

すぐできる！ ドメイン認証の設定方法 (SPF DKIM DMARC)

メール配信の到達率を最大化する
SPF / DKIM / DMARC設定 の徹底解説

1. はじめに

- 1.ドメイン認証未設定によるリスク
- 2.設定の前提:どこに設定する？

2. SPF／DKIM／DMARC 設定手順について

- 1.DNSサーバーの特定
- 2.3つの認証(SPF／DKIM／DMARC)設定
- 3.DNS登録に必要な3つの要素
- 4.SPFレコードの設定手順
- 5.DKIMレコードの設定手順
- 6.DMARCレコードの設定手順

3. Appendix

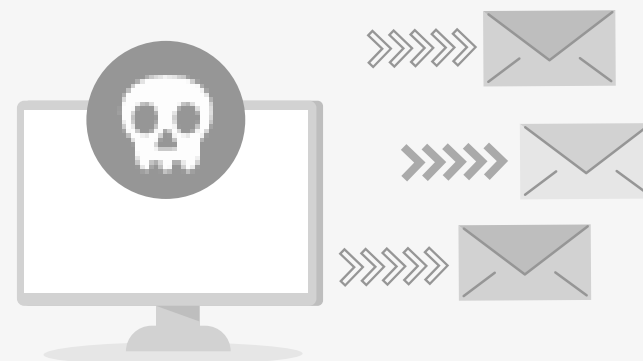
- 1.詳細情報

1. 到達率の著しい低下



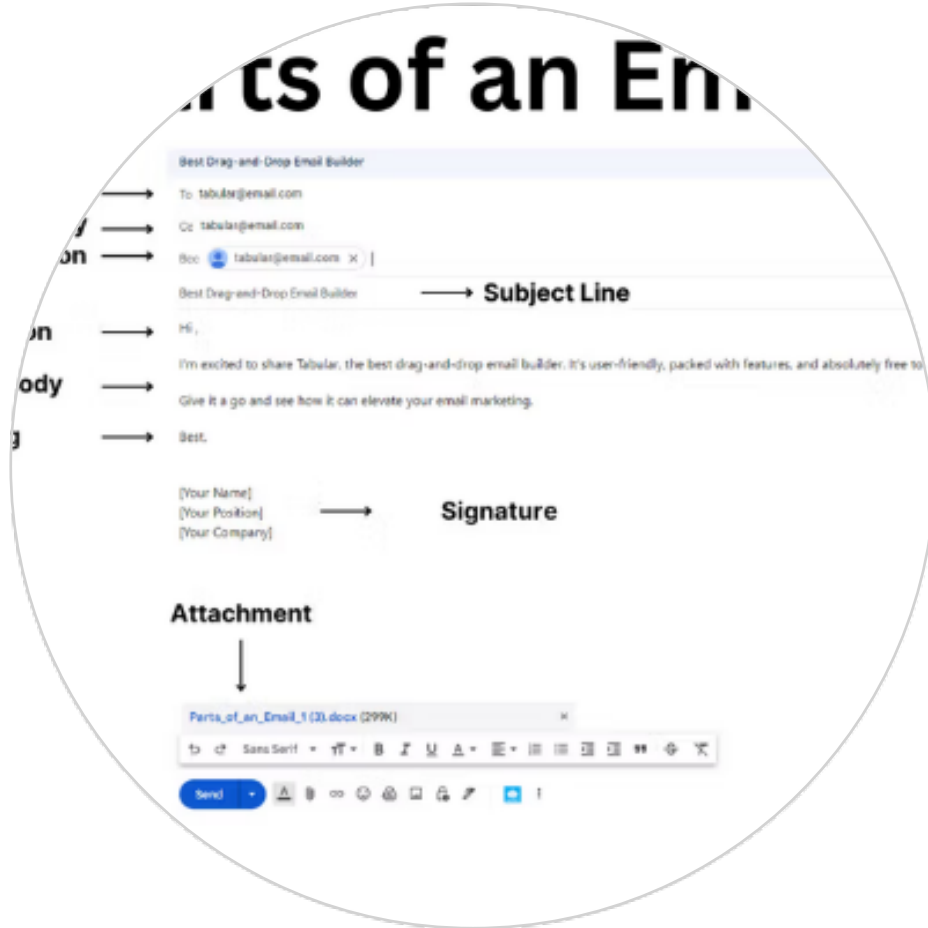
主要プロバイダによるフィルタリングが強化され、未認証のメールは自動的に「迷惑メールフォルダ」へ振り分け、または「配信拒否」の対象となります。

