迷惑メール送信を目的とした不正SMTP認証の増加

SMTP認証のためのIDやパスワードを使ってメールアカウントが第三者に利用され、迷惑メール送信に悪用される問題が増加傾向にあります。多くのケースにボットネットが利用されていること、そしてそのボットネットはSMTP認証をした上でメール送信を試みていることが分かっています。ここでは、IIJのメールサービスで観測した不正SMTP認証によるアクセスの動向を紹介します。

2.1 はじめに

このレポートでは、迷惑メールの最新動向やメールに関連する技術解説、IIJが関わる様々な活動についてまとめています。今回は、IIJのメールサービスで観測したデータを元にその分析結果を報告します。

最近、第三者が正当な利用者のアカウントと認証情報を利用して特定のサービスにログインを試みる事例が相次いでいます。ポータルサイトやウェブサービスにおいては、そのアカウント情報の搾取や改ざんが目的とされるケースが多いようです。一方、メールサービスにおいてもアカウントの不正な利用が以前から問題となっており、2012年にJPCERTコーディネーションセンターから、複数のISP事業者のメールサービスにおいて、メールアカウントの不正利用が観測されていることが報告されています[*1]。メールアカウントの不正利用の目的は、主に迷惑メールの送信であると言われており、その手口の多くにボットネットが利用されていることも分かっています。

本レポートでは、このメールアカウントの不正利用問題について取り上げ、IIJのメールサービスで観測した不正SMTP認証によるアクセスの動向について報告します。

2.2 不正SMTP認証によるアクセスの動向

2.2.1 不正SMTP認証

本来、SMTP認証は、メールの送信者が正当な利用者本人であることを確認するために利用されています。しかし、近年、このSMTP認証に使うメールアカウントのIDやパスワードの情報が、ウイルス感染など何らかの手段で盗まれ、正当な利用者ではない第三者により、迷惑メールの送信に悪用される事象が問題となっています。本レポートでは、このような第三者が正当な利用者の認証情報を使ってSMTP認証を行うことを「不正SMTP認証」と表現します。そしてIIJが提供するメールサービスにおいては、独自のサービス基準で、この不正SMTP認証によるアクセスの観測と対策を行っていますが、その観測数は増加傾向にあります。

2.2.2 不正SMTP認証の特定

不正SMTP認証によるアクセスを、正確かつリアルタイムに特定することは容易ではありません。メールアカウントの送信元IPアドレスの地理的傾向、メールの送信通数、宛先の傾向などを考慮し、総合的に判断する必要があるからです。その中でも、不正SMTP認証によるアクセスを特定するための重要な手掛かりとなるのが、送信元IPアドレスの地理的傾向です。不正SMTP認証によるアクセスは、地理的に分散した多数の送信元から行われていることが多く、これはボットネットからの迷惑メール送信に見られる特徴と共通しています。ボットネットは、その拡散と追跡を困難にするために年々知的化しており、最近では、ZeroAccess[*2]のようなP2P型のボットネットの脅威が報告されています。IIJでは、独自のサービス基準で不正SMTP認証によるアクセスを日常的に検出し、対策を行っています。

＊1　JPCERTコーディネーションセンター、「メールアカウント不正使用に関する情報提供のお願い」(http://www.jpcert.or.jp/pr/2012/pr120003.html)。
＊2　Over 9 million PCs infected - ZeroAccess botnet uncovered(http://nakedsecurity.sophos.com/2012/09/19/zeroaccess-botnet-uncovered/)。

2.2.3 不正SMTP認証の観測

IIJのメールサービスにおいて、特定期間に観測した不正SMTP認証によるアクセスを受けていたアカウントの数を図-1に示します。図-1から、不正SMTP認証によるアクセスを受けているメールアカウントが日常的に検出されていることが分かります。1日あたりの平均検出件数は数件程で、多いときは数十件程度でした。

多くの場合、不正SMTP認証によるアクセスを受けていたアカウントに傾向は見られませんが、特定ドメインの複数アカウントが同時に不正SMTP認証によるアクセスを受けていたケースも観測されました。これは社内のウイルス感染により、SMTP認証に使われるメールアカウントのIDやパスワードの情報が搾取されたのではないかと推測できます。

