

bit-drive 設定マニュアル
メールチェックゲートウェイ
DNS サーバ設定マニュアル

2011 年 6 月 15 日 Version 1.1

bit-drive

目次

1 本マニュアルについて	3
2 設定	3
2-1 利用サーバについて.....	3
2-2 MXレコード設定.....	4
2-3 SPFレコード設定	5

1 本マニュアルについて

本マニュアルは、メールチェックゲートウェイサービスをご利用いただくために最低限必要なお客さま DNS サーバの設定手順について記載しています。

サービスを利用開始するにあたり、お客さまドメインの MX レコードに弊社メールチェックゲートウェイサーバをご指定いただくことで、お客さま宛のメールについてウィルスの検知・駆除、スパムメールの検知を行えるようになります。

※メールチェックゲートウェイサービスとは、ウィルスチェックゲートウェイサービスとスパムチェックゲートウェイサービスの 2 つのサービスの総称です。

2 設定

2-1 利用サーバについて

お客さまにご利用いただくメールチェックゲートウェイサーバは、弊社インフォメーションセンターよりサービス開始時にメールにて送付している『[bit-drive メールチェックゲートウェイサービス ご利用サーバ確定のお知らせ](#)』に記載されております。

【bit-drive メールチェックゲートウェイサービス ご利用サーバ確定のお知らせ】

プライマリサーバ: vcgwpX.bit-drive.ne.jp
セカンダリサーバ: vcgwsX.bit-drive.ne.jp

[ウィルスチェックゲートウェイサービス]
サービス開始日: 20XX 年 XX 月 XX 日

[スパムチェックゲートウェイサービス]
サービス開始日: 20XX 年 XX 月 XX 日

“pX”と“sX”の部分はお客さま毎に異なります。X は 1 桁以上の半角数字となります。

尚、設定はサービス開始日以降に行ってください。事前に設定した場合、メールの受信ができなくなりますのでご注意ください。

2-2 MXレコード設定

お客さま DNS サーバにおいて、お客さまがご利用になられるドメインの MX レコードに弊社メールチェックゲートウェイサーバを登録することにより、お客さまドメイン宛のメールがメールチェックサーバ上を通過します。その際にウイルスチェック及びスパムチェックを行い、安全なメールとしてお客さまメールサーバに配送いたします。

MXレコードとは、DNSで定義される情報の1つで、電子メールの配送先を決定する際に参照されます。複数 MX レコードを定義し優先度を設定しておくことで、優先度の高い配送先メールサーバにて障害が発生して配送できなくなった場合でも、代替として次の優先度に指定されているサーバにメールを配送することができます。

可用性を高めるため、メールチェックゲートウェイサーバプライマリの優先度を上げ(=プリファレンス値を小さく設定)、障害発生時にはセカンダリへ切り替わるように設定する必要があります。

<ゾーンファイル MX レコード設定例>

```
IN MX 10 vcgwpX.bit-drive.ne.jp.
```

←メールチェックゲートウェイサーバのプライマリを指定

```
IN MX 20 vcgwsX.bit-drive.ne.jp.
```

←メールチェックゲートウェイサーバのセカンダリを指定

記述方法につきましては、弊社サポートサイトに掲載しております「DNS 設定例」(PDF ファイル)をご覧ください。

<http://www.bit-drive.ne.jp/support/technical/dns/index.html>

※MXレコードの設定変更はお客さまプライマリ DNS サーバで行います。

尚、弊社ではセキュリティの観点から「お客さまメールサーバ」を MX レコードに指定しないことを推奨しております。詳しくは、サポートサイトの「お客さまメールサーバの MX 登録削除」のページをご覧ください。

http://www.bit-drive.ne.jp/support/technical/mail-check/02-record_MX.html

2-3 SPFレコード設定

SPF (Sender Policy Framework) は送信ドメイン認証のひとつで、差出人となるメールアドレスが本来利用するメールサーバから送信されているかを認証する技術です。宛先となるメールサーバが SPF による認証を行って受信の制御を行っている場合、予め DNS サーバ上に SPF レコードを登録しておくことにより認証を通過させることができます。

反対に、適切に SPF レコードを設定していなかった場合、認証を行っているサーバに「なり済まし(詐称)メール」と判断され、メール配送が拒否されてしまう恐れがあります。

(弊社メールチェックゲートウェイサービスは SPF 認証を行っておりません)

そのため、ご利用いただいている送信元ドメインと送信元となる IP アドレスが関連した SPF レコードをお客さま DNS サーバに記述していただく必要があります。

以下に、SPF に対応するためのゾーンファイル設定例を記載いたします。

IN MX 10 vcgwpX.bit-drive.ne.jp.	←①
IN MX 20 vcgwsX.bit-drive.ne.jp.	←②
IN TXT "v=spf1 include:_mcgwspf.bit-drive.ne.jp ip4:XXX.XXX.XXX.XXX ~all"	←③

- ① メールチェックゲートウェイサーバプライマリ用 MX レコード
- ② メールチェックゲートウェイサーバセカンダリ用 MX レコード
- ③ SPF レコード (TXT レコード)

意味:

v=spf1 SPF バージョン (現在のバージョンは 2 ですが、互換性を保つため 1 と記載します)

include:<ドメイン(txt レコード)>

指定したドメイン (**_mcgwspf.bit-drive.ne.jp**) のテキストレコードを参照し、チェックを行います。

“_mcgwspf.bit-drive.ne.jp” は、弊社メールチェックゲートウェイサーバが属するネットワークを示していますので、SPF に対応する場合は必ずご指定ください。

ip4:<IP アドレス>

指定した IP アドレスをチェックします。

お客さまドメインにてメールを送信するメールサーバの IP を全て記述します。必ず弊社メールチェックゲートウェイサーバを経由させてメールを送信する場合、この設定は上記の”include~”を入れることにより不要となります。

- ~all 判定方式を表します。
 指定した以外のアドレス(txt レコードで指定しているアドレス範囲以外)からメール
 が送信された場合の扱いを指定します。
 all の前の記号は、次の意味を持ちます。

+	Pass (認証成功扱い)
-	Fail (認証失敗扱い) 指定した以外のホストからはメールが送信されることは絶対がないことを表します。
~	SoftFail (Neutral と Fail の中間の扱い) 認証情報を公開してはいるものの、場合によっては認証できないメールも存在することを表します。
?	Neutral (認証情報がないものと同様の扱い) 認証情報を公開していないことを表します。

上記判定基準を元に、配送先メールサーバがメールの受信・拒否を判定します。

記載例

- ・メールを送信するサーバが 1 台の場合

```
IN TXT "v=spf1 include: mcgwspf.bit-drive.ne.jp ip4:xxx.xxx.xxx.xxx ~all"
```

- ・メールを送信するサーバが複数台の場合

```
IN TXT "v=spf1 include:_mcgwspf.bit-drive.ne.jp ip4:xxx.xxx.xxx.xxx ip4:yyy.yyy.yyy.yyy ~all"
```

- ・ネットワークアドレスで設定する場合(例:ネットワーク範囲を/24 で設定)

```
IN TXT "v=spf1 include:_mcgwspf.bit-drive.ne.jp ip4:xxx.xxx.xxx.xxx/24 ~all"
```

尚、SPF の解説については JEAG (Japan Email Anti-Abuse Group: 迷惑メール対策技術検討グループ) がリコメンデーションを発行しています。あわせてご確認ください。

JEAG Recommendation ~送信ドメイン認証について~

<http://jeag.jp/news/pdf/SenderAuthRecommendation.pdf>