ＩＴコーディネータ実務研究会

情報セキュリティガバナンス

2009/ 05/23

大木栄二郎
工学院大学情報学部

目　次

1. 情報セキュリティガバナンスとは
- 経営層と管理者層の間のギャップ

2. 今なぜガバナンスなのか
- 企業価値の変化、経営者の困惑

3. マネジメントとガバナンスの構造
- ガバナンスの構造　DMER

4. 具体的取り組みに向けて
- 誰がギャップを埋めるのか
- 情報セキュリティの可視化の視点

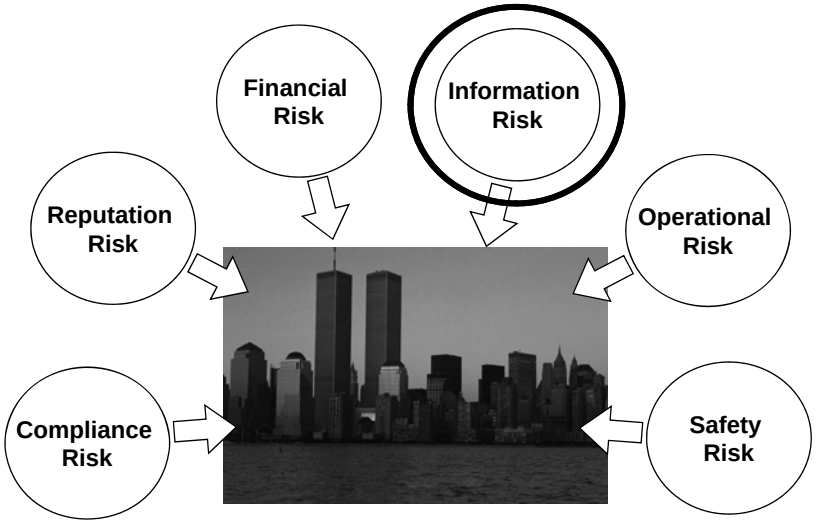
情報セキュリティガバナンスとは

企業経営の主目標は、株主、顧客、取引先、従業員、社会等の利害関係者に対して責任を果たすこと、つまり、「企業価値の向上」及び「社会的責任の遂行」にあり、これを支える重要な取組の一つにリスク管理が位置づけられる。

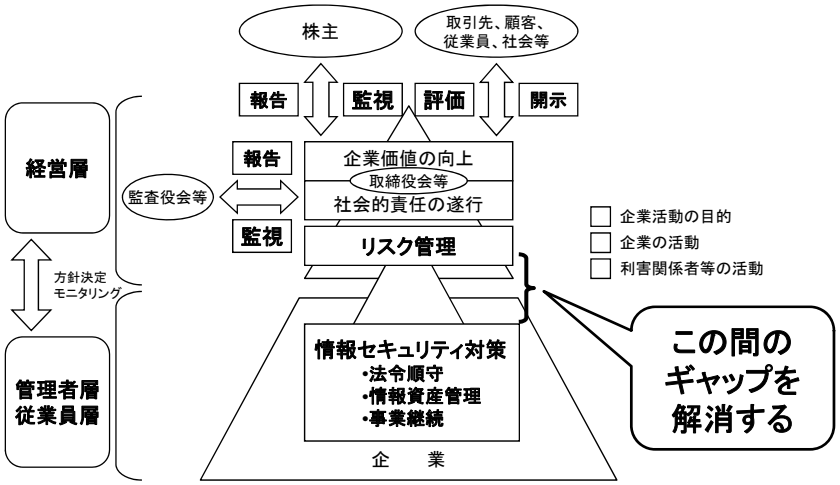
さまざまなリスクの内、情報資産に係るリスクの管理を狙いとして、情報セキュリティに係る意識、取組およびそれらに基づく業務活動を組織内に徹底させるための仕組みを構築・運用することを情報セキュリティ・ガバナンスと位置づける。

