第1回（平成25年度第1回）CRCフォーラム（平成25年7月4日（木）開催）
「ITシステムの利用者に安全安心をもたらすための研究開発」

ITシステムを取り巻く安全上の課題とITリスク学の提案

佐々木　良一　教授
未来科学部情報メディア学科

TDU
東京電機大学

ITシステムを取り巻く安全上の課題とITリスク学の提案

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

サイバー攻撃の激化

47NEWS ＞ 共同ニュース ＞ 記事詳細

ニュース詳細 | 東日本大震災 | 47トピックス | コラム「日めくり」

+1 26 ツイート 255 いいね！ 232 コメント B! チェック

韓国で放送局、銀行ネットダウン　サイバー攻撃か、ハッキング確認

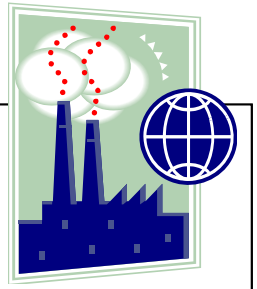
【ソウル共同】聯合ニュースによると、韓国のＫＢＳテレビとＭＢＣテレビ、ＹＴＮテレビの３放送局や新韓銀行、農協銀行など複数の金融機関の社内イントラネットなどが２０日午後、一斉にダウンした。政府機関の放送通信委員会は会見で「ハッキングによる不正プログラムの流布が確認された」と明らかにした。

警察はサイバーテロの可能性があるとみて調べている。

社内のパソコンが一斉にダウンした韓国のＫＢＳテレビ本社＝２０日午後、ソウル（聯合＝共同）

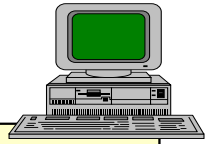
社会のITシステムへの依存

経済活動



国民生活

＜重要インフラ（Critical Infrastructure）＞
情報通信、金融、航空、鉄道、電力、ガス、
政府・行政サービス、医療、水道、物流 など



＜ITシステム＞
重要情報インフラ（Critical Information Infrastructure）

社会全体のITシステムへの依存増大

ITシステムの安全の問題が重要に

ITリスク問題が重要になった背景

社会全体のITシステムへの依存の増大によりITシステムの安全が重要に

従来よりも広い範囲のアプローチが必要に

故意の不正

天災・故障・
ヒューマンエラー

①ITシステムの扱う情報の安全

②ITシステムそのものの安全
③ITシステムが行うサービスの安全

Security

Privacy・Reliability
Safety・Usability等

工学的アプローチ

心理学的・社会科学的アプローチ

新しいアプローチ法の名称例

①トラスト
②ニューディペンダビリティ　など

採用した名称

ITリスク（学）
＜確率論的扱いが不可欠＞

ITリスク問題の統一的扱いが必要な理由の例

システムの信頼性をあげるためにデータを2重化して保持

2重化に伴う攻撃箇所の増加によるセキュリティの低下

ITリスク問題が重要になった背景

社会全体のITシステムへの依存の増大によりITシステムの安全が重要に

従来よりも広い範囲のアプローチが必要に

故意の不正

天災・故障・
ヒューマンエラー

①ITシステムの扱う情報の安全

②ITシステムそのものの安全

③ITシステムが行うサービスの安全

Security

Privacy・Reliability
Safety・Usability等

工学的アプローチ

心理学的・社会科学的アプローチ

新しいアプローチ法の名称例

①トラスト
②ニューディペンダビリティ　など

採用した名称

ITリスク（学）
＜確率論的扱いが不可欠＞

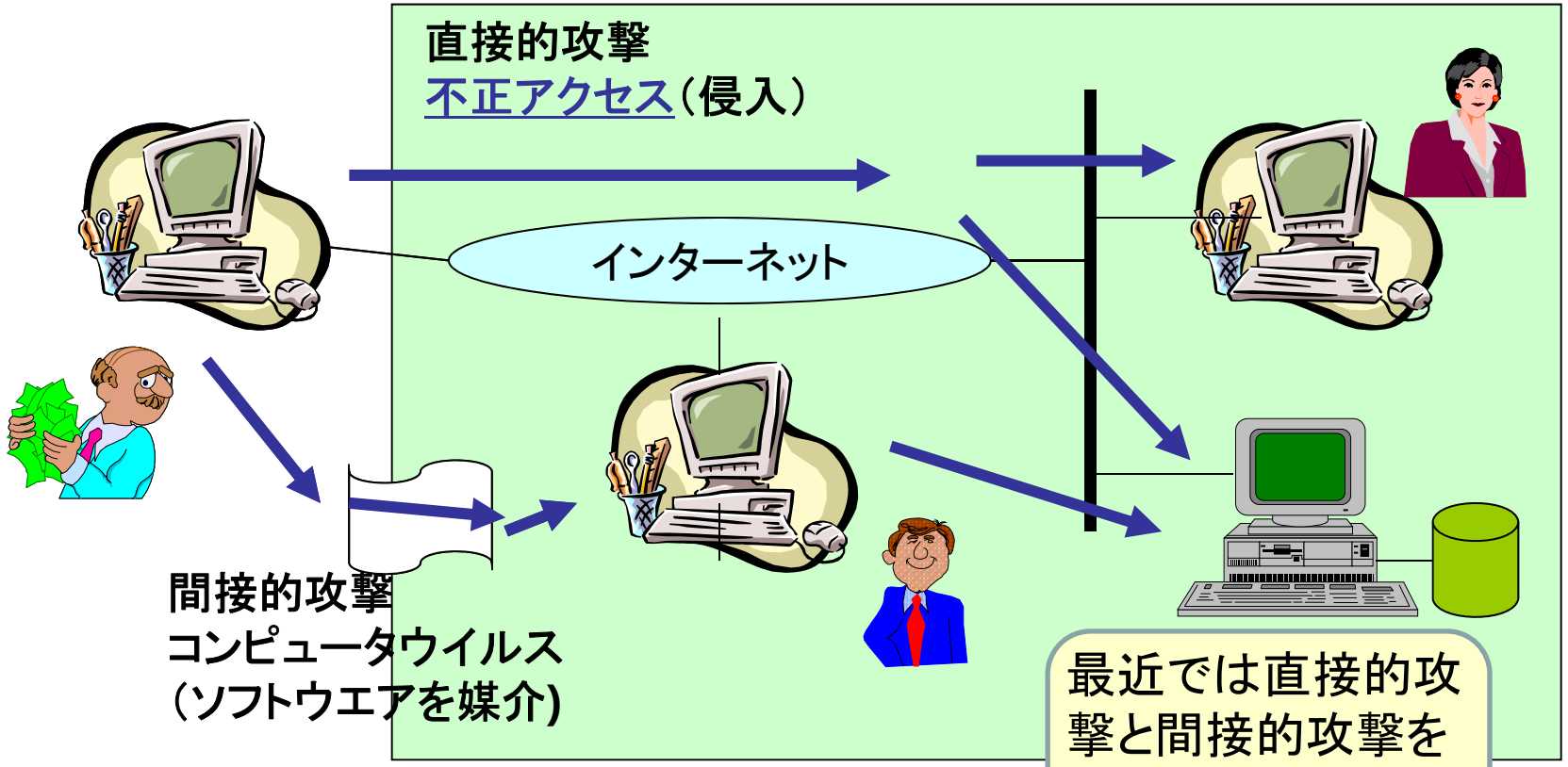
ITシステムの安全の階層化

階層	対象	扱う事故・障害	従来の学問・技術分野	指標
3	ITシステムが行うサービスの安全	発券サービスの停止、プライバシーの喪失など	システム工学 リスク学 社会科学など	プライバシー、ユーザビリティ
2	ITシステムが扱う情報の安全	情報のCIAの喪失	セキュリティ	セキュリティ（機密性、完全性、可用性）
1	ITシステムそのものの安全	コンピュータや通信機器の故障	信頼性工学 セキュリティ	リライアビリティ、アベイラビリティ

＊

＊　従来情報セキュリティが扱っていた範囲

インターネット社会の脅威



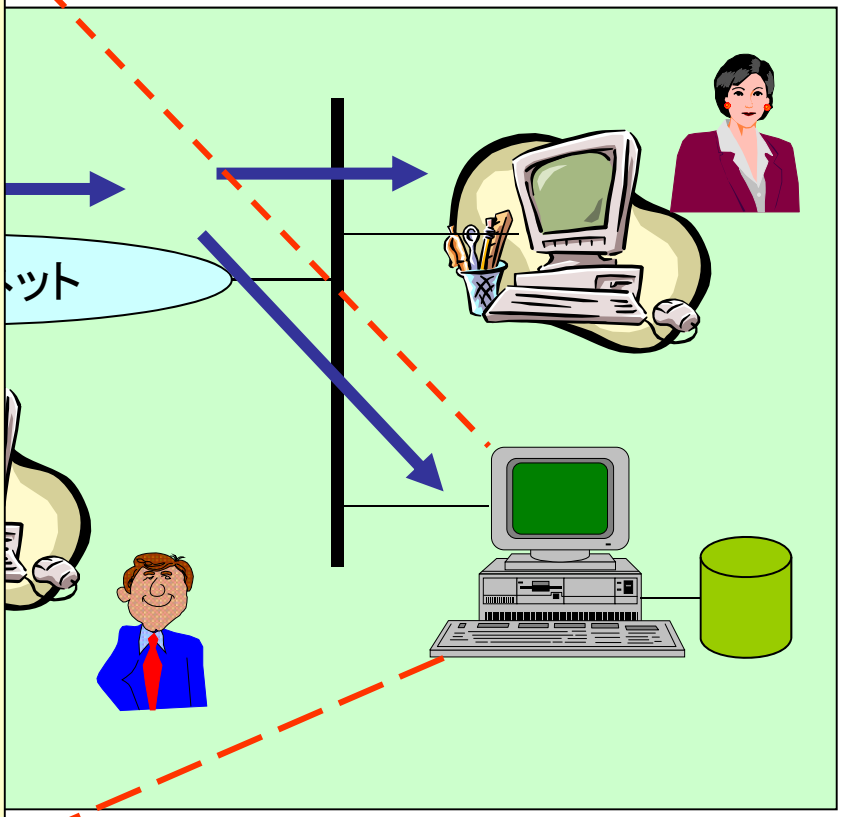
インターネット社会の脅威

脅威の分類(情報のCIA)

