SAPT研究発表講演会
Sept. 1, 2023

SBASの信号認証機能とサンプルメッセージ

国立研究開発法人海上・港湾・航空技術研究所
電子航法研究所　坂井 丈泰

Introduction

- SBAS（Satellite-Based Augmentation System）
  - 補強システム：GPS等コアシステムを補強し、これらと併用されることで民間航空用途に利用できる衛星航法を提供する。
    - Ø 日本では航空局がMSASを運用中（L1 SBAS：L1信号により送信）。
  - 最近、次世代規格（L5 SBAS）が制定されたところ。
    - Ø DFMC SBAS：Dual-Frequency Multi-Constellation対応による性能改善。
    - Ø 2020年末に規格を制定。現在は認証機能の追加が議論されている。
- GPS（GNSS）の脆弱性
  - GPS/GNSSの性質上、妨害やスプーフィング（なりすまし）が可能。
  - 最近はソフトウェア無線技術が進展し、脅威が増している。
- 「SBASの信号認証機能とサンプルメッセージ」
  - （1） GPS/GNSSの脆弱性、ディジタル署名技術によるなりすまし防止
  - （2） 広域補強システムSBASによる認証情報の配信
  - （3） プロトタイプの開発、サンプルメッセージの生成

GPS信号の性質

信号が微弱

- 2万km彼方に100Wの電球があるのと同じレベル。
- 同じ周波数で強力な電波があったらとても受信できない。

信号の形式・内容が公知

- 技術力さえあれば、誰でもGPS受信機をつくれる。
- 技術力さえあれば、誰でもGPS信号をつくれる。

正当な信号か検証する仕組みがない

- GPS信号は、暗号化はされておらず、認証情報もない。
- 第三者が生成した信号を、正当な信号と区別できない。

電波干渉

- **意図的ではない障害：電波干渉**
  - 無線機器の運用・故障などにより、GPS衛星が送信している電波（周波数1.6GHz帯）に干渉してしまうもの。
    - Ø *帯域フィルタの故障などで出た高調波による事例がいくつか報告されている。*
    - Ø *症状：GPSが使用できなくなる。*
  - 室内でGPSを使用するために設置するリピータの電波が漏れた例。
    - Ø *屋上でGPS信号を受信して室内に再放射するといった用途の製品がある。*
    - Ø *シールドが不十分だったりドアが開いていたりすると、電波が周囲に漏れる。*
    - Ø *症状：GPSにより測定される位置が大きくずれる。*

市販されているリピータの例
（イネーブラー（株）GPSRKL12G）

ジャミング（妨害）

- **意図的な場合（1）：ジャミング（妨害）**
  - 妨害電波を発して周辺のGPSを利用できなくするもの。
  - ソウル周辺における事例（2010年頃から）
    - Ø *航空機がGPSを利用できない事例がしばしば報告されている。*
  - PPD（Personal Privacy Device）
    - Ø *GPSを妨害する電波を発射する装置。*
    - Ø *米国でトラック等のドライバーが自己の位置を知られるのを嫌い、使用する例があった（当時は合法だった）。*
    - Ø *現在は違法とされている。*
  - 症状：GPSを利用できなくなる。
    - Ø *強力な妨害波ほど広い範囲のGPS受信機を妨害できるが、送信源を発見・特定するのは容易になる。*

