2022年Q4版

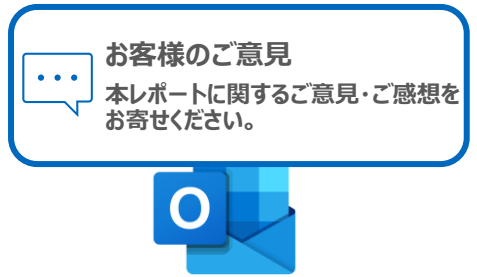
サイバーセキュリティ法規制ガイド

発行年月：2023年2月
レポート番号：539-22-Q4

目次

SAMPLE

539 - サイバーセキュリティ法規制ガイド



はじめに

今日、自動車のデジタル化は急速に進んでおり、コネクテッドおよび自動運転の機能が普及してきています。しかし同時に、このような新機能の導入により、車両はサイバーセキュリティの観点では外部の脅威にさらされてもいます。ハッカーが車両のミッションクリティカルな要素に不正アクセスするために悪用できる様々な「入口」がセキュリティ研究者によって発見されています。

『サイバーセキュリティ法規制ガイド』は主に欧州、米国、中国、日本（およびその他の国・地域）において政府による義務付け、ガイドライン、標準規格がもたらす脅威と機会を特定します。また、これら以外の国において重要な進展が見られた場合は適宜、関連法規制に関する情報も提供します。

本ガイドは有用な参照資料となるように構成されています。過去のレポートのポイントを挙げつつ最近の重要な発表を一覧にまとめることで、重要な問題にフォーカスしながら読み進められるように編纂されています。各法律、ベストプラクティス、標準規格の現状とタイムラインを示した上で特に関連性の高いトピックを詳しく解説しており、ロバスト性の高いサイバーセキュリティ戦略の策定に役立つ内容となっています。

セクション	内容
基本情報	本レポートで扱う様々な種類の法的側面の概要 **結論：**より広範な法律や政府の共通政策の一環である法律に含まれる規則がある。
最新情報	自動車サイバーセキュリティ分野の規制に関する主な出来事および活動 **結論：**既にサイバーセキュリティをより広範な「持続可能な交通輸送」政策の不可欠要素と見なしている国もあるが、まだ施策に着手していない国もある。
サマリー表	付属のExcelデータベースに収録された様々な立法活動の概要 **結論：**制定に向けて順調に進み施行に近づいている法律もあるが、法案提出後に何度か議論がなされたものの以降進展が見られないものもある。
追加調査	SBDが提供する調査サービス

注：本ガイドは実際の法規制活動のみを取り上げたものであり、何らかの提言を行うものではありません。
本ガイドで行っている分析や予測は法的助言と解されるものではありません。

本レポートで扱う法的側面の種類

法規制

「法律」とは国、州、自治体の立法機関により制定された法律もしくは一連の法律を指す。法律は法案の形で提案され、通常、一連の解釈・投票を経てから署名・施行される。これに対し「規則」はより一方的に発令できる。

規則

「規則」とは一般的に、法律をどのように施行するかを定めたルールと定義される。規則はより広範な法律の一部に関するものである場合があり、政府機関などの当局が発令できる。通常、立法プロセスを踏まずに規制機関の自由裁量で発令される。ただし、公衆や利害関係者の意見が考慮されることが多い。

ベストプラクティス

「ベストプラクティス」／「ガイドライン」は規制機関や標準規格策定団体などの信任された利害関係者が発行でき、参照することにより政策に盛り込めるが、準拠については本来任意である。通常、推奨される手順、技術、またはツールであり、政策などの要件の遵守を支援するものである。

標準規格

「標準規格」とはプロセスの評価基準となる文書化されたガイドラインを指す。通常、標準規格の策定作業は協調的に進められ、専門家からなるコンソーシアムの総意により確定される。ただし、法律／規則とは異なり、標準規格への準拠は実際には任意であることが多い。

本章について

本章では、自動車サイバーセキュリティ分野の政策における最新の動向を扱う。

自動車サイバーセキュリティエコシステム全体に直接影響を与える可能性のあるいくつかの政策における最近の活動を中心に取り上げる。また、過去数年／四半期の動向との相違点を示すとともに、現在進行中の政策の基盤が何らかの影響を及ぼしたかどうかについても着目する。

