

分析レポート

平成 20 年 2 月 29 日
警 察 庁

プロキシサービスを悪用した メール等の不正中継行為の情勢について

1 はじめに

通信の高速化や安全性の強化等を目的として利用されるサービスとして、「プロキシ」というサービスがある。プロキシサービスは、ユーザからのリクエストを受けて、代理で相手のホストにアクセスを行い、返された結果をユーザに返すものである(図1)。プロキシを利用することで、ネットワークに出入りするアクセスを一元管理し、内部から特定のサービスのみを許可し、外部からの不正なアクセスを遮断することができる。その他、プロキシでトラフィックをキャッシュすることで、アクセスの高速化を行なうことができる。

プロキシサービスは、内部ネットワークの代理接続要求を受け付けるものが一般的であるが、設定の不備等により外部ネットワークの第三者からの代理接続要求を受け付けるものもあり、オープンプロキシと呼ばれる(図2)。オープンプロキシは、外部ネットワークの第三者に悪用された場合、悪用した者の発信元を秘匿できるため、迷惑メール送信等、サイバー攻撃の踏み台として利用される可能性がある。

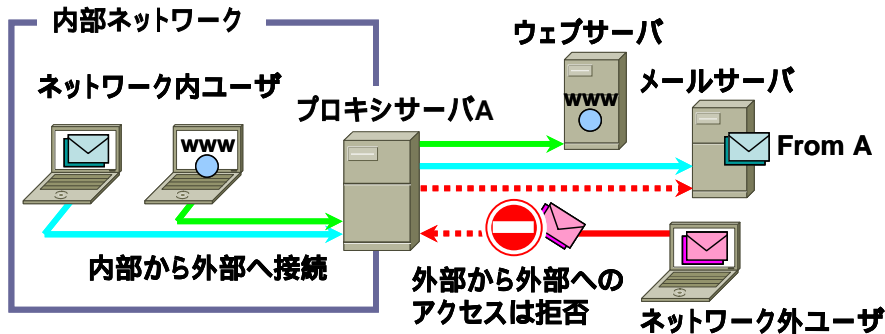


図1 一般的なプロキシサービス

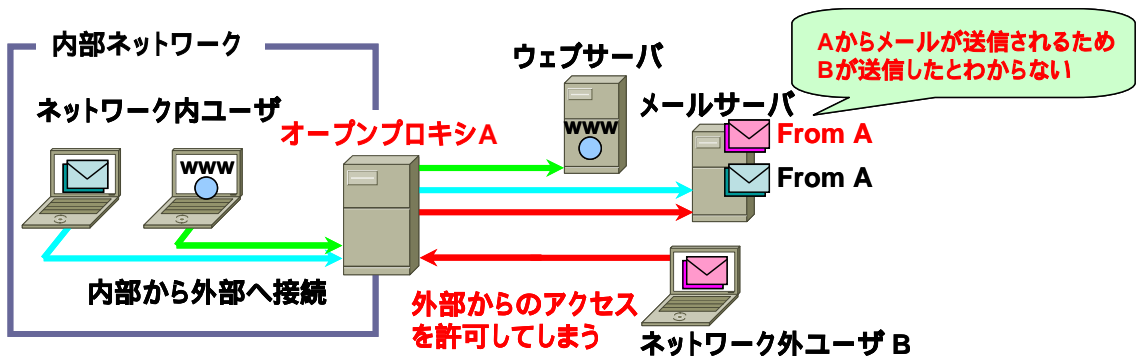


図2 オープンプロキシ

警察庁サイバーフォースセンターでは、プロキシサービスで利用されることが多い、1080/TCP、3128/TCP 及び 8080/TCP¹ の各ポートに対するアクセスを認知している。そこで、オープンプロキシへの接続状況についてより詳細に調査するため、インターネット上に観測環境を構築²して観測を行った。その結果、オープンプロキシに対して中継を試みるアクセスを多数検出した。これらのアクセスのうち、メールの不正中継を試みるものが多数存在したため、さらにメールの不正中継を観測する環境を構築³して観測を行った。

観測結果より、オープンプロキシの探索行為やオープンプロキシ経由による迷惑メール送信を確認することができた。1台のオープンプロキシに対して1日あたり2,355通のメールの不正中継試行を確認しており、オープンプロキシは迷惑メールの発信元の一つになっていると考えられる。

¹ 1080/TCP は Socks サービス、3128/TCP 及び 8080/TCP は HTTP プロキシサービスで利用される場合が多い。

² 外部ネットワークへの中継を実際には行わない。

³ 外部ネットワークへのメールの送信を実際には行わない。

2 オープンプロキシへのアクセス状況

警察庁サイバーフォースセンターでは、プロキシサービスで一般的に利用されている1080/TCP、3128/TCP 及び 8080/TCP に対するアクセスを定常的に観測している。これらの実態を調査するために、観測環境を構築し、接続状況を観測した。

(1) 観測環境

プロキシサービスに対する接続状況を観測する環境の概要は表1のとおり。観測期間は、2006年9月からの約16か月間である。

表1 オープンプロキシ観測環境の概要

<ul style="list-style-type: none">・プロキシサービス用サーバ：3台・プロキシサービス用グローバルIPアドレス：日本国内の連続する3つ・公開するサービスポート番号：1080/TCP、3128/TCP、8080/TCP
--

