JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

2006年度 セキュリティ被害調査WG
活動報告

株式会社JMCリスクマネジメント
大溝　裕則

2007 年 6 月6日

当WGの取り組み

- 活動の目的
  - 情報セキュリティ被害の実態把握
  - リスクの定量化
  - セキュリティの費用対効果の定量化
- 調査の方法
  - 情報セキュリティ被害の実態調査
    - 企業へのアンケート
    - 企業へのヒアリング
    - 独自算定式による被害の定量化
  - 個人情報漏えいインシデントの調査
    - 公開された情報の集計

個人情報漏えいインシデントの調査

- 個人情報漏えいインシデントを集計分析
  - 2002年度より毎年実施
    - その年の1月～12月に公表されたインデントを対象
  - 報道などで公開された情報を集計
- 独自の算定式による想定損害賠償額を算出
  - 2003年に算定式を改定
  - 現在までその算定式を利用
- 株価への影響度の算定
  - 漏えいによるブランドイメージ低下の定量化のために、漏えい企業の株価の動向を分析
  - 2004年以降は未実施
    - 母数が小さく有効な結果が得にくい
    - 他の団体でも同様のアプローチを始めたため、JNSAとしての役割は終えたと判断

2006年 集計結果①

JNSA

個人情報漏えいインシデント数

2002年	2003年	2004年	2005年	2006年
62件	57件	366件	1,032件	993件

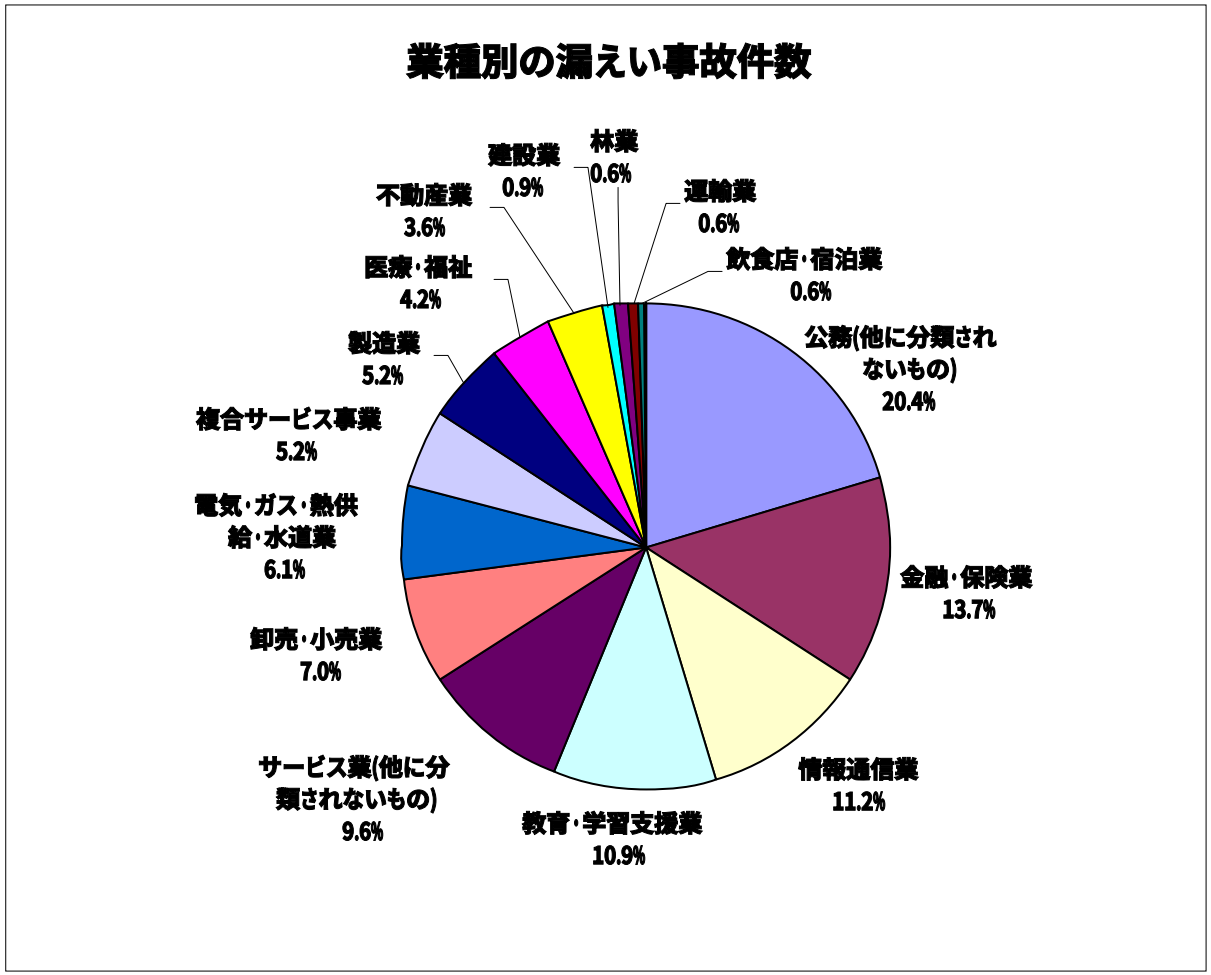
合計漏えい人数

2002年	2003年	2004年	2005年	2006年
418,716人	1,554,592人	10,435,061人	8,814,735人	22,236,576人

