MESSAGE

デジタルトランスフォーメーションに重要なセキュリティ戦略

野村総合研究所（NRI）執行役員
NRI セキュアテクノロジーズ代表取締役社長
小田島　潤

昨今、デジタルトランスフォーメーション（DX）が業種を問わず日本企業の喫緊の経営課題になっているのであるが、現実問題として取り組みの遅れは明らかである。NRIセキュアテクノロジーズ（NRIセキュア）が、米国・シンガポール・日本３カ国の企業におけるDXへの対応状況を調査したところ、米国・シンガポールでは約86％が「対応している」と回答したのに対し、日本企業は約31％にとどまった。

さらに深刻なことは、DXに取り組んでいる日本の先進的なユーザー企業の中核事業やサービスで、最近、金銭的被害や個人情報の漏洩につながった事案が発生したことである。DXにおいても、あらためてセキュリティの重要性や「怖さ」を認識した経営者も多いだろう。そこで本稿では、DXの文脈で特に重要な２つのセキュリティ戦略について述べてみたい。

従来のシステム開発は、その工程を「要件定義」「方式設計」「基本設計」などと明確に定義し、各工程の品質基準をクリアしていくことで、「水が上から下に流れ落ちるがごとく」大規模で高品質なシステムを構築する「ウォーターフォール型」が一般的であった。しかし、これでは素早い顧客ニーズの変化や、情報技術の進歩に追随できない。DXの実現に必要なのは、ユーザー企業の開発者と運用者が比較的小規模（「２枚のピザを分け合える」人数）のチームを組成し、優先的な機能から数週間単位で開発とリリースを繰り返す「アジャイル開発」または「DevOps」と呼ばれる手法である。

ウォーターフォール型のシステム開発では、開発工程の終盤、すなわち総合テストやユーザー受け入れテスト（UAT）の段階で、攻撃者

の目線からシステムの弱点を探る「脆弱性診断」によって、セキュリティの担保を行うのが一般的であった。しかし、この考え方をそのままアジャイル開発やDevOpsの世界に持ち込むには無理がある。脆弱性診断は診断の実施から報告書作成まで最短でも１週間は必要である。改修の時間を含めると、数週間のサイクルで開発とリリースを繰り返すアジャイル開発において、この遅れは致命的である。そこで、アジャイル開発の環境に自動的なセキュリティ検査機能などを埋め込み、プログラムのバグと同様にセキュリティの不備を検出し、開発者に修正を促す「DevSecOps」が提唱されている。

一方、非常に高い品質が求められる金融システムや、自動車の電子制御ユニット（ECU）などに組み込まれるソフトウエアの開発は、今後もウォーターフォール型で行われるであろう。脆弱性診断は、基本的に「ブラックボックステスト」であり、既知の攻撃手法に対して一定の耐性があることはいえるが、システムの仕様が本質的にセキュアであるとは言明できない。外部システムと連携する要件も増えており、「要件定義」や「方式設計」などの上流工程において、セキュリティを意識した設計・開発がますます重要になっている。その成果物である、設計書やソースコードに対するセキュリティ観点のチェックは「ホワイトボックステスト」に相当する。システム設計や開発に関する高度な知識や経験も必要となるため、実施できる専門家はそう多くないが、DevSecOpsも含めて「上流工程でのセキュリティ担保」こそが、DXにおける一つ目のセキュリティ戦略である。

DXの実現に向けて、AWSやAzureなどのクラウドサービスと、スマートフォンに代表されるモバイルデバイスを積極活用しない選択肢はあり得ない。従来、信頼できる社内と信頼できない社外（インターネット）の境界を、ファイアウォールなどのセキュリティ機器で守る「境界防御」がセキュリティの基本モデルであった。しかし、このクラウドとモバイル全盛の時代に、その「境界」が消失してしまった。そこで登場したのが「ゼロトラストモデル」である。

ゼロトラストモデルにおいては、通信相手を正しく認証し、相手と自分の置かれた状況に応じて、許可する処理や対象を動的に決定（認可）する。オンラインバンキングで普段とは異なる場所や端末からログインが行われた場合、追加でワンタイムパスワードの入力を求めるとか、登録済みの振込先以外には資金移動させないことが一例である。IDとパスワードによる認証だけでは、ゼロトラスト時代に通用しないことは明らかであり、生体認証や所有物認証を組み合わせた、多要素かつ継続的な認証が必要である。このように、ゼロトラストモデルを踏まえて、設計段階でしっかりと「認証と認可」を検討することが、DXの二つ目のセキュリティ戦略である。

上記以外にも、自社固有のIT環境（オンプレミス）と複数のクラウドから成る「マルチクラウド」におけるセキュリティや、ビジネス活用事例も出てきた「ブロックチェーン」のセキュリティも、DXの実現に向けては避けて通れない話題である。経営者は自らがセキュリティの専門家である必要はない。しかし、セキュリティを「自分事」として、主体的に関与する姿勢が求められる。　（おだしまじゅん）