◇KDDI 総研 R&A

2015年5月号

コネクテッド・カー：セキュリティの懸念と通信キャリアとしての市場機会

執筆者　KDDI総研　特別研究員　Jon Metzler（President, Blue Field Strategies）

記事のポイント

サマリー

スマホ普及によりBYODが話題になって久しい。最近、スマホ領域と同様に、Apple、Googleの2大OSプレーヤーは、自動車領域にも進出しており、4つ目のスクリーンの「土地の争奪」に必死だ。

コネクテッド・カー普及につれ、PC・スマホのように、セキュリティのリスクもつきまとう。とくに、自動車搭載のIVI （in-vehicle infotainment）システムは、ドライバー向けコンテンツ配信（地図情報・音楽・店情報・アプリなど）という、非クリティカル情報配信と、車載OSのアップグレードや自動車の診断情報などのよりクリティカル情報送受信を同じ無線通信（LTE / WLAN / BTなど）を通じて行うが、現時点でそれぞれのシステムの仮想化による切り分けが徹底されていない。加えて、AppleやGoogleが自動車市場へ注力しており、そのため、ある米国キャリアは、自動車を次のBYODの戦場として描く。

本レポートでは、コネクテッド・カーの現状と、コネクテッド・カーのセキュリティ・リスクについて紹介し、考察する。また、通信キャリアにとっての、市場機会についてもコメントする。とくに、低遅延のクラウド・サービスと低遅延の通信インフラの整備・提供に市場機会の可能性を感じる。

主な登場者　Ford　GM　BlackBerry　InterTrust　Sprint　Verizon　AT&T　Ericsson　Apple　Google

キーワード　自動車　テレマティクス　コネクテッド・カー　BYOD　セキュリティ

地　域　米国

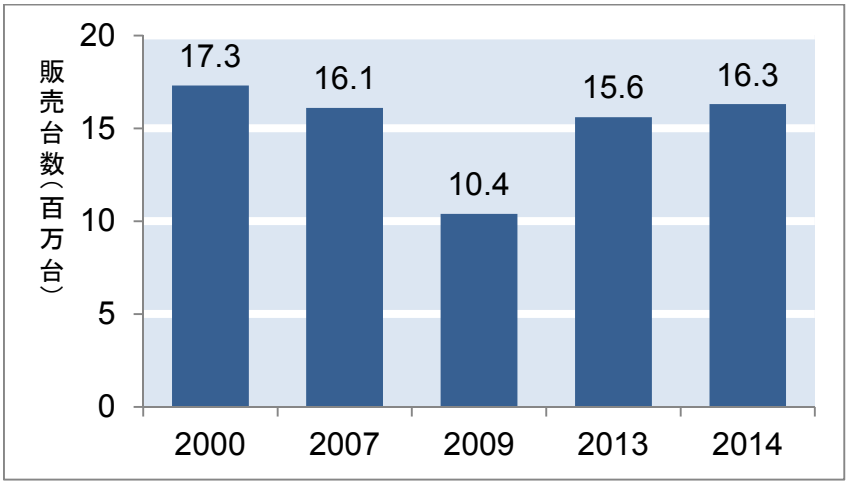
Title	Connected Car: Security Concerns and the Market Opportunity for Telecom Carriers
Author	Jon Metzler, President, Blue Field Strategies
Abstract	With the adoption of connected cars, security concerns have increased. In particular, critical systems, such as diagnostics and automotive OS updates, and “non-critical” systems, such as in-vehicle infotainment systems, share resources but virtualization is still nascent. One example is shared communications resources such as LTE, WiFi and Bluetooth radios. Further, both Apple and Google are investing in the automotive market, to the point that it’s been described as the next battleground for BYOD. In this report, we examine the connected car market and explore various security risks. We then comment on market opportunities for telecom carriers, such as providing low-latency cloud service or low-latency wireless infrastructure for connected car services.
Keywords	Ford GM BlackBerry InterTrust Sprint Verizon AT&T Ericsson Apple Google
Region	United States of America

1　米国自動車市場の現状

2009年の経済危機（クラッシュ）によって大きく再編した米国自動車市場。かつてのBig 3（General Motors、FordおよびChryslerからなるビッグ・スリー・メーカ）のうち、唯一、政府の関与を必要としなかったのはFord社で、GMは一時期国営化されて再編し、またChrysler社はイタリアのFiat自動車によって買収された。また2009年、ピークの2000年の1730万台に対し自動車販売台数が1040万台へ大きく減少した。

しかし、経済復興と自動車メーカ再編に伴い、販売台数が改めて増加し、2014年には販売台数が1630万台に及び、クラッシュ直前の2007年の1610万台のレベルに戻った（図表1参照）。

