SSL証明とは？

もくじ

SSL証明とは？

・相互の通信を暗号化し『なりすまし』『盗聴』『改ざん』を防ぐ手段です

・暗号化方法は『共通鍵暗号方式』『公開鍵暗号方式』と『秘密鍵』を利用

・またそのセキュリティを証明する事をさします

登場人物

REO

東京に単身赴任中

嫁さん

福岡にいる

悪いくま

いわゆるハッカー

嫁そっくりさん

ハッカーが作ったニセ嫁

ドラえくま

こわいくま

泣き虫くま

くまくん

アラブくま

つよいくま

SSL化されていない通信のリスク

REO

冷蔵庫に
チョコレート
アイスを
隠しています

はがきでのやりとり

嫁さん

悪いくま

はがきでやりとりしているな！
これならすぐにイタズラできるぞ！！

なりすまし

REO

預金通帳と
印鑑はどこに
置いているの？

嫁そっくりさん

お菓子を
入れている
箱の中だよ

悪いくま

嫁そっくりさんを使えば
簡単に情報が聞き出せる！！

盗聴

REO

預金通帳と
印鑑はどこに
置いているの？

嫁さん

お菓子を
入れている
箱の中だよ

悪いくま

暗号化されていない(はがき)
やりとりなんてイチコロ！

改ざん

REO

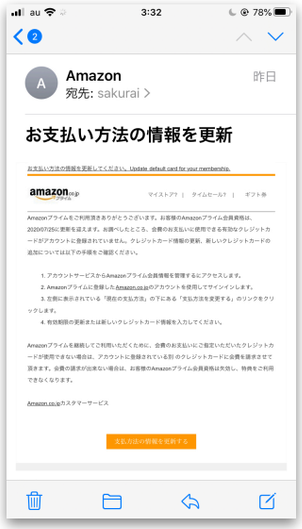
チョコレートは
どこにあるの？

預金通帳と
印鑑はどこに
置いているの？

悪いくま

なりすまし

Amazonや楽天を装い
支払い口座の再登録を促す



盗聴

例えばFree Wi-Fiに接続するとします。
利用するために、ID・パスワードを登録して利用します。
それは本当にFree Wi-Fiですか？
ハッカーが作ったテザリングだったら・・・
IDとパスワードを使い回ししていませんか？？

改ざん

上記２つでIDやパスワードが漏れてしまった場合
データの改ざんは容易です。
例えばAmazonにチョコレートを１ケース発注したのに
届いたのが１００ケースだった・・・
改ざんされた可能性があります

au 3:32 78%

2

A **Amazon** 昨日

宛先: [redacted]

お支払い方法の情報を更新

お支払い方法の情報を更新してください。Update default card for your membership.

amazon.co.jp プライム　マイストア? | タイムセール? | ギフト券

Amazonプライムをご利用頂きありがとうございます。お客様のAmazonプライム会員資格は、2020/07/25に更新を迎えます。お調べしたところ、会費のお支払いに使用できる有効なクレジットカードがアカウントに登録されていません。クレジットカード情報の更新、新しいクレジットカードの追加については以下の手順をご確認ください。

1. アカウントサービスからAmazonプライム会員情報を管理するにアクセスします。
2. Amazonプライムに登録したAmazon.co.jpのアカウントを使用してサインインします。
3. 左側に表示されている「現在の支払方法」の下にある「支払方法を変更する」のリンクをクリックします。
4. 有効期限の更新または新しいクレジットカード情報を入力してください。

Amazonプライムを継続してご利用いただくために、会費のお支払いにご指定いただいたクレジットカードが使用できない場合は、アカウントに登録されている別 のクレジットカードに会費を請求させて頂きます。会費の請求が出来ない場合は、お客様のAmazonプライム会員資格は失効し、特典をご利用できなくなります。

Amazon.co.jpカスタマーサービス

支払方法の情報を更新する

au 3:33 78%

全受信

【楽天市場】 金曜日

宛先: [redacted]

お支払い方法を更新してください知らせ(番号：820033)

Rakuten Card　楽天カードからのお知らせ

楽天カードアプリ | 楽天e-NAVI

お支払い方法を更新してください知らせ

[redacted]

残念ながら、あなたのアカウント
楽天会員個人情報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
楽天会員個人情報を確認する必要・ェあります。今アカウントを確認できます。

