

リスク・セキュリティの基礎

担当：宮本定明

授業の目的

リスクとセキュリティの基礎に関する講義のうち、以下の 4 項目について分担講義を行い、リスクとセキュリティの基本概念について理解させることを目的とする。

授業の各項目

1. リスク管理の基本概念
2. リスクとセキュリティ
3. リスクリテラシーとセキュリティリテラシー
4. リスク工学について

単位数：分担 0.4 単位（4 項目で 6 時間）

受講学生に望む到達度

上に述べたリスク・セキュリティの基本概念を習得し、あわせてリスク工学の意義について考察すること。

評価基準

授業時間内の演習、minute paper などの小レポート、レポートを合せて総合的に評価し、100 点満点のうち 60 点をこの項目についての合格基準とする。なお、分担講義のため、科目の合格基準としては、他の成績と合せて評価される。

各項目に関する概要

次ページ以降に示す。

教科書・参考文献

Powerpoint 等の handout を準備する。参考文献については、以下の各項目について示されている。

1. リスク管理の基本概念

様々な危機と不確実性が個人や組織をとりまくなかで、現代社会は確実にリスク管理社会になりつつある。と同時に、リスクの概念は多様であり、一般的に論じることが困難であるように思われる。リスク解析やリスク管理は必要とされ、様々な学問分野で研究されているが、異なる分野間でのリスク概念に関する相互の合意はどの程度あるかは明らかではない。

しかしながら、リスクの一般論を論じ、概念を明確にしようとする考察も見受けられる。ここでは、Ansell and Wharton, (J. Ansell, F. Wharton, eds., *Risk: Analysis, Assessment and Management*. Chichester : John Wiley, 1992) 1991 にもとづいて、リスク解析とリスク管理の一般論について述べるとともに、若干の私見をも付け加えることとする。

Ansell and Wharton による基本的立場は、この編著書の序文に明確に述べられている。

Risk is an unavoidable feature of human existence. Neither man nor the organizations and societies to which he belongs to can survive for very long without taking risks. (リスクは人間存在において避けられない特徴の一つである。どんな個人も、組織も、また社会もリスクをとることなくして永く生き延びることはできない。)

これが、リスク管理の一般論における *take risk* という基本的立場である。人間・組織・社会は全てのリスクを避ける(*risk avoidance*)は不可能であり、意思決定は、どのリスクをとるかということである、と述べたものである。

Ansell and Wharton による編著書の第1章には、リスク管理の一般論を述べたものである(第1章: リスク管理—基本概念と一般的原理; Chap.1. Risk Management: Basic Concepts and General Principles)。より詳しい内容については、別紙資料にゆずるが、この章では、リスク概念が学際的(*multidisciplinary*)であること、従って、基本的合意が必要であることから始めて、人間の進化とともに、リスク管理も進化してきたこと、リスクの語源とそれが、どのように現在のリスク概念に反映されているか、リスクの計量、リスクの基本モデル、リスク管理におけるいくつかの基本的観点とそれらの優先順位、などが解説されている。

以下は筆者の見解である。

筆者らの基本的立場は、社会科学であり、異なる分野を統括する立場は経済学や政治学のような社会科学にあると考えている。リスク管理のための社会的意思決定が社会科学的観点からなされることからみれば、このことは当然であるように思われるが、工学や自然科学と違って、社会科学におけるモデルの不確実性とあいまいさは格段に大きく、問題を限定しないと、定量的管理ができないという欠点もあろう。

著者(Wharton)によるリスクの定義は、「リスクとは、意思決定(*decision*)や行動(*action*)に伴う意図外の(*unintended*)、あるいは予期しない(*unexpected*)結果のことである。」という

測度を含まないものであり、専門的立場でのリスクの定義、たとえば「不利な結果の厳しさ(severity)と蓋然性(probability)の測度(measure)」が確率やサイズの計量を含んでいるのと比べると、かなり差がある。

計量を含まないリスクの定義をとれば、概念はより一般的になり、多くの分野における異なるリスク概念を包摂できるが、特定性 (specificity) は弱くなる。社会科学の立場からすると、定量性をもたないシナリオ解析などもリスク解析の中に含まれることになり、リスク定量化はリスクの様々なモデルの一部として扱うことになるのであろう。

リスク管理を学際的に捉えるとき、先行する分野のモデルが必要ではないかと思われる。筆者の見解では、環境科学・環境工学と比較しながら、リスク科学・リスク工学の教育・研究を進めるのが興味深い。もちろん環境科学・環境工学とリスク科学・リスク工学はかなり重複する部分があるが、基本的立場に相違があると思われる。すなわち、環境科学においては、人間の介在を必要としない部分も多く（地球科学的立場はその一例、環境の定義には、「自分自身以外の全て (everything except oneself)」という包括的定義もある）、人間の存在が環境に有害であるとする立場も有力であるが、リスク科学の場合は、人間や組織が主体であり、それらの意思決定が鍵となるであろう。

実際の講義においては、別紙資料を中心に、いくつかの補足資料を示し、リスクの一般論について学生・教員間の討論を含めながら進めていきたい。上記および資料に示された見解には異論も多いと思われるが、率直な意見を活発に交換し、それらを記録に留めることで、この分野・科目の理解を深め、研究の進展にも寄与することができよう。なお、討論にあたっては、role playing など一つの方法となるであろう。

使用テキスト：別紙 Powerpoint 資料

参考文献：

1. J.Ansell, F. Wharton, eds., Risk: Analysis, Assessment and Management, 1992
2. 上掲書第1章：Risk management:Basic Concepts and General Principles

2. リスクとセキュリティ

2. 1. セキュリティとリスク概念

この項では、主に甘利 (2004, 2006) によって示されたセキュリティの定義・実現要件について紹介する。

甘利 (2004) によれば、(狭義の) セキュリティを「正当な目的を持たないエージェントを管理区画の中に入れていないこと」と定義している。また、この定義に従い、セキュリティを実現する要件として次の4つを挙げている。

- (1) 管理区画の明確化
- (2) エージェントが正当かどうか区別
- (3) エージェントが正当なときだけ進入を許可する仕組み
- (4) 正当でないエージェントが進入した場合、それを早急に検知し、対応（排除・無力化）する仕組み

具体的に、いくつかの例が挙げられており、その意義が示されているが、ここでは省略し、講義時に述べる。

さらに、最近のセキュリティ概念の拡大に鑑み、甘利（2006）では、次のようにより包括的なセキュリティの定義として「オペレーション（日々の営み）が運営主体によってあらかじめ定められたプランに則って運営され、理由の如何によらず、それが阻害されないこと」と述べている。この場合の実現要件を、以下の5項目としている。

