セキュリティポリシーと電子メール

武藏 泰雄
熊本大学総合情報基盤センター･ネットコミュニケーション研究部

概要：熊本大学へのセキュリティポリシーの導入事例、基本ポリシー･実施手順書の策定事例、メールサーバにおけるスパムメール対策の現状、およびスパムボットの検知対策について考察したので報告したい。

キーワード：セキュリティポリシー、スパムメール対策、スパムボット検知

1. 緒言

電子メールは大学等の高等教育機関においては重要なインフラとなっている。例えば、メールで学生からレポートを受け取ったり、あるいは講義開催期日の変更などを通知したりする。また論文の投稿から掲載可否の通知から、学内の研究の打ち合わせまで、様々な場面で活用されているので、電気やガスと同様に既にインフラとなっている。

しかしながら、上記の様にインフラでありながら大学の経営側からは通常インフラとみなされていないので、予算措置などにおいては、その恒常性の高い支援は得られていない現状がある。

更に悪いことに、最近ではメールサーバの運用は複雑で非常に困難になってきている。その理由の一つとしてスパムメールの対策が挙げられる。スパムメールの目的は、大量の電子メールを送りつけ、出会い系サイトやE-コマースサイトへ誘導し紹介料を稼ぐことにある。

スパムメールはそのメール送信の大量性により様々な問題を引き起こしている。例えば、毎日一人あたりでも、数百通にのぼるスパムメールを受信させられることもある。筆者の場合は、平日は約70-80%、また土日祝日は、90-100%がスパムメールである。それにメールサーバ側で本格的なスパム対策を施すには、特別仕様のハードウェアで構成されたサーバが必要になることもあり、更にサーバ周辺のネットワークの構成変更が必要になることもある。

今回は、スパムメール対策を用意周到に行うために、大学に情報セキュリティポリシーを導入させ、メールサーバやPC端末側における本格的な技術対策について簡単に紹介し、今後どのようなソフト面での対策と技術面での対策を講じれば良いか考察する。

ところで大学におけるセキュリティポリシーに関する話題としては、2005年9月に内閣官房情報セキュリティセンターから示された「政府機関の情報セキュリティ対策のための統一基準」への対応が挙げられるだろう[1]。その後国立情報学研究所が中心となり、サンプル規定集が作られた[2]。また大学全体としてISMS（ISO27001）取得を目指す動きを見せる大学も現れている[3]。

大学における電子メールの話題にとしては、スパムメール対策が挙げられ、主として2つの対策があり、一つはスパムメールを受信しない（メールサーバ側の対策）対策であり、もう一つはスパムを送信しない対策（メールサーバ側の対策とスパムボットへの対策）がある。

2. 大学のセキュリティポリシー

2.1「政府機関の情報セキュリティ対策のための統一基準」への対応

政府の統一基準について大学内の何人かでこれを読んで見たところ、非常に良くまとまっていて、完成度は高いように思えた。次に国立情報学研究所が中心となり、政府の統一基準について、大学用へ変換する作業が行われ、サンプル規定集が発表された。このサンプル規定は当初は、300ページ程度だったのであるが、最終的には約600ページにわたるもので精読するに相当な人的リソースと時間を要すると考えられた。熊本大学では、せっかくのサンプル規定集であるので、できるだけこれに準拠できるように、精査中である。ぱっと一読した限りでは、詳細な検討がされており、導入コストが低いように思えるが、しかしながら、サンプル規定集をベースにした導入事例が、実際はあるのかも知れないが、私の知る限りでは、まだ見当たらない。

