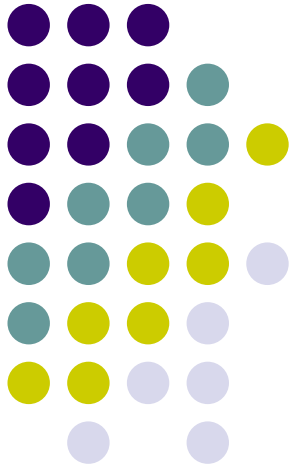
# リスク定量化BoF提唱のきっかけ

- 経済状況の悪化による影響
  - IT予算の削減：セキュリティも聖域ではなくなって・・・
  - セキュリティ予算の妥当性を説明できない・・・・
    - 結果的には経営判断だが、はたして経営に適切な判断材料を提供できているのだろうか
  - 積み上げ（ボトムアップ）では、評価誤差が累積して大きくなりすぎる。また説明が枝葉に陥りやすく経営層に届きにくい
  - 経営トップにもっともわかりやすい説明方法はないか
- ISマネジメント部門の立場から
  - 少ない予算をどこに使うか・・・。より精密なリスク分析が必要になる。
  - 手薄になったところでインシデントが発生する可能性はゼロではないが、そこを手薄にした理由に関する説明責任をはたす必要がある。
  - 漠然とした不安感から過剰な対策に陥る、もしくはリスクを軽視して対策がおろそかになるというようなことはない！！、といい切れない辛さ。
  - でも、まずは総枠で予算を確保できないと・・・・
- リスクは企業として全体で考えるべき（ERM)
  - 他のオペレーショナルリスク管理との統合も考えなくては・・・・

# オペレーショナルリスク としての セキュリティリスク定量化

2009年12月実施
リスク定量化BoF資料

（参考資料として）



By　二木真明（住商情報システム㈱）

# 企業としてみたリスクの分類

- 市場リスク
  - 株式、金利、為替、商品など流動性と市場があって、その市場価格の変動によって生じるリスク
- 信用リスク
  - 取引先の信用状態によって貸出金、債権などに生じるリスク
- カントリーリスク
  - 国、地域に依存するビジネスについて、その国の信用状態、治安状態、紛争などによって生じるリスク（国レベルの信用リスク）
- オペレーショナルリスク
  - 狭義には「事務リスク」「システムリスク」「法務リスク」の限定されるが、「戦略リスク」「風評リスク」などその他のリスクも含めた、「市場・信用リスク以外のすべて」とする広義の定義もある。セキュリティリスクや内部統制に関するリスクなども、これに含まれると考えるべき

# リスクの特性と定量化の状況

| | リスクへの対応 | リスク計量のためのデータ量 | 計量手法 |
|---|---|---|---|
| 市場リスク | リスク･リターンの極大化 | 多い | 確立 |
| 信用リスク | リスク･リターンの極大化 | 中程度 | ほぼ確立 |
| オペレーショナルリスク | リスク削減･損失回避 | きわめて少ない | 未確立 |

･市場リスク、信用リスクについては、利益･損失の両方の可能性がある。
･オペレーショナルリスクについては、損失が生じる可能性のみ。

＊参考文献：「トータルリスクマネジメント」 ベリングポイント著

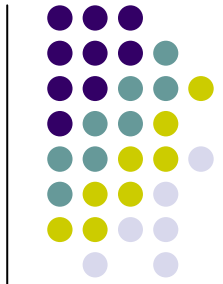
# オペレーショナルリスクの特性

- リスクを取ることで得られる「利益」がない
- 基本的にはリスクを「減らす」「回避する」ことが必要
- 管理手法
  - 基礎的手法（全社として概括的なリスク量を算出）
  - 標準的手法（業務部門ごとのリスク量を算出）
  - 先進的手法（業務部門、損失タイプごとのリスク量を算出）

