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 2013
【S2 講演】

個人特性とインシデント発生確率の関係

～個人のセキュリティ事故のデータを分析して～

セキュリティ被害調査WG
大谷 尚通 （株）NTTデータ

2013年 1月25日

セキュリティ被害調査ワーキンググループ

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報告書～個人情報漏えい編～』【上半期速報】公開準備中!

『2011年 情報セキュリティインシデントに関する調査報告書～発生確率編～』公開中!

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
	川上　昌俊	株式会社ラック
	北野　晴人	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	リコージャパン株式会社
	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

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～

【上半期速報】

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年上半期 個人情報漏えいインシデント

期間：2012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

	2012年上半期データ	2011年上半期データ（2012年の差分）
漏えい人数	150万7833人	208万5566人（-57万7733人）
漏えい件数	952件	807件（+145件）
想定損害賠償総額	250億4314万円	573億1642万円（-322億7328万円）
一件当たりの漏えい人数	1609人	2667人（-1058人）
一件当たり平均想定損害賠償額	2675万円	7329万円（-4654万円）
一人当たり平均想定損害賠償額	5万9776円	4万1192円（+1万8584円）

※2013年1月時点の速報値です。今後、データが修正される場合がありますが、ご容赦ください

2. 2012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	40万6632人	金融業，保険業	管理ミス
2	17万1518人	情報通信業	不正アクセス
3	11万0000人	サービス業	不正アクセス
4	10万0000人	金融業，保険業	管理ミス
5	8万0000人	運輸業，郵便業	管理ミス
6	3万5694人	医療,福祉	紛失・置忘れ
7	3万0000人	生活関連サービス業,娯楽業	盗難
8	2万7567人	サービス業	設定ミス
9	2万7284人	金融業，保険業	管理ミス
10	2万1764人	金融業，保険業	管理ミス

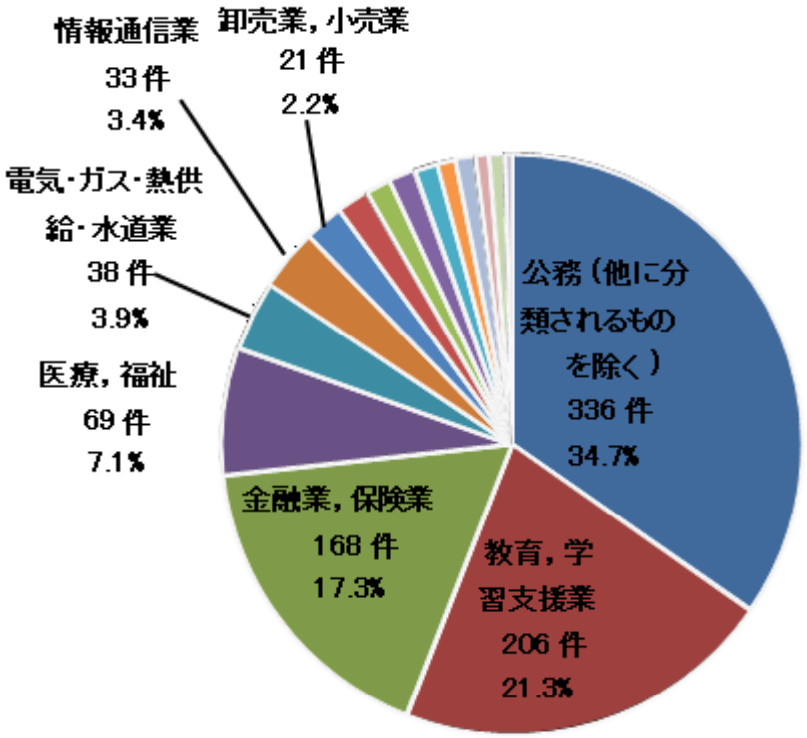
金融業がやや多い。

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）

◎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

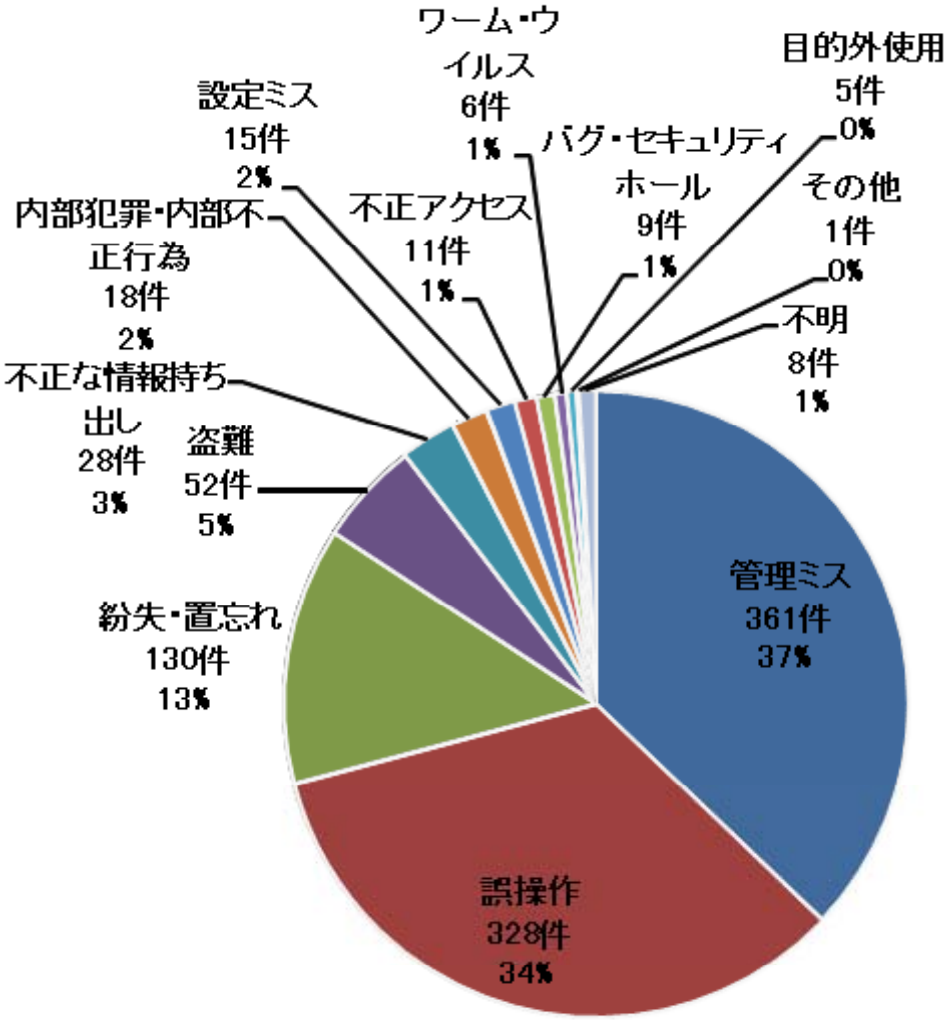
3.1 業種別の漏えい件数



2011年 上半期 (N=807件)		2012年 上半期 (N=972件)
公務（252件）	→	公務（336件）
金融業，保険業（226件）	→	教育，学習支援業（206件）
教育，学習支援業（97件）	→	金融業，保険業（168件）
医療，福祉（48件）	→	医療，福祉（69件）

