企業における
情報セキュリティ対策の実務

2014年11月29日

日本ヒューレット・パッカード株式会社
チーフ・プライバシー・オフィサー
佐藤慶浩

講師自己紹介

SecCap

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）　チーフ・プライバシー・オフィサー
（兼）BITA（ビジネス-IT・アライメント）エヴァンジェリスト
元　内閣参事官補佐（民間併任）
（内閣官房　情報セキュリティセンター　情報セキュリティ指導専門官）

【社外の活動】
IT総合戦略本部パーソナルデータ検討会技術検討ワーキンググループ　構成員
経済産業省 個人情報保護ガイドライン検討委員会　元委員
厚生労働省医療等分野における番号制度の活用等に関する研究会　構成員
杉並区　住基ネット運用監視委員会　委員長
世田谷区　情報公開・個人情報保護審議会　構成員
経済産業省 IT融合フォーラム パーソナルデータワーキンググループ　元構成員
JIPDEC　プライバシーマーク運営要領改正委員会　元委員
JIPDEC　ISMS適合性評価制度技術専門部会　委員
ISO/IEC JTC1/SC27 WG5 プライバシー小委員会　元主査、現エキスパート
情報ネットワーク法学会　前副理事長
デジタル・フォレンジック研究会　理事

【その他】
http://よしひろ.com/profile/

講演概要

企業における情報セキュリティ対策の実務（90分）

1．情報セキュリティ対策の組織的枠組みについて、国内企業へのコンサルティング実施や、政府内閣情報セキュリティ指導専門官を併任した経験などを踏まえて紹介します。（講義30分＋質疑応答15分）

2．システム管理権限者による不正防止をどのようにするかについて、技術面と運用面の両方から、防衛や金融機関でのシステム設計経験を踏まえて紹介します。（講義30分＋質疑応答15分）

目次

1. ルール作りとリスクマネジメント
   大きな事故を防ぐためのアイデア
   ルール作りの基本的考え方
   リスクマネジメントのすすめ

2. システム管理者権限からもデータを守る
   権限の最小化と分割
   技術を有効にする運用

大きな事故を防ぐためのアイデア

（参考）

ブロークン・ウインドウズ理論

Broken Windows Theory
March 1982, Atlantic Online

※一例であり、これを画一的に、あるいは一意に推奨するということではありません。

（参考）
ブロークン・ウインドウズ理論

第１段階
　落書きが放置されていると罪悪感が薄れやすくなる
第２段階
　軽犯罪が多発し治安が悪くなる
第３段階
　警察の監視がないと判断され、より凶悪な犯罪者が寄り付く
第４段階
　犯罪がエスカレートし凶悪犯罪が発生する
対策
(1)落書きを徹底的に消す
→警察や住民の監視があるというメッセージ
→軽い気持ちで罪を犯す人が減少する
(2)軽犯罪の取締りを強化する
→小さな犯罪も許さないという姿勢をアピール
→犯罪を起こそうと思う人間は近づかない
→凶悪犯罪は低減する

Home
Current Issue
Archive
Forum
Site Guide
Feedback
Subscribe
Search

Browse >>
Books & Critics
Fiction
Food
Foreign Affairs
Language
Poetry Pages
Politics & Society
Science & Technology
Travel & Pursuits

Send this page to a friend

March 1982

Broken Windows

The police and neighborhood safety

by James Q. Wilson and George L. Kelling

In the mid-1970s The State of New Jersey announced a "Safe and Clean Neighborhoods Program," designed to improve the quality of community life in twenty-eight cities. As part of that program, the state provided money to help cities take police officers out of their patrol cars and assign them to walking beats. The governor and other state officials were enthusiastic about using foot patrol as a way of cutting crime, but many police chiefs were skeptical. Foot patrol, in their eyes, had been pretty much discredited. It reduced the mobility of the police, who thus had difficulty responding to citizen calls for service, and it weakened headquarters control over patrol officers.

Many police officers also disliked foot patrol, but for different reasons: it was hard work, it kept them outside on cold, rainy nights, and it reduced their chances for making a "good pinch." In some departments, assigning officers to foot patrol had been used as a form of punishment. And academic experts on policing doubted that foot patrol would have any impact on crime rates; it was, in the opinion of most, little more than a sop to public opinion. But since the state was paying for it, the local authorities were willing to go along.

Five years after the program started, the Police

凶悪犯罪を未然に防止することはできるか？

軽犯罪の取り締まりを強化することで、結果的に、凶悪犯罪の発生率が下がる傾向になる。

情報セキュリティの大事故を防ぐには、日々の軽微な対策を全員が実施することが必要。

目次

1. ルール作りとリスクマネジメント
   大きな事故を防ぐためのアイデア
   ルール作りの基本的考え方
   リスクマネジメントのすすめ

2. システム管理者権限からもデータを守る
   権限の最小化と分割
   技術を有効にする運用

「ガバナンス構築」 HP社内の定義

達成目標の合意形成としての定義

- 遵守事項(すべきこととしてはならないこと)を、組織が定めていること
- 遵守事項を、組織が構成員に対して教育していること
- 遵守事項を、組織の構成員が理解していること
- 遵守事項を遵守することについて、組織の構成員が同意していること
- 組織の構成員の同意について、組織が確認していること

このとき、この組織において、その構成員の範囲で、遵守事項のガバナンスが構築されている。

参考:遵守事項策定の際は、それが計測可能であることを原則としている。

→「達成目標の合意形成」は、「動機付けの交渉」(宍戸善一著「動機付けの仕組としての企業」より)に相当

「規程」の策定

理解の促進→用語定義と遵守事項

用語などの定義

通常の業務で使用していない用語には定義が必要

社外の標準に合わせることを偏重しない（用語対応表で対処）

日本語での留意事項

カタカナの使用の最小化

→カタカナ用語は用語解説（付録）で定義

主語の明文化

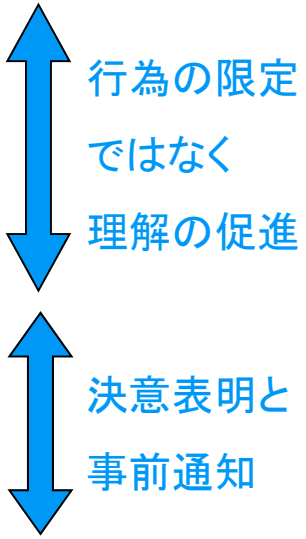
→英訳文の試作で検証

「規程」の策定

理解の促進→何を統一的に定めるか

文の種類の事前定義

- 定義事項の文
- 遵守事項の文
  - 必須行為（people Must Do：～しなければならない）
  - 推奨行為（people Should Do:～することが望ましい）
  - 禁止行為（people Must Not Do： ～してはならない）
  - 許諾行為（people May Do： ～することができる）
  - 支援義務（company Must Do：～する）
  - 権限留保（company May Do：～する場合がある）
  - 権限放棄（company Never Do：～することはない）



何を定める？　最低水準（baseline）と／か適正水準（just enough）

「規程」の策定

責任者の決定→逸脱手続き（WHO）

＊ビジネスの例外を前提にする

ビジネスの例外→情報システム使用の例外→情報セキュリティの例外

初期値は、代表取締役社長＝経営的・法的な最高責任者

~~「例外を認めない」~~ → 「社長決裁をしなければならない」

責務の委任　　経営資産＝人、物、金、情報

「規程」の策定

個々のポリシー文の記載内容の要件

- 何が目標か（WHAT）　→あるべき姿の考察
- なぜ、それが目標か（WHY）→受け入れられないリスクの考察
- 誰が責任者か（WHO）　→受け入れるリスクの考察

参考：政府機関統一基準見直しの考え方

- **基準外要因の確認 （リスク分析をする。必要なら、対応として許容リスクも見直す。）**

A. 政府内要件の変化への対応

- 情報セキュリティ対策に関係する行政事務要件について、その目標達成のために統一基準改訂の必要があれば、改訂方法を決定する

B. 政府外環境の変化への対応

- 世の中で起きた事件事故についての検証 （政府機関内で発生したと仮定して以下の検証をする）
  - 原因が基準違反とならなければ改訂必要
  - 原因が基準違反となるならば改訂不要 （ただし、「遵守事項や解説見直し」の材料とする。）
- 周知された注意喚起についての検証
  - 基準で対応していない潜在的脅威について、顕在化の可能性が高まっていればリスク対応する

- **基準におけるすべての内容確認 （改訂で許容リスクを変化させないことを原則とする。）**

C. 実務に則した遵守事項の見直し

- 運用に障害又は困難をきたす部分があれば、それを解消・軽減するための修正をする
  - 遵守事項の達成目標を変えずに表現（主語・述語・客体、条件等）を変更する
  - 遵守事項の達成目標を変える

D. 運用改善のための適用範囲・解説等の見直し

- 誤解のない表現の追加・修正

E. 文言の改善

- 表現漏れ、誤字脱字の修正

「対策実施基準」作成の注意点

文章としての注意点：

カタカナ使用の最少化すること

主語を明確にすること

述語（の語尾）を明確にすること

規定内容の注意点：

性善説を前提とすること

実施可能なことに限ること　→　事前合意が前提

例外発生を想定すること

リスク許容レベル及び範囲の拡大傾向を想定すること

運用時の注意点：


実施状況の確認指標を明確にすること

見直し時の注意点：


見直し作業方針をあらかじめ定めること（随時変更不可ではない）

ルール違反への対処

違反者には、謝罪させるのではなく、理由を説明させる。
- 原因の特定
- 特定した原因に基く再発防止策の検討
- 再発防止のための対策実施（周知・徹底以外に最低1つ）

