【BIZ-WEBご利用者さま向け】

＜インターネットバンキングご利用の際の注意事項＞

突然の詐欺行為、
焦らず対応できますか？

－目次－

会社の大切な資産を守るため、本資料を経営者様や経理担当者の皆さまに共有いただくことを推奨します！

第四北越銀行

はじめに

当行のインターネットバンキングサービス「BIZ-WEB」では、第三者のなりすましによるログインや不正操作を防ぐために以下のセキュリティを導入しております。これらの仕組みを理解し、ID・パスワード等の認証情報を適切に管理いただくことで、預金の不正な払出しは防止できます。

1．ID・パスワードによる認証

…基本となる知識情報による認証であり、ログインの都度必ず求められます。

2．電子証明書認証（無料のオプション）

…あらかじめパソコンにインストールした「電子証明書」と「パスワード」により、お客さまがご本人であることを確認するログイン認証方式です。

3．リスクベース認証

…普段と異なる端末からログインがあった場合に「秘密の合言葉」（ご本人情報の質問＋ご本人情報の答え）による本人確認を行います。

4．トランザクション認証

…取引内容を二次元コードに変換し、カメラ付きトークンで取引内容を復元することで、取引の改ざんを防ぎます。トークンに表示される認証コードをパソコンに入力することで、取引が実行されます。

ボイスフィッシング詐欺

突然ですが

こんな電話がかかってきたら、どうしますか？

【自動音声】
第四北越銀行からのご連絡です。インターネットバンキングのパスワード変更が行われていませんでしたので、ご連絡しました。オペレーターにお繋ぎしますので、番号の１番を押してください。

番号１を押すと

【オペレーター】
第四北越銀行EBデスクの○○と申します。インターネットバンキングのパスワード変更を受け付け致しますので、お客様のメールアドレスを教えてください。のちほど、メールをお送りしますので、そちらのメールに記載のURLから専用サイトに入っていただき、パスワード等を入力いただくようお願いいたします。

相手の指示に従い、メールアドレスを教える？

ボイスフィッシング詐欺

絶対にメールアドレスを教えないでください！

それ「ボイスフィッシング詐欺」です！！

- 「ボイスフィッシング詐欺」とは、**音声を使用したフィッシング詐欺行為であり、金融機関職員を騙り、**パスワード変更が行われていないなどの口実で**メールアドレスを聞き出して、偽メールを送り、その後に偽サイトに誘導**して、**IDやパスワード等の情報を盗み取る**詐欺行為です。
- IDやパスワードのほかにも**「秘密の合言葉」**や取引実行に必要な**ワンタイムパスワード**等も言葉巧みに（「必要なテストです」などと言って）盗み取る手口が確認されています。

金融機関が電話でお客様情報を聞き出すことはありません

金融機関が電話でお客さまの**メールアドレスや会社情報を聞き出すことはありません。不審な電話を受けた場合は、直接金融機関にお問い合わせください。**

巧妙に作られた偽サイトにご注意ください

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**ようにしてください。

ボイスフィッシング詐欺

ボイスフィッシング詐欺の手口を理解しましょう

典型的な手口の流れは以下のとおりです

1．**電話連絡**：犯人が銀行担当者などを名乗り、「インターネットバンキングのパスワード変更が必要」などと偽って電話をかけ、メールアドレスを聞き出す。
（先に自動音声が流れて、番号を押させてオペレーターにつなげることが多い）

