株式会社ディーネット
Digital-Effect Network CO.,LTD.



クラウド型　総合メールセキュリティサービス

あんしんクラウドメールフィルター　ご利用の手引き

株式会社ディーネット
大阪本社　〒541-0041
大阪市中央区北浜 2-6-11　近鉄淀屋橋ビル　5F
TEL:06-6231-8887　FAX:06-6231-8897

東京本社　〒105-0001
東京都港区虎ノ門 2-3-22　第一秋山ビル5F
TEL:03-3591-8887　FAX:03-3591-8886

第 13 版

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

内容

1 はじめに 3

1.1 本書について 3

1.2 当サービスについて 3

2 ご利用の手引き 4

2.1 サービス利用開始前の確認、ご同意事項 4

2.2 サービス利用開始までの流れ 6

2.3 メーラーにおけるスパムメールの仕分け 9

2.4 パーソナルメッセージ管理機能（PMM）オプションについて 10

2.5 転送されてきたメールのスパムチェックについて 11

2.6 スパムメールの検知の継続的な改善 11

3 FAQ 12

3.1 迷惑メールや、詐欺・なりすましメールなどは具体的に何を指すのか？ 12

3.2 正常なメールが届かない 12

3.3 件名に [SPAM?] と記載されているメールが届く 13

3.4 お客様側のメールサーバーを移設する場合 13

3.5 迷惑メールが配信されてきている 13

3.6 アクティブコンテンツを検知したメールについて 14

3.7 不正な形式のデータを検知したメールについて 14

3.8 メール本文中への注意喚起の文言の挿入について 14

3.9 一部のメールアドレスだけ利用することは可能か？ 15

3.10 レポート機能や、WEB ブラウザで利用状況を確認できるツールはあるか？ 15

3.11 メールフィルタガードマン ASP サービスからのお乗り換えのお客様へ 15

3.12 パスワード付 ZIP ファイル形式の検疫について 15

3.13 共有型レンタルサーバーご利用時のより高度なスパムメール対策について 16

3.14 Microsoft365 における受信制限回避のための設定 17

4 改訂履歴 18

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

1　はじめに

本書はあんしんクラウドメールフィルター（以下、「当サービス」と記載）をお申込みにつきまして、重要なお知らせ事項が記載されていますので、必ず最後までご覧いただきますようお願いいたします。

1.1　本書について

本書は当サービス契約約款第 4 条第 2 項にある、サービス内容の詳細を定めるものです。
対象の契約約款と併せてご確認ください。

https://cloudmailfilter.jp/
(※)上記サイト下部、「契約約款をダウンロードする」をご確認ください。

尚、本書は当社が必要と判断した場合、契約者の承諾無しに変更をすることがあります。
予めご了承ください。

1.2　当サービスについて

当社が提供する当サービスは、ウイルス（マルウェア）感染攻撃メール、詐欺・なりすましメール、標的型攻撃メール、スパムメールなどの迷惑メール対策を可能とする、総合メールセキュリティサービスです。
現在ご利用中のメールサーバーの受信経路に組み込むことで、この機能をご提供することができます。
この機能を提供する通信機器を本書では、「メールフィルターシステムサーバー」と記載します。

ドメインごとの利用体系を取り、予め定められたご利用アカウント数ごとのパック料金に応じた利用料金が設定されています。

また、機能の詳細はサービスページをご確認ください。
https://cloudmailfilter.jp/

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

2　ご利用の手引き

サービスご利用につきまして、本章の流れに沿って進めます。
前章までをご確認いただいたことを前提に記載します。

【よくあるご確認事項】

1. **お申込み、ご利用単位はドメインごと**になります(例:●●●●@example.com　等の@以下のドメイン名 1 種類につき 1 申込となります)
2. お申込みは対象のドメインで作成されているメールボックスを持つ**全てのアカウントが対象**です(例：info@example.com　アカウント 1 つのみ申し込みすることはできません)
3. 他ドメインで受信したメールを、あんしんクラウドメールフィルターに**お申込みのメールアドレスに対しての転送はスパム判定が正しくできません**ので予めご了承下さい（正しく届かない、またはスパムメールが通過するなど）

上記予めご留意の上、以下ご確認ください。

2.1　サービス利用開始前の確認、ご同意事項

当サービスをご利用開始の際には、以下についてあらかじめご了承、ご同意をいただく必要があります。

1. 当サービスは基本サービスとして、1.2 章にある迷惑メールチェック機能を持つメールフィルターシステムサーバーを経由させ(※1)、お客様メールサーバーに配送(静的配送)を行うサービスです。
2. ご利用開始にあたり、ネームサーバーの設定変更（MX レコードの変更）、及び必要に応じてお客様管理のメールサーバーの経路中にあるファイアウォールの設定変更が必要となります。(※2)
3. ご利用開始月から当月間の月額費用が発生します。
4. お申込みのアカウント数は、メールサーバーに作成されているメールボックスを持つ全てのアカウントを対象としてカウントし、指定のプランからご選択ください。
   - メールボックスを持たない転送のみをするメールアドレスが当該メール利用ドメインの主目的ではない場合、転送アドレスについては除外してよいものとします。

