

重要インフラに与えるGPS時刻信号の重要性の調査

Research of the importance of GPS timing affecting critical infrastructure

角田泰基・ネットワーク分科会・情報セキュリティ大学院大学

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. In order to research the importance of the GPS time data given to critical infrastructures, I research the relation between GPS and critical infrastructures, I will draw necessary measures for our country.

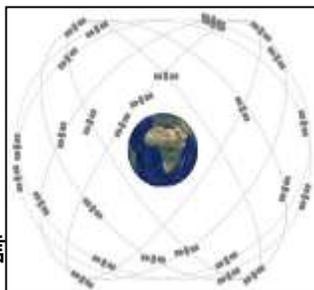
1. はじめに

重要インフラの維持にGPS時刻信号は、不可欠である。重要インフラに対する従来のサイバー攻撃対策は定着しているが、GPS時刻信号に対するセキュリティ対策は、重要インフラ分野では採られていない。一方、GPS専門家は、脆弱性を指摘している。本研究では、重要インフラに与えるGPS時刻信号の重要性を調査し、対策を導出する。

2. GPSと重要インフラ

2.1. GPSについて

- ・ GPS: 31個,
6軌道面×4個以上衛星
- ・ GPS運用期間: 約10年
- ・ 周期: 11時間58分
- ・ 高度約20,200kmを周回
- ・ 常時6~10機のGPS受信



2.2. GPS時刻信号

- ・ GPSは、セシウム等の原子時計2個以上搭載
- ・ 宇宙用セシウム発振器の精度は 10^{-13} 程度
- ・ GPSは、UTCと誤差40ナノ秒程度で時刻配信

2.3. GPS信号と重要インフラ

※青字は、重要インフラ

用途	分野	システム・サービス
航法誘導	航空・空港・鉄道	空港への精密進入、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、航空測量(UAV)、農業散布(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) 可降水量測定、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
	電力・ガス	送配電網管理、スマートグリッド

3. 衛星に対する攻撃

GPSを含む衛星システムに対する攻撃は、大きくサイバー攻撃、ジャミング、キネティック攻撃が想定され、アトリビューション、費用対効果、攻撃のインパクトの観点から分類すると次のとおり。

	サイバー攻撃	ジャミング	キネティック攻撃
アトリビューション	困難	困難	容易
情報収集	労力大	労力大	労力大
費用対効果	安価	安価	設備、開発費多額、 巨大な設備
技術	高度	低	高度
攻撃の柔軟性	多様なサイバー攻撃	アップリンクとダウンリンク	ミサイル攻撃
攻撃効果	可逆	可逆	不可逆
効果の確認	困難	困難	容易
その他	インパクトコントロール可	電波到達圏内	攻撃はASAT到達圏内

4. GPSセキュリティ対策

GSPに対するセキュリティ対策は以下のとおり

セキュリティ対策	細部
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
暗号化による対策	・ GPSでは、公開鍵暗号方式によりデジタル署名を施す方式
施設に対する対策	・ 指向性アンテナ、地上システムの堅牢化、衛星システムの堅牢化
多センサーの使用	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 航空分野ではAPNT、海洋分野ではeLORAN
受信機ネットワーク	多数のGPS受信機の受信情報を比較・照合して、矛盾点を検知する方法である

5. 考察

5.1. GPSに対する攻撃

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。

5.2. セキュリティ対策

重要インフラ対策を検討する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