

最近多くの迷惑メール（フィッシングメール）が多くなっているので、御注意を！

メールからウィルスの感染や個人情報をはき取りを防ぐ方法。

1. 迷惑メールが届いたら、まず確認し、怪しい場合は添付ファイルを開かぬこと

1) 送信元を確認すること

心当たりのないメールが届いたら、まず「送信元(差出人)」と「メールアドレス」を確認する。

いずれも表示されていないか、自分のメールアドレスが表示されている場合は、迷惑メールと断定してよい。

有名な会社やサービスからのメールだと思わせる、紛らわしい名前やメールアドレスが使用される場合もある。

例 1) 発信人が自分



例 2) 実在の会社をかたり、怪しいサイトに誘導。

リンクを張ったところにマウスを移動すると、リンク先が表示される。

リンク先が怪しいアドレスの場合、クリックしない。



前頁と同様、
最近多い
メール例

2019/10/07 (月) 0:14
Amazon.co.jp <admin9@amazonahktadmind.jp>
[meiwaku] Amazon.co.jp アカウントの支払い方法を確認できず、注文を出荷できません。 46D6AD

宛先 jkatch19

MEIWAKU

このメッセージの表示に問題がある場合は、ここをクリックして Web ブラウザーで表示してください。



Amazon お客様

残念ながら、あなたのアカウント

Amazonを更新できませんでした。
これは、カードが期限切れになったか、請求先住所が変更されたなど、さまざまな理由で発生する可能性があります。

アカウント情報の一部が誤っている故に、お客様のアカウントを維持するため

Amazon 情報を確認する必要・があります。今アカウントを確認できます。

<http://www.amazonahktadmine.jp/>
クリックしてリンク先を表示

[Amazon ログイン](#)

なお、24時間以内にご確認がない場合、誠に遺憾ながら、アカウントをロックさせていただくことを警告いたします。

パスワードを変更した覚えがない場合は、至急(03)-5757-5252までお電話ください。

返信 全員に返信

2017/11/06

 kansai ebusiness <kansai_ebusiness@sagawa-exp.co.jp>
[meiwaku] [佐川急便] 請求内容確定のご案内

宛先 jiron2@sirius.ocn.ne.jp; j-ishikawa@sirius.ocn.ne.jp; jjunyax0701@sirius.ocn.ne.jp; jk3-ojl@sirius.ocn.ne.jp; jk913@sirius.ocn.ne.jp;
jkatch19@sirius.ocn.ne.jp; jkiuchi@sirius.ocn.ne.jp; jkk@sirius.ocn.ne.jp; jkmo@sirius.ocn.ne.jp

例3) 有名な会社、請求書・開かせやすい形態をとっている。

請求書のメール宛先が複数表記してあり、不審なメールと思われる。

分類項目 赤

このメッセージではリンクなどの機能が無効になっています。これらの機能を有効にするには、メッセージを受信トレイに移動します。このメッセージをテキスト形式に変換しました。

平素は格別のご愛顧を賜り、心より御礼申し上げます。

※本メールは電子請求書発行サポートにご登録頂いたお客様を対象に送信しています。

請求の内容が確定しましたので、ご案内致します。

運賃請求書発行画面より請求書を取得して頂きます様、お願い申し上げます。

請求書番号

【3707695160】
<<http://vg.yourgraymatters.org/cnydodagepd6823/jdvjyfiimwmp65951zhzjiron2diykr900776192/fzutsavpl7938737>>

■取得方法

『電子請求書発行サポートメニュー』選択後、『運賃請求書発行』から取得して下さい。

例 4) 有名な会社

申込みの覚えがないもの 要注意！！

返信 全員に返信 転送



2017/11/14 (火) 15:28

mizuho-cardloan@p.onet.orico.co.jp

「みずほ銀行カードローン」仮申し込みの審査結果のご連絡

宛先 jjunyax0701@sirius.ocn.ne.jp; jk3-ojl@sirius.ocn.ne.jp; jk913@sirius.ocn.ne.jp; jkatoh19@sirius.ocn.ne.jp; jkiuchi@sirius.ocn.ne.jp

CC jltstrcr@sirius.ocn.ne.jp; Tue, 14 Nov 2017 10:27:53+0400@mf-omf-ucb021.ocn.ad.jp; jltstrcr@sirius.ocn.ne.jp