- (1) 運営主体の明確さ
- (2) 定められたオペレーションの存在
- (3) プラン遂行に必要なリソースプロパティが洗い出されていること
- (4) リソースプロパティに影響を与える阻害要因（インシデント）が網羅的に洗い出されていること
- (5) インシデントに対するリスクマネジメントがなされていること

また、同じ著者により、リスクマネジメントは、リスクコントロール、リスクファイナンス、クライシスマネジメントの3本柱からなる、とされている。

上記セキュリティの定義は洞察に富んだものである。講義時には、具体例を挙げながら紹介したい。また、この定義の妥当性と有用性について、討論し、小論文などをまとめる。

2. 2 リスクとセキュリティの規格・認証制度

リスクマネジメントについては、JIS Q 2001 の規格が存在する。また、個別分野においては、別にリスクマネジメント規格が定められている。この項では、リスクマネジメント規格の概略を述べ、その中心的な役割を果たすPCDAサイクルについて紹介する。

更に、情報セキュリティマネジメント (ISMS) 規格について紹介する。ISMSについては、第三者認証制度があり、この点で JIS Q 2001 とは異なっている。合せて、大学における認証制度は現在そうになっているかを述べる予定である。

評価に際しては、web ページを参照して、簡単なレポートを提出させる、などの方法もある。講義の状況に応じて選択すべきであろう。

使用テキスト：別紙 Powerpoint 資料、甘利論文（下記）、JIS, ISO に関する web ページ抜粋

参考文献：

1. 甘利康文、セキュリティの基本的考え方とリスクマネジメントとの関係について、信

学技法、Vo.104, No.528, 2004.

2. 甘利康文、セキュリティの上位概念的考え方について、信学技法、Vo.105, No.687, 2006.

3. リスクリテラシーとセキュリティリテラシー

リテラシーとは、英和辞書などで「読み書きの能力、識字能力、教育を受けていること」と説明されている。ここでは、リスクリテラシーとセキュリティリテラシーという用語を中心にいくつかの研究・考察について紹介する。

リスクリテラシーという用語が時々見られる。この用語は、リスクコミュニケーションという研究領域とともに使用されている。まず、この言葉を中心に、最近のリスク研究の1領域を紹介したい。

リスクコミュニケーションについては、多くの研究があり、分野としてほぼ確立しているのに対し、リテラシーという研究は比較的少ない。そこで、リスクコミュニケーションから見ていこう。ただし、リスクコミュニケーションについては、他の講義でより詳しく解説される予定である。

Wikipedia 日本版（平成19年2月14日）では、次のように述べている。「リスクコミュニケーション(Risk Communication)とは社会を取り巻くリスクに関する正確な情報を、行政、専門家、企業、市民などのステークホルダーである関係主体間で共有し、相互に意思疎通を図ることをいう。合意形成のひとつ。」

リスクコミュニケーションに際して、リスクの基本的知識が必要である。これをリスクリテラシーとしている場合がある。たとえば、竹内ら（2005）に、リスクコミュニケーション支援システムの一部として「水害に関する知識を学ぶ『水害リスクリテラシー学習支援ツール』を備えており」とあるのはこの一例である。また、林（2005）は、リスクリテラシー入門と題した著書の中で、様々な事故・災害などの事例を集めてコメントを加えているが、著書の副題が「現代リスクの基礎知識」というところからも、上記と同様の解釈がとられているといえよう。

一方で、セキュリティリテラシーという用語もみられる。情報リテラシーあるいはコンピュータリテラシーはよく聞く言葉で、コンピュータを操作するにはそのための素養が必要なことは明らかであるため、この言葉はなじみやすい。

セキュリティリテラシーという用語（下記文献3）が使われるのも、情報セキュリティあるいはより一般的なセキュリティに関する基礎的素養が多くの人にとって必要になってきたという社会情勢によるものであると思われる。特に情報セキュリティリテラシーは、今日のネットワーク社会において様々な情報リスクが存在し、それらへの対処は必ずしも専門家だけでなく、日常的に多くの人によって行われなければならないことから、現在のところ、リスクリテラシーよりも適切な用語であると思われる。

コミュニケーションやリテラシーという用語は、情報科学、ICT技術からの影響によるものであろうと思われるが、十分吟味して用いていく必要がある。また、一時の流行

に終わることなく、リスクリテラシーの概念が今後育っていくかどうかについて、注目している必要がある。

使用テキスト：別紙 Powerpoint 資料など

参考文献：

1. 林志行、事例で学ぶリスクリテラシー入門：現代リスクの基礎知識、日経BP社、2005
2. 竹内、高尾、下川、佐藤、福園、池田、水害リスクリテラシー学習支援ツールの構築、防災科学技術研究所研究報告、第67号、pp.63-71, 2005.
3. 内閣官房情報セキュリティセンター情報セキュリティ政策会議セキュリティ文化専門委員会報告書（2005.11.17）
4. D.M. Kammen, D.M. Hassenzahl, Should We Risk It? Exploring Environmental, Health, and Technological Problem Solving, Princeton Univ. Press, 1999 (注：邦訳が出ているが、原書を読むべきである)

4. リスク工学について

リスク工学という名称を用いている例は、国内では前例がなかったが、最近になって、文献1のような例が現れた。海外では、保険会社が以前より **Risk Engineering Workshop** を実施しているようであるが、概して例は少なく、大学の組織としては、筑波大学大学院システム情報工学研究科リスク工学専攻が唯一であると思われる。この節では、リスク工学、リスク科学、あるいはリスク学の可能性について述べる。

第1節の講義で述べることであるが、リスクの概念は、学際的であり、異なる分野では定義や扱いが異なる。経営分野では、リスクを **positive** に捉えるのに対し、伝統的な工学技術の分野では、**negative** に捉える。安全工学は従来の枠組みで議論されてきたが、工学の学際性が高まり、情報技術が益々普遍的になるにつれて、安全工学を超えるリスク工学の観点が必要となってきた。

また、先に述べたセキュリティとリスクの関連性を考慮すると、リスク工学には、セキュリティ工学の観点も加わる必要があると考えられる。

次に、なぜリスク工学であって、リスク科学ではないのかという問題がある。これを考えるには、環境科学と環境工学の違いを考え、類推してみれば良い。環境科学が諸科学の中にそれぞれ存在するのに対し、環境工学は、有用性と工学の主目的である人材育成の観点から、諸科学とは区別される。この違いが、リスク科学とリスク工学にもあてはまるであろう。当面のところ、リスク科学は、諸科学の中で独立に存在するのに対し、リスク工学は、社会における有用性と人材育成を追及しなければならない。

