

弊社発行カード(TS CUBIC CARD、ENEOSカード等)を名乗る不審なメールにご注意ください

2021年3月23日更新

弊社発行カード(TS CUBIC CARD、ENEOSカード等)を名乗る不審なメールが、会員さまを含む不特定多数の方へ送信される事象が発生しております。不審なメールを受け取った際は、URLをクリックせず、削除してください。

トヨタファイナンスから、下記のようなメールはお送りしません。

- クレジットカード番号・有効期限・カード裏面に記載のセキュリティコード・カード暗証番号などを、直接お尋ねする内容のメール

※このようなメールを受信されても、絶対に個人情報を入力しないでください。

- 添付ファイル付のメール
- ファイルのダウンロードを促す内容のメール

● 実際に確認されている不審メールの件名

※掲載の件名は一例です。(掲載のない件名の場合もございますのでご注意ください。)

- <重要>【TS CUBIC Card】ご利用確認のお願い
- 【TS CUBIC CARD】重要なお知らせ
- 【TS CUBIC】カードの一時利用停止は解除されました
- 【TS CUBIC】カードお届け内容のご変更受付のお知らせ

フィッシング(詐欺)メール、フィッシング(詐欺)サイトの例

フィッシングに騙されないために、具体例をご確認ください。

※掲載の画面は一例です。(掲載のない事例の場合もございますのでご注意ください。)

例① メールに記載されているURLと、実際にカーソルをあてた時に表示されるリンク先のURLが違う

【ご確認方法】

メールに記載されているURLにカーソルを合わせると、カーソルの近く、もしくはステータスバーに、実際に接続されるリンク先のURLが表示されます。

《フィッシングメールの一例》

From: MY TS3 [mailto:info@ts3card.com]
Sent: [REDACTED]
To: [REDACTED]
Subject: TS3 TS CUBIC CARDカード ダイレクトをご利用いただき、誠にありがとうございます

TS CUBIC CARD 様

先日、会社のカードのお支払い情報が変更されたことが判明いたしました。フォローアップするまでの間、カードは一時的にロックされているものと思われ、当方の運営でしたら個人予約情報を更新してください。この間、ご迷惑をおかけしますがご容赦ください。

<https://my.ts3card.com/webapp/ToTP01020106Action.do?command=doInit&vo.NO=0005298315&vo.KEY=0025664632&vo.S/KBN=00>

<http://www.vbgamhydnngba.icu>

なお72時間以内に本登録が完了しない場合は、このメールが無効となり再度お手続きが必要となりますので、ご注意願います。

カーソルをあて、URLが一致しているかをご確認ください

例② 送信元メールアドレスが違う

弊社からお送りするメールのアドレスは、「info@ts3card.com」

または「info@mail.ts3card.com」です。

※一部メールにつきましては、「@toyota-finance.co.jp」のドメインでの配信となります。

※弊社からお送りするメールアドレスに偽装されていることもあります。

例①の方法で、リンク先のURLを必ず確認してください。

《フィッシングメールの一例》

From: MY TS3 <info@ts3card.com>
Sent: [REDACTED]
To: [REDACTED]
Subject: TS3 TS CUBIC CARDカード 【重要：必ずお読みください】

弊社からお送りするメールアドレスに偽装されていることもあります

※このメールはお客様の会員登録の情報が変更されたことをお知らせする重要なご連絡です。

ただいま、お客様からの変更処理に基づいて会員登録情報が変更されました。あなたが正しいアカウントの所有者であるかどうかを確認する必要があります。

<https://my.ts3card.com/webapp/ToTP01020101Action.do?command=doInit&UNIQUEID=mvlej>

TSキュービックカードカスタマーサポートセンター

From: MY TS3 <myts3@ra.tscubic.co.jp>
Subject: TS3 TS CUBIC CARDカード 【重要：必ずお読みください】

myts3@ra.tscubic.co.jp

TS CUBIC CARDをご利用いただき、誠にありがとうございます。

アカウント情報の有効期限が切れました。

■ MY TS3ログイン ■

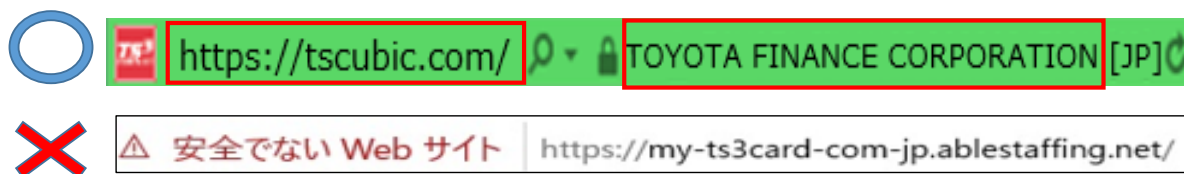
※本メールは、セキュリティ強化のため、電子署名をつけてお送りしています。

弊社のメールアドレスとよく似ている場合があります

例③ アドレスバーのURLが違う

TS CUBIC CARDモールのURLは、
「https://tscubic.com/」、「https://ts3card.com/」、
「https://my.ts3card.com/」 を使用しております。

