

第9章 架空請求について

依然として続いている架空請求は形を変えながら進化しています。

アダルトサイトを装った架空請求から実名会社を装った架空請求や弁護士を語った架空請求、最近では少額訴訟のシステムを悪用した架空請求まで存在します。

この他にも次の章で説明するインターネットを使ったネット詐欺的な物から、そのネット詐欺に便乗した架空請求まで、利用できる物は何でも利用できるようになって来ています。

請求方法も「葉書」や「PCメール」「携帯メール」「電話」などがあり、その中には「何がしたいか判らない物」まで様々です。

この中で注意すべきは「葉書」による物です。

その他の物は全く心配ありません。

では葉書の物は何が違うのでしょうか？

それは「名簿」が使われているのです。

メールはネット上などからアドレスは入手できますが、個人情報までは入手されません。

その証拠にメールで来る架空請求には「請求先名」は入っていません。

電話も番号を順番にかければ誰かにつながりますので「〇〇さんですか」と、電話をかけた先の名前を言わない場合が多いのです。

かけた先の名前を言うてくる場合は、その電話の前に間違い電話があつたりしますし、電話に出るとテープで請求してくる場合もあります。

結局、請求先の事を知らないのです。

しかし、名簿の場合は住所・氏名が知られており、少額訴訟のシステムを利用した手口に利用される可能性が高くなります。

この少額訴訟を使った手口は「架空請求は無視」が原則と言う事を利用して来るのです。

少額訴訟は、出廷や異議申し立てをしなければ、訴えた側の主張が全て認められてしまうのです。

つまり、架空請求を無視している相手に少額訴訟を起こす訳ですね。

それで、裁判所からの通知も無視してしまうと、相手の主張が認められて「架空請求」が「実請求」に変わってしまうのです。

まだ、実際に裁判所の通知まで無視して請求が認められた人は滅多にいませんが、この方法が多用されれば被害者も出てくると考えられます。

裁判所から通知が来たら「異議申し立て」または「問い合わせ」をすれば良いだけなんですけどね。

住所や名前を知られているという事は、こう言った変化技を仕掛けられる可能性が有る訳です。

では、次のページで実際の架空請求葉書をご覧下さい。

介入通知書

前略、御息ご申し上げます。

この度、貴方様から現在ご利用頂いている様々の金融機関の方々から債権回収の依頼を受理致しました。金子法律事務所と申し上げます。早速では御座いますが、現在貴方様にご利用されている金融機関での御契約条項の「期限の利益の喪失」に該当している事は十分御察しの事と存じます。よって貴方様はこれ以上御支払いをする意思が無いと判断させて頂いた事「金融法第二十四条 債権譲渡等の規制」により貴方様の債権回収業務を強制的に実行させて頂きます。これと同時に御利用されている金融機関の全停止処分、信用情報機関へのブラックリストとしての登録、更に財産と給与の差し押さえ等も行うことも付け加えさせて頂きます。尚、貴方様は既に一括請求が命じられていますので本日中に御入金、御連絡が無き場合は、弊社特別地方回収員がご自宅、勤務先は勿論の事、御親族関係者の方々に早急にお伺い、御相談させて頂く事になりますのでご了承下さい。しかし、貴方様の誠意遺憾によりましては御相談等に応じることも可能ですので、もし早期解決をお考えであれば至急下記まで御連絡下さい。

御 連 絡 先

080 - 3145 - 120

080 - 3435 - 184

受付時間 午前9時 から 午後3時

債権代理人 金子 総合法律事務所

(全国債権回収組合 加入)

(全国債権調査協会 加入)

尚、重要書類等は御入金確認後の郵送となりますので御承知申し上げます

この斜めの印刷と、お化けが出そうなフォントが何とも言えませんね。

法律事務所で連絡先が携帯電話な所が架空請求を物語っています。

この名前の法律事務所は実在しますが、その法律事務所が送っている訳ではありません。

(実名の文字は1文字消してあります)

この葉書の脅し文句は「信用機関へのブラックリスト」ですが、何処の金融機関かも書いていませんし、金額も書いてありません、重要書類はご入金確認後の郵送っておかしな話で、普通は最初に書類が来ます。

信用機関へのブラックリストも弁護士の仕事ではありません。

債権回収を名乗る架空請求の例

不良債権請求督促通達書（督促状）

第1 債権に対する債権の変更

貴方様のご利用されました**未納金**（有料番組等）について運営業者様から債権譲渡を承りました。

第2 裁判決議実施について

期日までに回答がない債務者につきまして、裁判決議に同意したとみなし、弊社顧問弁護士と共に協議の結果、次の通り最終和解案（債権減額措置、免責）を決定し最悪の場合、**裁判所の許可の下に担当回収員がご自宅に直接お伺いします**。ご自宅不在の場合はお客様の近隣調査を行い、会社等へ給料や財産等の差し押さえ手続きを行わせて頂きます。尚、ご本人様もしくは和解交渉の意思のある方は、大至急ご連絡して頂けるようお願いいたします。

この通達書は最終通告になります。

最終受付期限 平成16年5月31日（月）

お客様コード **DM14132**

担当者直通

090-9195-13

090-9179-31

090-9179-30

090-9179-31

090-9179-31

営業時間 平日 9:00~17:00

土曜 10:00~15:00

日曜祝日は営業しておりません。

株式会社 債権処理センター

〒110-0 東京都千代田区

債権回収は法務大臣認可しか債権回収を名乗る事も許されませんし、間違えやすい名前を使用する事も禁止されています。

認可の業者名簿にこんな名前の業者はありません。

しかも「債権に対する債権の変更」って何の事でしょう？

難しい言葉を使いたいのは理解出来ますが、無理やり使うと逆効果だと思いますけどね。

強調したい部分は赤字で、初めての葉書で最終通告とはおかしい話ですね。

債権回収業者の連絡先が携帯電話と言うのも「架空請求です」と言っているような物です。

有料番組となっていますが、どんな番組をいつ利用したとか、金額も書いてない債権回収って何なのでしょうね？

御請求通知書

整理回収グループ

TEL 6327-66

FAX 4622-63

担当

28 651

この度私どもは過去にあなた名義の電話回線から使用された有料アダルト番組について番組提供会社より未納利用料金に関する債権譲渡を受け、代わりに回収させて頂くこととなりましたので書面にてご連絡させていただきます。

現在下記記載の利用料金が未納となっておりますので遅延損害金、回収代行手数料と合わせて本請求通知書到着の翌日より銀行営業日以内を支払い期限として下記銀行口座までご入金頂くようお願い申し上げます。

本請求通知書の送付にもかかわらずご入金頂けず放置されますと最終的にあなたのご自宅まで訪問させて頂き、下記の合計支払い金額に交通費、人件費を加算して請求させて頂くこととなる場合がございますので必ずご入金下さい。

合計支払い金額	20,250 円
利用番組	モモコネット
未納利用料金	6,300 円
遅延損害金	4,450 円
回収代行手数料	9,500 円
振込先口座	三井住友銀行港支店 普通口座 口座名義 ヤマ カ ヤ

※振込の際は宛名面記載の回収整理番号を名前の前にご入力下さい。

これが初期の頃の架空請求で、請求がダイレクトですね。

家まで押しかけると言う脅し文句は今も使われていますが、この頃は債権譲渡と言ってはいませんが債権回収という言葉は使われていません。

こうして見ると使われる言葉が少しずつ巧妙になって行くのがよく判ります。

この葉書が架空請求の原型と言えます。

こう言った架空請求の葉書で「斜め印刷」になっている物は恐らく「プリントごっこ」で印刷した物でしょうね。

メールでの架空請求の例（ブラックリストタイプ）

[[電子消費者契約通信未納利用料金請求通達]]

