乗り物のハッキングと安全性

―航空交通管制における無線技術のセキュリティ―

応般

堀合 啓一（富士通システム統合研究所）

航空交通のセキュリティと航空交通管制システムの概要

航空交通のセキュリティという言葉で最初に連想されるのは，9.11 アメリカ同時多発テロ事件以来，非常に厳しくなってきた搭乗する際の手荷物検査や，プライバシーの侵害ではないかと騒がれたこともある，「ボディースキャナー」かもしれない．航空交通関連のセキュリティにもさまざまな分野がある．内閣官房サイバーセキュリティ戦略本部では（1）旅客，貨物の航空輸送サービス，（2）航空交通管制業務，（3）気象情報業務，（4）予約，発券，搭乗・搭載手続き，（5）運行整備，のように分類している．本稿では，地上業務などは一般的なサイバーセキュリティと共通点が多いので除外し，航空交通管制業務の中の無線技術に関連したセキュリティを話題とし，実際に発生した事例や，インシデントの事例はないがセキュリティの研究者などから脆弱性が指摘されている事項と各国の対応状況などを紹介したい．

航空交通管制システムの概要

航空交通管制システムは，航空機搭載の無線機器と地上の航空保安無線施設・有線ネットワークで構成されている．航空機は移動体であることから，通信手段等は無線に限られる．パイロットと地上の管制官の間で音声通信が繰り返され，フライトや航空交通管制に必要なさまざまな情報が無線で送受されている．円滑で安全な離着陸を支援するための各種のレーダ装置や ILS（Instrument Landing System：計器着陸装置），航空機が自機位置を知るための VOR（VHF Omnidirectional Radio Range）/DME（Distance Measuring Equipment）などの航空保安無線施設等が利用されている．ただし，これらの機器が利用できるのは直進する電波の特性から見通し内に限られる．以前は見通し外にも到達する NDB（Non Directional Radio Beacon：無指向性電波標識）や LORAN（LOng-RAnge Navigation）なども利用されていたが，GPS（Global Positioning System）の出現でその影が薄くなっている．以上のような航空交通管制に利用される無線機器の基本的な方式はセキュリティが考慮されておらず，一部の例外を除いて，実は半世紀以上に渡って変わっていない．例外の代表格は GPS の普及である．GPS はもともと米国の軍事用システムであったが，2000 年に民間利用に対する意図的な精度の劣化が解除された．その後，位置の分かっている基準局の情報を利用して誤差を補正する相対測位方式，干渉測位方式などの技術とあいまって，近年ではセンチメートル台の精度を得られるようになってきた．また，米国の GPS に対抗または補完する目的で，欧州，ロシア，中国も衛星を打ち上げており，総称して GNSS（Global Navigation Satellite System）と呼ばれている．我が国も，準天頂衛星初号機「みちびき」を 2010 年に打ち上げ，将来的には 7 機体制でのサービスを目指して開発が進められている．

航空交通管制における GPS の利用

航空機には，電波を利用した航法機器に加えて INS（Inertial Navigation System：慣性航法装置）を搭載し，自律航法が可能な機体も多い．しかし，INS は飛行時間とともに誤差が蓄積するため GPS などで補正が必要である．また，GPS の精度をさらに向上するために，地上または衛星からの電波を受信して，GPS の信号を

