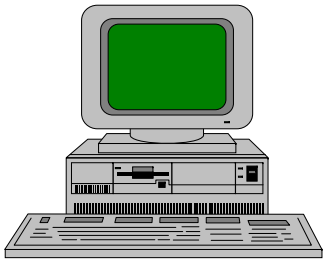
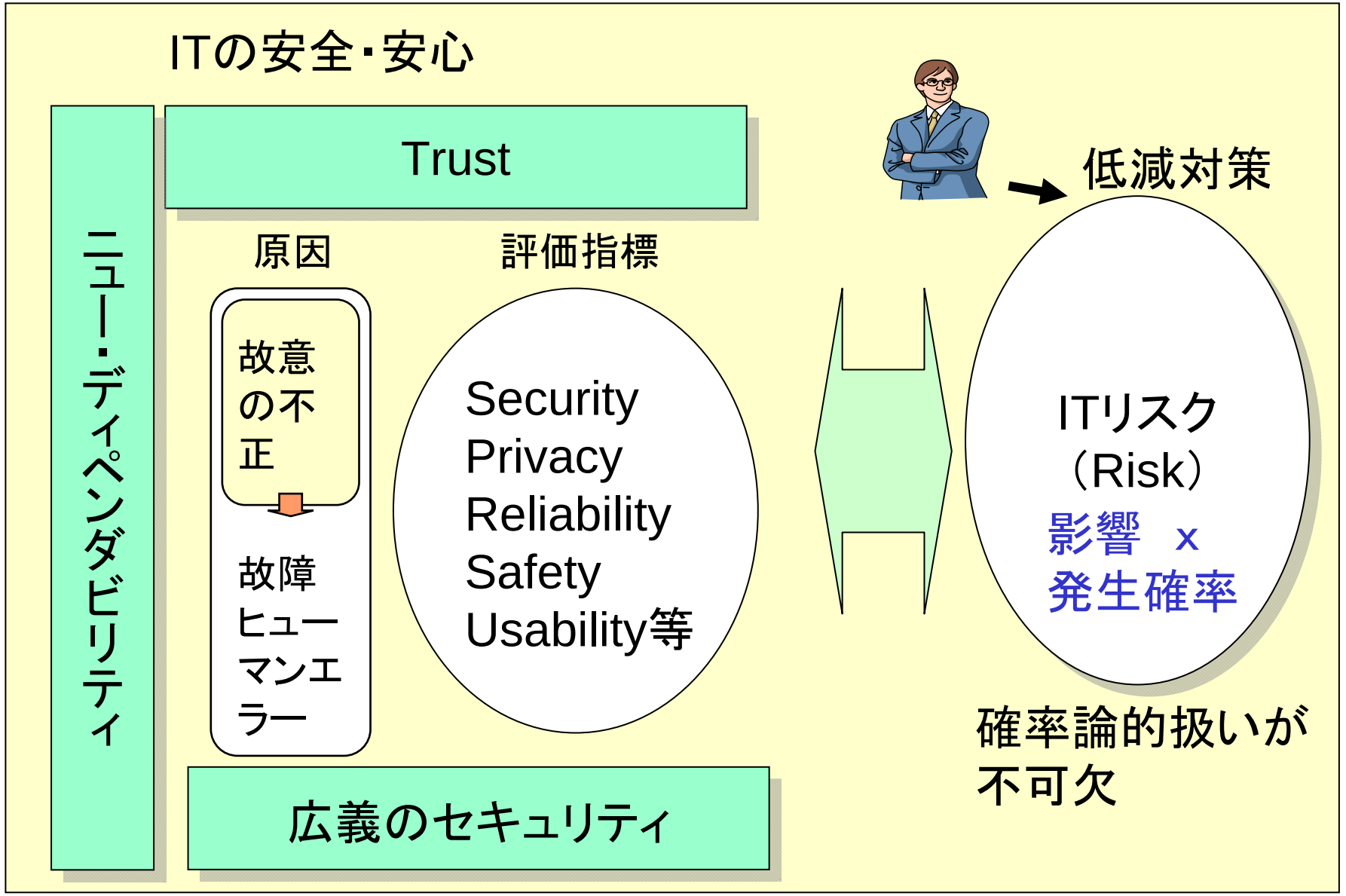
リスクアセスメントと
多重リスクコミュニケータ

