

JNSA 2015年度 活動報告会

【調査研究部会】

セキュリティ被害調査WGの 調査報告と 今後の活動方針について

セキュリティ被害調査WG

**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**

大谷 尚通 (株)NTTデータ

2016年 6月17日

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

1. 個人情報漏えいインシデント 調査データ (2002年～2014年)

1.1 個人情報漏えいインシデントデータ（13年分）

期間：2002年1月1日～2014年12月31日（13年間分）
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

	2002年～2014年 総計
漏えい件数	1万4798件
漏えい人数	1億6815万6124人
想定損害賠償総額	6兆7043億1922万円

1.2 個人情報漏えいインシデントデータ（13年分）

期間：2002年1月1日～2014年12月31日（13年間分）
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

	平均データ（13年分）
漏えい件数	1138件
漏えい人数	1293万5087人
想定損害賠償総額	5157億1686万円
一件当たりの漏えい人数	1万1923人
一件当たり平均想定損害賠償額	4億7535万円
一人当たり平均想定損害賠償額	4万4897円

1.3 インシデントデータの集計/分析の目的 **JNSA**

個人情報漏えいインシデント 集計データからわかること

組織から個人情報漏えいするインシデントが発生した場合

- 一件当たりの漏えい人数 = **1万1923人**
- 個人情報1件あたり想定損害賠償額 = **4万4897円**
- インシデント1件あたり想定損害賠償額 = **4億7535万円**

