情報ネットワーク法学会　研究大会

外部委託及びクラウドにおける情報セキュリティマネジメントシステム適合性評価の利用

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12月11日

©2010

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

©2010

関連研究

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)

©2010

外部委託及びクラウドにおける情報セキュリティマネジメントシステム適合性評価の利用

- (1) どのような契約で実施するのか？ How
- (2) どこで業務を実施するのか？ Where
- (3) どの時点を保証させるのか？ When
- (4) どちらがリスク評価するのか？ Who
- (5) どのようなデータを取り扱う業務を実施するのか？ What
- (6) 誰が対策を実施するのか？ Who
- (7) 委託する業務の付加価値は誰にあるのか？ Why

 ©2010

外部委託及びクラウドにおける情報セキュリティマネジメントシステム適合性評価の利用

- (1) どのような契約で実施するのか？ How
- (2) どこで業務を実施するのか？ Where
- (3) どの時点を保証させるのか？ When
- (4) どちらがリスク評価するのか？ Who
- (5) どのようなデータを取り扱う業務を実施するのか？ What
- (6) 誰が対策を実施するのか？ Who
- (7) 委託する業務の付加価値は誰にあるのか？ Why

 ©2010

外部委託及びクラウドにおける情報セキュリティマネジメントシステム適合性評価の利用

- (1) どのような契約で実施するのか？ How
- (2) どこで業務を実施するのか？ Where
- (3) どの時点を保証させるのか？ When
- (4) どちらがリスク評価するのか？ Who
- (5) どのようなデータを取り扱う業務を実施するのか？ What
- (6) 誰が対策を実施するのか？ Who
- (7) 委託する業務の付加価値は誰にあるのか？ Why