弊社は信用調査会社様からの依頼に基づいて利用料金支払遅延者のデータを一括管理している株式会社日本データ管理機構と申します。

この度は貴殿が使用されたプロバイダー及び電話回線から接続された有料サイト利用について運営業者より利用料金支払遅延に関してブラックリスト掲載要請を受けました。

これまで貴殿の利用料につきましてはコンテンツ事業者方に未だご入金がなくまた、誠意ある回答も頂いておりません。

よって「電子消費者契約民法特例法」上、以上の理由から信用調査会社を經由して弊社に貴殿の個人情報を利用料金支払遅延者リスト（ブラックリスト）掲載要請が弊社に届きました。貴殿の情報に関しましては、既にメールアドレス（フリーメール含む）及びIPから、プロバイダー・ISP業者から情報開示を受け、貴殿の住所、氏名、勤務先等の情報は判明しております。

利用料金支払遅延者リスト（ブラックリスト）に掲載されますと、各種融資・クレジット契約・携帯電話の購入及び機種交換他、貴殿の日常生活における信用情報に今後大きな支障が発生する可能性があります。

つきましてはコンテンツ事業者及び、債権回収業者並びに顧問法律事務所とも協議の結果、次の通り最終和解案を決定いたしましたので通知いたします。

入金確認後、延滞情報リストから貴殿に関する全データを削除し、株式会社日本データ管理機構保管の債権譲渡証明書、内容証明等の書類一切を、抹消させていただきます。

ご入金して頂けず、このまま放置されますと、最終的に各地域の事務所から数名の集金担当員がご自宅及び、勤務先まで訪問をさせていただきます。

また、その際に掛かります費用・調査費用・交通費等の雑費は別途回収手数料も合わせてご請求させていただきます。

また、場合によっては裁判所を通じた法的手段にて強制執行による給料差し押さえ等を含めあらゆる手段で対応させていただく事になります。

また、メールアドレス相違、その他いかなる事由により今まで連絡が取れなくなっていたにせよ、それは弊社に起因するものではなく、お客様の責任によるものです。

円満な解決を望むならば受付期限までに大至急ご連絡をお願い致します。

※注意事項

昨日までの時点でご入金の確認が取れない方にお送りしております。

もし行き違いに入金済みの場合はご容赦ください。

株式会社**データ管理機構

受付期限 平成16年 10月 8日

ご連絡先 03-3462-****

営業時間 10:00~19:00 休日 日曜日

東京都中央区銀座*****

この「メールの架空請求」は葉書と違いスペースに制限が無いので文章が長いのですが、請求書なのに請求先が全く書かれていません。

つまり、内容は何が書いてあったとしても、誰に送った物かが明記されていないのが致命的ですね。

葉書の請求でも同じなのですが、架空請求は無理に難しい単語を使おうとする傾向がありますね。

「電子消費者契約通信未納利用料金請求通達」などは良い例ですね。

これらの架空請求への対応は「無視する事」です。

決して支払ったり連絡を取ってはいけません。

支払ったり連絡を取る事が更なる被害を生む事になる場合があるのです。

支払いをしてしまうと「脅せば金を払う」という認識を持たれてしまい、別件請求や別会社の請求が頻繁に来るケースがあります。

連絡する事で「ナンバーディスプレイ」により電話番号を知られて、夜中などに脅しの電話がかかり精神的に追い詰めてくるケースもあるのです。

もし、どうしても相手に連絡がしたい場合は「公衆電話」を利用するようにしましょう。

非通知設定でも良いのですが、設定を間違える事も考慮すれば「公衆電話」には設定の間違いがありません。

架空請求の見分け方をまとめると

- 1) メールの場合は請求先の名前や住所・電話番号の記載が無い
- 2) 振込先が書いてある場合の口座名義人の名前が個人名である
- 3) 連絡先が携帯電話である
- 4) 請求元の住所と振込先の支店所在地が全く違う
- 5) 電話番号の使われている地域と所在地が異なる
- 6) 法人でない債権回収業者は存在しない
- 7) 債権譲渡の債権元が書かれていない
- 8) 請求部分や脅しの部分を強調している
- 9) 何かと責任を押し付ける文章である
- 10) 単語の表記が間違っている（例：データー ⇒ データ 小額訴訟 ⇒ 少額訴訟）
- 11) 出来ない事を書く
- 12) 存在しない法律が書いてある
- 13) 法律の条文を知らない
- 14) 場合によっては請求期限を過ぎた後に葉書やメールが届く
- 15) 葉書の場合「プリントごっこ」を使っている
- 16) 普通使わない単語や「無理やり難しい言葉」を使っている
- 17) 脅し内容ばかりで内容に品が無い
- 18) 住所を地図検索で調べると「法務省」などの省庁だったりする

以上が架空請求の特徴です

ここで、名簿対策として私が行っている方法をお教えしましょう。

私は個人情報を入力する事を求められる場合に、役場や免許などの公的な物やプロバイダーや正式契約の物には正確な表記をして、懸賞や会員証、メンバーズカードなどの類の物には名前の文字を一字似た漢字や同じ読みの漢字に変えます。

例えば「加藤」ならば「加東」に、「敏男」なら「俊夫」に、「恵子」なら「慶子」などに変えるのです。

また、ビデオショップの様に免許を提示する場合は「和夫」ならば「和天」と言った具合に字を変えて、わざと崩した字で書くのです。

普段からこうしておく、流通している名簿の記載もこの表記になるので、宛名をみただけで名簿が利用されている事が判るようになりますし、自分が登録した所は覚えていたり、会員証やメンバーズカードにその表記が有るので何処で流出した情報なのかが区別できます。

私の所に来れた葉書による架空請求は、全てこの間違っただけの物でしたので配達された時点で名簿からと判りました。

この方法を使うとDMなども名簿が使われている事が判ります。

名簿を使って営業してくる業者には詐欺商法の物もありますので、この間違っただけの文字の郵便物は読む価値が無い物と判断し、全て読まずに捨てる目印になります。

架空請求は「身に覚えの無い請求」です、くれぐれも架空請求にはご注意ください。

第10章 ネット詐欺について

ネット詐欺と言っても色々有ります「ねずみ講」や「マルチ商法」から「ネットオークション詐欺」や「ワンクリック請求」など実に多彩です。

まず「ねずみ講」ですが平成12年頃は盛んにメールが来ましたが、逮捕者が出てからは姿を消しつつあります。

これは4人の口座名が書いてあり、そこに2000円ずつ振込みをして、一番上の振込先を消して最後に自分の振込先を記入して、大勢の人にメールを送るという物で、メールには弁護士のコメントとして「違法ではない」と言う事が書いてありましたが違法ですよ。

ネットオークションを利用した詐欺の多くは「入金したのに商品が送られてこない」と言った物で、これは決済方法が「入金確認後の発送」としている相手の出品には参加しなければ引っかかる事ありません。

ここで間違えてはいけないのが「商品内容が違う」とか「思っていた物と違う」と言った物は詐欺ではなくて「トラブル」や「クレーム」の部類に入りますので混同しないように。

