～エンジニアも知らなきゃならない財務会計～

情報セキュリティにおける"成果"の構成要素

日本マイクロソフト株式会社
チーフセキュリティアドバイザー
高橋　正和

Microsoft

当プレゼンテーションの注意書き

- 経営者や経営学の専門家が書いたものでもありません
- 技術者が経営に関わっていく中で、「そういえば、だれも教えてくれなかった」と感じた点を、自分なりに整理したものです
- もしかすると、若手向けの資料に見えるかもしれませんが、自分では、経営陣と交渉する、または、図らずも経営陣になってしまった人向けに作っているつもりです

- そして、自分自身が経験した内容に基づいたものですが、必ずしも一般的な内容とはかぎりません。

Who am I

- 高橋　正和
  - 日本マイクロソフト株式会社
  - チーフセキュリティアドバイザー
- もともとはソフトウェア開発者・開発環境構築
  - マイコン、パソコン、ミニコン、汎用機
  - 標準ソフト、アプリケーション、開発環境、ネットワーク
- なぜか、1年の米国営業所駐在（コントローラーのアシスタント）
  - 初めて経営にかかわる
  - 自分の作った製品を売る人たちを知る
- 独自ＯＳをWindows NT/XPへの移行＋品質管理
  - 帰国後、引き続き標準ライブラリを担当しSocketライブラリなんかも作る
  - その後、ＯＳ部門のマネージャー（課長代理）へ
  - 独自ＯＳから、Windows NTへの移植プロジェクトを担当
  - その後、品質管理（検査課）の課長も担当
    - なんと、企画、開発、検査、出荷調整を担当

Who am I

- 1999年にインタネットセキュリティシステムズへ
  - 技術マネージャー、全社員で20人、社員番号は25番。
    - MAX 200人＋α、2005年にＩＢＭにより買収
  - サポート、プリセールス、ローカライズ、教育などを担当
    ≒技術関係は全部
  - セキュリティコンサルティングビジネスの立ち上げ
  - CIOとして社内システムの管理
  - CTOとして新技術の適用とビジネス開発
- 2006年から日本マイクロソフト
  - 製品カットではなく、マイクロソフトとしてのセキュリティの取り組みを、顧客、業界団体、政府機関、メディアなどに伝えていく役割
  - 日本からの本社へのフィードバックも行う
    - ただし、セキュリティに限る

AGENDA

- 良い会社って何だろう？正しい仕事ってなんだろう？

- 経営へのファーストコンタクト
  - 内部的なサプライチェーンモデル
- ロールという考え方
  - 年功序列モデルとロールモデル
- 事業のプロシージャ
  - リズム・オブ・ビジネス
- 計測すること、評価すること
  - ゲームの本質

- セキュリティROIの考察
  - リスクと想定損害額
  - 計測するためのセキュリティの定義
  - セキュリティの投資対効果

良い会社？
正しい（会社 | 仕事 | 考え）？

私のマネジメントに対する理解の歴史

EPISODE-I:経営へのファーストコンタクト

- 駐在員として、米国ブランチに赴任
  - コントローラーや、GMと一緒に活動
- ビジネスの流れ
  - 製品を入荷し、販売し、サポートする
  - 経理処理をし、計画をする
- オペレーション
  - 日本とは異なる給与体系
  - 営業現場との経営陣の関係

はじめてのフォアキャスト

		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
計画	在庫（月初）	6	6	8	5	6	7	5	6	8	5	6	5
	販売台数	6	6	8	9	10	11	9	10	12	9	13	15
	入荷	6	8	5	10	11	9	10	12	9	10	12	14
	在庫（月末）	6	8	5	6	7	5	6	8	5	6	5	4
	発注台数	5	10	11	9	10	12	9	10	12	14	8	9
実績	在庫（月初）	6	7	10	6	4	3	0					
	販売台数	5	5	9	10	12	11	10					
	入荷	6	8	5	8	11	8	11					
	在庫（月末）	7	10	6	4	3	0	1					
	発注台数	5	8	11	8	11	12	9					
差	在庫（月初）	0	1	2	1	-2	-4	-5					
	販売台数	-1	-1	1	1	2	0	1					
	入荷	0	0	0	-2	0	-1	1					
	在庫（月末）	1	2	1	-2	-4	-5	-5					
	発注台数	0	-2	0	-1	1	0	0					

発注に関する管理を行うだけなのだが、これだけでも結構難しい。
発注後2か月で入荷することにしている仕組み
この例では、9月に在庫が無くなり機会損失が発生したシナリオ

ＧＭのフォアキャストへのつぶやき
（ほんとにそう思っていたかは不明）

Sales Forecast is something like crystal ball

若手技術者頃の給与のイメージ

給与 = f(自分の能力)

自分の業務に応じて、
企業が責任をもって払うべき

会社

主に開発業務

製品開発

少しわかってきた給与のイメージ

給与 = f(売上)

売上が立たないと、
給料の原資がない事に気づく

売上

主に開発業務

製品開発 → 生産 → 出荷 → サポート

受注 → 出荷

加えて…

- エンジニアの給与 > マネージャーの給与
- 離職や解雇の仕組みの違い

EPISODE-II: 米国ベンチャー企業での技術責任者

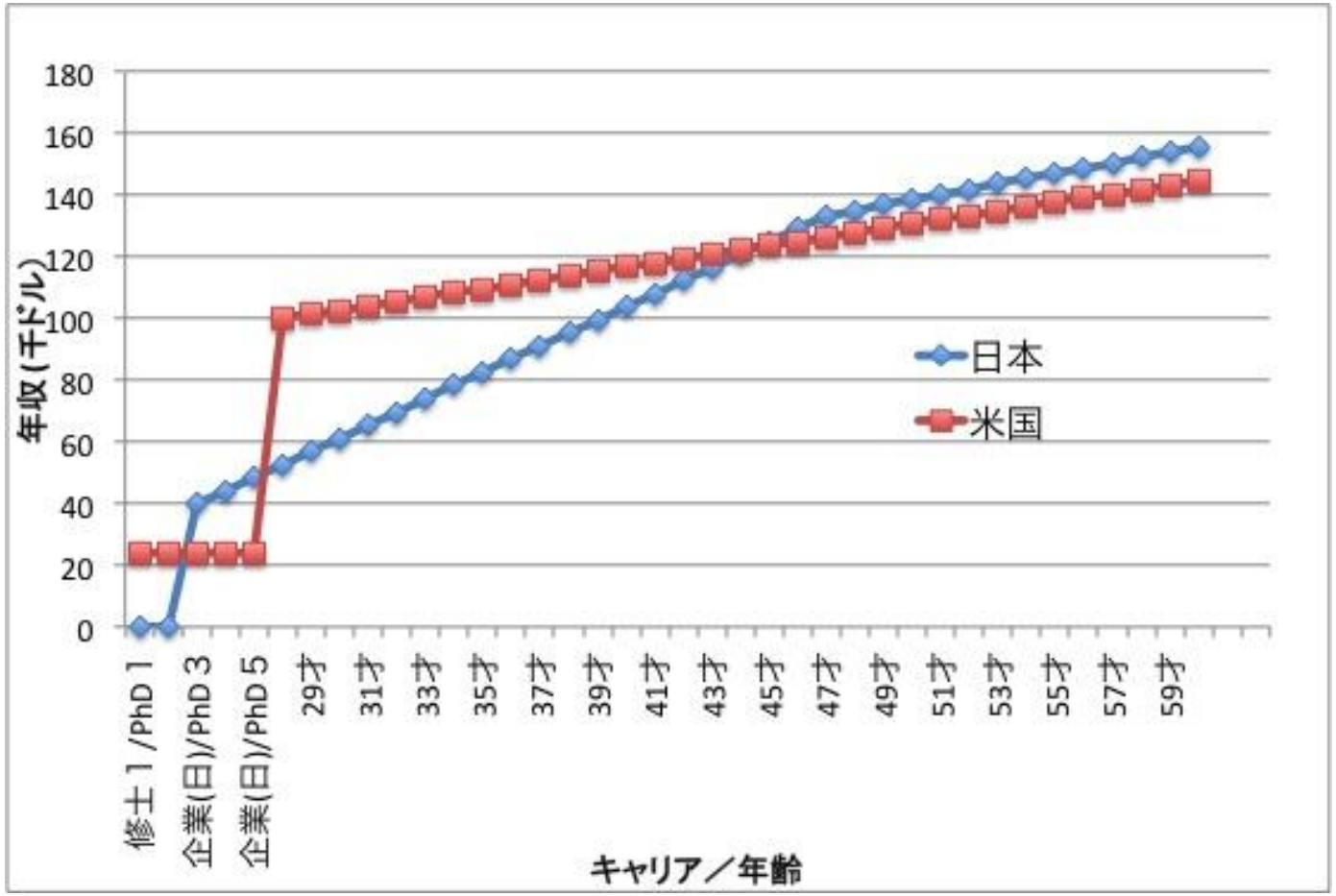
- 日本企業と米国企業の“ひとつ”の違い
  - 入社初日の会話にみるロールベース
    - 「高橋さん、この件決めてください」
    - 「え！、今日来たばかりでよくわからないんだけど、私が決めるの？」
    - 「マネージャーが決めないで、誰が決めるんですか？？？？」

