Doc.Number: LMDF-T-2025-0122

防衛技術シンポジウム LocationMind発表 無線指紋技術 研究・開発

衛星による測位・時刻同期の革新的な欺瞞対策技術の開発

2025.11

前書き：GNSS信号の脅威への対抗

GNSS信号を使用した社会インフラシステムへの挑戦・脅威への対抗手段の提案

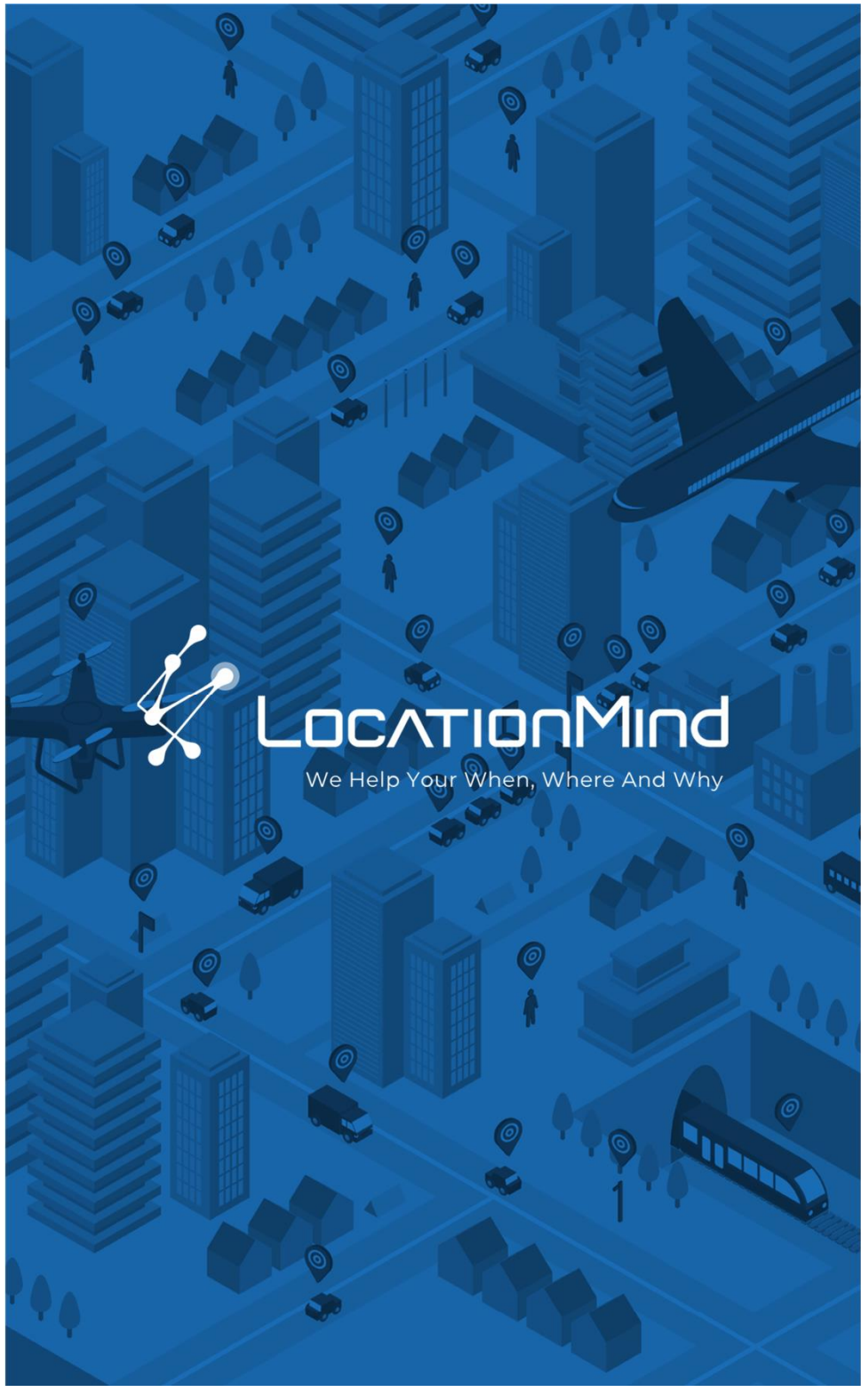
GNSS信号は、一般公開されている仕様に基づいて放送されており、
改竄や欺瞞等の脅威に対して脆弱である。

