フィッシング対策の理想と現実

～数千万ユーザーを守るメール事業者の365日～

KDDI株式会社
中島　直規

2026/11/06

Spark Your Journey

© KDDI CORPORATION

はじめに

本講演資料は、

・個人の見解を述べたものであり、会社としての見解・業界としての見解ではありません。

・スクリーンショット等にて引用させていただいたものは2026/11/02現在の情報です。
　資料同ページ内に引用元URLの記載、またはハイパーリンクを掲載しております。

・上記いずれも各会社の商号、商標または登録商標です。

・イラストには弊社イラストおよびAIにより作成したイラストを利用しております。



auサポーとり エナ オフィシャルサイト - auサポート情報

© KDDI CORPORATION

Spark Your Journey
KDDI

講演者紹介



中島 直規
（Naoki Nakajima）

KDDI株式会社
オペレーション本部
プラットフォームエンジニアリング部

座右の銘

めげるな、しょげるな、いじけるな！

明日は明日の風が吹く！



- **[2007年～2011年]セキュリティ対応部門（SOC）**
  - システム監査、NW/AP脆弱性診断
  - 総務省サイバー攻撃対応演習運営など
- **[2012～2018年]メール開発部門**
  - ISPメール設備
  - 設備更改／品質改善開発担当
- **[2018～2020年]メール運用部門**
  - キャリアメール/ISPメール
  - 運用リーダー
- **[2020年～]メールシステム DevOps**
  - KDDIメール設備の開発・運用全般（DevOps）
    - ・迷惑メールフィルタ
    - ・メール配信システム
    - ・メールボックスシステム

© KDDI CORPORATION

Spark Your Journey
KDDI

今日お伝えしたいこと

01 **すり抜けの「現実」を知る**

件数だけでなく、攻撃の中身と設備への影響を見る。

02 **届いたメールを、次の迷惑メールブロック対策へ生かす**

申告・本文特徴を生かし、精度と対応速度を磨き続ける。

03 **「止める」と「届ける」を、両立するには**

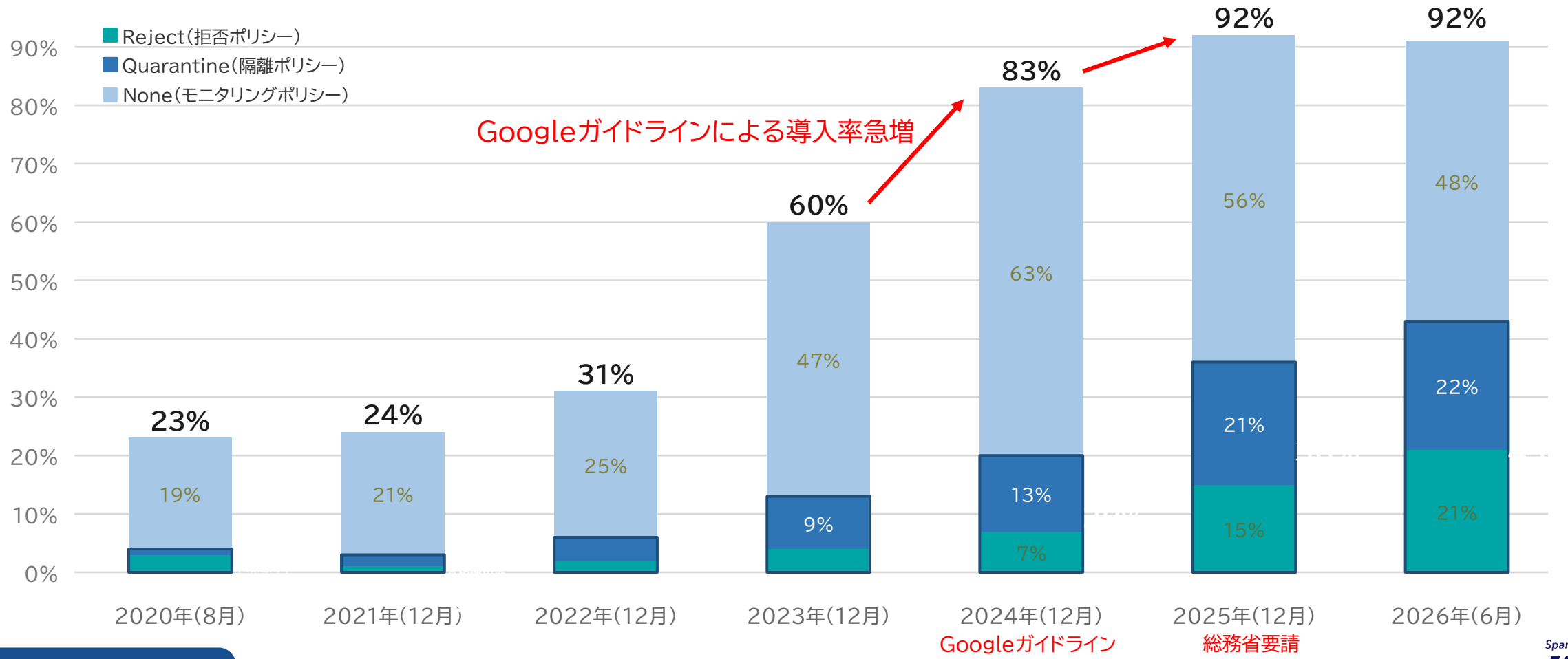
受信側の対策と、送信側の正しい運用を両輪で進め、安全なメッセージングの実現へ

迷惑メールを減らし、必要なメールが届く環境を守るために。

© KDDI CORPORATION

DMARC普及率の推移(日経225企業)

