JNSA

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

Network Security Forum 2009 【A1】

情報漏えい対策の次の一手に向けて

セキュリティ被害調査WG

大谷 尚通

(株) NTTデータ

2010 年 1月27日

本日の内容

■2009年 情報セキュリティインシデントに関する調査【上半期速報】

■情報漏えい対策の次の一手に向けて

セキュリティ被害調査WG

JNSA

目的

- **情報セキュリティインシデントにおける被害の定量化**
- **適切な情報セキュリティに対する投資判断、投資対効果の提示**
  - 企業における情報セキュリティインシデントに係る被害額・投資額などの実態をアンケートやヒアリングによって調査した。この調査結果をもとに**「情報セキュリティインシデントに関する被害額算出モデル」**を策定した。
  - 一年間に報道された個人情報漏えいインシデント（事件・事故）を調査・分析し、**「JOモデル（JNSA Damage Operation Model for Individual Information Leak）」**を用いて想定損害賠償額などを推定し、結果を報告書にまとめた。

新型インフルエンザによる
関西地域の経済損失は744億円（試算）

- 一般家庭の消費減= 720億円
  （四府県の全720万世帯 一律一万円の出費減と仮定）
- 観光関連＝50億円
- イベント中止＝100～120億円
- 休校による周辺への影響＝10億円

情報セキュリティ分野において
被害の定量化や投資対効果の
考え方をもっと普及・発展させたい

セキュリティ被害調査WG メンバ

ワーキンググループリーダー

大谷	尚通	株式会社NTT データ

メンバー

井口	洋輔	株式会社損保ジャパン・リスクマネジメント
大溝	裕則	株式会社JMC リスクソリューションズ
岡本	一郎	株式会社 インフォセック
佳山	こうせつ	富士通株式会社
北野	晴人	日本オラクル株式会社
佐藤	友治	株式会社ブロードバンドセキュリティ
清野	豪	日本オラクル株式会社
田中	洋	株式会社 インフォセック
広口	正之	リコー・ヒューマン・クリエイツ株式会社
丸山	司郎	株式会社ラック
山田	英史	株式会社ディアイティ
吉川	信雄	富士通株式会社
吉田	哲也	兼松エレクトロニクス株式会社
吉田	裕美	株式会社JMC リスクソリューションズ
やすだ	なお	株式会社ディアイティ

2009年
情報セキュリティインシデント
に関する調査

【上半期速報】

2009年上半期 個人情報漏えいインシデント

期間：2009年1月1～6月30日（※6ヶ月分）
インターネットニュースなどで報道されたインシデントの記事、組織からリリースされたインシデントの公表記事などをもとに集計。

漏えい人数	231万9,003人
漏えい件数	764件
想定損害賠償総額	1,545億5,887万円
一件当たりの漏えい人数	3,185人
一件当たり平均想定損害賠償額	2億1,231万円
一人当たり平均想定損害賠償額	4万5,365円

2009年 個人情報漏えいインシデントの比較

	2008年	2009年（上半期×2）
漏えい人数	723万2,763人	463万8,006人
漏えい件数	1,373件	1,528件
想定損害賠償総額	2,367億2,529万円	3,091億1,774万円
一件当たりの漏えい人数	5,668人	3,185人
一件当たり平均想定損害賠償額	1億8,552万円	2億1,231万円
一人当たり平均想定損害賠償額	4万3,632円	4万5,365円

$$\frac{\text{463万8,006人}}{\text{1億2,776万7,994人}} = \text{約28人に1人の割合}$$

一日平均4.2件

2008年
18人に1人
3.8件/日

2009年上半期 インシデント・トップ10

JNSA

No.	漏えい人数	業種	原因
1	148万6,651人	金融・保険業	内部犯罪・内部不正行為
2	14万0,151人	金融・保険業	管理ミス
3	11万0,000人	公務（他に分類されないもの）	不正な情報持ち出し
4	9万2,302人	卸売・小売業	設定ミス
5	7万6,155人	金融・保険業	管理ミス
6	5万0,000人	サービス業（他に分類されないもの）	ワーム・ウィルス
7	2万6,481人	金融・保険業	不正な情報持ち出し
8	2万5,000人	公務（他に分類されないもの）	盗難
9	2万2,937人	サービス業（他に分類されないもの）	盗難
10	1万4,125人	公務（他に分類されないもの）	管理ミス