GNSS信号を利用している社会インフラシステムがそのような脅威に曝されると、
致命的な障害、影響を受ける可能性がある。

本研究テーマである無線指紋で、GNSS信号の真贋を識別する技術を提供する。

この技術は、まだ有効な対抗手段がないミーコニングに対しても有効である。

LocationMind会社紹介



LocationMind at a Glance

Company Profile

会社名	LocationMind株式会社
設立	2019年2月
従業員	85名
事業	位置情報の分析、 測位のセキュリティ

東京大学柴崎亮介研究室がベンチャー化

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

多国籍な空間情報分析集団

- ✓ 従業員の40%が分析者（博士・ポスドクを含む）
- ✓ 従業員の30%が日本以外の国籍で、グローバルな分析を提供

Management Team

桐谷直毅
CEO
Goldman Sachs
Angel Bridge

小川竜馬
CFO
SMBC
SMBC NIKKO

藤田 智明 COO
BCG

Fundraise

累計49億円調達
（公表ベース）

Group Company

Advertisementmind

事業概要

空間情報AI

世界を牽引する空間情報技術

空間情報に係るビッグデータを80ヵ国以上に提供

GNSS Signal Security

System Design and Development

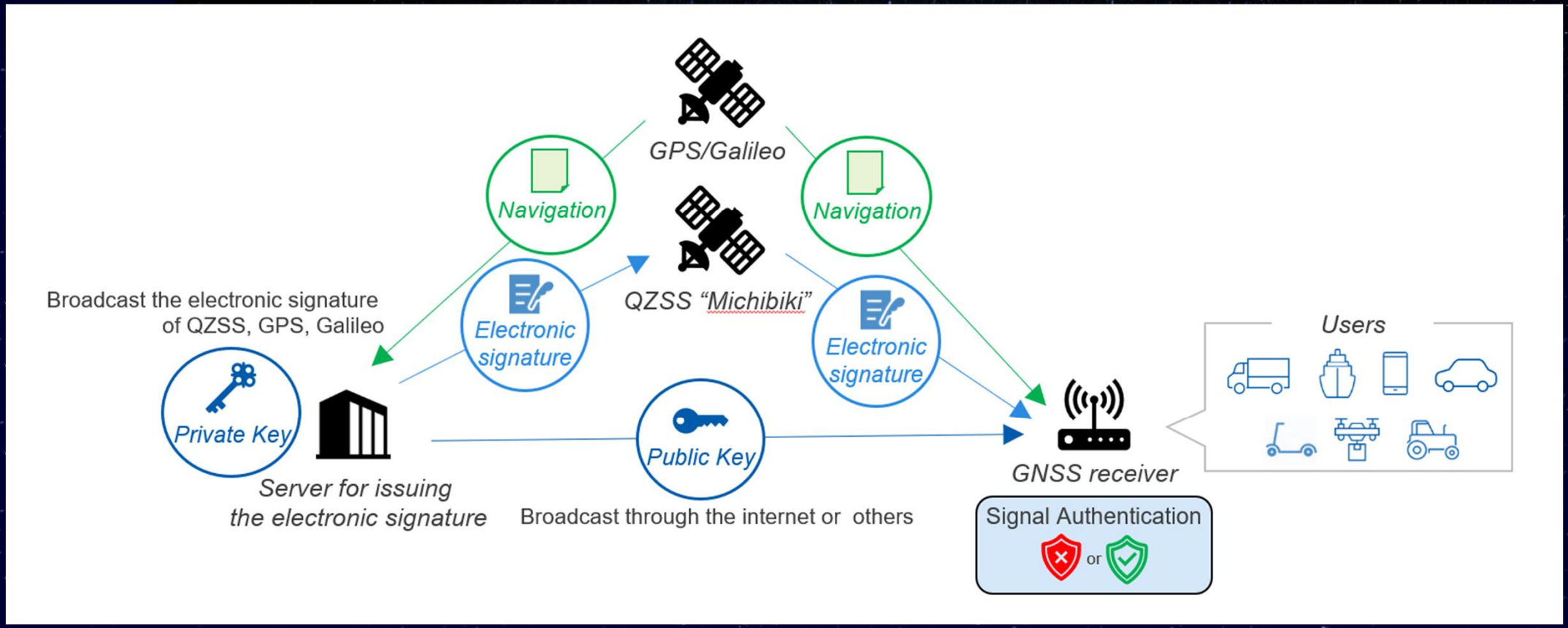
電波の視点から位置情報の安全性を高め、情報の真正性を確保

LocationMindの特許技術で
世界中の位置情報を『認証』する

年間25億台販売される
“GPS受信機”やそれを
使う広大な産業に
安心・安全を提供

QZSS信号認証の仕組み

準天頂衛星に対する
信号認証システムの開発・実装



GNSS信号に対する脅威

ジャミング、スプーフィング、
そしてミーコニング

GNSS Signal Threat

- GNSSをもとにした重要な情報として、位置情報、時刻情報がある。しかしこれらは、オープンな情報であり、妨害に対して脆弱である。
- GNSS情報は、様々なシステムで使用されており、もし、これらが失われたり、改ざんされた場合には、致命的な影響が生じる。
  - 通信基地局
  - ５G通信機器
  - Autonomous Vehicle
  - Drone
  - Etc.

