

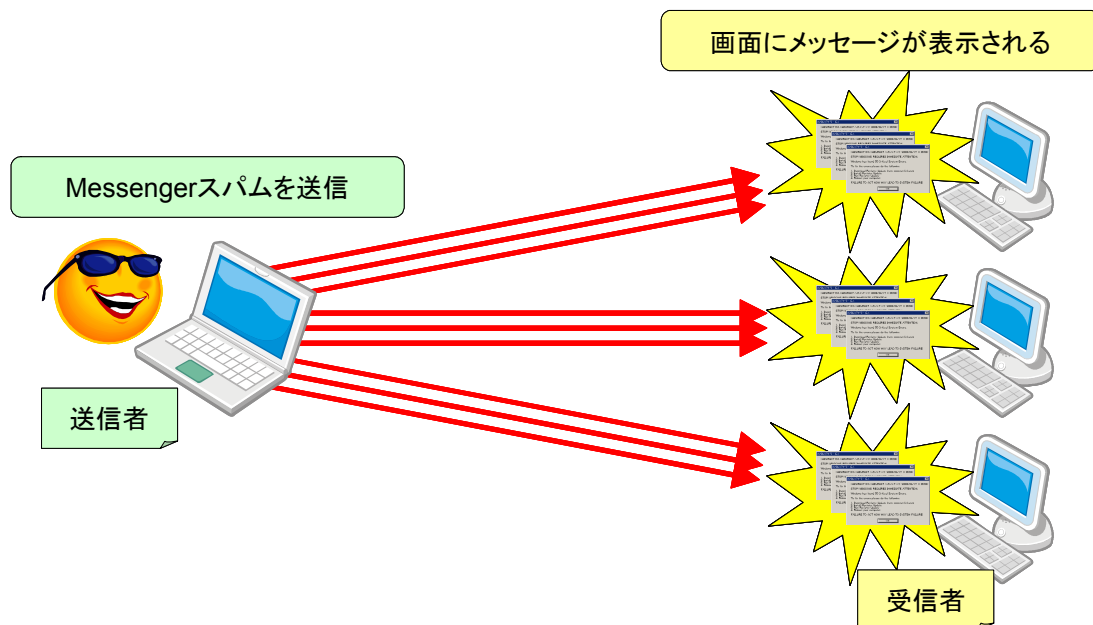
Messenger スパムの情勢について

1 はじめに

Messenger スпамとは、マイクロソフト社の Windows 上で動作する Messenger サービスを利用したスパムである。

警察庁のインターネット定点観測¹では、Messenger サービスで利用される 1026/UDP 及び 1027/UDP に対するアクセスを 2004 年から継続的に検知している²。これらのアクセスは、大半が Messenger スпамであり、2007 年 12 月頃から検知件数が増加しているため、Messenger スпамについて現状を調査した結果、次のことが判明した。

- ユーザをだまし、悪意のあるソフトウェアをインストールさせようとする Messenger スпамが存在
- Messenger スパムの受信頻度は、最大で 5 分に 1 回
- 1026/UDP 及び 1027/UDP 以外のポートへのアクセスを行う Messenger スпамが存在



¹ インターネット定点観測 : <http://www.cyberpolice.go.jp/detect/observation.html>

² 「UDP1026, 1027 番ポートに対するトラフィックの増加について」

http://www.cyberpolice.go.jp/important/2004/20040603_113507.html

2 Messenger サービスと Messenger スпам

(1) Messenger サービスとは

Messenger サービスとは、マイクロソフト社の Windows 上で動作するサービスの一つで、ネットワーク経由で簡単なメッセージをやり取りすることができる。

Windows のコマンドプロンプトから

```
net send <送信先の IP アドレス> <メッセージ内容>
```

と入力することで、メッセージが送信され、それを Messenger サービスが有効なコンピュータが受信した場合、図 1 のようなポップアップメッセージが表示される。

