

安心・安全を追求したご利用環境の整備

通常時

システム拠点を二重化

災害などでお取引ができなくなるような事態を避けるため、ネットワークの根幹をなす中継システムや、お客さまからのお問合せ窓口となるATMコールセンター、テレホンセンターを首都圏と大阪に設置しています。東西両方を常時稼働させ、一方にトラブルが発生しても、もう一方で業務を継続できるような態勢を整えています。

ATM内現金のモニタリング

パートナー企業である警備会社と連携してATM1台ごとに利用状況のモニタリングを行い、現金切れなどによるサービスの停止を防いでいます。また、個々の利用パターンに応じたタイミングで現金の補充や回収を行い、作業による停止時間を必要最小限に抑えています。



セキュリティ対策

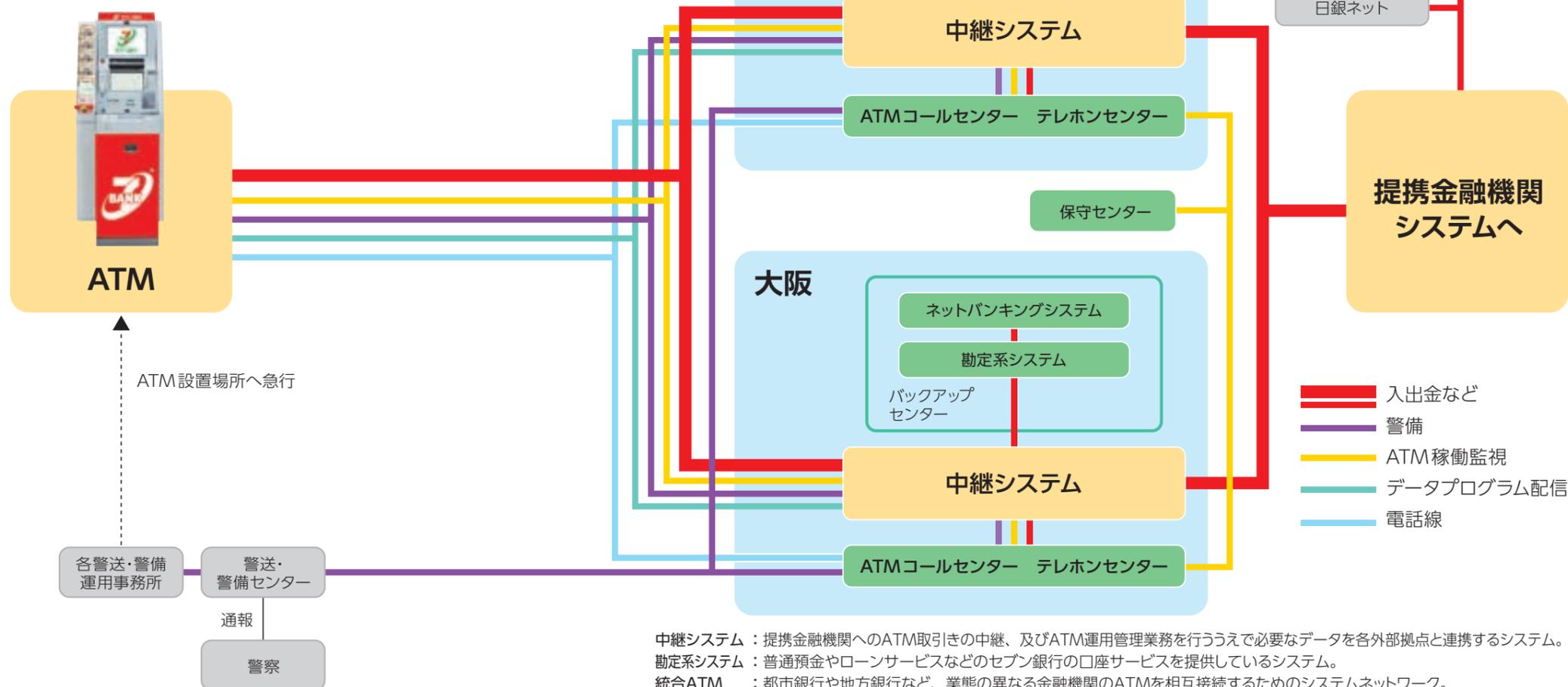
提携金融機関等とセブン銀行の通信は、データを暗号化するなどして、万全のセキュリティ対策を施しています。

