2.2 DoS/DDoS 攻撃観察日記(2) ～Antinny による ACCS サイトへの DDoS 攻撃～

小山　覚（(株) NTTPC コミュニケーションズ）
中川文憲（一般社団法人コンピュータソフトウェア著作権協会）

プロローグ

本稿は 2004 年から 2006 年にかけて行われた，一般社団法人コンピュータソフトウェア著作権協会（以降，ACCS）の公式サイトへの DDoS（Distributed Denial of Service）攻撃に関する対応経過をまとめたものである．

この取り組みは通信業界におけるインシデント情報共有・分析センターとして活動するテレコム・アイザック推進会議（以降，Telecom-ISAC Japan）が中心となり行われたが，インターネットサービスプロバイダ（ISP）各社，マイクロソフトならびにトレンドマイクロなどのアンチウイルスベンダだけでなく，最終的には日本国政府までを巻き込む取り組みに繋がった．単なる DDoS 対策にとどまらず，Winny で注目を集めた著作権問題を発端としたマルウェア「Antinny」による個人情報漏洩問題への対策など，総合的な IT リテラシー向上に向けた取り組みに発展した日本国内では初めての事例の紹介である．本稿の執筆は当時 Telecom-ISAC Japan 技術作業部会の副部会長を担当していた小山覚と，当時から現在も ACCS に勤務し著作権問題対策に従事している中川文憲が担当した．

第 1 章：緊急避難

■ 2004 年 3 月 1 日

朝一番 ACCS が利用していたレンタルサーバ業者から急報があった．ACCS サイトが急増したアクセスに耐えきれずダウンした．毎秒 5,000 回を超える Web ページへのアクセスが発生し Web サーバを守るファイアウォールがその負荷に耐えきれない状態に陥ったため，止むなく Web サーバを停止させる事態に陥ったという連絡だった．当時の ACCS サイトは 2,000 ～ 3,000 回／月のアクセスで，多いときでも 10,000 ～ 15,000 ／月のアクセスであったが，わずか 1 秒間に 1 カ月に相当するアクセスが月初から数日継続した．

3 月中旬にアンチウイルスベンダから連絡があり，ACCS サイトに過剰なアクセスを行い，ACCS サイトだけでなく同サイトを収容するホスティング環境ごと麻痺させてしまった犯人は，Antinny.G と呼ばれるマルウェアであることが明らかになった．Antinny は P2P ファイル共有ソフト Winny にばら撒かれたマルウェアで，感染すると当該 PC の情報を Winny ネットワークにばら撒く動作を行う．さまざまな個人情報や重要な機密情報の漏洩事件を引き起こした元凶となったマルウェアである．

ACCS はアンチウイルスベンダからの情報を自身でも確認するために，音楽ファイルに添付され蔓延していた Antinny らしき検体を Winny を使ってダウンロードし，アンチウイルスベンダに解析を依頼した．後に ACCS サイトに過剰なアクセスを行ったマルウェアは，これら Antinny の複数の亜種によるものであることが分かった．

■ 2004 年 3 月 29 日

トレンドマイクロやシマンテックが Antinny.G のパターンファイルを更新し世の中に警鐘を発したのは，ACCS サイトが攻撃された約 1 カ月後の 2004 年 3 月 29 日であった．ACCS によれば，3 月中旬にアンチウイルスベンダから ACCS サイトに過剰なアクセスを行うマルウェアの存在を知らされたが，具体的な対応策は技術的にも経済的に不可能な状態で，どうすることも

できなかったという．しかも，ホスティング事業者からは契約を打ち切られる可能性もあり，当時普及を始めたNTT東日本の「Bフレッツ」を敷設して専用環境での事業継続を模索していた．

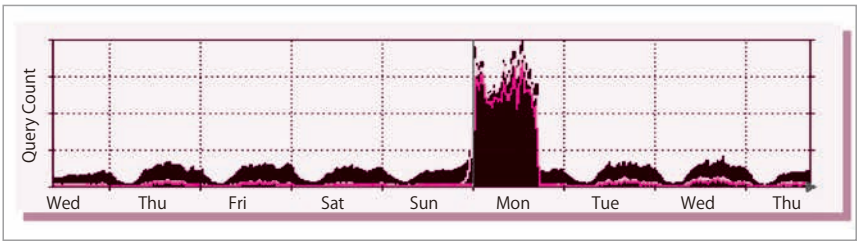

図-1　2004年4月4日OCNのDNSサーバへのDNSクエリ件数の推移

同じ頃，Telecom-ISAC Japan会員のISP各社では，通常とは異なる大量通信を観測していた．特に影響が大きかったのは，Webサーバの IPアドレスを調べるDNSサーバに，過大な負荷がかかる状態が発生したことである．

■ 2004年4月4日

Antinny.Kと呼ばれる新たな亜種が発生し再びACCSサイトを攻撃した．このマルウェアはシステムの日付が4月以降で，かつ，月と日の数値が同一の場合（ぞろ目）になると，感染したPCの個人情報を送信するために，10秒間隔でhttp://www.accsjp.or.jp/へのGETリクエストと，https://www.accsjp.or.jp/cgi-bin/form/piracy/webform.cgiへのPOSTリクエストを日付が変わるまで実行した．月初から攻撃を行うAntinny.Gとぞろ目の日に発動するAntinn.Kの影響で，ACCSサイトは毎月1日からぞろ目の日が終わるまで（5月の場合は5月5日まで）は運営が困難な状況に陥ったのである．

3月3日に発生した攻撃が再発したとの報告をホスティング事業者から受信したACCSでは，前回の攻撃時と同様にDNSサーバからACCSサイトのAレコードを削除することを決定し，ホスティング事業者にその旨を指示した．この対策案はホスティング業者から提案されたものであるが，過去に大規模に蔓延したマルウェアのDDoS攻撃を回避する際に採用された対策を参考にしたものである．ただし，Antinnyには後述する理由から有効に機能しなかった．さらに，月初やぞろ目だけでなく第一月曜日に発動するものまで，さまざまな亜種が登場し，まさに愉快犯に翻弄され続けた．

一方，ISPの運用を行うオペレーションセンタでは，名前解決要求（以降，DNSクエリ）が突然激増するのを観測していた．ISP（OCN）の談話によれば，通常の6倍ものクエリに襲われたDNSサーバでは過負荷状態になり，通常の名前解決の処理が滞り，メールの配送やWebサイトの閲覧が重く感じられる状況に陥った（図-1）．

このときTelecom-ISAC Japan会員のISP各社は突然のDNSクエリ増加の理由が分からず，回避策として設備増強などの策を講じた．また，インターネットの大規模な障害に繋がりかねない事態を憂慮し，「DNSクエリ増加に関して情報共有」を開始した．当時の会員が独自に集めた情報の中に，AntinnyがACCSを攻撃するとの情報があった．アンチウイルスベンダの解析情報を調査すると，攻撃日時など今回のDNSクエリの増加日時と符合していたことから，攻撃対象となっているACCSを訪問し詳細な情報を調査することになった．

同じ頃，Antinnyの調査していた外部機関から解析と観測情報が寄せられた．どうやらAntinnyがACCSサイトにアクセスする際にDNSサーバで名前解決を行うが，IPアドレスが得られない（NXDOMAIN）場合には，際限なくDNSクエリを出し続ける仕様であるとの情報を入手した．一般的なアプリケーションではDNSサーバがNXDOMAINを返した場合はDNSクエリ動作を停止させるようにプログラミングされている．しかしAntinnyは作者の意図の有無は別にして，このエラー処理を行わないためインターネットの安定運用に影響を及ぼしたのである．Telecom-ISAC Japanでは，この状況を前提とした対応策を複数検討し，ACCSに提案すべく訪問した．

■ 2004年4月26日

当時の通信事業者と著作権関連団体とは緊密とは言いがたい関係であった．知人を頼りつつ窓口を探り当てたような状態ではあったが，無事，Telecom-ISAC

Japan の代表者が ACCS を訪問する当日を迎えることができた．情報交換の結果，ACCS からは 2004 年 3 月から公式サイトへの過剰なアクセスが継続しており，ACCS サイトの閲覧が困難なだけでなくホスティング環境全体にも影響を及ぼしたため，2 つの対策を実施したとの説明があった．

