

◆お客さまに講じていただくセキュリティ対策◆

平素より空知商工信用組合をご愛顧賜り誠にありがとうございます。

インターネットバンキングをより安全にご利用いただくため、以下の対策をお願いします。

<ウイルスがお客さまのパソコンへ侵入することを防ぐための注意点>

| | 実施する内容 | 実施することによる効果 |
|---|--|---|
| ① | 基本ソフト OS（（例）Windows）ブラウザ（（例）Internet Explorer）等は、常に最新の状態に更新してください。 | 更新情報にはセキュリティ対策に必要な修正プログラム等が含まれています。 |
| ② | サポート期限が経過している基本ソフト等の利用はお控えください。 | サポートが終了した基本ソフト等のご利用を続けるとウイルスに感染しやすい環境になります。 |
| ③ | ウイルス対策ソフトを導入し、常に最新の状態に更新してください。 | 日々新しく誕生するコンピュータウイルスに対応するパターンファイルが更新されます。 |
| ④ | 不審なメールの開封および不審なサイトの閲覧は控えてください。 | 開封するだけで感染するウイルスが存在している可能性があります。 |
| ⑤ | 必要性がないダウンロード、USB 等の外部記録媒体の使用はしないでください。 | ダウンロードするファイルやデータにウイルスが存在している可能性があります。 |
| ⑥ | 当組合よりご案内する不正送金対策ソフト“Phish Wall プレミアム”をインストールしてください。 | 市販のウイルス対策ソフトと併用することで不正送金を防止できる可能性が高まります。 |
| ⑦ | インターネットバンキング専用のパソコンを用意していただき、可能な限り他の事で使用しないでください。 | ウイルス感染防止に繋がります。 |
| ⑧ | 長時間操作を中断する場合はパソコンや無線 LAN のルータ等の電源を切ってください。 | 遠隔操作等の不正ログイン防止に繋がります。 |

<インターネットバンキングを安全にご利用いただくための対策>

| | 実施する内容 | 実施することによる効果 |
|---|--|--|
| ① | パスワード等を定期的に変更してください。（推奨：1ヶ月に一度変更） パスワード入力時はソフトウェアキーボード推奨。 | 定期的に変更することで漏洩したパスワードが利用できなくなります。 |
| ② | 振込などの限度額を必要な範囲内で出来る限り低く設定してください。 | 不正送金被害を最小限に抑えられます。 |
| ③ | 取引時の通知メールは直にご確認してください。 | 不正送金被害の早期発見に役立ちます。 |
| ④ | 不審な前回ログイン履歴がないかログイン時に確認してください。 | 不正履歴が確認された場合、直ちに ID・パスワード等を変更し不正なログイン防止に繋がります。 |
| ⑤ | ID・パスワード等は、利用者以外に教えないでください。 | パスワード漏洩リスクを低減軽減できます。 |
| ⑥ | 通常とは異なる画面が表示された場合、直ちに操作を中止し、当組合までご連絡ください。 | 不正送金被害の防止に繋がります。 |
| ⑦ | インターネットバンキングをご利用になる際には、利用前にセキュリティソフトでウイルスチェックを行い、ウイルス感染がないことをご確認のうえでのご利用をお願いします。 | ウイルス感染の早期発見に役立ちます。 |
| ⑧ | 振込の申請者と承認者とで異なるパソコンをご利用ください。 | 申請者でデータ改ざんされた場合でも承認者で不正送金を防止できます。 |
| ⑨ | ログインは電子証明書方式をご利用ください。 | 電子証明書方式は使用パソコンを限定でき不正なログイン防止に繋がります。 |
| ⑩ | 電子証明書方式は、当組合が指定した正規の手順でご利用ください。 | 正規の手順以外で利用されると電子証明情報が漏洩されます。 |

※上記対策を講じていても完璧なセキュリティ対策が保証されたわけではありませんが安全性は向上します。