# 自動攻撃型マルウェアによるDDOS攻撃被害の長期間化問題の解析とその対策に関する検討

須藤　年章

NTTコミュニケーションズ株式会社
sudo@mfeed.ad.jp

あらまし　DDoS（分散型サービス拒否）は，ボットネットのように指令サーバーからの命令に従い実行されるものだけではなく指令系統をもたずあらかじめプログラミングされた対象や時間に従って攻撃を実行する自動攻撃型マルウェアによるものなどがある．このようなマルウェアの中には，自己破壊までプログラミングされているものもあるが，感染したまま使い捨てられるようなものも多く，その場合はすべての端末から駆除されないかぎりは攻撃は永久に続くことになる．本稿では，2005年に発生したAntinnyによるDDoS攻撃が5年以上継続している状況を解析するとともに，マルウェア対策の課題について述べる．

# Analysis of prolongment problem of DDoS attack damage with automatic attack type malware and examination of the measures

Toshiaki Sudoh

NTT Communications Corporation
sudo@mfeed.ad.jp

**Abstract** DDoS (distributed denial of service) has neither the one it executed like the botnet according to the instruction from the instruction server nor the instruction system and there are the one with the automatic attack type malware that executes the attack according to the object and time that the programming was done beforehand etc.The attack especially becomes it following permanence as long as in such a malware, there is the one that the programming is done even as for the self-destruction, too and a lot of things that use while infected and are thrown away are not exterminated from all terminals in that case. In this text, the situation in which the DDoS attack by Antinny generated in 2005 has continued for five years or more is analyzed, and the problem of the malware measures is described.

## 1.　はじめに

DDoS（分散型サービス拒否）攻撃は，ボットネットのように指令サーバーからの命令に従い実行されるものだけではなく指令系統をもたずあらかじめプログラミングされた対象や時間に従って攻撃を実行する自動攻撃型マルウェアによるものがある．このようなマルウェアの中には，自己破壊までプログラミングされているものもあるが，感染したまま使い捨てられるようなものも多く，その場合はすべての端末から駆除されないかぎり攻撃は永久に続くことになる．本稿では，2004年に発生し国内30万台弱の端末が感染したといわれるAntinnyによるDDoS攻撃の5年間の状況の変化を解析する．自動攻撃型のマルウェアはその攻撃特性から感染端末の数，影響度の変化を明確に追跡することができるため，攻撃そのものだけではなく，ユーザー環境を取り巻く状況の変化などを含め，多角的に解析することで，一度マルウェアに感染した端末群の数，そこから発生する攻撃がさまざまな要因によりどのように変化していくかを解析し，その影響の継続性，対策の問題点などを考察する．

## 2. P2P ネットワークで流通するマルウェア

最初に P2P アプリケーションの特徴，P2P ネットワークで流通、感染するマルウェアの特徴についてまとめる．

### 2. 1 P2P アプリケーションの利用動向

国内においては 2 バイト文字が利用できることで広く使われるようになった WinMX が 2001 年ごろに，さらに国産で高速なダウンロードが可能な Winny が 2002 年に登場して爆発的に利用されるようになった．その後は 2004 年に登場したさらに高速な Share や海外のアプリケーションも広く使われるようになっている．これらの P2P アプリケーションでは，フリーの OS のイメージファイルの配布など，それまでの ftp や http の代替として効率的なファイル配布に利用されるものもあるが，大半は著作権違反の映像や，ソフトウエアなどが占めている．

### 2. 2 P2P ネットワークで流通するマルウェア

P2P ネットワーク上で流通しているファイルの多くはマルウェアに感染しておりその被害は非常に大きい．利用されているマルウェアは，海外の P2P アプリケーション，国内の P2P アプリケーション毎に細かな特性の違いはあるが，悪意のあるプログラムが大量に流通している．主に日本国内の P2P ネットワークで流通しているマルウェアを分類すると下記のようになる．

