HITACHI
Inspire the Next

ITリスクを考える

～さまざまな分野から何を学んだか～

2010/1/16

株式会社 日立製作所

千葉　寛之　P.E.Jp, CISSP, CISA

uVALUE

0. 本発表の目的

HITACHI
Inspire the Next

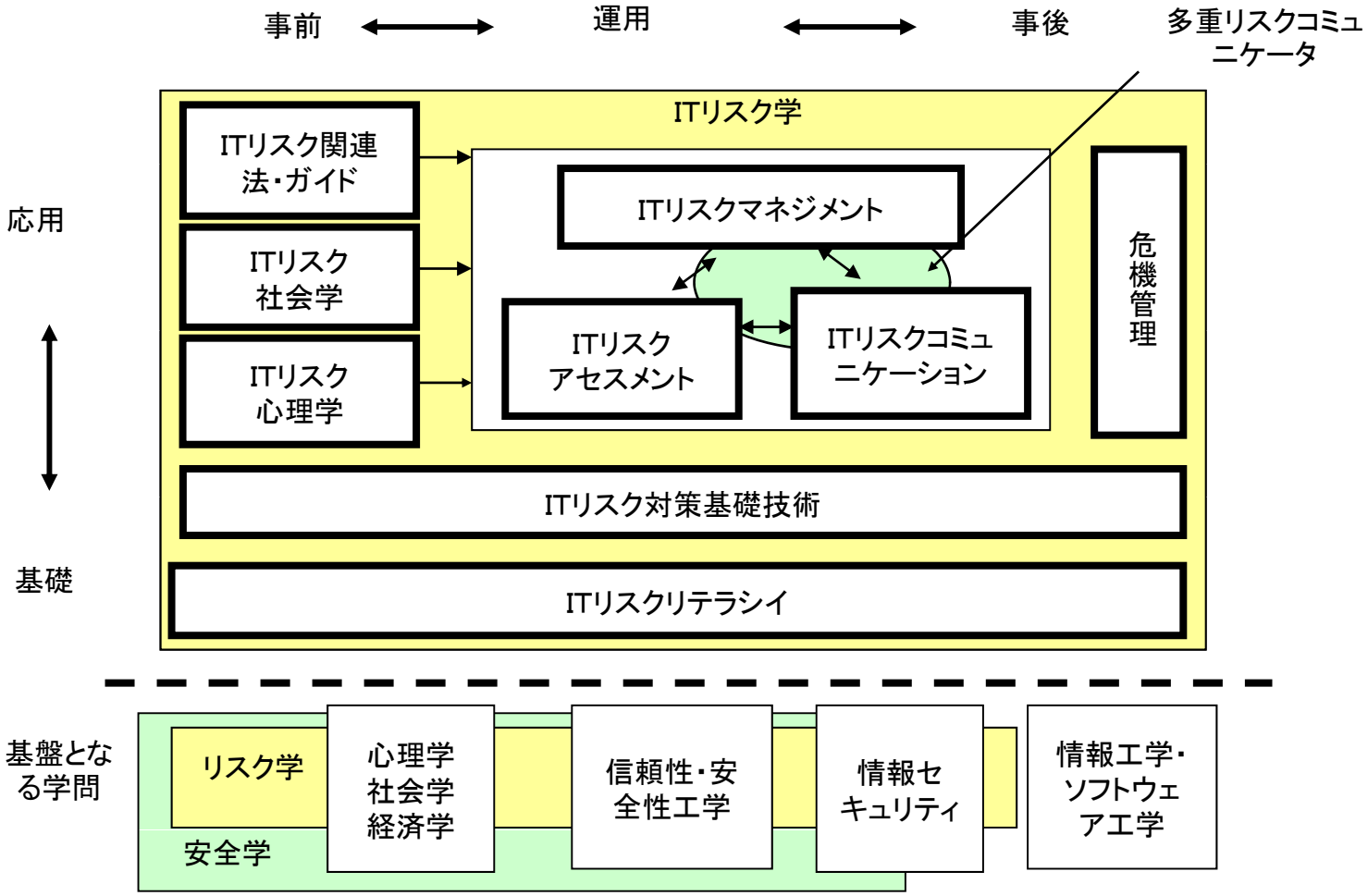
これまでITリスク学研究会にて拝聴してきた、多くの関連分野の専門家の方々の講演を踏まえて、複合的なリスク問題に対する知見を整理する. . .（ための議論に有益なネタを提示する）

