Chief PNT Strategist
- ISO TC20 SC14 WG8 Expert

２．　LocationMind㈱とは

LocationMind at a Glance

Company	
Name	LocationMind
Founded	2019 February 4th
Employees	85名
Group (100%)	AdvertisementMind - Irys / pinable

Foundation

東京大学 THE UNIVERSITY OF TOKYO

CSIS 東京大学 空間情報科学研究センター

SeriesB

5bn JPY

Aug 2024

Board of Directors

N.Kiritani
CEO
Goldman Sachs
Angel Bridge

R.Ogawa
CFO
SMBC
SMBC NIKKO

T.Fujita
COO
BCG

Managers

R.Shibsaki
CTO
東京大学
柴崎研究室

Dinesh M.
CDO
東京大学

Y.Usuba
CPO
IBM Google
RECRUIT

1

LocationMind

位置情報の Deep Tech ベンチャー

Our Vision

“世界最強の位置情報企業になる”

#AI #宇宙 #ビッグデータ #分析能力 #社会的意義 #成長 #収益力
#Text to Mobility #PDP #xPop #Authentication #PNT

2025のスローガン: “トップ企業としてのExcellence”

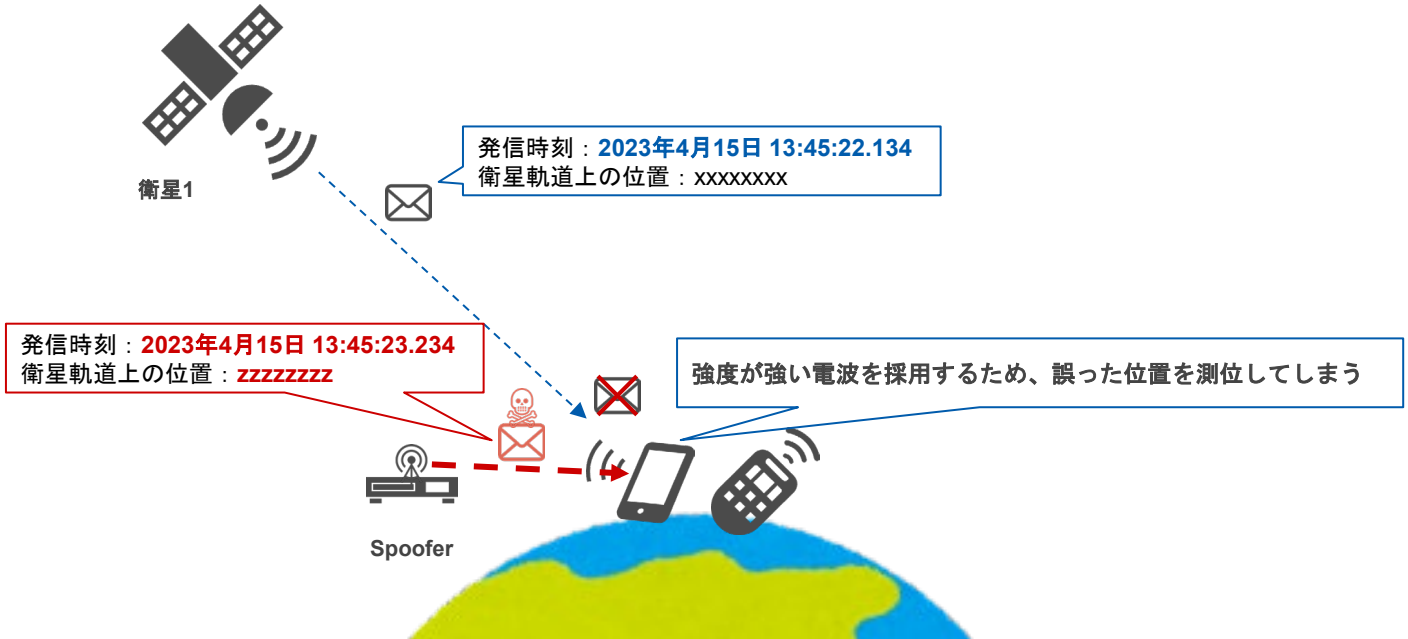
LocationMind 公式Facebook
https://www.facebook.com/locationmind

LocationMind 公式noteアカウント
https://note.com/locationmind/

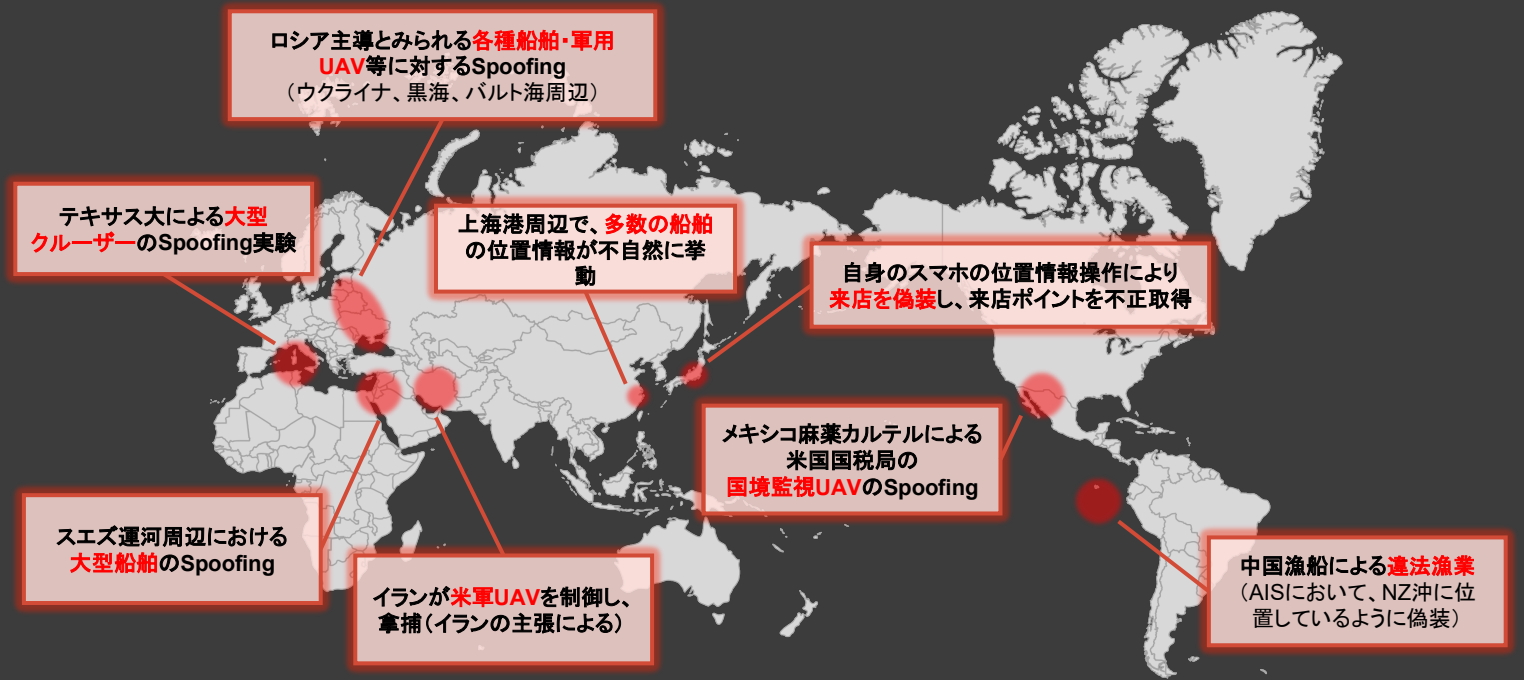
GNSSのリスク - Spoofingとは

GNSS衛星から送信される電波の仕様は公開されており、誰でも再現可能。
この様な技術を**Spoofing**、模倣電波を発するデバイスを**Spoofer**と呼ぶ。

本物の衛星と同じような電波を送出できるためSpoofingの検出は困難。



Spoofing事例：世界各地の特徴的な事案



https://www.gpsworld.com/european-agency-warns-of-gnss-outages-near-ukraine/?utm_source=Navigate%21+Weekly+GNSS+News&utm_medium=Newsletter&utm_campaign=NCMCD220316002&oly_enc_id=7021B4690290E2R https://www.linkedin.com/pulse/thousands-gnss-jamming-spoofing-incidents-reported-2020-guy-buesnel/ https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

Spoofing - 時刻情報の偽装

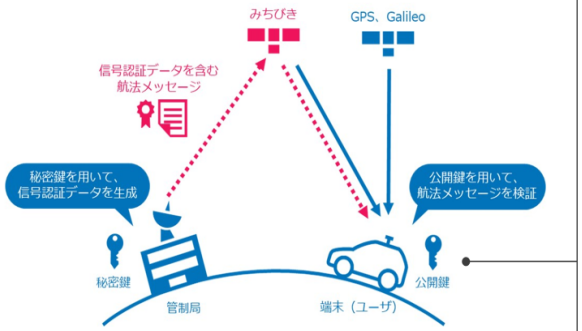
３．信号認証技術とはWhat is Signal Authentication Technology

Spoofing対策：信号認証技術

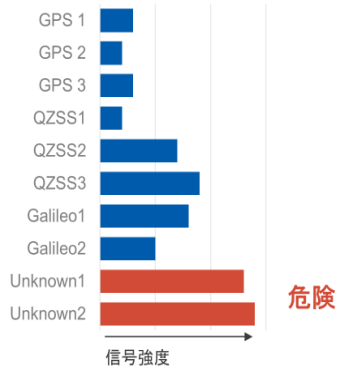
18

Spoofing対策として、みちびきに実装が進んでいる信号認証技術（弊社特許）を活用。

信号認証サービスのイメージ



GNSS信号受信のイメージ



- 仕様がICDで公開されているNAV Message
- 暗号技術
- 秘密鍵／公開鍵技術
- 電子透かし技術
- を適用して
- 位置情報の脆弱性にセキュリティを付与し
- 位置の安全を担保する技術