(1) システム破壊型
- HDD 消去
- 特定のファイル，ディレクトリ消去

(2) 情報漏えい型
- P2P 放流型
- 掲示板書き込み型
- メールフォーム利用型
- バックドア作成型
- 感染端末のサーバー化

(3) 攻撃型
- 掲示板攻撃型
- DDoS（分散型サービス拒否）攻撃型

(4) ボット化

インターネット上に広く蔓延しているマルウェアとほぼ同じようなカテゴリのマルウェアが存在しているが，P2P アプリケーションの利用者の特性にあわせているのか，一般ではあまり見られない目的をもったマルウェアが多数存在する．図 1 に各種マルウェアの分類と発生時期をまとめる．

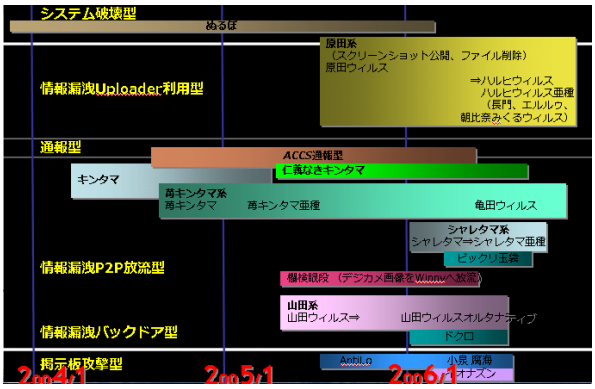


図 1 P2P ネットワーク上のマルウェア

初期は、おもに愉快犯のプログラムが多く，ハードディスクのフォーマットや特定のファイルを消去するシステム破壊型は古くから大量に流通し，今現在も多く存在する．その後，2006 年上旬ごろまでは，様々な形態での情報漏洩，バックドア作成，DDoS 攻撃用などの多種多様なマルウェアが大量に開発され，感染端末に Web サーバーを立ち上げ，スクリーンショットのリアルタイム公開などボットに比べても遜色ない機能をもったものまで登場した．最終的には BBS（掲示板）を CnC（指令サーバー）としたボット化に至った．ただし，これらのマルウェアの開発は 2006 年前半でほぼ終了し，新種，亜種の登場はごくわずかしか発見されておらず，今現在では，この当時のマルウェアがいまだに駆除されないまま流通しつづけている状況である．

### 2. 3 感染手法

P2P アプリケーションで流通しているマルウェアに感染させる手法は主に利用者に実行ファイルを実行させるという単純な手法である．脆弱性の利用，シームレスな感染手法はほとんどなく，その代わり人の操作ミス，判断ミスを誘発させるためのさまざまな工夫が凝らされている．基本的には次のような手法が用いられる．

(1) 拡張子偽装・隠蔽
(2) 流出ファイルに添付
(3) ISO イメージに感染

特に複雑なアーキテクチャは用いられていないが，P2P アプリケーションの利用者の目的，利用者のセキュリティ意識，リテラシなどのさまざまな要因に

より，このような簡単な手法でも有効に機能し感染者の数を増やし続けることが証明された．

## 3. Antinny

本稿ではこれらのマルウェアの中から Antinny と呼ばれるマルウェアの影響に着目して解析する．Antinny は 2004 年 3 月に登場した Winny ネットワーク上で流通するマルウェアである．大量の亜種が存在し，その機能は多岐にわたるが，その中から長期間にわたり影響を与え続けている DDoS 機能について解析する．

### 3. 1 攻撃機能

Antinny の攻撃機能は三種類ある．一つ目の機能を表 1 に示す．この機能が最初に登場した機能であり www.accsjo.or.jp のトップページへのアクセスと投稿フォームへの書き込みを自動的に行う．当初の目的は不正ファイルのやりとりをしていることを通報するという愉快犯的なものであったが，大量の感染端末の発生により 24 時間継続する HTTP Request Flood を発生させた．

