

Network Security Forum 2014

【A3 講演】

個人情報漏えいインシデントの 調査結果に基づく 最近のインシデント傾向について

大谷 尚通 (株)NTTデータ

2014年 1月29日

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

- 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
- 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、報告書を公開

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

2012年 情報セキュリティ インシデントに関する調査 ～個人情報漏えい編～

**共同調査： 情報セキュリティ大学院大学
原田研究室、廣松研究室**

1. 2012年 個人情報漏えいインシデント①

期間:2012年1月1～12月31日(※12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

	2012年データ
漏えい人数	972万65人
漏えい件数	2357件
想定損害賠償総額	2132億6405万円
一件当たりの漏えい人数	4245人
一件当たり平均想定損害賠償額	9313万円
一人当たり平均想定損害賠償額	4万4628円

1. 2012年 個人情報漏えいインシデント③

期間:2012年1月1～12月31日(※12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

	2012年データ	2011年データ (2012年比較)
漏えい人数	972万65人	628万4363人 (+343万5702人)
漏えい件数	2357件	1551件 (+806件)
想定損害賠償総額	2132億6405万円	1899億7379万円 (+232億9026万円)
一件当たりの漏えい人数	4245人	4238人 (+7人)
一件当たり平均想定損害賠償額	9313万円	1億2,810万円 (-3497万円)
一人当たり平均想定損害賠償額	4万4628円	4万8533円 (-3905円)

2. 2012年 インシデント・トップ10

No.	漏えい人数	業種	原因
1	76万0000人	情報通信業	設定ミス
2	40万6632人	金融業, 保険業	管理ミス
3	17万1518人	情報通信業	不正アクセス
4	12万4471人	金融業, 保険業	管理ミス
5	12万1191人	公務(他に分類されるものを除く)	不正な情報持ち出し
6	11万0000人	サービス業(他に分類されないもの)	不正アクセス
7	10万0000人	金融業, 保険業	管理ミス
8	9万6000人	金融業, 保険業	管理ミス
9	9万5689人	製造業	内部犯罪・内部不正行為
10	8万0000人	運輸業, 郵便業	管理ミス

金融業が
やや多い。

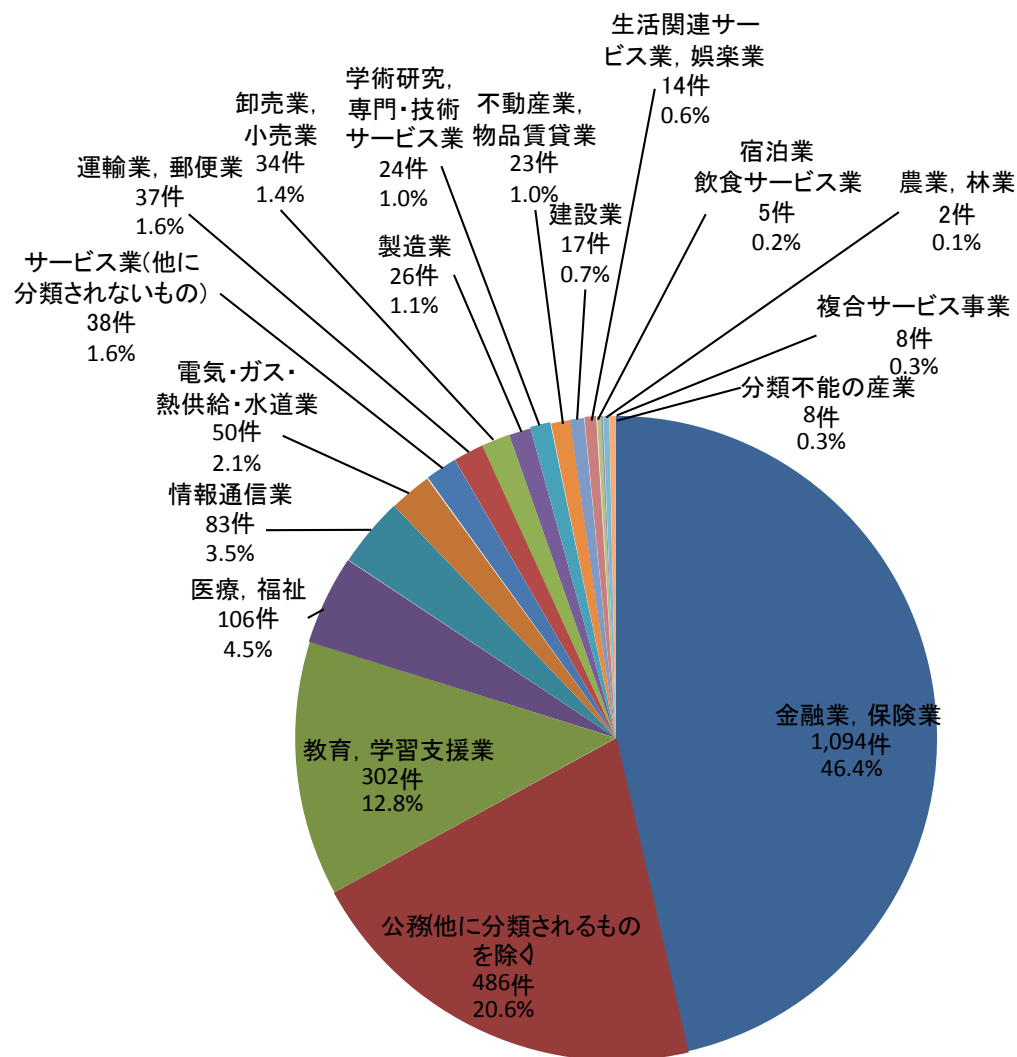
2007年以降、
管理ミスが多い

組織内の情報管理の強化
(内部統制対応)

数年特徴に変化なし

◎近年は、100万人を超える大規模なインシデントの発生が無い

3.1 業種別の漏えい件数①



2011年
(N=1551件)

2012年
(N=2357件)

公務
(516件)

金融業, 保険業
(1094件)

金融業, 保険業
(332件)

公務
(486件)

教育, 学習支援業
(216件)

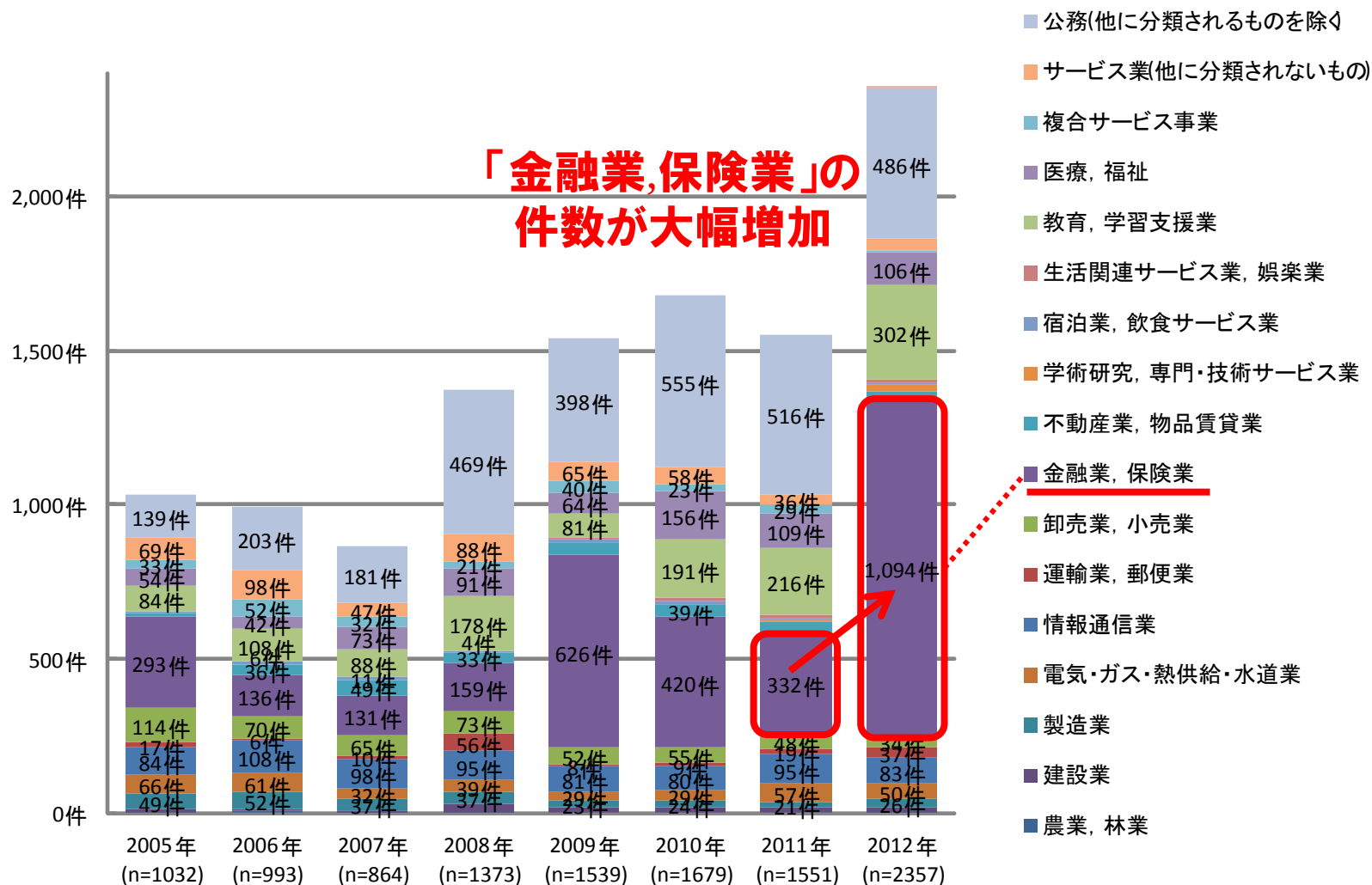
教育, 学習支援業
(302件)