以下の項目に役立つ議論ができれば. . .
・「ITリスク学」体系の具体化、洗練
・「ITリスク学」を理解・実践するための、理解モデルの確立
・「ITリスク学」に有効な対策技術の整理

1. ITリスク学の構成

HITACHI
Inspire the Next

ITリスク学は、ITリスクマネジメント・アセスメント・コミュニケーションの総合的アプローチを中心とし、さまざまな研究分野を対象として構成される。



第1回ITリスク学研究会佐々木先生資料より

uVALUE

2. 本研究会でのこれまでの特別講演の内容

HITACHI
Inspire the Next

回次	日時	特別講演内容	分野
2008年度 第1回	2008.6.28	中谷内一也氏(帝塚山大学 教授) 「リスク心理学の動向」	心理学
2008年度 第2回	2008.10.4	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」	医学(疫学)、リスク科学
2008年度 第3回	2009.1.10	南直樹氏(NHK解説委員) 「新型インフルエンザのリスクとマスメディア」	医学、マスコミュニケーション
2008年度 第4回	2009.3.28	氏田博士氏(財団法人エネルギー総合工学研究所) 「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」	工学、信頼性
2009年度 第1回	2009.5.28-29	(合同研究会のため、特別講演は開催せず)	ー
2009年度 第2回	2009.6.20	樋口晴彦氏(警察大学校　警察政策研究センター) 「新・組織行動の「まずい!!」学ーどうして失敗が繰り返されるのかー」	危機管理、組織学
2009年度 第3回	2009.9.19	名和利男氏(サイバーディフェンス研究所) 「最近のサイバー攻撃の実態とその考察についてー米韓DDOS攻撃、国内における標的型攻撃(0dayぜい弱性を悪用したマルウェア付きなりすましメール)、脅迫型DDOS攻撃等の対応経験から見出されたこと」	情報セキュリティ

3. 何を学んだか(1)

HITACHI
Inspire the Next

回次	日時	特別講演内容	分野
2008年度 第1回	2008.6.28	中谷内一也氏(帝塚山大学 教授) 「リスク心理学の動向」	心理学

- リスクの発生確率に関する人間の感覚は、かなりあいまいであること
- リスクを判断する個人の傾向
- マスメディアによる影響
- 専門家がもたらす問題(見栄、体裁、あいまい)
- 正しい知識の必要性を伝えることの重要さ

・対象となるリスクを正確に評価することにのみ着目するのではなく、正しく理解されない/伝わらないことによる影響も考慮する必要がある。
・正しく伝わらない要因について、心理学的に解明されているメカニズムがある。

4. 何を学んだか(2)

HITACHI
Inspire the Next

回次	日時	特別講演内容	分野
2008年度 第2回	2008.10.4	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」	医学(疫学)

- リスクの発生メカニズムではなく、統計的手法により対策(予測)することにより、原理が解明されていないリスクにもある程度対策を行うことができる。
- 放射線の危険性等について、公衆に正しい知識を伝えることは難しい(正しく説明すること＋説明を信用してもらうこと)
- 対策の組み合わせが有効であること
- 有害物質を積極的に取り除くというアプローチの可能性(今後の研究課題)

・メカニズムのみならずリスクを多角的に把握し、正しく知識を共有することが必要。

5. 何を学んだか(3)

HITACHI
Inspire the Next

回次	日時	特別講演内容	分野
2008年度 第3回	2009.1.10	南直樹氏(NHK解説委員) 「新型インフルエンザのリスクとマスメディア」	医学、マスコミュニケーション

