JNSA

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

PCネットワークの管理・活用を考える会
第1回 情報モラル・セキュリティ分科会

情報漏えいインシデントから学ぶセキュリティ対策

2008年10月15日(東京)
2008年10月29日(大阪)

JNSA セキュリティ被害調査WG
大谷尚通 (株)NTTデータ

セキュリティ被害調査WGの紹介

JNSA 解説

NPO 日本ネットワークセキュリティ協会（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を目標としている。
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、**「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。

目次

JNSA 解説

- 『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について
- 質疑応答

JNSA
解説

『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

JNSA 解説

漏えい人数	3,053万1,004人
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
一件当たりの漏えい人数	3万7554人
一件当たり平均想定損害賠償額	27億9,346.8万円
一人当たり平均想定損害賠償額	3万8,233円

過去最高

過去最高

過去最高

過去最高

一日平均2.4件

$$\frac{\text{3,053万1,004人}}{\text{1億2,777万1,000人}}$$ ＝ 約4人に1人の割合

2007年 インシデント・トップ5

JNSA 解説

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

JNSA 解説

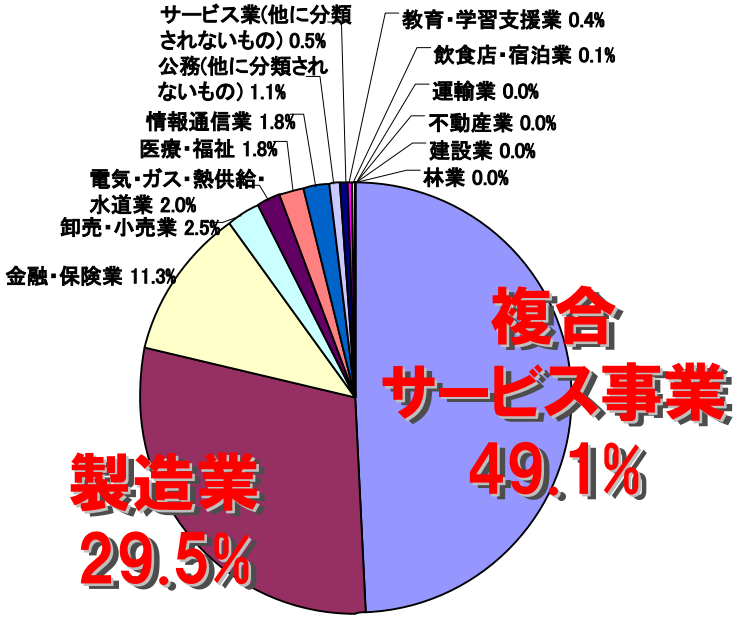


図 1：業種別比率（人数）

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

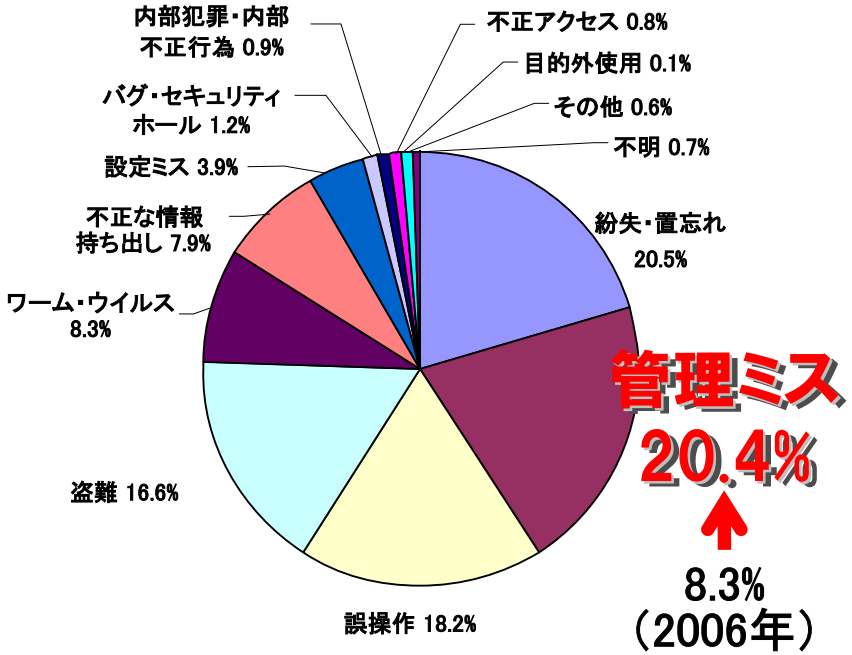


図 2：漏えい原因比率（件数）

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 単年・相関分析①

JNSA 解説

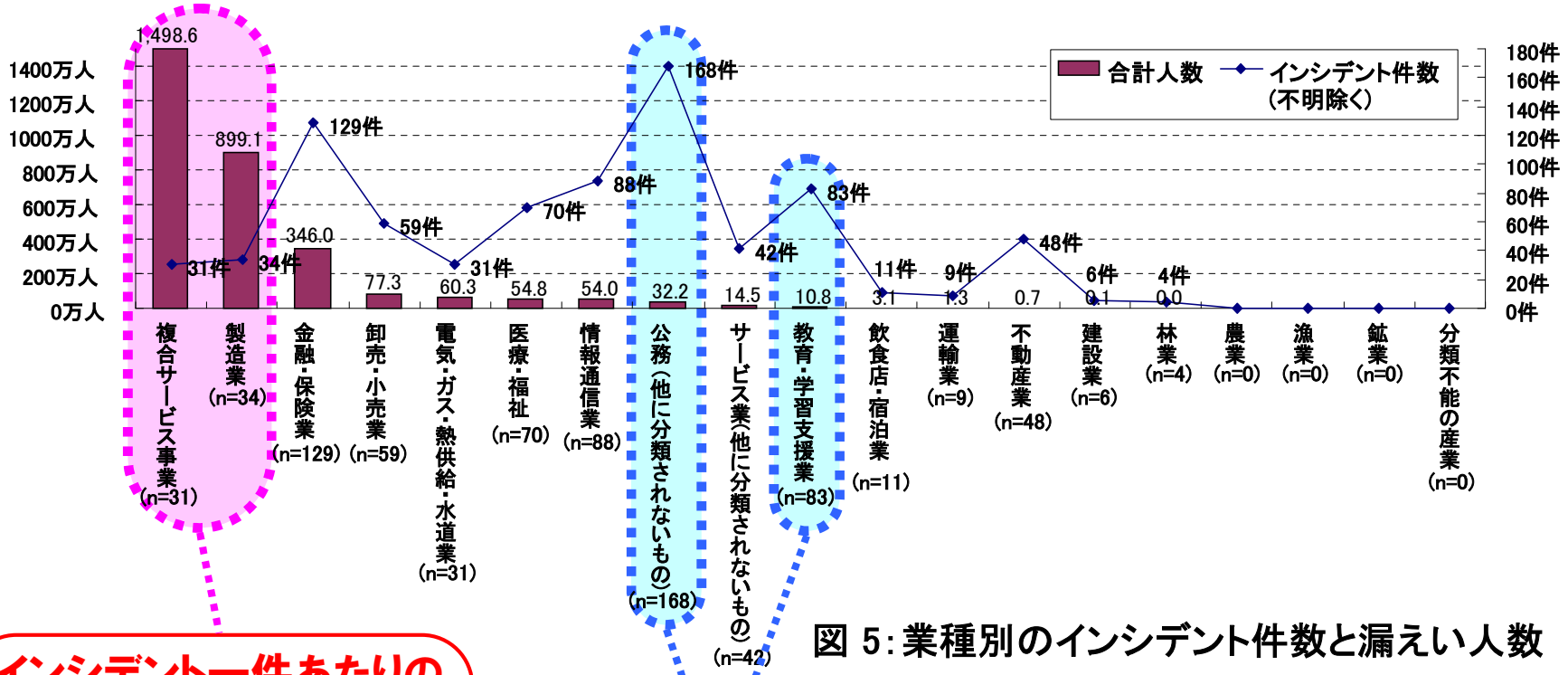


図 5：業種別のインシデント件数と漏えい人数

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）

大規模インシデントの影響

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

JNSA 解説

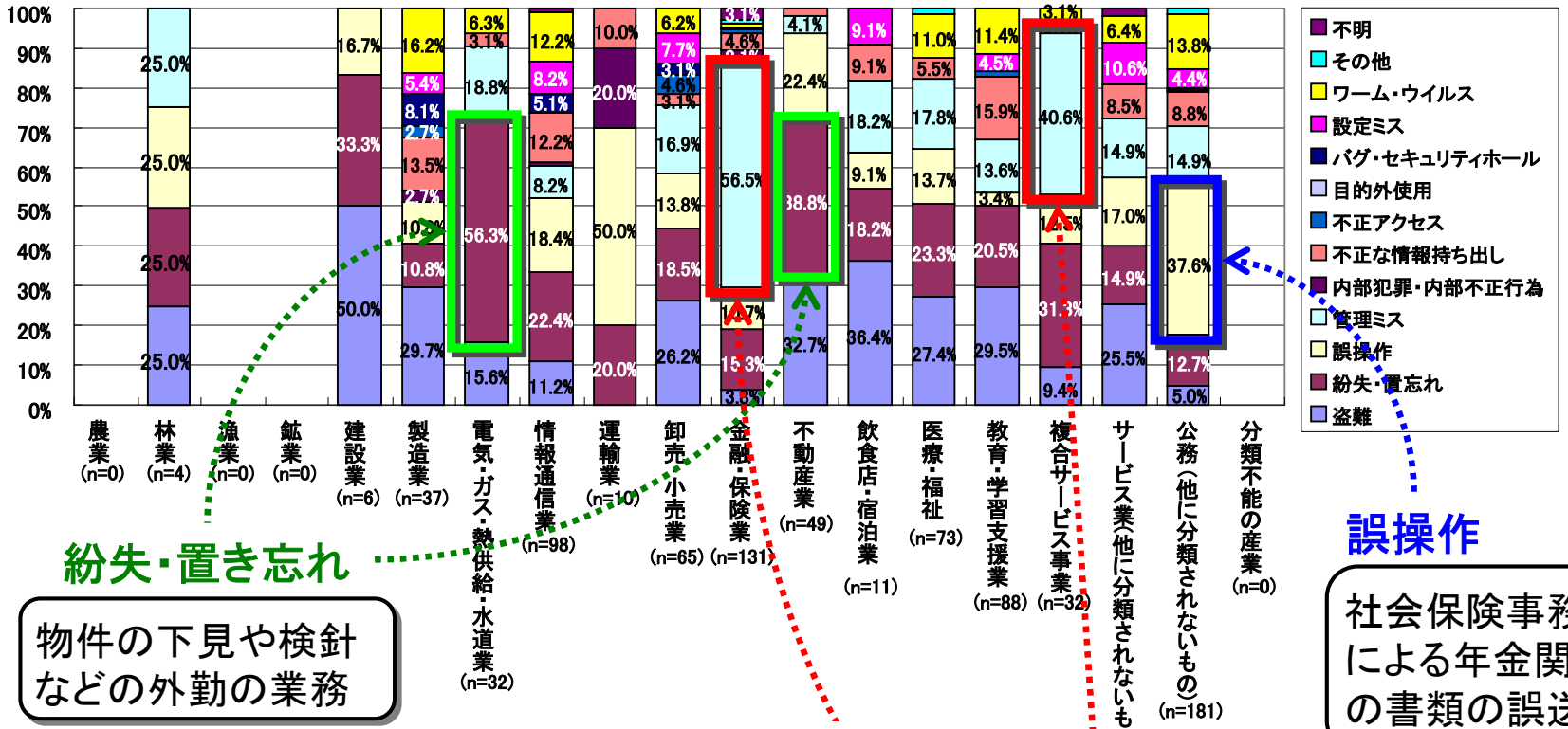


図 6:業種別の漏えい原因比率(件数)

