平成29年12月22日

各　位

常　磐　興　産　株　式　会　社
代表取締役社長　井上 直美

不正アクセスによる個人情報流出に関する最終ご報告

平成 29 年 7 月 12 日「不正アクセスによる個人情報流出に関するお詫びと報告」でご報告いたしました弊社の公式ショッピングサイト「ハワイアンズモール（https://www.hawaiians-mall.com/index.html)」の運営委託をしている株式会社システムフォワード（以下、「システムフォワード社」といいます）の提供するシステムが、外部からの不正アクセスを受け、一部のクレジットカード情報等が流出いたしましたこと（以下、「本件」といいます）により、お客様をはじめとする皆様に多大なるご迷惑をお掛けいたしましたことを心よりお詫び申し上げます。

弊社では、情報流出の可能性が判明した直後に公式ショッピングサイト「ハワイアンズモール」のクレジット決済の利用を停止したうえで、クレジットカード会社指定の調査会社へ調査を依頼しました。さらに、いわき中央警察署に報告・相談し、原因究明及び被害への対応、再発防止策の検討を進めてきました。

本件の最終的な認定事実の概要と弊社の対応、再発防止対策につきまして、下記の通りご報告いたします。

記

1. 事案の概要

（1）流出したお客様情報

平成 29 年 7 月 12 日にご報告させていただきました通り、情報流出の可能性が判明した後、弊社は直ちに外部調査会社「Payment Card Forensics 株式会社」（以下、「PCF 社」といいます）に調査を依頼し、平成 29 年 6 月 30 日に同社から以下の調査結果の報告を受けました。

ア　対象

平成 29 年 2 月 10 日～平成 29 年 5 月 25 日の間に公式ショッピングサイト「ハワイアンズモール」（物販・ｅチケット・施設内リストバンド決済の申込み）において、クレジットカード決済が行われたお客様情報

イ　項目

カード会員名、カード番号、住所、カード有効期限、セキュリティコード（なお、パスワードは含まれておりません。）

ウ　件数

6,860 件

エ 原因

公式ショッピングサイト「ハワイアンズモール」（以下、「ハワイアンズモール」といいます）

のロードバランサー（負荷分散装置）に使用していた OpenSSL の脆弱性を利用した、外部からの不正アクセスによるものでした。

（2）本件の原因

弊社によるシステムフォワード社に対するヒアリング調査により、以下の事実が本件の原因であることが判明しました。

① 本件サービス開始時において、当時としては安定稼動していた OpenSSL の旧バージョンを使用したこと、そのため脆弱性問題が該当しないと誤信し、旧バージョンのまま放置したこと。

② その後ロードバランサーの OS のバージョンアップと同時に OpenSSL のバージョンアップを実施したが、その際、脆弱性の対策がなされた最新バージョンがあることを確認せず、脆弱性の含まれた旧バージョンのままであったこと。

③ 前記①、②に対応する手順を定めた規範がなく、セキュリティ情報を逐次更新する体制も存在しなかったこと。

④ ペネトレーションテストや脆弱性診断をした事実がなく、そうしたルールも存在しなかったこと。

こうした事実関係から、本件の原因は同社の過失によるものであるとともに、そうした過失を未然に防止し、点検・監督する体制もなく、継続的にセキュリティ情報を確認し安全性を高めるという体制が不十分であったことが、より本質的な原因であると考えています。

（3）弊社と運営委託先との関係

本件は、ハワイアンズモールで利用するクレジットカード情報の取扱いをシステムフォワード社に委託していた案件であり、システムの脆弱性を放置した同社に主要な原因があるものの、弊社において適切な委託先管理を実施してこなかったことが、その脆弱性放置という状況につながった点において、本件の一因を作り出していたことも明らかです。

弊社は、地元企業であるシステムフォワード社との相互信頼は揺るぎのないものと認識しており、同社が弊社のために最善を尽くしているものと過信しておりました。

このような状況から、弊社はシステムフォワード社に対し特段の注意を払うことなく、セキュリティチェックを初めとするセキュリティ対策をおろそかにしていた事実がありました。