またブランド物に関しても、ネットオークションでは偽者かどうかの鑑定は出来ません。

本物が欲しければネットオークションを利用しない事です。

その他にもネットオークションは業者も出展しています、欲しい物が安く出品されていても最終的な落札価格は、通常価格とほとんど差が無かったり、場合によっては安売り店で買った方が安い場合がありますし、通常販売価格が1000円の物を、1円からの価格で出品しても「最低落札価格」が800円なんて物もあり、この場合800円以下の入札には意味が無いですね。

これはネットオークションを行っているサイトは「ショッピングモール」も併設しています。そのショッピングモールで出店している業者の販売促進の要素が強いのです。

現在多発している物は「ワンクリック請求」と呼ばれる手口が猛威を振るっています。

これは、前章の「架空請求」の進化版です。

架空請求は「身に覚えが無い請求」と書きましたが「ワンクリック請求」は「身に覚えのある請求」を装う手口なのです。

しかも「商行為」を装っていますので、表面上は「商取引上のトラブル」と思われがちなので、交番などに相談に行っても「当事者同士で話し合ってください」と見当違いなアドバイスをされたりしますが、決して相手に連絡をしてはいけません。

架空請求の章でも書きましたが、連絡をする事で個人情報を取られて被害が増大します。

次のページではワンクリック請求がどんな物かをご紹介します。

このワンクリック請求は今後も進化していく事が予想されますので、詳しくご説明していきます。

ワンクリック請求と言っても「携帯サイト」の物と「パソコンサイト」の物があります。
これらのサイトへの誘導方法は以下のものがあります。

1. 携帯電話のショートメール

これが最も厄介な物です。

携帯電話のショートメールはそのアドレス自体が電話番号であるためそのメールからアクセスすると電話番号とショートメールアドレスが知られてしまいます。

また、そのメールの内容も「友人」を装ったり「着メロサイト」を装ったり「出会い系サイト」だったりします。

そして、その URL をクリックするとワンクリック請求サイトにアクセスしてしまうのですが「登録しない」や「同意しない」を押しても「登録」になってしまう場合が多いのです。そこで色々な**個人情報と錯覚**してしまう情報が表示される訳ですが、これに関しては次の「サイト自体の説明」でご説明していきます。

2. E-Mail

E-Mail は携帯メールでもパソコンメールでもどちらにも送られてきます。

その内容はアダルトサイトの広告や「こんにちは」など、女性からのメールを装ったり「出会い系サイトの広告」だったりしますが、注意すべきはその記載されている URL です。

/の後に「bWFraUBqp2hVZ3VhcnQuY59t」などの記号が入った物などは、この部分が送信先のメールアドレスを意味しています。

その為その URL をクリックするとメールアドレスが知られてしまうのです。

また、HTML メールでこの部分を見えなくして送られてくるメールもあります。

この場合はソースモードで表示し、A href="http://と言うタグの後ろに上記のような記号が付いていた場合はアクセスしただけでメールアドレスが知られてしまう可能性が有ります。

これらの方法は、上記のショートメールでも同様の手法が使われています。

3. リンク集

リンク集からは何も知られていませんが、上記の様なメールからアクセスした場合そのリンク先がリンク集であっても、そのリンク集の運営者がワンクリック請求の運営者の場合があります。

4. 掲示板

掲示板からアクセスしてしまう場合には2種類の場合があります。

相談掲示板などに相談者が直リンしてしまう場合と、ワンクリ運営者が自分で書き込む場合があります。

相談する際は http://のhを抜いて ttp://と書くように心がけましょう。

また E-Mail で解説した記号の部分は消して書く事も必要です。

これらが誘導方法のご紹介ですが、これを踏まえてサイト自体の解説をしていきます。

この「ワンクリック請求」は勧誘から登録までが一体になった手口になっていますので、手口の流れを知る事も重要ですし、体系的にオレオレ詐欺とも共通部分が多い為このワンクリック請求が使っている心理トリックを知る事で、オレオレ詐欺対策も理解しやすくなります。

それでは順にご説明していきます。

まずは広告メールなどからアクセスして TOP ページへ行きます。
通常はこの時点で何もクリックせずにブラウザを閉じればなにもありません。
そこで何かをクリックすると直接登録画面が表示されるか下の様な動画が表示されますがサイトによって表示画面は異なりますので、代表的な物を 2 点ほど掲載します。



これを表示させる事で「情報を取られた」と信じ込ませやすくしています。
これは実際にはデータを送信している訳ではなく、JavaScript やFlash で動画を見せられているのです。
この動画が終わると、次のような画面が表示されます。

ご訪問ありがとうございます！

ご登録日 20●●年●●月●●日

あなたのIPアドレス	「65.39.205.●●」
あなたのリモートホスト	「65.39.205.●●」
あなたのプロバイダ	「65.39.205.●●」
あなたのネットワーク	「No match!!」

以上を登録させて頂き入会手続き完了しました。

IPアドレスとは？

インターネットやイントラネットなどのIPネットワークに接続されたコンピュータ1台1台に割り振られた識別番号。世界中にあるコンピュータを一意に決めるための住所のようなものです。

リモートホストとは？

Webユーザが利用したコンピュータに割り振られた名前に当たる情報です。Webユーザがどの組織に所属しているのか、どんなプロバイダを利用しているのかを知ることができます。

ご利用期間	「180日間」
ご利用料金	「¥45000」
	「ご入会日20●●年●●月●●日より4日以内」 に下記の口座までお振込み下さい。また、支払い期限を過ぎてお入金確認が出来ない場合、相約に基づきIPアドレス、

この画面の「あなたのIPアドレス」や「あなたのリモートホスト」や「あなたのプロバイダー」などが正確に表示される訳です。

そこに「IPアドレスとは？」とか「リモートホストとは？」とかの説明が表示されている訳です。

この画面が表示される前の「データ送信中」の後にこの画面が表示される訳ですから、「個人情報が送信されてしまった」と思い込まされてしまう訳です。

実際にはIPやリモートホストには個人情報は一切入っていませんが、先に説明しましたE-mailからアクセスした場合は、どのメールアドレスからアクセスがあったかが知られていますので、メールアドレスを表示したり、自動返信メールなどを使って登録通知を兼ねた請求メールを送ってくる訳です。

そんなメールが届いたら「個人情報が知られている」と思い込んでも無理はありません。

そしてこの表示画面には続きがあります。

表示画面の続きです

お振込み期日	「ご入会日20 年 月 日より4日以内」 に下記の口座までお振込み下さい。また、支払い期限を過ぎても入金確認が出来ない場合、規約に基づきIPアドレス、リモートホスト、アクセスログをプロバイダに提出しお客様のプロバイダ契約情報からご自宅、勤務先等へ直接請求させて頂く可能性がございます。その際に当番組管理部より延滞料金30,000円、延滞1日に付き1,000円の損害金を加算して請求される場合があります。
振込ID番号	「 」
お問い合わせ先	

銀行振込案内
振込先銀行名： 銀行 振込先支店名： 振込先口座番号：普通 受取人口座名義： 振込金額：¥ 45000 振込人名：あなたの振込ID番号を入れてください。
※お振込時の振込人名についての注意事項 振込人名は振込ID番号でお願い致します。 名前等でご入金された場合、処理できない可能性があります。 また、振込端末によってはご依頼人名が自動的にご利用口座名義となり振込ID番号での入力 ができない場合がございます。その際はお手数ですが確認のためご振込人名とお振込日、お振込み金額、及び振込ID番号をサポートまでメールにてお知らせください。

