UN-R155 Annex 5 チェックシート

UN REGULATION R155
Annex 5 : List of threats and corresponding mitigation
附則5：脅威リストと対応軽減策

背景

R155の車両型式認証の要件に、「リスクアセスメントは、 附則5のパートAに記載のある全ての脅威および関連リスクを考慮しなければならない」とあります。また、「この脅威に対する適切なリスク軽減策を実装しなければならない。この軽減策の実装にはパートB、Cの軽減策を含めなければならない」とあります。

このことから、パートB、Cのリスク軽減策は実装されなければなりませんが、その軽減策は曖昧なものが多く、車両メーカーの判断にゆだねられています。そこで、パートBおよびCをより理解しやすくしたものがこのチェックシートです。

仕様方法

チェックシートは、下記の構成になっています。左から軽減策までは規則書と同じ内容ですが、その後の列には、脅威の軽減策に対応する「ISO/SAE 21434要求」および「他の規格の要求」を示しています（該当する場合）。さらに「テュフ ラインランド ジャパン推奨」の列では、リスク軽減策を裏付ける最小限の証拠（作業成果物）を記述しています。

注）本資料は、現時点で有効と思われる内容をまとめたものです。

脅威 ID	脅威	軽減策 ID	軽減策	ISO/SAE 21434	他の規格	テュフ ラインランド ジャパン推奨

一例として以下の2つの内容について開示しています。
附則5 パートB「車両に対する意図的な脅威の軽減策」
　　表B6「十分に防御し堅固でないと起きうる潜在的脆弱性」
附則5 パートC「車両外部での脅威の軽減策」
　　表C1「バックエンドサーバーに対する脅威への軽減策」

www.tuv.com

TÜVRheinland®
Precisely Right.

Manufacturer:

Date:

表B6　「十分に防御し堅固なものにしておかないと起こりうる潜在的脆弱性」への軽減策

脅威 ID	脅威	軽減策 ID	軽減策	ISO/SAE 21434	他の規格	テュフ ラインランド ジャパン推奨
26.1	短い暗号鍵の組合せや、長期の有効性により攻撃者が暗号を破りやすくなる。	M23	ソフトウェアとハードウェアの開発時にサイバーセキュリティのベストプラクティスに従う。	RQ-08-12 RQ-09-05 RQ-09-07 RQ-09-08 RQ-09-09 RQ-09-10 RQ-10-01		▪ リスク対応策 ▪ TARA ▪ サイバーセキュリティ目標 ▪ サイバーセキュリティクレーム ▪ 検証報告書 ▪ サイバーセキュリティコンセプト
26.2	機密システムを防御するための暗号アルゴリズムの不十分な使用方法。					
26.3	既に、あるいは非奨励の暗号アルゴリズムを使用する。					
267.1	攻撃可能に設計された／攻撃を阻止する設計基準に準拠していないハードウェアやソフトウェア。					
28.1	ソフトウェアのバグ。ソフトウェアのバグの存在は潜在的脆弱性となる。ソフトウェアに既知の悪質なコードやバグがなく、未知の悪質なコードやバグが存在するリスクを減少させるような検証テストをしていない場合。	M23	ソフトウェアとハードウェアの開発時にサイバーセキュリティのベストプラクティスに従う。 十分なカバレッジのあるサイバーセキュリティテストをする。	RQ-08-12 RQ-09-05 RQ-09-07 RQ-09-08 RQ-09-09 RQ-09-10 RQ-10-01 RQ-10-10 RQ-10-18 RQ-11-01 RQ-11-03		▪ リスク対応策 ▪ TARA ▪ サイバーセキュリティ目標 ▪ サイバーセキュリティクレーム ▪ 検証報告書 ▪ サイバーセキュリティコンセプト ▪ 脆弱性分析報告書 ▪ 統合と検証報告書 ▪ 妥当性確認報告書 ▪ 新たな脆弱性と対応策
28.2	開発残滓（例：デバックポート、JTAG ポート、マイクロプロセッサー、開発証明、開発者パスワード等）を使用して ECU にアクセスしたり、攻撃者がより高い権限を取る。					
29.1	余分なインターネットポートがオープンのままで、ネットワークシステムへのアクセスが可能になる。					
29.2	ネットワーク分離を回避してコントロールを得る。非防衛ゲートウェイやアクセスポイント（トラックとレーラーゲートウェイ）を使用して防御を回避し、他のネットワークセグメントにアクセスして勝手な CAN バスメッセージを送付する。	M23	ソフトウェアとハードウェアの開発時にサイバーセキュリティのベストプラクティスに従う。 システム設計とシステム統合にサイバーセキュリティのベストプラクティスに従う。	RQ-08-12 RQ-09-05 RQ-09-07 RQ-09-08 RQ-09-09 RQ-09-10 RQ-10-01 RQ-08-01 RQ-08-02 RQ-08-04 RQ-08-06 RQ-08-08 RQ-08-09 RQ-08-10 RQ-08-11 RQ-08-12		▪ リスク対応策 ▪ TARA ▪ サイバーセキュリティ目標 ▪ サイバーセキュリティクレーム ▪ 検証報告書 ▪ サイバーセキュリティコンセプト ダメージシナリオ ▪ アセット定義 ▪ 影響評価 ▪ アタックパスの特定 ▪ アタック実現性評価 ▪ リスク値 ▪ リスク対応策

