平成 25 年５月１日

各　　位

上 場 会 社 名　株式会社ジェイアイエヌ
（コード番号：3046　JASDAQ スタンダード）
代　　表　　者　代表取締役社長　田　中　　仁
問 合 せ 先　専務取締役管理本部長　中　村　　豊
電　話　番　号　TEL（03）6406-0120（代表）
U　　R　　L　http://www.jin-co.com

不正アクセス（JINS オンラインショップ）に関する調査結果（最終報告）

平成 25 年３月 15 日「不正アクセスによるお客様情報流出の可能性に関するお知らせとお詫び」でご報告いたしました当社オンラインショップに対する不正アクセス（以下、「本件不正アクセス」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および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。

当社は、事案発覚直後より、逐次最新情報をご報告させていただいておりましたが、この度、当社、専門調査機関および情報漏えい事故調査委員会による本件不正アクセスに関する一連の調査が終了いたしましたので、下記のとおりご報告させていただきます。

なお、本件不正アクセスに関するお客様へのご対応および再発防止に対する取り組みについては引き続き行ってまいりますが、本件不正アクセスに対する調査結果につきましては、特段の報告事項が発生しない限り、下記をもって最終報告とさせていただきます。

記

１．調査の経緯

当社は、自社が運営する「JINS ONLINE SHOP」（以下、「当社オンラインショップ」といいます。）にかかる情報漏えい事故について、平成 25 年３月 14 日、当社オンラインショップのウェブサーバへの不正アクセスの痕跡を発見し、クレジットカード情報漏えいの可能性を認識した直後に、情報漏えい事故対策本部を設置いたしました。

同事故対策本部において、事故対応全般と情報漏えい範囲等の調査にあたる一方、クレジット情報漏えい事案の専門調査機関である「Payment Card Forensics 株式会社」へ、本件不正アクセスの発生原因の調査、情報漏えい範囲の特定を委託し、４月８日付で事故発生原因等に対する最終調査報告書を受領し、その内容を４月９日にご報告させていただいております。

なお、本件事故の原因究明、再発防止策、責任の所在については、専門的および客観的な見地からの調査、検討および評価が必要であると判断し、社外の専門家で構成される情報漏えい事故調査委員会を平成 25 年３月 18 日付で設置し、調査を委託いたしました。

２．調査概要

①情報漏えい事故対策本部

当社社長を対策本部長とし、執行役員および社内各部署の幹部社員により構成され、主に情報漏えい範囲の調査特定、情報収集およびその他各種事故対応全般を社内の立場から行いました。

②Payment Card Forensics 株式会社による調査

カード情報漏えい事故発生時の専門調査を行うための認定を受けた調査機関である Payment Card Forensics 株式会社（以下、「PCF 社」といいます。）に対し、本件不正アクセスの対象となったサーバのログの解析による不正アクセスの発生原因の究明、漏えい可能性があるデータ範囲の特定について調査を委託しました。

③情報漏えい事故調査委員会

PCF 社の調査と並行し、本件事故の原因究明、再発防止策、責任の所在について、専門的および客観的な見地から調査、検討および評価をするため、下記のとおり情報漏えい事故調査委員会（以下、「本調査委員会」といいます。）を設置し、調査を委託いたしました。

・メンバー構成

委員長　大井 哲也　（TMI 総合法律事務所　弁護士）
委　員　野﨑 周作　（Payment Card Forensics 株式会社　代表取締役）
委　員　吉田 和雅　（TMI 総合法律事務所　弁護士）

・委託内容

（１）本件事故の事実関係の調査
（２）本件事故の原因究明
（３）再発防止策に対する評価
（４）責任の所在に対する意見

④警察による捜査

上記①から③の他、当社は、事件が発覚した後速やかに、警視庁生活安全部サイバー犯罪対策課および原宿警察署生活安全課に対し、本件不正アクセスに関する捜査要請を行っており、要請に基づき、不正利用によって購入された商品の発送先住所地の確認、情報送信先サーバのログ解析等による捜査活動が行われております。なお当社は、本件不正アクセスに対する被害届を４月 22 日付で原宿警察署へ提出し、受理されております。

