独立行政法人等における
個人情報の安全確保措置について

～組織におけるルール作りと情報セキュリティ対策～

2015年2月2日

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長
佐藤慶浩

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

自己紹介

佐藤　慶浩（さとう　よしひろ）

日本ヒューレット・パッカード（株）　個人情報保護対策室長

元　内閣参事官補佐・情報セキュリティ指導専門官（民間併任）

（内閣官房　情報セキュリティセンター）

【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　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　元・副理事長

デジタル・フォレンジック研究会　理事

【その他】

http://yosihiro.com/profile/

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

ルール作りとルール運用の基本

社員を信じること

※企業以外の組織の場合、社員は職員と読み替えてください。

日頃のコミュニケーション
主業務に非正社員がいるなら、
彼らとのコミュニケーションも必要

コミュニケーションが希薄なコミュニティ
住人同士の会話のない街の治安
隣席者同士の会話のない職場の情報セキュリティ

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

目次

1. ルール作りと運用
   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
   ルールを守る環境作り

2. すぐに使える対策例
   データ提供時に経路でデータを守る
   システム管理者権限からもデータを守る

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

大きな事故を防ぐためのアイデア
街の治安：凶悪犯罪を防ぐための試み

（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。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

（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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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。

大きな事故を防ぐためのアイデア
社内情報セキュリティ対策への応用

情報セキュリティに関する軽微なルール遵守を徹底する。

例）

社員証をいつも見えるように携帯・掲示する

機密文書にはすべて「機密」の明記をする

パソコンから離席時は短時間でも画面をロックする

など

→対策は毎日・全員で漏れなくやることだという意識

→対策に会社（全員）が注力しているのだという意識

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

大きな事故を防ぐためのアイデア
社内情報セキュリティ対策への応用

参考

政府が情報セキュリティ対策統一基準を発行したときに、
用いたスローガン

情報セキュリティ対策は、

誰かがいつかどこかでやってくれることではなく、

全員がいつも各自の職場でやることです。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

目次

1. ルール作りと運用
   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
   ルールを守る環境作り

2. すぐに使える対策例
   データ提供時に経路でデータを守る
   システム管理者権限からもデータを守る

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

「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

1.遵守事項(すべきこととしてはならないこと)を、会社が定めていること

2.遵守事項を、会社が社員に対して教育していること

3.遵守事項を、社員が理解していること

4.遵守事項を遵守することについて、社員が同意していること

5.社員による同意状況を、会社が把握していること

このとき、会社において、対象とする社員の範囲で、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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

「規程」の策定

理解の促進→用語と文体

用語などの定義

社内で通常用いている用語を使う
社内で従来使っていない用語を安易に使わない
（認証取得のために標準用語に対応する必要があるならば、
　審査員に対する社内用語と標準用語の対応表で対処）

主語の明確化
　誰が実施することかを具体的に明記する
　受動態の文章で書かない
日本語での留意事項
　カタカナの使用の最小化
　→避けられないカタカナ用語は丁寧に解説する
　→専門用語を社内教育でドヤ顔で説明するのは注意信号

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

「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（employee Must Do：～しなければならない）
推奨行為（employee Should Do:～することが望ましい）
禁止行為（employee Must Not Do： ～してはならない）
許諾行為（employee May Do： ～することができる）

行為の限定ではなく理解の促進

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）

決意表明と事前通知

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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

「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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

「規程」の策定

個々の規程条項に記載すること

WHAT(,WHEN,WHERE):
何をすべきか(してはならないか)
(対策の手段の例示)

WHY:
なぜ、それをすべきか(してはならないか)
(受け入れられないリスクの考察)

WHO:
誰がそれをすべきか(してはならないか)
(受け入れるリスクの考察)

個々の規程条項で考えておくべきこと

HOW: その遵守状況の確認方法と確認基準

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

「規程」の見直し
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

「規程」の見直し
参考：政府機関統一基準見直しの考え方

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。）

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

規程違反への対処

違反者には、謝罪させるのではなく、理由を説明してもらう。

ガバナンスとしては、原因の特定を最優先する

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（始末書ではなく）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

規程違反の発生は、規程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

軽微な違反の予防と再発防止を徹底する

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

規程作成の注意点

策定時の注意点：

社内用語を使うこと、慣れない用語・カタカナ用語を最少化すること

主語（誰が実施するのか）を明確にすること

述語（どの程度実施するのか）を明確にすること

例外発生を想定すること

実施可能なことに限ること　→　事前合意が前提

性善説を前提とすること

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）

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

目次

1. ルール作りと運用
   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
   ルールを守る環境作り

2. すぐに使える対策例
   データ提供時に経路でデータを守る
   システム管理者権限からもデータを守る

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

リスクマネジメントの実践

リスクマネジメントの実践

組織は事業継続、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。
これらに関する取り組みについて、紹介します。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

