Vol.2019-DPS-178 No.1
Vol.2019-CSEC-84 No.1
2019/3/4

# 重要インフラに与えるＧＰＳ時刻信号の重要性の調査

角田泰基[†1]　大久保隆夫[†2]

**概要**：GPS を含む衛星システムは，デュアルユースとして，軍事分野だけでなく国民生活にとって必要不可欠な社会インフラとなった．GPS は，位置情報の取得に利用されるだけではなく，ナノ秒レベルの高精度の時刻信号を配信しており，重要インフラは，GPS 時刻信号に大きく依存している．
一方，重要インフラに関するセキュリティ対策は，NISC を中心に様々な対策を採っているが，従来のサイバー攻撃対策が中心であり，GPS 時刻信号の重要性に対する認識はなく，かつ脆弱性対策も取られていない．ただし，GPS の脆弱性は，宇宙分野や人工衛星分野において研究が進められその脆弱性が指摘されている．
本論文では，重要インフラに与える GPS 時刻信号の重要性を調査するため，まず，GPS と重要インフラの関係を調査する．次に，宇宙システムに対するサイバー攻撃，ジャミング，キネティック攻撃の蓋然性を調査する．併せて，日米の重要インフラ及び GPS 時刻信号に対するセキュリティ対策を調べ，今後，我が国にとって必要な対策を導き出す．

**キーワード**：GPS，重要インフラ，時刻信号

# Research of the importance of GPS timing affecting critical infrastructure

YASUMOTO TSUNODA[†1]　TAKAO OKUBO[†2]

**Abstract:** The Satellite systems including GPS became an essential critical infrastructure not only for the military affair but also for the people's lives as a dual-use. GPS is not only used for getting position information but also delivers highly accurate time data of nanosecond level, and critical infrastructures heavily depend on GPS time data.
Although NISC takes various security countermeasures about critical infrastructures, it focuses on conventional cyberattack countermeasures. There is no recognition about the importance of GPS time data and no measures are taken against GPS time data vulnerability. However, the vulnerability of GPS has been studied in the space field and satellite field, and its vulnerability has been pointed out.
In this paper, in order to research the importance of the GPS time data given to critical infrastructures, I research the relation between GPS and critical infrastructures, first. Next, we research the probability of cyberattacks, jamming and kinetic attacks against the space systems. At the same time, we research Japan and U.S. security measures against the critical infrastructures and the GPS time data, and we will draw necessary measures for our country.

**Keywords**: GPS, Critical Infrastructure, Timing

## 1. はじめに

GPS は，米国が主に軍事目的のために開発を始めたものであるが [1]，現在，GPS は，デュアルユースとして [2]，軍事分野だけでなく国民生活にとって必要不可欠な社会インフラとなっている．我が国では，GPS と言えば，位置情報が取得可能なシステムという認識が広まっており，実際，カーナビなど国民生活に身近なものから，農業，災害救援，レクリエーション，測量・地図作成まで幅広い分野で使用されている．しかし，GPS は，位置情報を取得できるだけでなく，ナノ秒レベルの高精度の時刻信号を配信し，重要インフラを含む様々な分野で利用されている．米国では，金融システム，電力グリッドなどの重要インフラが，GPS 時刻信号に大きく依存していることを認識し，脆弱性に対する対策等が採られている．

重要インフラは，国民生活を支える重要な社会インフラであるが，サイバー技術の急速な発展により，サイバー攻撃の脅威に晒されている．実際，世界各国で被害が発生し，国民生活に深刻な影響を与える事態も生起している．我が国は，昨年７月サイバーセキュリティ戦略本部が，「重要インフラの情報セキュリティ対策に係る第４次行動計画」[3]（以下，「第４次行動計画」という．）を改定し，重要インフラ対策を採っている．その結果，サイバー攻撃の完全な抑止は，できていないが，重要インフラ事業者の経営者等もサイバー攻撃の脅威を認識し，自助努力の対策が採られている．ただし，上記対策は，マルウェア感染や標的型攻撃対策といった従来のサイバー攻撃を中心に対策が採られており，重要インフラに与える GPS 時刻信号の重要性に対する認識はなく，セキュリティ対策も採られていない．

一方，GPS 研究者間では，GPS の脆弱性に関する研究が進められ，その脆弱性が指摘されている [4]．GPS を含む宇宙システムのセキュリティは，初めて衛星が打ち上げられて以降，キネティック攻撃やジャミングの脅威に晒されてきたが，衛星が物理的に地上から隔離されていることによる安心感や，コスト削減の観点からセキュリティは，置き去りにされてきた．その結果，近年のサイバー技術の著しい進歩により，宇宙システムは従来のキネティック攻撃やジャミングに加え，サイバー攻撃の脅威に晒され，その

Vol.2019-DPS-178 No.1
Vol.2019-CSEC-84 No.1
2019/3/4

脅威は年々増大し，かつ巧妙になっている．

現代においては，国民が安心かつ安全に生活をするには，重要インフラの可用性及び完全性の維持が不可欠である．しかし，重要インフラが GPS 時刻信号に大きく依存しているにも関わらず，GPS 時刻信号に対するセキュリティ対策は，政府が組織として取り組んでいないのみならず，重要インフラ事業者等も自主的に取り組んでいるわけではないと思われることから，本論文では，重要インフラに与える GPS 時刻信号の重要性を調査する．

