警視庁
サイバー犯罪対策課
相談マニュアル

※　本マニュアル作成の趣旨

1　このマニュアルは、生活相談の窓口において、サイバー犯罪に関する相談又はインターネットカフェ等に関する質疑がなされた際の回答例を載せていますので、執務の参考として下さい。

2　なお、相談として受理した場合であっても、犯罪として立件できる可能性がある場合は、事件化を念頭に適切な対応をして下さい。

3　また、サイバー犯罪の手口等は、日々新たなものが現れていることから、これらに的確に対処すべく、執務資料やニュース等で最新の情報を得るように心掛けて下さい。

目次

1　詐欺・悪徳商法に関するもの

Q1-1　パソコンでアダルトサイトを見ていた。年齢認証を済ませて無料動画のダウンロードをし閲覧したが、その後「登録完了」の表示がデスクトップに表示されて消すことができない。

・　ワンクリック詐欺サイトを閲覧したおそれがある。
・　電子消費者契約法によれば、インターネット上での契約において予め料金の明示等がない場合は、契約の無効を主張することができる。
・　特定商取引法によれば、インターネット上での契約を行うサイトには、クリックをすることが入会となる行為であることを事前に明示すること及び、利用者が申し込み内容を確認や訂正できるようにすることが必要である。
・　相談者を特定するような情報は通知されていないと考えられるので、業者への連絡は控えること。
・　請求について不安な点があれば、地元消費者センター等で相談をしてはどうか。
・　システムの復元①やＯＳの再インストールにより、登録完了の表示を消すことができるが、事前に重要データのバックアップをとること。

Q1-2　雑誌の広告にあったＱＲコードをスマートフォンで読み取り、アダルトサイトを閲覧した。電話番号を入力するページが表示されたので入力し、サイトを閲覧した。その後、電話がかかってきて高額な登録料を請求された。

・　ワンクリック詐欺サイトを閲覧したおそれがある。
・　電子消費者契約法によれば、インターネット上での契約において予め料金の明示等がない場合は、契約の無効を主張できる。
・　特定商取引法によれば、インターネット上での契約を行うサイトには、クリックをすることが入会となる行為であることを事前に明示すること及び、利用者が申し込み内容を確認や訂正できるようにすることが必要である。
・　相談者が連絡先情報等を入力したことが原因で、業者に電話番号が通知されたと考えられるが、着信拒否設定や電話番号の変更により無視すること。
・　請求について不安な点があれば、地元消費者センター等で相談をしてはどうか。

Q1-3　携帯電話に心当たりのないメールが届き、掲載されたリンクをクリックしたところ、アダルトサイトが開いた。そのようなサイトを見る気は無かったので、すぐにサイトを閉じたのだが、その後、料金請求のメールが届くようになった。

・　不当請求メールと思われる。
・　電子消費者契約法によれば、インターネット上での契約において予め料金の明示等がない場合は、契約の無効を主張できる。
・　特定商取引法によれば、インターネット上での契約を行うサイトには、クリックをすることが入会となる行為であることを事前に明示すること及び、利用者が申し込み内容を確認や訂正できるようにすることが必要である。

・　大量の請求のメールが届くようであれば、ホワイトリスト方式によるメールフィルタリング②やメールアドレスの変更を検討する。
・　請求について不安な点があれば、地元消費者センター等で相談をしてはどうか。
・　心当たりのないメールに掲載されたリンクサイトにアクセスする際には、慎重に検討すること。

Q1-4　携帯電話に利用した覚えのない有料情報サイトの利用料金の請求メールが届いた。送信相手に連絡すると、再三請求のメールを送信するも、受信拒否設定のためにブロックされており、滞納金と利子で高額な利用料金が発生しているという内容だった。

・　架空請求メールと思われる。
・　利用した心当たりがない内容であれば、無視をする。
・　大量の請求のメールが届くようであれば、ホワイトリスト方式によるメールフィルタリング②やメールアドレスの変更を検討する。
・　請求について不安な点があれば、地元消費者センター等で相談をしてはどうか。

Q1-5　携帯電話に届いたメールのリンクをクリックしたところ、登録無料の出会い系サイトのようであった。実際のやりとりにはポイントが必要であり、相手とやりとりをしていたところ、後になって高額な請求を受けた。

・　悪質出会い系サイトを利用したおそれがある。
・　料金の請求に直ちに応じることなく、不安であれば消費者センター等で相談をしてはどうか。
・　迷惑メールが大量に届くようであれば、ホワイトリスト方式によるメールフィルタリング②やメールアドレスの変更を検討する。

