被害調査WG・リテラシーベンチマーク作成WG
合同セキュリティ対策セミナー

情報漏えいインシデントの調査結果から学ぶセキュリティ対策

2008 年 8月22日

セキュリティ被害調査WG リーダー
(株)ＮＴＴデータ 大谷尚通

セキュリティ被害調査WGの紹介

JNSA セキュリティ被害調査ワーキンググループ（以下、WG）は、セキュリティインシデントの被害額や情報セキュリティの対策投資額を推計するモデルを構築し、情報セキュリティマネジメントにおける「リスクの大きさ(被害規模)」と「対策規模」の把握と効果の計測、効率的なマネジメント方法を実現することが、目標である。
当WGは、2001年より活動を開始し、これまでに以下の提案を行ってきた。

- 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・分析した。さらに「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。

２００７年報告書／データ集

2007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

- はじめに
- 報告書について
- 2007年の個人情報漏えいインシデントの分析結果
- 個人情報漏えいにおける想定損害賠償額の算出モデル
- 漏えいインシデントの事後処理コスト
- 最後に
- 付録1：WINNYインシデント解説
- 付録2：漏えい原因の定義
- 付録3：インシデント一覧表
  （全108ページ）

詳しくは
www.jnsa.org

- □ Excelファイル：
  本編の分析データ
  付録１：Winny解説の分析データ
  2007年 情報漏えいインシデント一覧データ
- □ Powerpointファイル：
  本編グラフ一式（単年／経年分析、単年・相関分析、
  想定損害賠償額算定／経年分析）
  Winnyインシデント解説
- □ PDFファイル：2002年～2007年の速報、報告書

目次

- 『2007年情報セキュリティインシデントに関する調査報告書』解説
- 事故事例から学ぶ、個人/機密情報漏えい対策
- 想定損害賠償額算定式の使い方
- 質疑応答

『2007年情報セキュリティ インシデントに関する調査報告書』

解説

2007年 インシデントの概要

漏えい人数	3,053万1,004人	過去最高
インシデント件数	864件	
想定損害賠償総額	2兆2,710億8,970万円	過去最高
一件当たりの漏えい人数	3万7554人	過去最高
一件当たり平均想定損害賠償額	27億9,346.8万円	過去最高
一人当たり平均想定損害賠償額	3万8,233円	

一日平均2.4件

3,053万1,004人

1億2,777万1,000人

＝ 約4人に1人の割合

2007年 インシデント・トップ5

No.	漏えい人数	業種	原因
①	約1,443万人	複合サービス事業	管理ミス
②	約864万人	製造業	内部犯罪・内部不正行為
3	約98万人	金融・保険業	管理ミス
4	約65万人	卸売・小売業	管理ミス
5	約47万人	電気・ガス・熱供給・水道業	管理ミス

管理ミス

2004年（個人情報保護法施行前）

被害人数	業種名	漏洩原因区分
452万人	情報通信業	不正な情報持ち出し
116万人	金融・保険業	不明
92万人	製造業	不正な情報持ち出し
63万人	サービス業	内部犯罪・内部不正行為
51万人	卸売・小売業	内部犯罪・内部不正行為

2005年

被害人数	業種名	漏洩原因区分
131万人	金融・保険業	紛失・置忘れ
85万人	情報通信業	内部犯罪・内部不正行為
57万人	金融・保険業	紛失・置忘れ
47万人	公務	盗難
32万人	公務	盗難

盗難
紛失・置忘れ

2006年

被害人数	業種名	漏洩原因区分
③ 538万人	製造業	不明
400万人	情報通信業	内部犯罪・内部不正行為
400万人	情報通信業	内部犯罪・内部不正行為
176万人	公務	紛失・置忘れ
96万人	金融・保険業	紛失・置忘れ

