

# Japan DKIM Working Group

## DKIM Recommendation

~送信事業者における DKIM 導入・運用について~

版数	第 1 版
作成年月日	2011 年 5 月 26 日

修正履歴表			
修正版数	修正日	修正概要	修正者

## 目次

1	はじめに.....	3
2	本 Recommendation の位置づけ.....	4
3	Recommendation .....	5
4	DKIM を導入・運用するにあたって.....	7
4.1	DKIM を導入するメリット .....	7
4.1.1	送信者のメリット .....	7
4.1.2	送信事業者のメリット .....	7
4.1.3	受信者のメリット .....	7
4.2	DKIM を導入・運用する際の留意事項・参考情報.....	7
4.2.1	DKIM 導入・運用チェックリスト.....	8
4.2.2	DKIM 関連サービス・機能の例 .....	8
5	用語解説.....	9
5.1	作成者署名と第三者署名 .....	9
5.2	DKIM-ADSP .....	10
5.3	ドメインレピュテーション .....	10
6	最後に .....	11
6.1	Recommendation の利用に際しての条件 .....	11

# 1 はじめに

電子メールは、今もなおインターネットを支える重要なコミュニケーションの手段である。一方で、迷惑メールの送信にも利用され、ワンクリック詐欺やフィッシング詐欺などの犯罪の温床ともなっている。総務省の調査によれば、メールの約 70% が迷惑メールという報告がある<sup>1</sup>。

迷惑メール対策が難しい理由のひとつとして、電子メールが利用する SMTP プロトコルに送信者の認証機能がなく、送信元の特定が困難であることが挙げられる。

この問題に対応するため、送信ドメイン認証と呼ばれる技術が考案された。送信ドメイン認証はメールの送信元の正当性確認を目的とした技術である。送信ドメイン認証には、主に SPF、Sender ID、DKIM の 3 種類の規格が存在する。SPF や Sender ID はメールの発信源を元に、DKIM は電子署名を元にしてそれぞれメール送信者のドメイン正当性を確認する。

我々 Japan DKIM Working Group (略称 dkim.jp、以下 dkim.jp とする) は以下の 2 点において DKIM に着目する。ひとつは、電子署名を用いていることから本文の正当性も評価できることなど DKIM の規格そのものに魅力があることである。もうひとつは、SPF、Sender ID、DKIM の 3 種類の規格の中で DKIM の対応が一番難しいことである。WIDE プロジェクトの 2010 年 10 月時点の調査では、SPF は日本国内で約 40% 程度普及している<sup>2</sup>のに対して、後発の DKIM の普及はまだこれからである。そして、DKIM の対応を実施することで迷惑メール対策が推進されると考えている。

我々は、送信ドメイン認証の規格のひとつである DKIM の導入/普及を通して、迷惑メールの削減だけでなく、電子メールサービスが社会のインフラストラクチャとしてより強固なものになることを期待する。

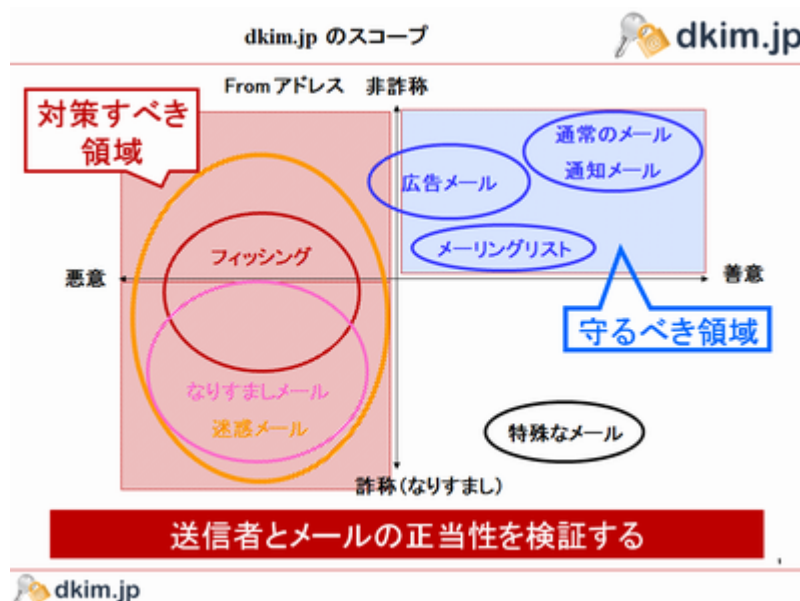


図 1-1. dkim.jp のスコープ

<sup>1</sup> [http://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/d\\_syohi/pdf/110302\\_1.pdf](http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/pdf/110302_1.pdf)

