NRI 未来創発
Dream up the future.

NRIセキュアテクノロジーズ
NRI SecureTechnologies

News Release

2017 年 5 月 25 日
NRI セキュアテクノロジーズ株式会社

「車両システムセキュリティ診断」サービスの提供を開始

～自動車や搭載機器を対象としたセキュリティ診断を専門チームが支援～

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、代表取締役社長：小田島 潤、以下「NRI セキュア」）は、自動車の車両全体および搭載機器を対象として、情報セキュリティに関する診断や評価を専門的に行うチームを立ち上げるとともに、「車両システムセキュリティ診断」サービス（以下「本サービス」）を本日から提供します。

■ 深刻化する自動車へのサイバー攻撃

昨今、燃費向上や自動運転実現のため、自動車には外部のネットワーク・スマートフォンや USB メモリなどのデバイスと接続する情報通信機器の搭載が増えています。これらはサイバー攻撃の対象として注目されるようになっており、不正な遠隔操作などがあると、人命に関わる重大な問題につながりかねません。

アメリカでは、自動車や運転者の安全を監督している米国運輸省道路交通安全局（NHTSA）が自動車へのサイバー攻撃対策に関するガイドライン※1 を昨年公開しており、攻撃者の視点で侵入を試みるペネトレーションテストの実施が求められています。これを受けて、北米を主たる市場とする日本の自動車メーカーや自動車部品メーカーの多くは、現在テストの実施を検討しています。

■ 専門チームによる自動車向けのセキュリティサービス

NRI セキュアではこれまで、自動車関連のシステムに対するセキュリティ評価を数多く提供してきました。今回、車両システムの評価実績を基に評価項目を作成し、「車両システムセキュリティ診断」としてサービス化します。

本サービスでは、組込機器の各種ガイドラインおよび NRI セキュアがこれまで IoT（モノのインターネット）機器向けの「デバイス・セキュリティ診断※2」で培ってきたノウハウを基に、ペネトレーションテストを実施します。車両システム向けペネトレーションテストに関して、多くの実績を持つメンバーを中心に構成した専門家チームを立ち上げ、机上での脅威分析により、リスクシナリオおよび侵入経路を洗い出した上で、実際の車両や搭載機器についてセキュリティ評価・診断を行います。また、自動車メーカーなどが診断を自社で行いたい場合も、専門家チームが支援します。

「車両システムセキュリティ診断」サービスの詳細は、以下の URL をご参照ください。
https://www.nri-secure.co.jp/service/assessment/automotive.html

NRI セキュアは、今後も企業・組織の情報セキュリティ対策を支援するさまざまな製品・サービスを提供し、グローバルな規模で安全な情報システム環境と社会の実現に貢献していきます。

※1 ガイドライン：Cybersecurity Best Practices for Modern Vehicles
（https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf）

※2 デバイス・セキュリティ診断： ゲーム機や電子書籍リーダー、デジタル家電や医療用機器、IoT 機器などを対象に、その機器が抱える脆弱性を既知・未知のものを含め、可能な限り検出するサービス。2012 年 11 月から開始。

【ニュースリリースに関するお問い合わせ】
株式会社野村総合研究所　コーポレートコミュニケーション部広報課　日下部、松本
TEL：03-5877-7100　E-mail：kouhou@nri.co.jp

【サービスに関するお問い合わせ】
NRI セキュアテクノロジーズ株式会社
サイバーセキュリティサービス事業本部　野口、橋本
広報　根本
TEL：03-6706-0622　E-mail：info@nri-secure.co.jp

【ご参考】

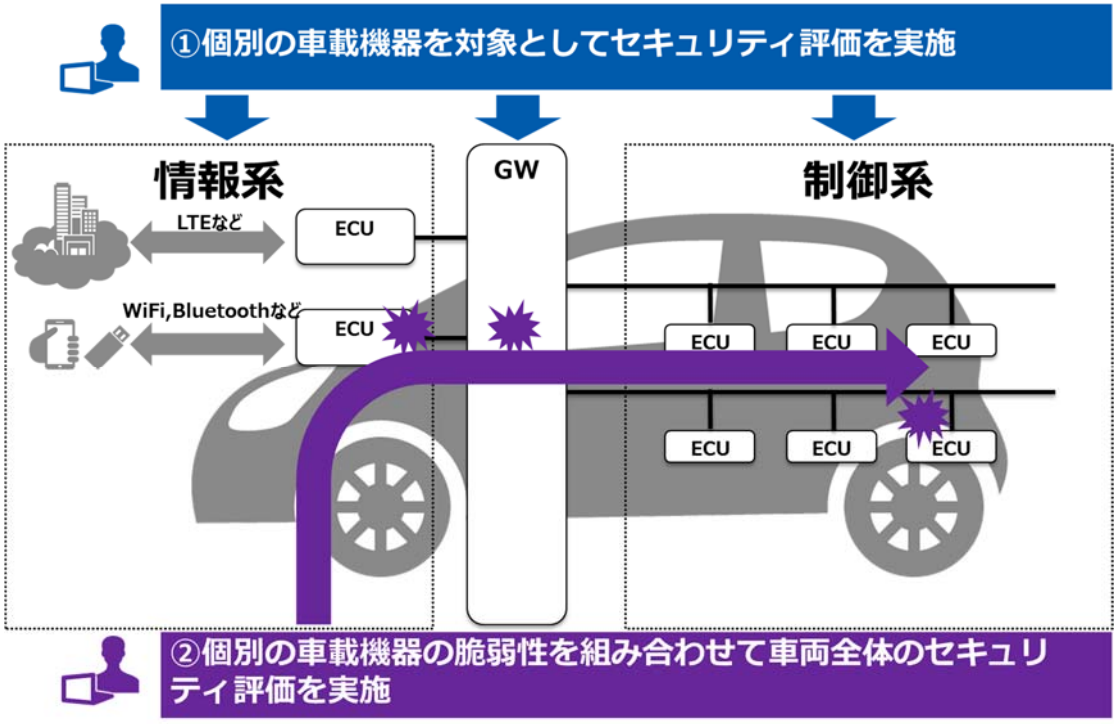
■「車両システムセキュリティ診断」サービスのイメージ

自動車に搭載される機器（ECU※3）やシステムは、外部のネットワークやデバイスと接続する「情報系」、車体の制御を司る「制御系」、その二者間を分離するための「ゲートウェイ（GW）」に大別できます。情報系が外部ネットワークやデバイスから攻撃を受けた場合、GW を経由して制御系へと侵入され、最終的に攻撃者によって不正な運転操作がなされる危険性があります。

本サービスでは、このような脅威に対するセキュリティ上の堅牢性を確認するため、下記の 2 つのフェーズに分けて評価を行います。

① 情報系、制御系の機器および GW について、個別に机上および実機の両方の面からセキュリティ評価を実施。

② フェーズ①で検出された脆弱性を組み合わせた結果、外部ネットワークもしくはデバイスからの攻撃が不正な運転操作に至るかどうかを、実機を用いてセキュリティ評価を実施。



※3　ECU：　Electronic Control Unit。車に搭載されているコンピューターのことで、エンジンやトランスミッションの制御、ABS（アンチロック・ブレーキ・システム）や EBD（電子制御制動力配分システム）などの制動も担っている。