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 2011 【A2】

リスク定量化への第一歩
～紛失は居酒屋ではない、社内で起きてるんだ！～

セキュリティ被害調査WG

大谷 尚通

(株) NTTデータ

2011 年 1月25日

セキュリティ被害調査WG

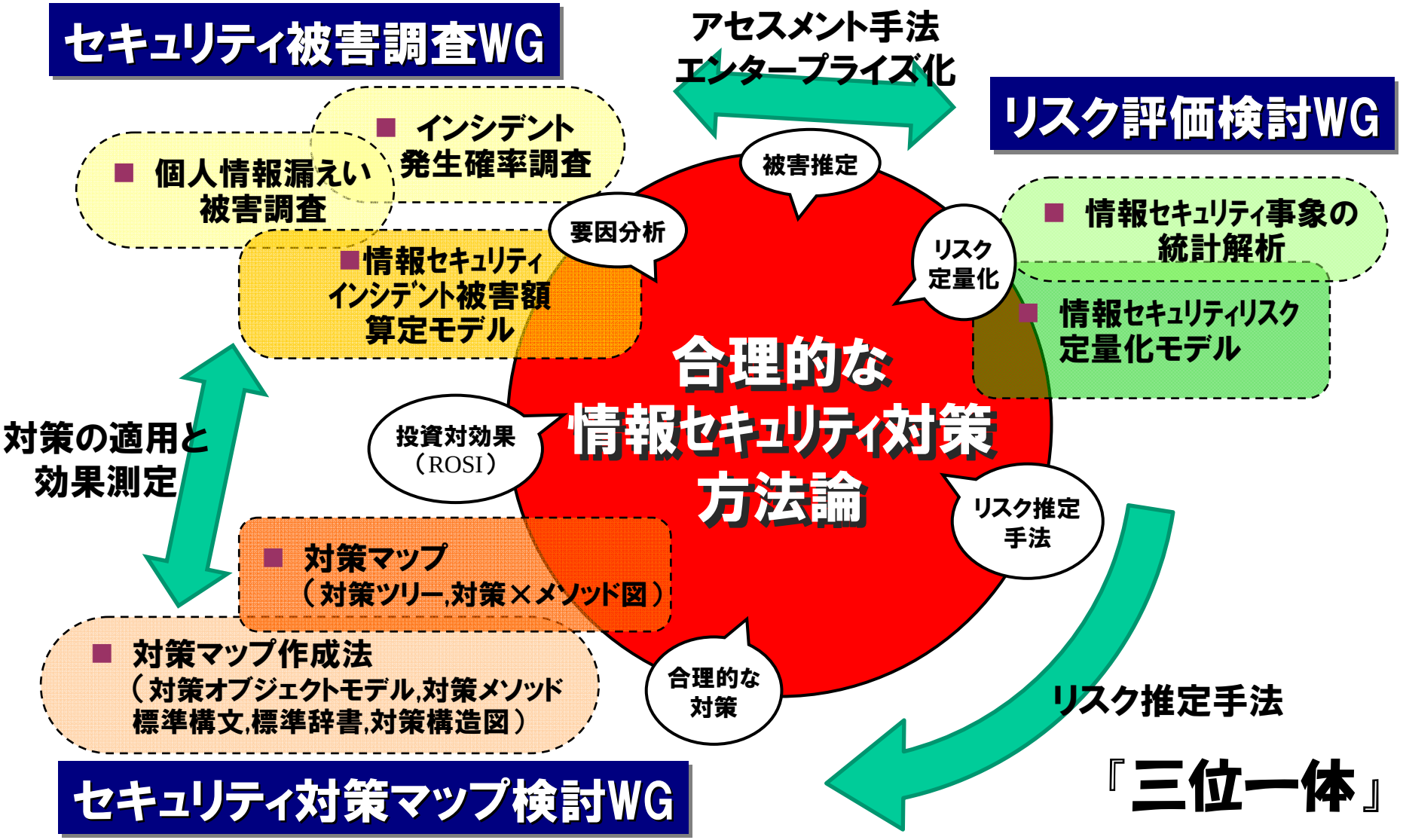
JNSA

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。

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

セキュリティリスク対策 三兄弟



『三位一体』

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【上半期速報】

■インシデント発生確率調査の結果報告

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
	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　康彦	マイクロソフト株式会社
	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
	吉田　裕美	株式会社ラック

2010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】

2010年上半期 個人情報漏えいインシデント

期間：2010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。

（2009年上半期 比較）

漏えい人数	127万 383人	−104万8,620人
漏えい件数	684件	−80人
想定損害賠償総額	364億3,705万円	−1,181億2,182万円
一件当たりの漏えい人数	1,951人	−1,234人
一件当たり平均想定損害賠償額	5,597万円	−1億5,634万円
一人当たり平均想定損害賠償額	4万823円	−4,542円

2010年 個人情報漏えいインシデントの比較

	2009年	2010年（上半期×2）
漏えい人数	過去最少 572万1,498人	約255万人
漏えい件数	過去最高 1,539件	約1370件
想定損害賠償総額	3,890億4,289万円	約729億円
一件当たりの漏えい人数	3,924人	3,185人
一件当たり平均想定損害賠償額	2億6,683万円	5,597万円
一人当たり平均想定損害賠償額	4万9,961円	4万823円

$$\frac{\text{255万人}}{\text{1億2,776万7,994人}} = \text{約50人に1人の割合}$$

一日平均3.8件

2009年
28人に1人
4.2件/日

2010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	20万1,414人	学術研究，専門・技術サービス業	管理ミス
2	19万7,907人	情報通信業	盗難
3	17万　325人	金融業，保険業	管理ミス
4	10万　　人	情報通信業	紛失・置忘れ
5	9万　700人	金融業，保険業	管理ミス
6	6万3,805人	サービス業	盗難
7	5万1,300人	金融業，保険業	管理ミス
8	3万3,600人	金融業，保険業	管理ミス
9	2万7,998人	金融業，保険業	管理ミス
10	1万5,521人	金融業，保険業	管理ミス

