情報セキュリティ心理学について

中央大学 研究開発機構
内田　勝也

目　　次

１．はじめに

「情報セキュリティ心理学」と大それた言葉を使っているが、四半世紀以上に渡って情報セキュリティを主に実務経験者として行ってきた立場からみると、国内では、技術だけが情報セキュリティという感じを受けている。海外、特に米国での情報セキュリティから感じるのは、技術、管理・運用、法制度等に対して、社会科学、人文科学等の分野からの調査研究もあり、情報セキュリティは総合科学であると感じている。国内でも多くの研究者が、技術だけでなく、組織や個人の特性を踏まえて情報セキュリティ研究を行うことになれば、情報セキュリティでの進展にもつながるのではないかと考えている。

１.１ 情報セキュリティとは？

情報セキュリティを考える場合、技術的な対策で相当の対策が可能であるが、他のシステムと同様 100%完璧に情報通信システムを保護できない。

当然ながら、技術的な対策で不十分な所は、関係する人間が対応しなければならない。このため、技術と人間の協力の下に情報セキュリティ対策を行う必要がある。

勿論、技術的対策でも人間的対策でも必要な対策を行われていなければ、情報セキュリティ対策全体に脆弱性が残ってしまう可能性はある。

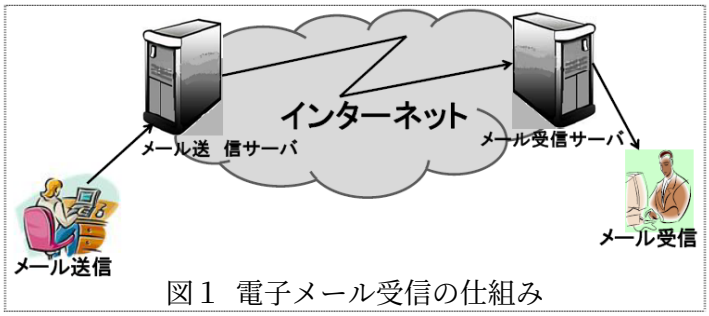

図１ 電子メール受信の仕組み

受信する電子メールの例で考えてみる。電子メールは、郵便での仕組みと基本的には同じ仕組みと言える。

外部からメールが送られて来ると、ISP(Internet Service Provider)や企業・団体のメー

ルサーバで受信され、利用者がメールソフト（メーラー）を起動し、メールサーバに保存されているメールを利用者のパソコンに取り込む[1]。

送信されてくるメールには、(1)本来利用者が受け取ってよい（正しい）メールと、(2)受け取りたくない（不正な）メールが含まれる。これら２種類のメールは、現在では、多くのメールサーバのソフトウェアが事前に設定されて基準に従って分類されるが、利用者が望む正しい判断が常に行われているとは限らない。

実際、(1)の場合、本来は「不正なメール」が、正しいメールと判断され、「受信メールボックス」に保存され、反対に、(2)の場合では、正しいメールが不正なメールと判断され、「迷惑メールボックス」に保存されることがある。これを整理すると以下のようになる。

(1-1)　ISP のメールサーバは正しいと判断しているが、不正なメールだった。

(1-2)　ISP のメールサーバは正しいと判断し、事実、正しいメールだった。

(2-1)　ISP のメールサーバは不正なメールと判断したが、正しいメールだった

(2-2)　IPS のメールサーバは不正なメールと判断し、事実、不正なメールだった

「不正なメール」の判断は、ISP や企業・団体の持つ知見（技術）を利用しているが、100%完全に行えない。図２には、「不正メール」が正しいものと判断され受信メールボックスに入っているもの（枠内）があり、図３には、本来正しいメールであるが、不正なメールと判断され、「迷惑メールボックス」に分類されている（枠内、２件ある）。このように全ての受信メールを正しく判断できないため、ISP や企業・団体では利用者に技術による判断に誤りがあれば報告を求め、適宜修正を行っている。

電子メールに関する情報セキュリティでは、上記分類の（1-1）に注目する必要がある。不正なメールが正しいメールとして判断されると、利用者はメール内容が正しいとして処理する恐れがある。例えば、メールに書いてあるウェブを閲覧し、クレジットカード情報を入力し、クレジットカードが不正利用された。オークションのユーザ ID／パスワードを入力したため、オークションで悪用されたといった事件が発生している。

また、企業・団体等では、メールにあるウェブを閲覧したため、ウイルスやスパイウェアと呼ばれる有害なソフトウェアが利用者のパソコンに導入され、利用者が管理していたウェブのユーザ ID／パスワードが盗まれ、ウェブを改ざんされ、改ざんされたウェブを閲覧した第三者が更に被害を受けた事件[2]も発生している。

この例でもわかるように、情報セキュリティ技術だけでは完全でなく、足りない部分は人間が対応しなければならない。また、人間の対応も完璧ではなく、更に問題は上記の例でもわかるように、たった一人の利用者の不用意な操作が組織全体のセキュリティが崩壊してしまうこともある。