さらに、法律の導入・施行の成否が国によって分かれる理由を分析するとともに、一部の規則が発効に至らない要因と課題を明らかにする。

本章の主なポイント

- サイバーセキュリティはNCAPの評価体系のどこに、どのように組み込まれているか？
- 影響力の大きい主な法規制関連トピックは何か？
- 特に自動車のサイバーセキュリティ業界が直面している政策上の阻害因子は何か？

サイバーセキュリティと改ざん対策はグリーンNCAPの必須要素

グリーンNCAPロードマップ2030

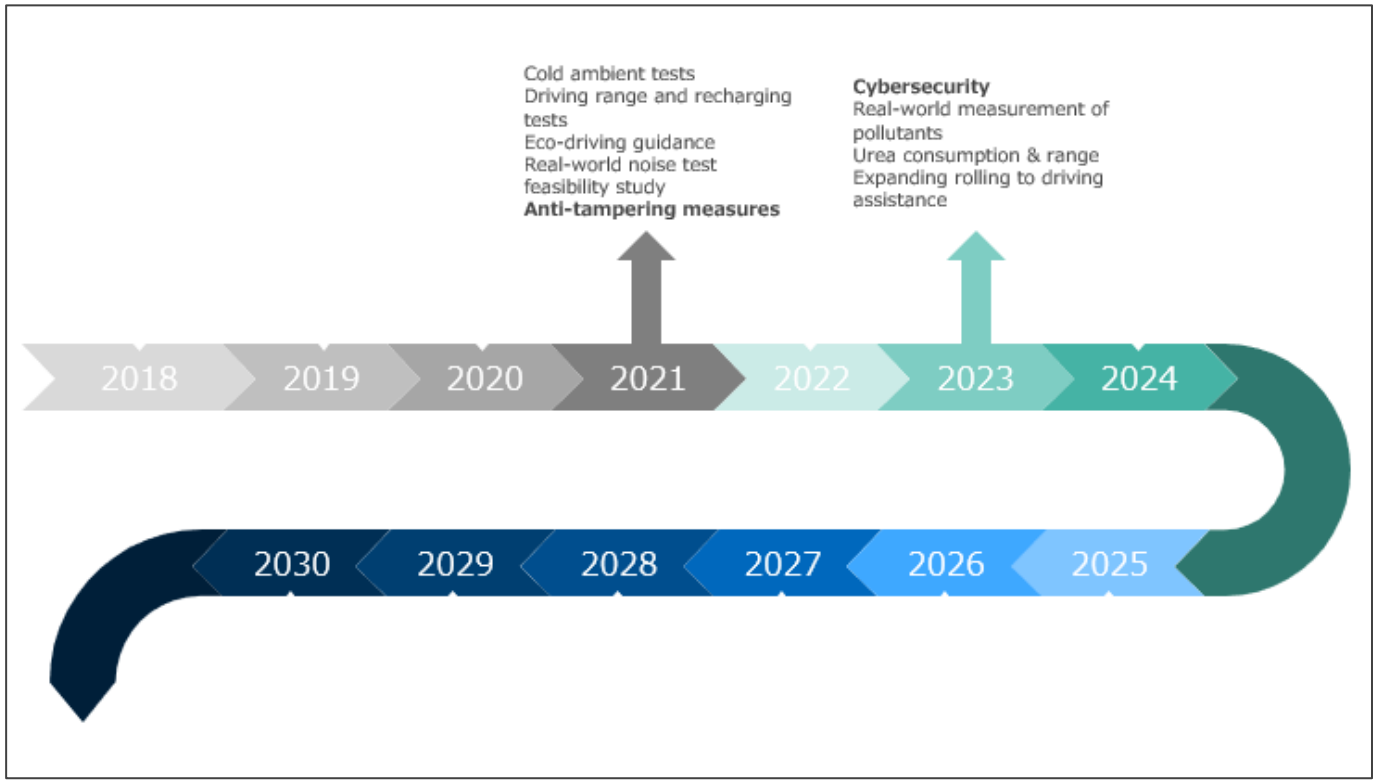
グリーンNCAPは**ユーロNCAPが立ち上げた**独立系プロジェクトであり、クリーンでエネルギー効率が高く、環境に優しい自動車の開発促進を目指している。グリーンNCAPは消費者やフリート運用事業者などに向けて**簡約評価体系の下で汚染物質および温室効果ガスの排出量を自動車のエネルギー効率と関連付けている。**

