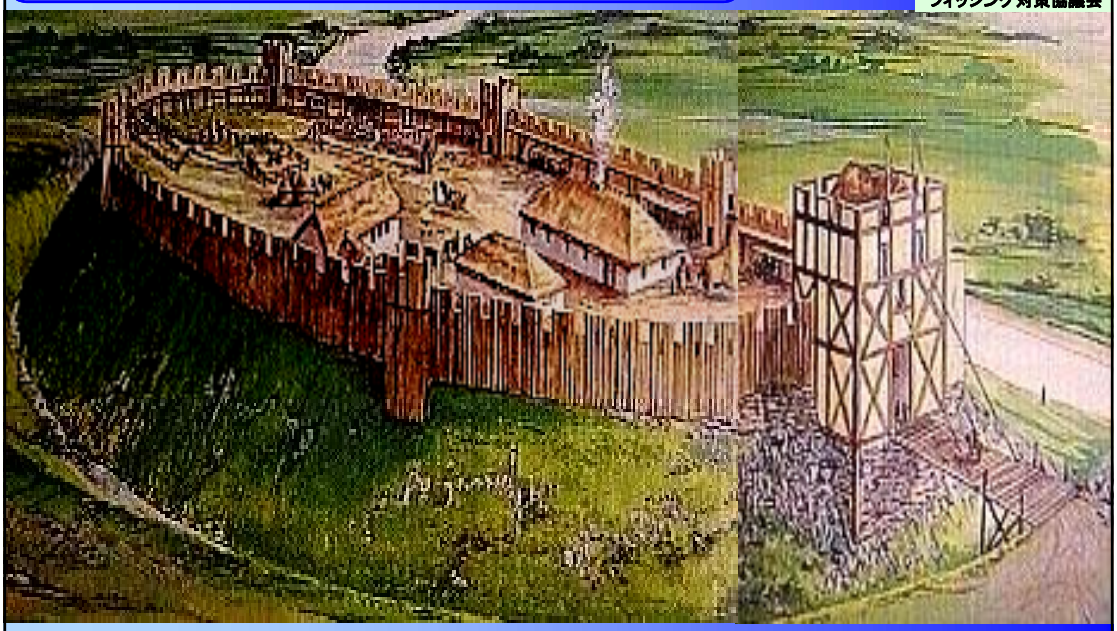
犯罪・犯罪予防を考える
～ オンライン犯罪を中心に ～

2009年10月06日
第2回情報共有勉強会
フィッシング対策協議会



情報セキュリティ大学院大学 & 横浜市CIO補佐監

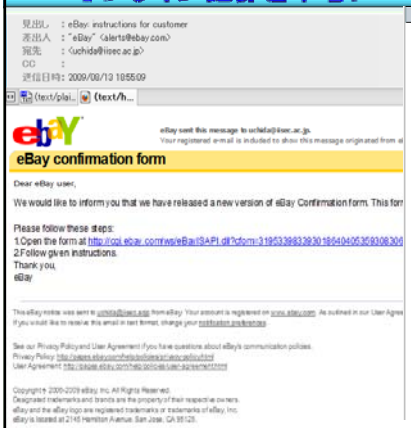
内田　勝也（uchidak@gol.com）

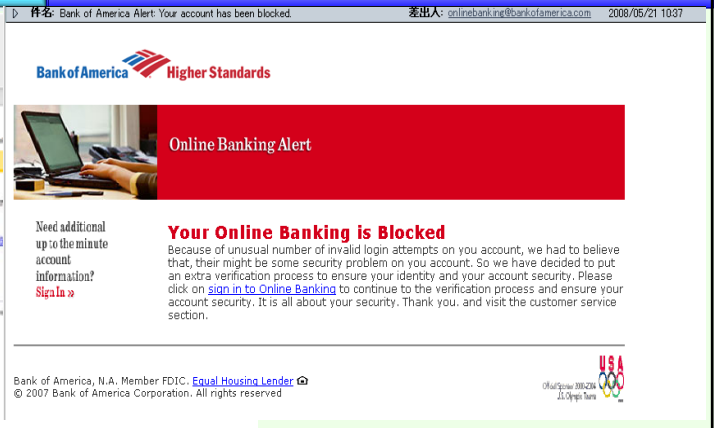
国内での分類を考える

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て、目的を達成する攻撃

- ソーシャルエンジニアリング
  - 広義のフィッシング
    - ネットワーク利用
      - メール利用
        - ウェブ利用
          - 狭義のフィッシング
          - フリーダイヤル利用
          - ワンクリック詐欺
            - 携帯電話利用
            - ウェブ利用
        - トロイの木馬（マルウェア：Malicious Software）
          - ターゲット型（スピア型）
          - 無作為型
            - キーロガー/スパイウェア – ID 盗難
      - ウェブ
        - トロイの木馬（Downward型マルウェア： Malicious Software）
    - 物理的機器の利用
      - Voice Phishing（ビッシング： Vishing）
        - 振込詐欺(電話 & ATM等の利用)
        - ID 盗難

英語のフィッシングメール





結構、多くのフィッシングメールが送られてきてるが、その多くは、日本語以外が多い

不幸（？）にして、最近指摘されている日本語のフィッシングメールは届いていません！

見出し	差出人	送信日時 △
2329	Michael Jacobs <extrextr@greenturtlebay.com>	2007/09/25 3:21:04
3367	Brian Beach <brandy@grapevine.ebay.sun.com>	2007/11/19 6:59:39
バイアアグラをオ&#1...	"Alfreda Reynolds" <pygmalionq146@ebay.de>	2009/02/14 17:58:19
バイアアグラ シア&#1...	"Twila Potter" <novass56@ebay.com>	2009/02/16 23:06:40
Fw:	"Suzanne Mckinnon" <truvniqipwex@bloomers.ebay.sun.com>	2009/06/09 2:44:29
New eBay form released Thu, 16 Jul 2009 06:27:07 -1200	"eBay" <alerts@ebay.com>	2009/07/17 3:27:07
urgent notification from customer service	"eBay" <alerts@ebay.com>	2009/07/18 4:13:43
official information	"eBay" <alerts@ebay.com>	2009/07/18 10:43:59
Important eBay mail (message ref: 6825008881)	"eBay" <alerts@ebay.com>	2009/07/18 16:35:37
important security update (message id: 5673323368)	"eBay" <alerts@ebay.com>	2009/07/18 23:04:26
security measures	"eBay" <alerts@ebay.com>	2009/07/19 4:29:48
important security update Sat, 18 Jul 2009 22:54:02 -0500	"eBay" <alerts@ebay.com>	2009/07/19 12:54:02
Security alert Sun, 19 Jul 2009 18:42:00 +0700	"eBay" <alerts@ebay.com>	2009/07/19 20:42:00
eBay: instructions for customer	"eBay" <alerts@ebay.com>	2009/08/13 18:55:09

