第3回JSSMセキュリティ
公開討論会

2009年2月28日

ITリスク学研究会

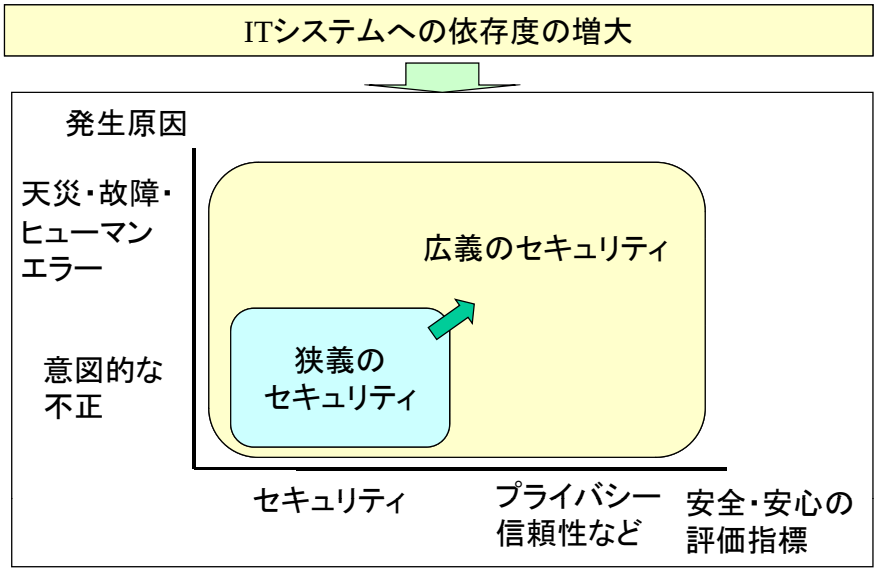
ITリスク学確立に向けて

東京電機大学未来科学部教授
佐々木良一
sasaki@im.dendai.ac.jp

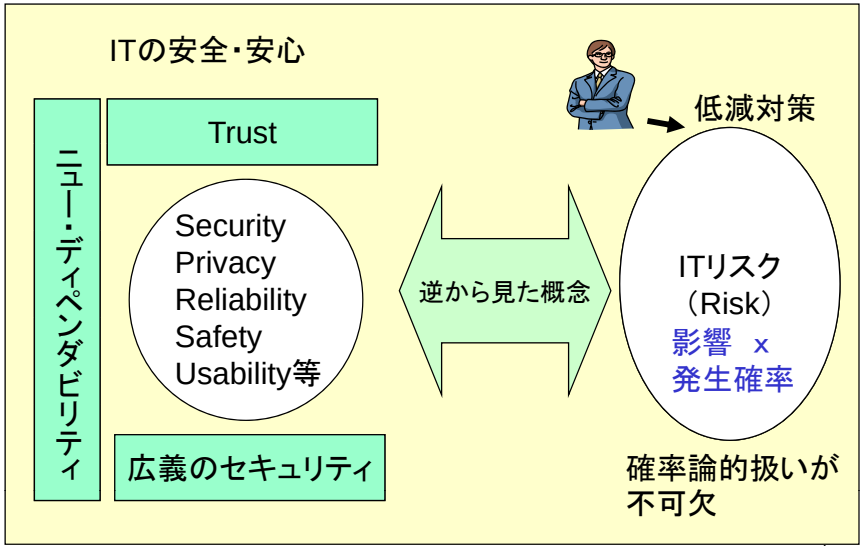
目次

1. 情報セキュリティからITリスクへ
2. ITリスク学の概要
3. ITリスク学の今後の展開

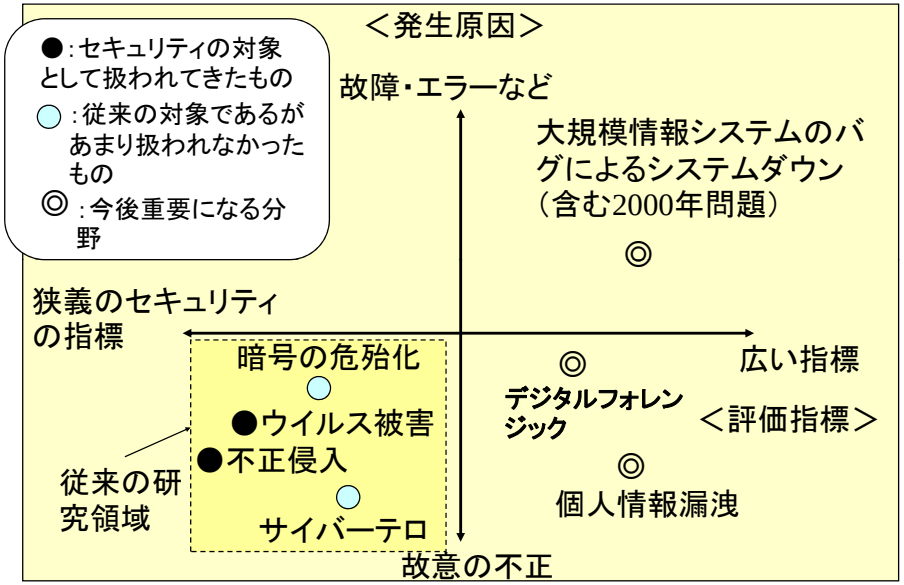
拡大する情報セキュリティ



ITリスク



代表的ITリスク



代表的ITリスクの現状の調査

1. 2000年問題
2. 個人情報漏洩リスク
3. 暗号の危殆化リスク
4. サイバーテロのリスク
5. 大規模情報システム故障のリスク

詳細は、佐々木良一「ITリスクの考え方」岩波新書、2008第2章、第4章参照

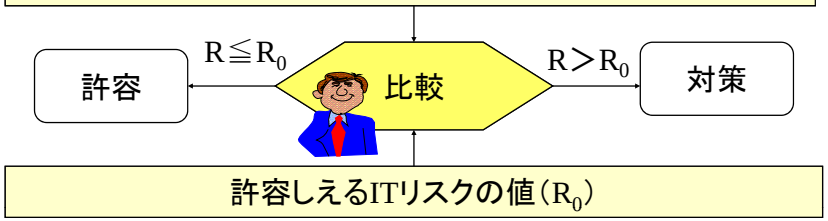
ITリスクに対する基本的考え方

ITリスクRの基本的定義

$R = P \times M$

P:事故などの発生確率や頻度（回／年）

M:事故などの影響の大きさ（被害額　円／回など　）



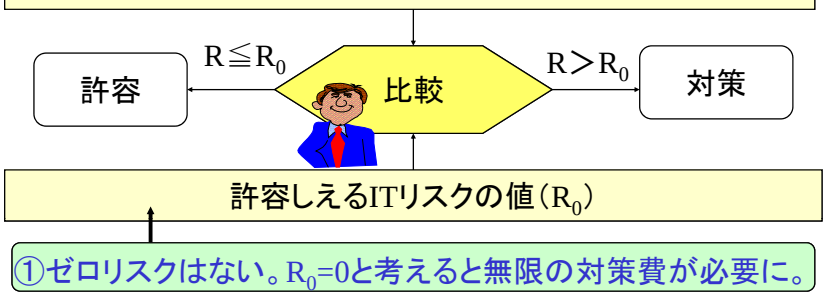
ITリスクに関する傾向

ITリスクRの基本的定義

$R = P \times M$

P:事故などの発生確率や頻度（回／年）

M:事故などの影響の大きさ（被害額　円／回など　）



ITリスクに関する傾向

ITリスクRの基本的定義

R = P × M

P:事故などの発生確率や頻度(回／年)

M:事故などの影響の大きさ(被害額　円／回など　)

②ITリスクの影響は大きくなり勝ち。

(例)個人情報の漏洩数

紙:数万件以下

電子媒体:数百万件も

ITリスクに関する傾向

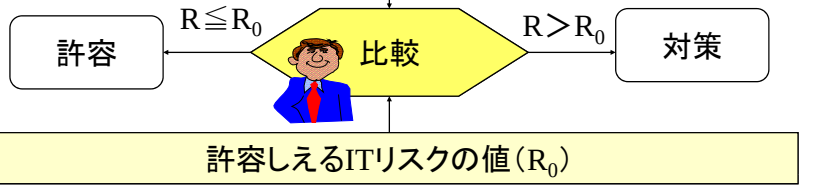
ITリスクRの基本的定義

R = P × M

③発生確率や頻度を直感的に把握するのは容易ではない。
(例) フィッシングメールの確率

P:事故などの発生確率や頻度(回／年)

M:事故などの影響の大きさ(被害額　円／回など　)



犯罪の発生頻度推定

