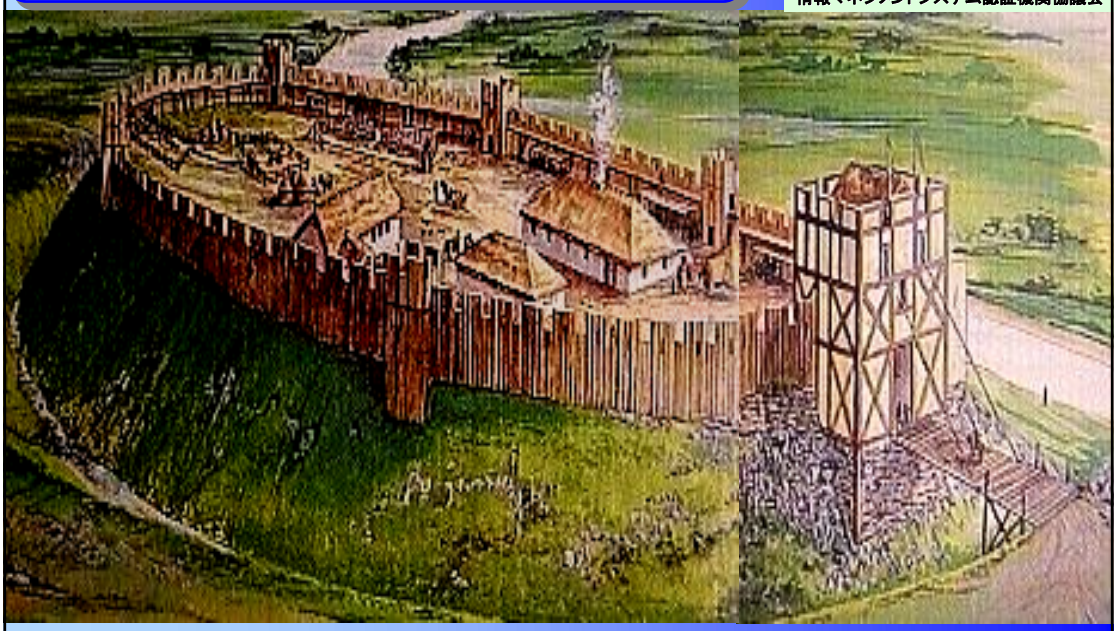
ISMSの有効性の向上と認証審査

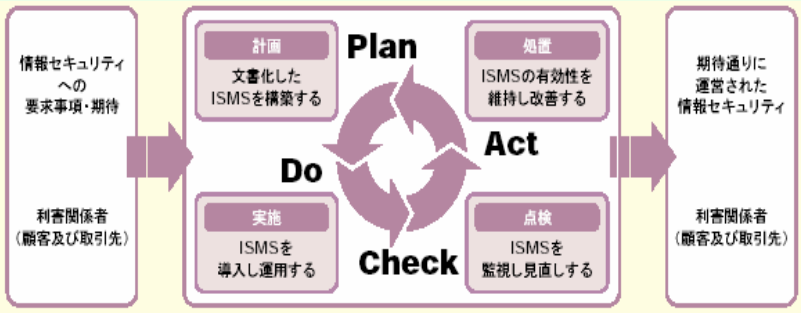
2009年3月03日
ISMSセミナー 2009
情報マネジメントシステム認証機関協議会



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）

PDCAモデルによるプロセスアプローチ



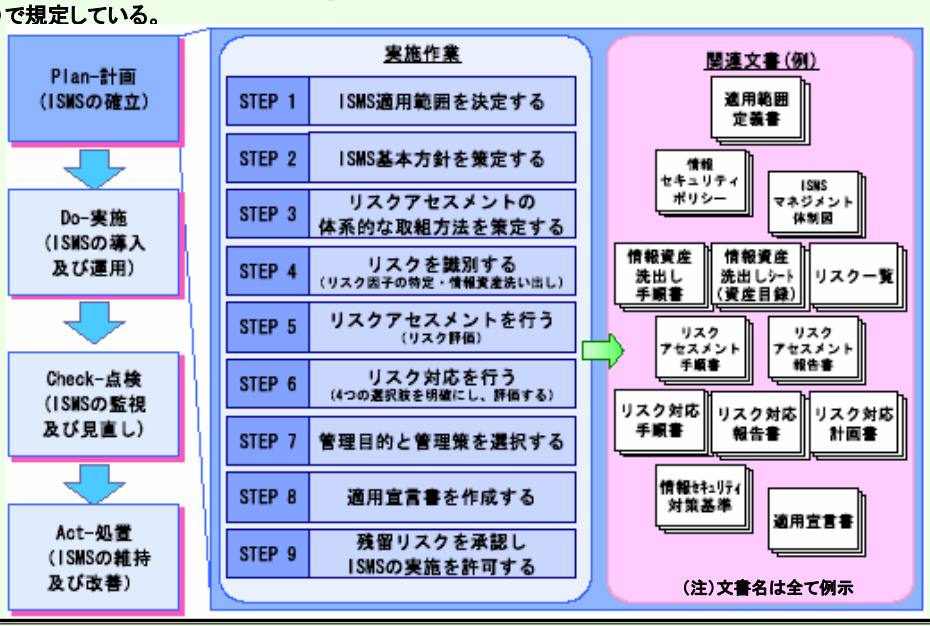
プロセスアプローチとは、インプットをアウトプットに変換するため、経営資源を使って運営管理される全ての活動をプロセスとみなし、組織内のプロセスを明確にし、その相互関係を把握し、一連のプロセスをシステムとして適用し、運営管理すること。
プロセスアプローチを採用するメリットは、個々のプロセス間のつながりを管理し、プロセスの組合せや相互作用を管理することにより、ISMSを有効に機能させることができる