Manufacturer:　　Date:

表C1　「バックエンド・サーバー」に関する脅威への軽減策

脅威 ID	脅威	軽減策 ID	軽減策	ISO/SAE 21434	他の規格	テュフ ラインランド ジャパン推奨
1.1 & 3.1	スタッフによる特権の悪用。 例：インサイダー攻撃	M1	インサイダー攻撃のリスクを最小化するためにバックエンドシステムにセキュリティ制御が適用される。	該当無し	IEC62443-4-2 技術セキュリテイ要求 Annex B	表 B.　FR1 識別と認証制御にある CR1.1 から CR1.14 の検証報告書
1.2 & 3.3	サーバーへの不正なインターネットアクセス。 例：バックドア、パッチが当たっていないシステムソフトの脆弱性、SQL 攻撃やその他の方法によるもの	M2	不正アクセスを最小化するためバックエンドサーバーにセキュリティ制御を適用する。 例は OWASP[*1] を参照。	該当無し	OWASP[*1]	OWASP Top 10 検証報告書 ▪ インジェクション ▪ 認証の不備 ▪ 機密データの露出 ▪ XML 外部実体参照 ▪ アクセス制御の不備 ▪ 不適切なセキュリティ設定 ▪ クロスサイト・スクリプティング ▪ 安全でないデシリアライゼーション ▪ 既知の脆弱性を持つコンポーネントの使用 ▪ 不十分なロギングとモニタリング
1.3 & 3.4	サーバーへの不正な物理的アクセス。 例：USB スティック等をサーバーに挿す	M8	システムデザインとアクセスコントロールを通して、不正な者が個人やシステムデータにアクセスできないようにする。	該当無し	IEC62443-4-2 7.3 7.13	CR3.1 コミュニケーションの完全性の検証報告書 CR3.11 物理的な耐タンパー性と検出の検証報告書
2.1	バックエンドサーバーへの攻撃でその機能が停止。 例：車両とのやりとりや、車両が依存するサービスの提供が阻止される。	M3	バックエンドシステムにセキュリティコントロールを適用する。バックエンドサーバーがサービス提供に必須であれば、システムが停止した場合にリカバリーの方法があるべき。 例は OWASP を参照	該当無し	OWASP CLASP[*2] (Comprehensive, Lightweight Application Security Process)	上記 OWASP Top 10 検証報告書参照 CLASP 7 ベストプラクティスの検証報告書 ▪ 研究所の意識向上プログラム ▪ アプリケーション評価を実行 ▪ セキュリティ要件をキャプチャ ▪ 安全な開発プラクティスを実装 ▪ 脆弱性修復手順を構築する ▪ メトリックを定義および監視 ▪ 運用上のセキュリティガイドラインの公開
3.2	クラウド内情報の紛失。データがサードパーティのクラウドサービスプロバイダーにより保管されている場合、攻撃や事故により機密データが紛失する。	M4	クラウドコンピューティングに関連するリスクを最小化するセキュリティコントロールを適用する。 例は OWASP や NCSC クラウドコンピューティングを参照	該当無し	OWASP NCSC[*3] のクラウドセキュリティ原則	上記 OWASP Top 10 検証報告書参照 NCSC 14 の原則の検証報告書 ▪ 転送中のデータの保護 ▪ 資産の保護と回復力 ▪ 消費者間の分離 ▪ ガバナンスのフレームワーク ▪ 運用上のセキュリティ ▪ 人員のセキュリティ ▪ 安全な開発 ▪ サプライチェーンのセキュリティ ▪ 安全な消費者管理 ▪ ID と認証 ▪ 外部インターフェースの保護 ▪ 安全なサービス管理 ▪ 消費者への監査情報の提供 ▪ 消費者によるサービスの安全な使用
3.5	意図しないデータの共有による情報侵害。 例：管理者エラー	M5	データ侵害を避けるためのバックエンドシステムへのセキュリティコントロールを適用する。 例は OWASP を参照	該当無し	OWASP	上記 OWASP Top 10 検証報告書参照

*1: OWASP: Open Web Application Security Project　https://owasp.org/www-chapter-japan/
*2: CLASP: Comprehensive, Lightweight Application Security Process
CLASP 7 best practice (P7)　https://owasp.org/www-pdf-archive//Us_owasp-clasp-v12-for-print-lulu.pdf
*3: NCSC: National Cyber Security Centre's　14 Cloud Security Principles: https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles

テュフ ラインランド ジャパン株式会社
カスタマーサービス
info@jpn.tuv.com
東日本地域Tel: 045-470-1850
西日本地域Tel: 06-6355-5400

横浜市港北区新横浜 3-19-5
新横浜第二センタービル
Tel. 045-470-1860 Fax 045-473-5221

www.tuv.com

TÜVRheinland®
Precisely Right.