報道関係各位

2025 年 12 月 19 日
トビラシステムズ株式会社

トビラシステムズ「スミッシングトレンドレポート 2025」を公開

～クレジットカード会社や宅配事業者をかたる SMS 急増、生成 AI 悪用で犯行効率化か～

特殊詐欺やフィッシング詐欺の対策サービスを提供するトビラシステムズ株式会社（本社：愛知県名古屋市、代表取締役社長：明田 篤、証券コード：4441、以下「トビラシステムズ」）は、独自の迷惑情報データベースをもとに、昨今増加する SMS を悪用したフィッシング詐欺「スミッシング」について調査し、2025 年に流行した手口の傾向をまとめた「スミッシングトレンドレポート 2025」を公開します。

＜調査サマリー＞

- スミッシングトレンドワードは「カード」「荷物」、金融機関や宅配関連が頻出
- 1 位は 5 年連続で宅配事業者、SMS 文面の変化や「春節」に特徴的な動き
- 2 位は金融・決済サービス、前年比 3 倍に急増、大手銀行かたりからクレカかたりに変化
- 3 位は官公庁、「国税庁」かたる SMS が急増、法人口座を狙うフィッシングも
- スミッシングで悪用されたブランド名ランキング、1 位は「Mastercard」
- 多様な詐欺 SMS の文面が発生、生成 AI 悪用で大量作成・効率化の可能性

■スミッシングトレンドワードは「カード」「銀行」など金融関連が頻出

スミッシングとは、「**SMS**」と「**フィッシング**」を組み合わせた造語で、SMS を悪用したフィッシング詐欺を指します。スマートフォン・携帯電話の普及や、インターネットサービスの利用機会増加などに伴い、被害が拡大しています。

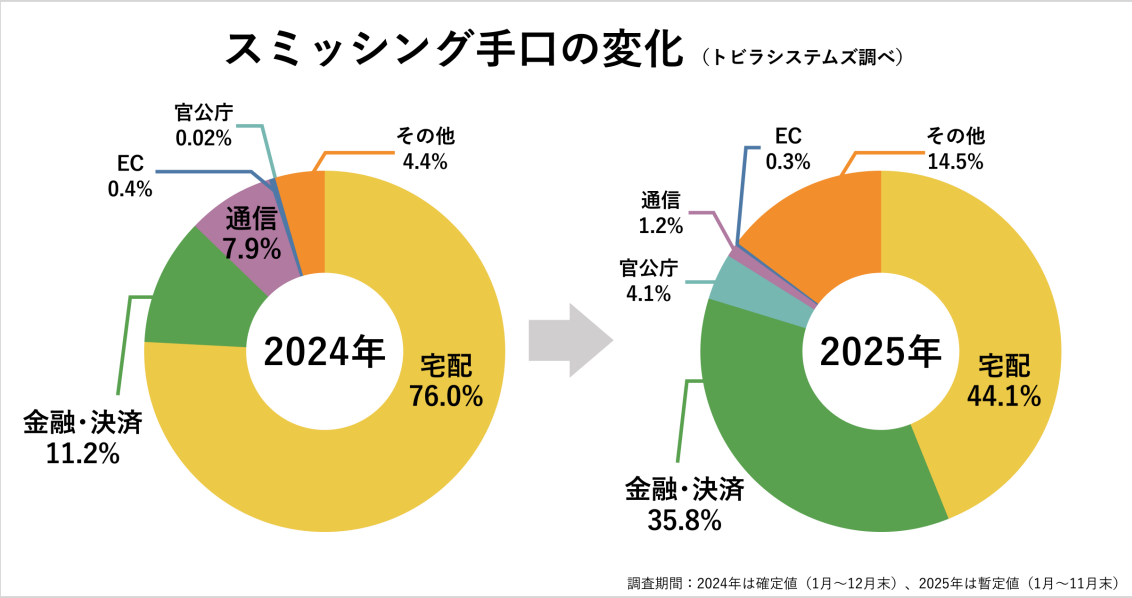
ワードマップに登場する単語は、トビラシステムズの調査において、2025 年にスミッシングの文面で頻出した単語です。文面に多く使われた単語ほど、大きく表示されています。

