別記様式第一（第八条第三項関係）

受付日	年　月　日
受付番号	

報告書

個人情報の保護に関する法律第 26 条第１項の規定により、次のとおり報告します。

令和●年５月 15 日

個人情報保護委員会　殿

報告者の氏名又は名称　　株式会社○○工業
住所又は居所　　○○県△△市××－××

１．報告種別（該当する□に印を付けること。）
新規又は続報の別：□ 新規　☑ 続報　前回報告：令和●年４月２日
速報又は確報の別：□ 速報　☑ 確報

２．報告をする個人情報取扱事業者（以下「報告者」という。）の概要

報告者の氏名又は名称	（フリガナ）カ）●●●●コウギョウ 株式会社○○工業												
法人番号（13 桁）	●	●	●	●	●	●	●	●	●	●	●	●	●
業種・業種番号	●●●●業									●	●	●	●
報告者の住所又は居所	○○県△△市 ××－××												
代表者の氏名（報告者が法人等の場合に限る。）	（フリガナ）コジョウイ　イチロウ 代表取締役 個情委　一郎												
事務連絡者の氏名	（フリガナ）カ）●●●●コウギョウ　ソウムブ　○○カ　ホゴホウ　ジロウ 株式会社○○工業 所属部署　総務部○○課　保護法　二郎 電話　●●●●（　●●　）　●●●● E-mail　●●●●@●●.jp												

３．報告事項

（１）事態の概要（該当する□に印を付けること。）

発生日：令和●年２月１日

発覚日：令和●年４月１日

発生事案：☑ 漏えい　□ 漏えいのおそれ　□ 滅失

□ 滅失のおそれ　□ 毀損　□ 毀損のおそれ

発見者：□ 自社/委託先　□ 取引先　□ 顧客/会員

☑ カード会社/決済代行会社　□ その他（　　）

規則第７条各号該当性：□ 第１号（要配慮個人情報）

☑ 第２号（財産的被害）

☑ 第３号（不正の目的）

□ 第４号（千人超）

□ 非該当（上記に該当しない場合の報告）

報告者に個人データの取扱いを委託した者（委託元）の有無：

□ 有（名称：　　）

（住所：　　）

（電話：　　）

☑ 無

報告者から個人データの取扱いの委託を受けた者（委託先）の有無：

☑ 有（名称：株式会社●●●●　　）

（住所：●●県●●市●●●●　　）

（電話：●●-●●●●-●●●●　　）

□ 無

事実経過：

概要：

弊社が運営するショッピングサイト「●SHOP」（△△（オープンソースの EC サイト構築用プログラム**（※製品名等を補記ください）**で構築））がクロスサイトスクリプティング（XSS）攻撃による不正アクセスを受けクレジットカード情報等が漏えいした。

発覚の経緯・発覚後の事実経過（時系列）：

R●.4.1　決済代行会社より、当社ショッピングサイト上でカード決済を行った顧客のカードが不正利用されている可能性があるとの連絡あり、顧客情報の漏えいのおそれがあるため、カード決済を停止した。
　当該サイトの保守運用を委託しているベンダーへ調査を依頼する。
　この時点では詳細な原因等は判明せず。

R●.4.3　決済代行会社の要請により外部業者へフォレンジック調査を依頼する。

R●.5.27　調査の結果、下記のとおり外部からの侵入の痕跡が確認された。

R●.2.1　△△の XSS に関する脆弱性を悪用され、注文システム内に悪性のスクリプトが挿入される。
R●.2.2　挿入された悪性スクリプトが実行され、ショッピングサイト「●SHOP」内に悪性ファイルが設置される。
R●.2.4～R●.4.1　悪性ファイルを利用し、この期間中にショッピングサイト「●SHOP」上で決済を行った顧客のカード情報が収集される。

※発覚の経緯・発覚後の事実経過欄に以下内容をご記入ください。
・発覚日、発生日、発覚に至る経緯（いつ、どのように）被害の拡大防止のためにとった措置を時系列に記載
・結果（ランサムウェアでデータを暗号化された、カード情報を取られた、他の攻撃（スパムメール送信）への踏み台にされた）を含む

外部機関による調査の実施状況（規則第７条第３号に該当する場合のみ記載）：
☑ 実施済（実施中）【依頼日：令和●年４月３日】
☐ 実施予定【依頼予定日：　　年　　月　　日】
☐ 検討中
☐ 予定なし
（詳細：　　）