【図表1】米国自動車市場：販売台数の推移

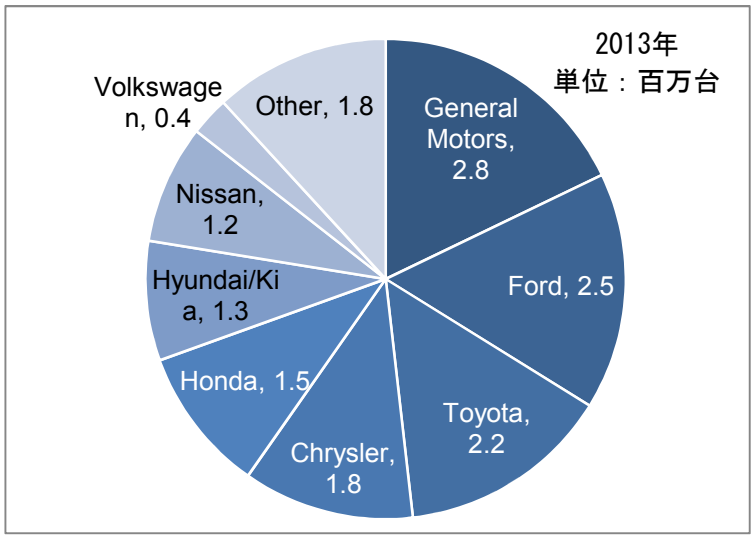


（出典）関連報道によって、執筆者作成

GM、Ford、Fiat Chryslerは3 社とも2011年までに（Fordは、2009年、GMは2010年、Chryslerは2011年）黒字転換を果たし、以降、利益を上げている。

米国における各メーカの販売シェアについては、GMとFordはそれぞれ1位と2位で、トヨタ社は市場3位である（図表2参照）。ホンダと日産は、それぞれ、5位と7位である。

【図表2】米国自動車市場：メーカ別販売台数



（出典）関連報道によって、執筆者作成

2　コネクテッド・カーの普及状況と今後の見込み

コネクテッド・カー（connected car、通信機能のある自動車）が注目を浴びて久しい。毎年1月、米国ラス・ベガス市にて開催されるConsumer Electronics Show（CES）では、コネクテッド・カー関連の展示が多く出展されている。2015年も変わりなく、自動車メーカやサプライヤーのコネクテッド・カー展示が目立った（図表3参照）。

【図表3】Panasonic社のCES展示ブース

（自動車での次世代インフォテーメントについて）

（出典）CES 2015にて、執筆者撮影

各自動車メーカは何かしらのコネクテッド・カー・サービスを提供している。ユ

ースケースは主にふたつで、ドライバー向けコンテンツ配信（地図情報、音楽、店情報や、場合によればapp storeなど）という、非クリティカル・システムへの情報配信と、車載OSのアップグレードや自動車の診断情報などのクリティカル情報送受信である。

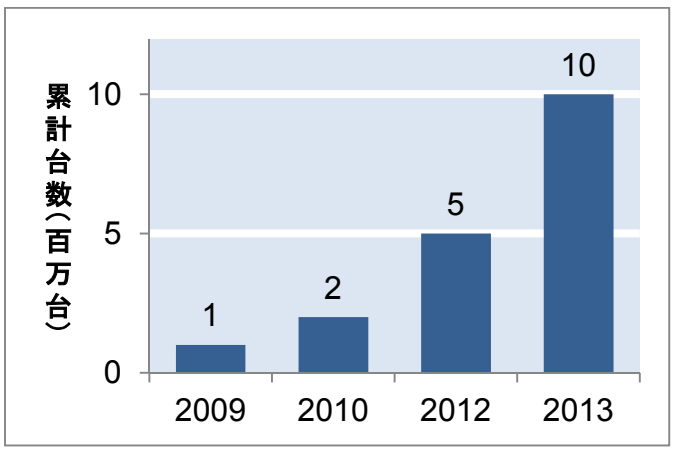
コネクテッド・カーの通信機能は基本的に2 パターンが存在する。Ford Syncのようにドライバーのスマホをモデムとして活用する方法と、TeslaやAudiのように車載3G/4G通信モジュールを使う方法である。

実際、米国市場では、自動車の平均保有期間が11年以上と長く、かつ、自動車の設計期間は約4年のため、設計にあたって通信事業者のネットワーク移行計画を配慮しておく必要がある。したがって、現存のコネクテッド・カーの多くが3G回線を利用するものの、最近のサービス提携事例は基本的に4Gサービスのみを前提とするのである。