アドレスバー(URLが表示される箇所)に企業名が表示されるブラウザの場合は、
「TOYOTA FINANCE CORPORATION」と表示されます。

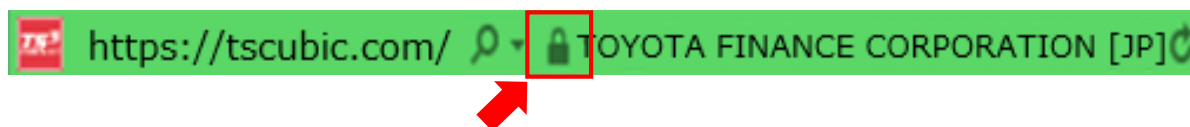


例④ 個人情報を入力する画面で、SSL証明書の鍵マークがない

アドレスバーに鍵マークが表示されていることを確認してください。

※鍵マークがあっても、必ずしもフィッシングサイトではないとは限りません。

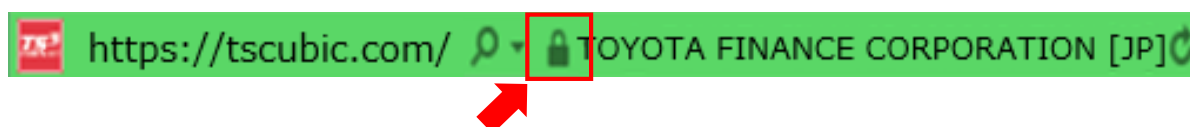
例①、②、③と併せてご確認ください。



鍵マークはSSLという通信技術によってやり取りが暗号化されている場合に表示されます。
その鍵マークをクリックすると、証明書の内容を表示することができます。

【ご確認方法】

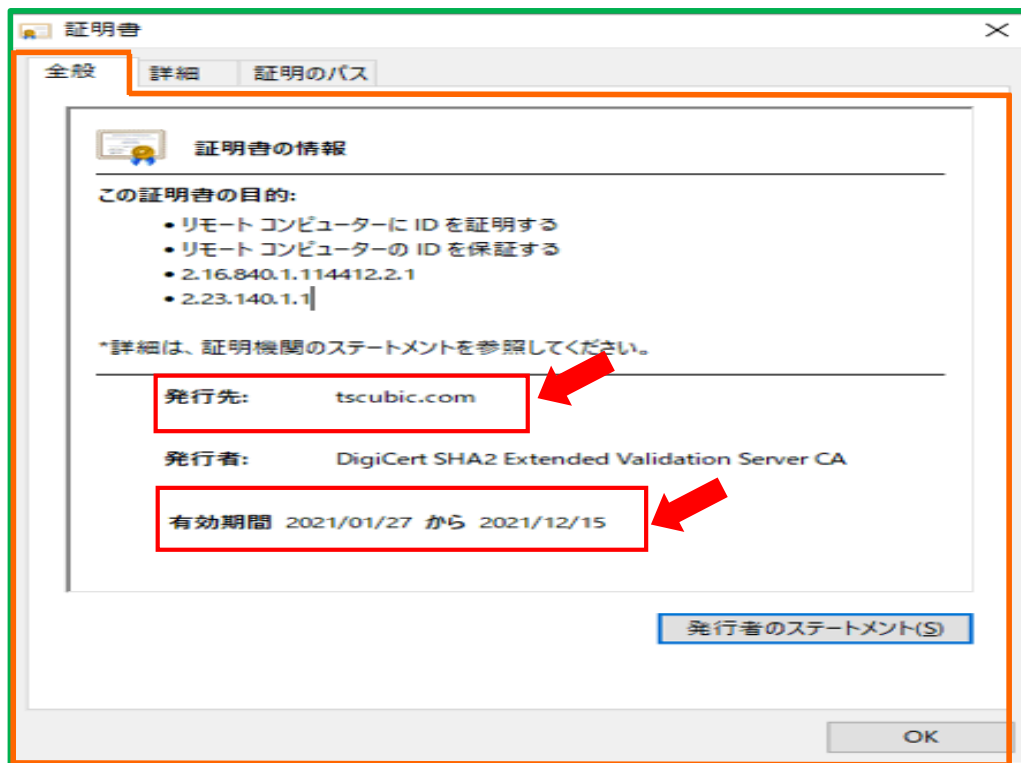
(1)鍵マークをクリックしてください。



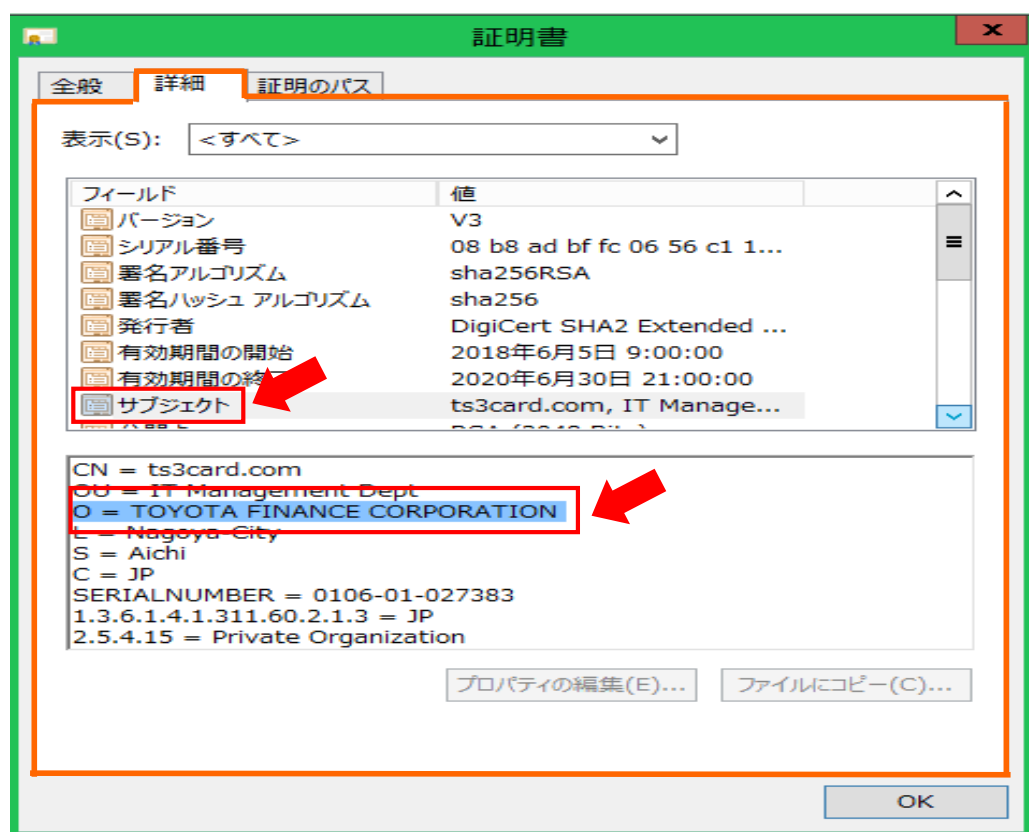
(2)「証明書の表示」をクリックして証明書の情報を表示してください。



(3) 証明書情報の「全般」タブ内の発行先が「tscubic.com」であること、有効期間が切れていないことを確認してください。



(4) 続いて、「詳細」タブ内の「サブジェクト」をクリックして、「O=TOYOTA FINANCE CORPORATION」であることを確認してください。



