QBIC海外展開WG
Feb. 4, 2021

2周波SBASの最新動向

坂井 丈泰
国立研究開発法人海上・港湾・航空技術研究所

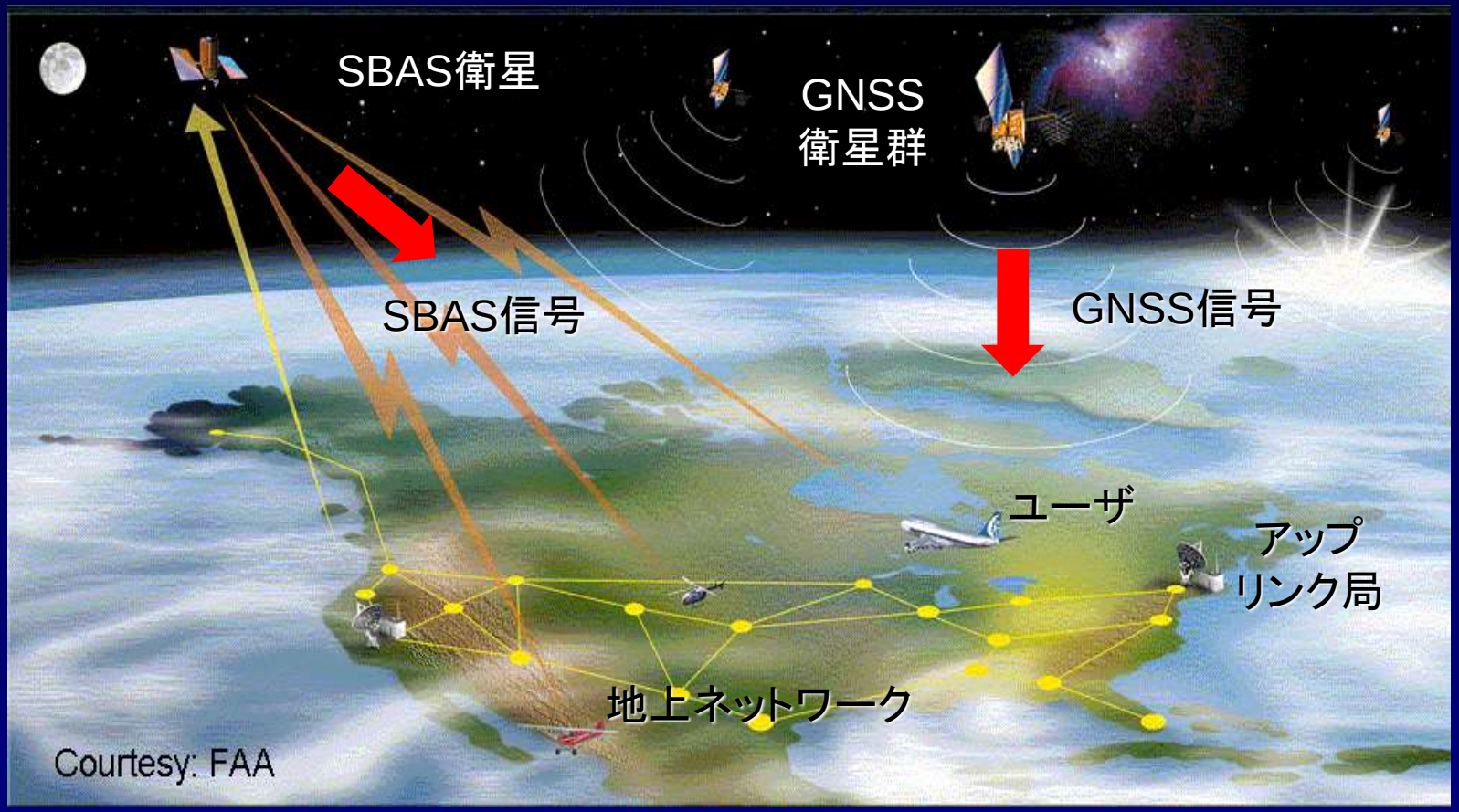
Introduction

- SBAS（Satellite-Based Augmentation System）
  - 補強システム：GPS/GLONASS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GNSSを構成するシステム
  - 現行SBAS = L1 SBAS：L1 C/A信号を使用して静止衛星によりサービス
    - *現行規格は単一周波数・単一システムのみ対応*
- 最近、次世代規格が制定された。
  - L5 SBAS = DFMC SBAS：Dual-Frequency Multi-Constellation SBAS
    - *二周波数の利用・複数コアシステムへの対応*
    - *L5信号を使用、非静止衛星からの送信を許容*
  - ICAO（国際民間航空機関）：2020年末に規格内容が確定、2022年発効予定
  - 信号認証機能（NMA）の導入：使用する信号のトレードオフ検討中
  - 電子航法研究所は準天頂衛星L5S信号を使用して実証実験を実施中
- 今回の内容：

  （1）SBASの仕組み／（2）L1 SBASの現況／（3）L5 SBAS（DFMC SBAS）の規格化

（1）SBASの仕組み

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
- 航空用途向けに開発されているが、非航空分野でも利用可能（規格は公開）

規格化の経緯

- ICAO SARPs（Standards and Recommended Practices）
  - ICAO（国際民間航空機関）による国際標準規格。
    - *航空無線関係は国際民間航空条約の第10附属書（Annex 10）として規定。*
  - 主に地上の航法援助施設の技術仕様を定めている。
    - *すなわち、サービスプロバイダ側の規格。*
- SBAS（Satellite-Based Augmentation System）
  - 補強システム：GPS/GLONASS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GNSSを構成するシステム。
  - 2001年のSARPS第76改訂でGPS・GLONASSとともに取り入れられた。
    - *現行規格（L1 SBAS）では、L1 C/A信号を対象として静止衛星によりサービス。*
    - *現行規格は単一周波数・単一システムのみ対応。*
- RTCA MOPS（Minimum Operational Performance Standards）
  - 米国RTCAが定める、アビオニクス機器の性能基準。
    - *すなわち、GPS/SBAS受信機側の規格。*
  - SBASについては、SC-159がDO-229（GPS/WAAS MOPS）を策定。

