Information Security Laboratory

JSSM

2008年2月24日

ITリスク学への道
―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

ITリスク

安全･安心

低減対策

ニュー･ディペンダビリティ

Trust

Security
Privacy
Reliability
Safetyなど

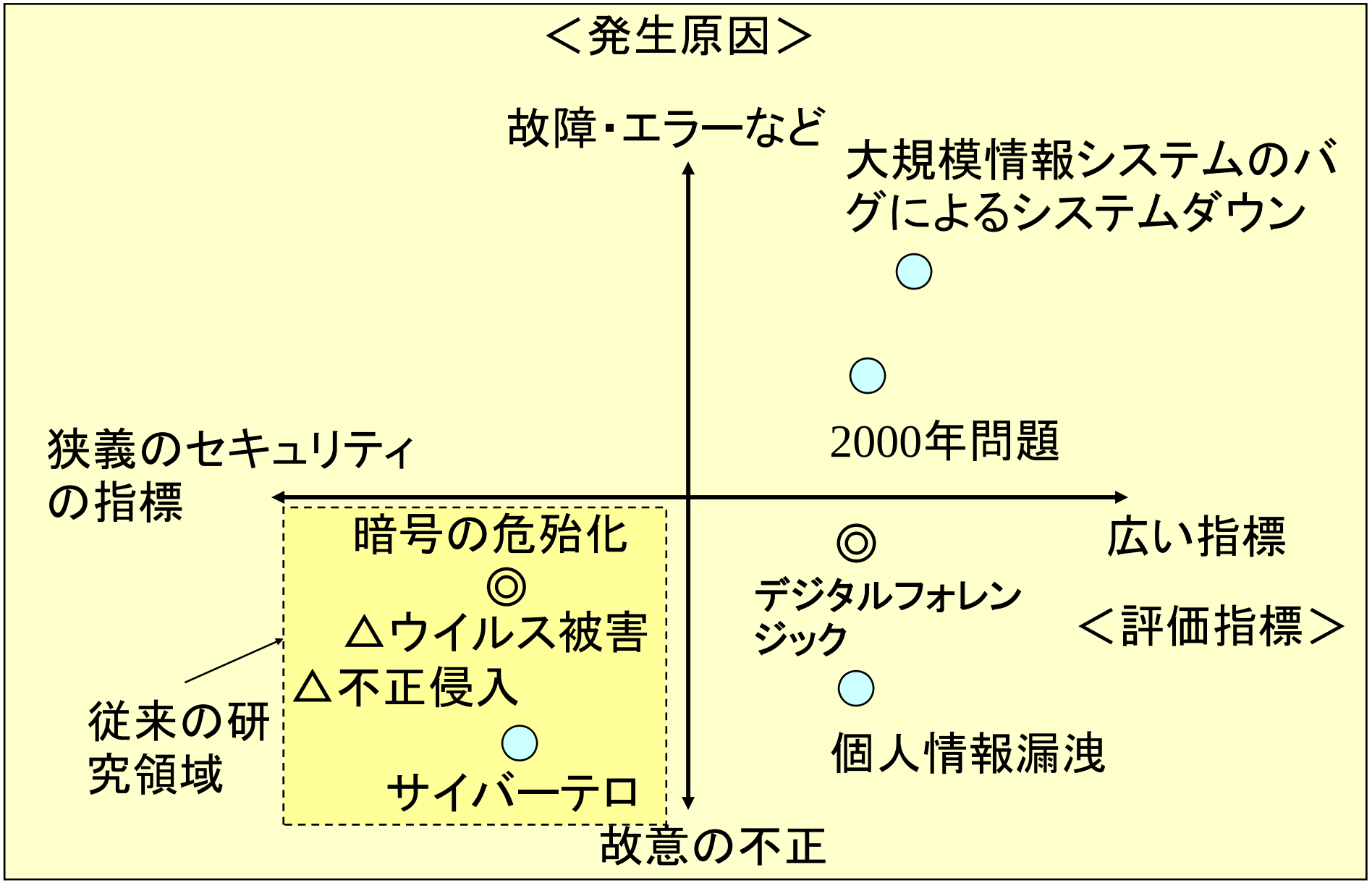
広義のセキュリティ

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
故意の不正
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
＜評価指標＞
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
従来の研究領域