３．調査結果

上記の調査等の結果、判明した事項は以下の通りであります。

（１）漏えいした可能性のあるクレジット情報の範囲

平成 25 年４月９日にご報告させていただきましたとおり、漏えいした可能性のあるクレジットカード情報の範囲は、平成 25 年３月６日から同年３月 14 日の間に当社オンラインショップにおいてクレジットカードによる購入手続きをされたお客様の情報2,059件であることが判明しております。

また、上記 2,059 件のうち、３月 15 日以降現在までにおいて、当社がお客様より不正利用があった旨の申告を受けている件数は 20 件でありますが、警察による捜査の結果、クレジットカードが不正利用され、商品が指定住所へ発送されたものの、逃走等により未到達となった結果、未遂に終わっているものも相当数含まれているとのことであります。なお、不正利用の申告は３月 30 日を最後に、その後本日に至るまで受付されておらず、不正アクセスの判明後、直ちにクレジットカード会社への通知を行っていたこともあり、当社としては不正利用はすでに収束しているものと認識しております。

なお、当該不正利用申告 20 件に対し、不正利用額の申告があったものについてはその申告額を損害額として、不正利用額の申告がなかったものについては申告があった金額の最高額を損害額であると仮定し算出する方法により、当社が現時点において合理的に見積もった最大損害想定額は3,053,000 円となります。なお、当該申告 20 件のうち、そのすべてが本件不正アクセスによるクレジットカード情報漏えいに起因する不正利用か否かは判明しておらず、また当社は、現時点においてクレジットカード会社から本件に関連した損害の請求を受けておりません。

今後も警察との情報共有、お客様からの被害申告の受付については継続して行い、その結果上記記載内容に加え、業績に重大な影響を与える可能性のある新たな事実が発生した場合は、速やかに開示させていただきます。

（２）事故の原因

PCF 社の調査によると、本件不正アクセスの原因は、第三者が当社オンラインショップのシステムに使用されていたミドルウェア（※）「Apache Struts2（以下、「Struts」といいます。）」の脆弱性を利用してシステムに不正に侵入し、ファイルの変更権限を不正に取得したことによるものであること、および当該システムに使用されていた Struts が、すでに過去に脆弱性が指摘されていた古いバージョンのものであったことによることが報告されております。

（※）ミドルウェア

プログラムの基本的機能を提供する汎用プログラム

（３）責任の所在

本調査委員会による社内外関係者のヒアリング調査により、本件不正アクセスの責任の所在についての本調査委員会としての見解につき、以下の通り報告を受けております。

・当社の責任

当社は、オンラインショップに関するシステムの構築および保守サポート業務をシステム開発業者（以下、「ベンダ」といいます。）に対して一括委託をしておりましたが、結果的に後述のとおりベンダにおける情報セキュリティ管理体制の不備が発生していることから、ベンダ選定時の調査・分析、システムの保守サポート業務品質の管理義務が充分になされていなかったという不備が認められると指摘されております。

・ベンダの責任

ベンダは、すでに脆弱性が指摘されていた Struts の古いバージョンを使用したまま、当社オンラインショップシステムの改修作業を完了しており、本来、システム開発会社として善良なる管理者の義務に基づき瑕疵のないシステム構成を設計すべき義務があるところ、それを看過してシステム構成の設計を行っていた点で責任があると指摘されております。