Q1-6　出会い系サイトを利用していたところ、相手女性から自身の性器画像を撮影して送るように求められた。相手の求めに応じて撮影画像を送信したところ、運営業者から「わいせつ画像の送信により業務が停止した」と損害賠償を求められた。

・　悪質出会い系サイトを利用したおそれがある。
・　料金の請求に直ちに応じることなく、損害賠償であれば民事訴訟となるので、弁護士へ相談する事を提示し、法テラス等を教示する。
・　迷惑メールが大量に届くようであれば、ホワイトリスト方式によるメールフィルタリング②やメールアドレスの変更を検討してはどうか。

【補足】
・　わいせつ画像を執拗に送りつけるような事案については、迷惑防止条例第５条の２第１項第４号（汚物、動物の死体その他の著しく不快又は嫌悪の情を催させるような物を送付し、又はその知りうる状態に置くこと）に該当するおそれがあることを警告する。

Q1-7　ネットショップで商品を注文したところ、メールで代金の振込先口座を指定された。案内に従って代金を振り込んだが、到着予定日を過ぎても商品が届かない。問い合わせをしようとしたが、メールアドレス以外の連絡先の表示がない。

・　振込先金融機関の金融犯罪被害相談窓口で相談をすることで、振り込め詐欺救済法に基づく被害回復分配金の支払いを受け取ることができる場合がある。
・　相談者から振込先口座等の情報を聴取し、所属において口座凍結を検討する。
・　「特定商取引に関する法律」第１１条（通信販売についての広告）に基づき住所、電話番号共に表示することが義務づけられているので、これに基づいていないサイトの利用は控えること。

【補足】
・　サイト情報を確認し、サーバが海外にあり、サイト運営者と連絡が取れない等の場合、サイバー犯罪対策課へサイトのURLを連絡する。（対策係　　7861-3031, 3032, 3033）
（宿直時間帯　7861-3012）

Q1-8　ＳＮＳサイトを利用して、コンサートチケット売買の取引をした。銀行口座を指定されて代金を振り込んだが、商品が送られてこない。相手にメッセージを送っても応答がない。

・　判明している連絡先に対して内容証明郵便等を利用して返金を求めてはどうか。
・　振込先金融機関の金融犯罪被害相談窓口で相談をすること。
・　法テラス等で弁護士に相談をすることができる。
・　悪質ユーザーとして、ＳＮＳサイト運営会社に通報してはどうか。

【補足】
・　相談者から振込先口座等の情報を聴取し、所属において口座凍結を検討する。

Q1-9　ウェブサイトを閲覧中に、パソコンから突然警告音が鳴り「ウィルスに感染しています。カスタマーサポートまで電話して下さい。」という警告画面が表示されて消せなかったので電話した。遠隔操作でパソコンを確認すると言われたので、相手の指示通り遠隔操作ソフトをインストールした後、表示された番号を伝えたところパソコンを遠隔操作された。相手から「ウィルスに感染しています。有償で除去します。二年間のサポート付です。」と言われたのでクレジットカードで支払った。

・　遠隔操作ソフト（Ｔｅａｍｖｉｅｗｅｒ、ＡｎｙＤｅｓｋ等）をアンインストールして下さい。
・　ウィルス対策ソフトを最新の状態にしてから、ウィルスチェックを実施して下さい。
・　不安であれば、遠隔操作される前に保存した復元ポイントまでシステムを復元してはどうか。またはパソコンを工場出荷状態に初期化してはどうか。
・　クレジットカード会社に連絡して、キャンセルの可否について確認すること。

・　契約に関しては消費者ホットライン（１８８）に相談してはどうか。

---

①　システムの復元
　Windows のシステムファイルを以前の状態に戻す機能。Windows に不具合が発生した場合に、不具合が発生した時点よりも前の状態に戻すことでトラブルが解決できる場合がある。写真等の個人用データを復元することはできない。
②　ホワイトリスト方式によるメールフィルタリング
　メールフィルタリングのうち、指定したメールアドレスからのメールだけを受信する設定。「携帯電話から発信されたメールのみ受信」等の設定も可能であり、多種のメールアドレスから迷惑メールが届く場合には有効。

２　インターネットオークション被害に関するもの

Q2　インターネットオークションで、ノートパソコンを１０万円で落札した。出品者と連絡を取り、指定された口座にお金を振り込んだところ、『入金を確認したので発送する』という内容のメールが届いたのだが、一向に品物が届かない。メールで問い合わせても返信がなく、電話もつながらない。

・　内容証明郵便を送付し、商品の送付や返金を促す。
・　取引をした金融機関において、組戻し①による返金について問い合わせる。
・　振込先金融機関の相談窓口に問い合わせる。
・　内容証明郵便を受け取っても対応しないのであれば、少額訴訟②等の民事的な手段を検討する。
・　サイト運営者が補償制度を提供している場合もあるので、その利用を検討する。