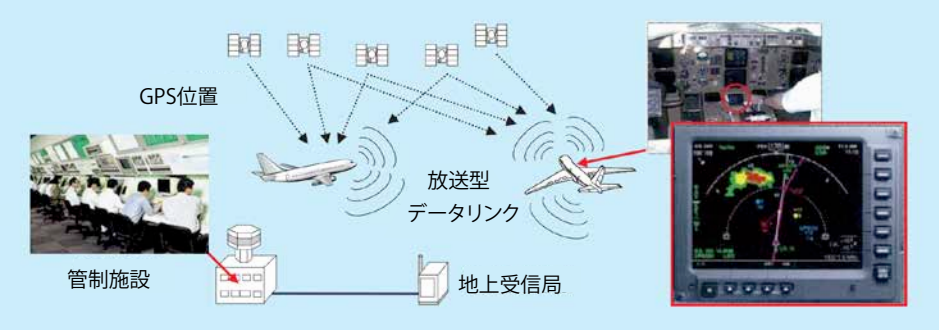

図 -1　ADS-B の概要（出典：国立研究開発法人 電子航法研究所）

補強するシステムが開発され GBAS（Ground Based Argumentation System） や SBAS（Satellite Based Argumentation System）などと呼ばれている．このようなシステムは，米国ではすでに FAA（Federal Aviation Administration）の認定を受けて実用化されている空港もある．これらの利用で，視程が悪い状況下でも ILS など地上施設からの支援なしに着陸が可能となる．さらに**図 -1** に示すように，GPS で得られる自機の位置情報を一定間隔でブロードキャストする ADS-B（Automatic Dependent Surveillance - Broadcast）が開発され，欧州では 2017 年，米国では 2020 年からの正式運用が予定されている．

従来の航空監視レーダによる位置精度は 1 ～ 2 海里程度であり，位置情報の更新にはアンテナが機械的に 1 回転する数秒が必要である．一方 ADS-B では，レーダよりも高精度で位置情報を取得できるだけでなく，更新頻度も高くできる．正確に航空機の位置を特定できるため，安全確保のために必要な運航間隔を狭めることが可能となる．また，自機位置や周辺を飛行する航空機の位置を正確に把握できるため，従来よりも自由度の高い飛行経路の選択が可能になり，飛行時間の短縮や消費燃料の節約に繋がる可能性があるといわれている．これらのシステムは，米国では航空交通管制システムの近代化計画である NEXTGEN の一部として開発や試験が進められているが，セキュリティの研究者などが脆弱性を指摘し，セキュリティ・カンファレンス等でこれを実証する講演が行われている．

ADS-B の脆弱性と偽 GPS 信号

ADS-B の脆弱性は，2011 年に米空軍の Donald L. McCallie 氏の論文 [1] で指摘された．ADS-B は仕様が公開され，かつ暗号化等のセキュリティ機能がない状態でブロードキャストされているので簡単に盗聴が可能であり，また偽の情報を送信することもできるというものである．米国のラスベガスで毎年開催されている世界最大のセキュリティ・カンフレンス BLACK HAT USA2012 等で，実際に偽の ADS-B 信号を発生させる攻撃例のデモが紹介された．昨年（2015 年）10 月 28 ～ 29 日に，日本発の国際セキュリティ・カンファレンスである CODE BLUE 2015 が東京の会場で開催されたが，この中で，筆者も「ワイヤレス技術をアタックで検証」という演題で，ADS-B の偽航跡インジェクションなどを含む発表を行った．

偽 GPS 信号（GPS spoofing）については，2003 年に spoofing 対策 [2] の方が先に発表され，その後 2008 年になって，実際に GPS の偽信号を発生するデモが行われた．2013 年にはテキサス大学 Todd Humphreys 氏のチームが偽 GPS 信号で大型のヨットの進路を変えて誘導することに成功し，2015 年に同チームはドローンの誘導に初めて成功している．またハッカーの祭典とも呼ばれている DEF CON 23（2015 年）で，Lin HuangLow らが，後述する SDR の技術を利用した低コストの GPS simulator[3] を発表し，受信した GPS 信号のリプレイや，独自に生成した GPS 信号でスマートフォンやカーナビの表示を狂わせることが可能であることを実証した．さらに昨年，海老沼拓史氏による

