委託先における
情報セキュリティ対策のあり方と
認証制度の関係

日本ヒューレット・パッカード
佐藤　慶浩

講演者

佐藤　慶浩　（さとう　よしひろ）

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　室長

現在、内閣官房情報セキュリティセンター内閣参事官補佐を併任。
その他に、27000シリーズなどを規格するISO/IEC JTC1/SC27委員会の国際委員、国内ISMS認証の技術専門部会委員、プライバシーマーク認証の判定委員を務めている。

詳細は、http://yosihiro.com/profile/　に掲載。

講演内容

- リスクマネジメントとは
- リスクマネジメントと業務の関係
- リスクマネジメントの集中管理
- リスクマネジメントとしての情報セキュリティ
- 情報セキュリティの傾向と課題
- 委託先における情報セキュリティ対策のあり方と認証制度の関係

リスクマネジメントとは？

資産
assets

脅威
threat

脆弱性
vulnerability

分析
analysis

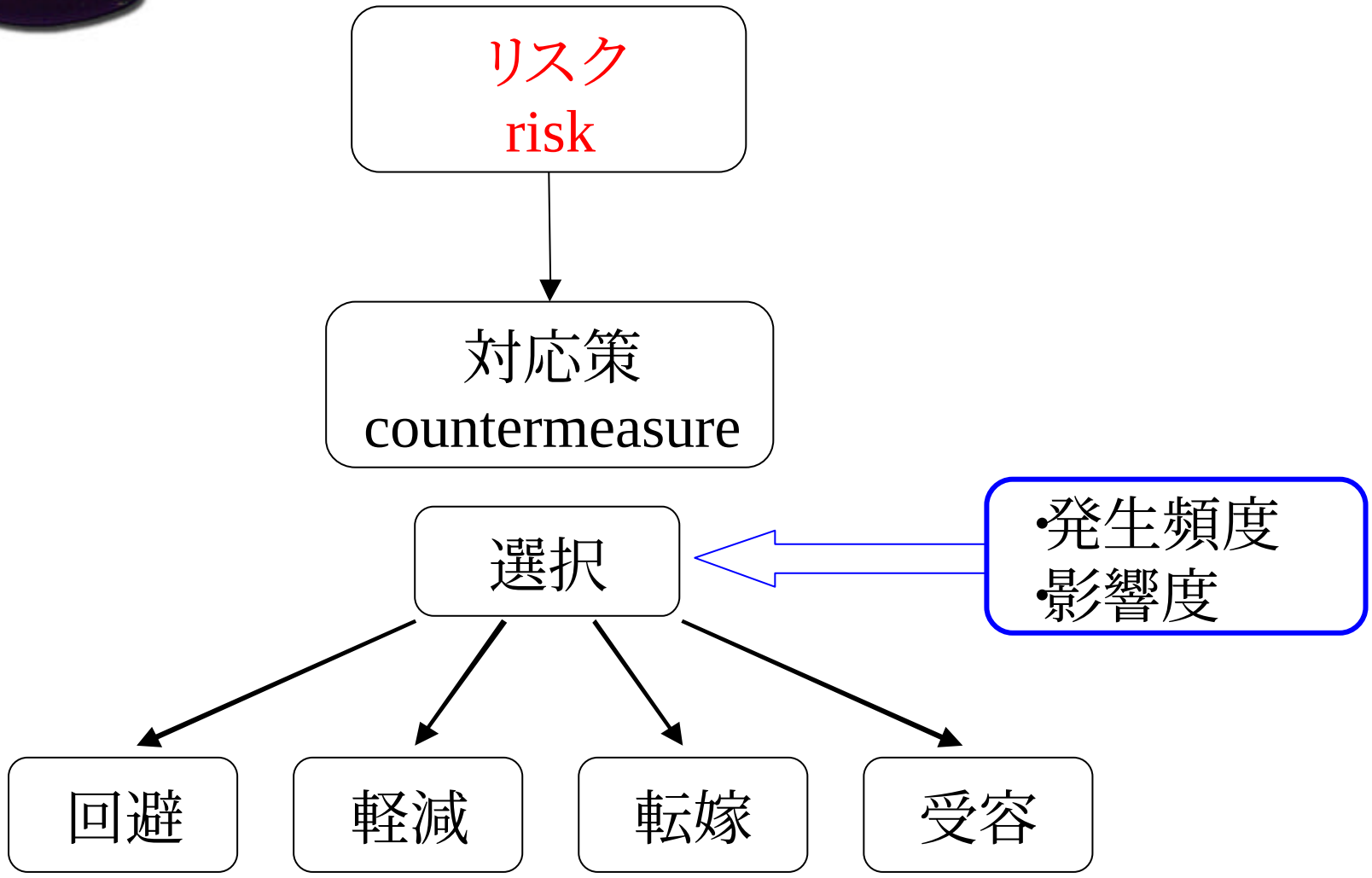
リスク
risk

