2009年度活動報告会

【調査研究部会】 セキュリティ被害調査WG

2009年 個人情報漏えいインシデント分析結果報告
～潜在している情報の漏えいや紛失の一端が明らかに～

富士通株式会社
佳山 こうせつ

2010年6月11日

セキュリティ被害調査WG メンバ

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
	猪俣	朗	トレンドマイクロ株式会社
	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
	菊谷	広	ドコモ・システムズ株式会社
	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
	佐藤	康彦	マイクロソフト株式会社
	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
	馬鳥	雄也	日本オラクル株式会社
	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	株式会社ラック
	やすだ	なお	株式会社ディアイティ/JNSA事務局

セキュリティ被害調査WG

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

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

報告内容

2009年 個人情報漏えいインシデントの分析結果の報告

- 2009年 個人情報漏えいインシデント
- 2009年 インシデント・トップ10
- 業種別、原因別、媒体別
- 漏えい件数と漏えい人数
- 想定損害賠償総額と漏えい件数
- 一件あたりの想定損害賠償額
- 現状から見える対策の特徴点
- 2009年情報漏えいインシデントの総括

2010年 活動計画

『2009年 情報セキュリティインシデントに関する調査報告書』は、近日公開予定です。

2009年 個人情報漏えいインシデント

漏えい人数	過去最少 573万5,673人
漏えい件数	過去最高 1,539件
想定損害賠償総額	3,894億1,144万円
一件当たりの漏えい人数	3,934人
一件当たり平均想定損害賠償額	2億6,709万円
一人当たり平均想定損害賠償額	4万9,961円

$$\frac{\text{573万5,673人}}{\text{1億2,751万5,000人}} = \text{約22人に1人の割合}$$

一日平均4.2件

2008年
18人に1人
3.8件/日

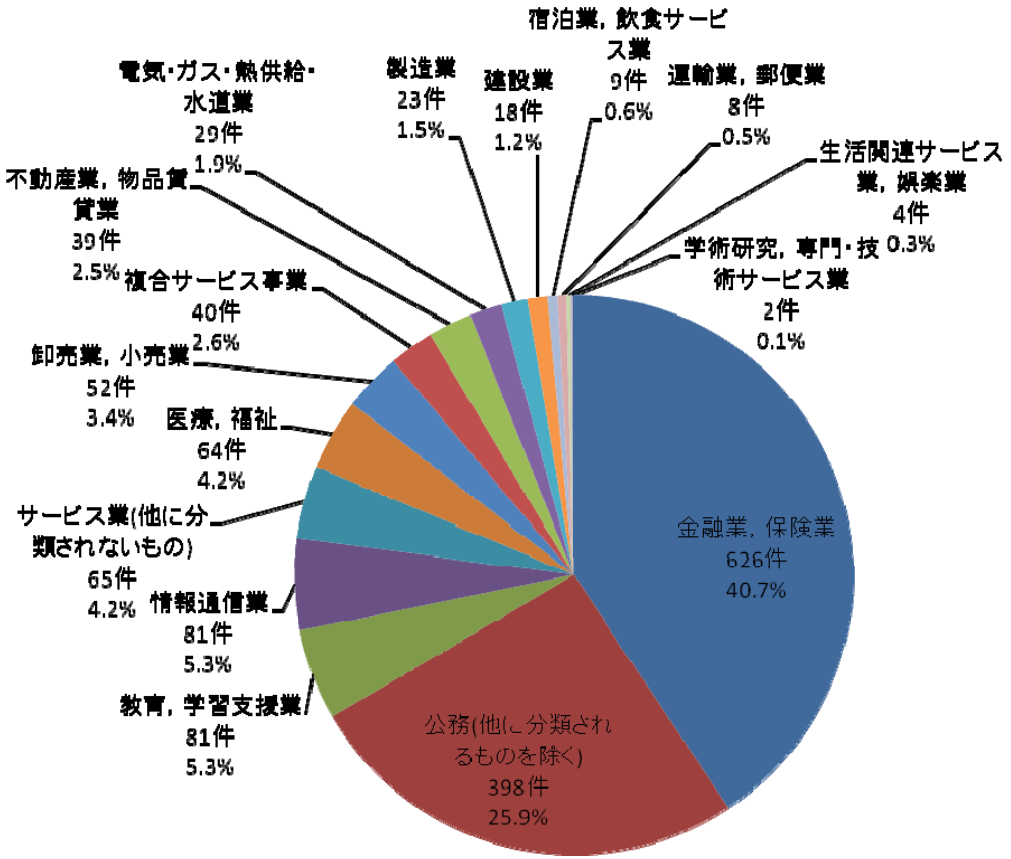
2009年 インシデント・トップ10

No.	漏えい人数	業種	原因
1	148万6651人	金融業，保険業	内部犯罪・内部不正行為
2	50万人	金融業，保険業	管理ミス
3	43万5990人	電気・ガス・熱供給・水道業	管理ミス
4	35万3605人	情報通信業	目的外使用
5	27万3000人	公務（他に分類されるものを除く）	管理ミス
6	19万4294人	サービス業（他に分類されないもの）	不正アクセス
7	15万0783人	卸売業，小売業	不正アクセス
8	14万8680人	サービス業（他に分類されないもの）	不正アクセス
9	14万0151人	金融業，保険業	管理ミス
10	14万0000人	公務（他に分類されるものを除く）	内部犯罪・内部不正行為

