2021 年 1 月 22 日

各　位

株式会社 SBI 証券

# 悪意のある第三者による不正アクセスに関する調査報告及び再発防止策について

2020 年 9 月 16 日付プレスリリースで公表したとおり、悪意のある第三者の不正アクセスにより、当社がお客さまからお預かりしていた資産が流出する事態が発生いたしました。お客さまをはじめとした当社のステークホルダーの皆さまには多大なご迷惑とご心配をおかけいたしましたことを、改めて深くお詫び申し上げます。

昨今、サイバー攻撃による被害が社会的に増大している中、当社は犯罪行為を許さない姿勢を改めて表明するとともに、そのような犯罪行為を未然に防止することができず、お客さまに重大な被害を発生させてしまったことを深く反省し、本事案についての徹底的な調査・分析、再発防止策の策定及び関係者の社内処分を実施いたしましたので、お知らせいたします。

**目次**



## 1. 本事案の概要

2020 年 7 月から 9 月にかけて、当社の 6 名のお客さまの口座において、お客さまの身に覚えのない出金先の銀行口座変更、有価証券売却及び当該銀行口座への出金が行われました。また、その他の 5 名のお客さまの口座において、不正出金には至らなかったものの、有価証券の売却が不正に行われました。

本件において攻撃者は、当社のメインシステムサイトに対して、何らかのリストを元にログイン試行を繰り返すリスト型アカウントクラッキングの手法により不正ログインを実行したと考えられます。実際に、不正ログインを行った攻撃者が、本事案における被害を受けたお客さまのアカウントに対してアクセスしている IP アドレスから、1,000 以上のアカウントへのログインを試みたことを確認しております。

不正ログインに成功した攻撃者は、出金先銀行口座の変更ページにアクセスし、取引パスワードを入力したうえで、不正に作られたお客さま名義の銀行口座に変更したと考えられます。取引パスワードを入力するにあたっては、複数種類のパスワードの入力試行が複数回なされたものと思われます。そのうえで、攻撃者は、銀行口座への出金ページにアクセスし、同様に取引パスワードを入力したうえで、既に変更を行った銀行口座への出金を実行するに至ったと考えられます。

本事案による被害の状況は、以下のとおりです。

・被害口座数:6 口座

（不正出金には至らなかったものの、有価証券の不正売却が行われたその他の被害口座数:5 口座）

・被害総額:不正出金合計 9,864 万円（ゆうちょ銀行:9,229 万円、三菱 UFJ 銀行:635 万円）

（その他の不正売却合計:7,184 万円）

## 2. 調査の方法

本事案については、社内の内部管理部門やシステム部門による調査のみならず、専門的及び客観的な見地から原因分析及び再発防止策の検討が必要であると判断し、当社と利害関係を有しない外部の専門家から構成される第三者委員会を設置し、調査・報告を受けたほか、サイバーセキュリティ対応に実績のある外部企業による調査も行っております。

調査にあたっては、各種資料、各種アクセスログなどの電子データの分析、当社及びその関係者に対するヒアリング、当社の端末のフォレンジック調査等を実施いたしました。

なお、本事案に関しては、当初発見されたお客さま以外に被害のあったお客さまが存在しないか、お客さまへの直接確認等の方法により社内調査を継続して行っております。また、当社の外部委託先を含む内部者が関与している可能性に関しては、第三者委員会のみならず、サイバーセキュリティ対応に実績のある外部企業に対しフォレンジック分析を含む徹底的な調査を依頼し、現在も調査を継続しております。現時点において、新たに被害のあったお客さまや内部犯行を疑わせる不審な点は発見されておりませんが、万一発見された場合は、捜査当局及び監督当局等に速やかに報告を行うと共に、適切に対応いたします。

【第三者委員会の構成】

| | | |
|---|---|---|
| 委員長 | 佐藤　明夫 | 弁護士　佐藤総合法律事務所代表 |
| | 2003 年に佐藤総合法律事務所を設立。<br>ジャスダック証券取引所コンプライアンス委員長等を歴任。 | |
| 委員 | 安田　博延 | 弁護士　平河町法律事務所代表 |
| | 2004 年に東京高等検察庁検事、2009 年に山口地方検察庁検事正。<br>2010 年に最高検察庁検事。<br>同年弁護士登録を行い、2017 年に平河町法律事務所を設立。 | |
| 委員 | 大河内　貴之 | Secure・Pro 株式会社代表取締役 |
| | PaymentCardForensics 株式会社（現 P.C.F.FRONTEO 株式会社）の設立に参画、また 2013 年より取締役を経て、2014 年に Secure・Pro 株式会社を設立。 | |

