# ＜法人インターネットバンキングサービス＞
# お客さまに実施していただくセキュリティ対策

## 電子証明書(無料)の導入

・電子証明書を導入してください（導入可能環境でない場合を除きます）。

・当組合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ください。

※　導入には書面によるお申込が必要です。お取引店にてお申込みください。

## ワンタイムパスワード（無料）の導入

・ワンタイムパスワードを導入してください(導入可能環境でない場合を除きます)。

※　ワンタイムパスワードのご利用にはアプリに対応するスマートフォンまたは
携帯電話が必要です（機種によってご利用になれない場合があります）。

※　導入には書面によるお申込が必要です。お取引店にてお申込みください。

## セキュリティソフトの導入

・パソコンには、必ずセキュリティソフトを導入し、最新版への更新をお願いします。

・パソコンがウィルスに感染していないことを定期的にご確認ください。

## 不正送金対策ソフト「フィッシュウォール」（無料）の導入

※　当組合ホームページよりダウンロードのうえ、ご利用ください。

## ソフトウェアは最新の状態に

・OSやブラウザ等の各種ソフトウェアは常に最新の状態に更新してください。

・提供元のサポート期限が経過したソフトウェアはウィルス等の感染や、
悪意のある攻撃を受ける可能性が高いため使用しないでください。

## 安全なパソコン環境でご利用ください

・インターネットカフェ等自分の管理しないパソコンや外出先の公衆無線LAN回線を
使ってのログインをしないでください。

・インターネットバンキングと、他のウェブサイトを同時に利用しないでください。

・使わないときはできるだけパソコンや無線ＬＡＮルータ等の電源を切ってください。

・パソコンでファイル交換ソフトを利用しないでください。
パソコン内の情報が流出する恐れがあります。

・心あたりのないメールやファイルは開かないでください。
また、不審なＷＥＢサイトにはアクセスしないでください。

## パスワード等（ログインＩＤ・パスワード・暗証番号）の厳正な管理

- 他のインターネットサービスと同一のパスワードや生年月日等、類推されやすいパスワード等を使用しないでください。
- パスワード等の入力は必ずソフトウェアキーボードをご利用ください。
- 当組合職員や警察官等が電話やメール等でパスワード等をお尋ねすることは絶対にありませんので、他人には教えないようご注意ください。
- パスワード等を記録する書類は第三者の目に触れないよう厳重に保管してください。また、パスワード等をパソコンや携帯電話等に保存しないでください。
- 利用者（一般ユーザー）の方の退職（異動）時には、ユーザーＩＤの削除をおこなう等、厳重な管理をおこなってください。

## 振込通知メール、利用履歴は必ずご確認ください

- メールの宛先を携帯電話等に設定し、いつでも不正アクセスが検知できるようにしてください。
- メールアドレスを変更された場合、必ずインターネットバンキングの「利用者管理」で変更登録をおこなってください。
- メール着信拒否設定等によりメール受信できない場合は、設定を変更してください。（振込等確認メールのメールアドレス　info@nozomi-shinkumi.co.jp　）
- インターネットバンキングのご利用の有無にかかわらず、利用履歴等を確認し、身に覚えのない振込や不正なアクセスがないかを定期的に確認してください。

## その他、ご対応いただきたい項目

- 振込限度額を必要な範囲内でできるだけ低く設定してください。振込限度額の変更については、お取引店にて書面により承ります。
- 複数のパソコンがご利用可能な場合、総合（給与）振込では、取引の申請者と承認者とで異なるパソコンを利用してください。

**インターネットバンキングについて、お問い合わせ、ご照会は**

のぞみネットバンキングヘルプデスク　平日　9:00～24:00

０１２０－３２２-４４３　土・日・祝　9:00～17:00

※1月1日～1月3日、5月3日～5月5日、12月31日は休止させていただきます。

**不正送金被害に遭われた場合や、不審な取引があれば至急下記までご連絡ください。**

平日　9:00～17:00　のぞみ信用組合(事務部)　０６－６９４４－２１０６

**上記時間外で緊急措置として資金移動を止める場合は、しんくみＡＴＭセンターまでご連絡ください。**

０１２０－００３－８１４