DMARC普及率自体はGoogleガイドラインにより9割以上　Good
隔離以上のポリシーの設定率は未だ半数に満たない　Bad
中小企業等も含めるとさらに低調な状況、日本の後進ぶりが目立つ(例:アメリカ等は83%)



© KDDI CORPORATION

Spark Your Journey
KDDI

直近の被害の状況

2025年のフィッシング報告件数は過去最多、被害も「高額化」している・・・。
日本語フィッシングメールを確実に止めていかない限り、被害はなくならない。



2,454,297件

2025年のフィッシング報告件数（過去最多）

約1.43倍

2024年比（報告件数）
※2025年3月は月間 約25万件で過去最多

約42.2億円

2025年上半期 ネットバンキング
不正送金被害総額（警察庁発表）

約7,393億円

2025年 証券口座乗っ取りによる
不正取引の規模

出典：フィッシング対策協議会「フィッシングレポート2026」（2026年6月1日公開）
https://www.antiphishing.jp/report/wg/phishing_report2026.html
※不正送金被害額は同レポートが引用する警察庁発表

© KDDI CORPORATION

Spark Your Journey
KDDI

auメールの迷惑メール対策の歩み

迷惑メール社会問題化以降、SPFを始めとした機能を強化
2013年に「迷惑メールおまかせ規制」としてデフォルトONへ
2023年12月、DMARC・BIMIの導入によりフィッシング対策をさらに強化





迷惑メールフィルタ

2000年頃～ 拒否機能を順次強化

各種拒否機能（指定拒否等）
SPF／SenderID認証

キャリアメールはSPF/SenderIDを
武器に迷惑メール対策を強化

2013年～ 全てのお客様に自動検知

迷惑メールおまかせ規制
デフォルトON

ほぼすべてのお客様で
迷惑メール対策機能を使って頂けるように

2023年～ 本格的なフィッシング対策

受信DMARC/BIMI対応

受信側対策としてDMARC/BIMI対応
送信側対策と合わせてよりセキュアへ！

2025年～

総務省要請受け、更なる強化へ。



auメールアプリ
（Android）

メーラでの拒否登録簡素化

手動拒否登録をワンタッチで可能に

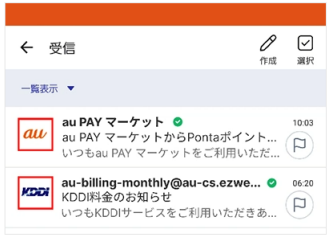
迷惑メール報告機能リリース

申告頂いたメールを迷惑メール対策に
利用し、迷惑メール対策ループを構築



迷惑メール申告機能（auメールアプリ）

BIMIロゴ表示対応



Android auメールアプリ



iPhone／iPadメールアプリ

© KDDI CORPORATION

Spark Your Journey
KDDI

日本語圏に対するフィッシングメールの集中

（昨年講演にて・・・）「とうとう日本が狙われ始めた」

生成AIを活用して「流ちょうな日本語」な見破るのが難しいフィッシングメールが作れるように。
「本文が不自然」で守られてきた、日本の消費者のフィッシングメール耐性の低さに目を付けられた？

2026年9月の報告
分野別割合

EC系47.9%＋クレジット・信販系35.0%

観点	公開情報で確認された事実	狙い
言語・地域	「CoGUI」は日本語圏を標的にしてきており、 IPロケーション・ブラウザー言語等で表示を選別している	日本語の文面だけでなく、 利用環境を選んだ攻撃へ。 セキュリティエンジンのサーチを潜り抜ける狙いも。
本文題材	2025年：証券会社の認証設定・補償通知を模倣 2026年：税金・公共料金等の請求を偽装するよう変化	利用者が普段受け取りそうな文面等で判断を 通知に紛れ込む。
行動変化	モバイル回線からのアクセス限定の偽サイトや、 氏名入りメール、不正アプリへの誘導を確認。	受信者の環境依存狙い（モバイルで決済させる等） 不正アプリをスマホにインストールし乗っ取りを狙う