Plan－計画（ISMSの確立）	組織の全般的な基本方針及び目標に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連する情報セキュリティ基本方針、目標、対象、プロセス及び手順を確立する。
Do－実施（ISMSの導入及び運用）	その情報セキュリティ基本方針、管理策、プロセス及び手順を導入し運用する。
Check－点検（ISMSの監視及び見直し）	情報セキュリティ基本方針、目標及び実際の経験に照らしてプロセスの実施状況を評価し、可能な場合これを測定し、その結果を見直しのために経営陣に報告する。
Act－処置（ISMSの維持及び改善）	ISMSの継続的な改善を達成するために、マネジメントレビューの結果に基づいて是正処置及び予防処置を講ずる。

- ISMSの確立（文書・記録管理）
- ISMSの導入・運用（教育）
- ISMSの監視・見直し（内部監査）
- マネジメントレビュー
- ISMSの維持及び改善

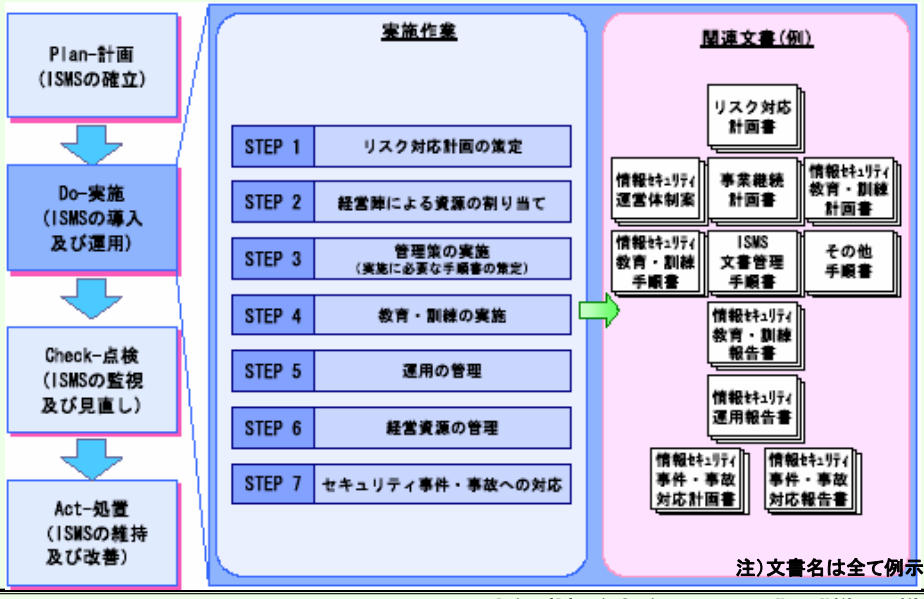
1．ISMSの確立（Plan-計画）

本認証基準の「ISMS の確立及び運営管理」では、(1) ISMS の確立の手順 を以下の9つのステップ（STEP 1～STEP 9）で規定している。



2. ISMSの導入及び運用(Do-実施)

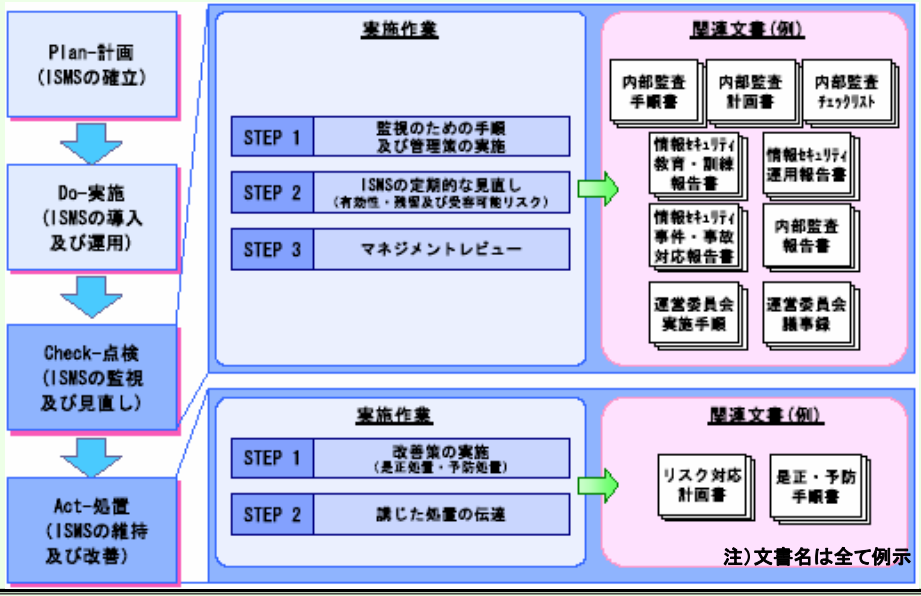
本認証基準の「ISMS の確立及び運営管理」では、ISMSの導入及び運用の手順 を以下の7つのステップで規定している。



注)文書名は全て例示

3. ISMSの監視及び見直し(Check-点検)・ISMSの維持及び改善

本認証基準の「ISMS の確立及び運営管理」では、(3) ISMSの監視及び見直し、(4)ISMSの維持及び改善の手順 を図のように規定している。



注)文書名は全て例示

情報セキュリティマネジメントシステムの基本的な考え方

- PDCAモデルによるプロセスアプローチ
- PLAN（計画段階）で、行うべきことは？
  - リスクを考え、そのリスクを許容できるようにする
  - ISMSの基準（クライテリア）である管理策・管理目的から、リスクを考慮して管理策・管理目的を作成し、
    - 適用宣言書に記載する
    - 適用宣言書の管理策・管理目的はISMSの管理策・管理目的と同じ？

この管理策・管理目的は唯一絶対だろうか？