電子メール ⇒ フリーダイヤル

BANKING INSURANCE INVESTMENTS

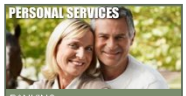
Home | News | Privacy | Alerts | Help | Contact Us

From: "AF Financial" <affinance@size.com>
To: <undisclosed-recipients>
Sent: Tuesday, May 13, 2008 9:12 PM
Subject: Telephone banking

We recently reviewed your account, and we suspect an unauthorized ATM based transaction. Therefore as a preventive measure we will temporary limit your access to sensitive features. To ensure that your account is not compromised please call our security center toll free at: +1-877 - 285 - 9764 and verify your identity to prevent deactivation.

If this is not completed by May 15, 2008, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes.
We thank you for your cooperation in this manner.
AF Financial Group, Customer Service.
If you do not have an account with us, please ignore this message as it has reached your email address by mistake. We are sorry for any inconvenience this may caused.
Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered.

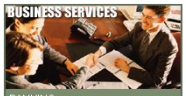
URGENT NOTICE: An email has been sent out saying it is from AF Financial Group with "Unusual purchase pattern" in the subject line. This email suggests that you call a toll free number to verify your debit card number, expiration date, and personal identification number (PIN). **THIS EMAIL IS A SCAM AND HAS NOT BEEN SENT BY AF BANK.** Please delete this email and do not call the phone number listed. If you have given out your debit card information please contact AF Bank Customer Support ASAP: 800-723-4718 or 336-246-4344.



BANKING:
Checking, Savings, CDs, Compare All Accounts, Consumer Loans, Mortgages

INSURANCE:
Auto Insurance, Homeowners Insurance, Health Insurance, Life Insurance, Bonds, Report a Claim, Samaritan's Purse Travel Protection, Request a Quote

INVESTMENTS



BANKING:
Checking, Compare All Accounts, Commercial Loans

BUSINESS INSURANCE:
Commercial Insurance, Group Health Insurance, Bonds, Report a Claim, Samaritan's Purse Travel Protection, Request a Quote

INVESTMENTS

Free Credit Report
Click Here

- 英語のメッセージだと、APWG_Japanにもまず届け出ない
- また、実際には、SPAMが多いため、メッセージを見逃しているケースも多々ある

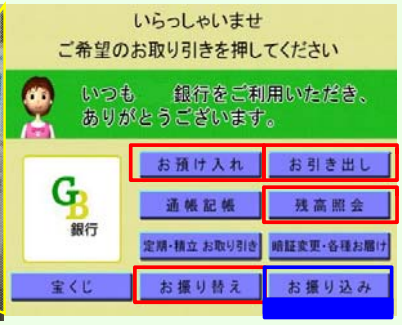
携帯電話のワンクリック詐欺

http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku35.htm

犯罪・犯罪予防を考える ～ オンライン犯罪を中心に ～

ATMの機能の相違

国内銀行のATM



海外（米国）のATM

- 現金引出
- 残高照会
- 預け入れ
- 振り替え

犯罪・犯罪予防を考える ～ オンライン犯罪を中心に ～

コンピュータウイルスについて

8. 感染台数

感染台数	届出件数 2009年8月		2009年7月（前月）		2008年8月（前年同月）	
0台	1,212	99.2%	1,248	99.4%	1,808	99.8%
1台	6	0.5%	5	0.4%	1	0.1%
2台以上　5台未満	2	0.2%	2	0.2%	1	0.1%
5台以上 10台未満	0	0.0%	1	0.1%	0	0.0%
10台以上 20台未満	1	0.1%	0	0.0%	0	0.0%
20台以上 50台未満	1	0.1%	0	0.0%	1	0.1%
50台以上	0	0.0%	0	0.0%	0	0.0%
合計	1,222		1,256		1,811	

これらの感染理由、感染経路等が分からないだろうか？

7. 感染（発見）経路別件数

メールにより感染（発見）したケースが最も多く、届出件数の約96%を占めています。

感染（発見）経路	届出件数 2009年8月		2009年7月（前月）		2008年8月（前年同月）	
メール	1,174	96.1%	1,182	94.1%	1,773	97.9%
ダウンロード（※）	4	0.3%	1	0.1%	1	0.1%
外部からの媒体	9	0.7%	9	0.7%	12	0.7%
ネットワーク	33	2.7%	62	4.9%	24	1.3%
不明・その他	2	0.2%	2	0.2%	1	0.1%
合計	1,222		1,256		1,811	