- 計画に基づいて事前に手を打つ責任と権限
  - 業務を適切に処理するための体制を構築するのだが、すぐに上手く機能しなくなる。
  - 人員や業務の計画に合わせて、体制も変えていく必要がある。

日本企業と米国企業の“ひとつ”の違い

出典：Wikipedia
マンモス：http://ja.wikipedia.org/wiki/%E3%83%9E%E3%83%B3%E3%83%A2%E3%82%B9
稲作　　：http://ja.wikipedia.org/wiki/%E7%A8%B2%E4%BD%9C

年功序列とロールベース



出典：　統計学＋ε：米国留学・研究生活　日米の専門職のキャリアと賃金カーブの違い
http://wofwof.blog60.fc2.com/blog-entry-534.html

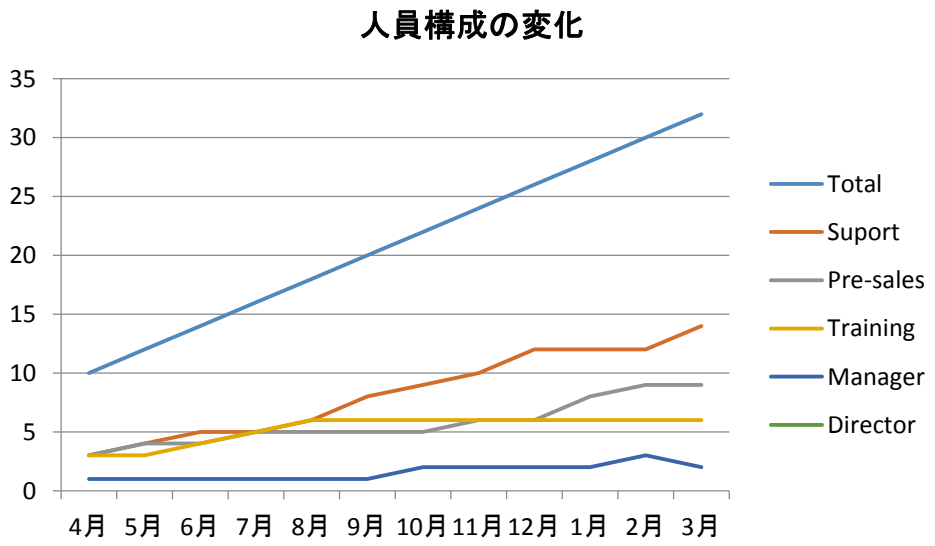
- 出典では、米国では学歴が給与を決める要因が強いと分析されている
- 私の理解では、ロール（役割・ポジション）が給与を決めており、そのロールに必要な要素のひとつが学歴
- 米国企業では「会社に人員を雇う」というよりは、「必要なポジションの要求を満たす人を雇う」ため、ポジション＝ロールによって給与が決まってくる。
- 「マネージャーの給与 < エンジニアの給与」も珍しくない

- ジョブホッパー(Job Hopper)は、転職によって給与やポジションを上げていく人たちのことだが、このグラフで分かるように単に長年勤めていても給与が上がらない。
- 別の会社により高いポジションの空きがあれば、「高いポジション＝高い給与」を得るために転職することが背景となっている

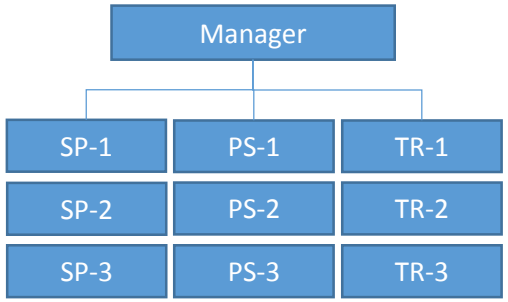
日本のセキュリティ人材育成政策は、この違いを見逃すか軽視しているように思われる

体制をマネージする

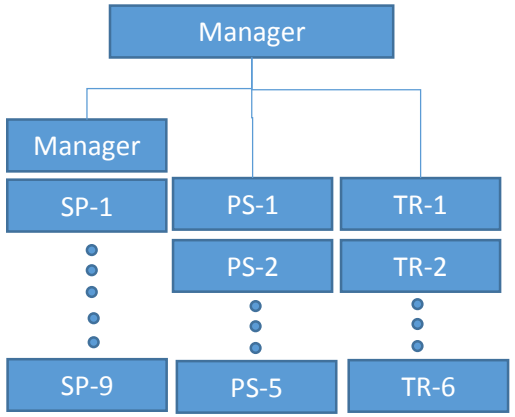
	Total	Suport	Pre-sales	Training	Manager	Director
4月	10	3	3	3	1	
5月	12	4	4	3	1	
6月	14	5	4	4	1	
7月	16	5	5	5	1	
8月	18	6	5	6	1	
9月	20	8	5	6	1	
10月	22	9	5	6	2	
11月	24	10	6	6	2	
12月	26	12	6	6	2	
1月	28	12	8	6	2	
2月	30	12	9	6	3	
3月	32	14	9	6	2	1



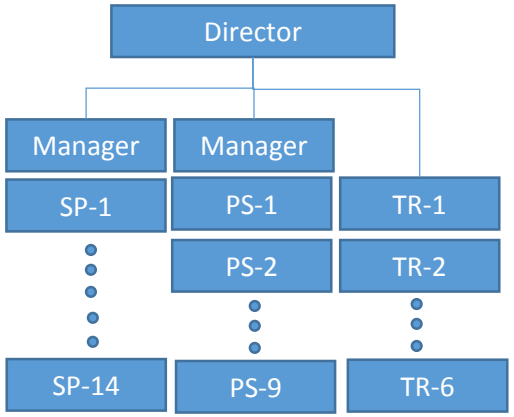
4月の体制



10月の体制



翌3月の体制



- この例では、うまく対応できていないが、一人が見れる人員は、５名までというのがコンセンサス
- 組織体制を変更する権限と責任は、Manager(Director)にあり、社長や誰かが決めるものではない。
- 計画と実績に基づいて、必要なリソースを確保することもManagerの責務

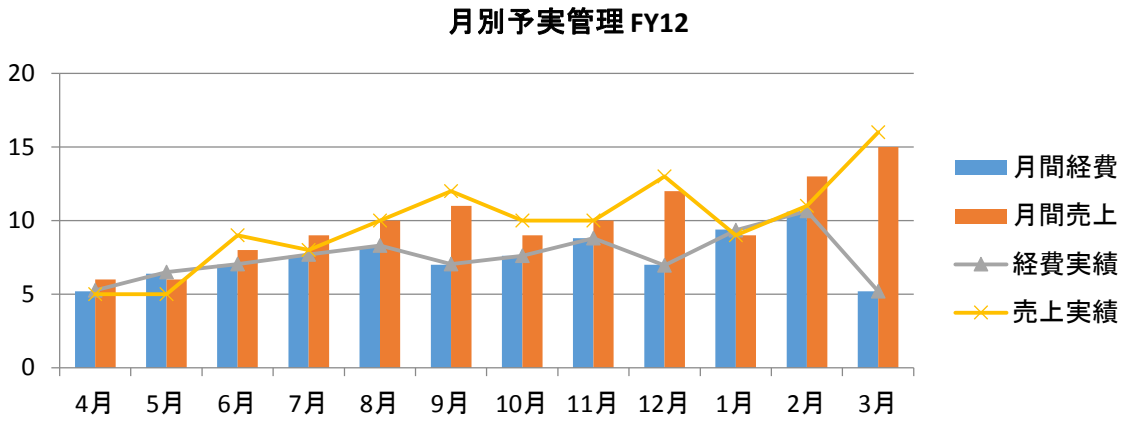
- 我慢してしのぐことは、美徳ではなくて、無能とされる可能性が高い
- 指標に基づいた計画が必要