【第三者委員会の調査期間】

2020 年 9 月 25 日から 2021 年 1 月 5 日まで

なお、第三者委員会から公表用として受領した報告書は、別紙のとおりです。

## 3. 原因の分析

### イ. オペレーショナルリスク管理態勢上の問題点

当社の取締役会は、内部統制基本方針及びリスク管理規程を制定し、「リスク管理部門は、リスクの定量的・定性的な評価方法を定め、評価する」こと、「リスク管理部門は、リスク管理取組み計画の策定、具体的施策の選定と実施、リスクの状況に関する報告を担う」ことを定めております。

リスク管理総括部署であるリスク管理部門は、リスク管理規程に基づき、オペレーショナルリスク管理規程・同基準及び情報セキュリティ管理規程・同要領を定め、事務事故や内部不正・外部不正行為等から想定されるリスクを特定し(洗い出し)、リスク顕在化の発生可能性と影響度を 5 段階評価して、コントロール後の残余リスクが大きい事象について、社内各部門においてアクションプランを策定し実行することとしております。

今回発生した事故を踏まえ、情報セキュリティリスクを含むオペレーショナルリスク管理態勢を改めて検証した結果、サイバー攻撃などの外部脅威に伴う情報流出リスク等を含む当社にとって重要なオペレーショナルリスク全般について、子会社及び重要な委託先を含む全社的な視点で合理的、整合的かつ最適な方法による洗い出しを行うプロセスが不十分であること、それぞれのリスク特性に見合った定量的・定性的な方法により評価を行うプロセスが不十分であること、そのためリスクが顕在化した場合、当社の財務に及ぼす影響や、風評、将来の事業計画に及ぼす影響などを総体的に捉え、あらかじめ決定したリスク限度の範囲内にリスクをコントロールするプロセスが不十分であることが判明いたしました。具体的な問題点は以下のとおりです。

### ロ. 過去の外部検査機関による検査指摘を踏まえた「システムリスク管理態勢の高度化」への取り組みが十分な水準でない問題

当社が過去に受けた外部検査機関による検査での指摘に対する改善状況報告書において、監査法人に態勢全般のレビューを依頼し、検査指摘の範囲にとどまらないシステムリスク管理態勢の強化に取り組むことを報告しております。

監査法人によるレビューでは、リスクの俯瞰的な視点として、「システムリスクの所在やリスクの大きさが適切に識別されていない。」という評価が行われております。リスク管理プロセスの入り口として重要な「リスクの特定」が適切に実施できていないことが判明し、その後、このレビュー結果を踏まえた「システムリスク管理態勢の高度化」への取り組みを行っておりますが、十分な水準ではありません。

### ハ. 全社的な視点で合理的、整合的かつ最適な方法によりリスクを洗い出すことができない問題

情報セキュリティリスクを含め、当社が晒される重要なリスクを実効的に特定するためには、内部要因及び当社を取り巻く外部要因のうち、とりわけトップリスク及びエマージングリスクの双方を考慮し、全社的な視点で合理的、整合的かつ最適な方法により、リスクを洗い出す必要がありますが、こうしたリスクを洗い出す仕組みを十分に導入していなかったため、網羅的な洗い出しができておりません。

**ニ. リスク顕在化時に財務等に大きな影響を及ぼすリスクが経営陣に十分に伝わっていなかった問題**

金融機関に限らず事業会社が経営の危機に晒される近年の事例の多くは、サイバーアタックや内部不正等オペレーショナルリスクが絡んで発生しております。こうしたことから、経営陣に対するオペレーショナルリスクにかかる報告については、リスクが増大しているカテゴリーはどこなのか、残余リスクが高くより実効的にコントロールを実施すべきリスクは何なのか、またこうしたリスクが顕在化した場合に当社の財務や風評、成長性に及ぼす影響はどの程度であるのかなどを、簡潔で分かりやすい形で的確な経営判断に役立つ資料の作成が求められております。