平均保有期間が11年ということは、消費者が2年に1度、スマホを買い替えるとすると、1台の自動車を乗り続ける間に、5〜6回もスマホを買い替える可能性がある。ドライバーのスマホをモデムとする方法は、通信会社のネットワーク機能の進化の恩恵を間接的に受けられるのに加え、自社のモデルの設計上、あるひとつのキャリアとの提携を前提としなくて済む。これはFord社のロジックである。一方、Tesla社は高級車に対するリッチなコンテンツ配信（17インチ・スクリーンをフルに活用する地図情報など）と、OSやその他のSWのアップグレードにAT&Tの通信ネットワークを利用する。Tesla社は8万ドルの高級車を販売するのでドライバーの車に対する期待値はその分高い。（Ford社も、2014年から高級車のLincolnにて車載通信モジュールを採用しはじめた。）

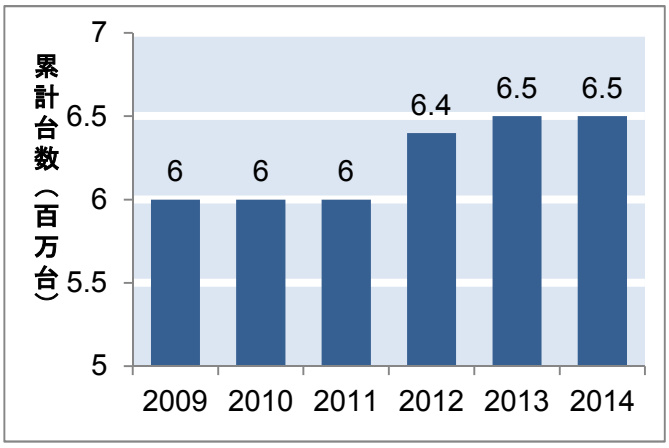
コネクテッド・カーの普及状況はどのようなものなのだろうか。Ford Sync（図表5）とGM OnStar（図表6）の普及台数（累計）を示す。Fordの数字は、米国と欧州へ出荷するモデルの両方を含む。GMの数字は、2012年以降、米国に加え中国へ出荷するモデルを含む。また、2014年から、メキシコでもOnStarサービスを開始した。

【図表5】Ford Syncの普及台数（累計）



（出典）関連報道によって、執筆者作成

【図表6】GM OnStarの普及台数（累計）



（出典）関連報道によって、執筆者作成

ちなみに、GMは、2013年以降、発表資料などにおいてOnStarの普及台数を650万台としており、変えていない。ただ、その間、中国への出荷も、メキシコへの出荷も開始しており、累計が増加していないことに注意すべきである。チャーンのせいなのか、違う理由なのか、現時点で確認できていない。

OnStarは1996年にサービス・インしたテレマティクスの老舗。2013年、AT&Tが、OnStarの通信機能提供契約を長年のパートナーのVerizonから奪ったことは話題を呼んだ。低コストの提案と、グローバルなローミング機能のおかげだといわれる。また、Hughes Telematicsを買収し、VAS（Value-Added Service）を中心とするVerizon Telematicsに対し、AT&Tの自動車メーカに対する提供内容はモジュール化（通信機能のみのオプションからVAS提供まで）されており、よりフレキシブルだという意見もある。AT&Tは、近年、米国キャリアのなかで、コネクテッド・カー領域において、Tesla、Audi、GMなどとの提携を勝ち取り、コネクテッド・カー市場で快調にみえる。

前述した通り、Ford Syncのようにドライバーのスマホの通信機能を活用するパターンのメリットとしては、通信会社のネットワーク移行計画（たとえば、3Gネットワークのシャットダウンなど）などをとくに留意する必要がなく、かつ、自動車メーカ側で通信料のコストを負担する必要もない。その一方で、数多いスマホの機種と、断片化された主要スマホOSに対応する必要があり、また同じ車種でも同じサービスを提供できるとは限らない。そのため、統一したUXをすべてのお客様に提供できない。

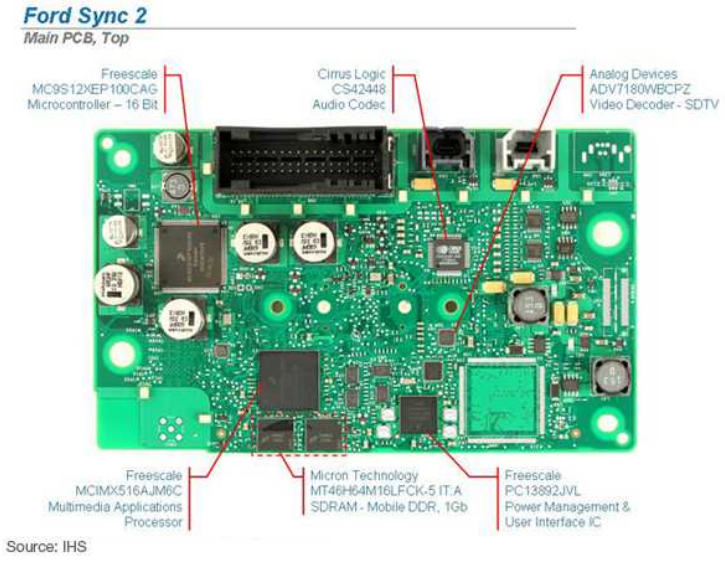
参考までに、Ford Syncの画面イメージ（図表7）と、プリント基板（PCB）（図表8）を示す。