リスクvsリスクの時代

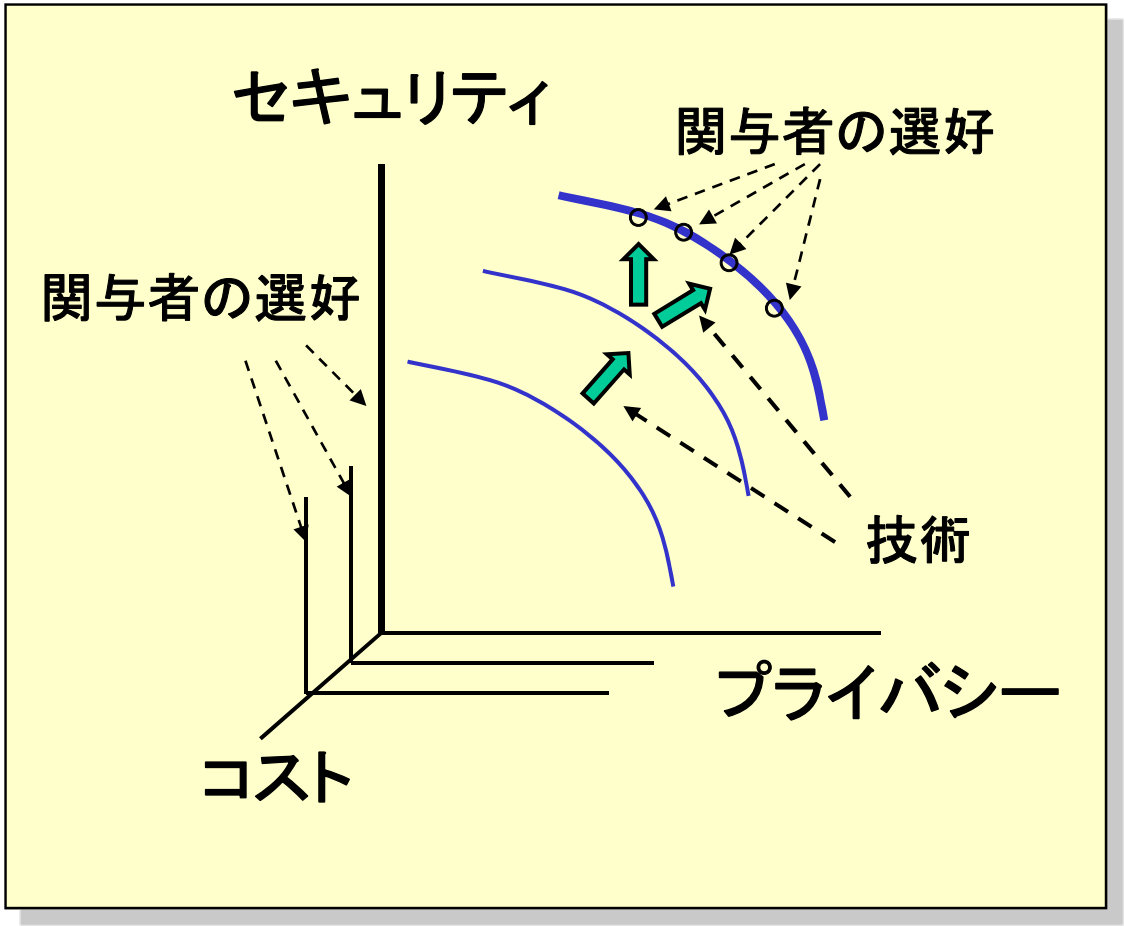
「こんなことが繰り返されてはならない。あらゆる手段を講じて再発を防止しなければならない。」

ブルース・シュナイアー氏は9．11事件の後のテロ対策時のそのような発言に対し、

「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、懸命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

