Usamimi.info - サポート #229

postfixの不正アクセスを防ぐ為、ユーザーのアクセス元を国内限定にする

2016/03/10 11:50 - Clelia ごりゅ

ステータス:	終了	**開始日:**	2016/03/10
優先度:	通常	**期日:**	
担当者:	Clelia ごりゅ	**進捗率:**	50%
カテゴリ:		**予定工数:**	0.00時間
対象バージョン:		**作業時間:**	0.00時間

説明

概要

スパムを弾く話はたくさん見つかる
個人利用であれば十分ですが
共用サーバーにおいては、沢山の利用者のセキュリティ状態も様々である為
パスワードが外部に漏れる、類推されるなどして認証を通り抜け
スパム送信の踏み台にされる状況がそこそこの頻度で発生しています。

根本原因をどうにかするには今のパスワードに頼るやり方を変える必要がありますが
とりあえず、接続元を国内に限定しかつパスワード認証を通ったらメールを送れるようにします。

設定

```
smtpd_restriction_classes =
  check_client_jp

check_client_jp =
  permit_sasl_authenticated

smtpd_recipient_restrictions =
  check_recipient_access hash:/usr/local/etc/postfix/reject_sender,
  permit_mynetworks,
  check_client_access cidr:/usr/local/etc/postfix/check_client_country,
  reject_unauth_destination,
  check_policy_service inet:127.0.0.1:10023
```

check_client_access cidr:/usr/local/etc/postfix/check_client_country部分で
特定のIPかどうかを判定します。check_client_countryにはJPのIPのみがリストされています。

smtpd_restriction_classes =
check_client_jp

check_client_countryにリストされているIPの場合「check_client_jp」フラグが立ちます。
フラグが立つと以下の処理に入ります。

check_client_jp =
permit_sasl_authenticated

メール認証に入り、認証が通れば処理が許可されます。
リストされたIPのみがメール認証に入れる、それ以外は後続の処理に回される為
国内以外は、アカウントのパスワードを知っていたとしても認証にたどり着けないわけです。

check_client_countryの作成には、参考URLで紹介されている「getApnicCidr.txt」を使いました。
全自動でJPの全IPを取得し、リスト化までしてくれるため大変助かりました。

効果

参考URL

http://cmf.ohtanz.com/antispam.html

履歴

#1 - 2016/03/10 11:51 - Clelia ごりゅ

- 説明 を更新

#2 - 2016/03/10 15:44 - Clelia ごりゅ

- 説明 を更新

- ステータス を 新規 から 進行中 に変更

- 進捗率 を 0 から 50 に変更

#3 - 2021/09/15 11:29 - Clelia ごりゅ

- ステータス を 進行中 から 終了 に変更