送信ドメイン認証（DKIM・DMARC）対応のご案内

v2.8

EmberPoint

更新履歴

バージョン	日付	更新内容
v1.0	2017/01/25	・新規作成
v1.1	2017/07/13	・「チーターデジタル」に社名を変更 ・docomoのなりすまし対策用SPF設定内容の変更
v2.0	2017/11/16	・DKIM/DMARC新機能リリースに伴い、適用手順の修正および全体ブラッシュアップ
v2.1	2018/04/26	・DKIM署名オプション全体適用に伴い、全体ブラッシュアップ
v2.2	2019/11/01	・「エンバーポイント株式会社」に社名を変更
v2.3	2020/01/22	・docomoのなりすまし対策用SPF対応に、レコードタイプSPFについて追記
v2.4	2022/01/20	・MailPublisher/FormFactoryを解約した場合の注意書き(不要になったDNSのTXTレコードの設定削除）を追記
v2.5	2023/01/12	・「なりすましメールによる被害」内容の更新
v2.6	2023/11/8	・DMARCレコードのrua値変更（P.24）
v2.7	2023/12/12	・送信ドメイン認証対応手順のマニュアル参照案内を追記
v2.8	2025/03/28	・DMARCレポートの提供案内の更新、引用資料の最新化

はじめに
本資料の目的

本資料は、MailPublisher/FormFactoryをご利用のお客様に「送信ドメイン認証」の対応をご案内するものです。

いまだに後を絶たないフィッシング詐欺・標的型サイバー攻撃・架空請求等の犯罪では、ほとんどの場合、差出人（Fromアドレス）を詐称した「なりすましメール」が使われています。

