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

JNSA 2010年度活動報告会

【調査研究部会】

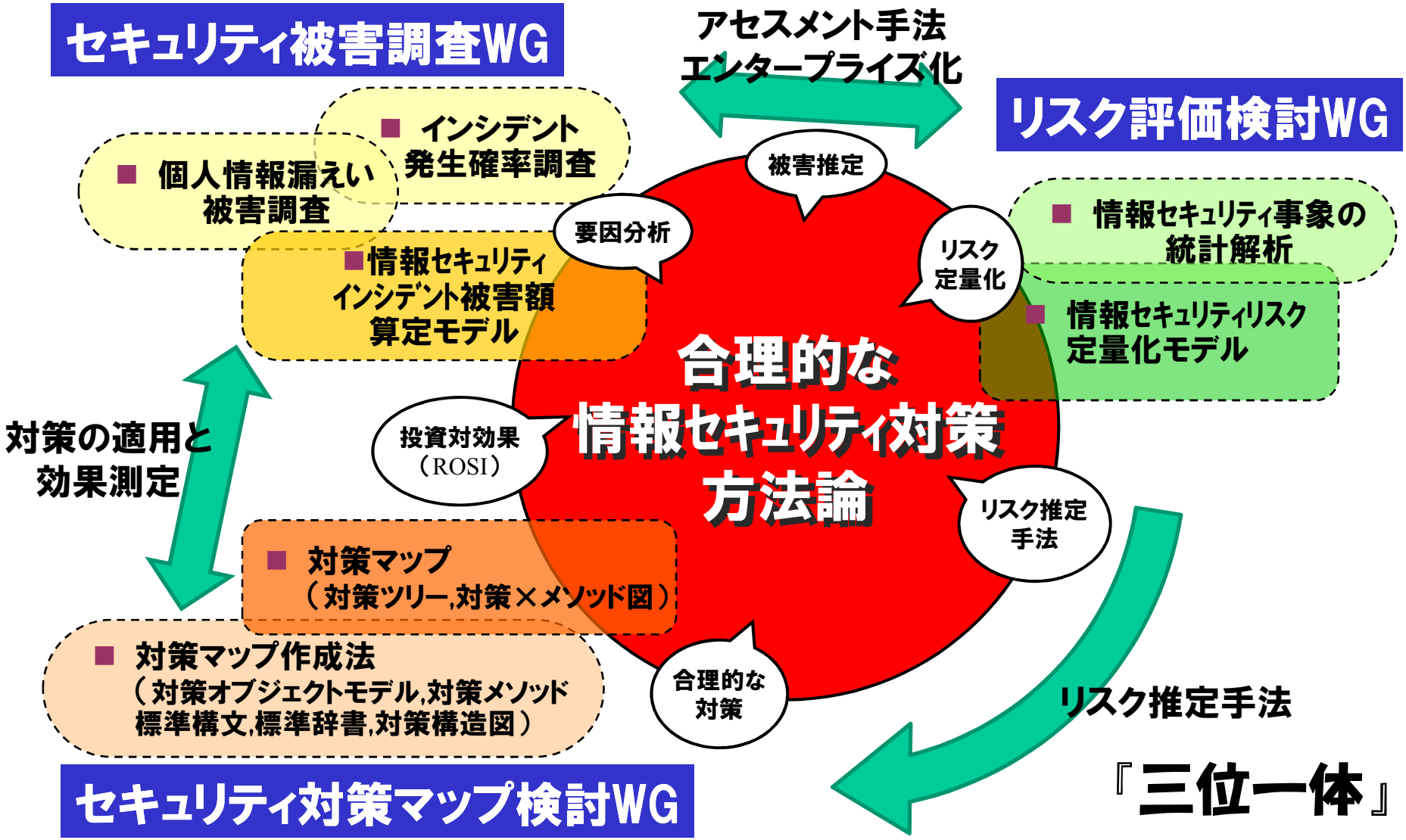
発生確率調査と
2010年個人情報漏えい調査の報告

セキュリティ被害調査WG

大谷 尚通
(株) NTTデータ

2011年 6月8日

セキュリティリスク対策 三兄弟



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	NKSJリスクマネジメント株式会社
	猪俣　朗	トレンドマイクロ株式会社
	大溝　裕則	株式会社JMC
	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　康彦	マイクロソフト株式会社
	佐藤　耕太郎	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

本日の内容

■2010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～

■2010年 情報セキュリティインシデントに関する調査 ～発生確率編～

2010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～

2010年 個人情報漏えいインシデント

JNSA

期間：2010年1月1～12月31日
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。

（2009年比較）

漏えい人数	557万9316人	−15万6357人
漏えい件数	1,679件	+140件
想定損害賠償総額	1215億7600万円	−2678億3544万円
一件当たりの漏えい人数	3,468人	−466人
一件当たり平均想定損害賠償額	7556万円	−1億9153万円
一人当たり平均想定損害賠償額	4万3306円	−6655円

2010年 インシデント・トップ10

JNSA

No.	漏えい人数	業種	原因
1	173万5841人	情報通信業	不正アクセス
2	46万3360人	情報通信業	内部犯罪・内部不正行為
3	31万人	医療，福祉	不正な情報持ち出し
4	25万4122人	卸売業，小売業	不正アクセス
5	20万1414人	学術研究，専門・技術サービス業	管理ミス
6	19万7907人	情報通信業	盗難
7	19万7077人	製造業	設定ミス
8	19万5132人	サービス業（他	不明
9	17万755人	サービス業（他	不正アクセス
10	17万325人	金融業，保険業	管理ミス