① DNS サーバに登録されている「www.accsjp.or.jp」の A レコードを削除することで，Web アクセスを発生させないようにした．

②サーバレンタル先で使用する回線を，共有回線から専用回線へ変更し，もしも大量通信が発生した場合でも他のユーザに迷惑をかけない対策を実施した．

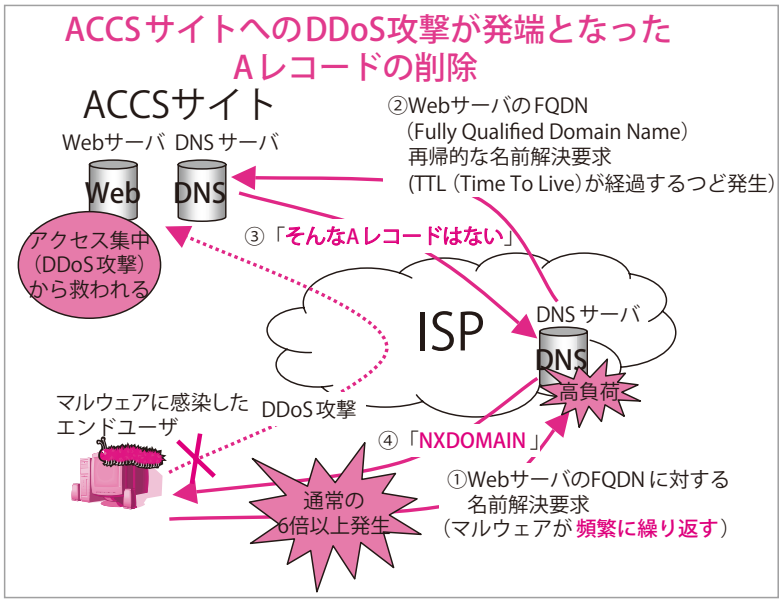

図 -2　攻撃発生のメカニズム

Telecom-ISAC Japan が想定した通り，対策①の影響で結果的に ISP の DNS サーバにクエリが集中し，インターネットアクセスに遅延が生じる状況となっていた．つまり図 -2 のように ACCS サイトが存在しない Web サイトになってしまったことから，DNS サーバが名前解決要求に対して NXDOMAIN を返す．Antinny は名前解決要求の無限ループに入り，通常では考えられない量の DNS クエリを発生させ DNS サーバの処理が追いつかない状態に陥ったようであった．

また Telecom-ISAC Japan から ACCS に対して，サイトの処理能力を向上させる設備増強策を提案したが，一時的な対策ならまだしも，その対策を ACCS が継続することは経済的に困難であるとの結論に達し断念せざるを得なかった．このため，5 月 5 日に想定される次回の大規模な攻撃には，次のように対応することを決定した．

- ACCS サイトへの攻撃を発生させないようにするため，DNS サーバのエントリから ACCS サイトの A レコードを削除する．
- ISP の DNS サーバには Antinny の DNS クエリの再帰的動作の影響に負けないよう設備増強等を行う．すなわち，ISP 各社が攻撃を正面から受ける．Telecom-ISAC Japan の会員以外の ISP 各社には，ACCS から（社）インターネットプロバイダ協会を通じて「ACCS の DNS サーバから www.accsjp.or.jp の IP アドレスを削除することで，ISP の DNS サーバに大量のアクセスが行われる可能性がある」旨を連絡してもらい，3 月と同様 A レコードを削除した．しかしながら，これまでの URL を指定するアクセスだけでなく，IP アドレスを直接指定するアクセスが大量にあったため，A レコード削除だけでは対処しきれず，サーバを物理的にシャットダウンして，アクセスを完全に停止するしかなかった．

■ 2004 年 5 月 5 日

Antinny の攻撃により，ISP の DNS サーバには大量の DNS クエリが押し寄せたが，事前に設備増強等の準備をしていたこともあり，安定した通信環境を確保することはできた．しかし Antinny 感染 PC 数が増加した場合や，DNS サーバの負荷増大を意図した悪意のマルウェアが出現した場合は，現状の対策技術で必要十分と言える保証はなかった．不測の事態に備え，Telecom-ISAC Japan では DDoS 対策 WG を発足し，対応策の検討を開始した．まず緊急避難的な対応策を検討し通信の安定性確保を最優先に取り組むことになった．ただ，Antinny の大量通信が原因で，ACCS のビジネスが阻害されたり，その対策に必要なコストや技術が，一般的な法人にとって過大なものである現状

を振り返ると，健全なインターネットの発展に寄与する目的からも，この問題の解決に取り組まねばならないとの思いと，ISP として電気通信事業法で定められた業務範囲を逸脱することのない対応策の実装について，相当に神経を使った議論を行った．その議論の中で出した当面の結論（優先順位）は次の通りであった．

- 優先順位 1：ISP の DNS サーバへの負荷を下げ，安定したインターネット環境を確保する（ACCS の救済は考慮しない）．
- 優先順位 2：Antinny などマルウェアの根治対策を実施し，ACCS サイトが通常の運営をできる状態にする．

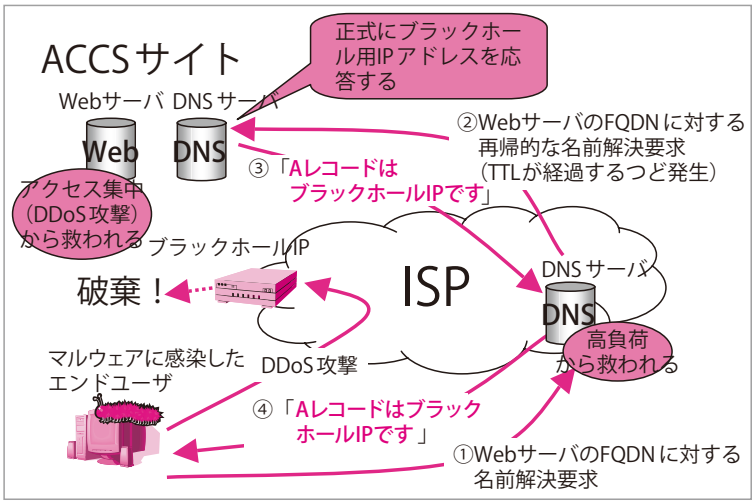

図 -3　対策のメカニズム

ISP はインターネット接続サービスを提供する電気通信事業者であり，通信サービスの安定提供が第一優先で，個別の顧客要望はその上で成り立つ個別契約の範疇である．一方でかかわる個々人の良心に反する微妙な部分はありつつも，ACCS 救済を第一優先順位に挙げることはできなかった．一部繰り返しになるが，DNS サーバは PC からの DNS クエリに対して該当する「IP アドレス」を通知する．その Web サーバのドメイン名や URL が存在しない場合は「NXDOMAIN」というメッセージを返す．一般的に「NXDOMAIN」を受け取った PC は目的とする IP アドレスが存在しないため，それ以上の通信要求は行わず通信は終了する．しかし，Antinny は「NXDOMAIN」を受け取っても，IP アドレス情報を受領するまで何度でも DNS クエリを出し続ける仕様であるため，一部 ISP では通常の 6 倍もの DNS クエリが発生していたのである．そこで打ち出された第一優先対策が，DNS クエリを必要以上に発生させないことであった．具体的には，Antinny に感染した PC からの 1 回目の DNS クエリに対して IP アドレスを応答する．要は，ACCS への攻撃を発生させることで，再帰的な DNS クエリを封じ込める方法である．さらに，わざと発生させた攻撃をインターネットの内部，第三者に影響が出ないバックボーン上で捨てる取り組みを行うことになった（図 -3）．

DNS サーバの負荷を軽減するためには，Antinny に Web サーバに対応した「IP アドレス」を教えることで，頻繁な名前解決要求による過負荷状態からまぬがれることができる．攻撃からインターネットを守るため，あえて攻撃を発生させる前代未聞の取り組みに対して，大手 8 社の ISP が協力を申し出た．

肉を切らせて骨を断つとも言うべきこの方法の場合，あえて発生させる攻撃により大量の通信が発生し，ACCS サイトおよびその経路上では通信設備等に影響を及ぼす可能性がある．そこで，通信設備等に影響を最小限にとどめる施策を導入した．具体的には，各 ISP の DNS が応答する IP アドレスは，ACCS サイトの IP アドレスではなく，攻撃通信を廃棄するために各々の ISP が用意したブラックホール IP アドレスとする．これにより，仮に大量の通信が発生しても各 ISP ネットワークの中に設置したブラックホールに吸い込んで捨ててしまう．かくして大胆な戦略が立案され実行に移されたのである（図 -4）．

当時の Telecom-ISAC Japan での議論として，攻撃発生時は設備への過剰な負荷が発生する蓋然性が高いが，通信パケットを捨てる行為は通信の秘密を侵害している．しかし，自社の設備保護や通信の安定確保の観点から，正当業務行為として違法性は阻却され，かつ対策方法としても ACCS サイトにアクセスする通信のみを対象とすることから，対策行為の相当性も確保されていると整理された．さらにこの対策は，通信当事者の ACCS からの依頼を受けるかたちで実行され，

かつ対策実施期間中は ACCS サイトを閉鎖する旨の告知を出すことで，電気通信事業法の通信の秘密を侵害することのないよう，十分考慮されたトライアルとしてスタートさせた．