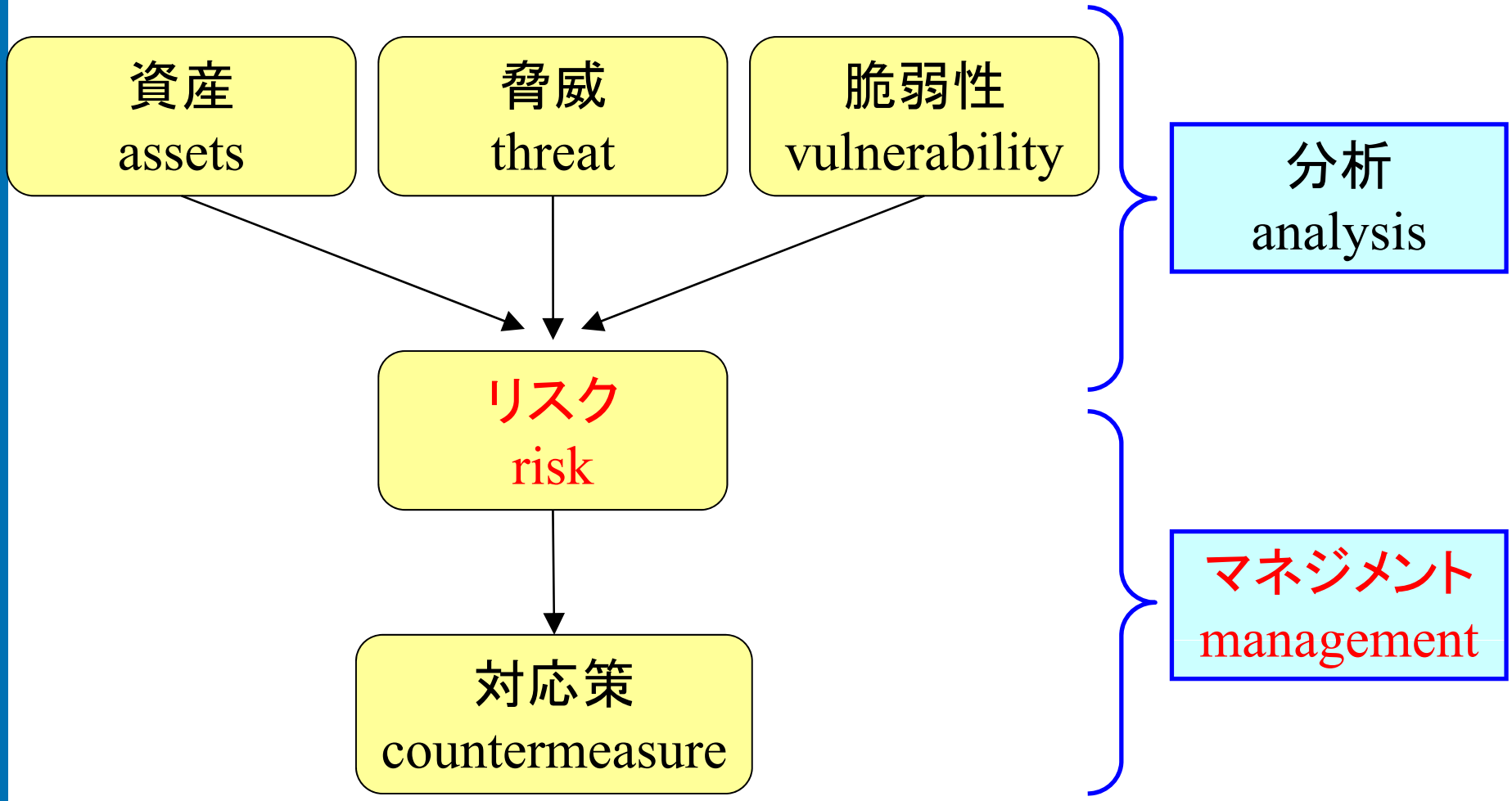
リスクマネジメントの実践

- 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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

リスクマネジメントとは

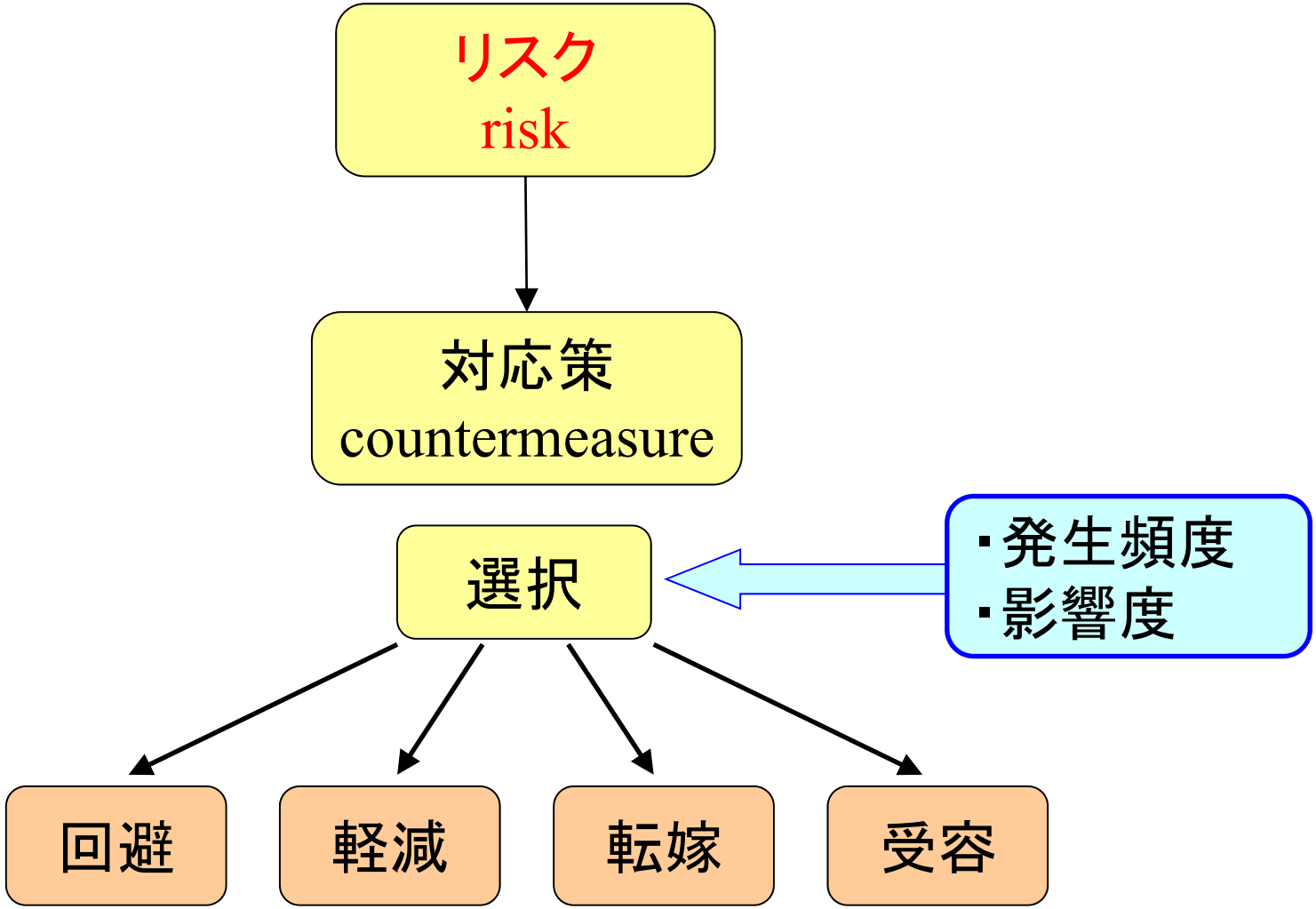
リスクマネジメントとは？



出典：CRAMM(CCTA Risk Analysis and Management Method)

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

リスクマネジメントとは？



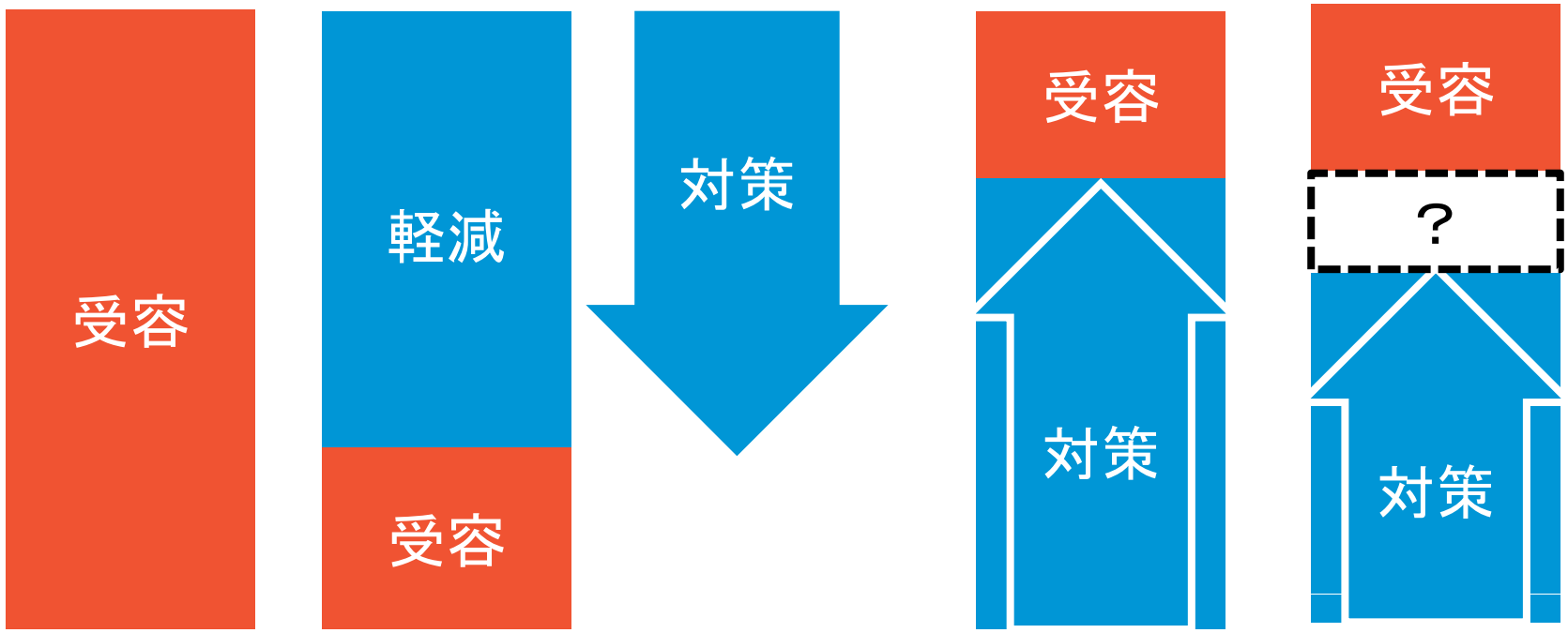
© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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



© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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・・・

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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。

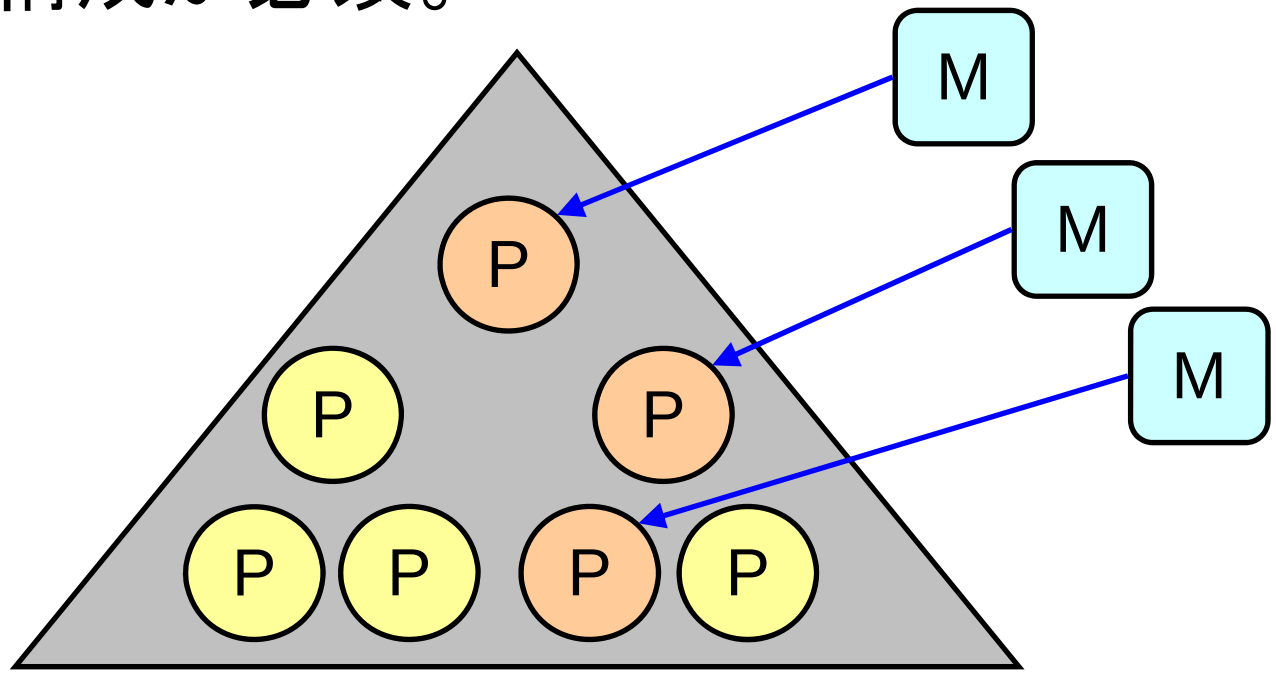
なぜなら、手順を裁量しているのが業務担当者である限り、業務担当者がリスクの分析やリスク対応策の選択をする部分があるため。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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。



© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

（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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

（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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

（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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

リスク対応策の展開

リスク対応策の展開
6つのチェックポイント

①性悪説だけでは組織は成り立たない

②性善説を前提とした対策

③不正行為の類型

④悪人を減らし、善人を増やす環境

⑤外部委託

⑥可視化

ルールを守る環境作り
4つのチェックポイント

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

ルールを守る環境作り　①

性悪説だけでは組織は成り立たない

- 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。。。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

ルールを守る環境作り 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。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

ルールを守る環境作り　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て保護との両立ができるルールを設けることが重要。

© Copyright 2010-2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

ルールを守る環境作り　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。

ルールが破られるという性悪説への対策は、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。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

ルールを守る環境作り　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悪人には効果がない。
- 悪人向け対策を担ってもらう善人が不可欠。
- 性善説を前提としない組織に非標準手順業務のリスク対応策の展開はあり得ない。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