Source: 内閣府HP

LocationMind

３．信号認証技術とはWhat is Signal Authentication Technology

- 日本国　特許第５４００５２９（登録2013年11月1日）
- 筆頭発明者：千野孝一、共著：柴崎亮介、Dinesh Manandhar
- [秘匿された暗号コードを利用した位置情報認証方法および位置情報認証システム]
- 出願番号：特願２００９－１８７０５８
- 出願日：２００９年８月１２日
- 公開番号：特開２０１１－４１０３８
- 公開日：２０１１年２月２４日

３．信号認証技術とはWhat is Signal Authentication Technology

■　技術分野：本発明は衛星測位分野、空間情報分野、ナビゲーション、ロケーションベースサービス分野、暗号化セキュリティ通信分野、受信端末開発分野等における位置情報認証技術に関するものである。

■　背景技術：従来の位置情報は屋外では主としてＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ：全地球測位システム）を利用してＧＰＳ受信端末によりＧＰＳナビゲーションメッセージ信号から経度緯度情報を計算により算出していた。この場合ＧＰＳの位置情報は正確であり、信憑性に足る情報として扱われていた。しかしながら、近年ＧＰＳの信号を複製するＧＰＳリピータ、ＧＰＳの振る舞いを擬似的に生成できるＧＰＳシミュレータの開発により、悪意の行為者による位置情報の改竄、他者へのなりすましという問題が発生する危険性がある。

■　解決課題：第一の課題は、ＧＰＳから受信した位置情報自体は性善説に基づき正しい位置情報であることを前提として、悪意の行為者や機関によるこれら位置情報の改竄、なりすましによる障害を未然に防止することである。

　第二の課題は、ＧＰＳリピータ、シミュレータ等により改竄された位置情報と改竄されない位置情報を暗黙に自動的に識別する方法を提供することである。

　第三の課題は、自然現象による影響（メッセージ信号の電離層遅延、対流圏遅延等）に関する対象地域の特徴が含まれていないデータを偽とみなす方法を提供することである。

　第四の課題は、既存の全地球測位システムとローカル測位システムの現状の運用にスムーズに接続可能な信頼性のあるシステムを提供することである。

LocationMind

３．信号認証技術とはWhat is Signal Authentication Technology

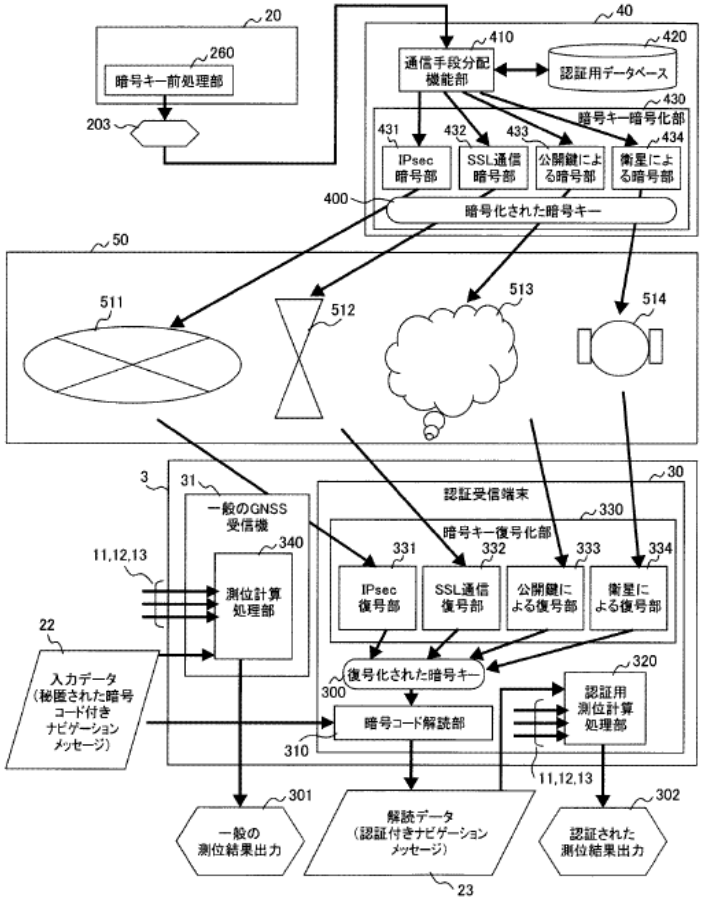
□ 目的：斯かる位置情報の信憑性の現況に鑑み、改竄防止、なりすまし対策を具備した位置情報認証方法、位置情報認証システム及び位置情報認証装置を提供することにある。また、本発明の目的は、上記位置情報認証方法、位置情報認証システム、及び位置情報認証装置を認証権限所有機関で運用することで、安心で安全な空間情報社会を提供することにある。

□ 効果：全地球測位システムと、地上セグメントと宇宙セグメント及び秘匿された暗号コードを解読可能なユーザセグメントを有するローカル測位システムを用いてユーザセグメントの位置情報を決定する位置情報認証システムにおいて、秘匿された暗号コードを有するナビゲーションメッセージを含む位置情報をローカル測位システムの前記宇宙セグメントから前記ユーザセグメントに送信し、秘匿された暗号コードを有するナビゲーションメッセージを用いてユーザセグメントの位置情報を決定することにより、全地球測位システムから送信された位置情報データの信憑性を担保して、改竄防止、なりすまし対策を具備した、安全で信頼性の高い位置情報認証方法およびシステムを提供する事が出来る。

３．信号認証技術とはWhat is Signal Authentication Technology

- [位置測位計算]：
- [秘匿された暗号コード]：
- [ナビゲーションメッセージの認証]
- [暗号キーの発生]
- [秘匿された暗号コードの生成]
- [暗号キーの送信]
- [認証受信端末での位置認証]
- [暗号キー・暗号コード生成アルゴリズム]
- [暗号キーの送付ステップ]
- [認証用データベース]
- [改竄情報の識別]
- [自然現象による影響]

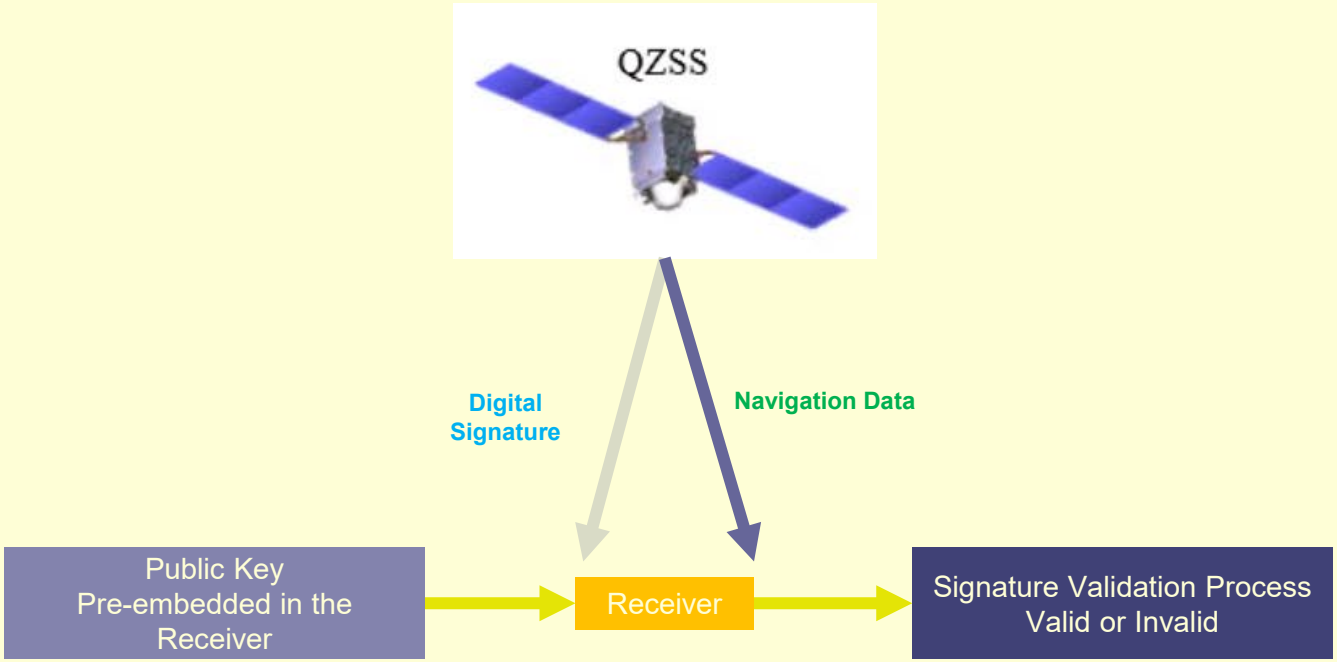
【図５】本発明位置情報認証システムの暗号キー送付方法を示すシステムブロック図



- ２０：秘匿された暗号コード及び暗号キー発生部
- ３０：認証受信端末
- ４０：認証権限所有機関
- ５０：通信媒体
- ５１４：衛星(QZSS & LEO)
- ５１３：インターネットベース(WiFi)
- ５１２：通信施設
- ５１１：インターネットベース(NetBase)

