情報セキュリティと
日本的経営におけるガバナンス

外部委託における
ISMS等の認証制度の活用

日本ヒューレット・パッカード株式会社
個人情報保護対策室　佐藤　慶浩
2010年6月17日

発表者紹介

佐藤　慶浩（さとう　よしひろ）
日本ヒューレット・パッカード　個人情報保護対策室　室長
（併任）内閣官房 情報セキュリティ指導専門官

社外活動
- JIPDEC　ﾌﾟﾗｲﾊﾞｼｰﾏｰｸ運営要領改正委員会　委員
- (社)ｺﾝﾋﾟｭｰﾀｿﾌﾄｳｪｱ協会　ﾌﾟﾗｲﾊﾞｼｰﾏｰｸ審査判定委員会　委員
- JIPDEC　ISMS適合性評価制度技術専門部会　委員
- 杉並区　住基ネット運用監視委員会　委員
- 経済産業省 個人情報保護ガイドラインQ＆A集検討会　元委員

本日の資料
http://yosihiro.com/

twitter
http://twitter.com/4416_310

2　

発表内容（以下の報告書から）

社会技術研究開発事業
研究開発領域「情報と社会」
研究開発プログラム「ユビキタス社会のガバナンス」

研究開発プロジェクト
「企業における情報セキュリティの実効性ある
ガバナンス制度のあり方」

研究開発実施終了報告書

研究開発期間　平成19年7月～平成21年12月

研究代表者氏名　林 紘一郎
(情報セキュリティ大学院大学　学長・教授)

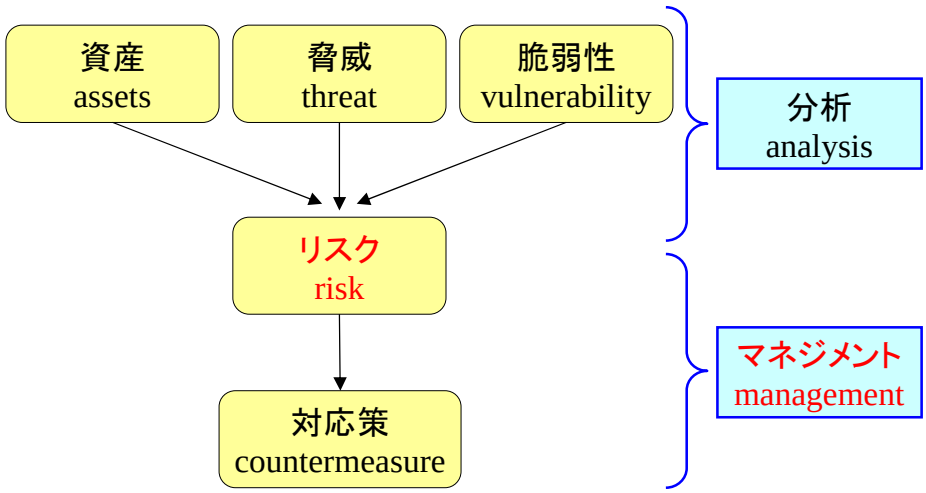
3　©2010

「企業における情報セキュリティの実効性ある ガバナンス制度のあり方」報告書

- 5.4 外部委託におけるISMS認証制度の活用
- 5.5 外部委託の種類
- 5.6 マネジメントシステムに係る認証制度
  - 5.6.1 対策のマネジメントシステムと対策レベルの違い　　存在リスク　残存リスク　許容レベル
  - 5.6.2 リスクの許容レベルの安定性　　許容リスク
- 5.7 組織のマネジメントシステムと委託先の関係
  - 5.7.1 業務委託関係と情報提供関係　　片務か双務　提供先の管理
  - 5.7.2 リスクの許容レベルの一貫性
- 5.8 現状の問題と適切な活用方法
  - 5.8.1 散見される問題
  - 5.8.2 適切な指示
  - 5.8.3 指示の適切な時制
  - 5.8.4 法制度検討時の留意事項