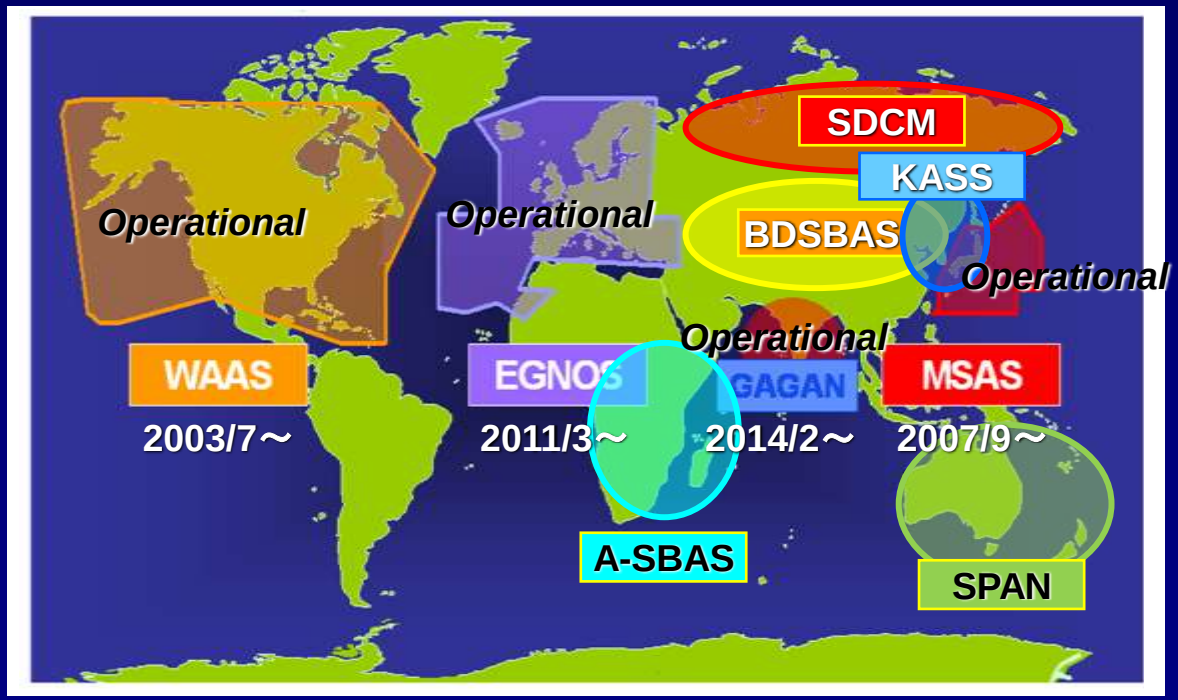
規格化の経緯

- 現行規格：L1 SBAS（2001年発効）
  - 1992～93年頃、日米欧がそれぞれSBASの整備を決定。現在サービス中。
    - *米国WAAS（2003年）・日本MSAS（2007年）・欧州EGNOS（2011年）・インドGAGAN（2014年）*
  - ICAOで標準化作業を開始、並行してRTCA MOPSが策定された（1996年）。
- 次世代規格：L5 SBAS（2022年発効予定）
  - 2004年頃にSBAS IWGで議論が開始された。
    - *SBAS IWG（Interoperability Working Group）：SBASプロバイダによる会合*
  - 2012年頃から具体的な内容を議論。2015年に欧州がICD案を提示。
    - *2016年秋にSBASプロバイダ各国がICD案（v1.3）に合意、ICAOに提示。*
  - 2016年末のICAO NSP/3会議で具体案の検討を開始。
    - *担当はNSP（航法システムパネル）会議*
    - *詳細な議論はDS2SG（DFMC SBAS SARPS Subgroup）にて行われている。*
  - 2020年末の会議で規格内容が確定した。2022年発効予定。
  - 欧州EUROCAEが主導してMOPSの策定作業中（EUROCAE WG-62）。

（2）L1 SBASの現況

SBASの普及

- 運用中のSBAS：すべてL1 SBAS
  - WAAS（米国、2003～）：段階的な改良を経て、現在はLPV200（CAT-I相当）モードまでサービス。2014年に二周波数対応の開発を開始、L5信号を試験的に送信中。
  - MSAS（日本、2007～）：現在はEnroute～NPAのサービス。航空局が整備・運用。2020年度から準天頂衛星3号機（GEO）を使用してサービスを継続。
  - EGNOS（欧州、2011～）：現在はLPV200モードまでサービス。二周波数対応及びGalileo対応のEGNOS V3を開発中。
  - GAGAN（インド、2014～）：Enroute～LPVをサービス。
- 整備中のSBAS：
  - ロシア：SDCMを整備中。静止衛星3機から試験送信中。
  - 中国：BeiDouの一部としてBDSBASを整備中。
  - 韓国：KASSを2022年頃に予定。
  - オーストラリア：SPANの試験中。
  - アフリカ：A-SBASの試験中。NIGCOMSAT-1Rを使用。



サービスプロバイダIDの割当て

SPID	プロバイダ	SPID	プロバイダ
0	WAAS（米国）	6	KASS（韓国）
1	EGNOS（欧州）	7	A-SBAS（アフリカ・ASECNA）
2	MSAS（日本）	8	SPAN（オーストラリア）
3	GAGAN（インド）	9～13	予備
4	SDCM（ロシア）	14, 15	予約
5	BDSBAS（中国）	16～31	予備（L5 SBASで使用できる）

- サービスプロバイダID:
  - MT17（SBASアルマナック情報）に書き込まれており、当該SBAS信号を送信しているSBASプロバイダがわかるようになっている。
  - 今秋のSARPS改訂で表のとおりになる予定で、A-SBASとSPANが追加される。
  - SPID 9～13はまだ空いており、今後あらわれるプロバイダが使用できる。
  - SPID 16～31はL1 SBAS（SPIDに4ビットしか割り当てられていない）では使用できないので、L5 SBASのみを送信するプロバイダが使用できる。

PRN番号の割当て

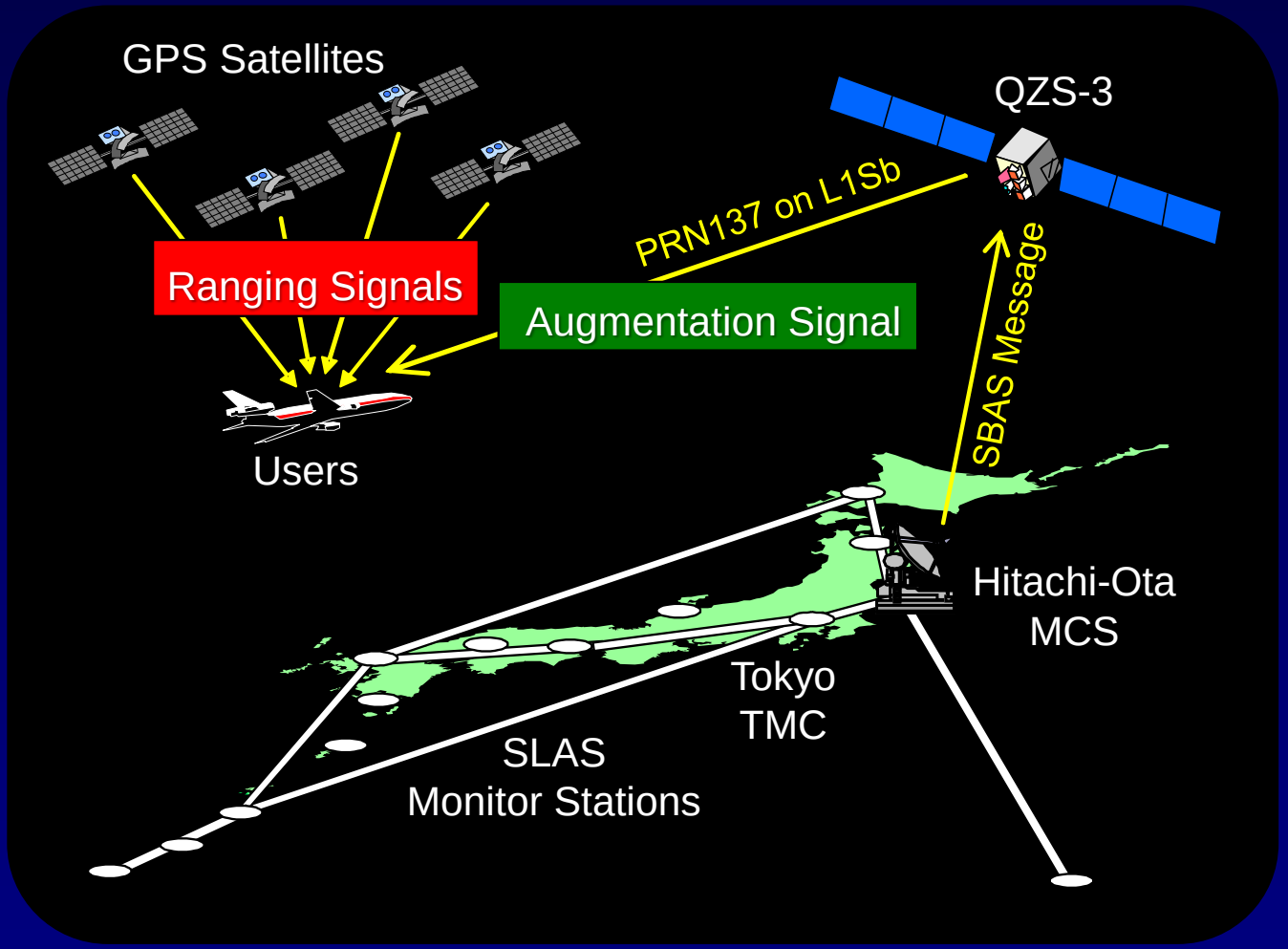
PRN	SBAS	静止衛星	位置
120	EGNOS	—	—
121	EGNOS	Eutelsat 5WB	5W
122	SPAN	INMARSAT 4F1	143.5E
123	EGNOS	ASTRA 5B	31.5E
124	EGNOS	—	—
125	SDCM	Luch-5A	16W
126	EGNOS	INMARSAT 4F2	63.9E
127	GAGAN	GSAT-8	55E
128	GAGAN	GSAT-10	83E
129	MSAS	MTSAT-2	145E
130	BDSBAS	G6	80E
131	WAAS	Eutelsat 117 WB	117W
132	GAGAN	GSAT-15	93.5E