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

- ✧ 例：ご利用のメールアドレス数が 1000 件あるが、900 件が転送アドレスで 100 件が実際のメールユーザーの場合、あんしんクラウドメールフィルター側には 1000 アドレス分のメールが届くことになるので、アカウント数 1000 件でのお申込みを行ってください。
- ➢ Postmaster アカウントは除外とします。

5. ゼロディ攻撃など、一部の攻撃の種類によっては、メールフィルターシステムサーバーをすり抜けるものがあります。また、メールに添付されたファイルのうちパスワード保護されたファイルは解析ができません。こういった性質上、全ての迷惑メールを隔離できない場合がありますので、予めご了承ください。
6. 利用アカウント数の計上方式について。
   - ➢ 当社サーバーサービスのメールサーバーをご利用の場合(※3)、ご利用アカウント数については、当社規定の手順により翌月 1 日の時点で計上され、その利用数に応じた料金をご請求します。お申込み時のアカウント数を超過していた場合は、計上時に該当するユニット数が当月のご請求内容となりますので、あらかじめご了承の上、ご同意ください。
   - ➢ 当社管理外のメールサーバーへの配送の場合、ご利用アカウント数については、お客様からの申告されたアカウント数のご契約となります。一定期間ごとにこのアカウント数を確認いたします。

(※1) 当サービスでは送信経路に対するセキュリティ機能については提供しておりません。別途お客様専用に AWS 環境上に構築し、当サービス以上のセキュリティ機能を有したメールフィルターシステムサーバーを構築することも可能ですので、お問い合せください。

(※2) メールフィルターシステムサーバーからのメール転送(静的配送)をファイアウォールで許可する必要があります。

(※3) extremeserv.、Palette UP、CloudServ.、クラウド運用支援サービス(クラウド保守運用サービス)等が該当。

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

2.2　サービス利用開始までの流れ

下記について、当社サーバーサービスをご利用されていないメールサーバー（当社が管理してしないメールサーバー）については、お客様にて導入までの必要な対応を行っていただく必要がございます。
ご不明な点は、当社までお問い合せください。

2.2.1 お申込書のご提出

別途ご提示する、お申込書に必要事項をご記入の上、お申込みください。

このお申込書にて、お客様メールサーバーでご利用のメールアカウント数をご申告ください。
この申告数に応じたユニット数が月ごとのご利用料金となります。
メールサーバーに作成されているメールボックスを持つ全てのアカウントが、アカウント数の対象となります。
（postmaster アカウントは除外可能です）
(※)当社のメールサーバーサービスをご利用の場合は、当社にてアカウント数を計上いたしますので、対応は不要です。

また、当サービスのメールフィルターシステムサーバーからの転送先となる、現在ご利用中のメールサーバー（メールボックスの存在するメールサーバー）の情報をご提示ください。
このメールサーバーの**名前解決ができるホスト名**、または **IP アドレス**をご提示いただきます。
詳細は 2.2.4 をご確認ください。

2.2.2 サポート窓口の開設

各種ご契約に関する事項や、「メールが届かない」、「迷惑メール等が配送されてきたのでブロックして欲しい」など、各種お困りごとのお問い合せをうけたまわる、サポート窓口をご用意しております。

■ **当社が運用保守を行うメールサーバーについて**
対象のメールサーバーに紐付く『運用アドミニストレータ』登録に準じてサービスを提供いたします。
ただし、通常のサポート依頼につきましては、当社営業時間中となりますので、ご了承ください。

■ **お客様管理のメールサーバーについて**
以下の問い合せ窓口までお問い合せください。

【お問い合せ窓口】

種別	受付時間	連絡先
電話	当社営業時間	0120-3889-80
メール	当社営業時間	desk@denet.co.jp

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

2.2.3 お客様メールサーバーへの設定

外部からメールを受信するための設定について、ファイアウォールの設定で特定のホストからのみメール配送を許可している場合は、ファイアウォールの設定において、メールフィルターシステムサーバーからのメール配送を許可してください。下記ホストからの TCP ポート 25 番での通信の開放が必要です。

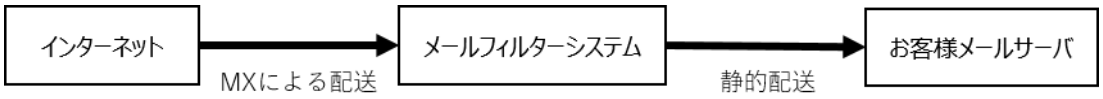
- **メールフィルターシステムサーバー　FQDN [IP アドレス]**
  - **acmf03.sendmail.ne.jp [13.231.98.150]**
  - **acmf04.sendmail.ne.jp [13.192.8.154]**

上記サーバーからの配送されてくるメールに対する迷惑メール対策（SPF、DKIM、DMARC 認証等によるブロック、また IP ブラックリストホスト等の判定によるブロック）は実施しないでください。
メールの受信に失敗する場合があります。