【補足】

・　相談者から振込先口座等の情報を聴取し、所属において口座凍結を検討する。
・　出品者のアカウントに不正アクセスをされているおそれもある。

---

①　組戻し
　振込人から受取人の口座に振り込まれた資金を、振込人により受取人へ資金返却の依頼を行うこと。資金の返却には、受取人の承諾が必要であり、必ず資金が戻ってくる訳ではない。
②　少額訴訟
　民事訴訟のうち、６０万円以下の金銭の支払いを求める訴えについて、原則として１回の審理紛争解決を図る手続き。簡易裁判所で行われる。

3　名誉毀損、誹謗中傷、脅迫、個人情報の流布に関するもの

Q3-1　自分の名前でウェブ検索をしたところ、私のことを誹謗中傷する書き込みがあるウェブサイトを見つけた。この書き込みを消してもらいたいが、どうしたらいいか。

- 書き込みの削除については、サイト管理者に依頼をすることとなる。
- サイト管理者が対応しないようであれば、ドメイン①登録者やサーバ②管理者に対応を求めることも検討する。
- ドメイン登録者情報やサーバ管理者情報はＷＨＯＩＳ③検索により閲覧することができる。
- 法務省人権擁護局④の窓口で相談をすることもできる。
- 検索サイトに対して検索結果に表示させないように求めることもできる。
- 削除の仮処分申請については弁護士に相談をする。
- ウェブページから削除されたにも関わらず、検索サイトの検索結果に反映されない場合は、検索サイトごとに削除依頼をする必要がある。

【重要】

- **掲示板サイト２ちゃんねるは、「５ｃｈ．ｎｅｔ」と「２ｃｈ．ｓｃ」の２サイトが存在している。**
- **「５ｃｈ．ｎｅｔ」への削除要請は、指定メールアドレス宛に要請又は、公開された削除依頼板に書込むこととなるため、慎重に検討をする必要がある。**
- **「２ｃｈ．ｓｃ」への削除要請は、公開された削除依頼板に書込むこととなるため、慎重に検討をする必要がある。**

Q3-2　自分の名前でウェブ検索をしたところ、私になりすましたフェイスブックのページを見つけた。私の友だちが、私のアカウントだと勘違いをしてやりとりをしており、悪質な発信もしているようだ。

- なりすましアカウントについては、ＳＮＳサイトの通報窓口を利用して対応を求めること。
- 友人等に対してなりすましアカウントであることを伝え、連絡を取らないように求めること。
- 法務省人権擁護局④の窓口で相談をすることもできる。

Q3-3　オンラインゲームを利用しています。掲示板サイトで、私のアカウントを指して中傷する書き込みが炎上している。取り締まってもらいたい。

- いわゆるハンドルネームを指しての誹謗中傷行為を取り締まることは難しい。
- 相談者自身を特定しての書き込みではないことから、静観をすることも対応の一つである。
- 書き込み者に対して、書き込みの中止を直接求めることで、書き込みが過熱する場合もある。
- 削除の仮処分申請については弁護士に相談をしてもらいたい。

Q3-4　掲示板サイトでＬＩＮＥＩＤを交換した女性とＬＩＮＥビデオ通話で、お互いの裸を見せ合った。相手の言う通りにアプリをインストールしたところ電話帳データを抜き取られてしまった。相手から「裸を録画した。動画を電話帳に登録されている人に対して公開されたくなければ金を払え」と脅されたので、コンビニで電子マネーを購入し支払ってしまった。

- 支払ったとしても動画を公開されてしまったケースも多い。
- インストールしたアプリをアンインストールすること。

【補足】

- セックストーションと呼ばれる手口であり、電話帳データについては、相手の指示で相談者がインストールしたアプリが原因で、相手に電話帳を抜き取られてしまうケースがある。
- ＳＮＳに登録している友人に対して動画を送ると脅してくるケースもある。

---

① ドメイン
ネットワークに接続しているコンピュータの場所を特定するものであり、インターネット上の「住所」にあたる。ドメイン名は登録機関に申請し登録する必要があり、代理店を通じて行うこともできる。（例・http://www.keishicho.ne.jp/の場合の下線部分）

② サーバ（ウェブサーバ）
ホームページやショッピングサイトを公開するためのスペースを提供するコンピュータ。

③ ＷＨＯＩＳ
インターネットで使用されるＩＰアドレスやドメイン名の登録者情報を照会するサービス。（ＪＰドメイン名登録者情報検索・http://whois.jprs.jp/）