グリーンNCAPはUNECE GRPEおよびWP29と足並みを揃えており、UNECEの作業部会と連携し知識や事実情報を共有することで、テスト要件をUNECEテスト手順と同期させようとしている。

グリーンNCAPのロードマップ2030の主なポイントの1つは、**改ざん対策を含める**ことによりコンポーネントの整合性と環境性能制御を確保することである。この中で、グリーンNCAPは最低限の保護レベルと車載データのアクセシビリティを自動車メーカーが実証することを推奨／要求する場合がある。これ自体が車両の総合評価に大きな影響を及ぼす可能性はないものの、従わなければ車両データが改ざんされていることが判明した場合に批判を招き得る。

ロードマップ2030のもう1つの重要なマイルストーンは**「サイバーセキュリティ」**である。グリーンNCAPは排出量／エネルギー効率制御システムのサイバー攻撃とリモート改ざんを防止するために、車内における最低限の保護レベルを要求する可能性がある。これは、保護レベルが許容範囲の車両と比べセキュアではない車両は排出量が多くなるためで、メーカーの設計よりも燃料／電力消費量は多くなる可能性があるという論拠に基づいている。

グリーンNCAPのロードマップ2030におけるサイバーセキュリティ対策期限



グリーンNCAP関連の最新情報：Tesla Model 3、NIO ET7、Renault Megane E-techがグリーンNCAPの持続可能性評価体系の下で5つ星を獲得。

SAMPLE

本章について

本章では、全ての法的活動（法律、法案、規則、政策、ガイドライン）をサマリー表に示すとともに、最新の法的状況（提出、起草、施行）を提示する。各スライドの右のセクションには法的トピック、最近の活動、次に予定されているアクション（該当がある場合）に関する主なポイントをまとめている。

左のマトリクス図には立法活動を活動時期と法的状況に基づいて示す。状況の分類は以下のとおり。

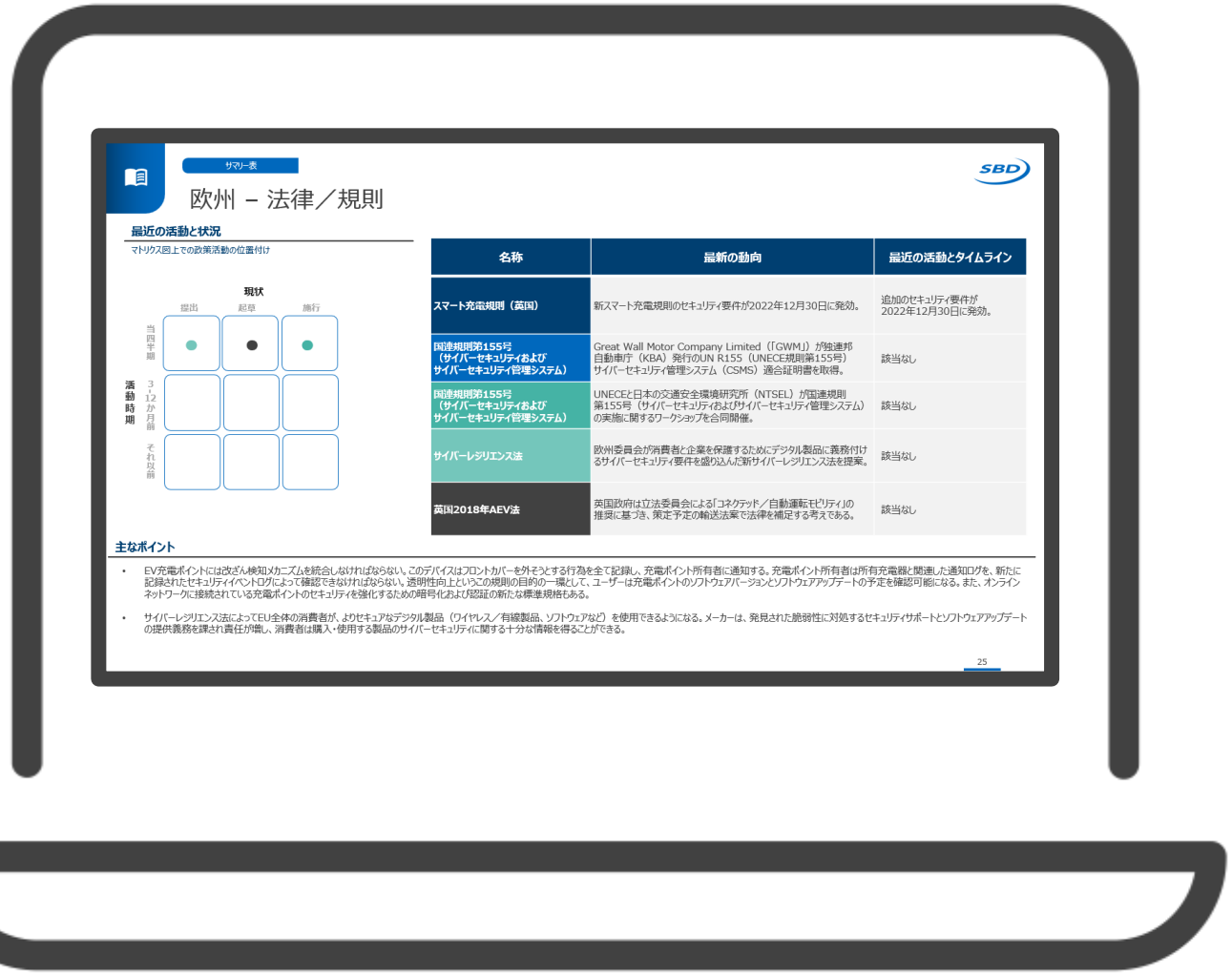
- **提出 –** 政策案が提出済み
- **起草** – 政策案が提出済みかつ検討中
- **施行／公布** – 政策が発効済み（またはガイドラインが検討を経て公開／発表済み）

