迷惑メール対策Guideline

Presents by 配配メール

株式会社ラクス　RAKUS Co., Ltd.

「配配メール」カスタマーサクセスチーム　Marketing Cloud Div.

CONFIDENTIAL

配配メール

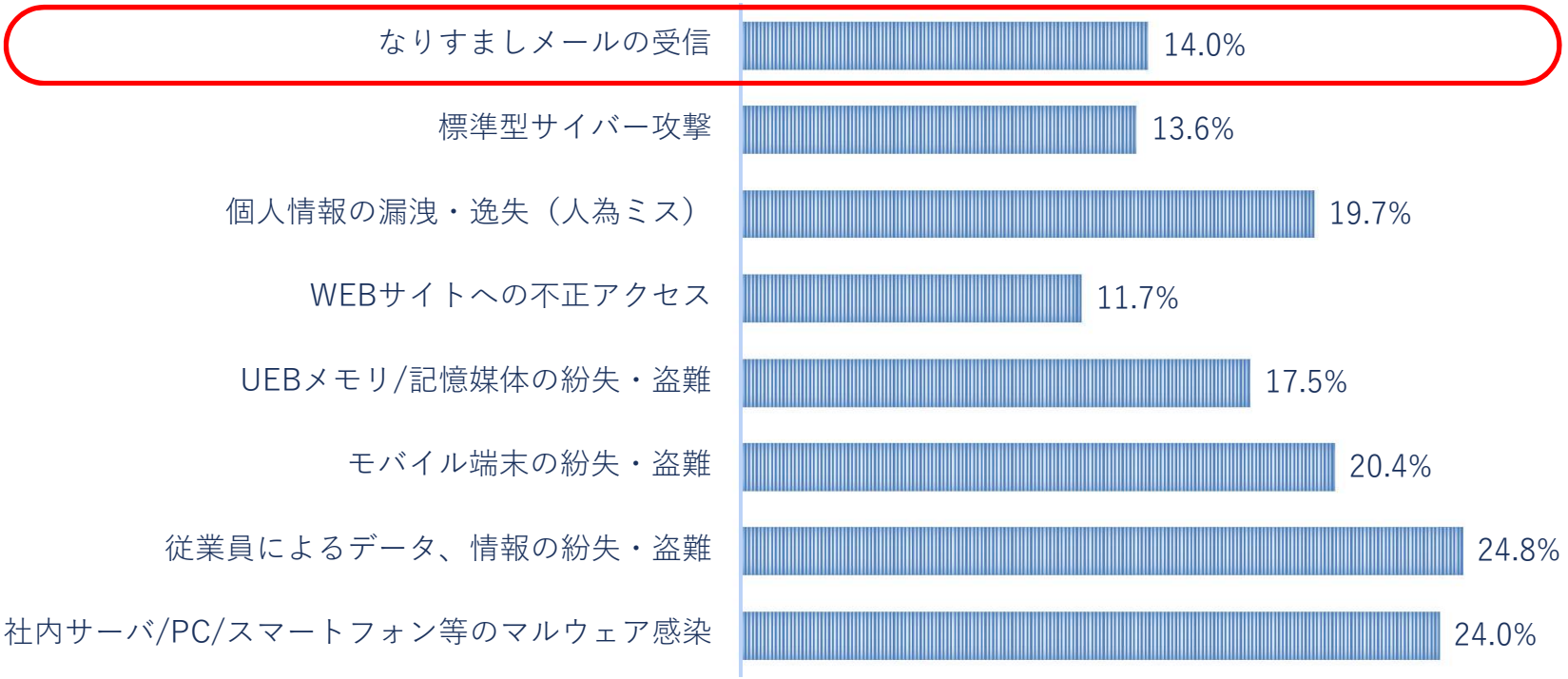
INDEX

CONFIDENTIAL

配配メール

前提（企業が抱えるセキュリティリスク）

Q. 過去１年間に経験したセキュリティインシデント（2020年1月14日～1月20日に調査）



なりすましメールによるインシデントは少なからず、
日本国内でも無視できない状態にあることが分かる。

引用：一般財団法人日本情報経済社会推進協会（株式会社アイ・ティ・アール）
2020年1月14日～1月20日：約5000人に対して実施

「企業IT利活用動向調査2020」集計結果（詳細版）
https://www.jipdec.or.jp/archives/publications/J0005162.pdf