2.2.4 お客様メールサーバーのホスト名、または IP アドレスのご提示

メールフィルターシステムサーバーから、お客様のメールサーバーにメールを転送させる必要があるため、お客様メールサーバーの名前解決ができるホスト名、または IP アドレスを当社までご提示ください。
お客様側でメールサーバーのホスト名、または IP アドレスが変更された場合は、配送出来なくなりますので、ご注意ください。
尚、この場合のお客様のメールサーバーまでの受信経路については、以下の通りです。

また、メールフィルターシステムサーバーと、お客様メールサーバー間に、迷惑メール処理機能を持つサーバーを経由する場合は誤判定される場合がありますので、お客様メールサーバー側での迷惑メール処理機能は除外していただくことが推奨となります。



2.2.5 当社側の設定完了のお知らせ

ここまでで事前の準備として、メールフィルターシステムサーバーご利用開始の準備が整いました。
当社から、次項の DNS 設定変更のご依頼がございましたら、DNS 設定変更作業を実施していただきますよう、よろしくお願いいたします。

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

2.2.6 該当ドメインのネームサーバーの設定

(※)本設定を実行した時点から、メールの配送経路が切り替わりますので、ご注意ください！

(※)DNS 設定作業の際は、必ず次項もご確認ください！

以下のドメイン名(FQDN)を該当ドメインの MX レコードにご指定ください。

それぞれ任意の優先度値（preference）を設定ください。

acmf03.sendmail.ne.jp
acmf04.sendmail.ne.jp

以下、お名前.com での設定例です。ご利用ドメイン名が『acmf.work』の場合を想定しています。

● 追加

A/AAAA/CNAME/MX/NS/TXTレコード

※オリジンのNSレコードは変更できません。
※オリジンのNSレコード機能で設定されたA/AAAAレコードは変更できません。

ホスト名	TYPE	TTL	VALUE	優先	状態	削除
acmf.work	MX	3600	acmf03.sendmail.ne.jp	10	有効	
acmf.work	MX	3600	acmf04.sendmail.ne.jp	20	有効	

この設定により、メールフィルターシステムサーバーにて、メールの検疫が始まります。尚、AI による検疫の学習の観点から、始めの 1 週間ほどはスパムメールがすり抜ける場合がございますので、予めご了承ください。

もしも、この設定後、メールが届かない等の問題が発生した場合は、当社までお問い合せください。

【注意！】

ご利用中メール環境から、あんしんクラウドメールフィルターを導入される場合、また、現在何らかの迷惑メール対策コンポーネントをご利用されている場合、既に MX レコードが存在していると思います。

この MX レコードの設定を残存させつつ、上記の MX レコードを追加されても、あんしんクラウドメールフィルターをご利用は開始できますが、残存した MX レコードにもメールが配送されることになり、そこから迷惑メールが流入しますので、現行の MX レコードにつきましては削除し、上記で指定した MX レコードのみを設定することを推奨しております。

これについて、設定の不明点がある場合は、当社カスタマーサポートまでお問い合せください。

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

2.2.7 SPF レコードの設定変更

前項で MX レコードを切替えた際に、以下のように DNS 設定における、SPF(送信ドメイン認証)の TXT レコード設定の箇所が『v=spf1 +mx ~all』となっている場合、お客様から送信したメールに SPF 認証でエラー(SPF soft Fail)が発生します。
これを回避するために、対象ドメインの DNS の TXT レコードの変更について、下記を参考に実施してください。

【SPF 認証エラーが発生する設定の例】
以下、お名前.com での設定例です。ご利用ドメイン名が『acmf.work』の場合を想定しています。

ホスト名	TYPE	TTL	VALUE	優先	状態	削除
acmf.work	TXT	3600	v=spf1 +mx ~all		有効	

(※)Value(値)の箇所が『+mx』のみですと、MX 対象がメールフィルターシステムサーバーに変更されたことで、送信メールについて SPF 認証エラーが発生します。
(※)はじめから下図のようになっている場合は、本項は設定不要です。

【SPF 認証エラーを回避する設定の例】

ホスト名	TYPE	TTL	VALUE	優先	状態	削除
acmf.work	TXT	3600	v=spf1 +mx +a:mail.acmf.work ~all		有効	

赤枠で囲った箇所のように、メール送信に利用しているメールサーバーの値を追加します。
『mail.acmf.work』の箇所を、ご利用中のメールサーバーのホスト名(FQDN)を入れてください。
メーラーの送信(SMTP)サーバー設定にあるホスト名を入れることが推奨です。
(※)レンタルサーバーの場合は、概ね『smtp.example.com』や『mail.example.com』になっています。詳細はご利用中のメールサーバーサービスをご確認ください。