1　最近はウェブメールを利用する場合もあるが、基本的な考え方は同じ

2 2009 年から 2010 年に「ガンブラーウイルス」と呼ばれた事件が発覚した。ウェブサイトが改ざんされ、そのウェブを閲覧した利用者が悪意あるウェブサイトに誘導され、ウイルスが利用者のコンピュータにダウンロードされてしまった。

枠内は、迷惑メールと分類されず、受信メールボックスに振り分けられた
図２受信メールボックスの内容

枠内（２項目）は受信メールボックスに分類されるものが、迷惑メールと判断された
図３迷惑メールボックスの内容

１.２ 安全と安心について

一般に、あるシステムが安全であると言う場合、どの様な状況を安全と言うのであろう

か。 安全の反対は危険であるが、危険が全くない状況を維持することは、現実の世界（ネットワーク等の仮想世界を含めても）では不可能であろう。 実際、安全は「絶対に安全」だとか、「100%安全」という意味ではなく、多少の危険はあるが許される範囲にある場合に安全と言われる（図４）[1]。 安全の程度は時間の経過や環境の変化、人間や機械等が動くことでも、安全の程度は変化する。 時間が止まっており、また、人間も機械も全く何もしなければ、安全の程度の変化はないが、そのような状態は現実の世界にはない。

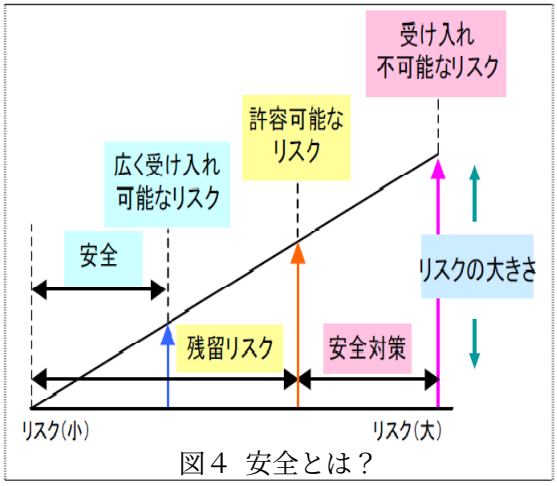

図４ 安全とは？

安全と同じような意味で、安心という言葉があるが、安全は「安全性」等と使われるように客観的な意味で使われるが、安心は「安心感」等と使われるように主観的な意味がある。

安全の反対は「危険」、安心の反対は「不安」と考えられる。 そこで、安全・危険、安心・不安をそれぞれ縦軸と横軸に 2 次元のマトリックスを考えると、図５のような４つの領域が考えられる。

① 安全であり、安心だと思う
② 安全であるが、不安を感じる
③ 危険であるが、安心と考える
④ 危険であり、不安を感じる

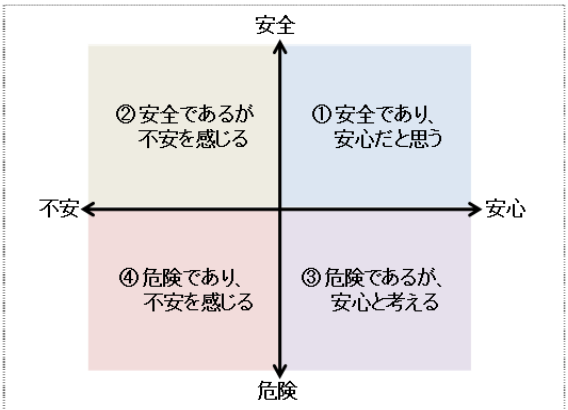

図５ 安全･危険、安心･不安マトリックス

安全が確保されれば、全ての人が安心と思ってくれることが望ましいが、実際には、安全が確保されていても、不安を感じる人がいる。 また、 逆に危険な状況を安心と思うことがある。

なお、安心を「信頼」と置き換えることも可能であろう。

図５のマトリックスで、「② 安全であるが、不安を感じる」あるいは、「③ 危険であるが、安心と考える」のは、何故だろうか？

例えば、自動車事故より、飛行機事故の方が統計的には少ないが、飛行機には乗らないが、自動車には日常的に乗っている人がいる。

最近の例で言えば、毎年流行の季節性インフルエンザでは、毎年死者がでており、１万人を超えたこともある。多くの企業・団体では、従業員の外出を控えさる、外出時にマスクをする、と言ったことを指示している形跡はあまり聞かない。

しかし、2009 年 4 月にメキシコで発生した「新型インフルエンザ」は瞬く間に、日本でも感染者が見つかり、マスコミによる連日の大報道もあり、多くの企業では海外渡航を禁

止したり、家族に感染者がでると１週間程度の自宅待機を社員に命じた。2010 年 5 月末までに、61 人が死亡し、2009 年からの累計で、200 名を超えた。一方、季節性インフルエンザは、2000 年以降、214 人（2001 年）～1,818 人（2005 年）の死者がでている[3]。