PRN	SBAS	静止衛星	位置
133	WAAS	SES-15	129W
134	KASS	MEASAT-3D	91.5E
135	WAAS	Intelsat Galaxy 30	125W
136	EGNOS	SES-5	5E
137	MSAS	MTSAT-2	145E
138	WAAS	Anik F1R	107.3W
140	SDCM	Luch-5B	95E
141	SDCM	Luch-4	167E
143	BDSBAS	G3	110.5E
144	BDSBAS	G1	140E
147	NSAS	NIGCOMSAT-1R	42.5E
148	ASAL	ALCOMSAT-1	24.8W

（規格範囲は120～158、記載のない番号は空き）

- PRN番号
  - それぞれのSBAS衛星には固有のPRN番号が割り当てられている。
  - IS-GPS-200にAdditional PRN Code Sequencesとして記載されているものと同じ。
  - 当初の規格では120～138だったが、数年前に139～158が追加された。
    - *後発プロバイダに割り当てられている。また、試験送信の際には139以降を使用する。*

MSASの概要（現状）



- 静止衛星（QZS-3）1機、主統制局（MCS）1局、バックアップ局（TMC）1局
- 地上監視局（GMS）としてはSLAS監視局（13局）を使用
- MCSがSBASメッセージを生成し、QZS-3にアップリンクする。L1Sb信号で送信

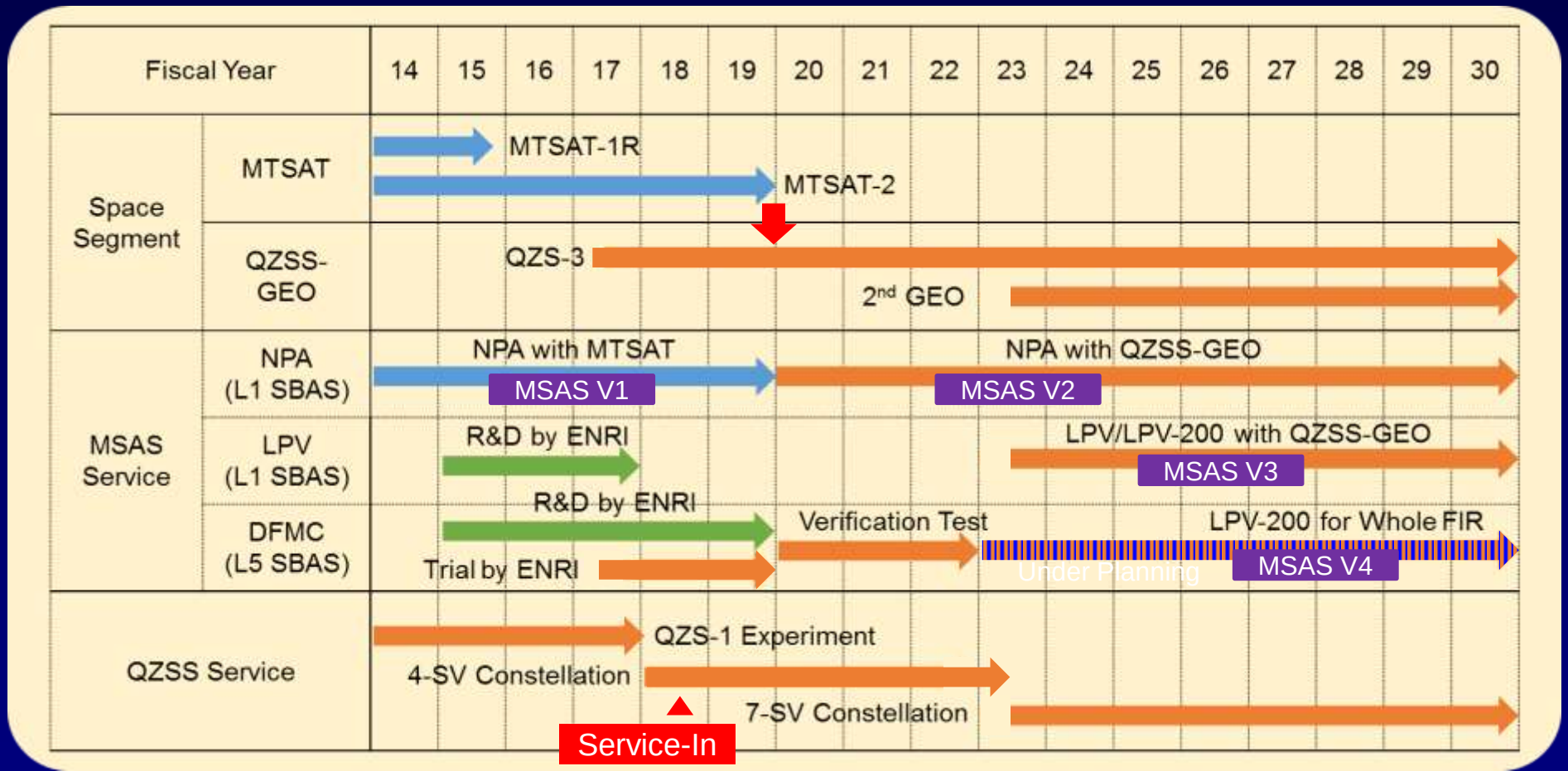
MSASの更新

- 2020年3月まで：旧システム＝MSAS V1
  - MTSAT-1R/-2を使用して、2007年9月27日に運用を開始。
  - MTSAT-1Rは2015年に運用を終了。
  - 2015年にMRS 2局（ハワイ・オーストラリア）を運用終了。
  - 地上施設の機器（MSAS-96）が老朽化しており、運用継続が困難だった。
- 2020年4月から：現行システム＝MSAS V2
  - 2020年3月末に、QZSS（準天頂衛星システム）の静止衛星に切替えを実施。
    - *QZS-3が備えるL1Sb信号を使用する。PRN137をMTSAT-2から引き継いだ。*
    - *世界初の軌道上でRF信号を生成するSBASとなった（他のSBASはすべてベントパイプトランスポンダ方式）。*
  - 同時に、MCS（主統制局）機器も更新された。
    - *MCS設備を常陸太田に設置。TMC（所沢）にバックアップ装置を配置。*
    - *GMS（地上監視局）としては、SLAS監視局（国内13局）を使用する。*
  - 性能・機能はMSAS V1と同等（航空路～NPA：水平航法のみ）。
    - *ただし、レンジング機能はなし。*

今後の計画

- 2023年：LPV性能向上＝MSAS V3
  - MSASの性能向上を実施し、垂直ガイダンスの提供を開始する。
    - *LPV（Localizer Performance with Vertical Guidance）航法モードを実現。*
  - SBAS衛星2機を追加する。
    - *SBAS信号の継続性を確保するために必要。*
    - *QZSSの7機体制で追加されるQZS-6/-7を使用する。*
  - このために必要な補強アルゴリズムを開発中。
- その後：DFMC対応＝MSAS V4
  - DFMC（二周波数・複数コアシステム）対応による性能向上。
    - *電離圏伝搬遅延の影響を受けないロバストな航法。*
    - *LPV/LPV-200航法モードをサービスエリア全域で安定的に供用可能。*
  - DFMC対応SBASは、L5 SBASとして規格化された。
    - *準天頂衛星システムが適合するよう調整。*
    - *準天頂衛星L5S信号を使用して、2017年夏から実証実験を実施中。*

全体スケジュール



- MSAS V1：2007年に運用を開始した旧システム（MTSATを使用）。
- MSAS V2：QZSS静止衛星への切替え・地上施設の更新（2020年）
- MSAS V3：LPV対応のための性能向上・静止衛星追加（2023年頃予定）
- MSAS V4：DFMC対応のL5 SBAS（2017年～実証実験を実施中）