（※）ホームページからの感染を含む

http://www.ipa.go.jp/security/txt/2009/documents/virus-full0909.pdf

日米 セキュリティ調査

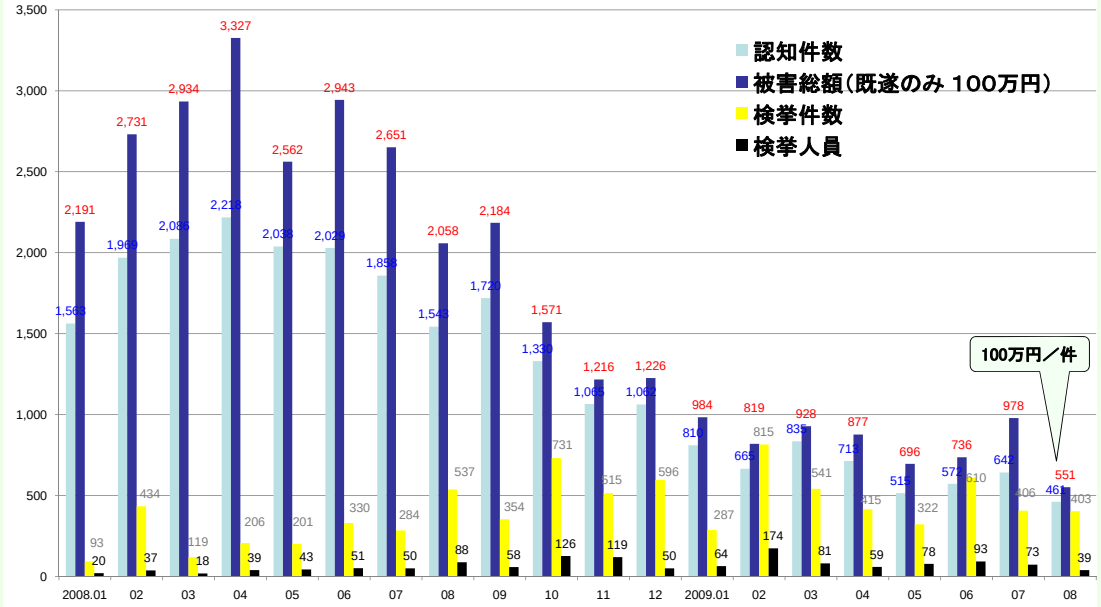
	2009J		2008J		2008C	
	順位	割合	順位	割合	順位	割合
ウィルス感染	1	50	1	60	1	60
発生していない	2	42	2	30	–	–
ノートPCの盗難	3	15	3	25	3	42
内部者のネット・アクセス乱用	4	10	4	16	2	44
Ｄｏｓ攻撃	5	7	5	9	6	21
		n=714		n=633		n=433

（注） 2009J, 2008J： 国内調査 （内田研究室）
2008C ： CSI 調査（http://www.gocsi.com/）

国内では、50%の企業がウイルス感染があると言っているが、
一方、40%以上がインシデント発生なしと回答している

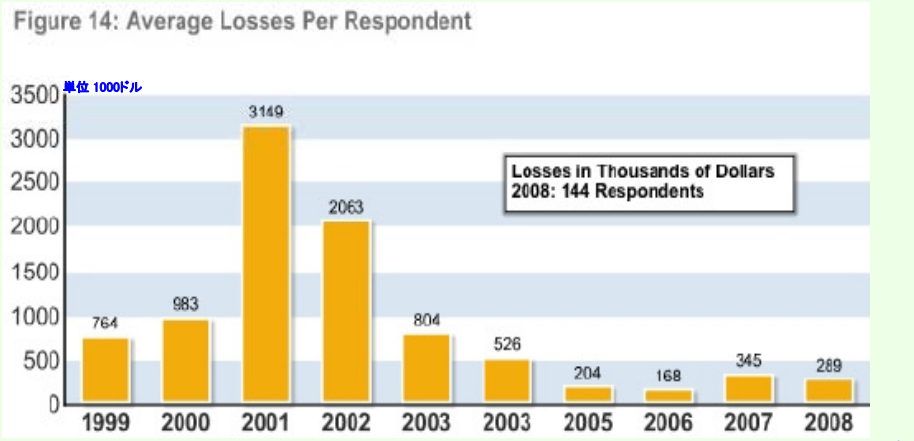
情報セキュリティ大学院大学 内田研究室
http://lab.iisec.ac.jp/~uchida_lab/

振り込め詐欺



http://www.npa.go.jp/sousa/souni7/furikome_H21_8.pdf

CSI 2008のインシデント費用損害



2,890万円／社

国内の費用損害は、1桁程度少ない

色々な統計資料について

色々な対策を考える場合、無尽蔵に投資できないのであれば、リスクの大きさを考えざるを得ないが、

- ZeroDay攻撃への対処方法：どんな方法が考えられるのだろうか？　技術的・人的面から
- 危なそうなURLへの対処方法：
- 多くの企業・組織がアンチウイルスソフトを導入しているが、何故、感染が多いのだろうか？
- 技術的な対応（ハード／ソフトの導入）の限界をどの様に見極めるのだろうか？
- どの様な教育・訓練が必要だろうか？

導入技術上位5位の経年変化（2009Jを基準に上位5位）

%

	2009J		2008J		2008C		2007C	
	順位	割合	順位	割合	順位	割合	順位	割合
ウィルス対策ソフト	1	98	1	99	1	97	1	98
ファイアーウォール	2	91	2	92	2	94	2	97
一般的なパスワード認証	3	81	3	78	14	46	9	51
アクセス制御	4	73	4	74	13	50	8	56
スパイウェア対策ソフト	5	60	6	54	4	80	4	80
VPN	6	54	5	55	3	85	3	84
IDS	11	30	11	23	5	69	5	69

情報セキュリティ大学院大学 内田研究室　http://lab.iisec.ac.jp/~uchida_lab/

ホップ・ステップ・ジャンプ（？）

一見関連なく発生している事柄を体系的に見ると、
大きな流れをみることができるのではないだろうか？

SQL Slammer（2003年1月25日発生）

- マイクロソフト社のデータベースソフトSQL Server 2000の脆弱性を利用した。
- この脆弱性は、2002年7月に発見され、修正プログラム（MS02-039）が配布されていたが、この修正を怠ったコンピュータが感染した。
- このワームは、ファイルとして感染対象のコンピュータに保存されるものではなく、Microsoft SQL Server 2000 で動作し、メモリー上に展開されるため、ウイルスワクチンソフト等では検知できない。
- 感染はUDPプロトコルを使うため、一方的な通信が行われることから、非常に多くの攻撃パケットを送ることができた。

Blasterワーム（2003年8月12日発生）

- Microsoft Windowsの脆弱性（MS03-026）を利用したワームが、2003年8 月12日より、急速にネットワーク上に広がっており、全世界的に感染被害の発生が報告されている。
- 2003 年8月16 日になると、windowsupdate.com（ネットワークを通じてWindows を最新版にアップデートするためのサイト）に対して、大量のパケットを送信する攻撃を仕掛けるという性質を持つ。
- このワームは、約1カ月前の2003年7月17日に発見されたWindowsの脆弱性（MS03-026）を利用して感染を広げるトロイの木馬型ウイルス。

