

個人情報流出に関する再発防止策について

アフラック生命保険株式会社（代表取締役社長：古出 眞敏）は、今年1月10日に公表した「個人情報流出に関するお詫びとお知らせ」に関して、以下のとおり再発防止策を策定し、速やかに実施しておりますので、その概要をお知らせいたします。

当社は、今回の事態を重く受け止め、委託先の管理強化を含む再発防止に努めるとともに、不正アクセスなどの犯罪行為には厳正に対処してまいります。

あらためまして、お客様及び関係者の皆様には、多大なるご迷惑とご心配をおかけしましたことを深くお詫び申し上げます。

1. 発生事象

今年1月6日、当社の業務委託先である外部業者が利用するサーバに対して第三者による不正アクセスがあり、9日に当社から当該事業者へ提供した個人情報の一部が情報漏えいサイトに掲載されていることを確認しました。

1月10日、当社が提供した個人情報について、当該事業者によりサーバから削除しました。また、13日にはセキュリティ専門業者を通して情報漏えいサイト上の当該データも消去しました。

なお、情報漏えいサイトに対する監視を継続しており、再び掲載を確認した場合には、速やかにセキュリティ専門業者と協力して適切に対応する体制を整えています。

2. 外部流出した個人情報

（1）個人情報の項目

- ① 姓のみ（漢字、カナ）・年齢・性別
- ② 証券番号
- ③ 保険種類番号・保障額・保険料

（2）対象となるお客様と件数

「新がん保険」「スーパーがん保険」「スーパーがん保険Vタイプ」のご契約者のうち1,323,468人（データ件数延べ3,158,199件）。

なお、上記の通り情報漏えいサイトに流出した個人情報の項目は限定されており、第三者に悪用される可能性は極めて低いと考えています。また、現時点まで具体的な被害も確認されていません。

3. 発生原因と再発防止策

今回、本件について第三者機関による調査結果も踏まえ、当社で検証を行った結果、業務委託先が当社のセキュリティ管理のルールに基づいた情報管理を行っていなかったことが、不正アクセスによる流出の要因であることが明らかとなりました。

これにより、業務の委託先・再委託先を管理監督する立場にある当社の責任として、「委託元部署による管理監督の基本原則に沿った委託先・再委託先の適切な管理」、「委託先・再委託先に対する情報セキュリティ管理態勢の有効性の検証」、「委託先による再委託先の適切な管理監督を確認するための点検」について、さらなる強化が必要であると認識しました。

当社は、「コーポレートガバナンス基本方針」のもと、内部統制の分野で内外の専門機関が推奨しているフレームワークなどを参考に、事業部門、管理部門、内部監査部門の機能を3つのラインとして整理し、第一ライン（事業部門）による自律的管理、第二ライン（管理部門）による牽制、第三ライン（内部監査部門）による検証、という強固な内部統制を確保する態勢の維持・強化を図っていますが、本件を踏まえて、再発防止策として委託先・再委託先の情報セキュリティ管理態勢をさらに強化すべく、第一ライン（事業部門）及び第二ライン（管理部門）において以下の措置を講じ、速やかに実施しています。

(1) セキュリティインシデント発生時の影響を低減させるための措置

インシデント発生時の影響を低減させるために、委託先での個人情報の取り扱いを最小限・最小期間とすることを徹底します。具体的には、以下を実施しています。

- ① 業務の委託に伴って当社外で個人情報が保管される場合、業務に必要な最小限のデータを提供することを徹底しました。
- ② 委託元部署による委託先の情報セキュリティ管理態勢の監督を徹底します（データ保持期間の明確化、保持場所の把握及び保持期間が終了したデータの消去確認）。
- ③ 当社における情報管理の第二ライン（管理部門）において、委託元部署が委託先を適切に監督しているかどうかを定期的に確認します。

(2) セキュリティインシデントの発生源を減らす措置

インシデントの発生源を減少させるために、当社管理外のシステム上で、個人情報を取り扱う委託先・再委託先数を制限します。具体的には、以下を実施しています。

- ① 個人情報の委託先及び再委託先の安全管理基準を厳格化し、厳格化された基準に満たない委託先及び再委託先との契約を不可としました。
- ② 見直された安全管理基準に満たない既存の委託先及び再委託先については、基準を満たす委託先及び再委託先に変更します。

(3) 委託先・再委託先における情報セキュリティ管理態勢の確認の強化

インシデント発生の確率を低減させるために、当社の委託先・再委託先における情報セキュリティ管理態勢の有効性を検証する手法の実効性を一層高めるように強化します。具体的には、以下を実施しています。

- ① 委託開始前の情報セキュリティ管理態勢評価において、委託する個人情報のデータ管理（データへのアクセス権限、データ保管場所、データ保管期限など）に関する確認項目を詳細化しました。証跡確認と合わせて検証することで、委託先・再委託先における情報セキュリティ管理態勢の有効性を確認します。また、委託開始前だけでなく、委託中の定期点検時点においても同様に実施し、情報セキュリティ管理態勢の有効性を確認します。
- ② 情報セキュリティ管理態勢の変更（含むシステム変更）に関する要件を詳細化しました。これにより、委託先・再委託先における情報セキュリティ管理態勢の変更を把握するとともに再評価を実施し、変更による当社への影響を確認します。
- ③ 委託先・再委託先における情報セキュリティ管理態勢の委託開始前の評価及び委託中の定期点検において、委託先による再委託先の管理監督状況を確認し評価します。
- ④ 情報セキュリティの重要事項を明示的に契約条項に追加しました。
 - ・ 不要となったデータの削除など、データのライフサイクルに応じたデータ取り扱いの厳格な管理に係る事項
 - ・ 情報セキュリティ管理態勢に影響が及ぶ変更に関する事前連絡と変更実施後の結果報告
 - ・ インシデント発生時の対応態勢に係る事項

4. 当社の再発防止策の有効性及び実施状況の評価

本事案の再発防止策が有効に機能しているかを確認・検証することを目的として、今年7月以降、第二ライン（管理部門）及び第三ライン（内部監査部門）による再発防止策の実施状況の評価を行います。また、評価結果に応じて、追加での再発防止策の実施を含めた必要な対応を行っていきます。

以上

<本件に関するお問い合わせ>

コールセンター：0120-332-856

受付時間：月～金 9:00～18:00

土曜日 9:00～17:00

（祝日・年末年始を除く）