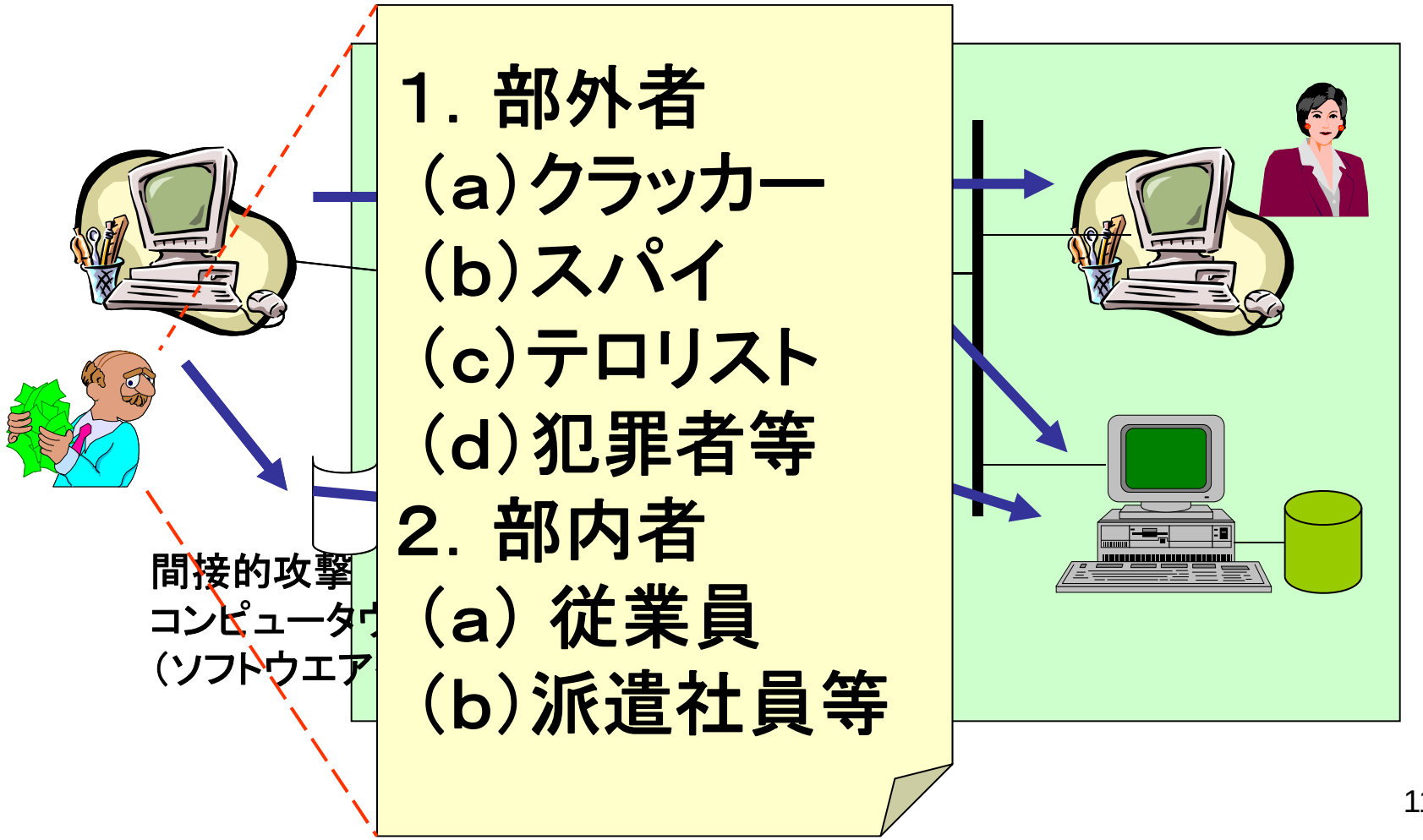
(1)機密性(Confidentiality)の喪失:情報を不当に見られる

(2)完全性(Integrity)の喪失:情報を不当に破壊、改ざんされる

(3)可用性(Availability)の喪失:不当な利用によりデータやコンピュータパワーが使えなくなる



インターネット社会の脅威



ITリスク問題が重要になった背景

社会全体のITシステムへの依存の増大によりITシステムの安全が重要に

従来よりも広い範囲のアプローチが必要に

故意の不正

天災・故障・
ヒューマンエラー

①ITシステムの扱う情報の安全

②ITシステムそのものの安全
③ITシステムが行うサービスの安全

Security

Privacy・Reliability
Safety・Usability等

工学的アプローチ

心理学的・社会科学的アプローチ

新しいアプローチ法の名称例

①トラスト
②ニューディペンダビリティ　など

採用した名称

ITリスク（学）
＜確率論的扱いが不可欠＞

目次

リスクとは

1．リスク とは，英語のRiskの訳であり，危険と訳される場合もある．「**将来の帰結に対する現在における予測**」という見方が下敷きになっていて常に**不確実性**を伴う。

2．工学分野の確率論的リスク評価では通常次のように定義することが多い。

リスク＝損害の大きさ　×損害の発生確率

3．「ISO/IEC 27005：2008」ではITのリスクを以下のように定義しているが、結局同じことを表している。

リスク＝資産価値 × 脅威 × 脆弱性

（注）英語のRiskが登場するのは1660年代。ハザードや災いを意味するイタリア語risicoからの転用

リスク社会

ドイツの社会学者ウルリヒ・ベック
「かつて人類は地震などの自然災害や病気などを恐れていたが，現在ではそれらのリスクをコントロールするために開発した科学技術そのものが新たなリスクとして問題になってきている．」と指摘．
「このような新たなリスクに覆われた社会を「リスク社会（翻訳では危険社会）」」と呼んだ．

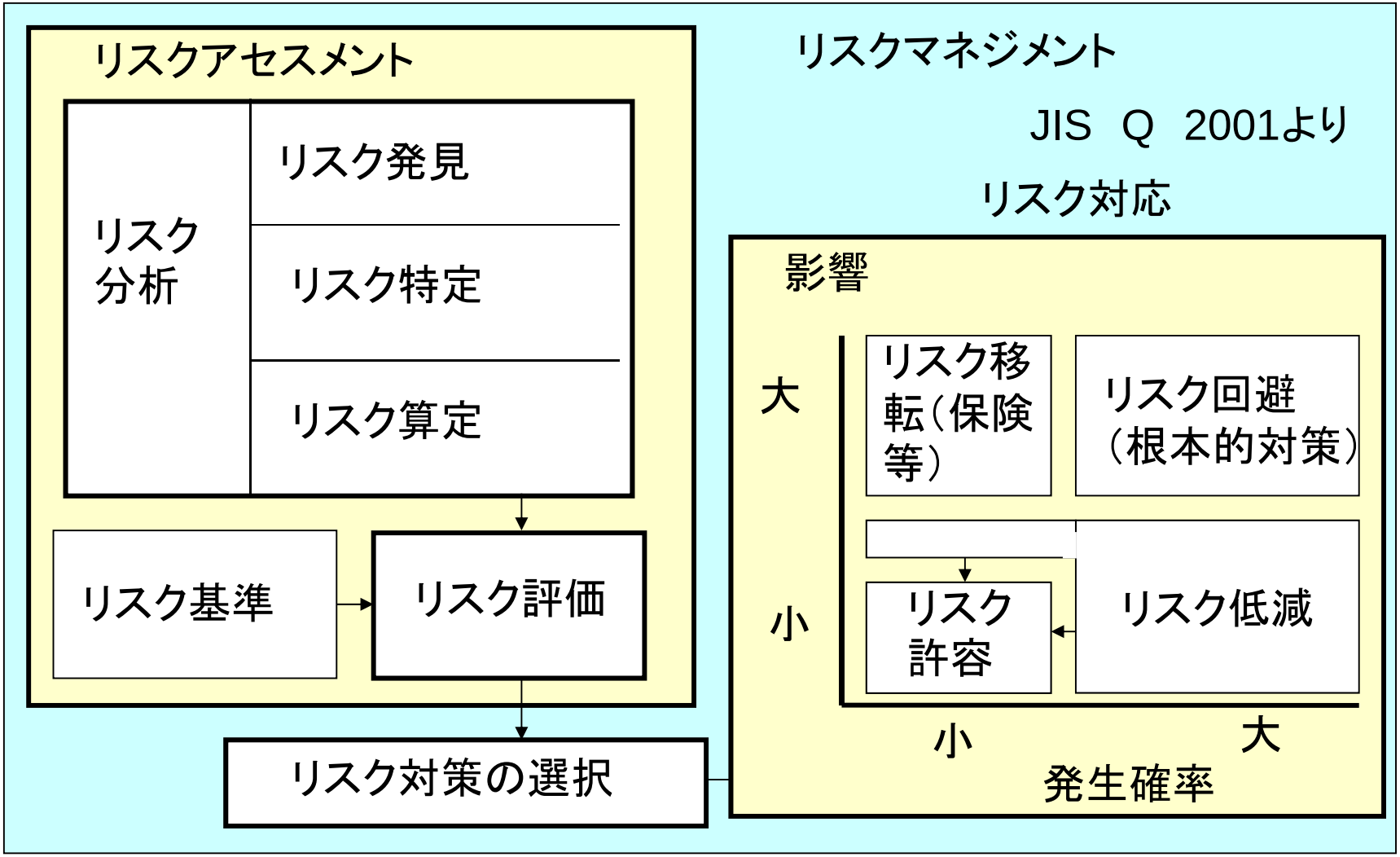
ウルリヒ・ベック（東廉／伊藤美登里訳）「危険社会　新しい近代への道」法政大学出版局，1998年

リスクははたして制御可能か

三上剛史は，原発や新型インフルエンザなどの新しいリスクが損害の深刻さ，補償不可能性ゆえに損失を最小限に抑え保障するというアプローチではなく，
潜在的リスクを洗い出し，あらかじめ排除する「警戒」型アプローチが必要となるという．
そして，その「警戒」の行為ゆえにリスクと向かいあわざるを得ず，リスク恐怖症を招きがちであり，さらにそれが監視社会を作り出すと指摘する．

私たちへの問いかけ：**リスクは果たして制御可能か？**

リスク分析・リスク評価とリスク対応



誤ったリスク認識の例

2001年の９．１１後、飛行機が危険という認識から１年間自動車の利用者が増えた。

それによって1年間で米国で1595人の自動車事故の死亡者が増加（これは９．１１の不幸なフライトの総死亡者の約6倍）

ベルリンのマックス・ブランク研究所の心理学者ゲルド・ギレンザーの調査結果

ダン・ガードナー「リスクにあなたは騙される」早川書房、2009、p11

犯罪の発生頻度推定

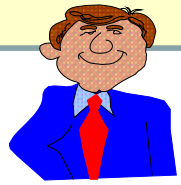
1年間で警察に届けられている強盗の件数はおよそ6千件です。

（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）

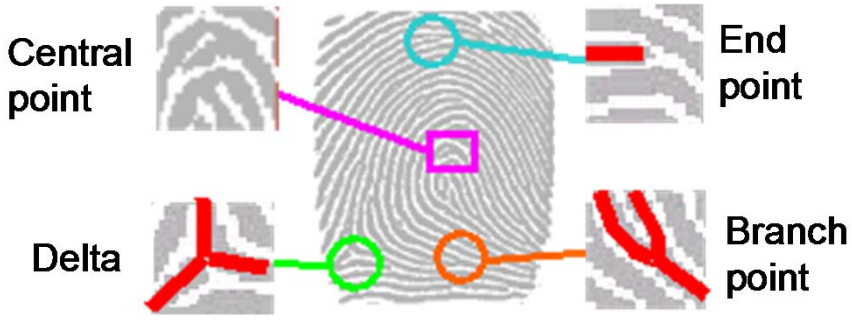
（4）薬物常用者による殺人 （　　件／年）



どちらが安全か

1．パスワードが合致した場合本人だと認める個人認証システム

2．指紋かパスワードかのいずれかが一致した場合、本人だと認める個人認証システム



日本人のリスク感の特徴

＜特徴＞

①リスクに極めて敏感でゼロリスクを求める傾向

②安全よりも安心を重視する傾向

③リスクに対しあきらめてしまう傾向

①②と③は矛盾するがこのようなリスク感を形成する要因として、日本人は不可実性を回避する傾向が高い、現状肯定的心情があるとしている。

奈良由美子「生活とリスク」放送大学教育振興会、2007 （林ほか「セキュリティ経営」勁草書房、2011より）

私たちの基本スタンス

リスク社会学者などが指摘するようにリスクを制御するのは限りなく難しい。

しかし、そこにリスクがある以上、当事者は万全の注意を払ってリスクに対応し続けるしかないと思う。

そのためITリスクに応じてどう対応すべきかを明確化していく。

目次

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）「リスク対リスク」「多重リスク」への考慮が不可欠である.

