



2007年 情報漏えいインシデント 分析結果報告

～ データから見る情報漏えい対策の現状～
(9:30 - 10:15)

セキュリティ被害調査ワーキンググループ
大谷 尚通
(株)NTTデータ

2008年6月13日

2007年報告書の公開のお知らせ



- 1 はじめに
- 2 報告書について
- 3 2007年の個人情報漏えいインシデントの分析結果
 - 個人情報漏えいインシデント・トップ5
 - 2007年 単年分析
 - 2007年 想定損害賠償額算定結果
 - 2007年 単年・相関分析
 - 2007年 経年分析
 - 2007年 想定損害賠償額の経年分析
- 4 個人情報漏えいにおける想定損害賠償額の算出モデル
- 5 漏えいインシデントの事後処理コスト
- 6 最後に
- 7 お問い合わせ先

- 8 【付録1】 WINNYインシデント解説
- 9 【付録2】 漏えい原因の定義
- 10 【付録3】 インシデント一覧表

目次

□ 『2007年情報セキュリティインシデントに関する調査報告書』

単年分析

想定損害賠償額算定結果

単年・相関分析

経年分析

想定損害賠償額の経年分析

今後の議論の題材になることや、
企業経営者が考えるべき情報セキュリ
ティのリスク量の把握や行うべき
投資判断の一助となることを目的として、
検討および提案を行なっている。

□ 裁判事例と算定結果の比較

Yahoo! BB

TBC

ジャパネットたかた

売上被害額と緊急対応費用の推定

□ 2007年情報漏えいインシデントの総括

2007年 インシデントの概要



漏えい人数	3,053万1,004人	過去最高
インシデント件数	864件	
想定損害賠償総額	2兆2,710億8,970万円	過去最高
一件当たりの漏えい人数	3万7554人	過去最高
一件当たり平均想定損害賠償額	27億9,346.8万円	過去最高
一人当たり平均想定損害賠償額	3万8,233円	

一日平均2.4件

3,053万1,004人

1億2,777万1,000人

= 約4人に1人の割合

2007年 インシデント・トップ5



No.	漏えい人数	業種	原因
1	約1,443万人	複合サービス事業	管理ミス
2	約864万人	製造業	内部犯罪・内部不正行為
3	約98万人	金融・保険業	管理ミス
4	約65万人	卸売・小売業	管理ミス
5	約47万人	電気・ガス・熱供給・水道業	管理ミス

管理ミス

盗難
紛失・置忘れ

内部犯罪
内部不正行為

2004年 (個人情報保護法施行前)

被害人数	業種名	漏洩原因区分
452万人	情報通信業	不正な情報持ち出し
116万人	金融・保険業	不明
92万人	製造業	不正な情報持ち出し
63万人	サービス業	内部犯罪・内部不正行為
51万人	卸売・小売業	内部犯罪・内部不正行為

2005年

被害人数	業種名	漏洩原因区分
131万人	金融・保険業	紛失・置忘れ
85万人	情報通信業	内部犯罪・内部不正行為
57万人	金融・保険業	紛失・置忘れ
47万人	公務	盗難
32万人	公務	盗難

2006年

被害人数	業種名	漏洩原因区分
538万人	製造業	不明
400万人	情報通信業	内部犯罪・内部不正行為
400万人	情報通信業	内部犯罪・内部不正行為
176万人	公務	紛失・置忘れ
96万人	金融・保険業	紛失・置忘れ

2007年 単年分析

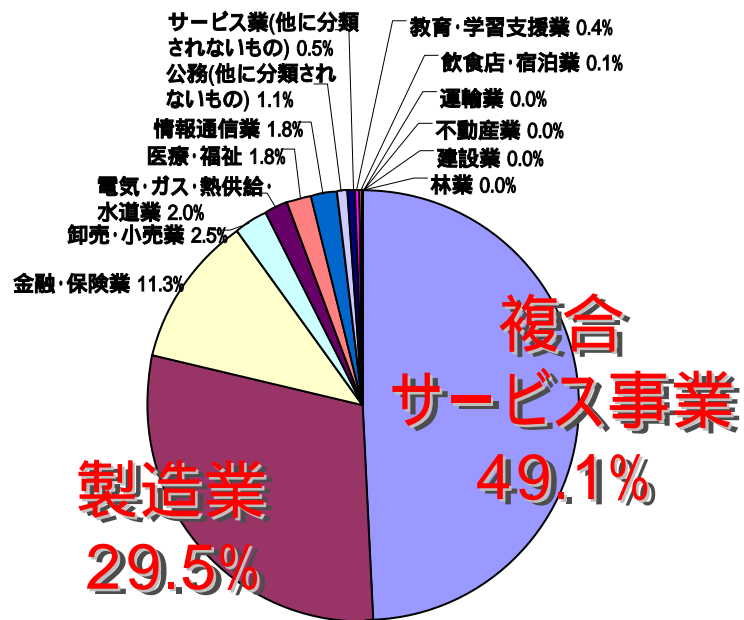


図 1: 業種別比率(人数)

大規模なインシデントの影響大
 ↓
 毎年、業種別比率の傾向が異なる
 業種との依存関係は弱い

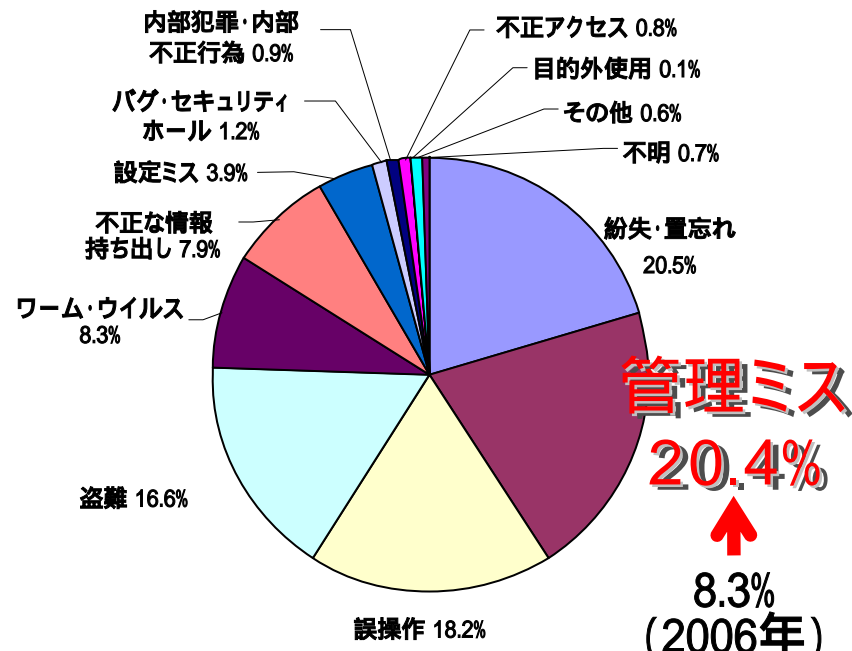


図 2: 漏えい原因比率(件数)

