2010 年 3 月 24 日

業務改善報告書の提出について

アリコジャパン（日本における代表者･社長：髙橋和之）は、個人顧客情報の漏えい事案に関する 2010 年 2 月 24 日付命令書（金監第 398 号)、及び同日付勧告書（金監第 399 号）に基づき、本日、金融庁に業務改善報告書を提出いたしました。

この度の個人顧客情報漏えい事案に関しましては、あらためて、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、既に多くの再発防止策に取り組んでまいりましたが、現在の取り組みに満足することなく、業務改善報告書に明記しました再発防止策を速やかに実行するとともに、業界最高水準の個人顧客情報保護態勢の構築に取り組んでまいります。

また、弊社では、本件発生以降、多大なご迷惑をおかけしましたお客様への対応を最優先事項とし、クレジットカード会社と連携の上、お客様の利益を保護する態勢を整えてまいりましたが、引き続き態勢強化に取り組み、お客様の信頼回復に努めてまいります。

なお、本件にかかる責任の所在を明確にするため、厳正な社内処分を実施いたしました。社内処分を含む業務改善報告書の概要は別紙のとおりです。

以 上

別紙

業務改善報告書（概要）

2010 年 3 月 24 日

アメリカン・ライフ・インシュアランス・カンパニー
日本における代表者･社長：髙橋和之

業務改善報告書（概要）

今般の弊社における個人顧客情報の漏えいは、お客様の安心を支え、お客様の信頼にお応えしていくべき保険会社としての信頼を著しく失墜させたものであり、弊社といたしましては深く反省するとともに、漏えいの対象となられたお客様はもとより、弊社のすべてのお客様や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、改めて深くお詫び申し上げます。

弊社におきましては、本件 2010 年 2 月 24 日付けの金融庁による業務改善命令の対象となりました個人顧客情報の漏えい事案（以下、「本件」または「本件クレジットカード情報漏えい事案」といいます。）の発生を経営上極めて重要な問題と認識し、本件発覚後、外部専門家の協力・助言を得て、システム本部、コンプライアンス本部、監査部等の関連部署の動員可能なすべての資源を投入し、漏えいしたと思われるデータファイル、漏えいに関与した実行犯および漏えい経路の特定のための徹底的な調査を行うとともに、適切なお客様対応を確保するための施策の策定および遂行、これにかかるクレジットカード会社との連携体制の構築等、お客様の利益の保護を最優先とした本件への適切な対応を経営上の最重要課題として取り組んでまいりました。

これまでの調査を踏まえ、本件は、弊社の業務委託先において発生したものと判断しており、この判断については、中立的な第三者による検証も受けておりますが、業務委託先における個人顧客情報の適切な管理を確保することは保険会社における重大な責務であり、弊社は、業務委託先の管理の強化を含む個人顧客情報管理の強化の取組みを継続し、お客様から信頼いただける会社となるために、全社一丸となって取り組んでまいります。また、今後も引き続き、多大なご迷惑をおかけしましたお客様への対応を最優先課題として取り組み、お客様の利益の保護に全社を挙げて取り組んでまいります。

本件業務改善命令にかかる 5 項目の施策および取組みの概要は以下のとおりです。

(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

1. 個人顧客情報管理を含む情報セキュリティ管理にかかる経営管理態勢の強化

1) 情報セキュリティ委員会の新設

2009 年 11 月、個人顧客情報管理を含む情報セキュリティ管理にかかる事項を専門に所管

する情報セキュリティ委員会を新設し、商品・サービス担当専務執行役員をその議長に任命しました。情報セキュリティ委員会においては、個人顧客情報保護にかかる施策を実務運営の観点およびシステム管理上の観点から総合的に検討することにより、経営陣による網羅的かつ深度ある議論を確保する体制としています。

2) 情報セキュリティオフィサーの任命

2009 年 11 月、個人顧客情報管理を含む情報セキュリティ管理にかかる事項を全社一元的に経営レベルで掌握する情報セキュリティオフィサーを設置し、情報セキュリティ委員会議長を務める商品・サービス担当専務執行役員をこれに任命しました。同時に当該専務執行役員を個人データ管理責任者に任命することにより、経営レベルにおける個人顧客情報を含む情報セキュリティ管理に関する責任を一元化しました。

3) 情報セキュリティ推進部の新設

2009 年 11 月、システム上のリスクを含む個人顧客情報管理にかかる事項およびこれらを含む情報セキュリティ管理全般にかかる事項を全社一元的に管理、推進する情報セキュリティ推進部を新設するとともに、同部にシステム分野にかかる深い見識を有する社員を配置し、システム部門に対する管理および牽制機能を強化しました。

