別紙

■本書で紹介する脆弱性検査

脆弱性検査は、検査対象や検出できる脆弱性によって様々な技術や手法が存在しており、主に以下に挙げる 5 つの検査からなります。また、その検査をソフトウェアライフサイクルのどのフェーズ（開発／運用）で実施するかが異なっており、その一覧を表 1 に示します。

- **ソースコードセキュリティ検査**

  ソースコードセキュリティ検査はその名の通り、PC 向けソフトウェア、組み込みソフトウェアやウェブアプリケーションのソースコードを対象に脆弱性を検出する検査です。

- **ファジングによる検査**

  ファジングによる検査は、PC 向けソフトウェア、組み込みソフトウェアなどに対して脆弱性を発現させやすいデータやファイルを送り込む検査です。バイナリー形式（実行形式）のソフトウェアを対象に検査でき、未知の脆弱性も発見できる可能性があります。

- **システムセキュリティ検査**

  システムセキュリティ検査は、システムや組込み機器を構成するソフトウェアにおける既知の脆弱性の有無を点検する検査です。この検査は開発フェーズで実施する場合や、運用フェーズでシステム公開後に発見された脆弱性を検査する場合にも活用されます。

- **ウェブアプリケーションセキュリティ検査**

  ウェブアプリケーションセキュリティ検査は、ウェブサイトを実現するためのソフトウェアを検査します。脆弱性を検出するためのリクエストをウェブアプリケーションに送ること等で実施され、主に既知の脆弱性が検査対象です。この検査は、サービス提供前のテスト段階での実施と、運用フェーズで発見された新たな脆弱性の検査としても実施されます。

- **ペネトレーションテスト**

  ペネトレーションテストは、他の脆弱性検査と目的が異なります。組織のサーバーやネットワークシステムに対して攻撃者が実際にどこまで侵入できるのか、何ができるのか、という点に着目して検査を行います。そのため、運用上のシステムに残存している既知の脆弱性を狙ったり、設計段階での不備を突いたりして実施します。

表 1　：脆弱性検査の実施フェーズと主な検査対象

検査名	実施フェーズ		主な検査対象
	開発	運用	
ソースコードセキュリティ検査	○	－	PC 向けソフトウェア 組み込みソフトウェア ウェブアプリケーション
ファジングによる検査	○	－	PC 向けソフトウェア 組み込みソフトウェア
システムセキュリティ検査	○	○	クライアント・サーバー （ネットワークシステム） 組み込みソフトウェア
ウェブアプリケーションセキュリティ検査	○	○	ウェブアプリケーション
ペネトレーションテスト	－	○	サーバー 組み込みソフトウェア