Vol.2014-IOT-24 No.9
2014/2/27

パスワード不正取得による迷惑メール発信に対する対策

山井 成良[1,a)]　藤原 崇起[1]　河野 圭太[1]　大隅 淑弘[1]　岡山 聖彦[1]

概要：
最近，パスワードリスト攻撃のように何らかの方法で不正取得したパスワードを用いて組織内の MSA（Message Submission Agent）から迷惑メールを大量に送信する事例が増加している．本稿では，その対策法として，送信元 IP アドレスから取得したクライアント地理情報などを利用して迷惑メール発信を早期に検出し，被害を最小限に抑える方法を提案する．また，この方法に基づいて作成したシステムを岡山大学で運用した結果，有効に機能することを確認している．

キーワード：
電子メール，迷惑メール対策，パスワード不正取得，地理情報

Countermeasure against Spam Mail Submissions with Password Cracking

Nariyoshi Yamai[1,a)]　Takaoki Fujiwara[1]　Keita Kawano[1]　Yoshihiro Ohsumi[1]
Kiyohiko Okayama[1]

Abstract:
Recently, incidents of spam mail submissions via Message Submission Agent (MSA) in an organization, abusing illegally obtained passwords such as those used by password list attack, have been reported increasingly. In this paper, we propose a countermeasure against such incidents that detects spam mail submissions earlier using geographic information of each client derived from its source IP address. We also implemented a spam submission prevention system based on the proposed countermeasure. According to our operation experience of the system in Okayama University, we confirmed that the system works effectively.

Keywords: E-mail, anti-spam method, password cracking, geographic information

1. はじめに

電子メールはインターネットで最も普及しているコミュニケーション手段の 1 つであり，社会的な活動を支えるものとして必要不可欠な存在となっている．一方，電子メールはセキュリティ的に様々な問題を抱えており，特に広告，フィッシング詐欺，マルウェア配布などを目的に不特定多数のアドレス宛に一方的に送りつけられる迷惑メールの蔓延は大きな社会問題となっている．この数年間はボットネットの閉鎖，OP25B（Outbound Port 25 Blocking）[1] など，迷惑メール送信を抑止する取り組みが進みつつあり，電子メール全体に占める迷惑メールの割合は 60%台まで減少してきている [2], [3]．特に日本国内では ISP（Internet Service Provider）を中心に OP25B の普及が進み，日本からの迷惑メール送信はかなり減少している [1].

ところが，OP25B の普及に伴い，パスワードリスト攻撃 [4] に代表されるように迷惑メール送信者が何らかの方法でパスワードを不正に取得し，正規の MSA（Message Submission Agent）を用いてユーザ認証を受けたうえで迷

[1] 岡山大学情報統括センター
Center for Information Technology and Management, Okayama University
3-1-1, Tsushima-naka, Kita, Okayama 700–8530, Japan
[a)] yamai@okayama-u.ac.jp

惑メールを発信する [*1] 事例が増加している [5]．自組織内の MTA（Mail Transfer Agent）から大量の迷惑メールが送信されると，社会的な信頼性の低下につながるだけでなく，当該 MTA が Spamhaus ZEN[6]，SORBS[7]，SCBL[8] などのブラックリストサービスに登録され，その結果として自組織から送信された正当な電子メールに対しても他の組織から受信拒否される危険性が高まるため，早期に対処する必要がある．これに対して，一般的には発信回数，宛先数などに基づくスロットリング（throttling）や詐称アドレスに対する発信制限などの対策 [1] が知られている．しかし，これらの対策は正当な利用を制限する可能性も高く，また効果的であるとは限らない．

そこで，本稿ではこの手口を用いて発信される迷惑メールは海外の不特定多数の通信元から MSA に接続されることが多い [5], [9] 点に着目し，送信元 IP アドレスをもとに取得したクライアントの地理情報などを利用して迷惑メール発信を早期に検出し，被害を最小限に抑える方法を提案する．また，実現が比較的容易な実装法および岡山大学における運用結果についても併せて示す．