2.3　メーラーにおけるスパムメールの仕分け

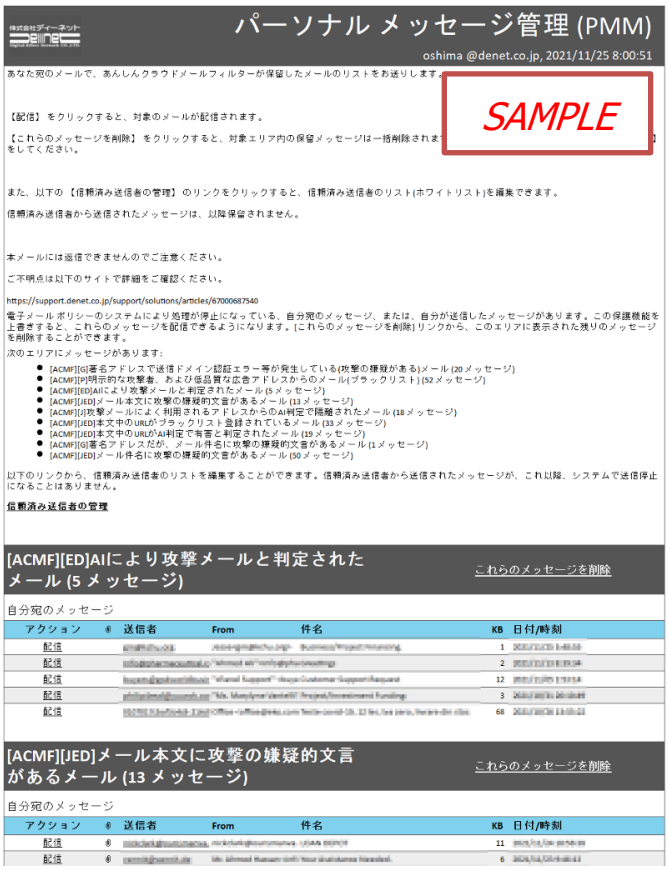
メールフィルターシステムサーバーでは、明らかな迷惑メール、スパムメールは事前に検疫し隔離されます。
これに加えて、『疑わしい』メールにつきましては隔離せずに、該当のメールの件名の文頭に［SPAM?］の文言を付記して配送します。
この［SPAM?］の文言を付記したメールにつきましては誤操作を防ぐためにも、お客様自身にてご利用のメーラーソフトのメッセージの振り分け機能を利用して、仕分けを行うことをおすすめいたします。

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

2.4　パーソナルメッセージ管理機能（PMM）オプションについて

メールフィルターシステムサーバーでは、明らかな迷惑メール、スパムメールは、検疫され隔離されます。(※1)

この検疫、隔離されたメールの宛先に右記の通知メールを配信し、受信者側でこの隔離されたメールを隔離エリアから配信、または削除を実行することができるオプションがパーソナルメッセージ管理機能(PMM)オプションです。
このオプションは無料でご利用いただけます。



メールフィルターシステムサーバーでは、誤検知され隔離されるメールがまれにあります。2.2.2 章にあるサポート窓口へのお問い合せいただけますと、誤検知であった場合は、可能な限り即座に配信処理をさせていただくことが可能ですが、PMM オプションをご利用いただくことで、この誤検知を含めて隔離したメールを、受信者自身で確認し、配信を実行することが可能になります。

PMM オプションでは、検疫されるメールが発生した場合、そのメールの宛先となるメールアカウントに対して、右図の通知メールが配信され、その通知メールに記載されたリンクから、配信、削除が出来ます。
ただし、このオプションのご利用には以下の制約がございますので、予めご了承の上ご利用ください。

【PMM オプションに関する前提事項】

1. PMM にお申込みの場合は、対象の全ユーザー宛のメールが対象となります。
2. 隔離されたメールが無い場合は、PMM のメールは配信されません。また、毎時 0 分にまとめて配信されます。
3. PMM はメール宛先となる各ユーザー様にのみ配信され、お客様側の管理者等に集約してお送りすることなどは出来ません。
4. PMM は、送信者(実際のメール送受信に利用される、所謂 Envelope-From アドレス)、From アドレス(メーラー上に表示される差出人のいわゆる Header-From アドレス)、件名、日時が確認出来ます。但し、システムの仕様上、From アドレスと、件名が全て表示されず、見切れる場合がございますので、予めご了承ください。
5. 迷惑メールとして検疫された実際に有害なメールが「配信」をクリックすると配信されますので、ご利用時はご注意の上ご利用ください。

PMM の詳細は下記の参考サイトをご覧ください。
【あんしんクラウドメールフィルターのパーソナルメッセージ管理メール（PMM）について】
https://support.denet.co.jp/support/solutions/articles/67000687540