内部犯罪
内部不正行為

2007年 単年分析

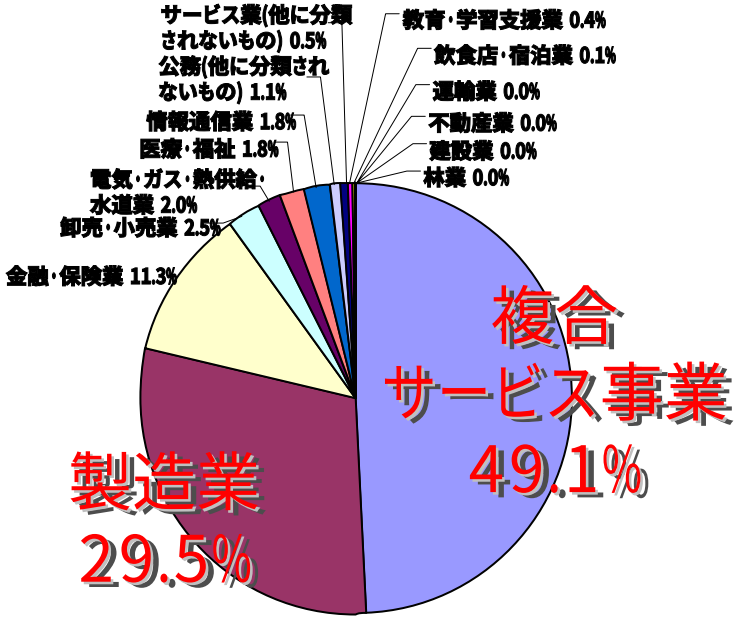


図 1：業種別比率（人数）

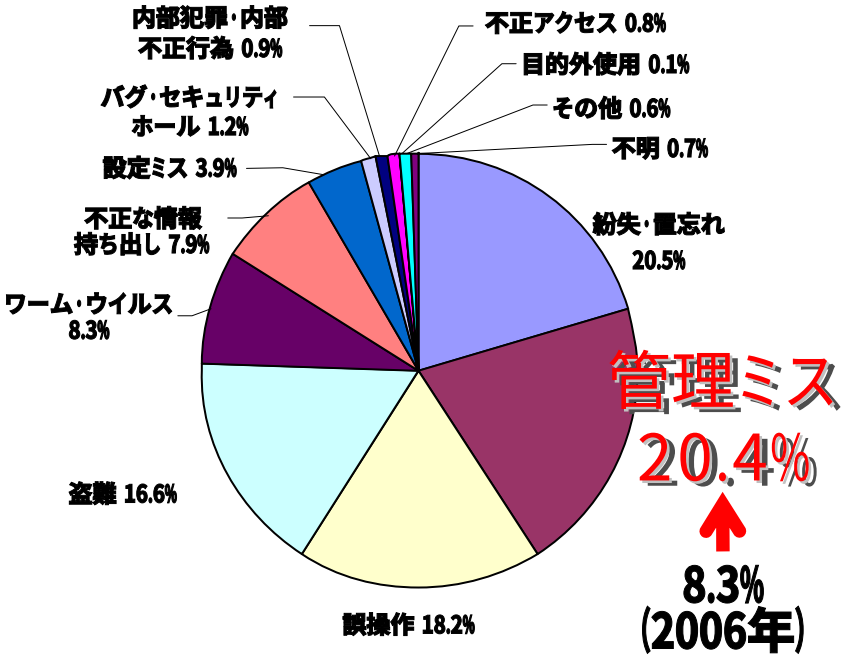


図 2：漏えい原因比率（件数）

大規模なインシデントの影響大

↓

毎年、業種別比率の傾向が異なる
業種との依存関係は弱い

個人情報漏えい対策の浸透
内部統制への取り組み

↓

組織内の情報管理が強化

↓

情報の棚卸しにより、
組織内の誤廃棄や紛失が判明

2007年 想定損害賠償額算定結果

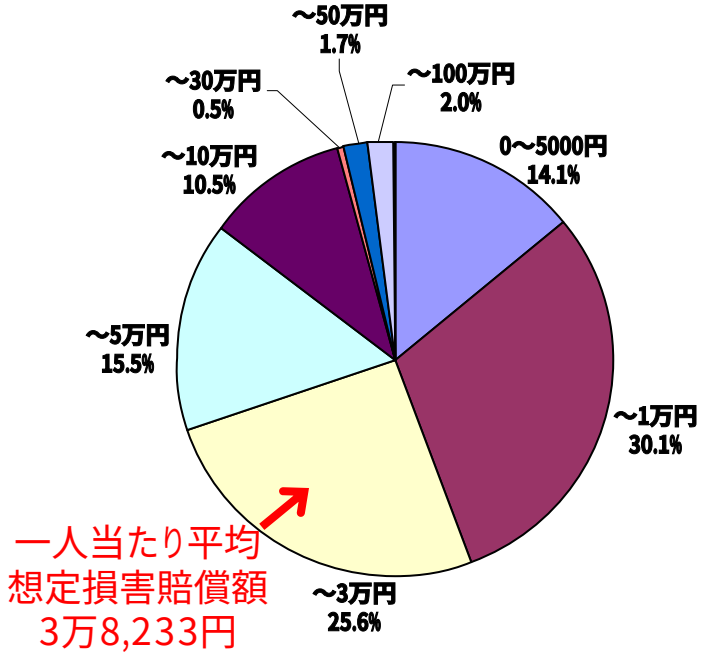


図 3：一人当たりの
想定損害賠償額比率（件数）

「5000円〜1万円」・「1〜3万円」= 55.7%
比較的、一人当たりの想定損害賠償額が
低いインシデントが多い

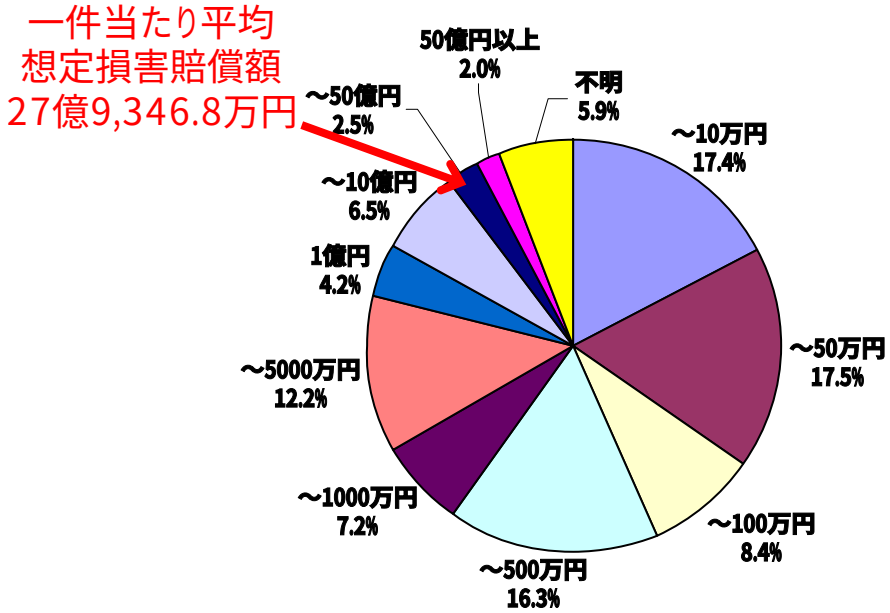


図 4：一件当たりの
想定損害賠償額比率（件数）

一件当たりの想定損害賠償額の
インシデントの分布は分散している。
50億円以下のインシデントに
顕著な傾向はない。

2007年 単年・相関分析①

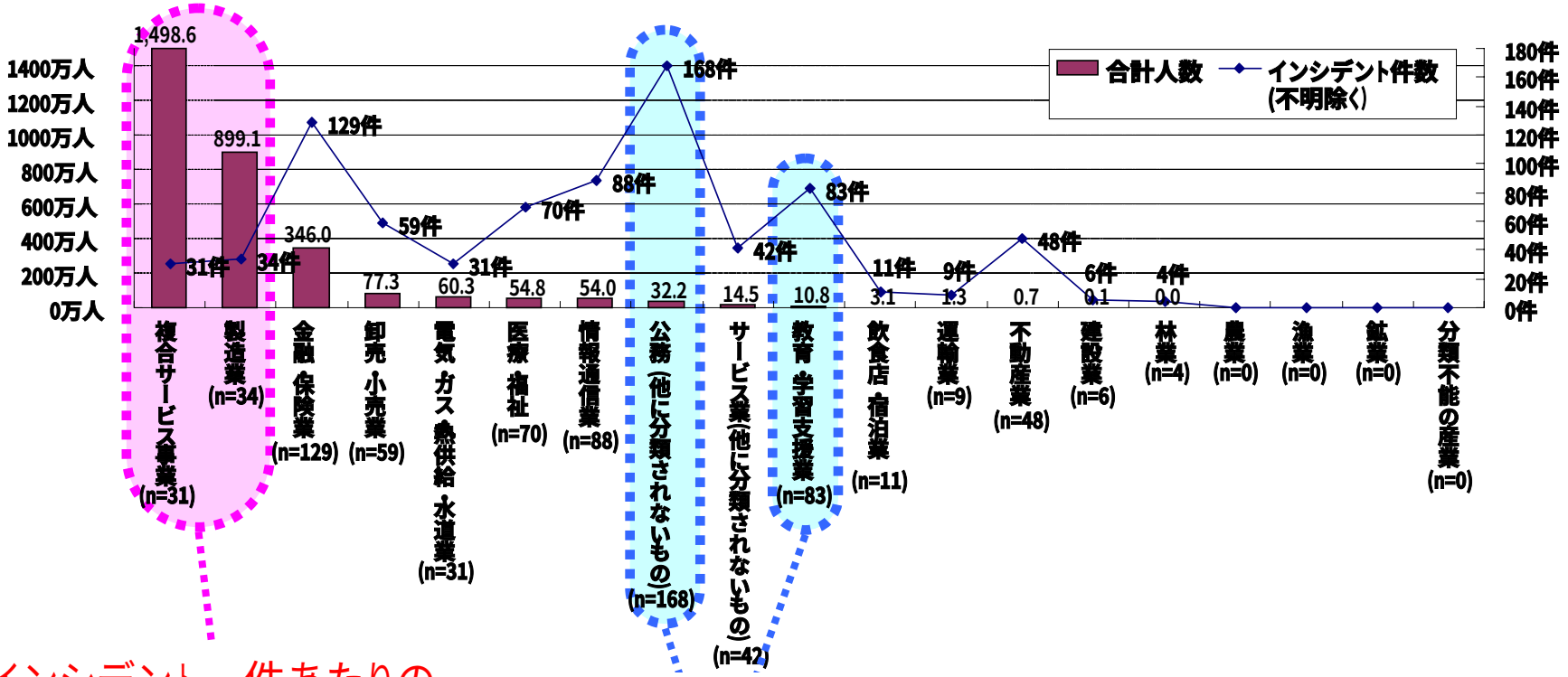


図 5：業種別のインシデント件数と漏えい人数

インシデント一件あたりの
漏えい人数が多い
(規模が大きい)

複合サービス事業	約1,443万人
製造業	約864万人

インシデント一件あたりの
漏えい人数が少ない
(規模が小さい)

公的書類(住民票、年金書類):一人単位
教育・学習支援業:クラス単位(20～40人)

2007年 単年・相関分析②

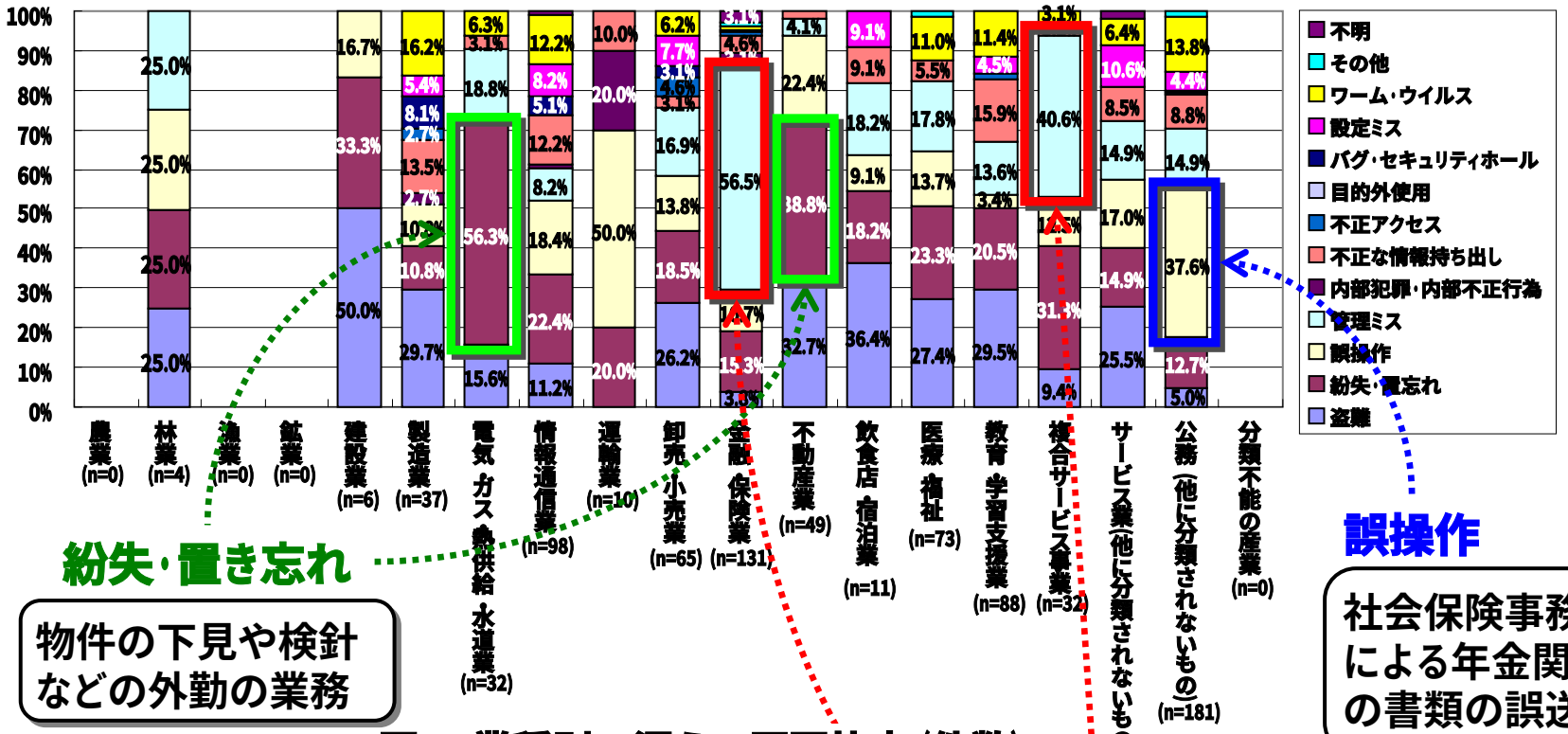


図 6：業種別の漏えい原因比率 (件数)