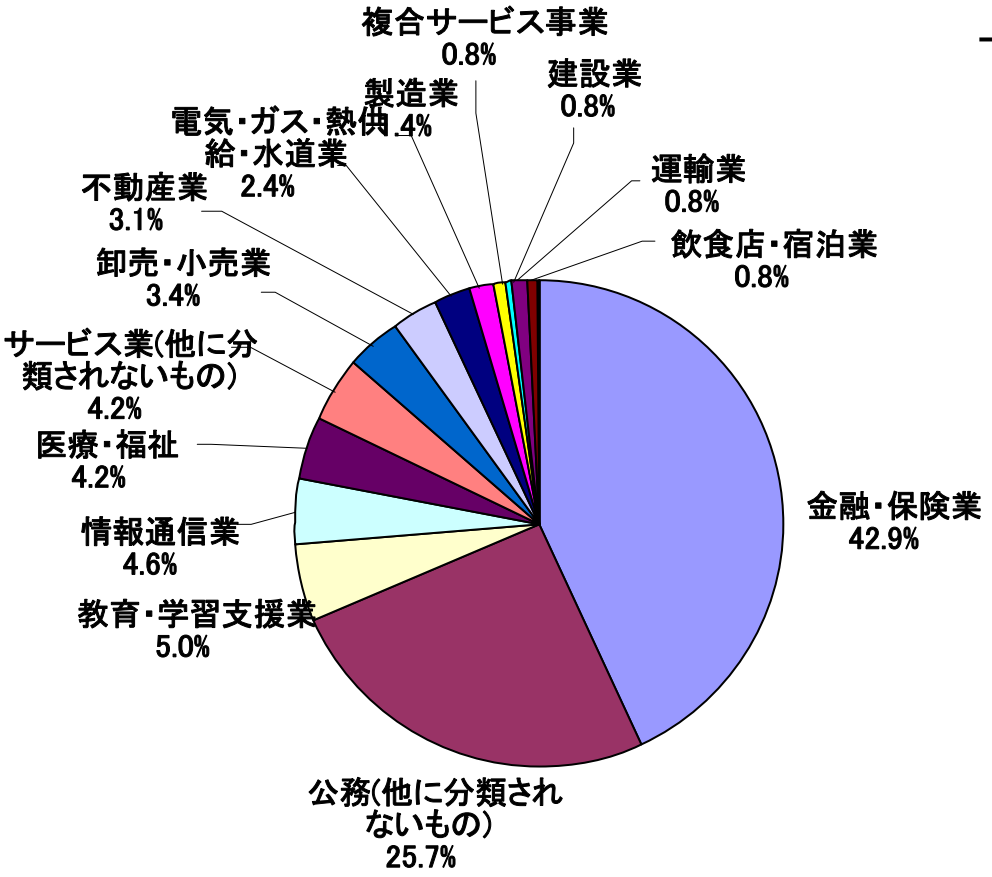
公務、金融が多い。

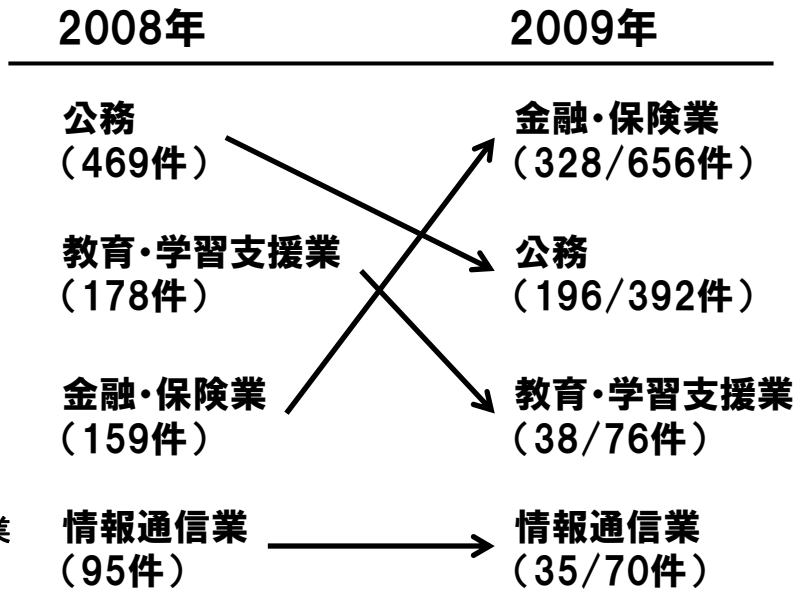
2007年以降、管理ミスが多い

組織内の情報管理の強化（内部統制対応）
↓
大量の誤廃棄

◎100万人を超える大規模なインシデントは1件のみ発生。