2009年は、金融、公務、サービス業が多い

2009年の原因にはばらつき

① 業種別の漏えい件数

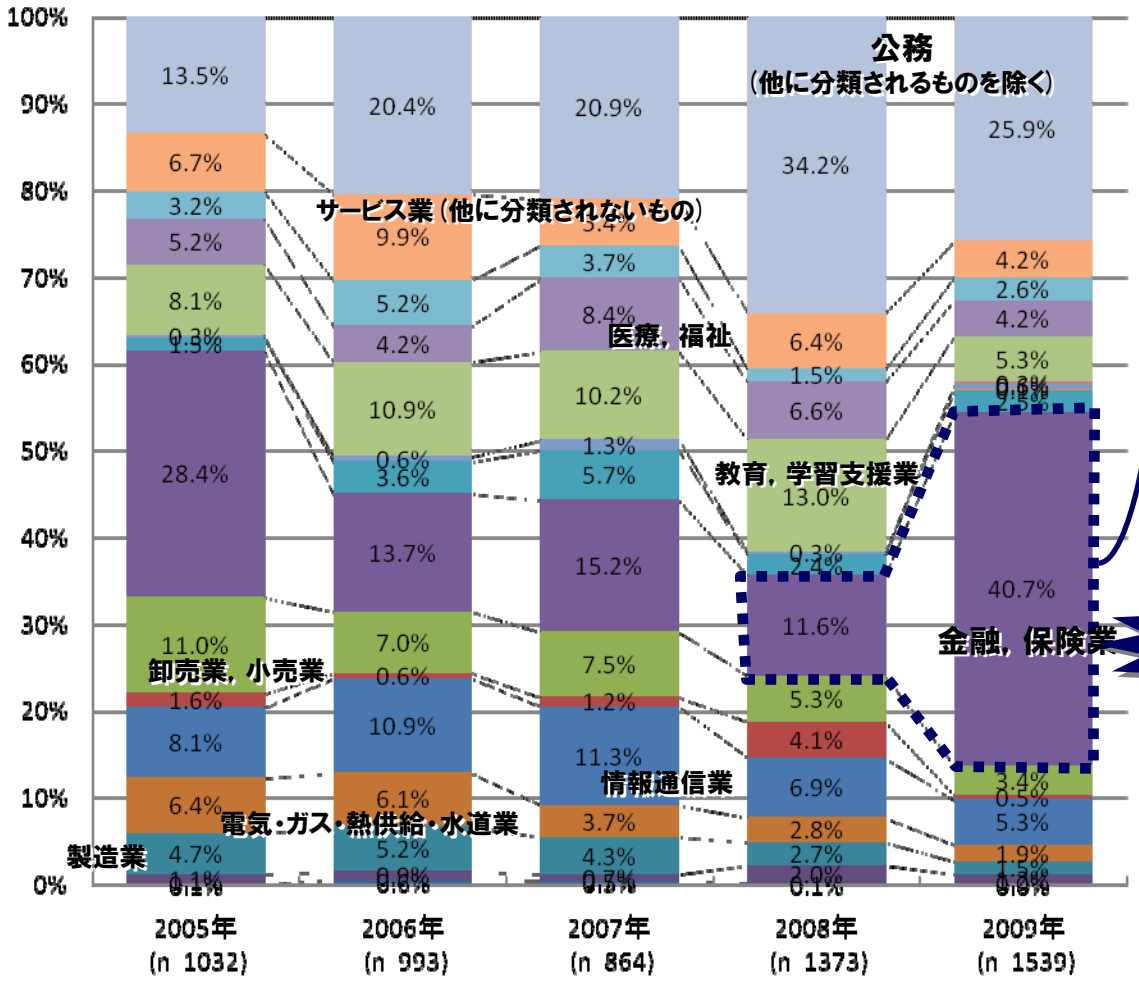


2008年	2009年
公務（469件）	金融・保険業（622件）
教育・学習支援業（178件）	公務（398件）
金融・保険業（159件）	教育・学習支援業（81件）
情報通信業（95件）	情報通信業（81件）

金融・保険業が突出して増加

漏えい件数が多い上位4業種は同じ

① 業種別の漏えい件数(経年)



漏えい件数が大幅に増加

金融、保険業(159件→622件)