金融業が多い。

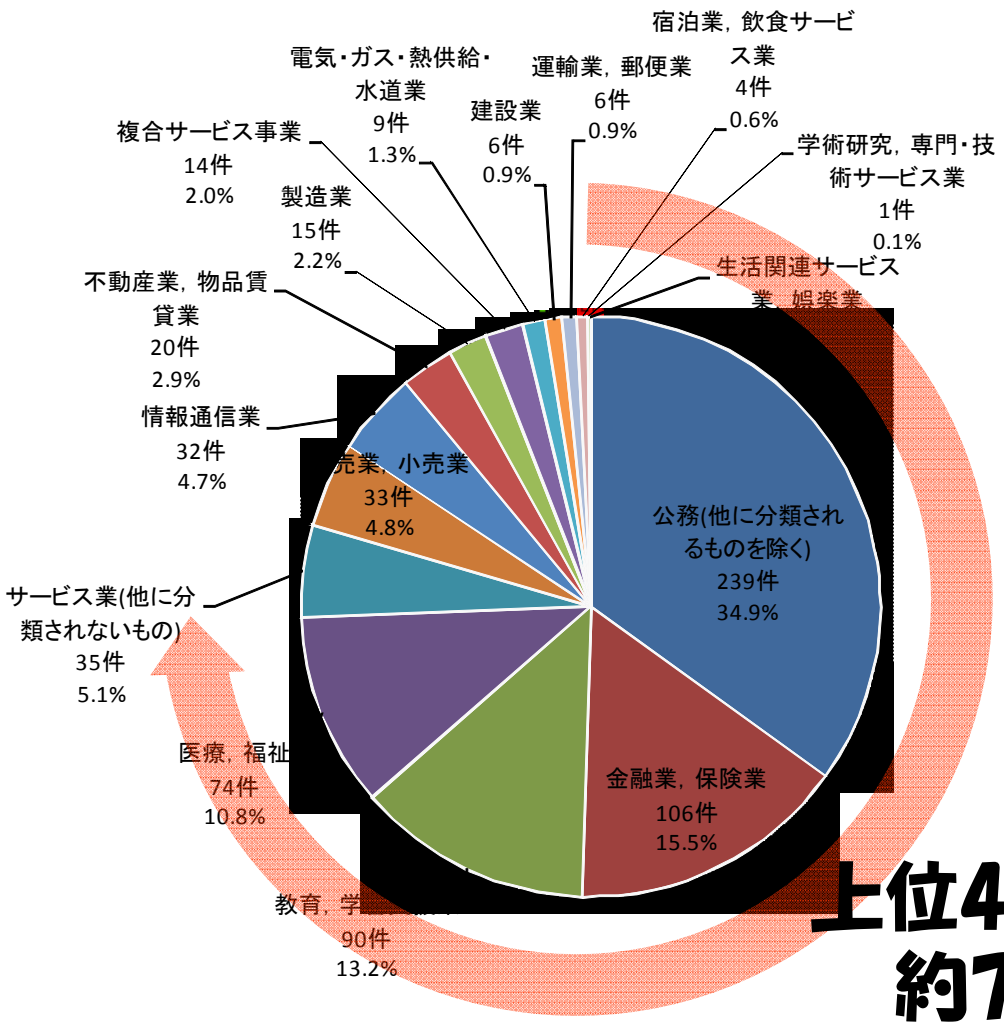
2007年以降、管理ミスが多い

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の発生が無い

① 業種別の漏えい件数



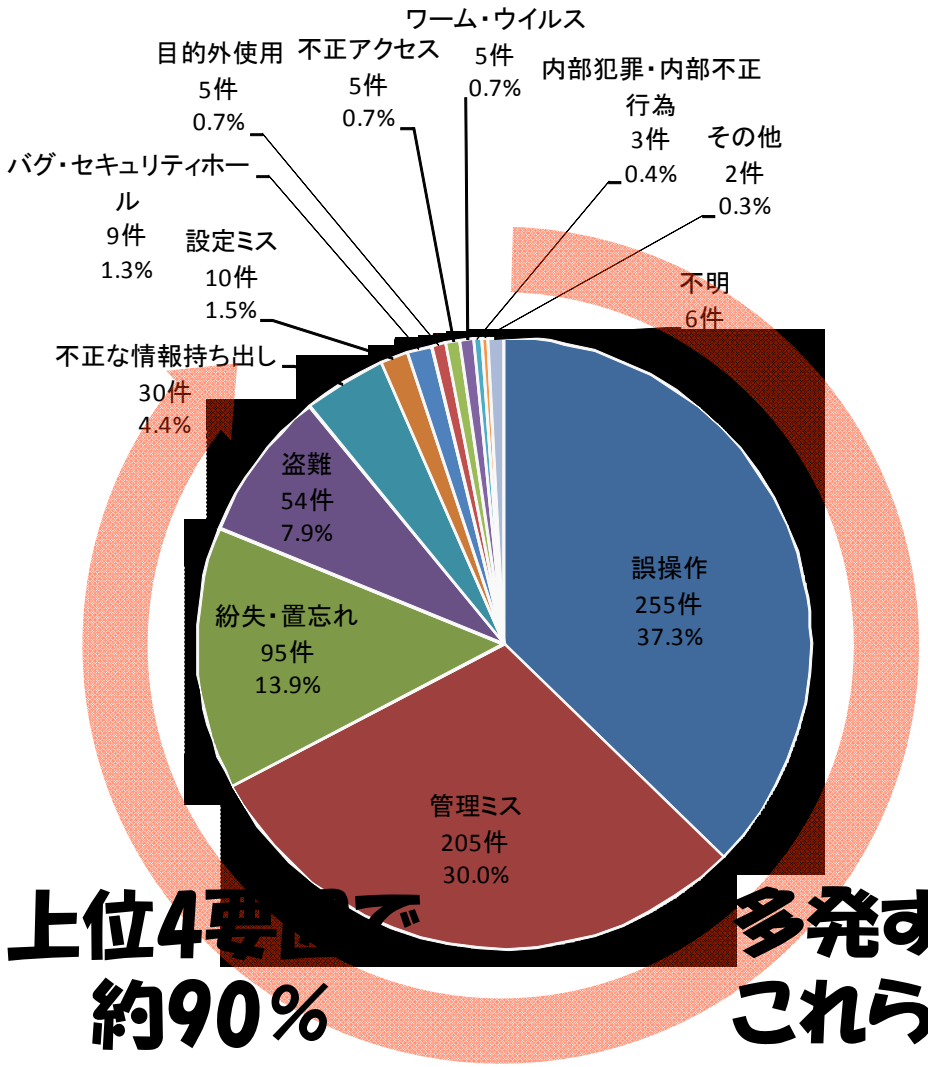
上位4業種で約75％

2009年	2010年
金融業，保険業（626件）	公務（239/478件）
公務（398件）	金融業，保険業（106/212件）
教育，学習支援業（81件）	教育，学習支援業（90/180件）
情報通信業（81件）	医療，福祉（74/148件）