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

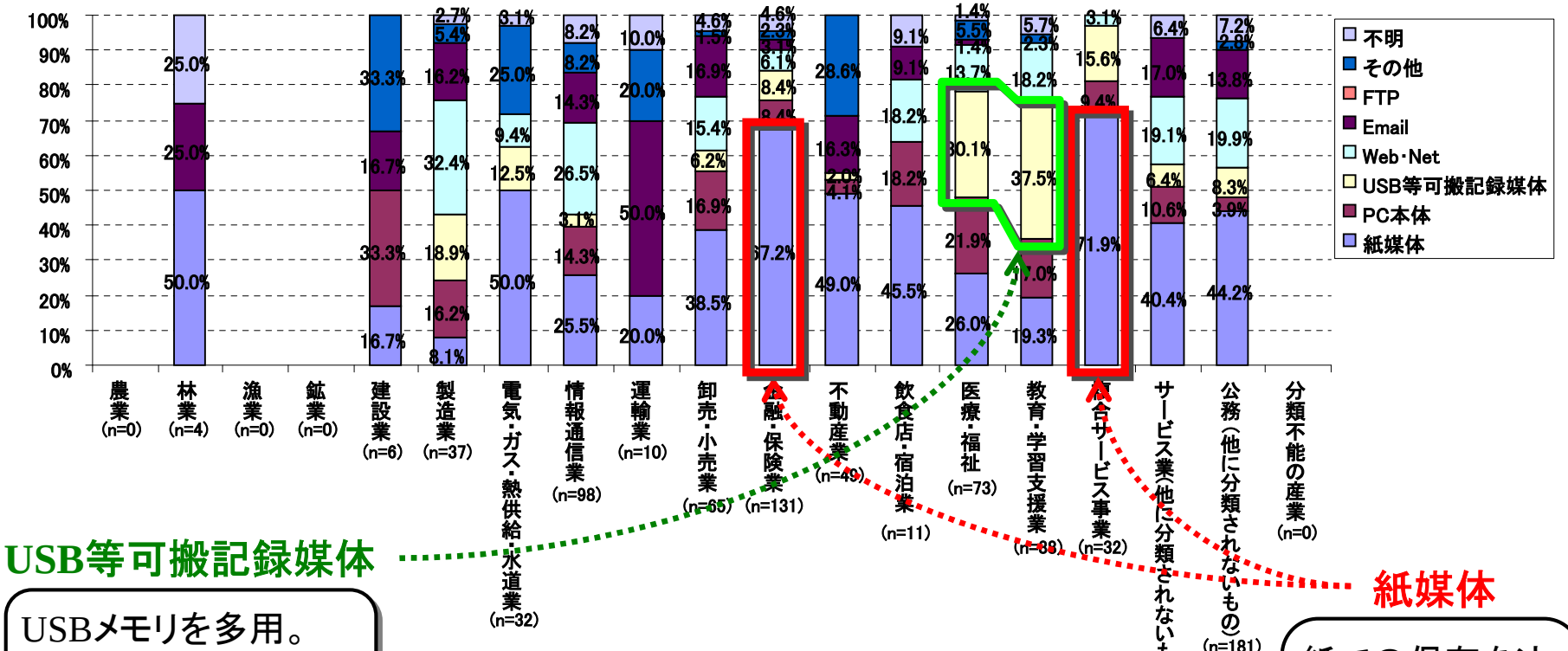
管理ミス

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。

漏えい原因は、個人情報を多く扱う業務・作業に関連する。

2007年 単年・相関分析③

JNSA 解説