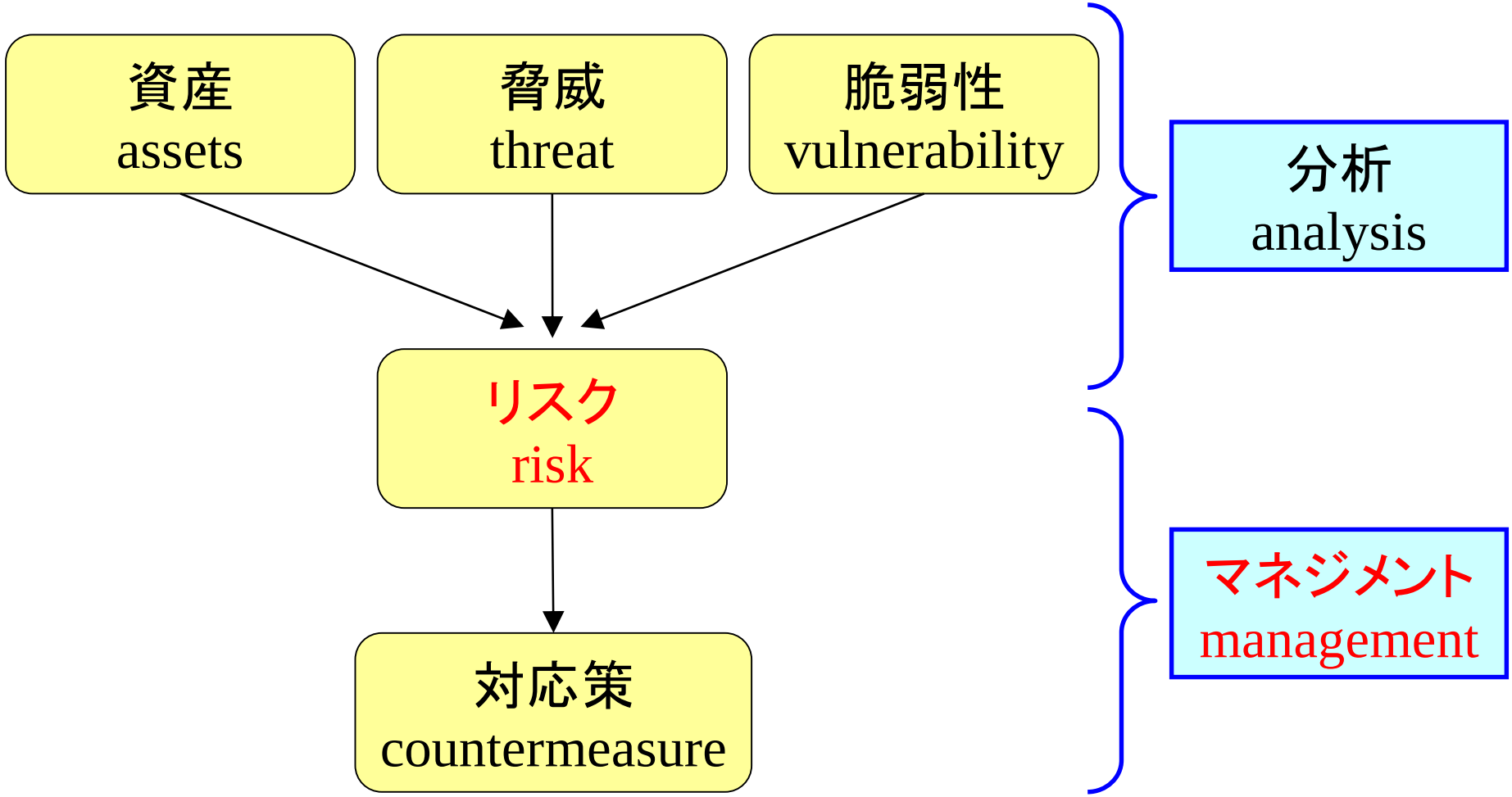
 ©2010

外部委託及びクラウドにおける情報セキュリティマネジメントシステム適合性評価の利用

- (1) どのような契約で実施するのか？ How
- (2) どこで業務を実施するのか？ Where
- (3) どの時点を保証させるのか？ When
- (4) どちらがリスク評価するのか？ Who
- (5) どのようなデータを取り扱う業務を実施するのか？ What
- (6) 誰が対策を実施するのか？ Who
- (7) 委託する業務の付加価値は誰にあるのか？ Why

