JNSA

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

NetworkSecurityForum2008

情報システム担当者が語る
『わが社の情報セキュリティ運用術』

2008 年 12月17日

JNSA ユーザー部会
(株)大塚商会　佐藤　憲一

セキュリティ被害調査ＷＧの紹介

JNSA

平成19年度、JNSA「情報セキュリティインシデント被害調査」、JISA「個人情報の取扱における事故報告の傾向と注意点」では、携帯電話やUSB等の紛失事故をはじめとして、winnyによる情報漏えい等、企業内ユーザーの過失による事故が上位を占めていた。

加えて、多くの情報システム担当者からも、社内ユーザーへの情報リテラシー向上や漏えい防止に直結する運用方法のノウハウを望む声が多くなってきた。

当セミナーでは、企業の情報システム担当者が、これらの課題に対して、どのように解決してきたかを紹介するとともに、講師の方々と意見交換を行いながら、皆様の抱えている課題解決への糸口を模索したいと思っております。

モデレーター：
佐藤　憲一氏／(株)大塚商会
パネラー：
山岡正輝 氏／(株)NTTデータ
平田彰禎 氏／オムロン(株)
中野　清 氏／(株)大塚商会

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』 -- JNSA
- 『平成19 年度　個人情報の取扱いにおける事故報告の傾向と注意点』 -- JISA
- 『わが社の情報セキュリティ運用術』 紹介
- 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』