新型インフルエンザは、「② 安全であるが、不安を感じる」、季節性インフルエンザは「③危険であるが、安心と考える」と言える。

多くの人々が安全なのに不安と感じる、あるいは、危険なのに安全と思うのは何故だろうか？

１つはマスコミ等の報道に大きく影響されていると思われる。「ニュース：News」（「新しい」ことが複数ある）という言葉通り、新しい事柄を数多く報道する使命がマスコミにある。 新しい問題を大々的に報道することは、読者の興味を引き、その問題に注目させることになる。このこと自体は決して悪いことではない。ただ、新型インフルエンザのように新しい事柄について、大々的な報道があると、多くの人が実際以上の不安を感じる可能性がある[2]。

このように、安全なのに安心、あるいは信頼できない状況について、専門家の立場から、大規模技術に関して、「専門家と専門家」あるいは、「専門家と地元住民」の対話が行われている[3]。

新しい事柄がでてくると、報道の多さ、その事柄に対しての情報の少なさ等により、不安・不信を抱く可能性が高いのではないだろうか？　情報セキュリティ分野でも同じような問題が発生していると考えており、「専門家と専門家」あるいは、「専門家と利用者」の対話が必要ではないだろうか。

２．情報セキュリティと組織・人

２.１ 情報セキュリティと組織・人について

（１）組織と人の概要

情報セキュリティにどのような人たちが関係するかを考えると、以下のようになる

① 外部攻撃者： 組織に所属する者でなく、何らかの形で故意に犯罪や ICT への攻撃を行う者。

② 内部犯行者： 組織に所属している（いた）者で、何らかの形で故意に犯罪や ICT への攻撃を行う者。なお、内部犯行者は以下の③システム管理者、④利用者であり、一般的には退職者も内部犯行者に含める。

③ システム管理者：組織の ICT を管理する人たち。ISP が代行していることもある。情報セキュリティ確保のための技術的な仕組みの導入・維持管理を行う人たち

④ 利用者：ICT の利用者。

なお、情報セキュリティでは、上記①、②に属する者は、故意に事件を起こす者である

[3] 厚生労働省 http://www.mhlw.go.jp/bunya/kenkou/kekkaku-kansenshou04/02.html#100

が、③、④に属する者は過失で事件・事故を起こす可能性がある。

更に、企業・団体等での情報セキュリティ事件・事故を考える場合、上記のような個人を考えるだけでなく、組織的な特性も考える必要がある。

組織的な違反の場合、個人の利益のために違法行為等を行うのではなく、会社のためと考え、その結果、個人が事件・事故を起こすことがある。緊急業務で、セキュリティポリシー違反をしてデータを自宅に持ち帰り、自宅のパソコンで処理を行ったが、Winny 等のソフトウェアが導入されていたため、情報漏えいを起こしたといったことなどがある。

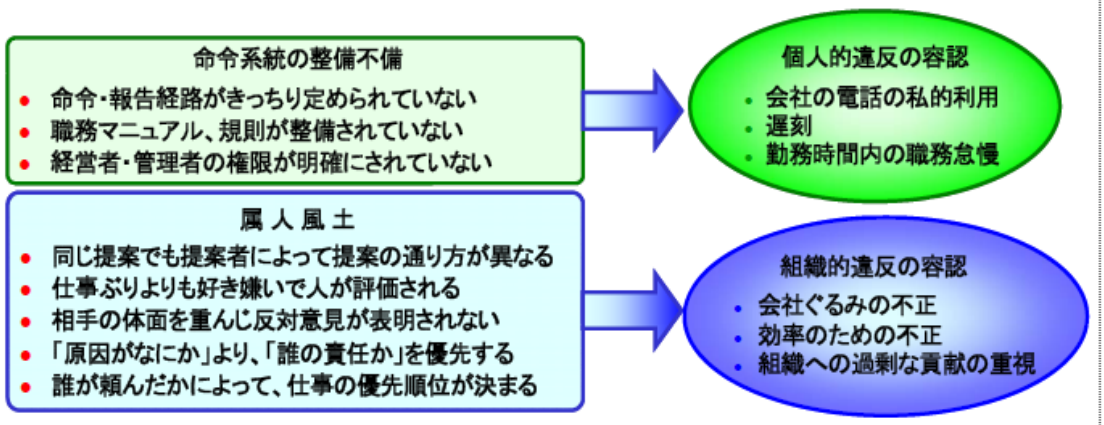

図４　組織違反について

鎌田晶子　「『組織風土』とヒューマンエラー」（大山正・丸山康則 編「ヒューマンエラーの科学」）

（２）内部犯行者の分析

内部犯行については、企業・団体の従業員を考える場合には、犯行を行った個人だけを考えるのではなく、組織的違反を含めて考えることが必要で米国では犯罪者のプロフィールを容易に取得できるため、早い時期から研究が行われている。米国 Carnegie Mellon 大学にある CERT/CC[4]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してのスパイ行為、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。Carnegie Mellon 大学の CyLab の研究者が MERIT プロジェクトを発足させ、内部犯行についてシステムダイナミックス等を使って、内部犯行者の研究[5]が行われている。