※ 想定損害賠償額は、あくまでも「もし被害者全員が賠償請求したら」という“仮定”に基づくもの

※ 被害者が漏洩元の組織に対して請求できる損害賠償額を示したものではない

一組織では、すぐに求めることが難しいデータ

データ提供

インシデントの特徴や賠償額(リスク)から 個人情報漏えい対策の方針や投資判断のめやす

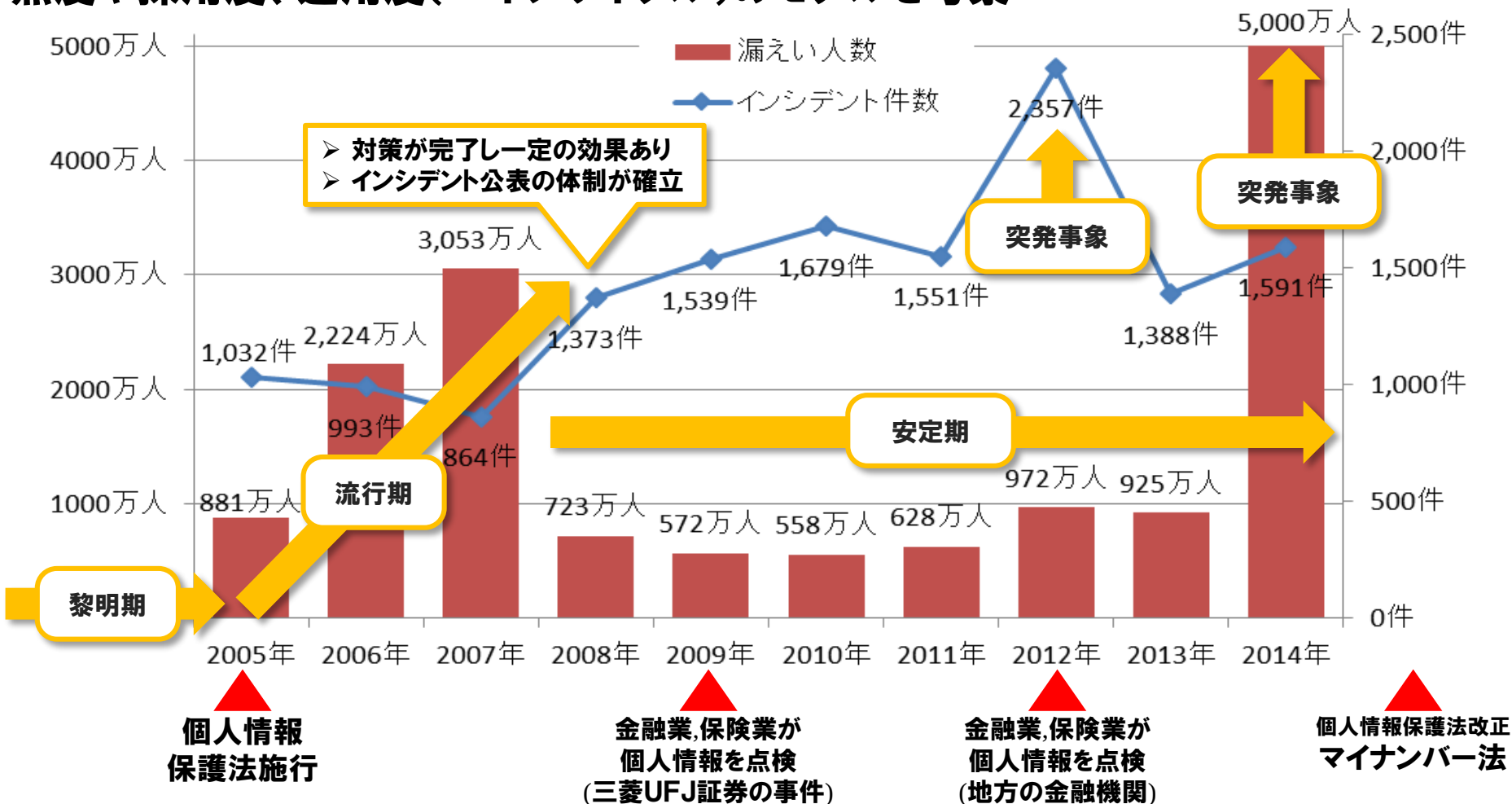
1.4 個人情報情報漏えいインシデント年表

個人情報情報漏えい対策に大きな影響を与えた注目されたインシデント

年	企業名	漏えい人数	原因	特徴
1999年	宇治市	22万人	内部犯	初めて損害賠償請求の裁判が行われた
2002年	TBC	3.7万人	設定ミス	身体的特徴を含む個人情報の漏えいして裁判で高額な賠償額が決定した
2003年	ローソン	56万人	その他	初めて被害者へお見舞金500円相当の引換券を配布した
2003年	ファミリーマート	18万人	不明	コンビニ会員情報の漏えいが相次ぎ、会員情報の管理の必要性を認識
2004年	Yahoo BB	452万人	内部犯	大規模な内部犯の事例。被害者を募って裁判を実施
2004年	ジャパネットたかた	51万人	内部犯	個人情報漏えい発覚時に再発を懸念して、サービスを全面停止した
個人情報保護法施行				
2007年	大日本印刷	864万人	内部犯	大規模な内部犯の事例
2009年	三菱UFJ証券	149万人	内部犯	高権限者による内部犯。お見舞金、事業損失、犯人への賠償請求が高額
2011年	ソニー(※)	7700万人	不正アクセス	攻撃者が特定組織を狙って不正アクセスし、個人情報の漏えいに成功した
2014年	ベネッセ	4858万人	内部犯	国内過去最大の個人情報の漏えい。技術的対策の隙を突いた内部犯
2015年	日本年金機構	101万人	不正アクセス	公的組織を狙った不正アクセス。個人情報を詐取された
マイナンバー法施行				

1.5 漏えい人数と件数の経年変化の特徴

インシデント件数と人数等の経年変化から、個人情報漏えいインシデント対応の成熟度や採用度、適用度(ハイプサイクル)のモデルを考察



2. 2014年 個人情報漏えい インシデント調査結果

**本日 6/17 午後
報告書を公開**

JNSA会員には、報告書 (Word版)、インシデント一覧データ (Excel) を提供

2.1 2014年 個人情報漏えいインシデント

期間:2014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

	2014年	年平均比較
漏えい件数	1591件	+453件
漏えい人数	4999万9892人	+3706万4805人
想定損害賠償総額	1兆6642億3910万円	+1兆1485億2224万円
一件当たりの漏えい人数	3万2616人	+2万0693人
一件当たり平均想定損害賠償額	10億8561万円	+6億1026万円
一人当たり平均想定損害賠償額	5万2625円	+7728円

2.2 2014年 インシデント・トップ10

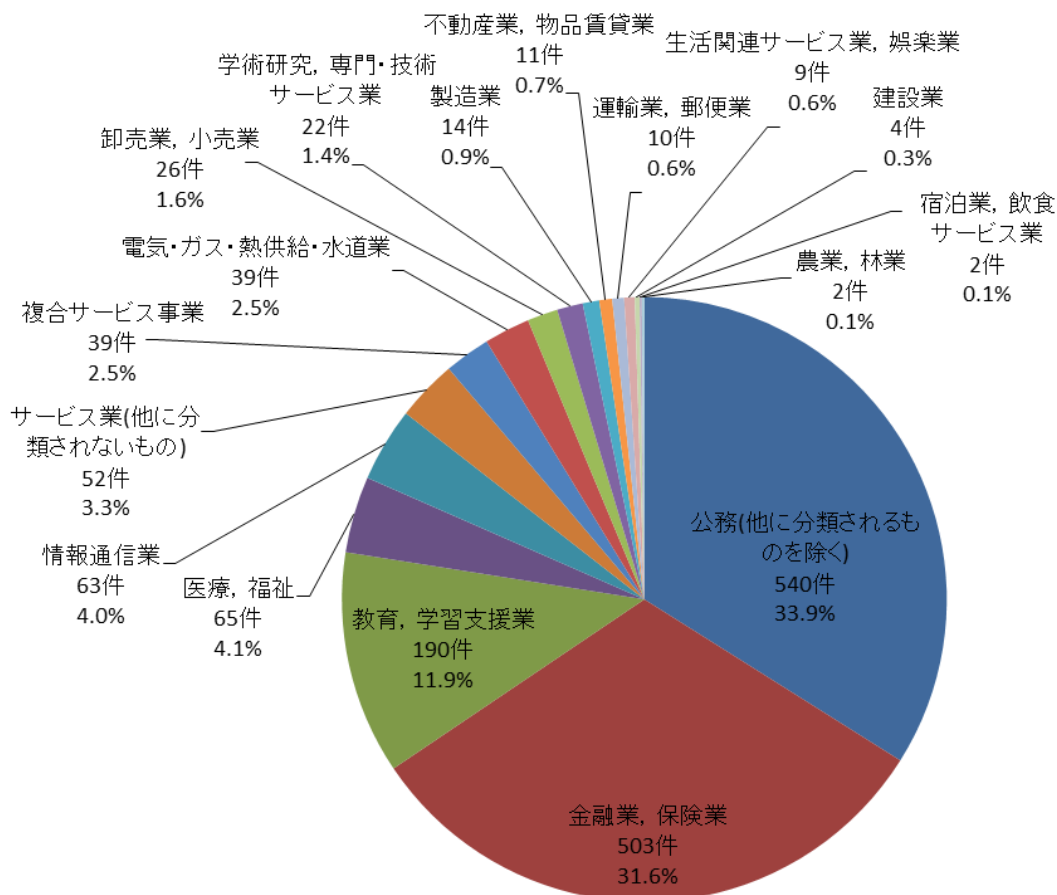
No.	漏えい人数	業種	原因
1	4858万人	教育, 学習支援業	内部犯罪・内部不正行為
2	16万4650人	情報通信業	誤操作
3	13万1646人	製造業	不正アクセス
4	9万4359人	情報通信業	不正アクセス
5	6万1977人	製造業	不正アクセス
6	5万6780人	公務 (他に分類されるものを除く)	誤操作
7	4万1477人	公務 (他に分類されるものを除く)	盗難
8	4万人	金融業, 保険業	管理ミス
9	4万人	公務 (他に分類されるものを除く)	内部犯罪・内部不正行為
10	3万9585人	金融業, 保険業	紛失・置忘れ