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WGメンバー

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

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

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

2006年

被害人数	業種名	漏洩原因区分
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

2007年 単年分析

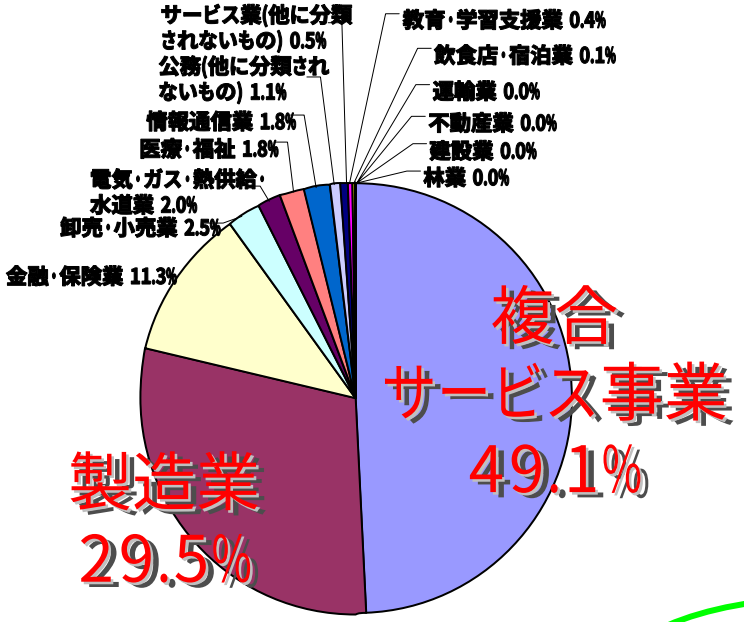

図 1：業種別比率（人数）

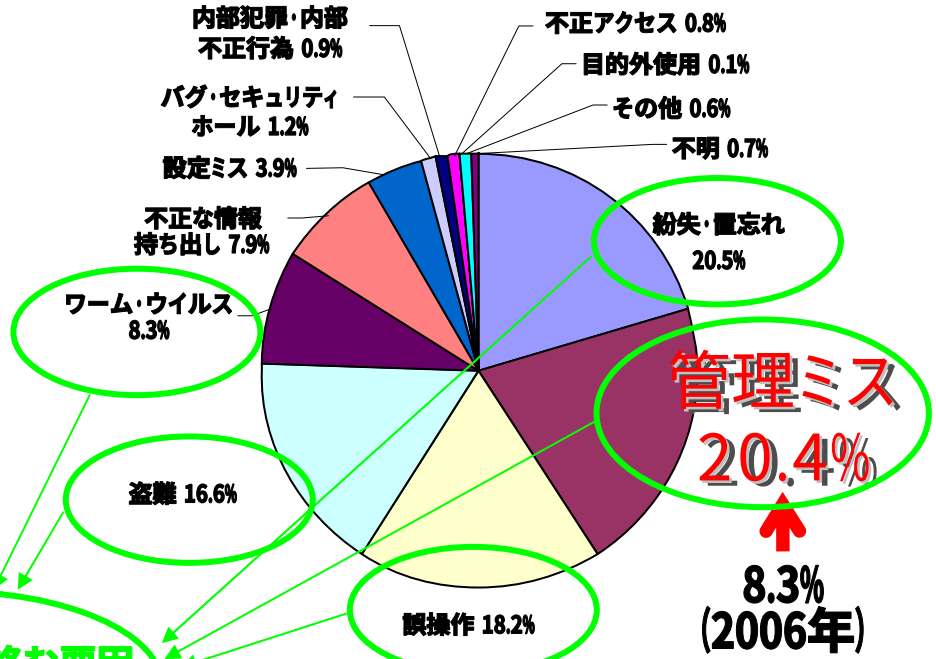

図 2：漏えい原因比率（件数）

「本人責任」が絡む要因
63．6%＝2／3

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 経年分析①

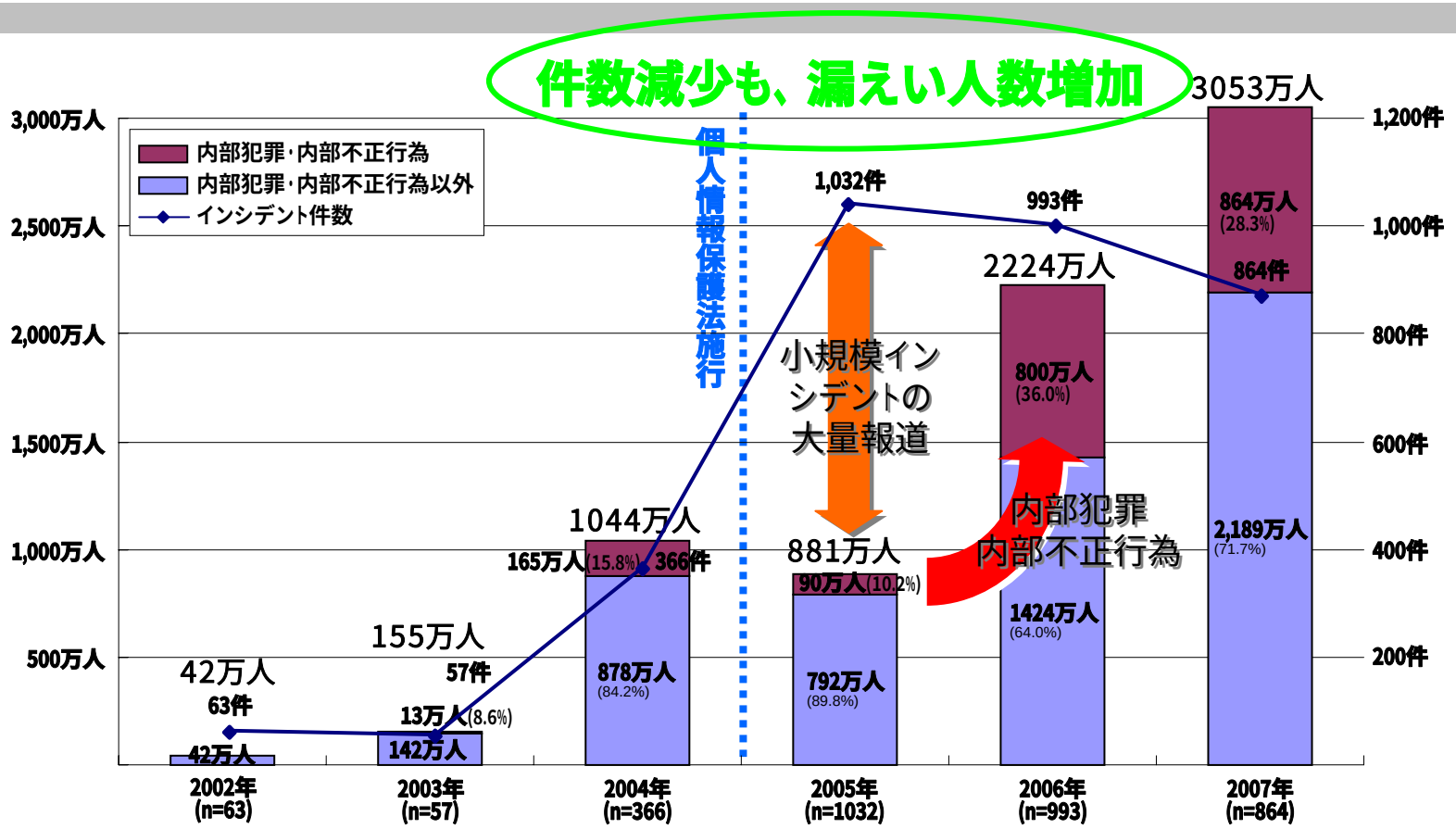

図 8:インシデント件数と内部不正による漏えい人数の経年変化(合計)

