blastmail blastengine

現代に不可欠なメールセキュリティ対策

BIMI 完全ガイド

- なりすましメール対策
- ブランド認知・開封率向上

BIMI(Brand Indicators for Message Identification)とは?

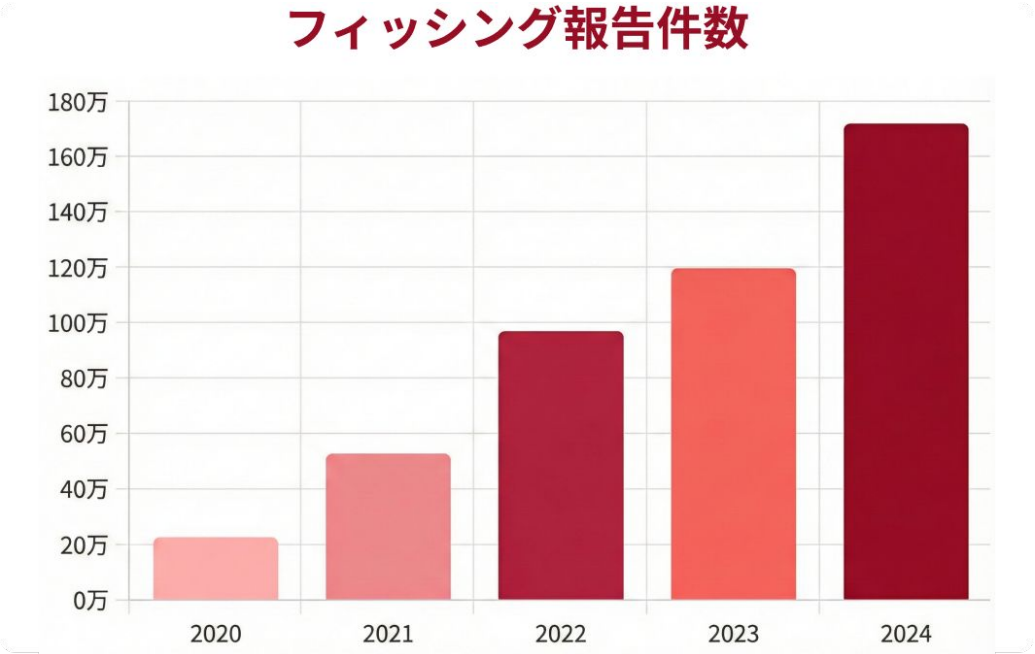
BIMI（Brand Indicators for Message Identification）とは、メール受信時に送信元のロゴマークを表示させることで、そのメールが正規の送信者から送られたものであることを証明する技術標準です。

