# チーターデジタル・
# メール配信ガイドライン
## 第 5.3 版

---

*Cheetah Messaging*

CHEETAH DIGITAL

# 改訂履歴

| | |
|---|---|
| 2007/11/16 | 第 1 版発行 |
| 2008/11/26 | 第 2 版発行<br>・「特定電子メールの送信の適正化等に関する法律」の改訂に対応 |
| 2010/6/7 | 第 2.1 版発行<br>・表紙（会社ロゴ）の差換え |
| 2011/8/30 | 第 3 版発行<br>・付録3以降を改訂し、DKIM に関する記述を追加<br>・各イメージ図を更新 |
| 2011/12 | 第 3.1 版発行<br>・「特定電子メールの送信等に関するガイドライン」の改正に対応 |
| 2012/11/1 | 第 3.2 版発行<br>・社名変更を反映 |
| 2016/10/27 | 第 4 版発行<br>・適切なメール配信のための十ヵ条を十三ヵ条に変更<br>・DMARC の導入に関する記載を追加<br>・「付録」と「参考」について、「付録」は MailPublisher/FormFactory を利用いただくために必要な設定情報とし、「参考」は技術的な参考情報という位置づけに変更<br>・参考情報に DMARC の導入方法を追加 |
| 2016/12/14 | 第 4.1 版発行<br>・表紙（会社ロゴ）の差換え |
| 2017/3/23 | 第 4.2 版発行<br>・DKIM、DKIM ADSP、DMARC の DNS 設定の記述例等を修正 |
| 2017/6/22 | 第 4.3 版発行<br>・DKIM ADSP の DNS 設定方法等を削除<br>・社名変更を反映 |
| 2018/5/24 | 第 5.0 版発行<br>・MailPublisher 版、Cross-Channel Marketing Platform 版の統合<br>・迷惑メール問合せ窓口の変更、他 |
| 2019/5/9 | 第 5.1 版発行<br>・「参考7：SPF チェック仕様」を追加<br>・情報の最新化、誤記修正 |
| 2019/11/1 | ・第 5.2 版発行<br>・分社化に伴い、Cross-Channel Marketing Platform 版として再構成<br>・新情報の反映、情報の最新化、誤記修正 |
| 2020/6/15 | ・第 5.3 版発行<br>・ブランド名変更に伴い、Cross-Channel Marketing Platform より Cheetah Messaging として再構成 |

# 目 次


改訂履歴 ..... 1
**目 次** ..... 1
■法律の構成とチーターデジタル版ガイドラインの位置づけ ..... 3
■2008 年（平成 20 年）法改正のポイント ..... 3
■オプトイン方式の導入 ..... 4
■実効性の強化（措置命令と罰則） ..... 4
■規制範囲の拡大 ..... 4
■国際連携の強化 ..... 5
適切なメール配信のための十三ヶ条 ..... 6
法令遵守編 ～法律の必須事項とチーターデジタル推奨ベストプラクティス～ ..... 7
1. 事前に同意を得た相手にのみ送信する ..... 7
2. 同意の記録を保存する ..... 10
3. 容易な方法でメール受信の拒否ができるようにする ..... 11
4. 送信するメールには「送信者」に関する情報を記載する ..... 12
5. 送信者情報を偽った送信をしない ..... 12
6. 架空アドレス宛の送信をしない ..... 13
チーターデジタル推奨編 ～よりよい運用のために～ ..... 14
7. メール受信制限に関する情報提供 ..... 14
8. 「正しい」形式のメールで送る ..... 14
9. 受信者メールアドレスの表示 ..... 15
10. 受信者からの返信の受付け ..... 15
11. 送信者ドメインの WHOIS 情報登録 ..... 16
12. 送信ドメイン認証への対応 ..... 16
13. 受信者の立場になって方針を考える ..... 17
ケーススタディ ..... 18
**★同意取得時に表示するべき事項とその方法** ..... 18
**★表示義務への対応** ..... 21
**★「送信者」と「送信委託者」** ..... 23
**★第三者を通じた同意の取得について** ..... 23
**付録(Cross-Channel Marketing Platform)** ..... 25
付録 1：送信ドメイン認証対応手順 ..... 26
付録 2：CCMP での表示義務内容への対応 ..... 27
**参考** ..... 29
参考1：メールヘッダ基礎知識 ..... 29
参考2：送信ドメイン認証とは ..... 30
参考3：ネットワーク方式（送信元 IP アドレス方式/SPF/SenderID）とは ..... 31
参考4：電子署名方式（DKIM）の導入 ..... 41
参考5：DMARC の導入 ..... 49
参考6：主要 ISP・キャリアのメール送信者向けガイドライン等 ..... 52
参考7：SPF チェック仕様 ..... 53
参考 8：本ガイドラインの参考資料 ..... 54


Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## はじめに

迷惑メールの法整備については、2002 年 4 月に制定された「特定電子メールの送信の適正化等に関する法律」が 2005 年 5 月の改訂を経て 2008 年 6 月に 2 回目の改訂が成立し、2008 年 12 月より施行されます。

2008 年の改訂では実効性の強化が大きなポイントのひとつとなっていますが、実際には、総務省をはじめとする行政機関だけでなく、ISP や携帯キャリアの他に送信側となる事業者、メールを受信する利用者など多くの関係者による様々な取り組みの結果として成り立つものです。

当社においてもメール配信事業者という立場から、総務省の指針に沿った自主的な対策に取り組むため技術的な対策の実装を進めると共に、2007 年 10 月に「迷惑メール配信対策委員会」を社内組織として設置しました。

本ガイドラインは、2007 年 11 月作成した初版を基に 2008 年の改訂に対応する内容で第 2 版として再編集した後、2011 年の「特定電子メールの送信等に関するガイドライン」の改正を反映しました。さらに送信ドメイン認証の新たな技術に対応し、現在の第 5 版に至ります。今後も法整備以外の業界動向の変化に応じて順次改訂を行って参ります。

当社メール配信システムをご利用頂くお客様はもちろん、多くの方の指針となれば幸いです。

2019 年 11 月
チーターデジタル株式会社
迷惑メール配信対策委員会

当社サービスでは、本ガイドラインに反する運用に関する報告を受けた場合、「迷惑メール配信対策委員会」よりお客様へ対する注意勧告、サービス利用の制限等の措置をとる場合があります。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## ■法律の構成とチーターデジタル版ガイドラインの位置づけ

迷惑メールを規制するための法律としては「特定電子メールの送信の適正化等に関する法律」（以下、特電法）が基本となりますが、「特定商取引に関する法律」（以下、特商法）の中でも該当する部分が含まれています。

特電法が電子メールの送信者に対する規制であるのに対して、特商法の中では販売事業者などの公告・宣伝活動の一環で電子メールを送信する際に関しての規制という位置づけになっています。

メール配信を行う企業から見ればどちらも意識する必要のある法律ですが、共通している部分も多いため本ガイドラインは特電法に沿って構成されています。なお、両者の違いがある部分については文中で解説します。

【特電法の構成】

法律では基本的なことしか書かれていないので詳細は省令（施行規則）で定められています。

特に特電法では総務省からガイドラインも公開されています。

【チーターデジタル・メール配信ガイドラインの位置づけ】

法律の定義ではややあいまいにかかれている部分について、当社製品、サービスを使用した運用に限定しない範囲で「推奨」される運用方法について解説し、法令上の文章だけでは分かりにくい点を実際のメール配信における具体的な例を示しながら解説します。

## ■2008 年（平成 20 年）法改正のポイント

- オプトイン方式の導入
- 実効性の強化
- 規制範囲の拡大
- 国際連携の強化

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## ■オプトイン方式の導入

「オプトイン」「オプトアウト」は今回の法改正の中で非常に重要なキーワードですが、「オプトアウト」については解説文書などによっては特電法の中での意味と異なる場合がありますのでご注意下さい。

オプトイン

電子メール送信対象となる相手からあらかじめメール受信の承諾を得ること

オプトアウト

一度受信を承諾した場合であってもその後メールの受信を拒否することができること

！誤解に注意！ ※オプトアウトに関する他の説明（例）

・ユーザの許諾無く、一方的に広告メールを送りつけること。
・また、それを拒否して広告を送付しないよう企業に依頼すること。
・ユーザの事前承諾なしに送られるダイレクトメールを「オプトアウトメール」と言う。

## ■実効性の強化（措置命令と罰則）

平成 20 年の改正では罰則が大幅に強化されており個人であっても「一年以下の懲役または 100 万円以下の罰金」が課されることになります。また、法人の場合には罰金の金額が最大で 3,000 万円という非常に大きな額になっています。

原則的には罰則が適用される前に改善措置命令があり、更にその命令に違反した場合に罰則が適用されることになりますが、送信者情報の偽装については措置命令なしに罰則が適用されます。

## ■規制範囲の拡大

特電法では、「特定電子メール」とは以下のように定義されています。

営利目的の団体または営業を営む個人が自己または他人の営業につき広告・宣伝を行うための手段として送信する電子メール

なお、規制の対象はメールを送信する側であり、「自己または他人の営業につき」とあるように、「送信者」と「送信委託者」それぞれが当てはまります。

特に「送信委託者」は規制の対象として新たに含まれるようになりました。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

送信者

電子メール送信操作の主体となる者（団体）

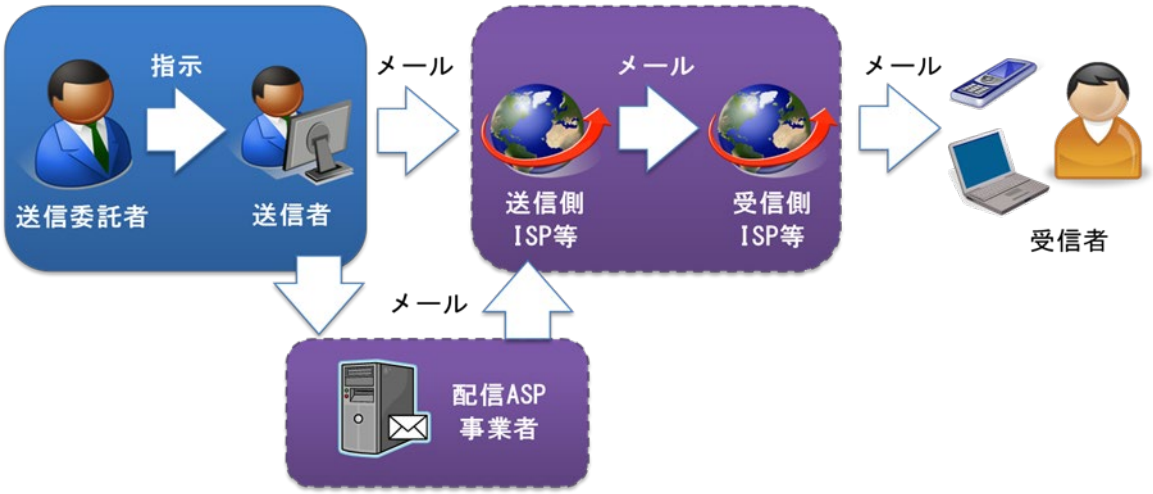
送信委託者

自らは操作を行わないが送信先や送信内容について一定の指示をしている者（団体）

以下の場合は送信者、送信委託者には該当しません

広告の依頼を行っている広告主

メール送信のためのシステムを提供する ASP 事業者




**＊ケーススタディ＝★「送信者」と「送信委託者」参照**

【特定電子メールにならないもの】

以下のような内容については広告・宣伝のための手段には当てはまらないため特定電子メールには当たらないとされています。

取引上の条件を案内する事務連絡や料金請求のお知らせなど取引関係に係る通知であって広告または宣伝の内容、Web サイトへの誘導もないメール

単なる時候の挨拶であって広告または宣伝の内容、Web サイトへの誘導もないメール

政治活動・非営利団体活動が送信するものは「営利目的の団体または営業を営む個人」が送信するものではないため当てはまらない

## ■国際連携の強化

条文では国内から送信されるケースだけでなく、送信元の地理的な位置に関わらず国内の受信者に当てて送信されるケースも当てはまることが明記されました。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

# 適切なメール配信のための十三ヶ条

チーターデジタル・メール配信ガイドラインでは、法令遵守と運用上の推奨となるポイントを絞って、「十三ヶ条」としてまとめました。なお、「適切なメール配信のための十三ヶ条」のうち1～6を「法令遵守編」、7～13を「チーターデジタル推奨編」として解説します。

| | |
|---|---|
| 法令遵守編 | **1. 事前に同意を得た相手にのみ送信する** |
| | **2. 同意の記録を保存する** |
| | **3. 容易な方法でメール受信の拒否ができるようにする（オプトアウト）** |
| | **4. 送信するメールには「送信者」に関する情報を記載する** |
| | **5. 送信者情報を偽った送信をしない** |
| | **6. 架空アドレス宛の送信をしない** |
| チーターデジタル推奨編 | **7. 受信制限に関する情報を提供する** |
| | **8. 「正しい」形式のメールを送信する** |
| | **9. 受信者メールアドレスを表示する** |
| | **10. 受信者からの返信を受付ける** |
| | **11. 送信者ドメインの WHOIS 情報を登録する** |
| | **12. 送信ドメイン認証に対応する** |
| | **13. 受信者の立場になって方針を考える** |

＊より理解を深めて頂くために、巻末に以下の情報をまとめていますので合わせてご活用ください。

ケーススタディ・・・当社サービスでの運用シーンを例に具体的な手順など

付録(Cheetah Messaging) ・・・ご利用サービス（Cheetah Messaging での設定方法等

参考・・・技術的な用語の解説

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

# 法令遵守編

## ～法律の必須事項とチーターデジタル推奨ベストプラクティス～

### 1. 事前に同意を得た相手にのみ送信する

特電法：第3条第1項

メールを送信するに当たり、必ず相手の明確な意志を確認する（オプトイン）ことが法的に必須です。同意取得時に表示するべき事項やその方法などにも言及があるので今一度確認しましょう。

**【同意の範囲】**

同意の範囲について求められるのは「広告・宣伝に関するメールを受信すること」でありメールの種類や詳細な内容等を特定することまでは義務付けられてはいません。

**【同意取得時に表示するべき事項とその方法】**

- 広告・宣伝メールの送信が行われること
- 送信者が誰であるか

上記2点が「通常の人間であれば認識できるような形」と定義されていますが、具体的な方法については限定されていません。少なくとも誤解を招くような表記方法を避け、シンプルな方法で認識されるような工夫が必要です。

例えば、最後の確認画面などで、受信者に対して、「広告・宣伝メールの送信について同意した状態となっていること」や「送信される広告・宣伝メールのタイトル等」を表示することが望ましいとされています。

なお、送信頻度が多い場合や容量の大きいメール（HTML メール、デコメールなど）を送信する場合など受信側の負担が大きくなることが想定されるような場合にはあらかじめその旨を伝えておく方が良いでしょう。

※同意の取得方法（好ましくない例）

- 電子メールアドレスの登録時に、契約を申し込むサービスの約款や利用規約に同意の通知の相手方の名称及び特定電子メールを送信する旨の記載があっても、極めて小さい文字で下部に記載されている場合。
- 約款や利用規約が長くウェブサイトを膨大にスクロールして、注意しないと認識できないような場所に記載されている場合。
- 「関連サイトから広告・宣伝メールが送信される」旨を記載していても、「関連サイト」、「姉妹サイト」という表現しかしていない場合。（送信者又は送信委託者を具体的に特定することができないため、適切に同意が取得されているとはいえない。）

