2023年6月22日

本市が運営する「志布志市ふるさと納税特設サイト」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ

平素は志布志市ふるさと納税事業にご支援・ご理解を賜り誠にありがとうございます。

この度、本市へのふるさと納税の窓口の一つであります「志布志市ふるさと納税特設サイト」（以下「当サイト」といいます。）において、第三者による不正アクセスを受け、当サイトを通じて本市にご寄附をいただいた方（以下「寄附者様」といいます。）の一部のクレジットカード情報（910件）が漏えいした可能性があることが判明いたしました。

外部専門機関で調査し、現時点で判明した漏えいした可能性のある寄附者様につきましては個別にご連絡いたします。

なお、初期的な調査の結果から、当サイトを通じたクレジットカード決済以外の方法（他のポータルサイトや郵便振替）によりご寄附をいただいた方のクレジットカード情報が漏えいしたおそれはないものと考えております。

寄附者様をはじめ関係者の皆様に多大なるご迷惑及びご心配をおかけする事態となりましたこと、深くお詫び申し上げます。

本市では、今回の事態を厳粛に受け止め、事実関係の調査を続けるとともに再発防止のための対策を講じてまいります。

寄附者様をはじめ関係者の皆様には重ねてお詫びを申し上げますとともに、本件に関する概要につきまして、下記のとおりご報告いたします。

記

1. 概要

2023 年 4 月 6 日、一部のクレジットカード会社から、当サイトを利用した寄附者様のクレジットカード情報の漏えい懸念について連絡を受けました（なお、2022 年 10 月 24 日には、本漏えいとは関係しない保守管理上の理由により、すでに当サイトでのカード決済を停止しております。）。

ご連絡をいただいたのと同時に、当サイトの保守管理会社及び第三者調査機関による調査を開始しました。現在、クレジットカード情報に関しては、調査が完了し、原因等の詳細が判明いたしましたが、それ以外の情報に関する調査が継続中です。クレジットカード情報以外の情報に関する調査結果につきましては、改めてご報告させていただきます。

2. 発覚の経緯及び現在までの対応状況

- 2023年4月6日、クレジットカード会社より、当サイトを利用した寄附者様のクレジットカード情報について漏えいし及び不正利用された可能性がある旨の連絡を受けました。本市は、直ちに、個人情報漏洩リスク対応マニュアルに基づき、対策本部を設置し、鹿児島県警察に事案を報告するとともに、保守管理会社と連携し、調査を開始しました。
- 4月7日、個人情報保護委員会に対する速報を行いました。
- 同日、保守管理会社による内部調査の結果、当サイトからのクレジットカード情報漏えい事実が確認されるとともに、他方で、遅くとも2022年10月24日に当サイトの決済機能を停止した段階で新たな情報漏えいは行われなくなったと考えられることが判明しました。
- 4月11日、外部専門業者を選定し、調査実施に向けた協議を開始しました。
- 4月24日、サイバーセキュリティを専門とする外部の弁護士に相談し、助言を得るとともに、今後の対応について連携を開始いたしました。
- 5月30日、外部専門機関から、技術的な調査の中間報告を受領しました。
- 6月5日、個人情報保護委員会に対する確報を行いました。
- 6月8日、鹿児島県警察に被害申告をいたしました。
- 6月9日、外部専門機関から、クレジットカード会員情報漏えいに関する調査の最終報告書を受領し、原因等の詳細が判明いたしました。

3.個人情報漏えい状況

(1)原因

当サイトのシステムの一部（EC-CUBE）の脆弱性を悪用したクロスサイトスクリプティングの手法による第三者の不正アクセスにより、サーバー内に、クレジットカード決済実行時において処理されるクレジットカード情報を窃取するためのプログラムを埋め込まれたと考えられます。

(2)クレジットカード会員情報漏えいの可能性がある寄附者様及び項目

クレジットカード情報に関する調査結果によりますと、2021年3月12日から2021年12月29日までの間に当サイトを通じてクレジットカード決済を行った寄附者様（910件）が対象となります。

漏えいした可能性のある情報は以下のとおりです。

・クレジットカード番号
・有効期限
・セキュリティコード
・Webサイトのログイン情報（eメールアドレス、パスワード）
・電話番号（ご注文時にログインも会員登録もされていない寄附者様）

上記に該当する寄附者様には、判明次第、別途、個別にメール又は書面にてご連絡

申し上げます。

(3)その他の個人情報漏えいの可能性について

クレジットカード情報以外の個人情報が漏えいした可能性については、現在も調査継続中です。判明次第、お知らせいたします。

4. 再発防止策

今後、本市及び保守管理会社は、次の再発防止策を実施いたします。

(1) 本市のセキュリティ管理体制の見直し

外部専門業者及び弁護士の助言の下、個人情報漏洩リスク対応マニュアル及び志布志市情報セキュリティ運用指針の運用を見直し、本市が運営するWebサイトについて、適切な管理体制を構築します。

