情報セキュリティ心理学とトラストの動向について

～情報セキュリティ心理学とトラスト(SPT)研究グループの活動～

2008年05月22日

内田 勝也
情報セキュリティ大学院大学
uchida@iisec.ac.jp

本日の発表内容

- 今、なぜ、情報セキュリティ心理学・トラストか？
- ソーシャルエンジニアリング
- 情報セキュリティは技術対策なのか？
- 人間の記憶について
- 人間の行動特性を考える
- 内部犯罪者の研究
- 環境犯罪学
- リスク心理学
- 組織の心理学
- 事故防止・再発防止のための分析
- 今後の課題

Katsuya Uchida uchidak@gol.com

何故、情報セキュリティ心理学か

CSI Conference

学会でなく、民間のセキュリティ団体であるが、情報セキュリティを「技術」としてでなく、技術、管理・運用、法制度等のバランスがとれている

	セッション数	割合（%）	
マネジメント系（M）	２０	２１．７	４３．４
マネジメント系（M＋）	２０	２１．７	
技術系（T）	９	９．８	３２．６
技術系（T＋）	２１	２２．８	
M&T	１５	１６．３	
M ＆ T＋	２	２．２	
M＋ ＆ T	５	５．４	
セッション数合計	９２		

注） 2007年11月（第34回）のConferenceの内容区分。 一部のセッションは2コマ実施ているが、1つとしてカウントした。
なお、マネジメント系に法制度も含めてある

2000年のConferenceの12トラック（各トラックは10セッションある）
Introduction to Computer Security
Awareness
Management
World Wide Web
E-Commerce
Tools & Techniques
Audit & Risk
Product Specific
Network Security
Round Tables
Infrastructure
Tracklets

Katsuya Uchida uchidak@gol.com

情報セキュリティ心理学とトラストの動向について

何故、情報セキュリティ心理学か

コンピュータ犯罪者像

- コンピュータ犯罪者・・・・・
  15～45歳の男性（女性も増えてきたが）。コンピュータの専門知識はさまざまで、過去の犯罪歴はほとんどない。個人的な資質としては頭脳明晰，やる気があって企業にとって望ましい人間のように思われてきた。
  犯罪者のほとんどは、企業や政府機関内部で信頼される地位にあり、コンピュータシステムに簡単に接近できる。 朝早くから、夜遅くまで仕事をし、休暇をとることも少ない。

「1970年～80年代初に米国で起こった数百件のコンピュータ犯罪の犯罪者のプロフィール」。
⇒ 当時を考えると大部分は 内部犯行者 であろう。 内部犯行者のプロフィールと考えらる

August Bequai「How to prevent computer crime」John Wiley & Sons Inc 1983
堀部政男・堀田牧太郎 訳「情報犯罪」啓学出版 1986

米国メインフレーム時代の調査事例。
犯罪者のプロフィール分析が行われていた

Security First

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

Katsuya Uchida uchidak@gol.com

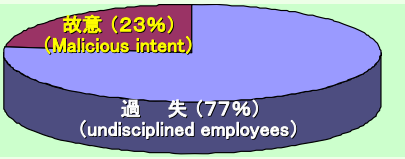
何故、情報セキュリティ心理学か

情報漏えいの原因

（1）InfoWatchの調査

- 2006年に世界各国で起きた情報流出事件のうち、1回でもメディアで取り上げられたケース145件の調査
- 流出原因は過失によるものが77%と圧倒的に多く、業種や地域による偏りは見られず、大企業や中小企業、政府機関、軍などでも流出が起きた