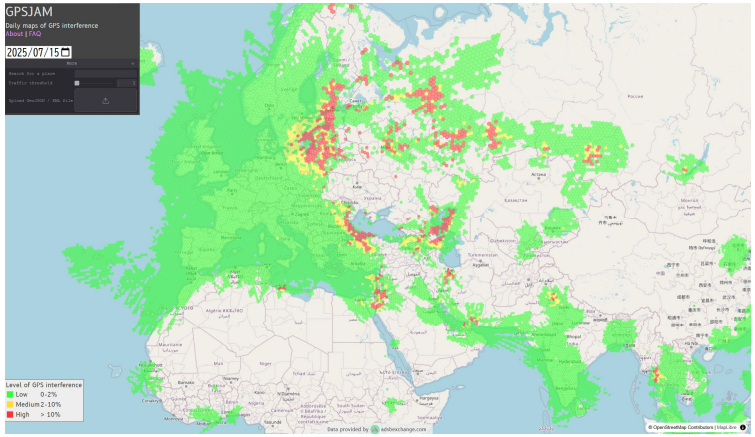
Position

Time

GNSS信号に対する脅威

世界各地の紛争地域もしくは、その周辺において、大規模な測位衛星信号に対する攻撃が観測され、民間・軍事活動ともに影響を受けている。

No.	タイトル	内容概要	ソースリンク
1	GNSS spoofing threatens airline safety, alarming pilots and aviation officials (GPS World, 2024)	民間航空でGNSSスプーフィング事例が急増し、**偽の信号により航法・安全システムが混乱を来している**。世界各地で1日1000件以上発生し、時計のリセットや誤警報・コース逸脱などが報告されており、バックアップ(A-PNT)の必要性が高まっている	GPS World記事
2	衛星測位システムへの攻撃が急増、航空機運航の脅威に (航空新聞社, 2024)	**紛争地域を中心にGNSSへのジャミング・スプーフィング攻撃が急増**し、航空機の安全運航を脅かしている。欧州航空安全庁(EASA)と国際航空運送協会(IATA)はワークショップでインシデント情報共有と短期・中長期の対策の必要性を確認した	航空新聞社記事
3	船舶:GPSスプーフィングの商業的リスク (McAfee Blog @ASCII.jp, 2020)	**船舶など運輸業ではGPSスプーフィングにより航路から外される危険**がある。偽の信号で船長が気付かぬうちに船を誤誘導し、海賊行為に悪用される可能性が指摘されている	ASCII.jp記事
4	自動運転車:Tesla Model S/3はGNSS欺瞞に脆弱 (GPS World, 2019)	**実験によりTesla車の自動運転ナビがGPSスプーフィングで欺かれ**、車両が突然減速・勝手に高速道路の出口へ逸脱する事象が確認された。**安価な機材で攻撃可能で、自動運転システムのGNSS依存の脆弱性**が浮き彫りとなっている	GPS World記事



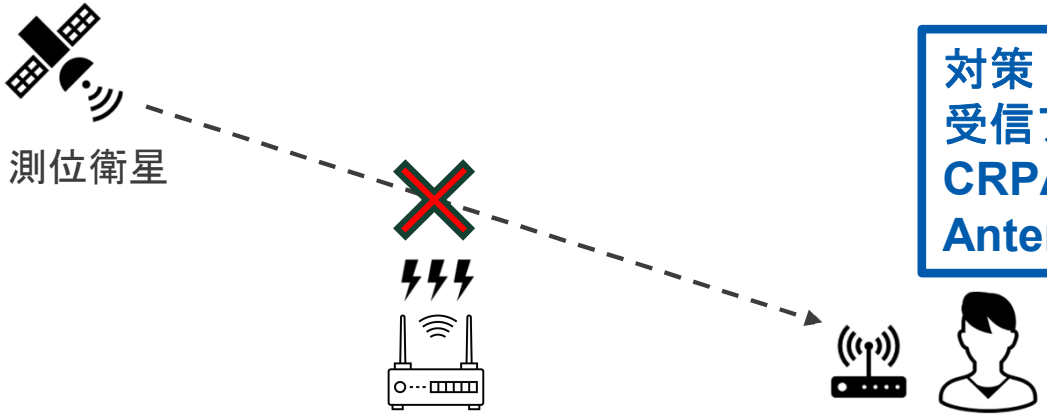
参考文献：
(1) 防衛技術ジャーナル2025年9月号　最新　対スプーフィング技術の動向
(2) 先端技術研究会　講演資料 CYPC-T-2025-0004

GPSJAM
https://gpsjam.org/?lat=45.00000&lon=35.00000&z=3.0&date=2025-07-15

GNSS妨害の種類と対策法について

ジャミング:

