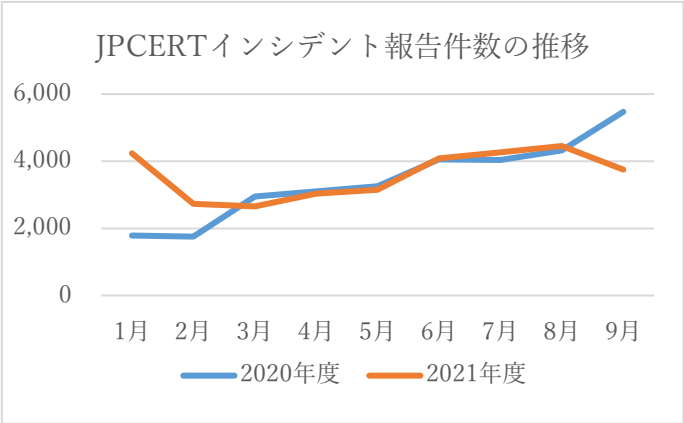
マンスリー・ハイライト　拝啓社長殿

マネジメントのための経営財務情報

第 610 号　この資料は全部お読みいただいて 2 分 30 秒です。

今回のテーマ：　高度化するフィッシング詐欺への対応について

2020 年以降の新型コロナウイルスの流行と DX（デジタルトランスフォーメーション）の加速度的な広がりによって、コロナ禍対策としてのテレワークをはじめとする IT 環境を急速に変化させている企業が増加している中、組織における IT 環境を狙った攻撃は前年度に引き続き高水準で推移しています。主なインシデントとして「E コマースサイトや金融機関を装ったフィッシングサイト」が全体の 7 割程度（前年度の 1.3 倍増加）を占めており、昨年度に引き続き情報流出の主要因として報告されています（一般社団法人 JPCERT /CC インシデント対応報告レポート[i]）。



2 段階認証の突破事例

金融機関でのネットバンキングサービス不正利用事例として、利用者を識別するための従来型パスワード認証方式と比較してより安全とされた E メールや携帯電話 SMS（ショートメールサービス）を組み合わせた「2 段階認証方式」がフィッシングサイトを用いた攻撃者により突破され、ネットバンキングサービスを悪用した不正送金が数多く報告されています。これらの事例では巧みに模倣したフィッシングサイトへ誘導された利用者から、2 段階認証に必要なワンタイムパスワードを詐取されたために生じています。

フィッシング被害に遭わないためには？

フィッシング被害に遭わないためには、フィッシング攻撃者がどのような手口を使うのかを知ることが被害を防止する重要な予防策となります。不適切な WEB サイトへのアクセスを防止するフィルタリング対策ソフトウェアなどの導入と共に、どれほど巧みに模倣したフィッシング手法であっても、①URL 欄に表示されるドメイン名が見慣れない国外ドメイン名ではないか、②メール本文に不自然な日本語や常用されない漢字（例:簡体字など）が利用されていないか、③ コロナ対策に乗じて従来とは異なる手法で情報を求めていないかなど、従業員レベルでの基本的な行動ルールの徹底がこれらの被害低減につながります。

お見逃しなく！

フィッシングサイト被害では自社の IT 環境におけるシステム障害は発生せず、組織内外からの情報漏洩が表面化しにくい側面があります。従業員個人が狙われるフィッシングメール、フィッシングサイトによる被害を防止するには、模擬演習が有効であるといわれています。演習を複数回実施し、まずは従業員がどのようなセキュリティ意識を持って行動しているのかを分析することが重要です。

[i] https://www.jpcert.or.jp/pr/2021/IR_Report20211014.pdf