上位4業種は同じ

3.2 原因別の漏えい件数

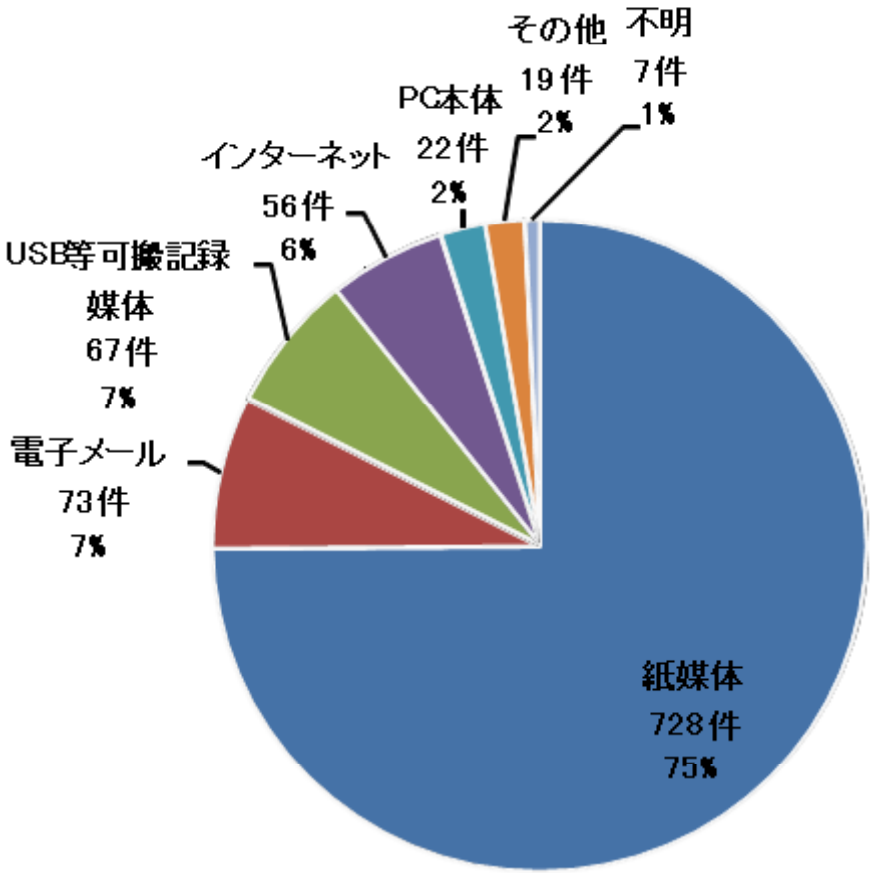


2011年 上半期 (N=807件)		2012年 上半期 (N=972件)
管理ミス (308件)	→	管理ミス (361件)
誤操作 (263件)	→	誤操作 (328件)
紛失・置忘れ (98件)	→	紛失・置忘れ (130件)
盗難 (42件)	→	盗難 (52件)

順位に変化なし

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

3.3 媒体別の漏えい件数

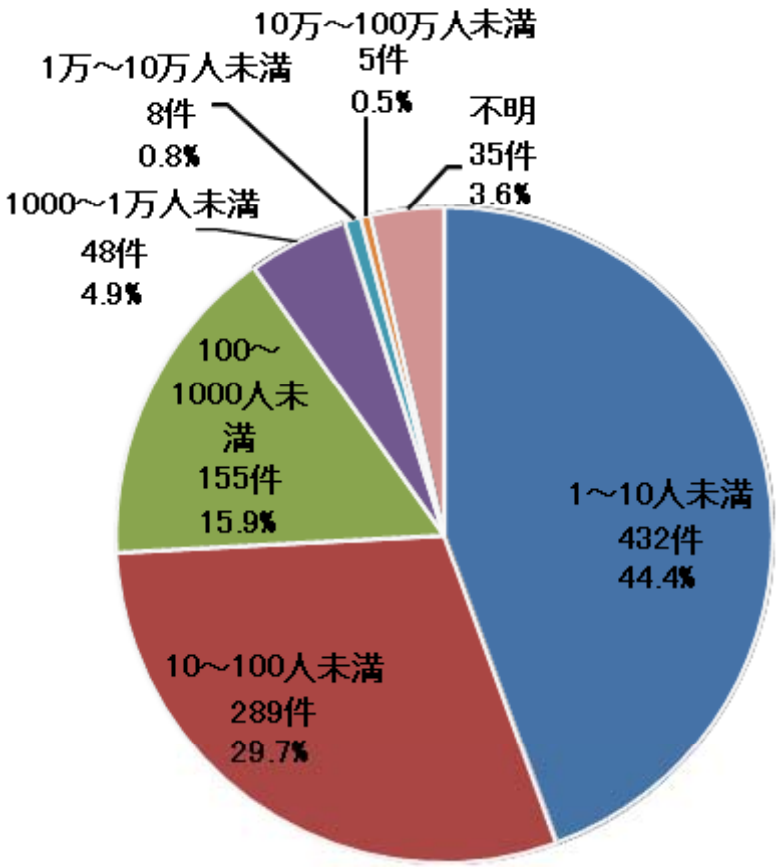


2011年 上半期 (N=807件)		2012年 上半期 (N=972件)
紙媒体 (569件)	→	紙媒体 (728件)
USB等可搬記録媒体 (85件)	→	電子メール (73件)
電子メール (60件)	→	USB等可搬記録媒体 (67件)
インターネット (36件)	→	インターネット (56件)

