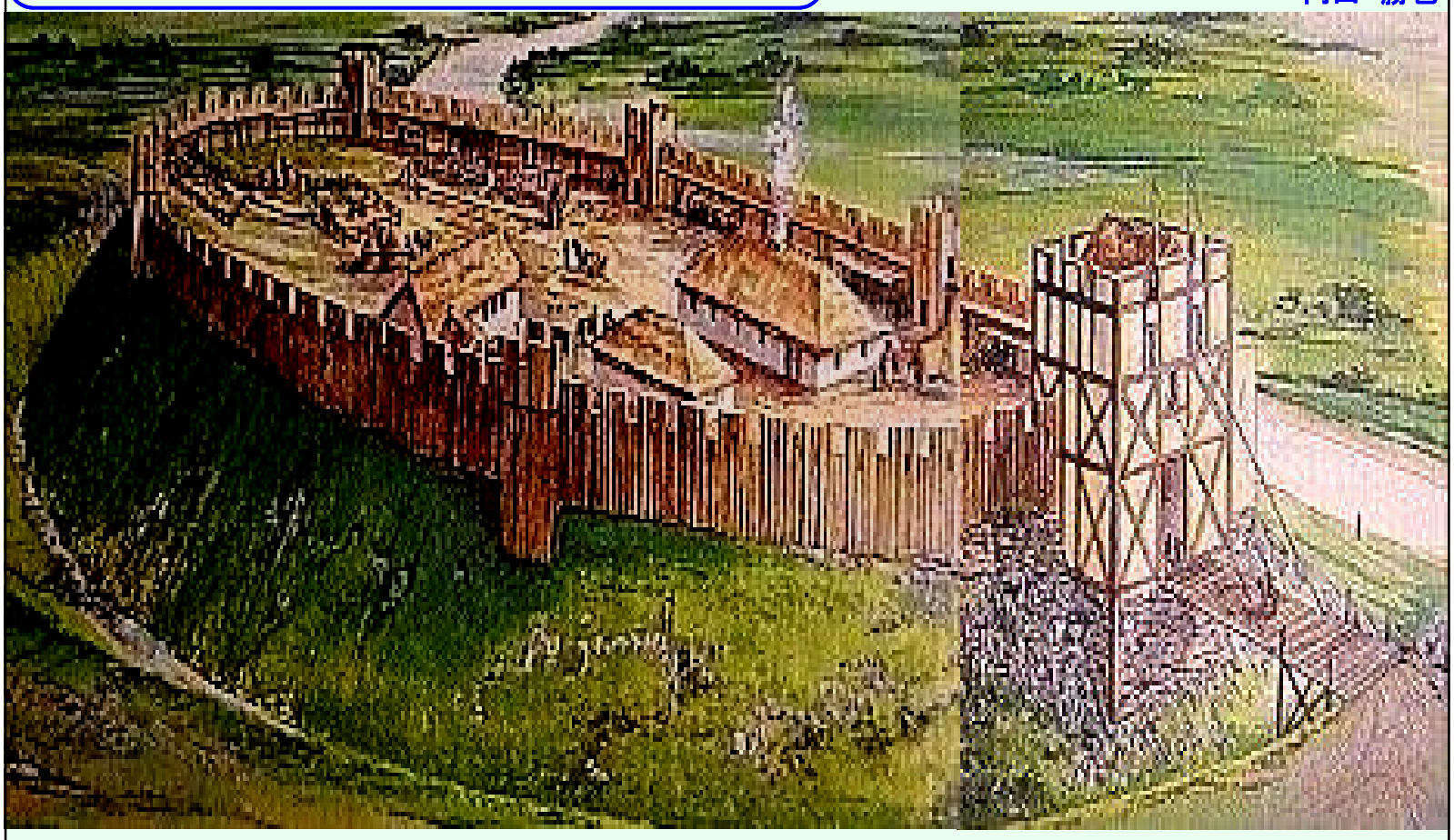
情報セキュリティ心理学の体系化を目指して

中央大学研究開発機構
内田　勝也

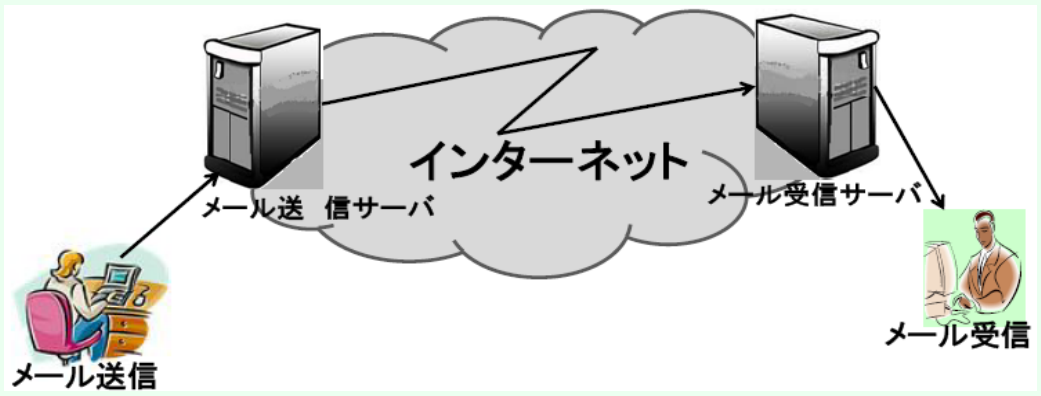


内田　勝也（uchidak@gol.com）

情報セキュリティ心理学の体系化を目指して

何が危険なのだろうか？

