別紙

株式会社 SBI 証券　御中

調査報告書の要旨

令和 3 年 1 月 5 日

第三者委員会

委員長：弁護士　佐藤　明夫
（佐藤総合法律事務所）

委　員：弁護士　安田　博延
（平河町法律事務所）

委　員：　　大河内　貴之
（Secure・Pro 株式会社　代表取締役）

第 1.本件インシデントの概要

令和 2 年 7 月から 9 月にかけて、株式会社 SBI 証券の顧客のアカウント 6 個において、顧客の身に覚えのない銀行口座変更、商品売却及び銀行口座への出金が行われた。そして、顧客が保有するものではない銀行口座へ出金がなされた結果、顧客の資産が不正に引き出されることとなった。

第 2.真因分析

本件の真因としては、以下の要素が挙げられる。

1.不正ログイン防止対策が不十分であったこと
2.不正取引（不正売買・不正口座変更・不正出金）防止対策が不十分であったこと
3.経営層において、不正ログイン及び不正取引に係るリスク認識が正確になされていたとはいえないこと
4.経営層に対し、不正ログイン及び不正取引に係るリスク認識を可能とするような情報のエスカレーションが不十分であったこと
5.システムリスクについて専門的な知見を持って判断できる人材を取締役に登用できていないこと
6.代表者による迅速な判断を行うことを重要視する観点から、社内全般において、報告内容及び議論内容を詳細に可視化する形で記録する運用が不十分であったこと
7.代表者のリーダーシップが強力であり、現場レベルの部署から経営陣に対して議論の土台となるような情報をエスカレーションする意識が不足していたこと
8.CSIRT 室において、現状のシステムリスクに係る提言を行う能力が不足していたこと
9.内部監査担当者において、現状のシステムリスクに係る指摘を行う能力が不足していたこと

別紙

第 3.再発防止策

本件の再発防止策としては、以下の再発防止策が挙げられる。

1.顧客に対する定期的なログインパスワードの変更要請
2.英数字及び記号を含む複雑なパスワードポリシーの設定
3.ログインパスワード入力失敗によるアカウントロックの解除ルールの強化
4.同一 IP アドレスからのログイン失敗に対するアカウントロック
5.ログイン時及び取引時における二段階認証又は二要素認証の導入検討
6.アクセスログの分析の強化
7.登録済みの端末からの不正アクセス防止策の検討
8.ログインパスワードと同一の取引パスワードの登録に係る防止策
9.ログイン時及び取引時における属性行動分析及び不正監視
10.システムリスクについて専門的な知見を持って判断できる人材の登用及び教育
11.経営層へのリスク認識を可能とするような情報のエスカレーション方法の検討
12.社内全般における、報告内容及び議論内容の可視化
13.現場レベルの部署において、経営陣に対して議論の土台となるような情報を積極的にエスカレーションできる雰囲気の醸成
14.CSIRT 室及び内部監査担当部署の体制の拡充
15.取締役会によるシステムリスクに係る対応状況のモニタリングの強化

以上