平成 28 年 6 月 24 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　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観光庁への報告について

先日6月16日に開示致しました、当社の連結子会社であります札幌通運株式会社にて事業運営を行っております旅行代理店業「クラブゲッツ」において、不正アクセスにより個人情報が漏えいしておりました件につきまして、同6月16日付けで所轄官庁であります国土交通省観光庁より、個人情報保護法に基づく報告の指示を受けておりましたが、本日、報告指示に基づき同庁に対して報告書を提出いたしましたのでご報告します。

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しておりますこと、誠に申し訳なく深くお詫び申し上げますと共に、係る対応と改善策につきましては誠意をもって対応し、皆様の信頼回復に努めてまいります。

記

観光庁に提出した報告の概要

（1） 本件に関する詳細な事実関係

本件漏洩の内容

第三者の調査機関の調査結果より、当社の旅行代理店業のホームページに対し、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あったとされております。

これにより、システムのプログラムの一部が書き換えられるなどの何らかの要因によって、2015 年 10 月 1 日から 2016 年 3 月 4 日までの期間にお客様がホームページの決裁画面に打ち込んだ 2,519 件の個人情報（氏名、住所、電話番号、メールアドレス、クレジットカード情報（番号、有効期限）が外部に漏えいしていたものと判断致しました。

（※1） SQL インジェクション攻撃：インターネットのウェブサイト等の入力画面に対しプログラミング言語（SQL）による任意の文字列を入力することで、システムに不正アクセスを行い、情報入手、データベースの破壊、ウェブページの改ざんなどを行うこと。

（2） 本件発覚前に講じてきた安全管理措置

「クラブゲッツ」のウェブサイトにおいては、ファイアウォールや DMZ 環境を（※2）設けるなどしており、セキュリティは確保できていると認識しておりました。しかしその堅牢性については、第三者による評価を受けておりませんでした。（別紙「ネットワーク構成図」参照）

（※2）DMZ 環境:インターネットに接続されたネットワークにおいて、ファイアウォールによって外部ネットワーク（インターネット）からも内部ネットワーク（組織内のネットワーク）からも隔離された区域のこと。

（3） 本件に関する問題点

・情報漏えい懸念を確認してから、報告・公表が遅かったこと。
・当社内において、本件発覚後カード情報漏えいの拡散防止を主に対応してまいりましたが、カード情報の以外の個人情報の漏えいの懸念があったことから、個人情報取扱事業者として対応に不備があったこと。

（4） 現在の状況

・本年 2 月にファイアウォールの冗長化を実施しております。
・第三者の調査機関による調査では、今回の情報漏えいの直接要因とされている、SQL インジェクション攻撃（前記※1）に対しては、本年 5 月 23 日現在で脆弱性はないとされております。
・本年 3 月 4 日にホームページ上でのクレジットカード決済を停止しており、以降のカード情報に関しての漏洩はございません。

（5） 今後の再発防止策等

情報セキュリティ専門会社による診断、コンサルティング等の実施

今回の情報漏えいの原因の詳細分析及び本件以外にも個人情報流出懸念がないかどうかの調査（セキュリティ診断）、並びにハード面のみならず組織体制、人的側面も含めた全般的な情報セキュリティ評価（情報セキュリティ監査）と今改善コンサルティングを大手の情報セキュリティ専門会社に委託することといたしました。

定期的なセキュリティ監査等の実施

今後については、定期的にセキュリティ診断、情報セキュリティ監査を実施し外部専門家の助言も得るなど、情報漏えいを防ぐため抜本的に業務運営を改善致します。

従業員に対する再啓蒙

全ての従業員に対して、改めて個人情報取扱事業者の従業員の認識を高め、個人情報の保護についての啓蒙を行います。また、クラブゲッツにおいては、内部統制の手順を見直し、個人情報の保護の観点から不十分な項目がある場合は、改定を行います。

システム改修

クレジットカード決済方法については、決済代行会社の運営するサーバ上に直接申し込み情報を入力するようにし、また決裁システムの入口をマイページ化することで、お客様が頻繁に個人情報を入力することのないような仕様に変更致します。

以上

（別紙）　ネットワーク構成図

個人情報の扱い

インターネット

■FWセキュリティポリシー

①インターネットからDMZへの許可

※アプリケーションサーバーWindowsパスワード管理

②インターネットからDMZ②への拒否

③DMZからDMZ②へのOracleポートのみ許可

※Oracleパスワード管理

④インターネットSSL暗号化通信

⑤社内LANからのVPN接続セキュリティ使用

※戻りポリシーも同様

ファイア
ウォール

DMZ環境

HUB

アプリケーションサーバー

HUB

DMZ環境②

インターネットVPN

クラスタリング　サーバー

個人情報・予約情報管理DBサーバー

※決済関連のDBは取扱っておりません