パネル・ディスカッション：

企業がセキュリティを守りやすくするには？

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10月30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
- 情報ネットワーク法学会　運営担当副理事長
- 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

©1996-2010 佐藤慶浩

「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

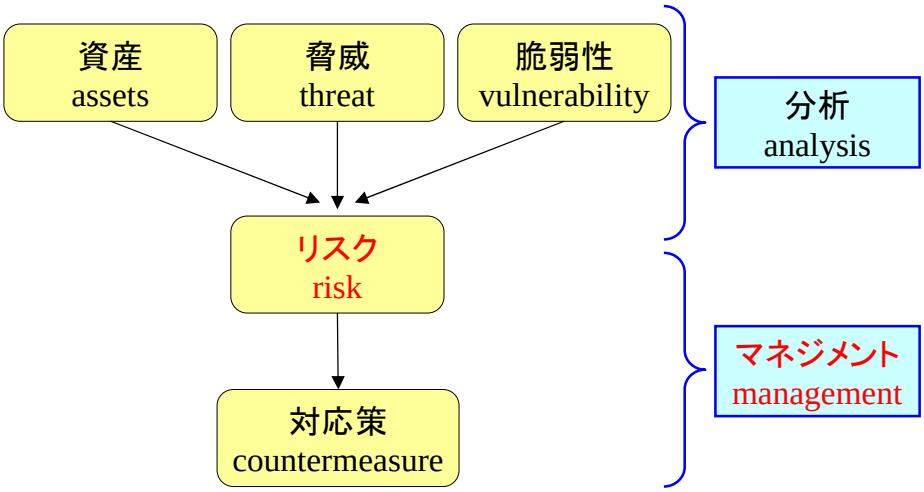
このとき、この組織において、その構成員の範囲で、遵守事項のガバナンスが構築されている。

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

©1996-2010 佐藤慶浩

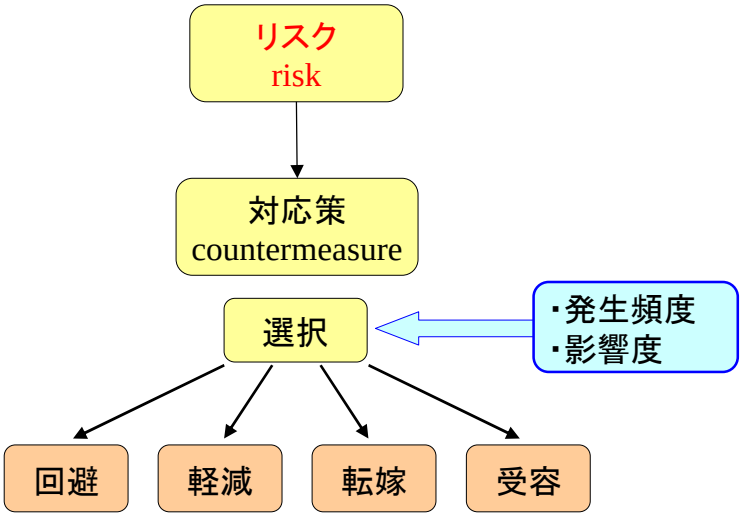
リスクマネジメントとは？



出典:CRAMM(CCTA Risk Analysis and Management Method)

©1996-2010 佐藤慶浩

リスクマネジメントとは？



 ©1996-2010 佐藤慶浩

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バランス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

 ©1996-2010 佐藤慶浩

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。

必ず遵守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、結果的に企業の内部統制レベルを向上することができる。
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、「ルールは必ずしも守らなくても良い」という意識を持たれることは好ましくない。
具体的な遵守方法が十分検討されていないようなルールを設けることは論外。
ビジネスの要求に即したバランスを保つ、事前合意されたルールを設けることが重要。

性善説を前提。性悪説も想定。

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。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。