この観測環境では、オープンプロキシに接続した発信元IPアドレスとポート番号、中継先のIPアドレスとポート番号を記録する(図3)。ただし、悪用を防ぐため、中継先への接続を許可していない。

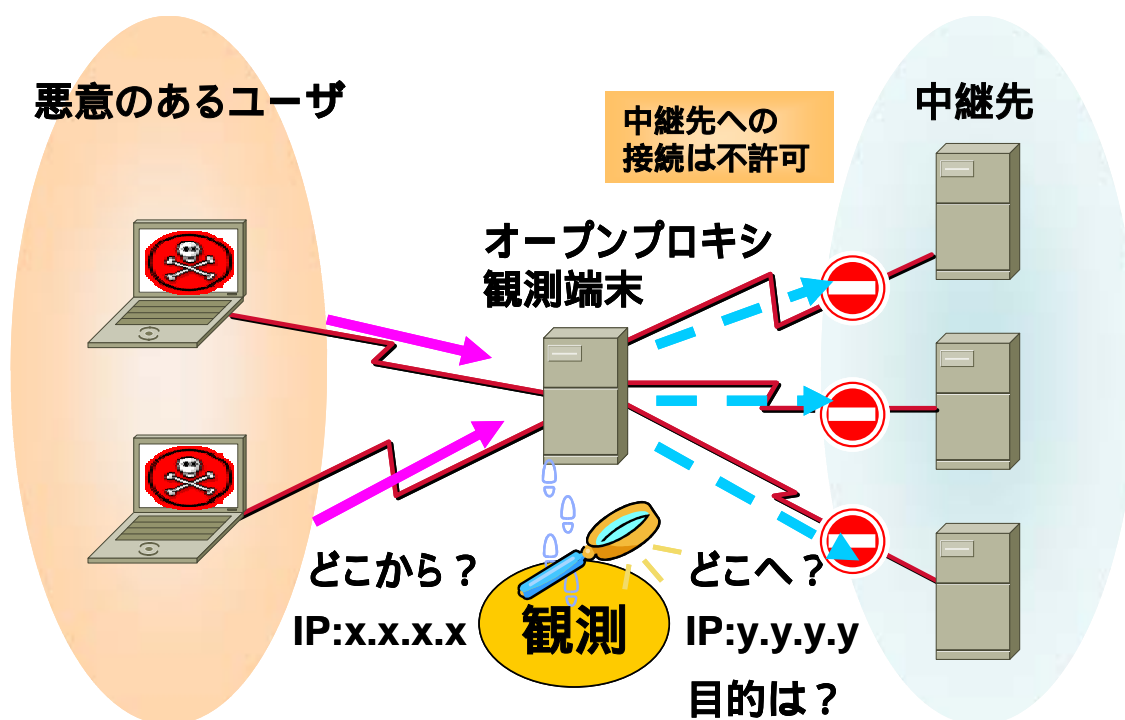


図3 オープンプロキシ観測環境

(2) アクセス状況

オーブンプロキシに対するアクセスをポート別に分類したものを図4に、オーブンプロキシを経由する中継先をポート別に分類したものを図5(a)に示す。オーブンプロキシに対する中継試行は、24の国/地域、合計413のIPアドレスから行われ、アクセスされた総数は、1サーバにつき2,087件、1日あたり平均4.3件であった。各ポートに対するアクセス状況は8080/TCP(18.4%)、3128/TCP(11.6%)、1080/TCP(70.0%)であった。

8080/TCPに対するアクセス(図5(b))は、1サーバにつき385件、1日あたり0.79件であり、そのうちWebのアクセス要求試行⁴を示すものが47.4%、続いてメールの不正中継試行⁵を示すものが39.8%であった。

3128/TCPに対するアクセス(図5(c))は、1サーバにつき243件、1日あたり0.50件であり、そのうちメールの不正中継試行⁵を示すものが46.3%、続いてWebのアクセス要求試行⁴を示すものが40.2%であった。

1080/TCPに対するアクセス(図5(d))は、1サーバにつき1,459件、1日あたり3.0件であった。そのうちの96.0%は脆弱性を突く攻撃と考えられるものであった。

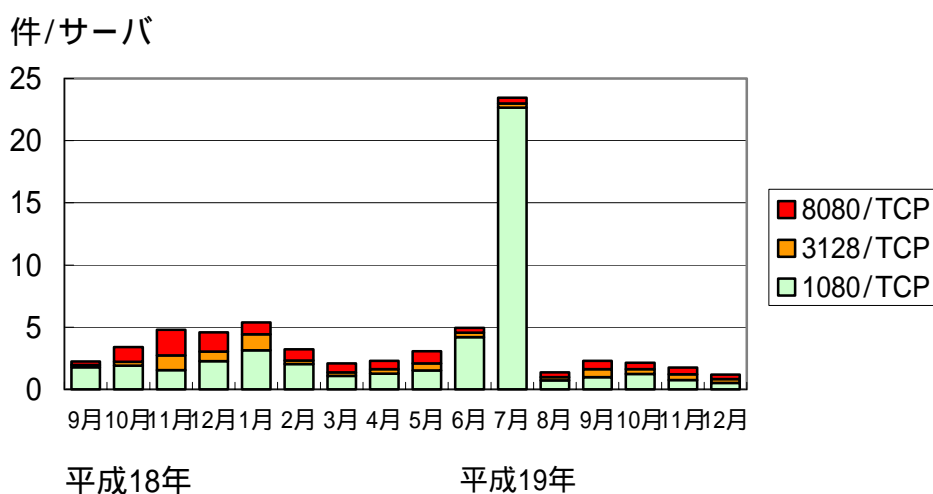


図4 オーブンプロキシに対するアクセス状況
(待ち受けポート別の推移)
(1サーバ1日あたりの件数)