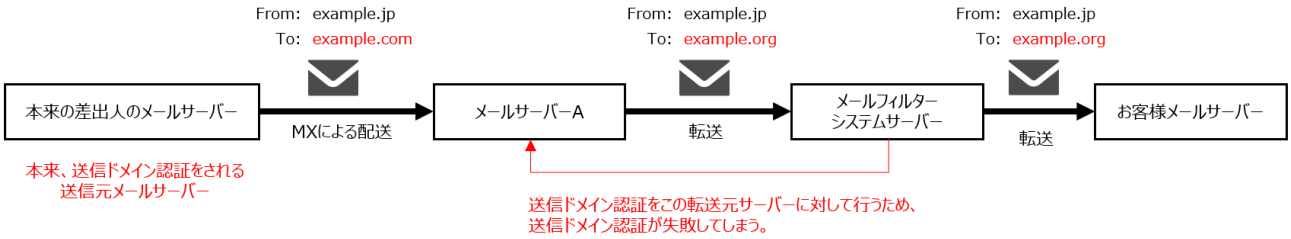
(※1)PMM は 2.3 章にある「疑わしいメール」は PMM 機能の有無に関係なく、メールの件名に[SPAM?]が付記され配信されます。

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

2.5　転送されてきたメールのスパムチェックについて

あんしんクラウドメールフィルターご利用外のメールアドレス宛のメールに対して、あんしんクラウドメールフィルターをご利用のアドレスへのメール転送（メールの再配送）は、送信ドメイン認証の失敗を引き起こし、正常にメールが届かない可能性がありますので、他ドメイン宛のメールをあんしんクラウドメールフィルターお申込みドメインに対する転送設定は原則禁止しております。

■転送メールが検疫の失敗を起こすメカニズム



通常、上図でいうメールサーバーA は、From アドレス（厳密には Envelope-From アドレス）をメールサーバーA 自身のものに書換えて転送を行いますが、一部のプロバイダー（当社では ODN 様のもので観測しております）では、From アドレスを書換えずに転送を行っておりますので、一部のメールでは正常にメールが届きません。
これを緩和するとスパムメールの流入を招きますので、当社側ではこのメール受信に対する対処は行いません。

2.6　スパムメールの検知の継続的な改善

メールフィルターシステムサーバーでは、AI や、複数の検知手法により、スパムメールの検知を行いますが、まれに検知をすり抜けるメールがございます。
これらのメールについて、正常に検知、処理するために、該当のメールを当社まで検体としてご提供いただけましたら、当社が明らかにスパムメールと判定したメールについては、メールフィルターシステムサーバーで判定するように、設定調整を行います。
但し、対象のメールによっては、判定ができないメールもございますので、あらかじめご了承ください。

また、スパムメールの誤検知と推測されるメールにつきましては、サポート窓口までご相談ください。

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

3 FAQ

3.1 迷惑メールや、詐欺・なりすましメールなどは具体的に何を指すのか？

当サービスにおいては、下記の文言に対する効果を提供しています。
それぞれの言葉の定義としては以下の通りです。
但し、この文言の定義につきましては、時期、時流により揺らぎがあるものであり、その内容を完全に補えるものでは無いことを予めご了承ください。

名称	定義
迷惑メール	次行以降のメール全般に対する総称として用いる。
ウイルス（マルウェア）感染攻撃メール	メールの添付ファイルにウイルス（マルウェア）を添付し、当該メール受信者に対して、その感染攻撃を仕掛けることを目的としたメール。 また、マルウェアとは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称です。ウイルスもマルウェアに含みます。（一部 JISA より引用）
詐欺・なりすましメール	ショッピングサイトや金融機関、各種 IT サービス等の利用者のアカウントや、クレジットカード情報、個人情報の搾取を目的としたメールで、メール文面中に攻撃の内容が記されているメールを指す。
標的型攻撃メール	メール受信者がそのメールを閲覧した際に、取引先や知り合いと認識させ、悪意有る添付ファイルや URL を送り付け、その端末を感染させることを目的としたメールを指します。
スパムメール	大量に同様の配信を行っているメールで、ほとんどのメール受信者が望まない、不快感を示すメールの総称。主には、大量に同様の配信を行っているバルクメール、ほとんどの人が望まないメール、ほとんどの人が不快感を表すメール、スパム判定チェックを回避する書き換えを行った攻撃メールなどがあります。

3.2 正常なメールが届かない

E メールの送受信のやりとりにおいては、送信元ドメインの DNS、メールサーバーの設定等、セキュリティ設定が正しく行われている必要があります。
この送信元ドメインの設定不備により、メールフィルターシステムサーバーで誤判定により、隔離される場合があります。

このような事象が発生した場合には、当社までお問い合せください。
対象のメールにウイルス（マルウェア）感染の問題が無いことが確認できましたら、そのメールの隔離を解除し、配送させていただきます。

お問い合せの際には、メールの送信日時と送信元アドレス、送信先アドレスをお伺いします。

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

3.3　件名に [SPAM?] と記載されているメールが届く

当サービスでは、スコア化された厳密なルールセットを適用していますが、当社側では関与できない送信元側の設定不備により、当該サービスでは検疫時に隔離される場合があります。
また、AI によるスパム判定を行っているため、お客様にとって正常なメールの件名に [SPAM?] と付記される場合があります。

