アリコジャパンに対する行政処分について

I. アメリカン・ライフ・インシュアランス・カンパニー日本支店(通称アリコジャパン。以下「当社」)における、個人顧客情報の漏えい事案について、保険業法第 200 条第 1 項及び個人情報の保護に関する法律第 32 条の規定に基づき、事実関係及び要因等につき報告徴求命令を発出したところ、以下の状況が認められた。

1. 当社からの報告に基づく事実関係

(1) 平成 21 年 7 月、当社は、クレジットカード会社から、当社の顧客名義のクレジットカードが不正使用されている疑いがあるとの情報提供を受け、内部調査を実施。調査の結果、当社の保有する個人顧客情報(カード番号、有効期限)が漏えいしたことが判明。

(2) その後の調査の結果、当社の業務委託先(以下「本件業務委託先」)の従業員が、平成 20 年 3 月から 5 月までの期間、本件業務委託先オフィスにあるコンピュータ端末から当社のホストコンピュータ(米国)に対して、委託業務遂行のために付与されていたアクセス権限を用いてアクセスし、個人顧客情報(推定約 3.2 万件)を社外に持ち出したものと、当社としては判断。

ただし、未だに、漏えいした個人顧客情報の具体的範囲及び実行者の最終的な特定には至っていない。

(注) 当社に対し、不正使用の疑いがあるとしてクレジットカード会社から照会があった件数は、平成 22 年 2 月 18 日までの累計で 6,592 件。なお、現時点で顧客に金銭的被害は生じていない。

2. 個人顧客情報の漏えいを生じさせた要因

今般の個人顧客情報漏えい事案については、未だ原因究明の途上ではあるが、当社からの報告を検証した結果、現時点において、当社(本件業務委託先を含む)の個人顧客情報の管理態勢について、以下のような問題が認められた。

(1) 本件業務委託先においては、ホストコンピュータへのアクセスに必要な ID 及びパスワードを日常的に担当者間で使い回しする等、個人顧客情報管理が社撰であり、情報漏えいが起こり易い状況にあった。また、ID の使い回しは、一旦、情報漏えいが生じた場合に、実行犯の特定を困難にするという問題にもつながった。

(2) 他方、当社においても、個人顧客情報の管理態勢に以下のような重大な不備が認められた。

① 当社のシステム部門においては、本件業務委託先が個人顧客情報を扱っていることについての認識が不十分であったため、本件業務委託先に対する立入検査においても、個人顧客情報保護の観点から、深度ある確認・検証を行っていなかった。そのため、上記(1)で述べたような、本件業務委託先における杜撰な個人顧客情報管理の実態を把握できず、また、牽制や是正も十分に行っていなかった。

② さらに、当社のシステム管理において、個人顧客情報保護上、以下のような問題が認められた。

i) ホストコンピュータへのアクセス権限の付与範囲について、業務遂行の実態に応じた必要最小限のものになっていないこと。

ii) サーバーや業務委託先のコンピュータ端末の一部において操作履歴が残らないものがあつたため、不正利用に対する牽制効果が不十分であるとともに、万一不正利用があつた場合に原因究明を困難にするという問題があつたこと。

iii) 業務委託先の従業員にホストコンピュータへのアクセス権限を付与する際の本人確認が不十分であり、付与後の管理も不十分であつたこと。

③ 上記①及び②の問題の背景には、個人顧客情報保護に係る担当部門において、業務委託先も含めた全社的な個人顧客情報の漏えいリスクを網羅的に把握・分析し、かつ予防的な施策を検討する態勢ができていなかったこと、更には、当社経営陣において当該リスクの重要性を踏まえた深度ある検証や、必要となる指示等を行っていなかったこと、といった問題があつたと認められる。

(3) 上記(2)のとおり、当社における個人顧客情報の管理態勢には重大な不備があつたと認められ、こうしたことは、個人顧客情報の適正な取扱いを求める保険業法第 199 条で準用する第 100 条の 2、同法施行規則第 160 条で準用する第 53 条の 8、個人情報の保護に関する法律第 20 条及び第 22 条に違反すると認められる。

II. 当社に対する行政処分等について

上記を踏まえ、本日、当社に対し、保険業法第 204 条第 1 項に基づき以下の内容の業務改善命令を発出するとともに、個人情報の保護に関する法律第 34 条第 1 項に基づく勧告を行った。

1. 保険業法第 204 条第 1 項に基づく業務改善命令

- (1) 個人顧客情報の管理態勢を強化し、現在構築中の再発防止策を含め個人顧客情報の安全管理を徹底するための施策を速やかに実行するとともに、その実効性を検証すること。
- (2) 個人顧客情報の安全管理を徹底するための措置が委託先において十分確保されるよう、必要かつ適切な監督を行うこと。
- (3) 引き続きクレジット業界と連携し、顧客保護の取組みを進め、信頼の回復に努めること。
- (4) 引き続き本事案の漏えい原因の究明に努めること。

- (5) クレジットカード情報が漏えいし、多数のクレジットカードの不正使用の試みを生じさせたという事案の重大性を踏まえ、経営陣を含む責任の所在の明確化を図ること。
- (6) 上記(1)～(5)への対応状況について、平成22年3月24日(水)まで(及び必要に応じて随時)に、書面で報告すること。併せて、これらの対応状況について、顧客等への周知を図る観点から、その概要を公表すること。

2. 個人情報の保護に関する法律第34条第1項に基づく勧告

- (1) 個人データの安全管理のための実効性のある措置を確保すること。
- (2) 個人データの取扱いの委託を受けた者に対する必要かつ適切な監督を行うこと。
- (3) 上記(1)・(2)への対応状況を、平成22年3月24日(水)までに、書面で報告すること。

Ⅲ. その他

なお、金融庁としては、今回の個人顧客情報の漏えい事案を踏まえ、「保険会社向けの総合的な監督指針」等を改正し、外部委託先等における個人顧客情報管理の強化や、クレジットカード情報等に対する、その特性を踏まえた情報管理の強化等を監督上の着眼点として追加することを予定。

お問い合わせ先

金融庁 監督局保険課

電話:03-3506-6000(代表)

(内線 3336、3486)