以下，2 章では従来の迷惑メール送信対策とその問題点について述べる．3 章では上記の手口に対する対策方法を提案し，その実現方法についても触れる．また，4 章では岡山大学で運用している不正発信抑制プログラムの運用結果を示し，今後改良あるいは追加すべき機能について考察する．

2. 従来の迷惑メール送信対策と問題点

本章では自組織内からの迷惑メール送信を抑制する従来の対策手法についていくつか説明し，またそれらの問題点について述べる．

2.1 OP25B

OP25B は自組織内から外部に対する TCP 25 番ポート宛の通信を原則として遮断する方法である．これにより，特定の MTA 以外からの外部宛電子メール送信はできなくなる．もし，組織内ユーザが組織外の MSA を使用して電子メールを発信する場合には，TCP 25 番ポートの代わりに TCP 587 番ポート（SMTP），あるいは TCP 465 番ポート（SMTP over SSL）などを用いることになる．この場合，発信時にユーザ認証 [10], [11] が必要であるため，組織内にボットとなった端末が存在する場合でも，通常はその端末が組織外の MTA を使用して迷惑メールを送信することができなくなる．OP25B によるメール送信制限の様子を**図 1** に示す．

しかし，この方法では，たとえば図 1 において組織 B の MSA で有効なアカウント情報が不正取得された場合には，

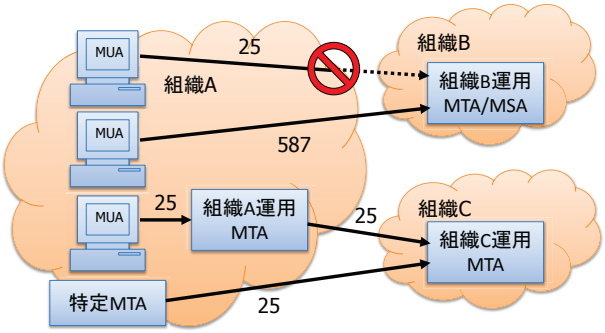

図 1 OP25B によるメール送信制限
Fig. 1 Mail transfer restriction by OP25B.

組織 A 内の端末から組織 B の MSA を用いて迷惑メールを発信できる．これが本稿の対象としている迷惑メールの発信手口である．

2.2 発信回数，宛先数などに基づくスロットリング

スロットリングは通信速度などを意図的に低下させることにより，迷惑メールの大量送信を妨害する方法を指し，迷惑メールの受信対策，送信対策の両方に適用可能である．MSA での迷惑メール発信対策として，IP アドレス毎に一定時間当たりの SMTP 接続回数，発信回数，宛先数，あるいは通信量を制限する方法がよく用いられている．

しかし，本稿で対象としている手口ではボットネットが利用されていると推測され，多数の IP アドレスから 1 台の MSA に接続して大量の迷惑メールを発信する [9] ため，IP アドレス単位で制限を設けてもそれほど効果的ではないと思われる．またこの方法により，一般ユーザによる正当な電子メールの発信が制限される可能性もある．たとえば，端末がネットワークに接続されていない状態でユーザが多数の電子メールを作成した場合，この端末がネットワークに接続された際に作成済みの全ての電子メールの発信が試みられるため，この制限により発信ができないことがあり得る．この他にも，特定多数の宛先へ正当な電子メールを発信する場合にその発信が制限されることも十分考えられる．

2.3 詐称アドレスに対する発信制限

一般に SMTP では差出人アドレスはエンベロープ，ヘッダとも任意に設定することが可能で，特に迷惑メールでは詐称されていることが多い．そこで，MSA では認証されたユーザ名とこれに対する差出人アドレスが一致しない場合に発信しないような機能を使用することが推奨されている．たとえば Postfix[12] では smtpd_sender_restrictions パラメータに reject_sender_login_mismatch などの値を設定することにより，認証されたユーザ名と MAIL FROM アドレスが一致しない場合には発信を抑制することができる．

[*1] 本稿ではユーザ認証後の電子メール送信を発信と記す．

ところが，本稿で対象としている手口では，迷惑メール送信者がユーザ名を入手しており，また多くの組織ではユーザ名をそのままメールアドレスのローカルパートとして使用しているため，迷惑メール送信者が差出人アドレスとして正しいアドレスを使用することが可能である．実際に筆者らの経験でも，正しいアドレスを使用した迷惑メールの発信が確認されている [*2].

