視点

情報セキュリティとソフトウェア工学

NRIセキュアテクノロジーズ
代表取締役社長
小田島（おだしま）　潤（じゅん）

筆者が小学生の頃に、マイコンブームというものがあった。日本電気製のPC-6001やシャープ製のMZ-2000が発売され、その上で動作するゲームで遊ぶことが流行したのである。筆者も近所の電気店に入り浸りでゲームに夢中になっていたが、何とか両親を説得して安価なマイコンを手に入れた。その後、マイコンはパーソナルコンピュータ（PC）と呼ばれるようになった。

当初は、雑誌に掲載されたBASIC言語のソースコードを打ち込んでゲームで遊んでいたが、そのうち飽き足りなくなり、自分でプログラムを書くようになった。その過程で、プログラミングという作業の面白さと苦労を身をもって知ると同時に、「どうしたらバグのないプログラムを書けるのか」ということに興味を持った。構造化プログラミングやプログラムの書き方に関する書籍を読みあさる、変わった小学生であったが、中学校に入ると部活が忙しくなり、自然とPCからは離れていった。

大学進学の時は、何を学ぼうかと迷った末に情報工学を選んだ。専攻過程に進む時にはソフトウェア工学を選んだ。ソフトウェア工学とは、品質の高いソフトウェアをいかに効率的に開発するかを考えることである。計算機アーキテクチャー、人工知能（AI）など人気のある研究室が多くあったなかで、選ぶ人の少ないソフトウェア工学をあえて専攻することにしたのは、プログラムのバグに苦しんだ筆者の原体験があったからだ。研究室では、コンピュータ支援ソフトウェア工学（Computer Aided Software Engineering：CASE）や、形式手法（ソフトウェアの仕様記述やモデルの検証を数学的に厳密に行う手法）が主な研究テーマであった。

就職先についてもいろいろと迷った末に、野村総合研究所（NRI）を選んだ。「金融機関やメーカーとは違い、システムの開発と運用が本業であり、ハードウェアもOS（基本ソフト）も開発しているわけではないNRIなら、アプリケーションソフトウェアの開発生産性が競争力の源泉ではないか。それならば、大学で学んだことが生かせるのではないか」と考えたためである。

残念ながら、ソフトウェア工学や開発生産性に直接関わる仕事に就くことはあまりなかったが、最近、IoT（Internet of Things）や制御システムのセキュリティの重要性が叫ばれ、システムの設計段階からセキュリティを作り込む「セキュリティ・バイ・デザイン」が提唱されるなかで、そこにソフトウェア工学の成果を生かせるのではないかと考え

るようになった。

情報システムやIT製品のセキュリティに関する国際標準規格にISO/IEC 15408がある。「Common Criteria for Information Technology Security Evaluation」と呼ばれ、略して「Common Criteria」や「CC」と言われることも多い。このISO/IEC 15408では、識別と認証、利用者データ保護などのセキュリティ機能が詳細に列挙されており、開発するシステムや製品で必要と思われる機能を選択すればセキュリティ対策が網羅されるようになっている。また、設計時に選択したセキュリティ機能がシステムや製品に正しく実装されているかを検証して保証する、評価保証レベル（EAL）が定められており、より下流の工程で検証するほど保証レベルが高くなる。例えば、概要設計レベルでの機能テストで検証されるとEAL1、ソースコードレベルで検証されるとEAL4となる。EAL4は、商用のIT製品や情報システムで求められる最高のレベルである。

IoTや制御システムの場合は、一般的な情報システムとは異なり、ファイアウオールなどのセキュリティ機構を後から組み込むことが難しいため、上流の設計段階からセキュリティを組み込むことが重要になる。制御システムのセキュリティに関する国際標準規格にはIEC 62443があり、機能安全に関するIEC 61508（電気・電子）やISO 26262（自動車）にも今後はセキュリティの観点が取り込まれる可能性がある。情報システムでもEAL5以上を目指そうとすると形式手法による仕様記述と検証が必要となるのと同様に、制御システムでも上位レベルの機能安全の認証に形式手法による検証・保証を求める動きがある。自動車のような人命を左右する制御システムやソフトウェアの開発においては、多少コストがかかっても形式手法を適用すべきだということである。

最近よく聞かれる「ビジネスIT」もソフトウェア工学と無縁ではない。基幹業務システムのような「コーポレートIT」では、時間とコストをかけてでも品質の高いシステムを構築しようとするのに対して、顧客体験を重視する「ビジネスIT」では、新しい機能を開発してはリリースすることを繰り返す「DevOps」（開発と運用の一体化）と呼ばれる手法が一般的である。しかし、だからと言ってセキュリティが犠牲にされていいはずはなく、最近では「DevOps」でセキュリティを担保する「DevSecOps」という概念が登場している。

「DevSecOps」には、実装・単体テストに相当するソースコード脆弱性診断や、総合テストに相当する外部アプリケーション診断などを自動的に行える統合開発環境が必要である。「DevOps」では開発成果物として残されることが少ない各種の設計書をソースコードから自動生成する機能も必要になる。これを含めて、統合開発環境の実現にはCASEツール研究の成果が生かせるのである。

情報セキュリティは、一見するとソフトウェア工学とは無縁のようでいて、実はそうではない。それどころか、これからのセキュリティ業界で違いを生み出す鍵はソフトウェア工学にあると筆者は考えている。 ■