このような場合は、当社までお問い合せください。
ルールセットのチューニングを行い、より正確な検知を行うようにいたします。

お問い合せの際には、検体メールか、メールの送信日時と送信元アドレス、送信先アドレスをお伺いします。

3.4　お客様側のメールサーバーを移設する場合

お客様メールサーバーが IP アドレスの変更を伴う移設をする場合は、メールフィルターシステムサーバーからの転送先を変更する必要がありますので、予めご連絡ください。
導入時にお客様のメールサーバーをホスト名（FQDN）でお申込みいただいた場合は、適切にお客様側で DNS 設定の更新をした場合は、メールフィルターサーバーの設定を変更する必要は有りません。

3.5　迷惑メールが配信されてきている

迷惑メールの定義としましては、詐欺・なりすましを目的としたメール、および AI によって判定されたスパムメールが該当します。
(※)スパムメールの検疫の内容は WEB サイトをご確認ください。

マーケティングオートメーション（MA）サービスを利用して配信されてきているメールなどの、通常の広告メールについて、適切なルールで配信されてきているメールにつきましては、各事業者が適切な手法で取得したメールアドレスに対して配送されてきていることを前提としているため、受信されたお客様は、ご自身でメール中にある「配信解除」等から配信を停止（オプトアウト）してください。

但し、配信を停止しない広告、公序良俗に反する広告につきましては、当社までお問い合せください。
当サービスの監査チームにて内容を監査し、内容によってはルールセットに組み込み、検疫を強化するチューニングを施します。
お問い合せの際には、検体メールか、メールの送信日時と送信元アドレス、送信先アドレスをお伺いします。

また、共有タイプのレンタルサーバーをご利用の場合、メールフィルターシステムサーバーを介さず、直接お客様のメールサーバーにスパムメールが配送され、スパムメールが届くことがあります。
より、セキュリティレベルの高い環境で当サービスをご利用されるために、3.13 節にチュートリアルをご用意しましたので、合わせてご確認ください。

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

3.6　アクティブコンテンツを検知したメールについて

メールの件名に［SPAM?］に加えて、件名の後尾に**［マクロ等の実行可能なコードを検出しました。お取扱いにご注意ください］**と記載されたメールが配送される場合があります。

これは、添付ファイル内に、スクリプトやマクロを含んだメールが該当します。
そのファイル内にマクロオブジェクトを含むものは全て検知しますので、例えばマクロを含んでいないように見える EXCEL ファイル(拡張子が.xlsx のもの)も検知する場合があります。

3.7　不正な形式のデータを検知したメールについて

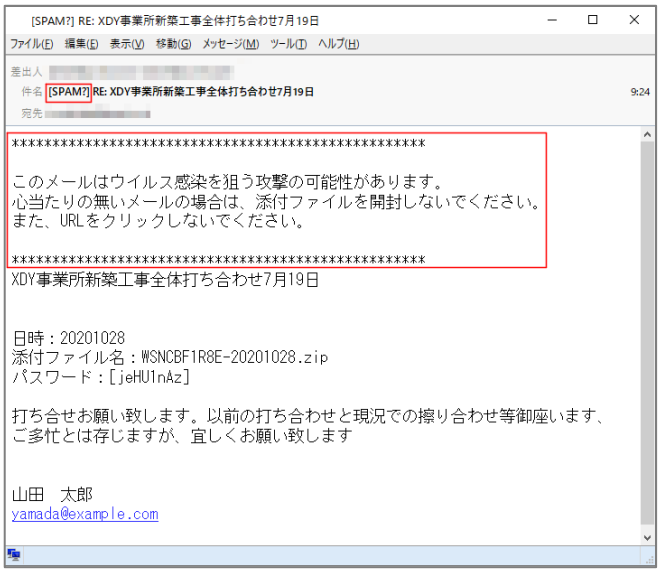
メールの件名に［SPAM?］に加えて、件名の後尾に［添付ファイル内に不正なデータを検出しました。お取扱いにご注意ください］と記載されたメールが配送される場合があります。

これはあんしんクラウドメールフィルターで、正しく読むことが出来なかった、また処理することが出来なかったファイルです。このようなデータは、脅威を隠すために意図的に破損させている場合や、外部プロセスの影響を受けている場合があります。
結果として、ウイルスチェック等の検疫ができていないファイルが送付されてきていることになりますので、信頼できない差出人からのメールである場合は、ファイルを開かないようにご注意ください。

3.8　メール本文中への注意喚起の文言の挿入について

Emotet(エモテット)対策のひとつとして、パスワード保護された添付ファイルを開かせようとするメールに対する攻撃に対して、下図のとおり、件名に［SPAM?］が追加され、さらにメール本文のはじまりに、注意喚起の文言を挿入しているメールが届く場合がありますので、正規のメールかどうかを十分ご確認の上、お取り扱いください。

■注意喚起の文言に関するサンプルメール



(※)上図の赤枠内がメールフィルターシステムサーバーで追加された文言。

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

3.9　一部のメールアドレスだけ利用することは可能か？

いいえできません。

お申込みはドメイン単位となります。

abc@example.com、def@example.com・・・というメールをご利用の場合は、ドメイン名は「example.com」になりますが、この「example.com」全体で利用している全てのメールアドレスが対象となります。