電子メールの例



（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

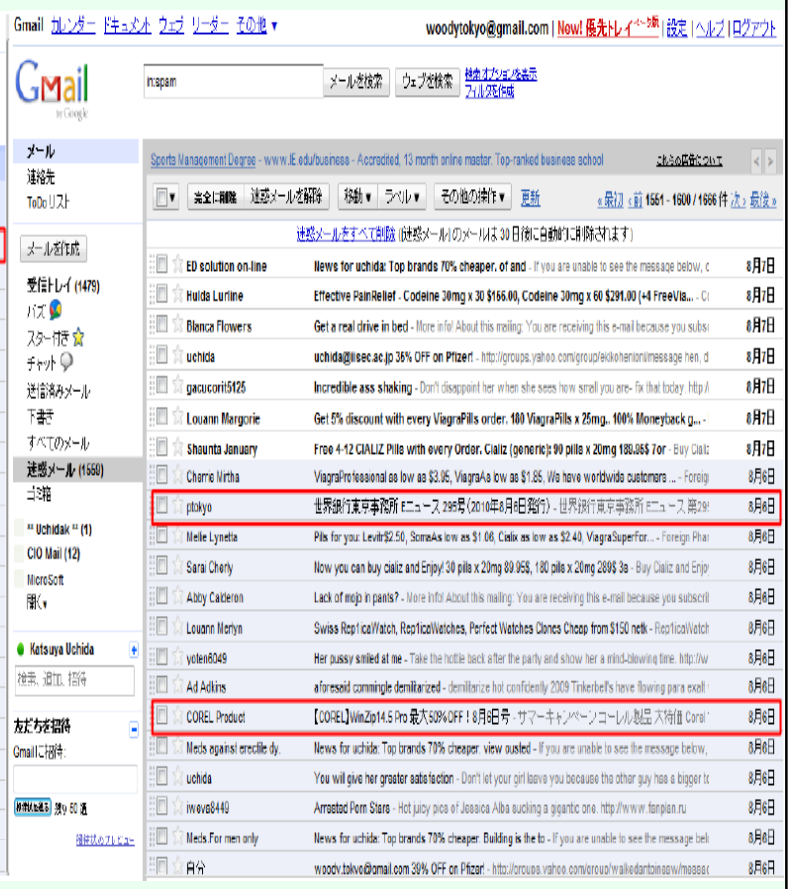
メールの危険性を考えると、(1-1) は危ない可能性があるが、
他は業務に支障（2-1）があるが、危険性の観点からは問題はない