↕

他の業種の比率および件数が減少傾向に見える

公務	(469件→398件)
教育学習支援	(178件→ 81件)
情報通信業	(95件→ 81件)
卸売業、小売業	(73件→ 52件)

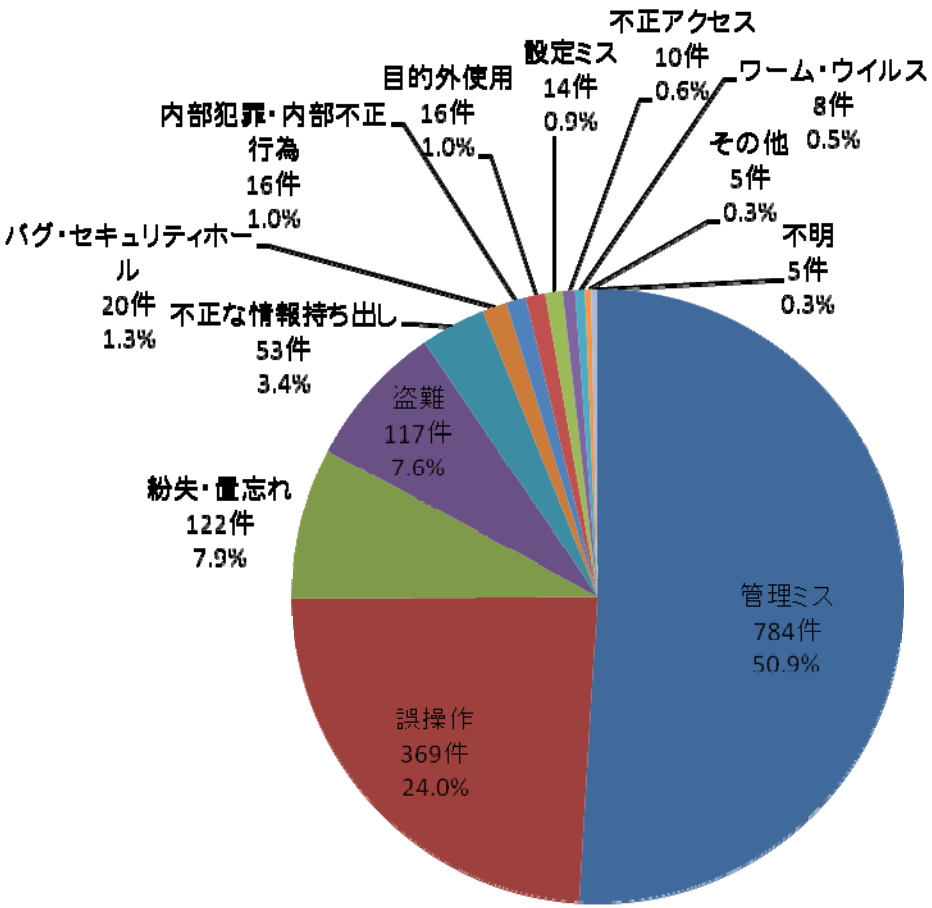
特徴点

全体的に減少しているが、金融保険業の増加が大きく影響している

2008年＝1373件　2009年＝1539件

※毎年のことだが、鉱業，採石業，砂利採取業および漁業は0件

② 原因別の漏えい件数

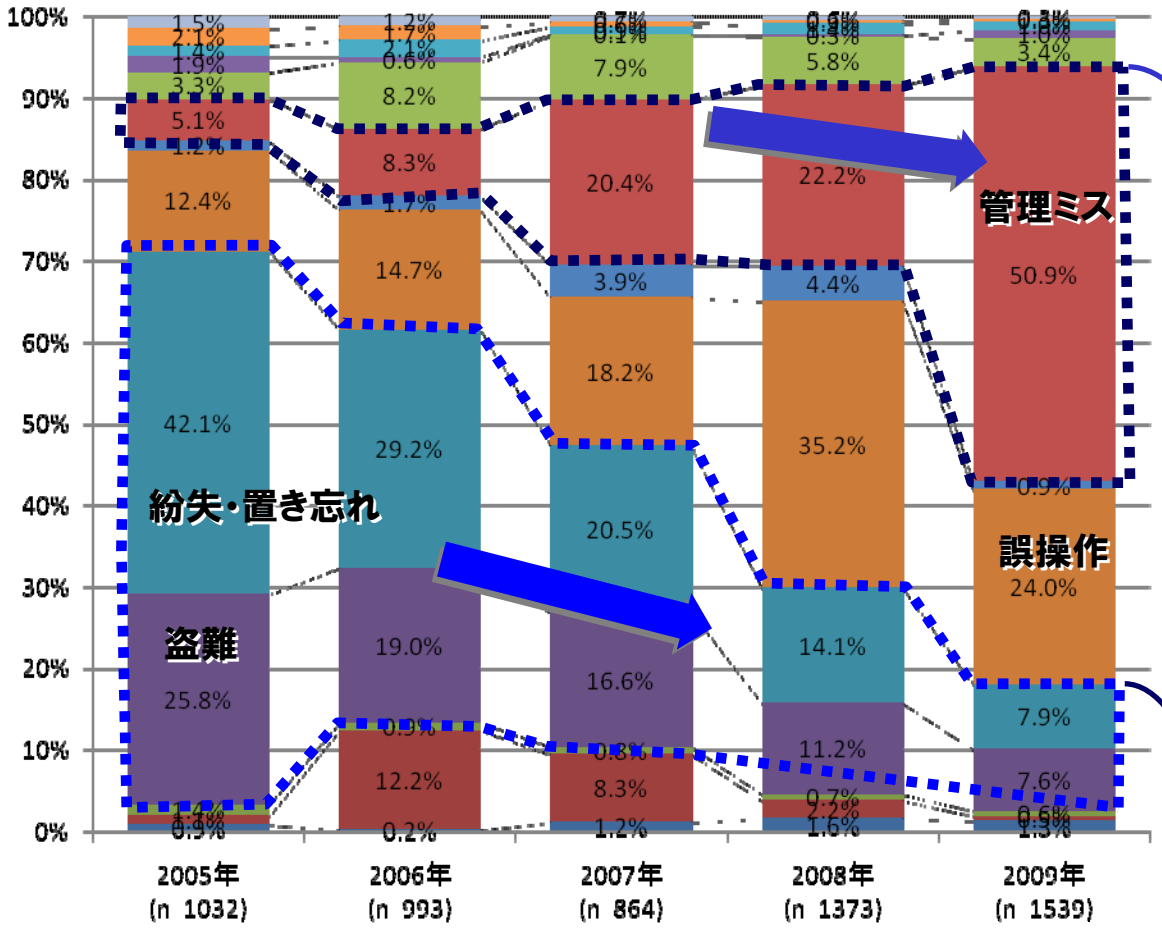


2008年		2009年
誤操作（483件）	↗	管理ミス（784件）
管理ミス（305件）	↘	誤操作（369件）
紛失・置忘れ（194件）	→	紛失・置忘れ（122件）
盗難（154件）	→	盗難（117件）

特徴点

管理ミス＝組織内紛失によるインシデントが増加

② 原因別の漏えい件数(経年)



