Information Security Laboratory
ISL

JSSM

2008年6月28日

ITリスク学研究会の進め方（案）
―情報セキュリティを超えて―

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

ITリスク

安全・安心

ニュー・ディペンダビリティ

Trust

Security
Privacy
Reliability
Safetyなど

広義のセキュリティ

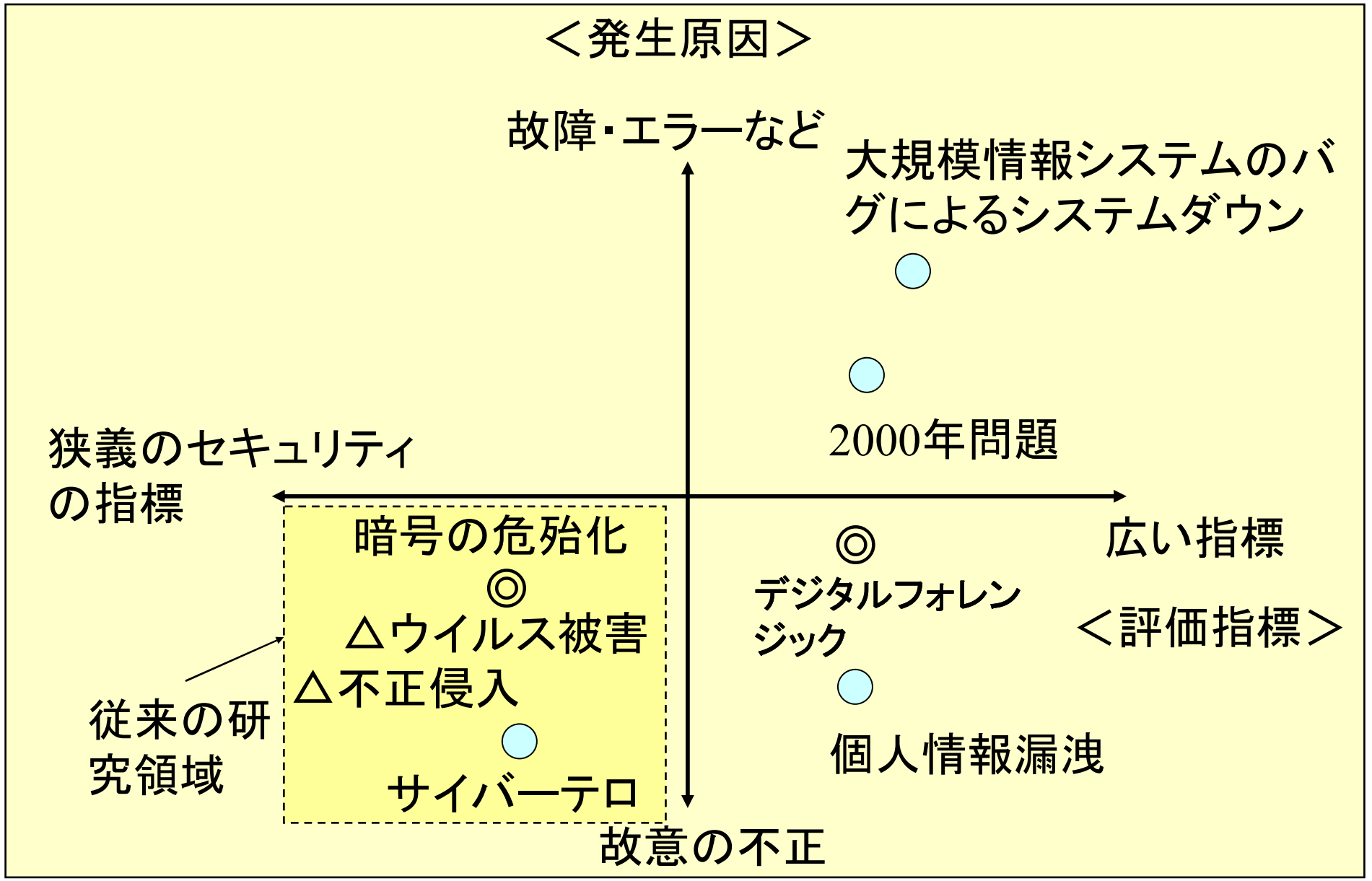
低減対策

逆から見た概念

ITリスク
（Risk）
影響　x
発生確率

確率論的扱いが
不可欠

代表的ITリスク


＜発生原因＞
故障・エラーなど
大規模情報システムのバグによるシステムダウン
2000年問題
狭義のセキュリティの指標
広い指標
暗号の危殆化
◎
△ウイルス被害
△不正侵入
サイバーテロ
◎
デジタルフォレンジック
個人情報漏洩
＜評価指標＞
従来の研究領域
故意の不正