ルールを守る環境作り 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

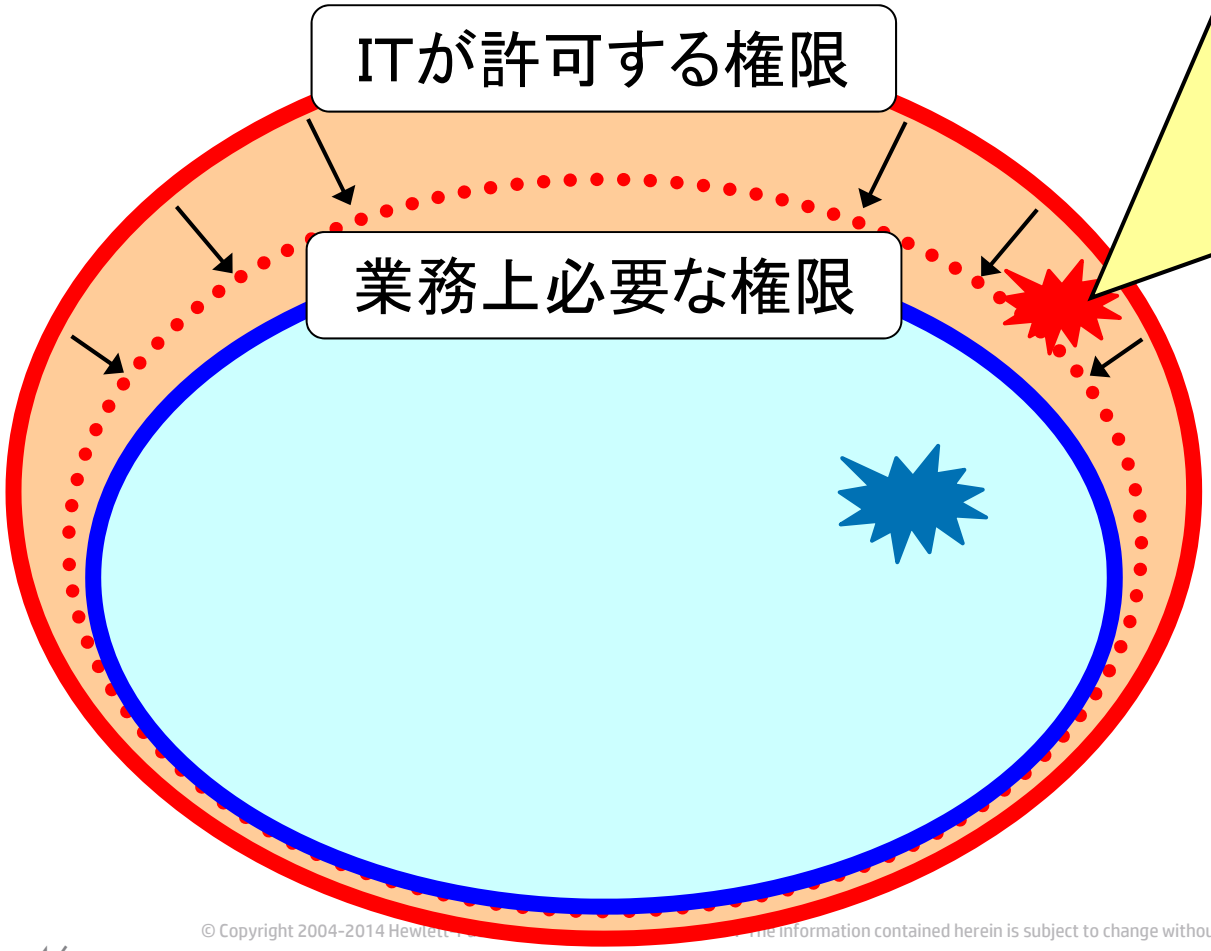
許可された者による不正行為（通称：内部犯）

- 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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

ルールを守る環境作り　③
不正行為の類型：権限の悪用

許可する権限の最小化



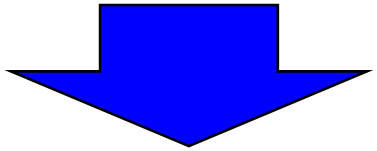
不必要な権限
を最小化する
↓
5W1Hの観点
で検証：
誰が？
何を？
いつ？
どこで？
どんな目的で？
どういう方法
で？

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

ルールを守る環境作り　④
悪人を減らすための環境作り

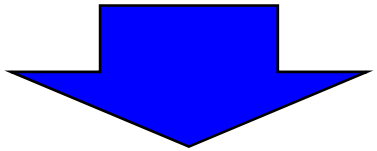
性悪説だけでは組織は成り立たない

- 性善説を前提にして、
- 性悪説を想定する



悪人を減らし、善人を増やす環境

- 基本は「正直者がバカをみない」環境



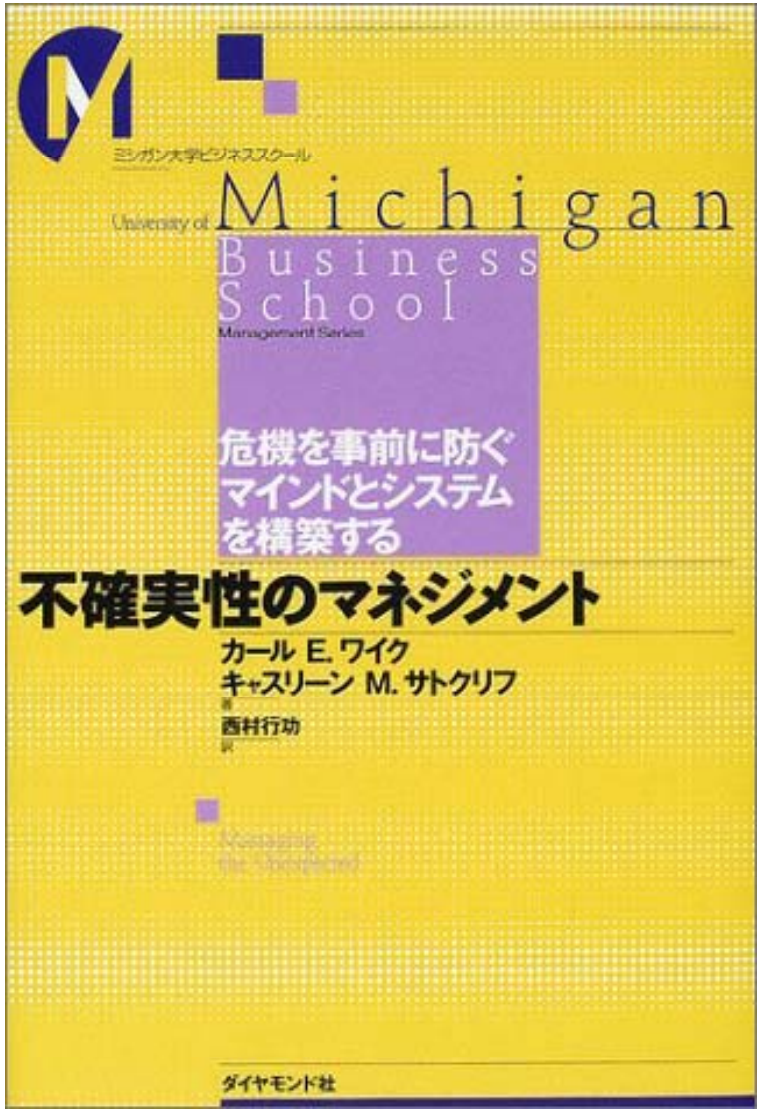
善人が増えれば・・・権限委譲できる

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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



© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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？

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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。。。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

リスク対応策の展開 ⑤
外部委託

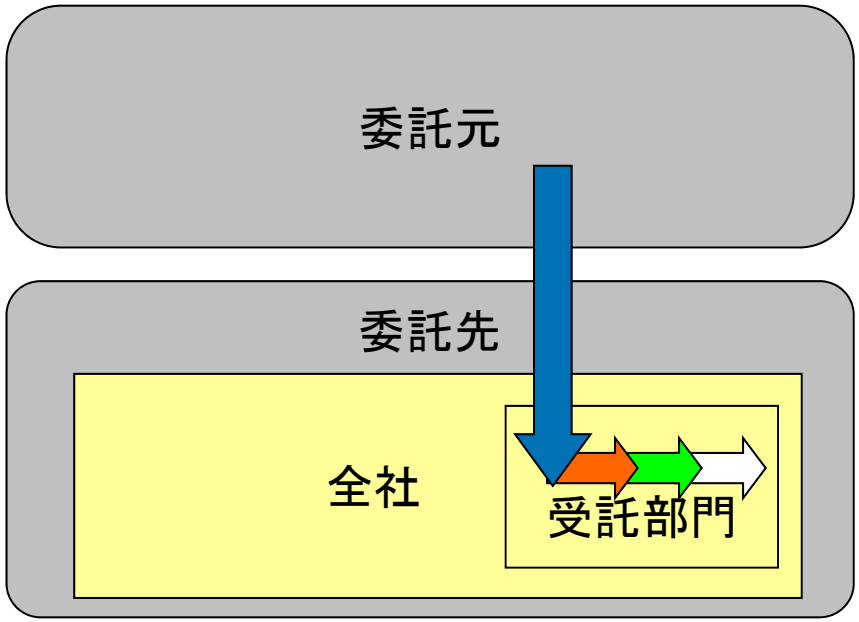
再確認すべき事項:

- 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？？？

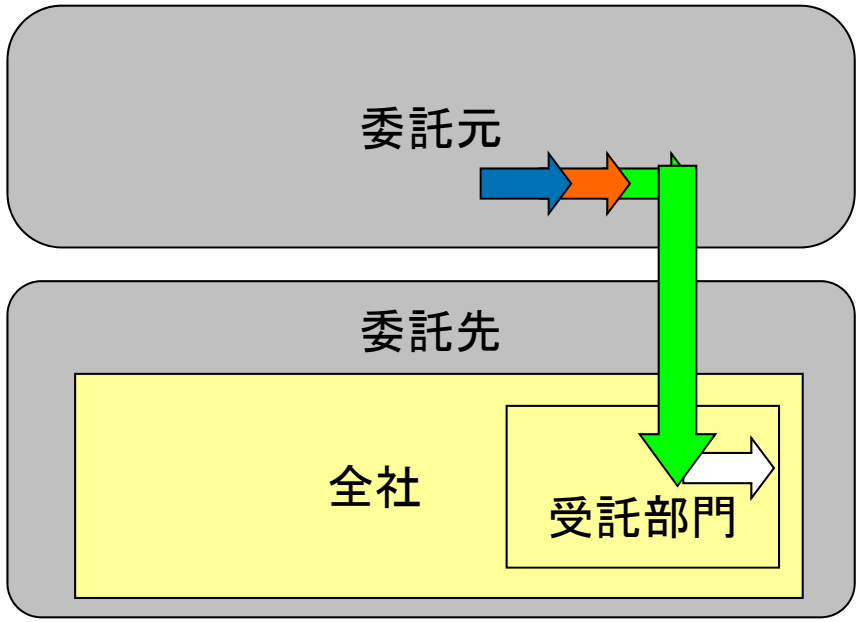
© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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？？？

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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."

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

（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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

リスク対応策の展開
6つのチェックポイント

①性悪説だけでは組織は成り立たない

②性善説を前提とした対策

③不正行為の類型

④悪人を減らし、善人を増やす環境

⑤外部委託

⑥可視化

ルールを守る環境作り
4つのチェックポイント

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

（参考）
ITアーキテクトによるセキュリティ設計

http://www.atmarkit.co.jp
/fsecurity/special/48arc/arc01.html

【特集】つぎはぎシステムを防ぐセキュリティアーキテクチャ

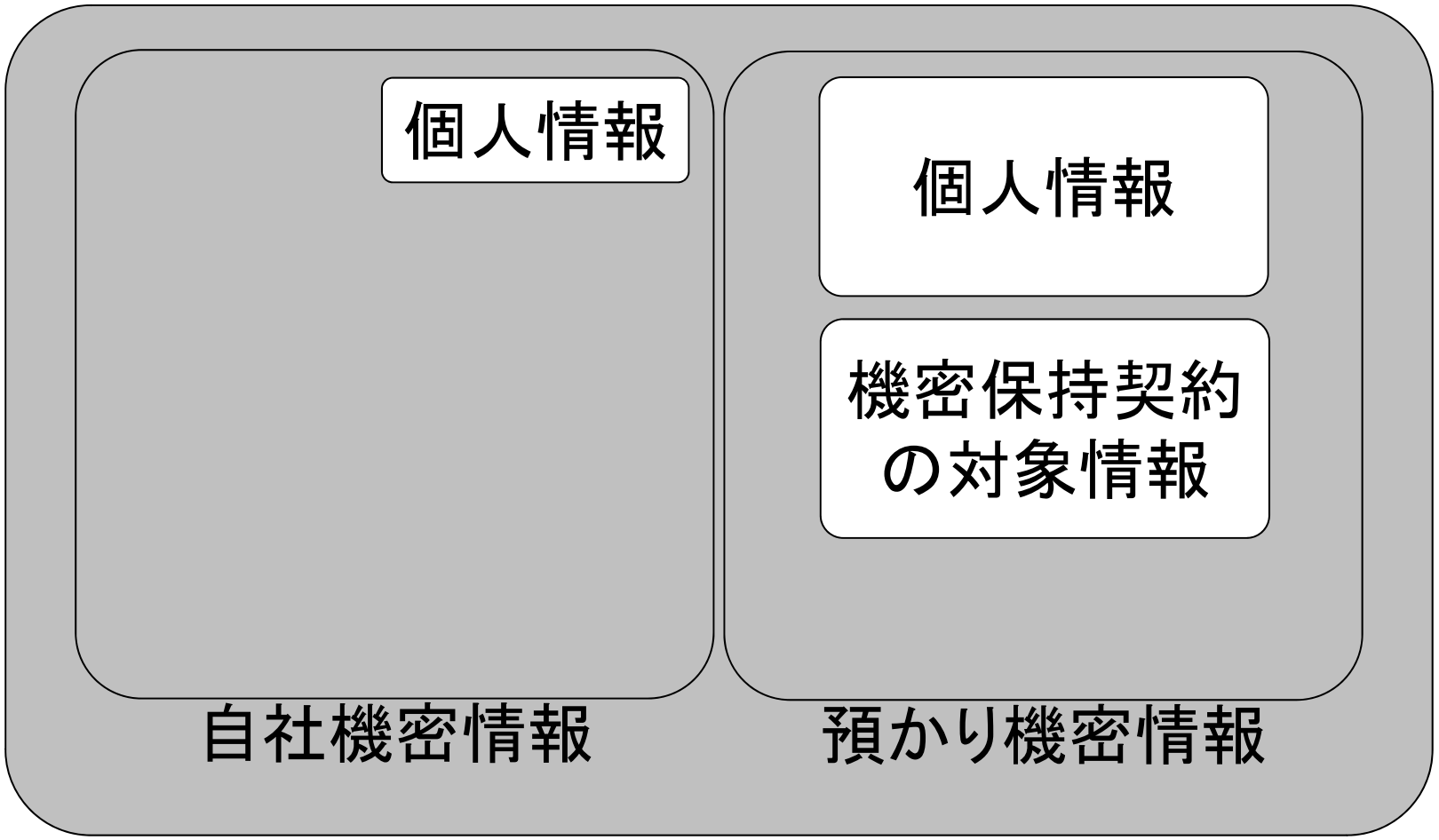
- SLAに見るセキュリティの位置付け
- セキュリティ要件の5つのA（真正確認、アクセス制御、権限管理、監査、保証）
- アイデンティティ・マネジメント
- プロビジョニング

※経済産業省個人情報保護法ガイドライン第２０条の補足説明としても有用な解説になっています。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

（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



© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

（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

http://www.meti.go.jp/policy/economy/chizai/chiteki/index.html

＞ 主要施策 | 営業秘密

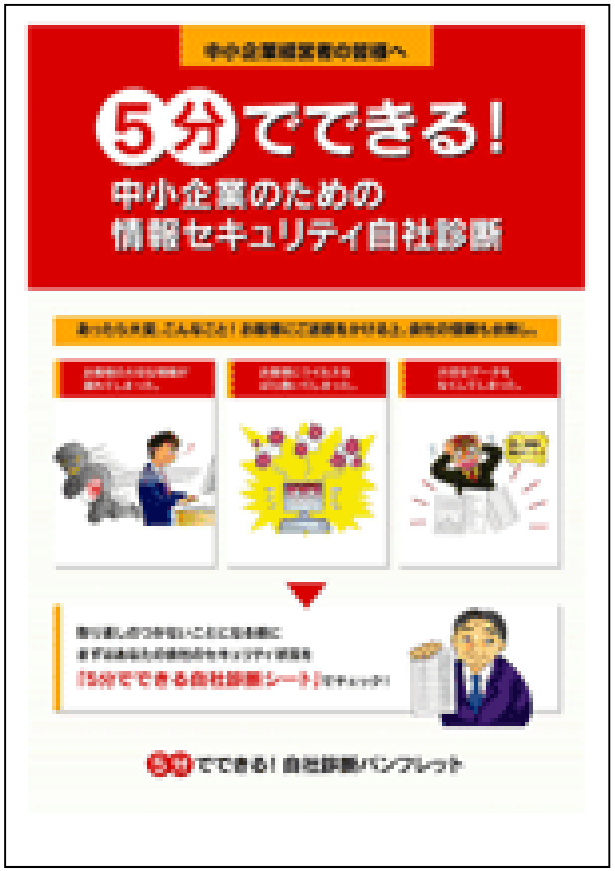
© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