漏えい件数が多い上位3業種は同じ

増加傾向の業種

② 原因別の漏えい件数



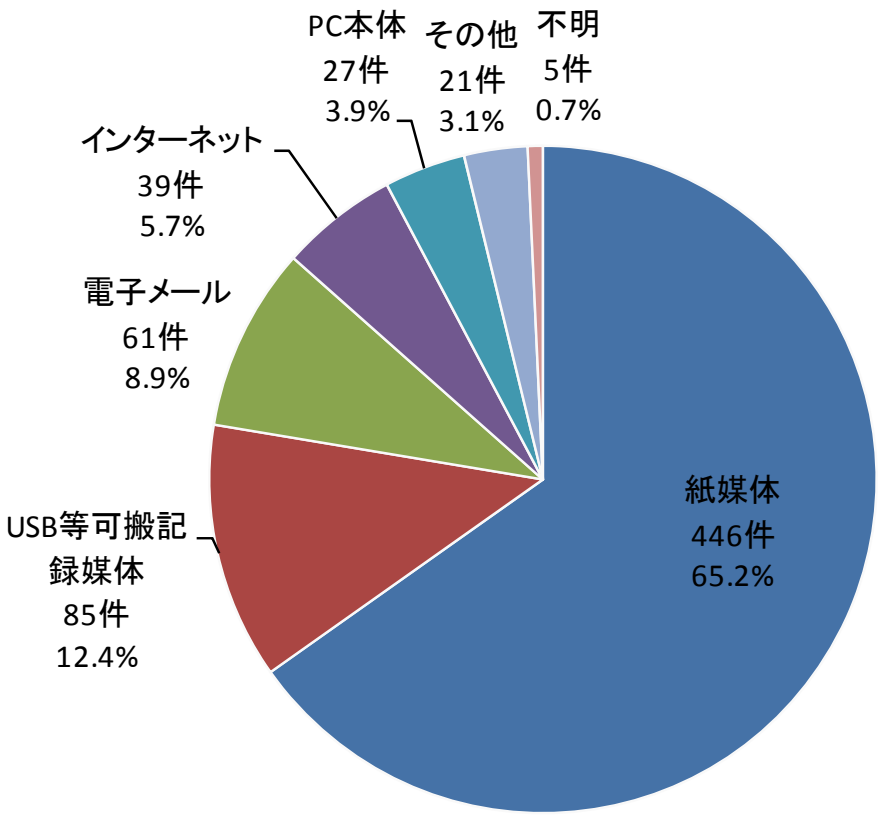
2009年	2010年
管理ミス（784件）	誤操作（255/510件）
誤操作（369件）	管理ミス（205/410件）
紛失・置忘れ（122件）	紛失・置忘れ（95/190件）
盗難（117件）	盗難（54/108件）

誤操作（＝ケアレスミス）
管理ミス（＝誤廃棄）
による漏えいが多い

上位4要因で約90％

多発する要因は、これらの4つで決まり。

③ 媒体別の漏えい件数

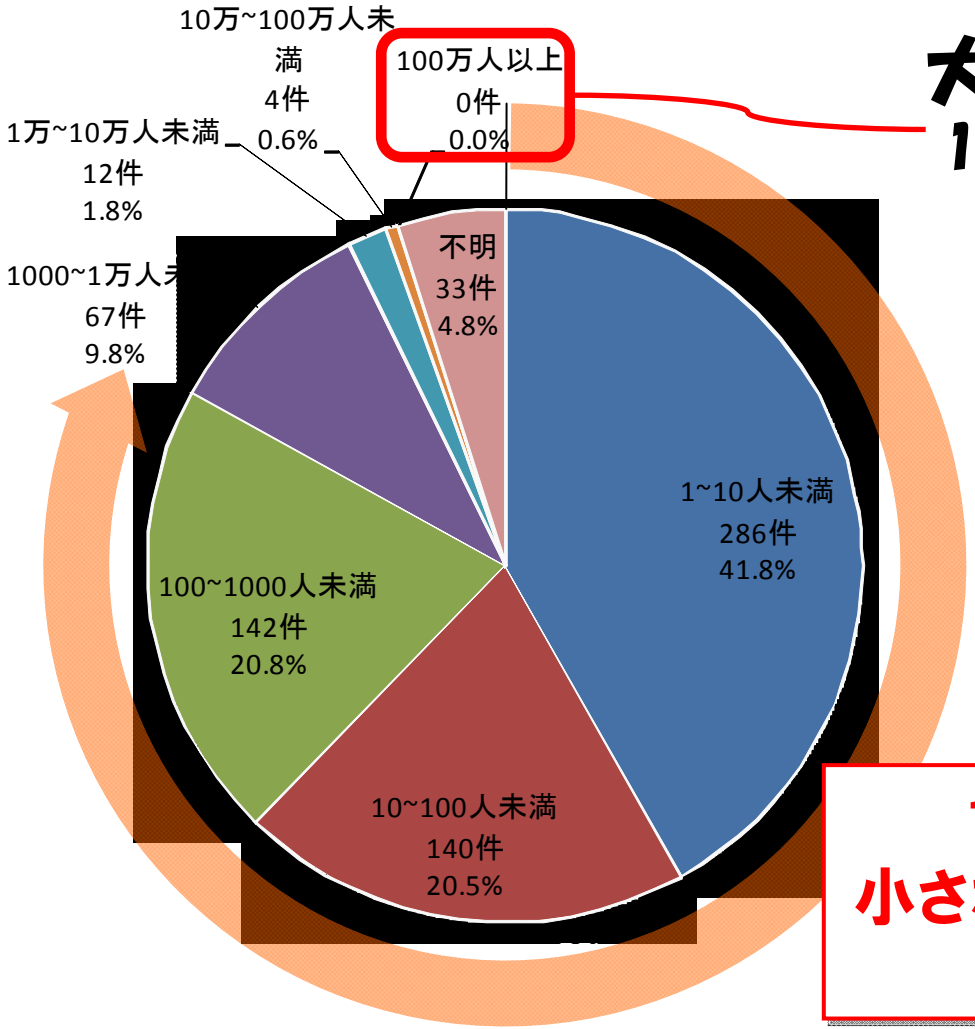


2009年		2010年
紙媒体（1,117件）	→	紙媒体（446/892件）
USB等可搬記録媒体（144件）	→	USB等可搬記録媒体（85/170件）
電子メール（108件）	→	電子メール（61/122件）
インターネット（70件）	→	インターネット（39/78件）

