不正アクセスによる「情報セキュリティ理解度チェックサービス」からの利用者個人情報漏えいの恐れに関するお知らせ（第一報）

2026 年 11 月 4 日、当協会が運営する情報セキュリティ理解度チェックサービスにおいて、第三者による不正アクセスを受けたことを確認いたしました。

この不正アクセスにより、利用者の個人情報の漏えいが発生した可能性があり、対象者は最大 15,128 件と見込まれております。漏えいしたと見込まれる情報はこれまで管理者登録された方および利用ユーザの以下の情報です。※

１．管理者氏名
２．管理者企業名
３．管理者メールアドレス
４．組織所在地、従業員数、業種
５．利用ユーザ数
６．利用者の ID/PW（パスワードはハッシュ化されています）

現在も調査を継続しており、対象件数や影響範囲については今後変動する可能性があります。
漏えいの可能性が確認された利用者の皆様には、対象者の特定が完了次第、個別にご連絡を差し上げる予定です。

本件の発覚後、被害拡大防止のため対象サービスを停止するとともに、外部専門事業者の協力のもと、原因究明および影響範囲の特定を進めております。
現在の調査では、不正アクセスは 2026 年 10 月 30 日夜頃から行われた可能性があることが判明しております。なお、詳細な侵入経路および影響範囲については、引き続き調査を進めております。

本来、日本のセキュリティレベルを向上させるべき協会でありながら、このような不正アクセスを受け、ご利用の皆様をはじめ、関係者の皆様に多大なるご心配とご迷惑をおかけしておりますことを深くお詫び申し上げます。

今後、調査の進展により新たな事実が判明した場合は、当協会 Web サイトにて速やかにお知らせいたします。
なお、メールアドレス等の情報が漏えいした場合、当協会や関係機関になりすましたメールが送信される可能性があります。不審なメールを受信した場合は、メール本文中のリンクや

添付ファイルを開かず、送信元を十分にご確認くださいますようお願いいたします。
また、当協会がメール本文中で URL リンクを示して、ID やパスワードの入力や変更を求めることはありません。 パスワードの入力や変更を求めるメールを受信した場合は、十分にご注意ください。

本件につきましては、11 月 6 日に個人情報保護委員会に報告を予定しております。

2026 年 11 月 6 日
特定非営利活動法人日本ネットワークセキュリティ協会
（お問合せ先：sec@jnsa.org）

※（参考）JNSA セキュリティ理解度チェック管理者とは、社員や職員のセキュリティモラル・リテラシーの向上、および組織全体の客観的な知識レベルを把握する目的で、組織の管理者が事前に受講者（社員・職員）を登録し、サイト上で情報セキュリティに関する問題を受講させて、結果を分析できるサービスです。管理者以外の受講者は、個人名を使わずに「受講者 ID」などで管理できます。