（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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

（参考）
コストをかけずにできるセキュリティ対策

常識として知っておきたい個人情報保護法
　第5回：コストをかけずにできるセキュリティ対策
http://thinkit.co.jp/free/article/0606/1/5/

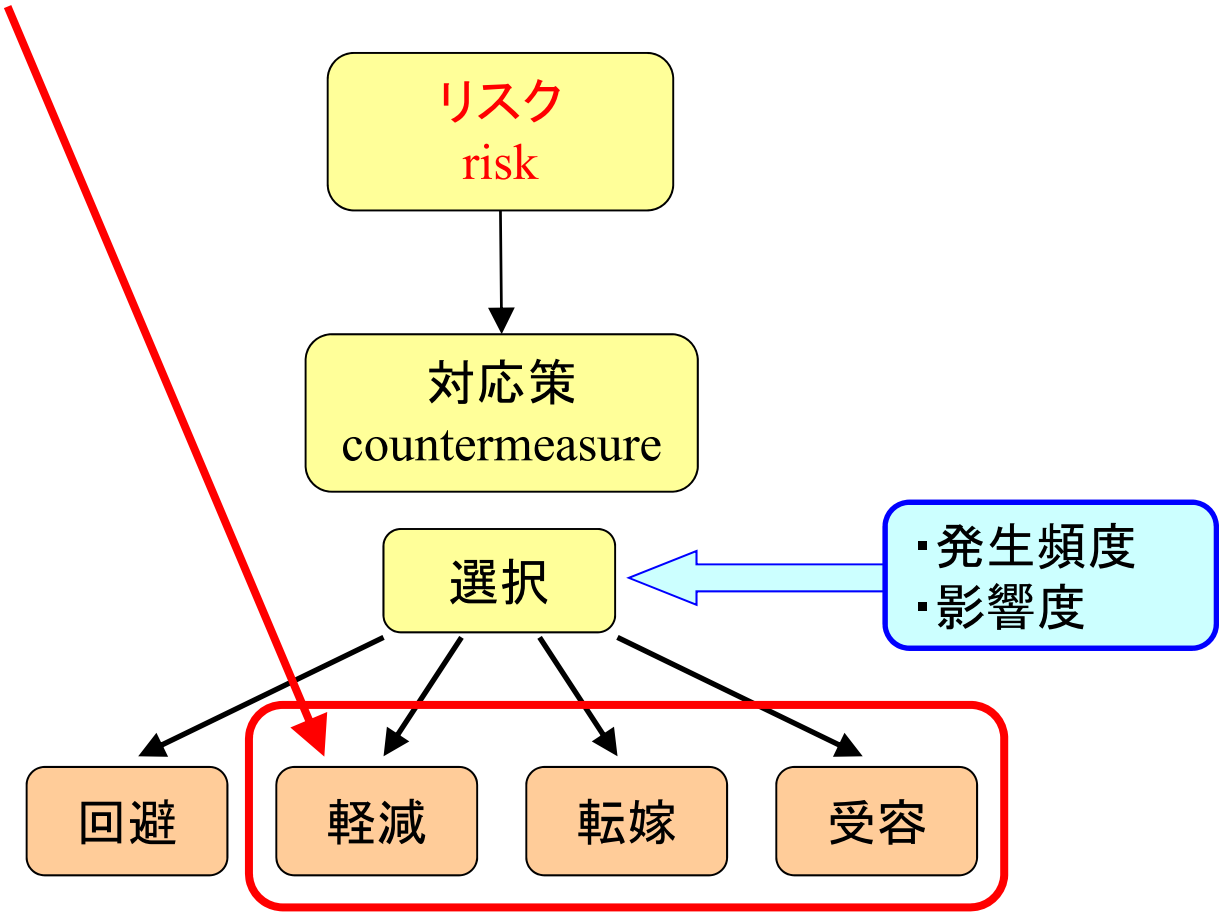
政府：内閣官房情報セキュリティセンター
政府機関の情報セキュリティ対策のための統一基準
http://www.nisc.go.jp/active/general/kijun01.html
政府機関統一基準適用個別マニュアル群
DM6-05：府省庁支給以外の情報システムによる情報処理の手順書 PC編 策定手引書
http://www.nisc.go.jp/active/general/pdf/dm6-05-101_manual.pdf