**【同意の取得方法（チーターデジタル推奨）】**

同意の取得の際には「本人による同意の意思表示」を確認することが非常に重要になります。

先ず、「本人」の確認以前にメールアドレスの正当性について確認しましょう。

- メールアドレスとして正しい形式になっているか
- 登録されたアドレスのドメインは実在するか

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

- 登録されたアドレスに正常にメールが届くか
- 携帯アドレス限定の場合、他ドメインのアドレスが登録できないようになっているか

ダブルオプトイン

登録依頼のメールや Web 画面で入力されたデータを受け取った時点で登録するのではなく、そのアドレスへ確認メールを返信し、確認メールに対する何らかの操作を以て本人の意志表示を確認するという「ダブルオプトイン」による同意取得が最も望ましいとされています。

また、最初の登録時だけでなく、受信者がメールアドレス等の変更をする場合にも「ダブルオプトイン」で変更の確認をすることが推奨されています。

返信メールがエラーになった場合は登録しないで下さい。

迷惑メールフォルダや受信拒否でエラーが戻って来ない場合もあるため「エラーがない＝登録」とすることは避けましょう。

＜参考：シングルオプトイン＞

登録依頼のメールやWeb画面で入力されたデータを受け取った時点で登録する「シングルオプトイン」は、入力ミスや虚偽のアドレスが増加し、配信エラー率やレピュテーションに影響する可能性があります。それにより配信ブロック発生やスパム判定のリスクがあるため、当社では「ダブルオプトイン」を推奨しています。

**【デフォルトオン／オフ】**

Web 画面などで同意を取得する際のチェックボックスは、デフォルトの状態がオン（同意）なのかオフなのかは、一概にどちらが良いということは定められていません。受信者の認識、同意の意思表示の確認が取れているかどうかがポイントです。

ただし、サービスの内容等により可能であれば「デフォルトオフ（同意しない）」にすることが推奨されています。

デフォルトオンにする場合は、チェックボックスを見えやすい場所に設置する、「チェックを外さない場合は同意したことになる」旨を簡単に認識できるような工夫をする、チェックボックスが複数ある場合には一括で全てのチェックを外す機能をつける等の対応を推奨します。

※デフォルトオンの好ましくない例
利用者の入力や閲覧が必要のない事項などが長く記載され、チェックボックスがその下部に設置されていて利用者が一覧できないような表示。（この場合は、画面上のわかりやすい場所に、下部にチェックボックスがある旨の注意文を明確に記載する工夫をすべきとされています。）
利用者がチェックを外して次の画面に進んだにもかかわらず、「戻る」ボタン等で前の画面に戻ると、チェックボックスに再度チェックがされている状態に戻っている場合は、有効な同意の意思表示とはみなされません。

※例外（同意取得が不要なケース）
事業者にとって過度な負担とならないよう、通常の商習慣などから、常識的にオプトインがなくても問題にならないようなケースは例外として認められることになっています。

**＊ケーススタディ ★同意取得時に表示するべき事項とその方法 参照**

**＊ケーススタディ ★第三者を通じた同意の取得について 参照**

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

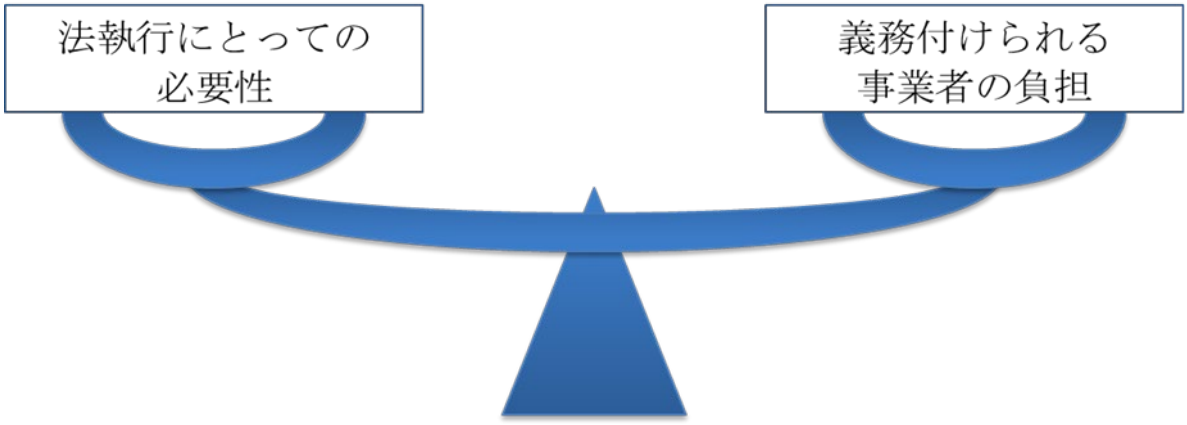
## 2.　同意の記録を保存する

特電法：第3条第2項

**【同意の保存】**

オプトイン規制では事前の同意の有無が適法であるかどうかが非常に重要な判断基準となるため、同意取得に関する記録が義務付けられています。

この記録については法執行にとっての必要性が高い一方で、保存を義務付けられる事業者にとってはその負担が大きくなってしまうことが懸念されるため、「過剰な負担とならない範囲」という配慮も行われています。




**【保存すべき内容】**

以下のいずれかの内容を保存するべきとされています。

1）各メールアドレスに関して同意を取得した際の時期、方法等の状況を示す記録

2）送信先メールアドレスが区別できるようにされている記録に加えて、以下の区分に応じた記録

－同意の取得を書面で行う場合：
　当該同意の取得に際して示す書面の書式
－同意の取得を電子メールの送信と返信により行う場合：
　当該同意の取得に際して示す電子メールの内容のうち定型的な部分
－同意の取得をウェブサイトから行う場合：
　当該同意に際して示すウェブサイトの画面構成

**【保存期間】**

特電法では、「メールの送信をしないこととなった日から1ヶ月」とされており、措置命令を受けた場合は、その命令に係る送信のタイミングにより変わりますが、命令を受けた日から1年間前後になります。

一方、特商法では措置命令の有無に関わらず3年間保存が必須となっているため、実質3年間の保存を意識した対応が必要になります。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 3. 容易な方法でメール受信の拒否ができるようにする

特電法：第3条第3項

**【オプトアウト】**

同意を取得した相手にメールを配信していても後から不要と意思表示された場合には以後送信してはならないと明記されています。従って、そのような申し出を受けた場合には速やかに配信対象から除外するような運用を行う必要があります。

特に、除外対応が遅れることにより、「解除依頼を出してもメールが届く」場合の反応が非常にシビアになってきており、受信者から非常に悪い印象を持たれてしまいます。

印象が悪くなると、たとえ送信元や解除方法が明記されていても、受信者が配信元と接触すること自体を嫌い、配信元の情報が ISP や迷惑メール相談センターなどの公的窓口や、民間のスパム DB 等へ“通報”されてしまいます。最終的には、ISP からの利用停止やスパムフィルター製品等が参照するブラックリストへ登録されてしまうなどの影響を受ける可能性があります。

【参考】配信解除を簡単な操作で

- 登録処理と同様に、解除用の空メールアドレスを用意する、Web 画面で解除を受け付けるなど、手続きが複雑にならないようにしましょう。例えば、Web 画面で複数のメールから選択して解除する場合は、一括で全てのメールを解除できる仕組みもあるとよいでしょう。
  また、メールにオプトアウト用のリンクを記載する場合は、リンクから登録削除が成功するように会員 ID・登録削除対象となるリスト情報など、オプトアウトに必要な情報を含めるとよいでしょう。

- 配信するメールに「List-Unsubscribe ヘッダ」を付加することで、登録解除に必要な情報（登録解除フォーム URL や退会用空メールアドレス等）が受信者に伝わりやすくなります。
  - ✧ Cheetah Messaging をご利用の場合
    キャンペーン（記事）を配信すると、List-Unsubscribe ヘッダが自動的に付加されます。

- 「なりすまし」や「操作ミス」などにより、本人の意思によらず解除されてしまうことがないように注意しましょう。登録処理と同様に、解除確認メールから Web 画面へ誘導することで、メール到達性による本人確認の精度を上げることをお勧めします。

【参考】解除処理は迅速に

解除を受け付けた後、何日もメールが送信されてしまうと、受信者の印象が非常に悪くなります。迅速に解除処理ができるよう、手順を整えておきましょう。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 4.　送信するメールには「送信者」に関する情報を記載する

特電法：第4条

【表示するべき内容】
オプトアウトを確実にするため、送信するメールには「配信事業者名」と「解除方法」に関する情報を記載することが義務付けられました。なお、携帯メールのように文字数が少ない場合は Web への URL でも構いません。

また、初めて配信する相手には「どのような経緯で配信対象になったか」を説明する内容のメールを前もって送信することを推奨します。

【表示に関する注意事項】
受信者にとって表示内容が「分かり易い」ことが重要です。
表示する場所は、送信するメール本文の先頭もしくは末尾とし、文字数などの制限がある場合にはリンク先での掲載も可能ですが、リンク先での表示内容が分かり易いようにしましょう。

また、オプトアウトを確実に行うため、連絡先として掲示したメールアドレス・URLからのフィードバックが確実に受け取れるようにしましょう。オプトアウトの対応は迅速に行うことが大事です。

**＊ケーススタディ「★同意取得時に表示するべき事項とその方法」参照**
**＊「付録 2：Cheetah Messaging での表示義務内容への対応」参照**

## 5.　送信者情報を偽った送信をしない

特電法：第5条

送信者情報には、From アドレスの他、IP アドレス等の情報も含まれますが、ここでは特に From アドレスについて注意事項を記載します。
なお、「■実効性の強化（措置命令と罰則）」に書いてあるとおり、送信者情報を偽った場合は、即時罰則が適用されてしまいます。

**【From アドレス】**
送信専用のアドレスであっても、ユーザやドメインが存在するものを設定し、「From アドレスは送信専用である旨」と「問い合わせ受付窓口」を明記の上、もしそのアドレスにメールが送信されてもエラーにならないようにしましょう。
受け取ったメールは内容確認できるのが望ましいですが、エラーになるのを防ぐため、少なくとも、受信したメールを適宜破棄してメールボックスフルを防止する等の準備をご検討下さい。

また、携帯アドレスのドメインや大手 ISP・Web メールサービスのドメインではなく、自社が管理するドメインを From に設定するようにした方が、受信者にも分かり易くなります。

【参考】当社サービスでは、From アドレスのドメインは事前登録制となっております。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 6. 架空アドレス宛の送信をしない

特電法:第6条

**【架空アドレスの定義】**

特電法の中では「架空電子メールアドレス」とは、次のいずれかに該当するアドレスであると定義されています。

- 多数の電子メールアドレスを自動的に作成する機能を有するプログラム(電子計算機に対する指令であって、一の結果を得ることができるように組み合わされたものをいう。)を用いて作成したものであること。
- 現に電子メールアドレスとして利用する者がないものであること。

多量のエラーアドレス宛に送信することは「架空アドレス宛」の送信と見られる可能性があります。

**【エラーアドレスへの送信は NG】**

携帯キャリアや大手 ISP では、エラーアドレスを多く含む配信に対する規制を行っています。

多量のエラーアドレスを含む配信を行うと、キャリアや ISP でメールの受信が拒否され、正しいアドレスに対しても送信ができなくなる場合があります。

キャリアや ISP の規制は、該当の配信だけではなく、同じ From アドレスからの配信や、同じサーバやシステムからの配信にも影響が及ぶ可能性があります。

架空アドレスやエラーアドレスを多量に含む配信は行わないでください。

【参考】キャリアや ISP によるこのような規制は、特電法の中で以下のように明示的に許容されているものです。

*(電気通信役務の提供の拒否)*

*第11条 電気通信事業者は、送信者情報を偽った電子メールの送信がされた場合において自己の電子メール通信役務の円滑な提供に支障を生じ、又はその利用者における電子メールの送受信上の支障を生ずるおそれがあると認められるとき、一時に多数の架空電子メールアドレスをそのあて先とする電子メールの送信がされた場合において自己の電子メール通信役務の円滑な提供に支障を生ずるおそれがあると認められるとき、その他電子メールの送受信上の支障を防止するため電子メール通信役務の提供を拒むことについて正当な理由があると認められる場合には、当該支障を防止するために必要な範囲内において、当該支障を生じさせるおそれのある電子メールの送信をする者に対し、電子メール通信役務の提供を拒むことができる。*

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

# チーターデジタル推奨編

## ～よりよい運用のために～

### 7.　メール受信制限に関する情報提供

チーターデジタル・レコメンド

**【受信制限】**

携帯キャリアは、「迷惑メール対処法」として携帯ユーザ向け受信制限（特定のドメインやアドレスからのメール受信を拒否する設定や受信を許可するドメインを明示的に設定するなど）を案内しています。
この制限により送信したメールが届かないといったことがないように、受信するドメインやアドレス等の情報を正確に伝え、受信制限の確認や解除を促しましょう。

また、安易に From アドレスを変更しないようにしましょう。

SoftBank や、au のデフォルト設定では、受信拒否のエラーが送信元に戻ってこないため、送信側では受信拒否に気付きにくくなっていますので、注意が必要です。

### 8.　「正しい」形式のメールで送る

チーターデジタル・レコメンド

正しいメール形式になっていない場合は受信者が見たときに文字化けしてしまったり、本文の内容が全く見えなくなってしまったりするだけでなく、迷惑メールフィルタによって本人が読む前に除外されてしまう場合もあります。

特に最近は携帯アドレス宛にも HTML 形式のメールが送信できるようになってきており、送信する内容が複雑化してきていますのでご注意下さい。

主に以下のような点に注意して正しいメール形式で送信しましょう。

**●文字化け（メール本文、標題の文字コード、機種依存文字）**

PC での Unicode 文字コード利用の拡大により、送信側のメールソフトでは入力・送信できるのに、受信側のメールソフトや携帯では表示できない、または、文字化けしてしまう漢字・記号も増えています。人名の漢字一文字のために、携帯が対応していない文字コードでメールを送信しまい、携帯側ではメール本文全部が文字化けしてしまうケースもあります。

**●携帯宛メールで「絵文字」を使う際の実装**

携帯宛メールでの絵文字の利用について、docomo、au、SoftBank から公式に情報提供されています。
絵文字の送信方法についてはそれらを参照してください。
送信方法の変更もあり得るので、十分かつ継続的な送信テストが必要です。」

- docomo
  https://www.nttdocomo.co.jp/service/imode_mail/function/pictograph/
- au
  https://www.au.com/mobile/service/emoji/
- SoftBank
  https://www.softbank.jp/mobile/service/mail/smartphone/pictgram/

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

**●HTML メール（PC、携帯）の形式**

デコメール（アレンジメール、デコレーションメール）については、PC の HTML メールと違い、細かな規定が必要となります。PC のメールソフトで HTML メールを作成しても、携帯側でデコメール表示とならない場合があります。また、各社各機種でデコメールのバージョンが異なり、受信者側の携帯で期待した表示とならないこともあります。

