令和３年４月吉日

インターネットバンキングご契約のお客さま　各位

大川信用金庫

拝啓　春暖の候、ますますご健勝のこととお慶び申し上げます。平素は格別のご高配を賜り、厚く御礼申し上げます。

さて、インターネットバンキングにおきましては、様々な対応にもかかわらず、新たなマルウェアにより、不正送金の被害は継続して発生している状況であります。

そのような中、ゴールデンウィークを迎え長期休暇となるお客さまもいらっしゃるかと存じますが、その間を狙ったサイバー攻撃等にご注意していただきますようお願いいたします。

また、下記に留意すべき、セキュリティ対応策等を記載しておりますので、ご参考にしていただきますようお願いいたします。

なお、本件におきまして、ご不明な点などございましたら、当金庫業務統括部（０９４４－８６－６９１２）にお問い合わせください。

敬具

記

①テレワークに関するセキュリティリスク

新型コロナウイルス感染症対策の一環として、テレワークが大幅に普及してきていますが、機密情報の窃取やランサムウェアの感染につながる事案が発生しています。

チェックポイント

- インターネット等の外部ネットワークからアクセス可能な機器については、セキュリティパッチを迅速に適用する、管理機能、不要なポートを外部に開放しない等の管理策等、IT 資産管理を改めて確認する。
- 必要な監視強化や、攻撃を受けた場合の対応策をあらかじめ確認しておく。

- クラウドサービスを利用している場合は、設定ミスや不十分なアクセス制御、多要素認証不採用などによる脆弱な認証などを考慮し、管理者権限の認証情報を適切に管理する。
- テレワーク等に関連し、職場から持ち出したパソコンについて、休暇中に長期間、十分な管理下になかったパソコンを職場で再び利用する際は、セキュリティパッチの適用やウイルススキャンの実施など必要に応じて実施する。

②最近のマルウェアに関するセキュリティリスク

最近では、マルウェア「Emotet」に代わり、マルウェア「IcedID」による攻撃が活発になってきています。IcedID は、Emotet 同様、返信を装ったなりすましメールや料金の請求を装ったメールを用いる等、様々な手口で感染を試みます。海外では、新型コロナウイルス感染症のワクチン接種に関連するフィッシングメールが確認されています。

チェックポイント
- ランサムウェアによるサイバー攻撃について、予防策、感染した場合の緩和策・対応策などについてあらかじめ検討しておく。
- 人の不安や心理的な手口を利用したマルウェアによる攻撃が行われる可能性があることに留意する。

③長期休暇に伴うリスク

その他、長期休暇に伴う以下のリスクについて、必要な管理策の実施が必要です。

チェックポイント
- 長期休暇明けに行われる大量のメール確認による不注意がマルウェアの感染につながる不審メール等を開封するリスクがあるので注意する。
- 長期休暇中に確認・公表された脆弱性、関係機関からの提供情報、OS、ソフトウェア等への対応が遅延するリスクがあるので注意する。
- 長期休暇中のインシデントに対して監視の目が届きにくくなるリスクがあるので注意する。
- 長期休暇中に発生したインシデント等が適切に担当者に伝達されないリスクがあるので注意する。

以上