⁴ Webのアクセス要求試行：80/TCPを中継先ポートとするものを観測。

⁵ メール不正中継試行：25/TCPを中継先ポートとするものを観測。

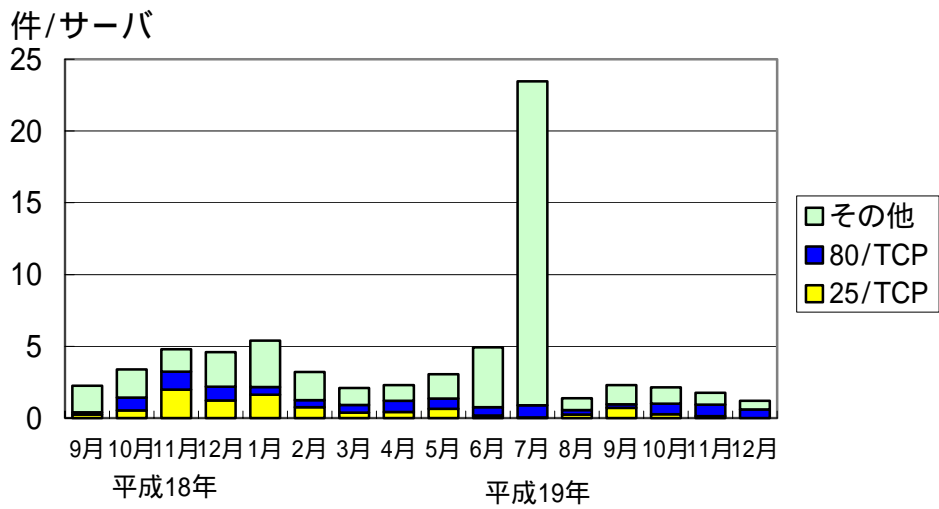


図 5 (a) オープンプロキシに対するアクセス状況
(中継先ポート別の推移)
(1 サーバ 1 日あたりの件数)

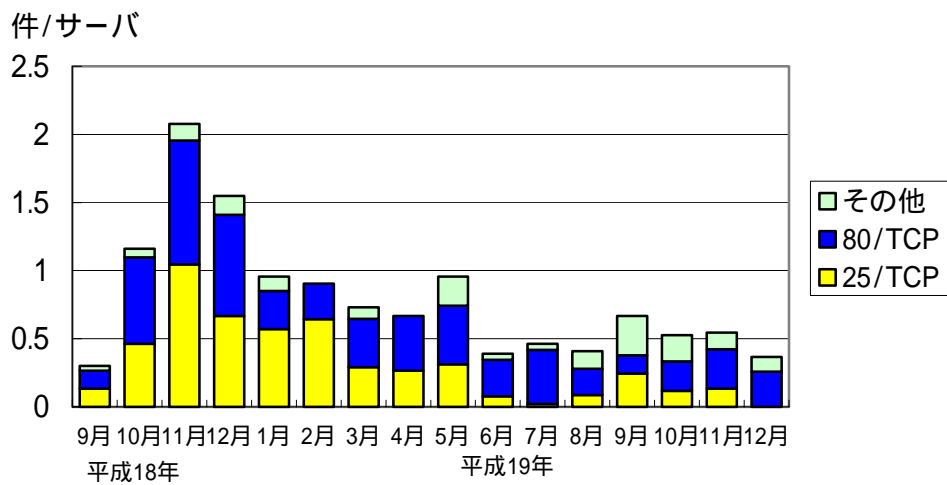


図 5 (b) 8080/TCP へのオープンプロキシに対するアクセス状況
(1 サーバ 1 日あたりの件数)