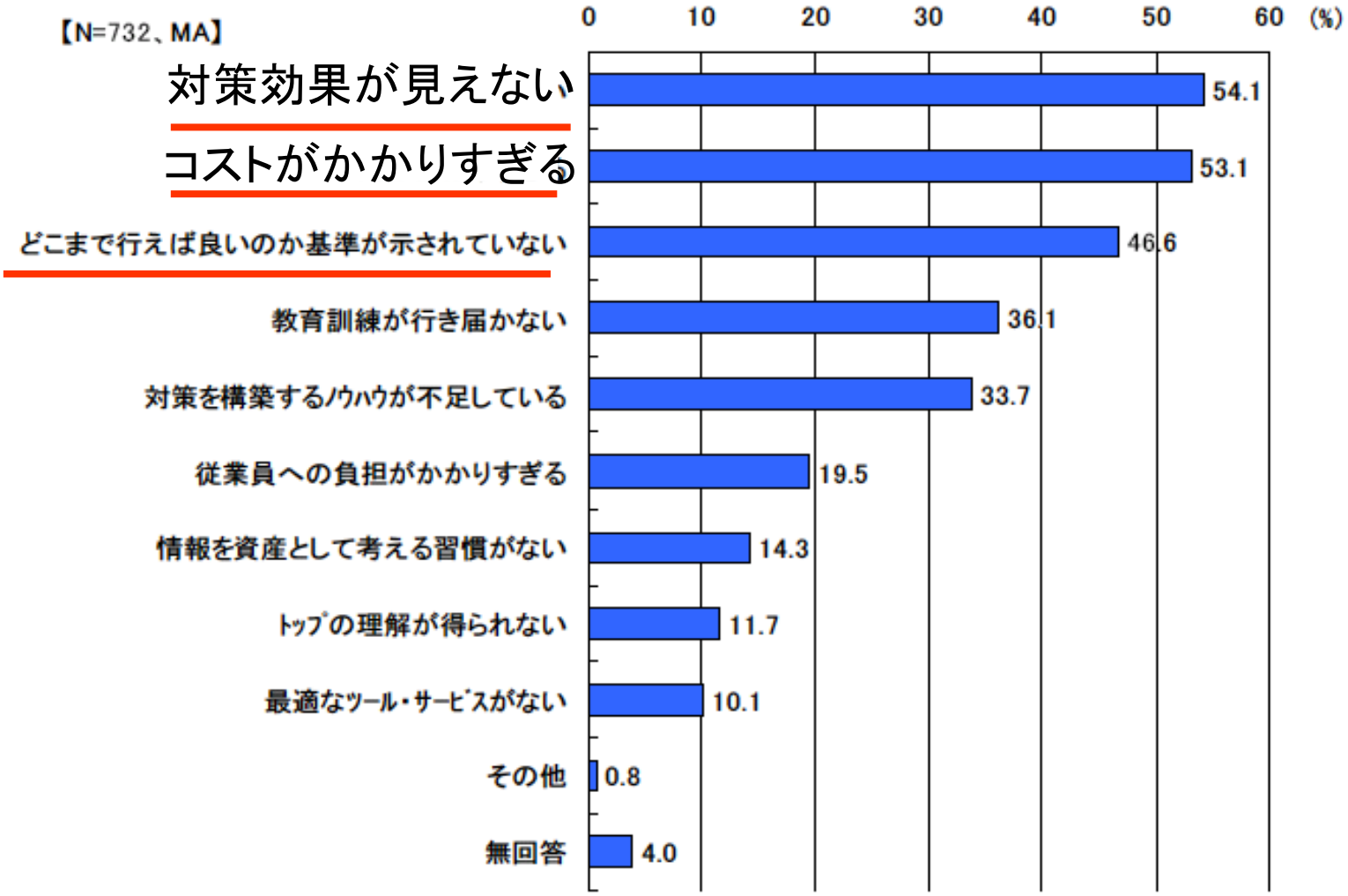
東京電機大学
佐々木良一
sasaki@im.dendai.ac.jp



ITリスク

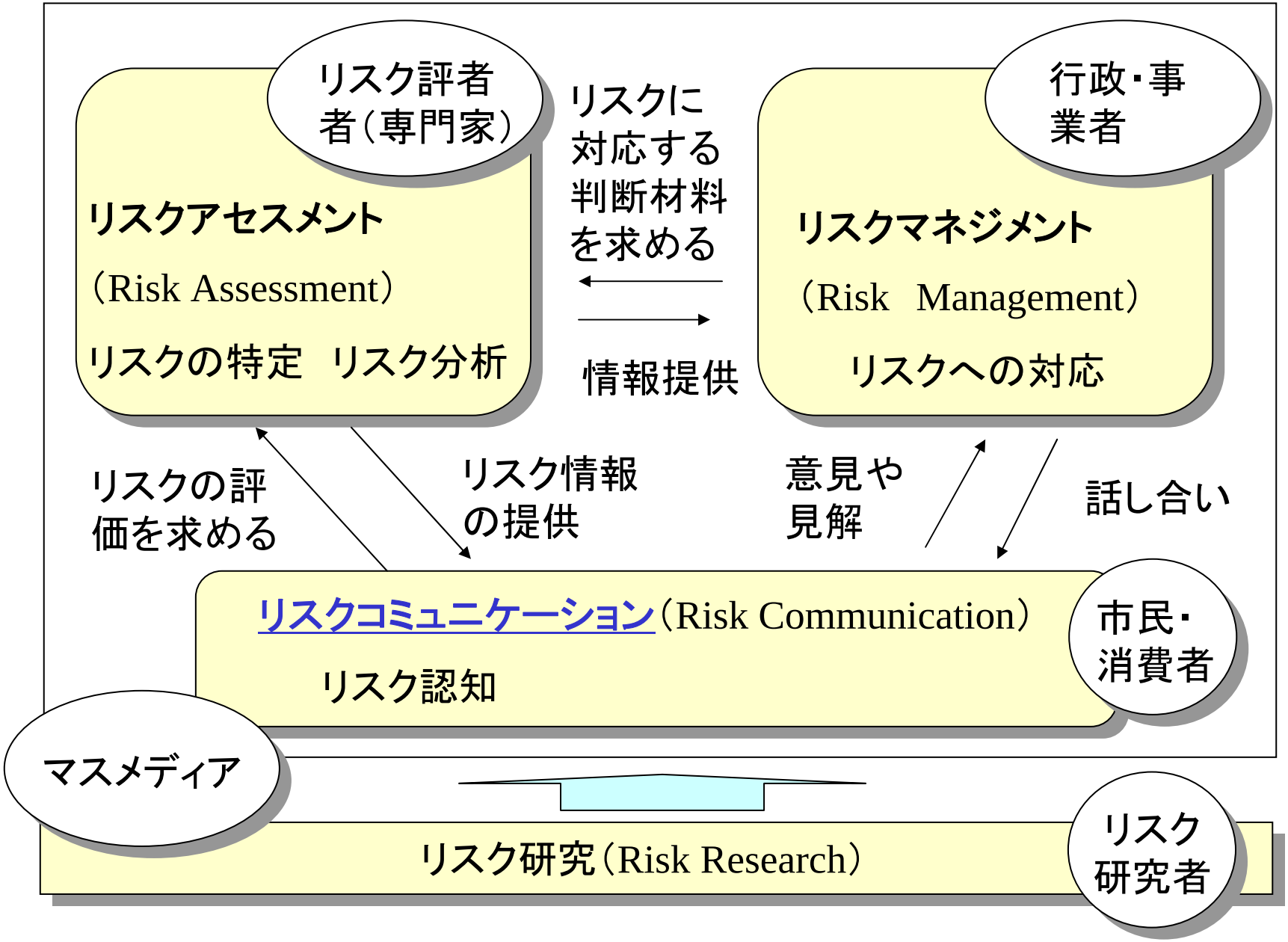

ITの安全・安心
ニュー・ディペンダビリティ
Trust
原因
評価指標
故意の不正
故障
ヒューマンエラー
Security
Privacy
Reliability
Safety
Usability等
低減対策
ITリスク
（Risk）
影響　x
発生確率
確率論的扱いが不可欠
広義のセキュリティ