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・媒体の比率（件数）

個人情報を扱う「業務・作業」と「媒体・経路」を把握
⇒特徴に応じて対策を実施

2007年 経年分析①

JNSA 解説

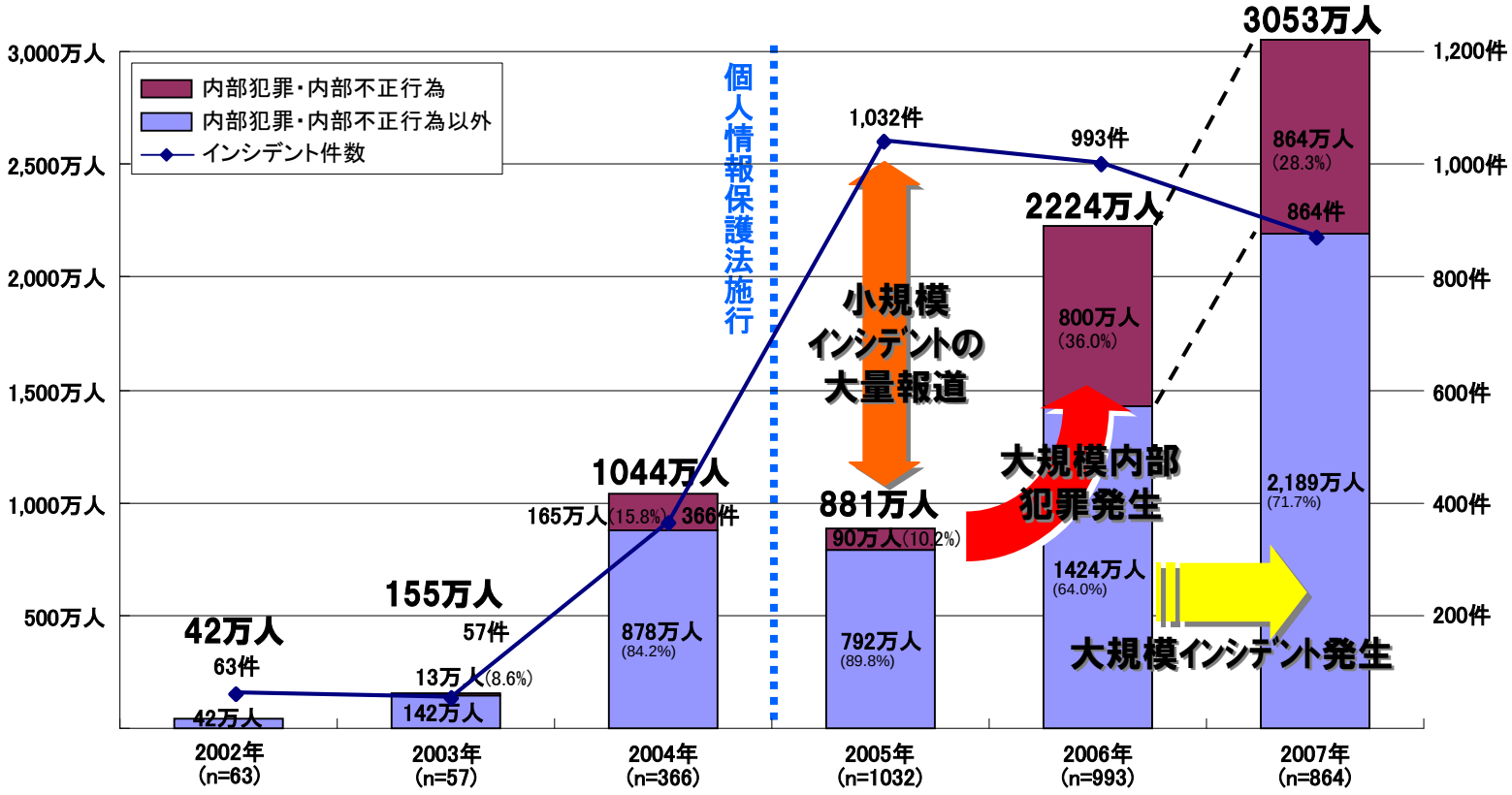


図 8:インシデント件数と内部不正による漏えい人数の経年変化(合計)

