

不正アクセスによるサーバ障害の発生とそれに関するお知らせとお詫び

2024年03月15日

株式会社エル・インターフェース（以下、「弊社」といいます。）は2023年12月および2024年1月に弊社顧客（スーパー英語 AcademicExpress3 導入校）からのご指摘で、弊社が保守を受託しているサーバに対し、第三者からの不正アクセス攻撃をうけていることを確認いたしました。

詳細を確認いたしましたところ、当社および、弊社顧客の契約するセキュリティ診断組織から弊社製品導入時に使用しているミドルウェア（Adobe ColdFusion）の脆弱性の問題への攻撃を起点としていることがわかりました。現時点では、不正アクセスより、利用しているサーバへのDBアクセスの可能性あり、受講者の学籍番号、氏名、所属組織名などの個人情報漏洩した可能性もあるものとしてお知らせいたします。なお、不正アクセスを受けたサーバでは上記以外に学習履歴情報が含まれておりますが、現段階では、これらが改竄や消去された状況は確認できておりません。

お客様をはじめ、関係者の皆様には多大なご迷惑とご心配をおかけすることになり、深くお詫び申し上げます。

以下に、本件の詳細及び、対応について記載させていただきます。

1. 発覚の経緯及びこれまでの対応

2023年12月弊社顧客の契約するセキュリティ診断組織より、弊社顧客へAE3のサーバから不正に発信されたリクエスト情報から他のサーバが攻撃をうけている形跡があるとの情報提供を受け、該当のサーバを調査したところ、弊社が提供していないプログラムソースがWebサーバ上に配置され、利用されていることを確認いたしました。

類似の事象が2024年1月にも別の学校様より報告を受けています。

本件発覚後、弊社及びお客様の窓口と協力し、サーバの隔離と被害の状況調査および原因調査をおこないました。

調査においては

- ・外部の第三者による侵入経路の特定
 - ・不正アクセスの影響を受けた機器等の特定
 - ・侵害状況および流出の恐れがある情報の範囲の特定
- を実施しました。

2. 漏えいの恐れがある個人情報

これまでの調査では、お客様の情報を利用した二次被害の報告は受けておりませんが、漏洩の恐れがある情報は以下の通りです。引き続き調査を行い、新たな漏えいの事実が判明した場合には、速やかに対応してまいります。

- ・お客様の学籍番号（ログインID）、氏名、所属番号、（一部メールアドレス）

3. 被害の対象となるお客様へ

対象となるサーバについては、バックアップ等を利用して復旧を行っておりますが、心当たりのない履歴や、個人情報の変化などお気づきの点がありましたら、弊社事務局までご連絡ください。

4. 今後の対策と再発防止策

今回の事態を重く受け止め、以後このような事態が再び発生しないよう、引き続き顧客窓口や、専門家等の助言をもとに、以下の点について取り組んでまいります。

- ・脆弱性管理の徹底
- ・適切なIT運営や体制の見直し
- ・製品サイクルに対する顧客との事前調整

5. お客様、お取引様先への対応

脆弱性の対象となるシステムに関しては、専用の窓口を通じて、メールや電話等を通じて、個別にご連絡させていただきます。可能な限り個別に対応を進めてまいります。ご連絡できない方々へは、本発表をもって、通知とさせていただきます。

この度は、皆様に多大なるご迷惑ご心配をおかけしますこと、あらためて深くお詫び申し上げます。

<本件に関するお問い合わせ窓口>

東京都渋谷区千駄ヶ谷5丁目18番20号 代々木フォレストビル8F

株式会社エル・インターフェース ITシステム(ISMS)担当

■メール : info@l-interface.co.jp

■電話番号 : 03-5312-6101 (受付時間: 平日 10:00 から 18:00、土日祝日除く)