産業構造審議会情報セキュリティ基本問題委員会　中間取りまとめ(平成20年6月)　より引用

企業を取り巻くさまざまなリスク

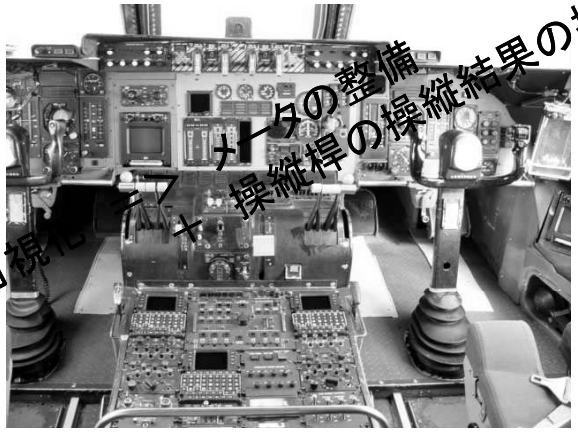


企業における情報セキュリティガバナンスの概念イメージ



産業構造審議会情報セキュリティ基本問題委員会　中間取りまとめ(平成20年6月)　より引用

経営者は企業のコックピットに座って操縦する



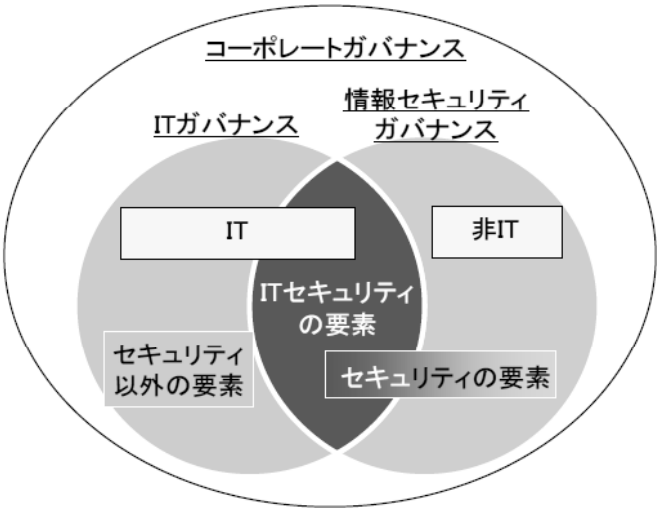
セキュリティがわかる
メータがあるか？

操縦桿で状況をコン
トロールできるか？

⇩

**情報セキュリティ
ガバナンスの確立**

コーポレートガバナンス、ITガバナンス と情報セキュリティガバナンスの関係



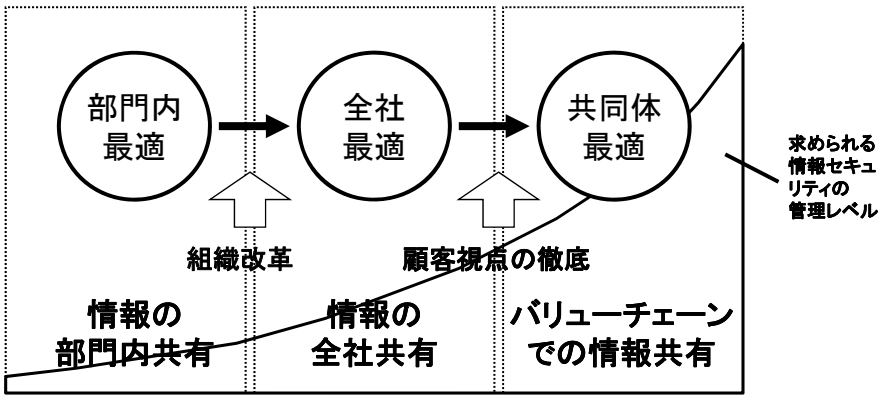
経済産業省 情報セキュリティガバナンス導入ガイダンス(案)より引用

目　次

1. 情報セキュリティガバナンスとは
   - ■ 経営層と管理者層の間のギャップ
2. 今なぜガバナンスなのか
   - ■ 企業価値の変化、経営者の困惑
3. マネジメントとガバナンスの構造
   - ■ ガバナンスの構造　DMER
4. 具体的取り組みに向けて
   - ■ 誰がギャップを埋めるのか
   - ■ 情報セキュリティの可視化の視点