2. 流出への対応の経緯

（1）平成 29 年 5 月 25 日、クレジットカード決済代行会社（以下、「決済代行会社」といいます）より、クレジットカード情報流出の可能性があるとの指摘を受け、ハワイアンズモールのクレジットカード決済の利用を停止いたしました。また、不正アクセスの全容解明及び被害状況の把握に向け、社内調査を進めるとともに、PCF 社に依頼し、調査を実施しました。

（2）平成 29 年 6 月 30 日、PCF 社から最終調査結果報告書を受領しました。同社の報告により、不正アクセスによりクレジットカード情報等が流出したことが判明しました。

（3）（2）の報告を受けて、弊社では直ちに以下の通り対応を行いました。

① ハワイアンズモールでのクレジットカードの利用停止

② 不正アクセスの監視強化

③ クレジットカード会社に対する不正利用モニタリングの実施要請

④ 関係官庁（個人情報保護委員会他）への報告

⑤ 警察への報告及び相談

3. 再発防止に向けた対策

弊社は、本件判明直後から、事業の再開復帰に向けた対応を行うとともに、再発防止対策を立案し実施してまいりました。

再発防止対策は、（１）委託先のシステム変更及び監督・管理の徹底強化（２）弊社自身のセキュリティ対応の強化からなります。

まず、本件の直接的原因が、システムの決済接続方式にあり、クレジットカード決済情報が委託先であるシステムフォワード社のサーバーを経由する方式であったため、弊社では、当該情報が利用者から直接決済代行会社に接続する方式へと変更いたしました。それとともに、委託先事業者のセキュリティ対応の点においてもその一因があったことから、委託先監督、委託先のセキュリティ対応の徹底を図るものとしました。

次に、本件を踏まえて、弊社全体の管理体制を見直し、さらに強化する対応を、再発防止対策の重要な柱として強化することといたしました。

（１）委託先のシステム変更及び監督・管理に向けた取り組み

ハワイアンズモールのシステム変更と運営委託先に対する委託先監督が重要な再発防止対策と位置づけました。

ア　決済接続方式の変更

これまで、ハワイアンズモールでのクレジットカード決済処理は、システムフォワード社のシステムで入力を受け、同社サーバーに格納し、当該情報を同社から決済代行会社に送信する方式（API 型）であったため、今回同社システムが脆弱性を有していたことにより、同社サーバーに格納されていた情報が流失したものです。

このため、弊社では、クレジット決済情報を直接決済代行会社のサイトで入力する方式（リンク型）へ変更いたしました。この変更により、ハワイアンズモールでのクレジットカード利用の際には、クレジットカード決済情報が利用者から直接決済代行会社に提供されるようになりました。

弊社としては、ハワイアンズモールからのクレジットカード決済情報が流出する可能性は消失したと考えておりますが、今後も同システム、リンク方式が安全に運用されていることを随時確認してまいります。

イ　事前監査

委託先であるシステムフォワード社が提供するシステムが平成 29 年 8 月 22 日の時点で PCIDSS 準拠の AVDS 診断に合格したことを確認しました。同社は四半期に一度、脆弱性診断を実施する予定であり、弊社に対して診断結果の報告を行う予定です。

また、システムフォワード社との委託契約の内容を見直し、委託先監督をより強化します。

ウ　委託先業務監督

①　セキュリティ監査

弊社は、システムフォワード社が、以下の安全管理措置を実施していることを監査するものとします。

すでに PCIDSS 準拠の AVDS 診断に合格しているとの報告を前提に、PCIDSS の要件を含め、さらに委託先監督に必要な点検・監査を実施します。

ｉ　組織体制の確立

システムフォワード社における業務遂行体制、システム管理体制、セキュリティ管理などの体制整備を点検・監督します。特に、セキュリティ確保に関する規範、職務分担、作業担当者の明確化、作業手順が確立されているかを点検・監督します。

ii　人的対策

システムフォワード社において、受託業務遂行に関し、十分な知識と情報を確保し、適正な運用が図られるよう社内教育が実施されていることを点検・監督します。

iii　技術的対策

システムフォワード社において、セキュリティ技術対策、ウイルス対策、パスワード対策、ファイアウォールの管理が、常に最新の情報に基づき、日々更新されていることを点検・監督します。

iv　物理的対策（施設の安全管理）

システムフォワード社におけるシステム管理に関し、システム管理場所の安全性が確保されていること、入退室管理が実施されていること、機器端末の持ち出しなどが厳重に管理されていることを点検・監督します。

