中間報告書

株式会社ユニバーサル・サポート・システムズがサービス運用をしているインターネット出願システムで 2023 年 10 月 26 日に発生した情報漏洩事故に関して

2023 年 11 月 9 日

事故対策本部

本部長　　岡山保美

（株式会社ユニバーサル・サポート・システムズ　代表取締役）

副本部長　高畑道子

（株式会社シービーラボ　副社長）

株式会社ユニバーサル・サポート・システムズ（以下 USS 社）が 2016 年よりサービス運用を行っているネット出願システムにおいて、2023 年 10 月 26 日午後に、志願者の個人情報等が他の志願者から閲覧できたこと、利用している学校の管理画面が他の学校の管理者から閲覧できたことの連絡が 2 名の志願者と 2 校の学校管理者から USS 社にあり、USS 社及びシステムの保守を担当している株式会社シービーラボ（以下 CB ラボ社）においてすぐにその原因究明と復旧活動を開始し、その後被害範囲の把握と関係者への連絡を行った。

以下にその状況や対応等について報告します。

この度は、志願者や利用者（学校）の皆様に多大なご迷惑とご心配をおかけしておりますことを心よりお詫び申し上げます。

【まとめ】

・ 本件は、悪意ある外部からのサイバー攻撃に対してシステムやデータを防御するために AWS WAF と CloudFront のサービス利用を推進する中で、CloudFront のキャッシュ機能を有効に設定したところ、キャッシュ情報のミスヒットという想定外の事象が生じ、その時点で CloudFront のキャッシュ上に存在した志願者の画面や学校の管理画面が、他の志願者や学校管理者から見えてしまったという事故である。

・ 10 月 26（木）日 11 時 44 分に USS 社担当者によるテスト出願では問題なく動作していたことから、キャッシュ機能も正常に動作しているものと判断していたが、同日 13 時 15 分頃と 15 時 15 分頃に志願者及び学校管理者から寄せられた情報で本件不具合の発生を確認し、技術的に検討した結果キャッシュのミスヒットの可能性があるとのことで、同日 15 時 41 分にキャッシュ機能を無効に設定し直した。

・ 10 月 26 日（木）11 時 00 分からの保守作業で CloudFront のキャッシュ機能を有効に設定してから、同日 15 時 41 分にキャッシュ機能を無効に設定するまでの 4 時間 41 分間がインシデント発生時間になる。

・ キャッシュ機能を無効に設定し直した結果、その後本件不具合の報告はなく、システム全体は正常に稼働している。

・ミスヒットで見えてしまった他の志願者や学校管理者のキャッシュ上の情報からその実データへアクセスしようとしても、インターネット出願システムそのものへの権限外のログインは拒否されることから、実データの漏洩等に繋がることはなかった。

・インターネット出願システムにログインして出願手続き等の作業をしていた志願者及び学校管理者の閲覧情報は、キャッシュ機能が有効中は一時的にキャッシュに格納されることから、インシデント発生時間内（キャッシュ機能が有効中）にログインした人の情報が閲覧された可能性があるとして被害対象範囲を特定した。

・対象者は、事故直後においては志願者数 292 名（所属学校数 60 校）、学校管理者数 66 名（学校数 60 校）としていたが、その後ログイン時間やログイン状況を考慮して 10 月 30 日には志願者数 291 名（所属学校数 59 校）、学校管理者数 48 名（学校数 41 校）を対象範囲として各利用者（学校）に連絡した。なお、その後より詳細のログ情報から対象者を精査した結果、一部にリストアップ漏れ等が発見されていることから、より正確な対象者の絞り込みを現在実施しており、11 月 13 日の週の前半には各利用者（学校）に再度連絡する予定でいる。

・CloudFront のキャッシュ機能で、誰のキャッシュ情報を誰が閲覧したかを追うことは難しいと AWS から回答があり、本件は被害の可能性がある範囲の絞り込みしかできないと考えている。

・CloudFront のキャッシュ機能でミスヒットに繋がったと思われるケースは、すでにログインしている状態で再読み込みを行った場合のような特定条件下でのアクセス等であると想定しており、数的に限られるものと考えている。