 ©2010

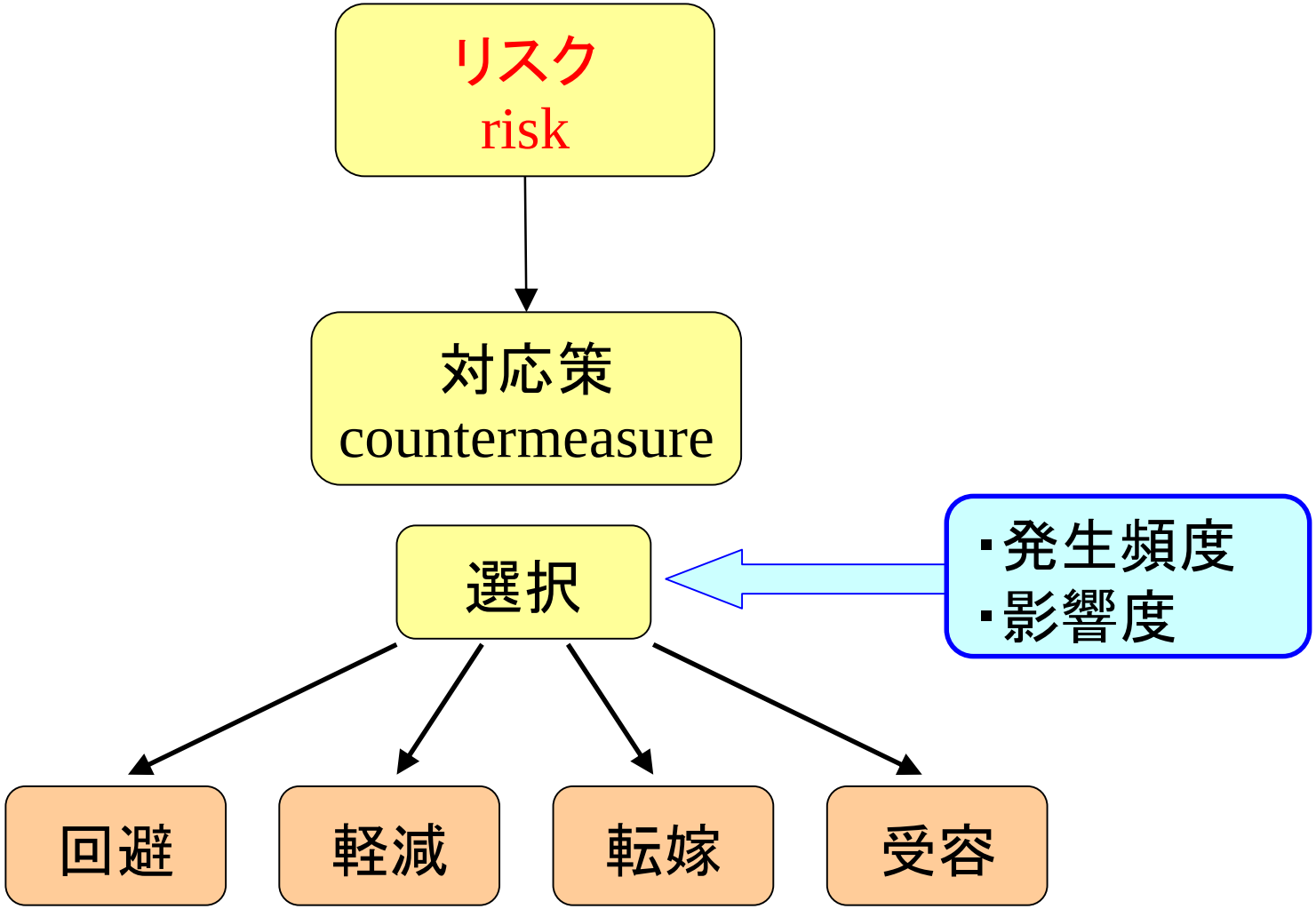
リスクマネジメントとは？



出典：CRAMM(CCTA Risk Analysis and Management Method)

