
Symantec
包括的なセキュリティ機能を
車に実装する

いまや車に対する脅威は、可能性を論じる段階を超えて悲惨な事故が現実となりうる段階へと至りました。

シマンテックは、ハッカーが車に侵入することを防止して車と乗員の安全を守るために、自動車メーカーやチップメーカーのほか先進的な企業とともに取り組みを進めています。

続きを読む >>


# 要約

自動車のセキュリティに対する脅威は、この数年間で理論から現実へと変貌を遂げました。欧州や北米では、技術に詳しい犯罪者が車の窃盗を繰り返しています。インターネットに投稿された動画では、ハッカーがリモート操作で車のブレーキをかけ、運転者や乗員を危険な目に遭わせています。ハッカーは、隣の車線を走る車に対して何の予告もなしに、このような脆弱性を悪用できます。他の脆弱性を悪用すれば、地球の反対側から携帯回線を介して同時に多数の車を攻撃することも可能です。

このようなセキュリティ問題の多くについては、解決できるテクノロジが存在しています。しかし、車に対してそれらを導入することは、従来の IT システムの場合よりもはるかに困難です。IT システムで問題が発生した場合は、インストール、アップデート、設定変更を迅速に行うことで解決できます。最悪の状況になっても、バックアップを復元したり、ディザスタリカバリサイトへのフェールオーバーを実行したり、セキュリティ対応チームを招集して高度な脅威に対処したりすることが可能です。

しかし、車の場合には状況が異なります。FMVSS（米国連邦政府自動車安全基準）の認定を取得するプロセスには何年もかかります。そのうえ、企業の IT 部門では当然となっている、毎週、毎日、リアルタイムのセキュリティアップデートは含まれていません。数百万世帯のガレージに置いてある車を調査するためにセキュリティ対応チームを招集することなど不可能です。車で故障が発生しても、別の車にフェールオーバーするわけにはいきません。IT システムでは、重要なレイヤーに冗長性を組み込むことで大量のデータを扱う Web サービスの信頼性を確保します。すべての車でそのような取り組みを行うには、NASA のような天文学的な費用が必要です。しかし、それが可能な自動車メーカーはあったとしてもごく少数です。

車を脅威から保護するためには、車の中だけでなく、より広範に自動車メーカー全体までを対象とする必要があります。責任の範囲は、工場の組立ラインにとどまりません。自動車メーカーとサプライヤとの間で複雑につながった関係の隅々にまで及びます。セキュリティは、このバリューチェーンにおけるすべての段階で考慮する必要があります。攻撃者はその中で最も脆弱な場所を狙うからです。

**拡張性の高い方法でセキュリティを組み込むには、次のようなセキュリティの基本原則を、協力しながら徹底的に適用する必要があります。**

1. すべての通信を保護する
2. 個々のセンサー、アクチュエータ、マイクロコントローラ（MCU）、マイクロプロセッサを保護する
3. 車全体の管理を OTA（無線通信）で安全かつ効果的に行う
4. 高度な脅威を軽減する

このホワイトペーパーでは、自動車に包括的なセキュリティ対策を実現していくうえで今後考えられる道筋とステップを示します。まず、個別に対処可能なコンポーネントやインターフェースを取り上げます。続いて、CAN バス（コントローラエリアネットワークバス）や FlexRay といった、テクノロジにかかわる根本的な問題について長期的視点からの対応を検討します。こうしたテクノロジは、複雑なサプライチェーンを統合するバックボーンとして長年にわたり使用されているものです。

**さらに、最も重要なトピックとして、次の状況を考慮したうえでセキュリティ対策を段階的に実現していく適切なタイムラインについて議論するための「たたき台」を提示します。**

1. 運転者と乗員の安全は最優先です。
2. 自動車業界が新しいテクノロジを安全に導入するにあたっては、認証のため長い期間が必要になります。
3. 状況は切迫しています。問題を放置したままでも、テクノロジが未熟なうちに導入しても、人命にかかわるおそれがあります。
4. 財務的な状況は厳しいものです。新しいテクノロジによって、顧客を増やすかマージンを高める必要があります。企業が倒産してしまったら安全な車など作れません。

