セキュリティ基準や契約書から見える
個人情報保護対策およびシステム監査における課題

個人情報保護専門監査人部会 個人情報保護専門調査員
富士通株式会社 桃澤 正和

目次

- 活動内容のご紹介
- 課題
- システム監査と専門監査人の役割
- 今後の活動予定

活動内容のご紹介

活動内容のご紹介

- セキュリティ基準書やモデル契約書などの分析
  - 省庁や団体から発表されている、
    セキュリティ対策の基準書やモデル契約書などから、
    課題となる点を議論

    - JISA「個人情報の取扱いに関するモデル契約書」
    - PCIDSS（ Payment Card Industry Data Security Standard ）
    - 社会保障・税に関わる番号制度　検討資料
    - 経産省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」

    など

課題

課題１：セキュリティ対策の実装
課題２：人的セキュリティ
課題３：監査に対する負荷の問題
課題４：監査品質の保証

課題1：セキュリティ対策の実装

- セキュリティ対策をどこまでやればいいのかわからない

個人情報保護法　第20条

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

- 企業としてはどこまで対策すれば十分なのか判断できない。
- 企業毎に自衛のためにとるセキュリティ対策が異なる。

課題1：セキュリティ対策の実装

- クレジットカード業界
  - PCIDSSで具体的な対策を示している。

例）パスワードの設定方法

・数字と英字の両方を含むパスワードを使用する。
・パスワードの長さは7文字以上にする。
・パスワードは少なくとも90日ごとに変更する。

課題1：セキュリティ対策の実装

- 業界団体毎に、より具体的な対策を示す必要があるのではないか

  - 特に、人間の生命や財産に関する情報について、
    具体的な対策を示し管理レベルを統一する。

  - また、個人情報がどのように管理されているか、
    本人からの情報開示の要求にも一定程度対応し、
    本人が選択できるようにする必要があるのではないか。

課題2：人的セキュリティ

- 内部犯行に対して、どこまで対処すれば効果があるのかわからない

個人情報保護法　経産省ガイドライン

従業者の採用時又は委託契約時における非開示契約の締結

雇用契約又は委託契約等における非開示条項は、
契約終了後も一定期間有効であるようにすることが望ましい。

- 特に高位のアクセス権限を持っている人の管理が重要。
- 抑止効果かを狙うか、人間に一切扱わせないかどちらか。

課題2：人的セキュリティ

- 退職後の秘密保持に関する誓約書の提出を求める

  JISA「個人情報の取扱いに関するモデル契約書」

- 雇用する前にバックグラウンドチェックを実施しているか確認する。

  PCIDSS

課題2：人的セキュリティ

- 確実に刑事罰を科せるよう、法律の見直しが必要ではないか

  - より高い抑止効果が期待できる。
  - また、管理する側においては、個人情報保護法施行前に持ち出した個人情報など、現制度開始前の情報管理についても考慮しなければならない。

課題3：監査に対する負荷の問題

- 委託先の監督責任を果たすためにどこまでやればいいのかわからない

> 個人情報保護法　第22条
>
> 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

- 監督責任を全うするため、各社監査を実施する。
- 監査を実施する側はもちろん、監査を受けた側の負担も大きい。

課題3：監査に対する負荷の問題

- 第三者による認証や監査結果を利用できる仕組みを構築する必要があるのではないか
  - 特に委託する側が、第三者認証やSLAなどを積極的に取り入れる。
  - クラウドサービスが浸透してくると、直接現場を見る等の監査は実施しづらくなる。

課題4：監査品質の保証

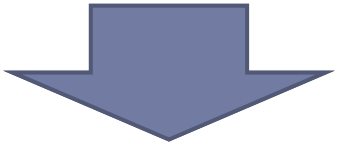
- 有効な監査ができているのかどうかわからない

個人情報保護法には監査に関する定めはない。

- どの企業においても内部監査を実施している。
- 委託先との契約においても監査権を要求している。

課題4：監査品質の保証

- 専門知識を持った専門家に任せる
  - 監査／監査人の役割りとして、本人に対する安心感を与えてあげるということが大切。
  - 企業からすれば、安全性をアピールすることができる



個人情報保護専門監査人に任せて安心

システム監査と専門監査人の役割

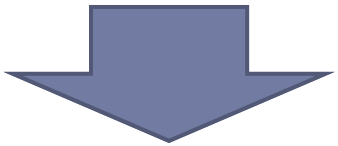
- セキュリティ対策や人的セキュリティなど、対策レベルを決めるのが難しいものに関しては、利害関係者を含めた適切なプロセスにより決定されたものなのかを評価する。

- クラウド技術を代表とする複雑化、高度化していく情報技術・知識を習得し、システム監査に活かす。

今後の活動予定

- 書籍発行に向けて、原稿執筆
- システム管理基準への反映検討

- 個人情報漏洩事故の裁判例分析
  - 裁判例をもとに、下記の点に着目して議論
    - どこに原因があったのか
    - 事前にシステム監査を実施していれば防ぐことができたのか



『東日本大震災と安全・安心
今すぐ使える個人情報保護の極意』（仮称）
～～震災・危機および日常における 個人情報流出の対策～～

年内発表に向けて鋭意執筆中！