情報セキュリティの意識と行動に関する調査

Survey on Consciousness and Behavior of Information Security

キーワード　インターネット、情報セキュリティ、情報ｾｷｭﾘﾃｨ･ﾏﾈｼﾞﾒﾝﾄ(ISM)、教育

１．調査の目的

本調査は、文部科学省「『情報セキュリティの社会技術』研究実施に関するフィージビリティ・スタディ」(研究リーダー　千葉大学文学部行動科学科教授　土屋　俊)における、「社会的ニーズの状況把握のための小規模実態調査」に位置づけられる。

情報セキュリティは大きな社会的要請となっており、様々な課題が指摘されているにも関わらず、その実態が明らかではなく、学術的裏付けも欠いている。このため、情報セキュリティを取り巻く意識と行動の実態について、企業・教育機関(大学)・行政機関を対象にインタビュー調査を実施した。

２．調査研究成果概要

（１）調査の方法

当研究所は、官公庁・自治体、教育機関(大学)、及び民間企業(計 16 機関)を対象に、インタビュー調査を実施した。インタビュー対象者は、情報セキュリティを管轄するマネジメント層と実働担当者である。

（２）調査項目

本調査は、情報セキュリティマネジメントと教育に関して焦点を当てた。インタビューの調査項目は、調査対象機関により異なるが、基本となる内容は下記の通りである。

１)セキュリティ対策の純技術的手段(ハード/ソフト)の概要

- アウトソーシングの有無
- 組織内ネットワークと外部インターネットとの接続に関して

２)想定されるリスクと実際の被害

①ネットワークのセキュリティ侵害(不正アクセス、ウイルス、SPAM など)

- 最近の攻撃の対象と内容(ネットワーク、データベース等)
- セキュリティ侵害を受けた時の対策(とった行動)と、課題点
- 攻撃を受けた時の組織内のコミュニケーションに関して

・ 内部→内部、内部→外部への攻撃に関して

②情報の漏洩(省内情報、個人に関わる情報、顧客情報)

・ 外部からの情報アクセス

・ 組織内におけるインサイダー

３)情報セキュリティポリシー

・ セキュリティポリシーの有無

・ その概要(基本方針、対策基準、実施手順(マニュアル))

・ 情報の重要度に応じたセキュリティレベルの設定の有無

・ 国際セキュリティ標準 ISO/IEC17799(BS7799)への対応、標準規格への考え方

４)情報セキュリティに対する組織体制　　(組織風土)

・ 情報セキュリティに関する責任者
(CIO, CISO(Cief Information Security Officer)の存在の有無)

・ 情報セキュリティに関するマネジメント体制

・ 情報セキュリティの組織全体における情報システム管理者の役割

・ 情報セキュリティの組織全体における情報セキュリティ担当者の役割・位置づけ

・ 情報投資額に占めるセキュリティ対策費用の割合

５)情報セキュリティに対する教育体制

・ 情報セキュリティに対する教育体制の有無

・ 対象者の範囲とその概要

・ 情報システム管理者への教育

６)国のセキュリティ施策の在り方、或いは国への要望

（３）調査結果概要

[実態編]

①情報セキュリティポリシーの策定

2001 年 7 月以降、CodeRedⅡや NIMDA 等のウィルスによるセキュリティ侵害が急増した。このため、調査対象機関は、情報セキュリティポリシーの策定と運用体制構築を急務としている。

官公庁や自治体は、内閣官房の提示するガイドラインに準じ、各組織に適したセキュリティポリシー(基本方針・対策基準・手順マニュアル)を今年度中に策定する予定である。民間企業は、調査対象が大企業、並びに IT ビジネスを担う、或いは参入している企業であることから、既にセキュリティポリシーやその運用体制を評価する段階に入っている。他方、大学は、未だ教職員や学生に徹底した情報セキュリティポリシー

を明文化していない。

②情報セキュリティ組織体制

行政機関や民間企業は、CISO(Chief Information Security Officer)を頂点にした、ピラミッド型の組織体制を構築している。CISO の配下には、各組織の長から構成される委員会が設置されている。実働の情報セキュリティ担当部門は、総務部門や情報システム部門が担当している。緊急時には、情報セキュリティ侵害の被害が実働部隊に報告され、更にピラミッド型組織を下部層から上部へ遡って報告される仕組みになっている。