近年、「なりすましメール」対策の有効な手段として、迷惑メール対策推進協議会をはじめとする業界団体や各ISPで「送信ドメイン認証」の普及・導入が進められています。

当社でも、お客様のなりすましメール被害リスクの低減と迷惑メール抑止効果の観点から、「送信ドメイン認証」への対応を強く推奨しております。

本資料をご一読の上、早期のご対応をよろしくお願いいたします。

Contents

EmberPoint

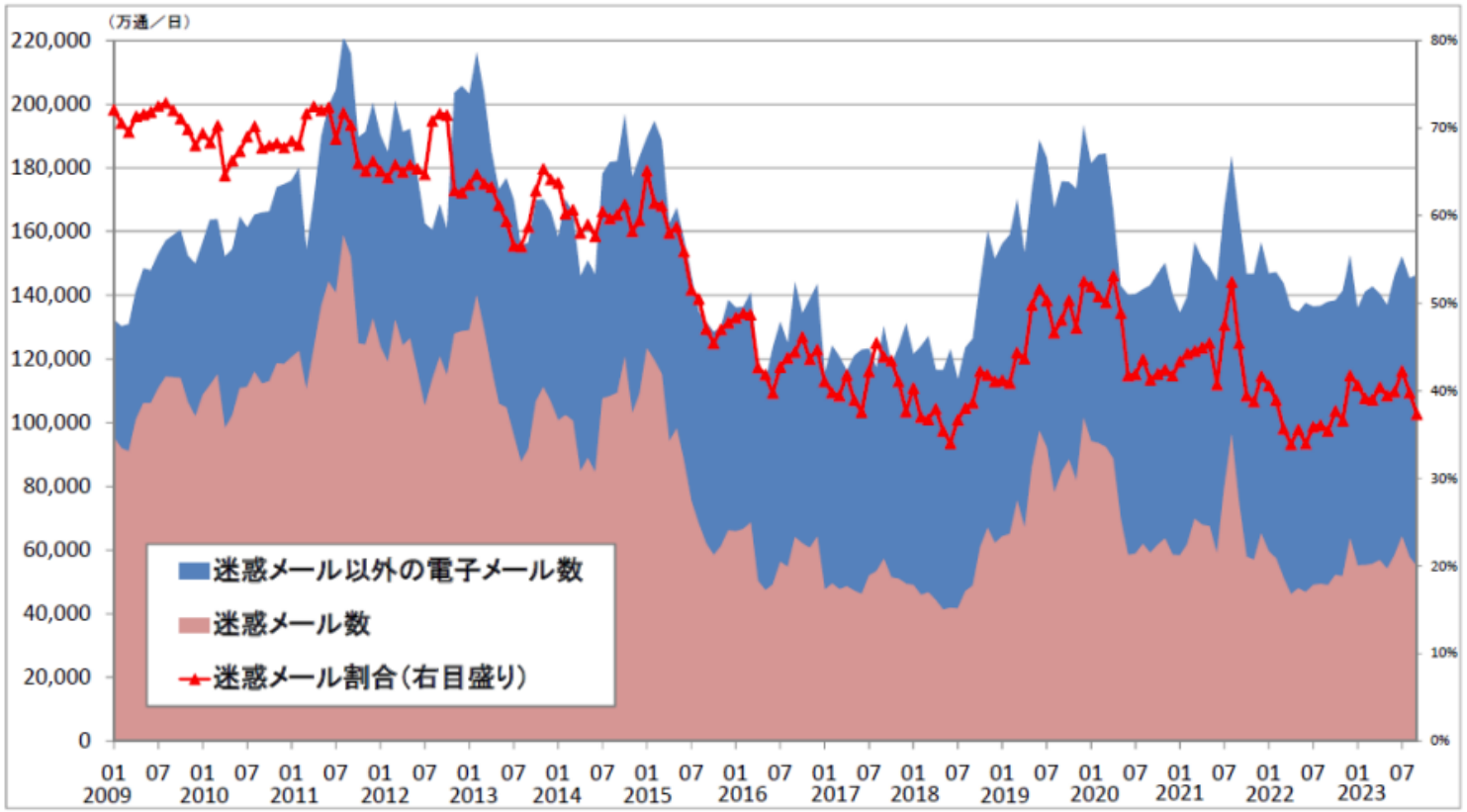
Contents

EmberPoint

なりすましメールによる被害

- 2021年8月の急増後の減少傾向を経て、2023年9月は約37%

図表 1－3－1　国内 ISP における迷惑メール数・割合の推移



出典：総務省「電気通信事業者 10 社の全受信メール数と迷惑メール数の割合（2023 年 9 月まで）」

出典：一般社団法人 日本データ通信協会
迷惑メール相談センター「迷惑メール白書2022-2024」

なりすましメールによる被害【例】

- 一般および事業者から受け付けたフィッシング報告のうち、
  消費者への影響が大きいと考えられるフィッシング

2025年03月05日	Apple をかたるフィッシング (2025/03/05)
2024年12月05日	えきねっとをかたるフィッシング (2024/12/05)
2024年12月05日	au PAYをかたるフィッシング (2024/12/05)
2024年12月04日	PayPayをかたるフィッシング (2024/12/04)
2024年10月30日	ORIX MONEY (オリックス・クレジット) をかたるフィッシング (2024/10/30)
2024年10月30日	レイク (新生フィナンシャル) をかたるフィッシング (2024/10/30)
2024年10月28日	WESTER をかたるフィッシング (2024/10/28)
2024年10月10日	プロミスをかたるフィッシング (2024/10/10)
2024年10月07日	アイフルをかたるフィッシング (2024/10/07)
2024年10月03日	JCB をかたるフィッシング (2024/10/03)

出典：フィッシング対策協議会
https://www.antiphishing.jp/

なりすましメールによる被害【例】

▶ フィッシングの例1

Apple をかたるフィッシング (2025/03/05)

X ポスト

2025年03月05日

▶ 概要

Apple をかたるフィッシングの報告が増えています。

▶ メールの件名

Apple ID のお支払い情報を更新！XX-XXXXXXXXX）
Apple ID情報が更新されました
サブスクリプションの有効期限がまもなく終了します
Apple IDに関するお支払い情報の更新が必要です
【Appleサポート】認証手続きを完了してください。番号：XX-XXXXXXXXX
Apple IDの認証情報が最新ではありません。番号：XX-XXXXXXXXX
Apple からの領収書です。
【重要】Apple ID アカウント確認のご案内
Appleよりご注文に関する重要なお知らせ

※ 上記以外の件名も使われている可能性があります。
※「X」部分は英数字文字で、実際の件名とは異なります。

▶ 詳細内容

Apple をかたるフィッシングの報告が増えています。

1. 2025/03/05 15:00 時点では、フィッシングサイトは稼働中であり、JPCERT/CC にサイト閉鎖のための調査を依頼中です。類似のフィッシングサイトが公開される可能性がありますので、引き続きご注意ください。

2. このようなフィッシングサイトにて、Apple Account (メールまたは電話番号、パスワード)、カード名義人、カード番号、有効期限、セキュリティコード等を、絶対に入力しないよう、ご注意

▶ メール・SMSの文面例

出典：フィッシング対策協議会
https://www.antiphishing.jp/news/alert/apple_20250305.html

なりすましメールによる被害【例】

- フィッシングの例2

えきねっとをかたるフィッシング（2024/12/05）

X ポスト

2024年12月05日

概要

えきねっとをかたるフィッシングの報告が増えています。

メールの件名

【重要なお知らせ】会員情報変更および退会に関するお知らせ
【ご注意】会員情報変更および退会に関するお知らせ
「新幹線eチケットサービス」えきねっとアカウントの自動退会処理について。メール番号:Ek2024-XXXXXXXX
えきねっとアカウントの自動退会処理について。メール番号:XXXXXXXX

