【別 紙】

（周知文）

オンライン取引サービスを顧客に提供する金融商品取引業者における システムリスク管理態勢の自主点検及び顧客被害の発生状況の確認のお願い

最近、オンライン取引サービスを顧客に提供する金融商品取引業者のシステムに悪意のある第三者が不正にアクセス（ログイン）し、顧客が保有する有価証券を売却・換金し、顧客の預り金を含めて、顧客が予め指定・登録していた銀行預金口座とは別の架空預金口座に向けて不正出金されて顧客が被害を受ける事象や顧客情報の漏えいする事象が複数発生していたことが確認されています[1]。

つきましては、以下の２点について自主点検とご確認をお願いいたします。

１．システムリスク管理態勢の自主点検

こうした事象が増加している現状を踏まえ、改めて、金融庁の「金融商品取引業者等向けの総合的な監督指針」に記載のある、特に以下の項目について、会員各社の皆様の業務規模・特性やリスク度合いに応じて、自主点検をお願いいたします。

会員各社の皆様における自主点検の結果、問題や脆弱性などが認められた場合にはその旨、及びその内容を会員各社でとりまとめ、１か月以内を目途にご連絡をお願いいたします。

「金融商品取引業者等向けの総合的な監督指針」
https://www.fsa.go.jp/common/law/guide/kinyushohin/03.html
III. 監督上の評価項目と諸手続（共通編）
III－２－８　システムリスク管理態勢
(1)主な着眼点
④　情報セキュリティ管理
ハ.　コンピュータシステムの不正使用防止対策、不正アクセス防止対策、コンピュータウィルス等の不正プログラムの侵入防止対策等を実施しているか。
ニ.　金融商品取引業者が責任を負うべき顧客の重要情報を網羅的に洗い出し、把握、管理しているか。

---

[1] 【例１】
「悪意のある第三者による不正アクセスに関するお知らせ」2020 年 9 月 16 日公表
https://www.sbisec.co.jp/ETGate/WPLETmgR001Control?OutSide=on&getFlg=on&burl=search_home&cat1=home&cat2=corporate&dir=corporate&file=irpress/prestory200916_02.html
【例２】
「お客様情報漏洩のお詫びとお知らせ」2020 年 8 月 28 日公表
http://www.comtex.co.jp/pdf/info200828.pdf
【例３】
「個人情報流出についての重要なお知らせ」2020 年 7 月 16 日公表
https://www.home.saxo/ja-jp/campaigns/whatsnew/jul-20200716
「個人情報流出についての重要なお知らせ（続報）」2020 年 7 月 17 日公表
https://www.home.saxo/ja-jp/campaigns/whatsnew/jul-20200717

ヘ．　顧客の重要情報について、以下のような不正アクセス、不正情報取得、情報漏えい等を牽制、防止する仕組みを導入しているか。
・職員の権限に応じて必要な範囲に限定されたアクセス権限の付与
・アクセス記録の保存、検証
・開発担当者と運用担当者の分離、管理者と担当者の分離等の相互牽制体制 等

ト．　機密情報について、暗号化やマスキング等の管理ルールを定めているか。また、暗号化プログラム、暗号鍵、暗号化プログラムの設計書等の管理に関するルールを定めているか。
　なお、「機密情報」とは、暗証番号、パスワード、クレジットカード情報等、顧客に損失が発生する可能性のある情報をいう。

チ．　機密情報の保有・廃棄、アクセス制限、外部持ち出し等について、業務上の必要性を十分に検討し、より厳格な取扱いをしているか。

⑤　サイバーセキュリティ管理

イ．　サイバーセキュリティについて、取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。

ロ．　サイバーセキュリティについて、組織体制の整備、社内規程の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。
・サイバー攻撃に対する監視体制
・サイバー攻撃を受けた際の報告及び広報体制
・組織内 CSIRT（Computer Security Incident Response Team）等の緊急時対応及び早期警戒のための体制
・情報共有機関等を通じた情報収集・共有体制　等

ハ．　サイバー攻撃に備え、入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。
・入口対策（例えば、ファイアウォールの設置、抗ウィルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入 等）
・内部対策（例えば、特権ＩＤ・パスワードの適切な管理、不要なＩＤの削除、特定コマンドの実行監視 等）
・出口対策（例えば、通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断 等）

ニ．　サイバー攻撃を受けた場合に被害の拡大を防止するために、以下のような措置を講じているか。
・攻撃元のＩＰアドレスの特定と遮断
・DDoS 攻撃に対して自動的にアクセスを分散させる機能
・システムの全部又は一部の一時的停止 等

ホ．　システムの脆弱性について、ＯＳの最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。

ヘ．　サイバーセキュリティについて、ネットワークへの侵入検査や脆弱性診断等を活用するなど、セキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。

ト．　インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような取引のリスクに見合った適切な認証方式を導入しているか。
・可変式パスワードや電子証明書などの、固定式のＩＤ・パスワードのみに頼らない認証方式
・取引に利用しているパソコンのブラウザとは別の携帯電話等の機器を用いるなど、複数経路による取引認証
・ハードウェアトークン等でトランザクション署名を行うトランザクション認証

等

チ．インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような業務に応じた不正防止策を講じているか。

・取引時においてウィルス等の検知・駆除が行えるセキュリティ対策ソフトの利用者への提供

・利用者のパソコンのウィルス感染状況を金融商品取引業者側で検知し、警告を発するソフトの導入

・電子証明書をＩＣカード等、取引に利用しているパソコンとは別の媒体・機器へ格納する方式の採用

・不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制の整備 等

リ．サイバー攻撃を想定したコンティンジェンシープランを策定し、訓練や見直しを実施しているか。また、必要に応じて、業界横断的な演習に参加しているか。

ヌ．サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。

⑧ 外部委託管理

ロ．外部委託契約において、外部委託先との役割分担・責任、監査権限、再委託手続、提供されるサービス水準等を定めているか。また、外部委託先の役職員が遵守すべきルールやセキュリティ要件を外部委託先へ提示し、契約書等に明記しているか。

ニ．外部委託した業務（二段階以上の委託を含む）について、委託元として委託業務が適切に行われていることを定期的にモニタリングしているか。

また、外部委託先における顧客データの運用状況を、委託元が監視、追跡できる態勢となっているか。

２．顧客被害の発生状況の確認

冒頭に述べた複数の事象の発生を踏まえ、過去に被害が生じていなかったか可能な限りご確認いただいた上で被害が発覚した場合や、新たに被害が発生した場合には、会員各社から直ちに当局にご一報をお願いします。

また、不正アクセスや顧客情報の漏えいによる被害を心配される利用者から相談や苦情等を受けた場合には、被害の有無に関わらず、利用者の不安を解消すべく、真摯な姿勢で迅速かつ丁寧に対応いただくようお願いします。

以 上