この大規模で複雑な問題に対処するには、自動車業界の企業と、IT や OT（オペレーションテクノロジ）のセキュリティに携わる企業の双方がノウハウと努力を結集する必要があります。隅々まで安全が行き渡った車を設計するには時間がかかります。そのため、双方の業界が、自動車のバリューチェーンにおけるすべての段階で、このようなセキュリティの問題への対処を始めることが必要です。影響はきわめて大きいので、遅れは許されません。

# 自動車への脅威

欧州や北米では、車の窃盗が多発しています。インターネットに投稿された動画では、ハッカーがリモート操作で車のブレーキをかけ、運転者や他の乗員を危険な目に遭わせています。ハッカーは、隣の車線を走る車に対して何の予告もなしに、このような脆弱性を悪用できます。また、地球の反対側から携帯回線を介して多数の車を同時に攻撃できてしまう脆弱性もあります。まず、今日存在している脅威を取り上げます。次に、このような脅威から車を保護するための先進的なテクノロジをみていきます。

従来の動画では、ハッカーが車の中から OBD-II（自己故障診断）ポートに接続して、ブレーキをかけたりエンジンを停止させたりしていました。

しかし最近では、こうした攻撃をリモート操作で行う事例が相次いでおり、メーカーは巨額を投じてリコールを行っています。

車を狙う攻撃はこれだけではありません。すでに多数の被害が発生しています。欧州や北米では、キーレスエントリシステムの脆弱性を悪用する窃盗犯が活動しています。キーレスエントリシステムは、ユーザーに利便性を提供するものです。キーをポケットや財布やかばんに入れたままでも、車の乗り降りやドアのロックのほかエンジンの起動や停止も可能です。

多くの脆弱なキーレスエントリシステムでは、キーが車の近くにあることを検出する仕組みを採用しています。キーの場所や距離を検出する手段として比較的安全性の高い方法は、GPS（全地球測位システム）、携帯回線、Wi-Fi、加速度計の測定値などを適切に組み合わせたものです。これらすべてに対して車とキーがともに適切なデジタル署名を行うことで、両者が近くにあると判断します。しかし、この仕組みを利用しているシステムはごく少数です。他の多くのシステムでは、より単純に車載センサーの信号強度のトライアングレーション情報で判断しています。このようなシステムは当然、窃盗犯が電子装置を利用する攻撃に対して脆弱です。窃盗犯は、財布にしのばせた偽のキーに車の信号をリレーしてから偽のキーの信号を車にリレーして、手元の偽のキーが本物であるように見せかけることができます。これまでに、Audi や BMW といったメーカーの車がこのような攻撃を受けています。ほかにもこの被害に遭ったメーカーは多数あるとみられます。

自動車メーカーがそのような被害を回避して、事後処理のコストやブランドへのダメージを防止するためには、場所のデジタルキャプチャ、キャプチャ時のデータ署名、セキュアブート、コードサイニングなどを組み合わせて、ファームウェアの改ざんを防ぐことが必要です。また、さまざまな OTA アップデートメカニズムを車に搭載しておけば、出荷時のキーには最新の高価なセンサーが搭載されていなかった場合などでも、こうした問題を迅速に解決する手段を増やすことができます。その手段としては、ユーザーのスマートフォンを使用する方法もあります。たとえば、TIMA（TrustZone™ Integrity Monitoring Architecture）のような技術が搭載された Android デバイスをキーの代わりに利用するものです。このようなモバイルデバイスにはすでに、前述のようなセンサーがすべて搭載されています。

しかし現状では、多くの自動車メーカーが製造販売する車に組み込まれているのは、基本的な OTA アップデート機能や構成管理機能にとどまります。このような OTA 機能で最も問題となるのは、ハッカーがリモートで車を操作できるような危険な脆弱性が発見されても、直接に修正できないことです。これを防ぐには、セキュリティの基本原則を単体の車だけに適用するのではなく、サプライチェーンの各段階に適用する必要があります。