（3）L5 SBAS（DFMC SBAS）の規格化

L5 SBASの特徴

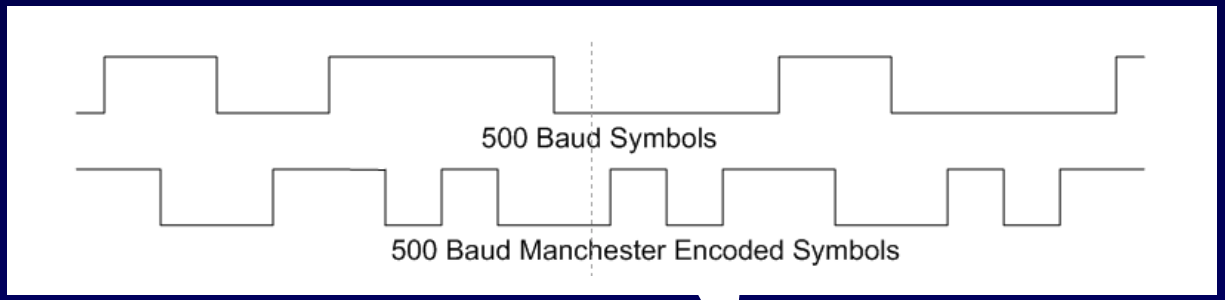
- L1 SBASとは独立した規格：L1 SBAS信号を受信する必要はない
  - L1 SBASのみ（現状はすべてのSBASが該当）・L5 SBASのみのサービスプロバイダも想定されている。
- 二周波数の利用
  - ユーザ受信機は、L1/L5の電離圏フリー線形結合擬似距離を使用する。
    - *電離圏伝搬遅延に影響されないロバストな測位。*
  - 電離圏遅延補正は送信しない。
    - *L1のみ・L5のみといった一周波数モードはいずれもサポートしない。*
- 複数コアシステムに対応
  - 補強対象：GPS・GLONASS・Galileo・BeiDou・SBAS
    - *システム間バイアスは未知数として処理する。*
- 非静止衛星によるSBASを考慮
  - 準天頂衛星を含む非静止衛星からSBAS信号を送信できる。しかしQZSSのみ？
- 信号認証機能の導入
  - L5 SBAS信号にて、信号認証機能（NMA）を導入するための議論が行われている。

L5 SBAS :RF仕様

項目	L5 SBAS	L1 SBAS	備考
周波数	1176.45 MHz	1575.42 MHz	GPSと同じ
帯域幅	20～24 MHz	≧ 2.2 MHz	
変調方式	BPSK		QPSK化の可能性あり
変調速度	10.23 Mcps	1.023 Mcps	
拡散符号	PRN 120～158		当初は120～138
符号速度	1 Ksps	500 sps	
符号化	½ FEC マンチェスター符号	½ FEC	K=7
データ速度	250 bps		
メッセージ長	250 ビット		
プリアンブル	4ビット 6パターン	8ビット 3パターン	GPSサブフレームに同期
CRC長	24ビット		$P_E<10^{-7}$

NH符号なし

メッセージのフォーマット

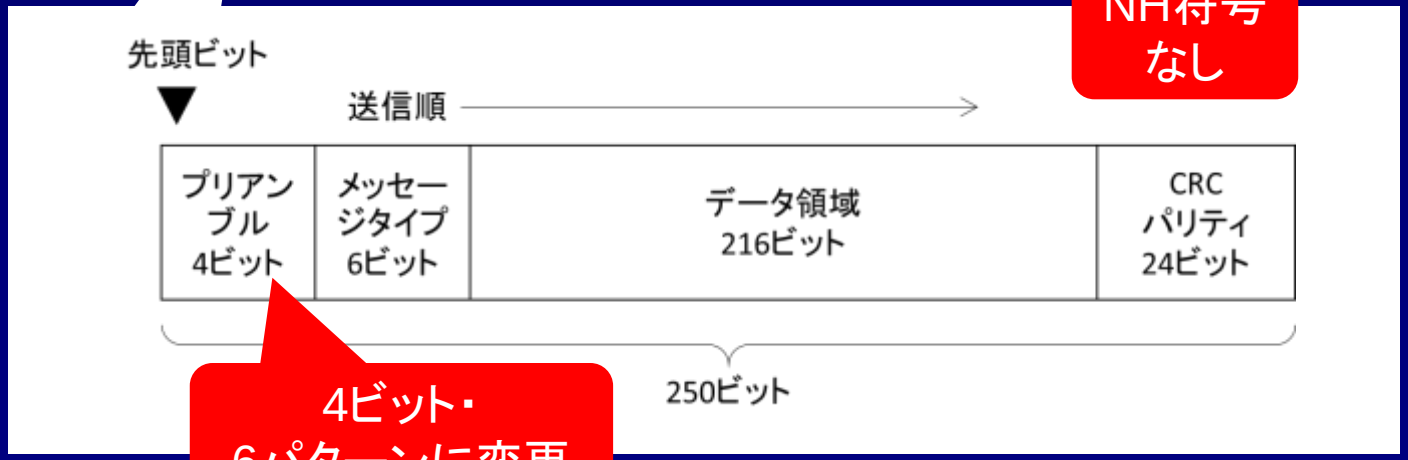


メッセージ → FEC符号化 K=7 → マンチェスター符号化 → BPSKで送信

250 ビット　500 シンボル　1000 シンボル

NH符号なし

オプションで QPSK化の可能性あり



4ビット・6パターンに変更

L5 SBAS：補強機能

項目	L5 SBAS	L1 SBAS	備考
補強対象	GPS・GLONASS・Galileo・BeiDou・SBAS・（QZSS）	GPS・GLONASS・SBAS	QZSSを加えるよう提案中
対応衛星数	214	210	
同時補強衛星数	92	51	
補強対象の擬似距離	L1 C/A + L5 電離圏フリー線形結合 （2周波数モードのみ）	L1 C/A （1周波数モードのみ）	L5のみの1周波数モードはない
補正情報	クロック補正 軌道補正	高速補正 クロック補正 軌道補正 電離圏遅延補正	SAは想定しない
SBAS衛星	制約なし	静止衛星のみ	レンジング機能はオプション

メッセージタイプ

MT	名称	内容	レンジング機能	補強機能
0	Do Not Use for SBAS	使用禁止	—	—
31	SBAS Satellite Mask	補強対象衛星を通知	○	○
32	Satellite Clock-Ephemeris Corrections and Covariance Matrix	各衛星の補正値と共分散行列（1衛星分）	—	○
34	Integrity Information Message	インテグリティ情報（DFREIの変化分を送信）	○	○
35/36	Integrity Information Message	インテグリティ情報（DFREIをそのまま送信）	○	○
37	Degradation Parameters and DFREI Scale Table	劣化係数及びDFREI→σ_{DFRE}テーブル	○	○

（○：必要、—：オプション）

- MT34と、MT35/36は、どちらかを送信すればよい。
  - *各衛星について6秒毎以内にインテグリティ情報が送信されるようにする。*
- MT37の劣化係数はコアシステム別に送信する。