出典：Proofpoint／フィッシング対策協議会／金融庁公表データを元に記載

© KDDI CORPORATION

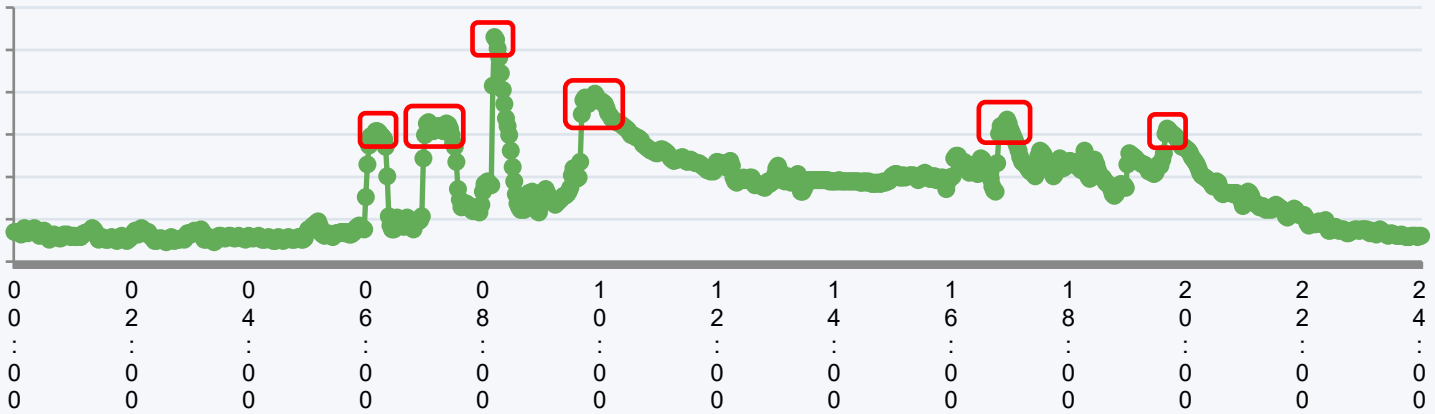
Spark Your Journey
KDDI

大量フィッシングメール受信が設備へ与える影響

お客さまに届く前から、メール受信設備への接続・受信処理のリソースを押し上げる送信方法が増加
守る対象は「利用者」は当然こと、「メールサービス基盤」もしっかり保護しなければいけない・・・。