HPにおける監査方針
- 違反については理由書の提出
- 監査者は被監査者と絶対に敵対してはならない
- 監査者は支援者・助言者と認識されなければならない

ルール違反の発生は、ルール見直しの機会と考える。
- ブロークンウインドウズ理論からの教訓

目次

1. ルール作りとリスクマネジメント
   大きな事故を防ぐためのアイデア
   ルール作りの基本的考え方
   リスクマネジメントのすすめ

2. システム管理者権限からもデータを守る
   権限の最小化と分割
   技術を有効にする運用

リスクマネジメンのすすめ

リスクマネジメントのすすめ

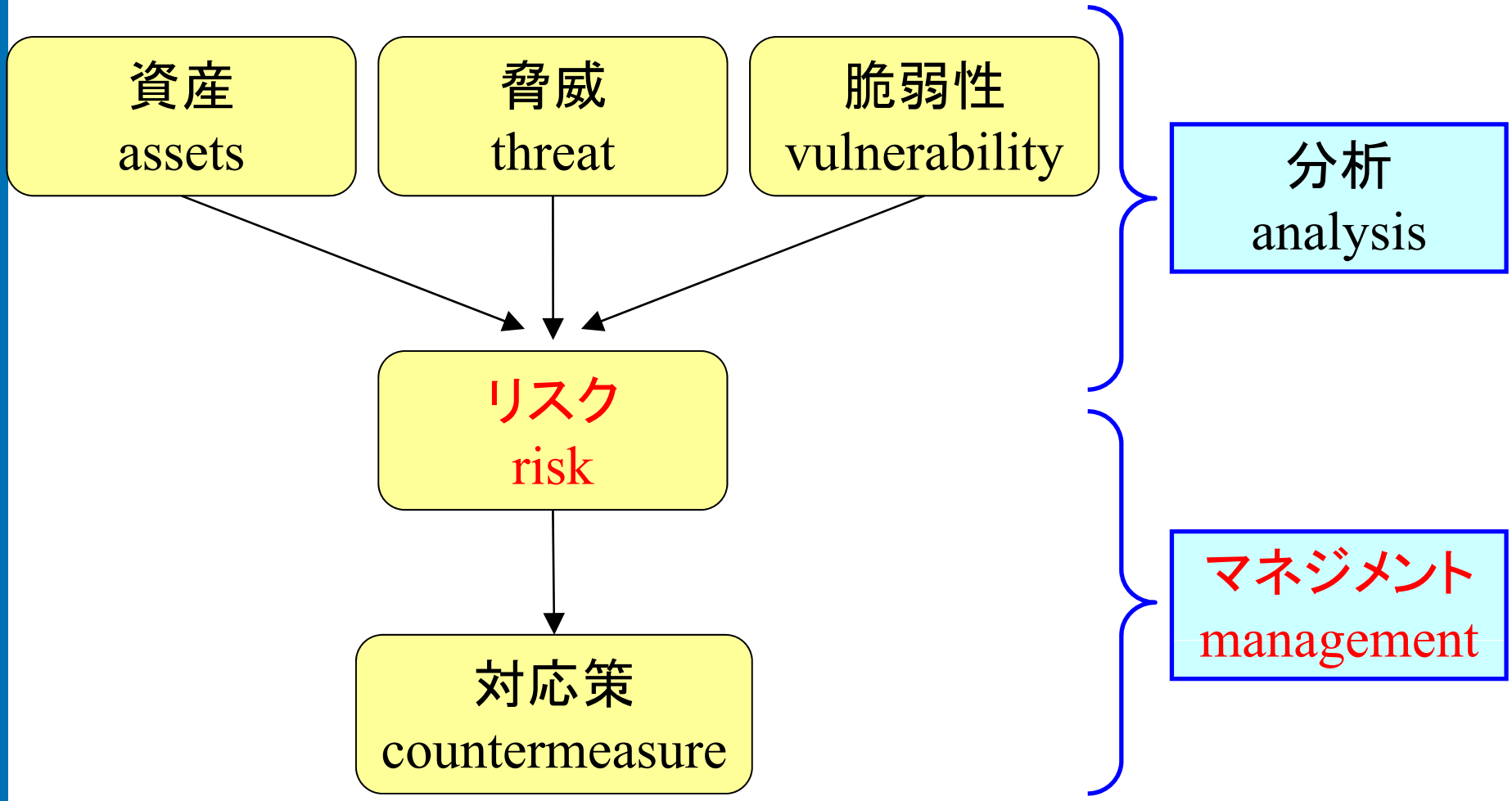
企業は事業継続、法令順守や情報管理など様々なリスクに対応する必要があり、年々増加傾向にあります。それらを統合しなければならない一方で、業務の意思決定を分散していくことも事業達成から求められています。
そのような集約と分散との相反する条件がある中でマネジメントシステムをどうやって統合していくのかは困難な課題となっています。
これらに関するHPの取り組みについて、紹介します。

リスクマネジメントのすすめ

- 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
- リスク対応策の展開
- リスクの傾向

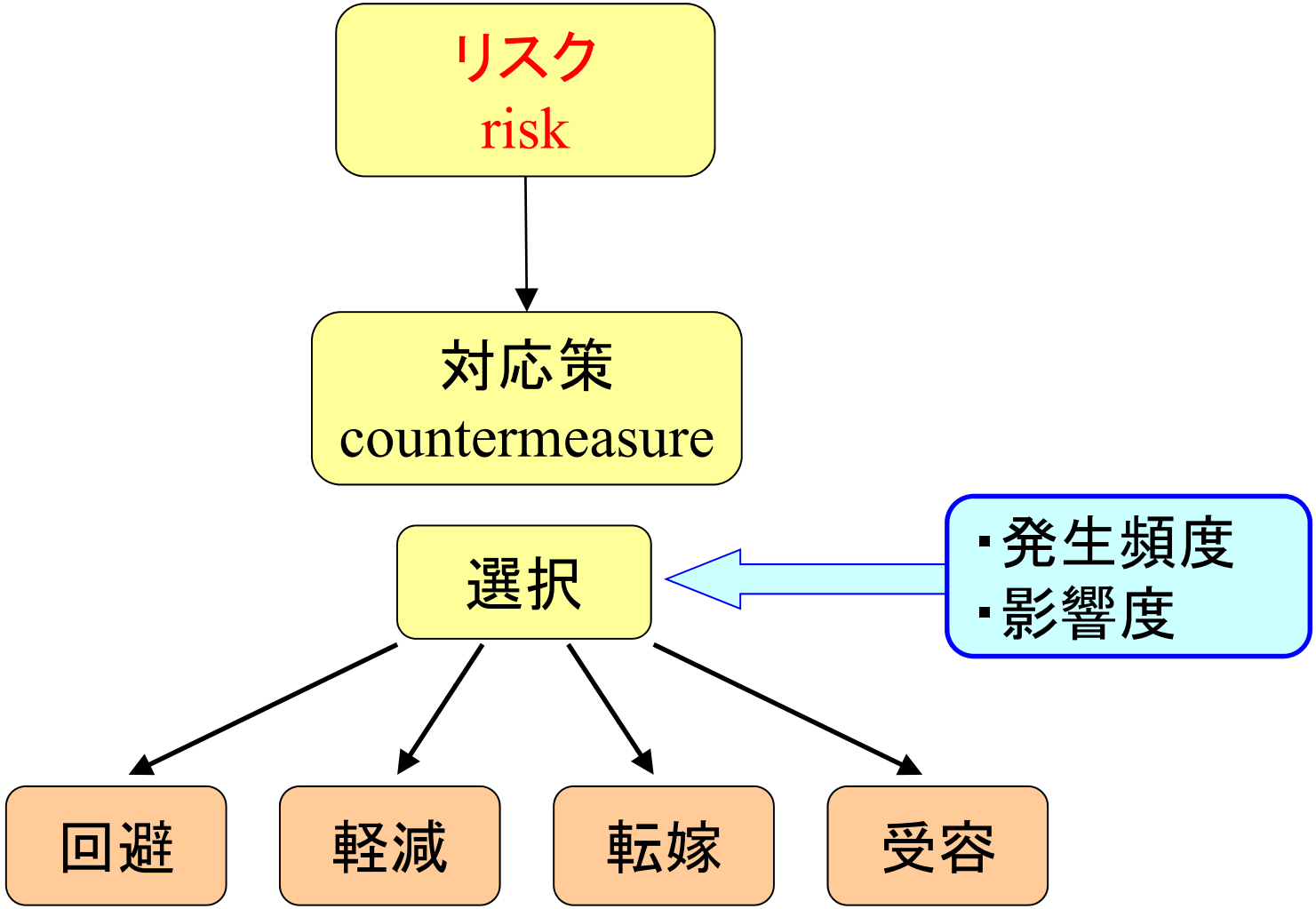
リスクマネジメントとは

リスクマネジメントとは？



出典：CRAMM(CCTA Risk Analysis and Management Method)