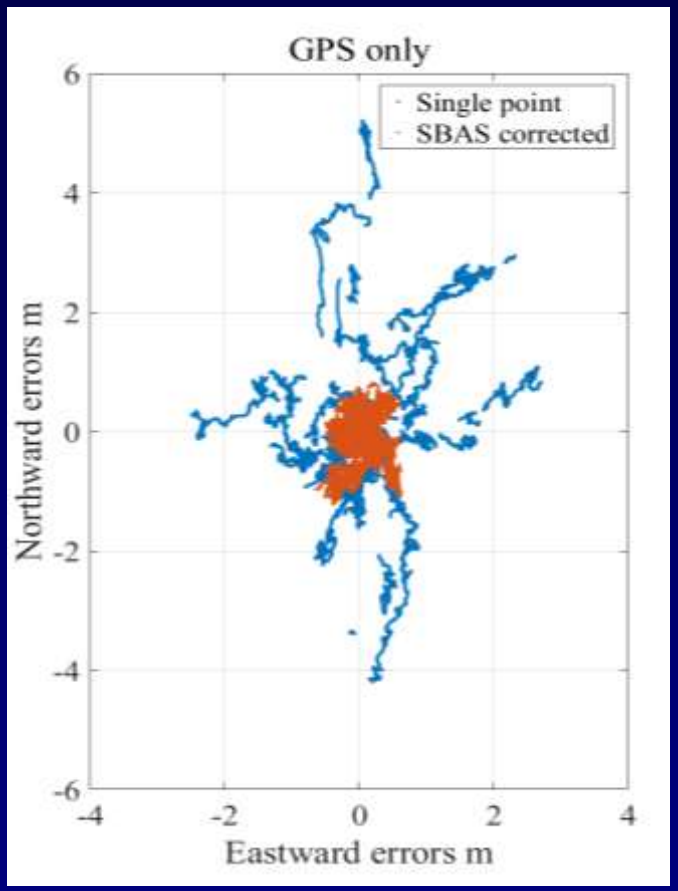
メッセージタイプ

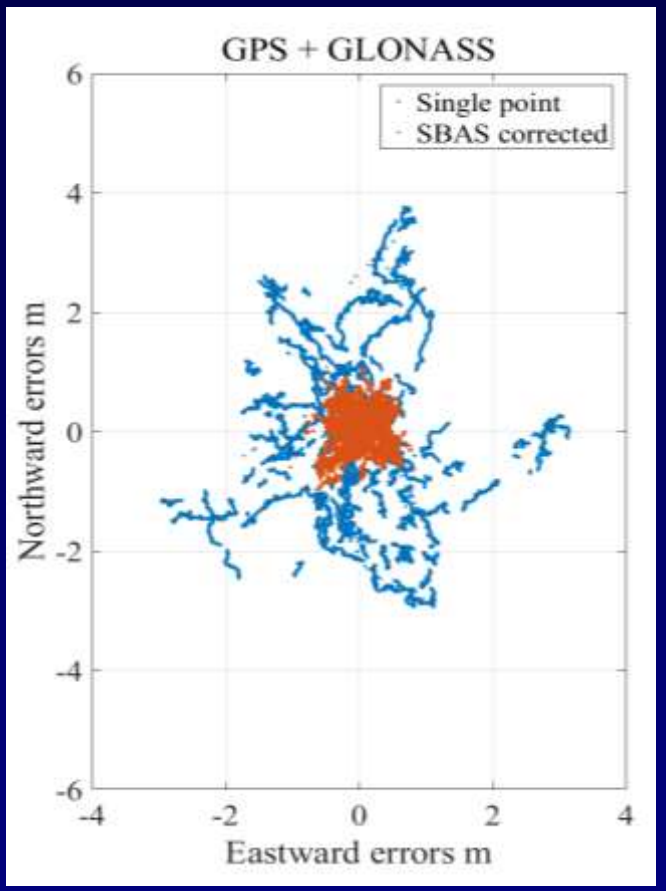
MT	名称	内容	レンジング機能	DF補正機能
39/40	SBAS Satellite Clock, Ephemeris and Covariance Matrix	SBAS衛星のエフェメリス情報と共分散行列（1衛星分）	○	—
42	GNSS Time Offset	時刻オフセット情報（コアシステム別）	—	—
47	SBAS Satellite Almanacs	SBAS衛星のアルマナック情報（2衛星分）	○	○
62	SBAS Internal Test Message	内部テスト用（内容は任意）	—	—
63	Null Message	空のメッセージ	—	—

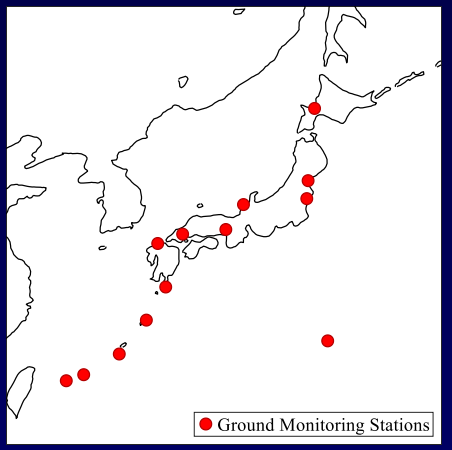
（○：必要、—：オプション）

- MT39/40は、セットで送信する。
  - *非静止衛星も表現できるようにケプラー要素による表現を採用。*
  - *アルマナック情報（MT47）もケプラー要素に変更されている。*
- MT42はオプション。
  - *実際は送信しないプロバイダが多数派と思われる。*

プロトタイプによる検証





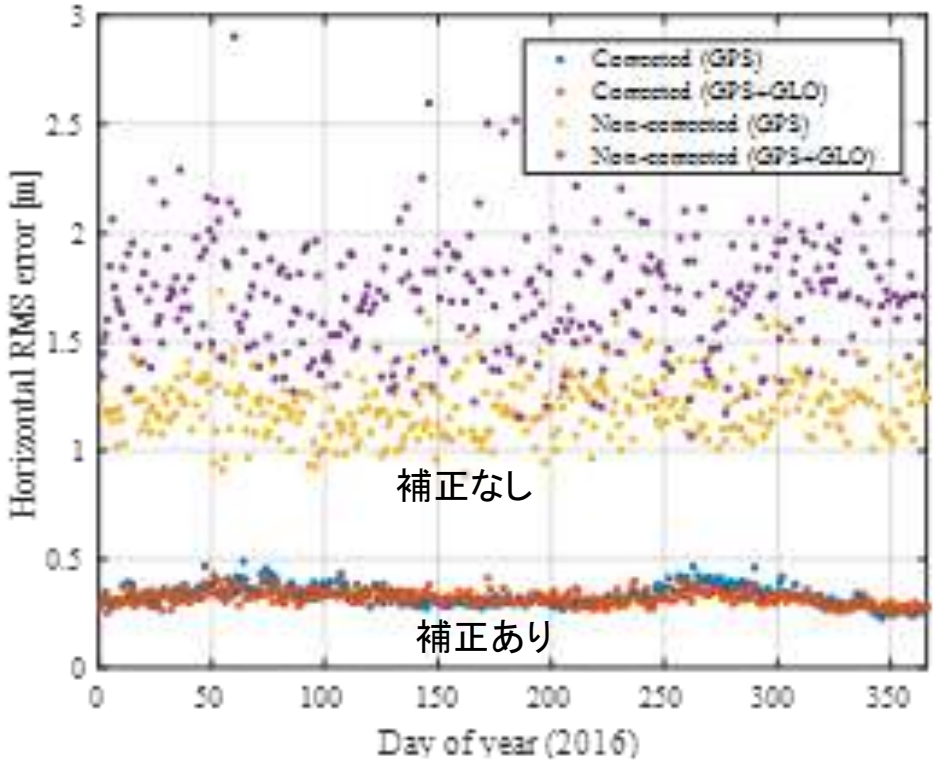


モニタ局の配置

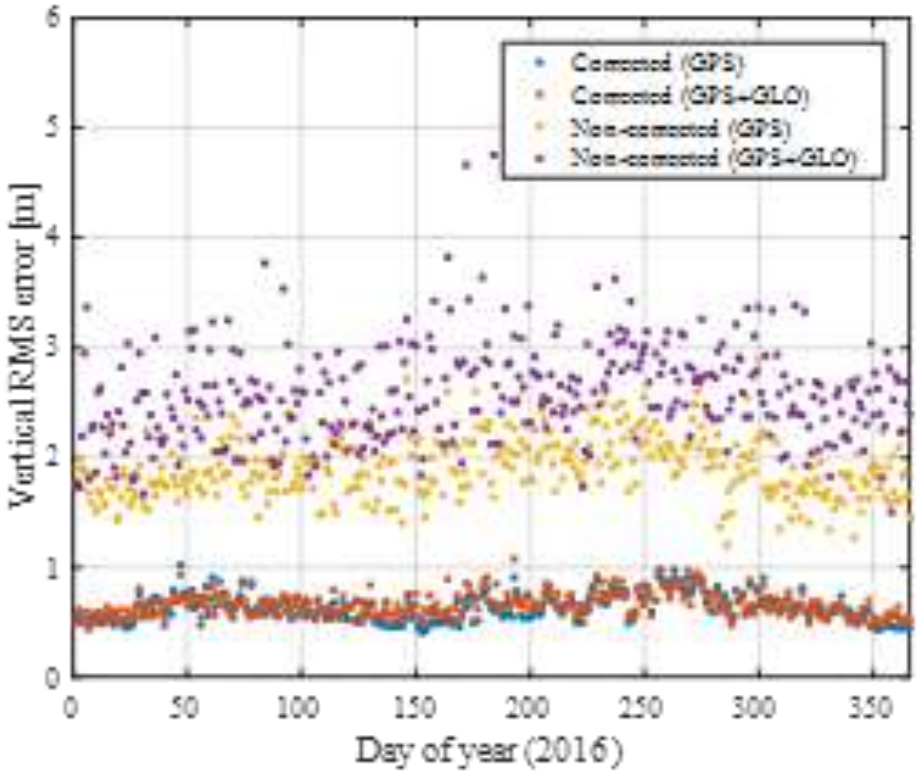
- Dual Frequency
- DFMC L5 SBAS
- Location:
  GEONET 950369
  (Wakayama)
- Period:
  2016/12/15 (24H)