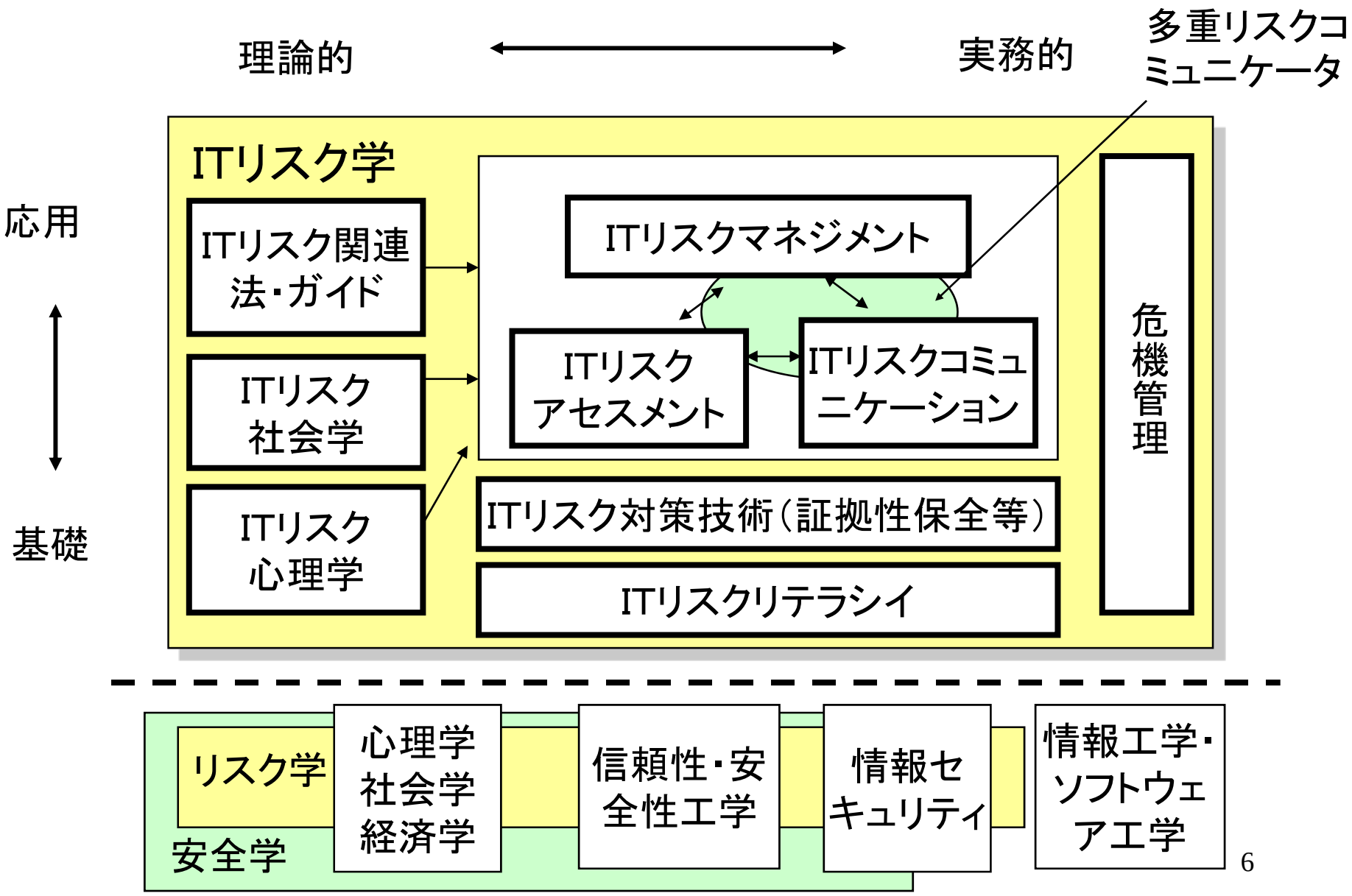
技術による解決

＜例＞

公開鍵証明書の利用

属性証明書の利用など

ITリスク学の構成


理論的
実務的
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リスク対策技術（証拠性保全等）
ITリスクリテラシイ
リスク学
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
安全学