2007年 経年分析②

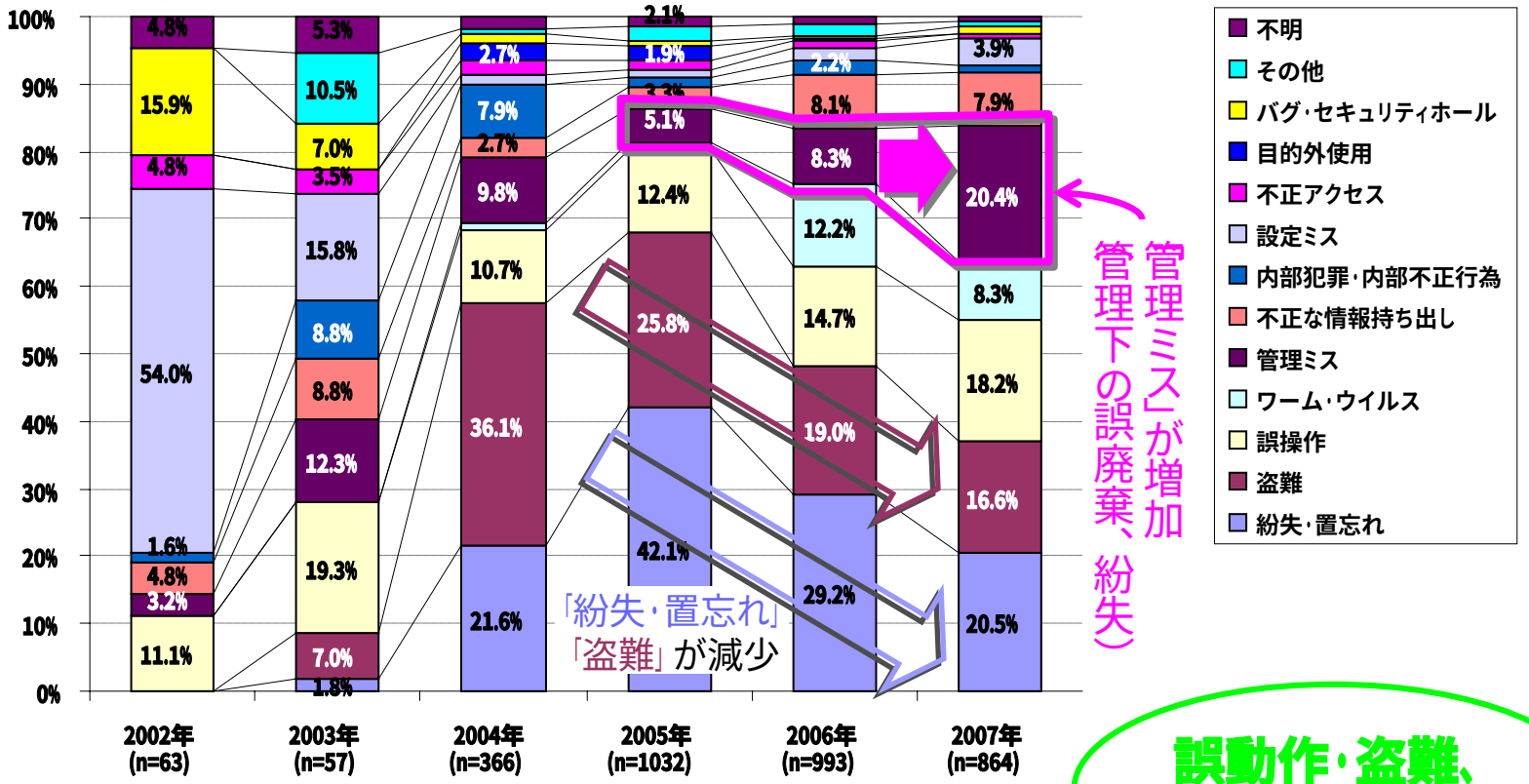

図 9：漏えい原因比率の経年変化（件数）

- **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