4) 情報セキュリティ管理にかかる内部監査機能の強化

外部専門家の知見も活用しつつ、個人顧客情報管理を含む情報セキュリティ管理にかかるシステムリスクに焦点をあてた独自のリスクアセスメントを実施し、個人顧客情報管理を含む情報セキュリティにかかるシステム監査の実効性の強化を図ります。

2. 個人顧客情報管理にかかるシステム上の安全管理措置等の強化

1) システム本部組織体制等の整備

2009 年 3 月、システム本部の組織変更を実施し、従前システム管理部が担当していたシステム運用にかかる業務について、システム開発業務とシステム運用業務を組織上明確に分離することを目的として新設した基盤システム部に移管・集約することにより、システム管理部は中立的な立場からシステムリスクの管理に特化する体制としました。

2) ホストコンピュータ上の個人顧客情報へのアクセス制限の徹底

2009 年 9 月、ホストコンピュータ上の個人顧客情報が存在する本番環境へのアクセス権の付与をシステム運用部門に限定するとともに、システム障害等の緊急事態におけるシステム開発部門による本番環境への例外的なアクセスにかかる厳格な管理措置を設けることにより、個人顧客情報へのアクセスの制限を徹底しました。さらに、システム運用

部門と開発部門のオフィスの物理的な隔離、監視カメラの増設等により、個人顧客情報にアクセスするシステム運用部門における情報セキュリティ管理態勢を更に強化します。

3) ホストコンピュータのユーザーID にかかる管理体制の強化

ユーザーID の付与についてシステム管理部による第三者的検証および承認の取得を義務付けるとともに、業務委託先の社員にユーザーID を付与するに際しては本人確認書類の提出を義務付ける等、ユーザーID の付与にかかる管理態勢を強化しました。また、ユーザーID の月次の棚卸しにかかるルールを整備し、棚卸しの結果についてはシステム管理部による検証を義務付ける等、ユーザーID にかかる継続的な管理態勢を強化しました。

4) 業務委託先における情報セキュリティ環境の検証と適切性の確保

非常駐の業務委託先に対して、委託する業務の種類および業務委託先において取り扱う個人顧客情報の重要度に応じた情報セキュリティ管理態勢の整備を義務付ける「情報セキュリティ管理基準」を制定しました。特にホストコンピュータのユーザーID を付与する業務委託については、業務委託先において PC 操作ログの取得、生体認証等の導入、メールの外部送信規制や外部記憶媒体への書出し制限等、最高位の情報セキュリティ管理態勢を求めており、立入点検等により弊社がこれを確認することとしています。

5) ログの取得および管理の徹底

ホストコンピュータおよびデータベースについてログの取得を徹底するとともに、個々のシステム毎に取得されるこれらのログ情報を集約しシステム横断的な統合的分析を行うことにより、不審なアクセスや処理を自動的に検知し警報を発する監視プログラムを導入しました。当該監視プログラムの活用により、不正なアクセス等に対する継続的な監視体制および牽制機能を強化します。

6) 研修等による個人顧客情報管理の徹底

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徹底のために、本社全部門長、全社員、業務委託先社員等に対する研修を実施しました。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態勢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。

7) 情報セキュリティ関連規程の整備および定期的な見直し

上記の改善策については、その継続的な実施を確保するため、情報セキュリティ関連規程において明文化しています。これらの情報セキュリティ関連規程については定期的な見直しを行い、継続的な実効性の確保および向上を図ります。

8) 内部監査の実施による個人顧客情報管理態勢の実効性の検証

個人顧客情報管理態勢にかかる上記の改善策の網羅性、実施状況およびその実効性を検証するため、2010 年 5 月末を期日として内部監査を実施しています。

(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

1) 業務委託先管理に関する組織等の整備

2009 年 12 月 1 日付で業務委託にかかる全社的な管理を事務リスク管理部に集約するとともに、全社一元的な業務委託先管理の高度化を図るため、全業務委託先および委託業務の特性等の詳細な情報を含むデータベースを新たに構築しました。

2) 業務委託先管理に関する規程等の整備

常駐・非常駐の別、委託する業務の種類や業務委託先において取り扱う個人顧客情報の重要度等、個々の業務委託の特性を反映した適切な委託先管理を実施するため、業務委託先管理に関する関連規程を全面的に改定しました。

3) 業務委託先に対する立入点検の強化

業務委託の実施に際して事前に、および業務委託継続中に定期的に実施する業務委託先に対する立入点検において、業務委託先の情報セキュリティ管理態勢の点検に使用するチェックリストを全面的に改訂し、個人顧客情報を取扱うすべての業務委託先に対してシステム分野の専門家の同行による業務委託先の情報セキュリティ管理態勢にかかる一斉立入点検を実施しています。