活動のタイムライン

- **当四半期** – 本レポートの調査対象である直近の四半期に行われた活動
- **3-12か月前** – 四半期以上前かつ1年以内の活動
- **それ以前** – 調査の時点で12か月以上前の活動

本章の主なポイント

- 自動車サイバーセキュリティ開発全般との関連性が高い法規制は？
- 活動のタイムラインは？法規制のこれまでの進捗は？
- 最近の活動から推測される次の活動は？



注：サマリー表の「最新の動向」欄には重視すべき最近の記事のみを掲載している。一部の記事は業界の最新情報であるため、*3X3*マスのマトリクス図には示されていない。
最近の活動の詳細は、*539-MS Excel*データベースを参照のこと。

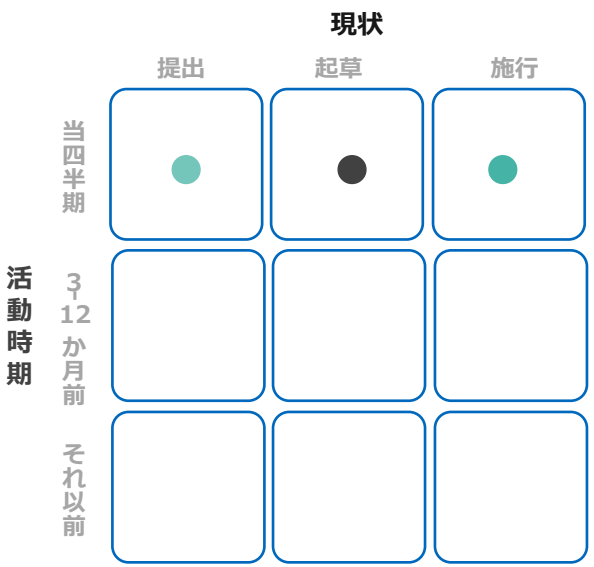
サマリー表

SAMPLE

欧州 – 法律／規則

最近の活動と状況

マトリクス図上での政策活動の位置付け



名称	最新の動向	最近の活動とタイムライン
スマート充電規則（英国）	新スマート充電規則のセキュリティ要件が2022年12月30日に発効	追加のセキュリティ要件が2022年12月30日に発効
国連規則第155号（サイバーセキュリティおよびサイバーセキュリティ管理システム）	Great Wall Motor Company Limited（「GWM」）が独連邦自動車庁（KBA）発行のUN R155（UNECE規則第155号）サイバーセキュリティ管理システム（CSMS）適合証明書を取得	該当なし
国連規則第155号（サイバーセキュリティおよびサイバーセキュリティ管理システム）	UNECEと日本の交通安全環境研究所（NTSEL）が国連規則第155号（サイバーセキュリティおよびサイバーセキュリティ管理システム）の実施に関するワークショップを合同開催	該当なし
サイバーレジリエンス法	欧州委員会が消費者と企業を保護するためにデジタル製品に義務付けるサイバーセキュリティ要件を盛り込んだ新サイバーレジリエンス法を提案	該当なし
英国2018年AEV法	英国政府は立法委員会による「コネクテッド／自動運転モビリティ」の推奨方針に基づき、策定予定の輸送法案で法律を補足する考えである	該当なし