1年間で警察に届けられている強盗の件数はおよそ6千件です。

(1)人質立てこもり事件　(　　件／年)

(2)空き巣　(　　件／年)

(3)自動車の盗難　(　　件／年)

(4)薬物常用者による殺人　(　　件／年)

標準化されたリスク比較セット案

項目	人口10万人当たりの年間死亡者概数
がん	250人
自殺	24人
交通事故	9人
火事	1.7人
自然災害	0.1人
落雷	0.002人

中谷内一也「リスクのモノサシ　安全・安心生活はありうるか」NHKブックス、2006より
その他　他殺　0．52人、入浴中の水死　2.6人、飛行機事故0.013人

ITリスクに関する傾向

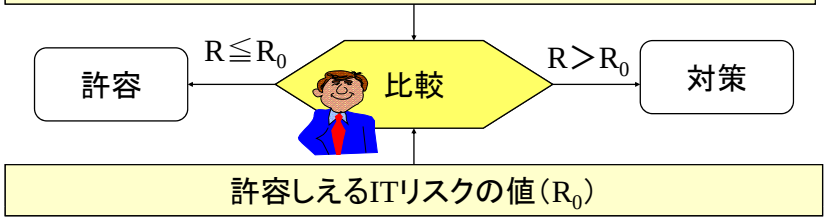
ITリスクRの基本的定義

$R = P \times M$

P:事故などの発生確率や頻度（回／年）

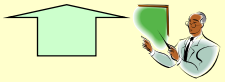
M:事故などの影響の大きさ（被害額　円／回など　）

④ある事故が発生するとその事故のことだけ考え、別の事故の発生も同じように起こることを忘れがち。



ITリスク対策の考え方

ITリスク
（個人情報漏洩など）



ITリスク対策
（ハードウエア暗号の利用など）

①ゼロリスクはないので対策にプライオリティ付けをしようとすると定量的評価あるいは準定量的評価が不可欠。

②1つのリスクへの対応が別のリスクを引き起こす。

リスクvsリスク、多重リスクの時代に

リスクvsリスクの時代（その1）

９．１１事件の後のテロ対策時の多くの発言

「こんなことが繰り返されてはならない。あらゆる手段を講じて再発を防止しなければならない。」

それに対する米国の有名な暗号学者でセキュリティコンサルタントのブルース・シュナイアー氏は

「そのような言葉に耳を傾けてはならない。これは恐怖にとらわれたものの言葉、典型的なナンセンスである。恐怖を乗り越え、賢明なトレードオフとは何かを考えなければならない。」

リスクvsリスクの時代（その2）

ブルース・シュナイアーの考え

「どんな対策をとってもテロを完全になくすることは不可能であり、

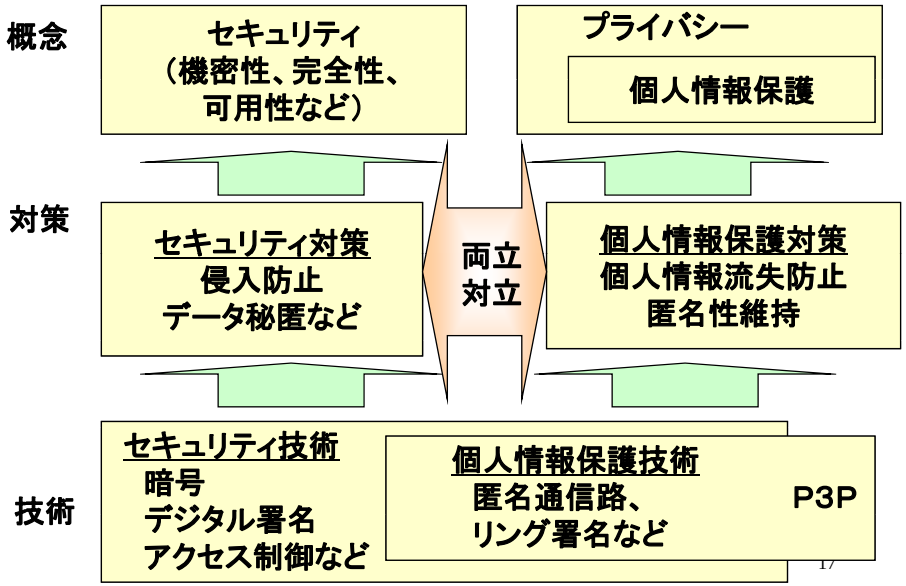
その対策によって生じる新たなリスクとテロのリスクとの間で真剣な比較検討が必要であり、