# アプローチによる違い

- トップダウンアプローチ
  - 会社もしくは部門全体の粗利益などのターゲットに対して影響をあたえるリスク要因や損失事例を分析
  - 統計的手法でターゲットに対する損失のリスクを定義する
  - リスクの大きさは、ある程度わかるが対処の方法が明確にならない問題がある
  - 短時間でリスクの概観をつかむには有効
- ボトムアップアプローチ
  - 部門ごとの業務分析を通じてリスクポイントを明確にし、リスクポイントごとのリスク量をタイプごとに積み上げていく方法。
  - 手間と時間はかかるが、BPRによって、リスクを減らすことが容易。
  - JSOXで行ったアプローチ（全般統制に関する業務フローやRCMなど）を一部利用して、個々のリスクを把握する方法も可能。
  - 個々のリスク評価で統計的手法を用いるためのデータが少ないため、外部の統計データなどを使用しなければならない可能性がある

# 管理手法による違い



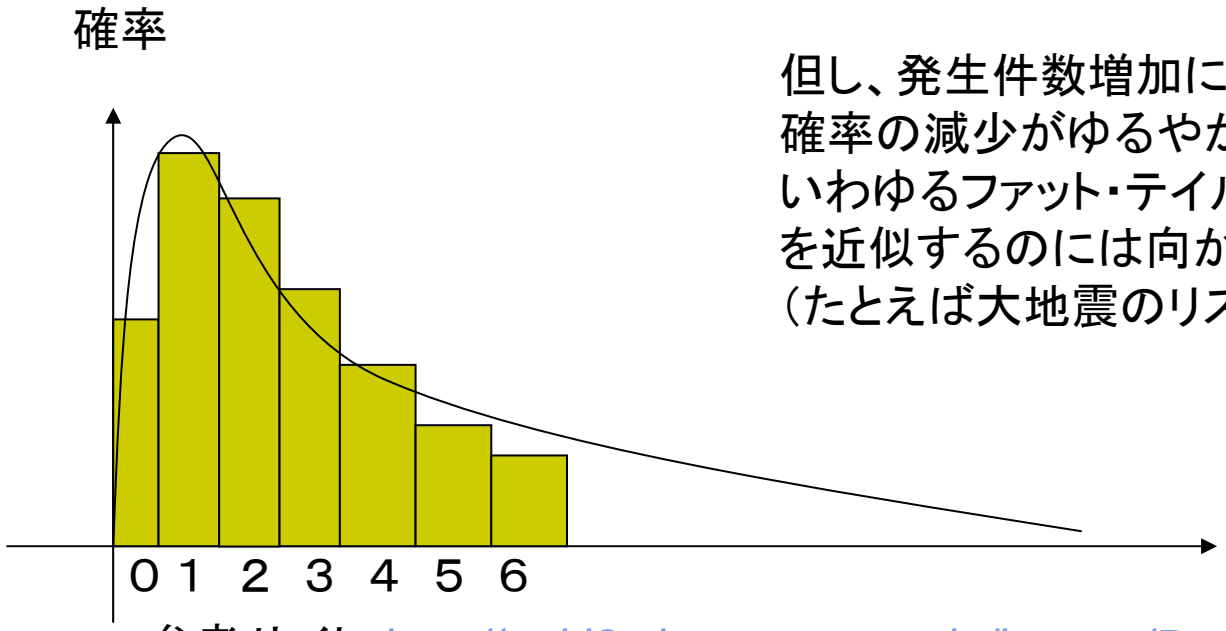
- トップダウンアプローチ（BIS規制対応などで利用）
  - 基礎的指標手法（全社で一つのリスク値を管理）
    - 会社としてのリスクの大きさはわかるが、そのリスクが会社のどこに存在するかはわからない
  - 標準的手法（ビジネスラインごとのリスク値管理）
    - ビジネスラインごとのリスク値の大きさはわかるが、その理由まではわからないので、対策には結びつかない。無理に対策しようとすれば、（売り上げ・粗利益）規模の大きなビジネスラインの縮小という本末転倒を招きかねない
- ボトムアップアプローチ
  - 先進的計測手法（ビジネスライン・業務ごとのリスク値管理）
    - 業務ごとのリスクポイントを明確にして、個々のリスク値を積み上げるため、具体的にどこにどのようなリスクが存在するかを掌握できる。
    - 作業的にはJSOX対応のリスクマネジメントと統合できる（すべき）