IT投資のステージとセキュリティ

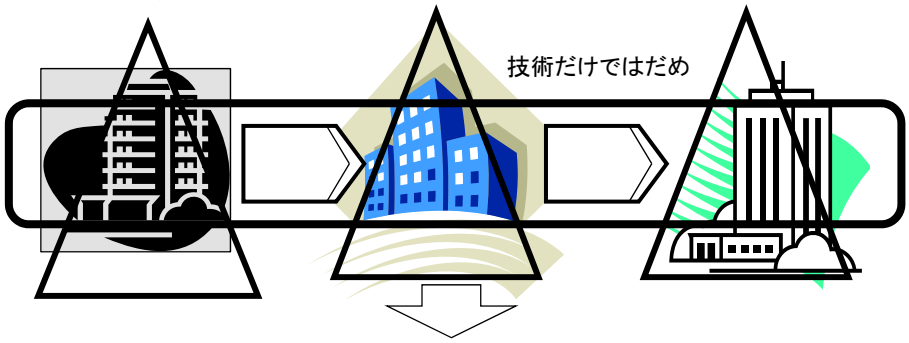
最適化のステージが進むとより高度のセキュリティが求められる



2009/05/23 情報セキュリティガバナンス 9

バリューチェーン全体の情報セキュリティ確保へ

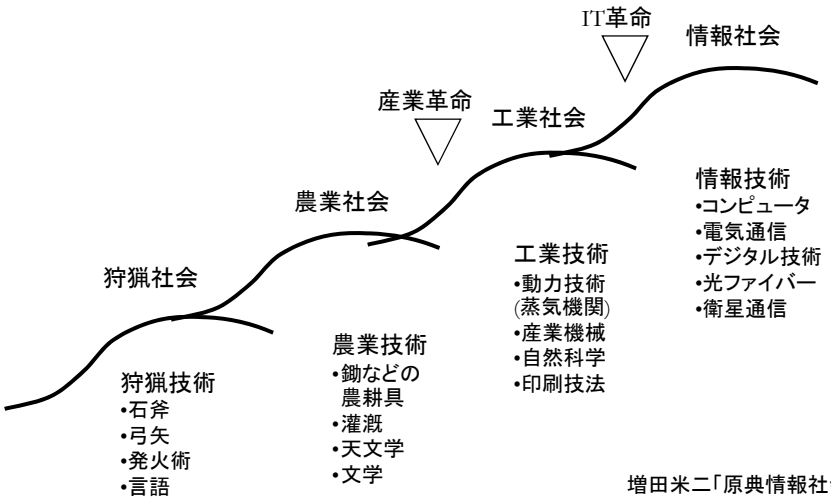
オンデマンド時代は、エンドツーエンドで統合される
多くの場合、重要情報は他社からの預かりもの