「情報通信業」が増加

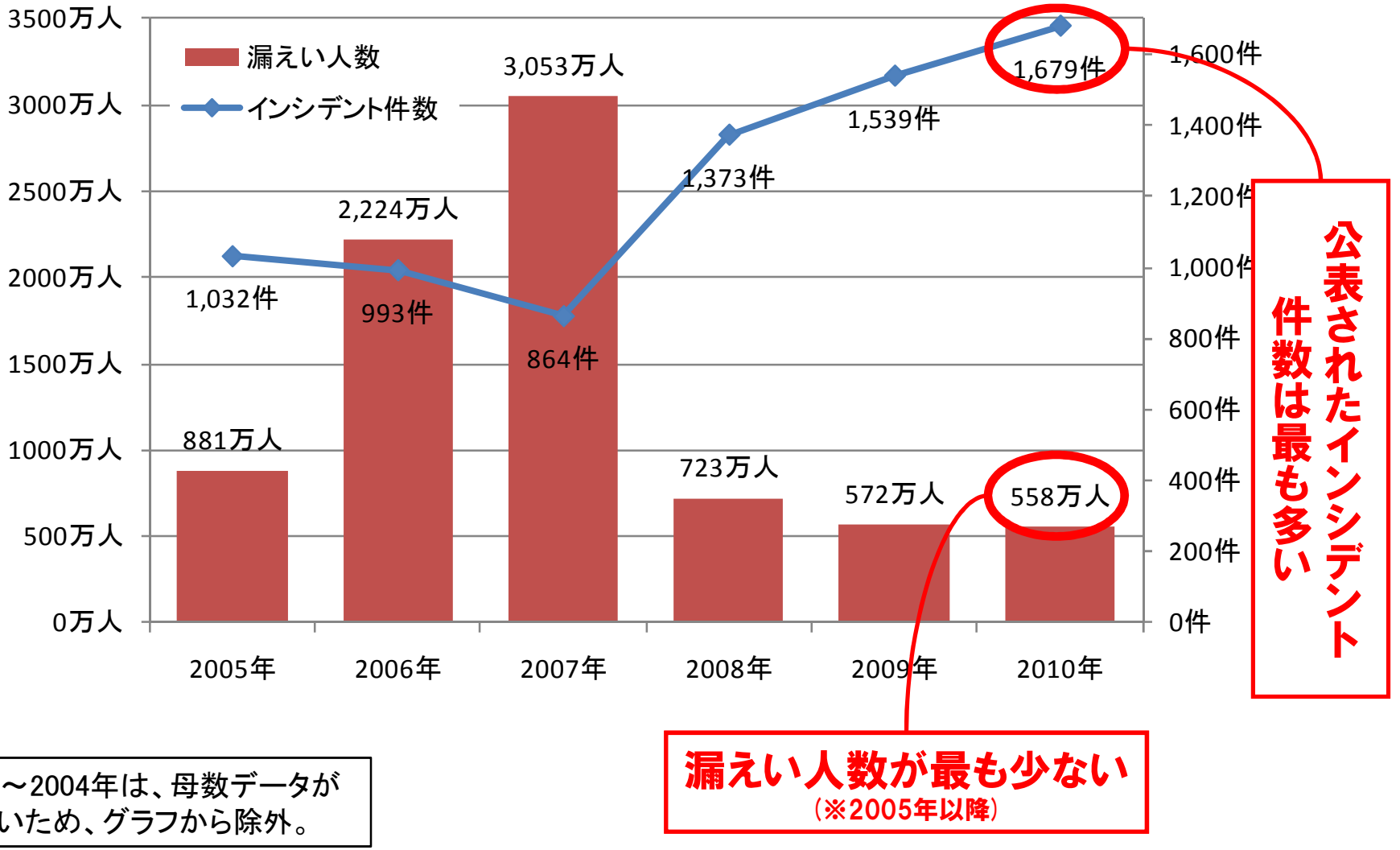
悪意を含む原因が増加

「金融業，保険業」「公務」が減少

「管理ミス」が減少

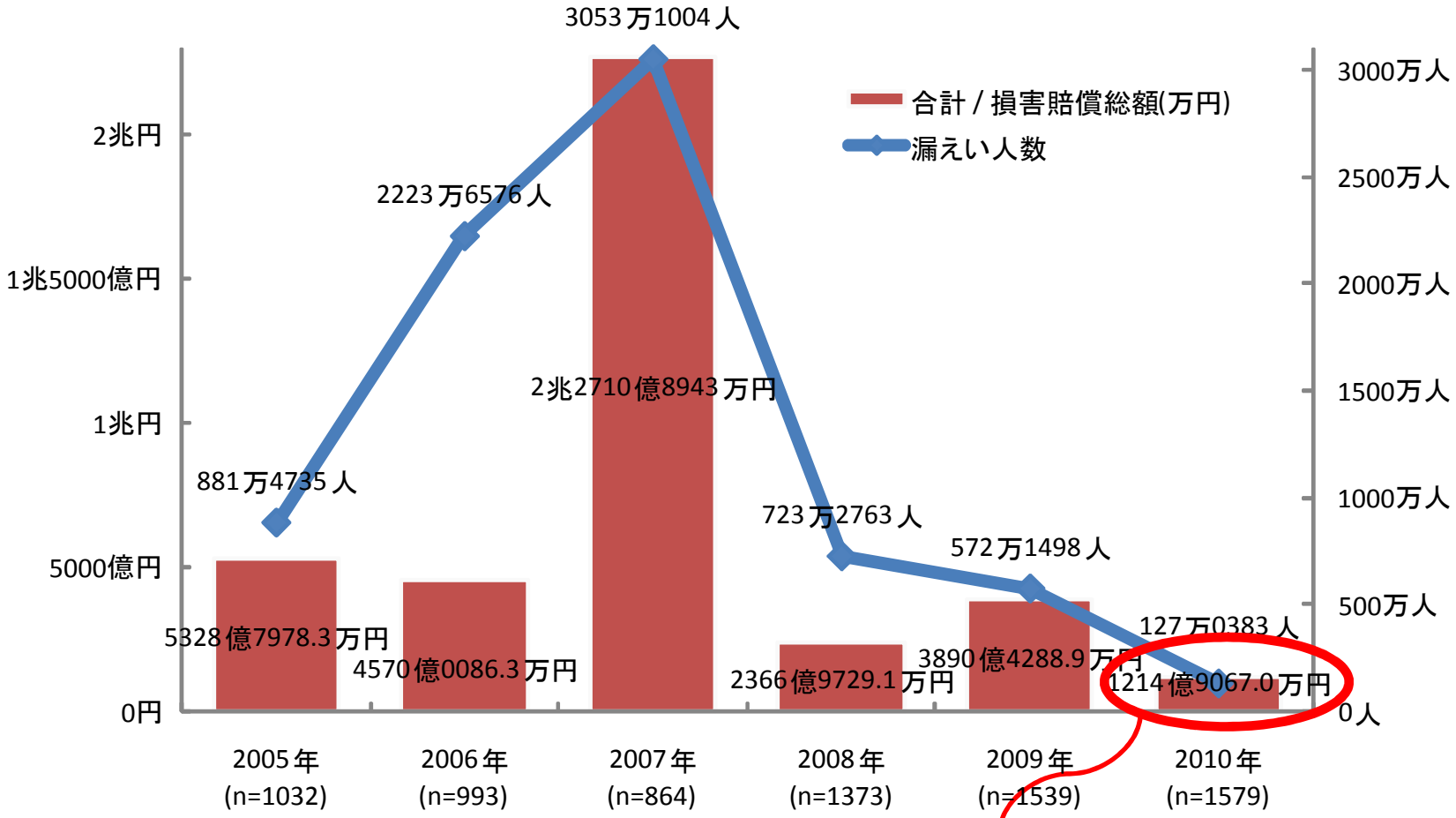
◎100万人を超える大規模なインシデントは１件のみ

漏えい人数と件数（2005～2010年）



2000～2004年は、母数データが少ないため、グラフから除外。

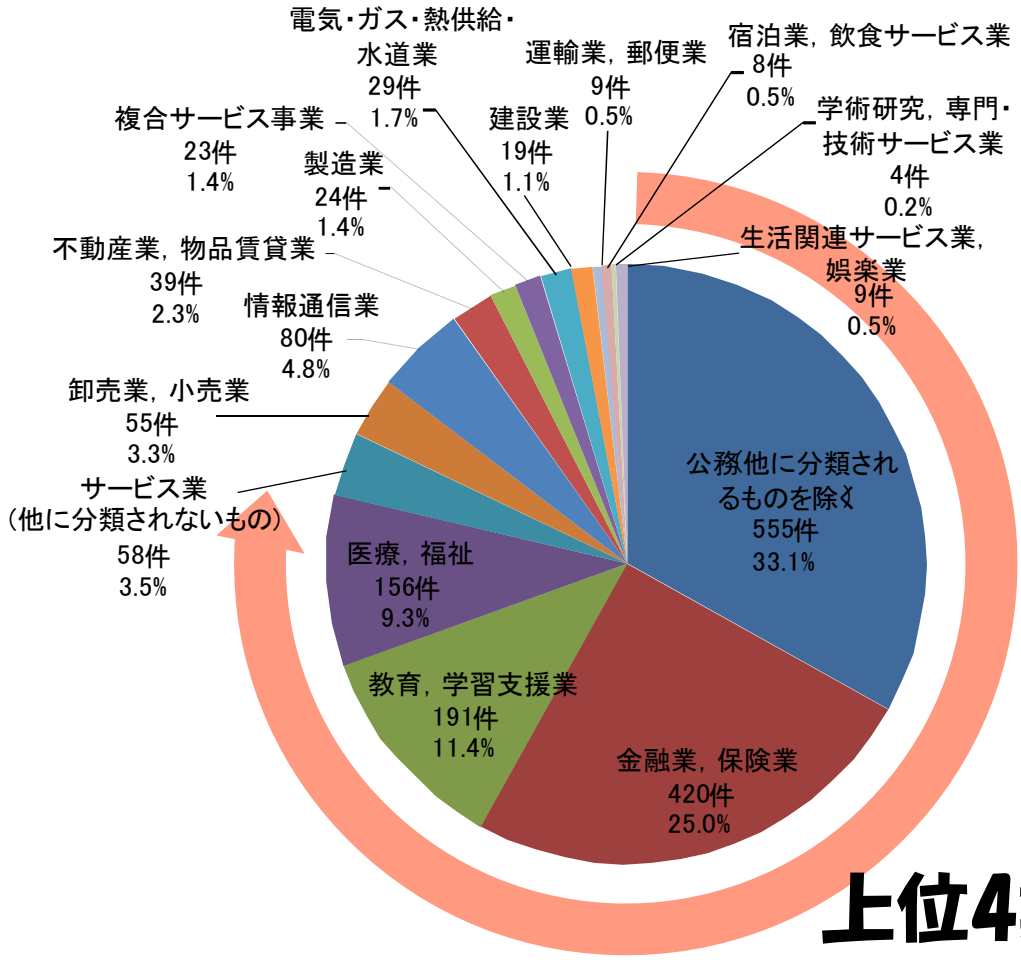
