平成 28 年 9 月 16 日

各 位

会社名　　株式会社ロジネットジャパン
代表者名　代表取締役社長　木村　輝美
（コード番号 9027　札証）
問合せ先
取締役経営企画・広報担当部長　斉藤　恭祐
（TEL 011-251-7755）

連結子会社における個人情報漏洩に関する改善・再発防止策について

平成 28 年 6 月 16 日及び 6 月 24 日に開示致しました、当社の連結子会社である札幌通運(株)の旅行代理店業「クラブゲッツ」のウェブサイトへのサイバー攻撃で、お客様の個人情報漏洩事案が発生しました件につきまして、平成 28 年 8 月 31 日付けで改善・再発防止策を含む最終報告書を観光庁に提出いたしました。また本日 9 月 16 日に、同庁主催の旅行業界情報流出事案検討会において、下記のとおり調査結果を報告いたしましたので、お知らせいたします。なお、セキュリティ上の関係から詳細内容の公表は控えさせていただきます。

本件に関しまして、お客様並びに関係者の皆様に多大なるご迷惑およびご心配をおかけいたしましたこと、誠に申し訳なく深くお詫び申し上げますとともに、改善・再発防止策を確実に実行し、個人情報取扱い事業者として皆様の信頼回復に努めて参ります。

記

１．事案の概要

本年 3 月 4 日に、クレジットカード会社から情報流出の懸念について連絡があったことを受けてクレジットカード決済機能を停止し、社内調査を開始するとともに、第三者調査機関である Payment Card Forensics 株式会社へ調査を依頼し、4 月 22 日より調査を開始いたしました。

5 月 30 日に同調査機関より最終報告書を受領のうえ、調査報告内容に基づきカード会社等と対応を協議し、関係諸官庁へ事象を報告すると共に、6 月 16 日に本事案について開示いたしました。

また、同日付けで所轄官庁であります観光庁より、個人情報保護法に基づく報告の指示を受け、6 月 24 日、当該指示に基づいて同庁に対して報告書を提出いたしました。

その後も引き続き情報流出原因について調査を行うと共に再発防止策を講じ、8

月 31 日付で改善・再発防止策を含む最終報告書を観光庁に提出いたしました。また報告内容について本日 9 月 16 日に同庁主催の旅行業界情報流出事案検討会に、下記のとおり報告いたしました。

２．クレジットカード情報漏洩原因について

・5 月 30 日に受領した調査機関の調査結果より、当社の旅行代理店業のウェブサイトに対し、SQL インジェクション攻撃（※1）という不正アクセスの形跡が見つかりました。
・この攻撃により、お客様がウェブサイトの決済画面に打ち込んだ個人情報が外部に漏洩していたものと判断し、本件事案について 6 月 16 日に公表いたしました。
（※1）SQL インジェクション攻撃：ウェブサイトの入力画面に対し命令文を入力することで、システムに不正アクセスを行い、情報窃取、データベースの破壊・改ざんなどを行うこと。
・その後も調査を継続して参りましたが、システム機能上、調査に必要なデータログが残っていないことから、クレジットカード情報を窃取した直接的な証拠が判明せず、原因を究明することができませんでした。

３．改善・再発防止策の方針について

・原因を究明することができなかったため新たな対処方針として、クラブゲッツのシステムで取り扱う重要情報の流出リスクを洗い出し、対策を講じることといたしました。
・本システムで扱う重要情報は、主にクレジットカード情報と顧客情報（個人情報）であることから、下記の方針に基づいて対策を講じました。
① クレジットカード情報をクラブゲッツのシステムで一切扱わないように変更し、リスクを回避する。
② システムの現状を追加調査し、個人情報を守るための安全対策を講じる。
・情報セキュリティ専門会社であるセコムトラストシステムズ(株)、並びに(株)LAC に、情報セキュリティ診断と情報セキュリティ評価を依頼し、これらの調査、診断結果及びアドバイスに基づき、再発防止に向けた改善策を実施して参りました。

４．本件個人情報漏洩事案発生及びセキュリティ診断・評価により認識した情報セキュリティ上の課題点

・診断の過程において、「クラブゲッツ」ウェブサイトのサーバやアプリケーションに、本件個人情報漏洩事案の原因ではないものの、脆弱性が発見されました。
・当社内部に情報セキュリティに関する規程はありましたが、個人情報の取扱いに係る手順書の整備や教育が不十分であり、またインシデント（問題）発生時の手順も整備

されておらず、個人情報取り扱い全般に関して運用不備がある状態でした。

・「クラブゲッツ」のウェブサイトは、外部委託先管理（ホスティング）の環境下にありますが、当社では、委託開始時以外に当該外部委託先のセキュリティ状況をチェックしておらず、また、当該外部委託先との契約においてはセキュリティ運用に関する役割分担が明確になっていないため、責任当事者が曖昧な状態でした。

５．改善・再発防止策の概要

本件事案発生から、本日（平成 28 年 9 月 16 日現在）までに実施、または完了した改善・再発防止策の概要は、次のとおりです。

項目		実施事項（9 月 16 日現在）
システムのセキュリティ向上	① 脆弱性対応	・クラブゲッツのシステムの主要構成要素をすべて点検し、緊急度の高い課題への対策を行った。
	② 診断の実施	・今後、定期的に実施
	③ クラウド WAF(※1)の導入	・導入完了、設定調整中
内部体制・制度の整備	④ セキュリティ体制の整備	・担当部門を設置 ・CISO（最高情報セキュリティ責任者）を任命し、インシデント発生時の経営判断を迅速化
	⑤ 外部委託先の管理	・外部委託先管理のルールを整備（管理項目を策定済み、契約、定期的監査について規定） ・現委託先への要望提出
	⑥ PDCA 構築	・セキュリティに関する PDCA のサイクルを構築・運用
クレジットカード決済再開に向けた対応	⑦ PCI DSS 準拠の仕組に移行	・決済入力時に決済代行会社のシステム上にある決済画面に遷移する仕組を構築、移行準備済み

※1 クラウド WAF（Web Application Firewall）：一般的なファイアウォールとは異なり、Web サイト上のアプリケーションに対する SQL インジェクション、クロスサイトスクリプティング、OS コマンドインジェクション、パスワードリスト攻撃などの攻撃を防ぐ仕組み

６.「クラブゲッツ」でのクレジットカード決済再開について

今後、「クラブゲッツ」の決済入力時に決済代行会社が運営するシステムの決済画面に遷移（リンク）する仕組を構築し、「クラブゲッツ」のシステム上でクレジットカード情報を処理、伝送、保管することのない仕組みと致しました。

なお、決済代行会社のシステムは、クレジットカード情報を安全に取扱うための基準であるPCI DSSに準拠し、毎年外部機関による準拠性監査を行っております。

既に当該改善につきましては、システム改修を完了しており、Webサイトでのクレジットカードの取扱いを再開する予定ですが、具体的な再開日時につきましては、「クラブゲッツ」のwebサイト(https://www.clubgets.com/)にて別途ご案内させていただきます。

以上