http://www.itmedia.co.jp/news/articles/0702/17/news011.html

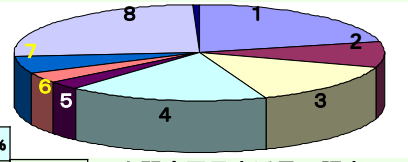


InfoWatchの調査
http://www.infowatch.com/threats?chapter=162971949&id=207784626

（2）内閣府国民生活局　個人情報の保護に関する事業者の取組実態調査 より

- 調査は平成19年3月実施、回答数4,060件（回収率 20.3%）

http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20070425kojin2.pdf



内閣府国民生活局の調査

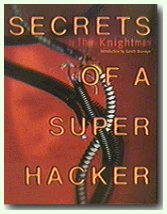
内閣府国民生活局の調査　漏えい発生原因	回答割合 %		
1. 従業者の置忘れ、施錠忘れ等の過失	21.3		1～3 合計 65 %
2. 従業者のインターネット利用上の過失（メール誤送信、HPへの誤掲載等）	8.6		
3. 従業者（含 退職者）が盗難にあった（含 車上荒し等）	14.2	(44.1)	
4. 委託先・運送業者の漏えい等	17.6	61.7	4～6 合計 35 %
5. サーバ／PCへの攻撃（ハッキング・ウイルス感染等）	2.8		
6. 従業者の個人情報持出し、売却・譲渡・漏えい等	3.6	6.4	
7. 原因は未だに不明である	5.4	5.4	
8. その他	25.8	25.8	
9. 無回答	0.7	0.7	

Katsuya Uchida　uchidak@gol.com

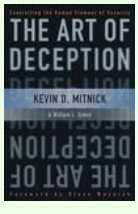
ソーシャルエンジニアリング

ソーシャルエンジニアリング（Social Engineering）

- 侵入するシステムにアクセスできる正当な権限を持っている人間の心理的な弱さを利用して、侵入するために必要な情報を取得する方法をソーシャルエンジニアリング（Social Engineering）という
- 侵入者にとって、困難な所から侵入を図るより、より楽な方法で侵入ができる方法が分かっていれば、そこからの侵入を図るのは、現実の世界でも、サイバーの世界でも同じ
- 情報システムの中で最も弱い部分（脆弱性）は、人であると言われている。 侵入者が権限を持った人から得た情報は目的とするシステムへ入るための正規の情報であるので、侵入者は正面からシステムへ侵入できる



- Knightmare, “Secret of a 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



- Kevin D. Mitnick , William L. Simon, “The Art of Deception” Wiley, 2002
  岩谷 宏 訳, “欺術”,ソフトバンククリエイティブ, 2003

Katsuya Uchida　uchidak@gol.com

情報セキュリティ心理学とトラストの動向について

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（Social Engineering）

- ソーシャルエンジニアリングの手法には、色々な方法がある
- それらの方法を単独で利用したり、いくつかの手法を組み合わせて行うことがある
- １人の人に対して行うだけでなく、複数の人に対して行うことにより、それらをまとめて目的情報を取得することもある
- 主な手法としては、以下のようなものがある。
  - （1）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
  - （2）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
  - （3）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
  - （4）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
  - （5）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

攻撃者だけに有効なツールを利用させておくことはない！

Katsuya Uchida uchidak@gol.com

情報セキュリティ心理学とトラストの動向について

ソーシャルエンジニアリング ～ 人間固有の脆弱性を突く ～

6つの人間の脆弱性（Six "weapons of influence"）

1. 返報性[Reciprocation]：親切や贈り物、招待等を受けると、その人にお返ししたくなる気持ち
2. コミットメントと一貫性[Commitment and Consistency]：自分の意志による行動がその後の行動に拘束をもたらすもの。 以下の3つの手法がある
   - ①ローボールテクニック：最初にある「決定」をさせるが、それが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。 例：特売商品購入客に、購入手続きの最中に在庫がないが、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
   - 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、できない場合、負担の軽い要求をだして、実現させる。 例：法外な借金依頼を行い、断られたら少額の借金を承諾させる
   - ③フット・イン・ザ・ドア テクニック：最初に誰も断らない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。 例：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
3. 社会的証明[Social Proof]：他人の考えにより、自分が正しいかどうかを判断する特性
4. 好意[Liking]：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
5. 権威[Authority]：企業・組織の上司等権威を持つ者の命令に従ってしまうこと
6. 希少性[Scarcity]：入手し難い物であるほど、貴重なものに思え、手に入れたくなってしまう特性

Robert B. Cialdini, "INFLUENCE – Science and Practice", Collins, 1988
社会行動研究会 訳,「影響力の武器」, 誠信書房, 1991

