IoT時代のセキュリティ絶対防衛ライン：

“ネットにつながるクルマ”に潜むセキュリティリスク　有効な対抗策とは

http://www.itmedia.co.jp/news/articles/1901/21/news007.html

各業界のIoT関連サービスが抱える問題点、そして有効な対応策とは？　セキュリティの専門機関が情勢を伝えます。

2019年01月21日 07時00分 更新

[エリザベス・バイアー（DigiCert）, **ITmedia**]

この記事はデジサートのWebサイトに掲載された「セキュリティソリューションが必要なコネクテッドカーの現状：PKIの採用」を、ITmedia NEWS編集部で一部編集し、転載したものです。

2020年までに、およそ2億5千万台のコネクテッドカーが全世界の道路を走るといわれています。既に2100万台のコネクテッドカーが実際に運転されており、その多くは私たちが運転している間にもスポーツの試合結果、交通情報、SNSの情報を常時アップデートするといった魅力的な機能を備えています。車同士が通信して連携することも難しい話ではありません。

米McAfeeによれば「コネクテッドカーは携帯電話、タブレットに次いで、急成長中の技術機器である」といわれるほど普及の兆しを見せています。

2018年12月に発表された新型「プリウス」。専用通信機を標準搭載し、コネクテッドカーになった。トヨタ自動車は「クラウン」「カローラ スポーツ」など、新型車のコネクテッドカー化を進めている

一方、セキュリティ上のリスクを懸念する指摘もあります。専門家による研究によって、コネクテッドカーに対する攻撃は不可能ではないことが明らかになっていますが、自動車セキュリティ業界において脅威に対する統一された指針などはまだ存在しないようです。

コネクテッドカーや道路をより安全にするためにはどうしたら良いのでしょうか。結局のところ、コネクテッドカーは守らなければいけないエンドポイントの1つにすぎません。業界全体で導入できるような仕組みは存在するのか、私たちは「ある」と考えます。

連載：IoT時代のセキュリティ絶対防衛ライン

住宅、クルマ、ウェアラブルデバイス、医療、工場のオートメーションなど、あらゆるモノがインターネットにつながる「IoT：Internet of Things」時代が到来しました。生活にインターネットが密着し始めた今だからこそ、これまで以上にセキュリティに気を配る必要があります。

この連載では、SSL／TLS証明書の電子認証局であるデジサートの専門家が、各業界が提供するIoT関連のサービスがどのような課題を抱えていて、どのような手法が対抗策として有効なのかをフラットな視点で伝えます。

コネクテッドカーの潜在的な脅威とは？

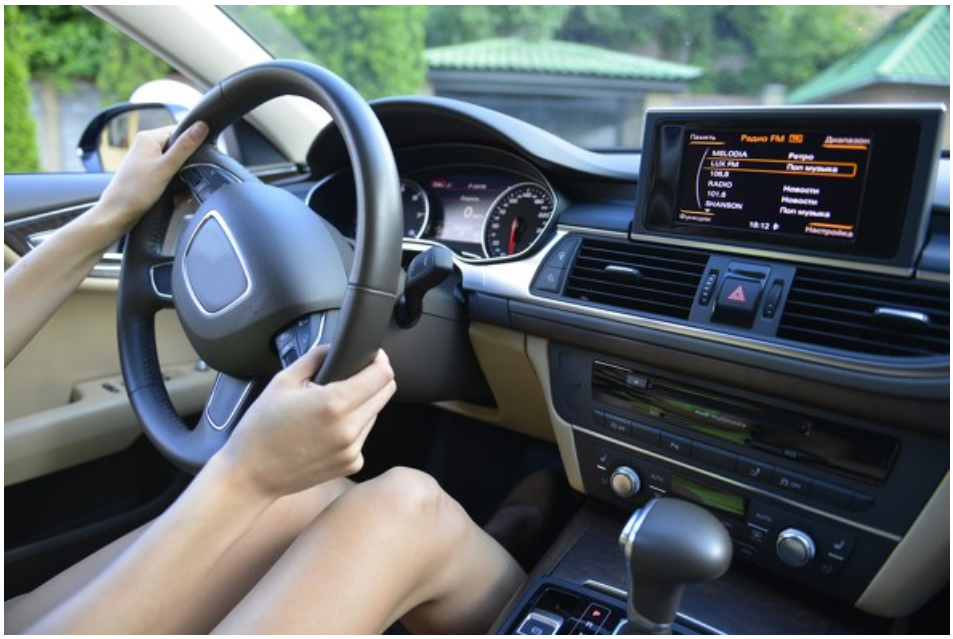
一般的な消費者はインターネットに接続する新しい機器やおもちゃを購入する際、セキュリティについて深く考えません。それよりも、生活をより簡単で便利なものにしてくれるかを購入のポイントにします。クルマも例外ではありません。

コネクテッドカーに車載されるコンピュータは、他のコンピュータと同じように外部との通信によって多くの情報を保存しています。自動車メーカーやセキュリティ専門家たちは、それらが攻撃対象となる可能性があることを知っています。

コネクテッドカー（あるいは実際に接続しているシステム）は、クルマのGPS座標や速度など、あなたの行動を示す特定の個人情報をたくさん収集しています。このデータを自動車メーカー（および潜在的な攻撃者）に提供することで、部品の摩耗を監視してメンテナンス時期を提示するような活用も実現しました。