PC 宛てでは、受信者が HTML メールに対応していない場合を考慮し、マルチパートでの送信をお勧めします。

**●メール本文中の URL**

メール本文に含まれる URL のドメインは、メール送信者の自社ドメイン、From アドレスのドメインまたはそのサブドメインなど、受信者にとって、送信者とリンク先の関係が明確なものが望ましいです。まったく関係のない URL の場合には、フィッシング詐欺などの疑いを持たれたり、フィルタリングソフトで誤判定されたりする場合もあります。

URL の長さは、携帯向けに限らず、長すぎる URL は折り返されてリンク先に遷移できない場合もあるので、注意が必要です。

URL の数が多いと、迷惑メールとみなされる可能性があります。目安として、URL 数は 60 個以内にすることを推奨します。

●メールサイズ

テキストメールで、メールサイズが大きいと、メール本文中の URL がクリックできない状態（シンプルなテキストのみ）になる可能性があります。目安として、テキストメールのメールサイズは 30KB 以内にすることを推奨します。

## 9. 受信者メールアドレスの表示

チーターデジタル・レコメンド

メールの受信者は複数の電子メールアドレスを所有し、1つの集約メールボックスに転送している場合があります。その場合、登録に利用したメールアドレスが所有する複数のメールアドレスのうち、どのメールアドレスで登録したかを忘れてしまう場合があります。送信先の電子メールアドレスをメール本文に記載し、受信者が登録に利用した電子メールアドレスを思い出せるようにしましょう。

## 10. 受信者からの返信の受付け

チーターデジタル・レコメンド

「3. 容易な方法でメール受信の拒否ができるようにする」で述べたように、オプトアウトが速やかにできないと受信者に非常に悪い印象をもたれてしまいます。メールや WEB サイトに記載したオプトアウトの案内の通りにオプトアウトできなかった場合でも、受信者がオプトアウトできるように、送信したメールの返信を受付け、受信者からの問い合わせに対応できるようにしましょう。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 11. 送信者ドメインの WHOIS 情報登録

チーターデジタル・レコメンド

WHOIS は IP アドレスやドメイン名の登録者などに関する情報を、インターネットユーザーが誰でも参照できるサービスです。送信者ドメインの情報を WHOIS に登録し、送信者情報の透明性を高めることで、受信者からの信頼を高めましょう。

## 12. 送信ドメイン認証への対応

チーターデジタル・レコメンド

送信ドメイン認証は大きく分けて SPF、DMARC、DKIM の 3 種類があります。

当社では、送信したメールの到達性への影響から、From ドメインの SPF の対応は必須としています。また、貴社ドメインのなりすましメール被害に対するリスク低減につながるため、DMARC への対応を推奨しています。

【送信ドメイン認証の普及状況】

- SPF

  多くの ISP や携帯キャリアで、なりすましによるメール送信をブロックするために送信ドメイン認証技術が採用され、ほぼ対応が完了しています（送信する側での対応および受信する際のフィルタリング）。特に携帯キャリアは From ドメインの SPF に対応していない場合は、なりすましメール判定するフィルタ機能を提供しているため、From ドメインの SPF は必須になっています。

携帯キャリアのユーザ向けなりすまし対策機能

| キャリア | 設備側の実装 | ユーザ向けの機能 |
|---|---|---|
| docomo | ドメイン認証が成功したものしか受信しない | なりすまし対策としてドメイン認証結果によるフィルタ設定を提供 |
| au | SPFにより送信ドメインが認証できないメールには宛先不明のエラーを返さない | SPFドメイン認証結果によるフィルタ設定を提供 |
| SoftBank | － | なりすまし対策としてドメイン認証結果によるフィルタ設定を提供 |

- DMARC

  Gmail や Outlook（Hotmail）をはじめとする海外の主要 ISP では、DMARC による送信ドメイン認証に対応しており、なりすましメール被害のリスクを低減する有効な手段と認識されており、国内でも普及が進むと考えられます。

- DKIM

  海外、国内の主要 ISP では DKIM による送信ドメイン認証に対応しています。

【送信ドメイン認証の対応方法】

- SPF / DKIM / DMARC

  お客様が From アドレスに指定したメールアドレスのドメインを管理する DNS にて設定が必要になり

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

ます。

＊「付録 1：送信ドメイン認証対応手順」参照

DMARC に対応すると、貴社からのメールであるかのようになりすましたメールを受信側でどのように処理するか制御できるようになります。具体的には、送信元ドメインをなりすましたメールに対して、「そのまま通す（none）」、「隔離する（quarantine）」、「受信拒否する（reject）」の 3 種類のポリシーのいずれかを選択することが可能です。

当社サポートセンターから DMARC の導入方法をご案内する際は、「そのまま通す（none）」のポリシーを採用した設定となりますが、このポリシーままでは、なりすましメール被害のリスクは低減されません。「隔離する（quarantine）」または「受信拒否する（reject）」に設定することを推奨します。

ただし、「隔離する（quarantine）」、「受信拒否する（reject）」のポリシーを設定するには注意が必要です。

詳しくは、「参考5：DMARC の導入」をご確認ください。

## 13. 受信者の立場になって方針を考える

チーターデジタル・レコメンド

【ポリシーの基準】

判断に迷った時にどうするかという基準を「ポリシー」として決めておくことは非常に大切です。

運用サイドの都合より受信者の立場を考え、常に「分かり易い説明、表記」を心がけましょう。

受け取り側の印象には個人差があります。「自分が受け取り側だったらどうか？」、複数の人、男性/女性、年代の異なる人の意見を聞きましょう。

「チーターデジタル・メール配信ガイドライン」に関するお問い合わせ

ご意見・ご要望・疑問点等は、下記までお寄せ下さい。

abuse.japan@cheetahdigital.com

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

# ケーススタディ

## ★同意取得時に表示するべき事項とその方法

同意取得時に表示するべき事項は、この 2 点とされています。
・広告・宣伝メールの送信が行われること
・送信者が誰であるか
同意の範囲について求められるのは「広告・宣伝に関するメールを受信すること」であり、メールの種類や詳細な内容までを特定することまでは義務付けられてはいません。ただし、【適切なメール配信のための十三ヶ条】の「13.受信者の立場になって方針を考える」から考えると、受信者の立場から安心して受信に同意＝登録してもらったメールは、迷惑メールと思われにくく、読んでもらうことにつながることは明らかです。当社の同意取得のあり方の推奨例は以下のとおりです。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

●フォーム登録（ダブルオプトイン）の場合の、メール応答例

SUBJ:メール登録手続きのお知らせ

このメールは○○メールマガジン登録用フォームにて
登録を希望されたメールアドレスに対して、
自動応答で返信しています。

○○メールマガジンに登録を希望される方は、
以下の URL をクリックし、配信に関する説明をご一読の上、
必要項目を入力し、登録ボタンを押して
配信に同意ください。
https://www.example.com/r.p?m=fe3rwah9
このメールに覚えのない方、あるいは登録をしない場合は、
捨て置きください。

また、このメールに覚えのない方で、何度もこのメールが
届くような場合にはお手数ですが、
info@example.com までお知らせください。
---
チーターデジタル株式会社
info@example.com/03-5786-2655

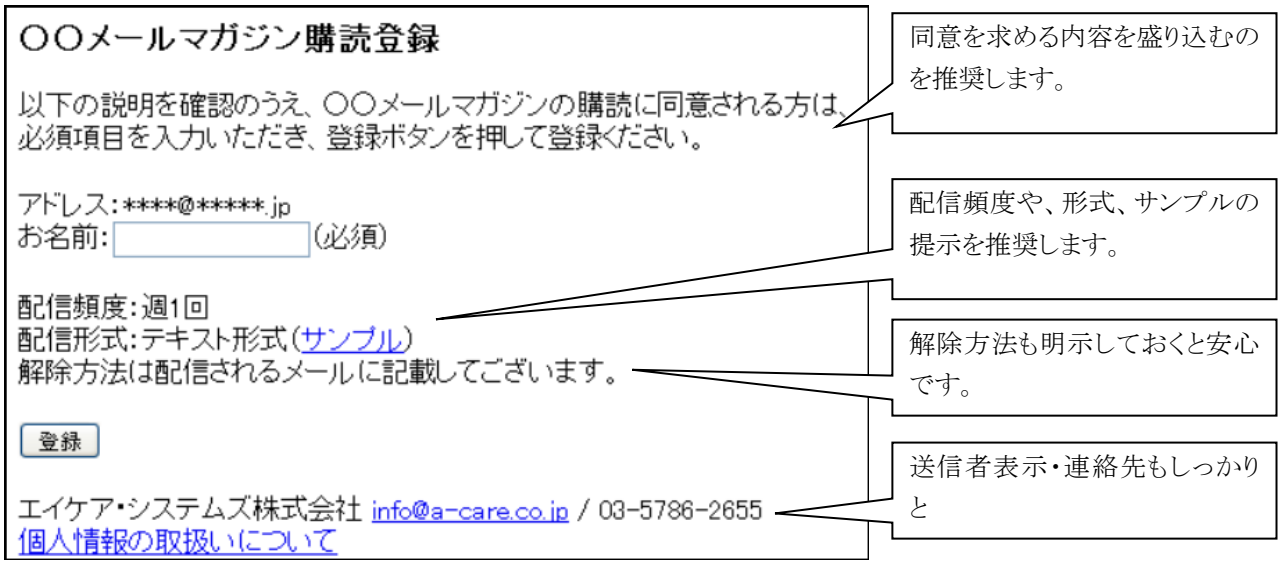
メール送信の理由を明記します。
フォーム入力に対する自動応答なので、
アドレス誤入力やいたずらで無関係の
人に送信される可能性があります。

Web だけでなく、メールにも同意を求める内容を盛り込むのを推奨します。

連絡先もしっかりと

送信者表示・連絡先もしっかりと

●メールマガジン登録フォーム画面例




同意を求める内容を盛り込むのを推奨します。

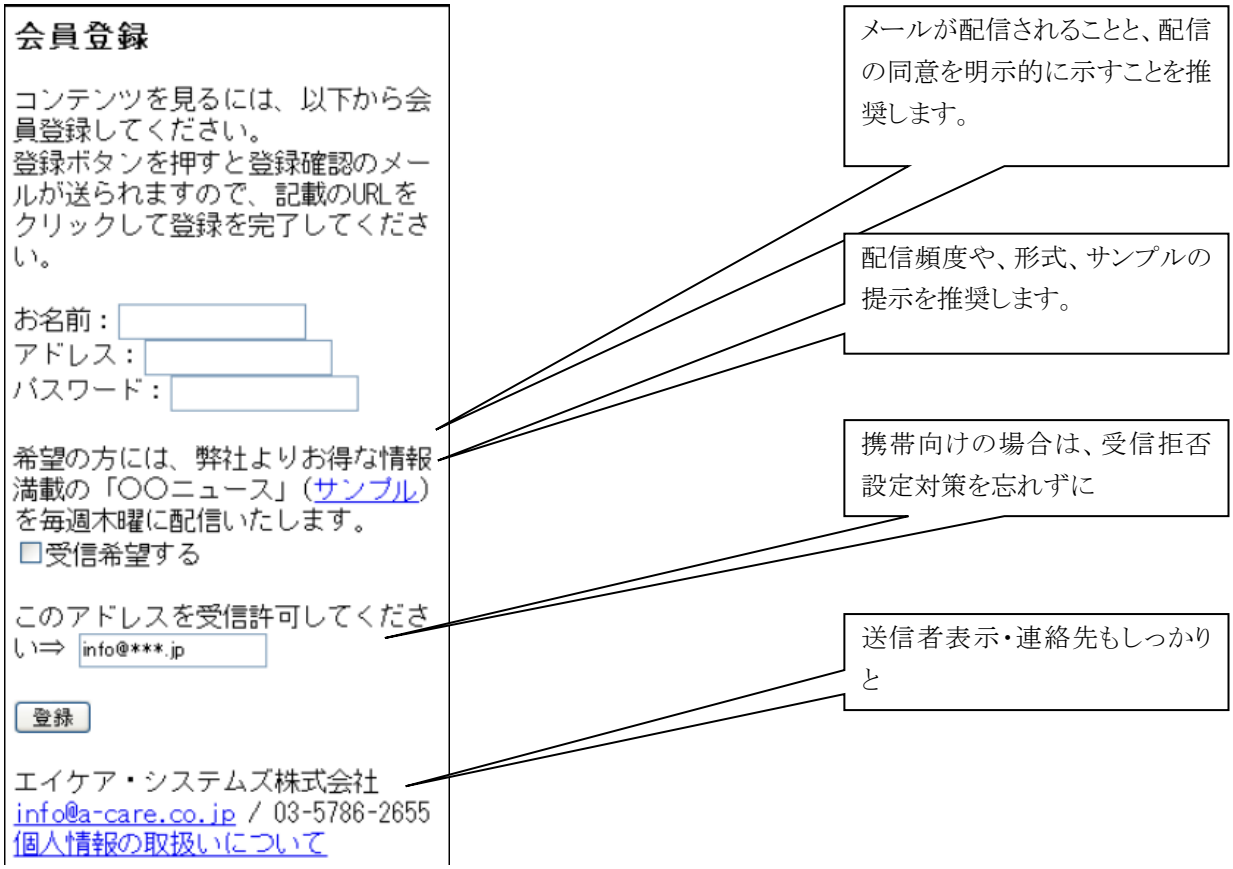
配信頻度や、形式、サンプルの提示を推奨します。

解除方法も明示しておくと安心です。

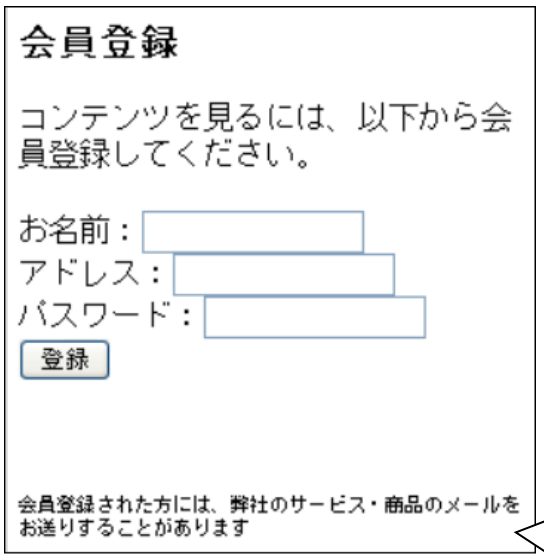
送信者表示・連絡先もしっかりと

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

●会員登録に付随してメールを送信する場合のフォーム画面例




●改正法に則らない表示例 （！注意！ 推奨例ではありません）




電子メールアドレスの登録時に、契約を申し込むサービスの約款や利用規約に同意の通知の相手方の名称及び特定電子メールを送信する旨の記載があっても、極めて小さい文字で下部に記載されている場合などのように、通常の受信者であればそれに気付くとは考えにくい場合などは、受信者が認識できるように表示されているとはいえません。

