

1 検疫メールとは

日常のメール利用において、システム（Microsoft 365）が「迷惑メール」や「詐欺の疑いがある」と判断したメッセージは、安全のために「[検疫](#)」という隔離スペースに一時的に保管されます。メールが隔離されると、ご自身のメールアドレス宛に以下の通知が届きます。

送信元 : guarantine@messaging.microsoft.com
件 名 : 「Microsoft 365 セキュリティ: 検疫にメッセージがあります」

■ 明らかな迷惑メールや詐欺メールの場合

心当たりのないメールであれば、この通知はそのまま無視してください。

（隔離されたメッセージは、一定期間が経過すると自動的に削除されます）

■ 業務や授業に必要なメールが隔離されてしまった場合

隔離されたメールは、ご自身の操作で「受信トレイ」に戻す（復元）ことができます。安全に手続きを行うため、以下の順番で操作を行ってください。

ステップ 1: 本当に安全なメールか中身を確認する

→ [「2.【重要】安全なメールを確認する手順」【P2】へ](#)

ステップ 2:

- メールを受信トレイに戻す。（復元）
- メールに「解放」と記載がある場合

→ [「3.メール文章に「解放」と記載がある場合の手順」【P4】へ](#)

- メールに「リリースの要求」と記載がある場合

→ [「4.メール文章に「リリースの要求」と記載がある場合の手順」【P6】へ](#)

< 検疫メール(例) >



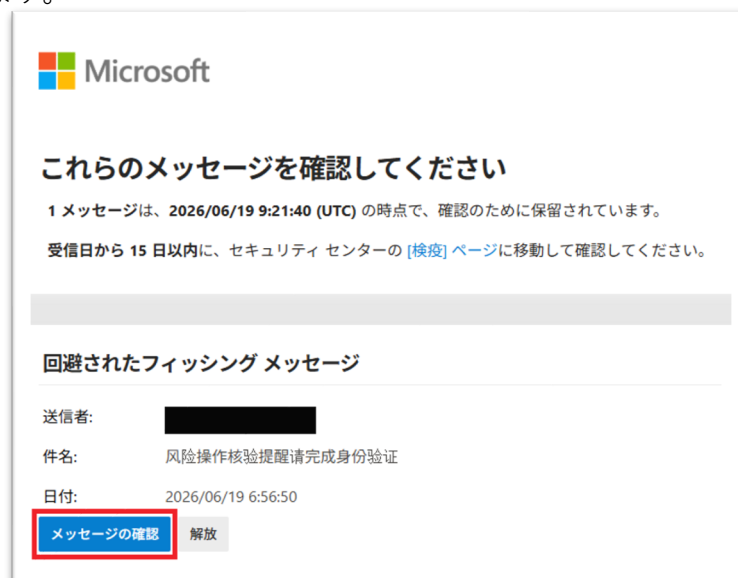
2. 【重要】安全なメールか確認する手順

メールを受信トレイに戻す（解放する）前に、本当に自分にとって必要な安全なメールかどうか、検疫ページ上で中身を確認（プレビュー）することができます。

安全のため、いきなり解放するのではなく、必ず以下の手順に従ってメールの内容確認をおこなったうえで解放するかを判断してください。

【メッセージの確認手順】

1. 届いた通知メール内にある「**メッセージの確認**」をクリックし、検疫ページを開きます。

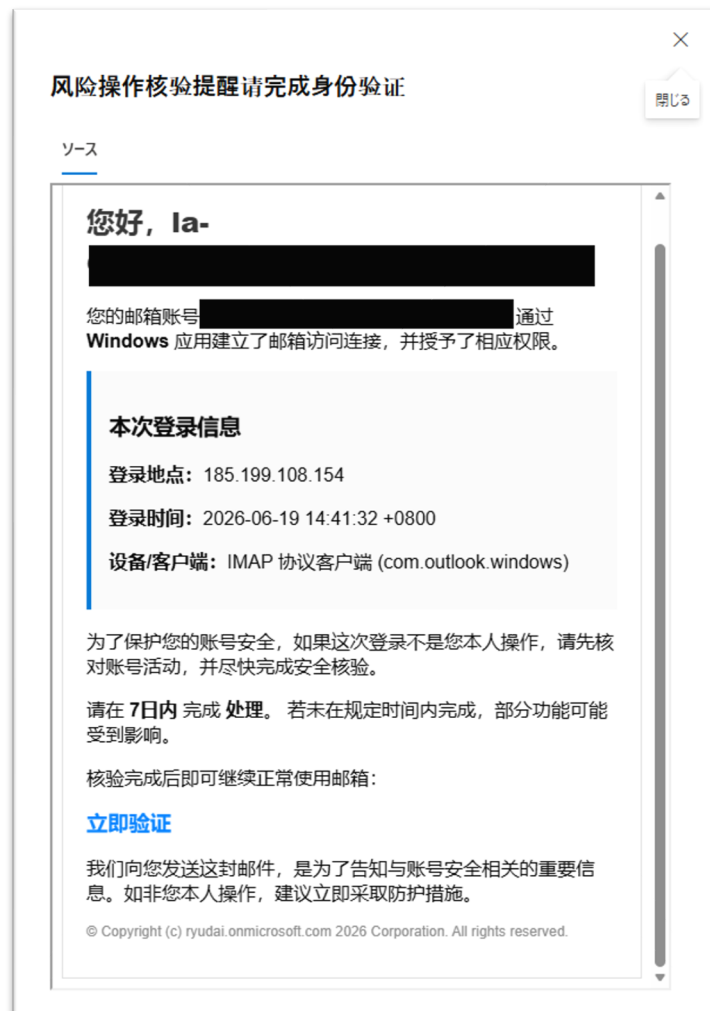


2. 隔離されているメールの一覧から、該当するメールの左側にあるチェックボックス（☐）にチェックを入れ、「**メッセージのプレビュー**」をクリックします。



3. メール本文が表示されます。

差出人のアドレス、件名、内容を読んで、本当に業務や授業に必要なメールかどうか確認してください。



メールの内容が安全で、業務や授業に必要なだと確認できた場合は、受信トレイに戻す操作を行います。お手元の通知メールに書かれている記載言葉に合わせて、以下の該当する復元手順へお進みください。