**表 1 Antinny の攻撃機能 1**

| | |
|---|---|
| 攻撃開始 | 2004 年 3 月 |
| 攻撃対象 | www.accsjp.or.jp |
| 攻撃日時 | 毎月第一月曜日<br>4～12 月のゾロメの日 |
| 継続時間 | 24 時間継続，または 0:00 に実行 |
| 攻撃内容 | GET / HTTP1.0<br>GET / HTTP1.1<br>PUT / HTTP1.0<br>PUT / HTTP1.1<br>PUT /cgi-bin/form/piracy/webform.cgi HTTP1.0<br>PUT /cgi-bin/form/piracy/webform.cgi HTTP1.1 |

表 2 に Antinny の二つ目の攻撃機能を示す．

**表 2 Antinny の攻撃機能 2**

| | |
|---|---|
| 攻撃開始 | 2005 年 4 月 |
| 攻撃対象 | www2.accsjp.or.jp |
| 攻撃日時 | 毎月第一月曜日 |
| 継続時間 | 24 時間継続，または 0:00 に実行 |
| 攻撃内容 | GET / HTTP1.0<br>GET / HTTP1.1 |

この攻撃はサイトの移動に伴い攻撃対象を変更した亜種によって発生するものである．最初の目的であった投稿フォームへ書き込み機能はなくなり単純に DDoS 攻撃を目的としたものに変化した．

次に表 3 に Antinny の三つ目の攻撃機能を示す．これも DDoS 攻撃の特化したものであるが，攻撃対象には存在する URL だけではなく，存在はしていないが既存の URL に近似した URL が含まれている．これは攻撃対象のサイトが DDoS 攻撃から逃れるために新しい URL に変更した場合を想定してあらかじめ移行可能性のある URL を事前に攻撃対象として組み込んでいると想定される．

**表 3 Antinny の攻撃機能 3**

| | |
|---|---|
| 攻撃開始 | 2005 年 7 月 |
| 攻撃対象 | www3.accsjp.or.jp<br>www0.accsjp.or.jp<br>www1.accsjp.or.jp<br>ww2.accsjp.or.jp<br>ww3.accsjp.or.jp<br>2www.accsjp.or.jp<br>accsjp.or.jp |
| 攻撃日時 | 毎月第一月曜日 |
| 継続時間 | 24 時間，または 0:00 に実行 |
| 攻撃内容 | GET / HTTP1.0<br>GET / HTTP1.1 |

このように Antinny の攻撃機能はあらかじめプログラミングされたとおり毎月決まった日にその日 24 時間だけ継続する HTTP Request Flood である．三種類ある攻撃は攻撃対象サイトの移動への対応および将来的なサイトの移動にも対応したバージョンアップである．またこれらの攻撃の際にはドメインの名前解決も同時に行うため，ISP 等の DNS サーバーへ同時に大量のクエリを送出するという副次的な DDoS 攻撃の効果も発生する．

## 4. 攻撃状況の変化

次に Antinny の実際の攻撃状況の変化についてのべる．攻撃はそれぞれ条件にあった日の 0 時 0 分 0 秒に開始される．攻撃は二種類にわかれこの瞬間のみ攻撃するものと，24 時間継続するものがある．そのため 0 時 0 分が攻撃のピークになる．ここでは，このピークトラフィックの帯域（Mbit/s）とパケット量（Packet/s）のトラフィックに関するグラフと，攻撃に参加した一日あたりのソース IP アドレス数の推移を解析する．

### 4. 1　第一ターゲットへの攻撃

一つ目のターゲットへの攻撃のピークトラフィックの 2005 年 4 月から 2009 年 6 月までの推移を図 2 に示す.

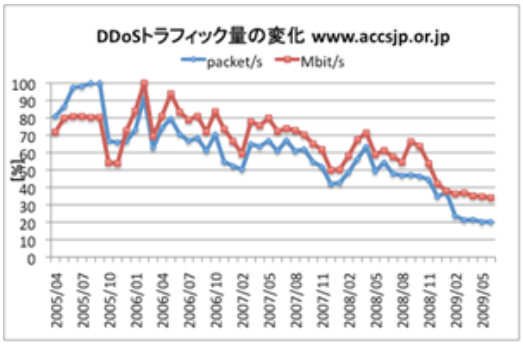


図 2　DDoS トラフィック量の変化 1

トラフィック量は，過去の最大値を 100%とした相対値であらわしている．2005 年前半から 2006 年前半にかけてピークを迎えているが，この時期は報道でもさかんに取り上げられた，感染による個人情報の P2P ネットワークへの漏えい事件が頻発した時期であり，そのタイプのマルウェアが蔓延していた時期に，同時に特定サイトを攻撃するタイプのマルウェアも蔓延していたことを表している．次に図 3 に攻撃に参加したソース IP 数の推移を示す.