セキュリティ管理者が困っていること

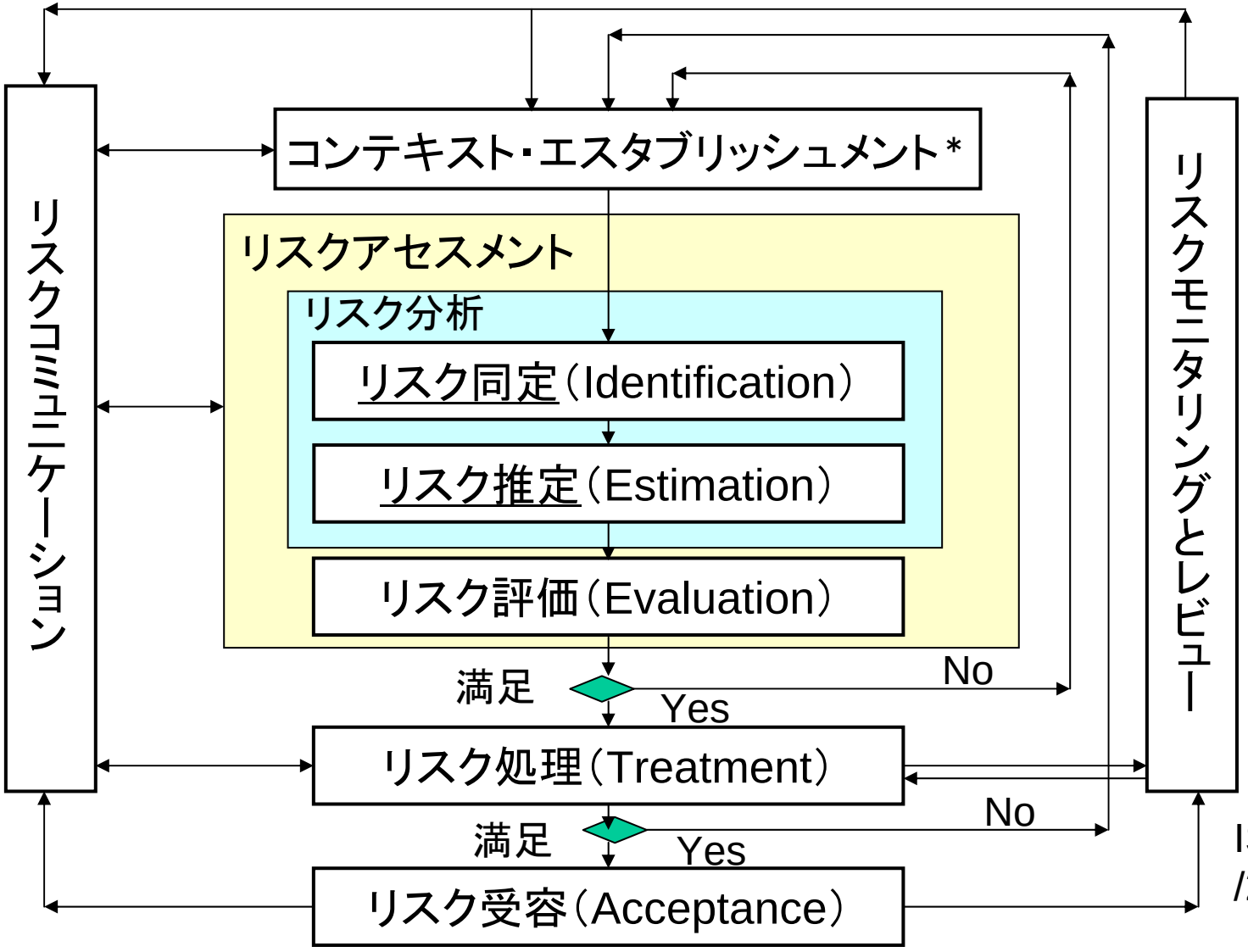


不正アクセス行為対策等の実態調査 調査報告書　警察庁　2003

リスク対応の基本構成


リスク評価者（専門家）
リスクアセスメント
（Risk Assessment）
リスクの特定　リスク分析
リスクに対応する判断材料を求める
情報提供
行政・事業者
リスクマネジメント
（Risk　Management）
リスクへの対応
リスクの評価を求める
リスク情報の提供
意見や見解
話し合い
リスクコミュニケーション（Risk Communication）
リスク認知
市民・消費者
マスメディア
リスク研究（Risk Research）
リスク研究者