近年の漏えい人数増加 ＝ 内部犯と大規模インシデント

2007年 経年分析②

JNSA 解説

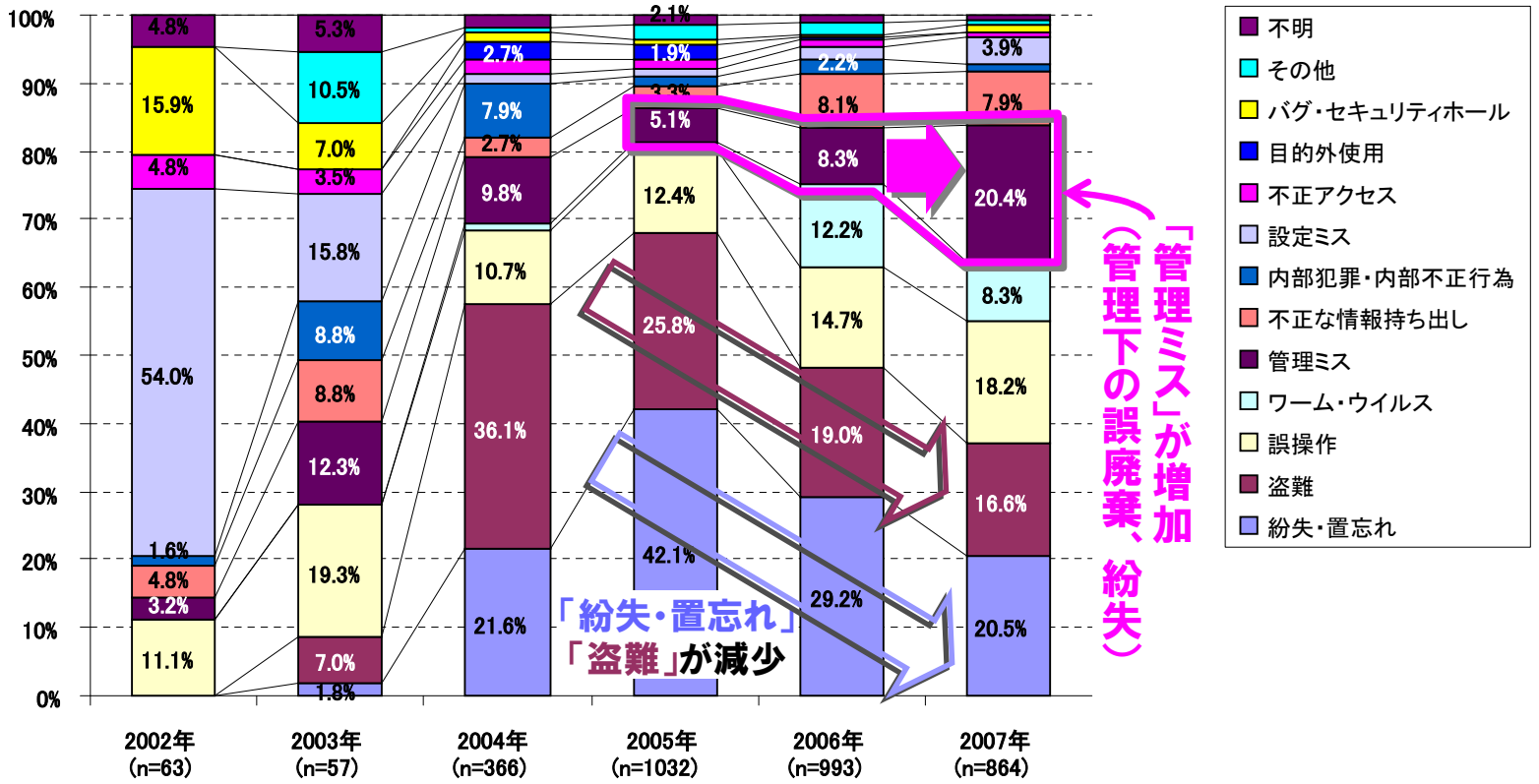


図 9:漏えい原因比率の経年変化(件数)

- 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

初期段階の情報漏えい対策が完了
情報漏えいの注意ポイントが変化

2007年想定損害賠償額の経年分析

JNSA 解説

	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年情報漏えいインシデントの総括

JNSA 解説

■ 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
→ 過熱報道・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
← 公表インシデントの統計結果の場合

Pマーク認定事業者のインシデント件数は、増加傾向
190件(2005年) → 708件(2006年) → 1,489件(2007年)
→ 認定事業者数の増加
事故報告の義務付け
潜在インシデントの顕在化

■ 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

JNSA 解説

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」

JNSA 解説

- 持ち出し許可を得て持ち出した情報を、個人のミスによって、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。
- 紛失した場合。
- （社内等において、保管すべき情報を紛失した場合は、管理ミスに分類する）

例）お客様の訪問にあたって正式に持ち出したPCを、電車に置き忘れて紛失してしまった。

メモリーカード紛失事件

JNSA 解説

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	想定損害賠償額／人	想定損害賠償総額
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**

漏えい二次被害の軽減策について

JNSA 解説

- **メモリーカード紛失事件**
  メモリカードを紛失したが、カード内のデータには暗号化を施している。
- **携帯型情報端末機 紛失事件**
  端末機を紛失したが、起動時のID・パスワード認証機能、時限式の全データ消去機能を備えている。

個人情報が漏えいした可能性は低い
（二次被害が発生する可能性が低い）

【Pマーク】欠格性の判断において、対応措置が軽減される

想定損害賠償総額
メモリーカード紛失事件　　＝51億1,218万円
携帯型情報端末機 紛失事件＝29億7,981万円

【注意】
個人情報のもつ潜在リスクを定量化した値である
軽減策については、考慮されていない

事故事例「盗難」

JNSA 解説

- 第三者によって、記録媒体と共に情報が盗まれた場合。
- （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