一定レベルの情報セキュリティの確保が出来ない企業は、結果としてバリューチェーンから排除されることにならざるを得ない

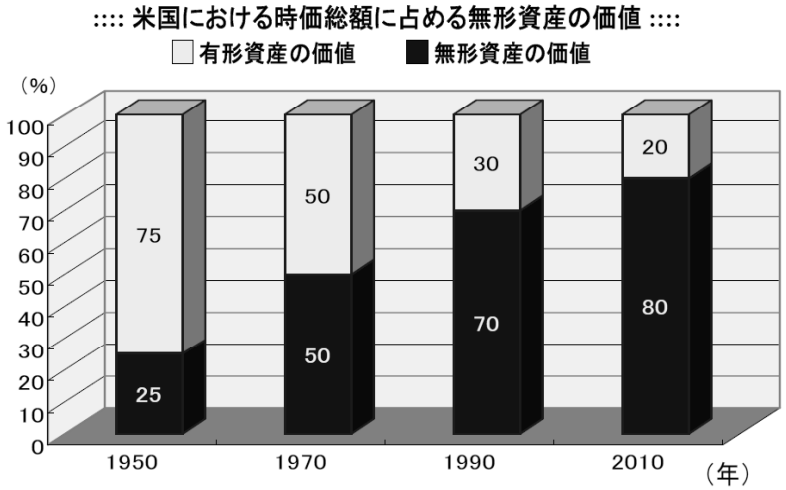
2009/05/23 情報セキュリティガバナンス 10

社会的技術と人類社会の変革



増田米二「原典情報社会」

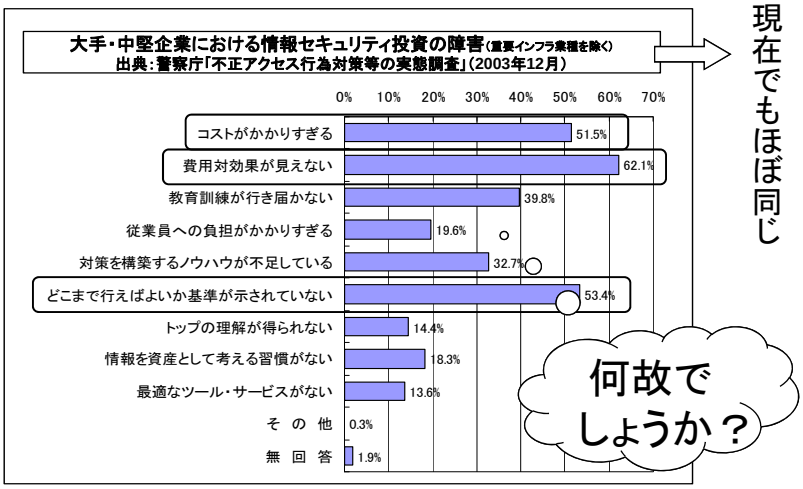
企業価値の変化



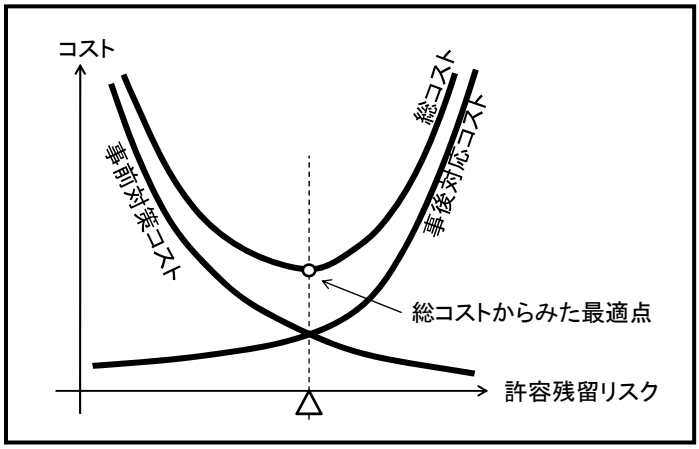
出典:「特許戦略ハンドブック」鮫島正洋 編著

しかし経営者は相変わらず困惑している

ガバナンスが進まない理由に変化なし



最適セキュリティ投資の概念



許容残留リスクとコストとの関係を知る必要がある

目　次

1. 情報セキュリティガバナンスとは
   - ■ 経営層と管理者層の間のギャップ
2. 今なぜガバナンスなのか
   - ■ 企業価値の変化、経営者の困惑
3. マネジメントとガバナンスの構造
   - ■ ガバナンスの構造　DMER
4. 具体的取り組みに向けて
   - ■ 誰がギャップを埋めるのか
   - ■ 情報セキュリティの可視化の視点

