



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 北浜エクセルビル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3版

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	5
2.2.1	お申込書のご提出	5
2.2.2	サポート窓口の開設	5
2.2.3	お客様メールサーバーへの設定(必要時)	6
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	6
2.2.5	当社側の設定完了のお知らせ	6
2.2.6	該当ドメインのネームサーバーの設定.....	7
2.3	メーラーにおけるスパムメールの仕分け.....	8
2.4	スパムメールの検知の継続的な改善	8
3	FAQ.....	9
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?	9
3.2	正常なメールが届かない	9
3.3	件名に [SPAM?] と記載されているメールが届く.....	10
3.4	お客様側のメールサーバーを移設する場合	10
3.5	迷惑メールが配信されてきている	10
3.6	アクティブコンテンツを検知したメールについて.....	11
3.7	メール本文中への注意喚起の文言の挿入について.....	11
3.8	一部のメールアドレスだけ利用することは可能か?	12
3.9	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?	12
3.10	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.....	12
4	改訂履歴.....	13

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://www.denet.co.jp/pdf/yakkan/acmf_kiyaku.pdf

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、お客様のご利用アカウント数、または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://www.denet.co.jp/service/>

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。

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、指定のプランからご選択ください。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対象となります。
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形状方式について。
 - 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いません。別途お客様専用で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、お問い合わせください。

(※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.、CloudServ.、VPmanageServ.、セキュアマネージメントサーバー、クラウド運用支援等が該当。

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、当社までお問い合わせください。

2.2.1 お申込書のご提出

別途ご提示する、お申込書に必要な事項をご記入の上、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

■ 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

以下の問い合わせ窓口までお問い合わせください。

【お問い合わせ窓口】

種別	受付時間	連絡先
電話	当社営業時間	06-6231-8887
メール	当社営業時間	desk@denet.co.jp

2.2.3 お客様メールサーバーへの設定(必要時)

通常は行う必要が無い設定ですが、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
 - **acmf03.sendmail.ne.jp**
 - **acmf04.sendmail.ne.jp**

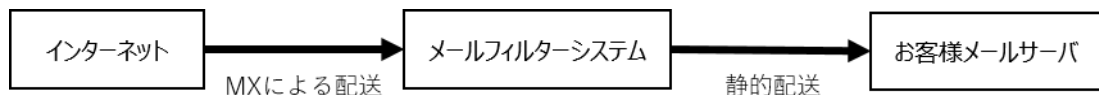
2.2.4 お客様メールサーバーのホスト名、または IP アドレスのご提示

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、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。

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！

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 ▼	<input type="checkbox"/>
acmf.work	MX	3600	acmf04.sendmail.ne.jp	20	有効 ▼	<input type="checkbox"/>

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。

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、当社までお問い合わせください。

【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 レコードを追加しても、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わせください。

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削除せずに、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。

2.4 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。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。

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？

本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な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、その艦船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。

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、当社までお問い合わせください。

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。

お問い合わせの際には、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。

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、当社までお問い合わせください。

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。

お問い合わせの際には、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。

但し、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、当社までお問い合わせください。

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。

お問い合わせの際には、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。

3.6 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。

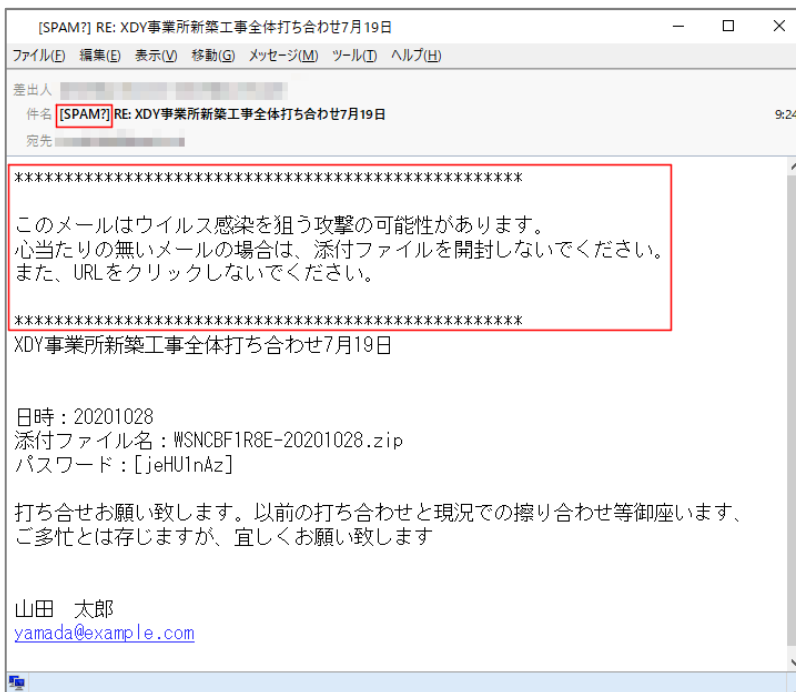
これは、添付ファイル内に、スクリプトやマクロを含んだメールが該当します。

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 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。

3.8 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。

3.9 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。

3.10 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。

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。