

【フィッシング詐欺】当社を騙った不審なメールの発生



被害にあわないためのポイント

ポイント 1 電子メールやショートメッセージ（SMS）からログインしないでください

電子メールやショートメッセージ（SMS）を使って、

当社側から**一方的にログインを依頼することはありません。**

また、ログイン ID・パスワード・ワンタイムパスワード・キャッシュカードの暗証番号などの**入力を依頼することはありません。**

ポイント 2 不審なメール・SMS の発信元を確認してください

りそなグループでは特定のメールアドレスや電話番号を使用しており、下記ページに掲載されていないメールアドレスや電話番号を使用することはございません。

また、**偽のメールアドレスは、当社メールアドレスと非常によく似たアドレスを使用しておりますので、よくご確認ください。**

ポイント 3 ログインページの URL を必ずご確認ください

りそなグループでは特定のドメイン（ページ URL の最初の文字）を使用しており、下記ページに掲載のないドメインを使用することはございません。

また、**偽サイトは見た目が当社ページと同様であり、非常によく似た URL を使用しておりますので、ログイン時には URL をよくご確認ください。**

| | 正しい URL | 偽サイト URL 例 |
|---------|---|---------------------------|
| 当社ページ | https://www.kmfg.co.jp/mrp/ | ●●～ kmfgmrp. ～ |
| わらかどひろば | https://kmfg-warakado.en-jine.com | ●●●●. en jine.com. |

n と j の間に - (ハイフン) が無い

【ご注意】デビットカード・クレジットカード等の情報を狙ったフィッシングサイトについて



- ❗ 偽のフィッシングサイトへ誘導し、入力させたカード情報等の個人情報を騙し取る詐欺が多発しています。個人情報の入力には充分ご注意ください。

偽のフィッシングサイトへ誘導し、入力させたカード情報等の個人情報を騙し取る詐欺が多発しています。個人情報の入力には充分ご注意ください。

金融機関等を装う電子メールにご注意ください

実在の金融機関等を装って電子メールを送付し、メールを受信されたお客さまをその金融機関とはまったく関係のない虚偽のページにアクセスさせ、暗証番号などの重要な情報を入力させることにより、個人情報を取得するという悪質な詐欺事件が発生しています（フィッシング詐欺）。

心あたりのない配信元からの電子メールのリンク先ウェブサイトへは、暗証番号などの重要な情報を入力なさないようご注意ください。

- ❗ 「重要」「わらかどひろば」を騙ったフィッシングサイトにご注意ください

昨今、お使いのブラウザ（Safari、Chrome、Firefox など）や通販業者等を偽るポップアップやメールやショートメッセージ（SMS）から、巧みにフィッシングサイトへ誘導し、入力させたカード情報やID・パスワードを騙し取る詐欺が多発しています。

フィッシングサイトでカード情報やID・パスワード等を入力することがないよう、充分ご注意をお願いいたします。

クレジットカード情報の管理全般についてご注意いただきたいこと

- カードを第三者に貸与しないでください。
- カード情報、本人認証サービス（ J/Secure™ / Visa Secure / Mastercard®SecureCode™ ）のパスワードは、パソコンやスマートフォン等に保存しないでください。
- 本人認証サービス（ J/Secure™ / Visa Secure / Mastercard®SecureCode™ ）のパスワード入力が必要な真のお取引の場合は、事前に設定いただいたパーソナルメッセージが表示されている専用の入力画面が表示されます。
パーソナルメッセージが表示されていない場合はパスワードを入力しないでください。
- 身に覚えのないメール、SMS やインターネット閲覧中のポップアップなどから遷移したサイトでのカード情報入力には最新の注意を払ってください。
- メールアドレスやサイトの URL が通常と異なる場合、カード情報を入力しないでください。

万が一、身に覚えのない、りそなカードのお引落しがあった場合には、速やかにカード裏面に記載のりそなカードインフォメーションセンターにご連絡をお願いいたします。