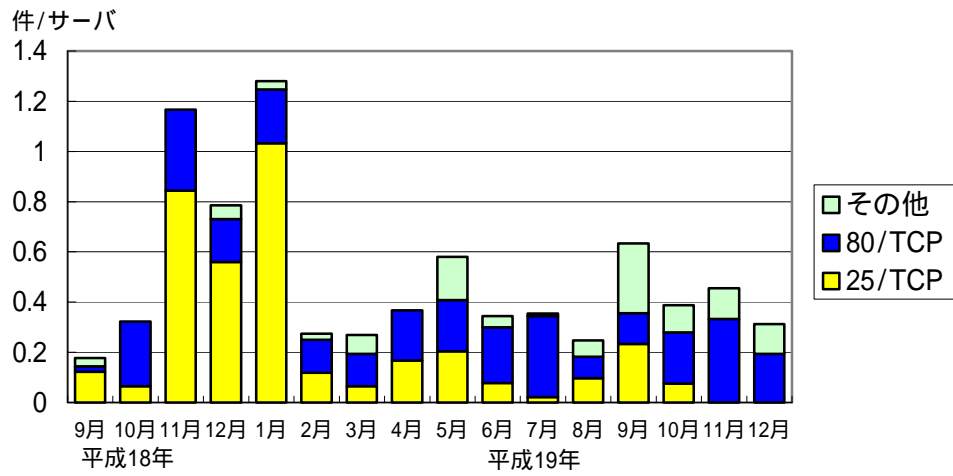


図 5 (c) 3128/TCP へのオーブンプロキシに対するアクセス状況
(1 サーバ 1 日あたりの件数)

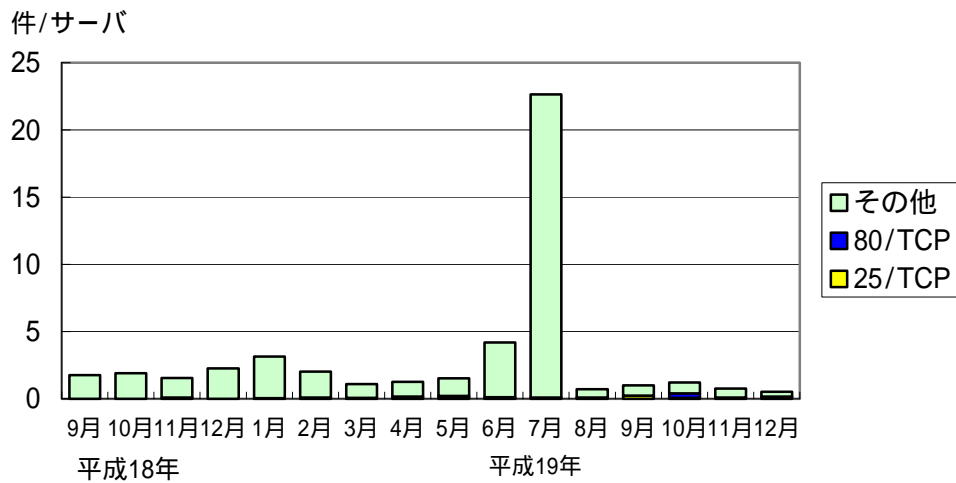


図 5 (d) 1080/TCP へのオーブンプロキシに対するアクセス状況
(1 サーバ 1 日あたりの件数)

オーブンプロキシにアクセスした発信元の国/地域別比率を図6に示す。米国及び台湾からのアクセスが全体の約70%を占めた。また、発信元IPアドレスの逆引き結果によると、一般利用者回線と推測されるものが多い。

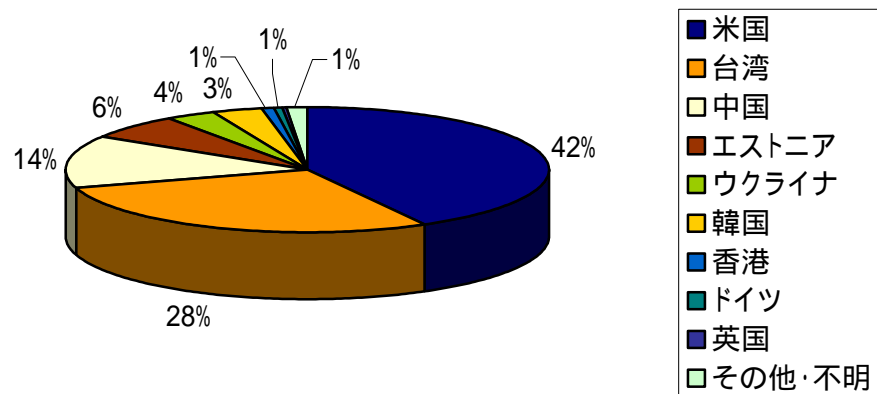


図6 オーブンプロキシにアクセスした発信元の国/地域別比率

メールの不正中継試行⁵による中継先の国/地域別比率を図7に示す。台湾、米国を中継先とするアクセスが多い。これらのアクセスの中には、メールの不正中継試行が可能なオーブンプロキシの探索行為を行なっているものが含まれると考えられる。