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

リスクの傾向

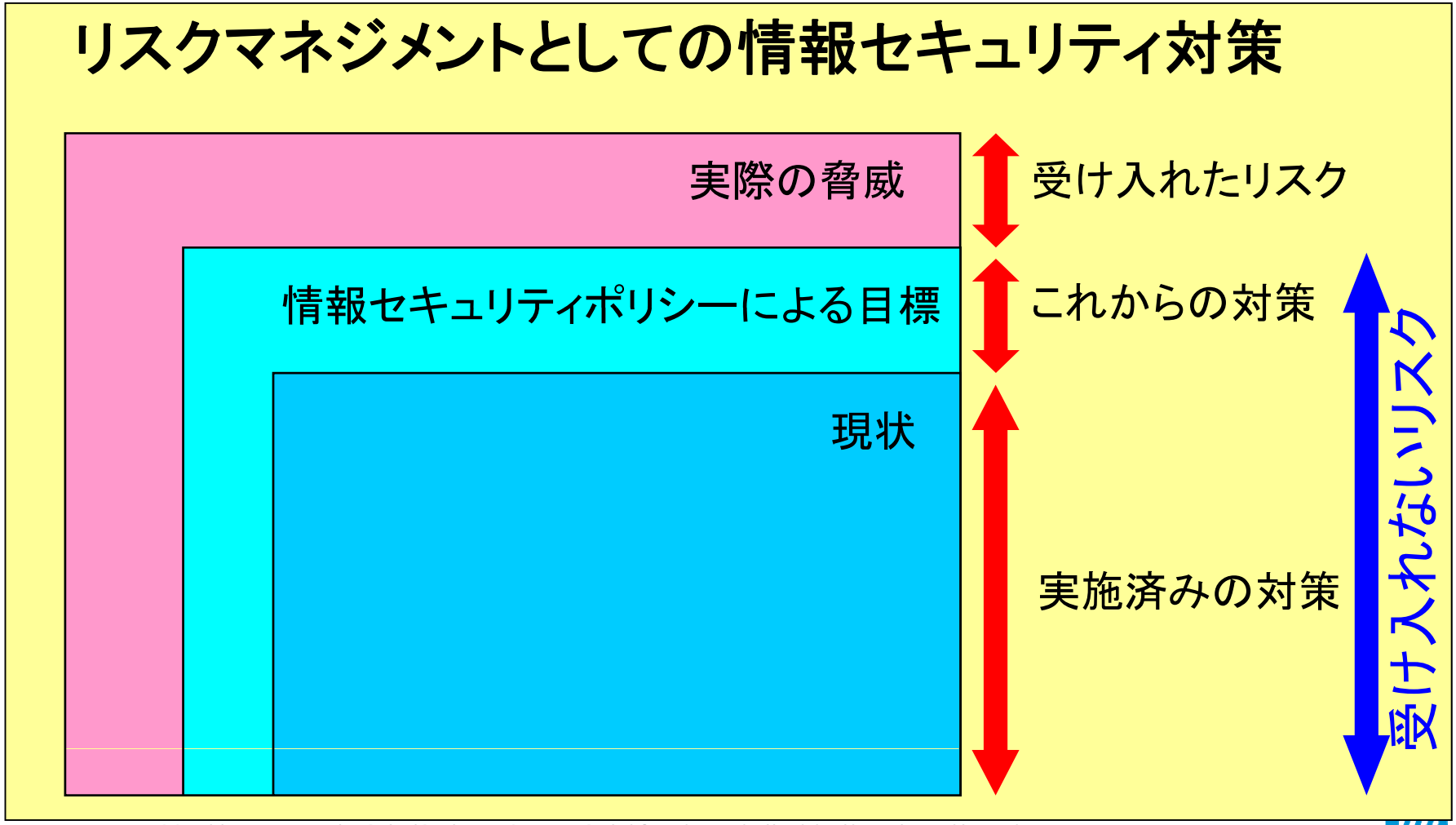
リスクの傾向

回避しないリスクは減らしていける？？？



© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

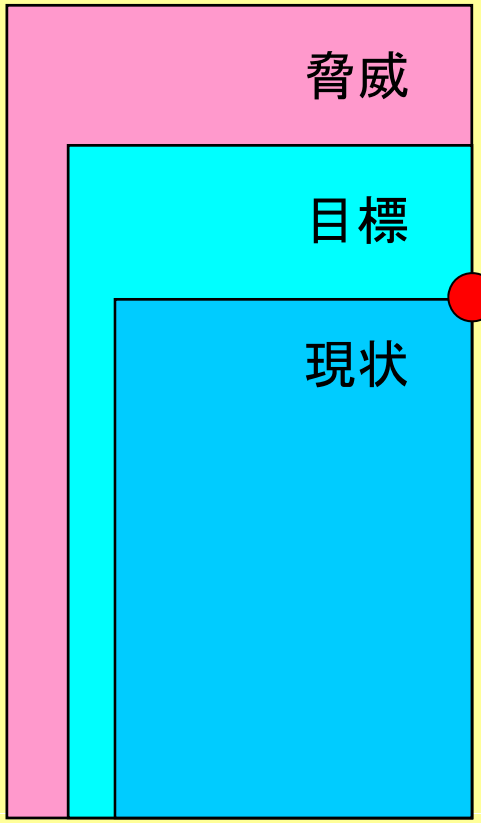
リスクの傾向
回避しないリスクは減っていくのか？



© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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事業に必要。
「何をすべきかだけでなく、何をしなくてもよいか」を示すことが事業には有用な場合がある。

© Copyright 2004-2014 Hewlett-Packard Dev

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。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

小まとめ
リスクマネジメントの実践

- 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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

目次

1. ルール作りと運用
   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
   ルールを守る環境作り

2. すぐに使える対策例
   データ提供時に経路でデータを守る
   システム管理者権限からもデータを守る

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

パスワード保護の危険性

パスワード保護は、時間をかければ必ず破られてしまいます。
多くの暗号化保護は、パスワードが破られると、どんなに強力な暗号も破られてしまいます。

デモ

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

データ提供時に経路でデータを守る秘密分散という技術の利用

・機密情報の安全な保管・移送に有益な技術

秘密分散
例）1080という数字を分散する

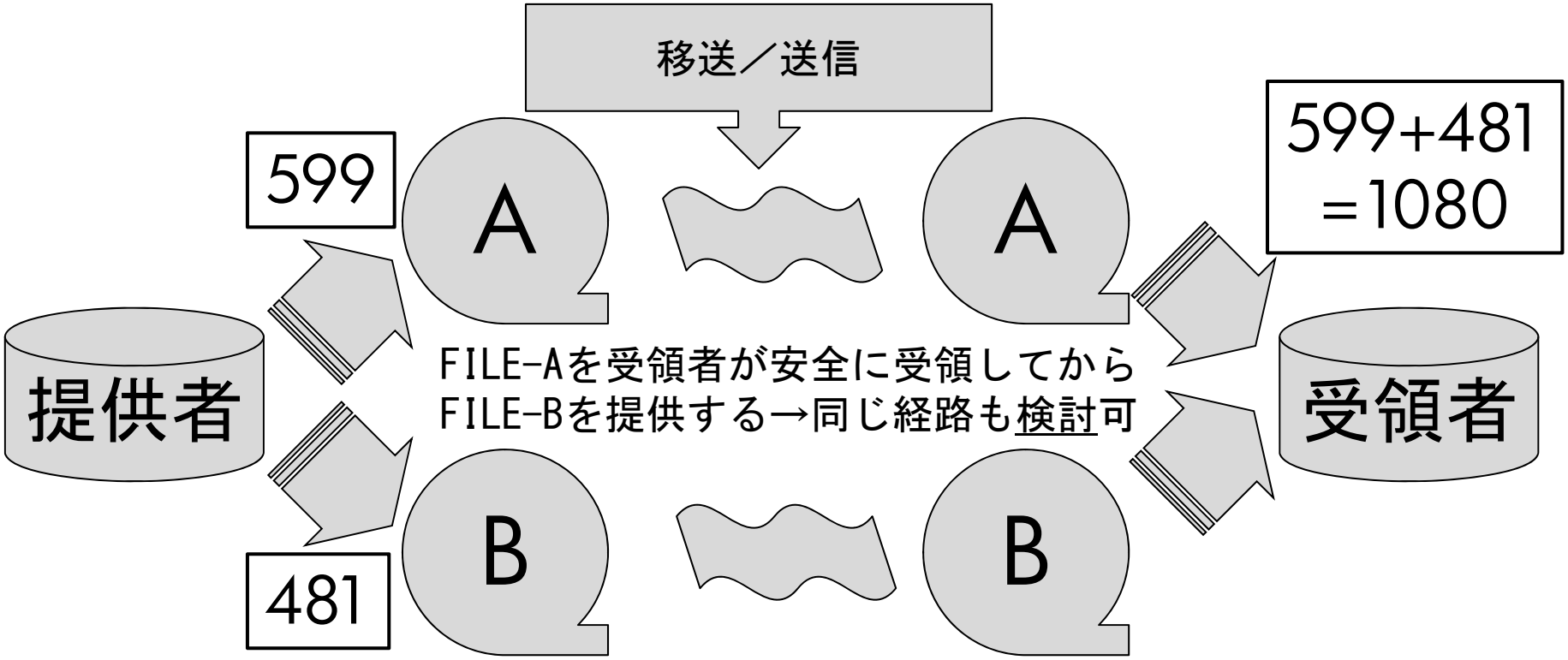
単純：桁の上と下で10と80に分割する
→10か80を知られると半分の情報がわかってしまう

ちょっと複雑：足し算を使って599と481に分割する（599+481＝1080）
→どちらかを知られても情報の一部もわからない

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

データ提供時に経路でデータを守る秘密分散という技術の利用

- 秘密分散による移送／送信



FILE-Aを受領者が安全に受領しなかったら、FILE-Bを破棄することで、FILE-Aの情報は無効になる。
秘密分散をやりなおす。たとえば、1080=672+408という分散にする。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

秘密分散の利用
機密ファイルの移送の具体的手順

- 作業用PCで機密ファイルを秘密分散ソフトを使って、FILE-AとFILE-Bに分散する。
- FILE-AとFILE-Bをそれぞれ記録メディア（CD-RやUSBメモリなど）に書き込む。
- 作業用PC上の機密ファイル、FILE-A、FILE-Bを抹消ソフトで抹消する。
- FILE-Aを移送する。
- FILE-Aの移送完了を確認してから、FILE-Bを移送する。

