

インターネットサービスの利用に関するガイドライン

はじめに

鳥取中央有線放送株式会社(以下「当社」と言います)では、さまざまなインターネットサービス(以下「本サービス」と言います)を提供しています。本サービスは、多くのユーザーによって共有されています。さらに、本サービスを利用して接続するインターネット上には、当社のユーザー以外にも世界中に存在する不特定多数のユーザーが存在しています。それぞれのユーザーは、インターネットを利用して、情報を共有したり、他のユーザーと通信をしたりなどの様々な恩恵を受けます。その一方で、他のユーザーの権利を侵害しない、迷惑をかけないなどの義務や責任を負うこととなります。

このサービスの利用に関するガイドライン(以下「本ガイドライン」と言います)では本サービス(開始しているサービスに限る)のご利用にあたり、守っていただきたい規則やガイドラインについて説明しています。本ガイドラインの内容をご一読の上、定められた規則を遵守していただきますようお願いいたします。

本ガイドライン及び契約約款に規定されている規則やガイドラインを破り、当社の警告を無視して他のユーザーに迷惑となる行為を続けた場合、契約約款の規定に基づき、サービスの停止を行う場合があります。

目 次

- 1.セキュリティについて
 - 1.1 アカウント情報及びパスワード管理
 - 1.1.1 パスワード管理上の注意事項
 - 1.1.2 パスワード管理を怠ると
 - 1.2 プライバシーの遵守
 - 1.2.1 プライバシーの保護
 - 1.2.2 他人のプライバシーを侵害する行為とは
 - 1.3 ウィルス対策
 - 1.3.1 コンピューターウィルスに感染しないための対策
 - 1.3.2 コンピューターウィルスに感染してしまうと
- 2.電子メール
 - 2.1 電子メールご利用において
 - 2.2 覚えのないメールには要注意
 - 2.2.1 メーリングリスト
 - 2.2.2 ねずみ講
 - 2.2.3 スпамメール
 - 2.2.4 チェーンメール
 - 2.2.5 爆弾メール
 - 2.2.6 ウィルスメール
- 3.ホームページ
 - 3.1 作成したホームページの内容に責任を持つ
 - 3.2 ホームページ公開時の考慮すべき事項
 - 3.2.1 著作権侵害をしない
 - 3.2.2 誹謗・中傷しない
 - 3.2.3 個人情報の取扱いに注意する
 - 3.2.4 他人のプライバシーに配慮する
 - 3.2.5 わいせつな画像や文章を載せない
- 4.データ転送速度、データ容量、その他の制限
- 5.個人情報の保護
6. 本ガイドライン違反が確認された場合
 - 6.1 当社からの警告
 - 6.2 警告を無視し続けた場合の措置
 - 6.2.1 送信防止措置について
 - 6.3 アカウント及び発信元の調査
 - 6.3.1 アカウント使用の停止に伴う措置
- 7.本ガイドラインの更新

1.セキュリティについて

セキュリティとは、インターネットを安心して利用するために注意を払うべき安全対策のことをいいます。インターネットは誰にでも開かれている自由な社会ですが、まだ秩序が整っていない発展途上の場という側面も持っています。自分の身は自分で守らなくてはなりません。したがって、侵入者や違法な行為を行う人々を日頃から十分認識しておくことが大切です。

1.1 アカウント情報及びパスワード管理

電子メールやショッピングサイト等インターネット上の取引を行う場合、自分のユーザーアカウントを登録する必要があります。ユーザーアカウントを使用するためには、与えられたユーザー名を使用して、本人性の確認のためにユーザー認証を受けなければなりません。ユーザー認証の際には、自分がそのユーザー名の正式な所有者であることを証明するために、パスワードを入力しなければなりません。

1.1.1 パスワード管理上の注意事項

自分の氏名、生年月日、電話番号など、容易に類推できるパスワードでは、危険から身を守るのには十分とはいえません。ショッピングサイト等を利用する場合、登録するパスワードをわかりにくいように工夫してください。また、当社では、無作為に作成された文字列を電子メールアカウントのパスワードとして発行しております。他人に自分のユーザーアカウントを使用されないよう、パスワードの管理には十分にご注意ください。