（２）漏えい等が発生し、又は発生したおそれがある個人データの項目（該当する□に印を付けること。）
媒体：☐ 紙　☑ 電子媒体　☐ その他（　　）
種類：☑ 顧客情報　☐ 従業員情報　☐ その他（　　）
項目：☑ 氏名　☐ 生年月日　☐ 性別
☐ 住所　☐ 電話番号　☐ メールアドレス
☑ クレジットカード情報　☐ パスワード
☑ その他（購入商品　　）

（３）漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数
（　500）人　　うちクレジットカード情報含む（　500）人

（４）発生原因（該当する□に印を付けること。）

主体：☑ 報告者　　□ 委託先　　□ 不明

原因：☑ 不正アクセス

（攻撃箇所：（ショッピングサイト（その他例）会員サイト、社内ネットワーク等））

（攻撃手法：（　クロスサイトスクリプティング攻撃　））

□ 誤交付　　□ 誤送付（メール含む。）

□ 誤廃棄　　□ 紛失　　□ 盗難　　□ 従業員不正

□ その他（　　）

詳細：

当社ショッピングサイトの脆弱性からクロスサイトスクリプティング攻撃を受けた。

当サイトの保守・管理は委託先に依頼していたが、セキュリティに関する契約が曖昧になっていたため、当然行われていると思っていた必要なセキュリティパッチが当たっていなかった。

※以下の内容をご記入ください。

詳細原因、手法（●の脆弱性、SQL インジェクション、マルウェア感染等、標的型攻撃メール、リスト型・総当たり、その他（不審なサイト閲覧、感染した USB 使用等））、攻撃を受けたシステム等の管理状況（委託先、自社）

（５）二次被害又はそのおそれの有無及びその内容（該当する□に印を付けること。）

有無：☑ 有　　□ 無　　□ 不明

詳細：

クレジットカード情報の不正使用

（令和●年５月 10 日時点、32 件、400 万円程度）

（６）本人への対応の実施状況（該当する□に印を付けること。）

本人への対応（通知を含む。）：☑ 対応済（対応中）　　□ 対応予定

□ 予定なし

詳細（予定なしの場合は、理由を記載）：

・個別に電話、メールにて、状況説明及び謝罪の連絡

・相談窓口の設置

（７）公表の実施状況（該当する□に印を付けること。）

事案の公表：☑ 実施済【公表日：令和●年４月 28 日】
□ 実施予定【公表予定日：　　年　　月　　日】
□ 検討中
□ 予定なし

公表の方法：☑ ホームページに掲載　　□ 記者会見
□ 報道機関等への資料配布
□ その他（　　）

公表文：

※公表文を記載してください。

（８）再発防止のための措置

実施済の措置：

・弊社ショッピングサイト上でのカード決済を停止 ・iSO27001 や PCI DSS を取得している新 EC サイトに移行（脆弱性診断実施済み） ・WAF の設置・保守管理契約の見直し ・セキュリティ運用体制の見直し（セキュリティ責任者を設置し、セキュリティ対策の実施状況を定期的に確認する。）

今後実施予定の措置（長期的に講ずる措置を含む。）及び完了予定時期：

・定期的な脆弱性診断の実施 ・外部との通信の監視の強化（セキュリティ専門事業社の監視サービスを利用等）

（９）その他参考となる事項：

記載要領

１．最上段の受付日及び受付番号の欄には記載しないこと。

２．続報として提出の際には、前回報告から記載を変更した箇所に下線を引くこと。

３．２．の「法人番号」とは行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）第２条第 15 項に規定する「法人番号」を指す。なお、法人番号を記載する欄に、同条第５項に規定する「個人番号」を記載しないこと。

４．２．の「業種」・「業種番号」（４桁）は、日本標準産業分類から記載すること。

５．２．の「事務連絡者の氏名」の「電話」には、代表電話番号ではなく、当該事務連絡者の直通電話番号を記載すること。

６．２．の「法人等」には、法人格を有しない団体等も含まれる。

７．３．（７）の「公表文」には、公表を予定している場合、公表予定の文案を記載又は添付すること。

８．用紙の大きさは、日本産業規格Ａ４とすること。