# 計量手法

- トップダウンアプローチの計量手法
  - 損失分布手法
    - 一定期間における既知の内部損失事例をもとに、損失規模あたりの発生件数の分布（被害額の分布）や、（リスクタイプごとの）期間あたりの発生件数の分布（発生確率分布）をとり、確率分布関数を決定する。
    - ある程度頻繁に発生する事象に対しては有効だが、災害的な被害など、頻度が極めて少ないが被害は大きいリスクについては有効でない可能性がある。
    - 分布関数が決まったら、それを使用して、シミュレーションを実施できるが、分布関数の選び方によっては誤ったモデルができる可能性があるので、各分布関数の特性を考慮して選ぶ必要がある。
      - よく使われる分布関数に、ポアソン分布、ワイブル分布などがある

# ポアソン分布

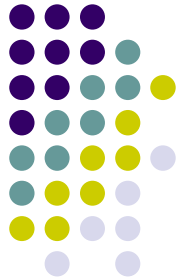
- サンプルの母数がある程度大きく、それに対して事象の発生頻度が比較的低い場合に、二項分布の近似として利用できる。




但し、発生件数増加に対して
確率の減少がゆるやかな、
いわゆるファット・テイルな分布
を近似するのには向かない。
（たとえば大地震のリスク）

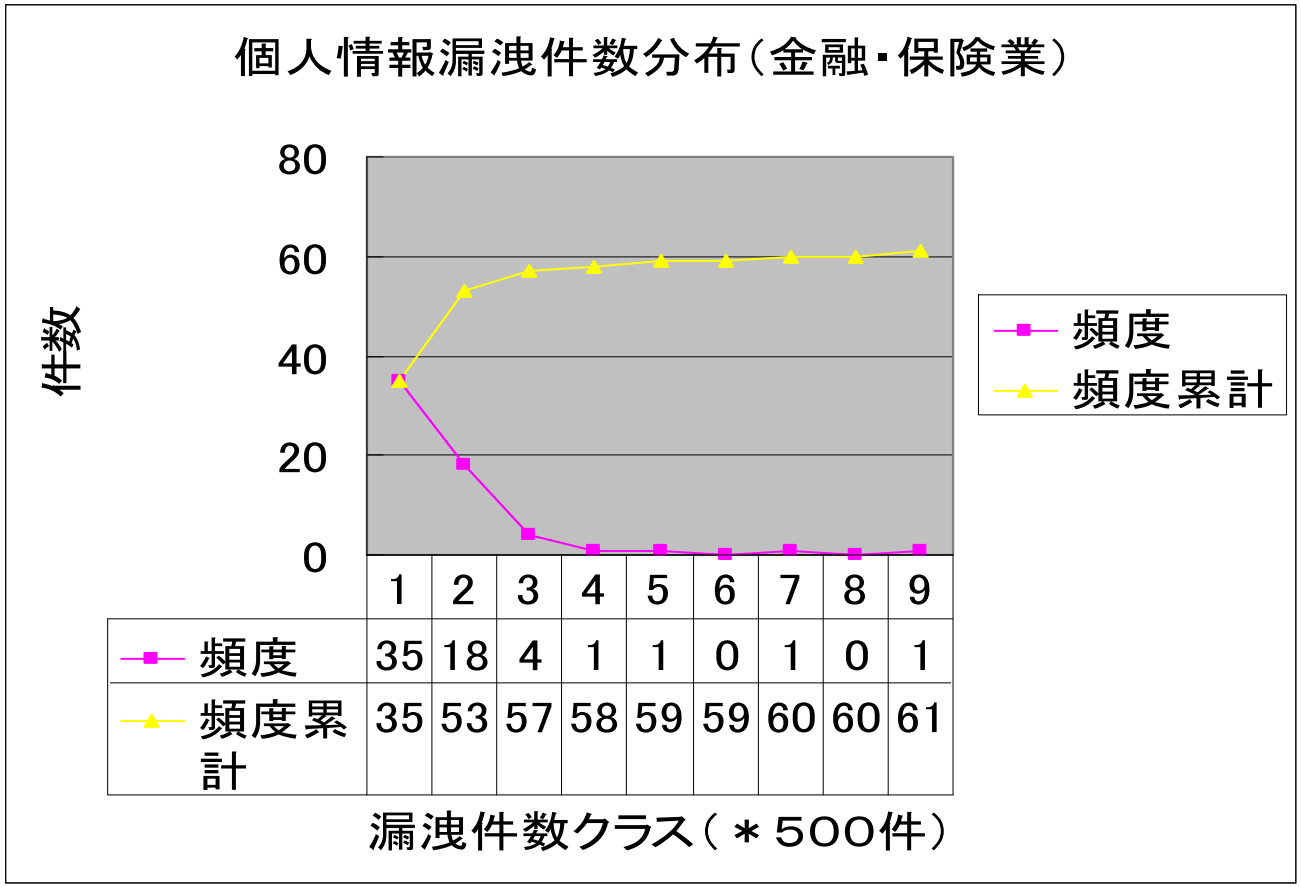
参考サイト：http://aoki2.si.gunma-u.ac.jp/lecture/Bunpu/poisson.html

