

このハンドブックでも解決しないときは、
お近くの総合通信局、または
総務省電気通信消費者相談センターへ

受付時間／平日 9:00~12:00、13:00~17:00



信越地区にお住まいの方

電話番号
026-234-9952

総務省 信越総合通信局
〒380-8795 長野市旭町1108
長野第1合同庁舎

北海道地区にお住まいの方

電話番号
011-709-3956

総務省 北海道総合通信局
〒060-8795 札幌市北区北8条西2-1-1
札幌第1合同庁舎

北陸地区にお住まいの方

電話番号
076-233-4429

総務省 北陸総合通信局
〒920-8795 金沢市広坂2-2-60
金沢広坂合同庁舎

東北地区にお住まいの方

電話番号
022-221-0632

総務省 東北総合通信局
〒980-8795 仙台市青葉区本町3-2-23
仙台第2合同庁舎

中国地区にお住まいの方

電話番号
082-222-3376

総務省 中国総合通信局
〒730-8795 広島市中区東白島町19-36

関東地区にお住まいの方

電話番号
03-6238-1935

総務省 関東総合通信局
〒102-8795 千代田区九段南1-2-1
九段第3合同庁舎

東海地区にお住まいの方

電話番号
052-971-9133

総務省 東海総合通信局
〒461-8795 名古屋市東区白壁1-15-1
名古屋合同庁舎第3号館

四国地区にお住まいの方

電話番号
089-936-5042

総務省 四国総合通信局
〒790-8795 松山市宮田町8-5

近畿地区にお住まいの方

電話番号
06-6942-8519

総務省 近畿総合通信局
〒540-8795 大阪市中央区大手前1-5-44
大阪合同庁舎第1号館

九州地区にお住まいの方

電話番号
096-326-7862

総務省 九州総合通信局
〒860-8795 熊本市春日2-10-1
熊本地方合同庁舎(A棟)

沖縄地区にお住まいの方

電話番号
098-865-2302

総務省 沖縄総合通信事務所
〒900-8795 那覇市東町26-29

総務省
電気通信消費者相談センター

電話番号
03-5253-5900

〒100-8926 千代田区霞が関2-1-2
中央合同庁舎第二号館

保存版 平成24年度版

知っていれば安心! 便利!

電気通信サービス

Q&A



携帯電話
スマートフォン



インターネット

災害時の
サービスって?

困ったことも
知りたいことも、
わたしたちが
お答えします!

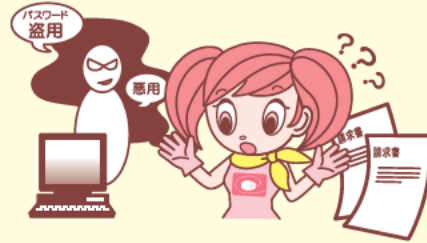
おしえて!
イザ! といふときの
電話サービス

はじめに

国内・国際電話、携帯電話・PHS、スマートフォン、インターネット…
電気通信サービス※の発達によって、わたしたちの生活はとても便利になりました。



その一方で利用者みなさまがトラブルに巻き込まれることも少なくありません。



電話やインターネットを安心して利用するために必要なのは、事前のちょっとした知識!



このパンフレットでは、
わたしたちE-NAVIフレンズがみなさまの疑問にQ&A方式でわかりやすくお答えします!
ぜひお手元に保存していただき、電気通信サービスについて不安になったりお困りになったときはいつでもお役立てください。

わたしたちが
お答えします!

E-NAVI
E-NAVI

リンちゃん

アミちゃん

ケイちゃん

※電気通信サービスって? 電気通信を利用して提供されるサービスのことをい、国内電話、国際電話、携帯電話・PHS、スマートフォン、インターネット、ADSL、マイライン等が対象になります。

文中に出てくる
2つのマークに **注目!**



利用するために知っておきたい
基礎知識です。



トラブルになる可能性があるので
十分に注意しましょう。

トピックス 「スマートフォンってナニ?」 03



ピックアップ情報

- 勧誘や契約時の説明等についてのQ&A 05
- 架空請求・不当請求トラブルについてのQ&A 07
- 携帯電話やスマートフォンの
高額パケット請求についてのQ&A 10

ピックアップ

携帯電話・スマートフォンを快適に利用するために

- 携帯電話利用時の注意点についてのQ&A 11
- 迷惑メールについてのQ&A 14
- フィルタリングについてのQ&A 17
- 携帯電話の番号ポータビリティについてのQ&A 20
- 携帯電話不正利用防止法についてのQ&A 21

スマートフォン
携帯電話

インターネットを楽しむために

- インターネット上の違法・有害情報についてのQ&A 22
- フィッシング詐欺についてのQ&A 23
- ネットセキュリティについてのQ&A 24
- インターネット上のマナーについてのQ&A 26

インターネット

電話サービスをいつも安心・便利に利用するために

- 災害時・停電時の電話サービスの利用についてのQ&A 27
- 災害用の伝言サービスについてのQ&A 28
- ユニバーサルサービス制度についてのQ&A 30

電話サービス



これまでの携帯電話と何が違うの?



スマートフォンは、**パソコンに近い性質を持った携帯電話**です。



多種多様な**アプリケーション**をインターネット上にあるサイト(マーケット)から**利用者自身が自由に選択してダウンロード**することで、利用者が自ら端末をカスタマイズすることができ、利用者自身のニーズに合った便利な使い方が可能となります。

パソコン用のウェブサイトの閲覧ができ、多様な情報収集が可能となります。

一方で、携帯電話事業者が管理するネットワークで提供するインターネット接続サービス(iモード、ezweb、Yahoo!ケータイ)を介さずにインターネットに接続することが可能となるため、**パソコンと同様の情報セキュリティ上の危険性**があります。

パソコン用のウェブサイトを閲覧すると**大容量のデータ通信**が行われます。また、スマートフォンの**アプリケーション(アプリ)**には、自動的に通信を行うものもあります。

スマートフォンについては、**こちらのページもどうぞ!**

Link!

- パケット通信料の高額請求について ————— p10 A10
- パケット通信料が高額になるのを防止するために ————— p10 A11
- 緊急地震速報の受信について ————— p11 A12
- 災害時や通信混雑時に使う場合の注意 ————— p11 A13
- 取り扱い上の注意について ————— p12 A14



スマートフォンを利用する場合はこんな点に注意!