auメール受信サーバのコネクション数（10月某日）

※ 実コネクション数は非公表とさせてください。。



6・7・8時台に急増、その後も突発的な“山”が継続発生。
最繁時間帯の山を打ち消すくらいのコネクション水準が継続。



調査で確認された大量受信（左の“山“）

外部の大手クラウド基盤が中心
年末調整・税還元系をかたるフィッシングメール

auメール設備で迷惑メールブロック処理をするための処理負荷が増加、ムダなリソースとなっている。。

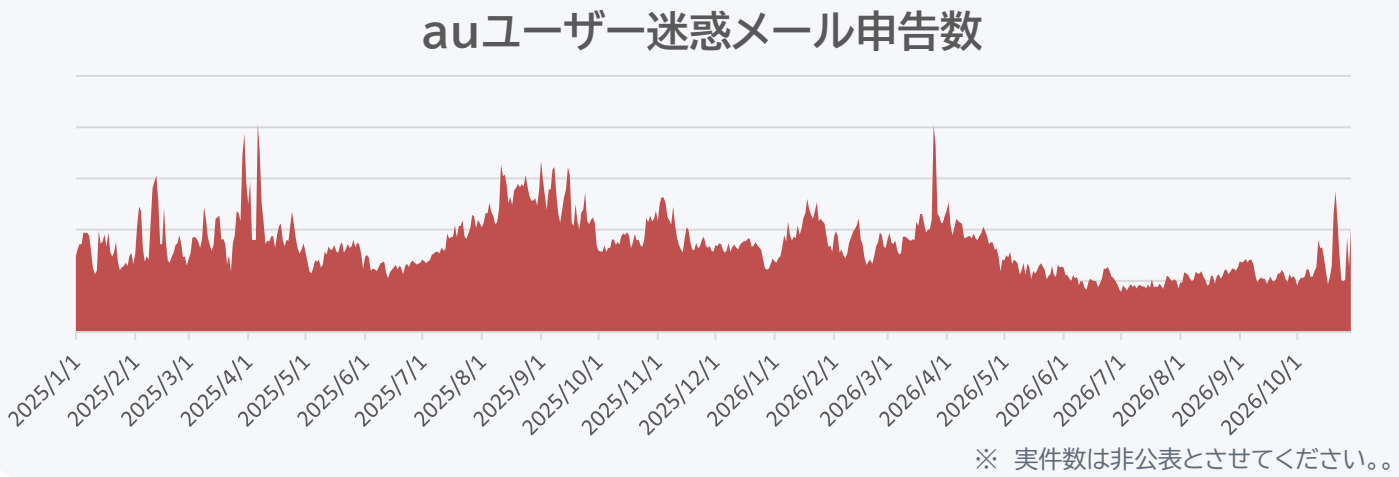
© KDDI CORPORATION

Spark Your Journey
KDDI

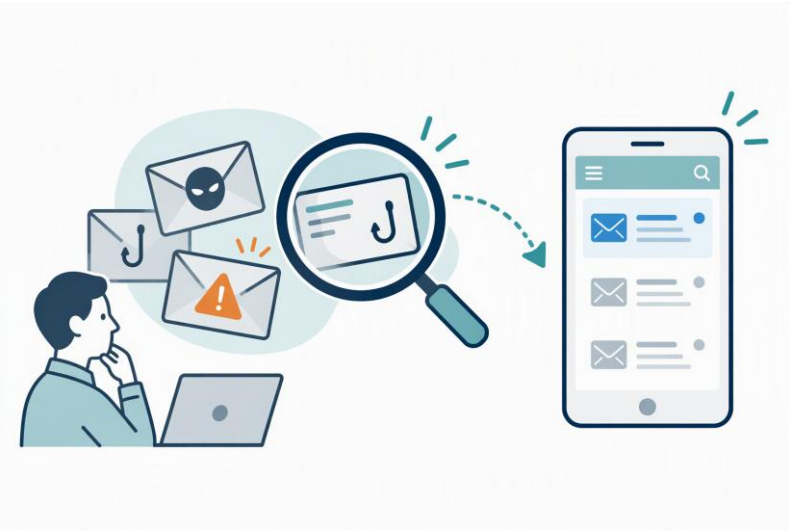
申告メールに見る変化の波

見るべき変化は“総量”だけではなく、「突発的な山」と「届くメールの悪質化」

量の変化｜申告数は長期トレンドだけでなく突発的な跳ね上がりに注意



※ 実件数は非公表とさせてください。。



特定機関・サービスをかたるメールが集中

突発跳ね上がりの主要因を申告の中身で確かめると・・・

急増日には特定の機関やサービスを狙ったフィッシングメールを
大量観測することが多い(もちろんすり抜けている・・・

「迷惑」から、金銭・情報を奪う脅威へ

申告メールの内容を分析すると、
直近2年では金銭被害・情報搾取を狙うフィッシングメールの増加が目立つ

申告の急増は、すり抜けて届いてしまった「フィッシングメール」の警報と同意
量と中身を捉え、すり抜けへの対策を急ぐ必要がある

© KDDI CORPORATION

Spark Your Journey KDDI

「届いた」「申告された」「被害に遭った」は別の数字

大量に止めていても、届いた一部のメールから被害は起こり得る・・・。

届いた“すり抜け”メール

迷惑メールの受信総量そのもの

遮断・破棄しきれず、受信箱に届いた迷惑メールの通数

申告された数

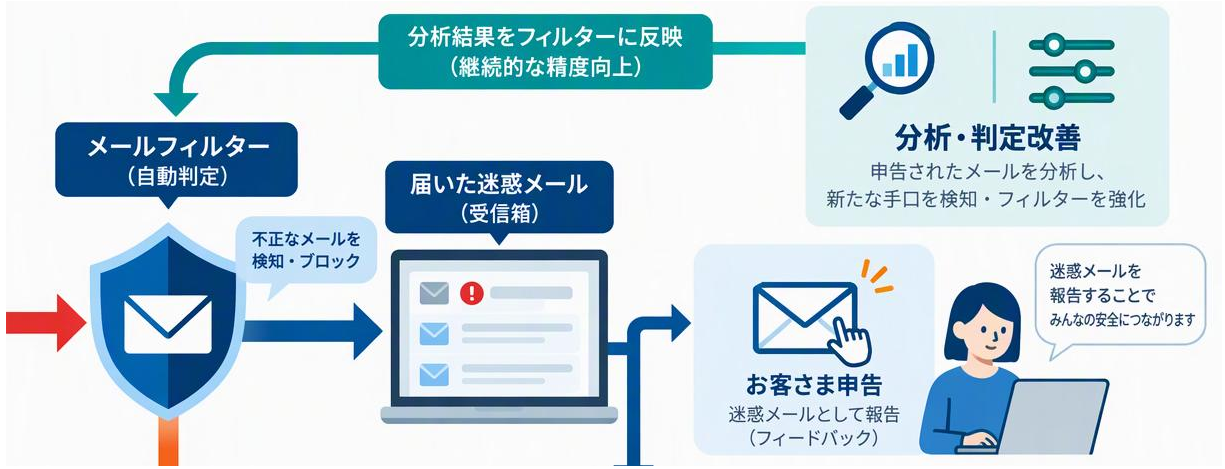
全体の一部を観測

届いた迷惑メールをお客さまがKDDIに迷惑メールとして申告した通数

被害に遭った数

最終的に減らす対象

情報詐取・不正送金・マルウェア感染などの被害件数



申告と被害は、到達後の別の観測軸

むしろ、未申告のメールから被害は起こる
申告メール通数が増えている＝被害拡大が危惧される状況であると認識すべき

申告メールを防御・改善に生かし、すり抜けを減らす取り組みを加速。

© KDDI CORPORATION

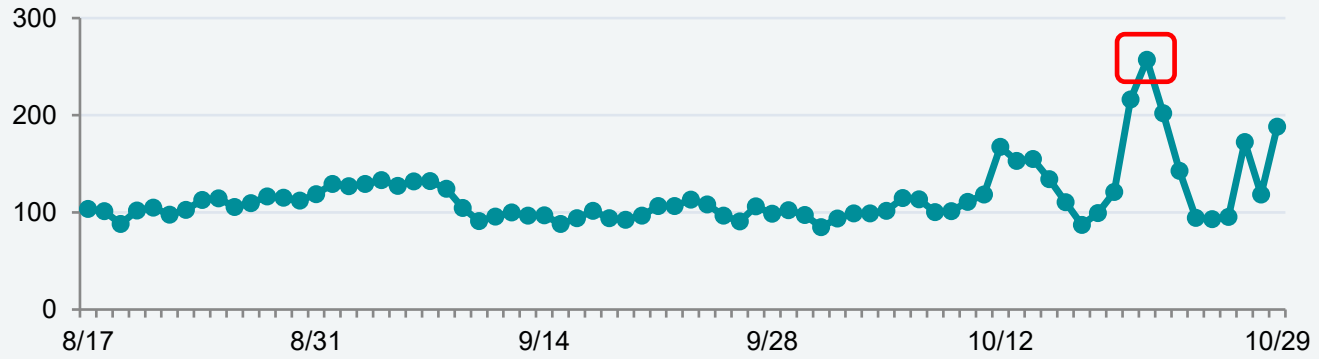
Spark Your Journey
KDDI

お客さまからの申告は、不完全だが貴重なデータ

申告される方は全体の一部のお客様だが、貴重なデータとして対策に生かせる！

お客さまから届く、すり抜け迷惑メールの申告数

突然2.5倍に跳ね上がる恐怖。。



8/17～8/23の平均＝100とした指標に変換したグラフです。(絶対通数ではありません。)

注意！全体像ではない

申告された一部のデータの範囲の情報