期間	8/23-26, 2010	3/4-14, 2011	4/28-5/13, 2013
場所	Kaesong	Kaesong, Mountain Kumgang	Kaesong
影響地域	Gimpo, Paju, etc.	Gimpo, Paju Gangwn etc.	Gimpo, Paju etc.
障害内容	181 Cell Towers 15 Airplanes 1 Battle Ship	145 Cell Towers 106 Airplanes 10 Ships	1016 Airplanes 254 Ships

表 -1　北朝鮮からの GPS 妨害による障害の事例（出典 : Jiwon Seo, Mincheol Kim : ENC 2013）

製品名	RTL-SDR	HackRF	BladeRF	USRP
周波数帯 [MHz]	24-1800	1-6000	300-3800	70-6000
A/D 変換 bit 数	8	8	12	12
帯域 [MHz]	2.8	20	28	56
送受信機能	受信のみ	半 2 重	全 2 重	全 2 重
価格	$20	$300	$420	$675

表 -2　安価な SDR ユニットの例

GPS の信号生成シミュレータ GPS-SDR-SIM[4] がオープンソースとして公開され，GPS spoofing 実験の敷居がさらに低くなった．これらは，あくまでも可能性の実証であるが，実際に GPS のジャミングや spoofing による影響，またはその疑いがもたれる事例が報告されている．

□ GPS にまつわる事例

2007 年 1 月カリフォルニア州サンディエゴで海軍医療センターの緊急ページャーが機能を停止し，港湾の船舶を誘導するシステムが誤作動，空港の航空管制システムが，予備のシステムでの運用を余儀なくされる事案が発生した．また携帯電話の利用，銀行の自動引き落としができなくなった．海軍の訓練のため，GPS 信号を含む周波数帯のジャミングが原因と判明するまでに 3 日を要した．

2010 年ニュージャージー州ニューアーク国際空港で GPS ベースの新しい着陸システムを設置した直後から，システムが 1 日に 1，2 回勝手にシャットダウンするようになり，その原因を突き止めるまでに数カ月を要した．ある運転手が高速道路の料金をごまかすために使っていたポータブル GPS 妨害機が原因で，空港の近くを通るつど空港のシステムをダウンさせていた．以上は偶発的に発生した例であるが，意図的な事例も発生している．

2010 ～ 2013 年にかけて，韓国が北朝鮮から GPS に対するジャミングを受け，これによって**表 -1** に示すように，数多くの携帯基地局，航空機，船舶が影響を受けたとされている．その後，今年（2016 年）の 3 月末～ 4 月初旬にも，同様の事案が発生した．

2011 年 12 月 4 日，アフガニスタンから発進した米国の偵察用ドローンがイランの核施設の捜索中に，制御不能で行方不明となった．故障などが原因で墜落した可能性もあるが，イランは鹵獲したと主張し，ジャミングや GPS の spoofing の可能性が指摘されている．また，2016 年 1 月に米海軍の 2 隻の巡視船がイランの領海を侵犯する事件があった．クエートからバーレーンへ向かう途中，ナビゲーション・ミスでコースを外れイランの領海へ侵入したことが原因とされている．ミスの内容は明らかではないが，これについてもイランが何らかの方法で GPS を狂わせのではないかと憶測されている．

ソフトウェア無線技術の発展に伴うハッキングの敷居の低下

従来の無線機器は，目的に応じた専用のハードウェア上に実装していたが，携帯電話や無線 LAN など，さまざまな周波数帯や変調方式に対応するために，ソフトウェアの書き換えで対応する技術が発展し SDR（Software Defined Radio）と呼ばれている．複雑な変調や復調などの信号処理には FPGA（field-programmable gate array）など専用の LSI が使われていたが，一般的な PC の処理能力の向上に伴い，これらの処理を PC 上で実行するソフトウェアが開発された．オープンソースの GNURadio がその代表例で，Linux/OSX/Windows など幅広い OS 上で利用できる．GNURadio には GUI ツールも用意されていて，あらかじめ定義されたさまざまな信号処理ブロックをドラッグ＆ドロップで利用できる．電波の送受信だけは PC で実現できないので，別途 SDR ユニットが必要となるが，たとえば**表 -2** に示すような比較的安価な SDR ユニットが市