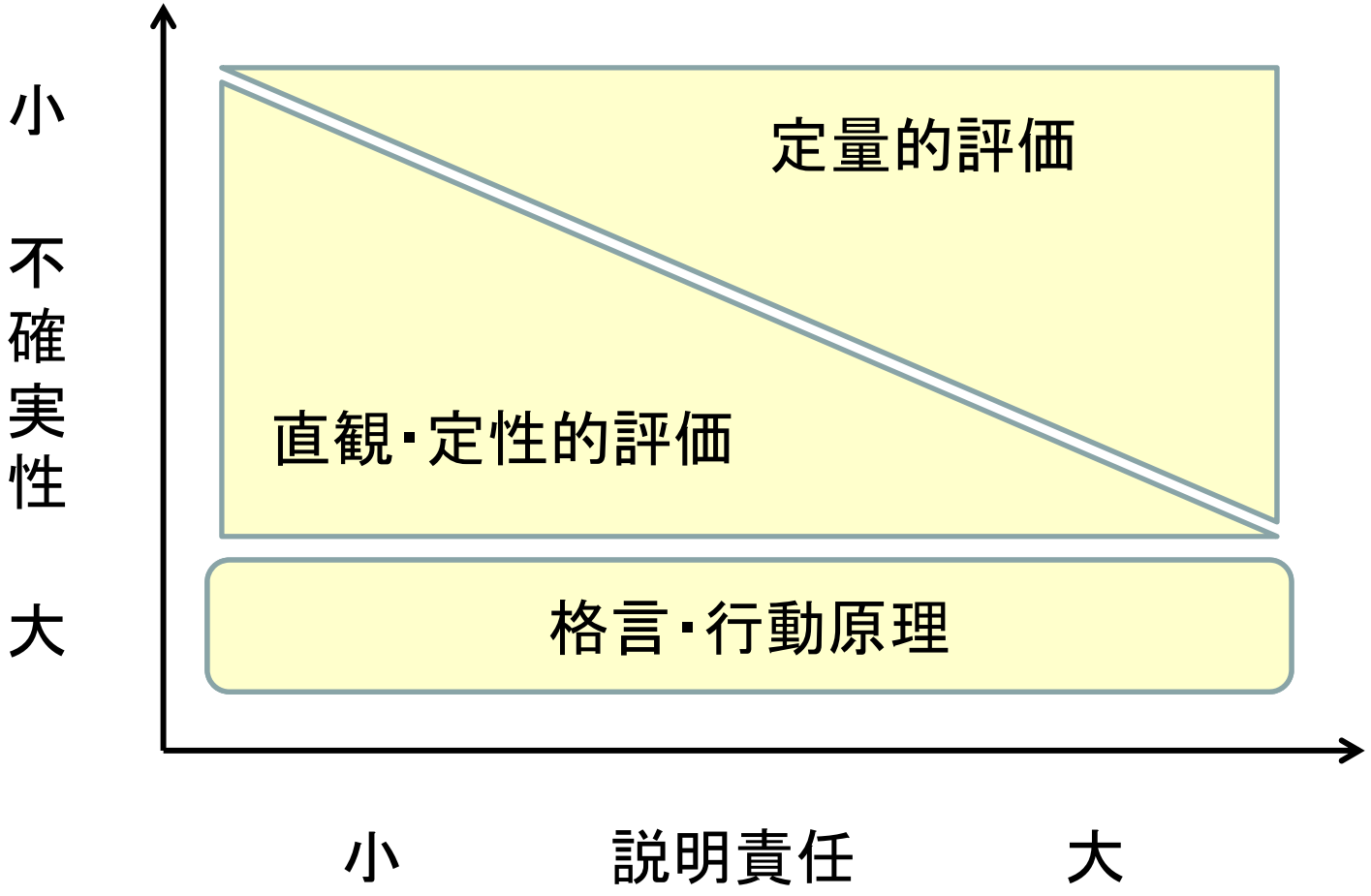
（4）多くの関与者とのリスクコミュニケーションが大切である.

＜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）動的リスクへの対応が必要である.

ITリスクの対応法



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）「リスク対リスク」「多重リスク」への考慮が不可欠である.

（4）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）動的リスクへの対応が必要である.