上位4業種は同じ

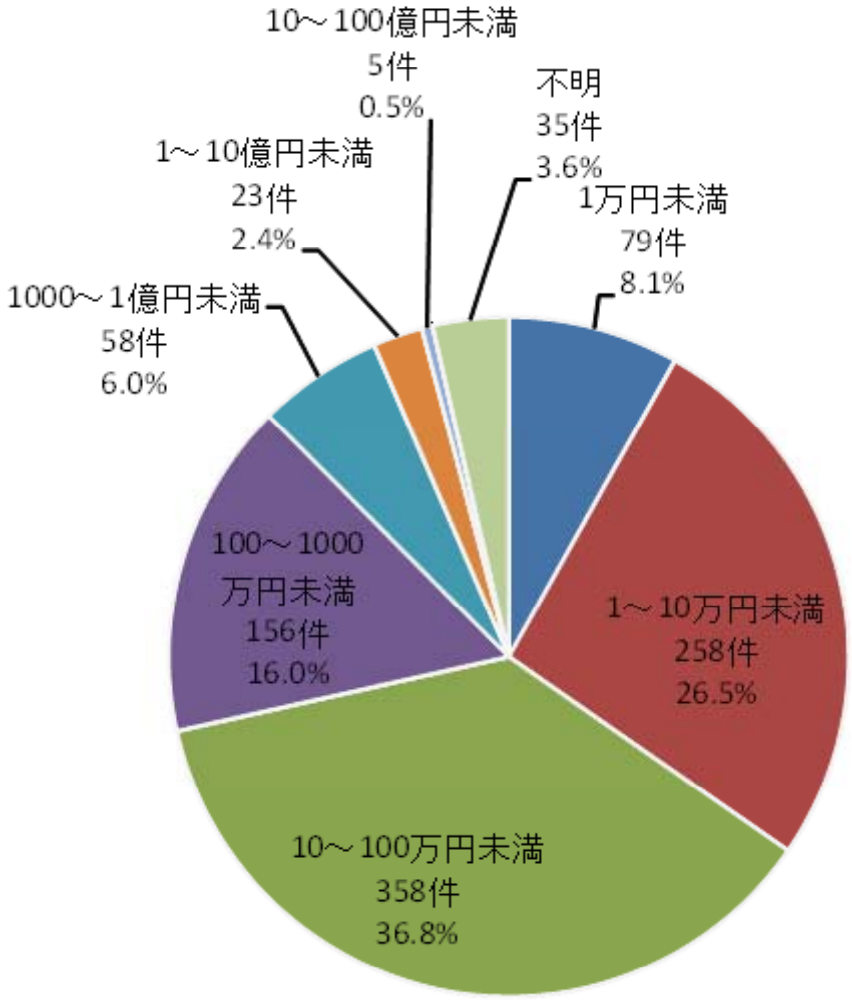
紙媒体による漏えいが多い。（例年通り）

3.4 一件当たりの漏えい人数



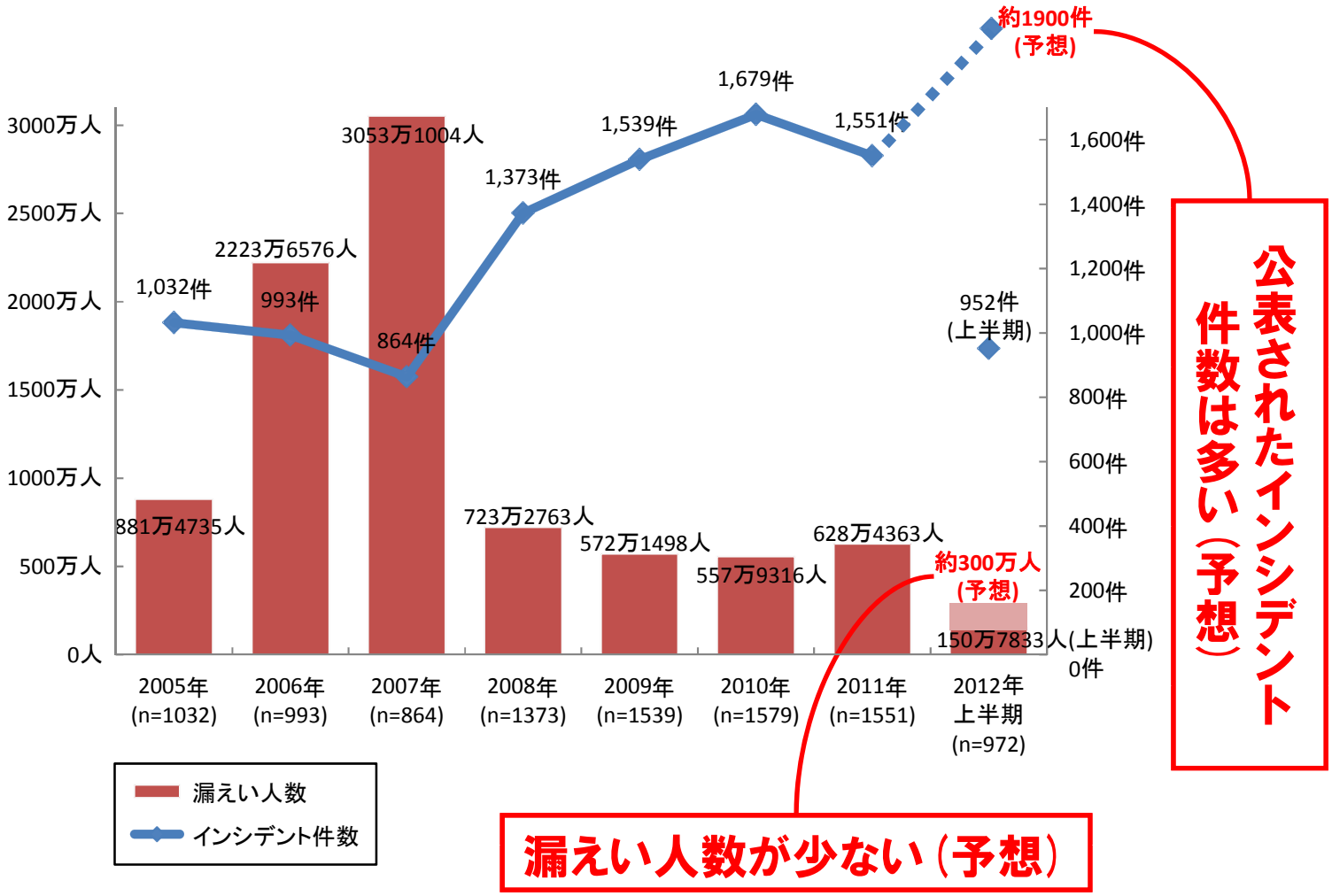
1000人/件未満の
小さなインシデントの件数が
約90%を占める。

3.5 一件当たりの想定損害賠償額

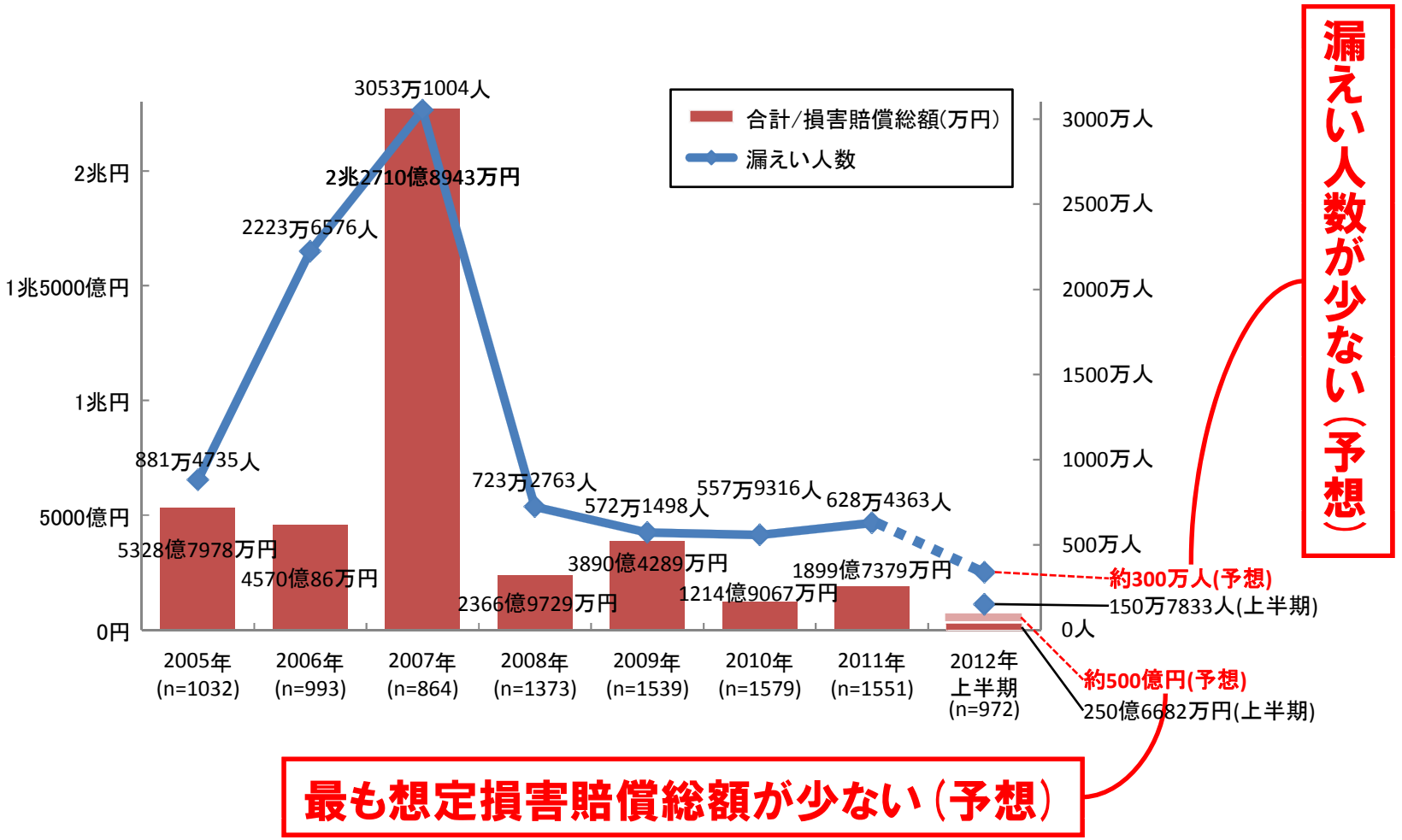


想定損害賠償額が
100万円未満の
小さなインシデントの件数が
約70%を占める。

3.6 漏えい人数と件数(2005～2012年上半期)



3.7 漏えい人数と損害賠償総額 (2005～2012年)



4. 2012年上半期調査結果より

個人情報漏えいインシデント件数(報告件数)は増加中、漏えい人数は減少の傾向が継続中

- 個人情報漏えいインシデントを積極的に報告、公表する姿勢が定着
- 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
- 個人情報漏えいの基本的な対策は、組織・企業へ広く行き渡りつつあると予想

ケアレスミスなどのヒューマンエラーが原因の大半を占めている

- ヒューマンエラー系の原因が、常に上位を占める。ヒューマンエラー系のインシデントは、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
- 「紛失・置き忘れ」の比率が継続的に減少
- 個人情報漏えいの基本的な対策は、組織・企業へ広く行き渡りつつあると予想(再掲)

組織、企業が保有する個人情報の漏えいよりも、個人のスマートフォンからの個人情報の漏えいのリスクが増大中

- 組織・企業の個人情報漏えいの基本的対策は、概ね一定レベルを確保済み
- スマートフォンのOSやアプリの脆弱性を狙ったウイルスの増加
- スマートフォン上の個人情報を狙った不正アプリの流行

組織、企業は、個人情報のセキュリティ対策を継続する

個人は、スマートフォン上の個人情報を守る

2011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～

