資料２

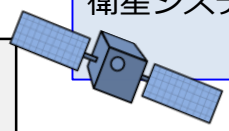
GPSの機能低下が金融システムに及ぼす影響に関する調査

平成30年9月20日

三井物産セキュアディレクション株式会社
公共事業部　宇宙・防衛グループ

衛星測位システム(GNSS)測位信号に対するSpoofing（なりすまし）攻撃

脅威の例：
改造したGNSS信号シミュレータによるSpoofing攻撃



衛星システム

通信リンク
（RF）

地上システム

ユーザ側システム

リスクシナリオ構成要素

- 人為的に偽の GNSS送信信号を模倣した信号を作り出し、目標とする受信機に受信させ、その使用者(情報システム)が認知する位置もしくは時刻情報を誤らせる。
- Spoofing攻撃に用いられる擬似的な改造されたGNSS信号シミュレータは数万ドルから数十万ドルで流通しており、テロ組織のような一定の資金力を持った反社会勢力が利用するリスクが大きい。

想定される影響

＜金融取引システムを題材として考察＞

✓テロ組織等の反社会的勢力が資金源として金銭を窃取することを企図し、金融取引システムに高精度な時刻情報を提供するGPS信号に対しSpoofing攻撃を加え、取引システムに障害が発生した隙に株価の変動を利用して鞘取りを行う。

✓金融取引のシステムは当然高いセキュリティレベルを担保した上で構築されているためこのような事態が現実に起こる可能性が高いとは言い難いが、複数の悪条件が重なった場合を想定する。

情報システムにおける時刻同期の仕組みについて

- 高精度な時刻同期を必要とする事業者のシステムではGPS等のGNSSを時刻ソースとするグランドマスタークロック（タイムサーバ）を設置している。

【精度の例】
- タイムサーバはNetwork Time Protocol (NTP) にてGPS(修正精度±1ms以内)、テレホンJJY (同±10ms) 、長波JJY (同±100ms) 、FM (同±100ms) を時刻ソースとして取得する。

【主なユーザ】
- 放送事業（放送設備）
- モバイルキャリア事業（基地局間同期）
- 金融事業（証券／対外取引）
- 鉄道事業（運行／送電管理）
- 電力事業（変電所間同期）
- IoT事業（センサー監視）　等

GPSと時刻同期ができない場合の機器の動作

- タイムサーバ側で[内部時計同期時間] にて設定した時間内（デフォルト設定で24時間）であれば、時刻源と同期ができなくとも時刻配信することができる。
- 設定した時間を経過してしまうと非同期の状態となる。

出所）セイコーソリューションズ株式会社,
http://www.seiko-sol.co.jp/wp-content/uploads/2016/03/TimeServer.pdf

超高速トレーディング環境について

- トレーディングシステムでは、アプリケーションレベルの時間遅延（レイテンシー）を正確に把握し、これをいかに縮めるかが重要となる。 証券取引所・金融情報サービス企業と証券会社・投資銀行のトレーディング基盤の間や証券会社・投資銀行の拠点間のレイテンシーを検知するためには、協定世界時(UTC)との同期誤差が50nsから100nsであることが必須となる。GPSとUTCの誤差は数十ns以下であり、この要求水準を満たすのはGPS（GNSS）のみである。

- 最近の超高速トレーディングシステム向けのレイテンシー監視システムでは、GPSと20ns～100nsの精度で時刻同期が取れるPrecision Time Protocol (PTP)と組み合わせたタイムスタンプが実装されている。

（補足）
このレイテンシーにより注文時の表示価格と実際の約定価格に差額が生じることを証券業界では「スリッページリスク」と呼ぶ。

出所）野村総合研究所， 超高速証券取引を可能にする衛星測位連系システム，
https://www.nri.com/jp/opinion/it_solution/2012/pdf/ITSF120103.pdf

PTP (Precision Time Protocol）とMiFIDⅡ(欧州第2次金融商品市場指令)