LocationMind

4. 衛星ベースの信号認証
: QZSS-based Signal authentication



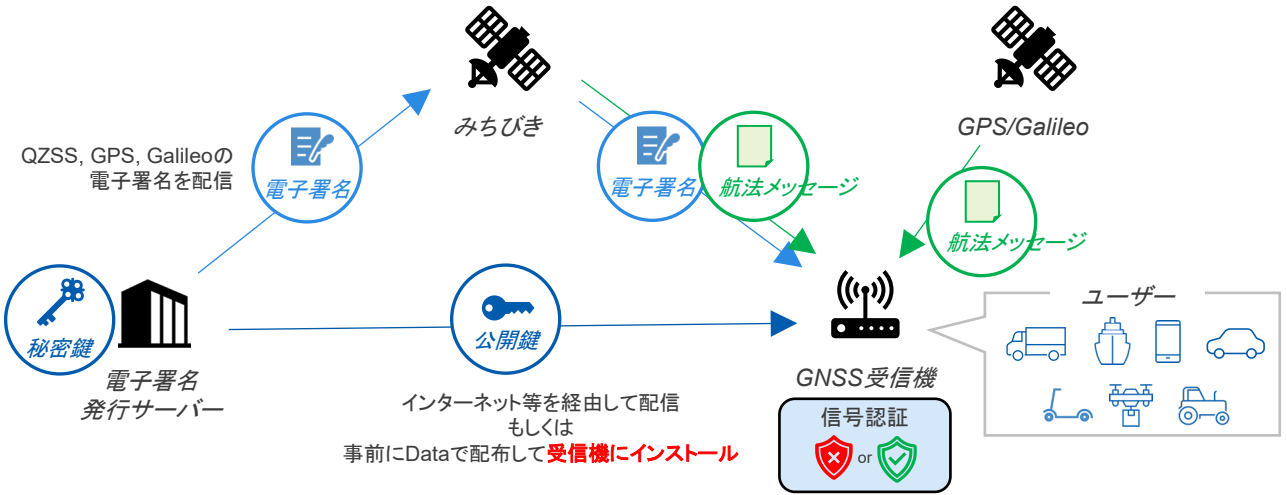
Signature verification process within the receiver
Or a device connected to the receiver in real-time

4. 1. The Status of Competitor (Galileo , GPS , BDS , (QZSS))

- Galileo : OSNMA (Open Service Navigation Message Authentication)
  - Walker, P., et al.: Galileo open service authentication: a complete service design and provision analysis. In: ION GNSS+ 2015, pp. 3383–3396
- GPS : Chimera (Chips-message robust authentication) for GPS civilian signals.
  - Anderson, M., et In: Proceedings of the 30th International Technical Meeting of the Satellite Division of the Institute of Navigation (IONGNSS+ 2017), pp. 2388–2416, Portland (2017). https://doi.org/10.33012/2017.15206
- BDS : RFC-SPA（Randomly Flipped Chip-based Signal Power Authentication）
  - Muzi, Y., et al.: Randomly Flipped Chip based signal power authentication for GNSS civilian signals. IET Radar Sonar Navig. 1–17 (2022). https://doi.org/10.1049/rsn2.12341
- QZSS : SAS (Signal Authentication System)
  - Chino, K., Manandhar, D., Shibasaki, R.: Authentication Technology using QZSS. In: Proceedings of IEEE/ION PLANS 2014, pp. 367–372, Monterey (2014)

衛星ベース信号認証

- 電子署名を秘密鍵を用いて生成し、みちびき衛星から航法メッセージで配信
- ユーザーは、予め入手した公開鍵を用いて、受信した電子署名と航法メッセージを検証することにより、測位信号の真正を確認



信号認証対応GNSS受信機

■ ビズステーション株式会社（以下、BS社）と信号認証対応GNSS受信機を開発

項目	内容	備考
信号認証対象 GNSSシステム	QZSS, GPS, Galileo	• QZSSは、2024年1月以降の試験配信にて評価予定
信号認証対象 航法メッセージ	QZSS, GPS: LNAV Galileo: I/NAV	• CNAVはL2にて検証実施（F9PがL5非対応のため） • F/NAV（E5a）は、BS社のRZSシリーズ（Septentrio Mosaic）で認証可能
GNSS受信機	BS社製 CLAS対応受信機 RWS.DC（u-blox F9P）	• 既存プロダクトに信号認証機能を追加実装
アンテナ	3周波 L1/L2/L6, E1/E5b対応	• GPSLX09U8Wなど

アンテナ

受信機
RWS.DC

既存F/W

RWS.DCに搭載の基本機能
・単独/SBAS/SLAS/CLAS/RTK測位
・DMP、Bluetooth/Wi-Fi
・デバイス制御
etc.

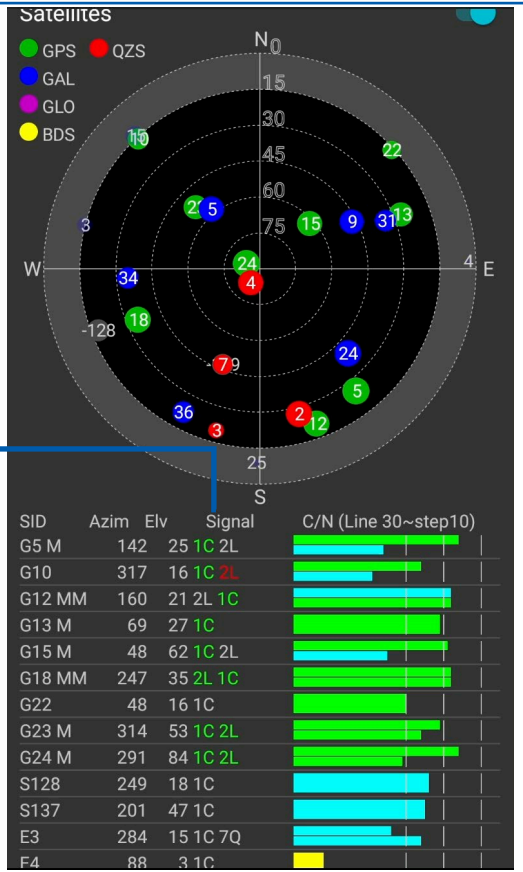
追加F/W

信号認証機能
・QZSS認証処理
・GPS / Galileo認証処理

https://www.bizstation.jp/ja/drogger/package_index.html?tab=rwp#RWS_DC
https://www.bizstation.jp/ja/drogger/package_index.html?tab=rwp#GPSLX09U8W