1. 年間予想被害額の計算式

情報セキュリティインシデントの被害額を計算できますか？

ALE = SLE × ARO

ALE（Annual Loss Expectancy）
情報セキュリティ事故の
年間予想被害額

SLE（Single Loss Expectancy）
個別の情報セキュリティ事故の
予想被害額

ARO（Annual Rate of Occurrence）
1年間の発生確率

SLE = AV × EF
AV = Asset Value（資産価値）
EF = Exposure factor（損失の割合）

業務内容によって
異なるので各自で
用意する。

例えば、
個人情報漏えいのリスクなら
JOモデルで算出可能。

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！

2. 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：2011年1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：2万2340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・紛失と、
電子メールの誤送信、SNSへの書き込みについて調査

予備調査
（発生確率調査）

12問
2万2340人

本調査
（発生状況調査）

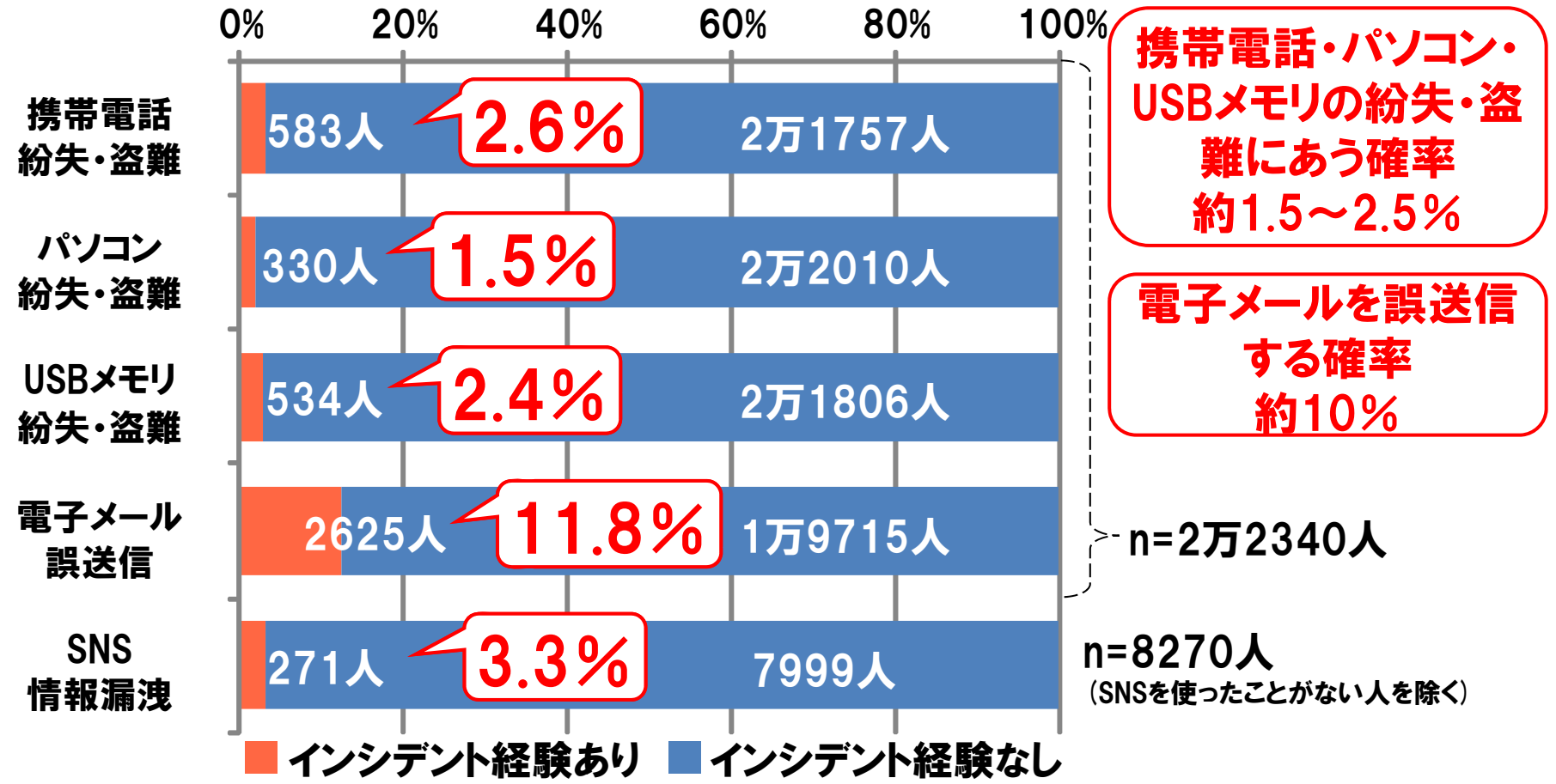
携帯電話、パソコン、
USBメモリ、電子メール
SNS
各5問×100人

表：職種の内訳

職種		人数	%
会社経営者・役員・団体役員		765人	3.4%
会社員・団体職員	正社員	10740人	48.1%
	契約・派遣	1971人	8.8%
地方公務員		953人	4.3%
国家公務員		195人	0.9%
自営業・個人事業主・フリーランス		2804人	12.6%
自由業（開業医・弁護士事務所経営・プロスポーツ選手など）		405人	1.8%
パート・アルバイト・フリーター		4507人	20.2%