図 3　ソース IP アドレス数の推移 1

2005 年 9 月をピークに減少しているが，2006 年 2 月に急増しているのはトラフィック増の原因と同様に新種の発生である．2006 年 8 月に増加が見られ新種の発生が疑われたが，特に原因となる事象はなく原因は不明である.

トラフィック量，ソース IP 数ともに 2005 年 10 月，2006 年 2 月に急激に減少しているのは，Antinny 関連のマルウェアに関して各種ウィルスチェックソフトでの対応が行われた結果である．その前後の状況からもさらなる感染の拡大を防いだ効果はあるように見られるが，撲滅といったレベルには程遠い結果だといえる．この結果は，適切な OS の設定，ウィルスチェクソフトの利用者がこの急増，急減の部分にあたるユーザーへの効果であり，減少にいたらなかったその前後の割合がそれらの対策が適切に行われていないユーザー層の割合を示しているのではないかと想定される.

### 4. 2　第二ターゲットへの攻撃

次に図 4 に二番目のターゲットへの攻撃トラフィックの変化を示す. この攻撃は 2005 年 4 月から開始された攻撃であり，最初は数 Mbps 程度であったが，6 月の攻撃では 17 倍にまで拡大し，半年後の 10 月には 50 倍にまで拡大している. その後は緩やかに減少している.

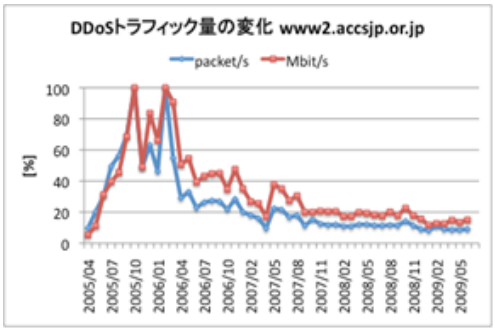


図 4 DDoS トラフィック量の変化 2

図 5 に第二ターゲットへの攻撃に参加したソース IP 数の推移を示す.

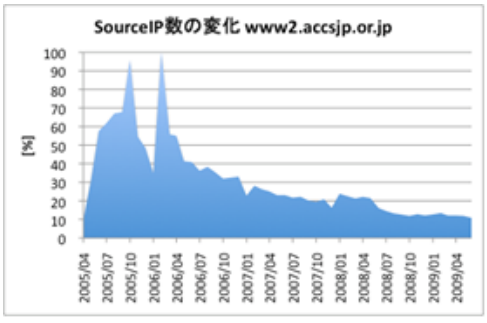


図 5　ソース IP アドレス数の変化 2

トラフィック量の推移とほぼ同様の変化を示しているが，第一ターゲットへの攻撃と同様に 2005 年 9 月と 2006 年 1 月の急増および 2005 年 10 月，2006 年 2 月の急減が発生している．新規の亜種の大量感染に対する対応が行われ減少させることができたが，3 ヶ月にはさらに亜種が発生し，前回のピークと同等の影響を出し，それに対する対応によりこの急増

を抑えることができたが，ベースラインは変わっておらず，ウィルスチェックソフトの効果の限界を示している．

### 4. 3　攻撃送信国

攻撃に利用されたソース IP アドレスの国の割合を図 6 に示す．95%は日本国内からであるがその他韓国，アメリカ等からも攻撃が発生している．これは Winny の利用者がそれらの国に存在し，日本国内ユーザーと同様に，同じ手法で感染していることを示している．