JNSA 解説

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	想定損害賠償額／人	想定損害賠償総額
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**

事故事例「目的外使用」

JNSA 解説

- 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。
- 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。

医療データの持ち出し事件

JNSA 解説

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）	目的外使用	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	想定損害賠償額／人	想定損害賠償総額
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。

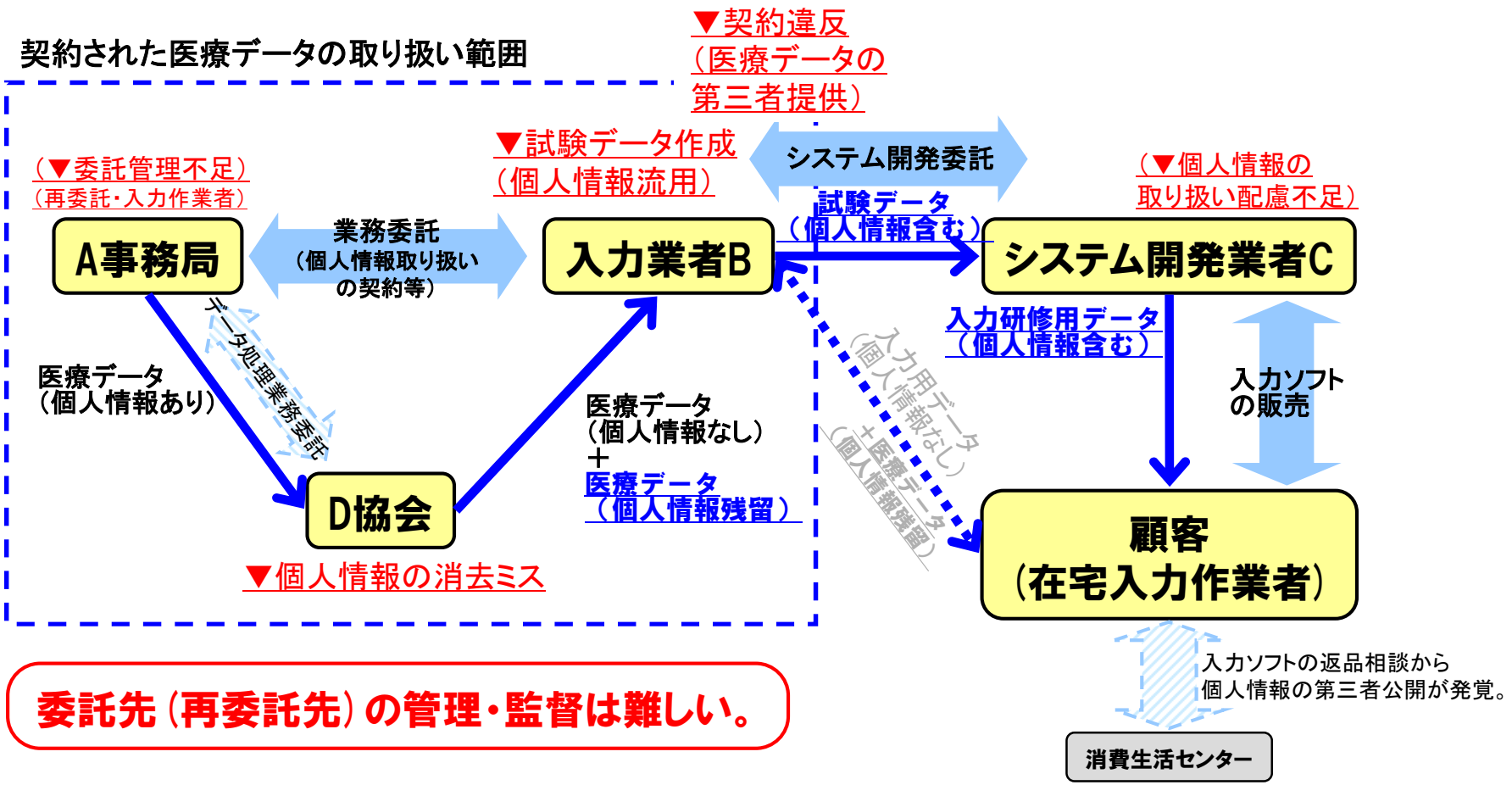
《問題点》
- ■契約違反（入力業者B）
- ■試験データ作成（個人情報流用）
- ■個人情報の消去ミス（D協会）

《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）

JNSA 解説

関係者が多く、かつ、情報漏えいの原因は、複数の関係者に及んだ。



事故事例「不正な情報持ち出し」

JNSA 解説

- 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、業務のために持ち出した場合は、悪意はないので、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。

私物USB紛失事件

JNSA 解説

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）	不正な情報持ち出し	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	想定損害賠償額／人	想定損害賠償総額
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

診療記録流出（Winny）事件

JNSA 解説

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	想定損害賠償額／人	想定損害賠償総額
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「ワーム・ウイルス」

