

# サイバーセキュリティに係る協定規則 UN-R155 について

一般社団法人 日本自動車車体工業会  
中央技術委員会

# 1. 自動車におけるサイバーセキュリティ規制導入の背景

## 1.1. 自動車の高度な電子化とネットワーク接続の進展 (CASE 革命)

- Connected (コネクテッド)

自動車が常時インターネットに接続され、ナビゲーション、エンターテインメント、車両データの送受信、OTA (Over-The-Air) アップデートといった様々なサービスが提供されるようになりました。これにより、外部からの不正アクセスやサイバー攻撃の経路が増加しました。

- Autonomous (自動運転)

自動運転技術の発展により、車両の制御システムが高度に電子化・ソフトウェア化されています。これにより、サイバー攻撃が運転機能に直接影響を与え、重大な事故につながるリスクが高まりました。実際に、遠隔操作で車両のエンジン停止やブレーキ操作を行った事例も報告されています。

- Shared & Services (シェアリングとサービス)

カーシェアリングなどの新しいモビリティサービスが登場し、車両データやユーザー情報が共有される機会が増えました。これにより、個人情報の漏洩や不正利用のリスクも考慮する必要が出てきました。

- Electric (電動化)

電動化に伴い、バッテリー管理システムや充電インフラなどもネットワークに接続されるようになり、これらのシステムに対するサイバー攻撃のリスクも考慮されるようになりました。

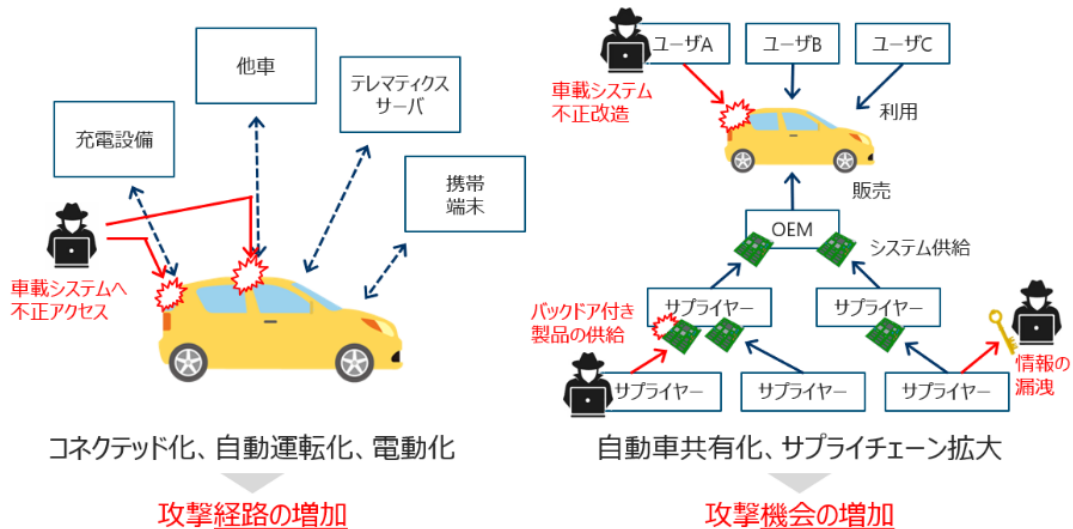
## 1.2. サイバー攻撃の高度化と現実の脅威

- 多様な攻撃手法

ランサムウェア、DDoS 攻撃、サプライチェーン攻撃、情報漏洩など、サイバー攻撃の手法は日々高度化・巧妙化しています。自動車業界においても、サプライヤのシステムが攻撃され、自動車メーカーの生産ラインが停止するといった事例も発生しており、サプライチェーン全体でのセキュリティ対策の重要性が認識されるようになりました。

- 人命に関わるリスク

従来の IT システムへのサイバー攻撃は、主に情報漏洩や金銭的損害が主でしたが、自動車へのサイバー攻撃は、車両の制御を奪われることで人命に関わる重大な事故に直結する可能性があり、その影響は甚大です。