マネジメント
management

対応策
countermeasure

出典：CRAMM(CCTA Risk Analysis and Management Method)

リスクマネジメントとは？



リスクマネジメントと業務の関係

脅威と脆弱性によりリスクが生まれる

脅威や脆弱性を生じる事象の分類：

- 業務によらない事象
  - 人為的な事象　→無許可のアクセス・・・
  - 人為的ではない事象　→自然災害・・・
- 業務による事象
  - 業務の不作為による事象　→注意不足・・・
  - 業務の作為による事象　→故意、過失・・・

リスクマネジメントと業務の関係

・業務の作為による事象」以外は、
　リスク対応策は、本来業務と独立又は区別できるリスク対応業務となる。

・業務の作為による事象」は、
　リスク対応策は、業務そのものに内在する。
　当該業務手順が標準化されていれば、その標準にリスク対応策を適用することができる。・・・はず。

リスクマネジメントと業務の関係

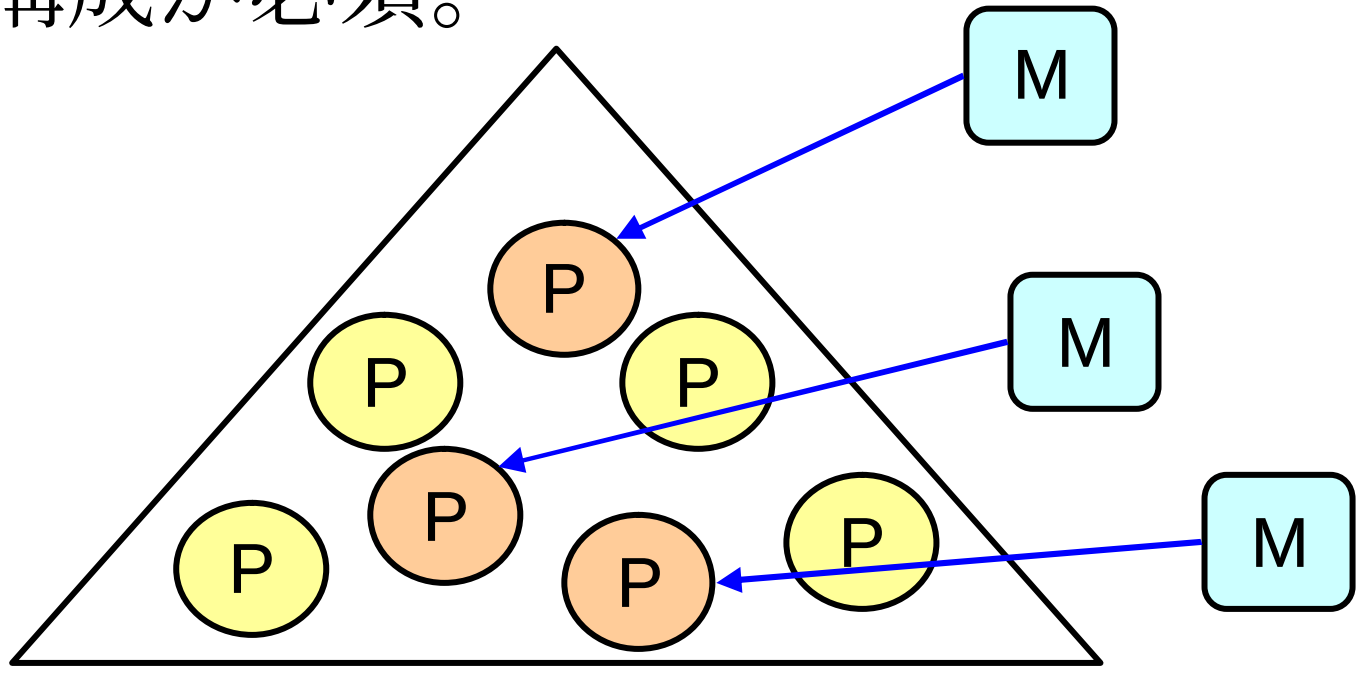
当該業務手順が標準化されていれば、その標準にリスク対応策を適用することができる。・・・はず。