1.1.2 パスワード管理を怠ると

他人に自分のユーザーアカウントを使用されてしまうと、以下のような危険にさらされます。

- 本来は使用権限が与えられていないユーザーがネットワークに接続できるようになる。
- 自分の電子メールアドレスに届いたメールの内容が他人に読まれる。
- ショッピングサイトなどで、商品の購入履歴や住所、電話番号などの個人情報が漏洩することになります。
- ショッピングサイトによっては、会員管理としてカード番号を登録していることがあるため、他人の登録したカードで買い物をされてしまう可能性もあります。

このような、第三者による不正アクセスを防止するためには、各々のユーザーがID 及びパスワードの管理に常に注意を払ってください。

1.2 プライバシーの遵守

インターネットの世界でも、実社会と同様に、プライバシーは守られなければなりません。特にインターネットでは不特定多数のユーザーが接続する可能性があるため、細心の注意を払って個人情報を管理しなければなりません。

1.2.1 プライバシーの保護

各々のユーザーにとって、最も大切なことは自分や知人の個人情報を不用意に公開しないことです。ホームページを開設し、掲示板やアンケートサイトなどを用意している場合は、収集した情報の管理について、責任があるということを認識しなければなりません。

個人の住所、氏名、電話番号、生年月日などのプライバシーに関わる情報を収集する場合には、万全な情報セキュリティ体制のもとで管理する義務があると言えます。また、複数の人に電子メールを送信する場合、宛先のメールアドレスを送信先すべてに公開してよいか判断する必要があります。

1.2.2 他人のプライバシーを侵害する行為とは

以下のような行為はプライバシーの侵害として問われる可能性があります。

- ・ 開設しているホームページ等で収集した他人の個人情報をインターネット上で公開した。個人情報とは、住所・氏名・電話番号など個人を特定可能とする情報だけでなく、本人に承諾のない電子メールの内容の引用、特定のメールアドレスからのアクセス履歴など、個人情報と関連性のあるデータ情報を含みます。
- ・ 複数の人に電子メールを送信する際に、宛先またはCC(Carbon Copy)に指定して送信した。この場合、受信者間に面識がない場合、個人が保持するメールアドレスが公開されたこととなります。

1.3 ウィルス対策

コンピューターウィルスは、電子メールやホームページ閲覧などによってコンピュータに侵入する特殊なプログラムです。最近ではインターネットの普及に伴い、電子メールをプレビューしただけで感染するものや、ホームページを閲覧しただけで感染するものが増えてきています。また、インターネット利用者の増加や常時接続回線が普及してきたことで、ウィルスの拡大が速くなってきています。

1.3.1 コンピューターウィルスに感染しないための対策

当社では、メールウィルスチェックサービスを無料で行っておりますが、これは電子メールによる感染を防止する対策となります。ウィルスの感染経路としては、

- ・ 電子メールの他に・ホームページの閲覧によるインターネットを介した感染
- ・ ネットワークのファイル共有によるネットワークを介した感染
- ・ マイクロソフト社のOffice アプリケーション(Word、Excel、PowerPoint、Access)のマクロ機能を利用したプログラムの実行による感染

などがあります。このようなコンピューターウィルスに感染しないようにするためには、以下のような対策があります。

- ・ ウィルス対策ソフトを導入し、常に最新のウィルスに対応できるように、インターネットなどでウィルス検知用データを更新しておきます。

- Windows のパソコンをご利用の場合は、マイクロソフト社が無償配布しているWindowsの修正プログラムを適用することで、パソコンのセキュリティを強化する対策となります。ウイルス対策ソフトを用いても、残念ながらウイルス対策は万全とはいえません。
- 不審な電子メールを受信した場合は、削除してください。このような電子メールに添付ファイルがある場合は、開かないことが賢明です。
- ファイルのダウンロードを行う際は、配信元が信頼できるサイトであるか確認してください。
- 定期的にデータのバックアップをとっておけば、万一ウイルスに感染しても被害を最小限に抑えることができるでしょう。

1.3.2 コンピューターウイルスに感染してしまうと

コンピューターウイルスに感染しますと、コンピュータが動かなくなったりファイルが壊れたり、さまざまな障害がでます。また、コンピュータに登録されている電子メールのアドレス帳や過去の送受信履歴を利用して、自動的にウイルス付きの電子メールを送信するものも多く、世界中にウイルスが蔓延する大きな原因となっています。