こうした中、足元のリスク管理委員会におけるオペレーショナルリスク管理に関する報告資料は、事務ミス件数や件数ベースの KRI 資料（全体 50 ページ中 30 ページ）やリスク管理の概要を説明する資料が大半であり、経営陣が重要なリスクに関する検討や意思決定を行うために十分な情報を提供するものとはなっておりません。

こうした情報は、当社にとって重要なオペレーショナルリスクが顕在化した場合に、①重大な損失が発生して損益計算書上の重大な損失等が発生する財務リスクへの影響度、②当社に対する信用や評判が悪化することにより重大な企業価値の毀損につながるレピュテーショナルリスクへの影響度、③今後将来にわたって顧客数や取引数が減少し、重大な成長の停滞が発生する成長性リスクへの影響度を評価できるものとなっていないことから、これらの影響度が大きいリスクを実効的にコントロールすることの重要性が経営陣に十分に伝えられておりません。

**ホ. 新たなリスクや重点的に取り組むべきリスクの管理計画が策定されていない問題**

近年のリスク管理は、現時点では影響は小さいあるいは顕在化していないものの、今後急速に顕在化し、財務、風評及び成長性に大きな影響を及ぼす可能性のあるリスク(エマージングリスク)を早め早めに管理するという「フォワードルッキング」なリスク管理の重要性が増しております。

こうした早期に低減・制御を行う必要のある重点的に取り組むべきリスクについては、年間基本計画を策定して経営陣に報告を行い、その中でシステム開発等コストのかかるものは費用対効果を勘案して経営判断を行う必要があるものの、上記のとおり重要なリスクについて経営判断に資する情報が提供されていないことから、現状ではこうした意思決定を十分に実施できておりません。

**ヘ. 事後的・対症療法的リスク管理となっている問題**

過去の検査で指摘された問題点に対し、当社の対応は、指摘されたとおりに対応し、発生した問題は解決したという形で終了するという事後的・対処療法的リスク管理となっており、指摘事項を踏まえて、顕在化したリスクに対して自主的に原因分析を行うとともに、指摘事項のみならず関連する事項について継続的にフォワードルッキングな視点を持ちつつ改善活動につなげるPDCAサイクルの仕組みが十分にできておりません。

例えば、過去の検査の改善状況報告において、「二要素認証の導入」を含めた検討を行うことを決めておりま

すが、・・・」と報告し、その後の「改善状況等の報告書改善策の対応状況」において、進捗状況を「顧客認証を一元管理することで二要素認証とのインターフェースを設けることが可能になります。2020 年の実装を目指して計画を進めております。」とし、完了予定を「2019 年 6 月末」、進捗を「対応済（2019/6/20）」と報告いたしました。

現在のリスク評価方法では、二要素認証を導入しない場合の将来損失額を適切に評価できておらず、情報セキュリティリスクの顕在化につながる可能性が高かったにも関わらず、対応済みとして報告したことで、その後の報告の対象外になりました。

改善状況報告の際に「検討する」と掲げ「検討した」と回答することで対応が完了したものとして整理したことは、2020 年の実装に向けたシステム開発が当初計画より大きく遅延が生じたことに対して、監視体制の強化や、攻撃のリスクが高い顧客に対する強制的なパスワード変更等の何らかの予防的対策を早期に行うことへの認識が甘くなり、本事案の発生を招く結果となりました。

**ト. 内部監査態勢の問題**

証券業務における内部監査部門の役割は、事後チェック型監査からフォワードルッキング型監査への転換（過去から未来へ）、準拠性監査から経営監査への転換（形式から実質へ）及び部分監査から全体監査への転換（部分から全体へ）を図ることが期待されております。

これを踏まえ、内部監査態勢は、リスクベースかつフォワードルッキングな観点から、組織活動の有効性等についての助言、見識を提供することにより、組織体の価値を高め、保全するという使命を適切に果たすことが必要であり、近年の証券業務を取り巻く内外の急激な環境の変化に応じて、内部監査を高度化していくことが求められております。

こうした中、当社の内部監査態勢は、事務不備監査（規程の準拠性等の表層的な事後チェック）といった限定的な役割に留まっている段階にあります。また、内部監査部門による発見事象の背景や原因の掘り下げが十分に行われておらず、事務ミスや事務不備の指摘が主体となっているため、監査指摘に対する所管部の意識においては、いわゆる「コンプラ疲れ」が見られます。