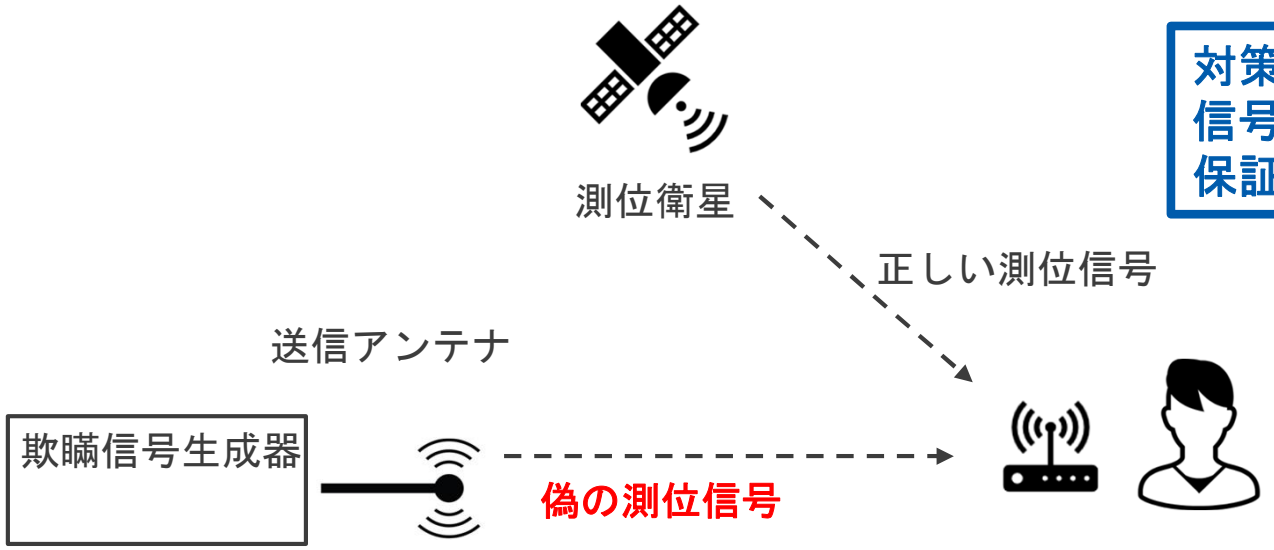
妨害電波により受信機がGNSS信号を受信できないよう妨害する手法
会話中に大声を出して妨害する行為に相当する。



対策：
受信アンテナを制御し、強い信号は受信しない
CRPA(Controlled Reception Pattern Antenna)等により対策する

スプーフィング (欺瞞、改竄):