この文面で更に不安に陥れる訳です。

これらの文面は「連想させる」様に書かれています。

例えば取立てが「自宅に来た時」「会社に来た時」の事を連想させる心理誘導なのです。

そしてプロバイダ契約情報から個人情報を提示させるように書いてありますが、プロバイダは個人情報を教える事はありません。

つまり出来ない事を出来ると書いているのです。

しかし、ここまで来たら「頭の中は真っ白」になってしまい、何とかしようと相手に連絡を取ろうとする訳ですね。

実際には何の個人情報も取られていないのですが、ここで連絡をする事で相手に個人情報を教える事になる訳です。

つまり、不安に陥れられるために自分で個人情報を教えてしまう訳ですね。

これは別のサイトの文面です

	<p>サイト利用されたにも関わらず、支払期限を過ぎても入金が確認出来ない場合は「お客様情報」を元にプロバイダに対して 法的な手段を経て、情報開示を求めます。</p> <p>情報開示情報(以下項目)</p> <ul style="list-style-type: none">● 勤務先情報● 勤務先電話番号● 自宅住所● 自宅電話番号 <p>上記ログを元に自宅や勤務先へ直接請求させて頂く可能性がございます。その際に当番組管理部より延滞料金 ¥18,000、延滞1日に付き1,000円の損害金を加算して請求されることがありますので期日の方、お忘れなくお願い致します。</p>
--	---

会社内からアクセスされた方へ	<p>就業規則において就業時間中、及び、社内設備からのアダルトサイトへのアクセスが禁止されている場合があります。その際に、アクセスが発覚した場合に懲戒解雇、減俸等になることがありますので本サイトへのアクセスの際は就業規則等に抵触しないようご注意ください。</p> <p>当サイトではそのようなことが起きた場合でも保証、補償等を行いません。あくまでもアクセスされる方の自由意志、判断で本アダルトサイトへのアクセスをお願いいたします。</p>
----------------	---

ここにも連想誘導の手法が使われています。

「就業時間中のアダルトサイトへのアクセス」「アクセスが発覚した場合の懲戒解雇」などへの連想誘導を「就業規則に抵触しないように」という注意事項の形で行っています。

これは親切を装った脅迫なのです。

これも親切を装った脅迫です

<p>このサイトはご覧になられる方の利便性を考慮して、便利な「後払い制」を採用しております。</p> <p>※もし万が一、あなたの御支払いが滞ったりいたしますと、ご利用になられたコンテンツ名などを記載した書面にて直接ご請求させていただく場合や、債権回収部から料金を御支払いいただく旨ご自宅および勤務先へお問い合わせする場合がございます。また、御支払いいただく為のご連絡等が取れない場合等、悪質な場合は業界流の対応、又は、所轄裁判所より訴状を送付させていただきますので、皆様の利便性の為、何卒ご了承ください。</p> <p>最初にアクセスした日より4日間以内に御支払いいただけますと、下記の料金にて90日間のご利用が可能です。5日間以上経過いたしますと、通常料金を御支払いいただく事になりますので、お早めに御支払いください。</p> <p>御支払いに関するお問い合わせはメールにて <input type="text"/> までお問い合わせください。 正当事由が成立される方に関しましては別途、特別措置を設けておりますので、メールにてご連絡いただき、ご相談ください。</p>

これも、便利な後払いと言いながら「4 日以内に振り込め、振り込まないともっと高額な金額を請求するぞ」と言っている訳ですね。

この「業界流の対応」という所が、連想をかきたてる文面ですね。

そして「架空請求」の常套句である「債権回収」もしっかり使われています。

これは最初の画面の所なのですが、この様に並列になっています。

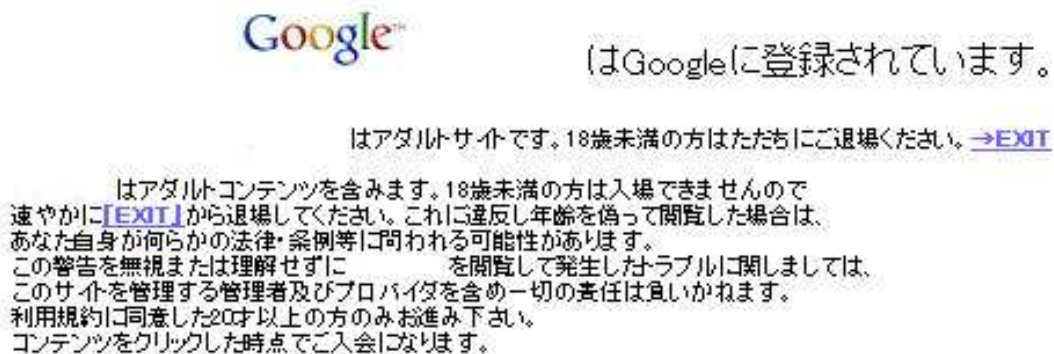


こう言った形で表示されている場合は、利用規約以外のどんな画像を押しても登録されてしまいます。

こう言ったワンクリック請求の TOP ページをソースモードで見ると、全ての画像に同じページへのリンクタグが埋め込まれているのが判ります。

登録された後に利用規約を読むと「画像を一つでもクリックした時点で登録になる」と書いてあり「規約を読まずにクリックした自分にも非がある」と思い込まれるのです。

また、TOP ページにこんな事を書いている所があります。



少しでも信用させる為に Google に登録されているって書いていますが、Google に登録って言っても「ロボはじき」にしていなければ、どんなサイトでも登録されているのです。

人気の Google に登録されていると言っても当然の事なので、こんな事を書く事自体が胡散臭いのですけどね。

検索エンジンに登録されている事を自慢できるのは Yahoo だけですし、Yahoo に登録されている所でも「登録されています」なんて事はあまり書きません。

架空請求も含めこう言ったワンクリック請求などには「権威主義」の傾向があります。

つまり信用させたり脅したりする場合にこの「Google」や「裁判所」などの「誰でも知っているが詳しい内容を知らない物」の名前を使用しているのです。

この「権威主義」はオレオレ詐欺も同じです。

オレオレ詐欺に関しては次章でご説明していきます

ここで携帯サイトのワンクリック請求についてご説明しましょう。

基本は同じですが、携帯サイトの場合の信じ込ませ方はもっと手が込んでいます。

まず情報の表示ですが、パソコンサイトでは IP アドレスやリモートホストでしたが、携帯サイトの場合は「使用機種名」「携帯電話のキャリア」「個別識別番号」などや、場合によっては「あなたのお住まい」などの情報も表示されています。

しかし、これらの情報にも全く個人情報が入っていないのです。

携帯電話は機種により画像解像度が異なりますので、画面の最適化をする為に機種情報などが送信されているのですが、それを表示しているに過ぎません。

「あなたのお住まい」などもアクセスポイントを表示しているだけで、住所が知られている訳では有りません。

しかし、ここまで自分の情報が表示されると「個人情報を知られている」と思い込んでしまうのも不思議ではありません。

また、パソコンサイトの場合は「利用規約」や「18歳未満」のリンク先だけは表示通りになっていますが、携帯サイトの場合は全てのリンク先が「登録」になる場合が多いのです。