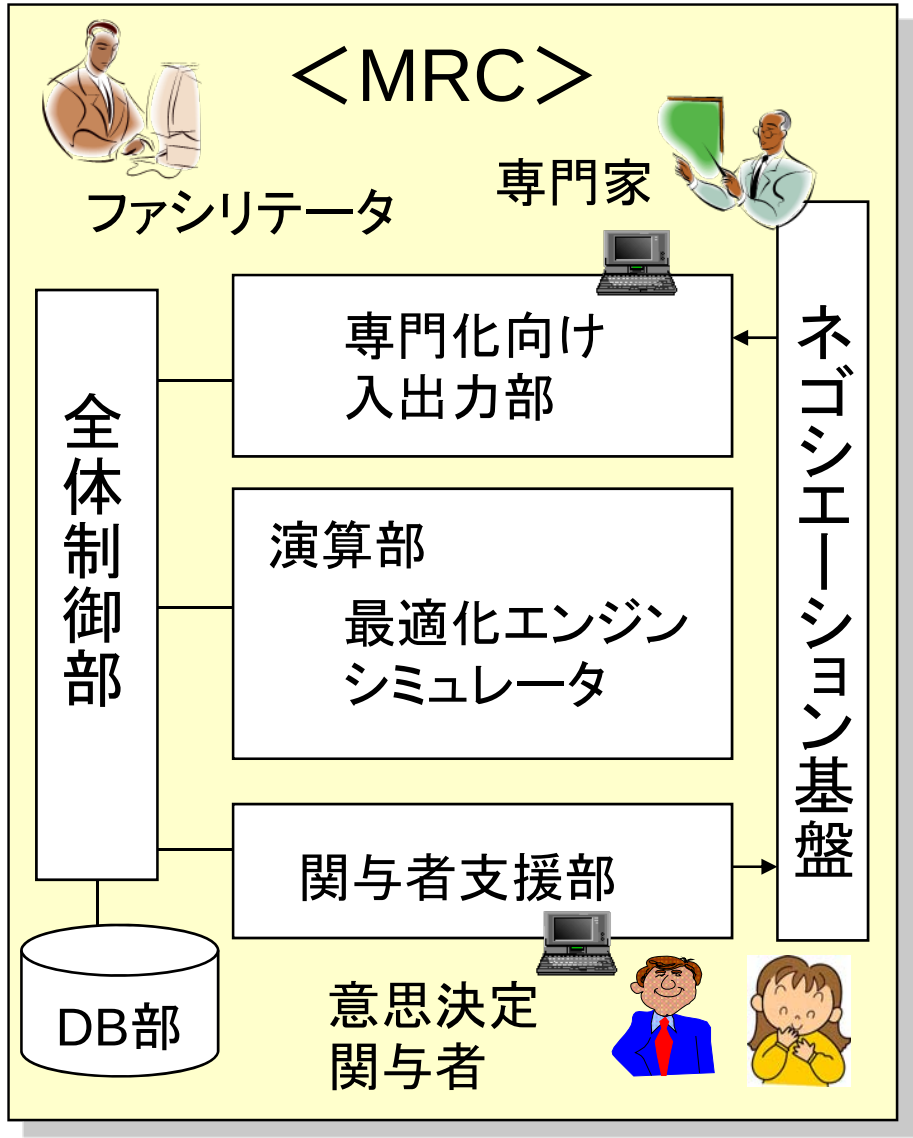
多重リスクコミュニケータ(MRC)開発の背景

＜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

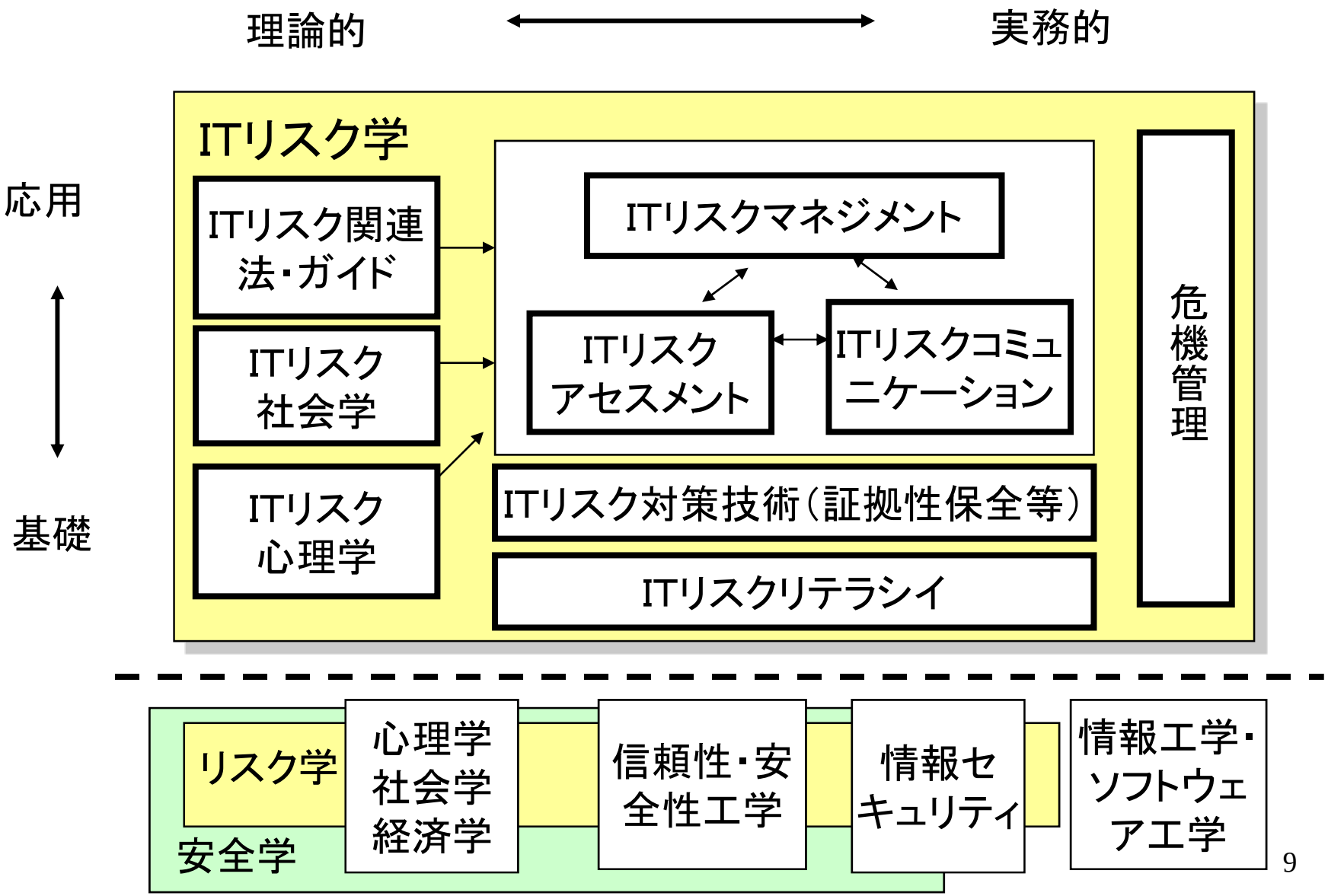


適用結果の概要