一方で、非標準化手順、すなわち、裁量業務については、リスクマネジメントの集約が困難である。と考えるべき。

なぜなら、手順を裁量しているのが業務担当者である限り、業務担当者がリスクの分析やリスク対応策の選択をする部分があるため。

リスクマネジメント
集中管理できるのか？

マネジメントのプロセスを集約化することは可能。
マネジメントするプロセスを集約化することは、プロセス再構成が必須。



リスクマネジメント
リスクは細部に宿りたもう

■リスクマネジメントの手続きを一元化しつつ、分析と判断を現場に任せることは現実的であると考えられる。

□判断基準の標準化を志してもよいが慎重にすべき。その場合、例外承認手続きとともに導入するのがよい。
□判断基準の標準化を現場が要望するのは注意信号である。

リスクマネジメント

JIS Q 2001「リスクマネジメントシステム構築のための指針」より

発生場所、原因、損害を受ける対象などによってリスクをグループとして扱うことが適切と判断できる場合には、そのグループごとに部門、部署、委員会などの形式でリスクマネジメントシステム担当者を定めてもよい。」

拙著 参考記事：

翔泳社Webサイト IT Compliance Web 内部統制と情報セキュリティ

リスクは集中管理できるのか ～企業における法対応とITのバランス～

http://www.itcomp.jp/a/article.aspx?aid=153

すぐに使える推奨資料

「先進企業から学ぶ事業リスクマネジメント実践テキスト」
平成17年3月　経済産業省
（事業リスク評価・管理人材育成システム開発事業）

情報セキュリティに限らない、企業におけるリスクマネジメント全般について検討すべきことを紹介している。
300ページと分量が多いが、図を多用し、企業事例にも具体的にふれてわかりやすく解説しているため、読むのにストレスはない。

以下のWebから無償ダウンロード可能
http://www.meti.go.jp/policy/economic_industrial/report/downloadfiles/g50331i00j.pdf

すぐに使える推奨資料

先進企業から学ぶ事業リスクマネジメント実践テキスト」
平成17年3月　経済産業省
（事業リスク評価・管理人材育成システム開発事業）

目次

1. リスクマネジメントとは
2. 事業リスクマネジメントシステム構築及び維持のための体制
3. リスクマネジメント方針
4. リスクマネジメント計画の策定
5. リスクマネジメントの実施
6. リスクマネジメントシステムに関する評価、是正・改善

