ギデオン アンチウイルス

GIDEON

ブロック システム

BLOC system

クイックガイド

重　要

page5「スパム判定で除外するグローバル

IPアドレス」を必ず設定してください。

第1章 アンチスパムの設定

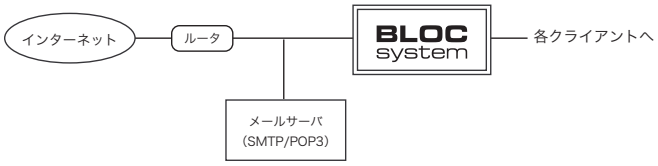
1.1 スパム判定について

BLOCを設置する位置によって、スパム判定のプロトコル（POP3、SMTP）が異なります。ご利用のネットワーク環境に適した位置にBLOCを設置してください。

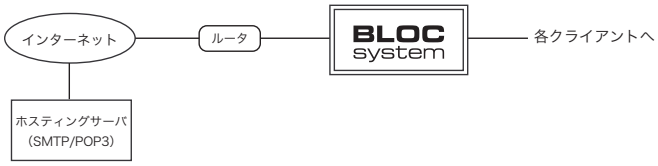
● POP3でのスパム判定

クライアントPCとメールサーバの間にBLOCを設置する場合、受信メールはPOP3によるスパム判定になります。例として、メールサーバのホスティングサービスや社外のメールサーバを利用している環境などがこれにあたります。ただし、メールの送信はSMTPのスパム判定になります。

例：メールサーバとクライアントPC間に設置



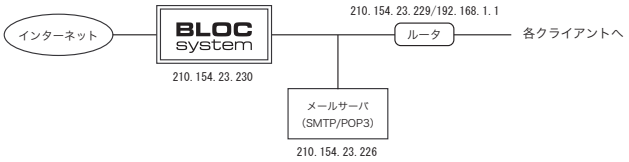
例：ホスティングサービスを利用している



● SMTPでのスパム判定

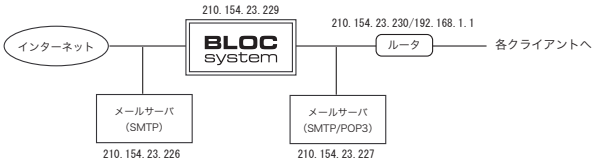
メールサーバの上位、もしくはリレーサーバとメールサーバの間にBLOCを設置する場合、SMTPによるスパム判定になります。リレーサーバとNotesまたはExchangeサーバ間の環境もこれにあたります。

例：メールサーバの上位に設置する例



※メールサーバ（210.154.23.226）を通過しないメール受信はPOP3でチェック可能

例：メールサーバ間に設置する例



1.2 メールサーバ情報の設定

スパム判定で除外するグローバルIPアドレス

BLOCでは、信頼できるメールサーバ（グローバルIPが振られている自社もしくはホスティングサーバ）の直前のメールサーバのIPアドレスをチェックしてスパム判定を行います。従って、利用しているメールサーバやリレーサーバのIPアドレスをスパム判定対象から除外する指定が必要です。

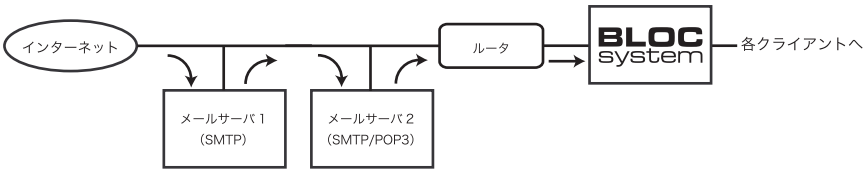
「スパム判定で除外するグローバルIPアドレス」の欄に、BLOCでメールを受信する経路上にあるスパム判定の対象外のサーバのグローバルIPを登録します。

注意

この設定を正しく行わないとスパム判定方法のR1、S25R、RESが有効でなくなるため、スパム判定精度が低くなります。

下記の例を見ると分かるように『スパム判定で除外するグローバルIPアドレス』は、BLOCの上位に存在する受信に利用しているSMTPサーバ及びPOPサーバの全てを記述する必要があります。