1000万人を超える大規模なインシデントが発生

公務が多い

2013年以降
不正アクセスが多い

2.3 業種別の漏えい件数



2013年
(N=1333件)

2014年
(N=1591件)

公務
(588件)

公務
(540件)

金融業, 保険業
(229件)

金融業, 保険業
(503件)

教育, 学習支援業
(161件)

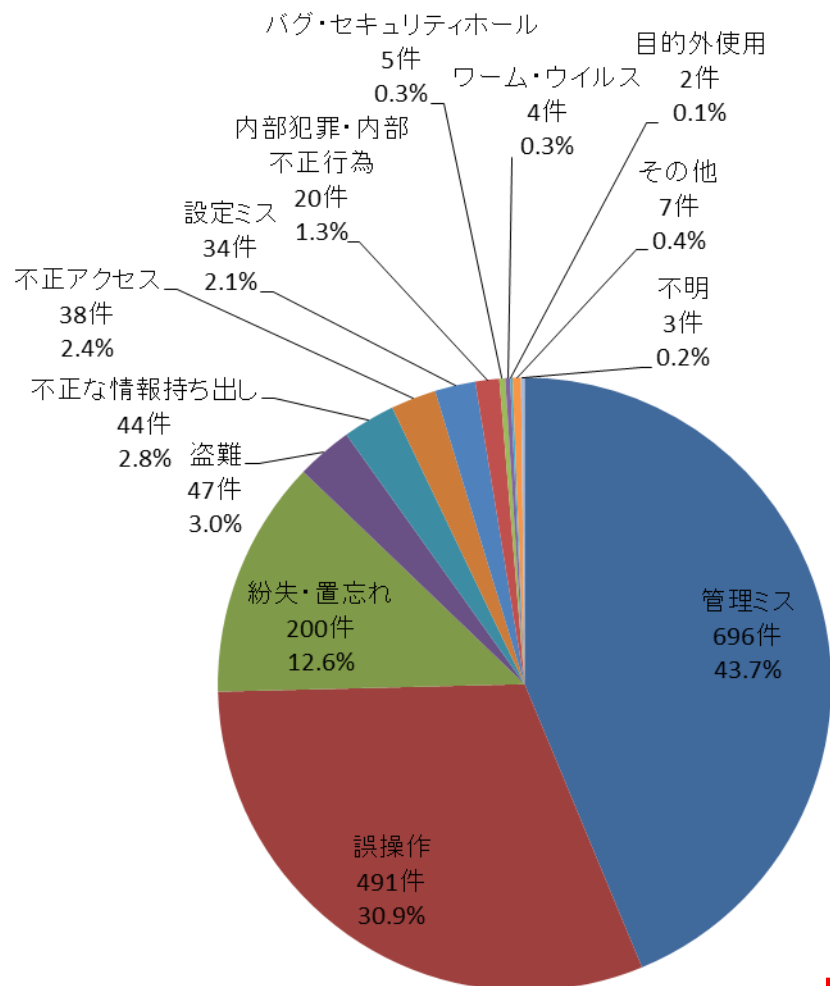
教育, 学習支援業
(190件)

情報通信業
(77件)

医療, 福祉
(106件)

上位3業種は同じ

2.4 原因別の漏えい件数



2013年
(N=1333件)

2014年
(N=1591件)

誤操作
(488件)

管理ミス
(696件)

管理ミス
(383件)

誤操作
(491件)

紛失・置忘れ
(200件)

紛失・置忘れ
(200件)

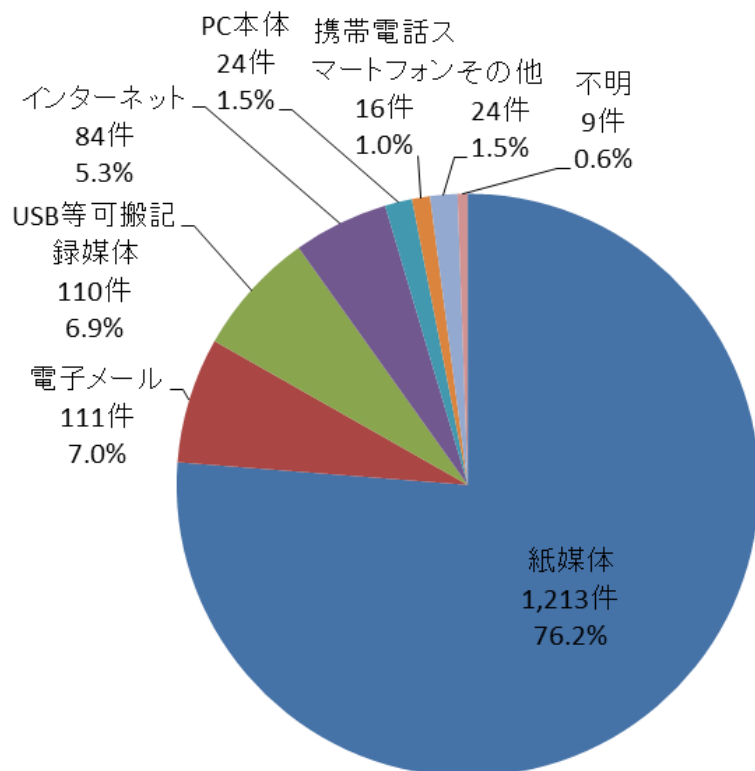
盗難
(79件)