医療, 福祉
(109件)

医療, 福祉
(106件)

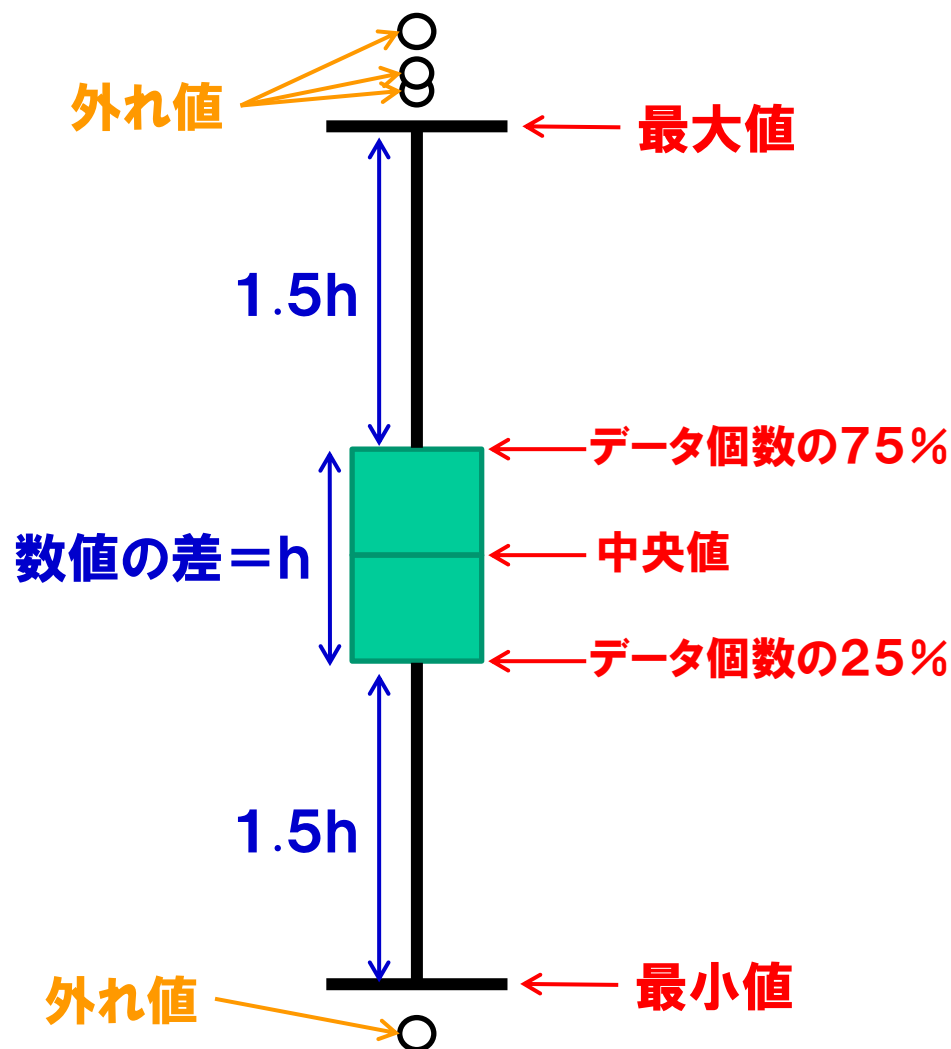
例年、上位4業種は同じ

3.1 業種別の漏えい件数(経年)②

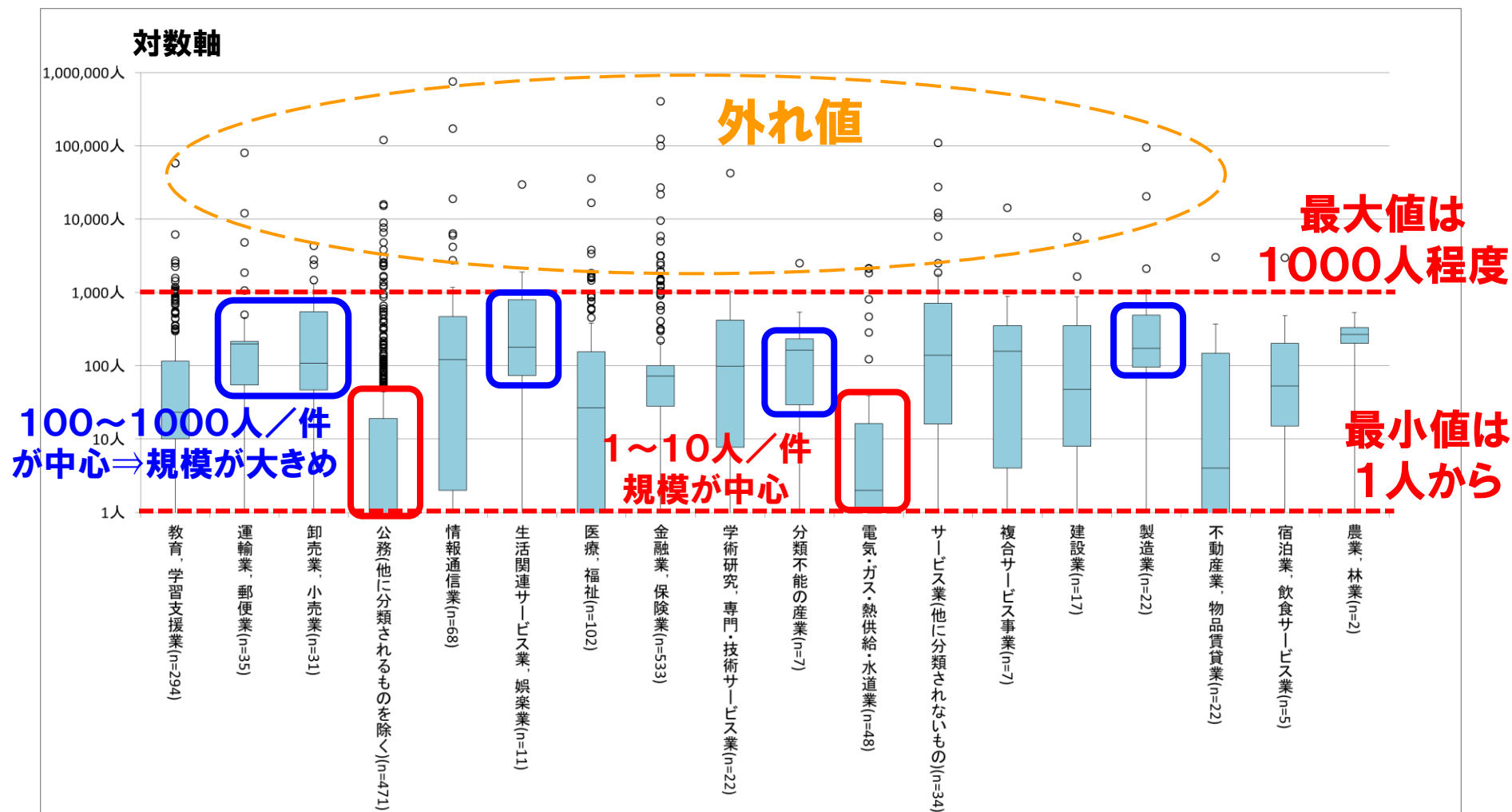


参考：箱ひげ図

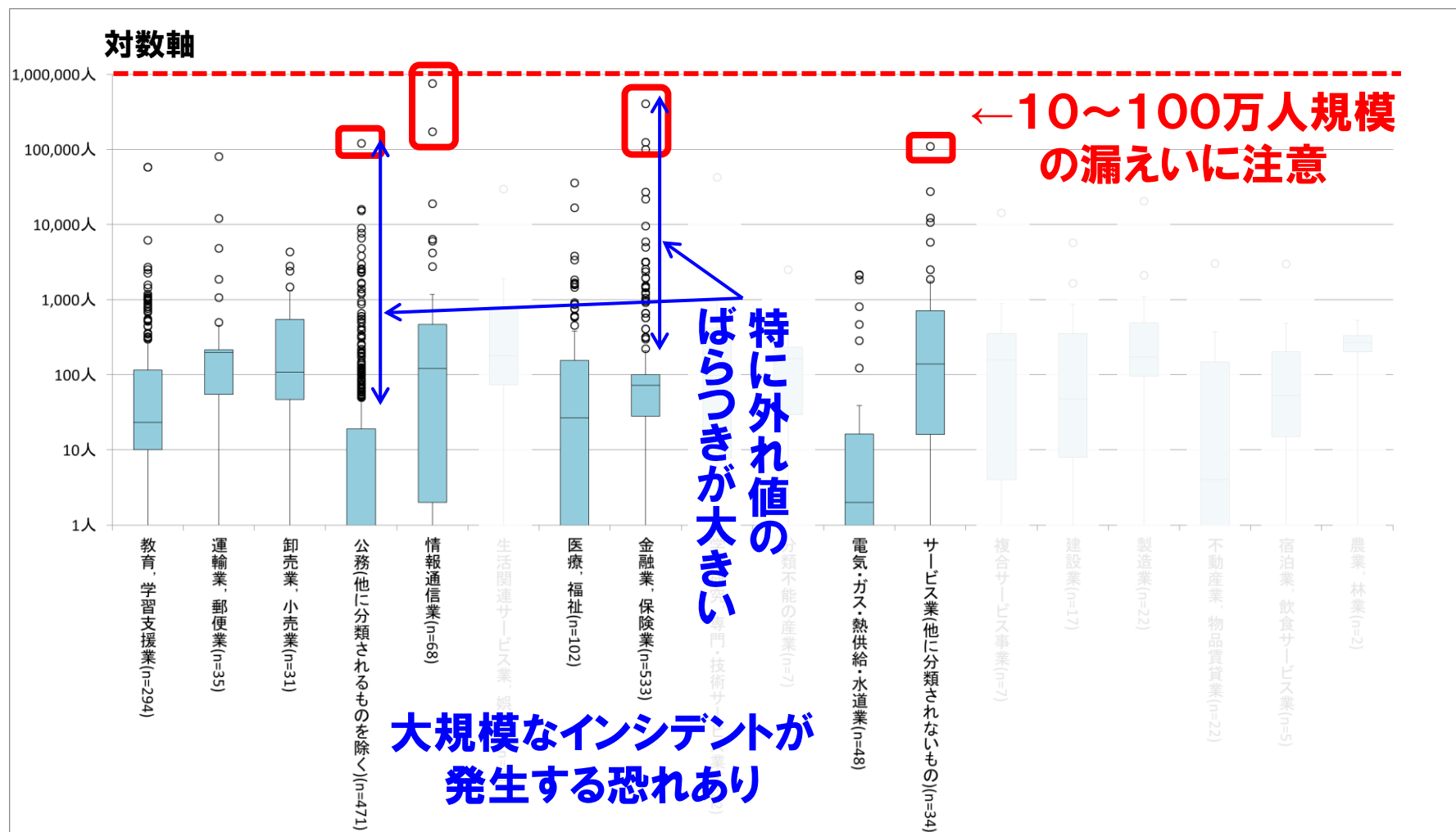
ばらつきのあるデータをわかりやすく表現するための統計学的グラフ