単なるアイコン設定ではなく、厳格なドメイン認証(DMARC) に基づいたセキュリティの証明で、なりすまし・フィッシングメールから顧客とブランドを守ります。

深刻化するフィッシング詐欺の実態

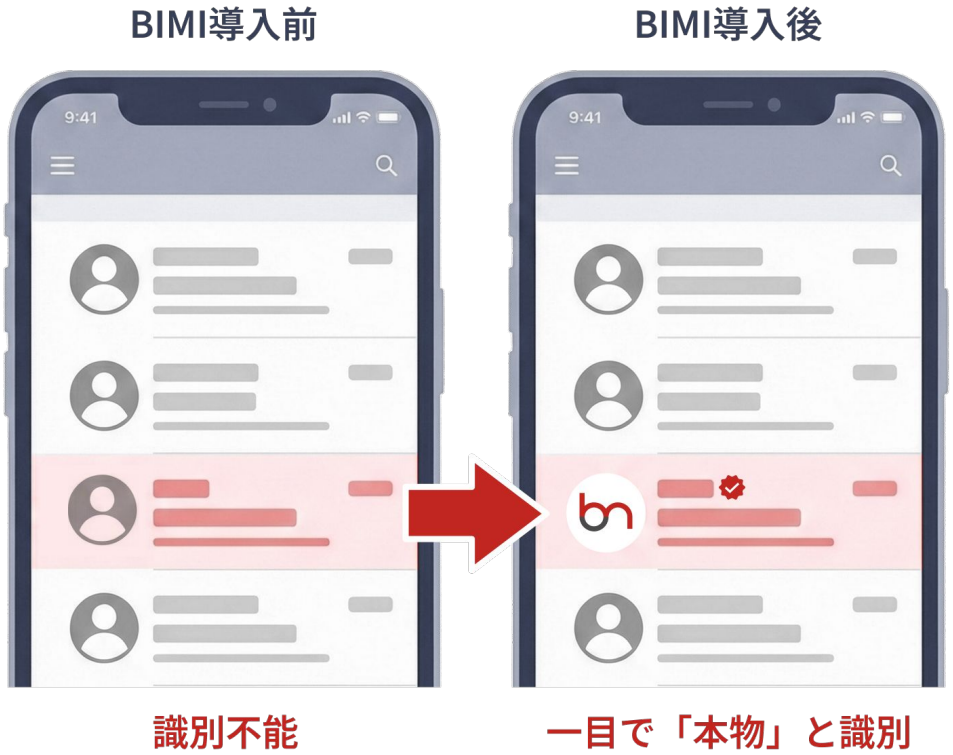
日本国内におけるフィッシング詐欺の報告件数は毎年上昇しており、2024年は年間170万件を突破しました。

スマートフォン利用者を狙った金融機関・通信事業者を騙る巧妙な手口が常態化しており、被害の入口は私たちの日常に深く入り込んでいます。



出典：フィッシング対策協議会フィッシングレポート　2025

従来のメールは「誰から来たか」が見分けられない



✔ロゴ表示

企業ロゴが表示されるため、視認性が向上。受信者は安心してメールを開封し内容を確認することができます。

✔認証マーク表示

Gmailでは、BIMIとVMCにより「青いチェックマーク (認証バッジ)」が付与されます。

「なりすましメール対策」で顧客を守る

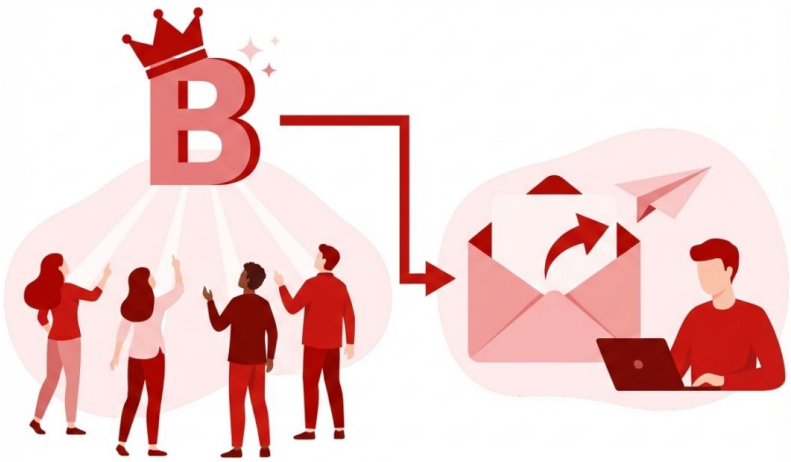
BIMIの導入には、SPF/DKIMの認証結果を厳格に制御する「DMARCポリシー（隔離・拒否）」の設定が必須です。