市販されていたPPDの例

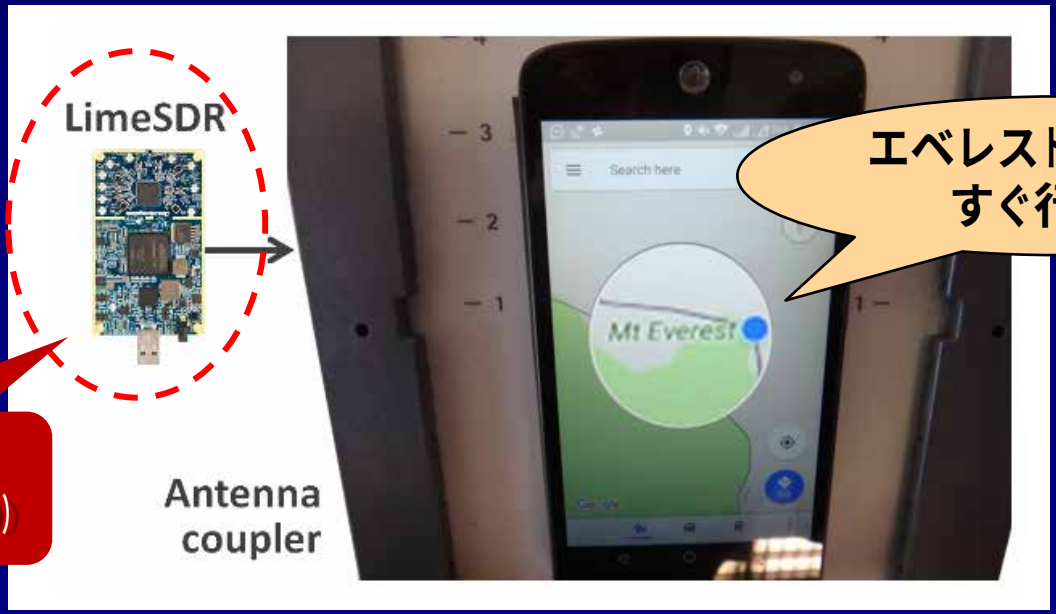
ミーコニング (プレイバック)

- **意図的な場合 (2) : ミーコニング (プレイバック)**
  - GPS信号をそのまま、あるいは多少の加工をして再送信するもの。
    - Ø *GPS信号そのもの : 微弱な電波でもGPSを妨害できる。*
    - Ø *RFレコーダによりGPS信号をプレイバックすれば簡単。*
  - 症状 : GPSを利用できなくなる or GPSにより測定される位置が大きくずれる。
    - Ø *時刻情報の照合が有効だが、統一的な対策はない。*
    - Ø *ごく短時間の遅延は対策が難しい。*
    - Ø *ただし、ユーザ受信機にて算出される位置を任意にコントロールすることはできない。*

RFレコーダ・プレイヤーの例
(イネーブラー (株) MP7200)

