



迷惑メール対策

迷惑メールを受信しないようにするには、メールアドレス提供事業者の迷惑メールフィルターを使う方法とセキュリティソフトやアプリを利用する方法があります。

各携帯電話事業者やプロバイダの多くは無料で迷惑メールフィルターを提供していますので、利用スタイルにあわせて自分の環境にあった設定をしましょう。

キャリアメール

2024年12月現在



迷惑メールフィルター
@docomo.ne.jp

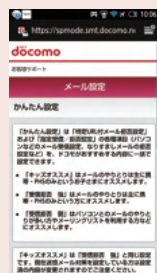


My docomoへ
ログインして
設定

おすすめ：「かんたん設定」

「携帯・PHS／パソコンなどのメール設定」・「特定URL付メール拒否設定」を、ドコモがオススメする設定値に一括で変更することができます。
2024年10月より、フィッシング詐欺の可能性のある不審なメールについて警告を表示する「なりすましメールの警告表示機能」が導入されました。

設定手順：迷惑メール対策のかんたん設定
https://www.docomo.ne.jp/info/spam_mail/spmode/easy_setup/index.html



迷惑メールフィルター
@au.com／@ezweb.ne.jp

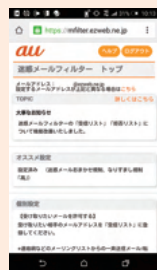


My auへ
ログインして
設定

おすすめ：「オススメ設定」

迷惑メールに多く見られる「なりすまし」メールや迷惑メールの疑いのあるメールをブロックします。

設定手順：オススメ設定
<https://www.au.com/support/service/mobile/trouble/mail/email/filter/recommend/>



迷惑メールフィルター
@softbank.ne.jp/
@i.softbank.jp



My SoftBankへ
ログインして
設定

おすすめ：「迷惑メールフィルター」

なりすましメールや、未承諾広告メール、悪意のあるウェブサイトへ誘導するような迷惑メールを受け取らないように設定する方法です。

蓄積されたスパム（迷惑メール）データベースをもとにメールの内容を機械的に判断し、スパムと判断されたメールの受信をブロックします。

設定手順：迷惑メールフィルター
<https://www.softbank.jp/mobile/support/mail/antispam/email-i-spammailfilter/>





迷惑メールフィルター
@ymobile.ne.jp



My Y!mobileへ
ログインして
設定

おすすめ：「迷惑メールフィルター」

迷惑メールデータベースを元に迷惑メールの受信を拒否することができます。また、メールの件名欄に「! 広告!」などが記載されているメールを未承諾広告メールとし受信を拒否することもできます。

設定手順：迷惑メール対策
https://www.ymobile.jp/support/relief/trouble_mail/



迷惑メールフィルター
@uqmobile.jp

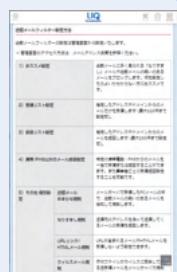


My UQ mobile
へログインして
設定

おすすめ：「おススメ設定」

迷惑メールに多く見られる「なりすまし」メールや迷惑メールの疑いのあるメールをブロックします。何を設定したらよいか分からない方にオススメです。

設定手順：メールサービス設定方法/迷惑メールフィルター
<https://www.uqwimax.jp/mobile/support/guide/mail/>



フィルター設定機能
@rakumail.jp



Rakuten Linkア
プリより設定可
能

おすすめ：「おすすめフィルター設定」

あらかじめ設定された迷惑メールフィルターの各種設定を「オフ・標準・強」から選んで設定できます。

※デフォルトはおすすめフィルター設定（強）になります。
設定手順：おすすめのメールフィルターを設定する
https://network.mobile.rakuten.co.jp/guide/rakumail/filter_2/#setting01



※操作方法や詳細は56ページの各窓口からお問い合わせください。

プロバイダメール・フリーメール

プロバイダ・フリーメールのメールアドレスで受信する迷惑メール対策としては、各種サービスが提供する迷惑メールフィルターを利用しましょう。一部をのぞき、無料で提供されています。メールサーバー上で迷惑メール判定を行うため、受信トレイに迷惑メールが届きにくくなります。詳しくは各種サービス窓口にお問い合わせください。