ただし、車への攻撃経路はこれだけではありません。他の経路としては、ユーザーのモバイルデバイスへの Bluetooth 接続、他のデバイスへの Bluetooth 接続、Bluetooth 機器への直接攻撃、IVI システムの脆弱性などが考えられます。特に IVI システムは、エンターテインメントとナビゲーションの両方のデータを配信しているため、非常に多くの企業にかかわる詳細情報が含まれています。悪質なファイルを仕込んだ DVD や CD を数百万枚コピーしてプレイヤーの脆弱性を悪用することは、簡単ではありません。しかし、無線インターフェースを経由したエンターテインメントの配信が開始すると、多数の脅威にさらされる機会が増えます。前述の OBD-II への脅威があるところに、IVI へのこうした脅威がさらに加わるのです。

現在の CAN バスや FlexRay バス用のプロトコルでは、特に走行中において機器の相互認証を適切に行う手段は多くはありません。エコシステムの非常に多くの部分に影響する最も重要な変化でさえ、実現するには長い時間がかかります。一刻も早く、多くの具体的な取り組みを始める必要があるのです。

## ソリューションの概要

このような脅威から車を守るには、セキュリティの基本原則をシステムの各レベルで厳格に適用することを協力して進める必要があります。

### 4 つの土台


長期的で包括的なセキュリティを実現するには、それぞれの段階で車にセキュリティを組み込むことが求められます。今日の車には、車が接続するクラウドベースのデータセンターシステムからモジュールそのものに至るまで、多くのレイヤーがあります。そこには、SBC（シングルボードコンピュータ）、BCM（ボディコントロールモジュール）、小型のセンサーモジュール、モジュールを動作させるチップ、モジュールを接続するバスプロトコルなどが存在します。サプライヤの関係が複雑に広がっていることを考えると、このようなレイヤー全体を上層から下層まで包括的なセキュリティ対策で保護するには、長い年月がかかります。今後は、OTA 経由の攻撃によるなりすましや改ざんを防ぐために、すべての重要なチップがハードウェアによるセキュアブートとクレデンシャルストレージをサポートすることが必要となるでしょう。

重要なチップには、駆動系、油圧計、その他車の安全に関連するあらゆるコンポーネントに影響する BCM やすべての MCU が含まれます。最終的には、すべての重要なモジュールが、暗号化機能や鍵管理機能を利用して他のモジュールとやり取りするデータを認証し、攻撃者がなりすましによって信号を制御できないようにする必要があります。このような変更のいくつかを実現するには長い時間がかかると考えられます。CAN バスや FlexRay バスの現在のプロトコルには、適切な認証手段が多数備わっているとはいえないからです。したがって、危険につながる異常を検出して対処可能とするためには、車のバス、すべての無線モジュール、携帯電話

網、Wi-Fi、Bluetooth にモニタリング機能をできるだけ早く装備することが喫緊の課題です。最終的には、システム全体が OTA 経由によるアップデート機能を備える必要があります。また、すべてのデータセンターおよびクラウドベースのシステムを高水準で保護して、これらのシステムに依存する人命の安全を確保する必要があります。

自動車業界を短期的な視点でみると、大きな効果を発揮するセキュリティ対策を実施する余地が数多くあります。これらの対策は包括的ではないものの、多くの脅威を低減するうえで大きな役割を果たすことになります。第一歩は、車にセキュリティを実装するための足掛かりを築くことです。多くの場合は、車のヘッドユニット（通常は SBC）を保護することから着手します。場合によっては IVI 機能も対象となります。次に、この足掛かりを土台として、車の他の部分を管理したりアップデートしたりします。同時に、他のセキュリティテクノロジを導入することで、CAN バスのモニタリングやネットワーク接続の試行など最も危険性の高い部分に対処できます。