CONFIDENTIAL

配配メール

1．　迷惑メール判定の仕組み

迷惑メール判定は受信側のサーバやセキュリティシステム側で
判断されており、原則として**送信側では関与ができません。**

送信者ユーザ

送信者ユーザの場合は
受信側のサーバからの
通知の有無で気づく…

受信側のサーバは複数台有しており、
判定基準は様々な要素から配信毎に判断されている。

⇒**同じドメインやメールアドレスも配信毎に判定が変わることがある**

【よく言われる判定基準の例】

- **SPF/DKIMの相互設定の有無**
- **配信内容に問題があるか** etc.

受信者ユーザ

受信者ユーザの
多くは気づかない

**送信側の
メールサーバ**

エラー通知（無い場合もある）

スパムフィルタ

**受信側の
メールサーバ**

セキュリティシステムも含む

ブロック

① 受信者は関与しない

迷惑メール判定は受信者ではなく
受信側のサーバが行っています。
※（例：Gmail, docomoなど）

② 判定は都度、変わる

様々な要素を基に総合的に判断し、
送られてきたメールを届かせるか
判断していると言われています。

※同じ会社ドメインやメーラでも、
受信側のサーバは複数あるため、
判定結果は都度、異なります。

③ 判定基準は非公開

判定基準を公開するメーラなどは
ごく一部分を除いて、ありません。
※調査することも出来ません。

CONFIDENTIAL

配配メール

2. なりすまし判定とは

なりすまし判定 / なりすましメールとは？

第三者が別の企業などを装って配信したとされる判定 / そのメールです。

電子メールでは差出人名や From アドレスを自由に書き換えることが出来てしまいます。
「配配メール」を含めた、メールの一斉送信サービスではこの仕組みを応用しています。

しかし、同時にフィッシングメールや詐欺メールを送る悪質な業者もこうした仕組みが
残念ながら世界中で悪用されており、各国で被害が出てしまっています。

各サーバ会社やメーラでも健全な配信を行っているユーザと悪質な配信を続ける業者の
判別が難しくなっているため、迷惑メール判定基準に「なりすましメール」であるかを
厳しく判断されるようになっていると言われています。