信号認証対応GNSS受信機

- ビズステーション株式会社の Drogger GPS アプリにて、信号認証状態の確認が可能
- NMEA出力に、各衛星の信号認証ステータス出力を追加

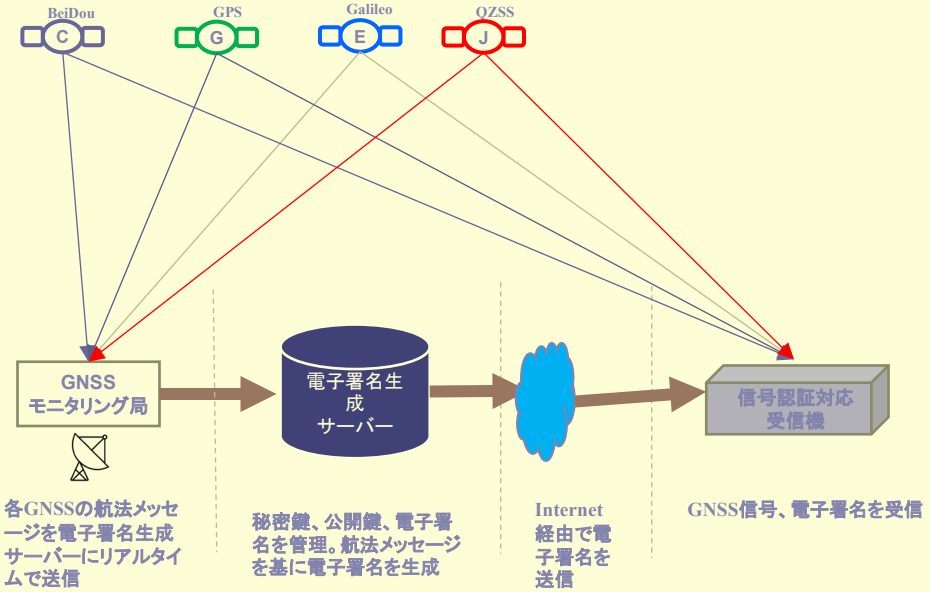


Signal (受信している衛星信号）に、認証状態を表示

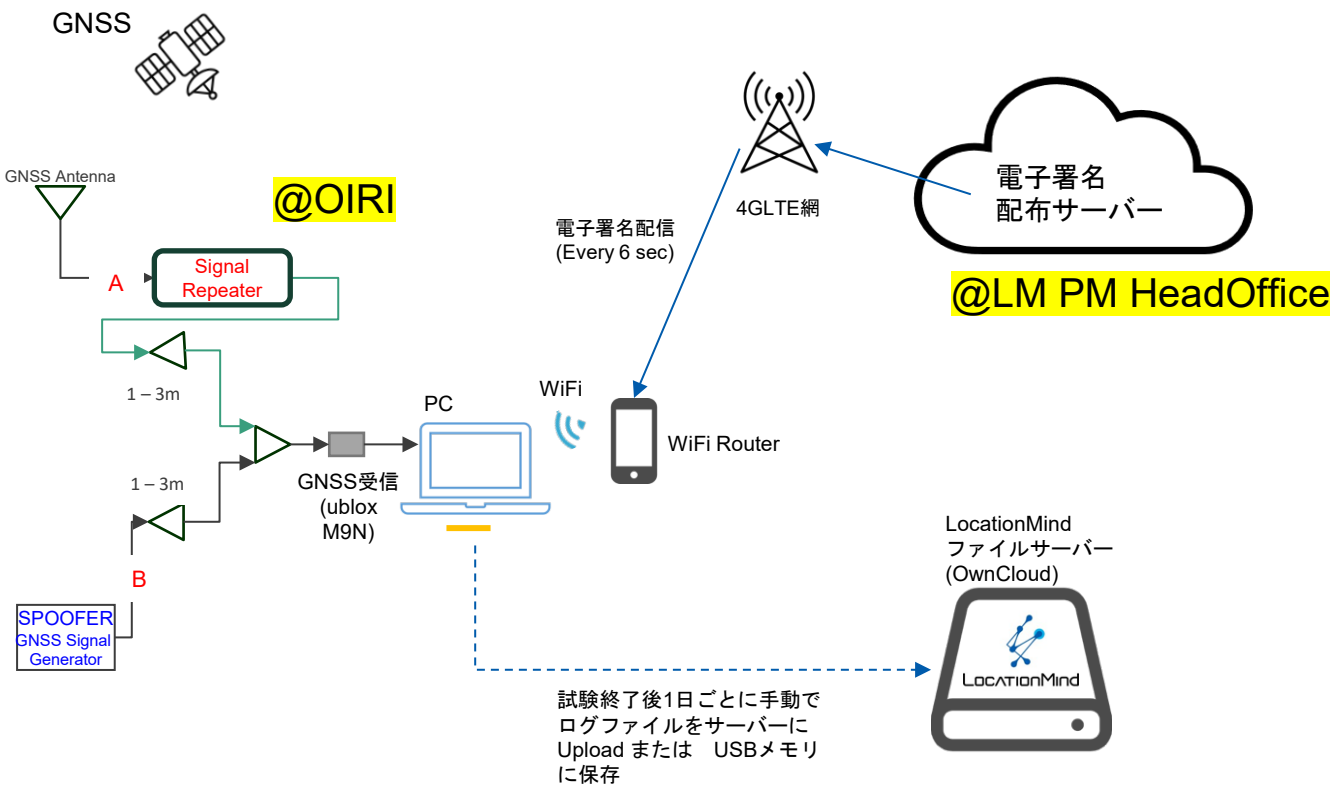
緑：信号認証成功
赤 ： 信号認証失敗
白：未検証

https://play.google.com/store/apps/details?id=jp.bizstation.drgps&hl=ja&gl=US
https://drogger.hatenadiary.jp/entry/drogger-gps_app_guide

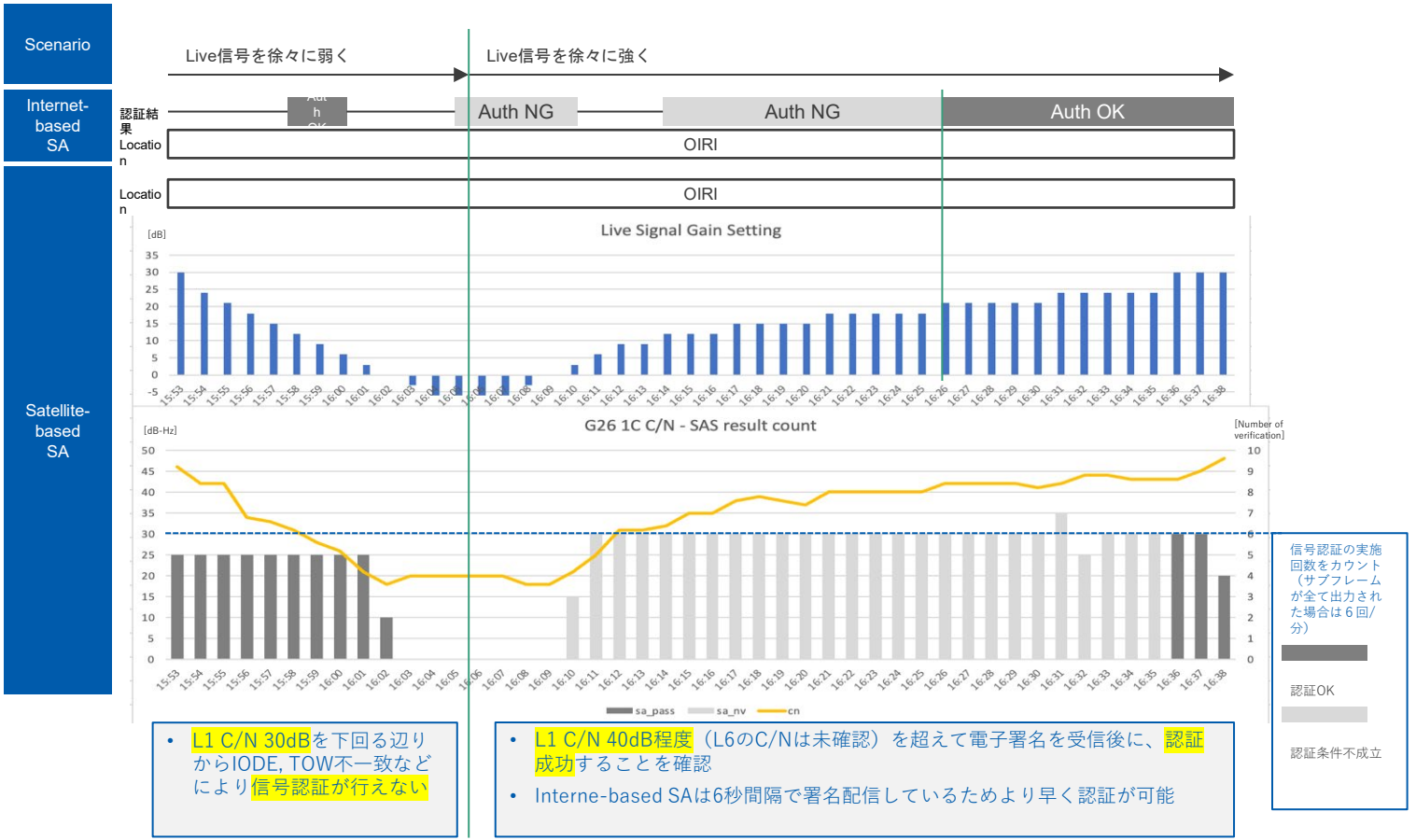
5．：インターネットベースの信号認証



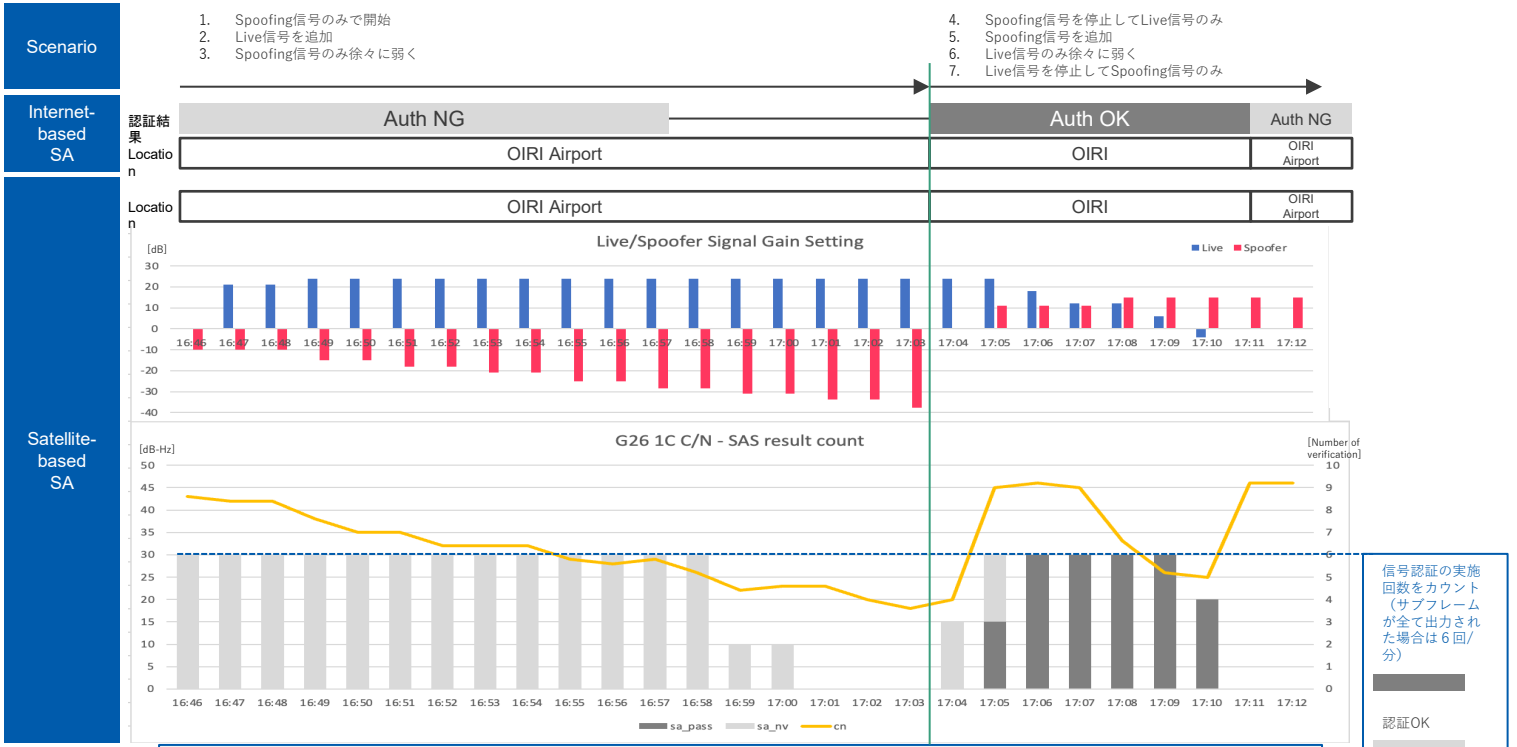
【概要】 Case_Study_1: Internet-based Signal Authenticator