リスクvsリスクの時代（その１）

（１） エネルギー問題解決のためのバイオエタノールの利用が食糧問題に

（２） ９．１１後のテロ対策とプライバシー・人権問題

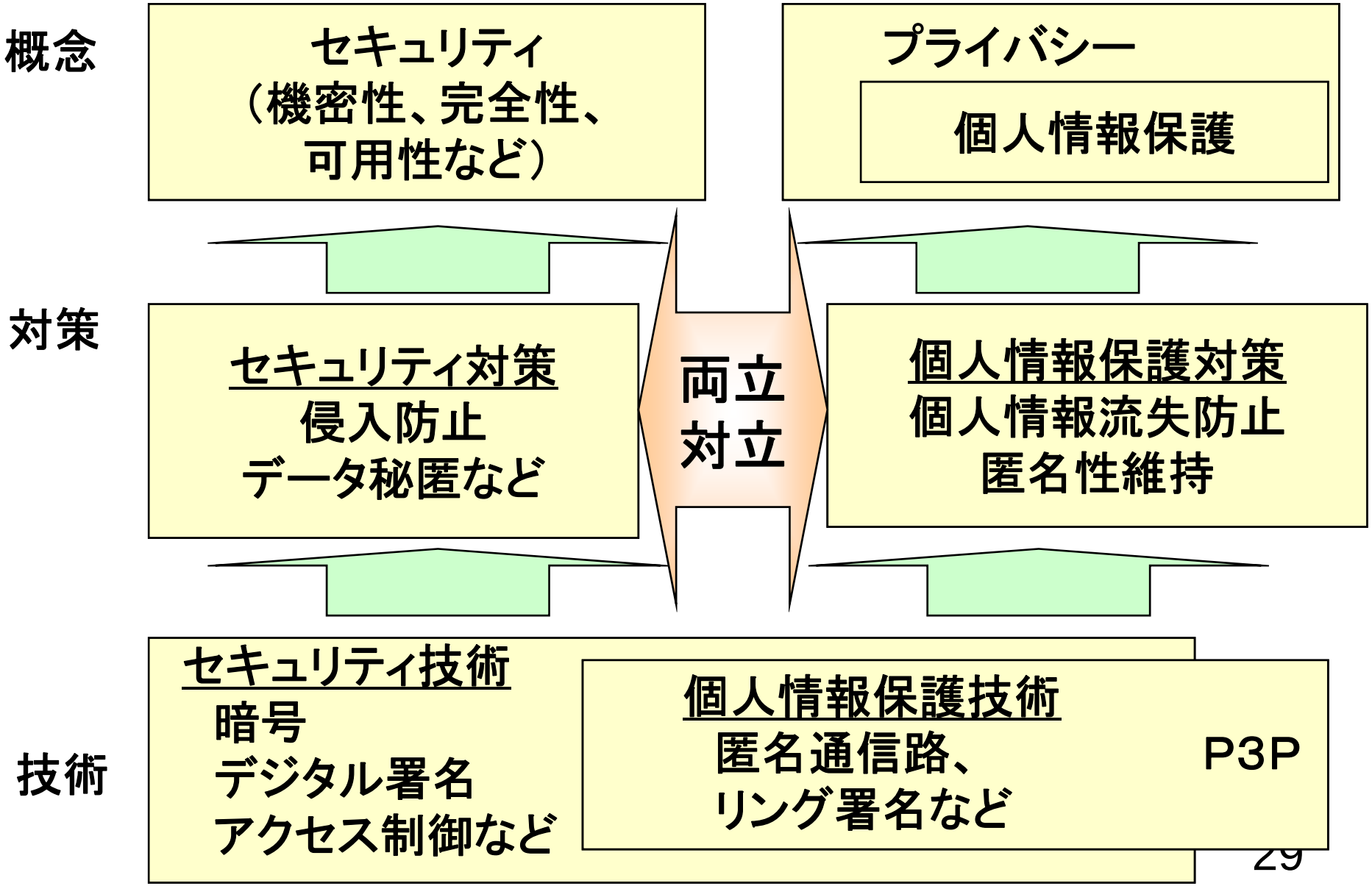
ブルース・シュナイアーの考え

「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、

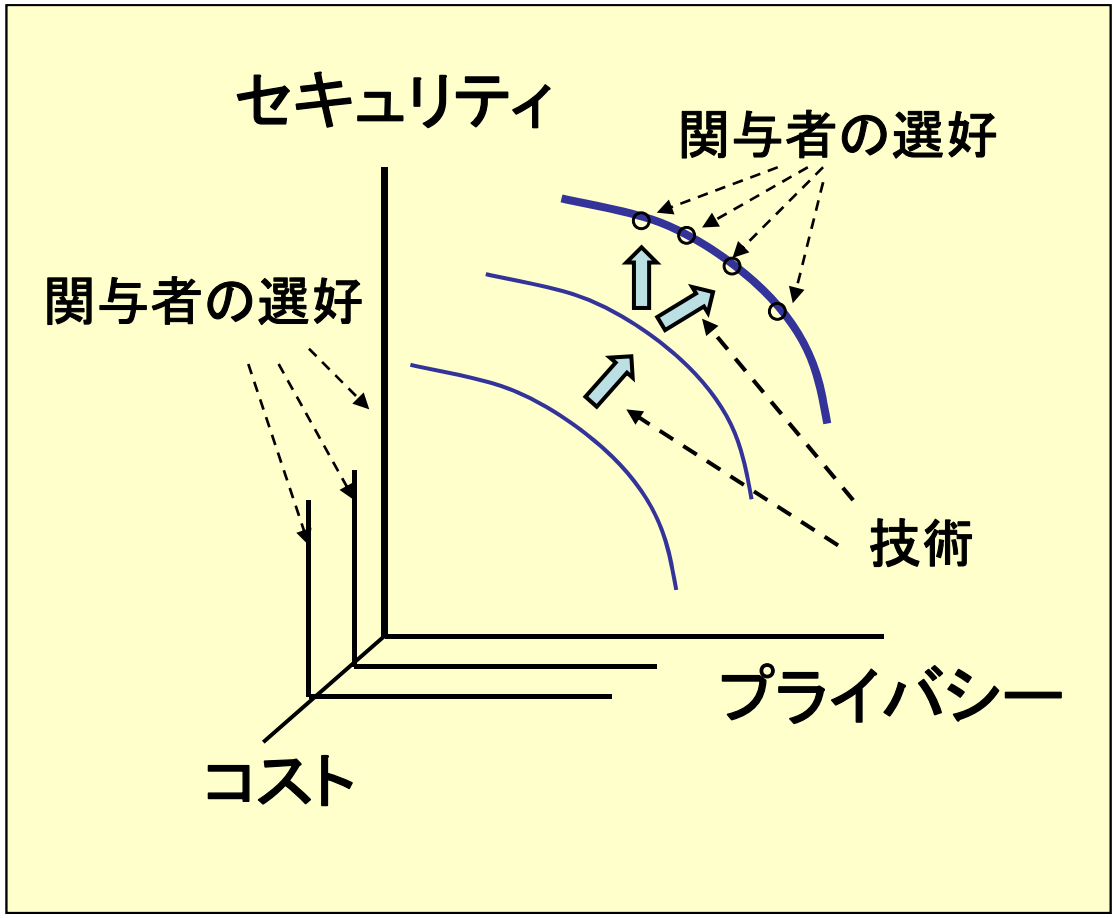
その対策によって生じる新たなリスクとテロのリスクとの間で真剣な比較検討が必要であり、バランスを欠いた対策は、プライバシーや人権の問題を引き起こす。」

「リスク対リスク」 あるいは「多重リスク」 の時代に

IT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）

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）「リスク対リスク」「多重リスク」への考慮が不可欠である.

（4）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）動的リスクへの対応が必要である.

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が必要になった背景

＜リスク対応の困難性＞

（1）人はリスクの存在そのものを認識できないのではないか.

（2）リスクの存在を認識できたとしてもフランク・ナイトが指摘するようにその事象の発生確率は測定できない場合が多い.

（3）事象の発生確率やその損害の大きさを推定できたとしてもそれらの値そのものに不確実性が残る.

（a）人はリスクに直面し判断せざるを得ない場合は少なくないが人知を超える判断はいずれにしろできない。

①従って、人知を集める手段としてのリスクコミュニケーションが大切に（リスクコミュニケーションベースアプローチ）

（b）ナシーム・タレブが指摘するようにすべての確率は主観確率。よって、各人の主観を明確にしそれらのあいだの合意形成を図るしかない

ITリスクコミュニケーション対象の分類

	ITに関するリスクコミュニケーション例			支援システム	他分野のリスクコミュニケーションの例
	ITシステム自体	ITシステムが扱う情報	ITシステムが行うサービス		
目的①個人的選択	自己PCのセキュリティホール対策	SNSにおける自己情報の秘匿対策	ネットショッピングのリテラシー	E-Learning支援ツールELSEC	禁煙の実施 インフルエンザワクチン接種
目的②組織内合意	BCPのためのITのバックアップ対策	オフィスにおける個人情報漏洩対策	ネットショッピング対象の品質維持対策	多重リスクコミュニケータMRC	工場の環境対策 オフィスの省エネ対策
目的③社会的合意	ウイルス作成罪の可否	情報フィルタリングの可否	薬のネット販売の可否	社会的合意形成支援システムSocial-MRC	原発再稼働の可否 BSE対策のための全頭検査

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）「リスク対リスク」「多重リスク」への考慮が不可欠である.

（4）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）動的リスクへの対応が必要である.

ITリスクに多くの対策が必要になる理由

① ITシステムはソフトウェアにより多様な機能を実現されているため，障害時の影響も多様である．

② ITリスクには意図的な不正も含むため，不正の高度化により，脅威がどんどん大きくなり，対応が難しくなっていく．

したがって，1つの対策だけで防止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．

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）「リスク対リスク」「多重リスク」への考慮が不可欠である.

（4）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）動的リスクへの対応が必要である.

ITシステムにおける動的リスク

ITリスクには意図的な不正も含むため，防御側の対策や状況の変化により攻撃方法が動的に変化する

したがって，動的なリスク対応が必要

今後の重要な研究課題

目次

ITリスク学の確立に向けての活動

① 2008年5月に日本セキュリティ・マネジメント学会の中に「ITリスク学」研究会を立ち上げ
② ITリスク学の定義
③ ITリスク学の全体像と構成要素の明確化
④ 構成要素の概要と研究課題の明確化
⑤ 研究課題の解決に向けての活動
⑥ 本の出版（2013年2月）

ITリスク学の確立に向けての活動

① 2008年5月に日本セキュリティ・マネジメント学会の中に「ITリスク学」研究会を立ち上げ
② ITリスク学の定義
③ ITリスク学の全体像と構成要素の明確化
④ 構成要素の概要と研究課題の明確化
⑤ 研究課題の解決に向けての活動
⑥ 本の出版（2013年2月）

ITリスク学の確立に向けての活動

① 2008年5月に日本セキュリティ・マネジメント学会の中に「ITリスク学」研究会を立ち上げ

② ITリスク学の定義

③ ITリスク学の全体像と構成要素の明確化

④ 構成要素の概要と研究課題の明確化

⑤ 研究課題の解決に向けての活動

⑥ 本の出版（2013年2月）

学問分野誕生の2つのタイプ

（1）分離独立型：ある学問分野の一部が大きくなって独立する場合．たとえば物理学の中から素粒子物理学が誕生するような場合である．情報セキュリティと情報セキュリティ会計学の関係もここに属する．

（2）統合・融合型：個別の学問分野の成果を統合的に扱うことにより個別のアプローチでは解決できなかったものの解決を図ろうとするものである．たとえば，脳生理学，心理学，精神医学，病蹟学，人工知能学などを脳科学として統合した例がある．

ITリスク学を取り巻く環境

（1）リスクそのものに関する研究は国内外で広く行われている。

（2）しかし、ITリスクに関する研究は少なく，それをITリスク学として確立しようという試みは海外にもなかった。

（3）そのため，海外の類似のアプローチを調査し，それを日本に適合するようにしていくというアプローチができず独自に確立していく必要があった。

ITリスク学の定義

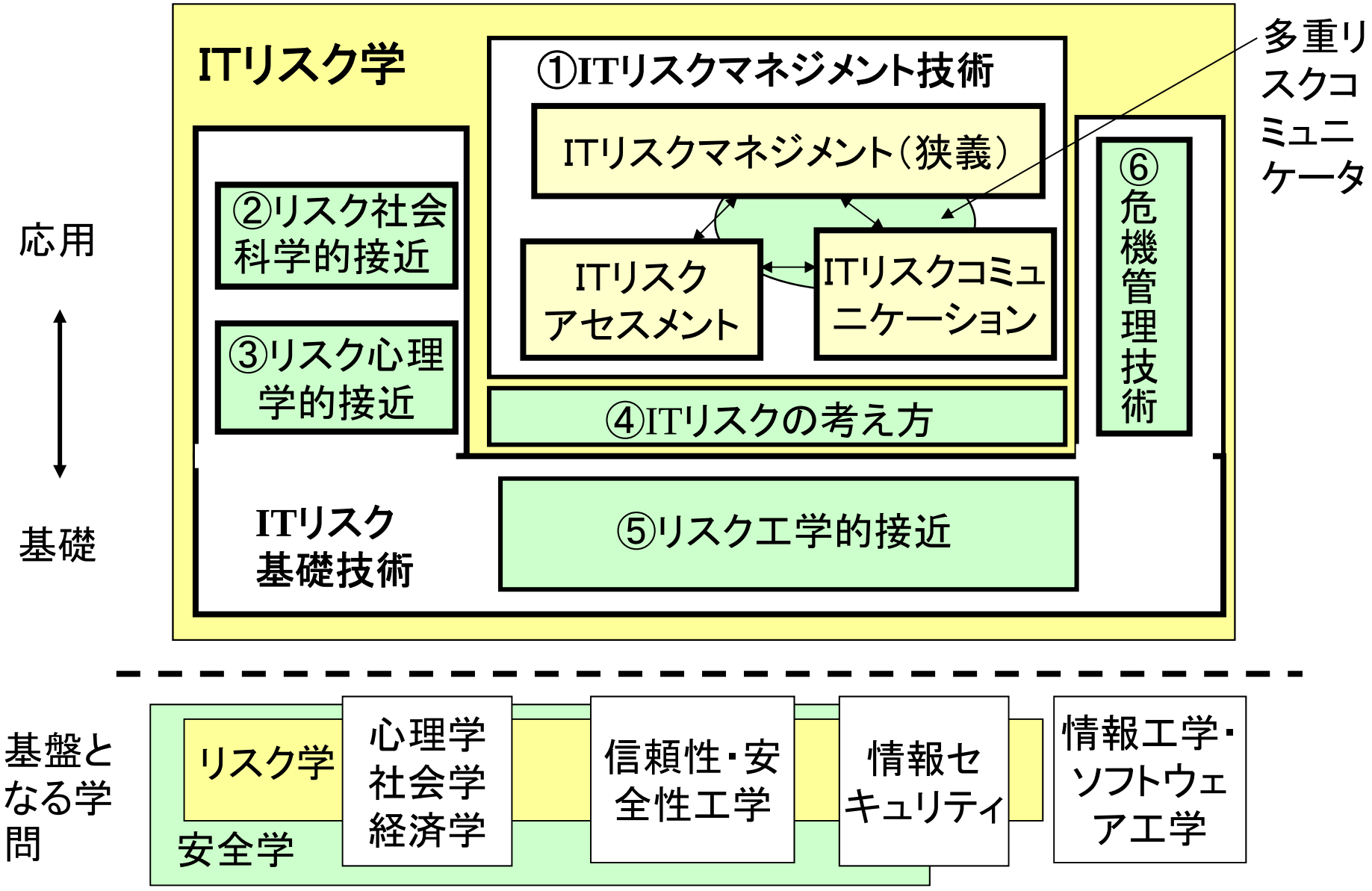
「不正によるものだけでなく，天災や故障ならびにヒューマンエラーによって生ずるITシステムのリスクならびにITシステムが扱う情報やサービスに関連して発生するリスクを，リスク対策の不確実性や，リスク対リスクの対立，関与者間の対立などを考慮しつつ学際的に対処していくための手段に関する学問」

