ネット社会というのは　ここ 20 年で　急速に出来上がってきたものです。
インターネットは特別な世界ではなく、現実の法律が働く実社会の一部です。
大人が持つ社会常識を適切に働かせることで、安全に利用することが可能なメディアです。
しかしながら　急速に出来上がってきたもので、一般のユーザーからは分かりにくい部分が多いのも確かです。

現在、サイバー犯罪といわれるものの多くは、一般ユーザーの不安な心の隙間や、無知を利用して引き起こされています。
トラブルに巻き込まれるのを未然に避けるためにも、少しの予備知識を身につけましょう。

【悪質サイトとは？】

- 利用者の個人情報を　無許可で搾取し、自分の利益に結び付けようとするサイト
- 利用者の無知に付け込んで、お金や情報を搾取しようとするサイト

【悪質サイトと疑うサイトの特徴】

1. 利用規約と会社概要が用意されていないサイト
2. 利用規約の記述に法的に有効だと認められない記述が　多い サイト
3. 個人情報に関しての記述がないサイト
4. 「利用者のため」として「外部の会社に必要な個人情報を提供する」としているサイト
5. トラブルが起こった際の窓口の設置がなかったり、記述がないサイト
6. 「入り口」や画像をクリックした時点で、契約完了や会員登録をされたとみなすサイト
7. 利用規約の中で、「法律上問題ない」とか「ワンクリック詐欺でない」などと主張しているサイト

利用規約
サービスなどを受けるに当たって、事前に承認すべきものとして規定されているルール。
サービスやコンテンツを提供しているサイト側の主張であり、合法的なものかどうかは保証されていない。

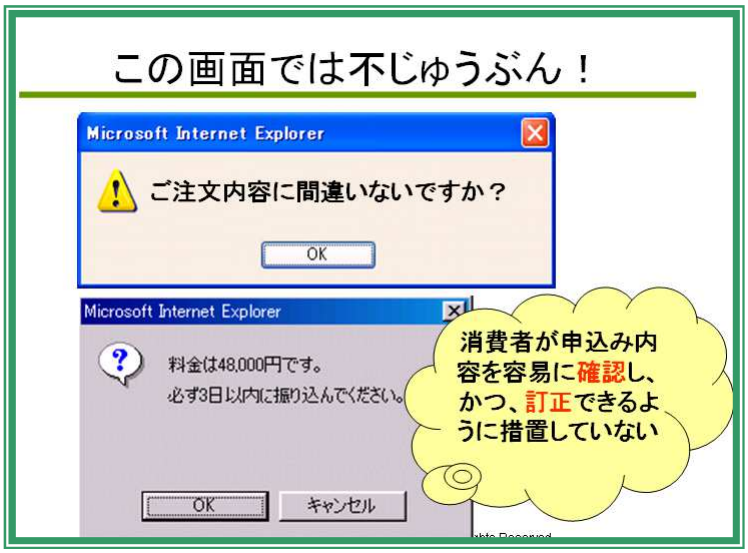
【知っておきたい法律 豆知識】

◎特定商取引法第 14 条・・・顧客の意に反して契約の申込みをさせようとする行為の禁止
◎電子消費者契約法　　・・・電子商取引などにおける消費者の操作ミスの救済、契約の成立時期の転換などを定めたもの

インターネット上で有料コンテンツの契約を成立させるには消費者に改めて料金が発生する事をわかりやすく　明確にしなくてはいけません。
民法では、法律行為の要素に錯誤がある場合に、意思表示は無効とされます。
表意者に重過失があっても、相手に悪意があれば無効の主張が認められます

事業者は、申込みボタンを押した後に、消費者が入力した申込み内容を一度確認させるための画面などを用意する必要があります

「ワンクリック詐欺」という言葉で代表されるように、一度のクリックで「登録完了」とか
「注文完了」とか主張するサイトは、**処罰対象**になります。



それではと、右記のような画面で確認を済ませようとするサイトも、消費者保護の見地から、
「申込みボタンを押す＝購入（有料）である」
「確認や訂正が容易にできる」
ように措置されていないので、**処罰対象**となります。

電子契約では、事業者側の申込み承諾の通知が消費者に届いた時点で契約成立となります
この「申込み承諾の通知」は、ディスプレイ上で**「登録完了」「注文を受け付けました」**とでても、契約成立とはなりません。
サイト運営側からメールなどで「申し込み承諾」「注文受付メール」が利用者に届いた時点で初めて契約成立となるとされています。

◎**個人情報保護法**・・・個人情報保護法が摘要されるのは「個人情報取扱事業者」になります。

- **個人情報を入手する際は利用目的を明示する。**
- **利用目的以外に個人情報を利用できない。**
- **購入した名簿でDMを出すことは出来ない。**
- **委託業者でのデータ処理は発注元に責任がある。**
- **個人情報保護の社内体制を構築する。**
- **個人情報苦情窓口を設置する。**