次に、リスク学について考えてみる。法律、哲学、社会学などは、リスク管理の観点から再構成されるべきであり、さらには政治学や国際関係は、リスク学の中核となるべきものである。しかしながら、これらを含めたリスク学全般は、教育課程としてはあまりに広

範で不適切であり、組織としての有機性をもたないであろう。少なくとも現在の社会に有用な人材は工学の中から育成されると思われる。

リスク学やリスク科学は、極めて重要かつ実現が必要な概念であるが、十分な形で実現するには、未だ時間を要すると考える。

この項目では、リスク工学、リスク科学、リスク学の可能性について討論、グループ討議を行わせ、その結果をレポートあるいはグループレポートにまとめさせて評価する。

使用テキスト：別紙 Powerpoint 資料など

参考文献

1. 谷口清隆、ファイナンスとリスク工学、システム/制御/情報、50(11) 405-411, 2006
2. リスク工学紀要、第1巻（2004年度）、第2巻（2005年度）

Fundamental Concept of Risk

Sadaaki Miyamoto

J. Ansell, F. Wharton, eds.,
*Risk: Analysis, Assessment and
Management*, 1992

- Preface より (first sentence)
 - リスクは人間存在において避けられない特徴の一つである。どんな個人も、組織も、また社会もリスクをとることなくして永く生き延びることはできない。
- Risk is an unavoidable feature of human existence. Neither man nor the organizations and societies to which he belongs to can survive for very long without taking risks.

リスク管理－基本概念と一般的原理
Chap. 1. Risk management: Basic Concepts
and General Principles

- The Evolution of Risk
- The Concept of Risk
- The Perception of Risk
- Risk Analysis
- Risk Assessment
 - The Economics
 - The Psychology
 - The politics
- Risk Management

Abstract

•

assessment

risk analysis

risk

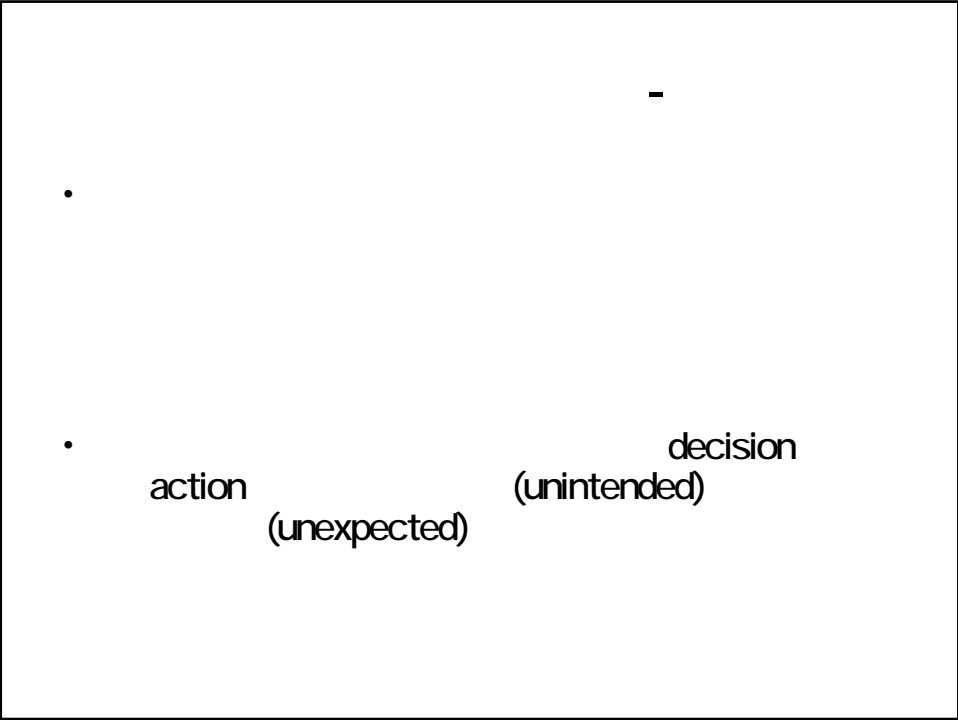
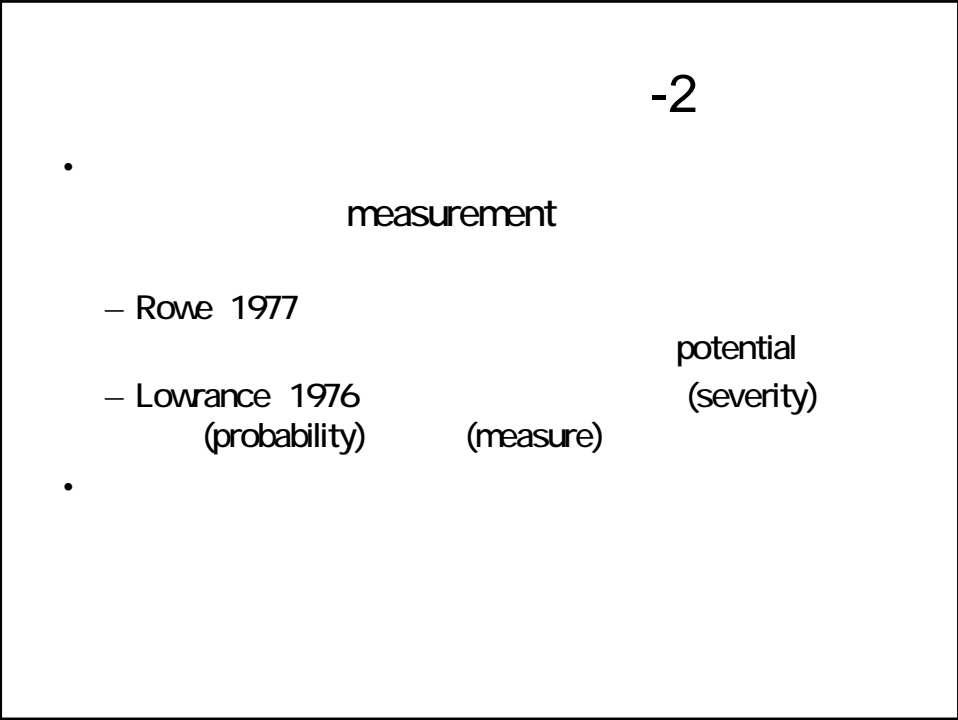
The Evolution of Risk