国内では、犯罪者のプロフィールを一般の研究者が入手することが困難であったため調査研究が進まなかったが、2009 年中頃から警察関係の研究者等が中心になって、情報セキュリティの内部犯行に関する研究[6]が行われるようになった。

---

[4] CERT/CC：Computer Emergency Response Team/ Coordination Center 1988 年に発生した「モーリスワーム」事件の教訓として、米国政府がインターネットの事件・事故への対応のため、カーネギーメロン大学内に設置した

[5] カーネギーメロン大学 CyLab MERIT(Management and Education of Risks of Insider Threat) http://www.cylab.cmu.edu/research/projects/2010/MERIT-ITL.html

[6] 情報セキュリティにおける人的脅威対策に関する調査研究

２.２ 外部攻撃者について

外部攻撃者は、いわゆる、ハッカーとかクラッカーと呼ばれており、高度なセキュリティ技術を持っており、攻撃対象のシステムに簡単に侵入できると言った考えがある。しかし、過去の調査等を見る限りにおいて攻撃対象になったシステムに何らかの問題（既知の脆弱性を放置していた）があったと言ってよい。いわゆる、ハッカーは、インターネット等の保存されている攻撃ツールを利用し、攻撃対象システムの脆弱性を探し出し、その脆弱性を利用して目的のシステムに侵入することが大部分であると言える。

勿論、全ての脆弱性への対応は必ずしも簡単ではないこともある。また、一部のソフトウェアメーカーは公開されたプログラムの脆弱性を長期間放置していることもあるが、修正プログラムが提供された後、適当な期間（1 ヶ月程度）内に対応を行うことで、ハッカー等からの攻撃を防ぐことができる可能性が高いとの調査（図５）もある。

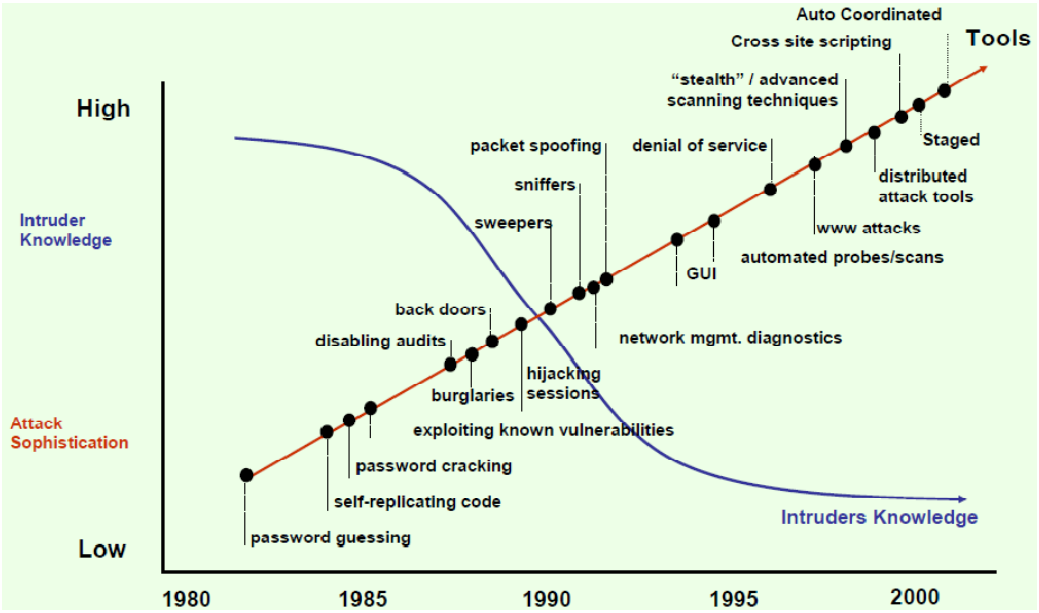

図５ 攻撃ツールの高度化と侵入知識の低下

２００２年７月、当時の米国大統領重要インフラ保護委員会 の副委員長 ハワード・シュミットは、インタビューで、『米国国防総省（ＤＯＤ）が行った２００１年の調査では、国防総省への攻撃の９７～９８％の攻撃はパッチ適用をしなかったか、設定ミスである』と述べている。

http://www.govtech.net/magazine/sup_story.phtml?id=18492

---

http://www.syaanken.or.jp/02_goannai/08_cyber/cyber2203_01/pdf/cyber2203_01.pdf 情報システムに関する内部犯行分析手法の調査研究

http://saka.jp/sss/InsiderThreatGR0904.pdf

既知の脆弱性を利用した攻撃によりデータ漏洩／侵害を受けた大部分はデータ漏洩／侵害の前に、その脆弱性のパッチが提供されていた。右図は既知の脆弱性を利用したデータ漏洩／侵害のどのくらい前に、その脆弱性パッチが入手できたかを示したもの。 脆弱性のパッチが入手後、1 ヵ月前位にパッチを当てておけば、脆弱性を狙った攻撃に遭遇してもデータ漏洩／侵害が発生することはなかったことになる。 また、重要なのことは、パッチは計画を立て、戦略的に実装するのがデータ漏洩／侵害を防止する上で有効である。パッチが出るたびにシステムに適用する「モグラたたき」的な方法より格段に効果的である。