情報セキュリティ心理学の体系化を目指して

何が危険なのだろうか？

（1－1）電子メールの例

（2－1）電子メールの例



ページ 3

情報セキュリティ心理学の体系化を目指して

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」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）j情報を取得できれば、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社への攻撃でも、ソーシャルエンジニアリングが使われている

- なりすまし：他人になりすまし、必要な情報を収集。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と呼ばれる。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、オフィスや工場等に侵入する
- 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

ページ 4

情報セキュリティ心理学の体系化を目指して

何が危険なのだろうか？

- 電子メールにおける情報セキュリティ技術では、100%完全な対応ができない
- 関係する人が対応する必要がある
- １人の関係者の不用意な対応が、組織全体のシステムを崩壊させてしまう可能性がある
- ソーシャルエンジニアリングによる攻撃も技術ではなく、人間の心理的弱さを利用している

- 技術だけでは防げない課題は、人間や組織の特性を考えて対応する仕組みが必要になる
- ソーシャルエンジニアリングを利用している攻撃者の一人は、
  ロバート・B・チャルディーニ「影響力の武器」誠信書房
  を、攻撃者・被害者のバイブルとしてあげている

情報セキュリティ心理学の体系化を目指して

ソーシャルエンジニアの武器！？

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
   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

情報セキュリティ心理学の体系化を目指して

組織と個人の特性

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

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

→ **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

→ **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

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」)

組織違反の例

組織にとって良いと考えたことが、結果的にセキュリティ事故に繋がる。
緊急業務のため、セキュリティ違反を承知で、自宅にデータを持ち帰り、自宅のパソコンで処理をしたが、Winnyによる情報漏えいを起こしてた

ページ 7

情報セキュリティ心理学の体系化を目指して

状況別犯罪防止論

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／酒の統制 ●breathalyzers in pubs ●alcohol-free events

B. Cornish, and V.Clarke. Twenty-five Techniques of Situational Crime Prevention. 2003
http://www.popcenter.org/library/crimeprevention/volume_16/OpportunitiesPrecipitators.pdf

ページ 8

情報セキュリティ心理学の体系化を目指して

情報セキュリティマネジメントシステム

情報セキュリティマネジメントシステム（ISMS）

管理策（チェックリスト）は、A.5からA.15の11グループに分かれており、各グループは更に39の中項目、133の詳細管理策からなっている

	管　理　策	中項目	小項目
Ａ．５	セキュリティ基本方針	１	２
Ａ．６	情報セキュリティのための組織	２	１１
Ａ．７	資産の管理	２	５
Ａ．８	人的資源のセキュリティ	３	９
Ａ．９	物理的及び環境的セキュリティ	２	１３
Ａ．１０	通信及び運用管理	１０	３２
Ａ．１１	アクセス制御	７	２５
Ａ．１２	情報システムの取得、開発及び保守	６	１６
Ａ．１３	情報セキュリティインシデントの管理	２	５
Ａ．１４	事業継続管理	１	５
Ａ．１５	順守	３	１０