2025 年は、金融機関をかたる SMS に関する「**カード**」や「**銀行**」、**金融機関名**などが頻出しました。また、宅配便の不在通知を装う SMS に関連して「**荷物**」や「**配達**」、**宅配事業者名**などが目立ちました。スミッシングの文面でよく使われる単語として、「**制限**」「**確認**」「**利用**」「**停止**」など、緊急性を連想させるワードも多く出現しました。ワードマップを参考に、スミッシング対策にお役立てください。

■2025 年は金融機関をかたる SMS の割合が急増、前年比 3 倍

トビラシステムズの調査で、2025 年に確認されたスミッシング手口の 1 位は宅配事業者をかたる SMS（44.1%）でした。 2 位は金融・決済サービスをかたる手口（35.8%）で、手口全体に占める割合が昨年比で 3 倍以上に増加しています。 3 位は官公庁をかたる手口（4.1%）がランクインしました。

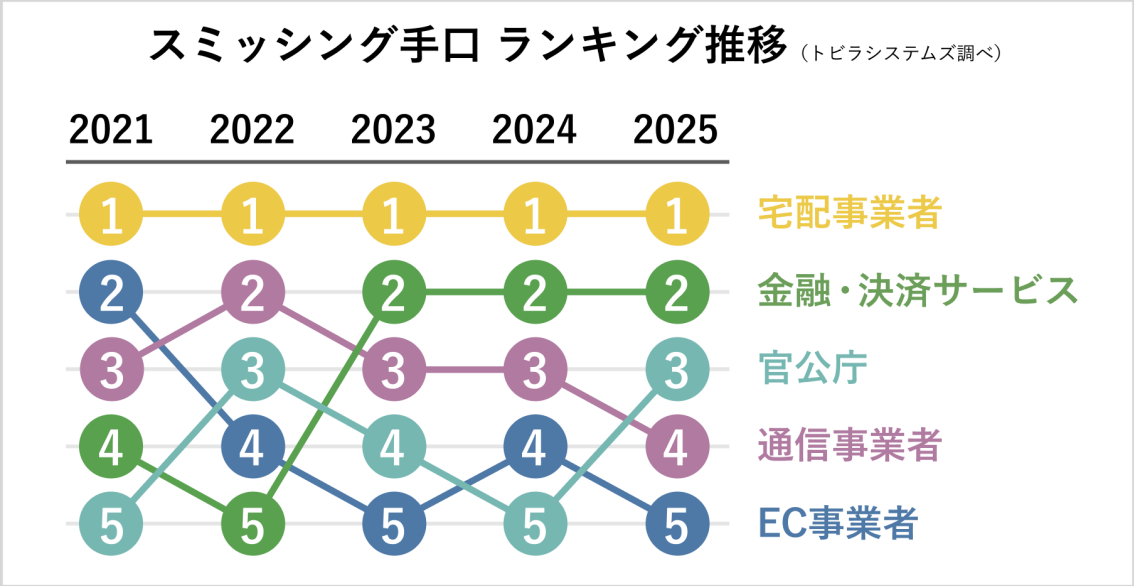
また、多種多様な企業名やブランド名をかたる手口が増えていることから、その他の手口に占める割合が大幅に増加しました。



トビラシステムズで観測したスミッシングの手口の割合を 5 年間の推移で見ると、2021 年から 2025 年まで 5 年連続で宅配事業者をかたる手口が 1 位となりました。

金融・決済サービスをかたる手口は、2023 年に急増し 2 位になってから、現在まで高水準で発生が続いています。

通信事業者・官公庁・EC 事業者をかたる手口は、時期や社会情勢などによって動きが変化しています。昨年にかけて緩やかに減少傾向だった官公庁をかたるスミッシングが、今年再び上昇し 3 位となりました。



■スミッシングで悪用されたブランド名ランキング、1 位は「Mastercard」

2025 年にスミッシングで悪用されたブランド名のトップ 3 は、1 位「**Mastercard**」、2 位「**佐川急便**」、3 位「**りそな銀行**」でした。

スミッシングで悪用されたブランド名ランキング
（トビラシステムズ調べ）

順位	2024年
1	三菱UFJ銀行
2	SoftBank
3	KDDI
4	東京電力
5	JCB
6	りそな銀行
7	Telegram
8	docomo
9	アイフル
10	みずほ銀行

