A-012

スプーフィングを対象とした民生用衛星測位システムの脆弱性軽減方法の開発

千野　孝一*[a)]，　Dinesh Manandhar*，　柴崎　亮介*

The development of decrease of vulnerabilities of Civilian GNSS in targeting of spoofing

Koichi CHINO*，　Dinesh Manandhar*，　Ryosuke Shibasaki*

あらまし　民生用途 GPS 信号は広く社会生活のインフラ分野に利用されているが，容易に成りすましされやすく，脆弱性(スプーフィングとミーコニング）を内在している。本論文では，まずスプーフィングのデモから如何に GPS 信号が脆弱であるかを示し，その対応策をナビゲーションメッセージにエラー訂正演算を施すことにより実現できることを示した。次に準天頂衛星システムの地上システム・衛星システム・受信機に秘匿化演算したナビゲーションメッセージを実装するアルゴリスムを示し，最後に秘匿化演算したナビゲーションメッセージが既存の GPS 信号の脆弱性を解決する有望な手段であることをシミュレーションと実験により示した。

Abstract　We address the current situation of the potential vulnerabilities (Spoofing and Meaconing) of Global Positioning System in the field of Civilian Users. In this thesis, we show how the GPS signal is easy to be spoofed and meaconinged by the Spoofing Demonstration, on the contrary ,we show the resolutions by means of implement in encrypted navigation message. We propose the implement of encrypted navigation message to ground system, space system and receiver of Japanese Quasi Zenith Satellite System. The potential vulnerabilities of Civil GPS signal will be resolved by the encrypted navigation message thorough simulation and experiments

␣**キーワード**　GPS,認証，成りすまし，脆弱性

␣**Keyword**　GPS，Authentication，Spoofing，Vulnerability

１．まえがき

GPS アプリケーションはコンシューマ用途のカーナビとスマートフォンによる位置情報サービスから，ミッションクリティカルな社会インフラのアプリケーションへと次第に拡大している。例えば，ミッションクリティカルなアプリケーションとは，電気通信網，銀行オンラインシステムと電力網の時刻同期，航空機誘導，公共交通機関の位置，危険物や産業廃棄物の追跡，電子通行料の徴税，トレーサビリティ関連のアプリケーションである[1] 。アプリケーションの信頼性は民生用 GPS 信号から得られる位置と時刻データに依存している。

GPS 衛星システムでは潜在的な脆弱性（スプーフィングとミーコニング）が問題になる可能性がある。なぜなら，GPS シミュレータとリピータの出現で，スプーフィングまたはミーコニング信号を意図的に生成することが可能である。

さらに，GPS 民生信号の仕様は， ICD- GPS ドキュメント[2]に公開されているので誰でも偽装した信号を生成，送信することができる。ここでスプーフィングとは衛星から送信された経度緯度情報と同じ位置情報をシミュレータ等から送信して成りすます技術である。ミーコニングとは衛星からの信号を受信し，記録し，時間遅れを伴った信号を再送信する技術である。

GPS 信号では，軍事用の暗号化された P-コード信号と民生用の暗号化されていない C/A コード信号がある。 P-コード信号はスプーフィングやミーコニングに対し強いが，C/A コード信号は,スプーフィングやミーコニングに弱い。民生用の C / A コード信号に対し，アンチスプーフィング技術やアンチミーコニング技術への強い期待がある。

*東京大学大学院
〒277-8568　千葉県柏市柏の葉 5-1-5
Centre for Spatial Information Science, The University of Tokyo 5-1-5, Kashiwanoha, Kashiwa-shi, Chiba, 277-8568
a)　chino@iis.u-tokyo.ac.jp

2　スプーフィングとは

ここでスプーフィングの例を図１に示す。いかに簡単に GPS 受信機や PND(Personal Navigation Device)のような任意のデバイスのなりすましができることを示すための例である。

最初に GPS 信号は，東京タワーの位置情報を示す信号が模倣されて送信された。 PND デバイスは，信号の送信から 30 秒内でマップ上に東京タワーの位置を表示した。

次のスプーフィングは，大阪城の位置情報を示す GPS 信号を模倣するように設定された。 PND デバイスは，信号送信から 30 秒内でマップ上に大阪城の位置を示した。

最後に富士山の位置情報を示す信号を模倣するようにスプーフィングの信号を変更した。PND デバイスは，信号の送信から 30 秒内に富士山の位置を地図上に示した。

これらのなりすましのテストの間，PND デバイスは何の警告もエラーメッセージも発行しなかった。あたかも信号が宇宙空間の GPS 衛星から送信されたかのように動作した。画面左側の上隅にある表示時刻を見ると，表示された

ディスプレイは 1 分ごとに異なるのがわかる。現実問題 1 分以内に東京タワーから大阪城に移動するのは不可能であり，再び富士山に戻るのも不可能である。

図1 スプーフィングの例

Fig. 1 Spoofing example of a PND

現在，全地球的航法衛星システム GNSS（Global Navigation Satellite System）のサービスプロバイダーは米国の GPS だけでなく，ロシアの GLONASS も存在しているが，ここ数年以内に，GNSS の他のサービスプロバイダーが増加されて衛星の数は 100 以上になると予想される。このような状況で，民生用途のユーザのために衛星システムの潜在的な脆弱性（スプーフィングとミーコニング）を克服する方法の開発が急務である。現在民生用途の GPS では，認証サービスと補強サービスの両方が不足している。たとえば，2001 年に，米国運輸省 DOT （Department of Transportation）が GPS の民生信号の脆弱性評価を Volpe レポート[3]で公開した。この報告書および他の多くの研究にもかかわらず，民生の GPS 信号がいまだにスプーフィングとミーコニングから保護するために必要なツールを欠いていると指摘されている。なお，新たに設計された近代化 GPS の信号も日本版 GPS の準天頂衛星システム QZSS(Quasi Zenith Satellite System)も，スプーフィングとミーコニングから保護するための機能を欠いている。QZSS の信号だけでなく，他の民生の GNSS 信号は，民生用 GPS 信号と同様に脆弱性がある。