リスクvsリスクの時代

９．１１事件の後のテロ対策時の多くの発言

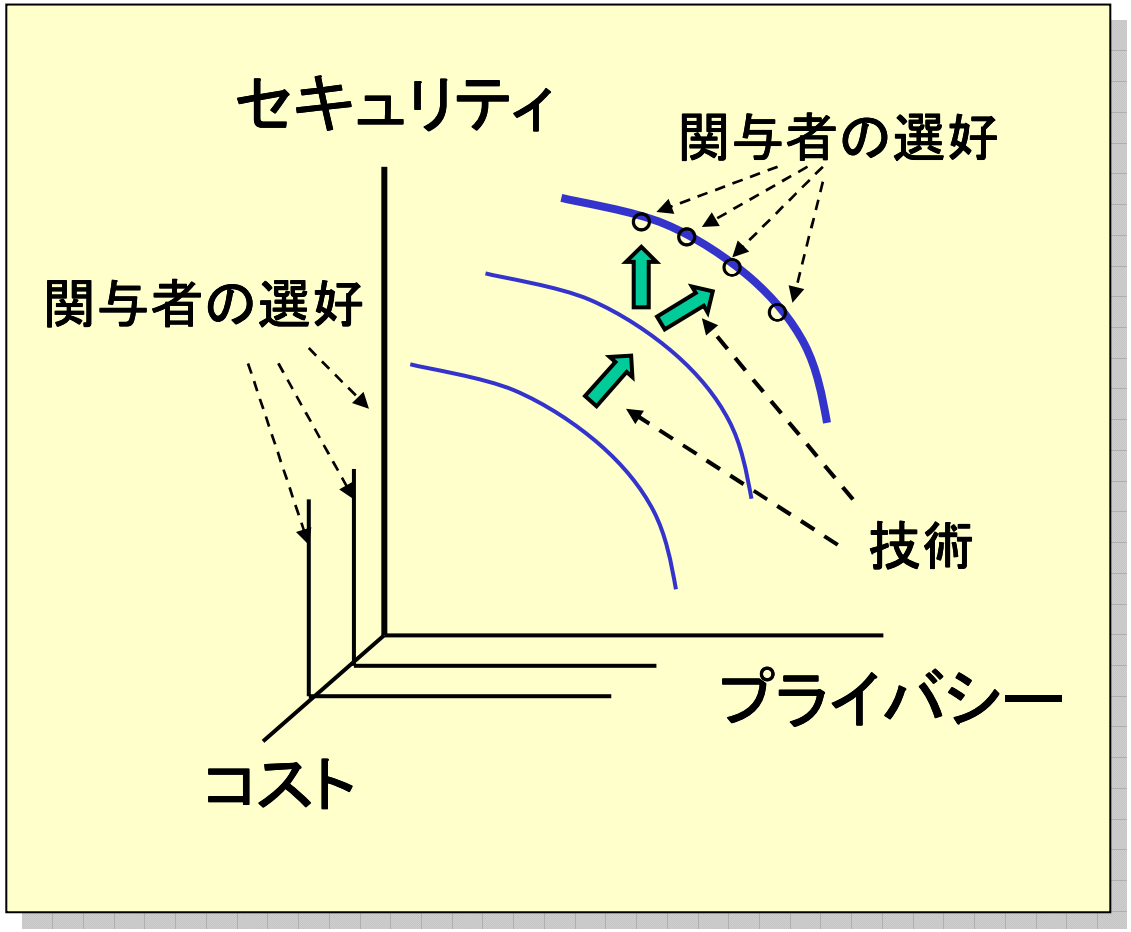
「こんなことが繰り返されてはならない。あらゆる手段を講じて再発を防止しなければならない。」

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。」

これは、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ということを言っているのであろう。

リスクvsリスクの時代



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）

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

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

ITリスクへの対応法の基本認識（１）

（１）ITシステムの安全性確保のため故意の攻撃だけでなく偶発的障害もITリスクの対象とすべきである。そのため、従来のセキュリティだけでなくSafetyやReliabilityも対象とすべきである。

（２）ITシステムは常に安全性が失われる可能性を確率的に持っておりゼロリスクはないという認識を持つべきである。

（３）したがって対策の順位付けには定量的リスク評価あるいは準定量的リスク評価が不可欠である。

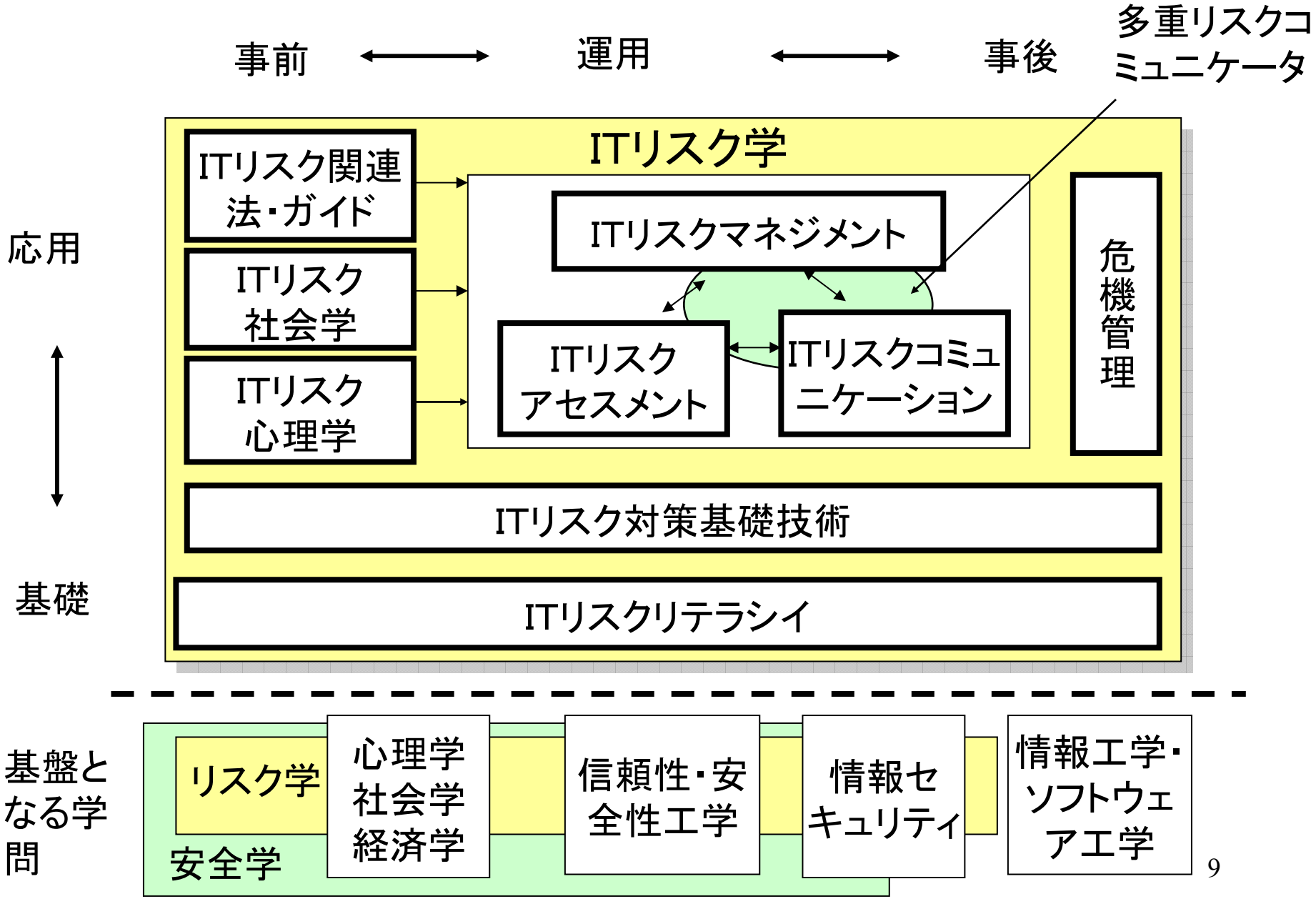
（４）1つのリスクへの対策が別のリスクの原因になる「Risk vs. Risk」あるいは「多重リスク」への考慮が不可欠である。