パケット通信料が**高額**になる場合、**セキュリティ上の危険性**に注意が必要です。

- パソコン用のウェブサイトを開覧すると大容量のデータ通信が行われます。また、スマートフォンのアプリケーション(アプリ)は自動的に通信を行ったり、自動更新が行われたりすることもあるため、これまでの携帯電話に比べてパケット通信料が高額になりやすくなっています。ご自身では通信をしているつもりがなくても予期せぬパケット通信料が発生する場合がありますので注意してください。
- パケット通信料が思いがけず高額となることを防止するには、パケット定額制を利用することも有効です。また、スマートフォンではパケット通信(データ通信)をオフにすることができる(一部機種では未対応のものもあります)ほか、パケット通信以外にWi-Fiなどの無線アクセスサービスを利用することができます。
- これまでの携帯電話端末と異なり、スマートフォンは、携帯電話事業者が管理するネットワークを介さずにインターネットに接続することが可能となるため、パソコンと同様、アプリケーションのダウンロードを通じてウイルスに感染するなど情報セキュリティ上の危険性があります。対策としては、信頼できるアプリケーション・マーケットからアプリケーションを購入することや、スマートフォン用のセキュリティ対策ソフトの利用を確認することが有効です。
- アプリケーションによっては、スマートフォンに保存された個人に関する情報(電話帳、位置情報など)にアクセスするものがあります。ダウンロード時はアクセスする情報や利用条件をよく確認しましょう。また、普段からパスワードロックを掛けておくなど端末の紛失や盗難にもご注意ください。
- 画面がフリーズする(固まってしまう)、バッテリーがすぐに無くなってしまふなどの現象も多く見られます。多くのアプリが同時に起動されているなどが原因ですので、ご注意ください。



落下 注意! 水濡れ
丁寧な取り扱いを!



- ゲームサイト(ゲームアプリ)を利用するときは ————— p12 A15
- 中古のスマートフォンを売買するときは ————— p13 A16
- 迷惑メールの対策について ————— p14 A17
- 番号ポータビリティについて ————— p20 A22
- スマートフォンの情報セキュリティ対策について ————— p25 A30

Q01 電気通信サービスを利用するためには、
どんな点に注意が必要なの？

A01



契約時にはサービス内容、
契約内容、利用料金、
契約条件等をよく確認しましょう。



電気通信サービスの契約内容などが十分に理解されていないことから生ずるトラブルを回避するため、電気通信事業者や代理店等には、契約する前に説明することが義務付けられています。一方で、利用者においても、サービス内容、料金その他の支払が必要になる経費、契約の解除に伴う制限や違約金の有無を積極的に確認するよう心がけましょう。



携帯電話等



- 携帯電話・スマートフォンやWi-Fiなど無線の電気通信サービスを選ぶときは特に、サービスを受けることができる地域か、通信環境によってサービスの品質が低下するかなどをよく確認しましょう。
- 携帯電話・スマートフォンの契約を結ぶときは、本人確認書類が必要になります。必要な書類や手続については、各電気通信事業者にお問い合わせください。
- 携帯電話を海外で利用する場合の通話料・パケット通信料は、日本の料金体系とは異なり、各種割引サービスの提供がなされず、高額になることがあります。



- オプション加入やパソコンとのセット契約で、低廉な価格で契約する場合、途中で契約を解約すると違約金が発生することがあります。見た目の安さで判断せず、契約内容をよく確認しましょう。
- 携帯電話が第三者に使われることにより、高額請求の被害にあうケースが発生しています。盗難・紛失した場合には、速やかに契約している携帯電話会社に連絡しましょう。

盗難・紛失の際は
速やかに契約している
携帯電話会社へ連絡
しましょう



固定電話・IP電話・インターネット接続サービス



- 電話サービスを選ぶときには、利用(接続)できない番号の有無をよく確認しましょう。
- 電話サービスやインターネット接続サービス等選ぶときは、サービス料金以外の工事費やモデムレンタル料の有無、サービス提供開始までの期間等をよく確認しましょう。



- インターネット接続サービスでは、契約時はプロバイダが回線事業者の契約の取次ぎをする場合がありますが、サービスを解約する場合には、プロバイダと回線事業者のそれぞれのサービスの解約手続きをしないと契約が継続されて、料金徴収が続くことになるので、注意が必要です。

未成年者の契約について



- 未成年者が携帯電話等、インターネットの契約を行う場合、親権者の同意が必要となります。
- 未成年者の加入契約の際に、親権者の同意を得ていない契約は取消しができる場合がありますが、未成年者が成人と偽って契約した場合等には取消しができないことがあります。
- 契約の際には、親権者の同意書類が必要になります。詳しい手続等については各電気通信事業者にお問い合わせください。

勧誘や契約時の説明についてのQ&A

Q02 インターネット回線(光ファイバーなど)などの
勧誘を受けたときは、どんな点に注意が必要なの？

A02  その場で**すぐ契約せず、十分に検討**しましょう。



サービス内容が分からない場合、加入する必要があるかどうか分からない場合、勧誘が強引だと感じた場合には、その場で**すぐ契約(申込み)したり、曖昧な返事をせず**に、**契約内容を確認し、十分に検討**を行うようにしてください。

- 電話勧誘や訪問販売によるトラブルが増えています。サービスの内容が分からない場合、その場で**すぐ契約(申込み)せず**に、**分かるまで説明を聞いたり家族に相談したりして決める**よう心掛けてください。
- 契約は口頭でも成立します。契約(申込み)する意思がない場合は、**曖昧な返事をせず、はっきりと意思表示**することも重要です。
- 電気通信サービスにクーリングオフは適用されません。契約(申込み)を行う際は慎重に検討しましょう。どうしても**不要だ**という場合、インターネット回線は**工事前**であれば**解約(キャンセル)**が可能な場合があります。契約先の電気通信事業者に相談してください。



架空請求・不当請求トラブルについてのQ&A


Q03 まったく身に覚えのない**料金請求**が届いたのですが、**支払う必要**はあるの？

A03  **全く契約した覚えがなければ、支払う義務はありません。**



架空請求・不当請求トラブルについてのQ&A

Q04 URLをクリックしたら、いきなり**「登録完了画面」**になってしまいました。どうしたらいいの？

A04  契約が**有効に成立しているとは限りません。**



パソコンや携帯電話に**「登録されました」**や**「入会ありがとうございます」**と表示されても、そもそも**契約が有効に成立しているとは限りません**。請求されても**安易に支払うことはやめ**ましょう。