これは異なるドメイン間の E メール配送の仕組みでは、メールアドレス単位の配送の設定がそもそも出来ないためです。

3.10　レポート機能や、WEB ブラウザで利用状況を確認できるツールはあるか？

いいえありません。

当サービスは低価格でご提供するために、全て自動運用にしており、それらの機能をお客様にご提供しておりません。

但し、当サービスの基盤である、Secure Email Gateway をお客様専用環境として AWS 上に構築し、ご提供することが可能です。詳細は当サービスページをご確認ください。

3.11　メールフィルタガードマン ASP サービスからのお乗り換えのお客様へ

当社の別サービスである、メールフィルタガードマン ASP サービスにおいては、ご要望をいただいた一部のお客様に対して、メール送信時のウイルスチェック等の機能をご提供していますが、当サービスにおいては、メール送信経路におけるウイルスチェック機能はご提供しておりません。

お乗り換えの際には、ご注意ください。

3.12　パスワード付 ZIP ファイル形式の検疫について

当サービスのウイルスチェックエンジンは Sophos（アメリカ合衆国製）を採用しておりますが、このウイルスチェックエンジンでは、「パスワード付 ZIP ファイル形式」の検疫は行いません。

尚、インターネット上で利用されている、多くのウイルスチェックエンジンではパスワード付 ZIP ファイル形式のウイルスチェックはできません（アプライアンス上で展開用パスワードを指定して解析するツールは存在します。パスワード付 ZIP ファイル形式のままでウイルスチェックができる製品がございましたら、当方までご一報ください）。

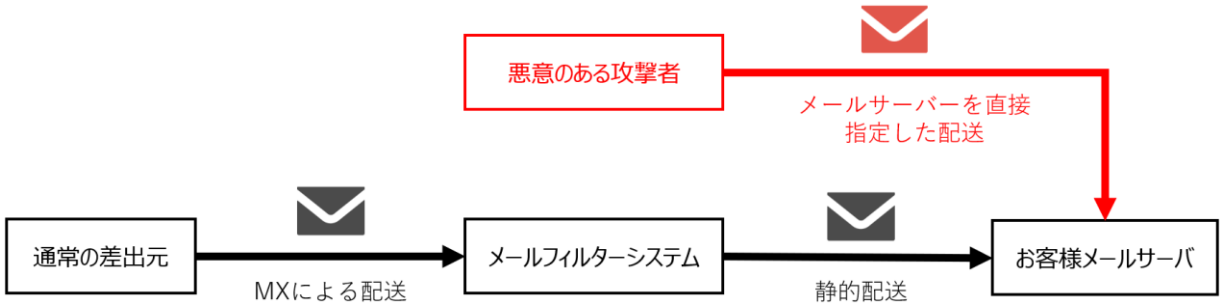
よって、Emotet を初めとする、パスワード付 ZIP ファイルについては、クライアント PC 上でそのファイルを展開し、ウイルスチェックソフトウェアで解析をしてお確かめください。

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

3.13　共有型レンタルサーバーご利用時のより高度なスパムメール対策について

当サービスをご利用いただいている場合、配送されてくるメールは、通常、DNS の MX レコードの設定（2.2.6 章参照）に従って配送され、貴社メールサーバーに配送される前にメールの検疫が行われます。
共有型のレンタルサーバーをご利用されている場合、下図のようにお客様のメールサーバーに対して、直接スパムメールを送りつける攻撃を受ける場合があります。

■お客様メールサーバーに直接スパムメールを配送させるメカニズム



これは**お客様のメールサーバーのファイアウォールが解放されているため、攻撃者が直接お客様メールサーバーのホスト名を類推して、メールを送り付けてくる**ことで発生します。
共有型レンタルサーバーの場合、メールセキュリティ対策に限度があり、特定のホストからのメールのみ受けつけるファイアウォール設定ができないことが多々あります。
これを悪用して、当サービスのメールフィルターシステムサーバーを介さずに直接お客様のメールサーバーに対して、直接スパムメールを送り付ける攻撃が、昨今増加しています。
このような攻撃を防ぐためには、以下の対策が取れます。より高度なメールセキュリティ対策の参考としてください。

【より高度なメールセキュリティ対策】

1. ファイアウォール機能を有する、専用型メールサーバーサービスに切替える。
2. 現在のレンタルサーバーにおいて、ファイアウォール機能を提供するサービスがある場合は、メールの配送元を当サービスからの接続に限定する設定をする(2.2.3 章　参照)。
3. レンタルサーバーサービスの DNS レコードの設定変更が可能であれば、これを見直す。