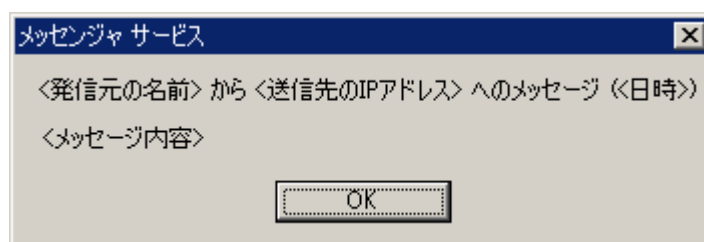


図 1 Messenger サービスで表示されるメッセージの例

(2) Messenger サービスの標準設定

Windows NT、Windows 2000 及び Windows XP SP1 の初期設定では、Messenger サービスは自動的に開始される。Windows XP SP2 以降では、Messenger サービスは無効に設定されている。Messenger サービスが無効に設定されている場合は、メッセージの送受信を行うことはできない。

(3) Messenger スпамとは

Messenger サービスの機能を利用してコンピュータの画面上に迷惑メッセージを表示させるものを、以降「Messenger スпам」と呼ぶ。

警察庁で観測した代表的な Messenger スпамを図 2 に示す。この Messenger スпамには、「Windows に深刻なシステムエラーが発生した。エラーを修復するためには、www.〇〇〇〇.com からプログラムをダウンロードして実行すること。この作業を行わない場合は、システム障害が発生する可能性がある。」と、英文で記述されている。

なお、図 2 の Messenger スпамは悪意のあるソフトウェアをインストールさせようとしているものである。この種のメッセージには十分に注意が必要である。



図 2 代表的な Messenger スпамの内容

(4) Messenger サービスに関する脆弱性

2003 年 10 月にマイクロソフト社から「メッセンジャ サービスのバッファ オーバーランにより、コードが実行される (828035) (MS03-043)」が発表されている³。Messenger サービスを使用する場合は、マイクロソフト社のサイトから適切なパッチをダウンロードし、適用する等の対策が必要である。

³ 「メッセンジャ サービスのバッファ オーバーランにより、コードが実行される (828035) (MS03-043)」
<http://www.microsoft.com/japan/technet/security/bulletin/MS03-043.aspx>

3 観測結果

(1) Messenger スパムのアクセス状況

Messenger スпамが主に利用する 1026/UDP 及び 1027/UDP について、警察庁のインターネット定点観測における検知状況は、以下のとおりである。

表1 Messenger スパムの観測条件

観測場所	： 全国の警察施設のインターネット接続点
送信先ポート	： 1026/UDP 及び 1027/UDP
観測期間	： 2005年1月1日から2008年3月31日