リスクマネジメントとは？

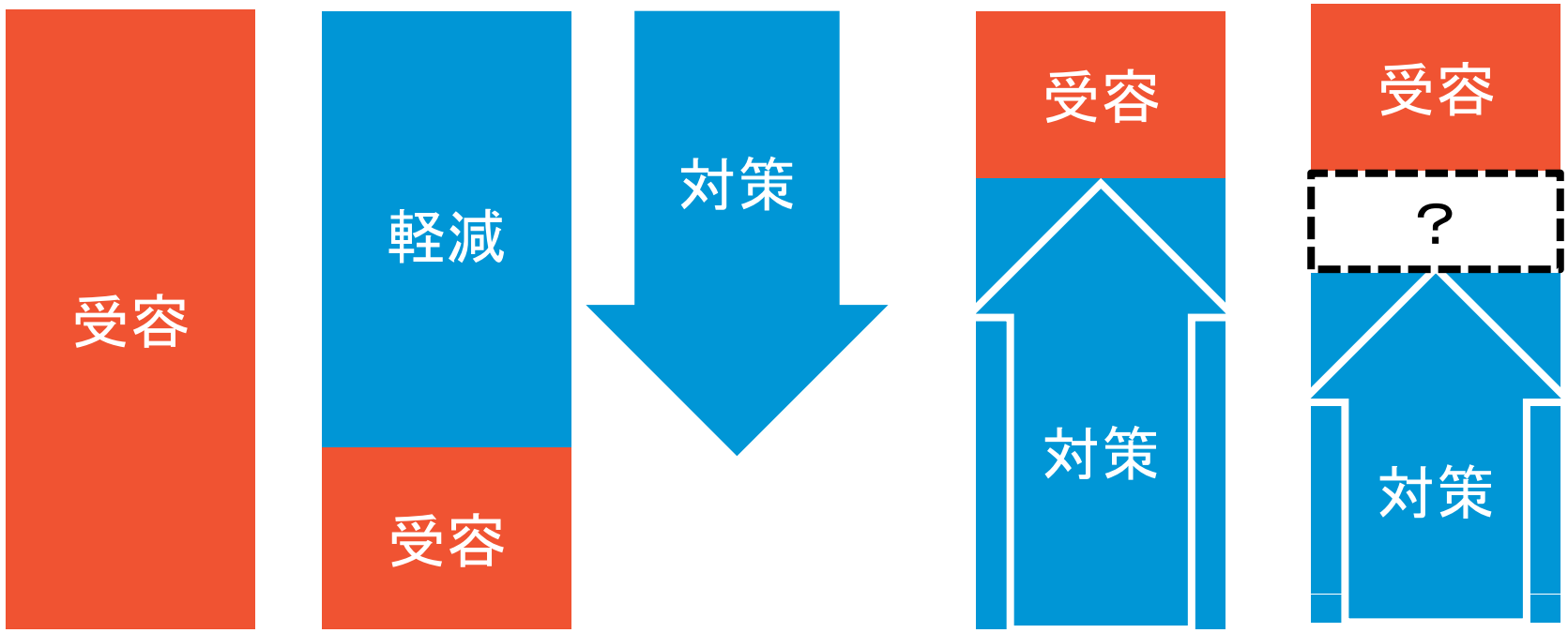


リスクマネジメントとは？

存在リスクと残存リスクの理解

リスクの保有と回避

保有リスクの受容と軽減、転嫁



リスクマネジメントと業務の関係

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。

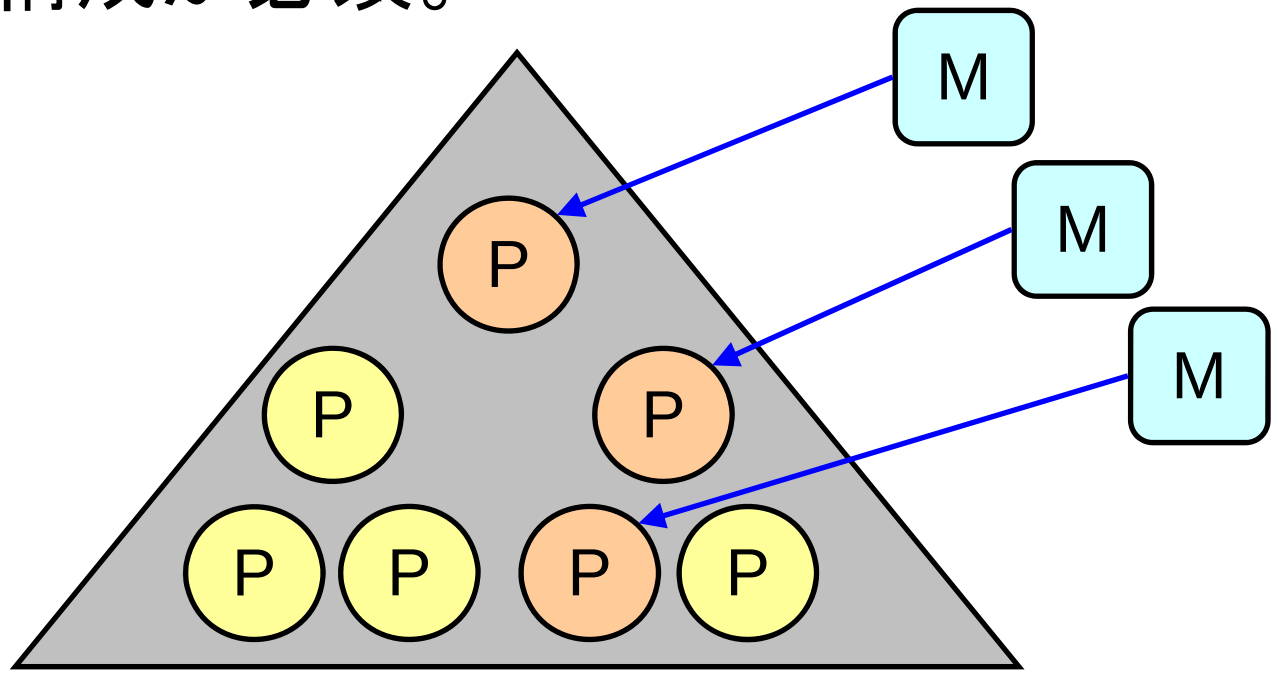
一方で、非標準化手順、すなわち、裁量業務については、リスクマネジメントの集約が困難である。と考えるべき。

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の集中管理

リスクマネジメント
集中管理できるのか？

マネジメントの方法を一元化することは可能。
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。

（参考）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

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

（参考）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

（参考）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

リスク対応策の展開

○○○に係る□△□という言葉の罠

- 情報セキュリティ・□△□

- 情報セキュリティ教育
- 情報セキュリティ監査
- 情報セキュリティ・リスクマネジメント
- 情報セキュリティ・ガバナンス

  - 「する」を付けることによる検証
  - 罠　と　カタカナの甘い誘惑

リスク対応策の展開
６つのチェックポイント

①性悪説だけでは企業は成り立たない

②性善説を前提とした対策

③不正行為の類型

④性悪者を減らし、性善者を増やす環境

⑤外部委託

⑥可視化

リスク対応策の展開　①

性悪説だけでは企業は成り立たない

- 性善説を前提にして、
- 性悪説を想定する

※政府の情報セキュリティ政策会議のいう「事故前提社会」とは、
「事故発生を想定」又は「事故対応を前提」の意で、
「事故発生を前提」ではない。。。

リスク対応策の展開 ②

性善説を前提とした対策とは・・・

- 「しなければならないこと」と「してはならないこと」を明確にしていること。
- それを守るべき者に教育していること。
- それを守るべき者が理解していること。
- それを守るべき者が、遵守することに同意していること。
- 同意した者の状況を確認していること。

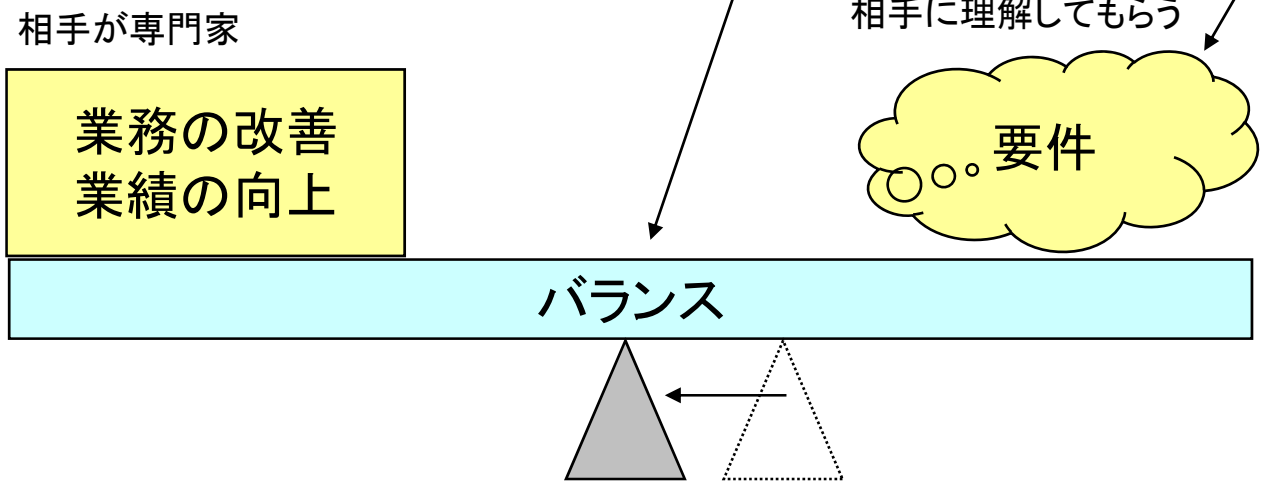
これが、すなわち、ガバナンスが構築された状態。

- コーポレート～，IT～，フィナンシャル～・・・

リスク対応策の展開 ②

性善説を前提とした対策とは・・・

- 「しなければならないこと」と「してはならないこと」を明確にしていること。
- それを守るべき者に教育していること。
- それを守るべき者が理解していること。
- それを守るべき者が、遵守することに同意していること。
- 同意した者の状況を確認していること。