**シマンテックでは、このようなニーズに対応するため次の製品を提供しています。**

1. Symantec Embedded Security: Critical System Protection は、ほとんどの車のヘッドユニットや IVI システムを保護します。Symantec™ Embedded Security: Critical System Protection は QNX ™ Neutrino RTOS をサポートしています。ご要望に応じて、特定の組み込み Linux ®（Android に組み込まれた Linux など）のサポートも簡単に可能です。™
2. Symantec Embedded Security: Critical System Protection は、ディーラー診断機や UBI ドングルなどの OBD-II インターフェース装置を保護します。
3. Embeddable Security Certificates for Device Authentication は、データ認証をサポートします。数十年前の 8 ビットデバイスなど厳しいリソース制約があるデバイスのデータも認証できるほか、接続の認証に加えてメッセージ認証とフレーム認証の両方が可能です。
4. Symantec Code Signing Certificates は、セキュアブート用のコードサイニングなど広範なコードサイニングをサポートします。また、Symantec Secure Application Service は、リアルタイムオペレーティングシステム（RTOS）でよく使用される Java や標準の ETF（Executable and Linkable File）フォーマットでのコードサイニングをサポートします。

**シマンテックではさらに、大手自動車メーカーや大手サプライヤと協力して、次のテクノロジが一般に広く利用可能となるように継続的な取り組みを進めています。**

5. Embedded Automotive Security Analytics は、CAN バスや FlexRay バスを監視します。このソフトウェアは、多くの車の IVI やヘッドユニットに使用される SBC などのシングルボードコンピュータ、および UBI ドングルなどの OBD-II ドングルに使用される 32 ビット MCU のほとんどに対して簡単に組み込むことができます。

6. Code Signing for Automotive Secure Boot を支えるのは、シマンテックが運営する先進的な認証局（CA）やコードサイニングのインフラです。シマンテックでは、関心を持つチップメーカーや半導体パートナーと提携し、自動車メーカー向けのコードサイニングとセキュアブートの開発に取り組んでいます。

7. Embedded Software Protection は、同じくシマンテックのコードサイニングおよび CA サービスに支えられたテクノロジですが、コードサイニングにとどまらない機能を持っています。不明瞭化やその他の方式の保護機能をコードに埋め込んでからサイニングを行うため、数十年前の 8 ビットデバイスや 16 ビットデバイスなどリソース制約がある MCU でも自動車メーカーのコードを保護できます。

8. Global IoT Security Analytics は、数百万台の車から収集されたデータの相関分析に基づいて高度な脅威を検出可能とします。すべてのモジュールや通信の保護そして車全体の管理を適切に実行したとしても、高度な脅威を検出するためにはさらにモニタリングと分析のフレームワークが不可欠です。

隅々にまで安全が行き渡るように設計された車の開発という長期ビジョンを実現するうえで、これらの機能が第一歩となるのです。


# 自動車のセキュリティに特有の課題

前述のとおり、自動車システムに対応したセキュリティ対策を構築するうえでの課題は、従来の IT に対応したセキュリティ対策とは大きく異なります。広告主導型の Web サイトは、1 時間ごと、または必要に応じてさらに短い間隔で更新がありえます。人命を預かる車の場合は、新しいテクノロジを導入するのに何年もかかることがあります。自動車システムに変更を加える場合には、常に慎重に行う必要があります。また、変更を行うと多くの場合、最も大規模で階層化されたサプライチェーンに属する多くのサプライヤに影響を与えることになります。企業における IT セキュリティには 20 年近い歴史がありますが、そのテクノロジのほとんどは車には適用できません。

自動車は 100 年以上にわたり、私たちの生活を変えてきました。それでも、「コネクテッドカー」への移行はごく最近のことです。インターネットへの接続により、ユーザーの生活を向上させるすばらしい新機能が提供されています。しかし、この接続は同時に、攻撃の経路としても利用できてしまいます。すでに強固に確立されている車のアーキテクチャにセキュリティを追加するのは非常に困難なことです。シマンテックではこれに対応するため、車を完全に保護するための長期的な取り組みのほか、より短期的な取り組みも進めています。自動車メーカー、ディーラー、そしてユーザーに少しでも早く成果を届けたいからです。

シマンテックは、すでにさまざまな分野で 10 億台を超える IoT（モノのインターネット）デバイスにセキュリティを組み込んできた実績があります。そこには、パートナーと協力して複数タイプのデバイスの生産ラインでキーインジェクションに取り組んでいる事例も含まれます。シマンテックは、高度な組み込みシステムの実績をすでに蓄積しているのです。シマンテックはこれまで、スマートメーター、ケーブルモデム、携帯基地局、8 ビット、16 ビット、32 ビットのデバイスにセキュリティを組み込んできました。