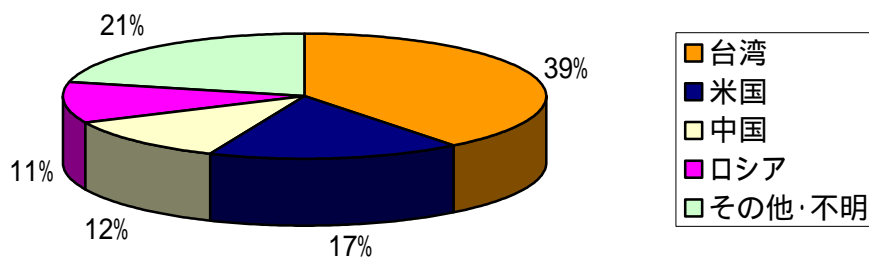


図7 オーブンプロキシに対するメールの不正中継先の国/地域別比率

Web のアクセス要求試行⁴による中継先の国 / 地域別比率を図 8 に示す。米国、中国を中継先とするアクセスが多い。

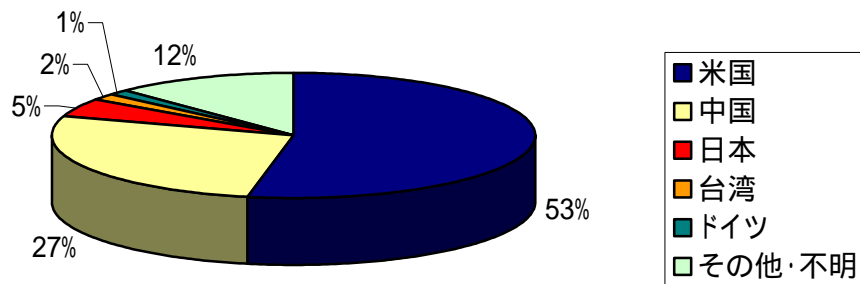


図 8 オープンプロキシに対する Web のアクセス要求試行先の国 / 地域別比率

(参考) メールサーバ(25/TCP)に対するメールの不正中継試行について

メールの送受信に利用されるポート(25/TCP)に対するアクセス状況について、オープンプロキシ観測環境を使用して調査した。⁶

メールサーバに対するメールの不正中継試行は、9の国/地域、合計282のIPアドレスから行われ、アクセスされた総数は、1サーバあたり395件、1日あたり平均0.81件であった(図9)。

メールサーバに対するメールの不正中継試行は、オープンプロキシに対するアクセス状況と同様に台湾からのアクセスが最も多く、約63%を占めている(図10)。

この状況から、外部からのメールを中継するよう設定されているメールサーバを探索する行為も少なからず存在することが窺える。

件/サーバ

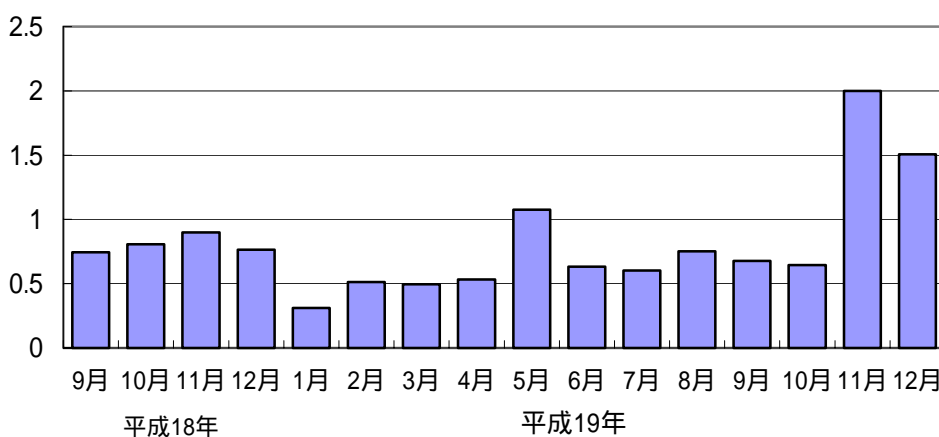


図9 メールサーバに対するメールの不正中継試行の状況
(1サーバ1日あたりの件数)

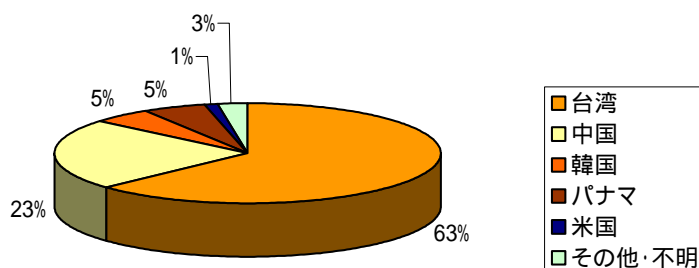


図10 メール不正中継を試行した発信元国/地域別比率

⁶使用しているIPアドレスについては、メールの送受信サービスは行っておらず、また、DNSにもメールに関するレコードは登録されていない。

3 オープンプロキシを経由するメールの不正中継

(1) 観測環境

前章において、オープンプロキシに対するメールの不正中継試行が多いことを述べた。そこで、別途オープンプロキシを不正中継するメールの観測環境を構築し、調査を行った。この観測環境ではオープンプロキシの探索行為と考えられる特殊な形式のメール(4(1)で詳述)にのみ応答し、その他のメールの送信は模倣するだけで、メールの中継は行わなかった(図 11)。観測環境の概要は表 2 のとおりである。観測期間は、2007 年 11 月からの 1 か月間である。

表 2 オープンプロキシを不正中継するメールの観測環境の概要

- | |
|---|
| <ul style="list-style-type: none">・プロキシサービス用サーバ：1 台・プロキシサービス用グローバル IP アドレス：日本国内の 1 つ・公開するサービスポート番号：8080/TCP |
|---|