原因は・・・

修正プログラムの未適用

ホップ・ステップ・ジャンプ（？）

個人情報漏洩＆ウェブ閉鎖事件

- 2005年6月：価格比較サービス大手のサイトを巡っては、警視庁が不正アクセス禁止法違反容疑で逮捕した中国人留学生の自宅から押収したパソコンに、利用者のメールアドレスなどの個人情報計約9万件が保管されていることが判明。同庁は今年4月から5月にかけ、同容疑者が日本国内から不正アクセスして入手したとみて、調べている。
  サイトの欠陥をついて、外部から不正な命令を入力してデータベースを直接操作する「SQLインジェクション」という手法を使用。攻撃用ソフトは、中国語のインターネットサイトから入手したという。調べに対し、「学費を稼ぐためにやった」と供述。
- 2005年11月：下着メーカーのインターネットショッピング
  7月14日～11月9日の間に商品購入顧客24,322名のうち、以下の人数。
  - 不正アクセスによりデータが流出したお客様の人数：　4,757名
    - このうち、クレジットカード情報（カード番号、有効期限）が含まれる人数：1,899名
    - このうち、クレジットカード情報（カード番号、有効期限）が含まれない人数：2,858名

  不正アクセスの原因は SQLインジェクション という手法を使った不正アクセス

他社のトラブルをみて、どこまでイメージを
広げられるだろうか？

SQLインジェクション
ユーザからの入力を埋め込んで検索のSQL文を組立てる時、入力データのチェックが甘いと、ユーザは自分の都合の良いSQL文を混入でき、データベースを操作できる

クロスサイトスクリプティング
Webページに入力データをそのまま表示していると、ページ内に悪意のスクリプトが埋め込まれ、Webを見たユーザとサーバ自身の両方に被害を及ぼす

犯罪・犯罪予防を考える ～ オンライン犯罪を中心に ～

ホップ・ステップ・ジャンプ（？）

モバイルSuica不正利用相次ぐ

- 携帯電話に入金した電子マネーで、電車に乗車したり、買物ができるJR東日本の「モバイルSuica」で、2006年12月頃から、不正入手したカード情報で他人になりすまし、電子マネーが使用される被害が相次いでいることが9日、分かった。確認できた被害総額は約1,000万円に上り、JR東日本は警視庁原宿署に被害届を提出。同署は電子計算機使用詐欺の疑いで捜査している。
- JR東日本などによると、モバイルスイカは、氏名、生年月日、クレジットカード情報などを携帯電話に入力して送信すると会員登録される。携帯電話に入金した電子マネーは、登録したクレジットカードで決済される仕組み。
- 会員登録の際、クレジットカードの暗証番号の入力が不要。また、会員情報とカード会社の情報が一部しか照合されず、不正に入手したカード情報を悪用して会員登録された可能性があるという。不正に使われたカードは65枚に上っている。
- モバイルスイカでは電子マネーの入金上限額は2万円だが、使用して残額が減れば、1日何度でも入金できる。クレジットカードでの決済は約1カ月後となり被害者は気が付きにくい。1枚のカードで300万円が使用されたケースもあるという。
- JR東日本は1日の利用額を2万円に制限するなどの対応策のほか、本人確認の強化に暗証番号入力やカード情報の照合項目を増やすことも検討している。同社広報部は「すでに再発防止対策に取り組んでいるが、今後ともシステム強化などさらなる対策に努める」としている。

2007年11月09日
http://www.itmedia.co.jp/news/articles/0711/09/news028.html

犯罪・犯罪予防を考える ～ オンライン犯罪を中心に ～

ホップ・ステップ・ジャンプ（？）

「プログラムのセキュリティ欠陥は開発者個人の責任」（Secure London 2005）

元米国大統領重要インフラ保護委員会委員長 ハワード・シュミット（Howard Schmidt）

- ソフトウェア開発者により充実したトレーニングを提供する必要がある
- ソフトウェア開発者は、自身の記述したコードが安全であることを個人のレベルにおいて保証する必要がある
- SSLを利用してバックエンドのデータベースとデータ送受信を行うウェブアプリケーションを構築した開発者達は強力な認証の仕組みや、強固なパスワード、暗号化された通信路を用意していた。また、格納されるデータの暗号化を行っていた。 しかしそのデータが購買担当者のオフィスに送信される際には、ただのテキストファイルとして送信されていた。これではエンドツーエンドのソリューションとはいえない。開発者のもとに行き、『これでセキュリティは完璧なのか？』と問えるよう、個々の開発者に対してエンドツーエンドのソリューションに関する説明を求められるようにしなければならない
- Microsoftの調査結果： ソフトウェア開発者の64%が安全なアプリケーションを記述する自信を持てずにいる
- 今までの大学のコースはセキュリティではなく、使い勝手、拡張性、管理のしやすさに重きをおいてきた。今では、多くの大学が情報保証やセキュリティを重視するようになったが、ウェブアプリケーション開発は従来より、マウスのクリック回数、すなわち、いかにしてユーザーにクリックさせるかで評価されてきた
- ソフトウェア開発企業も、従業員の採用時にセキュリティスキルの有無をチェックする役割を果たすべき

http://news.zdnet.co.uk/security/0,1000000189,39228663,00.htm

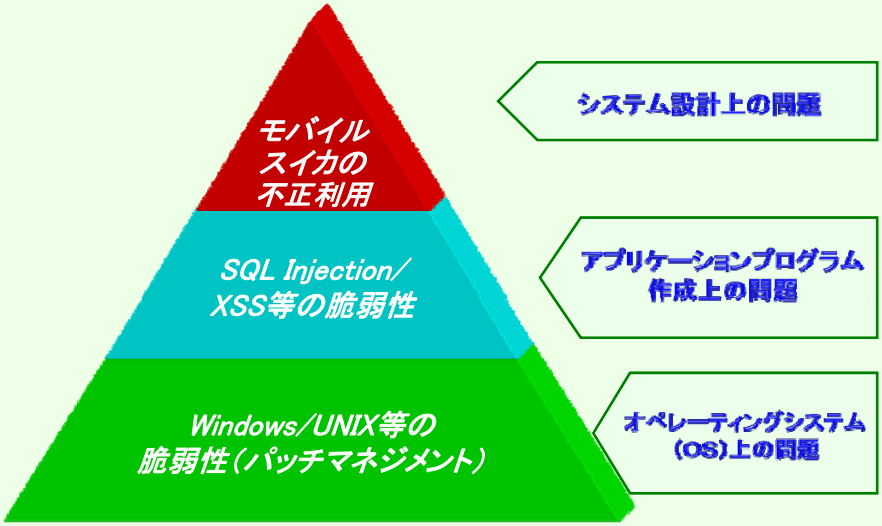
メインフレーム時代には、データ入力のプログラムを書けない者をプログラマーとは呼ばなかった・・・

