IT時事ネタキーワード「これが気になる！」（第148回）

世界規模でWindowsパソコンに突如インシデントが発生。原因は？

2024.08.27

日本時間7月19日午後1時以降、Windows パソコンが突然ブルースクリーンになり、再起動がループする「ブルースクリーン・オブ・デス（BSOD）」を引き起こす問題が発生し、世界各地で大きな混乱が発生した。特に被害を受けたのは、航空会社や医療機関、金融機関など。航空会社では予約システムなどの停止により、世界で3300便以上が欠航、銀行では一部の顧客が送金できないなどのトラブルが発生した。その他、スターバックスなど小売店でも決済や注文ができないなど、市民生活への影響も出た。

多くの企業のWindows パソコンに突然インシデント発生。原因は？

日本でも、航空会社やアミューズメント施設などで混乱が起きた。例えば、日本航空で一時、サイト上での航空券の予約や購入などのサービスが利用できなくなり、ジェットスター・ジャパンでは19日に国内・国際線で計28便が欠航した。また、ユニバーサル・スタジオ・ジャパンの園内店舗では、POSレジでの会計ができなくなった他、ローソンなどのコンビニで一部のプリペイドカードが購入できなくなるなどのトラブルが相次いだ。

原因は米CrowdStrike（クラウドストライク）社による、企業や公共機関向けクラウドベースの総合セキュリティソリューション「CrowdStrike Falcon」のドライバー・アップデートだという。CrowdStrike社は「Remediation and Guidance Hub:Falcon Content Update for Windows Hosts」などで、「WindowsホストのFalconコンテンツ更新で見つかった欠陥が原因」とコメントを発表し、修正プログラムを配布した。つまり、たった1つのアップデートファイルのミスが、ここまでの大騒動を引き起こしてしまったのだ。

これを受け、マイクロソフトは7月20日、公式ブログにおいて、CrowdStrike社がリリースしたソフトウエアアップデートでのインシデントについて、同社と協力してサポートを行う姿勢を明らかにした。ブログでは、「影響を受けたのは850万台のWindowsデバイスで、全Windowsマシンの1%未満であると推定。割合は小さいものの、経済や社会への影響や被害額は大きい」という旨を述べている。なお、CrowdStrike社によれば、7月25日時点で97%のパソコンが復旧しているという。

インシデント当日は、SNSなどでも「今日はブルースクリーンで対応に追われている」「ブルースクリーンで仕事にならない」などの投稿が数多くなされた。駅や空港、店舗などの掲示スクリーンやPOSシステムなどがブルースクリーン状態の写真も多く見られた。

原因はセキュリティソリューションのドライバー。近年はサイバー攻撃で業務ができない事態も頻発傾向に… 続きを読む