※ 上図は、ビジネスキューブ・アンド・パートナーズ(株)様の Web サイトから引用しました <https://biz3.co.jp/>

## 2. 法規の動向

これらの背景を受け、国連欧州経済委員会（UNECE）の WP.29(自動車基準調和世界フォーラム)において、自動車のサイバーセキュリティに関する国際的な規制が検討され、2021年1月に「UN-R155(サイバーセキュリティ及びサイバーセキュリティ管理システムに関する規則)」が発効しました。

これにより、自動車メーカーに対して、車両のライフサイクル全体(設計、開発、生産、運用、廃棄)にわたるサイバーセキュリティ管理システム(CSMS)の構築と、車両の型式認証におけるサイバーセキュリティ性能の確保が義務付けられました。

型式認定相互承認協定の加盟各国は、この UN-R155 に準拠する形で国内の保安基準を改正しており、日本においては、道路運送車両の保安基準 第17条の2 第3項がこれに対応しています。

その適用時期は以下のとおりです。

- 無線によるソフトウェアアップデートに対応している車両

新型車： 令和4年7月1日                      継続生産車： 令和6年7月1日

- 無線によるソフトウェアアップデートに対応していない車両

新型車： 令和6年1月1日                      継続生産車： 令和8年5月1日

## 3. 架装における留意点

UN-R155 は、車両型式取得にあたって車両メーカーが考慮しなければならないサイバー脅威を ANNEX5 Part A に列挙しています。

車両メーカーはこの要求に従って ANNEX5 Part A TableA1 の全項目について適切な対応を行っているので、架装の際には、これらの脅威を増大させる可能性のある電気工事を行わないよう留意してください。

※ 本資料の付録に ANNEX5 Part A TableA1 を掲載しています。

## 4. 用語

- ・ ランサムウェア  
感染したコンピュータのデータ等を暗号化して使用できない状態にした上で、その復号と引き換えに身代金(金銭や暗号資産)を要求する不正プログラムの一種。
- ・ DDoS 攻撃(分散型サービス拒否攻撃)  
複数のコンピュータから同時に大量のアクセスやデータを送りつけることで、Web サイトやサーバーに過剰な負荷をかけ、サービス提供を妨害するサイバー攻撃。
- ・ サプライチェーン攻撃  
ターゲット企業を直接攻撃をするのではなく、セキュリティ対策に弱点がある関連企業や取引先・委託先企業を「踏み台」として、そこを経由してターゲット企業に不正侵入を行うサイバー攻撃。

## 5. 参考文献

- ・ ビジネスキューブ・アンド・パートナーズ株式会社 - ISO/SAE 21434 について  
([https://biz3.co.jp/lp\\_category/iso21434](https://biz3.co.jp/lp_category/iso21434))
- ・ アクセンチュア株式会社 - CASE 時代の自動車におけるサイバーセキュリティの 6 つの要諦  
(<https://www.accenture.com/jp-ja/insights/security/connected-vehicle-1>)
- ・ 株式会社カスペルスキー - Black Hat USA 2015:ジープのハッキングの全容が明らかに  
(<https://blog.kaspersky.co.jp/blackhat-jeep-cherokee-hack-explained/8480/>)
- ・ 警視庁 - ランサムウェア被害防止対策  
(<https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html>)
- ・ KDDI - DDoS 攻撃とはどんな攻撃？ 攻撃の種類や対策をご紹介  
(<https://biz.kddi.com/content/column/smartwork/what-is-ddos/>)
- ・ NRI セキュアテクノロジーズ株式会社 - セキュリティ用語解説 - サプライチェーン攻撃  
(<https://www.nri-secure.co.jp/glossary/supply-chain-attack>)
- ・

## 付録：UN-R155 Annex 5 Part A

※ 本表は、CS型式審査マニュアル 2025 年 4 月 8 日改訂版(CS/OTA 国内採用 WG 編)から引用しました。

最新版については、UNECE(国際連合欧州経済委員会)の Web サイトにてご確認ください。URL : <https://unece.org/un-regulations-addenda-1958-agreement>