・本件は、個人情報保護委員会規則第 7 条の各号該当性に非該当（理由：第 4 項の千人を超えない為）であり、法的な届出の義務は USS 社、CB ラボ社、利用者（学校）ともにないとのことで、告知についても任意であるとの回答を得ている。

・USS 社は 2023 年 11 月 13 日以降にホームページで本件の告知を行う予定で、その内容は追って各利用者（学校）に案内する。

・対策本部では、本件インシデントでマイページ等を閲覧された可能性のある志願者に対し、その事故内容説明書と謝罪文、お詫びとして QUO カード 1,000 円の送付を予定しているが、その方法等については各利用者（学校）に相談の上連携して行う。

【詳細】

1．インシデントの発生と対応、当日の背景等の時系列事実

1）保守作業の実施

・ 2023 年 10 月 26 日（木）11 時 00 分～11 時 30 分

臨時保守として、悪意あるサイバー攻撃からシステム（データやアプリケーション）を守るための AWS WAF の再設定を行い、CloudFront のキャッシュ機能を有効にした。

2）インシデント報告

・ 2023 年 10 月 26 日（木）13 時 15 分頃

志願者より「自分のマイページを閲覧しようとしたら他の志願者のマイページが見えた」との報告が、志願先の学校を通じて USS 社事務局にあった。

・ 2023 年 10 月 26 日（木）15 時 15 分頃

2 校の学校管理者より「自校の学校管理画面を閲覧しようとしたら他校の学校管理画面が見えた」との報告が USS 社事務局にあった。

・ 2023 年 10 月 26 日（木）15 時 15 分頃

志願者より「自分のマイページを閲覧しようとしたら他の志願者 2 人のマイページが見えた」との報告が、志願先の学校を通じて USS 社事務局にあった。

3）復旧作業

・ 2023 年 10 月 26 日（木）15 時 41 分

AWS WAF の CloudFront のキャッシュ機能の有効設定が原因である可能性が大きいとして設定を無効にした。

2．インシデントの特定を行う作業

1）内容整理

学校や志願者からのインシデント報告をもとに、CB ラボ社と USS 社で本件を下記のように整理した。

・ 志願者が自分のマイページ等にアクセスしようとした時に、他の志願者（異なる学校の志願者を含む）のマイページ等が閲覧できてしまうという事態が発生することがあった。

・ 学校管理者が自分の出願管理画面にアクセスしようとした時に、他の学校管理者の出願管理画面が閲覧できてしまうという事態が発生することがあった。

2）事態発生の原因の整理

サービス運用環境の変更等で本件不具合の発生につながりそうな状況について、CB ラボ社技術者と USS 社代表とで整理した。（2023 年 10 月 26 日 15 時頃　電話）

・ USS 社インターネット出願システムにおいて、サーバーやデータベースからの情報漏洩や、アプリケーションに怪しい挙動が見られなかったこと。

・ 本件の事故を引き起こすようなアプリケーションの改修作業は行なっていないこと。

・ 今年度 5 月に AWS WAF の CloudFront のキャッシュ機能を無効にした状態で運用したことがあり、その際には今回のような事故が発生していないこと。（決済業社から送られる情報の取り込みの一部に不具合が発生したために一旦 AWS WAF と CloudFront の運用を停止して、今回その改修が完了したことから再設定を行った）

3）インシデントの原因の排除

2023 年 10 月 26 日 15 時 30 分頃に、本件の原因が USS 社インターネット出願システムシステム運用上のサーバーやデータベースにおける不具合である可能性が非常に小さいこと、AWS WAF と CloudFront の導入が原因である可能性が大きいと判断して、15 時 41 分に CloudFront のキャッシュ機能を無効に設定した。

その後、事故報告は無くなった。

キャッシュ機能を無効に設定し直したことで、マイページの個人情報や学校管理画面がキャッシュに上がることがなくなったことから、他人から見られるキャッシュへのミスヒットそのものがなくなり、他から閲覧される可能性があるという不具合は解消したと 16 時頃に判断した。

4）インシデント発生時間

保守作業を開始した 2023 年 10 月 26 日（木）11 時 00 分から、CloudFront のキャッシュ機能を無効にした 15 時 41 分までの間とした。