  ※FILE-Aの移送の安全性に問題があれば、FILE-Bを破棄することで、FILE-Aの情報は無効になるので、秘密分散をやり直す。
- 移送先のPCでFILE-AとFILE-Bを使って機密ファイルを復元する。
- 2つの記録メディアは移送先で破壊する。（破壊してもらう。）

© Copyright 2014-2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

秘密分散の利用
機密ファイルの送信の具体的手順

- 送信用PCで機密ファイルを秘密分散ソフトを使って、FILE-AとFILE-Bに分散する。
- 送信用PCで機密ファイルを抹消ソフトで抹消する。
- 送信用PCからFILE-Aを送信する。
- 受信者によるFILE-Aの受信を確認してから、FILE-Bを送信する。

  ※FILE-Aの受信の安全性に問題があれば、FILE-Bを破棄することで、FILE-Aの情報は無効になるので、秘密分散をやり直す。
- 受信者はFILE-AとFILE-Bを使って機密ファイルを復元する。
- 送信用PCから関連ファイルをすべて抹消ソフトで抹消する。
- 受信者はFILE-AとFILE-Bを抹消ソフトで抹消する。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

データ提供時に経路でデータを守る秘密分散という技術の利用

・機密情報の安全な保管・移送に有益な技術

秘密分散
例）1080という数字を分散する

実際には2進数にして排他的論理和という計算をします
排他的論理和(Exclusive OR, ExOR)の特性
A ExOR B = C ← Bを乱数にするとAがBとCに分散
B ExOR C = A ← BとCからAを復元できる

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

データ提供時に経路でデータを守る秘密分散という技術の利用

Microsoft Excel - ExOR.xls

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1															
2		桁重み	1024	512	256	128	64	32	16	8	4	2	1		
3		平文	1080	56	56	56	56	56	24	8	0	0	0		
4		平文	1	0	0	0	0	1	1	1	0	0	0	(10000111000)2	
5		平文	1024	0	0	0	0	32	16	8	0	0	0	1080	
6		乱数	1122	98	98	98	98	34	2	2	2	2	0		
7		乱数	1	0	0	0	1	1	0	0	0	1	0	(10001100010)2	
8		乱数	1024	0	0	0	64	32	0	0	0	2	0	1122	
9		ExOR	0	0	0	0	1	0	1	1	0	1	0	(00001011010)2	
10		ExOR	0	0	0	0	64	0	16	8	0	2	0	90	
11		ExOR	90												
12		検算													
13		ExOR	1	0	0	0	0	1	1	1	0	0	0	(10000111000)2	
14		ExOR	1024	0	0	0	0	32	16	8	0	0	0	1080	
15															
16			1080 ExOR 1122 = 90												
17															
18					1122 ExOR 90 = 1080										
19															

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

目次

1. ルール作りと運用
   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
   ルールを守る環境作り

2. すぐに使える対策例
   データ提供時に経路でデータを守る
   システム管理者権限からもデータを守る

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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

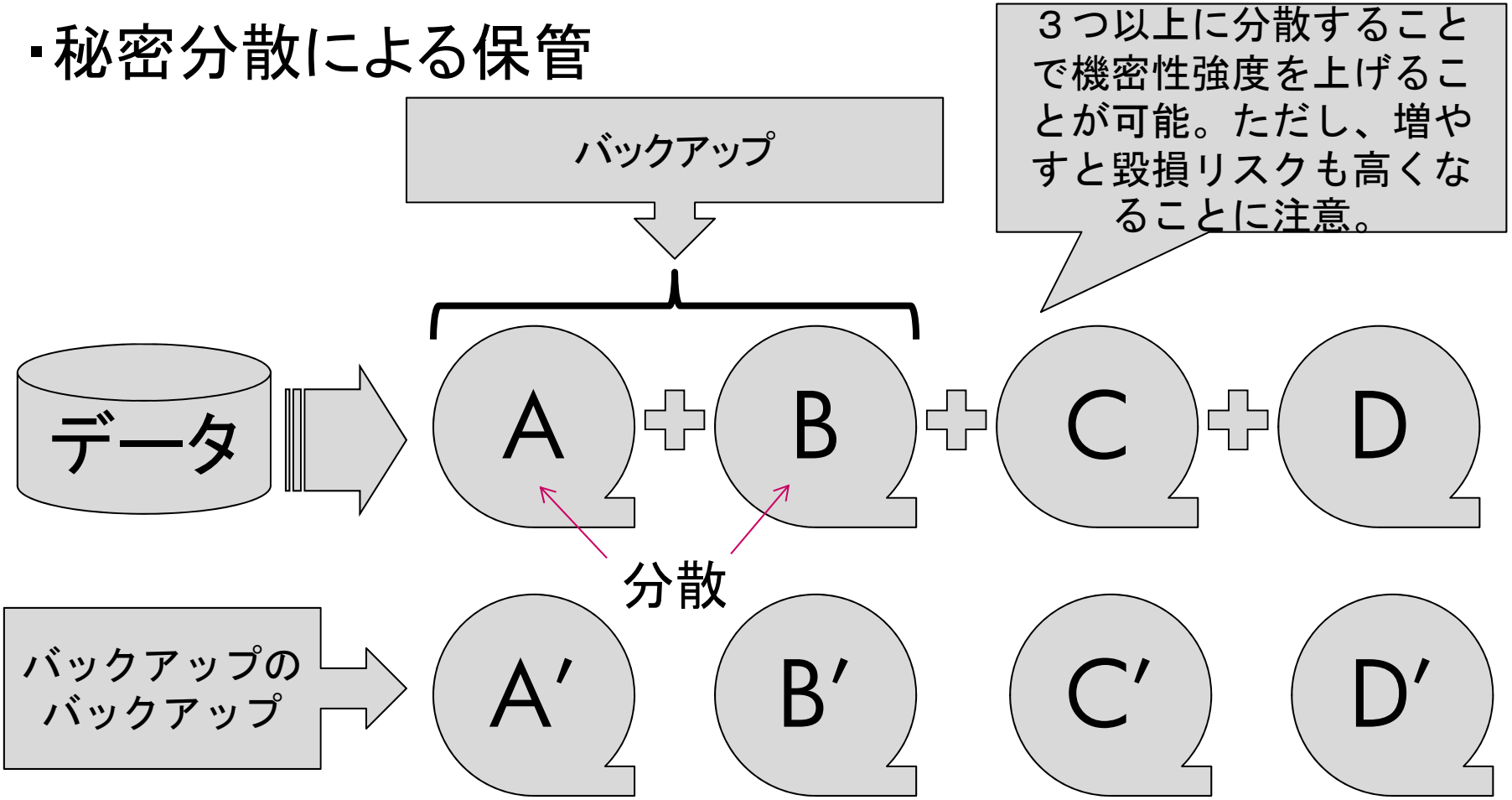
脅威や脆弱性を生じる事象の分類:

- 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・・・

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

システム管理者権限からもデータを守る秘密分散という技術の利用

- 秘密分散による保管



© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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)
免責制度(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

すぐにできる対策:
　システム管理者のパスワードを2つ以上に分割して管理

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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。

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

ルール作りとルール運用の基本

社員を信じること

※企業以外の組織の場合、社員は職員と読み替えてください。

日頃のコミュニケーション
主業務に非正社員がいるなら、
彼らとのコミュニケーションも必要

コミュニケーションが希薄なコミュニティ
住人同士の会話のない街の治安
隣席者同士の会話のない職場の情報セキュリティ

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

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

© Copyright 2004-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.