順位	2025年	前年比
1	Mastercard	↑
2	佐川急便	↑
3	りそな銀行	↑
4	三井住友カード	↑
5	Apple	↑
6	国税庁	↑
7	東京電力	↓
8	WhatsApp	↑
9	日本郵便	↑
10	セゾンカード	↑

宅配事業者　金融・決済サービス　通信事業者　官公庁　その他

2025 年の傾向として、「**Mastercard**」「**三井住友カード**」「**セゾンカード**」など、クレジットカードのブランド名を悪用する手口が目立ちました。さらに、「**佐川急便**」「**日本郵便**」などの宅配事業者名が上位にランクインしました。

また、「**Apple**」をかたる SMS が 5 位に、「**国税庁**」をかたる SMS が 6 位に急上昇しました。

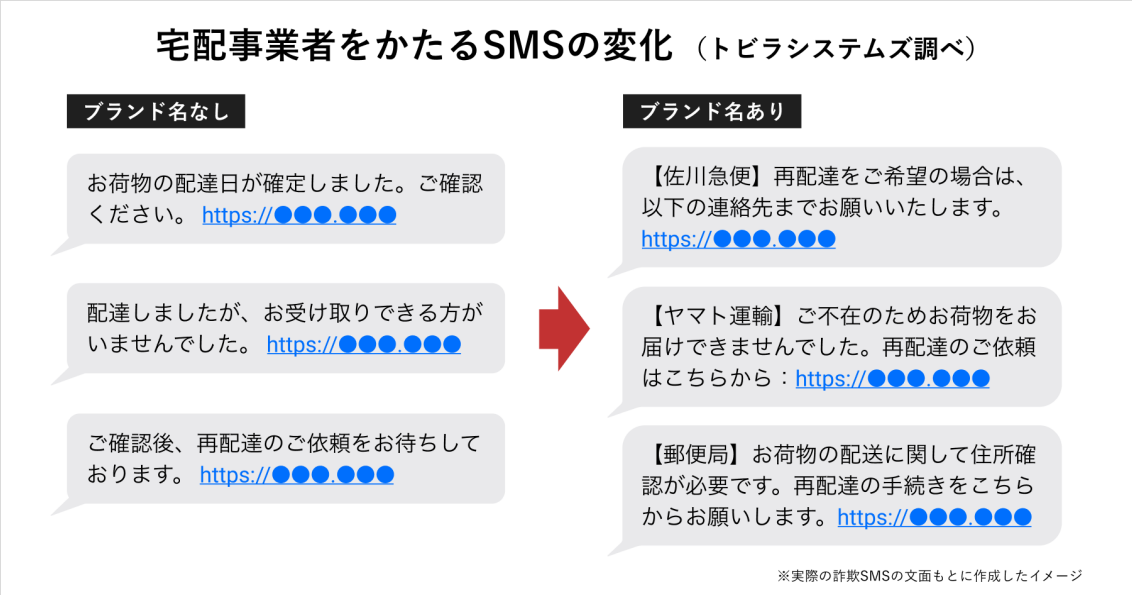
“電気料金の未納”や“送電停止”などの文面が特徴の「**東京電力**」をかたる SMS は、昨年から高水準で発生が続き 7 位となりました。世界的に広く使用されているメッセージアプリ「**WhatsApp**」を装う SMS も増加し、8 位となりました。