検出されたメールアカウントについては、そのアクセス元IPアドレスが極めて多く、かつ地理的に広範囲に分散している点が共通していました。

■ アクセス元IPアドレスの地理的傾向

次に、アクセス元IPアドレスの地理的傾向について調べてみました。図-2は、今回の対象期間に検出されたアカウントのアクセス元IPアドレスのうち、上位を占めた地域をピックアップして時系列に並べたものです。

この期間では、ポーランド(PL)、及び、インド(IN)からのアクセスが他のアクセス元地域に比べて大きな割合を占めていたことが分かります。

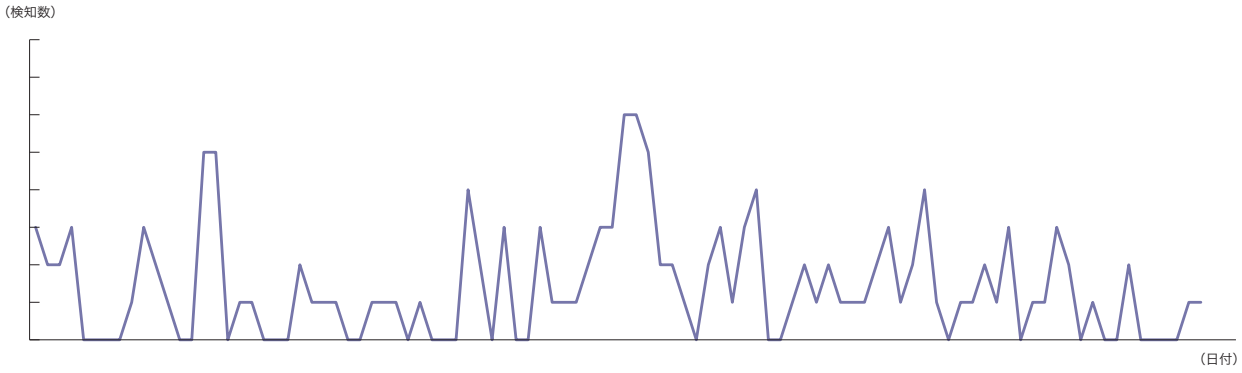

図-1 不正SMTP認証によるアクセスを受けたアカウント数

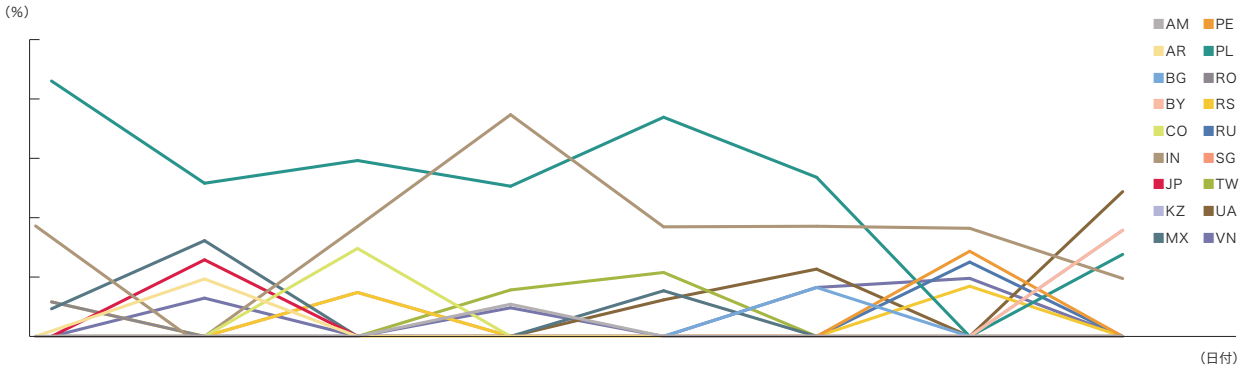

図-2 アクセス元地域の割合の推移

JPCERTコーディネーションセンターからの報告[*1]によると、メールアカウントの不正利用の多くは迷惑メール送信に悪用されていることが窺えます。また、迷惑メールの上位送信国ランキングを定期的に発表しているSophos社のレポート[*3]においても、ポーランド(PL)は2012年の迷惑メール送信国の10位、インド(IN)は1位にランクインしていました。これらの国は、今回の調査対象期間においても依然として迷惑メールの送信が多く行われていたことが推測できます。