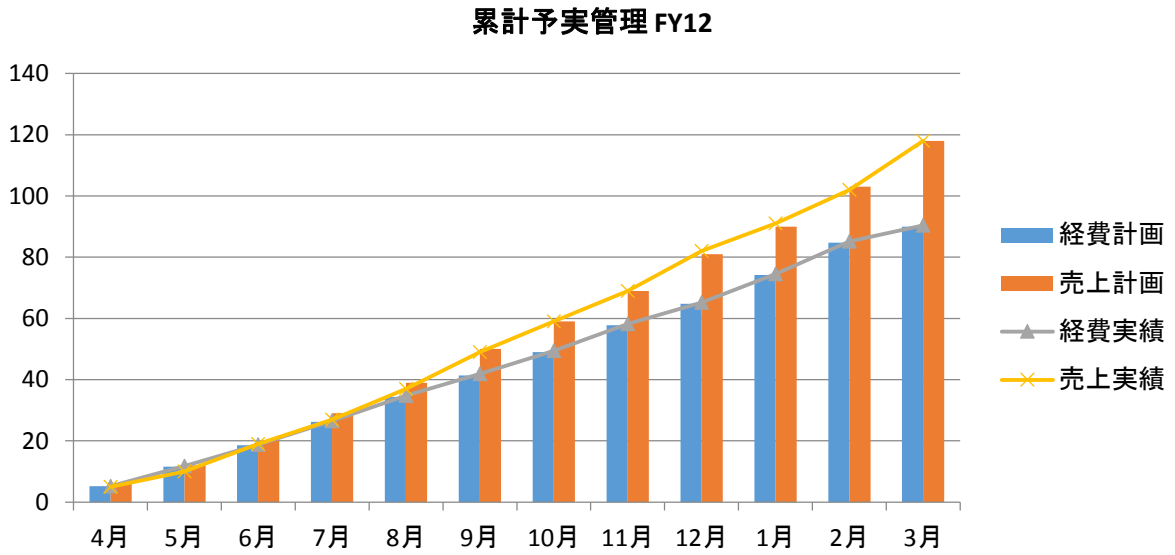
EPISODE-III: コンサルティング事業の立ち上げ

- 数字を持つということ
  - 事業責任者として数字を持つということ
  - 四半期決算と年間決算、または成果主義

- 顧客にとってのコンサルティングの価値
  - お客の言うとおりにやることが正しいのか
  - 問題を列挙することがコンサルティングなのか

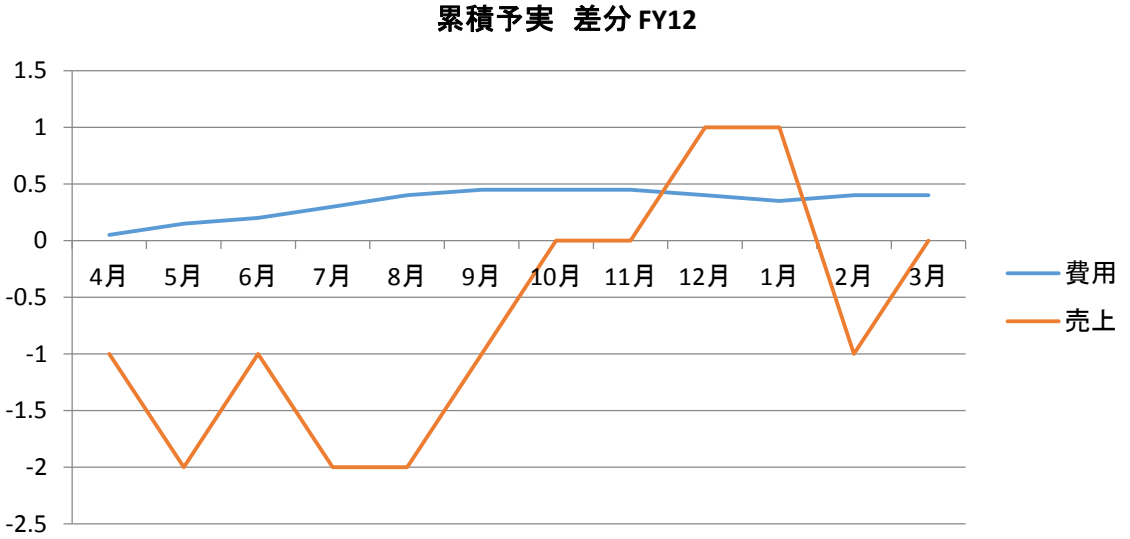
数字を持つということ





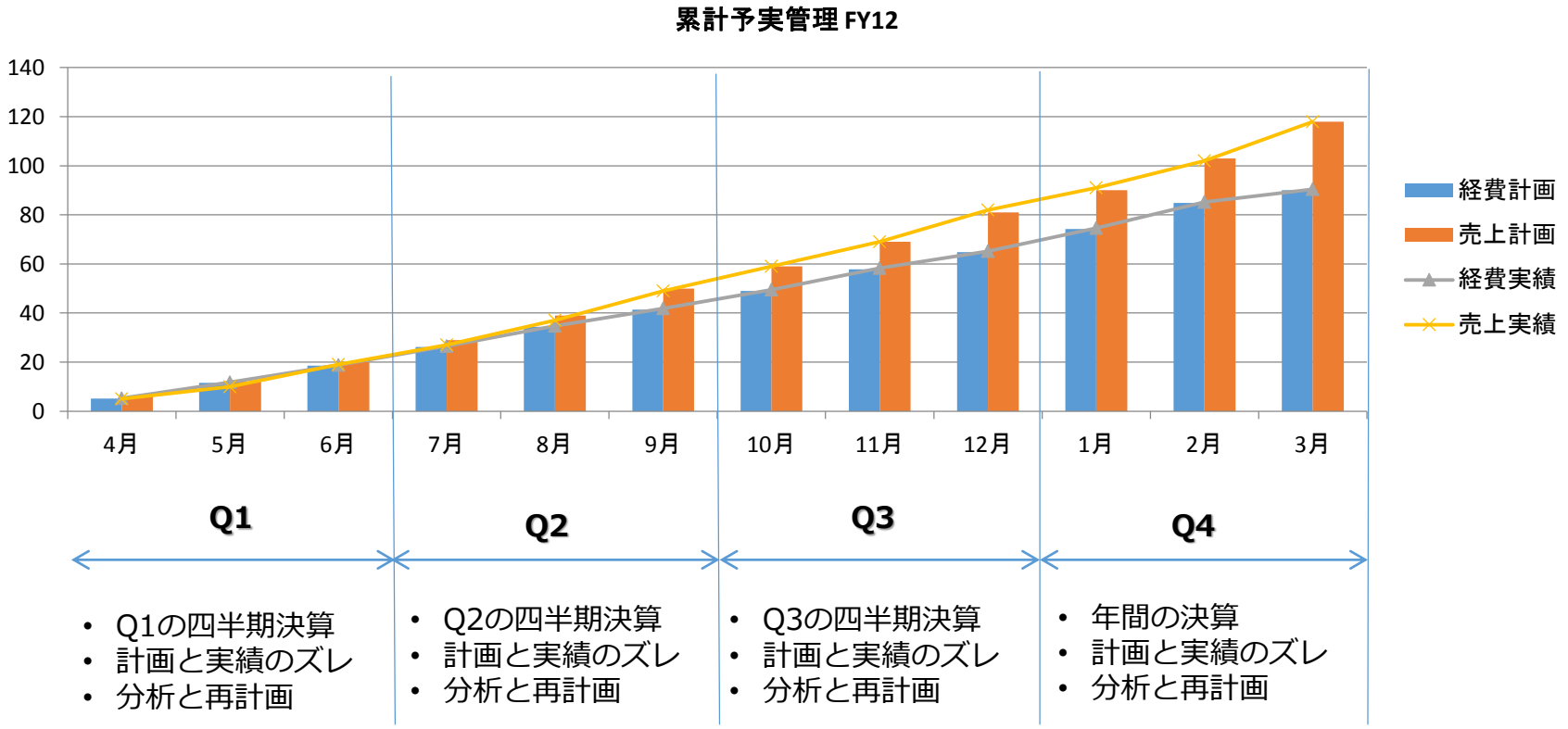
- 様々な理由で各月の売上見込みが変わるため費用と売上の管理が必要
  - 費用は、固定費と変動費に別れる
- 商品を仕入れて売上が立つまでは時間差があり、計画と実績の違いは売上の増減だけではなく、在庫過多や機会損失につながる。
- 右下図は、売上は目標を達成したが、計画とのずれにより、費用がかさみ、利益が確保できなかった例

- 売上の見込みが立たないときは、費用を削減して、利益を確保するように対処する
  - 変動費の削減 → 固定費の削減
  - この対処が下手だと、経営が出来ていないと判断される