- DO（実施段階）では、
  - 教育・周知と報告：計画したものが確実に実施されるためには、技術の実装も必要になるが、運用する人々（従業員：含 正規・非正規）への教育・周知を行うことと、報告（報告・連絡・相談）の仕組みの構築を行う必要がある

マネジメントの基本では？

- CHECK（監視・見直し）では、
  - 監査が非常に重要だが・・・

監査の考え方

4.2.1 ISMSの確立

関係者の多くが理解していないが、最も重要な事柄 では？

g）リスク対応のための、管理目的及び管理策を選択する
管理目的及び管理策は、リスクアセスメント及びリスク対応のプロセスにおいて特定した要求事項を満たすために選択し、導入しなければならない
選択は、法令、規制及び契約上の要求事項と同じく、リスク受容基準も考慮する
このプロセスの一部として、附属書A の中から、特定した要求事項を満たすために適切なように、管理目的及び管理策を選択しなければならない
管理目的及び管理策は全てを網羅していないので、追加の管理目的及び管理策を選択してよい。
注記　附属書Aは、様々な組織が共通的に関連する管理目的及び管理策を幅広く集めたリストである。 この規格の利用者には、附属書A を重要な管理策の選択に見落しがないことを確実にする、管理策選択の出発点として示す。

情報セキュリティマネジメントシステム－要求事項　JIS Q 27001: 2006 (ISO/IEC 27001:2005)

監査を前提にしている

監査概念が明示的でないが、常識として考えている？

検査と（業務）監査

- 検査：決まったルールに基づいて事務手続きが行われているかどうかをチェックする
- 監査：ルールがリスクを防ぎ、内部統制上、望ましい内容かどうかをチェックする

先端内部監査研究会著「これが金融機関の内部監査だ」（第1版）金融財政事情研究会　より

組織内外の環境の変化や時間の経過でも、リスクは変化する！

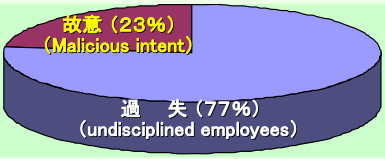
問題・課題の明確化（その1）

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



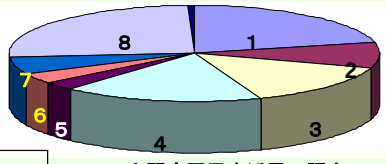
InfoWatchの調査
http://www.infowatch.com/threats?chapter=162971949&id=207784626