- 正しい知識を身につけることに重要性(知らない間に目をこすってしまう等)
- ほぼ確実に発生するが、いつ具体化するかわからないリスク事象に対する対応のむずかしさ
- マスコミを含む情報伝達の重要性
- 確実な対策がないことをどう伝えるか
- 社会的/組織的協力に基づく対策
- 被害予測の精度の問題
- 危機管理対策の難しさ

・社会的リスク(パンデミック)に対する対策において、リスクコミュニケーションが重要

6. 何を学んだか(4)

HITACHI
Inspire the Next

回次	日時	特別講演内容	分野
2008年度 第4回	2009.3.28	氏田博士氏(財団法人エネルギー総合工学研究所) 「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」	工学、信頼性

- ヒューマンエラーに関する工学的な分析手法
- 言霊等、日本人が持つ感覚的な阻害要因
- 個人と組織の関係
- リスクリテラシーの重要性
- 基本的に個人が行う判断を複雑にしないことが前提

・ヒューマンエラーに対する工学的・解析的アプローチの有効性

7. 何を学んだか(5)

HITACHI
Inspire the Next

回次	日時	特別講演内容	分野
2009年度 第2回	2009.6.20	樋口晴彦氏(警察大学校　警察政策研究センター) 「新・組織行動の「まずい!!」学ーどうして失敗が繰り返されるのかー」	危機管理、組織学

- 危機管理マニュアルの限界(想定範囲外、マニュアル依存)
- コストとのトレードオフ(という現実)
- 典型的な複合要因による事故(孫受け、再評価なし、伝達(伝承)不足)
- 成果主義の功罪(組織機能に対する)
- 中間管理職の重要性(現場を把握する能力)

・組織としてリスクを把握、対応するための管理的対策の有効性

uVALUE

8. 何を学んだか(6)

HITACHI
Inspire the Next

回次	日時	特別講演内容	分野
2009年度 第3回	2009.9.19	名和利男氏(サイバーディフェンス研究所) 「最近のサイバー攻撃の実態とその考察について－米韓DDOS攻撃、国内における標的型攻撃(0dayぜい弱性を悪用したマルウェア付きなりすましメール)、脅迫型DDOS攻撃等の対応経験から見出されたこと」	情報セキュリティ

- 情報セキュリティにおける国際的な脅威に対する対応の実態
- 各国の組織によって、対応が異なる。また、組織の縦割り構造が阻害するケースと、ワンヘッドで行動(指揮命令が統一)できているケースがある。
- テロ行為等は、背景が確実に判明しないケースが多数あり、憶測情報ベースに報道されるケースがある
- ブラックマーケットの発展

・組織的・国際的なセキュリティ脅威が顕現化してきており、個々の組織の対策では対応できないため、国家的、集団的対応を考慮する必要がある。

uVALUE

9.「ITリスク学問題(リスク)」の記述イメージ

HITACHI
Inspire the Next

ITリスクおよびその対策を把握するための項目（視点）

問題記述	リスクモデル	対策
・問題(リスク)概要 　リスク分類(ex.社会的) ・何を守る(防ぐ)べきか(※) ・関与者一覧 　関与者毎の目標 　問題に対する習熟度 　リスクリテラシー (※)関与者毎に異なる場合がある	・専門家によるリスク算出モデル 　解析的(メカニズム) 　統計的(ブラックボックス) ・リスク間のトレードオフ ・リスクに関する関与者の理解度とその限界 ・対策に対する心理学的側面 ・ヒューマンエラーに関するリスクモデル	・専門家によるリスク対策 　技術的対策 　管理的対策 　　運用的対策 　　組織的対策 ・対策間のトレードオフ ・理解を深めるための対策

10. 今後の課題

HITACHI
Inspire the Next

- ITリスクの法的側面からの検討
- ITリスクが対象とする問題の分類・種類の整理
- リスク算出モデルにおける心理学的側面等の考慮方法の確立
- 理解度を考慮したリスクコミュニケーションの促進方法の確立

「ITリスク」の体系化、理解モデルの確立
⇒リスクコミュニケーションの推進

uVALUE

HITACHI

Inspire the Next