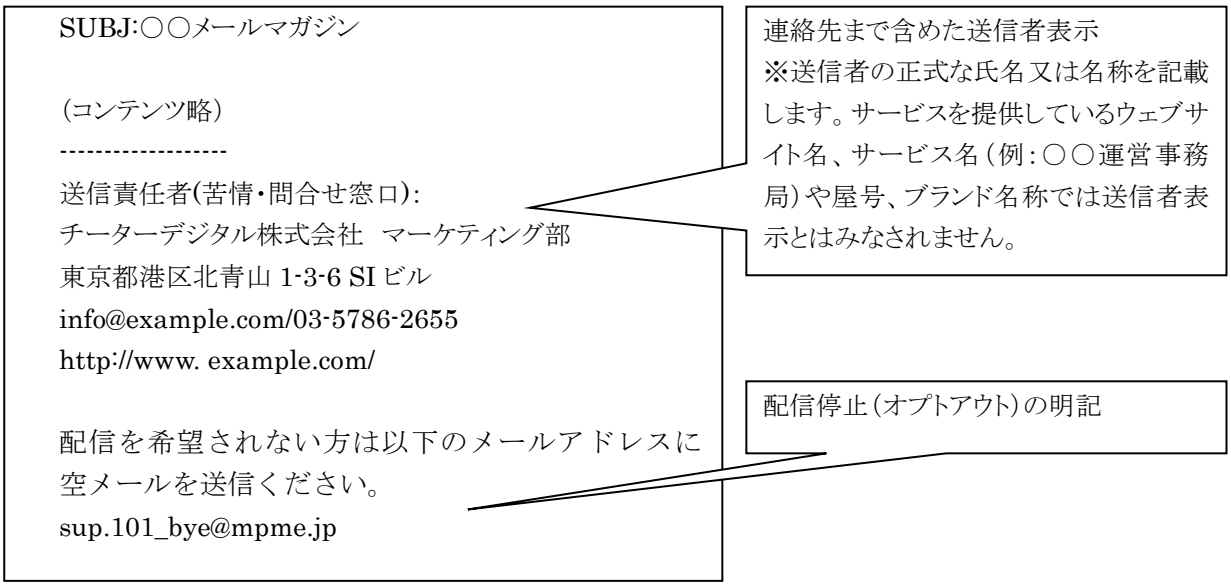
また、「関連サイトから広告・宣伝メールが送信される」旨を記載していても、「関連サイト」、「姉妹サイト」という表現しかしていない場合も、送信者又は送信委託者を具体的に特定することができないため、適切に同意が取得されているとはいえません。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

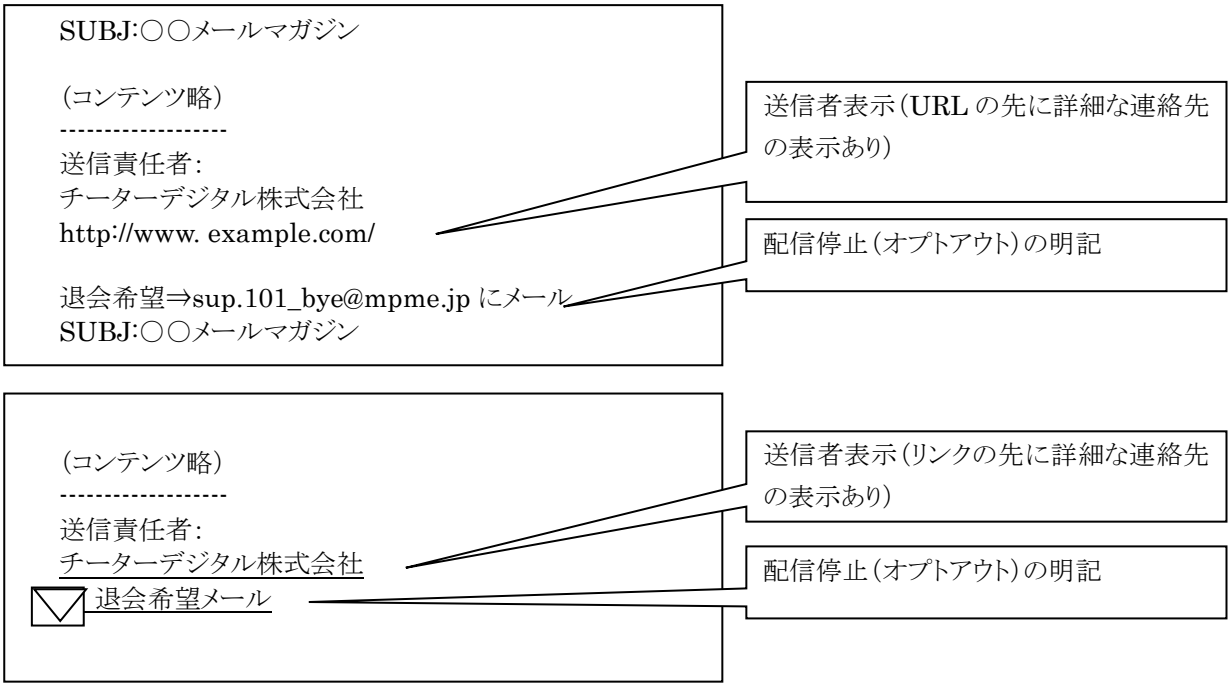
## ★表示義務への対応

送信するメールには「配信事業者名」と「解除方法」に関する情報を記載することが義務付けられています。なお、携帯メールのように文字数が少ない場合は Web への URL でも構いません。

●チーターデジタルの推奨例




●携帯メールなど文字数に限りがある場合




Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## ★「送信者」と「送信委託者」

わが社は「送信者」？「送信委託者」？それ以外？

改正法にのっとり、受信者から同意を取ってメール配信を行っているのであれば、「送信者」、「送信委託者」の差は実際にはほとんどありません。

仮に、実際には子会社が「送信者」で、自社は送信委託している「送信委託者」であっても、自社を『送信者』と表示することは、違法ではなく、むしろ受信者にとっては、「優しい」表示といえます。

注意するべきは、自社が「送信委託者」であって、第三者である「送信者」にメール配信を行わせている場合に、「送信者」が表示義務、オプトイン義務に違反しているような場合には、「送信委託者」も義務違反となってしまうケースです。

広告主のつもりで依頼していて「送信委託者」としての義務違反の指摘を受けるようなことがないように、実際に配信されるメールの内容をしっかり確認する必要があります。

●A 社が、広告主ではなく「送信委託者」とみなされてもおかしくないメールの例

○○様

耳より情報！
A 社の新サービス××！
新鮮な体験、ぜひ味わってください！
http://companyA.jp/

お問い合わせはこちらまで
info@companyB.jp

## ★第三者を通じた同意の取得について

「キャンペーン」「合同イベント」などを通じて収集されたメールアドレスにメール送信を行いたいというご要望を、当社にいただくことがございます。

改正特電法の総務省ガイドラインでは、

> (略)第三者を通じて利用者から同意を取得し、その送信者や送信委託者の名前で広告・宣伝メールを送信する(略)ような場合において、第三者を通じた同意の取得に際し、当該第三者とは別の特定の送信者・送信委託者から広告・宣伝メールが送信される旨を表示していないものや、そうした表示があったとしても通常の利用者が認識できるようには表示していないものもあるが、それらについては、法律で定めている送信者又は送信委託者に対する同意の通知には該当しないものである。

とあります。当社としては、送信者と送信されるメールについての対応が、先に推奨例として示したような、明確な形で受信者に示されていることが必要と考えております。

改正法の移行措置により、すでに送信に対して同意を得ているメールアドレスへの送信は、改めて同意を得る必要がないとされていますが(附則第 2 条)、このような第三者を通じて同意を得たメールアドレスが手元にあって同意を得た記録も改正法に準じた形で保管されていないようなケースでは、改正法施行後に、

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

受信者に改正法に則っていない「違法な」メールと受け取られる可能性が十分にあります。

当社としては、特に第三者を通じて同意を得たメールアドレスで、改正法に準じた形で同意の記録を得ていないメールアドレスへの送信は、送信しないことを推奨します。

やむを得ず送信を行いたい場合でも、同意を得た状況を可能な限り具体的に示し、改めて、同意を得る誘導を行い、同意が得られた受信者にのみ引き続き送信を行うことを推奨します。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

# 付録(Cheetah Messaging)

『付録 Cheetah Messaging)』は、チーターデジタルの Cheetah Messaging をご契約頂いたお客様向けの内容です。

貴社ご自身で送信ドメイン認証の運用を行ったり、当社サービス以外をご利用されたりする場合、別途設定や確認が必要となる可能性があります。

詳しい設定方法などは、**『迷惑メール対策推進協議会』**において公開されている各種資料や本書の参考情報をご覧ください。

https://www.dekyo.or.jp/soudan/aspc/

**また、本資料も上記『迷惑メール対策推進協議会』によって公開されている情報を参考として記述しております。**

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 付録 1:送信ドメイン認証対応手順

Cheetah Messaging、及び貴社の既存メール配信システムから配信を行う上で、メール配信到達性の担保・向上のためには、『送信ドメイン認証』に対応する必要があります。

### ◆対応手順の概要

メール送信で利用する[Header-From]ドメイン(送信者 From アドレスのドメイン部)に対して、送信ドメイン認証用の DNS 設定を行います。

| STEP | 項目 | 内容 | 担当 |
|---|---|---|---|
| 0 | **メール送信で利用するドメインの決定** | [Header-From ドメイン]を決定する | 貴社 |
| 1 | [Header-From ドメイン]のサブドメインの委譲 | STEP0 で決定した[Header-From ドメイン]を弊社 DNS に委譲する。<br>※[Header-From ドメイン]を委譲できない場合は、そのサブドメインを委譲する。その場合、Step2 以降の作業が必要です。 | 貴社 |
| 2 | [Header-From ドメイン]のサブドメインへの SPF レコードの登録 | 委譲された[Header-From ドメイン]のサブドメインに対して SPF レコードを登録する (SPF への対応) | 弊社 |
| 3 | [Header-From ドメイン]用の各種送信ドメイン認証用レコードの発行 | [Header-From ドメイン]に対して、以下のレコードを発行する<br>・Sender ID レコード<br>・DKIM／DomainKeys レコード<br>・DMARC レコードの発行 | 弊社 |
| 4 | [Header-From ドメイン]への SPF レコードの登録 | [Header-From ドメイン]に対して 3 で発行された Sender ID レコードを登録する (SPF／Sender ID への対応)<br>※注意点「参考7:SPF チェック仕様」参照 | 貴社 |
| 5 | [Header-From ドメイン]への DKIM／DomainKeys レコードの登録 | [Header-From ドメイン]に対して 3 で発行された DKIM レコードを登録する (DKIM への対応) | 貴社 |
| 6 | [Header-From ドメイン]への DMARC レコードの登録 | [Header-From ドメイン]に対して 3 で発行された DMARC レコードを登録する (DMARC への対応) | 貴社 |
| 7 | 既存メール配信システムへの送信ドメイン認証設定 (DKIM／DomainKeys) | Cheetah Messaging 以外のメール配信システムを利用中の場合、かつ本資料で挙げた送信ドメイン認証に未対応の場合、同様に対応することが望ましい<br>ただし、設定することが出来ないシステムの場合にはこの限りではない | 貴社 |

※ 4～6 は同時に作業して構いません (4→5→6 と順番に進める必要はありません)

※ 7 の設定方法は、当該システムの提供元に確認してください
(弊社サービスでない場合、弊社では回答出来兼ねます)

### ◆詳細手順

Cheetah Messaging 導入時にお渡しする以下の資料をご確認ください。

**「送信ドメイン認証対応用 DNS 設定依頼資料」**

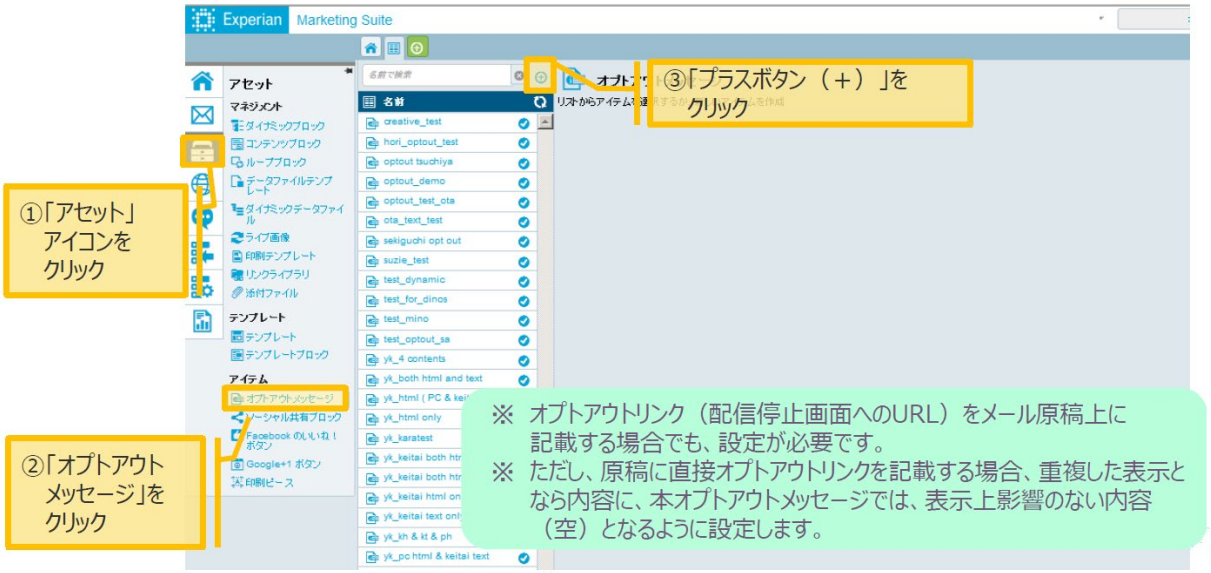
Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 付録 2：Cheetah Messaging での表示義務内容への対応

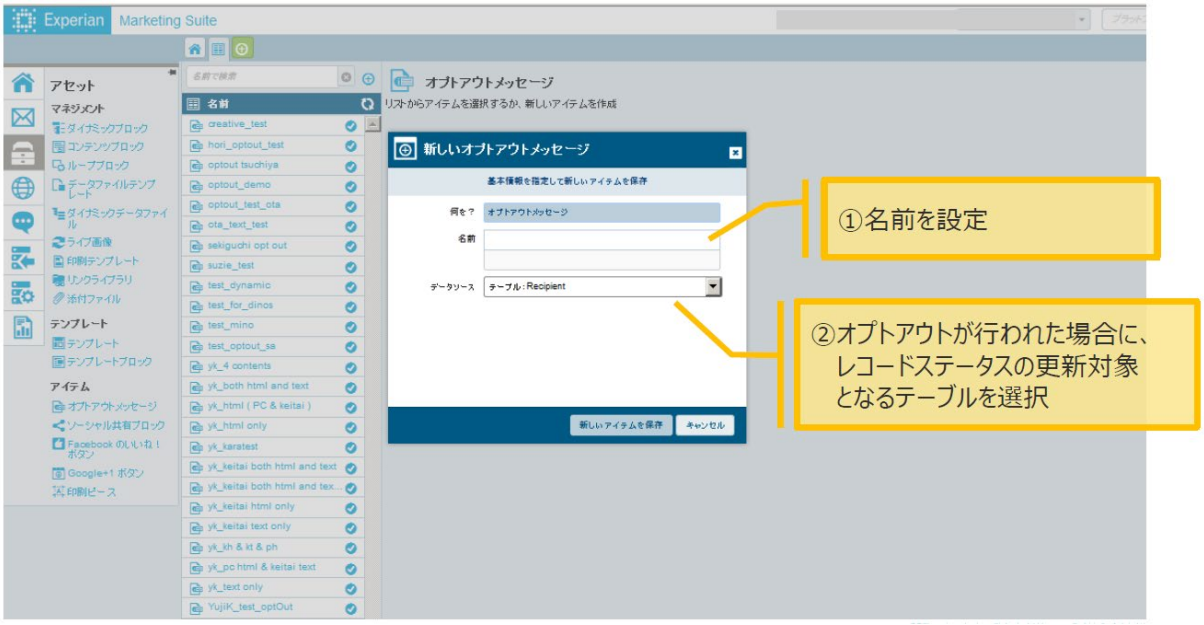
Cheetah Messaging では、配信解除表示（オプトアウトに関する記載）をもれなく行うため、オプトアウトメッセージを含まない原稿は送信できない仕様となっています。