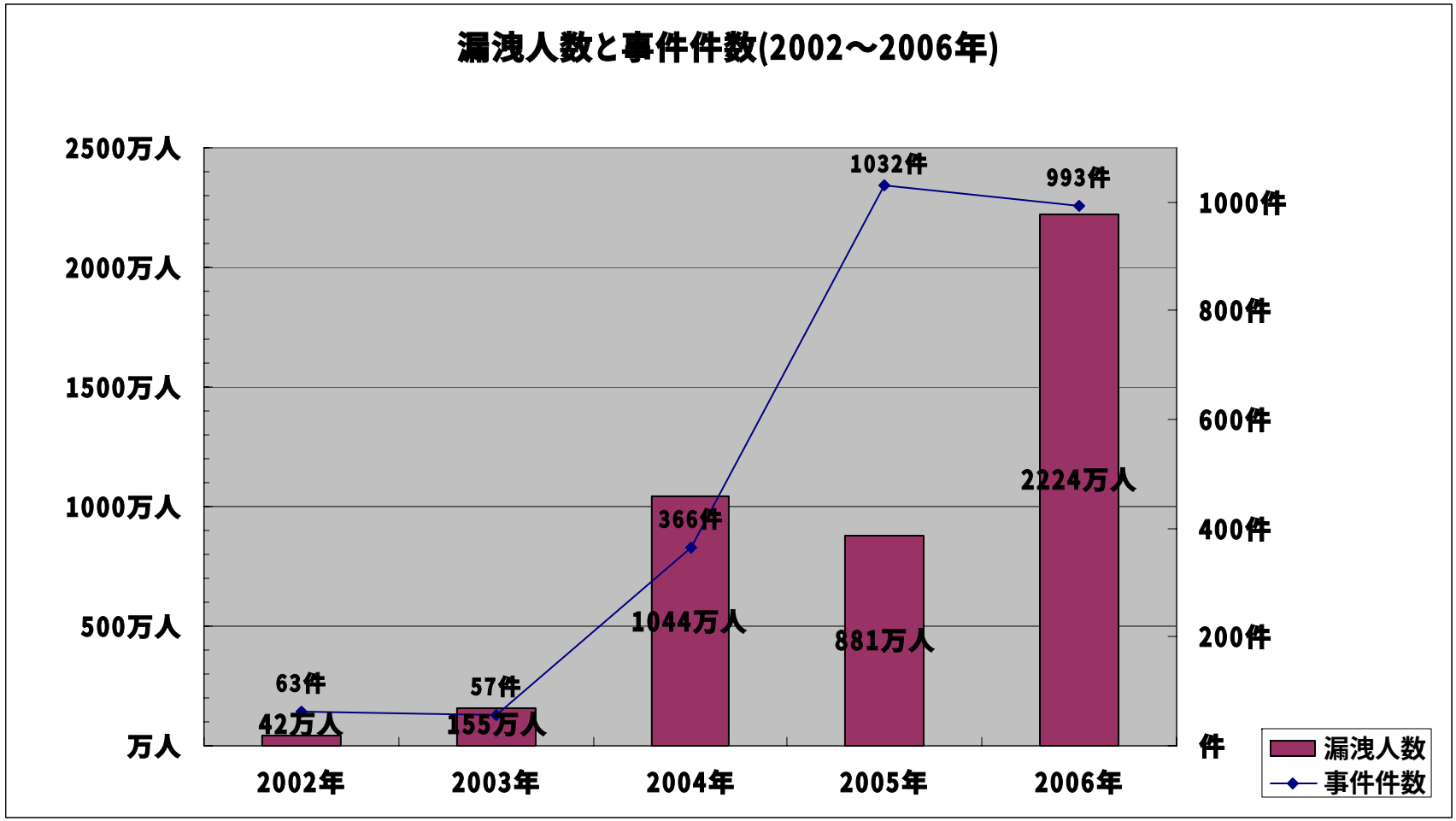
1件当たりの平均漏えい人数

2002年	2003年	2004年	2005年	2006年
7,613人	30,482人	31,057人	8,922人	23,432人

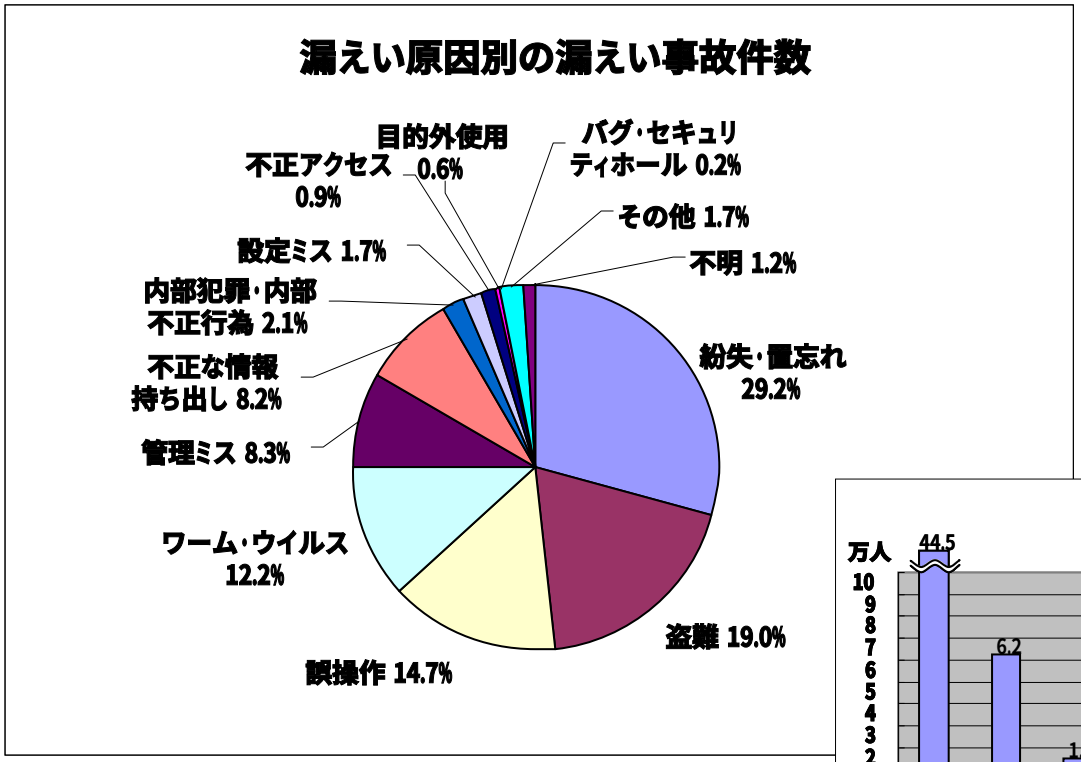
2006年 集計結果②

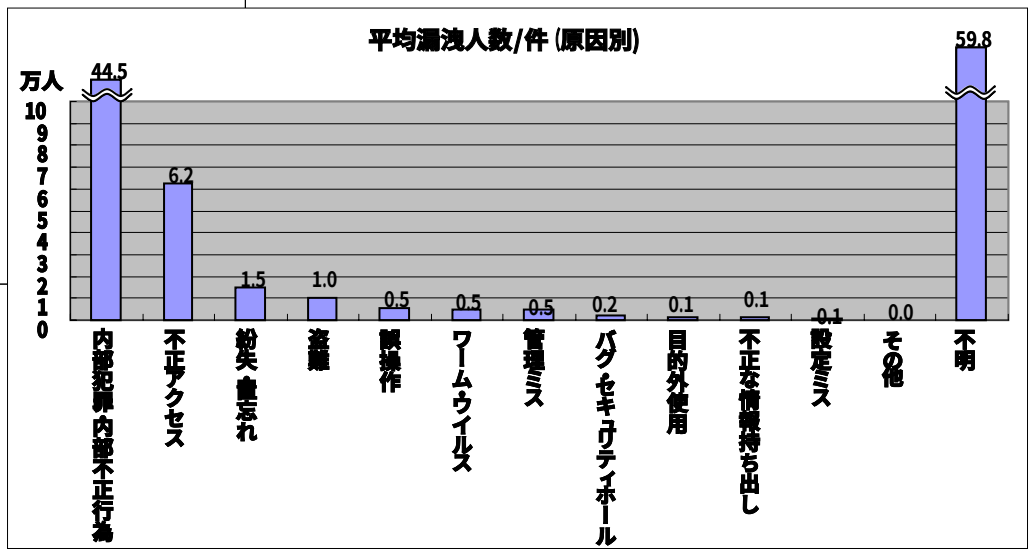