迷惑SMS対策

迷惑SMSを受信しないように、携帯電話事業者が提供している迷惑SMSフィルターを利用しましょう。不審なSMSや架空請求SMSなどを事前に届かないようにブロック設定することができます。自分の利用スタイルにあわせて選択して設定しましょう。

携帯会社のSMS(ショートメッセージ・Cメール)2024年12月現在

docomo



My docomoへ
ログインして
設定

5G (ahamo)
も同様

- ・ **SMS一括拒否**：すべてのSMSを拒否
- ・ **危険SMS拒否**：フィッシングSMSと判定されたSMSを拒否
- ・ **非通知SMS拒否**：非通知のSMSを拒否
- ・ **国際SMS拒否**：海外事業者から送信されたSMSを拒否
- ・ **国内他事業者SMS拒否**：ドコモ以外の事業者からのSMSを拒否
- ・ **個別番号拒否**：個別に指定した電話番号からのSMSを拒否
- ・ **個別番号受信**：個別に指定した電話番号からのSMSのみを受信
- ・ **なりすましメールの警告表示機能 (2024年10月より提供開始)**：フィッシング詐欺の可能性がある不審なメールに警告を表示

au



**UQ
mobile**



設定の詳細は
各HPをご覧
ください

- ・ **SMS(Cメール) 国内他事業者ブロック機能**：
au、UQ、povo以外の事業者からのSMS(Cメール) を拒否
- ・ **SMS(Cメール) 海外事業者ブロック機能**：
海外事業者から送信されたSMS(Cメール) を拒否
- ・ **SMS(Cメール) オプションの停止**：
すべてのSMS(Cメール) を拒否 (SMS(Cメール) の送信もできなくなります)
- ・ **迷惑SMSブロック**：
迷惑SMSの疑いのあるSMSを自動判定しブロックします。

SoftBank



My SoftBankへ
ログインして
設定

LINEMOも同様

Y!mobile



My Y!mobileへ
ログインして
設定

・なりすましSMSの拒否：

差出人をSoftBankなどになりすましたSMSを拒否

・すべての電話番号、または特定の電話番号から送られてくる
メールを「許可／拒否する」：

すべてのSMSを拒否

・特定の電話番号（SMS）で送られる迷惑メールの拒否設定：

個別に指定した電話番号からのSMSを拒否

・URLリンク付きのSMSを拒否：

携帯電話番号から送られるSMS本文にURLリンクが含まれて
いるSMSを拒否

・迷惑SMSフィルター：

受信したSMSを機械的に迷惑メールかどうか検知し拒否。悪
意あるウェブサイトへ誘導するSMSに有効。

Rakuten Mobile



拒否設定を利用
しない場合は、
Rakuten Linkア
プリより設定可能

・迷惑SMS拒否設定（2024年7月より提供開始）：

フィッシング詐欺対策として、有害なサイトのURLや電話番号
が含まれるSMSを自動で拒否。

※拒否設定については申し込み不要で、自動適用

※操作方法や詳細は56ページの各窓口からお問い合わせください。



セキュリティ対策

●スマートフォンはパソコンと同じ！セキュリティ対策は必須です

スマートフォンの機能はパソコン同等とも言われます。ウイルスや不正アプリでの被害を避けるため、セキュリティ対策を行うことが必要です。

●スマートフォンを狙うウイルス

パソコン同様のセキュリティを！

スマートフォンはパソコンと同じようにOS（基本ソフト）が搭載され、さまざまなアプリをインストールすることができる一方で、セキュリティ対策を怠るとウイルスに感染するおそれがあります。このため、パソコンと同様にセキュリティ対策を行っていくことがとても重要です。

また、ウイルスはインストールしたアプリ内にも仕込まれスマートフォン内で不正行為を働く場合もありますので、不正なアプリのインストールをしないよう注意する必要があります。