主なポイント

- EV充電ポイントには改ざん検知メカニズムを備えなければならない。このデバイスはフロントカバーを外そうとする行為を全て記録し、充電ポイント所有者に通知する。充電ポイント所有者は所有充電器と関連した通知ログを、新たに記録されたセキュリティイベントログによって確認できなければならない。透明性向上というこの規則の目的の一環として、ユーザーは充電ポイントのソフトウェアバージョンとソフトウェアアップデートの予定を確認可能になる。また、オンラインネットワークに接続されている充電ポイントのセキュリティを強化するための暗号化および認証の新たな標準規格もある。

- サイバーレジリエンス法によってEU全体の消費者がよりセキュアなデジタル製品（ワイヤレス／有線製品、ソフトウェアなど）を使用できるようになる。メーカーは、発見された脆弱性に対処するセキュリティサポートとソフトウェアアップデートの提供義務によって責任が増し、消費者は購入・使用する製品のサイバーセキュリティに関する十分な情報を得ることができる。

Excelデータベース

SAMPLE

539 - サイバーセキュリティ法規制ガイド

C A S E S

539-22-Q4 法規制

対象市場	国／地域（該当する場合）	トピック（自動車／IoT／セキュリティ研究者）	政策名／番号	カテゴリー（規則／法律／義務化）	背景	解説	最終更新時期	記事公開日	提出
英国	-	自動車	英国2018年AEV法	法規制	「2018年自動運転と電気自動車に関する法」（"AEV法"）は、自動運転車による事故が発生した場合に誰が責任を負うのか（法的責任の所在）を明らかにすると共に、EV充電インフラ整備の促進を規定する法律である。	AEV法は、この分野においてさらなるリスク要因となり得るサイバーセキュリティ問題に直接対処するものではない。しかし、同法は当局にとって今後、計画中の「The Electric Vehicles (Smart Charge Points) Regulations 2021（2021年EV（スマート充電ポイント）法）」のように下位法令を通じてサイバーセキュリティ要件を追加する際の指針となるであろう。最終報告の期限は2021年第4四半期。	2022年Q1版	2022/11/23	-
欧州	-	自動車	国連規則第155号（サイバーセキュリティおよびサイバーセキュリティ管理システム）	規則	WP.29（自動車基準調和世界フォーラム）は国連欧州経済委員会（UNECE）の下部組織である。WP.29の分科会であるGRVAが自動運転車／コネクテッドカーを担当しており、サイバーセキュリティとOTAソフトウェアアップデートの作業部会も運営している。WP.29はコネクテッドカーおよび自動運転技術（ADT）搭載	UNECE R155は自動車サイバーセキュリティに関する世界初の規則であり、市場に直接影響を及ぼすであろう。WP.29の規則の下、UNECE加盟国で販売を行うOEMはバリューチェーンおよび製品ライフサイクルの全体において十分なサイバーリスク管理を実施している証拠を提供しなければならない。さらに	2022年Q1版	2022/10/17	-
欧州	-	自動車	国連規則第155号（サイバーセキュリティおよびサイバーセキュリティ管理システム）	規則	WP.29（自動車基準調和世界フォーラム）は国連欧州経済委員会（UNECE）の下部組織である。WP.29の分科会であるGRVAが自動運転車／コネクテッドカーを担当しており、サイバーセキュリティとOTAソフトウェアアップデートの作業部会も運営している。WP.29はコネクテッドカーおよび自動運転技術（ADT）搭載	UNECE R155は自動車サイバーセキュリティに関する世界初の規則であり、市場に直接影響を及ぼすであろう。WP.29の規則の下、UNECE加盟国で販売を行うOEMはバリューチェーンおよび製品ライフサイクルの全体において十分なサイバーリスク管理を実施している証拠を提供しなければならない。さらに	2022年Q1版	-	-
欧州	-	自動車	国連規則第156号	規則	WP.29（自動車基準調和世界フォーラム）は国連欧州経済委員会（UNECE）の下部組織である。WP.29の分科会であるGRVAが自動運転車／コネクテッドカーを担当しており、サイバーセキュリティとOTAソフトウェアアップデートの作業部会も運営している。WP.29は車両にセキュアなOTAソフトウェアアップデートを提供	これはOTAを含む車両ソフトウェアアップデートに関する初の国際的規則である。WP.29の規則の下、UNECE加盟国で販売を行うOEMは要件を遵守している証拠を提供しなければならない。規則に違反した場合、新車種は型式認定されないためにUNECE加盟国では販売することができない。間もなく、同様の要件が	2022年Q2版	Jun-22	-
					中国当局はデータ保護に対する消費者意識と国家安全保障に対する政府の懸念の高まりを受け、重要ではあるが一般的なデータプライバ	中国の新しい自動車データ規則は消費者保護の点では欧州のGDPRに相当する。しかし、国家安全保障の点ではさらに進んでおり、収			