■2025 年のスミッシング三大手口を解説

2025 年に発生したスミッシングで特に多かった 3 つの手口について解説します。

1 位：宅配事業者をかたる手口

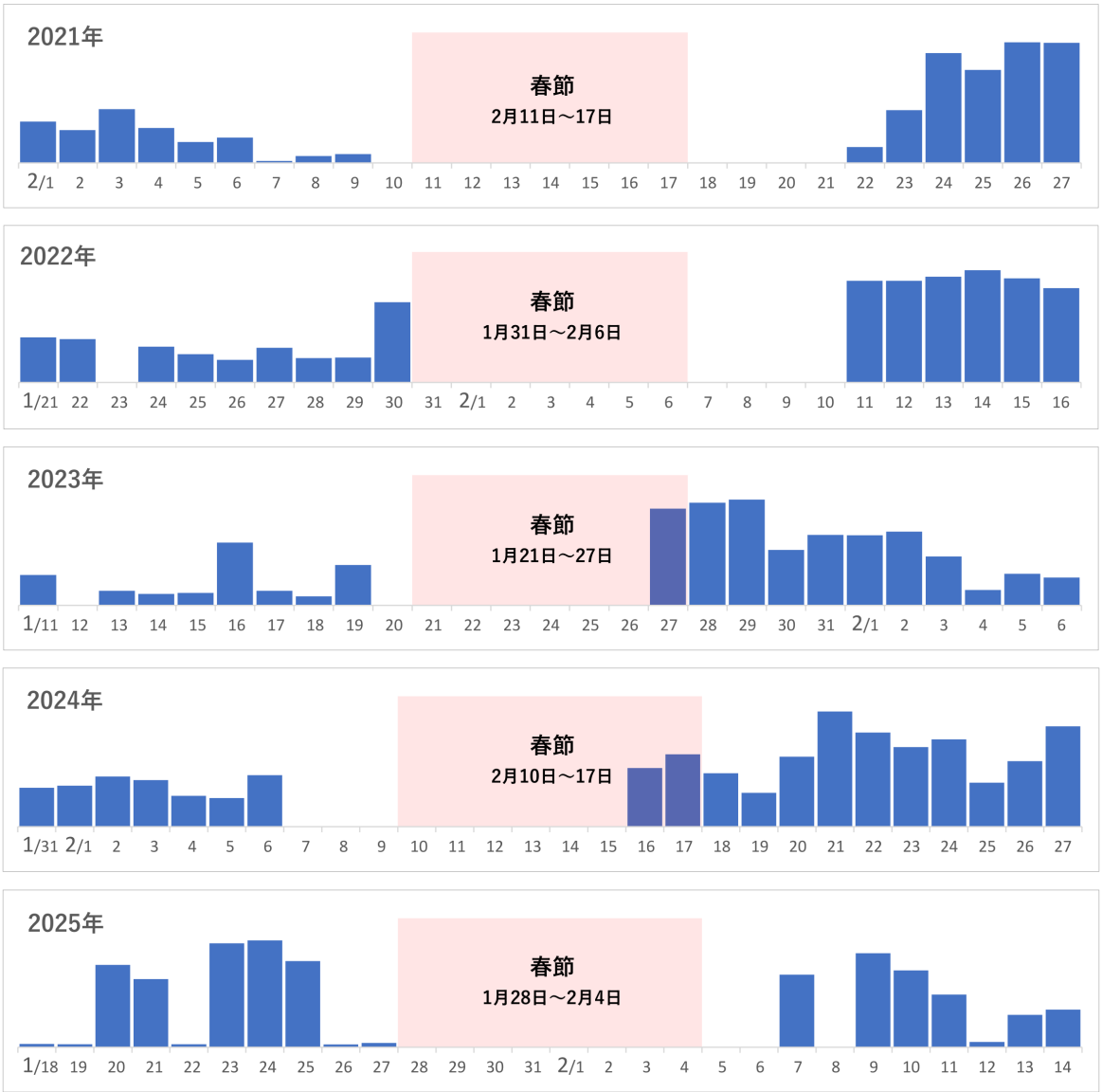
宅配事業者をかたる SMS の特徴として、これまでは特定の事業者名を記載せず不在通知を装う汎用的な文面が大多数を占めていました。しかし、2025 年は「**佐川急便**」「**ヤマト運輸**」「**日本郵便**」など、事業者名を記載した手口が目立ちました。



トビラシステムズの調査では、例年、旧暦の正月「**春節**」の休暇前後に宅配便の不在通知を装うスミッシングが大幅に減少し、春節が明けると元の水準に戻る特徴的な動きが確認されています。このことから、主に春節を祝う習慣があるアジア諸国を拠点とする犯罪グループが、これらのスミッシングに関係している可能性も推測されています。