-----例-----

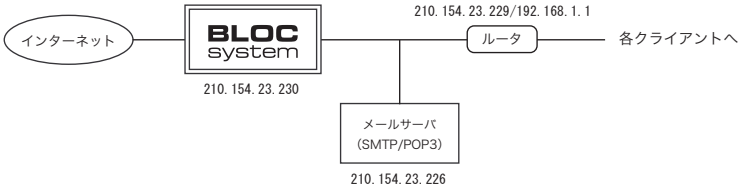


この例は、外部からのメールをメールサーバ1が受信し、自社内部リレー（メールサーバ2）の後ろにBLOCを導入した場合です。

- BLOCの直前に置かれたすべての受信メールサーバ（リレーサーバ含む）のIPアドレスを、スパム判定対象外に指定します。上記例の場合、「メールサーバ1」「メールサーバ2」のIPアドレスを「スパム判定で除外するグローバルIPアドレス」に入力します。その後、［更新］ボタンをクリックします。
- 転送目的のサーバ（例：メールサーバ1）のグローバルIPアドレスも入力してください。
- プライベートIPはスパム判定には使わないため、グローバルIPアドレスのみを指定します。

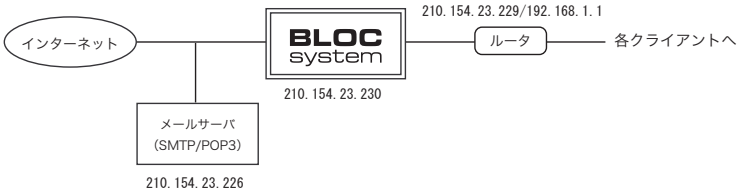
※ プライマリ／セカンダリなどスタンバイサーバがある場合や、複数台のメールサーバをバランサーで振り分けている場合でも、同様にすべてのIPを記述してください。
※ グローバルIPアドレスが不明な場合は、受信しているメールソフトのヘッダ情報をご参照ください。

典型的な例：1



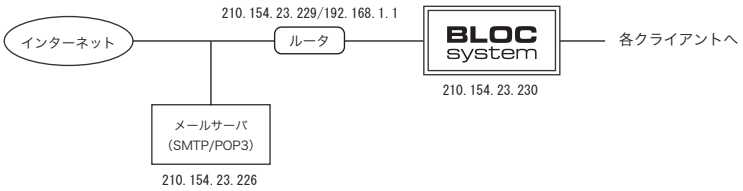
スパム判定で除外するグローバルIPアドレス［記述する必要はありません］
※ スパム検出−SMTP

典型的な例：2



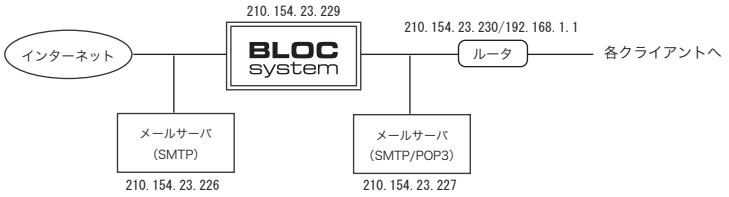
スパム判定で除外するグローバルIPアドレス［210.154.23.226］
※ スパム検出−POP3

典型的な例：3



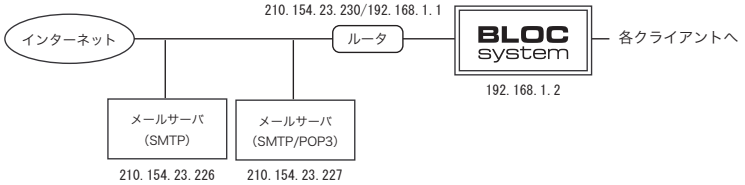
スパム判定で除外するグローバルIPアドレス［210.154.23.226］
※ スパム検出−POP3

