情報漏洩を防ぐ
情報セキュリティ対策のあり方

2010年11月26日
情報モラル啓発セミナー

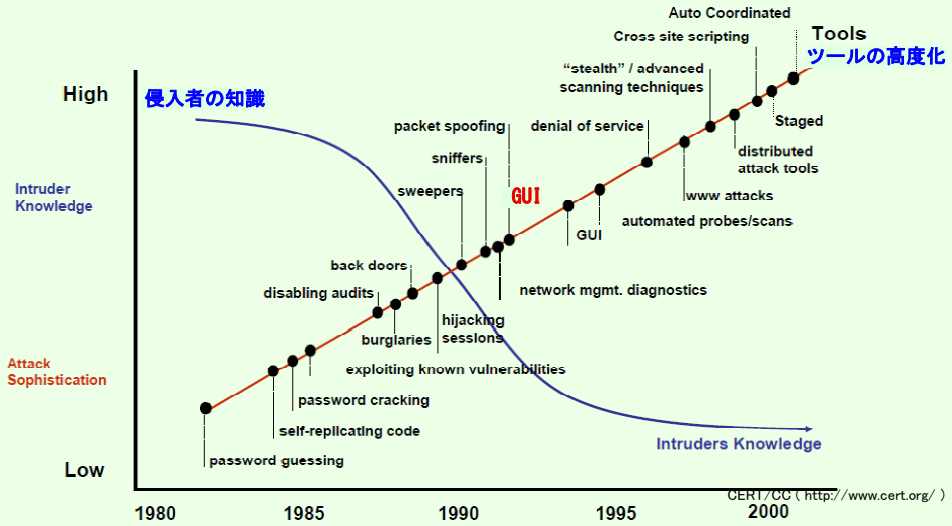
中央大学 研究開発機構 教授
兼　横浜市CIO補佐監
内田　勝也 （ uchidak@gol.com ）

本日の内容

１．インターネットの危なさはどこにあるのか？　～ 都市伝説？（その1）～
２．迷惑メールの問題の本質は？　～ 都市伝説 （その2）～
３．根本的原因分析の必要性
４．プログラム作成レベルの問題？
５．他者の資料をどう見るのか？
６．情報セキュリティ部門の責任放棄？
７．問題・課題の明確化
８．安全と安心について
９．マスコミ報道の特徴（その1）
１０．まとめ.

インターネットの危なさはどこにあるのか？
～ 都市伝説？（その1）～

攻撃ツールの高度化と侵入知識の低下



攻撃ツールの高度化に伴い、侵入者の知識が高くなくても、外部から簡単に侵入できる。
また、攻撃ツールはインターネット上から簡単に取得できると言われた。

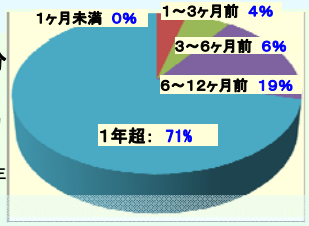
Katsuya Uchida uchidak@gol.com

情報漏洩を防ぐ
情報セキュリティ対策のあり方

インターネットの危なさはどこにあるのか？
～ 都市伝説？（その1）～

1．インターネットに簡単に侵入できるのだろうか？

- 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）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.com/security/Security-First.html
  ⇒ 2002年末頃から、この話をセミナー等で話しているが・・・
- 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。既知の脆弱性を利用したデータ漏洩／侵害のどれくらい前にその脆弱性パッチが入手できたかを示すと左図のようになる
  Verizon Business「2008年データ漏洩／侵害調査報告書」2008年



- セキュリティ会議 DefConでの CTF（Capture the Flag）競技の内容
  上位9チームと昨年の優勝チームの計10チームで争われ、各チームは自分のサーバを守り、相手のサーバの脆弱性を発見することを競う。サーバには予め点数の割り振られた幾つかの脆弱性が設定されており、相手サーバの脆弱性を見つけたら200点、自チームのサーバの脆弱性を見つけてそれを埋めたら100点という形で点数を積み重ね、最終的に点数の高いチームが優勝する。
  https://www.netsecurity.ne.jp/3_13308.html