【図表7】Ford Syncの車載画面のGUI

（出典）関連報道

2世代目のFord SyncのSync 用プリント基板（PCB）は、LTE通信機能は搭載しないが、Bluetooth/WLANのモジュールや、多数のコンポーネントを搭載する。

【図表8】Ford Syncの車載PCB事例



（出典）IHS社分析より

PCBの詳細は、以下の図表にて説明する。

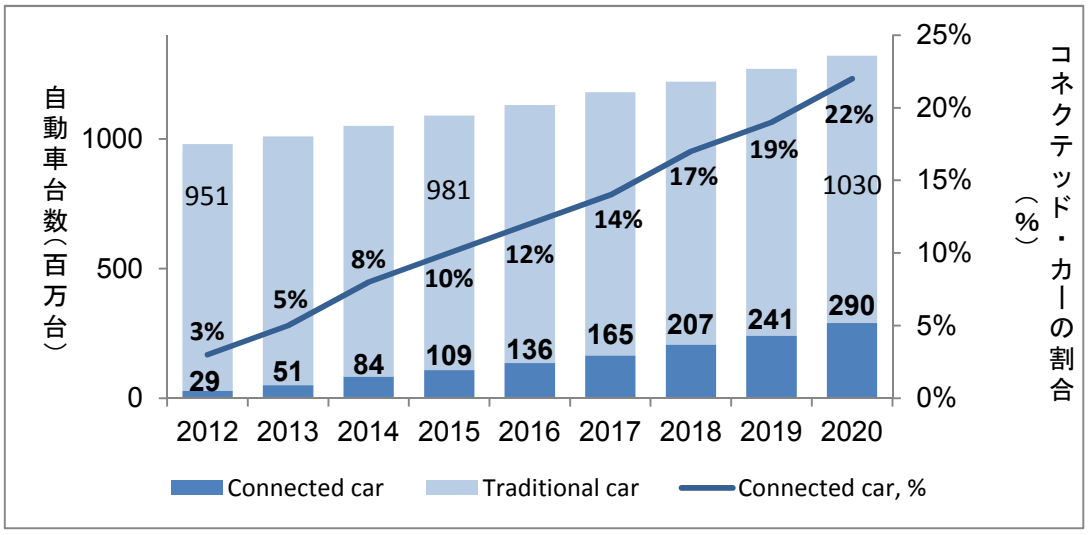
【図表9】Ford Syncの車載PCBコンポーネントの提供元やその他の主要パートナー

ベンダー	提供技術
Microsoft	Windows Automotive OS
Nuance	音声認識SW
Mitsumi	BT/WLANモジュール
Micron	SDRAM, Flash NAND
Continental	インテグレーション及び製造
Freescale	Applications processor
Analog Devices	Video decoder
Cirrus Logic	Audio decoder

（出典）執筆者調べ

コネクテッド・カーの今後の普及はどのように見込まれるのか。McKinsey社はCarPark社と共同で、今後の普及率とインストール・ベースを予測し、2020年までにコネクテッド・カーの普及台数は3億台弱へと成長すると見込む。

【図表10】全世界のコネクテッド・カーのインストール・ベースの推移と予測



（出典）McKinsey/CarPark社

3　コネクテッド・カーとセキュリティ

コネクテッド・カーのサービスそのものだけでなく、セキュリティへの注目も高まっている。さて、どのようなリスクが存在するのだろうか。「攻撃経路」「セキュリティ脅威」の2つの側面から整理してみたい。

攻撃経路として、図表11に示すように「フィジカル」「オーディオ」「通信」「クラウド」に分けて整理できる。

【図表11】コネクテッド・カーにおける攻撃経路

1	Physical （フィジカル）	車に直接、たとえばOBDIIポートを通じてフィジカルにアクセスし、何かの情報をとったりする
2	Audio （音声などオーディオ）	音声ファイルやMP3ファイルなどによるウィルス配信
3	Wireless （LTE、DSRCなど通信サービス）	無線通信を通じてアクセスしてハックすること
4	Infrastructure （クラウドなど）	コネクテッド・カーの利用するクラウド・インフラへアクセスし、車へたとえばマルウェアなどを配信するか、クラウドに蓄積した情報の漏洩など

（出典）執筆者作成

「フィジカル」の攻撃については、たとえば、米国国防省傘下の研究機関のDARPA（Defense Advanced Research Projects Agency）が「ハッキング実験」を開催してセキュリティに対しての注意喚起を行っている。セキュリティ専門家が実際の車両を使って、物理的な接続インタフェースから脆弱性を突く実験を行い、車両のCANbusへアクセス可能であったと発表している☞（脚注）（図表12）。