個人情報漏えい対策の浸透
 内部統制への取り組み
 ↓
 組織内の情報管理が強化
 ↓
 情報の棚卸しにより、
 組織内の誤廃棄や紛失が判明

2007年 想定損害賠償額算定結果

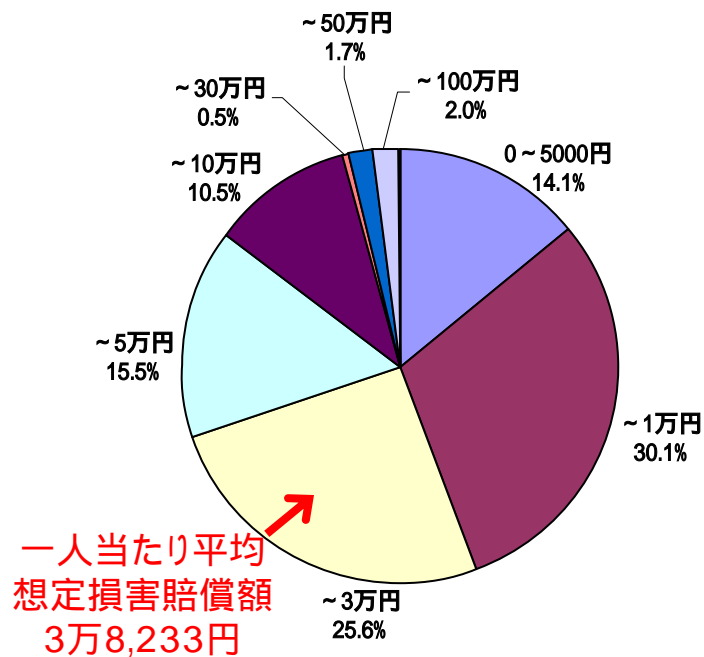


図3: 一人当たりの
想定損害賠償額比率(件数)

「5000円～1万円」・「1～3万円」= 55.7%
比較的、一人当たりの想定損害賠償額が
低いインシデントが多い

一件当たり平均
想定損害賠償額
27億9,346.8万円

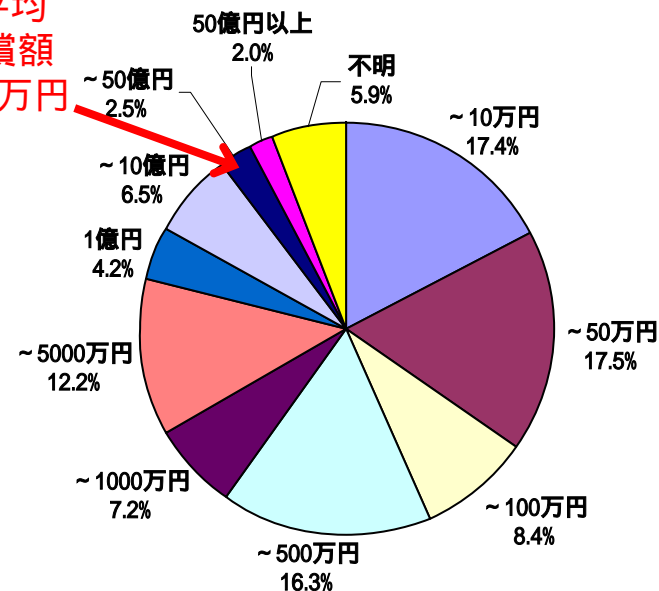


図4: 一件当たりの
想定損害賠償額比率(件数)