3. 迷惑メール発信に対する対策

前章で述べたように，従来の迷惑メール送信対策は，本稿の対象としている手口に対して有効性が乏しかったり，利用者による正当な電子メール発信を制限したりする点で問題があった．そこで，本章では送信元 IP アドレスからクライアントの地理情報を取得し，その情報をもとにパスワード不正取得による迷惑メール発信を制限する方法を提案する．

3.1 提案方法の概要

1 章で述べたように，パスワード不正取得による迷惑メール発信では海外の不特定多数の通信元から MSA に接続されることが多い．文献 [9] では，多い時には 30 を越える国からの迷惑メール発信が観測されたことが報告されている．また，筆者らの運用している MSA でも最大で 31 か国からの MSA への接続が観測されている．

そこで，送信元 IP アドレスに対応する国名を取得し，同一のユーザが一定期間内に多数の国から電子メール発信を試みた場合にこれを検出し，それ以降の発信を抑制する方法を提案する．この方法では，(1) 地理情報の取得方法，(2) 不正発信の検出方法，(3) 電子メールの発信抑制方法が設計上の問題となる．以下では，筆者らが作成したシステムで採用した方法について詳細に述べる．

3.2 地理情報の取得

IP アドレスから地理情報を取得する方法として，まず考えられるのは DNS の逆引きにより得られた FQDN（Fully Qualified Domain Name）の国別コードドメイン名（ccTLD: country code Top Level Domain）で判断する方法である．たとえば，150.46.X.X に対する逆引きにより host.sub.okayama-u.ac.jp のような FQDN が得られた場合，最後の jp は ccTLD であるため，国名は日本であると判断できる．しかし，この方法では特にボットネットを構成する PC の多くは逆引きできず，またたとえ逆引きが可能であっても，実際の位置が ccTLD が示す国名とは一致しなかったり，gTLD（generic Top Level Domain）で国名が不明であったりすることがあるため，確実性の面で大きな問題がある．

[*2] この事例では，不正使用されたアドレス宛に大量のバウンスメールが送られてきたため，迷惑メールの発信が発覚した．

```
Jan 21 12:34:56 mlsvr postfix/smtpd[123]:
A123BCD4567: client=unknown[192.0.2.123],
sasl_method=LOGIN, sasl_username=user1
```

図 2 Postfix における発信時のログの例
Fig. 2 An Example of Mail Submission Log of Postfix.

一方，IP アドレスから地理情報を得る別の手段として，Maxmind 社が提供する GeoIP[13] の活用がある．特に GeoLite データベースは精度こそ有償版に劣るが無料で利用することができる．そこで，筆者らはこれを利用して国名を取得することにした．

3.3 不正発信の検出

不正発信を検出する機能の実現方法としては，(1) milter の利用，(2) 外部ポリシサービスの利用，(3) ログファイルの監視などが考えられる．

このうち (1) は sendmail[14] や Postfix などの MTA で利用可能なフィルタプログラムで，これを用いればクライアント IP アドレスなどのパラメータを MTA から受け取り，メッセージを書き換えたり，MTA でのメッセージの処理内容を制御したりすることが可能である．したがって，この方法を用いれば不正発信の検出だけでなく，その抑制を行うことが可能である．

また (2) はメッセージの書換えは行えないが，(1) と同様にクライアント IP アドレスなどのパラメータを MTA から受け取り，受信の許可，恒久的拒否，一時的拒否など MTA の動作を制御することができる．この機能はたとえば Postfix では check_policy_service パラメータの設定により有効にすることができる．

一方，(3) は MTA とは独立したプログラムを用いてログファイルを監視する方法である．たとえば Postfix では電子メール発信時に**図 2** のようなログを記録するため，認証されたユーザ名とクライアントの IP アドレスを容易に取得することが可能で，実装上の制約が最も少ない．また，他の方法では milter や外部ポリシサーバの動作に異常が発生すると正当な電子メールの送信にも影響を及ぼす可能性が高いのに対して，この方法はその可能性が低い．このため，筆者らはこの方法を採用した．