本論文は，具体的に以下の通り展開する．

第 2 章では，調査を進めるに当たって，基礎となる GPS 及び重要インフラの現状を調査し，GPS 時刻信号と重要インフラの関係を調査する．

第 3 章では，GPS を含む宇宙システムに対する攻撃手法の特徴を調査する．ここでは，従来のキネティック攻撃及びジャミングに加え新たな脅威となったサイバー攻撃を調査する．

第 4 章で，我が国における重要インフラ及び GPS 時刻信号に対するセキュリティ対策を調査する．具体的に第 4 次行動計画からどのような対策が採られているか読み取る．

第 5 章では，米国での重要インフラ及び GPS 時刻信号のセキュリティに対する国土安全保障省を中心とする取り組みを調査する．

第 6 章において，第 1 章から第 5 章までの調査結果をもとに，重要インフラが依存する GPS 時刻信号に対する対策を検討し，最後に，結論を述べる．

## 2. GPS

### 2.1 GPS の諸元

GPS は，1978 年に米国によって打ち上げられた航法衛星である．2018 年 10 月現在，31 個aの GPS が地球上を周回しており，６面の軌道面にそれぞれ 4 個以上の衛星が配備されている [5]．GPS 受信機は，常時少なくとも 6 機程度，多いときは 10 機以上の衛星からの信号を測位に利用できる [6]．GPS の運用期間は，約 10 年であり [7]，また，GPS は，1 日 2 回 12 時間毎，地球上高度約 20,200km を周回している．GPS 信号は，L1(1575.42MHz), L2(1227.60MHz)バンドで送信されている．L1 には，民間用の C/A コード(coarse/acquisition code)と呼ばれる信号が乗せられている [6]. L2 では，暗号化された P(Y)コードが使用されており，政府及び軍用に利用されている．

### 2.2 GPS 地上システム

GPS 地上システムの主制御局は，米国コロラド州米空軍 Schriever 基地にある．地上システムは，この他にカリフォルニア州米空軍 Vandenberg 基地にある代替主制御局，11 個のコマンドコントロールアンテナ及び 16 個の監視サイトからなり，米空軍 2nd Space Operations Squadron(2SOPS)及び米空軍 Reserve's 19th Space Operation Squadron(19SOPS)が 24 時間監視している [8]．主制御局が，GPS を制御するときは，空軍基地のネットワークだけなく，Kwajalein, Ascension Island, Diego Garcia, Cape Canaveral Florida のアンテナを使用して航法情報を送信している [9].

### 2.3 GPS が使用されている分野

表 1 は，GPS が利用されている分野を GPS の航法誘導，精密測位及び時刻別に分類したものである．表から分かる通り，GPS 信号は，特定の専門分野のみならず国民の生活や社会インフラに密接に関わっている．

表 1　GPS が使用されている分野

| 用途 | 分野 | システム・サービス |
|---|---|---|
| 航法誘導 | 航空・空港・鉄道 | 空港への精密侵入，航路誘導，鉄道運航補助 |
| | 物流 | カーナビ配送・物流管理 |
| | 交通 | 自動走行，安全運転支援，道路課金システム，ドライブレコーダー<br>航空測量(UAV)，農薬散布(UAV) |
| | 船舶 | 船舶運航管理・漁場管理 |
| | 災害 | 捜索救難，災害情報収集(UAV) |
| | 情報通信 | 位置情報サービス |
| 精密測位 | 測量 | 地殻変動観測・測地観測，変位観測（ダム・大型橋梁，地滑り観測）<br>可降水量測定<br>精密地図作成，ハザードマッピング |
| | 農業 | 精密農業（農機自動制御）トラクターガイダンス |
| | 海洋 | 波浪・津波監視部位 |
| 時刻 | 金融・クレジット | 金融システム，電子商取引，タイムスタンプ |
| | 電力・ガス | 送配電網管理，スマートグリッド |

※下線部は，重要インフラ分野

### 2.4 GPS 時刻信号

#### 2.4.1 GPS 時刻信号の精度

GPS は，セシウムやルビジウムといった精度の高い原子時計 [5]を２個以上搭載し，GPS 受信機に正確な時刻信号を配信している．原子時計とは，セシウムやルビジウムなどの原子が発する光の波長を利用して正確な時計を実現するもので，その精度は $10^{-12}$ 程度と言われている [6].

また，GPS には，時刻同期用のための発振器が搭載されており，宇宙用セシウム発振器の精度はおおよそ $10^{-13}$ 程度と言われている．

GPS 時刻の基になっている時刻は，米海軍天文台(USNO:

a https://www.gps.gov/systems/gps/space/

The United States Naval Observatory)が決めている標準時(UTC: Coordinated Universal Time)であり，これを GPS へ定期的に送信している [10]．更に GPS は，時刻信号を UTC との誤差 40 ナノ秒程度で配信している [11].