（５）対策の決定に当たっては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リスクへの対応法の基本認識（2）

（6）ITリスクの顕在化は確率現象であり1つの対策だけで事前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必要な場合が多い。
（7）確率的に起こる現象への対策は一般に困難であり、対策がうまく行かない場合があるので、その場合に備えた危機管理も不可欠である。
（8）リスクマネジメント・リスクアセスメント・リスクコミュニケーションが対策のITリスク対策の3本柱でありこれらへの総合的アプローチが必要となる場合が多い。
（9）確率現象に対する人間の合理的対応は一般に困難であり、なぜ困難であるかの研究や、合理的に対応できるようにするための研究が不可欠である。

ITリスク学の構成


事前
運用
事後
多重リスクコミュニケータ
応用
基礎
ITリスク学
ITリスク関連法・ガイド
ITリスク社会学
ITリスク心理学
ITリスクマネジメント
ITリスクアセスメント
ITリスクコミュニケーション
危機管理
ITリスク対策基礎技術
ITリスクリテラシイ
基盤となる学問
リスク学
安全学
心理学
社会学
経済学
信頼性・安全性工学
情報セキュリティ
情報工学・ソフトウェア工学

ITリスク学の構成要素
ITリスク心理学

ITリスクに対する人々の認知活動の特徴を把握したり、適切なリスクコミュニケーションを行なったりするための基礎となる学問である。人々が、ITリスクに適切に対応し、安全なものに安心感を持ち、危険なものを危険と認識するようになっていくのに不可欠なものであると考えられる。

通常のリスク心理学と違いがあるのかないのかを明確化する必要がある。

ITリスク社会学

（a）社会や組織が、このようなITリスクにどのように関わっていく傾向があるかの分析や、

（b）マスメディアの対応方法など

いろいろな研究課題があると考えられる。

谷山らの「2000年問題に対するリスクコミュニケーションの研究」もここに位置づけられる。

ITリスク対応の法令

個人情報保護法、会社法、金融商品取引法などがある。

これらの法令は企業に対し、いろいろなITリスクの低減対策を促進するものとして機能する。また、情報セキュリティマネジメントシステムや事業継続管理のように、ITリスクを低減するためのガイドや制度がある。

これらの、法令や制度のあるべき姿や、企業として法令遵守などを効率的に実施していく方法も今後の研究課題であろう。

ITリスク法学ということでの研究対象にもなりうる

ITリスクリテラシ

ITリスクに適切に対応するための基本能力のことで、ゼロリスクはないといった基本的認識や、ITリスクへの対応方法の概要を知っていることなどをさすことにしよう。

このリテラシは、リスク対策実行者、一般の人々、専門家、マスメディア関係者、ITリスク対策を行う人で共通する部分と独自に必要となる部分がある。

危機管理

リスクマネジメントが、災害が起こる前の対策を対象とするのに対し、危機管理（クライシスマネジメント）は、災害が起こってからの対策を主な対象とする。

災害が起こっても事業をできるだけとめずに実行していくBCP,BCMなどの対応方法などが含まれる。

ITリスク対策基礎技術

ITリスク学に必要な基本的技術といったようなざっくりした定義をしている。

従来のセキュリティ対策技術や信頼性・安全性対策技術と重複する部分が多いと思う。また、ITリスクマネージメント・ITリスクアセスメント・ITリスクコミュニケーション、ITリスク心理学、危機管理学など分野を切り分けたものとの切り分けが困難な部分も多い。

とりあえず、これらの分野を渡って必要となる基礎技術を扱うことにすべきではないかと考えている。現状では、合意形成を支援する技術、リスクの大きさを推定する技術や、対策の組み合わせを決定するための技術などを考えている。ITリスク学の全体構造を構築する技術もここに入れるべきかも知れない。