リスク対応策の展開　②
性善説を前提とした対策・・・

情報は活用するためにある

情報セキュリティ偏重の過度の情報保護は禁物
情報活用が、企業における情報保持の目的
情報保護は、目的達成のための条件であり義務であるが、目的ではない
情報活用と情報保護の両立をはかる情報セキュリティ施策とすべき

ビジネスに貢献しない施策は要注意

コンプライアンス施策をROIで考えてはいけない
IT施策におけるTCO削減は避けれない
ビジネスに貢献するような、IT施策でなければ実効性は高まらない
セキュリティ対策のひとつは単純化。単純化はコスト低減になるはず
逆にコスト低減になっていないということは、複雑化をもたらしている危険信号
ITの最適化計画の中でコンプライアンス施策を設計し、業務に組み込むべき

リスク対応策の展開　②
性善説を前提とした対策・・・

守れるルールだけが、守られる。

実施できるルールだけを設けて、「ルールはすべて守るものである」という意識を定着させることが、結果的にルール遵守を定着させることができる。

できることの他に、できれば望ましいようなルールを混在させて、「必ずしも守らなくてもよいルールもある」という意識を持たれることは好ましくない。

遵守するための具体的な実施方法が明確になっていないルールを設けることは避ける。

情報利活用の要求に即したバランスを保つルールを設けることが重要。

リスク対応策の展開　②
性善説を前提とした対策・・・

性善説を前提にして性悪説も想定する

性善説を前提とする。その上で、性悪説についても想定すると考えることが重要。

性善説であれば、「ルールは守られる」というところから検討し始めることができる。

性悪説への対策は、ルールを守っている性善説の人達によって実施するしかないことを忘れてはいけない。

リスク対応策の展開　②
性善説を前提とした対策に、

性悪説を想定した対策を上乗せする。

- 性善説を前提とした対策を実施している人達に担ってもらう。

- いかなる規則や教育も性悪者には効果がない。
- 性悪者向け対策を担ってもらう人が不可欠。
- 性善説を前提としない企業に非標準手順業務のリスク対応策の展開はあり得ない。

リスク対応策の展開 ③
不正行為の類型

許可されていない者による不正行為（通称：外部犯）

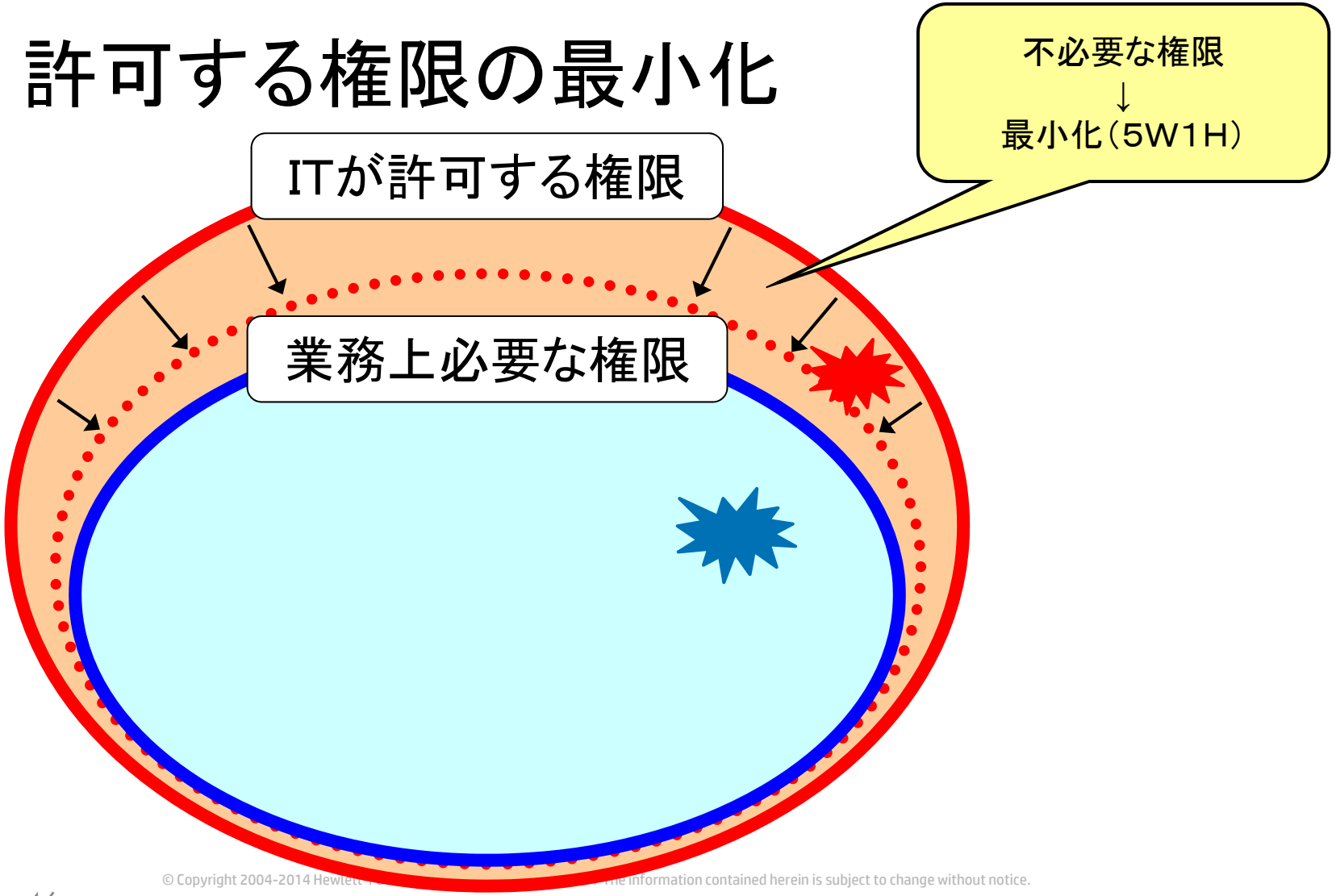
- 無許可の行為　悪意あり
  - 技術面：アクセス制御による防御・多重の防御

許可された者による不正行為（通称：内部犯）

- 誤操作・過失　悪意なし
  - 誤操作を軽減する設計
  - 啓発、教育、訓練
- 権限の悪用　悪意なし　悪意あり
  - 運用面：許可する権限の最少化
  - 技術面：監視による抑止効果
  - 技術面：アノマリ・アクセス（非通常行動）の検出

