セキュリティ脅威を招く落とし穴（第2回）

セキュリティ対策は“感染前提”へ

2017.10.04

2017年5月、世界中に広がったランサムウエア「WannaCry」は、各地に甚大な被害をもたらした。英国では国民保険サービスのコンピューターが被害を受け、病院・医療機関は患者情報へアクセスできなくなり、手術や救急患者の受け入れキャンセルが相次いだ。日本でも、日立製作所のシステムがWannaCryに感染し、業務に大きな支障を来したという。強固なセキュリティ対策を施しているはずの国営サービスや大企業が、なぜマルウエアに感染したのか。

セキュリティ対策がなぜ効かないのか



「水と安全はタダ」といわれた日本でも、近年企業のセキュリティ意識は高くなる一方だ。これは中小企業も例外ではない。2017年5月に独立行政法人情報処理推進機構（IPA）が発表した「中小企業における情報セキュリティの実態と中小企業の情報セキュリティ対策ガイドライン」によると、コンピューターウイルスを「脅威と感じている」という小規模企業や中小企業は89.1％（同ガイドラインP4）。実際に「ウイルス対策ソフト・サービスの導入」を実行している企業は全体で80.4％（P6）と、マルウエアやウイルスに対する防御意識は高い。

それでも悪意あるプログラムによる被害は根絶できない。場合によっては今回のランサムウエアのように世界中に大きな爪痕を残してしまう。その最大の原因は、これまでのセキュリティ対策がほとんど「防御」を主軸にしてきたからだ。

防御頼みの対策には限界がある… 続きを読む