（注1）ITシステムのサービスに関するリスクを含むので、セキュリティだけでなく，プライバシーユーザビリティなども含む
（注2）一般的に扱うとあまりにも広くなるので，ITリスクの特徴である「リスク対リスクの対立，関与者間の対立を考慮しつつ」を入れることにより研究範囲を明確にした
（注3）「制御する」ではなく「対処していく」にしたのはリスクの完全な制御は不可能であるとの認識に基づく
（注4）「手段に関する学問」としたが，手段を考える上での前提となるとなる周辺の学問も含むものとする

ITリスク学の確立に向けての活動

① 2008年5月に日本セキュリティ・マネジメント学会の中に「ITリスク学」研究会を立ち上げ
② ITリスク学の定義
③ ITリスク学の全体像と構成要素の明確化
④ 構成要素の概要と研究課題の明確化
⑤ 研究課題の解決に向けての活動
⑥ 本の出版（2013年1月）

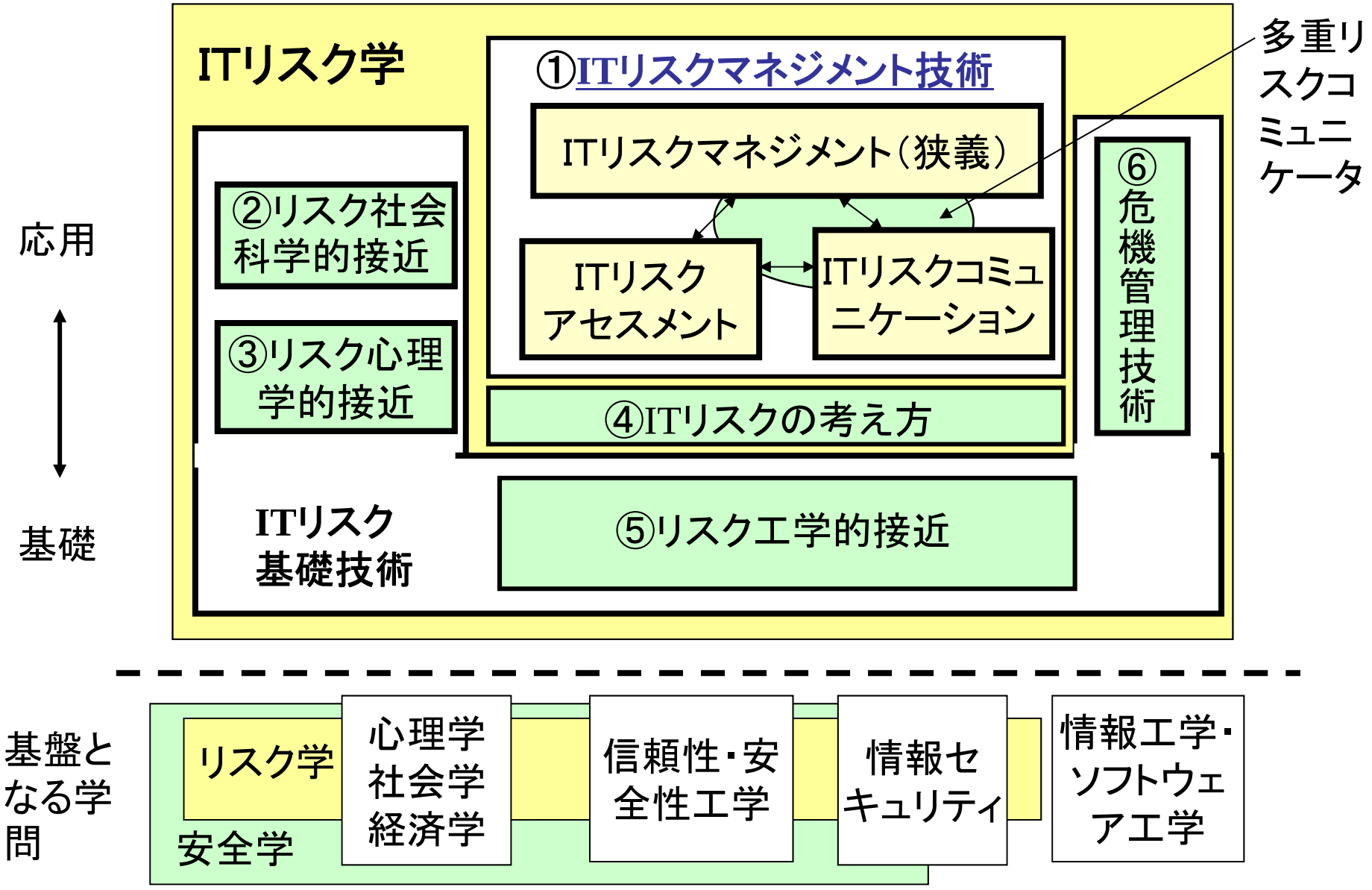
ITリスク学の構成（Version3）



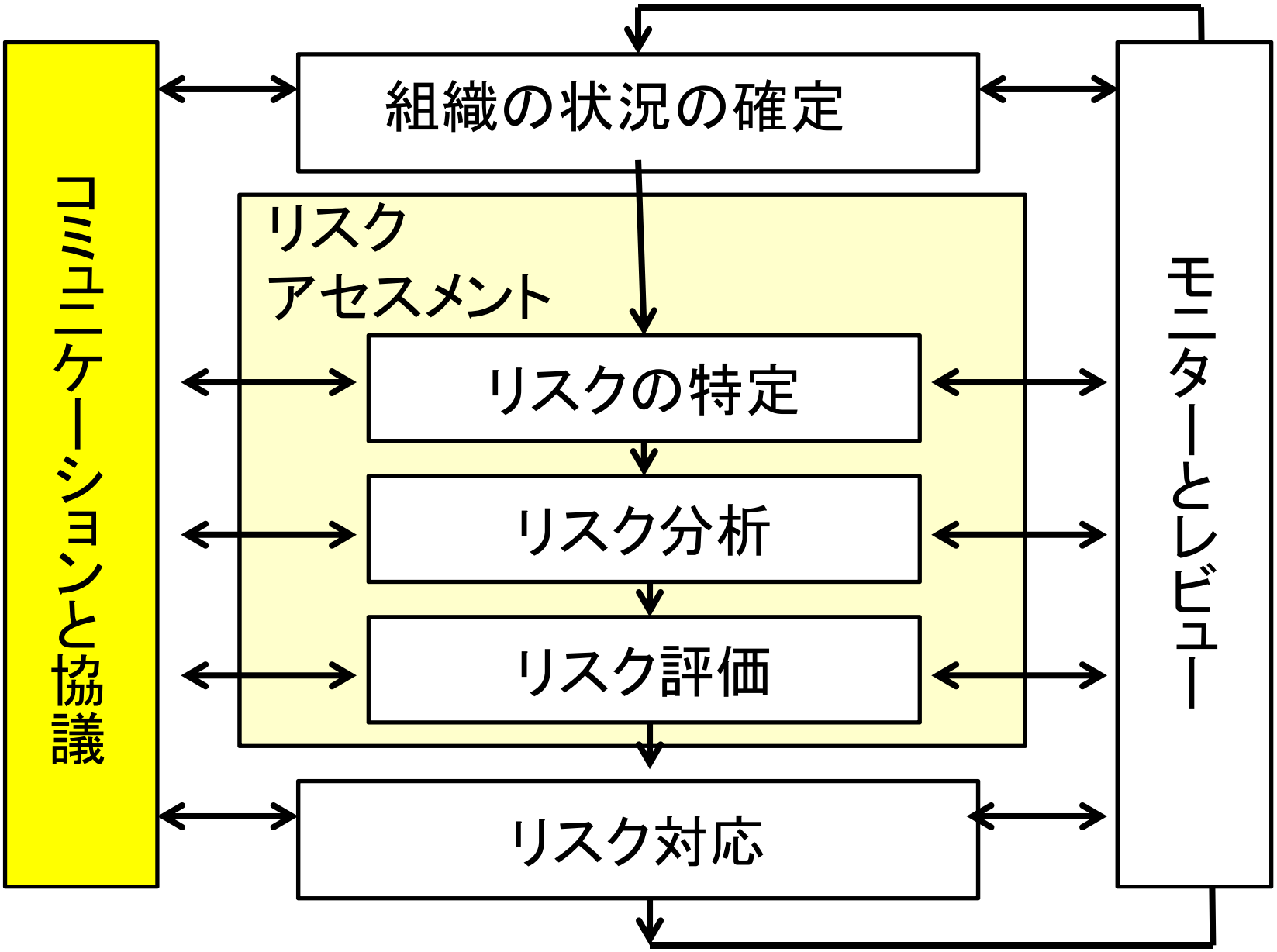
ITリスク学の確立に向けての活動

① 2008年5月に日本セキュリティ・マネジメント学会の中に「ITリスク学」研究会を立ち上げ
② ITリスク学の定義
③ ITリスク学の全体像と構成要素の明確化
④ 構成要素の概要と研究課題の明確化
⑤ 研究課題の解決に向けての活動
⑥ 本の出版（2013年2月）

