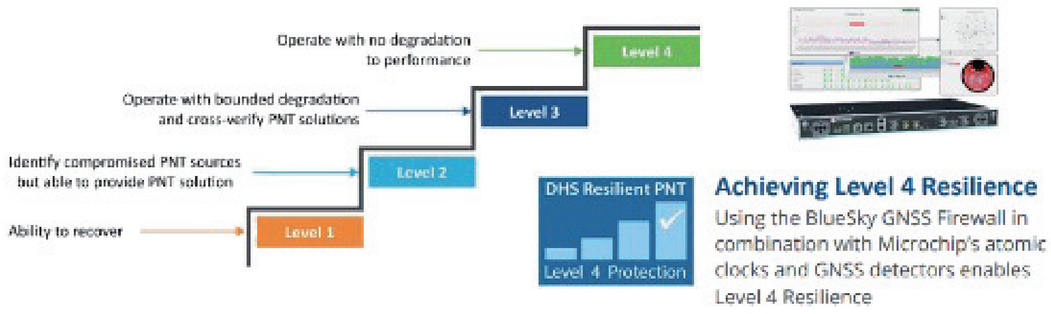
GPS/GNSS脆弱性対策の第一歩

位置･航法･時刻（PNT）システムの現在

現代では多くのシステムが、位置･航法･時刻（PNT）をGPS/GNSSに依存しており、各国の安全保障機関はこの点を潜在的なサイバーセキュリティ攻撃の標的であると捉えています。米国では国土安全保障省が位置･航法･時刻の強靭性に関する適合フレームワーク文書を公開し、4段階のレベルに分けてセキュリティ対策を求めています。
日本国内でも技術的な調査と対策が行われており、より安全で信頼性の高いGPS/GNSSシステムの確立に向けた取組みが進んでいます。



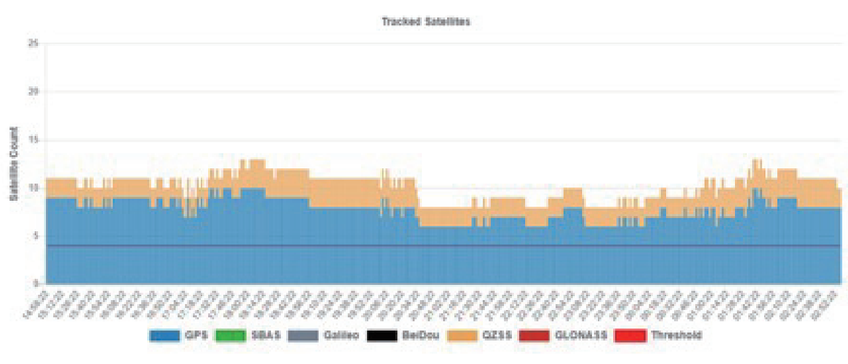
ジャミング･スプーフィングの脅威

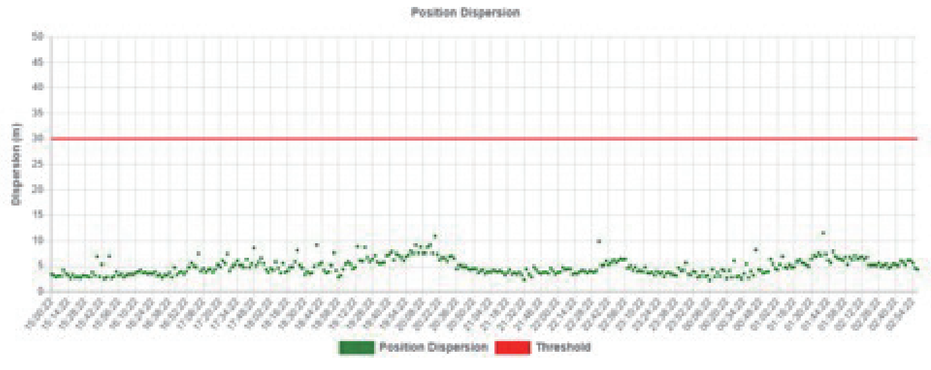
GPS/GNSSは、あらゆる重要インフラに欠かせない技術ですが、近年はそのセキュリティに関する懸念が高まっています。特に、ジャミングやスプーフィングといった攻撃手法により、GPS/GNSS信号が乱される事例が増加しています。このような攻撃を受けると、位置情報や時刻情報が改ざんされてしまい、交通インフラ、通信システム、金融システム、防衛システムなど、あらゆる重要インフラが影響を受ける可能性があるため、GPS/GNSSへの適切なセキュリティ対策が不可欠です。

GPS/GNSSモニタリング

システムの信頼性向上の第一歩として、弊社からはGPS/GNSS信号のモニタリングを提案します。
モニタリングにより、不正な信号や攻撃が検知されれば適切な対策を講じることができるだけでなく、過去のデータを分析することで将来の問題予測や障害時の原因分析が可能になります。
また、Microchip社の提供するGPSファイアウォール･周波数標準と組合わせれば、より強靭なシステム構築が可能になります。

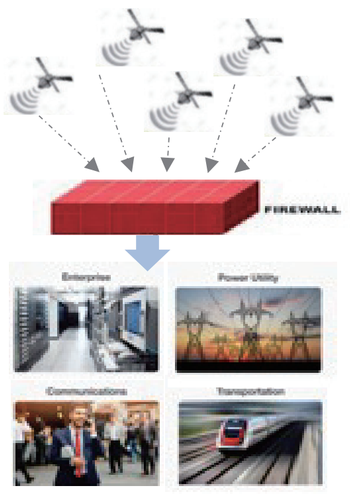
- Maximum C/No　：最大受信レベル（C/No）※受信している衛星の内、最大値のみを記録
- Tracked Satellites　：各衛星ごとの捕捉数 ※GPS/SBAS/GALILEO/BEIDOU/QZSS/GLONASS ※要マルチGNSSオプション
- Position Dispersion　：測位位置からの変動幅（m）
- CW Jamming　：同一周波数帯における干渉波信号の割合（%）
- Automatic Gain Control　：GNSSレシーバのAGC（Auto Gain Control）レベルの変動（%）※AGCレベルの変動を監視して攻撃を検知する手法





BlueSky GPSファイアウォール

米国Microchip社製BlueSkyは、GPS/GNSS信号への攻撃を検知し、攻撃を受けた場合には、アラートを発報してGPS/GNSS信号をシステムから遮断します。この際、製品内部または外部の周波数標準に参照先を切り替えることができ、システムを停止することなく運用を継続できます。



*ここでは、Microchip社製タイムサーバ SyncServer S6x0シリーズの、BlueSkyソフトウェアオプションの機能を紹介しております。
*仕様や性能は予告なく変更されることがあります。詳細については、担当営業までお問合せ下さい。

アントレプレナ事業本部 イーリスカンパニー　測位タイミング課
TEL:03-3639-1336, E-mail: syncserver@marubun.co.jp

Marubun Since 1844