- 規格化作業中のドラフト規格に沿ってメッセージを生成するプロトタイプシステムを構築。
  - *GPS/GLONASS対応、L1/L2二周波数モードで動作。*
  - *プロトタイプシステムが生成したメッセージを、擬似ユーザ受信機で評価。*
- DFMC SBASメッセージにより、GPSモード・GPS+GLONASSモードのいずれも精度を改善。

プロトタイプによる検証



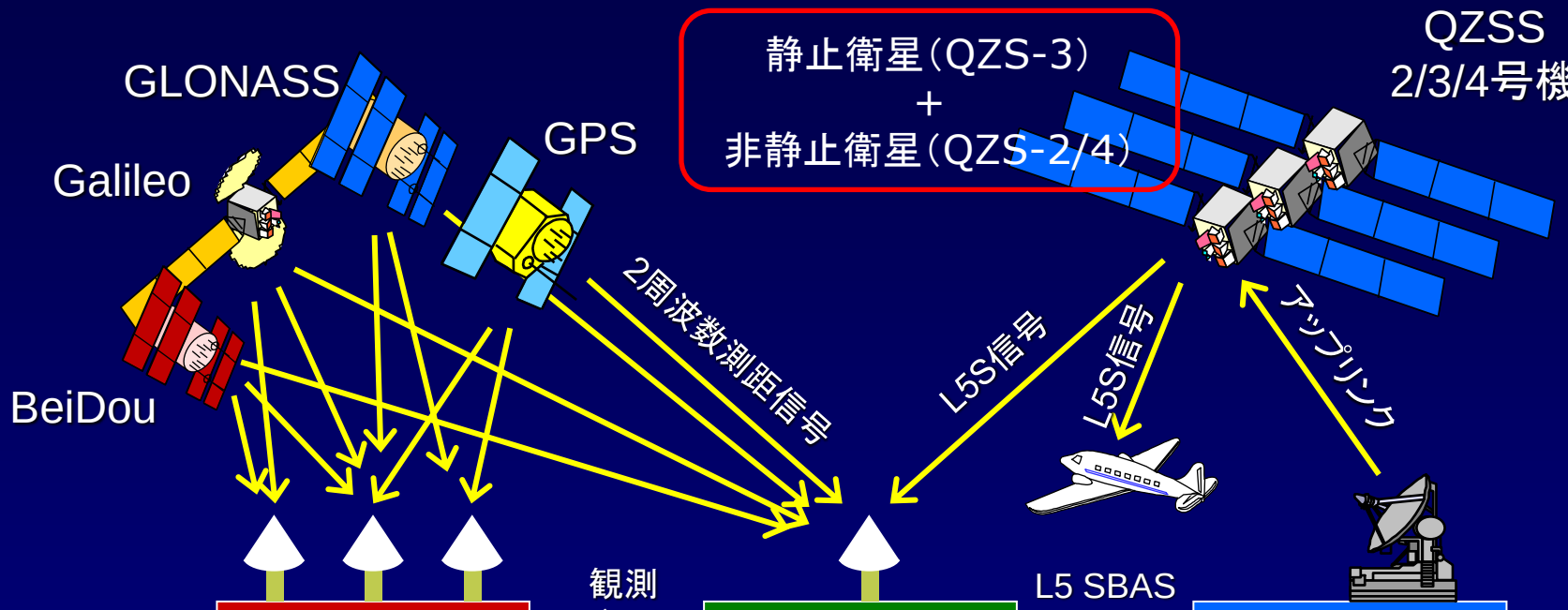
水平測位精度



垂直測位精度

- 1年間にわたる評価を実施（対象地点：GEONET 950369 Wakayama）
- 年間を通じて安定した測位精度が得られる：水平 ~0.5m、垂直 ~1m

実証実験の構成

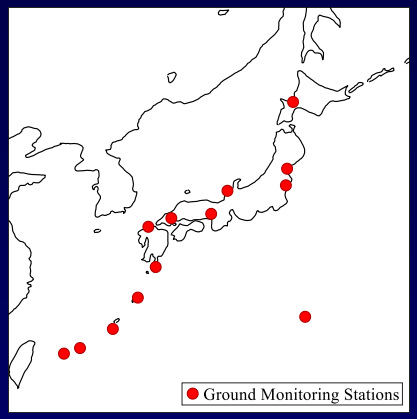


- 観測データをリアルタイム送信
- 二周波数・複数システム対応

- リアルタイム動作
- GPS/GLONASS/Galileo/QZSS対応
- L5 SBASメッセージを出力

- L5 SBASメッセージを準天頂衛星にアップリンク
- L5S信号により送信

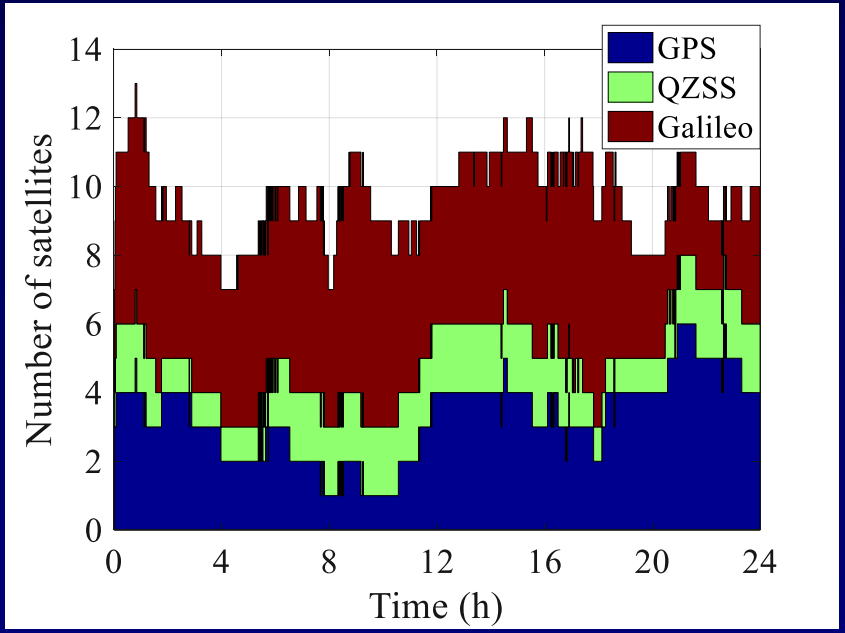
準天頂衛星L5S信号による実験



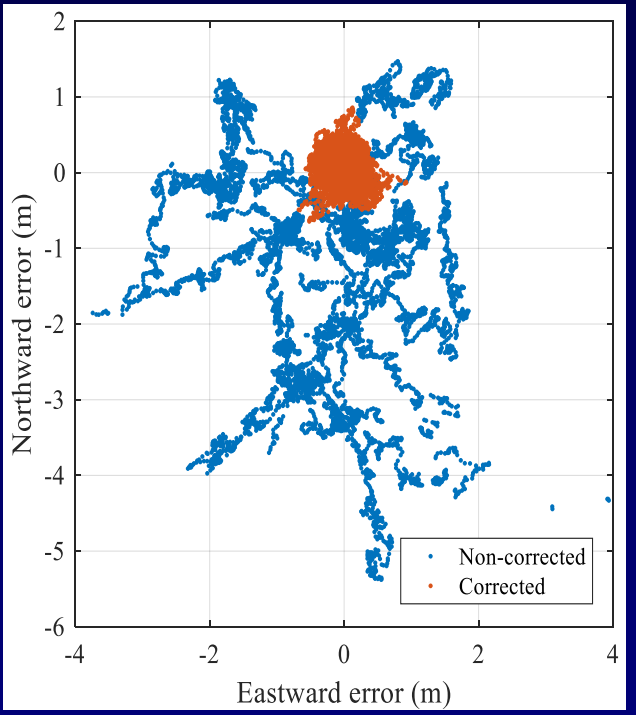
13 Monitor Stations

- Dual Frequency
- DFMC L5 SBAS
- Location:
  GEONET 950369
  (Wakayama)
- Period:
  2017/12/13 (24H)