情報セキュリティ心理学の体系化を目指して

状況別犯罪防止論とISMSのマッピング

状況的犯罪防止論と情報セキュリティマネジメントシステムのマッピングで、リアル空間での犯罪防止論をリアル・バーチャル空間の情報セキュリティに拡張

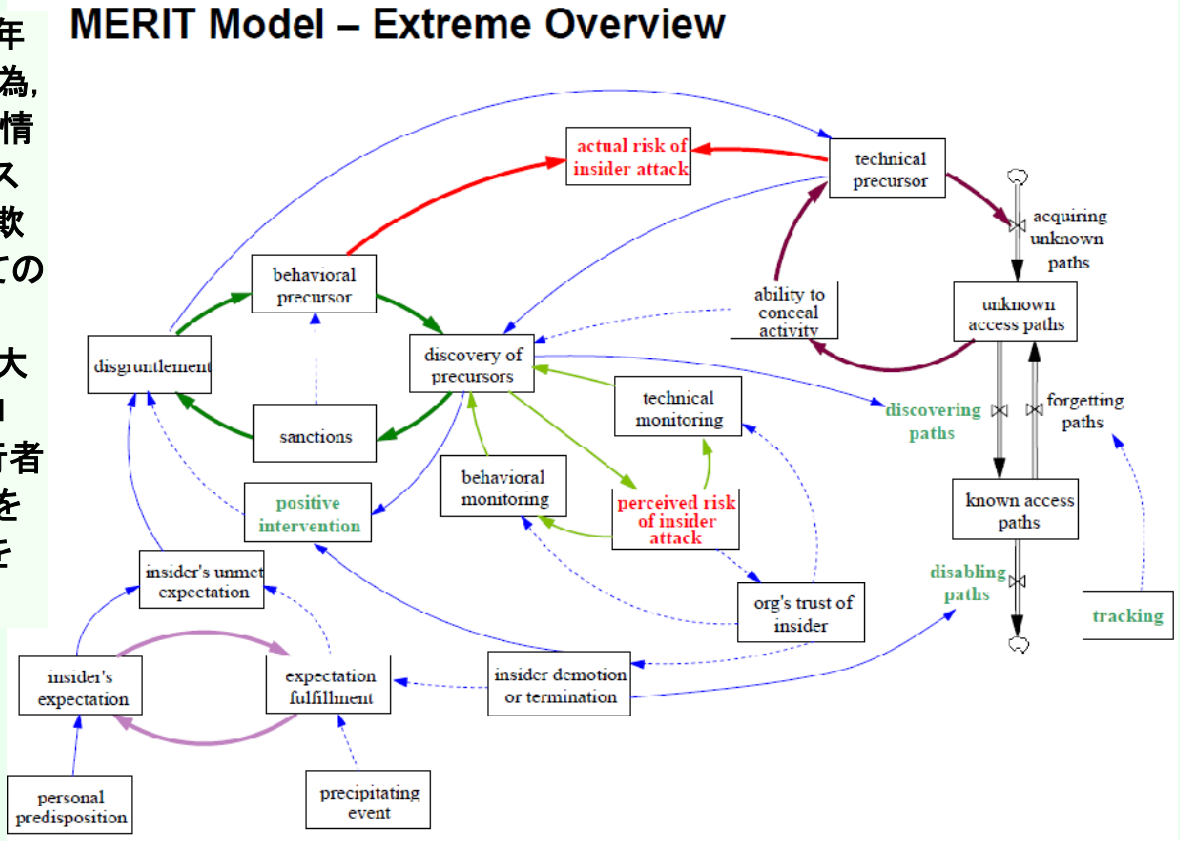
状況的犯罪防止論とISMSとのマッピング	犯罪の予防策の増強	犯罪へのリスクを高める	犯罪報酬の減少	犯罪誘因の減少	犯罪弁明の排除
セキュリティ基本方針					●
情報セキュリティのための組織					●
資産の管理			●		
人的資源のセキュリティ				●	
物理的及び環境的セキュリティ	●	●			
通信及び運用管理	●	●			
アクセス制御	●		●		
情報システムの取得、開発・保守					●
情報セキュリティインシデント管理	●				
事業継続管理		●			
順守					●

情報セキュリティ心理学の体系化を目指して

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。



http://www.cylab.cmu.edu/research/projects/current_projects/merit.html

ページ 11

情報セキュリティ心理学の体系化を目指して

内部犯罪者の研究(国内)