3. 情報セキュリティインシデントの発生確率

2011年1年間で、携帯電話／パソコン／USBメモリの紛失・盗難、電子メールの誤送信、SNSへの機密情報漏洩を経験したことがある人は？



3.1 年間発生確率の経年データ

紛失・盗難、誤送信などのインシデントの1年間あたりの発生確率は？

調査対象	2009年 (n=4884)	2010年 (n=4884)	2011年 (n=22340)
携帯電話	(6.6%)	(6.4%)	2.6% (3.8%)
パソコン	(3.1%)	(3.7%)	1.5% (2.4%)
USBメモリ	4.1%	4.7%	2.4%
電子メール	17.1%	40.3%	11.8%
FAX	12.1%	39.0%	–
SNS	–	–	3.3%

■年1回以上、インシデントを経験した人の割合。1年間に複数回あった人も1人としている。
■カッコの中の数値は、しそうになった人も含んだ場合の確率
■2009、2010年の調査値は、推測値

2011年の調査は、2010年と比べて、数値がやや変化した。
- **質問の表現や調査項目をわかりやすくした**
- **回答人数が大幅に多い**

⇒数値の精度は向上したと予想

3.2 職種と年間発生確率の分析

JNSAへいただいた質問：
組織に所属している人（いわゆるサラリーマン）とそれ以外の職種の間において、インシデント発生確率の違いがあるか？

回答者の職種 ＼ 情報セキュリティインシデント			携帯電話を紛失した・盗難にあったことがある（%）		パソコンを紛失した・盗難にあったことがある（%）		USBメモリを紛失した・盗難にあったことがある（%）		電子メールを誤送信したことがある（%）		ブログ・SNS・ツイッターで、業務上の秘密に関する情報や不適切な内容を書いてしまったことがある（%）	
会社経営者・役員・団体役員	組織に属している就業者（65.5%）	3.4%	4.2%	3.1%	1.7%	1.9%	3.7%	3.0%	18.3%	14.4%	3.9%	3.8%
会社員・団体職員（正社員）		48.1%	3.3%		2.0%		3.2%		15.8%		4.1%	
会社員・団体職員（契約・派遣）		8.8%	1.8%		1.1%		1.4%		9.1%		1.9%	
地方公務員		4.3%	2.2%		2.3%		2.5%		7.2%		4.6%	
国家公務員		0.9%	3.1%		2.6%		3.6%		11.3%		5.4%	
自営業・個人事業主・フリーランス		12.6%	2.5%		0.8%		1.7%		9.7%		2.4%	
自由業（開業医・弁護士事務所経営・プロスポーツ選手など）		1.8%	3.0%		2.7%		3.0%		13.1%		3.2%	
パート・アルバイト・フリーター		20.2%	1.1%		0.5%		0.9%		4.2%		2.1%	
全体		**100%**	**2.6%**		**1.5%**		**2.4%**		**11.8%**		**3.3%**	

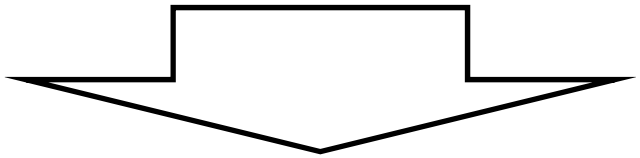
4. 個人特性と インシデント発生確率 の関係

4.1 個人特性と発生確率の関係

個人の知識や行動、性格とインシデントの発生に注目!

【仮説（例）】

■情報セキュリティの知識がある人は、情報漏えいなどのインシデントをおこしにくい
■忘れ物をしやすい人は、携帯電話やUSBメモリなどを紛失しやすい
■おっちょこちょいな人は、メールを誤送信しやすい　・・・等



