車両サイバーセキュリティの未来（3）

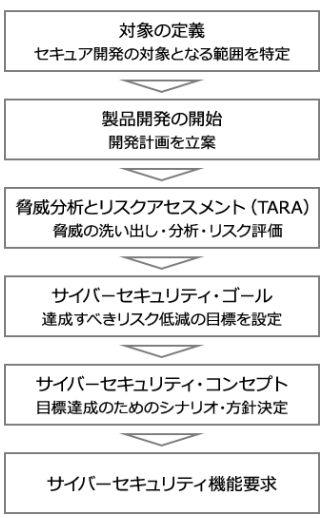
車両開発における脅威分析とリスクアセスメント

PwC コンサルティング合同会社　マネージャー 奥山 謙
PwC コンサルティング合同会社　アソシエイト 亀井 啓

コンセプトフェーズ概要

前回は、車両サイバーセキュリティ確保の基本的なアプローチがリスク管理（最小化）の取り組みであることを紹介しました。一方で全てのリスクをゼロにすることは現実的ではないため、限りあるセキュリティ対策のリソースを適切に分配し、製品ライフサイクルの各活動を通じて、十分なレベルまでリスクを低減する必要があります。そのためにはリスクを網羅的に把握した上で、各リスクの重大度に応じた対応レベルを定め、優先順位をつけて対策しなくてはなりません。第3回は製品ライフサイクル全体を通じたリスク管理活動の起点となる、コンセプトフェーズにおける「脅威分析とリスクマネジメント（TARA：Threat Analysis and Risk Assessment）」について考察します。

車両開発のコンセプトフェーズにおける主な業務は、図1の通りです。 図1.コンセプトフェーズ



具体的な活動内容については、車両の機能安全規格ISO26262*1に沿った現状の開発業務での経験から多くのヒントを得られます。一方、中でもセキュリティ特有の取り組みとなるのが、「TARA」です。

脅威分析とリスクアセスメント（TARA）

TARAは、コンセプトフェーズで実施するリスク管理のための一連の活動を指し、「資産の洗い出し」、「脅威の洗い出し」、「リスクアセスメント」の三つの工程で実施されます。

資産の洗い出し

はじめに、開発対象のユースケースや、参照可能な情報に基づいてシステム構造を整理し、守るべき情報資産・機能資産をリストアップします。

具体的な設計検討前のコンセプトフェーズでは、資産や、資産がどこに保持されるか未定のケースも珍しくありません。例えば、車両に電子決済機能を持たせる場合、決済に必要なクレジットカード情報が車両とバックエンドサーバーのどちらに保存されるのか、またその情報がより機密度の高いカード会員データなのかそれともトークン化した情報なのかといった未確定要素については、何らかの仮定を置いて分析を進める必要がでてきます。

こうした点は設計上具体化すべきポイントとして明確化し、後続フェーズでフォローアップしていく必要があります。また、前提の絞り込みには前工程の「対象の定義」で十分に技術上、制度上の制約を織り込むことも有効です。

このようにコンセプトフェーズの業務では、限られた前提条件や情報に基づいて分析を進める技術が必要となってきます。

脅威の洗い出し

洗い出した各資産に対し、起こり得るセキュリティ上の脅威を特定します。その上で必要に応じて各脅威の顕在化条件についても分析、整理します。悪意の第三者を考慮するセキュリティにおいては、実際の攻撃者（ハッカー）のアプローチや手法に関する専門性が必要になります。こうした属人性の高い作業の均質性確保や、洗い出した脅威の網羅性を一定レベルで担保するための構造的アプローチとして、各団体が提案する脅威分析手法があります。ただし、現状統一された手法は確立されていないため、各組織は製品の特性や開発現場の実情に適した手法を選択、または組み合わせて活用していく必要があります。例えば、詳細設計に依存しないようにSTRIDE*2脅威分類などを用いて脅威を洗い出し、より詳細な顕在化条件の分析には脅威の具体的な攻撃手段や可能性をツリー状に図表化するアタックツリーを用いるといったことができます。