(2) 外部委託先選定基準及び監督方法の見直し

志布志市情報セキュリティ運用指針に基づき、委託業者を選定するに当たっての留意事項を具体的かつ明確にするべく、外部委託先選定基準を明確化します。また、保守管理会社に対し志布志市情報セキュリティ運用指針及び情報セキュリティ対策特記事項を遵守するよう指導し、適切な監督を通じて適正なセキュリティ対策を実施します。さらに、保守管理会社に対し本市の基準に適合するセキュリティ運用規程の策定及び当該規程の運用並びにセキュリティ担当チームの運用の徹底を求めるとともに、情報漏えい事案を始めとするセキュリティインシデント等のモニタリングの強化を求めます。

(3) 当サイトについて、保守管理会社は、本市と協議の上、以下の対策を実行します。

① サイトに利用しているソフトウェアの脆弱性対応の徹底

当サイトに利用しているソフトウェア全てについて、脆弱性情報の取得と対応を徹底するとともに、サイト全体の脆弱性の定期診断の実施を徹底します。

② セキュリティ・ソリューションの導入

本件では、WAF(Web Application Firewall)を採用した2021年12月29日以降、クレジットカード情報の漏えいは確認されておらず、WAF による対策の効果が高い事案でした。今後も、WAFの使用を徹底してまいります。

また、不正侵入検知・防止に向けた更なるセキュリティ・ソリューションの導入・維持、及びその適切な運用を行ってまいります。

③ 重要ファイルの変更検知機能のチェック体制強化

今後、本件同様に不正なプログラムの埋め込み・プログラムの不正な改ざんが行われた場合、これを即時に検知し、情報漏えいを防止するために、サイト全体の重要ファイルの変更検知機能を搭載することを厳守し、変更検知を常に確認することが出来る体制、変更が検知された場合にどのような対策を実施するかの規程を作成し、重要ファイルの変更検知運用を徹底してまいります。

また、システム全体のログ記録の管理ポリシーを確立することで、不正なアクセスなどの記録を事後の調査に必要十分な期間、保管してまいります。

5. 寄附者様へのお願い

本市では、クレジットカード会社と連携し、漏えいした可能性のあるクレジットカードによる取引のモニタリングを継続して実施し、不正利用の防止に努めてまいります。

寄附者様におかれましても、誠に恐縮ではございますがクレジットカードのご利用明細書に身に覚えのない請求項目がないか、今一度ご確認をお願いいたします。万が一、身に覚えのない請求項目の記載があった場合は、たいへんお手数ですが同クレジットカードの裏面に記載のカード会社にお問い合わせいただきますよう、併せてお願い申し上げます。

なお、寄附者様がクレジットカードの差し替えをご希望される場合、カード再発行の手数料につきましては寄附者様にご負担をお掛けしないよう、本市よりクレジットカード会社に依頼しております。

6. 公表までに時間を要した経緯について

2023 年 4 月 6 日の漏えい懸念から今回の案内に至るまで、時間を要しましたことを深くお詫び申し上げます。

本来であれば漏えいの疑いがある時点で寄附者様にご連絡し、注意を喚起するとともにお詫び申し上げるところではございましたが、不確定な情報の公開はいたずらに混乱を招くおそれがあるため、寄附者様へのご迷惑を最小限に食い止める対応準備を整えてから行うべきと考え、また、初期的な調査からさらなる漏えいのおそれは小さいと判断されたことから、調査会社から調査結果を受領し、確実な情報をお知らせできるようにカード会社その他関係機関との連携を十分にとった上で公表することといたしました。

今回の発表までお時間をいただきましたこと、重ねてお詫び申し上げます。

7. 今後の見通しについて

引き続き外部専門機関によるデジタルフォレンジック調査等を進めており、クレジットカード情報以外の個人情報が漏えいした可能性等について調査してまいります。

そのうえで、最終的な調査の結果も踏まえて、外部専門機関や弁護士等の助言のもと、再発防止策の策定等に向けた取り組みを進めてまいります。

さらに、引き続き、個人情報保護委員会や警察をはじめとした機関への報告・連携も進めてまいります。

改修後の当サイトの再開日につきましては、決定次第、改めて本市 Web サイト上にてお知らせいたします。

8.本件に関するお問い合わせ窓口

≪志布志市ふるさと納税特設サイト　ご相談窓口≫

・受付時間：平日 10:00～19:00（2023 年 6 月 24 日及び 25 日は受付いたします。）

・電話番号：フリーダイヤル　0120－673－490

・メールアドレス：shibushi@furusato-call.jp

以　上