#### 2.4.2 時刻同期

GPS 受信機は，受信した GPS 時刻信号と GPS 受信機の内部時計を比較することにより内部時計を UTC と同期した正確な時刻に修正することができる. GPS 受信機は, GPS 信号を受信することにより，原子時計を直接保有又は，運用コストを払うことなく正確な時刻を得ることができる．

グローバルに分散したコンピュータ同士がネットワーク経由でやり取りをするためには，分散したコンピュータが同期を取らなければならず, 正確な時刻を配信する GPS 時刻信号を使用している．

また，正確な時刻配信は，タイムスタンプや文書の正当性を保証する電子署名を作成する際も必要となる．

コンピュータの時刻同期，タイムスタンプ及び電子署名のための時刻配信プロトコルとして NTP や PTP がある．GPS は，これらのプロトコルで使用するサーバに時刻を配信している．

### 2.5 重要インフラと GPS 時刻信号

我が国では，重要インフラを「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり，その機能が停止，低下又は利用不可能な状態に陥った場合に，わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの」bと定義し，NISC が中心となり情報セキュリティの観点から, 第 4 次行動計画において,「情報通信」,「金融」,「航空」,「空港」,「鉄道」,「電力」,「ガス」,「政府・行政サービス（地方公共団体を含む）」,「医療」,「水道」,「物流」,「化学」,「クレジット」及び「石油」の 14 分野を特定している [3].

前掲した表 1 中，下線を引いた分野が重要インフラ分野であり，航法誘導では,「航空」,「空港」,「鉄道」,「物流」,「情報通信」，時刻では,「金融」,「クレジット」,「電気」,「ガス」が含まれている．この表から重要インフラが GPS と密接に関わっていることがわかる．

金融ネットワーク，電力グリッドは，運用の効率性の観点やタイムスタンプの所要のため，正確かつ高精度の時刻同期が求められ，最も精度の高い時刻信号を配信できる GPS 時刻信号に大きく依存している．

GPS が使用される理由として，正確であることに加え，同報性や耐災害性が高く，無償という特徴を併せ持つ唯一のものであるという理由がある [12].

#### 2.5.1 電力グリッド

現在の電力グリッドは，電圧位相計測装置(PMU; Phasor Measurement Unit)を使用して状態監視を行っている．PMU は，位相，電圧，電流などの電力系統における計測情報に GPS から得られる絶対時刻を付加し，時系列の計測情報としてリアルタイムで計測する装置である [13]. PMU は, 電力グリッド上の複数のポイントにおいて，同期された電圧計測と位相計測を比較することで，電力の流れを計測している．これにより，電力グリッドの安定性を評価し，停電が起こる前に問題を検出し, 更には障害が発生した時に「修復」している [14]．これを実現するため，配電網から集録した高い伝送レートのデータを処理し，そのデータをコンピュータ制御システムに送信したり，制御室のオペレータにとって意味のあるデータに変換したりするリアルタイム解析機能が必要になり，これを支える高精度の時刻信号が必要になる．

このような事情から，タイムスタンプデータ収集の頻度が増加するとともに高精度のタイムスタンプが要求されている．SCADA では，1 秒間に 1 回であったものが，PMU では，1 秒間に 30 から 120 回の頻度でデータを収集している [15]．表 2 は，PMU と SCADA の諸元を比較したものである．

表 2　PMU と SCADA の比較

| 項目 | PMU | SCADA |
|---|---|---|
| データ収集頻度 | 30～120 回／秒 | 1 回／分 |
| 測定項目 | 電圧や電流などの大きさ及び位相 | 電圧や電流の大きさ |
| データ同期 | 高精度で同期可能 | 不可能 |
| 利用可能範囲 | 管轄エリアを超えた広域エリア | 管轄エリア内 |

#### 2.5.2 金融

高速トレーディング環境では，数ミリ秒の処理判断の差が数億円の取引の損得につながるため，高速トレーディング環境を支えるトレーディングシステムが適切に運用されていることを常時監視しなければならない [12].

高速トレーディング環境の精度に対応するためには，UTC との同期誤差が 50 ナノ秒～100 ナノ秒であることが必須となる [12]．したがって，GPS 時刻信号と 20～100 ナノ秒の精度で時刻同期がとれる PTP と組み合わせたタイムスタンプが実装されるようになっている．

## 3. 宇宙システムに対する攻撃

### 3.1 サイバー攻撃

宇宙システムに対するサイバー攻撃は，準備段階において，標的システムに関する事前の情報収集が必須であり，標的システムに精通していなければならない．

サイバー攻撃は，高度技術が要求されるが，必要なツー

b https://www.nisc.go.jp/active/infra/outline.html

ルは安価であり，かつ攻撃法が多様であり柔軟性がある．

しかし，アトリビューションは，困難である．攻撃者が，容易にサイバー攻撃の痕跡を改ざん，秘匿又は消去することが可能だからである．

更に，攻撃は，可逆であり，かつ攻撃効果を確認することが困難である特徴がある．

#### 3.1.1 サイバー攻撃の事例

2014 年にアメリカ海洋大気庁（NOAA, National Oceanic and Atmospheric Administration）が中国系と思われるハッカーによってハッキングされた事例がある．このサイバー攻撃によって，NOAA は，一時，サイトの閲覧が不可能になるとともに気象情報の配信が実施できなくなり，軍民両機関に著しい影響を与えた [16] [17].

