

TISAX(Trusted Information Security Assessment Exchange)

ドイツの自動車産業のための情報セキュリティ評価

自動車のサプライチェーンにおける保護可能な情報の確保



TISAX(Trusted Information Security Assessment Exchange)は、自動車のサプライチェーン全体の中で適切なレベルの情報セキュリティを評価するために、ドイツの自動車メーカーがサプライヤーに対して内部情報セキュリティ監査を行う仕組みのことです。TISAXはVDA（ドイツ自動車工業会：情報セキュリティ基準を発行）とENX（European automotive network exchange : TISAXの登録、及びTISAX監査サービスプロバイダの登録や認定書のためのプラットフォームを提供）を通じてドイツの自動車業界に徐々に拡大し、サプライヤーの情報セキュリティ能力を評価するための共通の評価・交換メカニズムを確立してきました。TISAXとそれに対応する情報セキュリティ評価は2017年に導入され、ドイツの自動車サプライヤーに義務化されました。自動車サプライヤー（部品、コンポーネント、サービスなどを提供）は、情報セキュリティマネジメントシステム（ISMS）を導入・維持し、その後、OEMとのさらなる契約および/またはドイツの自動車市場への参入のために、対応するレベルのTISAX監査に合格しなければなりません。

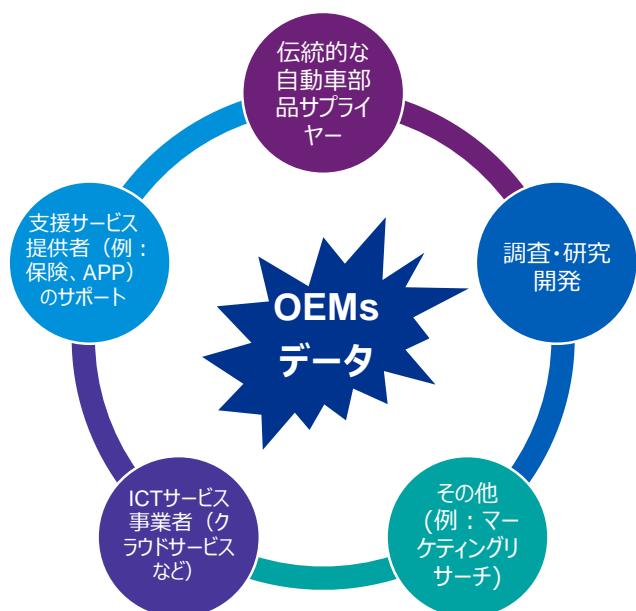
KPMGドイツ（KPMG AG監査法人）は、ENX認定TISAX監査サービスプロバイダとして、専門的な監査経験を有し、世界的に高い評価を得ています。KPMG中国は、当社のグローバルなサイバーサービス基準と内部のTISAX監査プロセスを厳格に遵守し、中国のクライアントにワンストップサービスを提供しています。ドイツと中国のKPMG TISAX専門家の相互チームワークにより、コミュニケーションコスト、監査サイクルを最小限に抑え、TISAX認定書の取得を含む監査プロセス全体を効率的に遂行します。また、クライアントのニーズに応じてカスタマイズされたサービスも提供いたします。

伝統的なサプライヤー → より広いビジネスパートナー

TISAXプロセスの参加者は、一般的には、中国国内及び多国籍企業の伝統的な部品及び/又は部品メーカーです。TISAX審査の対象となる拠点は、R&Dセンター、本社、事務所、研究所、生産工場、試験所などです。

自動車自身がより環境にやさしくデジタル化されたものへと進化していく中で、新エネルギー自動車、モバイルインターネット、自律走行の分野の企業とそれに対応する技術研究開発や関連サービスも自動車のサプライチェーンに欠かせないものとなってきています。さらに多くの有名な巨大テクノロジー企業や革新的なスタートアップ企業がTISAX認定の取得に動いています。

さらに、市場調査や顧客中心のサービス（調査会社のようなもの）に従事する企業や、それをサポートするICTサービス（システム運用、メールサービス、クラウドサービスなどを含む）を提供する企業も、OEM顧客や自動車の顧客に有効なTISAX認定書を提示する必要があります。



TISAX(Trusted Information Security Assessment Exchange)

ドイツの自動車産業のための情報セキュリティ評価

TISAX の流れ : 登録 → 監査 → 緩和→ 確認 → 報告書→ シエア

TISAXの要求事項によると、参加者はまず、OEM側から事前に定義されたスコープ（場所や評価対象を含む）をENXプラットフォームに登録する必要があります。KPMGは、第三者監査機関として、事前に定義されたスコープに基づいて評価を実施し、署名付きのTISAX監査報告書を発行し、ENXプラットフォームにアップロードします。参加者は、サプライヤーがOEMからの発注、プロジェクト協力、システムアカウント、サプライヤー資格更新を申請するための必要条件として、TISAX認定書（ラベルと呼ばれる。3年間有効）を取得することになります。



TISAX評価の目的、レベル、成熟度のスコアリング

ISO/IEC 27001及び27002に基づく情報セキュリティに加えて、TISAXの監査では、プロトタイプの保護、第三者との接続、データ保護の3つの評価目標が含まれている場合があります。サプライヤーが取得、処理、保存する情報の感度に応じて、保護の必要性は、高い（AL2）または非常に高い（AL3）になる可能性があります。AL3、プロトタイプの保護を伴うAL2、または第三者との接続を伴うAL2では、必ず実地監査が必要となります。これらの監査には、面接、実地検査、証拠確認などの伝統的な監査手順が含まれます。

監査結果は、成熟度レベルで表現され、VDA ISAの成熟度レベルの方法論に厳密に従っています。各管理について、0から5までの成熟度レベル（「該当しない」が適用される場合もあります）が審査員によって評価されます。TISAXラベルは、不適合のない一定の成熟度レベルを要求しています（受審企業は、特定の期間内に審査員によるフォローアップ審査で評価される所見や要求事項からの逸脱に基づいて、適時に是正措置を取らなければなりません）。



Wolf von Waldhausen
Head of TISAX, Cyber Security
KPMG Germany



Richard Zhang
Head of TISAX, Cyber Security
KPMG China



高部 一郎 Ichiro Takabe
Head of GJP: Global Japanese Practice
KPMG China

gjpmarkets.china@kpmg.com