令和４年３月

インターネットバンキングサービス
ご契約者さま　各位

大阪シティ信用金庫

コンピュータウィルスに関するご注意

日頃は、当金庫インターネットバンキングサービスをご利用いただき、誠にありがとうございます。

昨今、コンピュータウィルスによる被害は法人のお客さまのみならず、個人のお客さまにも全国的に拡大しております。

特に今年に入ってからは、「Ｅｍｏｔｅｔ」（エモテット）と呼ばれるウィルスが、実在する取引先や知人を装ったＥメールなどを媒介し、感染が拡がっています。

つきましては、コンピュータウィルスの感染対策などを、以下にまとめましたので、ご参考のうえ被害に遭われないよう、ご注意ください。

記

１．ウィルスに感染した（感染の疑いがある）場合

- ＬＡＮやＷｉ－Ｆｉによるインターネット接続を切断する。
- パソコンなど操作端末の電源をＯＦＦにする。
- 当金庫お問い合わせ電話番号に連絡をする。

受付可能時間	問い合わせ先	電話番号
平日 （午前９時～午後５時）	大阪シティ信用金庫 お取引店	店舗検索ページへ
平日 （午前９時～午後６時）	大阪シティ信用金庫 事務部	０６－６２０１－３０６１
平日（上記時間外） および土・日・祝日	しんきんＡＴＭ 監視センター	０６－６４５４－６６３１

＊お問い合わせの際には、ご利用口座の凍結やインターネットバンキングサービスの利用停止のご依頼にあたり、取引店、口座番号、口座名義、連絡者氏名についてお伝えください。

２．ウィルスに感染後の対処例

- 端末を購入した販売元や契約中の専門業者などに相談のうえ対処する。
- ご利用のセキュリティソフトによりウィルススキャン（駆除）を実施する。
- ウィルス添付メールを削除する。
- 端末を初期化する。

３．コンピュータウィルス「Ｅｍｏｔｅｔ」（エモテット）について

「Ｅｍｏｔｅｔ」は感染した端末内の情報を収集し、次の攻撃を引き起こすことを目的としたマルウェアとされています。

- 感染した端末からメールの内容やメールアドレス等の情報を収集する。
- 端末から収集した情報をもとに不正メールを送信する。
- 「Ｅｍｏｔｅｔ」に感染後、他のマルウェア（情報の窃取・身代金型のランサムウェア等）への感染を狙う。

４．お客様による主なセキュリティ対策

（１）パソコンやスマートフォンのアップデート

ＯＳのバージョンとセキュリティソフトは最新の状態で使用する。

（２）不審なＥメールやメッセージへの注意

取引先や知人からのメールであっても、受信が予定外であるなど不審な点があれば、開封前に発信元へ確認する。

５．当金庫による主なセキュリティ対策

（１）大阪シティ信用金庫から送信のＥメール

当金庫インターネットバンキングサービスにおけるＥメール配信では、クリックを促すようなＵＲＬや、開封が必要なファイルの添付はしておりません。

（２）不正操作による被害の未然防止

トランザクション認証対応のワンタイムパスワードサービスを採用し、専用トークンの操作により振込先口座を登録することで振込ができます。

以　上

問い合わせ先：大阪シティ信用金庫　事務部
電話番号：０６－６２０１－３０６１
（平日　午前９時～午後６時）