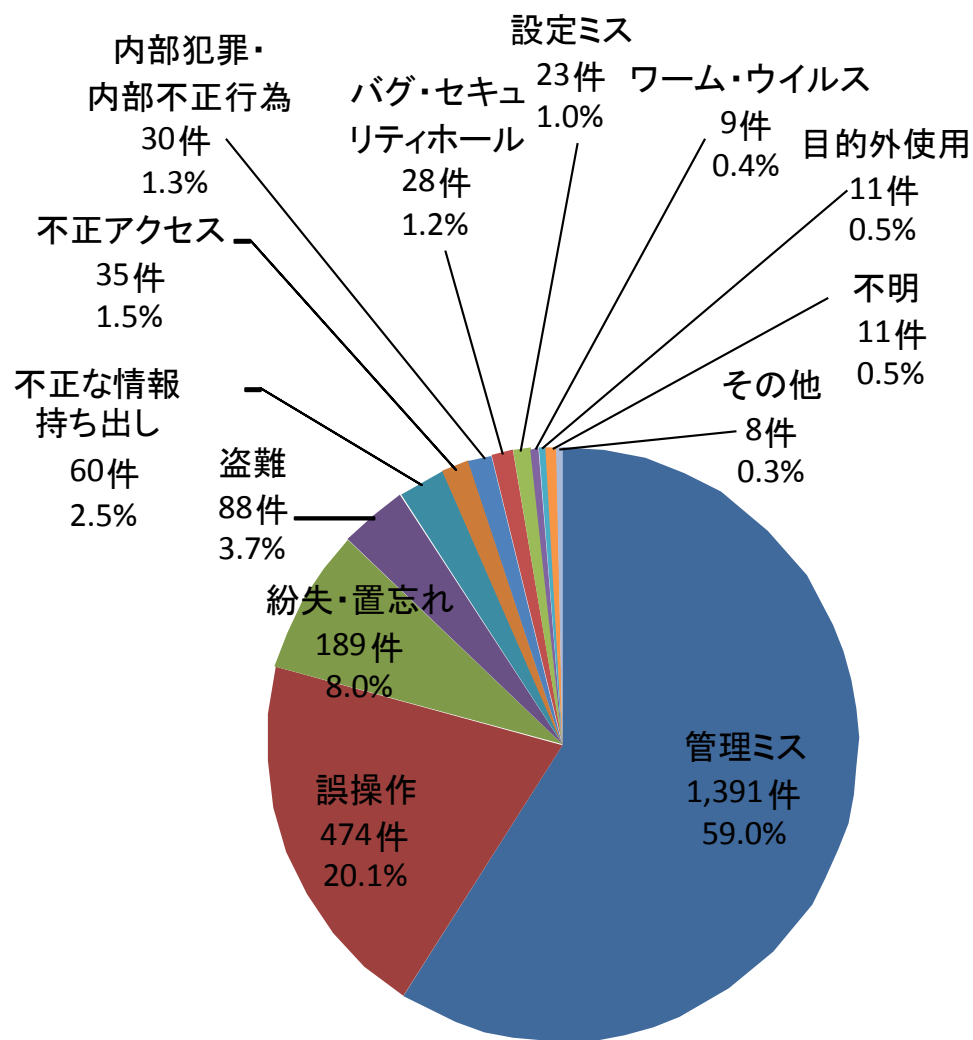
3.1 業種別の漏えい件数③ (箱ひげ図)



3.1 業種別の漏えい件数④ (箱ひげ図)



3.2 原因別の漏えい件数①



2011年
(N=1551件)

2012年
(N=2357件)

誤操作
(539件)

管理ミス
(1391件)

管理ミス
(497件)

誤操作
(474件)

紛失・置忘れ
(213件)

紛失・置忘れ
(189件)