未申告のメール数は、このデータでは推測できない

すり抜けたメールそのものを確認できる

メールヘッダ・本文・誘導先URL・手口など
手法そのものまで確認できる

申告数からはすり抜け通数全量・被害件数・フィルタの検知率などは分からないが、深刻度が分かる

丁寧かつ迅速に分析し、「すり抜けているメール」の特徴をつかみ、チューニングへ

© KDDI CORPORATION

Spark Your Journey
KDDI

次の勝負は「すり抜け」への対応速度

申告を受けてから、規制チューニングまで。
その時間を縮めるために、分析工程へ生成AI活用を取り組み中！

現在の申告メール分析ループ

申告メールを確認 ❱ 人の目で分析 ❱ チェック ❱ 規制チューニング

課題：確認・分析・チェックを経るため、対策への反映に時間がかかるのが従前からの課題。



分析工程での生成AI活用を加速中

分析スピードの向上・分析精度安定化
を両立することが目的

申告＝すでにお客様に届いてしまっている状況であることを認識し、
いかに早く次の迷惑メールをお客様に届けないようにするか。対応までの時間を縮める戦い

© KDDI CORPORATION

迷惑メール対策をより進めるために・・・

迷惑メールフォルダ機能で、お客さま自身が確認できる選択肢を提供開始（2026年12月以降～）
迷惑メール対策を、さらに強化できる準備と捉え、より対策を強化していきます



auメール／UQ mobileメール「迷惑メール」フォルダ機能 提供開始について｜スマートフォン・携帯電話｜au

お客さまの確認機会を確保

隔離対象のメールは破棄せず保存。
迷惑メールフォルダで
お客さま自身が確認できるように！

より進んだ対策を推進

確認できる仕組みを整えながら、
迷惑メール対策の強化を
さらに進めていく。

「ブロック」に加えて「隔離」を導入。
確認できる仕組みを、対策強化を進める土台にする。

© KDDI CORPORATION

総務省要請：2025年秋から更なる強化フェーズへ

フィッシングメール起因の不正取引被害の拡大を背景に、総務省より通信事業者へ「フィッシングメール対策の強化に関する要請」メール事業者の対策は新たな強化フェーズへ。

背景

情報窃取が、金銭被害につながる

証券会社を装うメール等で
ログイン情報を窃取
不正アクセス・不正取引の
被害が急増中・・・

2025年9月1日

総務省が対策強化を要請

① フィルタリング精度の向上
　AI活用・適切な強度設定
② DMARC等の導入・運用
③ 利用者への周知・啓発

KDDIのお知らせ｜2026年3月19日

「見抜く・知らせる・使っていただく」を強化

3月24日～：なりすまし警告
5月下旬～：おまかせ規制の
　　フィルタリング精度向上
設定OFFのお客さまへの利用促進

auメール、特殊詐欺・フィッシング対策の取り組みを強化｜KDDI ニュースルーム

© KDDI CORPORATION

auメールの迷惑メール対策の歩み（2026年度）

2026年上期にauメールアプリにおける警告機能の導入
正規メール疎通機能の改善による迷惑メール削減の取り組みを継続
2026年5月～　本文特徴データを用いた強化を行う新たなフェーズへ