バランスを欠いた対策は、プライバシーや人権の問題を引き起こす。」

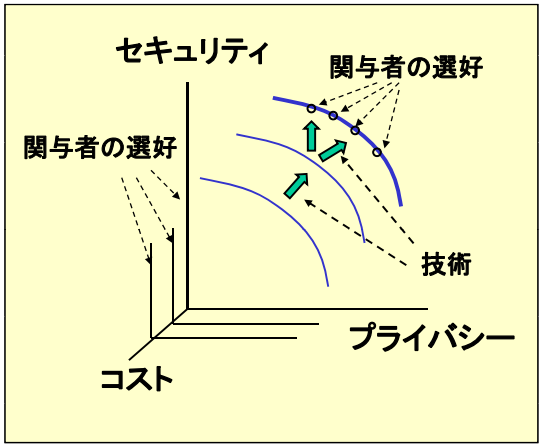
「リスク対リスク」 あるいは「多重リスク」 の時代に

（例）エネルギー問題解決のためのバイオエタノールの利用＝＞食糧問題に

リスクに関する対立する概念の例



リスクvsリスクの時代（その3）



技術による解決

＜例＞

公開鍵証明書の利用

属性証明書の利用など

多くの関与者が異なる選好を持つ
（リスクコミュニケーションが重要に）

ITリスク対策の考え方

ITリスク
（個人情報漏洩など）

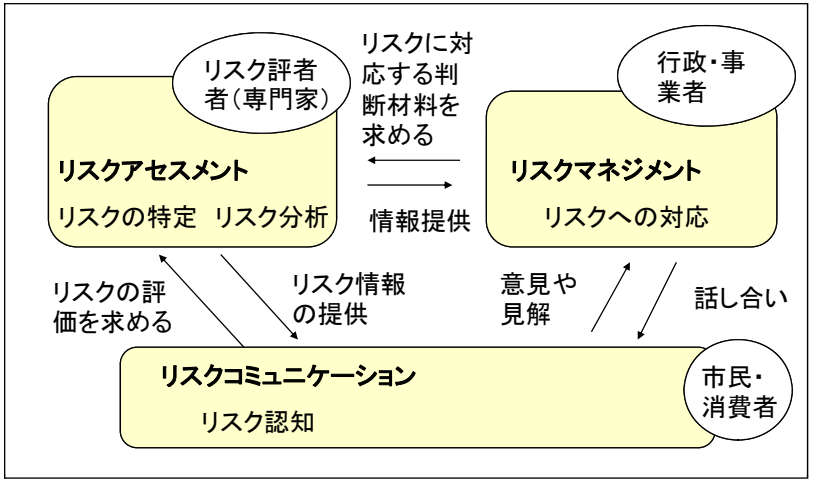
ITリスク対策
（ハードウエア暗号
の利用など）

③適切なリスク対策のためには、リスクマネジメント、リスクアセスメント、だけではなくリスクコミュニケーションも含めた総合的アプローチが重要に。

④対策効果は関与者の心理学的状況も考慮した対策が必要。

⑤対策がうまく行かない場合のために危機管理も不可欠。

ITリスクへの対応法の基本認識（2）



リスク・コミュニケーションとは

リスク・コミュニケーションの定義（U.S.NRC,1997）

リスク・コミュニケーションは、個人とグループ、そして組織の間で情報や意見を交換する相互作用的過程である。

民主主義を支える公民権、自己決定権、知る権利
説明責任、インフォームドコンセント、情報公開 と同じ根を持つもの

http://web.sfc.keio.ac.jp/~hfukui/class/riskmg/risk5_23.files/frame.htm

リスクコミュニケーションの対象

（1）個人的選択：個人個人がリスク情報を吟味し、どのように行動するかを決定するような事態。
(例)2000年問題に対応し、どのぐらいの期間の水や食料を用意するかといった問題など。

（2）社会的論争：どのような行動をとるかを、社会全体として決定しなければならないような事態。
(例)ウイルスプログラムを作ること自体を、犯罪として取締りの対象とするかどうかなど。

（3）組織内合意形成：企業や家族が採るべき対策を決めるような事態。
(例)個人情報漏洩対策など。

市民のリスク許容の特徴

（1）市民が受け入れるリスクのレベルは、専門家よりも非常に小さい。
例えば、生命や健康に関するリスクには敏感であり、事故や副作用等に対してリスクがゼロであることを求める傾向がある。

（2）市民は発生確率が低くても、被害規模が大きいリスクは受容しない傾向がある。
専門家は発生確率と被害規模によるリスクで判断するが、市民は被害規模を特に注目する。

http://tanesan.hp.infoseek.co.jp/kanbu-518risukukomi.html

マスコミと専門家（1）

リスクが少ないという立場で発言する専門家はマスメディアに対し次のような感想をもち勝ちである。

（a）マスメディアの人間は勉強不足である

（b）必要以上にセンセーショナルに取り上げる

（c）物事の全体像をとらえずに一部だけを誇大に報じる

（d）シロかクロかの二者択一で物事を単純化する

マスコミと専門家（2）

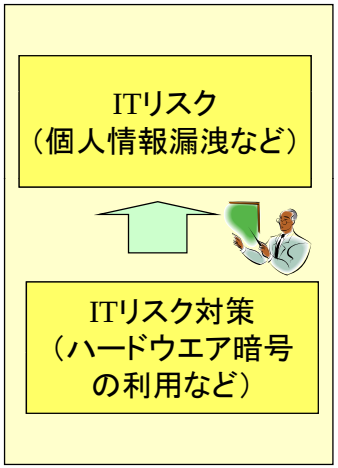
一方、マスメディア側は専門家に対し次のような不満を持つことになる
（a）専門家は都合の悪いことを隠しがちである