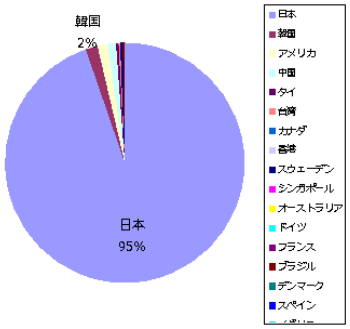


図 6　攻撃送信国

### 4. 3　亜種

実際の亜種数は明確にはわかっていないが百種類以上はあるとみられ検体が捕捉されずウィルスチェックソフトの対応もされなかったものが多数ある．

### 4. 4　攻撃力の変化

攻撃開始から 4 年経過しているにもかかわらず，攻撃に関連するソース IP アドレス数および発生する攻撃トラフィックはピーク時の 15%から 20%程度までしか減少していない．対策の効果が明確に見られる部分もあるが，基本的に緩やかな自然減の特性のみしか現れていないように見える．ボットネットに制御された攻撃ならほとんどの場合，攻撃期間は限定されるが，Antinny のような定期的に自動攻撃するマルウェアに一度狙われると，完全に駆除されるまでは攻撃され続けることになるといえる．

## 5.　要因分析

長期間にわたる Antinny をとりまく状況の解析から，マルウェアおよび感染端末、その所有者に関する直接的、間接的なさまざまな要因の変化とその効果，影響について分析し，対策の現実的な問題点を考察する．

### 5. 1　大量の亜種への対応

大量の亜種が短期間に集中的に作成され，DDoS 関連の解析でも対策の実施と新規亜種作成の繰り返しが見られる．結果的にはすべての亜種の捕捉，把握はできず，ウィルスチェックソフトの対応は，その当時もっとも目立つ活動をしたもので検体の捕捉をしやすかったものだけにとどまったのではないかと思われる特性を示している．図 3 や図 5 で説明した 2005 年 9 月，2006 年 1 月の急増とそれぞれその翌月の急減である．当然ウィルスチェックソフトの機能だけの問題ではないが，新種の発生によるバーストを抑える効果しかなかった．検体の捕捉，解析に基づくウィルス対策の限界および，ウィルスチェックソフト利用者の拡大の問題と考えられる．

### 5. 1　Antinny の開発の終了

Antinny だけではなく，その他の活発だった関連するマルウェアに関しても 2006 年 3 月以降目立った亜種は登場していない．特に Antinny の開発はその時点で終了しているものと思われる．つまり関連するマルウェア開発終了から 3 年半以上経過した状況でも完全駆除されることはなく，そのソース IP アドレス数の推移から感染者は 15%から 20%程度までしか減少していないことになる．新規感染者，再感染者の要素もあるが，それらの要素を含めた上でこの程度の減少度となる．ウィルスチェックソフトで対応できていない亜種が存在するのか，やはりウィルスチェックソフト利用者の拡大の限界の問題と考えられる

### 5. 2　P2P アプリケーションの変化

Antinny がもっとも活発に流通したのは Winny ネットワーク上であるが，前述のとおり今現在は Winny ネットワークの規模は縮小し別の P2P アプリケーションが中心となっている．このことも本来なら Antinny の感染効果を弱める要因のひとつと考えることができるが，マルウェア自体の流通場所は，感染可能性の高いユーザーの多い新たな P2P ネットワークに移るだけなので影響は小さいと考えられる．感染者の増加も認められないため，その面からもこの要素はほぼ影響ないと想定される．

### 5. 3　ユーザー環境

4 年という時間が経過することからユーザー環境も大きく変わることが想定される．

(1)　パソコンの買い替え
(2)　OS バージョンアップ，買い替え
(3)　それに伴うウィルスチェックソフトの普及

また，このようなセキュリティ対策とは無関係な要素によりセキュリティ対策の手が届かないユーザーも改善されていくことが期待されることがあるが，図 3，図 5 を見ると目立った影響はみられず，ゆるやかな自然減の要因として考えられるにとどまる．自然減の要素がすべてこの要因と想定すると，単純に計算すれば，Antinny に感染したユーザーの 80%が 4 年の間に何かしらの環境変化を行ったが，のこりの 20%はまったく環境が変わっておらず，感染したまま，もしくは環境が変わったとしても再感染してしまうようなセキュリティ対策しか行われていないのではないかと想定される．この問題については家電製品の買い替えサイクルや，新 OS の登場サイクル，パソコンに搭載される新機能，必要性能の変化などの買い替え需要の要因を総合的に解析する必要がある．