【実験結果】Case Study 3: GPS26 1C - Live Signal w/o Spoofer



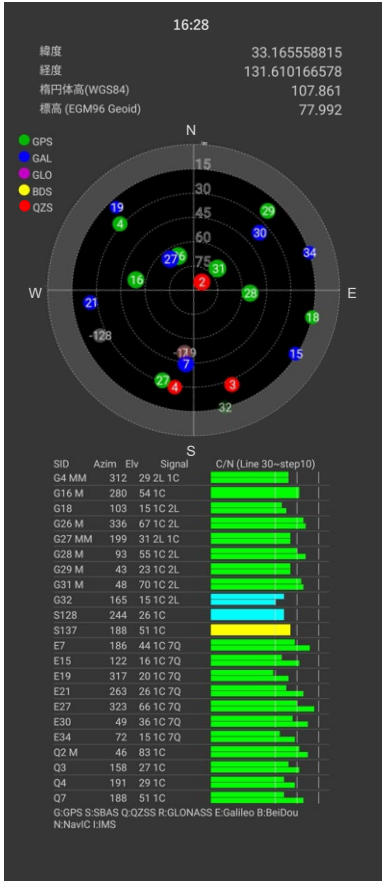
【実験結果】Case Study 3: GPS26 1C - Spoofer/Live to Mixed-mode



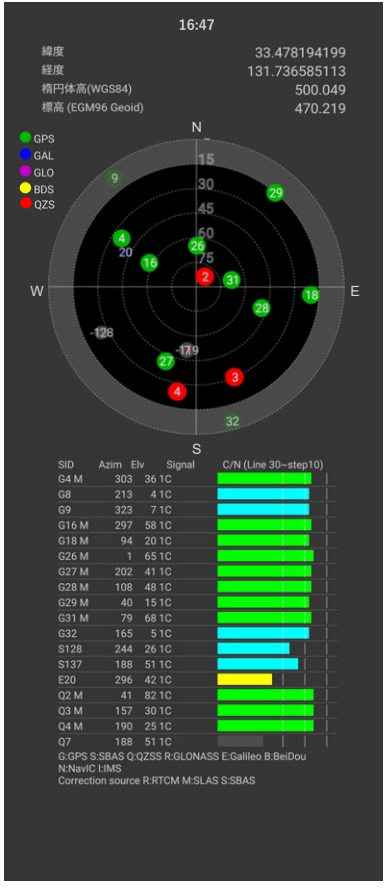
- 初回測位で補足した衛星信号を、その信号強度が弱くなっても追跡する特性が見られる。
- そのため、Spoof信号のみで開始した場合は、その後Live信号を追加してもSpoof信号を継続して追跡し、Live信号のみで開始した場合も同様にSpoof信号が追加されてもLive信号で測位する結果となった。
- Spoof信号のみで開始すると位置偽装が可能だが、信号認証によりLive信号と識別することは可能である。
- 初回測位時にLive信号とSpoof信号が混在しているケースを検証していないため、F9Pの挙動を確認したい。

【実験結果】Case Study 3: Satellite Constatation & Signal Status

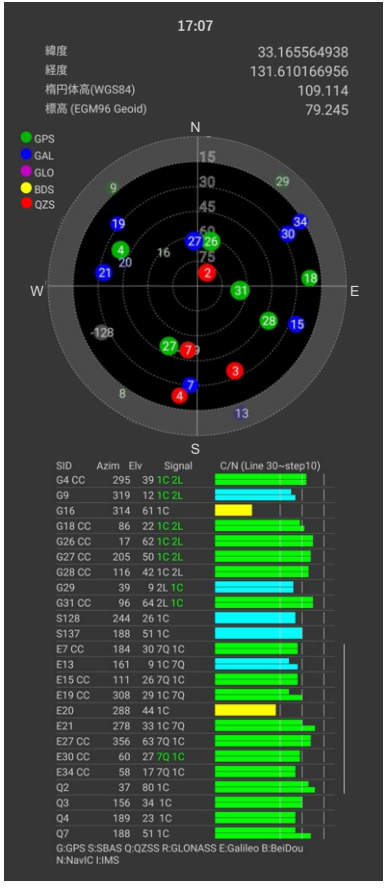
Live信号のみ



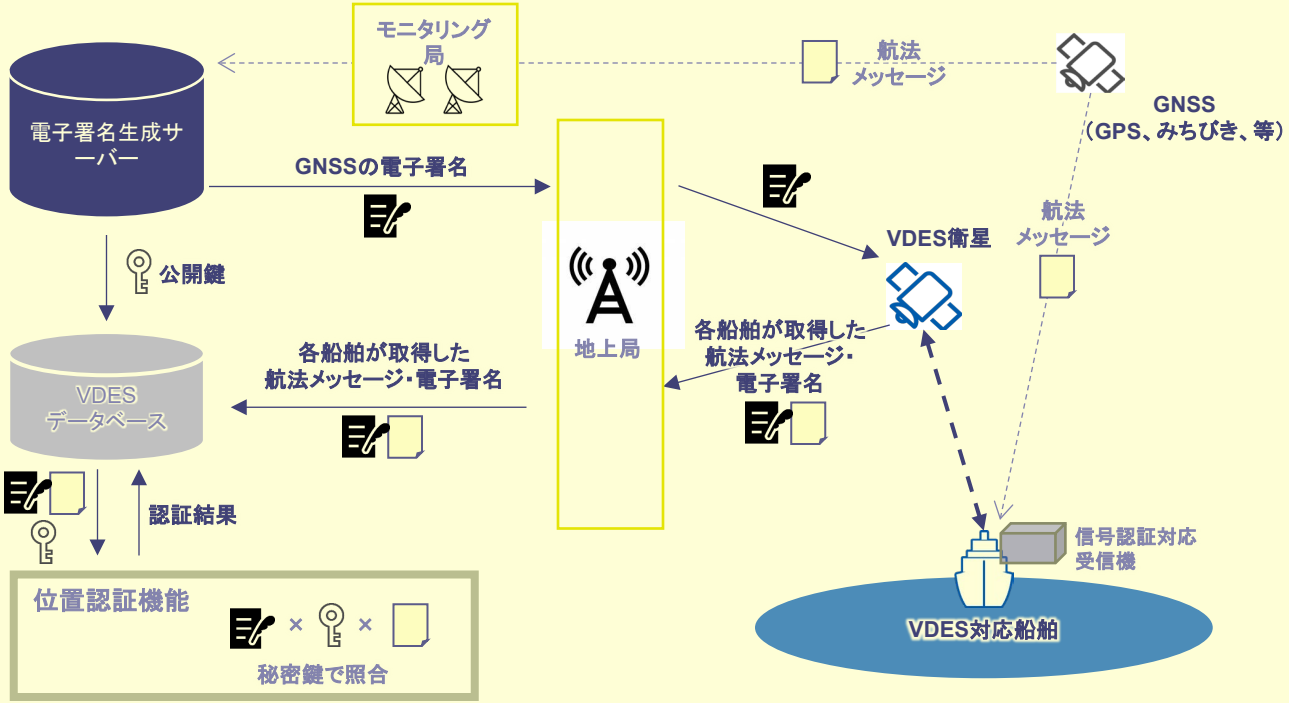
Spoof信号補足 + Live信号



Live信号補足 + Spoof信号



6. 通信衛星ベースの信号認証



VDES　Press Release

LocationMind、IHI、アークエッジ・スペースとともにNEDOのK-PRO「経済安全保障重要技術育成プログラム／船舶向け通信衛星コンステレーションによる海洋状況把握技術の開発・実証」に採択｜LocationMind株式会社｜位置情報解析の東大発スタートアップベンチャー

位置情報ビッグデータのAI解析によって様々な領域のお客様にEnd to Endのサービスを提供します。

東京大学柴崎研究室の技術を基盤に次世代技術の発展に欠かせない位置情報分析の社会実装を進めます。

こちらがホームページでリリースした際のURLです
https://locationmind.com/news/ndeo_vdes/

高精度測位部会
ジャミング/スプーフィング研究会

イントロダクション

２０２４．１０．３０

東京大学（兼務LocationMind㈱）
千野孝一

7.1.目的

GNSS技術５０周年の節目

空間情報社会のインフラとしてデジタルツインを実現する指標（緯度、経度、高度、時刻）

位置の欺瞞は容易であるために重要➡アンチジャミング／アンチスプーフィング技術

準天頂みちびきに２０２４年４月１日から信号認証サービス(SAS:Signal Authentication Service)が適用された

しかしながら、正しい位置情報の真正性を担保する技術基準・規格の制定が未着手

アンチジャミング/アンチスプーフィングの技術挙動・動作の解析をTeam Spoofing Test活動

7.2.Team Spoofing Test活動

高精度測位部会　ジャミング/スプーフィング研究会の有志による活動

事務局：東京大学　空間情報科学研究センター

ジャミング/スプーフィングの屋内・屋外実験および報告会実施

参加研究機関：８機関（大学、国研、私企業）

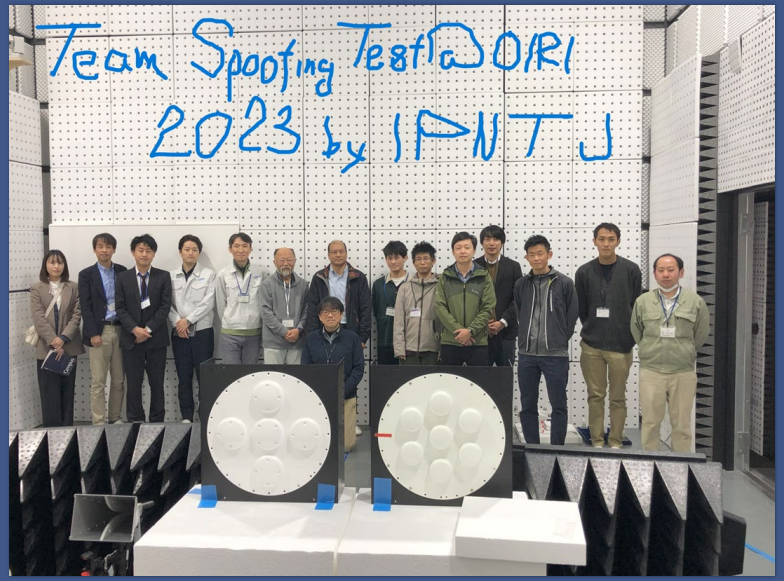
- 東京海洋大学、大阪公立大学、東京大学、JAXAつくば、JAXA航空、LM、TKK、OIRI