<sup>2</sup> <http://member.wide.ad.jp/wg/antispam/stats/index.html.ja>

## 2 本 Recommendation の位置づけ

本 Recommendation は dkim.jp 内で議論および検討された内容をまとめたものである。また、本 Recommendation は読み手にある程度のメールシステムや送信ドメイン認証に関する知識があることを前提にしている。

今回の Recommendation は、読み手として送信事業者を想定した内容であり、今後はその他の立場（ISP、企業など）に向けた Recommendation を順次追加していく予定である。ここで送信事業者とは、メール配信業務を受託する、あるいはメール配信機能を有する ASP・SaaS を提供する事業者を指す。

本文中では、実施しなければならない内容( Recommendation )については、必ず実施すべき、逆に絶対にすべきでない事項を「しなければならない」/「してはならない」/「MUST」、できる限り実施が必要、逆にできる限り実施しないようにすべき事項を「するべきである」/「するべきではない」/「SHOULD」、実施するかどうかは任意である事項を「してもよい」/「MAY」と表現している。

## 3 Recommendation

本章では、送信事業者が DKIM を導入・運用する際を守るべき事項を記載する。

### Rec 001.

**送信メールに対して作成者署名をつけるべきである。 [SHOULD]**

**作成者署名をつけることが不可能な場合は第三者署名をつけなければならない。 [MUST]**

DKIM 署名は、電子署名をつけたドメインによって作成者署名・第三者署名の 2 種類に分けられ、送信メールには原則として作成者署名をつけるべきである。ただし、技術的な理由やポリシーなどによって作成者署名をつけることが困難な場合は、第三者署名をつけることとする。作成者署名・第三者署名については第5章で解説する。

### Rec 002.

**DKIM-Signature ヘッダの 1 タグは設定すべきではない。 [SHOULD]**

DKIM-Signature ヘッダにはいくつかのタグが設定できる。その中のひとつに、電子署名の対象とした本文の長さを指定する 1 タグがある。大きなファイルを添付したメールの場合、電子署名の検証負荷がかかることが予想されるが、設定すべきではない。

### Rec 003.

**電子署名に利用するアルゴリズムは SHA-256 にしなければならない。 [MUST]**

DKIM の電子署名アルゴリズムは SHA-1 および SHA-256 の 2 種類が規定されている。しかし、SHA-1 はもはや安全ではないとも言われており、より堅牢な SHA-256 にしなければならない。現在、SHA-1 である場合は、速やかに SHA-256 に替えることとする。

### Rec 004.

**DKIM 署名に利用する秘密鍵は厳重に保管しなければならない。 [MUST]**

DKIM 署名に利用する秘密鍵のメールによる受け渡しや、ウェブ経由で秘密鍵をダウンロードするような機能を提供することは避けなければならない。

### Rec 005.

**セレクト名は運用性を考慮し、適切に名前付けしなければならない。 [MUST]**

DKIM の仕様上、セレクト名は任意文字列とされているが、運用性の面から考えて、初期設定の文字列(“default”等)とは異なるものを利用する。

#### (1) 任意の文字列+任意のシリアル番号

メール配送事業を複数の送信事業者に委託する場合、単純なセレクト名では重複する可能性がある。セレクト名としては任意の文字列と任意のシリアル番号の組合せにするとよい。任意の文字列