# 様々な確率分布関数



- 参考サイト
  - http://www.semiconductor-sanyo.jp/reliability/main.asp?id=DM30A156&part=8
  - どの分布関数で近似するかが重要なポイント
  - 実際はかなり難しい選択になる

# 2008年JNSA調査報告データをもとにした分布グラフの1例




| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| 頻度 | 35 | 18 | 4 | 1 | 1 | 0 | 1 | 0 | 1 |
| 頻度累計 | 35 | 53 | 57 | 58 | 59 | 59 | 60 | 60 | 61 |

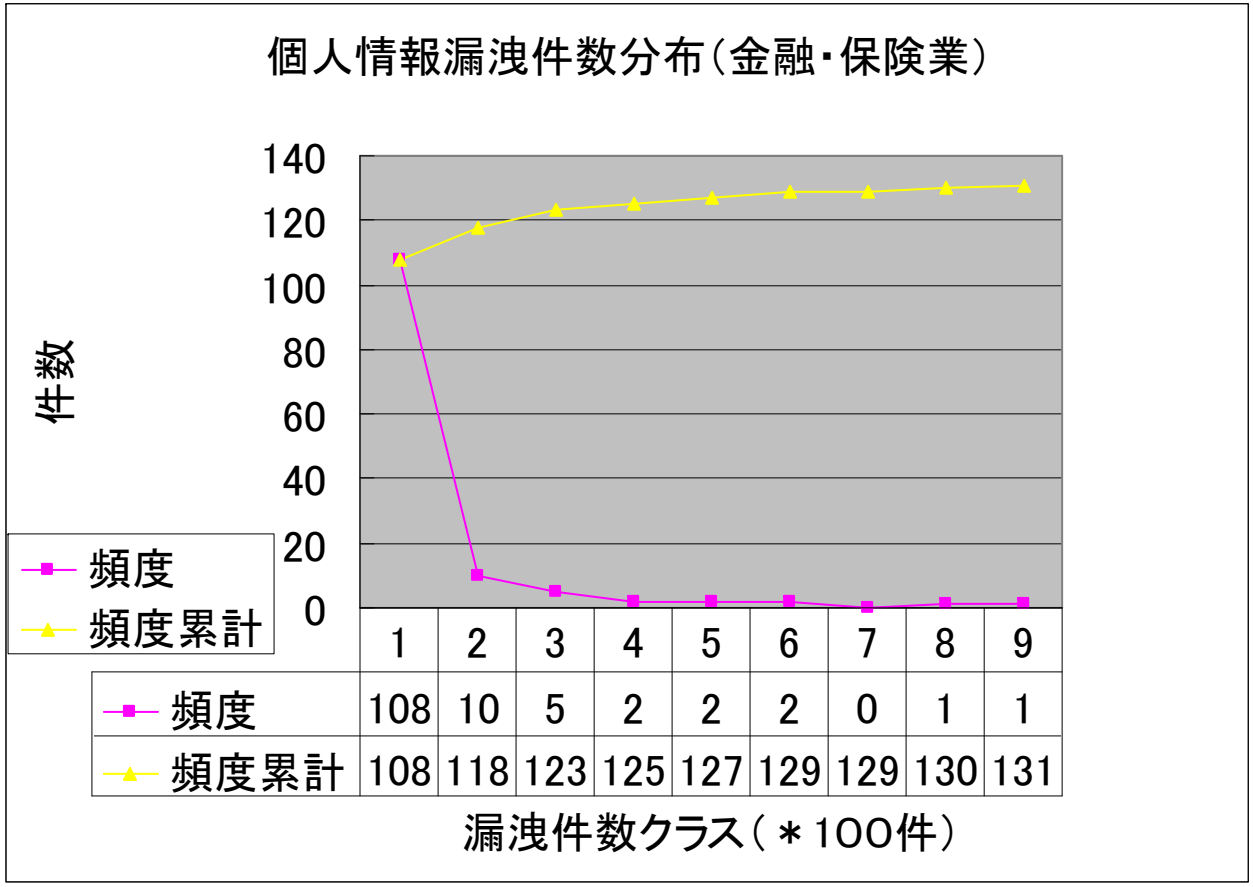
指数分布的な分布に見えるが
実は頻度1のクラスはかなり
上まで伸びている

最大値：349827
平均値：10990
標準偏差：3707

ほとんどが1500件未満の事故。
しかしこのグラフの右側にさらに
20回の事故が隠れており、この
グラフ内の事故の総漏洩件数が
51933件なのに対して、グラフ外
の事故の総件数は1563689件に
のぼる。