ここにも心理スポットが有るのです。

画面の一例



こんな画面が表示されるのですが、ここでNOをクリックしても登録になってしまう場合が多いのです。

これは携帯サイトを作った事があると理解しやすいのですが、実はYESとNOの画像は一体になっているのです。

この手法はアダルトサイトではかなり古くからある手法です。

携帯サイトでは、この様なバナー系の選択表示をする場合は縦に二列になる場合が多く、横一列になっている場合は、一体表示になっている可能性が高い訳です。

NOをクリックしたのに登録になってしまった場合、多くの方は「操作を間違えた」と思い込み「自分のミス」と勘違いしてしまう傾向が強いのです。

そして「自分に非がある」と思うってしまう訳ですが、実際には相手にそう思わされているのです。

実証ワンクリック請求

実際にワンクリックに登録して実験してみました

ステップ1（広告メール）

広告メールは色々な形で来ます

「この前の妊娠検査について県立白姫女子高校保健室からのお知らせです。

間違って受け取った方は、お手数ですが、破棄してください。

お詫び致します。

該当する人は下記リンクより入ってお知らせを確認して下さい。

http://just-feed.net/shirahime/?*****（この***の部分が送信先のメールアドレスになっています）」

このメールの***のメールアドレスを表す部分だけをメールソフトの検索機能で調べると「オンラインお得情報 VOL. 108」と言ったメルマガを装って来ていた他のメールとリンク先が同じです。この URL をクリックすると



こう言った TOP ページが表示されます。

この「18歳以上なので入場する」をクリックすると

当サイトへご登録ありがとうございます。
あなたにはご利用料金が発生しております。

個人特定情報

あなたの登録日	2005年01月24日
あなたのIPアドレス	218.225.
あなたのプロバイダ情報	johoguard. .jp
あなたの登録メールアドレス	@johoguard.com
あなたの個人認識ID番号	Q0B154
利用履歴	これまでに「1」回のコンテンツ読み込み履歴があります。

■IPアドレスとは：インターネットやイントラネットなどのIPネットワークに接続されたコンピュータ1台1台に割り振られた識別番号。世界中にあるコンピュータを一意に決めるための住所のようなものです。
■プロバイダ情報とは：WEBユーザーが利用したコンピュータに割り振られた名前につながる情報です。Webユーザーがどの組織に所属しているのか、どんなプロバイダを利用しているのかを知ることができます。

上記の情報で登録させて頂き、入会手続きを完了致しました。

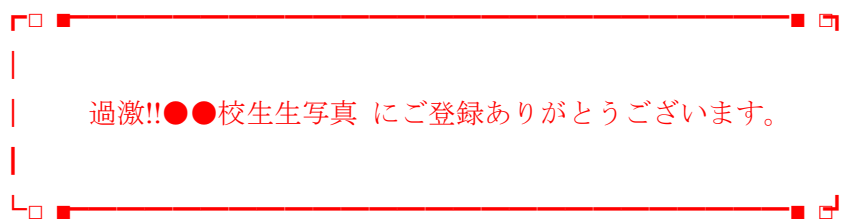
ご利用料金

当サイトの利用料金は全て税込み料金です。
90日間使い放題！完全定額制！

早期割引料金お申込みの方に限り、早期割引料金適用

典型的な登録画面になりました。

当然、広告メールにメルアド情報が入っていますので、登録完了メールが届きます



過激!!●●校生生写真にご登録ありがとうございます。

新規ご利用ありがとうございます。

入会手続きが完了致しました。

<入会記録>

■初回利用日時：2005-01-24 01:24:19

■登録 ID：CB*****

■商品名：過激!!○○○○生写真特別ページコンテンツ利用料金

■期間：90 日

あなた専用のメンバーページ

http://*****

次回より上記アドレスよりお入り下さい。

※この登録メールは会員登録された方に自動配信されております。

<サイトに関するお問合せ先>

080-5129-9***

この電話番号は AU 中部の物ですね。

ワンクリック請求の法的解釈はどのようなのでしょうか？

経済産業省の「電子商取引に関する準則」を元に解説していきます。

ワンクリック請求の登録には「確認画面」が存在しません。

これは電子契約法第3条の「確認を求める措置」で「最終的な意思表示となる送信ボタンを押す前に、申し込みの内容を表示し、そこで訂正する機会を与える画面を設定する事」

「あるボタンをクリックする事で申し込みの意思表示となる事を消費者が明らかに確認する事が出来る画面を設定する事」と規定されています。

また「意思の表明」で「確認措置を講じていない事業者が、一方的に確認措置を要しない旨同意した物とみなす。としているような場合や、確認措置を要しない旨表明いたしますと言うようなボタンをクリックしなければ、購入できないような場合はここで言う消費者の意思の表明には当たらない」とされています。

そして「事業者側が消費者の申し込み内容などの意思を確認する措置を設けていない場合には、原則として、操作ミスによる契約は無効となる」と規定されています。

特定商取引法第14条で規制されている「顧客の意に反して契約の申し込みをさようとする行為」にもあたり行政処分の対象になると規定されています。

つまり、確認画面が存在しないワンクリック請求は、その契約自体が無効になると思われれます。

ワンクリック請求の対応策ですが、対応はアクセスの状況などにより異なります。

1. リンク集などからアクセスした場合

リンク集などからアクセスした場合は何も知られていませんので、そのまま無視していれば何の請求も来ません。

2. 広告メールからアクセスした場合

広告メールからアクセスした場合はメールアドレスが知られていますので、メールでの請求が来ます。

代表的な請求メールの文面は以下の通りです

SUBJECT:◆料金請求事件告訴通達◆

訴状の提出日は月曜日の予定ですので必ず最後まで御読み下さい。

当サイトは貴殿に対し、誠心誠意の退会勧告を含めた警告状を再三に亘り送信致したにも拘らず、未だに自主退会手続きが完了致して居りません。

http://m*****

貴殿が自主退会手続きを未了の儘、故意に放置して居る事は、サーバーのログ等を見ても顕かです。

依って当サイトは止むを得ず、貴殿をサイト利用料金請求事件の被疑者として、簡易裁判所に提出する為の告訴状の準備を整えました。

これは貴殿に対する最後の警告と成りますが、自らの意思で退会手続きを完了される様今一度勧告致します。

《退会手順》空メール送信（アドレス確認）→電話番号認証→相応な PF 入力→本登録、退会処理を行って下さい。

期限：メール受信即時訴状の提出日は月曜日の予定です。猶、手続きの行き違い等が有りましたら御容赦下さい。

この文面のタイトルが「料金請求事件告訴通達」になっていますが、この他にも「未承諾勧告」なんていう物もあります。

これは「架空請求」でもご説明した「難しい単語を使おうとする傾向」そのままですね。ここで焦ってはいけません、実際に裁判をした経験があるのならばこう言った民事では「告訴」とは言いません「訴訟」になるはずです。

こう言った 60 万円以下の場合「少額訴訟」になり、その提出書類に「内容証明郵便での請求書」と言う物があります。

しかし住所も判らない相手には郵便物を送る事も出来ませんし、名前や住所も判らない相手に訴訟を起こす事も出来ません。

そしてこのメールにはもう一つ大きな欠点があるのです。

退会手順の所なのですが「相応な PF 入力→本登録」となっています。

つまり「登録されていない」と自分で言っている訳ですね。

このメールは空メール送信や電話番号認証と書いてあるのは「個人情報を教えろ」と言っている訳です。

このようなメールが来ても無視していれば良いですし、わずらわしければ「送信者を禁止する」の設定にすればゴミ箱へ直行しますし、メールアドレスを変更すればメールが来ることもなくなります。

