センシング制御の世界を変えるテクノロジの研究

cm級衛星測位 みちびきの世界

第10回　GNSS測位への妨害攻撃と対策

廣川 類

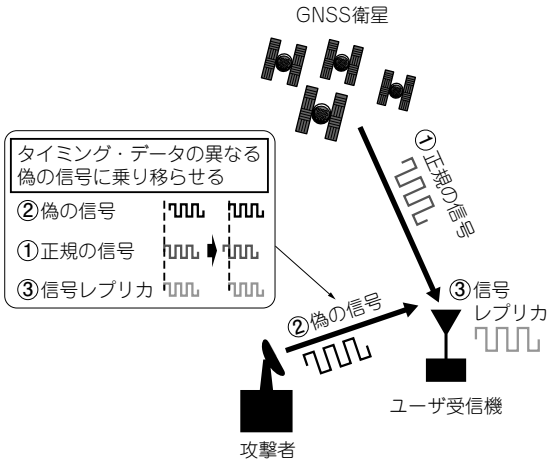

図1　GNSSにニセの情報を送るのは簡単（欺瞞攻撃）
本物からタイミングをずらすだけで偽の信号が作れてしまう

GNSSは妨害に弱い

● GNSSはもはや社会インフラ

GPSに代表される衛星測位システムGNSSは，位置を高い精度で得るセンサとして車やスマートフォンのナビゲーション機能などで便利に使われています．加えてGNSSは，モバイル通信，金融取引，送電ネットワークなど精密な時刻同期が必要なシステムで活用されており，まさに社会にとって欠くことができないシステムです．

● GNSSへの攻撃の種類

しかしGNSSは，L帯の低出力な電波を利用し，誰もが簡単に利用できるシステムであるため，意図的な妨害に対して脆弱（ぜいじゃく）であるとの指摘を受けています．代表的な攻撃手法には，

1. GNSSの電波よりも強い妨害波を送信してGNSSを使用できなくする飽和攻撃
2. 偽の情報を送信して誤った位置／時間情報をユーザ受信機に与える欺瞞（ぎまん）攻撃

などがあります．後者の欺瞞攻撃は，前者の飽和攻撃と比べて攻撃に要するリソース（電力）が低く，効率的なことが特徴ですが，GNSS信号を生成するために比較的高い技術が必要とされてきました．しかし，ソフトウェア受信機（SDR）技術の進歩により，数万円の機材でも信号生成が可能となったことで，従来は主に軍事目的で使用されていた高度なGNSS妨害技術が一般化し，社会基盤の脆弱化につながることが懸念されています．

例えば，位置情報を利用するゲーム「ポケモンGO」の位置情報を欺瞞することができたことが報告されています．

GNSSへの妨害の現状

● 改ざんした信号を送りつける

欺瞞攻撃の仕組みを**図1**に示します．衛星測位は4機以上の測位衛星からの電波を受信して距離を取得し，受信機の3次元位置と時計誤差を得る仕組みです．衛星と受信機の正確な距離はスペクトル拡散された符号系列の相関のピークを追尾することによって送信時刻および受信時刻の差として得られます．各衛星の拡散符号の仕様は公開されているため，タイミングをずらした（またはデータを改ざんした）信号を受信機に送信し，追尾させることにより，受信機の位置や時刻を誤らせます．

● 実際の妨害

こうした攻撃への対策としてさまざまな調査と研究が行われています．2019年3月に危機管理系NPOのC4ADSから主にロシアおよびシリアにおける欺瞞攻撃の実態に関するレポート(1)が公開されました．

本資料では，自動船舶識別装置（AIS）の出力に基づく解析により，2016年以降，黒海を航行する1000隻以上の船舶の位置が誤って計測され，数十kmも離れ