### ◆オプトアウトメッセージ機能

オプトアウトメッセージをパーツとして事前に作成しておき、キャンペーンの原稿に差し込みます。

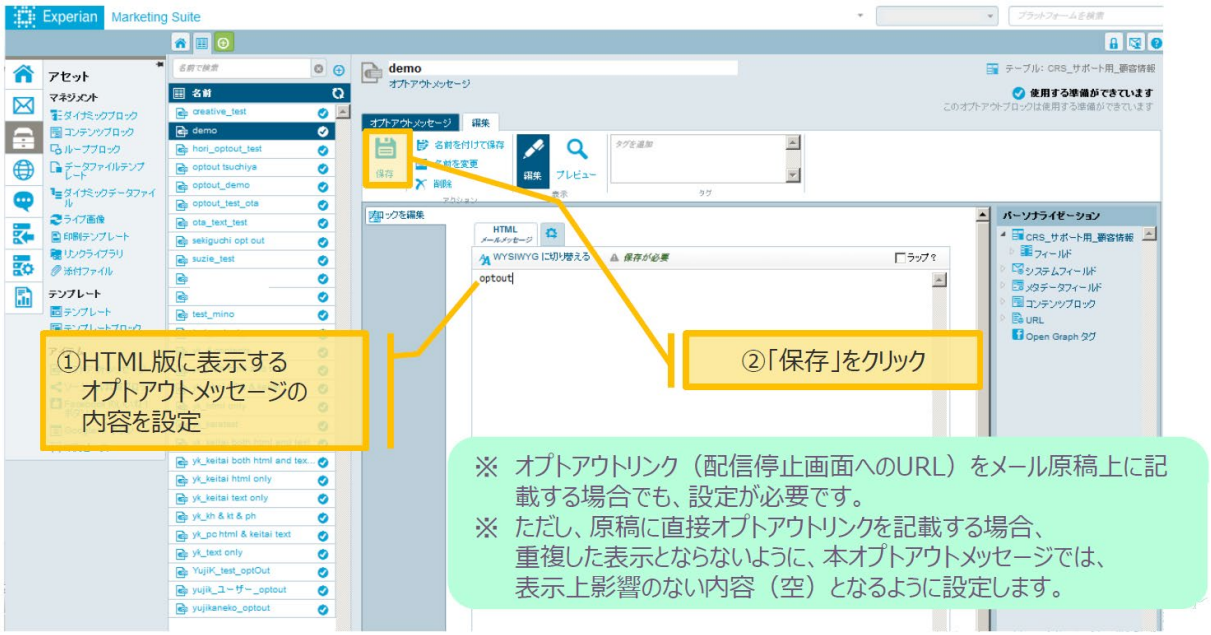



オプトアウトメッセージを利用してオプトアウトが行われた場合に、レコードステータスを更新する対象となるテーブル（予め送信者プロファイルが設定されている必要があります）を選択します。




HTML 版に表示するオプトアウトメッセージの内容を設定します。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

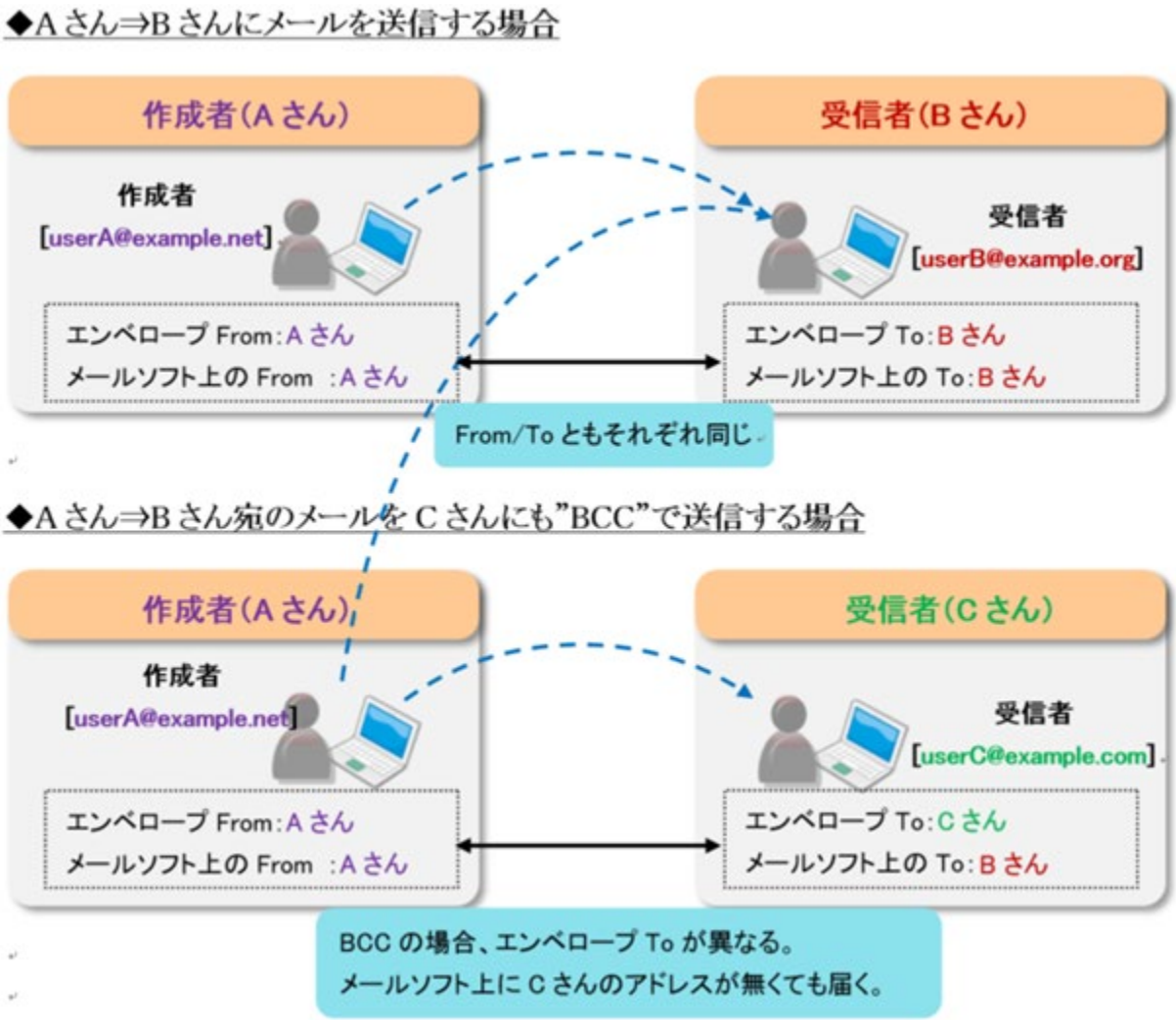



Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

# 参考

## 参考1:メールヘッダ基礎知識

メールを配信するときにメールサーバ間で使用するヘッダ(エンベロープ From、 To)と、メールソフトに表示されているヘッダ(From、 To)とは、異なります。
通常は、エンベロープ From と From、エンベロープ To と To は同じ値になっていますが、BCC でメールを送るときには異なる値になっています。




Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 参考2：送信ドメイン認証とは

・「なりすましメール」被害のリスクを低減する技術
・正規のドメインの所有者からのメールを識別できる
・送信元 IP アドレス方式、電子署名方式、とそれを組み合わせた方式の三つに大別される

### ◆送信ドメイン認証技術の種類

| 方式 | ①ネットワーク方式<br>（送信元 IP アドレス方式） | ②電子署名方式 | ①と②の組み合わせ |
|---|---|---|---|
| 代表的な規格 | SPF※1/SenderID | DKIM※2 | DMARC※3 |
| 特徴 | ・国内で普及が進んでいる<br>・送信側で導入が容易<br>・送信元のIPアドレス確認のみ可能 | ・欧米で普及が進んでいる<br>・送信側で導入に若干手間がかかる<br>・メールヘッダ（件名・差出人など）、本文に改竄がないことを保証 | ・欧米で普及が進んでいる<br>・送信側で導入に若干手間がかかる<br>・なりすましメールを隔離、拒否できる<br>・第三者からなりすましメールが送られたことを検出できる |
| 仕組み | 送信元を IP アドレスやホスト名により確認する | 送信元を（送信時に）付加された電子署名の検証により確認する。 | ・SPF と DKIM の組み合わせで送信元の正当性を評価する。 |

※1 SPF･･･Sender Policy Framework の略称
※2 DKIM･･･ DomainKeys Identified Mail の略称
※3 DMARC･･･ Domain-based Message Authentication, Reporting & Conformance の略称

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 参考3：ネットワーク方式（送信元 IP アドレス方式/SPF/SenderID）とは

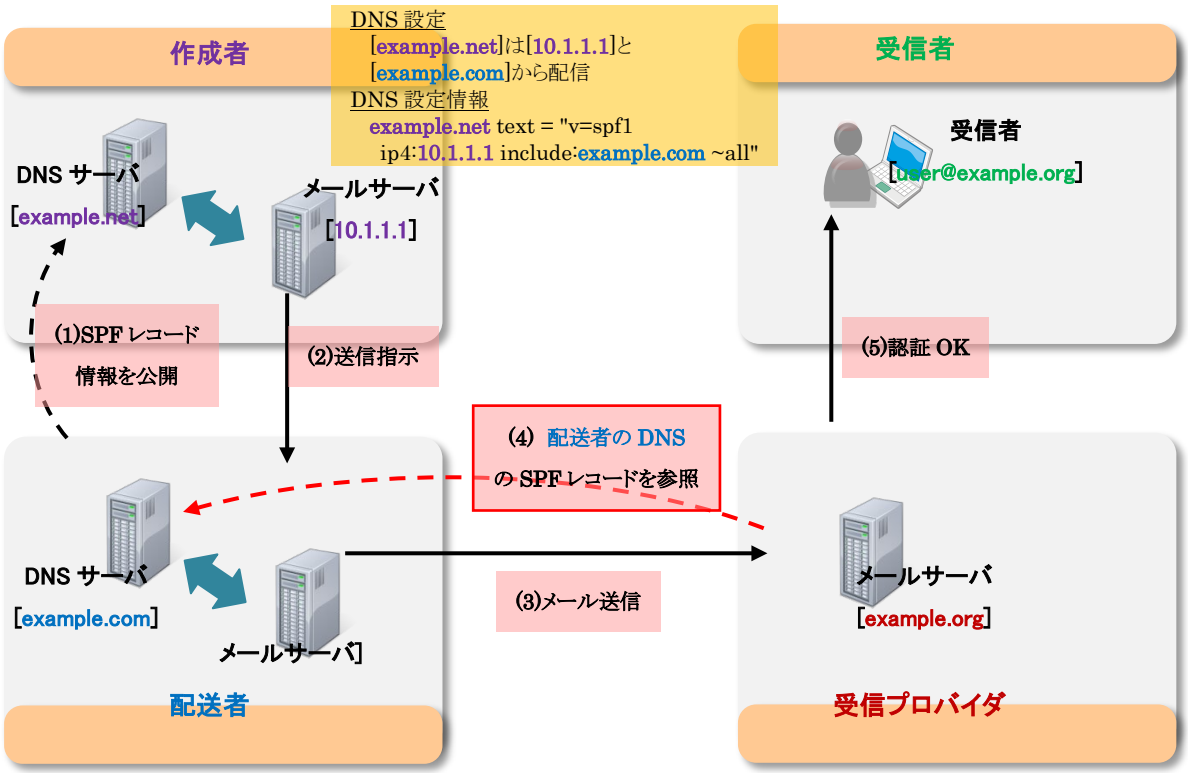
・SPF と Sender ID の基本的な仕組みは同じ
・送信元ドメインの DNS から正規の送信元ホスト情報を取得し、 それと実際の送信元 IP アドレスを照合して検証

### ◆SPF と SenderID の違い

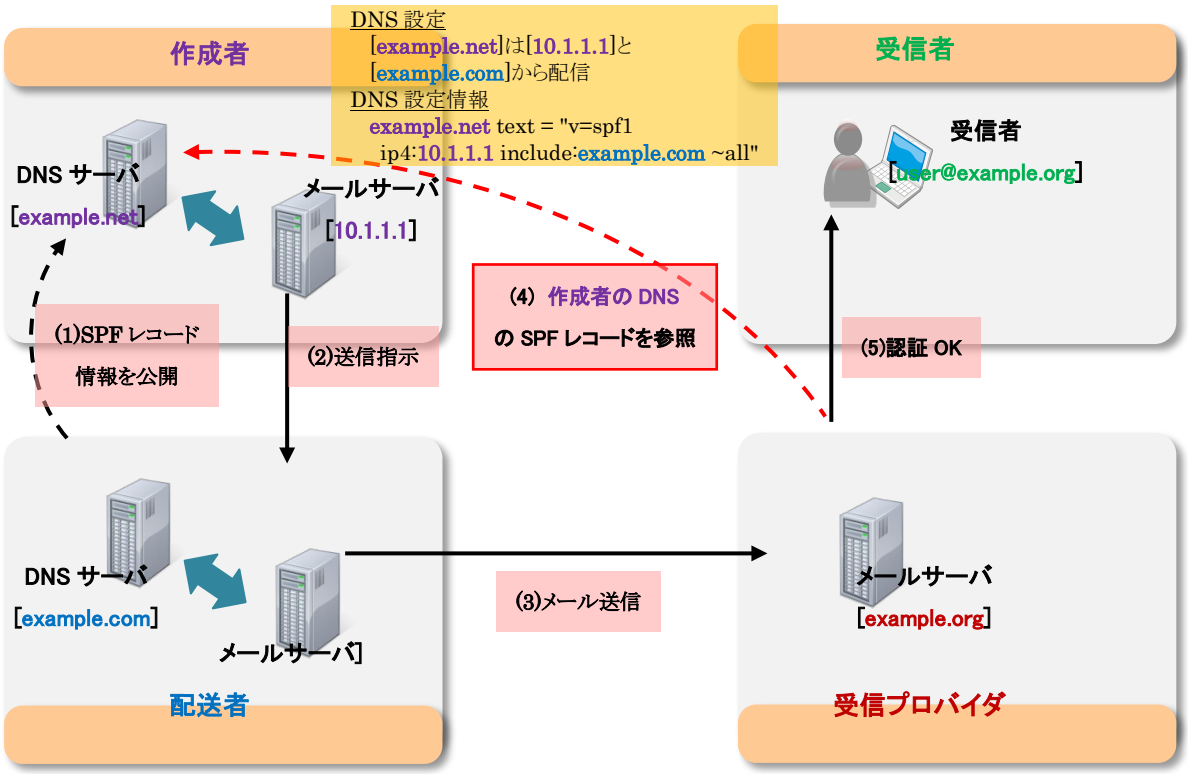
| 方式 | 提唱元 | 検証対象のヘッダ情報 | SPF レコード<br>バージョン番号 |
|---|---|---|---|
| SPF | Pobox.com の<br>Meng Wong 氏 | Envelope-From のみ検証 | v=spf1 |
| SenderID | Microsoft | 検証するヘッダの指定と順番が v=の値で指定可能 | |
| | | Envelope-From、Resent-Sender、Resent-From、Sender、From を順番に検証 | v=spf1（Sender ID として解釈）または、Spf2.0/mfrom.pra |
| | | Envelope-From のみ検証 | Spf2.0/mfrom |
| | | Resent-Sender、Resent-From、Sender、From を順番に検証 | Spf2.0/pra |