一件当たりの想定損害賠償額の
インシデントの分布は分散している。
50億円以下のインシデントに
顕著な傾向はない。

2007年 単年・相関分析

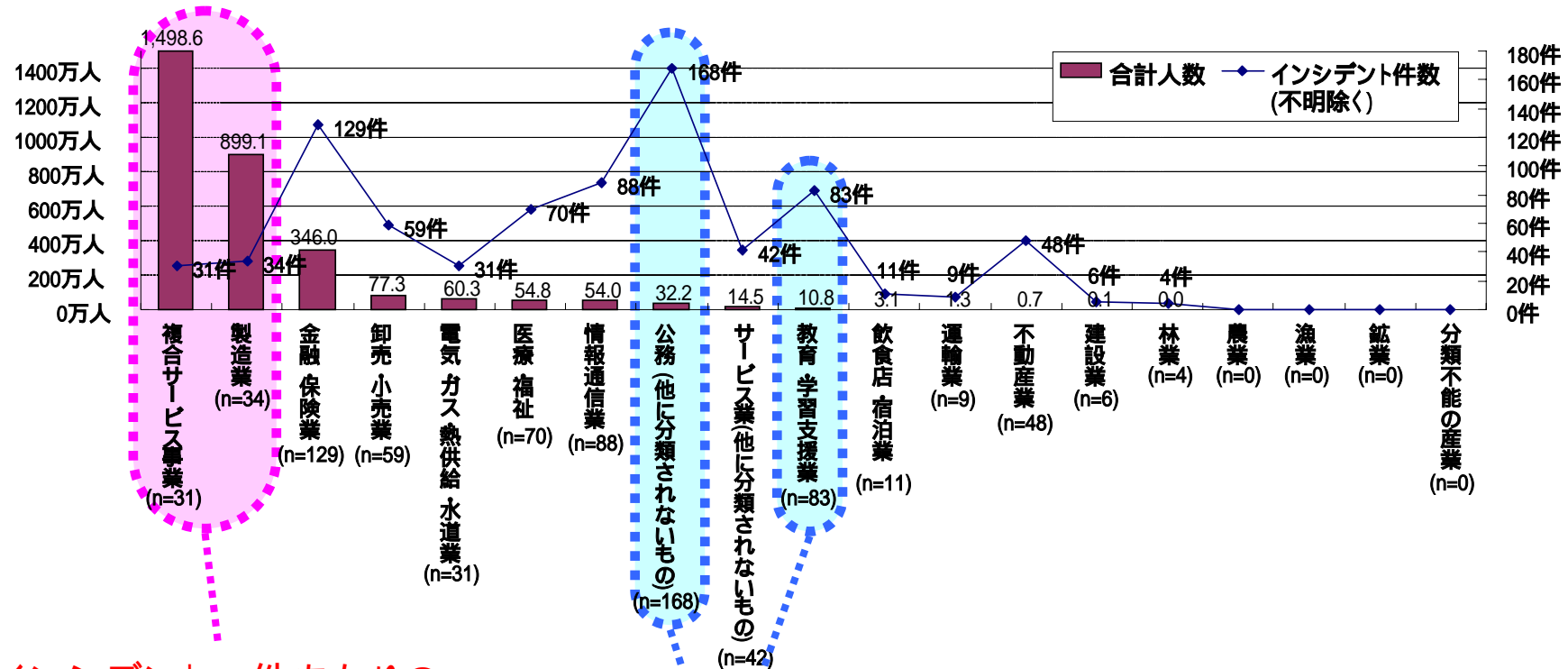


図 5: 業種別のインシデント件数と漏えい人数

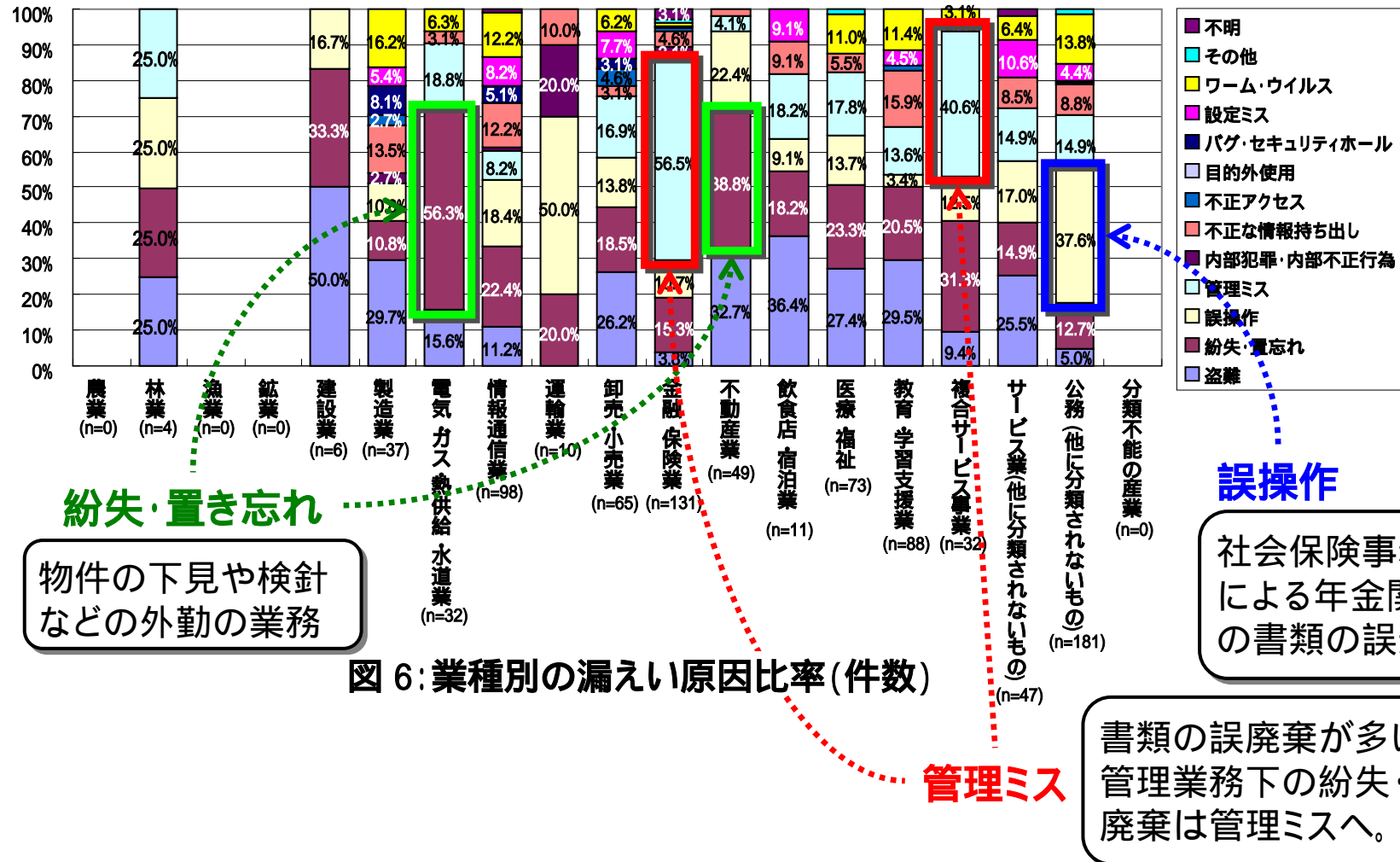
インシデント一件あたりの漏えい人数が多い (規模が大きい)

複合サービス事業	約1,443万人
製造業	約864万人

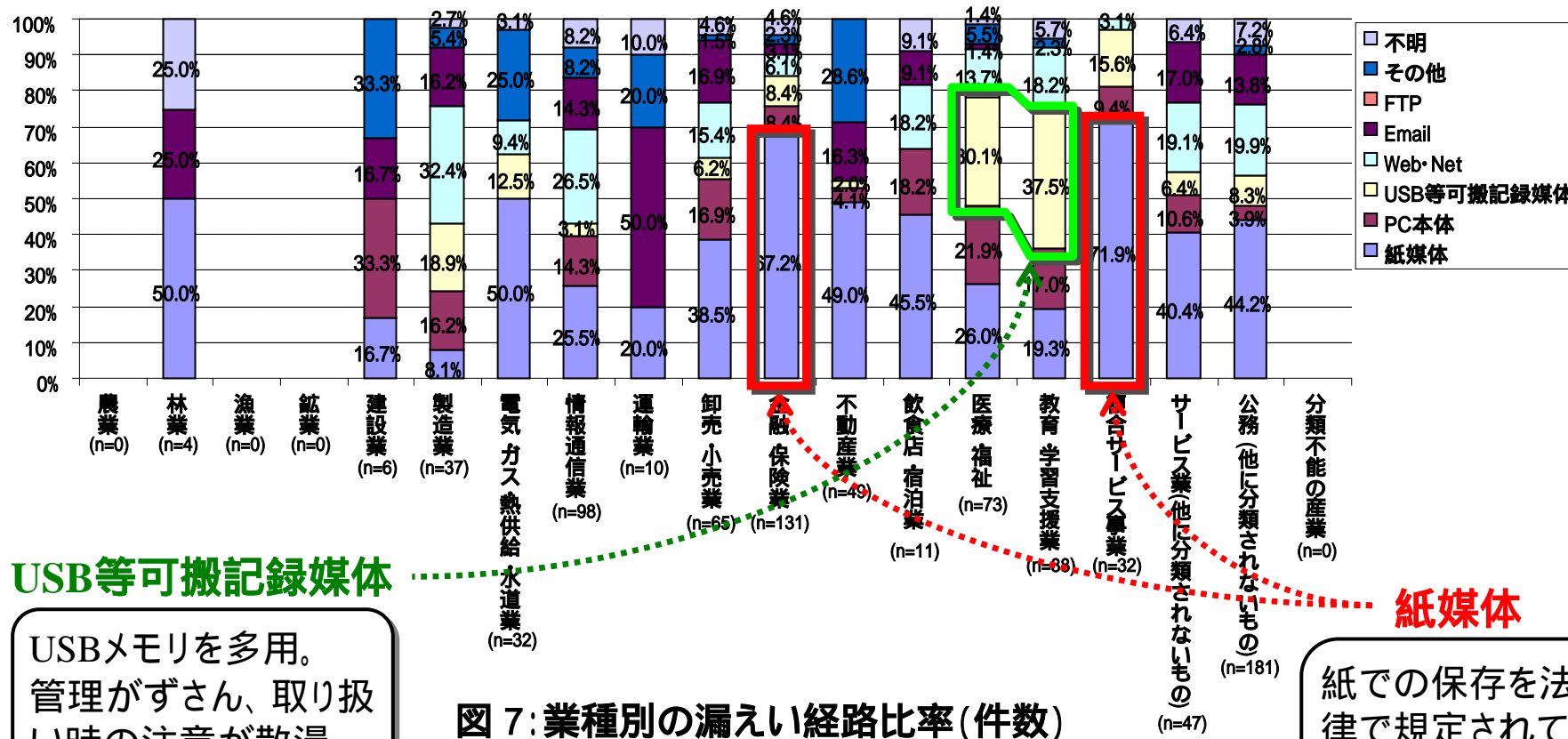
インシデント一件あたりの漏えい人数が少ない (規模が小さい)