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。

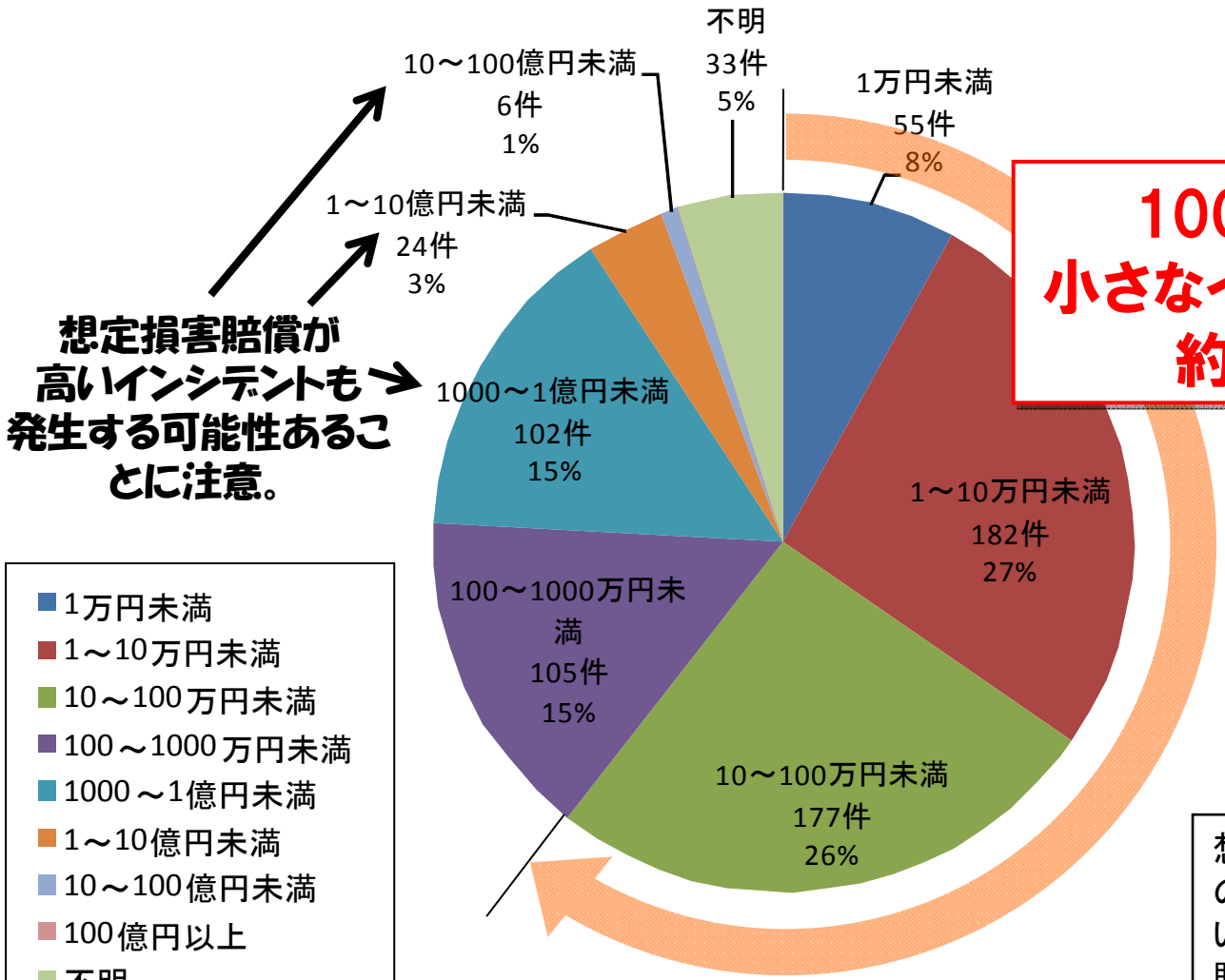
④ 一件当たりの漏えい人数



大事件は起きてない。
100万人を超える大規模な
インシデントの発生なし

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。

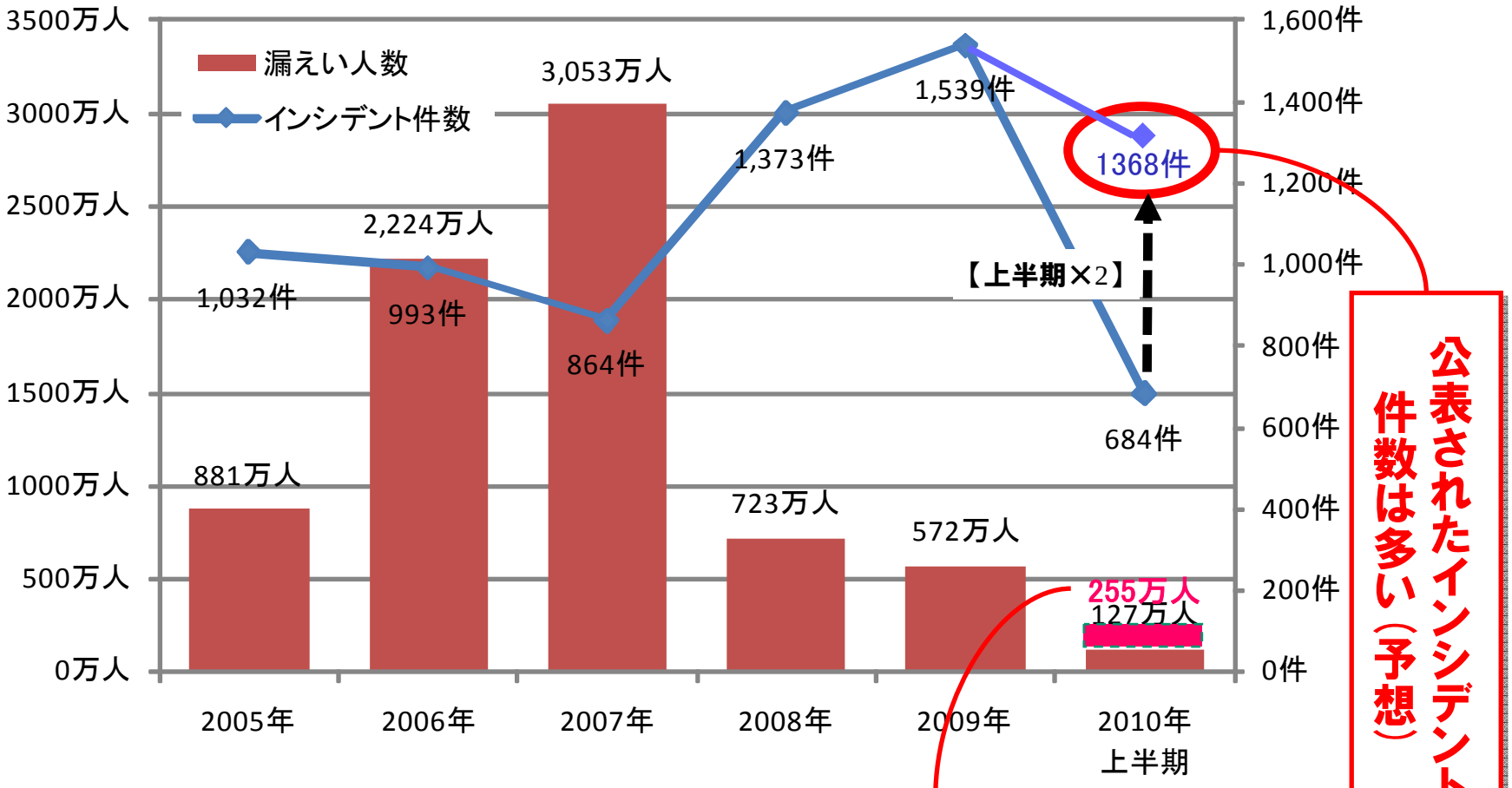
⑤ 一件当たりの想定損害賠償額



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。

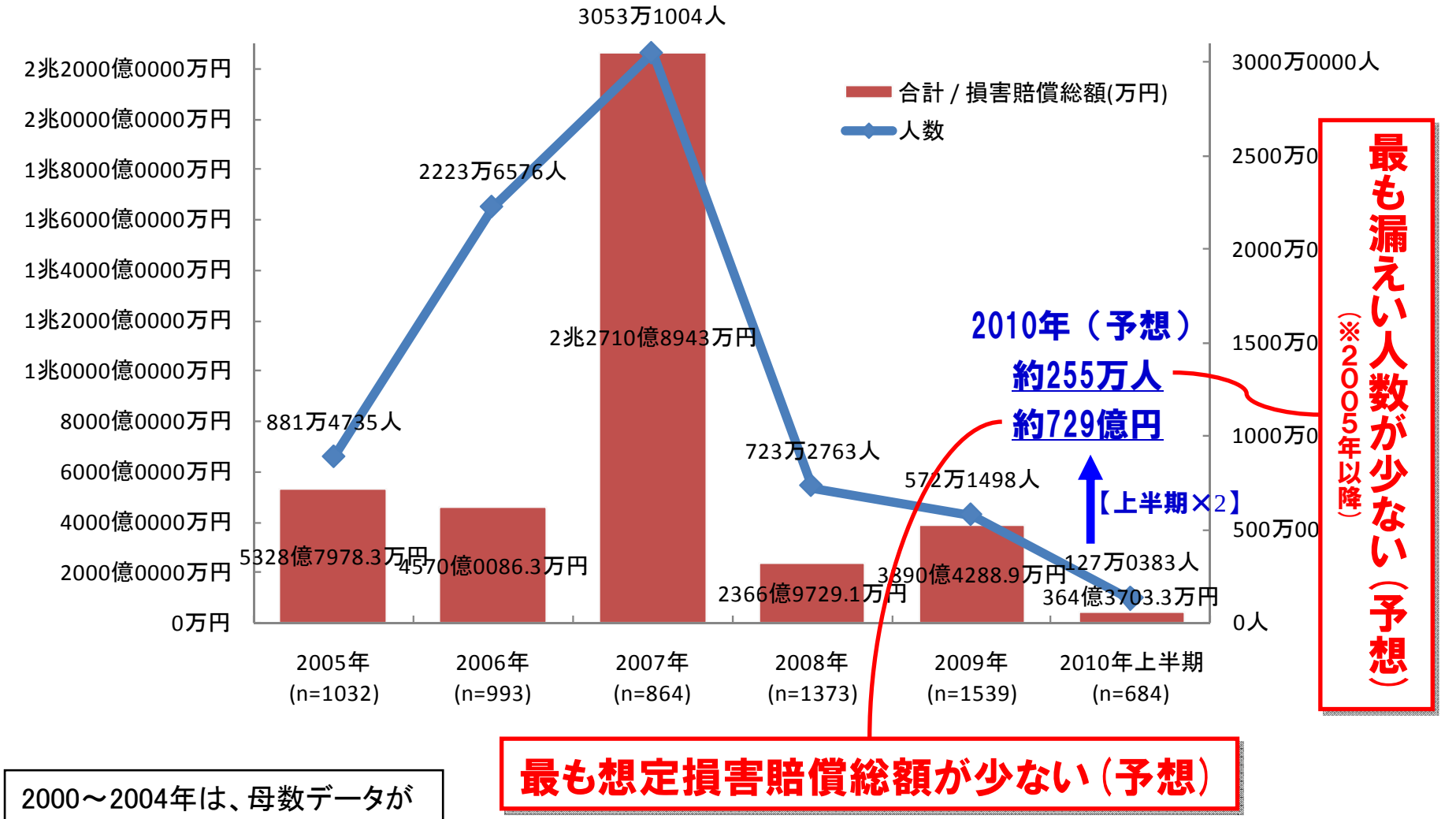
想定損害賠償額は、漏えい人数分の損害賠償額をJOモデルに基づいて算出した金額であり、実際に賠償された金額ではない。

⑥ 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。

⑦ 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。

2010年上半期調査結果より

JNSA

■ **漏えい人数が大幅に減少。**
100万人規模の大規模な個人情報漏えいインシデントが、発生していない。
発生件数に大きな変化はない。偶然発生しなかっただけかもしれない。

■ **想定損害賠償総額が大幅に減少。**
一件当たりの想定損害賠償額が、100億円以上のインシデントが発生しなかった。

■ **漏えい原因に新たな変化（？）**
管理ミスの割合が減少。（※最終判断は、2010年下半期のデータの分析待ち）

- 紛失と盗難の割合は、10%前後で安定か？
- 管理ミス（組織内の紛失、誤廃棄）が減少。誤操作が増加。
- ケアレスミス（誤操作）と内部犯罪・内部犯行へ二極化!?