※ 上記以外の件名も使われている可能性があります。
※「X」部分は英数字文字で、実際の件名とは異なります。

詳細内容

えきねっとをかたるフィッシングの報告が増えています。

1. 2024/12/05 15:00 時点では、フィッシングサイトは稼働中であり、JPCERT/CC にサイト閉鎖のための調査を依頼中です。類似のフィッシングサイトが公開される可能性がありますので、引き続きご注意ください。

2. このようなフィッシングサイトにて、ユーザーID、パスワード、お名前（姓、名）、生年月日、郵便番号、都道府県、市区町村、町名番地、アパート・マンション・建物名、電話番号、カード番号、カード名義人、有効期限、セキュリティコード等を、絶対に入力しないよう、ご注意ください。

3. フィッシングサイトは本物のサイトの画面をコピーして作成することが多く、見分けることは非

メール・SMSの文面例

出典：フィッシング対策協議会
https://www.antiphishing.jp/news/alert/ekinet_20241205.html

Contents

EmberPoint

送信ドメイン認証とは

インターネットでメール送信に使用されるプロトコルであるSMTP (Simple Mail Transfer Protocol)は、 差出人のメールアドレス(Fromアドレス)を自由に設定することが可能です。

このため、送信元を偽った「なりすましメール」を簡単に送ることができてしまい、これが迷惑メールに利用されてきました。

「送信ドメイン認証」は、電子メールの送信元ドメインが詐称されていないかを検査するための仕組みです。

正規のドメインの所有者からのメールを識別し、なりすましメール被害のリスクを低減することができます。

識別の方式により、大きく分けて３種類あります。

- **SPF（エスピーエフ）**
- **DMARC（ディーマーク）**
- **DKIM（ディーキム）**

送信ドメイン認証とは

SPF	docomoのなりすまし対策用SPF	DKIM	DMARC
Envelope-Fromのドメインと送信元IPアドレスで評価	**Header-From**のドメインと送信元IPアドレスで評価	電子署名を根拠に正当性を検証する技術	SPFとDKIMの組み合わせで評価なりすましの疑いがある場合の扱いを送信元が決定できる
MailPublisher/FormFactoryに標準装備	お客様にて設定が必要	お客様にて作成者署名の設定が必要	お客様にて設定が必要
			※なりすまし状況レポートを作成する仕組みがある

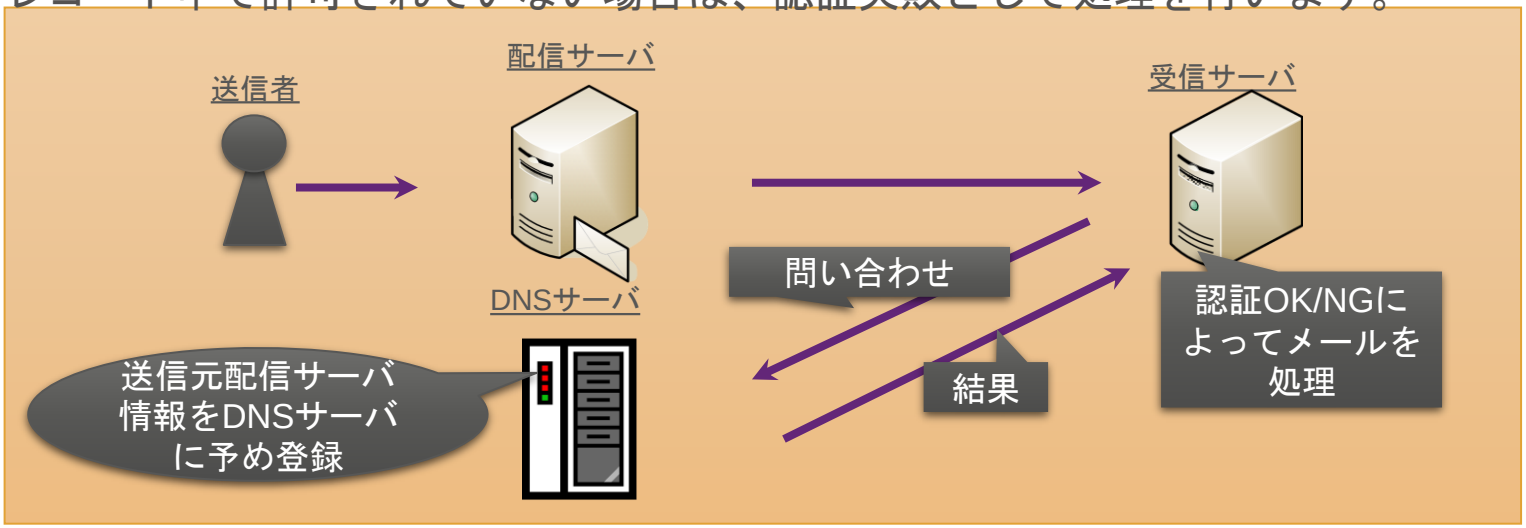
12

送信ドメイン認証とは【SPF（エスピーエフ）】

SPF（Sender Policy Framework）は、送信元サーバのIPアドレスとDNSを利用して、あらかじめ想定された送信元以外からのなりすましメールを検出できるようにする機構で、より多くのドメインがこの仕組みに対応することで、その効果が高くなります。