2. ブランド信頼の失墜



自社ドメインが「なりすましメール」の踏み台にされるリスクが高まります。
不正利用を妨げないことは信頼性低下につながる可能性があります。

設定の前提:どこに設定する？



「@以降」のドメインが対象

ドメイン認証は、使用しているメールアドレスの「@以降」に対して設定を行います。

例) support@haihaimail.jp

↑ このドメイン部分の設定を編集します

設定の前提:どこに設定する？

ドメイン認証(SPF・DKIM・DMARC)を有効化するには、
「ドメインの管理元」と「配信サービス(「楽楽メールマーケティング」)」の両方で設定が必要です。



設定手順 - STEP 1

DNSサーバーの特定

設定作業を行う「管理画面」を
見つけるための事前確認

管理サービスはどこ？

管理サービスを見つける方法



契約書の確認

ドメイン取得時の契約書や、月々の支払い明細（請求先）を確認しましょう。



IT部門・情シスへの確認

自社のネットワークやドメインを管理している部署（情報システム部・IT部門）へ、DNSサーバーの管理権限やログイン情報の所在を確認します。

主な代表サービス

お名前.com

ムームードメイン

XSERVER

AWS（Route53）

さくらインターネット

Cloudflare

設定手順 - STEP 2

3つの認証設定 (SPF/DKIM/DMARC)

それぞれの役割と、
なぜ「3点セット」で必要なのか

3つの認証の意味

到達率向上のためには、この「3点セット」での設定が推奨されます。

SPF



送信元サーバーの許可

送信元IPアドレスを検証し、許可されたサーバー以外からの「なりすまし」を防止します。

DKIM



「改ざん」を防ぐ証明

電子署名を付与し、メールが配送途中で改ざんされていないことを証明します。

DMARC



認証失敗時の指示

SPF／DKIMの認証失敗時に「拒否」や「隔離」を指定する、ドメイン保護の最終ラインです。

設定手順 - STEP 3

DNS登録に必要な 3つの要素

管理画面に入力する
「パズル」の正体を知る

DNS登録に必要な3要素

項目名	概要	具体的な入力例
ホスト名	レコードを紐づける場所	@ (空欄), _dmarc, s1._domainkey など
タイプ	レコードの種類	TXT
値 (Content)	認証の定義本文	v=spf1 include:spirit-p.jp ~all など

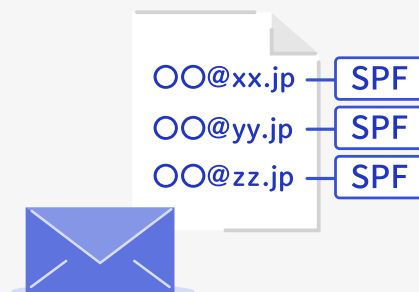
※ 利用する配信サービス(「楽楽メールマーケティング」)から提供される値を**そのままコピペ**するだけです。
本資料後半へ認証項目ごとに3要素情報を記載しております。

全角・スペース禁止



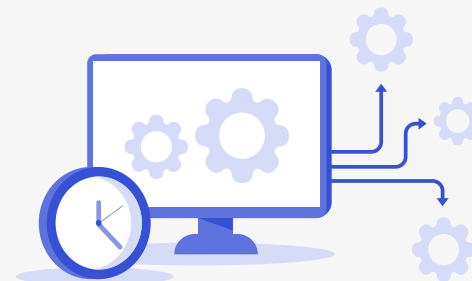
すべて「半角」で入力します。
末尾に不要なスペースが入らないよう注意してください。

