2014 年 8 月 1 日
株式会社みずほ銀行

「法人インターネット・バンキング」の預金等の不正な払戻しに対する対応について

株式会社みずほ銀行（頭取：林 信秀、以下「当行」といいます）は、一般社団法人全国銀行協会より公表された、2014 年 7 月 17 日付「法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方（以下、「補償の考え方」）」を踏まえ、インターネット・バンキングの信頼性を高め、お客さまに安心してご利用いただくために、さらなる取り組みを進めていくとともに、法人のお客さまの不正な払戻し被害について補償を開始いたします。

【不正な払戻し防止に向けた取り組み】

当行は、お客さまに法人インターネット・バンキング・サービスを安心してご利用いただくため、これまでに導入済のセキュリティ対策に加え、新たな対策を導入してまいります。

一方で、「補償の考え方」にも示されているとおり、お客さまにも、不正払戻し被害防止のための対策を実施していただくことが重要です。

お客さまにおかれましては、「補償の考え方」で公表されている「お客さまに講じていただくセキュリティ対策事例」を参考にしていただき、当行が、お客さまにご依頼しておりますセキュリティ対策を実施していただきますようお願い申しあげます。

【補償の概要】

対象となるお客さま：当行の法人インターネット・バンキング（みずほ e-ビジネスサイト、みずほビジネス WEB）をご利用頂いている法人のお客さま

補償開始日：2014 年 8 月 1 日

補償内容：お客さまが不正な払戻し被害に遭われた場合には、原則、年間 5,000 万円を上限に当該被害の補償を検討いたします。
具体的な補償の内容につきましては、お客さまのご利用状況やセキュリティ対策の導入状況、警察当局による捜査結果等も踏まえ、個別に検討させていただきます。

【お客さまに実施していただきたいセキュリティ対策】　（2019 年 1 月 21 日更新）

みずほ e-ビジネスサイト	みずほビジネス WEB
(A) 振込データを作成するユーザーとデータを承認するユーザーを分け、異なるパソコンでサービスを利用すること（「特権承認権限」を付与しないこと） (B) セキュリティ対策ソフト「Rapport（ラポート）」をインストールしたパソコンでサービスを利用すること (C) パソコン本体ではなく、IC カードに格納した電子証明書により、サービスを利用すること（サービスを利用しない時は、IC カードをカードリーダーから抜いておくこと） ※IC カードの新規お申し込みは、2019 年 1 月 20 日をもって停止いたしました。 (D) 取引認証付きワンタイムパスワードを利用すること 当行では、上記セキュリティ対策のうち、複数を組み合わせて実施していただくことを推奨いたします。	(a) 振込データを作成するユーザーとデータを承認するユーザーを分け、異なるパソコンでサービスを利用すること（承認機能は「シングル承認」または「ダブル承認」を利用し、かつ、1 人のユーザーに振込の「依頼」権限と「承認」権限の両方を付与しないこと） (b) セキュリティ対策ソフト「Rapport（ラポート）」をインストールしたパソコンでサービスを利用すること (c) 2 経路認証（データ作成したデバイスとは異なるデバイスによるデータ承認）を利用すること (d) 取引認証付きワンタイムパスワードを利用すること 当行では、上記セキュリティ対策のうち、複数を組み合わせて実施していただくことを推奨いたします。

以上

（ご参考）2014 年 7 月 17 日付全国銀行協会「法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方」より

お客さまに講じていただくセキュリティ対策事例

1. 法人のお客さまに実施していただくセキュリティ対策	
	(1) 銀行が導入しているセキュリティ対策の実施 銀行が導入しているセキュリティ対策を着実に実施していただくこと
	(2) インターネット・バンキングに使用するパソコン（以下、単に「パソコン」という）。に関し、基本ソフト(OS)やウェブブラウザ等、インストールされている各種ソフトウェアを最新の状態に更新していただくこと
	(3) パソコンにインストールされている各種ソフトウェアで、メーカーのサポート期限が経過した基本ソフトやウェブブラウザ等の使用を止めていただくこと
	(4) パソコンにセキュリティ対策ソフトを導入するとともに、最新の状態に更新したうえで、稼動していただくこと
	(5) インターネット・バンキングに係るパスワードを定期的に変更していただくこと
	(6) 銀行が指定した正規の手順以外での電子証明書の利用は止めていただくこと
2. 法人のお客さまに推奨するセキュリティ対策	
	(1) パソコンの利用目的として、インターネット接続時の利用はインターネット･バンキングに限定していただくこと
	(2) パソコンや無線 LAN のルータ等について、未利用時は可能な限り電源を切断していただくこと
	(3) 取引の申請者と承認者とで異なるパソコンを利用していただくこと
	(4) 振込・払戻し等の限度額を必要な範囲内でできるだけ低く設定していただくこと
	(5) 不審なログイン履歴や身に覚えがない取引履歴、取引通知メールがないかを定期的に確認していただくこと

補償減額または補償せずの取扱いとなりうるケースについて

1. 以下のような対応がお客さまに実施されていないケース	
	(1) 上記 1.「法人のお客さまに実施いただくセキュリティ対策」の導入
	(2) 身に覚えのない残高変動や不正取引が発生した場合の、一定期間内の銀行への通報
	(3) 不正取引が発生した場合の、一定期間内の警察への通報
	(4) 不正取引が発生した場合の、銀行による調査および警察による捜査への協力
2. お客さまに過失があると考えられる以下のような事象が認められたケース	
	(1) 正当な理由なく、他人に ID・パスワード等を回答してしまった、あるいは、安易に乱数表やトークン等を渡してしまった場合
	(2) パソコンや携帯電話等が盗難に遭った場合において、ID・パスワード等をパソコンや携帯電話等に保存していた場合
	(3) 銀行が注意喚起しているにも関わらず、注意喚起された方法で、メール型のフィッシングに騙される等、不用意に ID・パスワード等を入力してしまった場合
3. その他、以下のような事例に相当するケース	
	(1) 会社関係者の犯行であることが判明した場合
	(2) その他、上記 2. の場合と同程度の注意義務違反が認められた場合