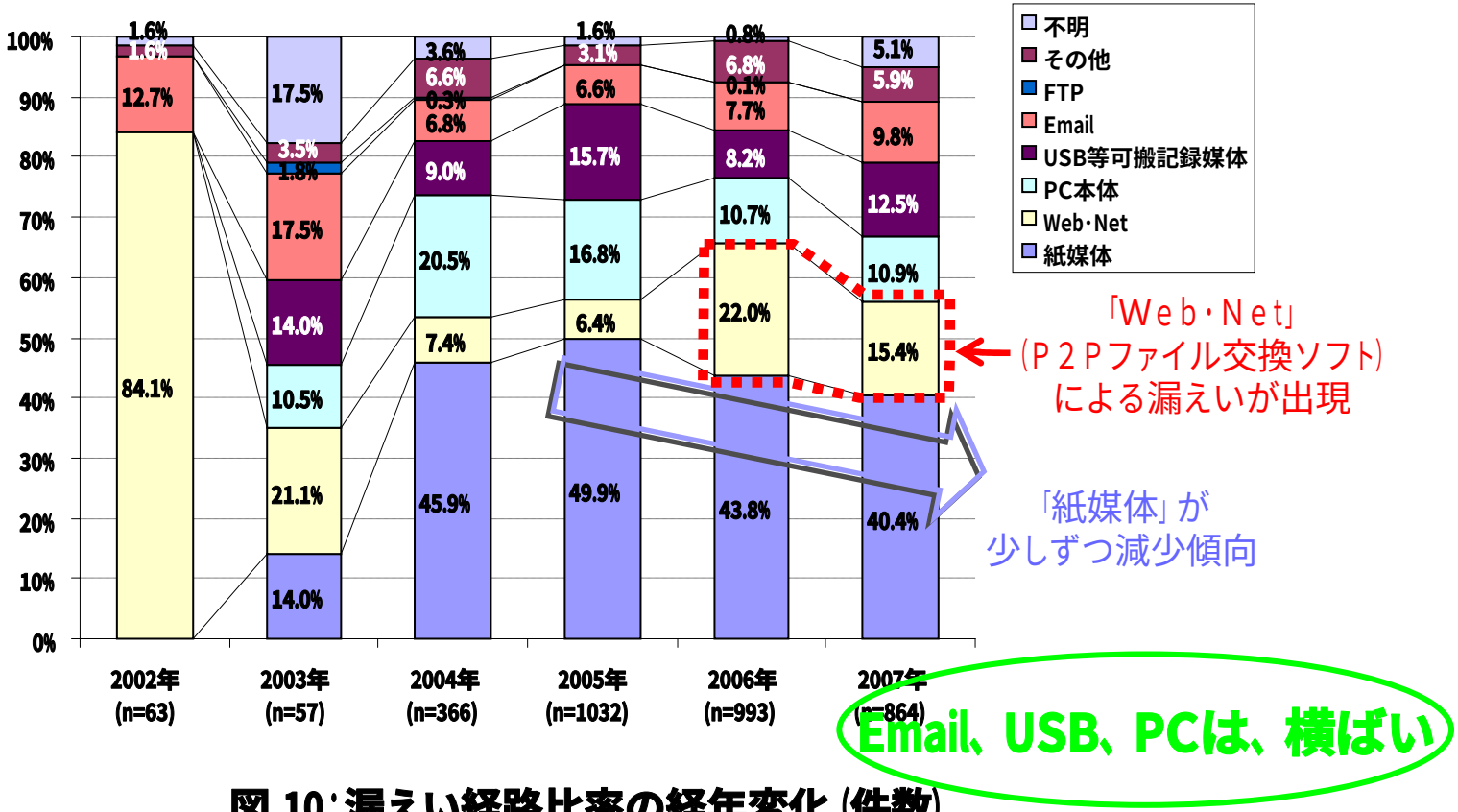

図 10：漏えい経路比率の経年変化（件数）

- **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**

事故事例と対策(1)