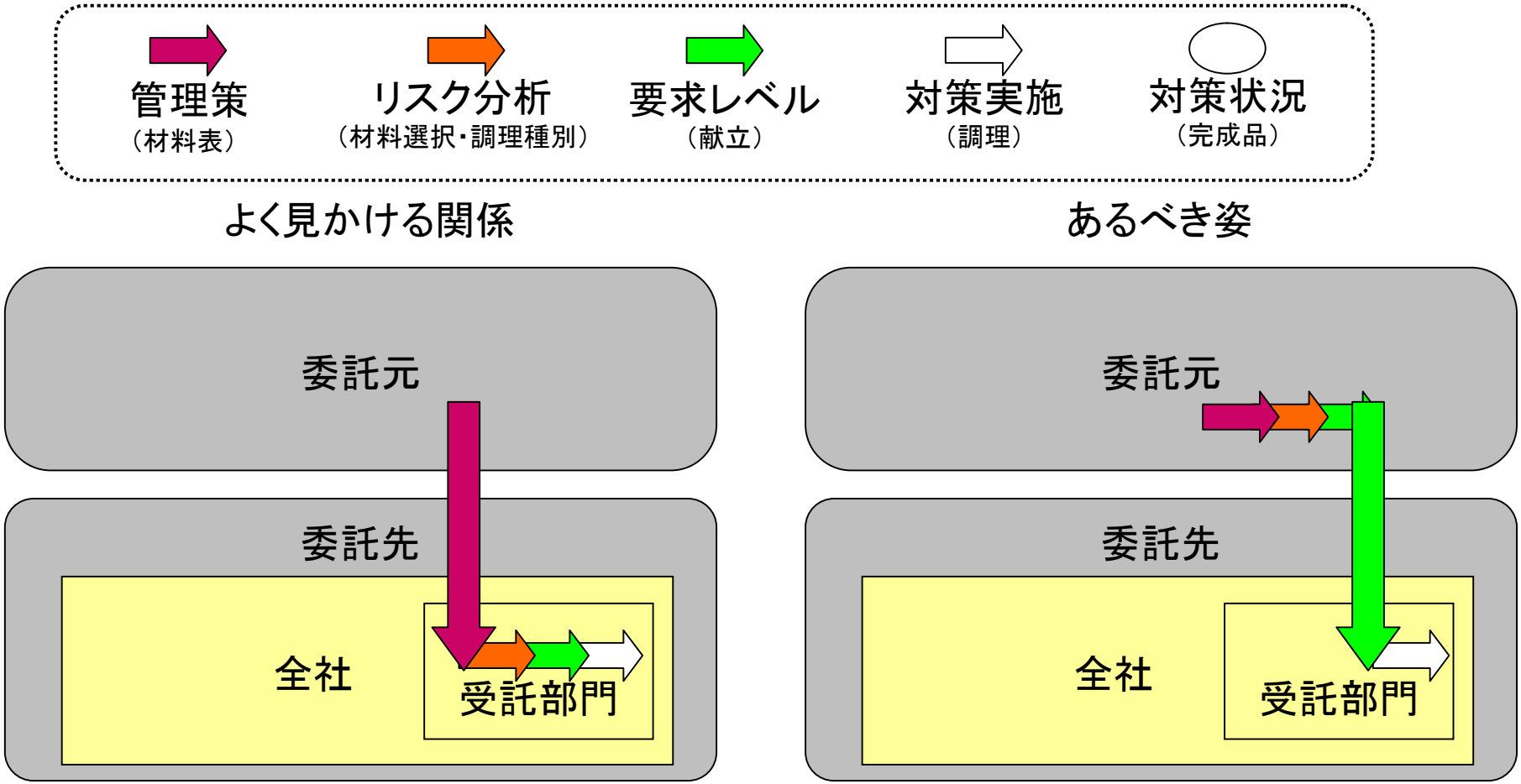
©2010

リスクマネジメントとは？



©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

 ©2010

外部委託及びクラウドにおける情報セキュリティマネジメントシステム適合性評価の利用

- (1) どのような契約で実施するのか？ How
- (2) どこで業務を実施するのか？ Where
- (3) どの時点を保証させるのか？ When
- (4) どちらがリスク評価するのか？ Who
- (5) どのようなデータを取り扱う業務を実施するのか？ What
- (6) 誰が対策を実施するのか？ Who
- (7) 委託する業務の付加価値は誰にあるのか？ Why

 ©2010

外部委託及びクラウドにおける情報セキュリティマネジメントシステム適合性評価の利用

- (1) どのような契約で実施するのか？ How
- (2) どこで業務を実施するのか？ Where
- (3) どの時点を保証させるのか？ When
- (4) どちらがリスク評価するのか？ Who
- (5) どのようなデータを取り扱う業務を実施するのか？ What
- (6) 誰が対策を実施するのか？ Who
- (7) 委託する業務の付加価値は誰にあるのか？ Why

 ©2010

外部委託及びクラウドにおける情報セキュリティマネジメントシステム適合性評価の利用

- (1) どのような契約で実施するのか？ How
- (2) どこで業務を実施するのか？ Where
- (3) どの時点を保証させるのか？ When
- (4) どちらがリスク評価するのか？ Who
- (5) どのようなデータを取り扱う業務を実施するのか？ What
- (6) 誰が対策を実施するのか？ Who
- (7) 委託する業務の付加価値は誰にあるのか？ Why

 ©2010

委託する業務の付加価値は誰にあるのか？

再確認すべき事項:

■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

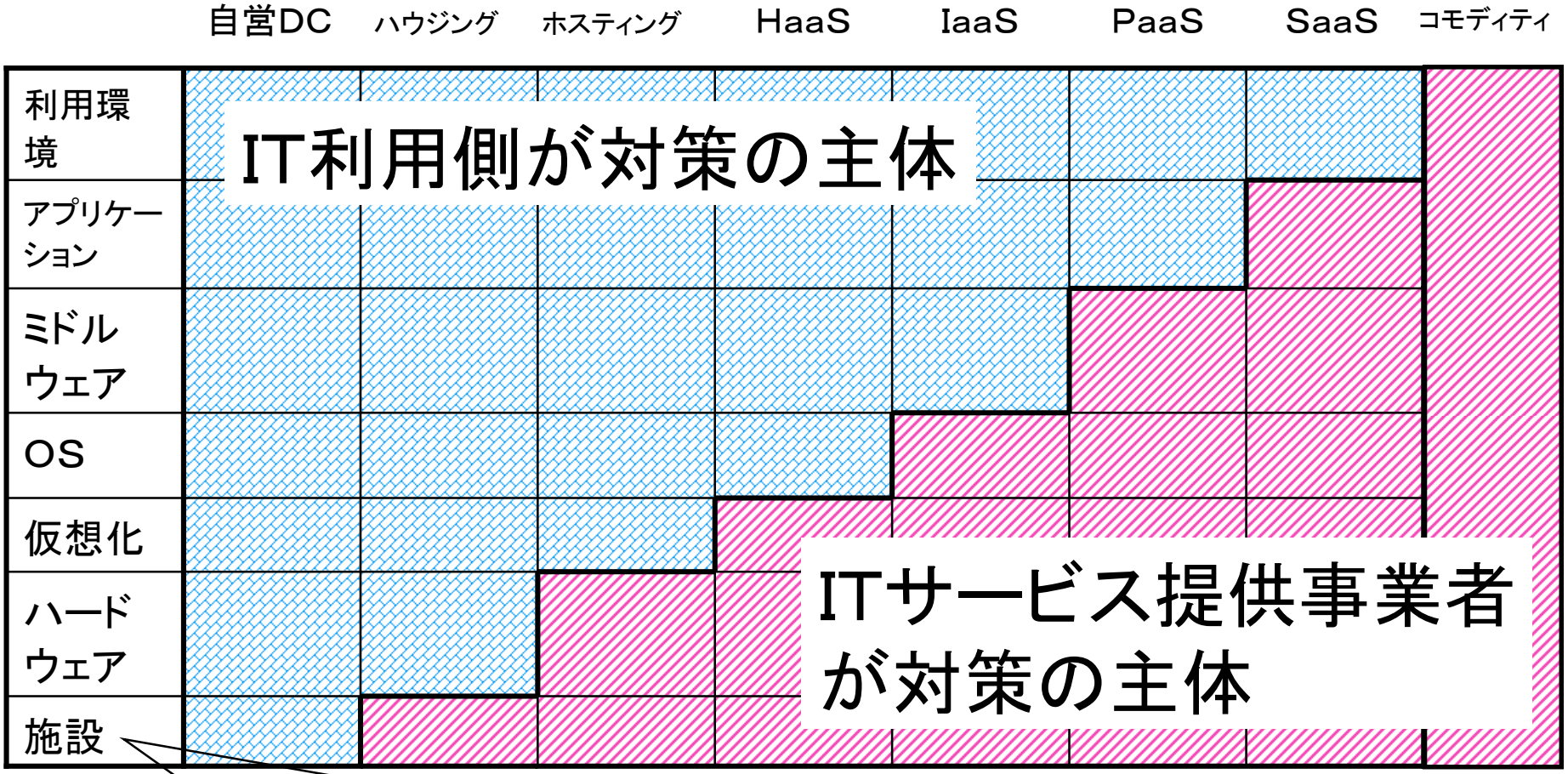
　　■付加価値のあることを安く済ませるのか？

　　■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？？？

 ©2010

クラウド
ITサービス形態とセキュリティ対策主体の関係



各階層でのリスク管理に違いはない。
対策実施主体が異なる。
提供されるサービスレベルにより、リスク対応策は異なる結果になり得る。

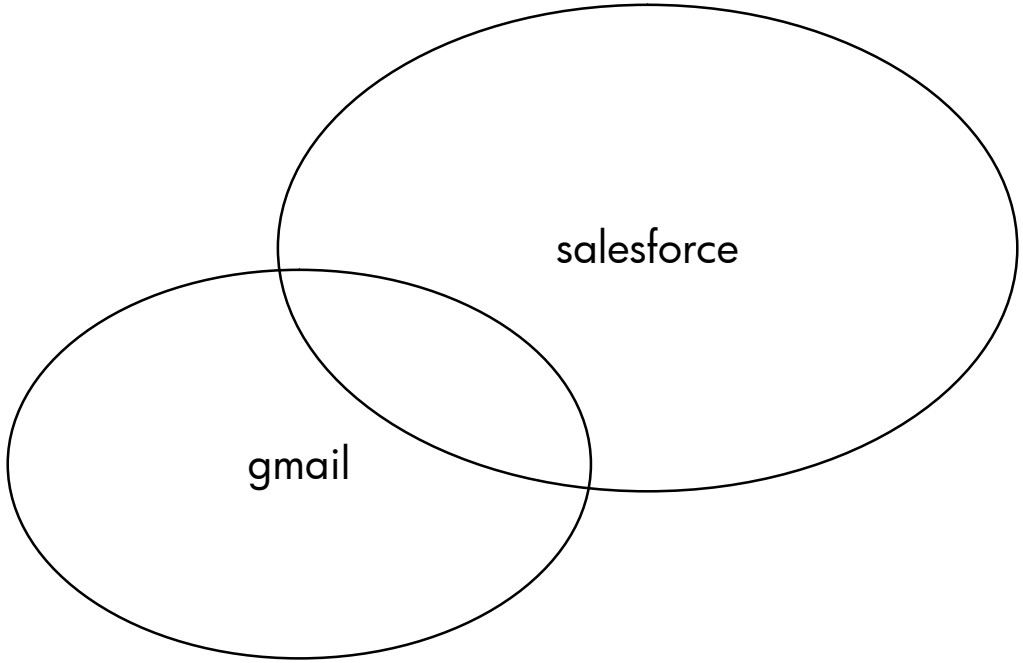
 ©2010

クラウド
影響範囲と契約者・契約形態の関係

影響範囲に係るリスク評価に影響