加えて、人材について、内部監査部門として中長期的な方針は策定しておりません。また、内部監査の品質評価は、形式的である等、PDCA サイクルが確立されておりません。

**チ. 課題**

今回の真因分析を踏まえた当社におけるリスク管理態勢に関する課題は以下のとおりです。

①経営上のリスクの軽重の判断が行える情報提供が必要である
②主要なリスクの網羅的な洗い出しや特定方法の整備が必要である
③監督当局の期待水準と業界の実務水準を踏まえたリスク管理が必要である
④リスクの見える化への工夫が必要である
⑤リスクの大きさを適切に評価する方法の整備が必要である
⑥リスク管理上の3ラインズディフェンスにおける役割・責任の整理が必要である
⑦ビジネス戦略、リスクアペタイト、リスクプロファイル及び資本力に見合った適切なリスク管理態勢の整備及びリスク文化の醸成が必要である
⑧重要な子会社及び外部委託先を含めた当社の組織横断的な管理態勢の整備が必要である
⑨内部監査の高度化を図る必要がある

## 4. 再発防止策

本件と同様の事案の発生を防止するため、当社は以下のような方策を実施してまいります。

### 4-1. 技術面における再発防止策

外部の専門家からのアドバイスを踏まえて、以下のセキュリティ施策を導入いたします。

**多要素認証の導入**

ログイン及び出金指示等の特定の操作の認証手段として、多要素認証を実装いたします。

従来のパスワード認証と新たに導入する他の認証方法を組み合わせることで、より安心・安全なお取引環境を提供いたします。

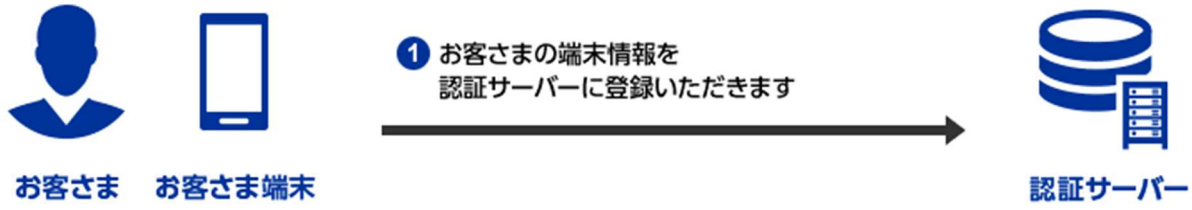
**【FIDO 認証】**

スマートフォンの生体認証等を連携させた多要素認証である FIDO 認証※を、各チャネルに順次導入いたします。

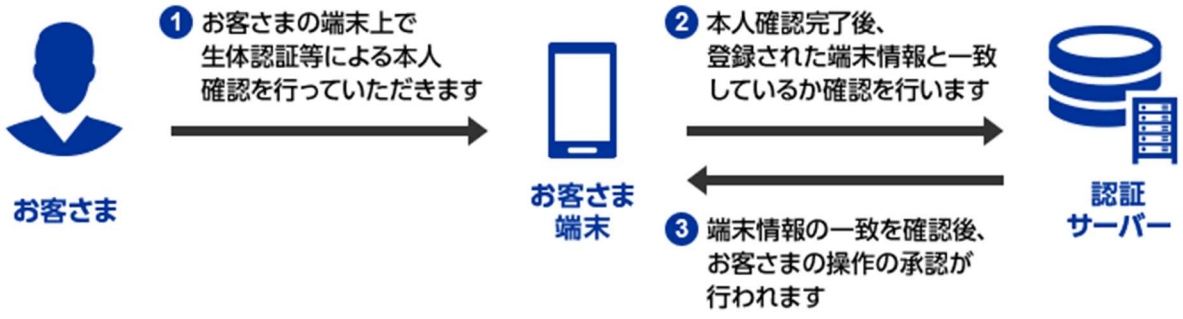
※ FIDO 認証はパスワード認証とは異なり、多要素認証という新しい認証方式の一つです。なお、生体認証に関わるお客さまの生体情報は、当社サーバー上に保存されることはございません。FIDO 認証のご利用には、当社が提供する「SBI 証券 株アプリ」が必要となります。