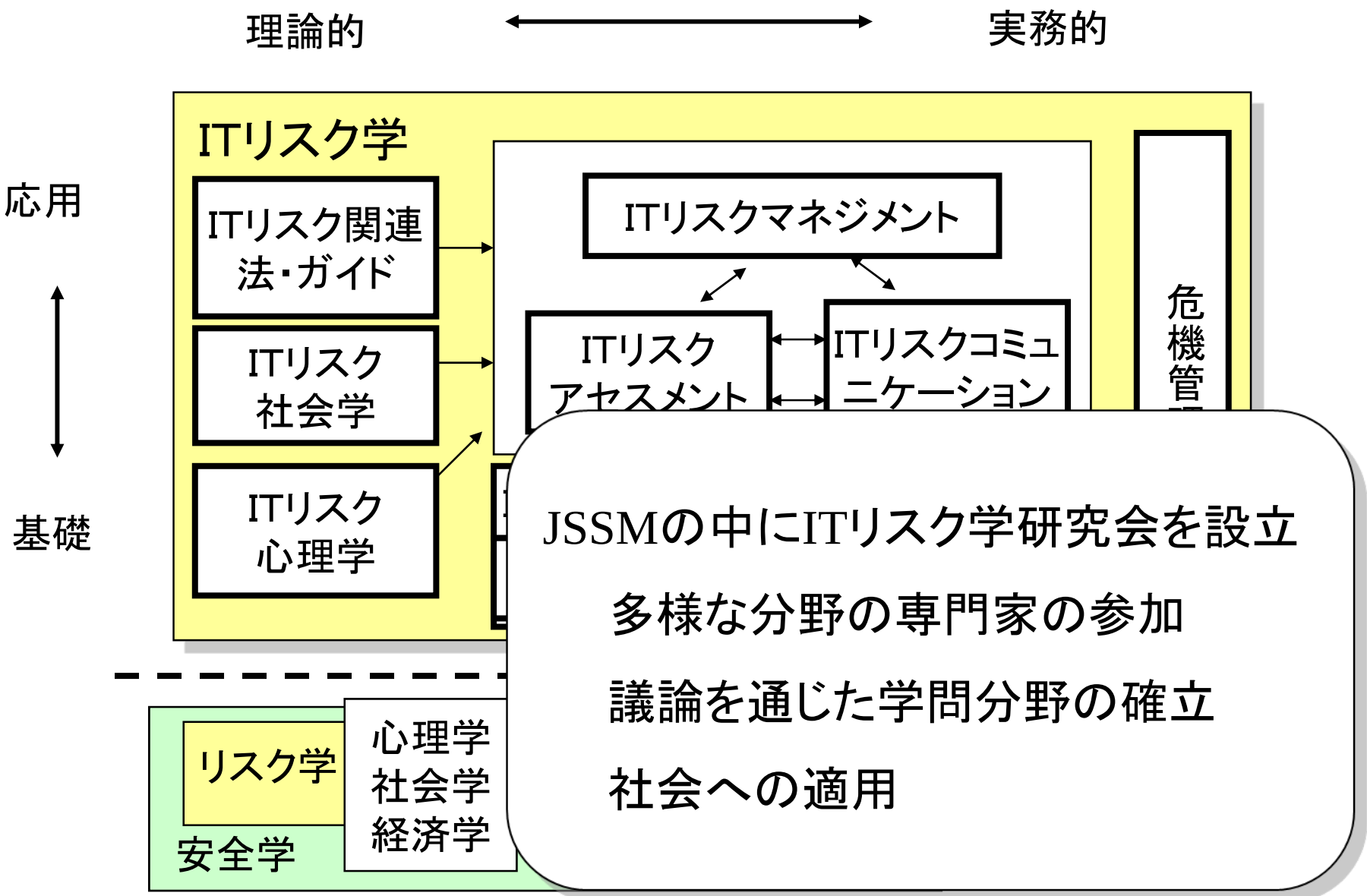
	対象	目的	関与者	分析手法	備考
1	個人情報漏洩への適用	従業員の負担も考した対策案の合意形成	経営者 顧客 従業員	FTA	プロバイダ 一般企業 区役所
2	不正コピーによる著作権侵害問題への適用	対策後の不正者の行動を想定した効果予測に基づく合意形成	レコード会社 消費者	FTA （不正者はシミュレータで実現）	CSS2006で発表
3	内部統制問題への適用	公的資金の適切な運用に関する内部統制対応	センタ 教授 学生	ETA	CSS2007で発表予定
4	暗号の危殆化対策への試適用	暗号危殆化時の署名つき文書への安全性対策の合意形成	政府 署名者 検証者	ETA	CSS2006で発表