このような分析を国内ではみないが、
国内ネットワークは、簡単に破られるのか？
それとも・・・

名古屋市の河村たかし市長は、「住民基本台帳ネットワーク（住基ネット）への侵入実験を行いたい」と話した。住民の個人情報を管理する住基ネットは、外部からの不法な侵入を防ぐ仕組みになっているが、実験で安全性を再検証する
侵入実験は、長野県が2003年秋に実施しているが、本体へ侵入できる可能性を指摘した長野県に対し、総務省は「本体には侵入されておらず、全く問題ない」との立場で、実験結果の見解は分かれている 朝日新聞 2010年1月30日

Katsuya Uchida uchidak@gol.com

迷惑メールの問題の本質は？
～ 都市伝説？（その2）～

2. 迷惑メールが多いのは何故だろうか？

あるメールシステムに送付されたメールを
別のメールシステムに転送したもの

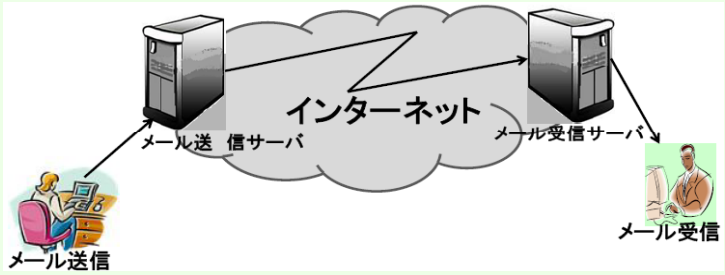
実際に送られてきたメール（55件）の内、
受信トレイに入ったメール（15件：27%）

実際に送られてきたメール（55件）の内、
迷惑メールに入ったメール（40件：73%）

情報漏洩を防ぐ
情報セキュリティ対策のあり方

迷惑メールの問題の本質は？
～ 都市伝説？（その2）～

電子メールの仕組み



(1-1) メールサーバは正しいと判断したが、不正なメールだった。
(1-2) 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) 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) 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

電子メールでのリスクを考えると、

- (1-1) はリスクが高いが、
- (2-1)は業務に支障がある可能性があるが、リスクは低い

情報漏洩を防ぐ
情報セキュリティ対策のあり方

迷惑メールの問題の本質は？
～ 都市伝説？（その2）～

（1－1）電子メールの例

LogLogic	Log Matters - August 2010 - If you	8月31日
CIO & CSO Security Alert	Microsoft Dynamics CRM as a Bu	8月31日
Ruperta Osorio	Buy qulaityy softwware tooday, :	8月31日
ptokyo	世界銀行東京事務所 Eニュース 297	8月30日
Dusty Hochberg	AllNedeedSoftaware.Easy-To-Dow	8月29日
Janina Kemp	PouplarSoftwaare-EeasyAndFastDc	8月28日
TechMentor Las Vegas	Conference eBrochure Now Ava	8月28日

（1-1） メールサーバは正しいと判断したが、
不正なメールだった。

（2－1）電子メールの例

迷惑メールをすべて削除 (迷惑メール)のメールは 30

Cherrie Mirtha	ViagraProfessional as low as $3.95, V	8月6日
ptokyo	世界銀行東京事務所 Eニュース 295	8月6日
COREL Product	【COREL】WinZip14.5 Pro 最大50%OF	8月6日
Meds against erectile dy.	News for uchida: Top brands 70% ch	8月6日
uchida	You will give her greater satisfaction -	8月6日
Louann Merlyn	Swiss Rep1caWatch, Rep1caWatche	8月6日
yoten6049	Her pussy smiled at me - Take the hott	8月6日
Ad Adkins	aforesaid commingle demilitarized - de	8月6日

（2-1） メールサーバは不正メールと判断したが、正しいメールだった
（2-1)の多くは送信元を詐称（「アドレス詐称」）

情報窃取を目的として特定の組織に送られる不審なメール 「標的型攻撃メール」

標的型攻撃メールに関する情報提供のお願い

- 不審なメール(*1)を受信した場合は、送信者の組織に問合せて送信していないことを確認した上で、「情報セキュリティ安心相談窓口」にご連絡ください。

注(*1) 不審なメールとは、実在の企業名や官公庁名をかたって特定の組織や人に送られるメールで、添付ファイルを開いたり本文中のURLをクリックするとその組織の情報を盗むウイルスに感染する仕掛けをほどこされた、「標的型攻撃メール」を想定しています。不特定多数に送られるマスメールウイルスや広告メール、架空請求メール、フィッシングメールは除きます。標的型攻撃メールの特徴と被害例については別紙1を、標的型攻撃メールが届いた場合の対応については別紙2をご覧ください。
http://www.ipa.go.jp/security/virus/fushin110.html