リスクマネジメントプロセス



ISO/IEC27
/27005

＊リスクマネジメントのための適用範囲と境界、組織と責任、各種基準などを設定

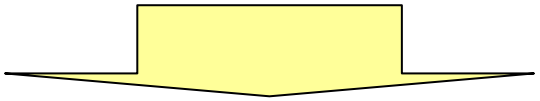
従来のITリスク評価の方法（その１）
―JIPDECのリスク算出式―

＜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

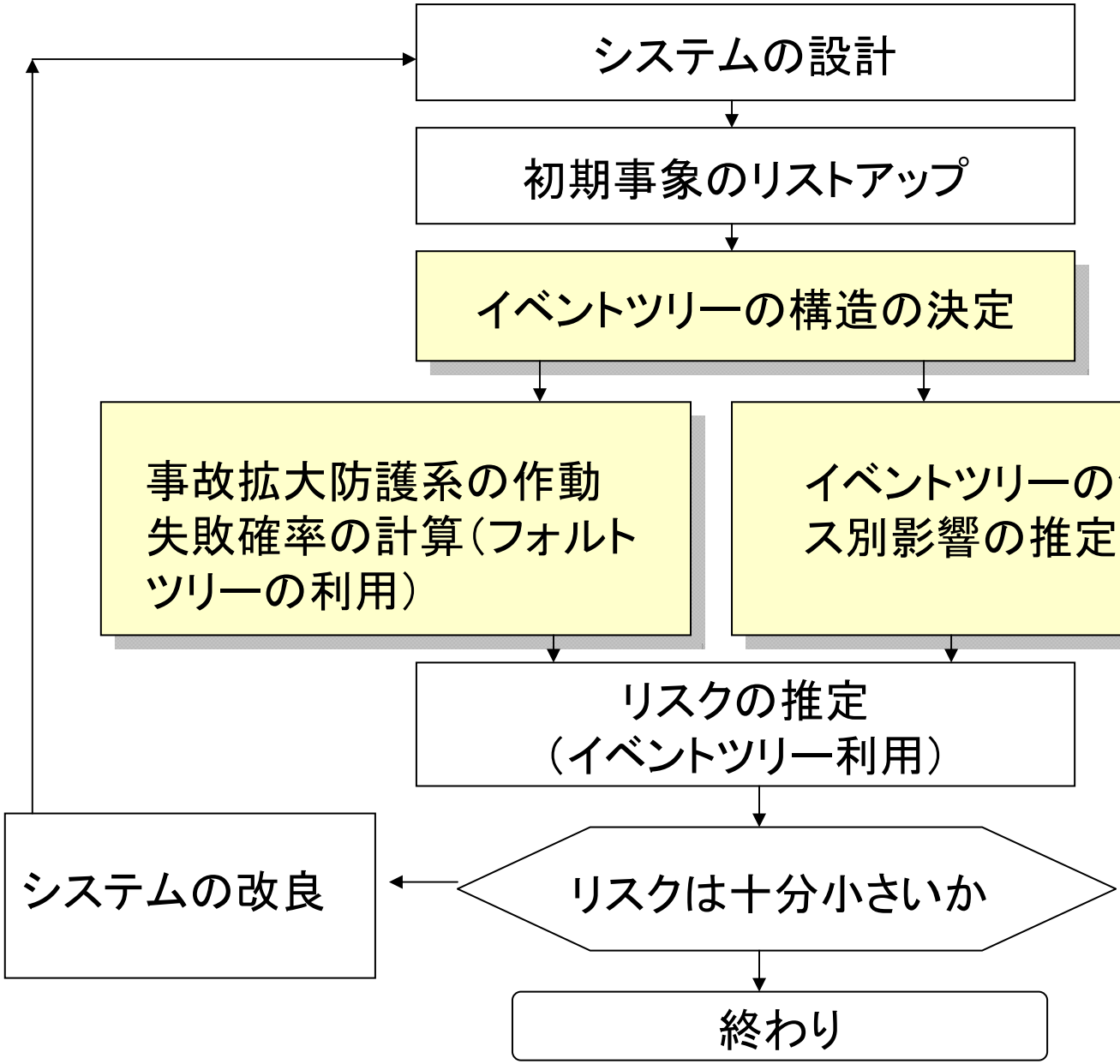
＜適用例＞

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

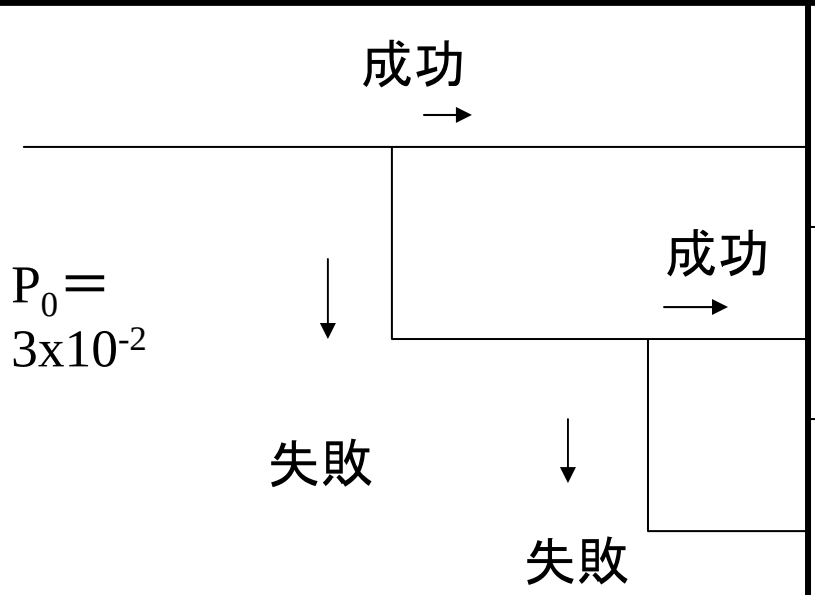
確率論的リスクアセスメントの概要



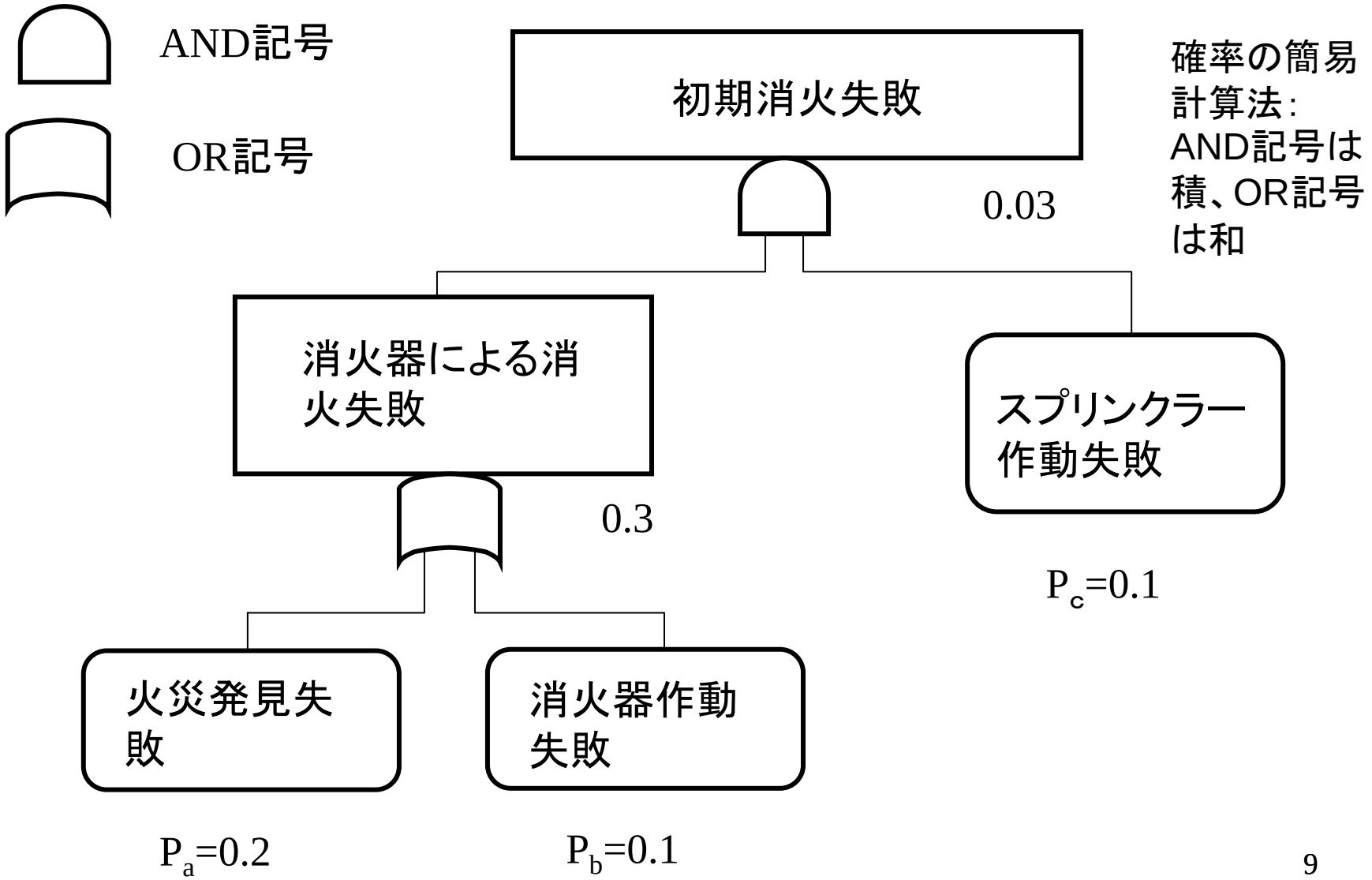