④ 法務省人権擁護局
インターネット上での人権侵害について、人権侵害情報の削除依頼の方法について助言を行うなど、被害者による被害の回復の手助けをする。被害者による回復が困難な場合等には、法務局が削除依頼を行う場合がある。

4　児童ポルノの流布等に関するもの

Q4　ツイッターのアカウントアイコン（インターネットのサイト）に、明らかに未成年の裸を出している。

・　掲示板や出会い系サイトでの児童買春の周旋・勧誘、画像掲示板への児童ポルノの投稿、オークションや掲示板での直接取引での児童ポルノの売買等の情報が寄せられた際には、事件化を念頭に適切に対処する。

5　不正アクセスによる被害、ネットワークセキュリティに関するもの

Q5-1　オンラインゲームを利用している。ログインをしたところ、登録しておいたはずのゲーム上のアイテムがなくなっている。

・　相談者のアカウント情報を悪用した不正アクセスのおそれがある。
・　早急にアカウントのパスワード変更を行うこと。他のウェブサイトで同じ文字列のパスワード登録をしているのであれば、全て変更する必要がある。
・　ログインができないようであれば、アカウントの復旧等についてゲーム運営会社に問い合わせること。
・　不正アクセスの被害者はゲーム運営会社であるので、警察へ届け出る際には相談者は参考人として相談をすることになる。
・　アイテムの復旧については、ゲーム運営会社の対応となる。
・　二段階認証①等のセキュリティ対策の機能が利用可能であれば、導入を検討すること。

Q5-2　オンラインショッピングサイトでアカウントに登録していたクレジットカード情報を悪用され、買い物をされてしまっている。

・　クレジットカード会社にカードの停止依頼を実施する等、追加被害の防止措置を講じ、併せて、被害額が補償の対象となるのかどうか確認する。
・　早急にアカウントのパスワード変更を行うこと。他のウェブサイトで同じ文字列のパスワード登録をしているのであれば、全て変更する必要がある。
・　ログインができないようであれば、アカウントの復旧等についてサイト運営者に問い合わせること。
・　不正アクセスの被害者はサーバ運営者であるので、警察への届け出については参考人として相談をすることとなる。
・　二段階認証①等のセキュリティ対策の機能が利用可能であれば、導入を検討すること。

Q5-3　ＳＮＳサイトのアカウントがハッキングを受けてログインパスワードを変更されてしまい、私の意図しない書き込みがされてしまった。

・　アカウントのパスワードを早急に変更すること。
・　ログインができないようであれば、アカウントの復旧等についてサイト運営者に問い合わせること。
・　ＳＮＳサイトによっては、専用の通報フォームを設置している場合がある。
・　不正アクセスの被害者はサイト運営者であるので、警察への届け出については参考人として相談をすることとなる。
・　自身のアカウントで削除可能な書き込みについては削除を行い、その他については、サイトの利用規約で削除依頼方法を確認の上、管理者に対して削除依頼を行うこと。
・　二段階認証①等のセキュリティ対策の機能が利用可能であれば、導入を検討すること。

Q5-4　当社が管理しているホームページがハッキングを受けて、ホームページが改ざんされてしまった。

・　早急に、アカウントのパスワード変更を行うこと。
・　可能な限り、被害サーバの証拠保全を行うこと。
・　必要に応じてＩＰＡ②等の機関へ相談を行うこと。

Q5-5　ドコモのｄアカウントやグーグルアカウント等に対して、不正にログインされたかもしれない。

・　自分でログイン履歴を確認すること。
・　第三者にログインされた形跡があれば、パスワードを変更すること。
・　ログインができないようであれば、アカウントの復旧等について運営会社に問い合わせること。
・　不正アクセスの被害者は運営会社であるので、警察への届け出については参考人として相談をすることになる。
・　二段階認証①等のセキュリティ対策の機能が利用可能であれば、導入を検討すること。

---

①　二段階認証
　ログインＩＤとパスワードに加え、セキュリティコードの入力が求められる。
　セキュリティコードは、ログインＩＤとパスワードを入力した直後に、本人が登録した携帯電話機へ送信したり、本人が登録した専用アプリに表示させる方法等がある。
　よって、ログインＩＤとパスワードが第三者に知られたとしても、ログインする者の手元に本人が登録した携帯電話機や専用アプリがなければログインできない。
　更に、セキュリティーコードは認証の度に異なり、認証に使用できる時間も数十秒から数分間と限られていることから、セキュリティの高い認証方法である。
②　ＩＰＡ（独立行政法人　情報処理推進機構）
　コンピュータウイルスやセキュリティに関する調査・情報提供を初めとした事業を行っている。マルウェア及び不正アクセスに関する総合的な相談窓口として「情報セキュリティ安心相談窓口（03-5978-7509）」を開設している。

