平成 29 年 6 月 30 日

各　位

会 社 名　東洋商事株式会社
代表者名　代表取締役　　西　澤　　淳

当社通販サイトへの不正アクセスによる
個人情報流出に関するご報告と対応についてのお知らせ

当社は、平成 29 年 4 月 14 日付「当社通販サイトへの不正アクセスによる個人情報流出の可能性についてのお知らせ」にて公表いたしましたとおり、当社が運営する通販サイト「東商マート(https://toshomart.com)」（以下、当該サイトといいます。）におきまして、不正アクセスがあり、個人情報が一部流出した可能性があることについて、外部の専門調査機関とともに、事実調査・原因究明および再発防止策の策定に取り組んでまいりましたので、その内容についてご報告いたします。

記

1　個人情報の漏洩とその件数

平成 29 年 4 月 1 日から同年 4 月 10 日に、当該サイト管理画面への不正アクセスにより、55 件の顧客情報が閲覧されました。
閲覧された情報には
・お名前（ご発注担当者のご登録のあったご利用明細のみ）
・ご住所
・電話番号
・メールアドレス
が含まれておりました。

また、Web プログラムの改ざんにより、平成 29 年 4 月 1 日から同年 4 月 10 日に当該サイトにて新たにクレジットカード情報を入力いただいたお客様 13 件(閲覧された顧客情報 55 件とは異なる。）のクレジットカード情報が流出した可能性があります。
漏洩の可能性があるクレジットカード情報は、
・カード番号
・カード会員名
・カード会員住所
・有効期限
・セキュリティコード
となります。

2　個人情報の漏洩の経緯とその後の事実関係

平成 29 年 4 月 10 日 当該サイト利用顧客より、クレジットカード決済が行えない旨の問い合わせが当社に寄せられ、これを受けて、システム提供元事業者での調査を開始いたしました。

この調査の中で、プログラムの改ざん並びに、不正ファイルがサーバー内に存在していることを確認し、クレジットカード情報流出の懸念から、当該サイトでのカード決済を停止いたしました。

同年 4 月 17 日より 外部の専門調査機関による調査を行い、その結果、一部のお客様のクレジットカード情報が流出した可能性があることを確認いたしました。

当該サイトに対して、平成 29 年 3 月 19 日より、SQL インジェクション攻撃が頻繁に行われ、同年 3 月 31 日 23 時 28 分、SQL インジェクション攻撃により取得された管理画面へのログイン情報を用いて、管理画面へログインされました。同年 3 月 31 日 23 時 31 分、管理画面で提供するファイルアップローダーを経由して、バックドアプログラムが Web サーバー上に設置され、以降、不正アクセスを検知し、不正アクセス元のアクセス制限を行った同年 4 月 10 日 13 時までの期間に、管理画面上の取引情報の一覧及び、会員マスタへアクセスし 55 件の顧客情報が閲覧されました。

さらに、同年 4 月 8 日 21 時 14 分にカード情報入力フォームの実行キャッシュファイルの改ざんが行われ、これ以降カード情報入力フォームへ入力されたカード情報は、画像ファイルに偽装されたファイルとしてサーバー内に記録されました。この改ざん以降、当該サイトにて、顧客がカード情報を入力しました 2 件のクレジットカード情報、および、当社並びにシステム提供元事業者にてテスト入力を行いましたカード情報 3 件が、ファイルに記録されておりました。

また、バックドアプログラムが設置された同年 4 月 1 日以降についても、カード情報漏洩の可能性が否定できないとの外部の専門調査機関の調査により指摘を受けており、この期間 8 件のカード情報を入力いただいた取引が存在しておりました。

3　初期対応の実施について

平成 29 年 4 月 10 日、システム提供元事業者により、不正アクセス元 IP を特定し、サーバーへのアクセスを遮断、改ざんにかかわる全てのファイルの隔離、管理画面への管理者パスワードの変更、管理画面へのアクセス元 IP の制限、データベースパスワードの変更、ディレクトリに対する権限制限の実施、SQL インジェクション発生箇所の特定と脆弱性への対応など、情報漏洩の防止対策を行いました。

また、当社は同年 4 月 17 日警察への報告、4 月 19 日警察への被害状況の説明を実施し

、同年 6 月 22 日にシステム提供元事業より、所轄官庁への報告を行いました。

4　原因と再発防止策について

この度の事態を真摯に受け止め、前述のとおり平成 29 年 4 月 17 日に外部の専門調査機関への詳細調査を依頼し、不正アクセスの詳細な事実調査を行った結果、SQL インジェクション攻撃への脆弱性およびサーバー実行権限の不適切な設定が判明いたしましたので、以下のとおり再発防止策を策定し、現在実行にあたっております。

① システムセキュリティにおける対策について

個人情報の漏洩の直接的原因となったシステムセキュリティにおける不備項目について、以下緊急対策を実施済みです。

1) 当該システム全体の SQL インジェクションへの対応
2) jQuery 等の潜在脆弱性への対応
3) 当該システム全体のディレクトリ実行権限、アクセス権限の見直し、再設定
4) 不正アクセスの監視及び、ブロック対応
5) パスワードを非可逆式の高度な暗号化に変更
6) 管理画面に対して IP アドレスによるアクセス制限の実施

② 保守・運用における対策について

一定のセキュリティレベルを維持するために、システム提供元事業者にて、下記の対策を実施することで恒久的な対策を実施いたします。

1) 定期的な外部機関による脆弱性調査の実施
2) サーバーシステムや使用しているプラグイン等の潜在的な脆弱性情報の早期取得と、バージョンアップの早期対応

5　お客様へのご連絡とお詫びについて

個人情報の漏洩および漏洩の可能性があるお客様には、平成 29 年 4 月 13 日より電話にてご連絡を差し上げております。また、平成 29 年 6 月 23 日に書面郵送による最終報告書を送付させていただきました。

① クレジットカード情報の漏洩懸念のあるお客様へのお願い

カード会社からのご利用明細書に、身に覚えのないお取引がないかご確認をお願い致します。万一、身に覚えのない請求がございましたら、カード裏面記載のクレジットカード会社の連絡先にお問い合わせ下さい。不正な請求と確認できた場合、お客様へのご負担が発生することがないようクレジットカード会社に依頼しております。

② クレジットカード再発行について

お客様がクレジットカードの再発行をご希望の場合、お手数をおかけいたしますが、ご本

人様よりご依頼いただくことが必要条件となりますため、カード裏面に記載の電話番号へ直接ご連絡いただき、クレジットカードの再発行手続きをご依頼いただきますよう、よろしくお願い申し上げます。漏洩懸念のあるお客様がカードの再発行をご希望された場合においては、お客様へのご負担が発生することがないようクレジットカード会社に依頼しております。

なお、本件に関するお客様からのお問合せは、下記の「東商マートカスタマーセンター専用ダイヤル」にて承ります。

専用ダイヤル： 03-4531-9877（9時～17時 土・日・祝日を除く）
メールアドレス：support@toshomart.com

以上