（b）知りたいことに答えてくれない（説明が回りくどく、結論がなかなか出てこない）

（c）メディアを敵視しがちで、率直でない

（d）メディアが締め切りに追われる立場であることを、理解してくれない

ITリスク対策の考え方

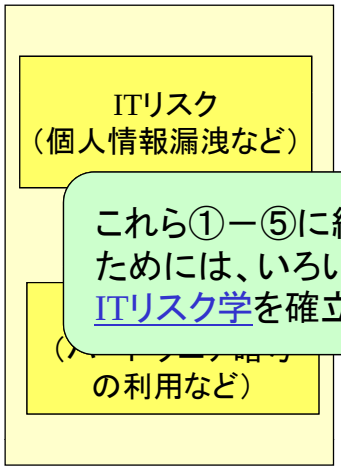


③適切なリスク対策のためには、リスクマネジメント、リスクアセスメント、だけではなくリスクコミュニケーションも含めた総合的アプローチが重要に。

④対策効果は関与者の心理学的状況も考慮した対策が必要。

⑤対策がうまく行かない場合のために危機管理も不可欠。

ITリスク対策の考え方

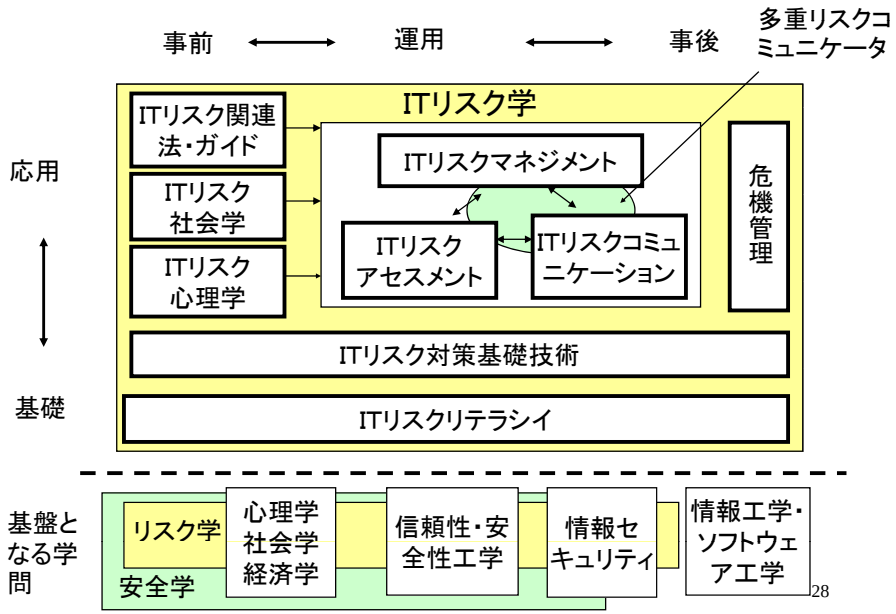


③適切なリスク対策のためには、リスクマネジメント、リスクアセスメント、だけではなくリスクコミュニケーションも含めた総合的アプ

これら①－⑤に総合的に対応できるようにするためには、いろいろな分野の人たちが協力してITリスク学を確立していくことが不可欠に

⑤対策がうまく行かない場合のために危機管理も不可欠。

ITリスク学の構成



多重リスクコミュニケータ開発の背景

ITリスク対策の合意をとるために開発

1. 多くのリスク(セキュリティリスク、プライバシーリスクなど)が存在＝＞リスク間の対立を回避する手段が必要

2. 多くの関与者(経営者・顧客・従業員など)が存在＝＞多くの関与者間の合意が得られるコミュニケーション手段が必要

3. ひとつの対策だけでは目的の達成が困難＝＞対策の最適な組み合わせを求めるシステムが必要

多重リスクコミュニケータ(MRC)の開発

従来のITリスク評価の方法(その1)
ーJIPDECのリスク算出式ー

＜リスク値の計算式＞

リスク値＝情報資産の価値　X　脅威　X　脆弱性

＜適用例＞

情報資産	資産価値	脅威レベル	脆弱性レベル	リスク値
A	4	3	3	36
B	2	4	5	40

リスク値の大きい情報資産Bに対する対策を優先

従来のITリスク評価の方法(その2)