偽の測位信号を生成し、位置・時刻情報を捏造する妨害する手法

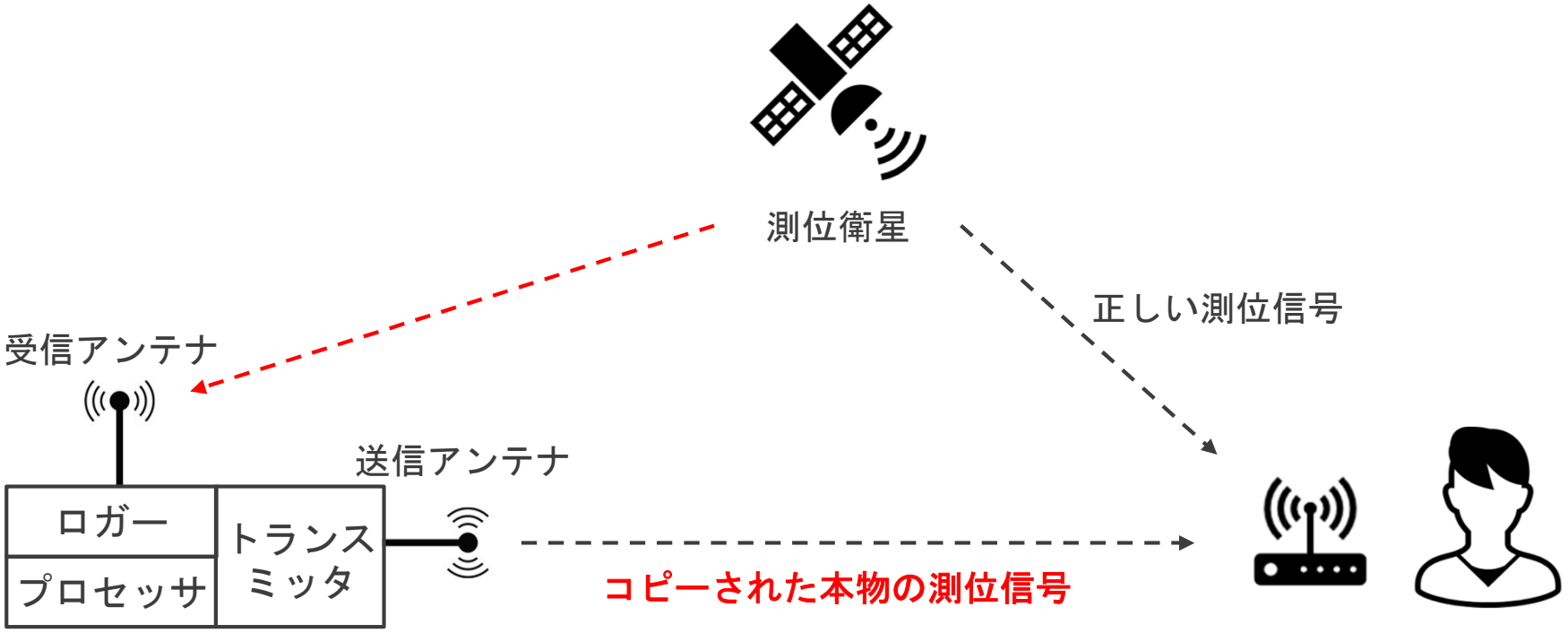


対策：
信号認証機能などにより、GNSSの真正性を保証する。（信号認証機能 LocationMind)

GNSS妨害の種類と対策法について

ミーコニング:

測位信号をそのまま記録・コピーし、再放送して妨害する手法
正常なGNSS信号をコピーして、再放送するため、真の信号との識別が困難
受信機では、測位信号の受信時刻がずれ、結果として位置情報、時刻情報にずれが生じる。
高速で移動する飛行体や精密な時刻同期を必要とする金融システムに対しては、わずかな位置、時刻のずれが致命的な影響を与える可能性がある。



