情報セキュリティ・マネジメントの制度設計

２００３年１０月２２日

Network Security Forum 2003

田中秀幸／東京大学社会情報研究所

松浦幹太／東京大学生産技術研究所

本報告の狙いと位置づけ

(狙い)

- 情報セキュリティ技術と社会制度の相互連関に着目しつつ、社会基盤としての施策を提言。
- 具体的には、規制ではなく、民間での経済的動機付けにより、情報セキュリティ投資を確保する情報セキュリティ・マネジメントのあり方を理論的に提示。
- 学際性が進む情報セキュリティ分野での新たな手法を開拓。大胆な政策提言を目指す。

(独創性)

- 「法と経済学」の枠組みを中心として、情報セキュリティ問題を動機付けの点から解明する本格的な研究はこれまでなく、本研究は独創性を有する。

(社会的貢献)

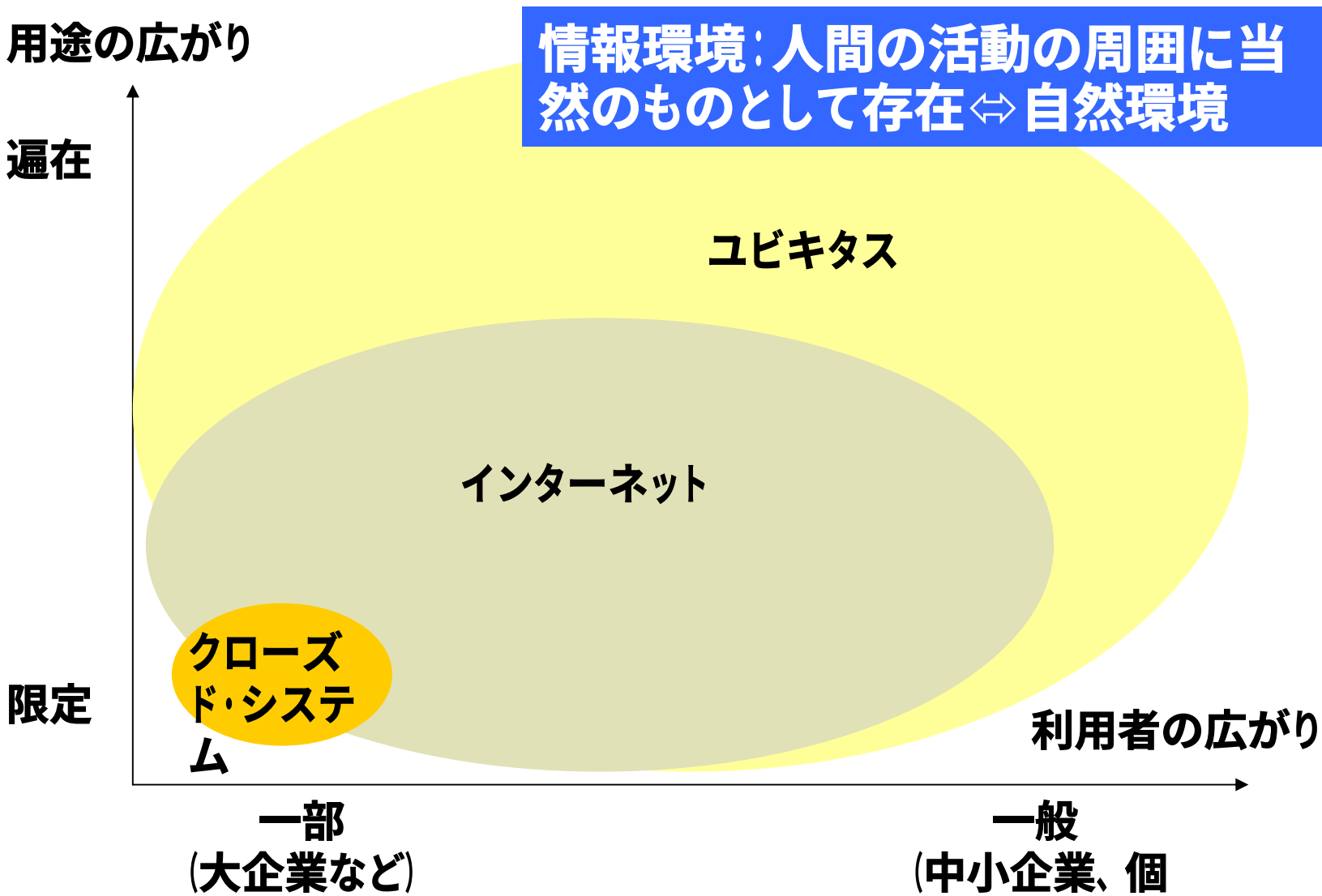
- 本研究は、政府の具体的施策(リスク定量的手法開発)の理論的・学術的意義付けとなる。

