

＜インターネットバンキングご利用者さまは要注意＞

突然の詐欺行為、 焦らず対応できますか？

－ 目次 －

フィッシング詐欺・・・・・・・・・・ P.1

サポート詐欺・・・・・・・・・・ P.3

架空料金請求詐欺・・・・・・・・・・ P.6

**お客さまご自身やご家族の資産を守るため、
本資料で詐欺行為についての理解を深めてください！**



DAISHI HOKUETSU
Financial Group

第四北越フィナンシャルグループ



フィッシング詐欺

突然ですが

こんなメールが届いたら、どうしますか？



[緊急] インターネットバンキングの
IDとパスワードが漏えいしています！

第四北越銀行から緊急のお知らせです。
ご利用中のインターネットバンキングのIDとパスワードが漏えいしています。
至急、下記URLからIDとパスワードの変更を行ってください。

<http://www.dhbk.....>

ID	
パスワード	
ログイン	

URLをクリックし、パスワードを変更する？



フィッシング詐欺

絶対にID・パスワードを入力しないでください！

それ「フィッシング詐欺」です！！

- 「フィッシング詐欺」とは、実在する企業等を詐称したメールやSMSで偽サイトに誘導し、**IDやパスワード等の情報を盗み取る**詐欺行為です。
- インターネットバンキングのアクセス情報の他にも、銀行の口座番号と暗証番号、住所や氏名等、クレジットカード情報を盗み取ろうとしてきます。
- 最近では、**金融機関職員を騙り電話音声で**メールアドレスを聞き出して、フィッシングメールを送る「**ボイスフィッシング**」が新たな手口として確認されています。



メール等に記載されたURLはクリックしない

偽サイトは、見た目やURLが正規のサイトに似せて作成されることも多く、一見して**偽サイトだと見破ることが難しい**場合があります。あらかじめ**正規サイトをブックマーク**しておき、**メール等に記載されたURLはクリックしない**ようにしましょう。



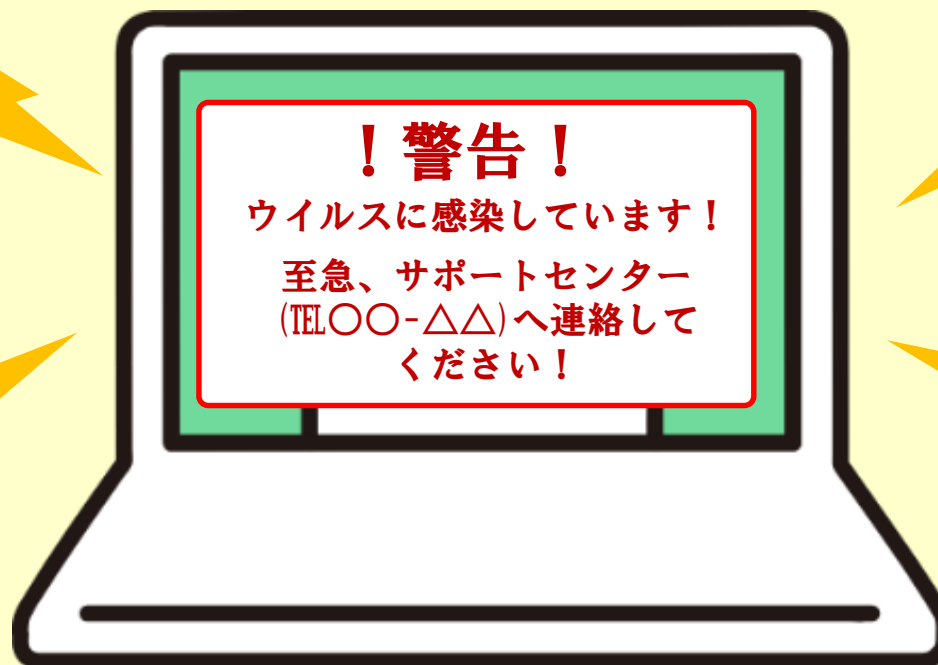
金融機関等がIDやパスワードを聞き出すことはない

金融機関や警察、サポートセンター等の職員が、IDやパスワードを聞き出すことはありません。そのような行為は詐欺である可能性が極めて高いです。



突然ですが

こんな画面が表示されたら、どうしますか？



表示されたサポートセンターへ連絡する??



