

Webサイトのセキュリティの現状

岡 博文

2007年度の1年間に実施したセキュリティ診断（Webアプリケーション診断）では、Webサイトの41%に情報漏えいにつながる致命的な欠陥が発見されている。Webサイトに対する脅威やセキュリティ対策など、安全なWebサイトを構築するための情報は容易に得られるようになっているにもかかわらず、致命的な問題が高い割合で発見されているのは、企業が独力でWebサイトの安全性を確保することに限界があるからだと考えられる。このようなことから、安全性の高いWebサイトを構築するために、専門家によるセキュリティ診断が不可欠である。

増加するWebサイトへの不正アクセス

近年、Webアプリケーションソフトのぜい弱性を利用し、データの改ざんや個人情報の取得などを目的とする不正アクセス事件が増加してきている。特に2007年11月ごろからは、「SQLインジェクション（パラメーターにSQL文〈データベースへの問い合わせ〉を仕込んでデータベースを不正に操作する手法）」による危険度の高い攻撃が目立っている。

多くのWebサイトに潜む致命的な欠陥

NRIセキュアテクノロジーズでは、Webサイトのセキュリティ対策を支援するための「セキュリ

ティ診断サービス」を提供している。Webサイトを運営する企業から依頼を受け、潜在するセキュリティ上の問題を発見し、安全性を評価するサービスである。

2007年度に実施したセキュリティ診断サービスの結果を集計すると、不正な手段（Webサイトの管理者が通常想定しない手段）を用いることで、利用者の個人情報をはじめとする重要情報へのアクセスが可能になってしまう重大な欠陥を抱えたWebサイトが41%にものぼっている（図1）。

また、重要情報に不正にアクセスはできないものの、情報漏えいにつながる可能性のある問題が確認できたWebサイトも30%という割合であった。

2007年度に初めてセキュリティ診断を実施した企業（以下、初診企業）に限ると、54%の企業のWebサイトで、不正な手段による重要情報へのアクセスを可能にしてしまうという深刻な問題が見つまっている。2007年度以前にセキュリティ診断を実施したことのある企業でも、35%で同様の問題があったが、診断経験の有無による差も明らかといえる（図2）。

診断経験の有無と問題の状況とがどんな関係にあるかを、ぜい弱性の種類ごとに分析してみたのが図3である。SQLインジェクションに対するぜい弱性は、初診企業のWebサイトでは診断経験のある企業の2倍以上の高い割合で発見されていることがわかる。

実際には、初診企業でもSQLインジェクションに対して何も対策をしていないWebサイトは少数で、多くの場合、ある程度の対策は取られている。しかし、それが部分的な対策にとどまっているために、ぜい弱性を抱えた企業が多いという結果になっている。

SQLインジェクション攻撃の事例や対策方法は理解しつつも、対策をどこまでやればよいのかという判断が困難であるため、このような状況になっていると考えられ

る。

昨今は、Webサイトに対する脅威や対策方法などに関する情報は広く公開されており、企業が安全なWebサイトを構築するための情報は比較的容易に得られるようになっている。

しかし、すでに構築したWebサイトが最新の攻撃手法にも耐える堅牢性を確保できているかどうかを確認することは難しい。企業が独力でWebサイトのセキュリティ対策を進めるには限界があり、知らず知らずのうちに何らかのセキュリティ上の問題を抱えてしまうことや、それを見逃してしまうことは十分に起こりうる。

専門的なセキュリティ診断の必要

初診企業の半数以上のWebサイトで重要情報に不正にアクセスできてしまうことから、多くのWebサイトが情報漏えいの危険と隣り合わせの状況にあると考えられる。いったん不正アクセスによって情報漏えいなどの事件が発生すると、企業はその事後対応に追われ、Webサイトの復旧費用、取引先への謝罪、場合によっては損害賠償など、多くの損失を被ることになる。Webサイトの安全

図1 Webサイトのセキュリティ診断結果

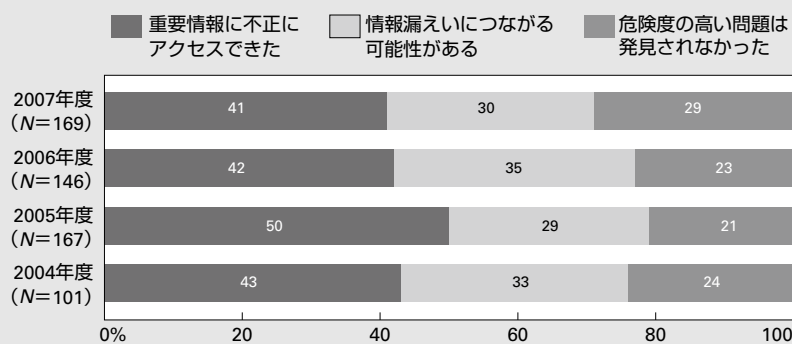


図2 診断経験別のセキュリティ診断結果

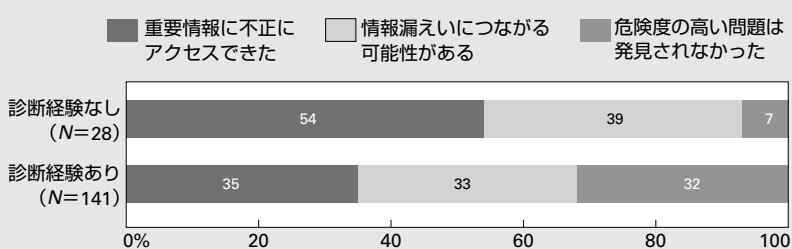
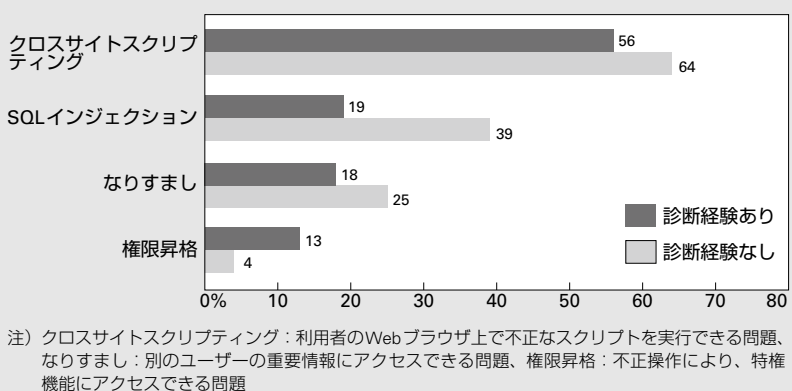


図3 主要なぜい弱性が発見された割合（診断経験別）



性を高めることは、もはやインターネットビジネスを展開するうえで不可欠な施策の一つである。まずはセキュリティ診断によって自社のぜい弱性の現状を正確に把握することから始めるべきである。

なお、本稿で述べた診断結果の詳細については、[http://www.nri-secure.co.jp/news/2008/](http://www.nri-secure.co.jp/news/2008/0728_report.html)

0728_report.htmlをご参照いただきたい。

『ITソリューションフロンティア』
2008年10月号より転載

岡 博文（おかひろふみ）
NRIセキュアテクノロジーズコンサルティング事業部主任セキュリティコンサルタント