Q05 **業者に連絡**した方がいいの？

A05  **あわてて業者へ連絡することは、絶対にやめ**ましょう。



あわてて業者へ連絡することは、**氏名や電話番号などの新たな個人情報**を知らせることになるので**絶対にやめ**ましょう。一般的に、インターネット上のウェブページにアクセスした場合、**メールアドレスや携帯電話事業者名**が相手に伝わる場合があります。しかし、これらの情報だけでは、**アクセスした人を特定することはできません**。過度に不安になる必要はありません。

Q06 **「裁判所に訴える」、「強制執行する」**などと言われていますが、どうしたらいいの？

A06  **そうした文言に惑わされることなく、落ち着いて対処**しましょう。



「裁判」、「強制執行」、「債権回収」等の法律用語を持ち出してくる場合がありますが、**そうした文言に惑わされることなく、落ち着いて対処**しましょう。もしも、**公的機関からの通知文書等**が送付された場合には、その通知文書等の真偽について、**すぐに無料法律相談等、最寄りの自治体の相談窓口**に相談しましょう。

架空請求・不当請求トラブル についてのQ&A(つづき)

Q07 請求が脅迫めいています。どうしたらいいの？

A07  最寄りの警察署に相談しましょう。

脅迫めいた請求や、常識的に考えて迷惑な時間帯に何度も執拗に連絡してくるような場合は、恐喝等の犯罪に該当する可能性があります。最寄りの警察署に相談しましょう。



Q08 何度もメールによる身に覚えのない請求が届く場合には、どうしたらいいの？

A08  身に覚えのない請求のメールは無視しましょう。

契約しているプロバイダや携帯電話会社の迷惑メール対策サービスを利用して、迷惑請求メールをブロックすることも有効です。設定の方法については、契約しているプロバイダや携帯電話会社にご確認ください。



Q09 パソコンに請求画面が表示され続けてしまいます。どうしたらいいの？

A09  プログラム削除の方法を確認してください。

パソコンに請求画面が表示されて消えないのは、請求画面を表示させるプログラム(コンピュータウイルス)に感染しているためです。ウイルスを駆除するためには、パソコンメーカーや契約しているプロバイダ、独立行政法人情報処理推進機構(IPA)「情報セキュリティ安心相談窓口」にプログラム削除の方法を確認してください。


情報セキュリティ安心相談窓口
<http://www.ipa.go.jp/security/anshin/>



携帯電話やスマートフォンの 高額パケット請求についてのQ&A




Q10 携帯電話やスマートフォンのパケット通信料金が思いがけず高額となる理由として、どのようなものがあるの？

A10  携帯電話やスマートフォンのパケット通信料金は、通信時間ではなくデータ量によって変わります。また、パケット通信料金が一定額で収まるプラン(パケット定額制プラン)を選んだ場合も、その対象外となる通信に注意が必要です。

- 携帯電話やスマートフォンでウェブサイトを開いたり、ウェブサイトから音楽ファイルをダウンロードしたり、電子メールを送受信する場合にはパケット通信料が発生しますが、次のような場合に特に注意が必要です。
 - 音楽ファイル、動画、ゲームソフト等データ量が多いアプリケーション等をダウンロードする場合
 - 通常のパソコン向けのウェブページ(フルブラウザ)を開覧する場合
 - パソコン等に携帯電話を接続してインターネット接続を行う場合
 - 海外でインターネットへ接続する場合
- スマートフォンでは、アプリケーションの利用や自動更新等により、ご自身では通信をしているつもりがなくても予期せぬパケット通信料が発生する場合があります。



Q11 パケット通信料金が高額となるのを防止するためには、どのような対策が必要なの？

A11  契約時にパケット通信に関する説明を受けることや、携帯電話事業者のカタログ、ホームページなどで確認することが必要です。

次のような点について、確認する必要があります。

- パケット定額制プランの利用
- パケット定額制プランの対象外となるサービス
- パケット通信料金が一定額を超えた場合に、利用者に通知されるサービスや利用が制限されるサービス
- ファイルのサイズなどを参考に、ファイルをダウンロードする場合のパケット通信料金(なお、ゲームサイト等では、ゲームのコンテンツ料金は無料でも、パケット通信料金は別途発生するので注意が必要です。)
- 海外において携帯電話やスマートフォンを利用される際の渡航先における使用条件



Q12 携帯電話やスマートフォンで緊急地震速報が受信できると聞きましたが、本当なの？


A12  機種によっては受信できます。

気象庁が発表する緊急地震速報は、テレビ・ラジオ、防災行政無線、専用受信端末の他、携帯電話やスマートフォンでも見聞きすることができる機種があります。

- 通話中やメール送受信中には受信することができません。
- また、スマートフォンの場合、アプリケーションのダウンロードが別途必要な場合があります。受信設定の詳細はお使いの電気通信事業者にご確認ください。



Q13 災害時や通信混雑時に携帯電話を使うには、どんな点に注意が必要なの？

A13  緊急時以外は通話を控え、災害用伝言サービスや電子メールを利用するよう心掛けましょう。

p28 Q33 参照

災害時などには、本当に必要な通信を確保するため、音声通話の規制を行うことがあります。緊急を要する場合以外の通話は控え、災害用伝言サービスや電子メールを利用するよう心掛けましょう。

- 利用者が一斉に電話を掛けることが予想される場合、電気通信事業者では、一定時間音声通話の利用を制限することがあります。これにより、通信網の障害を回避し、緊急通報などの通話を可能とすることができます。
- 通話の集中が予め予想される災害時や年末年始などは、電話の利用を控え、災害用伝言サービスや電子メールを利用するようにしてください。また、緊急時の連絡手段については、家庭や職場において日頃から確認を行っておくことも重要です。




Q14 携帯電話が故障したので修理に出したところ、水濡れが原因だと言われました。水に濡らした覚えはないのに…。

A14  携帯電話やスマートフォンは精密機械です。取扱いには注意しましょう。

携帯電話は、精密機械なので湿気に敏感です。携帯電話を胸ポケットなどに入れている場合には、汗や体温による湿気が発生することがあります。また、スマートフォンの液晶は割れやすい上、機能が高度化しているため、水濡れや落下等の衝撃によって故障につながるおそれがあります。取扱いには十分注意しましょう。