-
-
-

-

take risk

-



The perception of Risk

-
-
- - outcome (risk analysis)
 - identification (risk assessment)
 - estimate

Risk Analysis

-
- Concise Oxford, 1976
- - risk paradigm
 - outcome
 - gain-
 - loss
 - The basic options

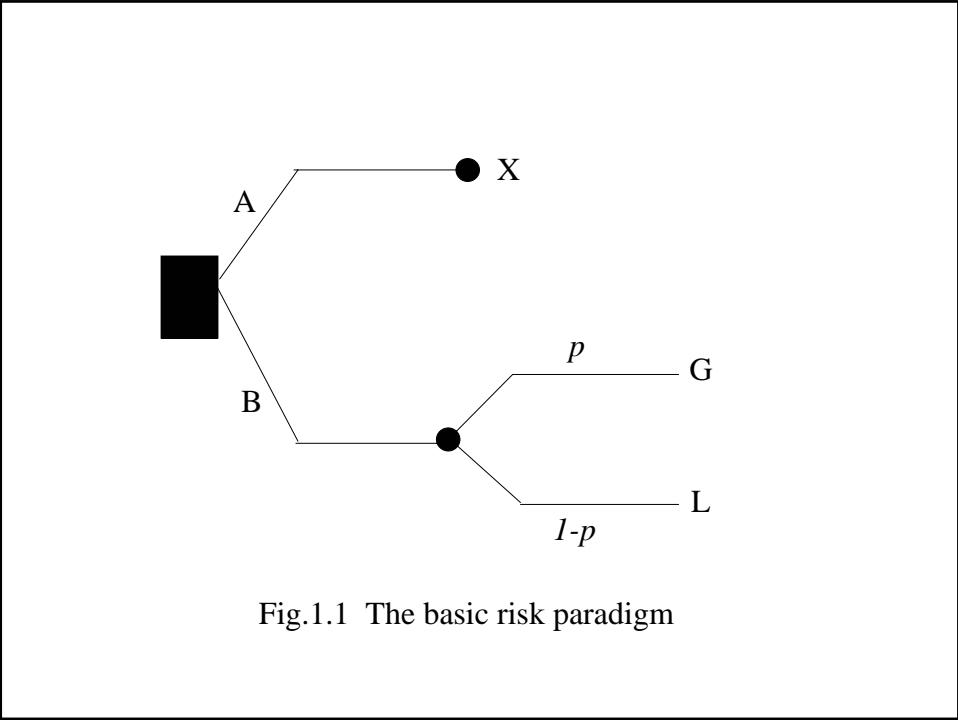
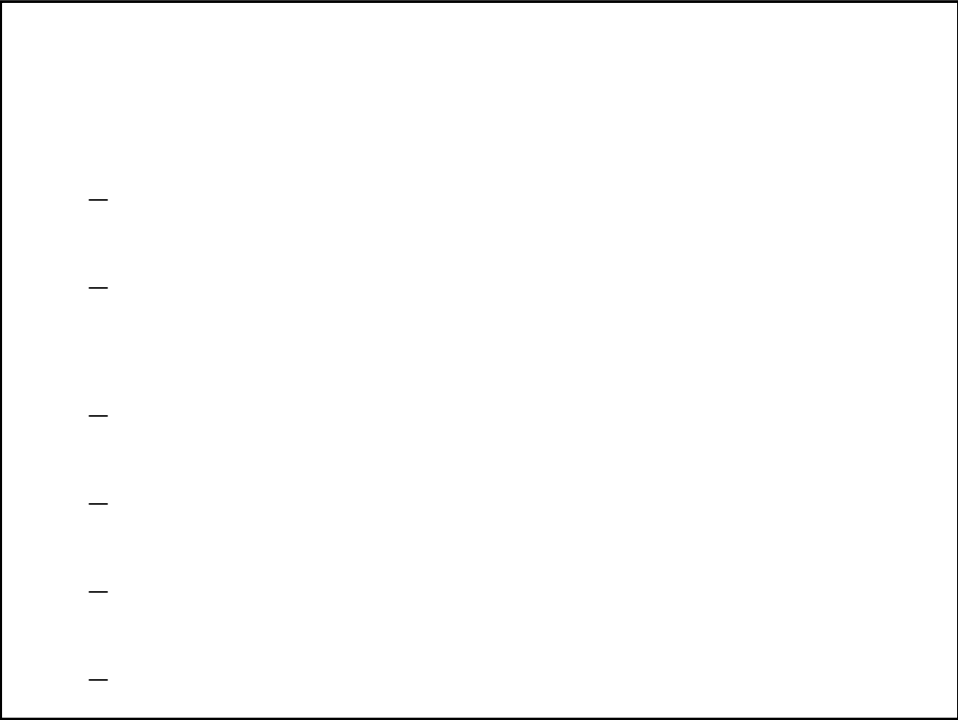


Fig.1.1 The basic risk paradigm



-
-

Risk assessment

- decision theory

- $$E[B] = pG + (1-p)L$$

- $$v_i \quad \quad \quad \begin{matrix} n \\ i \end{matrix} \quad \quad \quad p_i \quad \quad \quad \text{outcome } i$$

$$E[v] = \sum_{i=1}^n p_i v_i$$

-

B

$$V[B] = p(G - E[B])^2 + (1 - p)(L - E[B])^2$$

-

$$V[v] = \sum_{i=1}^n p_i (v_i - E[v])^2$$

-

-

- Bernoulli(1738)

-

-

•
—
Real,1991)