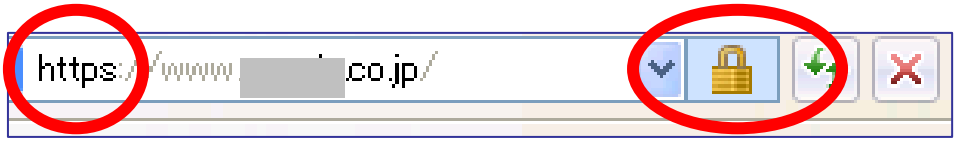
顧客の情報を取り扱うサイト運営者は、**個人情報保護指針(プライバシーポリシー)**や**利用規約**等のなかで、入手した情報の取り扱い方を公表することが望ましいとされています。

悪質サイトの中には、
IP アドレス・固体識別番号・プロバイダー名
を表示して
「**あなたの情報を把握しました**」「**未払いの場合、IP 等の情報を元に自宅・通勤先などに請求をさせて頂きます**」
などと威嚇してくるものがありますが、これだけでは、一般人では個人を特定することはできません。
少なくとも、プロバイダー自身が「個人情報保護法」を遵守しなければいけない立場なので
おいそれと　顧客の情報を流すようなことをしないためです。

もし　これらの表記に出会ったなら、その後あなたから　連絡を取らない限り相手はあなたを特定出来ません。
利用者としては、決して快いものではありませんが、対応としては、連絡しない・支払わない・**無視**が基本です。

【情報送信時の暗号化】
まともなサイトは、顧客が個人情報を送信する際、情報が外部に漏れたり改ざんされるのを防ぐため、「送信情報を暗号化する」システムを導入しています。

ＳＳＬと呼ばれるウェブサイトで入力する個人情報や金融関係の情報などを暗号化して安全に
送受信する技術を使っている場合、サイト利用者が　確認できます。



アドレスバーの表示が　https://　　通常(暗号化されない場合)は　http://
鍵マークが表示される　　通常は表示されない。

※鍵マークをクリックすると　サイトの身元確認ができる「SSL サーバ証明書」が表示されます。

ウェブサイトでパスワードやクレジットカード情報などを入力する前には必ず確認しましょう。

【フィッシング詐欺に気をつけよう】
◆フィッシング詐欺とは
悪意の第三者が、会員制ウェブサイトや有名企業を装い、クレジットカードの会員番号や銀行預金口座を含む各種サービスの ID やパスワード・個人情報を、獲得することを目的とする行為

◆誘導の手口
成りすましメール
・・・銀行やクレジット会社　その他サービスサイトを装い、ID・パスワード入力画面へ誘導
懸賞サイト・パチスロサイトへのお誘いメール
・・・楽しいサイトや、興味をひくサイトへ誘導し、メールアドレスやその他情報を取り出したりスパイウエア（ボット）を埋め込んだりする

フィッシング詐欺の被害

•クレジットカード情報の不正利用

クレジットカード番号・暗証番号などを盗まれ、ショッピングをされたり、
偽造カードをつくられてしまう

•インターネットバンキングによる不正出金

ID・パスワードを盗まれ、銀行口座に入っていた預金を
他の口座に送金される

•インターネットオークションにおけるなりすまし

ID・パスワードを盗まれ、オークション詐欺などに利用されてしまう。

•個人情報の不正売買

重要な個人情報を盗まれ不正に売買された結果、
不特定多数の犯罪者に悪用されてしまう

【悪質サイト対策】

- **利用規約・プライバシーポリシーの中に眼を通し最低限の必要事項は把握しておくこと。**
  - 入会・契約・退会・解約時の　要件
  - 個人情報の取り扱い方
  - トラブル時の　窓口・問い合わせ先
  - 運営会社が主張する免責事項
- **個人情報を入力するとき、暗号化されているサイトであることを確認する。**
  - アドレスバーをみて　「https://～」から　始まっているか
  - 鍵マーク（電子証明書）がついているか
- **ＯＳ・ブラウザーのアップデートを行い、最新の状態にしておく。**
- **ウイルス対策ソフトを導入し、最新の状態にしておく。**
- **不審な Web サイトを閲覧したり、迷惑メールなどのリンクをクリックしない。**

【資料引用・参照】

ｳｨｷﾍﾟﾃﾞｨｱ　フリー百科事典	http://ja.wikipedia.org/wiki/
携帯裏技倉庫	http://www.urawazasouko.com/e/urawaza.html
平成 24 年 3 月 15 日発表　警察庁　広報資料	http://www.npa.go.jp/cyber/statics/h23/pdf01.pdf
画像「こどもや赤ちゃんのイラストわんパグ」	http://kids.wanpug.com/
フィッシング対策協議会	https://www.antiphishing.jp/
日本ベリサイン株式会社	https://www.verisign.co.jp/
初級詐欺師の館	http://zero-trickster.blogspot.jp/