四半期決算のオペレーション

このサイクルが PDCA



なぜ、利益を伸ばさなければいけないのか？

経営はそういうゲームだから

- 投資家の視点
  - 例えば毎年 一定の伸びなければ、投資対象とならない
  - 上場企業はもちろんだが、非上場企業においても、投資を得るために利益の伸びが必要
- 内部の視点
  - 商品の延命や、新しい商品の開発のためには投資が必要
  - ビジネスのスピード：先行優位を得るためには投資が必要
    - 待っていたのでは、後手に回ってしまう

- 各四半期ごとの決算発表が、影響を与えるもの（たぶん）
  - 株価/時価総額
  - 投資の適格性
  - 格付け
  - 金利
- 株価・時価総額が下がると、買収の対象になる可能性がある
- 資金繰りのコスト（金利）が上がると、投資ができなくなったり、コストが高くなる可能性がある
- 最悪、資金繰りの悪化で、キャッシュフローがなくなり、倒産になることも考えられる

顧客にとってのコンサルティングの価値

目標としたこと

- エンジニアリングとしてのセキュリティを提供する
  - 合理的で再現性が高く、具体的な対策が提案できること
- 顧客に対して提案をする
  - SEは顧客の依頼通りの作業をすることが正しい、と考える事が多い
    - 受託開発は、顧客の言うとおりにやることが基本（リスクが低い）
    - 顧客が何をするかを決める事が基本
  - コンサルティングは顧客と一緒にゴールを探る作業
    - ゴールがわかっているのであれば、コンサルティングは必要ない
    - 専門家として、議論し、モデル化し、提案する
  - 脆弱性の報告ではなく、脆弱性対策を提案をする
    - 脆弱性の一覧表を顧客に提示しても、あまり意味がない
    - 診断結果から、システムや運用上の課題を洗い出し対策を提示する

EPISODE-IV: ＣＩＯという仕事

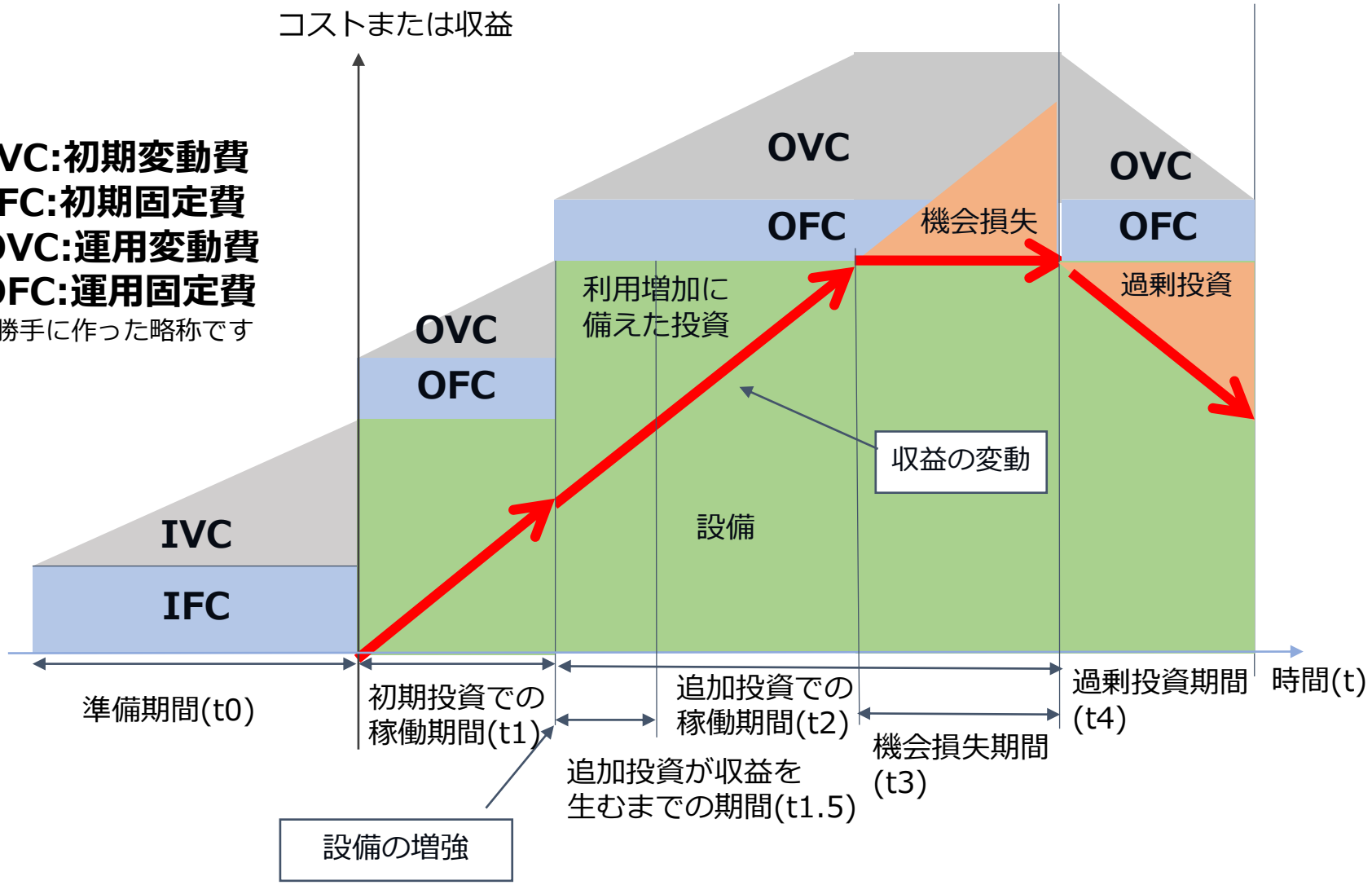
- 実際に見ることの重要性
  - ネットワークに流れているものは…
  - ITガバナンス…
- 成果を定義し計測する
  - ITの成果を定義する
  - 権限のないネットワークをマネージメントする
    - インフラは、基本的に本社が管理。日本法人ができることは限られている
- 経営陣の一員として働く（必ずしも数字に表れないが…）
  - 透明性と予測可能性の確保
  - 後手に回らない
  - 会社レベルの重要度・優先度の判断

実際に見ることの重要性

- ネットワークの状況
  - 社内ネットワーク上では色々なことが起きている
  - ヒヤリハット的なアプローチ
    - 事故にならなかった小さな問題を改善することで、大きな事故を防ぐ
      - 「大事故」を防ごうとしても難しい
      - モニターしていることを理解させ、懲罰の対象になることを肌で感じさせ、事故の火種を減らしていく
- ITガバナンスの状況（SOX対応）
  - SOXの対応を通じて、個別運用では統制が困難なことを認識
    - SOX対応が、技術的な対応であるように言われることがある（General Control)が、本来は、経営責任を明確するもので、財務的な取り組み

成果を定義する：ゲームの仕組み

IVC:初期変動費
IFC:初期固定費
OVC:運用変動費
OFC:運用固定費
*勝手に作った略称です



ゲームの仕組み
- 事業を継続する
  - 利益を上げ続ける
  - キャッシュフロー
- 利益を最大化する
  - 売上（規模）を最大化する
  - コスト（出費）を最小化する
- 計画と結果を公表する
  - 四半期ごとの中間決算
  - 年間の決算

ゲームの戦略
- 商品寿命を計画に組み込む
- 投資を迅速に回収し再投資する
- 機会損失を避ける
- 過剰投資を避ける

派生する戦術
- 固定費を抑え変動費とする
- 売上をサブスクリプション化する
- 予測可能性を高める
- オペレーションを速くする

IT部門の価値を定義する（ある程度できたこと）

- **ありがちなIT部門の主張**
  - **残業時間の長さ、昼夜をいとわぬ対応、技術的な知識**
    - **しかし、これは「ゲーム」の中では成果にはならない**

- システムの稼働率を上げて機会損失を減らす
  - 計測をして現状を把握し目標を具体化する
    - 計測がなくては、現状も目標もわからず、課題や成果を経営陣に提示できない
    - 数字を持つことで、問題が把握できるとともに、交渉がしやすくなる
  - 事業の優先度を理解する
    - 状況やタイミングによって、システム障害の影響度は異なる点を理解する