（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

問題・課題の明確化（その2）

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3）

心理学の知見の利用：記銘時のエラー（記憶について）

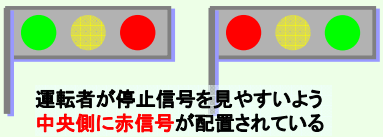
- 記憶の過程には、記銘（符号化）、保持（貯蔵）、想起（検索）の三段階がある
- 記銘は、記憶の第1段階で新しい情報を覚えることで、
  - 意識的に記憶しようとして覚える場合と
  - 自然に記憶に残る場合がある

  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）



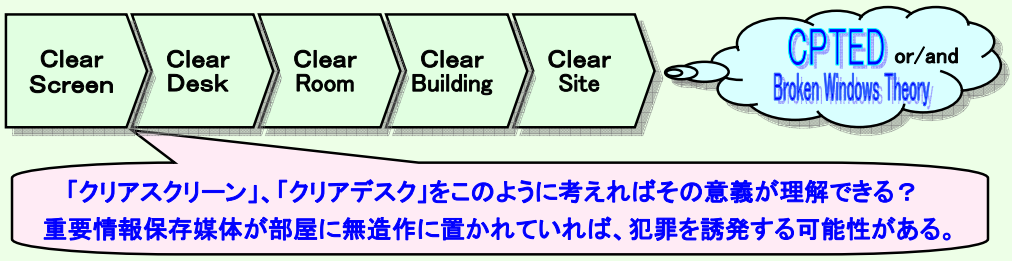
運転者が停止信号を見やすいよう
中央側に赤信号が配置されている

- 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3）

「クリアスクリーン」・「クリアデスク」の考え方



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

声明・通達に無意味さ！

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

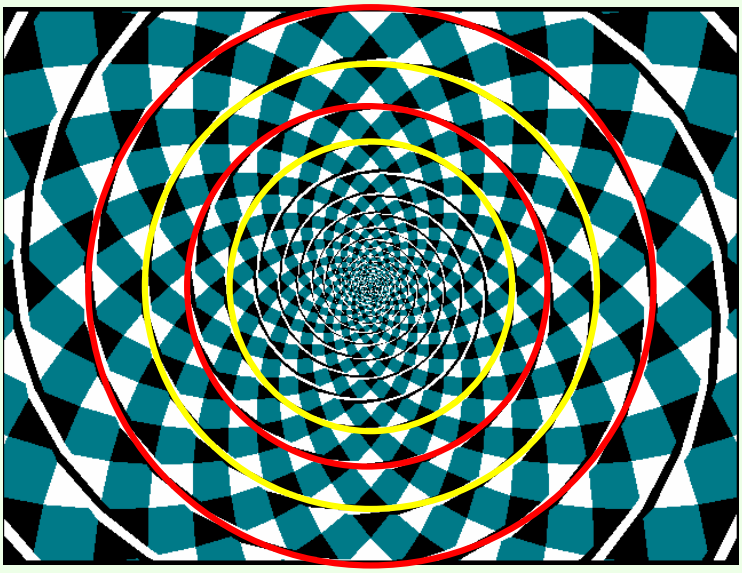
「理性が働いている」前提の対策でなく、「理性が働いていなくても、可能な対策」

- 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　ピーンチ！」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4）

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5）

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1986年に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。

組織内の全ての個人が安全に対し責任を負うもので、基本方針、管理者、個人の3階層のレベルがあるとした

- 基本方針レベル： 政府・経営層等、組織の高い意思決定レベルにおける決定事項で、組織・個人活動を左右する
- 管理者レベル： 基本方針に則った個人の態度や慣行を醸成する環境作りと制度の整備
- 個人レベル： 安全に関係するタスクに取りかかる前に、自分の任務、責任、知識が十分か、状況に異常がないか、支援が必要か等を常に問いかける姿勢で臨むことが求められる。 規則・手順等の遵守し、問題発生時には立ち止まって考え、近道や大胆な行動を避けるような厳密かつ慎重なアプローチで臨まなければならない