分類項目 赤

このメッセージではリンクなどの機能が無効になっています。これらの機能を有効にするには、メッセージを受信トレイに移動します。このメッセージをテキスト形式に変換しました。

「みずほ銀行カードローン」仮申し込みの審査結果のご連絡

いつもみずほ銀行をご利用いただき、ありがとうございます。

この度は「みずほ銀行カードローン」をお申し込みいただきありがとうございます。

以下の URL から仮申し込みの審査結果をご確認ください。

※確認の際には仮申し込み時にご登録いただいたパスワードが必要になります。

>一時的な仮登録のためのパスワード

<<http://shen2.ioemarrone.com/uinyw525civqg6313/ktmvr7161yipbpi78514jngsfjjunyax0701lu3127/uvs1zsq0036075>>

※URL をクリックいただくと、保証会社である株式会社オリエントコーポレーションのサイトへ移動します。

■ご留意事項

※審査の結果によっては、ご希望にそいかなる場合がございますので、ご了承ください。

※申し訳ございませんがこのメールへの返信はお受けしておりません。

例 5) セキュリティに関連すると思わせて、添付ファイルを開かせる。

返信 全員に返信 転送



2017/11/07 (火) 23:41

noreply@email.apple.com

[meiwaku] あなたのApple IDのセキュリティ質問を再設定してください。

宛先 jk913@sirius.ocn.ne.jp; jkatoh19@sirius.ocn.ne.jp; jkiuchi@sirius.ocn.ne.jp

分類項目 赤

このメッセージではリンクなどの機能が無効になっています。これらの機能を有効にするには、メッセージを受信トレイに移動します。このメッセージをテキスト形式に変換しました。

安全のため、この Apple ID はすでにロックされました。

あなたの Apple ID は windows PC の iCloud にログインしたりダウンロードしたりする操作があったと Apple ゲームのセキュリティチームは発見しました。

日付と時間：2017/11/05

iCloud バージョン：6.2.2.35

IP：220.31.289.137 (岐阜)

あなたのアカウントの安全性を守るために、セキュリティ質問を再設定して頂く必要があります。再設定された後、たとえばあなたの Apple ID とパスワード及び元のセキュリティ情報を知っているとしても、それを使用することができません。

この問題を解決するにはこちら <<http://help-id-cloud.online/>>

このリンクとあなたの Apple ID のセキュリティ質問とは、2017 年 10 月 21 日から失効になります。詳細情報について、「よくある質問」をご利用いただけます。

以上

Apple ID サポートセンター

例 6) 送信元が不明

返信 全員に返信 転送

2017/11/08 (水) 1:35

info@f-5bo9i8h78jk3.tokyo
[meiwaku] 【【御注文、誠に有難う御座います。】】 -

宛先 jkatoh19@sirius.ocn.ne.jp

分類項目 赤

このメッセージではリンクなどの機能が無効になっています。これらの機能を有効にするには、メッセージを受信トレイに移動します。

【タイトル】
【【御注文、誠に有難う御座います。】】 -

【本文：閲覧無料】
<http://c7sndf-8n39nf41.tokyo/user.app?cmd=message&k=915b2bdca55d7f6e9f155345f2ace7f&toID=782882&resID=206856591>

【BitOash(ビットキャッシュ)&銀行振り込み&クレジットカード(Visa デビット&JCB デビット含)利用可!詳細は↓コチラを御確認下さい。】
<http://c7sndf-8n39nf41.tokyo/members.app?k=915b2bdca55d7f6e9f155345f2ace7f&cmd=buypoint>

【キャンペーンに関するお問合せ→ Amazing キャンペーン事務局】
<http://c7sndf-8n39nf41.tokyo/members.app?k=915b2bdca55d7f6e9f155345f2ace7f&cmd=message&toID=852416>

【その他お問い合わせ・配信停止→ Amazing サポート部】
<http://c7sndf-8n39nf41.tokyo/members.app?k=915b2bdca55d7f6e9f155345f2ace7f&cmd=message&toID=8288>

※電話による対応は承っておりません。このアドレスは送信専用アドレスです。お問合せ・配信停止の際は必ず上記の URL よりログインされた上でお問合せ下さい。

Amazing

2) 紛らわしいメールがウィルス付き、迷惑メールかを確認するため、“JC3”の情報を確認すること。

日本サイバー犯罪対策センター (Japan Cybercrime Control Center:JC3)