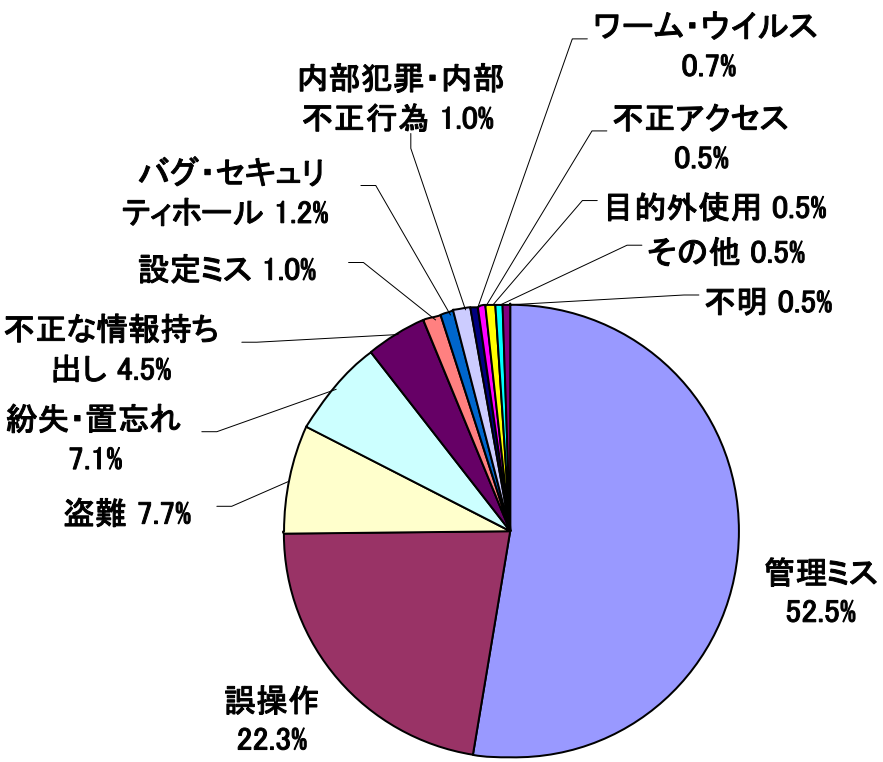
① 業種別の漏えい件数

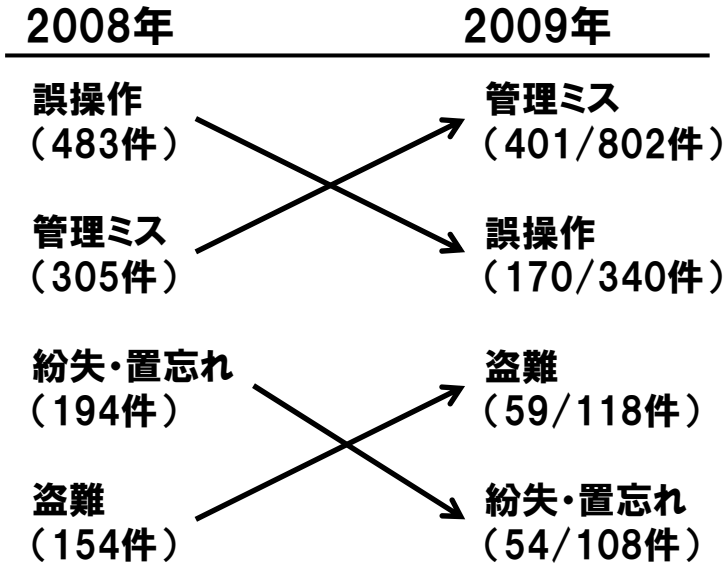




漏えい件数が多い
上位4業種は同じ

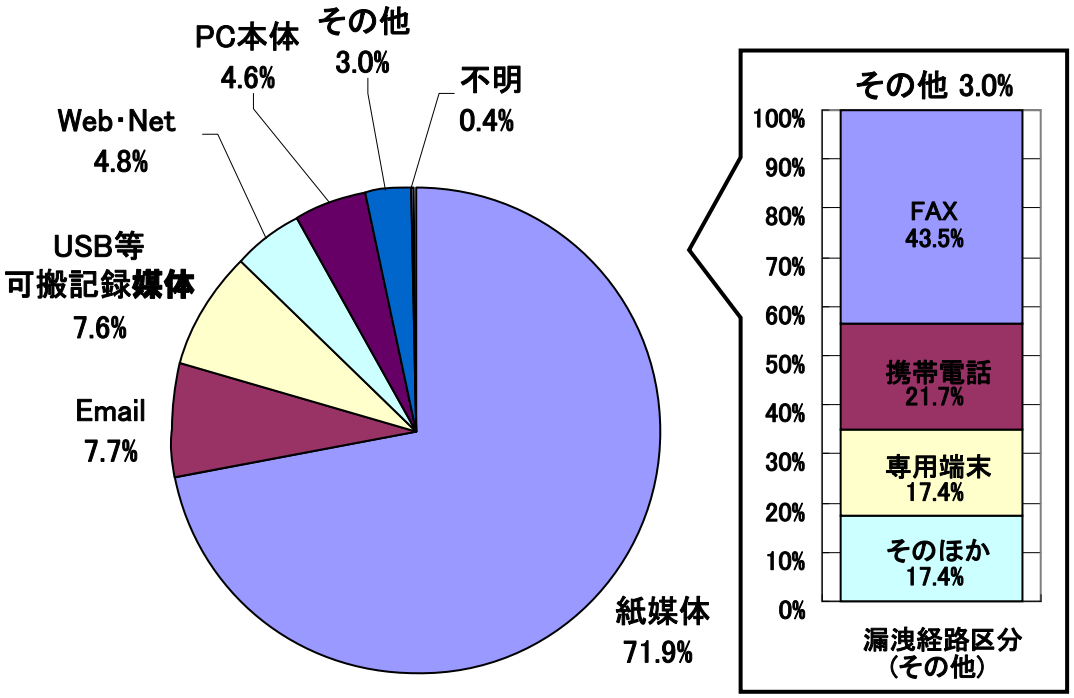