迷惑メールフィルタ

2026年3月
auメールアプリによる啓蒙

2026年5月
おまかせ規制へのお客様加入促進

2026年5月～
本文特徴データを用いた
精度向上の取り組み

2026年X月

正規メール疎通安定化機能の強化

受信メール本文の特徴を用いたフィルタ精度向上

本文特徴データ用いた精度向上の規制反映

正規メールを通過しやすくする機能のチューニングにより
巻き添えで迷惑メールを素通りさせてしまう通数を削減

受信側対策としてDMARC/BIMI対応
送信側対策と合わせてよりセキュアへ！



auメールアプリ
（Android）

送信ドメイン認証に
基づく警告表示

おまかせ規制未加入時の
加入推奨メッセージ表示

迷惑メール申告ユーザーの
おまかせ規制強制ON

なりすましメールによる被害の最小化

おまかせ規制未利用のお客様に
フィルタ機能を利用して頂く取り組み



迷惑メールおまかせ
規制加入促進画面

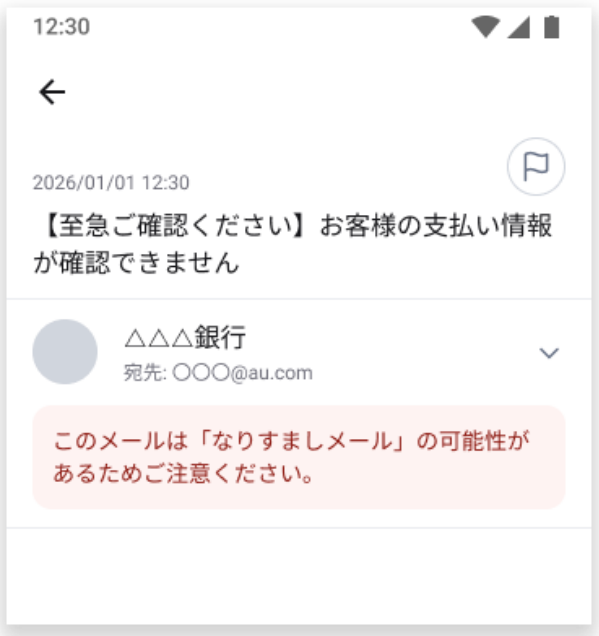
「判定」するだけでなく、「見える化」する取り組み

auメールアプリに送信ドメイン認証失敗メールに対する警告表示機能を追加
メール本文表示／Webサイト遷移時に警告メッセージによって注意喚起を行う

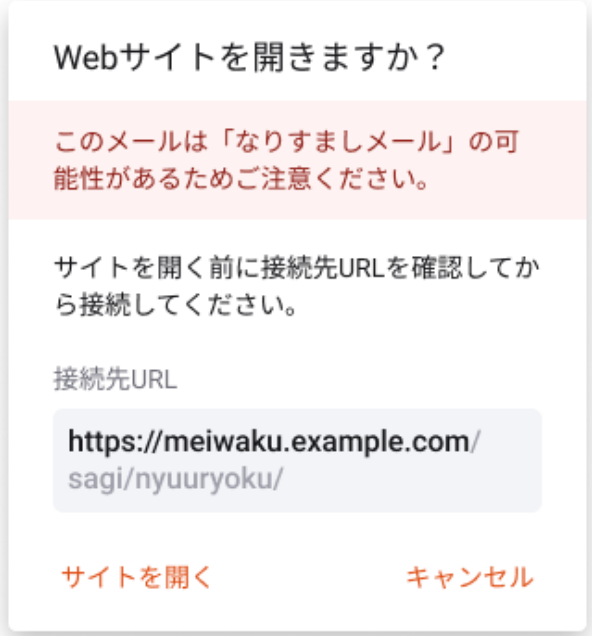
送信元認証未実施



送信元認証失敗時



送信元認証失敗メールでのWebサイト遷移時



表示条件	SPF/SenderID/DMARCの送信ドメイン認証が成功しない場合
対象・開始時期	Android版 auメールアプリ Ver.16.01.2G以上／2026年3月24日以降順次

ただし、認証成功＝本文やリンク先の安全性を保証するものではないことには引き続き注意が必要

© KDDI CORPORATION

Spark Your Journey KDDI

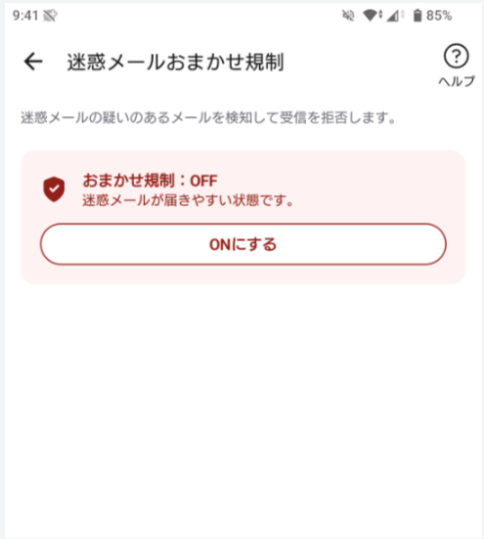
“守る”機能をよりたくさんのお客様にご利用頂くために

迷惑メールおまかせ規制機能を未利用のお客さまに、アプリでお知らせ。
その場でONへ進める導線を用意し、迷惑メールフィルタ設定率を引き上げへ。

①
未設定のお客様への注意喚起表示



②
おまかせ規制をON



おまかせ規制
ONに変更完了

この取り組みによる
新規迷惑メールフィルタ利用開始

1日

1,000人以上/日

おまかせ規制をONにし、
迷惑メール対策を享受できるお客様を最大化！

© KDDI CORPORATION

Spark Your Journey
KDDI

「通す」と「止める」の間にある現実（正規メール疎通安定化機能強化）

迷惑メールを止めたい。けれど、正しいメールは止められない。

厳しく止める

迷惑メールの遮断を強化！

一方で、
正規メールまで
止めるおそれ

誤検知（False Positive）



正しく通す

正規メールの到達性を確保

一方で、
緩和措置によって
迷惑メールも通るおそれ

すり抜け（False Negative）

正規メール疎通の安定化機能の適用条件と判定ロジックを高度化し、すり抜けを防止する！

© KDDI CORPORATION

Spark Your Journey
KDDI

お客さまに届いたメールが、防御を育てる

申告は、「いま何がすり抜けているか」を映す、対策改善のための宝の山。
しかし、「一部」のメールであることも事実・・・
いよいよ、受信メールから精度を向上する取り組みが開始！