本報告の構成

- 環境問題から学ぶべき点
- 外部性：情報セキュリティの相互依存性の検討とそれを踏まえた政策対象の議論
- 規制的手段：セキュリティ確保のための国家規制の可能性
- 経済的手段：所有権ルールと責任ルールの適用。具体的制度としての保険と監査制度。
- 次の課題：リスクの経済的定量化に向けて

環境問題から学ぶべき点

自然環境に近づく情報環境



環境問題の基本的原因＝外部性

- **外部性**

  ある経済主体の活動が、市場取引を経由しない形で直接他の経済主体に影響し、それに対して、何の経済取引も伴わない。

  ↓

  <u>市場の失敗</u>

  ↓

  ＜いかに治癒するか＞

環境政策の4つの手段

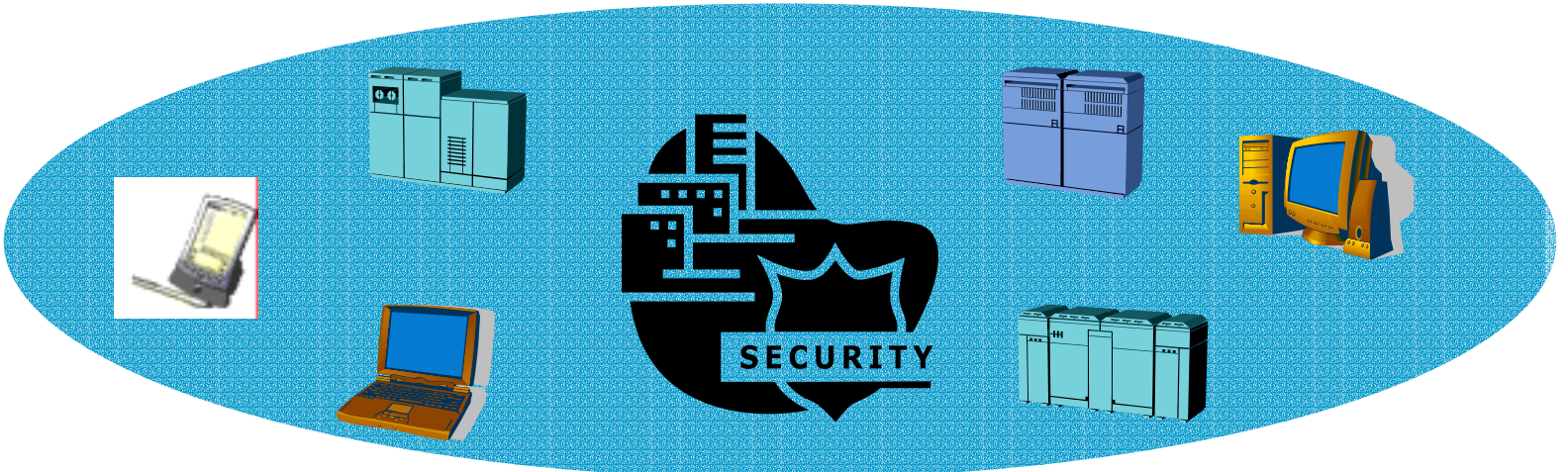
政策手段	自然／地球環境	情報セキュリティ
インフラ整備	一部廃棄物処理施設、研究開発	PKI、電子政府・自治体、研究開発
規制的手段	使用規制、排出規制、技術規制	不正アクセス禁止法、迷惑メール規制法
経済的手段	課税、補助金 排出権取引	(補助金 (優遇税制)) <民間の動機付け>
社会的手段	公教育、情報開示、社会的貢献	情報セキュリティ監査制度、教育

情報セキュリティの相互依存性とその問題

相互依存セキュリティと外部性

- **相互依存セキュリティ**(Kunreuther and Heal[2003])
- **セキュリティ投資／努力水準の決定：他の主体の行動に依存**
- **情報セキュリティ：相互依存的**