② 原因別の漏えい件数

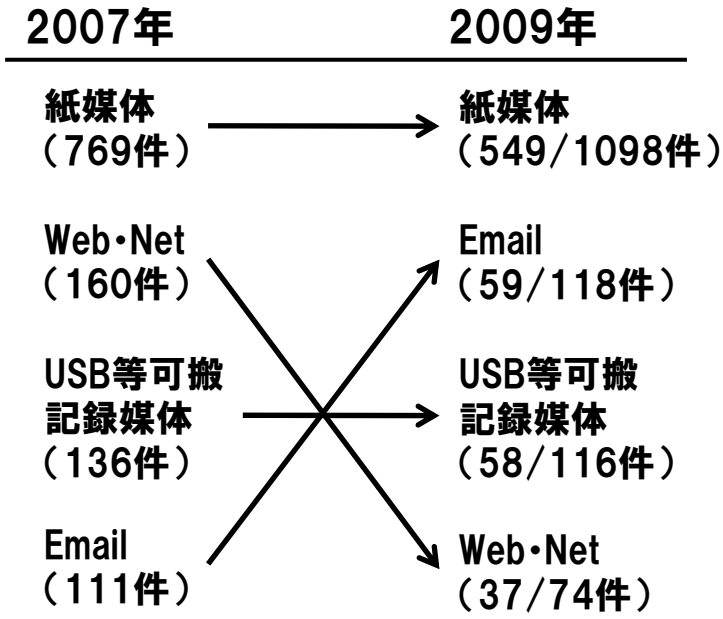




管理ミス＝誤廃棄
誤操作＝ケアレスミス
による漏えいが多い

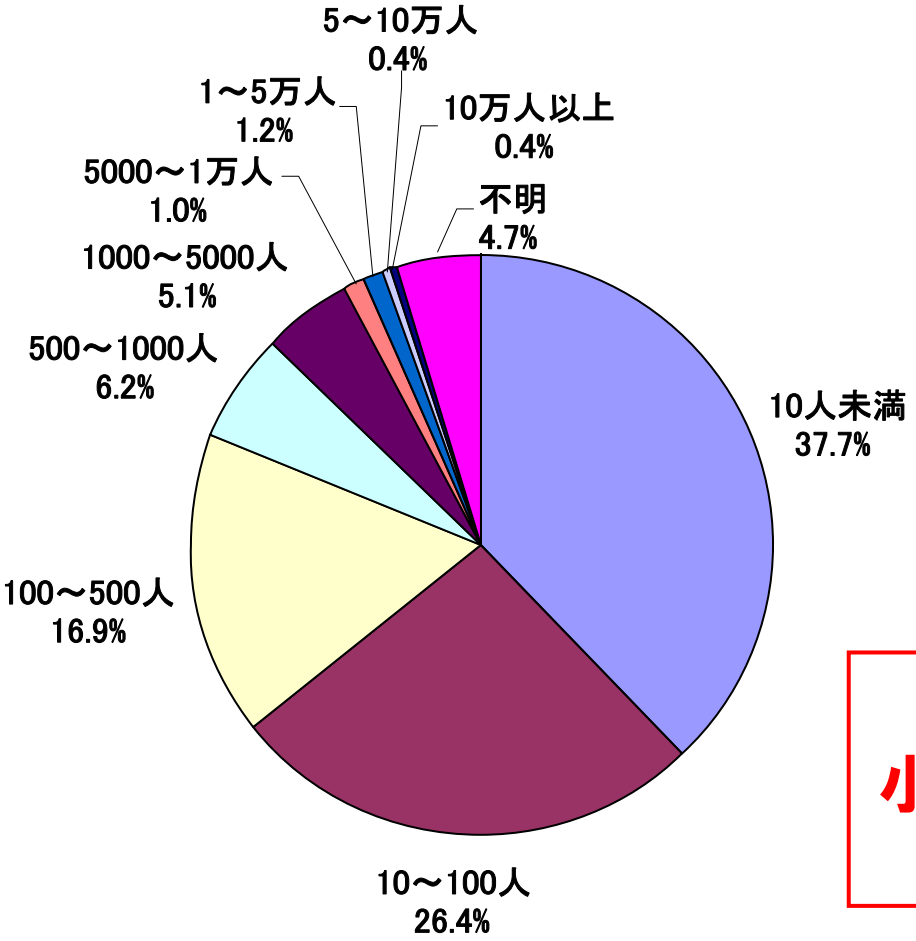
③ 媒体別の漏えい件数