実験実施および報告会実施時期：３回／年（冬、春、夏）

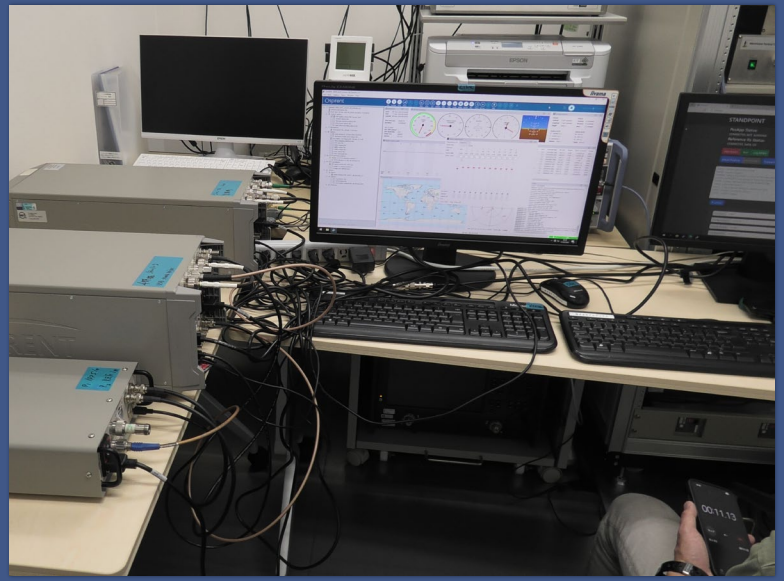
7.3.Team Spoofing Test活動【詳細】

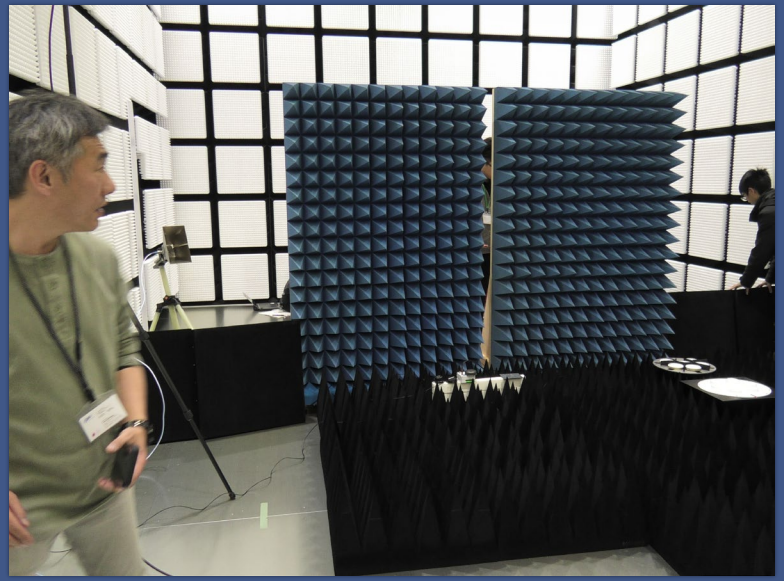
準備段階	第１回屋内実験@OIRIの電波暗室	第２回屋内実験（同期攻撃）@福島RTFの電波暗室	第３回屋外実験@福島RTF市街地フィールド
• 「実験試験局」免許取得のため総務省本省と９か月関東総合通信局と３か月交渉 • 免許期間2023年７月６日～2025年7月5日の2年間 • 諸元：GPS L1C/A 1,575,74MHz EIRP<10nW	• 2023年11月29日～12月1日 • 信号のっとりは実現できず • ※OIRI;大分県産業科学技術センター	• 2024年3月12日～14日 • 位置の攻撃と時刻の攻撃（原子時計Cs,Rb) • ※福島RTF;福島Robot Test Field	• 2024年6月17日～21日 • 車上慣性航法IMU実験、ドローンIMU実験

第1回屋内実験@OIRI



第2回屋内実験@福島RTF





7.4.Handbook α版の条件

共有データ：実験データの相互共有

データ蓄積：実験データの各機関保持

データ流通：データ・パラメータの相互流通

オープン化：学会発表、知財活動でオープン化

相互利用：オープン化したドキュメント、データ、パラメータの相互利用

標準化　　：国内・国際機関、等への標準化に貢献

Handbook化：実験手法、データ取得、パラメータ調整のノウハウの具現化

7.5.将来展望

国際活動としてNorwayでのJammertest2025(2025年9月)に参加を計画が断念

総務省へ「実験試験局」の免許期間延長(2026年7月まで)と免許範囲拡大申請 (2025年10月 申請)

Spoofing Testの追加（２０２５年３Q、２０２６年１Q、３Q）

受信機メーカ／ドローンメーカがTeam Spoofing Testに共同参加（２０２５年２Q～４Q）

Handbook　α版の作成（２０２７年７月予定）

測位航法学会２０２６年秋の大会で報告（２０２６年９月）

謝辞

- 本Spoofing Testは測位航法学会「ジャミング／スプーフィング研究会」参加各機関の協力のもと行われました。
- Team Spoofing Test@OIRI 2023&福島RTF 2024,2025powered by IPNTJ Sponsored by LM,JAXA,TUMSAT,OMU,SSS,NGNSS,TKK,EN

8.1.　AP-CAST委員会

- **AP-CAST(Action Plan for Criteria of Anti-Spoofing Technology)**
  - 耐スプーフィング技術の評価基準に関するアクションプラン
- **Team Spoofing Testに参加中の各機関の中からAP-CAST委員会に参加頂いた。**
  - JAXAつくば、JAXA航空、東京大学、大阪公立大学、東京海洋大学、LocationMind㈱、麗澤大学
- **AP-CAST委員会の目的**
  - Team Spoofing TestのField実験活動とSpoofingに関する標準化活動を重ね合わせる
- **活動期間と内容**
  - 2025年5月～8月まで計４回委員会活動を実施
  - 主に、ISO（欧州EN)の衛星測位のセキュリティに関する規格書を読み込む
  - Team Spoofing Testで目標のSpoofingに関するHandBook　α版の参考にする

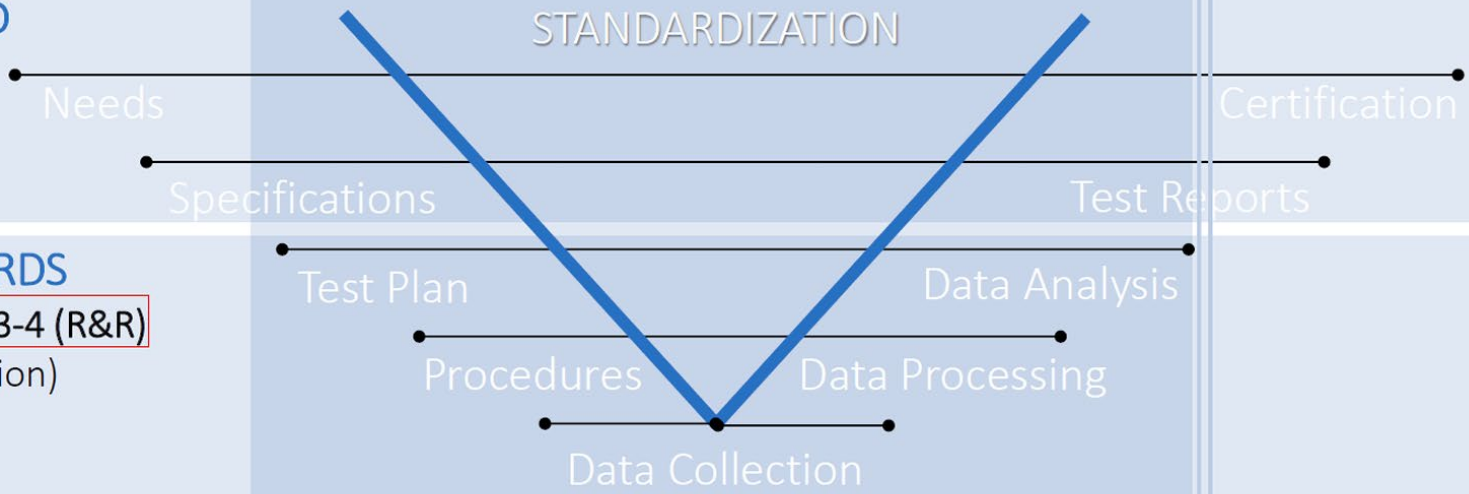
8.1. European Standardization

FRAMING STANDARD

- EN16803-1

OPERATING STANDARDS

- EN 16803-2 & EN16803-4 (R&R)
- EN 103 246-3 (Simulation)
- ...



DISTURBANCE SENSITIVITY STANDARDS

- EN16803-3
- ...