JNSA 解説

- ワーム・ウイルスによって、情報が漏えいした場合。
- セキュリティホール等を利用したワーム、ウイルスによって、情報が漏えいした場合も含む。
- （ワーム・ウイルスがファイル交換ソフトに感染して情報が漏えいした場合、自宅に情報を持ち帰るなどの不正な情報持ち出しや社内のPCでファイル交換ソフトを使用するなどの管理ミスが伴った場合、原因は不正な情報持ち出しや管理ミスに分類する。）

例）社内のPCがワームに感染し、ワームがメールアドレス一覧などの個人情報を含んだメールを社外の多人数に発信してしまった。

職員情報の漏洩(Share)事件

JNSA 解説

発生年	業種	漏えい情報	原因	経路・媒体
2007年	公務	個人情報(15,000人)	ワーム・ウイルス	Web・Net
漏えい情報	氏名、ID、メールアドレス、部署名			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	想定損害賠償額／人	想定損害賠償総額
1	1	2	3	6,000円	9,000万円

地方自治体Aの職員のICカード作成業務を担当していた委託先B社の社員Cが、職員情報を自宅に持ち帰って私有パソコンで作業を行った。この私有パソコンにはP2Pファイル交換ソフト「Share」がインストールされており、ウイルスに感染していたことから、インターネット上に職員情報が流出した。

《問題点》
- ■ウイルス感染
- ■ファイル交換ソフト(Share)の使用
- ■個人情報の持ち帰り
- ■自宅PCの業務利用

《解決案》
- ■ウイルス対策ソフト
- ■Shareの危険性の把握／利用禁止
- ■個人情報の持ち出し禁止(ルール／機能)
- ■委託先のセキュリティ管理
- ■個人PCの業務利用禁止

事故事例「内部犯罪・内部不正行為」

JNSA 解説

- 社員、管理下にある他社社員(派遣社員など)が、犯罪などの目的のために悪意を持って不正アクセス、その他不正な行為を行って情報を取得し、持ち出した場合。
- 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)派遣社員が、個人情報を転売目的のため、不正に取得して、社外に持ち出した。持ち出した情報は、売買された後、インターネット上に漏えいした。

個人信用情報の不正流出事件

JNSA 解説

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
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	想定損害賠償額／人	想定損害賠償総額
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

事故事例「管理ミス」

JNSA 解説

- 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など、紛失の責任が組織にある場合。
- 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。
- （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）

例）引っ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。

保管書類の誤廃棄事件

JNSA 解説

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	想定損害賠償額／人	想定損害賠償総額
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

事故事例「バグ・セキュリティホール」

JNSA 解説

- OSやアプリケーション等の既存ソフトウェア上のバグ・セキュリティホールが原因で情報が漏えいした場合。
- ユーザ側でバグ・セキュリティホールが放置されていた場合や、ソフトウェアベンダーやシステムベンダーによる対処がされていなかった場合も含む。

例）Webアプリケーションのバグ・セキュリティホールにより、Webサーバ上の機密情報が閲覧可能となり、漏えいした。

バグによる情報漏洩事件

JNSA 解説

発生年	業種	漏えい情報	原因	経路・媒体
2007年	製造業	個人情報（46人）	バグ・セキュリティホール	Web・Net
漏えい情報	氏名、住所、電話番号、生年月日、メールアドレスなど			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	想定損害賠償額／人	想定損害賠償総額
1	1	2	6	6,000円	27万6,000円

PCパーツの製造販売を行うA社のショッピングサイトにおいて、アクセスしている顧客を識別する「セッションID」が重複して発行されるバグがあり、同時にサイトを利用していた他顧客の個人情報が表示されたり、他の顧客のカード情報で買い物の決算が行われるなどの問題が発生した。

《問題点》
■プログラムのバグ
（セッションIDの重複生成）

《解決案》
■信頼性のあるプログラムの利用
（セッションIDの生成処理プログラム）
■アルゴリズム／コードのレビュー
■負荷試験（レースコンディション）

事故事例「不正アクセス」

JNSA 解説

- 第三者が、主にネットワークを経由して不正にアクセスを行い、組織の管理する機密情報が漏えいした場合。
- （従業者・使用人など内部の人間の不正アクセスの場合は、内部犯罪・不正行為に分類する。）

例）インターネットから、サーバのアクセス制御を破って侵入され、機密情報が外部に持ち出されて漏えいした。

SQLインジェクションによる個人漏洩事件

JNSA 解説

発生年	業種	漏えい情報	原因	経路・媒体
2008年	卸売・小売業	個人情報（97,500人）	不正アクセス	Web・Net
漏えい情報	氏名、性別、生年月日、メールアドレス(ログインID)、パスワード、カード番号、有効期限			

精神的苦痛	経済的損失	機微情報度	本人特定容易度	想定損害賠償額／人	想定損害賠償総額
1	2	6	1	9,000円	8億7,750万円

楽器等を販売するA社が独自開発したショッピングサイトに対して、SQLインジェクション攻撃によってバックドア（不正侵入用の裏口）が作成され、そのバックドアを経由してサイトのWebサーバに悪性プログラムが置かれた。悪性プログラムは、データベースから顧客情報を抽出し、外部へ送信した。