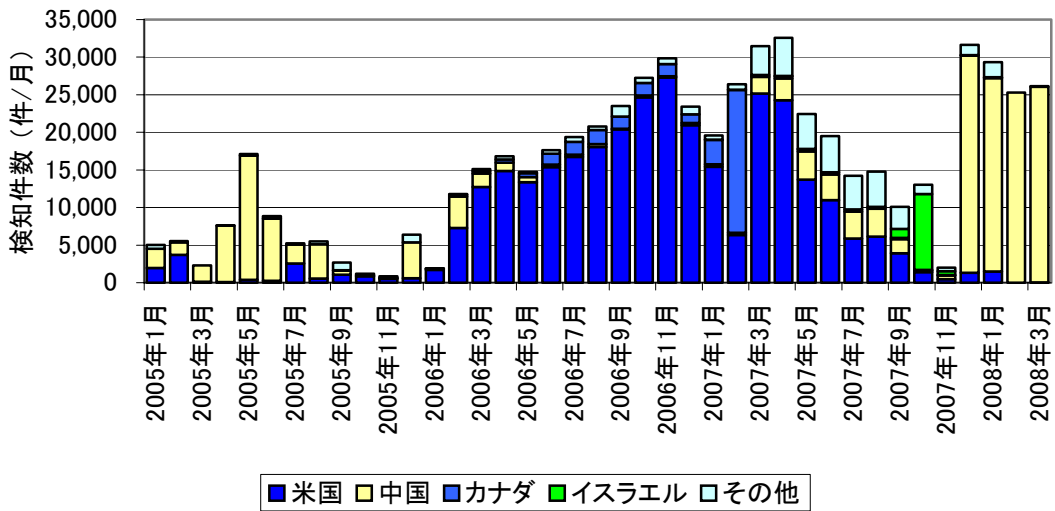


図3 1026/UDP での検知件数の推移

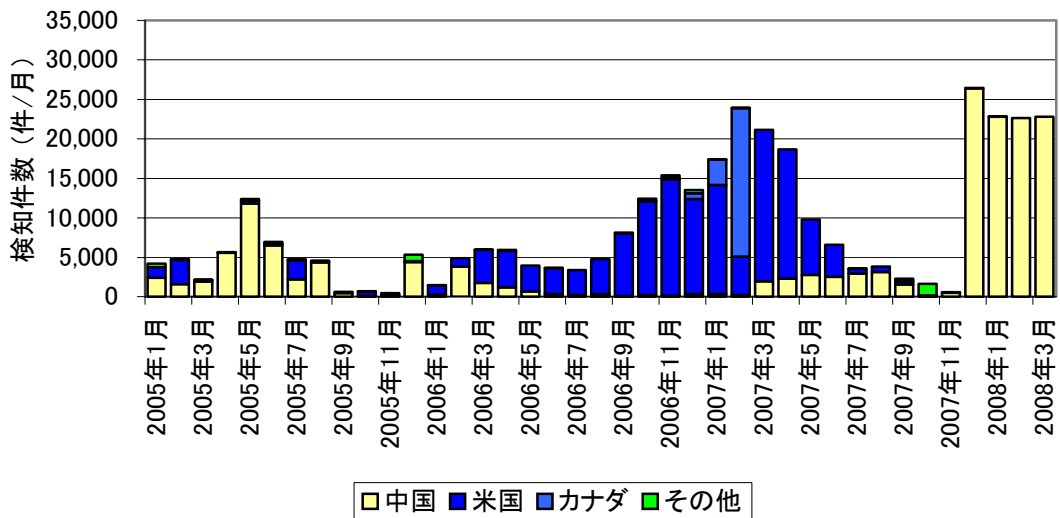


図4 1027/UDP での検知件数の推移

2005年4月から2005年7月の間は、検知した多くのアクセス発信元IPアドレスは中国に割り当てられているものであった。その後、2006年1月から2007年9月の間は、発信元の多くが米国となっており、カナダを発信元とするものも含まれている。また、わずかではあるが、日本を発信元とするものも確認された。2007年12月以降は、中国を発信元とするものが大半を占めている。

一般に、Messenger スпамは、UDP プロトコルを使用しているため、「発信元 IP アドレスを詐称しやすいこと」が知られている。2006年2月から2007年5月にかけて、カナダから発信された Messenger スпамについては、発信元を詐称されている可能性が高い。これについては、4 (2) 「Messenger スпамの発信元 IP アドレス詐称の可能性」で述べる。

1027/UDP の状況は、1026/UDP と概ね同じである。(図 4)

これら 1026/UDP 又は 1027/UDP にアクセスを行う Messenger スпамについては、最も多いとき、5分に1回の間隔で観測された。

(2) 1026/UDP、1027/UDP 以外に対する Messenger スпам

警察庁のインターネット定点観測では、1026/UDP 及び 1027/UDP 以外にも Messenger スпамと思われるアクセスを検知している。そこで、1026/UDP、1027/UDP を含め、すべての UDP ポートから Messenger スпамを抽出した。(図 5)