リスク対応策の展開　③
不正行為の類型：権限の悪用

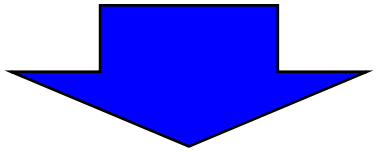
許可する権限の最小化



リスク対応策の展開　④

性悪説だけでは企業は成り立たない

- 性善説を前提にして、
- 性悪説を想定する

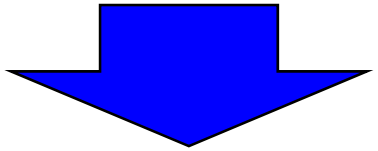


性悪者を減らし、性善者を増やす環境

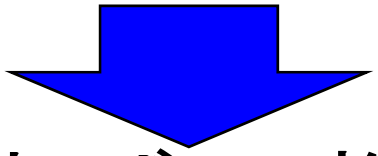
リスク対応策の展開　④
性悪者を減らすための環境作り

性悪説だけでは企業は成り立たない

- 性善説を前提にして、
- 性悪説を想定する



性悪者を減らし、性善者を増やす環境

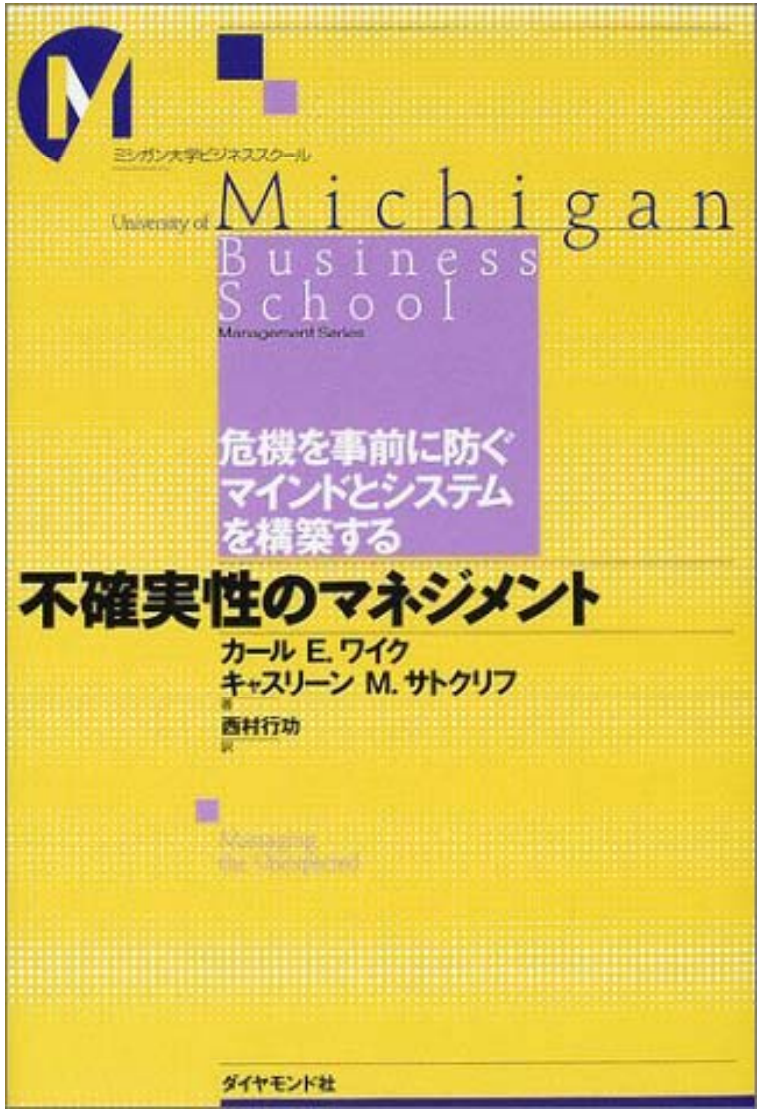


性善者が増えれば・・・権限委譲できる

参考書籍

「不確実性のマネジメント」
Managing Unexpected
カール E.　ワイク著

キーワード:
・HRO (High Reliability Organization)
　　高信頼性組織
・マインドフル



（参考）
徹底する？？？

- 「徹底」という言葉は、その瞬間までを評価することにしか使えない
- 事故が起きるまでは「徹底」できており、事故が起きた瞬間に「徹底」できていなかったことになるだけ
- 対策の文脈において、「徹底」とはその時点の状態を表現するだけの言葉でしかない

- 「徹底する」という言葉には、何の期待も信頼も置けない

by 佐藤慶浩

リスク対応策の展開　⑤

外部委託先は、リスクマネージメント体制の
外部？それとも内部？

リスク対応策の展開　⑤
外部委託

■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。

リスク対応策の展開 ⑤
外部委託

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

林紘一郎先生が「悪化は良貨を駆逐する」についても研究中

■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。

リスク対応策の展開 ⑤
外部委託

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。。。

リスク対応策の展開 ⑤
外部委託

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。

リスク対応策の展開 ⑥
可視化（見えるようにすること）

- ちゃんとやっていても、やっていることをわかってもらえなければ、見てもらえなければ意味がない。
- 全数対策工数は、サンプリング対策工数より多い。少ない工数を選ぶのは得策か？
- 最低限のサンプリング基準を達成することは、ビジネスに貢献するのか？

- すべてを可視化できることは、ビジネスに貢献する。
  - Customer chain, Supply chain, Financial chain
- 企業規模による処理の多少はITの限界に達していない。
  - １０人なら処理できて、１０万人なら処理できない？？？

リスク対応策の展開 ⑥
可視化（見えるようにすること）

2002年 米国SOX法

- Section 404 -- -- Management Assessment of Internal Controls

- Section 409 -- Real Time Issuer Disclosure -- mandates that companies must disclose on a rapid and current basis "material changes in the financial condition or operations of the [company], in plain English, which may include trend and qualitative information."

（参考） アダプティブ・エンタープライズの実現方法 ～4つの設計指針～

シンプル化
- 要素数の削減
- カスタマイズの低減
- 変更の自動化

＋

標準化
- 標準技術と標準インタフェースの採用
- 共通アーキテクチャの適用
- 標準プロセスの導入

＋

モジュール化
- 単純構造に分割
- 再利用可能な構成要素を作成
- 論理的なアーキテクチャの導入

＋

統合化
- ビジネスとITの連携
- 企業内外でのアプリケーションとビジネスプロセスの結合

一貫した適用:
- ビジネスプロセス
- 情報
- アプリケーション
- インフラストラクチャ

リスク対応策の展開
６つのチェックポイント

①性悪説だけでは企業は成り立たない

②性善説を前提とした対策

③不正行為の類型

④性悪者を減らし、性善者を増やす環境

⑤外部委託

⑥可視化

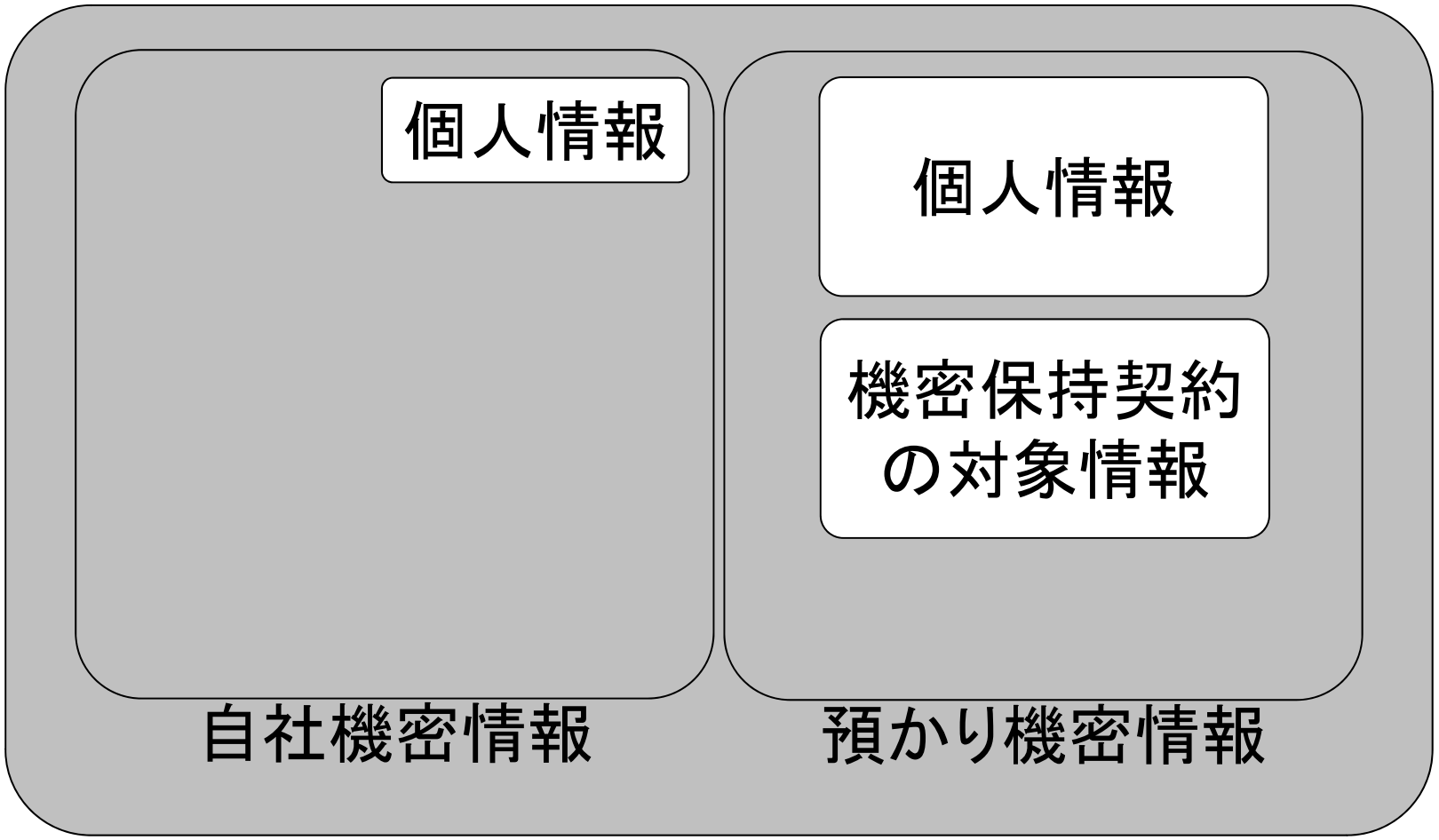
(参考)経済産業省
個人情報保護法ガイドライン 第20条

http://yosihiro.com/infosec/index.html#security_architecture

- つぎはぎシステムを防ぐセキュリティアーキテクチャ
- **5A (Authentication, Access Control, Administration, Auditing, Assurance)**

（参考）
個人情報の安全管理措置

個人情報と機密情報の関係



（参考）情報管理の不徹底の顕在化
新たな脅威が登場したわけではない

- 機密情報管理が徹底していなかった。
- 個人情報の流出や紛失等でそのことが顕在化した。

- 管理が不十分であったとは言い切れないが、不徹底が潜在的にあった。

- 情報に対する価値観や環境の変化。
- 現代の企業は、変化に対応することで安定する必要がある。（変化しないことが安定ではない）

（参考）
営業秘密　～営業秘密を守り活用する～

経済産業省 http://www.meti.go.jp/

不正競争防止法

営業秘密管理指針

－参考資料１：営業秘密管理チェックシート

トップページ ＞ 政策別に探す ＞ 経済産業 ＞ 知的財産の適切な保護 ＞
知的財産政策／不正競争防止 ＞ 営業秘密

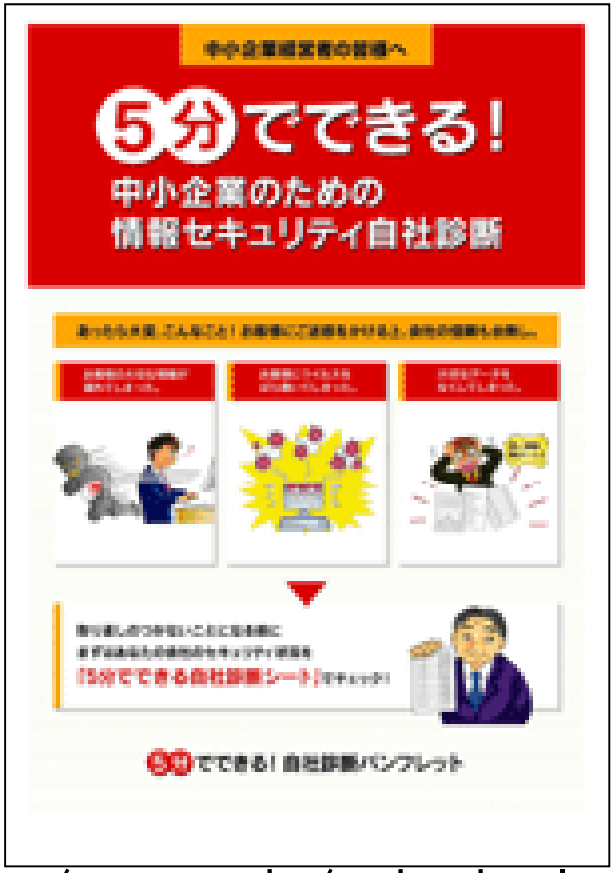
http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