適切なメールシステムの利用で、標的型攻撃メール（アドレス詐称）は、ほぼ100%対応できる。
でも、何故、そのようなメールシステムの採用を推奨しないのだろうか？

情報漏洩を防ぐ
情報セキュリティ対策のあり方

根本的原因分析の必要性

ガンブラーを例にして

ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起

- 閲覧した利用者のパソコンにウイルスを感染させることを狙ったウェブサイトの改ざん事例が発生しており、ウェブサイト管理者等へ注意を喚起し、ウェブサイトの運用を再度見直すことを推奨する
- 改ざんされたウェブサイトの管理者は、被害者に留まらず、閲覧した利用者のパソコンにウイルスを感染させてしまう加害者となります。このような被害の拡大を防ぐため、ウェブサイトの管理者は、運営しているウェブサイトが改ざんされていないか確認し、ウイルスの “ばらまきサイト” に仕立て上げられないようにしてください

(1) 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に、ftp※のアカウント情報の盗難がある。 盗んだ ftp アカウント（ID/パスワード）を使い、正規ユーザになりすまし、改ざんしたページをウェブで公開（アップロード）する
- ftp 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等の方法が一般的
  ※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、一般利用者が悪意あるウェブサイトを閲覧。利用者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する

（抜粋） http://www.ipa.go.jp/security/topics/20091224.html

根本的な問題は何か？

情報漏洩を防ぐ
情報セキュリティ対策のあり方

根本的原因分析の必要性

ウェブサイト改ざんに関する注意喚起

① ウェブ管理者のFTPアカウント(ID／パスワード)を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で盗取され、ウェブが改ざんされる

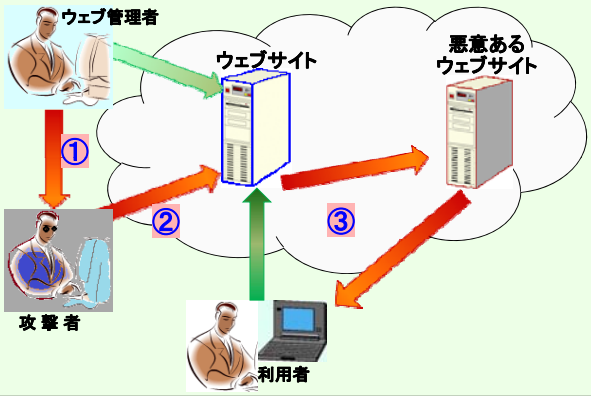
② 改ざんされたウェブページには不正なスクリプトが埋め込まれ、そのページを閲覧した一般利用者を、ウイルスが仕掛けられた悪意あるウェブサイトにアクセスさせる

③ 悪意あるウェブサイトを閲覧した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る

疑　問

1. どの様にしてスパイウェア(キーロガー)をウェブ管理者のPCの送り込むのだろうか？
2. それを防ぐ方法は？
3. FTPアカウントを盗取されてしまった場合の対処方法は？

・・・・・・・・・・・・・・・



Katsuya Uchida　uchidak@gol.com

情報漏洩を防ぐ
情報セキュリティ対策のあり方

根本的原因分析の必要性

1. どの様にしてスパイウェアをウェブ管理者のPCの送り込むのか？

- メールに添付されたファイルをクリックしたため
- インターネット経由でダウンロードするフリー・ソフトウェアにバンドルされていた
- ポップアップ・ウインドウ、ActiveX技術、Web ブラウザ等のセキュリティ・ホールを利用
- FTPのユーザID/パスワード盗難：約8,700件 日本企業も (2008.02.27)
  http://www.finjan.com/Pressrelease.aspx?id=1868&PressLan=1819&lan=3
- その他

2. また、それを防ぐ方法は？

- サーバとの通信に暗号化される SFTP、FTPSやSCP(Secure Copy)を使う

3. FTPアカウントを盗取されてしまった場合の対処方法は？

- 盗取後には、パスワードの変更を。 但し、スパイウェアが生きている可能性があるので対応には十分な注意が必要
- FTPアカウントが盗取されても、ウェブ改ざんを防ぐ方法を考えておく。 例えば、ウェブ管理はインターネット(外部ネットワーク)からはできない仕組みにする