なお、2026 年の春節の休暇は 2 月 15 日～23 日で、この期間の前後にも同様の傾向が発生する可能性があります。

春節における宅配便関連の詐欺SMSの動き（トビラシステムズ調べ）



2 位：金融・決済サービスをかたる手口

金融・決済サービスをかたる手口では、2024 年は大手銀行や地方銀行を装う SMS が目立った一方、2025 年は**クレジットカード会社をかたる SMS** が急増しました。2025 年にスミッシングで悪用された金融・決済サービスのブランド名トップ 10 のうち、クレジットカード会社が 7 つを占めています。

スミッシングで悪用された金融・決済サービスのブランド名
（トビラシステムズ調べ）

順位	2024年
1	三菱UFJ銀行
2	JCB
3	りそな銀行
4	アイフル
5	みずほ銀行
6	広島銀行
7	三井住友銀行
8	d払い
9	静岡銀行
10	岩手銀行

順位	2025年
1	Mastercard
2	りそな銀行
3	三井住友カード
4	セゾンカード
5	三菱UFJニコス
6	アメリカン・エキスプレス
7	SBI証券
8	JCB
9	PayPay
10	VISA

2025 年上半期には、インターネット証券口座のアカウントが不正に乗っ取られ、株を勝手に売買される事案が急増しました。被害の一因として、フィッシング詐欺によりログイン ID・パスワードなどが盗み取られ、不正ログインに悪用された可能性があり、金融庁や各証券会社が注意喚起を行いました。トビラシステムズの調査では、この 1 年間で 6 社の証券会社をかたる SMS が観測されました。

【スミッシングに悪用された証券会社名】※2025 年トビラシステムズ調べ
楽天証券、SBI 証券、三菱 UFJ モルガン・スタンレー証券、野村證券、マネックス証券、インタラクティブ・ブローカーズ証券

証券会社をかたるSMSの文面例（トビラシステムズ調べ）

【楽天証券】セキュリティ強化に伴い、24時間以内に再ログインし口座有効化をお願いします。 https://●●●.●●●

【野村證券】お客様の取引を一時的に制限中です。詳細はこちらをご確認ください。 https://●●●.●●●

【SBI証券】お客様の口座を保護するため、24時間以内に二要素認証を設定してください。リンク: https://●●●.●●●

【MONEX証券】疑わしい活動が検出されましたので、直ちにログインしてご確認ください。 https://●●●.●●●

【三菱UFJ証券】疑わしい活動が検出されましたので、直ちにログインしてご確認ください。 https://●●●.●●●

IBKR：新契約は2025年8月発効、未同意は取引停止の恐れあり、速やかに https://●●●.●●● へ

※実際の詐欺SMSの文面もとに作成したイメージ

3 位：官公庁をかたる手口

2025 年は「**国税庁**」を名乗る SMS の発生件数が著しく増加し、トビラシステムズの調査では、国税庁をかたる SMS が前年比約 152 倍も確認されました。特に、2 月～3 月の**確定申告シーズン**を狙い、SMS から国税庁の偽サイトに誘導し、税金納付の名目で電子マネー支払いを求める手口が多発しました。

さらに、2025 年 3 月中旬には「**法務局**」や「**北海道警察**」をかたる SMS が発生し、誘導先の偽サイトで法人の銀行口座番号や口座残高の入力、企業の代表者の情報、銀行取引に関する書類のアップロード等を求めるフィッシングが確認されました。個人のみならず、法人の情報や資産がフィッシングの標的として狙われていることが伺えます。