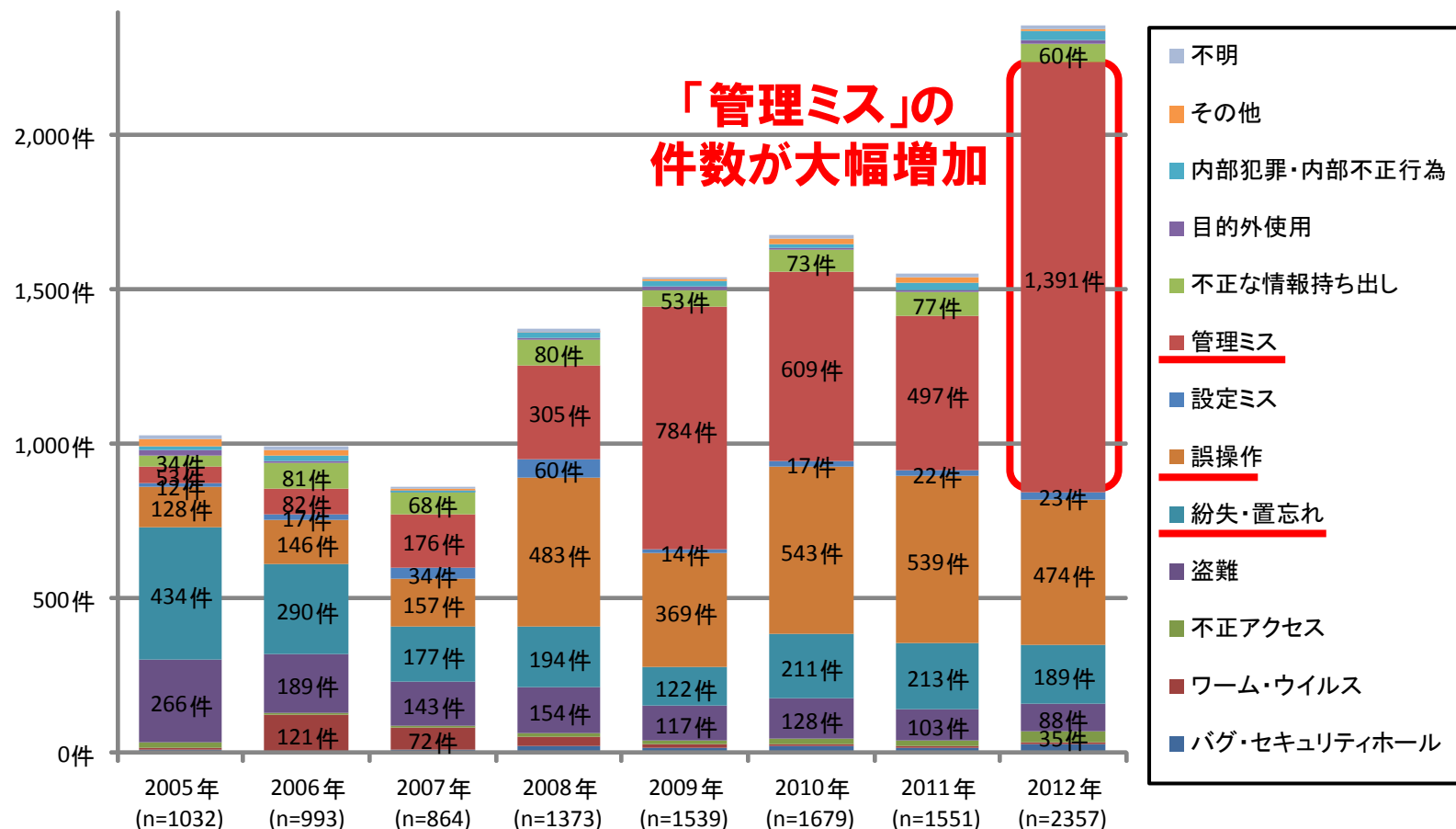
盗難
(103件)

盗難
(88件)

