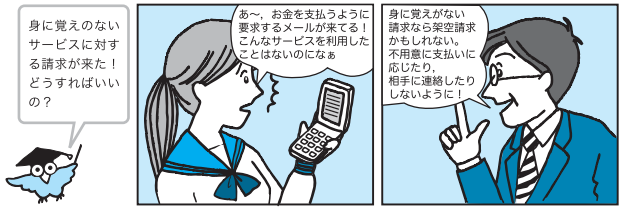
1
携帯電話に潜む危険

1-1 架空請求メール詐欺



架空請求とは

架空の未納料金に対する請求を架空請求といいます。Webサイト管理者や債権回収業者を装った者が無差別に，一方的にメールで有料Webサイトの利用料金などの通知書を送付する場合がほとんどです。実際にはまったく根拠がなく，業者が適当なメールアドレスを使ってやみくもに送信しているだけです。

架空請求の内容には入金をうながすものや，返信をうながすものなど，いろいろなパターンがあります。また，「入金がない場合には自宅やまで回収に出向く」「勤務先を調査する」などと不安をあおる文句が書かれているものもあります。こういった請求書を送りつけておき，恐怖心や勘違いにつけこむ悪質な手口といえます。

架空請求メールがきたら

利用していないサービスに対しては当然支払い義務がありません。無視をするのが良策です。確認の電話やメールでの返信は個人情報をわざわざ相手に知らせるようなものです。個人情報を教えてしまうとつきまとわれ，逃げ出せなくなる危険性があります。

また，一度支払ってしまうとさらに請求がひどくなり，大きな被害を受けることになります。もしトラブルに巻き込まれたり，身の危険を感じたりしたら，国民生活センターや警察署に相談しましょう。メールなどの証拠は，保管しておくことも大事です。

架空請求メールの例

貴殿が以前利用された「情報通信料金」について今日現在入金の確認がとれていません。お手数ですが至急当社までご連絡ください。
担当090-0000-0000
尚、入金のない場合は、消費者電子民法に基づき給与差し押さえ及び動産物差し押さえを強制執行させていただきます。
http://○○.jp/ij/××
まで返信ください。

- 存在しない法律を持ち出して，不安をあおっている
- 電話をかけさせようとしている
- 個人情報をリストに追加しようとしている

未納料金
未だに支払いがされていない料金。架空請求の場合は，有料サイトや有料番組など，何らかのサービスに対する対価を指すことが多い。

個人情報
住所・氏名・生年月日・性別・電話番号・メールアドレスなど，特定の個人を識別することができる情報のこと。
携帯電話番号などを返信させることで，個人情報のリストに追加する手口も見られる。

1-2 ワンクリック料金請求詐欺

ワンクリック料金請求とは

送られてきた電子メールに記されているURLをクリックしたときに，あるいはネットサーフィンしているうちに錯誤契約などし，突然利用料金を請求されるものをワンクリック料金請求といいます。特に携帯電話の場合，請求画面で個体識別番号や位置情報などを表示するよう仕組まれているため，個人情報が漏えいしたのではないかと不安を増幅させるのが特徴です。

ただし，携帯電話の個体識別番号や位置情報が事実だとしても，そこから個人情報を特定することは一般的にきわめて困難です。また，携帯電話事業者も請求元に個人情報を無条件に開示することはありません。よって，あわてて電話をしたり，メールを返信したりしてはいけません。

法律を知ることが大事

電子消費者契約法によると，事業者は，消費者に対して申し込み内容を再確認させるための画面を用意しなければなりません。つまり，このような措置が講じられていない場合には，その申し込みの無効を主張できるのです。ただし，利用規約に同意したうえでサービスを利用した場合は，支払義務が発生するおそれがあります。

以上を整理すると，意図して「登録」や「申し込み」などのボタンをクリックしていないなら，料金を支払う必要はないといえます。「不正なものは不正である」という強い気持ちを持って，無視することが重要です。

ワンクリック料金請求に対する心構え－５か条－

1. 利用規約がない場合は無視する。
2. 利用規約がある場合はよく読んで確認する。
3. 再確認画面がなければ申し込みの無効を主張できる。
4. 利用規約・再確認画面に同意した場合は支払い義務のおそれがある。
5. 悪質なものに対しては個人情報を伝えない。

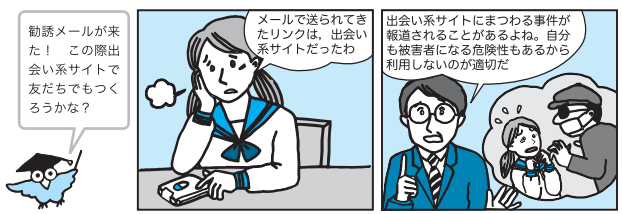
警視庁HPより

錯誤契約
いわゆる勘違いで成立した契約。ワンクリック料金請求の場合は，操作ミスによる契約を指すことが多い。

ワンクリック料金請求の画面の例

ご登録ありがとうございます！！
■あなたの携帯電話の個体識別番号
2Dot3f8ruY-3iK-pjNn
■あなたの現在位置情報
大阪府豊中市
を登録させていただきました。手続き完了です。ありがとうございました。
ご利用料金　￥36,000