リスクマネジメントとしての情報セキュリティ対策

リスクマネジメントとしての情報セキュリティ対策

実際の脅威

情報セキュリティポリシーによる目標

現状

受け入れたリスク

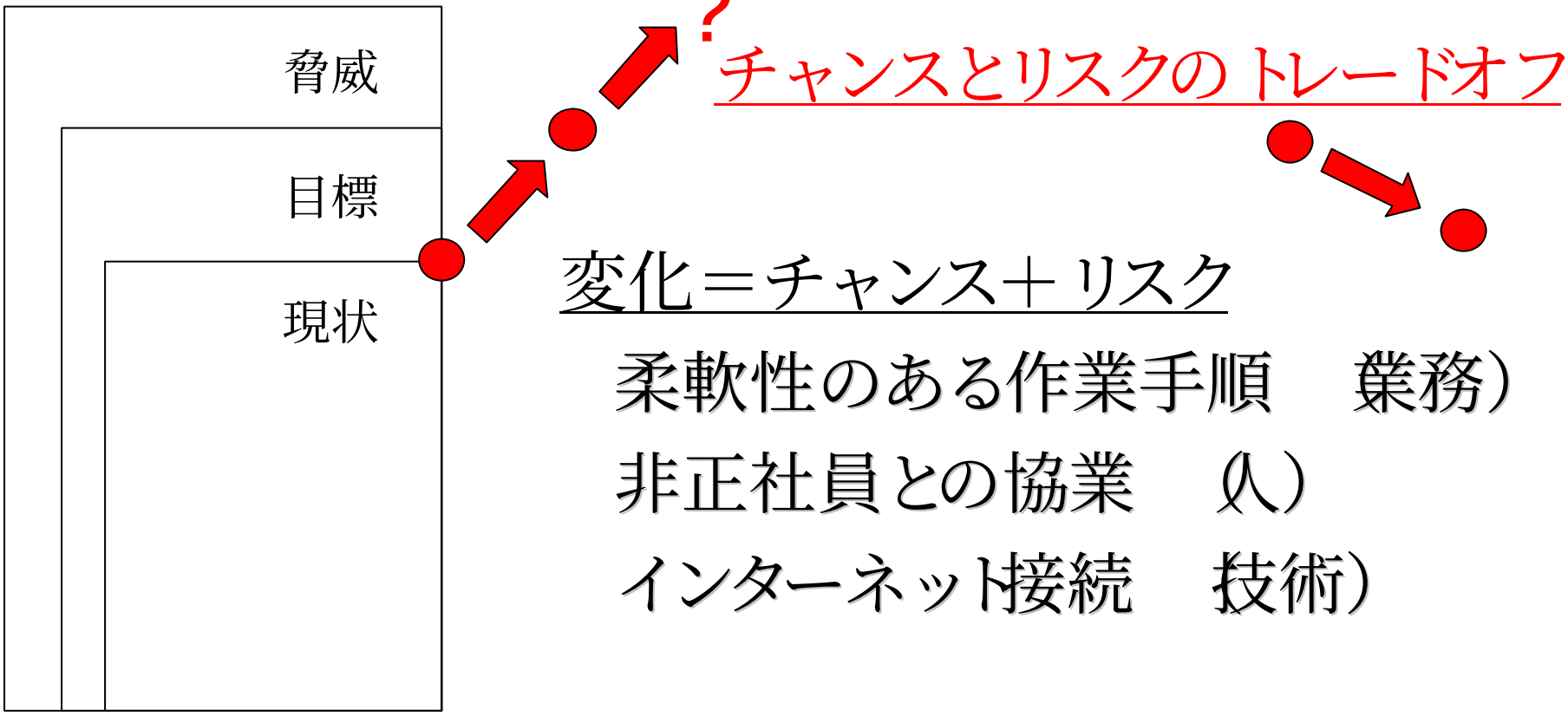
これからの対策

実施済みの対策

受け入れないリスク

最低基準ではなく適正基準
何ができるかより、何をしないか」

リスクマネジメントとしての情報セキュリティ対策



変化＝チャンス＋リスク

柔軟性のある作業手順　（業務）

非正社員との協業　（人）

インターネット接続　（技術）

情報セキュリティ
従来の傾向

情報セキュリティとは、機密性、完全性、可用性を確保すること。

機密性 C: Confidentiality
完全性 I: Integrity
可用性 A: Availability

■従来の情報セキュリティ対策は、C:機密性に偏っている傾向がある。

情報セキュリティ 今後の方向性

CIAからAICへ

□実際には、Cに加えて+Iさらに+A

□しかし、CとIとAの要求が相反する場合にトレードオフを図る必要に迫られる。

□情報セキュリティを直接トレードオフすることはできない。リスクのトレードオフとなる。

■情報セキュリティマネジメントシステムにおいては、+I&+Aによって、対策そのものに加えてリスク評価が重要になる。

情報セキュリティ
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。

□委託先に対してPマークやISMS認証の取得を義務付けることの意味の再確認。

委託関係において あってはならないこと

■委託関係において、委託元が具体的なセキュリティ対策要求事項を示さず、結果責任（たとえば賠償責任）だけをリスク転嫁することは、健全なマネジメントシステムを形成するとは思われない。