販されており，これを接続することで，PC が高性能な無線機に早変わりする．筆者は，制御用として Raspberry Pi を利用してバッテリで駆動できる装置を試作し，スマートフォンなど多くの GPS 搭載の民生機器で，地図上の位置や時刻表示，ファイルのタイムスタンプなどが影響を受けることを確認している．SDR の技術の進歩により，無線機器に対するハッキングの敷居が確実に下がっている現状を認識する必要がある．

GPS 依存への懸念と対応

GPS の機能は NPT（Navigation, Positioning, Timing）と呼ばれ，対象を重要インフラに絞っても，金融，電力，情報通信などの分野で取引のタイミングやネットワークの同期の確保などが GPS の正確な Timing 機能に依存している．FAA の NEXTGEN も GPS なしでは機能しない．このため GPS に対するジャミング等の影響を局限するため，たとえば複数周波数の利用や符号体系の工夫など，GPS の可用性を向上させる対策も進んでいる．しかしながら，GPS 衛星は地球から 20,200km の遠方にあり，電波は距離の二乗に比例して減衰するため，近距離からのジャミングや spoofing に完全に打ち勝つことは難しい．GPS そのものの精度向上や完全性・可用性を高める努力はもちろん重要であるが，バックアップとしてほかの手段についても検討が必要な状況にあるのではなかろうか．事実欧州では，冒頭でも述べた LORAN の精度を向上させた eLORAN の運用を開始した．北朝鮮から GPS のジャミングを受けた韓国も eLORAN の設置を開始している．米国の DARPA（Defense Advanced Research Projects Agency）は，Timing のバックアップとしてモバイルで使用が可能な新たな原子時計の開発を計画している．技術的対策ではないが，米海軍は中断していた天測航法の訓練を再開したという．GPS の機能が喪失する可能性を脅威として認識していればこそ，これらの行動を起こしているものと思われる．

航空交通管制に関するシステムの変更は，国際的な調整が必要であり，10 年単位の期間を要する．ADS-B の例を挙げれば，開発は 1990 年頃には完了していたが，その後の SDR などの技術の発展もあって，各国の正式運用開始前に脆弱性が指摘されているのが実情である．米国の GAO（Government Accountability Office）は 2015 年 1 月に「FAA は航空交通管制システムの脆弱性に対処が必要」というタイトルで報告書を公開し，「十分な脅威分析による適切な対応」を求めている．事態を想定した代替手段の確保，対処手順の充実や訓練の実施など，各国が独自で対応できる分野については，重大インシデントの発生を待つことなく，適切なリスク分析に基づく計画的な施策が求められる時代となっているといえよう．

参考文献

1) McCallie, D. L. : EXPLORING POTENTIAL ADS-B VULNERABILITES IN THE FAA' S NEXTGEN AIR TRANSPORTATION SYSTEM, AFIT/ICW/ENG (2011).
2) Warner, J. S. and Johnston, R. G. : GPS Spoofing Countermeasures Homeland Security Journal (Dec. 12, 2003).
3) Lin, H. and Qing, Y. : GPS SPOOFING Low-cost GPS Simulator, DEF CON 23 (2015).
4) 海老沼拓史：ソフトウェア無線による GNSS 信号シミュレータの開発，測位航法学会 研究発表予稿集，p.7 (2015).

（2016 年 3 月 22 日受付）

堀合啓一（正会員） horiai.keiichi@jp.fujitsu.com

防衛大理工学研究科（電子工学），情報セキュリティ大学院大学博士課程修了．博士（情報学），CISSP．航空自衛隊および防衛省技術研究本部にて研究開発業務に従事．現在は富士通システム統合研究所でサイバーセキュリティの研究を担当．