各位

2026 年 11 月 2 日

会 社 名　株式会社トレードワークス
代表者名　代表取締役社長　齋藤　正勝
（コード番号：3997　東証スタンダード）
問合せ先　取締役　徳島　直哉
（TEL. 03-6230-8900）

（開示事項の経過）当社が提供するシステムへの不正アクセスに関するお知らせ（第 3 報）

当社が岩井コスモ証券株式会社（以下「同社」）に提供するインターネット取引システムへの不正アクセスにつきましては、2026 年 10 月 16 日付および 10 月 23 日付でお知らせしております。

このたび、本件の原因および影響についてこれまでに確認した事実、事案後の対応状況ならびに今後の取り組みを取りまとめましたので、下記のとおりお知らせいたします。

同社のお客様をはじめ、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、改めて深くお詫び申し上げます。

記

1. 本件の概要

・原因

10 月 16 日付および 10 月 23 日付でお知らせしたとおり、同社向けシステムの一部の管理機能の設定上の不備により、本来は限定された環境からのみ利用されるべき機能が外部から利用できる状態となっていたことが原因です。これは、当社の設計および運用管理が不十分であったことによるものと認識しております。

・影響

10 月 23 日付でお知らせしたとおり、同社のお客様の一部の口座において意図しない売買注文が成立しましたが、同日中に取引前の状態に復元されており、お客様に金銭的なご負担は生じておりません。また、同じく 10 月 23 日付でお知らせしたとおり、同社のお客様 4,975 名の氏名、メールアドレス等の情報が漏えいした可能性があることを確認いたしました。なお、これらの情報のみでは、お客様の口座へのログインや売買及び出金、情報の変更を行うことはできない仕組みとなっております。お客様の資金の不正な流出、およびシステム内部への侵入の痕跡は確認されておりません。

・他のシステムへの影響

当社が他の金融機関向けに提供しているシステムについても点検し、必要な対策を講じるとともに、同社向けシステムと同様の強化策を併せて実施しております。他の提供先において、本件と同様の事象は確認されておりません。

2. 事案後の対応状況

当社は、事案発生直後から連日、全社を挙げて同社向けシステムの対策に着手し、他の金融機関向けのシステムにも展開して、継続して強化しております。

区分	実施した対策
封じ込め	本件の経路となった管理機能の外部からの利用を遮断。対策本部を設置
総点検（外部公開経路）	インターネットから到達可能な経路を点検し、防御機能を経由しない迂回経路を閉塞
専門部門による診断	当社の専門部門による、本番環境に対するペネトレーションテスト、およびプログラムソースコードと環境設定の組み合わせを含めた複合的診断を実施
防御ルールの強化	攻撃的な通信を遮断する防御ルールの強化、国・地域別のアクセス制御の見直し・強化
ログイン保護・経路の多層化	ログイン時に正規の通信であることを確認する仕組みの追加と、管理機能への経路の多層化
監視・証跡	攻撃者のアクセスを監視する専用システムを構築し、横断的な監視と不審なログイン試行の通知を導入。操作記録は改変・削除できない設定で保全
体制・報告基準	当番体制と、不審なアクセスを検知した際の報告基準（検知から 5 分以内の連絡、15 分以内の判断）の運用開始
他金融機関向けシステムの点検・強化	当社が他の金融機関向けに提供しているシステムについて、同社向けシステムと同様の点検と強化策を実施

・当社が他の金融機関向けに提供しているシステムにつきましても、同社向けシステムと同水準の点検を継続的に行う体制を整えております。現時点において、いずれのシステムも通常どおり稼働しております。

・事案後も国内外から攻撃的な通信が観測されておりますが、いずれも防御の仕組みにより遮断・拒否しており、新たな被害は確認されておりません。引き続き、同社をはじめとする提供先と連携し、監視と防御を継続してまいります。

・なお、当社は、同社が行う関係当局への報告および説明に協力しております。また、警察に相談のうえ、その捜査に協力しております。

3. サイバー脅威の高度化に対する当社の取り組み

生成 AI をはじめとする先端的な AI（フロンティア AI）の悪用により、脆弱性の探索から攻撃の実行までが自動化・高速化し、金融分野を標的とするサイバー攻撃は、質・量ともに高度化しております。2026 年 5 月には、金融庁および日本銀行から金融機関等に対し、フロンティア AI による脅威の変化を踏まえた対応が要請されております。

当社は、本件をはじめとする一連のサイバー攻撃への対応の経験を通じて、基本的な対策を確実に固めることと、侵入を前提とした検知・封じ込め・証跡の確保の両輪で取り組むことが不可欠であると認識しております。金融機関に取引システムを提供する事業者として、次の考え方に基づき、当社が提供するシステム全体の防御の水準を引き上げてまいります。

・基本対策の徹底

社内・社外の区別なく、すべてのアクセスをその都度検証し、管理機能などの特権的な機能は多要素認証と必要最小限の権限で保護します。あわせて、外部から到達可能な資産の継続的な管理、脆

弱性の評価から修正までの期限管理、企画・設計段階からのセキュリティの確保（セキュリティ・バイ・デザイン）を徹底します。

・侵入を前提とした検知・封じ込め・証跡

多層防御に加え、振る舞いの監視による予兆の早期検知、封じ込め・復旧の手順の整備と提供先との合同訓練を進めるとともに、操作記録を改変できない形で保全し、説明責任を果たせる体制を整えます。

4. 今後の強化策

本件を契機として、当社は次の 3 点を基本線として強化策に取り組みます。同社向けシステムの安全性を確実に担保すると同時に、当社のシステムをご利用いただいている皆様、ならびにご採用をご検討いただいている皆様に、安心してご利用いただける体制を構築してまいります。

（1）社内リスクマネジメント関連組織の統合・強化

システムリスク、情報セキュリティなどのリスク管理に関する社内の委員会・組織を統合し、サイバー攻撃の高度化に対応する実践的な体制とします。本件で設置した対策本部の機能を常設化し、全社のリスクを一元的に把握・管理します。

（2）監視と報告基準の標準運用の展開

高度なサイバー攻撃を前提として、当社が提供するすべてのシステムを対象に、毎時の監視と報告基準（検知から 5 分以内の連絡、15 分以内の判断）の標準運用を展開します。

（3）セキュリティ水準の標準化とモニタリングの強化

多要素認証の適用、権限の最小化など、本件を踏まえた対策を当社製品の標準構成とし、すべての提供先に展開します。あわせて、不審な通信や攻撃の予兆を早期に捉えるモニタリングを強化します。

あわせて、同社が行う関係当局への報告および説明に全面的に協力し、そこで明らかになる課題を踏まえて、抜本的な再発防止策を講じてまいります。上記の 3 点はその基本線であり、再発防止策の策定と実行に、経営として責任をもって取り組んでまいります。

5. 業績への影響

・本件に伴う損失の見込額は、10 月 23 日付でお知らせしたとおり約 50 百万円（確定した額ではありません）です。なお、当社が加入するサイバー保険について、保険会社所定の手続を進めております。

・業績への影響につきましては現在精査中であり、現時点では通期連結業績予想の修正は行っておりません。今後、開示すべき事項が判明した場合には速やかにお知らせいたします。

6. 今後について

本件の詳細につきましては同社と引き続き確認を行っており、新たにお伝えすべき事項が生じた場合には、速やかにお知らせいたします。

以上