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

ITリスク学の検討のために



ITリスク学の検討のために

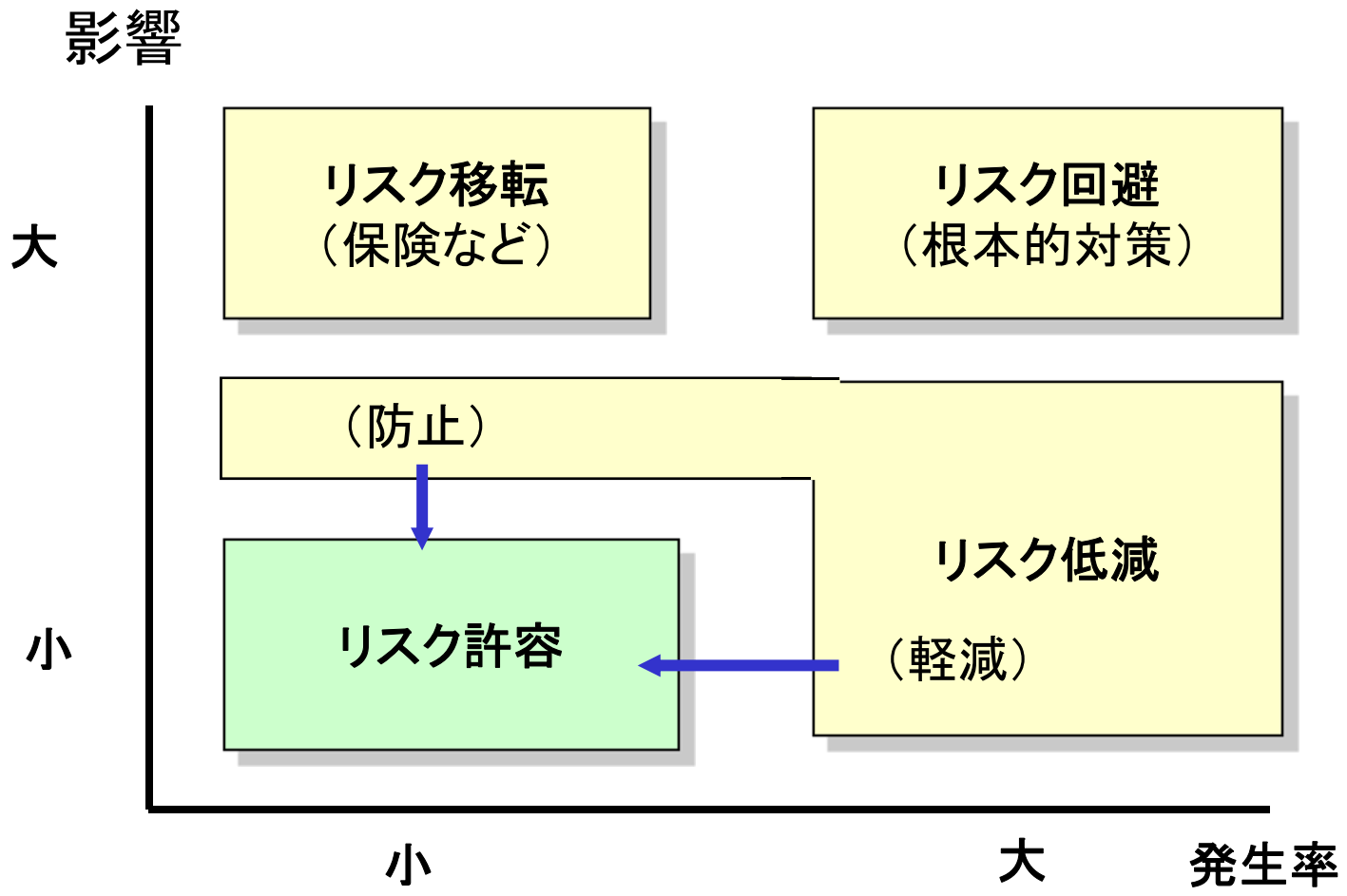