Katsuya Uchida uchidak@gol.com

ソーシャルエンジニアリング ～ その対応のいくつか ～

これら人間の脆弱性を考慮した情報セキュリティ対策への試み

- ソーシャルエンジニアリングの研究
  - Mr. Jonathan J. Rusch (US DoJ) “The ″Social Engineering″ of Internet Fraud”
    http://www.isoc.org/inet99/proceedings/3g/3g_2.htm
- 企業・組織における教育・周知等での利用
  - 山口健太郎(情報セキュリティ大学院大学) ”情報セキュリティの効果的な研修スキームの提案 ～心理学的アプローチを適用した試み～” 日本セキュリティ・マネジメント学会 全国大会 2007年6月
- アクセスコントロールへの利用
  - 矢竹清一郎(情報セキュリティ大学院大学) “ソーシャルエンジニアリングの分析およびアクセス制御の提言” 情報処理学会 コンピュータセキュリティ研究会(CSEC) 2007年7月
- その他
  - コールセンター等へのソーシャルエンジニアリング攻撃に対して、リアルタイムでその分析を行い、判断できるのではないかと机上での研究がPurdue大学で行われた
    http://www.cerias.purdue.edu/news_and_events/events/symposium/2005/materials/pdfs/D04-6B4.pdf

技術的対策なし？ Winny 関連暴露ウイルス

Winny関連暴露ウイルス

- ウィニーウイルス猛威、対策手詰まり――官公庁や企業、止まらぬ情報流出
  - 捜査資料流出:ネット上に誘拐事件対応文書も 愛媛県警 (2006年3月発覚)
  - 捜査資料流出:流出元はセキュリティー指導員 岡山県警 (2006年3月発覚)
  - 私物パソコン使用禁止 ・・・ 各省庁、情報流出対策急ぐ
  - 私用パソコンで情報を扱うミスが原因で、「決め手はなく、個人のモラル頼み」と戸惑っている
  - 情報漏えいを防ぐ最も確実な対策は、パソコンでWinnyを使わないこと。 私(官房長官)からも国民の皆さんにお願いしたい(2006年3月15日:官房長官声明) http://www.kantei.go.jp/jp/tyoukanpress/rireki/2006/03/15_a.html

流出やまず

- 陸上自衛隊:ミサイル資料流出(2006年5月12日)
  陸上自衛隊配備の地対艦誘導ミサイル運用システム等に関する内部教育用資料が、ファイル交換ソフト「Share」でネットに流出。「秘」情報が含まれているか不明だが、「秘事項が多いので諸元(ミサイル性能等の数値)等は他言しない」との注意書きがあるファイルも。 防衛庁は「Winny(ウィニー)」を介した相次ぐ重要情報の流出を受け、4月に再発防止策の最終報告をまとめたばかり。今回の流出は5月初旬とみられ、情報管理が改めて問われるのは必至
  http://www.mainichi-msn.co.jp/today/news/20060512k0000m040171000c.html
- イラク米軍 配置情報流出、空自隊員のパソコンから(2006年11月29日)
  イラクに展開する米軍の6―7月の人員配置等の情報が、航空自衛隊那覇基地所属の幹部隊員の私物PCから今月24日、ファイル交換ソフトを通じてインターネット上に流出
  http://it.nikkei.co.jp/security/news/index.aspx?n=SSXKD0902%2029112006
- 陸自の内部資料、ウィニー通じて流出 (2007年2月3日)
  陸上自衛隊の訓練などに関する内部資料が、陸自第14旅団(香川県)に所属する三等陸曹の私物パソコンから、ファイル交換ソフトを通じて昨年8月に資料が流出
  ttp://it.nikkei.co.jp/security/news/sec_virus.aspx?n=SSXKG0022%2003022007
- 1万件の捜査情報流出 警視庁、巡査長のPCから(2007年6月13日)
  警視庁北沢署の巡査長が、個人所有PCから警察内部文書(取り調べ調書、捜査関係事項照会書等)をファイル交換ソフトを通じ、文書約 9,000件と写真約 1,000件を流出。 巡査長は、同僚の巡査部長から外付けハードディスクを借り、自宅のパソコンに取り込んでいた
  http://it.nikkei.co.jp/security/special/winny.aspx?n=NN000Y692%2013062007

