滋賀県警察からのお知らせ

サイバーセキュリティ情報 CSI

事業者の皆さまに、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。

R３年度No.13

【警戒情報】 サイバーセキュリティ対策の強化を

国内外そして、県内においてサイバー攻撃が多数、確認されております。
昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられますので、下記の表を参考にサイバーセキュリティ対策の確認、強化をお願いします。
また、サイバー攻撃は、サプライチェーンによって多くの企業や団体に影響を及ぼします。国内だけでなく海外のグループ企業や取引先が踏み台にされて攻撃を受ける可能性もあります。

対策の項目	着眼点	具体的な確認・対策
リスク低減のための措置	本人認証の強化	□ パスワードが単純でないか □ アクセス権限の確認 □ 多要素認証の利用 □ 不審なアカウントの削除
	脆弱性対策の強化	□ Iot機器、VPN装置、ゲートウェイ等インターネットとの接続を制限する装置の脆弱性情報の確認 □ 脆弱性がある場合は、セキュリティパッチの適用、ファームウェアを含めてソフトウェアのアップデート　等
	組織内のユーザに対する注意喚起	□ メールの添付ファイルを不用意に開かない □ URLを不用意にクリックしない □ 連絡・相談を迅速に行う
インシデント（攻撃）の早期検知	攻撃の兆候及び被害の把握	□ サーバ等の各種ログの確認 □ 通信の監視・分析 □ アクセスコントロールの再点検
インシデント発生時の対処・回復	被害の拡大防止 事業継続	□ データ及びシステムのバックアップ □ バックアップからの復旧手順の確認 □ インシデントを認知した際の対処手順の確認 □ 対外応答や社内連絡体制の準備

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/press/pdf/20220301NISC_press.pdf

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。

感染チェックツール「EmoCheck」

Emotetに感染しているがどうかをチェックできます。下記URLで詳細閲覧できます。（ダウンロード可能）
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

«バックアップは必ず実施してください»

サイバー攻撃を受けると情報流出、システム破壊の被害が発生するおそれがあります。
重要データは必ずバックアップを実施してください。
なお、同一ネットワーク内のバックアップは、ウイルス感染のおそれがありますので、**オフライン**での**バックアップ**を行うようにしてください。
また、復旧手順も確認してください。

«随時受付»「体験型サイバーセキュリティセミナー」詳細は下記までご連絡下さい。

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）