Table A1 List of vulnerability or attack method related to the threats

High level and sub-level descriptions of vulnerability/ threat				Example of vulnerability or attack method			
4.3.1 Threats regarding back-end servers related to vehicles in the field	フィールドの車両に関連するバックエンドサーバーに関する脅威	1	Back-end servers used as a means to attack a vehicle or extract data	車両を攻撃する手段またはデータを抽出する手段としてバックエンドサーバーが利用される	1.1	Abuse of privileges by staff (insider attack)	スタッフによる特権の悪用 (インサイダー攻撃)
					1.2	Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	サーバーへの不正なインターネットアクセス (例えば、バックドア、パッチが適用されていないシステムソフトウェアの脆弱性、SQL 攻撃またはその他の手段によって可能となる)
					1.3	Unauthorized physical access to the server (conducted by for example USB sticks or other media connecting to the server)	サーバーへの不正な物理的アクセス (例えば、USB、またはサーバーに接続する他の媒体によって行われる)
		2	Services from back-end server being disrupted, affecting the operation of a vehicle	バックエンドサーバーからのサービスが中断され、車両の動作に影響を与える	2.1	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on	バックエンドサーバーへの攻撃による機能停止。例えば、サーバーと車両との相互作用ならびに車両が依存しているサーバーによるサービスの提供が妨げられる。
		3	Vehicle related data held on back-end servers being lost or compromised ("data breach")	バックエンドサーバーに保持されていた車両関連データが損失または危殆化される (データ漏洩)	3.1	Abuse of privileges by staff (insider attack)	社員・職員による特権の悪用 (インサイダー攻撃)
					3.2	Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers	クラウドにおける情報損失。取扱いに注意を要するデータがサードパーティクラウドサービス提供者により保管されているときに攻撃または自己によりデータが損失される可能性がある。
					3.3	Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	サーバーへの不正なインターネットアクセス (例えば、バックドア、パッチが適用されていないシステムソフトウェアの脆弱性、SQL 攻撃、またはその他の手段によって可能となる)
					3.4	Unauthorized physical access to the server (conducted for example by USB sticks or other media connecting to the server)	サーバーへの不正な物理的アクセス (例えば、USB、またはサーバーに接続する他の媒体によって行われる)
					3.5	Information breach by unintended sharing of data (e.g. admin errors)	意図的でないデータ共有による情報漏洩 (例：管理者のエラー)

High level and sub-level descriptions of vulnerability/ threat				Example of vulnerability or attack method			
4.3.2 Threats to vehicles regarding their communication channels	通信路に係る車両への脅威	4	Spoofing of messages or data received by the vehicle	車両が受信したメッセージまたはデータのなりすまし	4.1	Spoofing of messages by impersonation (e.g.802.11p V2X during platooning, GNSSmessages, etc.)	なりすましによるメッセージ偽装 (隊列走行中の802.11p V2X 通信、GNSS メッセージなど)
					4.2	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)	シビル攻撃 (あたかも路上に多くの車両が存在しているかのように他の車両になりすますため)
		5	Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	車両に保存されているコード/データの不正な改ざん、削除またはその他の変更を行うために通信路が利用される	5.1	Communications channels permit code injection, for example tampered software binary might be injected into the communication stream	通信路がコード注入を許可する。例えば、改ざんされたソフトウェアバイナリが通信ストリームに注入される可能性がある。
					5.2	Communications channels permit manipulate of vehicle held data/code	通信路が車両に保存されているデータ/コードの改ざんを許可する。
					5.3	Communications channels permit overwrite of vehicle held data/code	通信路が車両に保存されているデータ/コードの上書きを許可する。
					5.4	Communications channels permit erasure of vehicle held data/code	通信路が車両に保存されているデータ/コードの消去を許可する。
					5.5	Communications channels permit introduction of data/code to the vehicle (write data code)	通信路が車両へのデータ/コードの導入 (データ/コードの書き込み) を許可する。
		6	Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks	信用できない/信頼できないメッセージの受け入れを許可する通信路、またはセッションハイジャック/リプレイ攻撃に対して脆弱な通信路	6.1	Accepting information from an unreliable or untrusted source	信頼できない、または信用できないソースからの情報を受け入れる。
					6.2	Man in the middle attack/ session hijacking	中間者攻撃/セッションハイジャック
					6.3	Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway	リプレイ攻撃。例えば、通信ゲートウェイに対する攻撃により攻撃者がゲートウェイのファームウェアまたは ECU ソフトウェアをダウングレードすることが可能になる。
		7	Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	情報が容易に開示される可能性がある。例えば、通信の盗聴によって、または取扱いに注意を要するファイルやフォルダへの不正アクセスを許可することによって。	7.1	Interception of information / interfering radiations / monitoring communications	情報の傍受/干渉放射/通信の監視
					7.2	Gaining unauthorized access to files or data	ファイルまたはデータへの不正アクセス

