

サイバーコネクトSHIG@

今、注目のサイバーセキュリティに関する情報をお届けします。

Cyber connect shig@

標的型メールの情報提供をお願いします



滋賀県内事業者の皆様。今回は、標的型メールの情報提供のお願いです。

昨今、事業者に対するサイバー攻撃は、VPN機器の脆弱性やRDPの設定不備を突いた攻撃が多数を占めますが、フィッシングメールによる認証情報の窃取など、電子メール経由のサイバー攻撃もまだまだ多い状況です。

標的型メール攻撃は、一時期に比べると減少傾向にありますが、ある調査では、事業者に対するセキュリティ被害のうち、最も攻撃を受けた攻撃手法であったとの報告もあり、全く油断できない情勢です。

サイバー攻撃は日進月歩で、対策を講じればその対策をかくぐる攻撃が実行されるなどいたちごっこの様相です。サイバー攻撃と見られる通信を見分けるには、皆様からの情報提供が必要です。

提供していただきたいメール内容の例を上げますので、それぞれのお手元に同様のメールが届いたときは、当県警警備第一課サイバー攻撃対策係まで情報提供いただきますよう、お願いします。

情報提供いただきたいメール（例）

例1：他国企業名を名乗り、高額報酬と引き換えに、移籍、共同研究の呼びかけ、技術情報の提供を提示した。

例2：グループ企業の研究機関サポートチームを騙り、システム不具合により早急にパスワードを変更するよう勧める内容のメールが送付された。URLを押下させ、遷移後のページでIDとパスワードを窃取することが目的であった。同様のメールは他の事業者にも送付されており、同じ内容、同じ遷移先URLが記載されていた。

例3：取引先や関係先を名乗り、添付ファイルを開かせる内容

例4：就職希望を騙り、エントリーシートを開かせる内容

上記以外にも、事業者が標的となるものや技術情報の窃取を目的とした不審メールを受信されれば、遠慮なく情報提供をお願いします。職員個人へ送信されるメールもありますので、広く組織内へ呼びかけてください。

〈情報提供先〉 cyber-defense@police.pref.shiga.jp
(サイバー攻撃関係)

上記以外の、例えば、〇〇クレジットからの更新のお知らせ・・・などの一般的な不審メールは、サイバー犯罪対策課や各警察署及び全国警察サイバー事案相談等統一受付窓口へお願いします。

<https://www.npa.go.jp/bureau/cyber/soudan.html> (全国警察サイバー事案相談等統一受付)

◀ 留意事項 ▶

- 上記情報提供先に、会社(所属)名、お名前(担当者名)、連絡先を記載して送信してください。
- メールを転送するとメールヘッダが変わってしまいますので、メール本体をzipファイルなどに圧縮し、その圧縮したファイルをメールに添付して情報提供先へ送信してください。
- 情報提供いただいたメールの内容によっては、追加で調査協力をお願いする場合がありますので御協力をお願いします。
- 情報提供いただいたものすべてに回答するものではありませんので、御承知おきます。
- 滋賀県以外に拠点を有する事業者様は、所在地を管轄する警察に御相談ください。

◀CS情報SHIG@▶ フィルタリングを設定しましょう！！

滋賀県警察本部 警備第一課 サイバー攻撃対策係 077-522-1231 (代表)