企業情報システムのセキュリティ対策は設計・開発段階から～「未然防止」対策の重要性

企業システムのセキュリティ対策の不備は、意図しない情報流出や、サイバー攻撃による事件に巻き込まれる危険性を孕む。情報漏洩を起こした企業が払う代償は、「未然防止」のためのセキュリティ対策投資の比にならない。

大手医療保険会社のシステムセキュリティ対策不備の代償

米大手医療保険会社WellPoint社は、データベースのセキュリティ対策の不備により、2009年～2010年に60万人以上の個人情報を漏洩した。データベースには、保険加入者の氏名、社会保障番号、医療情報等のセンシティブ情報が格納されており、米保健福祉省[1]は、同社が医療保険の携行性と責任に関する法律[2]に違反したとして170万ドル（約1.6億円）の罰金の支払いを命じた[3]。

セキュリティ専門組織のSANS[4]は本事件について、「罰金170万ドルは多額に感じられるが、60万人への対応費用は2,000万ドル（約19億円）を超えるだろう。セキュリティ対策を少しばかり講じたところですべての問題を防げるわけではないが、『未然防止のための対策コスト』は、事故被害総額の20%にも満たないのでは？」としている。

システムに作り込まれた脆弱性の修正や情報漏洩のコスト

システムの開発時に作りこまれてしまった、情報漏洩のリスクとなり得る脆弱性を、運用開始後に発見・修正するには多大なコストがかかる。上流工程である設計段階からセキュリティを意識した対策を行っていた場合に比べ、運用後になってセキュリティ対策を実施しなければならなくなった場合の総セキュリティ対策費は60～100倍にも跳ね上がると試算されている[5]。そして、ひとたび情報漏洩事故が発生すると、原因となった脆弱性の修正費用に加え、セキュリティ専門家費用、弁護士費用、裁判費用、被害者への損害賠償費用が必要となる。また、

図表1　2012年上半期 個人情報漏洩インシデント 概要

漏洩人数	123万9626人
インシデント件数	954件
想定損害賠償総額	347億9,865万円
一件当たりの平均漏洩人数	1349人
一件当たり平均損害賠償額	3,787万円
一人当たり平均損害賠償額	5万7,710円

（出所）2012年情報セキュリティインシデントに関する調査報告書【上半期 速報版】

企業の信用失墜による機会損失等、間接的な被害も含めると、その総コストは莫大なものになる。こうした情報漏洩事故は、国内でも数多く起きている。JNSA[6]の調査によると、2012年上半期に発生した国内の情報漏洩事故の一件当たりの平均漏洩人数は1349名、平均損害賠償額は一件当たり3,787万円に上る（図表1）。

システム運用開始後の脆弱性修正や情報漏洩事故による企業の負担は大きい。これを「未然防止」すれば、セキュリティ対策投資の削減と費用対効果を高めることが可能になる。それが、システム開発の上流工程（すなわち設計段階）から行うセキュリティ対策である。

システムに脆弱性が組み込まれる理由と「未然防止」の方法

情報漏洩のリスクとなるセキュリティ上の問題がシステムに作り込まれる原因をまず考えてみてほしい。それは、システム開発を「委託する側の問題」と「受託する側（開発側）の問題」の2種類に大別できる。

「委託側」の問題とは、複数のシステムを統一された基準で委託できず、暗黙のうちに「受託側」の能力や善意に委ねてしまうケースが多いことである。「委託側」にセキュリティ要件の仕様がないため基準を示すことができず、「受託側」の自主点検を信頼するしかない。さらに、完成したシステムを受け入れる際、セキュリティ要