【私物ＵＳＢ紛失事件】

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、生年月日などが私物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

【携帯型情報端末機紛失事件】

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

事故事例と対策(2)

【ノートPC紛失事件】

**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

【ノートPC盗難(車上荒らし)事件】

**営業社員が、自宅駐車場の車の中から、夜間に業務用ノートPC1台を盗まれた。
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。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

事故事例と対策(3)

【個人信用情報の不正流出事件】

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

【医療データの持ち出し事件】

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

事故事例と対策(4)

【診療記録流出(Winny)事件】

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、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

【電子メール同報送信事件】

プロバイダA社は、電子メールで同社サービスの障害報告を同報メールで送る際、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

平成19 年度
個人情報の取扱いにおける
事故報告の傾向と注意点

平成20年7月16日
社団法人情報サービス産業協会
審査業務部

社団法人情報サービス産業協会

http://www.jisa.or.jp

表１ JISA 認定事業者における個人情報関連事故の原因別割合

１．１ 事故報告件数

平成19 年度の1 年間で当協会が受け付けた事故報告件数は88 社141 件です。事故の件数は、平成18 年度の報告（52 社74 件）に比してほぼ倍増しています。

	平成17年度		平成18年度		平成19年度		19/18比
紛失（パソコン・携帯電話・書類など）	25	36.2%	16	21.6%	45	31.9%	281%
電子メールの誤送信	3	4.3%	12	16.2%	25	17.7%	208%
委託先業者による事故	9	13.0%	11	14.9%	＊19	13.5%	173%
発送物やFAX の誤送付（誤封入）	4	5.8%	9	12.2%	18	12.8%	200%
盗難（空巣・車上荒らし・置引き）	5	7.2%	4	5.4%	10	7.1%	250%
ファイル交換ソフト（Winny など）	5	7.2%	13	17.6%	10	7.1%	77%
プログラムミス	2	2.9%	1	1.4%	7	5.0%	700%
宅配便・郵便による紛失	1	1.4%	4	5.4%	3	2.1%	75%
外部からの不正アクセス	2	2.9%	2	2.7%	1	0.7%	50%
従業者による不正持ち出し・悪用	2	2.9%	1	1.4%	0	0.0%	-
その他	11	15.9%	1	1.4%	3	2.1%	300%
合計	69	100%	74	100%	141	100%	191%

＊平成19 年度「委託先業者による事故」の内訳は、ファイル交換ソフト6 件、電子メールの誤送信5 件、発送物やFAX の誤送付4 件、紛失3 件、盗難1 件です。

2．事故等の問題点及び事故等防止のための注意点(1/3)

2．1 紛失（パソコン･携帯電話･書類など）による事故について

ノートパソコン、携帯電話、書類等の置き忘れや所在不明による個人情報の紛失事故は依然として後を絶ちません。特に、携帯電話の紛失に係る事故報告は最近増加傾向にあります。

再発防止策としては、従業者の意識の向上を図ることが最も重要です。ノートパソコン等を紛失した際には、二次的被害として大量の個人情報の漏えいにつながることを想定し、持ち出しを必要最小限にする、私物の持ち込みを禁止する、持ち出し及び持ち込みについて記録を残すといった管理ルールを定め、それらを従業者に周知徹底することが必要です。重要データの暗号化等の安全管理措置も有効ですが、そもそも持ち出す必要のない個人情報は社外に持ち出さないという意識付けも重要です。

また、携帯電話についても、紛失時には記録された個人情報が二次的被害として悪用されるおそれがあるため、管理ルールを定め、教育等を通じて従業者に周知徹底する必要があります。携帯電話の安全管理措置としては、紛失防止対策（ストラップ、チェーン等）、セキュリティ対策（ダイヤルロック、生体認証、遠隔データ消去等）が挙げられます。

2．2 電子メールの誤送信による事故について

送付物等の誤封入･誤送付に続いて、メールの送信に伴う漏えい事故も増えています。添付ファイルを誤って送信することのほか、複数の者に一斉にメールを送信（同報メール）する際に宛先が見える形（本来Bcc で送信すべきところTo やCc で送信する）で送信し、メールアドレスを漏えいするケースが非常に目立っています。