公的書類(住民票、年金書類): 一人単位
教育・学習支援業: クラス単位(20~40人)

2007年 単年・相関分析



2007年 単年・相関分析



USB等可搬記録媒体

USBメモリを多用。
管理がずさん、取り扱い時の注意が散漫

図 7: 業種別の漏えい経路比率 (件数)

紙媒体

紙での保存を法律で規定されているため、紙を多く使う

2007年 経年分析

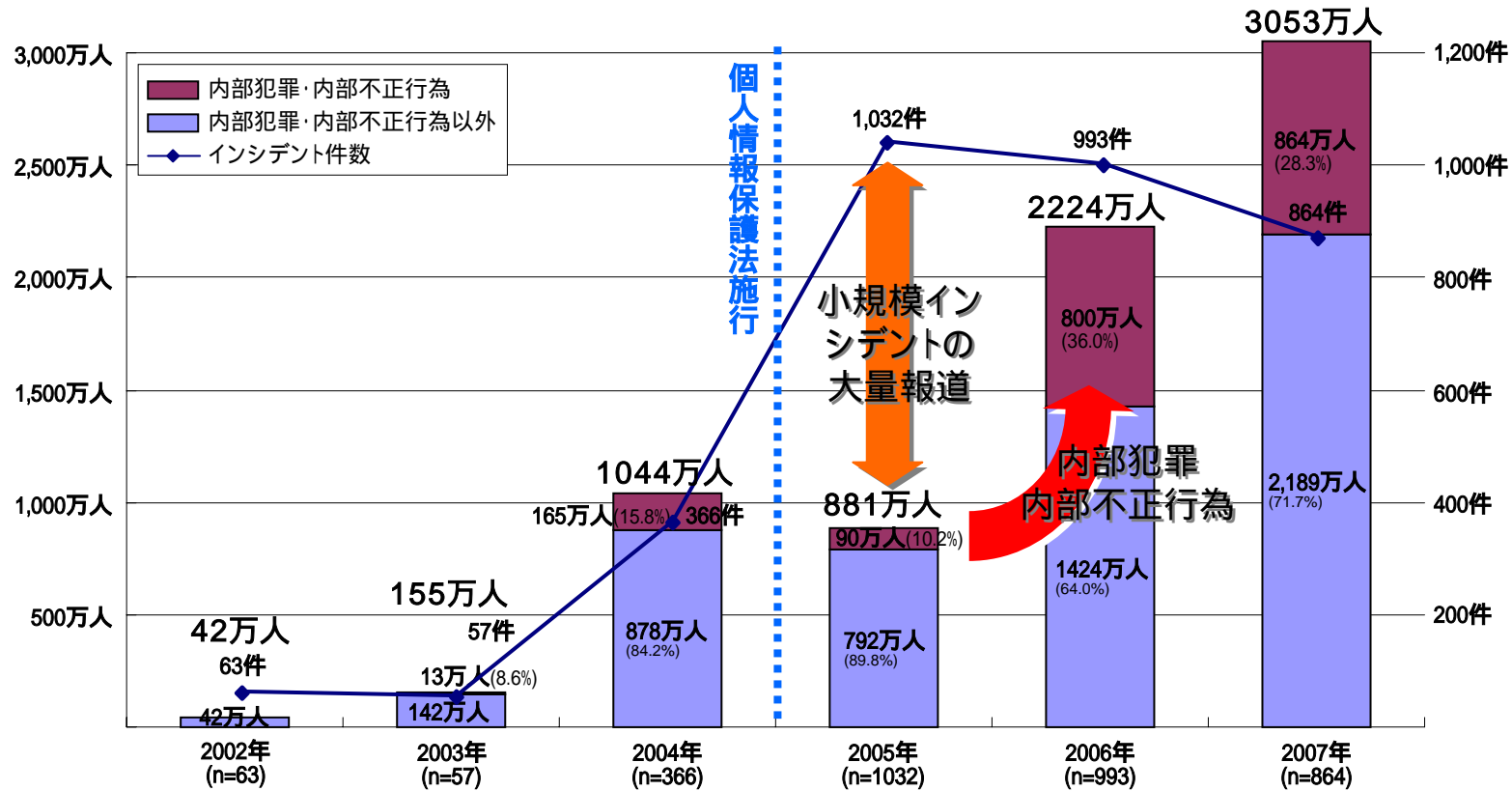


図 8: インシデント件数と内部不正による漏えい人数の経年変化(合計)