には、サービス名やシステムの識別子等を、また任意のシリアル番号には、作成日や鍵番号等を用いるとよい。

(例)

feb2011msa

201102.msa

noticemail201102

(2) セレクタ名の文字列長

DNS の仕様を考慮し、セレクタ名は長くなりすぎないようにする。長くても 20 バイト程度のセレクタ名を目安とする。

**Rec 006.**

**鍵長は 1024bit 以上とし、ロールオーバーを定期的実施しなければならない。[MUST]**

電子署名の安全性は、電子署名に用いる RSA 公開鍵暗号の鍵長が決定するので、鍵長の目安として 1024bit ないし 2048bit を推奨する。ただし、DNS 設備によっては強度の高い 2048bit の公開鍵で電子署名を検証できない場合があることに注意する。

また、万が一秘密鍵の漏えいや解読が確認された場合には、速やかにロールオーバーを実施しなければならない。こういった状況を想定して、ロールオーバーの手順をあらかじめ作成しておく。

(例)

1. 新しい鍵ペアを生成
2. 新しい公開鍵を DNS 上に設置
3. 新しい秘密鍵で電子署名
4. 一定期間後、古い公開鍵を削除

古い公開鍵との併用期間は、メールサーバのキューの生存期間を目安に決定するとよい。

また、定期的なロールオーバーを実施する間隔の目安としては、半年ないし 1 年以内とする。

## 4 DKIM を導入・運用するにあたって

本章では、DKIM を導入・運用する事業者のメリットや留意事項・参考情報について記載する。

### 4.1 DKIM を導入するメリット

DKIM を導入する事業者を、送信者・送信事業者・受信者に分類して、以下にそれぞれの立場での DKIM 導入のメリットをまとめる。

#### 4.1.1 送信者のメリット

- ✓ From アドレスの詐称が受信者側で確認できるようになる。これによって、送信者のドメインを騙ったフィッシング行為をされるリスクを減らすことができる。
- ✓ ドメインレピュテーションを上げることができ、迷惑メールと誤判定されにくくなる。

#### 4.1.2 送信事業者のメリット

- ✓ From アドレスの詐称が受信者側で確認できるようになる。これによって、送信事業者のドメインを騙ったフィッシング行為をされるリスクを減らすことができる。
- ✓ 作成者署名をつけることで、それぞれのクライアント送信者ごとのドメインレピュテーションを実現できる。すなわち、健全なクライアントのメールは保護されやすくなり、万が一不健全なクライアントによるメール送信が行われた場合にも影響の範囲を小さくすることができる。
- ✓ IP アドレスのレピュテーションと比較して、ドメインレピュテーションはクライアント送信者ごとに異なる評価結果を実現しやすい。これにより、正当なメールがよりスムーズに受信されることが期待できる。

#### 4.1.3 受信者のメリット

- ✓ From アドレスを詐称したメールを容易に判別できるようになる。これによって、フィッシング被害を受けるリスクを減らすことができる。
- ✓ ドメインレピュテーションによって、正当なメールが迷惑メールと誤判定されにくくなる。また、迷惑メールであるか否かをより適切に判断しやすくなり、迷惑メールの受信も減らすことが期待できる。
- ✓ 将来的な IPv6 アドレスの普及によって、IP アドレスのレピュテーションが困難になると予想される。ドメインレピュテーションがこの問題を解決すると期待できる。

### 4.2 DKIM を導入・運用する際の留意事項・参考情報

送信事業者が DKIM を導入・運用する際に注意しておきたい事項や DKIM に関連して提供するサービス・機能の例がいくつかある。以下に、注意点をまとめたチェックリストおよび サービス・機能提供の例を示す。

#### 4.2.1 DKIM 導入・運用チェックリスト

---

- ✓ DKIM-Signature ヘッダのタグ指定(c タグなど)が適切であることを確認する
- ✓ DNS に設置された公開鍵が DKIM 署名に利用する秘密鍵とペアであることを確認する
- ✓ 配信されるメールが宛先に届くことを、テスト配信などを実施して定期的に確認する
- ✓ 万が一、DKIM 署名の検証に失敗した場合、不達となった場合の対応方法を定めておく
- ✓ DKIM 署名ポリシーをクライアントに周知しておく
- ✓ 送信事業者のドメインレピュテーション結果が保護されるような契約をクライアントと締結する