### 3.2 ジャミング

ジャミングは，送信者が受信機に送信する信号と同一周波数で同等以上の出力を持った信号を送信することにより，受信機に正規の信号とジャミング信号の区別をできなくさせる，又は正規の信号を認識できなくさせる攻撃である．ジャミングには,地上システムから衛星システムに送信する信号に対するアップリンクジャミングと反対のダウンリンクジャミングがある．また，同様の攻撃としてスプーフィング(Spoofing)，ミーコニング(Meaconing)がある．

スプーフィングは，生成した偽信号を標的の受信端末に送信することにより，標的に偽情報を与えて混乱させるものである．また，ミーコニングは，正規の送信信号を記録し，一定時間遅延させて，標的に送信することにより，標的を混乱させるものである．

#### 3.2.1 ジャミングの特徴

アップリンクジャミングの場合，地上局からの送信出力と同程以上の出力が必要なため，ダウンリンクに比べ衛星までの距離の分，大出力が必要である．そのため，指向性アンテナを使用する．

ジャミングは,周波数や出力など事前の情報収集が必要であるが，高度な技術は必要ない．また，アップリンクジャミングとダウンリンクジャミングのみであること，攻撃は電波到達圏内という制約から柔軟性に乏しい．しかし，攻撃ツール自体は，インターネット上で，数万円程度の安価で購入が可能である [4].

その他，攻撃が可逆という特徴がある．攻撃を停止すると正規の信号を元通り受信可能であり，また受信機に対して恒久的な損害を必ずしも与えるわけではない．

しかし，攻撃のアトリビューションは困難である．被攻撃時，攻撃方向の探知は可能であるが，距離の測定が困難だからである．また，レーダー画面上に異変が出現した場合，それが意図的な攻撃か障害によるものか速やかに判別できないため，障害と攻撃の判別が困難である．

#### 3.2.2 ジャミングの事例

北朝鮮は，過去複数回(2018 年 8 月，10 月，2011 年 3 月 2012 年 4 月，2016 年) [18]，韓国に対してジャミングを実施している．その中でも 2012 年 4 月の活動が大規模であり，北朝鮮の GPS ジャミングにより，韓国は，仁川及び金浦国際空港の航空管制が中断し，空港側は代替の航法装置の使用を余儀なくされた [19].

### 3.3 キネティック攻撃

衛星システムを物理的に攻撃する場合，地上から発射されたミサイルを標的衛星まで誘導して攻撃する．

キネティック攻撃は，ミサイルを標的衛星まで誘導するため，高度な技術が要求される．また，ミサイルを対衛星兵器として使用するためには，ミサイルの開発，発射設備の構築が必要であり，加えて，実戦配備前に多くの試験が必要であり，多額の費用及び資源が必要となる．

一方，キネティック攻撃は，アトリビューションが可能である．ミサイルの場合，米国等が発射の兆候がある段階から監視を開始しており，ミサイル発射後もレーダー等による追尾を継続して実施しているためである．また，被害を容易に知覚できることから，攻撃効果を確認することが可能である．

#### 3.3.1 キネティック攻撃の事例

中国は，2007 年 1 月 11 日，四川省の西昌宇宙センター付近において，高度約 850～860km の老朽化した気象衛星を，固体ロケットを使用して破壊した人工衛星破壊実験（ASAT 攻撃）を行った [20]．このとき，10cm 以上のデブリが 2317 個放出したとされている．

### 3.4 攻撃手法の比較

攻撃手法を比較すると表 3 のとおり．

表 3　攻撃手法の比較

| | サイバー攻撃 | ジャミング | キネティック |
|---|---|---|---|
| ① | 困　難 | 困　難 | 容　易 |
| ② | ・情報収集労力大<br>・費用：安価<br>・技術：高度<br>・柔軟性：大 | ・情報収集労力大<br>・費用：安価<br>・技術：低<br>・柔軟性：小 | ・情報収集労力大<br>・費用：多額<br>巨大な施設<br>・技術：高度<br>・柔軟性：小 |
| ③ | ・コントロール可能<br>・攻撃効果：可逆<br>・攻撃効果を確認困難 | ・攻撃は、電波到達覆域内<br>・攻撃効果：可逆<br>・攻撃効果の確認困難 | ・攻撃は、ミサイル到達圏内<br>・攻撃効果：不可逆.<br>・攻撃効果の確認が容易 |

①アトリビューション②費用対効果③攻撃のインパクト

## 4. 日本のセキュリティ対策

### 4.1 宇宙システムのセキュリティ対策

#### 4.1.1 フィルタによる対策

受信機やアンテナに特定の周波数帯域の信号のみ通過を

許可または拒否する設定を行う対策である．

**4.1.2 暗号化による対策**

多くの商用衛星は，信号を暗号化することなく設計され，通信は，オープンアクセスであるため，暗号化は，サイバー攻撃やスプーフィング攻撃から信号を防御するため重要である．