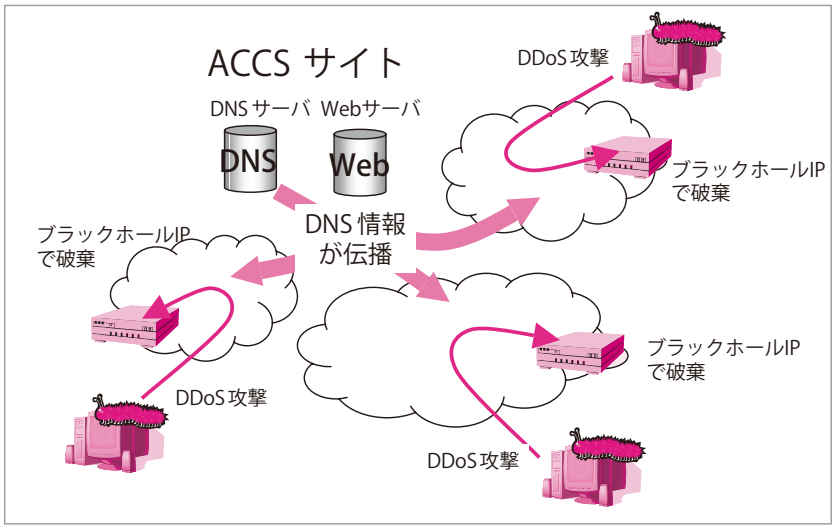

図 -4　ISP が連携して攻撃通信を捨てるブラックホール作戦

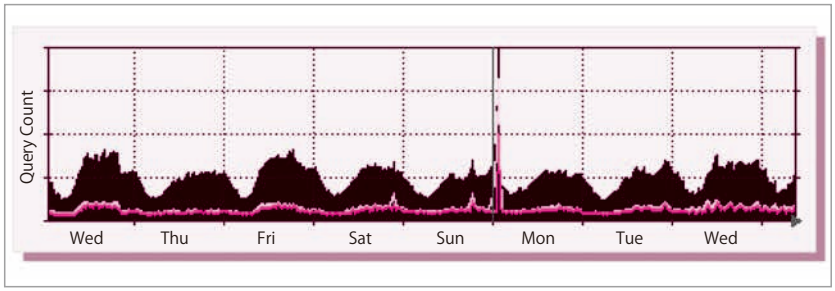

図 -5　2004 年 6 月 6 日 OCN の DNS サーバへの DNS クエリ件数の推移

■ 2004 年 6 月 6 日

理論武装も自画自賛するレベルで整理したものの，問題は ISP 社内をどう説得するか，自社の説得が関係者の頭を一番悩ませた．6 月 6 日の大規模な攻撃まで猶予は残されていない．DNS サーバに負荷をかけた通信と言えども，通信を遮断することに関する通信事業者の反応は重い．通常の意思決定フローに乗せると，次回発生する 6 月 6 日の攻撃発生には間に合わないかもしれない．しかも前例がない取り組みである．さらにブラックホールなどと突っ込みどころ満載のネーミングなので，Telecom-ISAC Japan では止むなく「皆さんそうなさっています作戦」を実行することになった．どこの ISP にも通信先が存在しない通信パケットを自社網内通信の早い段階で捨てるブラックホール的な仕組みは何らかのかたちで持っており，そう特別なことをやるのではない．これを前置きにして，当時大手 ISP8 社が一斉に社内に持ち帰り，「Telecom-ISAC Japan 会員各社は皆さん実施の方向で検討中である」ことを社内に伝えた．称して「皆さんそうなさっています作戦」である．かくして DNS サーバは守られたのである（図 -5）．しかし，ACCS の Web サイトは守られないままであった．

第 2 章：百聞は一見に如かず

ISP としてはここで取り組みを終了するのが一番楽な選択肢であった．しかし，ACCS サイトへの大量のアクセスは，結果的に DDoS 攻撃となっており，通信設備への影響の可能性を考えると看過することはできない．また，毎月ゾロ目の日に攻撃をしかけてくる相手がいるのであれば，この機に練習試合をやって日本のインターネットコミュニティとして，DDoS 攻撃対応能力を向上させようということになった．多少の不謹慎はお許しいただきたい．当時の考えとして，所詮は Winny が媒介するマルウェアだし，NXDOMAIN のエラー処理も行われていないプログラム相手なので，大したことはないだろうという甘い見込みもありつつ調査を開始した．具体的な調査方法としては，ACCS サイトに通信キャプチャ装置を仕込んで攻撃を観測することにした（図 -6）．この調査は Telecom-ISAC Japan の会員各社が持ち出し覚悟で実施したものである．

■ 2004 年 6 月～ 8 月

Telecom-ISAC Japan の会員企業が共同でブラックホール IP に攻撃通信を捨てる運用を実施している間，ACCS サイトは誰からも閲覧できない状態が続いた．このままではインターネットの平和が守られているとは言えない．そこで 2004 年 8 月，いったんブラッ

クホール IP アドレスの運用を停止し，ACCS サイトへの攻撃を発生させ，攻撃通信の全容把握に取り組むこととした．調査期間は 7 月 31 日から 11 日間とし，その間攻撃通信のデータ取得を試みた．しかし，想定以上の大量通信が発生し ACCS サイトやファイアウォールがダウンしてしまったことから，測定期間全体を通じたデータの取得はできなかったのである．図 -7 が示すように，攻撃が発生する期間になると，グラフに欠損が生じている．

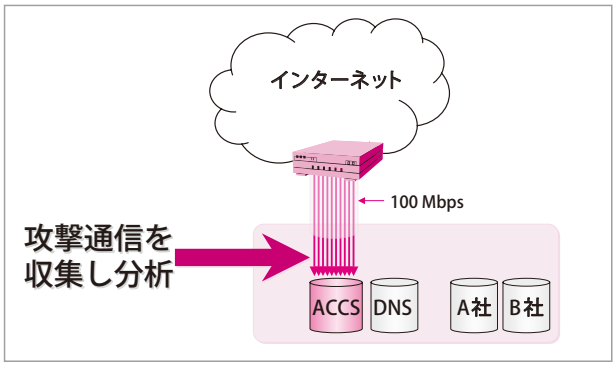

図 -6　ACCS サイトへの攻撃観測方法のイメージ

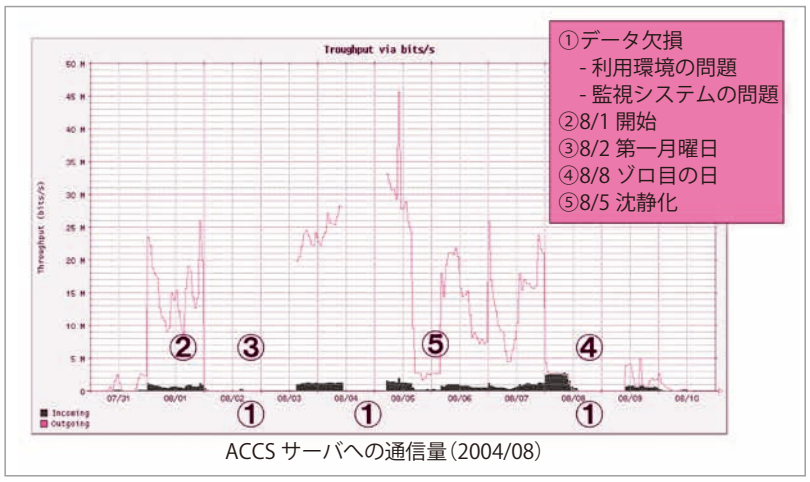

図 -7　ACCS サイトにおける攻撃通信の状況

同期間の通信パケットのフラグ別の通信量を表示したのが図 -8 である．データ欠損が生じている期間①は，TCP SYN パケットが急増後にシステムダウンしていることから，TCP SYN Flood 攻撃と同様の状況が発生しているものと思われる．つまり瞬間的に捌ききれない通信確立要求が Antinny から送信され，通信が成立しない状況が続くことでファイアウォール等のコネクションテーブルがオーバフローし，システムダウンに追い込まれた可能性がある．

また，データが欠損している期間以外は，回線容量を超える急激な通信量の変化は記録されていない，当時の ACCS サイトの設備耐力でも物理的には対応可能であったと考えられた．

Web サイトではユーザのアクセス量に応じて，回線帯域やサーバを増強することで対応してきた．たとえば，注目を集める発表を行う際は事前に Web サーバ関連リソースを増強し負荷分散装置を介することで負荷分散するか，コンテンツデリバリネットワーク等を利用することで，急激なユーザのアクセスに対応している．今回観測された Antinny のアクセスも外見的には一般的な Web アクセスとの見分けがつきにくいため，Antinny のアクセスを止めることは他のユーザのアクセスも遮断する可能性が高い．このような場合は，Antinny の大量アクセスを含むすべての通信に耐え得る設備環境を作るのが最も単純な対応策となる．Telecom-ISAC Japan が ACCS に最初に提案したのもこのような対策であったが，コスト負担ができない ACCS の経済的な理由のため実現には至らなかった．そこで今回は ISP の商用インフラクラスの設備を用意し，Antinny が行う TCP のコネクション要求に対応するために十分な回線とマシンリソースを整えることで，ACCS サイトの事業継続が可能なのか設備規模について検討を行うことにした．ここでも Telecom-ISAC Japan の会員企業の協力を得て，図 -9 のような環境を準備し，ACCS サイトのコンテンツを移植して攻撃通信の発生状況を観察した．

この環境は 2004 年当時としては，上場企業クラスの Web サイトの規模を超えるものであり，巨大な Web サイトを運営するネットコンテンツ企業のサイトに匹敵する環境である．