SPFに対応するには、そのドメインが登録されたDNSにSPFレコードという情報を追加します。 SPFレコードには、そのドメイン名を送信元としてメールを送ってもよいサーバのIPアドレス等を記述します。

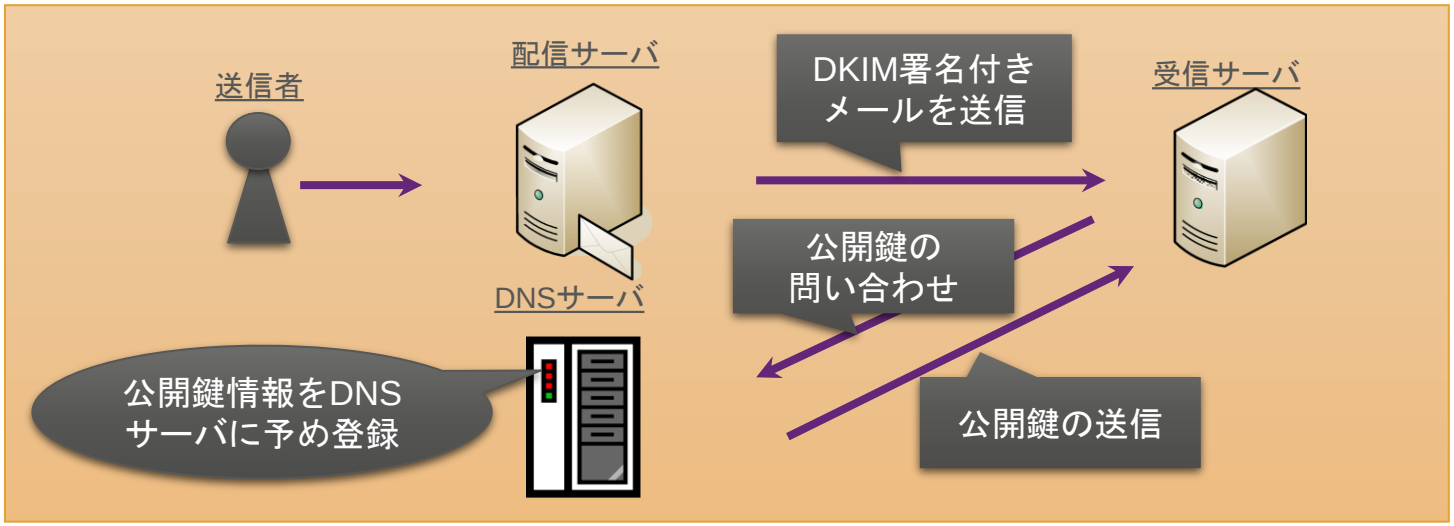
一方、SPFに対応したメール受信サーバは、メールの受信時にそのメールの送信元となっているドメインのSPFレコードを、DNSで問い合わせます。 送信元のサーバがSPFレコード中で許可されていない場合は、認証失敗として処理を行います。



送信ドメイン認証とは【DKIM（ディーキム）】

DKIM（DomainKeys Identified Mail）は、Fromアドレスのドメインとメールの電子署名から、受信側でDNSを利用してメールの正当性を判定する仕組みです。

DKIMに対応するには、そのドメインが登録されたDNSに予め署名の公開鍵（DKIMレコード）を設定した上で、メールにDKIMの電子署名を付加して送信します。一方、DKIMに対応したメール受信サーバは、メールの受信時に、DNSに対して署名の公開鍵を問い合わせ、DKIM電子署名と公開鍵を照合し、認証を行います。