Q15 携帯電話やスマートフォンのゲームサイト(ゲームアプリ)を利用するためには、どのような点に注意が必要なの？

A15  料金についてきちんと確認するようにしましょう。

- 携帯電話のゲームサイトやスマートフォンのゲームアプリには、ゲーム自体は「無料」であっても、ゲーム内の自分の分身を飾るアイテムやゲームを有利に進めるための特別なアイテムは、「有料」となっている場合があります。また、サイトの利用にはパケット通信料が発生します。利用の際には、これらについてきちんと確認するようにしましょう。また、未成年者が利用する際には、親権者に確認するようにしましょう。
- 有料のゲームサイトによっては、アイテム課金などの利用金額に上限を設定することが可能な場合があります。気が付かないうちに高額な利用料となることを防ぐために有効な手段です。



ゲーム自体は無料でもゲーム内のアイテムは有料の場合があります

Q16 中古の携帯電話端末やスマートフォンを**売買**したいのですが、何か注意する点はあるの？

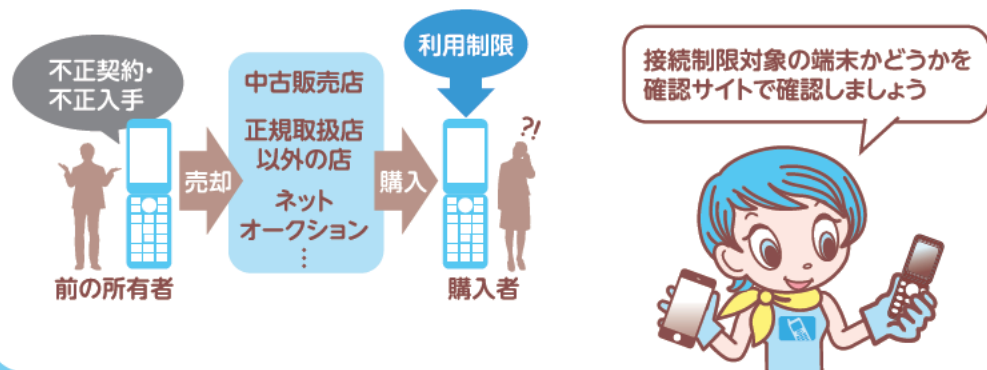
A16



一部の携帯電話事業者では、通話・通信サービスが利用できないように**制限**をかけることがあります。また、自分が携帯電話事業者と契約していて、通話することができる携帯電話端末を他人に譲渡する場合は、親族等に譲渡する場合を除いて、あらかじめ**携帯電話事業者の承諾**が必要です。



- 盗難や契約時における本人確認書類の偽造等により、不正に入手された携帯電話端末の一部が中古市場に流通している事実があります。このため、一部の携帯電話事業者では、現在の利用者としては不正な方法で入手していない携帯電話端末であっても、盗難や本人確認書類の偽造等により不正に入手された携帯電話端末であることが明らかになった場合、通話・通信サービスが利用できないように接続制限をかけることがあります。
- 携帯電話事業者などの販売店以外(ネットオークションなど)で携帯電話端末を購入する場合には、接続制限対象の端末かどうかを携帯電話会社が開設している確認サイトで確認してから購入しましょう。
- 自分が携帯電話事業者と契約していて、通話することができる携帯電話端末を他人に譲渡する場合は、親族等に譲渡する場合を除いて、あらかじめ携帯電話事業者の承諾を得なければなりません。携帯電話事業者の承諾を得ずに、業として有償で譲渡すると処罰されます。勧誘や広告行為についても、同様に処罰されますのでご注意ください。



Q17 迷惑メールを受信しないようにするためにはどうしたらいいの？

A17



迷惑メールを受信しないようにするための基本の対処法

- ① **アドレスを安易に公表しない**
- ② **不用意に同意(登録)しない**
- ③ **推測されにくいアドレスを使う**を守りましょう。

また、携帯電話事業者などが提供する迷惑メールフィルタサービスを利用することも有効です。



- 迷惑メール送信者は、様々な手段を講じてあなたの大切なアドレスを入手しようとしています。迷惑メールを受信しないようにするために次の基本の対処法を守り、アドレスを知られないようにしましょう。

1 アドレスを安易に公表しない

あなたのアドレスをホームページ、ブログ、SNSなどインターネット上に安易に公表すると、アドレス収集ソフト等により迷惑メール送信者にアドレスを収集される危険があります。アドレスの公表には十分に注意しましょう。

2 不用意に同意(登録)しない

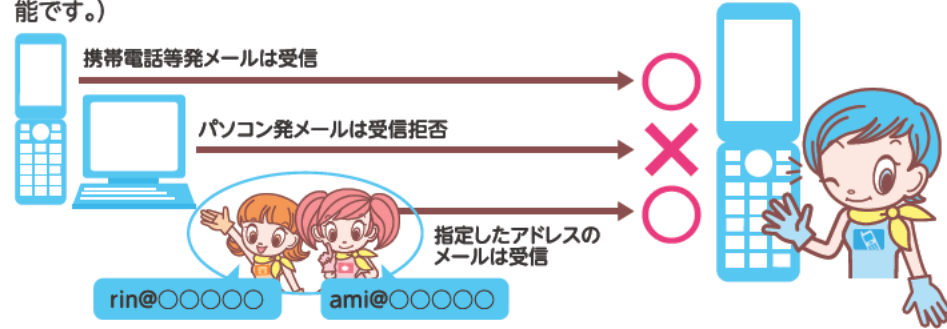
インターネット上には、アドレスの収集を目的とするいわゆる「おとりサイト」があります。懸賞サイト、占いサイトなど、様々なサービスの無償提供を装って利用登録時にアドレスを入力させる手口です。サイト運営者がよくわからないなど、少しでもサイトの利用に不安を感じた場合は、サイトの利用に同意(登録)しないようにしましょう。

3 推測されにくいアドレスを使う

迷惑メール送信者は、アドレスに使われそうな文字を推測してメールを送信することがあります。短くてわかりやすいアドレスは、友人に教えたりする際に楽ですが、その分迷惑メール送信者にアドレスを推測される危険が高まります。英字と数字を組み合わせ、さらに文字数も多くして推測されにくいアドレスを使いましょう。