• payoff-
• 1945

psychology

•

—

—

•

possibility

remote

effectively zero

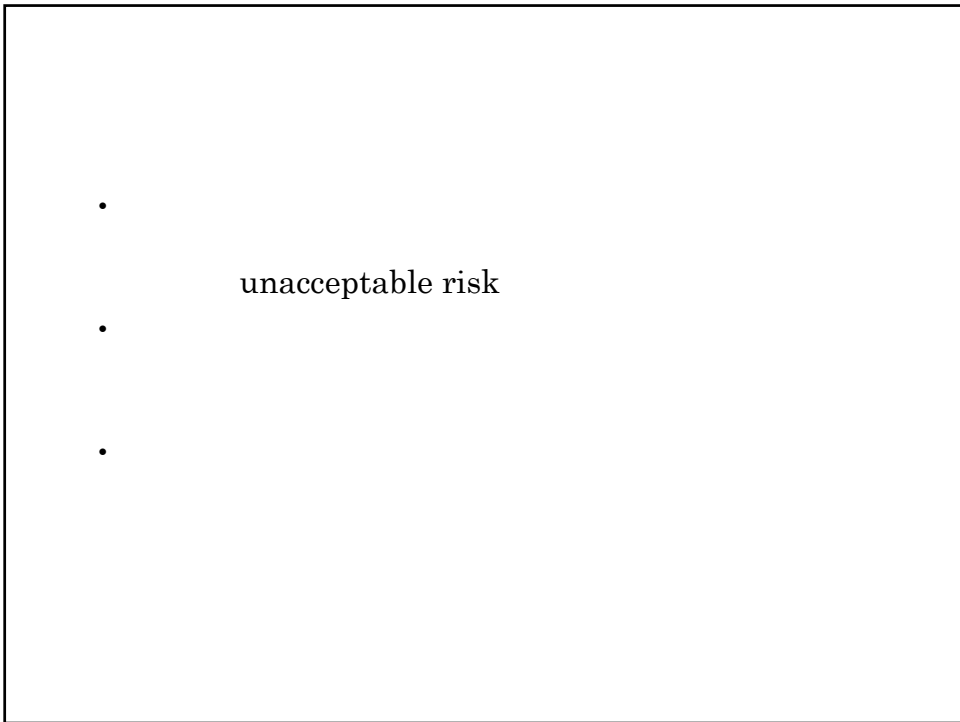
—

threshold of significance

100

1

$10^{-6} = 0.000001$



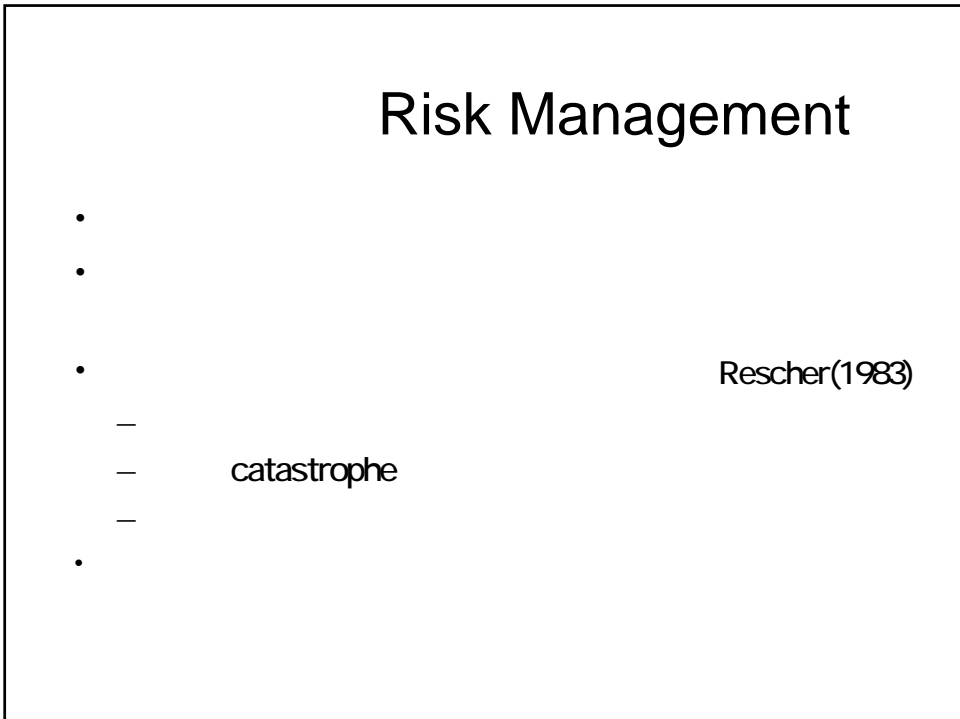
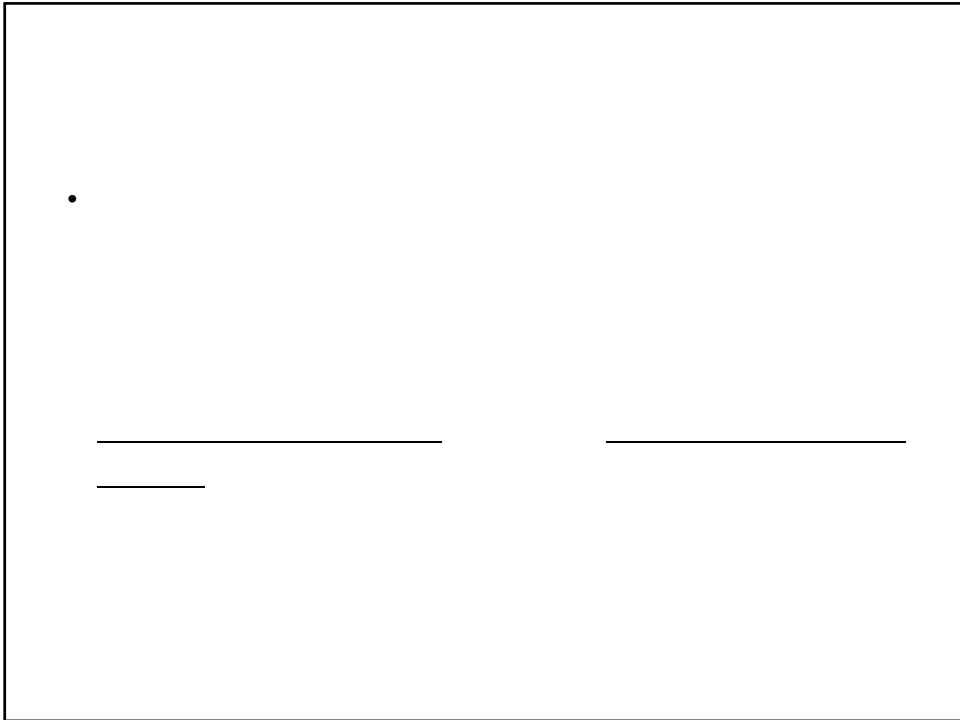
politics