４．対応および再発防止策

（１）情報漏えいに対しこれまでに行った対応

当社は、本件不正アクセスの発生以降、以下の対応を行ってまいりました。

・本件不正アクセス専用の問合せ窓口の設置
・当初情報漏えいの可能性がある旨発表した 12,036 人のお客様がクレジットカードを再発行された場合の再発行手数料を、当社が負担する旨の各クレジットカード会社に対する意思表示と、対象のお客様へのその旨のご案内（その後、上記の PCF 社最終調査報告により、実際の情報漏えい期間（３月６日～３月 14 日）と漏えい件数（2,059 件）が判明しておりますので、当該情報漏えいの可能性のあるお客様以外の方については、クレジットカード再発行の必要はございません。）
・同じく上記 12,036 人のお客様に対する謝意として 1,000 円分の QUO カードの送付
・メールによる当社オンラインショップ会員への最新情報のご報告と、クレジットカード不正利用早期発見のためのクレジットカード会社への確認、利用明細確認等のお願いのご連絡

（２）今後の再発防止策

当社は、情報漏えい事案の再発防止のため、以下の施策の実施を決定し着手しております。

・クレジットカード決済システムの国際的なセキュリティ基準である「PCI DSS」への準拠

同基準に準拠した体制構築をすることにより、当社の情報セキュリティレベル全体の向上につながることのみならず、同基準からの要求事項のひとつとして、一定以上の外部委託先の管理水準の実現が挙げられていることから、前出の本調査委員会からの当社に対する指摘事項である、「ベンダの調査・分析、システムの保守サポート業務品質の管理義務」についても充分に果たすことが可能となります。

・画面遷移型のクレジットカード情報非保持サービスの採用
　このサービスを採用することにより、オンラインショップの購入画面で決済方法としてクレジットカード決済を選択した場合に、決済代行会社が管理するウェブサイトへ画面が遷移することで、購入者のクレジットカード情報が当社サーバ等のシステムを一切通過しないこととなり、当社システムからの情報漏えいの可能性が排除されることとなります。

なお、上記再発防止策に対しては、本調査委員会より、非常に高い情報セキュリティレベルが実現可能であり、セキュアなクレジット決済を行うことが可能になる施策であると評価されております。

５．業績への影響

既報の通り、本件不正アクセスが今後当社業績に与える影響は、下記理由により軽微であると考えております。

・オンラインショップの売上が当社グループの売上全体に占める割合は約４％程度（平成 25 年８月期第２四半期累計期間実績）であり、かつ休止期間により見込まれるオンラインショップ売上の減少は、平成 25 年４月４日に開示した修正後業績予想数値にすでに反映していること
・これまで行った各種対応に要した費用（調査委託費用、QUO カードの購入代金等）、および今後発生が見込まれるクレジットカードの再発行手数料、システム更改にかかる投資コストについても、同じくその見込額を平成 25 年４月４日に開示した修正後業績予想数値にすでに反映していること

なお、今後本件不正アクセスに関し、当社業績に重大な影響を与える事象が発生した場合は、速やかに開示いたします。

６．オンラインショップ再開予定時期

すでに、前述の再発防止策の実施と並行し、オンラインショップ再開に向けた作業に着手しております。今後、新システムの完成、PCI DSS 準拠の監査、クレジットカード会社の審査等の段階を経て、平成 25 年６月中の再開を見込んでおります。

７．問い合わせ窓口について

これまで、本件不正アクセスに関するお問い合わせにつきましては、下記専用問合せ窓口にて受付させていただいておりましたが、本最終報告を受け、５月 10 日（金）をもちまして専用問合せ窓口を終了させていただき、以後のお問い合わせにつきましては、当社カスタマーサポートセンター（営業時間：平日 10:00～17:00）にてお受付させていただきます。

JINS お客様情報対応窓口（平成 25 年５月 10 日（金）19 時まで）
電　話：0120-393-301
（9:00～19:00　月～金（５月４日（土）・５日（日）は営業いたします））
メール：privacy@jins-jp.com

カスタマーサポートセンター（平成 25 年５月 13 日（月）10 時から）
電　話：0120-588-418
（10:00～17:00　土日祝日を除く）
メール：support@jins-jp.com

以上