盗難
(47件)

**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**

上位の原因に大きな変化はなし

2.5 媒体・経路別の漏えい件数



2013年
(N=1333件)

2014年
(N=1591件)

紙媒体
(876件)

紙媒体
(1213件)

USB等可搬
記録媒体
(109件)

電子メール
(111件)

電子メール
(121件)

USB等可搬
記録媒体
(109件)

インターネット
(123件)

インターネット
(84件)

**紙媒体による漏えいが多い。
(例年通り)**

3. 2015年 個人情報漏えい インシデント調査結果 (速報)

**本日 6/17 午後
報告書を公開**

※2015年調査分は速報値を使用しているため、数値やグラフなどの一部が変更される恐れがあります。

3.1 2015年 個人情報漏えいインシデント

期間:2015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

	2015年(速報)	年平均比較
漏えい件数	799件	-339件
漏えい人数	496万0063人	-797万5024人
想定損害賠償総額	2541億3663万円	-2615億8023万円
一件当たりの漏えい人数	6578人	-5345人
一件当たり平均想定損害賠償額	3億3705万円	-1億3830万円
一人当たり平均想定損害賠償額	2万8020円	-1万6877円

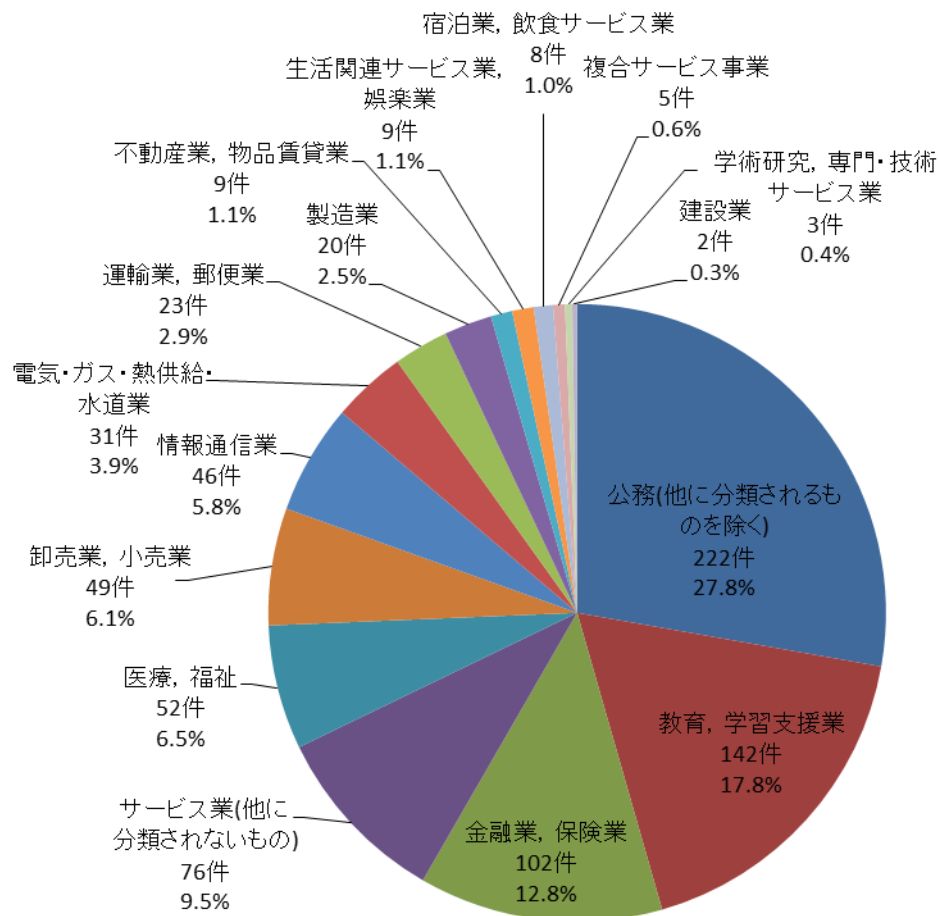
3.2 2015年 インシデント・トップ10

No.	漏えい人数	業種	原因
1	101万4653人	公務（他に分類されるものを除く）	不正アクセス
2	69万4217人	金融業，保険業	管理ミス
3	68万人	公務（他に分類されるものを除く）	不正な情報持ち出し
4	26万7000人	情報通信業	不正アクセス
5	20万9999人	卸売業，小売業	不正アクセス
6	18万人	公務（他に分類されるものを除く）	不正な情報持ち出し
7	14万2000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
8	13万1096人	卸売業，小売業	不正アクセス
9	11万4400人	医療，福祉	盗難
10	10万7368人	製造業	不正アクセス

公務が多い

2013年以降
不正アクセスが多い

3.3 業種別の漏えい件数



2014年
(N=1591件)

2015年(速報)
(N=799件)

公務
(540件)

公務
(222件)

金融業, 保険業
(503件)

教育, 学習支援業
(142件)