紛失・置き忘れ

物件の下見や検針などの外勤の業務

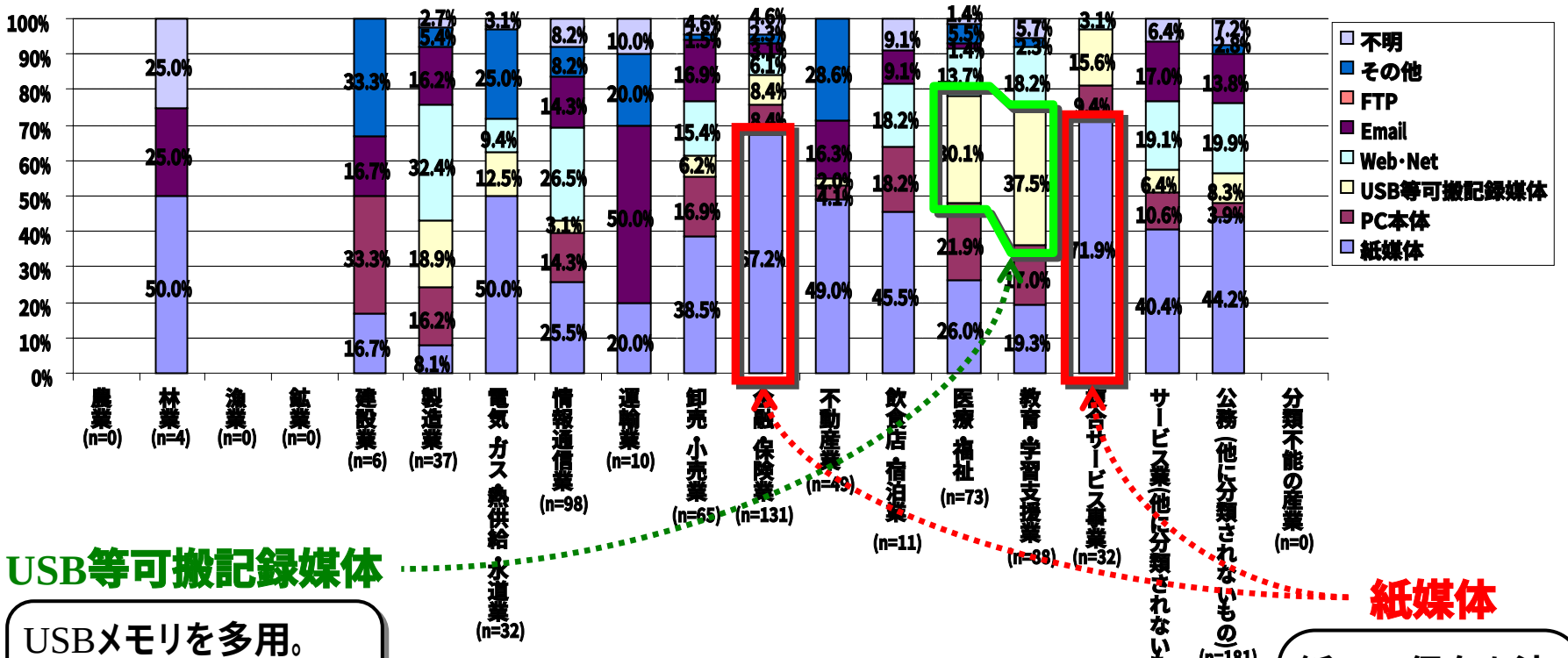
誤操作

社会保険事務所による年金関連の書類の誤送付

管理ミス

書類の誤廃棄が多い。管理業務下の紛失・誤廃棄は管理ミスへ。

2007年 単年・相関分析③



USB等可搬記録媒体

USBメモリを多用。
管理がずさん、取り扱い時の注意が散漫

紙媒体

紙での保存を法律で規定されているため、紙を多く使う

図 7：業種別の漏えい経路比率（件数）

2007年 経年分析①

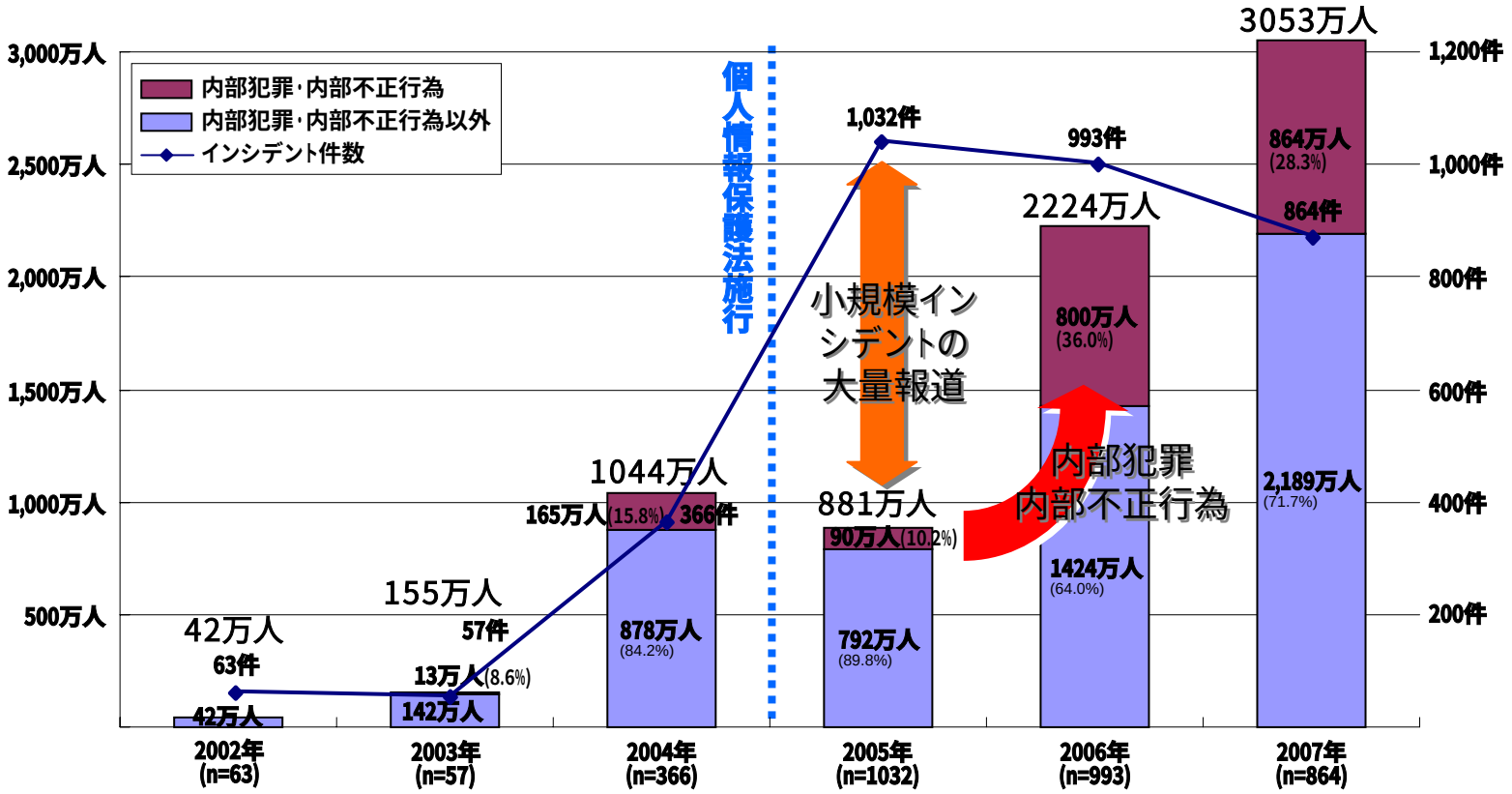


図 8:インシデント件数と内部不正による漏えい人数の経年変化(合計)