2．**偽メール送信**：聞き出したメールアドレス宛に、銀行を装った偽メールを送信。
メールには偽サイトへのURLやQRコードを記載。

3．**偽サイトへ誘導**：電話で指示しながら、被害者を偽のログインサイト（フィッシングサイト）へ誘導。

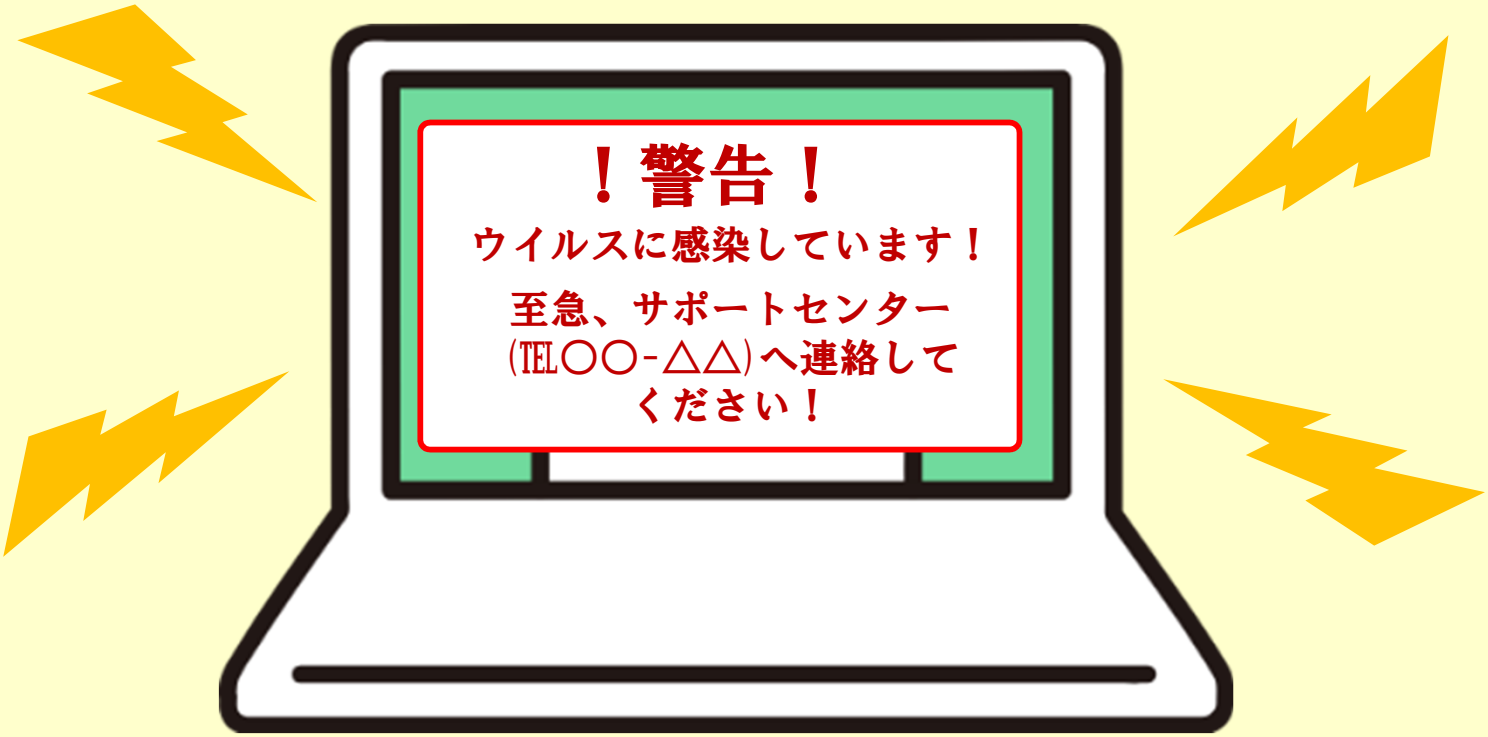
4．**情報詐取**：偽サイトでログインID、パスワード、リスクベース認証の「秘密の合言葉」等を入力させて情報を盗み取る。

5．**不正送金**：盗み取った情報を使い、犯人が被害者の口座から不正送金を行う。
※なお、トランザクション認証ついては、犯人側が送金操作を行い、二次元コードを画像コピーし被害者にメール送信し、被害者にカメラ付きトークンで読み取りをさせて、表示されたワンタイムパスワードを答えさせる。

サポート詐欺（パソコンの遠隔操作）

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（パソコンの遠隔操作）

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に連絡させる**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、**パソコンの販売元の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！

サポート詐欺（パソコンの遠隔操作）

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。

ビジネスメール詐欺

突然ですが

こんなメールが届いたら、どうしますか？

［至急］振込手続きをお願いします

お疲れ様です。
□□（社長や上司の名前）です。

最近取引を開始した㈱△△さまへの支払いが漏れていることがわかりました。
急で申し訳ないけど、XXX,XXX円振込をしてください。
［振込先口座］○○銀行　XXXX-X-XXXXXXX

振込先口座の変更のご依頼

いつもお世話になっております。
株式会社〇〇の△△でございます。

弊社の取引金融機関の変更に伴い、今月より振込先口座の変更をお願いいたします。

［新しい振込先口座］
□□銀行　XXXX-X-XXXXXXX

メールの要求通り、資金を振り込む？？

ビジネスメール詐欺

メール内容を鵜呑みにせず、別途、依頼者に確認してください！

それ「ビジネスメール詐欺」かも！？

- 「ビジネスメール詐欺」とは**経営者や取引先になりすまし**、資金の振込を指示し、騙しとろうとする詐欺行為です。
- 経理担当者など、**会社の資金を動かす権限を持つ方が狙われます。**経営者へのなりすましでは、「機密事項」や「周りの人へ相談不可」など、経理担当者単独で対応を促すような文面が送られることもあります。

メールの内容に不審な点がないか確認する

経営者や取引先になりすましたメールでないか確認しましょう。**普段と異なるメールアドレスや言葉遣いである場合、特に注意**が必要です。

メール以外の方法で本当の依頼か確認する

受け取ったメールに返信するのではなく、**普段利用している電話番号等へ連絡し、本当の依頼であるか確認**しましょう。メールに連絡先が記載されていた場合、それもまた詐称している可能性がありますので、普段利用している電話番号等へ連絡することが重要です。

最後に

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。

- **知らない電話番号**からの着信や、**登録されていないメールアドレス**からのメールは、詐欺の可能性があります。絶対に応答しないでください。
- 万一応答してしまった場合でも、相手の話を鵜呑みにせず、**いったん電話を終了し、会社の上司や同僚に相談**するか、**インターネットで同様の手口が報告されていないか確認**してください。
- 送金手続きは**担当者だけに任せず**、**上席者の承認を得る運用**とすることをお勧めします。
- カメラ付きトークンは**上席者が保管**し、必要なときにのみ担当者に貸与するなど、**厳格に管理すること**をお勧めします。

最後に

劇場型詐欺には、誰もが騙される可能性があります。

<u>最後の砦は、ワンタイムパスワードです！</u>

送金先と金額は本当に正しいですか？
【疑問をもったら絶対に入力しない】

信じてはダメ！伝えない

テストだから大丈夫です。
読み上げてください

トークンが故障して
いないか確認します。
読み上げてください