MERU MAMORI PARTNER SAMPLE REPORT

中小企業向け
不審メール月報サンプル

2026年4月版。相談窓口に届く不審メールを、顧客説明・社内注意喚起・月次報告に使いやすい形へまとめたサンプルです。

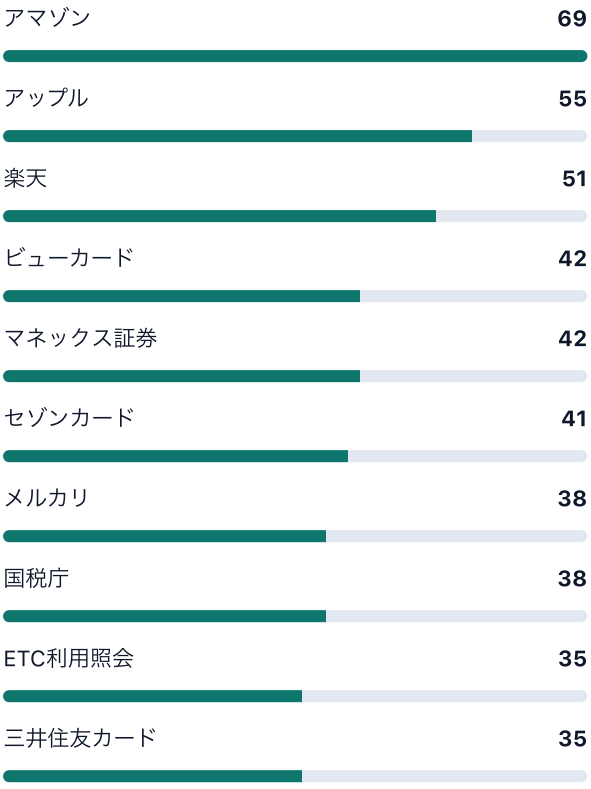
公開案例	収集素材	高危険度	主要ブランド
555	1061	1019	86

1. 今月の概要

高危険度比率	公開案例化	件名パターン	送信元ドメイン
96%	555	7	402

今月は、配送通知、本人確認、カード利用制限を装うパターンが目立ちました。特にブランド名を自然に使い、公式通知に見える文面でログインや支払い確認へ誘導する例が多く確認されています。

ブランド分布



テーマ分布

テーマ	件数
支払い・利用確認	214
ポイント失効	202
セキュリティ認証	163
アカウント停止	139
本人確認	134
カード停止	87
本人確認・ログイン通知	79
請求トラブル	71

2. 件名パターン

パターン	件数	注意点
本人確認・アカウント確認	173	公式ログインに見せかけ、ID・パスワード入力へ誘導する。
その他	163	ブランド名や通知文の自然さだけでは判断しない。
支払い・請求	92	未払い・決済失敗を理由にカード情報入力へ誘導する。
セキュリティ警告	42	不正ログイン警告を装い、偽の確認画面へ誘導する。
キャンペーン・ポイント	40	特典や当選を口実に個人情報入力を促す。
配送・不在通知	28	荷物確認や再配達を装い、スマートフォンでの操作を狙う。
利用制限・停止通知	19	急がせる表現で、確認ボタンのクリックを促す。

件名は短く、緊急性を出し、公式名を添える傾向があります。従業員向けには「メール内ボタンではなく、公式アプリ・ブックマークから確認する」運用を徹底するのが現実的です。

3. 高危険度サンプル

高危険度

au（KDDI）

1. 【重要】au PAYポイント有効期限のお知らせ（失効予定）

au（KDDI）を装い、公式通知に見える件名で確認や入力を促す内容です。送信元やリンク先が公式と一致するかを確認する必要があります。

- 送信元 zzty30.cn はau（KDDI）の公式ドメイン (au.com, kddi.com) ではない
- メール内リンクが公式サイトではない不審なドメイン (*www.au.com*) に誘導
- 送信元ドメインが公式と異なる

> **「ポイント失効」「マイル期限」を装うメールは、公式アプリでポイント残高を直接確認してください。メールから遷移したページでログイン情報を入力しないでください。**

高危険度

楽天

2. 【重要】楽天ポイント有効期限が迫っています｜お早めにご利用ください.