初期事象：大事故の引き金になる可能性のある異常事象

FTA（Fault Tree Analysis）とETA（Event Tree Analysis）は別々に用いることも可能

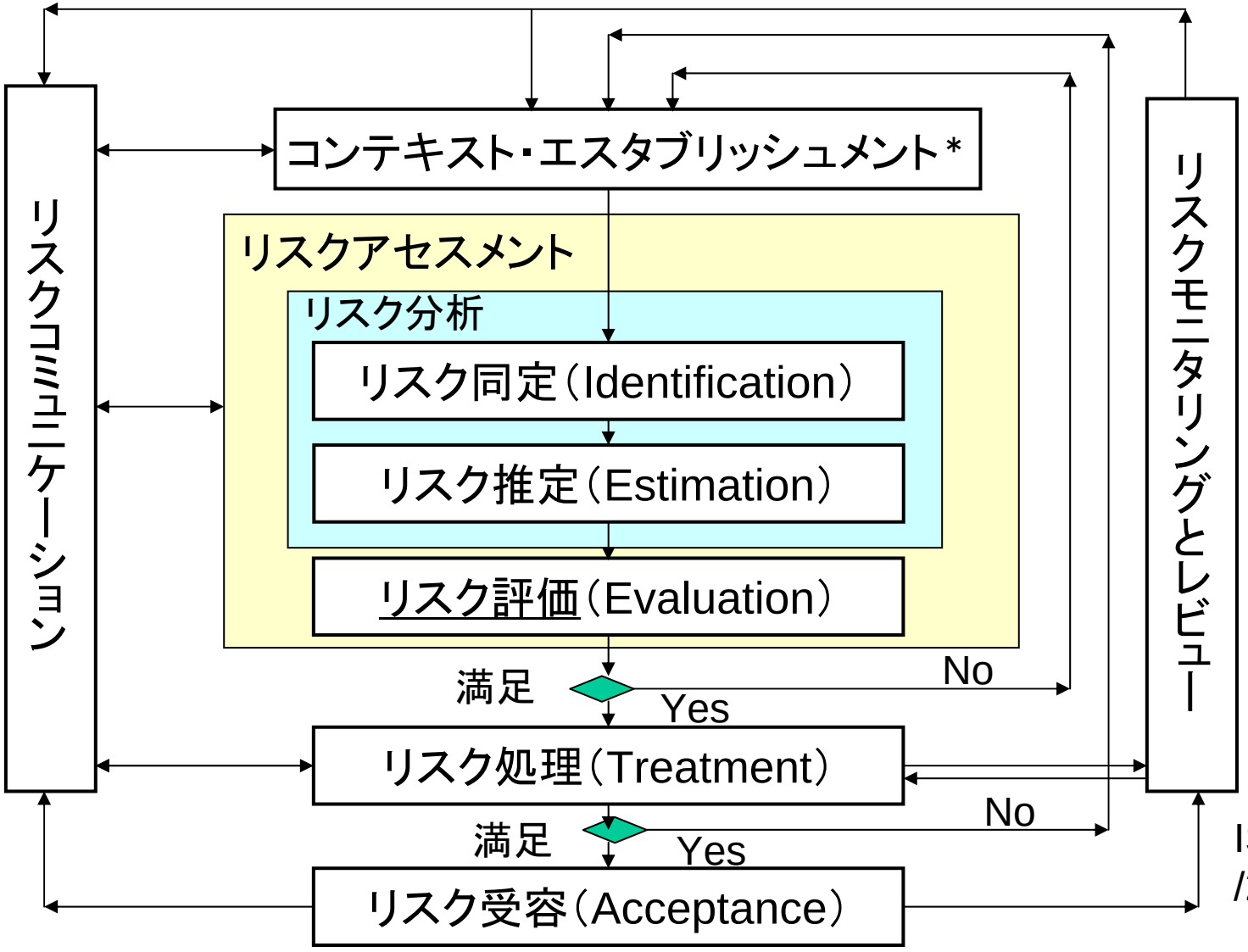
イベントツリーの一例

初期事象	ヘッディング項目		シーケンス	A 発生頻度（回／年）	B 影響＜消失被害＞（円）	A×B リスク（円／年）
火災発生	初期消火	本格消火				
			S1	$3x10^{-2}$	30万円	9000円
			S2	$9x10^{-4}$	500万円	4500円
			S3	$4.5x10^{-5}$	2000万円	900円
失敗確率	P_1＝$3x10^{-2}$	P_2＝$5x10^{-2}$	—	—	—	14400円

フォルトツリーの一例


AND記号
OR記号
初期消火失敗
0.03