Culture of Security の概念の導入

ネットワークのセキュリティに関する新たな「思考や行動の方法」を総称して、‘Culture of Security’という概念を導入した

http://www.soumu.go.jp/s-news/2002/020807_13.html

ISMSの有効性の向上と認証審査

問題・課題の明確化（その5）

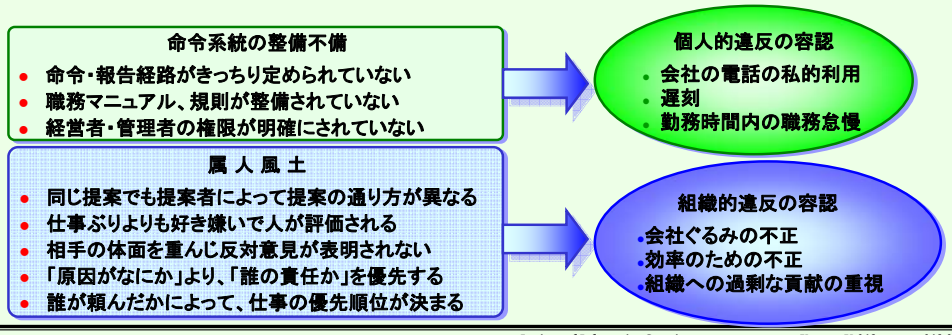
組織の心理学（その2）

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

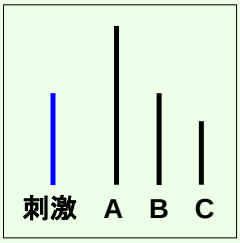
- 組織違反の特徴の1つに「無責任の構造」がある
- 無責任構造を生みだし易い組織風土の特徴は、「属人主義」がある
- 属人主義：評価・決定時に、「誰がそれを行っているのか」という、人情報を重視する傾向が強い。これを「属人風土」と呼ぶことにする
  - 会議・ミーティングでは、同じ提案でも誰が提案者かによって、提案の通り方が異なる
  - 仕事ぶりよりも好き嫌いで人を評価する傾向がある
  - 相手の体面を重んじ、会議・ミーティング等で反対意見が表明されないことがある
  - トラブルが生じると、『原因が何か』より『誰の責任か』を優先する雰囲気がある
  - 誰が頼んだかにより、仕事の優先順位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