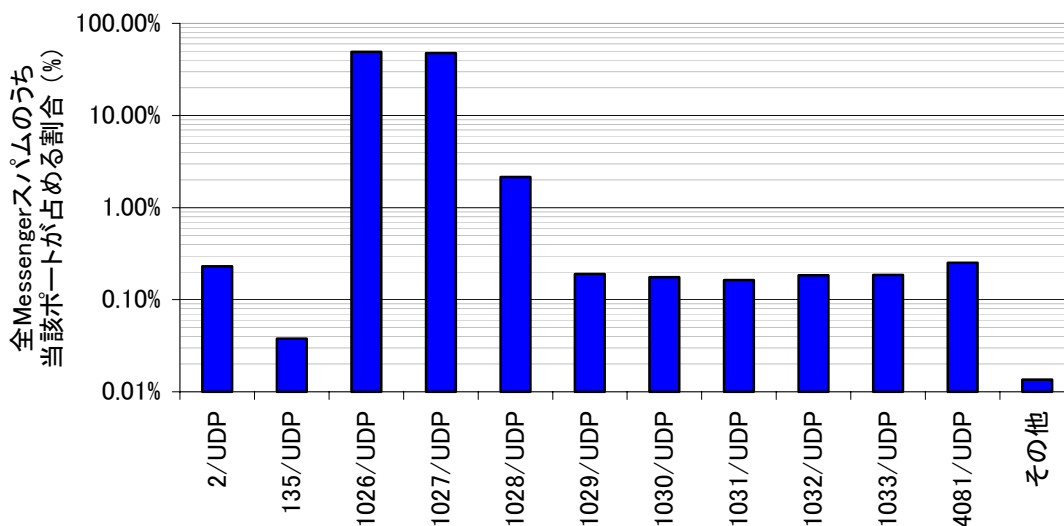


図 5 Messenger スпамで使用された送信先ポート一覧

1026/UDP 及び 1027/UDP が大半 (約 96%) を占めた。一方で、同じく Messenger サービスで使用されている 135/UDP や、1024 番よりも大きな UDP の一時ポート等に対してアクセスを行う Messenger スпамの存在も確認された。

(3) Messenger スパムの内容

警察庁で観測した Messenger スпамについては、そのほとんどが英語で記述されていたが、わずかに中国語で記述されたものも確認できた。日本語で記述された Messenger スпамは確認できなかった。また、その内容の多くが、プログラムのダウンロードとインストールを促す内容のものであった。

(4) Messenger スпамに記述された URL

上記のとおり、観測した Messenger スпамの大半は、メッセージ本文にホスト名（ドメイン名）が記述されており、プログラムのダウンロードを促すものとなっている。

そこで、これらのホストにアクセスしたところ、現在は Web ページが存在しないものが大半であったが、「OS のエラーを修復するプログラム」と称するソフトウェアをダウンロードできるホストがあることを確認した。

今回ダウンロードできたソフトウェアは、すべて、OS にセキュリティ上の問題がないにも関わらず、「OS に〇件の問題が見つかりました。」等と虚偽のメッセージを表示し、セキュリティソフトと称するものを購入させようとする、悪意のあるソフトウェアであった。

4 考察

(1) 1026/UDP 及び 1027/UDP に対する Messenger スпам検知件数

1026/UDP と 1027/UDP の検知件数を比較したところ、米国及びイスラエルを発信元とする Messenger スпамは、1026/UDP のみに送信しているケースが見られるものの、全体的には 1026/UDP と 1027/UDP の検知件数が、ほぼ同様の結果になることを確認した。

特に、中国を発信元とする Messenger スпамについて、発信元 IP アドレスを調査したところ、同じ IP アドレスから、1026/UDP 及び 1027/UDP に対して、同じ内容の Messenger スпамを同程度、送信していることを確認した。(図 6) これは、1026/UDP と 1027/UDP の両ポートに対し、Messenger スпамを送信するようプログラムされたツールやボットネット等の利用が考えられる。