確率の簡易計算法：AND記号は積、OR記号は和
消火器による消火失敗
0.3
スプリンクラー作動失敗
P_c=0.1
火災発見失敗
消火器作動失敗
P_a=0.2
P_b=0.1

リスクマネジメントプロセス



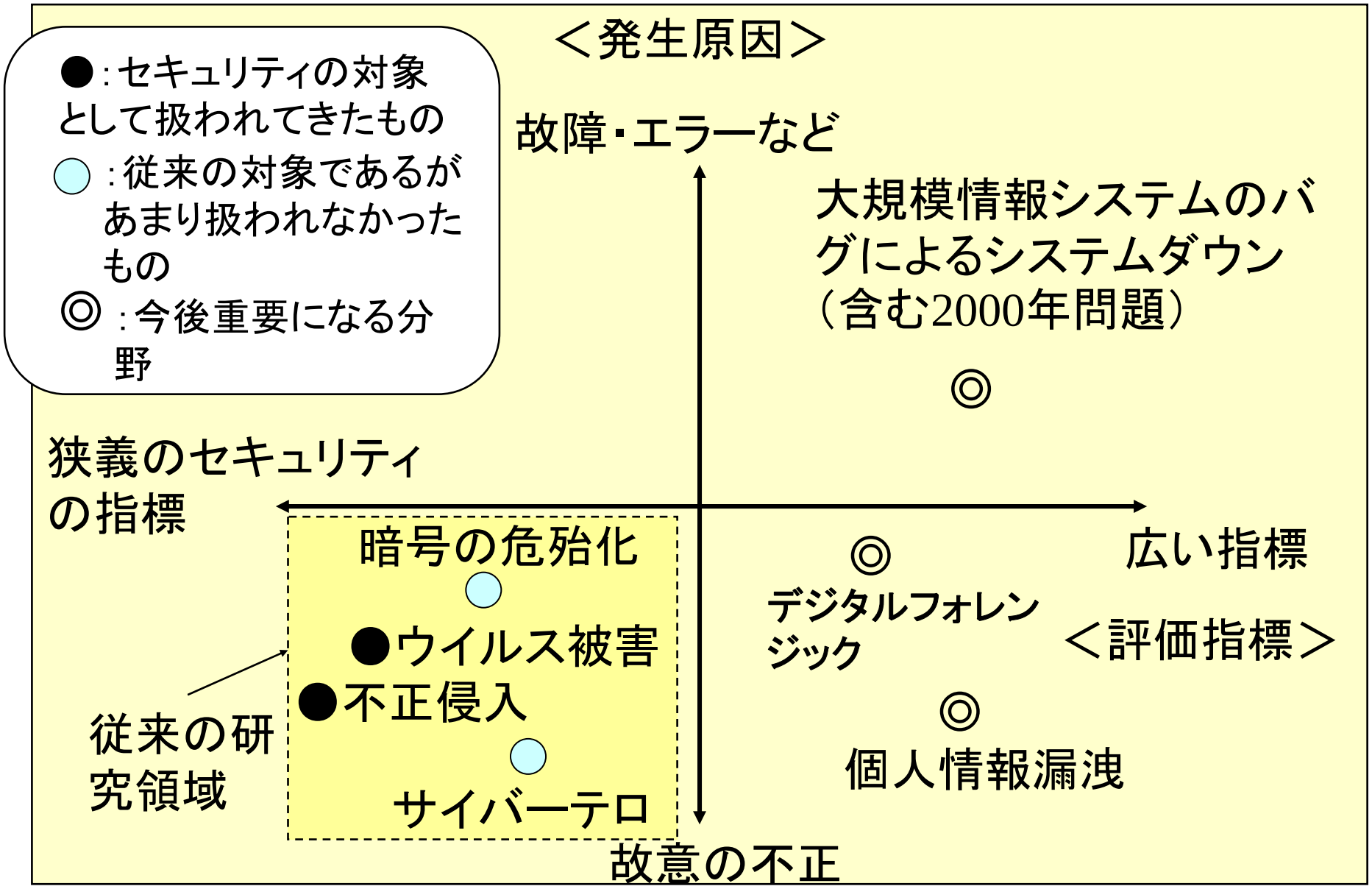
ISO/IEC27
/27005

＊リスクマネジメントのための適用範囲と境界、組織と責任、各種基準などを設定

表３．２　リスク評価基準の比較

評価指標	対象となる対策案やシステムの数	
	1つ	2つ以上
リスクのみ	(a)基準クリア型	(d)単純リスク比較型
リスク＋アルファ (コスト、 その他のリスク、 ベネフィット)	(b)リスクーベネフィット型 (c)リスクーリスク型	(e)リスクーコスト比較型 (f)リスクーコストーベネフィット比較型 (g)その他の型
備考	採否決定用	対策案選択用 組み合わせ決定用