3. ショートメールからアクセスした場合

この場合は上記請求メールの他に携帯電話に請求の電話がかかってきます。

電話がかかって来た場合は相手をせずに電源を切り、しばらくしてから電源を入れてその電話番号を拒否設定にし、非通知及び公衆電話も拒否に設定します。

電話番号を変えてきたらこれを繰り返します。

とにかく相手をしない事です。

警察に行ったと相手に言っても「何処の警察だ！」とか開き直りますし、法的なことを言っても「そんな物は知らん」とか言った対応なので話をするだけ時間の無駄です。

4. 解約などの連絡を取ってしまった場合

メールを送ってしまった場合は、メールで請求が来ますので 2 のメール対策をして下さい、また、携帯電話で連絡をしてしまった場合には 3 の電話対策をして下さい。

固定電話で連絡をしてしまった場合は、留守番機能が付いていれば留守番電話にして、相手を確認して、請求電話なら無視して必要な電話なら出るようにしてください。

また、夜中などに電話をしてくるケースがありますので、その際はボイスワープで携帯に転送し、3 の方法を行う方法もあります。

請求が悪質な場合は警察へ相談してください。

5. 振込みをしてしまった場合

振込みをしてしまった場合で、カード決済の場合はカード会社に掛け合ってみてください
カード会社によっては支払いの停止を行ってくれます。

通常はカード会社が調査して事実確認が取れば対応してくれるのですが、カード会社によつては「相手と話し合ってください」と相手にしてもらえません。

最近ではカード決済が出来なくなっている所が多くなっています。

銀行振り込みの場合は残念ですがお金が戻ってくる確立はかなり低いです。

この場合は警察に被害届けを出してください。

(お金を支払っていない場合は被害者にはなりませんので“相談”と言う事になります)

※一週間程度支払いを遅らすと、口座自体がなくなっている場合があります。

※振り込んでしまう事が一番最悪の結果になる場合が多いので要注意！

進化？するワンクリック請求

ワンクリック請求は進化？しています。

進化と言っても騙す手口が巧妙になってきているのです。

ワンクリック請求サイトにアクセスもしていないのに、こんなメールが届きます。

メールその1

Subject: 今すぐ御確認をお願い致します。

当番組では、この度システムを大幅に変更しました為、サーバーの改修作業を行っております。その際、貴殿の登録状態が「仮登録」となっていることを確認致しました。つきましては下記 URL より早急に「退会」の手続きをして下さい。システムの都合上、手続きをなさらない場合、貴殿の御意思の有無に関わらず自動的に「登録」され、番組使用料が高額となり貴殿に御負担戴くこととなります。

http://*****&cm=ok 退会手順

http://*****

メールその2

Subject: ■確認してください■

あなたが登録の途中で完了せずにいるため、準利用者として 課金請求対象となっています。ご利用の意志のない場合は、本メール到着後、6時間以内に登録を完了し、本人様により退会して頂く必要があります。

http://***** 1&cm=ok

<http://*****&cm=ok> ※重要※手続きが行なわれていない場合は当サイトをご利用になられていると判断し、ご利用料金の請求を行なう場合もございます事も併せてお知らせ致します。退会手順→http://*****/ 処理を行なわない場合は、お客様の御意思の有無に関わらず自動的に「有料会員登録」となり、番組利用料をお客様に御負担戴くこととなりますのでご注意ください。

メールその3

Subject: ご覧ください！

当サイトにアクセスされた際仮登録の状態で個人情報が残された可能性が有ります。

この度はシステム改正の為の至急の退会処理をお勧めする為のご報告です。《処理手順》⇒
http://*****メール送信（受信後 URL をクリック）⇒必要を事項入力し決定⇒電話認証⇒番組入口
より入場⇒必須 PF の入力⇒更新後『メニュー』へ⇒ 退会手続きご協力有難うございます。

これらのメールはワンクリック請求の架空請求と言える物で、アクセスをしていないにも関わらず登録をさせようとする物で、アクセスさせて請求する事と同時に個人情報名簿を作成し名簿販売を目的としていると思われます。

騙されやすい誘導メール

その1（友人タイプ）

Subject: あけましておめでとうございます。

ことしもよろしくお願ひ致します。

新年会が下記アドレスに決定しましたのでお願ひします。

↓アドレス

http://*****

今すぐ GoGoGo!!!!

これもワンクリック請求の誘導メールです

このアドレスにアクセスして、何か一つでも画像をクリックすると登録になってしまいますし、
場合によってはこの URL をクリックしただけで登録になってしまう場合もあります。

その2（訴訟タイプ）

Subject: ◆訴訟警告書◆

件名 貸借金事件

裁判所 管轄裁判所

猶予期間 本日中

http://*****

貴殿がご利用になった当番組（倶楽部人妻）の登録手続きが
未だ仮登録状態のまま放置されて居り、正規会員とみなされ
料金を請求される恐れが有る旨は以前通告した通りです。

貴殿ご自身に退会の意思がお有りでしたら直ちに退会処理を行なってください。

【退会手順】アドレス確認（メール送信）⇒電話番号認証⇒必須 PF 入力
⇒本登録⇒メニューより退会処理を行なってください。

http://*****

再三の通達にも拘らず処理を

なぜかここで文面が切れてました。

このメールの発信元アドレスが「chisai-000〇〇@docomo.ne.jp」なのですが「chisai」となっており、細かい所まで気を配っていますが「chisai⇒地裁 が docomo.ne.jp」とは間が抜けていますね。

しかも、アクセスもしていないサイトの未払いの架空請求なのですが、なぜ賃借金になるのでしょうか？メールが届いた時間が 23:56 で猶予期間が本日中になっていますので、猶予は 4 分しかありませんし、そんな時間にどうやって振り込めと言うのでしょうか？

しかも途中で文面が切れてます。

その 3 (JavaScript)

不況でも安心!!やっぱり出会い系サイトは無料だよ!!

直アド送信もOKだからGET率も高いよ!!

[ご登録はこちら](#)

一見何の変哲も無いメールですが、このメールには添付ファイルが付いています。

その添付ファイルを開けても何も表示されません。

実はこれ JavaScript メールなのです。

このメールはフィッシング詐欺にも使われる手口で、アドレスバーやステータスバーの詐称等に使用されます。

その 4 (HTML メール)

是非見て下さい！

[サンプルを見に行く！](#)

JavaScript メールに似ていますが、添付ファイルありません。

これもリンク先を隠しているメールですが、添付ファイルがついておらず見た目には普通のメールの様に見えるのが特徴です。

この他に、ワンクリック請求にアクセスした人の所へ通常の「葉書による架空請求」が届いた時に、全く別物にもかかわらず「アクセスしたワンクリック請求」からの物と思い込み、パニックに陥り「葉書による架空請求」に支払ってしまう方も相当数いらっしゃいます。

これは完全な思い込みによる「自滅」です。

そう言った葉書による架空請求には「サイト名」は記載されていません。

出会い系サイトとの関連

ワンクリック請求を色々調べると出会い系サイトとの関係も浮上しています。

ワンクリック請求のドメインの「/」の後ろのサブホルダに「/images/」と入力すると、某出会い系サイトの TOP にジャンプする場合があります。

これは棒出会い系サイトの運営するサーバーと同じサーバーを使用している事を意味します。無料のホームページスペースを使用したサイトが削除された場合に、その無料ホームページスペースを提供していた会社の画面になるのと同じで、そのサーバーの運営者のホームページが表