- オペレーションのスピードを上げる
  - 月次を週次に、週次を日次に
  - リモートアクセスによる移動時間の削減

- 売上に貢献する
  - ITのマネージメントに利用したツールを、ビジネスに展開することで収益に貢献

数値化しないと、他の経営陣と価値について議論し共有することが難しい

経営陣の一員として働く

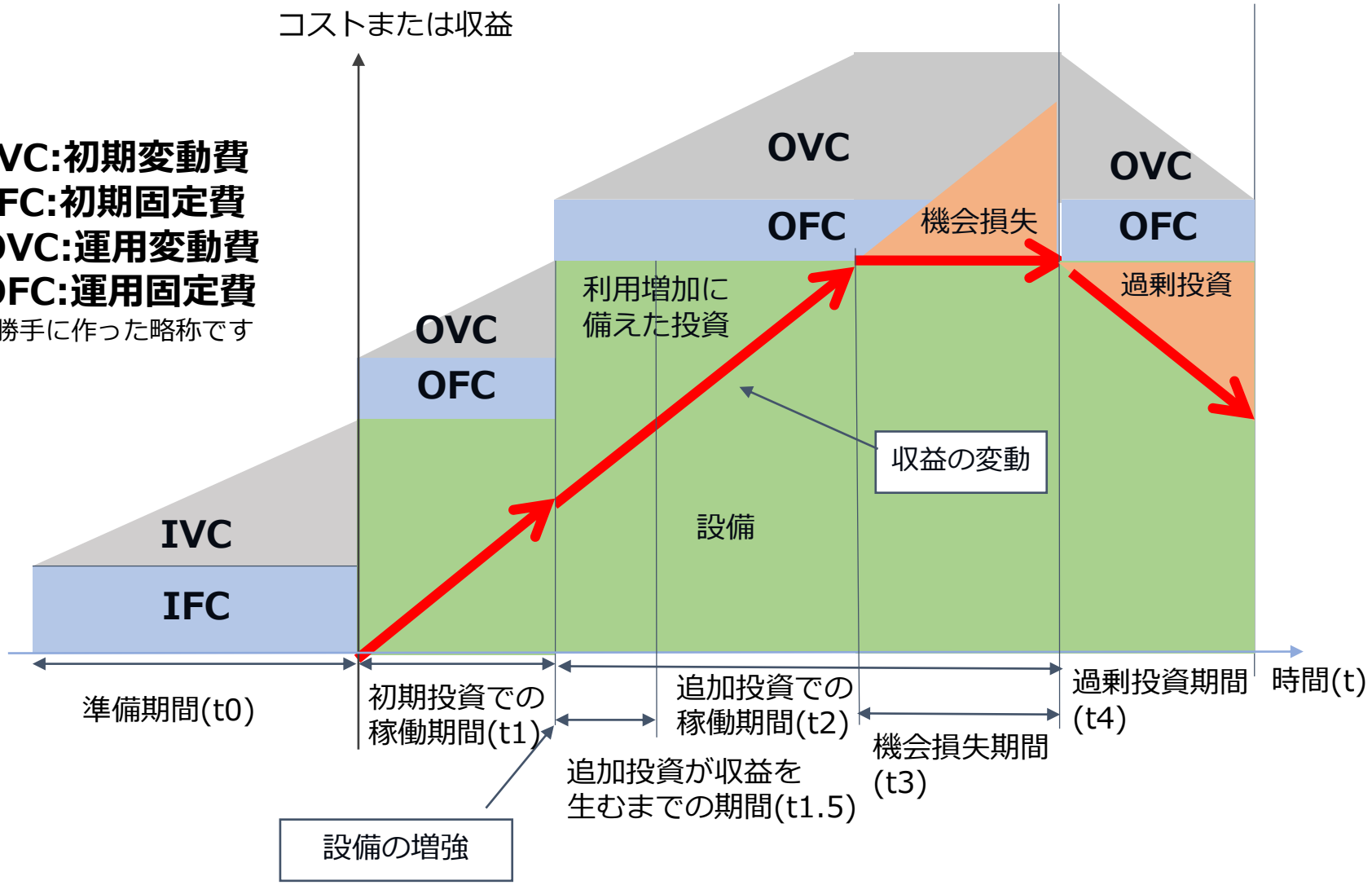
必ずしも数字に表れないが…

- 透明性・予測可能性の確保
  - トラブルが起きた場合は、そのことを周知する
    - トラブルの発生、原因、復旧の見込み、復旧
    - インフラが止まっているときは、全館を回って周知＋張り紙
- 後手に回らない
  - 計測システムを利用し、利用者がトラブルに遭遇する前に対処を始め、透明性・予測性を確保する
- 会社レベルの重要度・優先度の判断
  - あるトラブルの際の依頼：「経理から復旧してくれないか？」
    - 決算の前日であることが判明
    - 全社の復旧よりも、経理が最低限の作業ができることを優先（微妙な判断ですが）

情報セキュリティにおける成果の考察

ゲームの仕組みは同じ

IVC:初期変動費
IFC:初期固定費
OVC:運用変動費
OFC:運用固定費
*勝手に作った略称です



ゲームの仕組み

- 事業を継続する
  - 利益を上げ続ける
  - キャッシュフロー
- 利益を最大化する
  - 売上（規模）を最大化する
  - コスト（出費）を最小化する
- 計画と結果を公表する
  - 四半期ごとの中間決算
  - 年間の決算

ゲームの戦略

- 商品寿命を計画に組み込む
- 投資を迅速に回収し再投資する
- 機会損失を避ける
- 過剰投資を避ける

派生する戦術

- 固定費を抑え変動費とする
- 売上をサブスクリプション化する
- 予測可能性を高める
- オペレーションを速くする

SROI (Security Return on Investment)

- セキュリティの成果は、損害を防ぐこと
  - つまり、起きたはずのことを、防ぐことが成果
    - 上手くいくと、なにも起こらない
  - 起きなかったことを数値化する

  - SROI (Security Return on Investment)の考え方

    - 損害が発生した場合を想定し、必要な投資との効果を算出
    - SROIは、計画としてのROIで、結果としてのSROIはない。

SROIについて考える-I
予測損失額

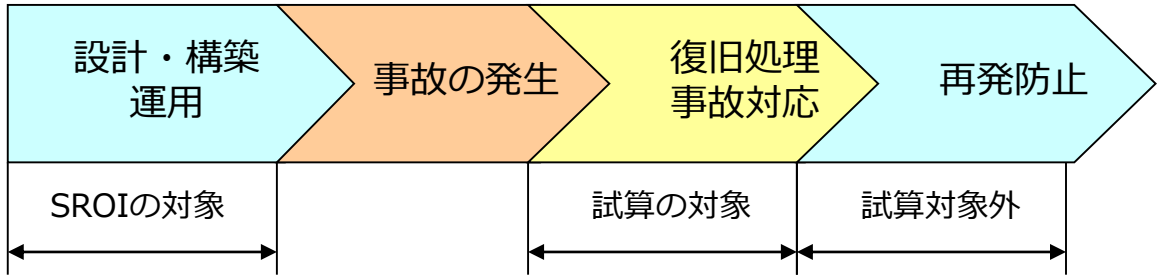
リスクと予測損失額試算のスコープ

- **リスク測度と因子**
  - **リスク = 予測損失額　×　発生確率**

- **復旧処理、事故対応フェーズだけを対象とする**
  - 事前の対策や、再発防止策は含まない
- **単純化するためECサイトをモデルとする**
  - 通常の業務活動における試算は、また別途
- **試算におけるパラメータは経営的な項目を使う**
  - 事業計画書からすぐに算出できることを目指す

予測損失額試算のパラメータ

事業規模	売上、顧客数、運用人員、単価、構築費用
個人情報漏えい	賠償費用、間接費 / 件数
機会損失	復旧時間、停止の影響、機会損失、顧客流出
システム関係	復旧工数、暫定対応費用
営業的な対応	顧客、社内、パートナ、報道、関係省庁



試算する予測損失額の項目

賠償費用 （お詫び金）	技術的な 復旧作業	営業的な 対応	機会損失 直接的・間接的

試算項目

技術的対応費用

ここでは、ざっくりと以下の2つの指標で試算（試算の結果、全体に占める割合が低いため）

運用人員の60%人日、システム構築費用の10%

営業的対応費用

顧客対応	顧客からの問い合わせ
ビジネスパートナー対応	代理店や、ECサイトにおける参加企業など
社内対応	本社対応等を含む
監督官庁・関連団体対応	業種により大きく異なるものと考えられる
報道対応	報道発表など