ブランドロゴや認証マークが表示されるということは、セキュリティ対策が万全で、なりすましではない『本物のメール』であることの証明になります。

「ブランド認知」と「開封率」の向上

受信トレイにロゴマークが表示されることで、数あるメールの中でも一目で送信元を認識させることができます。

視覚的なインパクトは、メールの開封率向上に直結し、継続的なブランディング効果をもたらします。



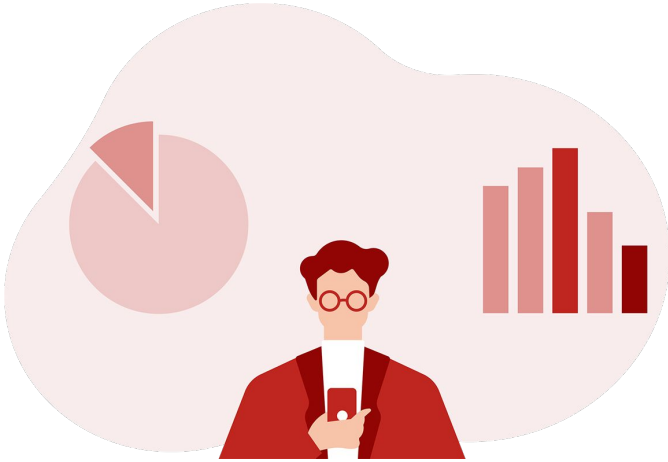
メールマーケティングの効果改善

✔到達率・開封率・クリック率が向上

BIMIを実装することで送信元の正当性が可視化され、メールの信頼性が向上します。その結果、重要なお知らせやプロモーションメールの到達率・開封率・クリック率等の改善が期待できます。