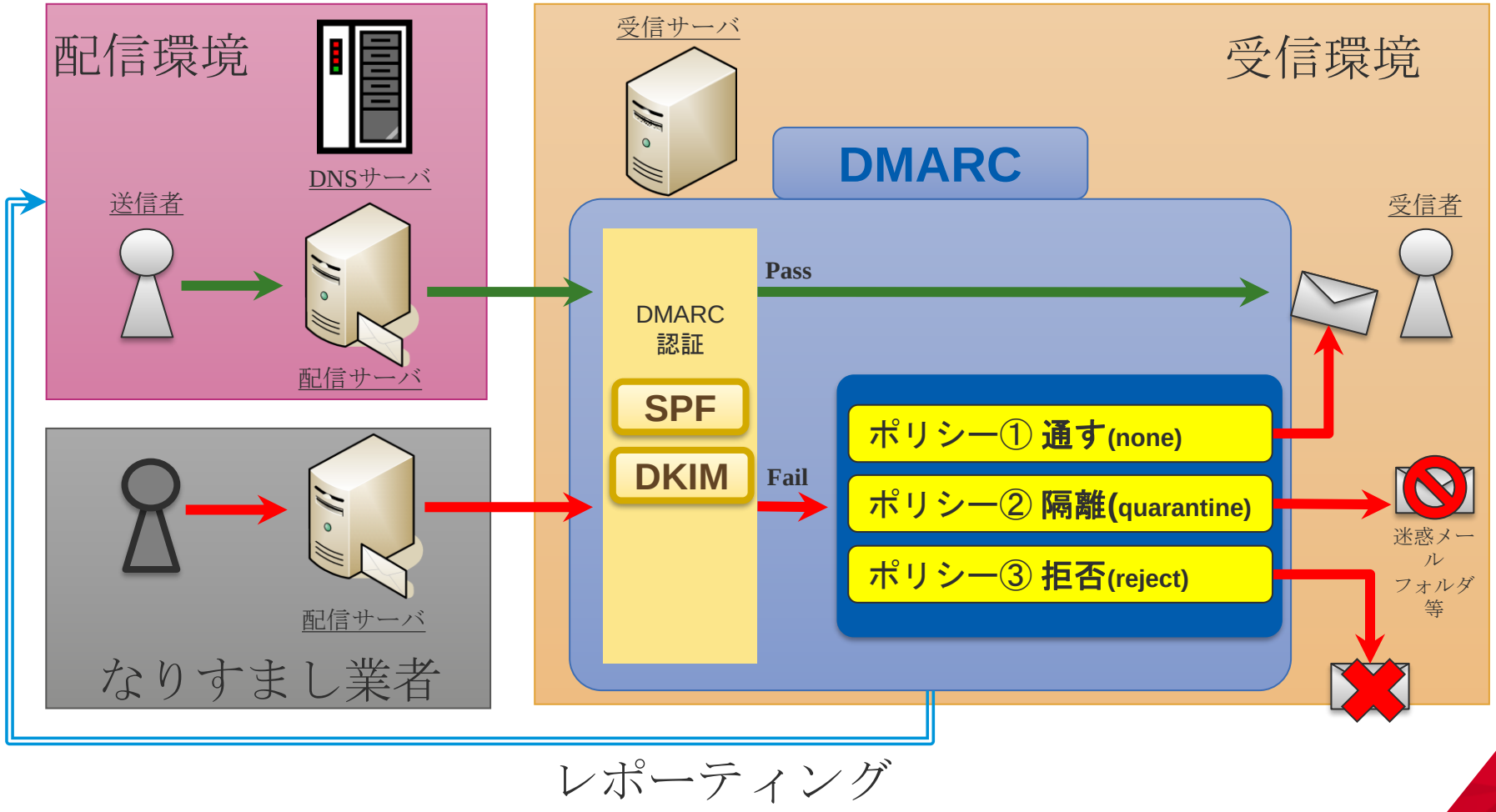


送信ドメイン認証とは【DMARC（ディーマーク）】

- 送信ドメイン認証(*1)技術のひとつ
  - 「DMARC（ディーマーク）」は、 送信元を詐称した迷惑メール（なりすましメール）への対策に有効な送信ドメイン認証技術のひとつです。
  - SPFとDKIMの認証結果を利用して、なりすましメールを受信側がどう扱うべきかのポリシーを、ドメイン管理者が宣言するための仕組みです。
  - レポート機能があり、ドメイン管理者などがなりすましメールの発生状況を把握することもできます。

- 貴社ドメインを偽装した迷惑メールを処理
  - Fromアドレスを偽装して貴社ドメインで送信されるなりすましメールを受信側でどのように処理するかを、詳細に制御することができます。
  - 送信元ドメイン管理者は、SPFとDKIMの認証に失敗したメールの処理方法をDMARCポリシーとして宣言します。
    - DMARCポリシー
      ①そのまま通す（none）
      ②隔離する（quarantine）
      ③受信拒否する（reject）

送信ドメイン認証とは
【DMARC（ディーマーク）】



送信ドメイン認証とは
【DMARC（ディーマーク）】なぜDMARC対応が必要か

- 貴社ドメインを偽装したなりすましメールを排除
  - 受信時の処理方法をDMARCポリシーとして宣言することにより、貴社ドメインを偽装して送られるなりすましメールを排除する効果を高められるなど、貴社のドメインから送信されるメールの信頼性を確保することが可能になります。
- レポート機能による状況把握
  - 受信側から送信者に対し詳細な認証結果のレポートを送る仕組みがあり、なりすましメールの発生状況の把握や送信元の特定などが可能になります。
- 業界標準の流れ
  - 迷惑メール対策推進協議会やフィッシング対策協議会は、その協議会が発行するガイドライン等でDMARCへの対応を呼びかけており、既に対応しているGmailやMicrosoft(hotmail)に加えて、日本のISPでの普及も推進されています。