2. 電子メール

当社から提供されている電子メールアドレスを使用して、インターネット上に存在する世界中の人と電子メールをやり取りすることができます。メッセージを送ることもできますし、ちょっとした電子ファイルを添えて送ることもできますが、セキュリティはそれほど高くありません。たくさんのネットワークを経由して届けられることから、送信の途中で紛失したり覗かれたりする危険もあります。

2.1 電子メールご利用において

すぐに配達される電子メールは会話のように気軽に楽しむことができますが、便利である反面、メッセージがどのように相手に受け取られるかなど、電子メールの特性を考慮し、ご利用においては十分に注意しなくてはなりません。電子メール使用时には、以下のようなことを考慮してください。

- インターネット上のメールは安全ではないものと考えておかなければなりません。クレジットカード番号やパスワードなど他人に知られたくない個人情報や非公開情報などは決してメールに含めてはいけません。
- 相手に対して常に寛容であるよう心がけ、人を不愉快にさせるような話や言葉遣いは慎みましょう。
- あなたが送ろうとするメッセージがどれだけ大きいのかを知っておきましょう。容量の大きなメッセージや添付ファイルは、宛先のコンピュータシステムや途中経由するインターネットサーバの故障を誘発する可能性があります。送信しようとしているメッセージや添付ファイルの容量が大きいと思うときは、相手先に確認してから送信しましょう。
- 電子メールでは、絶対にチェーンメールを送ってはいけません。チェーンメールとは、はっきりと相手を特定しないで伝言を求める電子メール。

- ・宛先にメールのアドレスを書く時には、間違いのないよう慎重に入力しましょう。また、個人のアドレスのように見えても、実はあるグループに送られるというアドレスもあります。誰に送ろうとしているのかを知っておきましょう。
- ・返事をするときには、cc (Carbon Copy) の宛先に気をつけましょう。メッセージが1対1のやりとりになるときは、他人を巻き込み続けてはいけません。
- ・不愉快な内容の電子メールを受取ったら、相手にしないようにしましょう。また、挑発的な言葉を投げかけられても応じてはいけません。常に冷静に対応するよう心がけましょう。
- ・電子メールの内容を他の場所に転載したりすると著作権の侵害にあたる場合もあります。また、あなた以外の人に知られることによって本人の名誉が傷つくことや、プライバシーに関する情報が漏れて迷惑をかけるかもしれません。受け取った電子メールを転送したり転載したりする場合には、本人に連絡して承諾を得るのが良いでしょう。私信である電子メールをホームページなどの公開された場所に掲載するときは、ことさら慎重に取り扱うべきです。

2.2 覚えのないメールには要注意

2.2.1 メーリングリスト

加入に際しては、そのメーリングリストが信頼にあたいするものであるかどうか良く検討してください。またリストから除外してもらいたい場合どのようにすれば良いのかを事前に確認してから加入しましょう。また知人が勝手に登録していたというような例もあるので、自分が登録した覚えがなければその旨連絡して登録を抹消してもらいましょう。

2.2.2 ねずみ講

実社会同様、自分が被害者になると同時に加害者になる可能性もあるので、ねずみ講メールかなと思ったら、絶対に転送しないことです。

事例:「住所氏名がリストアップされている5人に500円を送り、リストの一番上を消し、二番目以降を順次繰上げ五番目に自分の住所氏名を載せメールを出来るだけたくさんの人に送れば、数百万の収入がある」

2.2.3 スпамメール

身に覚えのないところから届くダイレクトメールなど自分にとって不要なメールが頻繁に届き、本来の必要なメールを捜すのに大変苦勞することになります。このようなメールは、返信などせず無視して削除することが賢明です。このようなメールの受信が永続的に続く場合は、メールアドレスを変更することもひとつの対策となります。

2.2.4 チェーンメール

自分の所で断ち切る勇気を持ちましょう。このようなメールは他人に再送信すると、拡大してメールサーバーに障害を与える恐れや、通信混乱を招く恐れがあるので、決して転送せずに、即刻削除することです。

事例:「幸せのメールという電子メールが届き、5人に送るように指示が書かれていた。」

2.2.5 爆弾メール

一度に大量のメールを送信され、メールBOX 容量がいっぱいとなり、必要なメールが取り出せなくなったりします。加入するプロバイダに連絡し、自分のメールボックスにあるメールの削除を依頼するなどの対処となります。お使いのメールソフトに、特定のメールアドレスからの受信拒否を行う機能があれば、それを使用することも対策のひとつです。

