社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－DPS－130 (56)
2007－CSEC－ 36 (56)
2007／3／2

情報セキュリティ心理学の提案

内田 勝也†, 矢竹 清一郎†, 森 貴男†, 山口 健太郎†, 東 華枝†
† 情報セキュリティ大学院大学

企業、組織において、IT技術の革新により対象業務が飛躍的に高度化し、システム管理者や管理職に対して、組織をより強固にするために、IT技術に関する調査、攻撃者の動機、組織の脆弱性を考慮することが求められてきた。近年、脅威は多様化しており、多くの攻撃者は人間の脆弱性を攻撃する手法、いわゆる”Social Engineering”を利用するようになってきた。このような攻撃に対して近年の技術的対策や物理的対策だけで解決することは非常に困難になっている。このため、攻撃者、利用者や管理者に関する心理学的研究は、従来の情報セキュリティ対策を飛躍的に向上させることが考えられる。本論文では心理学的な側面からの研究を「情報セキュリティ心理学」とし、その確立を目指したい。

キーワード:情報セキュリティ心理学、ソーシャルエンジニアリング、内部犯行

Proposal for Establishing Information Security Psychology

Katsuya Uchida†, Seiichiro Yatake†, Takao Mori†, Kentarou Yamaguchi†, Hanae Azuma†
† Institute of Information Security

Developing information technology and hardware technology makes System Administrators and Managers consider not only many information technologies to make organizations become more secured but also attackers' motivation and organization's vulnerability. Recently the threat has become diversification, many attackers take advantage of "Social Engineering" which can be regarded as 'hacking a psychological weakness'. It is very difficult to protect or to prevent these attacks by recent system solutions & physical solutions. Therefore information security level can be improved by psychological research for attackers, end users, and managers of the information systems. We propose for establishing "Information Security Psychology" in the information security.

Keyword: Information Security Psychology, Social Engineering, Internal Threat

1．はじめに

従来の情報セキュリティ対策は、物理的、技術的対応が中心に行われてきた。しかし、インターネット環境が一般的となり、コンピュータが爆発的に普及したことで、企業、組織では、一人1台のコンピュータを利用することが当たり前となった。

このことは同時に、専門的領域であり、物理的・技術的な対応で一定の成果を上げることができた情報セキュリティの状況を大きく変え、むしろ、それを利用する人間の問題を大きくしたといえる。

ネットワークやコンピュータを始め、様々なシステムを利用するのは人間であり、それらを攻撃するのもまた人間であることを考えると、情報セキュリティに関して、人間的側面からの研究を行うことは、ごく自然なことであるとともに最も重要な観点であるといえよう。

さらに、企業や組織における情報セキュリティマネジメントの維持・更新をしていくためには、教育・訓練、周知等の効果を高め、継続的な対応を行うことが重要になる。これらの方法も、ただそれらをわかりやすく行えばいいというのではなく、人間がどのように考え、行動するのかという視点で方法論を研究していくことが求められてい

る。

2．これまでの情報セキュリティ心理学的研究について

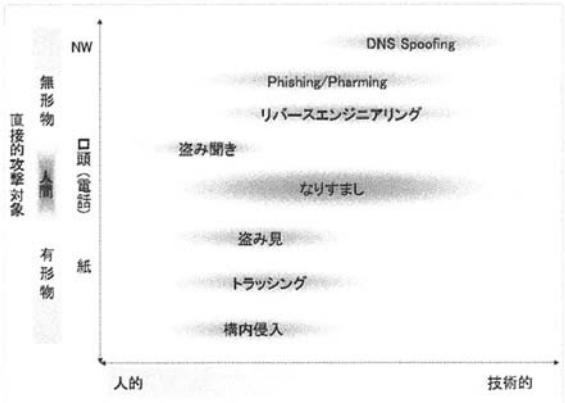
これまで、情報セキュリティ心理学として、体系的・統合的な研究は行われていない。しかしながら、いくつかの分野については実践的な研究事例等がある。代表的なものを概観する。

2.1 ソーシャルエンジニアリング

ソーシャルエンジニアリングとは、目的とするシステムに対して技術的な攻撃を利用して侵入を図るものではなく、人間の行動的側面・心理的側面を巧みに利用し、情報の取得・改ざん・破棄を受動的、能動的に実施させる手段である。

ソーシャルエンジニアリングの目的は、①情報を取得するための情報収集、②施設・システムへの侵入、③情報を開示させる、④情報を破棄・破壊させる、⑤情報を変更させる、等が考えられる。但し、必要な情報を取得する直接的な対象は、必ずしも人だけではなく、ごみ箱を漁って書類、マニュアル、記録媒体等を収集するといった手法も該当する。また、ディスプレイ画面に表示されている内容を盗み見たり、電子メールで偽情報を送付して、偽サイトにおびき寄せて、ユーザ ID やパスワードを収集することもソーシャルエンジニアリングに含まれる。