3.4 電子メールの発信抑制

前節で述べたように milter や外部ポリシサービスを利用した場合には不正発信の検出と同時に抑制を行うことが可能である．しかし，ログファイルの監視による不正発信の検出では，別の方法でパスワード漏洩が疑われるユーザによる電子メール発信を抑制する必要がある．

たとえば Postfix では smtpd_sender_restrictions オプションにより差出人アドレスに基づいて電子メール送信を制限

する機能が利用可能である．しかし，この機能では MAIL FROM アドレスに対する制限しか行えないため，ユーザ名に基づいて制限するためには 2.3 節で述べたように reject_sender_login_mismatch などの値を設定する必要がある．

また，特にユーザ認証に必要なパスワードが，MRA（Mail Retrieval Agent）へのアクセスを含めて他のサービスと共通である場合には，MSA を含めた各サービスへの不正アクセスを防止するためにパスワードを強制変更することが望ましい．ただし，一般に MSA では一度認証に成功すると電子メール発信を何度でも行うことができるため，認証成功後の発信可能件数を制限するか，制限の対象となる SMTP コネクションを強制切断する必要がある．

さらに，不正発信の検出はログファイルの監視で行うものの，電子メールの発信抑制は milter や外部ポリシサーバを用いる方法もある．たとえば Postfix では外部ポリシサーバとして postfwd[15] を利用することで容易に sasl_username に基づいた発信抑制を行うことができる．

4. 不正発信抑制プログラムの運用および考察

筆者らの所属する岡山大学情報統括センターでは，上記の実現方法に基づいて不正発信抑制プログラムを実装し，2012 年 10 月より運用を開始している．本章ではこれまでの運用実績について述べる．また，今後改良あるいは追加すべき機能について考察する．

4.1 不正発信抑制プログラムの運用

当初作成したプログラムは不正発信の監視を行い，不正発信を発見した場合には管理者宛てに電子メールで通知する機能だけを実装し，自動的に発信を抑制する機能は実装していなかった．しかし，それでも従来よりも早めに不正発信を検出することができ，その面では有用であった．その後，自動的に発信を抑制する機能を実装し，何度か改修を行いながら現在に至っている．これまでに不正発信を検出した回数は 9 回で，そのうち 4 回は自動的に発信を抑制することができた．誤検出，検出漏れはともに 1 回あった．これまでの運用実績を**表 1** に示す．

このうち，誤検出の原因は不正発信検出基準が低すぎたためであった．当初は 24 時間以内に国内を含めて 3 カ国以上から MSA に接続があった場合に不正発信を検出するように設定していたが，あるユーザが海外出張する際に日本国内，経由地，目的地の 3 カ国でメール発信を行ったため，誤検出となった．このため，現在では 24 時間以内に 4 カ国以上から MSA に接続があった場合に不正発信と見なすように検出基準を変更している．一方，検出漏れの原因は 1 か国から多数の接続があったためであった．この対策については次章で考察する．

次に不正発信抑制機能について述べる．同機能の実装では，運用当初は Postfix の smtpd_sender_restrictions オプションにより特定の MAIL FROM アドレスが指定された電子メールの発信を抑制するようにしていた．これは当時の手口では，認証ユーザの正規のアドレスが MAIL FROM アドレスとして使われたためである．その後，ランダムなローカルパートを持つアドレスを使う手口が出現したため，アカウントを停止する方法に改めた．しかし，3.4 節で述べたように，この方法では同一の SMTP コネクションを用いた多数の発信を抑制することができないという問題が存在したため，2013 年 10 月 7 日にアカウント停止後に Postfix を再起動する方法への変更を行い，現在に至っている．この変更以降では同様の手口によるメール送信事例が 3 回発生したが，いずれも早期のうちにこれを検出し，不正利用されたアカウントの停止に成功している．

表 1 不正発信抑制プログラムの運用実績
Table 1 Operation Records of the Spam Submission Prevention System.

