

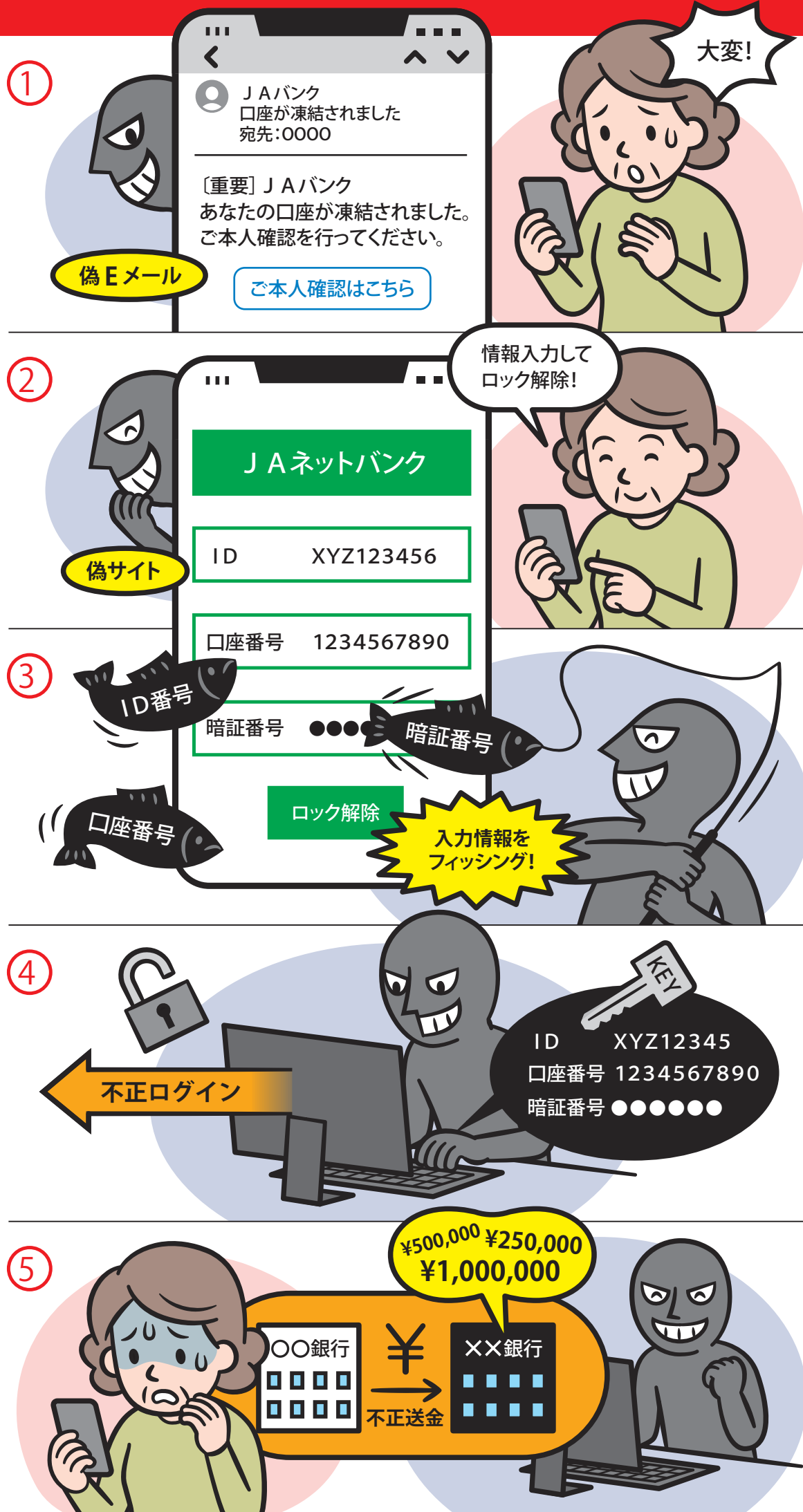


特殊詐欺にご注意ください

詐欺の手口は年々多様化、巧妙化しており、電話だけでなく、メールやインターネットを悪用した見分けが付きにくいケースが増えています。
偽物のメールやサイトにアクセスすることで、不正送金や情報漏えいなど重大な被害に遭う危険があります。