2007年 経年分析

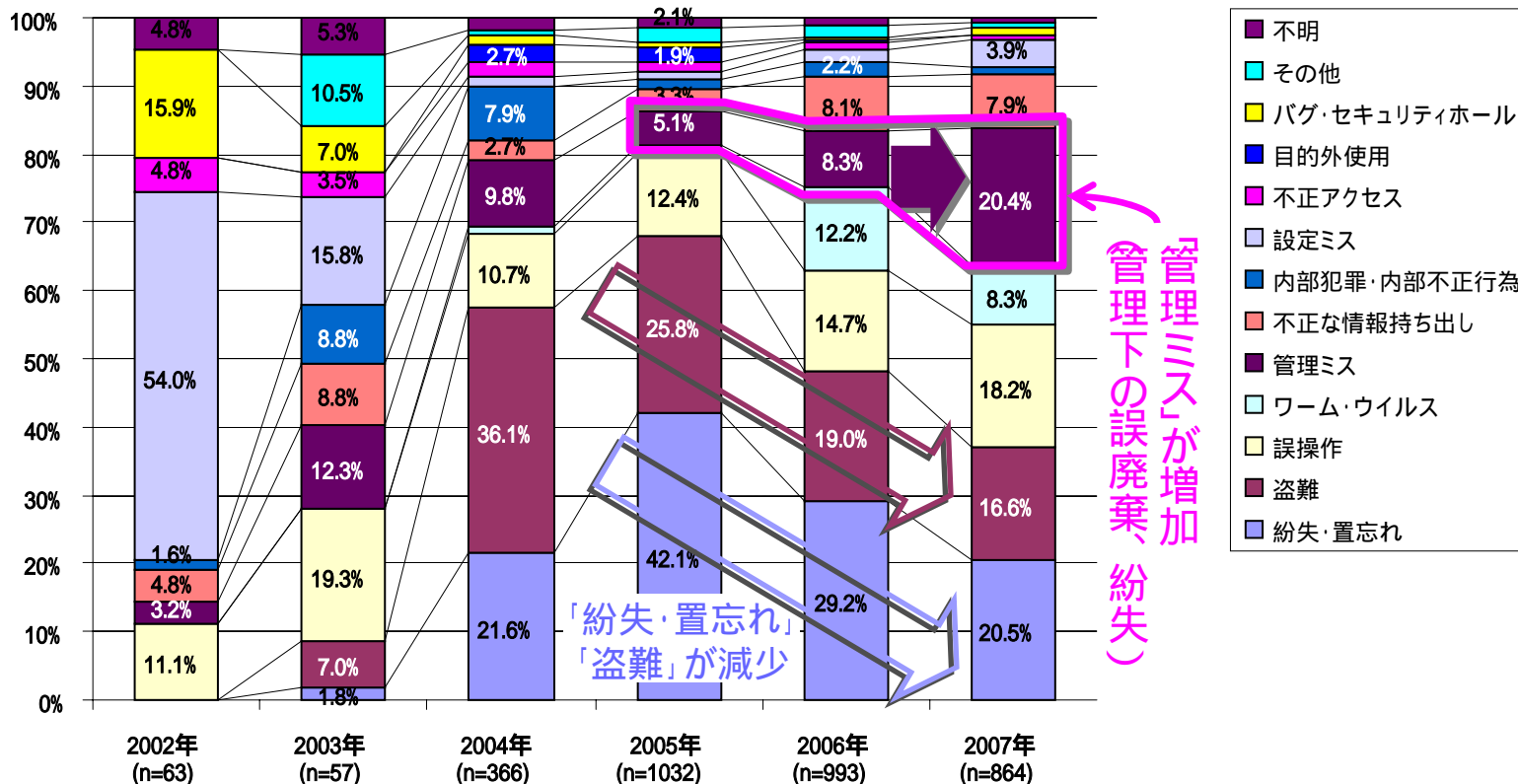


図 9: 漏えい原因比率の経年変化 (件数)

- 個人情報対策が進み、遅れていた組織内の管理体制や管理方法に対策対象が拡大
- 「紛失」を内部統制の観点から「管理ミス」として分類

2007年 経年分析

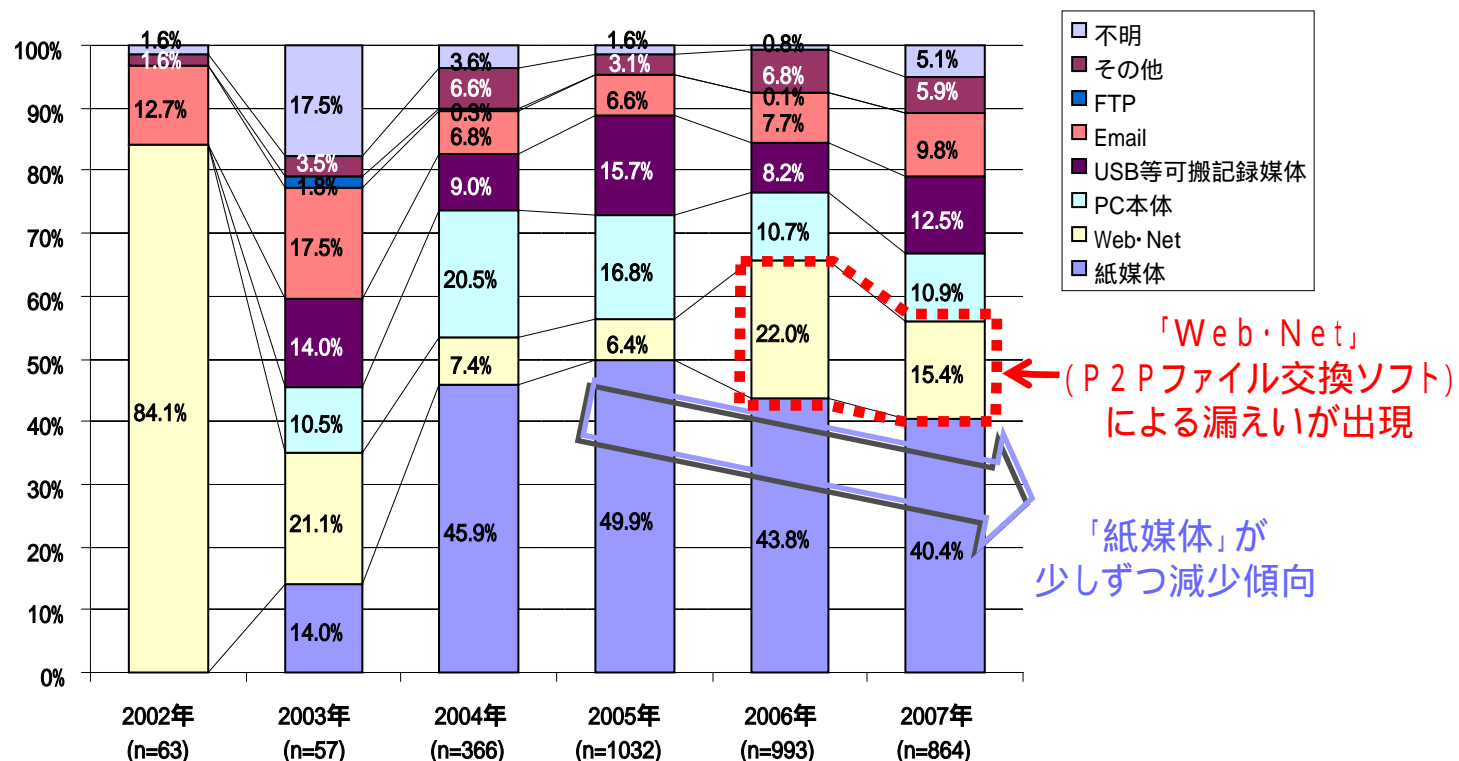


図 10: 漏えい経路比率の経年変化 (件数)