2009/05/23　情報セキュリティガバナンス　15

ISO/IEC27001 にみる ISMS の構造

仕組の確立	導入運用	監視見直し	維持改善
1. 適用範囲と境界の定義 2. 基本方針の策定 3. リスクアセスメントの取り組み方法 4. リスクの識別 5. リスクの分析・評価 6. リスク対応の選択肢の評価 7. 管理策の選択 8. 残留リスクの承認 9. 仕組みの承認 10. 適用を宣言 **P**	1. リスク対応計画の策定 2. リスク対応計画の実施 3. 管理策の実施 4. 管理策の有効性評価 5. 教育訓練および認識プログラム 6. 仕組みの運用管理 7. 経営資源の管理 8. インシデント対応 **D**	1. 監視・見直しの手順実施 2. 有効性の定期的見直し 3. 管理策の有効性測定 4. リスクアセスメントの見直し 5. 内部監査の実施 6. マネジメントレビューの実施 7. セキュリティ計画の更新 8. 活動・事象の記録 **C**	1. 改善策の実施 2. 是正措置・予防措置の実施 3. 利害関係者への処置の伝達 4. 改善による意図した目的の達成 **A**

管理策集

2009/05/23　情報セキュリティガバナンス　16

情報セキュリティマネジメントの考え方

国際規格　ISO/IEC 27001 より

経営陣の責任

●経営陣のコミットメント
●経営資源の運用管理

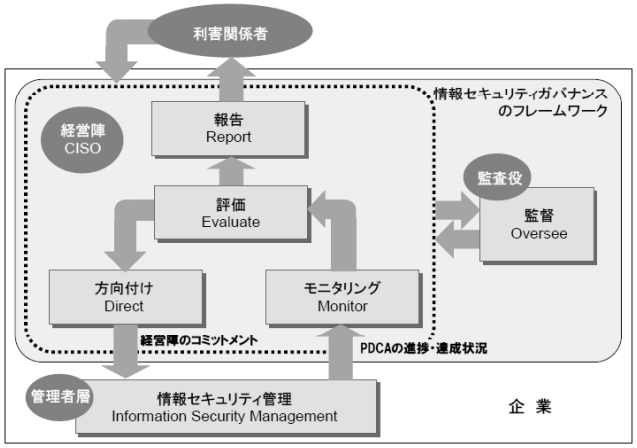
情報セキュリティマネジメント

仕組の確立	管理策の導入運用	監視と見直し	仕組の維持と改善
Plan	Do	Check	Act

a. 基本方針を確立する
b. 目的を定め、計画の策定を指示する
c. 情報セキュリティに対する役割や責任を定める
d. 情報セキュリティの重要性を組織内に周知する
e. 必要な経営資源を提供する
f. リスク受容の基準、受容可能なリスクの水準を決める
g. 内部監査の実施を指示し支援する
h. 経営者の視点からレビューを実施する