《問題点》
- **脆弱性（SQLインジェクション）の存在**
- **ログ監視（不正アクセス監視）**
- **セキュリティ診断**

《解決案》
- **製造過程でのセキュリティ対策（事前）**
  （システム改修時のセキュリティ対策）（事後）
- **Webアプリケーション診断**
- **WAF**

「事故事例」から学ぶ

JNSA 解説

もし、自組織の状況に似た事故事例があったら・・・

- 自組織の業務と比較、発生する可能性を検討してみる
- 自組織のセキュリティ対策と比較、再点検してみる

実際に起きた事故事例から・・・

- 自組織の事故発生のシナリオをシミュレーションしてみる
- シミュレーションから、個人や組織のリスクを理解しておく
- 事故発生直後からの社員の対応手順をシミュレーションしてみる

JNSA 解説

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

JNSA 解説

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

JNSA 解説

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

- 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

「想定損害賠償額算定式」
（誰でも使える簡単な定式化！）

JNSA 解説

想定損害賠償額算定式の使い方

（算出例）

算定例 ステップ1

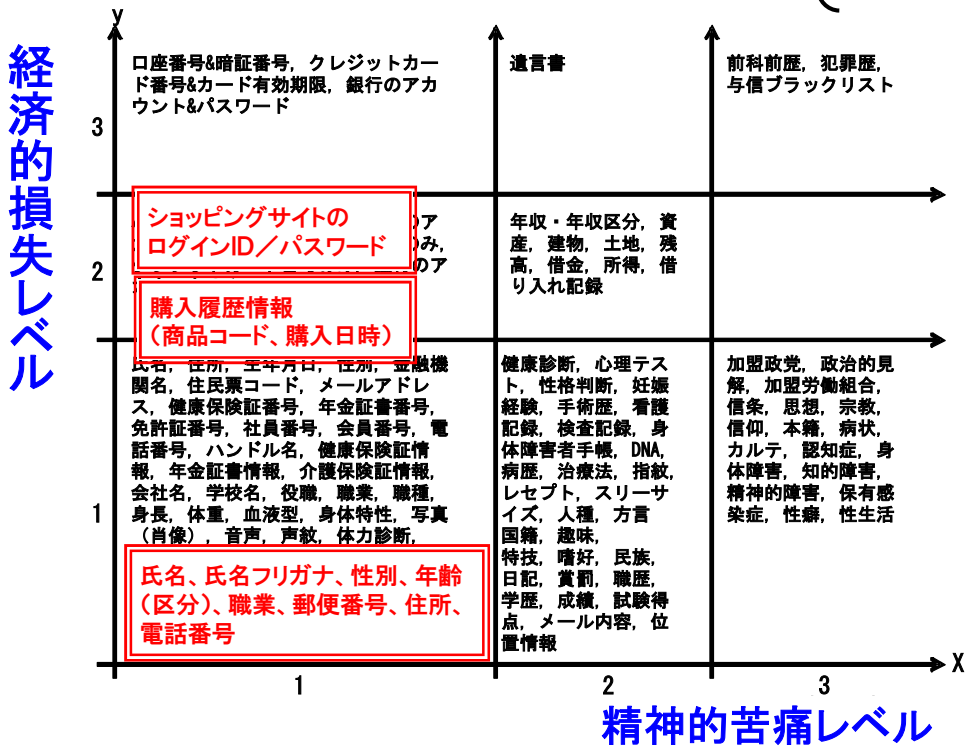
JNSA 解説

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

【Simple-EP図】



{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

JNSA 解説

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

JNSA 解説

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

利用例：
■個人情報を含むシステムのリスク把握
■複数のシステムのリスク比較 優先順位づけ

売上被害額と緊急対応費用の推定

JNSA 解説

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)

想定損害賠償額算定式のまとめ

JNSA 解説

■ **想定損害賠償額算定額（算定式）はリスクを比較する”ものさし”**

実際の損害賠償額ではない

保有する個人情報によるリスクを定量的に示す方法

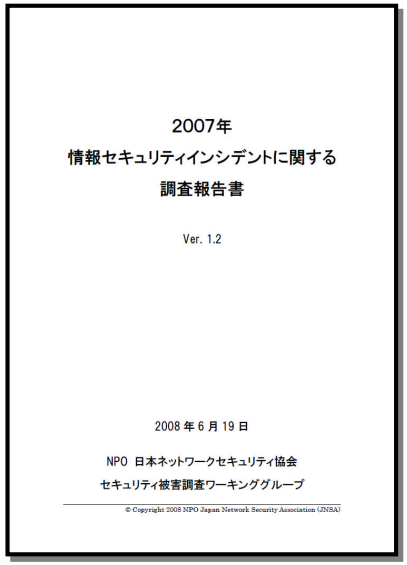
■ **まず、個人情報を保有／扱うことのリスクを把握する**

保有する個人情報によるリスクを明確化して把握する

算定結果は、対策優先度などの判断材料に利用

2007年報告書／データ集

解説


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

Ver. 1.2

2008 年 6 月 19 日

NPO 日本ネットワークセキュリティ協会
セキュリティ被害調査ワーキンググループ

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