- 紙媒体はわずかに減少傾向だが、依然として多い
- 2006年に続き、P2Pファイル交換ソフトによる漏えいが続いている

2007年 経年分析

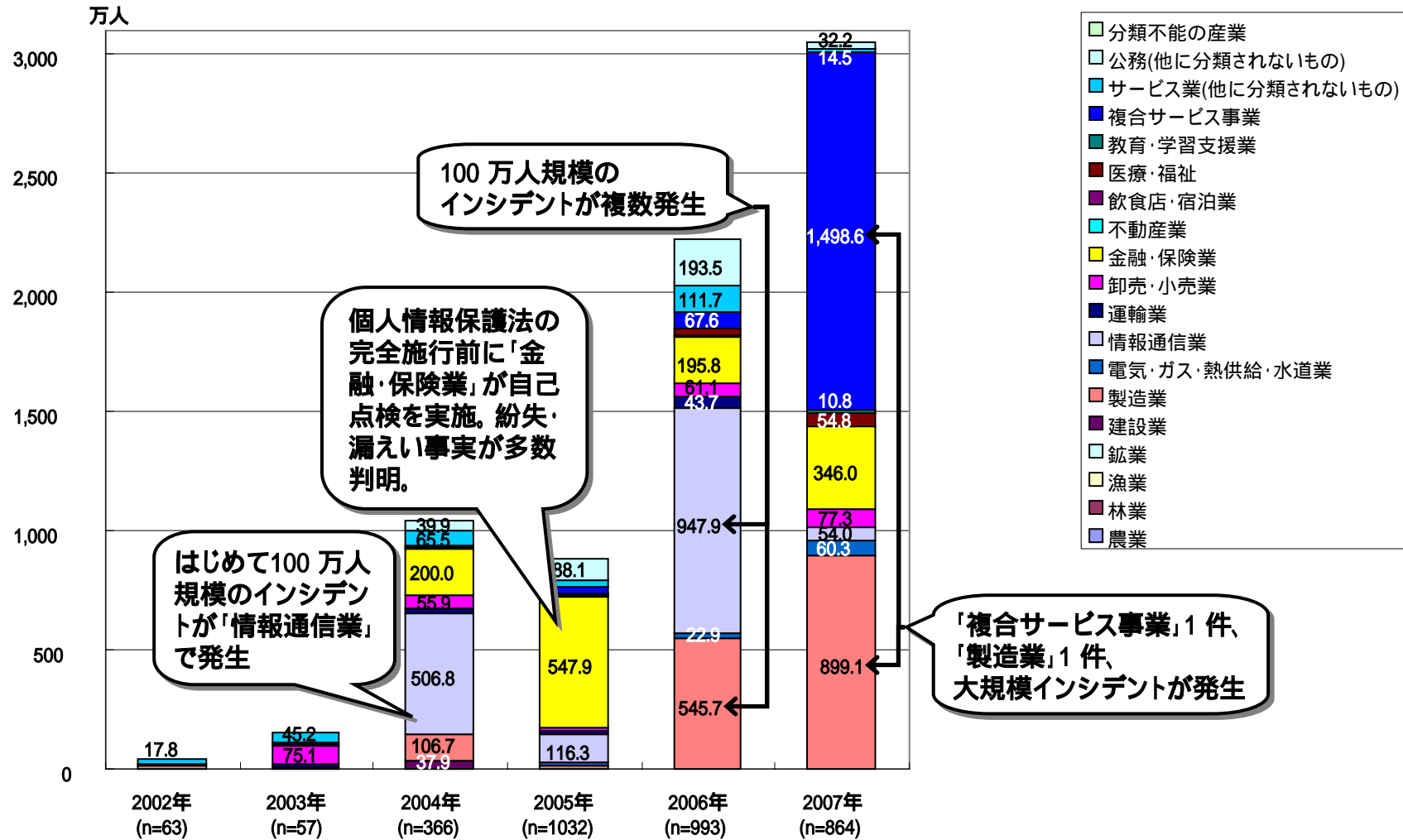


図 11: 業種別漏えい人数の経年変化(合計)

2007年想定損害賠償額の経年分析 **JNSA**

	想定損害賠償総額	一件当たりの 平均想定損害賠償額	一人当たりの 平均想定損害賠償額
2002年 (n=63)	約189億円	2億7,532万円	1万6,855円
2003年 (n=57)	約281億円	5億5,038万円	8万9,140円
2004年 (n=366)	約4,667億円	13億 730万円	10万5,365円
2005年 (n=1032)	約7,002億円	7億 868万円	4万6,271円
2006年 (n=993)	約4,570億円	4億8,156万円	3万6,743円
2007年 (n=864)	約2兆2,711億円	27億9,347万円	3万8,233円

