「みずほダイレクト」のセキュリティ対策について

- インターネットパンキング等のご利用をより安全に

株式会社みずほ銀行(頭取 杉山清次)は、2005年8月22日(月)より、「みずほダイレクト」のセキュリティ強化策の一つとして、お客さまが「みずほダイレクト」をご利用いただく際にパソコン等から暗証番号等が漏洩することを防ぐために下記の対策を実施いたします。これにより、キーロガー 1 やスパイウェア 2 といったソフトを利用した犯罪による被害発生防止に、一定の効果が見込めるものです。

また、お客さまご自身の暗証番号やパスワードの管理方法につきましても、引続きご注意を呼びかけていくとともに、その他のセキュリティ対策についても、順次検討・実施していく予定です。

- 1:キーロガー》インターネットを利用するパソコンにキーボード操作を記録するプログラム を忍ばせ、ID・パスワード等のデータを収集する手口。インターネットカフェなどの不特 定多数が共用するパソコンに仕込まれる可能性がある。
- 2 : スパイウェア》フリーソフトや電子メールなどの形でパソコンに侵入し、パスワード等の 個人情報を勝手に外部へ流してしまうプログラム。

記

1.[インターネットパンキング・モバイルパンキング]第2暗証番号の入力方法変更

インターネットバンキング・モバイルバンキングでお振込・お振替などを行う際の、第2暗証番号の入力方法を変更いたします。

変更前	変更後
	バンキングサービス ³ のご利用に関しては、第2暗証番号6桁のうち当行が都度指定する4桁のみを、当行が都度指定する順序でご入力

3:投資信託サービスにつきましては、当面従来どおりのご利用方法となります。

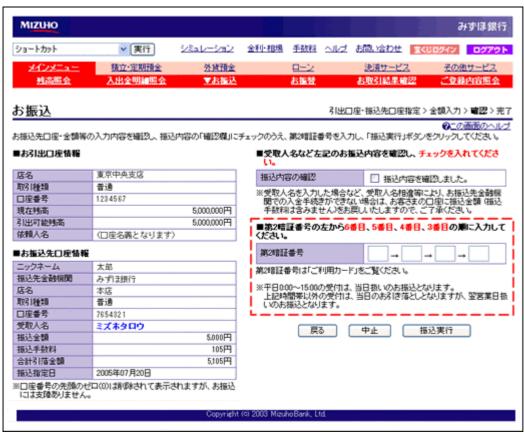
本対応により、万が一お客さまがキーボードで入力される内容を第三者に知られた場合でも、 なりすましは難しくなります。

2.[インターネットバンキング] ソフトキーボードによるログインパスワード入力

インターネットバンキングにおいて、**マウスのクリックだけでログインパスワードを入力できる、ソフトキーボードの機能を追加**いたします。

なおソフトキーボードをご使用いただくことにより、キーボードで入力した内容を第三者が 不正に取得することができなくなります。

1.第2暗証番号の入力方法変更



2.ソフトキーボードによるログインパスワード入力