ーシュナイアーの5段階評価法 ー

ステップ1:守るべき資産は何か

ステップ2:その資産はどのようなリスクにさらされているか

ステップ3:セキュリティ対策によってリスクはどれだけ低下するのか

ステップ4:セキュリティ対策によってどのようなリスクがもたらされるか

ステップ5:対策にはどれほどのコストとどのようなトレードオフが付随するか

ブルース・シュナイアー (著), 井口 耕二 (翻訳)「セキュリティはなぜやぶられたのか 」日経BP企画、2007

5段階評価法の適用例

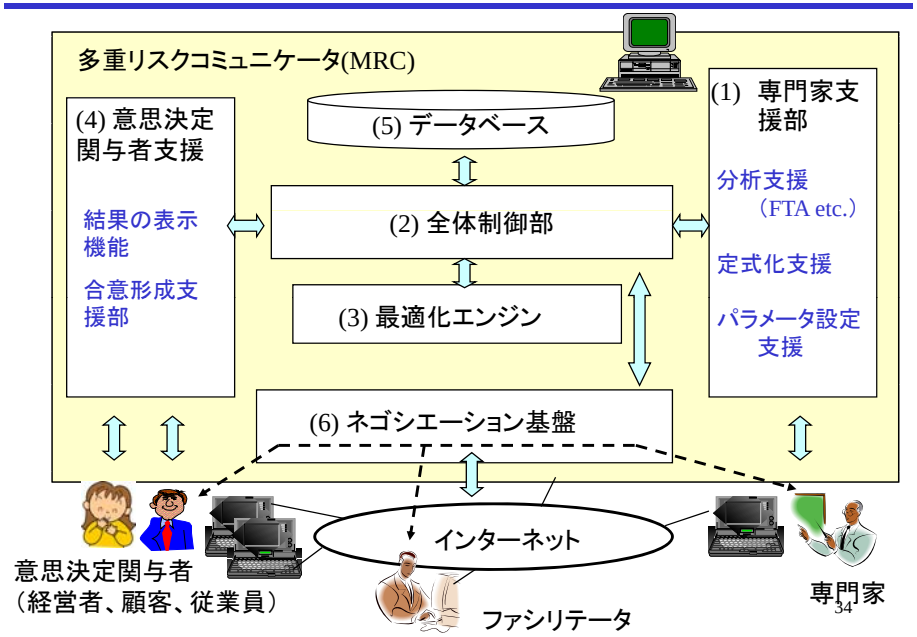
ステップ1:守るべき資産は自宅と家財およびそこに住む人であるとする。
ステップ2:その資産がさらされているリスクは自宅に押し入ってくる窃盗犯である。
ステップ3:「家庭用の防犯装置の導入」というセキュリティ対策によって、不正侵入などを検知対応してくれるのでリスクは大幅に低下し、安全性があがるという。また、これを導入することにより抑止力も向上する。ただし、誤報が大きな問題だという。
ステップ4:このセキュリティ対策を採ることによって、警報機をオフにするためのアクセスコードを覚えておかなければならないなどのリスクがもたらされる。
ステップ5:この対策にはXXドルの対策費用と利便性の低下というトレードオフが付随する。

ブルース・シュナイアー (著), 井口 耕二 (翻訳)「セキュリティはなぜやぶられたのか 」日経BP企画、2007

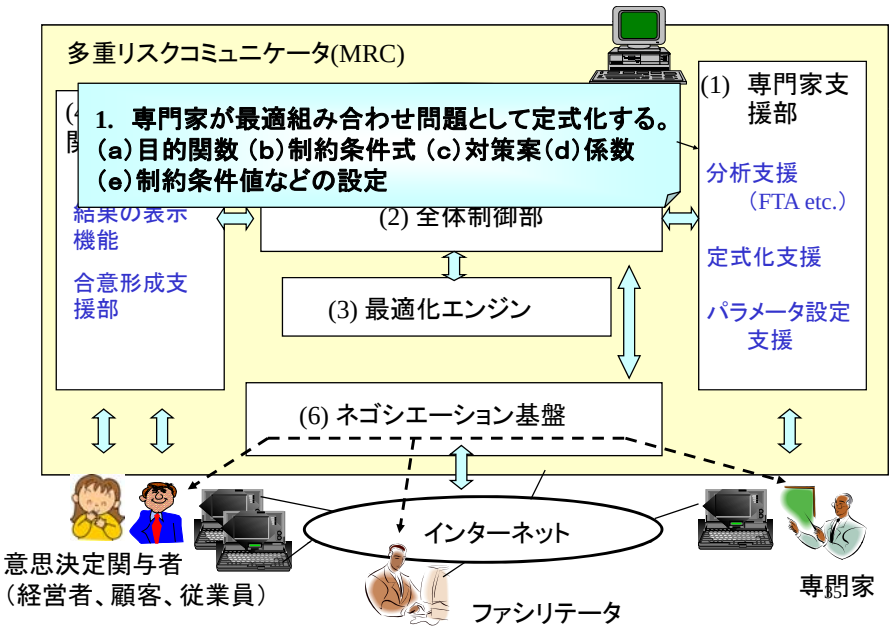
ITリスク評価法の比較

評価指標 ＼ 方式	JIPDEC方式	5段階方式	MRC方式
1．多くのリスク（セキュリティリスク、プライバシーリスクなど）が存在＝＞リスク間の対立を回避する手段が必要	X	○	○
2．多くの関与者（経営者・顧客・従業員など）が存在＝＞多くの関与者間の合意が得られるコミュニケーション手段が必要	X	X	○
3．ひとつの対策だけでは目的の達成が困難＝＞対策の最適な組み合わせを求めるシステムが必要	△	X	○