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## ◆SPF によるドメイン認証のイメージ




## ◆SenderID によるドメイン認証のイメージ




Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## ◆主要各社のドメイン認証（SPF・SenderID）実施状況

※当社調べ

<table>
<tr><th colspan="2">主要各社</th><th>SPF</th><th colspan="3">Sender ID</th></tr>
<tr><td rowspan="4">携帯キャリア</td><td rowspan="3">docomo</td><td rowspan="3">－</td><td colspan="3">○フィルタリング(オプション)<br>“成りすましメール拒否フィルタ”<br>利用者は「拒否しない（＝フィルタを適用しない）」「存在しないドメインを拒否」「すべてを拒否」から選択可能。</td></tr>
<tr><td rowspan="3">Fromアドレスのドメイン</td><td>存在しないドメイン</td><td>「存在しないドメインを拒否」<br>「すべてを拒否」で受信拒否</td></tr>
<tr><td>SPF レコードの設定が無い</td><td>「すべてを拒否」で受信拒否</td></tr>
<tr><td>SPF レコードの設定に無い<br>IP からの配信</td><td>すべてを拒否」で受信拒否</td></tr>
<tr><td>au</td><td>○フィルタリング（オプション）<br>認証 NG の場合でもエラーは返さない</td><td colspan="3">－</td></tr>
<tr><td>SoftBank</td><td>－</td><td colspan="3">－</td></tr>
<tr><td rowspan="2">Web メール</td><td>Windows LiveMail</td><td>－</td><td colspan="3">判定失敗で受信拒否</td></tr>
<tr><td>Gmail</td><td rowspan="4">ヘッダに判定結果追加</td><td colspan="3" rowspan="4">－</td></tr>
<tr><td rowspan="3">ISP</td><td>OCN</td></tr>
<tr><td>DION</td></tr>
<tr><td>Biglobe</td></tr>
</table>

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## ◆SPF/Sender ID によるドメイン認証に対応するための DNS 設定

ドメイン認証に対応するには、送信元ドメインを管理するDNSサーバに IP アドレス情報を設定します。

■送信元ドメインとは

【SPF の場合】

エンベロープヘッダ（MAIL FROM）に指定されているドメイン。

【SenderID の場合】

一般のヘッダ情報※1（From、Sender など）に指定されているドメイン。

※1 PRA（Purported Responsible Address）と呼ばれるヘッダ情報。

■設定の記述先

DNS の TXT レコード

■設定内容

送信元ドメインについて発信元となるサーバの IP アドレスを登録します。

メールを送信する全てのサーバの IP アドレスを把握する必要があります。

■設定書式

**［バージョン］［定義］［定義］ ・・・**

【バージョン】

SPF の場合 「v=spf1」

SenderID の場合 「v=spf2.0」

【定義】

［ディレクティブ］と［修飾子］で構成される。

また［ティレクティブ］は［限定子（クオリファイア）］と［機構（メカニズム）］で構成される

【限定子（クオリファイア）】

メカニズムの定義にマッチしたホストの扱い。省略時は認証成功（PASS）と扱う。

| クオリファイア | 認証結果 | 意味 |
|---|---|---|
| ＋<br>（プラス） | PASS | 認証成功 |
| －<br>（マイナス） | FAIL | 認証失敗<br>この定義にマッチするホストからはメールが送信されることはない |
| ～<br>（チルダ） | SoftFail | 認証情報を公開しているが、場合によっては認証できないメールも存在する |
| ？<br>（クエスチョン） | Neutral | 認証情報を公開しない |

【機構（メカニズム）】

送信元ホストを定義するルール。（※以下、主なものを抜粋）

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

| メカニズム | 引数 | 意味 |
|---|---|---|
| all | なし | 全てのホストにマッチ<br>all 以降に指定されたものは無視されるため通常 SPF の末尾に記載し else 的な役割を持つ |
| a: | ドメイン名 | 指定されたドメインスペックの A レコードにマッチ |
| include | ドメイン名 | 指定されたドメインスペックの SPF レコードを読み出してチェックする |
| mx: | ドメイン名 | 指定されたドメインスペックの MX レコードに指定されているホストの A レコードにマッチ |
| Ip4: | IP アドレス | 指定された IPv4 アドレスまたはネットワークアドレスにマッチ<br>ネットワークの指定には CIDR 標記が可能 |

【認証結果】

| 値 | 意味 |
|---|---|
| none | SPF レコードが宣言されていない |
| neutral | 送信元のドメインでは、該当のホストが認証できたかできないかを明らかにしない |
| pass | 認証に成功した |
| policy: | 認証は成功したがローカルなポリシーによってその認証結果は受け入れられない |
| hardfail | 認証が失敗した |
| softfail | 認証は失敗であるが、はっきりと認証失敗としては扱ってほしくない |
| temperror | 一時的な問題で認証処理を実行できなかった |
| permerror | SPF レコードの文法的な誤りなど永続的なエラーで認証処理を実行できなかった |

■設定記述例

*"v=spf1 +ip4:xxx.xxx.xxx.xxx ?all"*

メール送信元が[xxx.xxx.xxx.xxx]であれば認証成功。
それ以外からの場合は認証情報を公開しない(?all)。
テスト公開などの場合に ?all の記述を用いる。

*"v=spf1 +ip4:yyy.yyy.yyy.yyy/28 ~all"*

メール送信元が[yyy.yyy.yyy.yyy/28]のネットワークに含まれていれば認証成功。
それ以外からの場合は SoftFail とする(~all)。
受信側での SPF レコードの利用をより積極的に(メールフィルタの情報として)利用してもらいたい場合に[~all]の記述を用いる。
**SPF はメールが転送された場合に相性が悪いので、~all の記述が現実的。**

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

*"v=spf1 -all"*

web サーバなど、メールを全く送信しない場合の公開例。

■[?all] [~all] [-all] の使い分け

(1) メール配信を行うドメインで、SPF レコードを最初に設定する際には、[?all]で設定するのが無難
この場合、「+」クオリファイアにマッチした場合は認証成功として扱われる。
「+」クオリファイアが指定されていないサーバからメールが送信されていた場合でも受信側では特に何もせず SPF レコードが無い場合と同様の扱いを行う。
そのため、SPF レコードを公開していない場合と同じである、といえる。

(2) 次のステップとして SPF レコードの登録に漏れや記述間違いなどがないことが確認できてから[~all]に移行するのが望ましい

(3) -all としてしまうのは、メールが転送された場合を考慮すると(現時点では)推奨できない
SPF のチェックは、受信側サーバが最終的にメールを送ってくるサーバの情報を利用して行うため、メールが転送されてしまった場合は SPF チェックで -all にマッチしてしまうため。

**ネットワーク方式(送信元 IP アドレス方式)の問題点**

◆メール転送時の問題

認証処理を行う MTA の直前にある MTA のみが認証可能な対象直前のサーバしかチェックできない

→SPF の場合の対策:Sender Rewriting Scheme(SRS)
転送時にエンベロープの送信者に転送した(オリジナルの)送信者の情報を追加する。
※受信者による転送で SRS が実装されている場合、バウンス解析情報を失う

→Sender ID の場合の対策:Purported Responsible Address(PRA)
メール転送時に「Resent-From:」や「Resent-Sender」の追加認証処理を実施する MTA では、
Resent-Sender → Resent-From → Sender → From の順番でアドレスをチェックする。

◆DNS 設定内容の問題

原則として IP アドレスをキーとして設定を行うが、将来的に IPv6 の普及が進んだ場合、テキストレコードのメンテナンスに大きな影響を及ぼすと考えられる。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## ◆SPF レコードの記述例

### ■正しい記述例

SPF レコードは、記述ミスを防ぐため、なるべく簡潔に記述するよう心がけましょう。また、簡潔に記述することが、受信側での認証処理の負荷を軽減することにもつながります。
include や redirect、またマクロの機能等は、間違いを起こしやすいので、本当に必要な場合にのみ利用し、ip4 や ip6 の記法で簡潔に記述することを推奨します。

■ホストの IP アドレスで記述

```
example.net. IN TXT "v=spf1 ip4:10.0.3.1 ip4:10.0.3.2 ip4:10.0.3.3 -all"
```

メール送信サーバの IP アドレスを直接指定します。送信メールサーバの数があまり多くない場合には、この記述方法を推奨します。

■ホスト名で記述

```
example.net. IN TXT "v=spf1 a:mx01.example.net a:mx02.exmaple.net a:ns.example.net -all"
```

メール送信サーバのホスト名を指定します。IP アドレスを直接指定する方法に比べて、メンテナンスが簡単ですが、受信側の認証処理で DNS への負荷が少し増える可能性があります。ホスト名は、必ず FQDN で指定します。

■ネットワークでの指定

```
example.net. IN TXT "v=spf1 ip4:10.0.4.0/28 -all"
```

メールを送出する可能性のあるホストが存在するネットワークを、CIDR 方式で指定します。CIDR にあまり小さい値を指定すると(つまりネットワークの領域をあまり広く指定すると)、SPF レコード自体の意味がなくなるため、最小限のネットワーク範囲で利用します。

■ホストの IP アドレスとネットワークアドレスの混在

```
example.net. IN TXT "v=spf1 ip4:10.0.3.0 ip4:10.0.3.1 ip4:10.0.3.2 ip4:10.0.4.0/28 -all"
```

ホストの IP アドレスの指定とのネットワークの指定とを混在させることも可能です。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

■サブドメインに個別の SPF レコードを定義する

```
example.net. IN TXT　"v=spf1 ip4:10.0.3.0 ip4:10.0.3.1 ip4:10.0.3.2 -all"
announce. example.net. IN TXT　"v=spf1 ip4:10.1.4.0 ip4:10.1.4.1 -all"
campaign. example.net. IN TXT　"v=spf1 include:example.org -all"
```

メール配信を外部業者に委託しているよう場合、それらの配信メールの送信元サーバの IP アドレスを SPF レコードに追加する必要があります。しかし、外部業者が多数に上る場合など、レコードの管理が複雑になることが考えられるので、可能であれば、それらの業者ごとに専用のサブドメインを払い出して、本来の業務用のドメインと切り離して管理するという方法もあります。業者が既に SPF レコードを公開していれば、include を利用してそのレコードを利用できます。

## ■誤った記述例

文法的に間違った SPF レコードを公開すると、受信側では permerror と扱われ、せっかく公開しても正しく扱われないことになってしまうばかりでなく、受信側で認証を pass したメール以外受信しないようなサービスを提供していた場合、メールが届かなくなる可能性があります。

■バージョンの間違い(その1)

```
example.net. IN TXT "v=spf1.0 ip4:10.0.3.1 ip4:10.0.3.2 ip4:10.0.3.3 -all"
```

"v=spf1.0" は間違っており、"v=spf1" でなければなりません。

■1つのドメインに対して複数の SPF1 レコードを公開している

```
example.net. IN TXT "v=spf1 ip4: 10.0.3.0 ip4: 10.0.3.1 ~all"
example.net. IN TXT "v=spf1 a:mx01.example.org ~all"
example.net. IN TXT "v=spf1 a:web.example.org ~all"
```

1 つのドメインに対しては1つの SPF1 レコードだけ公開可能です。複数公開するとエラーになります。ただし、SPF2 のレコードと SPF1 のレコードを1つずつ同時に公開することはできます。

■入力ミス

```
example.net. IN TXT "v=spf1 ipv4: 10.0.3.0 ip4: 10.0.3.1 ~all"
```

" ipv4" は間違っており、" ip4" でなければなりません。

```
example.net. IN TXT "v=spf1 ip410.0.3.0 ip4: 10.0.3.1 ~all"
```

" ip4" の後ろには":(コロン)"が必要です。";(セミコロン)"や"=(イコール)"も間違いやすいので気をつけてください。

■半角スペースが抜けている

```
example.net. IN TXT "v=spf1 ip4: 10.0.3.0ip4: 10.0.3.1 ~all"
```

各レコード情報の区切りに" (半角スペース)"を入力する必要があります。全角スペースとも間違えないよう、注意が必要です。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

■各ドメインのレコード情報が相互参照している

```
example.net. IN TXT "v=spf1 include:_spf.example.net ~all"
_spf.example.net. IN TXT "v=spf1 include:example.net ~all"
```

includeしている先のドメインのSPFレコードで、元となるドメインをincludeしてしまい、相互参照が起こるとエラーになります。IPアドレスやホスト名は必ず正引き/逆引き検索などを行い、相互参照となっていないことを確認してください。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 参考4:電子署名方式(DKIM)の導入

・あらかじめ公開鍵を DNS に設置し、メールヘッダに電子署名を付与して送信。
・受け取ったメールサーバは、基本的にはその電子署名の引数からドメインを取り出し、DNS に公開鍵を問い合わせ、取得した公開鍵で電子署名を検証する。

