DDoS等の動向と異常トラフィック対策技術の実用化に向けた取り組み

雨宮 俊一（あめみや しゅんいち） /渡瀬 順平（わたせ じゅんぺい）
NTT研究企画部門

本稿では，DDoSやSPITと呼ばれる異常トラフィックに関する脅威の動向，およびNTT研究所の実用化に向けた取り組みを紹介します．

はじめに

近年のブロードバンドの普及や業務のICTへの依存が高まり，組織にとってセキュリティ確保は重要な課題となっています．ICT技術が発展するに伴い複雑化するセキュリティ問題に対して，セキュリティ対策技術や対策製品・サービスの選択肢が増え，さまざまな脅威に対処できるようになってきました．一方，古くから脅威として認識されていたものの，まだ根本的な対処が確立されていないものにDDoS等の異常トラフィック系の脅威があります．本稿では，DDoSやSPITに関する動向，および対策システムの実用化に向けた取り組みを紹介します．

セキュリティ脅威

まず，セキュリティ脅威は，**図1**のように，脅威が意図的に引き起こされたものなのか，それとも，過失，自然現象によって引き起こされたものなのかによって，また，脅威の発生原因が内部に起因するのか，外部に起因するのかによっても分類されます．

最近では，個人情報保護や内部統制対応といったコンプライアンス強化のため，内部不正対策としての端末から外部記録媒体への書き出しを禁止する製品，メールの送受信を記録する製品や端末の紛失対策としてモバイルシンクライアント等，内的要因に関する脅威に対するセキュリティ製品・サービスが注目を集めています．

一方で，外的要因に関する脅威も，年々，ますます複雑化，多様化，巧妙化してきています．IPA（情報処理推進機構）の『情報セキュリティ白書2007年版』では，最近の動向を「脅威の“見えない化”が加速する！」というキャッチフレーズで表しています[(1)]．

ボット等のマルウェアに関しては，感染した際にDDoS攻撃やスパムメール発信のための踏み台とされ，他人に多大な迷惑をかけることになるなどと悪質化しています．一方このようなマルウェアは，多種多様になっており，ウイルス対策ソフトでも検出が困難になってきていること，従来のウイルスのように感染しても利用者に分かる不審な挙動を示さないことにより，感染した事実に気付くことが難しくなっていく傾向にあります．

外的要因に起因する脅威である不正

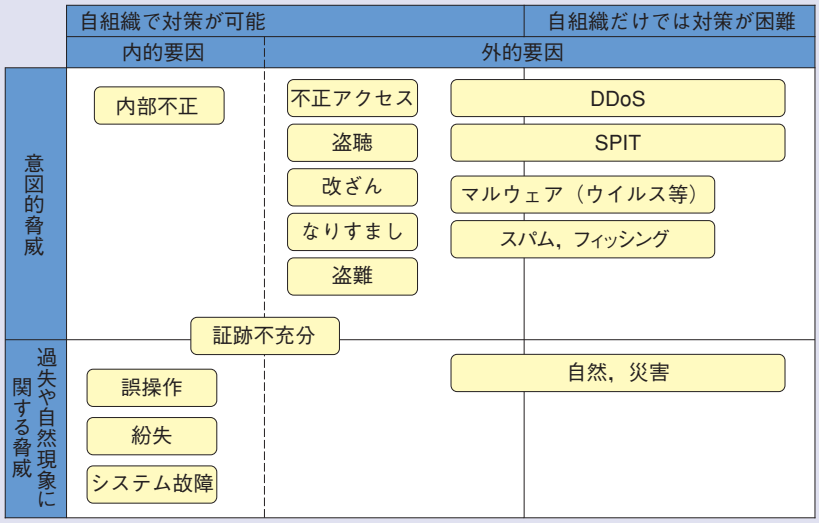

図1　セキュリティ脅威

アクセス，盗聴，改ざん，なりすましといった脅威は，例えばその組織にファイアウォールを導入すれば対処が可能となります．これらの脅威に対しては，セキュリティ製品やサービスも豊富に存在し，組織がきちんとセキュリティ人材やセキュリティ予算の割り当てといったリソースの手当てを行えば，対策を実施することが容易になってきています．一方，DDoS，SPIT等は，利用者組織だけで取れる対策に限りがあり，通信サービス事業者と連携するなど，幅広い関係者と連携したうえでないと対処が難しい脅威となっています．