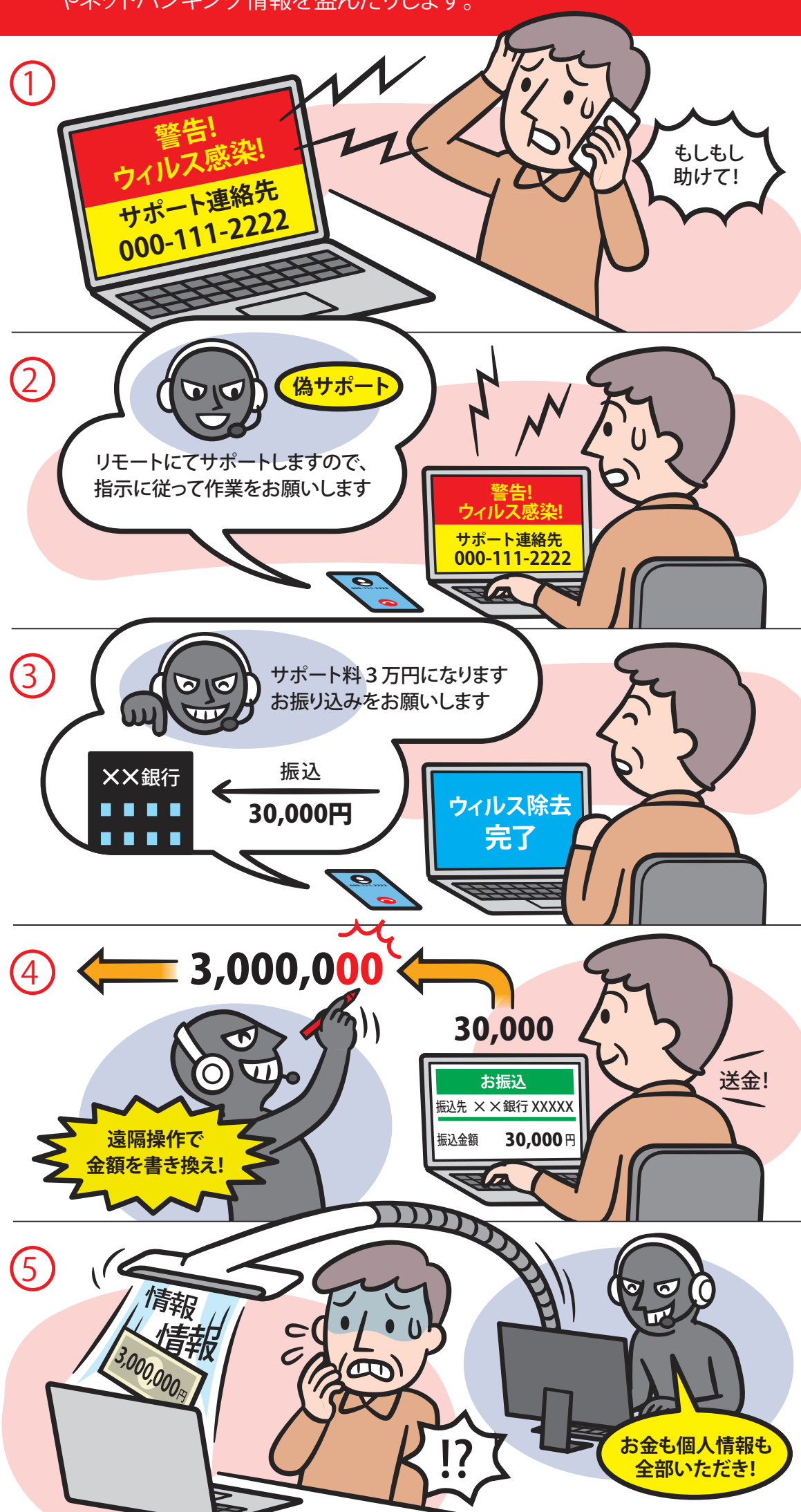
フィッシング詐欺

金融機関や公的機関、通販サイトを装い、偽メールや偽サイトへ誘導し、ID・パスワード、口座情報、暗証番号などの個人情報を入力させることで情報を盗み取ります。



サポート詐欺

パソコン上で「ウイルスに感染しました」「サポート窓口にご連絡してください」などと偽の警告画面を表示し、サポート窓口で解決をするフリをして高額な費用を請求したり、遠隔操作ソフトをインストールさせ、個人情報やネットバンキング情報を盗んだりします。



Check! 特殊詐欺チェックリスト

- ☐ 暗証番号を教えてください
- ☐ お金が戻ってきます
- ☐ カードの交換が必要です
- ☐ カード・口座が悪用されています
- ☐ 警察がご自宅に伺います
- ☐ このままだと逮捕される可能性があります
- ☐ このやり取りを口外すると罪に問われます
- ☐ 期日までに対応を行わないと取引が制限されます
- ☐ 指示に従ってATMの操作をしてください

1つでも当てはまったら詐欺です!