楽天を装い、公式通知に見える件名で確認や入力を促す内容です。送信元やリンク先が公式と一致するかを確認する必要があります。

- メール内リンクが公式サイトではない不審なドメイン (yuyihome.com) に誘導
- 送信元アドレスが楽天公式と無関係（例: [メールアドレス]）

> **「ポイント失効」「マイル期限」を装うメールは、公式アプリでポイント残高を直接確認してください。メールから遷移したページでログイン情報を入力しないでください。**

高危険度

Apple

3. iCloudストレージプラン更新のお知らせ

Appleを装い、公式通知に見える件名で確認や入力を促す内容です。送信元やリンク先が公式と一致するかを確認する必要があります。

- 送信元 mail18.tagdoing.com は当該ブランドの公式ドメイン (apple.com) ではない
- メール内リンクが公式サイトではない不審なドメイン (gdhisq.com) に誘導
- 件名に「[meiwaku]」が含まれ不自然

> **不審なメールが届いた場合、メール内のリンクは絶対に開かず、公式サイトや公式アプリから直接確認してください。送信元アドレス、リンク先URL、文面の不自然さに注意してください。**

高危険度

マネックス証券

4. 【緊急】不正アクセス検知に伴うパスワード変更およびパスキー確認のお願い no.

マネックス証券を装い、公式通知に見える件名で確認や入力を促す内容です。送信元やリンク先が公式と一致するかを確認する必要があります。

- 送信元ドメイン「jreast.co.jp」はmonexの正規ドメイン「monex.co.jp」と一致しません。
- 件名に「緊急」など緊急性を煽る表現が含まれています。正規のmonexが急かすことは通常ありません。
- 「パスワード」を装って個人情報やログイン情報の入力を促す内容です。

> **メール内リンクではなく、公式サイトや公式アプリから直接確認してください。**

高危険度

東京電力

5. 【tepco】振替不能に伴う電気料金お支払いのお願い

東京電力を装い、公式通知に見える件名で確認や入力を促す内容です。送信元やリンク先が公式と一致するかを確認する必要があります。

- 送信元ドメイン「04510.jp」はtepcoの正規ドメイン「tepco.co.jp」と一致しません。
- 件名に「24時間」など緊急性を煽る表現が含まれています。正規のtepcoが急かすことは通常ありません。
- 「tepco」を名乗っていますが、件名「【tepco】振替不能に伴う電気料金お支払いのお願い」のパターンは典型的なフィッシング手口です。

> **メール内リンクではなく、公式サイトや公式アプリから直接確認してください。**

4. 社内注意喚起テンプレート

【2026年4月 不審メール注意喚起】

今月は、本人確認、配送通知、カード利用制限を装う不審メールが目立っています。

メール内のボタンやリンクからログインせず、公式アプリまたはブックマーク済みの公式サイトから確認してください。
判断に迷うメールは削除せず、社内の不審メール相談窓口へ転送してください。

特に以下の表現には注意してください。
・「本人確認が必要です」
・「アカウントの利用を一時制限しました」
・「お荷物の配達に失敗しました」
・「支払い情報を更新してください」

この文面は、そのまま Slack、Teams、社内メールで共有できます。月次報告では「今月多かった見せ方」と「迷った時の社内転送先」を必ずセットで伝えると、現場が動きやすくなります。

5. パートナー提供時の価値

顧客向け

怪しいメールを相談する窓口が明確になり、自己判断でリンクを開くリスクを減らせます。

IT支援会社向け

月次報告の材料が増え、既存顧客との定例接点でセキュリティ支援を説明しやすくなります。

4週間テスト導入で確認する指標

指標	見る理由
相談件数	顧客内に実際の不安・相談需要があるか
高危険度比率	単なる迷惑メールではなく被害防止につながるか
月報閲覧・共有	報告資料として継続価値があるか
運用負荷	既存サポート業務に自然に乗るか

6. 次月に注意したい動き

ブランド名だけで判定せず、送信元、リンク先、本文の要求内容を組み合わせて確認してください。特に、本人確認、利用制限、配送通知、未払い請求の文面は継続して注意が必要です。

推奨運用

- メール内リンクを開かず、公式アプリ・公式サイトから確認する。
- 判断に迷うメールは削除せず、社内相談窓口へ転送する。
- 同じブランドの不審メールが増えた場合は、月報で短く共有する。