指定したドメインやアドレスからのメールのみ受信するように設定する。

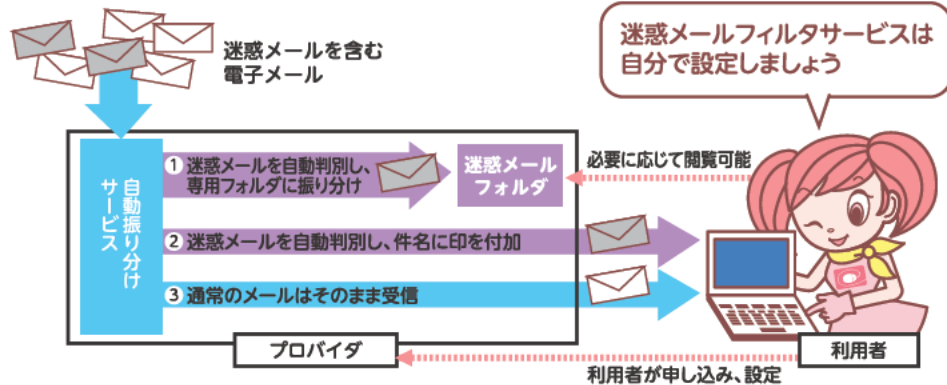
迷惑メール送信業者は、パソコンから大量に送信するのが通例です。そこで、携帯電話を利用している場合は、パソコン発の迷惑メールをブロックするため、携帯電話事業者のドメインから送信されるメールのみ受信するなどの「ドメイン指定受信」機能を活用することも有効な対策となります。(なお、この場合、パソコン発のメールであっても、受信したいメールがある場合は、事前にその特定のアドレス等を受信するよう設定しておけば、受信することが可能です。)



迷惑メールフィルタサービスを利用する。

携帯電話事業者やプロバイダでは、迷惑メールと思われる受信メールを自動的に判別して振り分けたり、件名に迷惑メールと分かる印を付けるなどのサービス(迷惑メールフィルタサービス)を提供したりしていることがあります。迷惑メールを受信しないためには、そういったサービスを利用することも有効な対策の1つです。

迷惑メールフィルタサービスは、基本的に利用する側が設定して初めて有効化できるようになっています。利用している事業者の提供するサービスを確認して、自分で設定を行うことが大切です。



Q18 身に覚えのないメールを受信してしまった場合には、どうすればいいの?

迷惑メールを受信した場合の基本の対処法

- A18**
- ①メールを開かない
 - ②メールに記載されたURLをクリックしない
 - ③個人情報を入力しないを守りましょう。



●迷惑メールを受信しないように注意していても、様々なきっかけで、あなたのアドレスが迷惑メール送信業者に渡ってしまう可能性があります。迷惑メールフィルタを使用しても、迷惑メールがすり抜けてくることもあります。迷惑メールを受信した場合における次の基本の対処法を守り、迷惑メールからつながる第2、第3のトラブルを未然に防ぐことが大切です。

- ① メールを開かない**
迷惑メールや迷惑メールに添付されているファイルを開いてしまうと、ウイルス感染や望まない画像などが表示される恐れがあります。心当たりがないアドレスから送信されたメールは開かずそのまま削除しましょう。
- ② メールに記載されたURLをクリックしない**
迷惑メールに記載されているURL(リンク先)をクリックしないようにしましょう。安易にURLをクリックすると、サイトの運営者からサイトの閲覧料や利用料と称して不当な料金請求などを受けるきっかけになります。
- ③ 個人情報を入力しない**
迷惑メールの中には、有名企業を装った偽サイトへ誘導し、IDやパスワードなどの個人情報の入力を要求する、いわゆる「フィッシングメール」もあります。個人情報を要求する怪しいメールを受けとった場合は、安易に個人情報を入力するのではなく、直接利用会社に問い合わせを行うなどの確認をしましょう。

●また、迷惑メール相談センターでは、迷惑メールに関する情報提供を受け付けています。迷惑メールを受信された場合は次のアドレスに転送してください。

転送先アドレス
meiwaku@dekyo.or.jp

※携帯電話から転送する場合は、本文の文頭に「受信月日」「送信者アドレス(Fromアドレス)」を追加記載してください。

Q19 フィルタリングってなに?

A19



出会い系サイト、アダルトサイト等、青少年に見せたくないサイトの閲覧を制限する機能のことです。



フィルタリングは、違法・有害なサイトを見ることができないようにするばかりでなく、悪質・違法なサイトにアクセスすることによって発生するトラブル(不当な高額請求、迷惑メールの受信等)からの回避効果もあるため、子供たちをインターネットを通じたトラブルから保護する有効な手段でもあります。

フィルタリングの方式としては、①ホワイトリスト方式、②ブラックリスト方式があり、お子さんの成長にあわせて適切な方式を選択することが重要です。

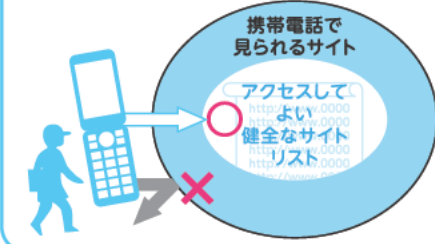
- ①**ホワイトリスト方式**:子どもにとって安全で有益と思われる、一定の基準を満たしたサイトのみアクセス可能で、それ以外のサイトへのアクセスを制限する方式
- ②**ブラックリスト方式**:原則すべてのサイトにアクセス可能ですが、出会い系やギャンブル等、子供に有害と思われる特定のサイトへのアクセスだけを制限する方式

有害サイトから子供たちを守りましょう



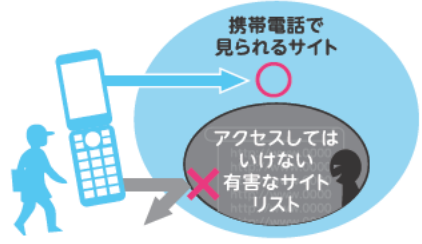
ホワイトリスト方式

健全なサイトのみをリスト化し、それ以外は見られないようにする方式



ブラックリスト方式

有害なサイトをリスト化し、それらを見せないようにする方式



Q20 フィルタリングを利用するには、どのような方法がありますか。

A20



市販のフィルタリングソフトをインストールする方法や、フィルタリングサービスを利用する方法があります。



パソコンの場合、市販のフィルタリングソフトをインストールする方法や、プロバイダが提供しているフィルタリングサービスを利用する方法があります。また、従来の携帯電話・PHSの場合は、携帯電話各社がフィルタリングサービスを提供(無料)しています。なお、スマートフォンについては、フィルタリングサービスを利用するだけでなく、フィルタリングソフトをインストールする方法もあります。

- 「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」(平成21年4月1日施行)に基づき、青少年が使用する携帯電話・PHSの契約時には、親権者からフィルタリングサービスを不要とする申出がない限り、フィルタリングサービスが設定されます。また、親権者は、青少年(18歳未満の者)に使用させる携帯電話の契約時に、使用者が青少年であることを携帯電話各社に申告する義務があります。
- スマートフォンは従来の携帯電話と異なり、多くのアプリをダウンロードできるほか、無線LANによってインターネットに接続できます。これらについても青少年にとって有害な情報の閲覧を制限するためにアプリの利用を制限するソフトや、無線LANの機能を制限するソフトなどが提供されています。