DDoS攻撃等について

■DDoS攻撃

ここでDDoSとは何かを整理します．DoSとは，Denial of Serviceの略称で，サービス拒否攻撃，サービス妨害攻撃，サービス不能攻撃とさまざまな呼ばれ方があります．意味のないパケットを大量に送り付けることで，大量トラフィックによりネットワーク帯域を使い切る，異常なパケットや不正な要求によりサーバやサービスをクラッシュさせる，大量な要求によりサーバの処理リソースを使い切る等の被害を与える攻撃を総称して，DoSといいます．DDoSというのは，Distributed DoSの略称で複数の拠点から行われるDoS攻撃を指します．典型的には，攻撃者は攻撃が特定されにくいように攻撃者の制御下にあるボット等に感染した不特定多数のPCを介して，サーバにDDoS攻撃を仕掛けます．

DoS攻撃には，大量のパケットを送信する攻撃，プロトコルの脆弱性をつく攻撃に大きく分類されます（**表**）．大量のパケットを送信する攻撃には，SYN Flood，UDP Flood，Smurfと呼ばれる攻撃があります．警察庁が観測しているbotnetにおいて，攻撃者の指令サーバから出されるDDoS攻撃命令のうち約80％がSYN Floodに関するものという統計もあります[(2)]．プロトコルの脆弱性をつくタイプの攻撃にはPing of Deathと呼ばれる攻撃があり，比較的少量のパケットでサービスの反応を遅くさせたり，停止させたりすることが可能であり，一撃で大きな損害を与えます．

DDoS攻撃の検知技術が進展しているため，市販製品でも上記に挙げたような攻撃を検知できるようになってきていますが，誤検知も発生し，いかに正確に検知できるかが課題となっています．最近は，アノマリ分析といったネットワークの正常なトラフィックの状態を曜日や時間帯単位で学習し，誤検知を少なくするような分析技術を搭載した製品も出てきています．

■IP電話サービスに対する攻撃

IP電話サービスに対する攻撃のうちSPITと呼ばれるものがあります．SPITとは，SPAM over IP Telephonyの略称であり，名称のとおり，IP電話上のスパム（迷惑電話）のことを意味します．SPIT攻撃が発生した場合には，電子メールのスパムと異なり，電話のベルが鳴り受話器を取らなければならないといったユーザに物理的な手間を取らせることになります．SPIT対策の課題としては，通話はリアルタイムでなされるため処理速度に対する要求が厳しいこと，スパム対策のようなコンテンツフィルタリングが難しいことが挙げられます．

SPIT以外にもIP電話においては，ワンギリ，電話番号のスキャン，IP電話を構成する機器へのDDoS攻撃，Fuzzing攻撃（プログラムの不具合を誘発することを目的とした不正形式のメッセージを含むパケットを送り込む攻撃手法）[(3)]といった攻撃があります．

表　DDoS攻撃，IP電話サービスへの攻撃例

	サーバへのDDoS攻撃	IP電話サービスへの攻撃
大量のパケットを送信する攻撃	SYN Flood, UDP Flood, Smurf, Connection Flood, HTTP Get Flood	・ワンギリ，電話番号のスキャン ・IP電話を構成する機器へのDDoS攻撃 ・SPIT，迷惑電話
プロトコルの脆弱性をつく攻撃	Ping of Death，Teardrop	・Fuzzing

