情報セキュリティ投資のゲーム分析
―シミュレーションによる最適投資額の決定の考察―

高藪学（東京学芸大学）

JUAS 企業 IT 動向調査によれば IT 投資への期待は自動化・効率化などから「戦略型 IT 投資」へと変化している。IT 投資は企業競争力や企業価値の源泉である一方、情報化が進展する一方で新たなリスクも生じている。不正アクセスやコンピュータ・ウィルス感染による企業情報システムへの攻撃による被害が生じ、こうした被害は企業イメージ悪化や企業価値の損失を生じさせている。

企業と情報セキュリティについて考えるとき、セキュリティ確保のための技術的側面だけではなく、セキュリティ維持確保のための企業活動として「情報セキュリティ投資」という観点がある。企業の投資行動という視点で情報セキュリティ維持活動を考察する場合には、企業の投資に関わる経済的動機づけが重要である。さらに、情報セキュリティ投資の最適な水準といった概念について考察が可能であろう。

特定の企業にクラッキングなどを行い情報セキュリティ侵害を引き起こすハッカー（クラッカー）の分布特性が企業の情報セキュリティ投資に与える影響についてのゲームモデルを構築し、分析を行なう。このことによって、企業の最適な情報セキュリティ投資水準決定に関わる要因とその影響が明らかになり、最適投資水準の決定に寄与するものと考える。

Cavusoglu(2008)の「企業–ハッカーモデル」をもとに、複数のハッカーの努力水準を分布として与える形で拡張し、モデルを構築した。このゲームモデルを用いて、ハッカーの努力水準の分布の性質が、企業情報セキュリティ投資行動に影響を与えることを考察した。