- ・メールに「解放」と記載がある場合

→ 「3.メール文章に「解放」と記載がある場合の手順」【P4】へ

- ・メールに「リリースの要求」と記載がある場合

→ 「4.メール文章に「リリースの要求」と記載がある場合の手順」【P6】へ

3.メール文章に「解放」と記載がある場合の手順

- (1) 通知メール、または検疫ページ内にある「解放」をクリックします。



- (2) 「解放」ボタンをクリックすると、以下の完了画面が表示されます。



※ 検疫ページの一覧画面は反映されるまでにタイムラグがありますが、手動で更新をかけると解放の状態が「解放済み」という表示になります。

(検疫ページの参考)



※ メールを解放しても受信トレイに届かない場合、「迷惑メール」フォルダに振り分けられていることがありますのでご注意ください。

4.メール文章に「リリースの要求」と記載がある場合の手順

検疫理由が「高確度のフィッシング」となっているメールは、セキュリティ上の危険性が極めて高いと判断されているため、ユーザー自身の操作による解放が制限されています。誤検知（安全なメールが誤って隔離された）と思われる場合は、管理者へ「リリースの要求（解放依頼）」を行う必要があります。

リリースの要求の手順

（１） 要求の実行

検疫通知メール、または検疫ページにて該当のメールを確認し、「リリースの要求」をクリックします。（例：検疫通知メール）



(例：検疫ページ)



(2) 管理者への通知：

「リリースの要求」をクリックすると、システム管理者へメールの解放要求が自動的に送信されます。管理者が要求を受け取り、対象メールの安全性を確認します。

管理者が安全であると判断した場合のみ、メールが解放（受信トレイへ配信）されます。

解放後「迷惑メール」に分類される場合があります。

※注意：管理者が「安全でない」と判断した場合は、解放されません。

5.しばらく経っても解放されない場合

リリースの要求を行ってから一定時間が経過してもメールが解放されない場合は、以下の必須情報を添えて情報基盤統括センターまでお問い合わせください。

- 送信日時
- 送信者メールアドレス
- 受信者のメールアドレス
- 件名

お問い合わせ連絡先：admin@cc.u-ryukyu.ac.jp

※ お問い合わせは、原則として学内メールアドレスからのみ対応いたします。
セキュリティを考慮しての対応ですのでご了承ください。

(参考) フィッシングメール等

フィッシングメール

本物の企業やサービスを装って、個人情報やパスワード、クレジットカード番号などをだまし取ろうとする詐欺メールのこと。

スパムメール

受信者の意思に関係なく一方的に大量に送りつけられる迷惑メールです。

フィッシングメールは、銀行・通販サイト・宅配業者などになりすまし、「重要なお知らせ」「緊急」などと不安をあおって、偽サイトへ誘導し、ID・パスワード等の情報を入力させようとします。

◇ フィッシングメールの例

- ・ 「アカウントが凍結されました。今すぐログインしてください」
- ・ 「不正利用の疑いがあります」
- ・ 「荷物が届けられませんでした。再配達の手続きをしてください」
- ・ 「当選しました！こちらをクリック」 → 偽サイトへ誘導

◇ 見分けるポイント

- ・ 送信元アドレスが怪しい（公式ドメインと違う）
- ・ 日本語が不自然（翻訳っぽい文章）
- ・ 「急いで対応してください」と急かしてくる
- ・ URL が本物と少しだけ違う（例：amazom.co.jp など）等

◇ 対策

- ・ メール内のリンクはクリックしない。
- ・ 必要な場合は公式サイトから直接アクセスする。
- ・ パスワードやカード情報を安易に入力しない。
- ・ 不審なメールは無視・削除する。

(参考) 危険度のレベル

判定理由 (危険度)	状態	ユーザーの対応方法
スパム 一括送信メール (低～中)	迷惑メール や広告メールの 可能性	ご自身で内容を確認し、「解放」が可能
フィッシング (中)	情報を盗み取ろ うとする詐欺の 可能性	ご自身で内容を確認し、「解放」が可能
高確度のフィッ シング (高)	詐欺の可能性が 極めて高い	ご自身での解放は不可。 管理者へ「リリースの要求」が必要
マルウェア (最高)	ウイルス感染の 危険性あり	ご自身での解放は不可。 管理者へ「リリースの要求」が必要

参考：Microsoft365 Learn

- ・ [検疫されたメッセージとファイルをユーザーとして管理する](#)
- ・ [検疫済みメッセージに関する FAQ](#)
- ・ [検疫ポリシーに関する詳細](#)
- ・ [検疫通知の詳細](#)
- ・ [共有メールボックスの検疫の詳細](#)