教育, 学習支援業
(190件)

金融業, 保険業
(102件)

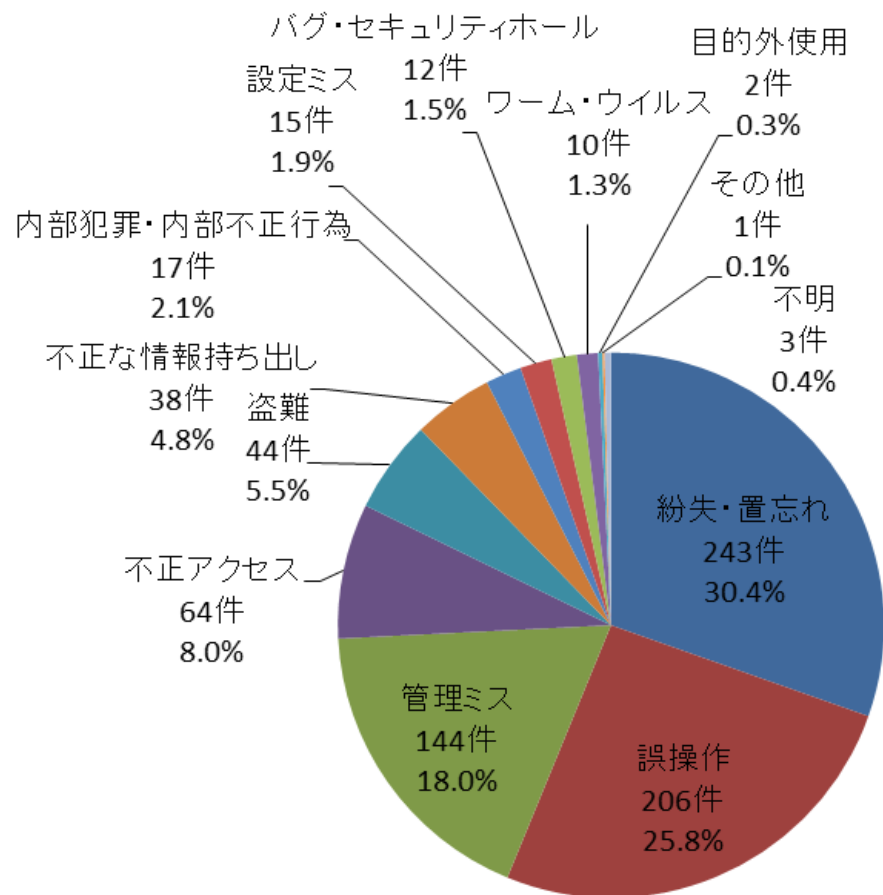
医療, 福祉
(106件)

サービス業
(76件)

上位3業種は同じ

教育, 学習支援業が多い

3.4 原因別の漏えい件数



2014年
(N=1591件)

2015年(速報)
(N=799件)

管理ミス
(696件)

紛失・置忘れ
(243件)

誤操作
(491件)

誤操作
(206件)

紛失・置忘れ
(200件)

管理ミス
(144件)

盗難
(47件)

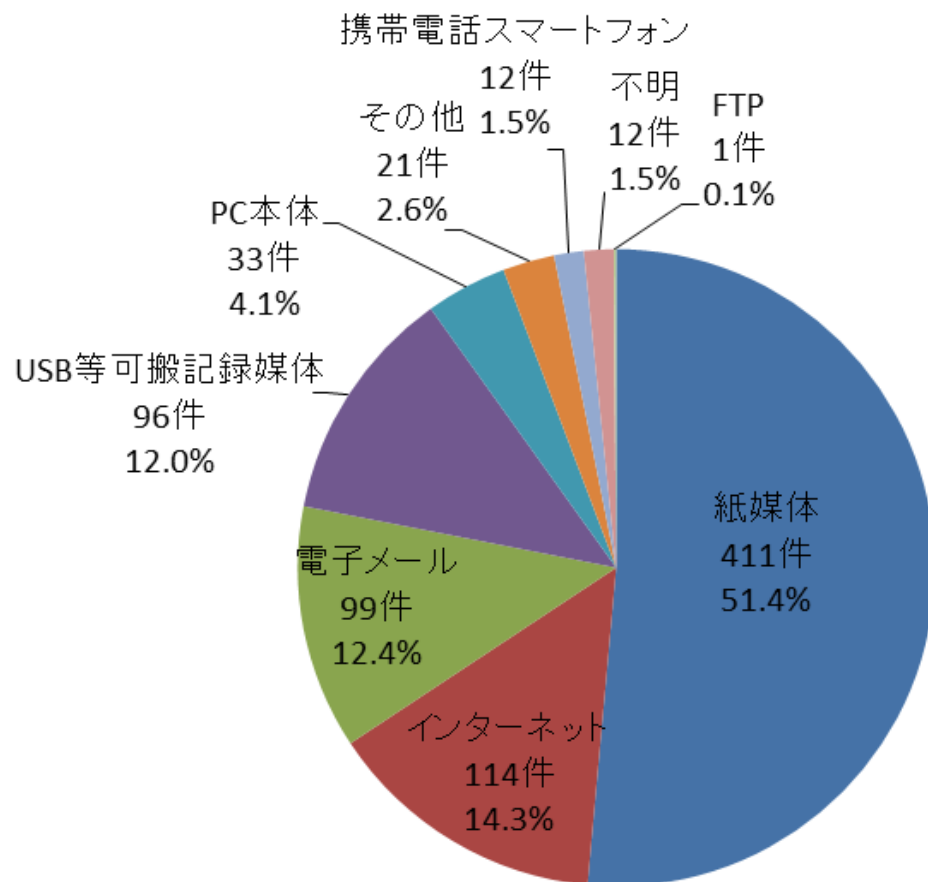
不正アクセス
(64件)