漏えい人数と損害賠償総額(2005～2010年)



2000～2004年は、母数データが少ないため、グラフから除外。

想定損害賠償総額が最も少ない
(※2005年以降)

① 業種別の漏えい件数



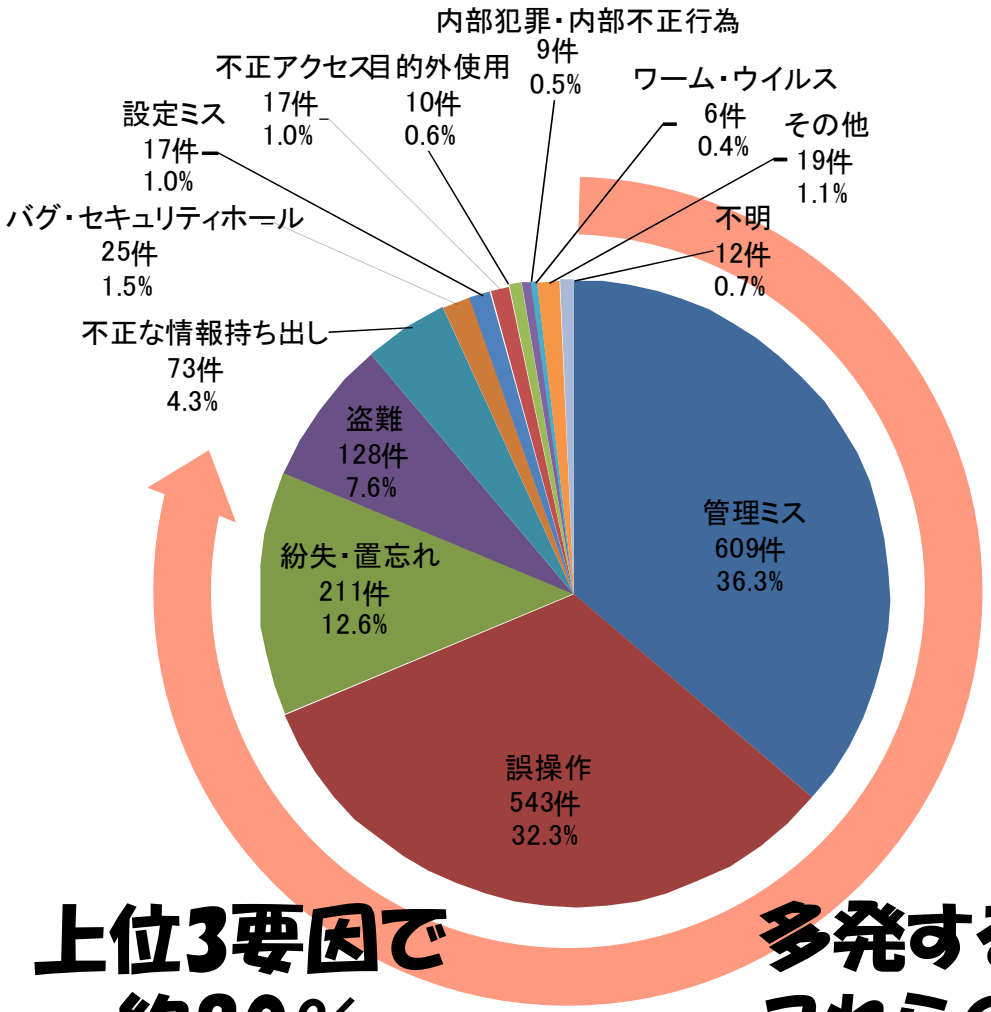
2009年	2010年
金融業，保険業（626件）	公務（555件）
公務（398件）	金融業，保険業（420件）
教育，学習支援業（81件）	教育，学習支援業（191件）
情報通信業（81件）	医療，福祉（156件）