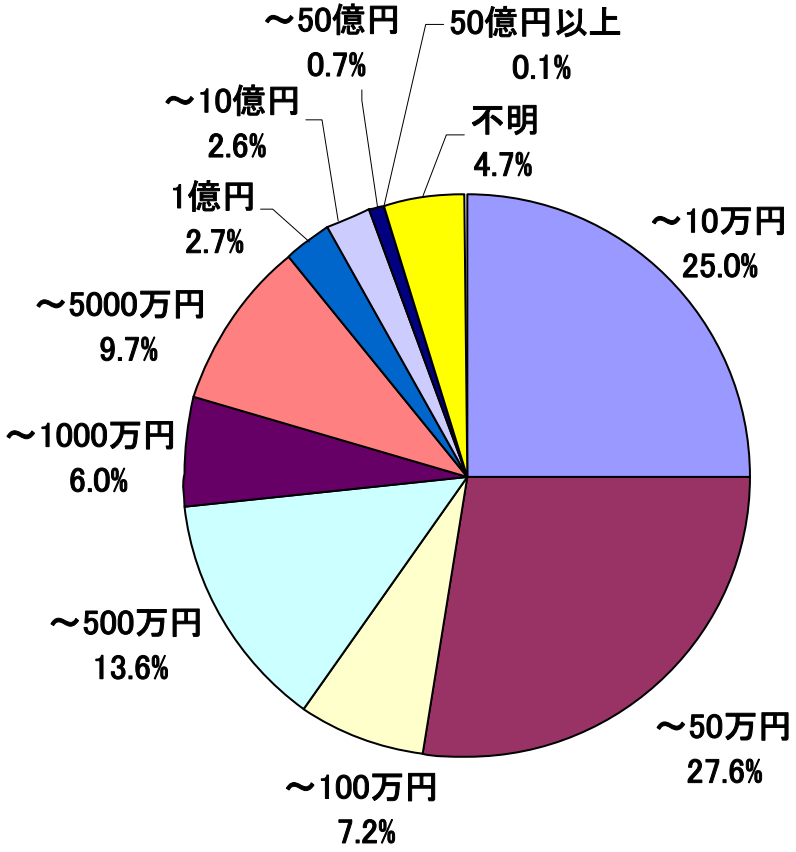
紙媒体による漏えいが多い。
件数が増加（予想）。

④ 一件当たりの漏えい人数



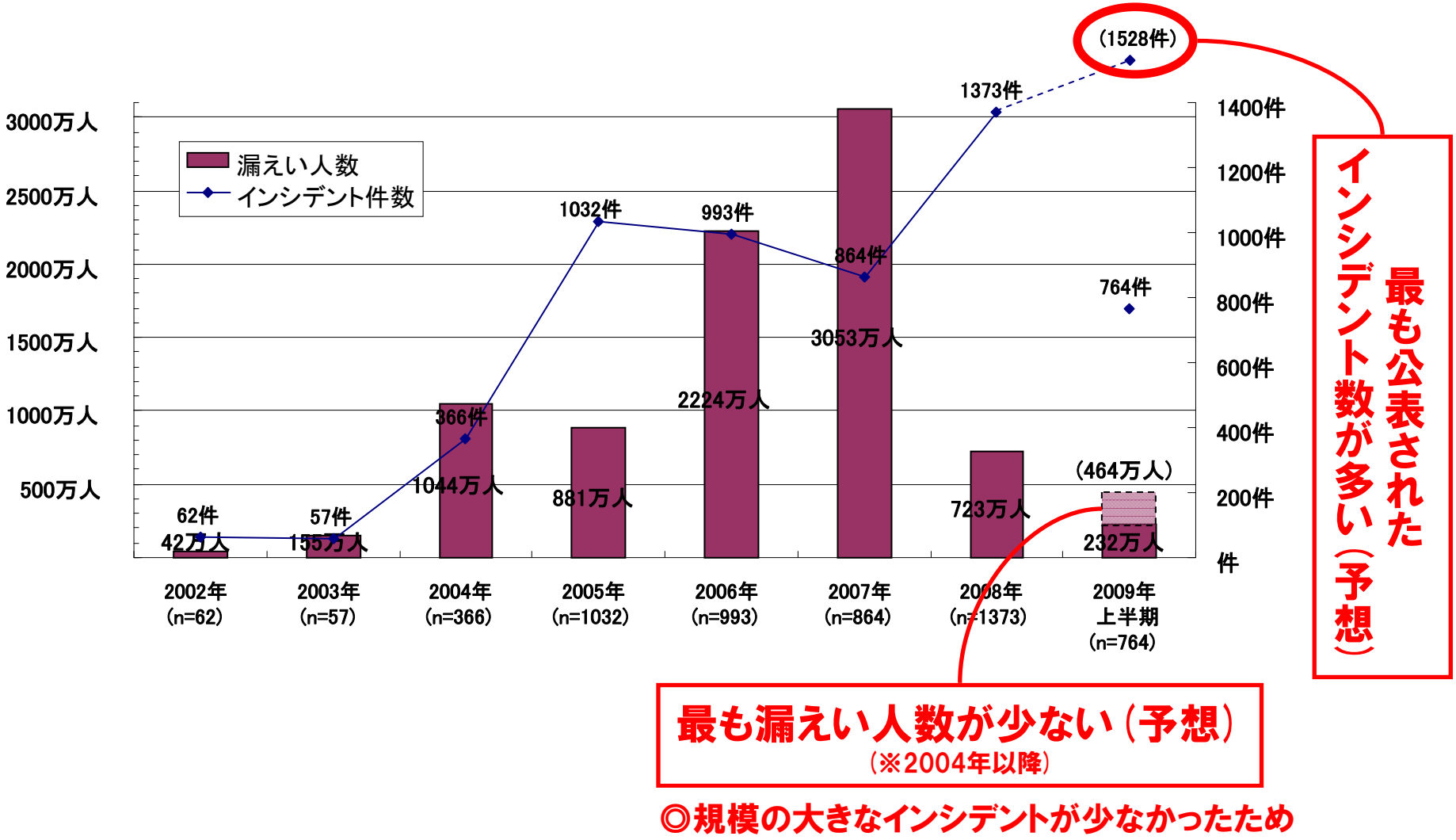
500人/件未満の小さなインシデントの件数が81%を占める。

⑤ 一件当たりの想定損害賠償額