2011年の調査では、以下に関する質問を追加して調査した。

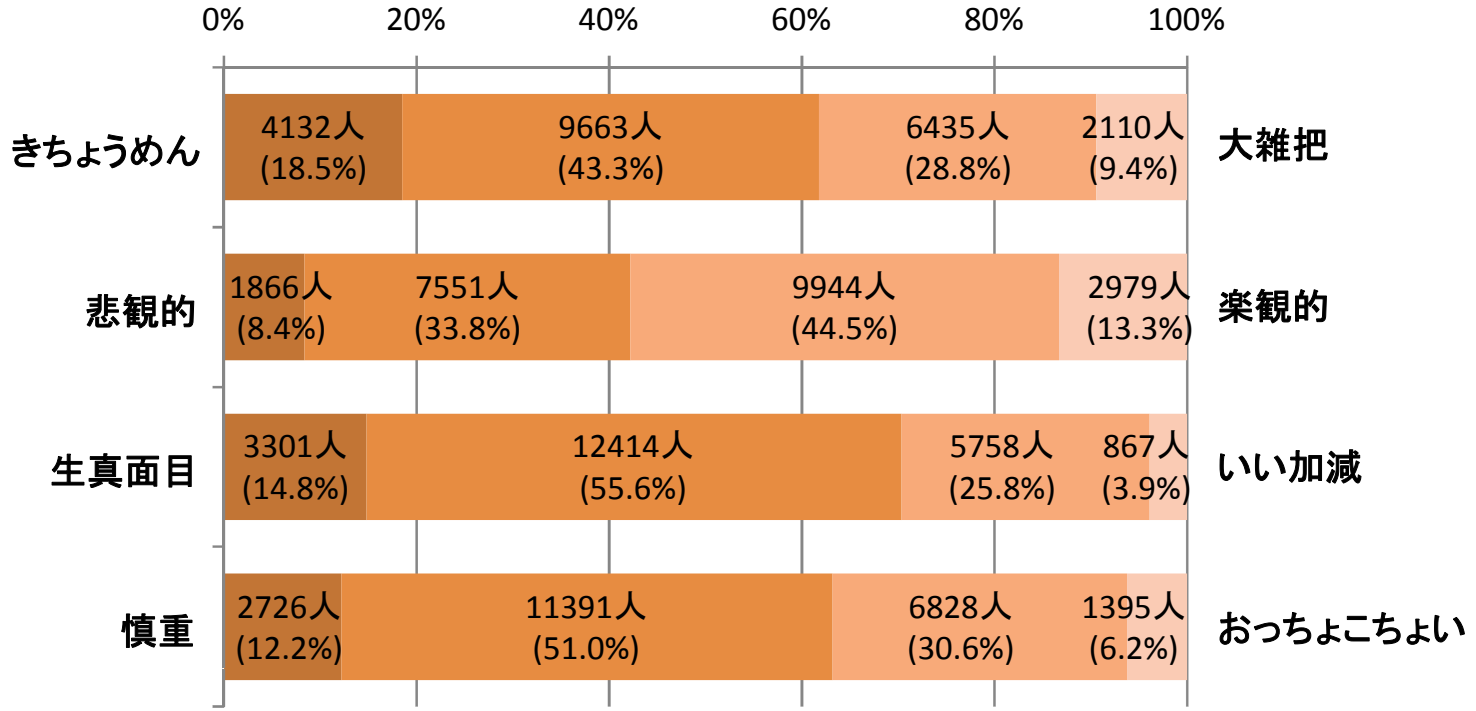
性格　**行動**　**情報セキュリティ知識**

4.2 性格に関する質問（4問）

『人の性格をあらわす以下の言葉の中から、あなた自身の性格にもっとも近いと思う選択肢を選んでください。』

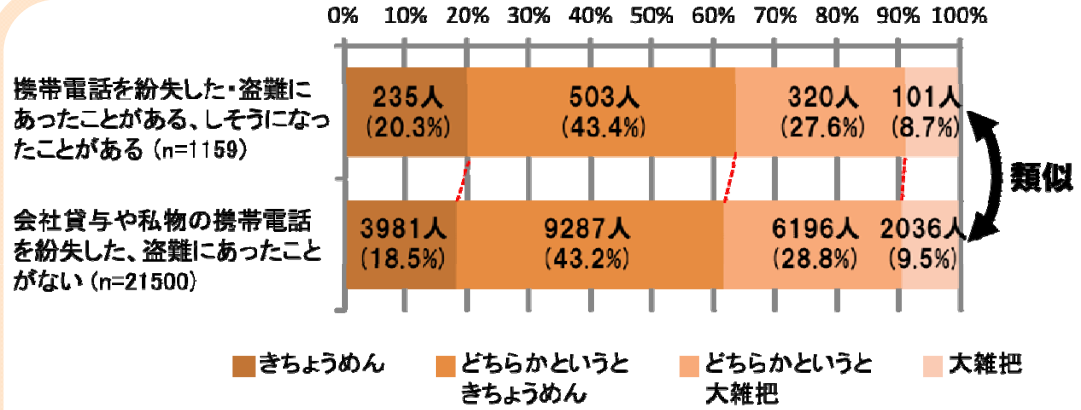
■ きちょうめんな/大雑把な　■ 悲観的な/楽天的な
■ 生真面目な/いい加減な　■ 慎重な/おっちょこちょいな

【仮説】
おっちょこちょいな人は、
メールを誤送信しやすい



【性格に関する質問の回答 (N=22340)】

4.2 性格と発生確率の関係



携帯電話の紛失・盗難の経験があるグループと経験がないグループは、
きちょうめん／大雑把な性格による違いがない。

調査した性格の例
- きちょうめんな／大雑把な
- 悲観的な／楽天的な
- 生真面目な／いい加減な
- 慎重な／おっちょこちょいな

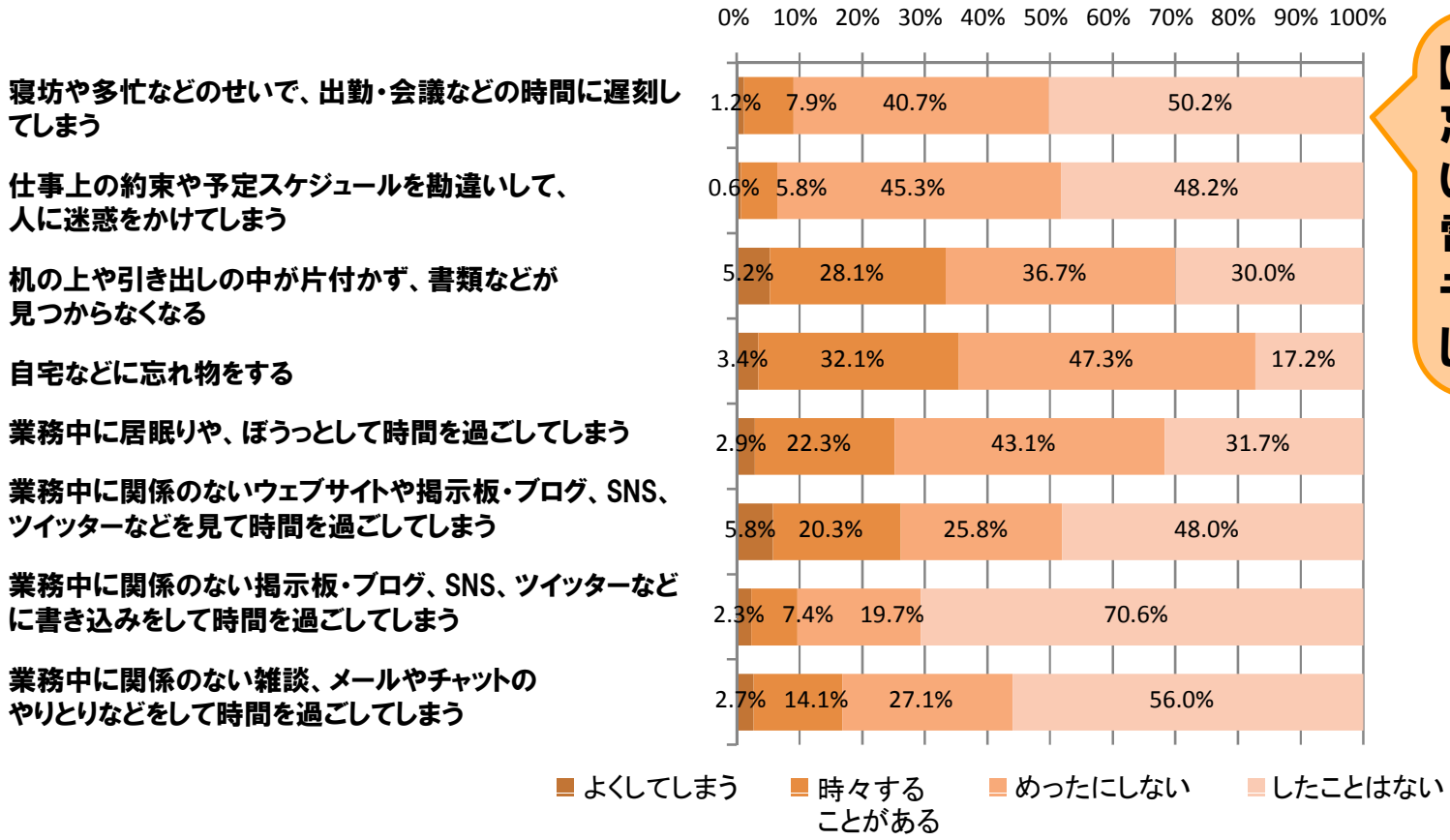
■ 携帯電話／パソコン／USBメモリの紛失・盗難事故、電子メールの誤送信、SNSでの機密情報漏えいと調査した性格の間には、**顕著な関係が見つからなかった。**

【仮説】
おっちょこちょいな人は
メールを誤送信しやすい
NG

セキュリティ事故の発生と性格は関係性が低い

4.3 行動に関する質問（8問）

『あなた自身は普段、仕事中に以下のようなうっかりした失敗をしてしまうことは、どれくらいありますか。』



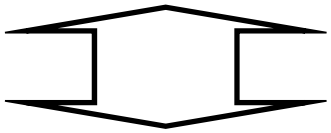
【仮説】
忘れ物をしやすい人は、携帯電話やUSBメモリなどを紛失しやすい

【行動に関する質問の回答 (N=22340)】

4.3 行動と発生確率の関係①

■携帯電話の紛失・盗難の経験があるグループと経験がないグループは、以下の4つの行動に関して顕著な違いがある。

- 『遅刻』　寝坊や多忙などのせいで、出勤・会議などの時間に遅刻してしまう
- 『約束の勘違い』仕事上の約束や予定スケジュールを勘違いして、人に迷惑をかけてしまう
- 『SNS書き込み』業務中に関係のない掲示板・ブログ、SNS、ツイッターなどに書き込みをして時間を過ごしてしまう
- 『雑談』　業務中に関係のない雑談、メールやチャットのやりとりなどをして時間を過ごしてしまう