2009/05/23　情報セキュリティガバナンス　17

ガバナンスの構造



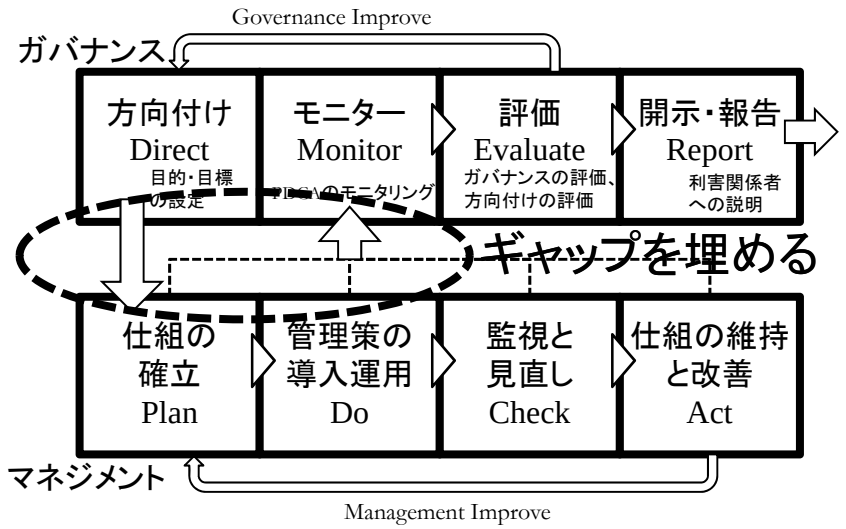
経営陣の活動モデルを提示する

マネジメントシステムとの関係を明示する

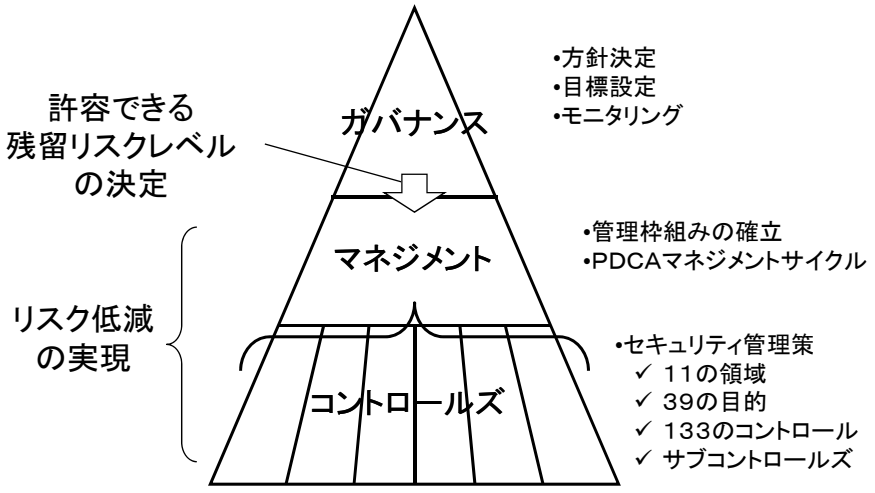
経済産業省　情報セキュリティガバナンス導入ガイダンス（案）より引用

2009/05/23　情報セキュリティガバナンス　18

ガバナンスとマネジメントの構造



ガバナンス、マネジメント、コントロール



目　次

1. 情報セキュリティガバナンスとは
   - 経営層と管理者層の間のギャップ
2. 今なぜガバナンスなのか
   - 企業価値の変化、経営者の困惑
3. マネジメントとガバナンスの構造
   - ガバナンスの構造　DMER
4. 具体的取り組みに向けて
   - 誰がギャップを埋めるのか
   - 情報セキュリティの可視化の視点

2009/05/23　情報セキュリティガバナンス　21

GとMのGAPをつなぐのは誰か

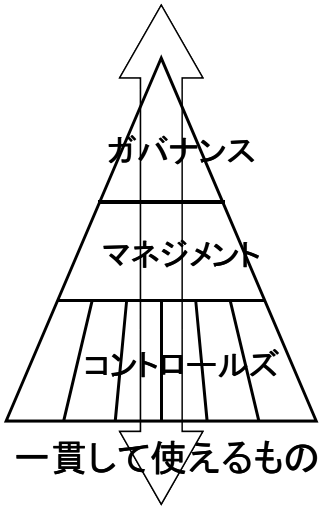
- **GAP Fill の役割を担うのは誰か**
  - **企業/企業グループの CISO**（Chief Information Security Officer）**が、経営若しくはそれに近い立場からこのリスク管理方針を情報セキュリティ分野において解釈し、情報セキュリティ目的・目標の設定と、その実現に必要な体制（権限や責任）や経営資源の提供を図る**
- **CISO**：**役員級若しくは部長級の人材が担当するケースが多い。企業によっては、**CIO(Chief Information Officer)**や**CSO(Chief Security Officer)**、**CPO（Chief Privacy Officer）**が兼ねるケースもある。**

