e-ラーニングシステム（manabie：マナビー）
不正アクセス報告書

令和 6 年 7 月 31 日

長崎県立大学

1. はじめに

本報告書は、長崎県立大学（以下、本学と称する。）において令和 5 年 8 月 4 日に判明した e-ラーニングシステム（manabie：マナビー：以下、本システムと呼びます。）の不正アクセス（以下、本件と称する。）に関する経過と、痕跡調査の結果および今後の対策についてまとめたものです。

2. 本件の経過

以下、本件の経過を概説します。

① 令和 5 年 8 月 4 日、本学の公式ホームページを通じて、本システムが第三者による不正アクセスを受けているとの情報提供がありました。本システムは、本学の全学教育科目「しまなび」プログラムにおいて、平成 26 年から利用しているものであり、学生（卒業生含む）・教員・地域連携者（計約 6,500 人分）の以下の個人情報が含まれていました。

「氏名」、「性別」、「電話番号」、「メールアドレス」、「パスワード」、
「学籍番号」、「本システムに関連する特定科目の成績または評価指標」

② 同日、本システムを開発した委託業者の協力のもと、関係する教職員で直ちにネットワークを切断するなどの初動対応をするとともに、大学幹部にも情報共有しました。

③ 8 月 8 日、本件は個人情報漏えいリスクがありうると判断し、学内に学長をトップとする不正アクセス対応チームを設置し、対応を開始しました。

④ 8 月 9 日および 10 日、情報を整理の上、関係部署（文部科学省、情報処理推進機構、個人情報保護委員会、長崎県警察本部、長崎県）に連絡し、その後も適宜、情報提供しました。

⑤ 8 月 22 日、本学ホームページとメールを用いて、個人情報漏えいのおそれがあることを在校生および卒業生に連絡しました。

⑥ 8 月 31 日、外部調査機関に不正アクセスの詳細と情報漏えいを示唆する痕跡調査（フォレンジック調査）を依頼しました。調査の結果、不正アクセスの直接原因は、本システムで使用しているオープンソースの e-ラーニングプラットフォーム「Chamilo」の脆弱性を悪用されたことと判明しました。詳細は、本報告書の第 3 章

をご参照ください。

⑦　11 月 29 日～令和 6 年 2 月 26 日、外部調査機関に依頼してインターネットに接続する学内のサーバーやネットワーク機器の脆弱性診断（プラットフォームの診断と、Web アプリの診断の両方）を実施しました。

⑧　令和 6 年 3 月、本システムを廃棄しました。廃棄前には、本システム上の「講義に使用していた資料」および「発表会動画、発表会資料」の PDF データ・動画データを DVD 等へ保存しました。令和 5 年度の授業において、本システムを利用していた「しまなび」プログラムは、Google アプリ（ドライブ、ドキュメント、スプレッドシート等）やオリジナルテキストを利用して実施しました。また、「しまなび」の新システムについては、令和 6 年度の授業の中で必要性を検証します。

3．痕跡調査（フォレンジック調査）結果

以下、２章⑥で述べた痕跡調査（フォレンジック調査）結果の概要を説明します。

【不正アクセスの直接原因】

・不正アクセスの直接原因は、本システムに使われていたオープンソースの e-ラーニングプラットフォーム「Chamilo」の脆弱性を悪用されたことです。
・「Chamilo」の脆弱性は、令和 5 年 8 月 1 日に CVE-2023-34960 として公開されているものです。本脆弱性を利用すると、攻撃者は遠隔から任意のコマンドを実行することが可能となります。

【不正アクセスの内容】

・令和 5 年 8 月 3 日 13 時前後に、上記 Chamilo の脆弱性を利用して、外部に公開するデータを格納している場所に以下２つのファイルが設置されました。
  (1) readme.txt：readme.txt には、インドネシア語で「ハッキングした」という意味の文章が記述されていました。
  (2) 404.php：404.php は、攻撃者がブラウザからシステムを操作するプログラムであり、(1)の readme.txt を設置するために使用されたと考えられます。
・上記２つのファイルの設置については、海外のハッカーフォーラムと思われる Web サイトに掲載されていました。