管理ミスが増加

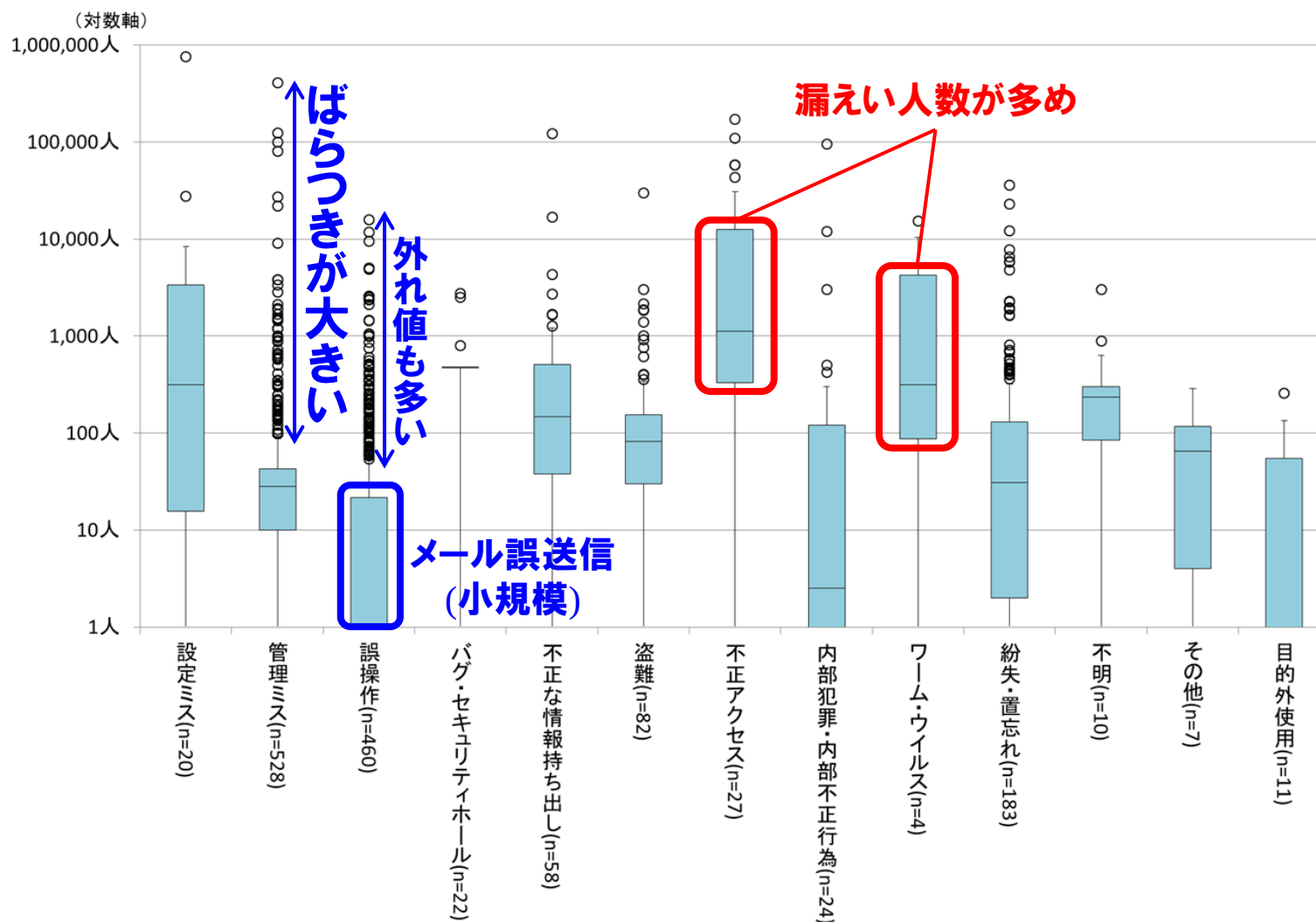
**管理ミス(=誤廃棄)
誤操作(=ケアレスミス)
による漏えいが多い**

3.1 業種別の漏えい件数(経年)②

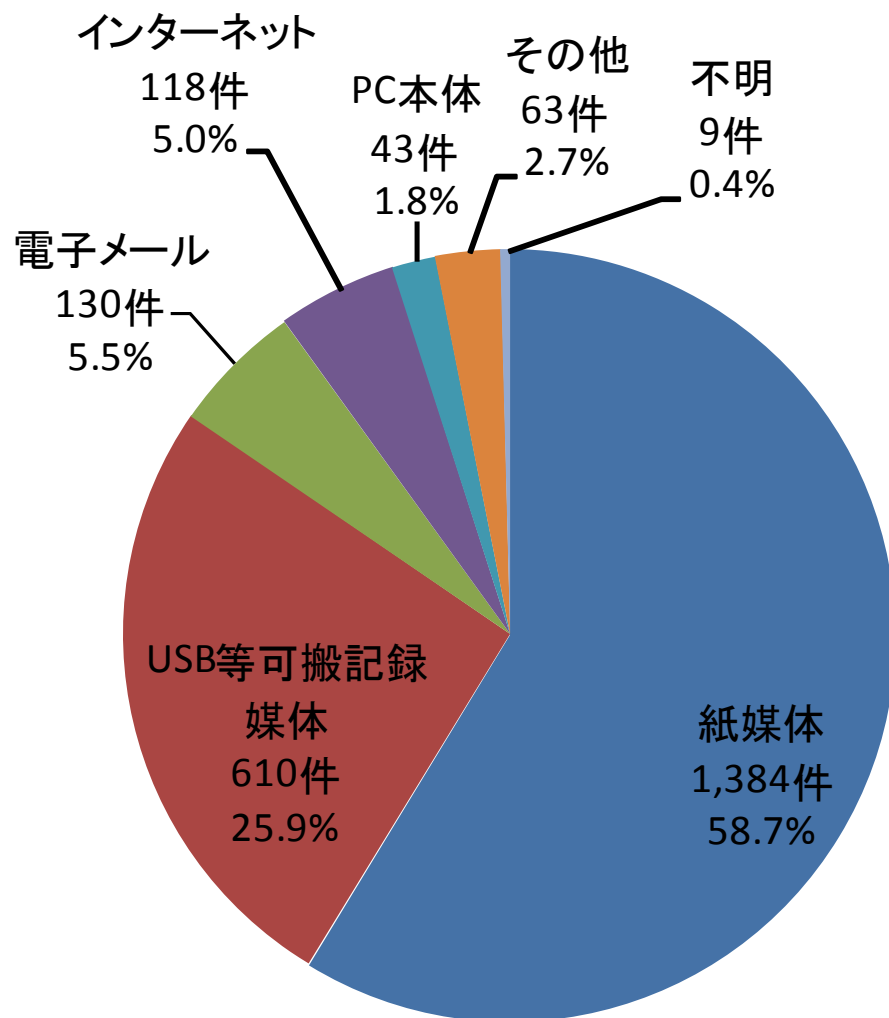


「管理ミス」「誤操作」「紛失・置き忘れ」の
ヒューマンエラー系のインシデントが3大要因

3.2 原因別の漏えい件数③ (箱ひげ図)



3.3 媒体別の漏えい件数



2011年
(N=1551件)

2012年
(N=2357件)

紙媒体
(1065件)

紙媒体
(1384件)

USB等可搬
記録媒体
(156件)

USB等可搬
記録媒体
(610件)

電子メール
(126件)

電子メール
(130件)

インターネット
(68件)

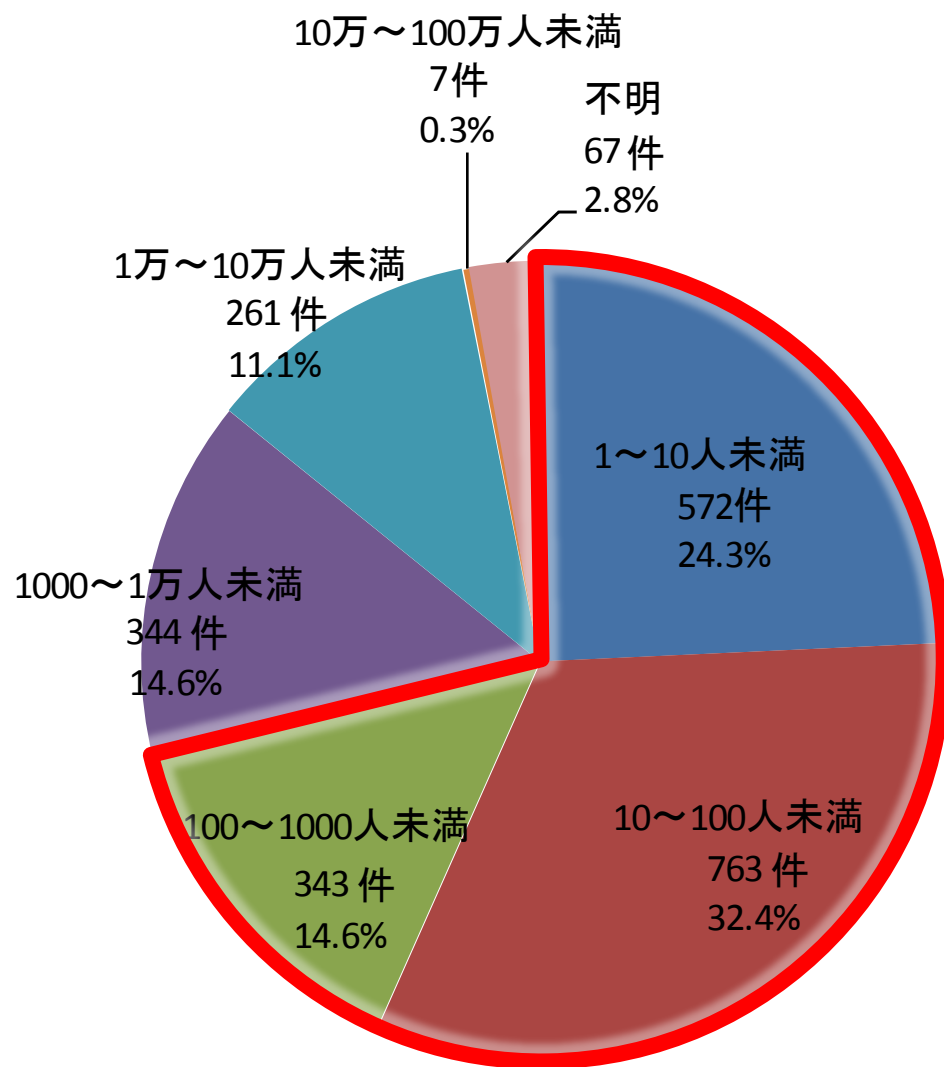
インターネット
(118件)

