車両サイバーセキュリティの未来（6）

車両開発におけるセキュリティテスト

PwC コンサルティング合同会社　ディレクター 村上　純一

目的別のセキュリティテスト分類

前回までは、実装段階に発生する脆弱性に対する施策として「セキュアコーディング」について紹介しました。今回は、実装された車両/車載製品に対するテスト段階での施策である「セキュリティテスト」について紹介します。

セキュリティテストは、大きく脆弱性診断とペネトレーションテストの二つの概念を含みます。

脆弱性診断

前回までに紹介したとおりセキュリティに関する取り組みは、コンセプトフェーズ、開発フェーズ、実装フェーズごとに行われ、各フェーズにおいて脅威分析の実施とその結果に基づいたセキュア設計、セキュアコーディングなどが行われます。このように、上流工程において想定された脅威への対策が想定どおり適切に実施されているか否かを確認するテストが、脆弱性診断になります。脆弱性診断は、前述の性質上、事前に想定脅威とその対策が明確であるためチェックリストなどを作成することが可能であり、その網羅性についても一定の説明をすることが可能です。

ペネトレーションテスト

一方、ペネトレーションテストは攻撃による達成目標を定め、その目標を達成するために攻撃（評価）を行うテストになります。ペネトレーションテストは性質上、網羅性を求めるものではなく、例えば「特定のECU（Electronic Control Unit）上で任意コードを実行する」などの目的を達成できるか、できない場合はどこまで目標に迫れたか、目標を達成できない理由・原因はなにかを明らかにすることが目的となります。ペネトレーションテストは上流工程でのさまざまな取り組みを考慮せずに実施するため、上流工程で想定していなかった脅威、すなわち上流工程での検討漏れを明らかにする効果が期待できます。別の言い方をするとペネトレーションテストで実施する各テスト項目は、脆弱性診断に含まれる項目である可能性もあります。

これは、世の中の攻撃者が製造企業のセキュリティ対策とは無関係に、目標達成に向けてあらゆる手段を講じてくる状況と同一であり、攻撃者目線で評価を行うことを意味します。

図表1に示すように脆弱性診断とペネトレーションテストではその思想が異なり、一方が他方を包含するというものではありません。全ての製品に対して全てのセキュリティテストを実施することはコスト的に現実的ではないため、実施に当たっては、製品モデル、類似モデルとの機能差分などに基づいて対象を選定することが重要です。

図表1：脆弱性診断とペネトレーションテストの概要

	目的	メリット	デメリット
脆弱性診断	上流工程で想定した脅威に関する対策の充足状況を確認する。	一定の網羅性を説明することができる。	上流工程で想定していなかった脅威、対策を検討してなかった脅威への対策状況を評価できない。
ペネトレーションテスト	達成目標を設定し、目標が達成できるかどうか、できない場合はその理由・原因を明らかにする。	上流工程で想定していなかった脅威に対する評価を行うことができる。上流工程での検討結果自体の評価を行うことができる。	網羅性を説明することは難しい。各テスト項目は、脆弱性診断と重複する可能性がある。

テスト対象別のセキュリティテスト観点

脆弱性診断、ペネトレーションテストともにテスト対象、アプローチとしてHW（ハードウェア）に対するテストとSW（ソフトウェア）に対するテストが考えられます。

HW（ハードウェア）を対象としたセキュリティテスト

HWに対するテストは、いくつかのレベルがあり、一つには製品が提供している標準的な外部インターフェースに対するテストが考えられます。例えば、イーサネットポート（LANポート）、Wi-Fi、Bluetoothなどのネットワークの接続インターフェース、USBポートなどの外部デバイスの接続インターフェース、CD/DVDなどのメディア入力、筐体（きょうたい）に設置されているボタンなどが想定されます。こうしたインターフェースは、利用者が標準的に利用できるものであり、また、マニュアルなどに利用方法が記載されているため最もテストがしやすい一方、内部仕様が分からない場合は無意味なテストを行ってしまう可能性もあり、効果的なテストが難しい領域です。

次に考えられる項目としては、筐体の分解などを行い、内部のプリント基板などを対象とした調査・分析が考えられます。例えば、利用している各種チップの種類・用途、シルク印刷の有無・内容、デバッグポートの有無、出荷前のピン利用の痕跡の調査・分析などが挙げられます。

こうした調査・分析は製品仕様の推定を行う上で有益であり、また、デバッグポートなどを発見・特定できた場合、それ自体が大きなリスクであると同時に開発者向けの内部情報にアクセスできるため後続のテストを行う上でも有益であると言えます。また、こうした分析の結果、通信機能を有するファームが格納されたチップを特定できた場合、当該チップからファームウェアの抽出ができるか、抽出したファームウェアの分析ができるか、というテストも考えられます。

SW（ソフトウェア）を対象としたセキュリティテスト

SWに対するテストもHWに対するテストと同様、いくつかのレベルがあり、最も基本的なテストは利用者に提供されているユーザーインターフェース（UI）を操作し、セキュリティ機能のバイパスやセキュリティ上問題のある操作ができないか確認することが挙げられます。また、ネットワークへの接続インターフェースが提供されていた場合、不要なサービスが起動していないか、実行されているソフトウェアに既知の脆弱性が存在しないかの確認、脆弱性が存在した場合は実際に攻撃を行い、攻略可能か確認するといった内容が考えられます。

こうしたテストに関しても内部仕様を把握せずに外部からテストする場合、やみくもなテストとなり、効果的なテストが難しくなる可能性があります。そのため、HWに対するテストにおいて抽出したファームウェアを分析し、内部仕様を明らかにした上でSWのテストを行うなどの方法も想定されます。図表2にHWテストとSWテストの内容例をまとめています。

セキュア開発ライフサイクル全体におけるセキュリティテストの位置づけ

こうしたさまざまなテストが脆弱性診断として実施すべき項目か、ペネトレーションテストとして実施すべき項目かは上流工程でどこまでどのような脅威を想定し、その対策をどの程度、どのように組み込んだかに依存します。別の言い方をすると上流工程で想定された脅威への対策の充足状況は脆弱性診断として実施することが可能であり、そもそもの想定の充足性・妥当性を確認するために行うことがペネトレーションテストと言えます。

このようにセキュリティテストは、テストフェーズのみで実施方針、内容を検討するのではなく開発プロセス全体の取り組みを踏まえて策定することが重要です。次回は、実際に自動車を製造する工場におけるセキュリティの取り組みについて紹介します。

図表2：HWテストとSWテストの内容例

HWテストの内容例	SWテストの内容例
・外部インターフェースに対する操作、異常入力の挿入 ・筐体の分解、プリント基板上の情報の分析 （使用チップ・用途、シルク印刷、デバッグポートなど） ・チップの取り外し、ファームウェアの抽出、など	・ユーザーインターフェース（UI）の操作 ・ネットワーク経由でのスキャン、脆弱性診断 ・ファームウェア解析 ・脆弱性に対する攻撃の実施

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