■ 2004 年 9 月 2 日

ISP のバックーン上に ACCS サイトを複製し，攻撃の実態調査を開始した．

調査の結果，Antinny と ACCS サイト間で行われ

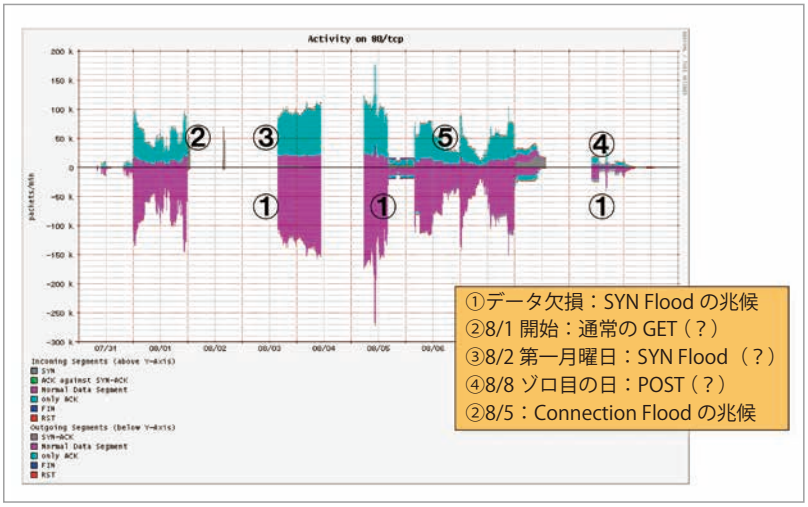

図 -8　ACCS サーバ (80/tcp) へのフラグ別の通信量

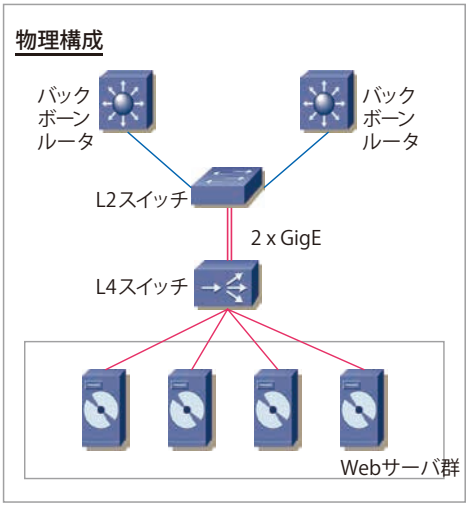

図 -9　Antinny 攻撃通信調査のために準備した環境イメージ

た通信は，最大 700Mbps にも達することが判明した（図 -10）．ISP 級の設備耐力であれば攻撃を受けながら Web サイトの情報公開（コンテンツ配信）は可能だが，ネットビジネスを行わないような情報発信を目的とした Web サイトに対して企業が支払えるコストでは収まらない規模の通信量であることが再確認できた．これは想像を大きく上回る通信規模だった．

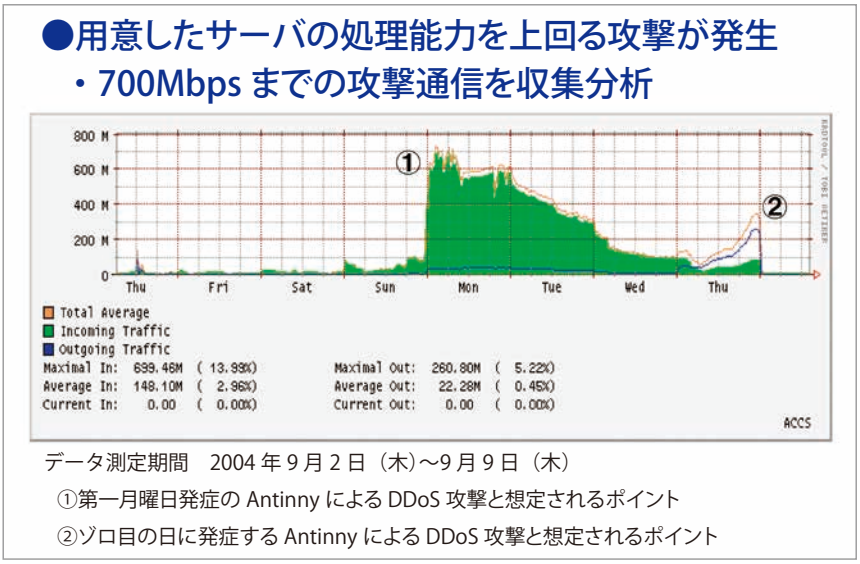

図 -10　Antinny 攻撃通信の調査結果

この規模の通信量が突然あちこちで吹き荒れる状況を想定すると，ISP の設備増強も追い付かず，その対策費用を考えると看過することができない問題である．何らかの対策は必要であるものの，打つ手がないまま，インターネットコミュニティに対する報告を Telecom-ISAC Japan と ACCS は連名で行うことにした．当時 ACCS ではこれら調査結果を受けて，今後の対応策について表 -1 のような検討を行ったが，いずれも ACCS 単独での実現は困難との結論に至っている．

■ 2004 年 12 月 2 日

InternetWeek2004 で問題提起したのはおおむね，『インターネットコミュニティを破壊するリスクが顕在化』，『いつ誰のサイトに攻撃が訪れても不思議ではない』，『経済的理由でユーザはサーバの増強すらできない』の 3 つで，講演の最後にインターネットコミュニティに対して『さて，どうしましょう』と問いかけた．

その間，ACCS は毎月月初になると始まる攻撃に悩まされ続けた．また，ISP では，攻撃が開始されると，インターネットの他のユーザに迷惑をかけることがないように，ACCS サイトへの通信をすべてブラックホールに飲み込むような運用を続けざるを得なかった．

2005 年 1 月になると，特定の日だけでなく，ACCS サイトに対して毎日大量のアクセスが行われ，月初以外のすべての日において Web サイトの閲覧がまったく

対策案	検討結果	理由
回線容量を増強し，サーバを複数立てるなどして堅牢な環境を構築する	断念	Telecom-ISAC Japan の協力のもと，DDoS 攻撃の実態を調査する実験を行ったところ，ピーク時には 700Mbps を超える通信が行われていることが判明した．この DDoS 攻撃に耐えるためには，年間で億単位の費用をかけて，環境を整備する必要があり，年間予算 2 億円程度の ACCS ではその費用を捻出できない．
Antinny 制作者を刑事告訴する	断念	マルウェアの制作者を探し出すことにかかる費用や労力，またそこまでしても見つけられない可能性が高い．マルウェアの制作者そのものを断ずる法制がその時点では存在していなかった．
ACCS サイトの URL を変更する	実施するも効果を得られず	当初，URL の変更は，現在のネットワーク社会において社名変更と同義であり，変更したことの告知にかかる労力も相当なものであると予測されたため，最終手段であると考えていた．しかし，後述するように 2005 年 1 月は，特定の日だけでなく，毎日大量のアクセスが行われ，1 日も閲覧できなかった．やむをえず，URL を http://www2.accsjp.or.jp（以下，www2 と呼ぶ）に変更することとなった．その結果，3 カ月は安定して運用することができたが，2005 年 4 月に「www2」に対しても DDoS 攻撃が行われるようになった．
DDoS 攻撃を行っているユーザを告訴する	断念	マルウェアが原因で起こっていることなので，ユーザ自身に攻撃の意図がない，または攻撃していることを認識していない可能性が高いこと，刑事告訴を行うにしても，異常と思われる IP アドレスとアクセス時間は判明しているものの，それが実際にどこの誰なのかは ISP でないと分からない．
DDoS 攻撃であることが判明した場合，即座にその IP アドレスからのアクセスを止めてもらうことを ISP に依頼する	断念	ISP に DDoS 攻撃の判別を依頼するということは，「www」または「www2」へのアクセスを監視しつづけてもらう必要があり，それは大変な負担を ISP にかけることになってしまう．

表 -1　ACCS における今後の対応策の検討結果

できない状態に陥った．Antinny の新たな亜種が投入されたことによる影響と考えられた．

■ 2005 年 1 月 25 日

ACCS はやむをえず，URL を www2 に変更することとなった[1]．これは www.accsjp.or.jp に対して集中していた Antinny の攻撃をかわすための方策である．Antinny の作者が早晩攻撃対象 URL を追加または変更するであろうことも想定の範囲であったが，DDoS 攻撃対策の試行錯誤を始めた最初の打ち手でもあった．その結果，3 カ月は安定して運用することができたが，2005 年 4 月に「www2」に対しても DDoS 攻撃が行われるようになった．

第 3 章：反撃開始

このような状況を鑑み，ACCS など技術的にも資金的にも攻撃に対応する能力が不足している団体や個人が，マルウェアからの攻撃で Web サイトが閉鎖に追い込まれたり，転じて ISP のサービスの安定提供に影響を及ぼす事態を避けるために，Telecom-ISAC Japan の会員 ISP が相談し，攻撃を減少させ被害を軽減するための対策として「DDoS 攻撃対策装置の導入」と「攻撃元 IP アドレス保持者への注意喚起」を開始した．

■ 2005 年 3 月～

DDoS 攻撃対策装置の導入

即効性のある対策として，ISP のネットワークに DDoS 攻撃対策装置を導入し，攻撃トラフィックを減少させる取り組みを行った（図 -11）．

DDoS 攻撃対策装置とは，通過する通信を分析し，DDoS 攻撃を峻別し通信をブロックする機能を搭載したファイアウォールのことで，当時はシスコシステムズが発売していた機器を借用し，ACCS サイトに接続された回線サービスの上部側の ISP ネットワークに導入した．その結果，最大で攻撃通信の 99.6% をブロックすることができたが，実際に導入してみると，装置が攻撃に反応するわずかなタイムラグがあり，そのわずかな時間でも攻撃に晒されると ACCS サイトがダウンすることが何度か発生した．チューニングによりダウンする回数を減らすことができたが，DDoS 攻撃対策装置の導入と併せて，Web サイトの設備構成を増強する必要があることも確認できた．