■リスクの転嫁の連鎖だけが発生する

具体策がないまま見積もりをする
リスク軽減度合いの高いところは見積もり価格が高くなる
リスク軽減度合いの低いところは見積もり価格が安くなる
委託元としての具体策がないため、価格以外での評価ができない

■リスクが潜在化するだけ

結果責任だけを押し付けると、委託元の周囲に粗悪業者が蔓延し、リスクが顕在化するその日まで、リスクが温存される。

委託先に対する 認証取得の義務付け」の意味

■認証取得の適用範囲とリスク判断基準を明示的に指示している場合だけ意味がある。
■暗黙のままでは、プライバシーマークや ISMSの適用範囲及びリスク分析・評価は、それを取得する委託先によるものとなる。
最悪の場合は、適用範囲が異なることすらあり得る。

□委託先への丸投げは、委託先のリスク判断基準（受容レベル）を、委託元として暗黙にそのまま受け入れることを意味する。
□委託先に結果責任だけを負わせることは、リスク転嫁策のように思われるが、リスクが表出（事故発生等）したときに、それが実際に転嫁されるのだろうか・・・青天井賠償の有効性はあるのか。
□さらに、現場での責任意識・危機管理意識の希薄化を招く。
■百害あって一利なし。ということはないのか。。。

個人情報保護法ガイドライン 経済産業省の例）

■第22条　委託先の監督）

•個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合、法第20条に基づく安全管理措置を遵守させるよう、受託者に対し必要かつ適切な監督を行わなければならない。

・必要かつ適切な監督」には、委託契約において、当該個人データの取扱に関して、必要かつ適切な安全管理措置として、委託者、受託者双方が同意した内容を契約に盛り込むとともに、同内容が適切に遂行されていることを、あらかじめ定めた間隔で確認することも含まれる。なお、優先的地位にある者が委託者の場合、受託者に不当な負担を課すことがあってはならない。