特徴点

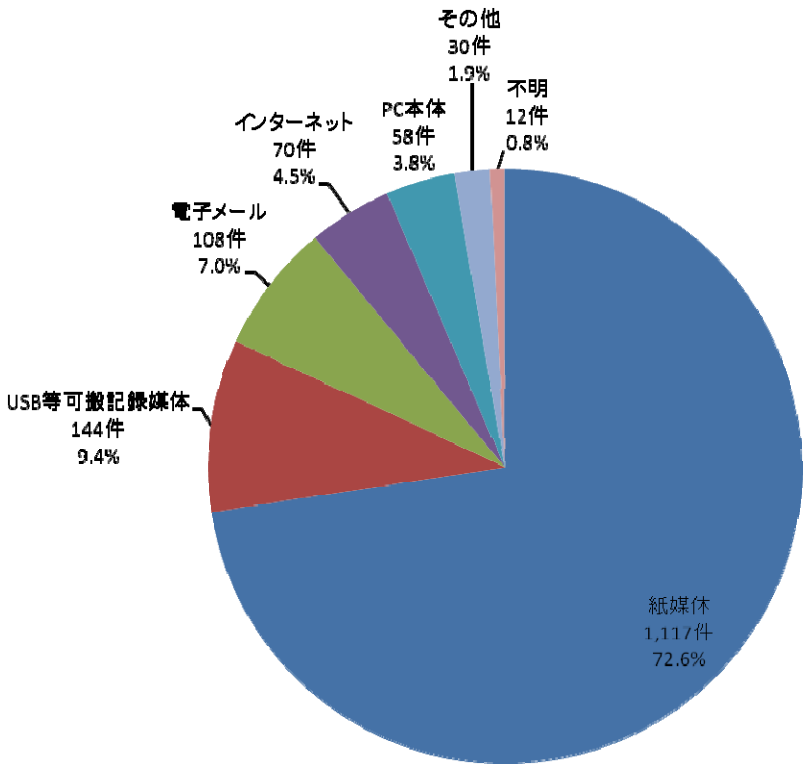
◎管理ミスの比率が増加

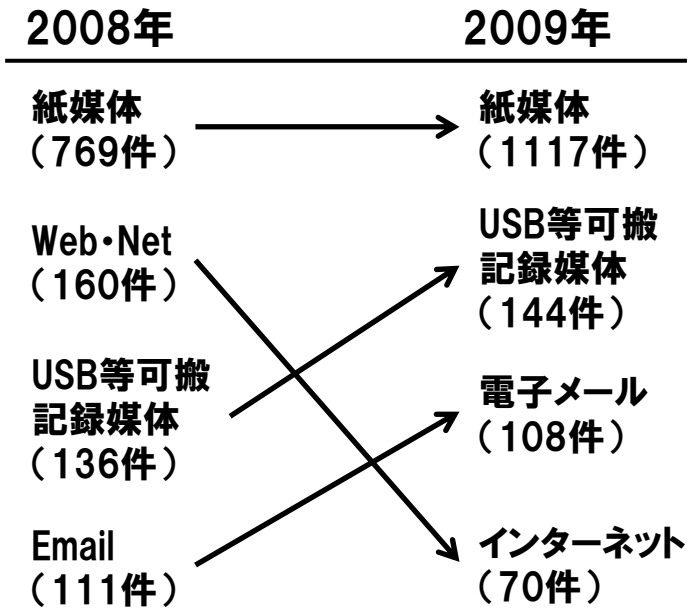
監査や組織内統制の強化に伴い
誤廃棄や紛失が判明

紛失・置き忘れ、盗難が減少傾向

不必要な情報の持ち運びが減少していることが要因と推察する

