認証取得・運用支援

標的型攻撃メール対応訓練

そのメール、開けちゃダメ！

標的型攻撃メールとは

特定の組織や個人を狙って情報窃取等を行う標的型攻撃が多くなっています。標的型攻撃メールは、あたかも正当な業務や依頼であるかのように見せかける件名や本文でメールが届き、受信者が騙されやすいような仕掛けをしています。

標的型攻撃メールによる被害

標的型攻撃メールを開封した受信者が、添付ファイルを開いたり本文に記載されているリンクをクリックすることでマルウェアに感染します。マルウェアから重要情報や個人情報が摂取されます。個人情報の漏えいにより訴訟や事後処理にかかる費用は膨大です。さらに、社会的信用を失い、取引停止や営業停止に追い込まれます。

標的型攻撃メールへの対策

標的型メール攻撃においては、マルウェアに感染しないことが最大の防御となります。標的型攻撃メールは巧妙に偽装されていて、怪しくないメールであることが特徴です。そのため、メールの確認ポイントをしっかりと身につけるための教育や、それを習慣化するための訓練を定期的に繰り返し行うことが効果的です。

標的型攻撃メール対応訓練の流れ

当サービスの範囲はこちら

1．事前教育	訓練の目的、標的型攻撃メールの見分け方、受信時の対応方法を説明・周知します。
2．標的型攻撃メール送信	標的型攻撃メールを送信します。
3．対応誤り検知	メール本文のリンクをクリックしたり、添付ファイルを開いてしまった受信者の検知を行います。
4．検知結果報告	検知した結果をご報告いたします。
5．事後教育	攻撃への対応を誤ってしまった受信者に再度説明・周知します。
6．アンケート	訓練に対するアンケートをとり、今後のセキュリティ強化に役立てます。

Q&A

Q. 事前教育、事後教育を実施したいが、何を説明したらよいかわからないのでお願いできますか？

A. セキュリティに関するいろいろな教育を当社で承っておりますので、ご相談ください。

Q. 訓練を依頼するにあたり、事前に準備しておくものはありますか？

A. 訓練対象者の受信可能なメールアドレスの一覧を用意してください。また、訓練実施前に送信テストを実施いたします。

Q. 検査結果はどのように提供されますか？

A. 標的型攻撃メール送信の翌日、3日後、1週間後にリストをお渡しいたします。リストの内容はメールアドレスと検知の有無、検知日時を一覧にします。

Q. 大量のメールがメールサーバに届くことがありますか？（メールサーバに負荷がかかりますか？）

A. 標的型攻撃メールが一斉に送信されることはありません。適度に間隔をとり、順次送信しますのでメールサーバへ大きな負荷はかかりません。

～ お問い合わせ先 ～

■担当 ： セキュリティビジネス部　セキュリティコンサルティングG
■mail ： 弊社ホームページの「お問い合せ」をご利用下さい。
■TEL ： 03-3496-1674（営業担当直通）
■URL ： http://www.cic-kk.co.jp/
■住所 ： 〒150-0043 東京都渋谷区道玄坂2-16-4（本社）