Volpe レポートによると，脆弱性を軽減する方法として，真の GPS 信号との比較で到達時間の差，ドップラーシフト量の差，振幅の差，電磁波の極方向偏差，到達角度の差などが提案されている。しかしながらこれらの差を用いた手法であり，GPS 信号の電気的特性に関係することであり，一般的に利用しやすい軽減策とは言えない。一般的に利用しやすい軽減策は以下のような要件を満足する必要がある。つまり，ナビゲーションメッセージに脆弱性特に，スプーフィングを検知できる仕組みを挿入しておき，受信機においてその仕組みを解読する要件を満足することである。ここで，GNSS で発生するスプーフィングとミーコニング攻撃をチェックするメカニズムを開発するために，既存のシステム内で動作することである。しかし，信号の構造を変更せずに，受信機のアーキテクチャも変更せずに既存の信号と同様なメカニズムを開発することは極めて困難な作業である。さらに，そのような変更が可能であった場合に，既存のアプリケーションへの影響はあってはならない。

3 これまでの技術

これまで，アンチスプーフィングとアンチミーコニングの問題を解決するためにいくつかの推奨方法が提案されてきた。ナビゲーションメッセージに秘密拡散シーケンスである所謂スプレッド拡散スペクトラムコードを挿入して受信機で相関を取る方法，P コードをレファランスとして利用する方法，GNSS 信号の認証に信号認証シーケンス(Signal Authentication Sequence)を利用する方法があるが，問題の処理に独自の制限があった。

たとえば， Scot らの考え 0 は，スプレッド拡散スペクトラムコード(SSSCs ;Spread Sequence Spectrum Codes)はナビゲーションメッセージで送信されて，認証性を検証するため受信機で相関をとるが，このアプローチでは現状の変調スキームに修正が必要であるという制限がある。

Sherman らの考え方[4]は，ユーザの位置とレファランスステーションの位置を P コード信号で比較することによりミーコニングの問題を解決する方法である。その方法はユーザ受信機とレファランスステーションが異なる場所で集められ比較される。Q-チャンネルの生データからドップラーを削除する方法で，そうすれば，もし信号が同じであるならば(信号がスプーフィングされていないならば)，二つの信号の相関を取れば，相関のピーク値はノイズレベルを超えることで証明される方法である。この方法は，信号レベルのコードの暗号化に注力することであり，他の信号を参照として利用する方法であるが，信号処理アルゴリズムの変更を伴うとの制限がある。

また，Pozzobon らの方法[6]は信号の認証にナビゲーションメッセージレベルではなくレンジングコードの信号に暗号化を施すことであり，BPSK 信号の正弦にオープンコード変調を施すために信号変調レベルで暗号化を施す制約があった。

4 位置認証の解決案

GPS 信号の脆弱性にはスプーフィングとミーコニングがある。ミーコニング信号はスプーフィング信号の時間遅れを伴った信号と見なされるので，本論文ではスプーフィング対策手法を論ずることにする。

GPS 信号のナビゲーションメッセージを認証することによって GPS 信号のスプーフィングの問題を解決する方法論を提案する。ナビゲーションメッセージの認証は，QZSS L1C/A 信号または L1SAIF (L1 Submeterclass Augmentation with Integrity Function) 信号を使用して実現される。本提案手法によれば GPS 受信機のハードウェアアーキテクチャの変更は必要ないので，すでに市場に流通している多くのユーザやアプリケーションへ受け入れられ易い。位置データを認証したいユーザは準天頂衛星モニタリングステーションで観測された GPS のナビゲーションメッセージの特定ビットに対し暗号化データを計算し，その暗号化データを L1SAIF 信号と一般の通信手段で提供し，両信号を比較することによって実現できる。この提案手法は，

認証のために受信機のソフトウェア/ファームウェアの変更が小修正であるので既存の GPS 受信機から容易にアップグレードでき，位置情報認証機能を付加できる。現行のＧＰＳシステム，ＧＰＳ衛星，ＧＰＳ受信機の構造を変えることなく，本提案の認証システムをアドインする方針に従って開発を推進した。その結果提案する位置認証の主な特徴は以下の 7 項目となった。

① 受信機のアーキテクチャを変更しない
② 信号捕捉・追跡手順の変更を必要としない
③ ナビゲーションメッセージのデコードにいかなる変更も加えない
④ 信号が認証される必要がある場合にのみ，メッセージのビットの分析をする。
⑤ GPS 信号からナビゲーションメッセージビットを利用して，秘匿化されたデータビットを生成する。このようなデータビットは QZSS L1C/A 信号または L1SAIF 信号を使用して送信される。
⑥ GPS と QZSS の信号構造が同じであるため同一の方法が QZSS 信号の認証に適用可能である
⑦ QZSS L1C/A 信号または L1SAIF 信号を利用すると，PNT（位置，ナビゲーションと時刻）の目的を超えて，準天頂衛星システム特有の新機能（認証機能）が強化されたアプリケーションを提供することが可能である。