漏えい件数が多い上位3業種は同じ

上位4業種で約80％

増加傾向の業種

② 原因別の漏えい件数



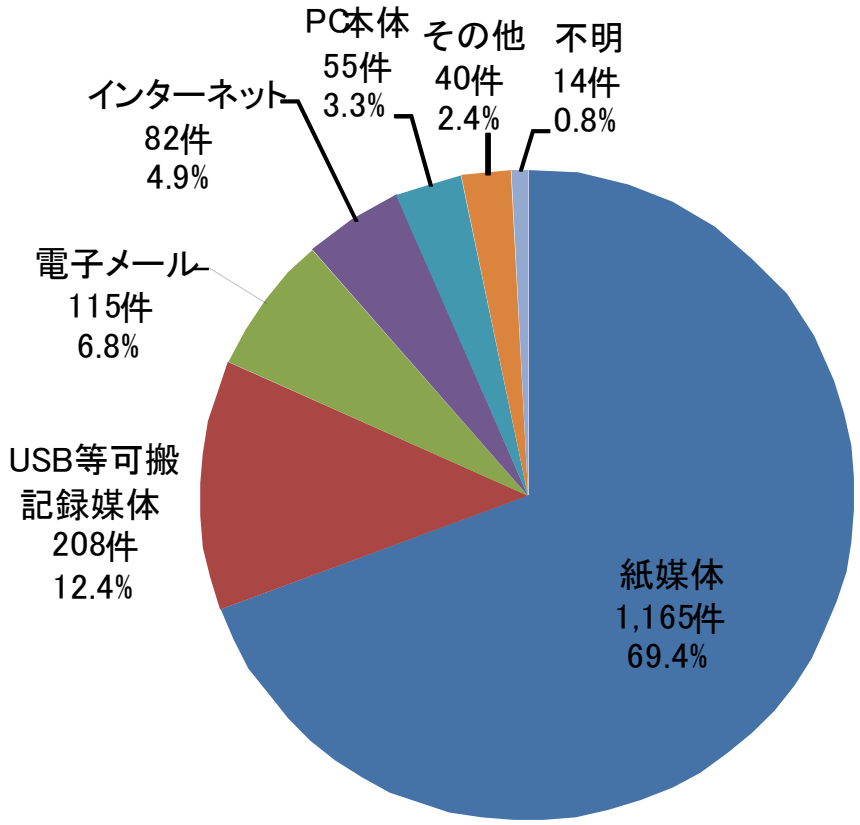
2009年		2010年
管理ミス（784件）	→	管理ミス（609件）
誤操作（369件）	→	誤操作（543件）
紛失・置忘れ（122件）	→	紛失・置忘れ（211件）
盗難（117件）	→	盗難（128件）