犯罪・犯罪予防を考える ～ オンライン犯罪を中心に ～

ホップ・ステップ・ジャンプ

OS等 下位層の問題から、適用業務システムの問題へ！

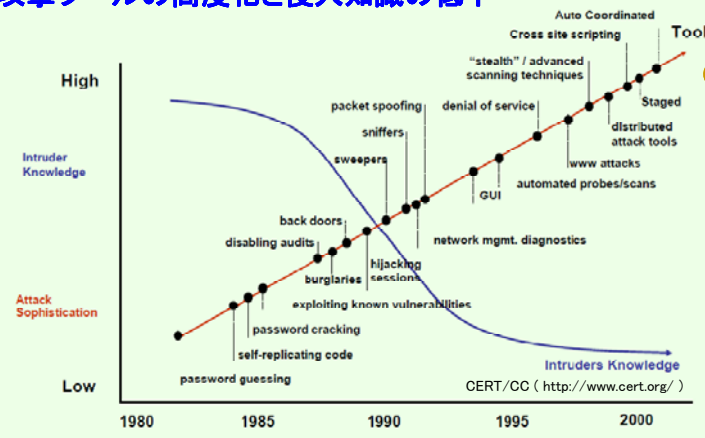
その対応ができているのだろうか？



犯罪・犯罪予防を考える ～ オンライン犯罪を中心に ～

ヒューマン対策の必要性（その1）

攻撃ツールの高度化と侵入知識の低下



スクリプトキディの活躍の場が広がっている？

2009 Data Breach Investigations Report

経過時間	件数
1ヶ月未満	0
1～ 3ヶ月	0
3～ 6ヶ月	0
6～12ヶ月	1
1年以上	5

脆弱性の放置期間と攻撃件数

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

問題は 防御側 では？

情報セキュリティは技術の問題 ？

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

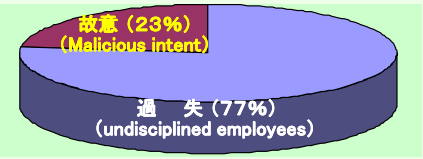
ヒューマン対策の必要性（その2）

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



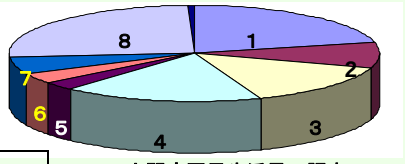
InfoWatchの調査
http://www.infowatch.com/threats?chapter=162971949&id=207784626

（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　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	



内閣府国民生活局の調査

情報漏えい原因の明確化の大切さ ？

投資対効果を考える

ヒューマン対策の必要性（その3）

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ることもできる。
>
> August Bequai著、堀部政男・堀田牧太郎 訳
> 「情報犯罪：How to prevent computer crime」啓学出版 1986

質問

下の左右の人物の絵をみて、どちらが犯罪を行うかわかるでしょうか ・・・・・

ヒューマン対策の必要性（その4）

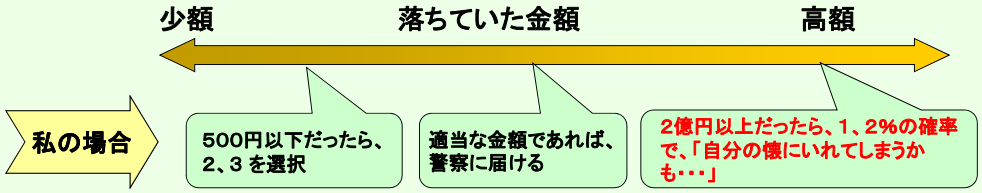
質問

以下の質問についてどのように回答されるでしょうか？
（考えられるものを選択して下さい。 この質問はパズルや引っかけ問題ではありません。
情報セキュリティを考える上で、大切なものだと思っています。）

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ました。
ざっと見るとXX円ありそうです。 この時、以下のどれをとる可能性があるでしょうか？
（全てを取る選択肢もあります）

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、皆さんのとる手段は1～3で変化がありますか？
下の線の所に、上記1～3までを実際の金額を入れて回答して下さい。



問題・課題の明確化（その1）

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

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） 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）
  http://it.nikkei.co.jp/security/news/index.aspx?n=SSXKD0902%2029112006
- 陸自の内部資料の流出（2007年2月3日） http://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）
  http://it.nikkei.co.jp/security/special/winny.aspx?n=NN000Y692%2013062007

振り込め詐欺対策での知見

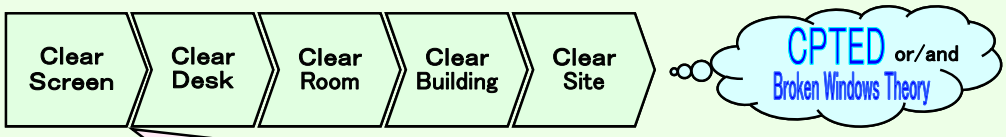
「理性が働いている」前提の対策でなく、「理性が働いていなくても、可能な対策」

- 家族間のコミュニケーションを深めておく： 普段から家族同士で頻繁に連絡を取り合い、「理性が働いていなくても、明らかに詐欺だと見抜ける手がかり」を増やしておき、気づきの可能性を高めようという対策
- 詐欺の「避難訓練」を行う： 災害の避難訓練は、理性が働いていなくても、勝手に体が動いて避難できることを目的としている。 これを詐欺の電話にもあてはめようというものです
- それでもだまされかけたときに備え、振り込む直前に「われに返る」タイミングを用意する： 一例として、キャッシュカードに「理性君 ピンチ！」という文言を書き入れることを提案している

NHK「ためしてガッテン」2009年2月18日放送 より http://www3.nhk.or.jp/gatten/archive/2009q1/20090218.html

