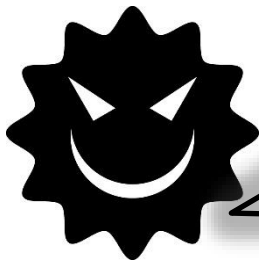


「サポート詐欺」にご注意ください！！

そのセキュリティ警告画面・警告音は、偽物です！
警告画面に表示された電話番号にかけないでください。



パソコンがウィルスに感染しているので
除去します。
コンビニで電子マネーを買ってください。
(クレジットカードで支払ってください。)

サポート詐欺とは、インターネットを閲覧中に「ウィルスに感染しました」等のメッセージが表示され、電話をかけさせ「ウィルスの除去」等の名目で金銭を詐取する詐欺です。

「サポート詐欺」による被害が多数確認されております。

インターネット閲覧中（インターネットバンキング操作時）において警告音が鳴り、警告画面が表示されても安易に画面の指示に従わないでください。

画面に記載されている電話番号に電話をかけたり、**犯人側**が要求するセキュリティソフト等のダウンロードをしないでください。

偽の警告画面については、ブラウザを閉じたり、パソコンを再起動することで表示されなくなります。

注意事項につきましては、以下のページをご参照ください。

警視庁ホームページ

https://www.keishicho.metro.tokyo.lg.jp/sodan/nettrouble/jirei/warning_screen.html

国民生活センターホームページ

https://www.kokusen.go.jp/news/data/n-20220224_2.html

<インターネットバンキングに関するお問合せ>

TEL：06-6772-1525（平日のみ）

※ガイダンスに従ってお選びください。

操作に関するお問合せ ① 受付時間（9：00～22：00）

操作以外に関するお問合せ ⑨ 受付時間（9：00～16：00）

<時間外におけるお客様カード紛失等によるインターネットバンキング停止に関するお問合わせ>

しんきんATM監視センター

TEL：06-6454-6631（夜間・休日）

セキュリティ対策チェックシート

(ビジネスインターネットバンキングご利用のお客様)

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にご活用ください。

チェック項目		チェック欄
【パソコンの使用状況について】		
1	パソコンは当金庫の推奨環境内のOS (Windows) およびブラウザ(Internet Explorer 等)を使用している。	
2	信頼できるウイルス対策ソフトを導入し、最新の状態に更新し、定期的にウイルスチェックをしている。	
3	当金庫推奨の無料セキュリティ対策ソフト (Rapport) を利用している。	
【インターネットの利用状況について】		
4	パソコンは、インターネットバンキング専用で利用をする。	
5	パソコンの未利用時は電源を切断する。	
6	無線 LAN 使用時は、通信暗号化設定を行っている。	
7	複数の人が利用する共用のパソコンを使用したり、公衆回線 (Wi-Fi) を使用してインターネットバンキングを使用しない。	
【パスワード等の管理について】		
8	お客様カード・ID・パスワードは厳重に管理する。	
9	パスワードは、第三者に推測されにくいものを使用している。	
10	パスワードは、定期的に変更している。	
11	パスワードは、他のサイト等で使い回しをしない。	
12	パスワードは、パソコンやクラウド上に保存しない。	
【その他注意事項について】		
13	インターネットバンキングの1回、1日あたりの限度額は、最低限にし、必要時のみ限度額を変更する。 * 申込限度額内であれば、管理者で引下げが可能です。	
14	当日の資金移動(振込・振替)がなければ、当日の資金移動を停止しておく。 * 書面により停止可能 (ビジネスインターネットバンキング当日指定の資金移動(振込・振替)停止依頼書)	
15	Eメール通知の設定を行い、不審なログイン履歴や身に覚えのない取引履歴、取引通知メールがないか都度、確認する。	
16	心当たりのない発信元からの電子メールは絶対に開かない。 身に覚えのないメールの添付ファイル、本文中のURLはクリックしない。	
17	画面表示の警告(詐欺)の指示に従わない。	