一方で、少数であるが、一部の大学の中には、まず情報基盤を管理する部門などで

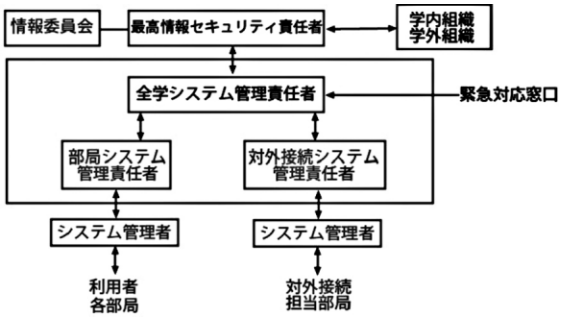

図1　情報セキュリティポリシーと各組織図

ISMS（ISO27001）を取得し、これを大学全体へスケールアップしようと試みる大学が現れてきた。例えば静岡大学の場合がそれであり、ISMSの取得のみならず、電気代節約のためのグリーンIT [4] や事業継続性（BCP）のため戦略的SaaSをも試みているところが興味深い。今後その動向を注視したい。しかしながらこれを取得しても構成員への教育周知徹底は非常に困難を伴い、取得してもセキュリティを守れなかったという痛い事例も実際にある。

2.2 熊本大学へのセキュリティポリシーと実施手順書の導入事例

熊本大学では2001年8月～2003年2月の期間にセキュリティポリシーの基本ポリシーとスタンダードの策定作業を、また2003年6月～2004年3月の期間に実施手順書の策定作業を行った。

基本ポリシーとスタンダードにおいて参考にしたのは、2002年4月に配布された「大学における情報セキュリティポリシー」と呼ばれる雛形であり、これをベースにして原案を作って提出したが、熊本大学の情報推進専門委員会および上部組織である情報推進化会議で了承された。この基本ポリシーとスタンダードは、図1に示すような組織を作り、目標や対象範囲、そして対策基準からなる文書で構成されている。また図2には、実際基本ポリシーとスタンダードの内容を示している。

さてこの基本ポリシーとスタンダードの原案であるが、学内から特段の反発もなくスムーズに承認していただいた。それで実施手順書もスムーズに行くだろうと思っていたのだが、別の大学から情報をいただいたところ、基本ポリシーやスタンダードを承認するのも大変だったのに加え、実施手順書については更に強く反発されたとのことであった。そのため当大学でも大変なことになるだろうと予

A. 情報セキュリティポリシーの内容
・目標
　情報セキュリティに対する侵害を阻止
　学内外の情報セキュリティを損ねる加害行為を禁止
　情報資産に関して、重要度による分類とそれに見合った管理
　情報セキュリティに関する情報取得の支援
・対象・範囲
　教職員、学生、来学者、外部委託事業者等
システム管理者（研究室のPCなどは教職員）
　外部から持ち込まれたPCも含む
　情報システムは24時間365日稼動
・対策基準
　組織・体制
　情報の分類と管理
　物理的セキュリティ
　人的セキュリティ
　技術的セキュリティ
　評価・見直し

図2　情報セキュリティポリシーの内容

想された。実施手順書は、基本ポリシーとスタンダードを実現するための手順書であるため、直接大学の構成員に負荷がかかる。この負荷がかかることが、大きな反発の要因と考えられる。また実際のその文書量が多ければ、つまり見た目が悪ければ反発されるのは必至である。

取り敢えずこの情報を踏まえた上で、もらった雛型を敢えてそのまま利用して、57頁もある実施手順書案を作成し、情報化推進専門委員会へ望んだ。すると予想通りに、大きな反発が出る結果となった。

そのため2004年1月～3月の期間にメーリングリスト上で、情報化推進専門委員による継続審議となったのである。いずれにしてもこの情報推進委員会で承認を得れば、大学全体で情報セキュリティポリシーとその実施手順書が認められたことになる。

