

プライバシーマークサーベイランスのための  
社内教育テキスト

— 事例から学ぶ —

見本

平成25年4月25日

アイエスオー株式会社

個人情報保護推進委員会

## 目次

	ページ
1. はじめに	2
2. パソコンの盗難、紛失による個人情報漏えい	3
3. USB の盗難、紛失による個人情報漏えい	5
4. 書類の盗難、紛失による個人情報漏えい	7
4. 1 書類の所在不明	7
4. 2 書類の紛失	9
4. 3 廃棄書類の紛失	11
5. データベースの盗難、紛失による個人情報漏えい	13
6. メールの誤送信による個人情報漏えい	15
7. 個人情報保護方針	17
8. 個人情報保護管理体制	18



## 1. はじめに

導入セミナーでは、

- 1) 個人情報保護法
- 2) 当社のプライバシーマークの取り組み
- 3) 個人情報保護マネジメントシステムに適合することの重要性及び利点
- 4) 個人情報保護マネジメントシステムに適合のための役割と責任
- 5) 個人情報保護マネジメントシステムに違反したら
- 6) 個人情報保護のための社内ルール

について学びました。

ステップアップセミナーでは、

- 1) 個人情報保護法
- 2) 情報漏えいの現状
- 3) 情報漏えい事故の実際

について学びました。

今までのセミナーで、個人情報保護法についての重要性と社内対応は、十分に理解して頂いたと思います。



今回のセミナーは、他社の情報漏えい事故を検証し、なぜ、情報漏えいしたのか、どのような対応をすれば良かったのかをみなさんに考えて頂きます。

正解・不正解はありませんので、遠慮なく、色々の意見を考えてみましょう。

参考として、事故発生企業の企業・団体が行った事故分析を掲載しています。また、改善すべき例を挙げています。自社も採用すべきということであれば、例と同じでも結構です。

温故知新ではありませんが、過去の事例を検証し、注意すべき点、考慮すべき点を学び、今後の自部門の活動につなげていって頂ければと思います。

## 2. パソコンの盗難、紛失による個人情報漏えい

山口大学 パソコンの盗難

平成 22 年 1 月 22 日

パソコンの盗難に伴う個人情報の漏えいの可能性について（お詫び）

このたび、本学医学部附属病院の患者さんの個人情報を保存していたパソコンが本学大学院生の自宅において盗難に遭い、当該個人情報が漏えいする可能性があることが判明しました。

御迷惑をおかけした患者さんには心からお詫び申し上げます。

当該大学院生及び指導教員その他全職員に対して個人情報の保護について一層の周知徹底を図り、再発防止に向けて万全を期す所存です。

### 1. 盗難にあった個人情報

- ・患者情報 6名分 (氏名、計測方法)
- ・患者情報 1名分 (氏名、年齢、性別、計測部位)



### 2. 経緯と対応

本学医学系研究科所属の大学院生が昨年末に個人情報を保存したパソコンを自宅へ持ち帰り、盗難に遭ったことが判明しました。当該大学院生は即日所轄署に盗難届を提出しましたが、現時点でパソコンは発見されておりません。

患者さん御本人に対しては、盗難にあった個人情報の内容や経緯について説明し、謝罪を行いました。

なお、今回の個人情報の盗難に係る被害等は確認されておりません。

情報ソース

[http://ds22.cc.yamaguchi-u.ac.jp/~www-yu/cgi-bin/topics\\_event/2009/topic100122.cgi](http://ds22.cc.yamaguchi-u.ac.jp/~www-yu/cgi-bin/topics_event/2009/topic100122.cgi)

1) この事件の問題点を挙げて下さい。

山口病院：

今回の事態に至ったのは、当該大学院生が個人情報を学外に持ち出す際の安全確保の措置を怠ったためです。本法人では、患者さんの個人情報については「個人情報の取扱いに関する方針」、「患者さんの個人情報の取扱いについて」を策定し、個人情報の学外への持ち出しは原則禁止としており、学外へ持ち出す場合は暗号化その他の匿名化に必要な措置又はこれに代わる安全確保の措置を講じるものとしていますが、それがなされていませんでした。このような事故が起きた背景として職員及び学生を指導・監督する体制が不十分であったことは否めません。

2) 自社で、改善すべき点がありますか。

例)

- ・パソコンの持出しを禁止にする規定を作成する。
- ・BIOS パスワードを設定する。
- ・ログオンパスワードを設定する。
- ・データのアクセス権を設定する。
- ・個人情報データは、暗号化する。