① 届く・申告する



今まで

届いた迷惑メールを、
お客さまがKDDIへ申告。

これから

届いたすべてのメールから、
KDDIが代わりにデータを抽出

② 分析する



申告データから、
すり抜けの特徴を把握。

③ 連携・調整する



Hornetsecurity社への連携
＋KDDIの対策スキームで調整。

HornetSecurity社へ連携し、
日本語特徴データを含む豊富なデータで
機械学習を推進

④ フィルタエンジンへ反映



判定情報へ反映し、
速やかな保護につなぐ。

日本語フィッシングメールに
対応し、更なる精度向上へ

© KDDI CORPORATION

Spark Your Journey
KDDI

実際に届いたメールを、そのまま迅速な精度改善へつなげるために

本文特徴データの利用に向けた取り組みは順調に進んでおり、あとひと息！の段階。

1	機械学習	HornetSecurity社には、日本語データを含むメールの機械学習環境はReady！
2	利用するための条件整理	事前同意の取得を条件に、総務省との間で通信の秘密との関係を整理
3	個別同意の取得	全てのauのお客さまにメールで周知（新規のお客さまには契約約款の改正で対応）
4	メール本文特徴データ提供	本文から得られる特徴データの、Hornetsecurity社への提供を開始
5	**届いたデータで、精度を磨く**	**提供データを基に日本語フィッシングメールを機械学習し、調整を継続。** **今はココ**
6	学習の成果を、エンジンへ反映	改善結果を規制エンジンへ順次反映し、迷惑メールが届きにくい環境へ。

2026年中にすべての工程を終え、精度向上を実現するべく、鋭意頑張って頂いております！

© KDDI CORPORATION

Spark Your Journey
KDDI

従来の判定の限界

「誰が送ったか」だけで判断する時代から、「何が書かれているか」も捉える対策へ

現場で見られる変化	送信元の情報だけでは判断しきれない理由
独自ドメインで送られる迷惑メールが増加	他社ドメインを詐称しなくても、迷惑メールは送れる。
送信元IPを逆引きできないメールが増えた時期	逆引きの可否だけで、本文の危険性までは分からない。
特定の送信基盤からの大量受信	基盤や受信量の情報だけでは、個々のメールの内容を捉えきれない。

送信元の手がかり

IP・逆引き・ドメイン・認証結果

内容の特徴を重ねる

件名・本文等から、判定に有効な特徴を分析

すり抜けを減らすには、送信元の情報に、実際に届いたメールの特徴を重ねる。

© KDDI CORPORATION

Spark Your Journey KDDI

「誰が送ったか」から「何が書かれているか」へ

送信元・認証の判定を続けながら、実際に届いたメールの特徴で判定情報を育てる

判定の観点	具体的に見る情報	捉えられること・狙い	限界・今回の位置づけ
送信基盤・挙動	送信元IP／逆引き 特定基盤からの受信量	どの基盤から、どの程度 送られているかを捉える	逆引きの可否や受信量だけでは、 一通ごとの内容は判断できない
送信ドメイン認証	SPF／DKIMの認証結果 DMARCのFrom整合性	ドメインの使用が認証されるか、 Fromと整合しているかを確認	認証成功は内容の安全性を保証しない。 独自ドメインの迷惑メールも対象外ではない
ヘッダ由来の特徴	メールのヘッダ情報から 判定に有効な特徴データ	実際の受信メールから得た特徴を、 判定情報の改善へつなげる	今回の提供対象。 個別フィールドや抽出方式は非提示
件名由来の特徴	件名から得られる特徴 例:「確認」「手続き」等の表現※	送信元だけでは見えない、 メール内容の特徴を材料に加える	今回の提供対象。 特定の語句だけで迷惑と断定しない
本文等の特徴	本文等から得られる特徴 例:確認や操作を促す文面※	提供データを基に日本語フィッシングを 機械学習し、エンジン精度を磨く	現在は学習・調整中。 規制への反映と実測効果は区別する