(例) ＳＱＬスラマー・ワーム，踏み台など



ユーザーの貢献とセキュリティ水準の問題

- **セキュリティ水準決定の3つのプロトタイプ**
  (Hirshleifer[1983])
  ＝＞1)総和型、2)最小努力依存型、3)最大努力依存型
- **ナッシュ均衡**(Varian[2002])
  ○費用対便益比率がメルクマール
  ○総和型：費用対便益比率の高いユーザーに依存。同比率の低いユーザーはただ乗り。社会的最適解を実現するとは限らない。
  ○最小努力依存型：費用対便益比率の低いユーザーに依存。同比率の高いユーザーの努力は無駄となる(負の外部効果)。
- **対策のターゲット：費用対便益比率の低いユーザー**

費用対便益比率が低い中小企業

便益：小

外部からのアクセスの必要性が低い

・外部公開コンピュータの設置*
　大企業：８１％、中小企業５４％
・外部から内部に業務上アクセス不要*
　大企業：１５％、中小企業３３％

費用：大

固定的費用の負担が相対的に高い

・セキュリティ担当者がいない*
　大企業：１４％、中小企業３０％
・セキュリティ対応せず／わからない
　大規模事業所：１１％、零細事業所３６％**

＝

中小企業ユーザー

総じて、費用対便益比率が低くなる

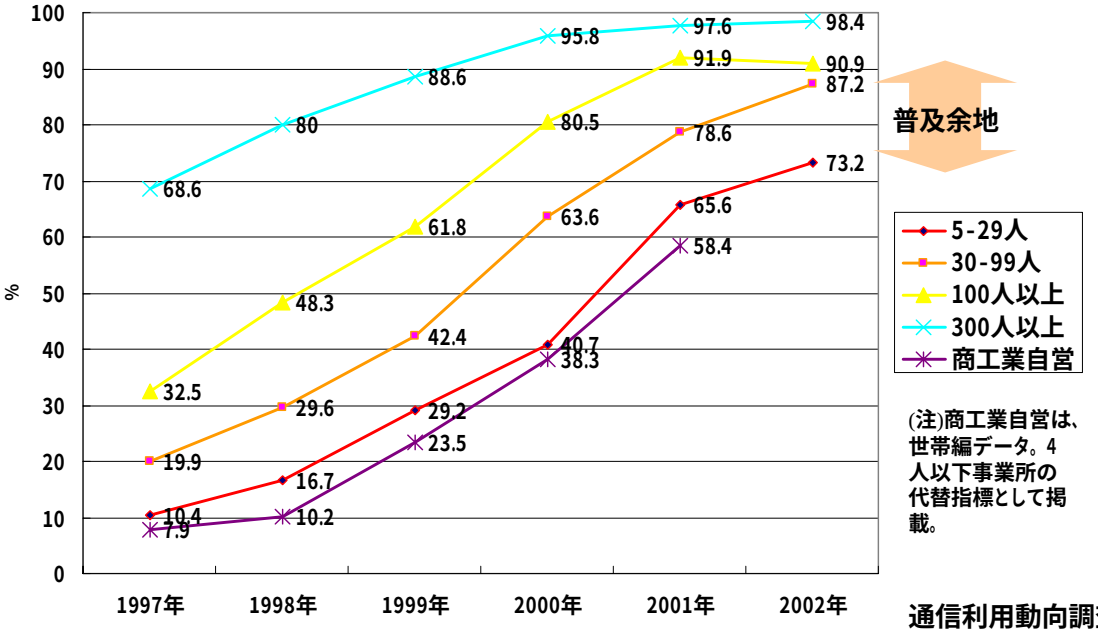
*：三菱総研[2002], **：2002年通信利用動向調査

普及余地がある中小企業

- 小規模な事業者ほど情報通信技術利用の普及の余地が残されている。
- 絶対数としては、小規模な事業者が圧倒的に多い。

→<u>小規模な事業者へのセキュリティ確保の動機付けなどの対応は、相互依存セキュリティの観点からも今後重要。</u>

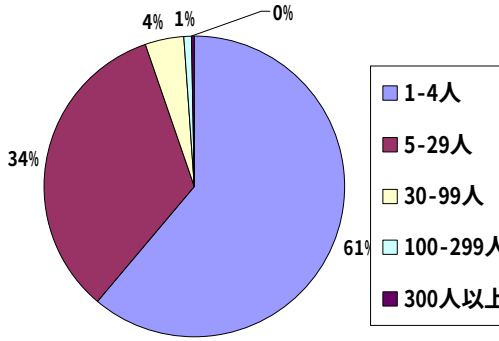
従業者規模別インターネット利用率推移



(注)商工業自営は、世帯編データ。4人以下事業所の代替指標として掲載。

通信利用動向調査により作成

従業者規模別事業所数割合（2001年）

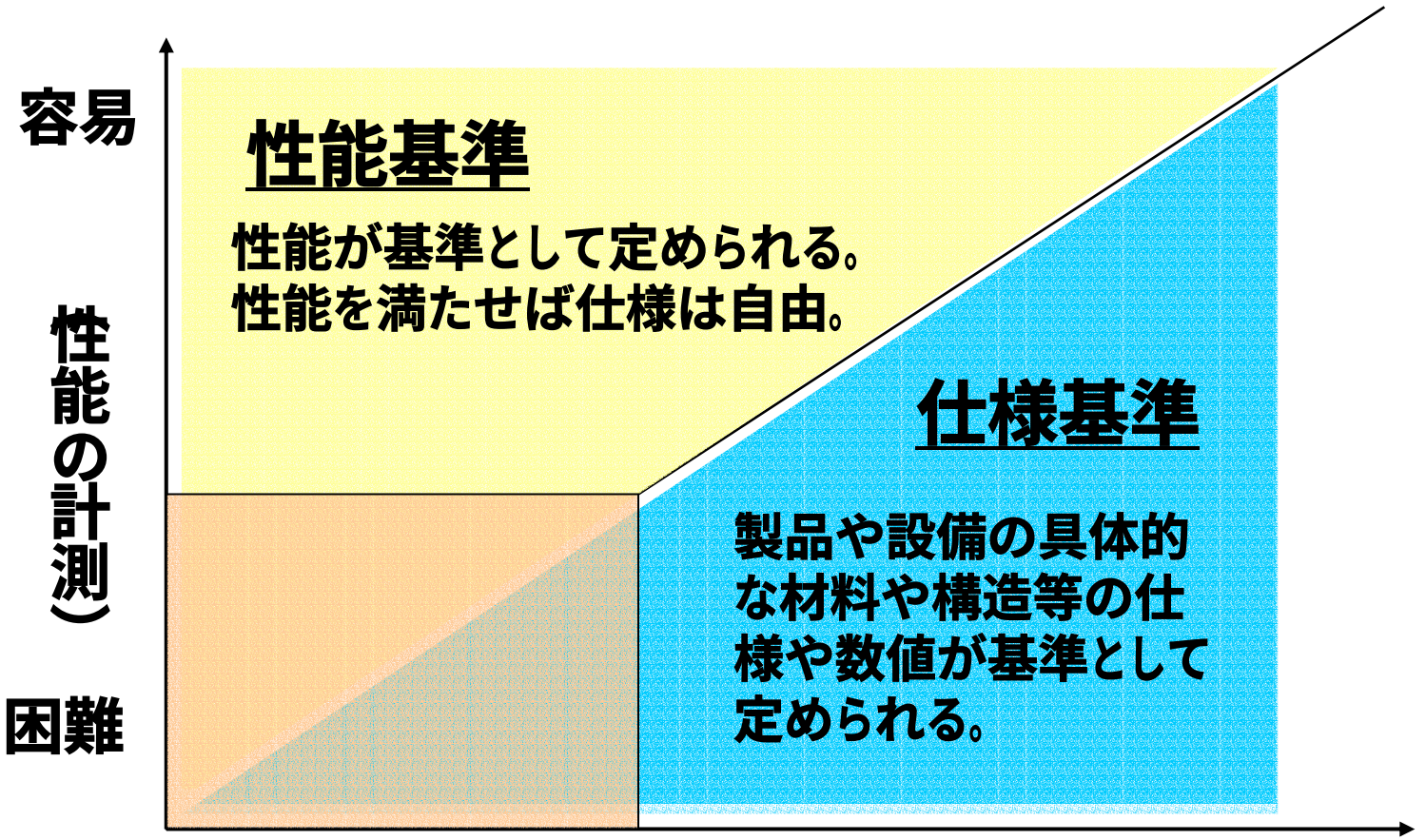


事業所･企業統計調査により作成

規制的手段