③ 媒体別の漏えい件数

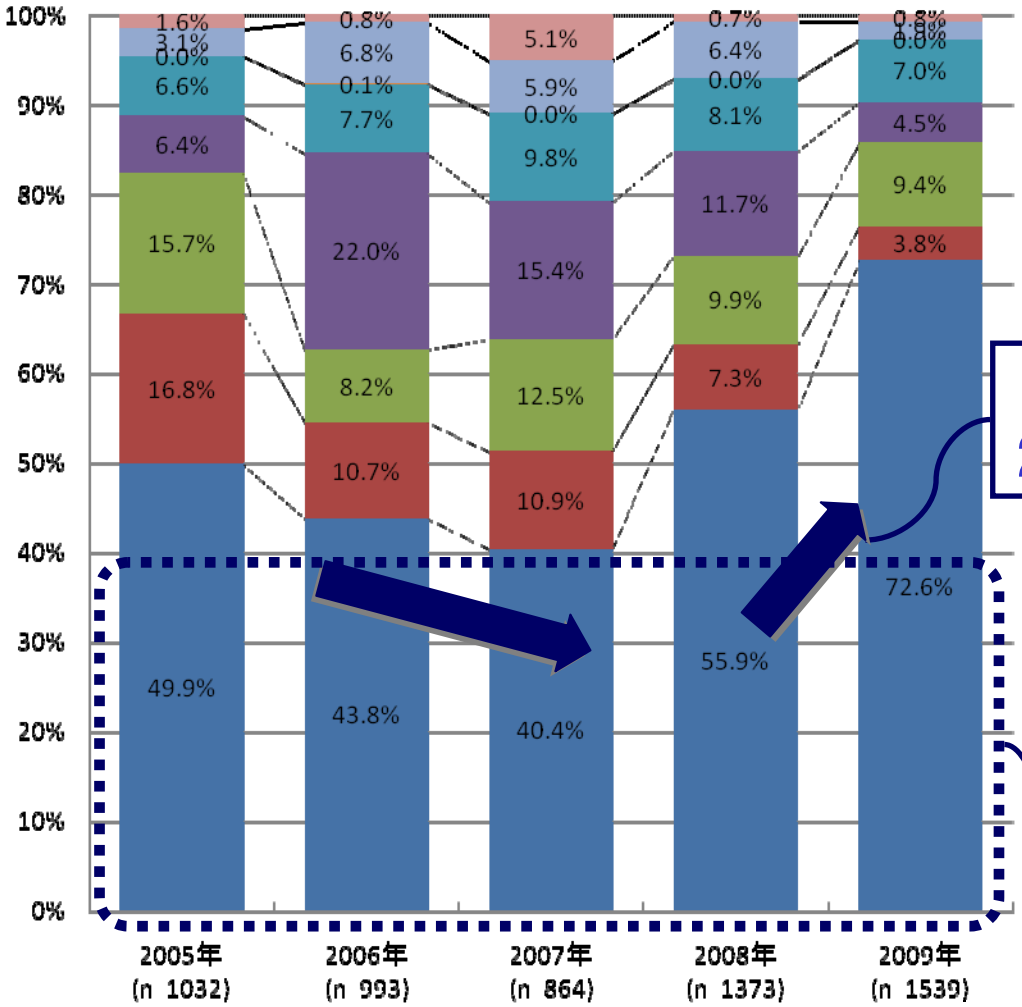




【ご注意】
今年から以下の用語が変更になりました。
Web・Net ⇒ インターネット
Email ⇒ 電子メール

あいかわらず紙媒体による漏えいが多い
件数が大きく増加

③ 媒体別の漏えい件数(経年)

