2019 年 9 月 24 日

各 位

不正アクセスによるお客様情報流出について（ご報告）

一般社団法人日本経営協会

標記の件につきまして、下記のとおりご報告申し上げます。
大変なご迷惑と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。

記

1.事案の概要
2019 年 8 月 22 日、本会 EC サイト（https://noma-ec.jp/）のステージング環境（テスト用サーバー）に対する外部からの不正アクセスによってデータベース情報の抜取りが発生した。

1）発生経緯

日時	内容
8 月 21 日（水） 16：30	【本会】 ・本会担当者より委託事業者に対し、EC サイトの商品データ更新をメールにて依頼。
8 月 22 日（木） 10：00～ 11：20	【受託事業者】 ・商品データを変更するためステージング環境（テスト用サーバー）にアクセスしたところ、対象の作業用データベースがなくなっていることに担当者が気づいた。〔A〕 ・このままではデータ更新ができないため、担当者の判断で一時的に本番環境の個人情報を含むデータベースをステージング環境へ投入し、商品データを更新した。〔B〕 【本会】 ・本会担当者が、受託事業者よりステージング環境でのデータ更新確認の依頼メールを受信。それを受けて商品データが変更されたことを確認した。（この時点で作業用データベース喪失及び本番データベース投入の事実は本会に報告なし。） なお、上司が不在だったため本番環境への反映は保留した。
8 月 23 日（金） 10：00～	【受託事業者】 ・ステージング環境のデータベースを確認したところ、昨日投入し更新したはずのデータベースが再びなくなっていることが発覚した。

11：40 12：00	・サーバーを調べたところ、見覚えのないデータベースに身代金要求のメッセージ（後掲）が記載されていることを発見した。 ・本番環境及びステージング環境のデータベースパスワードを変更。本番環境サーバーのアクセスログを検証し、同様の事案が発生していないことを確認した。 【本会】 ・受託業者より本事案発生の第 1 報を受ける。

2）事故原因

〔A〕作業用データベースがなくなっていることに気づいた時点で、その原因を調査すべきであった。

〔B〕個人情報を含んでいた本番サーバーのデータベースを、そのままステージング環境に投入すべきではなかった。

2.判明している事実

1）抜き取られたデータベース

テーブル数：15

総データ件数：8987 件

内個人情報を含むデータ件数：2851 件（メールアドレスによる一意：2121 件）

2）流出した個人情報の内訳

2018 年 9 月 1 日～2019 年 8 月 22 日の期間に本会 EC（https://noma-ec.jp/）サイトから個人で次の申込をされた方の個人情報。

① 経営学検定試験の受験申込

② 経営学検定、ファイリングデザイナー検定、電子ファイリング検定、公文書管理検定、ITPS 検定のテキスト及び過去問題集の購入申込

③ 通信教育の受講申込

3）個人情報の内容：

氏名※、住所※、メールアドレス※、電話番号※、生年月日、会社名、FAX 番号、性別（※は必須項目、その他は任意項目）

4）不正アクセスの痕跡

8/10　138.197.199.81（アメリカ）からの不正アクセスによりステージング環境のデータベース（ダミー）の抽出及び削除

8/22　138.197.199.81（アメリカ）からの不正アクセスにより本番環境から投入したデータベースの抽出及び削除

5）身代金要求のメッセージ

本会は下記要求には応じず、返信等一切行っておりません。

（以下原文）

To recover your lost Database send 0.03 Bitcoin (BTC) to our Bitcoin address 1rm6Xk4Buk42vHE55X7VseErFHjqd93vH and contact us by Email with your Server IP or Domain name and a Proof of Payment. Your Database is downloaded and backed up on our servers. Backups that we have right now: *******. Any email without your server IP Address or Domain Name and a Proof of Payment together will be ignored. If we dont receive your payment in the next 10 Days, we will delete your backup.

（訳）

失われたデータベースを回復するには、ビットコインアドレス 1rm6Xk4Buk42vHE55X7VseErFHjqd93vH に 0.03 ビットコイン（BTC）を送信し、サーバーIP またはドメイン名と支払い証明をメールで連絡せよ。

お前のデータベースはダウンロードされ、我々のサーバーにバックアップされている。

我々が現在持っているバックアップ： *******。

サーバーの IP アドレスまたはドメイン名と支払い証明が一緒に記載されていないメールは無視される。10 日以内に支払いを受け取れない場合には、バックアップを削除する。

6）本番環境について

本事案発生直後に本番 EC サイトサーバーのアクセスログを検証し、不正アクセスによる侵入は発生していないことを確認している。

3.発覚後の対応

8 月 23 日（金） 17：00　受託事業者から本会に対し口頭にて状況の報告を受ける。
直ちに緊急情報対策チームを編成し対応にあたることを決定。受託事業者に対し事実関係の確認と流出情報の特定を指示。所轄の警察署へ通報。

8 月 26 日（月） 四谷警察署へ赴き直接報告。

8 月 27 日（火） 流出個人情報を特定。個人情報保護委員会への報告。

8 月 30 日（金） 流出した個人情報の該当者の方々へメールにてお詫びと報告。ホームページに事案の報告を掲示。安全性再検証のため EC サイトを一時停止。

4.公的機関への届出等

・四谷警察署 生活安全課 保安係へ報告。
後日、警視庁サイバー犯罪対策課へ捜査協力のため該当のアクセスログを提出。

・個人情報保護委員会（PPC）へ届出

・独立行政法人情報処理推進機構（IPA）へ届出

5.実施済み対応策

EC サイトの本番環境、ステージング環境ともに一時停止し、下記の対応を行っております。

１）IP アクセス制限

ステージング環境においても、限られた IP アドレスのみアクセス可能な設定へ変更。

2）設定ファイルの修正

セキュリティレベルの設定を変更。

古いブラウザからの閲覧はできなくなるが、セキュリティチェックサイトでの評価は B→A+　に向上。(https://www.ssllabs.com/ssltest/)

3）脆弱性テストの実施

「OS・ミドルウェアレベル」、「WEB アプリケーションレベル」の 2 段階で脆弱性テストを実施し、安全性を確認。

4）運用担当者のセキュリティ教育

個人データ取り扱いに対する運用ルール変更、周知・徹底を実施。

6.今後の再発防止策

再発防止策として、以下の内容を強化、徹底いたします。

１）委託先事業者管理の徹底（監査等の実施も含む）

２）委託先事業者選定基準の見直し

３）社内ネットワークセキュリティの見直し

４）全職員への個人情報取り扱いに関する再教育の実施

7.お客様へのお願い

不審なメール、ハガキ、封書、電話などの広告・勧誘・セールスにご注意ください。

8. 本件お問い合わせ先（ご対応時間：平日 9：15～17：15）

一般社団法人日本経営協会　情報対策チーム

Mail security@noma.or.jp

TEL 03-3403-6394