2007年 経年分析②

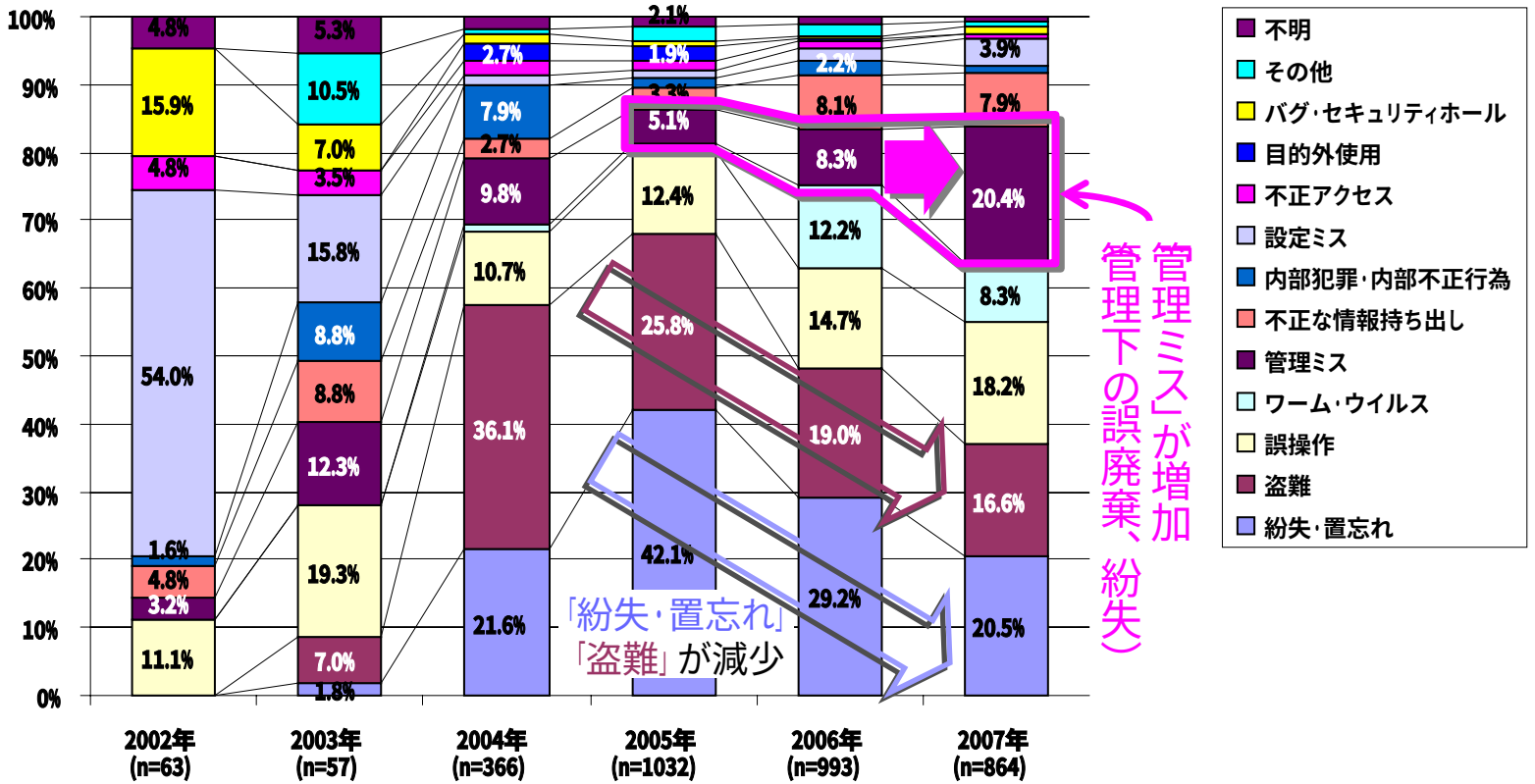


図 9：漏えい原因比率の経年変化（件数）

- **個人情報対策が進み、遅れていた組織内の管理体制や管理方法に対策対象が拡大**
- **「紛失」を内部統制の観点から「管理ミス」として分類**

2007年 経年分析③

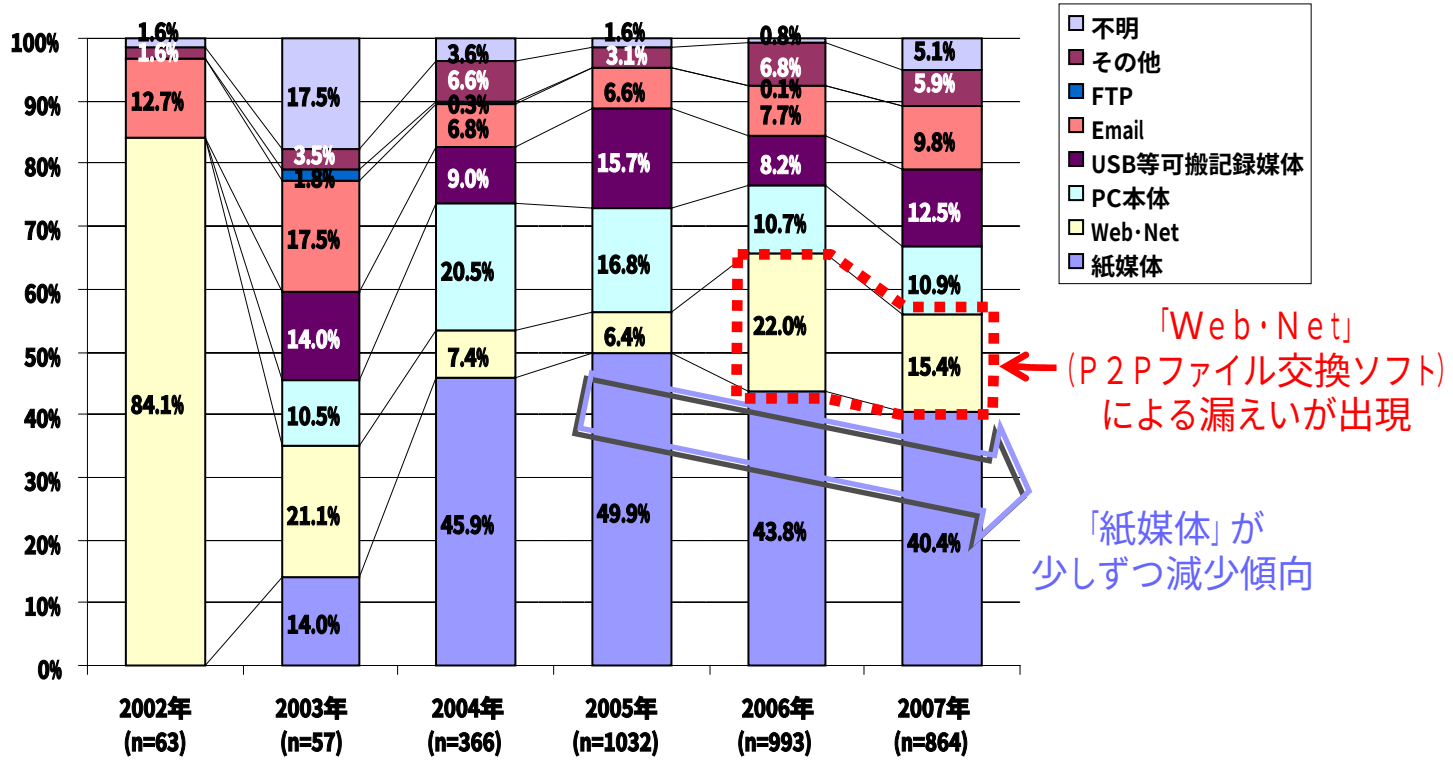


図 10：漏えい経路比率の経年変化（件数）

- **紙媒体はわずかに減少傾向だが、依然として多い**
- **2006年に続き、P2Pファイル交換ソフトによる漏えいが続いている**

2007年 経年分析④

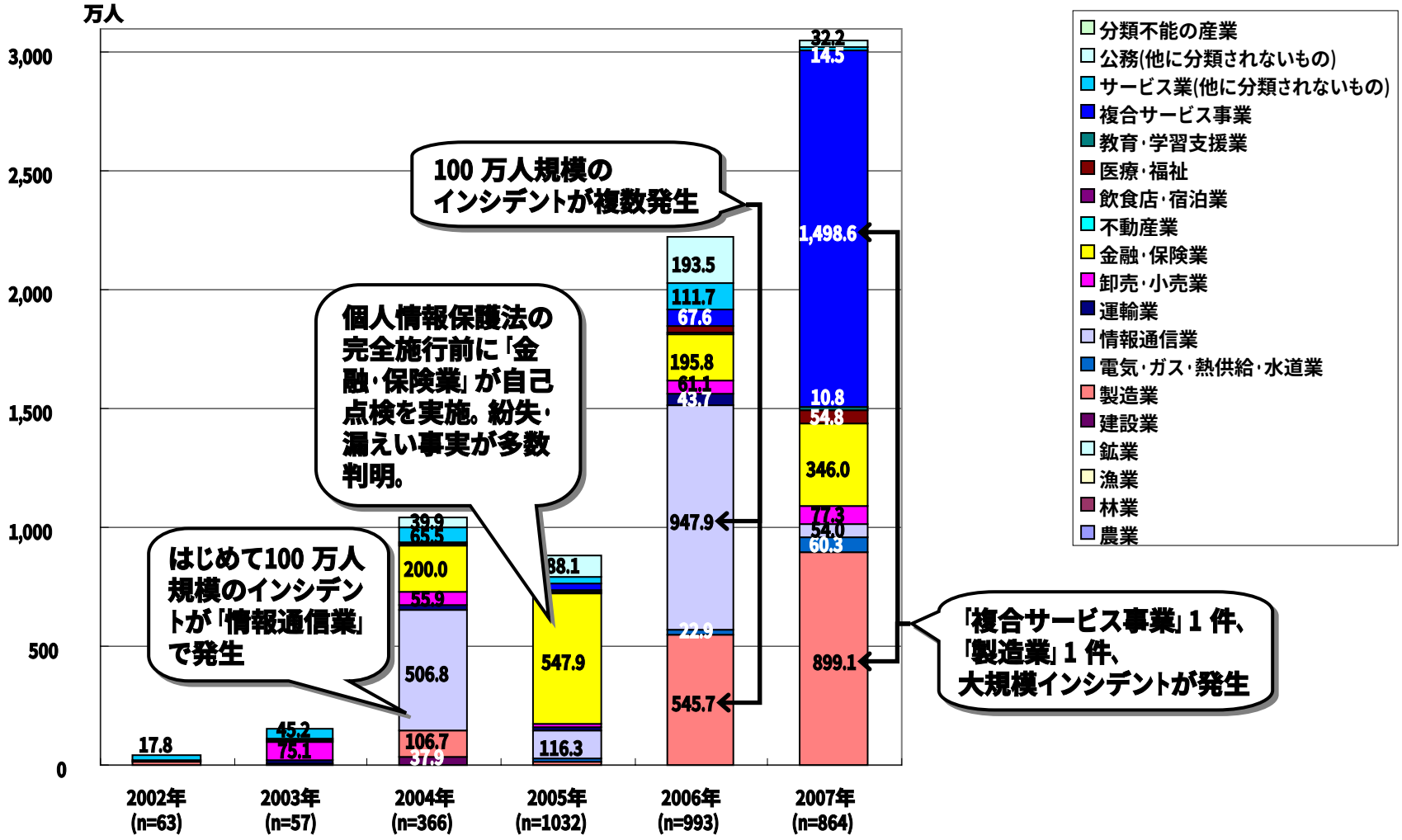


図 11：業種別漏えい人数の経年変化（合計）

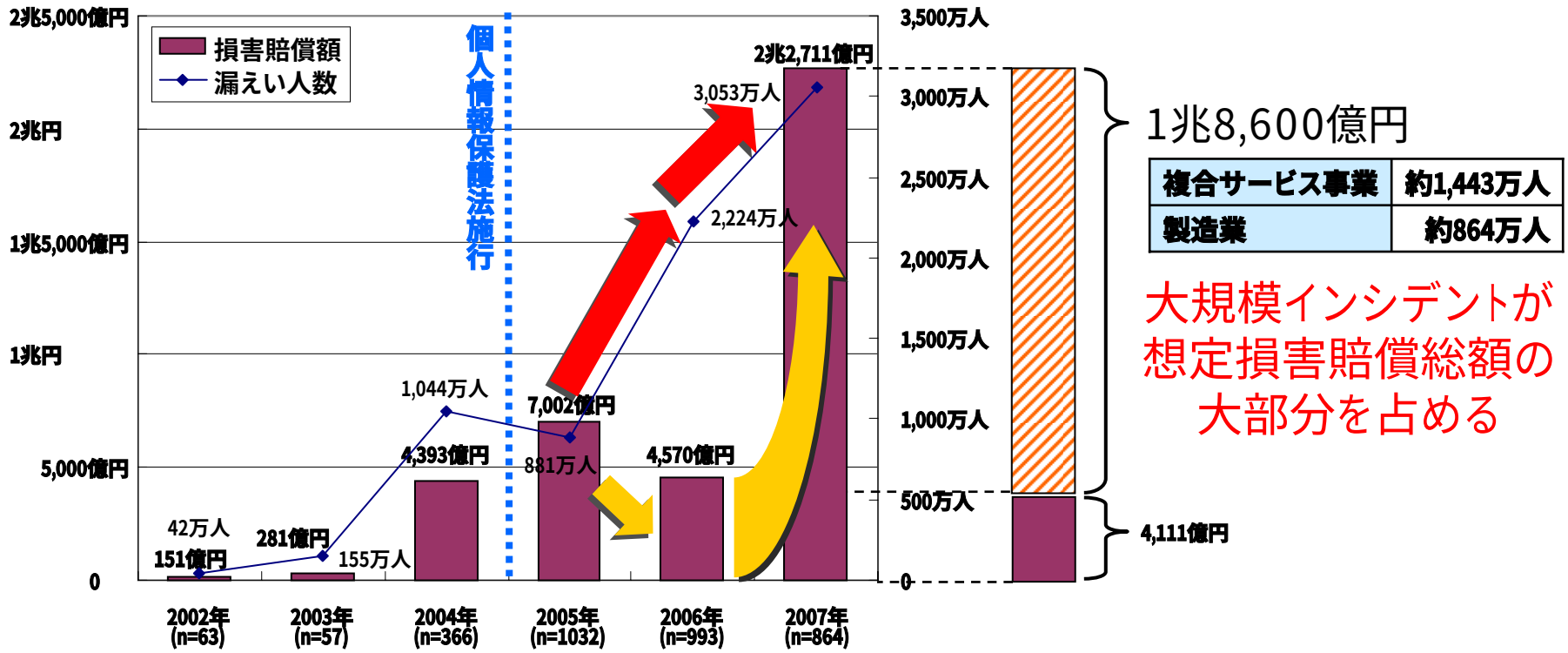
2007年想定損害賠償額の経年分析

	想定損害賠償総額	一件当たりの 平均想定損害賠償額	一人当たりの 平均想定損害賠償額
2002年 (n=63)	約189億円	2億7,532万円	1万6,855円
2003年 (n=57)	約281億円	5億5,038万円	8万9,140円
2004年 (n=366)	約4,667億円	13億　730万円	10万5,365円
2005年 (n=1032)	約7,002億円	7億　868万円	4万6,271円
2006年 (n=993)	約4,570億円	4億8,156万円	3万6,743円
2007年 (n=864)	約2兆2,711億円	27億9,347万円	3万8,233円

過去最高　過去最高

大規模で深刻なインシデントのみ報道。統計データとしては偏りが大きい。

2007年想定損害賠償額の経年分析



複合サービス事業	約1,443万人
製造業	約864万人

大規模インシデントが想定損害賠償総額の大部分を占める

図 12：想定損害賠償総額と漏えい人数

2007年情報漏えいｲﾝｼﾃﾞﾝﾄの総括

JNSA

■ 情報漏えいインシデントの注目度はやや薄れてきている

2005年：個人情報保護法の施行
2006年：Winnyによるインシデント多発
➡ **加熱報道・過剰反応がひと段落**

■ 情報の外部持ち出し対策が浸透

インシデント件数は、2005年以降、減少傾向
小規模インシデントの件数が、全体的に減少傾向

■ 内部統制との相乗効果により情報管理が強化

対応が遅れていた組織内情報の管理に対策対象が移行
管理強化により、保有情報や資料の再点検・棚卸しを実施
組織内での誤廃棄や紛失が判明。原因を管理ミスと定義

事故事例から学ぶ
個人/機密情報漏えい対策

事故事例「紛失・置忘れ」

持ち出し許可を得て持ち出した情報を、持ち出し先や移動中に置き忘れたり、紛失したりした場合。個人の管理ミスによって発生した場合。（社内等において、管理すべき情報を紛失した場合は、管理ミスに分類する）

例）電車、飲食店などに、PC、記録媒体等を紛失または置き忘れてしまった。

私物ＵＳＢ紛失事件

発生年	業種	漏えい情報	原因	経路･媒体
2005年	運輸業	個人情報（5,048人）	紛失･置忘れ	可搬記録媒体
漏えい情報	氏名、所属、役職名、生年月日			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
1	1	2	3	6,000円	3,028万8,000円

運輸業A社の人事課社員が全社員と取引先会社役員の名前や所属、職名、生年月日などを記録した私物USBメモリーを一時紛失した。紛失の報告は無く、USBメモリーが同封された匿名の封書が同社に届き発覚した。書簡には、インターネットカフェのパソコンに差し込まれていたと書かれていた。同社は、個人情報の社外への持ち出しを内規で禁止している。

《問題点》
- ■個人情報の持ち出し（ルール違反）
- ■私物USBの業務利用
- ■インターネットカフェで作業

《解決案》
- ■セキュリティ教育（ルールの遵守）
- ■私物USBの使用禁止/制限機能

メモリーカード紛失事件

発生年	業種	漏えい情報	原因	経路・媒体
2006年	公務	個人情報（650人）	紛失・置忘れ	可搬記録媒体
漏えい情報	氏名、住所、生年月日、役職、入社年、株主情報			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
1	1	2	6	1万2,000円	780万円

男性職員が、関係先企業の従業員と株主の個人情報を含むメモリーカード1枚を出張時に紛失した。社内の業務ごとに物理的に閉鎖されたネットワークを使用しており、ネットワーク間でファイルを交換するためにメモリーカードを使用している。メモリカードにデータを保存する際には暗号化を施している。

《問題点》
- メモリーカードの持ち出し（出張）
- 不要な情報の残留

《解決案》
- メモリーカードの管理方法
- ファイル交換後の情報削除

ノートPC紛失事件

発生年	業種	漏えい情報	原因	経路･媒体
2007年	情報通信業	個人情報（56,802人）	紛失･置忘れ	PC本体
漏えい情報	氏名、住所、電話番号、メールアドレス、購入情報			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