DDoS等の攻撃の動向

DDoSやSPITについては，被害を受けた組織が詳細を公表したがらないということもあり，なかなかその頻度や被害の大きさといったことの実態がつかみにくい状況にあります．ここでは，海外や国内の調査結果で公表されている事項について紹介します（**図2**）．

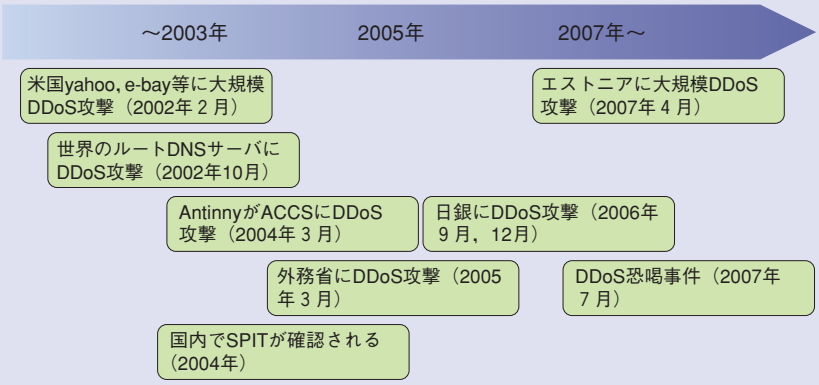

図2　DDoS，SPIT攻撃の動向

■DDoS攻撃の動向

DoS攻撃に関しては，CSI（Computer Security Institute）の『The 12th Annual Computer Crime and Security Survey』[(4)]によると，米国企業の25%が1年以内にDoS攻撃を受けたと認識しており，1社当り1万4 890米ドルの被害を受けているとされています．この調査によると2003年に約40%超あったDoS攻撃が2007年には25%までに減少していることがうかがえます．ただし，これは全般的にセキュリティインシデントの被害件数自体も減っていることもあり，DoS攻撃だけが減ったということではないようです．

IPAの『2006年 国内における情報セキュリティ事象被害状況調査報告書』[(5)]によると，日本企業においても3.7%がDoS攻撃による被害経験があると回答しています．JPCERT/CC（Japan Computer Emergency Response Team/Coordination Center）の『標的型攻撃について』[(6)]によると，標的型攻撃としてDoSをしかけるという脅迫メールを受けた企業の割合が1.2%存在し，標的型攻撃の被害としてDoSを受けたという回答が25%と高い割合を占めています．今後，標的型攻撃が増加していくという予測がある中，DoS対策も無視できなくなるものと思われます．

また，2007年には，エストニアで大規模なDDoS攻撃がなされ政府や金融機関が被害を受けたり，国内ではDDoS攻撃を止めてほしければ金銭を払えと恐喝する事件も発生しており，さまざまな対策により，被害件数が減少しているとはいえ，むしろ大規模化したり，金銭目的で悪質化する傾向にあり，注意が必要です．

DoS攻撃は，必ずしも政府機関や官公庁や大規模商業サイトだけが攻撃対象となっているわけではなく，インターネットに接続しているどんな組織においても起こり得る攻撃ですので，今後ますます対策が必要となっていくものと思われます．

■IP電話サービス攻撃の動向

2004～2005年にかけて国内のIP電話事業者にSPITが出始めたと報道されています．また，IP電話サービスに対する攻撃に悪用可能なツールがインターネットで公開されるなど，IP電話サービスに対する攻撃の障壁が下がっていくことが予測されます．その後，IP電話を使ったフィッシング詐欺が発生したりしていますが，IP電話サービスに対する大規模な攻撃による被害というのは報道されていないようです．今後IP電話ユーザが増加するに伴い，脅威が深刻化する可能性があります．

総務省で2007年1月に実施された電気通信事業分野におけるサイバー攻撃対応演習の中でも，DDoS攻撃への対応演習のほかにSPIT攻撃への対応演習も実施されるなど，官民ともに対