☞（脚注）

http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf

【図表12】米DARPAがスポンサーした自動車ハッキング事例

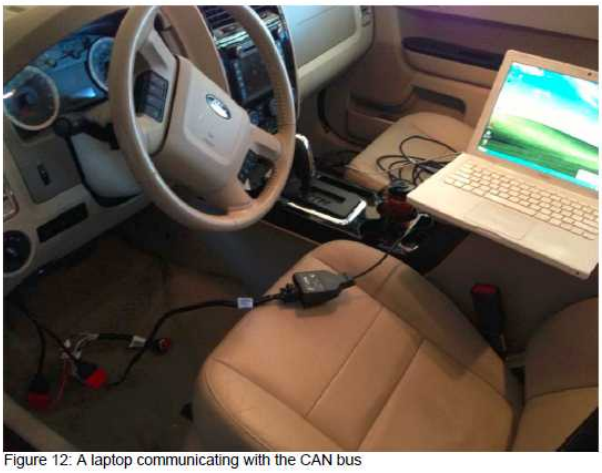


Figure 12: A laptop communicating with the CAN bus

（出典）研究者の研究成果より

また、MP3ファイルや、音声メッセージとして録音されたファイルによるリスクも存在するようだ。米San Diego大学の研究者が、米Washington 大学の研究家と共同で、自動車へアタックできるさまざまな手法を研究した事例の中で☞（脚注）、音楽ファイル（例：WMA、MP3など）を通じてCAN パケットを配信できることがわかった。これは、CD上のファイルとして、また、より恐ろしいことに、HDラジオ（FM放送）のデータ放送機能を使ってできるという。

無線機能については、コネクテッド・カーにはローカル（例：Bluetooth）の通信機能と、長距離の通信機能（例：LTE）の両方が搭載される。同じSan Diego大の研究者は、Bluetoothを通じてAndroidのマルウェア、移動通信機能を通じて TCC（Telematics Call Center）と自動車の間の認識コードを偽造し、アクセスできることがわかった。

また、クラウド・インフラのリスクも、ほかのクラウド・サービスと同様に存在する。たとえば、コネクテッド・カー・クラウドをサービスとして提供するベンダー（例：Ericssonなど）のインフラがハックされたら、どのような情報にアクセスできるのだろうか。以下の情報が、コネクテッド・カー・サービス提供上、ユーザが提供する 個人情報やサービス利用を通じて取得できる個人情報であろう。

☞（脚注） http://www.autosec.org/pubs/cars-usenixsec2011.pdf

【図表13】コネクテッド・カー・サービスにより蓄積できる個人情報事例

自動車関連	携帯電話 関連データ	サービス利用 関連データ	Vehicle Health Reportが 必要とするデータ
現在の位置	携帯電話番号	ユーザのリクエスト	VIN （Vehicle Identification Number）
移動方向		住所情報	走行距離
移動速度		ユーザが指定した ルート情報	自動車の動作状況関連情報
自動車の 診断データ		ユーザの検索履歴	
		スポーツ、ニュース、 などの嗜好	
		車内で録音された 音声情報	

（出典）Fordの資料などを基に執筆者調べ

コネクテッド・カー・サービス提供により蓄積されるこうした個人情報が漏洩された事例はあるのか。幸い、コネクテッド・カー領域においては、 TargetやHome Depotなど、米国のリテール分野にみられるような大型ハッキングはまだ報道されていないが、もしクラウド・インフラがハッキングされたら、大量のユーザの移動パターンを含む個人情報が漏えいすることとなる。2015年1月、BMW Connected Driveのシステムの脆弱性が指摘され、同社は、220万台の自動車に対して、ソフトウェア・パッチを提供することになった☞（脚注）。

次にセキュリティ脅威について紹介する。セキュリティ脅威には、設定ミスやウィルス感染といった利用者の操作に起因するものもあるが、悪意を持って行われる攻撃者によるセキュリティ脅威を示す。（図表14参照）

自動車の場合は、走行の安全が脅かされる可能性があり、利用者のパソコンやスマートフォンにおける脅威に比較して、侵害された時の影響が大きい。

☞（脚注）

http://www.pcworld.com/article/2878437/bmw-cars-found-vulnerable-in-connected-drive-hack.html