対策：
有効な対策手段なし

衛星による測位・時刻同期の革新的な欺瞞対策技術の開発

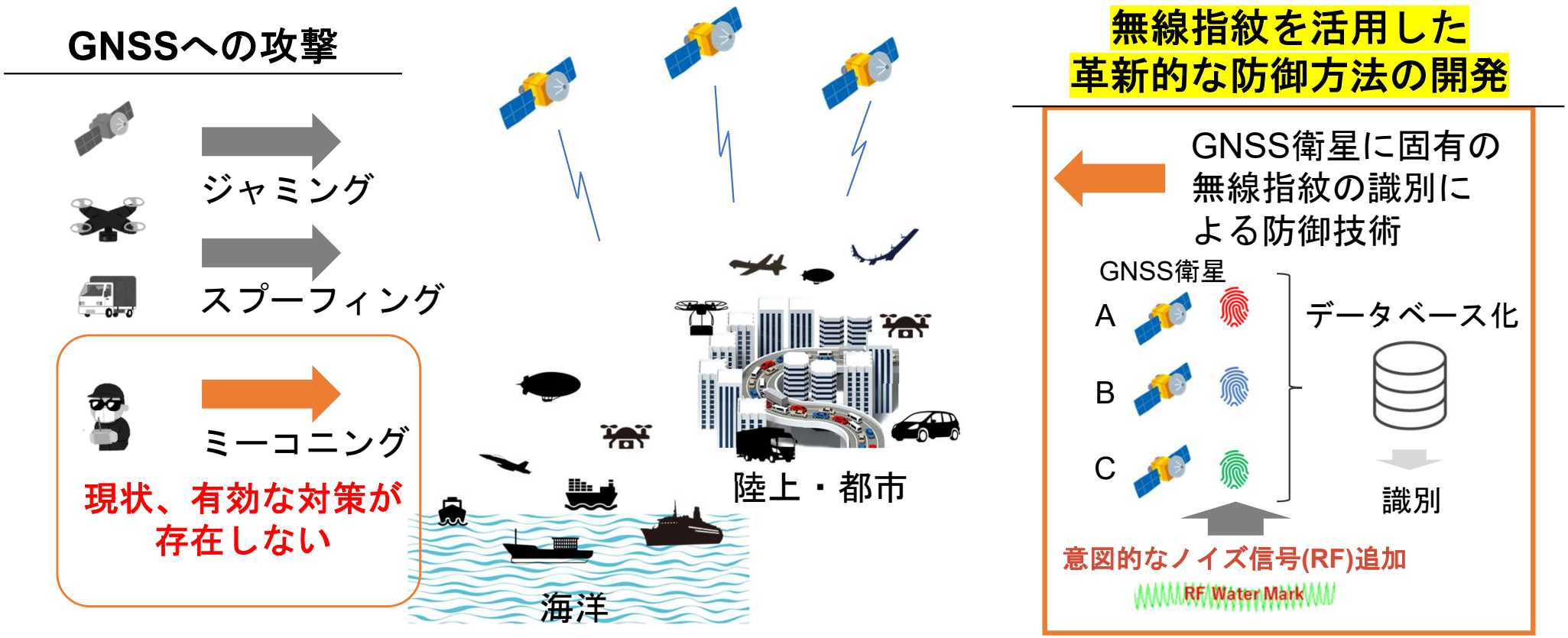
無線指紋技術開発

衛星による測位・時刻同期の革新的な欺瞞対策技術の開発

研究概要

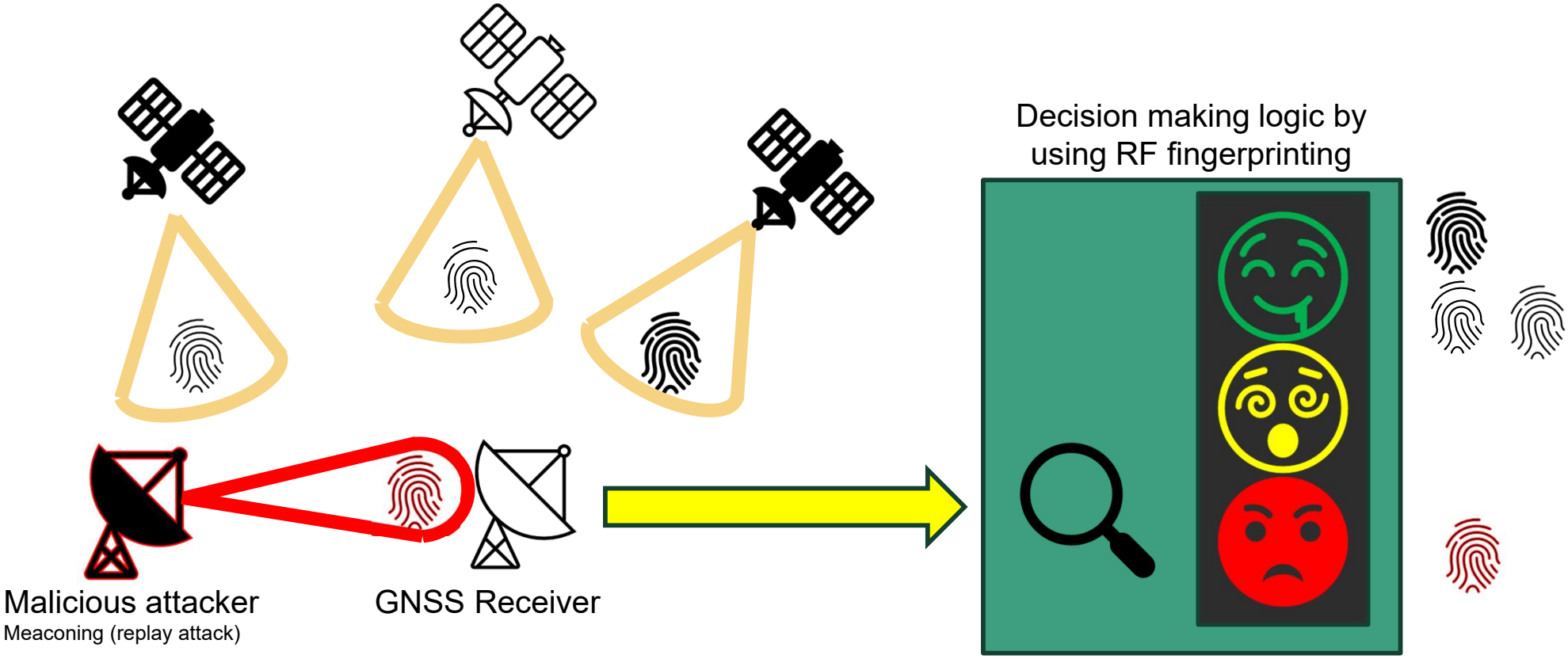
LocationMind株式会社　CTO　柴崎亮介

測位衛星による測位・時刻同期システムは、自動運転、ドローン管制、高速無線通信システム等を支える社会インフラだが欺瞞や改竄攻撃に脆弱である。本研究では、現状有効な対策がない**ミーコニングに対し、無線指紋技術を活用した革新的な防御手法**を開発する。



無線指紋とは何か？

あらゆる無線信号は、**送信機の特徴（製造上の特徴、製造誤差、使用デバイスによる特徴）に起因する特徴点**をもつ。
それを無線指紋と呼ぶ。
すなわち、様々な無線信号は、送信機に起因する特徴を有し、それを特徴点としてとらえることにより、**無線信号の真正性を判断することが可能**になるのではないだろうか？
この考え方をGNSS信号に適用することにより、
真の測位信号と悪意のあるミーコニング信号とを識別できないだろうか。
これが研究テーマである。



進捗

LocationMindの提案した無線指紋によるGNSS信号の真正性検証手法に関しては、
安全保障技術研究推進制度　令和５年度・タイプSに採択され、研究を進めている。

