

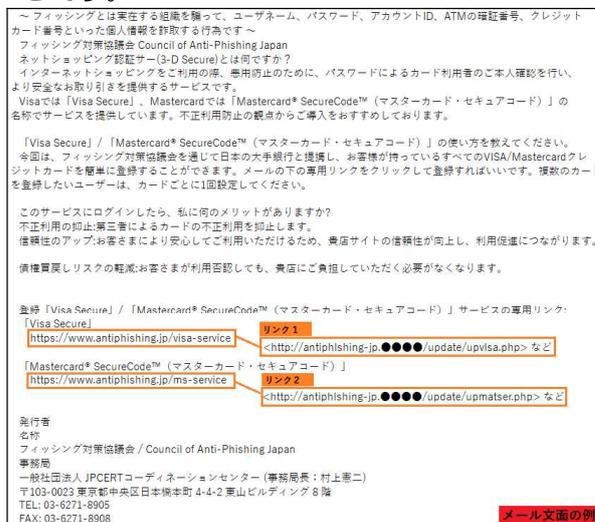
サイバーセキュリティ関連情報（6月号）

鳥取県警察本部サイバー犯罪対策課

○ フィッシング対策協議会をかたるフィッシングに注意！！

フィッシング対策協議会は、今年5月、フィッシング対策協議会をかたるフィッシングの報告を受けているとして注意を呼び掛けています。

この手口は、フィッシング対策協議会をかたるメールから、不正サイトに誘導し、クレジットカード情報等の入力を促すもので、「<重要>【フィッシング対策協議会】※全日本銀行によるネットショッピング認証サービス（3-D Secure）アップグレードに関するお知らせ」などの件名で送信されているとのことです。



【メール文面の例】



【誘導先サイトの例】

フィッシング対策協議会では、

- ・日頃から個人情報やクレジットカード情報の入力を要求された場合は、入力する前に一度立ち止まり、似たようなフィッシングや詐欺事例などがいないかを確認する。
- ・迷惑メールフィルターを活用する。

などの対策を呼び掛けています。

このようなフィッシングサイトにカード情報や認証情報を入力してしまうと、クレジットカードの不正利用や不正アクセスの被害に繋がりますので、十分に注意するようお願いいたします。

引用：【フィッシング対策協議会】 https://www.antiphishing.jp/news/alert/apc_20220506.html

○ QNAP社製のNASに対するランサム被害の発生！！

今年1月頃から発生しているNAS（ネットワークに接続された記憶装置）に対するランサムウェア「DEADBOLT」による攻撃について、5月13日から新型が登場し世界的に被害が発生しています。

このNASは、台湾の電気機器メーカーであるQNAP社が提供するものであり、攻撃を受けると、保存されているデータやシステム情報が暗号化され、使用不能となります。

国内においても中小企業を中心に被害が確認されており、業務上必要なデータが使用不能になる等、事業に大きな打撃を与えることとなります。

QNAP社のNASを利用されている企業や事業者の方は、

- ・QNAP社が提供する最新のアップデートを適用する。
- ・アップデートを行っていないNASをインターネットから直接アクセスできないようにする。

などの対策を行うようお願いいたします。

