福岡県警察からのお願い

注意喚起 個人情報漏えいによる二次被害を防ぐ！

企業を狙うサイバー攻撃により、大規模な個人情報の漏えいが多発しています。
個人情報を悪用した「二次被害」へ注意を払ってください。

想定される主な二次被害

1 【フィッシングメール】

漏れたメールアドレスや電話番号宛てに、官公庁や企業を装った偽メール・SMSが届き、偽サイトへ誘導され、更に個人情報を盗まれる。



2 【不正アクセス】

漏れたIDやパスワードと同じパスワードを使用している他のサービスに不正アクセスされ、保有する資産を勝手に売却・送金される。



3 【不正利用】

クレジットカード情報を不正利用されて、買った覚えのない買い物の請求が来る。



4 【なりすまし】

本人確認書類の画像を悪用される「なりすまし」により、登録したことのないショップから会員登録の確認メールが来る。



今日からできる主な対策

1 パスワードの使い回しをしない。 【防げる被害】:不正アクセス・不正利用

攻撃者は漏えいしたリストを使い、様々なサイトへのログインを試みます。
使い回しを避けることで「不正アクセスの連鎖」を防ぐ。

2 「パスキー」や「多要素認証」の活用 【防げる被害】:不正アクセス・なりすまし

指紋や顔認証等の「パスキー」や「多要素認証」を活用し、犯人の侵入をブロックする。

3 メール内のリンクは押さない。 【防げる被害】:フィッシングメール

不安をあおる偽メールが送られてくる可能性があるため、メール内のリンクは避け、常に「公式アプリ」や「ブックマーク」からアクセスする。

4 個人情報の登録は最小限に 【防げる被害】:なりすまし

使用しなくなったアカウントは削除するなど「攻撃される的(まと)」を減らす。

注意喚起 情報が漏えいした際の対応

情報が洩れたら、放置せず、速やかな対応を！

情報が漏えいした際の主な対応例

1 ID・パスワードが漏えいした場合 ～不正にログインされるおそれ～

- 対象サービスのパスワードを速やかに変更する。
- 同じパスワードを使う他のサービスも変更する。
- パスキーや多要素認証を設定する。



2 クレジットカードが漏えいした場合～身に覚えのない決済のおそれ～

- すぐに該当するカード会社へ連絡する。
- 不正利用の確認と、利用停止・再発行を相談する。
- 利用明細を定期的に確認する。



3 氏名・住所・メール・電話番号・本人確認書類の情報が漏えいした場合 ～偽メール・詐欺電話・なりすまし契約などに警戒～

- 突然のメールやSMSは偽メールの可能性が高いことを認識する。
- メール内のURLは絶対に押さない。
- 身に覚えのない不審な郵便物などは受け取らない。
- 不正契約のリスク軽減のため、各信用情報機関への本人申告（漏えい事実の登録）を検討する。

※ 不正な契約や不正利用を必ず防げるものではありません。



最新脅威の把握と防犯ツールの活用

- **福岡県警察防犯アプリ「みまもっち」のインストール** 【みまもっち】

  国際電話や警察が把握した犯行使用電話をブロックし、詐欺電話対策として有効。

- **公式X（旧Twitter）等による最新手口の把握** 【国家サイバー統括室】【X】

  福岡県警察公式SNSや、国家サイバー統括室公式Xアカウント等を確認し、最新のサイバー犯罪の手口について把握する。

少しでも「不安」と思ったら、迷わずに相談を！

最寄りの警察署又は警察相談専用電話「＃9110」番に連絡。

福岡県警察サイバー犯罪対策課