薩摩川内市危機対応
（サイバー攻撃等）
令和８年１０月２５日
１３時００分現在

令和８年１０月１５日以降のサイバー攻撃等による危機事象に係る対応状況及び注意喚起（第１報）について

１　事象概要

対象サービス名等	内　容
⑴　NET119 緊急通報システム	不正アクセスによる個人情報漏えいの可能性
⑵　ふるさとチョイス	不正アクセスによる個人情報漏えいの可能性
⑶　いくかメール	不正アクセスによる個人情報漏えいの可能性
⑷　PHP 脆弱性事象	PHP 脆弱性による不正アクセス等のおそれ
⑸　GIGA スクール端末における web フィルタリングソフト	不正アクセスによる端末情報漏えいの可能性

２　対応状況

⑴　活動体制

体　制	設　置	解　除
危機警戒本部体制	10/15(木)　8:30	10/22(木)　8:00
危機対策本部体制	10/22(木)　8:00	継続中

⑵　会議開催状況

会議名	設　置
第１回個人情報等の漏えい危機警戒本部会議	10/15(木)　16:00～
第２回個人情報等の漏えい危機警戒本部会議	10/21(水)　16:00～
第３回個人情報等の漏えい危機警戒本部会議 （＝危機対策本部に切替）	10/22(木)　11:30～
第１回危機対応総合会議（危機対策本部会議） （サイバー攻撃等による危機事象に関すること）	10/23(金)　8:00～
第２回危機対応総合会議（危機対策本部会議） （サイバー攻撃等による危機事象に関すること）	10/25(日)　13:15～

３　事象の状況

⑴　NET119 緊急通報システム

①　概要

全国の自治体向け防災システムを提供する株式会社アルカディアの「NET119 緊急通報システム」に対する不正アクセス事象に関する報道を受け、薩摩川内市（北薩３消防本部指令センター）で運用している NET119 利用登録者の個人情報についても、漏洩した可能性があることが判明した。

項　目	内　容
⑴　対象サービス	NET119 緊急通報システム （音声による 119 番通報が困難な聴覚・言語障害者が円滑に消防へ通報を行えるようにするシステム）
⑵　対象 URL	net119.speecan.jp　net119fd.speecan.jp
⑶　対象機器	北薩３消防本部指令センター（３消防本部）NET119 緊急通報システム
⑷　対象人員	薩摩川内市消防局　（登録者 41 人＋緊急連絡先 13 人）計 54 人
⑸　対象情報	氏名・生年月日・性別・メールアドレス・電話番号・ＦＡＸ番号・障害内容・緊急連絡先（氏名・本人との関係・電話番号・ＦＡＸ番号・メールアドレス） ※　個人によっては、登録情報が上記全てではない。

② 被害状況

薩摩川内市における被害等は覚知していない。

③ 想定されるリスク

株式会社アルカディアのホームページに公表されていたフィッシング詐欺（※）へのリスクがさらに拡大するおそれあり。

（※　実在する企業等を装い、偽サイトなどへ誘導して情報を盗み取る手口）

④ 対応・対策

消防局で、情報漏洩した可能性のある利用登録者及び関係者に、メール・FAX（登録がある方）・電話（登録がある方）で、注意喚起のお知らせを行っている。

⑵ ふるさとチョイス

① 概要

令和８年１０月１９日、ふるさとチョイスを運営している、株式会社トラストバンクより、「同社システムに不正アクセスの疑いがある事象を検知したため、被害拡大の防止及び安全確保を最優先に、関連サービスを一時停止し、調査を行っている」と報告がなされた。

翌日、第三者による不正アクセスが行われ、会員登録いただいている寄付者の個人情報の一部が外部に流失したことが判明した。

項　目	内　容
⑴　対象サービス	ふるさとチョイス
⑵　対象者数	4,454,097 件
⑶　うち本市該当者	ふるさとチョイスを利用している市民：58 人
⑷　対象情報	氏名、メールアドレス、住所、電話番号、ハッシュ化されたパスワード、寄附控除試算額

② 被害状況

薩摩川内市における具体的な被害数等は覚知していない。

③ 想定されるリスク

不正取得された情報による悪質メール、特殊詐欺の接触

④ 対応・対策

- トラストバンク社が、全ての会員にメールで個人情報流出事象の発生を連絡済み
- 流出が確認できた会員には、トラストバンク社が個別で対応中
- 漏えいした会員のうち本市民分について、トラストバンク社に情報提供を依頼中

⑶ いくかメール

① 概要

株式会社ラクスライトクラウドから、第三者による不正アクセスを受け、同社が保有する個人情報の一部が外部に漏えいしたとの報告がありました。

なお、本市の「いくかメール」の配信業務を行っている市内事業者が同社のシスエムを利用していることから「いくかメール」会員のメールアドレスについても、漏えいした可能性があります。

項　目	内　容
⑴　対象サービス	いくかメール
⑵　対象者数	約 1,100 人
⑶　対象情報	メールアドレス

② 被害状況

薩摩川内市における具体的な被害数等は覚知していない。

③ 想定されるリスク
・ メールアドレス（約1,100件）の情報漏えい
・ 不正取得されたアドレスへの悪質メールの送信
④ 今後の対応・対策
・ いくかメールの配信情報は、観光物産ガイドこころで情報発信中であり、観光物産ガイドこころでの注意喚起の情報発信
・ 市公式Facebook、Instagramでの注意喚起の情報発信

⑷ PHP脆弱性事象
① 概要
ウェブサイト※1やウェブアプリケーション※2の裏側を動かすために利用されるＰＨＰ（プログラミング言語）に脆弱性があることが、ＰＨＰ開発団体から１０月２１日に発表された。脆弱性については、悪用されると、不正アクセスや情報の改ざん、システム停止などの被害につながるおそれがあることから、世界的に注意喚起が行われている。

※１　ホームページのこと
※２　「Google Chrome」「Safari」「Microsoft Edge」などのウェブブラウザ上で利用するアプリケーションのこと

② 被害状況
不正アクセスや情報の改ざん等について覚知していない。
③ 想定されるリスク
脆弱性を突かれた不正アクセスによる個人情報等の流出、情報の改ざん、システム停止
④ 対応・対策
・ ＰＨＰを利用したウェブサイトやウェブアプリケーションの休止、修正プログラムの適用
・ 各部局担当課において運用しているウェブサイト等のPHP利用に係る状況を確認

⑸ GIGAスクール端末におけるwebフィルタリングソフト
① 概要
デジタルアーツ株式会社より、GIGAスクール端末におけるwebフィルタリングソフト「iFilter@cloud」にて不正アクセスがあったとの連絡がなされた。
② 被害状況
薩摩川内市における被害等はない。
③ 想定されるリスク
業者によると情報流出のおそれ等はなく、本件に起因する情報の悪用や二次被害の報告はなし。
④ 対応・対策
・ 端末のログイン用のパスワードの変更を実施（市）
・ 監視の強化とネットワークの再構築（デジタルアーツ株式会社）

４　注意喚起
不正アクセスによる情報漏洩事案は全国的に発生しています。不審なメールを受信した場合には、記載されたURLへのアクセスや添付ファイルの開封、個人情報の入力等を絶対に行わず、速やかに削除し、不審な電話には応じないようお願いします。