対策が遅れている

リスク定量化に向けて・・・

JNSA

■ 情報セキュリティインシデントに関する調査
（＝個人情報漏えいの被害額）

インシデントの被害額を推定する手法の
目処が立ってきた。

次は?

**インシデントの発生確率を
知りたい！**

インシデント発生確率調査
結果報告

さて、問題です。

- １年間に電子メールを誤送信する人の確率は、おおよそ【　　】%
- 会社貸与のパソコンを紛失しても報告しない人は、紛失した人のおよそ【　　】人に1人。
- ノートパソコンは、居酒屋よりも【　　】で 紛失しやすい。

答え合わせです。

- １年間に電子メールを誤送信する人の確率は、およそ【 40 】%
- 会社貸与のパソコンを紛失しても報告しない人は、紛失した人のおよそ【　3　】人に1人。
- ノートパソコンは、居酒屋よりも【　社内　】で 紛失しやすい。

はじめに

JNSA

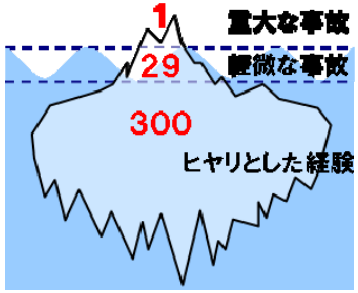
当WGの目的

- 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

情報セキュリティインシデントの発生確率を求めたい！

個人情報漏えいインシデント調査の問題点

- 報道、公表データ中心
  - ⇒組織の公表姿勢によるデータの偏り
- 個人情報の漏えいインシデント中心
  - ⇒個人情報以外の機密情報漏えいの情報不足
  - ⇒情報漏えい以外のインシデントの情報不足
- 組織のインシデント情報の把握状況次第
  - ⇒把握出来ていないインシデントの存在



ハインリッヒの法則

ルールや作業手順など人間が介在する部分が存在するならば、ケアレスミスによって一定数の情報セキュリティインシデントが発生しているのでは？

「情報セキュリティインシデントは0件」と報告しているけど、本当!?

インシデント発生確率調査の目標

JNSA

情報セキュリティインシデントの発生状況を より高い精度で把握したい。

インシデント情報の情報源の問題点
・組織が把握できていないインシデント
・組織の公表姿勢によるデータの偏り

・組織が把握できていない軽微なインシデントの状況の把握
・本音の収集

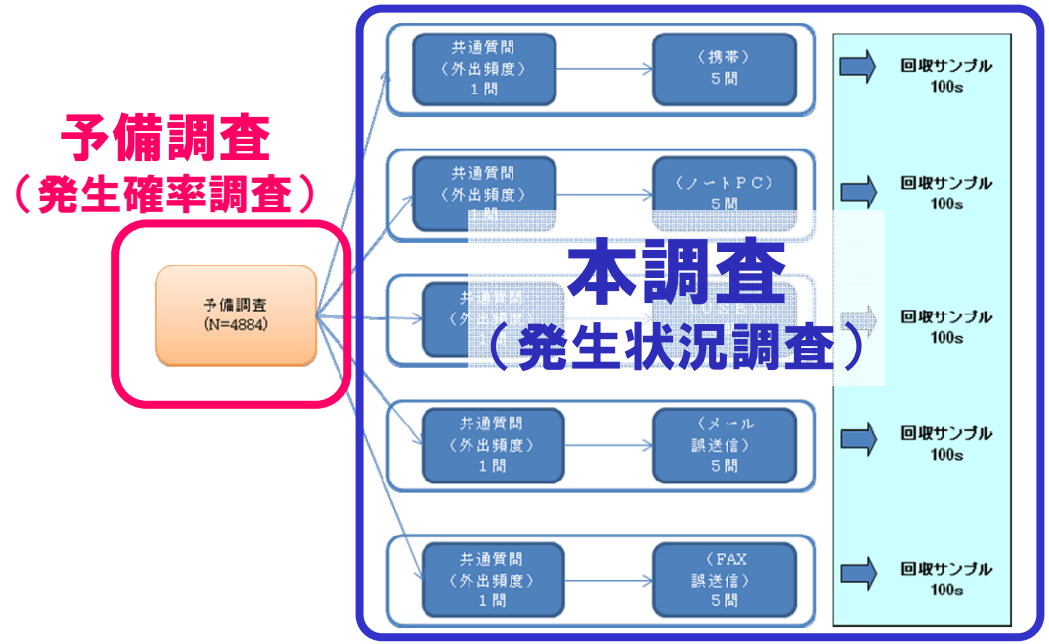
情報セキュリティインシデントの実態を 会社員個人へアンケート調査

2010年度目標
個人に対するアンケート方式による情報収集・分析のトライアルの実施

・調査対象の選択？
・調査結果の有効性？
・データへのニーズ？

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：全国の会社員（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