この対策は大きな効果を発揮したが，DDoS 攻撃対策装置が非常に高価であり，個社単位で購入することが困難であること，また ISP ネットワークに導入することで

効果が得られることから，ISP が導入してユーザにはサービスとして貸し出すような運用形態が考えられたが，それでも月額勘算にすると，機器の償却費だけで数十万円以上のコストが発生するため，運用を含めたコスト負担については解決困難な課題であることが浮き彫りになった．

攻撃元 IP アドレス保持者への注意喚起

攻撃そのものを減らす対策としては，Antinny が P2P ファイル共有ソフト Winny のユーザ PC に感染していることから，このマルウェアを駆除することで攻撃を減少させる取り組みを行った．

- マルウェアの駆除ツールの開発
- 攻撃元 IP アドレスの調査
- 攻撃元 IP アドレス保持者への注意喚起

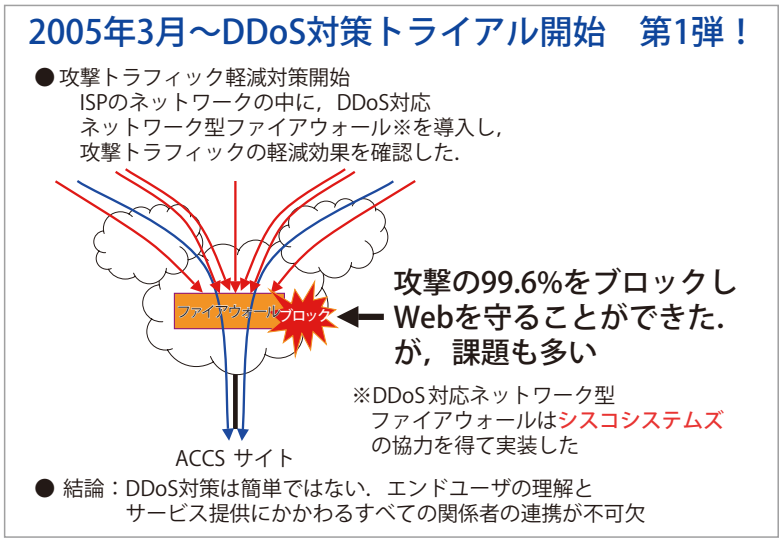

図 -11　DDoS 攻撃対策装置導入のイメージ

(a) マルウェアの駆除ツールの開発

Winny ユーザの多くが感染しているマルウェア Antinny は，当時のアンチウイルスベンダの製品の多くが対応していなかったため，Telecom-ISAC Japan が働きかけることで，大半の製品が最新のパターンファイルで対応してくれることになった．しかし，P2P ファイル共有ソフトのユーザは，ファイルダウンロードの効率性を優先させるために，アンチウイルスソフトをインストールしていない場合が多いとの意見を参考にし，トレンドマイクロなどアンチウイルスベンダの協力を得て，無料で提供可能な「駆除ツール」を開発し，各社の Web サイトで配布を開始した．

(b) 攻撃元 IP アドレスの調査

ACCS サイトに攻撃を仕掛ける IP アドレスの保持者に対して，注意喚起を行うために，ACCS 自身が通信ログを分析し，毎秒数十回以上など通常では考えられないアクセス頻度で，ACCS サイトにアクセスしている通信を攻撃通信と見なしてリストアップした．

(c) 攻撃元 IP アドレス保持者への注意喚起

ACCS は攻撃元 IP アドレスを ISP 別に分類し，当該 IP アドレス保持者に対して ACCS が作成した注意喚起文を電子メールで届けるように依頼した．注意喚起文は，当該 IP アドレスを持つ PC がマルウェアに感染している可能性があること，またその結果 ACCS サイトを攻撃している事実と，駆除ツールによるマルウェアの駆除を呼び掛ける内容となっていた．

各 ISP は，ACCS の依頼に基づき IP アドレスとタイムスタンプから，契約者を調査し，ACCS が作成した注意喚起文をユーザに届けた．Telecom-ISAC Japan の会員企業が連携し数千通のメールを送信し，ごく一部のユーザからは反応があったが，攻撃通信は減少しなかった．この注意喚起の取り組みに関しては ISP 間でも賛否両論があり，取り組みに参加するかどうかの判断は各 ISP に委ねられた．というのも，このような取り組みは，通信の秘密との関係上，合法性について判断が難しかったためである．

この後に「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」が策定されることになるが，この DDoS 対策の取り組みが端緒となっている．

■ 2005 年 3 月 17 日

マルウェアに感染していると思われるユーザに注意喚起を発し駆除ツールを推奨する取り組みについては，ユーザが能動的に実行する必要がある．「駆除ツール」は意識レベルの高いユーザには受け入れられるが，大半のユーザは無関心との想定は対策実施当初からあった．そこで並行して，ユーザに受け入れやすい注意喚起方法の検討や，ユーザが特別に意識せずとも「マルウェア」等を強制的に駆除する仕組みが実現できない

か検討を進めていた．有望案としてマイクロソフトの Malicious Software Removal Tool（以降，MSRT）の対象に Antinny を含める対策が効果的であるとの意見が出され，検討の俎上に上がった．

当時 PC の多くには MSRT が導入された WindowsXP SP2 がインストールされていた．このため，MSRT の駆除対象マルウェアに Antinny を登録してもらい，多くの PC から Antinny を駆除できれば，効果的な DDoS 攻撃対策が実現できる．問題はあのマイクロソフトが協力してくれるかどうかである．そこで，2005 年 3 月 17 日にマイクロソフト社幹部が来日する機会を捉えて訪問し，Antinny の亜種を MSRT の駆除対象リストに加えてもらうように依頼した．当然ながら即答が得られる類の話ではないため，何度かマイクロソフトと交渉を重ねていたが，2005 年 8 月にオランダのアムステルダムで，マイクロソフトと ISP の国際会議が開催され，その会議期間中の意見交換の場において，日本の DDoS 攻撃の実態や，Antinny による個人情報漏洩や政府や企業の機密情報漏洩の実態が紹介された．マイクロソフトは情報漏洩対策の必要性を理解しついに重い腰を上げた．当時，原子力発電所関連情報が情報漏洩した事実がマイクロソフトを決断させたとも言われている．腰を上げると動きが早いのが米国企業の特徴かもしれない，早速 9 月の MSRT に盛り込みたいが準備が可能かどうかとの打診が来た．残念ながら 9 月は間に合わず 10 月に照準を合わせて取り組むことになった．

図 -12　2005 年 10 月 12 日，Telecom-ISAC Japan とマイクロソフトの共同報道発表資料（Telecom-ISAC Japan ならびにマイクロソフトの Web ページより）

■ 2005 年 10 月 12 日

Telecom-ISAC Japan とマイクロソフトは，MSRT を活用して Antinny 対策を行う具体的な方法を検討し，2005 年 10 月 12 日に共同で報道発表を行った（図 -12）．

Antinny を駆除する MSRT は 10 月期のアップデートとしてユーザに提供され，多くの PC に取り込まれ Antinny を駆除した．マイクロソフトの発表によれば，11 万台のコンピュータから，20 万を超える Antinny が駆除されたとのことだった．この結果が DDoS 攻撃の減少にもつながっており，攻撃量の減少が確認できた．当時のマルウェア Antinny の攻撃先は，www.accsjp.or.jp と www2 であり，www.accsjp.or.jp は常時約 4 万の攻撃被疑 IP アドレスから 200,000pps（400Mbps）の攻撃を受けていた．www2 も常時約 1.4 万の攻撃被疑 IP アドレスから 25,000pps（25Mbps）の攻撃を受けていた．MSRT による Antinny の駆除の効果で攻撃量が減少した状況を，図 -13，図 -14 に示す．www.accsjp.or.jp への攻撃被疑 IP アドレスは 39.8% 減少，攻撃トラフィックも 33.4% 減少し，www2 への攻撃被疑 IP アドレスは 43.2% 減少，攻撃トラフィックも 51.4% 減少したことが確認されている．

攻撃被疑 IP アドレスの減少度合いが約 40% 程度であることから，残る 60% は MSRT が導入されていない古い OS の利用者など何らかの理由によって，Antinny ワームが駆除されずに残っている可能性がある．なお，このような観測データの取得は，ACCS サイトの上位 ISP（OCN）に設置した DDoS 対策装置で測定していたが，情報量のない白紙の Web ページを掲載した www.accsjp.or.jp が，常時 4 万の攻撃被疑 IP アドレスから 200,000pps（400Mbps）の攻撃を受けていたことは驚くべき事実であり，攻撃先がなくなっていても執拗