問題・課題の明確化（その6）

- 「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。

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

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

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

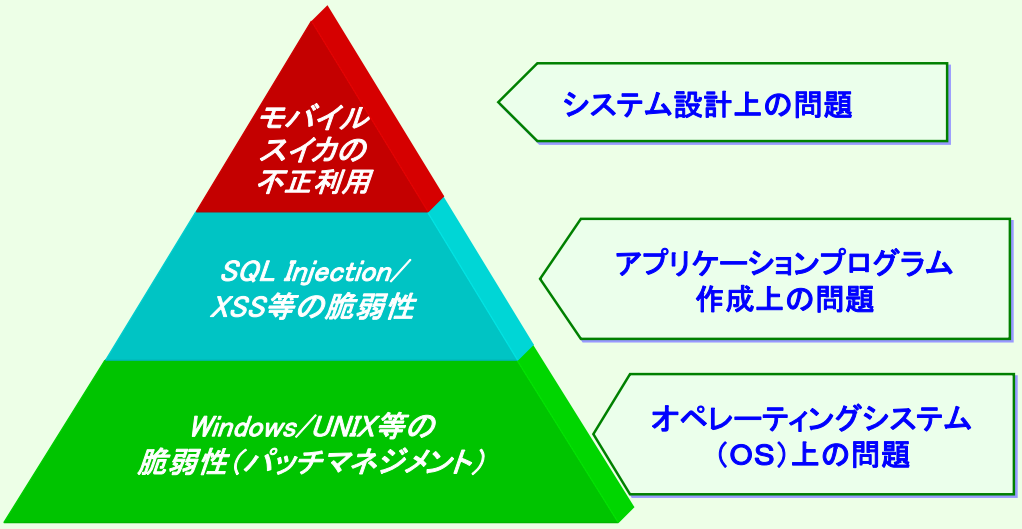
ここまではなかなか言えないが・・・

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・・・

ホップ・ステップ・ジャンプ

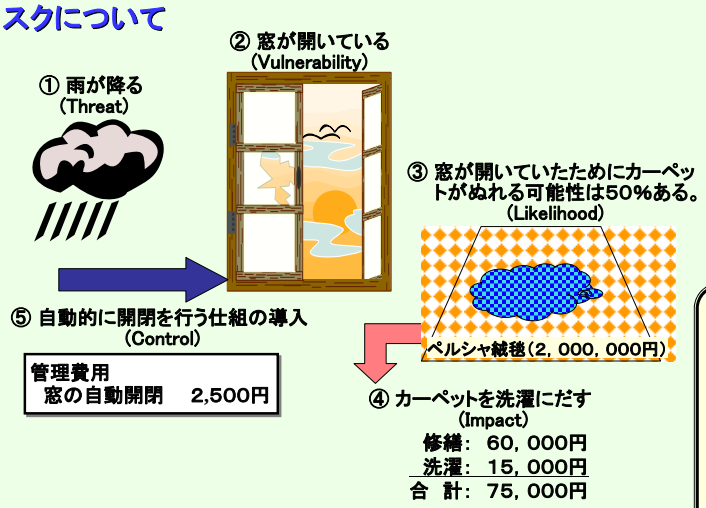
OS等の下位層の問題から、適用業務システムの問題へ！

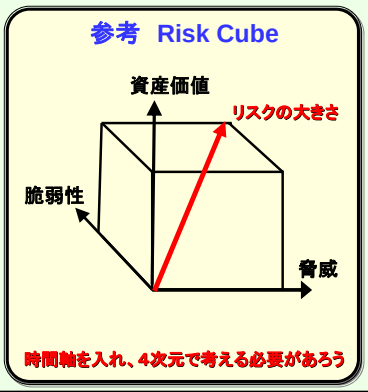
その対応ができているのだろうか？



リスクの考え方

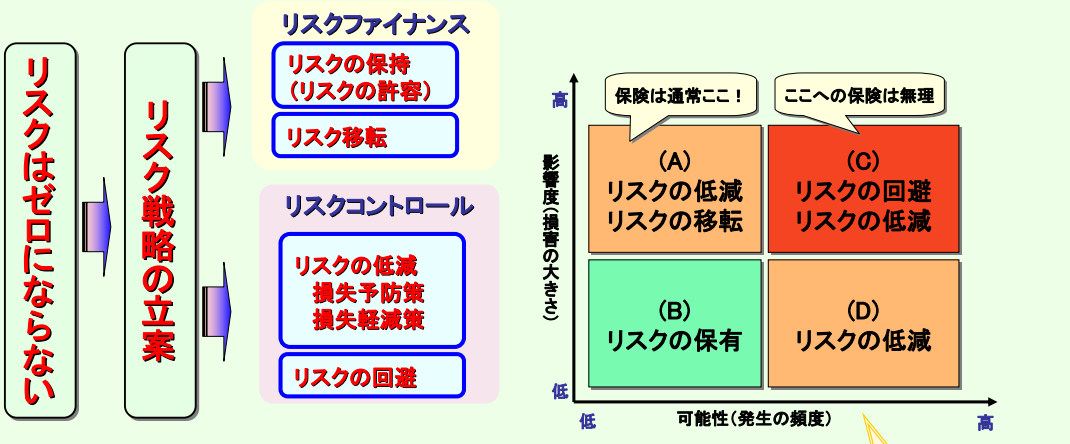
リスクについて





上記の①～⑤をリスク管理では以下のように定めている。
① 脅威　(Threat)
② 脆弱性 (Vulnerability)
③ 可能性 (Likelihood)
④ 影響　(Impact)
⑤ 管理策 (Control)

リスクの考え方



(A) 影響度が大きいが、発生頻度は低いので、損害を小さくするための「リスクの低減」を施すとともに、保険による「リスクの移転」も検討する。
(B) 影響度も可能性も低いので、「何もしない」(リスクの保有)選択がある。
(C) 影響度も可能性も高い場合、「影響度、可能性を減らす」ことが大切になる。
(D) 可能性が高いが、影響度(損害)は小さいので、リスクの低減を行う。また、リスク保有の検討も行う。

リスクを考える（他山の石？）

コンピュータウイルスによるネットワーク障害

平成15年8月22日（金）大阪府発表資料より

- 庁内ネットワークの復旧状況 （平成15年8月22日（金）15時現在）

作業経過

- 8月19日（火）午前9時10分ごろ、コンピュータウイルス「Welchia（ウエルチア）」によるネットワーク障害が発生
  初日の対応： 状況把握、作業方針の確認、ウイルス対策ソフト（CD－ROM）の作成（約500枚）、作業手順書作成
- 2日目（8月20日）：本庁及び出先機関の職員への説明会で作業手順を説明。本来は、この対応作業を行い安全確認された端末機を順次接続することにしていたが、ウイルス対策が不完全な状態のものが接続され、ウイルスがネットワークに広がる恐れが出たため、端末機のクリーニング作業のみを実施
- 3日目（8月21日）：感染した端末機が接続されないよう、所属単位で責任を持って対応することを徹底し、準備の整った所属から順にネットワークに接続を開始した。この結果、本庁・出先あわせて92所属、端末機全体の約半分を接続
- 4日目（8月22日）：本日も同様の手順で接続作業を継続し、ネットワークの再接続はほぼ完了する見込み
- 当面の対応：感染した端末機が残っている恐れもあるため、ネットワークの常時監視を継続する