6 コンピュータウィルスによる被害に関するもの

○　コンピュータウィルス
　以下の特徴の１つ以上を有するプログラムの一種
　①　自己感染・・・他のプログラムに自分の複製をコピーして感染
　②　潜伏・・・ある契機（トリガ）が発生するまで発病せずに潜伏
　③　発病・・・ある契機（トリガ）が発生して感染以外の意図しない動きをする

○　ウィルスの法的規制
　情報処理の高度化等に対処するための刑法等の一部を改正する法律が平成23年6月24日に公布され、改正法により、刑法に新たに「不正指令電磁的記録に関する罪（いわゆるコンピュータ・ウィルス罪）」が設けられ、同年7月14日に施行された。
　この法律により、いわゆるコンピュータ・ウィルスの作成、提供、供用、取得、保管行為が罰せられることになった。

○　ウィルス防止対策
・　ウィルス対策ソフトを導入し、アップデートをきちんと行い、常に最新の状態にしておく。
・　ＯＳやブラウザ等のアップデートをこまめに行い、セキュリティホールを埋めておく。
・　インターネットからファイルをダウンロードした場合は、不用意に開かず、ウィルス対策ソフトでチェックしてから開くようにする。
・　見知らぬ送信者からのメールを安易に開いたり、添付ファイルを開いたり、リンクをクリックしたりしない。
・　出所不明な記録媒体を使用しない。
・　ウィルスに感染した場合は、感染拡大を防ぐため、ネットワークから切り離し、ウィルス対策ソフトによる駆除、リカバリーディスク等を用いての初期化等の措置を取る。

○　スパイウェア
　パソコンを使うユーザの行動や個人情報を収集したり、演算装置の空き時間を借用して計算を行ったりするアプリケーションソフト。
　悪用されると個人情報やカード情報等を窃取される危険性がある。

○　ランサムウェア（身代金要求型）
　感染したパソコンやスマートフォン等の端末をロックしたりファイルを暗号化する等により使用不能にし、元に戻すことと引き換えに身代金を要求する。
・　感染してしまった端末を元に戻す場合は、基本的にはバックアップから復元する

等の作業を行う必要があるが、セキュリティ会社等が解除ツール（暗号化されたファイルを元に戻すためのソフト）を公開している場合がある。

・　解除ツールで元に戻らない場合は、データが復旧できる可能性は低い。

○　特殊なサイバー犯罪

民間企業等を対象としたサイバー犯罪で、報道発表が行われる等、社会的反響が大きいと思慮される様なものは、サイバー犯罪対策課へ速報すること。

（情報２係　　7861-3082, 3083, 3084, 3085）

（宿直時間帯　7861-3012）

【参考】

Tracking Cookie（Cookie）

Ｗｅｂサイトの提供者が、ブラウザを通じて訪問者のパソコンに一時的にデータを書き込んで保存させる仕組み。

ユーザに関する情報やサイトを訪問した日時、回数等を記録しておくことができ、ユーザの識別にも用いられる。

スパイウェアとして検知される場合があるが、特に問題は無い。

7　迷惑メール、スパムメールによる被害に関するもの

Q7-1　迷惑メールが大量に届く。届いたメールアドレスに対して受信拒否設定をしているのが、次々にアドレスを変更してくるので対応しきれない。

・　ホワイトリスト方式によるメールフィルタリング①を設定してはどうか。

・　メールアドレスの変更も検討してもらうこと。

・　メールアドレスのドメイン（「@」以降の文字列）からメールサーバを特定し、サーバ管理会社に通報をすることもできる。

・　警視庁ホームページ「迷惑メールに関する情報提供」ページを通じて情報提供を受け付けている。

・　広告宣伝メールであれば、迷惑メール相談センター②に対して情報提供をすることもできる。

・．広告宣伝メールのうち、住所・電話番号等の表示がないものについては、電子商取引モニタリングセンター③に通報することもできる。

Q7-2　「佐川急便」を名乗るメールが届いた。配達確認としてリンクＵＲＬが掲載されており、リンク先にアクセスをしたところ「ありがとうございます」と表示されるのみであった。よく確認したところ佐川急便の公式メールアドレスとは異なるアドレスだった。