（参考）
中小企業向け情報セキュリティ対策

IPA（情報処理推進機構）http://www.ipa.go.jp/

– 5分でできる！自社診断パンフレット

– 5分でできる！自社診断シート



http://www.ipa.go.jp/security/manager/know/sme-guide/index.html

リスクの傾向

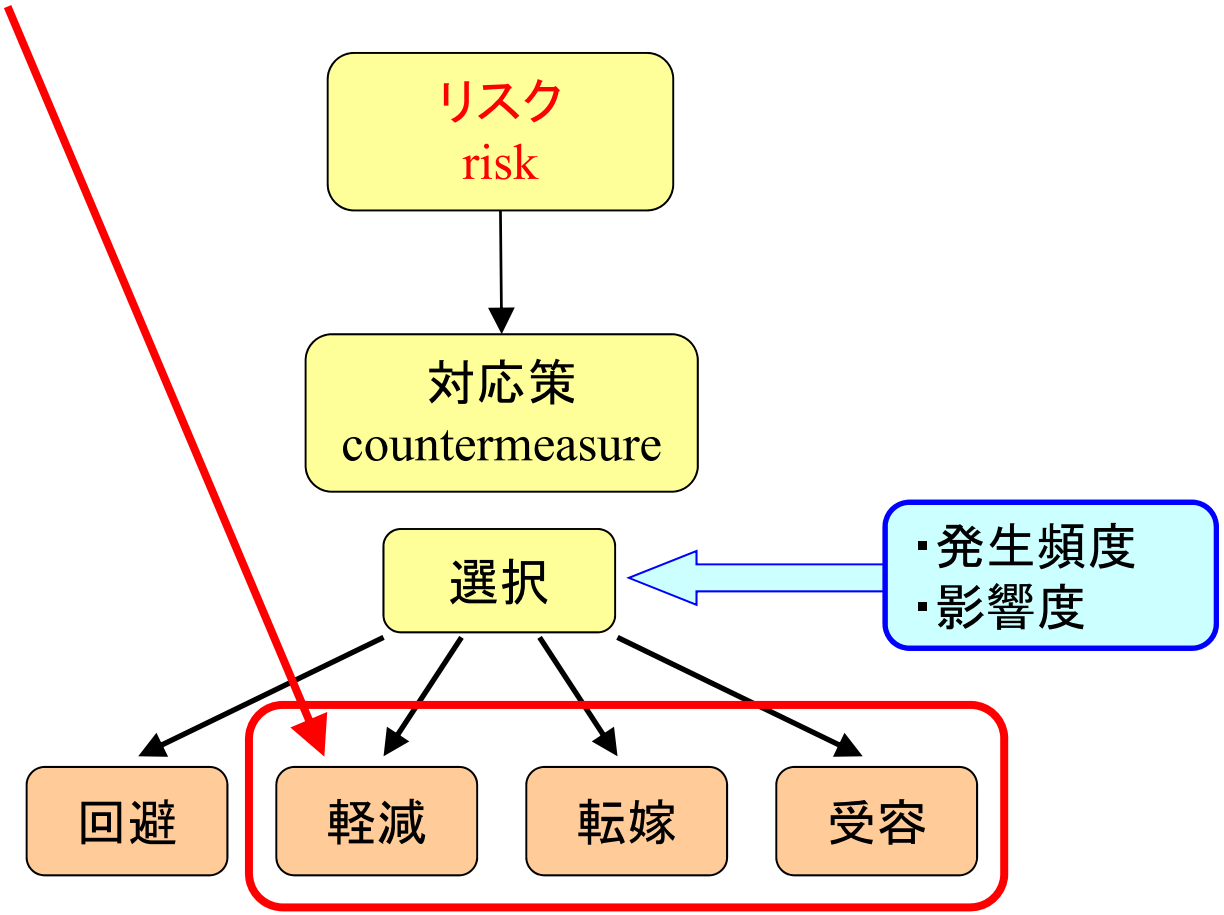
傾向と課題

傾向
- 情報セキュリティ対策の緩和
- CIAからAICへ
- 情報利用目的管理

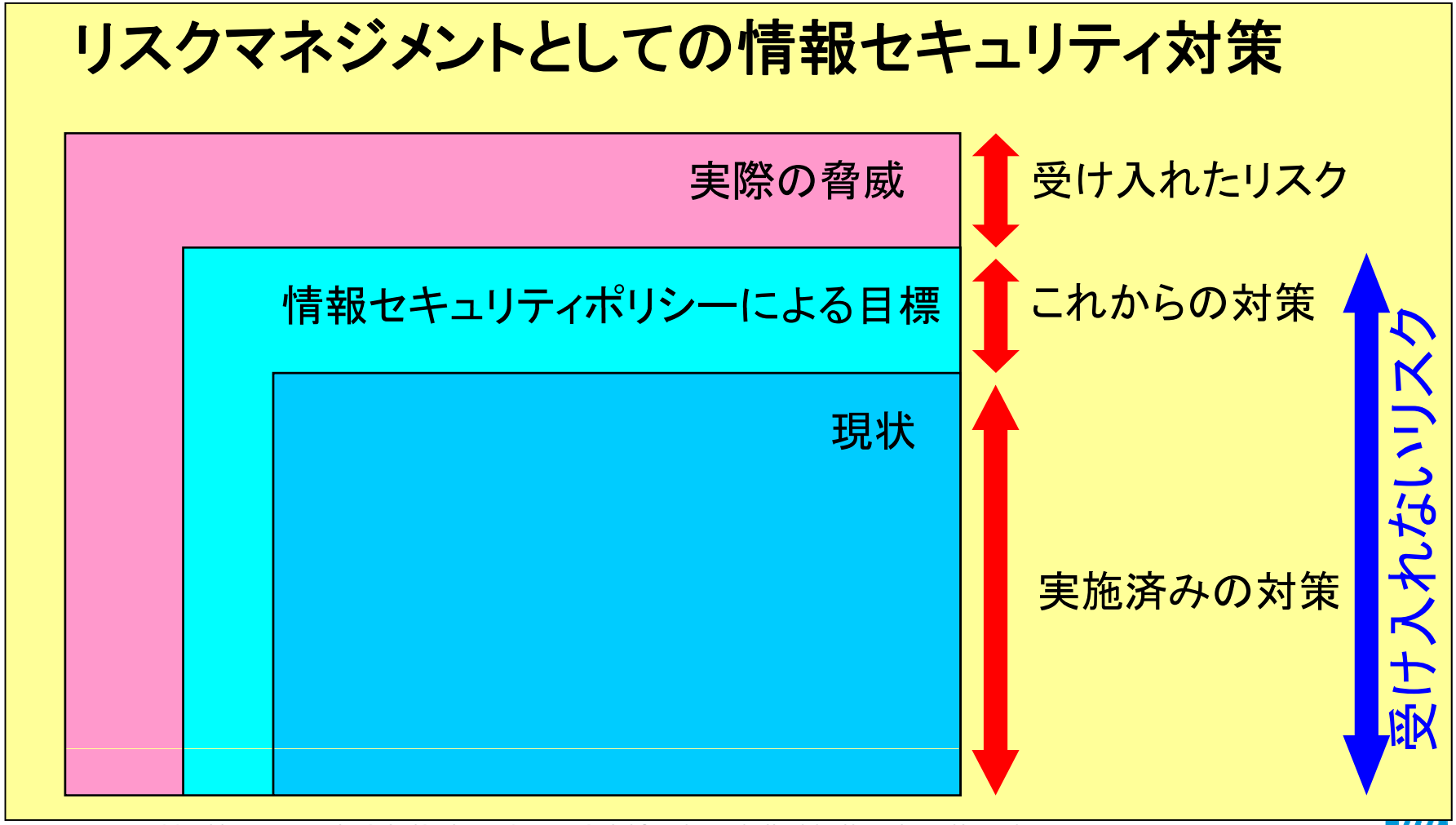
課題
- インシデントマネジメント
- 外部委託

リスクの傾向

回避しないリスクは減らしていける？？？

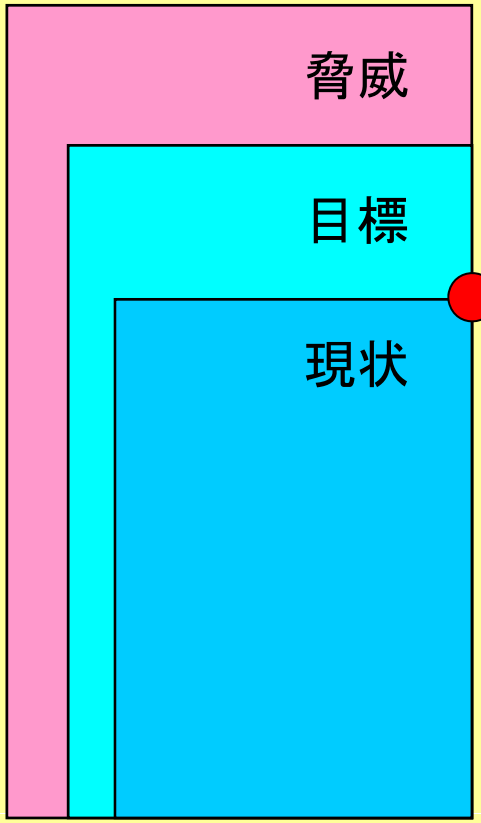


リスクの傾向
回避しないリスクは減っていくのか？



リスクの傾向
回避しないリスクは減らない

リスクマネジメントとしての情報セキュリティ対策



？

チャンス獲得とリスク回避のトレードオフ

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）

最低基準ではなく適正基準がビジネスに必要。
「何をすべきかだけでなく、何をしなくてもよいか」を示すことがビジネスには有用な場合がある。

CIAからAICへ
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。

CIAからAICへ
今後の方向性

CIAからAICへ

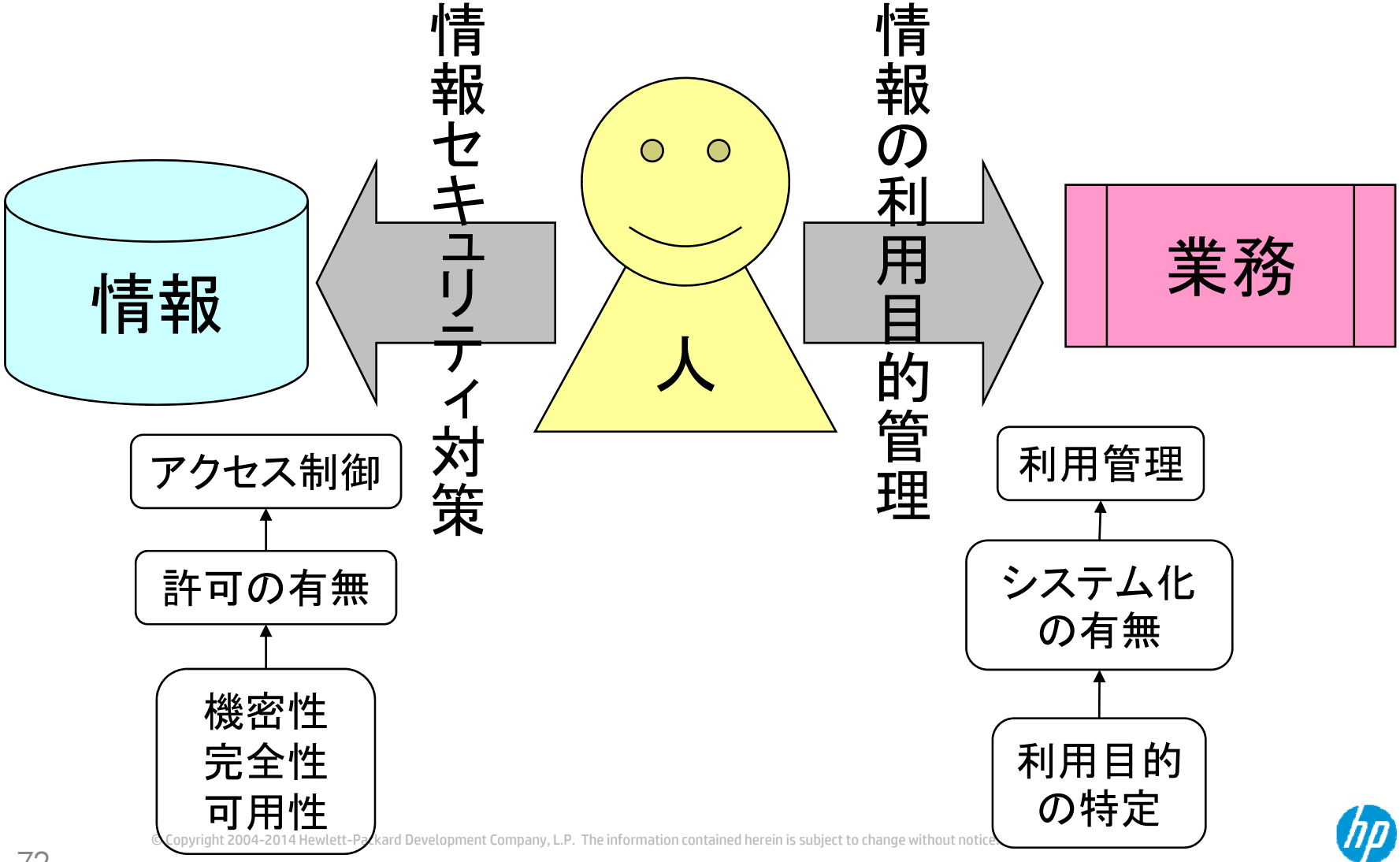
□実際には、Cに加えて+Iさらに+A

□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。

情報の利用目的管理



小まとめ
リスクマネジメントのすすめ

- 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
- リスク対応策の展開
- リスクの傾向

目次

1. ルール作りとリスクマネジメント
   大きな事故を防ぐためのアイデア
   ルール作りの基本的考え方
   リスクマネジメントのすすめ

2. システム管理者権限からもデータを守る
   権限の最小化と分割
   技術を有効にする運用

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・・・

リスクの傾向
回避しないリスクは減らない

性善説を前提にして、性悪説を想定する。

× 事故前提

○ 事故想定　又は　事故対応前提

悪いことができないようにする。→しかし、完全に防ぐことはできない。

悪いことができないように努める。

加えて、以下のことを予防する。

「悪いことだと知らなかった。」を防ぐ。→禁止事項

「悪いことだと思わなかった。」を防ぐ。→禁止目的

「悪いことだと知っていたが、ばれるとは思わなかった。」→記録重視

悪いことをすればできるが、やったらばれる仕組み作り。

総じて、周知・教育・訓練が重要。

システム管理者権限からも データを守る

デュアルロック（二重鍵）

司法取引

事後において

　原因究明を重視

事前にも

　抑止による未然防止

参考

- インシデントマネジメント