人間の記憶について

理由を明確化させることにより、人の記憶は確かになるのだが・・・

記銘時のエラー（記憶について）

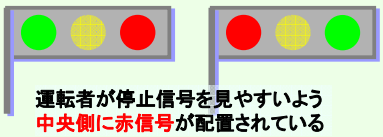
- 記憶の過程には、記銘（符号化）、保持（貯蔵）、想起（検索）の三段階がある
- 記銘は、記憶の第１段階で新しい情報を覚えることで、
  - 意識的に記憶しようとして覚える場合と
  - 自然に記憶に残る場合がある

  この場合でも、刺激の中の注意を向けた特徴だけが記憶にとどまる

駐車禁止マーク

駐車禁止マークは、「No」をイメージして作成（？）

交通信号（日本）



運転者が停止信号を見やすいよう
中央側に赤信号が配置されている

- 上の2例のように、漠然としており、その意味等に注意を向けられていないため、記銘されていないことが考えられる。
- 最初から「覚えていない」タイプの記憶エラーでは、その時には何も役立たない

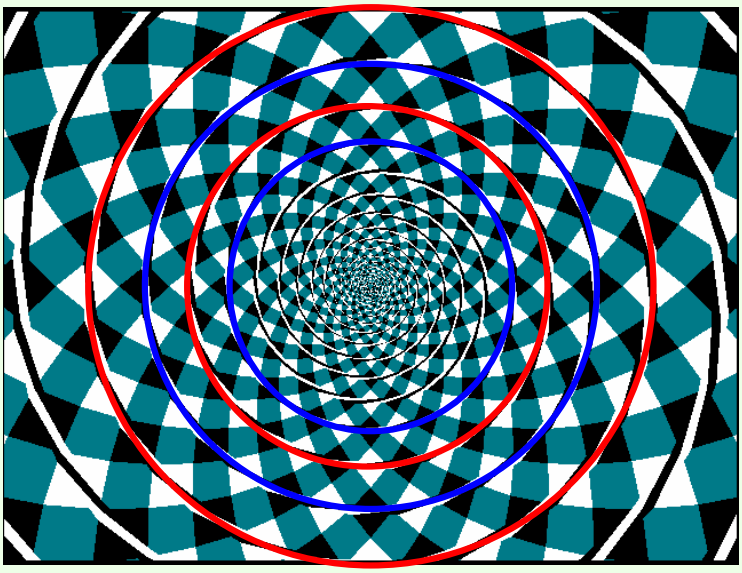
覚えさせない？

芳賀繁「ヒューマンエラーのメカニズム」（大山正・丸山康則 編「ヒューマンエラーの科学」）

Katsuya Uchida uchidak@gol.com

人間の記憶について

人は何故ミスをするのか（経験は有用）？



フレーザーの錯視

- 左図では、誰にも渦巻きにみえるが、実際には同心円になっている。
- 人間の五感は騙されやすいが、このような図が錯視の可能性があることを知っていれば、渦巻きにみえる部分を実際になぞることで、錯視かどうかの判断をすることが可能であろう。

経験したことのない問題では、正しい判断をすることは困難であるが、過去に経験があれば、確認することで、誤った判断を防ぐことが可能になる

Katsuya Uchida uchidak@gol.com

人間の行動特性を考える

企業・組織でのパソコンの持ち出し禁止

- 個人情報保護の高まり等から、企業や政府・自治体ではパソコンの持出を禁止令がでているが、それで業務活動などが円滑でできるだろうか？
- 全ての従業員がそれで問題ないので、あればいいのだが・・・
  - ◆ 電車内にパソコンを忘れてしまう人の特質を考えた管理方法を考えることも必要では？
  - ◆ また、車内に置いたパソコンや重要書類が車上荒らしにあうことも多いようであるが、そのためには何を考える必要があるだろうか？

➢ 電車内にパソコンを忘れる人の多くは、以下のような方が多い

① 普段、何も持たない
② 電車内で荷物を網棚に上げ、座っても荷物を膝上に置かない
③ パソコンを持っているのに、お酒を飲んで帰る
④ 荷物を2つに分けて持たなければならない場合

