

インターネット詐欺対策マニュアル

有限責任中間法人 EC ネットワーク

目次

1.	オークション次点詐欺.....	3
2.	ワンクリック詐欺.....	5
3.	オークションなりすまし.....	7
4.	フィッシング詐欺.....	8
5.	偽ブランド品詐欺・コピーCD・DVD・PCソフト.....	9
6.	代理出品詐欺.....	10
7.	オークション返品詐欺.....	11
8.	懸賞サイトのポイント詐欺.....	12

1. オークション次点詐欺

◇手口

オークション入札で、落札できず次点以降の落札候補者になった人に対し、出品者を“騙って”「落札者が辞退したので、貴方の入札価格で直接取引したい」と持ちかけて、指定した口座に入金させ騙し取る手口です。

大手オークションサイトでは、ユーザーサービスのひとつとして、登録した ID に対し、その ID 番号をつけたメールアドレスを無料で発行しているサイトがあります。そしてオークション上では、入札者の ID 番号と入札価格がオークションページに公開されるため、おのずと、その ID 所有者に対し直接メールを送れるシステムが成り立ち、このような被害が発生します。

また、オークション外で取引しているため、大手オークションサイトに設けられているような補償制度の対象外になります。

◇未然に防ぐには

次点落札候補者が繰り上げ落札者になった場合は、出品者がオークションシステムに則って手続きをする流れになるので、必ずオークションシステムよりその旨落札候補者に連絡が届きます。従って、最初から出品者より直接メールが届くことはありません。

また、次点詐欺を回避するため、ID 所有者に直接メールが送れるシステムのオークションサイトでは、登録 ID 番号とは違うメールアドレスに無料で変更できるシステムをとっているため、オークションを利用する前に、それを利用して、外部から直接メールが送られてこないようにしておくことも有効です。

いずれにしても、オークションシステムに乗らない、直接取引はしないように心掛ける事が必要です。

◇被害に遭ってしまったら

先にお話したように、補償制度は適用されません。

住所や名前を知らされている場合は、内容証明郵便や配達記録郵便などを利用して、相手に通知してみてください。郵便物が戻ってくるかどうかで、相手の所在が確認できます。

ただ連絡先も名前もデタラメなことがほとんどですので、書面を出すと同時に、すぐに警察に相談してください。

振込みをしているのであれば金融機関に連絡して事情を説明して、振り込んですぐの場合は組み戻し手続きを申し出たり、また金融機関より口座名義人に連絡を取ってくれるよう依頼してみるこ

ともひとつです。架空口座の可能性がある場合は、口座凍結措置が可能な場合もありますが、残高より返金を受けるには、今の制度では裁判所の許可が必要な場合もありますので注意が必要です。金融機関への働きかけは、警察の協力があつたほうがスムーズです。

※警察にご相談する際は、お近くの警察署にてご相談ください。

警察には下記の窓口もあります。

警察庁 サイバー犯罪対策

<http://www.npa.go.jp/cyber/>

都道府県警察本部のサイバー犯罪相談窓口等

<http://www.npa.go.jp/cyber/soudan.htm>

2. ワンクリック詐欺

◇手口

広告メールによる誘導やネットサーフィンでたどり着いたサイト上で、画像や入り口をクリックすると、最後まで有料サイトであることを明示しないまま、いきなり画面上に「登録されました」という表示がなされ、料金を指定口座に振り込むよう指示されるといった手口です。

登録画面には、同時に IP アドレスやプロバイダ名も表示され、期日までに料金を振り込まないと、これら情報より個人情報調べて訴訟を起こしたり、自宅に直接回収に行く旨の記載がされていたりします。

また、サンプル動画などと偽ってファイルをダウンロードさせ、PC 画面に請求書がはりついて消えないといったトラブルもあります。

主にアダルトサイトに多い手口ですが、最近は芸能人のサイトと偽って誘導するケースも目立ちます。

◇未然に防ぐには

先ず、あわてて料金を支払わないことです。

有料であることがきちんと明示されていない、若しくは料金のことが利用規約にだけ書かれているような場合は契約不成立、また、有料サービスの契約であることがきちんと確認できるような確認画面が設けられていない場合は錯誤による契約の無効が主張できると思われます。クリックしたときに表示されるウィンドウに「利用規約に同意します」といった記載がされていることにより請求根拠を主張するサイトもありますが、それも無効です。

そして、サイトに連絡を取ることは、自らの個人情報を知らせることにつながり、脅しの材料や架空請求の元になります。リスクの高い行為になりますので、自分から連絡を取ってはいけません。メールや電話が来ても無視してください。IP アドレスやプロバイダからは利用者の個人情報は一切分かりません。会社の PC でアクセスしてしまっても同じです。