国内でも内部犯行者の調査研究が行われるようになった

http://www.syaanken.or.jp/02_goannai/08_cyber/cyber2203_01/pdf/cyber2203_01.pdf

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報告書

平成 22 年 3 月

目　次

財団法人 社会安全研究財団
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会

ページ 12

情報セキュリティ心理学の体系化を目指して

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。

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

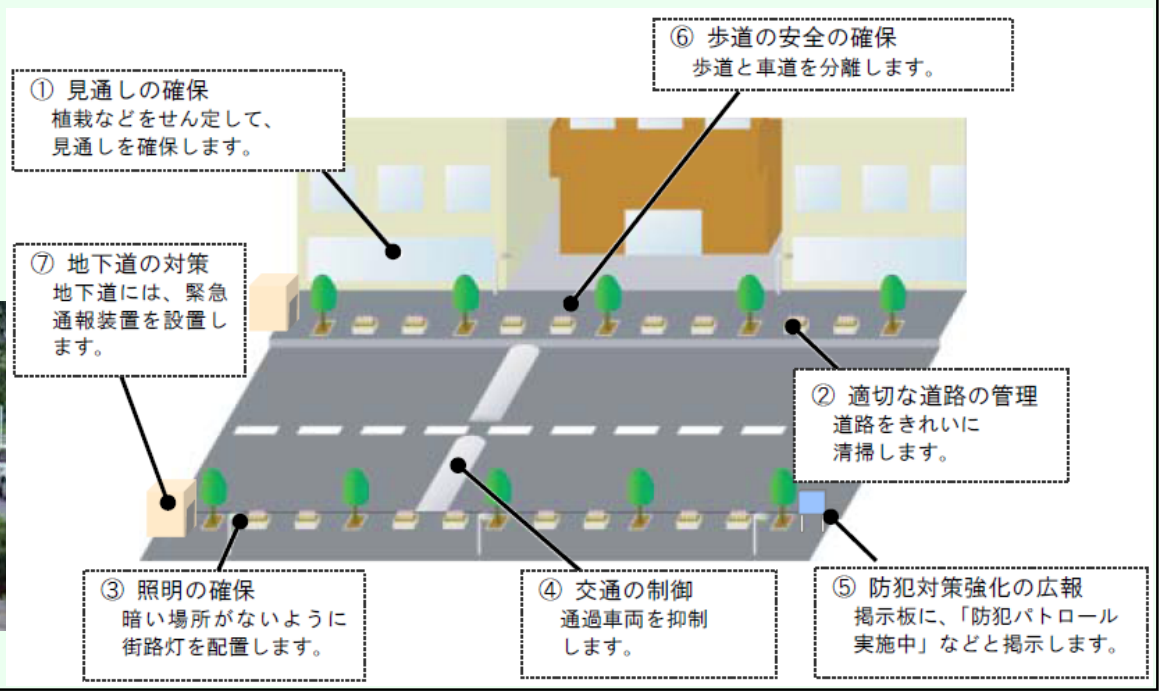
ページ 13

情報セキュリティ心理学の体系化を目指して

環境犯罪学・CPTED

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



ページ 14

情報セキュリティ心理学の体系化を目指して

教育・訓練について

教育・訓練には以下のようなものがあると考えている

- 手順を（無意識の行動として行うために）記憶するもの
- 可能な限り本質や背景にあるものを説明することにより、長く記憶に留めるためのもの
- 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
- 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

ページ 15

情報セキュリティ心理学の体系化を目指して

教育・訓練について

- 教育・訓練の評価・効果測定
  カークパトリック（Donald L. Kirkpatrick）の４段階評価
- Clear Screen/Clear Desk → CPTED/整理整頓
- 根本原因を探る
- IAT（Implicit Association Test）：まだ、研究レベルだが
- 事故防止・再発防止：SHELモデル分析
- 他者の調査データ分析は正しく行われているだろうか？
- 危険予知訓練（KYT: Kiken Yochi Training）
- 行動科学マネジメント：少人数・個人教育？　コンサル？
- 教育手段で行動変容を起こすことが可能か？　簡単な調査から見えてきたもの

詳細は、午後のWS（13:30～17:30　WS109　情報セキュリティ教育を支援する心理学の援用　A102）にて話題提供をします。

ページ 16