■携帯電話の紛失・盗難の経験があるグループと経験がないグループの間には、以下の4つの行動に関して顕著な違いがない。

- 『整理整頓』　机の上や引き出しの中が片付かず、書類などが見つからなくなる
- 『忘れ物』　自宅などに忘れ物をする
- 『居眠り』　業務中に居眠りや、ぼうっとして時間を過ごしてしまう
- 『ウェブサーフィン』業務中に関係のないウェブサイトや掲示板・ブログ、SNS、ツイッターなどを見て時間を過ごしてしまう

4.3 行動と発生確率の関係②

■パソコン、USBメモリ、電子メール、SNSも、携帯電話と
同じ4つの行動について、事故の経験があるグループと経験がない
グループの間に顕著な違いがあった。

4つの行動
『遅刻』『雑談』
『約束の勘違い』
『SNS書き込み』

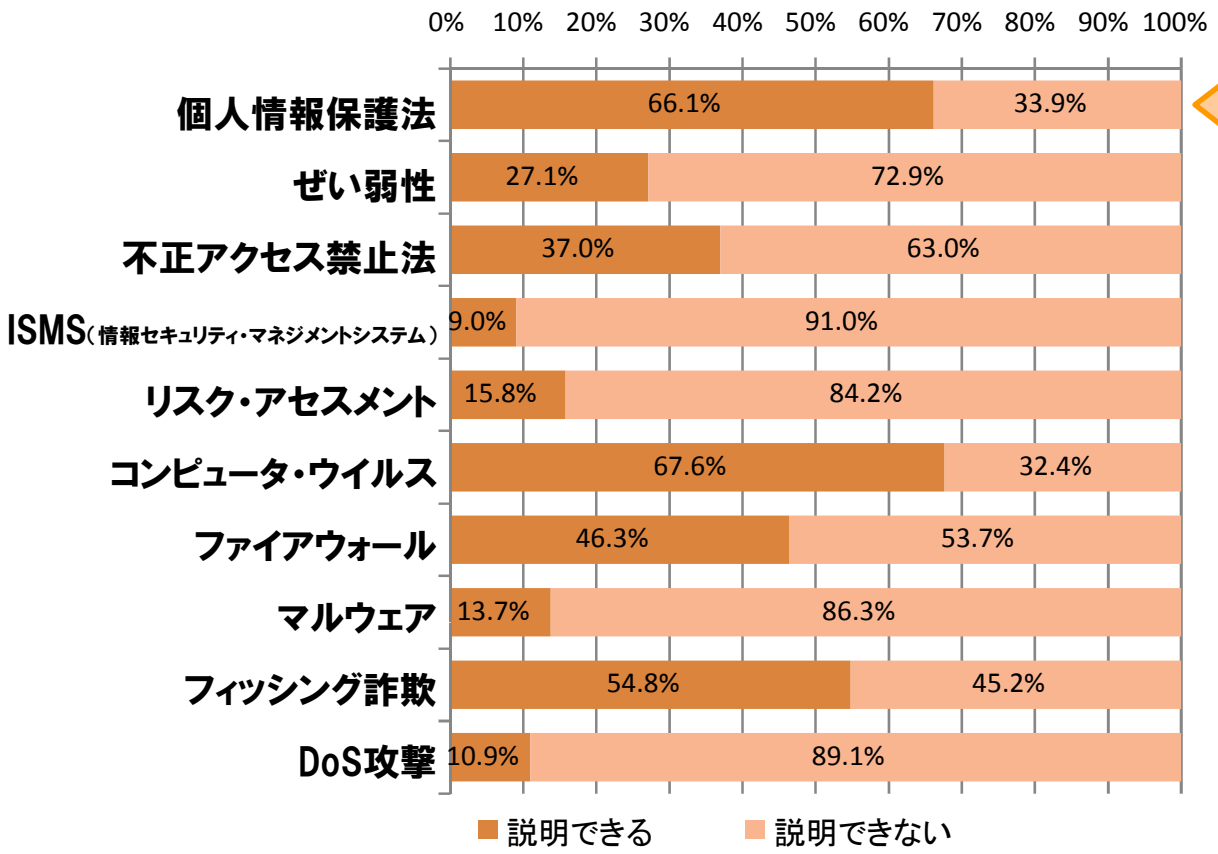
『遅刻』『雑談』『約束の勘違い』『SNS書き込み』の
行動とる人は、行動しない人に比べて
事故を起こす確率が高い

