インターネットバンキングでの不正送金被害防止のためのお願い

最近、全国の複数の金融機関において、コンピュータウィルス等により不正に暗証番号が盗取されたり、遠隔操作されるなどして、預金が不正に引き出される被害が発生しております。

このような被害に遭わないよう、お客さまにおかれましては以下の対応を行っていただきますようお願い申し上げます。

１．ご利用のパソコンの状態に関する対策

（１）基本ソフト（ＯＳ）やブラウザ等、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する。

（２）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、最新の状態に更新する。

（３）不審なサイトは閲覧しない。不審なメール、その添付ファイル・リンクは絶対に開かない。

２．インターネットバンキングの運用に関する対策

（１）なるべく、管理者と利用者とで異なるパソコンを利用する。

（２）暗証番号および確認暗証番号は毎月変更する。

（３）取引限度額は必要な範囲内でできるだけ低く設定する。

（４）不審なログイン履歴が無いか確認する。

３．銀行を騙る偽メール等に係る注意喚起について

当行では発生しておりませんが、他行において不審なメール、不審なサイト、ウィルス感染を原因とする不正アクセスによる被害が発生しておりますので、十分にご注意願います。

（１）インターネットバンキングのパスワード等を盗み取ろうとする不審な電子メール等が不特定多数の方に送信されております。大光銀行では、電話、電子メール等でインターネットバンキングのパスワード（暗証番号・確認暗証番号）をお尋ねすることはありません。そのような照会には絶対にお答えにならないでください。

（２）インターネットバンキングのパスワード等を盗み取ろうとするフィッシングサイトの発生が確認されております。フィッシング対策ソフト「PHISHCUT」をご利用になって、サイトの正当性を確認してください。（PHISHCUT ツールバーの青色点灯を確認）。なお、フィッシング対策ソフト「PHISHCUT」は当行ホームページより無料でダウンロードできます。

（３）銀行を不正に騙り、「入金のお知らせ」「セキュリティのお知らせ」等と称して、銀行とまったく関係ないサイトに誘導する電子メールが不特定多数の方に発信されております。このような電子メールに記載されているリンク先をクリックしたり、添付ファイル等を開いたりすると、インターネットバンキングのパスワード等を盗み出すサイトに誘導されたり、パソコンがウィルスに感染したりする恐れがありますので、不審なメールを受信した場合は、メールを開く、リンク先を開く、添付ファイルを開く等は絶対に行わないでください。

万一、不正送金被害が発生した場合、または、発生が疑われる場合は、速やかに以下の連絡先までご連絡ください。

○　平日のＡＭ９：００～ＰＭ５：００
　　ＴＥＬ：0120-585-376（たいこうオフィスｅ－バンキングヘルプデスク）

○　上記以外の時間帯
　　ＴＥＬ：0258-36-4100（ＡＴＭサービスセンター）

以上