もちろん、それでも忘れる人はいるので、ファイルの暗号化等は必要であろうが

➢ 車上荒らしにあう場合・・・

パソコン、アタッシュケース、重要そうな書類封筒を助手席、後部座席に残している

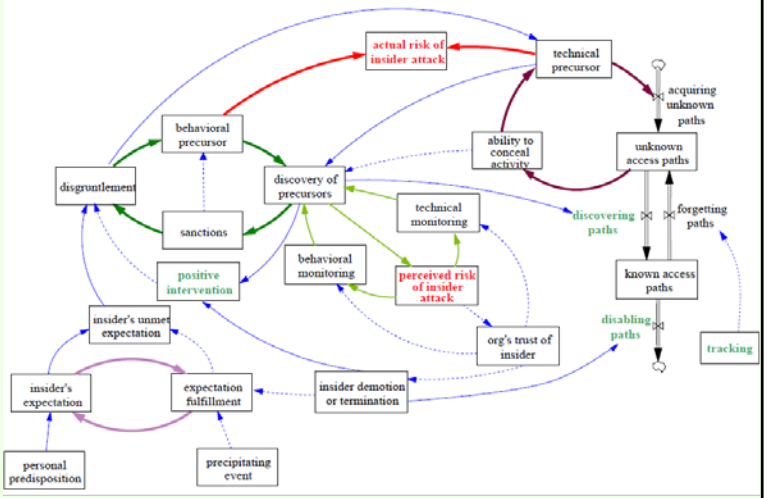
① トランクやダッシュボードにいれることで、車上荒らしにあう可能性を減らせる
② 大きな駐車場では、駐車場所も重要になる

内部犯罪者の研究

MERIT(Management and Education of Risks of Insider Threat)

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。
これから，Carnegie Mellon大学CyLab では，MERIT 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をシステムダイナミックス等を使って行っている。

MERIT Model – Extreme Overview



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

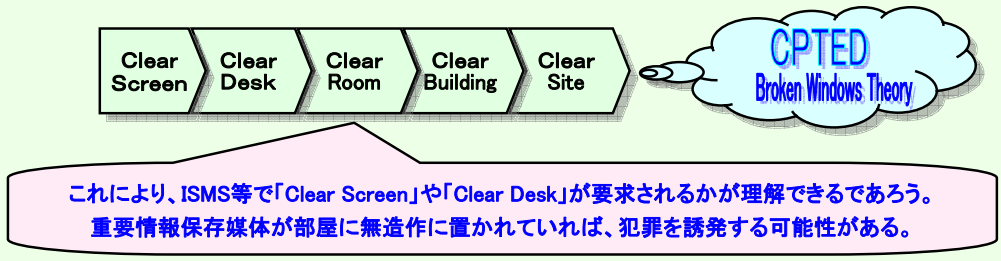
環境犯罪学

環境設計による犯罪予防（CPTED）

- 物理的セキュリティを考える場合の対策として、コンビニエンスストア等の設計に利用されている。敷地、建物、データセンター、オフィス等設計にも利用されている。

割れ窓理論（Broken Windows Theory）

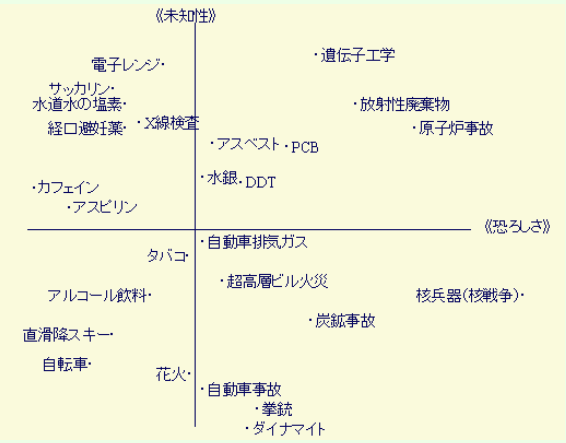
- 人は匿名性が保証されている・責任が分散されているといった状態におかれると、自己規制意識が低下し、「没個性化」が生じる。その結果、情緒的・衝動的・非合理的行動が現われ、又、周囲の人の行動に感染しやすくなる。（心理学者フィリップ・ジンバルド：Zimbardo, Phillip. G. 1969）
- ビジネス界においても割れ窓理論を適用して成功を収める例が増えている。日本のテーマパークの経営では、些細な傷をおろそかにせず、ペンキの塗りなおし等の修繕を惜しみなく夜間に頻繁に行うことで、従業員や来客のマナーの向上をその成功の果実として手にしている 割れ窓理論 – Wikipedia