多重リスクコミュニケータMRCの概要



多重リスクコミュニケータMRCの利用手順（1）



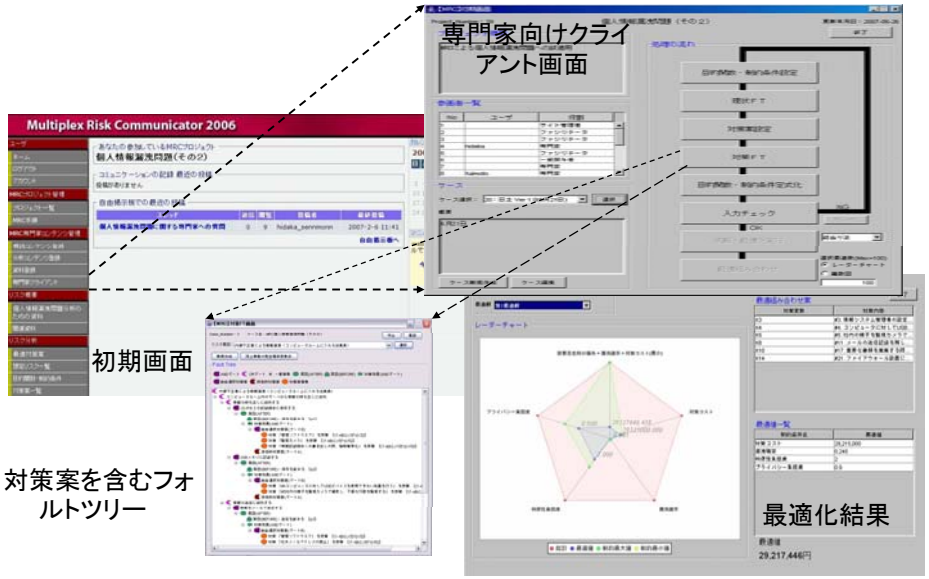
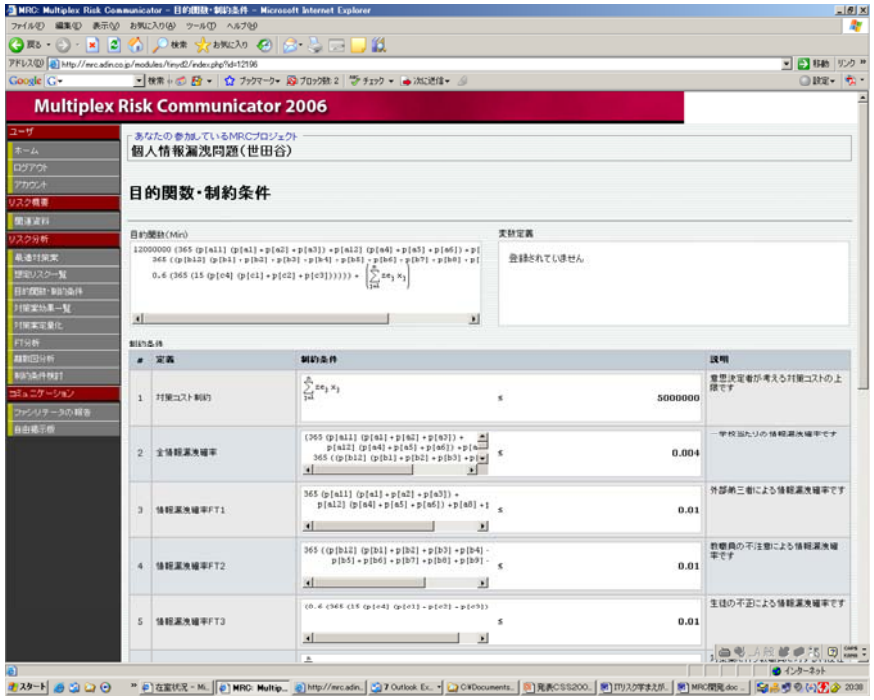
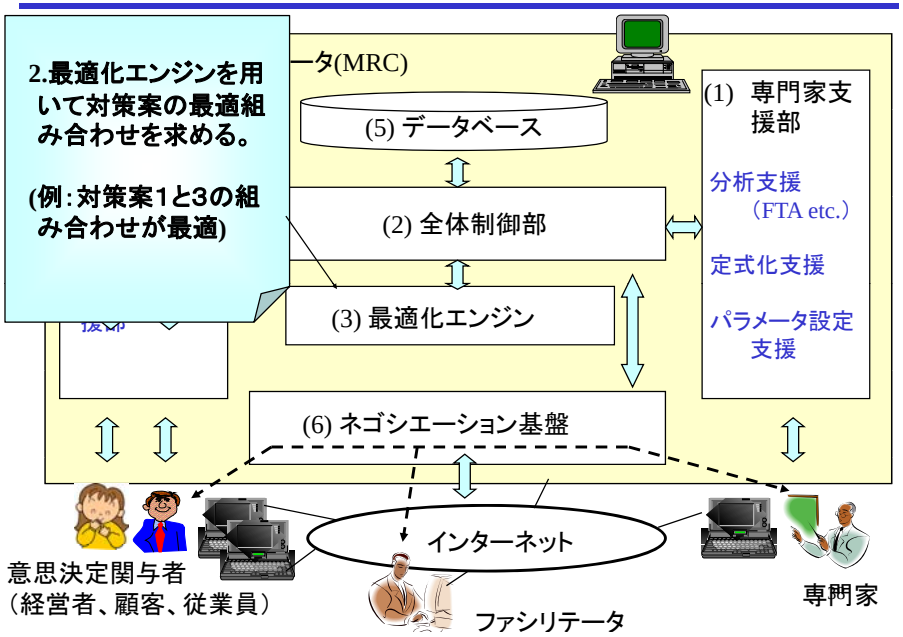