サポート詐欺

警告画面の指示内容には従わないでください！

それ「サポート詐欺」です！！

- 「サポート詐欺」とは偽の警告画面や警告音を鳴らすことで不安を煽り、**警告画面に表示された電話番号まで連絡させる**手口です。
- 電話をかけてしまうと、**嘘の有償サポート**として資金の振込を指示されます。また、セキュリティソフトと偽って**遠隔操作ソフトをインストールさせられ、パソコンが乗っ取られる**ことで、資産を騙し取られることもあります。



表示された電話番号には連絡しない

警告画面は、ウイルス感染の有無に関わらず表示されます。表示された電話番号には連絡せず、**パソコンの販売元担当者や正規のサポートセンターへ連絡**してください。



(電話をかけてしまったら) オペレーターの不審点に気づく

電話をかけてしまった場合に備え、“何か変だ”と気づくポイントを知っておきましょう。**金銭の要求、インターネットバンキングのID・パスワードを聞き出そうとする行為は詐欺**です。**オペレーターが外国人であるケースも多い**ので、外国人だった場合は特に注意が必要です。



次ページで、「警告画面」の消し方・対処法を説明します！



警告画面は以下の方法で消すことができます

落ち着いて以下の操作を試してみてください

- サポート詐欺に用いられる警告画面は、**全画面で表示され、マウス操作でページを閉じることが中々できない**といった特徴があります。
- マウス操作で画面が閉じれない時は、次の**キーボード操作（ショートカットキーの活用）**を試してみてください。



全画面表示を解除し、ページを閉じる

キーボード左上にある「**Esc（エスケープ）**」キーを長押し（**2～3秒間**）する、または**【Alt】キーを押しながら【F4】キーを押す**と、全画面表示が解除されます。全画面表示が解除されたら、**ウィンドウタブ右上の「×」**を押して、表示中のページを閉じてください。



タスクマネージャーからブラウザアプリを強制終了

【Windows PCの場合】**CtrlキーとAltキーとDelキーを同時に押して、タスクマネージャーを起動**させ、タスクマネージャーから**ブラウザアプリ（Microsoft EdgeやGoogle Chrome）を選択し、右クリック→「タスクの終了」をクリック**してください。



架空料金請求詐欺

突然ですが

こんなSMSが届いたら、どうしますか？

有料動画の利用履歴があります。
未納料金が発生しており、本日ご連絡がない場合は、強制執行の法的手続きに移行します。
至急、相談窓口までご連絡ください。

相談窓口
XXXX-XX-XXXX

ご利用料金の確認が取れておりません。
本日中に03-XXXX-XXXX
〇〇ファイナンスサポートセンターまでご連絡ください。

とりあえず電話を試してみる??



架空料金請求詐欺

身に覚えがなければ、連絡してはいけません！

それ「架空料金請求詐欺」かも！？

- 「架空料金請求詐欺」とは**未払いの料金があるなど架空の事実を口実**とし金銭等を騙し取る手口です。
- **実在する電話会社や動画サイト**を騙り、利用したサービス内容や発生金額、支払期日、延滞料金などを提示し、**支払がない場合は法的手段をとる**として受信者を脅迫します。



身に覚えがなければ詐欺を疑う

架空料金請求詐欺についての典型的な手口が**警察庁のホームページ**に公開されています。相手に電話をする前に一度、ネット検索で類似の事象がないか情報収集してみてください。



どうしても不安であれば公的機関に相談してみる

ご自身で判断がつかなければ、まずは家族や知人に相談し、それでも解決できなければ、**消費生活センターなど公的機関**へご相談ください。

インターネットバンキングを安全にご利用いただくために、以下の点にご留意ください。

- **ID・パスワードは決して他人に教えないでください。** それらを聞き出そうとされたら詐欺を疑ってください。
- **ウイルス感染の警告画面**が表示されても、**指示内容に従わないようにしてください。** 落ち着いて**パソコンの販売元担当者や正規のサポートセンターへ連絡するか、ショートカットキーを使って画面を閉じる**ようにしてください。
- 相手に少しでも不審な点があれば、**電話を切電し、家族や警察に相談**するようにしてください。