GPS + Galileo + QZSS



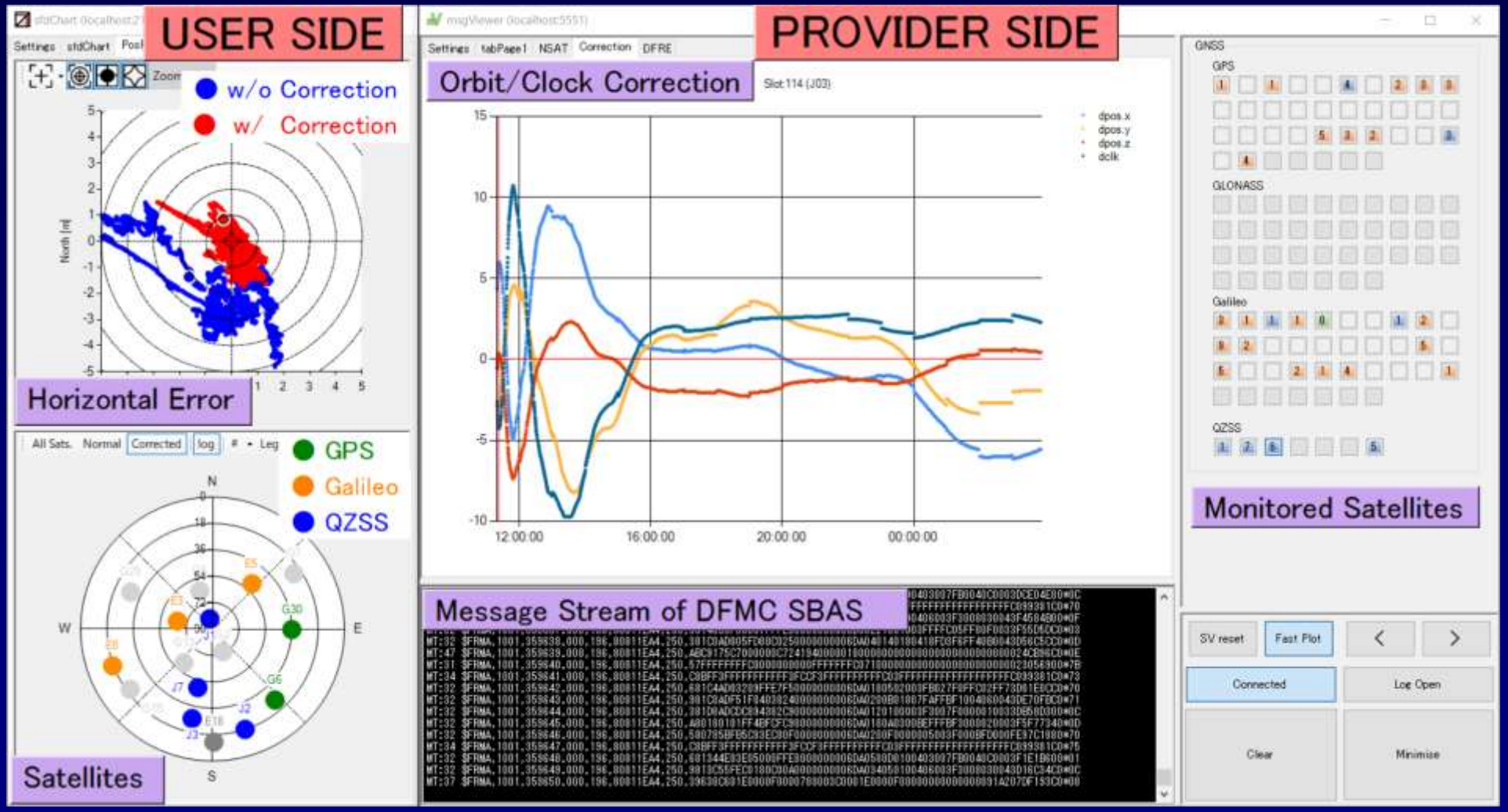
Message Generation



User Side Test

- L5 SBASメッセージをリアルタイムに生成し、評価した例。
  - *GPS/Galileo/QZSS対応、L1/L5二周波数モードで動作。監視局：国内13局*
  - *プロトタイプシステムが生成したメッセージを、擬似ユーザ受信機で評価。*
- L5 SBASによりGPS+Galileo+QZSSの補強が可能であることを確認。

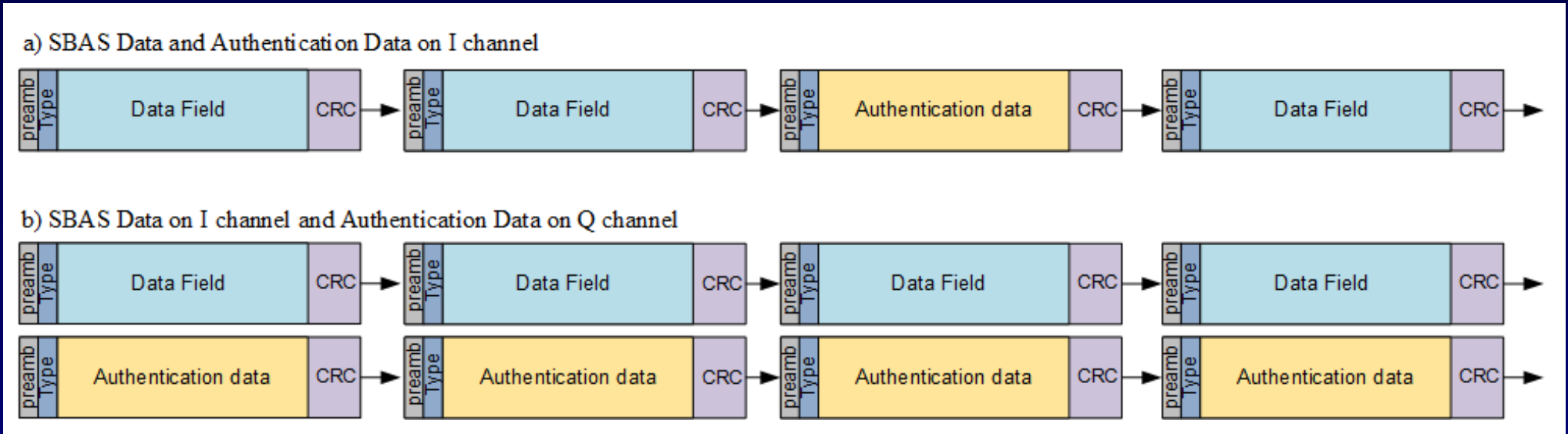
準天頂衛星L5S信号による実験



SBASによるGNSS信号認証

- SBASによる信号認証
  - 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。
    - *NSP JWGs/2（Navigation Systems Panel - Joint Working Group）WP/10*
  - 欧州はEAST（EGNOS Authentication Security Test-Bed）プロジェクトにより検討してきた。
    - *GalileoについてもI/NAVメッセージにNMAを付与することとしている。*
  - 2020年末までの規格化が目標だったが、2021年末に延期された。
    - *当面はL5 SBAS規格本体の制定に注力する。*
- NMA：Navigation Message Authentication
  - 航法メッセージの認証情報（及び公開鍵）をSBAS信号により送信。
    - *オプション：I-ch or Q-ch、L1 or L5、暗号化方式：TESLA or ECDSA*
  - OTAR：On-the-Air Rekeyingによる公開鍵の更新
    - *送信頻度とTTFA（Time to First Authentication）の兼合い*
  - 現在のところ、L5 Q-chで送信することになる方向。

オプション: I-ch or Q-ch



- L5 SBAS I-chにはすでにDFMC SBASメッセージがある。
  - *空きがどの程度か。逆に、どの程度の空きがあればNMAを送信できるか。*
- L5 SBAS Q-chはまだ使われていないので、空いている。
  - *ただし、Q-chに信号を乗せると、他信号にとってはL5帯の雑音が増える。*
    - ◆ このため、データレートを下げて送信電力を抑える議論があった。
  - *量子計算機に耐える方式とするには、Q-ch で十分なデータレートを確保すべき。*