②　セキュリティ報告の徴収

弊社は、システムフォワード社に対して毎月セキュリティ報告を求め、さらに必要に応じて追加での報告を求め、受託業務遂行のための監督を実施するものとします。

③　立ち入り検査等

弊社は、必要に応じて、システムフォワード社の運用する弊社システムに対して、立ち入り検査を実施します。

（2）弊社のセキュリティ体制の強化

弊社のセキュリティ体制を一新するため、「公式ショッピングサイト『ハワイアンズモール』情報セキュリティポリシー」を作成し、以下の通り、弊社のセキュリティ体制・監査体制を強化することとしました。

ア　弊社における安全管理措置の実施

①　業務企画室がハワイアンズモールの運営委託における委託先監督部門となり、その委託先監督責任者として業務企画室室長を選任し、委託先監督の総責任者と定めます。

②　委託先監督責任者は、毎月委託先からセキュリティ報告を求めるとともに、業務の遂行状況、セキュリティ対策の状況、トラブル・インシデント・アクシデントの有無等について定期的に情報交換を実施します。

③　委託先監督責任者は、外部のセキュリティ専門事業者によるセキュリティ監査を受ける等、監査の実効性を確保するための指導を受け、これを実施するものとします。

イ　インシデント（事故を含む）対応

①　エスカレーション対応

委託先事業者及び弊社担当部門が、何らかのセキュリティ上の異変を察知し、また外部から何らかの攻撃を受けたことが判明した場合には、直ちに事象を整理、調査した上で、委託先監督責任者に連絡するものとし、弊社はその手順を予め確認することとします。

②　事故対策委員会の開催

委託先監督責任者は、①の連絡を受けた場合、あるいは外部からセキュリティに関する何らかの情報を受けた場合には、速やかに事故対策委員会を開催し、事案分析、緊急対応、再発防止対策を立案しなければならないものとします。

③　緊急対応

委託先監督責任者は、委託先の管理責任者と連携し、事故対策委員会の判断に従い、緊急対策を実施しなければならないものとします。

④　報告の実施

委託先監督責任者は、事故対策委員会の開催後、事案の解決のための方向が定まったとき、及び事案解決に至ったときに、それまでの対応等を整理し、レジャーリゾート事業本部長に報告するものとします。

以上の再発防止策を実施すべく「公式ショッピングサイト『ハワイアンズモール』委託先監督ポリシー」を定め、委託先監督責任者を中心に再発防止に取り組んでまいります。

4. 業績への影響について

本件が当社連結業績に与える影響は軽微と考えております。

5. 公式ショッピングサイト「ハワイアンズモール」営業再開について

弊社は、前述の再発防止策の実施と並行し、公式ショッピングサイト「ハワイアンズモール」の営業再開に向けた作業に着手してまいりました。

すでに新システムが完成し、PCIDSS 準拠の監査、クレジットカード会社の審査等も終了しており、本最終報告を経て、平成 29 年 12 月 23 日より営業を再開いたします。

6. 問い合わせ窓口について

本件に関するお問い合わせにつきましては、本最終報告を経て、平成 30 年 1 月 2 日より、下記の通り、受付時間を変更して受付させていただきます。

■本件に関するお問い合せ専用窓口＜お客様特別相談窓口＞

■専用フリーダイヤル　：　0120-034-294

受付時間

平成 29 年 12 月 29 日（金）迄：　9：30～18：30　（土日祝日除く）

平成 30 年 1 月 2 日（火）より：　10：00～17：00　（土日祝日除く）

以　上