公益社団法人自動車技術会

1. 講座名	脅威分析ツールを活用した効率的な脅威分析演習
2. 講座概要	本講座では、車載ネットワークのコンセプトフェーズにおける脅威分析の効率化をテーマとします。従来のDFD＋STRIDEによる手作業の脅威抽出に加え、脅威分析支援ツールを活用することで、より多くの脅威シナリオを短時間で抽出し、リスク評価や対策検討までの流れを体験します。 特に、保護資産に着目したDFD作成から、ツールによる脅威シナリオの自動抽出、ISO/SAE 21434に基づくリスク評価、攻撃経路の分解と対策検討までを一連の演習として実施します。 本講座は、脅威分析の実践方法を学びたい方や、効率的な分析手法を検討中の方に適しています。
3. 想定する受講者	・自動車メーカー・部品サプライヤのセキュリティ担当者（新任含む） ・IoTベンダ等で自動車業界の脅威分析手法に関心のある方
4. 習得する技術	・DFDを用いた脅威分析の基本手法 ・脅威分析支援ツールによる脅威シナリオの効率的抽出 ・ISO/SAE 21434ベースのリスク評価 ・公知情報を活用したセキュリティ対策検討
5. 受講の前提条件	ECU、CAN、TCP/IP等の基礎知識
6. 日数（時間数）	1日（6時間）
7. 最大受講人数	20名
8. セミナー講師	倉内 伸和（パナソニック アドバンストテクノロジー株式会社）
9. 受講者の制限	特になし
10. 実習機材	・Microsoft Excelのインストールされ たWindows PCをご用意ください。 ・同PCにEnterprise Architect 64ビット版、Java 64ビット版（推奨:Microsoft build on OpenJDK Java17以降）を事前インストールしておいて下さい(ライセンスをお持ちの方のみ)。 ・Enterprise Architectをご用意いただける方は、当日に弊社製脅威シナリオ自動生成ツール【Threat Scenario Detector】をインストールしていただき、演習でご使用いただきます。 ・演習ではグループ内でファイル共有が必要となります。USBメモリ等をご持参ください。
11. 到達目標	・DFDの各要素に対する脅威抽出手法の理解 ・ツールを用いた脅威シナリオの効率的な抽出手法の理解 ・攻撃パターンに着目した体系的なリスク評価手法の理解 ・公知情報を用いたセキュリティ対策の選定
12. 講座計画	【座学】 ・セキュリティ バイ デザイン概論 【演習】 ・保護資産に着目したDFD作成 ・DFD＋STRIDEによる脅威抽出(手作業) ・脅威分析支援ツールによる脅威抽出(自動) ・ISO/SAE 21434ベースのリスク評価 ・攻撃経路への分解とセキュリティ対策検討
13. 開催時期	2026年6月8日（月）10：00～17：00