Information Security Laboratory

ISL

さらに知りたい人のために

リスクへの対応方法



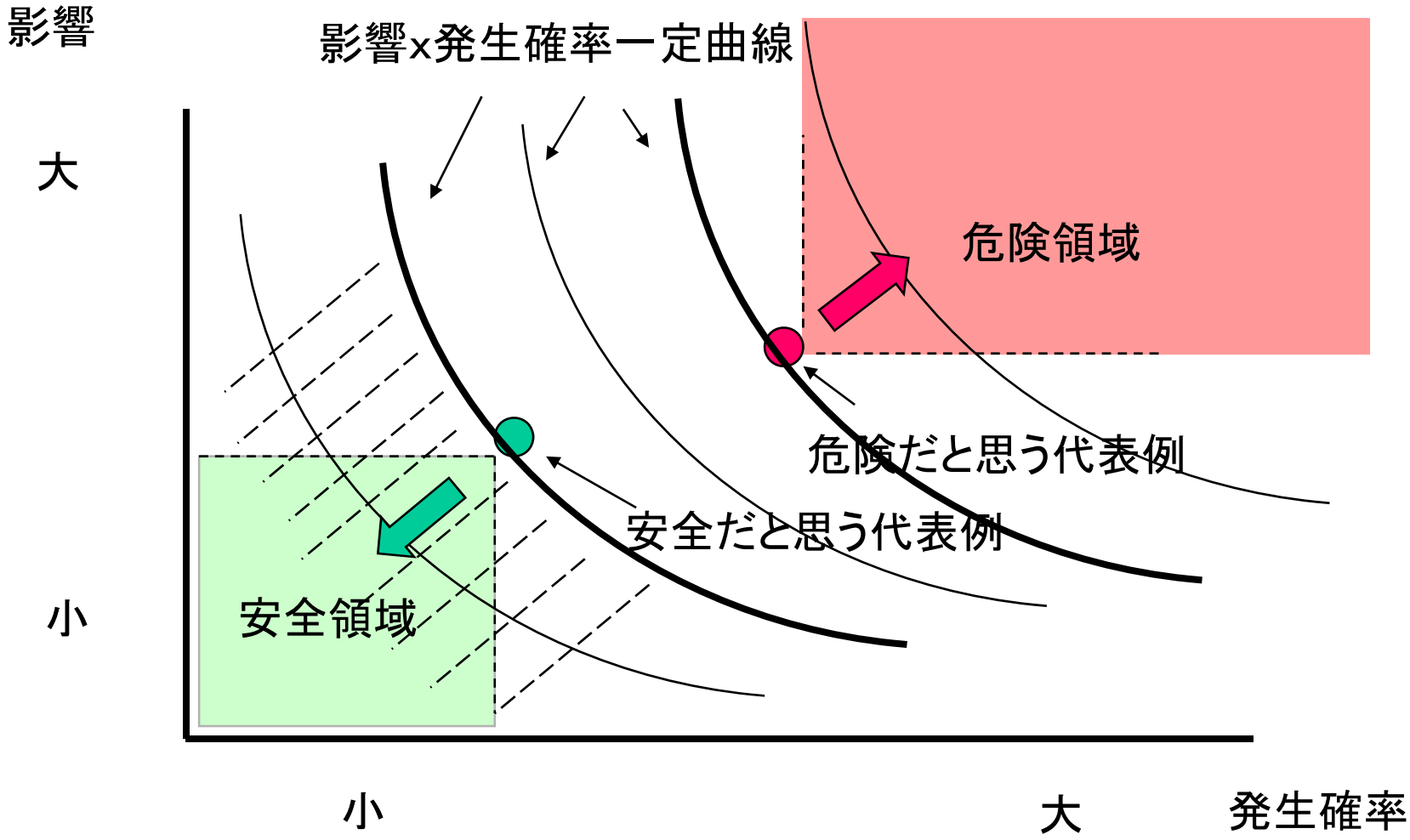


図5．12　リスクへの対応法