4　©2010

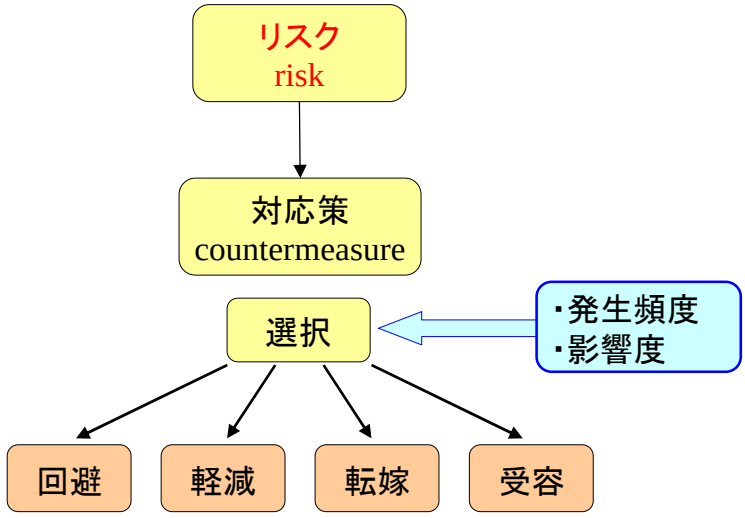
リスクマネジメントとは？



出典：CRAMM(CCTA Risk Analysis and Management Method)