順位に変化なし

**紙媒体による漏えいが多い。
(例年通り)**

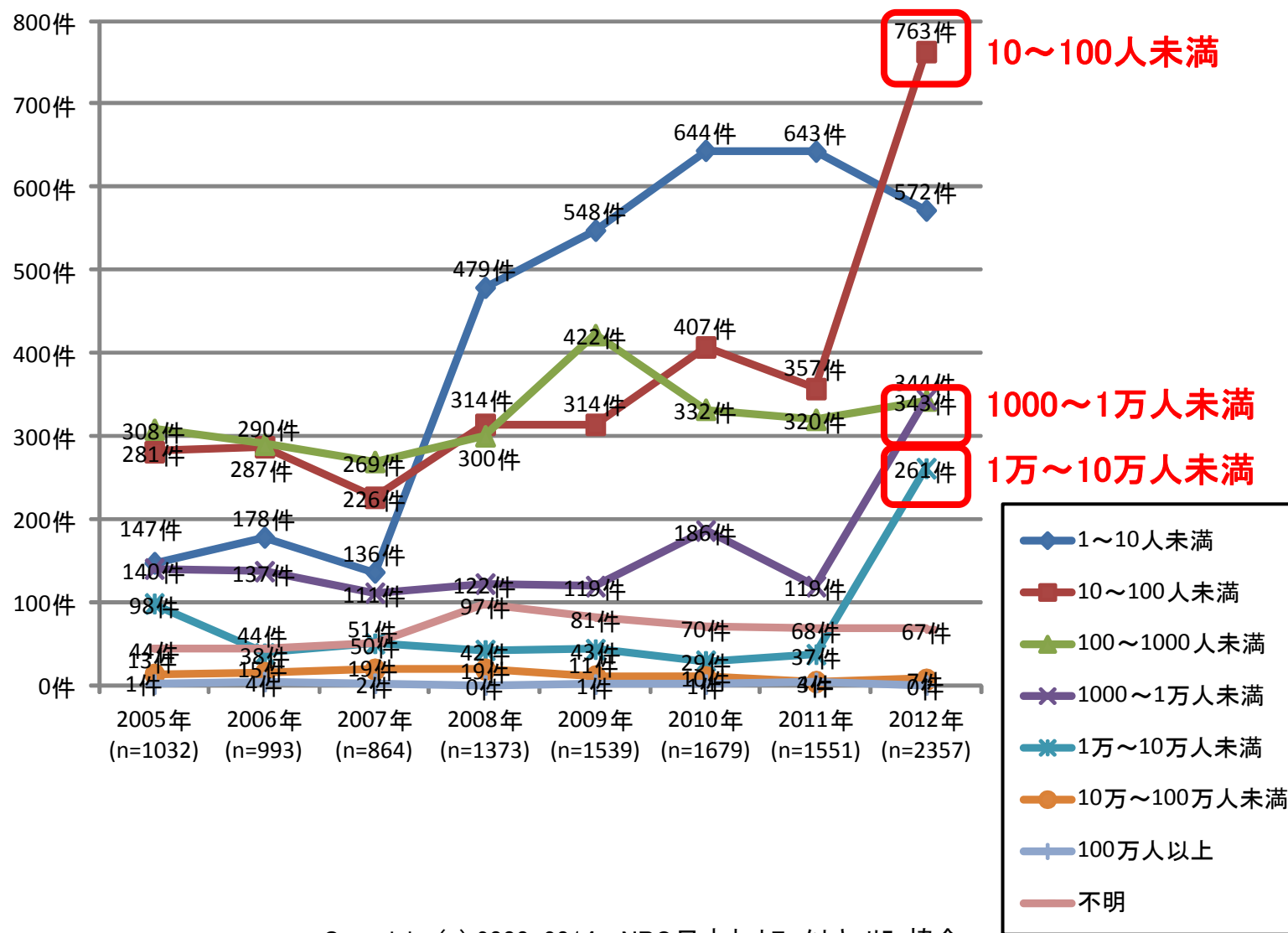
USBが増加

3.4 一件当たりの漏えい人数①

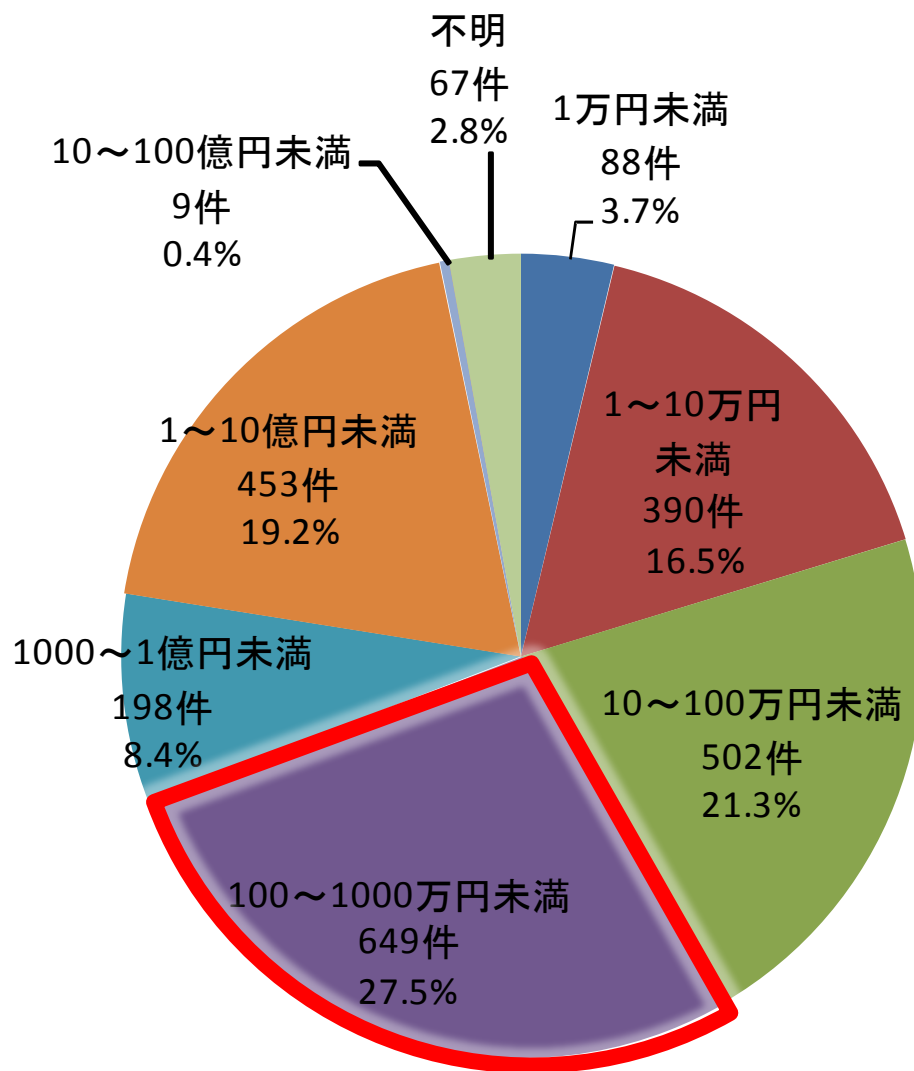


**1000人/件未満の
小さなインシデントの件数が
約70%を占める。**

3.4 一件当たりの漏えい人数(経年)②

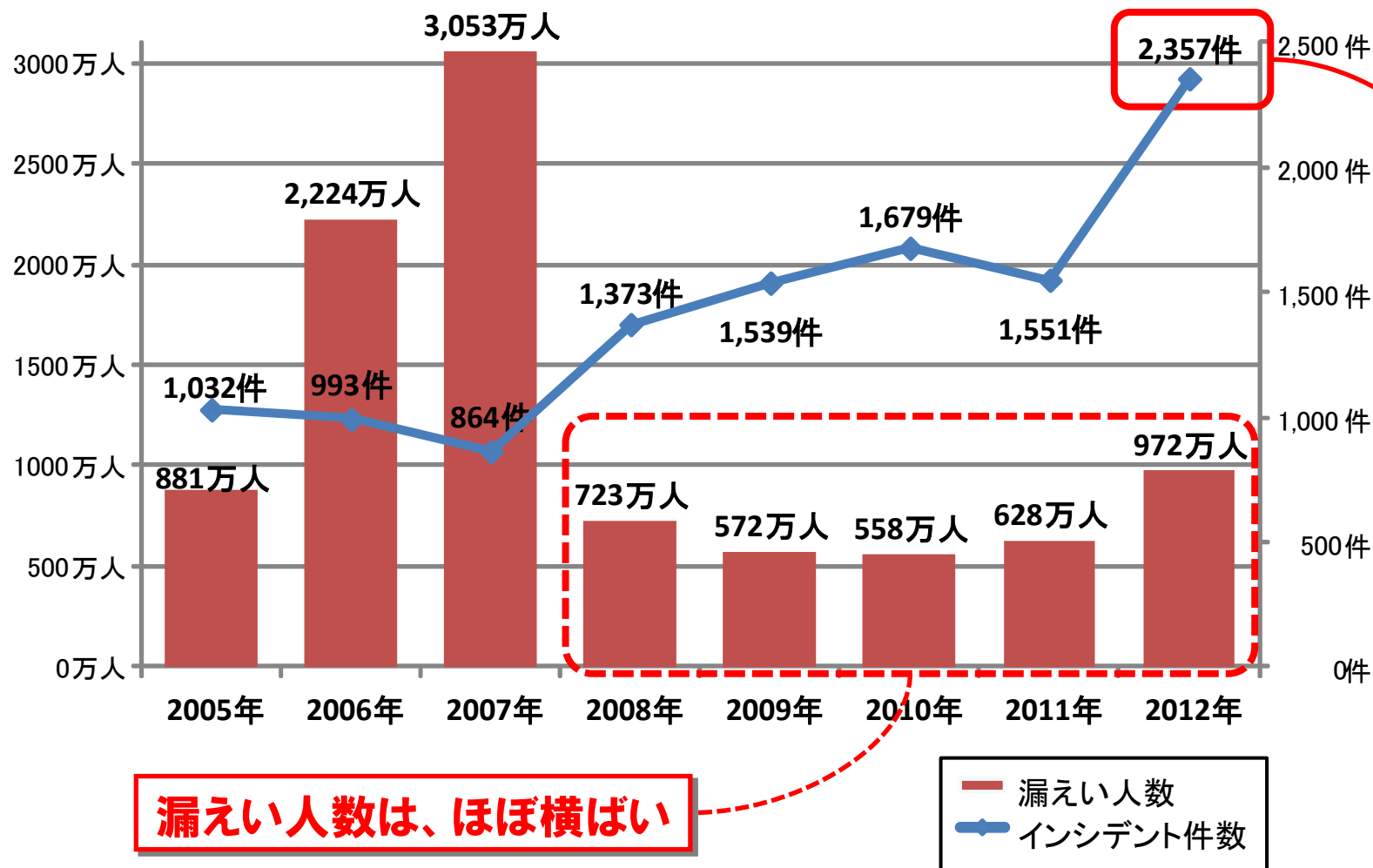


3.5 一件当たりの想定損害賠償額

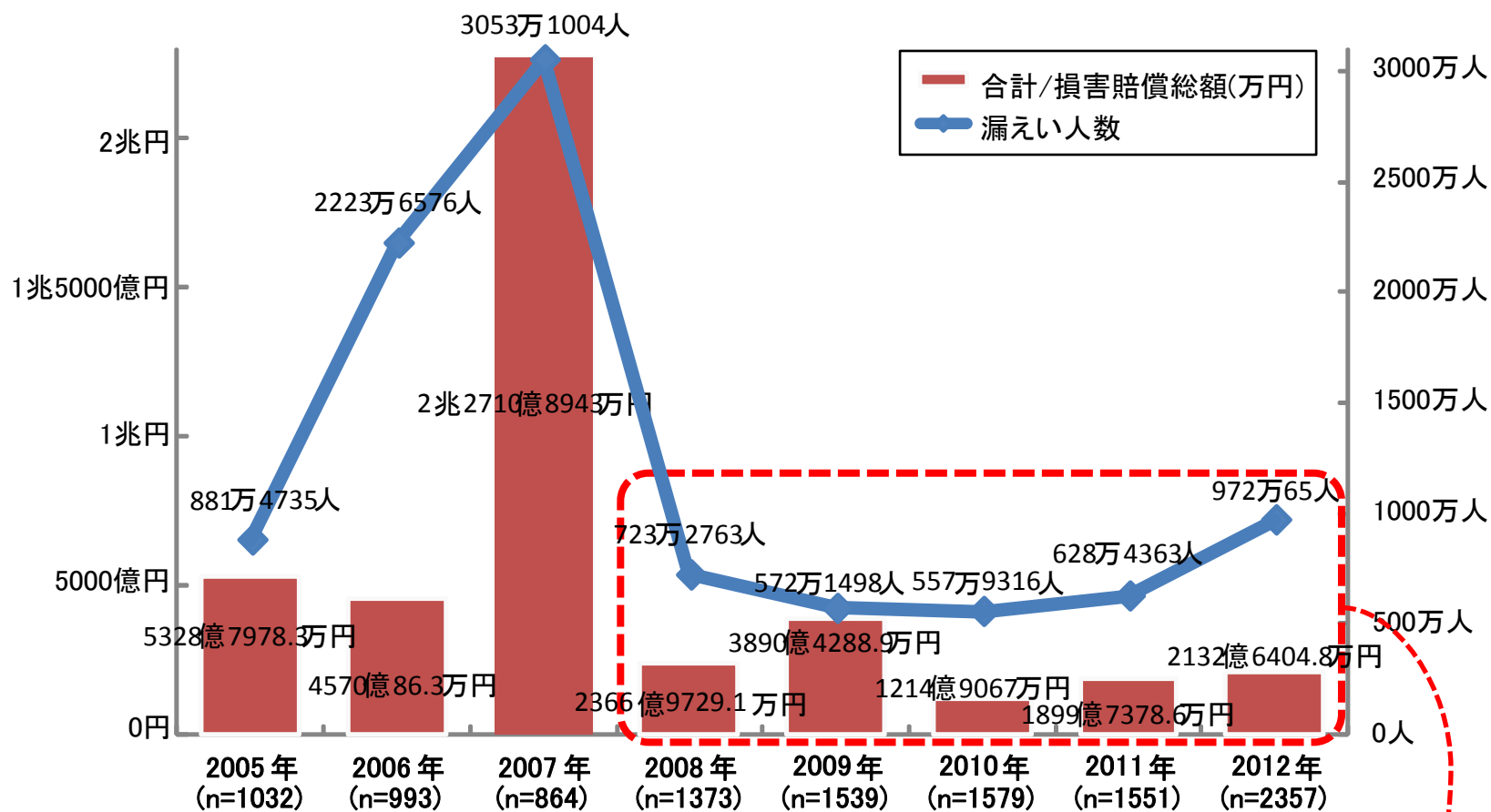


**想定損害賠償額が
100~1000万円未満の
インシデントの件数が増加**

3.6 漏えい人数と件数（経年）



3.7 漏えい人数と損害賠償総額（経年）



