

安全なWebサイト構築に必要不可欠なセキュリティ診断

鴨志田昭輝

NRIセキュアテクノロジーズによるセキュリティ診断では、2006年度1年間で42%のWebサイトに情報漏えいにつながる致命的な欠陥を発見している^{注1}。このことは、不正アクセスの手法が日々高度化する現在では、開発現場の努力だけでは安全なWebサイトを構築することが困難であることを示していると考えられる。こうした背景から、専門家によるセキュリティ診断は、安全なWebサイトの構築に必要不可欠となってきている。

なくなるWebサイトへの不正アクセス事件

Webサイトが不正アクセスによって被害を受ける事件が後を絶たない。

報道などで事件が公になったもののほか、外部には知らされないケースや、企業側が不正アクセスの事実気づいていないケースも決して少なくないと思われる。特に近年は、企業が独自に開発したWebアプリケーションのぜい弱性が狙われ、不正アクセス事件につながるケースが急増している。

Webサイトの安全性を評価するセキュリティ診断

こうした背景から、システムの安全性を評価するために外部のセキュリティ専門会社のセキュリティ診断を受ける企業が増えてい

る。

セキュリティ診断は、いわゆる「ハッカー」が行う不正アクセス（ハッキング）と同じ手法を用いて、システムの外側からセキュリティ上の問題点を探すことを主な目的としている。

NRIセキュアテクノロジーズでは、2006年度（2006年4月から1年間に146のWebサイトのセキュリティ診断（Webアプリケーション診断）を行った。すでに稼

動しているWebサイトだけでなく、最近では公開前に診断を実施するケースも増えてきている。

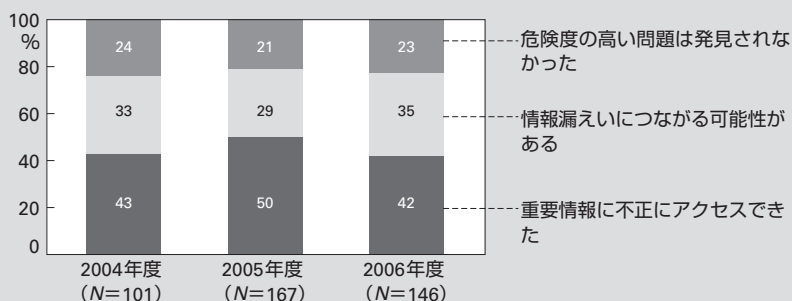
42%のWebサイトに致命的な欠陥

2006年度に実施したセキュリティ診断の結果を集計したところ、42%のWebサイトで、他の利用者の個人情報をはじめとする重要情報に不正にアクセスできる致命的な欠陥が確認された（図1）。

また、35%のWebサイトでは、重要情報に不正にアクセスできることは確認できなかったものの、情報漏えいにつながる危険のある問題点が発見された。

セキュリティ診断を行ったWebサイトを、運営主体の業種別にサンプル数の多い上位3業種（金融、情報通信、サービス）とそれ以外に分類したところ、高いセキュリティレベルが要求されるはず

図1 Webサイトのセキュリティ診断（年度別）



の金融機関のWebサイトにおいても、セキュリティ診断を実施すると多くの問題点が発見された(図2)。

インターネットバンキングのような金融機関のWebサイトは、金融自由化に伴って取り扱う金融商品の種類が増え、また、企業同士の提携や合併・吸収によってシステムの連携・統合が頻繁に行われるためにWebサイトが大規模になり、処理が複雑になることが多い。これが、セキュリティ対策の徹底を難しくしていると考えられる。

一方、セキュリティ診断の実施時期を見ると、金融機関と情報通信関連企業の場合、公開前のWebサイトに対するセキュリティ診断が多いことが理解できる(図3)。

このことから、金融機関では公開前のWebサイトのセキュリティ診断はすでに定着しており、インターネットに公開される時点では安全な状態になっているケースが多いと考えられる。

不十分なWebサイトのセキュリティ対策

NRIセキュアテクノロジーズが

図2 Webサイトのセキュリティ診断(業種別)

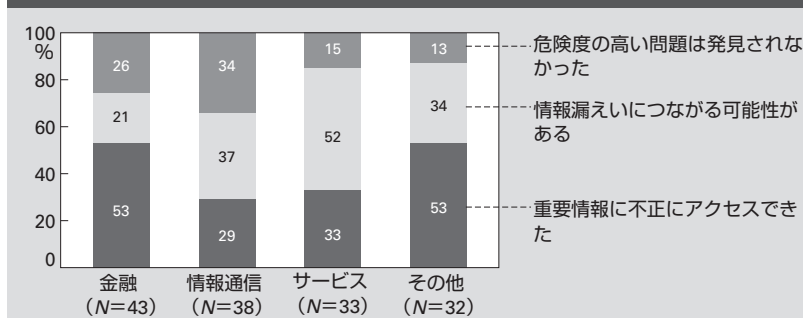
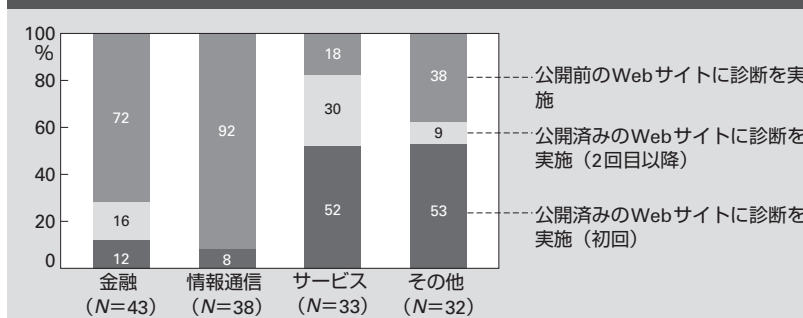


図3 セキュリティ診断の実施時期(業種別)



行ったアンケート調査によると、セキュリティ診断を実施している企業は全体のおよそ2割程度である注2。

高い確率で致命的な欠陥が発見された前述のセキュリティ診断の結果を踏まえると、いまだに多くのWebサイトがセキュリティ上の問題を抱えながら運営されていると推測される。そのことも、不正アクセス事件がいっこうにない理由の一つであろう。

注

- 1 詳細は、http://www.nri-secure.co.jp/news/2007/0619_report.html参照。
- 2 詳細は、http://www.nri-secure.co.jp/news/2006/0726_report.html参照。

『ITソリューションフロンティア』
2007年10月号より転載

.....
鴨志田昭輝(かもしだあきてる)
NRIセキュアテクノロジーズ(株) 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