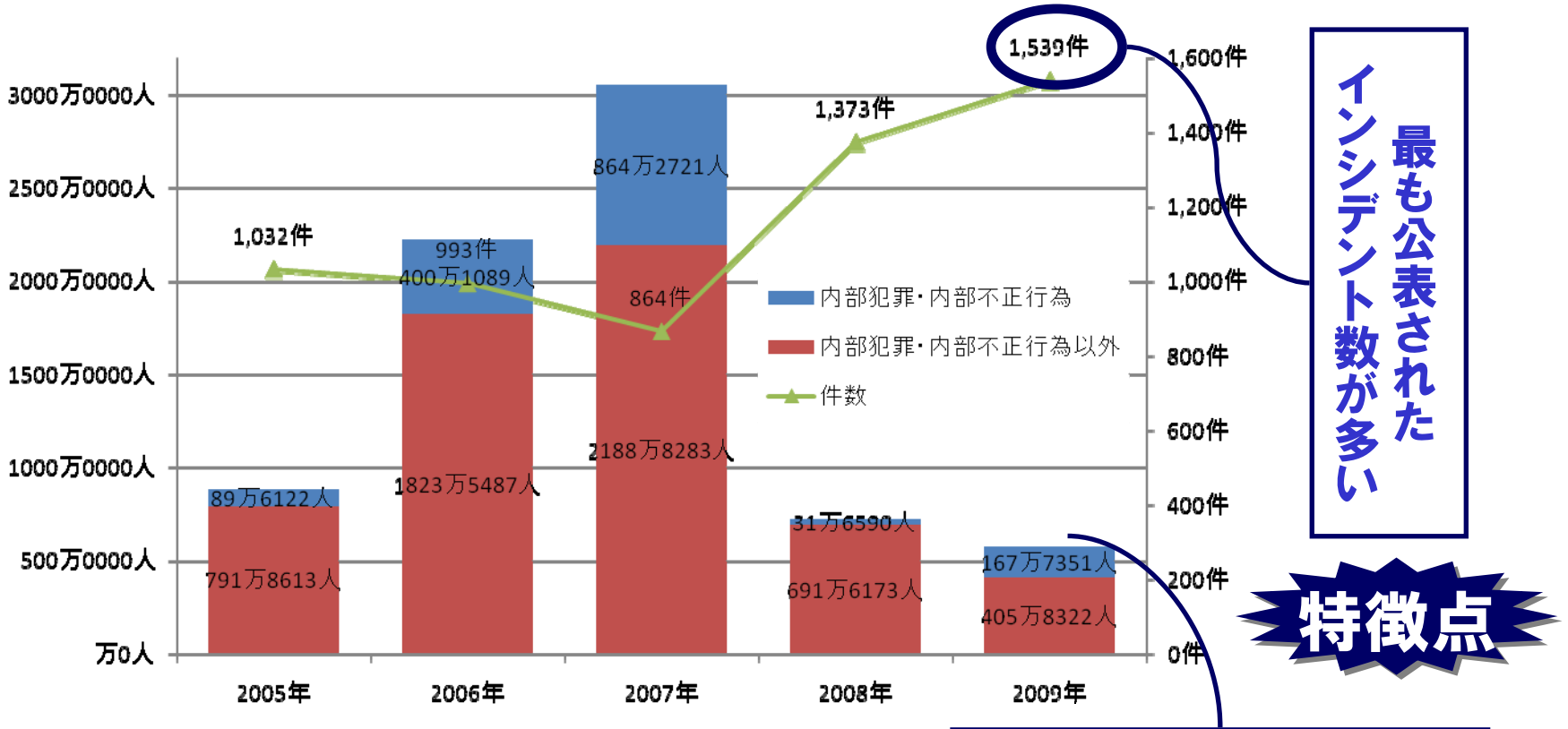


誤操作、管理ミスの
増加傾向と相関がある

紙媒体による漏えいが
2008年に引き続き増加傾向

相変わらず紙媒体による
漏えいが多い

④ 漏えい件数と漏えい人数(経年)