ホーム | 法規制 | ベストプラクティス、ガイドライン | 標準規格 | 経緯 | 用語定義

Excelデータベースには完全なデータセットを収録しており、フィルタリングや並べ替え機能を使用して特定の規則/法律/政策/標準規格や関心のあるその他の関連データの検索が可能です。

Excelデータベース

SAMPLE

539 - サイバーセキュリティ法規制ガイド

539-22-Q1

C A S E

ベストプラクティス

対象市場	国／地域（該当する場合）	トピック（自動車／IoT／一般）	政策名／番号	カテゴリー（ベストプラクティス／ガイドライン）	背景	解説	最終更新時期	記事公開日
米国	-	IoT／一般	NIST SP 800シリーズ	-	国立標準技術研究所（NIST）特別刊行物（SP）は一連のセキュリティ／プライバシーガイドライン、推奨事項ドキュメント、および参考	NIST SP 800シリーズのドキュメントはかなりの数が自動車業界に関連している。同シリーズは多くの車両ユースケースに適用可能	2022年Q4版	Dec-22
欧州	ドイツ	自動車	DE VDA – 自動車CSMS監査	-	VDAが「自動車サイバーセキュリティ管理システム（ACSMS）の監査」を発行。これは体系的なリスクベース管理システムに基づく自動車	VDAの監査ドキュメントはUNECE R155規則を補完するものであり、OEMとサプライヤーが自社CSMSの成熟度と適合性を評価する	2020年Q4版	Dec-20
欧州	-	自動車	ユーロNCAPビジョン2030	-	ユーロNCAPが今後10年間にわたり消費者テストプログラムをどのように進化させていくかを概説したビジョン文書を発行した。 サイバーセ	セキュリティ機能の標準化テストは議論を呼ぶトピックであり、OEMはR155の技術を回わない（制御そのものではなく開発プロセスを指定	2022年Q4版	2022/11/9
欧州	-	自動車	ENISA – 自動車サイバーセキュリティ	ベストプラクティス	ENISA（EUのサイバーセキュリティ機関）の「スマートカーのサイバーセキュリティとレジリエンス」は、コネクテッドカーと自動運転車のためのの	ENISAの元のサイバーセキュリティガイドラインは現在、大部分が国際規則／規格によって置き換えられている。しかし、その後発行された	2019年Q4版	2019/11/25
カナダ	-	自動車	カナダ - 自動車サイバーセキュリティガイダンス	ガイドライン	カナダ運輸省（Transport Canada）が、車両のサイバー安全性確保のための技術的に中立かつ既定の枠組みに捉われない指導原	カナダはUNECE R155やISO/SAE 21434などの国際サイバーセキュリティ規則／規格に積極的に対応しており、関連トピックについて米	2020年Q1版	Mar-20
英国	-	自動車	英国運輸省 - Cyber Signposting	ガイドライン	英国のTransport Technology ForumがCyber Security Signposting Guidanceを発表。これはITS（高度道路情報システ	英国の「Signposting」ドキュメントは自動車サイバーセキュリティ関連の規格、指令、その他のドキュメントの包括的リストである。しか	2020年Q4版	2021/6/23
グローバル	-	IoT／一般	OWASP	-	Open Web Application Security Project（OWASP）はソフトウェアのセキュリティ強化を専門とする高名な非営利財団。	OWASPガイドラインは車載システムに特化したものではないものの、自動車エコシステム全体において高度なコネクテッド機能の開発およ	2022年Q4版	2022/9/20
欧州	-	自動車	グリーンNCAPロードマップ2030	-	グリーンNCAPはユーロNCAPが立ち上げた独立系プロジェクトであり、クリーンでエネルギー効率が高く、環境に優しい自動車の開発促進	グリーンNCAPはUNECE GRPEとWP.29による方針と決定に厳密に従っており、要件をUNECEと合わせるよう取り組んでいる。2021	2022年Q4版	2022/11/7
