



コンプライアンス

マネー・ローンダリングおよびテロ資金供与防止に向けた取り組み

当行は、マネー・ローンダリングおよびテロ資金供与（以下、「マネー・ローンダリング等」という）防止を経営戦略等における重要な課題の一つとして位置付け、基本方針に基づきマネー・ローンダリング等の防止に向けた管理態勢の構築に努めております。

また、全役職員に対し、マネー・ローンダリング等防止の重要性の理解促進に努めるため、研修等を継続的に実施し、関係法令や適切な事務取扱いの周知徹底を図っています。

反社会的勢力の排除

当行は、反社会的勢力排除の基本方針を定め、反社会的勢力との一切の関係遮断に向けて取り組んでいます。また、基本方針に基づき、反社会的勢力に対する具体的な関係遮断の取り組みを定めたマニュアルを策定し、研修等を通じて従業員の啓発に努めています。

反社会的勢力排除の基本方針

1. 当行及び武蔵野銀行グループは、社会の一員として市民社会の秩序や安全に脅威を与える反社会的勢力及び団体（以下、反社会的勢力と呼ぶ）とは一切の関係を遮断しこれを排除する。
2. 当行及び武蔵野銀行グループは、金融機関としての業務の公共性に鑑み、公共の信頼を維持し、預金者等の保護を確保すると共に金融の円滑を図り、業務の適切性及び健全性を確保するために、反社会的勢力と一切の関係を遮断、排除し、反社会的勢力に対し毅然とした態度で対応する。

公益通報制度

当行は、法令等違反行為、その他不祥事に繋がる事象を早期発見・是正するため、公益通報制度に係る規程・マニュアルを制定し、行内のほか、行外の弁護士事務所に通報窓口を設けて、全従業員が直接通報し相談できる態勢を整えています。

顧客保護等管理体制

Ⅰ 顧客保護等管理体制

顧客保護への取り組み

当行は、お客さまからの信頼を第一と考え、お客さまの資産、情報およびその他の利益を保護すること、並びに利便の向上を図るための顧客保護等管理の重要性を十分理解し、整備・確立に努め、以下に定める事項を実行いたします。

- ア. 顧客説明管理…お客さまとの取引又は商品の説明および情報提供に際し、お客さまの知識、経験、財産の状況および金融商品の投資の目的や意向に照らして適切かつ十分な説明および情報提供を行います。
- イ. 顧客サポート等管理…お客さまからの相談・苦情等については、適時・適切に対応し、再発防止および改善に努めます。
- ウ. 顧客情報管理…お客さまの情報は、法令等並びに行内規程等に従い、適切に取得・利用し、安全管理に努めます。
- エ. 外部委託管理…お客さまとの取引に関連して、その業務を外部委託する際には、お客さま情報その他お客さまの利益が損なわれないよう適切に管理いたします。
- オ. 利益相反管理…お客さまとの取引にあたり、お客さまの利益が不当に害されるおそれのある取引を適切に管理し、お客さまの利益を保護するとともに、お客さまからの信頼向上に努めます。

金融ADR制度

「金融ADR制度」とは、紛争事案について裁判によることなく（裁判外で）、紛争解決（ADR）機関によるあっせん・調停・仲介のもと、紛争の解決を行う制度です。

当事者間で解決を図ることが困難な場合に、お客さまと金融機関のいずれか一方からの申立てにより、当行が契約している指定銀行業務紛争解決機関である一般社団法人全国銀行協会が、裁判手続よりも迅速、簡易、安価で柔軟な解決を図ります。

〈当行が契約している指定銀行業務紛争解決機関〉

一般社団法人全国銀行協会

連絡先: 全国銀行協会相談室

電話番号: 0570-017109 または 03-5252-3772

顧客保護等管理体制

お客さまの大切なご資産を守るために

●インターネットバンキングおよびスマートフォンアプリの不正使用被害の未然防止

お客さまに安全にご利用いただくため、さまざまなセキュリティ対策を実施しているほか、ホームページ等を通じてお客さまへの注意喚起に努めています。

インターネットバンキングのセキュリティ対策

- 個人インターネットバンキング「むさしのダイレクト」では、スマートフォン専用のセキュリティアプリ「むさしのダイレクトアプリ」やお振込みの際に利用する一回限りの使い捨てパスワード「ワンタイムパスワードアプリ」の無償提供等を行っています。
- 法人インターネットバンキング「むさしのビジネス・ダイレクト」では、トラザクシオン認証※機能付ワンタイムパスワードを採用し、不正使用被害の防止に努めています。フィッシングや不正なポップアップをはじめさまざまな攻撃に対応し、不正送金被害からお客さまを守る「PhishWallプレミアム」を無償提供するほか、不正取引の早期発見等のセキュリティ強化策として登録メールアドレスへ取引結果を即時に通知しています。

※トラザクシオン認証とは、強固なセキュリティ対策の一つで、振込先口座番号等のお客さま情報を使用しパスワードを生成することで、悪意の第三者が振込先を改ざんし、意図しない口座に振り込むという犯罪等を防止できるものです。



スマートフォンアプリのセキュリティ対策

- お客さまのスマートフォンと銀行との間のインターネット通信は、暗号化して盗聴や改ざんを防止しています。
- 指紋認証や顔認証によるアプリへのログインを可能とすることで、セキュリティの一層の強化を図っています。
- 振込等のお取引時には、届出電話番号にSMS（ショートメッセージ）または電話（自動音声）にて認証番号を通知し、本人確認のための追加認証を行っています。
- 普段と異なる端末から初回登録があった場合は、メールでお知らせします。
- 外部のセキュリティ診断会社から安全性に関する第三者評価を受けています。

●埼玉県警察との「特殊詐欺等の被害防止にかかる協定」締結

2024年10月、特殊詐欺等の被害防止に向けた取組みの一層の実効性向上を目指し、県内に本店を置く銀行・信用金庫・信用組合とともに協定を締結しました。埼玉県警察が保有する不正利用口座データによるモニタリングを行うとともに、詐欺被害の実態や手口を学ぶ研修会を実施しています。

●振り込め詐欺等特殊詐欺被害の防止

店頭やATMコーナー、また、お客さまに積極的な注意喚起を行っているほか、お客さまのご意向を確認のうえ、ご本人さま名義の口座への振込みによるお取引をご案内しています。

また、ATMに誘導する振り込め詐欺被害の防止とキャッシュカード手渡し型詐欺被害を最小限に食い止めるため、一定条件に該当するご高齢のお客さまの口座を対象にキャッシュカードの振込機能の利用制限および1日当たりの利用限度額の引下げを行っています。

●電子決済サービスの不正使用防止

当行では、お客さまが電子決済サービスに当行口座の登録を行う際、生年月日・キャッシュカード暗証番号等のお客さま情報のほかに、ワンタイムパスワードによる本人確認を行っています。