ウイルスに感染したらこんな事態も…

- ・アドレス帳や写真、個人情報などの重要な情報が抜き取られてしまう。
- ・抜き取られた情報を使われて、クレジットカードやオンラインの決済サービスを不正利用されてしまう。
- ・SNSやWebサービスのアカウント情報が抜き取られ不正利用されてしまう。
- ・スマートフォンが外部から遠隔操作されて知らない間に迷惑メールの大量送信をされ、迷惑行為を行う加害者となってしまう。
- ・端末に保存したデータが消えてしまう。



●携帯電話事業者が提供するセキュリティサービス

2024年12月現在

NTTドコモ あんしんセキュリティ	・アプリをインストールする際、ウイルスが混入していると検出する ・設定で、定期的にウイルスの検出を行うことができる ・ウェブサイトの安全性を判定して、フィッシングサイトなど危険なサイトへのアクセスを警告しブロックする ・危険なWi-Fiスポットに接続すると、警告を出す
au ウイルスバスター™ for au/ウイルスブ ロック	Android端末を対象に ・ウイルスを検知、侵入をブロックする ・不正サイトへのアクセス規制および警告表示を行う ・決済アプリの保護機能 ・アプリをインストールする際にリアルタイムでセキュリティの脅威をチェックする ・フィッシング詐欺やワンクリック詐欺など危険なWebサイトへのアクセスをブロックする
SoftBank・ ワイモバイル セキュリティOne	・危険サイトチェック 悪意のある詐欺サイトを検知し、警告する ・危険Wi-Fiチェック 危険なWi-Fiへの接続や不正アクセスを検知し、警告する ・迷惑電話チェック 振り込め詐欺などの迷惑電話からの着信時に警告する ・迷惑メッセージチェック 「メッセージSNSアイコン」に届いた迷惑メールを自動で検知し振り分ける
UQ mobile ウイルスバスター モ バイル for UQ mobile	・不正なアプリのダウンロードやインストールをブロックする(不正アプリ対策(ウイルス対策)) ・Webサイトの安全性を判定し、不正アプリの配布元サイトや、フィッシングサイト、不正アプリの情報送信先サイトなどへのアクセスをブロックする(Web脅威対策)
楽天モバイル ノートン™ モバイル セキュリティ	・Web保護：悪質なサイトや詐欺サイトなど、危険なWebサイトへのアクセスの際に警告 ・Wi-Fiセキュリティ：安全でないWi-Fiネットワークに接続の際に警告(Android版) アプリアドバイザー：アプリの危険性を判定し警告(iOS版) デバイスセキュリティ：OSが古くなっているとユーザーに通知し、その影響について警告

被害にあわないための
セキュリティ対策

※サービスの詳細は、ご利用中の携帯電話事業者へお問い合わせください。

●セキュリティベンダーが提供する対策ソフトの利用

セキュリティ対策ソフト提供会社でも、スマートフォン用のセキュリティソフトを発表しています。盗難・紛失対策、Web脅威対策などの機能を搭載しているものもありますので、スマートフォンの機種毎の対応状況を確認して利用するとよいでしょう。





有害サイト・有害アプリ対策

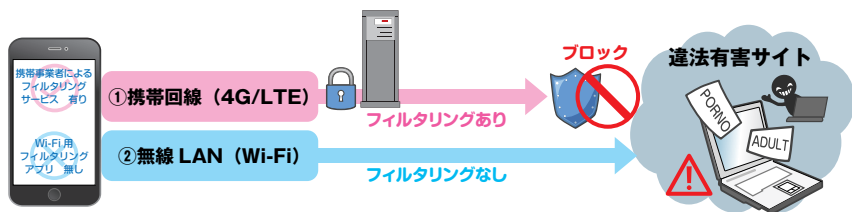
スマートフォンを利用して、いつでも・どこでも膨大なインターネットの情報にアクセスできるようになりました。しかし、インターネット利用で、思いがけず危険な情報へアクセスしてしまいトラブルに巻き込まれる可能性が高くなっています。

特に、スマートフォンの利用が低年齢化し、小学生が利用することめずらしくなくなった現状では、子どもたちが知らないうちに有害な情報へアクセスしてしまう危険性が高くなっています。

