

### ブラウザベース攻撃が次なるITセキュリティの脅威に

《Browser-based Attacks May Pose Next Big IT Security Nightmare Annual CompTIA survey identifies them as emerging threat [http://www.comptia.org/pressroom/get\\_news\\_item.asp?id=426](http://www.comptia.org/pressroom/get_news_item.asp?id=426)》

IT業界において、急増するブラウザベース攻撃が次なるセキュリティ脅威になる可能性がある - これはCompTIAの「ITセキュリティとワークフォース」に関する調査結果である。

約900の企業を対象に行われた同調査によると、36.8%が過去6ヶ月において、一度以上の「ブラウザベース攻撃」による被害を受けたと回答した。この数字は昨年より、25%の増加を示している。ブラウザベース攻撃とは、ブラウザシステム及びユーザのシステムパーミッションを使用し、コンピュータ機能を混乱させることである。こうした攻撃は、コンピュータの破壊や、プライバシーを脅かす目的で隠された悪質コードを含む、一見無害に見えるWebページを訪れることにより拡散される。また、その影響はブラウザの故障というレベルから、個人情報盗難や機密データの紛失といった深刻な問題へとつながる。

「Webページの急増により、企業のシステムは新たなセキュリティの脅威にさらされています。もはや、セキュリティ教育を一握りのITメンバーだけに限るべきではないのです。ITインフラストラクチャを安全に保つことは、企業全員の責任であるのです。」とCompTIA President、ジョン・A・ベネターは述べている。コンピュータウイルスとワーム攻撃は、いまだ大きな脅威といえるが、昨年と比べると、80%から68.6%へと、その頻度の低下が見られる。

また、昨年では頻度として2位にランクしていた「ネットワーク侵入」も65.1%から今年は39.9%へと低下。VPNやダイヤルアップ接続などの「ウイルスリモートアクセスによる問題」も昨年の49.9%から41.7%に減少。「ソーシャルエンジニアリング問題」も、21.9%から17.9%に低下した。

一方、セキュリティ強化対策としては、アンチウイルスのアプリケーションが最も一般的な措置であり、調査では、企業の95.5%がある種のアンチウイルス技術を導入していることがわかった。続いて、ファイヤーウォールやプロキシサーバーがランクインしているが、企業によるその導入率は昨年の93.7%から90.8%へ低下している。

セキュリティ監査および侵入検査は、一般的なセキュリティパフォーマンスをモニターする対策として増加を示しており、回答率は53%から61%へと上昇している。他の対策としては、システムのベースラインセキュリティ(46.5%から51.4%の増加)、チェンジ・コントロール・トラッキング(39.1%から44.3%の増加)がある。また、企業の15%が、セキュリティパフォーマンスの監視に必要な対策を何も行っていないと回答している。

この調査はCompTIAの委託によるTNS Prognostics (IT産業の今サルタンティングに基いた、カスタム調査会社)により実施された。

- CompTIA とは - <http://www.comptia.jp>

1980年初頭、EDIが様々な規格で利用され情報が飛び交う中、ISOやIEEEに対し標準化を提言するため、各社が集まる場として1982年にシカゴで設立。その後、欧米を中心とし9拠点を持つ非営利グローバルIT業界組織として、技術標準化の提言や各業務の業務保証となる実務能力基準の認定活動等を行っています。会員は、IT企業や各種団体、教育機関など89ヶ国16,000機関以上が参加しています(2003年12月現在)。尚、日本では、支局が平成13年4月に設立されています。

【お問い合わせ先】

CompTIA 日本支局 <http://www.comptia.jp>

〒101-0061 東京都千代田区三崎町3-4-9 水道橋MSビル7F

TEL:03-5226-5345 FAX:03-5226-0970

E-Mail: [info\\_jp@comptia.org](mailto:info_jp@comptia.org)

担当: 広報