その対象や手法との関係を概括的に示したのが、図表１である。



図表１ ソーシャルエンジニアリングの範囲

ソーシャルエンジニアリングについては、その手法を実際に利用した経験を綴った書籍[1][2]が有名で、特に Kevin Mitnick 等は、その著書[2]の中で「ソーシャルエンジニアリングを行うものは、人間の性質（性格）を巧みに利用する」と述べている。

人間の性質を利用してある行動へと誘導するといった分野については、多くの研究が行われているが、Robert. B. Cialdini はそれらを体系的にまとめた[3]。

Cialdini はその中で承諾誘導の戦術として「返報性」、「コミットメントと一貫性」、「社会的証明」、「好意」、「権威」、「希少性」の６つをあげているが、それはまさにソーシャルエンジニアが利用する人間の性質そのものである。

この６つの要素について、Mitnick 等はソーシャルエンジニアたちが利用する「６つの人間の脆弱性」と述べているが、この６つの要素について、もう少し詳しく述べる。

(A) 返報性： 親切や贈り物、招待等を受けると、それを与えてくれた人に対して将来お返しをせずにいられない気持ちになること。

(B) コミットメントと一貫性：自由意志によりとった行動がその後の行動にある拘束をもたらすことで、代表的なものに以下のような手法がある。

① ローボールテクニック：最初にある「決定」をさせるが、決定した事柄が実現不可能である事を示し、最初の決定より高度な要求を認めさせる方法。例えば、特売の商品を購入しにきた客に、購入の手続きの最中に在庫がなく当該の商品は購入できないが、色違いの少し高いものならあると言って高い商品を購入させてしまうというようなこと。

② ドア・イン・ザ・フェイス テクニック：最初に実現不可能な要求を行い、対応できない状況の中で、それに比べて負担の軽い要求をしてそれを実現させる方法。例えば、法外な借金の依頼を最初に行い、断られたら少額の借金を申し出てそれを承諾させるようなこと。

③ フット・イン・ザ・ドア テクニック： 最初に誰もが断らないようなごく軽い要求を行ってもらい、次のより重い要求の承諾を得る方法。例えば、最初に簡単な署名を依頼し、その後時間がかかる調査に協力してもらうといったこと。

(C) 社会的証明： 他人が何を正しいと考えているかによって、自分が正しいかどうかを判断する特性。

(D) 好意： 好意を持っている人から頼まれると、承諾してしまうというもの。パーティを開いて、商品を購入させる場合、好意を持っている隣人がホスト役として販売を行うと、そうでない場合に比べて簡単に購入してしまうといったこと。

(E) 権威： 企業・組織の上司等権威を持つものの命令に従ってしまうこと。

(F) 希少性： 文字通り、手に入りにくい物であるほど、貴重なものに思え、手に入れたくなってしまう特性。

ソーシャルエンジニアはこのような人間の特性を利用して正当なアクセス権を持つ人間を騙し、内部機密情報への正当なアクセス権を手に入れる。

このように、正当なアクセス権を得て、攻撃者になった者に対しては、もはや今までの技術的対策のみでは防御しきれない。それに対する場合は、こういった手法をよく理解するとともに、継続的に教育・訓練や警戒心の喚起を行い、常に一定レベルの注意力を、社員ひとりひとりの働きかけにより維持することが有効であると考えられている。

2.2 内部犯行者の研究

一般的には、内部犯行、つまり、もともと正当な権限を持つ者の犯行についても、心理学的、あるいは、組織心理学的な面からの研究がある。

内部犯行者は、現在あるいは過去にその企業・組織の従業員（役員）であった者で、所属企業・組織の情報システムやネットワークシステムへのアクセス権限を持っている（持っていた）者であるため、必要な情報を正規の手段で入手できたり、システムに対する技術的な知識が高いのが特徴であろう。

米国 CERT/CC では、2001 年から内部犯行者の不正行為、例えば、企業・組織の機密情報や重要情報に対すてのスパイ行為、IT 妨害行為、詐欺行為、窃盗行為等についての情報収集を行ってきた。

これを受けて、Carnegie Mellon 大学 CyLab では、MERIT（Management and Education of Risks of Insider Threat）プロジェクトを組織し、内部犯行者の心理的な面からの研究[4]を行っている。

