サイバー攻撃による
～個人情報の漏えい～

その後、想定される

☑ 犯罪被害事例

☑ 被害防止対策



三重県警察

～漏えいした個人情報の悪用による更なる被害を防ぐために～

- ☑ **「警察庁推奨アプリ」を直ちにインストール！**
- ☑ **自宅の防犯性能を高める！**
- ☑ **メール内のリンクを安易にクリックしない！**
- ☑ **安全なパスワードを設定して使い回さない！**

事業者や団体、企業等を狙うサイバー攻撃により、大規模な個人情報の漏えい事案が多発しています。

また、フィッシングや不正アクセス等により、個人からも個人情報が漏えいしています。

「知らない間に自分の個人情報が漏えいしている」ことを前提に、常に「電話の相手は漏えいした情報を悪用した詐欺犯人かも」と注意を払ってください。

皆様が安全・安心に日々の生活を送る上で、想定しておくべき『犯罪被害事例』と、それらを防ぐための『被害防止対策』をまとめたので、参考にして対策を講じてください。

特殊詐欺

【悪用される漏えい情報】
住所、氏名、電話番号、メールアドレス、金融資産、家族構成等

想定される事例

- 警察官等を装った電話があり、「あなたの流出した情報で被害者が出ています。捜査に必要なので、あなたのキャッシュカードと通帳を預かります。」などと言われ、金品をだまし取られる。
- ＳＮＳのダイレクトメッセージやメールが来て、投資の専門家などを名乗る犯人のトークグループに招待され、簡単に投資でお金を増やせるかのように誤信させられ、多額の金銭をだまし取られる。

被害防止対策

□ 国際電話不取扱受付センターへの申込みにより、固定電話にかかる犯人からの電話をブロックしましょう。

□ 「警察庁推奨アプリ」を直ちにインストールして、スマートフォン等への犯人からの電話をブロックしましょう。

□ 電話やＳＮＳ上でお金の話をされたら、詐欺です。最寄りの警察署又は＃９１１０（警察相談専用電話）に相談しましょう。

警察庁推奨アプリ

携帯電話、スマートフォンへの国際電話経由による詐欺電話や犯行に利用した電話番号をブロックします。

警察庁推奨特殊詐欺対策アプリ

詐欺対策 by NTTタウンページ　／　詐欺バスター Lite TREND

国際電話不取扱受付センター

固定電話への国際電話の発着信を利用停止することで、自宅への詐欺電話をブロックします。

電話番号： 0120-210-364
自動音声案内： 平日、土日祝 24時間
オペレータ案内： 平日 9:00～17:00



三重の詐欺防ぎ隊
サギかもしか

このページで紹介した対策に加えて、三重県警察が発信する防犯情報をチェックしよう！

Ｘ（旧Twitter）
三重県警察本部犯罪抑止対策係公式Ｘ

Lorcle（ロークル）

Yahoo!防災速報アプリ

フィッシング

【悪用される漏えい情報】
氏名、メールアドレス、電話番号

想定される事例

漏えいしたメールアドレス、電話番号に対して、実在する有名企業や官公庁を装ったメールやＳＭＳが送付されて、本物そっくりのサイトへ誘導され、更に個人情報を盗まれる。

被害防止対策

□ 不安をあおるような内容のメール・ＳＭＳは「だまそうとしているのではないか」と疑いましょう。

□ メール等に記載のリンクは安易にクリックしないようにしましょう。

□ 公式アプリやブックマークから正規のサイトにアクセスして確認しましょう。

メール内のリンクを安易にクリックしない！

【フィッシングの手口】

① 実在する企業を名乗るメール・ＳＮＳが届く。
② 記載のリンクをクリックすると、偽物のサイトが開く。
③ 偽物のサイトで、ログインＩＤ・パスワード、クレジットカード情報などの個人情報の入力を要求される。
④ 入力した情報を悪用されてしまう。