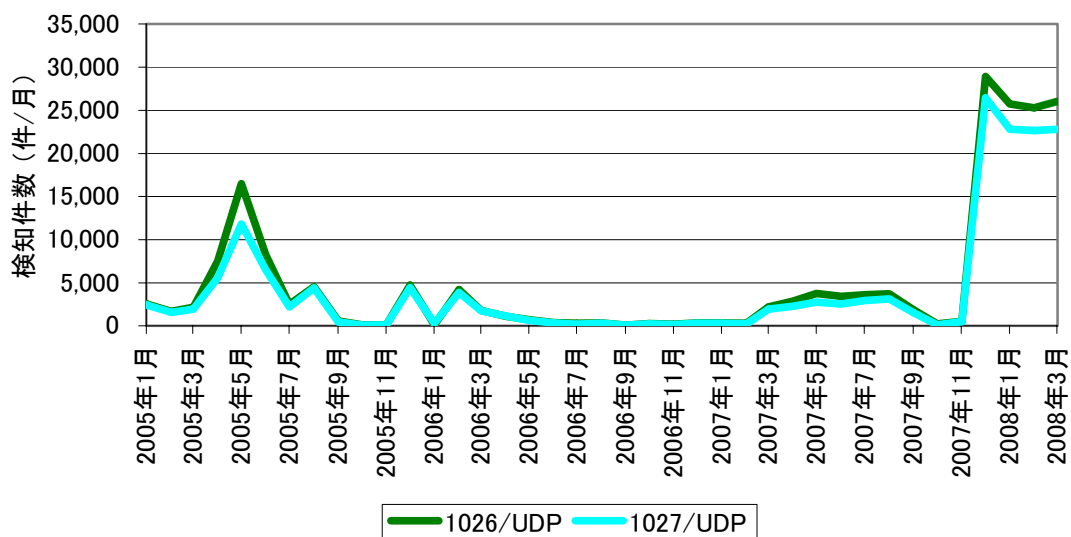


図 6 中国を発信元とする Messenger スпамの件数の推移

(2) Messenger スパムの発信元 IP アドレス詐称の可能性

Messenger スパムの通信で使用されている UDP プロトコルは、発信元の IP アドレスを簡単に詐称することが可能である。

3 (1) 「Messenger スパムのアクセス状況」の観測において、発信元 IP アドレスの検知件数を調査したところ、カナダに割り当てられた IP アドレスでは、1IP 当たり 1.2 件、米国の一部では、1IP 当たり 2~16 件であった。

それに対し、中国を発信元とする Messenger スパムは、1IP 当たり 1,510 件であり、顕著な違いがあることが判明した。

カナダや米国の一部のように、IP アドレス数と Messenger スパムの検知件数がほぼ同程度のものについて、発信元 IP アドレスを確認したところ、発信元 IP アドレスは連続したものであった。通常、連続した多くの IP アドレスからアクセスされるという状況は考えにくい。このような発信元 IP アドレスは、詐称されているものと考えられる。

(3) ボットネット等を利用した可能性

観測期間において、1,000 件以上の Messenger スパムを検知した発信元 IP アドレスについて調査した。

このような IP アドレスから送信される Messenger スパムは、一定期間送信された後に停止し、再び別の IP アドレスから一定期間送信される、というパターンを繰り返しており、乗っ取られたサーバやボットネット等を利用して送信されている可能性が考えられる。

それらを利用していると考えられる Messenger スパムについて、国別の割合を示す。

(図 7)

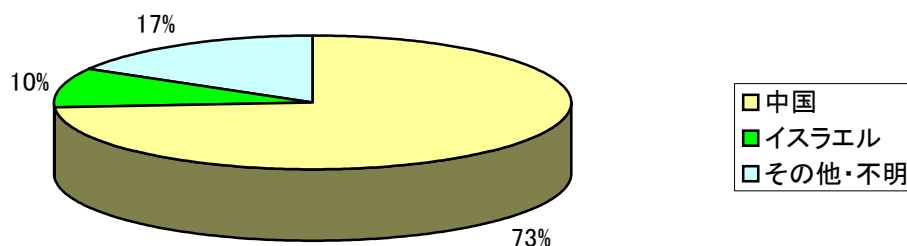


図 7 ボットネット等を利用したと考えられる発信元国別の割合

5 対策

マイクロソフト社は、Messenger スпам対策として、「ルータやファイアウォールにおいて、NetBIOS および UDP ブロードキャストの着信トラフィックをブロックする」ことを挙げている⁴。一般的に

使用しないポートは閉じて、不要な通信を遮断する

ことが、Messenger スпамだけでなく、各種のコンピュータウイルス、ワームへの対策となる。

また、Messenger サービスを使用する必要がある場合には、

Messenger サービスを無効にする

ことも有効な対策である。

Messenger サービスを利用する場合は、Messenger スпамによるメッセージが表示される可能性がある。そのようなメッセージには、図2のように、悪意のあるソフトウェアをインストールさせようとするものが存在するので、その内容をよく確認し、

送信者やアクセス先の URL に不審な点がある場合には、記述されているサイトにアクセスしない

ことは当然として、一部のブラウザやウイルス対策ソフトに搭載されている、悪意のあるサイトを閲覧しようとするすると警告する機能を有効に活用することも肝要である。

6 まとめ

今回、調査した Messenger サービスは、Windows XP SP2 以降では標準で無効になっており、この設定を有効にしない限り、Messenger スпамを受信しない。

しかし、警察庁のインターネット定点観測において、Messenger スпамで主に利用される 1026/UDP、1027/UDP の検知件数は高位で推移しているため、Messenger サービスを利用する際は、十分に注意する必要がある。

警察庁サイバーフォースセンターでは、セキュリティポータルサイト「@police」等を通じて、今後も情報セキュリティ対策などに資する情報の提供を行う予定である。

⁴ 「インターネット広告を含む Messenger サービス ウィンドウが表示される」
<http://support.microsoft.com/kb/330904/ja>