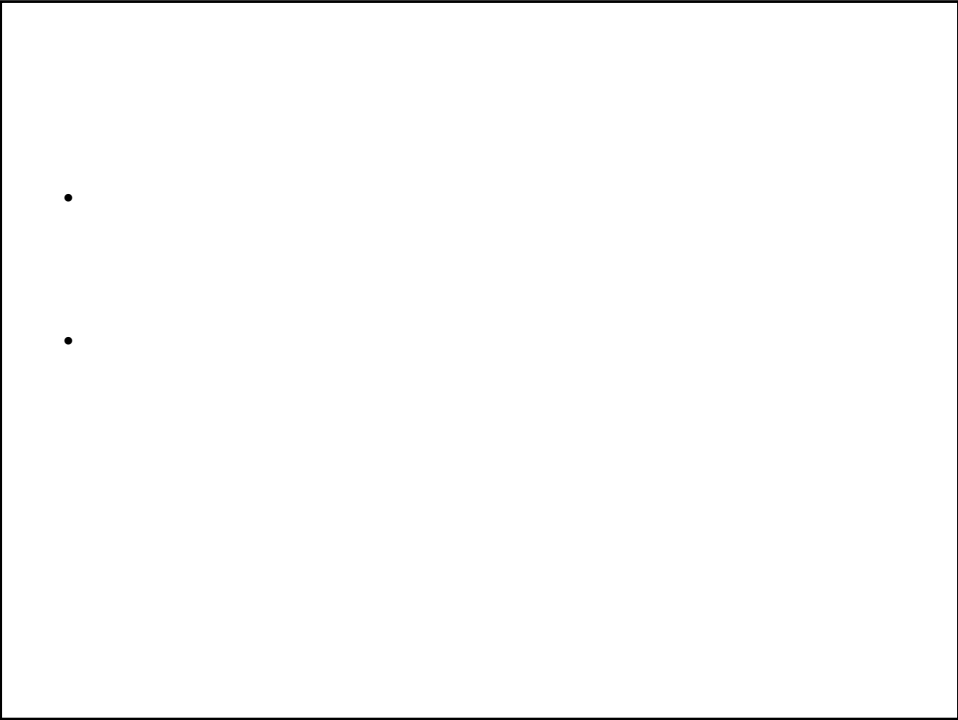
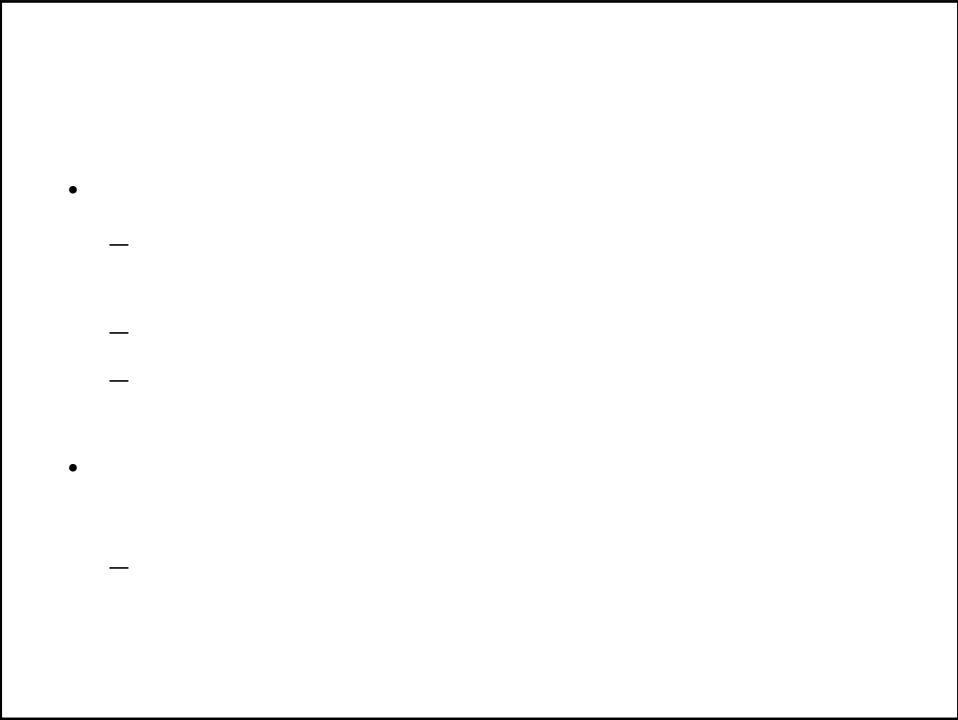
-

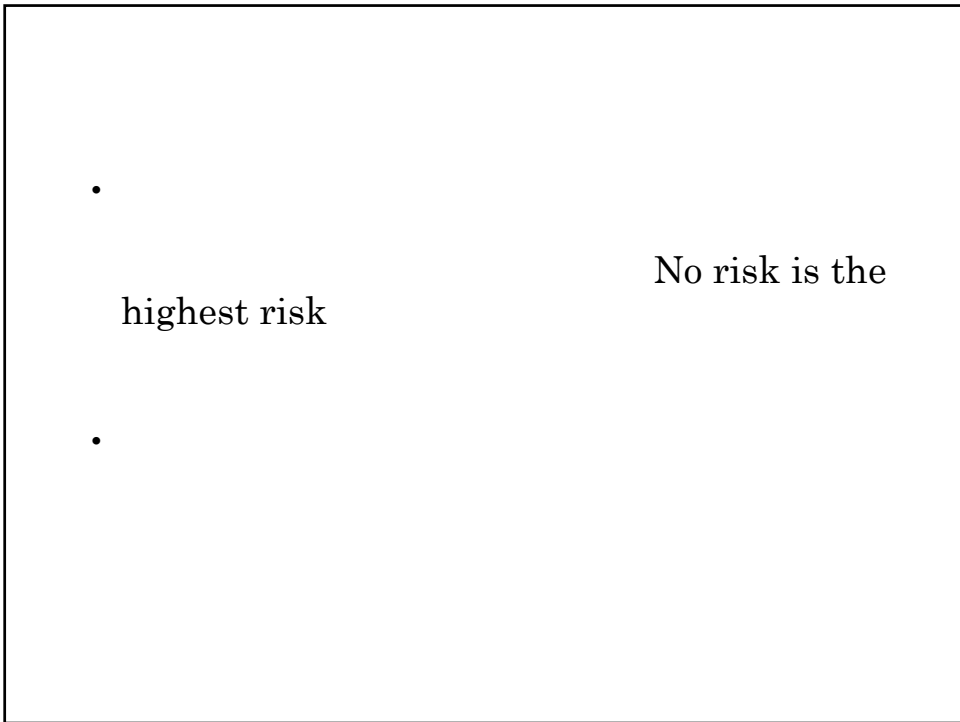
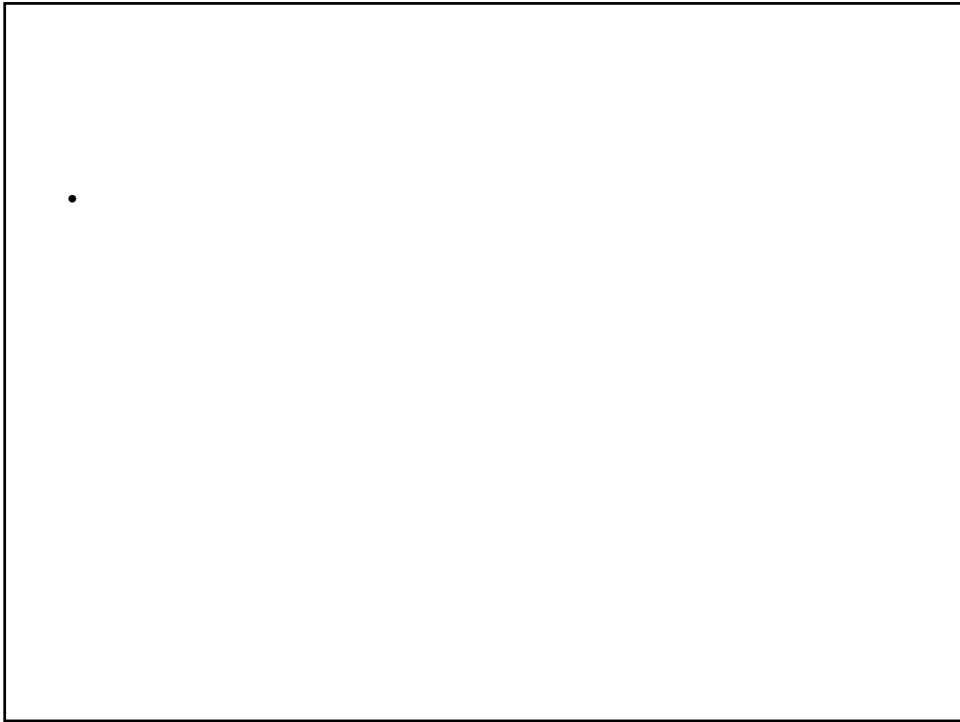
Rescher, 1983