再発防止策として、メールソフトの設定変更や同報メール用の専用ソフトを使うことも考えられますが、最終的には送信前の確認行為を徹底することが重要です。そのためには、確認行為のルールを教育等を通じて従業者に周知徹底し、それが実際に行われているかを定期的に確認することが必要であり、個人情報保護マネジメントシステムにおける運用の確認に取り込むことが重要です。

また、添付ファイルの送信については、送信先を誤った場合に備えて、暗号化やパスワード保護等の安全管理措置を講じることが有効と言えます。

2．事故等の問題点及び事故等防止のための注意点(2/3)

2．3 委託先業者による事故について

事故等については、自社のみならず、委託先会社（協力会社）等においても生じており、郵便事業株式会社や宅配便事業者による紛失事故を合わせると平成19 年度は22 件15.6%となりました。

JISA 個人情報保護ガイドライン第25 条（JIS Q 15001:2006 の3.4.3.4）では、委託する個人情報の安全管理が図られるよう、委託先の監督について、特に委託先との契約内容が適切に遂行されていることを確認することが規定されています。

委託先において事故が発生した場合は、委託元は原則として免責されることはなく、過失割合によって責任を負う可能性があることを認識しなければなりません。また、委託先によって生じた事故についても、事故による経済的損失より、本人に及ぼす影響、社会的信用の失墜が大きいことを認識しなければなりません。

事故報告においては、委託元として、①委託先における個人情報の取扱い状況を把握していない、②委託先の調査を定期的に実施していない、③定期的な業務報告を受けていないといった管理ルールの不十分さが目立ちました。

管理上のポイントとしては、①委託業務の実態に見合った委託先選定基準・評価基準であるか、②継続的な委託を行っている場合は、定期的に業務の監督・チェックを実施しているか、③業務上委託する必要のない個人情報まで委託していないかを精査することが重要です。また、委託業務によって再委託、再々委託が生じる場合には、その再委託先での業務の状況、実態を常に把握しておくことも必要です。

2．4 発送物やFAX の誤送付（誤封入）による事故について

平成19 年度は、発送物の宛名記載ミス、誤封入による発送物等の誤発送、個人情報の入った書類の授受ミス等の事故報告件数が平成18 年度に比べ倍増しました。

再発防止策としては、複数の者によるダブルチェックが有効ですが、当該措置のみならず、事故発生の原因と影響について社内で情報共有することが重要です。また、事故が発生していなくとも、事故が発生した場合に生じる本人への影響及び会社の信用失墜を従業者に十分に認識させる教育と、その教育を受講しなければ業務に従事させない等の社内体制の整備が必要となります。

2．事故等の問題点及び事故等防止のための注意点(3/3)

2．5 盗難（空巣・車上荒らし・置引き）による事故について

平成19 年度は、盗難（空巣・車上荒らし・置引き）による個人情報紛失等の事故が平成18 年度の2.5 倍（4 件から10 件）に増加しました。

車上荒らしや置引き等の盗難による個人情報漏えいの事故は、不可抗力的な側面もあるものの、個人情報を取り扱う担当者の認識の問題によるところも否定できません。

再発防止策としては、個人情報を社外に持ち出すことの必要性の確認、持ち出す場合にはそのリスクを十分に認識した上での対応策をルール化し、従業者にルールの徹底を図る等の教育を継続的に行うことが挙げられます。

2．6 ファイル交換ソフト（Winny など）による事故について

平成16年頃から現在にかけて多くの企業や公的機関において、ファイル交換ソフト（Winny、share等）のウィルス感染による情報漏えいが相次いでいます。当協会でも、数度にわたり、書面等で注意喚起を図っており、事業者側において「自宅も含めたファイル交換ソフトの使用禁止」「従業者の私物パソコンの社内持ち込み禁止」「自宅での持ち帰り作業の禁止」等の措置が徹底された影響もあってか、ファイル交換ソフトに起因した個人情報漏えい等の事故報告件数は平成18年度に比して若干減少しています。

ただし、プライバシーマーク認定事業者の委託先となる事業者や退職者を発生源としたファイル交換ソフトによる情報漏えい事故は依然として発生しており、予断を許さない状況にあります。