詐欺サイトなどの危険なサイトや出会い系・アダルト系などの性的な表現を含むもの、違法情報などを表示させないように、あらかじめフィルタリングを設定しましょう。

フィルタリングの特徴

1. スマートフォンから有害サイトへのアクセスを制限できます
2. アクセスを制限しても閲覧が必要なサイトは個別に許可することができます
3. 一般向け、小学生向け・中学生向けなど、年代や利用スタイルにあわせて設定できます
4. 専用アプリを利用することで、無線LAN（Wi-Fi）利用時にも有害サイトへのアクセス制限ができます



ポイント

- Wi-fi接続時は、携帯回線のフィルタリングが適用されません。
- スマホ本体へのフィルタリングアプリのインストールが必要です。

●携帯電話事業者が提供するフィルタリングサービス

2024年12月現在

		①Web利用	②Wi-Fi利用	③アプリ利用
NTTドコモ	iPhone※ 2	あんしんフィルターfor docomo ※ 1 ※ 4		端末本体の「機能制限」 設定により制限可能
	Android	あんしんフィルターfor docomo※ 3		
au・ UQ mobile	iPhone※ 2	あんしんフィルターfor au※ 1 ※ 4		端末本体の「機能制限」 設定により制限可能
	Android	あんしんフィルターfor au（Android™）※ 6		
SoftBank・ ワイモバイル	iPhone※ 2	あんしんフィルター※ 1 ※ 5		端末本体の「機能制限」 設定により制限可能
	Android	あんしんフィルター※ 3		
楽天モバイル	iPhone※ 2	あんしんコントロール by i-フィルター※ 5		端末本体の「機能制限」 設定により制限可能
	Android	あんしんコントロール by i-フィルター※ 3		

- ※ 1 iOS端末の場合、フィルタリングアプリの利用と併せて、Safari（標準搭載ブラウザ）を「OFF」
にしておく必要があります。
- ※ 2 携帯電話事業者で回線契約したiPadを含みます。
- ※ 3 AndroidOS 6以上が対象です。
- ※ 4 iOS 9.0以上が対象です。
- ※ 5 iOS 13以上が対象です。
- ※ 6 AndroidOS 5.0以上が対象です。
- ※ サービスの詳細は、各携帯電話事業者へお問い合わせ
ください。



スマホの場合、
3つのフィルタリングが
必要なのね

被害にあわないための
セキュリティ対策

●セキュリティベンダーが提供するフィルタリングサービス

セキュリティベンダーでも、スマートフォン用のセキュリティソフトを提供しています。盗難・紛失対策、Web脅威対策などの機能を搭載しているものもありますので、スマートフォンの機種毎の対応状況を確認して利用するとよいでしょう。

※ サービスの詳細は、各セキュリティベンダーへお問い合わせください。

子どもの安全なスマートフォン利用のために

子どもがスマートフォンを利用する際には、親子で話し合いながら、使う時間、対処の仕方、ルールを守れなかった場合の対応などのルールを決めておきましょう。

【中学生向けルールの例】（スマートフォン利用の注意点チェックリストとしてもご利用ください）

使い方のルール	✓
利用してもいい時間【平日 : ~ : 休日 : ~ : 】	
アプリに使える金額は1ヶ月に_____円までとする	
ルールを守れなかったときは「一時利用停止」する	
トラブルにあったらすぐに保護者が先生に相談する	
有害サイト・迷惑メールのトラブルを防ぐために	✓
Web（Wi-fi利用時も）・メール・アプリの3つのフィルタリングを設定する	
アダルト系や犯罪・違法情報などを掲載している不適切なサイトは利用しない	
不用意に電話番号やメールアドレスを教えない	
知らない人からのメールやメッセージに返信しない	
ネットで知り合った人に誘われても会いに行かない	
迷惑メールやメッセージは開かない、返信しない	
料金請求メールが突然届いてもあわてて支払わない	
誰かに転送を促すチェーンメールやメッセージは無視して転送しない	
SNS（ソーシャルネットワーキングサービス）でのトラブルを予防するために	✓
ネット上に名前や住所など個人情報に関する書き込みをしない	
情報を公開する範囲は友人のみなど「必要最低限」に設定する	
誹謗中傷や犯罪予告、悪ふざけなどは絶対に書き込まない	
ネット上に写真を掲載する時は肖像権や位置情報に注意する	
オリジナルルール	✓
歩きながらや自転車に乗りながらスマートフォンを使わない	

