

1. 講座名	ソフトウェア開発の各段階におけるセキュリティ強化に有効な手段と自動化の方法
2. 講座概要	本講座では自動車業界をとりまくセキュリティトレンド、規格・ガイドラインを踏まえ、オートモーティブ・ソフトウェア開発ライフサイクルの各ステップでセキュリティを向上させるための取り組みについて紹介します。特に、ソフトウェア開発の早期段階での脆弱性発見と自動化にフォーカスし、静的解析ツールを用いたバグの検出、オープンソースソフトウェアに含まれる既知の脆弱性の特定、ファジングによる未知の脆弱性の発見といった手法について解説します。
3. 想定する受講者	自動車業界の技術部門・開発部門等の担当者およびマネージャー(特に自動車部品のサプライヤー、自動車メーカーの担当者)
4. 習得する技術	<ul style="list-style-type: none"> <li>・ソフトウェア開発プロセスにおいてセキュリティを向上させる方法</li> <li>・ソフトウェアの開発段階における脆弱性の検出と、その自動化</li> </ul>
5. 受講の前提条件	<ul style="list-style-type: none"> <li>・ソフトウェア開発やセキュリティの基礎的な用語を理解していること</li> </ul>
6. 日数(時間数)	1日(計6時間)
7. 最大受講人数	30名
8. セミナー講師	日本シノプシス合同会社 岡 デニス 健五
9. 受講者の制限	日本シノプシスの競合関係にあたる企業は受講をお断りする場合があります。
10. 実習機材	なし
11. 到達目標	ソフトウェア開発ライフサイクルの各ステップでのセキュリティ強化において、どの様なツールによりどの様な脆弱性が検出できるか、またその自動化の利点と方法について理解する。
12. 講座計画	<ul style="list-style-type: none"> <li>・自動車業界を取り巻く現状：サイバーセキュリティのトレンド、規格・ガイドラインの解説</li> <li>・オートモーティブ・ソフトウェア開発ライフサイクルにおけるセキュリティ</li> <li>・コネクテッドカーの対する脅威・リスクとソリューション</li> <li>・オートモーティブ攻撃の事例の解析</li> <li>・ソースコードの静的解析 - MISRAの事例</li> <li>・オープンソースソフトウェアのリスク - 解析結果</li> <li>・ファジングによるソフトウェア製品の脆弱性検出要件定義と、環境構築、テスト自動化の要点</li> <li>・量産後の自動車セキュリティ：脆弱性管理、インシデントレスポンス、OTAアップデート</li> </ul>