典型的な例：4



スパム判定で除外するグローバルIPアドレス［210.154.23.226］
※ スパム検出−SMTP

典型的な例：5



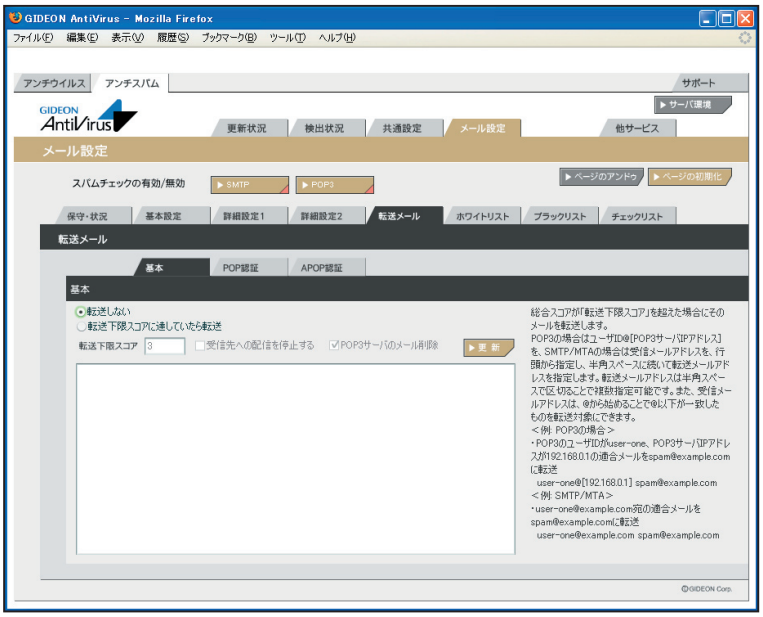
スパム判定で除外するグローバルIPアドレス［210.154.23.226］［210.154.23.227］
※ スパム検出−POP3

第2章 メール転送(削除)の設定

2.1 POP3でのメール転送の設定

2.1.1 転送するメールアドレスの指定と転送先の設定

管理画面【アンチスパム】−【メール設定】−【転送メール】−【基本】を開きます。



画面2.1.1

1. 「転送下限スコアに達していたら転送」にチェック
2. 転送する下限スコアを設定(デフォルトは4点以上を転送)
3. 転送するメールアドレスと転送先メールアドレスを指定(必須)

以下の例を用いて説明します。

個人アドレス	user-1@example.co.jp、user-2@example.co.jp、…
POP3サーバIP	210.154.23.226(example.co.jp)
転送先アドレス	spam-A@example.co.jp、spam-B@example.co.jp、…

例1：ユーザ(メールアカウント)毎に転送先を設定する場合

user-1、user-2 はspam-A@example.co.jpに転送、user-3はspam-B@example.co.jpに転送する

user-1@[210.154.23.226] spam-A@examole.co.jp
user-2@[210.154.23.226] spam-A@examole.co.jp
user-3@[210.154.23.226] spam-B@examole.co.jp

例2：ドメイン(examole.co.jp)宛てのすべてをspam-A@examole.co.jpに転送する設定

@[210.154.23.226] spam-A@examole.co.jp

例3：送受信するメールすべてをspam-A@examole.co.jpに転送する

@ spam-A@examole.co.jp

※ POP3での転送するメールアドレスの指定はすべて［IPアドレス］の記載方法となります。

重要

転送するメールアドレスに「@」のみを指定した場合、受信するすべてのメールアドレスがその対象となります。会社で利用している以外のプライベートのメールなどをすべて判定します。あらかじめご留意ください。

2.2 POP3でのメール削除の設定

2.2.1 プリフェッチ機能とは?

POP3 でのスパムメール削除／転送を行うには、BLOC が持つプリフェッチ機能を用います。
プリフェッチ機能とは、クライアントPC でメールを受信するのと同じ動作をBLOC が行う仕組みで、BLOC がサーバのメールボックスのメールを巡回しながらチェックします。
スパムと判定した場合、転送／削除の指定をあらかじめ設定しておくことで、ユーザがメール取得する際には通常メールのみ受信する仕組みです。

ユーザ (POP アカウント)情報はBLOC が自動で登録 (POP 認証の場合)するため、ユーザ情報の設定は必要ありません。また、BLOC 自身はメールを保持しないため、メール紛失の危険はありません。

2.2.2 プリフェッチ機能を使ってスパムメールを削除する

【アンチスパム】–【メール設定】–【転送メール】–【基本】管理画面を開きます。

1. 「転送下限スコアに達していたら転送」にチェック
2. 転送する下限スコアを設定(デフォルトは4点以上)
3. 転送するメールアドレスと転送先メールアドレスを指定(必須)
4. 「POP3サーバのメール削除」にチェック

削除するメールアドレスの設定につきましては、前述の「2.1.1 転送するメールアドレスの指定と転送先の設定」POP3でのメール転送の設定」の項をご参照ください。

POP認証の場合

通常のPOP認証の場合、スパムメール削除の設定後、クライアントPCから初めてメール取得するときにユーザ情報はBLOCに自動登録されます。
デフォルトでは【アンチスパム】–【メール設定】–【転送メール】–【POP認証】で「自動的にユーザリストを追加する」にチェックが入っていますが、手動で設定したい場合はチェックをはずし、次項「APOP認証の場合」の設定方法をご参照ください。
一度登録されたユーザ情報は一定期間BLOC内に保持されます。