**＜FIDO 認証のご利用イメージ＞**

①初回登録時




②ご利用時

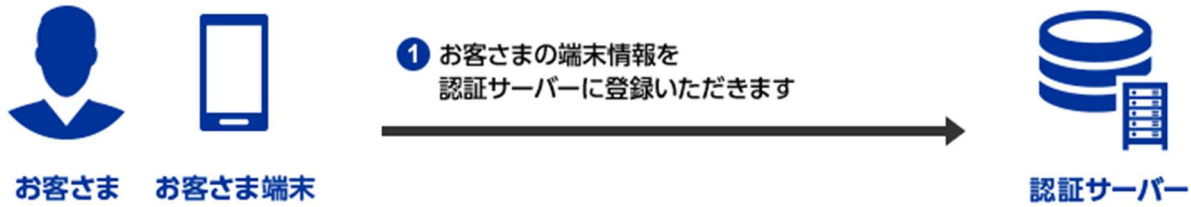


**【デバイス認証】**

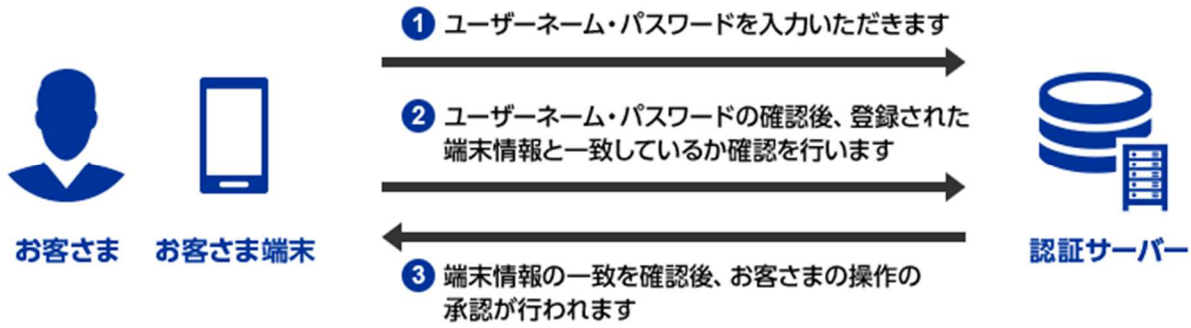
　認証手段の一つとしてデバイス認証を各チャネルに順次導入します。ユーザーネーム・パスワードによる認証に加えて、操作可能なデバイスを限定することで、より安心・安全なお取引が可能となります。

**＜デバイス認証のご利用イメージ＞**

①初回登録時




②ご利用時




**通知機能の強化**

　ログイン、出金指示、住所変更等のメール配信の対象となる手続きの拡充をはじめ、お客さまへの通知機能の強化を進めてまいります。

**【メール配信の対象となるお手続きの拡充】**

以下のお手続きの際にメール配信を行います。

・お名前の変更
・ご住所の変更
・お電話番号（ご自宅）の変更
・携帯電話番号の変更
・国内上場外国株配当金振込先口座の変更
・E メールアドレスの登録
・E メールアドレスの削除
・出金指示

・ログイン

**【ログイン履歴の拡充】**

すべてのお取引チャネルにおけるログイン履歴をお客さまにご確認いただけるようにいたします。

**その他のセキュリティ強化**

**【当社サイトにおけるお客さま情報のマスキング】**

お客さまの PC の背後からの盗み見や、万が一悪意のある第三者にログインされた際の個人情報漏洩防止のため、当社サイト内のお客さまを特定する情報に、マスキングを行います。

**＜マスキングの対象となる項目＞**

氏名
生年月日
住所
電話番号
メールアドレス
振込先金融機関の口座番号

**【パスワードの桁数拡張及び複雑化】**

安全性を高めるために、パスワードを長く複雑にすることが推奨されております。お客さまからも多数ご要望をいただいていることから、パスワードの桁数拡張及び複雑化を行います。

**ログイン監視機能の強化等**

当社内における、不審な取引の監視・未然防止の機能を強化するため、以下の施策を行います。

・不正アクセスに対する 24 時間モニタリング体制のさらなる強化
・不正アクセス検知システム（WAF）による新たな攻撃手法への対応
・不審な IP アドレスからのアクセス排除（IP レピュテーションサービスの一層の活用）