2	2	15	6	9万円	51億1,218万円

アイドル公式サイトを運営するA社の委託先B社の社員が、タクシーで移動中、ノートPC入りのカバンを紛失した。ノートPCには、アイドル関連商品を注文した顧客の氏名、住所、電話番号、メールアドレス、購入情報が保存されていた。PCにはログイン認証、データの一部にはパスワードが設定されていた。
B社は、パソコンを持ち出す場合に個人情報の削除を義務付けていた。

《問題点》
- ルールの不徹底（個人情報削除）
- 個人情報の取り扱い方法がずさん

《解決案》
- セキュリティ教育（ルールの遵守）
- 個人情報の取り扱い方法の見直し

携帯型情報端末機紛失事件

発生年	業種	漏えい情報	原因	経路・媒体
2007年	金融・保険業	個人情報（33,109人）	紛失・置忘れ	その他
漏えい情報	氏名、住所、生年月日、口座番号、取引情報			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
2	2	15	6	9万円	29億7,981万円

外回りをしていたA信用金庫の渉外担当職員が、個人情報を記録した業務用の携帯型情報端末機1台を紛失した。携帯端末には、顧客の氏名と口座番号、住所、生年月日、取引情報などが登録されていた。
端末には、起動時のID・パスワードによるセキュリティ機能と、翌日の午前0時を過ぎると全データを消去する機能を備えている。

《問題点》
■ミスによる紛失（避けられない）

《解決案》
■緊急時の対応方法の教育
■緊急対応体制の構築

事故事例「盗難」

第三者によって、記録媒体と共に情報が盗まれた場合。車上荒らし、事務所荒らしなど。（情報のみ盗難された場合は、不正アクセスに分類する）

例）車上荒らし、事務所荒らしなどにより、PC等の記録媒体とともに機密情報が盗難された。

クレジットカード情報盗難事件

発生年	業種	漏えい情報	原因	経路･媒体
2005年	卸売･小売業	個人情報（698人）	盗難	紙媒体
漏えい情報	氏名、クレジットカード番号、有効期間のほか、給油量			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
1	3	26	3	3万9,000円	2,722万2,000円

大手系列ガソリンスタンドから、ガソリンスタンド利用者の伝票が盗まれた。
伝票には、ローマ字の氏名、クレジットカード番号、有効期間、給油量などが記載されていた。
盗まれた伝票のデータが悪用されて、インターネット上で商品購入の申し込みが行われた。

《問題点》
- 伝票の保管がずさん
  （人の出入りが多く、盗難のリスクが高いにもかかわらず）
- 伝票上へのカード番号の印字

《解決案》
- 伝票の施錠保管
- 伝票上へカード番号を印字しない

ノートPC盗難（車上荒らし）事件

発生年	業種	漏えい情報	原因	経路・媒体
2005年	製造業	個人情報（23,444人）	盗難	PC本体
漏えい情報	顧客、取引先、同社社員の氏名、企業名、自宅住所、電話番号など			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
1	1	2	3	4,500円	1億549万8,000円

営業社員が、夜間に自宅駐車場の車内から、業務用ノートPC1台を盗まれた。ノートPCは、JR東京駅構内で発見された。ノートPCには、ログインIDとパスワードが設定されていたが、侵入され、第三者による個人情報へのアクセスの形跡が認められた。ノートPCのHDDやファイルの暗号化措置は取られていなかった。

《問題点》
- 夜間の車内へPCを放置
- 機密情報の暗号化なし

《解決案》
- PCの適切な管理
  （車内に放置しない）
- 機密情報の暗号化
- ディスクレスPC

事故事例「誤操作」

最終的な操作、作業段階によるミスを誤操作とする。あて先を書き間違えたり、操作ボタンを間違えて押したりするなどの人間の操作によって情報が漏えいした場合。
（メール配信システムの設定が間違っていた場合には設定ミスに分類する）

例）あて先間違いによって、電子メール・FAX・郵便・宅配便等の誤送信が発生した。

電子メール同報送信事件

発生年	業種	漏えい情報	原因	経路･媒体
2005年	情報通信業	個人情報（46人）	誤操作	Email経由
漏えい情報	メールアドレス			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
1	1	2	1	2,000円	9万2,000円

プロバイダA社は、同社サービスの障害報告を電子メール（同報）で送る際、宛先欄に顧客のメールアドレスを入力して送信したため、他の顧客のメールアドレスが閲覧可能な状態となった。A社は事実確認後、該当者に電話とメールで事実関係を説明し謝罪するとともに、誤送信メールの削除を依頼した。

《問題点》
- 操作ミス
- 確認漏れ

《解決案》
- メール送信時の確認徹底
- メール送信作業の手順化（ルール）
- 同報メールのシステム化

事故事例「目的外使用」

組織ぐるみ、もしくは組織の業務に関連して、個人情報を目的以外の用途で使用するなど、個人情報を当初の目的以外の用途に使用した場合。関係会社など、決められた開示範囲を越えて個人情報を公開した場合。

(社員、派遣社員などの内部の人間が、個人的に個人情報を目的外使用した場合は、内部犯罪・内部不正行為に分類する)