5. 解決案の具体例

上記に掲げた目的の解決策をそれぞれについて検討する。

①. 受信機のアーキテクチャを変更しない。

本件は多数普及しているＧＰＳ受信機のハードウェアを変更することは，認証機能の普及の妨げになるとの観点から，第一番目に要件として定義した。つまり，現状普及しているＧＰＳ受信機のファームウェアの変更で変更部分は吸収して，ハードウェアは変更しない。このことにより認証機能ありのＧＰＳ受信機は認証機能なしのＧＰＳ受信機と親和性を持てる。また，昨今普及目覚しい GPS 機能付きのスマートフォンにおいても同様である。

②. 信号補足・追跡手順の変更を必要としない。

認証機能付きＧＰＳ受信機でも当然，測位計算をする。その際，信号補足・追跡手順に変更があると，測位計算を行うＣＰＵのアーキテクチャ，もしくは専用ロジックの変更が発生する。これはハードウェアの変更のみならず，内臓ファームウェアの変更へも影響を受ける。高感度ＧＰＳ受信機など，マルチコリレータ内臓の GPS 受信機ではなおさら，変更がシステムの構成自体に及ぶ可能性もある。

③. ナビゲーションメッセージのデコードにいかなる変更も加えない

ナビゲーションメッセージのデコードは意味あるビット内容を解読してエフェメリス，アルマナックを GPS 受信機に取り込む。この際，ナビゲーションメッセージのデコードに変更が加わっていると，意味のない解読となり，誤った信号を解読したことになる。このことから，我々は現行のナビゲーションメッセージのビット構成を調べ，リザーブビットを調べた。さらに 24 時間Ｘ7 日間それらのリザーブビットを観察し，エフェメリスアップロードの 4 時間に 1 回以外は変化のないことを突き止めた。この観察において，GPS サブフレーム１とサブフレーム 4 に纏まったリザーブビットを見出した，後述するように QZSS においても，リザーブビット構成は基本的に GPS に準拠しており，GPS のリザーブビットを参考にした。加えて，QZSS の補強信号である L1SAIF 信号の空きビット 212 ビットもリザーブビットとして活用した。

④. 信号が認証される必要がある場合にのみ，メッセージのビットの分析が必要である

③項で利用したリザーブビットに認証のための信号を埋め込む。認証機能付き GPS 受信機ではどのような認証機能が埋め込まれているかを解読するためにメッセージビットの分析が必要となる。

⑤. GPS 信号からナビゲーションメッセージビットを利用して，暗号化されたデータビットを生成する。このようなデータビットは QZSS L1C/A 信号または L1SAIF 信号を使用して送信される。

③項で述べたようにＧＰＳ信号のナビゲーションメッセージを利用して暗号化されたデータビットは地上設備で生成される。認証機能を持った地上設備からユーザの GPS 受信機へ認証機能を送信するに際しては秘匿化が必要であるので認証機能に暗号化を施す。さらに，そのようなデータビットは QZSSL1C/A 信号または L1SAIF 信号のリザーブビットを利用して送信されるのが有用である。

⑥. GPS と QZSS の信号構造が同じであるためもちろん同一の方法が QZSS 信号の認証に適用可能である

QZSS は基本的に補完部分は GPS と同様である。GPS において適用された方法が QZSS 信号の認証においても適用可能である。一方 L1SAIF は QZSS の補強部分であるが，日本独自の認証機能をこの L1SAIF 補強信号で実現することはユニークなことである。さらに L1SAIF はＳＢＡＳ信号と互換性があるので SBAS 互換の WAAS，EGNOS への適用も将来考えられる。

⑦. QZSS L1C/A 信号または L1SAIF 信号を使用すると，PNT（位置，ナビゲーションとタイミング）のための目的を超えて，準天頂衛星システムのための新機能（認証機能）が強化されたアプリケーションを提供することが可能である。

本来 QZSS は測位衛星との位置付けであるためその信号の使命も位置の精度向上，ナビゲーションの高度化，タイミングの精度向上とされている。しかしここで，新機能として，（認証機能）が強化されるアプリケーションでは，本認証機能が大いに重要である。たとえば，電力網，銀行オンライン網，の時刻同期，産業廃棄物，放射性廃棄物の不法投棄防止，エネルギーグリッドの時刻同期，自動車のツールコレクションの時刻管理と課金，電気自動車の充電認

証，原産地物証明，などに位置の認証は大いに活用できる。このことにより PNT(Position, Navigaton, Timing) 機能であった位置情報に新規に認証機能(Authentication)が加わることで GPS/QZSS 信号に新しい付加価値がつく。すでに欧州 Galileo では認証機能(Authentication)が検討が進められており，日本の準天頂衛星システムにおいて機能検証，軌道上実証を行うことは有意義である。

6　提案アーキテクチャ

本論文では，GPS の潜在的な脆弱性を克服するためのアーキテクチャを提案する。アーキテクチャ提案の前提条件は３章で掲げた位置認証の解決策を満たすことである。つまり，既存の宇宙セグメントと地上セグメントには手を加えずに，新たに認証局（仮想）を設けて GPS 信号の秘匿化を行うことである。受信機では秘匿化された GPS 信号を認証できる仕組みを設けることである。ここで提案するアーキテクチャは次の 3 点から構成され，夫々４章で論じた目的の解決策に対応する。