なお、AWS WAF とキャッシュ機能を有効にした CloudFront の運用開始後に、USS 社においてのテストログインを 11 時 44 分と 11 時 50 分に行っているが、その際は全く正常に動作しているので、キャッシュ機能は正常に動作していた事例もあったことを申し述べておきたい。

3．インシデント発生後の対応

1）被害の範囲特定

インターネット上のキャッシュ情報へのミスヒットにより引き起こされている現象であることから、インシデント発生時間内にキャッシュに情報が上がっていた志願者マイページ及び学校管理画面が他者に閲覧された可能性があるとして、インシデント発生時間内に USS 社インターネット出願システムのサーバーへログインした志願者及び学校管理者のメールアドレスと時間情報を、サーバーへのアクセスログ情報から抽出した。（CB ラボ社：2023 年 10 月 26 日 20 時以降）

2）CB ラボ社と USS 社との情報共有

本件事故に関わる情報の共有を CB ラボ社と USS 社で行った。

・ 第 1 回リモート会議（2023 年 10 月 27 日 9 時 00 分から 10 時 00 分）

事故内容及びそれへの対応、被害範囲の特定等について情報共有を行った。

・ レポート

インシデント発生内容と対応についての内部報告、インシデント発生時間（少し範囲を広げた時間を含む）内での志願者ログイン情報を共有した。（10 月 27 日 9 時 49 分）

・ レポート

インシデント発生時間内の学校管理者ログイン情報を共有した。（10 月 27 日 13 時 54 分）

・ 第 2 回リモート会議（2023 年 10 月 27 日 15 時 00 分から 16 時 00 分）

ログ情報の分析から分かったこと、今後の調査の方向性について情報共有を行った。

・ 第 3 回リモート会議（2023 年 10 月 30 日 10 時 00 分から 10 時 30 分）
対策本部の設置と役割分担を行った。
ログ情報から分かったことについて情報共有を行った。

・ 第 4 回リモート会議（2023 年 10 月 31 日 14 時 00 分から 14 時 30 分）
引き続きログ情報から分かったことについて情報共有を行った。

・ 第 5 回リモート会議（2023 年 11 月 2 日 15 時 00 分から 16 時 00 分）
原因究明につながる個別情報についての考察と今後の調査の方向性について情報共有を行った。

・ レポート
インシデント発生時間内の学校管理者ログイン情報（更新版）を共有した。（11 月 2 日 15 時 33 分

・ 第 6 回リモート会議（2023 年 11 月 6 日 10 時 30 分から 11 時 00 分）
今後 USS 社が行う対応及び CB ラボ社が行う資料収集と提供について打ち合わせた。

本件事故で利用者（学校）の個別の調査依頼及びその結果の共有を CB ラボ社と USS 社で行った。

・ 2023 年 10 月 27 日から随時必要に応じて Chatwork を通じて利用者（学校）からの個別の調査依頼及びその回答、質疑応答の内容を共有した。

3）USS 社からの各利用者（学校）への報告

CB ラボ社からの提供情報をもとに、本件事故の概要や学校別資料を作成して、該当校へメールで報告するとともに、必要に応じて電話やリモート会議で説明等を行った。

・ マイページ情報等がキャッシュに上がってしまって他の志願者から閲覧が可能であったと思われる志願者が 10 名以上存在する利用者（学校）に対して、その対象者リスト（メールアドレスとログイン時間）をメールで報告し、電話でわかる範囲の状況説明を行った。（10 月 27 日 15 時から順次）

・ マイページ情報等がキャッシュに上がってしまって他の志願者から閲覧が可能であったと思われる志願者が存在する利用者（学校）に、その時点で判明している全体の状況を書面にしてメール添付で送付した。（10 月 30 日 18 時 33 分頃）

・ マイページ情報及び学校管理画面等がキャッシュに上がってしまって他の志願者や学校管理者から閲覧が可能であったと思われる志願者や学校管理者が存在する利用者（学校）に、利用者（学校）別の対象者リスト（メールアドレスとログイン時間）と学校管理者（メールアドレスとログイン時間）を記載した文書を作成しメール添付で送付した。（10 月 31 日 18 時 10 分以降に順次）