リスクM・A・C

リスクマネジメント・リスクアセスメント・リスクコミュニケーションのリスク学を構成する基本要素。いろいろな方法が提案され一部適用されている。

この3つに関する統合的アプローチが重要と考えており、その一例に「多重リスクコミュニケータ」の開発がある。

3．ITリスク学のーアプローチ

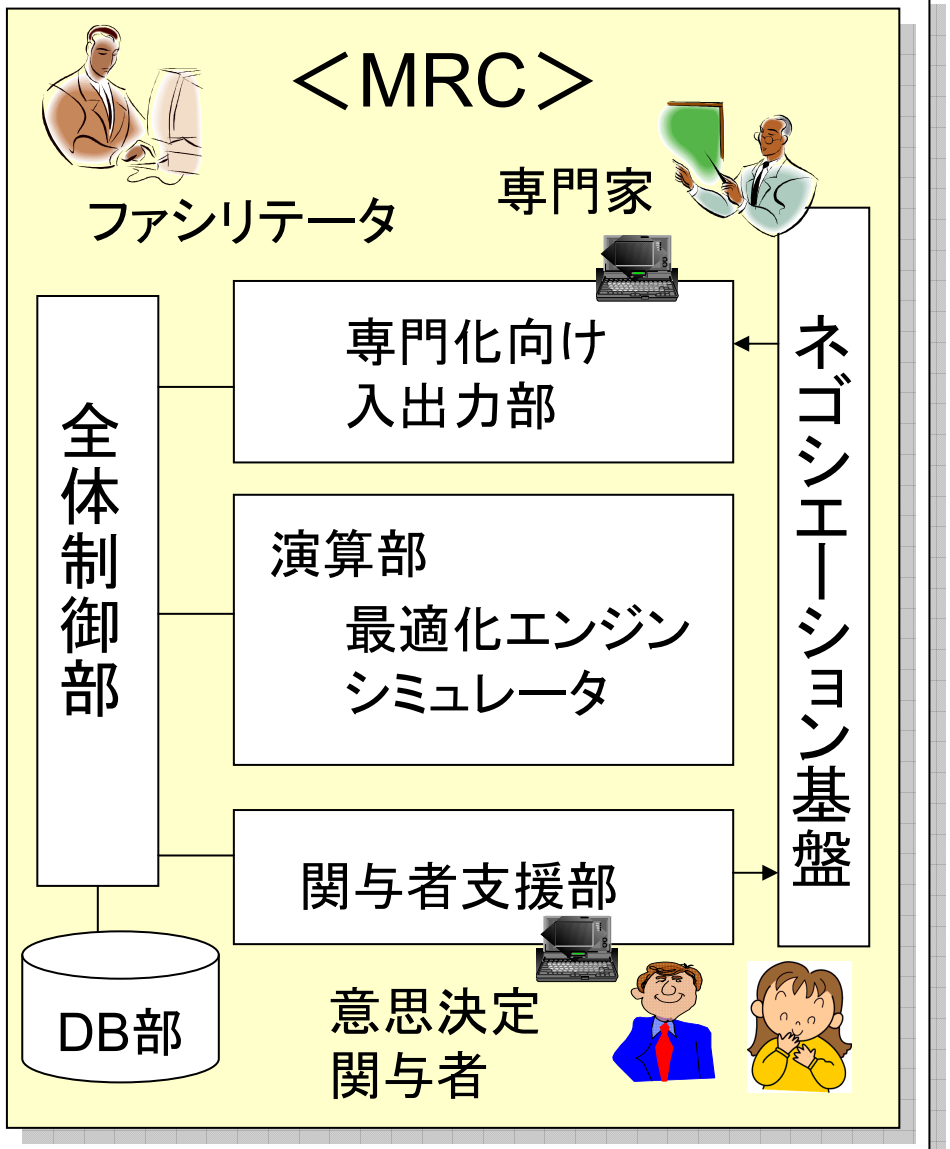
多重リスクコミュニケータ（MRC）開発の背景

＜背景＞

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



3．ITリスク学の一アプローチ

多重リスクコミュニケータ（MRC）開発の背景

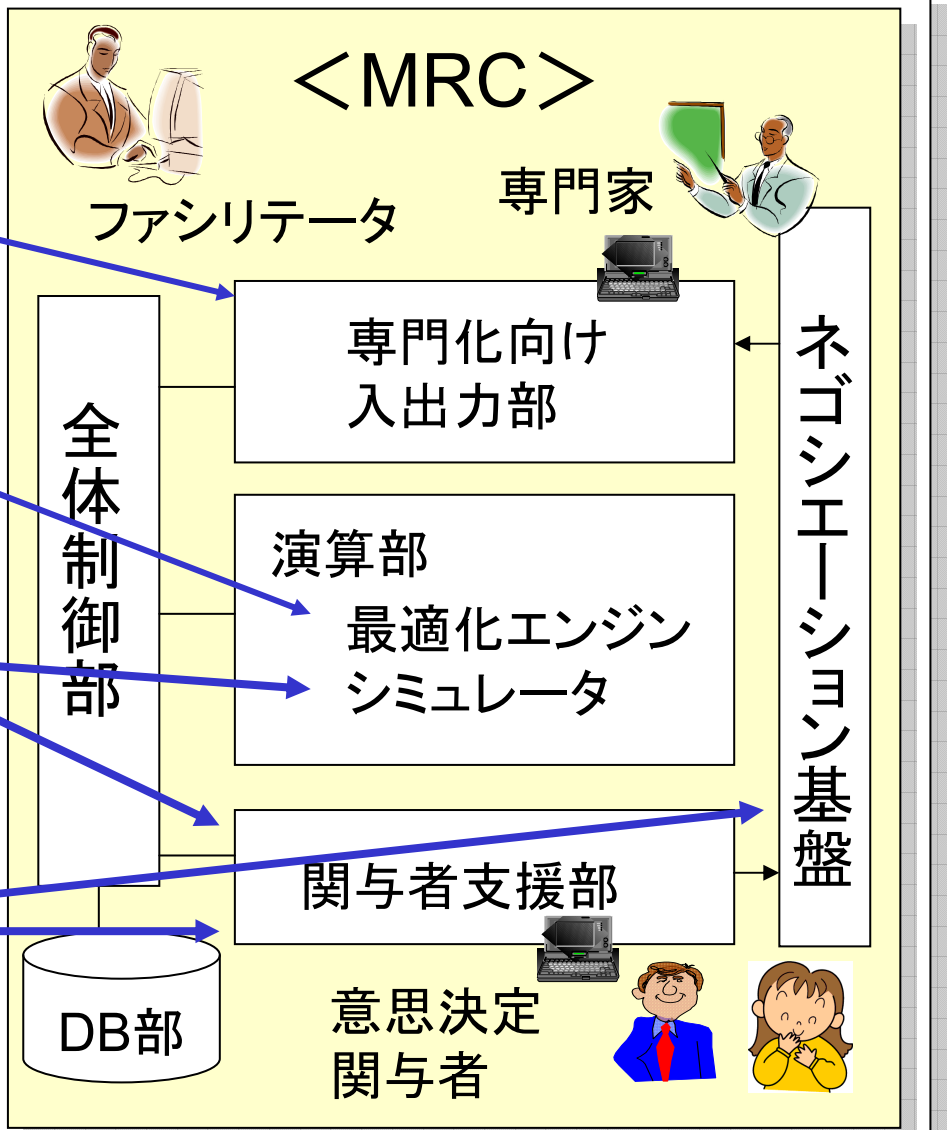
適用手順

①専門家が対象を分析し最適組み合わせ問題として定式化する。

②最適化エンジンを用いて、最適組み合わせを求める。（例：対策1と3の組み合わせなど）

③この結果をシミュレータや関与者支援部を用いてわかりやすく表示

④「もっと別の対策案が考える」とか「制約条件値が違う」などの意見を言う。この結果は専門家によって反映され、MRCを用いて結果が再表示される。

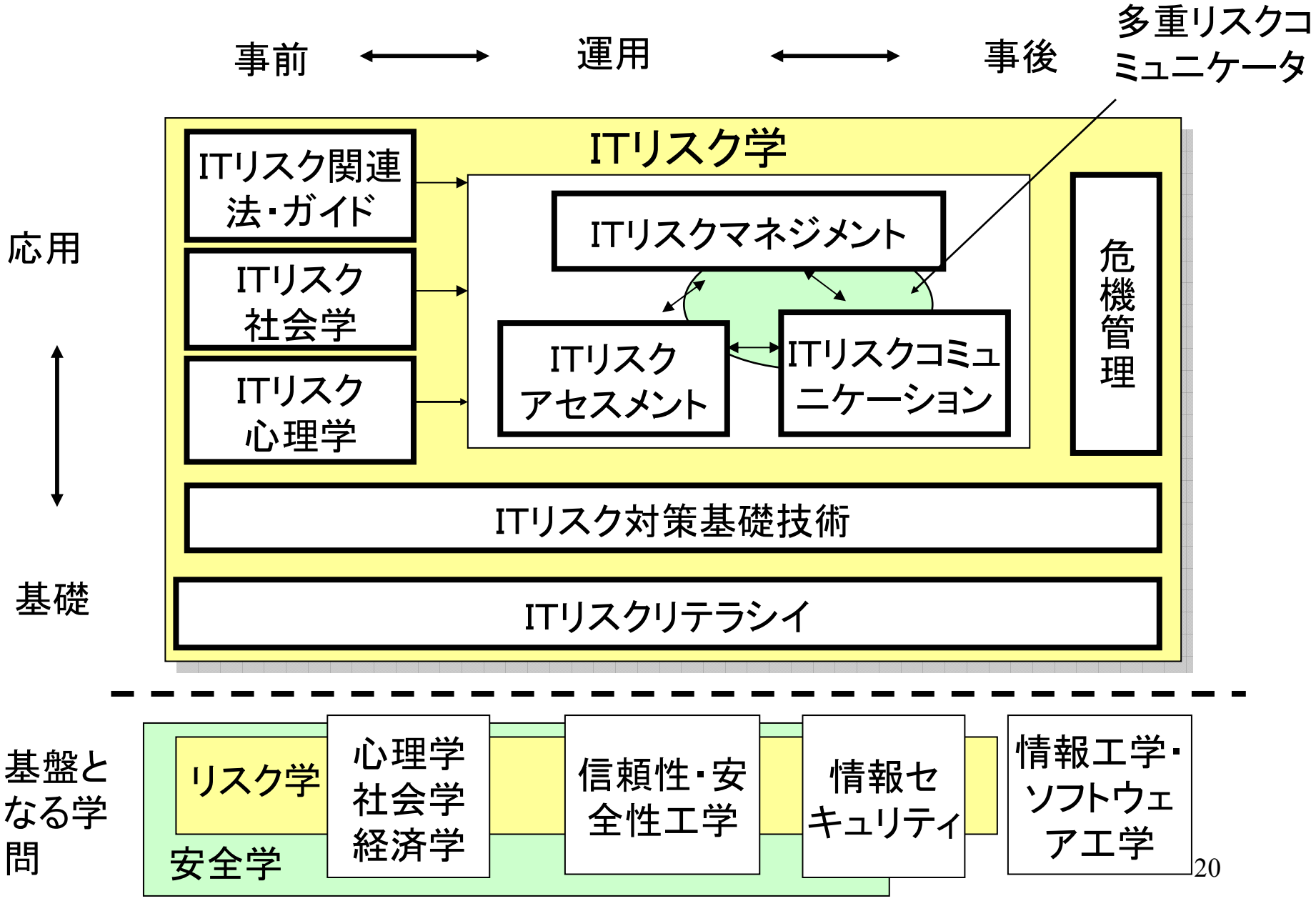


適用結果の概要

	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

ITリスク学の構成


事前
運用
事後
多重リスクコミュニケータ
ITリスク学
ITリスク関連法・ガイド
ITリスク社会学
ITリスク心理学
ITリスクマネジメント
ITリスクアセスメント