1. MCS※，衛星と受信機間の全体構成
   位置認証の解決策⑥，⑦
2. 認証局(仮想）における構成：信号の送信方法
   位置認証の解決策③，④，⑤
3. 受信機での構成：信号の認証方法
   位置認証の解決策①，②

※MCS(Master Control Station)

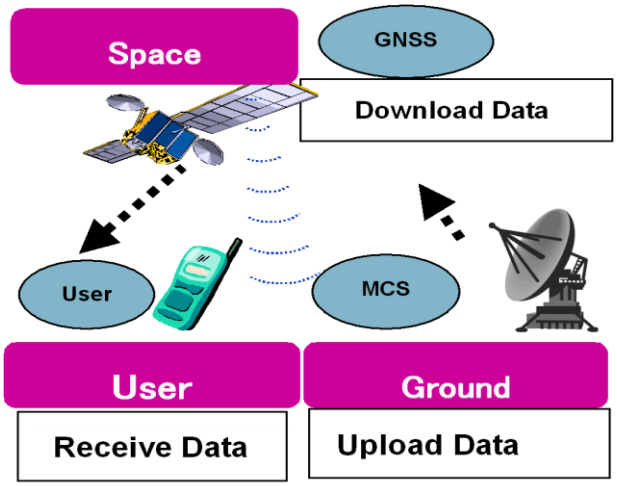

図 2 全体システム構成
Fig. 2 System Configuration

6.1　MCS，衛星と受信機間の全体構成

図２に全体システム構成を示す。システム構成は３つのセグメントから構成される。つまり地上セグメント，空間セグメント，ユーザセグメントであり，各々異なる特徴を有する。地上セグメントの役目は秘匿化ナビゲーションメッセージデータを生成して空間セグメントへナビゲーションデータをアップリンクすることである。空間セグメントの役目は秘匿化ナビゲーションメッセージデータを折り返してユーザセグメントにダウンロードすることである。ユーザセグメントの役目は空間セグメントからデータを受信し，復号化の機能を利用して地上セグメントからの秘匿化ナビゲーションメッセージデータを解読することである。

つまり位置認証の解決策⑥と⑦が解決されたのである。

6.2　認証局(仮想）における構成：信号の送信方法

信頼性の高いシステムを実現するため，現行の GPS へ適用可能な認証方法の概念を提案する。図 3 に信号の送信方法における認証データ生成の概念を示す。その概念には次の４つのステップがある

（ア）RAND メッセージ生成
（イ）SEED 値生成
（ウ）LDPC 演算
（エ）QZSS ナビゲーションメッセージの加工

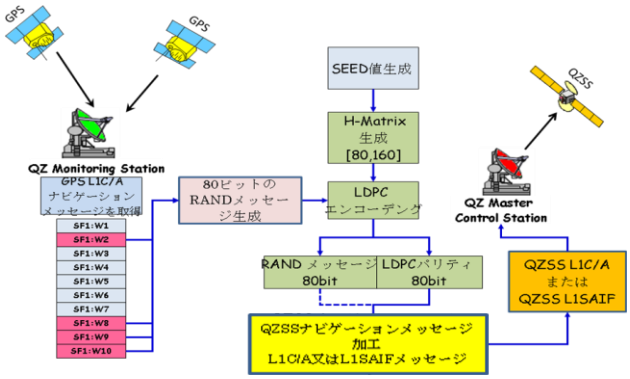

図3 信号送信における認証メッセージの概念
Fig. 3 Concept of Authentication Methodology: In Signal Transmitter

このコンセプトは，ナビゲーションメッセージに低密度パリティ補正 LDPC（Low Density Parity Correction）エラー訂正の生成機能を適用して，ナビゲーションメッセージの秘匿化の認証メカニズムを示すことである。

（ア）　ここで新規にレファランス認証ナビゲーションデータを定義する。このリファレンス認証ナビゲーションデータ RAND (Reference Authentication Navigation Data) とは，GPS の L1C/A 信号から週コード(TOW:Time of Week)と擬似ランダムノイズ(PRN ID:Pseudo Random Noise ID)とエフェメリスデータを抽出した参照データで，図 4 に RAND 構成を示す。

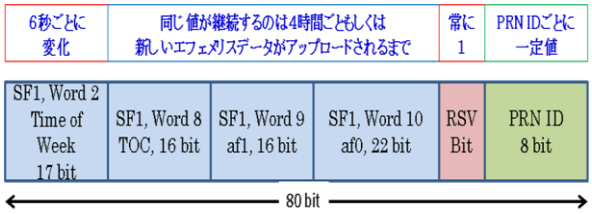

図４　ＲＡＮＤ構成

Figure4 RAND Structure

（イ）　本参照データは，GPS L1C/A 信号のナビゲーションメッセージから抽出されると SEED 値から得られたH－Matrix を利用して LDPC 符号化時に計算される。

（ウ）　LDPC 符号化を行うためには，H-Matrix は時刻可変のシード値から生成される。シード値が時刻可変の理由は，ミーコニングアタック対策である。時刻可変の認証信号が送信機で解読されれば，時間差を伴うミーコニング信号は解決可能であるからである。

（エ）　RAND のメッセージと LDPC パリティビットは地上部分で生成されて L1SAIF 信号の QZSS ナビゲーションメッセージのリザーブビットに埋め込まれる[7] 。リザーブビットだけを利用するならば，GPS システムのハードウェアの変更は発生しない。LDPC パリティビットは，ナビゲーションメッセージの所謂『暗号文』である。GPS 信号もしくは GPS システムのどちらにもできうる限り"触れる"ことなく，認証を提供することが可能となる。このことは，信号が認証される場合のみナビゲーションメッセージのビットの分析が可能である。