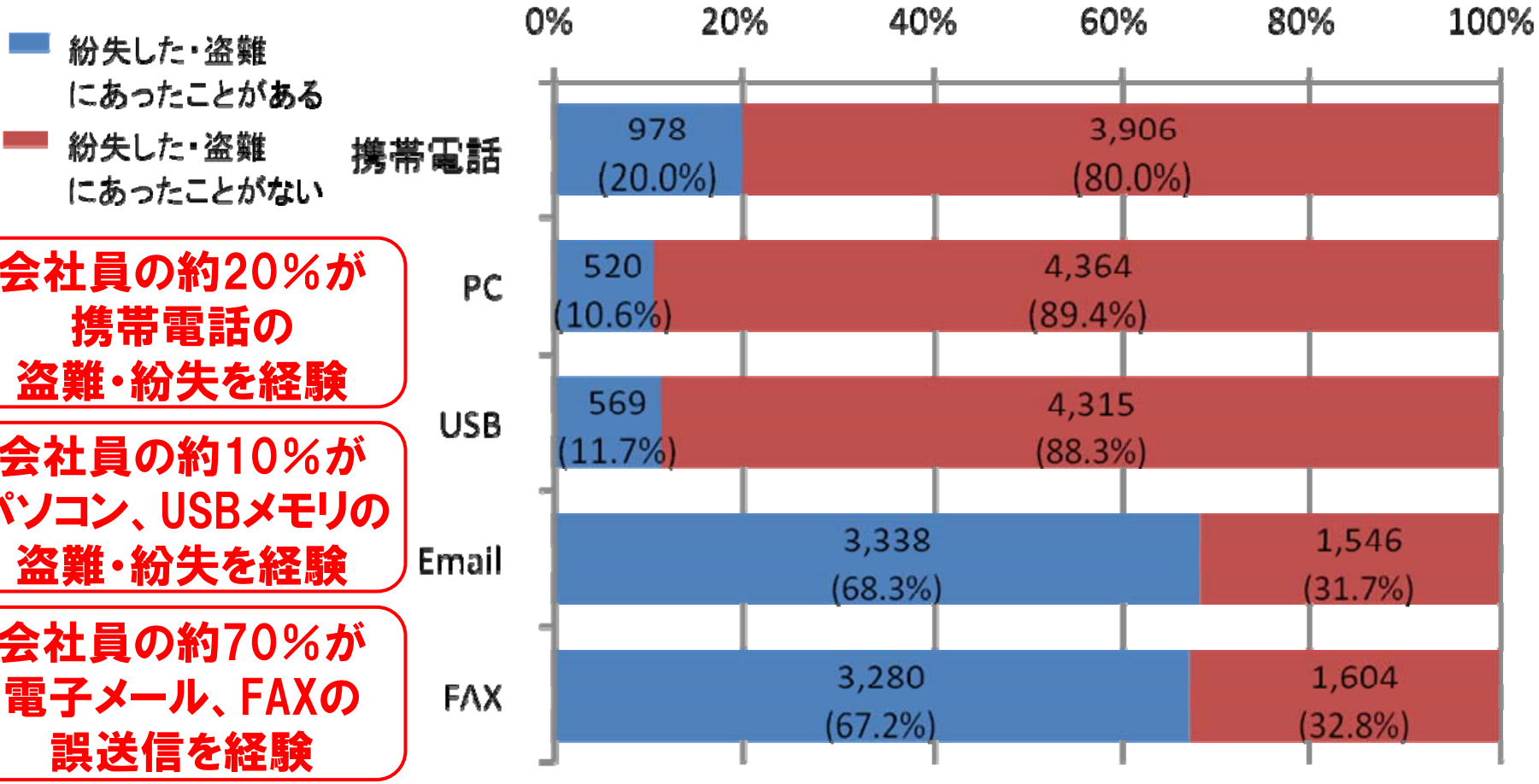
表：職種の内訳

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？



会社員の約20%が携帯電話の盗難・紛失を経験

会社員の約10%がパソコン、USBメモリの盗難・紛失を経験

会社員の約70%が電子メール、FAXの誤送信を経験

紛失・盗難の年間発生確率

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種類の盗難・紛失、誤送信の年間の発生確率を算出。

調査対象	2010年	2009年
携帯電話	6.4%	6.6%
パソコン	3.7%	3.1%
USBメモリ	4.7%	4.1%
電子メール	40.3%	17.1%
FAX	39.0%	12.1%

注) 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。

■携帯電話／パソコン／USBメモリ
- ◆ 紛失した場合、盗難された場合、紛失しそうになった場合（未遂）を含む
- ◆ 私物、会社貸与の両方を含む

■電子メール／FAX
- ◆ 宛先間違い、内容・添付の間違いの両方を含む

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%

※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人とする。

パソコン紛失のリスクは社内にあり!?

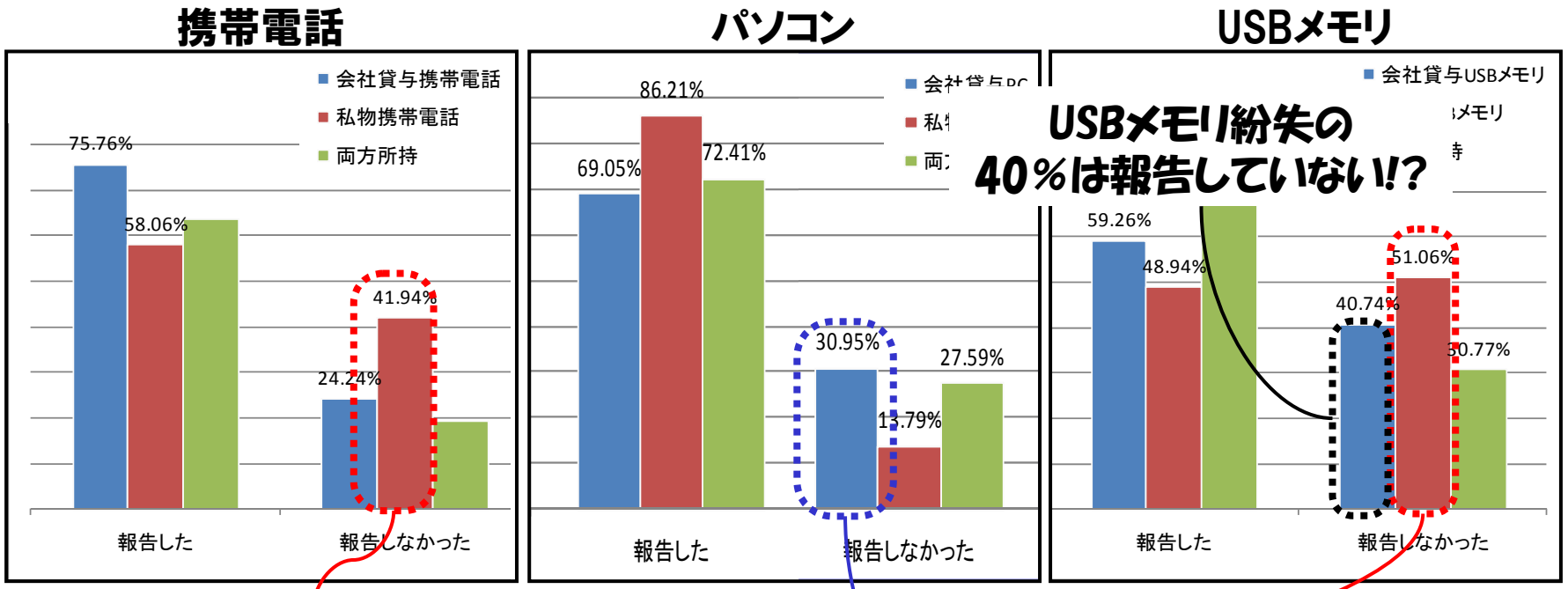
パソコンの紛失・盗難は、どこで、どんな状況で多く発生するのか？

パソコンの紛失・盗難の場所と状況	%
勤務中、社内で無くした	29.0 %
通勤中、勤務で移動中に、タクシー、電車、飛行機などの乗り物に置き忘れた	24.0 %
取引先、出張の宿泊先、セミナ会場など、勤務中に滞在した施設で無くした	14.0 %
自宅、プライベートの出先で無くした。	8.0 %
飲酒して酔っているときに、飲食店、タクシー、電車などの交通機関で無くした	4.0 %
通勤中、勤務中にひったくり、置き引き、車上荒らしなどの盗難にあった	6.0 %
自宅、プライベートの出先で盗難にあった	9.0 %
その他の盗難	2.0 %
いつ、どこで無くなったのか分からない	4.0 %