【図表14】コネクテッド・カーに攻撃者からのセキュリティ脅威

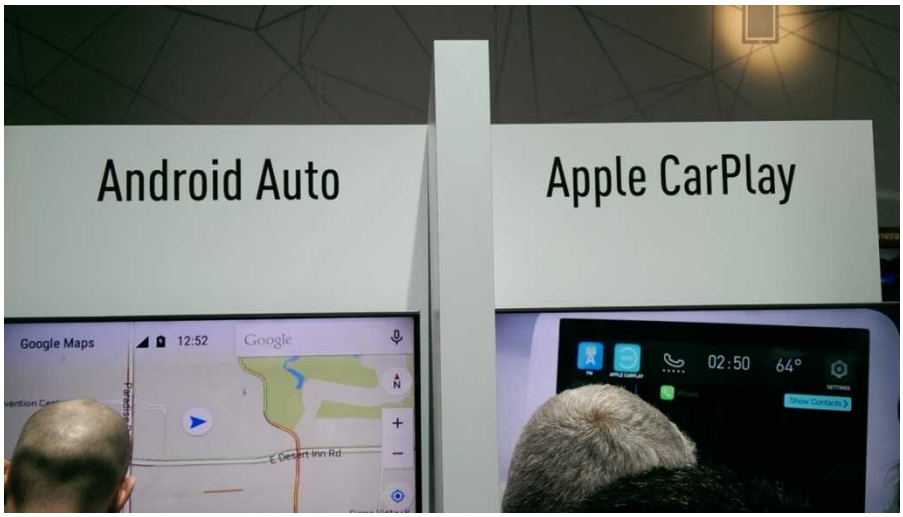
脅威	説明
不正利用	なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者に自動車システムの機能を利用される脅威。 ・解錠用の通信をなりすます事により、自動車の鍵を不正に解錠する、等
不正設定	なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者に自動車システムの設定値を不正に変更される脅威。 ・ネットワーク設定を変更し、正常な通信ができないようにする、等
情報漏えい	自動車システムにおいて保護すべき情報が、許可されていない者に入手される脅威。 ・蓄積されたコンテンツや、各種サービスのユーザ情報が、機器への侵入や通信の傍受によって不正に読み取られる、等
盗聴	自動車内の車載機同士の通信や、自動車と周辺システムとの通信が盗み見られたり奪取されたりする脅威。 ・ナビゲーションや渋滞予測を行うサービスのために自動車から周辺システムに送付される自動車状態情報（車速、位置情報等）が途中経路で盗聴される、等
DoS攻撃	不正もしくは過剰な接続要求によって、システムダウンやサービスの阻害をひきおこす脅威。 ・スマートキーに過剰な通信を実施し、利用者の要求（施錠・解錠）をできなくさせる、等
偽メッセージ	攻撃者がなりすましのメッセージを送信することにより、自動車システムに不正な動作や表示を行わせる脅威。 ・TPMS（タイヤ空気圧監視システム:Tire Pressure Monitoring System）のメッセージをねつ造し、実際には異常がない自動車の警告ランプをつける、等
ログ喪失	操作履歴等を消去または改ざんし、後から確認できなくする脅威。 ・攻撃者が自身の行った攻撃行動についてのログを改ざんし、証拠隠滅を図る、等
不正中継	通信経路を操作し、正規の通信を乗っ取ったり、不正な通信を混入させる脅威。 ・スマートキーの電波を不正に中継し、攻撃者が遠隔から自動車の鍵を解錠する、等

（出典）IPA（情報処理推進機構）
『自動車の情報セキュリティへの取り組みガイド』
9ページ表2-6 （2013年3月）

4　コネクテッド・カー・セキュリティのソリューション事例

コネクテッド・カー・サービスは、車両の遠隔保守といったクリティカルなユースケースと、単に情報を照会するといった非クリティカルなユースケースがあるが、これら性質の異なる利用目的に、同じ通信回線、同じCANbusを利用するのは、ある意味でスマホ普及におけるBYOD （個人のスマートフォンやタブレットを企業ネットワーク内に接続して使うこと）に類似するといっていいだろう。実際、ある米国キャリアのヒヤリングで、担当者はそのようにコメントした。また、AppleやGoogleのOSプレーヤーが自動車領域へも進出してきたことでなおさらそうであろう。