APOP認証の場合

APOPは、パスワードを暗号化して認証を行うため、BLOCにあらかじめユーザ情報を登録しておく必要があります。
【アンチスパム】–【メール設定】–【転送メール】–【APOP認証】の管理画面より以下の方法で登録を行ってください。

アカウントを以下の情報で設定する場合、例のような記載方法になります。

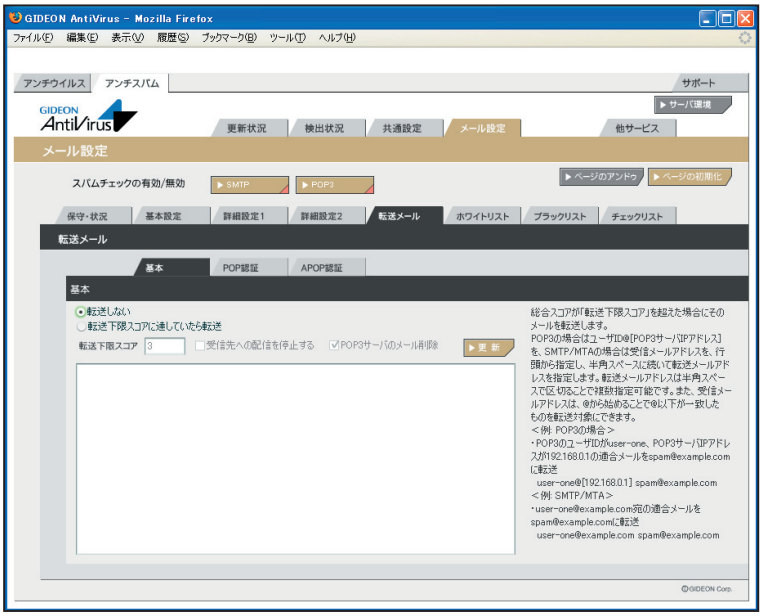
ユーザID：user-1
パスワード：123456
POP3サーバのIPアドレス：192.168.0.1

例： user=user-1 password=123456 host=192.168.0.1

※ 登録されたパスワードは、次回表示時には「＊」で表示されます(password=*)。
パスワードを編集したい場合は、「＊」を消去し、新たなパスワードを入力してください。

2.3 SMTPでのメール転送の設定

SMTPでのメール転送設定を解説します。
【アンチスパム】−【メール設定】−【転送メール】の管理画面を開きます。



画面2.3

1. 「転送下限スコアに達していたら転送」にチェック
2. 転送下限スコアを変更(通常はデフォルト設定の4)
3. 転送するメールアドレスと転送先メールアドレスを指定(必須)

例:個人毎に転送先を指定する場合

(user-one宛てのスパムメールをspam-adminに転送、user-two宛てのスパムメールを admin@example.comに転送する)

user-one@example.com spam-admin@example.com
user-two@example.com admin@example.com

例:ドメイン毎に転送先を指定する場合

@example.com spam-admin@example.com
@sample.ne.jp spam@sample.ne.jp

この設定を行うことでスパムメールをユーザに届かないようにすることが可能です。
注:スパムメールの転送は、必須の設定項目ではありません。運用形態に合わせてご利用ください。

2.4 SMTPでのメール削除の設定

SMTPでのメールの設定を解説します。
【アンチスパム】−【メール設定】−【転送メール】の管理画面を開きます。

1. 「転送下限スコアに達していたら転送」にチェック
2. 転送下限スコアを変更(通常はデフォルト設定の4)
3. 転送するメールアドレスと転送先メールアドレスを指定(必須)
4. 「受信先への配信を停止する」にチェックを入れる

転送対象となるメールアドレス、転送先の設定につきましては、前項の「2.3 SMTPでのメール転送の設定」をご参照ください。

第3章 設定のポイント

3.1 転送アドレスの設定

転送メール設定でよく発生する問題として、メール転送先のアドレスを指定しているにも関わらず、メールがそのアドレスに転送されないというものがあります。この問題は、いくつかの設定箇所を確認することで解決する可能性は非常に高くなります。