発生日	国数	抑制	備考
2012/10/17	14	–	同一 MAIL FROM
2012/10/17	3	–	誤検出
2012/10/31	22	–	同一 MAIL FROM
2012/10/31	–	–	MAIL FROM による抑制
2013/05/25	4	成功	同一 MAIL FROM
2013/06/27	1	失敗	検出漏れ
2013/08/31	31	失敗	ランダムローカルパート
2013/09/05	26	失敗	ランダムローカルパート
2013/09/13	–	–	アカウント停止による抑制
2013/10/03	22	失敗	同一コネクションでの送信
2013/10/07	–	–	postfix 再起動による抑制
2013/10/07	4	成功	
2013/10/11	4	成功	
2013/11/29	4	成功	

4.2 不正発信抑制プログラムの改良点に関する考察

これまでの運用経験に基づき，不正発信抑制プログラムの改良点について考察する．

4.2.1 検出漏れへの対策

4.1 節で述べたように，検出漏れの原因は 1 か国から多数の接続があったためであった．この対策としては，検出に地理情報ではなく IP アドレス数を用いる方法が考えられる．ただし，特に最近ではスマートフォンにおいて移動しながら携帯網と無線 LAN の両方を使用するなど，短時間で複数の IP アドレスを用いる場合が考えられるため，検出基準の設定を慎重に行う必要がある．

また，この方法では同一の IP アドレスから多数の発信が試みられた場合には効果がないため，一定期間内の発信回数や宛先数で制限する方法を援用する必要が生じる．そ

の際，地理情報を利用して，たとえばクライアントの位置が国内か国外かに応じて異なる検出基準を適用する方法を採用すれば，正当な電子メール発信の誤検出を減らす効果が期待できる．

4.2.2 検出精度の向上

4.1 節で述べたように，当初の検出基準である 24 時間以内に 3 カ国以上からの接続では誤検出が発生した．そのため，誤検出発生以降では検出基準を 24 時間以内に 4 カ国以上からの接続としたが，これにより検出漏れの可能性が上昇し，また検出までに要する時間が増加したことになる．そこで，国数ではなく検出期間を調整し，たとえば 6 時間以内に 3 カ国以上からの接続を検出基準とする方法が考えられる．検出基準の調整は，今後に同様の攻撃を受けた場合にログを精査し，適切な国数および検出期間を求める予定である．

また，以前に接続があった国からの再接続であっても，以前の接続との間に別の国からの接続が存在した場合，この再接続をさらに別の国から行われたと解釈する方法も考えられる．たとえば，検出基準が一定時間以内に 3 カ国以上からの接続であった場合において，A，B の 2 カ国だけから交互にメール発信が試みられた状況を想定すると，従来の解釈では不正発信を検出できないのに対して，新しい解釈では 3 回目の接続で不正発信を検出できることになる．この解釈での検出基準の調整も今後の課題である．

4.2.3 POP before SMTP との併用

POP before SMTP[16] は，MTA（あるいは MSA）に接続したクライアントが直前の一定期間内に POP での認証に成功した場合に限り，このクライアントからの組織外への配送を許可する方法である．この方法は MSA でのユーザ認証が普及する以前に不正中継対策として提案された方式であり，アドレス変換などにより異なるクライアントが同じアドレスを使用して不正中継を行う可能性が無視できないため，現在はほとんど用いられていない．

一方，筆者らのこれまでの経験によると，本稿で対象としている手口では各クライアントは MSA を利用した電子メール発信のみを行い，同一 IP アドレスから事前に POP サーバを含む MRA へアクセスされた形跡がなかった．したがって，POP before SMTP と MSA でのユーザ認証との併用が，不正発信抑制を強化する方法の一つとして考えられる．すなわち，MSA はたとえクライアントがユーザ認証に成功したとしても，直前の一定時間内に同一の IP アドレスから POP サーバを含む MRA への同一ユーザ名でのアクセスが確認できない場合には不正発信と見なして発信を拒否する方法が有効な対策になり得る．