今後、同様な問題が発生しても対応出来る仕組みを考えることが大切では？
対症療法的な方法でなく、根本療法的な対応が必要では・・・

更に言えば、この程度の知識もないウェブ管理者は専門家なのだろうか？

Katsuya Uchida　uchidak@gol.com

プログラム作成レベルの問題？

個人情報漏洩＆ウェブ閉鎖事件（SQLインジェクション）

- 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

SQLインジェクション

第2章 セキュアDBプログラミング
[2-1] SQL組み立て時の引数チェック
ユーザからの入力を埋め込んで検索のSQL文を組み立てるということはしばし ば行われる。このとき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，データベースに干渉できるという問題が起こる。

クロスサイトスクリプティング

第1章 セキュアWebプログラミング
[1-2] 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おうむ返しに表示している部分があると，ページ内に悪意のスクリプトが埋め込まれ，それを見たユーザとサーバ自身の両方に被害を及ぼす「クロスサイトスクリプティング」という不正の手口に利用されてしまう。

http://www.ipa.go.jp/security/awareness/vendor/programming/a02_01_main.html

Katsuya Uchida　uchidak@gol.com

他者の資料をどう見るのか？

墜落ネコの死亡率：　falling cats‘ death rate

ネコは着地がうまい。 高い所から落ちたネコはどうなるだろう？
この興味深い話題について、ニューヨーク・タイムズの科学別冊『サイエンス・タイムズ』1989年8月22日号に次のような記事が載った

1984年の5ヶ月間に、ニューヨーク市の高層マンションからネコが落ちた事故のうち、落ちた時の階の記録があるのは129匹である（2階～32階）

- 死亡は8匹だったが、階が高いほど生存率も高い
- 7階以上から落ちたネコ 22匹のうち死んだのは1匹だけ
- 9階以上から落ちた13匹は全て生き延び、骨折は1匹のみ

- 129匹中・・・・・・・死亡8匹
  - 7階以上・・・・・死亡1匹
  - 6階以下・・・・・死亡7匹

- 高階層から落ちたネコの生存率が高い理由（獣医師の説明）：
  - ネコは、落ちると「終端速度」（それ以上速くならない最高落下速度）に速やかに達する
  - 終端速度は時速60マイル（約100Km/時）で、人間の大人の半分
  - ネコは終端速度に達するまで脚を突っ張って抵抗するので、着地したとき怪我をしやすい
  - 終端速度に達した後は、ネコはリラックスし、脚をムササビのように広げるので、空気抵抗が高まり、着地時に衝撃が均等に分散されるため、生存率が高い

この調査は問題ないでしょうか？

山村武彦、人は皆「自分だけは死なない」と思っている、宝島社、2005年
http://members.jcom.home.ne.jp/miurat/puzzl3-y.htm

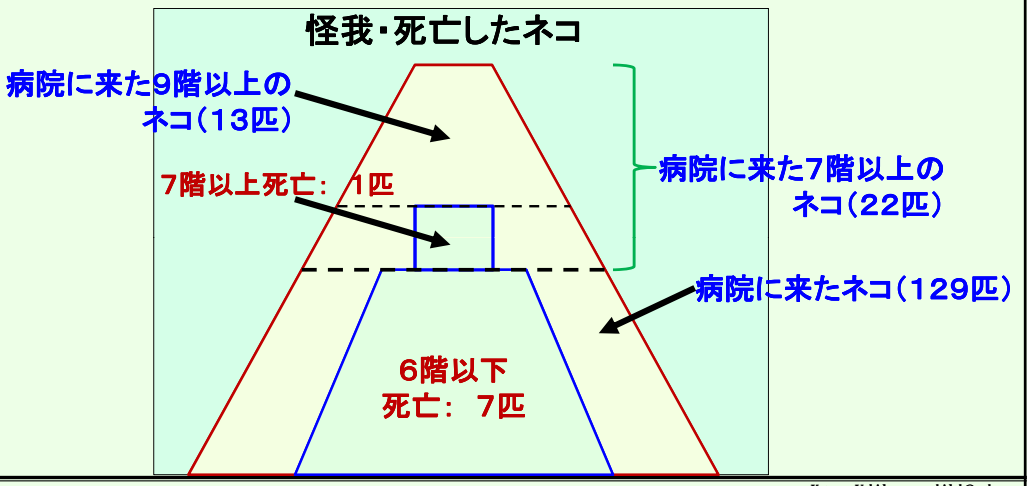
Katsuya Uchida　uchidak@gol.com

情報漏洩を防ぐ
情報セキュリティ対策のあり方

他者の資料をどう見るのか？

怪我・死亡したネコの全体像

- 病院に来たネコは、少なくても、生きていた可能性が高い
- 既に死亡したネコは、病院に来る可能性は非常に低い
- 調査のサンプルの取り方が異なれば、結果も異なるのは当然では。
  でも、このような形で書かれるとだまされやすいので注意が必要