参 考

- ・スマホ・ケータイファミリーガイド on WEB（au）
<http://www.kddi.com/family/rules/>
- ・家族で話そう！お子さまの携帯電話利用のルール（SoftBank）
<https://www.softbank.jp/mobile/support/3g/protect/kids/rule/>

●こんな時どうする？保護者のお悩みにお答えします

子どもから「あのアプリが使えないからフィルタリングを外して！」って言われて困っています。

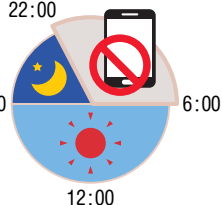
- アプリ起動のフィルタリングを設定したままでも、利用したいアプリがある場合には、そのアプリを個別に起動できるように設定変更することができます。

例えば、フィルタリング設定で起動できなくなっているアプリをどうしても利用したいのであれば、一覧からそのアプリを選んで起動できるようにしてください。

アプリの起動制限を外すと、そのアプリはフィルタリングサービスによる保護がなくなります。制限を外した後は、子どもが安全に使っているか、保護者の方がしっかり見守ってください。

子どもがスマートフォン依存にならないか心配です。 22:00

- フィルタリング機能のカスタマイズで、サイトアクセス可能時間帯の制限やWeb毎に起動可能時間帯の設定をして使い過ぎを防止することができます。



iPhoneで子ども向けの安全なアプリを知りたい！

- App Storeで配信されるアプリには、アプリ毎に対象年齢が設定されています。iPhone本体で「許可するAppのレート設定」を行うことで、まとめて対象年齢外のアプリのダウンロードを制限することができます。対象年齢は4+（4歳以上9歳未満）、9+（9歳以上12歳未満）、12+（12歳以上17歳未満）、17+（17歳以上）から選択できるので、お子様の年代に応じてレートを設定すると、対象外のアプリは表示されないようになります。



「設定」>スクリーンタイム>コンテンツとプライバシーの制限>コンテンツ制限の「App」の順にタップ。許可するAppのレートに対象年齢を選んでください。

例えば、「12+」に設定すると【App Store】から「17+」のレーティングがかけられたアプリはダウンロードすることが出来ません。





迷惑メールは法律違反

● 広告宣伝メールの送信は法律で規制されています

平成14年（2002年）4月に広告宣伝メール送信のルールを定めた「特定電子メールの送信の適正化等に関する法律」（以下、「特定電子メール法」といいます。）が成立し、同年7月1日から施行されました。

その後、メール送信手法の悪質化および巧妙化が進んだことから、平成17年5月（同年11月1日施行）と平成20年6月（同年12月1日施行）に法律の改正が行われ、平成20年の改正では、広告宣伝メールは、原則としてあらかじめ同意した者に対してのみ送信が認められることとなっています。

同意を得て広告宣伝メールを送信する場合でも、次の表示が義務づけられています。（右ページの図を参照してください）

- ① メール本文に、送信者などの氏名又は名称
- ② メール本文に、受信拒否の通知を受けるための電子メールアドレス又はURL
- ③ 受信拒否の通知先の直前又は直後に、受信拒否の通知ができる旨
- ④ 任意の場所に、送信者などの住所
- ⑤ 任意の場所に、苦情・問合せなどを受け付けることができる電話番号・電子メールアドレス又はURL

また、送信者情報を偽って送信することは禁止されています。
詳しい法律のポイントについては以下の資料をご覧ください。



特定電子メールの送信の適正化等に関する法律
のポイント

— 広告宣伝メールに係るオプトイン方式の規制
などについて —



健康サプリが特別価格！

差出人: soushinsya@example.xx
 送信日時: 2018.7.10(Tue) 00:01
 To: 総務次郎[jiro@soumu-syo.xx]
 件名: 健康サプリが特別価格！

【このメールの送信者】
 △△株式会社

<配信停止手続はこちらから↓>
<http://www.example.com/xx/teishi@example.xx>

【製品の販売事業者】
 ☆☆株式会社

<配信停止手続はこちらから↓>
<http://www.jigyosya.example/xx/teishi@jigyosya.xx>

！キャンペーン実施中！
 ☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆
 忙しいあなたに
 健康サプリが特別価格！
 ☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