示される物と思われます。

ドメイン情報を見ても同じサーバーで、会社住所は違っていても所在する都市は同じです。これで、その出会い系サイトがワンクリック請求を運営していると言う証拠にはなりません、関連性の可能性は高いと思います。

また、広告メールが出会い系の物であったり、出会い系サイトからワンクリック請求に行ってしまったたりしている事も含めると、送られてくる広告メールの送付先メールアドレスは出会い系サイトで入手した物が使われている可能性が高いと思われますので、出会い系サイトの登録には十分注意してください。

出会い系サイトへの誘導メールにはこんな物まで有ります。

第一弾メール

空のメールがそちらから届いたんですけど送信されましたか？

本文にはなにも書かれてなくて、件名にはこんばんはと書かれていました。

知らない人から空メール来ることなんて初めてなので戸惑ってます。

メールを出した覚えが無いので「こちらからメールをしていない」と言うメールを送りました。

第2弾メール

なんだか話が食い違ってるみたいでしたので私のほうで確認してみたのですが、

なんだか間違えてそちらのアドレスに私のメールが届いてしまってるみたいですね...(>_<)

実は他のアドレスに対して返信したつもりがなぜかそちらに届いてしまったみたいで..

.ほんとご迷惑おかけしました(>_<)一昨日からPCがおかしくていろいろ確認したらウイルスに感染したのかもしれないみたいで、そのせいで色々な方にご迷惑をお掛けしてしまったみたいでして... ホントにすみませんでした。

このメール、女性のように見えますが絵文字の使い方からして恐らく男性ですね。

第3弾メール

こんなのって厚かましいかもしれないけど、

今回こんなタイミングで知り合ったのも何かの縁だと思うので、差し支えなかったら

このままメール交換しませんか？私、主婦なんですけどそれでもいいですか？

最近インターネットをよく使うようになったのですがまだ良く知らない事多くて...

もし宜しければ色々日常の相談とかお話もしたいなとか思ってるんですが...

しっかり男のスケベ心をくすぐっています

第4弾メール

あのそういえば私の方からメールしておいてまだ私のこと何もお話してませんでしたよね！！

簡単に自己紹介しておきますね。名前は〇〇〇(〇〇〇)です。

スリーサイズも教えたほうがいいのかな（笑）一応専業主婦です。
結構変わってる奴ですけどよろしくです。あ、できれば貴方の事も差し支えない程度で構いませんから
教えてください。

スケベ心に駄目押しのメール、しかし無視！

第5弾メール

届いてるか知りたいです(>_<)パソコンの調子が悪いんでメールが届かないのです。。
このメールも送れてるかどうかは私にはわかりません。。
ちゃんと届いてますか？

無視しているので確認してますね。

メールが届いていなければ迷子メールで戻ってくるし、現に何通も送ってきていますし、パソコン調子悪くてもメールの設定や接続が悪いのでなければメールの送受信位は出来ますけどね。

第6弾メール

やっぱりメール受信が出来ませんね。。私のパソコン、ウィルス入ってるのかな。。
どうすれば連絡取れるか考えたんだけど携帯でいつも使ってるサイトがあるんだ
そこに私いるから携帯のほうに直接メールほしいな。それでも大丈夫？
パソコンじゃメール見れないから連絡取ろうにも取れないでしょ？

http://pc.*****.jp/****e.html?media=p110

パソコンじゃメールできないので
携帯のメールで連絡取りましょう！？

実はこのアドレス、出会い系サイトなんですね。

メールの受信が出来ないのでなくて送ってないんですけど・・・

男のスケベ心をくすぐって、その気にさせて出会い系サイトに登録させるって魂胆ですね。
別に連絡を取るなら出会い系サイトを使う必要はありません。

第7弾メール

来ないってことは私はダメってことですか？
ダメなら理由が聞きたいですけどパソコンじゃ無理だし・・・
顔写真見てくれたのかなあ？それとも見ないでダメってことなのかなあ？
何枚か写真入ってると思うのに残念です。
出来ればお互いの携帯アドレス交換してこれから仲良くしたかったのに・・・

http://pc*****.jp/****e.html?media=p110

私、前に男性で登録してすぐ辞めれるか試したところすぐ辞めれたし
それからサイトから連絡はまったくないから大丈夫でしょ？
新しいフリーアドって簡単に入れるから登録したらハンドルネーム
教えてね。

なぜこの人は男性で登録して試す必要があったのでしょうか？

これらのメールは私の個人メールアドレスに送られてきた物で、メールアドレスを知っているのに、なぜ出会い系サイトを使う必要があるのでしょうか？

そして、このアダルトサイトのドメインでメールの検索を行うと、しっかり広告メールでも同時期に来ています。

また、検索エンジンで調べると同じメールが多数発送されている事も確認しましたので、このメールが個人に送られた物でなく大量発送のメールであった事が判ります。

つまり、広告メールですね。

誘導メールには飴と鞭があります、裁判や取立てなどの鞭系の他にも、こういった飴系の誘導メールもありますので、甘い誘いにはくれぐれもご注意ください。

フィッシング詐欺

最近出始めたネット詐欺に「フィッシング詐欺」という物があります。

フィッシング詐欺はカード会社のホームページを装い、カード情報を取得する手口です。

カード会社や銀行などを装ったメールを送り、そのメールからホームページへ誘い込みカード番号などを入力させる事でカード情報を盗みます。

そのカード情報を元に「なりすまし」などの不正利用を行う訳です。

送られてくるメールの送信元などは詐称されていますので、送信元のアドレスはそのまま信じてしまうと騙されてしまいます。

詐称される物は「カード会社」「銀行」「通販」「義援金」と様々で、本物との区別は非常に困難です。

例えば「カードの期限」や「カードの確認」などを装っていたり、「義援金にご協力」などなっていたりしますが、こう言った手口に対する既成概念を持つのではなく、メールで「カード情報を入力させる物全て」を疑う必要があります。

「おかしい」と思ったらメールに記載されている連絡先ではなく、実際の会社の連絡先を調べて確認する事が必要です。

例えば通販のカード決済の場合、カード情報の入力画面の URL を見て「https://」になっているか確認します。

カード決済などのカード情報を入力する場合、SSL で暗号化されるのが普通ですが、https は SSL を意味する物であり、カード入力画面が https でなければ怪しいのです。

また、カード会社系や銀行系のフィッシング詐欺はホームページも本物のように偽装しますので、それを確認する為の一つの方法としては yahoo の利用です。

例えば「A 社」からメールが来ていたとします。

その「A 社」を yahoo で検索するのですが、検索結果で「yahoo 登録サイト」になっているかを確認し「yahoo 登録サイト」のリンクをクリックして「A 社」のホームページを開き、URL などの細かい点をメールで来た URL と比較します。

同じデザインのページが表示されていても Yahoo の登録サイトから開いた URL が「http://www.A.co.jp」でメールからの URL が「http://www.A.com」ならばおかしい訳です。

Google と yahoo の違いは、Google はロボット検索エンジンで、基本的にはどんなページでも登録されていますが、yahoo の登録サイトは yahoo のネットサーファーによって選ばれたサイトと有料広告掲載のサイトなので、素性が調べられたサイトの為に信頼度が高いのです。