動画で確認

フィッシングの手口と対策を動画で確認しましょう。

※ 下記二次元コードを読み込むと「警視庁公式ホームページ」にアクセスします。

スマホによる個人情報流出「偽サイト誘導情報」
偽サイトに誘導して情報を盗み出す手口や、その対策について確認できます。

巧妙化するフィッシング詐欺「偽サイト誘導編」
ショッピングサイトを装うフィッシングメールの手口と対策について確認できます。

巧妙化するフィッシング詐欺「金融機関を装ったSMS編」
金融機関を装うフィッシングメールの手口と、その対策について確認できます。

不正アクセス・なりすまし
不正利用

【悪用される漏えい情報】
住所、氏名、生年月日、電話番号、クレジットカード番号・セキュリティコード、本人確認書類・画像、ＩＤ・パスワード等

想定される事例

- 漏えいした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で不正アクセスされ、保有する資産を勝手に売却・送金される。
- 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。
- 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。

被害防止対策



□ パスワードは英数字や記号を含んだセキュリティ強度の高い安全なパスワードを設定して使い回さないようにしましょう。

□ パスワードが漏えいした場合は速やかに変更しましょう。各種カード情報が漏えいしたおそれがある場合は、カード会社や銀行などに連絡し、必要に応じて停止・再発行手続きをしましょう。

□ 知識情報（ＩＤやパスワード）、所持情報（カードやスマートフォン）、生体情報（指紋や顔）のうち、２つ以上の要素により認証を行う「多要素認証」を活用しましょう。

□ 指紋認証や顔認証、パスキーを活用しましょう。

□ ログイン時やクレジットカード利用時の通知サービスを利用するとともに、ログイン履歴やクレジットカードの利用明細を定期的に確認し、身に覚えのないログインやクレジットカードの利用がないかを確認しましょう。

□ クレジットカードの本人認証サービス（３Ｄセキュア）に登録するとともに、銀行やクレジット会社から身に覚えのない認証メールやＳＭＳが来た場合は絶対に認証しないようにしましょう。

基本的なセキュリティ対策

警視庁公式ホームページ「サイバーセキュリティインフォメーション」で基本的なセキュリティ対策を確認しましょう。

※ 右記二次元コードを読み込むと「警視庁公式ホームページ」にアクセスします。

強盗・侵入窃盗
悪質訪問業者による飛び込み営業

【悪用される漏えい情報】
住所、氏名、電話番号、本人確認書類・画像、金融資産、家族構成等

想定される事例

- 資産状況等から標的対象として設定され、生活状況調査、訪問販売等を装い家屋内の状況を探るなどして強盗・侵入窃盗被害に遭う。
- 悪質訪問業者からの飛び込み営業を受け、「屋根や分電盤の修理・交換が必要」などと言われ、本来は必要のない工事の契約をさせられる。

被害防止対策

☐ 不審者の徘徊等があった場合は、すぐに警察へ通報しましょう。

☐ 家の玄関等にマーキングがされていた場合は写真を撮った上で、マーキング箇所をすぐに消し、警察に通報しましょう。

マーキング事例

「マーキング」とは、犯罪の下見活動の可能性のあるしるし等をいいます。
必ずしも犯罪に直結するとは言えないものの、防犯対策の観点から注意が必要です。





☐ 在宅中でもドアや窓の施錠を徹底し、各種防犯設備を設置して、自宅の防犯性能を高める。

☐ 悪質訪問業者が自宅を突然訪問して来た際は、ドアを開けずに対応し、身分や用件を確認して、無料と言われても点検はさせない、その場で契約をしないようにしましょう。

自宅の防犯性能を高める

- 自宅玄関及び窓を常時施錠し、補助錠を取り付ける。
- 見通しの良いフェンス、センサーライト、カメラ付きインターホン等を設置する。

【センサーライト】



【カメラ付きインターホン】



- 防犯性能の高い建物部品（ＣＰ部品）を活用する。

【CPマーク】

【ＣＰ部品とは】
警察庁等関係省庁及び建物部品関連５団体による官民合同会議において、基準値以上の防犯性能を有すると認定されたガラス等の建物部品をいう。

三重県警察の防犯情報

三重県警察本部生活安全企画課が最新の情報をお届けする情報発信ツールです。ダウンロード・フォローで、あなたの毎日に安全・安心をプラス！

X（旧Twitter）

三重県警察本部犯罪抑止対策係公式X

Lorcle（ロークル）

中日新聞が運営する自治体や事業者等の情報発信のためのプラットフォーム

Yahoo!防災速報アプリ

地震や津波、集中豪雨等の人命に関わる必要な防災情報を配信するアプリ

複数の対策を組み合わせることで防犯力を高めて、自分と大切な人達の安全・安心な生活を守りましょう！



犯罪抑止対策犬