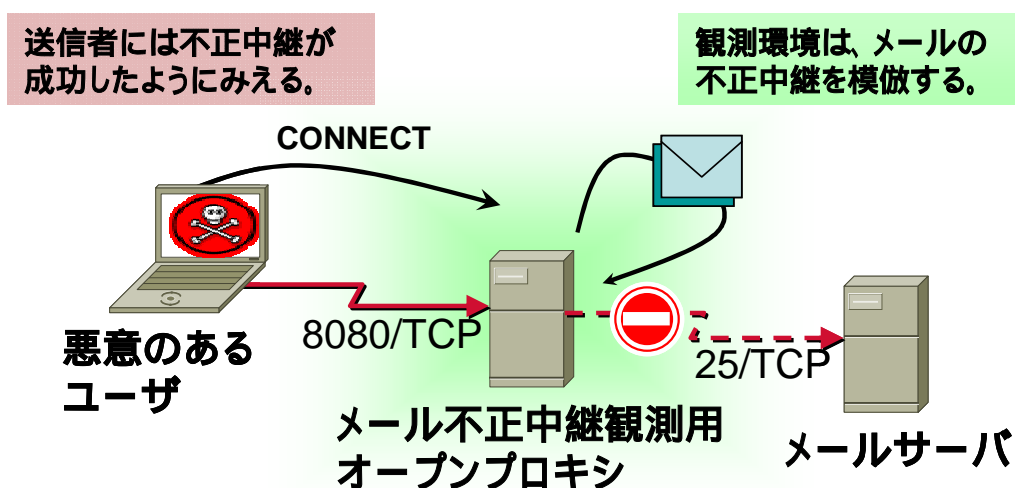


図 11 オープンプロキシを不正中継するメールの観測環境

(2) アクセス状況

受信したメールは全てメールの不正中継試行を意図したものであり、受信したメールの総数は70,661件、1日あたりの平均は、約2,355件、1日あたりの最大件数は14,430件であった(図12)。その他、オーブンプロキシの探索行為(後述)に使用していると考えられるメールも含まれていた。

受信したメールの中には、中継先メールサーバと宛先メールアドレスの受信サーバが異なるものがあった。これは、中継先メールサーバがオープンリレーメールサーバである可能性を示している。

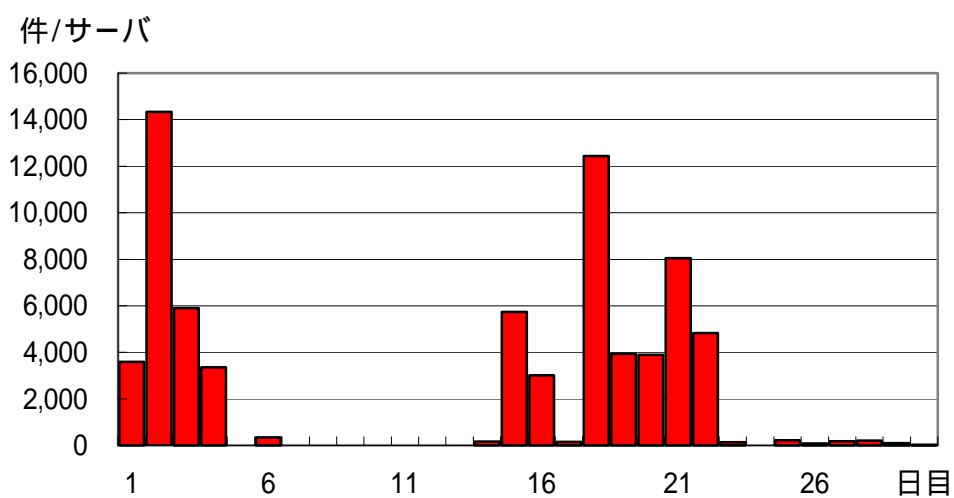


図12 オープンプロキシを不正中継するメールの受信状況
(1サーバ1日あたりの件数)

4 考察

(1) オープンプロキシの探索行為

オープンプロキシに対する接続状況を分析したところ、メールの件名に「xxx.xxx.xxx.xxx:8080」といったような内容を含むメールを多数確認した。この「xxx.xxx.xxx.xxx」は観測環境のグローバル IP アドレスであり、「8080」はオープンプロキシをサービスしているポート番号である。このようなメールの中継要求に 응답したところ、しばらくして大量の迷惑メールの不正中継試行⁷があった。したがって、このようなメールはメールの不正中継が可能なオープンプロキシの探索行為に使用されているものと考えられる。メールの不正中継が可能なオープンプロキシの探索行為の概要は以下のとおりである(図 13)。