DMARC導入

Contents

EmberPoint

送信ドメイン認証とは

SPF	docomoのなりすまし→対策用SPF	DKIM	DMARC
Envelope-Fromのドメインと送信元IPアドレスで評価	**Header-From**のドメインと送信元IPアドレスで評価	電子署名を根拠に正当性を検証する技術	SPFとDKIMの組み合わせで評価 なりすましの疑いがある場合の扱いを送信元が決定できる
MailPublisher/FormFactoryに標準装備	お客様にて設定が必要	お客様にて作成者署名の設定が必要	お客様にて設定が必要
			※なりすまし状況レポートを作成する仕組みがある

19
EmberPoint

送信ドメイン認証対応手順
【SPF】【docomoのなりすまし対策用SPF対応】

- 【SPF】は、MailPublisher/FormFactoryに標準装備しておりますので、お客様での対応は不要です。
- 【docomoのなりすまし対策用SPF】については、以下の手順でご対応ください。

手順		補足
1	ご利用のサービスに合わせたSPFレコードを確認する MailPublisher Smart Edition・ MailPublisher Mobile Edition・FormFactoryの場合 `"v=spf1 include:spf-bma.mpme.jp ~all"`	
2	貴社にて、Fromアドレスのドメインの DNSのTXTレコード（「IN TXT …」行）に、手順1の記述が反映されるよう設定する。 ※合わせて、レコードタイプ SPFのSPFレコード（「IN SPF …」行）がある場合は、削除するか、上記TXTレコードと同じ内容を設定する。	● 詳細は「メール配信ガイドライン」の付録をご参照ください

※MailPublisher/FormFactoryを解約した場合、 不要になったDNSのTXTレコードの設定は適宜削除して頂きますようお願いいたします。

送信ドメイン認証対応手順 【DKIM作成者署名対応】【DMARC導入】

- MailPublisher/FormFactoryで【DKIM作成者署名対応】【DMARC導入】を行うには、管理画面から設定・申請を行ってください。

各手順詳細は「操作手順マニュアル」内の「DKIM 作成者署名の設定および適用申請手順」参照

- MailPublisher Smart Edition 操作手順マニュアル
- FormFactory 操作手順マニュアル
- MailPublisher Mobile Edition 操作手順マニュアル

手順			補足
1	管理画面左メニュー［送信ドメイン認証］-［DKIM/DMARC］から、作成者署名に必要な情報（セレクタ情報）を入力し、DKIMレコード・DMARCレコードをダウンロードします。	お客様	● DMARCレコードは導入用のサンプルで、ポリシーは「そのまま通す（none）」です。
2	FromアドレスドメインのDNSのTXTレコードに、DKIMレコード・DMARCレコード（※）を登録します。	お客様	● FromアドレスドメインのDMARCレコードをDNSに登録済みの場合は、改めて登録する必要はありません。
3	管理画面［DKIM/DMARC］で、DKIMレコードが有効なことを確認したら、「事前チェック」依頼します。	お客様	● 事前チェックは、依頼後、1-2営業日で完了します。
4	管理画面［DKIM/DMARC］で、事前チェックの完了を確認したら、作成者署名の「適用申請」を行います。	お客様	● 適用は、申請後、1-2営業日で完了します。

（※）DMARCレコード内のDMARCポリシー（「p=」の設定値）について、DMARC対応を初めて行う等でポリシーが未定の場合は、管理画面からダウンロードしたファイルをそのままご登録ください。すでに貴社にてポリシーを定めている場合は、その設定値をご反映ください。