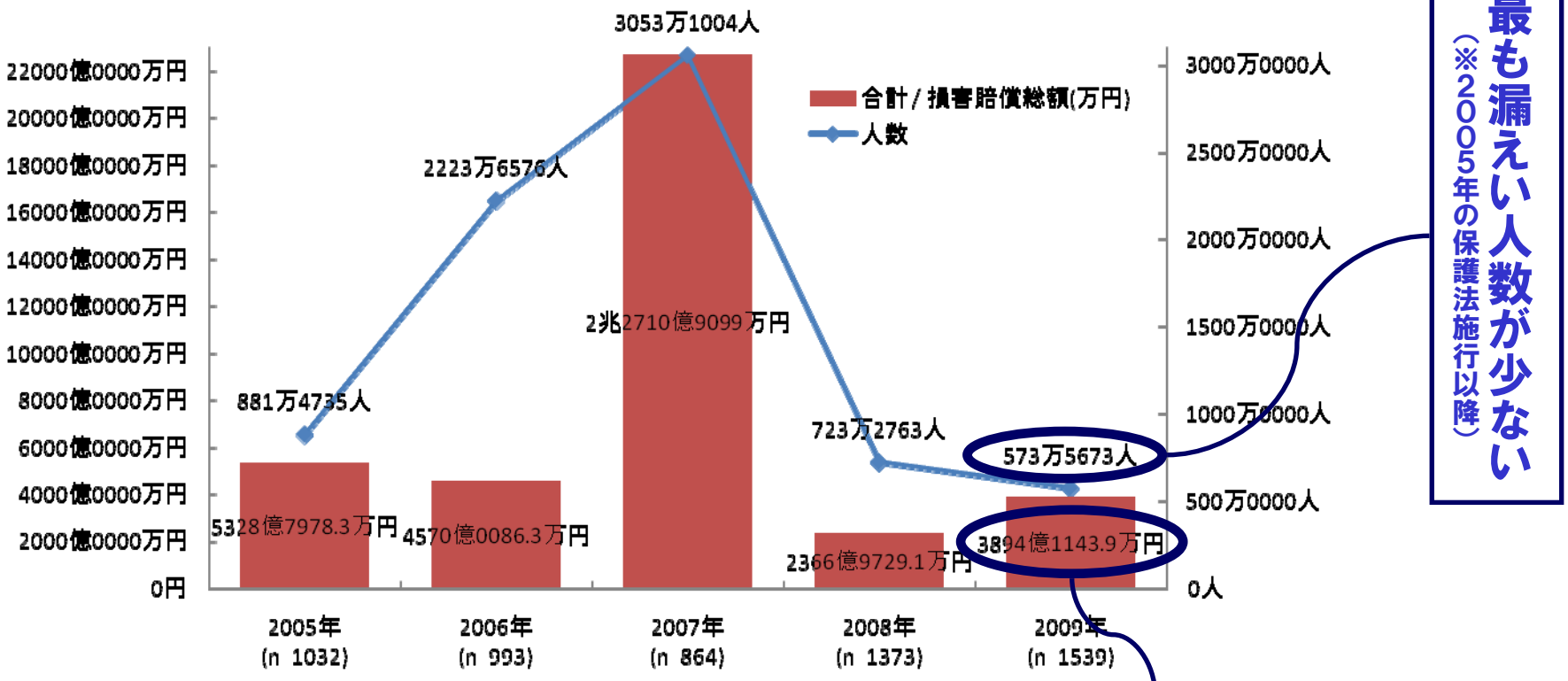
最も公表されたインシデント数が多い

特徴点

最も漏えい人数が少ない
(※2005年の保護法施行以降)

◎10万人以上の大規模なインシデントが減少したため

⑤ 想定損害賠償総額と漏えい件数(経年)



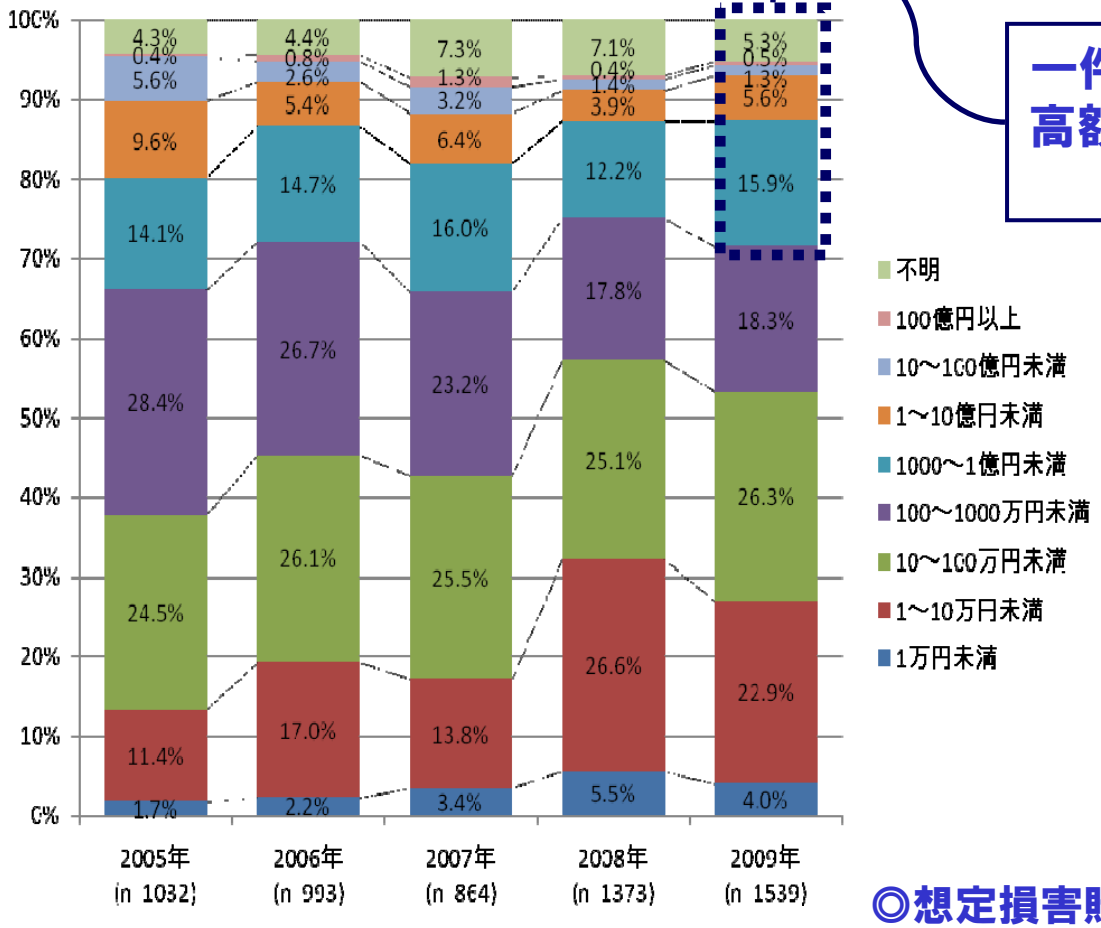
最も漏えい人数が少ない
(※2005年の保護法施行以降)