High level and sub-level descriptions of vulnerability/ threat				Example of vulnerability or attack method					
4.3.2 Threats to vehicles regarding their communication channels	通信路に係る車両への脅威	8	Denial of service attacks via communication channels to disrupt vehicle functions	車両機能を妨害するための通信路を介した DoS 攻撃	8.1	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	車両情報システムが正常な方法でサービスを提供できないように、当該システムに対しゴミのようなデータを大量に送信する。		
					8.2	Black hole attack, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles	ブラックホール攻撃。車両間通信を妨害するために、攻撃者が車両間のメッセージをブロックする。		
		9	An unprivileged user is able to gain privileged access to vehicle systems	非特権ユーザーが車両システムへの特権アクセスを取得できる	9.1	An unprivileged user is able to gain privileged access, for example root access	非特権ユーザーが特権アクセスを取得できる。例えば、ルート権限。		
		10	Viruses embedded in communication media are able to infect vehicle systems	通信媒体に埋め込まれたウイルスが車両システムに感染する可能性がある	10.1	Virus embedded in communication media infects vehicle systems	通信媒体に組み込まれたウイルスが車両システムに感染する。		
		11	Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content	車両によって受信されるメッセージ（例えば、X2Vまたは診断メッセージ）または車両内で送信されるメッセージに悪意のあるコンテンツが含まれている	11.1	Malicious internal (e.g. CAN) messages	悪意のある内部メッセージ（例：CAN）		
					11.2	Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)	悪意のある V2X メッセージ 例：インフラ対車両、または車両間メッセージ（例：CAM、DENM）		
					11.3	Malicious diagnostic messages	悪意のある診断メッセージ		
					11.4	Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier)	悪意のある専用メッセージ（例：通常は OEM またはコンポーネント/システム/機能サプライヤから送信されるメッセージ）		
		4.3.3. Threats to vehicles regarding their update procedures	更新手順に関する車両への脅威	12	Misuse or compromise of update procedures	更新手順の不正利用または危殆化	12.1	Compromise of over the air software update procedures. This includes fabricating the system update program or firmware	OTA ソフトウェア更新手順の危殆化。これはシステム更新プログラムまたはファームウェアの偽造を含む。
							12.2	Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware	ローカル/物理的ソフトウェア更新手順の危殆化。これはシステム更新プログラムまたはファームウェアの偽造を含む。
12.3	The software is manipulated before the update process (and is therefore corrupted), although the update process is intact						更新手順は損なわれていなくても、更新手順前にソフトウェアが改ざんされている（したがって破損している）		
12.4	Compromise of cryptographic keys of the software provider to allow invalid update						無効な更新を許可するためのソフトウェア提供者の暗号鍵の危殆化。		