緊急時

故障・不具合発生時の対応

パートナー企業と連携し、すべてのATMやネットワークシステムをリアルタイムで管理しています。故障や不具合が発生すると自動的にシグナルが送られるようになっており、スピーディーかつ的確な対応でサービス停止時間を最小限に抑えられるよう努めています。

■ セブン銀行のシステムネットワーク



中継システム：提携金融機関へのATM取引の中継、及びATM運用管理業務を行ううえで必要なデータを各外部拠点と連携するシステム。
勤定系システム：普通預金やローンサービスなどのセブン銀行の口座サービスを提供しているシステム。
統合ATM：都市銀行や地方銀行など、業態の異なる金融機関のATMを相互接続するためのシステムネットワーク。
全銀システム：国内にある銀行間の振込などの取引に関するデータの交換、及び資金決済を行うシステム「全国銀行データ通信システム」の略称。銀行や信用金庫など、日本のほぼすべての民間金融機関が参加。

災害発生時の対応

2011年3月の東日本大震災後、ATMの営業再開に相応の時間が必要な地域へ移動ATM車両を派遣しました。2015年10月から2016年3月には、東京電力福島第一原子力発電所事故による避難指示区域に指定されている福島県の葛尾村へ定期的に移動ATM車両を派遣し、地域の復興支援を行いました。

災害時の業務継続

大規模災害や事故発生時でも業務を継続できるようにBCP（業務継続計画）を作成し、「ATM業務」「銀行間及びATM提携先との資金決済業務」「当社預金の払出しと為替業務」の3つを優先して継続すべき業務と定義しています。首都圏と大阪のどちらかが被災した場合は、もう一方

が単独で業務を継続できるようにさまざまな機能を二重化していますが、交通機関が使用できない状況の中で、必要な人員を搬送するため、航空会社とヘリコプターの緊急出動契約を締結しています。

金融犯罪への対応

お客さまの大切な資産を守り、安心してお取引をしていただけるよう、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}」を設置しました。

※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、素早く適切な対処をするための組織のこと。

ATMでの対応

ATMには万一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年度には、ATMの犯罪利用を防ぐため、国内金融機関の取引で導入していたICカード対応を海外発行カード取引にも拡充しました。システムによる取引の監視も実施しています。

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。

※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。

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。

※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。

警察への迅速な協力

警察からの協力依頼に対し、迅速な対応を行っています。2015年度は、ATM取引の通信内容を開示するATMジャーナル照会 約63千件、防犯カメラ映像を開示するビデオ照会 約1千件、セブン銀行口座の取引内容を開示する口座照会 約12千件への対応を行いました。

お客さまの声を活かした改善

お客さまのニーズをふまえて生まれた銀行だからこそ、お客さまから寄せられるご意見・ご要望を大切にしています。ATMコールセンターやテレホンセンター

に寄せられたご意見を、社内で共有・検証・分析することで、より便利な商品・サービスの提供につなげています。

改善事例①



「ATMにカードを入れた後、
どうしたらよいか
分からない。」

海外からのお客さまや、ご高齢のお客さまからの声にお応えして、カードを入れた後に一定時間が経過すると、オペレーターによる対応をご案内する動画を表示するようにしました。



オペレーターによる対応をご案内する動画

改善事例②



「ATMで入金した後
カードを取り忘れて
しまった。」

ATMでお取引いただいた後に、お金やカードを取り忘れてしまうお客さまが多かったため、「呼びかけ」の機能を強化しました。たとえば、ATMに入金した後、カードを受取らずにATMから離れると、センサーで検知して、「お客さま、お忘れものはございませんか?」と呼びかけます。入金以外の取引では違うパターンの呼びかけをしますが、これらの機能を導入後、お客さまがお金やカードを取り忘れる件数を減らすことができました。

セブン銀行テレホンセンターが三つ星を獲得!

セブン銀行のテレホンセンターは、HDI-Japan (ヘルプデスク協会) が主催する2015年度「問合せ窓口格付け」において、国内最高評価である「三つ星」を獲得しました。



授賞式の様子