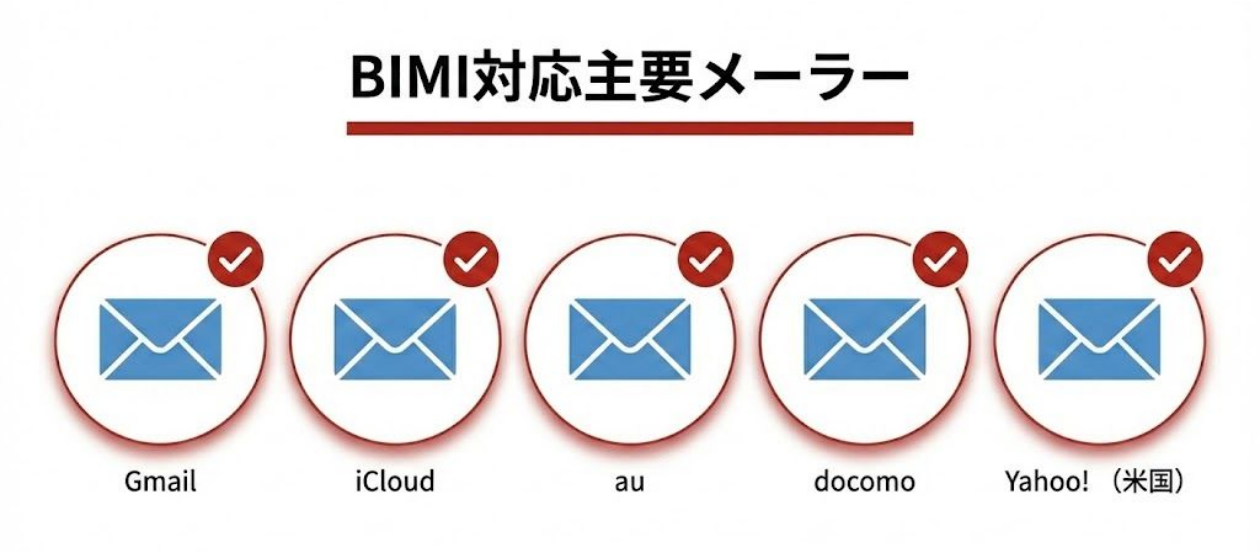
✔競合と差別化できる

受信トレイ内での視認性を高めることで、競合他社のメールに埋もれないブランドポジションを構築し、差別化を図ることが可能です。



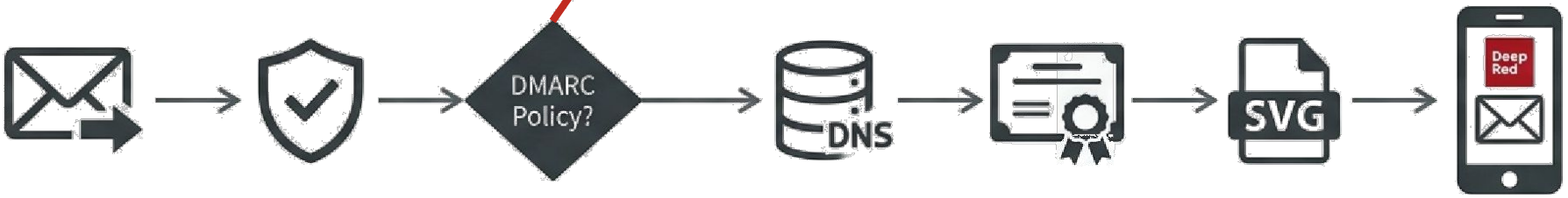
BIMIに対応しているメーラー

ロゴ表示には、BIMIに準拠したメール受信環境が必要です。



BIMIでロゴが表示されるまでの流れ

受信サーバーが DMARCポリシー (quarantine/reject) を確認



送信者

認証チェック
(SPF/DKIM/DMARC)

BIMIレコードを
確認

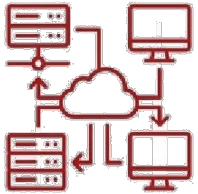
VMC検証

SVG取得

受信者

ロゴ表示

BIMIでロゴを表示させるための4つの準備

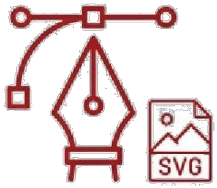


1. SPF/DKIM/DMARCの設定

送信ドメイン認証の整備

2. DMARCポリシーの強化

p=quarantineまたは p=reject



3. SVGロゴの準備

SVG Tiny PS形式 (高セキュリティな形式)