統合の必要性



SPFは1ドメインに1つです。既存のものがある場合は上書きではなく「追記・統合」します。

反映待ち



保存後、世界中に反映されるまで数分～最大24時間程度かかる場合があります。

設定手順 - STEP 4

SPFレコードの設定手順

確認ツールからSPFレコード登録の有無を確認してください

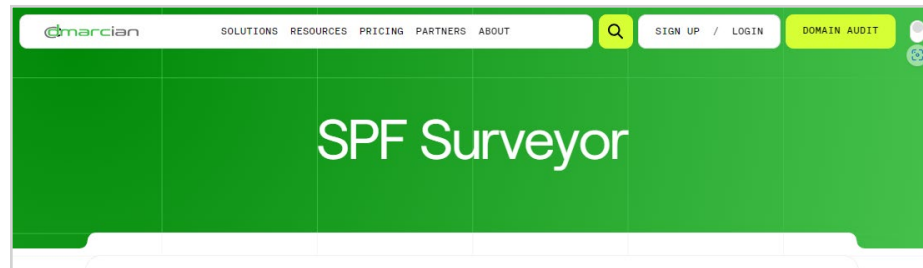
確認ツールはこちら

<https://dmarcian.com/spf-survey/>

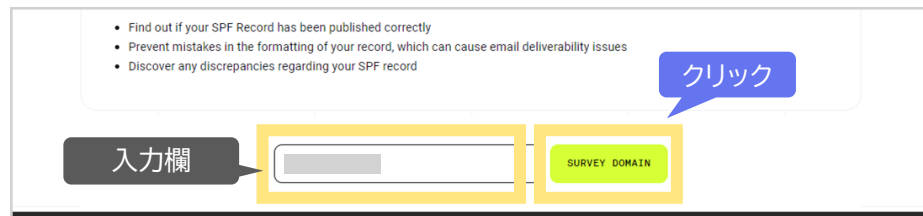
SPFレコードの設定状況確認方法

利用ツール:<https://dmarcian.com/spf-survey/>

Step1 ドメイン入力と実行



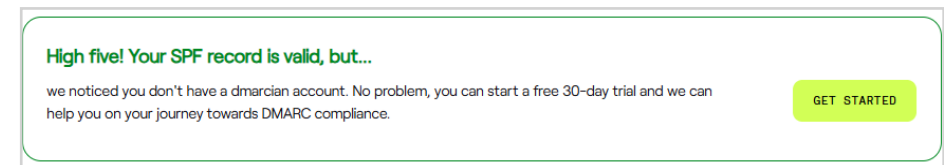
= 中略 =



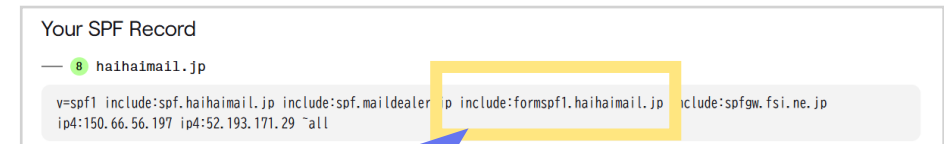
Fromアドレスのドメインを入力し、
ボタンをクリックします。



Step2 結果の確認と判定



= 中略 =



「楽楽メールマーケティング」の
レコードが追加されている

既存のレコード内に、
指定の記述が含まれていれば設定完了です。

CASE-A

既存のSPFレコードがある場合
→設定資料P16へ

②クリック

①Fromアドレスのドメインを入力
(@は含めずにご入力ください)

High five! Your SPF record is valid, but...
we noticed you don't have a dmarcian account. No problem, you can start a free 14-day trial and we can help you on your journey towards DMARC compliance.

GET STARTED

Access/bookmark this inspection at <https://dmarcian.com/spf-survey/?domain=haihaemail.jp>

既存のSPF設定内容が表示された場合

Fromアドレスのドメイン

EXPAND ALL COLLAPSE ALL

v=spf1 include:spf.haihaemail.jp include:spf.maildealer.jp include: jp ip4:150. .29 ~all

CASE-B

既存のSPFレコードが無い場合
→設定資料P17へ

②クリック

①Fromアドレスのドメインを入力
(@は含めずにご入力ください)

No SPF Record for this domain.
Let us help you get that fixed and start a free 14-day trial.

GET STARTED

Click here to read our "Getting Started with DMARC" guide.
Access/bookmark this inspection at <https://dmarcian.com/spf-survey/?domain=jupita.biz>

Fromアドレスのドメインを①へ入力後、ボタンをクリックし
No SPF Record for this domainと
メッセージが出てきた場合

CASE-A

既存のSPFレコードがある場合

High five! Your SPF record is valid, but...

we noticed you don't have a dmarcian account. No problem, you can start a free 14-day trial and we can help you on your journey towards DMARC compliance.