紛失は居酒屋ではない
社内で起きてるんだ！

紛失・盗難の報告

携帯電話・パソコン・USBメモリを紛失・盗難したら、報告しているか？



（業務に使用している）
私物の携帯電話・USBメモリの
紛失は報告しない傾向がある

会社貸与のパソコンの紛失は
報告しない傾向がある
（3人に1人）

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メモリを紛失・盗難にあった人が、他の紛失・盗難にあっている確率を調査

		全体(N)	会社携帯紛失		会社PC紛失		会社USB紛失		
1	アンケート全体	4,884	184	3.8%	148	3.0%	146	3.0%	← 単独の発生確率
2	業務データが入った会社貸与の携帯電話を紛失した・盗難にあったことがある	184			108	58.7%	102	55.4%	
3	業務データが入った会社貸与のパソコンを紛失した・盗難にあったことがある	148	108	73.0%			97	65.5%	
4	業務データが入った会社貸与のUSBメモリを紛失した・盗難にあったことがある	146	102	69.9%	97	66.4%			

- 携帯電話・パソコン・USBメモリを紛失・盗難にあった人は、50%以上の確率で他の物の紛失・盗難にあっている。
- 会社貸与のパソコンを紛失・盗難にあっている人が、会社貸与の携帯電話の紛失・盗難する確率は70%を超えている。

紛失しやすい人（おっちょこちょい）は存在する

インシデント発生確率調査の結果より

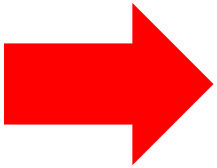
- 携帯電話・パソコン・USBメモリの紛失・盗難、電子メール・FAXの誤送信は、一定の確率で発生している。
  - インシデントの年間発生数が推定可能
  - インシデント対応費用の確保のめやす
- 業務で私物の携帯電話・パソコン・USBメモリが使われている。
  - 業務と個人（プライベート）の分離が不十分
  - 会社貸与・支給の不足
- 電子メール・FAXの誤送信発生確率が高い
  - 電子メール・FAX使用の危険性の認識不足

ケアレスミスが
次の対策のポイント

セキュリティインシデントが発生する要因

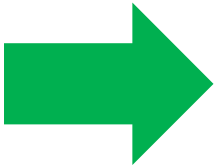
紛失・誤送信のインシデントが発生する要因

- **ケアレスミス(ヒューマンエラー)**
  （誤操作、手違い、ミス）



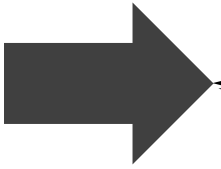
次の対策ポイント

- **意識不足、対策不備**
  （ルールの欠落、無防備）



インシデント削減
（意識向上、
対策普及）

- **内部犯罪・内部不正行為**
  （悪意、怨恨、金銭目的）

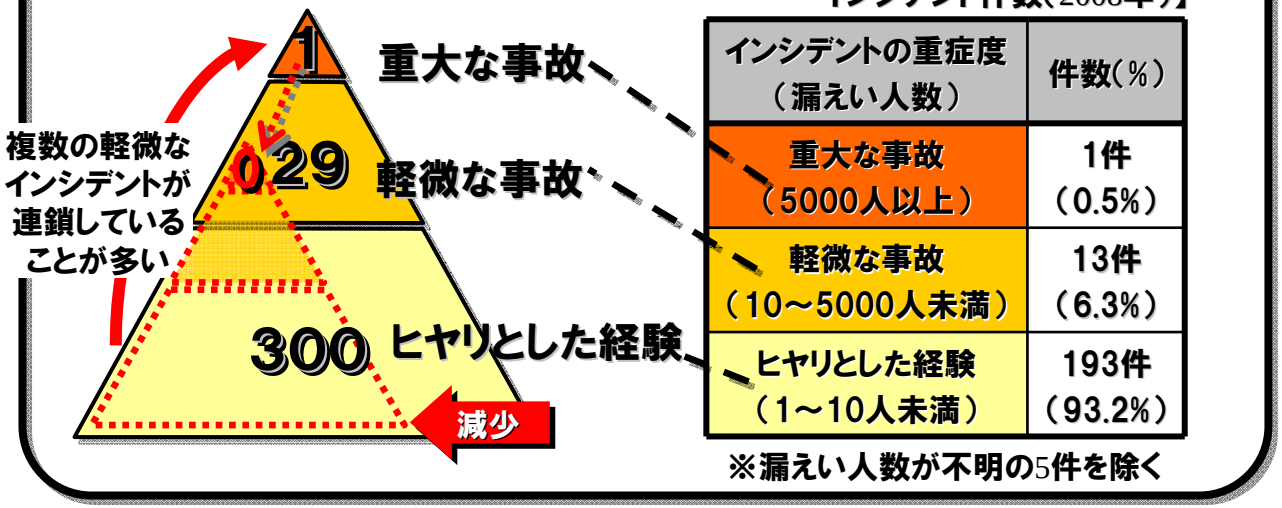


対策が遅れてるポイント

ハインリッヒの法則を考慮した対策

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・・・。

個人情報漏えいにおけるハインリッヒの法則



【表：ある組織の個人情報漏えいインシデント件数（2008年）】

インシデントの重症度（漏えい人数）	件数（%）
重大な事故（5000人以上）	1件（0.5%）
軽微な事故（10～5000人未満）	13件（6.3%）
ヒヤリとした経験（1～10人未満）	193件（93.2%）

※漏えい人数が不明の5件を除く

【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

■ヒヤリとした経験、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

→経験として蓄積されやすい、共有しやすい

2010年度の成果物（予定）

- 2010年 情報セキュリティインシデントに関する調査 【上半期速報版】
- 2010年 インシデント発生確率調査結果書（仮称）

近日、公開予定です。

おたのしみに。