4. VMCの取得

商標登録済みのロゴに対する証明書

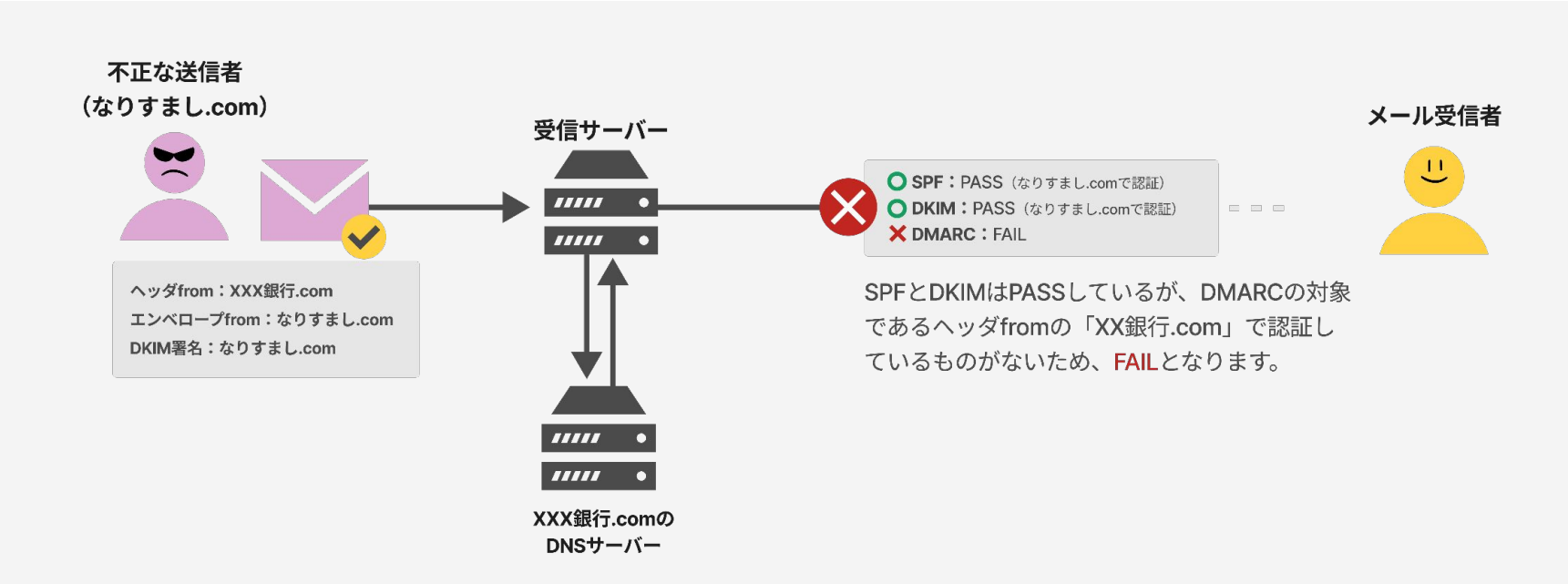
SPF・DKIM・DMARCとは？

メール送信における「なりすまし」や「改ざん」を防ぐため、現在では以下の 3つの送信ドメイン認証技術を組み合わせて導入することが標準となっています。

認証技術	仕組み	役割
SPF	ドメイン管理者が、メール送信を許可するサーバーのIPアドレスをDNS（SPFレコード）に登録します。	受信側は、届いたメールが登録済みの正規のIPアドレスから送られてきたかを確認し、不正なサーバーからのなりすましを検知します。
DKIM	送信メールに電子署名を付与します。受信側で署名を検証することで、メール内容の改ざん検知と送信元の正当性の証明を行います。	受信側で署名を検証することで、配送途中でメールの本文や件名が書き換えられていないか（改ざん検知）、および送信元の正当性を証明します。
DMARC	SPFやDKIMの認証に失敗したメールを「どう扱うか（そのまま通す・隔離する・拒否する）」というポリシーをDNSで宣言します。	ユーザーが目にする差出人の詐称を厳格に検証します。また、認証結果のレポートにより、自社ドメインの不正利用状況を可視化できます。