また、アクセス元IPアドレスが数千を超えるような大規模なアクセスでは、前述した中東欧の地域に加え、アルゼンチン(AR)や南アフリカ共和国(ZA)なども含め、多いときには30を越える国からのアクセスがあるケースも観測されました。このように、アクセス元の上位には中東欧の地域が目立っていますが、ほぼ全世界からのアクセスが確認できており、不正SMTP認証によるアクセスにはボットネットが利用されていると推測できます。

■ アクセス元IPアドレス数の推移

図-3に、不正SMTP認証によるアクセスを検出したメールアカウントのアクセス元IPアドレス数の推移を示します。今回の対象期間において、検出したアクセス元IPアドレス数は平均で数百個、最大では数千個にも上りました。

■ アクセス元IPアドレスと迷惑メール送信試行回数

今回の対象期間において、アクセス元IPアドレスが迷惑メール送信に使われる頻度を調査したところ、2つのパターンに分けられることが分かりました。一方は、1つのIPアドレスから数千通に及ぶメール送信を試みているケース、他方は1つのIPアドレスから数通程度のメール送信を試みているケースです。今回の対象期間に検出した結果では、後者が9割を占め、前者が1割でした。前者のケースについて、あるメールアカウントのアクセス元IPアドレスごとの不正SMTP認証によるメール送信の試行回数を図-4に、後者のケースについて同様に図-5に示します。

更に、図-4で調査を行ったアカウントに対して、各アクセス元IPアドレスのアクセス時間の間隔を調べたところ、1つのIPアドレスあたり約1時間に渡って、1秒あたり数回の頻度で連続的にメール送信を試みている形跡がありました。一方、図-5で調査を行ったアカウントに対しても同様に調べたところ、同一のIPアドレスから連続してメール送信を試みた形跡はありませんでした。

1つのIPアドレスから連続的かつ大量にメールを送信するのではなく、数通程しか送らずに大量のIPアドレスからメールを送信する手法は、アクセス元の追跡を困難にしようとする迷惑メール送信者の典型的な手法です。

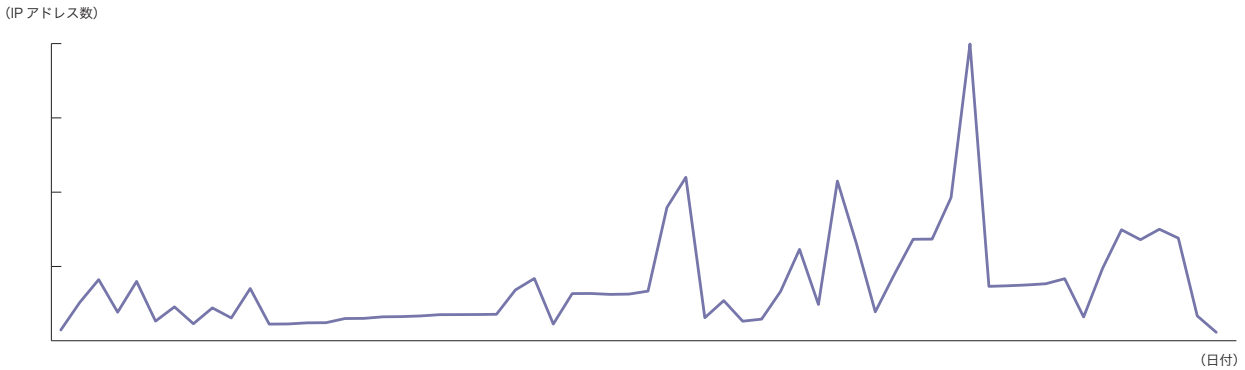

図-3 アクセス元IPアドレス数の推移

*3　Sophos Security Threat Report 2013(http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf)。

2.3 おわりに

本レポートでは、メールアカウントの不正利用問題について取り上げ、IIJのメールサービスにおける不正SMTP認証によるアクセスの傾向について、その観測状況を報告しました。不正SMTP認証によるアクセスの観測結果から、その送信元は、ほぼ全世界に分散した多数のIPアドレスであることから、ボットネットを利用したアクセスである可能性が高いと考えられます。また、送信元IPアドレスの地理的傾向から、迷惑メールの送信地域の上位に報告されている地域から、依然として迷惑メール送信が試みられている可能性が高いことも窺えました。更に、不正SMTP認証によるメール送信の試行形態が一律でない点についても観測しました。不正SMTP認証アクセスによる証拠を正確に捉えることは容易ではありませんが、IIJでは独自のサービス基準で早期に不正なアクセスを検知し、対策を行っています。