**漏えい人数、想定損害賠償総額ともに
以前より変化が少ない**

8. 2012年調査結果のまとめ

個人情報漏えいインシデント件数(報告件数)と漏えい人数が増加

→ **「金融業,保険業」の件数の増加が顕著**

- 地方銀行からの報告が増加。監督官庁の指示などが影響？
- その他の要素は、前年からあまり変化していない
- 100万人規模の大規模な個人情報漏えいインシデントは発生していない
- 個人情報漏えいの基本的な対策は、組織・企業へ広く行き渡った。(対策が一巡した)

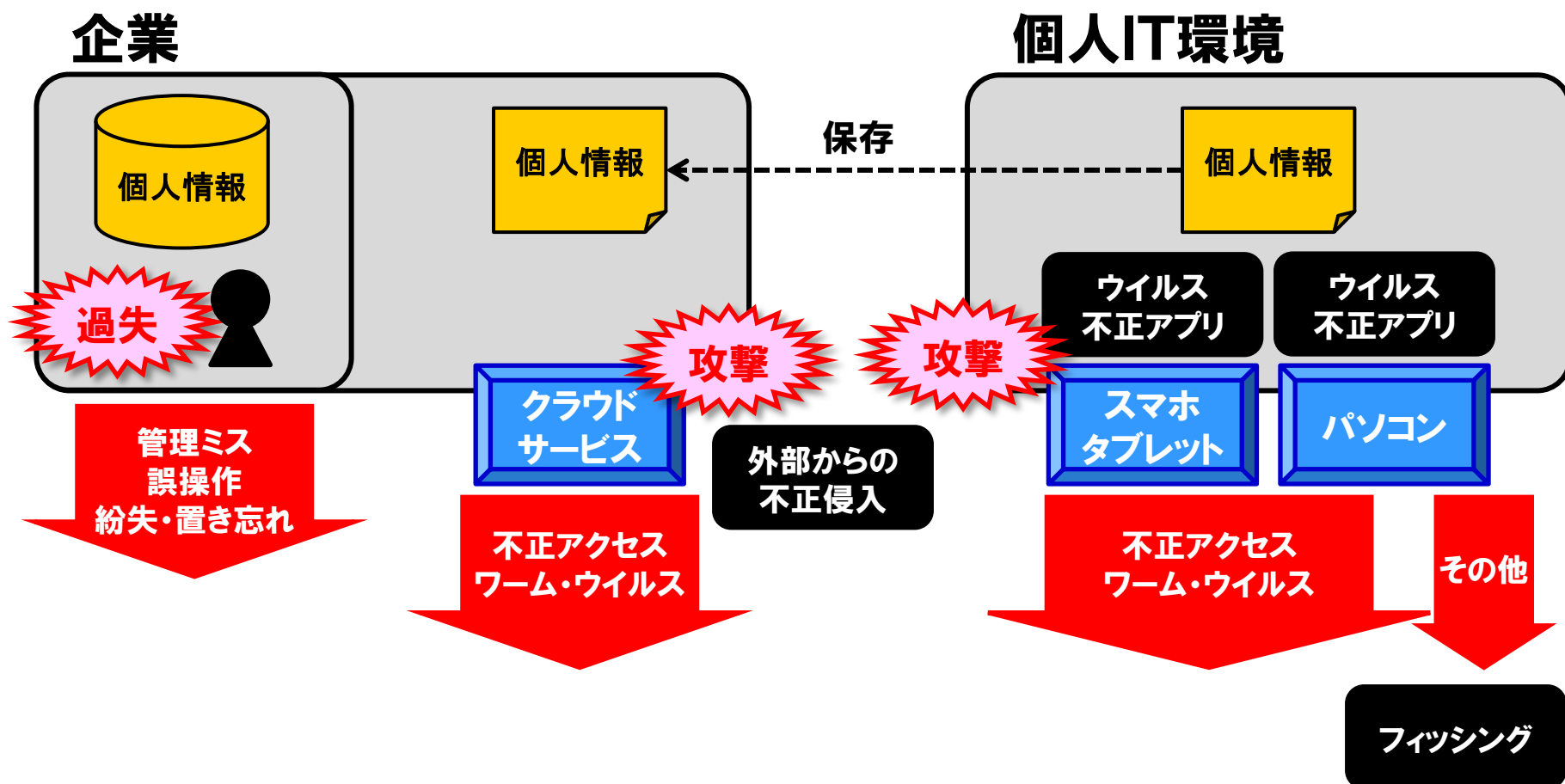
「管理ミス」が増加

- 「管理ミス」=計1391件のうち、1065件は「金融業,保険業」→増加の影響
- ヒューマンエラー系のインシデント「誤操作」「紛失・置忘れ」の件数はほぼ例年通り
→ 一定の割合で発生するため、インシデントの発生を完全に防ぐことが困難