出典：第１回AP-CAST委員会

8.2.EN16803-3

第３部：干渉、妨害、 ミーコニング、スプーフィングなどのセキュリティ攻撃に焦点を当てている。

1. 範囲

目的: 実環境またはシミュレートされた道路環境におけるGNSSベースの測位端末 (GBPT) の性能評価。

対象:干渉、妨害、ミーコニング、スプーフィングなどのセキュリティ攻撃。

2. セキュリティ・テストの一般的な論理

録画と再生の原則: R&R (Record & Replay) 手法を使用し、PVT(位置、速度、時間) 情報の基本性能を評価。

妨害電波試験アーキテクチャ: 妨害信号を別々に記録し、再生時に組み合わせる。

スプーフィング/ミーコニング・テスト・アーキテクチャ: 基準GNSS信号とスプーフィング信号を一緒に記録。

3. セキュリティ性能に関する測定基準

精度指標: PVT出力の精度を測定。

可用性と継続性の測定基準: Xの可用性 (T) と連続性(T)を評価。

インテグリティ・メトリクス: 保護レベルのパフォーマンス指標、誤解を招く情報測定基準。

タイミング測定基準: タイムスタンプ分解能、公称出力レイテンシー、公称出力レート、出力待ち時間の安定性、出力レートの安定性、最初の修理に時間。

4. 試験手順および試験装置の説明

再生テストベンチのセットアップ:再生装置のキャリブレーション、リプレイ・テストベッド・アーキテクチャ。

データの再生: ジャミング・シナリオ、スプーフィングとミーコニングのシナリ オ

メトリクス劣化の計算: 妨害シナリオ、スプーフィングとミーコニングのシナリオ。

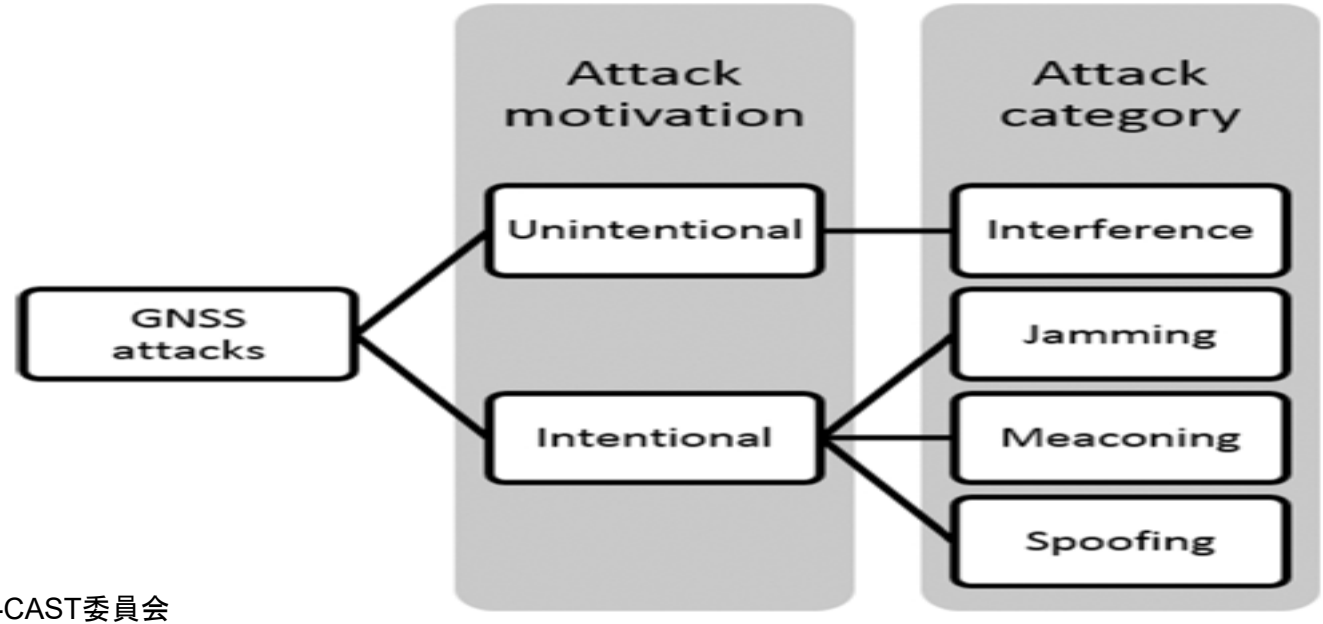
出典：第１回AP-CAST委員会

LocationMind

8.3. GNSS攻撃の分類法

非意図的な攻撃(Unintentional);GNSS周波数付近で高周波干渉信号（電磁放射）を送信し、
少なくとも１つのGBPTのPVT機能の意図しない（または無知な）性能低下を引き起こすこと。

意図的な攻撃(Intentional);GNSSの使用を阻止するため、少なくとも１つのGBPTに対して、
誤ったPVT解を誘導するために意図的に送信された信号から構成される。



出典：第１回AP-CAST委員会

8.4. なりすまし攻撃(スプーフィング)のグループ化

チャネルスプーフィング:この基本的なタイプの攻撃は、GNSSチャネルのダイナミクスを変化させ、本物の信号に対してドップラー周波数シフトや擬似レンジオフセットをもたらします。このタイプの攻撃は、市販のGNSS受信機のPVT計算にほとんど影響を与えません。なぜなら、特定の受信機アルゴリズムや機能(例えば、 受信機自律完全性監視・RAIM)が、簡単に矛盾を検出し、攻撃対象のチャンネルを除外することができるからです。これらの修正された攻撃は、サービス拒否(妨害攻撃と同様) またはサービスの欺瞞 (偽のPVTデータなど)につながる可能性があります。

軌道スプーフィング: このタイプの攻撃は、基本的なチャンネル・スプーフィングを一般化したものですが、GNSS コンステレーション全体を改ざんすることを目的としています。具体的には、攻撃者は偽の位置に対応する複数の衛星から偽の信号を生成し、被害者の受信機に送信します。

データレベル・スプーフィング:この場合、攻撃者は本物の信号ダイナミクスに変更を加えることはしませんが、PVT損なうために送信されるナビゲーションデータを変更します。例えば、この種の攻撃は、衛星ベースの補強システム (SBAS) からの差分補正を使用するように設定されたGNSS受信機の場合に有効です。

出典：第１回AP-CAST委員会

8.5. ACAIとTTFF

EN 16803-3のセキュリティテストは、EN16803-2に記載されているテストと同じ方法論に基ずき、以下の指標を評価するために設計されている。

- 可用性（Availability)
- 継続性（Continuity)
- 正確性（Accuracy)
- 完全性（Integrity)
- 初回修正までの時間（TTFF;Time To First Fix)

これらの指標を評価するための手法は「記録と再生」
(R&R;Record＆Replay）と呼ばれ、EN16803-2に詳述されている。

出典：第１回AP-CAST委員会

8.6. スプーフィングテストアーキテクチャ

SISにロックされた受信機からエフェメリス、観測値、パルス毎秒 (PPS) を取得し、フロントエンドの前に本物のSISと合成されるスプーフィング信号を生成する無線周波数信号シミュレータ (RFCS) を記録車両に装備するSIS

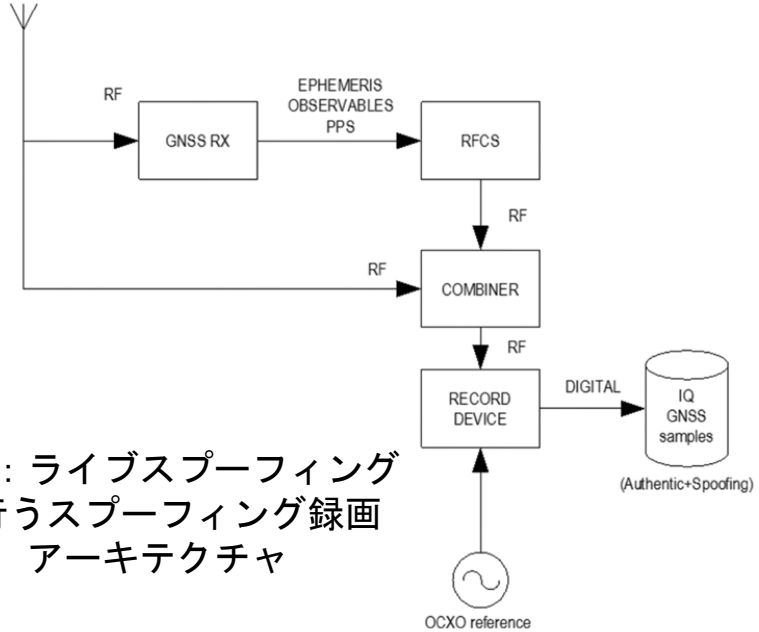


図１：ライブスプーフィングを行うスプーフィング録画アーキテクチャ

出典：第１回AP-CAST委員会

RFCSで合成信号(SIS+ スプーフィング)を生成し、出力を記録する。

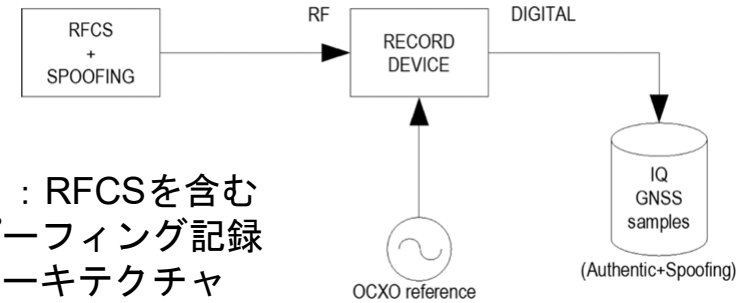


図２：RFCSを含むスプーフィング記録アーキテクチャ

LocationMind

8.7. 精度劣化メトリクス

下図は精度劣化の指標を示している。
青い曲線は、公称状態(すなわち、攻撃を受けていない状態)でテスト中のGBPTで得られた公称精度性能に対応する。
赤い曲線は、同じ GBPTで攻撃を受けているときに得られた性能を表しています。
注目するパーセンタイルで得られた劣化のパーセンテージが表示されています。