【仮説】
忘れ物をしやすい人は、
携帯電話やUSBメモリ
などを紛失しやすい

**情報セキュリティ事故の発生と
特定の行動は、関係性が高い**

4.4 知識に関する質問（10問）

『あなたは、情報セキュリティやITに関する以下の言葉について、他人に大まかな説明ができるくらいに知っていますか。』

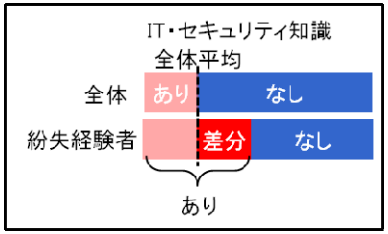


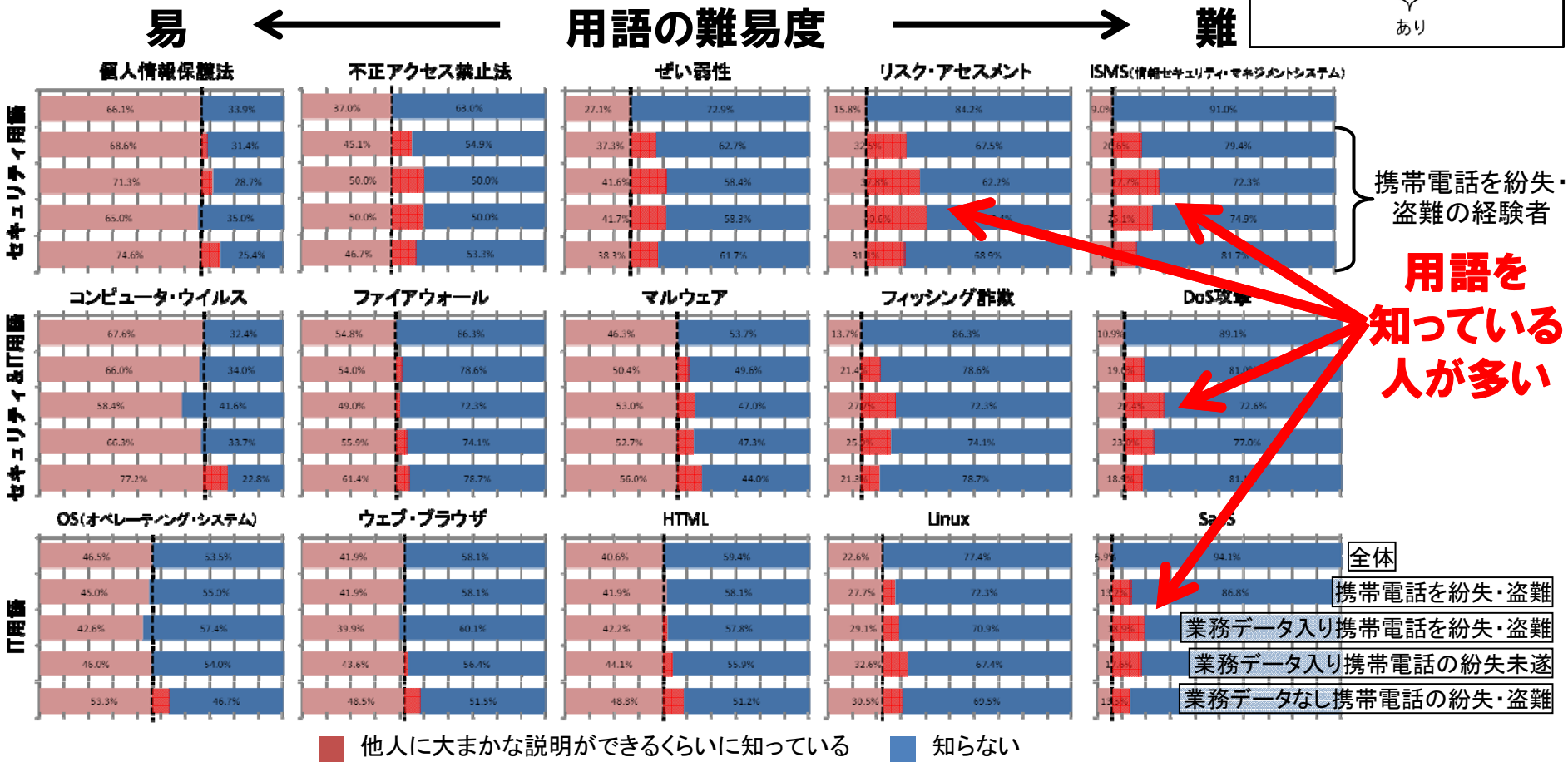
【仮説】
情報セキュリティの知識がある人は、情報漏洩などのインシデントをおこしにくい

【知識に関する質問の回答 (N=22340)】

4.4 知識とセキュリティ事故の関係①

IT/セキュリティ知識を持っている人のほうが、
携帯電話の紛失・盗難の経験者の割合が高い

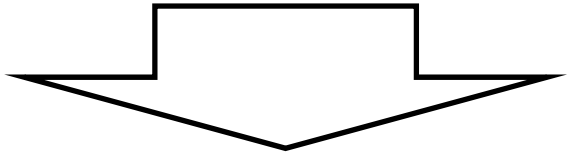




4.4 知識とセキュリティ事故の関係②

IT/セキュリティ知識を持っている人のほうが、
パソコン、USBメモリも紛失・盗難の経験者の割合が高い

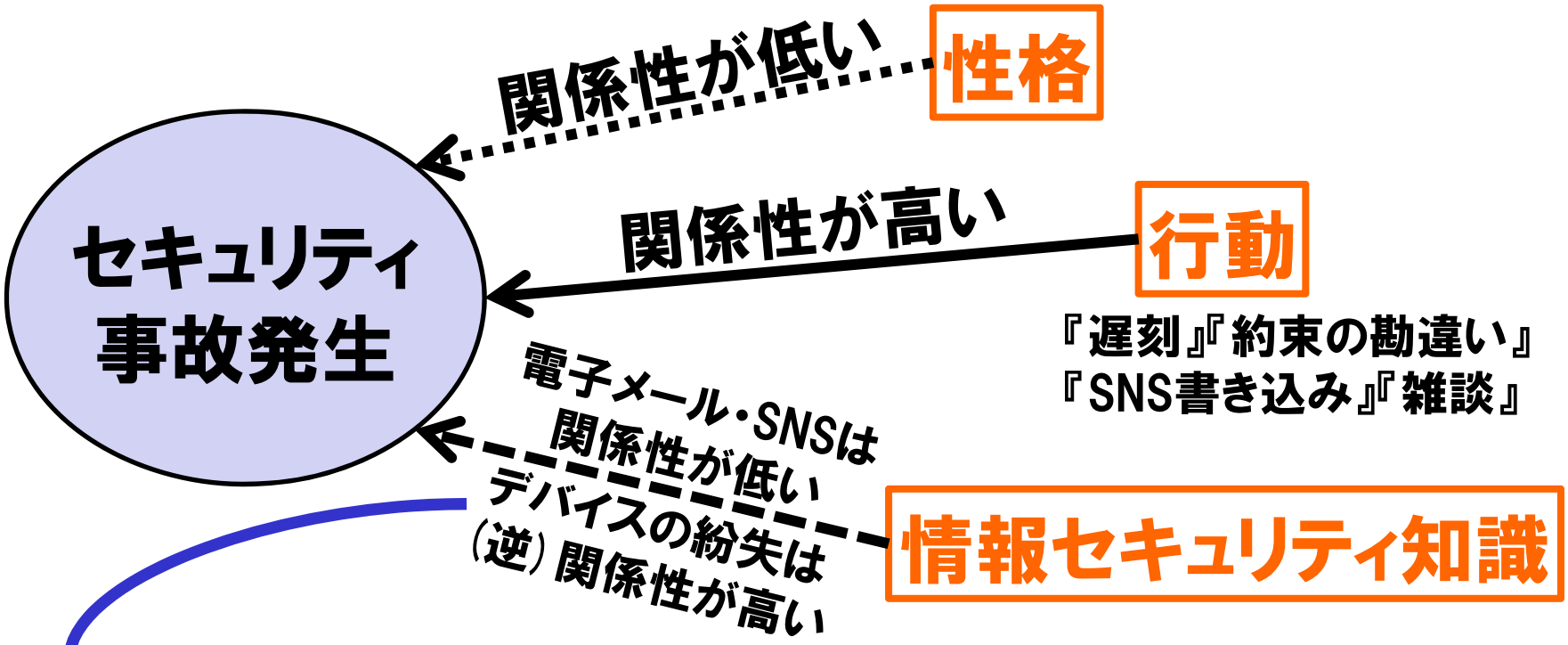
電子メールの誤送信、SNSへの機密情報の書き込みは、
IT/セキュリティ知識と経験者の割合の関係性が低い



IT/セキュリティ知識を持っている人のほうが、
デバイスの紛失・盗難の確率が高い

電子メールの誤送信、SNSへの機密情報の書き込みは、
IT/セキュリティ知識との**関係性が低い**

4.5 個人特性との関係 まとめ①



- 情報セキュリティ知識を持っていると、リスクを回避できると思い込んで、リスクが高い状況へ踏み込んでしまうおそれ
- 情報セキュリティインシデントが発生する確率の高い仕事をしている人々は、教育により、必ずIT知識や情報セキュリティ知識を持っている

4.5 個人特性との関係 まとめ②

セキュリティ事故を起こしやすい人を判断できるか？

- ■性格（=内面性）からの判断は難しい
- ■行動（=客観的）は、判断の手がかりになる
- ■知識はITの活用率・依存度と関係する

例）上記の行動が、あてはまる人は、注意しよう！

周囲の人が対象者の行動を客観的に把握し、注意を払う

知識があるだけでなく、行動が伴わなければ意味がない。

情報セキュリティ教育：
× 漠然とした禁止事項や表面的な知識
○ 具体的な対策を実行できるレベルの知識