直接的な機会損失

直接的な機会損失　＝　システム（業務）停止時間×想定売上高×影響度

影響度 = 売上に占めるシステムの割合　×

停止中に同様のサービスを提供する競合に顧客が流れる可能性

間接的な機会損失

セキュリティ事故が発生したために失う顧客、売上など（2004年の事例から）

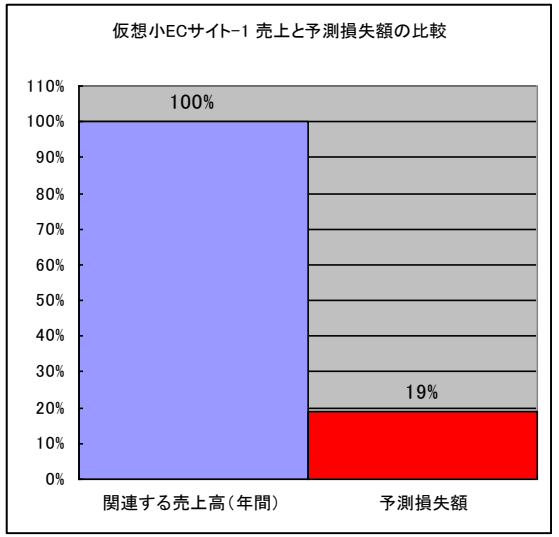
新規加入者　　44%減（公表の翌月:2004年3月）

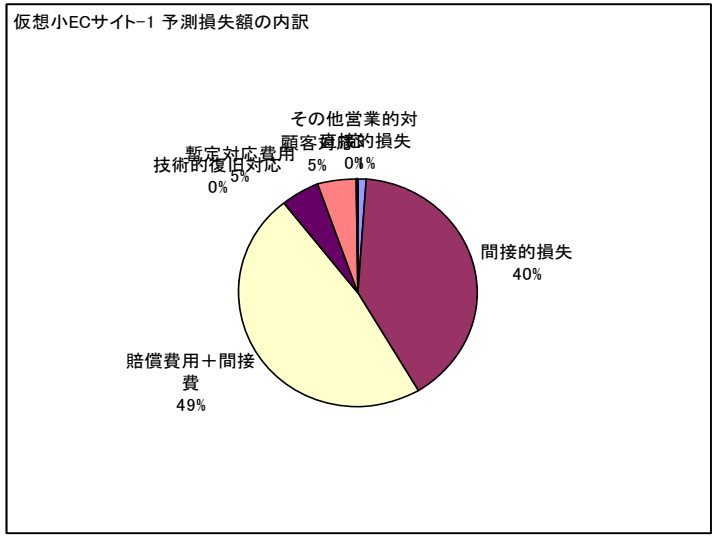
解約を考えている利用者

利用者	7.2%
無作為	28.1%

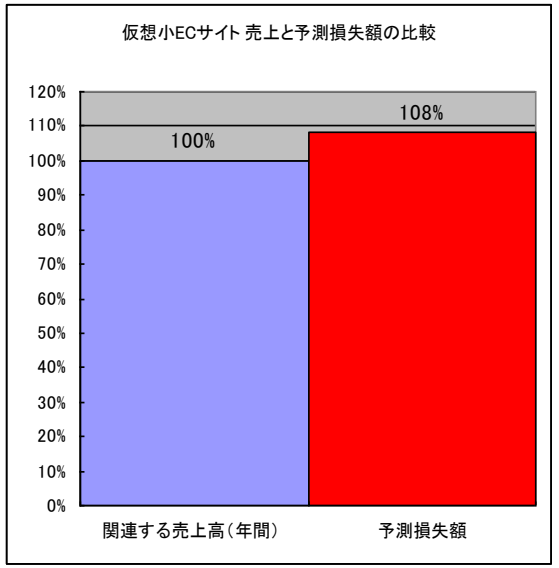
仮想ECサイトでの比較

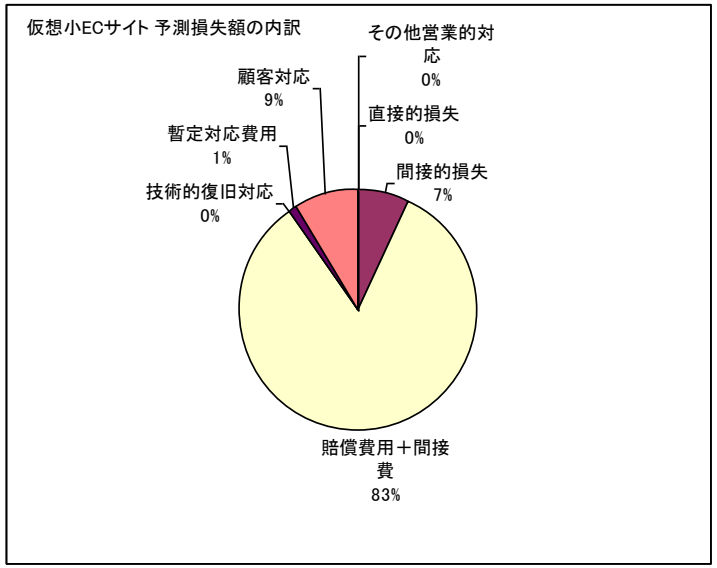
- 売上１億円、平均顧客単価　１万円
- 直接的な機会損失 0、間接的な機会損失 7.6%
- お詫び金 500円＋経費400円