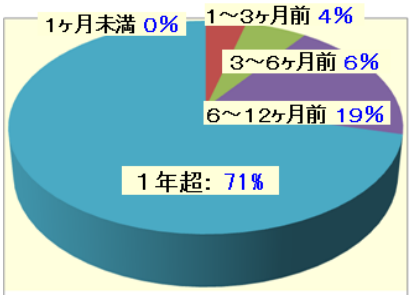

図６ Verison Business「2008 年データ漏洩／侵害調査報告書」2008 年

２.３ ソーシャルエンジニアリング

人間の心理的な弱さを利用し、攻撃者が必要としている情報等を攻撃対象に関係する人々から取得する方法を「ソーシャルエンジニアリング」[4][5]と呼んでいる。

この方法は、攻撃者にとって強固に保護されたネットワークの脆弱性を探して、侵入を図るより、より簡単な方法で侵入できれば、その方法を用いて侵入するのは、現実の世界でも、サイバーの世界でも同じである。情報通信システムを考える場合、最弱な部分（脆弱性）は人間である。攻撃者が権限を持った人から得た情報は、攻撃対象システムに対して、正規の情報であり、攻撃者は正面からシステムへ侵入できる。

例えば、利用者のアカウント（ID ／パスワード）をこの方法で取得できれば、正面からシステムへ侵入できる。 2009 年末に発生した米国 Google 社への攻撃[6]でも、ソーシャルエンジニアリングが使われている。

また、一人に対してソーシャルエンジニアリング手法を利用するだけでなく、複数の関係者から得られた断片的な情報をまとめることにより、目的の情報を得ることもできる。

ソーシャルエンジニアリングの主な手法

- なりすまし： 他人になりすまして、必要な情報を収集する。電話を利用することが多いが、電子メールや手紙を使ったり、FAX を利用することもある
- ゴミ箱漁り： トラッシング（Trashing）とか、Dumper Diving と呼ばれているが、 ゴミとして廃棄された物の中から、目的の情報を取得する。オフィスからゴミとして出されたハードディスク、フロッピーディスク等の磁気媒体や CD、DVD、マニュアル、報告書等、重要書類等の印刷物を回収して、有効な情報を取得する
- サイト侵入： 清掃員、電気・電話工事人、警備員等になりすまして、オフィスや工場等のサイトに侵入する
- のぞき見： 他人のものをこっそりのぞき見するもの。情報が机上やコンピュータ上に露出しているものを意識的にのぞき見したりして、情報収集を行う
- メーリングリスト、ブログ等： メーリングリスト等の質問メッセージを利用して、質問者の技術レベル、利用システム、ソフトウェア、セキュリティ等の情報を収集する

ソーシャルエンジニアリングは、人間の持つ本質的な弱さを利用している。人間の弱さを利用してその人をある行動へと誘導することの研究は、情報セキュリティ分野以外では多くの研究がある。その 1 つに、ロバート・チャルディーニ（Robert B. Cialdini）の研究

[7]があり、チャルディーニは人間の弱さについて、体系化を図っている。

チャルディーニは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で利用される人間の性質そのものである。

ソーシャルエンジニアでは、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から内部機密情報への正当なアクセス権等を手に入れる。正当なアクセス権を得た攻撃者に対しては、最早、情報セキュリティ技術だけでは防御できない。

このため、情報セキュリティ対策では、技術だけでなく、ソーシャルエンジニアリング等の手法をよく理解するとともに、関係する人々に対して、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一人一人に働きかけ、維持することが有効であると考えられている。

６つの人間の脆弱性（Six weapons of influence）

(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・フェィス 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。

２.４ 情報セキュリティ教育

（１）教育・訓練の評価、効果測定について

情報セキュリティの重要性が認識されて、情報セキュリティ教育・訓練が重要になってきており、集合教育だけでなく、e-Learning 等も行われている。しかしながら、厳密な調

査結果ではないが、教育の評価や効果測定については、大企業等でも必ずしも十分に行われていないことが多い。

教育・研修における評価・効果測定では、カークパトリック（Donald L. Kirkpatrick）の４段階評価[5]が有名である。

これは、教育研修評価を４段階、すなわち、①Reaction（研修満足度）、② Learning（学習到達度）、③Behavior（行動変容度）、④Results（成果達成度）に分けて評価を行っている。

カークパトリックの４段階評価

レベル	説　　明
1 Reaction（研修満足度）	受講直後のアンケート調査等による受講者の研修に対する満足度の評価
2 Learning（学習到達度）	筆記試験やレポート等による受講者の学習到達度の評価
3 Behavior（行動変容度）	受講者自身へのインタビューや他者評価による行動変容の評価
4 Results（成果達成度）	研修受講による受講者や職場の業績向上度合いの評価