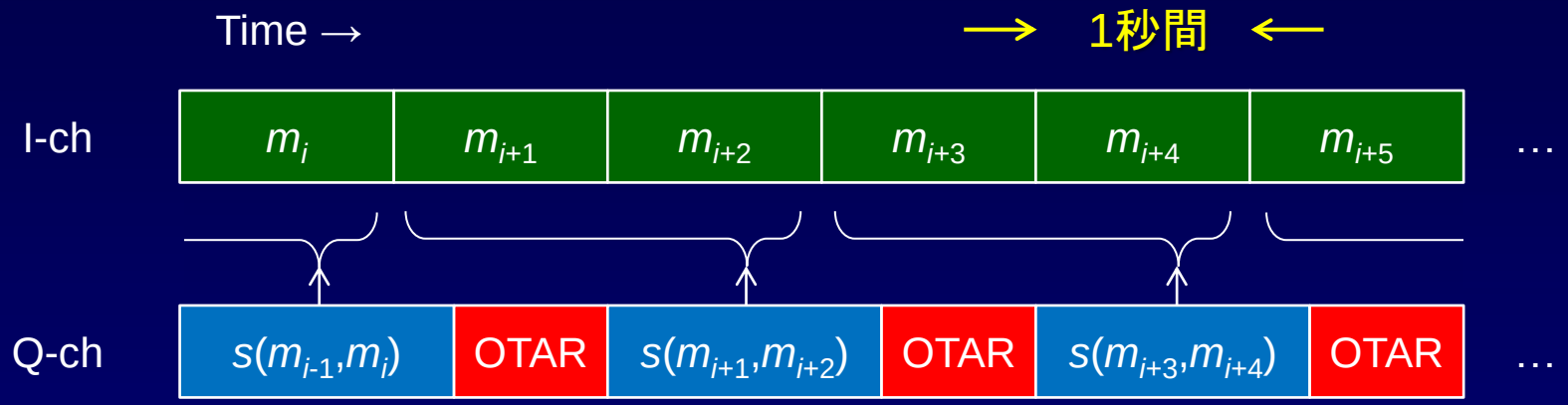
ベースライン

標準的に用いられる楕円曲線とセキュリティレベル

楕円曲線	セキュリティレベル（ビット）	公開鍵長（ビット）	ディジタル署名長（ビット）
P-192	96	192	384
P-224	112	224	448
P-256	128	256	512
P-384	192	384	768
P-521	256	521	1042

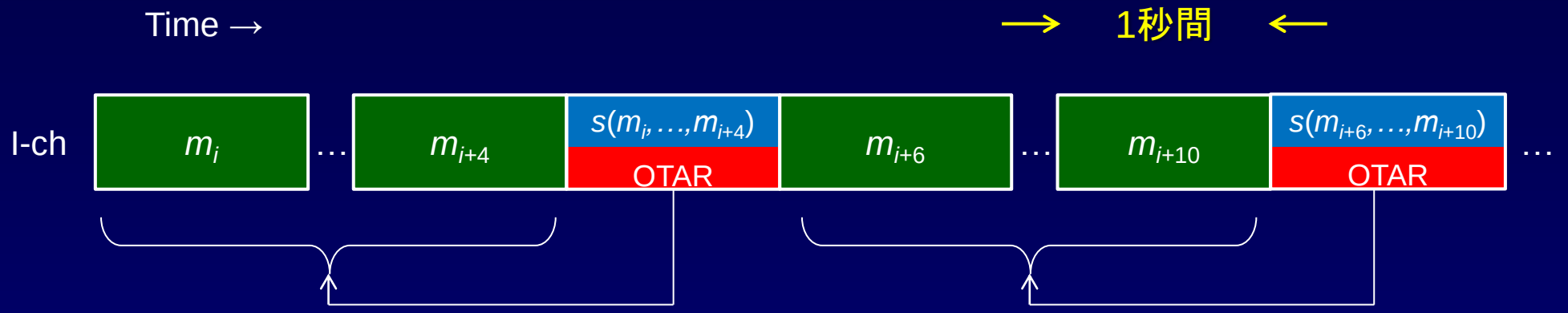
- P-256以上の使用が推奨されているが、P-224程度を採用する方向。
  - *GNSS信号認証では認証情報の寿命が短いので、暗号強度を多少落としてもよい。*
  - *Q-ch（毎秒250ビット）を使用する想定であっても、伝送容量に余裕がない。*
- 448ビットのディジタル署名を2秒間で送信する。
  - *プリアンブル及びCRCパリティを省略し、毎秒250ビットのすべてをNMAに利用する。*
- OTARのための鍵情報はECDSAで送信する。
  - *メッセージ認証情報を送信した残りの伝送帯域を使用する。*

Q-chの利用:ECDSAによるNMA



- ECDSA P-224によるディジタル署名情報を直接送信する。
  - *I-chで送信されるSBASメッセージに対するディジタル署名をQ-chで送信する。*
- 448ビットのディジタル署名を2秒間で送信する。
  - *Q-chについてはプリアンブル及びCRCパリティを省略し、毎秒250ビットのすべてをNMAに利用する。*
  - *SBASメッセージ2個を1組としてディジタル署名を生成する。*
- OTARのためのスペース:52ビット／2秒＝1560ビット／分
  - *試算例:TTFA 64秒、全情報の受信に要する時間は20分以上*

I-chの利用:TESLAによるNMA



- L5 SBAS(I-ch)の空き伝送容量を使用する。
  - *補強対象衛星数にもよるが、経験上1/5～1/6程度の空きがある(図では1/5)。*
- 認証のための鍵情報はキーチェーンとして次々に更新する。
  - *ルートキーから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。*
  - *SBASメッセージと鍵情報から30ビットのMAC(Message Authentication Code)を生成して送信する。*
  - *ルートキーはECDSA暗号により送信する。*
- OTARのためのスペース:68ビット/認証メッセージ
  - *試算例:TTFA 134秒、全情報の受信に要する時間は80分以上*

KPI（性能に関わるもの）

KPI		定　義
APFA	Authentication Probability of False Alarm	認証機能により誤警報を生じる確率
AER	Authentication Error Rate	認証プロトコルに誤りを生じる確率（必要な情報を受信できないなど）
ASA	Authentication System Availability	認証機能を利用できる時間割合
MTBA	Mean Time Between Authentications	認証機能を実行できるタイミングの平均間隔
TTFA	Time to First Authentication	最初に認証機能を実行できるまでの時間
MAL	Maximum Authentication Latency	航法メッセージを受信してからそのメッセージを認証できるまでの最大時間
ATTD	Authentication Time to Detect	スプーフィングが開始されてから検出できるまでの最大時間
ATTA	Authentication Time to Alert	受信機が影響を受け始めてから警報するまでの最大時間
APMD	Authentication Probability of Missed Detection	スプーフィングを見逃す確率

Conclusion

- 次世代SBAS規格の制定に向けた作業が行われている
  - ICAO（国際民間航空機関）／NSP（航法システムパネル会議）
    - *実質的な作業はDS2SG（DFMC SBAS SARPS Subgroup）が担当*
  - 2020年末に規格内容が確定した。2022年発効予定。
- 主な特徴：
  - L1 SBASとは完全に独立した規格
  - 二周波数の利用：電離圏フリー線形結合擬似距離による測位
    - *電離圏伝搬遅延の影響を受けない測位*
    - *低緯度地域を含む全世界でロバストな測位機能を提供できる*
  - 複数コアシステムへの対応
    - *GPS・GLONASS・Galileo・BeiDou・SBAS・（QZSS）*
  - 非静止衛星によるSBASへの対応：IGSOを含む非静止衛星からSBAS信号を送信可
  - 信号認証機能（NMA）の導入：現在、使用する信号のトレードオフ検討中（規格化は2021年以降）
  - L1 SBASに引き続き、非航空分野でも利用可能（規格内容は公開されている）
- 電子航法研究所は準天頂衛星L5S信号を使用して実証実験を実施中
  - QZS-2/3/4を使用して随時送信中