大規模で深刻なインシデントのみ報道。統計データとしては偏りが大きい。

過去最高

過去最高

2007年想定損害賠償額の経年分析 **JNSA**

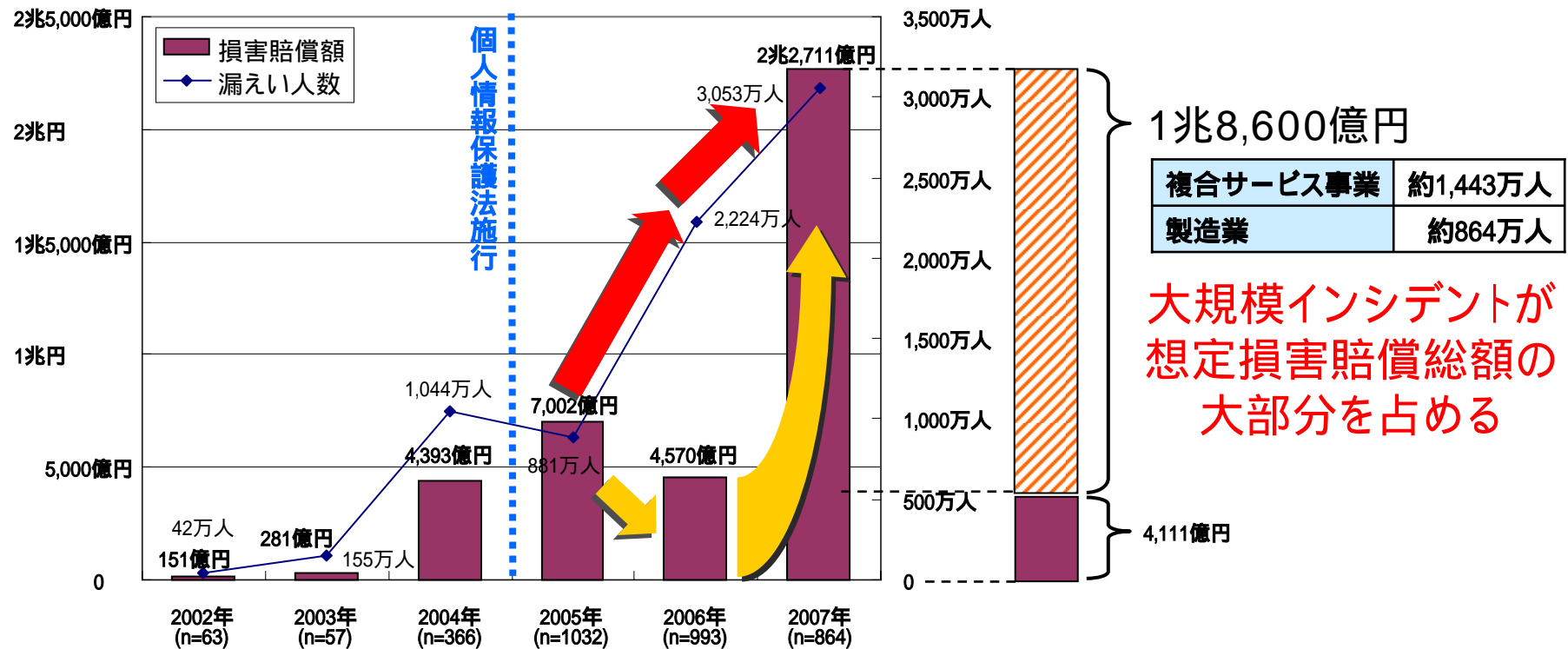
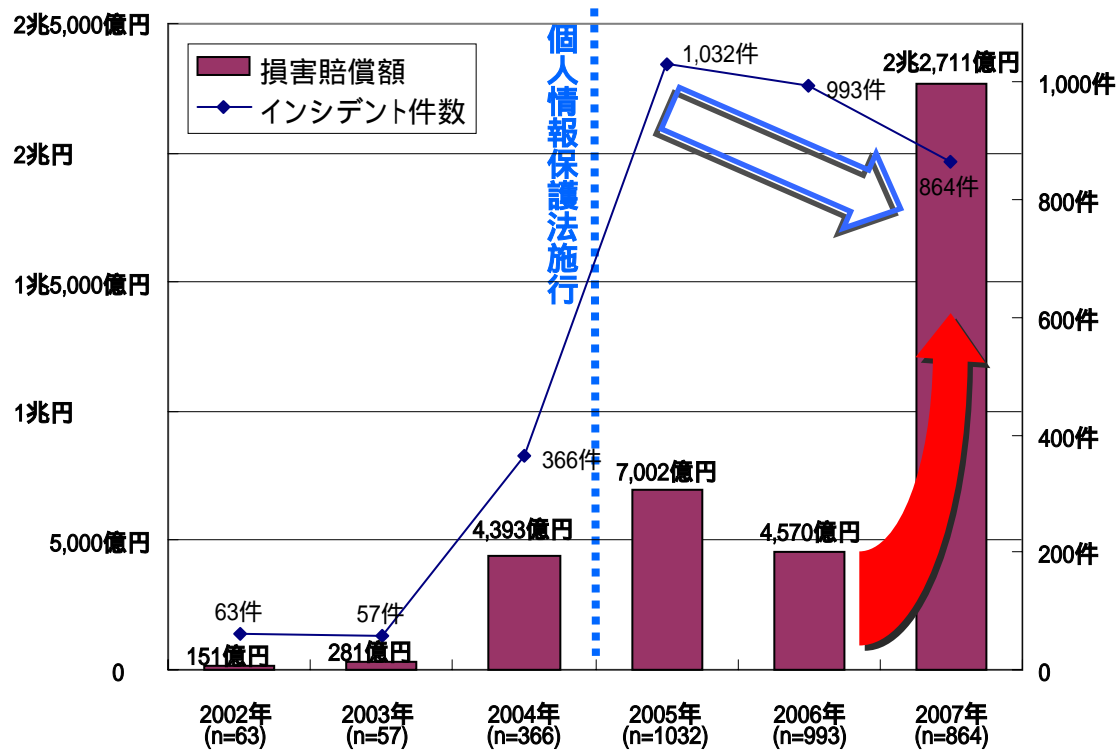


図 12: 想定損害賠償総額と漏えい人数

2007年想定損害賠償額の経年分析 **JNSA**

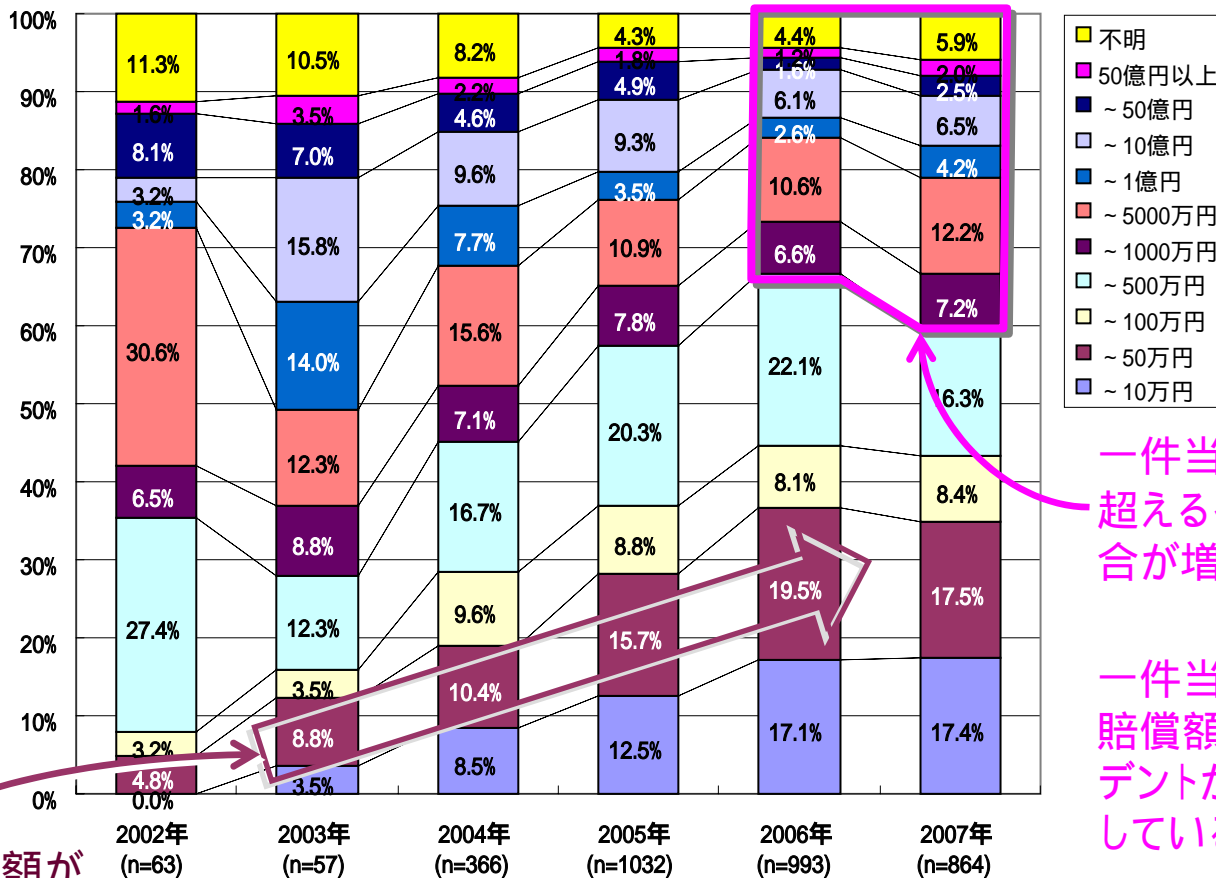


インシデント件数は
減少傾向

想定損害賠償総額は
大幅増加

図 13: 想定損害賠償総額と漏えい件数

2007年想定損害賠償額の経年分析



一件当たり500万円を超えるインシデントの割合が増加

一件当たり500万円を超えるインシデントの割合が増加

一件当たりの想定損害賠償額が高額なインシデントが全体的に増加している

想定損害賠償額が低額のインシデントは増加傾向

図 14: 一件当たりの想定損害賠償額比率の経年変化(件数)