#### 4.2.2 DKIM 関連サービス・機能の例

---

- ✓ クライアント送信者ごとの鍵ペア生成機能・公開鍵のダウンロード機能
- ✓ DNS 管理の委譲による鍵ペアの管理サービス
- ✓ クライアント送信者ごとの DKIM 署名用サブドメイン提供サービス

## 5 用語解説

本章では、第 3 章で挙げた Recommendation の他に DKIM 導入・運用する際に知っておきたい情報や Recommendation の前提となる基本的な DKIM について説明する。<sup>3</sup>

### 5.1 作成者署名と第三者署名

DKIM 署名には 2 種類の署名が存在する。

- (1) 作成者署名：メール作成者ドメインによる電子署名
- (2) 第三者署名：メール作成者ドメイン以外のドメインによる電子署名

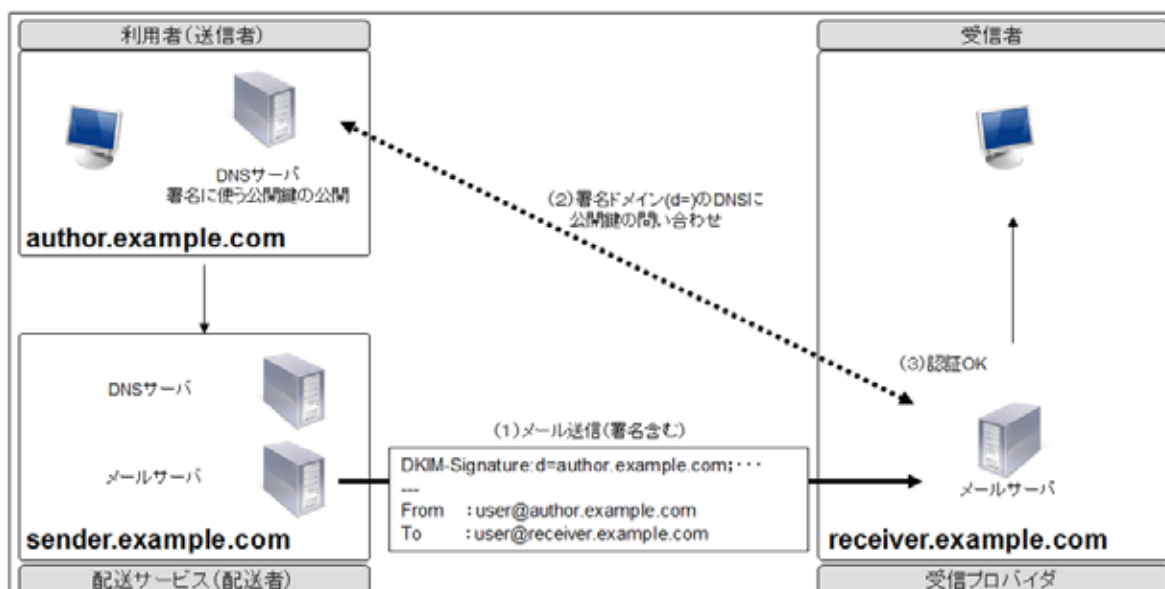


図 5-1. 作成者署名の模式図

<sup>3</sup>本 Recommendation では DKIM の技術解説を目的とせず、技術的な説明は必要最低限に留める。技術的な解説を必要とされる方は、迷惑メール対策推進協議会の発表した「送信ドメイン認証技術 導入マニュアル」

[http://www.dekyo.or.jp/soudan/anti\\_spam/image/2010/201007\\_DTIM\\_00.pdf](http://www.dekyo.or.jp/soudan/anti_spam/image/2010/201007_DTIM_00.pdf) を参照されたい。