2006年 集計結果③

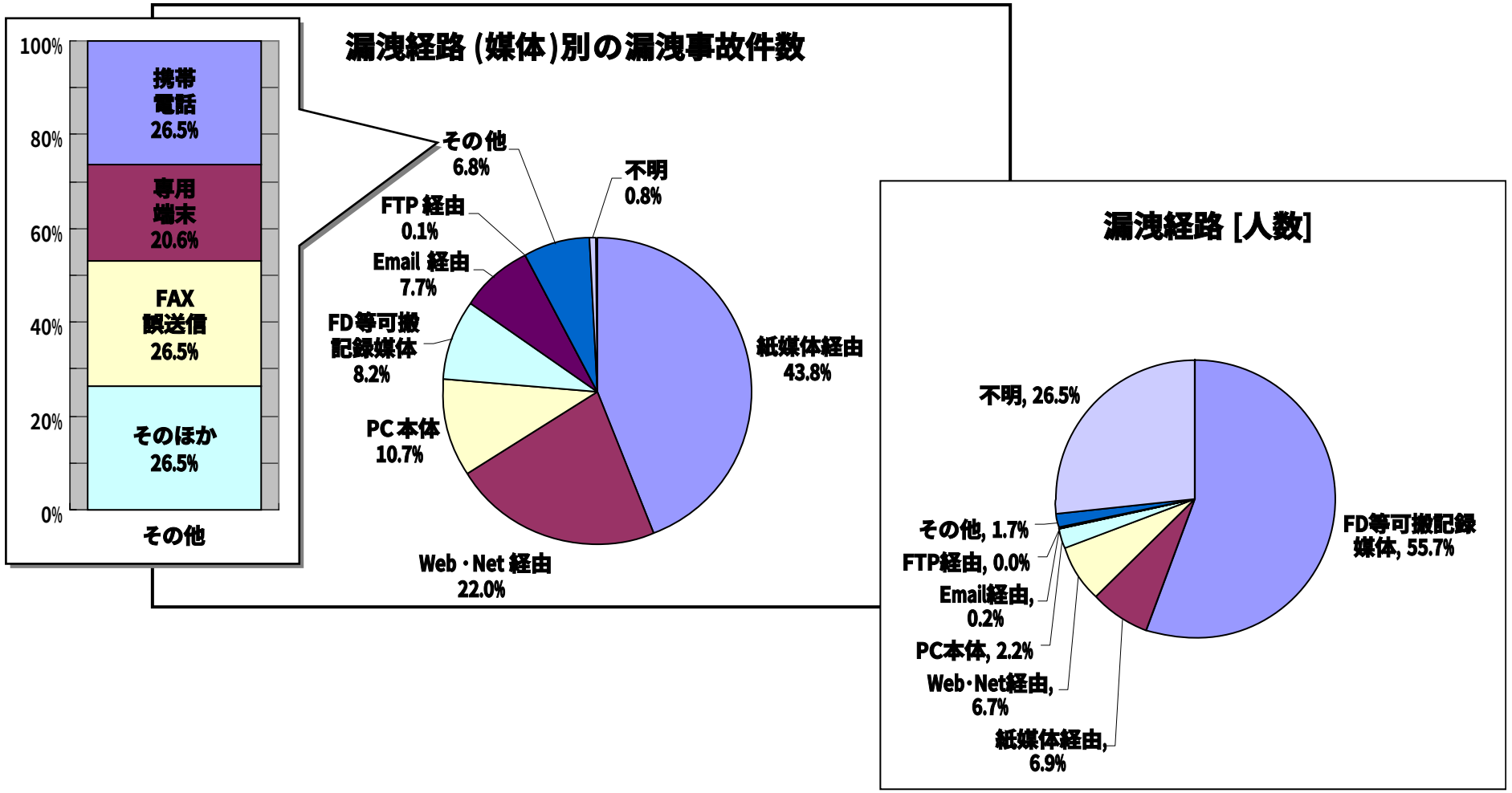


2006年 集計結果④

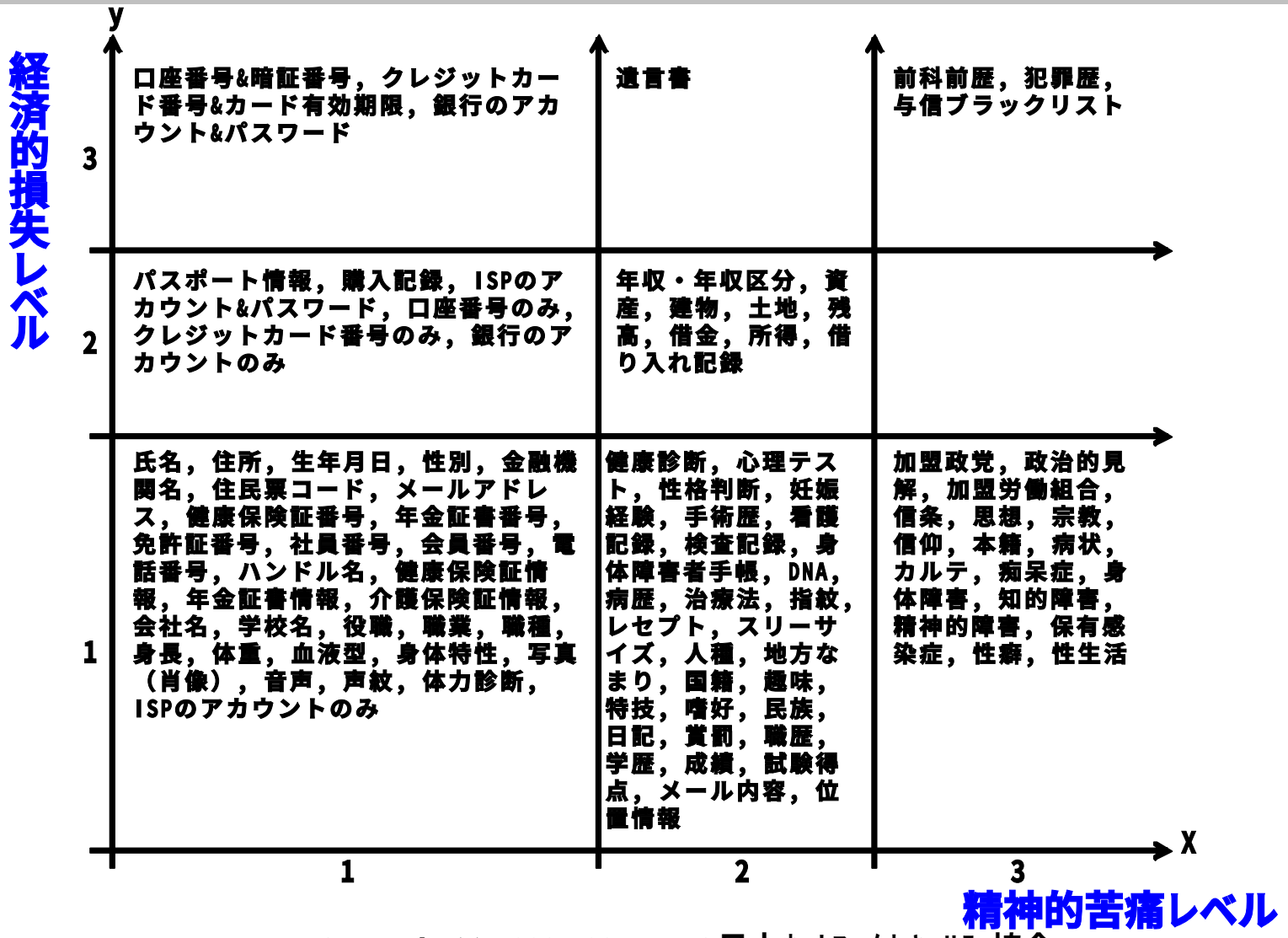




2006年 集計結果⑤



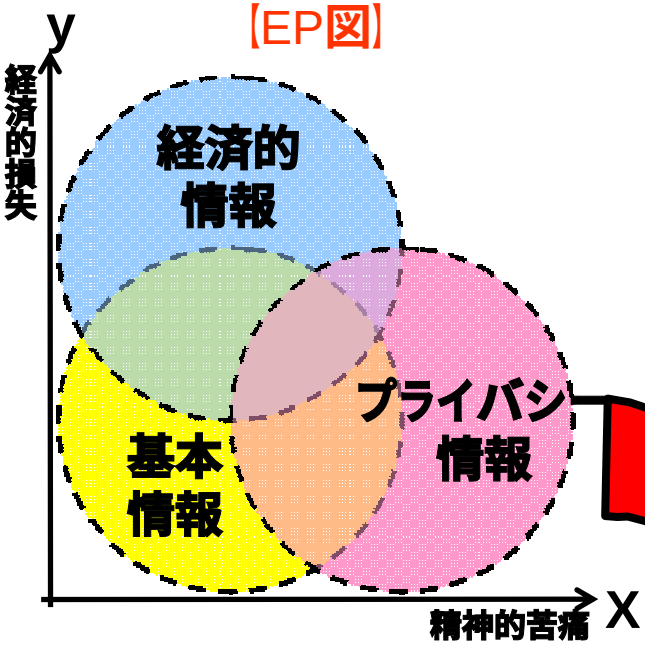
2006年 想定損害賠償算定①



2006年 想定損害賠償算定②

- **想定損害賠償額算定式**

【EP図】



【判定基準表】

判定基準		社会的責任度
一般より高い	適正な取扱いを確保すべき個別分野の業種（医療、金融･信用、情報通信等）および、知名度の高い大企業、公的機関。	2
	および団体、組織。	1

判定基準	事後対応評価
適切な対応	1
不適切な対応	2
不明、その他	1

判定基準	本人特定容易度
単に特定可能。「氏名」「住所」が含まれること。	6
コストを掛ければ個人が特定できる。「氏名」または「住所+電話番号」が含まれること。	3
特定困難。上記以外。	1

損害賠償額＝（基礎情報価値 × 機微情報度 × 本人特定容易度）
×情報漏えい元組織の社会的責任度
×事後対応評価

2006年 想定損害賠償算定③

JNSA

想定損害賠償額総計

2002年	2003年	2004年	2005年	2006年
189億2201万円	280億6936万円	4666億9250万円	7001億7879万円	4565億8403万円

