ＭＩＧＡコラム「世界診断」

2014 年 10 月 22 日

意外と大きい“ヒト”の要素

金 野 和 弘

明治大学研究･知財戦略機構 客員研究員
島根県立大学 総合政策学部 准教授

広島大学大学院社会科学研究科博士課程単位取得退学。独立行政法人科学技術振興機構常勤研究員、岡山学院大学専任講師、島根県立大学総合政策学部専任講師を経て、2013 年から現職。専門は情報経済論、情報政策論。最近は、経済学と心理学の境界領域である行動経済学の知見をとりいれた研究を進めている。

筆者が所属しているプロジェクトでは、情報ネットワークの脆弱性問題の解決に取り組んでいる。これまで定期的に研究会を開催し、多岐にわたる分野の専門家から貴重な情報の提供をいただき、有益な議論を行なってきた。そこで実感するのは、予想以上に“ヒト”の要素が大きく影響しているいということである。

情報セキュリティにとって技術が重要な役割を果すことは疑いないが、ヒトの側面もまた重要である。いくら技術的に堅牢さを確保したとしても、ヒトがセキュリティホールを作り出してしまっては意味がない。実際、ソーシャルエンジニアリング（social engineering）を代表例とする、利用者がパスワードの漏洩元となってしまった事件が数多く報告されている。これらは、人間的要素により情報セキュリティが脅かされた事案として捉えることができる。そのため、技術的側面を対象とする情報科学やインターネット工学などの分野ばかりでなく、人間的側面を対象とする心理学をはじめとする行動科学や、経済学などの社会科学の知見が今後より一層重要になってくることが予想される。

情報システムの脆弱性が引き起こす事案にはさまざまな種類がある。なかでも筆者が現在、関心を持って研究に取り組んでいるのは、情報セキュリティ投資がなされないために生じる諸問題である。本来なされるべき投資が行われない、もしくは過少となってしまうために生じる問題であり、これらはまさに人間的要素が関係するものである。以下では、この情報セキュリティに関する過少投資問題を中心に採り上げる。

自我関与度の低さが引き起こす問題

最近では、情報セキュリティが脅かされることによって引き起こされた事案（以下、「情報セキュリティ事案」と呼ぶ）が新聞紙上やニュース番組で目にすることは珍しくない。にもかかわらず、対策を講じようとしないのはなぜか。これに対する回答を用意するためのヒントとなるのが「自我関与度」という心理学の概念である。

世間では情報セキュリティ事案が生じているが、自分には関係ないと思って対策を怠ってしまう。この状態を、心理学の術語を用いて「情報セキュリティに対する自我関与度が低い」と表現できる。自我関与度の低さが情報システムの脆弱性を生み出す大きな要因の１つではないかと、筆者は考えている。

「自分ごと」として認識していない結果、そのことに対する注意が疎かになってしまったり、本来すべき対策を怠ってしまう。これは、情報セキュリティの分野に限らずさまざまな場面で見聞きし、場合によっては自分自身も経験することであろう。たとえば、飲酒運転をする、無灯火で自転車を運転するなどであり、これらは本来そうすべきでないにもかかわらず、どこかで「自分は大丈夫だ」という根拠のない自信から、注意や対策を怠ってしまうことがある。将来的なリスクを認識していながら、直近の発生可能性が実感できないために「他人ごと」として認識してしまうのである。

この自我関与度の低さは、情報セキュリティに対してもみられる。大学の講義の中で筆者が直近の情報セキュリティ事案について説明しても、自分のこととして事件を捉えている学生が少ないことを痛感する。筆者の説明の仕方に問題があるのかもしれないが、自分にも振りかかる可能性があるリスクとして認識し対策を採ろうという意識を持った学生は、残念ながらごく僅かである。その結果、危険なサイトに安易にアクセスしたり、パスワードを変更せずに使い続けたり、制作元の信頼性を確認せずにフリーソフトをインストールしたりする学生が未だに多い。

本来は、情報セキュリティ事案を自分ごととして認識し、適切な情報セキュリティ投資を行わなければならない。ここでいう投資とは経済学で扱う広義の投資であり、金銭的なものばかりではなく、時間の消費や手間を必要とする活動全般を指す。個人が行なう情報セキュリティ投資には、ウィルス対策ソフトをインストールする、対策ソフトのパターンファイルを常に最新のものに更新する、閲覧先のサイトの安全性を常に確認する、などが挙げられるが、自我関与度が低いとこれらの投資が疎かになり、その結果、自らがセキュリティ事案を生み出してしまう可能性がある。