ITリスクコミュニケーション
危機管理
ITリスク対策基礎技術
ITリスクリテラシイ
応用
基礎
基盤となる学問
リスク学
安全学
心理学
社会学
経済学
信頼性・安全性工学
情報セキュリティ
情報工学・ソフトウェア工学

４．ITリスク学研究会の進め方（１）

（１）JSSMの中にITリスク学研究会を設立する。

5月末に正式認可。主査：佐々木、幹事：千葉、幹事補佐：芦野とする。

（２）第一回会合は6月28日に東京電機大学で実施の予定。

（３）研究会自体は年に4回程度。

外部の人の講演と、会員による発表を実施する。

会員による発表はpptを用い、希望者にはPDFをダウンロード可能とするが論文誌は発行しない。発表のうちよいものを、JSSM全国大会での発表や、JSSM誌への投稿を薦める。

（４）メーリングリスト：jssm_it_risk@freedomsoft.net

４．ITリスク学研究会の進め方（２）

（４）外部の発表者候補は下記のとおり。

（a）中谷内一也（帝塚山大学 教授）「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の著者

（b）松原純子氏（元原子力安全委員会委員）生物関連のリスク学の専門家

（５）第一回会合には「ITリスク学は可能か」などといったパネルを実施する。

（６）研究会の中にWGを設置し、そこでの検討結果をこの研究会で発表するなどの対応も行いたい。

（７）情報処理学会のSPT研究グループなどとの共同開催も行っていきたい。

第一回研究会

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
４．その他
登録メンバー以外にも参加を広く呼びかける予定