一般的なメール送信の仕組み

@example.com を
管理しているサーバ

ドメイン（この場合example.com）を
管理するサーバとメール送信サーバは
同じ会社が契約しているのが一般的。

受信者のフォルダ

受信側サーバと**受信者**は「A さん」から
「A さんが作ったメール」が届いたと識別

Ⓐ 送信者

Ⓐ 受信者 Ⓐ

内容

内容を作成し、差出人を指定

内容

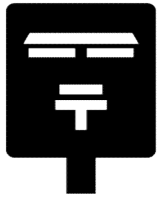
@example.com送信サーバ
※メール送信サーバ

= メールの差出人（From）

内容 = メールの件名と本文

= メール送信用のサーバ

受信側のサーバ



Ⓐ

内容

From：xxx@example.com をFromに設定
実際の送信も ×××@example.com を使用

CONFIDENTIAL

配配メール

なりすましメール送信の仕組み

Ⓐ 送信者

外部サービスにログイン
（例：配配メールなど）

メールの一斉送信などを行う外部サービスでは**差出人名やFromアドレス/内容を自由に変更・選択する**ことが可能。

Ⓑ

外部サービスの送信サーバ
From：123@haihaimail.jp

From：xxx@example.com をFromに設定
実際の送信には 123@haihaimail.jp を使用

実際はこっち

受信サーバでの識別 ➡ Ⓐ 内容 × Ⓑ

受信者側の見え方 ➡ Ⓐ 内容 = Ⓐ

受信側サーバは「なりすまし」と判断、
一般的に**受信者本人側では分からない**。

「Aさん」の差出人名と Fromアドレスが
「Bさん」の送信サーバから届いたぞ！？

受信側のサーバ

内容 ? =

Ⓐ Ⓑ

受信者

CONFIDENTIAL

配配メール

3. 対策 ① SPF

@example.com を
管理しているサーバ

IPアドレス：×××.○○○.■■■.△△△

ユーザ様

@example.comが管理されているサーバ以外の
送信サーバから届いたので、管理元へと確認

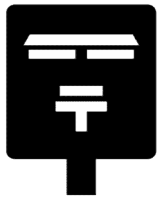
SPF Check

@example.comを管理しているサーバ内に
「配配メール」の送信サーバのIPアドレスを
設定することで送信サーバの相違を許可

「配配メール」送信サーバ
From：123@haihaimail.jp

IPアドレス：○○○.◇◇◇.△△△.×××

受信側のサーバ