High level and sub-level descriptions of vulnerability/ threat				Example of vulnerability or attack method						
4.3.3. Threats to vehicles regarding their update procedures	更新手順に関する車両への脅威	13	It is possible to deny legitimate updates	正規の更新が拒否される可能性がある	13.1	Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features	重要なソフトウェア更新のロールアウトおよび/または顧客固有機能のロック解除を妨げるための、更新サーバーまたはネットワークに対するDoS攻撃。			
4.3.4 Threats to vehicles regarding unintended human actions facilitating a cyber attack	サイバー攻撃を助長化する意図しない人間の行動に係る車両への脅威	15	Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack	正規の行動主体が意図せずにサイバー攻撃を助長化するような行動をとることができる	15.1	Innocent victim (e.g. owner, operator or maintenance engineer) being tricked into taking an action to unintentionally load malware or enable an attack	罪のない被害者（例：所有者、操作者またはメンテナンス技術者）が騙されて、意図せずにマルウェアをロードする行動または攻撃を可能にする行動をとる。			
					15.2	Defined security procedures are not followed	定められたセキュリティ手順に従っていない。			
4.3.5 Threats to vehicles regarding their external connectivity and connections	外部接続および接続部に係る車両への脅威	16	Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications	車両機能の接続性の改ざんによって、サイバー攻撃が可能になる。これにはテレマティクス、リモート操作が可能なシステム、および短距離無線通信を利用したシステムが含まれる	16.1	Manipulation of functions designed to remotely operate systems, such as remote key, immobilizer, and charging pile	リモートキー、イモビライザー、充電パイルなど、システムを遠隔操作するための機能の改ざん			
					16.2	Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)	車両テレマティクスの改ざん（例：温度測定を改ざんし、貨物ドアを遠隔解除する）			
					16.3	Interference with short range wireless systems or sensors	短距離無線システムまたはセンサへの干渉			
		17	Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems	車両システムを攻撃する手段として、ホストされているサードパーティソフトウェア（例：娯楽アプリケーション）が利用される	17.1	Corrupted applications, or those with poor software security, used as a method to attack vehicle systems	改ざんされたアプリケーションまたはソフトウェアセキュリティが不十分なアプリケーションを、車両システムを攻撃する方法に使用する			
					18	Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems	車両システムを攻撃する手段として、外部インターフェース（例：USBポート、OBDポート）に接続された装置が利用される	18.1	External interfaces such as USB or other ports used as a point of attack, for example through code injection	USBまたはその他のポートなどの外部インターフェースが、例えばコード注入の攻撃場所として利用される
								18.2	Media infected with a virus connected to a vehicle system	ウイルスに感染した媒体を車両に接続する
18.3	Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)	例えば（直接的または間接的に）車両パラメータを改ざんするなどの攻撃を容易化するために、診断アクセス（例：OBDポートのドングル）が利用される								

High level and sub-level descriptions of vulnerability/ threat					Example of vulnerability or attack method		
4.3.6 Threats to vehicle data/code	車両データ/コードへの脅威	19	Extraction of vehicle data/code	車両データ/コードの抽出	19.1	Extraction of copyright or proprietary software from vehicle systems (product piracy)	著作権または所有権のあるソフトウェアを車両システムから抽出する (製品の著作権侵害)
					19.2	Unauthorized access to the owner's privacy information such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.	個人 ID、支払いアカウント情報、アドレス帳情報、位置情報、車両の電子 ID など、所有者のプライバシー情報へ不正にアクセスする
					19.3	Extraction of cryptographic keys	暗号鍵を不正に取り出す
4.3.6 Threats to vehicle data/code	車両データ/コードへの脅威	20	Manipulation of vehicle data/code	車両データ/コードの改ざん	20.1	Illegal/unauthorized changes to vehicle's electronic ID	車両の電子 ID を違法/不正に変更する
					20.2	Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend	ID 詐称。例えば、通行料金徴収システム、製造業者のバックエンドと通信する際に、ユーザーが他の ID を表示させたい場合。
					20.3	Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)	監視システムを回避する行動 (例: ODR トラッカーデータや実行回数のようなメッセージのハッキング/改ざん/ブロック)
					20.4	Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc.)	車両の運転データを偽るためにデータを改ざんする (例: 走行距離、車速、走行方向等)
					20.5	Unauthorized changes to system diagnostic data	システム診断データを不正に変更する
		21	Erasure of data/code	データ/コードの消去	21.1	Unauthorized deletion/manipulation of system event logs	システムイベントログの不正な削除/改ざん
		22	Introduction of malware	マルウェアの導入	22.2	Introduce malicious software or malicious software activity	悪意のあるソフトウェアまたは悪意のあるソフトウェアアクティビティを導入する
		23	Introduction of new software or overwrite existing software	新しいソフトウェアの導入または既存のソフトウェアの上書き	23.1	Fabrication of software of the vehicle control system or information system	車両制御システムまたは情報システムのソフトウェアの偽造
		24	Disruption of systems or operations	システムまたは操作の途絶	24.1	Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging	DoS 攻撃。例えば、大量のメッセージが送りつけられた結果、CAN バスのあふれ、または ECU に障害が発生することによって、引き起こされる可能性がある