ただし、自動車業界に対する取り組みは比較的新しい分野です。そこで、シマンテックでは、パートナーとの長期的な関係構築に努めながら、すべてのパートナーに対してより短期的で測定可能な成果を提供するための取り組みも続けています。シマンテックは、自動車サプライヤの間では大規模で複雑な「システムのシステム」が統合されていること、およびすでに確立されている階層化されたサプライチェーンが自動車メーカー各社にメリットをもたらしていることを十分に理解しています。すべてのレベルでセキュリティの確保が求められるいま、シマンテックはパートナーを積極的に募集しています。求めているパートナーとは、サプライチェーンの中で高機能のコアテクノロジを開発できるほどセキュリティ分野での能力を高め、高度なセキュリティで平均販売価格（APS）を上昇させたいと考える企業です。


# 重要なモジュールの保護

ヘッドユニット、IVI、OBD-II ポート、GSM モジュール、BCM はすべて、車と乗員の安全とセキュリティを確保するうえで重要な役割を果たしています。これらのモジュールは、乗車体験の質を高めるとともに車を管理するための強力な資産です。しかし、このような資産に対して適切なセキュリティ対策が施されていなければ、悪用されてメーカーや運転者に損害を与えるおそれがあります。幸いにも、これらのモジュールの多くは通常、予測通りの機能を実行するものです。つまり、これらのモジュールは常に既知の状態にあり、既知の動作を行う「正常な」コードを持っています。これによりシステムの大部分を強力なセキュリティ機能で保護できるので、ハッカーがシステムを悪用してメーカーやユーザーに被害を与えることはできません。

Symantec™ Embedded Security: Critical System Protection を利用すると、こうしたモジュールの多くで「正常な」コードのホワイトリストを強制的に適用するように設定できます。これによって、事前に承認済みのコードのみが実行されるようにしたり、コードで許可される動作を管理したりすることが可能です。Symantec™ Embedded Security: Critical System Protection は、毎日無数の金融取引を保護しているという実績を備えたテクノロジに基づいた製品です。このテクノロジは、金融サービスを手がける世界最大級のプロバイダの主要なバックエンドシステムに配備されています。また、ユーザーインターフェースとして機能する無数の ATM にも組み込まれています。これは、IVI が運転者との重要なインターフェースとして機能しているのとよく似ています。シマンテックは、金融業界に提供しているこのような基本的な保護機能を応用して、自動車システムに利用できるようにしました。

もちろん、Symantec Embedded Security: Critical System Protection で実行できる機能は、正常なコードのホワイトリスト化だけではありません。サンドボックス内でコードを実行する機能により、コードの動作を厳しく管理できます。そのため、カーネルレベルに至るまで緊密に統合されている RTOS よりも、強力できめ細かく、柔軟で迅速なセキュリティ設定が可能です。Symantec Embedded Security: Critical System Protection では、既知のコードにのみ既知の機能の実行を許可する最小権限の保護戦略の一環として、ホワイトリストとサンドボックスを使用しています。Symantec Embedded Security: Critical System Protection は、アプリケーションの動作を直接監視するだけでなく、ファイル、設定、イベント、ログを監視して異常な動作をレポートします。また、高度なポリシーベースの監査と監視、検索やアーカイブや取得が容易な統合ログ、高度なイベント分析、レスポンス機能などを備えています。メーカーが製造する車の重要なモジュールを強力に保護するセキュリティ製品なのです。


Symantec Embedded Security: Critical System Protection を利用すれば、ほとんどのヘッドユニット、IVI、OBD-II ドングル、OBD-II ディーラー診断機、32 ビット BCM を保護できます。Symantec Embedded Security: Critical System Protection は、QNX ™ Neutrino RTOS 環境でも保護を強化できるとともに、ご要望に応じて特定のバージョンの Linux（組み込み Linux）や他の組み込み OS で実行できるようにカスタマイズも可能です。Symantec Embedded Security: Critical System Protection をコネクテッドカーに利用すると、疑わしい異常な動作や検出された脅威がリアルタイムでメーカーにレポートされます。それ以外の車では、セキュリティの遠隔測定結果を保存しておき、定期点検の際にディーラーがその結果を取り込むことができます。