©1996-2010 佐藤慶浩

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。

©1996-2010 佐藤慶浩

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
  - 技術面：アクセス制御による防御・多重の防御

悪意あり

許可された者による不正行為（通称：内部犯）

- 誤操作・過失
  - 誤操作を軽減する設計
  - 啓発、教育、訓練

悪意なし

- 権限の悪用
  - 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

悪意なし　悪意あり

©1996-2010 佐藤慶浩

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

↓

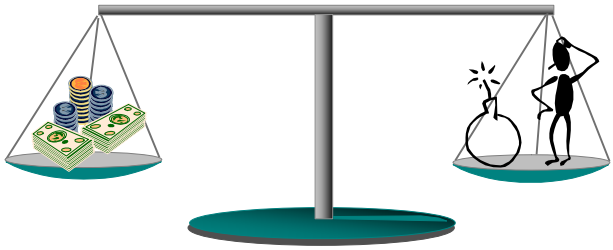
性善者が増えれば・・・権限委譲できる

©1996-2010 佐藤慶浩

全社情報セキュリティポリシーの策定

情報セキュリティに対する基本姿勢

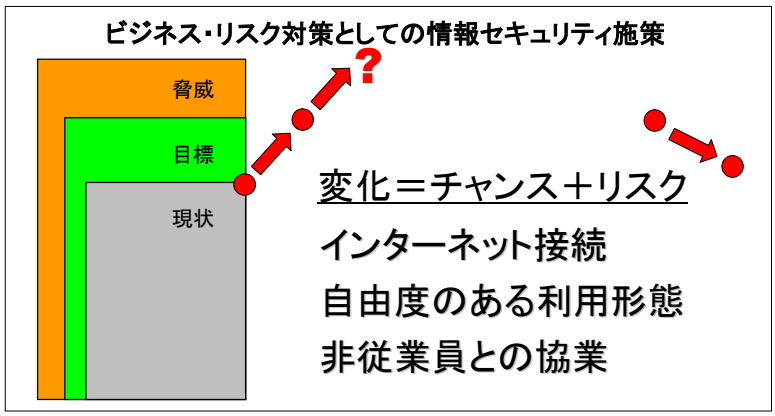
「情報資産に対するアクセスへのビジネスニーズ」と「これらの資産の機密性、保全性、可用性および適正な使用を守る」との効果的なバランスを取る。



 ©1996-2010 佐藤慶浩

全社情報セキュリティポリシーの策定

Step 1.5.1 目標設定とその根拠→本文（WHAT）と目的（WHY）



環境の変化には、もれなくリスクの認識が必要

 ©1996-2010 佐藤慶浩

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

Step 1.5.2 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

 ©1996-2010 佐藤慶浩

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

Step 1.5.2 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）

行為の限定ではなく理解の促進

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）

 ©1996-2010 佐藤慶浩

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

Step 1.5.3 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

方針内のそれぞれに異なる条件を記載可。　　一般的規則とﾎﾟﾘｼｰの違い

 ©1996-2010 佐藤慶浩

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

Step 1.5 個々のﾎﾟ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

 ©1996-2010 佐藤慶浩

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

 ©1996-2010 佐藤慶浩

「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）

 ©1996-2010 佐藤慶浩

社内標語の例：HP is protected by you

「内閣官房からの政府機関及び国民向けメッセージ」にも同じ

情報セキュリティ対策は、「誰か」が「いつか」がすることではありません。

情報セキュリティ対策は、「どこかの部署の人」が「ある時期」にすることでもありません。

情報セキュリティ対策は、「みんな」が「いつも」することです。

最近は、あなたは、どんな情報セキュリティ対策をしましたか？

 ©1996-2010 佐藤慶浩

宣伝：情報ネットワーク法学会　研究大会

開催日：12月11日（土）

開催場所：成城大学

基調講演のテーマ：「クラウドをめぐる3つの視点」

個別研究発表募集
ポスターセッション発表募集
参加申し込み受付

すべて本日から！

 ©1996-2010 佐藤慶浩