一方で、組織も危険にさらされています。米General Motorsの車載テレマティクスシステム「OnStar」のようなエンターテインメントや便利なサービスを提供する企業が自動車メーカーと連携しているため、攻撃者は企業のシステム基盤に侵入するためのバックドアとしてコネクテッドカーを使えるのです。

自動車のセキュリティは、情報を危険にさらすだけでなく物理的な危険も引き起こします。あなたの個人情報が流出する以上の危険が存在するのです。悪意のある特注デバイスがあれば、遠隔操作で車を検知し、ロックを解除、そして動かすことができます。最悪の場合、攻撃者は移動中の車を物理的に乗っ取ることさえできます。



米メディアのTechCrunchは、サイバーセキュリティの障害についてより深く掘り下げています。「車のサイバーセキュリティにおける主な課題の1つは、車内のさまざまな電気部品（電子制御ユニット、またはECU）が内部ネットワークで接続されている事です。従って、ハッカーが車のBluetoothや情報提供システムのような脆弱な電子制御ユニットにアクセスできるようになると、ブレーキやエンジンといった安全性の高い電子制御ユニットまでもコントロールし、混乱を招く可能性もあります」。

自動車のサイバーセキュリティは、多くの可動部品が存在するため簡単に解決できない問題であり、堅牢なソリューションが求められています。

コネクテッドカーのためのセキュリティ

幸いにも、多くの自動車メーカーはセキュリティを重要視しています。例えば、米Ford Motorは車両制御システムのネッ

トワークを情報通信システムとは分離して構築し、ソフトウェアの更新やデータ通信を暗号化で保護、Fordによって認証されたソフトウェアだけが車載システムを更新可能にするなど、通信や車両を保護するための仕組みを組み込んでいます。

コードサイニング証明書（コード署名）は、自動車メーカーおよび企業が信頼する発信元と通信のみを承認する電子署名の仕組みです。コネクテッドカーのセキュリティには欠かせない要素です。

コード署名は、PKI（公開鍵基盤）テクノロジーであり、暗号化、実在認証および個人認証などを行って豊富なセキュリティソリューションを提供します。中でも、SSL/TLS証明書を使用してWebサイトにHTTPSを提供するWeb PKIは、最も広く知られているPKIの利用方法です。

全てのPKIシステムには、認証局（CA）と証明書の2つの主要コンポーネントが存在します。認証局は集中管理を行い、個々のユーザーまたはコンピュータに証明書を発行します。これらの証明書がデバイスを識別して安全に通信し、なりすましや物理的な改ざんを防止します。公開鍵暗号は、ネットワーク上の公開暗号鍵を安全に交換するために使用され、データの暗号化、デバイスの認証などに使用できます。

PKIは、さまざまな事例で何十年も利用され、信頼が証明されたソリューションです。インターネットの信頼性は、PKIにより実現されたと言えます。PKIはインターネットに接続する数十億のデバイスやシステムで使用され、暗号化の提供、ユーザーまたはデバイスの認証、個人の認証を行います。これは非常に適応性の高い技術であり、コネクテッドカーにはさまざまな方法で導入が可能です。コード署名がその一例ですが、PKIを使用して個々の車両（あるいは車両内に組み込まれた個別のチップさえ）をそれぞれ認証して、システム間のデータ通信を暗号化し、整合性チェックを行う事が可能になります。

コネクテッドカーがドライバーを保護するための暗号化と認証を導入していないと、2015年に140万台の大規模リコールに発展したJeepのハッキング問題のようなものが表面化するのです。コネクテッドカー向けのPKIによってリモート攻撃を防ぎ、オンラインでセキュリティ更新プログラムを配信し、かつ通信を保護することが重要となるでしょう。

著者：エリザベス・バイアー、日本語監修：デジサート・ジャパン

デジサートは、ベリサイン、シマンテック・ウェブサイトセキュリティとして、SSL／TLSサーバ証明書などを販売していた会社を前身としており、それらの製品を発行する基盤（PKI=公開鍵基盤）で作られたデバイス機器向けの証明書やコードサイニング証明書を発行しています。

関連記事


IoTデバイスは危ない？　インターネット草創期から学んだセキュリティ対策、IoT時代に生かすためにできること
各業界のIoT関連サービスが抱える問題点、そして有効な対応策とは？　セキュリティの専門機関が情勢を伝える新連載。


「英語キーボード」の根強い人気が続く理由
メーカーの中の人だからこそ知っている“PCづくりの裏話”を明かすこの連載。今回は、一部に根強い人気がある「英語キーボード」についてご紹介します。


実は万能ではない？　SIMロックフリー端末の落とし穴とは
メーカーの中の人だからこそ知っている“PCづくりの裏話”を明かすこの連載。スマートフォンで主流になりつつある、音声入力やフリック入力。それでもPCのキーボードがなくならない理由とは？


「LTE対応」のノートPCが少ない理由
メーカーの中の人だからこそ知っている“PCづくりの裏話”を明かすこの連載。今回は、一部ユーザーに根強い人気を持つ「LTE対応」ノートPCのお話。


日本の常識は世界の非常識!?　軽いだけのノートPCが海外で売れない理由
メーカーの中の人だからこそ知っている“PCづくりの裏話”を明かすこの連載。今回は、私が米国担当者に「軽量ノートPC」の提案をしたときの話をご紹介します。