パネルの進め方

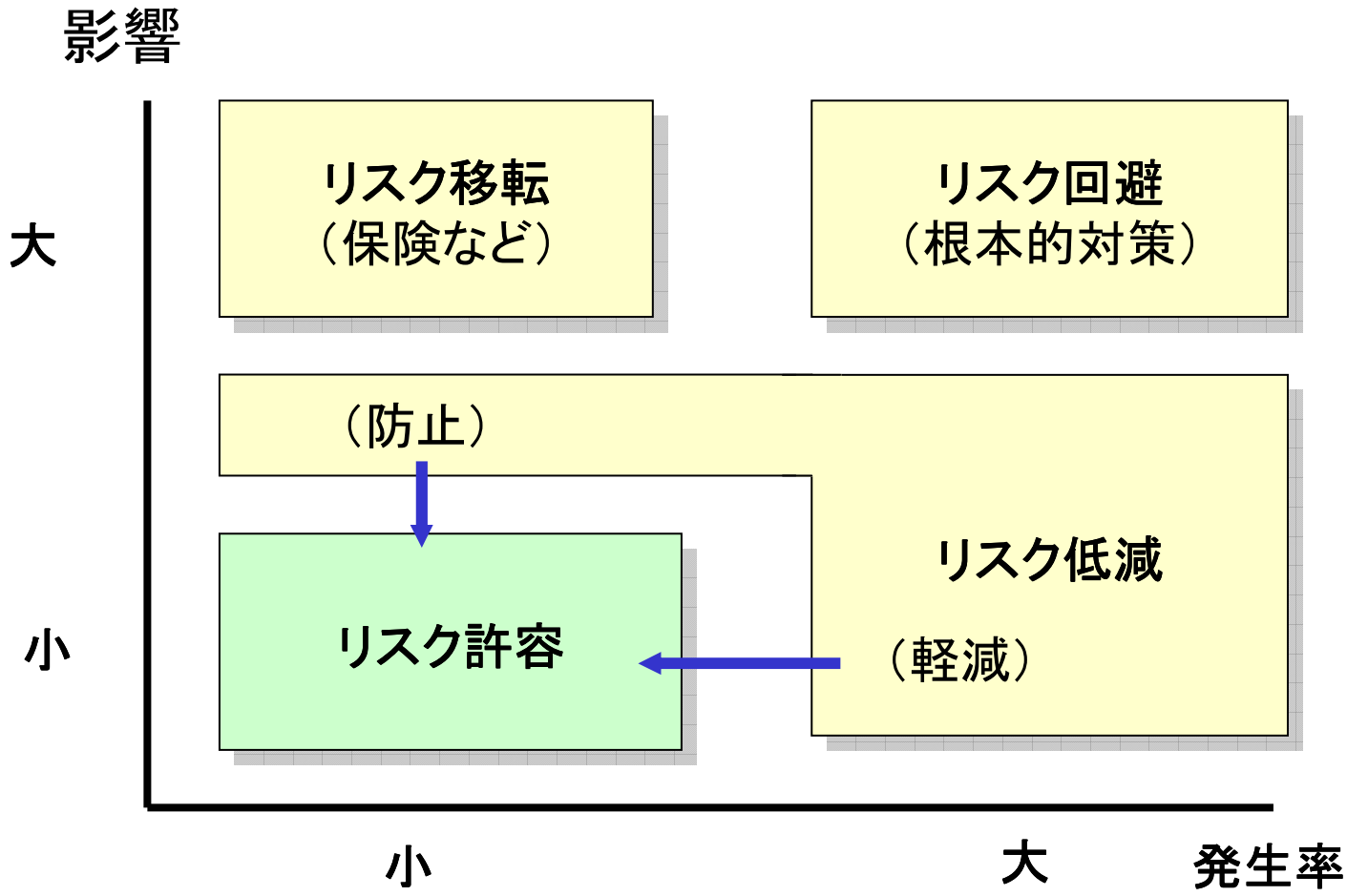
- 佐々木の「 ITリスク学とITリスク学研究会の進め方の構想」に続き、大木先生、千葉さんより、ITリスク学のとらえ方と、自分として力を注いで行きたいテーマについて説明を追加する。
- 丸山さん、岩下さん、関口さんのそれぞれの立場からITリスク学のとらえ方に関する意見と、ITリスク学に期待するものを述べる。自分ならITリスクの研究をどのように進めるかがあればさらにうれしい。
- それらを受けて相互に、意見を交換し、ITリスク学はいかにすれば有益なものとなりうるかを明確にしていく。