GPS では，公開鍵暗号方式によりデジタル署名を施す方式がある．航法メッセージのダイジェストに対してデジタル署名を生成し，認証情報とする方法である [4]．ただし，この方法は，スプーフィング対策になるが，正規の信号を送信するミーコニングに対しては，効果がない．また，復号鍵の配送や管理が課題となる．

**4.1.3 施設に対する対策**

(1)指向性アンテナ

指向性アンテナを使用して，GPS が実際に存在する方向から到来する電波だけを受信する対策である [4]．問題点は，受信装置が物理的に大きくなること，位置が刻々と変化する移動体では，利用しにくい点がある．

(2)地上システムの堅牢化

地上環境の物理的な防御は，アクセスコントロールシステムなどの防御装備を構築することである．

また，ジャミング対策として攻撃者が接近可能な位置から視認できないように地上局の衛星アンテナを防護施設等により，秘匿することである．

(3)衛星システムの堅牢化

衛星システムは，放射能，流星，スペースデブリ等の宇宙空間の厳しい環境や意図的な攻撃に耐える程，十分な堅牢性をもつ設計をしなければならない．また，被害を最小限にするため，複数の衛星や地上局を組み込んだ冗長性ある衛星ネットワークを構築することが必要である [21]．

**4.2 GPS に対するセキュリティ対策**

GPS は，暗号化や認証がなく，諸元が米政府機関によって公開cされているため，技術力さえあれば，GPS 受信機及び GPS 信号を作成できる．

GPS に対するセキュリティ対策は，前項の宇宙システムに対する対策の他，次のものがある．

**4.2.1 他センサーの使用**

GPS 以外の位置情報把握センサーを併用し，GPS 信号と比較することにより，矛盾点をチェックする方法である [4]．航空分野では APNT(Alternative Position, Navigation, and Timing)，海洋分野では，eLORAN (e Long-Range Navigation) が使用されている．

**4.2.2 受信機ネットワーク**

複数の受信機で受信機ネットワークを構築し，ネットワークに参加している GPS 受信機同士が相互に情報交換し，矛盾点を検知する方法である [4]．攻撃者は，GPS 衛星と同じ位置に送信アンテナを設置することは不可能であり，特定の地点の GPS 受信機に対して攻撃した場合，他の地点では矛盾を生じることになる．

**4.3 日本の重要インフラに対するセキュリティ対策**

**4.3.1** 第 3 次行動計画に対する評価

第 4 次行動計画策定にあたって，第３次行動計画の評価を行なっており，各種重要インフラ分野におけるガイドライン等及び各重要インフラ事業者等における内規等の行動規範は，それぞれ自主的な見直しが進められており，重要インフラ事業者等の行動規範として浸透しつつあると認めるとしている．

また，重要インフラの情報セキュリティ対策は，平成 12 年以後，行動計画として策定・公表され，5 つの施策群（安全基準等の整備及び浸透，情報共有体制の強化，障害対応体制の強化，リスクマネジメント，防護基盤の強化）に基づく対策が着実に進展していると評価している．

**4.3.2** 第 4 次行動計画の方針

第 4 次行動計画は,「サイバーセキュリティ基本法」の基本理念に則り，第 3 次行動計画及び「サイバーセキュリティ戦略」を踏まえて策定されており，前述の５つの施策群を基本的な骨格として維持している．この施策群を補強・改善するものとして 3 つの重点的な取組方針を定め，そのうちの一つに,「重要インフラ事業者等における先導的取組の推進」があり，他の重要インフラ分野からの依存度が高く，かつ，比較的短時間の重要インフラサービス障害であってもその影響力が大きくなるおそれのある重要インフラ分野として，電力，情報通信，金融を挙げている．これらの分野は，相対的に高度な情報セキュリティ対策を自主的に実施し，推進している実態があり，更に強化・推進していく必要があるとしている．

一方，電力，情報通信，金融分野は，GPS 時刻信号が重要な役割を果たす分野である．

更に，第 4 次行動計画別紙では，重要インフラ分野毎に「対象となる重要システム」及び「重要インフラサービスの障害」が例示されている．この中で，広域分散システムやタイムスタンプが必要なシステムは，GPS 時刻信号が必須のシステムである．

**4.4 日本の重要インフラと GPS 時刻信号の関係**

重要インフラに対する脅威は,以前から認識されており，2005 年に情報セキュリティ政策会議が決定した「重要インフラの情報セキュリティ対策に係る行動計画 [22]」には，既に重要インフラに対する対策が記載されている．しかし，標的型攻撃や DDoS 攻撃，マルウェア感染，サプライチェーンなど従来のサイバー攻撃が想定されており,これらの対策は，重要インフラ事業者や官公庁にも浸透しており，対策が採られている．しかし，第 4 次行動計画からは，重

c https://www.gps.gov/technical/icwg/

要インフラと GPS 時刻信号の依存関係や GPS の脆弱性を認識しているということは読み取れず，未対策である．

一方，GPS の専門家は，早くから GPS の脆弱性を認識し，技術力があれば，簡単に GPS 受信機を作成でき，かつ GPS 信号を作成又は欺瞞できることを指摘している [4].

