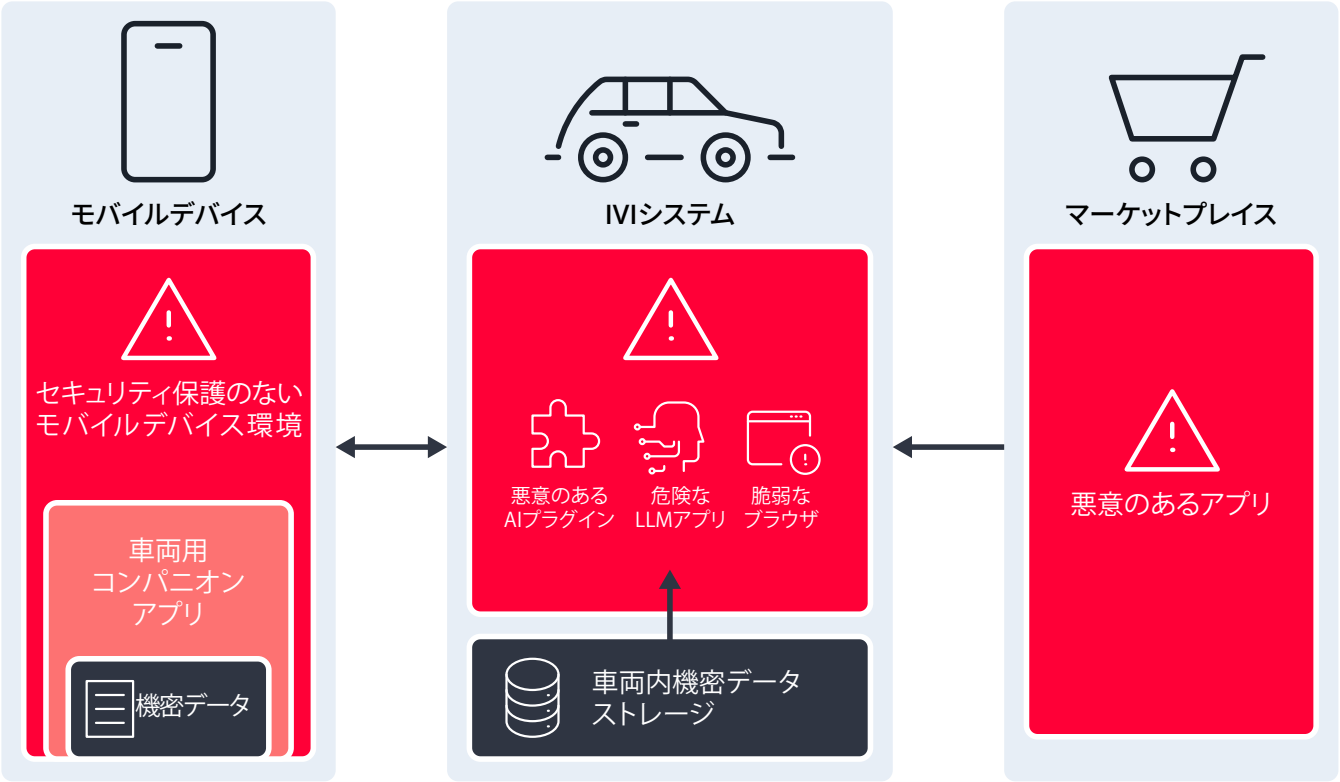
Smart Cockpit Protection

機密データ漏洩対策とセキュリティリスクの軽減で
AI搭載コックピットを安全に進化

AI搭載コックピットのリスク:機密データ漏洩との闘い

2023年上半期だけでも、自動車業界はデータ漏洩と個人識別情報(PII)の流出により、95億米ドル以上の損失を被りました*。SDV(ソフトウェア・デファインド・ビークル)の進化に伴い、ユーザーデータの保護が最重要課題となっています。VicOneの分析によると、悪意のあるAIプラグイン、危険なLLM(大規模言語モデル)アプリ、脆弱なブラウザ、その他悪質なソフトウェアなど、機密データ漏洩の原因となり得るさまざまな種類のサイバー脅威の存在が明らかになりました。これらの脅威は、AI搭載コックピット時代におけるユーザーの機密データを保護には強固なセキュリティ対策が極めて重要であることを強く示しています。