・　配送業者や通信販売事業者になりすましたメールが発信されている場合があること。

・　メールアドレスのドメイン（「@」以降の文字列）により、公式メールアドレスかを判断できる場合がある。

・　ホワイトリスト方式のメールフィルタリングを設定してはどうか。

・　リンク先にアクセスをすることで、相談者がメールを閲覧したかの確認をとっていると考えられ、迷惑メールが増加することも考えられる。

・　相談者の氏名や電話番号等の情報が通知されているわけではない。

・　メールに添付ファイルがあった時は、安易に開くことが無いようにする。

Q7-3　迷惑メールに対してフィルタリングをしたくない。メールアドレスの変更もしたくない。

・　迷惑メールの受信を規制するには、自己の判断で対応をしてもらいたいこと。

・　知人との連絡用と、会員登録用等のメールアドレスを使い分けてはどうか。

・　迷惑メール相談センター②や電子商取引モニタリングセンター③にも、通報してもらいたい。

---

①　ホワイトリスト方式によるメールフィタリング

メールフィルタリングのうち、指定したメールアドレスからのメールだけを受信する設定。「携帯電話から発信されたメールのみ受信」等の設定も可能であり、多種のメールアドレスから迷惑メールが届く場合には有効。

② 一般社団法人日本データ通信協会　迷惑メール相談センター
　特定電子メール法に違反する迷惑メール（架空請求や誹謗中傷などには対応していない）に関する相談や情報を受け付けている。これにより総務大臣及び消費者庁長官による行政処分が行われる場合がある。（http://www.dekyo.or.jp/soudan）
③ 一般財団法人日本産業協会　電子商取引モニタリングセンター
　特定商取引法の表示義務（住所、電話番号等の表示義務）に違反する迷惑メールに関する情報を受け付けている。これにより消費者庁長官による行政処分が行われる場合がある。
（http://www.nissankyo.or.jp/spam/index.html）

8　クレジットカード番号盗取等クレジットカード犯罪被害に関するもの

Q8　クレジットカードの利用明細書に、心当たりのない請求があった。私が登録をしたことのないショッピングサイトで注文をされているようだ。

・　直ちにクレジットカード会社に問い合わせて、利用停止等の対応を求めること。
・　クレジットカード不正利用の被害者は、カード名義人ではなく、カードを使用され品物やサービスを提供した事業者側となる。
・　自身に請求が来ていることから、自分が被害者だと誤解し、警察の対応に不満を持つ相談者も多いことから、誤解の無いよう説明する。
・　金銭的な負担については、相談者、カード会社、使用先の事業者の間で交渉する。（クレジットカード会社の約款によっては、損害を補償される場合がある。）

［補足］
・　クレジットカード情報が漏れた原因としては、実際にカードを使用した際等にスキミングされるようなケースだけでなく、正規サイトを装ったフィッシングサイトに誘導され、そこでカード情報を入力してしまうようなケースもある。（正規の業者を装ったフィッシングメールのリンクから誘導される場合等）
・　ショッピングサイトにクレジットカード情報が登録されていると、カード情報が盗まれていなくとも、相談者のＩＤ・パスワードを使ってログインされてしまうことにより、カード決済で買い物されてしまう場合がある。
・　家人が相談者の知らないうちにクレジットカードを使用しているような場合があることから、請求内容等からその可能性が疑われるときは、相談者に確認させた方がよい。
・　契約内容の誤解から相談者が不当な請求だと判断している場合もあり、そのようなものである場合は、消費者センター等に相談するよう教示する。

9　違法有害なホームページ・掲示板等の通報、取締要望に関するもの

○　違法有害情報

・　違法情報

わいせつ画像、他人を脅迫するメッセージ等、情報自体が違法であるもの、並びに銃器、薬物、毒劇物、わいせつ図画等禁制品及び規制品の売買に関する情報等、犯罪が行われている疑いのある情報

・　有害情報

犯罪方法を教示する情報、少年の健全育成を阻害するおそれのある情報等、違法情報には該当しないが、犯罪や事件を誘発する等、公共の安全と秩序の維持の観点から放置することが出来ない情報

○　警察の基本姿勢

・　把握した違法情報については積極的に事件化を図る。

・　違法情報の送信を知りながら放置しているプロバイダに対しては、当該違法情報の削除を要請するとともに、同種事案の再発防止等について指導する。

・　有害情報に関しては、その流通による害悪の発生の防止を図るため、プロバイダ等関係団体との連携を図り、個々のプロバイダに対し、ガイドライン、会員規約等に基づく当該情報の削除等の措置、同種事案の再発防止等の必要な措置をとるよう促す等、自主的な対応を要請する。

○　プロバイダによる自主規制

「インターネット接続サービス等に係る事業者の対応に関するガイドライン」において、プロバイダは、違法・有害情報が発信されたことを知った場合は、送信停止等の措置を講じることと規定されている（同ガイドライン９条）。