誤操作（＝ケアレスミス）による漏えいの割合が増加

上位3要因で約80％

多発する要因は、これらの3つで決まり。

③ 媒体別の漏えい件数

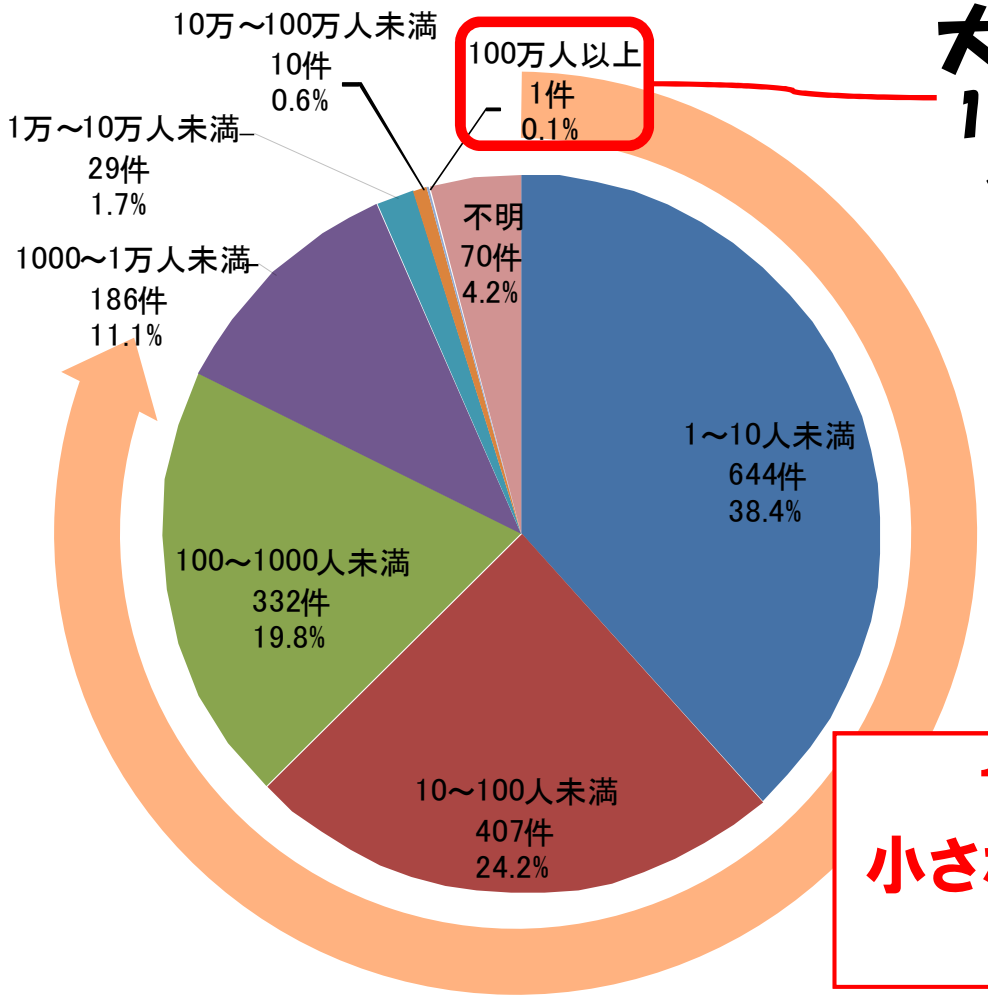


2009年		2010年
紙媒体（1,117件）	→	紙媒体（1,165件）
USB等可搬記録媒体（144件）	→	USB等可搬記録媒体（208件）
電子メール（108件）	→	電子メール（115件）
インターネット（70件）	→	インターネット（82件）

紙媒体による漏えいが多い。（例年通り）

情報漏えいが起きやすい経路・媒体も、これらの4つに絞られる傾向にある。

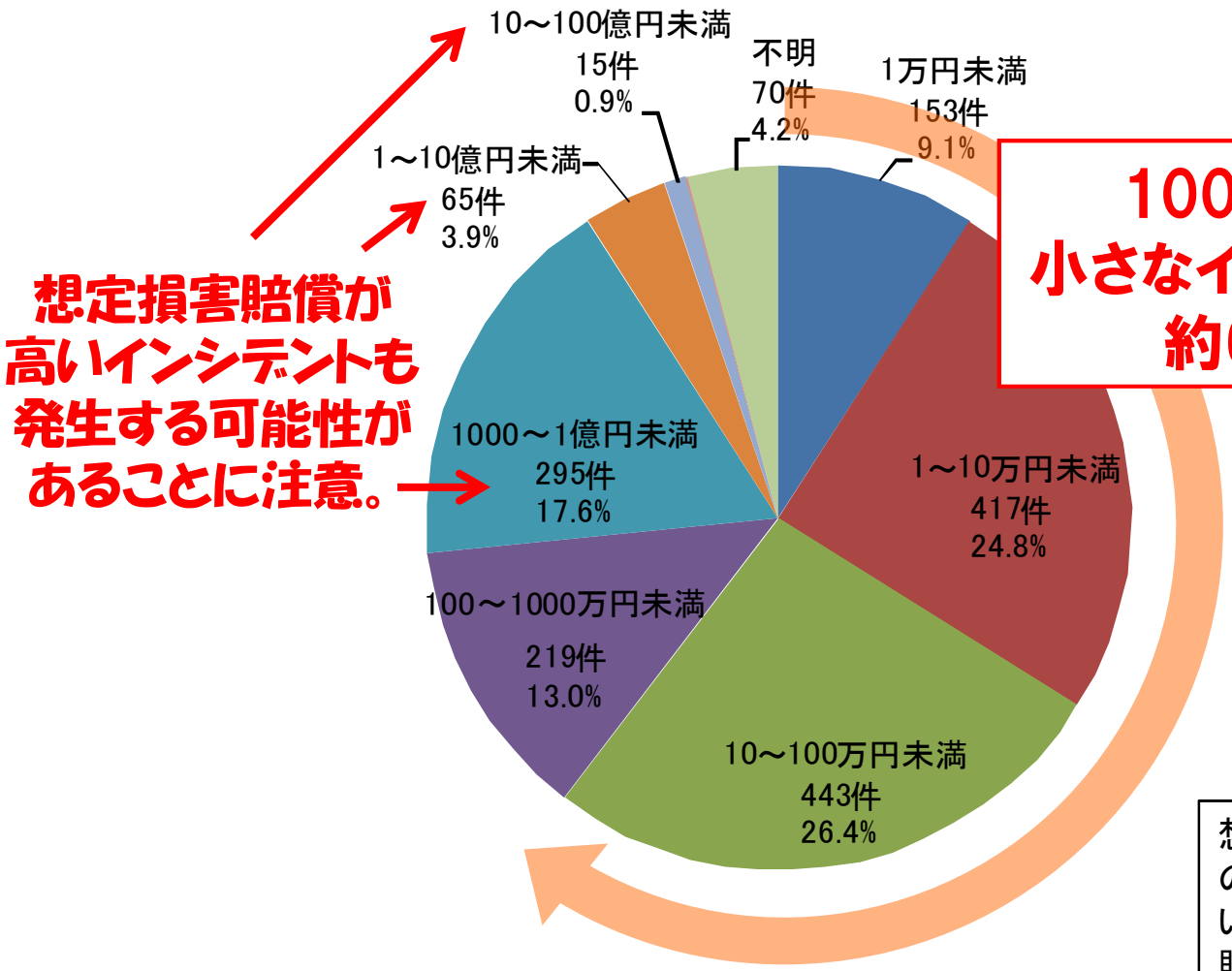
④ 一件当たりの漏えい人数



大事件は起きてない。
100万人を超える大規模な
インシデントは1件だけ。

1000人/件未満の
小さなインシデントの件数が
約80%を占める。

⑤ 一件当たりの想定損害賠償額



想定損害賠償が高いインシデントも発生する可能性があることに注意。

100万円未満/件の小さなインシデントの件数が約60%を占める。

想定損害賠償額は、漏えい人数分の損害賠償額をJOモデルに基づいて算出した金額であり、実際に賠償された金額ではない。

2010年の調査結果より

JNSA

■ **インシデント件数が最多で、漏えい人数が最少**（※2005年以降）
想定損害賠償額の総額も過去6年間で最少。2008～2010年の傾向。
・小規模なインシデントも報告（公表）されている。
・想定損害賠償額が大きいインシデントが少ない。

インシデント・トップ10は、悪意を含む原因が増加

■ **原因の新たな変化：誤操作によるインシデントが増加**
「誤操作」によるインシデント件数および割合が増加。ケアレスミスの顕在化？
「管理ミス」は減少傾向。内部統制対応や誤廃棄対策の効果？

