Anritsu envision:ensure

セルラ通信を使用する車載機向け サイバーセキュリティ脆弱性評価方法

シグナリングテスタ MD8475A/B

コネクテッドカーの普及に伴い重要性を増すサイバーセキュリティ

近年、自動車にセルラ通信を使用した車載器が搭載され、交通情報の取得や遠隔での車両状態監視、スマートフォン連携などのサービスを提供するアプリケーションが展開されています。
こういったアプリケーションを使用して、運転がより快適で安全なものになるような取り組みが各自動車メーカ、車載器メーカによって行われています。しかし、自動車がより便利になる一方で、サイバー攻撃に対するセキュリティ面での問題が顕在化しており、自動車のセキュリティ脆弱性評価が重要性を増しています。

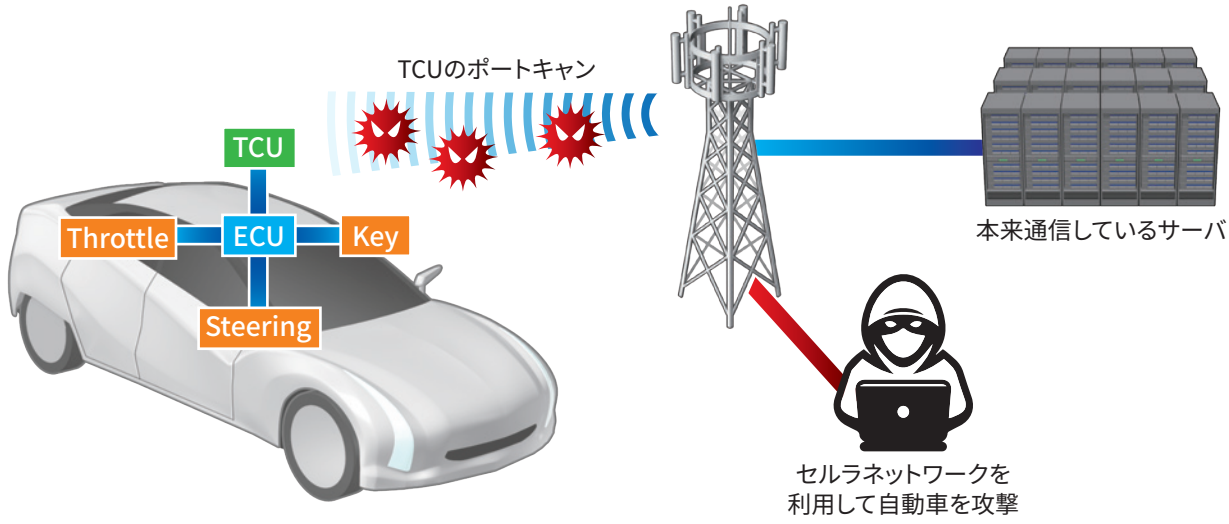

図1：TCUへのポートスキャンを使用したサイバー攻撃

実際にTCU（Telematics Communication Unit）へポートスキャンを実施して、自動車の制御を乗っ取るといったようなサイバー攻撃を受けるリスクがあります。セルラ通信を利用したサイバー攻撃の例として、下記のような事例が報告されています。

- **自己診断用ポートのドングル経由による、SMSでの自動車遠隔操作**
- **CS（Circuit Switched）フォールバックを悪用した、音声通話、SMSの乗っ取り**

今後、自動運転の技術が進んで行くにつれ、ますますこういったサイバーセキュリティが自動車業界での重要な課題となることが予測されます。そのためにも、各自動車メーカ、車載器メーカにおいて事前にサイバーセキュリティへの脆弱性を評価する取り組みが必要になります。

アンリツの基地局シミュレータ MD8475A/Bを利用したセキュリティ脆弱性評価

サイバーセキュリティに脆弱性がある自動車が出回ってしまうと重大な事件や事故に繋がりかねません。
アンリツは、基地局シミュレータ MD8475A/Bを利用した、セルラ通信経由での車載器向けサイバーセキュリティ脆弱性評価方法を提案いたします。
アンリツの基地局シミュレータ MD8475A/Bとサイバー攻撃模擬ソフトウェアを組み合わせることにより、実環境と同等の条件下で、セルラ通信経由のサイバー攻撃の耐性を評価できます。

＊ 組み合わせ可能な製品、評価可能な脆弱性については、担当営業にお問い合わせください。

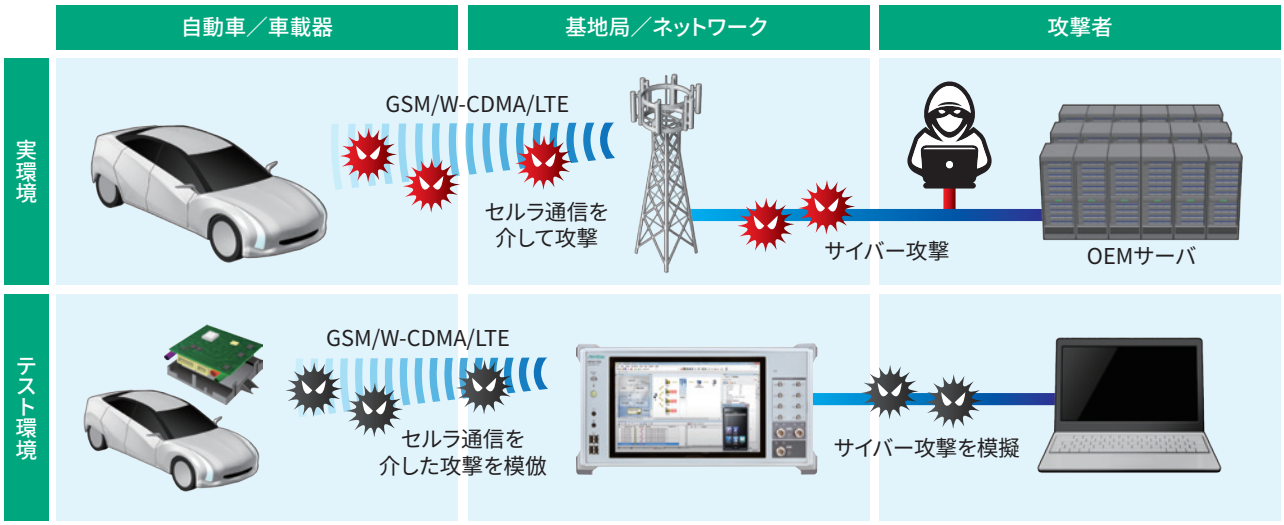

図２：実環境とテスト環境

他サイバーセキュリティ評価への応用

MD8475A/Bは、さまざまなセキュリティ評価システムと組み合わせることができ、ポートスキャン以外のサイバー攻撃に対する脆弱性の評価にも応用できます。
アンリツは現在、DoS攻撃や、なりすましSMS、ファームの改ざんといったさまざまな無線環境下での脆弱性診断を実現する取り組みを実施しております。

アンリツ株式会社
https://www.anritsu.com

計測器営業本部　営業推進部
TEL：0120-133-099/FAX：046-296-1248
E-mail：SJPost@zy.anritsu.co.jp

MD8475_Security-J-A-2-(1.00)　2019.02　ddcm/CDT