GET STARTED

Access/bookmark this inspection at <https://dmarcian.com/spf-survey/?domain=haihaimail.jp>

Click on nodes to expand.

EXPAND ALL COLLAPSE ALL

8 [redacted].jp
v=spf1 include:spf.haihaimail.jp include:spf.maildealer.jp include:[redacted]
ip4:150 [redacted].29 ~all

ここに設定されている内容が表示されます

DNSサーバー管理会社へ以下の文章をそのまま共有ください

※ご自身で設定される場合は赤文字をDNSサーバーのSPF項目へ追記してください。

既存のSPFレコードに「楽楽メールマーケティング」のレコード「**include:spf.haihaimail.jp**」を追加してください。

例)

既存のレコード:

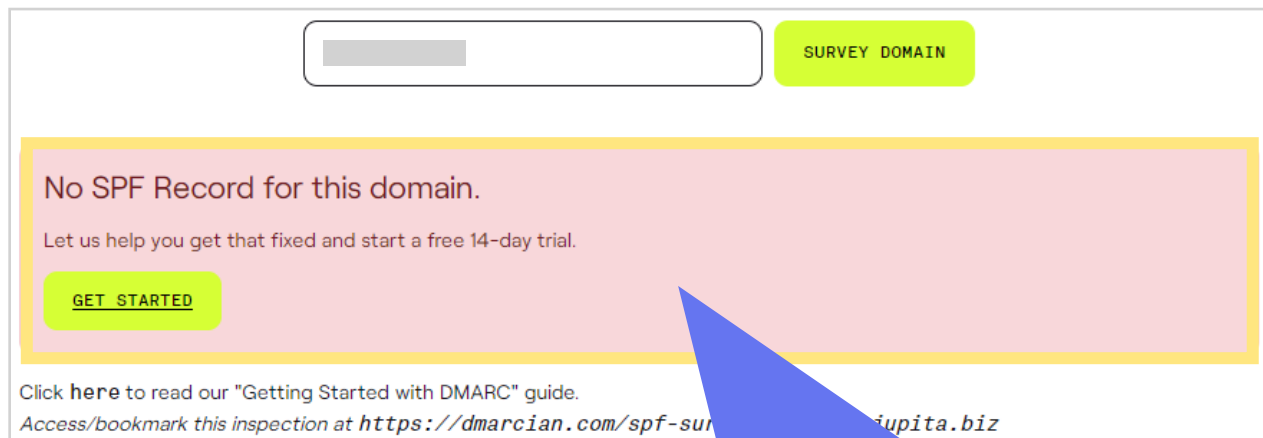
v=spf1 include:test.com ip4:000.00.00.000 ~all

追加後のレコード:

v=spf1 include:test.com ip4:000.00.00.000
include:spf.haihaimail.jp ~all

CASE-B

既存のSPFレコードが無い場合



Input field: [] SURVEY DOMAIN

No SPF Record for this domain.

Let us help you get that fixed and start a free 14-day trial.

[GET STARTED](#)

Click [here](#) to read our "Getting Started with DMARC" guide.
Access/bookmark this inspection at <https://dmarcian.com/spf-sur> [iupita.biz](#)

Fromアドレスのドメインを①へ入力後、ボタンをクリックし
No SPF Record for this domainと
メッセージが出てきた場合

【対応内容】

下記内容に沿って、DNSサーバーへ新規レコードを追加してください。

ホスト名	レコードタイプ
そのまま	TXT
内容	
v=spf1 ip4:送信メールサーバのIPアドレス include:spf.haihaimail.jp~all	
※ ip4:送信メールサーバのIPアドレスは、そのドメインで利用するメール送信サーバのIPをご入力ください。	

設定手順 - STEP 5

DKIMレコードの設定手順

DKIMレコードの設定状況確認方法

利用ツール:<https://dmarcian.com/dkim-inspector/>

Step1 ドメイン+セクタ入力と実行

The screenshot shows the DKIM Record Checker interface. The title 'DKIM Record Checker' is at the top. Below it, a text box explains the tool's purpose. There are two input fields: 'Domain' (ドメイン入力) and 'Selector' (セクタ入力). A yellow box highlights these fields and the 'INSPECT DKIM' button. A blue speech bubble with 'クリック' (Click) points to the button. A grey box with '入力欄' (Input field) points to the domain field.