### ◆DKIM の特徴

・メール本体(ヘッダーや本文)を元に電子署名を作成するので、転送されたメールに対しても認証が可能です。

### ◆DKIM 作成者署名と第三者署名

A. 作成者(送信者)署名

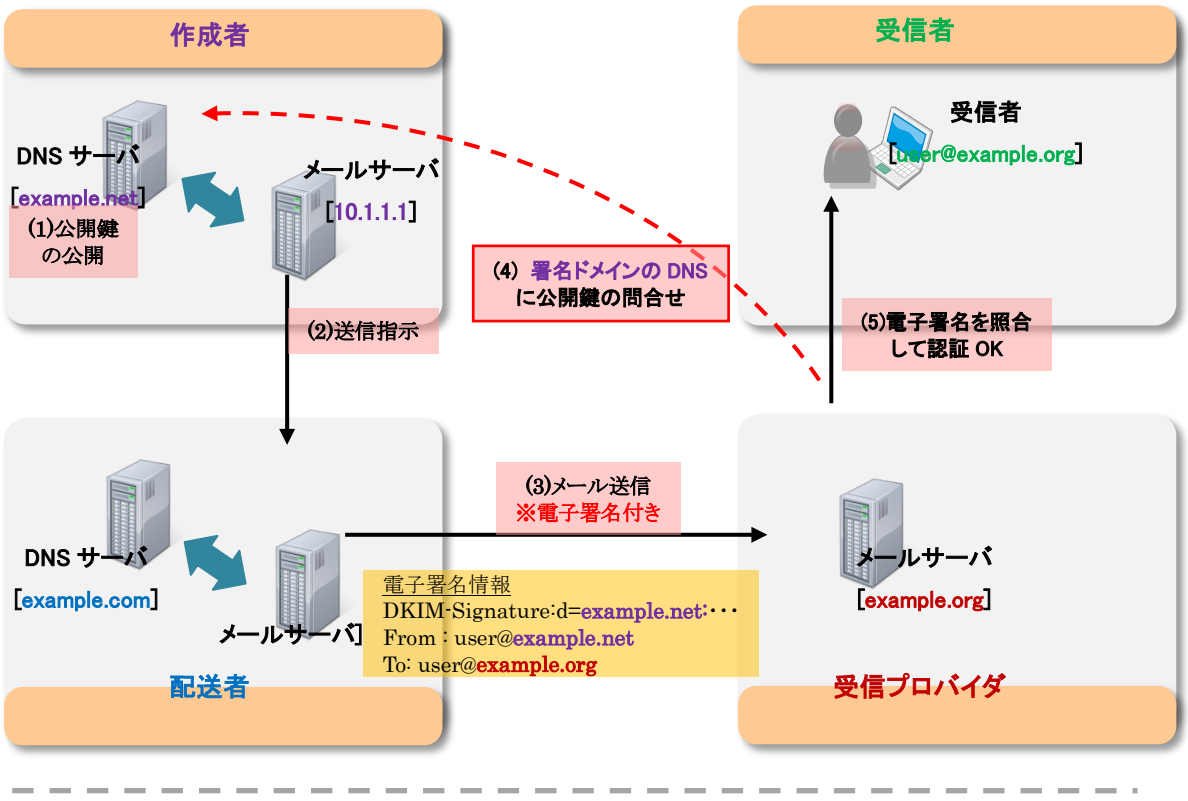
メール作成者ドメインによる電子署名
メール作成者側の DNS において公開鍵を公開します。

B. 第三者署名

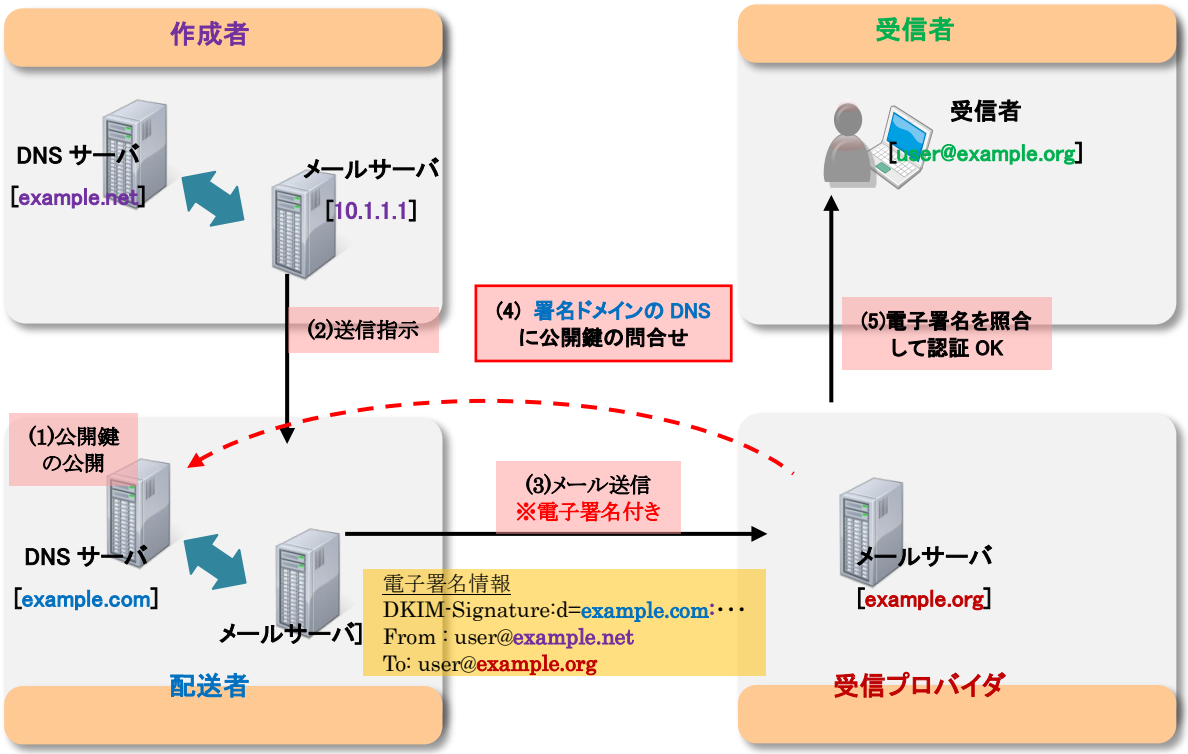
メール作成者ドメイン以外(配送者等)のドメインによる電子署名
メール作成者以外(配送者等)側の DNS において公開鍵を公開します

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## ◆A.作成者（送信者）署名によるドメイン認証のイメージ




## ◆B. 第三者署名よるドメイン認証のイメージ




Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## ◆DKIM によるドメイン認証に対応するための DNS 設定

### ▼設定内容

DKIM によるドメイン認証に対応するには、下記の設定が必要です。
・送信者もしくは配送者のDNSサーバに DKIM 公開鍵を設定します。
・送信者もしくは配送者は、署名を必要とするメールに DKIM-Signature ヘッダを添付します。
※配送者のメールサーバに、電子署名をメールに付与するソフトウェアが必要です。

### ▼公開鍵の設定書式

【DKIM 公開鍵の記述例】

*[セレクタ]._domainkey IN TXT "[タグ]=[値]"*
例）
abc1234._domainkey IN TXT **"v=DKIM1; g=*; k=rsa; p=xxxxxxxxxxxxxxxxx（中略）xxxxxxxxxxxxxxxxxxxx"**

【セレクタ】
DKIM の仕様上、セレクタ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、単純なセレクタ名では重複する可能性がある。セレクタ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。

【ドメイン名】
[ドメイン名]は、DKIM-Signature ヘッダの d タグに指定されたドメイン名となる。
異なるセレクタを用意することで、同じドメインに対して複数の公開鍵を運用できる。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

【タグ】

DKIM レコードで利用できるタグは下記の通り（以下は代表的なものを記載）。

| タグ | 値 | 説明 | 省略の可否 |
|---|---|---|---|
| v | Key レコードのバージョン番号 | ・ 指定する場合は、「DKIM1」になる。省略した場合も、「DKIM1」になる。<br>**・ 指定する場合は、レコードの最初に記述する。** | 設定することが推奨されるが省略可能 |
| g | 鍵の適用条件パターン | ・ 電子署名の対象とするメールのメールアドレスのローカルパートにマッチする条件パターン。<br>・ ワイルドカード文字「*」が利用できる。<br>・ この鍵を利用できる送信者のメールアドレスを限定する場合に利用する。省略時は「*」になる。 | 省略可能 |
| h | 利用可能なハッシュ方式 | ・ 電子署名の作成の際に利用できるハッシュ方式を限定する。省略した場合には、すべてのハッシュ方式を許容する。<br>・ 電子署名の作成者と照合者の両方が sha256 方式をサポートする必要がある。また、照合者は sha1 もサポートする必要がある。 | 省略可能 |
| k | 鍵の形式 | ・ 電子署名の作成の際に利用できる鍵の形式を指定する。省略した場合には、「rsa」になる。 | 省略可能 |
| n | 説明 | ・ 可読な説明文を保持するタグ。省略した場合には、無（長さ0の文字列）になる。 | 省略可能 |
| p | 公開鍵データ | ・ 公開鍵のデータを保持するタグ。鍵データは base64 でエンコードする。<br>・ 値が指定されない場合は、該当の鍵が無効になっていることを示す。 | 必須 |

## ▼電子署名（DKIM-Signature）の作成

送信側では、メール本体（ヘッダ及びメール本文の内容）をもとに電子署名を作成します。作成した電子署名を、DKIM-Signature ヘッダとして付与します。DKIM-Signature ヘッダの書式は、「タグ=値」の組を[;（セミコロン）]で区切って列挙します。

【DKIM-Signature ヘッダの記述例】

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=example.net; s=file.dkim;
        t=125784337; bh=xxxxxxx（中略）xxxxxxx=;
        h=subject:Mime-virsion:Content-Type:From:In-Reply-To:Date
          Cc:content-Trancefer-Encording:Message-Id:References:To;
        b=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx（中略）xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

【タグ】

DKIM-Signature ヘッダで利用できるタグは下記の通り(以下は代表的なものを記載)。

| タグ | 値 | 説明 | 省略の可否 |
|---|---|---|---|
| v | バージョン | ・ バージョン番号を示す。<br>・ 現時点では、「1」と指定する。 | 必須 |
| a | 電子署名の作成に利用したアルゴリズム | ・ 電子署名の作成に利用したアルゴリズムを指定する。<br>・「rsa-sha1」と「rsa-sha256」が利用できる。 | 必須 |
| b | 電子署名データ | ・ 電子署名データ。base64 にエンコードして指定する。 | 必須 |
| bh | 本体のハッシュ値 | ・ 電子署名の対象とした本体のハッシュ値。 | 必須 |
| c | メール本文とヘッダの正規化方式 | ・ 電子署名の作成に利用する正規化処理の方法を指定する。「/」で区切って、それぞれメール本文正規化に利用したアルゴリズムを表示する。<br>・ 「 simple 」と「 relaxe 」が指定できる。省略した場合には、「simple/simple」になる | 省略可 |
| d | ドメイン名 | ・ 電子署名の作成を行ったドメイン名、すなわち、送信ドメイン名を指定する。公開鍵の取得の際に参照するドメイン名の一部になる。<br>・ 後述の i タグに与えられるアドレスのドメイン名は、このタグに与えられる値と同じか、又は、サブドメインであることが必要である | 必須 |
| h | 電子署名の対象としたヘッダ | ・ 電子署名を作成するデータに含まれたヘッダ。: で区切って複数列挙できる。<br>・ 送信者を示すヘッダである From や Sender などは、必ず電子署名の対象に含めることが必要である。 | 必須 |
| i | 認証対象送信者アドレス | ・ メールの送信者や送信プログラム(メーリングリストなどの場合)のメールアドレス。省略した場合には、 d タグに指定したドメイン名の先頭に @ を追加した値になる。 | 省略可 |
| l | 電子署名の対象とした本文の長さ | ・ 電子署名の作成を行ったメール本文の先頭からの文字長(バイト長)。省略した場合は、メール本文すべてを電子署名の対象とする。 | 省略可 |
| q | 公開鍵取得方法 | ・ 公開鍵を取得する方法を指定する。現時点では「dns/txt」のみ指定可能。省略した場合には、「dns/txt」となる。 | 省略可 |
| s | セレクタ | ・ 公開鍵を取得する際に、クエリを発行する対象のドメイン名の一部に利用する。<br>・ 複数のセレクタを持つことで、1つのドメインで複数の公開鍵を利用できる。 | 必須 |
| t | 電子署名実施時のタイムスタンプ | ・ 電子署名を作成した日付を EPOC(1970 年からの秒数)で指定する。省略時は未定義となる。 | 利用推奨(省略可) |
| x | 有効期限 | ・ 電子署名の有効期限について、有効である日時を EPOC(1970 年からの秒数)で指定する。省略した場合は、無期限になる。 | 利用推奨(省略可) |

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

| | | | |
|---|---|---|---|
| z | 電子署名の対象としたヘッダのコピー | ・ 電子署名の対象にしたヘッダの電子署名の作成時の値を保持する。「｜」記号で、複数の指定が可能である。<br>・ デバッグ目的であり、認証処理には利用しない。 | 省略可 |

## ▼受信者のメールサーバ設定

受信側では、メールに付与された DKIM-Signature ヘッダを取り出し、次の手順で電子署名の検証を行います。

1. DKIM-Signature ヘッダの d タグ、s タグの値から、公開鍵を取得する FQDN を作成する
2. 公開鍵を取得する。このとき、i タグに設定してあるメールアドレスのローカルパートが DKIM レコードの g タグの条件パターンにあわない場合は、電子署名の照合を行わない

3. h タグに記述してあるヘッダと、メール本文の内容（l タグで有効な本文の長さが指定してある場合は、先頭からその長さだけを切り出したもの）及び電子署名データ以外の DKIM-Signature ヘッダの値を併せてハッシュを作成する
4. 公開鍵を利用して、DKIM-Signature ヘッダの電子署名データからハッシュを取り出す（復号する）
5. 電子署名から取り出した（復号した）ハッシュと、受信したメールから作成したハッシュを比較して、同じであれば認証成功

## ▼DKIM での認証結果の扱い

DKIM では、認証する対象の送信ドメインは、メールの From ヘッダから取り出すのではなく、DKIM-Signature ヘッダに指定されているドメインや送信アドレスを対象に認証します。

このため、ヘッダ上の送信者である From 行の値と、認証に利用したドメイン名が異なる場合が存在します。

【DKIM での認証結果の値】

| 値 | 意味 |
|---|---|
| none | メールに DKIM の電子署名が付与されていない |
| neutral | メールは DKIM の電子署名が付与されていたが、DKIM の電子署名の文法上の誤りなどで、照合処理できなかった |
| pass | メールに DKIM の電子署名が付与されており、その電子署名は受信者にとって受け入れられるものであり、かつ、電子署名の照合が成功した |
| policy | メッセージには DKIM の署名が付与されていたが、ローカルなポリシーによってその電子署名は受け入れられない |
| fail | メールに DKIM の電子署名が付与されており、その電子署名は受信者にとって受け入れられるものであるが、電子署名の照合が失敗し、認証が失敗した |
| temperror | 一時的な問題で認証処理を実行できなかった |

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

| | |
|---|---|
| permerror | 照合に必要なヘッダが存在しない場合など永続的なエラーで認証処理を実行できなかった |

## ▼DKIM レコードの記述例

DKIM レコードは SPF レコードに比べる指定する内容は簡単ですが、バージョンの記述など間違えないように気をつけて記述するようにこころがけましょう。DKIM レコード公開後に必ず、試験的にメールを送信して認証成功するかどうかを確認することが必要です。

### ◆正しい記述例

※セレクタを「abc.1234」とした場合

◇一般的な正しい記述例

```
abc.1234._domainkey IN TXT
"v=DKIM1; g=*; k=rsa;
p=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
```

◇一般的な正しい記述例（テスト配信用）

```
abc.1234._domainkey IN TXT
"v=DKIM1; g=*; k=rsa; t=y;
p=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
```

### ◆間違った記述例

DKIM のレコードの確認方法の例文法的に間違った DKIM レコードを公開すると、受信側では permerror と扱われ、せっかく公開しても正しく扱われないことになってしまうばかりでなく、受信側で認証を pass したメール以外受信しないようなサービスを提供していた場合、メールが届かなくなる可能性があります。

