

GPSはじめ他国の測位衛星が使用不可能になるケース (論点 1 - 2) に関する考え方

平成 22 年 12 月 27 日
内閣官房宇宙開発戦略本部事務局

他国の測位衛星システムはそれぞれの主権にもとづいて運用されており、一部に国際的に規定されているものがあるもの^(注)、それぞれの衛星によるサービス提供は国際法上義務づけられたものではない。仮に各国が測位サービスの無償提供を継続する前提とした場合でも、以下のとおり、他国の測位衛星システムが使用できないケースが想定される。

注) 例えば、船舶及び航空分野では、国際条約で地球的航法衛星システムとして GPS 及びグロナスが規定されている。

1. 意図的な妨害

(1) 外部からの意図的な妨害

GPSはじめ測位衛星においては、外部からの意図的な妨害により使用不可能になるケースが考えられるが、具体的には、ジャミング(敵対的信号妨害)やスプーフィング(偽信号によるかく乱)という電波に対するソフトな妨害と、主として GPS 地上関連施設を破壊する等のハードな妨害が想定される。

ジャミングとは、通信を阻止するために、通信が行われている周波数に妨害信号(ノイズ等)を送る行為をいう。これについては、外国製の GPS 妨害装置が市場に出まわっているといわれ、砂漠の嵐作戦の間、米国の兵器システムを妨害するため、イラクに敵国のジャマーが配備された(資料元:

<http://www.aiaa.org/Aerospace/Article.cfm?issuetocid=393&ArchiveIssueID=41> 他)。また、2010年8月23~25日、韓国全土の GPS 受信及び監視局 29カ所のうち、全羅南道紅島から忠清南道安興に至る西海岸の一部地域で数時間、GPS 電波受信障害が断続的に生じたが、これについて韓国は、北朝鮮が GPS 信号への妨害能力がある車載型の装置をロシアから輸入し、50~100kmの距離内で GPS 受信障害能力があるものと判断している(資料元:2010年10月4日聯合ニュース)。

GPSは電波が弱く、小さな出力でも妨害が可能なため、テロ等

による妨害や悪意あるいたずらによって被害を受ける蓋然性は高い。特に現行のGPS信号であるL1、L2は周波数の帯域が狭いため脆弱である。軍用コードや次世代GPSの信号であるL5は周波数幅が広く、電波出力も高いため、現行の民生コードよりも相対的に脆弱性は低い。ただし、軍用及び民生コードどちらも弱い電波であることから、いずれにせよジャミングを受ける可能性がある。

また、ジャミングは周波数ごとに行われるため、周波数を増やすことによりジャミングに対する脆弱性を減らすことが可能である。

スプーフィングとは、GPS信号を受信、解読した後、その信号に偽情報を組み込んだものを、あたかも本来のGPS信号のごとく送信することにより、受信者側に誤った情報を提供することで、正確な測位を妨げる行為をいう。スプーフィングは技術的には可能であり、民生コードについては技術情報を開示していることから、妨害を受ける可能性はある。ただし、軍用コードについては、技術情報が非開示であるため、信号の受信、解読は極めて困難であり、スプーフィングの妨害には抗たん性があると考えられている。

(2) 米国による意図的な地域的制限 (Regional Denial)

GPSによる測位情報が、敵により米国及び同盟国への攻撃にも利用されかねない（他国からミサイルを撃ち込まれるなど）ことから、米国はかつてGPSから発信される電波に「わざと」誤ったデータを混ぜ、結果的に受信機側で位置の誤差が出るようにする、いわゆるGPS信号に対する意図的な精度劣化政策である選択利用性 (SA: Selective Availability) を採用していた。

しかし、米国政府は、2007年9月、将来のGPS衛星にSA対応の機器を搭載しないことを宣言している。その代替手段として、米国によるGPSサービスの意図的な地域的制限 (Regional Denial) を講じることで、有事等の際、平和利用者へのインパクトは最小限に止めつつ、敵による宇宙ベースのPNT (Positioning, Navigation, Timing) 利用を阻止することについてコミットしている（資料元: SPACE-BASED POSITIONING NAVIGATION & TIMING NATIONAL EXECUTIVE COMMITTEE Frequently Asked Questions）。

2. 非意図的な干渉

GPS受信器の近傍で高出力の電波やGPSが利用する周波数帯に近い電波が放出される場合、電波干渉が起こり、GPS利用の障害となることがある。

例えば、ニューアーク国際空港の着陸システム（GPS信号を受信）について、電波受信が途絶える事案が発生し、数ヶ月にわたり原因探求したところ、PPD（Personal Privacy Devices）が原因と特定された（資料元：National PNT Advisory Board comments on Jamming the Global Positioning System – A National Security Threat : Recent Events and Potential Cures (November 4, 2010)）。

また、2007年1月22日、米海軍リサーチセンターにおいてテストジェネレーターが放置されたことに起因してサンディエゴ湾周辺で電波干渉が生起し、医療ページャータネットワークを含む周辺15Km域内の全ユーザーに影響が及んだ（資料元：

<http://www.gpsworld.com/gnss-system/receiver-design/innovation-interference-heads-up-4240>等）。

上述したとおり、GPSは電波が弱く、小さな出力でも妨害が可能なため、非意図的な電波の干渉により、特に帯域幅の狭い現行の民生コードについては被害を受ける可能性は十分にありうる。

3. システム障害

GPS衛星の故障により、測位情報が送信されない、もしくは誤った情報が送信されることがある。このような場合でも、GPS衛星の運用状況は地上関連施設で管理されており、GPSシステム側の被害を最小化する体制はとられているが、人為的ミス等により、対処に時間がかかり、GPSシステムに障害が生じることがある。

例えば、2004年1月1日現地時間11:30（18:30 UTC）頃、GPS衛星（PRN23）の位置ずれが急激に30mのしきい値を超え始め、「異常」と判断されたのは3時間後となり、その間、民生コード（L1 C/A）信号の誤差は280kmに達するという事象が発生した（これ以降このような事態は確認されていない。）（資料元：http://www.insidegnss.com/auto/IGM_lavrkas-janfeb10.pdf）。

このような障害による影響を回避するため、米国政府は全てのGPSユーザーに対してバックアップ手段を確保することを推奨している。GPSのシステム障害自体を完全に抑えることは出来ないものの、代替手段を確保することにより、これら障害による影響を最小化することが可能となる。