

2024年11月14日

お客さま 各位

中央労働金庫

詐欺メール（フィッシング詐欺）にご注意ください

いつも〈中央ろうきん〉をご利用いただき、誠にありがとうございます。

近時、ろうきんダイレクトを装ったフィッシングサイトが複数確認されており、そのフィッシングサイトに誘導しお客さま情報の詐取を試みるメール・SMSが無作為に送信されていることが確認されています。

これらのサイトは、正規の労働金庫サイトに似せて作られており、お客さまのログイン情報（ログインID・パスワード等）や個人情報を入力させることを目的としています。

万が一、フィッシングサイトにアクセスしてしまった場合や個人情報を入力してしまった場合は、速やかにろうきんダイレクトヘルプデスク（下記参照）までご連絡ください。

<お客さまへのお願い>

- ・正規のサイトは、必ず公式のURLをご確認のうえ、アクセスしてください。

当金庫ろうきんダイレクトの公式URL <https://ib.rokin.jp/?bid=13>

- ・公式アプリ「ろうきんアプリ」からのログインを推奨します。



- ・メールやSMSに含まれるリンクをクリックする際は、常に送信者の正当性を確認してください。なお、当金庫からの正規のメールやSMSでは、お客さまの個人情報やパスワードを入力するよう求めることはありません。不審なメールやメッセージに記載されたリンクをクリックしないようご注意ください。

今後もお客さまの安全を最優先に考え、フィッシングサイトの監視と対策を強化してまいります。

何卒ご理解とご協力を賜りますようお願い申し上げます。

以上

【ろうきんダイレクトヘルプデスク】

電話番号：0120-698-956（フリーダイヤル）

受付時間：9:00～21:00

※1月1日～1月3日および定期メンテナンス時はご利用いただけません。

<偽（フィッシング）メールのイメージ>

労働金庫 宛先: [REDACTED] 10:26

**【労働金庫】お取引
目的等のご確認のお願い**

平素より、労働金庫をご利用いただきありがとうございます。
す。

労働金庫では2019年6月より金融庁の「マネー・ローンダリング及びテロ資金供与対策に関するガイドライン」に基づき、お客さま情報やお取引の目的等を定期的に確認させていただいております。お客さまにはお手数をおかけいたしますが、何卒ご理解とご協力をお願い申し上げます。

※なお、確認させていただく時期はお客さまごとに異なります。
※2024年11月7日までに「お取引目的等の確認」より、お取引の目的等のご確認をお願いいたします。

▼お取引目的等確認
[https://\[REDACTED\].okinbk.html](https://[REDACTED].okinbk.html)

※確認後、口座の全ての機能が正常にご利用いただけるようになります。
※一定期間内に確認が取れない場合、口座のお取引が制限されます。
※お客さま情報等の定期的なご確認にご協力ください

【ご注意】

- ・ お客さま個別の事由で口座のお取引が制限されている場合、本件のお手続きを完了しても制限は解除されません。
- ・ その他重要なお手続きのご案内が表示される場合があります。ご案内を確認後、回答画面が表示されます。

お客さまにはお手数をおかけいたしますが、何とぞご理解、ご協力のほどお願いいたします。

お問い合わせは下記まで
労働金庫 お客さま情報管理センター
0120-[REDACTED]

差出人：一般社団法人全国労働金庫協会
このメールアドレスは送信専用です

※上記文面のメール以外も偽（フィッシング）メールが確認されているため、ご注意ください。

本メールの各種不正な URL をクリックすると<ろうきんダイレクト>を装ったフィッシングサイト（本物そっくりの偽サイト）に誘導されます。

 **絶対にクリックしないでください。**

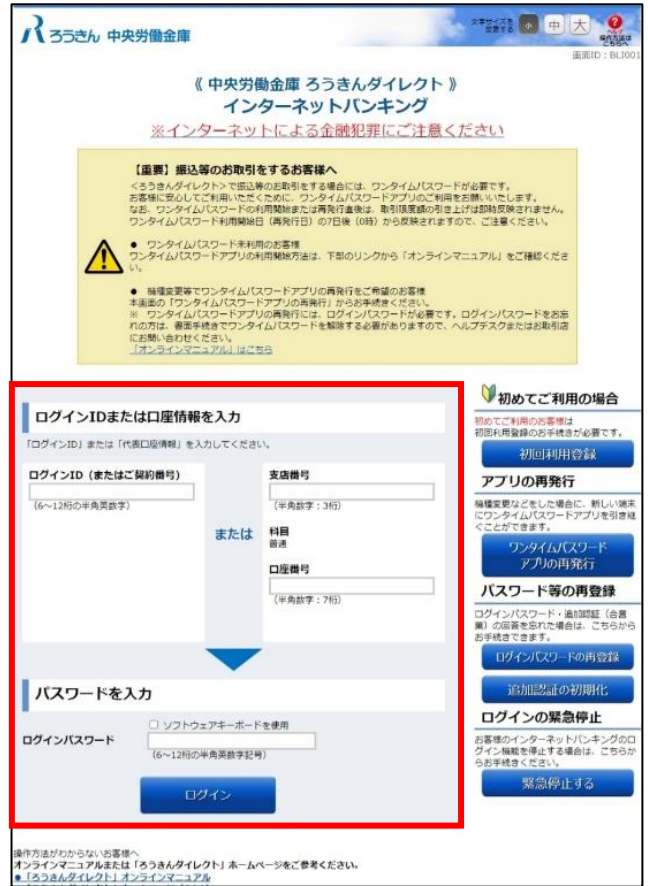
万々クリックしても、誘導先でログイン ID やログインパスワード、キャッシュカードの暗証番号などの個人情報等を絶対に入力しないでください。

- <中央ろうきん>では、メールに記載されたリンクや添付ファイル等からログイン ID やログインパスワード、暗証番号などの個人情報等の入力を促すようなことは一切ございません。
- <ろうきんダイレクト>からお客さま向けに送信するメールは、以下のドメインから送信されます。

【正しいメールアドレス】

- ・ @rokinbank.or.jp
(ろうきんダイレクトから送信されるメール)
- ・ @otp-auth.net
(ワンタイムパスワードアプリから送信されるメール)
- ・ @chuo-rokin.or.jp
(<中央ろうきん>から送信されるメール)

＜偽サイトのイメージ＞



! 本誘導されたフィッシングサイトに、お客さまのログイン情報（ログイン ID・パスワード等）や個人情報 は絶対に入力しないでください。



※以降の画面でキャッシュカードの暗証番号の入力やワンタイムパスワードを発行するアプリの認証用電話番号に架電等をするよう誘導される場合があります。