

第12回 不適正利用対策に関するワーキンググループ 事業者ヒアリングご説明資料

2025年11月21日

楽天モバイル株式会社

当社メールサービス概要

- ✓ 楽天ドメインのメールが利用可能な無料オプションサービス「楽メール」を2022年7月より提供。
- ✓ 楽天モバイル契約者が、Rakuten Linkアプリ内で申込することで利用可能。
- ✓ 楽天モバイル解約後も「楽メール」を継続してご利用可能な「楽メール持ち運び」を提供（税込330円/月）。

「楽メール」サービス概要

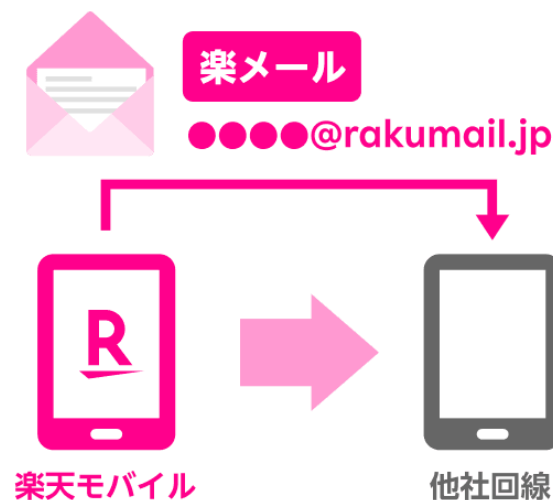
【楽メールの特長】

- 「rakumail.jp」ドメインのメールが利用可能
- Rakuten Linkアプリ内で利用可能
- メールサイズ制限は最大受信50MB・最大送信25MB（ファイルあたり10MB）であり、大容量メールの送受信にも対応



【楽メール持ち運び（税込330円/月）】

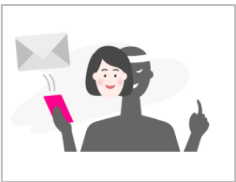
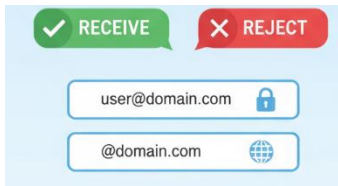
楽天モバイルを解約・譲渡もしくは他の携帯電話会社へ移行後も、「楽メール」を引き続きご利用可能



フィルタリングの実施及びなりすましメール対策

- ✓ なりすましメール、大量送信者からのメール、ウイルスメールを検知し、迷惑メールとしてフィルタリングする機能を提供。なりすましメールへの対策として、受信メールのDMARCレコードを照合することで認証し、ポリシーに基づき隔離・拒否を実施。
- ✓ AIや機械学習の活用等によるフィルタリング精度の一層の向上等に引き続き取り組む。

迷惑メールフィルター機能

メールフィルター				受信・拒否リスト	携帯/Webメール拒否設定
なりすまし●	大量送信者●	ウイルス●	URLリンク		
					
アドレスを偽って送られてくるメールを受信しない(DMARC対応)	大量送信者からのメールを迷惑メールフォルダーに保存	添付ファイルがウイルスに感染しているメールを迷惑メールフォルダーに保存	URLが含まれるメールを迷惑メールフォルダーに保存	受信・拒否したいメールアドレスやドメインを個別設定可能	携帯/Webメールを拒否設定可能

●デフォルトオン

様々な利用者に向けた周知・啓発

- ✓ Webサイト等にて、フィッシングメールや偽SMS、なりすましメール等の様々な不正手口を紹介。
- ✓ 各不正手口の詳細やスマートフォンでの具体的な対策方法等に関する周知・啓発を実施。

Webサイトでの掲載・発信例

【お客さまへの注意喚起】 通信事業者などを装うフィッシング詐欺にご注意ください

- ・身に覚えのないSMSやメールが届いた場合、記載されたリンク先サイトへのアクセスには、十分にご注意ください!
- ・不正アプリのインストールを促される場合がありますので、インストールすることがないよう、十分にご注意ください!