原因について

- 現在原因究明中だが、何らかの原因によりウイルスに感染したパソコンが庁内ネットワークに接続されたと考える
- また、ウイルス定義のパターンファイルが最新のものに更新されていないパソコンが一定数あり、感染が一気に拡大し、感染されたパソコンからの異常な通信がネットワーク回線を埋め、他のパソコンからの通信ができなくなった

今後の対応

- セキュリティホールに対するセキュリティパッチの適用
- 個人所有PCの庁内使用の禁止など、ネットワーク利用モラルの徹底
- ネットワーク管理体制及び監視機能の強化

ウイルス感染状況（8月21日16時現在）	調査台数：4,174台	感染台数：1,314台（約 31.5%）	
端末機との再接続（8月22日15時現在）	本　庁	80／ 91	約88%
	出先機関	73／106	約69%
	全　体	153／197	約77%

- 府の発表をみている限り、2日間、パソコンを利用した作業ができなかった
- 3日目に半数が復旧し、完全復旧は4日目になった
- 直接的な作業（費用）
  - CD-ROM（500枚）作成、 作業手順書の作成
  - 端末クリーニング（8000台？）作業

他山の石： よその山から出た粗悪な石でも、自分の宝石を磨く役には立つという意から）自分より劣っている人の言行も自分の知徳を磨く助けとすることができる ［岩波書店 広辞苑第五版］

リスクを考える（他山の石？）

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

この様な他社事例から、「投資対効果」を考えることができるのでは？

忘れてはいませんか？

情報について

- 個人情報保護法の施行以降、「情報セキュリティ＝個人情報保護」と考える傾向が強い？
- 本来、情報あるいは、関連する（情報）資産には、以下のものがある
  - 関連設備　　建物、電源、空調設備、監視設備等
  - ハードウェア　　コンピュータ機器、ネットワーク機器等
  - ソフトウェア　　基本ソフト、アプリケーションソフト等
  - 情報　　IT情報、印刷物等
  - 人間　　関連要員

ここにもっと
注目すべきでは？

- 東京大学 藤本隆宏教授の定義
  - 全ての産業は広義の情報産業と考えられる
    - 情報が無形メディアにあれば、サービス業
    - 情報が有形のモノにあれば、製造業
  - 「製品開発・生産・販売」の一連の企業活動で、
    - 製品開発は、製品設計情報の創造し、生産へ伝達する機能
    - 生産は、製品設計情報の転写する機能
    - 販売は、製品（製品設計情報）を顧客に発信する機能

藤本隆宏「生産マネジメント入門」日本経済新聞社

知的財産

- 発明、考案、植物の新品種、意匠、著作物その他の人間の創造的活動により生み出されるもの
- 商標、商号その他事業活動に用いられる商品又は役務を表示するもの
- 営業秘密その他の事業活動に有用な技術上又は営業上の情報

改革への戦略（？）

改革を進めるために

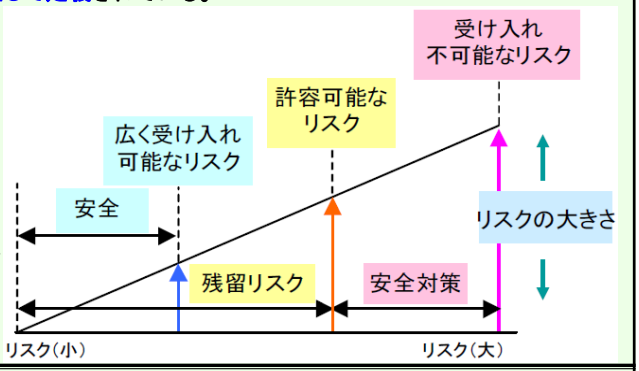
- 時間の経過や環境の変化によって、当初、策定した制度や仕組みも色々な課題がでてくる。 制度検討時点で全ての課題を解決して、制度を構築できなければ、一定期間後に見直しをするのは必要であろう。 最近の第三者認証制度等のマネジメントシステムを見ていると特に感じる。 PDCAサイクルやリスクを考える制度が、制度の見直しを不要と考えることは、自己矛盾であろう

- 制度を改善するには、制度自体に大きな問題がないと変更が難しいと言われる。小さな問題に対処することが、結果的に制度自体を長期に安定化することになる。 これは、「割れ窓理論」を実践したことにより、安全な町になったニューヨーク市の例を考えれば明らかであろう。
  労働安全分野では、「ハインリッヒの法則」があるが、基本的には同じ

安全と安心（1）

- 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。



安全と安心（2）

- 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，数量的に評価される試みが行われている。リスクという概念が用いられ始めたのは，このためと考えられる。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。
- 一方，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。
  安心について，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。