**組織、企業が保有する個人情報の漏えいよりも、
その他からの個人情報の漏えいのリスクが増大中**

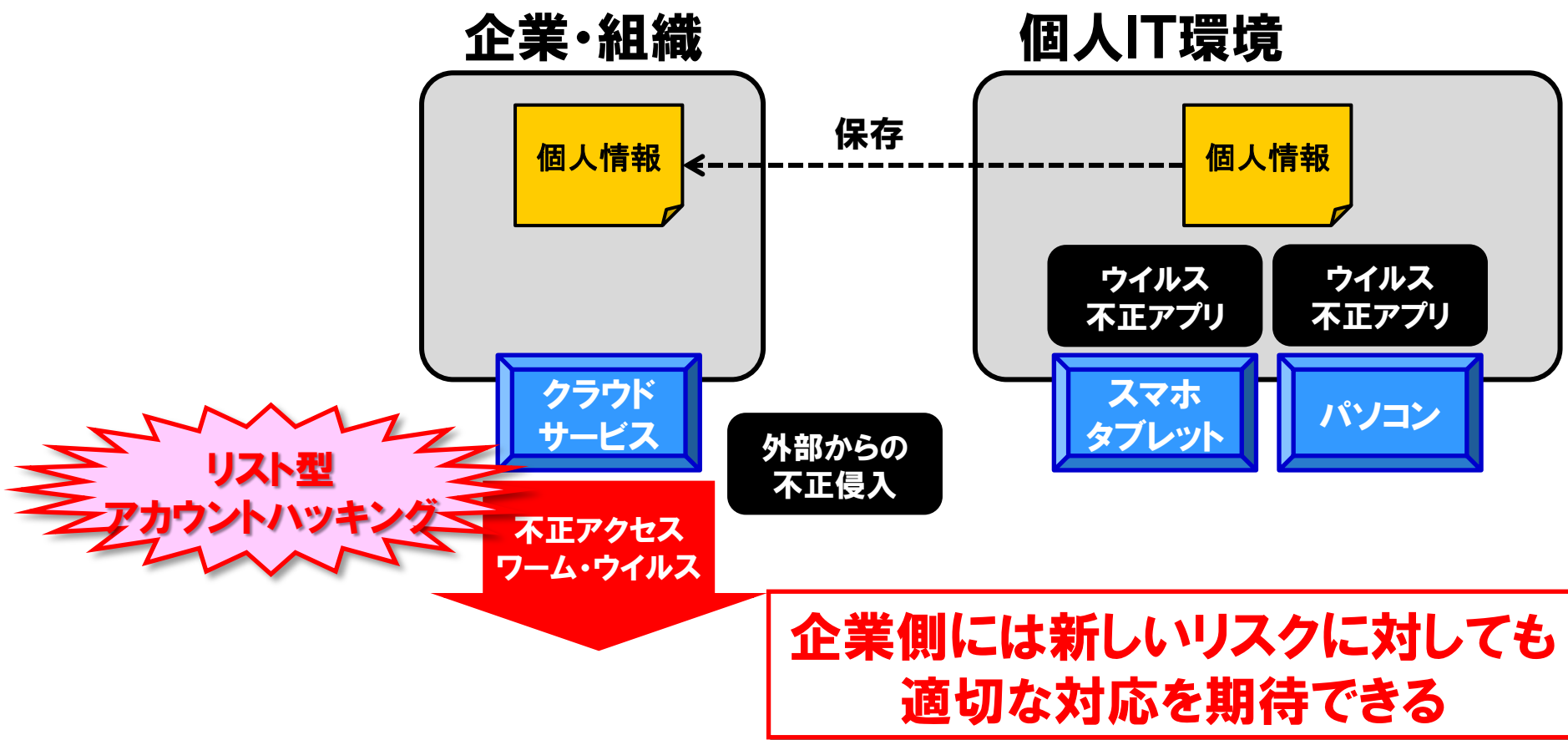
9. 新たな個人情報の漏えいリスク①

集約された個人情報データベースからの過失による漏えいだけでなく、個人のIT環境を直接攻撃して個人情報を詐取するリスクが増加

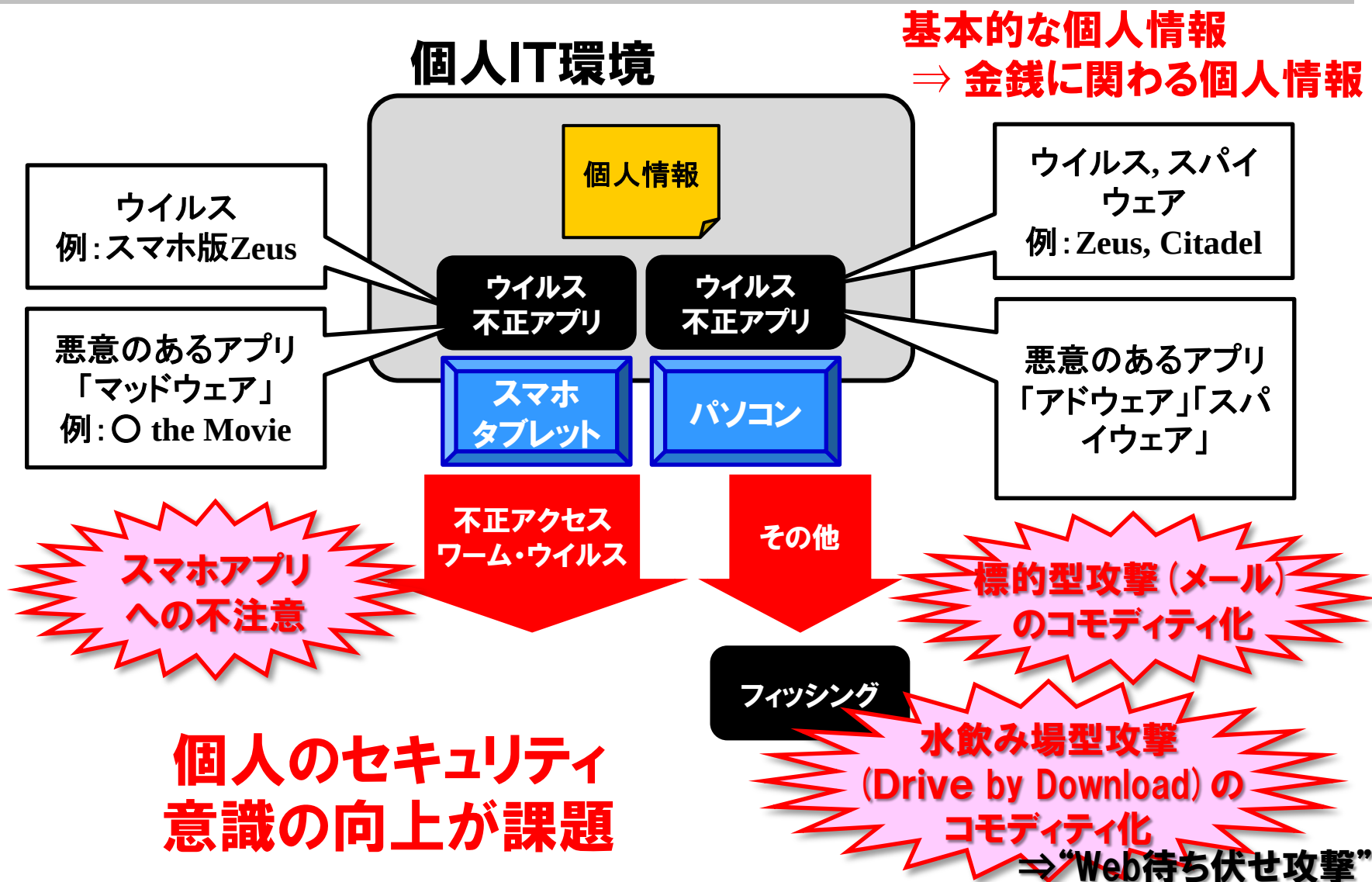


9. 新たな個人情報の漏えいリスク②

個人の利用率の高い複数のクラウドサービスの存在と、パスワードの使い回しの問題から、リスクが顕在化



9. 新たな個人情報の漏えいリスク③



10. セキュリティ被害調査の方向

- 企業・組織の機密情報／個人情報漏えいリスクの調査
⇒ 情報セキュリティ大学院大学と連携して実施
- 個人特性とインシデント発生確率の調査
- 個人IT環境からの個人情報漏えいリスクの調査
⇒ リスク定量化に向けて調査

**情報セキュリティ被害がある限り、
リスク定量化や投資対効果(ROSI)の
確立に向けて活動します。**