2.2.6 ウィルスメール

知らない人から届いたメールの添付ファイルを開いて、コンピューターウィルスに感染する場合があります。身に覚えのないメールは開かずに削除することが賢明です。少なくとも添付ファイルは安易に開かない(添付ファイルはウィルスが入っている場合がある)ことです。市販のパソコンウイルスチェッカーを導入して、新しく受信したファイル等を開く前に必ずウイルスチェックをすることも対策のひとつです。いずれにしても、重要なファイルやプログラムは、必ずバックアップを取ることが必要です。

3.ホームページ

広い範囲の人々に向かって情報を発信できるホームページは、インターネットの大きな魅力の一つとなっています。当社のホームページサービスやその他インターネットサービスで公開する情報については、個人が発信する情報に責任を持つことになります。

3.1 作成したホームページの内容に責任を持つ

ホームページの掲載内容には、ホームページ開設者個人が責任を持つことになります。当社は、ユーザーが開設しているホームページの内容について責任を負うことはできません。

3.2 ホームページ公開時の考慮すべき事項

インターネット上で公開されるホームページは、多くの人に閲覧されます。責任を問われることにならないよう、掲載内容には十分な注意を払う必要があります。

3.2.1 著作権侵害をしない

文章や写真、音楽、ソフトウェアなどの著作物には著作権があります。他人のホームページや電子掲示板や雑誌に載っている著作物を、無断で使用してホームページを作成する等、著作権を侵害しないようにしましょう。

3.2.2 誹謗・中傷しない

ホームページ上で人を批判するときには、相手の人格を否定するような過激な書き方をしてはいけません。あまり度が過ぎると、法的な責任を問われる深刻な事態になることがあります。

3.2.3 個人情報の取扱いに注意する

自分や家族の住所、氏名、電話番号などはもちろん、家族の写真などを安易に公開するのは危険です。犯罪から身を守るため、ホームページでの個人情報の開示には十分に注意しましょう。

3.2.4 他人のプライバシーに配慮する

他人の住所、氏名、電話番号などはもちろん、他人の私生活上の事実や秘密、写真や似顔絵などを本人の許諾なくホームページで公開してはいけません。その人に嫌悪、羞恥、不快感など精神的苦痛を与え、プライバシーや肖像権の侵害となる他、場合によっては名誉または信用の毀損となります。

3.2.5 わいせつな画像や文章を載せない

ホームページでわいせつ、売春、暴力、残虐等いわゆる「公序良俗」に反する情報を公開しないようにしましょう。

4.データ転送速度、データ容量、その他の制限

本サービス利用にあたって、規定されたデータ転送速度、データ容量、その他の制限に準拠してください。ご自分の活動が、他のユーザーのサービス利用を不適切に制限したり、抑制したり、迷惑をかけたりしていないことを常に確認してください。また、ネットワークに異常に大きな負荷がかからないように注意してください。当社のサービス、バックボーン、ネットワークノード、その他ネットワークサービスを監視する機能などへの不適切な制限、抑制、混乱、品質低下及び妨害につながるような行為は避けてください。

当社の書面による同意なしに、当社から提供されるサービスやその他の機能又はその一部を第三者に再販売したり、供与したり、再提供したりすることはできません。当社のサービスは、個人がインターネットを使う為のものです。当社のサービスを商業目的に使うことはできません。

5.個人情報の保護

インターネットは、匿名性の世界です。したがって自分であることを証明するIDやパスワードの管理には、万全の注意を払って下さい。また、あなたが自分の住所、電話番号等をインターネット上に公開することは大変危険です。一瞬のうちに、あなたの個人情報が世界中を駆けめぐってしまうということを十分に認識して下さい。

当社は、当社のユーザーに係る個人情報の保護については、当社の定めた「お客様個人情報保護方針」、「個人情報保護規程」等の他、個人情報保護に関する法令等を遵守します。また、当社が管理するユーザーから提供いただいた個人情報は、以下の場合を除き、第三者に提供されることはありません。

- ・ ユーザーにご承諾をいただいた場合
- ・ 当社が個人情報保護契約を締結している業務委託先又は業務提携先(販売代理店や運送会社等)に対し、業務を行う上で必要と思われる範囲の情報を開示する場合
- ・ ユーザーによる商品の注文や有料サービスの利用等で、その代金決済のため金融機関等に個人情報を開示する必要がある場合
- ・ 法令等に基づく要請に応じる場合