再発防止策としては、ファイル交換ソフトの使用禁止だけでなく、個人情報を含む業務情報の社外持ち出しの禁止を徹底することが有効です。また、過去に自宅等で持ち帰り作業をしていた場合でも、業務終了後に使用した業務情報をすべて削除しているかを改めて確認することも重要です。そのため、事業者においては、教育等を通じた従業者への周知徹底や、定期的な自主点検を実施する必要があります。

3．全般的な注意点(1/2)

3．1 内部犯罪･内部不正行為への対策

当協会への事故報告のうち従業者による内部犯罪･内部不正行為は割合として極めて低いですが、過去に内部犯罪･内部不正行為による個人情報の漏えい等で本人等への二次被害、業界の社会的信用失墜が生じた事例がありました。

内部犯罪･内部不正行為への対策としては、過去の「性善説」に基づく管理方針から「性悪説」に基づく管理方針へ転換を図ることが重要なポイントとなります。

具体的な対策としては、以下のものが例として考えられます。

① 業務内容や責任に応じて個人情報へのアクセス権を見直し、アクセスの範囲及び権限者を必要最小限に絞り込むこと。

② アクセス権限者の不正行為の抑制のため、入退室記録や個人情報を取り扱うシステムへのアクセスログ等の取得を行い、定期的に記録の確認を行うこと。

③ 社会人としてのモラル、仕事･役割への責任感、ルール違反によって生じる被害･不利益等について、コミュニケーション機会や教育の中で継続的に啓発を行い、従業者の自覚、個人情報保護の意識の向上を図ること。

3．2 従業者への教育

JISA 個人情報保護ガイドライン第33 条（JIS Q 15001:2006 の3.4.5）では、従業者に個人情報保護マネジメントシステムの運用を確実に実施できる力量を備えさせるための教育について規定しています。従業者に対して一方的に教育を行うだけでなく、テスト等の実施により従業者の理解度を把握し、教育の内容･実施方法について定期的に評価を行った上で必要な見直しを行うこと、また、教育を受けたことを自覚させる仕組みを取り入れることが重要です。

事故報告では、教育自体は実施されているが、従業者が自覚を持って受講していなかった、漫然と受講していたなど、教育内容の不備よりも従業者への浸透不足、従業者の理解度不足が目立ちました。

3．全般的な注意点(2/2)

3．3 運用の確認及び監査

個人情報の取扱いにおける事故等の発生については、個人情報保護マネジメントシステムの内容、運用に問題があることが原因の1つとして考えられます。そのため、監査や運用の確認によって内部にチェック機能が働いていなければなりません。

監査のポイントとしては、① 規格（JISA 個人情報保護ガイドライン及びJIS Q15001:2006）への適合状況、②運用状況が監査項目にて反映されているかが重要となります。

また、監査以外でも、日常の業務において個人情報保護マネジメントシステムが適切に運用されているかを定期的に確認し、必要に応じて注意喚起、改善を行うことも必要です。

3．4 再発防止策の効果の確認

事故報告においては、再発防止策を含めた形で報告を求めていますが、再発防止策については、その実施のほかに効果の確認と検証も必要です。その結果、改善を要する場合には単に現場レベルの対応ではなく、代表者又は個人情報保護管理者等において対応を確認しなければなりません。

事故への対応については、発生した事象に対して単に措置を講じるのでなく、PDCA サイクルの中で取り組む必要があり、生じた事故における原因の究明、対策の立案･実施、対策における効果の確認を行うことが求められます。

以上

『わが社の情報セキュリティ運用術』

報告書から見えてきた事

情報セキュリティマネジメント

情報資産の機密性、完全性、可用性を維持

→『情報資産』　のための規程、しくみ、管理、監査。。。

事故原因

紛失、盗難、誤送信(eMail、郵便)、ウィルス、管理ミス

→　全て『就労者』が対象

★　規程/基準より、運用マニュアル
★　知識教育より、モラル教育
★　管理する事より、自発的活動

わが社の情報セキュリティ運用術

㈱大塚商会

→ 就労者目線に立った運用

オムロン㈱

→ 情報マネジメント統制を施行するため社内運用

㈱ＮＴＴデータ

→ グループ会社での情報を積極的に共有、活用する運用