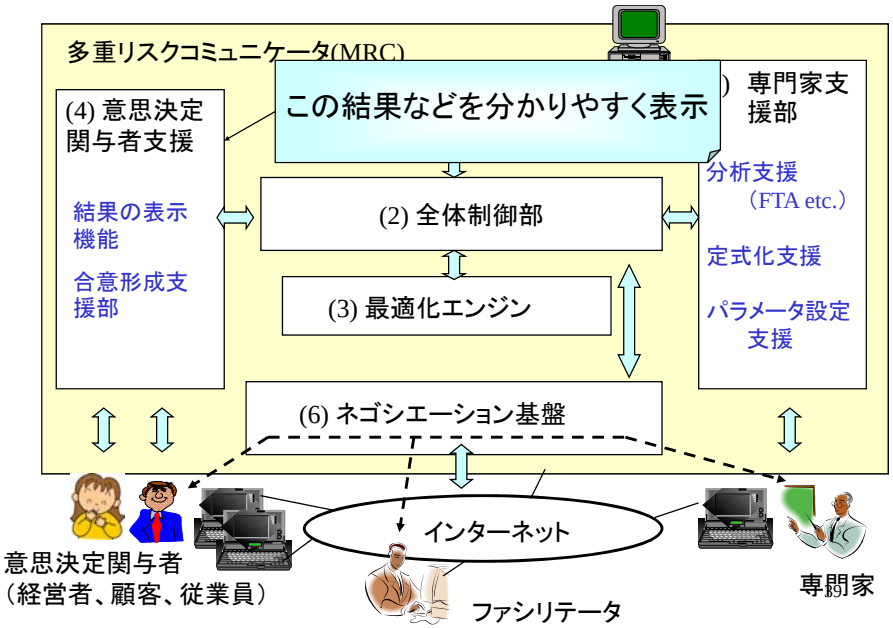
図6　MRCプログラムの専門家向け画面イメージ



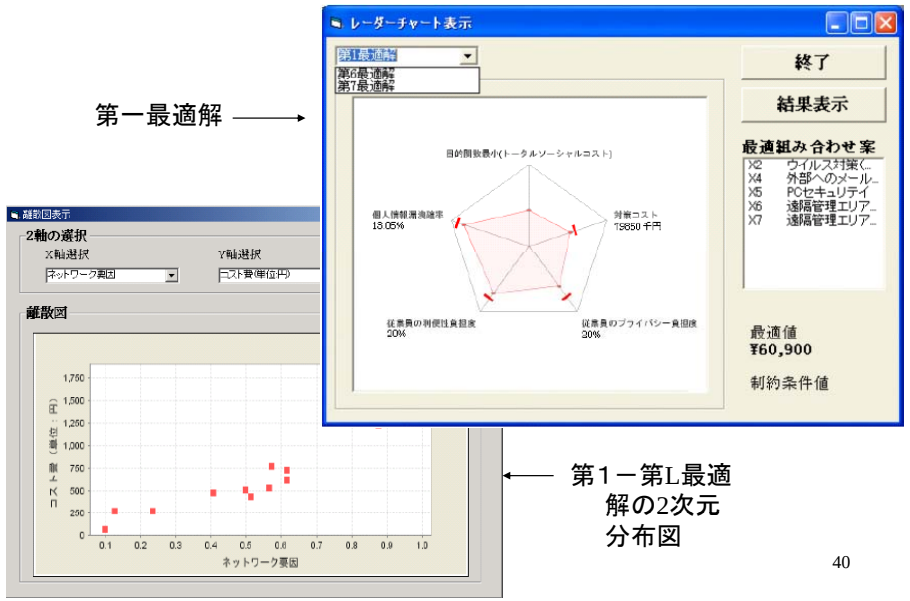
多重リスクコミュニケータMRCの利用手順（2）



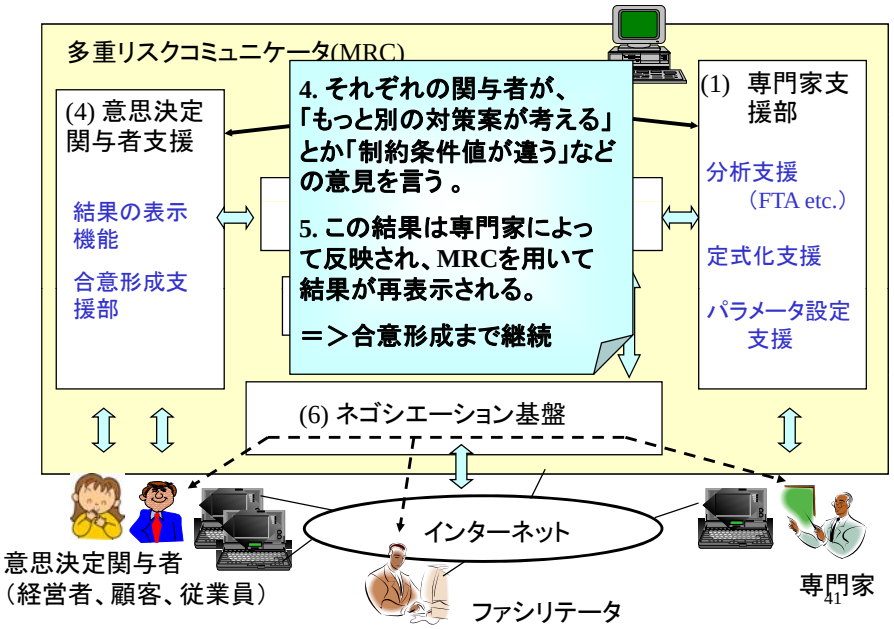
多重リスクコミュニケータMRCの利用手順（3）



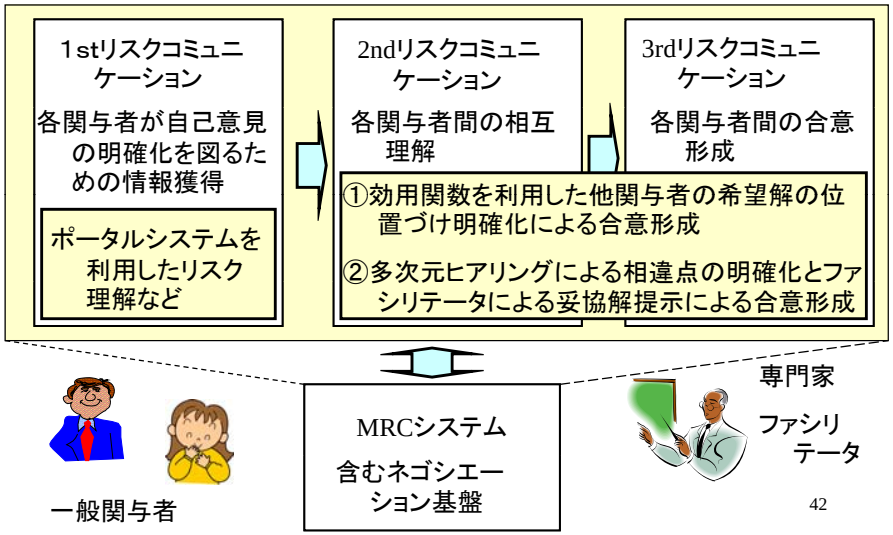
一般関与者向け画面



多重リスクコミュニケータMRCの利用手順（4）



リスクコミュニケーションのフェーズ



適用結果の概要

	対象	目的	関与者	分析手法	備考
1	個人情報漏洩への適用	従業員の負担も考した対策案の合意形成	経営者 顧客 従業員	FTA	プロバイダ 一般企業 区役所
2	不正コピーによる著作権侵害問題への適用	対策後の不正者の行動を想定した効果予測に基づく合意形成	レコード会社 消費者	FTA （不正者はシミュレータで実現）	CSS2006で発表
3	内部統制問題への適用	公的資金の適切な運用に関する内部統制対応	センタ 教授 学生	ETA	CSS2007で発表予定
4	暗号の危殆化対策への試適用	暗号危殆化時の署名つき文書への安全性対策の合意形成	政府 署名者 検証者	ETA	CSS2006で発表

FTA: Fault Tree 分析法 ETA:Event Tree 分析法

最近のアプローチ

1. 佐々木良一「ITリスクの考え方」岩波新書2008発刊

2. 日本セキュリティ・マネジメント学会内にITリスク学研究会設立、活動

第1回研究会

1．日時：平成20年6月28日14:00－17:00
2．東京電機大学神田キャンパス11号館大会議室
（http://www.dendai.ac.jp/map/kanda2.html）
3．実施項目案
（1）特別講演：中谷内一也（帝塚山大学 教授）
「リスク心理学の動向」 約1時間