にアクセスを続けるマルウェアによる攻撃の恐ろしさを物語っている．

一見すると効果的な対策に思われた MSRT ではあるが，現実問題として ACCS から見た場合には，攻撃が 400Mbps に半減しても，ACCS の経済力でこの攻撃を含む Web サイトへのアクセスを捌く環境を作るのは困難であり，Web サイトで情報発信ができなくなると，法人の活動として大きなダメージを受けると言わざるを得ない状況は継続していた．ACCS に限らず Web サイトでの情報発信は，多くの法人によって活動の生命線であることは言うまでもないが，一度攻撃対象にされると，感染 PC をすべてシラミ潰しに根絶するまで攻撃が止まない．現実的には不可能に近い状況であり，一度狙われると法人生命の危機とも言える．

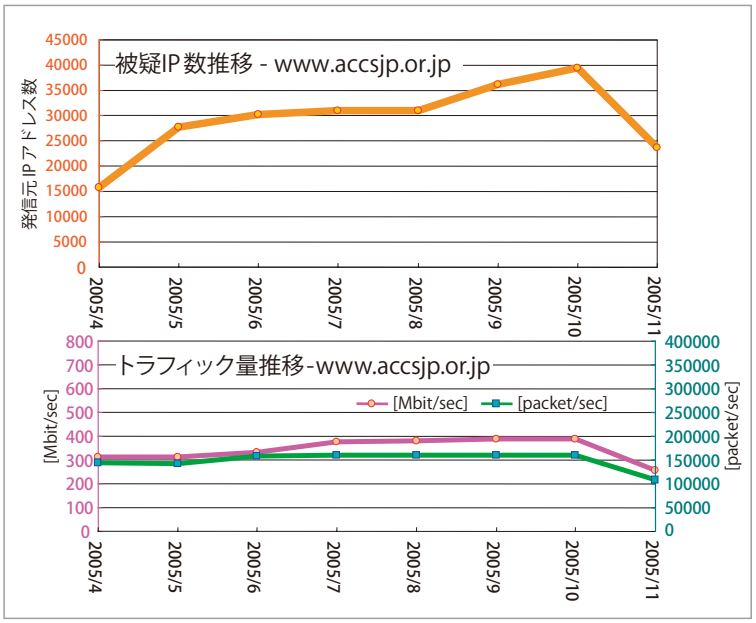

図 -13　www.accsjp.or.jp への攻撃活動の変化
上段：攻撃被疑 IP アドレス数，下段：攻撃トラフィック

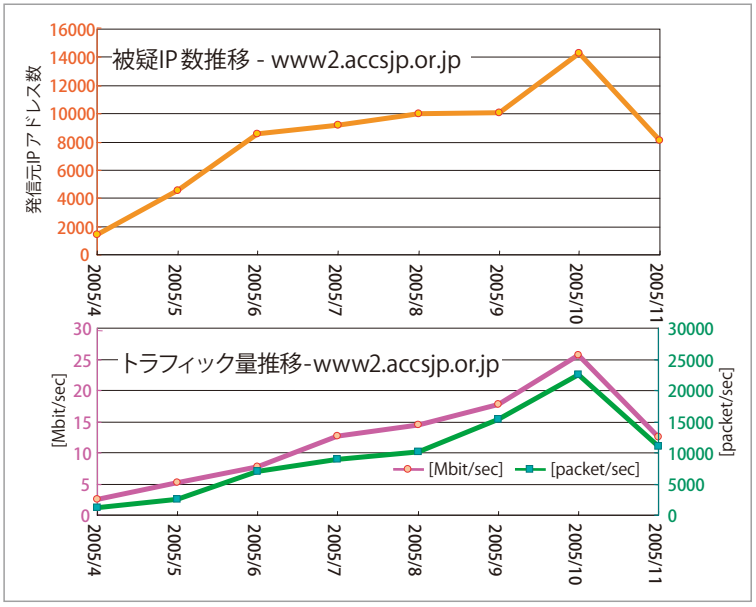

図 -14　www2.accsjp.or.jp への攻撃活動の変化
上段：攻撃被疑 IP アドレス数，下段：攻撃トラフィック

■ 2005 年 12 月

MSRT の効果で減少していた Antinny の攻撃が増加に転じた．MSRT が駆除する Antinny の亜種は 2005 年 9 月頃に確認していたものであり，その後に出現した亜種には対応できないこと，一度 Antinny 駆除されても何度でも再感染してしまう意識の低いユーザの存在などが増加の理由と考えられる．Telecom-ISAC Japan ではめげずに善後策の検討に入った．

第 4 章：リベンジ

■ 2006 年 1 月

Antinny の DDoS 攻撃は猛威をふるい続けたが，同様にこの時期になっても Winny 利用者からの情報漏洩が止まらない状況が継続し社会問題の様相を呈していた．メディアでは情報漏洩した人がマルウェアに感染した被害者であるかのような報道が相次いだ．しかし事実は，他人の著作物等に偽装されたマルウェアを自らダブルクリックしインストールしている．すなわち，他人の著作物等が不正にダウンロードされているという事実が伝わっていないことから，継続的な啓発も並行して行うべきとの議論が行われていた．具体的には，情報漏洩と ACCS への DDoS 攻撃は，Antinny に感染した PC が引き起こす事象であるため，IT リテラシーの向上が最も重要であり，2005 年 3 月に実施した Antinny 感染者への注意喚起を，もう一度粘り強く行う必要があるとの結論に達した．

■ 2006 年 2 月

Antinny 感染者への注意喚起について，昨年の経験を踏まえより効果的なものとするための議論が行われ，ACCS は Telecom-ISAC Japan とマイクロソフトやトレンドマイクロと連携し，Antinny 感染者への注意喚起の効果を測定できるシステム（図 -15）を構築した[2]．システム構築自体は費用負担を含め Telecom-ISAC Japan が担当した．

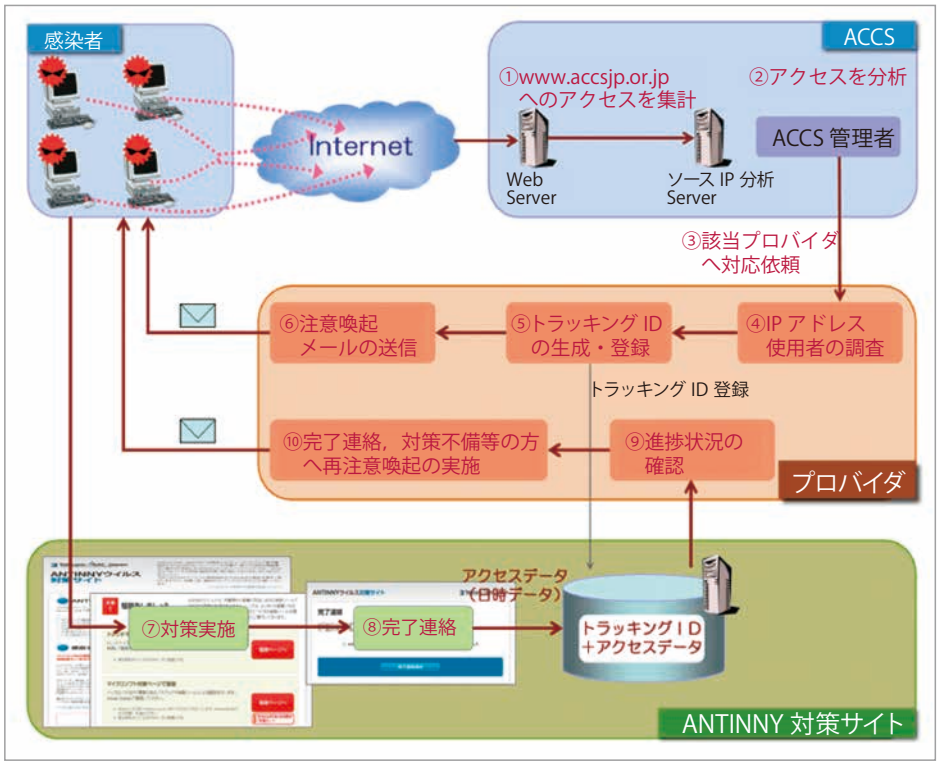

図 -15　Antinny 対策サイト・システムの概要

このシステムはインターネットを介して，複数法人が協調し Web サイト間連携で機能するもので，ACCS サイトに攻撃を仕掛けている人に対して効率的に注意喚起を行い，マイクロソフトやトレンドマイクロが準備した，Antinny 対策や Windows アップデートを推奨するサイトに誘導し，セキュリティ対策を勧奨するとともに，Antinny 対策サイトにアクセスした人をカウントできる機能を実装している．

本システムによる Antinny 感染者への注意喚起は次のような手順で行うことで関係者の整理が行われた．Antinny 対策サイト・システムの構築および運用フローの検討で最大限考慮したのは，Antinny 感染被疑者のプライバシーと個人情報保護である．また 1 つの IP アドレスを複数のユーザが利用していることを想定し，注意喚起メールが契約者に届いた場合に，その契約者が Antinny 感染被疑者ではなくかつ，Winny 等の P2P ファイル共有ソフトとも無関係な場合などを想定し，トラッキング ID（識別子）による問合せの円滑化と，対策サイトのリンク先などの情報を整理した（表 -2）．

■ 2006 年 2 月 20 日

Telecom-ISAC Japan では ACCS の「攻撃者に対する注意喚起」に向けた取り組みについて，対応方針を決定し Web サイトにて以下の発表を行った．