個人ばかりではない自我関与度の低さ

自我関与度の低さが引き起こす問題は、個人ばかりではない。組織が情報セキュリティ投資を行なうか否かの判断にも影響を及ぼす場合がある。

近年では、組織が対象となった情報セキュリティ事案が巷を賑わせているにもかかわらず、いざ自社の情報セキュリティ投資をする場面になると、十分な投資がなされないことが多々ある。実

際、投資案件を起案する立場である情報担当者の口からこのような不満を耳にすることがしばしばある。では、なぜ十分な投資がなされないのか。

原因の１つとして挙げられるのは、経営者と情報担当者との間に存在する「情報の非対称性」である。これは、経営者が持つ情報システムに関する知識が情報担当者に比べて大幅に少ないことを指す。情報の非対称性が存在する結果、経営者が投資の重要性を理解できず、本来すべき水準の投資がされないという問題を引き起こす。このような情報の非対称性問題は経営学上、重要な問題の１つとなっており、非対称性を解消するための方策が検討・提案されている。

もう１つ大きな原因として挙げられるのが、情報セキュリティに対する経営者の自我関与度の低さである。他社が引き起こした事案を日々目にしているにもかかわらず、「自社は情報システム被害には遭わない」「事案を引き起こさない」「対策を採らなくても大丈夫だ」という認識を経営者が持っていることが少なくない。このような認識を持つ理由として、事象が必ず起こるとは限らず、あくまでも確率の問題として捉えがちである（つまり実際に起こる確率が低いと考えている）こと、そしてどれほど投資をし対策を講じたとしても損害をゼロにできる保証がないこと、などがあると推測される。いざ実現してしまうと甚大な被害が及ぼすにもかかわらず、リスクは実感が得られにくいために投資が後回しになってしまいがちである。その結果、リスクが実現し損害が生じたときにはじめて対処がなされ、対応が後追いになってしまう。

根拠なき自信が原因で情報セキュリティ投資が阻害されるのは問題である。それゆえ、経営者はもちろん、対策を採る組織全体の自我関与度を向上させることが必要であると筆者は考えている。

自我関与度に関する研究

現在、筆者は共同研究者とともに自我関与度の高低が情報セキュリティ投資に対して与える影響の調査を進めている。この関係を証明することができれば、自我関与度を向上させることで情報セキュリティ投資の過少問題を解決するための方策を検討することが可能となる。現在でも、情報教育の推進や講習会の開催などの形で情報セキュリティへの関心を高める努力がなされているが、自我関与度という概念を用いることでより詳細で的確な対策を検討することができるのではないかと筆者は考えている。

さらに、この自我関与度は国や地域によって傾向が異なることが予想される。まずは日本で調査をした後、他の国でも同様の調査を実施した上で国別比較を行ないたいと考えている。

自我関与度を高めるためには

情報セキュリティに対する自我関与度を向上させることは、個人、組織を問わず情報システムの脆弱性を解決・緩和するためには有効であろう。先に触れたように、そのための代表的な方策として情報教育の強化や講習会の開催が挙げられるが、それ以外の方策として情報セキュリティ監査

やCSIRT（サイバー攻撃に対応するための組織横断の専門チームのこと。詳しくは、山賀正人客員研究員のコラムを参照）の活用などが有効であると思われる。

一般的に、世間で重大事案が発生した直後にはそれを見聞きした者の自我関与度が上昇するが、時間の経過とともに低下する傾向がある。この持続性問題を解決するには自我関与度を高い水準に維持するための「仕組み」が必要であり、セキュリティ監査やCSIRTは有効な仕組みの1つとなるであろう。

国際的な知見の共有の必要性

情報社会のさらなる進展に伴い、情報セキュリティ事案が今後一層増加することに異論を挟む余地はないであろう。自我関与度の向上は、事案の発生を抑制し被害を軽減するための有効な一手段であると筆者は確信している。

インターネットの性質上、それを活用した情報ネットワークに対するセキュリティ政策は、国独自のものばかりでなく国境を跨いだものが必要となる。そのため、研究成果を共有した上で国際レベルと国家レベルからの多層的な対応が求められる。