すぐに電話を切って家族や身近な人に相談しましょう。

Point! 詐欺にだまされないためには

- 警察・公的機関を名乗る者から突然電話が来ても、一度電話を切り、申し出内容が正しいか確認するため電話をかけ直しましょう。その際、電話番号は自分で調べ直しましょう。
- 少しでも様子がおかしいと感じたら、家族や友人など身近な人に相談しましょう。事前に家族間で話し合っておくのも効果的です。
- 詐欺の手段は電話が8割近くを占めています。常に留守番電話機能を設定しておき、通話の録音や防犯機能が付いた迷惑電話防止機器を使いましょう。
- 警察・検察は個人のスマートフォンに突然ビデオ電話をすることはなく、国際電話で連絡することもあります。不審な点がないか、落ち着いて確認しましょう。



JAバンクは被害拡大防止に向けて、店舗での「声掛けの徹底」に取り組んでいます。

ATM付近で携帯電話を利用している方や窓口で多額の現金を引き出そうとしている方には、

現金のご利用目的などをお伺いすることがございます。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。

<日本農業新聞掲載>

JA ネットバンクを装ったフィッシングメールにご注意ください

JA バンク利用者を狙ったフィッシングメールが継続して確認されており、偽の JA ネットバンクサイトが引き続きかつてない規模で開設されています。

不審なメールと気付かず、認証に必要な情報を入力してしまい、不正送金の被害に遭う可能性があります。

不審なメールを受信された場合は削除いただき、メールに記載されている URL には絶対にアクセスしないようご注意ください。

<確認されているフィッシングメールの件名例>

※一例であり、その他にも類似した件名が確認されています。

- ・セキュリティ設定未完了の方へ(振込制限の可能性)
- ・本人確認未完了による一部機能停止
- ・JA バンクセキュリティ強化のお知らせ
- ・お取引目的の確認のお願い
- ・要確認 登録個人情報再確認のお願い
- ・【緊急のお知らせ】 お客様の資産保護のための本人確認のお願い
- ・【JAネットバンク】取引制限に関する重要なお知らせ
- ・【本人確認】未完了の確認をお願いします。
- ・【重要通知】システム更新に伴う再ログインのお願い
- ・【重要】ご本人様による口座利用の確認について
- ・振込サービスのご利用に制限がかかる可能性があります
- ・取引目的等の定期的なご確認にご協力ください

<電子メールでお取引目的やお客様情報を確認することはありません>

お客さまとお取引のある JA から「お客様情報確認書」が圧着式往復はがき、または封書でお手元に届くことがあります。これはマネー・ローンダリング防止対応の一環として、お客さまに関する情報やお取引目的等を定期的に確認するものですが、JA バンクにおいては、電子メールや JA ネットバンクを経由した確認依頼は行っておりません。

口座番号・暗証番号等を電子メール等でお尋ねすることはございませんので、そうしたものに回答しないようご注意ください。

万が一不正サイトに口座情報等を入力してしまった場合、速やかにお取引 JA または JA ネットバンクヘルプデスクあてにご連絡いただき、JA ネットバンクの利用を停止ください。

【お問い合わせ先】

フリーダイヤル: 0120-058-098

お問い合わせ時間: 平日 9:00~21:00 土日祝日 9:00~17:00

JA ネットバンクを装ったフィッシングメールにご注意ください

JA バンク利用者を狙ったフィッシングメールが継続して確認されており、偽の JA ネットバンクサイトが引き続きかつてない規模で開設されています。

不審なメールと気付かず、認証に必要な情報を入力してしまい、不正送金の被害に遭う可能性があります。

不審なメールを受信された場合は削除いただき、メールに記載されている URL には絶対にアクセスしないようご注意ください。

<確認されているフィッシングメールの件名例>

※一例であり、その他にも類似した件名が確認されています。

- ・セキュリティ設定未完了の方へ(振込制限の可能性)
- ・本人確認未完了による一部機能停止
- ・JA バンクセキュリティ強化のお知らせ
- ・お取引目的の確認のお願い
- ・要確認 登録個人情報再確認のお願い
- ・【緊急のお知らせ】 お客様の資産保護のための本人確認のお願い
- ・【JAネットバンク】取引制限に関する重要なお知らせ
- ・【本人確認】未完了の確認をお願いします。
- ・【重要通知】システム更新に伴う再ログインのお願い
- ・【重要】ご本人様による口座利用の確認について
- ・振込サービスのご利用に制限がかかる可能性があります
- ・取引目的等の定期的なご確認にご協力ください

<電子メールでお取引目的やお客様情報を確認することはありません>

お客さまとお取引のある JA から「お客様情報確認書」が圧着式往復はがき、または封書でお手元に届くことがあります。これはマネー・ローンダリング防止対応の一環として、お客さまに関する情報やお取引目的等を定期的に確認するものですが、JA バンクにおいては、電子メールや JA ネットバンクを経由した確認依頼は行っておりません。

口座番号・暗証番号等を電子メール等でお尋ねすることはございませんので、そうしたものに回答しないようご注意ください。

万が一不正サイトに口座情報等を入力してしまった場合、速やかにお取引 JA または JA ネットバンクヘルプデスクあてにご連絡いただき、JA ネットバンクの利用を停止ください。

【お問い合わせ先】

フリーダイヤル: 0120-058-098

お問い合わせ時間: 平日 9:00~21:00 土日祝日 9:00~17:00