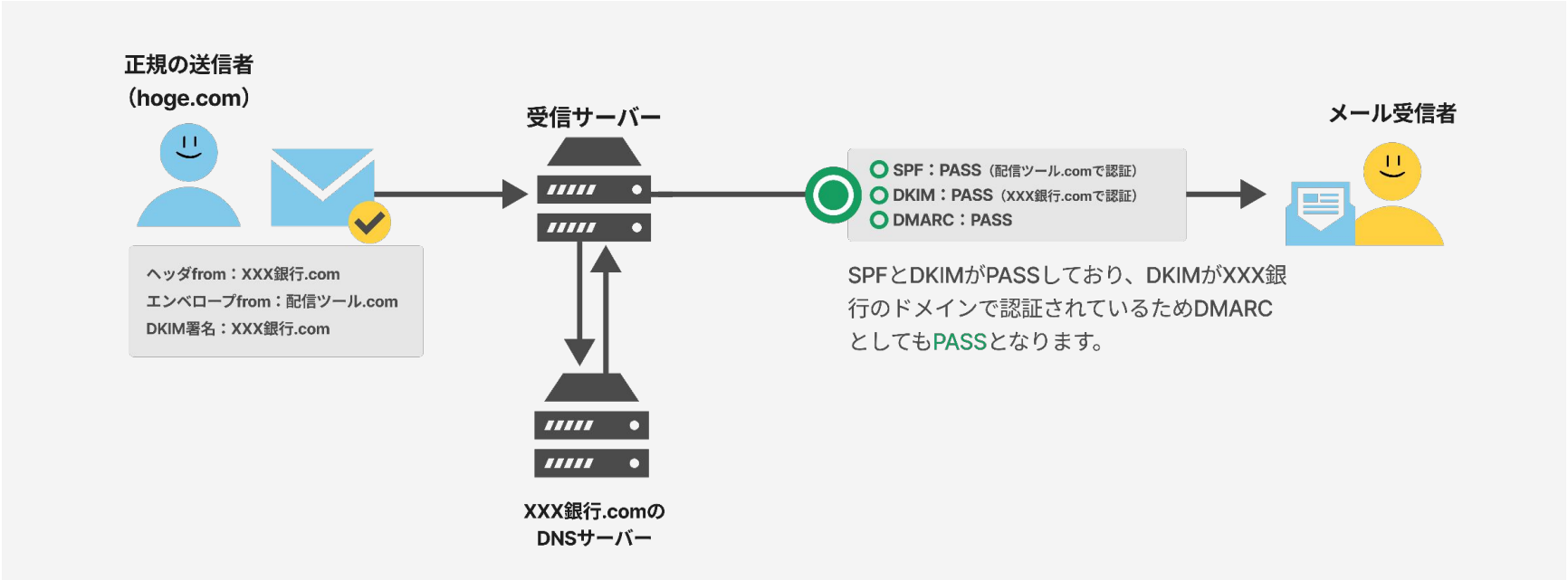
1. SPF/DKIM/DMARCの設定（DMARCの認証プロセス）

SPFとDKIMの双方の認証が成功(PASS)であり、かつ、**どちらかのアライメントが取れていたら成功**となります。DMARCアライメントとはヘッダfromのドメインと認証に使われたドメインが一致しているかのことです。



1. SPF/DKIM/DMARCの設定（DMARCの認証プロセス）

一般的にサードパーティーのメール配信ツールなどを利用する際は、DKIMの秘密鍵をツール側に登録することで、配信ツール側が「作成者署名」をして、DMARC のアライメントを取ることができます。



2. DMARCポリシーの強化

BIMIの導入には、DMARCポリシーを「quarantine（隔離）」または「reject（拒否）」に設定することが必須条件です。しかし、認証設定が不完全なままポリシーを厳格化してしまうと、本来届くべき自社メールまでブロックされてしまうリスクがあります。以下の手順を踏んで、安全に移行を進めましょう

ポリシー (p=)	仕組み	BIMI表示	役割
none	監視、そのまま配信	不可	DMARC認証に失敗したメッセージは、監視はされますがそのまま受信者の受信トレイに配信される
quarantine	迷惑フォルダへ隔離	**可**	DMARC認証に失敗したメッセージを、受信トレイではなく迷惑メールフォルダに隔離される
reject	拒否、配信されない	**可**	DMARC認証に失敗したメッセージは、受信者に配信されない

1. **現状確認：**自社から送信されるメールが正しく認証(SPF/DKIM/DMARC)をパスしているか確認
2. **関係各所へのアナウンス：**事前に社内や取引先へ状況を共有しておく
3. **段階的なポリシー移行：**配信状況を慎重にモニタリングし、少しずつポリシーを強化していく

3. SVGロゴの準備

4. VMCの取得

VMC（認証マーク証明書）とは?

認証局が「組織がロゴを正式に所有している」ことを証明する電子証明書です。 Gmailなどでロゴを表示させるためには、VMCの取得が必須条件です。

※「なりすまし・フィッシング対策を視覚的に強化　- BIMI/VMC | GMOブランドセキュリティ」より引用し弊社で編集して作成

BIMI導入までの5ステップ

STEP.1
DMARC設定

DMARCは送信ドメインのなりすましを防ぐ認証プロトコルです。 BIMIを有効にするためには、DMARCポリシーを、「 quarantine」または 「reject」に引き上げる必要があります。

STEP.2
ブランドの商標登録

Gmail等でブランドロゴを表示させるには、電子証明書「 VMC」の取得が不可欠です。この VMC 発行の絶対条件として、対象ロゴが「商標登録済み」であることが求められます。

STEP.3
SVGロゴ画像を準備

BIMIで表示させるロゴには、一般的な SVG形式ではなく、SVG Tiny 1.2をベースにセキュリティ制限を加えた「 SVG Tiny PS (Portable/Secure)」プロファイルが必須となります。