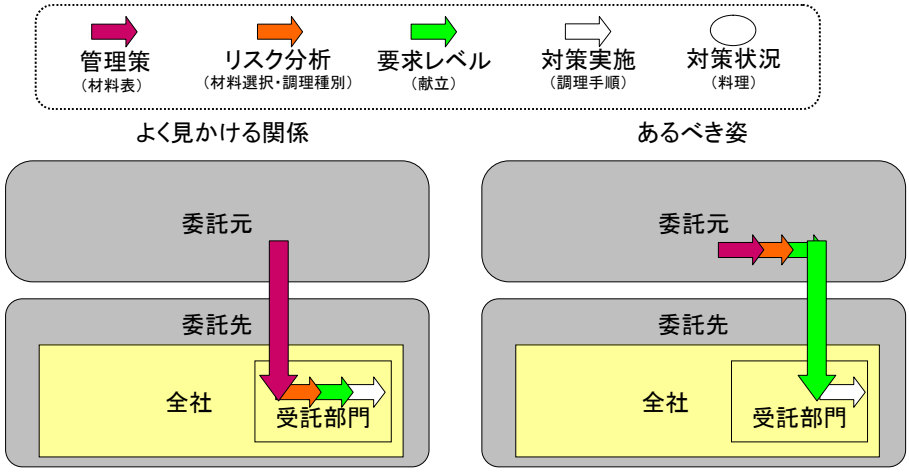
5 ©2010

リスクマネジメントとは？



6 ©2010

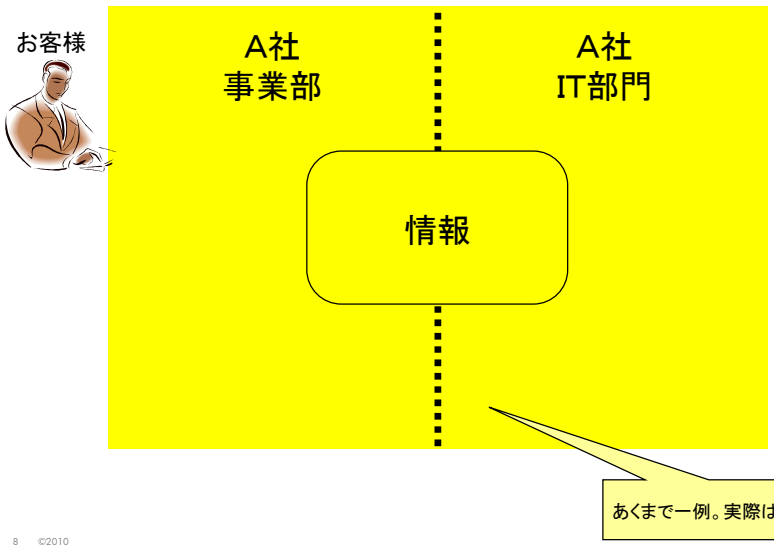
「適切な指示」の問題
例）27002を引用した場合のISMSと外部委託



ただし、リスク管理能力について、委託元≫委託先という暗黙の前提に注意を要する

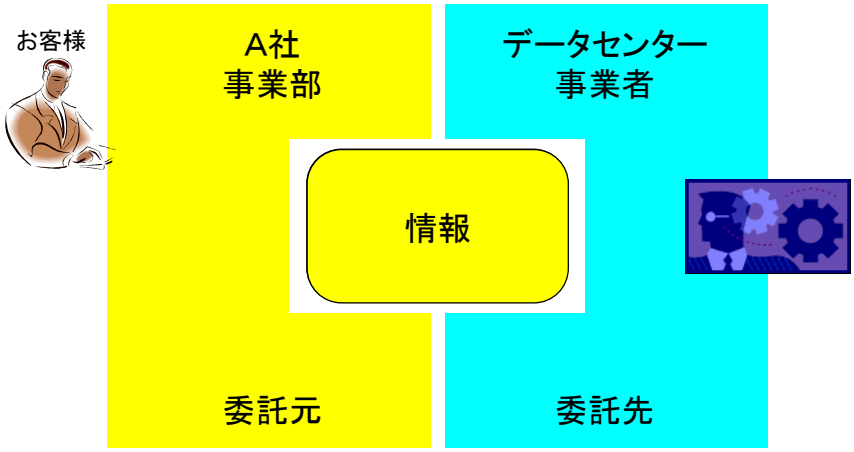
7 ©2010

「指示の適切な時制」の問題
例）外部委託のない場合の情報の責任所在



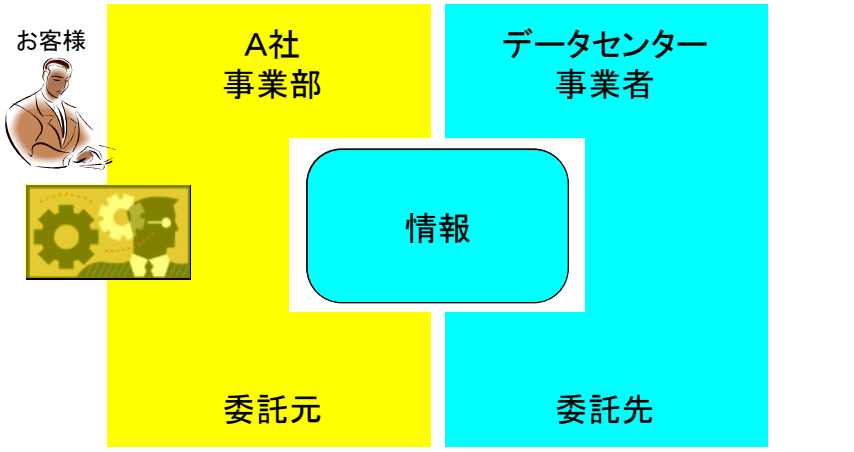
8 ©2010

「指示の適切な時制」の問題
例）外部委託する情報の責任所在



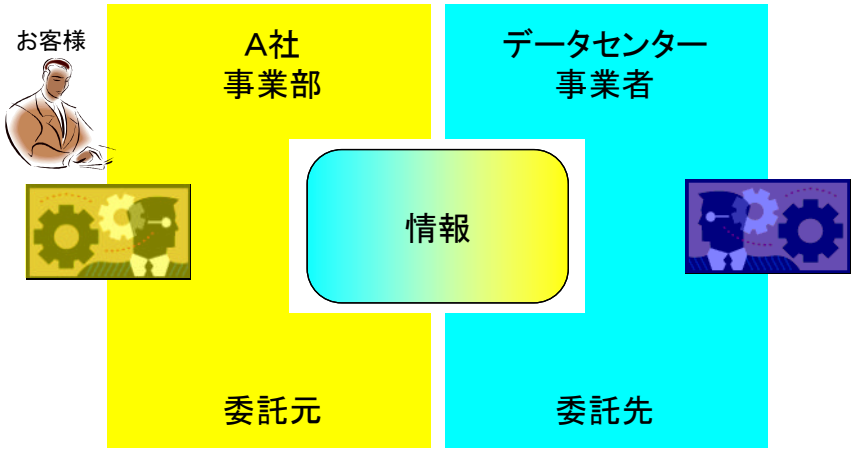
9 ©2010

「指示の適切な時制」の問題
例）外部委託する情報の責任所在



10 ©2010

「指示の適切な時制」の問題
例）外部委託する情報の責任所在



11 ©2010

外部委託についての再考の必要性

再確認すべき事項：

■委託先における情報セキュリティマネジメントシステムについて、リスクマネジメントの視点で再確認することが重要である。

■自身で実施できないことを監督できるのか？

■社員のできることを委託するならば、
　■期待効果＝処理量拡大→標準化作業は処理費軽減

■社員のできないことを委託するならば、
　■期待効果＝委託先の付加価値だったはず
　　■付加価値のあることを安く済ませるのか？
　　■未経験者が経験者を監督するのか？
　　■・・・ITゼネコンの構造的破綻？？？

12 ©2010