



セキュリティバイデザイン —モデリングとプロセス技術の活用—

情報システム学部 情報セキュリティ学科
日下部 茂 教授

ソフトウェアは、期待通りに動作させるという意味ではそれほど“ソフト”ではなく、その開発プロジェクトは“ハード”な建築物のプロジェクトに例えられることもあります。いきあたりばったりで大規模な建築物を構築するのが不可能なように、いきあたりばったりで大規模で複雑なソフトウェアを開発することはできないのです。

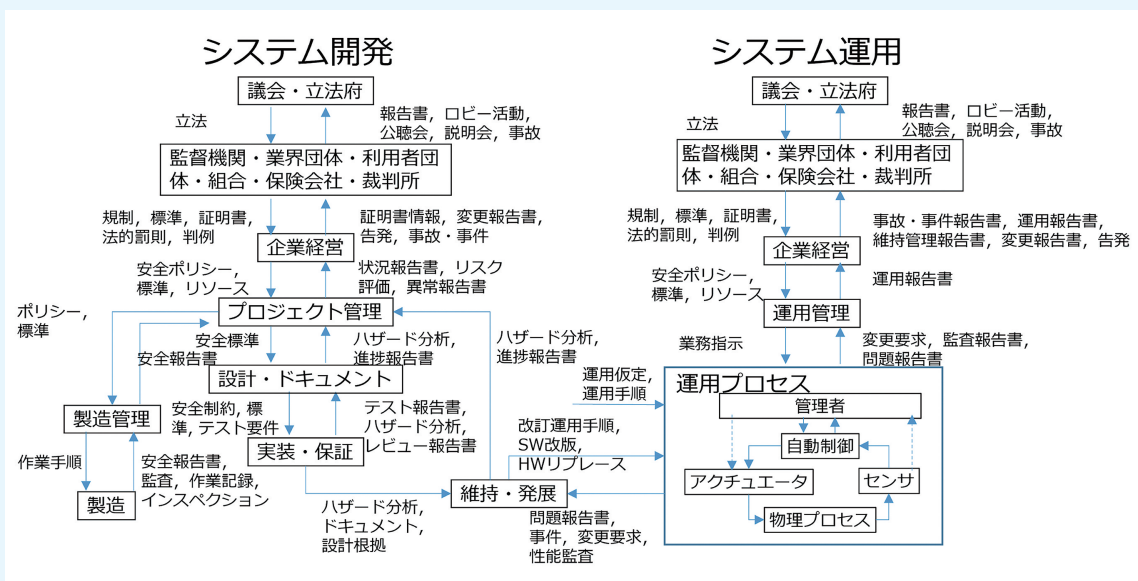
大規模なソフトウェアの開発では、将来にわたる利用法や管理法まで見据えて、構想段階から適切な検討を行い、必要な仕様を明らかにし、実現の仕組みを設計、具現化して構築します。また、その各段階で適切な確認を行い必要なら修正も行います。このような手順を決めるにも専門知識が必要で、詳細は開発対象の特性によって異なります。このように考えると、大規模・複雑なソフトウェアはそれ自身に加え、その開発手順（開発プロセスと呼びます）も必要に応じて開発・改良される高度な人工物といえます。

ここでテーマとするセキュリティバイデザインは、システムを開発・導入して運用を始めた後に、後付け的に

セキュリティ対策をするのではなく、上流工程からセキュリティ対策を行うよう改良した開発プロセスを用いることでサイバーセキュリティを確保しようとするものです。

現代のソフトウェアシステムは社会技術システムに組み込まれ、その開発運用には様々な利害関係者が関わっています（図参照）。そのようなシステムのセキュリティ上の脅威には、人的脅威、技術的脅威、物理的脅威があります。予備知識も異なる様々な利害関係者がこのような脅威について分析しながらセキュリティバイデザインを実践するには、必要な確認が可能な程度に厳密だけれども、特別な専門知識なしで読解可能な表現や実践可能な分析技術が必要とします。

このような背景の下、ソフトウェア向けのモデリング技術に加え、システムエンジニアリングやレジリエンスエンジニアリングのモデリング手法も用いて、技術的側面に加え人や組織の側面も分析できるようなセキュリティバイデザインの研究を行っています。



(図:社会技術システムの開発と運用、N. G. Leveson, “Engineering a Safer World”, MIT Press, 2011 の図4.4がベース)