したがって，重要インフラ事業と GPS の専門家が情報共有を図り，重要インフラに対する GPS 時刻信号の重要性について共通の認識を持ち，対策を採らなければならない．

## 5. 米国の取り組み

### 5.1 米国の重要インフラに対する取り組み

米国の重要インフラ保護への対応は、1993 年 2 月のニューヨーク世界貿易センター爆破事件と 1995 年 4 月のオクラホマ連邦政府ビル爆破事件という 2 つの出来事が大きく影響している [23]．このとき，米国は，重要インフラがテロの脅威に晒されていることを認識し，9.11 同時多発テロを契機として国土安全保障省を発足させ，重要インフラに対するテロ対策及びサイバー攻撃対策の取り組みを行い、最終的に重要インフラ 16 分野を選定した。

### 5.2 米国の重要インフラに与える GPS の影響

国土安全保障省は，重要インフラが GPS 時刻信号に依存していることを認識しており，ジャミング等から防護する対策を採っている．別の調査では，米国の重要インフラ 16 分野のうち，エネルギー，防衛産業基盤，医療・公衆衛生，金融サービス，商用原子力施設・核燃料・核廃棄施設，化学産業，商業施設，重要な製造業，ダム，情報技術，通信，緊急サービス，政府施設，人・物の輸送の 14 分野において GPS 時刻信号が使われているとしている [24].

### 5.3 米国による GPS の調査及び研究

#### 5.3.1 GPS の脆弱性調査

米国は，早くから GPS の脆弱性を認識しており，国防総省が，GPS の脆弱性を 9 ヶ月に渡って調査したところ，調査対象エリア内で，のべ約 782 時間中断（調査機関 9 ヶ月の約 12%）が発生し，アメリカ大陸の約 4.5%に影響を与えていると発表した [15]．国土安全保障省は，この結果に高い関心を示し，エネルギーセクターとともに「U.S. GPS Interference, Detection and Mitigation Program」を立ち上げた．

GPS 信号の中断は，米国の国家安全保障，国土安全保障，経済安全保障に影響を与えるため，GPS のバックアップの法案を提出した [25].

#### 5.3.2 GPS 脆弱性の研究

国土安全保障省 Science and Technology Directorate では，GPS 受信機に対するジャミング，スプーフィング試験，正確な時刻を配信する代替手段，GPS の中断を認識する技術，PNT 運用要求の理解の深化を研究している [26].

### 5.4 米国による GPS 脆弱性対策

国土安全保障省は，一般に使用されている GPS 信号は，低出力で暗号化されておらず，干渉やジャミングに対して脆弱であることから，抗たん性を高めるため，ベストプラクティス [27]及び改善策 [28]を Web サイト上に公開しているd. 前者は，ユーザが正確な時刻信号を受信するためのベストプラクティスが記載され，後者は，国土安全保障省が GPS 関連のオーナー，オペレータ，研究者，設計者及び製造業者に対し，GPS 信号のセキュリティ及び抗たん性を改善する情報が記載されている．

このように，米国は，GPS 時刻信号の重要性を早くから認識し，重要インフラ事業者のみならず，広く関係者に対して対策を具体的に公開している．

## 6. 議論，評価

### 6.1 GPS 時刻信号のサービス停止

#### 6.1.1 同時受信数

GPS 受信機が，時刻信号を受信する場合，最低 1 個の GPS 時刻信号が必要である．

一方，GPS 受信機は，常時少なくとも 6 機，多いときは 10 機以上の GPS から信号を受信することが可能である上 [6]，信号を受信できない場合は，他の航法衛星によって補完することが可能である．

#### 6.1.2 サービス停止のための攻撃

GPS 自体又は GPS 時刻信号を受信する受信機に対する攻撃が成功すれば，GPS 時刻信号の配信を停止させ，重要インフラのサービスを停止することが可能である．

よって，GPS 又は GPS 受信機に対するサイバー攻撃，ジャミング又はキネティック攻撃の可能性を考察する．

(1)サイバー攻撃の場合

6 機の GPS に同時を攻撃するためには，まず，GPS をコントロールしている地上システムに侵入しなければならない．GPS のコントロールは，米空軍が 24 時間体制で実施しているため，システムのセキュリティは堅牢であり，システムの侵入は困難である．一方，GPS 受信機は,脆弱であるため，サイバー攻撃が可能である．

(2)ジャミングの場合

アップリンクジャミングの場合，大出力かつ指向性の電波で，6 機の GPS 対して同時にジャミングを実施しなければならないため，困難である．重要インフラの受信機に対するダウンリンクジャミングは，可能である．

