

2014年4月25日  
中央労働金庫

## ろうきんインターネットバンキング（団体向け）を使った不正送金にご注意ください

インターネットバンキングでの不正送金の被害が、複数の金融機関において発生しております。これまで安全性が高いとされていた「電子証明書方式」をご利用のお客さまにおかれましても、お客さまのパソコンがウイルスに感染した場合は、お取引に必要な情報の詐取や、パソコンの遠隔操作等により、被害に遭われる可能性があります。

このようなパソコンのウイルス感染や不正送金の被害等を防ぎ、サービスをより安全にご利用いただくために以下の点にご注意いただきますようお願い申し上げます。

1. ウィルス対策ソフトを利用してください。  
ウィルス対策ソフトを導入し、常に最新のウィルス対策を講じてください。  
なお、労働金庫では無償でウィルス対策ソフト「SaAT Netizen」をご提供していますので「ろうきんインターネットバンキング（団体向け）」ホームページよりダウンロードのうえご利用ください。
2. パソコン環境は推奨している環境を使用してください。  
パソコンのOSやブラウザソフトは、推奨している環境を使用し、最新の状態に更新してください。
3. 電子証明書のインストールされたパソコンは厳重に管理してください。  
電子証明書がインストールされたパソコンが第三者等に不正に利用され悪用されることのないようご使用のパソコンの厳重な管理をお願いいたします。  
また、電子証明書を含むデータ消去が不十分のまま、パソコンを廃棄しないでください。  
労働金庫の電子証明書は複製（エクスポート）を不可としています。パソコンの変更時には新しく電子証明書を取得し、あらためて設定してください。
4. 不審なメールは速やかに削除してください。  
心あたりのないメールは開かずに削除してください。万一開いた場合は、メールに記載されたホームページや添付ファイルを開かないようにしてください。
5. インターネットバンキングの権限やセキュリティ設定は適切に行ってください。
  - ・被害を最小限に抑えるため、一日あたりの資金移動限度額を必要最低限に設定してください。（資金移動限度額の変更は、インターネットバンキング上から設定することができます。）
  - ・パスワードは定期的に変更してください。
  - ・離席時等には、ログアウトを励行してください。
  - ・ご利用履歴を確認し、身に覚えのないログインがないか確認をしてください。

万一不審な取引等をご確認された場合は、お取引店にご連絡いただきますようお願いいたします。

以 上