続けるにはこちらをクリック

なお、24時間以内にご確認がない場合、誠に勝手ながら、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。どうぞよろしくお願いいたします。メ。

サイト製作者(出品者)

つよいくま

WEBサーバー
（メルカリ）

＊WEBサーバーは世界中の莫大な情報(無料や有料級)が格納されているデジタル版メルカリと思って下さい。
そしてSSLはそれぞれの出品者が設定をします
配送の仕方を『ハガキ』で行うか『宝箱』で行うか？
です。そしてこのやりとりが高速で行われています

チョコレートの作り方を知りたい

チョコレートの作り方レシピ

強くなる方法

強くなる方法が知りたい

シレッとハガキを盗み見する

悪いくま

ハッカー(泥棒)

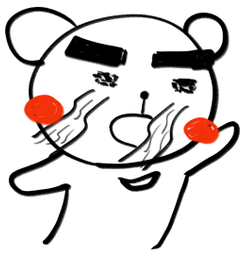
REO

クライアント(購入者)

嫁さん

ドラえくま

こわいくま



泣き虫くま

くまくん

アラブくま

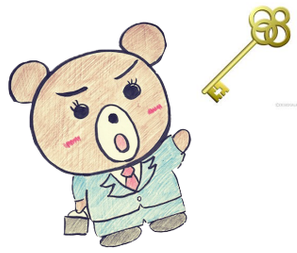
暗号化による通信の仕方

『共通鍵暗号方式』と『公開鍵暗号方式』『秘密鍵』を使った通信方法です

暗号による通信

共通鍵暗号方式

お互い共通の鍵を持っている



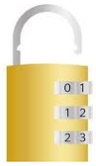
REO

嫁さん

悪いくま

鍵がないとあの宝箱は開けられない・・・

公開鍵暗号方式



手紙を宝箱に入れてこのダイヤル式南京錠
をかけてから送って！！

嫁さん

REO

僕も番号はわからないけど、とりあえず
鍵かけて送るねー！！

ダイヤル式南京錠を解除する『番号』は
私しかしらない『秘密鍵』だから安心！

嫁さん

サイト製作者(出品者)

REO

WEBサーバー
（メルカリ）

チョコレートの作り方を知りたい

強くなる方法が知りたい
この鍵をかけて宝箱にいれて送って！

盗み見ができない

ハッカー(泥棒)

悪いくま

強くなる方法

クライアント(購入者)

嫁さん

ドラえくま

こわいくま

泣き虫くま

くまくん

アラブくま

つよいくま

SSL化をするという事は『暗号化する為の』『鍵』や『宝箱』を使える様になる事と思って下さい

『鍵』や『宝箱』を提供してくれるのが『WEBサーバー』ですが、
そのWEBサーバーに『認証局』から発行された『証明書』を提出する事で
『WEBサーバー』は『鍵』と『宝箱』を提供してくれます

REO

①鍵や宝箱を使いたいを申請

認証局

②諸々確認して証明書を発行

③証明書を持って『鍵』『宝箱』をもらい
以後、WEBサーバーにあるデータを
『鍵』と『宝箱』を利用して利用者に
提供をする事ができる

WEBサーバー
（メルカリ）

利用者

④鍵と宝箱を使えるため
安心してREOさんが
作ったサイト(本)を
借りる事ができる

SSLの種類

・ドメイン認証

・企業実在認証

・EV認証

の３種類によってSSLは段階的に証明されています

ドメイン認証
DV認証

無料〜約３万円(年払い)

そのドメインをちゃんと契約して利用しているか？(WHO IS情報)
を確認して認証されます。

ドメインの契約書をもとに発行されるので、個人事業主での容易に取得

有料と無料がありますが、違いは『サポートの有無』のみです

企業実在認証
OV認証

約６万円(年払い)

そのドメインをちゃんと契約して利用しているか？(WHO IS情報)
を確認して認証されます。

また帝国データバンクなどを活用し『実在する会社』どうかの実態を把握します

EV認証

約１２万円(年払い)

上記に加え、登記簿等を確認します。
また、アドレスバーが緑色になりますので、
大手ECサイト・銀行・証券会社などが採用しています

楽天などはEV認証です！
EV認証だとアドレス自体が緑色で表記されたりしますので、偽物が本物か
判断しやすいと思います！(ブラウザによっては色が変わりません)