■多種多様な手口が発生、生成 AI 悪用で効率化か

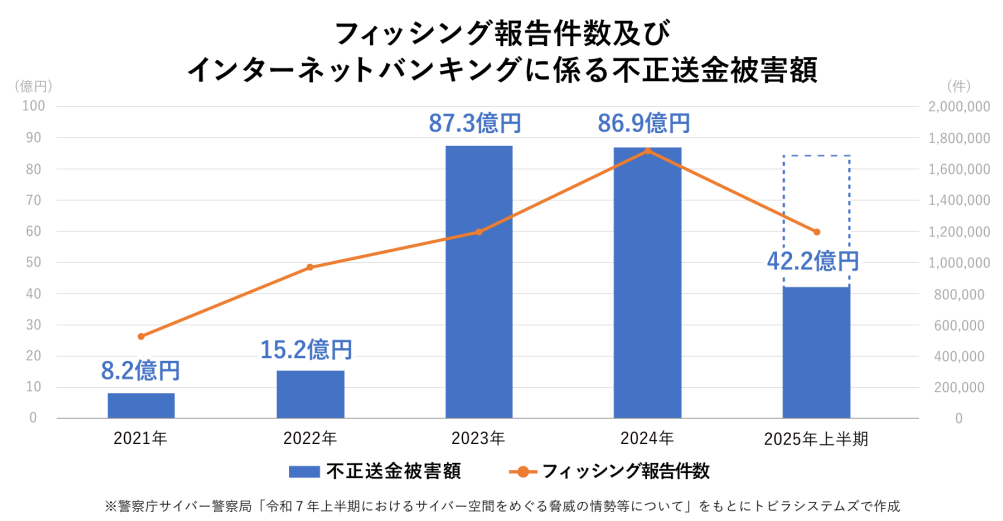
2025 年は、宅配事業者や金融・決済サービス、官公庁をかたる手口のほか、多種多様な企業名やブランド名をかたる SMS が確認されました。

生活インフラに関連の深い「**東京電力**」をかたる SMS は、年間を通じて継続的に発生しました。また、「**Google**」「**Apple**」「**Amazon**」「**Netflix**」などの身近なインターネットサービスや、「**Telegram**」「**WhatsApp**」「**LINE**」といったメッセージアプリをかたる SMS も確認されています。

文面のバリエーションが増加し、多い日には 5,000 種類以上の文面が確認されました。このことから、犯行グループが生成 AI を悪用し、大量の文面を効率的に作成している可能性が考えられます。

■インターネットバンキングに係る不正送金被害額は上半期で 42.2 億円

フィッシング報告件数およびインターネットバンキング不正送金被害額は年々増加しており、深刻な社会問題となっています。警察庁の発表では、2024 年のインターネットバンキング不正送金被害額は 86.9 億円で、高水準で推移が続いています。2025 年上半期は既に 42.2 億円に達し、前年同期比で 1.7 倍に上っています。



＜参考資料＞

令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁サイバー警察局）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

■スミッシングの被害にあわないための対策

スミッシングの被害にあわないために、日頃から対策を徹底してください。また、年末年始に家族や知人など周囲の方への注意喚起や、対策方法の見直しを行ってください。

迷惑 SMS 対策サービスで、詐欺の可能性がある SMS に対して自動で警告表示や迷惑フォルダ振り分けを行うことが可能です。日頃の対策とあわせてご活用ください。

＜スミッシング被害を防ぐ３つの対策＞

◉身に覚えのないメールや SMS が届いた場合、文面に添付された URL に触らない
◉日頃利用するサービスは、公式アプリやブックマークしたサイトから情報を確認
◉迷惑 SMS 対策サービスを活用し、フィッシング詐欺などの不審な SMS を自動で遮断

トビラシステムズの迷惑 SMS 対策サービス
https://tobilaphone.com/mobile/

詐欺 SMS の検知状況をリアルタイムに観測し可視化する「詐欺 SMS モニター」
https://smon.tobila.com/

■トビラシステムズについて

テクノロジーで社会課題の解決を目指し、特殊詐欺やフィッシング詐欺、グレーゾーン犯罪撲滅のためのサービスを提供しています。詐欺電話・詐欺 SMS 等の情報を収集・調査してデータベースを構築し、自動でフィルタリングする「迷惑情報フィルタサービス」は、固定電話、モバイル、ビジネス向けに展開し月間約 1,500 万人にご利用いただいています。

＜会社概要＞

会社名　　：トビラシステムズ株式会社
代表者　　：代表取締役社長　明田 篤
証券コード：4441（東証スタンダード市場）
設立　　：2006 年 12 月 1 日
所在地　　：愛知県名古屋市中区錦 2-5-12 パシフィックスクエア名古屋錦 7F
公式サイト：https://tobila.com/

＜本件に関する報道関係のお問い合わせ先＞

トビラシステムズ株式会社　広報担当
電話番号：050-3646-6670（直通）
お問い合わせフォーム：https://tobila.com/contact/