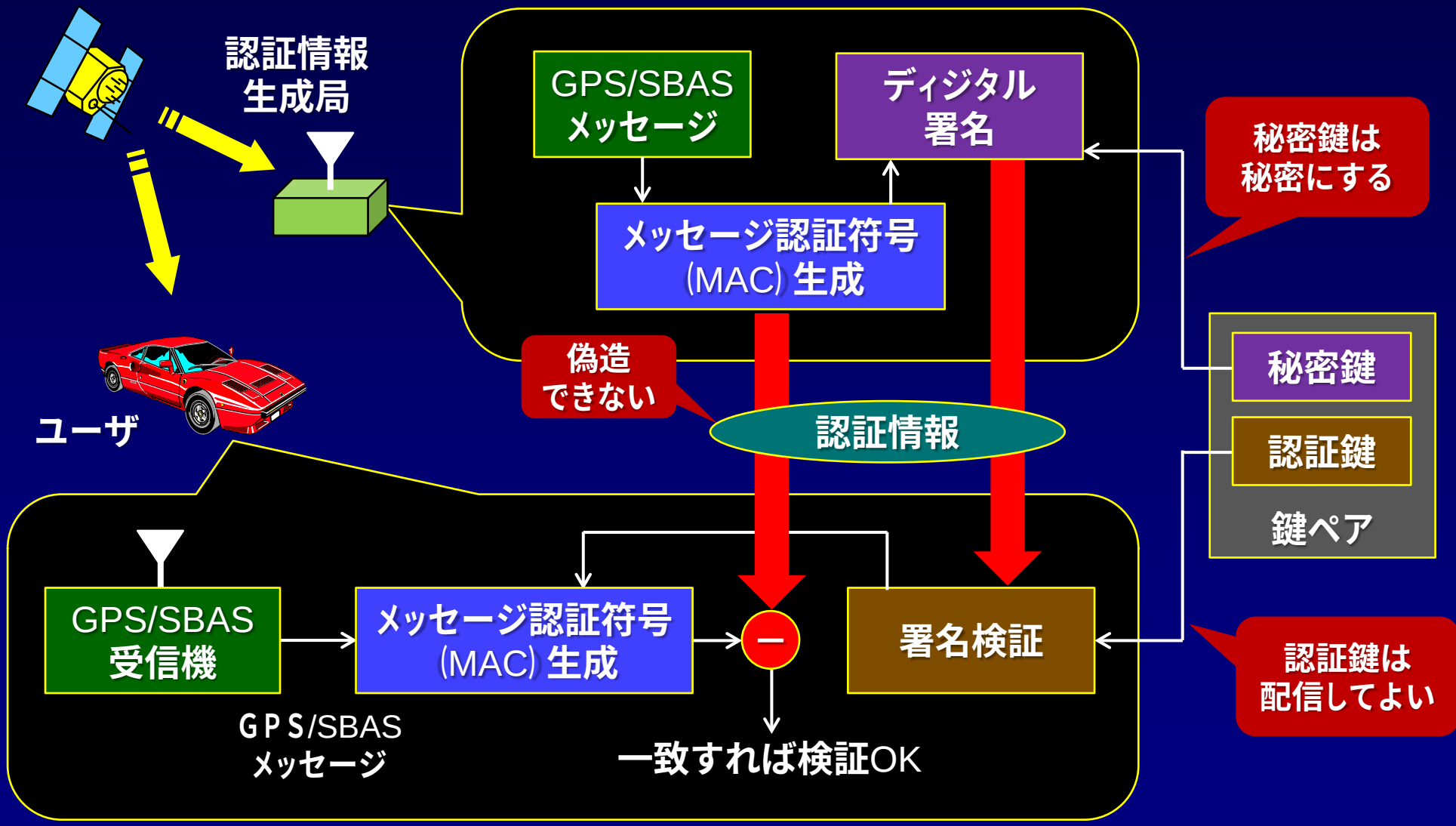
スプーフィング（なりすまし）

- **意図的な場合（3）：スプーフィング（なりすまし）**
  - GPS信号を独自に生成（偽造）して送信するもの。
    - Ø *微弱な電波でもGPSを妨害できる。本物のGPS信号と区別できない。*
    - Ø *最近は、ソフトウェア無線技術の進展により簡単・安価に実行できる環境。*
      - u **オープンソースのGPSシミュレータが公開されている。**
  - 症状：GPSにより測定される位置が大きくずれる。
    - Ø *攻撃者の意図する位置を算出させることが可能。*