そして何より怪しげなサイトには行かないことが一番ですが、知らないところから届く迷惑メールや掲示板等に張られているリンク先には、簡単にアクセスしないことが必要です。

また、素性の知れないサイト上では、アクセスしたりダウンロードすることにより、悪意のあるプログラムを入れられたりウイルスに感染する危険性もあります。ファイル名に「exe」とつくファイルは実行しないようにしてください。日ごろから使用している PC にはセキュリティソフトを入れておきましょう。

◇被害に遭ってしまったら

間違えて支払ってしまった場合は、すぐに警察に相談してください。振込口座が分かっている場合は、警察に相談した後に、警察からその振込口座のある金融機関に連絡を取ってもらい、すぐに

口座の凍結措置をしてもらってください。

また、PC 画面に請求書がはりついて消えない場合は、市販のウイルス対策ソフトを利用して検索、削除したり、IPA セキュリティセンター^{注1}に相談してみてください。

注1 IPA(独立行政法人情報処理推進機構)セキュリティセンター
ウイルス／不正アクセス相談110番

<http://www.ipa.go.jp/security/>

※警察にご相談する際は、お近くの警察署にてご相談ください。

警察には下記の窓口もあります。

警察庁 サイバー犯罪対策

<http://www.npa.go.jp/cyber/>

都道府県警察本部のサイバー犯罪相談窓口等

<http://www.npa.go.jp/cyber/soudan.htm>

※参考情報 東京都 STOP！架空請求！

<http://www.anzen.metro.tokyo.jp/net/>

3. オークションなりすまし

◇手口

悪意のある第三者が別人のオークションの ID を不正利用して大量の出品を行い、詐欺を行う手口です。ID を不正利用されたユーザは、全くの別人が自分の ID を使って詐欺を働いていることに気がつかないまま、オークションサイトから ID が削除されたり高額なオークション手数料を請求されたときに、初めて気がつきます。

ID とパスワードが別人に知られてしまうと、登録しているメールアドレスなどの情報も勝手に変更されてしまいますので、当の本人は気がつきにくいということもあります。

◇未然に防ぐには

オークション ID やパスワードは厳密に管理して、推測されやすいパスワードは使用しないこと、定期的にログインして自分のアカウント情報を確認しておくことが必要です。

勝手に外部に情報が流れていないか、普段使用している PC のセキュリティにも気をつけましょう。情報漏えいには、フィッシングメールによるものや、ウイルスや悪意のあるプログラムのインストールによる被害も考えられます。

そして、何より ID やパスワードを他人に決して教えないことです。PC にメモで貼り付けておくなどはもってのほかです。杜撰な管理体制は、最終的に自分に責任が及ぶということを常日頃から自覚しておくことが大切です。

◇被害に遭ってしまったら

まずは ID を削除することをお勧めします。

悪用された ID でオークション被害に遭った人から連絡があったら、警察に相談したり、オークションサイトが設けている補償制度を利用するよう勧めてください。ただ、ID の所有者には、オークションサイトから落札にかかる数パーセントの手数料を請求されます。これは規約等により、たとえ本人に覚えが無くても ID 所有者に請求がなされますので、これはオークションサイトと交渉するしかありません。

※警察にご相談の際は、お近くの警察署にてご相談ください。

警察には下記の窓口もあります。

警察庁 サイバー犯罪対策

<http://www.npa.go.jp/cyber/>

都道府県警察本部のサイバー犯罪相談窓口等

<http://www.npa.go.jp/cyber/soudan.htm>

4. フィッシング詐欺

◇手口

金融機関やクレジットカード会社、又はオークションサイトを装って送られてきたメールから、またはそのメールから誘導されたニセのサイトから、個人情報のほか、ID やパスワード、口座番号やクレジットカード情報を盗み取られるという手口です。

「システム改善のため、ここから新たな登録が必要」といって、登録情報を入力させます。

ニセのサイトは、本物のサイトと良く似せたつくりになっていて、ブラウザに表示される URL も良く似せて作られています。注意深く見なければ気がつかないかもしれません。

◇未然に防ぐには

事業者からユーザに対して、直接 ID やパスワード、またその他重要な情報をメールにより知らせるよう言ってきたり、フォームなどに入力させるよう誘導することはありません。

不安に思ったら、すぐにその事業者に連絡を取って確認していただく必要があります。ブラウザを立ち上げ直し、その事業者の URL を新たに入力してサイトを開き、そこに書かれている電話番号やアドレス、フォーム等から連絡を取るようになしてください。他に被害が発生していれば、事業者のサイトに情報提供や注意喚起がなされているかもしれません。

◇被害に遭ってしまったら

すぐに情報を盗まれたクレジットカード会社や金融機関に相談し、指示された対策を行ってください。具体的にはクレジットカード番号等の変更や解約、警察への相談です。オークションの ID であれば、すぐにパスワードの変更を行ってください。