※MailPublisher/FormFactoryを解約した場合、 不要になったDNSのTXTレコードの設定は適宜削除して頂きますようお願いいたします。

送信ドメイン認証対応手順 【DMARC導入後のステップ】

- 最終的な目標は、DMARCポリシーを「受信拒否する（reject）」にすることです。

	DMARCポリシー	説明	貴社作業
step 1	そのまま通す（none）	→DMARC導入時の状態（前ページでご案内している管理画面からダウンロードしたファイルのDMARCレコードはこのポリシーになっています）	エンバーポイント・メール配信ガイドライン「参考５：DMARCの導入」内の『◆「そのまま通す（none）」から「隔離する（quarantine）」や「受信拒否する（reject）」ポリシーへの変更のステップ』に記載されている1)～4)の対応を行ってください。
			この間は、貴社が送信するメールのトラフィックを監視して、SPF, DKIM未対応のメールや偽装の疑いのあるメールなどがないかを確認します。結果に問題がなければ、ポリシー設定を「隔離する(quarantine)」に変更
step 2	隔離する（quarantine）	未認証メールは、受信サーバで隔離します。一般的には迷惑メールフォルダに振り分けられ、復帰させることもできる状態です。	
			この間に結果を確認し、すべてのメールが確実に署名されるようになったら、ポリシー設定を「受信拒否する(reject)」に変更
step 3	受信拒否する（reject）	未認証メールは完全に拒否し、受信しません。	DMARC のオプション設定で、試験導入とサンプリングを行うことができます。具体的にはpct タグ（省略可）を使用することで、受信時に実際に処理されるのはすべてのメールではなく、部分的にメールを隔離して拒否することが可能です。まずは低い割合から始めて、数日ごとに割合を上げていくことを推奨します。

DMARC対応の注意点1
＜DKIMは作成者署名を＞

- DMARCを正しく運用するため、DKIMは作成者署名を適用ください。

- DKIM第三者署名の場合、DMARC認証がFailします。
  DKIM作成者署名を適用してください。

- 当社のDKIM署名オプションでは「作成者署名」をご案内していますので、ご案内どおりに設定している場合は問題ありません。

⇒第三者署名でDMARC認証がFailする理由は、「付録2」をご覧ください。

DMARC対応の注意点2
＜DMARCレポートの受信＞

- 当社からご案内しているDMARCレコードでは、DMARCレポートの受信先（rua）として当社のメールアドレスを設定しています。

  DMARC推進のため、DMARCレポートを当社で参照させていただきますがDMARCレポートの提供は承っておりません。
  ruaには複数アドレスを設定することが可能ですので、定期的なレポートの確認のご予定がございましたら、お客様アドレスの設定をお願いいたします。

サービス	DMARCレコード抜粋（rua値部分）
MailPublisher Smart Edition	rua=mailto:rua-mpse@mpub.ne.jp
MailPublisher Mobile Edition	rua=mailto:rua-mpme@mpub.ne.jp
FormFactory	rua=mailto:rua-fofa@mpub.ne.jp
MailPublisher Transaction	rua=mailto:rua-mptx@mpub.ne.jp
メールリレー	rua=mailto:rua-mrs@mpub.ne.jp
EngageCros	rua=mailto:rua-encr2@mpub.ne.jp

＜参考＞
複数サービスご利用の場合は、利用中のサービスと異なる場合もありますがいずれかが含まれていれば問題ありません。

- 貴社にてDMARCレポートを受信する場合は、DMARC設定用情報内のruaの設定値に「mailto:[貴社のメールアドレス]」を追加してください。

＜参考＞ruaに複数のメールアドレスを設定する場合は、「,（半角カンマ）」でつなぎます。
例：rua=mailto:rua-mpse@mpub.ne.jp,mailto:bbb@example.com;

⇒受信するDMARCレポートについての詳細は、「付録4」をご覧ください。

DMARCレポートの解析・サポートをご希望の際は、弊社パートナー企業のサービスをご提案させていただますので、ご希望があればお申し付けください。

DMARC対応の注意点3
＜メーリングリストアドレスの挙動＞

- メーリングリストアドレスが宛先に含まれる場合、メーリングリストサーバの仕様により、メーリングリストで展開された宛先に送信されるメールのDMARC認証が、failになる可能性があります。

- DMARCを導入して、ポリシーを「通す（none）」にしている間は配信に影響はありませんが、「隔離（quarantine）」や「拒否（reject）」に変える際には、レポートを確認して受信状況を確認しながら進める必要があります

  - 例：
    DMARCは、SPFやDKIMの結果を元に認証します。
    例えば、メーリングリストサーバで件名が書き換えられるとメールの内容が変わったことでDKIM認証がFailし、DMARC認証がfailするなどのケースが考えられます。

DMARC対応の注意点4
＜MailPublisher/FormFactory以外のシステムからの配信＞

- MailPublisher/FormFactory**以外**のシステムで、当該ドメインをFromにしてメール配信を行っている場合は、そのシステムの配信についてもDKIM作成者署名に対応してください。
  - DMARCポリシーはドメインごとに1つです。
  - MailPublisher/FormFactoryからの配信分については、当社のDKIM署名オプションに対応していればDMARC認証がPassします。
    同じドメインをFromにした、それ以外のシステムのからの配信については、DKIM作成者署名がないと、DMARC認証がFailしてしまう可能性があります。
  - DMARCを導入して、ポリシーを「そのまま通す（none）」にしている間は配信に影響はありません。
    「隔離する（quarantine）」や「拒否する（reject）」に変えると、DMARC認証がFailするものは迷惑メール判定されますので、その前までにDKIM作成者署名対応が必要です。