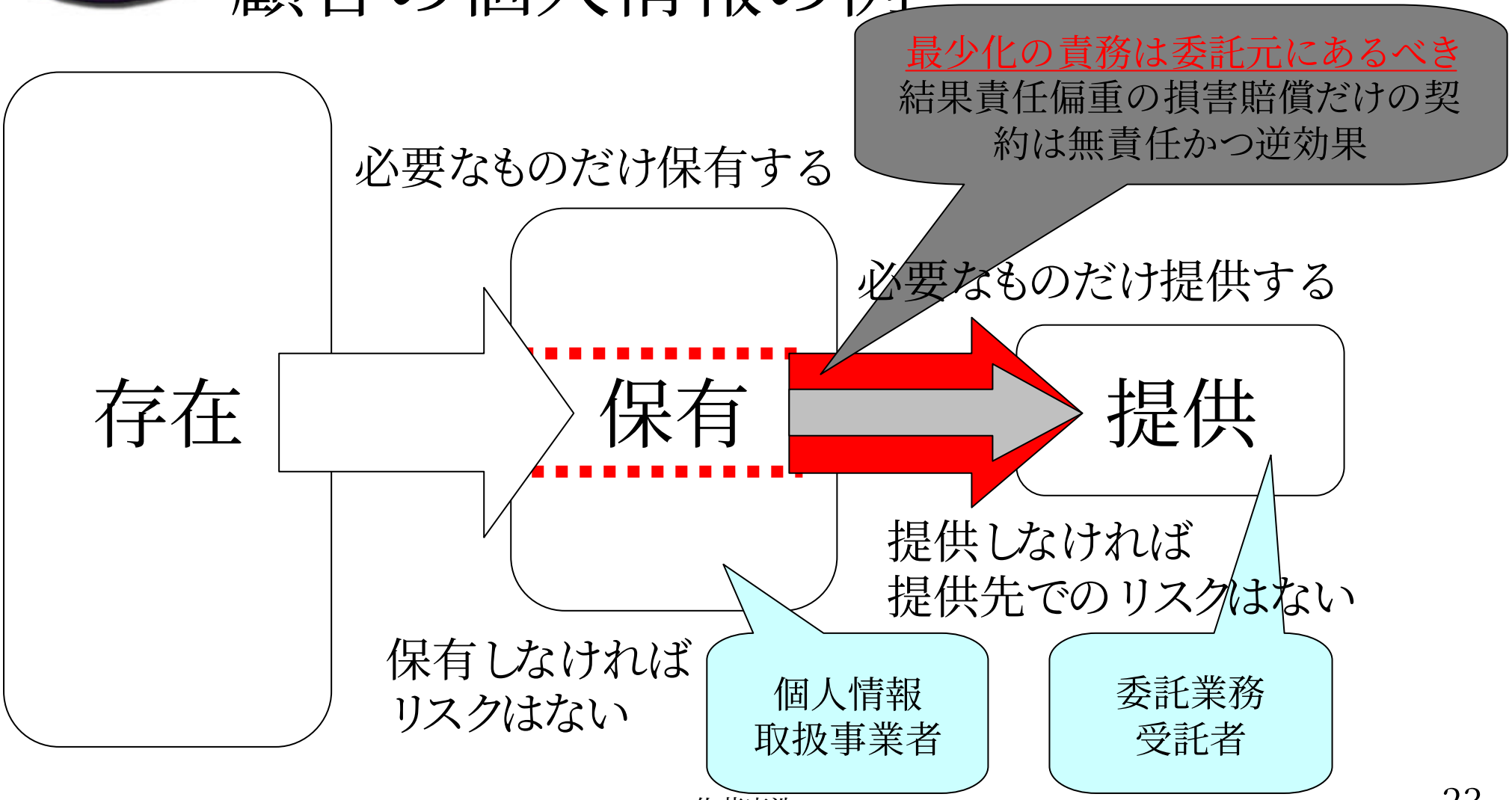
•委託者が受託者について 必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意する。