【図表15】 Apple CarPlay、Android Autoの展示事例（CES 2015にて）

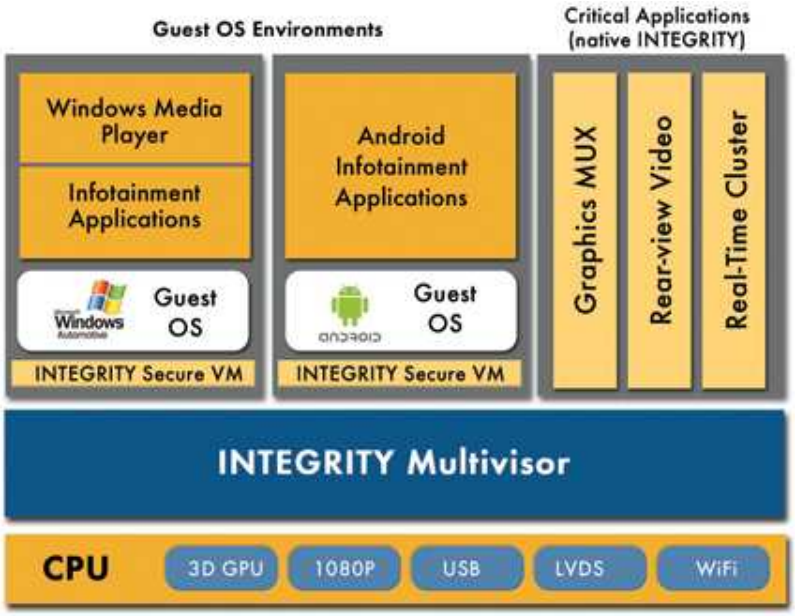


（出典）執筆者撮影

スマホの2大OSに慣れ親しんだドライバーは、自動車の中でも、IVIシステムの画面で同じアプリやサービスにアクセスしたいニーズはよく理解できる。さらにいえば、高機能なスマホの普及により、消費者が車載IVIシステムに要求する機能性やUXの期待値が高まったといえよう。一方、自社のUX、自社のサービスを推進したい自動車メーカにとっては、AppleやGoogleに車内が席巻されるのは 悩ましい光景であろう。

自動車＝新しいBYODのバトルグランドだとすると、スマホでみたBYODと同様なソリューションが通用するだろう。実際、自動車IVIシステムに対して、ハイパーバイザー（hypervisor）機能、つまり仮想化機能のあるOSを提供する会社がある。米Green Hills Software社はその事例のひとつである（図表16参照）。同社は、自動車のIVIシステムに対してIntegrity OSとして提供する。

【図表16】Green Hills Software社のIntegrity ハイパーバイザー概要



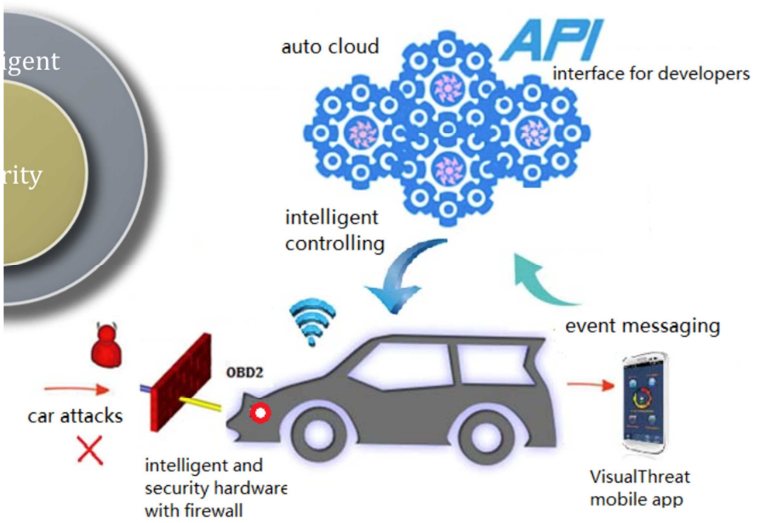
（出典）Green Hills Softwareウェブサイト

同社のハイパーバイザー機能の市場参入の影響を受けて、リーダーのQNX社も2015年2月、ハイパーバイザーを発表した☞（脚注）。

また、OBDIIポートについては、最近、OBDII firewallという製品を出したベンチャー企業がでてきた。2013年9月に設立されたVisual Threat 社である。以下は、同社のソリューション概要だ。ハードウェアの製品で、OBDIIのファイヤウォールとして機能する。加えて、クラウド・サービスも提供し、自動車向けアプリの認証（ホワイトリスト化など）も行えるという。現在、中国のカーシェリング・プロバイダーにより採用されているという（ヒヤリングでのコメント）。