Information Security Laboratory

ISL

さらに知りたい人のために

リスクへの対応方法



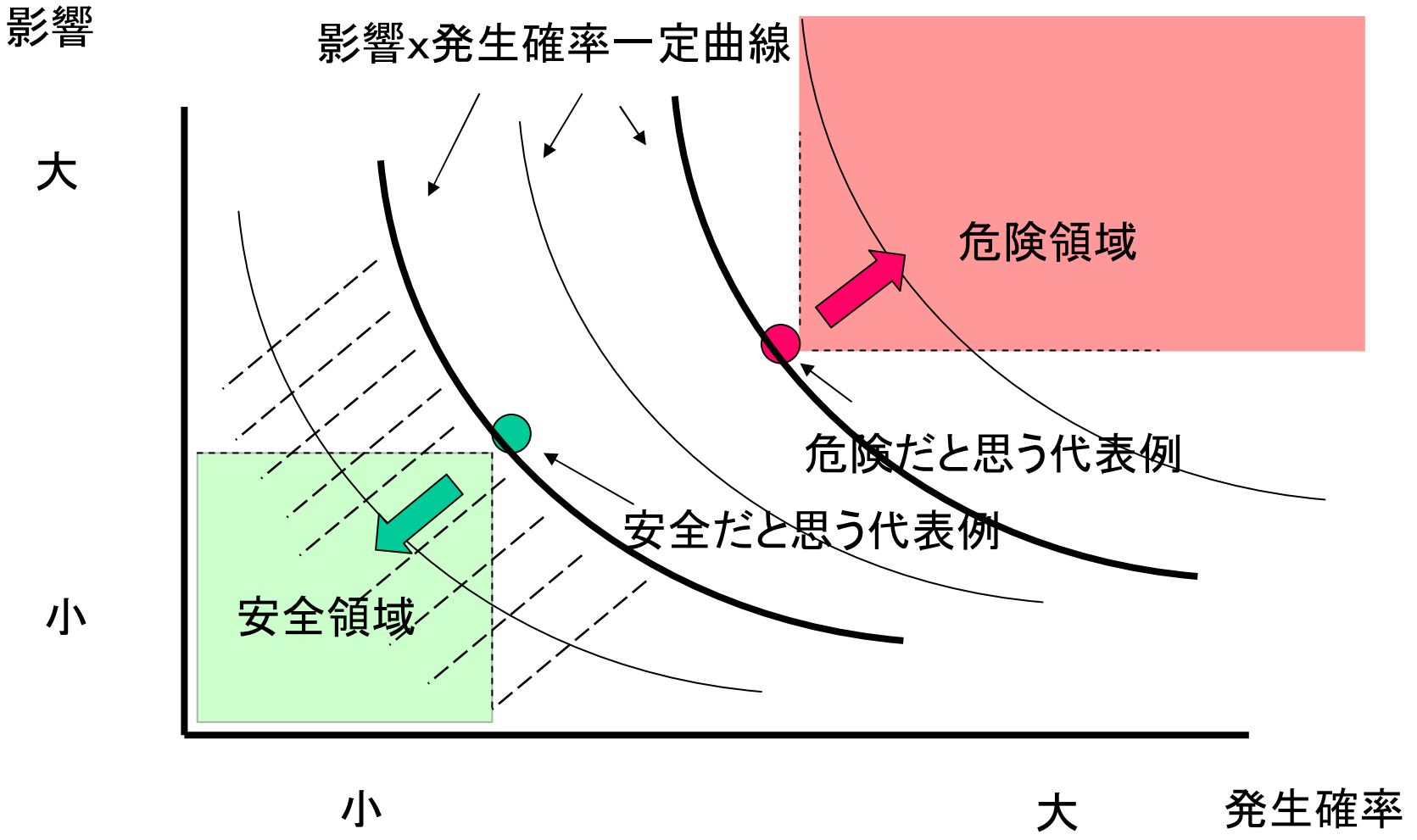


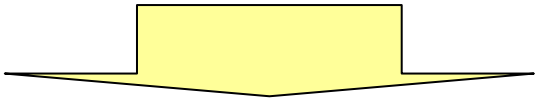
図5．12　リスクへの対応法

＜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＞

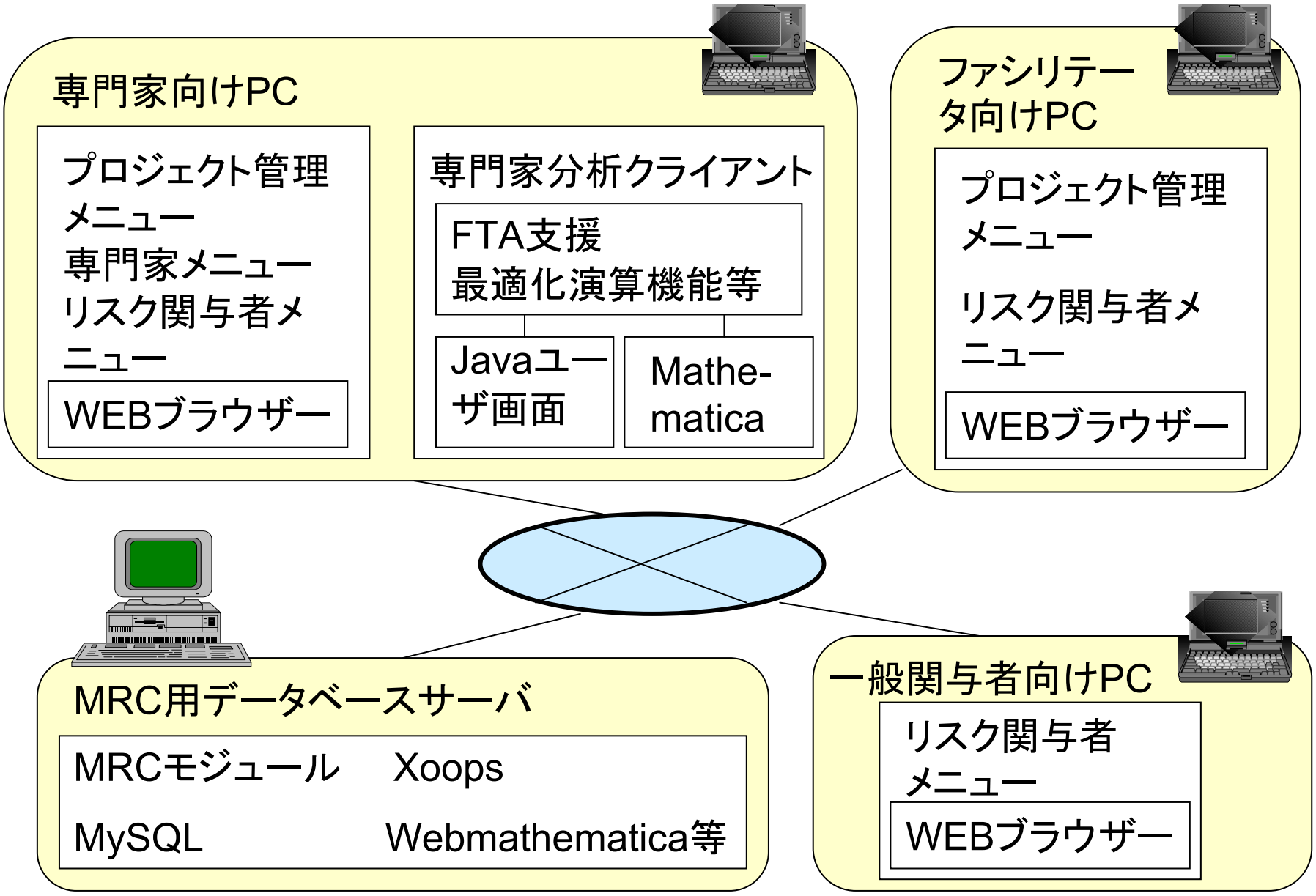
情報資産	資産価値	脅威レベル	脆弱性レベル	リスク値
A	4	3	3	３６
B	2	4	5	４０