裁判事例と算定結果の比較

【Yahoo! BB】

背景

- ・ 日時: 2004年1月23日公表 (2003年発生)
- ・ 原因: 元従業者による持出し
- ・ 漏えい件数: 約471万人分
- ・ 漏えい情報: 氏名、住所、電話番号、メールアドレス、申込日
- ・ 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

$$\begin{aligned} & \text{基礎情報価値} \times \text{機微情報度} \times \text{本人特定容易度} \times \text{社会的責任度} \times \text{事後対応評価} \\ & = 500 \times (10^{1-1} + 5^{1-1}) \times 6 \times 2 \times 1 \\ & = 1万2,000円 \end{aligned}$$

裁判事例と算定結果の比較

【TBC】

背景

- ・ 日時: 2003年5月27日公表 (2002年5月26日発生)
- ・ 原因: 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
- ・ 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
顔写真など
- ・ 被害: 迷惑メール、掲示板への掲載
- ・ 原告: 14名

判決

- ・ 3万5,000円 / 人 (13人) 2万2,000円 / 人 (1人)

算定式

$$\begin{aligned} & \text{基礎情報価値} \times \text{機微情報度} \times \text{本人特定容易度} \times \text{社会的責任度} \times \text{事後対応評価} \\ & = 500 \times (10^{2-1} + 5^{1-1}) \times 6 \times 1 \times 1 \\ & = 3万3,000円 \end{aligned}$$

裁判事例と算定結果の比較

【ジャパネットたかた】

背景

- ・ 日時: 2004年3月9日公表 (1998年2月発生)
- ・ 原因: 個人情報 を不当に記録して売却
- ・ 漏えい件数: 51万3940人
- ・ 漏えい情報: 氏名、性別、住所、電話番号、生年月日、年令
- ・ 被害: (たかた側被害 = 売上減150億円?)
- ・ 原告: ジャパネットたかた

判決

- ・ 1億1,000万円
(5,000円/人 × 51万人 = 25億5,000万円のうち賠償可能な額)

ジャパネットたかたが
被った被害?

算定式

$$\begin{aligned} & \text{基礎情報価値} \times \text{機微情報度} \times \text{本人特定容易度} \times \text{社会的責任度} \times \text{事後対応評価} \\ & = 500 \times (10^{1-1} + 5^{1-1}) \times 6 \times 1 \times 1 \\ & = 6,000\text{円} \end{aligned}$$

想定損害賠償総額 30億8,364万円

裁判事例と算定結果の比較

再考



インシデント被害額 = 直接被害額 + 間接被害額 + 潜在化被害

逸失利益
復旧に要したコスト
営業継続費用
喪失情報資産額
機会損失額

システムの規模に
応じた被害額

補償、補填、損害賠償
など、間接的に生じた
被害額

補償・損害賠償
訴訟費用

業務にかかわる潜在化被害
業務外の潜在化被害

ブランド価値、顧客イメージ

裁判で提示した損害額
(顧客からの損害賠償請求は無い)

営業活動自粛期間 = 2004年3月9日 ~ 4月24日 = 47日
2003年度売上高 = 705億4000万円
47日分売上高 = 90億8323万円
ジャパネットたかたの利益率 = 6%

||
5億4499万円

その他にも、対策費用、業務を停止していた間の社員の給料など...

売上被害額と緊急対応費用の推定

詳細は、「2003年度 情報セキュリティインシデントに関する調査報告書 第二部」を参照。

【企業プロフィール】
 想定した企業は、雑誌やインターネット上のカタログに商品を掲載し、商品の販売を行う通信販売業とした。近年は、インターネットショッピングサイトも運用し、インターネットショッピングサイトの売り上げは、会社全体の売り上げの約10%程度とした。以下に想定企業のプロフィールを示す。(インターネットショップ部門の利益率 = 約10%、年間成長率 = 約10%とする。)

企業規模	
売上高	約1000億円
従業員	約1000名
カタログ販売部門	
会員数	約600万人
売上げ	約900億円
インターネットショップ部門	
会員数	約100万人
売上げ	約100億円
従業員	約30名

30万人分が漏洩!

項目			費用
直接被害	逸失利益	インターネットショッピングサイト利益額(1ヶ月分)	約8,330万円
	機会損失	インターネットショッピングサイトの成長率分(1ヶ月相当)	約830万円
間接被害	業務継続費用	対策組織業務に係る人件費(1ヶ月分)	約2,000万円
		セキュリティコンサルタントの依頼費用(1ヶ月分)	約500万円
	損害賠償費用	損害賠償費用	約108万円
		弁護士費用、裁判費用	約9万円
	見舞品費用	見舞品代+送料他(30万人分)	約2億1,000万円
	謝罪訪問費	謝罪訪問に掛かる費用(15人分)	約165万円
	広報費用	謝罪広告費(新聞5紙)	約1,000万円
		情報公開ページ作成費用(5回)	約25万円
臨時的な対策費用	コールセンター設置費用(1ヶ月分)	約1,000万円	
	問い合わせ窓口常駐人員(1ヶ月分)	約300万円	
潜在化被害	影響業務	影響を受けた業務の人件費(1ヶ月分)	約3,000万円
	業務外の潜在化被害	ブランド価値の低下	+ α
合計			約3億8,237万円

2007年情報漏えいインシデントの総括



情報漏えいインシデントの注目度はやや薄れてきている

2005年：個人情報保護法の施行

2006年：Winnyによるインシデント多発



加熱報道・過剰反応がひと段落

情報の外部持ち出し対策が浸透

インシデント件数は、2005年以降、減少傾向

小規模インシデントの件数が、全体的に減少傾向

内部統制との相乗効果により情報管理が強化

対応が遅れていた組織内情報の管理に対策対象が移行

管理強化により、保有情報や資料の再点検・棚卸しを実施

組織内での誤廃棄や紛失が判明。原因を管理ミスと定義。

2008年 活動計画

【主な活動内容】

- 2008年の情報漏えいインシデントの調査・分析、報告書の作成
- **情報漏えい以外の情報セキュリティインシデントのモデル検討**

【年間活動予定】

- 5月 2007年度調査結果の速報公開、プレスリリース
- 6月 2007年度調査結果報告書の公開、報告会開催
- 7月 2007年度調査結果CDROMの提供開始
- 7月 新しい被害額算定モデルの検討・調査活動の開始**
- 1月 2008年度情報漏えいインシデント調査の分析、報告書作成

報告書の引用、質問について



JNSAのホームページ上にある問い合わせフォームを御活用ください。

- 引用・質問の問い合わせページ
- 当報告書のFAQページ

「成果物」のページ