> Telecom-ISAC Japan が行った発表文（抜粋）
> 今般，ACCS の依頼に基づき「www.accsjp.or.jp」に過度のアクセスを継続しているユーザに対して，Telecom-ISAC Japan 会員のインターネットサービス ISP の協力を得て再び注意喚起を行います．Telecom-ISAC Japan としては，Antinny ウイルスの駆除を呼びかけるセキュリティ対策ポータルサイトを構築し運用します．Telecom-ISAC Japan が ACCS の取り組みに協力する背景には，Antinny ウイルスをはじめとする Malware（マルウェア）に感染したユーザが第三者に対する攻撃を行う加害者になるだけでなく，情報漏洩の被害者になるような事案が顕在化しつつあり，このような状況を改善するためには，Antinny ウイルス等の Malware に感染しているインターネットユーザに対する注意喚起が必要不可欠であると考えているためです．今後はこのような注意喚起活動で得られた知見をノウハウとしてまとめ，適時情報共有していく予定です．

目的	実施主体	実施内容
① www.accsjp.or.jp へのアクセスを集計	ACCS	1 年前に閉鎖した ACCS サイト「www.accsjp.or.jp」に大量のアクセスをしている PC は Antinny に感染している可能性が高いと想定．攻撃以外の Web アクセスが含まれている www2 へのアクセスは集計の対象外とした．
②アクセスを分析	ACCS	ブラウザを使ったアクセス頻度を著しく上回る送信元 IP アドレスを分析し，ISP のアドレスレンジごとに整理した．
③該当 ISP へ対応依頼	ACCS	注意喚起メッセージを自社の契約者に届けることについて，協力を申し出た Telecom-ISAC Japan 会員の ISP に，Antinny 感染者への注意喚起を依頼した．
④ IP アドレス使用者の調査	ISP	ACCS から依頼を受けた，IP アドレスについて，ACCS サイトへのアクセスログのタイムスタンプから，契約者を特定した．
⑤トラッキング ID の生成・登録	ISP	注意喚起メールを受け取ったユーザからの問合せ対応や，Web サイトへのアクセス状況の確認を円滑に行うために，注意喚起を行う契約者ごとに識別子（乱数）を生成した．ユーザごとの識別子を注意喚起サイトに通知する．※注意喚起サイトでは識別子のみを管理しユーザ名等の個別の情報は一切関与しない．
⑥注意喚起メールの送信	ISP	注意喚起メールには，Antinny に感染している可能性や，セキュリティ対策について整理された Web サイトが紹介されており，ユーザごとに準備された Web サイトの URL が書かれている．
⑦対策実施	ユーザ	メールを読んだユーザが対策サイトにアクセスし，Antinny の駆除や Windows アップデートを行い，対策完了ボタンを押す．対策サイトは Telecom-ISAC Japan・マイクロソフト・トレンドマイクロが構築し連携し提供している．
⑧完了連絡	Telecom-ISAC Japan	注意喚起したユーザが対策サイトにアクセスしたログは，トラッキング ID ごとに整理して蓄積し，ISP からの問合せに対応できるようにした．
⑨進捗状況の確認	Telecom-ISAC Japan ISP	対策サイトへのアクセス状況は，トラッキング ID ごとに集計され，ISP に届けられる．ISP はトラッキング ID とユーザを紐づけることで，ユーザからの問合せに円滑に応えることが可能となる．
⑩完了連絡，対策不備等の方への再注意喚起の実施	ISP	ACCS への攻撃や，ユーザ本人の情報漏洩のリスクが高い状況のため，対策サイトへのアクセスが確認できないユーザや，対策サイトの途中で動きが止まったユーザに対しては，再度の注意喚起や問合せ対応ができるように ISP での対応体制を構築した．

表 -2　Antinny 対策サイト・システムの運用フロー

この発表直後から，Antinny 対策について我が国の主要な省庁や企業が呼応し，連携した動きを始めた．内閣官房情報セキュリティセンター，総務省，経済産業省などの中央省庁とも相談し，3 月 15 日に一斉に啓発活動を行うことになった．

■ 2006 年 3 月 15 日

官民のセキュリティ関係者が一斉に報道発表や記者会見を行い，Winny 使用に関する警鐘を鳴らし，大きくニュースにも取り上げられた．NHK はニュースに取り上げるだけでなく，積極的に特別番組を編成しその役目を担った．この注意喚起で特筆すべきは，各々の関係者の立場が異なる点である．Telecom-ISAC Japan は DDoS 対策を主眼に置きつつ，マルウェアに感染した被害者が，第三者を攻撃する加害者になる点を訴求した．これに対して政府中央省庁は個人情報漏洩や機密情報漏洩と，漏洩した情報が個人のプライバシーや著作権等の権利を侵害しており社会問題化していることに対する対策を訴え，マイクロソフトは OS のアップデートによるセキュリティ対策レベルの向上を，トレンドマイクロはマルウェア対策の重要性を訴えた．特に大きな動きを見せたのは，内閣官房情報セキュリティセンターであった．当時の内閣総理大臣小泉純一郎氏と内閣官房長官の安倍晋三氏をして，Winny 不使用について記者発表をさせ，世の中に広く浸透させる取り組みを行った（図 -16）．この動きの背景には，日本の情報セキュリティレベル向上に取り組む有志団体である「亀山社中」の関係者が奔走し，利害が対立しがちな中央省庁と競合関係にある民間企業をまとめ，まさに日本を 1 つにする取り組みを行っていたことがある．

NHK 等のニュースに取り上げられるつど，Telecom-ISAC Japan が構築した「対策サイト」には DDoS 攻撃を思わせる激しいアクセスが殺到した．図 -17 は対策サイトへの Web アクセス数と NHK ニュースの放映時刻との相関を示すべくグラフ化したものである．また同時刻帯の Web 応答時間も併記しているが，ニュース報道により多くのユーザが行動を起こして，Web サイトを閲覧している様子が窺える．やや不謹慎な表現であるが，DDoS 対策を目的として，Antinny の駆除ツールを感染被疑者に提供する注意喚起を行い，セキュリテ

ィ対策の啓発を行う対策サイトを運用してきたが，Telecom-ISAC Japan の「対策サイト」に DDoS 攻撃を思わせる激しいアクセスが押し寄せることは想定外であった．当時の Web サイト管理者がサービス継続に四苦八苦していたことに感謝したい．

なお，このニュース報道や NHK の特集番組の編成は，Telecom-ISAC Japan の会員 ISP が行った Antinny 感染被疑者への注意喚起メッセージをより効果的なものにしたと考えられる．

図 -16
2006 年 3 月 15 日，NHK ニュースの報道例（日本放送協会 Web ページより）

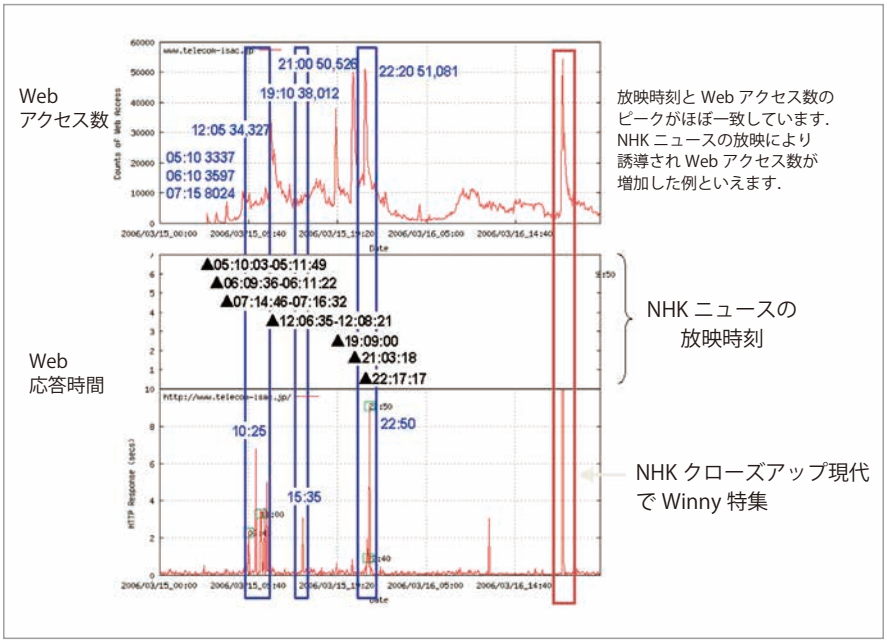

図 - 17　ニュース報道と Web アクセスの関係

■ 2006 年 6 月

官民連携して行った一連の対策の成果を Telecom-ISAC Japan と ACCS が振り返って分析してみたところ，www.accsjp.or.jp への攻撃は，図 -18 が示すとおり 2005 年 10 月から 2006 年 6 月では 54% 減少していることが明らかになった．

2005 年 10 月のマイクロソフトが行った MSRT による Antinny の一斉駆除以降，毎月増加傾向にあった攻撃が 2006 年 3 月以降は減少傾向に転じている．2006 年 1 月～ 3 月の期間は「4 月 4 日」などの「ゾロ目日」に攻撃を行う亜種の活動が停止していたためグラフに欠損が見られるが，2006 年 2 月をピークに攻撃は減少し続けていることが見てとれる．