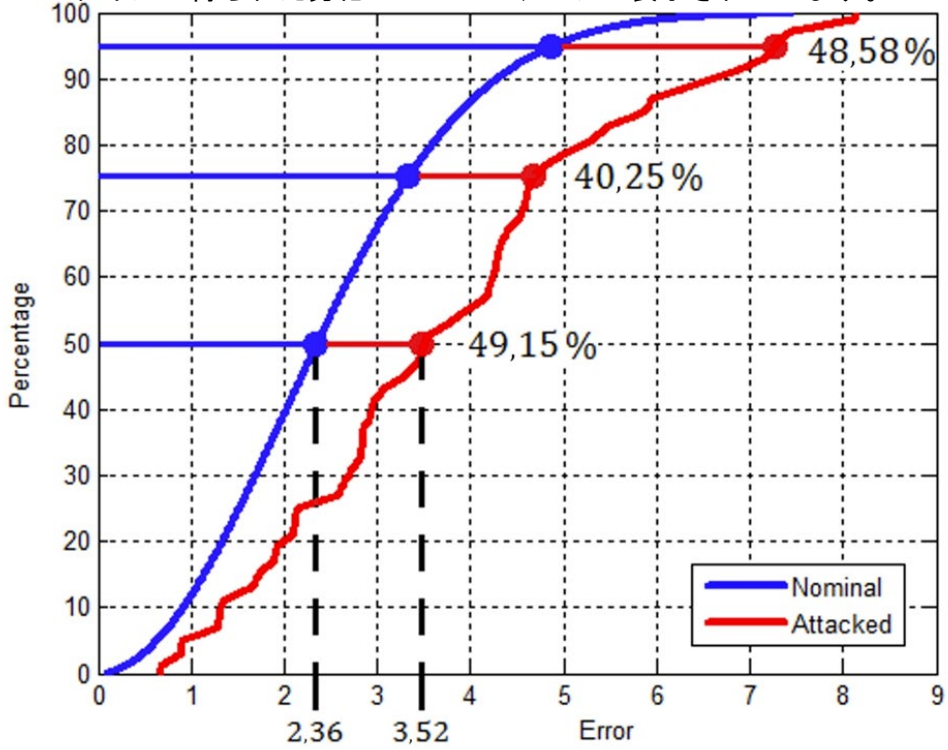


図３：
精度劣化
メトリクス

出典：第１回AP-CAST委員会

8.8. スプーフィングシナリオ(NDS vs ADS)

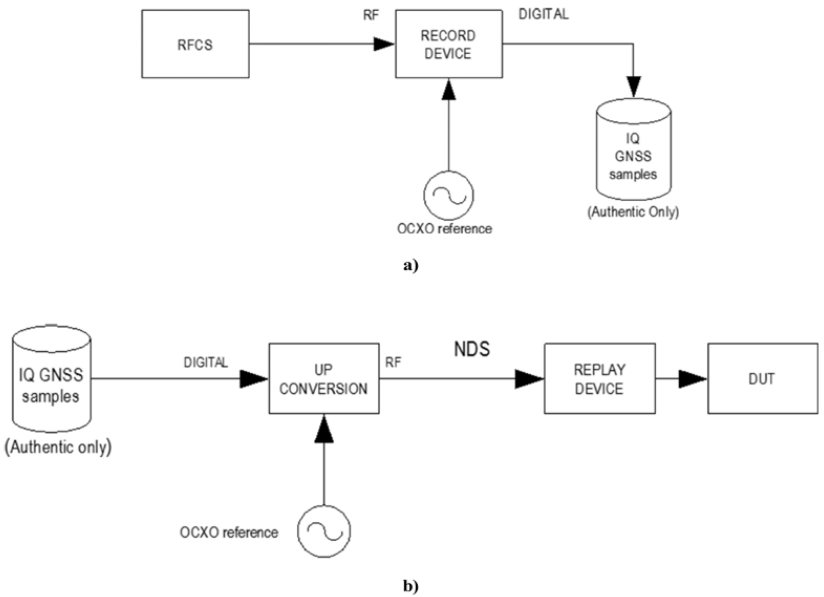


図４：スプーフィングテストアーキテクチャにおけるNDSの位置付け

NDS; Nominal Data Set
（攻撃信号のないデータセット）

ADS; Attacked Data Set
（攻撃信号で特別に記録されたデータセット）

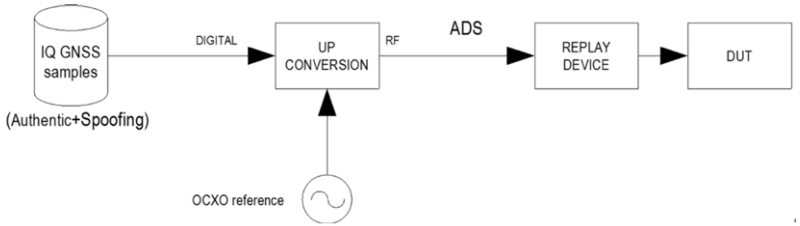
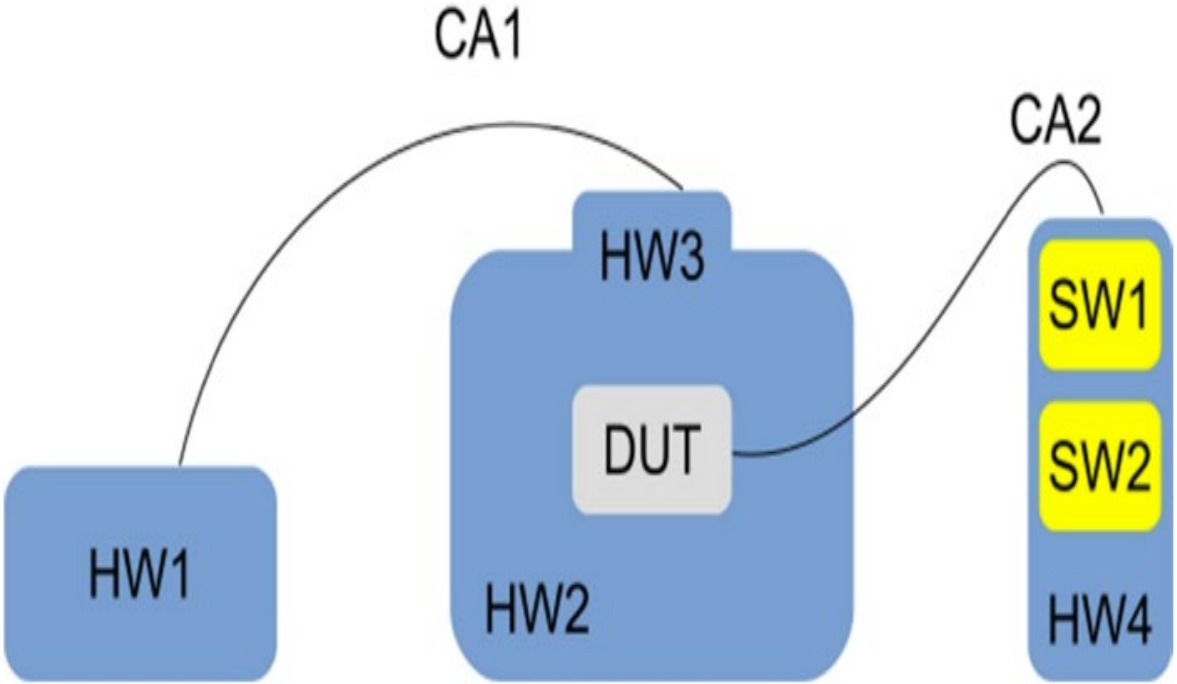


図５：スプーフィングテストアーキテクチャにおけるADSの位置付け

出典：第１回AP-CAST委員会

LocationMind

8.9. テストベンチのブロック図



HW1:GNSS信号記録再生装置
HW2:無響室（電波暗室）
HW3:送信アンテナ
HW4:パソコン

SW1:メトリクスアナライザー
SW2:GBPTコントロール＆
ログツール

CA1:GNSSリプレーヤーHW1と
アンテナHW3をつなぐケーブル
CA2:コンピューターにデータを
記録するために使用するケーブル
つまりDUTが出力するHW4

出典：第１回AP-CAST委員会

LocationMind

8.10.評価指標

評価指標		使用DUT出力
評価された**精度劣化**指標 (EN 16803-3に準拠)	AccDegPosition - 水平 AccDegPosition - トラック沿い AccDegPosition - トラック横断 AccDegSpeed -水平	GNGGA GNGGA GNGGA GNVTG
インテグリティ 劣化評価指標 (EN 16803-3に準拠)	PL_DegPosition - 水平 PL_DegPosition - トラック沿い PL_DegPosition - クロストラック PL_DegVelocity - 水平	GNTBD [a] GNTBD [a] GNTBD [a] GNTBD [a]
可用性と継続性 劣化メトリクスの評価（EN 16803に準拠）	AvailDegPosition - 1秒のTウィンドウ AvailDegPosition - 60年代のTウィンドー	GNGGA GNGGA
タイミング 劣化メトリクスの評価 (EN 16803による)	TTFF_Deg(T)	GNGGA

出典：第１回AP-CAST委員会

LocationMind

LocationMind

お問合せ先

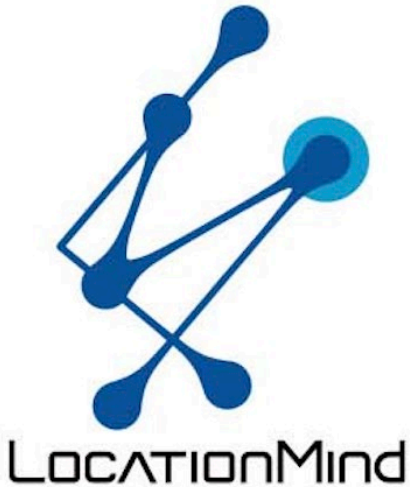
LocationMind株式会社

R＆D Division

Senior Project Manager & Chief PNT Strategist

千野孝一

chino@locationmind.com


LocationMind