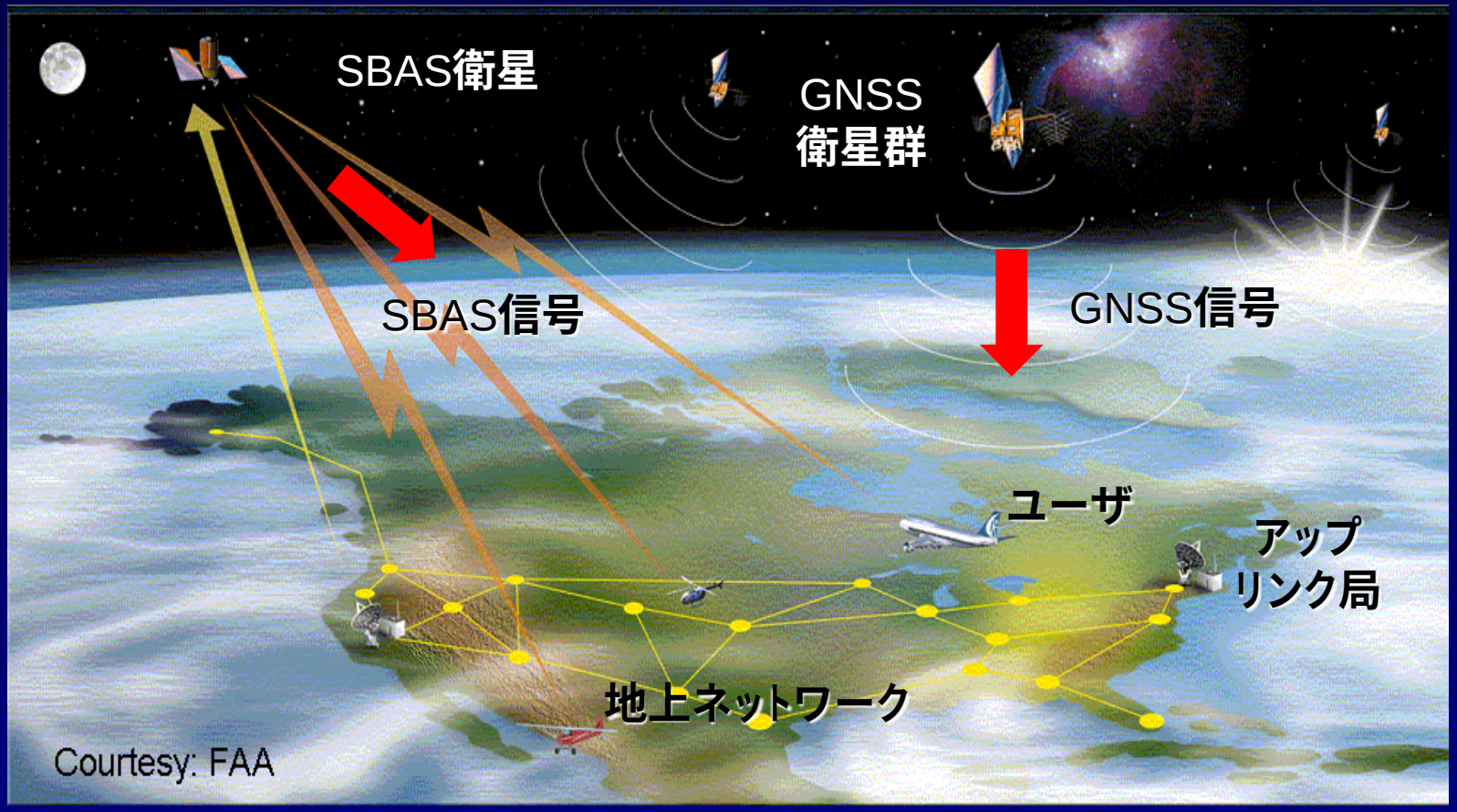


（Septentrio社HPより）

対策：ディジタル署名による認証



SBASの仕組み

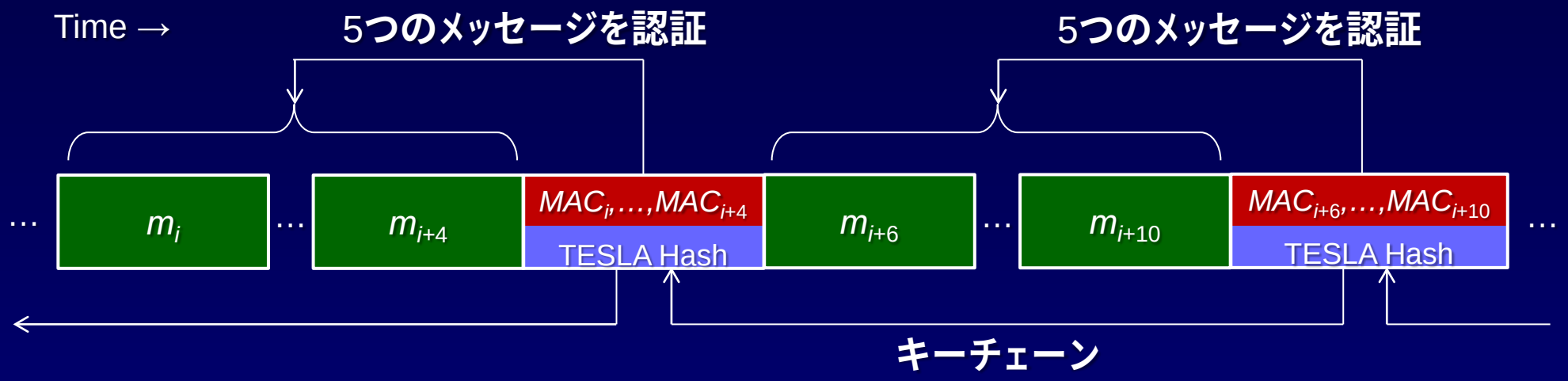


- 地上ネットワークによりGNSS信号を監視（異常の有無・測距誤差）
- ディファレンシャル補正情報及び完全性情報をSBAS衛星経由で送信
- L1 C/AコードまたはL5信号を使用：GPSとアンテナ・RF回路を共用

SBASによるGNSS信号認証

- SBASによる信号認証
  - 広域補強の一環として信号認証サービスを提供する。
  - 2017年6月に開催されたICAO会議において欧州から提案された。
  - 2020年末までの規格化が目標だったが、2022年末以降に延期された。
    - Ø *GSWG（GNSS SARPS Working Group）の下にアドホック会合を設けて検討中。*
- NMA：Navigation Message Authentication
  - SBASメッセージの認証情報をSBAS信号により送信する。
    - Ø *MAC（メッセージ認証符号）：認証に直接用いる短い符号。*
    - Ø *ディジタル署名：MACの偽造を防止するための、十分な暗号強度をもつ署名。*
    - Ø *ディジタル署名の偽造防止：トップレベルの認証鍵を受信機に内蔵させる。*
      - u 通常は認証局による公開鍵証明書が使われる。
  - 現在のところ、L1及びL5のI-chについてオプションとして規格化する方向。
    - Ø *毎秒250ビットしか伝送容量がない：TESLA方式を採用。*