つまり位置認証の解決策③と④と⑤が実現されたのである。

6.3 受信機での構成：信号の認証方法

認証された GPS 受信機のプロトタイプを図 5 に示す。 本 GPS 受信機は，現行の GPS 受信機であり，暗号化認証ハードウェア部分は変更がない。信号送受信のファームウェアが QZSS の L1C/A 信号，L1SAIF 信号や MSAS の SBAS 信号

図５　プロトタイプ GNSS 受信ボード

Figure5 Superstar-II GNSS Receiver Board

対応できるように改造した。これにより本受信機は認証データを処理できる受信機となった。現行の GPS 受信機ボードを利用する理由は本提案の認証方法はファームウェアを改造するだけで，ボード全体のハードウェアを改良する必要がないことを明確にするためである。

つまり位置認証の解決策①と②が実現されたのである。

受信機での信号の認証の概要を，図 6 に示す。これは一般的な GNSS 受信機とは異なる認証に対応した GNSS 受信機の一例である。受信信号を認証する必要がないユーザのプロセスは，従来の GPS 信号の処理と同じである。（図左半分）

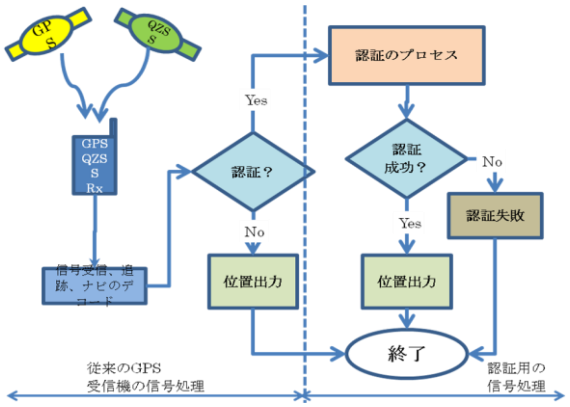

図6 受信機での信号認証の概念

Figure6 Signal Authentication Concepts at the Receiver.

認証が必要な場合にのみ，認証処理が必要である。このことは信号捕捉・追跡手順の変更を必要としない上に，受信機のアーキテクチャも変更しないことを意味する。（図右半分）

つまり認証機能の解決策③と④が実現されたのである。

図7に受信機の認証プロセスの詳細を表示した。提案認証システムの動作確認のため現時点ではシミュレータとPC上のバーチャルな認証データベースセンタ間のデータを確認するものである。将来的に軌道上のQZSS衛星と認証データベースとプロトタイプの受信機を使って実証実験を行う予定である。

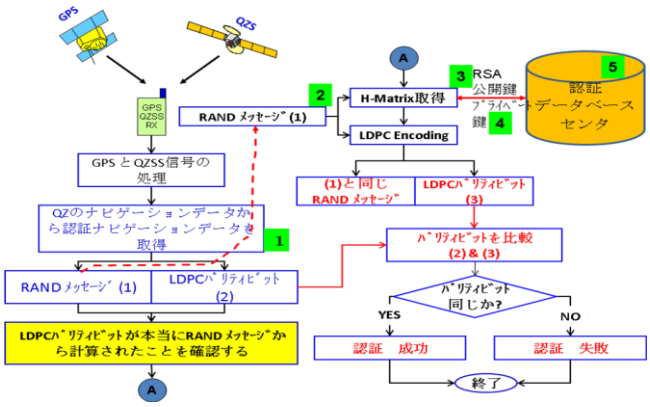

図7 受信機での信号認証手順の詳細

Figure7 Detail Authentication Procedure at Receiver.

図 7 の 緑色の①～⑤の動作を時系列にしたがって説明する。

①GPS/QZSS認証機能付き受信機はQZSナビゲーションメッセージから認証ナビゲーションデータ(RAND)を取得する。本QZSナビゲーションメッセージはRANDのメッセージとLDPCパリティビットを含むのでその値を抽出する。

②一方RANDメッセージの中のTime of WeekとPRN IDを検索キーとする。

③ 検索キーを元に認証データベースセンタから必要なデータを入手する。

④認証データベースセンタからRANDメッセージを生成した時のH-Matrixのデータを入手する。H-Matrixは最大80ｘ160の行列値である。

⑤受信機は公開鍵秘密鍵のRSA暗号化方式で認証データベースセンタにアクセスする。 RANDのメッセージは，6秒ごとに変化するので，H-Matrixも，6秒ごとに異なる。さらに，先にデータベースセンタから入手したH-MatrixでLDPC演算を実行する。受信機で受信したLDPCパリティビットとH-MatrixでLDPC演算して得られたLDPCパリティビットを比較する。等しい値であれば認証成立と判定する。

7 実験とシミュレーション結果

提案アーキテクチャが，衛星システムの脆弱性を克服するのに適していることを確認するため 2 種類の実験を実施した。

第一の実験の目的は既存の GPS 信号のナビゲーションメッセージに秘匿化データを挿入するにあたり，既存の信号体系に影響を及ぼさないようにリザーブビット位置を特定することと，そのリザーブビットの変化タイミングを確認することである。現在の GPS 信号 L1C/A信号のナビゲーションメッセージリザーブビットの位置を確認し，リザーブビットの変更間隔を 24 時間ｘ7 日間観測して確認した。観測結果から 4 時間毎もしくはエフェメリス暦の変更タイミング時刻であることが判明した。