4) 業務委託先にかかる直接の監査の実施

主要な業務委託先については弊社監査部門による直接の立入監査を実施することにより業務委託管理態勢の実効性を継続的に検証することをルール化し、2010 年度より実施することとしています。

5) 研修等による業務委託先管理の徹底

新たな業務委託先管理態勢の周知徹底のために、本社全部門長に対して研修を実施しました。研修については今後とも定期的に実施し、引き続き業務委託先管理態勢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。

6) 内部監査の実施による業務委託管理態勢の実効性の検証

業務委託管理態勢にかかる上記の改善策の網羅性、実施状況およびその実効性を検証す

るため、2010 年 5 月末を期日として内部監査を実施しています。

(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

1) 専門コールセンターの設置

本件クレジットカード情報漏えい事案にかかる公表を行った 2009 年 7 月 23 日より、弊社において本件クレジットカード情報漏えい事案に関するお客様からのお問い合わせに対応する専門のコールセンターを設置し、通常のコールセンターとあわせて最大約 600 名のオペレーターがお客様からのご照会に迅速かつ適切に対応する体制を構築しています。

2) お客様への個別のご連絡

本件クレジットカード情報漏えい事案にかかる調査の進展に伴い、クレジットカード情報が漏えいしたまたはその可能性のあるお客様に個別のご案内状をお送りし、本件にかかる事実関係のご説明とお詫びを行うとともに、クレジットカードご利用明細書等への注意をお願いしています。

3) お客様への「お詫びのしるし」の送付

本件クレジットカード情報漏えい事案においてクレジットカード情報が漏えいしたものと特定された約 32,000 名のお客様に対して、お客様の精神的なご負担やクレジットカード切り替えに伴うご負担、弊社の社会的責任等を考慮し、「お詫びのしるし」として 1 万円相当のギフト券を送付いたしました。

4) 弊社ホームページにおける継続的なご案内

弊社のホームページにおいて、お客様にクレジットカードご利用明細書等への注意をお願いする案内を継続的に掲載するとともに、お客様からのご照会の多い事項にかかるご説明や本件にかかる調査の進捗状況についてご案内しています。

5) 不正使用の防止に向けたクレジットカード会社との連携

弊社より各クレジットカード会社に対して本件により漏えいした可能性の否定できないクレジット番号等のデータを連絡し、これらのクレジットカード番号にかかる不正検知の監視水準を引上げていただいています。

6) クレジットカードの再発行にかかるクレジットカード会社との連携

クレジットカード会社各社との合意に基づき、本件クレジットカード情報漏えい事案に起因するクレジットカードの再発行については、再発行手数料を無料とする取扱として

います。

7) お客様対応におけるクレジットカード会社との連携

各クレジットカード会社と緊密な連携を図り、お客様対応において疎漏が発生しないよう万全の対応を図るとともに、個別のお問い合わせ事項の迅速な連絡の確保等、お客様の利益の保護を最優先とした対応を行っています。

(4) 引き続き本事案の漏えい原因の究明に努めること

1) 弊社による調査結果

本件クレジットカード情報漏えい事案における個人顧客情報漏えい行為は、弊社のホストコンピュータ関連開発業務を委託していた業務委託先中国企業の社員が、中国にある同社オフィスのコンピュータ端末から弊社のホストコンピュータにアクセスし、個人顧客情報（クレジットカード番号および有効期限）を社外に持ち出したものと判断しています。

2) 弊社調査結果にかかる中立的な第三者による検証結果

上記の弊社による調査の結果および判断については、中立的な第三者である KPMG LLP による検証を受けており、KPMG LLP も上記の弊社による調査の結果および判断を支持しています。

3) 調査の状況

当該業務委託先においてユーザーID およびパスワードの共有が行われていたこと、不正に抜き取られた実際のデータや印刷された紙なども未だ発見されていないことから、本件クレジットカード情報漏えい事案にかかる実行犯の特定および実際に漏えいしたデータの特定には至っていません。

4) 漏えい原因の究明にかかる今後の対応方針

実行犯の特定に向けて中国警察当局による捜査をお願いすべく、中国警察当局に対して当該業務委託先との協力のもと被害届を提出し、2010 年 3 月 24 日付けで受理されました。今後とも当該業務委託先と連携しつつ、中国警察当局による捜査に全面的に協力してまいります。

(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

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本件の重大性を踏まえ、現日本における代表者・社長については、月例報酬の 30%を 4 ヶ月間返上いたします。個人情報保護法が施行された当時の日本における代表者を含むその他の関係役員 5 名については、月例報酬の 20%～30%を 1～3 ヶ月間返上いたします。また、関係部門の責任者等、職員 4 名に対するけん責処分を実施いたしました。

以 上