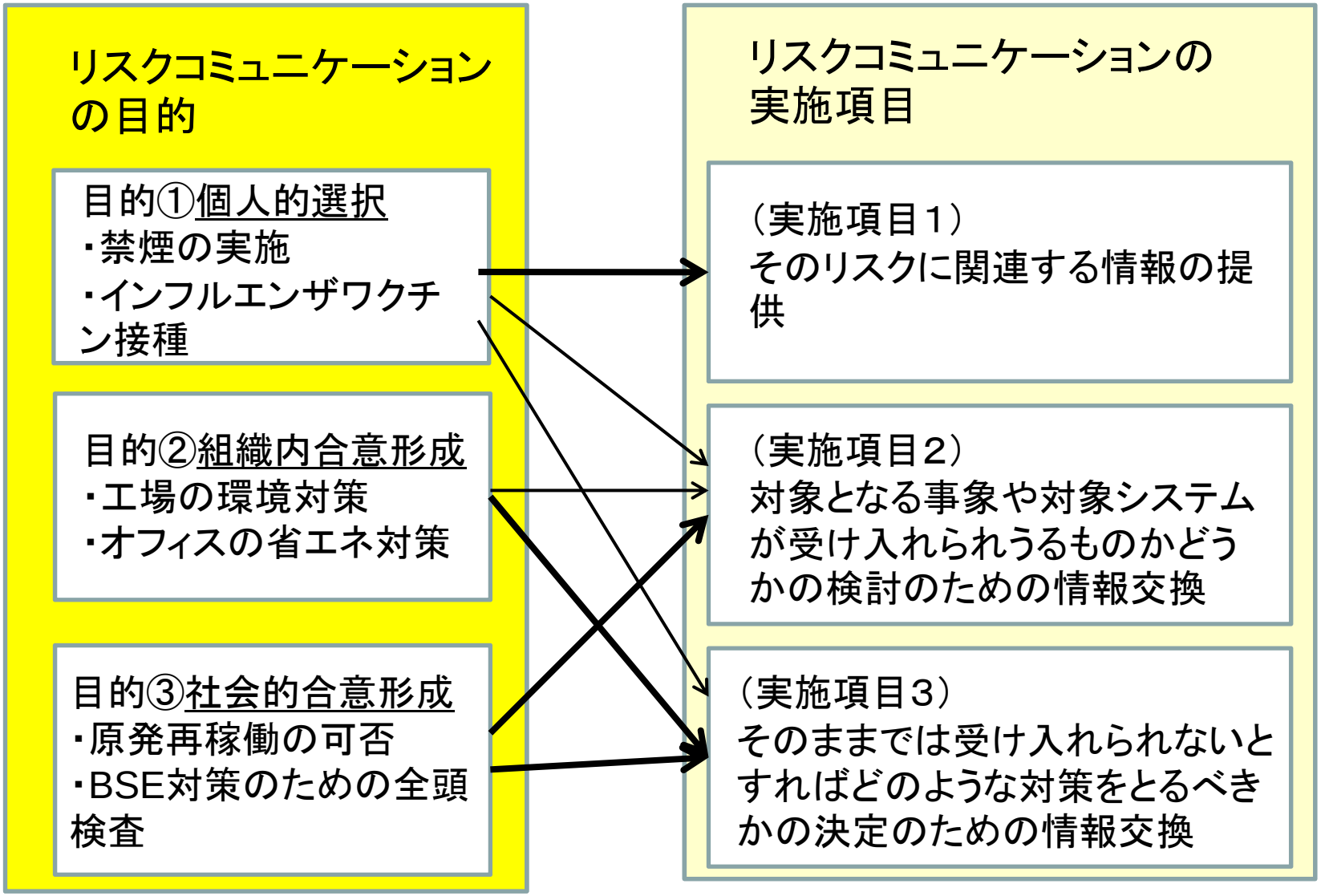
ITリスク学の構成（Version3）



リスクマネジメントのプロセスの流れ



リスクコミュニケーションの目的と主要実施項目



ITリスクコミュニケーション対象の分類

	ITに関するリスクコミュニケーション例			支援システム	他分野のリスクコミュニケーションの例
	ITシステム自体	ITシステムが扱う情報	ITシステムが行うサービス		
目的①個人的選択	自己PCのセキュリティホール対策	SNSにおける自己情報の秘匿対策	ネットショッピングのリテラシー	E-Learning支援ツールELSEC	禁煙の実施 インフルエンザワクチン接種
目的②組織内合意	BCPのためのITのバックアップ対策	オフィスにおける個人情報漏洩対策	ネットショッピング対象の品質維持対策	多重リスクコミュニケータMRC	工場の環境対策 オフィスの省エネ対策
目的③社会的合意	ウイルス作成罪の可否	情報フィルタリングの可否	薬のネット販売の可否	社会的合意形成支援システムSocial-MRC	原発再稼働の可否 BSE対策のための全頭検査

多重リスクコミュニケータ（MRC）の対応

＜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

背景2．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

背景3．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

MRCにおける対応

①多くのリスクやコストを制約条件とする組み合わせ最適化問題として定式化

②関与者の合意が得られるまでパラメータの値や制約条件値を変えつつ最適化エンジンを用い求解

専門家

対策案
①②③④

定式化結果

多重リスクコミュニケータ MRC

最適解
対策案
①③の組合せ

満足

Y

END

N

制約条件などの変更

ファシリテータ　関与者

MRCの適用

①適用対象
（a）個人情報漏洩対策（含む：世田谷区役所の個人情報漏洩対策への実適用など）
（b）内部統制問題など
＝＞参加者が5-6人までなら基本的有効性を確認

②受賞
（a）日本セキュリティ・マネジメント学会2009年度論文賞受賞
（b）情報処理学会DICOMO2010最優秀論文賞受賞
（c） IEEEのCFSE2012での招待講演

詳しくは佐々木良一他「多重リスクコミュニケータの開発と適用」情報処理学会論文誌、Vol49,No9、2008年9月号

新たなニーズ

社会的合意形成が必要な問題の存在

関与者の数が

数千人を超える社会的合意形成の問題

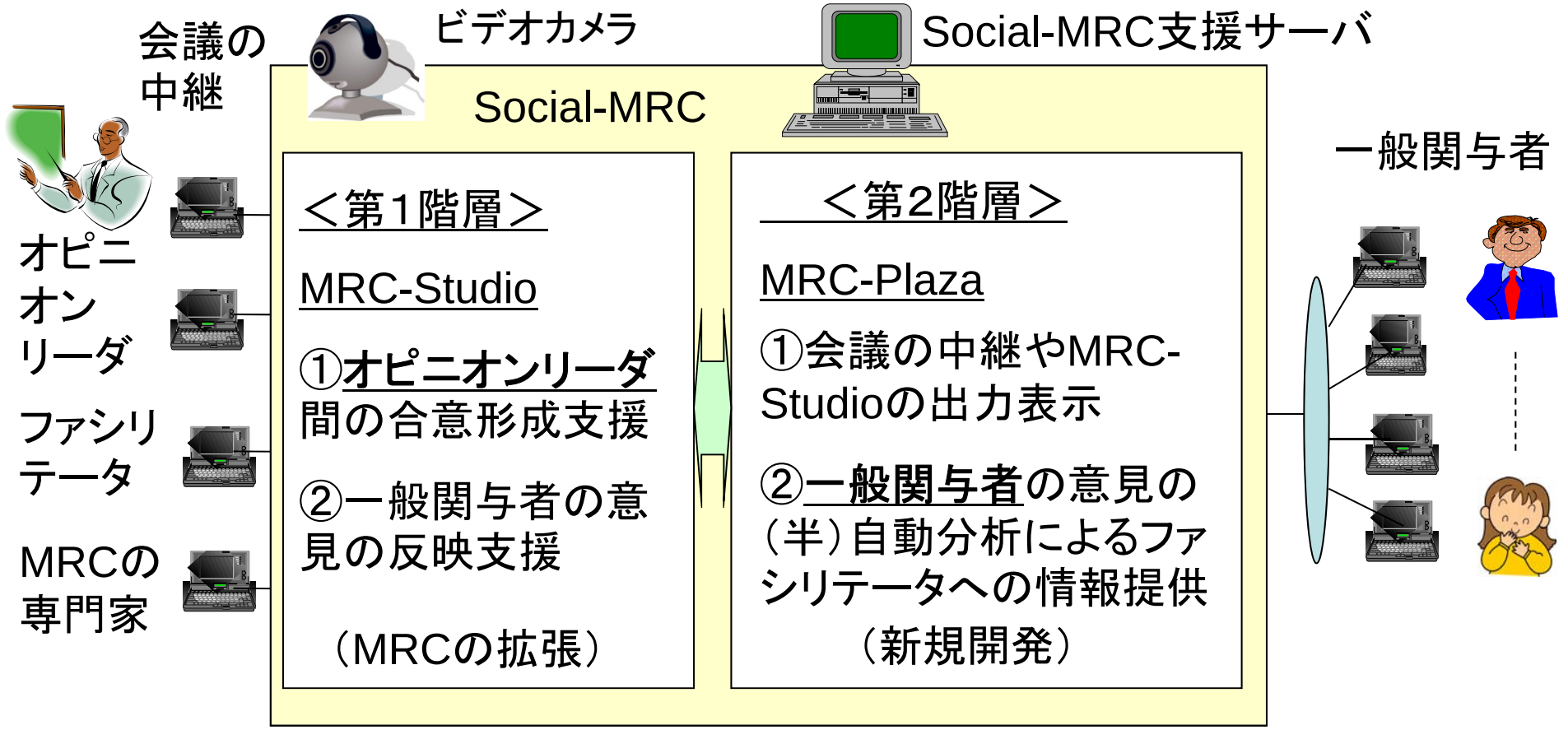
(情報フィルタリング問題など)

に適用する必要

ITリスクコミュニケーション対象の分類

	ITに関するリスクコミュニケーション例			支援システム	他分野のリスクコミュニケーションの例
	ITシステム自体	ITシステムが扱う情報	ITシステムが行うサービス		
目的①個人的選択	自己PCのセキュリティホール対策	SNSにおける自己情報の秘匿対策	ネットショッピングのリテラシー	E-Learning支援ツールELSEC	禁煙の実施 インフルエンザワクチン接種
目的②組織内合意	BCPのためのITのバックアップ対策	オフィスにおける個人情報漏洩対策	ネットショッピング対象の品質維持対策	多重リスクコミュニケータMRC	工場の環境対策 オフィスの省エネ対策
目的③社会的合意	ウイルス作成罪の可否	情報フィルタリングの可否	薬のネット販売の可否	社会的合意形成支援システムSocial-MRC	原発再稼働の可否 BSE対策のための全頭検査