《被害に遭わないために》

1.個人情報やクレジットカード番号等の入力を促すメールに注意しましょう

メールで直接クレジットカード番号や暗証番号等を問い合わせたり、回答をお願いすることはありません。メールに記載されている URLはクリックせず、メールを削除してください。

2.届いたメールに記載されているURLが正しいものか確認しましょう

公式WEBサイトのURLと相違がないか必ず確認するようにしてください。

3.IDやパスワードの管理をしましょう

複数のWEBサイト(オンラインサービス)等で同じIDやパスワードの使いまわしはせず、WEBサイトごとに異なるIDやパスワードを設定しましょう。

4.OS、ブラウザ、メールソフトのアップデートをきちんと行いましょう

セキュリティ上の欠陥を放置しておく、ホームページを見たり、メールを開いただけで、不正なプログラムをインストールされる場合があります。

5.トヨタファイナンスやTS CUBIC CARDを名乗る疑わしいメールが届いた場合は、すぐにインフォメーションデスクまでお問い合わせください

● 万一、クレジットカード番号などを入力してしまった場合は、カード情報が第三者に不正に利用される可能性があります。

会員番号変更のご相談をさせていただきますので、カード裏面の電話番号までご連絡くださいますようお願いいたします。

● ご請求金額確定のご案内(メール、またはご利用代金明細書)が到着しましたら、お支払い金額のご確認とともに、ご利用明細のご確認をお願いいたします。