(3)キネティック攻撃の場合

GPS 自体をキネティック攻撃する場合，少なくとも 6 機の GPS を同時に攻撃しなければ，重要インフラのサービスを停止することが出来ない．しかし，6 機の GPS に対して少なくとも 6 発のミサイルを誘導して攻撃すること

d https://www.dhs.gov/science-and-technology/gps-program

は，技術的な面及び費用の面から極めて困難である．また，1機の衛星の破壊に伴うスペースデブリに対しても非難が挙がっている現状から，6機分のスペースデブリは国際社会に到底受け入れられないと考えられる．更に，キネティック攻撃は，アトリビューションが可能であるため，米国からの反撃を覚悟しなければならないことを考えると，キネティック攻撃による重要インフラのサービス停止は困難と考える．

#### 6.1.3 評価

重要インフラのサービスを停止するためには，重要インフラが有するGPS受信機をサイバー攻撃又はジャミングにより攻撃することが適当である．

逆に考えると，衛星システム及び地上システムにおいては，抗たん性や冗長化の対策が採られていることを意味している．重要インフラのサービスを停止させる場合，GPS時刻信号を受信するユーザシステムが最も脆弱であり，狙われやすいということになる．

### 6.2 重要インフラに対するGPS時刻信号のジャミング対策

#### 6.2.1 重要インフラ対策の現状

サイバーセキュリティ戦略本部が，第4次行動計画を策定し，重要インフラのセキュリティ対策は重要インフラ事業者が自らの責任において実施しつつ，政府レベルでも対策を採っている．

また，第3次行動計画の評価において，行動計画等は，策定されてから通算16年を経ており，対策が着実に進展し，定期的な評価により適切な見直しが行われたものと評価している [3].

しかしながら，重要インフラに対する対策は，従来のサイバー攻撃を想定した対策に終始しており，重要インフラがGPS時刻信号に依存していることを認識し，GPS時刻信号に対するジャミング等を脅威として捉えた対策は採られていない．

また，第4次行動計画別紙では，重要システムの不具合が引き起こす重要インフラサービスの障害を例示しているが，金融分野では預金の払い戻しの遅延・停止，保険金等の支払いの遅延・停止等，電力分野では，電力供給の停止など，国民生活に多大な影響を及ぼすことが想定されている．したがって，特に金融，電力では，サービスを維持するためには，標的型攻撃等の対策のみでは不十分であり，GPS時刻信号を正常に受信するための対策が必須である．

#### 6.2.2 GPSのジャミング対策

重要インフラのセキュリティ対策の枠組みでは，GPSのジャミング対策は，明確には採られていないが，宇宙システムの枠組みやGPS研究の枠組みでは，GPS信号の脆弱性が指摘され，対策も具体的に検討されている．

また，米国では，重要インフラの大部分を主管する国土安全保障省が，重要インフラに対するGPS自国信号の重要性を認識し，GPSの脆弱性についての研究を行っており，具体的な対策やベストプラクティスをWeb上に公開し，広く対策を促している．

#### 6.2.3 今後の対策

以上のことから，重要インフラの対策を検討するNISCの重要インフラグループに宇宙システム，特に，GPSの脆弱性対策に知見のある者を参加させ，既存のGPS脆弱性対策が重要インフラに適応可能であるか検討する必要がある．また，検討した対策を，「重要インフラの情報セキュリティ対策に係る行動計画」に盛り込み，政府として重要インフラ事業者に広く公開し，周知していく必要がある．

## 7. 結論

国民生活に不可欠な重要インフラとGPS時刻信号の関係を調査した結果，その重要性を認識することができた.重要インフラを維持するためには,GPS時刻信号の安定的な配信が不可欠である. しかし, GPSを含む衛星システムは，悪意ある攻撃者の標的になっており，予想される攻撃をアトリビューション，費用対効果及び攻撃のインパクトの観点から考察すると，サイバー攻撃又はジャミングによる攻撃の蓋然性が高いことが判明した．また，GPS時刻信号に対する攻撃を考えると, GPS自体に対する攻撃は,現実的ではなく，GPS受信機に対するサイバー攻撃又はジャミングが実現可能な攻撃法であるが判明した.

また, 重要インフラがGPS時刻信号を確実に受信するための対策を調査すると，従来の標的型攻撃や情報窃取等の従来型サイバー攻撃に対しては，対策が採られているが，公の文書等でセキュリティ対策を明確に読み取ることはできなかった．したがって，今後の我が国のとるべき対策としては，重要インフラとGPS専門家が情報共有を図り，セキュリティ対策に，GPS時刻信号に関する対策も盛り込んでいくことが必要である．

## 8. 参照文献

[1] 吉田直子, “GNSSの基本知識,” 測位衛星技術株式会社, 2016.

[2] M. R. R. L. Matthew Horowitz, "Space Cybersecurity’s Final Frontier," London Cyber Security, June 2015.

[3] サイバーセキュリティ戦略本部, "重要インフラの情報セキュリティ対策に係る第4次行動計画," 25 JUL 2018.[Online].Available:https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf. [Accessed 25 DEC 2018].

[4] 坂井丈泰, "GPSのセキュリティ　脆弱性とその対策," 24 AUG 2018. [Online]. Available: https://www.enri.go.jp/~sakai/pub/sane1808_sakai.ppt.