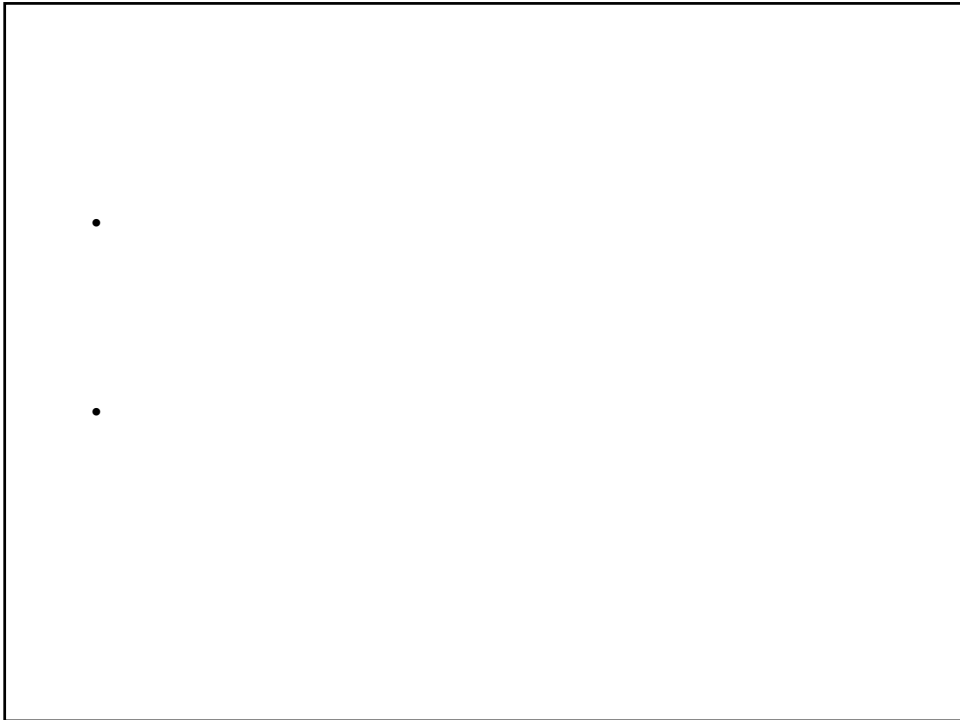
-

—



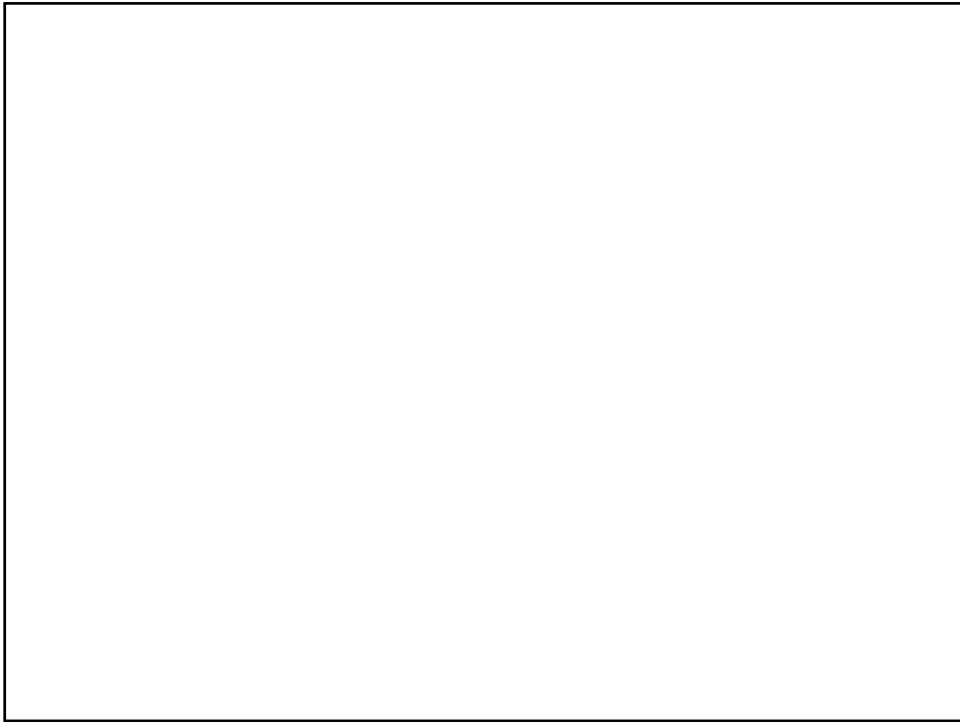






Questions

1. $E[B]$ $V[B]$
 $G = L = \text{JPY}10,000$ $p = 0.52.$
- 2.
3. 1



- , Tech Rep. IEICE 2004
 - 3
 - Risk control
 - Risk finance ()
 - Crisis management ()
- - Risk control ABS
 - Risk finance:
 - Crisis management:
- Risk control Crisis management