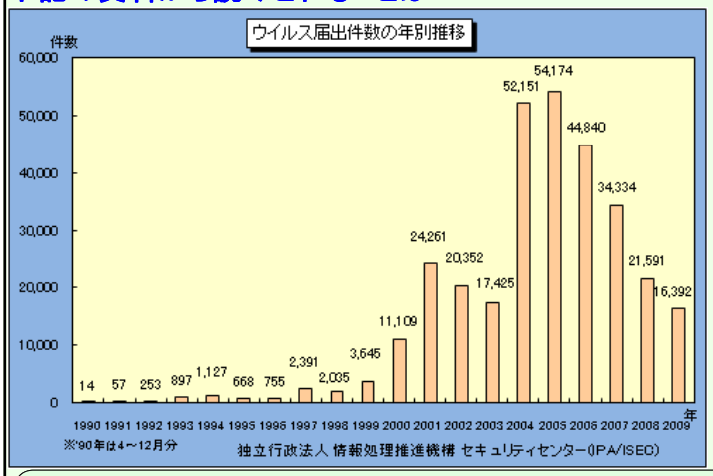


Katsuya Uchida uchidak@gol.com

情報漏洩を防ぐ
情報セキュリティ対策のあり方

他者の資料をどう見るのか？

下記の資料から読みとれることは？



でも、実際に感染は・・・

2009年	感染台数	
	感染なし	1台以上
1月	1,857	3
2月	1,448	15
3月	1,666	8
4月	1,434	4
5月	1,382	5
6月	1,452	8
7月	1,248	8
8月	1,212	10
9月	1,291	10
10月	1,204	6
11月	1,129	11
12月	972	9
合計	16,295	97

http://www.ipa.go.jp/security/txt/list.html

- 2009年の感染は100件未満(0.6%)です。 ウイルス届出件数は多いが、感染はわずか
- 何故、感染したのだろうか？
  ① ワクチンソフトが導入されていなかった ② 期限切れのワクチンソフトを使っていた
  ③ ワクチンが最新状態（パターンファイルが最新）でなかった ④ ワクチンソフトで検出できなかった（ゼロディウイルス） ⑤ その他

青丸数字のものは、利用者側で対応可能では？

Katsuya Uchida uchidak@gol.com

情報漏洩を防ぐ
情報セキュリティ対策のあり方

情報セキュリティ部門の責任放棄？

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持出が禁止されているが、それで業務活動が円滑にいくのだろうか？
- 単なる情報セキュリティ部門の責任放棄ではないだろうか？
- 「持出禁止」にすれば、持ち出された場合の対応策が全くないことになるが・・・
  - ◆ 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？
  - ➢ 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
  - ➢ 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・・・
    - 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（車内に何もなければ、犯罪者が狙う可能性は低くなる）
    - ① 大きな駐車場では、駐車場所も重要になる

  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

Katsuya Uchida uchidak@gol.com

情報漏洩を防ぐ
情報セキュリティ対策のあり方

問題・課題の明確化

組織の心理学

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？

このような個人的／組織的違反を許す組織で、
情報セキュリティだけが例外で済むだろうか？

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」）

命令系統の整備不備
- 命令・報告経路がきっちり定められていない
- 職務マニュアル、規則が整備されていない
- 経営者・管理者の権限が明確にされていない

個人的違反の容認
- 会社の電話の私的利用
- 遅刻
- 勤務時間内の職務怠慢

属 人 風 土
- 同じ提案でも提案者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が評価される
- 相手の体面を重んじ反対意見が表明されない
- 「原因がなにか」より、「誰の責任か」を優先する
- 誰が頼んだかによって、仕事の優先順位が決まる