1-3 出会い系サイトによる犯罪



出会い系サイトの被害実情

仲間を探したり，仲間と会話したりするのに非常に便利なサービスに電子掲示板やチャットなどがあります。このうち，異性と知り合う場を提供するWebページの総称がいわゆる出会い系サイトです。

警察庁には，出会い系サイトに関連した事件として，年間1500以上の検挙件数が報告されています（2004年中）。全事件のうち，携帯電話を使用したものが95％以上を占め，結果的に携帯電話が被害を拡大しているといえます。

この出会い系サイトを仲介に，見知らぬ者同士が接することで，殺人・強姦・恐喝・脅迫・児童買春などに発展する事件が多発しています。この事件の被害者のほとんどが18歳未満の児童で，その大多数が女子児童です。

また，出会い系サイトに書き込んだ個人情報が悪用されて事件に巻き込まれるケースがあることも見逃せません。

被害にあわないようにするために

出会い系サイトに関連する事件から18歳未満の児童を守るため，2003年に出会い系サイト規制法が施行されました。その概要は，

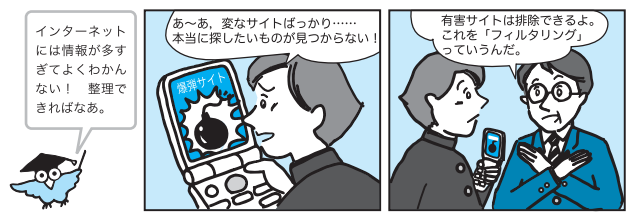
1．**児童が出会い系サイトを利用することの禁止**
2．**出会い系サイトで児童を性的行為に誘うことの禁止**
3．**出会い系サイトで児童にお金などを支払う約束をし，異性交際に誘うことの禁止**

です。大人だけでなく，もちろん児童も処罰の対象となります。

犯罪に巻き込まれないようにするには，出会い系サイトに危険が潜んでいる事実を認識し，出会い系サイトを「見ない」ことが最善策です。出会い系サイトの勧誘の携帯メールが届いても，やはり「見ない」ことが大切です。もし周りに出会い系サイトを利用している友だちがいたら注意しましょう。あなたのちょっとした一言で，事件をくい止めることができる可能性があるのです。

出会い系サイト規制法
正式名称「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律」。2003年6月13日公布。違反者は100万円以下の罰金。

1-4 有害サイトの氾濫



有害サイトの種類

インターネット上には利用価値の高い有益なWebサイトがある反面，倫ぴょう性に欠けるサイトや，害を及ぼす有害サイトが氾濫しています。近年特に，凶悪事件にまで発展する有害サイトが多数見られ，一歩インターネットの世界に足を踏み入れると，危険ととなり合わせであるという事実を認識しておく必要があります。

有害サイトは，以下の種類に分けられると考えられます。

1．**犯罪を誘発するもの**
　わいせつな画像・文章，出会い系，薬物売買など
2．**精神的に悪影響を与えるもの**
　暴力の画像・描写，自殺幇助，過激な主張，誹謗中傷など
3．**物理的に悪意を及ぼすもの**
　コンピュータウイルスの感染，スパイウェアの感染など

インターネットでは，だれにでも情報を発信する権利がありますが，受信する側にも情報を選択する権利があるといえます。

有害サイトへの対策

有害サイトへの対応としては，以下の方策があるといえます。

1．**行政による法規制**
2．**ソフトウェアによる制限・遮断**
3．**業界によるガイドライン作成**
4．**ホットラインの確立**
5．**利用者のメディアリテラシーの向上**

利用者の視点に立った場合，２と５が重要になります。特に２において，すでに有害サイトを制限・遮断する技術が築かれており，これをフィルタリングといいます。携帯電話事業者やプロバイダでこの機能の申し込みが可能です。また，フィルタリングソフトとして市販もされています。

フィルタリングを導入することで，ある特定の有害サイトへのアクセスを遮断することができ，またインターネット利用時間も制限することができます。

スパイウェア
コンピュータ利用者の行動パターンや個人情報を収集し，利用者の許可なく特定の場所へ送信するアプリケーションプログラム。

フィルタリングソフトとして市販
有料のものも多数出回っているが，「財団法人インターネット協会」では無料でソフトを入手できる。なお，Microsoft社のMicrosoft Internet Explorerでも，メニューバーから［ツール］→［インターネットオプション］でフィルタリングの設定をすることができる。