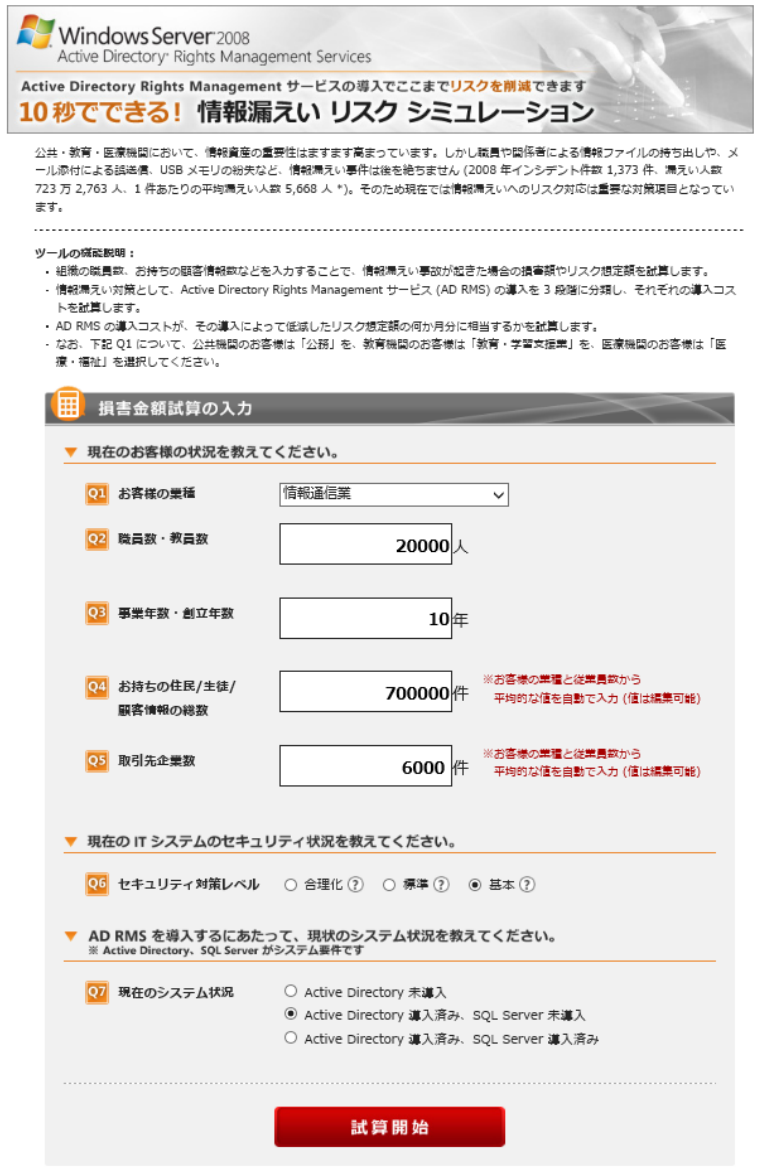


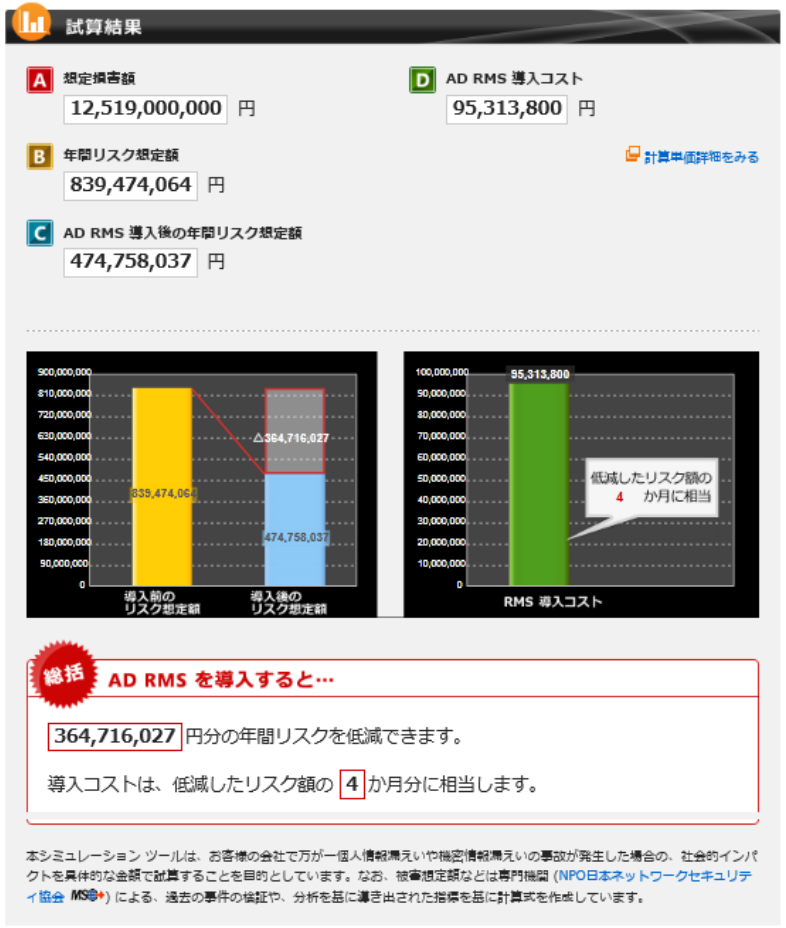
- 売上１億円、平均顧客単価　１千円
- 直接的な機会損失 0、間接的な機会損失 7.6%
- お詫び金 500円＋経費400円





情報漏えい事件のリスクを一般化する試み





JNSA（NPO日本ネットワークセキュリティ協会外部）「情報セキュリティインシデントに関する調査報告書」掲載された過去の事件の検証や、分析を基に導き出された指標に基づき、マイクロソフトが独自に算出したもの
（若干、宣伝も入っています）

10 秒でできる! 情報漏えい リスク シミュレーション
http://www.microsoft.com/ja-jp/business/industry/gov/sim-rmsdeployment.aspx

SROIについて考える-II
セキュリティの定義を考える

セキュリティの定義を再考する

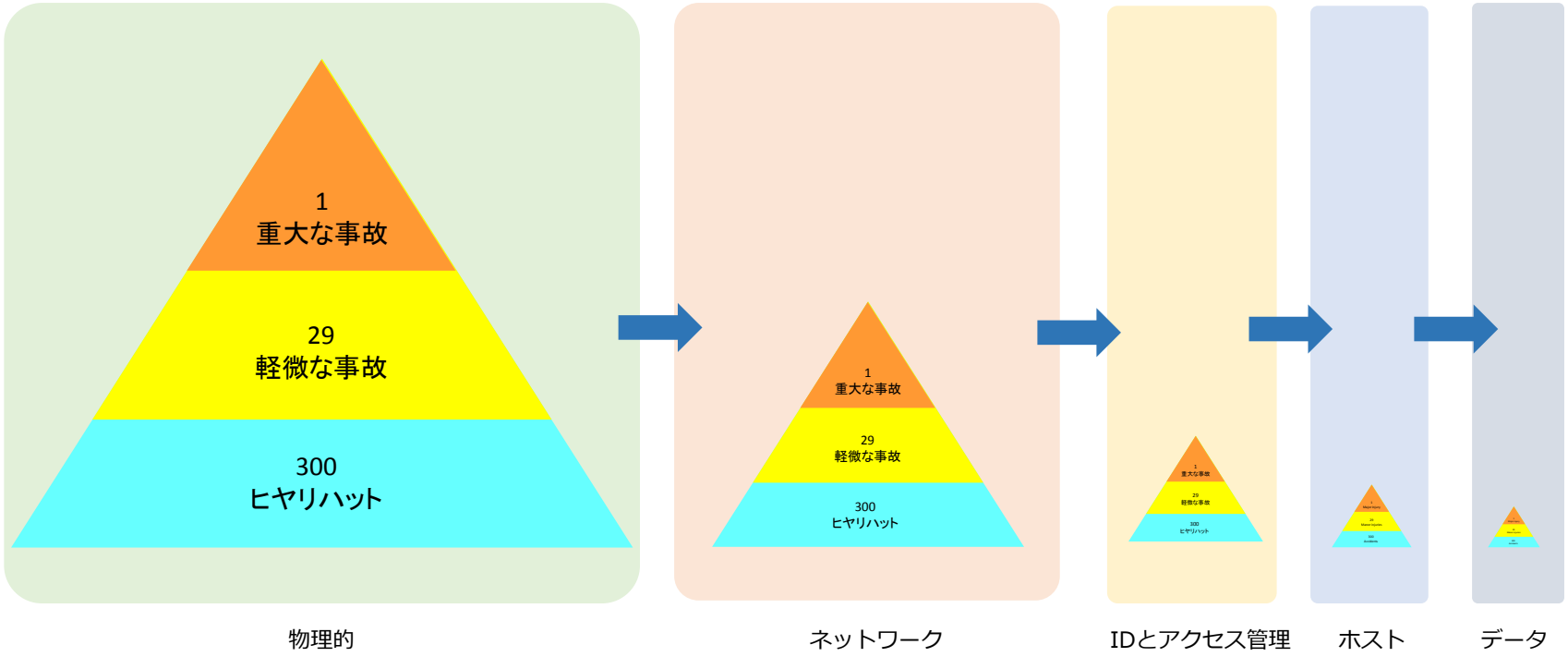
- セキュリティ ＝ CIAを守る？

  機密性：Confidentiality, 完全性：Integrity, 可用性：Availability
  - 具体的に何をするとCIAを守れるのかが定義しにくく、効果を数値化しにくい
  - 起きてしまった事故の評価には利用できる考え方だが、対策を考える上では、あまり役に立たない
- マルウエアや攻撃の検知率は？
  - 検知率は、有限のサンプルに対して実験を行った結果
  - 実環境においては、検知できないものは認知できないので、基本的に検知率を計測することはできない
  - 感染率、侵入率、被アクセス率なども同様に母数がわからない

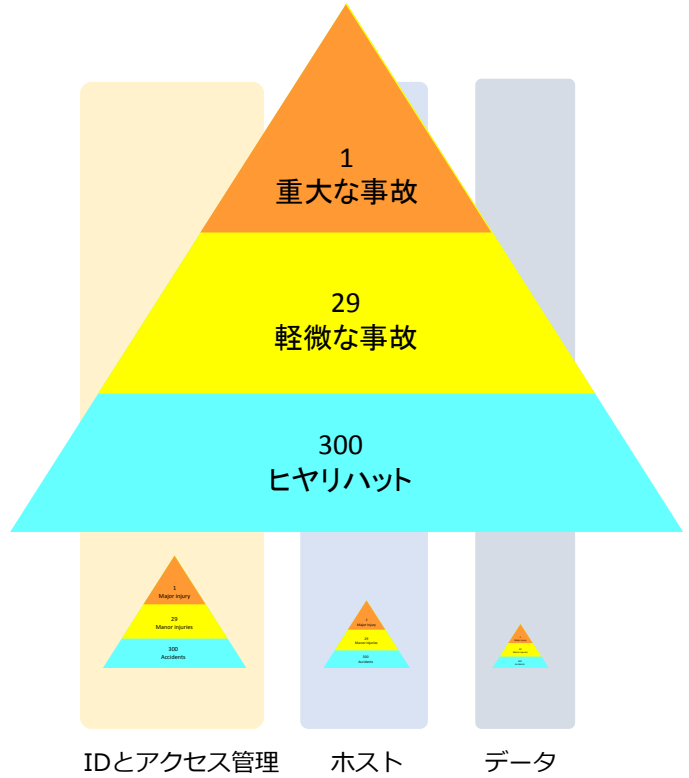
- セキュリティ＝ヒヤリハットを段階的に減少させる取り組み
  - と、ここでは考えてみる

リスク管理＝ヒヤリハット

境界領域防御におけるヒヤリハットの軽減



標的型攻撃における ヒヤリハットの軽減



SROIについて考える-III
投資対効果の算出要素

標的型攻撃を前提として

セキュリティの投資対効果を試算

投資対効果を試算するにあたっての仮定

想定損害額は1億円、セキュリティ施策をレベルで表し、
レベルが上がるごとに、リスクが 1/10になると仮定

試算結果

- Level-1の年間の標的型攻撃に対するリスク
  1000万円　　1億円 x 1/10
- Level-2の年間の標的型攻撃に対するリスク
  100万円　　1000万円 x 1/10
- Level-3の年間の標的型攻撃に対するリスク
  10万円　　100万円 x 1/10

セキュリティレベルを上げるほど、投資対効果が悪くなる。
つまり、最低限の対策だけをしていることが、もっとも投資対効果が高くなるように見受けられる。

この試算の問題点：目標レベル（成果）の定義がない

目標（成果の定義）のない投資対効果は意味がない
例えば、次のような達成目標レベルを設定し、「目標レベルを達成するための費用対効果」という視点で考え考える必要がある