    - Ø *既存SBAS規格にメッセージタイプを追加する（非対応受信機は処理しないだけ）。*

認証メッセージ



- 直前の5メッセージに対応するMAC（メッセージ認証符号）を6秒毎に送信する。
  - Ø *MAC：メッセージ当たり16ビット、メッセージの認証に直接用いる符号*
- TESLA方式：MACの生成にはキーチェーン（ハッシュ値のシーケンス）を使用。
  - Ø *一方向ハッシュ関数で生成したキーチェーンを生成順と逆の順序で使用。*
    - u 送信順にたどることはできない：将来のハッシュ値は予測できない。
  - Ø *MACの生成に使用したハッシュ値を、一つ後の認証メッセージで送信する。*
    - u 認証対象のメッセージが認証されるまでに7～11秒の遅れを生じる。
  - Ø *キーチェーンの最終ハッシュ値に対して、ディジタル署名を付して偽造を防止する。*

必要な伝送容量

- 規格案として提案されているMT20及びMT21（L5 SBASではMT50とMT51）について、必要な送信回数は次の通り。

MT	所要数	送信間隔（s）	帯域占有率（%）
20	1	6	16.67
21 (Level 3)	4	9	11.11
21 (Level 1 & 2)	8		
合　計			27.78

- MT20（L5 SBASではMT50）：MAC（メッセージ認証符号）
  - Ø *直前の5メッセージのMACを含む。6秒毎に送信する必要がある。*
- MT21（L5 SBASではMT51）：キーチェーンに対するディジタル署名等
  - Ø *ある程度定期的に送信されればよい。*
- あわせて、少なくとも30%程度の伝送容量が必要。
  - Ø *L5 SBASでは大きな問題はない。現用のL1 SBASでは工夫により可能な見込み。*