-
-

- Tech. Rep., IEICE 2006
-
- -
 -
 -
 -
 -

- JIS Q 2001
 - 1995
 - PDCA (Plan, Do, Check Action)
 - ISO
 -
 -
 - X 5080 ISO/IEC 17799 **JIS**

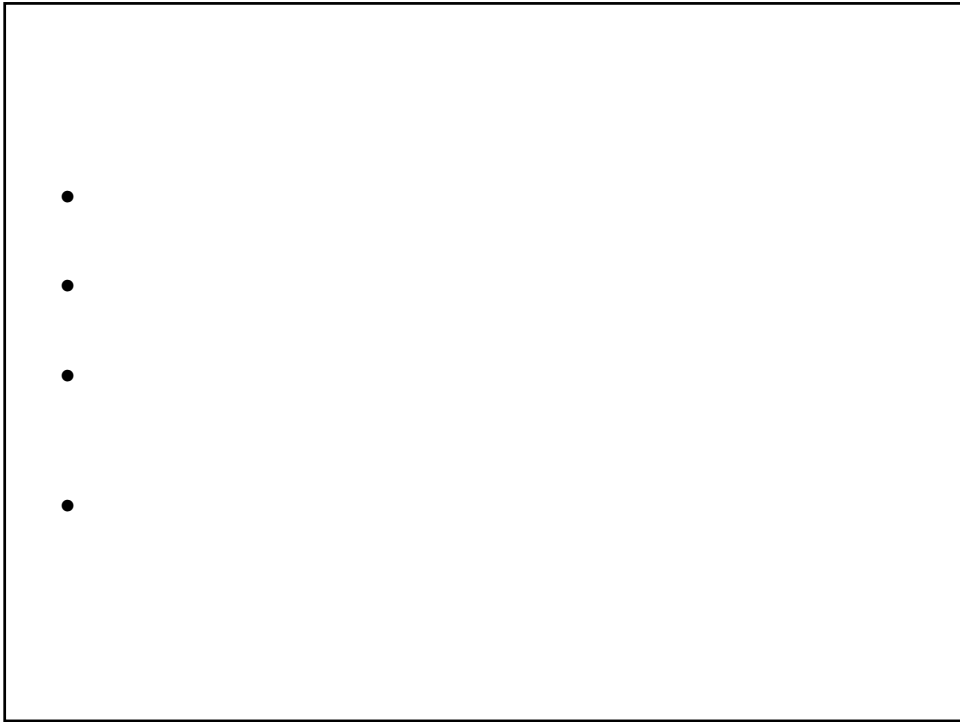
ISMS

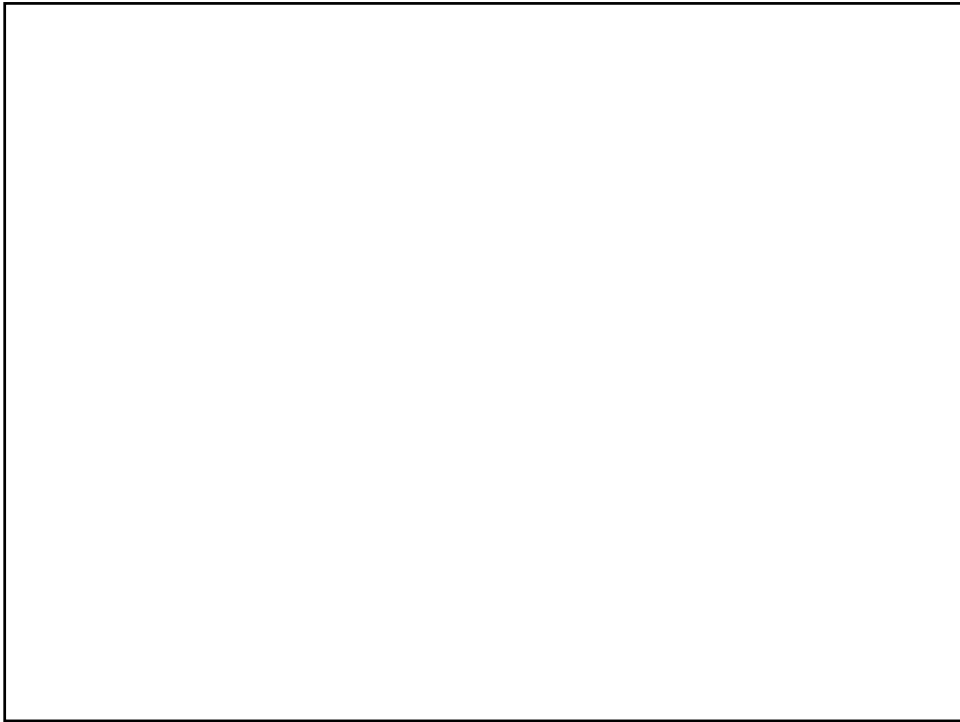
- ISO/IEC27001
 - BS7799
 - BS7799
 - ISMS

- ISO9001
 - ISO9001
ISO 1991
1987

(<http://www.rtri.or.jp/rd/iso14001/iso/iso9001.html>)
- ISO14001
 - ISO 14000
(EMS:Environmental Management Systems)
ISO 14001

(Wikipedia)
-





-
-
-
- University of Birmingham
-
- BP 2005
-
-

(literacy)

- 1 [U]

,

. 2

,

[

]

-

[

]

(literacy)

- Literacy- 1. the quality or state of being literate (educated) 2. an ability to read a short simple passage and answer questions about it. (Webster's Third New International Dictionary)
- media literacy

(Wikipedia

2007/01/16)

- information literacy
- (literacy)
-
-
- Committee on Information Literacy 1 ALA Presidential
- (Wikipedia 2007/01/16)

-
-
- 2005
- —
- —
- —
- —
- — 5
-

Pafrics()

-

-

- <http://research.goo.ne.jp/Result/0306cl25/01.html> 2007/02/16

ID
5

7

ID

ID

4

- NISC National Information Security Center

–

2005.11.17)



-
- risk literacy
- risk communication

-

–

–

-

-

<http://blog.hitachi-system.co.jp/securyman/hitachisecuryman.html>

-