リスクアセスメント

各脅威に対して、共通の評価基準からリスクレベルを算定し、算定結果に基づいて対策（リスク低減）の優先度を決定します。評価基準には、リスクが実現した際の影響度や発生可能性といった従来のITセキュリティの指標を活用できますが、自動車のセキュリティでは「安全（safety）」への影響にも考慮が必要です。

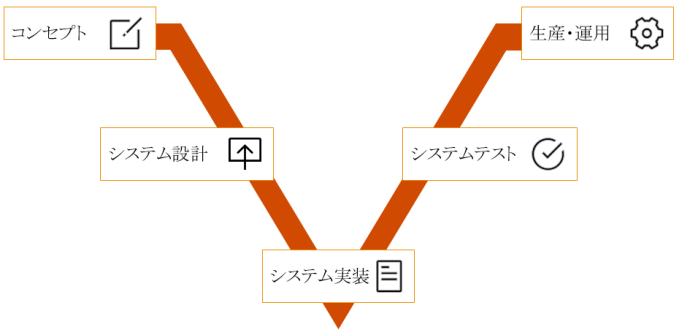
例えば、図2に示す通り、影響度と発生可能性のマトリクスに基づいた4段階のリスクレベルを設定しつつも、「安全」を脅かすリスクについては発生可能性の値に関わらずレベル4を与える、といった考え方です。逆にITセキュリティのみの観点では重大なリスクでも、物理的に作用する機能安全の機構により容易にリスクを回避・制御でき、実際の影響度はそれほど高くないといったケースも出てきます。このような場合は、機能安全における制御難易度（controllability）といった観点での考慮が必要になります。

図2.リスクレベル（4段階）算定表の例

	発生可能性（Exposure）			
影響度（Severity）		低い	中程度	高い
	非常に小さい	1	1	2
	小さい	1	2	3
	中程度	2	3	4
	大きい	3	4	4
	非常に大きい（安全に影響）	4	4	4

さらに現在策定中の自動車向けサイバーセキュリティ規格ISO/SAE21434では、製品ライフサイクル全体を通じたリスクマネジメントの単位としてCAL（Cybersecurity Assurance Level）の導入が検討されています。CALは機能安全規格ISO26262におけるASIL（Automotive Safety Integrity Level：安全性要求レベル）に相当する分類で、セキュリティ上の達成目標を複数段階で定め、そのレベルに応じて目標達成に必要な設計、実装または運用上の対策が施されます。組織は、CALで定めた達成目標が製品ライフサイクルの各工程を通じて最終的に達成されるよう管理する必要があります。

TARAの成果は、その後の製品開発フェーズにおけるリスク分析・管理の活動に引き継がれます。コンセプトフェーズにおいては、設計・実装が未定でリスクの顕在化条件や必要な対策を具体化できないケースがあります。これは、開発プロセスが進むにつれて明らかになるため、システム・ハードウェア・ソフトウェアの各開発フェーズにおいても繰り返しリスク分析を行い、リスクを管理していく必要があります。本連載では設計情報も踏まえた具体的な攻撃成立条件としての「脆弱性」に係るリスク分析をTARAと分けるために、「脆弱性分析」と呼びます。この活動の内容については次回考察します。



*1：ISO26262は自動車用の機能安全規格。自動車開発における安全設計のガイドラインとして、自動車メーカーや車載機器サプライヤーなどは準拠する必要がある。
*2：STRIDEは脅威を識別するための分類手法の一つ。Spoofing（なりすまし）、Tampering（改ざん）、Repudiation（否認）、Information Disclosure（情報漏えい）、Denial of Service（サービス拒否）、Elevation of Privilege（権限昇格）の六つの分類を用いて、脅威を洗い出す。

参考文献：
・Status of Work in Process on ISO/SAE 21434 Automotive Cybersecurity Standard
・SAE International. “SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems” 2016

お問い合わせ
PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel：03-6250-1200（代表）　Mail：jp_cyber_inquiry@pwc.com