Social-MRCの概要



対象問題	青少年のための情報フィルタリング 国民ID問題、監視カメラの設置問題など
利用場面	WEB利用公聴会、コンセンサス会議、テレビ討論番組など

Social-MRCの出力画面の一例

Ustream表示部

Social-MRC固有部

Twitter用入力部

実験概要

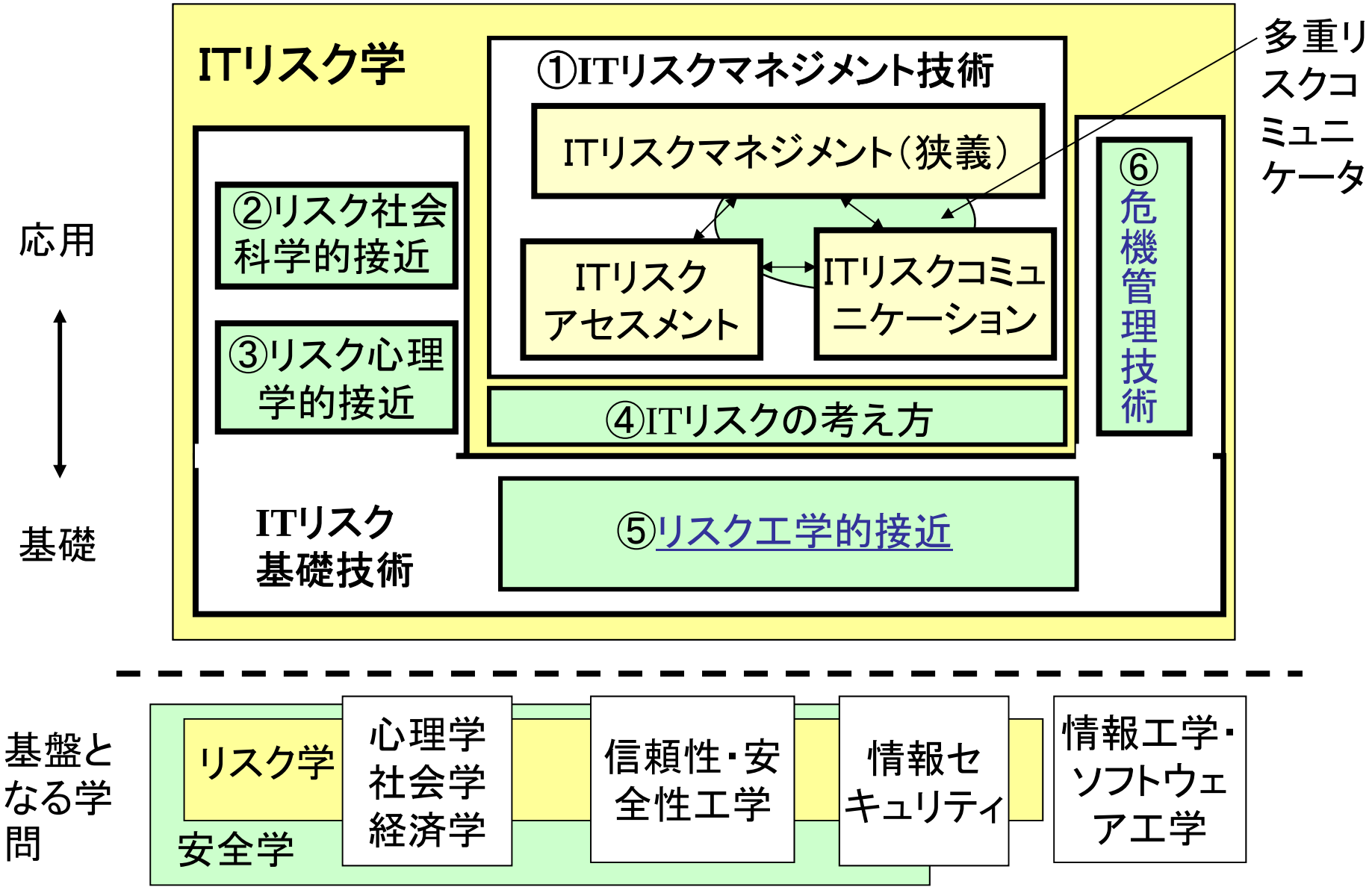
- 情報フィルタリング問題への合意形成の手順
  1. オピニオンリーダの主張と各最適解の説明
  2. 支持するオピニオンリーダへの投票
     ＝＞規制反対派を選出
  3. 支持するオピニオンリーダの最適解をベースに改良案の議論　＜＝一般関与者の意見
  4. 暫定合意解の導出＝＞2回目の最適解でオピニオンリーダ間で暫定合意
  5. 暫定合意会への投票＝＞86%支持

基本的有効性を確認。個別には処理速度など解決すべき課題も

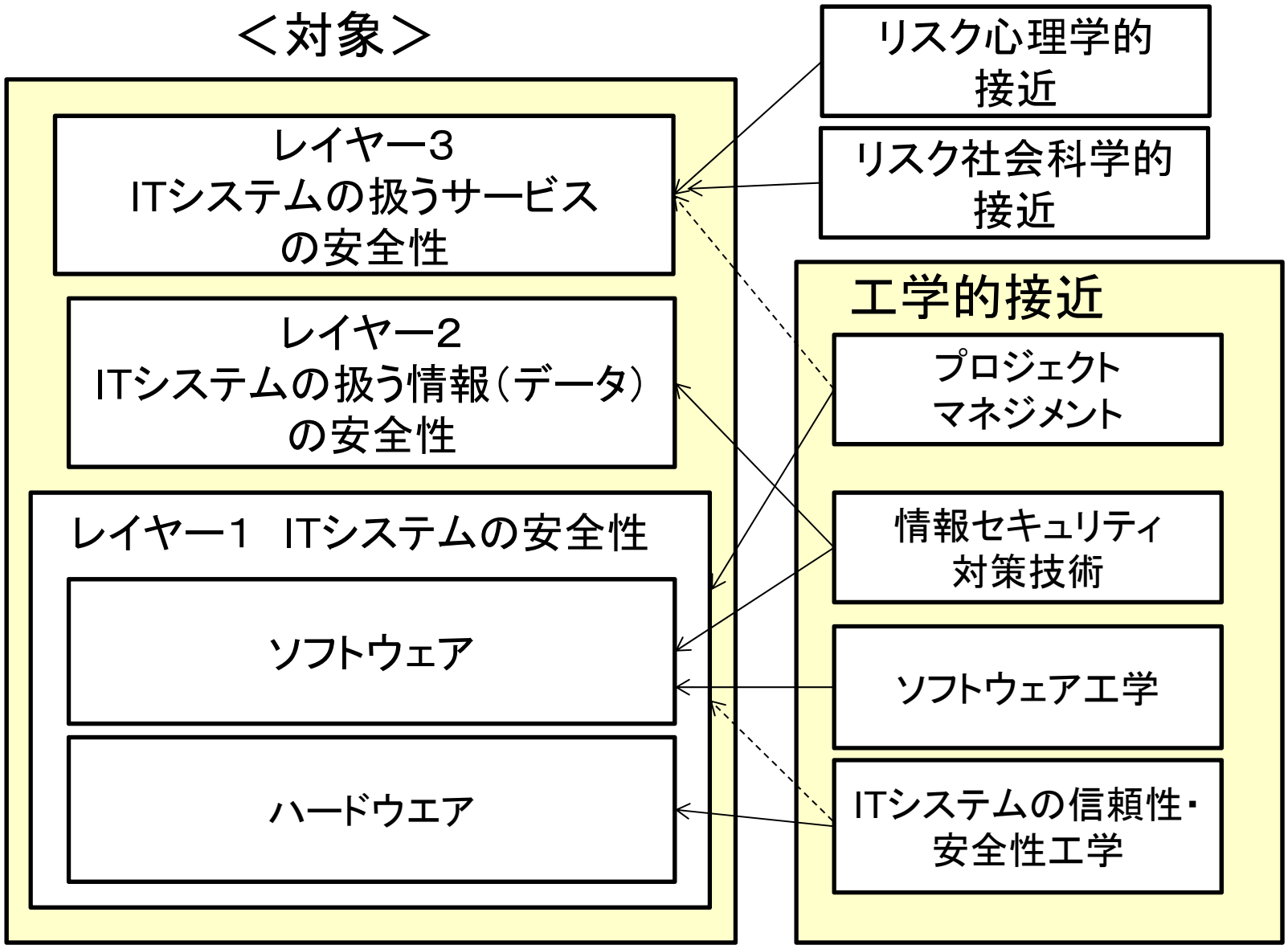
リスクコミュニケーションの困難性と対応

	困難性	関与者			対策案
		専門家	送り手	受け手	
①	リスク管理者への不信（情報を正確に発信か）		◎	○	不誠実な行いが発覚した場合には致命的な処分を自らに課す公約の実施
②	専門家の知識や中立性への疑問	◎		○	複数の専門家の参加と一般関与者による観察
③	リスクアセスメントの評価基準への疑問	◎	○		方式の開発
④	客観確率への不信（今後も同じかなど）	◎		○	すべては主観確率であるとしての対応
⑤	情報の受け手のバイアス（非自発的なリスクなど）		○	◎	バイアスを修正する過程の導入
	備考				詳しくは佐々木ほか「ITリスク学」13章参照

ITリスク学の構成（Version3）



ITリスクに対する接近法の対象



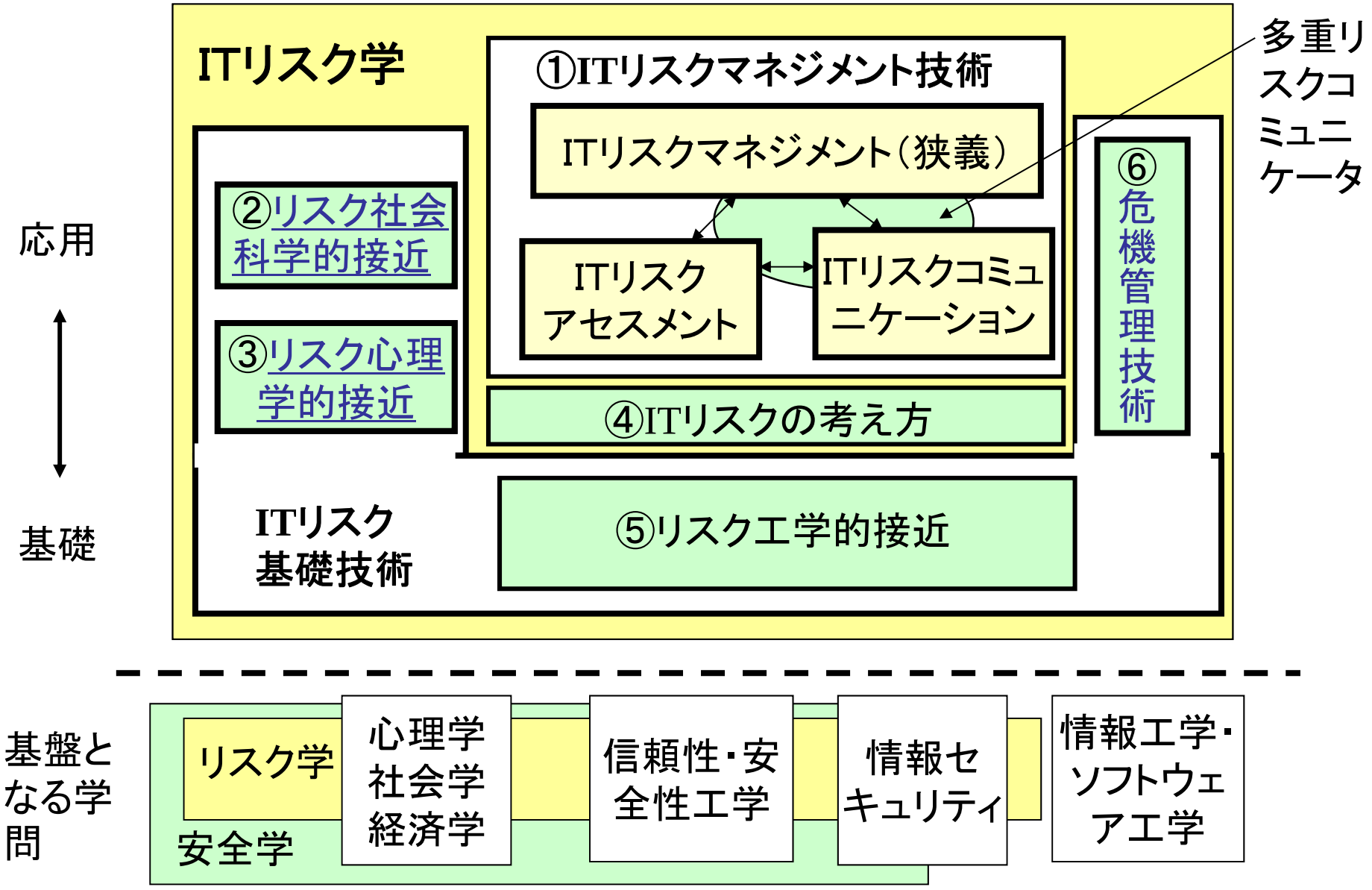
⑤ リスク工学的接近

ITシステムのリスクへの工学的接近の基本技術
（a）情報セキュリティ技術
（b）安全性・信頼性技術のうちITシステムに関連が深いもの
（c）ソフトウェア工学のうち信頼性に関連する技術
（d）ITシステムのプロジェクト管理技術