■商品の購入はこちらから↓
<http://www.kenko/xx/x>

■送信者の住所はこちらに記載↓
<http://jyusyo/example>

■各種問合せはこちらから↓
<http://toiawase/example>

送信者情報(送信に用いた電子メールアドレス、IPアドレス、ドメイン名)を偽って送信することは禁止されています。

✓送信者など(※1)の氏名または名称

✓受信拒否の通知ができる旨
 受信拒否の通知先の直前または直後に表示する必要があります。送信に用いられた電子メールあてに送信することで通知できる場合は、その旨を電子メールの中の受信者が容易に認識できる場所に表示する必要があります。

✓受信拒否の通知を受けるための電子メールアドレスまたはURL(※2)
 URLとする場合は、リンク先において、受信拒否に必要な情報が明確かつ平易に提供され、受信拒否の通知が容易に行うことができるよう、必要な措置が講じられている必要があります。

特定商取引法上の販売業者などと送信者などが異なる場合

✓販売業者などの氏名または名称
 ✓相手方が電子メール広告の提供を受けない旨の意思を表示するための電子メールアドレスまたはURL(※2)

特定商取引法に基づくその他の表示事項はリンク先での表示とすることも可能です。

✓送信者などの住所
 ✓苦情・問合せなどを受け付けることができる電話番号、電子メールアドレス、URL(※2)
 リンク先での表示とすることも可能です。その場合は、表示場所を示す情報を電子メールの中に表示する必要があります。

- ※1 電子メールの送信を委託している場合は、送信者または委託者のうち送信に責任を有するもの
- ※2 ハイパーリンクとすることも可能

★表示義務には一定の例外があります(例えば、受信拒否の対象とならない広告宣伝メールにおいては、受信拒否の通知ができる旨や受信拒否の通知先を表示する必要がないなど)。



詳しくは、総務省のホームページをご覧ください。

https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html

情報提供のお願い

●「特定電子メール法」に違反して 広告宣伝メールを配信すると処罰されます

広告宣伝メールについては、「特定電子メール法」によって「原則としてあらかじめ送信の同意を得た者以外の者への送信禁止」「一定の事項に関する表示義務」「送信者情報を偽った送信の禁止」「送信を拒否した者への送信の禁止」などが定められています。

これらのルールを守っていないメールは違法となり、総務大臣及び内閣総理大臣は、メールの送受信上の障害を防止するため必要があると認める場合、送信者に対しメールの送信方法の改善に関し必要な措置をとるよう命ずることができます。

送信者情報を偽って送信した場合や、送信者が総務大臣及び内閣総理大臣の命令に従わない場合には、1年以下の懲役または100万円以下の罰金（法人の場合は、行為者を罰するほか、法人に対して3000万円以下の罰金）に処せられます。



●違反メールの情報提供にご協力を！

「特定電子メール法」に違反していると思われる迷惑メールを受け取られた場合は、以下の方法で迷惑メール相談センターまで情報提供をお願いします。

ご提供いただきました違反情報につきましては、総務大臣及び内閣総理大臣による違反送信者への措置に活用させていただきます。

注意！

- ※情報提供に際しては、個人情報が必要としないので、氏名・住所・電話番号などの個人情報は入力しないで下さい。
- ※個々の情報や送信者への措置状況などについての照会には対応いたしませんので、あらかじめご了承ください。

法律に違反していると思われるメールの情報提供は、以下のいずれかの方法によりお願いします。送信者情報を偽ったメールの情報提供の際には、ヘッダ情報の添付をお願いします。

メール

モバイルやPCから

メールを転送
送信先アドレスmeiwaku@dekyo.or.jp



ウェブから

フォームへの入力
https://www.dekyo.or.jp/bingo/mail_ihan_meiwakuform/



被害にあわないための
セキュリティ対策

SMS(ショートメッセージサービス)

モバイルから

フォームへの入力
https://www.dekyo.or.jp/bingo/mail_ihan_meiwakuform/

