2010 年 2 月 24 日

弊社に対する行政処分等について

アリコジャパン（日本における代表者･社長：髙橋和之）は、本日、金融庁より保険業法第 204 条第 1 項の規定に基づく業務改善命令及び個人情報の保護に関する法律第 34 条第 1 項に基づく勧告を受けました。

お客様の安心を支え、信頼にお応えしていくべき保険会社として、大切なお客様情報の流出という事態が生じましたことを深く反省するとともに、お客様ならびに関係者の皆様に多大なご迷惑、ご心配をおかけいたしましたことを謹んで深くお詫び申し上げます。

弊社では、お客様にご迷惑をおかけしないことを最優先に、本件発生以降、改善に向けた取り組みを行っております。今回の行政処分等を厳粛に受け止め、現在行っている改善の取り組みを継続し、お客様から信頼いただける会社となるために、全社一丸となって万全を尽くしてまいります。なお、行政処分等の内容と弊社の改善に向けた取り組みは下記のとおりです。

記

Ⅰ．業務改善命令の内容

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から５への対応状況について、2010 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。

Ⅱ．個人情報の保護に関する法律に基づく勧告の内容

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．個人データの取り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及び２への対応状況を、2010 年 3 月 24 日（水）までに、書面で報告すること。

III. 行政処分等の理由

業務改善命令について

1 . 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 条の規定に基づく報告徴求命令に基づく弊社からの報告において、以下の事実が認められた。

（１）2009 年 7 月、弊社は、クレジットカード会社から、弊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、弊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、弊社の業務委託先（以下「本件業務委託先」）の従業員が、2008 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弊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、弊社としては判断。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。

２．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、弊社からの報告を検証した結果、現時点において、弊社（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となる 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杜撰であり、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、弊社においても、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 弊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、弊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ったため、不正利用に対する牽制効果が不十分であるとともに、万一不正利用があった場合に原因究明を困難にするという問題があったこと。

(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ったこと。

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、弊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、といった問題があったと認められる。

（3）上記（2）のとおり、弊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ったと認められ、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 に違反すると認められる。

勧告について

弊社の個人顧客情報の漏えい事案に関し、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（以下「法」という。）第 32 条の規定に基づく報告徴求命令に対する弊社からの報告を検証した結果、弊社の個人データの管理態勢について問題があり、法第 20 条に規定する安全管理措置の実施義務及び法第 22 条に規定する委託先の監督義務に違反していると認められたことから、個人の権利利益を保護する必要があるため。

IV. 改善に向けた主な取り組み

弊社では、本件の発生をうけ、個人顧客情報の管理態勢強化と業務委託先における安全管理徹底のために、以下のような取り組みを実施しております。

（1）個人顧客情報の管理態勢強化

2009 年 11 月 1 日付で個人顧客情報管理を含む情報セキュリティに関する事項を専門的に所管する情報セキュリティ委員会を新設し、さらに、情報セキュリティオフィサー、情報セキュリティ推進部を新設いたしました。これにより個人顧客情報管理を含む情報セキュリティ態勢の網羅的な検証、改善策の策定、全社的な推進等を図っております。

（2）本件をうけたアクセス制限の厳格化と ID 管理の強化

アクセス制限の厳格化と ID 管理の強化を実施いたしました。今後、アクセス管理のさらなる強化、システムのアクセス履歴や操作履歴の分析および管理の高度化等を行ってまいります。

（3）業務委託先における個人顧客情報管理

業務委託先選定基準を強化するとともに、業務委託先管理データベースの整備・強化を行いました。弊社立入検査の実効性を確保するため、個人顧客情報を扱う非常駐の業務委託先に義務づけている情報セキュリティ管理基準に基づいた立入検査用チェックシートを使用し、立入検査を実施しております。

（4）社員等の意識向上

個人情報保護を含む新たな情報セキュリティ管理態勢の周知のために、本社全部門長、全社員、業務委託先社員等に対して研修を実施しております。
研修については、今後とも定期的に実施し、引き続き個人顧客情報管理の強化とこれにかかる意識の向上に継続的に努めてまいります。

（5）監査

本件にかかる改善策の網羅性、実施状況および、その実効性については、弊社監査部門による監査を改善策の完了まで継続的に実施し、その結果を経営陣に報告いたします。

V. お客様保護の取り組み

不自然なアクセスがあったファイルに含まれていた約 46 万件のお客様のカード情報につきまして、カード会社各社と緊密に情報連携を行い、不正使用の試みをブロックできるよう、最大限の監視態勢をカード会社に継続いただいております。これにより、お客様には、引き続きご安心いただける態勢が確立されております。

VI. 漏えい原因究明に向けた取り組み

昨年 11 月から本年 1 月にかけて約 2 ヶ月間、中立性のある第三者機関により、本件に関する調査の検証を受け、その結果、中国における業務委託先の社員が情報漏えいの原因であるという弊社による調査結果についての支持を得ております。
なお、中国の関係捜査当局への被害届の提出ならびに不正にデータの抜き取りを行った者の特定に向けて、弊社は、引き続きあらゆる可能性を検討し、適切に対処してまいります。

VII. 今後の予定

弊社は、このたびの行政処分等に基づき、業務改善命令への対応状況については 2010 年 3 月 24 日まで（及び必要に応じて随時）に、また勧告への対応状況については同年 3 月 24 日までに、それぞれ金融庁に報告書を提出するとともに、各報告書を提出後、その概要を公表いたします。

以 上