**4-2. ガバナンス面における再発防止策**

**オペレーショナルリスク管理態勢高度化への取り組み**

オペレーショナルリスクに関する 3 ラインズディフェンスにおける役割責任を整理し、1st ラインにおける自発的なリスク管理プロセスを促進するとともに、2nd ライン、3rd ラインを含む全社的なリスクガバナンスにおけるアカウンタビリティ向上、収益・コスト・リスク（財務・風評・成長性）の一体的管理、健全なリスク文化の醸成に取り組みます。また、情報セキュリティリスクを含むオペレーショナルリスク管理におけるリスクの特定・評価と、モニタリング及びコントロールというリスク管理プロセスを以下のとおり再構築します。特に、「サイバー攻撃などの外部脅威に伴う情報流出リスク」の制御は喫緊の課題であり、再構築作業の進捗と並行してサイバー攻撃に対する防御レベルの向上を図ります。

高度化を図るリスク管理のプロセスは以下のとおりです。

**イ. リスク管理のプロセス**

リスク管理のプロセスについては、リスクの特定、評価、モニタリング及びコントロールの一連のプロセスのPDCA を継続的に回していくことで、当社を取り巻く外部環境や競合環境、内部環境の変化に応じ絶えず改善を図っていくため、既存プロセスの高度化を図ります。

**ロ. リスクの特定**

当社がどのような重要なリスク(トップリスク)に晒されているのか、また、現時点では顕在化していないが、将来顕在化し当社に大きな影響を及ぼす可能性があるリスク(エマージングリスク)としてどのようなリスクが考えられるのかを、フォワードルッキングな視点で行います。こうしたリスクの特定に当たっては、外的要因(サイバー攻撃等)及び内的要因(システムリスク等)の双方を考慮して、当社のビジネス特性やリスクプロファイル、足元のリスク顕在化事例や外部環境(規制環境を含む)の変化、競合他社との関係、システム開発環境等を踏まえて行います。

**ハ. リスクの評価**

リスクの評価に当たっては、どのような事象が生じた際に特定されたリスクが顕在化するかの「リスクの見える化」を行うことで、現場部署及びリスク管理部署並びに経営陣がリスク評価について実効的な議論を実施できるようシナリオ分析を行います。特定されたリスク事象が顕在化するであろう具体的なシナリオを想定した上で、それが当社の財務、風評及び成長性に与える影響度、経営上のリスクとしての軽重を判断するために、想定したシナリオが生じた場合のリスクの発生規模及び発生頻度を段階評価します。

**ニ. リスクのコントロール**

リスクのコントロールについては、コントロール手段をその性質に応じて分類した上で、各コントロール手段のリスク削減効果を勘案し、当該コントロール手段適用後のリスクを残存リスクとして評価することで当社が晒されているリスクの現状を把握することに加え、今後取り得るコントロール手段の候補を洗い出し、当該コントロール手段を適用することにより残存リスクがさらにどの程度減少するのかを評価することで、経営陣がコントロール手段導入に伴うコストと合わせて適切に意思決定が行えるようにいたします。

**ホ. リスクのモニタリング**

リスク及びコントロール状況を経営陣にわかりやすい形でモニタリング可能となるよう、またそれにより的確な意思決定につなげることができるよう「ダッシュボード」、「リスクマップ」を作成・アップデートします。具体的に当該「リスクマップ」等は、取締役会及びリスク管理委員会がリスク管理状況を適切に把握し、必要な改善指示を実施できる情報を提供する形といたします。

**ヘ. スケジュール**

オペレーショナルリスク管理態勢高度化のスケジュールについては、2020 年 12 月にスタートし遅くとも 2021 年中に完了する予定です。

**内部監査の高度化への取り組み**

準拠性監査からの脱却を意識し、経営環境等の変化を捉えた予兆的な観点からの監査を志向いたします。現在、取り組んでいる内部監査の高度化を着実に進め、その実効性や、3 ラインズディフェンスの第 3 線としての独立的評価の適切性確保のため、内部監査をリスクベースで行うための監査実施基準及び手順書等の整備を行います。