これらの技術を、広く理解するとともに、これらをITリスク向けに発展させた技術（（a）と（b）、（a）と（c）の組み合わせ技術など）の開発が必要

宮保教授「超分散技術を応用したディザスタリカバリシステムの研究実用化」
桧垣教授「安全安心のための通信基盤 無線マルチホップネットワーク」
もリスク工学的接近と考えることも可能。

ITリスク学の構成（Version3）



③ リスク心理学的接近

ITリスクへのリスク心理学的接近の基本
（イ）リスクの認知
（ロ）リスクと受容
（ハ）リスクの定量化（プロスペクト理論）など

これらの接近法を、広く理解するとともに、ITリスクに適した接近法の開発と適用が必要

先行的研究をIPAの小松らが実施

① Ayako Komatsu, Tsutomu Matsumoto, "Empirical Study on Privacy Concerns and the Acceptance of e-Money in Japan", Journal of Information Processing, Vol.19,pp307-316, 2011.7

② 花村，竹村，小松，情報セキュリティインシデント被害者の属性に関する考察，暗号と情報セキュリティシンポジウム2012 論文集，2012/05/31

② リスク社会科学的接近

ITリスクへの社会科学的接近の基本
（イ）リスクへの経済学的接近
（ロ）リスクへの経営学的接近
（ハ）リスクへの法学的接近
（ニ）リスクへの社会学的接近など

これらの接近法を、広く理解するとともに、ITリスクに適した接近法の開発と適用が必要

① 東大の松浦らが情報セキュリティに関する経済学的接近を実施
② 情報セキュリティ大学院大学の林がITリスクへの経済学・経営学・法学の統合的接近法を提案

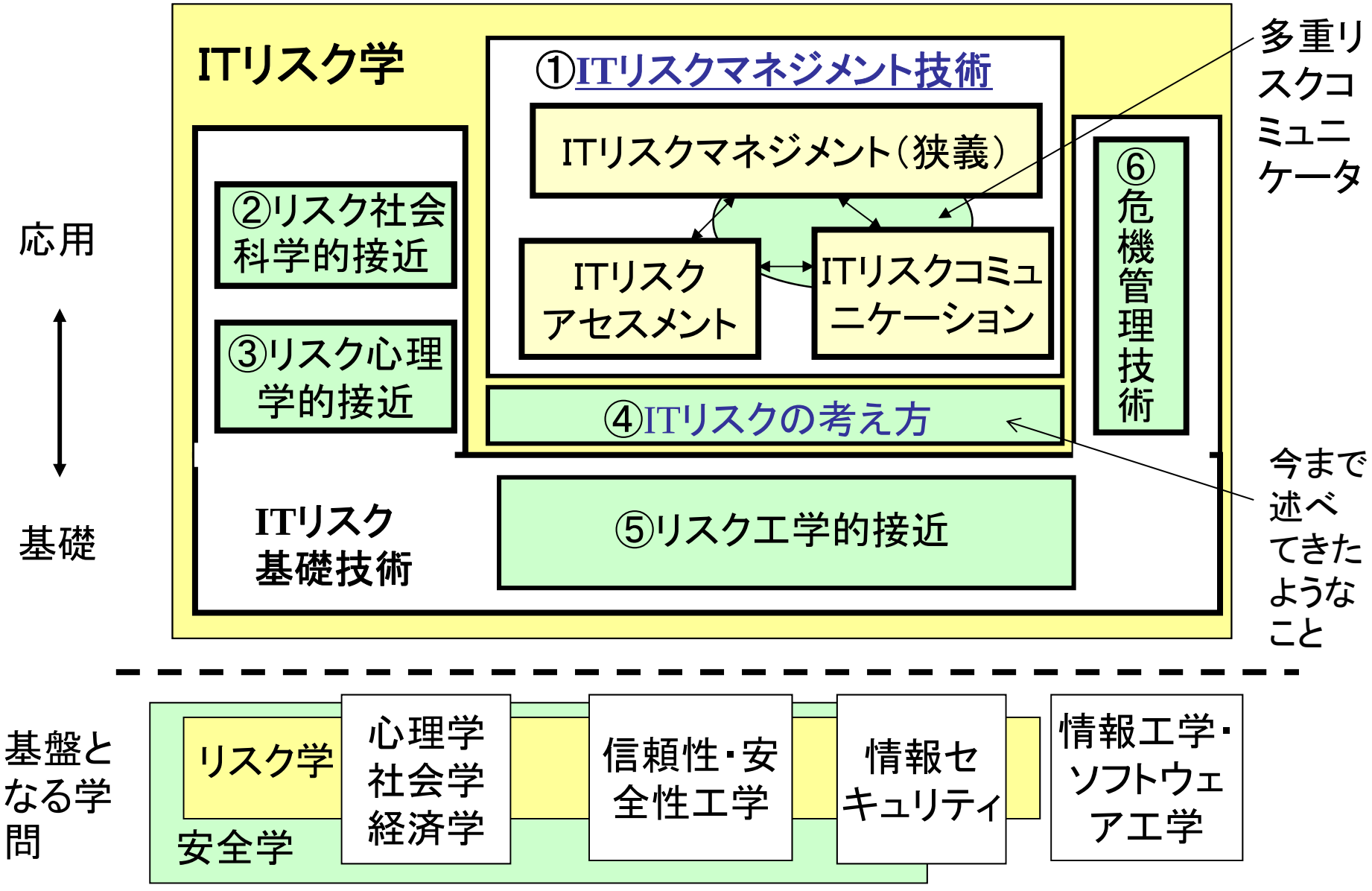
⑥ 危機管理技術

危機管理技術はリスク対策がうまくいかなかった場合に備えるためのもの.
障害時に事業を継続するためのBCP（Business Continuity Plan）やBCM（Business Continuity management）などがここに含まれる.

天災や機器故障、バグ、不正侵入などにより障害が発生した場合の自律的復旧ともいうべきレジリエンスの実現などが重要な技術となる

研究会としてはまだ調査段階で、独自の技術を開発する段階には至っていない。世の中では研究が進みつつあるが今後さらに強化が必要。

ITリスク学の構成（Version3）



ITリスク学の確立に向けての活動

① 2008年5月に日本セキュリティ・マネジメント学会の中に「ITリスク学」研究会を立ち上げ
② ITリスク学の定義
③ ITリスク学の全体像と構成要素の明確化
④ 構成要素の概要と研究課題の明確化
⑤ 研究課題の解決に向けての活動
⑥ 本の出版（2013年2月）

目次

今後の展望

社会のITシステムへの依存度の増大

サイバー攻撃の激化

→ ITリスク問題がますます重要に

→ ITリスク学＊研究がさらに重要に

特にITリスクマネジメント技術は大切に

＊「ITリスクに関する理論から実務までの体系化」という名で内閣官房の情報セキュリティセンターの「情報セキュリティ研究開発戦略」において12の重要なテーマの1つに
（内閣官房情報セキュリティセンター「情報セキュリティ研究開発戦略」(2011年7月8日)　http://www.nisc.go.jp/active/kihon/pdf/kenkyu2011.pdf ）

ITリスクマネジメント技術の研究

① 太田敏澄らは，ゲーム理論や社会心理学などに基づく「モデル・ベースド・アプローチ」

（太田敏澄，諏訪博彦、「モデル・ベースド・アプローチに基づくセキュリティ・マネジメント」，日本セキュリティ・マネジメント学会，第27巻，第1号，pp27-33）

② 佐々木良一ら「リスクコミュニケーションベースアプローチ」

（a）もっと簡単にリスクアセスメントを行い，合意形成を行って行く方法の確立

（b）今回開発したツールはPlan用のものであるが，Do-Check-Actと連携したツールの開発も

ITリスク関連基礎技術の充実

(a)リスク心理学的接近法:内部犯罪対策などにおいて対策の犯罪者に与える心理的効果の推定法の確立など

(b)リスク社会科学的接近法:経済学・経営学・法学などを総合的に組み合わせた対策案の創出法の確立など

(c)リスク工学的接近:セキュリティ技術と安全性工学やソフトウエア高額を組み合わせた対策案の創出と評価方法の確立など

(d)危機管理技術:障害が発生した場合の自律的復旧ともいうべきレジリエンス対策の明確化と評価手法の確立など

終わりに

(a)ITリスクへの対策が必要な背景や，ITリスクの特徴，必要となる対応方法に関する考察を行うとともに，ITリスク学の提案を行い，その定義や，ITリスク学を構成する要素技術などの明確化や一部開発を行ってきた.

(b)しかし，ITリスク学がさらに充実したものになるためには，技術開発と適用を相互に繰り返しながら発展していく必要があり，やらなければならないことはまだまだ多く残されている.

(c)この分野の研究に多くの方々が参加いただくことを期待する.

ITリスク参考文献（１）

１）佐々木良一「ITリスクの考え方」岩波新書、2008
２）佐々木良一他「多重リスクコミュニケータの開発と適用」情報処理学会論文誌、Vol49,No9,２００８年９月号
３）谷山 充洋、佐々木良一 他「多重リスクコミュニケータの企業向け個人情報漏洩問題への適用 」日本セキュリティマネジメント学会誌、Vol.23,No.2、pp34-51
４）谷山 充洋、佐々木良一「多重リスクコミュニケータの教育方法の提案と分析」日本セキュリティマネジメント学会誌、VOL.23,No.2、pp52-64
５）土方広夢、佐々木良一他「デジタル・フォレンジクスを考慮した個人情報漏洩対策に関する合意形成のための多重リスクコミュニケータの適用」日本セキュリティマネジメント学会誌　26巻第1号2012年5月pp3-14
６）佐々木良一「 ITリスク学の動向－技術と社会と安全と一 」IEICE Fundamental Review Vol.4 No.3(電子通信学会)

ITリスク参考文献（2）

7）佐々木良一他「ITリスク対策に関する社会的合意形成支援システムSocial-MRCの開発構想」情報処理学会論文誌VOL.52,No.9、pp 2562-2574
8） Ryoichi Sasaki et al., “ Proposal for Social-MRC: Social Consensus Formation Support System Concerning IT Risk Countermeasures”, International Journal of Information Processing and Management（2012）Vol.2,No.2 pp48-58
9）Ryoichi Sasaki,” Consideration on Risk Communication for IT Systems and Development of Support Systems” Journal of Information Processing Vo.20（2012）-4, pp814-822
10）大河原優、佐々木良一他「ITリスク対策に関する社会的合意形成支援システムSocial-MRCの情報フィルタリング問題への試摘用と考察」日本セキュリティマネジメント学会誌 25巻第3号2012年1月pp15-23