特徴点

人数減に対して想定損害賠償総額が増加
(※2008年との比較)

◎想定損害賠償総額を押し上げる要因である
経済的損失レベルが高いインシデントが増加したため

⑥ 一件あたりの想定損害賠償額(経年)



一件あたりの想定損害賠償額が高額な漏えいインシデントの比率は増加に転じた

1,000万円以上の漏えい件数は、2006年以降、ほぼ横ばい(約300件)であったが、2009年は439件に増加

想定損害賠償総額が1,000万円以上
‖
機微な個人情報の取り扱う場合

◎想定損害賠償総額を押し上げる要因である経済的損失レベルが高いインシデントが増加したため

⑦ 現状から見える2009年の特徴点

特徴点 業種ごとで見ると、金融・保険業でのインシデントが大幅に増加

⇒特に、地方銀行や地方の支店などによる一括公表が多かった

特徴点 管理ミス（組織内紛失）によるインシデントが増加

⇒保管義務のある顧客文書の組織内紛失が目立った

特徴点 最も公表されたインシデント数が多く、最も漏えい人数が少ない（※2005年の保護法施行以降）

⇒小規模の事故でもしっかり公表する動きが活性化

特徴点 想定損害賠償総額が増加している（※2008年との比較）

⇒口座番号などの、機微情報が多く含まれていた

金融検査の強化がされた影響が数字に現れてた

2009年情報漏えいインシデントの総括

■ 金融保険業以外の業種の情報漏えい事故/大規模な事故は減少

情報漏えい事故に対する対策と教育の浸透による効果が出ているのではないかと考えられる。ただし、公にされていないインシデントもあるはず。

■ 金融保険業界の情報漏えい事故を教訓に金融庁が監督を強化

組織内で個人情報の管理状況を再度確認したところ、実は紛失していたことが判明し、公表に至っている。

⇒情報漏えい事故に対する対策が進む一方で、潜在している情報の漏えいや紛失の一端が明らかになった。

金融保険業界がセキュリティ対策に遅れを取っているのではなく、むしろ対策をしっかり行おうという動きが読み取れる。

管理をしっかりやろうとしている金融・保険業界だからこそ潜在する情報漏えい事故を把握することができ、公表できた

⇒「漏えいを公表している組織＝管理が甘い組織」とは一概に言えない。

いま一度、潜在する管理ミスの把握と管理の徹底の確認が必要

潜在リスクの把握は、被害調査の統計データだけでは限界か？

2010年 活動計画

【主な活動内容】

■2010年 個人情報漏えいインシデントの調査、報告書の作成

■インシデント発生確率調査

これまでの調査だけでは、管理が徹底されている組織も、管理に不備があり情報が漏れていることすら把握できていない組織（公表しない組織）も、同等にインシデント0件となっている。そのため、特定の省庁に監督されている業種しか、把握できず、全体の把握には至っていない。

そこで当WGでは、ハインリッヒの法則や歩留まり・バグ発生率と同様の考え方で一定の発生確率が求められるのではないかという仮説のもと、**組織の対策の徹底度合いとインシデントの発生確率**の調査・分析活動を行っていく予定である。うまくいけば、**対策の定量化**に繋げていきたい。

【年間活動予定】

6月 2009年 情報セキュリティインシデントに関する調査報告書の公開

7月 新しいインシデント発生確率調査の検討、調査活動の開始

11月 2010年 情報セキュリティインシデントに関する調査報告書 集計速報（2010年前半）の公開

もし、セキュリティ被害の推定などで、困っていること、WGへの要望などがありましたら、アンケート用紙へご記入ください。

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