また、内部監査部門の地位向上や専門性の確保を図るため、中長期的なキャリアパスを明確化し、計画的な専門人材育成・配置を行い、内部監査態勢を充実させる取組みを目指します。

マネー・ローンダリング及びテロ資金供与対策やサイバーセキュリティといった高リスクの専門分野において、グループ一体の監査を行うため、内部監査部門に専担チームの設置について検討いたします。

**レガシーシステムからの脱却**

当社のシステムは、新たに商品・サービス・取引チャネル等を追加する過程で、それぞれのベンダーによるシステムを結合し積み重なったという特色があります。そうした点が、システム開発を複雑化させる弊害を生じさせております。

また、利用しているデータ・センターの一部が、拡張性に乏しく、セキュリティ対策等の設計思想が陳腐化している状況にあります。

そうした、所謂「レガシーシステム」への対応策も、サイバー攻撃全般のリスク低減のために必要なものであると従前より経営課題として認識しております。

まず、システムが結合し複雑に積み重なっている問題に関しては、アプリケーションを再構成して単純化を実現するプラットフォームを構築し、各システムを順次搭載する「モデル先導方式」を採用し、既に取り組んでおります。ベンダーが異なるそれぞれのシステムごと、カテゴリーごとに、柔軟かつ迅速に、順次更新を継続的に繰り返しながら進めるためには、一括して全てのシステムを更改する「ビッグバン方式」ではなく「モデル先導方式」が適しているため、これを選択いたしました。

また、重要な課題であるデータ・センター問題に関しては、拡張性や設計思想に優れたデータ・センターへの移設を随時進めております。またこの際には、単にそのまま移設するのではなく、移設時に各システムを順次更新いたします。その中で、サイバーセキュリティ対応のためのシステムについては最優先で対応いたします。

**5. 内部犯行の可能性について**

本事案に関し、当社の外部委託先を含む内部者が関与している可能性に関しては、以下のように調査を進めております。

まず、仮にお客さまのユーザーネームやパスワードが当社内から持ち出されたとすると、当社内の特定のデータベースへのアクセスがなされない限り不可能です。これに関し当社の本番環境は、アクセス権限管理システムによる厳重なアクセス権管理がなされているうえに、特定の踏み台サーバー経由でしかアクセスできないよう制限を設けております。

また、システム監視ツールによる監視や操作ログ記録の定期的な検査を行っております。本事案を踏まえて改めてお客さま情報を含むデータベースへのアクセス履歴や踏み台サーバーでの疑わしい操作の確認を行いましたが、現時点において不審な点は認められておりません。

なお、当然のことながら、当社による調査のみで内部犯行を否定できるものではなく、第三者委員会及び外部企業による調査も行っております。そのような外部調査においても現時点で不審な点は見つかっておらず、内部犯行の可能性は極めて低いとの見解を得ておりますが、外部企業による調査は引き続き実施していくことを予定しており、不審な点が認められた際には、改めて公表を行うとともに、厳格に対処いたします。

**6. 関係者の社内処分**

本事案における責任の所在を明確化するため、以下のとおり社内処分を行うことといたしました。

| | | | |
|---|---|---|---|
| 髙村　正人 | 代表取締役社長 | 減俸 30% | 3カ月 |
| 齋藤　岳樹 | 専務取締役　内部管理統括責任者 | 減俸 20% | 2カ月 |
| 日下部　聡恵 | 常務取締役　リスク管理部門担当 | 減俸 20% | 2カ月 |
| 小川　泰幸 | 執行役員常務　システム部門担当 | 減俸 10% | 1カ月 |
| 尾﨑　晃 | 執行役員　内部管理統括補助責任者 | 減俸 10% | 1カ月 |

なお、上記処分とは別に、本事案に関する道義的責任の観点から、以下のとおり、当社における報酬に関し自主返納の申し出を受けております。

| | | | |
|---|---|---|---|
| 北尾　吉孝 | 代表取締役会長 | 報酬額全額 | 6カ月 |

このたびは、お客さまをはじめとした当社のステークホルダーの皆さまに多大なご迷惑とご心配をおかけしておりますことを、重ねてお詫び申し上げます。当社は、二度とこのような事態を起こさぬよう、前記の再発防止策を徹底し、お客さまが安心してサービスをご利用いただけるよう、努めてまいります。

**********

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