➔ **CISOの任命、および職責と権限の明確化**

2009/05/23　情報セキュリティガバナンス　22

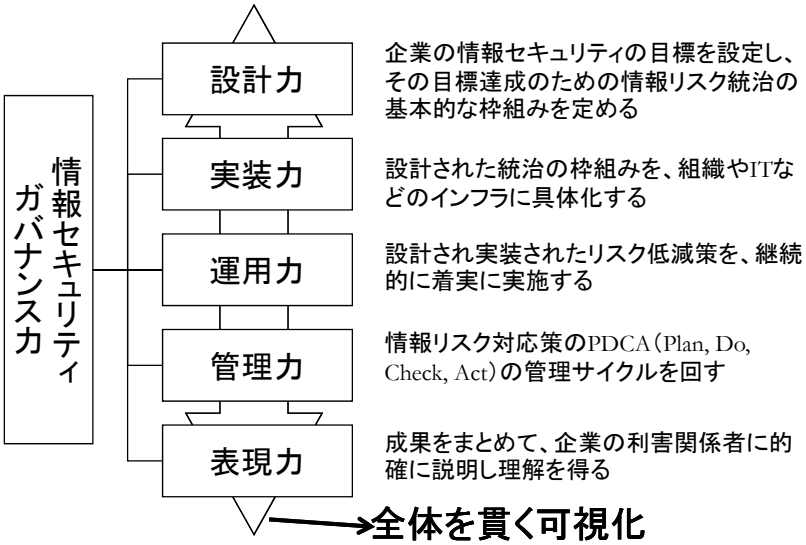
ガバナンスの視点から求められる可視化

- リスク判断に直結するもの
- マネジメントの目標を設定するもの
- コントロールの設計目標にまでブレークダウン可能なもの
- 現状の評価結果からリスク評価につながるもの



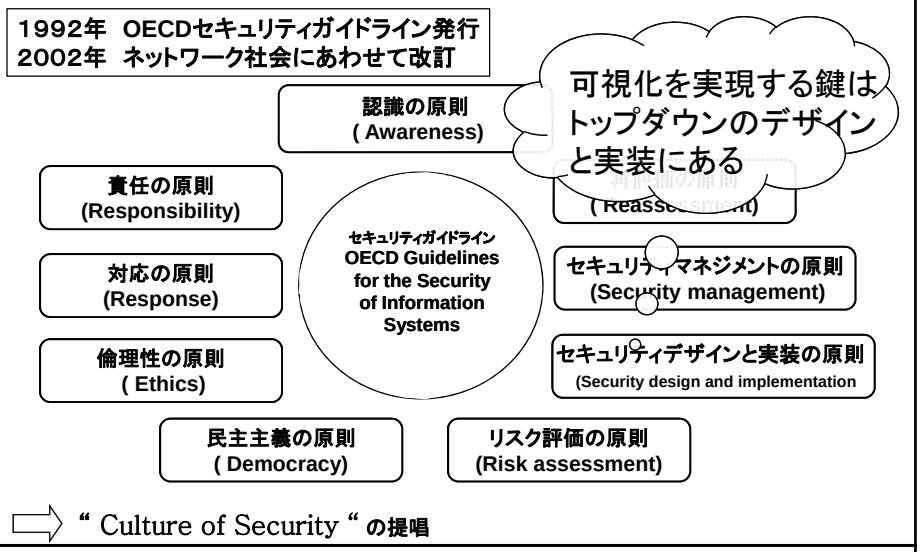
2009/05/23 情報セキュリティガバナンス 23

情報セキュリティガバナンスはリスク統治能力



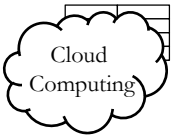
2009/05/23 情報セキュリティガバナンス 24

セキュリティデザインと実装が鍵を握る



ガバナンスについての私見

- Technologyが社会革命を起こす
  - Technologyのガバナンスが大事
  - そのうちTechnologyが当たり前になる
    - その効果がガバナンス対象の変化を起こす



- IT GovernanceからInformation Governanceへ
  - 現実に起きている現象（表層）
  - マクロの歴史的トレンド（底流）
  - 本質は何か
- ガバナンスの構造はガバナンス対象によらず普遍か？
  - ガバナンスの対象が変化
  - 物の統治のための構造、金の統治のための構造と、情報統治のための構造は異なるのではないか

おわり

ありがとうございました

Eijiroh Ohki

Professor,

Faculty of Informatics, Kogakuin University

eohki@cc.kogauin.ac.jp