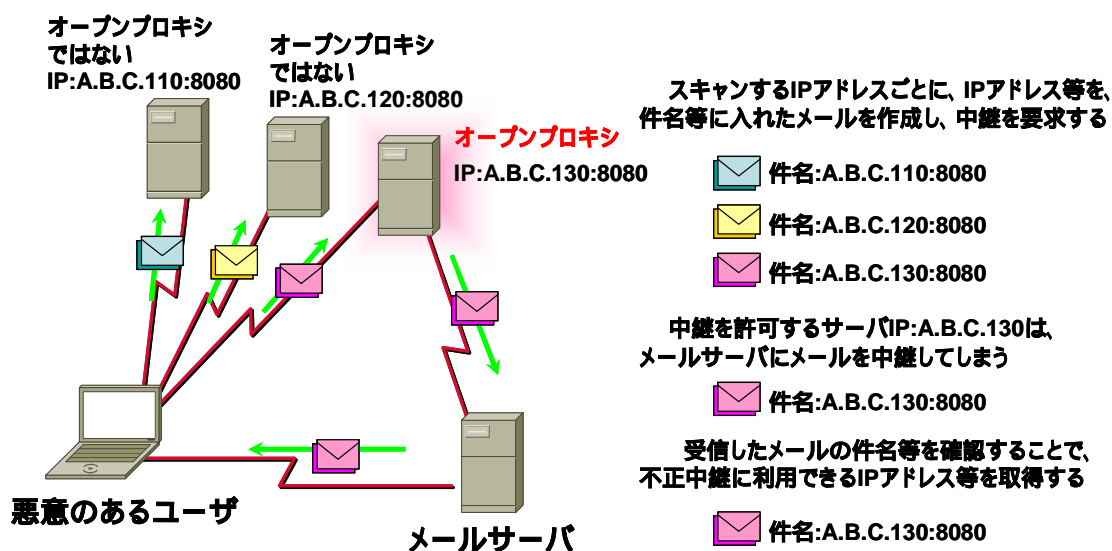


図 13 メール不正中継が可能なオープンプロキシの探索行為

オープンプロキシを探している悪意のあるユーザは、メールの件名に探索対象の IP アドレス及びポート番号を記載し、インターネット上の任意の端末に対して、メールの不正中継を試みる(図 13 中)。メールの宛先は悪意のある利用者が使用しているメールアドレスと考えられる。メールの不正中継が可能(図 13 中)ならば、このメールアドレス宛てに不正中継を試みた端末の IP アドレス及びポート番号を記載したメールが届く(図 13 中)。この結果、メールの不正中継が可能なオープンプロキシを知ることができる。悪意のあるユーザは、このような手法を使用することによって、メールの不正中継が可能なオープンプロキシを探しリスト化しているものと考えられる。

⁷ オープンプロキシに対して 1 日当たり 2,355 件のメールの不正中継試行があった。

オープンプロキシを経由して迷惑メール送信が行なわれた場合、被害者が利用しているメールサーバにはメールの不正中継が行われたオープンプロキシの IP アドレスが記録されるため、メールの発信者を特定することが困難になる(図 14)。

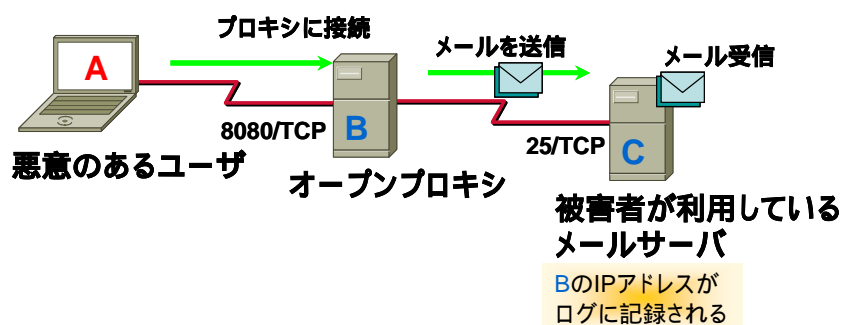


図 14 オープンプロキシを経由する迷惑メール送信

(2) オープンプロキシとオープンリレーメールサーバ

観測環境で確認したメールの中に、中継先メールサーバと宛先メールアドレスの受信サーバが異なるメールが存在した。中継先がオープンリレーメールサーバである場合、メールの不正中継が多段となり、メールの発信者の特定がさらに困難になる(図 15)。

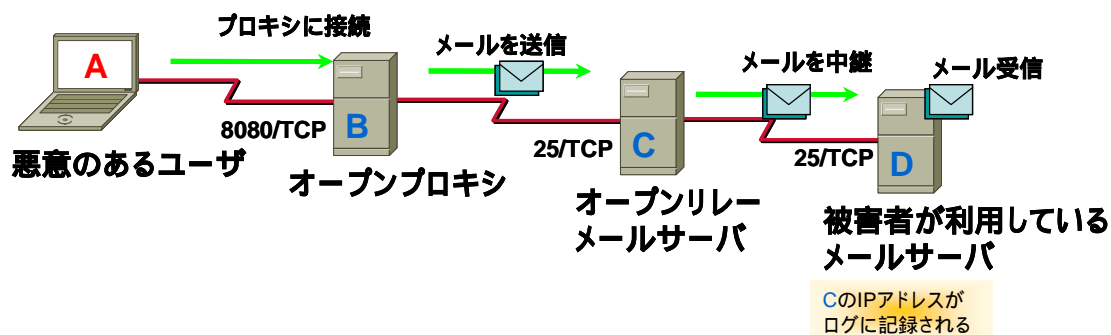


図 15 オープンプロキシとオープンリレーメールサーバを併用した迷惑メール送信

(3) 不正プログラムとメールの不正中継

メールの不正中継試行を行う発信元 IP アドレスの逆引き結果によると、一般利用者回線と考えられるものが少なからず存在した。これらの中には、一般の利用者のコンピュータでは通常立ち上がっていないサービスが提供されていると懸念されるものも見受けられ、ボットプログラムをはじめとした不正プログラム等の感染により、そのようなサービスが提供されている可能性も否定できないところであった。また、オープンプロキシの中継先がオープンリレーメールサーバとなっているメールサーバを複数確認した。以上の状況から、迷惑メールを送信するにあたって、その中継等を行うコンピュータを複数介することにより、発信元の特定を困難にし、全容の解明を煩雑にするような複雑なメール送信システムを構築しているユーザが存在する可能性を否定できない(図 16)。