（2）佐々木「ITリスク学とITリスク学研究会の進め方の構想」
約30分

（3）パネル「ITリスク学はいかにすれば有益なものとなりうるか」
司会：佐々木
大木先生、日立千葉氏、日銀岩下氏、トーマツ丸山氏、日経関口氏　約1時間30分

第2回研究会

1．日時：平成20年10月4日（土）15:00－17:30
2．会場：東京電機大学アネックス6階の大会議室（601）
http://atom.dendai.ac.jp/info/access/kanda_map.html
3．プログラム
15:00－16:00
（1） 特別講演：松原純子氏（放射線影響協会、元原子力安全委員会委員長代理） 「私の研究ー疫学・リスク科学と積極的防御への道」

16:00－16:30
（2）講演：中村達氏 （アイネス）
「ITリスクの落とし穴」
16:30－17:00
（3）講演：杉本尚子氏（アドイン）
「多重リスクコミュニケータ用プログラムの開発と今後の展開」
17:00－17:30
（4）講演：矢島敬士氏 （東京電機大学教授）
「リスクコミュニケーションにおける合意形成支援方式」

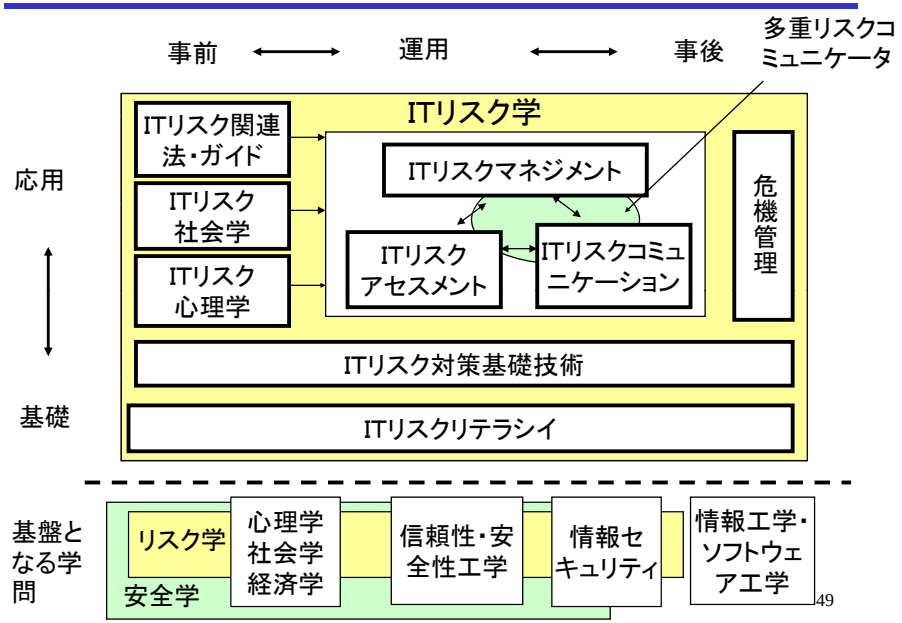
第3回研究会

1．日時：平成21年1月10日（土）15:00－17:30
2．会場：東京電機大学神田キャンパス11号館17F大会議室
3．プログラム
15:00－16:00
（1）特別講演：「新型インフルエンザのリスクとマスメディア」
南直樹氏（NHK解説委員）
16:00－17:10
（2）特別報告：「多重リスクコミュニケータ（MRC）の適用教育」
（a）「MRCの適用教育の概要」
20分 谷山充洋（東京電機大学）
（b）「MRCの適用結果の報告」
10分 情報セキュリティ大学院大学学生
10分 中央大学学生
10分 東京電機大学
（c）「適用教育結果のまとめと今後の展開」
20分 谷山充洋、佐々木良一

第4回研究会（予定）

1．日時：平成21年3月28日（土）15:00－17:30
2．会場：東京電機大学神田キャンパス11号館16F1601会議室
3．プログラム
15:00－16:00
（1）特別講演：「原子力分野におけるリスク評価とヒューマンエンジニアリング」
氏田博士氏（財団法人エネルギー総合工学研究所 ）
16:00－17:10
（2）研究発表：
（a）「インターネット上の知識を利用したリスクの検知 」
20分 渡辺夏樹，吉浦裕（電気通信大学）
（b）「RCにおけるファジィ理論を用いた意思決定支援法 」
20分 鹿野哲矢（東京電機大学）
（c）「暗号危殆化リスクへの対応（仮題）」
20分 西本敬志（東京電機大学）

ITリスク学の構成



特に対応が必要な項目

- ITリスク学が成り立つ条件と全体像の見直し（学が成り立つ条件とは？）
- 多重リスクコミュニケータMRCの改良
- ITリスク対策基礎技術の明確化と掘り下げ
- ITリスク心理学、ITリスク社会学などの研究の深化
- ITリスクの危機管理研究の立ち上げ

MRCの要改良点

1．MRCの拡張

（1）合意形成の容易化支援技術（一般からの意見収集技術など）

（2）対立が大きい対象への適用法の確立

（3）簡易版（短時間適用版）の検討（テンプレート方式の改善）

2．MRCプログラムの改良

（1）求解の高速化（含む近似解法）

（2）使い勝手の改良

（3）ETA支援ツールの組み込み

（4）専門家向けPCへのMathematica搭載必須の緩和など

3．その他

（1）MRC利用教育の推進

（2）利用範囲の拡大（対象、主体）

ITリスク基本技術の構成要素

- リスクの扱い方の基本
- 合意形成支援技術（リスクコミュニケーションなど）
- 高信頼化、高セキュリティ化主要要素技術
- 証拠性維持要素技術（デジタルフォレンジックなど）

など

今後の予定

1．デジタル･フォレンジックも組み込んだIT
リスク学の概念の第一次確立（2010年度）

2「ITリスク学入門」執筆（2012年） 他

終わり

犯罪の発生頻度推定（答）

1年間で警察に届けられている強盗の件数はおよそ
6千件です。

（1）人質立てこもり事件 （ 3 件／年）

（2）空き巣 （ 9万1千 件／年）

（3）自動車の盗難 （ 3万6千 件／年）

（4）薬物常用者による殺人 （ 11 件／年）

中谷内一也「安全。でも、安心できない」筑摩新書，2008