例）製品の保守等を目的として登録されたユーザ情報(個人情報)を他関連会社に渡して他製品のセールスに使用した場合。

顧客情報流用事件

発生年	業種	漏えい情報	原因	経路･媒体
2006年	金融･保険業	個人情報（100人）	目的外使用	その他
漏えい情報	氏名、電話番号、住宅公庫顧客情報			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
1	1	2	3	6,000円	60万円

住宅金融公庫業務の取扱金融機関であるA銀行のB支店は、住宅金融公庫の顧客情報を利用して借り換えの勧誘を行なった。住宅金融公庫は、取扱金融機関に対して、住宅金融公庫ローン利用者の個人情報を使って借り換えを促すなどの目的外使用を禁じている。

《問題点》
- 住宅金融公庫ローン利用者の個人情報の不正利用
- 業務委託契約違反
- 組織全体のモラルの問題

《解決案》
- 管理体制の強化
- 罰則規定の強化、事件の公表

医療データの持ち出し事件

発生年	業種	漏えい情報	原因	経路･媒体
2004年	公務	個人情報（9000人）		紙媒体
漏えい情報	氏名、生年月日、性別、被保険者番号、傷病歴			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
1	3	101	3	30万3,000円	27億2,700万8,000円

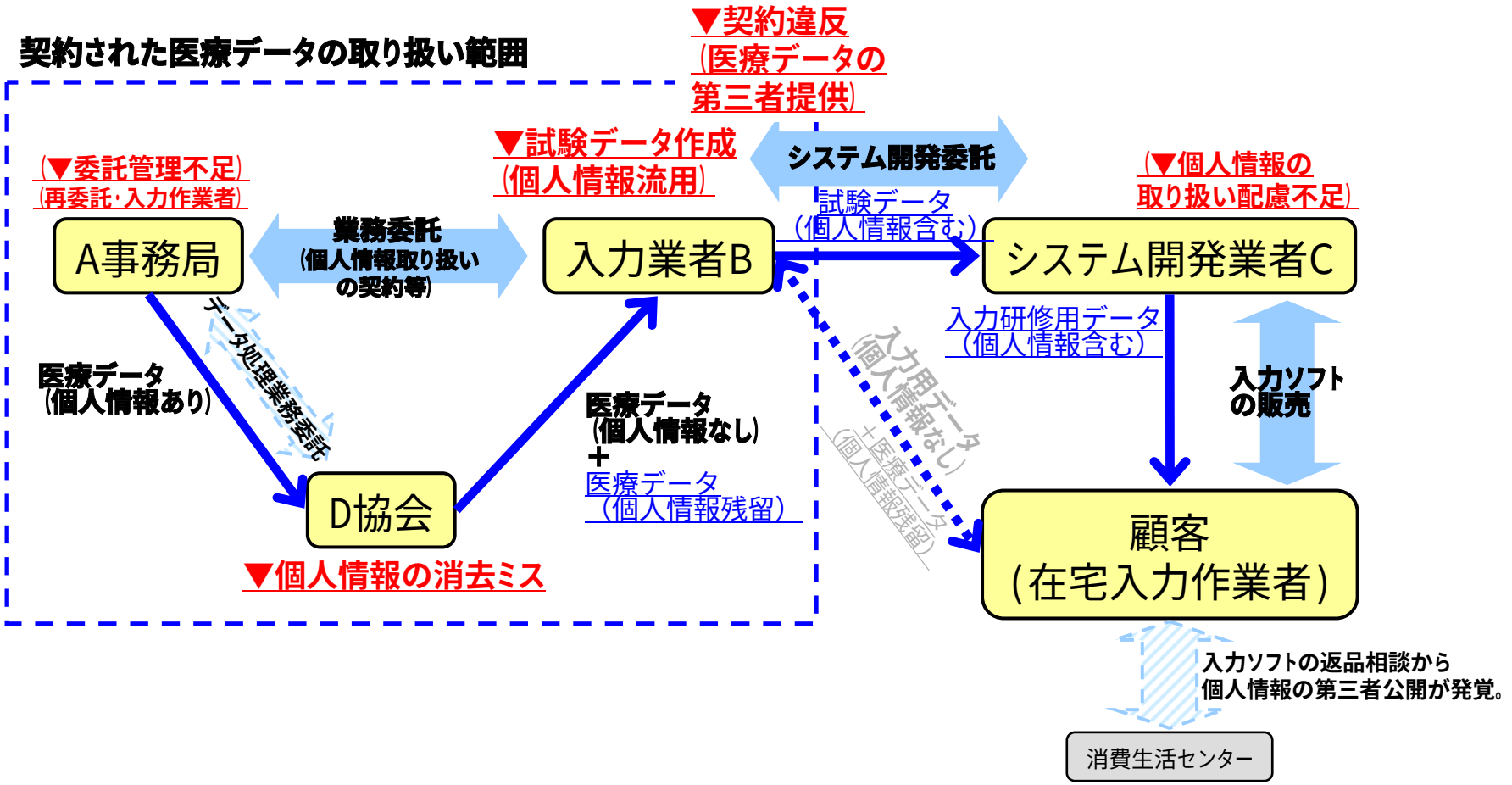
A事務局は、入力業者Bに医療データの入力業務を発注した。受注した入力業者Bは、入力システムの開発をシステム開発業者Cに依頼し、個人情報を含む医療データの一部を試験データとして提供した。システム開発業者Cは、入力業務の作業者（顧客）に対し、上記試験データを研修用データとして送付した。A事務局と入力業者Bの委託契約では、医療データの第三者提供を禁じていた。また、A事務局から医療データを入力用データに加工する処理を請け負ったD協会は、氏名、傷病名の消去確認作業を怠っていた。

《問題点》
- ■契約違反（入力業者B）
- ■試験データ作成（個人情報流用）
- ■個人情報の消去ミス（D協会）

《解決案》
- ■契約内容の遵守
- ■試験データの作成（個人情報なし）
- ■個人情報の取り扱いの配慮
- ■発注者による管理強化

医療データの目的外利用事件(補足説明)

情報漏えいの原因は、複数の関係者に渡って存在した。



事故事例「不正な情報持ち出し」

業務上の必要性などから、ルールを逸脱して情報を持ち出した場合。ただし、ルールを逸脱して情報や記録媒体を持ち出した場合、厳密には盗難であるが、下記のような場合は、不正な情報持ち出しとする。社員がルールを逸脱して機密情報を自宅に持ち帰り、ファイル交換ソフト経由で漏えいした場合も、不正な情報持ち出しに分類する。

例）社員、派遣社員、外部委託業者、出入り業者、元社員などが、顧客先、自宅などで使用するために情報を持ち出して、持ち出し先から漏えいした。

患者情報の持ち出し事件

発生年	業種	漏えい情報	原因	経路･媒体
2005年	医療、福祉	個人情報（262人）	不正な情報持ち出し	紙媒体
漏えい情報	氏名、住所、電話番号			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
1	1	2	6	1万2,000円	314万4,000円

医師Bは、A病院を退職する際に自分が診察した患者の名前、住所などの情報を持ち出した。医師Bは、医師と患者の連絡用ノートから、氏名と住所を自分のノートに転記し、医院開業の挨拶状を患者に送付した。

《問題点》
- 個人情報（営業秘密）の持ち出し
- 退職時の情報管理の不徹底

《解決案》
- 個人情報（営業秘密）に関する教育
- 退職時の情報管理の徹底

診療記録流出(Winny)事件

発生年	業種	漏えい情報	原因	経路･媒体
2005年	医療、福祉	個人情報(63人)	不正な情報持ち出し	PC本体
漏えい情報	氏名、生年月日、年齢、診療記録			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
2	1	11	3	3万3,000円	207万9,000円

医師が小児科の診療記録を研究目的で持ち帰り、データを保存した自宅の個人用PCが、P2Pファイル交換ソフトWinnyの新種ウイルスに感染し、診療記録がインターネット上に流出した。同病院では、個人情報の院外への持ち出しについては、口頭による注意を行っていたが、強制ではなく、自主規制に任せていた。

《問題点》
- 不要な個人情報の記録
- ファイル交換ソフト(Winny)の利用
- 自宅･個人PCの業務利用

《解決案》
- 個人情報の取扱いルール化
- 症例データ(研究用)の匿名化
- Winnyの危険性の把握/利用禁止
- 個人PCの業務利用禁止

事故事例「内部犯罪・内部不正行為」

社員、管理下にある他社社員(派遣社員など)が、不正アクセス、その他不正な行為によって情報を持ち出して悪用した場合。

外部の人間との結託や不正アクセスを伴う場合も、内部の人間の積極的な不正行為があれば内部犯罪・不正行為に分類する。

(業務上の必要性などから、ルールを逸脱して情報を持ち出した場合は、不正な情報持ち出しに分類する)

例) 社員・派遣社員など内部の人間が、機密情報を悪用するために不正に取得して持ち出した。持ち出した情報を使って犯罪を行ったり、売買したりして、漏えいした。

個人信用情報の不正流出事件

発生年	業種	漏えい情報	原因	経路･媒体
2007年	金融･保険業	個人情報（3806人）	盗難	Web･Net経由
漏えい情報	氏名、住所、電話番号、生年月日、性別、職業、信用情報			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
2	2	15	6	9万円	3億4,254万円

クレジットカードA社のカスタマーセンターの契約社員、派遣社員、アルバイトが、業務時間中に情報端末を使って個人信用情報機関にアクセスし、個人信用情報を不正に取得して第三者に提供していた。同社は、役員や従業員から確認書を徴収、従業員の面接を実施し、不正利用者を特定。経済産業省や警察へ事態を報告し、いずれの社員についても解雇や派遣契約解除を行った。

《問題点》
- ■不適切な操作権限
- ■業務上の不正操作の監視

《解決案》
- ■業務担当者･操作権限の見直し
- ■管理者によるログ監視
- ■照会記録の保管期限延長
- ■社内教育の実施

顧客リスト悪用（強盗）事件

発生年	業種	漏えい情報	原因	経路・媒体
2005年	複合サービス事業	個人情報（不明）	内部犯罪・内部不正行為	紙媒体
漏えい情報	氏名、住所、電話番号、生年月日、性別、簡易保険の情報			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
2	2	15	6	9万円	不明

