クラウド型 総合メールセキュリティサービス

FNP-WEB オプションサービス
クラウドスパムチェックサービス ご利用の手引き

株式会社 グローバル・パートナーズ・テクノロジー
FNP-WEB 事務局
TEL/FAX：06-6231-8882
E-Mail：info@fnp-web.jp
https://fnp-web.com
（営業日：平日月～金曜日の 9：00～18：00）

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

2.3 メーラーにおけるスパムメールの仕分け 6

2.4 転送されてきたメールのスパムチェックについて 6

2.5 スパムメールの検知の継続的な改善 6

3 FAQ 7

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？ 7

3.2 正常なメールが届かない 7

3.3 件名に [SPAM?] と記載されているメールが届く 8

3.4 迷惑メールが配信されてきている 8

3.5 アクティブコンテンツを検知したメールについて 9

3.6 不正な形式のデータを検知したメールについて 9

3.7 メール本文中への注意喚起の文言の挿入について 9

3.8 一部のメールアドレスだけ利用することは可能か？ 10

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？ 10

3.10 パスワード付 ZIP ファイル形式の検疫について 10

4 改訂履歴 12

1 はじめに

本書はクラウドスパムチェックサービス（以下、「当サービス」と記載）のお申込みにつきまして、重要なお知らせ事項を記載しておりますので、必ず最後までご確認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。

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. ご利用開始月から当月間の月額費用が発生します。
3. 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。
   - 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。
     ① 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、クラウドスパムチェックサービス側には 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。
4. 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。
5. 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(※2)、ご利用アカウント数については、当社規定の手順により毎月 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、予めご了承の上、ご同意ください。

(※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。

(※2) FNP-WEB が対象となります。

2.2 サービス利用開始までの流れ

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。

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。

2.2.2 当社側の設定

お申込書を受領後、約 3 営業日でサーバー側の設定をさせていただきます。
設定完了後、ご担当者様宛にメールでご報告させていただきます。
(※)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！

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。
万が一、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。

2.2.3 サポートについて

お問い合せ窓口、営業時間は下記の通りです。
営業時間外にメールでお問い合せいただきました場合は翌営業日に回答させていただきます。

【お問い合せ窓口】

種別	受付時間	連絡先
電話	当社営業時間	06-6231-8882
メール	当社営業時間	info@fnp-web.jp

【営業時間】
土日祝日を除く平日 9:00～18:00

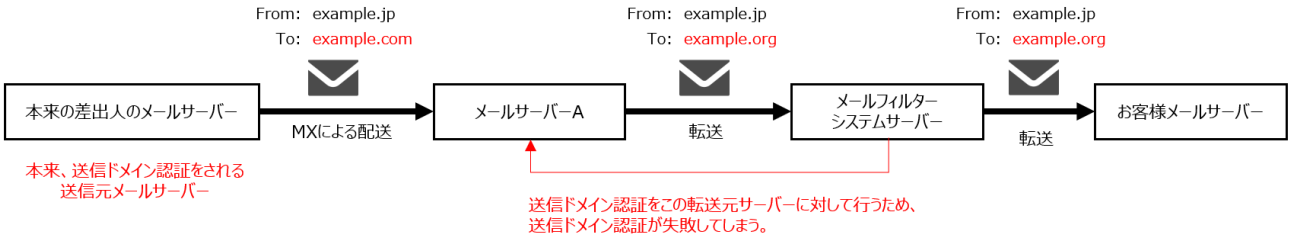
2.3 メーラーにおけるスパムメールの仕分け

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。

2.4 転送されてきたメールのスパムチェックについて

クラウドスパムチェックサービスご利用外のメールアドレス宛のメールに対して、クラウドスパムチェックサービス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クラウドスパムチェックサービス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。

2.5 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。

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され、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。

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 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。

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。

3.5 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。

3.6 不正な形式のデータを検知したメールについて

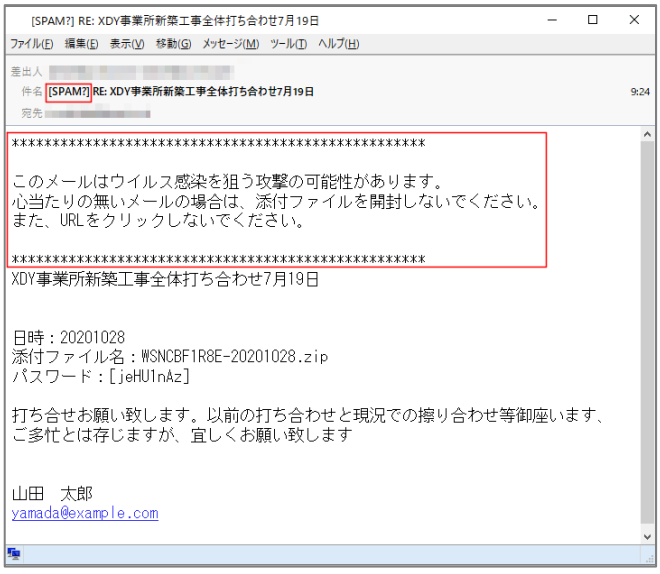
メールの件名に［SPAM?］に加えて、件名の後尾に［添付ファイル内に不正なデータを検出しました。お取扱いにご注意ください］と記載されたメールが配送される場合があります。

これはクラウドスパムチェックサービスで、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。

3.7 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。

3.10 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。

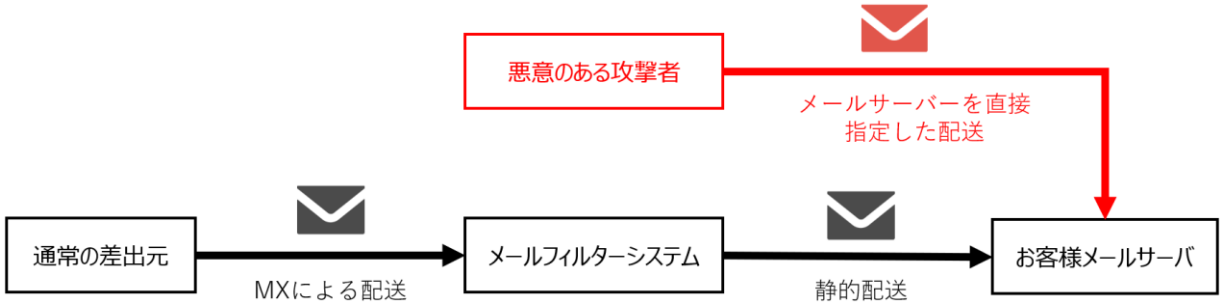
尚、インターネット上で利用されている、多くのウイルスチェックエンジンではパスワード付 ZIP ファイル形式のウイルスチェックはできません（アプライアンス上で展開用パスワードを指定して解析するツールは存在します。パスワード付 ZIP ファイル形式のままでウイルスチェックができる製品がございましたら、当方までご一報ください）。

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。

3.11 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（2.2.5 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。

4 改訂履歴

発行	改訂日	改訂項目	改訂内容
第 1 版	2022 年 06 月 30 日	ー	新規作成
第 2 版	2023 年 02 月 28 日	3.11	左記の項目を新規追加
第 3 版	2024 年 09 年 19 日	2.1	加筆
		2.4	加筆