リスク心理学

リスク認知

リスクの認知には、「恐ろしさ」と「未知性」の2つの因子により認知図の作成が可能。 認知図は個人差（専門家、素人、知識の有無等）や国民によっても異なる



アメリカ人のリスク認知，Slovic(1986)

クライシスコミュニケーション

事件・事故発生時のマスコミ対応も大切になる。 マスコミ報道は多くの人達に大きな影響を及ぼすものであり、マスコミ人の考え方、報道姿勢等についての研究も必要であろう

岡本浩一 リスク心理学入門

組織の心理学

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」)

個人的違反と組織的違反

- 「個人的違反」: 職務怠慢や備品の私物化に代表されるもの
- 「組織的違反」: 組織や職場の利益を上げる目的での違反。 作業の効率化やコスト削減を目的として、組織の利益を上げるために行う違反
  - 安全文化(Safety Culture): 国際原子力機関(IAEA)が国際安全基準として示した
  - 厚生労働省「安全な医療を提供するための10の要点」での安全文化

これらでは、事故・不正を防止するには、組織風土の重要性の認識が高まっている

国際原子力機関(IAEA)の国際原子力安全諮問グループ(INSAG)がまとめた報告書(1991年)によれば、「安全文化」とは「『原子力施設の安全性の問題が、すべてに優先するものとして、その重要性にふさわしい注意が払われること』が実現されている組織・個人における姿勢・ありようを集約したもの」である。「安全」とは、技術的な意味で原子力施設を運転しても、放射能漏れなどの事故を引起こす危険がないことをいう。原子力施設の「安全」は、施設の設備の健全性と、施設の運転管理をする人間の「安全文化」の徹底によって実現されるものである。そして、このような努力により「安全」を積み重ね、また、事業者や規制機関が情報公開を行っていくことで、地元の人々に「安心」を提供することができる。

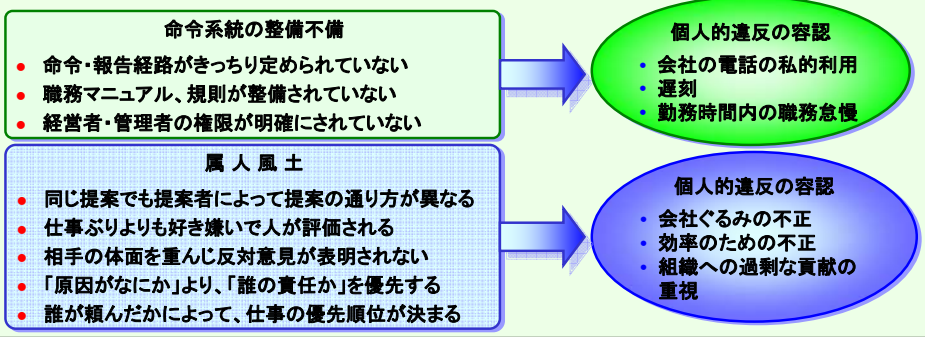
組織の心理学

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」)

組織違反について

- 組織違反の特徴の1つに「無責任の構造」がある
- 無責任構造を生みだし易い組織風土の特徴は、「属人主義」がある
- 属人主義: 評価・決定時に、「誰がそれを行っているのか」という、人情報を重視する傾向が強い。これを「属人風土」と呼ぶことにする
  - 会議・ミーティングでは、同じ提案でも誰が提案者かによって、提案の通り方が異なる
  - 仕事ぶりよりも好き嫌いで人を評価する傾向がある
  - 相手の体面を重んじ、会議・ミーティング等で反対意見が表明されないことがある
  - トラブルが生じると、『原因が何か』より『誰の責任か』を優先する雰囲気がある
  - 誰が頼んだかにより、仕事の優先順位が決まることが多い

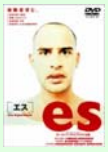
違反者が属人風土から受ける圧迫感は個人の倫理観だけでは解決できない?