監禁、恐喝した疑いで逮捕された元郵便局員らのグループは、簡易保険の顧客リストを悪用して、資産家を狙って強盗を繰り返していた。元郵便局員らは、在職中に簡易保険の営業をしていた。

《問題点》
- 顧客リストの悪用

《解決案》
- 顧客リストの厳重な管理
- 業務体制の見直し（相互監視）
- 人事考課（生活態度）

事故事例「管理ミス」

社内や主要な流通経由において紛失･行方不明となった場合。作業手順の誤りや、情報の公開、管理ルールが明確化されていなかったために業務上において漏えいした場合。紛失の責任が組織にある場合。(管理ミスによって盗難が発生した場合は、盗難に分類する。社内において、管理が行き届かずに誤って破棄した場合も含む)

例）引越し後に個人情報の行方がわからなくなった。

個人情報の受け渡し確認が不十分で、受け取ったはずの個人情報が紛失した。

情報の公開、管理ルールが明確化されておらず、誤って開示してしまった。

郵送物未配達事件

発生年	業種	漏えい情報	原因	経路･媒体
2004年	公務	個人情報（180人）	管理ミス	可搬記録媒体
漏えい情報	氏名、住所、免税証の利用記録			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
1	1	2	6	6,000円	108万円

自治体Aの支所Bは、個人情報を含む免税証の利用データを記録した可搬記録媒体（ＭＯ）を自治体Aに郵送したが、届かなかった。

《問題点》
■送付方法の選択ミス
（郵送中の紛失）

《解決案》
■書き留め等の信頼性の高い送付手段の利用

受領後書類の紛失事件

発生年	業種	漏えい情報	原因	経路･媒体
2007年	公務	個人情報（2人）	管理ミス	紙媒体
漏えい情報	住所、氏名、生年月日、被保険者番号、被保険者証、要介護状態、認定結果			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
1	1	2	6	6万6,000円	13万2,000 円

居宅介護系施設Aは、運輸会社Cに委託して介護保険の認定調査結果等の書類を自治体Bへ発送したが紛失した。運輸会社Cには配達記録があった。配達日は、自治体Bの休庁日であり、夜間･休日受付窓口に届けられた。自治体B内の関係各所を捜索したが、書類は見つからなかった。

《問題点》
- 書類の保管ミス
- 到着日指定ミス

《解決案》
- 書類管理の徹底
- 到着日の考慮

保管書類の誤廃棄事件

発生年	業種	漏えい情報	原因	経路･媒体
2007年	金融･保険業	個人情報（169,019人）	管理ミス	紙媒体
漏えい情報	氏名、住所、生年月日、運転免許証番号など			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	損害賠償額／人	損害賠償総額
1	1	2	6	1万2,000円	20億2,822万8,000 円

A銀行は、口座開設時などに作成した記録書と本人確認用の身分証明書の写しなどの書類を誤って破棄した。法改正により保存期限が5年間から7年間に変更されたが、保存年限修正などの具体的な指示がなかったため、5年間を過ぎた書類が順次廃棄されていた。書類は手順を経て廃棄されているため流出のおそれはない。事情説明と謝罪の文書を送付し、問い合わせ窓口を設置した。

《問題点》
■業務手順の変更忘れ

《解決案》
■外部要因の変化(法改正など)に伴う業務手順の変更徹底

想定損害賠償額算定式の使い方

想定損害賠償額/算定式の注意点

想定損害賠償額算定式は、各組織が所有する個人情報の潜在的リスクを把握するためのひとつの推定方法である。

- **保有する個人情報によるリスクを定量化し、個人情報を取り扱う組織のリスクを把握するもの**
- **算定結果は、対策するときの判断材料とするもの**

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”に基づくものである。

- **実際に各事例においてその金額が支払われたものではない**
- **被害者が漏えい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**

個人情報漏えいインシデントの被害額

インシデント被害額 ＝ 直接被害額 ＋ 間接被害額 ＋ 潜在化被害

- 逸失利益
- 復旧に要したコスト
- 営業継続費用
- 喪失情報資産額
- 機会損失額

システムの規模に応じた被害額

- 算出には多くの情報が必要
- 情報（資産）が失われない
- 個人情報が漏洩しても システムは停止しない

実被害額

- 補償、補填、損害賠償など、間接的に生じた被害額

補償・損害賠償 訴訟費用

- 報道された情報で推定可能

想定額

想定損害賠償額に限定して簡単な定式化を試みる

- 業務にかかわる潜在化被害
- 業務外の潜在化被害

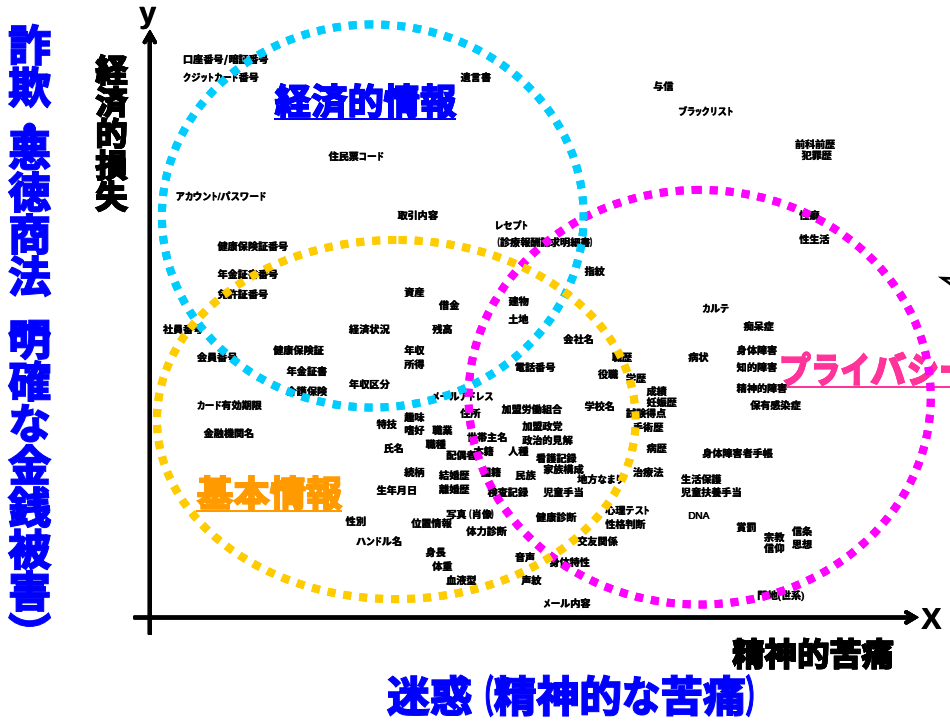
ブランド価値、顧客イメージ

- インシデントの報道は、株価に現れる可能性がある

想定額

個人情報の価値の考え方：EP図

個人情報の価値を「精神的苦痛」と「経済的損失」の2つのリスク値（座標値：x=精神的苦痛, y=経済的損失)を用いて定量化。



「個人情報の保護に関する法律（個人情報保護法）」、「個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS Q 15001）」などを参考に EP図上へ個人情報をプロット。

（情報セキュリティ被害調査WGの独自の考え方に基づく）

【EP図（Economic - Privacy Map）】

XとYの値が測りにくい・・・。

個人情報の価値の考え方：Simple - EP図

個人情報の価値の評価尺度を3段階とし、基準判断を簡易化

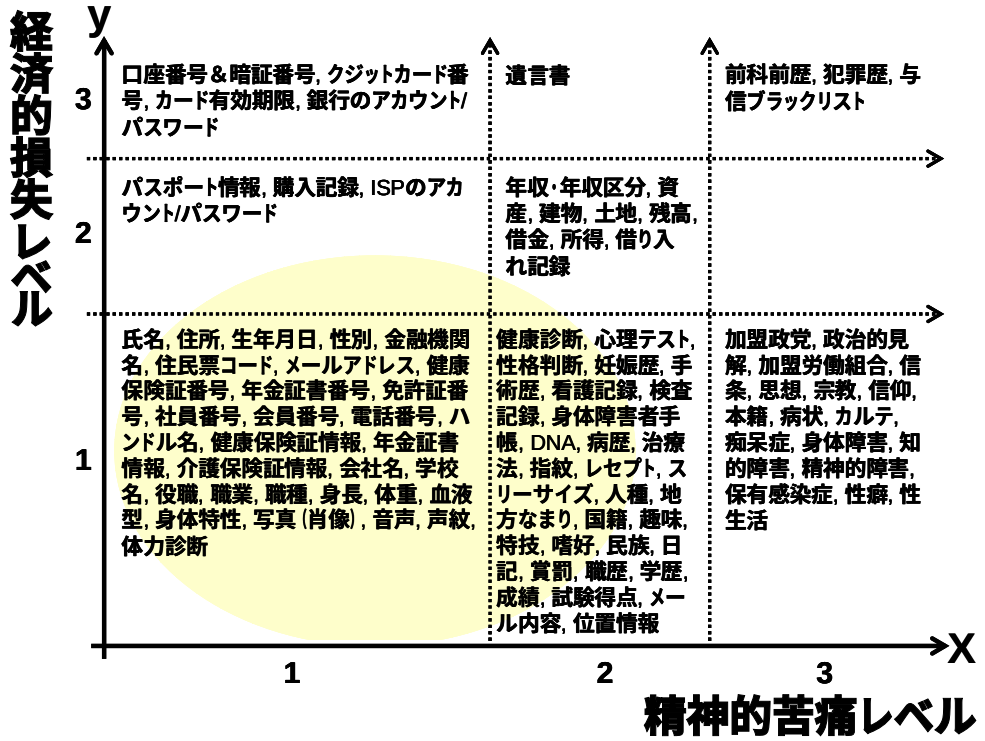
Simple-EP図から個人情報の機微情報度を算出

機微情報度

$$= (10^{x-1}+5^{y-1})$$

$10^0 \sim 10^2$ 精神的苦痛 ＝1～100万円

$5^0 \sim 5^2$ 経済的損失 ＝1～30万円



【Simple - EP図】

個人情報価値の算定式

個人情報価値＝基礎情報価値×機微情報度×本人特定容易度

■ **基礎情報価値：**
＝５００

2003年6月、ローソンカードの会員56万人の個人情報が漏えい。
同社は115万人全員に謝罪文と商品券500円分を郵送した。
これにより「1人あたり500円の謝金を配る」とする対応が増えた。