＊金額はGMOを参照

おまけ

SSLとTSLの違いは？

偽サイトにアクセスしようとしています・・・

この接続ではプライバシーが保護されていません

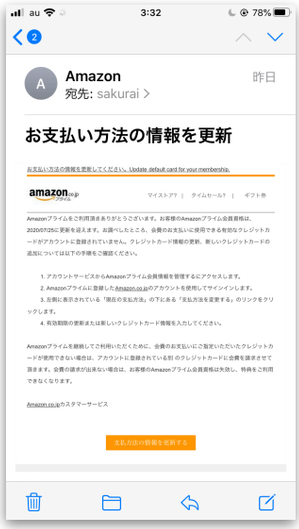
SSLとTLSの違いは

SSL(セキュア・ソケッツ・レイヤー)
TLS(トランスポート・レイヤー・セキュリティ)

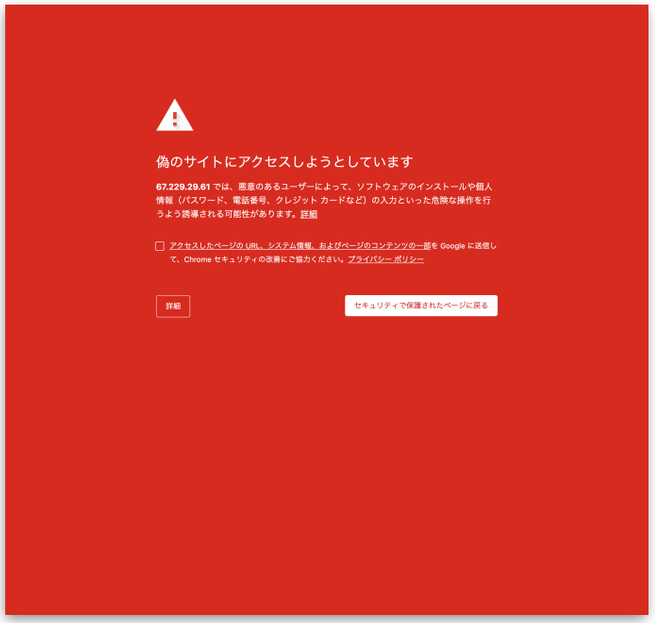
これは一緒です。もともと一つの企業がSSLを取り組み始め、
脆弱性が発見されてきたため、第三者期間がSSLの研究を始めました
それからTLSと呼ばれるようになっただけです。
要はSSLの次世代型がTLSなのです。

ただ、昔の名残でSSLと今でも呼ばれています

偽サイトにアクセス



アクセスすると・・・

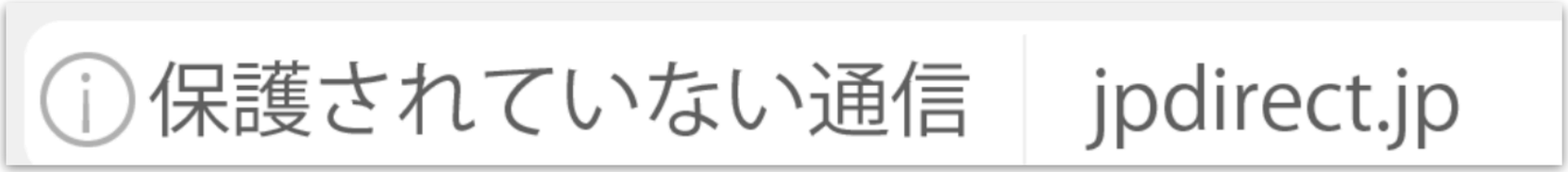


これはGoogle Chromeを利用すると上記の様に教えてくれます。
これはGoogleがフィッシングサイトと認識しているので上記の様な表示なるのです

間違って偽サイトにアクセスしようとしても一応上記のように教えてくれるので
安心ですが、自分自身もウィルス対策やちょっとした知識をいれる勉強はしましょう！

保護されていない通信

SSL化されていないサイトは左記の様な
警告が表示されます
この場合でも詳細設定からサイトを
閲覧する事は可能ですが、ちょっと嫌ですよね



また、SSLが十分で
ない場合はアドレス
バーが左記の様にな
ります。

左記の様に南京錠のマークが出れば
問題ありません！

サイトの信頼はこういうところが大事です！
『被害者』にならない『加害者』にもならない！しっかり意識しましょう！