自動運転を見据えた電波政策とセキュリティのあり方

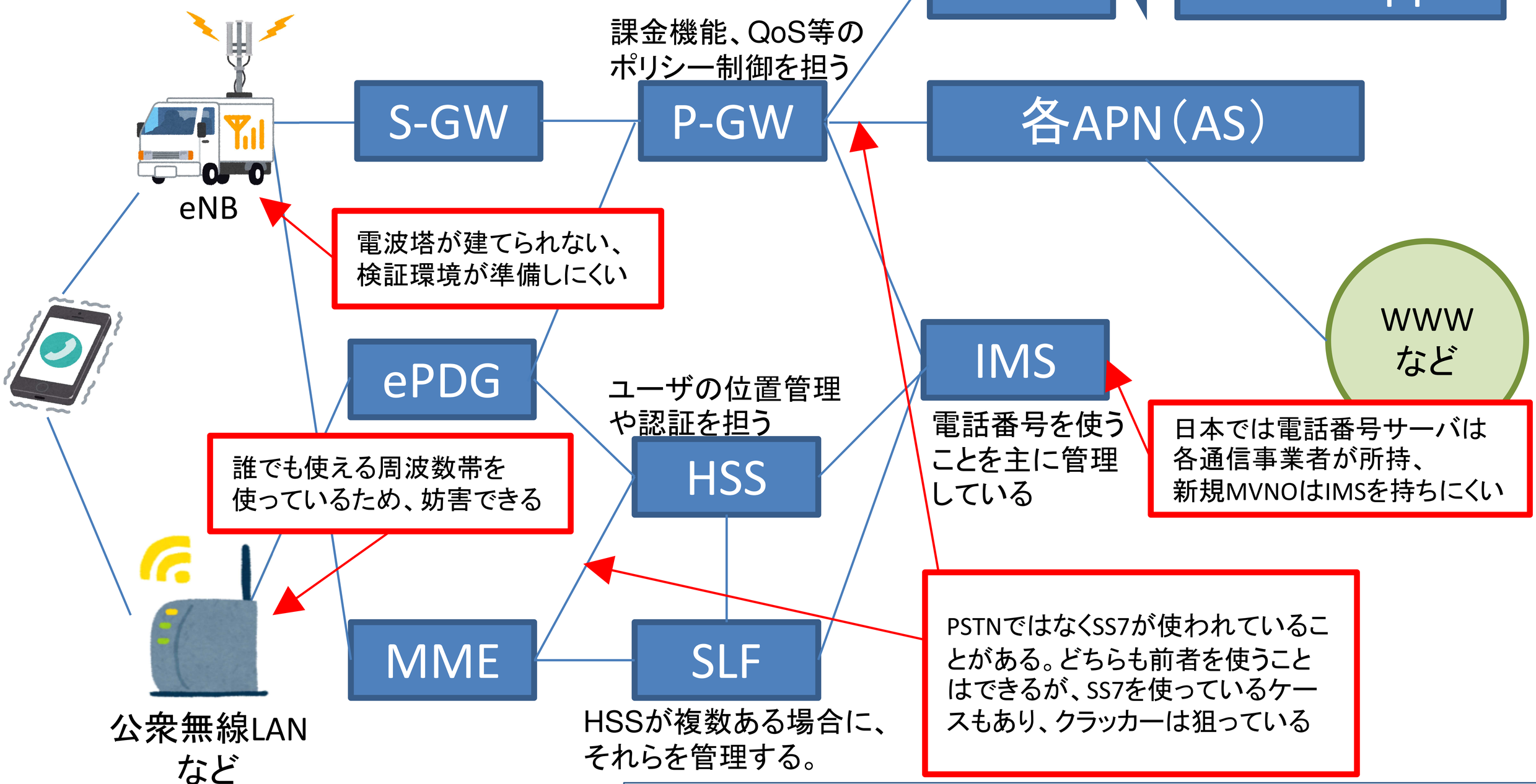
Way of Radio Policy and Security looking for Automatic Connected Car

杉山由朗・システム分科会・情報セキュリティ大学院大学

While everything and M2M Device are about to be connected to the Internet via Wireless, it is not considered to secure communication quality with respect to mobile bodies such as automobiles in particular. In this state, when a mobile body that performs remote control such as automatic driving level 4 comes out, considering the service utilization rate, some side channel attack is added to the ″automatic driving vehicle″ which is the device which is ″the device must not stop″ Etc., it will be possible to cause accidents involving other moving bodies even by disturbing the latency. In this paper, we describe the countermeasures to consider after explaining the background to it.

- 自動車を含め、すべての機器がつながる中で「内部機器の時計にどこまで差があってよいのか」は定義されていない
  - 「携帯キャリア網内」「NTPサーバ」「GPS」など、何で合わせるのか検討されず、ただM2M/IoTのことだけが言われている
- 脆弱性を作りにくく、かつ必要以上にコストをかけないシステムの構築をするうえで、日本ではHLR/HSSがNTTドコモ以外では解放していないため海外向けに輸出するときはシステム更改の量が増す。
- ますますトラフィック量が増えていく中、レイテンシを考慮したうえでの電波の有効利用がしずらい状況にある。

4Gでいうと・・・



まだ4Gがベースとなることを想定し4Gの設計から指摘。イラストは「いらすとや」より。