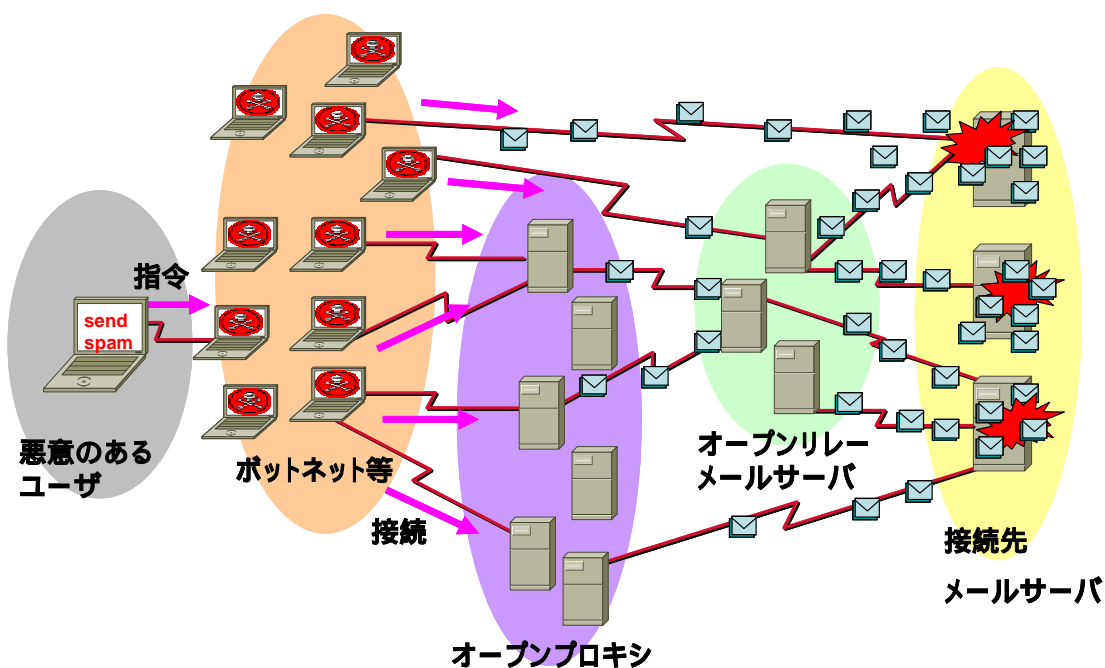


図 16 オープンプロキシとオープンリレーメールサーバを併用した迷惑メール送信システム

5 対策

今回、調査対象としたオープンプロキシは、以下の対策をとることで防ぐことができる。

(1) システム環境設定の見直し

プロキシサービスが不要な場合は、サービスを停止する。プロキシサービスを使用する場合は、第三者にプロキシサービスを悪用されないように適切なアクセス制御を行う。

(2) 修正プログラム等の適用

セキュリティの脆弱性のため、ネットワークに接続可能な家電製品や、一部のアプリケーションソフトウェア等が、オープンプロキシとして機能する事例がある。これらの脆弱性を修正するためには、修正プログラム等を適用する必要がある。

また、PC 等がコンピュータウイルスやボットプログラム等に感染することで、意図せずオープンプロキシとして機能する場合もあり、一般的な情報セキュリティ対策が必要である。

6 まとめ

今回、オープンプロキシに対するアクセス状況、オープンプロキシの利用実態について調査を行うため、環境を構築して観測を行った。観測結果より、オープンプロキシを利用する迷惑メールを多数確認することができた。

オープンプロキシは、プロキシサーバの設定の不備のみならず、ソフトウェアの脆弱性、運用者の瑕疵等に起因したボット等の不正プログラムへの感染や不正なアクセス行為によって構築されてしまう可能性があるため、基本的な情報セキュリティ対策の確認が必須である。

また、迷惑メール対策として、近年、電気通信事業者等が実施している OP25B⁸ は、オープンプロキシを利用する迷惑メール対策の一つとして有効であることから、電気通信事業者等の提供するセキュリティサービスの一つとして、一般の利用者の方にも着目してもらいたい。

サイバーフォースセンターでは今後とも情報セキュリティ対策等に資する情報があれば、警察庁セキュリティポータルサイト@police「インターネット治安情勢」を通じて情報の提供を行なう予定である。

⁸ OP25B(Outbound Port 25 Blocking)とは、ポート 25/TCP を塞ぐことで外部ネットワークへの直接メール送信を防ぐ方式のこと。メールを送信する場合、プロバイダのメールサーバを経由する必要がある。