

企業みなさまへ

インターネットバンキング利用者の預貯金が他人名義の口座へと送金される**不正送金**が多発しています。法人が被害者の場合、被害金額が多額になる可能性もあります。しっかりと対策をお願いします。

インターネットバンキング不正送金被害に遭わないために

不正送金の主な手口としては**ウイルスによるもの**と**フィッシングによるもの**があります。

【手 口】

(1) ウイルスによるもの

メールの添付ファイルを開いてウイルスに感染するという手口だけでなく、**サイトを見るだけでも感染する**というケースもあります。感染すると、インターネットバンキング利用ページを開いた時にウイルスが動き出し、**偽の「ID・パスワード」入力画面が表示される**などの症状が起こります。

(2) フィッシングによるもの

金融機関を装ってメールが届き、「システム改修のため ID・パスワードを再登録してください。」等の文章で巧みに**偽の「ID・パスワード」入力画面があるページへと誘導**されます。

【対 策】

上記のような手口でインターネットバンキング用の「ID・パスワード」を盗み取り、それを使用して不正送金が行われるケースがほとんどですが、**新しいウイルスも次々と発見**されていますので、**こまめな対策が必要**です。

対策は万全ですか？すべてにチェックがつけますか？

- ☐ ウイルス対策ソフトを導入し、常に最新のパターンに更新している。
- ☐ windows などの OS や他のソフトのアップデートはきちんと実施している。
- ☐ ログイン用 ID やパスワード、送金用パスワードはしっかり管理している。
- ☐ ログイン用 ID やパスワードを他のサイトに使い回していない。
- ☐ ID・パスワードは定期的に変更している。
- ☐ 正規のネットバンキングページを「お気に入り」に登録し、そこからアクセスしている。
- ☐ ワンタイムパスワード等複数の認証システムを利用している。
- ☐ 送金通知サービスを利用している。
- ☐ ほかのサイトを閲覧しないネットバンキング専用のパソコンを設置している。
- ☐ 金融機関等からメールが来たら、金融機関に電話等で確認後、開封している。