組織の心理学

組織の問題

- 組織としての問題は、個人の人格が場面、相手、状況等により変化することにある
- 社会的に、あるいは客観的にみて、極端に悪い方向に向かうことがあるが、各個人がそれを打ち破ることができないことが多い



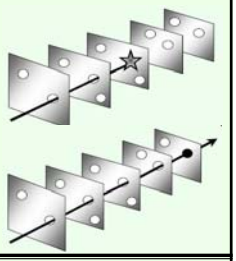
スタンフォード監獄実験

1971年8月14日から1971年8月20日まで、米国スタンフォード大学心理学部で、心理学者フィリップ・ジンバルド(*Philip Zimbardo*)の指導の下、刑務所を舞台にし、普通の人が特殊な肩書きや地位を与えられると、その役割に合わせて行動してしまう事を証明しようとした実験

倫理的意思決定方法

- 普遍化可能性(Universalizability)テスト: 皆がそれを行ったらどうなるか？⇒例:「データ改ざん」
- 可逆性(Reversibility)テスト: 自分が逆の立場でもそれを行うか？

スイスチーズモデル



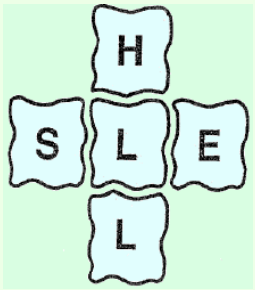
- セキュリティ防御やエラーに対応するために、階層的な防御を行うことにより、事故等への対応を行う(多層防御)
- 各層での防御は完璧ではないため、チーズの穴(防御が不十分な所)がたまたま重なって所をくぐり抜けてしまう場合に事故が発生する
- 多層防御をくぐり抜けてしまわないような体制(対応)を考えることも大切

Katsuya Uchida uchidak@gol.com

事故防止・再発防止のための分析
SHELモデル分析

Event	SHEL	要因	対策例
手術室交換ホールにおいて、患者及びカルテの受け渡しをする際に患者を誤認し別の手術室に移送した	L−S	患者(A氏)にB氏の名前を呼びかけたところ返事をしたことから、患者がB氏であると思いこんだ	患者本人に名前を応答させることにする
	L−H	患者を受け渡すハッチウェイとカルテの受け渡し台が別々になっていたことが、患者からカルテが離れる原因になった	カルテの受け渡し台は使用せず、ハッチウェイにおいて、患者及びカルテを受け渡すことにする
	L−E	朝の看護業務が多忙であったため、1名ずつ移送すべきところを、看護婦1名が2名の患者を移送した	業務量に応じて手術日朝の看護体制を見直し、1名ずつ移送できる体制にする
	L−L	病棟看護婦と手術室看護婦の間で、確認作業を行わなかった	病棟看護婦と手術看護婦が患者の名前の復唱などにより共同で患者確認を行うことにする

- SHELモデルは、1972年にイギリスの学者であるエドワーズが原型を提案し、1975年にオランダのKLM航空の機長であったホーキンズ が改良を加えて完成させたものである。SHELモデルでは、右図のようにシステムを図式化し、システムの中心に人間(L-Liveware)、その周囲にソフトウェア(S-Software)、ハードウェア(H-Hardware)、環境(E-Environment)及び人間(L-Liveware)を配置している
- このモデルを用いて、上図のとおり事故・インシデントの分析を行うことが、航空業界において推奨されている。その分析に当たっては、中心のL自体の問題と併せて、L-S、L-H、L-E及びL-Lのそれぞれのインターフェースに問題がなかったかを分析し、その結果に基づいて改善方策を検討することになる。



http://www1.mhlw.go.jp/houdou/1105/h0512-2_10.html

Katsuya Uchida uchidak@gol.com

事故防止・再発防止のための分析
Medical SAFERでの分析手順

ヒューマンエラーにおけるエラー分析

河野龍太郎「医療におけるヒューマンエラー」医学書院 より

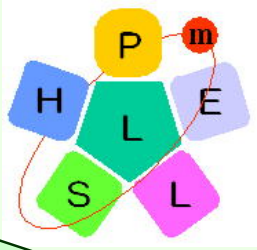
手順１　事象の整理	事象を整理し、何がどのように発生したかという事実を把握する
手順２　問題点の抽出	事象をよく理解して、含まれている問題点を抽出する
手順３　背後要因の探索	なぜ、そのような問題が発生したかを推定、調査する
手順４　対策案の列挙	実行可能性を考えず、その問題や背後要因をなくす対策を列挙する
手順５　実施する対策の決定	現実の制約を考え、実施する対策を決定する
手順６　対策の実施	誰が、いつまでに、どのように、ということを具体的に決め、実施する
手順７　対策の効果の評価	実施した対策の効果、新たな問題等を評価する

