令和２年 11 月 10 日

電子決済等代行業者　各位

金融庁監督局長
栗田　照久

電子決済等代行業者のセキュリティの高度化等について（要請）

１．経緯

○　電子決済等代行業者が電子決済等代行業を行うにあたり、利用者の銀行口座に対し送金の指図を行うことが可能となるＩＤやパスワード等の認証情報（以下、単に「認証情報」という。）を保有している例があるところ。

○　昨今、悪意のある第三者による不正な出金事案が発生していることも鑑み、電子決済等代行業者においても情報セキュリティ管理態勢を改めて確認し、必要に応じてその高度化を図る必要がある。

○　「主要行等の総合的な監督指針　Ⅸ　電子決済等代行業」においても、サイバー攻撃が日々、高度化・巧妙化していることを踏まえたサイバーセキュリティに係る体制の整備や、他社における不正事案等も参考に、情報セキュリティ管理態勢の PDCA サイクルによる継続的な改善の必要性について記載しているところ。こうしたことに留意し、下記について確認・検討いただきたい。

なお、令和２年９月 14 日、一般社団法人全国銀行協会から「資金移動業者の決済サービス等での不正出金への対応について」が発表されているので、参考にされたい。

（全国銀行協会ＨＰ）　https://www.zenginkyo.or.jp/news/2020/n091401/

２．確認・検討いただきたい事項

① ＡＰＩ接続契約への移行を前提とした暫定的な契約により利用者の認証情報を保有する場合、当該契約の期限に関わらず、可能な限り早急にＡＰＩ接続に移行できるよう取り組むこと。

② 接続契約が暫定的なものであるかどうかに関わらず、利用者の認証情報を保有する場合においては、自社の漏えい防止等の体制の整備状況を改めて確認し、必要に応じて高度化を図ること。

③ 昨今の不正出金事案を踏まえ、電子決済等代行業者がサービス（電子決済等代行業再委託者が存在する場合は当該再委託者におけるサービスも含む）を提供するにあたり、銀行口座との接続を行うプロセスや、自社のサービス全体を通じた一連のプロセスに脆弱性がないか確認すること。

（注）例えば、銀行口座との接続に係る認証に際してワンタイムパスワード等の多要素認証を実施していない場合など、不正に預金者の口座情報を入手した悪意のある第三者が、預金者の関与なしに送金可能なケースは脆弱性があると考えられる。

④ 上記確認により問題や脆弱性が見出だされた場合には、電子決済等代行業者及び銀行が協力し、認証を強化するなどの堅牢な手続きの導入を検討すること。

⑤ 本事案に関して、被害を心配される方からご相談を受けた際には、被害の有無によらず、相談者の不安を解消するべく、真摯な姿勢で迅速かつ丁寧に対応すること。

上記①について、ＡＰＩ接続への移行が完了した場合には当局に連絡いただきたい（当局においても引き続きフォローアップする予定）。

上記②、③の確認により問題や脆弱性が確認された場合には、その旨を直ちに、また、上記④の対応の内容を速やかに当局に連絡いただきたい。

また、過去に被害が生じていなかったか確認いただき、被害が確認された場合や、新たに被害が発生した場合にも、その旨を直ちに当局に連絡いただきたい。

以上