代表的ITリスク


●：セキュリティの対象として扱われてきたもの
○：従来の対象であるがあまり扱われなかったもの
◎：今後重要になる分野
＜発生原因＞
故障・エラーなど
故意の不正
狭義のセキュリティの指標
広い指標
＜評価指標＞
大規模情報システムのバグによるシステムダウン（含む2000年問題）
◎
◎
デジタルフォレンジック
◎
個人情報漏洩
暗号の危殆化
●ウイルス被害
●不正侵入
サイバーテロ
従来の研究領域

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

調査・分析によるITリスクの特徴

＜リスクの一般的特徴＞

（1）ゼロリスクはない.

（2）定量的リスク評価が必要である.

（3）多くの関与者とのリスクコミュニケーションが大切である.

＜ITリスクの特徴＞

（1）ITリスク対策は1つの対策だけで対応するのは困難であり，いろいろな対策の組み合わせが不可欠である.

（2）「リスク対リスク」「多重リスク」への考慮が不可欠である.

調査・分析によるITリスクの特徴

＜リスクの一般的特徴＞

（1）ゼロリスクはない.

（2）定量的リスク評価が必要である.

（3）多くの関与者とのリスクコミュニケーションが大切である.

＜ITリスクの特徴＞

（1）ITリスク対策は1つの対策だけで対応するのは困難であり，いろいろな対策の組み合わせが不可欠である.

（2）「リスク対リスク」「多重リスク」への考慮が不可欠である.

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、

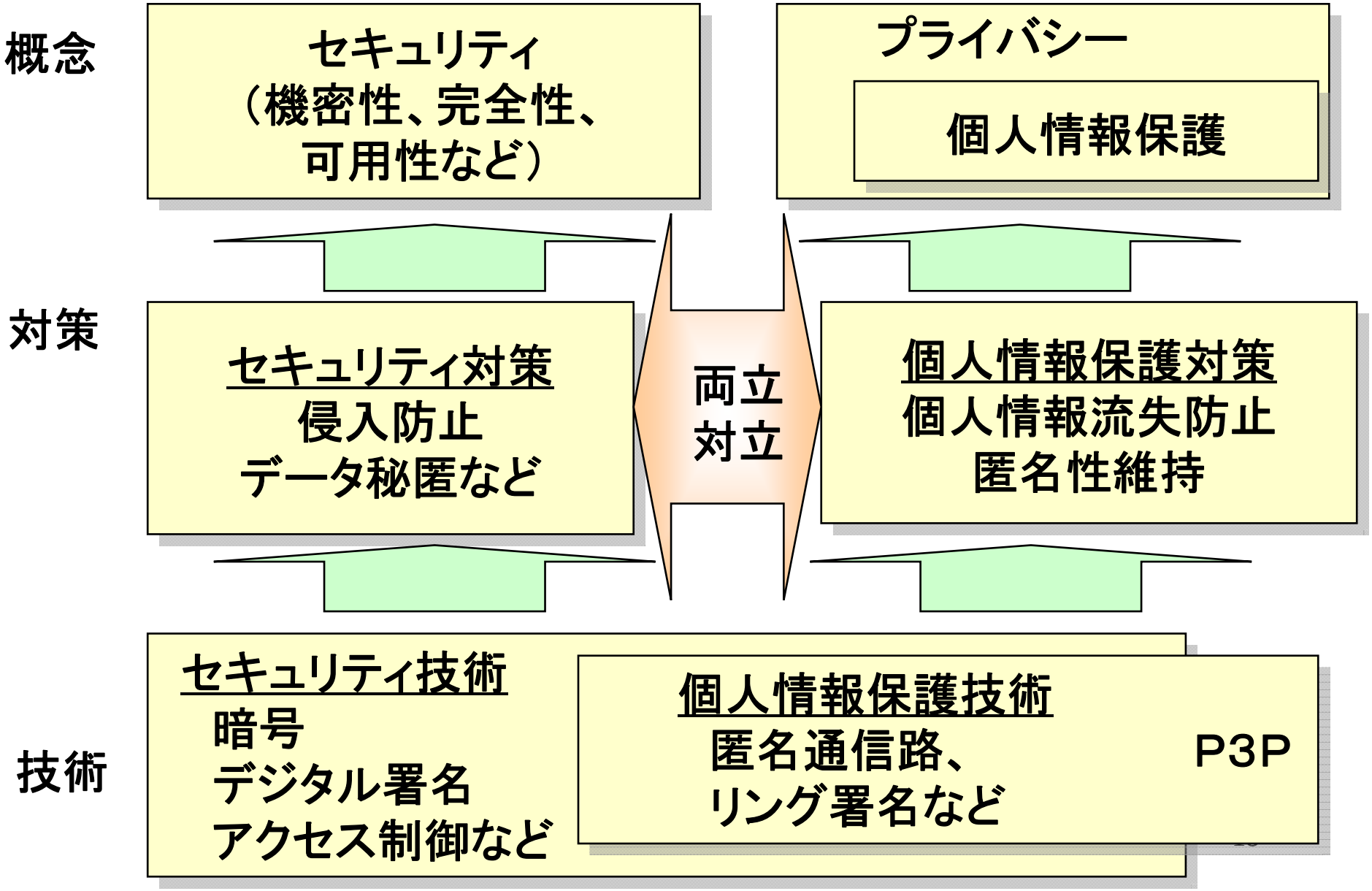
その対策によって生じる新たなリスクとテロのリスクとの間で真剣な比較検討が必要であり、