Fromアドレスのドメインと「楽楽メールマーケティング」の管理画面内で設定をしたセクタを入力し、ボタンをクリックします。

Step2 結果の確認と判定

The screenshot shows the results page. At the top, a green box says 'Congratulations! Your DKIM record is valid.' Below it, a grey box says '= 中略 =' (Omitted). Then, a yellow box titled 'Your DKIM Record' contains a long string of text: 'v=DKIM1; h=sha256; k=rsa; s=s1; t=_dmarcian; c=relaxed; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQYAMIIBCgKCAQEA...'. A grey box below it says '「楽楽メールマーケティング」管理画面内で作成した公開鍵情報' (Public key information created in the 'Rakuraku Email Marketing' management screen). A blue box with a green checkmark and 'OK!' says '「楽楽メールマーケティング」の公開鍵のV=以降が追加されている' (The V= and following are added to the public key of 'Rakuraku Email Marketing').

既存のレコード内に、指定の記述が含まれていれば設定完了です。

DKIMレコードの設定方法 （「楽楽メールマーケティング」管理画面）

①「楽楽メールマーケティング」管理画面の設定をする

各種設定 > システム設定タブ > 基本設定：DKIM署名付きメール送信「利用する」→ 変更

The screenshot illustrates the navigation path to the DKIM settings in the Rakus Mail Marketing management interface. The path is as follows:

- From the main menu, click on **各種設定** (Various Settings).
- In the **各種設定** menu, click on **システム設定** (System Settings).
- In the **システム設定** menu, click on **基本設定** (Basic Settings).
- In the **基本設定** section, click on **DKIM署名付きメール送信** (DKIM Signed Mail Sending).
- In the **DKIM署名付きメール送信** settings, click on **変更** (Change).

The **DKIM署名付きメール送信** settings page shows the following options:

- DKIM署名付きメール送信**: ☒ 利用する, ☐ 利用しない. DKIM署名は「各種設定」.
- スマホの自動判別**: ☒ する, ☐ しない. "i.softbank.jp"のアドレス.
- 顧客レコード数の集計**: ☐ 顧客レコード数 (グループ別).
- 配信リストを確定するタイミング**: ☒ メール作成時, ☐ 配信直前. 配信予約後に追加される.
- メールアドレス確認の入力欄**: ☐ 登録フォームにメール入力欄.
- メールアドレスの登録**: ☒ メールアドレスなし, ☐ メールアドレスあり. 一度メールアドレスを登録すると、そのメールアドレスは登録済みとして扱われます.
- 配信目的と業種/業態**: 配信目的: 営利 (), 業種/業態: 広告代理店 (). ☐ 既存のすべての配信.

At the bottom of the page, there is a link: [各種設定メニューへ戻る](#).

DKIMレコードの設定方法 （「楽楽メールマーケティング」管理画面）

①「楽楽メールマーケティング」管理画面の設定をする

各種設定 > Fromの設定 > DKIMの設定 > 新規登録：セクタ・ドメインを入力 → 登録

セクタは半角英数字20字の好きな文字列を入力してください。
入力内容に困ったら mail とご記載いただいても大丈夫です。

各種設定 > 各種設定メニュー

システム設定

来訪タグ設定
トリガー起動対象のWEBページに埋め込む

コンバージョンタグ設定
コンバージョン計測用の設定を行います。

テンプレート設定
テンプレートの設定を行います。

Fromの設定

各種設定 > 各種設定メニュー > DKIMの設定

メールの到達率を高めるには
SPFやDKIMの設定が到達率向上に大きく寄与します。
設定方法を確認する

Fromの設定

DKIMの設定

+ 新規登録

各種設定 > 各種設定メニュー > DKIMの設定 > DKIM署名の新規登録

セクタ * mail

ドメイン * haihaimail.jp

自動作成する（秘密鍵と公開鍵のペアが自動で作成されます）
○ 手動登録する（他のサーバで作成された秘密鍵を入力してください）

秘密鍵 *

登録

Fromの設定 DKIMの設定

+ 新規登録

選択したレコードを 削除

開覧	ID ↓	セクタ	ドメイン	FQDN	作成日時
☐	31	mail	haihaimail.jp	mail._domainkey.haihaimail.jp	2024/02/16 12:23:48