組織的違反の容認
- 会社ぐるみの不正
- 効率のための不正
- 組織への過剰な貢献の重視

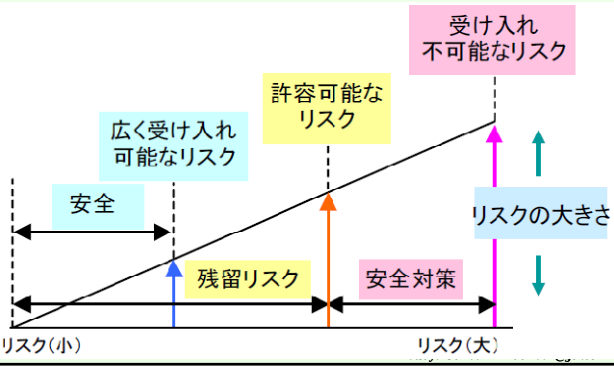
Katsuya Uchida uchidak@gol.com

安全と安心について

安全と安心

- 安全を“絶対に事故が起きないこと”と解釈している人がいるが，これは間違いである。無論，絶対に事故が起きないことは理想ではあるが，これは，「何もしない」こと以外，確実な実現は不可能だからである。「何かする」以上，安全を脅かす何かは必ず存在する。問題はその何かを人知を尽くしてコントロールすることにある。
- 具体的には，リスクという考え方が必要となる。機械やシステムの分野では，絶対安全はあり得ないとして，安全は，「人への危害または損傷の危険性が，許容可能な水準に抑えられている状態」(ISO8402：品質管理及び品質保証－用語の定義)，または，「受け入れ不可能なリスクが存在しないこと(受け入れることの出来ないリスクからの開放)」(ISO/IECガイド51：規格に安全面を導入するためのガイドの定義)と定義されている。安全が絶対安全を意味しているのではなく，“常に危険性(リスク)は残されており，それが許容可能，または受け入れ可能なもののみになっていること”としている。ガイド51 の安全の定義にはリスク(risk)という用語があり，安全はリスクを経由して定義されている。

ISO8402の定義にある「人への危害または損傷の危険性」とは，リスクのことで，リスクとは，「危害の発生する確率及び危害のひどさの組み合せ」と定義されている。ここで“組み合せ”とは，危害の発生確率の大きさと危害の大きさとの両方を勘案して，リスクの大きさを決めることを意味し，発生確率が大きいほど，また危害が大きいほど，リスクは大きく設定しなければならない。



情報漏洩を防ぐ
情報セキュリティ対策のあり方

安全と安心について

- 安全は，科学技術，社会技術の問題として論理的に，客観的に，数量的に評価されている。
安全は科学技術や社会技術として実現させることを通して，客観性を重んじる方向を目指して発展してきている。しかし，安全の定義にリスクの概念が用いられ，リスクには危害のひどさという主観的な面が含まれており，また，安全目標には価値観が含まれているので，安全をすべて客観的に，技術的に取り扱うことは困難。

- 安心は主観的に判断され，個人によって大きく異なる。人間の心理に深く根ざしている。
安心は、人が知識・経験を通じて予測している状況と大きく異なる状況にならないと信じていること、自分が予想していないことは起きないと信じ何かあったとしても受容できると信じていること。安心は、“信頼する”という人間の心と強く関係している。

- 安全の反対は危険であるが，安心の反対概念は，心配，ないしは不安であろう。安全であることは安心に大きく貢献するはずであるが，安全であっても安心できない例，逆に安心しているが実は安全でない例もあり，必ずしも一致しない。
- また、安心・不安の代わりに、信頼・不信 と言うこともできる

平成2005年8月31日
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 人間と工学研究連絡委員会安全工学専門委員会
http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-19-t1034-1.pdf