委託関係において配慮すべきこと

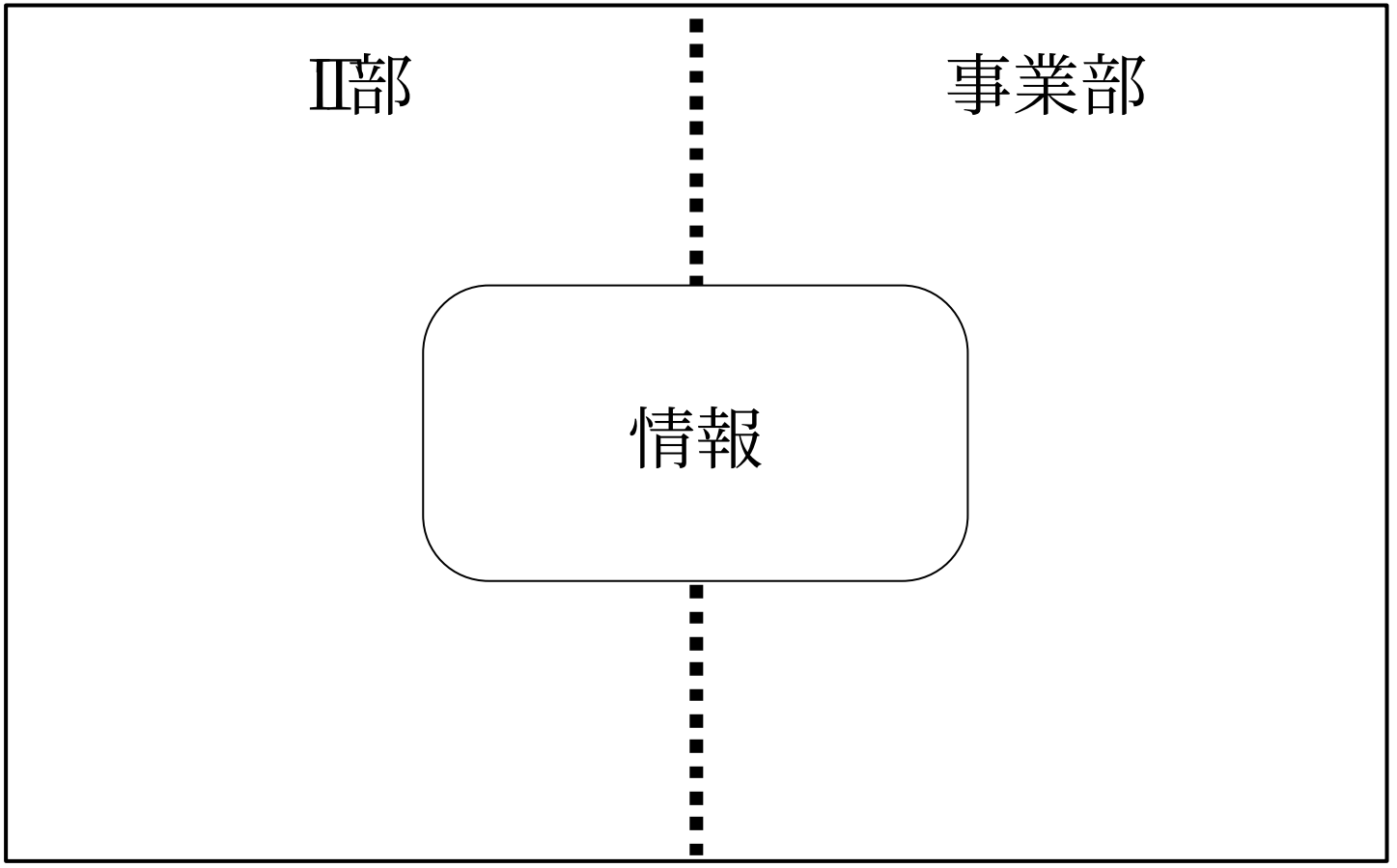
■委託元は、一次的な責任主体である。
□委託元は、自身のセキュリティ対策要求事項を具体的に定めて徹底する。
□委託元は、その要求事項を発注時に具体的に示す。
□委託先は、指示された要求事項に必要な対策を具体的に立案し、必要な費用を見積もる。
□双方が、各々の立場において必要なマネジメントシステムを構築する。
（たとえば、情報受け渡しプロトコル＝次のスライド）