1 について、専有型メールサーバーは当社でもご提供可能です。
3 について、お客様のメールサーバーのホスト名（FQDN 名）が**類推しやすい名前**になっていることにより攻撃を受けている場合があります。これを類推されにくいホスト名にすることで、攻撃を受けにくくする効果があります。
例えばご利用ドメイン名が example.com の場合、多くのメールサーバーのホスト名（FQDN 名）は、標準的な設定として『mail.example.com』『smtp.example.com』『pop.example.com』『imap.example.com』とされている場合が多く、この名前を類推して攻撃者は攻撃を仕掛けてきます。
上記赤字部分を類推しにくい任意の名前に変更することが対策となります。
この場合、PC でご利用のメーラーのメールサーバー設定も併せて変更する必要があります。ご注意ください。

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

3.14 Microsoft365 における受信制限回避のための設定

Microsoft365 の Exchange では、標準で受信の制限（メールの受信遅延）機能が働いております。
当サービスは、当サービスシステム（インターネット上の複数のメール転送サーバー）から、Microsoft365 の Exchange に対してメールを転送する仕組みとなっており、この影響を受けます。

受信制限を招くエラーコード例（メールは再送されます。失われることはありません）

- said: 451 4.7.500 Server busy. Please try again later from
- said: 452 4.5.3 Too many recipients (AS780090)

このような事象の発生を避けるため、Microsoft365 の Exchange をご利用のお客様は予めお客様側で以下の Microsoft365 の設定を実施ください。

1. メール通数に対する受信の制限の回避設定

Microsoft365 側では 1 時間当たりのメッセージ数の制限が掛けられています。

https://docs.microsoft.com/ja-jp/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#receiving-and-sending-limits

これを回避するために、以下を参考に受信コネクタの設定を行ってください。

https://learn.microsoft.com/ja-jp/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/set-up-connectors-for-secure-mail-flow-with-a-partner#set-up-a-connector-to-apply-security-restrictions-to-mail-sent-from-your-partner-organization-to-microsoft-365-or-office-365

(※) Microsoft 365 へログイン→管理センター→Exchange→コネクタからコネクタを追加→接続元に「パートナー組織」、接続先に「Office365」→命名は任意→「送信側サーバーの IP アドレスが、パートナー組織に属する次のいずれかの IP アドレスと一致することを確認する」で IP アドレスを設定→「TLS を使って送信されていないメール メッセージを拒否する」を選択肢、設定を保存する。

受信元の IP アドレス帯については、以下を設定してください。

- 13.231.98.150/32
- 13.192.8.154/32

2. スパムメール対策としての受信制限

メール通数により、あんしんクラウドメールフィルター側のサーバーがスパムメールの送信ホストと認識されます。
これを回避するため、以下の『スパム信頼レベル (SCL)』設定を行ってください。

https://learn.microsoft.com/ja-jp/microsoft-365/security/office-365-security/anti-spam-spam-confidence-level-scl-about?view=o365-worldwide

https://learn.microsoft.com/ja-jp/exchange/security-and-compliance/mail-flow-rules/use-rules-to-set-scl

(※)当社技術ブログの参考サイト

https://blog.denet.co.jp/acmf-ms365/

IP アドレスの範囲は前項の「受信元の IP アドレス帯」を参照ください。

尚、The Junk Mail Reporting Program (JMRP)への登録は予め当社側で行っておりますので対応は不要です。

https://sendersupport.olc.protection.outlook.com/snds/JMRP.aspx

Copyright © Digital-Effect Network CO.,LTD. All right reserved.

4 改訂履歴

発行	改訂日	改訂項目	改訂内容
第 1 版	2018 年 06 月 01 日	―	新規作成
第 2 版	2020 年 11 月 01 日	―	全体構成の更新
第 3 版	2021 年 09 月 29 日	2.2.6	注意喚起を目的とした、但し書きを追加。
第 4 版	2021 年 12 月 01 日	2.2.2	お問い合せ先電話番号をフリーダイアルに変更
		2.4	パーソナルメッセージ管理機能オプションの新規追加
第 5 版	2022 年 07 月 01 日	2.5	左記の各項目を新規追加
		3.7	
		3.12	
第 6 版	2023 年 02 月 16 日	3.13	左記の項目を新規追加
第 7 版	2023 年 02 月 28 日	2.2.7	左記の項目を新規追加
第 8 版	2023 年 07 月 12 日	3.14	左記の項目を新規追加
第 9 版	2024 年 02 月 21 日	2.2.3	注意喚起等の記載を追加。
第 10 版	2024 年 09 月 13 日	1.1	サイト URL の更新
		1.2	サイト URL の更新
		2.1	加筆
		2.5	加筆
第 11 版	2026 年 02 月 01 日	表紙	大阪本社ビル名変更による更新
		2	【よくあるご確認事項】の新規追加
		2.1	注釈を一部更新
第 12 版	2026 年 08 月 13 日	2.2.3	メールフィルターシステムサーバーIP 変更に伴う更新
		3.14	
第 13 版	2026 年 09 月 30 日	1.2	サービス提供プラン改定に伴う文言の調整。
		2.1	

Copyright © Digital-Effect Network CO.,LTD. All right reserved.