問題・課題の明確化（その2）

「クリアスクリーン」・「クリアデスク」の考え方



「クリアスクリーン」、「クリアデスク」をこのように考えればその意義が理解できる？
重要情報保存媒体が部屋に無造作に置かれていれば、犯罪を誘発する可能性がある。

環境設計による犯罪予防（CPTED： Crime Prevention Through Environmental Design）

- 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

問題・課題の明確化（その1）

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

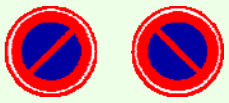
問題・課題の明確化（その2）

心理学の知見の利用：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

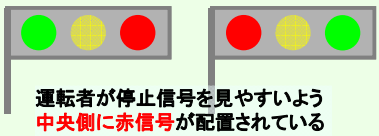
  この場合でも、刺激の中の注意を向けた特徴だけが記憶にとどまる

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あると言える

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」）

問題・課題の明確化（その5）
～ 研修の評価・効果測定 ～

● カークパトリック（Donald L. Kirkpatrick）の4段階評価

研修評価・効果測定に関し、米国には標準的な考え方がある。カーク・パトリックの4段階評価と呼ばれるもので、米国では約7割近くの企業が採用し、日本でもかなり普及しているモデルである。この4段階評価は、研修評価・効果測定をいくつかのレベルに分けて考えている

レベル	説　明
1. 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. 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. 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. 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
5. 投資収益率	効果測定は、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　（ジャック・フィリップス（Jack J. Phillips）の提案）

アンケートは常に
正確ではない？

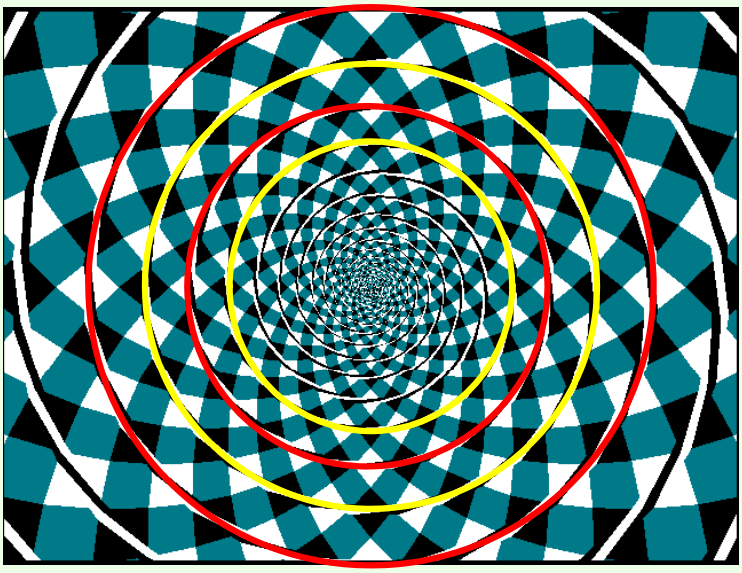
● IAT（Implicit Association Test）について

- 人は、「心の中にあるもの」をいつも語ってはいない。また、「心の中にあるもの」を正確に知っているかも疑わしい。 こういった乖離を理解することは、科学的心理学にとって重要です
- 人は、言いたくないと思っていたり、実際、言えない場合、心の中で思っていても口に出さない場合がある。 例えば、1日に4箱のタバコを吸う人が、「喫煙本数」を聞かれた場合、わざと「1日に2箱」と回答することがある。正確な数を答えると、バツが悪いと思ったり、質問はプライベートな問題だとして回答しないこともある（わかっていることを報告しようとはしない場合の例です）。 しかし、1日に4箱のたばこを吸う人でも、本人が1日に2箱程度しか吸っていないと本気で信じているために「1日に2箱しか吸いません」と答えることがあるかもしれません。（知らず知らずのうちに間違った回答をすることは、時に自己欺瞞と呼ばれます。これは、要求されている回答をすることができない状態を意味します）
- 「しようとしないこと」とそれが「できないこと」との区分は、意識的に他者から何かを隠していることと、意識せずにあなた自身から何かが隠されていることの違いと似ています。潜在的連合テスト(IAT)は、この両タイプの隠蔽を見破ることを可能にします。IATでは、人々が報告しようとはしないか、あるいは、報告することができない潜在的な 態度や信念を測定します

https://implicit.harvard.edu/implicit/japan/

問題・課題の明確化（その6）

人は何故ミスをするのか（経験の有用性）？

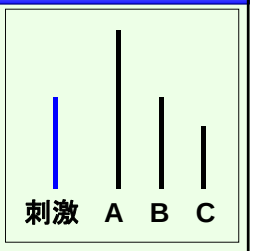


フレーザーの錯視

- 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。

問題・課題の明確化（その8）

- 「Not Me Syndrome」： 自分だけは騙されないと思いこんでいること
- 同調実験（Asch,1951）： ９人の前に、１本の線分を示し、それから長さの異なる3本の線分を見せる（右図）。 そして、皆の前で、８人に最初に見せたものと同じ長さの線分を選択させる。 実験参加者9名の内、実際の参加者は、１名だけで、他の8名は、実験協力者で、8名はA だと回答するように言われている。 最後に実験参加者が回答するが、25%の人は、他の参加者と同じ回答をする。
  なお、実験協力者は、3名でも、多くの人は同調すると言われている。
  同様の実験を、ロボットゴキブリでやっても同じだとか。（日本経済新聞（2007年11月28日）夕刊 脳研究者 池谷 裕二）