また、主要プロバイダ等によって、プロバイダ等における違法性判断基準や、警察からの削除依頼への対応方法等が示された「インターネット上の違法な情報への対応に関するガイドライン」が策定されている。

１０　プロバイダとの契約、トラブルに関するもの

○　本分類に属する相談は、基本的には契約トラブルであり、警察が介入すべき事案ではないが、可能な範囲でアドバイスを行い、また、然るべき相談先を案内する等、適切な対応を心掛ける。

○　契約トラブル等については消費者センターに相談することができる。インターネットで相談先を探すと、消費者センターを装った悪質業者に騙されてしまう場合もあることから、消費者ホットライン（電話番号「１８８」）を案内するとよい。

１１　情報流出、自殺予告等及び人身安全関連事案に関するもの

○　情報流出等

Q11-1 社員のパソコンがウィルスに感染し、そのパソコンに保存していた顧客データ等が、インターネット上に流出してしまった。どう対処したら良いか。

・　速やかに、流出したデータに関係する顧客に状況を説明し、二次被害が発生しないよう、然るべき措置(パスワードの変更、カード番号の変更等)をとるよう求める。
・　ホームページやメールで、状況の説明と謝罪を行う。
・　流出してしまったデジタルデータを完全に回収することは出来ない。
・　サイト上で流出した情報が晒されているような事があれば、サイト管理者やプロバイダ等に削除依頼を行う。
・　刑事的に責任を問われる事は無いと思われるが、情報の管理体制の甘さに対する社会的非難や、情報が流出した顧客からの民事的な責任の追及があるものと予想されることから、それらへの対応も検討しておく必要がある。

Q11-2 退職した社員に貸与していたパソコンを調べたところ、当社の顧客データをライバル会社にメールで送信していたことが発覚した。元社員を訴えることはできるだろうか。

・　情報自体は窃盗罪の客体とはならない。
・　営業秘密に当たる情報であれば、不正競争防止法違反に該当する可能性がある。
・　刑事事件としては扱えない場合であっても、当該社員に対し、民事的に責任を追及する事は可能だと思われる。

[補足]

・　不正競争防止法の営業秘密となるための３要件
①　秘密として管理されていること（秘密管理制）
②　事業活動に有用な情報であること（有用性）
③　公然と知られていないこと（非公知性）
※　①につき、判例では、「秘密」の表示性（客観的認識可能性、例：「機密情報」「㊙」等の表示）とアクセスの制限性を求めている。

○　インターネット上の自殺予告等

・　自殺予告の通報があった場合は、プロバイダ等関係団体と連携して発信者の特定に努め、早急に人命保護等、的確な措置を行う必要があることから、サイバー犯罪対策課へ速報すること。(対策係 7861-3038, 3039　宿直時間帯 7861-3012)

・　プロバイダ等に照会を行う事が出来る要件

自殺の危険性が高く、緊急に対処する必要があり、下記【要件】を全て満たす場合に行う。

【要件】

・　掲示板等における自殺予告事案の書込み
①　自殺（殺害）予告の書込みがされた日時、書込みの内容等から判断して自殺決行の時期が切迫していると認められる。
②　書込みの内容から、自殺する動機、場所、方法等が示されること等により、現実に自殺を実行する可能性が高いと認められる。
③　書込みの内容に「自殺します」、「首をつります」、「一緒に死にませんか」、「自殺する人募集しています」等の表現により、自殺を決行する意思が表示されている。
④　書込みがなされている掲示板等の性質、他の書込みの内容等や書込み者に関する情報等に照らして、自殺の決行を疑わせる特段の事情が存在しない
・　メール等による自殺予告事案
①　基本的には掲示板等の場合と同様。ただし、メール等の受信者から送信者の住所、氏名等が聴取できる場合は、その方法による。

【発信者特定の方法】

・　[掲示板等の書込みの場合]
①　掲示板等の管理者に、当該書込みの日時、ＩＰアドレスを問い合わせる。
②　判明したＩＰアドレスを管理するプロバイダに対し、書込みの日時、ＩＰアドレスを元に契約者情報の開示を求める。
※　掲示板管理者の連絡先が不明の場合、ＷＨＯＩＳ検索（ドメイン検索）によりドメインの登録者情報を調べて連絡し、掲示板管理者の連絡先を問い合わせる。
※　会員制サイト等の場合、当該書込み者のＩＤから登録情報を開示してもらう方法もあるが、登録に際し、本人確認を行っているようなところでない限り、偽名等の可能性が高い。
・　[メールの場合]
①　当該メールアドレスが、送信者自身のものであると思われる場合であれば、当該メールアドレスを元に、プロバイダやフリーメールの運営者に登録情報の開示を求める。
②　メールのヘッダ情報から送信日時と送信元ＩＰアドレスを確認し、判明した送信日時、ＩＰアドレスから、プロバイダに契約者情報を問い合せる。