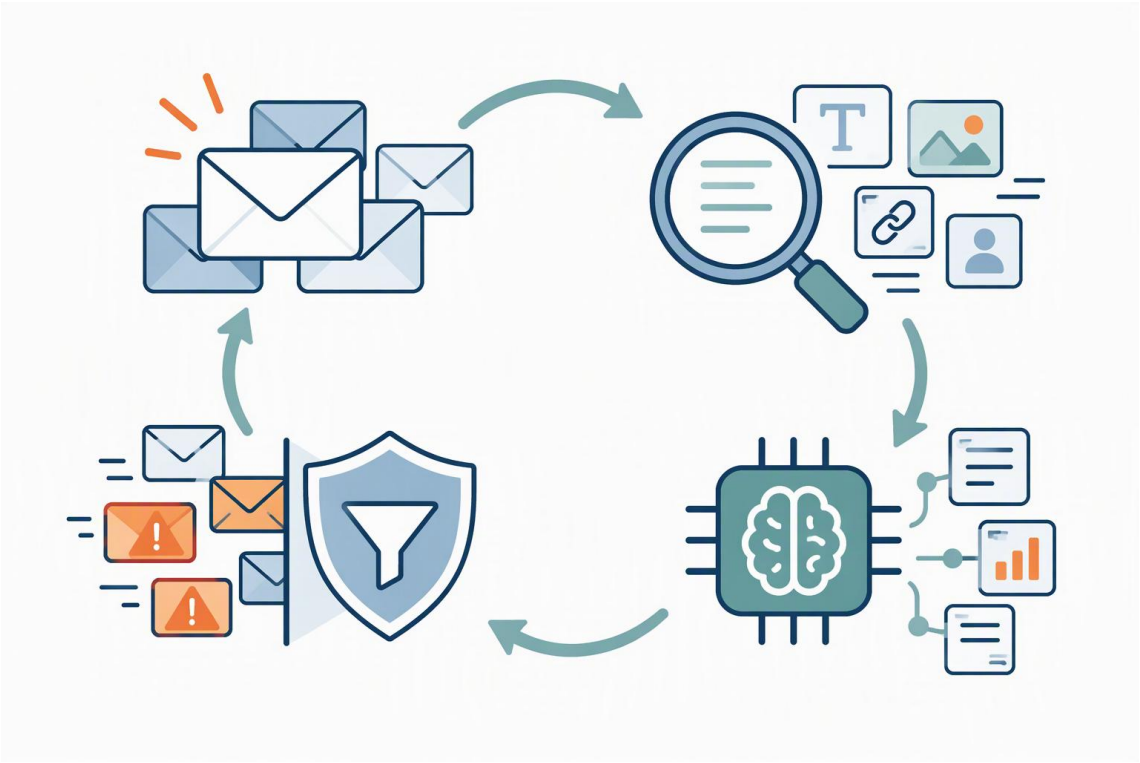
認証を置き換えるのではない。送信元の情報と内容の特徴を重ね、すり抜けを減らす。

© KDDI CORPORATION

Spark Your Journey KDDI

【受信側対策】ポジティブループ24時間365日継続へ

本文特徴データの提供は、継続的な精度向上の出発点
機械学習は24時間365日継続して取り組むポジティブループへ



01 変化を捉える

新たなフィッシングの手法・特徴を捉えるため、
本文特徴データの提供を継続。

02 学習・改善を重ねる

機械学習による判定の改善を続け、
規制精度の向上に継続的に取り組む。

03 次の変化にも追随する

手法が変わっても追随する試みを続け、
規制強化を積み重ねる。

**攻撃が変わり続ける限り、いたちごっこは続く。
が、ひたすら追いついていける迷惑メール対策へ**

© KDDI CORPORATION

Spark Your Journey
KDDI

【送信側対策】送信者ガイドラインの整備へ

送信者の皆さまへのお願い。昨年お伝えした6項目を、認証・基盤・運用の観点で整理。

01 SPF

Passになるように設定するだけでなく、
広すぎるIP範囲の指定などはしない。

02 DMARC

未設定は論外。
ポリシーはrejectを目指す。

03 DKIM

送信メールには、
全てのメールに有効なDKIM署名を。

04 逆引きDNS

送信元IPには、
正しい逆引きホスト名を登録する。
可能な限り、HELOドメインとの一致を。

05 宛先リスト

宛先不明を多数発生させない。
リストを継続的にメンテナンスする。

06 送信量・接続数

短時間に送りすぎない。
必要以上の同時接続を張らない。

**止めるべきメールを止め、届けるべきメールを届ける。
そのために、送信者の皆様に守っていただくべきルールの整備を。**



KDDIは、国内メール通信事業者で進めるガイドライン整備推進に全面協力していきます。

© KDDI CORPORATION

Spark Your Journey
KDDI

迷惑メールを止める！正しいメールを届ける！の両立へ

迷惑メール対策を進めることと、必要なメールを届けること。その両立が、私たちの責任です。

受信側｜メール事業者

攻撃への対策を、止めない。

判定の改善・すり抜けへの対応を継続。
正当なメールの受信も、同時に守る。

＋

送信側｜メールを届ける皆さま

正しいメールを、正しい送り方で。

送信元を認証できる設定と、
受信側に配慮した送信運用を。

対策強化のために、正しいメールが届きづらくなることがあってはならない。

「止める」と「届ける」を両立するために。
（正しい）送信者の皆様のご協力、受信事業者側の相互協力で、安全なメッセージング環境へ

© KDDI CORPORATION

Spark Your Journey KDDI

Spark Your Journey

KDDI

「つなぐチカラ」を進化させ、
誰もが思いを実現できる社会をつくる。

KDDI VISION 2030