フィルタリング紹介サイト

総務省「フィルタリング(有害サイトアクセス制限サービス)をご存知ですか?」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/filtering.html

(社)電気通信事業者協会 ホームページ「有害サイトアクセス制限サービス」
<http://www.tca.or.jp/mobile/filtering.html>

(財)インターネット協会ホームページ「フィルタリング、知っていますか?」
<http://www.iajapan.org/rating/>

携帯電話各社におけるフィルタリングサービスのお問い合わせ先 <2012年1月現在>

NTTドコモ	ドコモの携帯電話から	局番なし151(無料)
	一般電話から	0120-800-000(無料)
au	auの携帯電話から	局番なし157(無料)
	一般電話から	0077-7-111(無料)
ソフトバンクモバイル	ソフトバンクの携帯電話から	局番なし157(無料)
	一般電話から	0800-919-0157(無料)
ウィルコム	ウィルコムのPHSから	局番なし116(無料)
	一般電話から	0120-921-156(無料)
イー・モバイル	イー・モバイルの携帯電話から	局番なし157(無料)
	一般電話から	0120-736-157(無料)

Q21 携帯電話のフィルタリングサービスを設定すると、コミュニティサイト*等にも一律**アクセスできなくなり**、使いにくいと聞きましたが、本当なの？

※同じ興味や関心を持つ者同士が、掲示板等を利用して情報を交換・共有することができるサイト

A21 第三者機関*が認定したサイトについては、**現在、携帯電話事業者が提供するフィルタリングサービスで閲覧することが可能となっています。**

一部の携帯電話事業者では、閲覧制限の対象となっているサイトについて、保護者が閲覧可能なサイトを個別に設定できる機能(いわゆる「カスタマイズ機能」)を提供しており、この機能を利用すれば、お子さんの成長やご家庭の方針に合わせて閲覧可能な範囲を設定することができます。

※**モバイルコンテンツ審査・運用監視機構(EMA)** 有害サイトから子供を守る!
青少年を違法・有害情報から保護し、健全なモバイルコンテンツの発展を促進することを目的として設立された第三者機関です。現在の認定サイトについては、こちらをご覧ください。

PC <http://www.ema.or.jp/ema.html>
携帯 <http://www.ema.or.jp/m/>



Q22 携帯電話の**番号ポータビリティ**とはどのようなサービスなの？

A22 携帯電話の利用者が**携帯電話会社を変更**した場合に**電話番号はそのまま**で変更後の携帯電話会社のサービスを利用できるサービスです。



Q23 利用の際の**注意点**はあるの？

A23 携帯電話の番号ポータビリティを実施すると、**変更前の携帯電話会社との契約は解除(解約)となり、変更後の携帯電話会社と新たに契約(新規契約)することとなります。**



以下のような点に気をつけましょう。

- ①090・080の電話番号であっても、衛星船舶電話サービス及び衛星携帯電話サービス、データ通信専用サービス、新規契約の受付を停止している場合など、携帯電話の番号ポータビリティが利用できない場合があります。
- ②現在契約している携帯電話会社が発行したメールアドレスは引継ぎできません。
- ③現在契約している携帯電話会社が提供しているサービス(料金プラン・割引サービス等)は解約とともに終了となります。
- ④コンテンツプロバイダが提供しているコンテンツや電子マネー等は引継ぎできない場合があります。
- ⑤年間契約等の割引サービスを契約している場合は、解約に伴い、別途費用が発生する場合があります。
- ⑥変更後の携帯電話会社から発売されている携帯電話端末が必要になります。
- ⑦番号ポータビリティによって携帯電話会社を変更した場合、固定電話から携帯電話への通話料金が変化する場合があります。

総務省「携帯電話の番号ポータビリティ広報サイト」
http://www.soumu.go.jp/joho_tsusin/mnp/index.html

Q24 携帯電話不正利用防止法って
どのような法律なの？

A24



携帯電話を契約するときの本人確認の義務付けや、携帯電話やSIMカードを無断で譲渡すること等を禁止する法律です。



携帯電話不正利用防止法^{※1}は、携帯電話事業者^{※2}及び携帯電話のレンタル業者に対して契約時・譲渡時の本人確認等を義務付けるとともに、携帯電話の無断譲渡の禁止等を内容としています。携帯電話の契約をする際には店頭で本人確認を求められます^{※3}。

※1 正式には「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信業務の不正な利用の防止に関する法律」といいます。

※2 PHS事業者も含まれます。

※3 データ通信専用端末の場合を除きます。

主な内容

- 携帯電話事業者は、契約時・譲渡時に契約者及び譲受人の本人確認を行わなければなりません。
- 自己名義の携帯電話等を携帯電話事業者に無断で譲渡してはいけません。
- 他人名義の携帯電話等を譲渡したり、譲り受けたりしてはいけません。
- 携帯電話のレンタル業を営む場合は、契約者の本人確認を行わなければなりません。
- 警察から携帯電話等が犯罪に利用されている旨の通知を受けた場合、携帯電話事業者は契約者の確認を行うことができます。
- 携帯電話事業者は、契約者が確認に応じない場合には役務の提供を拒むことができます。

Q25 携帯電話を契約する際、または借りる際の
本人確認はどのように行うの？

A25



免許証やパスポート等、顔写真付きの公的身分証の提示が求められます。



本人確認の際は、原則として免許証、パスポートといった顔写真付きの公的身分証の提示を求められることになります。具体的には、各携帯電話事業者にお問い合わせください。

総務省 携帯電話不正利用防止法のページ

http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/050526_1.html

Q26

インターネット上で違法・有害情報を発見
した場合には、どうしたらいいの？

A26

「インターネット・ホットラインセンター」か、
警察に通報してください。



インターネット上で違法な情報を発見した場合には、「インターネット・ホットラインセンター」か、警察に通報してください。公序良俗に反するような有害情報を見つけた場合には、「インターネット・ホットラインセンター」へ情報提供してください。

なお、違法・有害情報が掲載されているサーバや電子掲示板の管理者に情報提供する方法も考えられます。

● インターネット・ホットラインセンターは、インターネット利用者から違法・有害情報に関する情報提供を受け付け、一定の基準に従って情報を選別した上で、警察への情報提供、電子掲示板の管理者等への送信防止措置依頼等を行う民間団体です。詳しくは、ホームページをご覧ください。