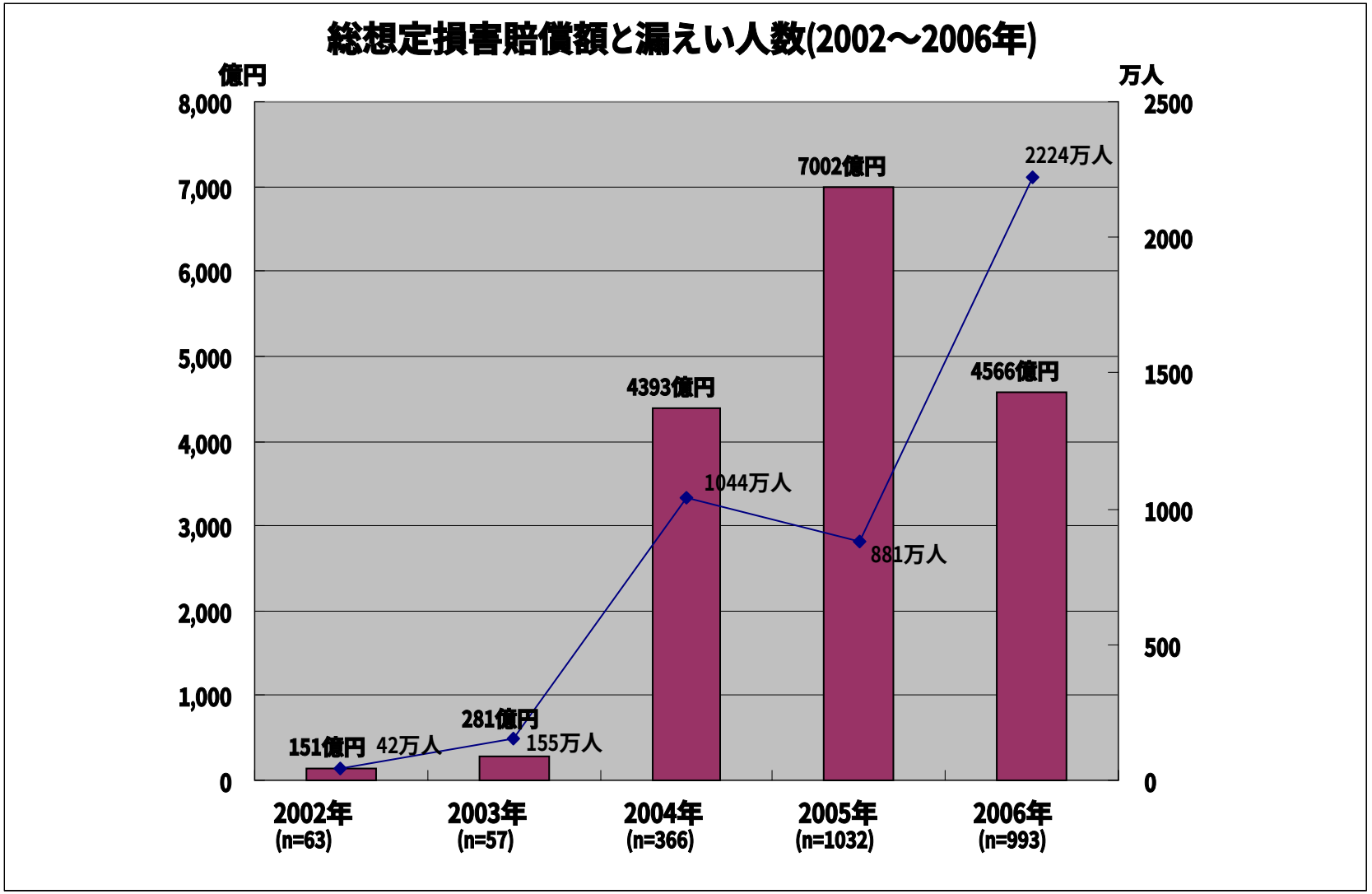
1件当たりの平均想定損害賠償額

2002年	2003年	2004年	2005年	2006年
3億4404円	5億5038万円	13億8897万円	7億868万円	4億8112万円

1人当たりの平均想定損害賠償額

2002年	2003年	2004年	2005年	2006年
1万6855円	8万9140円	10万5365円	4万6271円	3万6628円

2006年 想定損害賠償算定④



実際の判決と算定式による算定の比較

- Yahoo! BB の例
  - 背景
    - 元従業者による持出し
    - 漏えい件数： 約471万人分 (2003年)
    - 漏えい情報： 氏名、住所、電話番号、メールアドレス、申込日
    - 実被害なし
    - 原告： 5名
  - 判決
    - 6,000円／人　運営会社 BBテクノロジー (旧ソフトバンクBB)
  - 算定式

    基礎情報価値×機微情報度×本人特定容易度×社会的責任度×事後対応評価

    ＝ 500×（10^{1-1}＋5^{1-1}）×6×2×1

    ＝ 12,000円

実際の判決と算定式による算定の比較

- TBC の例
  - 背景
    - CGIの設定ミス（ハッキングの可能性）
    - 漏えい件数： 約3万7千人分（2002年）
    - 漏えい情報： 氏名、住所、電話番号、メールアドレス、スリーサイズ
    - 実被害： 迷惑メール、掲示板への掲載
    - 原告： 14名
  - 判決
    - 13人に対し 35,000円／人　1人に対し 22,000円／人
  - 算定式

    基礎情報価値×機微情報度×本人特定容易度×社会的責任度×事後対応評価

    ＝ 500×（10^{2-1}＋5^{1-1}）×6×1×1

    ＝ 33,000円

現行の課題

- 調査対象が個人情報漏えいに特化している
- 定量的分析に終始している
- 汎用的な被害額算定式の必要性

今後の活動案

- 個人情報漏えい以外のインシデントの調査
  - 同様の調査を行なっている組織との差別化が懸案
- インシデントの定性的評価
  - 初心に返ってヒアリング調査の実施
- 汎用的な被害額算定式の策定
  - 煩雑ではない使い易い算定式の策定