Katsuya Uchida uchidak@gol.com

情報漏洩を防ぐ
情報セキュリティ対策のあり方

マスコミ報道の特徴

通常、マスコミ報道では、非常に大きな特徴があり、それを理解しないと誤った判断をする可能性がありますが、現役の新聞記者が述べたものの一部を抜粋

- 人命に軽重があり、日本人の命は外国人より重い。有名人の命は無名人より重い
- 交通事故は1名死亡すれば地方版に載る（他の重要記事との兼ね合いがあるが）。2名以上死亡の場合は社会面、高速道路での玉突き事故では一面に載る可能性が高い。更に、子供が関係すると顔写真は必須。ひき逃げでは1人の死亡でも社会面が多い。車の欠陥の場合は怪我だけでも大きなニュースに
- 航空機事故は被害者に日本人がいるかどうか。日本人死亡者は全員顔写真を載せる。死亡者が多いと事故原因等は一面、社会面は搭乗者の情緒的報道（搭乗理由、乗る前の様子等）を行う
- 原発事故は公開原則があるため、小さな事故でも必ず載せる。海外での大事故では膨大な紙面を割く。また、推進派と反対派の双方からコメントをとるため、大きな紙面をとることになる
- 工場等での爆発・火災等の事故では、被害者が従業員だけだと情緒的報道になることは少ないが、目が痛くなった程度でも周辺への被害があれば大きく報道され、声高に管理ミスを批判する
- 医薬品の副作用等で、医薬品を全否定する記事は過去にはあったが、最近は少ない。厚労省の「副作用モニター」で死亡者等の発表を始めたため、扱いが小さくなった
- 食品添加物等は表示の義務づけ後は死亡事故もなかったため記事も少なくなった
- 発がん性物質も「大量の摂取」での研究についての批判もあり、少なくなった

Katsuya Uchida uchidak@gol.com

情報漏洩を防ぐ
情報セキュリティ対策のあり方

マスコミ報道の特徴

新型インフルエンザ報道

最近の例では、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・団体で従業員の外出を控えさる、外出時にマスクをする、早めに休暇を取る、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の禁止、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。しかし、季節性インフルエンザでは、2000年以降、214人（2001年）～1,818人（2005年）の死者がでている 。

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、安心と考えている。」

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。

マスコミの特徴として、とらえておくことが大切です。
更に、最近はインターネット（ブログ、SNS、ツイッター等）からの情報もあります

Katsuya Uchida uchidak@gol.com

ご注意を！

パスワードを暗号化していないウェブサイトについて

- 最近、大規模なアカウント情報（ユーザID/パスワード）の漏えいが発生しました
- アカウント情報を要求しているが、パスワードを暗号化（ハッシュ化）せず、保存しているウェブサイトでした
- 従来から、一部のセキュリティ専門家は、このようなウェブサイトの危険性を指摘していました
- ウェブサイトがパスワードの暗号化をしているかの判断方法としては、以下のことを行って下さい
  - アカウント情報のログイン画面で、「パスワードを忘れた方」等の表示をクリックし、その処理に従う（通常は、登録メールアドレスに情報が送付される）
  - 登録したメールに送られてきた情報に、自分の入力したパスワードが表示されていたら、危険なウェブサイトです

    適切なウェブサイトは、新しいパスワードを入力させるための画面のURLを送ってきます
- なお、このようなウェブサイトのパスワードを企業内のパスワード等と同じにしない。 また、重要情報（クレジットカード情報、銀行口座情報等）は、ウェブサイトに保存しない方法を選択しましょう

ハッシュ化： 一方向関数とも呼ばれる方法で、テキストファイルを一定の文字列に変換します。ハッシュを利用すると、元のテキストに戻せません。 もし、「パスワードを忘れた」との処理を行って、入力したパスワードをメールで送ってくるウェブサイトは、このハッシュ化をしていないことになります。このため、パスワードファイルが何らかの方法で漏えいすると、利用者全てのアカウント情報が漏えいします。 このようなサイトを利用しないことが一番ですが・・・

Katsuya Uchida uchidak@gol.com

まとめ

- 情報セキュリティの危険性は、報道等より遙かに安全である感じを受ける
- 情報セキュリティには、多くの「都市伝説」が存在する感じを受ける
- 危険だと報道されている内容も、それなりに対応策がある
- 対策を行わず、被害者だと考えていいのだろうか？
- 個人情報漏えいであれば、多くの人々の人権を侵害する可能性もある
- もちろん、100% の安全は情報セキュリティでも確保できない
- 自社で対応できなければ、外部に委託せざるを得ないが、「100%完璧なシステムを構築できる」と言うような業者は避けるべきかも？
- 情報セキュリティの確保には、現実の世界での防犯等の知見も役に立つ

Katsuya Uchida uchidak@gol.com

参 考 資 料

- 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
- 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1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
- ダン・ガートナー リスクにあなたは騙される 早川書房 2009年
- ノーマン 誰のためのデザイン 新曜社 1990年
- M. A. ロベルト なぜ危機にきづけなかったのか 英治出版 2010年2月

ありがとうございました

中央大学 研究開発機構 教授

兼 横浜市CIO補佐監

情報セキュリティ大学院大学 名誉教授

内田 勝也

uchidak@gol.com

http://www.uchidak.com/