その一方で、JPCERTコーディネーションセンターからの報告[*1]によると、攻撃者がメールアカウントのSMTP認証情報を盗む手口としては、POPサーバに対する辞書攻撃、フィッシング、ウイルス感染などが代表的です。従って、端末へのウイルス対策やパスワードの定期更新、不要なメールアカウントの削除など、利用者側での適切な防御を継続的に行うことが求められています。

IIJでは、今後も継続的に不正SMTP認証によるアクセスの傾向を分析し対策を行うことで、安心して利用できるメールサービスの運用を行って参ります。

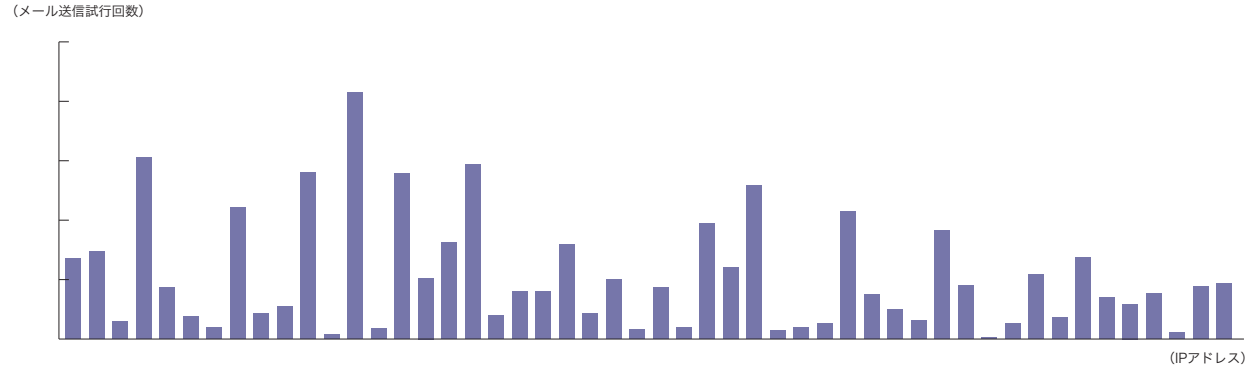

図-4 アクセス元IPアドレスあたりのメール送信試行回数

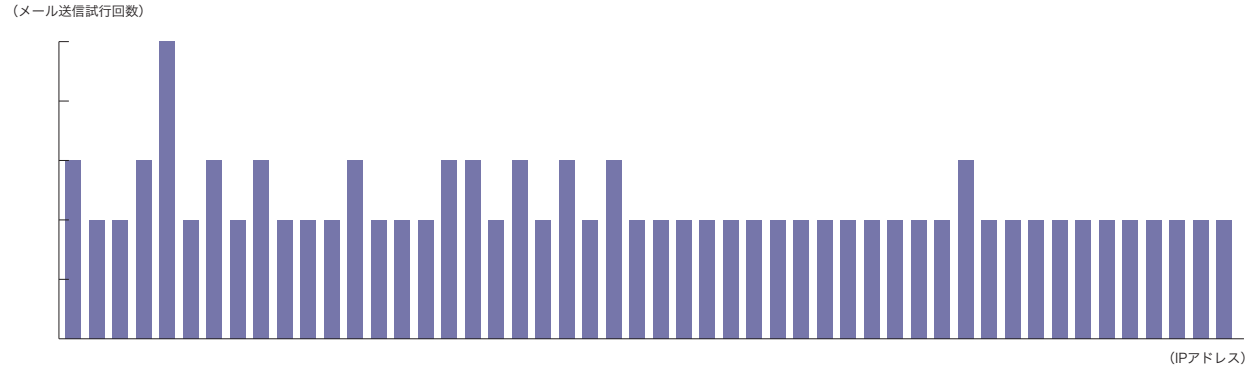

図-5 アクセス元IPアドレスあたりのメール送信試行回数

執筆者：

渡辺 崇文（わたなべ たかふみ）
IIJ プロダクト本部 プロダクト開発部 メッセージングサービス課。2009年入社。IIJメールサービスの開発に従事。M^{3}AAWGメンバー。