- Level-1　偶発的な攻撃しか想定できない組織
- Level-2　攻撃の標的とされる可能性が無視できない組織
- Level-3　攻撃の標的となることが十分に想定される組織

セキュリティレベルの定義 (Protection)

施策強度	Level-1	既知の脆弱性・攻撃を防御できる	• セキュリティ更新（OS、アプリ、その他） • ウィルス対策ソフト • コンピューターの基本的なセキュリティ設定 （パスワード強度、ロックアウト、共有、LM Hashなど） • ブラウザなどの主要なソフトウェアのセキュリティ設定
	Level-2	未知の脆弱性・攻撃をある程度防御できる	• Level-1に加えて • セキュリティ強度の高いOSの利用 • セキュリティ強度の高いシステムの設定 （NISTの標準リストからEnterprise Clientを適用） • セキュリティ強度の高いプログラムの利用 （Office 2010, Acrobat X, etc）
	Level-3	未知の脆弱性・攻撃を相当程度に防御できる	• Level-2に加えて • よりセキュリティ強度の高いコンピューターの設定 （NISTの標準リストからSSLF*を適用） • アプリケーションのホワイトリスト化 • EMETなどによるアプリケーションの脆弱性対策
施策適用率	Level-1	• 設定などを確認する手段があり、問題のあるノードを特定できる	
	Level-2	• 策定した設定などを、各ノードに強制することができる • 条件を満たさないノードのネットワークへの接続を遮断できる	
	Level-3	• イントラネット外で利用するPC等についても設定などを強制することができる	

*SSLF: Specialized Security – Limited Functionality (SSLF)

セキュリティレベルの定義 (Isolation)

分離（Isolation）	Level-1	インターネットとの通信が一元化され、制御されている	• Outboundのアクセス制御が定義され実施されている • HTTP/HTTPSのアクセスが、PROXYを経由することが強制されている
	Level-2	イントラネット内のセグメント間の通信が制御されている	• ホスト間のロジカルセグメンテーションが行われている • 重要なサーバーに対するネットワークレベルのアクセス制御が行われている
	Level-3	管理セグメントが分離されている	• 特に、Domain ControllerやLDAPなどの重要なサーバーに対する、操作が厳密に分離されている • その他サーバーのメンテナンス用のセグメントが分離している

セキュリティレベルの定義 (Detection)

監視レベル

• 重要なサーバー（DC/LDAPなど） • 重要なネットワーク機器 • セキュリティ機器 • インターナル・ハニーポット	高	Level-1
• サーバー • ネットワーク機器	中	Level-2
• 一般のPC	低	Level-3

高	中	低
• 特権アカウント • 重要なシステムの挙動 • フェイク・アカウント • IDS/IPSのアラート • 主要なイベント • セキュリティ機器の検出数 • 重要なアクセス違反	• 一般アカウント の重要な挙動 • AppLockerのエラーログ • IDS/IPSのワーニング • Layer7 Switch等 • 軽微なアクセス違反 • アノマリー検出	• 一般アカウントの挙動 • アプリケーションエラー • IDS/IPSのインフォメーション • アノマリー分析

もう一度
情報セキュリティの成果を
考察する

Security as a business enabler

ISMSは、なぜ普及したか？

- ISMSの理念
  - 組織のセキュリティマネジメントを確立する
    - SROI的な、損害を防ぐという方向性
- 実際の理由
  - 取引で必要とされるから取得する
    - 収益を向上、維持するための方向性

- つまり、ISMSがBusiness Enablerとして働いた
  - たぶん、損害を防ぐために働いている可能性は低い

Business Enablerとしての可能性

- まず、ITが経営に貢献することを考える必要がある
  - その計画を実現するためにセキュリティを確保する
- 自分でやらないことも選択肢
  - 例えばCloud, SaaSの利用することで、財務的・経営的な数字にインパクトを与えることができる
    - 投資の回転率が上がる可能性がある
    - 費用化により、新規事業のワーストケースのコントロールと、ベストケースの対応が容易になる可能性がある
      - 大企業の社内ベンチャーが活性化するのでは？
    - 属人性の減少による人材流動性の確保
- 業務形態・雇用形態を変える可能性
  - 在宅勤務などの柔軟な就業形態
    - スキルのある従業員の継続的な雇用
    - 他社との差別化による人材確保

おわりに

今、なぜ技術者に経営の知識が必要か？

- なぜ必要なかったのだろう？
  - 右肩上がりの経済
  - モデル・目標の存在
- なにが変わったのだろう？
  - 最も安定していると考えられていた企業の倒産や大幅な減益
  - 目標となるモデルの喪失
  - 右肩下がりの国内経済（逆ピラミッドの人口構造）

- マネージメントの二つの意味
  - 管理と経営
  - より経営としてのマネージメントが求められている

管理から経営へ

- 私の経験した日本企業の管理職研修は庶務管理研修
  - 人事関係、能力開発、庶務手続がほとんど？
  - マネージメントの入門書の多くも似たような感じ
    - マネージメント≒「上手に部下を管理する」こと
- 考えてみると、技術者が経営に関する教育を受ける機会がない
  - 学校教育でも、技術者を目指す者が経営を学ぶチャンスはないように思う
- 苦しみながら学んでいるのが現状では？
  - 「本質＝ゲームの仕組み」がわからないので、枝葉で対応しようとしてしまう
    - 「言われたとおりにやったのに」は、まったく無意味
    - 言われ通りにやる人を雇うのなら、マネージャーではなくて、秘書を雇います！

成果主義についての再考

- そもそも、成果主義以外の評価方法はあるのか？
  - 年功序列主義も、永年勤続が成果の基準であるだけでは？
  - 成果を評価しないで経営ができるのだろうか？
- いわゆる、「成果主義の失敗」に感じること
  - 成績至上主義と成果主義は違うのではないか？
    - 現在の四半期の成果と並行して、将来のための投資も欠かすことができない
  - 成果の定義ができないと、成果主義は機能しないのではないか？
    - どこからか借りてきたKPIではうまくいかない
  - 成果主義のゴールが間違っているのではないか？
    - 成果主義　　≠ 人員削減の道具
    - 計画の合理化 ≠ 経営責任の免除
- 指標化・スローガン化の危険性
  - EVA経営　　投資家と執行責任者は違うのでは？
  - QCとTQC　　経営の品質とはなんだろう？
  - BSC　　KPIを考察する上でのツールとしてのBalanced Score Card

良い会社、良い仕事、”正しい“こと

- 良い会社って何だろう？
  - 給与が高いこと？
  - やりがいがあること？
  - コーヒーがただで飲めること？
- 良い仕事って何だろう？
  - 残業をたくさんすること？
  - 知識レベルが高いこと？
  - 仕事ができる人・頑張っている人
- 正しいって何だろう
  - 会社が間違っている？
  - 上司が間違っている？
  - 顧客が間違っている？

参考：関連する寄稿など

- MSBC
  - ITマネージャーの道具箱
    - https://www.microsoft.com/japan/msbc/info.aspx?fname=security/managertool
    - 第1回　セキュリティとマネージメント　～投資対効果を考える～
    - 第2回　Windows 7　社内展開の勘所　～セキュリティの視点から～
    - 第3回　DirectAccessが提案するネットワークの形態　～End to End Trustの構築を目指して～
    - 第4回　PDCAでよいのか？　～アセスメントとマネージメントサイクル～
  - ITマネージャーの道具箱 「2011年日米情報セキュリティ事故から学ぶ、標的型攻撃とその対策」
    - 第1回　データで探るサイバー攻撃の実態
    - 第2回　標的がこうg系が狙うITセキュリティの盲点
    - 第3回　標的型攻撃対策の方向性
    - 第4回　標的型攻撃対策の投資対効果
- Enterprise Customer Care
  - マイクロソフトが提唱する企業セキュリティ
    - http://www.microsoft.com/ja-jp/business/enterprise/ecc/article/cxo1102_security_top.aspx
    - クラウドを安心して活用するためのアプローチ
- 10秒でできる情報漏えいリスク試算
  - http://www.microsoft.com/ja-jp/business/industry/gov/sim-rmsdeployment.aspx

- 日経BP Itpro: 事件と課題から考えるWindows Vistaのセキュリティ
  - ［システム管理編］●第5回　群管理の効果を試算してみた
  - http://itpro.nikkeibp.co.jp/article/COLUMN/20090814/335511/
- 失敗事例に学ぶセキュリティ対策の投資対効果
  - 日経情報ストラテジー 2004 年 8 月号 ～ 11 月号 (日経 BP 社)