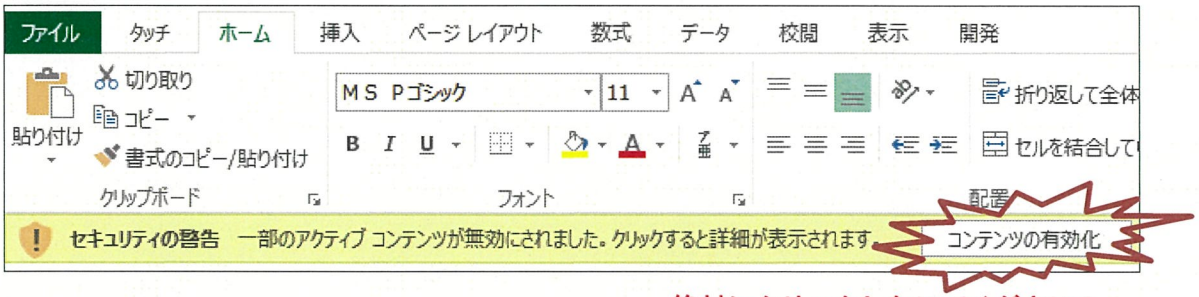
不審な電子メールにご注意ください！

非常に悪質なサイバー攻撃「Ｅｍｏｔｅｔ」（エモテット）」による被害が全国で多数確認されております。Ｅｍｏｔｅｔは、**メールに添付されたファイルの開封**や、メール本文に記載された**悪意のあるリンク（ＵＲＬ）を開く**ことで感染します。

Ｅｍｏｔｅｔの特徴は、過去に電子メールのやり取りをしたことのある、実在する相手の氏名、メールアドレス、メールの内容等の一部が、攻撃メールに流用され、**正規のメールへの返信を装う内容**であったり、巧妙な文面となっております。身に覚えのないメールの添付ファイル、本文中のＵＲＬはクリックしないようご注意ください。

Ｅｍｏｔｅｔの攻撃メールの添付を開くと**コンテンツの有効化**　**編集を有効にする**のボタンをクリックするよう指示が書かれています。不審なメールを開いた際には絶対に上記ボタンをクリックしないようにしてください。



絶対にクリックしないでください！

Ｅｍｏｔｅｔとは、非常に感染力・拡散力が強いマルウェアの一種で、情報の窃取に加え、他のウィルスへの感染を導く土台としても利用されるウィルスです。

Ｅｍｏｔｅｔの感染は、メールに添付されたファイルの開封や、悪意のあるリンクを開くことで活動を開始します。感染すると過去のメール情報が窃取され、過去のメールを引用し、返信を装った不正メールが作成され、更なるＥｍｏｔｅｔの拡散に悪用されます。

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。

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
http://www.shinkin.co.jp/info/security_01/index.html

※　万が一、不審なメールや添付文書を開いてしまった場合や不審な取引があれば、下記の番号まで至急、ご連絡ください。

＜平日９時～１６時＞
大阪信用金庫　事務集中部
０６－６７７２－１５２５　（ガイダンスに従い⑨をお選びください。）

＜夜間・休日＞
しんきんＡＴＭ監視センター（インターネットバンキングの停止）
０６－６４５４－６６３１

”

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	信頼できるウィルス対策ソフトを導入し、最新の状態に更新し、定期的にウィ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。**	