リスク値の大きい情報資産Bに対する対策を優先

図５．３　JIPDECのリスク算出式

MRCシステムの構成


専門家向けPC
プロジェクト管理
メニュー
専門家メニュー
リスク関与者メ
ニュー
WEBブラウザー
専門家分析クライアント
FTA支援
最適化演算機能等
Javaユー
ザ画面
Mathe-
matica
ファシリテー
タ向けPC
プロジェクト管理
メニュー
リスク関与者メ
ニュー
WEBブラウザー
MRC用データベースサーバ
MRCモジュール
Xoops
MySQL
Webmathematica等
一般関与者向けPC
リスク関与者
メニュー
WEBブラウザー

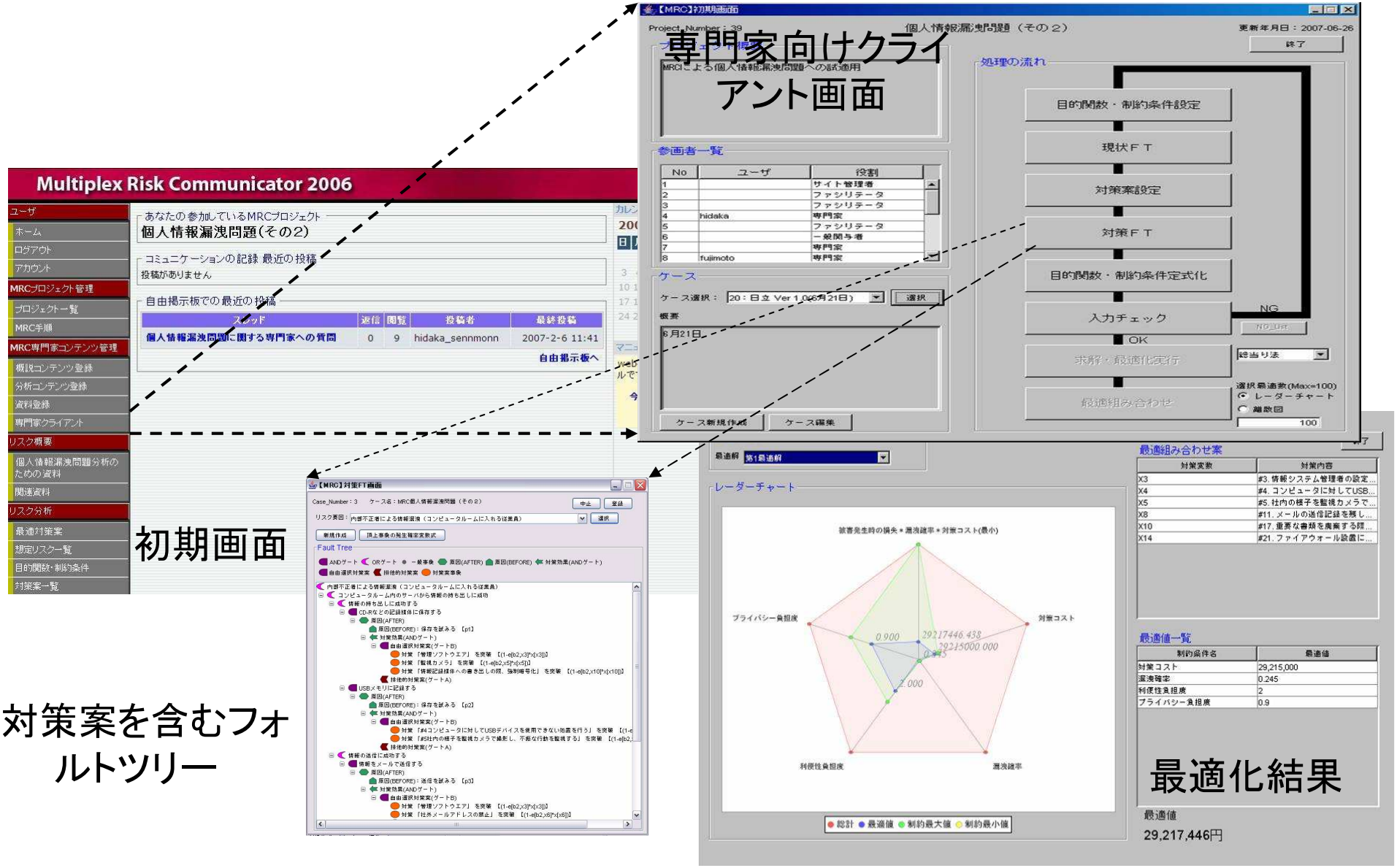


図6　MRCプログラムの専門家向け画面イメージ

RC:リスクコミュニケーション

1st RC

（リスク理解）

2nd RC

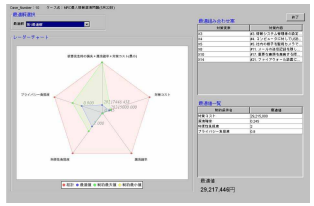
（関与者間の相互理解）

3rd RC

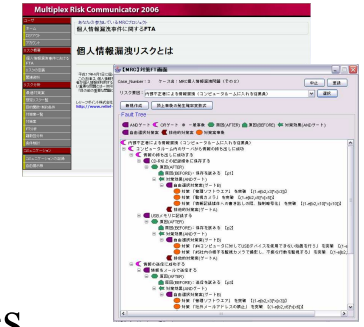
（合意形成）

①専門家による最適解の求解

②求解の前提と第１－第L最適解の表示



③ポータルシステムを利用した関与者のリスク理解



④目的関数・制約条件式、対策案への合意形成

⑤パラメタ値、制約条件値の合意形成

no

yes

⑥専門家による関与者ごとの最適解の求解

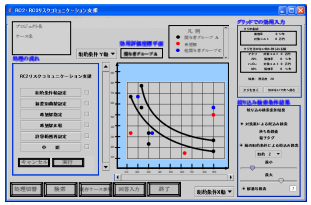
⑦専門家による最適解の求解

⑧効用関数を利用した他関与者の希望解の位置づけ

⑨関与者間で相互理解できたか

no

yes



⑩ファシリテータによる妥協解の提示など

⑪合意形成なし

⑫合意の形成（対策案組合わせ）

図　合意形成のためのフロー