[Accessed 30 DEC 2018].

[5] トランジスタ技術編集部, GPS のしくみと応用技術, CQ 出版㈱, 2016.

[6] 坂井丈泰, "GPS/GNSS の基礎知識," 電波航法研究所, 2007.

[7] J. Coffed, "The Threat of GPS Jamming The Risk to an Information Utility," Harris Corporation, 2016.

[8] GPS.GOV, "Control Segment," 8 NOV 2018. [Online]. Available:https://translate.google.com/translate?hl=ja&sl=en&tl=ja&u=https%3A%2F%2Fwww.gps.gov%2Fsystems%2Fgps%2Fcontrol%2F&anno=2. [Accessed 13 JAN 2019].

[9] Los Angeles Air Force Base, "Master of Space Keep GSP constellation grounded and on time," 29 FEB 2016. [Online].Available:https://www.losangeles.af.mil/News/Article-Display/Article/734612/masters-of-space-keep-gps-constellation-grounded-and-on-time/. [Accessed 13 JAN 2019].

[10] 日経 NETWORK, “インターネットを支える技術「時刻」のしくみ,” *日経NETWORK,* pp. 24-39, 2018.7.

[11] GPS.GOV, "Timing," 6 MAR 2018. [Online]. Available: https://www.gps.gov/applications/timing/. [Accessed 5 JAN 2019].

[12] 橋本卯夫, "超高速証券取引を可能にする衛星測位連携システム-進化するレイテンシー監視システム-," *IT ソリューションフロンティア 01 2012,* vol. 29, no. 1, pp. 12-15, 2012.

[13] 加藤大祐、堀井博夫、河原大一郎, "再生可能エネルギー大量導入を考慮した次世代系統監視制御システムの動向," *日立評論,* vol. 95, no. 12, pp. 807-810, DEC 2013.

[14] NATIONAL INSTRUMENTS, "電力計測・制御システムの内部," NATIONAL INSTRUMENTS, 9 JUL 2013. [Online]. Available: http://www.ni.com/white-paper/14331/ja/. [Accessed 11 JAN 2019].

[15] Symmetricom, "Power Utilities; Mitigating GPS Vulnerabilities and Protecting Power Utilities Network Timing,"2013.[Online].Available:https://aventasinc.com/wp-content/uploads/2017/09/WP_Power_Utilities.pdf. [Accessed 29 DEC 2018].

[16] 佐々木雅英, "宇宙×ICT の安心、安全対策," 22 FEB 2017.[Online].Available:http://www.soumu.go.jp/main_content/000471115.pdf. [Accessed 22 DEC 2018].

[17] A. Crawley, "Successful Cyber Attack Highlights Longstanding Deficiencies in NOAA's IT Security Program," NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION, 2016.

[18] K. J. T. G. R. Todd Harrison, "Space Threat Assessment 2018," CSIS, 2018.

[19] 西村金一, "北朝鮮のサイバー攻撃とＧＰＳ妨害 2012," DEC 2012. [Online]. Available: http://www.mis-research.jp/img/pdf/010.pdf. [Accessed 24 APR 2018].

[20] 青木節子, “自衛隊の衛星利用 : 憲法による制約の考察,” *国際情勢,* pp. 365-378, 2009.

[21] A. A. Hudaib, "Satellite Netowrk Hacking & Security Analysis," *International Journal of Computer Science and Security,* vol. 10, no. 1, pp. 8-55, 2016.

[22] 情報セキュリティ政策会議, "重要インフラの情報セキュリティ対策に係る行動計画," 13 DEC 2005. [Online].Available:https://www.nisc.go.jp/active/infra/pdf/infra_rt.pdf. [Accessed 13 JAN 2019].

[23] 望月武志, "重要インフラのサイバーセキュリティ、米国はどう法整備を進めたのか," デトロイト　トーマツサイバーセキュリティ先端研究所, 30 JUL 2018. [Online].Available:http://www.itmedia.co.jp/smartjapan/articles/1807/30/news013.html. [Accessed 24 NOV 2018].

[24] M. Graham, "GPS Use in U.S. Critical Infrastructure and Emergency Communication," 2012. [Online]. Available: https://www.gps.gov/multimedia/presentations/2012/10/USTTI/graham.pdf. [Accessed 4 JAN 2019].

[25] A. Dhuria, "RELIANCE ON GPS FOR CRITICAL INFRASTURE AND THE NEED FOR GPS DISCIPLIED OSCILLATOR," Bliley Technologies, 2017.

[26] J. Dragseth, "The Office of Infrastructure Protection," 15 SEP2015.[Online].Available:https://www.gps.gov/cgsic/meetings/2015/dragseth.pdf. [Accessed 4 JAN 2019].

[27] Homeland Security, "Best Practice for Improvement Robustness of Time and Frequency Sources in Fixed Locations," Homeland Security, 2015.

[28] Homeland Security, "Improving the Operation and Development of Global Positioning System(GPS) Equipment Used by Critical Infrastructure," Homeland Security.