Katsuya Uchida　uchidak@gol.com

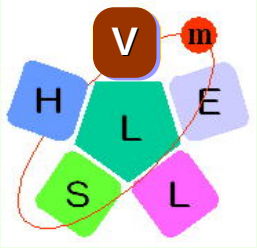
事故防止・再発防止のための分析
V−mSHELLモデルによる分析

ヒューマンエラーにおけるエラー分析
（背後要因関連図の作成） P−mSHELLモデル

要　素	例
P: patient 患　者	● 症状 ● 心理的・精神的状況 ● 価値観
m: management 管　理	● 組織・管理・体制 ● 職場の雰囲気作り ● セーフティカルチャーの醸成具合
S: software ソフトウェア	● マニュアル ● チェックリスト ● 教育・訓練用教材
H: hardware ハードウェア	● ヒューマン・マシン・インターフェース（操作スイッチや計器など） ● 自動化レベル
E: environment 環　境	● 作業環境（温度・湿度・照明・騒音） ● 作業特性（緊急作業など）
L: liveware 本人（中心のL）	● 身体状況 ● 心理的・精神的状況 ● 能力（技能・知識）
L: liveware 周りの人（右下のL）	● コミュニケーション ● リーダシップ ● チームワーク



P: patientを被害者（Victim）に置き換えて考えてみると・・・



河野龍太郎「医療におけるヒューマンエラー」医学書院 より

Katsuya Uchida　uchidak@gol.com

今後の課題

- 体系的な整理を考える必要がある
- 心理学分野の知見を情報セキュリティ分野での事例に適用させて確認を行う
- 心理学分野を体系的にみながら、残している分野の研究を行う必要がある
- 心理学分野の研究者との交流

参考資料

- リン・シャープ・ペイン著 バリューシフト 毎日新聞社
- ロバート・チャルディーニ著 影響力の武器 誠信書房
- 大山正、丸山康則編 ヒューマンエラーの科学 麗澤大学出版会 2004年
- 大山正、丸山康則編 ヒューマンエラーの心理学 麗澤大学出版会 2001年
- CERT/CC Insider Threat Research http://www.cert.org/insider_threat/
- CIAO Practices for Securing Critical Information Assets Critical Infrastructure Assurance Office 2000
- Michael Erbschloe Physical Security for IT Digital Press 2004年
- 芳賀繁 失敗のメカニズム －忘れ物から巨大事故まで 日本出版サービス 2000年
- J. S. ジェラルド 交通事故はなぜなくならないか リスク行動の心理学 新曜社 2007年
- 岡本浩一 リスク心理学 サイエンス社 1992年
- 中谷内一也 リスクのモノサシ 日本放送出版協会 2006年
- 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
- 厚生労働省 患者誤認事故防止方策に関する検討会報告書 1999年 http://www1.mhlw.go.jp/houdou/1105/h0512-2_10.html
- 矢竹清一郎,内田勝也,森貴男,山口健太郎,東華枝 情報セキュリティ心理学の提案, 情報処理学会CSEC発表論文, 2007
- 矢竹清一郎 Social Engineeringの分析およびアクセス制御の提言 情報セキュリティ大学院大学 修士論文 2007
- 山口健太郎, 人間の行動特性を利用したセキュリティ研修効果向上方策の提案, 情報セキュリティ大学院大学 修士論文 2008
- 小林泰典, P2Pソフトウェアのウイルス感染についてのインシデント分析, 情報セキュリティ大学院大学 修士論文 2008

ありがとうございました

情報セキュリティ大学院大学
（http://www.iisec.ac.jp/）

内田　勝也

uchida@iisec.ac.jp
uchidak@gol.com
http://www2.gol.com/users/uchidak/