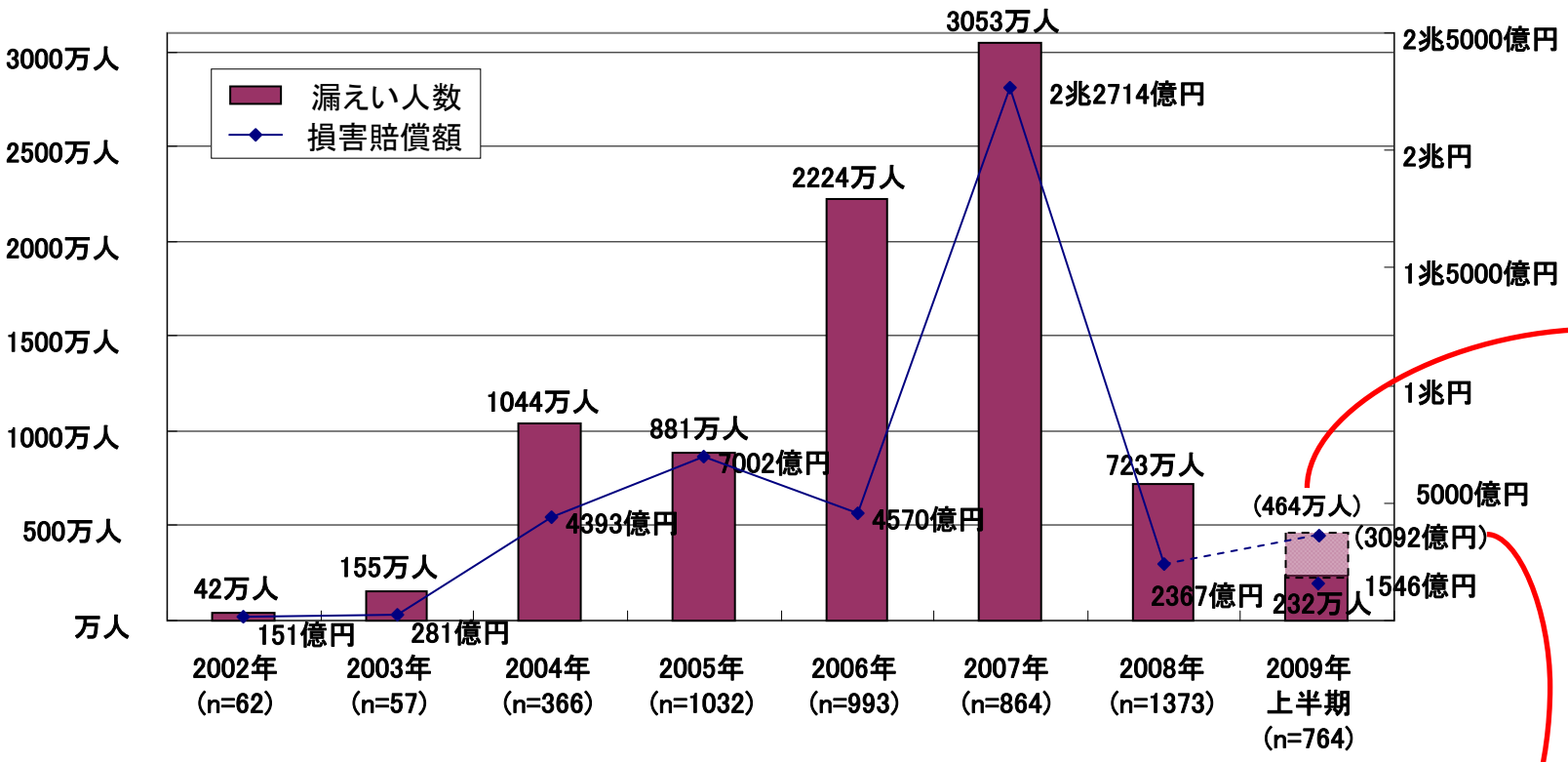


50万円未満の
小さなインシデントの件数が
約半数を占める。

⑥ 漏えい人数と件数(2002～2009年)



⑦ 漏えい人数と損害賠償総額
(2002～2009年)



最も漏えい人数が少ない（予想）
（※2004年以降）

想定損害賠償総額はやや増加（予想）
（※2008年比較）

◎重要な情報を含む100万人を超える
インシデントが1件発生したため。

現状から見える対策の弱点

漏えい件数が大幅に増加（予想）。
（把握できていなかった個人情報漏えいインシデントが明らかになってきている、
インシデントを公表する姿勢が継続しているなど、良い傾向の場合もある。）