◇記述間違いの例① 誤ったFQDN上にDKIMレコードを公開している（その1）

```
example.net IN TXT
"v=DKIM1; g=*;
k=rsa;p=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
```

直接該当ドメインの TXT レコードとして公開しています。DKIM の場合、SPF とは異なり、"[セレクタ]._domainkey" サブドメインに公開する必要があります。

◇記述間違いの例② 誤ったFQDN上にDKIMレコードを公開している（その2）

```
_domainkey.example IN TXT
"v=DKIM1; g=*; k=rsa;
p=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
```

[redacted]している。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

正しくは、″セレクタ._domainkey″サブドメインに公開する必要があります。

◇記述間違いの例③　公開鍵方式指定の誤り

```
_domainkey.example.net IN TXT
″v=DKIM1; g=*; k=sha1;
p=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx″
```

公開鍵方式の指定をハッシュの方式と間違えています（k=sha1 ではなく k=rsa)。

◇記述間違いの例④　バージョン記述の誤り

```
_domainkey.example.net IN TXT
″v=DKIM1.0; g=*; k=rsa;
p=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx″
```

DKIM のバージョンを間違えています（v=DKIM1.0 ではなく、v=DKIM1)。

◇記述間違いの例⑤　バージョン記述の位置の間違い

```
_domainkey.example.net IN TXT
″k=rsa; v=DKIM1; g=*;
 p=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx″
```

タグの順番を間違えています。v=タグがレコードの先頭に必要です。

## ▼DKIM のレコードの確認方法の例

現行の送信ドメイン認証技術は、認証情報及びポリシーの公開のために DNS 上に TXT レコードを公開する手法が一般的であるため、これを調査することにより、任意のドメインが送信ドメイン認証技術に対応しているか、ある程度調べることもできます。
下記では例として、UNIX host コマンドの TXT レコードオプションを利用していますが、同様のクエリが発行できれば問題ありません。このような操作を行うことにより、有効なレスポンスがあるかどうかでレコードの有無を判断できます。

◇DKIM / DomainKeys レコードの確認方法
※セレクタを「abc.1234」、From ドメインを「example.net」とした場合

```
$ host -t txt abc.1234._domainkey.example.net
abc.1234._domainkey.example.net descriptive text ″v=DKIM1¥; g=*¥; k=rsa¥;
p=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx″
```

ただし、DKIM の場合は、ドメインに加えて前述のセレクタが分からなければ確認することは困難です。
また、そもそも、これらの DNS レコードは、送信者が試験として一時的に設置している可能性もあり、DNS レコードが存在しているからといって送信ドメイン認証技術に対応しているかは断定できません。したがって、以上のような確認方法は、あくまで補助的な確認方法となることに注意して下さい。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 参考5:DMARC の導入

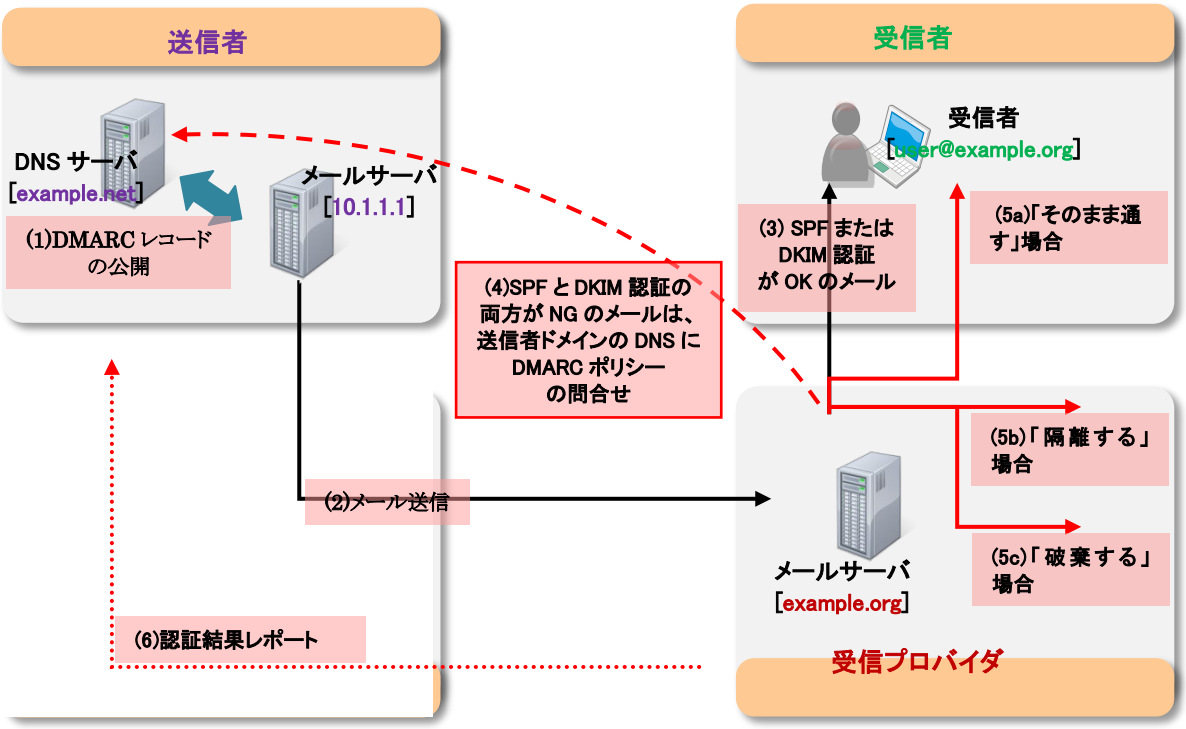
送信元を詐称した迷惑メールへの対策に有効な送信ドメイン認証技術のひとつで、SPF とDKIM の認証結果を利用して、詐称されたメールを受信側がどう扱うべきかのポリシーを、ドメインの管理者が宣言するための仕組みです。

迷惑メールの送信者(差出人)アドレスは、貴社からのメールであるかのように偽装されている場合があります。このような偽装を防ぐため、貴社ドメインで送信される迷惑メールを受信側でどのように処理するかをドメイン管理者が詳細に制御できるようにします。

送信元ドメインの管理者は、SPF と DKIM の両方の認証に失敗したメールに対して、「そのまま通す(none)」、「隔離する(quarantine)」、「受信拒否する(reject)」というように、受信時の処理方法を DMARC ポリシーとして宣言します。これにより、貴社のドメインを偽装して送られるフィッシングメールなど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。

さらに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を有しており、フィッシングメールの発生状況の把握やなりすましメールの送信元の特定などが可能になります。

### ◆DMARC のイメージ




### ◆DMARC レコードの公開

DMARC も DNS 上に TXT レコードで公開します。DMARC TXT レコードでよく使用されるタグは次のとおりです。

| タグ名 | 必須 | 目的 |
|---|---|---|
| v | 必須 | プロトコルのバージョン |
| p | 必須 | ドメインのポリシー |
| pct | オプション | フィルタ処理するメールの割合 |

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

| | | |
|---|---|---|
| rua | オプション | 集計レポートの報告先となる URL |
| ruf | オプション | フォレンジックレポートの報告先となる URL |
| ri | オプション | 集計レポートのフォーマット |
| rf | オプション | フォレンジックレポートのフォーマット |
| sp | オプション | ドメインのサブドメインポリシー |
| aspf | オプション | SPF の調整モード |
| adkim | オプション | DKIM の調整モード |

## ◆DMARC レコードの記述例

*_dmarc IN TXT "[タグ]=[値]"*
例）
_dmarc IN TXT "v=DMARC1; p=none; rua=mailto:postmaster@example.net"

## ▼DMARC レコードの確認方法の例

この例では UNIX host コマンドの TXT レコードオプションを利用していますが、同様のクエリが発行できれば問題ありません。このような操作によって有効なレスポンスがあるかどうかで、レコードの有無を確認できます。

```
$ host -t txt _dmarc.example.net
_dmarc.example.net descriptive text "v=DMARC1¥; p=none¥;
rua=mailto:postmaster@example.net"
```

## ◆DMARC のさらなる活用

DMARC 導入時は「そのまま通す（none）」のポリシーであるため、貴社からのメールであるかのように偽装されたメールも受信側でブロックすることはありません。そのため、「隔離する（quarantine）」または「受信拒否する（reject）」ポリシーに変更することで、送信元を偽装した迷惑メールのリスクを低減することにつながります。

## ◆「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

貴社が送信するメールが SPF/DKIM に対応していないと、貴社のメールもそのポリシーに従い隔離される、または受信拒否されてしまいます。以下に「受信拒否する（reject）」ポリシーに設定するまでのステップを示します。

1） **DMARC を設定する対象のドメインを差出人に使用しているメールの種類を整理する**
該当ドメインを送信元として当社サービス以外のシステムからメールを送信しているかを確認します。

2） **DMARC 検証に失敗し不達となった場合の対応方法を定める**
メーリングリストサービスのメールアドレスに送信すると、メーリングリストサービスが展開したメールは、SPF や DKIM に未対応な場合があります。そのメールは、ポリシー設定を「そのまま通す（none）」や「隔離する（quarantine）」にした場合に、実際に隔離される、または受信拒否される場合があるため、不達となった場合の対応方針を定めておきます。

3） 当社サービスから送信するメールに対して、SPF/**DKIM を導入する**
当社からのご案内に従い、SPF/DKIM を設定します。

4） **当社サービス以外から送信するメールに対して、SPF/DKIM を導入する**

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

1)で整理した情報を基に、各メールシステムの SPF/DKIM の設定状況を確認し、全てのメールに対して、SPF/DKIM を導入する。

5) SPF/DKIM 未対応のメールが無いかを確認する

rua/ruf のレポートを確認して、SPF/DKIM 未対応のメールがないかを確認します。問題ない場合は次のステップに進みます。gmail.com に定常的にメールを送信している場合は、Google Postmaster tools を利用確認することも可能です。

6) ポリシー設定を「そのまま通す（none）」から「隔離する（quarantine）」に変更する

rua/ruf のレポートを確認して、偽装の疑いのあるメールなどがないかを確認します。問題ない場合は次のステップに進みます。

7) ポリシー設定を「隔離する（quarantine）」から「受信拒否する（reject）」に変更する

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。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 参考6：主要 ISP・キャリアのメール送信者向けガイドライン等

各 ISP やキャリアが公開しているガイドラインやポリシー、案内情報です。

| ISP・キャリア | 公開情報 |
|---|---|
| Gmail | ■一括送信ガイドライン<br>https://support.google.com/mail/answer/81126?hl=ja |
| Yahoo!メール | ■迷惑メール対策<br>https://mail.yahoo.co.jp/info/guidelines/about.html<br>■Yahoo!メールヘルプ － 送信したメールが相手に届いていない<br>https://www.yahoo-help.jp/app/answers/detail/a_id/80688/p/622/related/1<br>■Yahoo!メールヘルプ － 送信したメールが Yahoo!メールの[迷惑メール]フォルダに振り分けられてしまう<br>https://www.yahoo-help.jp/app/answers/detail/a_id/80798/p/622 |
| iCloud Mail | ■Postmaster information for iCloud Mail（英語）<br>https://support.apple.com/en-us/HT204137 |
| Microsoft<br>（outlook.com、<br>hotmail.com 他） | ■迷惑メール対策<br>https://sendersupport.olc.protection.outlook.com/pm/junkemail.aspx<br>■ポリシー、プラクティス、およびガイドライン<br>https://sendersupport.olc.protection.outlook.com/pm/policies.aspx<br>■[PDF] Improving E-mail Deliverability into Windows Live Hotmai（英語）<br>https://download.microsoft.com/download/e/3/3/e3397e7c-17a6-497d-9693-78f80be272fb/enhance_deliver.pdf |
| docomo | ■同報メールを大量に送信されるお客様へ<br>https://www.nttdocomo.co.jp/service/imode_mail/notice/mass_send/<br>■送信ドメイン認証（Sender ID／SPF）について<br>https://www.nttdocomo.co.jp/service/imode_mail/notice/sender_id/ |
| au | ■EZweb へメール送信する際の注意事項<br>https://www.au.com/mobile/service/attention/<br>└メール送信時のお願い<br>https://www.au.com/mobile/service/attention/request/<br>└技術仕様・・・「EZweb のメールサーバが受信できないもの」「EZweb あてにメール送信する際の禁止行為」等<br>https://www.au.com/mobile/service/attention/specification/ |
| SoftBank | ■メールを送受信する際の注意事項<br>https://www.softbank.jp/mobile/support/mail/antispam/howto/wrestle/ |

※状況や改訂タイミングにより、本ガイドラインの推奨内容が上記情報と異なる場合があります。
※上記情報内の、当社（メール送信ツール）で実施可能なものについては、順次対応を検討しております。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 参考7:SPF チェック仕様

一部のモバイルキャリアでは、RFC(*1)と異なる SPF レコードチェックを行っています。

SPF チェック仕様の違いは下記のとおりです。

SPF チェック時は、該当の From アドレスドメインの DNS を参照し、SPF レコードを検索します。
DNS 検索回数が上限を超えると、SPF チェックがエラーになります。
その検索回数の上限が異なります。

- RFC7208(*2)
  - DNS の検索回数は、10 回まで
  - DNS 検索が必要なメカニズムや修飾子は、mx, a, include, redirect, ptr, exists
- 一部のモバイルキャリア
  - DNS の検索回数は、9 回まで
  - DNS 検索が必要なメカニズムや修飾子は、mx, a, include, redirect, ptr, exists
  -

SPF レコードを設定する際は、チェック条件が厳しい「一部のモバイルキャリア」の仕様(検索回数 9 回まで)に合わせて頂くことをお勧めいたします。

▼参考:SPF レコードの DNS 検索回数の調べ方
(例)
dmarcian SPF Surveyor (SPF 診断ツール)
https://dmarcian.com/spf-survey/

(*1) RFC(Request for Comments)は、インターネット技術の標準化などを行う IETF(Internet Engineering Task Force)が発行している、技術仕様などについての文書群。各種プロトコルの標準仕様などが記されている。

(*2) https://datatracker.ietf.org/doc/rfc7208/

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

## 参考 8:本ガイドラインの参考資料

本メール配信ガイドラインは、特電法等の法律や当社独自の知見のほか、以下の資料を参考にしています。

- 迷惑メール対策推進協議会 「迷惑メール白書」他各種資料
  https://www.dekyo.or.jp/soudan/aspc/

  「迷惑メール対策推進協議会(Anti-Spam mail Promotion Council(ASPC))」は、電気通信事業者、送信事業者、広告事業者、配信 ASP 事業者、セキュリティベンダー、各関係団体、消費者団体、学識経験者、関係省庁など迷惑メール対策に関わる関係者が幅広く集まり、効果的な迷惑メール対策推進を目的としている団体です。

- M3AAWG（マーグ） ベストプラクティス日本語版
  https://www.m3aawg.org/japanese

  「M3AAWG（マーグ:The Messaging, Malware and Mobile Anti-Abuse Working Group）」は、スパムやウイルス・ワームなどの迷惑メール対策を目的とするグローバルな業界団体です。参加する企業や組織は、スパムやフィッシングなどの防止に向けたメール認証技術について、標準仕様の策定を行っています。

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*

Copyright © 2020 Cheetah Digital Co., Ltd. All rights reserved.
*Confidential*