インターネット・ホットラインセンター

<http://www.internethotline.jp/>

● なお、サーバや電子掲示板の管理者が誰かわからないときは、.jpdメインの場合には(株)日本レジストリサービス、.comや.netドメインの場合には国際組織INTERNICの提供するWhoisサービスを利用することで、連絡先を調べることができます。

(株)日本レジストリサービス Whois
<http://whois.jp.rs.jp/>

INTERNIC Whois
<http://www.internic.net/whois.html>

Q27

インターネット上で自分の権利を侵害するよう
な書き込みを発見した場合には、どうしたらいいの？

A27

本人からサイトの管理者等に対して
削除の要求をすることが可能です。



ご自身の権利を侵害するような書き込みがあった場合には、プロバイダ責任制限法[※]や名誉棄損・プライバシー関係ガイドライン等に基づき、本人からサイトの管理者等に対して削除の要求をすることが可能です。[※]「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報開示に関する法律」

● 具体的な手続き等については、以下をご覧ください。

プロバイダ責任制限法 関連情報webサイト
<http://www.isplaw.jp/>

Q28 フィッシングってなに?

A28



金融機関等を装い、銀行口座番号、クレジットカード番号、暗証番号、IDやパスワードといった個人情報を巧みに詐取する行為です。



フィッシング (Phishing) とは、クレジットカード会社や銀行、オンラインショッピング事業者、オークション事業者などを装った電子メールを不特定多数に送り、偽のホームページにアクセスするよう仕向け、銀行口座番号、クレジットカード番号、暗証番号、IDやパスワードといった個人情報を巧みに詐取する行為です。

金融機関等が個人情報をメールで尋ねるようなことはほとんどありませんが、もし、個人情報を入力させるようなメールを受信した場合は、メール本文にあるリンクはクリックせずに、金融機関等の正規のホームページを確認するなど十分注意して対応してください。

また、最近はセキュリティの脆弱性を利用し、正しいホームページアドレスを入力しても偽のホームページに自動的につながるようにして、個人情報を入力させようとするファームング (Pharming) と呼ばれる新たな手口も出現していますので、注意が必要です。

- フィッシング対策に対する政府の取組

警察庁「フィッシング110番」

<http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm>

フィッシング対策協議会

<http://www.antiphishing.jp>



Q29

コンピュータウイルスへの感染や第三者の不正な侵入 (不正アクセス) といった、インターネット上の危険からコンピュータを守るためには、どのような対策をすればいいの?



A29

基本となる情報セキュリティ対策には、以下の3つがあります。

① ソフトウェアの更新 (最新のセキュリティパッチの適用)

Webブラウザや電子メールソフト、OSでは、情報セキュリティ上の問題を解決するための修正プログラムが、メーカーから提供されることがあります。これらの修正プログラムを定期的に適用して、できる限りソフトウェアを最新の状態に保つように心がける必要があります。

② ウイルス対策サービス・ソフトの導入


最近のコンピュータウイルスは、電子メールやホームページを見ただけで感染するウイルスばかりではなく、勝手にインターネットを通じて感染するタイプのウイルスも出現してきています。ウイルスに感染しないようにするためには、ウイルス対策サービス・ソフトを導入することが有効です。

③ パーソナルファイアウォール・ブロードバンドルータの利用

コンピュータへの不正アクセスを防ぐためには、パーソナルファイアウォールというソフトウェアの導入が効果的です。パーソナルファイアウォールを導入すると、クラッカーの不正侵入やウイルスの侵入を防いだり、自分のコンピュータを外部から見えなくしたりすることが可能になります。また、ブロードバンドルータにはファイアウォール機能が内蔵されているため、ブロードバンドルータを設置することでパーソナルファイアウォールを導入した場合と同じ効果を得ることができます。



Q30 スマートフォンにも情報セキュリティ対策が必要だと聞きました。本当なの？

A30  **利用者自身が情報セキュリティ対策を取ることが必要です。**



スマートフォンの一部には、これまでの携帯電話端末と違い、アプリケーションを通じたウイルス感染や不正アクセスなどのおそれがあります。利用者自身が情報セキュリティ対策を取ることが必要です。

スマートフォン情報セキュリティ3か条

- ① **スマートフォンは、OSの更新(アップデート)が必要です。**
古いOSを使っていると、ウイルス感染の危険性が高くなるので、更新の通知が来たら、速やかにインストールしましょう。
- ② **各電気通信事業者やセキュリティソフト提供会社では、スマートフォン向けのセキュリティ対策サービスを提供しています。**
※サービスには有償のものもあります。また、ウイルス定義ファイルのアップデートのためにパケット通信料が必要な場合があります。
- ③ **信頼できるアプリケーション・マーケットからアプリケーションを入手するようにしましょう。また、インストールする際には、アプリケーションの機能や利用条件に注意しましょう。**

● インターネットを利用する際の情報セキュリティ対策については、この他にも利用の際の心構えなどのご留意いただきたい事項があります。これらについては、以下のサイトをご覧ください。

参考にしてね



総務省「国民のための情報セキュリティサイト」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/



Q31 チェーンメールが送られてきました。同じ内容のメールを他人にも送るように書いてありますが、どうしたらいいの？

A31 チェーンメールは受信しても転送せずに**削除し、後は気にしないように**しましょう。



チェーンメールとは、一般的に同じ内容を不特定多数の人に転送するように求める迷惑メールのことです。転送されることを目的としているため、「転送すると幸せになる」、「転送しないと不幸になる」等、さまざまな内容で転送させようとする。しかし、チェーンメールは人の心につけ込み、勝手に転送を押しつけるメールであり、貴方の周囲に悪影響を及ぼすことにもなりかねませんので、絶対に転送してはいけません。チェーンメールを受信した場合は、転送せずに削除し、後は気にしないようにしましょう。

また、どうしても不安になり、無視できないときには、次のサイトにチェーンメール転送用アドレスが書かれていますので、そちらに転送して下さい。

迷惑メール相談センター「チェーンメールの転送先」
<http://www.dekyo.or.jp/soudan/chain/tensou.html>



Q32 災害や停電が起きたとき、どんな点に注意して電話サービスを利用すればいいの？

A32 災害発生時は、音声通話の規制を行うことがあります。停電時は基本的に通話ができなくなります。



災害発生時は、災害関連機関などの本当に必要な通信を確保するため、音声通話の規制を行うことがあります。また、停電時は基本的に通話ができなくなります。不要不急な通話は避けるよう心掛けましょう。