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。」

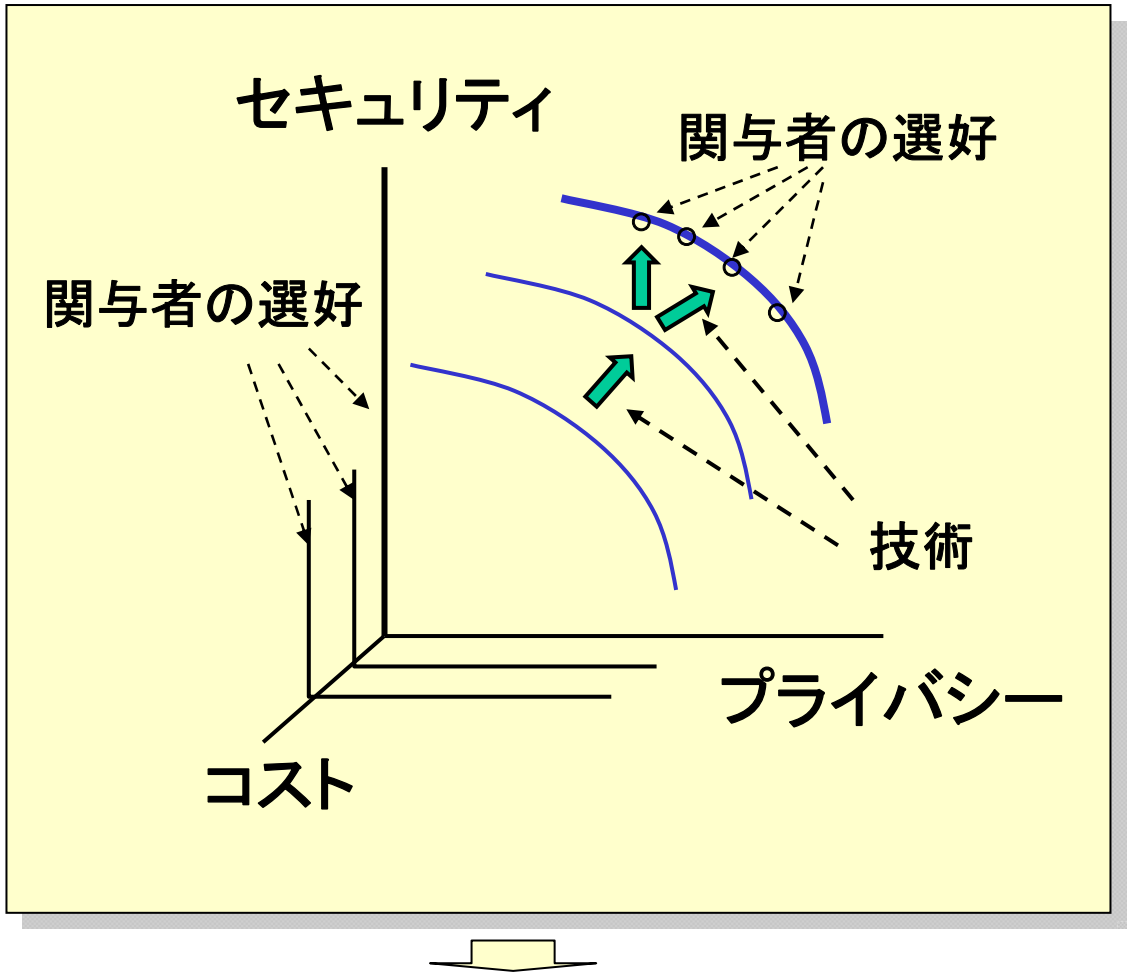
「リスク対リスク」 あるいは「多重リスク」 の時代に

（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）

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

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	世田谷区役所で実適用
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	JSSM論文（Vol.22,No.3）
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	情報処理学会論文（2008.3）

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

問題点と対策

(a)制約条件値を与えるのが簡単でない:
　昨年比，他社比，対策を行わない場合との比などで与えるようにすることで，比較的容易に制約条件値を与えてもらえるようになった.

(b)専門家が対象を理解し，分析し，リーゾナブルな入力を入れるのに時間がかかる:
　始めて適用する場合3ヶ月以上かかることも少なくない．これは，ある程度仕方の無い問題ではある．個人情報漏洩問題など，同じような対象に繰り返し適用することにより，作業の効率化を図ることが可能であり，1-2週間で適用可能となった例もある.

(c)リスクコミュニケーションで関与者が自説を強く主張し，パラメータの値についてまず，合意が得られない場合もある:
　この点については，どうしようもない場合もあるが，別々の条件でそれぞれ最適解を求め効用関数上に図示するなどの関与者支援機能の強化により解決がつく場合もあると考えている。この機能の有効性を実験を行う予定である．

適用結果

（1）MRCは，多重リスク下のリスクコミュニケーションの支援に基本的に有効である見通しが得られた.

（2）MRCプログラムを利用することにより，インターネットに接続できるところならどこでもリスクコミュニケーションが可能となり，関与者の意見の反映が容易となった.

（3）変数の数が15程度までなら，実用上問題がない時間で求解が可能であり，多くの実際的問題を扱えることが明らかになった.

この後の進め方案

パネリスト：大谷さん（被害調査WG）奥原さん（対策マップWG)
郷間さん（旧：脆弱性定量化WG)　二木 さん

・リスクアセスメントと定量化
　－なぜ定量化したいのか（各パネリストの思い）
　－定量化とはどういうものか（各パネリストの思い）

・定量化の切り口
　－トップダウンか、ボトムアップか（目的と手法）
　－被害調査結果からみたリスクの定量化
　－脅威／脆弱性の強さから見たリスクの定量化
　－対象と脅威、対策の関係とリスクの定量化

・リスクマネジメント全体から見た定量化の意味
　リスクマネジメント全体からみて、定量化の意味と使い方を
　考えてみる。また、ビジネスにとって正しくリスクを評価
　できることはどのような意味を持つのか、というような点