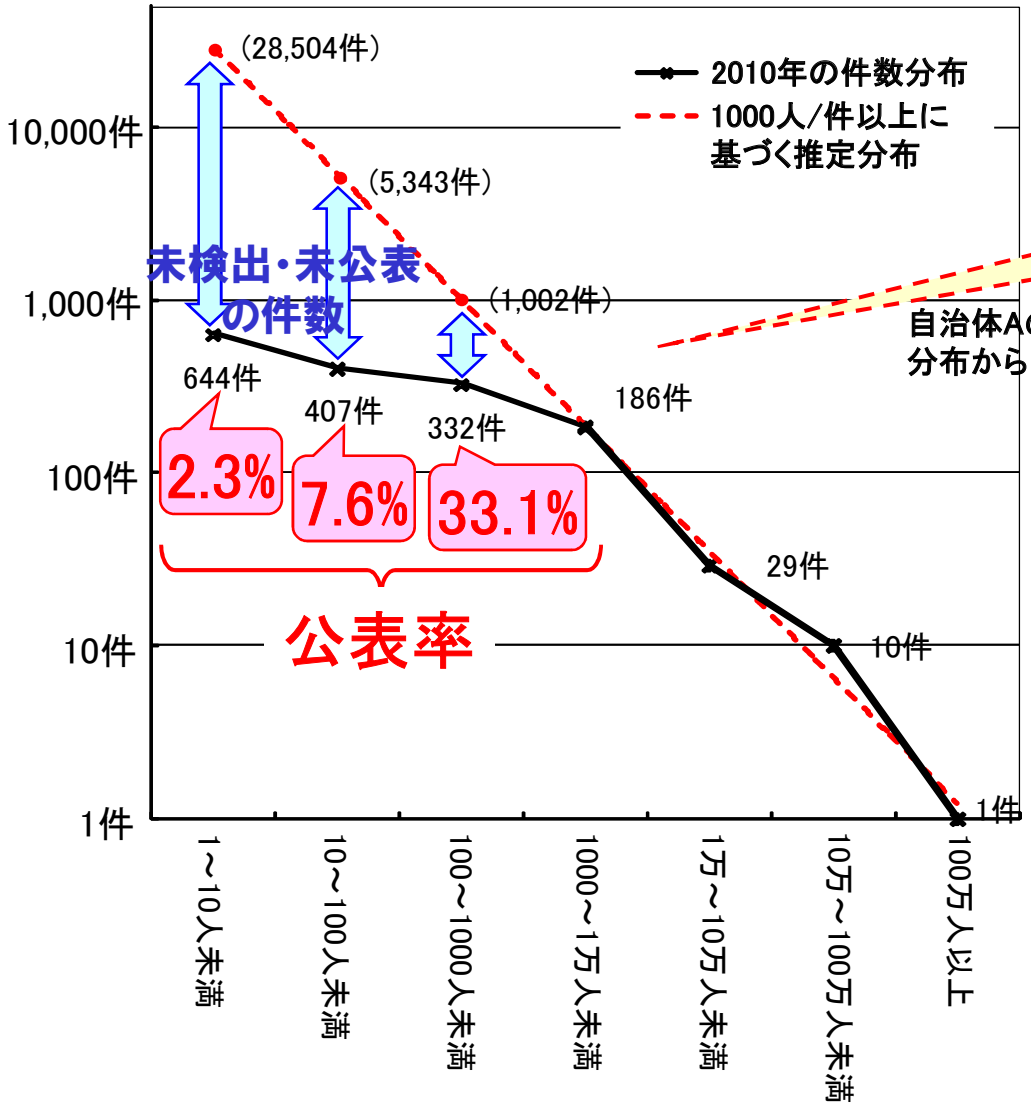
➢「ケアレスミス（誤操作）」と「悪意による漏えい」の二極化!?

■ **件数の増加：小規模なインシデントを公表する傾向**
業種別では、公務のインシデント件数がトップ。
特定の自治体が積極的に公表している。（A=212件、B=108件）
発生件数は改善していない。（2008年=212件, 2009年=190件,2010年=239件）

“説明責任”よい姿勢。

➢公表するだけでなく、継続的な改善を
➢情報セキュリティ報告書にて改善効果を報告

インシデント公表率の推定



- ある自治体Aは、小規模なインシデントから大規模なインシデントまで、ありのままを公表している。
- 漏えい人数が1000人/件以上のインシデントは、隠さず公表される。

自治体Aの分布と1000人/件以上のインシデントの分布から、インシデント全体の発生件数の分布を推定。

- 事前に公表の基準を設ける
  1000人を越えると連絡が困難な被害者が増える。→メディアを利用して公表
- 小規模なインシデントは、被害者へ個別対応できれば、その都度公表する必要性は低い
- 情報セキュリティ報告書にて報告。継続的な改善状況を報告

2010年
情報セキュリティインシデント
に関する調査

～発生確率編～

おっちょこちょいの確率

携帯電話・USBメモリ・パソコンを紛失しやすい人（通称：おっちょこちょい）は、存在するのか？

業務データが入った携帯電話・パソコン・USBメモリの紛失・盗難にあった人が、
複数の物の紛失・盗難にあっている確率を調査

	会社携帯 紛失・盗難	会社PC 紛失・盗難	会社USB 紛失・盗難
業務データが入った会社貸与の 携帯電話を紛失・盗難（n=184人）		108人 （58.7%）	102人 （55.4人）
業務データが入った会社貸与の パソコンを紛失・盗難（n=148人）	108人 （73.0%）		97人 （65.5%）
業務データが入った会社貸与の USBメモリを紛失・盗難（n=146人）	102人 （69.9%）	97人 （66.4%）	
全回答者（n=4886人）	18.4人 （3.8%）	148人 （3.0%）	146人 （3.0%）