このような分布を表すために、
どのような分布関数を用いる
べきなのだろうか

# 漏洩件数を100件単位のクラス分けした場合



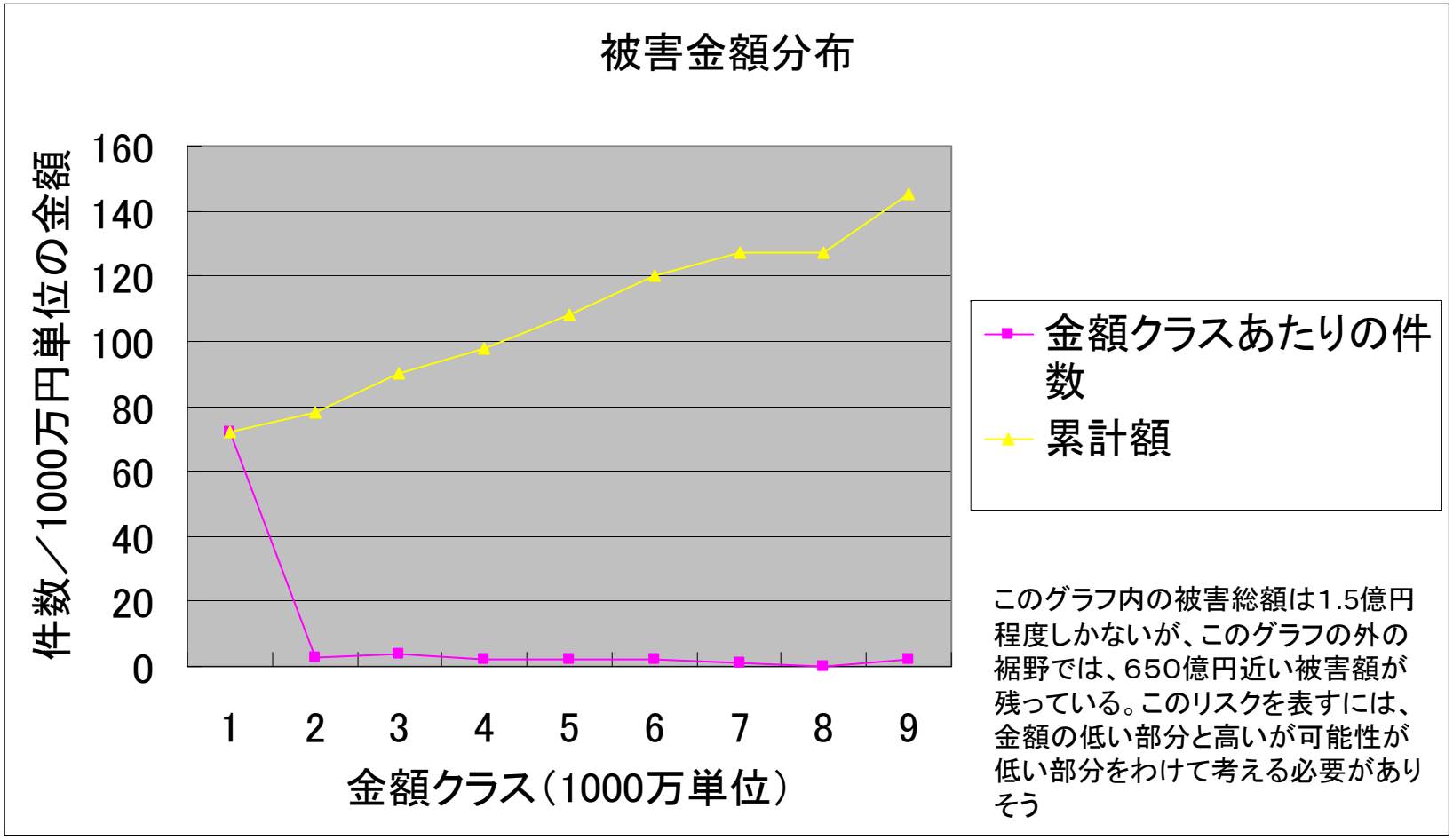

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| 頻度 | 108 | 10 | 5 | 2 | 2 | 2 | 0 | 1 | 1 |
| 頻度累計 | 108 | 118 | 123 | 125 | 127 | 129 | 129 | 130 | 131 |

100件単位のクラスで区切ってみた頻度分布グラフ

より細かくなってはいるが、これ以上細かくするとばらつきも大きくなる。

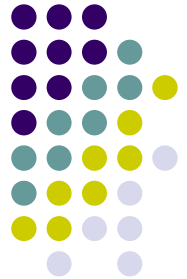
グラフ内に含まれる総件数は逆に少し増えて、9万件弱となるが、依然として150万件以上がこの外の裾野に分布している。

# 漏洩被害金額で見てみる




このグラフ内の被害総額は1.5億円程度しかないが、このグラフの外の裾野では、650億円近い被害額が残っている。このリスクを表すには、金額の低い部分と高いが可能性が低い部分をわけて考える必要がありそう

# BoFでの議論から



- 頻度分布の背景には、様々な要素があるので、単純な分布関数にはならないはず。まず、モデルをきちんと検討する必要があるのではないか。
- モデルを検討しだすときりがない。トップダウンアプローチならば、ある程度単純化したモデルでもいいのではないか
- 目的によって、トップダウン、ボトムアップそれぞれのアプローチを使い分ける必要がある
- リスクの概観をつかむためにはトップダウンは有効。たとえば、セキュリティにかける予算の総枠を考えるような場合。特に経営層やセキュリティソリューションのユーザに対する情報としては有用
- 一方、細部にわたって優先順位をつけた対策を考えるにあたっては、脅威、脆弱性、とそのターゲット、対策の緻密なマッピングを行った上でボトムアップで考える必要がありそう。