

法人のお客さまのセキュリティ対策事例

法人のお客さまに取り組んでいただきたいセキュリティ対策は、以下のようなものです。当行では、法人のお客さまに下記1. に挙げる対策を実施していただくようお願いするとともに、2. の対策についても推奨しています。

1. 法人のお客さまに実施していただくセキュリティ対策

①銀行が導入しているセキュリティ対策を実施してください。

※現時点では、ソフトウェアキーボードや、サートネチズン、ワンタイムパスワードのことで、ご利用については任意のもの、必須のものが混在しておりますが、可能な限りご利用ください。



ソフトウェアキーボード



サートネチズン
当行HPから無料配布



ワンタイムパスワード
(ハードトークン)

②インターネットバンキングに使用するパソコンに関し、基本ソフト(OS)やウェブブラウザ等、インストールされている各種ソフトウェアを最新の状態に更新してください。

※パソコン立ち上げ時にアドビソフトやJAVA等のアップデートメッセージが出る場合は、もれなく更新してください。ウィンドウズ7のパソコンを8に買い換える等のことではございません。



③パソコンにインストールされている各種ソフトウェアで、メーカーのサポート期限が経過した基本ソフトやウェブブラウザ等の使用はお止めください。

※OS等には必ずメーカーによりサポート期限が設定されています。それが経過したOS等の使用を止めていただくということです。最近では、ウィンドウズXPとインターネットエクスプローラー(IE)6のサポート期限が平成26年4月9日に切れましたので、ウィンドウズXPのパソコンやIE6ブラウザソフトを利用したIB取引は止めてください。



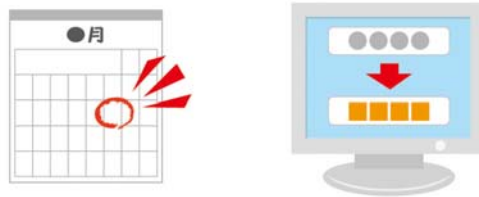
④パソコンにセキュリティ対策ソフトを導入するとともに、最新の状態に更新したうえで、ご使用ください。

※セキュリティ対策ソフトとは、具体的には、市販の「マカフィー」や「ウィルスバスター」、「ノートン」等のことです。当行では無料で「SaAT Netizen(サートネチズン)」というソフトも配布しておりますので、是非ご利用ください。



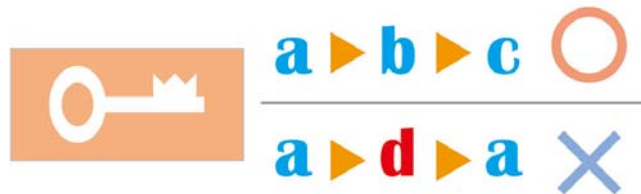
⑤インターネットバンキングに関わるパスワードを定期的に変更してください。

※どのくらいの頻度で行っていれば安全、という指標はございませんので、お客さまのご判断により変更してください。なお、当行のビジネスバンキングWebでは、90日ごとに変更をお願いする画面が出てまいります。



⑥銀行が指定した正規の手順以外での電子証明書の利用はお止めください。

※正規の手順とは、例えば、PCを買い換えた場合は銀行に届出いただき、電子証明書を再発行していただくことです。そのような手順以外では利用しないでください。

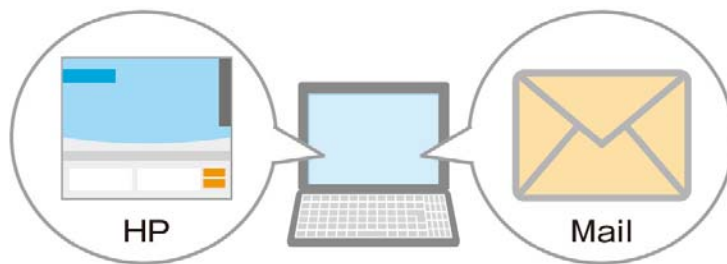


⑦不審なログイン履歴や、身に覚えがない取引履歴および銀行から送信するインターネットバンキングの取引に関する電子メールがないかを頻繁に確認してください。

※万が一、ネット犯罪に遭った場合に早期に発見するためにも、ご登録のアドレスを、頻繁に確認できるアドレス(例えば、携帯電話等)に変更することをおすすめします。



⑧銀行がホームページや電子メール等で注意喚起あるいは対応依頼した内容を確認し、実施してください。



2. 法人のお客さまに推奨するセキュリティ対策

①パソコンの利用目的として、インターネット接続時の利用はインターネットバンキングに限定してください。



②パソコンや無線LANのルータ等について、未利用時は可能な限り電源を切断してください。



③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。



④振込・払戻し等の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。