当然ながら、重要なモジュールを保護するには、Symantec Embedded Security: Critical System Protection による動作中の保護に加えて、最終的にはコードサイニングとセキュアブートが必要になります。Symantec Code Signing Certificates は多様なフォーマットをサポートしています。ただし、コードサイニング用の Symantec Secure Application Service がサポートしているフォーマットは少数です。RTOS でよく使用される Java と標準の ELF フォーマット、および Windows の組み込みバージョンに固有のフォーマットなどです。もちろん、ここには先進的な CA インフラが利用されるほか、オンプレミスのコードサイニング証明書とクラウドベースのサービスが含まれます。これらによって、サプライヤがメーカーのチップ上でコードサイニングを実行する機能を管理できるようにします。シマンテックはより長期的な観点からも、関心を持つチップメーカーや半導体パートナーと協力した取り組みをすでに進めています。サポートするフォーマットの種類を拡大して、すべての MCU 上で自動車メーカーが簡単にコードサイニングとセキュアブートを実行できることを目指すものです。

また、さらに重要なこととして、8 ビットや 16 ビットのデバイスなどリソース制約があり OS を持たないデバイスを保護するために、コードサイニングを超える機能を実行する Embedded Software Protection の開発に取り組んでいます。この新しい製品は、不明瞭化やその他の方式の保護機能をコードに埋め込んでからサイニングを行います。そのため、数十年前の 8 ビットや 16 ビットのデバイスなどリソースに制約がある MCU でも、実行時の攻撃やリバースエンジニアリングから自身を保護できるようになります。

# 高度な脅威の軽減

最も重要なモジュールをどれほど適切に保護したとしても、数年後には新しい脆弱性が出てくるでしょう。豊富なリソースを備えた忍耐強い攻撃者が、いずれはこの脆弱性を悪用する方法を発見するはずです。そのため自動車メーカーは、このようなリスクを軽減する能力を備える必要があります。

セキュリティ分析では、車のFlexRayバスやCANバスで発生するすべての動作を裏で監視し、バス上のすべてのモジュールについて通常の動作モデルを「学習」できます。そして、コンポーネントが通常の動作から逸脱して危険性のある異常な動作をしている場合には通知を行います。このような分析テクノロジは、ほとんどの車に搭載されている数多くの SBC（IVI やより強力な一部の BCM）や、より小型なアフターマーケット製品の OBD-II ドングルで利用できます。コネクテッドカーでは、このような異常な動作状況をすぐにメーカーに送信して他の車のデータと相関分析を行うことで、さらにビッグデータ分析の威力を利用できます。それ以外の車では、蓄積された状況データを定期点検の際に車から取得してメーカーに送信できます。どちらの場合でも大きな技術的課題となるのは、セキュリティの観点から通常の動作のコンパクトモデルを学習し、既存の SBC と小型のドングルという制約のある環境にモデルを適合させながら、攻撃と疑われる動作を検出可能にすることです。当然ながら、フェールセーフ動作の設定はメーカーによって異なります。ただし、シマンテックがパートナーと共同で解決に取り組んでいるのは、車で発生している危険な可能性のある異常な動作を検出するという問題なのです。そこで、シマンテックでは、共同でソリューションの開発に取り組んでいただけるパートナーをさらに募集いたします。

Symantec Embedded Automotive Security Analytics に採用されているコアテクノロジでは、他の IoT システムにおいて最も高度な APT（Advanced Persistent Threat）を検出した実績があります。シマンテックではこのテクノロジを CAN バスと FlexRay バスのプロトコルに適合させて、現在の車に搭載されている SBC や、パートナーが販売している OBD-II ドングルで利用できるようにしています。

Global IoT Security Analytics は対照的に、数百万台の車から収集したデータの相関分析を行うことにより高度な脅威を検出できるようにします。データに起因するほとんどの問題と同じように、ビッグデータ分析テクノロジでは、さまざまなデータを利用してパフォーマンス（この場合は、高度な脅威を検出するパフォーマンス）を大幅に向上させることができます。シマンテックでは、セキュリティ分析用ビッグデータテクノロジの利用を 7 年ほど前から水面下で始めていました。シマンテックでは、車で発生している危険な可能性のある異常な動作を検出するために、自動車以外の業界で高度な APT を多数検出した実績があるテクノロジを応用しています。