6. 本ガイドライン違反が確認された場合

6.1 当社からの警告

ユーザーの皆様は、本ガイドラインを守り、インターネットコミュニティ内の良き住民となるよう常に努力してください。他のユーザーや当社サービス利用者以外のユーザーから苦情等が届いた場合、又は本ガイドラインや契約約款に著しく違反した活動を行っている場合、当社は警告を出す等の適切な対応を行う場合があります。当社には、サービスやネットワークを監視する義務はありませんが、帯域幅(データ転送の状態)、サービスの使用方法、ユーザーの開設したホームページ等を随時監視する権利を保有しています。これらの活動は、サービスを円滑に運営し、違反行為を見つけ、ネットワークと当社のユーザーを守る上で必要であることをご理解ください。

6.2 警告を無視し続けた場合の措置

当社はユーザーが不適切な行為を行った場合、警告を発するなどの適切な処置を実行します。本ガイドラインや契約約款に違反した行為を続け、他のユーザーによるサービス利用や当社の営業活動を著しく妨害した場合は、当社の適切と考える対応処置を実行します。

このような対応処置には、ホームページの一時的又は永続的な削除、インターネット転送の制限、サービスの全部又は一部の一時停止又は強制解除などがありますが、これだけに限定されるわけではありません。当社には、このような対応処置を実行する義務はありません。上記の処置は例外的な処置であり、通常であれば、当社は、適切と考えられる他の合法的又は技術的な手段を実行します。

6.2.1 送信防止措置について

ユーザー(以降発信者)がホームページなどで公開している文章や画像などに対して、知的財産権、肖像権、プライバシー権及びパブリシティ権を侵害するものである等の理由により、他のユーザーや当社サービス利用者以外のユーザーから送信防止措置の申立てが発生した場合、当社はプロバイダ責任制限法に則り、以下の手続きを行います。

- ・ 該当の文章や画像などの自主的削除要と判断される場合は発信者へ削除要請を行います。発信者の自主的処置がなされない場合、当社にて削除措置を講じる場合がございます。
- ・ 該当の文章や画像の自主的削除の要否が困難な場合は発信者へ削除等措置を講じて差し支えないか否かを確認します。発信者の承諾を得られた場合、又は、7日間以内の反論がない場合は該当の文章や画像の削除措置を講じます。

ユーザーホームページなどで公開している文章や画像に対して、他者の著作権を侵害するものであるという理由により、他のユーザーや当社サービス利用者以外のユーザーから送信防止処置の申立てが発生した場合、著作権の侵害であると判断される場合は、当社はプロバイダ責任制限法に則り、以下の手続きを行います。

- ・ 当該侵害情報の送信を防止するために削除等の措置を講じます。
- ・ 当該侵害情報の送信防止措置を講ずる旨又は講じた旨を発信者及び申出者へ通知します。

6.3 アカウント及び発信元の調査

当社は、本ガイドライン及び約款に違反したおそれのあるアカウント及び発信元を調査する権利を有しています。調査を行うケースとしては、以下のような場合があります。ただし、これだけに限定されるわけではありません。

- ・ ウィルスメールやスパムメールなどの不正な電信メールが発信されていることが確認された場合
- ・ 当社のユーザーや当社サービス利用者以外のユーザーが運営する電子掲示板サイトに不正な書き込みをするなどして、サイト管理者より対処依頼があった場合
- ・ 特定のコンピュータに対して不正なアクセスが繰り返され、そのコンピュータの管理者より対処依頼があった場合
- ・ 当社のユーザーが公開するホームページの掲載内容に不適切な文章や画像が確認された場合上記の場合、関係ユーザーや苦情を伝えてきた人々から情報を集めたり、当社のサービス利用を一時停止したり、問題のあるホームページを削除したりする場合があります。
- ・

6.3.1 アカウント使用の停止に伴う措置

ユーザーがアカウントの使用を停止した場合、当社は、そのアカウントに関連するファイル、プログラム、データ、電子メールメッセージを削除する権利があります。当社が、何らかの理由でこの権利を遂行できなかった場合でも、権利を放棄したわけではありません。

7. 本ガイドラインの更新

当社は本ガイドラインを事前の通知なしに随時改訂できるものとします。

平成21年4月1日

鳥取中央有線放送株式会社_