紙媒体による個人情報漏えいは、依然として多い。
（管理上の問題、追跡できない、暗号化できないなど）

誤操作などのケアレスミスによる漏えいが、至るところに潜んでいる。
（オフィスルールや手順を定めても、どこかで発生してしまう）

**権限を持った内部犯による悪意に基づくインシデントの防止は、
難しい。**（対策の限界、費用対効果）

情報漏えい対策の次の一手に向けて

情報漏えい対策は進んでいるのか？

JNSA

■ 2008年の情報漏えいインシデントの傾向から

- 1000人/件以上の漏えい件数は、2007年からほぼ横ばい。
- 500万円以上の漏えい件数は、2006年以降、約300件でほぼ横ばい。
- 損害賠償額が1億円以上のインシデントの発生件数は多い。
  （2008年＝計78件、6件/月）

突発的な大規模インシデントの発生ゼロ(?)、漏えい人数の減少、
想定損害賠償総額の減少
⇒一部に対策の効果があったが、全体的には改善していない。

組織内の情報管理の強化
（個人情報保護法対応）
（内部統制対応）
↓
把握できていなかった個人
情報漏えいインシデントが
明らかになってきている

『検知』は向上中

対策効果は停滞気味？

これまでの対策の問題点

JNSA

これまでに組織で行われてきた対策

トップダウンに
もたらされた対策

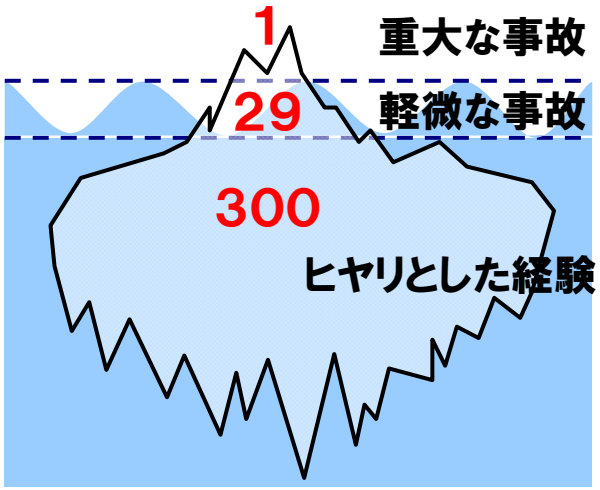
- **持ち出し禁止等のルールの策定**
  - → **ルールが守られない。形骸化。**
  - → **現場の仕事のやり方と合わない。業務に悪影響。**
- **暗号化や書き出し禁止等の対策システムの導入**
- **セキュリティ教育**
  - → **「やらされてる」感。形骸化。**
  - → **意識・リテラシーは向上している?**

次の一手へ

守るべき情報を扱う現場の人々が
積極的に関わるボトムアップな対策へ

ハインリッヒの法則

米国の技師ハインリッヒ氏(H. W. Heinrich)
労働災害の発生確率の研究から導いた経験法則
「1:29:300の法則」、「ヒヤリ・ハットの法則」
人間の行為に基づくインシデントの確率的な考え方



これまでの個人情報漏えいインシデントの調査結果から

- 複数の軽微な問題が連なってインシデントが発生する
- ルールや作業手順など、必ず人間が介在する部分が存在する
- ケアレスミスによって、漏えいインシデントが発生してしまう
- 人間が介在する限り、インシデントは無くならない

対策にハインリッヒの法則を適用できないか？

ハインリッヒの法則を活用した対策

JNSA

■軽微なインシデントを検出し、対応する。
→軽微なインシデントが引き金となって大きなインシデントに拡大することを防ぐ
→より早い段階のちょっとした失敗やヒヤリとした体験レベルの原因に対処するほうが、対応しやすく、効果的な対策が行える

■ヒヤリとした経験、軽微なインシデント経験を蓄積
→多くの現場の実務者に経験として蓄積されやすい
→インシデント未経験者と情報共有して、軽微なインシデントの原因となる不安全行動や状態を未然に防ぐ

【発生確率が高く、影響が小さいリスクの対策】
一見、遠回りの対策に感じられるが、
重大なインシデント対策の一環

必要条件：

小さなインシデントであっても、現場から率先して報告を行う仕組み
インシデントの情報を分析・共有・活用する仕組み
自組織や対象システムにあったより効果的な対策の模索