この研究では、内部犯行者の所属する組織の性格、犯行者の性格や心理的な面などがテーマとされている。

2.3 リスク心理学

災害やリスクについても心理学的側面からの研究[5]が行われている。

リスク心理学は、情報セキュリティを直接扱っているものではないが、最近の内部統制についてリスクマネジメントが語られているように、情報セキュリティにおいても、リスクを考えることは必要なことである。

リスクに関する人間の感じ方は、必ずしも現実的な数値（たとえば発生確率）に因ったものではない。そのことは、リスクについての対応を誤らせる原因ともなる。

例えば、航空機事故と自動車事故を比較すると、航空機事故の発生確率は自動車事故の発生確率より低いが、一部の人は自動車事故より、航空機事故の発生が高いと考えている。これで、航空機の方が事故に遭いやすそうだから自動車がよい、または、自動車が安全と考えて適切に対策を行わないのはおかしな事となってしまう。

これは明らかに、航空機事故のイメージが強烈なもので、それを恐れている事から起こる誤認識であろう。なぜ、このようなことが発生するのだろうか。

安全や安心とその対極にある危険と不安について、その本質を認識するためには、心理面からのアプローチが非常に有効であると考えられる。

2.4 犯罪機会論

犯罪者に犯罪の機会を与えないことにより、犯罪を未然に防止しようとする考え方である。

犯罪を行なうことができると思わせるような環境を作らなければ、犯罪者が犯行を思いとどまると考えるものである。

つまり、この考え方は、犯罪を行おうと考えていない者でも、犯罪機会があれば犯罪を行うことがある。また、犯罪を行おうと考えている者でも、犯罪機会がなければ犯罪を行うことはないと考えるものである[1]。

---

1 内田は、情報セキュリティは、「性悪説」でなく、「性弱説」のものとしている。目の前に貴重な情報（お金になる）が落ちており、誰にも見つからないと思

この考え方に基づいて、物理的環境の設計や人的環境の改善を行うことにより、犯行が行い難い環境や状況を作り出し、犯罪機会を与えず、犯罪を防止することができる。

犯行に都合の悪い状況はどのようにして作られるかの研究は、情報セキュリティだけに関係したものではないが、犯罪者の標的と犯行の場所については、図表２のように考えられている。

	犯罪に強い要素	ハードな要素	ソフトな要素
標的	**抵抗性** 犯罪者から加わる力を押し返そうとすること	**恒常性** 一定不変なこと	**管理意識** 望ましい状態を維持しようと思うこと
場所（地域）	**領域性** 犯罪者の力が及ばない範囲を明確にすること	**区画性** 区切られていること	**縄張意識** 侵入は許さないと思うこと
	監視性 犯罪者の行動を把握出来ること	**無死角性** 見通しのきかない場所がないこと	**当事者意識** 自分自身の問題としてとらえること

図表２ 犯罪は「この場所」で起こる[6]

2.5 ハインリッヒの法則

米国H.W. Heinrichは、労働災害の事例の調査から、重傷以上の災害が１件起きる背景には、軽傷を伴う災害が29件起きており、さらには危うく惨事になるような「ヒヤリ」「ハッと」するような出来事が300件あるという「1:29:300の法則」を見いだした。いわゆる、「ハインリッヒの法則」である。

この法則は労働災害だけでなく、リスクを考えなければならない多くの分野に適用できるものと考えられている。

更に、ハインリッヒの法則は、犯罪防止の観点から考えると、J. Q. WilsonとG. L. Kellingの「割れ窓理論（Broken Windows Theory）」[7]と同じであると言える。即ち、割れ窓理論では、１枚の割れたガラスを放置しておくと、他のすべての窓ガラスが割られてしまうと考える。その割れ窓と同じで、小さな問題を放置しておくと、荒廃した地域だけでなく、環境の良い地域でも犯罪が発生する可能性が高いと言うことである。これを逆に考えると、軽微な犯罪を徹底的に取り締まることにより、凶悪犯罪を含めて、犯罪を抑止することができることを示している。

2.6 犯罪者プロファイリング

犯罪者プロファイリングとは、「ある犯行や、ある一連の類似犯罪で示された行動を研究対象とし、そこから犯人像を推定すること」[8]と定義している。

情報セキュリティ分野での適用は時期尚早と言われる可能性があるが、広い意味で考えると「2.2 内部犯行者の研究」は、この分野の１つであると考えることもできる。

たとえば、犯罪者プロファイリング分野の１つに、「地理的プロファイリング」がある。地理的プロファイリングでは、犯行の場所、複数の犯行場所の空間的な関係等から犯人の居住地区を絞る事などを行う。