- 外部委託

インシデントマネジメントの基本
「事象（イベント）」と「インシデント」

- 組織では、インシデントへの対応手順や体制を整備しなければなりません。しかし、インシデントを迅速に対応できる体制が確立しても、日常的に発生している多くの事象を、現場の当事者がインシデントとして認識するのが遅れると、結果的に対応が遅れてしまいます。
- そのようにならないためには、インシデントと認識された以後のことばかりではなく、それ以前の事象にも広く注意をする必要があります。つまり、インシデントの管理をする際に、インシデントから始めるのでは不十分な管理策となってしまいます。
- そこで、インシデントとなる可能性や未知の状況を示している「事象」が、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高くなることで「インシデント」に変遷するという考え方をすることが重要であり、インシデントの管理では、インシデントになる前の事象も対象とする管理策を講じなければなりません。

インシデントマネジメントの基本「事前想定」と「想定外対応」

- 計画準備段階として事前計画に基づく対応手順を充実させて、実際のインシデント発生時に、手順に従って対応することを基本にしています。しかし、その一方で、計画準備段階に用意した手順がインシデントの実情に沿わないときには、手順以外の方法による対応をするための手続きが必要であることも指摘しています。なぜなら、インシデントとは、予測不可能な状況となることもあり、その場合には、事後対応を事前計画で想定した範囲内だけで実施することは、むしろ想定外の状況に柔軟に対応をできなくなる場合がるからです。そのため、想定外の状況に遭遇した場合には、実際の担当者の判断で、事前に定められた処置とは異なる例外処置をできるようにすることも必要です。そのような例外処置についても管理するような管理策を講じることについて述べています。

インシデントマネジメント

- ワンストップ＆ノンストップ
  - 事象を見落とさないようにする
  - 管理と判断、暫定対応、恒久対応、渉外対応
  - 事前計画の策定と、想定外（例外）対応の整備。
  - 事前計画：計画に沿った処理、役割分担、全員連携
  - 例外対応：計画に沿わない処理、役割排除、個別判断

- 解決策は問題の中にはない
  - 目的達成のために、手段を選ばないようにする

インシデントマネジメント

- 今後の課題:
  計測できないことは改善できない
  - ISO/IEC 27035 検討中
    Information Security Incident Management

インシデントマネジメント
ISO/IEC 27035

- ISO/IEC 27035 作成開始
  発行済みの ISO/IEC TR 18044 を差し替えるもの。
  発行済みの Security event と Security Incident によるモデルを踏襲する予定。(incident = unwanted & unexpected impact)
  インシデント処理そのものは、PDCAモデルを直接的には用いず、発行済みの before/during/after モデルを用いて改善する案で検討開始。
- （佐藤私見）
  Response time from the time when event was known のような考え方もひとつの考え方。

