

# 証券会社の不正アクセス防止態勢の高度化支援

2021年3月16日、日本証券業協会は「インターネット取引における不正アクセス等の防止に向けたガイドライン」を公表しました。7つの分野について対応が必要とされている留意事項「スタンダード」と対応することが望ましいとされている留意事項「ベストプラクティス」が策定され、証券会社は未達成事項について対応することが求められています。

あずさ監査法人では、当局指針や関連するフレームワーク、業界におけるベストプラクティス等に関する豊富な知見を基に、証券会社の不正アクセス防止態勢の高度化を支援するアドバイザリーサービスを提供します。

## オンライン証券会社における不正アクセス事案の概要

「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」

—金融庁「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について」（2020年9月7日）\*

\*「顧客情報の漏えい」事案については省略

## 不正アクセス事案の手口と対策の種類

不正アクセス事案の手口		対策の種類
1	証券口座を保有する <b>利用者の情報</b> を不正に入手	入口対策
2	当該利用者名義で架空の銀行口座を開設	
3	出金先の <b>銀行口座を変更</b> し、保有する証券等を <b>売却・換金</b> した上で証券口座から当該架空 <b>銀行口座へ資金を移転</b>	内部・出口対策
4	当該架空銀行口座から不正な出金等	外部事業者との連携
<b>入口対策</b> <ul style="list-style-type: none"> <li>ファイアウォール、スパムフィルター、IDS/IPS（不正侵入検知・防御システム）などのゲートウェイ対策</li> </ul>		<b>内部・出口対策</b> <ul style="list-style-type: none"> <li>内部対策の代表例としては、ログ監視とファイルの暗号化など</li> <li>出口対策の代表例としては、サンドボックス型の標的型攻撃対策やWAFなど</li> </ul>

## 証券会社における不正アクセス防止態勢の構築に係るガイドラインと監督指針



### 日本証券業協会「インターネット取引における不正アクセス等の防止に向けたガイドライン」

口座開設時の本人確認のeKYCの導入、ログイン時の多要素認証と不正アクセスを検出する手法や態勢の整備等を求めています。



### 「金融商品取引業者等向けの総合的な監督指針」

サイバー攻撃に備え、多層防御態勢と外部委託先の定期的なセキュリティモニタリングの態勢整備などを求めています。

## 不正アクセス防止態勢の高度化支援に係るベンチマークおよび不正アクセス防止ガイドラインの項目

ベンチマーク	不正アクセス防止ガイドラインの項目
<ul style="list-style-type: none"><li>不正アクセス等防止に向けたガイドライン</li><li>金融商品取引業者等向けの総合的な監督指針</li></ul>	<ol style="list-style-type: none"><li>1 口座開設、ログイン、取引、出金等</li><li>2 脆弱性対策および情報管理</li><li>3 モニタリング</li><li>4 顧客情報（個人情報）に係る安全管理措置</li><li>5 不正アクセス発生時の対応</li><li>6 公表対応等</li><li>7 その他（社内教育や利用者への通知など）</li></ol>

## 不正アクセス防止に関する方針の策定および規程等の整備支援サービスのご提供例（2ヵ月～4ヵ月）

01 現状把握	02 分析	03 態勢整備
<p>不正アクセス防止等に係る態勢の現状について現状をヒアリングや資料閲覧等を通じて把握します。</p> <ul style="list-style-type: none"><li>ギャップ分析シートの作成</li><li>関連文書、エビデンスの閲覧</li><li>対象プロセスの実態に係るヒアリング</li></ul>	<p>監督指針、ガイドライン等のベンチマーク、他社事例を基にギャップ分析を行います。</p> <ul style="list-style-type: none"><li>現状把握結果とベンチマークの比較</li><li>ギャップ（対応すべき事項）の特定</li><li>課題に対する対応策の提示</li></ul>	<p>ギャップ分析結果に基づく規程等の整備支援および態勢構築に係る助言を提供します。</p> <ul style="list-style-type: none"><li>ギャップ分析結果の取りまとめ</li><li>規程等の整備支援</li><li>態勢高度化に向けた助言の提供</li></ul>

### 有限責任 あずさ監査法人

金融統轄事業部 金融アドバイザリー事業部

保木 健次

Kenji.Hoki@jp.kpmg.com

〒100-8172

東京都千代田区大手町1丁目9番7号

大手町フィナンシャルシティ サウスタワー

home.kpmg/jp/fintech

本リーフレットで紹介するサービスは、公認会計士法、独立性規則及び利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくは有限責任 あずさ監査法人までお問い合わせください。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供できるよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. 22-5095

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.