プロトタイプの開発

MSAS

当所受信設備

MSAS
メッセージ

MT63を
MT21で置換

MT21（署名）
生成

MT2〜4を
MT6／20で置換

MT20（MAC）
生成

キーチェーン
生成（1週間分）

ディジタル署名
生成

あらかじめ生成

秘密鍵

認証鍵

鍵ペア

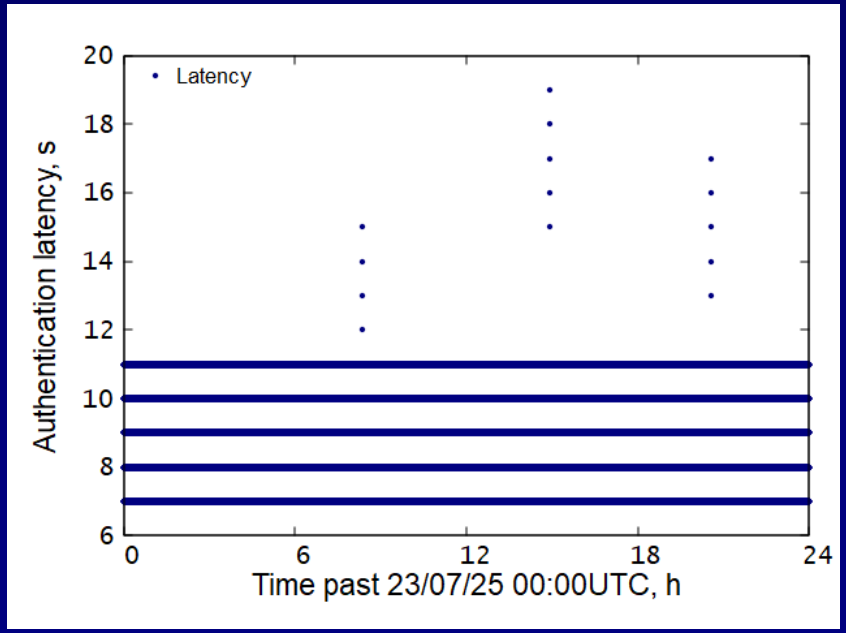
出力
メッセージ

受信機側
ソフトウェア

認証メッセージ生成
プロトタイプ
MIVEX-AUTH

プロトタイプの開発

- ICAO NSPで提案されているMT20/21のフォーマットに沿って、実際に認証メッセージを生成する。
  - Ø *MSASが送信したメッセージについて、MT6を使用したメッセージの置換えを行う。*
  - Ø *空いたスロットに、MT20及びMT21を生成して格納する。（L1 SBASでの工夫点）*
- フリーソフトウェアの暗号ライブラリLibgcryptを使用。
- 受信機側ソフトウェアも作成し、メッセージ認証が行われることを確認した。