<https://www.jc3.or.jp/topics/virusmail.html>

JC3 の内容

2016 年 11 月 7 日 作成

2018 年 3 月 30 日 改訂

2019 年 10 月 4 日 更新

[最新の具体例はこちら](#)

JC3 では、IT 事業者、セキュリティ事業者、金融機関、警察などの JC3 会員と協力して、不正送金の被害軽減に向けた分析を進めており、昨今、インターネットバンキングマルウェア (Gozi 等) の感染拡大を図るウイルス付メールが日本を標的として大量に送信されていることを把握しております。これらのウイルス付メールの添付ファイルを開き、インターネットバンキングマルウェアに感染すると、金融機関関連情報が窃取されることなどにより、インターネットバンキングの不正送金などの犯罪の被害にあうおそれがあります([Gozi の詳細はこちら](#))。

今般、これらのウイルス付メールの配信を早期に把握し、同メールの件名や本文等を解明できるようになりました。

このため、JC3 では、本日より警視庁と連携し、JC3 ウェブサイトを通じ、これらのウイルス付メールが配信される際に早期警戒情報を発信することとしました。

現在確認されているウイルス付メールは以下のとおりです。これらのメールは、犯罪者から送付されたウイルス付

メールであり、**添付ファイルは写真や文書等を装ったマルウェア**ですので開かないようにしてください。

さらに、以下の例以外にも、ウイルス付メールは多数配信されていますので、添付ファイルの開封を促したり、リンク先のサイトの閲覧を促すような不審なメールには十分ご注意ください。

なお、警視庁では、広報課及び犯罪抑止対策本部の twitter アカウントにより同様の内容の情報を発信しており、また、警察庁においても、警察庁の twitter 公式アカウントにより、注意喚起を実施しております。

これらのウイルス付メールにより感染するおそれのある DreamBot・Gozi については、JC3 で感染チェックサイトを試験運用していますので、ご活用ください。[\(チェックサイトはこちら\)](#)。

※マルウェア: **マル**シヤス(悪意のある)、ソフト**ウェア**の合成語、悪意のあるソフトウェア

ウイルス付メールの具体例

2019年10月4日午後3時 更新 [INDEX 版はこちら](#)

※**青字**は下記のランダムな文字列が入ります

A: 英字

X: 英字または数字

0: 数字

【送信日】 2019年10月4日

【件名】 できるだけ早くアカウント情報をご更新ください。【添付ファイル】

【本文】

Apple ID ユーザーの皆様、これは非常に重要なメールです。アカウントのログイン IP の異常により、一部の情報が失われるため、アカウント情報の更新が完了するまで、一部のアカウント権限をロックさせていただきます。この期間中は、アカウントからアプリを使用してダウンロードすることはできません。手順に従ってアカウント情報をご更新ください。ご理解いただきありがとうございます。ご不便をおかけして申し訳ありません。

アカウント更新 (※) (※)フィッシングサイトへのリンク

3 営業日以内に情報が更新されない場合、アカウントは完全に廃止されます。

ご迷惑をかけて、大変申し訳ございません。

Apple サポートセンター

【送信日】

2019年10月3日

【件名】

アカウント情報を更新、確認してください。

【添付ファイル】

【本文】



Amazon からのご挨拶です。お客様のアカウントの保護を重視しております。ログイン方法は少し尋常ではないので、アカウントが Amazon の利用規約を満たしていることを確認するために、アカウント情報を更新および確認してください。

情報の確認と更新(※) (※)フィッシングサイトへのリンク

必要な情報を確認および更新しないと、アカウントおよび販売活動が停止される可能性があることにご注意ください。画面の指示に従って変更または確認を行ってください。

ご理解いただきありがとうございます。

Amazon.co.jp

3) 返信しないこと

迷惑メールは気味が悪く、精神的にも嫌なものですが、何らかの対応(返信することなど)は絶対禁物です。

迷惑メールの送信者の多くは、不特定多数に一齐送信しており、返信することはそのメールアドレスが実在することや、受信者がメールを開いたことをわざわざ送信者に教えることになる。

【お金貸します】他社で断られた方でもご融資します！！

他社で断られた方、既に多くの借り入れがある方でも
即日で100万円までならお貸し致します♪
保証人不要、早くて便利♪
まずは下記をご覧ください、金利などをご確認の上ご連絡下さい。