From：xxx@example.com をFromに設定
実際の送信には 123@haihaimail.jp を使用

CONFIDENTIAL

配配メール

SPFの確認と設定手順

1：自社ドメインにSPFレコードが設定されているか確認する

dmarcian（SPF確認サイト）

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

Enter domainに Fromアドレスで
使うドメイン（@の後ろ）を入力

Survey domain をクリック

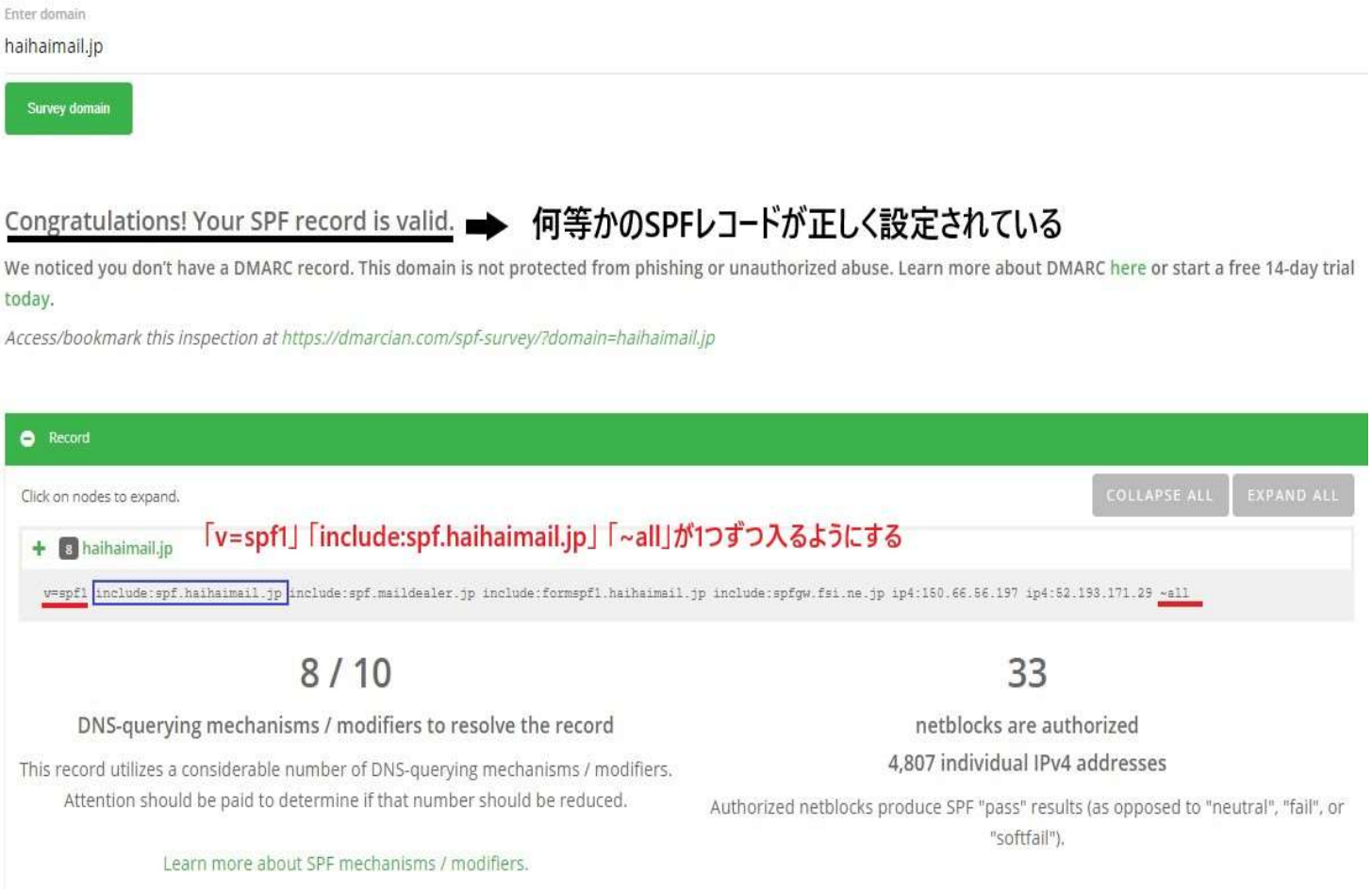
【 SPFレコードが未設定 】

No SPF Record for this domain と表示

CONFIDENTIAL

配配メール

【 SPFレコードが設定されている場合 】



※「include:spf.haihaimail.jp」が含まれるように追記が必要
※ 設定してから反映されるまで最大72時間掛かる場合があります。

配配メール

2 ：SPFレコードの設定方法 / 追記する方法

システム担当がいる
※社内SEや情報システム部など

「DNSサーバに以下のSPFレコードを追記してください」と伝える。

include:spf.haihaimail.jp

SPFレコードが未設定の場合は下記のレコードを伝える
TXT “v=spf include:spf.haihaimail.jp ~all”

システム担当がいない
※社内SEや情報システム部など

ドメインを管理するサーバ会社を調べ
サーバ会社のサポートサイトやFAQで
「DNS編集」や「SPF」と検索頂き、
include:spf.haihaimail.jpを追記

【自身で設定して頂くサーバ会社の一例】
https://support.haihaimail.jp/arrivalimprovement/spfset/#i
※設定例が開示されているため、ご紹介しております。

DNSサーバに「配配メール」のSPFレコードを設定する

CONFIDENTIAL

配配メール

4. 対策 ② DKIM（作成者署名）

@example.com を管理しているサーバ

「セレクタ★」の公開鍵を登録

ユーザ様

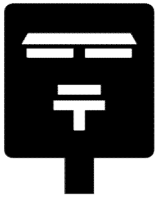
@example.comが管理されているサーバ以外の
送信サーバから届いたので、管理元へと確認
（メールの内容を改ざんしていないかと疑う）