■なぜなら、委託元である企業を顧客は信頼しているのであって、委託先にリスク転嫁されることを期待していない。

委託先への提供
顧客の個人情報の例

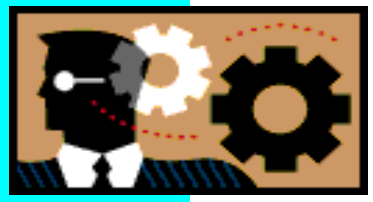


委託する情報の責任所在



委託する情報の責任所在

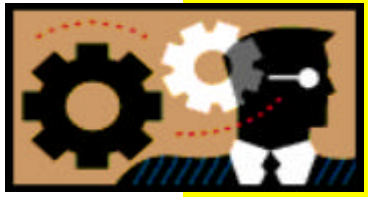
情報



IDC委託先

IDC委託元

委託する情報の責任所在

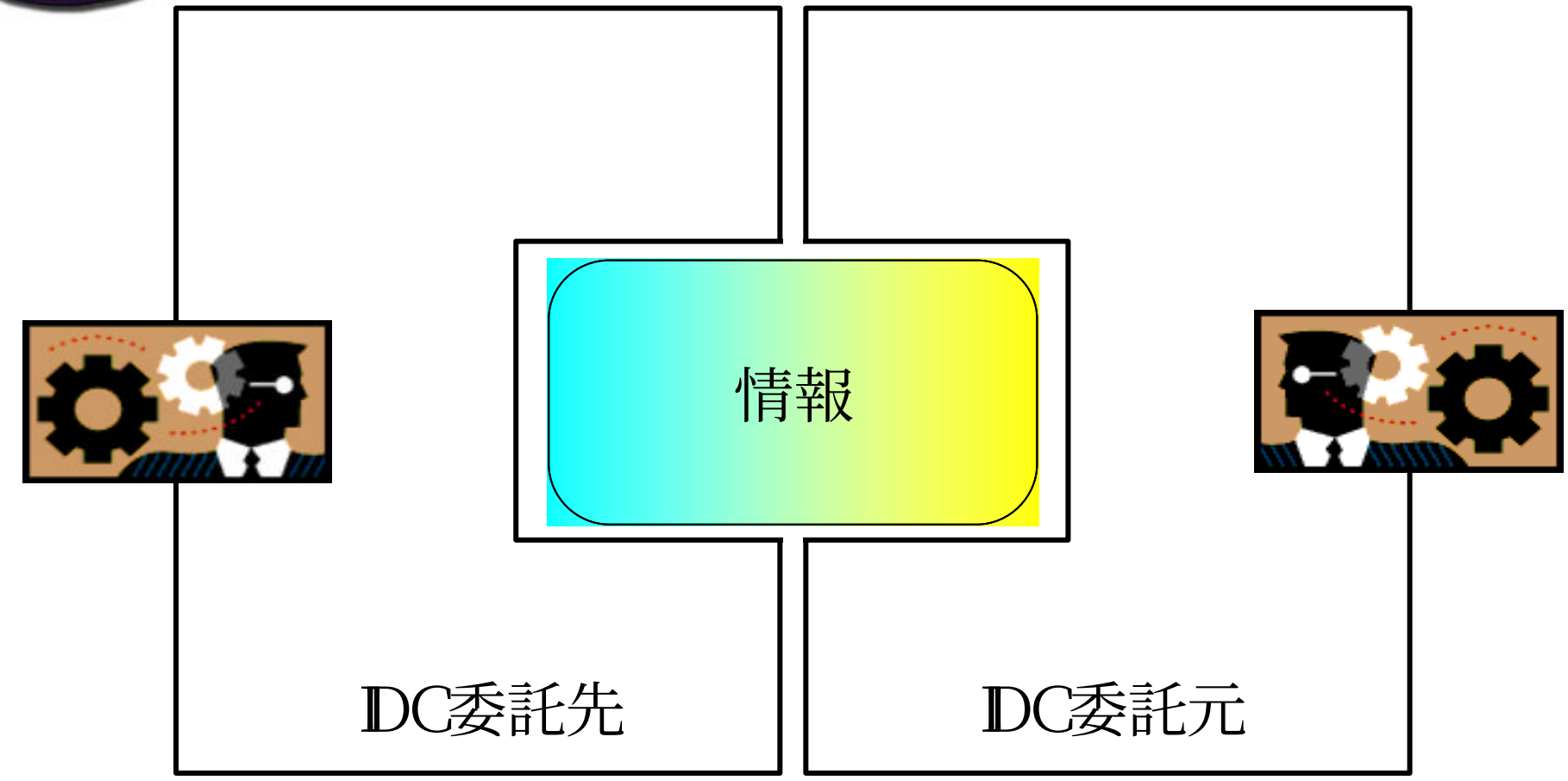


情報

IDC委託先

IDC委託元

委託する情報の責任所在



情報セキュリティ
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？
    ■・・・Ⅱゼネコンの構造的破綻

講演内容

- リスクマネジメントとは
- リスクマネジメントと業務の関係
  - 非標準手順による業務
- リスクマネジメントの集中管理
  - リスクは細部に宿りたもう
- リスクマネジメントとしての情報セキュリティ
  - 最低基準ではなく適正基準
- 情報セキュリティの傾向と課題
  - ＣＩＡからＡＣＥへ
  - 委託先におけるマネジメント

情報ネットワーク法学会

http://in-law.jp/

随時、入会受付中

発表資料のダウンロード

http://yosihiro.com/go/2008-02-23-isaca