最近、通信事業者や宅配業者などを装った身に覚えのないSMSやメールが届き、本文に記載されているURLにアクセスすると、本物と見分けのつかない不正なサイトが表示され、お客さまのIDやパスワード(暗証番号)の入力を求められるという情報が寄せられています。また、不正なアプリのインストールが求められるケースも確認されています。不正なサイトにIDやパスワードを入力した場合や、不正なアプリをインストールした場合、意図しない第三者による不正な購買や決済につながる恐れがありますので、十分にご注意ください。

当社においても対策を実施しておりますが、お客さまにおかれましても、フィッシング詐欺の被害に遭わないよう、以下の点にご注意ください。

フィッシング被害を防ぐため、お客さまにご注意いただきたいこと

- 高額請求やアカウント停止など、お客さまの不安を煽るような内容の場合、リンク先URLをクリックせずに、普段ご利用されているブックマークやアプリなどを経由し、正規サイトにアクセスしましょう。
- ※SMSやメールの送信元は偽装されている場合がありますのでご注意ください。
- GooglePlayストア(注)など、正規のアプリ配信サイト以外からのアプリをインストールする場合は、十分に注意しましょう。
「提供元不明のアプリ」と表示がされる場合は、インストールを許可しないようにしましょう。
- 生体認証やパスワードレス認証を利用できる場合は、積極的に活用しましょう。パスワードを入力しなければ、悪意ある第三者にそのパスワードが奪い取られることもありません。

なりすましメールの対処方法

個人のお客様 法人のお客様 Language

Rakuten Mobile 900万回線 プラン・製品 通信エリア・店舗 キャンペーン お知らせ・サポート 検索 my 楽天モバイル お申し込み

トップ > お客様サポート > その他 > なりすましメールの対処方法

なりすましメールの対処方法

↓ なりすましメールとは ↓ 「楽メール」のなりすましメールフィルター ↓ なりすましメールを受け取ってしまったら

なりすましメールとは

「なりすましメール」とは、知り合いや有名企業などを装ったフィッシング詐欺メールの一種です。

- 信憑性の高い文章や緊急性の高い文章を使用したり、送信者の身元を詐称することで、メールの内容を確認させようとしています。
- メール内のリンク先から個人情報を入力してしまったり、添付ファイルをダウンロードしたりしてしまうことで、ID・パスワードやクレジットカード番号などを盗まれる可能性があります。

過去に発生したなりすましメールの事例

楽天銀行株式会社 2021/10/26

宛先: 楽天株式会社【重要なお知らせ】

このようなメールを楽天グループから送ることはありません!

- 件名が「楽天株式会社」で、本文が「楽天銀行株式会社」など、複数のサービス名が記載されることはありません。

その他取組状況

- ✓ オールインワンのセキュリティオプション「最強保護」を2025年8月より提供（税込990円/月）。
- ✓ 危険な Web サイトへのアクセスを検知し警告を表示する機能を具備。また、トラブルが発生した際には専用のコミュニケーションセンターによる365日電話サポートにより復旧をサポート。

最強保護

個人情報流出対策



ダークウェブモニタリングで危険を素早く検知

個人情報が売買されるダークウェブ上のWebサイトなどをスキャンして、お客様の個人情報を検知した際に通知

広範囲に及ぶ保護

メールアドレス、電話番号、クレジットカード番号などの幅広い個人データを検知し通知

ウイルス対策



危険なアプリやサイトを警告

悪質なWebサイトやウイルスからスマホを保護。アプリスキャン技術でウイルスや迷惑アプリを検出し、インストール前にブロック

危険なWi-Fiを警告

セキュリティが弱いWi-Fiや個人情報収集を目的とした悪質なWi-Fiに対し、警告を表示

トラブル解決サポート



専用のコミュニケーションセンター

万が一、トラブルが発生した際にも専用のコミュニケーションセンターによる365日電話サポートにより復旧をサポート

クレジットカード不正利用補償

対象のクレジットカード情報がダークウェブ上に流出、不正利用が検知された場合に補償

サイバーリスク補償

スマートフォン利用で発生したサイバー攻撃や情報漏えい等のリスクを補償

Appendix. 最強保護のフィッシングメール対策機能

- ✓ 危険な Web サイトへのアクセスを検知し警告を表示する機能を具備しており、フィッシングメール等に記載された悪質な Web サイトへの遷移を防ぐことが可能。



Rakuten Mobile