NOTE

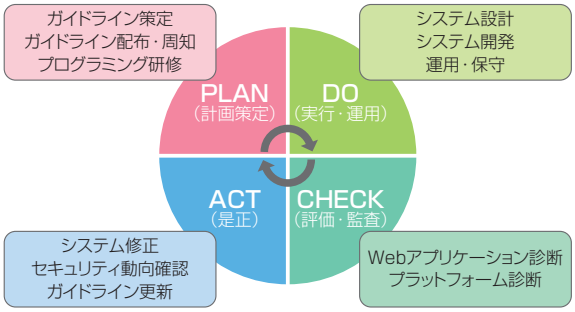
1) U.S. Department of Health & Human Services
2) Health Insurance Portability and Accountability Act（HIPPA）
3) 出所：U.S. Department of Health & Human Services　2013年7月11日付ニュースリリース（http://www.hhs.gov/news/press/2013pres/07/20130711b.html）
4) SANS Institute：政府や企業・団体間における研究、およびそれらに所属する人々のITセキュリティ教育を目的として1989年に設立された界トップレベルのセキュリティ研究・教育機関（本部：米国メリーランド州）（http://www.sans.org/）
5) 出所：Kevin Soo Hoo, "Tangible ROI through Secure Software Engineering" Security Business Quarterly, Vol.1, No.2, Fourth Quarter, 2001
6) 特定非営利活動法人日本ネットワークセキュリティ協会（http://www.jnsa.org/）
7) NRIセキュアでは、「セキュア設計・開発ガイドライン策定支援」等、企業の情報システムセキュリティの維持・向上を支援するサービスや、ガイドラインを深く理解するための研修「Webアプリケーションセキュリティ：1-DAY ハンズオン」も提供している。
・セキュリティ診断（脆弱性診断）/設計開発支援（http://www.nri-secure.co.jp/service/assessment/index.html）
・Webアプリケーションセキュリティ：1-DAY ハンズオン（http://www.nri-secure.co.jp/service/learning/original3.html）

件の確認方法が明確でなければ、後日、「受託側」に起因する問題が発覚しても、ほとんどの場合委託側の責任において追加の修正費用を支払わなければならなくなる。

一方、「受託側」の問題は様々である。たとえば、要件定義時にセキュリティ要件が欠落しているケース、設計段階での検討不足により根本的な再検討が必要となるケース、実装時の取り決めがなかったために脆弱性を作り込んでしまうケースなど、その多くは事前に考慮されていれば発生しない問題である。前述のWellPoint社の場合、オンラインデータベースに適切なセキュリティ対策が施されておらず、60万人の個人情報がインターネット上で長期に渡り誰もが閲覧可能な状態だった。また他の企業では、上流工程でアプリケーションに脆弱性が組み込まれ、その結果、SQLインジェクションによりクレジットカード情報や機密情報が窃取された例や、基盤の設定においてミドルウェアにパッチを充てないまま放置していたため、システムに外部から侵入された事例がある。

こうしたシステム的なセキュリティ上の問題点を作り込まないために、システム開発における基準や、運用開始前のテスト基準を明文化し、「委託側」と「受託側」の両者が未然に防ぐ努力をすることが必要である。事前に定められた基準（ガイドライン）に基づいた開発を行い、それに沿った開発が行われているかを確認し、問題点が見つかったら修正した上で運用を開始する。また、最新のセキュリティ動向も確認し、必要に応じて基準の更新も行っていかなければならない（図表2）。これは非常に骨の折れる作業であり、かつ高度なセキュリティ知識が求められる。筆者が実際にガイドライン策定に携わった企業では、ガイドラインを策定、告知し、実際に現場で運用するまでに平均2〜3年を要している。設

図表2　セキュリティ対策のためのPDCAサイクル



（出所）NRIセキュアテクノロジーズ

計・開発ガイドラインの策定やシステムのセキュリティ診断などを、常に最新のセキュリティ情報を持っているセキュリティ専業ベンダーに委託することも選択肢として考えられるだろう[7]。

今こそ「未然防止」の取り組みを

企業にとって情報漏洩事件・事故は、事業の存続にまで影響を与えかねない、重要な経営課題である。これを未然に防ぐためには、システム的セキュリティ対策を上流工程からしっかりと行い、それを運用・開発する担当者のセキュリティ意識を高めることが必要だ。重大な情報漏洩事故を未然に防止すべく、組織内のセキュリティ文化を醸成していく必要がある。企業を取り巻く脅威は、年々増加する一方である。今こそ、「未然防止」の取り組みの一歩を踏み出していかなければならない。

Writer's Profile
上田 健吾 Kengo Ueda
NRIセキュアテクノロジーズ　テクニカルコンサルティング部
主任セキュリティコンサルタント
専門はサイバーセキュリティ
focus@nri.co.jp