令和5年度：

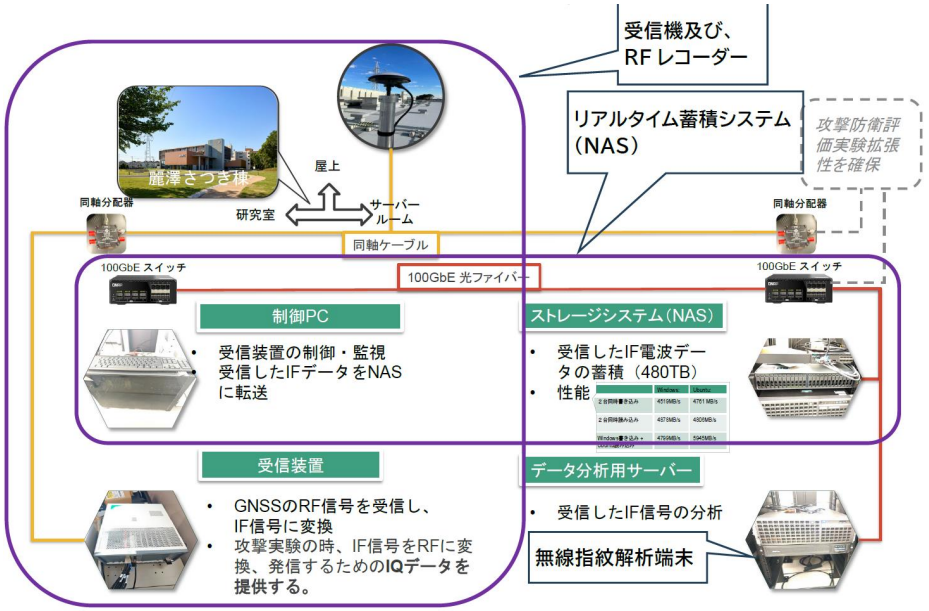
無線指紋評価のためのGNSS信号データセット選定

無線指紋評価のための装置調達、準備

令和6年度：

無線指紋評価装置をシステムインテグレーション

令和5年度に選定したGNSS信号データセットをGNSS信号受信システムで記録/評価開始



GNSS信号受信システム

デジタル信号処理された
大量のGNSS信号データを安定して、
高速にストレージに蓄積することを
実現！！

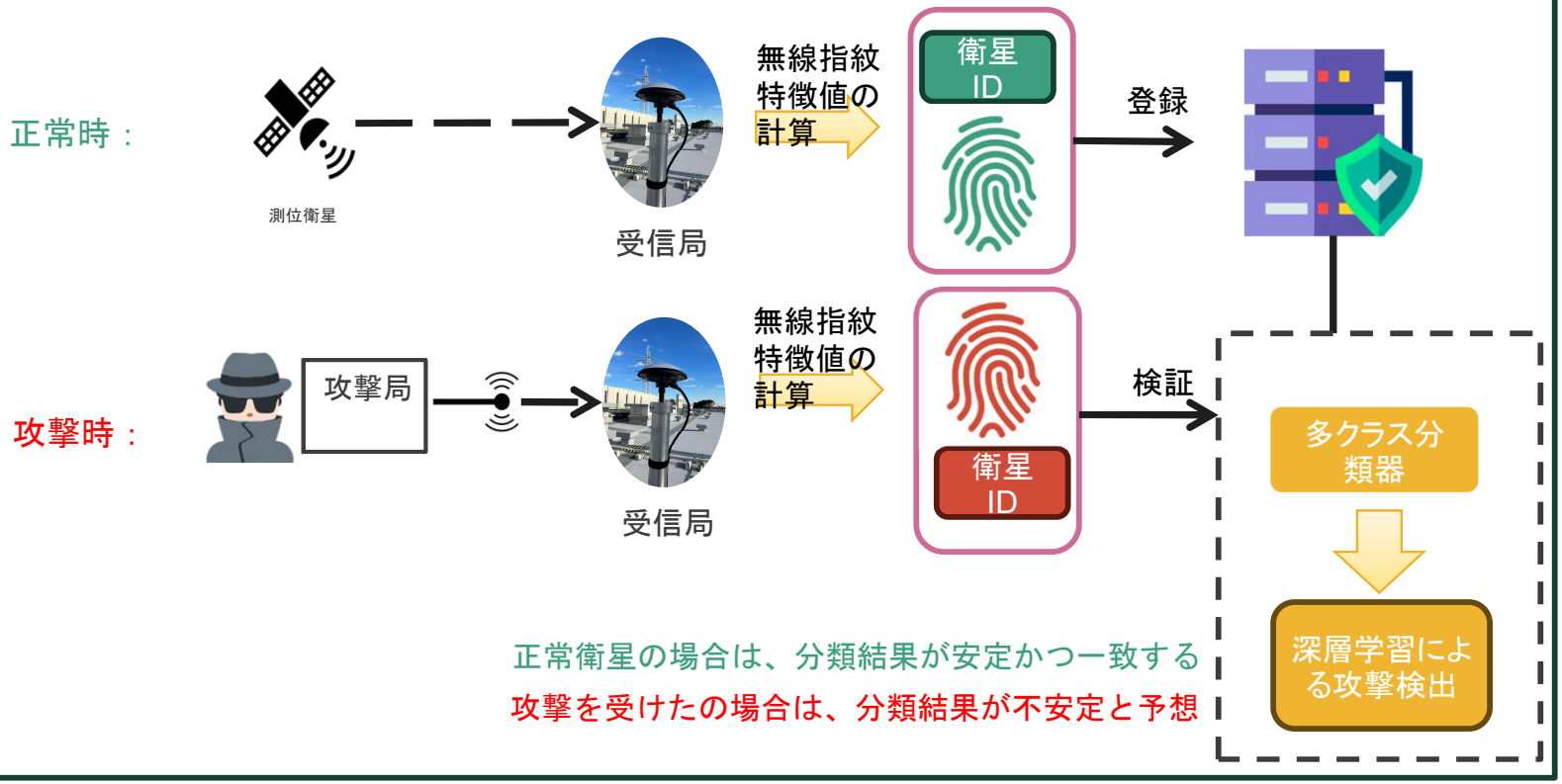
令和7年度：

無線指紋特徴点抽出アルゴリズムの評価開始

現時点での成果

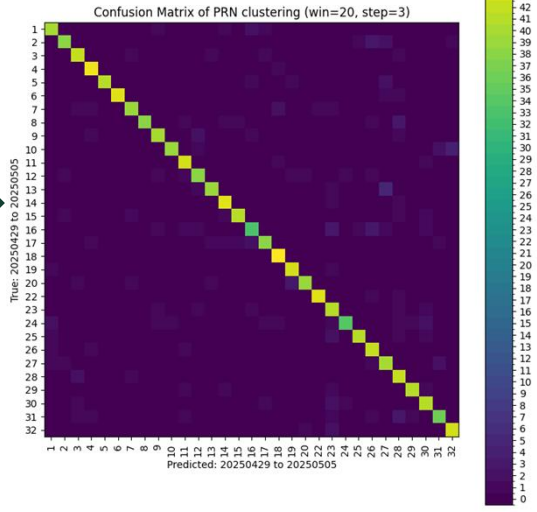