STEP.4
VMCの取得

VMCは「ロゴのパスポート」とも呼ばれ、認証局が組織の実在性と商標権を証明するものです。法的書類に基づく厳格な審査を経て発行されます。

STEP.5
BIMIの利用設定

HTTPSサーバー上に「 SVGロゴ」と「 VMC証明書（PEM形式）」を公開し、その公開 URLを記述したBIMI用TXTレコードを DNSに追加します。

BIMIについて詳しく話を聞く ▸

BIMI導入で信頼を可視化し、選ばれるブランドへ

- ☑️ なりすまし・フィッシングから顧客を守る。
- ☑️ 「本物」であることを視覚的に証明する。
- ☑️ 開封率を高めメールマーケティングの成果を最大化する。

お問い合わせ　資料の不明点やご利用に関して詳細の確認はお気軽にご相談ください

「BIMIの導入を検討している」「BIMIについてもっと詳しく知りたい」など、どんなことでも**お気軽にご相談ください**。

無料相談（オンライン MTG）

下記リンクより日程調整が簡単にできます。

日程調整ツール

https://form-gw.hm-f.jp/hai2appoint/jYG1TAIdQuSd98fUQu341zEzNEBici1hMDUuaG0tZi5qcA837da

日程調整はこちら

お問い合わせフォーム

下記URLよりお問い合わせください。

お問い合わせフォーム

https://blastmail.jp/blog/download/bimi

お問い合わせはこちら

サービス紹介

blastmail
ブラストメール

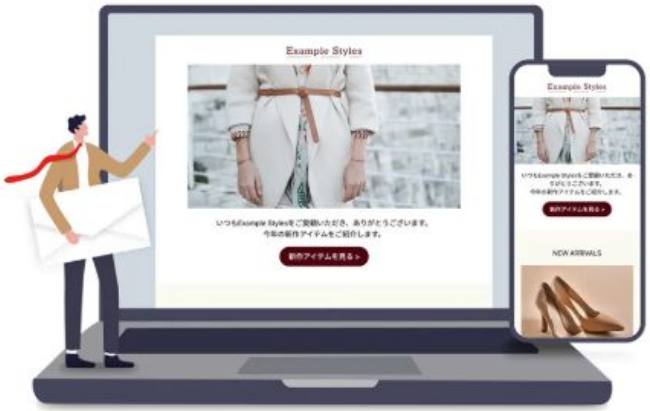
導入数シェア15年連続No.1のメール配信システム

20年以上にわたるサービス提供で培ったノウハウを活かし、国内トップクラスの配信速度と到達率を誇る高品質なメール配信システムです。

より多くの企業様にご利用いただけるよう、業界最安クラスの価格と使いやすさにこだわったシンプルな操作性で提供しています。

27,000社以上の顧客基盤を活かし、大規模配信を低コストで実現します。

無料トライアル　資料ダウンロード



大手企業、自治体に選ばれ
導入社数27,000以上

サービス紹介

blastengine
ブラストエンジン

API連携・SMTPリレー特化のメール配信システム

お客様のシステムとブラストエンジンをAPIやSMTPリレーで連携することで簡単に一斉メール配信やトランザクションメールを配信することができます。

メールサーバーの運用・メンテナンスはブラストエンジンで行うため、常に高いIPレピュテーションを保ってメールを送ることができ、エンジニアを面倒な業務から解放します。

無料トライアル　資料ダウンロード

会社概要

会社名	株式会社ラクスライトクラウド
事業内容	クラウド型ソフトウェアサービスの提供
所在地	〒151-0051 東京都渋谷区千駄ヶ谷5-27-5 リンクスクエア新宿7F
代表取締役	大塚 智史
資本金	1800 万円
TEL	03-6675-9281

URL	https://blastmail.jp
関連会社	株式会社ラクス https://www.rakus.co.jp/
取引銀行	三菱UFJ銀行
資格等	プライバシーマーク取得番号 第10821806 号 一般第二種電気通信事業者 A-15-5714