DKIM Check

@example.comを管理しているサーバ内に
「配配メール」で生成したセレクタの公開鍵を
設定することで改ざんしていないことを証明。

「配配メール」送信サーバ
From：123@haihaimail.jp

「セレクタ★」の秘密鍵を登録



受信側のサーバ

From：xxx@example.com をFromに設定
実際の送信には 123@haihaimail.jp を使用

CONFIDENTIAL

配配メール

1：「配配メール」の管理画面内で事前の設定を行う

①：DKIMを設定可能にする

「**各種設定**」＞「**システム設定**」
「**基本設定**」の順にクリック。

②：DKIMを設定可能にする

「**DKIM署名付メール送信**」を
「利用する」にチェックするに
変えて「変更」をクリック。

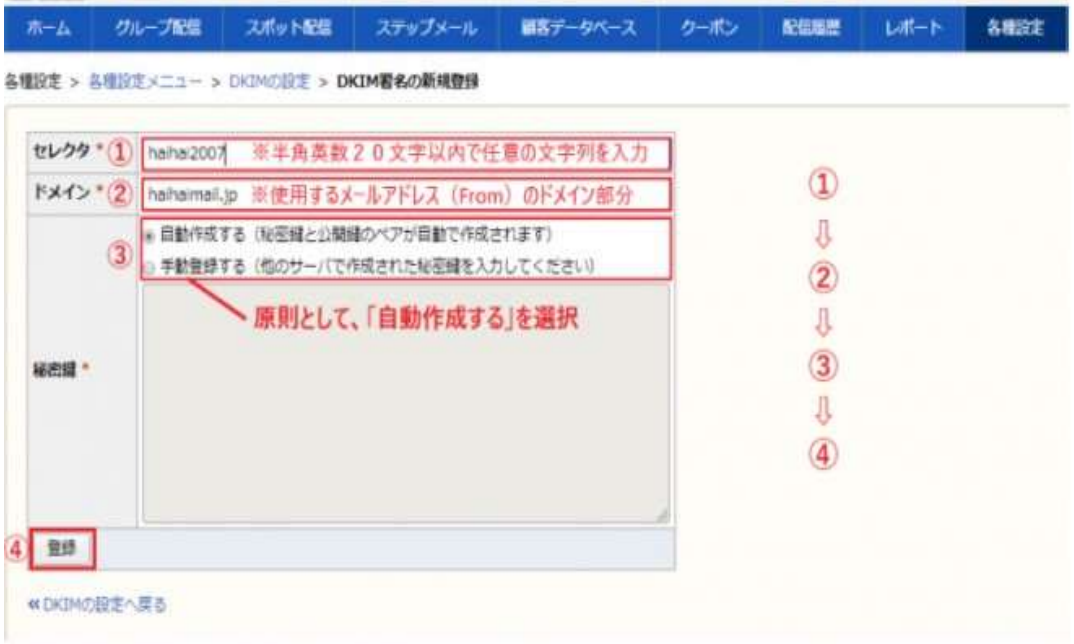
CONFIDENTIAL

配配メール

2：「配配メール」の管理画面内で署名を作成する

③：署名を作成する

「各種設定」＞「Fromの設定」
「DKIMの設定」＞「+新規登録」



④：セレクタとドメインを入力

【セレクタに入力する内容】
・半角小文字・英数 20字以内
・任意の文字列（基本何でもOK）
・特に覚える必要はない

【ドメイン（@の後ろ）】
・Fromで設定しているドメイン
※@は入力しない

【秘密鍵】
・「自動作成する」にチェック

CONFIDENTIAL

配配メール

３：システム担当者に伝える情報を確認する

⑤：サーバに設定する情報を確認

「**DKIMの設定**」＞「**閲覧**」＞
「**BINDでの設定例を表示する**」

「BINDでの設定例を表示する」
記載されている文字列と併せて
「DNSサーバにTXTレコードを設定してください」と伝えます。

ID	8
セレクタ	sakura-sake
ID	haihaimail.jp
FQDN	sakura-sake._domainkey.haihaimail.jp
秘密鍵	-----BEGIN PRIVATE KEY----- MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAOZaqXSDBtCVGvfR o5HdyTedAlBrU390a+fN6jmJuogY4dIpZJ1HjLpJmmdD/WjI3YEz0R8JoezTEZEQ pOFC9rsvYAQIBd0vKieXzkdwk4z/JSpm0wYGcgzIFn4yJKWpC2dIc/21Hu+rSko2 tcvbj/jPVI26zfENE8cyYCsmIYZLAgMBAAECgYBBF4dg1BGd6TRYqNWWx1wvqd9Y iCttDaHcO9Se86tQ/xXzxByZUPmUPm4yFgVKkc/9zX2fTqKCAFarbk+ZE8oSK5mL BXgrZk/9Cf+EAxKxbI54HcwEHXQHVGI8IPN3H/c+aVTKJhwmnMhXhxb7pKRqc14D UMfYth/iiKTrerafOQJBAPeTUyQFZHeuJ7g0a/208OklYiYM3+CjSjfuQDKOd3rL a9ZS/8CtICIZHLpFkHoJiIkvtG24gkBAtFPKluodS1kCQQDuMVGI3OqzJvcmog3z wF67imbc5XI/bKEiV78edd+dbaoEQXwYOo4oiAtrLe/98+EJYZxdcubGqiydI9Sh SX5DAkEAt1BgyVUs1OkhA+Xc6Fhn+QuqRDZYNq7xr4O8CLMwiL3CtUIzkal1AUC4 YrxLg/E3JcOq3es2InjSjRB+ug7COQJACSIpAFUY3s/CsF+Ma2IX+JcBBL1j4Ef5 EckNkgxxC6dY2p3sNUN1ogY9cdmsFy/P1DzNJyQtxzZISZG13I114wJBALHUWGke FUPiKFsPzwaDXeF5x8dfGRaWdueOhXr30wjbRRpejP1kzU8A1k0zRkvsvpjInoGS zWfdSnk2K5nupTO= -----END PRIVATE KEY-----
公開鍵	MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDmWqI0gwbQIRr30aOR3ck3nQJQa1N/dGvn zeo5ibqIFeHSKWSdR4y6SZpnQ/1oyN2BM9EfCaHs0xGREKThQva7L2AEJQXdLyonl85HcJO M/yUqZtMGBnIM5RZ+MiSIqQtnSHP9tR7vq0pKNrXL24/4z1Zdus3xDRPHMmArJiGGSwIDAQA B 公開鍵はDNSに登録していただく必要があります。コピーしてご利用ください。 BINDでの設定例を表示する クリックしてください。