☞（脚注） http://www.qnx.com/news/pr_6138_1.html

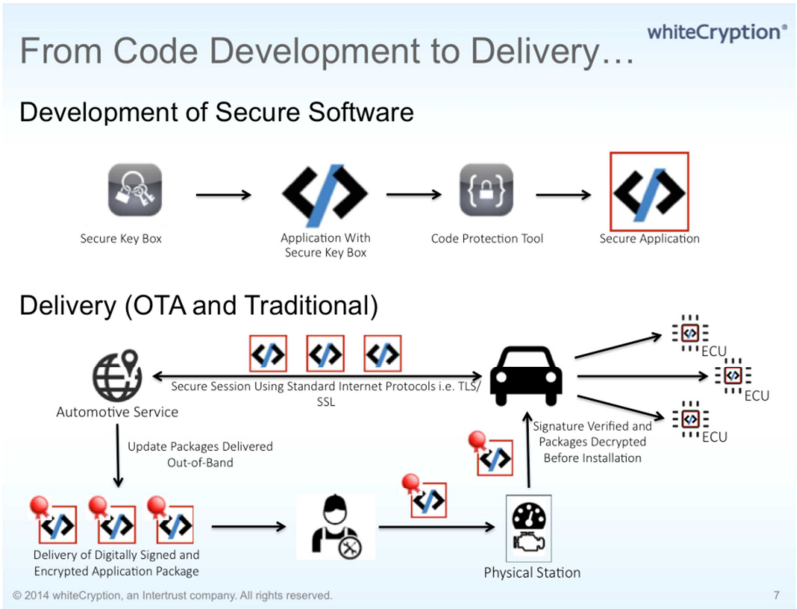
【図表17】 Visual Threatソリューション概要



出典：Visual Threat社資料

また、自動車向けアプリやソフトウェアを利用するために必要なキーの更新状況にフォーカスするベンチャー企業もある。セキュア・コンピューティングに特化するIntertrust社のスピンアウトでWhiteCryption 社である。たとえば、スマホ上のバンキングアプリの場合、アプリ利用のためのキーがメモリに保存される。それが再利用されれば、別のユーザでもアクセスできてしまう。同社は、暗号化キーを管理するKDC （key distribution center） により、自動車向けサービス（例：音楽配信など）と自動車のECUの間のキー管理を行い、必要なサービスに対して必要なアクセスのみを提供する。OTA（Over the Air）サービス配信と従来（技師が物理的にアクセスして）の配信の両方に対応するという（図表18参照）。

【図表18】 WhiteCryption社のソリューション概要



出典：WhiteCryption社資料

また、ファームウェアなどのOTAアップグレードのために、AT&T は自社のAT&T DriveにてRed Bend社を採用した。Red Bend社は、1999年設立のベンチャー企業で、2015年1月、オーディオ製品メーカのHarman社により買収された☞（脚注1）。（Harman社は、以前、QNX社のオーナーであったが、BlackBerryに売却した。） Harman社は合わせて自動車向けエンベデッドSWを開発するSymphony Teleca社の買収を発表した。

さて、通信キャリアあるいは通信インフラ・プロバイダーにとってどのような市場機会があるのか。とくにV2I（vehicle to infrastructure）またV2V（vehicle to vehicle）通信においてDSRCなど専用の短距離通信インフラの活用が期待されるが、WiFi APのようにローカルに設置・運用する必要がある。せっかくのキャリアのLTEインフラまたはクラウドを活用できれば、DSRCなど専用インフラの設備投資を省けるかもしれない。DSRCに対して、LTEは遅延が生じやすく、遅延をDSRCなみ（例：100ms間隔での情報更新と共有）のレベルへ抑えるには、クラウド機能をなるべくエッジへ移転する必要がある。また、自動車向け情報配信の手段として、LTEブロードキャストと呼ばれる、eMBMSの活用を検討する米国キャリアがある☞（脚注2）。

執筆者コメント

ここ数年、コネクテッド・カーのセキュリティ・リスクについての記事などをしばしば目にするが、幸い、リテール分野にみる大型ハッキング事例はみない。実際、フィジカルな攻撃経路のハッキングの場合、スケールしにくい。

一方、IVIシステムとクリティカル・システムが同じ通信モジュール、同じ動作環境を併用していくのであれば、Green Hills、QNXが提案するように仮想化を徹底する必要があるだろう。自動車もスマホのようにOSやファームウェアを必要に応じアップグレードするようになるのであれば、通信キャリアにとって、そのファイル検証あるいはホスティングを提供する機会があるかもしれない。また、交通状況の情報共有など、V2V、V2xの試みにみられるような、よりリアルタイムな通信については、遅延を最低限に低くすることや、LTE方式が機能としてもつ放送機能（eMBMS）を活用することで通信キャリアが市場機会とすることができるかもしれない。

☞（脚注1）

http://www.redbend.com/en/company/news-and-events/in-the-news/-harman-to-acquire-red-bend-software

☞（脚注2）

http://www.fiercewireless.com/tech/story/unlike-verizon-att-takes-its-lte-broadcast-trial-inside-stadium/2015-01-09

【執筆者プロフィール】

氏　　名： Jon Metzler

経　　歴：Blue Field Strategies 創業社・社長。米シカゴ生まれ、現在サンフランシスコ在住。90年代初頭、5年間の滞日時、朝日新聞出版局、TBS、CBSなどを経て、98年本国へ帰国。帰国後、UC-Berkeleyにて日本とシリコンバレーを比較研究し、ビジネスと東洋学の修士号を取得。Blue Fieldでは、とくに通信、メディア、ハイテックの領域にて日米、US-アジアのクロースボーダー市場分析・市場参入・戦略投資などにおいて多岐にわたる顧客企業を支援する。Blue Fieldの傍、UC-BerkeleyのHaas School of Businessの MBAプログラムにて講師を務め、またJapan Society of Northern Californiaのボードメンバーを務める。