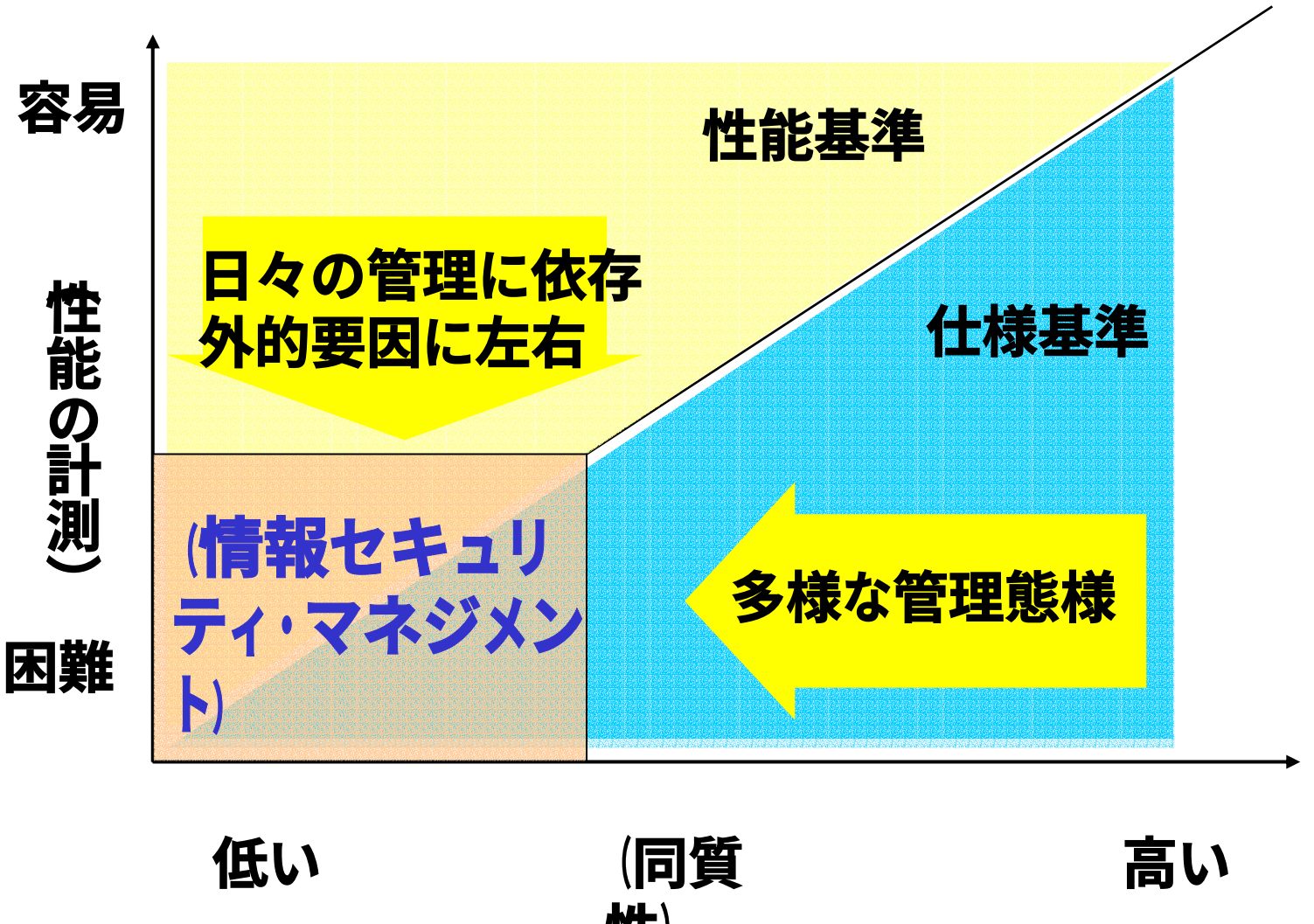
情報セキュリティ確保のための国家規制の可能性

国家による規制基準の態様（仕様基準と性能基準）



Coglianese and Laser[2002]を参考に作成

国家による一律の規制基準設定困難な情報セキュリティ・マネジメント



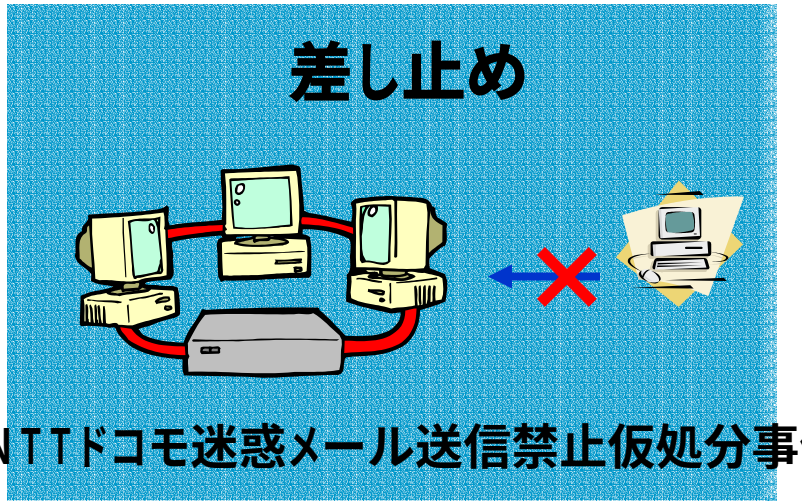
経済的手段

・所有権ルール(property rules)と責任ルール(liability rules)
・保険と監査制度

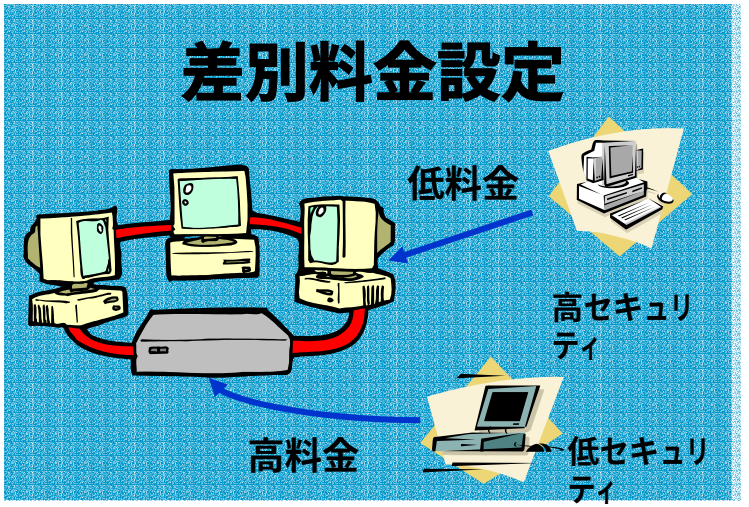
所有権ルールと情報セキュリティ

所有権ルール (property rules)
　外部性をコントロールする権原(entitlement)**を取引対象とすることで、外部性を内部化するルール。**
　環境分野での例：排出権取引

（情報セキュリティでの想定例）



NTTドコモ迷惑メール送信禁止仮処分事件



問題：ネットワーク全体の管理方法

責任ルールと情報セキュリティ

責任ルール (liability rules)

負の外部性が発生した場合に、事後的に発生者に賠償責任を負わせるルール。

環境分野での例：公害訴訟

責任ルールが適用される場合（所有権ルールではなく）

1)**市場での取引費用が高い**（Coase[1960]）

2)**潜在的被害者のリスク回避費用を外部から把握困難**(Kaplow and Shavell[1996])

情報セキュリティ

○情報セキュリティの確保は、外形的基準だけではなく、管理形態に依存＝潜在的被害者が情報優位。

→ 責任ルール適用の可能性

責任ルールの誘因構造と問題点

責任ルールの効果
- ○損害賠償によって事後的に被害者を救済
- ○将来の問題の抑止

賠償責任の所在による事前のセキュリティ投資動機付けの例（A社→B社、B社で損害が発生）

賠償責任なし	無過失責任	過失責任
B社のみ対応	A社のみ対応	A，B社ともに対応

問題点
- ○損害賠償額がA社の資産を大幅に上回る場合（賠償責任があってもA社の対応は動機づけられなくなる）：中小企業
- ○訴訟に要する費用（直接の補償に充当されるのは4割）