例：認証処理の遅れ時間

- 7～11秒で設計通り
- アラートシーケンスがあると遅れる

サンプルメッセージの例

```
# SBAS Authentication by ENRI/MPAT 2023-05-13T04:08:46Z
#  REFERENCE: Draft SARPS (JWGs/9-IP20, TESLA Little-MAC) revised on 2022-09-06
#  GENERATOR: MIVEX-AUTH static L1 (May 13 2023)
#  FORMAT: PRN YY MM DD HH MM SS MT Message
#          Note - Time stamp corresponds to start of transmission of message.
# AES ENCRYPTED LEVEL 1 KEY:
#  0: 6656FA2548A7C133627ACBC0F0993479DB86806B9B6D5CE207E97DE742756C65186C0AF3AF796B936B49A09A18B6E1C2,0
#  1: D361F55715D017F3C547D7D0D46949958A02EF943822FAE020FBA25592A4FB88EDA8CD136285AD87DD5E6A6545802F9A,1
                                                    (中略)
# 15: A1EDD8F70A16318F81B90338A70BF50C1F8EA26765188626A333C5D9909655D26AB43A35AFE7CAD1F2AA60E07A26843C,1
137 22 08 07 00 00 00 28 53731904C2019047FFFF7F3FE7E3FF8000000000000000000000000000E15FC0
137 22 08 07 00 00 01 21 9A552145FE143D14405F0F4C90C569FCE346A5F30A2000000000000031A908C0
137 22 08 07 00 00 02  1 C607FFFFFFFC0000000000000000000000020000000000000000D18501C0
137 22 08 07 00 00 03  2 530AC005FFC001FFDFFFFFDFFFFF9FFDFFDFFDFFDFFE3A3BABA3BBBB99590840
137 22 08 07 00 00 04  6 9A1AA03DFFC001FFDFFFFFDFFFFF9FFDFFDFFDFFDFFE3A3BABA3BBBBB97981C0
137 22 08 07 00 00 05 20 C652998915A2798CCCE8BD880F7AA1AA497968C64A2DA399505BAD4681ECF480
137 22 08 07 00 00 06 28 537355088542304002060 1C0701FF6000000000000000000000000309C9780
137 22 08 07 00 00 07 21 9A56B1457E02474372DF29384DAA0906B37A9863F36B9FBFE8F7E7B5348DE540
137 22 08 07 00 00 08  7 C61C0000000000000000000000000000000000000000000000000FFFDD6D27C0
137 22 08 07 00 00 09  3 530CFFFDFFDFFC005FFFFFDFFFFF9FFDFFDFFDFFDFFE7BA3AFA3BBBBA44CB2C0
137 22 08 07 00 00 10  6 9A1803C5FFC001FFDFFFFFDFFFFF9FFDFFDFFDFFDFFE3A3BABA3BBBBAA4E95C0
137 22 08 07 00 00 11 20 C65243BF5685E4535CAEB3B782B2F6B33580DE406C864490DFD1323A9DF9AC40
137 22 08 07 00 00 12 25 53641B480003FD01D3330201013FD6000000000000000000000000002ED64C0
137 22 08 07 00 00 13 21 9A56B2EBA32EF432793AF826463DEA972E857374A5357232BB9A30174CB79EC0
137 22 08 07 00 00 14 26 C669C841C1AE0BE05702780FD06E83341FE20F10F88BC3DC19E0B6601D5DC8C0
137 22 08 07 00 00 15  4 5311DFFDFFDFFDFFDFFDFFDFFDFFDFFDFFDFFDFFDFFDFFFBBBBBBBBBBBB87E24E40
137 22 08 07 00 00 16  6 9A195007FFC001FFDFFFFFDFFFFF9FFDFFDFFDFFDFFE3A3BABA3BBBB924F0140
137 22 08 07 00 00 17 20 C653C8C63229CCB3F1C624981E7B38448679D9BECB5D8E019A42E6DAB7508CC0
137 22 08 07 00 00 18 28 537379058281804004 01FFC04FEC0780000000000000000000000171E5D80
137 22 08 07 00 00 19 21 9A56B3CE883AF5652EEA76478CB7D0166E78C173BF7FE9B80443C9E2E8B3C840
137 22 08 07 00 00 20 26 C669CC27211B07E037419A10E10F88BC3FC18E0B604E42320FB06E601D0F3280
137 22 08 07 00 00 21  2 530AC005FFC001FFDFFFFFDFFFFF9FFDFFDFFDFFDFFE3A3BABA3BBBB99590840
137 22 08 07 00 00 22  6 9A1AA03DFFC001FFDFFFFFDFFFFF9FFDFFDFFDFFDFFE3A3BABA3BBBBB97981C0
```

トップレベルの認証鍵 (16個)

ディジタル署名

MAC

ディジタル署名

MAC

ディジタル署名

MAC

ディジタル署名

Conclusion

- **SBAS信号によるGNSS信号認証の検討**
  - SBASメッセージの認証情報をSBAS信号により送信する。
  - ディジタル署名技術によるNMA (Navigation Message Authentication)
  - L1 SBAS及びL5 SBAS規格にオプションとして追加することが検討されている。
- **現用L1 SBASでの対応可能性**
  - 現用システム (MSAS) では伝送容量の空きがない。
    - Ø *全体の30%程度 (75bpsに相当) の伝送帯域幅が必要。*
    - Ø *MT2～5 (高速補正) の一部をMT6 (インテグリティ情報) に置き換えることで対応できる見込み。*
- **プロトタイプの開発**
  - MSASメッセージに対して、MT2～5→MT6の置換を行ったうえで、認証メッセージMT20/21を生成する。
  - 生成したメッセージをサンプルとしてEUROCAE及びICAOに提供した。