参考

インシデントマネジメント

外部委託

外部委託

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？？？

外部委託

委託先の誤った管理：

- 委託先に単にプライバシーマーク認証取得を指示する

→愚の骨頂

- 委託先に単にISMS認証取得を指示する

→誤解されやすい

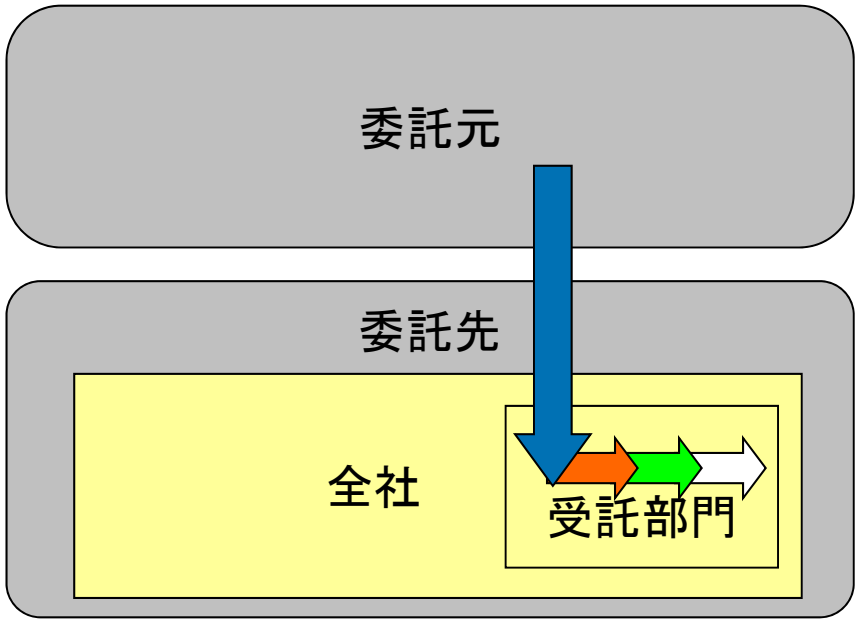
事業者として、社外への丸投げ体質は許されない。

委託はリスク転嫁策のように思われるが、事故発生後のことを考えれば、それが正しくないことは、すぐにわかること。

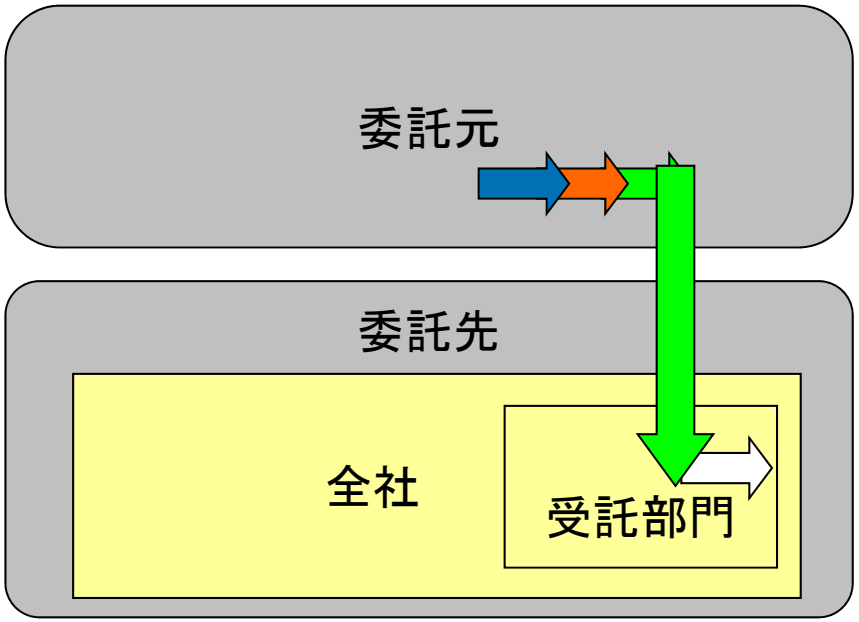
さらに、自社内の現場での責任意識・危機管理意識の希薄化を招くため、むしろ、百害あって一利なし。

27002を引用した場合のISMSと外部委託

よく見かける関係

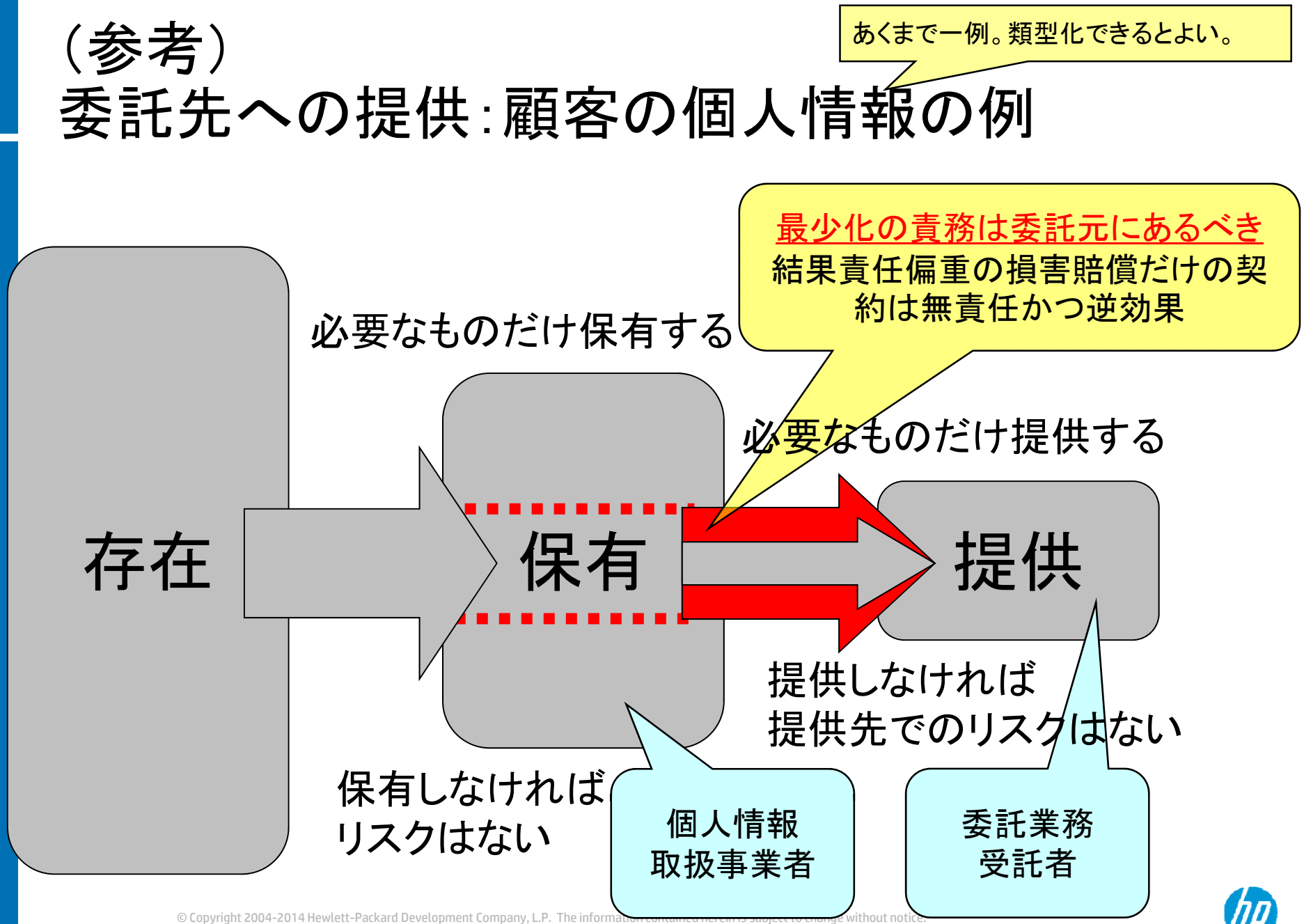


あるべき姿



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

（参考）
委託先への提供：顧客の個人情報の例



経済産業省個人情報保護ガイドライン改正案のパブコメ

http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595114087&Mode=0

電子政府パブコメ　検索

改正箇所：

個人情報の取得関係（法第１７条～１８条関連）

安全管理措置（法第２０条関連）

従業者の監督（法第２１条関連）

委託先の監督（法第２２条関連）

経済産業省個人情報保護ガイドライン改正案のパブコメ

http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595114087&Mode=0

電子政府パブコメ　検索

改正での問題

　委託先での対策の先細り

　損害賠償責任の偏重

もともとの問題

　目的と手段の区別が不明瞭

　「等」の乱用

　外形的な形骸化の懸念

　安全管理措置対策の主体

経済産業省個人情報保護ガイドライン改正案のパブコメ

http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595114087&Mode=0

電子政府パブコメ　検索

2-2-3-2.安全管理措置（法第20条関連）

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。その際には、特に、中小企業者においては、事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。また、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。なお、クレジットカード情報については、別添の「クレジットカード情報を含む個人情報の取扱いについて」に掲げられた措置を講じることが望ましい。

経済産業省個人情報保護ガイドライン改正案のパブコメ

http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595114087&Mode=0

電子政府パブコメ　検索

2-2-3-4.委託先の監督（法第22条関連）

③ 委託先における個人データ取扱状況の把握

委託先における委託された個人データの取扱状況を把握するためには、定期的に（少なくとも年１回）、監査を行う等により、委託契約で盛り込んだ内容の実施の程度を~~相互に確認する~~調査した上で、個人情報保護管理者（CPO）等が、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。

（現行）

委託先における委託された個人データの取扱状況を把握するためには、委託契約で盛り込んだ内容の実施の程度を相互に確認することが望ましい。

発表資料のダウンロードと録音の掲載
http://よしひろ.com/

お問い合わせ
twitter
http://twitter.com/4416sato