

## サイバーセキュリティ情報

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。

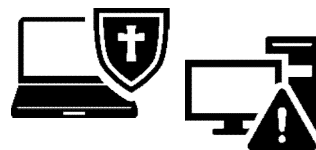
R3年度NO. 9

## 令和4年もサイバーセキュリティ対策を



新年、あけましておめでとうございます。

滋賀県警察では、益々進化するデジタル化社会において、事業者の皆さま、県民の皆さまが、安全安心に事業活動、社会活動が行えるようにサイバーセキュリティ対策を推進してまいります。今年もよろしくお願いたします。



## 最近のサイバー攻撃事例

近年、サイバー攻撃を完璧に防ぐことは困難と言われています。

サイバー攻撃による情報流出やシステム障害は、事業継続に大きな影響を及ぼしますので、攻撃を受けても最小限の被害に抑える対策及び攻撃を受けた後の対応方法を検討しておくことが重要です。また、操作ミスや設定不備による情報流出も発生していますので、注意をお願いします。

業種	情報流出件数	概要等
衣料通販	クレジットカード情報等 約800件	脆弱性を突かれてWebサイトが改ざんされ、不正なファイルを置かれた。またクレジットカード情報等が外部に流出した。(12月)
書籍販売	顧客メールアドレス 約90件	顧客にメールを送信した際、設定ミスにより別の顧客のメールアドレスが閲覧できる状態になっていた。(11月)
インテリア販売	クレジットカード情報等 100件以上	脆弱性を突かれて決済アプリケーションが改ざんされ、クレジットカード番号、有効期限、セキュリティコード、会員ID、パスワードが流出した。(10月)
観光	不明	ランサムウェア攻撃により、サーバや端末に保存していた業務関連情報や個人情報暗号化された。情報が外部に流出したおそれがある。(9月)
金融	顧客情報 約200件	顧客情報を管理するクラウドサービスの設定不備により、外部からの不正アクセスが発生し、顧客情報が外部に流出した。(8月)

## ～緊急性の高い脆弱性情報～

「Apache Log4j」に深刻な脆弱性  
バージョン確認とアップデートを！

Javaを使っているWebサイトやサービス、ソフトウェアを運用されている方は、バージョンアップの確認とアップデートをお願いします。

「Apache Log4j」は、ログを出力するライブラリで、多くのサービスに使用されています。

昨年11月に、Log4jに脆弱性が見つかりました。

この脆弱性では、特定の文字列が「ログ」に含まれた場合に、システムが自動的に外部と通信を行ってしまい、外部から任意のコードが実行できるようになり、ウイルス感染や遠隔操作のおそれがあります。

脆弱なバージョンを使用している場合は、最新バージョンへのアップデートが強く推奨されています。

参照：日本サイバー犯罪対策センター「脅威情報」

<https://www.jc3.or.jp/threats/topics/article-418.html>↑昨年下半年に、公表された主なサイバー攻撃による情報漏えい事案（インターネットで公表された情報を元に作成。）  
※カッコ内は公表された月を表す。クレジットカードの  
不正利用に注意してください。

クレジットカードが不正に利用され、知らない間に商品を購入され、購入代金を請求されるという事案が発生しています。

フィッシングサイトに騙されて、クレジットカード情報を入力してしまうケースがありますので、クレジットカード情報の入力には注意してください。

また、利用明細を定期的に確認して、身に覚えのない支払や請求があった場合は、速やかにクレジットカード会社に連絡してください。

≪随時受付≫「事業者向け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)