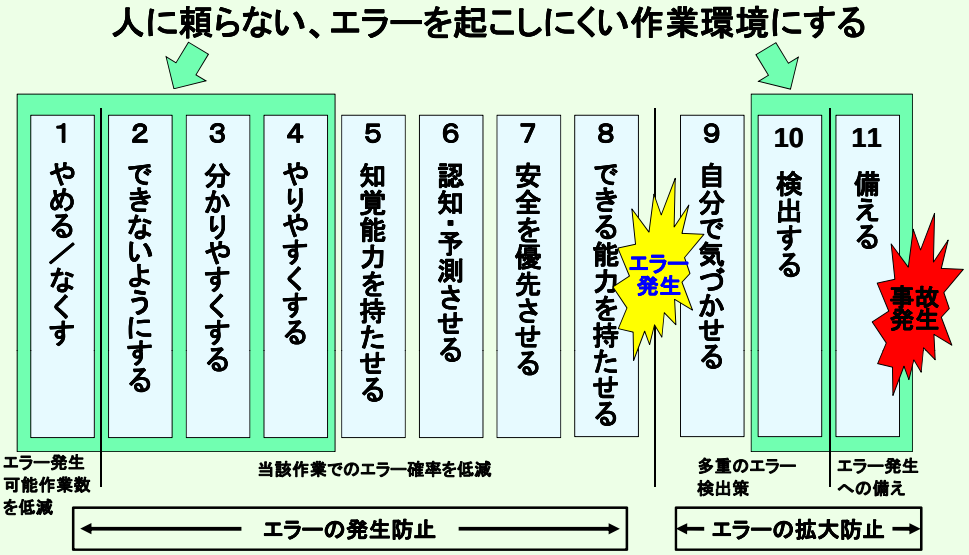


三人寄れば言うがまま―― （日本経済新聞（2007年11月28日）夕刊 脳研究者 池谷 裕二）

近所のラーメン屋に行った。塩ラーメンが食べたかった。回転と同時に一人ひとり順に注文してゆく。私の前に十人ほど並んでいただろうか。なぜか皆、醤油(しょうゆ)ラーメンを頼んでいる。この状況……思わず私も醤油ラーメンに注文を変えてしまった。
周囲が同じ行動をすると、類似した振る舞いをせざるを得ない雰囲気になる。このように集団圧力に屈して意見や行動を変えることを「同調」という。
同調するのは人間だけではない。最近の研究によれば、ゴキブリも似た行動をとるという。ベルギーのハロイ博士の実験だ。ゴキブリは複雑な社会行動を示す知的生物である。光を嫌い暗所に群がる習性に目を付けた博士は、ロボットを使って実験を行った。16匹のゴキブリを観察するのだが、その中の4匹はロボットである。ロボットはゴキブリたちと社会協調するように精巧にプログラムされており、暗い巣で過ごしている。
そこで、この4台のロボットのプログラムを、明るい巣を好むように書き換える。すると周囲のゴキブリたちも追随して、明るい巣へと移動した。同調である。
4匹という数字が面白い。私たち人間の場合、「皆がそうするから」というときの「皆」とは具体的に何人を指すのだろうか。試してみればすぐにわかる。答えは3人以上だ。2人が醤油ラーメンならば私はまだ塩ラーメンを注文できるが、3人続くと状況が一変し、集団圧力が生まれる。
2人と3人。数の上では大差なく思えるものの、心理的には大きな隔たりがある。これは裏を返せば、ある人に何かを同調させるためには他の3人の意見を事前に揃(そろ)えておけばよいとも言えるわけだ。

教 育 ・ 訓練

事例による教育・訓練



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

リスクにあなたは騙される

ポール・スロヴィック(Paul Slovic)の研究 素人がリスクを過大評価する理由

1. **大惨事の可能性**：１回の事件で多数の死者がでる場合、リスクの認識が高まる
2. **馴染み**：よく知らない、あるいは聞いたことがないリスクは、余計に心配する
3. **理解**：活動あるいは、技術の働く仕組みがよく理解できないと、危険意識が高まる
4. **個人による制御**：被害の可能性が自分で制御できるレベルを超えていると感じると、より心配する
5. **自発性**：リスクに関わらないことをすると余計に恐ろしく感じられる
6. **子どもの関与**：子どもが関与すると、より深刻になる
7. **未来の世代**：リスクが未来の世代に脅威を与える場合、余計に心配する
8. **犠牲者の身元**：身元の分かっている犠牲者だと、危険意識が高まる
9. **極度の恐怖**：生じる結果が恐怖心を引き起こす場合、危険意識が高まる
10. **信用**：関係している機関が信用できないと、リスクは高まる
11. **メディアの注目度**：メディアで扱われることが多ければ多いほど、余計に心配になる
12. **事故の歴史**：過去に良くない出来事があると危険意識が高まる
13. **公平さ**：一方に利益がもたらされ、他方に危険がもたらされる場合、リスクの順位が上がる
14. **利益**：活動あるいは、技術のもたらす利益が明確でないと、明確な場合よりリスクが大きいと判断
15. **復元性**：何かがうまく行かなかった時、その結果を元に戻せないと、リスクは高まる
16. **個人的なリスク**：自分を危うくするものであると、リスクは高まる
17. **人工的な原因**：人工のリスクは自然起源のリスクよりリスクが大きい
18. **タイミング**：差し迫った脅威ほど大きく感じられ、未来の脅威は割り引かれる傾向がある

参考： http://eco.nikkei.co.jp/column/ecowatching/article.aspx?id=MMECcd000014072009&page=1

心理的な攻撃手法
（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）

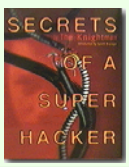
- 侵入するシステムにアクセスできる正当な権限を持っている人間の心理的な弱さを利用して、侵入するために必要な情報を取得する手法。 いわゆる、技術的手法ではない
- 侵入者にとって、困難な所から侵入を図るより、より楽な方法で侵入ができる方法が分かっていれば、そこからの侵入を図るのは、現実の世界でも、サイバーの世界でも同じ
- 情報システムにおいて、最も弱い部分（脆弱性）は、人である。 侵入者が権限を持った人から得た情報は、侵入システムへの正規の情報であり、侵入者は正面からシステムへ侵入できる
- 色々な手法があり、それらを単独、あるいは、複数手法を組み合わせて行うこともある
- また、一人だけでなく、複数人に行い、部分情報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

心理的な攻撃手法
（ソーシャルエンジニアリング）

国内ではソーシャルエンジニアリング例は殆どない！？

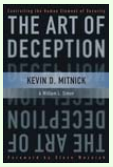
- 昭和56年（1981年）10月　H相互銀行事件
  犯人は、H相互銀行の某支店に「Kの者だが機械のテストをするからS支店の口座へ3500万円の入金操作をして欲しい」と指示し、預金係主任が本店からの指示と信じて操作を行った。共犯の女性が事前に開設してあった口座に入金がされた時間頃に別のS支店で3000万円を引き出し、騙し取った
  犯人は電話で行内用語（ジャーゴン[Jargon]：符丁）で指示をしたため、支店の預金主任は完全に騙された
- 昭和60年（1985年） 某郵便局
  郵便局の窓口の係員に「すぐにお金を持ってくるので、この通帳の口座に入金しておいて欲しい」と頼み、それを信じて入金手続きを端末機で行わせ、他の郵便局のATM端末から現金1100万円余りを引き出した。 忙しかったり、顧客が忙しそうにしていると、つい親切に対応することが良いと錯覚してしまう。どんなに切迫している状況の場合でも、どこまでは対応してもよいかを判断できる教育・訓練が必要になる。