令和6年度時点の検討

衛星の無線指紋特徴量を測って、その衛星からの電波なのかを検証する



令和7年度　9月時点の評価で、
衛星の識別の可能性を確認した。

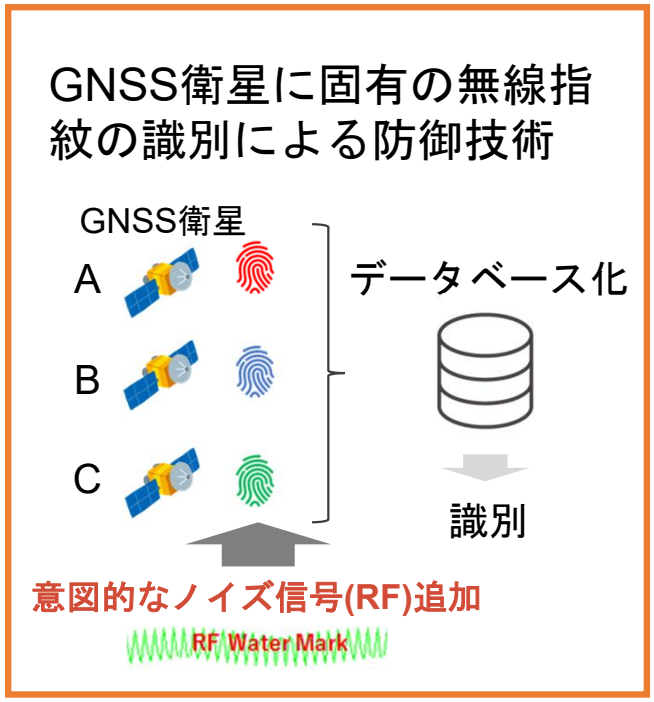
令和7年度9月時点
初期識別評価結果



将来の展望

GNSSに対する脅威に対して、無線指紋を活用した革新的な防御方法を開発することにより、社会システムの安定・安全性確保に寄与する。

無線指紋を活用した革新的な防御方法の開発



- ドローン管制システムの安全性強化、実装
- 空飛ぶクルマの運用システムへの実装
- 自動運転システムへの実装
- 船舶自動航行システムの安全性強化、実装

ご清聴ありがとうございました