DKIMレコードの設定方法 （「楽楽メールマーケティング」管理画面）

①「楽楽メールマーケティング」管理画面の設定をする

各種設定 > Fromの設定 > 署名の設定 : DKIM署名「作成者署名」 → 登録

DKIMの設定タブ > BINDでの設定例を表示 > 表示の情報をDNSへ登録

The process is shown in four sequential screenshots:

- Fromの設定 > DKIMの設定**: The user navigates to the 'From Settings' page and selects the 'DKIM Settings' tab. A table lists existing DKIM records, with the '署名の設定' (Signature Settings) button highlighted for the selected record.
- 署名の設定**: The 'Signature Settings' page shows options for the signature type. '作成者署名' (Author Signature) is selected, and the domain 'mail._domainkey.haihaimail.jp' is chosen from the dropdown. The '登録' (Register) button is highlighted.
- DKIMの鍵の選択**: A dialog box prompts the user to select a DKIM key for the specified domain. The '作成者署名' (Author Signature) key is selected, and the '登録' (Register) button is highlighted.
- Fromの設定 > DKIMの設定**: The user returns to the 'DKIM Settings' page, where the '表示' (View) button is highlighted for the newly registered key.

The final screenshot shows the generated DNS records:

ID	31
セレクト	mail
ID	haihaimail.jp
FQDN	mail._domainkey.haihaimail.jp
秘密鍵	-----BEGIN PRIVATE KEY----- [Redacted Private Key] -----END PRIVATE KEY-----
公開鍵	-----BEGIN PUBLIC KEY----- [Redacted Public Key] -----END PUBLIC KEY-----

A blue callout box points to the public key section with the text: **表示の情報をDNSへ登録** (Register the displayed information to DNS).

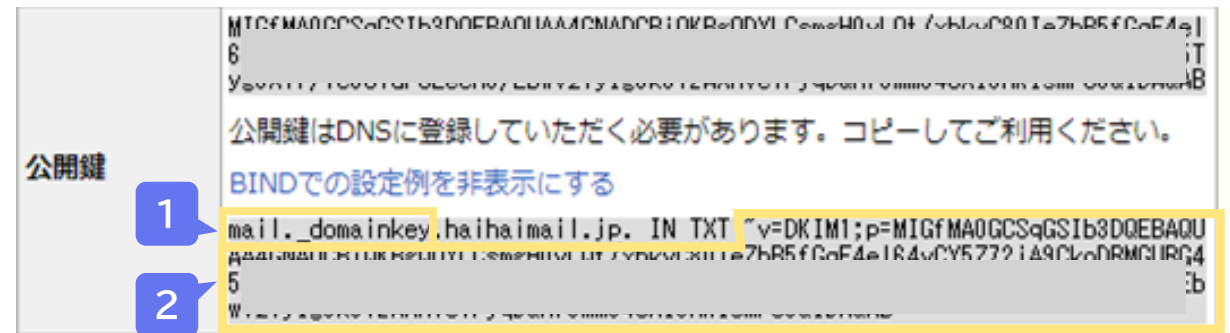
DKIMレコードの設定方法(DNSサーバー)