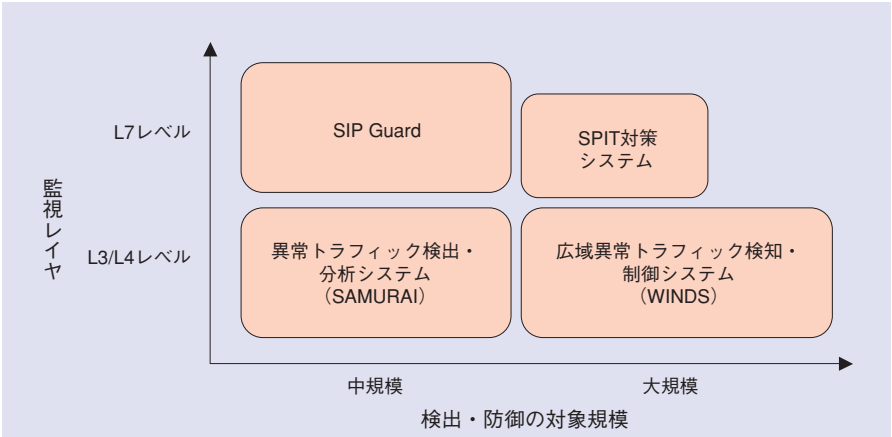

図 3　NTT研究所の取り組み

応の準備を進めているところです．

DDoS等に対する取り組み

NTT研究所では，DDoSやSPITというような異常トラフィックに対する対策技術として，**図 3** に示すようにTCP/IPレイヤでの異常検知が可能な技術として「異常トラフィック検出・分析システム（SAMURAI）」「広域異常トラフィック検知・制御システム（WINDS）」があり，SIPレイヤで異常検知が可能な技術として「SIP Guard」「SPIT対策システム」があります．「WINDS」や「SPIT対策システム」は，より大規模な異常や攻撃に対して検知が可能となっています．広域異常トラフィック検知・制御システム（WINDS）に関しては，参考文献⑺に解説がありますので，そちらをご覧ください．それ以外の技術の特徴等については，本特集の他の記事で詳しく説明します．NTT研究所では，さまざまなシーンにおいて異常トラフィックに対処できるよう，対策技術の研究および実用化を進めています．

ま と め

本稿では，最近のDDoSやSPITの動向，およびNTT研究所が開発したそれらの対策技術を紹介しました．

DDoS対策システム（SAMURAI）は，NTTコミュニケーションズにおいて機能強化等を行い，商品化することになっています．本特集ではこの後，DDoSやSPITに対する対策技術の解説とともに，実際のネットワークへの導入や運用イメージなどを紹介します．

NTT研究所では，DDoSやSPITといった脅威に対する対策技術の研究および実用化を通じて，皆様がネットワークを快適に利用できる環境を実現していく予定です．

■参考文献
⑴ http://www.ipa.go.jp/security/vuln/documents/2006/ISwhitepaper2007.pdf
⑵ 警察庁：“平成19年のサイバーフォースセンターでの観測結果について，”2008. 2.
⑶ IPA：“SIPに係る既知の脆弱性に関する調査報告書，”2007. 12.
⑷ http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf
⑸ http://www.ipa.go.jp/security/fy18/reports/virus-survey/documents/2006_virus_domestic.pdf
⑹ http://www.jpcert.or.jp/research/2007/targeted_attack.pdf
⑺ 西田・村山・石橋・小林：“広域異常トラヒック検知・制御システム（WINDS）のアーキテクチャ，”NTT技術ジャーナル，Vol.20, No.3, pp.12-15, 2008.

（左から）雨宮　俊一/ 渡瀬　順平

NTT研究企画部門セキュリティプロデュース担当では，研究所のセキュリティ関連技術のプロモーションや事業会社のビジネスにつなげていくための活動を行っています．

◆問い合わせ先
NTT研究企画部門
プロデュース担当
TEL　03-5205-5816
FAX　03-5205-5369
E-mail　s.amemiya@hco.ntt.co.jp