情報セキュリティの集合教育では参加者へのアンケート調査による教育の満足度評価を行う程度が多く、出欠の確認しか行わないと言う例もある。また、e-Learning ではスライド形式の説明を提供するだけで、クリックして最終ページまで行けば、教育は終了したと見なすと言った話もある。

前述したソーシャルエンジニアリング攻撃等を考えると、情報セキュリティ教育も「レベル３：行動変容」を起こすことができる程度の教育・訓練を考える必要があるのではないだろうか。

なお、ジャック・フィリップス（Jack J. Phillips）は、カークパトリックの４段階評価に５段階目を追加した。レベル５として、「投資収益率」（効果を収益に換算し、収益を教育研修への投資額との比較ではじめて有意義になる）を定義し、以下の２つに細分化している。

- レベル５A：収益貢献度＝その成果を収益金額に換算
- レベル５B：顧客満足度＝顧客の満足に与えた成果をみたもの

レベル４ないし、５になると教育・訓練で可能かの疑問もあるが、行動科学等の知見を利用した少人数での教育・訓練や実際の現場で指導注を行うことでレベル５に結びつくようなものが注目されている。情報セキュリティ分野でも、これらを応用した形で、少人数の集合教育や個人の特性を考慮した形での e-Learning を行うことも可能だと考えている。

注）個人や少人数でのコンサルテーションとも思えるが、少人数での指導（教育・訓練）と考えることもできる

（２）教育・訓練内容について

行動変容を起こすための教育・訓練として、

① 単なる記憶させるのではなく、可能な限り本質や背景にあるものを説明する
② 根本原因分析を行うことにより、疑似体験ができるような環境を構築する
③ ケーススタディを行うことやプレゼンテーションを行うことで、一人で考えるだけでなく、全員参加の環境で教育を行う

①の例としては、心理学では有名なものであるが、図７の左右に示すいずれかが駐車禁止マークかを考えるものがある。

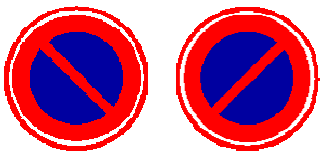
図７ 駐車禁止マークは？

多くの人は左右どちらが正解か知らない。それは、１つの図を示して「これが駐車禁止マーク」としか教えないため、似たようなマークが並ぶと判断できなくなる。

『駐車禁止マークは、「No Parking」の「No」を模式化して作成した。このため、図７では、左側が駐車禁止マークになる。他の禁止マークも基本的には同じ考えで作成されている』と教えられたらどうであろう。

多くの受講者は教育内容が長く記憶に残り、同じような事柄が起こった場合でも、正しく判断できるであろう。

②の例としては、2009 年に発生した「ガンブラーウイルス」と呼ばれる事件があった。ガンブラーウイルスの概要を下記に説明してある。

ガンブラーウイルスについて

ウェブサイト改ざんの概要と主な原因

ウェブサイト改ざんの原因として、ftp※のアカウント情報の盗難事例がある。 盗んだ ftp アカウント（ID/パスワード）を使い、正規のユーザになりすまし、改ざんしたページをウェブサーバに公開（アップロード）する

ftp のアカウント情報を盗む手口は、スパイウェアをターゲットのパソコンに送り込むなどの方法が一般的です

※ File Transfer Protocol の略。ネットワークでファイルを転送するためのプロトコル

改ざんされたウェブページには不正なスクリプトが埋め込まれ、そのページを閲覧した一般利用者を、ウイルスが仕掛けられた悪意あるウェブサイトにアクセスさせます。一般利用者が悪意あるウェブサイトを閲覧した場合、利用者のパソコンに脆弱性があると、それを悪用されウイルスに感染させられてしまいます

この内容等から、ガンブラーウイルスにおける「根本原因」を考え、また、今後の課題について、個人あるいは、グループで考えて、発表させる、と言ったもの等が考えられる。

③の例としては、事故・事件を題材に、損失金額の計算や事件・事故の背景を考えさせ、受講者によるプレゼンテーションや議論を行うもの等が考えられる。

行動変容を起こすような教育・訓練であったかは、一定時間経過後（1 ヶ月程度）に受講者にインタビューを行い判断することが必要と言われている。

厳密な調査ではないが、上記①～③を含んだ講義／セミナーを行い、終了時にアンケート調査を行う方法で分析を行った。アンケート結果では、受講者約 50 名の 80%程度が「行

動変容を起こす」、又は「起こす可能性がある」との回答をした。なお、回答者は全員社会人（社会人修士学生を含む）である。

今後、この様な簡易は方法で有用性を確認できるコンテンツを増やすと共に、レベル３（行動変容）以上の効果を測定できる方法についても調査研究を進めて行きたい。

疑似体験的な教育・訓練では、より多くの人たちに参加してもらうためには、専門的な知識を使わなくても簡単にできる方法を考える必要がある。その１つの方法として、河野龍太郎は図８に示すような方法を提案している[9]。この様な手法は情報セキュリティ分野でも利用できることを確認している。

