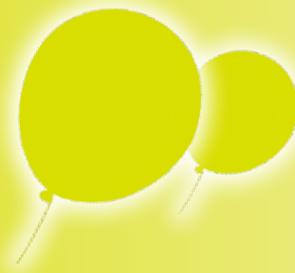


金融犯罪への対応



お客さまの大切な資産を守り、安心してお取引をさせていただけるよう、さまざまな犯罪防止策を講じています。2015年10月には、金融機関を狙ったサイバー攻撃などが

近年高度化・巧妙化していることをふまえ、これらに対応する専門組織「セブン銀行CSIRT^(※1)」を設立しました。

|| ATMでの対応

ATMには万が一の際の記録用カメラを設置しているほか、お客さまのプライバシー保護のため画面や入力ボタンを周囲から見えにくくするなどの配慮をしています。振込め詐欺被害を未然に防ぐため、ATMでお振込をされる際には、画面表示や音声で注意喚起も行っていきます。また、ATMに

取付けられた不審物の検知やカード情報の不正取得被害（スキミング被害）の防止対策も常時行っています。

2015年12月からは、ATMの犯罪利用を防ぐために国内銀行取引で導入していたICチップ取引対応を、海外発行カード取引にも順次拡大しています。

|| セブン銀行口座での対応

セブン銀行口座の犯罪利用を防止するため、口座開設時の本人確認の厳格化や、過去に犯罪にかかわっていた人物などのフィルタリングを行っています。口座開設後は、リアルタイムに取引状況のモニタリングを行うことで不審な取引を検知する「口座モニタリングシステム^(※2)」を導入しています。また、高度化するインターネットバンキングを狙った犯罪に右記の対策などを行っています。

〈個人のお客さま〉

- ・2015年11月よりインターネットバンキングにスマートフォン認証^(※3)を導入しています。
- ・お客さまのパソコンがマルウェア^(※4)に感染していることを検知するシステムを導入しています。

〈法人のお客さま〉

- ・ワンタイムパスワード^(※5)を導入しています。

|| 警察への迅速な協力

警察からの協力依頼に対し、ATM取引の通信内容を開示するATMジャーナル照会、防犯カメラ映像を開示するビデオ

照会、セブン銀行口座の取引内容を開示する口座照会などを迅速に行っています。

※1 CSIRT (Computer Security Incident Response Team): コンピュータセキュリティに関する事案の発生時に、素早く適切な対応をするための組織のこと。

※2 口座モニタリングシステム: 振込め詐欺などで使われた口座の動きを分析し、似た動きをする口座をチェックするシステム。不審と思われる取引や口座の動きがあった場合、一旦振込を停止して振込元の金融機関に入金の正当性を確認後、振込を実行しています。

※3 スマートフォン認証: インターネットバンキングで「新しい振込先への振込」などのお取引をされる際に、スマートフォンの専用アプリから承認していただく認証方法です。ご利用には登録手続きが必要です。

※4 マルウェア: コンピュータに不正にアクセスし、攻撃や情報を漏えいさせるなどの有害な動作を行う目的で作成されたソフトウェアの総称。

※5 ワンタイムパスワード: 一度限り(一定時間限り)有効なパスワード。第三者による不正利用のリスクを低減させます。