【不正アクセスの影響範囲】

・調査した範囲においては、情報漏えい等の痕跡は確認されませんでした。しかし、システムの設定ミスでデータベースのログが取得されておらず、詳細の調査ができなかったため、漏えいがなかったとは言い切れません。

4. 今後の対策

本件の要因を踏まえ、下記のとおり今後、同様の事例を発生させないための対策を実施します。なお、実施にあたっては、優先度を決めて計画的に進めます。

【既に実施済みの対策】

（ア）脆弱性情報収集と定期的な脆弱性診断

早期にシステムの脆弱性を発見して対処するためには、複数のルートで公開されている脆弱性情報を収集し、その脆弱性が本学システムに関係あるかどうかのチェックが重要です。しかしながら、今までは十分ではありませんでした。

このため、令和 5 年度には、本件の発生以前から実施していた定期的なプラットフォーム診断に加え、Web アプリ診断を実施しました。今後も継続的、定期的に同様の診断を実施していく予定です。

【今後実施する対策】

（イ）委託契約スキームの見直し及び委託業者の監督

不正アクセスの原因を分析し適切に対策するためには、システムの利用状況やデータ通信などの履歴記録（アクセスログ、ユーザの活動、システムパフォーマンスなど）の取得が必須です。しかしながら、本件においては、本システムで使用されているデータベースは、システムの設定ミスで、履歴記録ファイルが出力されない設定になっていました。また、本システムを見直すことなく、本学が長期にわたり委託業者に任せきりであったことは一番の問題と考えています。

今後は、類似の委託契約時に、適切なシステム設定を含むセキュリティ項目をシステム要件の契約書類に具体的に明示するよう見直します。また、委託業者の情報セキュリティマネジメントシステムの認証取得を求めるなどの委託契約スキームの見直しを行います。そして、本学が責任をもって適切にシステムを点検し、委託業者とともに PDCA サイクルを循環してセキュリティの品質を維持向上します。

（ウ）不正行為の発生を想定した適切な体制づくり

本件においては、不正アクセスの発生当日に委託業者との連絡窓口が一本化されておらず、初動対応の際の十分な指示ができず、不正アクセスやその影響の痕跡が保全され

ませんでした。このため、不正アクセスの侵入経路の解析等の痕跡調査（フォレンジック調査）に影響が生じました。

本学では、インシデント発生時の初動マニュアルが整備されておらず、不正アクセスが生じたときの担当者の対応などの徹底も不十分でした。

また、いわゆる CSIRT（日頃から脆弱性情報をチェックし、インシデントの際の対応の中心となる機能）の体制が十分に整備されていませんでした。

今回のようなサイバー攻撃は、できうる限りの万全の防御対策は施す一方、100%避けることはできないものもあることを想定し、今後、万が一不正アクセスが発生した場合においても、できるだけ早期に発見し、適切に対応して早期に回復することが重要と考えます。初動マニュアルや本学に適した CSIRT の体制について検討、整備します。

（エ）実効性のある情報セキュリティに関する教育・訓練

情報セキュリティについては、組織全員での意識改革と取り組みが重要と考えています。全教職員に対して現状実施している基礎的な情報セキュリティ教育に加え、今後は、e-ラーニングなどによりさらに知識を習得する教育や、例えば標的型攻撃メールへの対応訓練や、前述の初動マニュアルに沿った訓練など、より実効性のある情報セキュリティ訓練を実施するなど、継続した教育を徹底します。

（オ）適切な予算と人員の確保

以上のような適切なセキュリティ運用を行うための対策について、継続的に実施できるよう、予算や人員の確保についても努めます。

5. おわりに

この度の不正アクセスにおいて、関係する皆様に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。今回の事態を重く受け止め、必要な対策を講じ、再発防止に努めてまいります。