■ **機微情報度：**
漏えいした個人情報に含まれる機微情報の量

機微情報度＝ $(10^{x-1}+5^{y-1})$

Simple-EP図上の個人情報の座標値 (x,y) より
x = 漏洩した情報の精神的苦痛レベルの**最大値**
y = 〃 経済的損失レベルの**最大値**

■ **本人特定容易度：**
漏えいした個人情報からの個人特定しやすさ

判定基準	本人特定容易度
個人を簡単に特定可能。「氏名」「住所」が含まれること。	6
コストを掛ければ個人が特定できる。「氏名」または「住所+電話番号」が含まれること。	3
特定困難。上記以外。	1

想定損害賠償額の算定式

判定基準表を用いて、計算式への代入値を求める

想定損害賠償額

＝個人情報価値×社会的責任度×事後対応評価

＝基礎情報価値　　[500]
**　×機微情報度　　[Max (10^{x-1}+5^{y-1})]**
**　×本人特定容易度　　[6,3,1]**
**　×社会的責任度　[2,1]**
**　×事後対応評価　[2,1]**

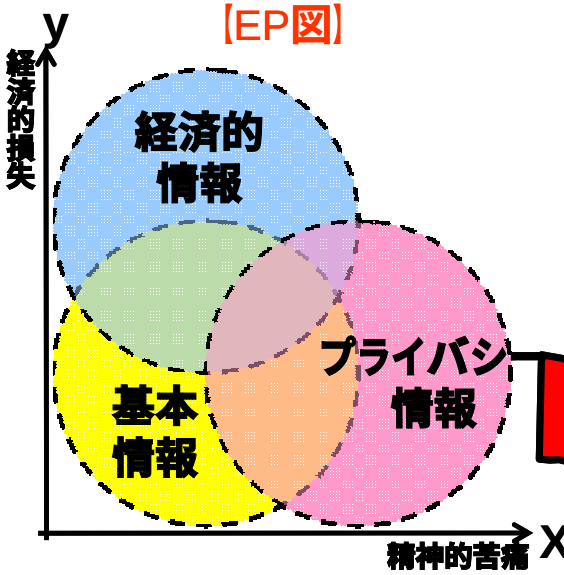
判定基準		社会的責任度
一般より高い	適正な取扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信等）および、知名度の高い大企業、公的機関。	2
一般的	その他一般的な企業および団体、組織。	1

判定基準	事後対応評価
適切な対応	1
不適切な対応	2
不明、その他	1

想定損害賠償総額＝想定損害賠償額×漏えい人数

想定損害賠償算定式のまとめ

【EP図】



【判定基準表】

判定基準	社会的責任度
一般より高い	適正な取扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信等）および、知名度の高い大企業、公的機関。
一般的	び団体、組織。

判定基準	事後対応
適切な対応	
不適切な対応	
不明、その他	

判定基準	本人特定容易度
個人を簡単に特定可能。「氏名」「住所」が含まれること。	6
コストを掛ければ個人が特定できる。「氏名」または「住所+電話番号」が含まれること。	3
特定困難。上記以外。	1

損害賠償額＝（基礎情報価値 × 機微情報度 × 本人特定容易度）
×情報漏洩元組織の社会的責任度
×事後対応評価

個人情報の基本的な価値を算出

漏洩組織の対応を評価

＝ 基礎情報価値[500]
×機微情報度[Max（$10^{x-1}+5^{y-1}$）]
×本人特定容易度[6, 3, 1]
×社会的責任度[2, 1]
×事後対応評価[2, 1]

想定損害賠償額算定式の使い方

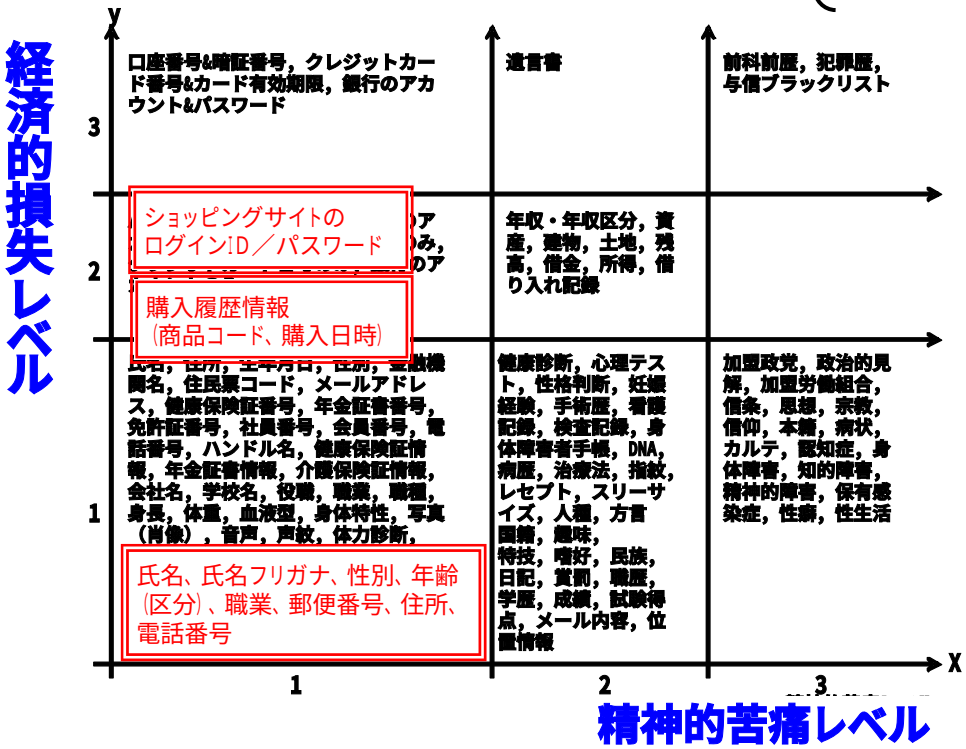
(練習問題)

算定例 ステップ1

機密情報度を算出する。

例えば次の情報が漏洩したとすると

- **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**



{氏名、氏名フリガナ、性別・・・}
→ 精神的苦痛レベル＝ 1
{購入履歴情報、ログインID/パスワード}
→ 経済的損失レベル＝ 2

機微情報度＝Max $(10^{x-1}+5^{y-1})$
$=10^{1-1}+5^{2-1}$
$=1+5=6$

算定例 ステップ2

判定基準表から、本人特定容易度、社会的責任度、事後対応評価を決定する。

【判定基準表】

判定基準	本人特定容易度
個人を簡単に特定可能。「氏名」「住所」が含まれること。	6
コストを掛ければ個人が特定できる。「氏名」または「住所+電話番号」が含まれること。	3
特定困難。上記以外。	1

漏洩情報に「氏名、住所」が含まれるので

本人特定容易度＝6

判定基準		社会的責任度
一般より高い	適正な取扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信等）および、知名度の高い大企業、公的機関。	2
一般的	その他一般的な企業および団体、組織。	1

漏洩元の組織が「卸売・小売業」とすると

社会的責任度＝1

判定基準	事後対応評価
適切な対応	1
不適切な対応	2
不明、その他	1

事後対応は適切だったとすると

事後対応評価＝1

※公表された内容からは、事後対応内容を性格に読み取ることが難しいため、ほとんどの場合において、適切な対応と判断している。

算定例 ステップ3

想定損害賠償額算定式に当てはめて、算出する。

機微情報度＝Max（$10^{x-1}+5^{y-1}$）
＝$10^{1-1}+5^{2-1}$
＝1+5＝6

本人特定容易度＝6

社会的責任度＝1

事後対応評価＝1

損害賠償額　＝　（基礎情報価値 × 機微情報度 × 本人特定容易度）
×情報漏洩元組織の社会的責任度
×事後対応評価
＝　基礎情報価値[500]
×機微情報度[Max（$10^{x-1}+5^{y-1}$）＝6]
×本人特定容易度[6, 3, 1]
×社会的責任度[2, 1]
×事後対応評価[2, 1]
＝　500 × 6 × 6 × 1 × 1
＝　18,000円

売上被害額と緊急対応費用の推定

詳細は、「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 第二部」を参照。

【企業プロファイル】
想定した企業は、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とした。近年は、インターネットショッピングサイトも運用し、インターネットショッピングサイトの売り上げは、会社全体の売り上げの約6%程度とした。以下に想定企業のプロファイルを示す。(インターネットショップ部門の利益率＝約6%、年間成長率＝約10%とする。)

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
従業員	約30名

30万人分が漏洩！

項目			費用
直接被害	逸失利益	インターネットショッピングサイト利益額(1ヶ月分)	約5,000万円
	機会損失	インターネットショッピングサイトの成長率分(1ヶ月相当)	約500万円
間接被害	業務継続費用	対策組織業務に係る人件費 (1ヶ月分)	約2,000万円
		セキュリティコンサルタントの依頼費用(1ヶ月分)	約500万円
	損害賠償費用	損害賠償費用	約108万円
		弁護士費用、裁判費用	約9万円
	見舞品費用	見舞品代＋送料他 (30万人分)	約2億1,000万円
	謝罪訪問費	謝罪訪問に掛かる費用(15人分)	約165万円
	広報費用	謝罪広告費(新聞5紙)	約1,000万円
		情報公開ページ作成費用(5回)	約25万円
	臨時的な対策費用	コールセンター設置費用(1ヶ月分)	約1,000万円
		問い合わせ窓口常駐人員(1ヶ月分)	約300万円
潜在化被害	影響業務	影響を受けた業務の人件費(1ヶ月分)	約3,000万円
	業務外の潜在化被害	ブランド価値の低下	＋α
		合計	約3億4,577万円

- 年間利益額＝約6億円 (年間売上げ＝約100 億円) に対して、約3億4,577万円は、企業にとって大きな影響。
- 費用 約3.8 億円のうち、約80%は、直接被害額と見舞品費用。
  (2003 年は、見舞品として500円～1000 円程度の商品券を進呈していた)