アンケート回答者
約5000人のうち、
複数の物を紛失した
人は約100人

＝ 約2%

紛失しやすい人（おっちょこちょい）は存在する

被害額を計算できますか？

JNSA

ALE ＝ SLE × ARO

情報セキュリティインシデントの
年間予想被害額

個別の情報セキュリティ
インシデントの予想被害額

1年間の発生確率

業務内容によって
異なるので各自で
用意してください。

一朝一夕では求めることができない。
公開された値が非常に少ない。

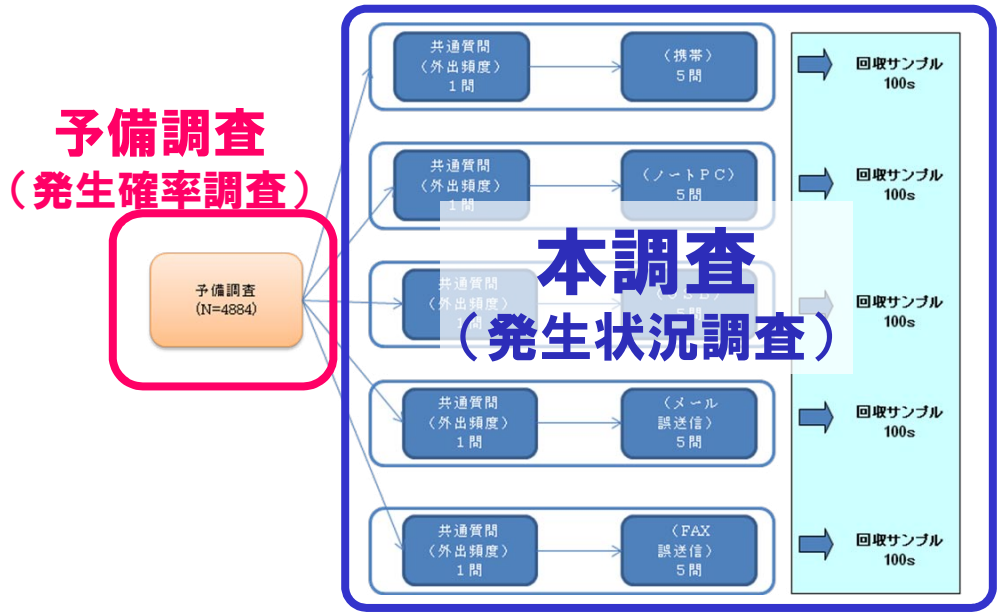
インシデントの
発生確率を知りたい！

アンケート調査方法

- インターネットWebアンケート
- 調査期間：2010年10月15日（金）～19日（火）
- 調査対象：全国の就業者（男女）、18～69歳
- 有効回答数：4,884名（予備調査）、500名（本調査）
- 調査方法：予備調査と本調査の2段階
  - 携帯電話／パソコン／USBメモリの盗難・紛失
  - 電子メール／FAXの誤送信の経験について調査

表：職種の内訳

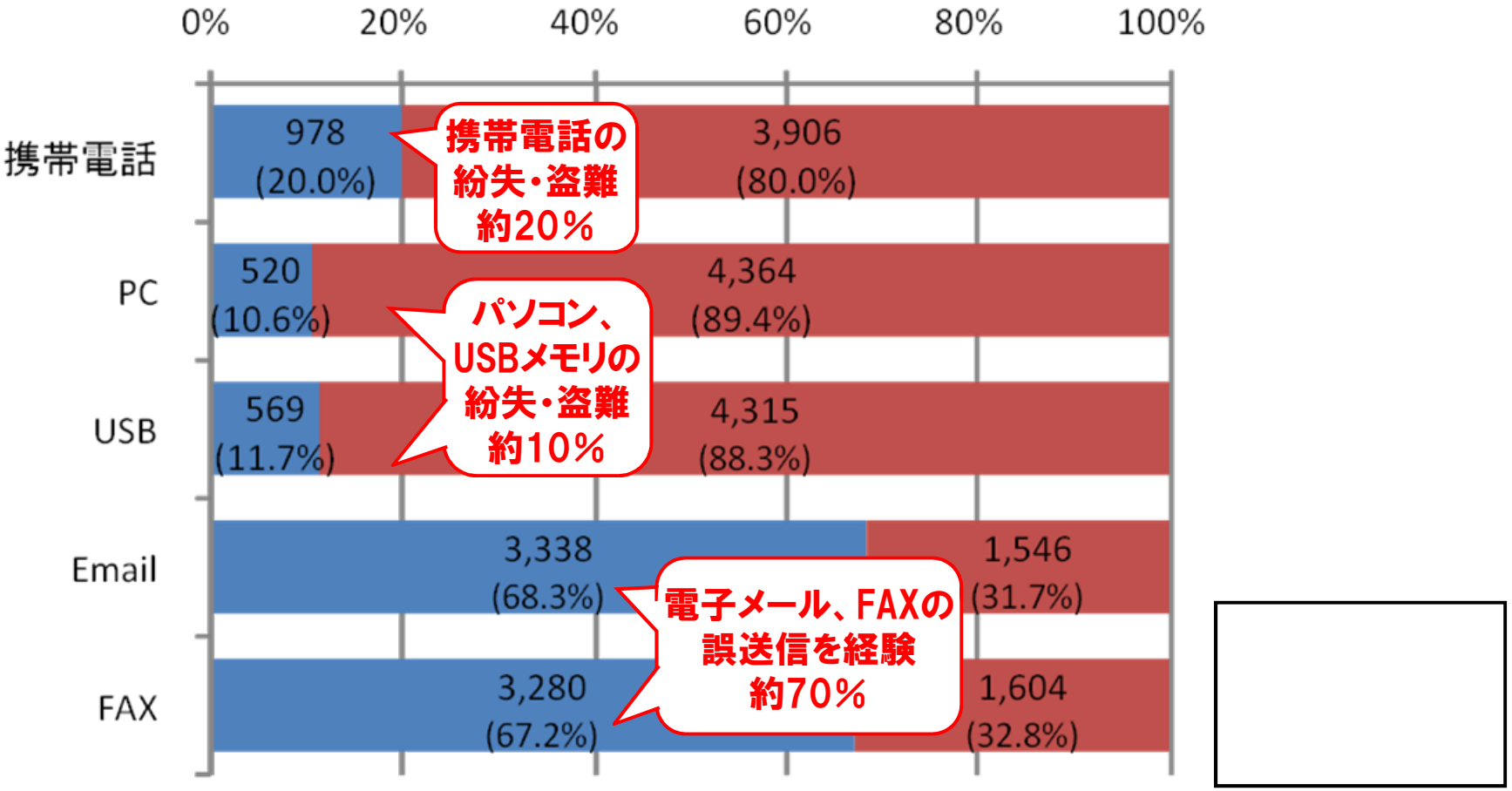
職種		人数	%
会社経営者・役員・団体役員		240人	4.9%
会社員・団体職員	正社員	2,787人	57.1%
	契約・派遣	388人	7.9%
地方公務員		144人	2.9%
国家公務員		40人	0.8%
自営業・個人事業主・フリーランス		582人	11.9%
自由業（開業医・弁護士事務所経営・プロスポーツ選手など）		101人	2.1%
パート・アルバイト・フリーター		602人	12.3%



