

金融機関をかたるフィッシングメールに注意！

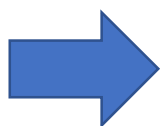
北海道内の金融機関をかたるフィッシングメールが急増しています。
金融機関をかたるSMS（ショートメッセージサービス）に記載されているURLにアクセスすると、金融機関の**偽ホームページ**に誘導され、口座番号や暗証番号、個人情報などが盗まれ、**インターネットバンキング不正送金・口座の不正利用**などの被害にあってしまいます。
不審なSMSに記載されたURLには、**絶対にアクセスしない**でください。

【金融機関をかたるフィッシングメールの例】



【〇〇〇銀行】
重要なお知らせ、必ずご確認ください。
<https://〇〇-bank.co/〇〇>

URLにアクセスすると・・・



〇〇〇銀行

口座番号

暗証番号

偽

偽ホームページに誘導
口座番号などが盗まれる

フィッシングの被害に遭ってしまったら・・・

- その金融機関に連絡する
→ 口座の利用停止措置を行い、被害拡大を防止
→ 被害の補償についての相談
- パスワード等を変更する
→ 二次被害防止のため、**別サービス**のパスワードなどを変更
→ パスキー・多要素認証の導入
- 警察に通報・相談する
→ 最寄りの警察署や相談ダイヤルに通報・相談



北海道警察 H P
サイバーセキュリティ広場

北海道警察



YouTube動画
サイバーセキュリティ講座



そのメール、フィッシングかも！

こんなメールやSMSに要注意！

From：XYZ銀行
件名：【重要】取引停止のお知らせ

本人かどうか確認が取れない取引がありましたので停止しました。
確認してください。
<http://xyz-bank.com>

取引の停止



From：XYZカード
件名：【緊急】不正アクセスを検知しました

第三者からの不正なアクセスを検知しました。
確認してください。
<http://xyz-card.com>

不正アクセス



050xxxxxxx

お荷物のお届けがありましたが、不在の為持ち帰りました。
<http://xxx.com>

不在持ち帰り



メールやSMSによるフィッシング被害が発生中！！



フィッシングに騙されるとどうなるの？

銀行等を装ったメールやSMSから偽のウェブサイトに誘導され、金融情報や個人情報を不正に盗まれると・・・



- 銀行口座を操作されて勝手に送金される
- ECサイトで勝手に買物をされる
- アカウントを乗っ取られる

フィッシングに対してできること



- メールやSMSに記載されたリンクをクリックしない
→ 内容の確認は、公式サイトやアプリを利用する
- パソコンやスマートフォンを安全な状態に保つ
- 携帯電話会社等の迷惑メッセージブロック機能を活用する
- ID・パスワードの使いまわしはしない
- ワンタイムパスワード等を活用する

※詳細なフィッシング対策はこちら⇒

<https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html>



北海道警察



フィッシングの被害拡大中！！



そのメールは本物ですか？

フィッシングメール（なりすましメール※）のリンクをクリックして、

※なりすましのSMSも含みます。

「銀行預金を不正に送金された」

「クレジットカードを不正に利用された」

という被害が後を絶ちません。

！ フィッシングメールの特徴

- ✓ 正規のメールと見分けることが困難。
- ✓ 【重要】、【不正アクセスを検知】、【取引を制限】等のタイトルで不安にさせ、リンクをクリックさせようとする。
- ✓ 宅配業者、金融機関、通信事業者、ネットショップ、官公庁等の実在の企業等を装う。

フィッシング被害に遭わないためには？

- ➡ メールやSMSに記載されたリンクをクリックしない。
- ➡ 内容を確認するときは、公式サイトやアプリを利用する。
- ➡ 携帯電話会社等の迷惑メッセージブロック機能を活用する。