# まとめ

コネクテッドカーは、自動車メーカーにもユーザーにもすばらしいメリットを提供します。しかし同時に、新たなリスクももたらします。車の窃盗事件や不安を抱かせる動画などは氷山の一角に過ぎず、今後はさらに深刻な事態が発生する可能性も考えられます。隅々まで安全が行き渡った車を製造するには、長い年月がかかります。シマンテックは、強い決意をもってこの取り組みを支援していきます。自動車メーカーもユーザーも、「最終的な」成功まで待つことはできません。

シマンテックでは、最大級の脅威に対処する初めのステップとして、実績のあるテクノロジを車に応用した新製品を投入して、今日の車に搭載されている最も重要なモジュールの多くを保護しています。Symantec Embedded Security: Critical System Protection は、市場で発売されるほとんどの車に搭載される、ヘッドユニット、IVI、32 ビット BCM に簡単に組み込むことができます。ディーラーの OBD-II 機器にこのテクノロジを利用することで、保守点検で車に接続するディーラー診断機を経由して車に攻撃や感染を仕掛けられることを防止できます。

シマンテックでは次のステップとして、Embedded Automotive Security Analytics と呼ばれるテクノロジを開発し、車のバス全体を保護しようとしています。これには、まだ設計段階の車の IVI やヘッドユニットといった SBC も、すでに道路を走っている車の OBD-II ポートも含まれます。当然ながら、シマンテックが IoT 向けに提供している他の多くのセキュリティテクノロジ（デバイス証明書、コードサイニング、OTA 管理、ルート証明書など）もすべて、自動車のセキュリティに役立ちます。実際、これらを組み合わせることで、コネクテッドカーに適した最も包括的な IoT セキュリティのポートフォリオが実現するのです。これは、強く求められている長期的な変化の基礎を築くのに役立ちます。Symantec Embedded Security: Critical System Protection と Embedded Automotive Security Analytics は、自動車業界のセキュリティにおいて、現在そして将来にわたる大きな進歩を示しているのです。

さらに、シマンテックでは、世界で最も包括的なセキュリティテクノロジを利用しています。具体的には、すでに10億台を超えるIoTデバイスにセキュリティ証明書を組み込んでいる、世界でも先進的な CA インフラです。そして、自動車に適した数種類の初期段階のファイルフォーマットに対応して複雑なサプライチェーンの関係をすでにサポートしている、コードサイニングの製品とサービスです。シマンテックは、これらのテクノロジを利用して、実行時のセキュリティを確保する Embedded Software Protection を提供しようとしています。これは、厳しいリソース制約がある MCU でも利用でき、さまざまな自動車用 MCU でセキュアブートに必要な多数のフォーマットをサポートします。シマンテックでは、このような新しいテクノロジを提供すると同時に、長期的な観点からもパートナーとの連携を進めています。

シマンテックはすでに、10 億台を超える IoT デバイスを保護し、他の垂直市場に向けた IoT システムで高度な脅威を多数検出しています。そして現在、世界でも先進のセキュリティテクノロジのポートフォリオを自動車業界のニーズに適合させようと取り組んでいるのです。

セキュリティを車に組み込むことに関心をお持ちでしたら、iot_security@symantec.com までお問い合わせください。

# 略語一覧

**BCM:** ボディコントロールモジュール
**CAN バス:** コントローラエリアネットワークバス
**FMVSS:** 連邦自動車安全基準
**GPS:** 全地球測位システム
**IVI:** 車載インフォテインメント
**MCU:** マイクロコントローラユニット
**OBD-II:** 自己故障診断
**OTA:** 無線通信
**SBC:** シングルボードコンピュータ
**TIMA:** TrustZone™ Integrity Monitoring Architecture
**UBI:** 利用ベース自動車保険

Symantec

http://www.symantec.com/ja/jp/iot/