実際になりすまし等により被害が発生しても、クレジットカード会社や金融機関により補償される可能性があります。あきらめずに必ず申し出てください。

※警察にご相談の際は、お近くの警察署にてご相談ください。

警察には下記の窓口もあります。

警察庁 サイバー犯罪対策

<http://www.npa.go.jp/cyber/>

都道府県警察本部のサイバー犯罪相談窓口等

<http://www.npa.go.jp/cyber/soudan.htm>

※参考情報 フィッシング対策協議会

<http://www.antiphishing.jp/index.html>

5. 偽ブランド品詐欺・コピーCD・DVD・PCソフト

◇手口

偽ブランド品に関しては、オークションや掲示板などでブランド名を明記して出品しているにもかかわらず、届いた商品はニセモノであったというケース、また“本物”であるとは明記せず「ご理解いただける方のみ」「店舗で販売されているものとは仕様が異なります」といった注意書きがされていて、市販より格安で販売するというケースがあります。

コピー品に関しても、個人でTVドラマなどを録画したものが出品されているケースや、登録変更が出来ないソフトが出品されているケースがあります。

また、オークションなどで「国内発送」と表記されているにも関わらず、実際は海外から送られてくるケースもあります。この場合は組織的です。

◇未然に防ぐには

オークションは、特にニセモノ・コピー商品が出回りやすい環境ともいえます。先ずはそのリスクを充分注意して、確実と思えるものだけを取引する必要があります。

少なくとも“本物”という表記やブランド名が明示されていない商品の取引は避けるべきです。

また、カタログ画像しか使用していないような出品物も避けたほうが賢明です。

コピー品に関しても、パッケージ画像を表示していない、また一般にショップサイトなどで使用されているパッケージ画像だけを表示している出品物は避けてください。

◇被害に遭ってしまったら

ニセモノやコピー商品は知的財産権の侵害に該当するので、取引自体が違法とされる可能性があります。被害者はその権利を持った企業になります。オークションであれば再発防止のため、必ずオークションサイトに経緯を報告してみてください。

また、海外との取引であった場合、申し出ると返品自体はすぐに応じてくれるときもありますが、返送しても代金がなかなか返還されない場合もありますので、交渉時には相手方の存在を確実に把握しておくようにしてください。

個人間取引の場合「自分も本物と思って出品していた」と主張して返品を拒否することもあります。返金に応じなければならないことには変わりありません。

※ 参考情報 有限責任中間法人 ユニオン・デ・ファブリカン東京

<http://www.udf-jp.org/>

6. 代理出品詐欺

◇手口

以下のような流れが一般的です。

- ・ 代理出品の依頼主が、掲示板などに「いいアルバイトがあります、高額収入」と書き込みして、一緒に連絡先メールアドレスを書いておき、連絡を待ちます。
- ・ それを見て申込んできた人に対し、依頼主は出品代理人としてオークションの代理出品をさせます。
- ・ その際依頼主からは、指定の画像を使って代理出品するよう指示され、さらに落札者には依頼主が指定する口座に代金を振り込ませるよう、代理出品者に指示します。・ 落札者から代金が支払われたら、依頼主が商品を落札者に発送し、全て終了したら代理出品者にはその報酬を支払うと約束します。

しかし、実際は落札者に商品が依頼主から発送されることはありません。落札者から振り込ませた代金を持ち逃げして、結局その人には報酬すら支払われないことがほとんどです。依頼主は身分を明かすことは無く、また明かしていたとしても虚偽で連絡がつかなくなります。当然、落札者からはその人に対しクレームがきます。

◇未然に防ぐには

高額なアルバイト代につられ、会ったことも無い第三者の代理出品やオークション ID の貸し出しは絶対にしないことです。口座を用意するよういわれる場合もありますが、犯罪に加担してはいけません。

そうでなくても、誰かの代理出品をするということは、落札者とのやり取りやトラブルに関しては全て自分で責任を取る、という覚悟が無ければ安易に引き受けるべきではないと思われます。委託販売であれば、古物商の許可が必要です。

◇被害に遭ってしまったら

この場合、被害者は誰なのでしょう。ID を詐欺に使われ、挙句、報酬ももらえなかった、その人でしょうか。

被害者は落札者です。外から見たら、残念ですが依頼主とその人が結託して落札者を騙している構図になります。加害者となるその人は、自ら行った無責任な行動を反省し、被害者である落札者を補償制度などで救済出来るよう、協力するべきであると思います。