責任ルールと保険

責任ルールにおける保険制度の機能

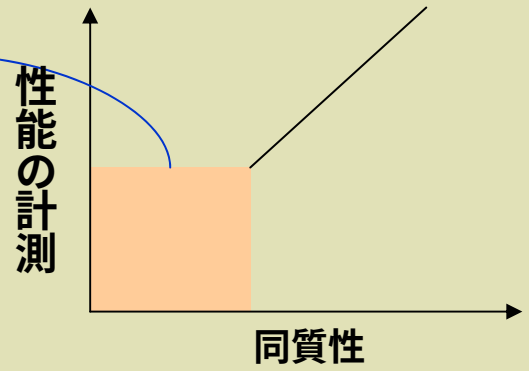
- ■リスク分担機能（多額の賠償への対応）
- ■効率性の確保（2／3が直接の補償に充当）
- ■行政的規制の代替機能

一定の基準の担保 ← 逆選択

事後的な監視 ← モラルハザード

規制の困難さに対応

行政コスト増の回避
（被保険者の負担により実現）



第三者サービスとしての監査制度

情報セキュリティ・リスク水準の計測　←　付保

高度な専門性　多様な管理形態→より多くの専門家

自ら維持することの問題

第三者機能の活用

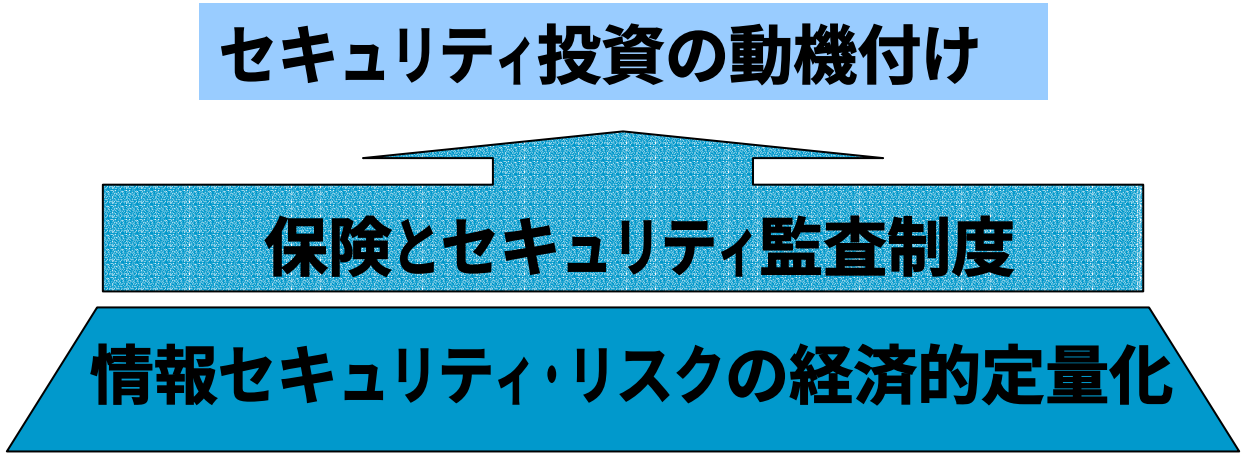
・ソフトウェア等の導入をメルクマールに
・ハード／ソフトウェア企業と提携

・監査制度との組合せ

(利点)
対象の一般化、マネジメント水準、判断の正確性、被害発生時の負担軽減

情報セキュリティ監査制度と保険の補完的活用

リスクの経済的定量化に向けて



次の課題：データの収集とデータに基づくモデルの実用化

【具体的な施策へ】
経済産業省『情報セキュリティ総合戦略』(2003/10)
第3章戦略実現のための具体的施策
「リスクに対する定量的評価手法の開発」

むすび

- 情報セキュリティ・マネジメントの制度設計には、相互依存性（外部性）の考慮が必要。
- 制度設計としては、国家による一律の規制では対応が困難。
- これまで整えられた制度に加えて、民間による経済的手段を中心とする制度が必要となるが、当面の実効性確保には、責任ルールを前提とした保険とセキュリティ監査制度の組合せが有効。
- セキュリティ投資の経済的動機付けを機能させるためは、次なる課題として、リスクの経済的定量化が必要。