- IP電話※には、警察や消防機関等への緊急通報(110番、119番等)が利用できないもの(050番号で始まる電話の場合)があります。
● 停電時は、商用電源を使用しない電話機などを利用してアナログ電話を利用している場合や公衆電話を除き、基本的に通話ができなくなります。
● 災害発生時は、災害関連機関などの本当に必要な通信を確保するため、音声通話の規制を行うことがあります。

※IP(Internet Protocol)技術を利用した音声電話サービスのことで、次の2種類あります。
①0AB～J型IP電話:アナログ電話と同様の電話番号を用い、高品質な通話や緊急通報の利用が可能です。
②050型IP電話:050で始まる電話番号を用い、低料金での通話が可能ですが、緊急通報が利用できず、アナログ電話に比べ通話品質が低い場合もあります。



Q33 災害用伝言サービス(「災害用伝言ダイヤル」・「災害用伝言板」・「災害用ブロードバンド伝言板」)ってどんなサービスなの？

A33 家族や知人の中で安否確認や避難場所の連絡等を行えるサービスです。



地震や大雨・洪水などの大規模災害が発生すると、大量の電話が被災地に集中するため電話がつながりにくくなる場合があります。このような場合でも、家族や知人との間での安否確認や避難場所の連絡等を行えるよう電気通信事業者が提供しているサービスです。

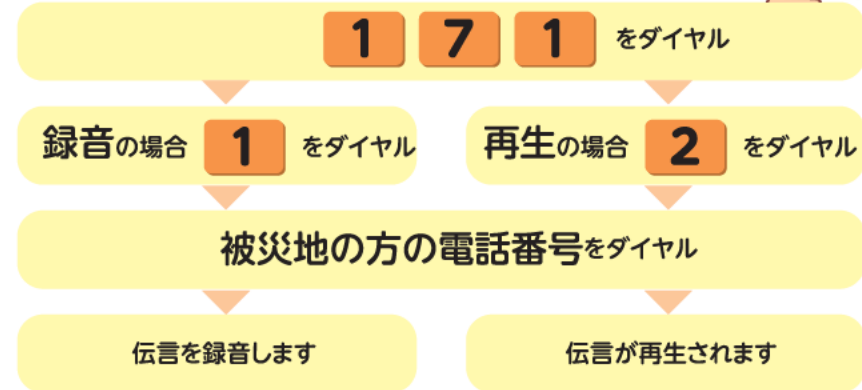
※災害が発生した際に、開設されるサービスです(ただし、体験利用出来る期間があります)。

災害用伝言ダイヤル

自宅や勤務先の固定電話、公衆電話、携帯電話・PHSや一部のIP電話から「171」番に電話することで、伝言を録音・再生することができます。



操作手順



◆災害用伝言ダイヤルでは、災害発生に備えて利用方法を体験利用できる機会を設けています。

体験利用提供日 毎月1日及び15日、正月3日、防災週間(8/30~9/5)、防災とボランティア週間(1/15~1/21) ※伝言の録音・再生時に通話料が発生します。

災害用伝言板

携帯電話・PHSによるインターネット接続サービスのトップ画面に表示されるリンクからアクセスすることで、伝言を登録・確認できます。



操作手順

アクセス方法

- パソコン等から利用する場合は、下記のURLをご利用ください。
- docomo** <http://dengon.docomo.ne.jp/top.cgi>
 - au** <http://dengon.ezweb.ne.jp/>
 - SoftBank** <http://dengon.softbank.ne.jp/>
 - WILLCOM** <http://dengon.willcom-inc.com/>
 - EM** <http://dengon.emnet.ne.jp/>

1 トップメニューから災害用伝言板を選びます。

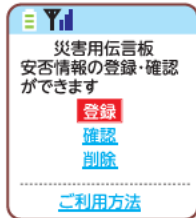
▶ 災害用伝言板



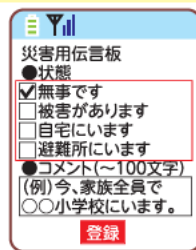
伝言を登録するとき ※各社で表示方法が若干異なります。

1 「災害用伝言板」メニューから登録を選択

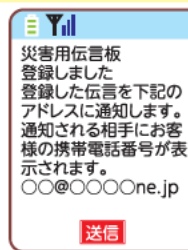
▶ 登録



2 伝言を選択 (各社100字前後のコメントが書き込めます)



3 伝言板登録完了



伝言を確認するとき ※各社で表示方法が若干異なります。

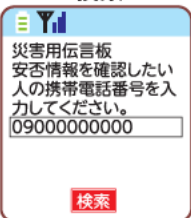
1 「災害用伝言板」メニューから確認を選択

▶ 確認



2 伝言板確認

▶ 検索

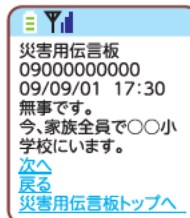


3 伝言板登録結果表示

▶ 結果表示



4 伝言表示



災害用ブロードバンド伝言板

「<https://www.web171.jp/>」にアクセスすることで、音声や映像を登録・確認できます。



Q34 ユニバーサルサービス(基礎的電気通信役務)ってどんなサービスなの?



A34 電気通信事業法により、「日本全国で提供が確保されるべき」と規定されているサービスです。

加入電話の基本料や、社会生活上の安全及び戸外での最低限の通信手段を確保する観点から設置されている第一種公衆電話、さらに特例料金となる離島通話及び緊急通報(110番、118番、119番)がこれに当たります。

Q35 ユニバーサルサービス料金を支払うのはなぜ?



A35 ユニバーサルサービスの確保に必要な費用が不足しているからです。

携帯電話やIP電話の普及及び電話サービスの競争の進展等で、ユニバーサルサービスの確保に必要な費用が不足しています。このままでは、NTT東日本・西日本だけでユニバーサルサービスを維持することができなくなるため、NTT東日本・西日本のユニバーサルサービス提供設備と接続等することによって受益する固定電話、携帯電話、IP電話等の電話会社でもその費用を応分に負担し、全体で支えていくこととなりました。

多くの電話会社では、ユニバーサルサービス料金として、利用者にもご負担をお願いしています。

総務省「電話のユニバーサルサービス制度」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/universalservice/

(社)電気通信事業者協会「ユニバーサルサービス支援業務」
<http://www.tca.or.jp/universalservice/>

「加入電話」「公衆電話」
「緊急通報(110番、118番、119番)」を
全国どこでも公平に利用できるよう
みんなで支える仕組みになっています