大学は、情報セキュリティ運営委員会を設置している。緊急時の対応について明文化している大学は、5 校中 2 校であった。

③情報セキュリティ教育

情報セキュリティ担当者や全職員を対象としたセミナーや集合研修が開催される方向にある。民間企業は、集合研修の他に、全社員を対象とした e ラーニングによる研修を実施、計画している。いかにして全社員の情報セキュリティ意識を高めるかが、民間企業にとっての課題である。

教育内容は、情報セキュリティポリシーの徹底と運用対策に関する内容である。教育内容に、情報セキュリティの倫理面の内容(情報倫理)を含めると回答した行政機関や民間企業は少ない。他方、大学は、学生のいたずら的なセキュリティ侵害の実態があることから、学生を対象とした情報倫理教育を実施している。

④情報セキュリティコストと被害金額の算出

本調査において、情報セキュリティコストの算出の有無を質問した。本調査対象機関では、この質問に対して即答したのは一機関のみであった。

情報セキュリティコストは、技術的対策コスト(ネットワーク制御等)、人的コスト(運用管理、教育等)、及び物理的コスト(室入退管理等)から成る。例えば、情報セキュリティの技術的対策コストは、情報通信システムのハードウェアやソフトウェアのコストの一部分として含まれる。人的コストについても、他業務コストと容易に切り分けることができない。このため、多くの機関は、情報セキュリティコストのみを算出していないのが実状である。

また、情報セキュリティ侵害の被害金額の算出について、同様に質問したところ、被害の程度を単純に計ることは難しいことから、実際に算出している機関は存在しなかった。

[考察編]

⑤情報セキュリティマネジメントを決定する三つの視点:

「技術的対応」、「情報セキュリティ運用管理」、「仕事のやり方(人の働き方)」

企業は一般に、IT を、仕事の効率化や生産性向上のために導入している。或いは、IT 技術を自由に操ってビジネスを拡大しようとも考えている。他方、情報セキュリティの確保は、仕事の効率性や生産性向上とは相反する部分がある。インタビュー調査の結果、情報セキュリティを確保するために、IT の使用を制限、或いは使用にあたって認証や申請手続きを義務付ける企業や自治体が多いことが明らかになった。

組織において、IT の導入効果を最大限に発揮しつつ、情報セキュリティを確保するためには、情報セキュリティ技術にかけるコスト、運用管理体制の複雑さの程度、及び仕事のやり方(人の働き方)の観点からマネジメントする必要がある。

⑥情報セキュリティ担当者の負担の軽減:

情報セキュリティポリシーの徹底と個人の情報セキュリティ意識の向上が重要

本調査対象の行政機関や民間企業は、情報セキュリティには十分な対策を講じる姿勢で臨んでいる。情報セキュリティ担当部門は専任部隊であり、負担の多い場合には人員を投入する、或いは外部にアウトソーシングする形態をとっている。

このような体制をとっていても、セキュリティ侵害が多発し、組織に与える影響が大きくなると、情報セキュリティ担当者の稼動面の負担は増大する。各機関が、この解決の方策として取り組んでいるのが、情報セキュリティポリシーを明文化し、組織個人の情報セキュリティ意識を向上させることである。しかし、全構成員の情報セキュリティ意識の向上を図るのは容易ではない。このような現状認識に基づき、各企業とも情報セキュリティ教育の具体的な方法と内容を模索している。

⑦研究の自由や大学・学部の自治と情報セキュリティ

大学が所属教官から構成される評議会によって運営され、学部が学部教授会によって運営される事実は、大学と学部の自治を端的に示している。また、各教官の研究内容に対する干渉を排除することも大学教官の共通認識であって、これは研究者の研究の自由という原則にもとづいている。

個々の部局・研究室がインターネット・サーバーを運用管理する分散管理体制は、大学教官の自律・自治意識によって支えられていると考えることができる。

一方、今後、情報セキュリティの運用コスト低減や、セキュリティ侵害のリスク軽減のために大学におけるインターネット･サーバーの集中管理が推進される場合、大学教官の自律・自治意識との葛藤が大きな問題となることが予測される。