第二の実験の目的は受信機での認証が成功したことの確認である。認証シミュレーション実験によって受信機で受信したパリティビットと認証データベースセンタから獲得した RAND 値で計算されたパリティビットとの比較で認証可否を判断できることをシミュレーションで確認した。

7.1 メッセージリザーブビットの位置確認と時間変化

GPS L1C/A 信号のナビゲーションデータフォーマットを図 8 に示す。サブフレーム 1～3 までは各 10 ワード 300 ビット構成である。サブフレーム 4,5 は各 25 ページある。

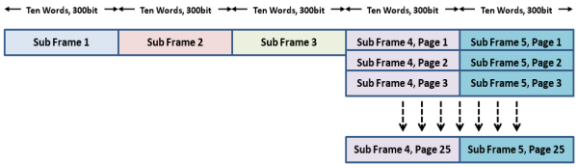

図 8　ナビゲーションデータフォーマット
Figure8 Data format of navigation message of GPS L1C/A

各サブフレームのビット構成からリザーブビット位置と長さを抽出する。サブフレーム 1 のビット構成例を図 9 に示す。リザーブビットは紫色で示す 87 ビットである。

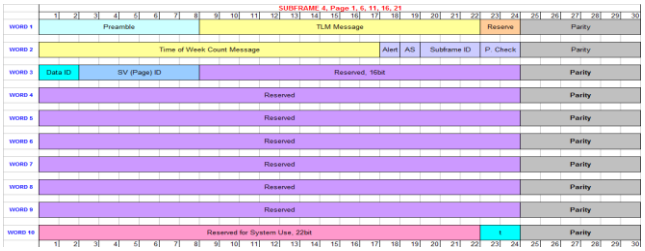

図 9GPS L1C/A サブフレーム 1 ナビゲーションメッセージ
Figure9 Navigation Message of GPS L1C/A サブフレーム

サブフレーム 2 には Word1 のリザーブビット 2bit を除く以外に存在しないので対象から除外する。
サブフレーム 3 のビット構成例では Word1 のリザーブビット 2bit を除く以外に存在しないので対象から除外する。
サブフレーム 4Page1, 6, 11, 16, 21 には Word3～9 までに 160 ビットある。
以下同様にフレームフォーマットを調べると，利用できるリザーブビットはサブフレーム 4Page12, 19, 20, 23, 24 には Word3～9 までにリザーブビット 136 ビットあり，サブフレーム 5 では存在しない。

ここで利用可能なリザーブビットとしてサブフレーム 1 のナビゲーションメッセージに着目する。実測データから Word1～Word10 まで GPSW e e k，GPSsec を 16 進で整理した結果を図 10 に示す。30 秒間隔で規則的にサブフレーム 1 は現れ，GPS Sec が 30 秒ずつカウントアップしている。Word4, 5, 6 のリザーブビットは予想通り，固定値である。変化点は 4 時間に一回である。

ここで Word2 の TOW(Time of Week count message)に着目すると，規則正しい変化が見られた。つまり，5884A5→588724→5889A7→588C24→588EA6→588126→5883A4→588627→5898A4→となった。時間変化成分として RAND に採用した根拠がここにある。 また，Word8 の TOC16bit と Word9, 10 の Clock はともに 4 時間ごと，もしくは新しいエフェメリスデータがアップロードされるまで一定値（42CC, 000012, 2A055A）である。一定間隔一定値である成分として RAND に採用した根拠である。

GPS Week	GPS Sec	Word 1	Word 2	Word 3	Word 4	Word 5	Word 6	Word 7	Word 8	Word 9	Word 10
1623	271896	8B095C	5884A5	95D000	64DDC9	CFD73C	949345	A9F6DB	0F42CC	000012	2A055A
1623	271926	8B095C	588724	95D000	64DDC9	CFD73C	949345	A9F6DB	0F42CC	000012	2A055A
1623	271956	8B095C	5889A7	95D000	64DDC9	CFD73C	949345	A9F6DB	0F42CC	000012	2A055A
1623	271986	8B095C	588C24	95D000	64DDC9	CFD73C	949345	A9F6DB	0F42CC	000012	2A055A
1623	272016	8B095C	588EA6	95D000	64DDC9	CFD73C	949345	A9F6DB	0F42CC	000012	2A055A
1623	272046	8B095C	589126	95D000	64DDC9	CFD73C	949345	A9F6DB	0F42CC	000012	2A055A
1623	272076	8B095C	5893A4	95D000	64DDC9	CFD73C	949345	A9F6DB	0F42CC	000012	2A055A
1623	272106	8B095C	589627	95D000	64DDC9	CFD73C	949345	A9F6DB	0F42CC	000012	2A055A
1623	272136	8B095C	5898A4	95D000	64DDC9	CFD73C	949345	A9F6DB	0F42CC	000012	2A055A

Decoded Week, Time from Word 1 & 2 / Preamble and Telemetry / TOW, Week and Other Data / SF1, Reserve Bits / Reserve, TGD, IODC, TOC / Clock Data

図 10GPS L1C/A ｻﾌﾞﾌﾚｰﾑ 1 PRN 10 のﾅﾋﾞｹﾞｰｼｮﾝﾒｯｾｰｼ
Figure10 Navigation Message of GPS L1C/A Subframe1 PRN10

7.2 認証データベースの動作

表 1 に認証データベースのサーバのサンプルデータ
Table1 Sample Data of Authentication message from DB Server to Receiver