《 フィッシングメール対策動画 》



制作：サイバーセキュリティ対策本部



フィッシング詐欺って
知ってますか？



制作：北海道警察学生ボランティアJumpers

北海道警察

YouTube動画
サイバーセキュリティ講座
公開中です！

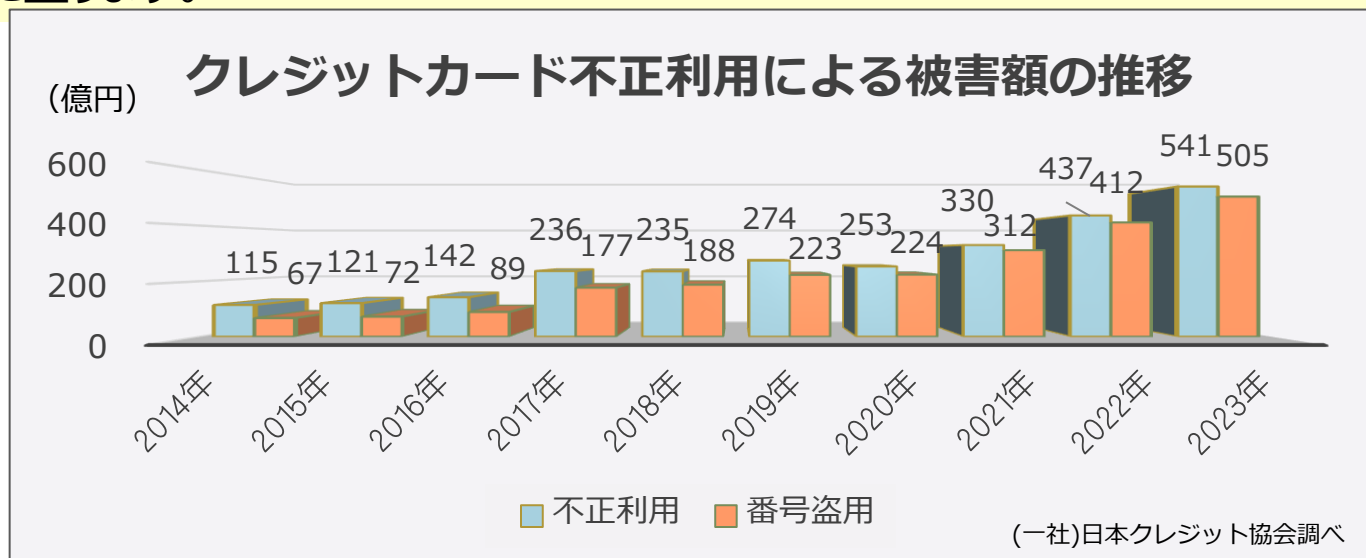


北海道警察公式HP
サイバーセキュリティひろば

クレジットカードの不正利用が多発！

クレジットカードの不正利用は、年々増加の一途をたどり、2023年の**被害額**は**540億円**に達しました。

そのうちの**93%**を「**クレジットカード番号盗用**」が占め、被害額は**505億円**に上ります。



クレジットカード番号盗用の主な手口は？

- ◆ **フィッシング詐欺**：カード会社や宅配便業者などをかたったメールを送りつけ、偽サイトに誘導し、カード情報を盗み取り、不正に利用する。
- ◆ **ネット通販詐欺**：ネット通販サイトの購入手続きを装ってカード情報を盗み取り、不正に利用する。

特に多いのが以下のような「フィッシングメール」です

不正利用



From：XYZカード
件名：不正利用について

不正な利用がありました。
至急確認してください。

<http://xyz-card.com>

高額当選



090xxxxxxx

大当たり！！
賞金〇億円が当選しました。
受取手続きはこちら
080xxxxxxx

不在持ち帰り



050xxxxxxx

お荷物のお届けがありました
が、不在の為持ち帰りました。
再配達はこちら
<http://x-unsou.com>

被害に遭わないための対処法等

- ◆ メールに記載されたリンク（URL）からサイトにアクセスしない。
- ◆ ログインする際は、「公式ホームページ」を検索したり「公式アプリ」を使用する。
- ◆ ID・パスワードは使い回さず、パスキーや多要素認証を導入する。
- ◆ 被害に気付いたら、すぐに情報を入力したカード会社や金融機関等へ連絡する。



被害に遭った場合は、所在地を管轄する警察署に通報を！

北海道警察・北海道クレジットカード犯罪対策協議会