付録

1. DMARCレポート
2. DMARC認証の仕組み（Pass/Fail判定）

付録1. DMARCレポート

- DMARCレポートは、受信側ISPがDMARCに対応している場合、送信者がDNSのDMARCレコードに受信先等の情報を設定することで入手可能です。

レポートの種類	▼集約レポート 認証結果・是正措置・DMARCポリシー効果を把握するために必要な情報をフィードバック。 ▼失敗レポート Failしたメールについての詳細。Failの原因調査や送信元の特定に利用する。
レポート形式	xmlファイル（レポートとして受信したメールに添付されている） ※レポートの受信先メールアドレスは、送信者（ドメイン所有者）がDNSのDMARCレコードに設定した「rua」タグ（集約レポート）、「ruf」タグ（失敗レポート）に基く。
レポート間隔（頻度）	送信者（ドメイン所有者）がDNSのDMARCレコードに設定した「ri」タグの値に基く。
レポート内容	▼集約レポート SPF・DKIM判定結果、SPF・DKIMアラインメント結果、全メール数、Passした数、等 ▼失敗レポート FailしたメールのURI、ヘッダー情報等
レポートサンプル	（次ページ参照）

付録1. DMARCレポート

レポートサンプル （集約レポート）	<?xml version="1.0" encoding="UTF-8" ?> - <feedback> - <report_metadata> <org_name>google.com</org_name> <email>noreply-dmarc-support@google.com</email> <extra_contact_info>https://support.google.com/a/answer/xxxxxxxx</extra_contact_info> <report_id>10527584617073234618</report_id> - <date_range> <begin>1476921600</begin> <end>1477007999</end> </date_range> </report_metadata> - <policy_published> <domain>bma.mpse.jp</domain> <adkim>r</adkim> <aspf>r</aspf> none <sp>none</sp> <pct>100</pct> </policy_published> - <record> - <row> <source_ip>xxx.xxx.xxx.xxx</source_ip> <count>1</count> + <policy_evaluated> <disposition>none</disposition> <dkim>fail</dkim> <spf>fail</spf> </policy_evaluated> </row> - <identifiers> <header_from>bma.mpse.jp</header_from> </identifiers> - <auth_results> - <spf> <domain>bma.mpse.jp</domain> <result>softfail</result> </spf> </auth_results> </record> ・ ・ ・ </feedback>

付録2. DMARC認証（Pass/Fail判定）

DMARC認証では、まず、対象となるメールのヘッダFromドメインと、送信ドメイン認証（SPF・DKIM）で利用したドメインとの関係性について正しいかを検証します。

この関係性のことを「 アラインメント（Alignment）」と呼びます。

SPF アラインメント	メールのヘッダーFromドメインと、SPFがpassしたエンベロープFromドメインの関係
DKIM アラインメント	メールのヘッダーFromドメインと、DKIMがpassしたドメイン（DKIM署名ヘッダーの”d=“に書かれているもの。作成者署名の場合はヘッダーFromドメイン、第三者署名の場合はエンベロープfromドメイン）の関係

2つのドメインが同じまたは関係がある場合はアラインメント「In」(*)、異なる場合は「Not In」と表します。

SPFアラインメントとDKIMアラインメントの組み合わせで、DMARC認証がPassかFailか判定します。（→次頁参照）

(*) DMARCの設定により、ドメインが全く同じ場合のみ「In」とすることもできます。

付録2. DMARC認証（Pass/Fail判定）

- SPFおよびDKIMのアラインメントの組み合わせによるDKIM認証の判定

パターン	SPF アラインメント	DKIM アラインメント	DMARC認証結果
1	In	In	Pass
2	Not in	In	Pass
3	未設定	In	Pass
4	In	Not in	Pass
5	Not in	Not in	Fail
6	未設定	Not in	Fail
7	In	未署名	Pass
8	Not in	未署名	Fail
9	未設定	未署名	Fail

MailPublisher/FormFactoryを利用する場合

▼SPF Alignment
ヘッダーFromドメインは貴社のもの、エンベロープFromドメインは当社のものなので、関係性がないとみなされ「Not in」
▼DKIM Alignment
◇DKIM未署名の場合⇒パターン8(fail)
◇DKIM第三者署名の場合、ヘッダーFromドメインと第三者署名に含まれるドメイン（当社のもの）が不一致なので「Not in」⇒パターン5(Fail)
◇DKIM作成者署名の場合、ヘッダーFromドメインと作成者署名に含まれるドメイン（貴社のもの）が一致するため「In」⇒パターン2(Pass)

DMARC運用には、「DKIM署名オプション」適用が必須
（当社は、作成者署名をご案内しています）


EmberPoint
Experience is the Ember of New Communication