下記内容に沿って、
DNSサーバーにレコード追加してください。

ホスト名 : ●●.domainkey
※ 1 の情報を記載してください。

レコードタイプ:TXT

内容 :v=DKIM1;p=MI~~中略~~AQAB
※ 2 の情報を記載してください。



設定手順 - STEP 6

DMARCLレコードの 設定手順

DMARCレコードの設定状況確認方法

利用ツール:<https://dmarcian.com/dmarc-inspector/>

Step1 ドメインの入力と実行

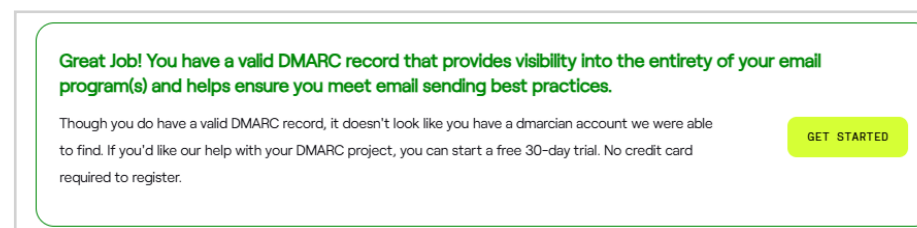
入力欄

ドメイン入力

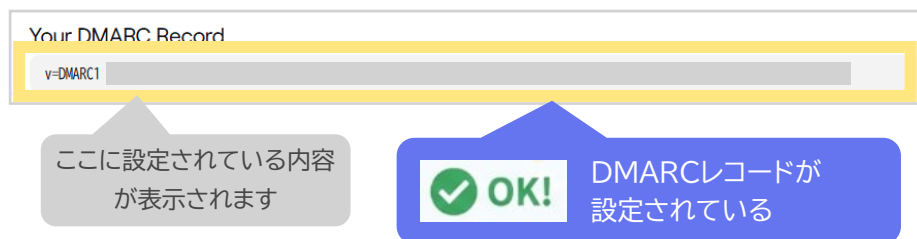
クリック

Fromアドレスのドメインを入力し、
ボタンをクリックします。

Step2 結果の確認と判定



= 中略 =



既存のレコードが存在すれば
設定完了です。

CASE-A

既存のDMARCレコードがある場合

The screenshot shows the DMARC Inspector interface. At the top, there is a text input field containing a domain name and a green button labeled "INSPECT THE DOMAIN". Below this, a message box states: "Great Job! You have a valid DMARC record that provides visibility into the entirety of your email program(s) and helps ensure you meet email sending best practices." It also mentions that a dmarcian account was not found and offers a 14-day trial. A green "GET STARTED" button is present. Below the message box, a URL is provided: "Access/bookmark this inspection at <https://dmarcian.com/dmarc-inspector/?domain=haihaimail.jp>". At the bottom, a yellow box displays the DMARC record details, including the policy and a confirmation message. A blue callout bubble points to this yellow box.

INSPECT THE DOMAIN

Great Job! You have a valid DMARC record that provides visibility into the entirety of your email program(s) and helps ensure you meet email sending best practices.

Though you do have a valid DMARC record, it doesn't look like you have a dmarcian account we were able to find. If you'd like our help with your DMARC project, you can start a free 14-day trial. No credit card required to register.

GET STARTED

Access/bookmark this inspection at <https://dmarcian.com/dmarc-inspector/?domain=haihaimail.jp>

v=DMARC1 ; p=none ; rua= .jp;

DMARC record policy details and comments:

You have a valid DMARC record that provides visibility into the entirety of your email program(s) and helps ensure you

ここに設定されている内容が表示されます

設定されていれば、
作業は終了となります。

CASE-B

既存のDMARCレコードが無い場合

INSPECT THE DOMAIN

We were unable to find a DMARC record. As a result, this domain is not protected against abuse and likely does not meet the new Google and Yahoo sender requirements.

Add DMARC to disallow unauthorized use of your email domain to protect people from spam, fraud and phishing.

Get started with your DMARC project in just a few minutes with our Free 14 Day Free trial. No credit card required to register.

GET STARTED

Click [here](#) to read our "Getting Started with DMARC" guide.
Access/bookmark this inspection at <https://dmarcian.com/dmarc-inspector/?domain=jupita.biz>

【対応内容】 下記内容に沿って、DNSサーバーにレコード追加してください。

ホスト名	レコードタイプ	内容
<code>_dmarc.自社ドメイン</code> ※ 自社ドメイン はFromアドレスのドメインに置き換えてください。	TXT	<code>v=DMARC1 ; p=none ; rua=mailto:指定アドレス; ruf=mailto:指定アドレス2;</code> ※「 指定アドレス 」「 指定アドレス2 」は、レポートを受け取る宛先のメールアドレスに置き換えてください。 ※「 指定アドレス 」「 指定アドレス2 」は、同じメールアドレスをご設定頂いて問題ございません。

今回の設定情報についての背景や詳細は、
下記サポートサイトにまとめております。

ご不明点がございましたら、下記リンクから詳細をご確認ください。

SPFの設定【重要】

<https://support.haihaimail.jp/arrivalimprovement/spfset/>

DKIM署名の設定【重要】

<https://support.haihaimail.jp/arrivalimprovement/dkimset/>

DMARCの設定

<https://support.haihaimail.jp/arrivalimprovement/dmarc-set/>