情報セキュリティにおいては、どこから攻撃されるかによって、どの様な犯行の可能性が高いかを初期の段階で推測して、その対応を準備することなどが考えられる。

３．まとめと課題

3.1 現在の取り組み

現在は「2.1 ソーシャルエンジニアリング」や「2.2 内部犯行者の研究」を除いては、情報セキュリティへの適用はまだまだこれからであると言わざるを得ない。

また、比較的取り組みの進んでいるソーシャルエンジニアリングについても、体系的で学問的な形での研究は非常に少ない。

さらに本稿で指摘した「６つの承諾誘導の戦術」つまりソーシャルエンジニアが利用する「６つの人間の脆弱性」は、ソーシャルエンジニアが攻撃の対象者に対して利用するという視点などが中心になっているが、この「６つの人間の脆弱性」を、教育・訓練や周知等に対して適用し、有効性を高めるために応用することも十分に考えられる。

我々は実際に「６つの人間の脆弱性」のうちの「(B) コミットメントと一貫性」を利用して、行動を誘導することで、情報セキュリティ研修の効果を上げるための調査・研究を行っている。

また、最近はISMS等の認証取得企業が増加しているが、情報セキュリティマネジメント体制の構築・維持については、改善すべき点が多い。そこ

えば、人はそれを自分の懐に入れてしまう可能性はゼロではない。情報セキュリティは、人間の弱さを防止するための仕組みであるとしている。

で、認証取得企業における認証取得後の体制の維持やセキュリティポリシー等を効果的に実現する方法についての調査・研究も行っている。

犯罪機会論、ハインリッヒの法則、割れ窓理論等については、物理的セキュリティ等への適用が既に行われているものもある。例えば、ハードウェアが被害を受けないための設置場所や設置方法等への適用はその１例であろう。

人間の心理面への適用ではないが、ハインリッヒの法則では、機器の故障等の現象をモニターすることにより、機器の完全故障の時期を推測することで、事前にその対策を行うことも行われている。更に、ネットワーク等への攻撃の兆候によって、大規模な攻撃を事前に予測する「攻撃者プロファイリング」は、既にSOC (Security Operation Center)においてSOC要員が経験的に行っている。

3.2 情報収集

前述したCarnegie Mellon大学CyLabのMERITにおける内部犯行者の特性の研究は、米国国防総省やシークレットサービス等と連携して研究を行っているが、同様な方法を日本国内で行うことは現在では困難であろう考えられる。

また、セキュリティに関する情報については、各企業が積極的に提供しない場合が多く、そういった面でも困難さがつきまとう。

しかしながら、適切なデータ、情報の収集は非常に重要であるため、情報収集については、今後、国の機関や企業等と協力していくことが望まれるといえよう。

3.3 今後の方向性と課題

情報セキュリティは、本来学際的・総合的な学問分野であると言えるが、その対象が「人間」に拡大し、不可欠な要素であることが明確になってきたことで、特に心理学的なアプローチが重要になってきている。その意味で、心理学分野の研究者が数多くこの分野の研究を行って欲しいと考えているが、まだまだ、そのような取り組みは少なく、課題の一つであると考えている。

一方、本グループは情報セキュリティ分野の研究を心理学的見地から行っているものであるが、心理学の専門家ではない。ここで言う「情報セキュリティ心理学」については、心理学分野の専門家と、情報セキュリティ分野の専門家の協働による研究が非常に有効な効果を出すことができると考えている。そのような協働体制の創出についても大きな課題である。

今後、情報セキュリティ分野において、より多くの共同研究が行われることを期待したい。

参考文献

[1] The Knightmare, “Secrets Of Super Hacker”, Loompanics Unlimited, 1994 (松藤留美子他訳「シークレット・オブ・スーパーハッカー」, 日本能率協会マネジメントセンター, 1995)

[2] Kevin D. Mitnick & William L. Simon, “The Art of Deception”, Wiley Publishing, Inc., 2002 (岩谷宏訳, 「欺術 ―史上最強のハッカーが明かす禁断の技法」, ソフトバンクパブリッシング, 2003)

[3] Robert. B. Cialdini, “Influence: Science and Practice”, Allyn and Bacon, 2000 (社会行動研究会訳, 「影響力の武器 ―なぜ、人は動かされるのか―」, 誠信書房, 1991)

[4] http://www.cylab.cmu.edu/default.aspx?id=2013

[5] 岡本浩一, 「リスク心理学」, サイエンス社, 1992

[6] 小宮信夫, 「犯罪は「この場所」で起こる」, 光文社新書, 2005

[7] J. Q.Wilson, G. L.Kelling, “Broken Windows”, The Atlantic Monthly, 1982 (http://www.ap-soken.com/info/2002/020410.html)

[8] ジャネット・L・ジャクソン他、田村雅幸監訳, 「犯罪者プロファイリング」, 北大路書房, 2000年