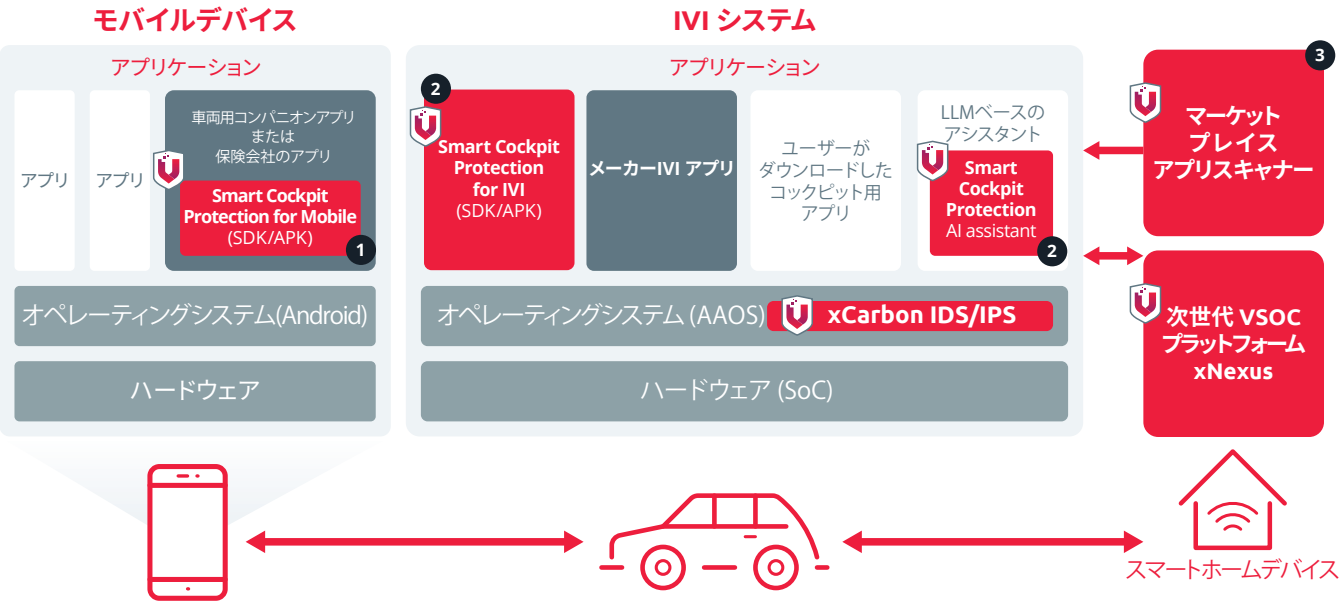


出典:VicOne 2023年 自動車サイバーセキュリティ脅威動向

AI搭載コックピット時代のイノベーションを安全に実現

スマートコックピットをあらゆる側面から保護

1. **モバイル向け Smart Cockpit Protection**
   車両用コンパニオンアプリを保護
2. **IVI向け Smart Cockpit Protection**
   IVIシステムとLLMアプリケーションを
   データ漏洩とセキュリティリスクから保護
3. **マーケットプレイス向け Smart Cockpit Protection**
   ダウンロード公開前にアプリをスキャン



主な機能

- **車両搭載AIを監視：**クラウドまたは車載環境に搭載されたLLMモデルを対象に、プロンプトインジェクション攻撃やセキュリティが脆弱なプラグインをはじめとしたOWASPトップリスクへの対策を講じ、LLMアプリをデータ漏洩から保護します。
- **ブラウザ対策：**ブラウザの脆弱性検出や悪意のあるURLへのアクセスを検知し、疑わしいウェブサイトを即座にユーザーへ警告します。これにより、フィッシングサイト詐欺やIVIシステムを危険にさらす可能性のあるリモート攻撃を防止し、ユーザーと車両の安全を守ります。
- **高リスクアプリの検出：**疑わしいAPIコール、悪意のあるURLへのアクセス、過剰な権限要求などセキュリティリスクの高いアプリを検出することにより、IVIシステムから車両用コンパニオンアプリまで、ユーザーの機密データと個人情報を確実に保護します。
- **24時間365日のモニタリング：**ダークウェブを含むインターネット上の広範囲にわたる領域において、PIIやVIN（自動車識別番号）などのデータ漏洩を監視します。漏洩を検出した場合はユーザーへ即座に通知し、迅速な対応を可能にします。
- **安全でないWi-Fi接続の検知：**
  不正またはセキュリティ保護されていないWi-Fiへの接続を検知し、なりすまし攻撃や認証情報の漏洩リスクを特定します。
- **マーケットプレイスアプリのスキャン：**
  マルウェア、ウイルス、APKの脆弱性、悪意のあるAIプラグインのスキャンにより、アプリストアへ公開前のアプリの安全性を確保します。
- **自動車用モバイルアプリの保護：**
  車両用コンパニオンアプリや保険会社のアプリにモバイル向けスマートコックピットプロテクションSDKを統合することで、個人情報の漏洩を防ぎ、安全なモバイル環境を確保します。

VicOne

SCPSolutionBrief_2024.08
Copyright © 2024 VicOne Corp.
All Rights Reserved.

詳しくはVicOneウェブサイトをご覧ください。
（vicone.com/jp または
右の QR コードよりアクセス）