【お名前 .com / さくらインターネット 】
【ムームードメイン / エックスサーバー】

右記の情報を基にした上で下記のページに記載した設定例をご参照ください。

DNSサーバでの設定例
https://support.haihaimail.jp/arrivalimprovement/dkimset/#i-4

CONFIDENTIAL

配配メール

4 ：作成・設定した署名をFromアドレスと紐づける

⑥：Fromアドレスと紐づける

「**各種設定**」＞「**Fromの設定**」
「**署名の設定**」の順にクリック

「**作成者署名**」に変更します。

※それぞれの From アドレスで
選択する必要があります。

※ドメイン（@ の後ろ）ごとに
選択できる署名が異なります。

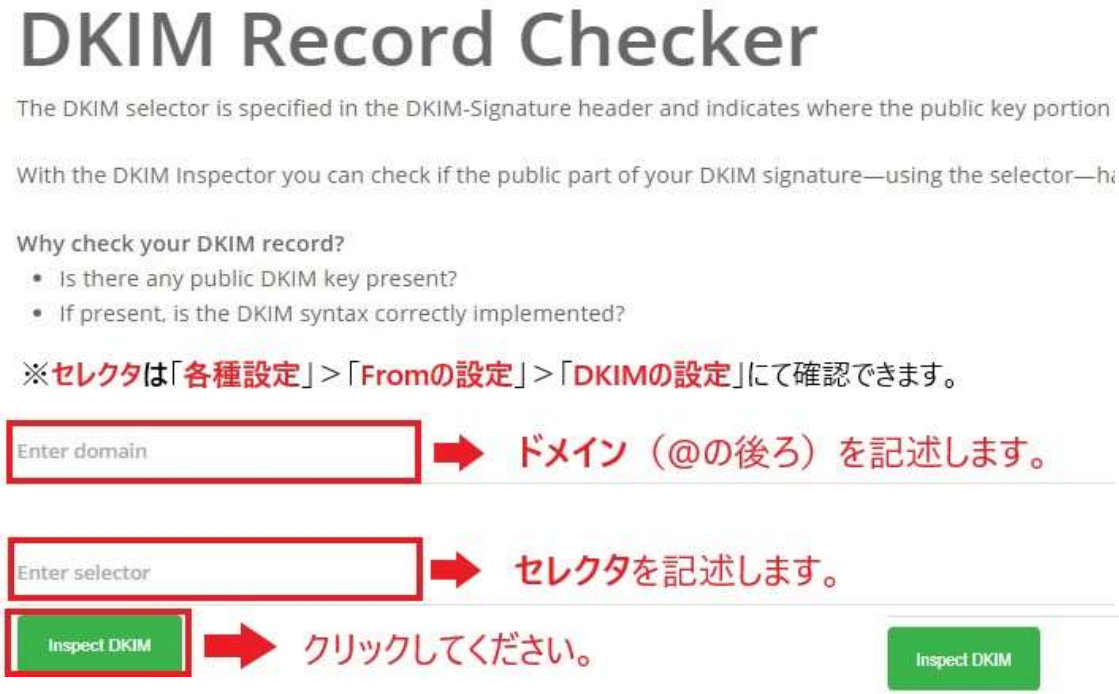
DKIMの設定は最終的に自社のドメインを管理するDNSサーバにて設定致しますので、
「配配メール」上での作業だけでは設定が完了しません。