7. オークション返品詐欺

◇手口

出品者が狙われる詐欺です。

落札者より何らかの理由により返品を申し出られ、それに応じると、自分が送った商品とは別の商品、若しくは別の状態のものが返送されてくるというものです。

もちろん、落札者から返品を求められたときに、初めて自分が見落としていた問題点や不具合に気付く場合もあります。その場合は、落札者に悪意があるわけではありませんので、きちんと誠意ある対応をしてください。

ただ、返品詐欺の場合は、明らかに違う状態のものが返送されてきます。

主な被害としては、以下のケースがあります。

- ・ ブランド品を出品、返送されてきた物は同じ型のニセモノだった。
- ・ 衣料品を出品、返送されてきたものは確かに同じ物だが、明らかに状態の悪い物だった。
- ・ わざと傷をつけて返すという嫌がらせ。

この場合、どちらに悪意があったのか、第三者的に判断が難しいところで、水掛け論になる場合もあります。落札者側に悪意がある場合は、その水掛け論となり、結局出品者側でも証明が付かず、解決できなくなることを見越して仕掛けてきます。

◇未然に防ぐには

返品を求められたとき、まずは商品を先に返送してもらい、その商品の状態を必ずチェックしてください。何が何でも先に返金を求められた場合は注意が必要でしょう。

また、相手には、返送前に手元の商品の画像を送付するよう求めてみてください。

よく、このようなトラブルを避け、出品時に「ニセモノを返品されると困るのでノークレームノーリターン」と表示する人もいますが、もちろん、この表記を隠れ蓑に、他の理由があっても一切返品返金に応じなくて良いとはなりません。

ただ、見知らぬ相手との取引には、常日頃から客観的な証拠を残す習慣をつけておく必要があります。

◇ 被害に遭ってしまったら

この場合、大手オークションサイトが設置しているオークション補償制度が申請できず、補償による救済がなされないことがほとんどと思われます。

また、警察に相談しても、自分が被害に遭っていることを客観的に証明することが難しく、相手と水掛け論になると收拾が付かず何も解決がなされないこともあり、なかなか救済が難しい被害でブランド品を出品する場合は、購入時、店舗から貰ったレシート等を保管しておいて、自分の主張が正しいという証拠を出来るだけ集めておきます。

被害救済に関しては、最終的には訴訟等、民事的な解決が必要になるかと思えます。

8. 懸賞サイトのポイント詐欺

◇手口

懸賞サイトや広告サイト等にて無料登録して、そのサイト上に広告が出ているスポンサーサイトの広告を見たり申込みをすることでポイントが付き、そのポイントが現金換金出来るというサービスがインターネット上に多々あります。

しかし、実際はそのポイントが約束通り付かなかったり、換金しようとしても換金してくれなかったり、サイトと連絡が取れなくなってしまうケースがあります。

さらに、全く登録の覚えのないところからも、どんどん広告メールが届くようになっていたりすることがあります。

また、そのような懸賞サイトには、サイトの利用規約等、目立たないところに「この懸賞サイトは〇〇会社が運営しており、〇〇会社は出会い系サイトを運営しています」と書かれていて、自動的に有料出会い系サイトにも登録され、異性からのメールが届き、開くことで課金がされ料金請求を受ける悪質なケースもあります。

◇未然に防ぐには

登録しようとするサイトの所在地や連絡先、担当者などの確認を必ずしてください。電話番号が書かれていないようなサイトには登録しないほうが良いと思います。

そしてよく言われていることですが、やはりタダほど恐いものはありません。登録する際には、必ず利用規約を確認して、登録した個人情報などがどのように扱われるのか、必ず確認して欲しいと思います。提携サイトがあると書かれている場合、また提携サイトの名称が公開されていないようなサイトへの登録は避けてください。

登録は無料だからといって、少しでも換金率を上げようと、複数のサイトに登録するのはお勧めできません。少しでも信用できないと思われたサイトには、個人情報の登録はしないようにしましょう。クレジットカード番号を登録させるサイトもありますので、注意が必要です。

◇被害に遭ってしまったら

無料サイトに登録したにもかかわらず、サイトから何らかの請求が行われた場合は、すぐに応じずに、まずは相談機関などに相談して、その請求が正しいのかどうか確認してください。

ポイントを換金してくれない、約束通り付いていない、サイトと連絡が付かないようであれば、所在地に配達証明などの書面を送り、受取るかどうか確認してみてください。

また、このようなサイトに対しては、残念ながら登録した個人情報の厳密な管理も期待できません。そして、1度流されてしまった個人情報は、既に回収不可能です。

流された個人情報を利用して架空請求が行われる場合もあります。身に覚えのない請求があても決して応じないことです。

クレジットカード番号を登録している場合は、これら勝手に登録された出会い系サイト等の料金請求が、そのクレジットカードになされる可能性があります。すぐにクレジットカード会社に相談してください。