MSA と MRA でユーザ認証に用いるユーザ名とパスワードが同じ場合，迷惑メール送信者は事前にこれらの認証情報を入手しているため，この対策方法を回避することは容易である．ただし，この対策方法の存在を迷惑メール送信者に気付かれない限り有効に機能することが期待できる．また，MRA と MSA で異なるパスワードを用いるようにすれば，両方のパスワードを入手したうえで発信前に MRA へのアクセスが必要となるため，従来の対策と比べて大幅な有効性の向上が期待できる．

5. まとめ

本稿では，不正に取得したパスワードを用いてユーザ認証を受けたうえで迷惑メールを発信する行為への対策として，特にクライアントの地理情報に基づいて発信を抑制する方法を提案し，その実現方法を示した．また，提案方法に基づいて実装した不正発信抑制システムの運用実績を示し，システム改良後は不正利用されたアカウントを早期に停止できていることを確認した．さらに，これまでの運用実績に基づき，現在の不正発信抑制プログラムにおいて改良すべき点を考察した．今後の課題としては，この考察結果に基づいたプログラムの改良が挙げられる．また，運用実績を積み重ねることにより，誤検出や検出漏れが少なくなるように検出基準の調整を行うことも重要な課題である．

謝辞 本研究の一部は平成 23〜25 年度科学研究費補助金 (基盤研究 (C)，課題番号 23500122) の補助を受けている．ここに記して感謝の意を表する．

参考文献

[1] 迷惑メール対策推進協議会 : 迷惑メール対策ハンドブック 2013 (online)，入手先 ⟨http://www.dekyo.or.jp/soudan/image/anti_spam/book/2013/2013MHB_all.pdf⟩ (2014.01.21).

[2] Symantec Corporation: Internet Security Threat Report 2013 :: Volume 18 (online), available from ⟨http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf⟩ (2014.01.21).

[3] Symantec Corporation: Symantec Intelligence Report :: DECEMBER 2013 (online), available from ⟨http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_12-2013.en-us.pdf⟩ (2014.01.21).

[4] 独立行政法人情報処理推進機構 : 2013 年 8 月の呼びかけ（online），入手先 ⟨http://www.ipa.go.jp/security/txt/2013/08outline.html⟩ (2014.01.21).

[5] Telecom-ISAC Japan : 認証情報を不正に利用したスパムメールの送信について (online)，入手先 ⟨https://www.telecom-isac.jp/news/news20111205.html⟩ (2014.01.21).

[6] The Spamhaus Project Ltd.: The Spamhaus Project - ZEN (online), available from ⟨http://www.spamhaus.org/zen/⟩ (2014.01.21).

[7] SORBS: SORBS (Spam and Open-Relay Blocking System) (online), available from ⟨http://www.sorbs.net/⟩ (2014.01.21).

[8] Cisco Systems, Inc.: SpamCop.net – Blocking List (bl.spamcop.net) (online), available from ⟨http://www.spamcop.net/bl.shtml⟩ (2014.01.21).

[9] 渡辺 崇文 : “迷惑メール送信を目的とした不正 SMTP 認証の増加”，Internet Infrastructure Review (online), インターネットイニシアティブ, Vol.20, pp.28–31 (2013), 入手

先 ⟨http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol20.pdf⟩ (2014.01.21).
[10] Myers, J.: Simple Authentication and Security Layer (SASL), RFC 2222, IETF (1997).
[11] Myers, J.: SMTP Service Extension for Authentication, RFC 2554, IETF (1999).
[12] Venema, W: The Postfix Home Page (online), available from ⟨http://www.postfix.org/start.html⟩ (2014.01.21).
[13] Maxmind Developer Site: "GeoIP Products << Maxmind Developer Site (online), available from ⟨http://dev.maxmind.com/geoip/⟩ (2014.01.21).
[14] Sendmail, Inc.: Open Source – Sendmail.com (online), available from ⟨http://www.sendmail.com/sm/open_source/⟩ (2014.01.21).
[15] Kessler, J. P.: postfwd – postfix firewall daemon (online), available from ⟨http://postfwd.org/⟩ (2014.01.21).
[16] Harkins, N. and Levine, J.: POP before SMTP (online), available from ⟨http://spam.abuse.net/adminhelp/smPbS.shtml⟩ (2014.01.21).