MiFIDⅡ(欧州第2次金融商品市場指令)における時刻精度要件

- 2018年からEUではMiFIDⅡ(欧州第2次金融商品市場指令)が適用。そのひとつの要件として、取引の透明度を満たすため各金融機関に求められる時刻同期の要件が厳しく定義されており、従来のNTPによる時刻同期（精度msレベル）を超えPTPによるμs以下の同期精度が求められている。

■MiFIDⅡの時刻精度要件
- ✓ 時刻基準：UTC(協定世界時)に同期していること
- ✓ 時刻の確度(UTCからの誤差)：100μs以内（高頻度アルゴリズム取引の場合）
- ✓ 時刻の粒度(時刻表示の桁)：1μs以上（高頻度アルゴリズム取引の場合）

国内においてもPTPサービスを提供するデータセンター事業者が登場

- データセンター事業者であるアット東京ではMiFIDⅡの時刻精度要件に対応したサービスの提供を2018年春から開始することを発表。
- データセンターにおいてGPSアンテナ～PTPグランドマスター～顧客までの構内配線を完全2系統で提供することで冗長性を確保。

出所）アット東京プレスリリース， http://www.attokyo.co.jp/news/20171221.html

PTPに対応するタイムサーバのスペック例
- ✓ 修正精度 UTC within <100ns（GNSS同期時）
- ✓ 時刻ソースはGNSS(GPS・QZSS)、ToD(放送局標準時計装置から出力されるシリアル時刻情報)、光テレホンJJYから選択
- ✓ 原子時計を内蔵

出所）セイコーソリューションズ株式会社， http://www.seiko-sol.co.jp/wp-content/uploads/2016/03/TimeServer.pdf

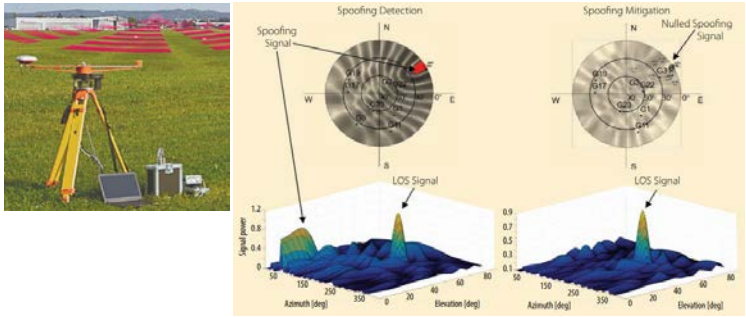
参考）海外におけるSpoofing攻撃への対策検討（例）

- 欧米では以下に示すような対策を複数組み合わせる「多層防御」の視点からGNSSのResiliencyを高めるという考え方が重要であるという議論が交わされている。

1）受信機側での対策

- ”Selective Availability Anti-Spoofing Module（SAASM）”を組み込んだGPS Military Code（Mコード）対応タイムサーバ（米国）
- Anti-spoofing対応受信機 “Multi-Constellation and Multi-Frequency Receivers”
- 測位信号到来方向の識別によるSpoofing攻撃の回避（例えば、回転GNSSアンテナによる研究開発として ESAによる”the Galileo Evolution Programme EGEP funded project SETI (No. EGEP-ID 89-1.11)”がある）
- 測位信号の暗号化と１～２分おきの認証確認

Microsemi SyncServer S650
(GPS Directorate Security Approval認証取得)
出所）Microsemi社



Spoofing信号の到来方向の推定と軽減に関する研究開発
出所）Inside GNSS

2）複数システムによる冗長化

- （航空機や車両等の移動体において）IMUやLIDAR等とのセンサフュージョン
- 複数のPNTソースからの情報取得（eLoranの整備や低軌道衛星の活用、複数GNSSからのデータ収集）
- “Simultaneous spatial consistency” 物理的に離れた受信機の測定値データを比較することでPNTデータの正しさを検証

3）組織マネジメント面での対策

- TTXをはじめとする各種机上演習等の実施（例えば 米国DHSによるストリートワイドでのJam-X演習、GPS関連機器メーカが参加するThe GPS Testing for Critical Infrastructure (GET-CI) コンテストの開催　等）

出所）各種海外カンファレンス、海外関係機関インタビュー等より三井物産セキュアディレクション作成