

セキュリティ分野における安全神話とその崩壊

--永遠のビギナー対策から標準化まで、穴だらけのセキュリティ？--

- セキュリティの第一歩はパスワードの設定に始まる「永遠のビギナー」対策だと言われる。実はその対極にあるセキュリティシステムおよびそれらの製品自体に脆弱性を抱えている。ブラウザやOS等の脆弱性がよく問題にされるが、それだけではない。無線LANにおけるWEPの脆弱性は周知のとおりであり、WPAにも脆弱性がないとは言えない。
- また、最近では認証局の運用における脆弱性が問題となっているが、根本的なSSL/TLSでの脆弱性も指摘され、脆弱性を超えた機能不全状態もまじかに迫っている。本講演ではこれらのいくつかのシステム上の問題点を上げ、その対策について議論する。

森井昌克