TOW	PRN ID	RAND MSG	PARITY DATA	SEED VALUE	H-Matrix Data	RSA KEYS
272726	8	58B1A1660000007BC708	73DBEA93E7961A5FB2E3	653012443	HMAT_DAT_1	RSAKEY_DATA_1
272816	10	58B1A1667FFBFBA6C50A	0D2E53CCA0D967C248A8	653015706	HMAT_DAT_2	RSAKEY_DATA_2
272846	13	58B1A1667FFA127FD30D	AD5EB63397267847FCC3	653018415	HMAT_DAT_3	RSAKEY_DATA_3
272877	26	58B1A1667FD5F7F9731A	E73E9799583AC510FD58	653020857	HMAT_DAT_4	RSAKEY_DATA_4

この認証データベースはTime of WeekとPRN IDをインデックスにして８０ビットのRANDメッセージと同じく８０ビットのLDPCパリティビットと３６ビットのSEED値と80X160のH-MatrixデータとRSAキーから構成される。SEED値に対し一意にH-Matrixデータが決定される。同時にRANDメッセージとH-MatrixでLDPC演算されたLDPCパリティビットも一意にきまる。つまりTime of Week⇒PRN ID⇒SEED値⇒H-Matrix⇒RANDメッセージ⇒LDPCパリティビットの順に値が決まる。そしてこれらの値は認証データベースセンタでRANDメッセージを生成する時点でGPS/QZSS認証機能付き受信機に送信される。GPS/QZSS認証機能付き受信機はQZS衛星からの信号受信時にRANDメッセージとLDPCパリティビットを抽出する。抽出したLDPCパリティビットと認証データベースセンタから入手したLDPCパリティビットを比較して，認証可否を判断できる。なぜならば，認証データベースセンタのTime of Weekは６秒ごとに変化し，同一のPRN IDの衛星に対しデータベースの値はユニークな値となるからである。

表２に受信機から出力されたサブフレーム 1 のﾅﾋﾞｹﾞｰｼｮﾝﾒｯｾｰｼを示す。４種類のデータ構造を示す。

Case1 は GPS Week が 1623 で GPS Sec(TOW)が 272726 時点のサブフレーム 1 のデータである。RAND 値と LDPC ﾊﾟﾘﾃｨﾋﾞｯﾄに着目して表１と表２を比較する。Case1 の RAND 値(58B1A1660000007BC708)に対し LDPC ﾊﾟﾘﾃｨﾋﾞｯﾄ値は表１(73DBEA93E7961A5FB2E3)と表２(73DBEA93E7961A5FB2E3)で同一の値をとることがわかる。これは図 7 における RAND メッセージ(1)，ＬＤＰＣﾊﾟﾘﾃｨﾋﾞｯﾄ（２）が表２の値の LDPC ﾊﾟﾘﾃｨﾋﾞｯﾄ値に相当し，図 8 における LDPC ﾊﾟﾘﾃｨﾋﾞｯﾄ（３）が表１の LDPC ﾊﾟﾘﾃｨﾋﾞｯﾄ値に相当することがわかる。よって，認証成功したと判断される。つまり目的のための解決策⑤と⑥と⑦が実現されたのである。

表２　受信機からのサブフレーム 1 のﾅﾋﾞｹﾞｰｼｮﾝﾒｯｾｰｼﾞ

Case	Week	TOW	Word 1	Word 2	Word 3	Word 4	Word 5	Word 6	Word 7	Word 8	Word 9	Word 10
1	1623	272726	8BAAAA	58C712	7958B1	A16600	00007B	C7083C	73DBEA	93E796	1A5FB2	E330FC
2	1623	272816	8BAAAA	58CE90	7A58B1	A1667F	FBFBA6	C50A3C	0D2E53	CCA0D9	67C24B	A825FC
3	1623	272846	8BAAAA	58D110	7B58B1	A1667F	FA127F	D30D3C	AD5EB6	339726	7847FC	C32DFE
4	1623	272877	8BAAAA	58D392	7958B1	A1667F	D5F7F9	731A3C	E73E97	99583A	C510FD	582AFD

RAND, 80 bits　　LDPC Parity, 80 bits

7.3. 認証シミュレーション実験

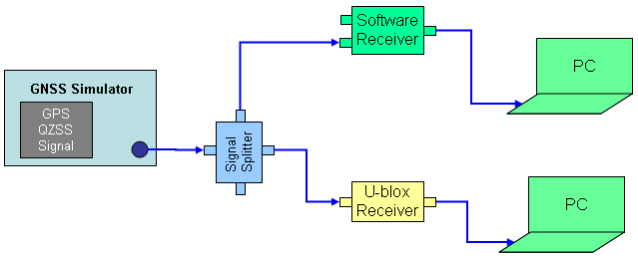

図 11　GNSS 信号シミュレータと u-blox 受信機とソフトウェア受信機を利用した認証シミュレーション実験例
Figure 11: System setup for authentication simulation using GNSS signal simulator, u-blox receiver and software receiver

図 11 に認証シミュレーション実験例を示す。GNSS シミュレータ内で 5.2 節で提案した認証メッセージを生成して u-blox 受信機とソフトウェア受信機へ送信する。u-blox 受信機は認証機能に対応していないので，通常の GNSS 受信機として振舞う。一方ソフトウェア受信機には認証機能を解読できる復号化機能を内在しているので，図 6，図 7，の認証解読機能を実施する。

