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



広島県警察本部

～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」や広島県警察安全安心アプリ「オトモポリス」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、個々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」と注意を払って下さい。

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下さい。

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、投資の専門家や有名人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、固定電話への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、携帯電話・スマートフォンへの犯人からの電話をブロックしましょう。

☐ 広島県警察安全安心アプリ「オトモポリス」をダウンロードして、特殊詐欺の最新の手口をチェックしましょう。

☐ 電話やSNS上でお金の話をされたら、詐欺です。最寄りの警察署に相談しましょう。

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

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

広島県警察安全安心アプリ「オトモポリス」

迷惑電話ブロック機能のほか、特殊詐欺の最新手口など、防犯に役立つ様々な情報・機能が満載のアプリです。

スマホであなたに“オトモ”する
広島県警察安全安心アプリ
オトモポリス

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

・　資産状況等から強盗等の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。

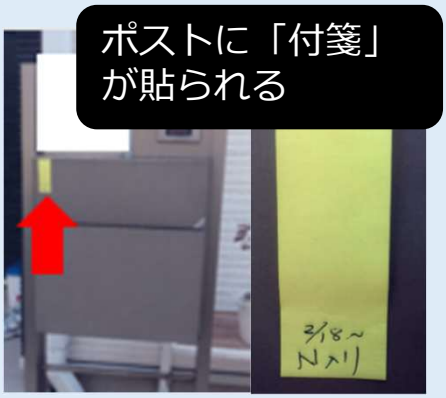
被害防止対策

☐ 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、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印等をいいます。
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、その場で即決して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。
・ 防犯性能の高い建物部品（CP部品）を活用する。


【センサーライト】



【カメラ付きインターホン】

【CPマーク】


【見通しの良いフェンス（例）】

【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、錠、ドア等の建物部品をいう。

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。

☐ メールやSMS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！

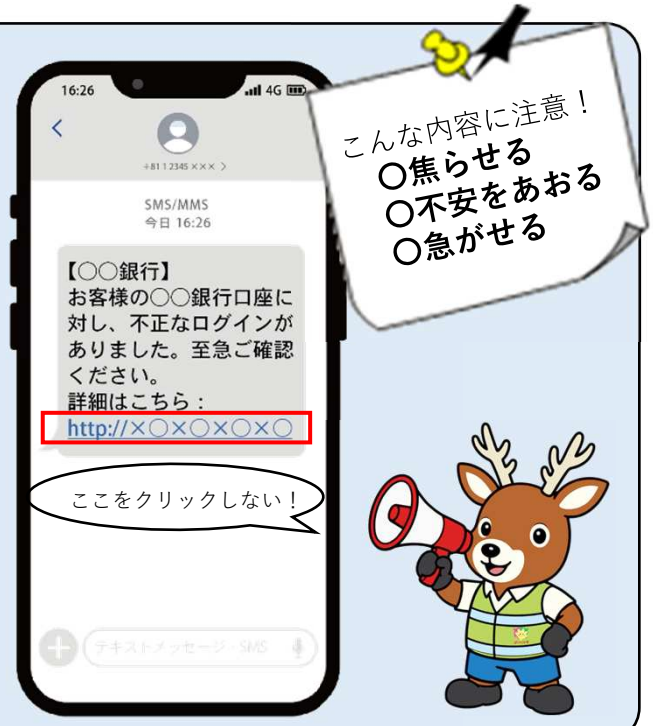
【フィッシングの手口】

① 実在する企業を名乗るメール・SMS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。（警視庁ホームページにリンクします。）

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、覚えのない買い物の請求が来る。

被害防止対策



☐ パスワードは数字のみではなく、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、端末に紐付けられて保存されている暗証番号などを使ってログインする「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

広島県警察のホームページで、基本的なセキュリティ対策を確認しましょう。

メール相談等（サイバー犯罪に関する相談、偽サイト等の通報先）

ホームページ内で、サイバー犯罪に関する相談について、メール相談を受け付けています。

※執務時間外（平日の午後５時１５分から翌日午前８時３０分、土曜日、日曜日、祝日）に送信された場合、翌執務日以降の受付となります。

その他の被害（ストーカー、脅迫・恐喝、嫌がらせ等）

【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、勤務先・役職、位置情報・行動履歴等

想定される事例

・ ストーカー被害に遭い転居していたが、漏えいした情報から加害者に転居先の現住所を知られてしまい、更なるストーカー被害に遭ってしまう。
・ SNS上での公開情報やダイレクトメッセージによるやりとりで一方的に妬みの感情を持った相手から、漏えいした位置情報・行動履歴等を家族や職場に知らせるとの脅迫被害に遭う。
・ 漏えいした情報を入手した見ず知らずの相手から、悪意の感情による無言電話や中傷行為、つきまとい行為を受ける。

被害防止対策



□ 不審な人物に待ち伏せ・つきまといをされていることに気づいたら、すぐに１１０番通報しましょう。

□ 嫌だと思うことについて、相手方にはっきりと意思表示をしましょう。難しい場合は、一人で悩まずに、早めに周囲の家族・友人、警察へ相談しましょう。

□ 「相手が押し掛けてきた」、「電話がかかってきた」等、相手にされたことの日時や場所、内容などを記録しておきましょう。

□ ストーカー事案は、相手の行動が急にエスカレートして重大な犯罪につながる危険性があるため、自分や家族等の大切な人の身を守るため、相手方が知らない場所や一時保護施設に避難することも考えましょう。

□ 「SNSやブログの更新を控える」、「スマートフォンのGPS機能をオフにする」、「郵便物を捨てる際はシュレッダーに掛ける」など、更なる個人情報の流出防止に努めましょう。

□ 自分が公開していない個人情報やプライベートな画像が、インターネット上などに公開されていることを発見したら、サイト管理者等に削除依頼をしましょう。

□ 電話に相談「不安だな」と思ったら、お住まいを管轄する警察署又は警察安全相談電話に相談しましょう。

広島県警察警察安全相談電話

※ 相談は最寄りの警察署でも直接受け付けています。

相談内容に応じて相談窓口等をご案内します。

電話番号：＃９１１０

（広島県内でダイヤルすると、広島県警察の相談電話につながります。）



警察庁推奨アプリ【特殊詐欺対策】

直ちにインストールして、詐欺電話をブロック！

詐欺対策 by NTTタウンページ

詐欺バスター Lite TREND

迷惑電話ブロック機能のほか、防犯に役立つ様々な情報・機能が満載のアプリ！

スマホであなたに“オトモ”する
広島県警察安全安心アプリ
オトモポリス

広島県警公式SNS

広島県警察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　Facebook　Instagram　YouTube

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！

