早稲田大学生協における個人情報保護監査への取組み

赤塚 尚之 （Naoyuki AKATSUKA）＊
池村 恵一 （Keiichi IKEMURA）†
海老原 崇 （Takashi EBIHARA）‡

1. はじめに —個人情報保護監査実施の背景—

経済主体においては，個人情報保護体制の運営，管理，および業務遂行が内部統制(1)の大きな課題となりつつある．日本でも，2003（平成 15）年 5 月に制定された「個人情報の保護に関する法律」（以下，「個人情報保護法」）により，個人情報保護の枠組みが確立され，監査の分野においても同法に基づく「個人情報保護監査」の必要性が生じることとなった．

早稲田大学生活協同組合は，6 万人超の学生を有する早稲田大学の学生を主な組合員とする全国最大規模の大学生協であり，その保護すべき個人情報は膨大かつ多岐にわたる．

このような状況のもと，早稲田大学生活協同組合監事会は，2004（平成 16）年 6 月に開催された総代会において，通常の監査報告に加えて個人情報保護法に基づく個人情報保護監査の必要性を提案している．そして，平成 17 年度の監事会から，通常の監査に加えて「個人情報の保護に関する法律」第 20 条の規定に基づき，2006（平成 18）年 3 月 28 日現在における早稲田大学生活協同組合本部およびトラベルサービスセンターによる個人情報の保護対策について「個人情報保護に関する監査～主要事項点検表モデル」に依拠して監査を実施した．

本報告においては，早稲田大学生活協同組合における個人情報保護監査実施初年度の取組みを紹介し，今後検討すべき点について取り上げることを目的としている．

2. 早稲田大学生活協同組合本部における個人情報保護監査の実施と監査意見

「個人情報保護に関する監査～主要事項点検表モデル」を参照して監査を実施した結果（点検項目【5】物理的安全管理措置および【6】技術的安全管理措置を除く），早稲田大学生協本部による個人情報の保護対策の実施状況は，適正であると認める．

もっとも，③「個人情報安全管理手順書」に照らして，職員等に対する個人情報保護に関する継続的教育および研修の実施，教育方法等の立案および導入時期について早急かつ具体的に検討される必要があると考える．

3. 早稲田大学生活協同組合トラベルサービスセンターにおける監査の実施と監査意見

「個人情報保護に関する監査～主要事項点検表モデル」における点検項目【5】物理的安全管理措置および【6】技術的安全管理措置を参照して監査を実施した結果，早稲田大学生活協同組合トラベルサービスセンターによる個人情報の保護対策の実施状況は，パスワード管理体制の見直しおよびソーシャルエンジニアリング対策の実施に関する提案事項を除き，④「個人情報安全管理手順書」に照らして適正であると認める．

＊ 早稲田大学商学学術院助手，平成 17 年度早稲田大学生活協同組合代表監事
† 早稲田大学商学学術院助手，平成 17 年度早稲田大学生活協同組合監事
‡ 早稲田大学大学院商学研究科博士後期課程，平成 17 年度早稲田大学生活協同組合監事

4. トラベルセンターへの提案

4.1 パスワード管理体制の見直し

トラベルサービスセンターにおいて管理されているPCには，BIOSレベル，OSレベルで認証設定がなされており，外部委託のサーバで運用されている個人情報データへのアクセスに対してVPNを利用しているが，職員間で単一のアカウントを運用している状況にある．また，個人情報へのアクセスログは記録しているが，単一のアカウントを運用しているために，誰がアクセスしているか特定されないという問題点を指摘せざるを得ない．

そこで，次に掲げる対策を早急に実施するよう提案する．

①個々の職員へのアカウント発行，ないしは利用者を容易に特定できるアカウント運用体制の確立

②職員の異動または退職に伴う不要アカウントの適時削除

③担当者変更時のパスワード変更等のアカウント管理体制の確立

④アカウント付与者に対するID・パスワード管理に関する適切な教育・指導体制の確立

4.2 ソーシャルエンジニアリング対策の実施

トラベルサービスセンターにおいて管理されているPCにはスクリーンセーバが付与されていない．PCは，外部者が容易に立ち入れない店舗奥のスペースに設置されてはいるものの，ソーシャルエンジニアリングを考慮した場合には対策が十分になされているとはいえない．

そこで，管理PCに対するスクリーンセーバ/パスワードロックの付与を早急に実施するよう提案する．

5. おわりに

平成17年度は，個人情報保護監査実施初年度ということもあり，本部とトラベルセンターの2箇所を監査するにとどまったが，翌年度以降からはすべての箇所を網羅的に監査できるような体制を構築していきたい．

また，本部およびトラベルセンターへの監事会からの提案事項に基づき，いかなる改善が実施されているのか，継続的に監査を行えるように監事会における審議事項として個人情報保護監査を毎回取り上げて行きたいと考えている．

注

(1) 内部統制とは，企業組織・事業組織における「経営・管理」（management）と「業務」（operations）遂行ができるように，あらゆる階層に属する人間の行為に対して，事前に，行為を遂行する段階で，そして，事後に働きかける制御機能である．米国では，エンロンやワールド・コムの経営破たんを受け，内部統制の確立を図り，部外者による監査を行い適正な情報開示を実行させ，私的や不正の取引･運営を駆逐することを目的とする企業改革法（SOX法：Sarbanes-Oxley Act）が制定された．米国でのSOX法制定の流れを受け，日本においても内部統制の評価および監査の基準のあり方が検討されている．