ここで，QZSS のサブフレーム 1 を代表例としてサブフレーム 1 のリザーブビット Word3～9 に RAND メッセージと LDPC パリティビットを割り当てて認証局から QZS にアップロードしたと仮定して GNSS シミュレータから QZSS サブフレーム 1 をソフトウェア受信機に送信した。認証機能解読機能付きソフトウェア受信機は表 2 に示す QZSS サブフレーム 1 のナビゲーションメッセージを受信する。図１０の Case1～Case4 は同じ週コード(1623H)で週コードカウント(TOW)が時系列に（272726～272877）変化した例である。

提案手法の認証機能が正しく動作した。一方認証なしの信号が入力された u-blox は正常動作した。これより、GNSS シミュレータにより、認証機能あり/なしでの受信機の正常動作が確認できた。

8. 結論

航法メッセージを認証することによって GPS 信号のなりすましの問題を解決するための方法論を提案することで，目的のための解決策を提示した。結論は，次のとおりである。

① 受信機のアーキテクチャを変更しないで実現した。
② 信号捕捉・追跡手順の変更を必要としないで実現した。

③ ナビゲーションメッセージのデコードにいかなる変更も加えないことを確認した。
④ 信号が認証される場合にのみ，メッセージのビットの分析を行った。
⑤ GPS 信号から航法メッセージビットを利用して，暗号化されたデータビットを生成した。このようなデータビットは QZSS L1C/A 信号または L1SAIF 信号を使用して送信されることを示した。
⑥ GPS と QZSS の信号構造が同じであるため同一の方法が QZSS 信号の認証に適用可能であることを提示した。
⑦ QZSS L1C/A 信号または L1SAIF 信号を使用すると，PNT（位置，ナビゲーションとタイミング）のための目的を超えて，準天頂衛星システムのための新機能(認証機能）が強化されたアプリケーションを提供することが可能である。

全地球的航法衛星システムを使用してこの認証の通信がセキュアで安全な場所に基づくサービスを提供できる。さらに，準天頂衛星システムと SBAS（衛星航法補強システム）にこの手法を適用すると，位置情報の真生性を担保したバリュースタンプ機能（認証機能）の空間情報サービスを実現できることをシミュレーションによって確認できた。

9. 今後の課題

本論文のなかで、認証センターのデータベースとユーザ受信機間の通信手法については見当されていないが、PKI 手法によって暗号化された秘匿信号(PRN No, TOW, H-Matrix, 等）の送受信については今後の課題とした。

10. 謝辞

我々の研究に関して QZSSS Authentication プロトタイプ受信機を作成頂いた東京大学大学院海老沼卓司准教授と認証技術について共同研究中の JAXA 準天頂衛星システムチームの小暮聡氏，山下次郎氏，舘下弘明氏に感謝の意を示す。なお，本研究は 2010～2012 の科研費挑戦的萌芽研究の助成をうけています。また，成果物として特許２件を出願して，１件は公開された。特許公開 2011－41038 と特願 2011-277792 である。

（平成 25 年　Ｘ月ＸＸ日受付）

文　献

[1] K. Chino, D. Manandhar, R. Shibasaki, paper published in GPS World, “Seamless Tracking - GNSS plus RFID-” Vol20 August, 2009, pp.30-34
[2] GPS Joint Program Office, Interface Specification, IS-GPS-200, Revision D IRN-200D-001 (Navstar GPS Space Segment/Navigation User Interface) 7 March 2006
[3] John A Volpe National Transportation Systems Centre, Vulnerability Assessment of the Transport Infrastructure Relying on the Global Positioning System, commissioned by US Department of Transportation, August 29, 2001
[4] Scott, L., “Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems,” Proceedings of the Institute of Navigation GPS/GNSS 2003 conference, pp. 1543-1552, 2003
[5] Sherman Lo, D. De Lorenzo, P. ENGE, D. AKOS, P. Bradley “Signal Authentication- A secure Civil GNSS for Today” Inside GNSS published at September/October 2009, pp. 30-39.
[6] Pozzobon, O. (2), and L. Canzian, A. Dalla Chiara, and M. Danieletto “Anti-Spoofing and Open GNSS Signal Authentication with Signal Authentication Sequences,” IEEE/NAVITEC 2010, Noordwijk, The Netherlands, 10 December 2010
[7] Quasi Zenith Satellite System navigation service, “Interface Specification for QZSS”, submitted for publication .http://qzss.jaxa.jp/is-qzss/index_e.html

著者紹介

千野　孝一　（正員）　昭 56 東京工業大学電気電子工学科卒業．同年㈱日立製作所入社．平 15 年新衛星ビジネス㈱．現在，㈱日立情報制御ソリューションズ　兼務東京大学大学院　空間情報科学研究センタ協力研究員．主として衛星測位とセキュリティに関する研究に従事．電子情報通信学会正員．
衛星測位航法学会正員 ISO/IEC JTC1 SC37(Biometrics)エキスパート

Dinesh Manandhar　（非会員）　平 14 東京大学大学院博士後期課程了．工学博士．現在，東京大学大学院　空間情報科学研究センタ客員研究員，および測位衛星技術株式会社のシニアリサーチャであり衛星測位ソフトウェア受信機技術，インドアナビゲーションシステム，GNSS 信号の認証に関する研究に従事．

柴崎　亮介　（正員）　昭 62 東京大学大学院博士後期課程了．工学博士．現在，東京大学大学院　空間情報科学研究センタ教授．3 次元 GIS，GIS 環境におけるエージェントベースマイクロシミュレーション，GPS 技術に関する研究に従事．