しかしながら、DNSサーバ上の作業を行っても上記の「署名の設定」を変更しないと
DKIMが有効になりませんので、ご注意ください。

CONFIDENTIAL

配配メール

5 ：DKIMが設定されているかを確認する



dmarcian（DKIM確認サイト）

https://dmarcian.com/dkim-inspector/

Enter domainに Fromアドレスで使うドメイン（@の後ろ）を入力

Enter selector に管理画面内にて設定したセレクタを入力

Inspect DKIM をクリック

DNSサーバで設定が反映されている場合、
「Conguraatulations! Your DKIM record is valid.」
と表示されるようになります。

※設定してから反映されるまで、最大で72時間掛かる場合があります。

CONFIDENTIAL

配配メール

5. 対策 ③ DMARC

@example.com を
管理しているサーバ

※SPFとDKIM（作成者署名）が
事前に設定していることが必要

受信側のサーバで認証に失敗した場合、
認証できなかったメールを受信側にて、
どのように扱って欲しいかを指定する。

ユーザ様

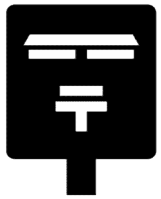
受信拒否（Reject）

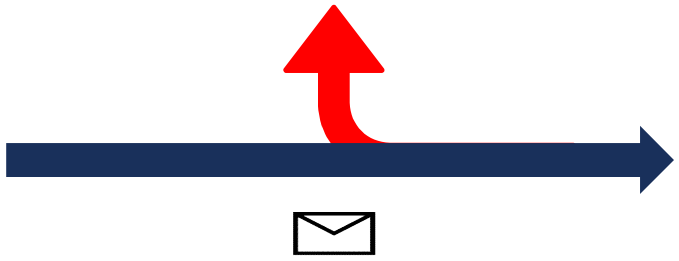
隔離（Quarantine）

何もしない（None）

「配配メール」送信サーバ
From：123@haihaimail.jp

受信側のサーバ





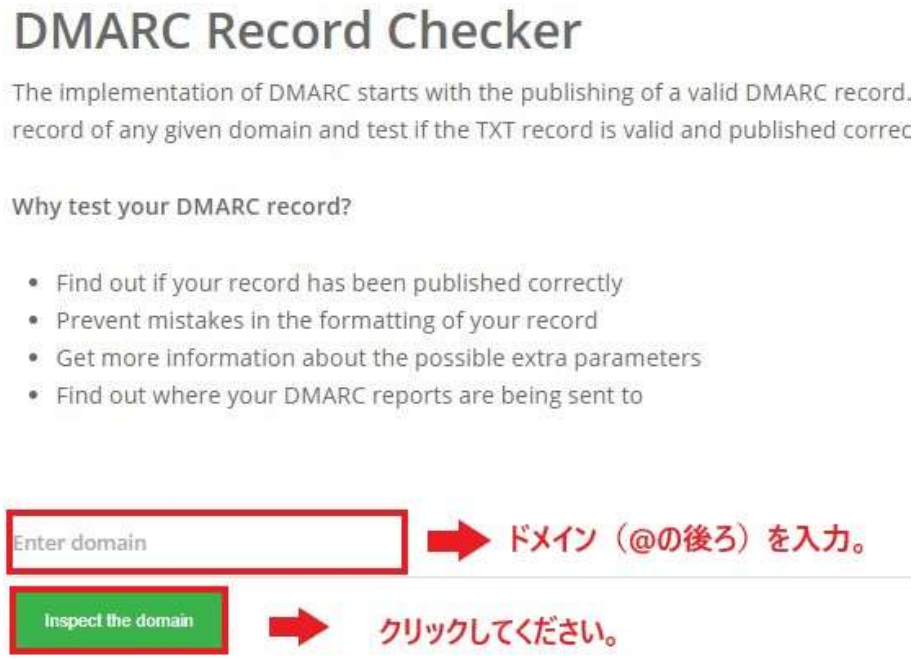
From：xxx@example.com をFromに設定
実際の送信には 123@haihaimail.jp を使用