注意喚起の成果については，Antinny 感染者に注意喚起を行った ISP の IP アドレスからの攻撃通信の減少度合いで評価したところ，注意喚起を行った ISP では IIJ：68%，Nifty：74%，OCN：64% と全体平均 54% と比較し大幅な減少となった．

対策サイトの成果については，注意喚起を行うユーザごとに設定したトラッキング ID を追跡し，注意喚起メッセージを受け取ったユーザの行動を分析したところ，ISP により差はあるものの，注意喚起メッセージを送付したユーザの 30 ～ 50%が「対策サイト」を訪問し，その約 50%程度のユーザがさらに Antinny の駆除ツールのダウンロードサイトにアクセスしていることが判明した．一般的に ISP からのメールを好んで開封するユーザは

少なく，その反応率は数％程度とも言われているが，今回の注意喚起メールに対してはニュース報道も手伝ってか，30 ～ 50％と高い割合でユーザの行動に繋がっていることは特筆に値する．

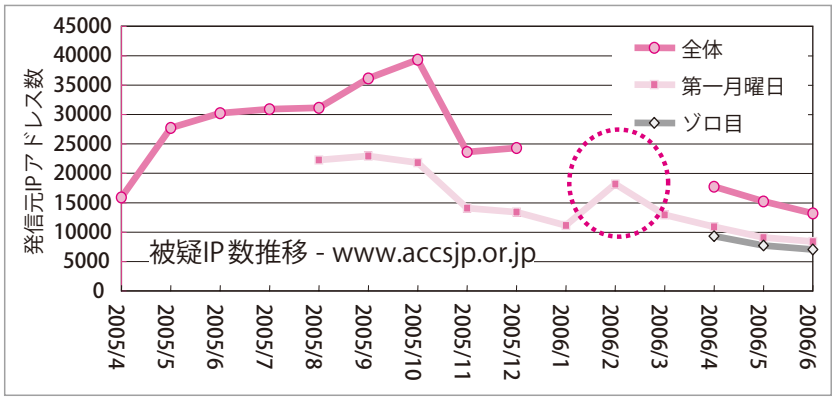

図 -18　www.accsjp.or.jp に対する攻撃通信の変化

■ 2006 年 6 月 1 日

Antinny 対応への取り組みが評価され，マイクロソフト社が「平成 18 年度 情報通信月間 総務大臣表彰」を受賞した．

■ 2006 年 12 月 13 日

これら Antinny 対策の取り組みが契機となり，2006 年 12 月にサイバークリーンセンターが設立された．サイバークリーンセンターは総務省と経済産業省が連携した「ボット対策事業」であり，2006 年から 5 カ年継続し世界的にも「マルウェア対策」の手本となった取り組みである [3]．

■ 2007 年 5 月 30 日

一方で，このような DDoS 対策に対して ISP がかかわる際の注意事項をまとめた業界ガイドラインの執筆が始まり，「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」が 2007 年 5 月 30 日に策定され，ISP 間で共有された．現在は第 2 版（2011 年 3 月 25 日）となり業界ガイドラインとして広く公開されている [4]．

エピローグ

残念なことにこの DDoS 観察日記が終わる 2006 年 6 月時点では，ACCS への攻撃は 50％以上減少したものの，ACCS サイトへの攻撃が激増し始めた 1 年前のレベルに戻したにとどまっており，ACCS サイトには依然大量の攻撃が押し寄せていた．上位 ISP である OCN が設置した DDoS 対策装置が ACCS サイトへの通信を浄化し DDoS 攻撃をブロッキングしていたため，ACCS サイトの事業継続は保たれていたが，DDoS 対策装置を止めると瞬時にダウンさせられてしまうほどの状況はこの後もしばらく継続する．世の中からは一定の成果を得た今回の取り組みであるが，ISP 間ではさまざまな課題を残す結果となった．

ACCS は Winny における著作権侵害対策を行っており，その関連で Antinny およびその亜種の製作者が ACCS をターゲットにすることを考え，その結果，過剰なアクセスを行う結果に繋がったと思われる．過去にも互いの利害関係から当事者間やその関係者間でインターネット越しに攻撃をしあうようなケースは珍しいことではなかった．現在でも日常茶飯事と言えよう．しかし，ACCS サイトのように感染拡大をしていくマルウェアに攻撃された事例の中でも，ここまで長期化した例は稀であり，ISP にとってこのようなユーザの存在は，過大な通信を発生させ ISP の収支を圧迫し，時には安定した通信サービスの提供を阻害する点では，大きなリスク要素である．

ISP はサービス提供約款に基づき，ACCS のような過大な通信を行い，他のユーザ通信に障害を与えるユーザを解約することは可能である．しかし，ACCS のようなセキュリティ対策面での弱者を ISP 間でたらい回しにしても何の解決にもならない．また ISP が民間企業である限り，正義の味方として ACCS を救済し続けることはできない．いくら費用対効果の高い対策を打てたとしても，収入に結び付かなければ長続きはしない．この DDoS 対策のコストは誰が負担すべきか，今一度冷静に考える必要がある．

一方で，法律的な問題もある．ISP 各社は，2004 年 3 月に Antinny が ISP 各社の DNS サーバを超負荷

状態に陥れ，安定的なサービス提供ができない可能性があったため，通信の秘密に配慮しながら，さまざまな対策を行ってきた．しかし，ISP 各社が DNS サーバを増強したり，OCN が自社コストで導入した DDoS 対策装置により攻撃の負荷が減少し，自社サービスへの支障が無視できる範囲に低減した時点で，このような行為の妥当性が問われる可能性がある．費用対効果に見合わないとの理由から，OCN が撤去した場合は再度インターネットが混乱する可能性は残っているが，さりとてそのコストはだれが負担するのか整理されてもいない．

健全なインターネットの発展を考えた場合は，ネットワークの安定運用と ISP と利用者の果たすべき役割について，またインターネットは国跨りの通信が前提と考えると，民間だけではなく国の果たす役割について，立ち止まって考える時期に来ているのかもしれない．

今回は DDoS 攻撃への ISP 目線を中心に「DDoS 攻撃観察日記」をまとめた．一方で攻撃を受けた被害者である ACCS がどのような被害を受けたのかについて紙面を割くことができなかったため，巻末であるが簡単に紹介したい．

ACCS では，Web サイトを利用した情報発信と情報収集を行っている．このため，特に DDoS 攻撃活動が活発であった 2004 年 3 月から 2006 年末までは，Web サイトを安定して運用することができず，さまざまな事業活動に影響を及ぼしている．

(1) ACCS の認知に関する影響

ACCS の名称を，出版物やニュースなどで知った一般の方が，活動概要などを調べることができなくなった．また，ソフトウェアの不正使用を防止するために行うソフトウェア管理に関する情報や資料を配布することができなくなった．

(2) 収益事業に関する影響

ACCS の収益事業であるセミナへの参加申し込みや講師派遣の依頼，書籍の販売などを行うことができなくなったため，収益が減少した．

(3) 広報活動に関する影響

著作権侵害に関する事件リリース，ACCS が主催するセミナや講師派遣などの募集，新たに発行した書籍の紹介などができなくなった．その上，これらを広報するために，FAX やダイレクトメールなどを利用し，そのための費用がかかることとなった．

(4) ソフトウェアの不正使用情報の収集に関する影響

ソフトウェアの不正使用情報を収集し傾向と対策を検討していくことができなくなった．特に，企業など組織内における不正使用の情報は，当協会が独自に調査することでは発覚せず，一般からの情報提供に頼らざるを得ない．情報収集することができなくなることは，組織内における不正使用への対策がまったく行えなくなることと同義であり深刻な問題である．しかも，URL を「www」から「www2」に変更したことによって，DDoS 攻撃が行われていない期間であっても，アクセス数は 1 日数百アクセスまで減少しており，情報提供数も DDoS 攻撃前の約半数にまで激減していた．

参考文献

1) ACCS : ACCS ホームページの URL 変更について，http://www2.accsjp.or.jp/activities/2004/news36.php
2) Telecom-ISAC Japan : ISP との連携による ANTINNY ウイルス感染ユーザへの注意喚起の取り組み，https://www.telecom-isac.jp/news/news20060315.html
3) サイバークリーンセンター，https://www.ccc.go.jp/
4) JAIPA : 電気通信事業者における大量通信等への対処と通信の秘密に関するガイドラインの改定について，http://www.jaipa.or.jp/topics/?p=400

(2013 年 1 月 8 日受付)

謝辞 この Antinny 対策は Telecom-ISACJapan がかかわった DDoS 対策事例の中でも長期間継続的に取り組まれたことから，さまざまな知見を蓄えることができた．この場を借りてご尽力いただいた当事者ならびに関係者の皆様と執筆の機会をいただいた日立製作所の寺田真敏氏に感謝の意を表する．

■小山 覚 skoyama@nttpc.co.jp
(株) NTTPC コミュニケーションズ カスタマサービス部長．

■中川文憲 fuminori@accsjp.or.jp
一般社団法人コンピュータソフトウェア著作権協会（ACCS）戦略法務室 室長．