Google でも偽者サイトは上位表示されませんので、区別は付きますが SEO（検索エンジン最適化）などで短期的に上位に表示させる事は可能ですので、信頼度から言えば yahoo 登録サイトの方が上と思われれます。

これは、現在被害の中心は欧米ですが、日本でも被害が報告され始めており、今後日本でも被害の拡大が予想される手口ですので、予め知っておく事が被害の防止につながります。

第十一章 振り込め詐欺（オレオレ詐欺）について

この振り込め詐欺も最近猛威を振るっていますね。

主な物としては「交通事故」「借金返済」「中絶費用」「誘拐」「災害援助」など、年を追うごとに新手の手口が発生しています。

最近の傾向は権威を利用する権威主義が見受けられます。

「警察」「弁護士」「消防隊員」「自衛隊」「保険会社」など、権威の威光を利用しています。

話術も非常に巧みで、簡単に信じ込んでしまっても不思議ではありません。

また、ターゲットは綿密に調べられているので、家族構成から勤務先などはすでに知られていると思ってください。

そんな事を知っていたからと言って信じ込まない事が大切です。

まずは一番多い「交通事故」を例にご説明していきます。

これは一度でも交通事故を起こした経験があれば「おかしい」と気付くはずです。

私も数回事故を経験しておりますが、事故後に最初に来るのは「救急車」の場合が多く、警察が来た時にはすでに病院に搬送された後なので、警察官は被害者を見ていない場合が多く、その後の診断書の提出で怪我の度合いを知る為、事故当日に警察官が相手の怪我の具合を言って来る事はありません。

また一番重要なポイントとして「警察は民事不介入」である為「示談」の話は一切しません。

ましてや自宅に示談の件で電話してくる事自体ありえないのです。

私が事故をしたときも、家への連絡は自分でしましたし、警察から家族へ電話があった事は一度もありません。

また、警察などで公開されている振り込め詐欺の録音テープを聴くと、最初は民事と刑事を分けているように話をしていますが示談の話の時には混同しています。

脅し文句で「交通刑務所」などが使われますが、交通刑務所などは刑事に属し示談金などは民事に属しますので、示談金を支払ったと言って交通刑務所へ行かなくても良くなる訳でもありませんし、事故の当日に決まる物でもありません。

しかも刑の確定は警察ではなくて「裁判所」で、警察官が交通刑務所に入る事になると言う事は言いません。

この示談金にしても、治療などが一通り終了した後に事故比率を話し合い「示談書に署名捺印」をして決定される物で、通常は「保険会社」が代行します。

相手が妊娠8ヶ月などという言葉も出てきますが、ハッキリ言って関係ありません。

私の事故も「相手は妊婦」で出産間近であり、診断書にも「切迫早産の恐れ」とありましたが、警察は「切迫早産の恐れは事故の直接の傷害ではない、事故による傷害は頭部と右上腕部打撲なので、軽傷扱いだよ」と言う対応でした。

振り込め詐欺に共通する点は「相談させない事」「使い慣れない難しい言葉を使う事」「自分が何処の誰かを名乗らない事」があります。

警察から電話があるときは「〇〇署の〇〇ですが」と自分の素性を名乗りますし、弁護士にしても「〇〇弁護士事務所の〇〇です」と名乗ります。

相手の所属や住所・氏名を名乗らない者は相手をしない事ですし、聞いても答えなければ怪しいと思ってください。

誘拐タイプは厄介なのですが、このタイプの特徴は「電話を切らせない」事です。

電話を切らせずに「確認させない」ようにする所に特徴があります。

例えば実際の誘拐犯の場合は人質がある訳ですから、確認されても困りませんが「振り込め詐欺」の場合は確認されたら困ります。

ここに大きな違いが出てくるのです。

本物かどうか確かめる意味でも一旦電話を切る必要があります。

誘拐タイプは電話をかけたまま郵便局や銀行まで誘導される事が多いので、携帯電話にかかってくるか、固定電話にかかってくる携帯にかけ直しになります。

電話を切らしてくれない場合は、携帯電話であることを利用して電話を切る方法があります。それは相手の声が聞こえない振り（通話状態が悪い振り）をして「もしもし、もしもし」を繰り返しながら、電源を切ります。

つまり、圏外や電池切れを装うのです。

このまま電源を切った状態で確認を取るか、警察へ行きましょう。

本物の誘拐なら必ず再度電話がかかってくるし、振り込め詐欺は15時を過ぎると電話は滅多にかかってくるません。

「振り込め詐欺」の多発する時間帯は「10:00~14:00」が一番多いと言われています。

これは銀行や郵便局の当日振込み扱いが15:00で終わる為で、その時間に合わせた犯行なのです。

特にこの誘拐タイプは電話をかけたまま、そのまま入金に走らせますので15:00を過ぎれば犯行は成り立たないのです。

振り込め詐欺の対策はよく言われることですが

1. 相手に名乗らせる事

不審な電話があったら最初に所属の確認をする事です。

本物の警察官の場合は最初に所属を名乗ります。

最初に所属を名乗らなければ「何処の警察署のどなた様ですか？」と質問してください。

そこで話をごまかす様なら信じない事ですし、弁護士やその他の職業の場合でも自分の所属と名前を名乗るのは当然の礼儀です。

それを名乗らなかつたり怒り出したりするのは、やましい事を行っている証拠です。

2. 確認が取れない物は振り込まない事

示談金などの相談を「守秘義務」があるから誰にも話すなと言う事はありません。

どんな場合でも確認する事が基本です。

警察などの公務員系や誘拐犯に至るまで確認が基本になりますので、相談や確認させないと言う事は、詐欺を行っている証拠です。

3. 電話を切り誰かに相談する事

これが一番の基本ですね。

実際に相手から電話があった場合に電話を切る事は、結構難しい場合がありますので「電波状態が悪い」「バッテリー切れ」を装い一方的に切りましょう。

固定電話であっても「コードレス子機」のバッテリー切れはありますので、コードレスを装えば良いのです。

最初に自分の素性を名乗らない電話があったら、相手の話を聞かず、一方的に「今、空き巣の現場検証をしている最中で、手が離せないから数時間後にかけなおしてくれ」と言って勝手に電話を切るという手もあります。

ここで言う数時間後とは 15 時から現時間を引いた時間です、電話がかかって来た時間が 13 時なら 2 時間後と言い、10 時なら 5 時間後になるので「3 時頃」と言う様にします。

もう一つの方法は「他人になることです」相手が警察であろうとなんであろうと、全ての知らない相手からの電話に「他人として電話に出る」事です。

電話がかかってきたら「ハイ〇〇ですが」と言う所は普段通り出ます。

そして「自分から素性を名乗らない相手」で、「〇〇さんのお父さんですか」とか「〇〇さんのお母さんですか」などと確認してきたら「違います」と答えます。

誰かと聞かれたら、「叔父」とか「叔母」などを名乗ります。

こうする事で「直接の親族でないけれども、電話に出ても不自然でなく、家族の事情に詳しい」人物を演出しておくとその後の対処が楽になります。

怪しいと思えば「私では判らない」と逃げることが出来ますし、大事な用件なら「今戻りましたので変わります」と言って電話に出れば良いわけです。

こう言った事は急にやろうと思っても出来ません。

振り込め詐欺対策としてではなく、電話セールスなどの対策の一環として普段から癖にしておく事が「いざ」と言う時に役立つのです。

※上記の方法は、あくまでも個人責任において行ってください