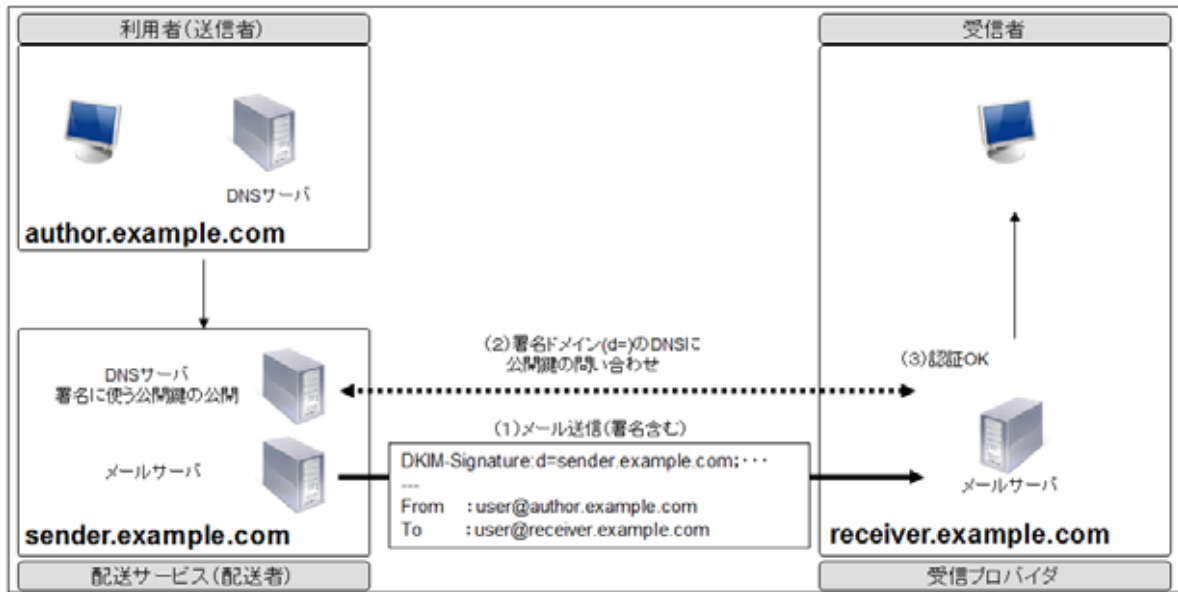


図 5-2. 第三者署名の模式図

## 5.2 DKIM-ADSP

DKIM-ADSP とは、RFC5617 に定義され、DKIM 署名(作成者署名)の検証に成功しなかった場合の受信ポリシーを規定する規格である。送信者が DKIM 署名に対応していても、メール作成者の意図によらず電子署名が壊れる場合があるので、DKIM-ADSP の受信ポリシーを宣言する際にはこの点を考慮する必要がある。特に、「discardable」の宣言は慎重に実施することとする。

## 5.3 ドメインレピュテーション

ドメインレピュテーションとは、特定ドメインから配信されるメールの量・質・評判などを基準にした、メール発信元の評価である。DKIM を導入することで、電子署名したドメインは、当該メールが自ドメインから配信されたことを証明することができるため、自ドメインのレピュテーションを守る手立てとすることができる。

## 6 最後に

DKIM の普及が進まなかった要因のひとつとして、電子署名の付与(送信側)と検証(受信側)のいずれの立場も、他方の普及を待っていたことが挙げられる。本 Recommendation が、まずは送信事業者の電子署名付与の普及に役立ち、続いて受信側も含めた DKIM 普及の一助となることを期待する。

送信事業者は、送受信者間のメールの安定疎通に貢献するために、DKIM の普及に努めるべきである。

### 6.1 Recommendation の利用に際しての条件

本文書は、日本の著作権法、国際条約により保護されている。

本文書の利用は DKIM 普及のための非営利活動の目的に限るものとし、Japan DKIM Working Group (以下、当団体)による事前の承諾なく、本文書を複製・配付 (以下「配付等」という)できるものとする。

本文書で示している運用指針については、DKIM 導入時の工数削減や相互運用性の向上を主な目的としており、いかなる拘束力も持つものではない。本文書に従うことで発生したいかなる不具合やトラブルについても、当団体は一切補償しない。

配付等は、かかる複製物に本文書に記載された著作権標記及び本条件の記載が付されることを条件とする。また、当団体による事前の書面による承諾がなければ、本文書の改変・翻案等はできないものとする。改変・翻案等に関する問合せは、以下に願います。

Japan DKIM Working Group

2011 年 5 月 26 日

連絡先:

Tel : 050-5817-7650

E-mail: info@dkim.jp