

エグゼクティブサマリー

2024年を通じて、自動車およびスマートモビリティのエコシステムではサイバー脅威が急増し、大規模なランサムウェア攻撃による前例のない混乱を引き起こしました。サイバーリスクが規制対応のスピードを上回る中、リスクと組織のレジリエンス（回復力）の間のギャップがますます拡大しています。

この拡大するギャップに対処するため、組織は規制対応を超えたレジリエンスの強化が必要となります。

Upstreamの「2025年グローバルモビリティサイバーセキュリティレポート」では、このサイバーセキュリティのギャップや、中国のEV市場の拡大、更には2024年にエコシステムに影響を与えた主なトレンド、脆弱性、インシデントについて詳しく分析しています。

2024年の主な動向

自動車とスマートモビリティのサイバーセキュリティリスクの規模と影響が更に拡大

2023年～24年にかけて、重大な影響を及ぼすインシデント（数千～数百万のモビリティ資産に影響）が増加し、全インシデントの

**60%
以上**

を占めました

大規模インシデントは3倍以上に増加し、全インシデントの

19%

を占めました

92%

の攻撃がリモートで実行されました

65%

の攻撃はブラックハット（悪意のあるハッカー）によって実行されました

ブラックハットの脅威アクターはディープウェブやダークウェブを攻撃の起点として活用し、大規模な影響をもたらすことにますます意欲的になっている

70%

ブラックハットによる活動の70%が重大な影響を及ぼしました

76%以上

76%以上の攻撃が複数の利害関係者を標的とし、グローバルな影響を及ぼしました

出典: Upstream Security

中国は世界の自動車市場とサイバーセキュリティ環境の再構築を試みている

- 中国の戦略的投資と政府の支援により、同国は世界のEV市場におけるリーダーシップを確立しました。
- 2024年、中国はインテリジェントカー向けの新たなサイバーセキュリティ基準を導入し、グローバルな業界基準へ影響を強める計画を発表しました。
- 米国の対応と将来の課題
サイバーセキュリティリスクの高まりを受け、2024年9月米国商務省は、中国及びロシア製の特定のハードウェア、ソフトウェアを搭載したコネクティッドカーの販売を禁止する規制案を発表しました。

サイバーセキュリティのギャップを埋めるため、AIドリブンの検知、調査機能の導入を加速し、vSOCの監視および修復機能を向上させることが求められます。