紛失・置忘れが増加

不正アクセスが多い

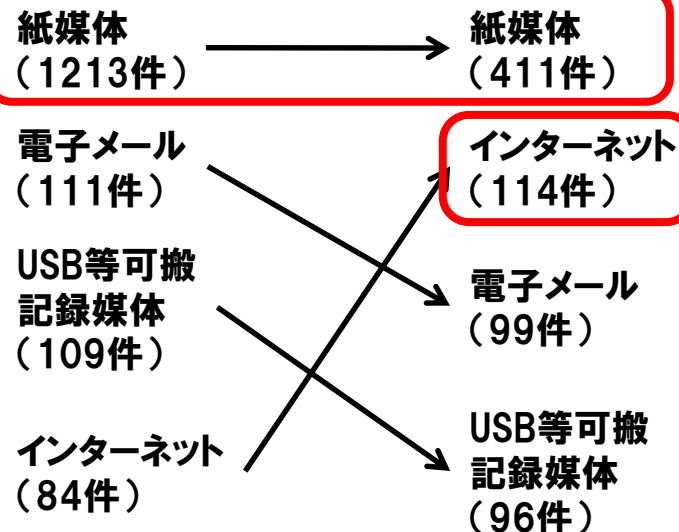
2015年 インシデント・トップ10のうち、不正アクセスが5件

3.5 媒体・経路別の漏えい件数



2014年
(N=1591件)

2015年(速報)
(N=799件)



**紙媒体による漏えいが多い。
(例年通り)**

インターネット経由が多い

付録

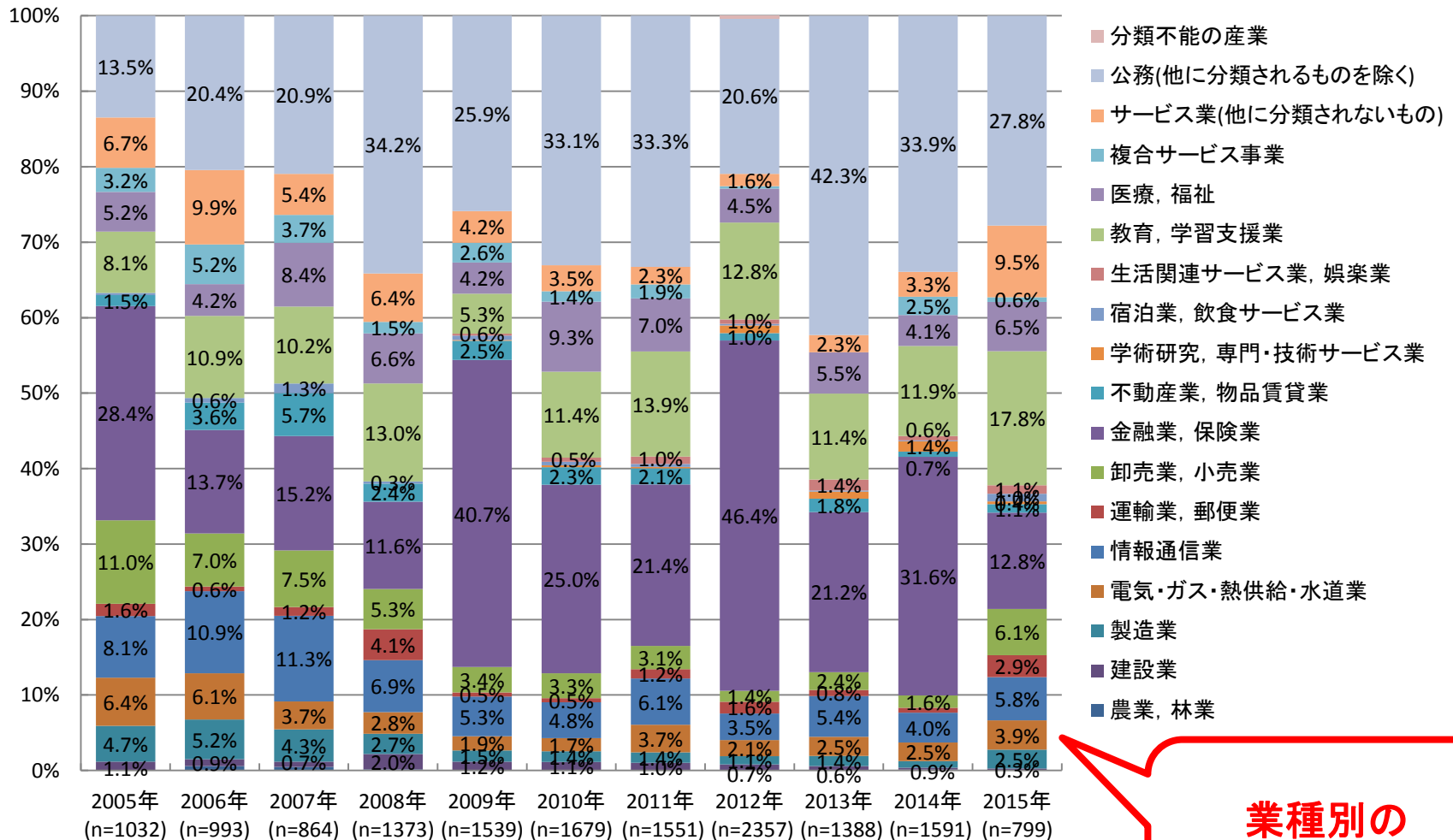
2014/2015年 個人情報漏えいインシデント比較

JNSA

	2014年	2015年 (速報)
漏えい件数	1591件	799件
漏えい人数	4999万9892人	496万0063人
想定損害賠償総額	1兆6642億3910万円	2541億3663万円
一件当たりの漏えい人数	3万2616人	6578人
一件当たり平均想定損害賠償額	10億8561万円	3億3705万円
一人当たり平均想定損害賠償額	5万2625円	2万8020円