※　送信元メールアドレスの偽装は容易であるため、偽装されている可能性が低い場合や、ネットカフェ等から送信している事が明らかな場合を除き、送信元ＩＰアドレスから問い合わせた方が良い。

○　インターネット上の人身安全関連事案に関するもの

・　人身安全関連事案の相談については、人身安全関連事案総合対策本部と連携を図り、相談者等の安全確保を最優先に対処すること。

１２　インターネットカフェ等について

インターネット利用サービスを提供するインターネットカフェ等は、低価格で気軽にインターネットが利用できることに加え、多くの店舗が個室を備え、また、まんが、DVD、フリードリンク等多様なサービスを併せて提供することから、年齢、性別、国籍問わず、多くの人が利用している。

しかし、個室等においてインターネットを利用させる店舗においては、本人確認を実施していない店舗を中心に、その匿名性・密室性からサイバー犯罪のみならず、置引きや性犯罪さらには少年の健全育成を害する多くの事案が発生している現状にあった。

こうした現状を踏まえ、都民が安全に安心してインターネットカフェ等を利用できる環境を保持するため、個室等においてインターネットを利用させるサービスを提供する店舗に対して、顧客の本人確認等の義務を課す全国初の「インターネット端末利用営業の規制に関する条例」を制定し、平成２２年７月１日に施行されるに至った。

※　インターネット端末利用営業とは･･･

「個室等を設けて、顧客に対し、インターネットを利用することができるパソコン等を提供して、当該個室等においてインターネットを利用することができるようにするサービスを提供する営業」

○　インターネット端末利用営業者の義務等

①　本人確認義務

インターネット端末利用営業者は、店舗内において、インターネットを利用することができるようにするサービスの提供を行うに際しては、運転免許証等の本人確認書類の提示を受け、顧客の氏名・現住居及び生年月日(以下「本人特定事項」という。)を確認しなければならない。

※　顧客は本人確認を行う際、氏名等を偽ると罰金20万円が科せられる。

②　本人確認記録の作成・保存

インターネット端末利用営業者は、本人特定事項、本人確認を行った日時等の本人確認記録をサービス提供終了日から３年間保存しなければならない。

※　営業者は、「個人情報保護法」または「東京都個人情報の保護に関する条例」に該当する事業者となり、個人情報の適正な取扱いが義務づけられることになります。

③　通信端末機器特定記録等の作成・保存

インターネット端末利用営業者は、顧客が利用したパソコン等の番号、顧客の入

退店日時等の通信端末機器特定記録等をサービス提供終了日から３年間保存しなければならない。

④　不正利用防止措置等

インターネット端末利用営業者は、

ア　顧客が入力した情報を他人が不正に利用できないようにする機能を有するソフトウェア(セキュリティ対策ソフト、リカバリーソフト等)を備えたパソコン等の提供

イ　防犯カメラの設置

等、インターネット端末利用営業が犯罪に利用されることを防止するための措置を講じ、また

ウ　防犯上必要な店内の照度の確保

エ　アダルト向けまんが等有害図書の区分配列

オ　青少年に対するフィルタリングソフトが導入されたパソコンの提供

カ　不用意な識別番号の入力の危険性やインターネットを利用した犯罪行為に関する警告など利用者への注意喚起

等、顧客が安心してサービスを受けることができる環境を整備するために必要な措置を講ずるよう努めなければならない。

○　条例対象外店舗への指導

・　「インターネット連絡協議会」への参加促進

条例施行に伴い、本人確認が行われていない条例対象外の店舗において、サイバー犯罪等が行われると予想されることから、条例対象外店舗に対しても、自主的な本人確認等を依頼するなど協力体制の構築が必要とされる。

条例対象店舗だけではなく、条例対象外店舗に対しても、各警察署に設置されている「インターネットカフェ等連絡協議会」への積極的な参加を促すとともに、同協議会を通じて、条例の義務に準じた本人確認等を求め、サイバー犯罪等の防止を図る。

○　インターネットカフェ等利用時の注意事項

インターネットカフェ等は不特定多数の人が利用する公共の場所です。

自分の席と他人の席との距離が近かったり、他人が自分の席の後ろを通ったりします。また、自分が使ったパソコンを他人が使うので

・　ネットバンキングやオークション等、ID・パスワードや暗証番号の入力を必要とするサイトの利用や個人情報の送信等は控える。

・　利用後、履歴等を削除する。

等、自己防衛の意識を持ち、セキュリティ等の安全対策を心掛ける。