滋賀県警察サイバーセキュリティ情報 RENEWAL
サイバーコネクトSHIG@
R４年度 No.1
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。

【警戒情報】
現下情勢を踏まえた
サイバーセキュリティ対策の強化を

昨今のサイバー攻撃事案の高まりを踏まえて、政府において３回にわたり「サイバーセキュリティ対策の強化」の注意喚起が出されています。（１回目: ２月23日、2回:目3月1日、3回:目3月24日）

国内では、ランサムウェアによる攻撃をはじめとするサイバー攻撃事案が続いているほか、「Emotet」によるウイルス感染が増加しています。

米国においては、バイデン大統領が、国内の重要インフラ事業者等に対して、ロシアが潜在的なサイバー攻撃の選択肢を模索しており、警戒を呼び掛ける声明を発表するとともに、企業等に対してサイバーセキュリティ対策を強化する具体策を提示しています。

- 滋賀県内においても、Emotetによるサイバー攻撃が多数確認されています。
  世界とつながる事業者も多く、サプライチェーン（供給網）は複雑化しています。
  海外から攻撃を受ける場合もありますし、他社が受けた攻撃の影響により、自社に影響が及ぶこともあります。昨今の情勢を踏まえると滋賀県内の一企業、一個人であっても、他人ごととは言えない状況です。この機会にぜひサイバーセキュリティ対策の点検、強化をお願いします。

参照：内閣サイバーセキュリティセンター「サイバーセキュリティ対策の強化について」
https://www.nisc.go.jp/pdf/press/20220324NISC_press.pdf

サイバーセキュリティ対策のポイント

① リスク低減のための措置
- **本人認証の強化**
- **脆弱性対策の強化**
- **組織内のユーザに対する注意喚起**

② インシデントの早期発見
- **攻撃の兆候及び被害の把握**

③ インシデント発生時の適切な対処・回復
- **被害の拡大防止**
- **事業継続の体制作り**

Emotet（ウイルス）感染拡大

メールの添付ファイルに注意してください。

滋賀県内で、Emotetと呼ばれているウイルス感染が多数確認されています。 ウイルス感染は、メールに添付されるファイルによって広がっているとみられます。

特にパスワード付きZIPファイルが添付されているメールには注意してください。

エモテット感染チェックツール「EmoCheck」

下記URLで無料でダウンロード可能です。

JPCERT/CC「マルウェアEmotetの感染拡大に関する注意喚起」
https://www.jpcert.or.jp/at/2022/at220006.html

【お知らせ】 サイバーコネクトSHIG@（シガ）

滋賀県警察では、県内のサイバーセキュリティ対策を強化する取組みとして「サイバーコネクトSHIG@」を開始します。

日々変化するサイバー空間の情勢において、セキュリティ対策は「一人」では難しくなっています。効果的なセキュリティ対策を行うためには、脅威情報やセキュリティ対策情報を活用することが重要です。

そこで、県警では、令和4年度から、多くの人や会社、団体、学術機関、行政機関と連携（コネクト）を強化し、情報発信、情報共有を一層推進していきます。

滋賀県のサイバーセキュリティ対策を推進し、インターネットを使った社会活動、経済活動をバックアップします。

«サイバーセキュリティ情報SHIG@»フィッシングによるクレジットカードの不正利用に注意してください。

滋賀県警察本部 サイバー犯罪対策課 077-522-1231（代表） 詳細は県警webページで →