国内における最大のソーシャルエンジニアリングは？



シークレット・オブ・スーパーハッカー
（Secret of a Super Hacker）
初版は1994年（翻訳は1995年）発行

ケビン・ミトニックのソーシャルエンジニアリング技術は右にでるものがいないと言われ、多くのネットワークに侵入
2002年10月「The Art of Deception」（欺術）を出版



ソーシャルエンジニアの武器！？
～ 影響力の武器 ～

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、それを与えてくれた人にお返しをせずにいられない気持ちになること
2. コミットメントと一貫性[Commitment and Consistency]：自分の意志でとった行動がその後の行動にある拘束をもたらすもの。以下のような手法がある
   - A) 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
   - B) 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
   - C) 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
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

ロバート・B・チャルディーニ 著「影響力の武器」
(Robert B. Cialdini "INFLUENCE – Science and Practice") 誠信書房 より

教 育 ・ 周 知

訓練等での対応

- 山口健太郎 他 "ユーザへの予防接種というアプローチによる標的型攻撃対策集合教育／e ラーニング等での対応" 情報処理学会 73回全国大会 2009年3月
  標的型メール攻撃に対する情報セキュリティ教育手法のひとつ「予防接種（Inoculation）」に注目、その有効性を実験により検証するとともに、その結果から有効な実施手法等について考察、提案
- KYT（危険予知訓練：Kiken Yochi Training）の情報セキュリティへの援用
  工場や工事現場などの作業の従事者に、事故・災害を未然に防ぐことを目的に、作業に潜む危険を事前に予想し、指摘しあう訓練。 情報セキュリティ分野でも研究が始まっている
  重住 牧（NEC）"情報セキュリティ意識を向上させるためには(KYT手法を応用した参加型教育による情報セキュリティ意識の向上)" （財）防衛調達基盤整備協会 懸賞論文 http://www.bsk-z.or.jp/kenkyu_center/kyoukaisho/090101kensho_ronbun1.pdf
  大和田竜児（情報セキュリティ大学院大学）"従業員のリスク行動に対する企業の取り組みに関する考察"

犯罪・犯罪予防を考える ～ オンライン犯罪を中心に ～

他分野の知見の利用を！

状 況 別 犯 罪 防 止 論
(Techniques of Situational Prevention)

Increase the Effort 犯罪予防策の増強	Increase the Risks 犯罪へのリスクを高める	Reduce the Rewards 犯罪報酬の減少	Reduce Provocations 犯罪誘因の減少	Remove Excuses 犯罪弁明の排除
1. 犯罪対象物の強化 • Immobilizers in cars • anti-robbery screens	6. 防犯意識の向上／拡大 • cocooning • neighborhood watch	11. 犯罪対象物の隠蔽 • gender-neutral phone directories • off-street parking	16. フラストレーション／ストレスの削減 • efficient queuing • soothing lighting	21. ルール設定 • rental agreements • hotel registration
2. 入退館アクセス管理 • alley-gating • entry phones	7. 自然管理性の支援 • improved street lighting • neighborhood watch hotlines	12. 犯罪対象物の排除 • removable car radios • pre-paid public phone cards	17. 紛争の回避 • fixed cab fares • reduce crowding in pubs	22. 指示標識の提示 • 'No parking' • 'Private property'
3. 出口での審査 • electronic tags for libraries	8. 匿名性の排除 • taxi driver ID's • 'how's my driving?' signs	13. 所有者の明確化 • property marking • vehicle licensing	18. 感情の高まりの削減 • controls on violent porn • prohibit pedophiles working with children	23. 良心への警告 • roadside speed display signs • 'shoplifting is stealing'
4. 犯意をそらす • street closures in red light district • separate toilets for women	9. 施設管理者の利用 • train employees to prevent crime • support whistle blowers	14. 裏市場をなくす • checks on pawn brokers • licensed street vendors	19. 仲間からの圧力の無力化 • 'idiots drink and drive' • 'it's ok to say no'	24. 法令遵守への支援 • litter bins • public lavatories
5. 道具／武器の管理 • toughened beer glasses • photos on credit cards	10. 公共監視の強化 • speed cameras • CCTV in town centers	15. 犯罪利益をなくす • ink merchandise tags • graffiti cleaning	20. 模倣犯罪の抑止 • rapid vandalism repair • V-chips in TV's	25. 薬物／お酒の統制 • breathalyzers in pubs • alcohol-free events

B. Cornish, and V.Clarke. Twenty-five Techniques of Situational Crime Prevention. 2003

犯罪・犯罪予防を考える ～ オンライン犯罪を中心に ～

参考資料

- 土居範久監修 情報セキュリティ事典 共立出版社
- 東京商工会議所 編 危機管理対応マニュアル サンマーク文庫
- 先端内部監査研究会著 これが金融機関の内部監査だ 金融財政事情研究会
- リン・シャープ・ペイン著 バリューシフト 毎日新聞社
- 財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について(意見書) http://www.fsa.go.jp/singi/singi_kigyou/tosin/20070215.pdf
- ブルース・シュナイアー著 セキュリティはなぜやぶられたのか 日経BP社
- (財)日本ニューメディア協会 ISMSの維持管理における実態調査報告書 http://www.nmda.or.jp/rio-net/library/newmedia2/index.html
- 内田勝也 情報セキュリティ認証制度、実態調査で見えてきた課題 日経新聞社ネット時評 http://www.nikkeidigitalcore.jp/archives/2007/06/post_109.html
- 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4月
- 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4月
- CERT/CC Insider Threat Research http://www.cert.org/insider_threat/
- 芳賀繁 失敗のメカニズム ー忘れ物から巨大事故まで 日本出版サービス 2000年1月
- 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2月
- 岡本浩一 リスク心理学 サイエンス社 1992年1月
- 中谷内一也 リスクのモノサシ 日本放送出版協会 2006年7月
- 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7月
- 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5月 http://www1.mhlw.go.jp/houdou/1105/h0512-2_10.html

ありがとうございました

ご質問・コメントがございましたら ・・・・

電子メールでのご質問・コメントはいつでもどうぞ

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

教授　内田　勝也

uchidak@gol.com
http://www2.gol.com/users/uchidak/

内田研究室：　http://lab.iisec.ac.jp/~uchida_lab/