- 組織外への業務サービス提供に利用
- チーム間利用
- チーム内利用
- 個人作業に利用

影響範囲 広 ↕ 狭



Where

How

無償登録 ↔ 定形約款 ↔ 個別契約

契約の有無に係るリスク評価に影響

Who

個人 ↔ IT部門以外 ↔ IT部門

IT利用側でリスク管理する者が誰であるかに影響

©2010

クラウド
ITサービス形態選択とリスク管理の枠組み

Enabled service

Enabling technology

Why

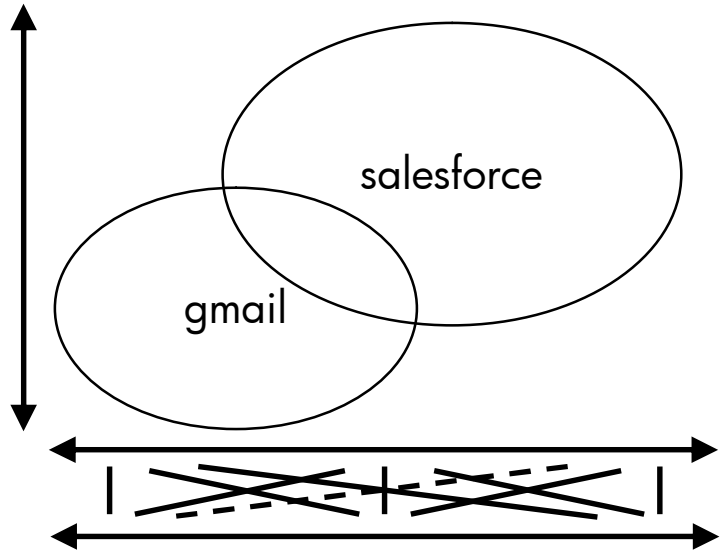
When

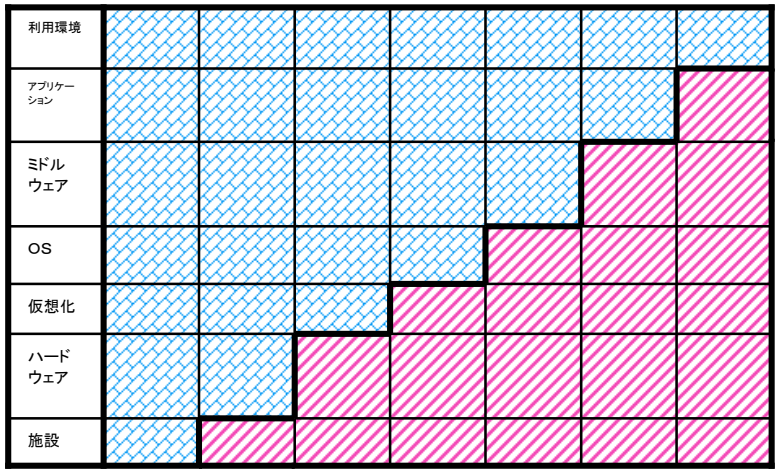
Where

How

Who

What





 ©2010