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

「事故前提社会」とは、事故が有り得るから諦めて事前予防に向けた対策を行なわないとか、どのような被害にあっても、それは仕方ないものであると諦めさせるとかいうことを意味するものでは決してない。

2008年6月19日
情報セキュリティ政策会議「次期情報セキュリティ基本計画に向けた第1次提言」

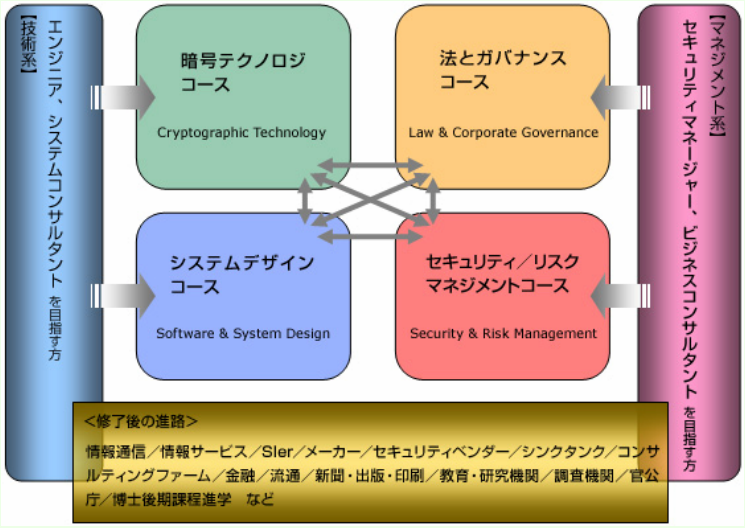
なぜ、「事故前提社会」という言葉を使わなければならないのだろうか？
「安全・安心な社会」の方が分かり易いし、前向きな感じがするのだが。

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

情報セキュリティ大学院大学 修士課程コースのご案内

広い視野に立ち、現実の情報セキュリティの問題解決を担う高度な専門技術者、
実務家と、将来方向をリードする創造性豊かな研究者を育成



本日の内容は、ISMS講座を中心に述べたものです

情報セキュリティ大学院大学
博士前期(修士) 及び博士後期(博士)課程

カリキュラム： 技術・管理運営・法制度・情報倫理を相互に連携、協調させ横断的で創造的な情報セキュリティ教育を目指す

情報セキュリティ輪講Ⅰ	*情報セキュリティ特別講義*	暗号・認証と社会制度	暗号プロトコル
アルゴリズム基礎	数論基礎	暗号理論	計算代数
個人識別と個人情報保護	インターネットテクノロジ	不正アクセス技法	ネットワークシステム設計・運用管理
セキュアシステム構成論	情報デバイス技術	情報システム構成論	オペレーティングシステム
セキュアプログラミングとセキュアOS	プログラミング	ソフトウェア構成論	セキュアシステム実習
情報セキュリティマネジメントシステム	セキュリティシステム監査	セキュリティ管理と経営	リスクマネジメント
組織行動と情報セキュリティ	統計的方法論	プレゼンテーション技法	セキュア法制と情報倫理
法学基礎	知的財産制度	国際標準とガイドライン	セキュリティの法律実務
情報セキュリティ輪講Ⅱ	特設講義	**以上は全て2単位**	
研究指導(6単位)	*プロジェクト研究指導(4単位)*	**1年コースの場合、研究指導の代わりに、プロジェクト研究指導**	

以下は、博士後期(博士)課程

情報セキュリティ特別研究(6単位)	情報セキュリティ博士演習	情報セキュリティ技術特論	情報セキュリティ管理特論

注) 科目名の後ろに単位が記載されていないものは、全て2単位　　*赤字* の科目は必修科目

修了要件：

- 博士前期(修士 2年制)課程　年限 = 原則2年　修得単位 = **30単位**以上(含 研究指導6単位)　修士論文
- 博士前期(修士 1年制)課程　年限 = 原則1年　修得単位 = **46単位**以上(含 プロジェクト研究指導4単位)　プロジェクト研究
- 博士後期(博士)課程　年限 = 原則3年　修得単位 = 8単位以上　博士論文

科目履修(最大10単位修得可能)制度も活用されている

博士前期(修士 2年制)では；

- **1年目は平日夜間3日程度と土曜日で、所要単位を取得。(夜間：18:20～19:50、20:00～21:30　土曜日：9:00～16:50)**
- **2年目は研究指導(修論作成)を中心にして、卒業を目指している。 社会人で昼間を利用する学生は1、2名程度**

後期博士課程：①修業年限：3年以上(教授会が優秀な研究業績者と認めた者は1年以上)　②所要単位：8単位以上
③博士論文審査および最終試験

ウェブ：http://www.iisec.ac.jp/

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/