● 見るべき設定箇所その1

【共通設定/基本設定】−【報告メールに記入するFROMフィールド】

例えば、「postmaster@example.com」と設定していた場合、@以降のドメイン名（example.com）のMXが引ける必要があります（メールサーバによる）。
「メール送信に使用するSMTPサーバ」とは直接関係なく、FromアドレスがDNSで解決できる必要があります。

=== DNS登録の調査方法 ===

C:\Windows> nslookup アドレス部のドメイン部分
C:\Windows> nslookup -type=mx アドレス部のドメイン部分

● 見るべき設定箇所その2

【共通設定/詳細設定】−【メール送信で使用するSMTPサーバ】

BLOCから送信が可能であるメールサーバを指定します。送信でPOP認証が必要となるメールサーバの場合は、BLOCが対応できていないため不可能です。他のメールサーバを指定してください。

=== 指定のメールサーバが利用可能かどうかの調査方法 ===

C:\Windows> telnet メール送信で使用するSMTPサーバ smtp

上記コマンドで、
220 サーバ名
というメッセージが返ってくるならば少なくともSMTPサーバは存在しています。

注：Fromアドレスに該当するメールサーバが、Fromアドレスでリレー拒否など設定されているようであれば他のアドレスを指定してください。また、メール送信で使用するSMTPサーバの名前が解消できない場合は、IPアドレスを指定してください。

● 見るべき設定箇所その3

【メール設定/詳細設定2】−【転送メール設定】

例として以下の設定をした場合、

@example.com spam-master@example.com
（先頭の@example.comは転送対象アドレス、次のspam-master@example.comは
転送先アドレス）

この設定でスパムメールと判定されたメールのenvelope toが@example.comとメールアドレスの一部で“@”を含む文字列が完全に一致した場合に、spam-master@example.comへスパムメールを転送します。

注1：左側に指定するドメイン名、メールアドレスは、メールの宛先ではなく、envelope toのアドレスを指定します。転送できない場合には、SMTP ログの to= を参照してください。
注2：@ 以降がドメイン名だけになっているのか、ホスト名が付加されているのか等々を注意。
注3：大文字、小文字の区別をしています。よくわからなければ両方指定してください。

転送対象アドレス
転送先アドレスにメールが届いてない場合、転送対象アドレスが一致していない可能性があります。これを確認するためには【メール設定/保守状況】−【SMTPログ】で、のto=のアドレスが一致するかどうか見ます。

例として以下の設定をした場合、

@example.com spam-master@example.com

この設定の状態でSMTPログを見ます（ログ中で下記3行は1行）。

192.168.1.1 192.168.1.3 [Mon, 28 Aug 2006 18:28:37 JST]
from="spammer@example.net" to="user01@mail.example.com"
message-id="20060828182821.bf48b29c.user01@example.com"

to=のアドレスのドメインの部分は@mail.example.comとなっています。この場合、設定の@example.comと一致しないため転送されません。よって以下のように設定することで転送されるようになります

@mail.example.com spam-master@example.com

転送先アドレス

転送先アドレスには有効なメールアドレスを記述します。
FQDN、ドメイン名がMXまたは Aレコードで解決できる必要があり、ユーザが存在するものです。
ただし、FQDNで指定する場合、FQDNがCNAMEで指定された名前であった場合、配送できない可能性があります。

C:\Windows>nslookup FQDN

でAliasesにそのFQDNがある場合、そのFQDNはエイリアスであり、メールを送信できない可能性があります。AレコードかMXレコードで登録されているFQDNやドメインを記載してください。但し、FQDNで指定する場合、FQDNがCNAMEで指定された名前であった場合配送できない可能性があります。

例として以下の設定をした場合、

@example.com spam-master@alias.example.com

この設定の状態でコマンドプロンプトから以下のコマンドを実行してみます。

C:\Windows>nslookup alias.example.com
Server: ns.example.com
Address: 192.168.1.2

Name: mail.example.com (Aレコード)
Address: 192.168.1.3
Aliases: alias.example.com (CNAME=エイリアス)

この場合、spam-master@alias.example.comへはメールが配信できない可能性がありますが、以下のようにspam-master@mail.example.comであればメール配信が可能な場合があります。

@example.com spam-master@mail.example.com

「ギデオン アンチウイルス BLOC system」
クイックガイド

2009年 3月 6日　　第4刷

発行所　株式会社ギデオン
〒223-0056　神奈川県横浜市港北区新吉田町3448-4
http://www.gideon.co.jp/