3.6 業種別比率の経年変化

スライド
表示のみ



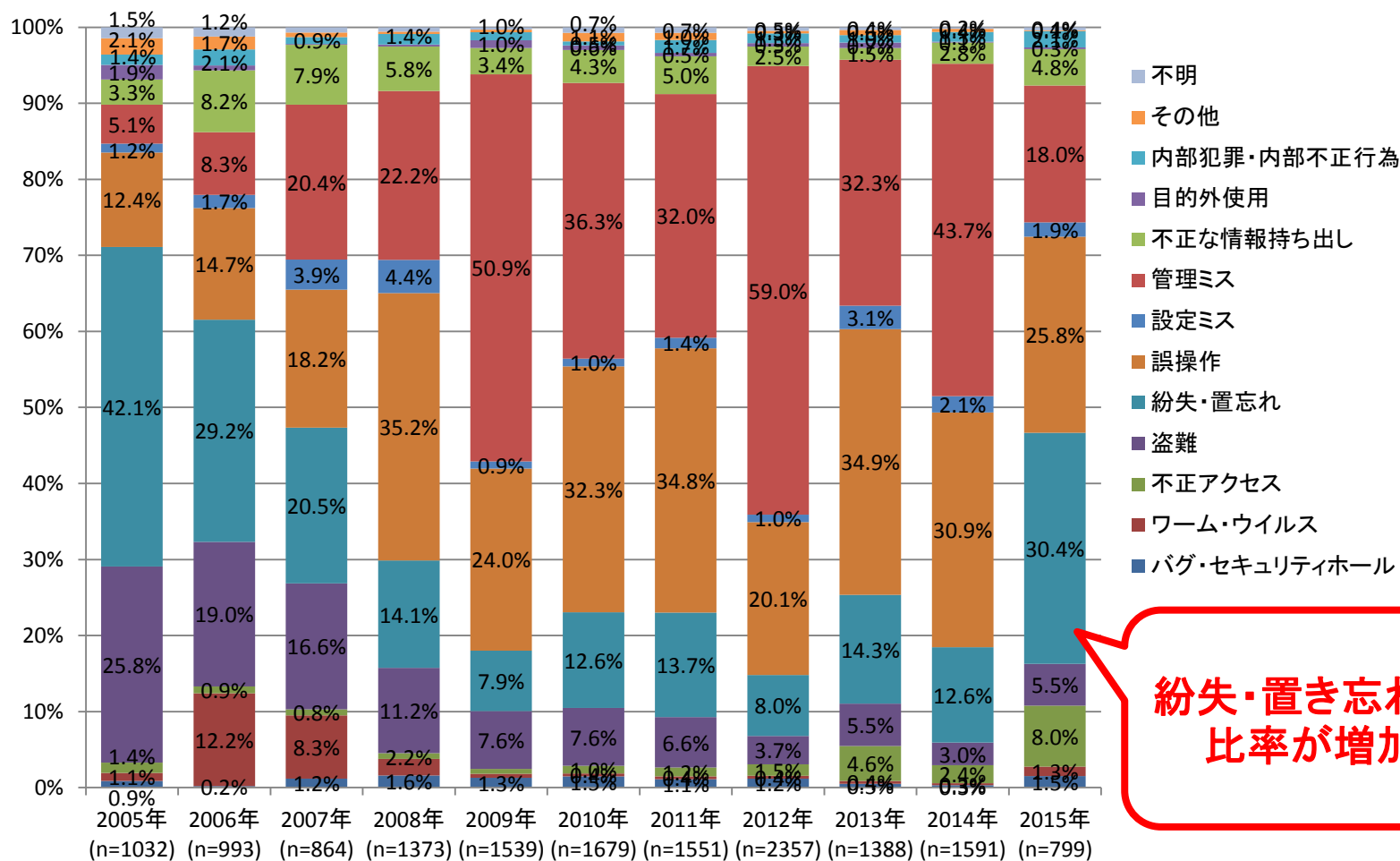
図：業種別比率の経年変化(件数)