## 6. 類似するマルウェア

ここで述べてきた自動攻撃は Antinny 特有の機能ではなく，古くから多くのマルウェアに搭載されてきた．DDoS はボットネットのような指令サーバーによる命令によって実行されるものもあるが，単一の目的のために実施するには攻撃対象と攻撃タイミングをあらかじめプロミングした自動攻撃型のマルウェアによって簡易に行われるものが多い．古典的な手法であるが，今現在でも有効な手法として用いられている．

例えば 2007 年から 2008 年に活発だった W32/Allaple，W32/Rahack などがもつ DDoS 機能によって発生するトラフィックは非常に大きい．

表 4　Allaple，Rahack の DDoS 機能

| | |
|---|---|
| 攻撃対象 | www.starman.ee<br>www.if.ee<br>www.online.if.ee |
| 攻撃日時 | 感染と同時に発生，常時 |
| 攻撃内容 | ICMP flood<br>HTTP GET requests flood<br>SYN Flood（TCP443 など） |

このマルウェアはハニーポットなどを設置すると簡単に捕捉でき，この攻撃トラフィックを観測できた．今現在はこの攻撃も減少している．

またボットなどが感染時に端末の疎通性確認，到達可能ネットワーク確認のために特定のサイトに対して icmp や HTTP GET Request などを送出する場合が多いが，本来の目的ではないが，大量感染の結果継続的な DDoS 攻撃としての効果を生み出すことも多い．

## 7. 考察

本稿で解析した結果から，現状の問題点をまとめると，ウィルスチェックソフトによる直接的なマルウェア対策の効果は短期間しか有効ではなく，大量の亜種が存在する場合その効果は 50%程度である．そしてさらなる新しい亜種の登場によりすべての対策効果はゼロクリアされる．しかし対応を続けないと爆発的な蔓延が想定されるため，50%程度の効果だとしても爆発的な拡大を抑えるために亜種の開発が終わるまでは繰り返し対応する必要がある．また，パソコンの買い替えなど，セキュリティ対策とは関係ないが影響の大きいと想定されるユーザー環境の変化による改善も，それほど大きくなく，ゆるやかな自然減で 4 年かけて 80%減にしかなっていない．自動攻撃型のマルウェアの影響はこの間継続し続けることになり，影響がないレベルまで駆除されるには 6 年以上を必要とするのではないかと想定される．

したがってより効率的な対策を実施するには既存のマルウェア対策の仕組みの精度向上だけではなく，基盤となるインターネットサービスの仕組みとして感染を防ぐ，もしくは感染したとしても影響を最小限に抑える仕組み，またはサービスの提供の検討が必要だと考えられる．

## 8. おわりに

本稿では国内 30 万台弱まで感染を広げた大規模感染マルウェアである Antinny の 4 年間の変化を解析し、さまざまな要因変化にも関わらず駆除されず攻撃力を維持し続ける原因について分析を行い必要な対策の考察を行った。今後は他のマルウェアにおいても同様な解析を行い，さらに多角的な要因分析をすることにより，既存手法にとらわれないマルウェア対策の検討を行う．

謝辞

本研究を進めるにあたり，有益な助言と協力を頂いた Telecom-ISAC Japan の関係者各位に深く感謝致します．

## 参考文献

[1] http://www.ccc.go.jp/

[2] https://www.telecom-isac.jp

[3] http://project.honeynet.org/

[4] 高橋正和，村上純一，須藤年章，平原伸昭，佐々木良一：”フィールド調査によるボットネットの挙動解析”，情報処理学会論文誌 Vol.47 No.8 (2006)