High level and sub-level descriptions of vulnerability/ threat					Example of vulnerability or attack method		
4.3.6 Threats to vehicle data/code	車両データ/コードへの脅威	25	Manipulation of vehicle parameters	車両パラメータの改ざん	25.1	Unauthorized access of falsify the configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc.	ブレーキデータやエアバッグ展開しきい値など、車両の主要機能の設定パラメータを改ざんするために不正にアクセスする
					25.2	Unauthorized access of falsify the charging parameters, such as charging voltage, charging power, battery temperature, etc.	充電電圧、充電電力、バッテリー温度などの充電パラメータを偽装するために不正にアクセスする
4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened	十分な保護または堅牢化されていない場合に悪用される可能性がある潜在的な脆弱性	26	Cryptographic technologies can be compromised or are insufficiently applied	暗号技術が危殆化または不十分に適用される可能性がある	26.1	Combination of short encryption keys and long period of validity enables attacker to break encryption	暗号鍵が短く、長期間鍵の更新を行わないという状況の組み合わせにより、攻撃者は暗号を破ることができる
					26.2	Insufficient use of cryptographic algorithms to protect sensitive systems	機密性の高いシステムを保護する際に不十分な暗号アルゴリズムを利用する
					26.3	Using already or soon to be deprecated cryptographic algorithms	すでにまたは間もなく非推奨となる暗号アルゴリズムを使用する
		27	Parts or supplies could be compromised to permit vehicles to be attacked	部品または供給品が危殆化されて車両が攻撃される可能性がある	27.1	Hardware or software, engineered to enable an attack or fails to meet design criteria to stop an attack	攻撃が可能となるように設計された、または攻撃を停止するための設計基準を満たしていないハードウェアまたはソフトウェア
		28	Software or hardware development permits vulnerabilities	ソフトウェアまたはハードウェアの開発が、脆弱性を許容する	28.1	Software bugs. The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present	ソフトウェアバグ。ソフトウェアバグの存在は、悪用可能な潜在的脆弱性の根拠になり得る。これはとりわけ、既知の悪いコード/バグが存在しないことを検証し、かつ未知の悪いコード/バグの存在のリスクを減らすためのテストを、ソフトウェアに対し実施していない場合に当てはまる。
					28.2	Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, ...) can permit access to ECUs or permit attackers to gain higher privileges	開発の残り（例：デバッグポート、JTAG ポート、マイクロプロセッサ、開発証明書、開発者パスワード・・・）を利用すると、ECU へのアクセスが可能となる、または、攻撃者がより高い特権を取得することが可能となる。

High level and sub-level descriptions of vulnerability/ threat					Example of vulnerability or attack method		
4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened	十分な保護または堅牢化されていない場合に悪用される可能性がある潜在的な脆弱性	29	Network design introduces vulnerabilities	ネットワーク設計が脆弱性をもたらす	29.1	Superfluous internet ports left open, providing access to network systems	不要なインターネットポートが開放されており、ネットワークシステムへのアクセスが可能となる。
					29.2	Circumvent network separation to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages	ネットワーク分離を回避し、制御を奪取する。具体例は、任意の CAN バスメッセージの送信などの悪意のある行為をするため、保護を回避して他のネットワークセグメントへのアクセスを取得するために、保護されていないゲートウェイまたはアクセスポイント（トラック-トレーラーゲートウェイなど）を使用することである。
		31	Unintended transfer of data can occur	意図しないデータ転送が発生する可能性がある	31.1	Information breach. Personal data may be leaked when the car changes user (e.g. is sold or is used as hire vehicle with new hirers)	情報漏えい。車両のユーザ変更の際にパーソナルデータが漏えいする可能性がある（例：車両が販売されたり、もしくは新たな人に使用されたときなど）
		32	Physical manipulation of systems can enable an attack	システムの物理的改ざんが攻撃を可能にする可能性がある	32.1	Manipulation of electronic hardware, e.g. unauthorized electronic hardware added to a vehicle to enable "man-in-the-middle" attack	電子ハードウェアの不正操作。例：中間者攻撃を可能にするために車両に不正な電子ハードウェアを追加するなど。
						Replacement of authorized electronic hardware (e.g., sensors) with unauthorized electronic hardware	正規の電子ハードウェア（例：センサ）を不正な電子ハードウェアと交換する。
						Manipulation of the information collected by a sensor (for example, using a magnet to tamper with the Hall effect sensor connected to the gearbox)	センサーが収集した情報の改ざん（例：ギアボックスに接続されたホールセンサーを改ざんするために磁石を使用する）