※ 2015年調査分は速報値を使用しているため、数値やグラフなどの一部が変更される恐れがあります。

業種別の
偏りが少ない

3.7 漏えい原因比率の経年変化

スライド
表示のみ

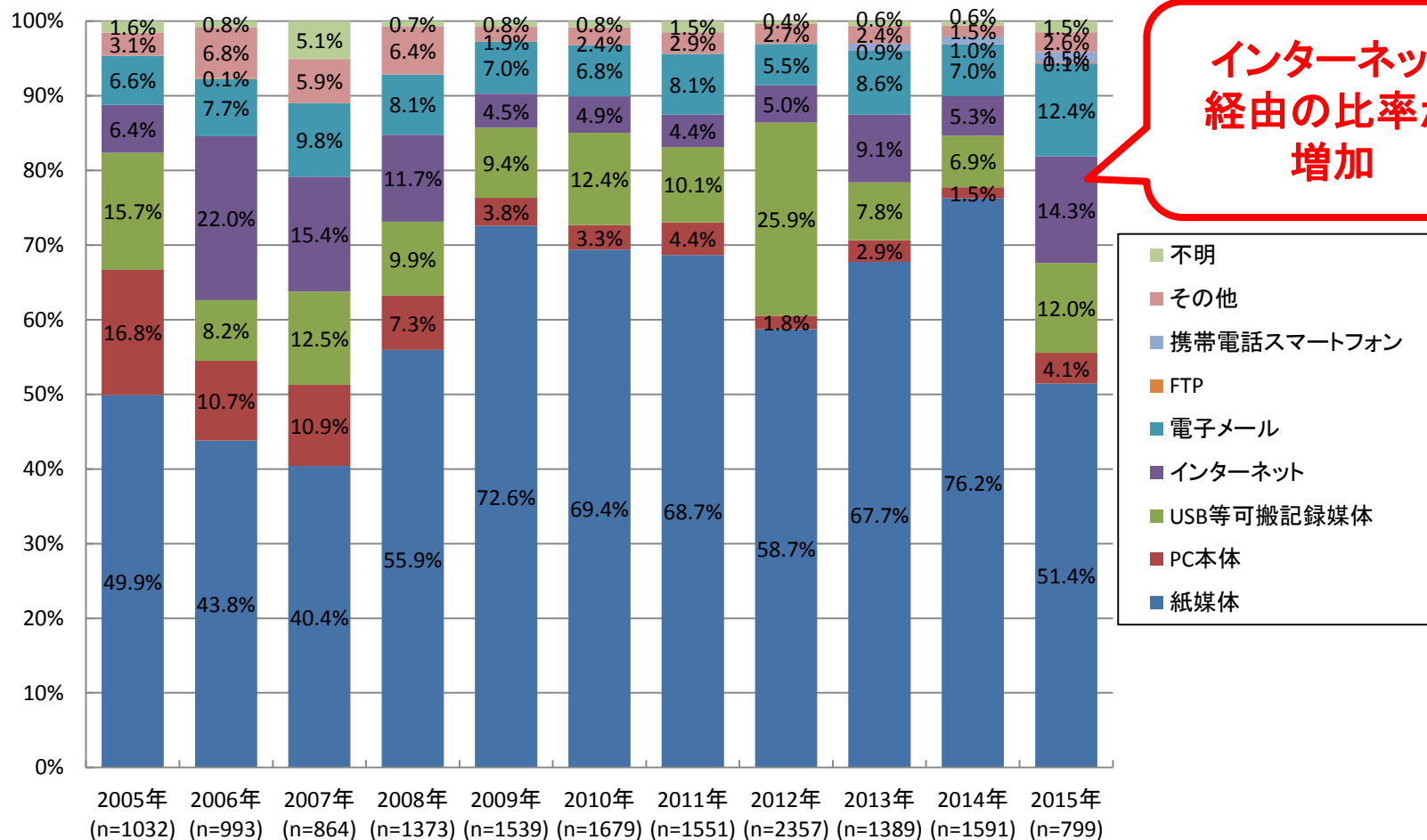


紛失・置き忘れの
比率が増加

※ 2015年調査分は速報値を使用しているため、数値やグラフなどの一部が変更される恐れがあります。

3.8 漏えい経路比率の経年変化

スライド
表示のみ



図：漏えい経路比率の経年変化(件数)

※ 2015年調査分は速報値を使用しているため、数値やグラフなどの一部が変更される恐れがあります。

4. 今後の活動

サイバーセキュリティの侵害やリスクの 情報開示に関するガイドライン

(出展: NISC, 我が国のサイバーセキュリティ戦略, 2015年3月20日)

サイバーセキュリティ 経営ガイドライン

(出展: 経産省, サイバーセキュリティ経営ガイドライン,
2015年12月28日)

(出展: NISC, 「サイバーセキュリティ2016(案)」
に関する意見の募集について, 2016年6月13日)

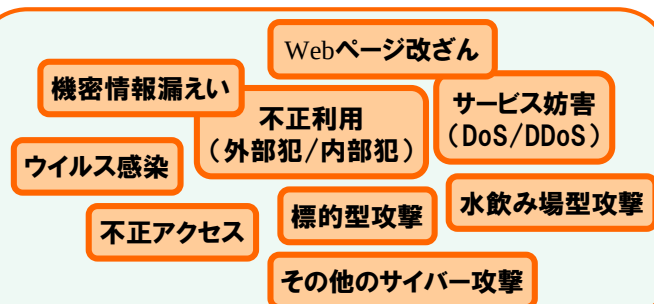
被害の定量化や投資対効果の測定が必要！

4.2 課題の解決へ向けた活動

【課題】 被害の定量化や投資対効果を測定できる方法がない

セキュリティ被害調査WGの次のテーマ

- 個人情報漏えい以外のインシデントの
 - 損害モデルの構築
 - 被害額や対応費用の算定式作成
- セキュリティ投資対効果「Security Return On Investment(SROI)」の算出モデル構築
- 適切なセキュリティ対策投資のベストプラクティスの提示



経営戦略へ情報セキュリティ対策も組み込んでほしい

4.3 今後のWGの活動方針

1. 個人情報漏えいインシデントの調査活動は、継続する。
情報セキュリティ専攻の研究室と共同研究体制で運営する。
2. WG活動は、次テーマの検討を中心にすすめる。
合理的なセキュリティ対策を促進するためのセキュリティ被害やセキュリティ費用対効果(SROI)などの定量化、算定モデルの構築をすすめる。

WGメンバーを募集！

**本日 6/17 午後より
報告書を公開**