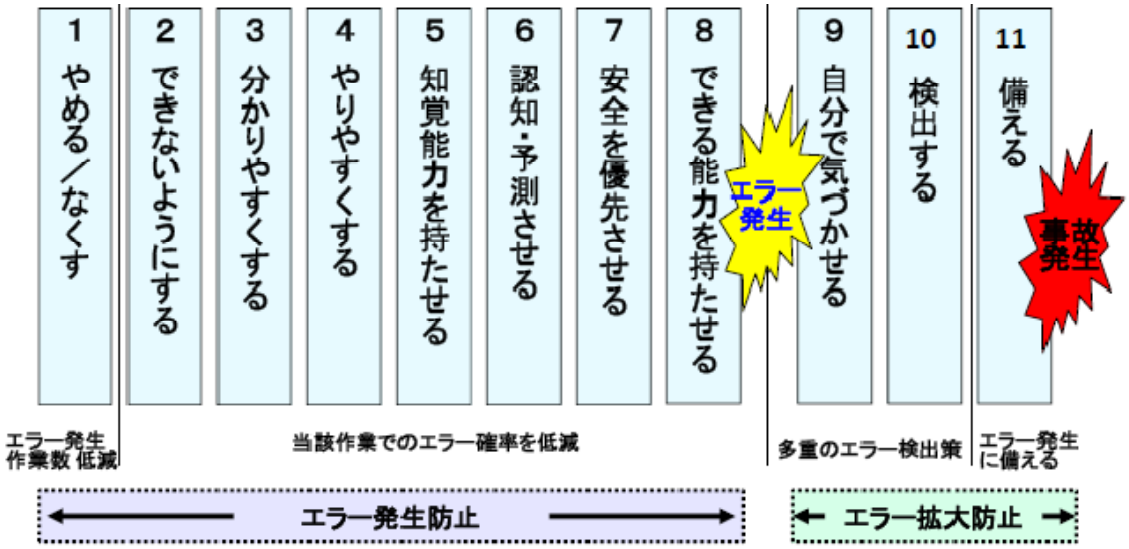

図８事故防止・再発防止

（３）教育・訓練方法について

① 危険予知訓練（KYT：Kiken Yochi Training）

行動変容を起こすための教育・訓練方法として、危険予知訓練も有効であると考えている。情報セキュリティ分野では、まだ多くの実績は報告されていないが、知識の定着率は高い[13]。動画や画像を取り入れた e-Learning だけでなく、集合教育でも可能である。

② 潜在連合テスト（IAT：Implicit Association Test）

IAT は、1998 年グリーンワルド（Greenwald）とバナジ(Greenwald and Banaji)が開発したもの。情報セキュリティ教育に関連して、教育効果測定に可能ではないかと考えているが、現時点では試行の段階である。2009 年に修士論文[13]で行ったが、明確な結論が得られなかった。どの様な方法で適用するのか、どの様な対象者を想定するのか等と言った点等、IAT を情報セキュリティ分野に利用するのであれば、更なる調査研究が必要であると考えている。

３．犯罪防止と情報セキュリティ

３.１ 犯罪機会論

（１）犯罪機会論と性弱説

犯罪者に犯罪の機会を与えないことで、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。

犯罪は「この場所」で起こる

	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

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、犯罪防止を図ることが可能になる。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、情報セキュリティでも同じように考えることができる。犯罪者の標的と犯行の場所についての考え方もある[10]。

また、犯罪機会論を性弱説で説明することも可能であろう。ここで、性弱説は、元来人間の心は弱いものである。目の前に大金が落ちており、誰も見ていない環境と思われた時に、果たして正常心でいられるだろうか。人間は環境によって結果的に犯罪を行う可能性を否定できないと言った内容である。

犯罪機会論＝性弱説（性悪説、性善説でなく）の例？

見知らぬ所で、周りを見回して誰も近くにおりません。ふと見るとお金が落ちていた。ざっと見るとＸＸ円ありそうだ。この時、あなたは以下のどれをとる可能性があるか？

1. 拾って警察に届ける
2. 自分の懐に入れてしまう
3. 無視してそのままにする

また、この時の金額によって、１～３で変化があるか？

ここで「お金」を情報に置き換えれば、情報セキュリティの問題として考えることができる。

（２）環境犯罪学

犯罪機会論や性弱説の考え方は、人が犯罪を行おうとする考えを何等かの方法でとどめる（あきらめさせる）ことが大切になる。1971 年に Ray Jeffery が環境的に犯罪予防を行うことを理論付け、CPTED（Crime Prevention Through Environmental Design）と呼ば

れる。CPTED は、「防犯環境設計」等と訳されているが、建物、地域等の環境が抱える犯罪誘発要因を分析・排除するものである。

例えば、公園に面した道路には車両の速度を制御（遅くする）する仕組みや植栽を低くして道路から公園内の見通しを確保する等がある。また、コンビニエンスストアでは、レジを道路側から見えるような配置している。

情報セキュリティに関連する設備では、コールセンターでの対応を周りから見えるような設計をして、不正等ができない仕組みを構築しているものもできており、CPTED の考えを取り入れた設計が行われている。

