



コネクテッドカーのための HARMAN SHIELD

コネクティビティは変革をもたらしますが、リスクと無縁ではありません。コネクテッドカーの売上は伸び続け、2020年までには推定3億8,000万台に達する見込みです。ますます複雑さを増すコネクテッドカーエコシステムを保護することは、場合によっては困難な作業です。異なるコネクテッドデバイスを横断するデータの急増によって脆弱性がかつてないほど高まっているなら、なおさらです。HARMAN SHIELDは最も包括的な侵入検知・防止ソリューション (IDPS) として、コネクテッドおよび自動運転車両へのサイバー攻撃の検知、管理、緩和、対応を行い、車両を常に安全に保護します。

コネクテッドカーのためのHARMAN SHIELDは、可能性のある有害な活動を完全に可視化し、車内におけるサイバー攻撃の脅威を検知します。こうした脅威を評価・調査する手段が搭載され、リアルタイムで脅威の報告、対応、緩和を行う機能を備えます。ソリューションは主要な構成単位から成り、モジュール式の拡張性のあるアーキテクチャを提供します

車載エージェント:

All HARMAN SHIELDエージェントは、受賞歴のあるHARMANのIDSテクノロジーを採用し、完全なバックエンド報告機能とOTAアップデート機能を搭載します。

- HARMANテレマティクスSHIELD: TCUシステムのための総合スイートで、最高のセキュリティ技術を活かして攻撃対象領域を最小化します。3G/LTEおよびV2Xなど、外部通信プロトコルの代表的な脆弱性を保護する、本格的な侵入検知システムが含まれます。
- HARMAN車載インフォテインメントSHIELD: セキュリティのベストプラクティスを提供し、BluetoothやWi-Fiなど、一般的なコネクティビティインターフェースの潜在的な弱点に対処することで、HARMANの主要なヘッドユニット、車載インフォテインメント (IVI) システム、デジタルコックピットソリューションをサポートします。
- HARMANゲートウェイSHIELD: 車内ネットワーク向けの侵入検知・防止ソリューション (IDPS) として、ハッキングと通信途絶に対する保護を提供するとともに、ECUまたはスマートゲートウェイへの容易な組み込みが可能。機械学習 (ML) アルゴリズムによってオフラインで学習された車両の通常挙動に基づいて、システムは異常を検出します。この機械学習された基準はリアルタイムで実際の車両挙動と比較されます。

主要なメリット

コネクテッドカーのためのHARMAN SHIELDは、次の手段を通じて常に自動車を守ります。

- 車両からセキュリティ関連データを収集
- 異常およびルールに基づくイベントを検知
- フリート全体で車両ごとにセキュリティ関連のステータスを発見
- 要約データを利用してセキュリティ上の脅威、リスク、傾向、影響を管理
- 科学捜査の手法、攻撃の再生、事後分析を用いて調査
- リアルタイムで脅威を緩和し、将来の対応策 (OTAソフトウェアアップデート、インシデントレポートなど) について推奨することで対応

Why HARMAN?

Shortening Time-to-Market

ハーmanınターンのキー・デリバリーや豊富な人的リソースを活用し、製品のコンセプト段階から市場投入までの期間を大幅に短縮する事が可能です。

Cross-platform

様々な業界における弊社の実績と他社に先行したプラットフォームを利用することで、新しい市場へのアプローチを迅速に行って頂くことが可能です。

Global delivery footprint

ハーmanın熟練した優秀なエンジニアたちが各センターから世界中の企業にソリューションをお届けします。

Solution accelerators

ハーmanınソリューション・アクセラレーターと世界じゅうに広がるパートナーシップを利用して、最先端の革新とベストプラクティスを手に入れてください。

www.harman.com

©2018 HARMAN INTERNATIONAL INDUSTRIES, INCORPORATED
本文書は情報提供のみを目的としています。無断転用禁止。

さまざまな機能とメリット

主要なコンポーネント	<ul style="list-style-type: none">• HARMAN SHIELD車載エージェント——内蔵され、重要アセットへの主要な侵入地点を保護。ここにはTCU、ヘッドユニット、セントラルゲートウェイが含まれます• HARMAN SHIELDスマートクライアント——データのスマート集約とバックエンドへの標準レポートを提供する集中型のクライアントサイドオーケストレーター• サイバーセキュリティアナリティクスセンター (CSAC) ——完全なダッシュボードおよびアナリティクスソリューションとして、HARMAN SHIELDエージェントからの広範な車両セキュリティ関連イベントを24時間365日にわたって可視化し、HARMAN Igniteプラットフォームに統合されます• サードパーティー統合向けAPI——HARMAN SHIELDデータをセキュリティオペレーションセンター/セキュリティインシデントおよびイベント管理 (SOC/SIEM) ソリューションにインポート
あらゆるプラットフォームとオペレーティングシステムに容易に組み込み可能	<ul style="list-style-type: none">• 自動車ソフトウェアプラットフォームとオペレーティングシステムを問わず、既存の生産ラインに容易に統合
低いメンテナンスコスト	<ul style="list-style-type: none">• 低リソースおよびリアルタイム環境向けに構築
アーキテクチャの再設計が不要	<ul style="list-style-type: none">• OEMまたはサプライヤーの既存システムでアーキテクチャの変更が一切不要• 既存ネットワークアーキテクチャへの迅速な統合とAUTOSAR準拠
内蔵のOTA統合	<ul style="list-style-type: none">• HARMAN遠隔車両アップデートサービスにより、効率的な完全車両ソフトウェア管理を実現• 遠隔車両アップデートサービスにより、デジタル署名・完全認証されたSmart Delta OTAソフトウェアパッケージを、OMA-DMプロトコルに最も厳格に準拠してコネクテッドカーに直接提供
車内および外部通信チャネル両方のための二重の境界セキュリティ	<ul style="list-style-type: none">• 単一のインストールで完全な緩和機能を提供• 広範な自動車攻撃シナリオにおいてコネクテッドECUおよびTCUを保護• 複数の防御レイヤーを提供し、自動車機能を損なったり、オーナーの個人情報盗難を引き起こしたり、ドライバーの安全を危険にさらしたりする可能性がある危険なウイルス、マルウェア、ハッキングの試みを阻止• CAN、CAN-FD、ETHERNETといった多彩なネットワークプロトコルに対応

業界のエキスパートと連携

当社のWebサイト ([harman.com/security](https://www.harman.com/security)) に是非アクセスしてください
本ソリューションに対するお問い合わせは下記までご連絡下さい。
ハーマンインターナショナル株式会社 奥田 正和
電話: +81-52-307-8816
Eメール: Masakazu.Okuda@harman.com