英国	-	自動車	英国運輸省 - 基本原則	-	「コネクテッドカーおよび自動運転車（CAV）サイバーセキュリティ基本原則」は、英国運輸省（DfT）と国家インフラ保護センター	英国は2016年に基本原則を発行した当時、自動車業界向けサイバーセキュリティ要件策定の最前線にいた。同じ頃、NHTSAはベスト	2022年Q4版	2022/10/21
英国	-	IoT／一般	UK NCSCのスマートシティに関する原則	-	英国国家サイバーセキュリティ機関（NCSC – 国家サイバーセキュリティセンター）は地方自治体向けに、ネットワークとインフラのサ	コネクテッドカーおよび自動運転車は路側インフラ、自動駐車システム、モビリティシステム、さらに最終的にはロボットタクシーネットワークと	2022年Q4版	2022/10/21
欧州	-	自動車	EDPB – 自動車向けデータプライバシー	-	欧州データ保護会議（EDPB）が、「コネクテッドカーおよびモビリティ関連アプリケーションにおける個人情報処理に関するガイドライン	EDPBのガイドラインはOEM向けに、車上の個人データとモバイルアプリやクラウドプラットフォームに転送された個人データをどう保護すべきか	2022年Q4版	2022/10/12
欧州	ドイツ	自動車	DE VDA – ASPICE for Cybersecurity	ガイドライン	VDAは「Automotive SPICE for Cybersecurity」の草案を発行した。これはISO/IEC 33020:2015およびISO/SAE	「ASPICE for Cybersecurity」はソフトウェアの観点でサイバーセキュリティ関連の開発プロセスの評価を可能にする。事実上、	2021年Q2版	2021/4/9
欧州	-	自動車	欧州ACEA - サイバーセキュリティ原則	-	ACEA Principles of Automotive Cybersecurity（ACEA自動車サイバーセキュリティ原則）は、近年増大する自動車のセ	2010年代後半に発行された他の大半のベストプラクティスガイドラインと同様にACEAの「原則」ドキュメントは現在、大部分がUNECE	2022年Q4版	2022/10/12
米国	-	自動車	「未来の輸送に備える：自動運転車3.0」	ガイドライン	「連邦自動運転車開発ガイドライン」は遵守を義務付ける法的要件ではなく、あくまで自動車メーカーなど関連企業や団体に対してHAV	米国運輸省とNHTSAによる一連の自動運転車方針ドキュメントの目的は、米国の自動運転車を対象とした投資と開発が円滑に進めるよう	2018年Q4版	2018/10/4

ホーム | 法規制 | ベストプラクティス、ガイドライン | 標準規格 | 経緯 | 用語定義

Excelデータベースには完全なデータセットを収録しており、フィルタリングや並べ替え機能を使用して特定の規則/法律/政策/標準規格や関心のあるその他の関連データの検索が可能です。

SBD Automotive のお問い合わせ先

本書の内容、SBDのその他の調査・サービスについてのお問い合わせ

本書の内容、SBDのその他の調査・サービスについてお問い合わせは
SBD Automotive ジャパン（Postbox@sbdautomotive.com）
およびSBDのグローバル各拠点にて承っております。

Postbox@sbdautomotive.com

お問い合わせ

米国 | 英国 | ドイツ | インド | 中国 | 日本

各拠点のサポートエリアと担当窓口

日本、韓国、オーストラリア
日本オフィス
postbox@sbdautomotive.com
+81 52 253 6201

中国
中国オフィス
salesChina@sbdautomotive.com
+86 18516653761

英国、西・南欧
Luigi Bisbiglia
luigibisbiglia@sbdautomotive.com
+44 1908 305102

ドイツ、北・東欧
Andrea Sroczynski
andreasroczynski@sbdautomotive.com
+49 211 9753153-1

北米
Garren Carr
garrencarr@sbdautomotive.com
+1 734 619 7969