<http://bit.ly/2gWDCkx>

迷惑メールには絶対に返信ない。

配信停止はこちら haisin_teisi_uketuke@yahoo.co.jp

4) 添付ファイルを開いたり、本文中のリンクをクリックしないこと

添付ファイルはウイルスの可能性が高いので、絶対に開かない。

迷惑メールの本文にある URL リンクをクリックすることも同様。

最近の迷惑メールは、受信者のパソコンやスマートフォンをウイルスに感染させようとする悪意あるものが増え、添付ファイルを表示する裏でウイルス感染を進める手法も使われている。

Amazon.co.jp からの連絡とフィッシングの見分け方について

Amazon.co.jp を装った詐欺と思われる連絡を受け取った際はこのページをご覧ください。

不審な E メールや SMS を受信した場合

• Eメールの場合

本文に記載されているリンクや添付ファイルを開かずに、メールを削除してください。もし開いてしまった場合は、[コンピューターを保護する](#) をご覧ください。

補足：不審なメールを受け取ったと思われる場合は、stop-spoofing@amazon.com 宛てにメールを送信してください(受信専用)。

• SMS の場合

本文に記載されているリンクや添付ファイルを開かずに、メールを削除してください。もし開いてしまった場合は、速やかに閉じて、各携帯電話会社でフィッシング対策として提供している迷惑メール設定機能で特定のドメインや電話番号以外から不審なメッセージを受信しないよう速やかに設定してください。

補足：各携帯電話会社で申告窓口が設けられています。今後の被害防止のためにも[フィッシングやなりすましメール、SMS を報告する](#)からご報告ください。

注: Amazon.co.jp では、お客様にご登録のアカウント情報(パスワード、クレジットカード情報など)の開示を求めことはありません。受け取られた E メール、SMS、はがきなどに記載されている連絡先(電話番号、URL など)に連絡しないようご注意ください。

フィッシングやなりすましの主な手口

内容	対策例/注意事項
未納料金の請求	<ul style="list-style-type: none">商品代金や、有料コンテンツの料金が未納というメッセージが届いた場合、注文履歴をご確認ください。法的手続きを持ち出す詐欺メッセージもあります。注文履歴にない請求に応じたり、記載された番号に電話をかけたりしないでください。
お支払い情報の更新依頼	<ul style="list-style-type: none">カードの有効期限が切れた、請求先住所が変更された、という内容で偽サイトに誘導する E メールがあります。

- [お支払いオプションを管理](#)にアクセスし、支払い方法の更新指示が出ていない場合は、Amazon.co.jp から送信した E メールや SMS ではありません。

Amazon.co.jp を装った
偽サイトへのリンク

- Amazon.co.jp サイトの URL は、「https:// × × .amazon.co.jp」で始まります。
- 以下の場合も偽装された E メールや SMS の可能性がありますのでご注意ください。

その他

- 添付ファイルやソフトウェアのインストールを求める内容
- 本文中に多くの誤字や文法の間違いが含まれる内容

Amazon.co.jp で使用している送信情報

Amazon.co.jp では、以下の送信情報を使用してお客様にご連絡をしています。しかしながら、Amazon.co.jp を装った偽 E メールアドレスまたは電話番号でフィッシングやなりすましの E メールや SMS が送信されるケースがあります。E メールまたは SMS の「差出人」欄に下記ドメイン以外の情報が含まれている場合は、不正な E メールまたは SMS の可能性がありますのでご注意ください。

補足： Amazon.co.jp が送信した E メールは、[メッセージセンター](#)でもご確認いただけます。

- | | |
|--------------|---|
| | <ul style="list-style-type: none"> • amazon.co.jp • amazon.jp • amazon.com • amazonbusiness.jp |
| E メールを送信する場合 | <ul style="list-style-type: none"> • email.amazon.com • marketplace.amazon.co.jp • m.marketplace.amazon.co.jp • gc.email.amazon.co.jp • gc.amazon.co.jp • payments.amazon.co.jp |
| SMS を送信する場合 | <ul style="list-style-type: none"> • 09090097540 • 08021585817 • 01085264515445 • Amazon • TheDrop |
| サービス、その他 | <ul style="list-style-type: none"> • Amazon ショッピングアプリ • LINE アプリ |