CONFIDENTIAL

配配メール

DMARCの確認と設定方法

1：自社ドメインにDMARCレコードが設定されているか確認する



dmarcian（DMARC確認サイト）

https://dmarcian.com/dmarc-inspector/

Enter domainに Fromアドレスで
使うドメイン（@の後ろ）を入力

Inspect the domain をクリック

【 DMARCレコードが未設定の場合 】

No DMARC record published. Add DMARC to disallow unauthorized use ofyour email domain to protect people from spam, fraud and phising. と表示

CONFIDENTIAL

配配メール

２：システム担当者に伝える情報を確認する

「DNSサーバに以下のTXTレコードを設定してください」と伝える。
※「自分のアドレス」と「別のアドレス」はそれぞれご自身の異なるメールアドレスを代入します

_dmarc.ドメイン IN TXT “v=DMARC1 ; p=none ; rua=mailto:自分のアドレス ; ruf=mailto:別のアドレス”

「DMARCレコード」はSPFやDKIMと異なり、「配配メール」側が指定する固有のDMARCレコードなどはございません。

お名前.com、さくらインターネット、ムームードメイン、エックスサーバーの場合
※ご自身でサーバの管理画面にログインして頂き、設定するサーバ会社になります。

ホスト名（サブドメイン、エントリ）：_dmarc.ドメイン
種別（TYPE）：TXT
値（内容、VALUE）： v=DMARC1 ; p=none ; rua=mailto:自分のアドレス ; ruf=mailto:別のアドレス”
優先度（TTL）：（記入や編集は不要です）

CONFIDENTIAL

配配メール

設定しないとどうなるのか？

送ったメールが受信先に届かない、または**迷惑メール判定を受けたことで配信エラーになる**、**受信先に届いたものの迷惑メールフォルダに振り分けられる**などの可能性が高まります。

実際に Gmail や iCloud など大手メーラでは各社で発行するガイドラインにこれらの設定の要求と設定が無い場合は迷惑メール判定にしやすくする旨が公開されています。

※他のメーラなどでは判定基準が公開していませんが、上記のGmailやiCloudなどと同様に送信ドメイン認証の設定有無を判定基準の一部に用いていると一般的に言われています。

また、受信側における判定基準は予告無く突然厳しくなることも珍しくないと言われており、昨日まで届いていたのに突如として届かなくなることも起こり得ます。

「設定して」という受信側の都合になぜ合わせる必要があるの？

「受信者保護」などの点から原則として受信側における都合が優先されるためと言われます。
配信エラーや迷惑メール判定も原則として全て受信側のサーバやシステムにて行っています。
また、世界各国で「受信者保護」の法律が施行されているため、各メーラやサーバ会社でも受信者を悪質な業者から守ることを優先する取り組みを強化しています。

そのため、受信側が求めている設定をされていない場合は「受信者に害がある」と判断され、受信者に届かせる必要が無いと見なされますので、設定することを推奨致します。

CONFIDENTIAL

配配メール

6. NGワード、配信リスト精査の必要性

Q. NGワードなどはありますか？

⇒ 「**ある**」可能性が高い（開示されてないため）

※ 具体的な内容については開示がされていないため言及できません。
※ 公序良俗に反している、同じ単語が連続で含まれているなど。
※ ベイズ推定を応用したAIを用いて、文脈からも判断されます。

Q. 配信リストの精査は必要ですか？

⇒ **定期的に確認・精査頂くことが必須となります。**
ブラックリストに登録される可能性もあります。

※ 使われていないアドレスや入力間違いがあるアドレスなどに対して、
何度も配信するとブラックリスト登録される可能性も起こり得ます。

【配配メールFAQ】スパム・トラップについて
https://support.haihaimail.jp/faq/spamtraps/

CONFIDENTIAL

配配メール

参考サイト

「配配メール」サポートサイト

マニュアル、FAQ（Q&A）、セミナー情報など

https://support.haihaimail.jp/

障害・メンテナンスサイト

障害情報や予定しているメンテナンスを公開してます。

https://support.rakus.co.jp/hai2/