情報セキュリティインシデントの経験

JNSA

これまでに、携帯電話／パソコン／USBメモリを紛失・盗難、
電子メール／FAXの誤送信を経験したことがある人は、どのくらい？



紛失・盗難の年間発生確率

JNSA

紛失・盗難、誤送信は、1年間にどのくらい発生するのか？

予備調査と本調査の結果をもとに、以下5種類の紛失・盗難、誤送信の年間の発生確率を算出。

調査対象	2010年	2009年	発生確率
携帯電話(※)	6.4%	6.6%	約6.5%
パソコン(※)	3.7%	3.1%	約3.5%
USBメモリ	4.7%	4.1%	約4.5%
電子メール	40.3%	17.1%	約40.0%
FAX	39.0%	12.1%	約40.0%

（私物、会社貸与の両方を含む）

（※）紛失未遂を含む

社員が携帯電話・パソコン・USBメモリの紛失・盗難にあう確率は約4～6%

社員が電子メール、FAXを誤送信する確率は約40%

注1) 紛失・盗難や誤送信にあった年を1つ選択させている。
2009年も2010年も誤送信した人は、2010年を選択している。
したがって、2009年の誤送信の割合が少ないとは言えない。

注2) 年1回以上あった人の割合。
1年間に複数回あった人も1人としている。

紛失リスクと
セキュリティ対策投資額

①企業プロファイル

個人情報漏えいが発生した場合の想定被害金額を試算し、
それを対策するためのセキュリティ対策投資額を算出してみよう。

情報セキュリティインシデントの
年間予想被害額の算出式

$$ALE = SLE \times ARO$$

- SLE（個別の情報セキュリティインシデントの予想被害額）→ 緊急的な対策費用などの間接被害の想定被害額
- ARO（1年間の発生確率）→ USBメモリの紛失盗難発生確率

■ 企業プロファイル（想定）
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。インターネットショッピングサイトも運用し、売り上げは、会社全体の約10%程度。

「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」参照

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

収集・管理しているCRM用の顧客情報

- 氏名、氏名フリガナ、性別、年齢（区分）、職業
- 郵便番号、住所、電話番号
- 購入履歴情報（商品コード、購入日時）
- ショッピングサイトのログインID/パスワード
- クレジットカード番号、有効期限、金融機関の口座番号

※クレジットカード番号、有効期限等の信用情報は、分離された別システムのため、企業内から参照できない

会社支給のUSBメモリを使用してショッピングサイトの出店企業や配送委託先と顧客情報をやりとりしている。上記業務に従事している従業員は全体の10%（100名）程度。

②被害額の想定

■USBメモリ等の可搬型媒体を経由した平均の漏えい人数＝2万8340人(※3)
USBメモリの紛失によって、会員情報 2万人分が漏洩したと仮定。
■サイトの閉鎖などの対応なし＝逸失利益、機会損失などの直接被害なし。
被害額は、緊急的な対策費用などの間接的な想定被害額。

表：間接的な想定被害額の内訳

項目		費用
業務継続費用	対策組織業務に係る人件費（1ヶ月分）	500万円
	損害賠償費用（訴訟参加率※1=0.1%）	36万円
	弁護士費用※2・裁判費用	30万円
見舞い品費用	見舞い品代＋送料他（2万人分※3 ）	1,400万円
謝罪訪問費	謝罪訪問に掛かる費用（10人分）	110万円
広報費用	謝罪広告費	なし
	情報公開ページ作成費用（2回）	10万円
臨時的な対策費用	コールセンター設置費用（1ヶ月分）	500万円
	問い合わせ窓口常駐人員（1ヶ月分）	200万円
合計		2,786万円

＝2786万円

※1 訴訟参加率については、近年の個人情報保護意識の高まり等を鑑み、やや高めの想定。
※2 弁護士費用については、実務的な現実では相当額の着手金が必要なことから、民事訴訟等の着手金における現実的な金額として30万円を想定した。（参考：日本弁護士連合会「中小企業のための弁護士報酬目安［2009年アンケート結果版］」）
※3 （※3）「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」

③想定被害額と対策投資額の算出

■ 想定企業におけるUSBメモリの紛失状況

- ➢USBメモリを使って顧客情報をやり取りしている社員＝100名
- ➢紛失・盗難の発生確率＝約4.5%
- ➢紛失したUSBメモリに個人情報が含まれている確率＝約33%

■ 漏えい被害額とセキュリティ対策投資額の検討

「USBメモリの紛失・盗難に遭う」事象と「紛失したUSBメモリに個人情報が含まれている」事象が同時に起こる確率：

4.5% × 33% ＝ 約1.5% ARO（1年間の発生確率）

社員100名の中で、1年間に個人情報を含むUSBメモリを紛失するインシデントを引き起こす人：

100人 × 1.5% ＝ 1.5人

１年間のUSBメモリからの個人情報漏えいリスク：

SLE（個別の情報セキュリティインシデントの予想被害額）

2,786万円 × 1.5人 ＝ 4,179万円/年

3年分としてまとめて投資をする場合：（IT機器、ソリューションなどのライフサイクル＝約3年）

“最大”4,179万円/年 × 3年 ＝“最大”1億2,537万円

投資額、投資先の対策（システム/体制整備/教育など）は、各自判断。

発生確率調査の結果より

JNSA

- 携帯電話・パソコン・USBメモリの紛失・盗難、電子メール・FAXの誤送信は、一定の確率で発生している。
  - インシデントの年間発生数が推定可能
  - インシデント対応費用の確保のめやす
- 業務で私物の携帯電話・パソコン・USBメモリが使われている。
  - 業務と個人(プライベート)の分離が不十分
  - 会社貸与・支給の不足
- 電子メール・FAXの誤送信発生確率が高い
  - 電子メール・FAX使用の危険性の認識不足

ケアレスミスと(悪意)が次の対策のポイント

2010年の成果物の公開

JNSA

- 2010年 情報セキュリティインシデントに関する調査
  ～発生確率編～　（公開済み 2011/4/1）
- 2010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～（近日公開予定）

2011年も上記の成果物を公開予定です。

WGメンバも募集