・ マイページ情報等がキャッシュに上がってしまって他の志願者から閲覧が可能であったと思われる志願者が存在する利用者（学校）に、利用者（学校）別の対象者リスト（メールアドレスとログイン時間）を記載した文書を作成しメール添付で送付した。（10 月 31 日 18 時 10 分以降に順次）

・ 学校管理画面等がキャッシュに上がってしまって他の学校から閲覧が可能であったと思われる利用者（学校）に、その時点で判明している全体の状況と学校管理者（メールアドレスとログイン時間）を記載した文書を作成しメール添付で送付した。(10 月 31 日 18 時 30 分以降に順次)

・ インターネット出願システム利用校で本件事故での対象者が存在しない利用者（学校）に本件事故発生の報告をメールで行った。(11 月 7 日 17 時 39 分)

4）各利用者（学校）の個別質問への対応

USS 社からの報告に対して各利用者（学校）から寄せられた質問メールや問い合わせ電話に、都度対応を行った。(10 月 27 日 15 時以降　現在に至る)。

5）法的な報告

個人情報保護法に基づく初期報告を行った。

・ 10 月 27 日午前に個人情報保護委員会に CB ラボ社より報告書を提出した。内容は、事実経過と初期対応が中心であった。

本件について USS 社、CB ラボ社及び利用者（学校）の対応等について個人情報保護委員会にヒアリングした。(11 月 2 日)

・ 本件は、個人情報保護委員会規則第 7 条各号該当性に非該当（非該当となる理由：規則第 7 条第 4 項の千人を超えない為）であり、法的な届出の義務は USS 社、CB ラボ社、利用者（学校）ともにないとのことで、告知についても任意であるとの回答を得ている。

6）事故の原因追求

CloudFront キャッシュへのヒット情報が収集できるかどうかについて AWS へ問い合わせた。(10 月 30 日 11 時 32 分)

以下 AWS からの回答（10 月 30 日 16 時 18 分）

要約：アクセスを行った利用者がどの利用者の情報にヒットしたのかを追跡する有効な手段はない。

アクセスを行った利用者がどの利用者の情報にヒットしたのかを追跡する有効な手段はございません。もし現在もキャッシュが残っている状態であれば、同様のリクエストを再現することでキャッシュがどの利用者の情報であるかは確認できる可能性がございます。 しかし、もし残っていたとしてもそのキャッシュが事象発生時のものかは特定できず、追跡は困難であると考えております。

CloudFront キャッシュへのミスヒットが生じる可能性があるアクセス方法について AWS に問い合わせを行う。(11 月 1 日 19 時 43 分)

以下 AWS からの回答(11 月 2 日 17 時 25 分)

要約：CloudFront のキャッシュに関する内部アルゴリズムについての詳細は案内できない。

CloudFront のキャッシュ動作について、どのような制御が行われているものかご質問を承りました。内部情報についてはご案内を差し上げることができません。CloudFront では最

低でも 1 秒間はオブジェクト（HTML に限りません）がキャッシュされることを想定しておりますが、CloudFront としてはその 1 秒を待たずにキャッシュの削除を行う可能性がございます。

【今後の対策本部で対応する内容とスケジュール】

① 利用者（学校）様ごとに、マイページを閲覧された可能性のある志願者のログイン情報を精査し、最終確定版としてメールアドレスとログイン時間を整理して通知します。（11 月 13 日から順次）
② 利用者（学校）様ごとに、閲覧された可能性のある学校管理画面を操作した学校管理者のログイン情報を精査し、最終確定版として学校管理者メールアドレスとログイン時間を整理して通知します。（11 月 13 日から順次）
③ 利用者（学校）様ごとに、連携・相談しながらマイページを閲覧された可能性のある志願者に対して状況説明・謝罪文とお詫びの QUO カードの送付を行います。（11 月 20 日から順次）
④ CB ラボ社主導で原因の追求と再発防止のための技術検討を継続して行います。

【本件お問い合わせ先】

株式会社ユニバーサル・サポート・システムズ
代表取締役　　岡山保美
インターネット出願システム担当
阿部　衣川
＜お問い合わせ先＞　06-6765-8010
info@uss-cc.co.jp