（３）教育・訓練による犯罪防止

現在の電子メールは多くの技術を駆使して、不正メールを利用者まで届かない工夫をしていることは、「１.１　情報セキュリティ」で述べたが、技術だけでは防ぐことができないメールを個々の利用者の判断だけに任せる訳にはいかない。何等かの教育・訓練も企業・団体等では必要になるが、その一例として、「予防接種」というアプローチにより利用者の訓練も行われている[11]。技術的な対応だけでは防ぎきれないものを人智により排除しようという訓練である。

（４）割れ窓理論／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、情報セキュリティ分野等、他の分野でも適用できると考えている。

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）」[12]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。

情報セキュリティ事故（インシデント）報告に活用することが大切であるが、大量のインシデントが分析者には集約した形でしか集まらない。あるいは、現場からの報告内容が集約され、送付されるといった問題が情報セキュリティ分野でも行われていることが、大企業等へのインタビュー等で判明している。

このため、インシデント件数が一定以下に減少しないとか、的を射た対策が行わないという問題があることが判明しており、他分野と同じ課題が情報セキュリティ分野にもある

ことがわかっている。

（5）プロファイリング

プロファイリングという言葉から、直ちに「犯罪者プロファイリング」という言葉を連想しがちであり、「2．1 （2）内部犯行者の分析」で、情報セキュリティ分野でも内外で、犯罪者プロファイリング的なことが行われている。ただ、国内では研究者が情報セキュリティ犯罪者のプロファイルを収集することは多少困難な面もあり、警察関係者等の法執行機関等での研究を期待したい。

情報セキュリティを考える場合、企業・団体での重要情報を扱う必要があるため、適切な要員であるかについて何等かの対応が必要なのではないだろうか？

実際にあったケースだが、業務上、ノート PC を持ち出して業務を行わなければならない立場の従業員がたびたびノート PC を紛失したことが発覚した。ユーザ ID／パスワードの設定、保存ファイルの暗号化等は行っていたが、何度目かの時点で、その従業員をノート PC の持出が不要な職場に異動させた。

これは、極端な事例かもしれないが、従業員の教育・訓練が第一であるが、情報の取扱についての適性を考える必要もあるのではないかと感じている。

4．今後の課題

情報セキュリティは新しい分野であり、国内では暗号やネットワーク技術者が中心に研究を行ってきたこともあり、人間に関係した調査研究、実践はあまり進んでいない。

また、インターネット等を利用した ICT は危険が多いとの指摘もあるが、情報セキュリティ研究を行っている者としては、多くの企業・団体を含め、人々にリスク認識が薄いことが問題なようにも思われる。

最初に取り上げたメールについても、技術を含めて考えると、多くのものは阻止可能ではないだろうか。　例えば、企業・団体のメールアドレスを詐称して送られてくるターゲット型メールと言われるものは、ISP や企業・団体のサーバで 100%阻止可能であろう。

技術で対応すべきもの、人々が持つ知見で対応すべきものをもう少し明確にすることが必要なのではないかと考えている。

心理学、行動科学、犯罪学等、他の分野での知見を情報セキュリティに取り入れていく必要があるのではないかと考えている。

参考資料

[1] 人間と工学研究連絡委員会 安全工学専門委員会、「安全・安心な社会構築への安全工学の果たすべき役割」、日本学術会議、2005 年
http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-19-t1034-1.pdf

[2] 岡本浩一「リスク心理学入門 6章：リスクとマスコミ」サイエンス社 2004年
[3] 未来科学技術共同センター「組織マネジメントプロジェクト」
http://www.procom.niche.tohoku.ac.jp/index.php
[4] ナイトメア「シークレット・オブ・スーパーハッカー」日本能率協会、1995 年
[5] ケビン･ミトニック「欺術」ソフトバンククリエイティブ、2003 年
[6] G. Chapman「China Google cyberattack part of spying campaign: experts」2010 年
http://www.google.com/hostednews/afp/article/ALeqM5h2xYXYW0pSBOHaTYYcDsP5_cI31g
[7] ロバート・B・チャルディーニ「影響力の武器」2007 年9月 誠信書房
[8] （独法）雇用･能力開発機構 職業能力開発総合大学校能力開発研究センター「訓練効果測定に関する調査・研究」（6章 研修評価と効果測定の一般的な考え方と進め方）2005 年
[9] 河野龍太郎、「医療におけるヒューマンエラー」 医学書院、2006年
[10] 小宮信夫、「犯罪は「この場所」で起こる」、光文社新書、2005年
[11] 山口健太郎、「ユーザへの予防接種というアプローチによる標的型メール攻撃対策」日本心理学会、2010年
[12] G. L.Kelling、J. Q.Wilson、「Broken Windows」、The Atlantic Monthly, 1982
(http://www.theatlantic.com/magazine/archive/1982/03/broken-windows/4465/)
[13] 大和田竜児、「従業員のリスク行動に対する企業の取り組みに関する提案」、防衛調達基盤整備協会「情報セキュリティに関する懸賞論文」、2009年