筆者は、実施手順書案を眺めているうちに、情報を圧縮するための何らかのモデルの必要性があると感じ始めた。実際データの分類の事項が多く、恐らくこの辺りを弄れば良いというところまで判って来た。そして情報セキュリティポリシーの対策基準のところで（図2）、「情報の分類と管理」という項目があり、そこに「非公開情報」という言葉があったこと、またその当時個人情報漏洩事件が頻発していたことからヒントを得て、大学におけるデータ資産の分類を「公開データ」と「非公開データ」という単純なモデルに分類することで、実施手順書を圧縮することができることに気付いた。実際このモデルを当てはめて、文書の不要部分を削り、圧縮を試みたところ、

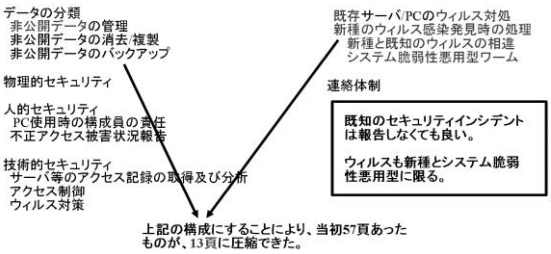

図3　実施手順書の文書量を減らすテクニック

当初57頁が13頁になった。

「公開データ」と「非公開データ」は下記のように定義した。

・公開データ
　データの漏洩（流出）により、該当データの作成者（管理者）、データの利用者および大学へ不利益が生じないものであり、公開可能なデータと定義する。
・非公開データ
　個人情報や大学の運営に関る重要な機密情報を含むものと定義する。

「公開データ」では、理想的には個人情報をまったく含まないデータを意味する。現実的には多少の個人情報を含んでいても公開しないといけないデータも含めている。また「非公開データ」は、具体的には、学務情報（SOSEKI）や附属病院、保健センター等の診療に関する情報、大学の財務、経理、ネットワークIPアドレスや全学向けサーバ、メールサーバ、研究目的で知り得るところの企業秘密やログ情報、情報の非公開契約をした情報が含まれているデータということになる。

この様な単純な情報資産データの定義で良いのかという反論はあったが、大学という組織で、情報セキュリティを実施するためには当時としては仕方がなかったという点がある。また当時データ分類では、まずは単純なものにしてから、後で厳密なものして行けば良いのではないかという雰囲気も感じられたこともあって、この様な単純な案を提案してみた。すると予想に則して、情報化推進委員らへの受けも良く、なんと次回の委員会で承認するというところまで漕ぎ着けることができた。情報セキュリティポリシーの策定に関連する実質的な作業はここで終わった。

この顛末は、2004年9月に国立情報学研究所の一橋記念講堂で開かれた文部科学省･情報セキュリティセミナー [5] で発表した。この発表後、その反響は大きく、他大学の先生方から発

プロセス	手続きを行う者	手続き
(I) システムログ提出の依頼	全学システム管理責任者	• 「サーバ及びネットワークのアクセスに関するシステムログ提出依頼書」に必要事項を記入する。 • 記入済みの依頼書を部局情報セキュリティ責任者に依頼する。
(II) ログ採取依頼	部局情報セキュリティ責任者	• 依頼書に基づき該当するシステムを管理するシステム管理者へログの採取を依頼する。
(III) ログの採取	システム管理者	• ログを提出形式の媒体等に採取、部局情報セキュリティ責任者に提出する。
(IV) ログの提出	部局情報セキュリティ責任者	• ログの記録された媒体等と依頼書を全学システム管理責任者に提出する。
(V) 確認	全学システム管理責任者	• 提出されたログの解析を行う。

図4　不正アクセス被害状況報告手順

プロセス	手続きを行う者	手続き
(I) 連絡	構成員	• 不正アクセスを発見した場合、緊急連絡として部局システム管理責任者へ連絡し、指示を仰ぐ。 注1)システム管理者または部局システム管理責任者による連絡は、6.1.1「事案発生時の連絡」に従う。
(II) 報告	構成員	• 「不正アクセス被害状況報告書」に必要事項を記入する。 • 記入済の報告書をシステム管理者、部局システム管理責任者及び部局情報セキュリティ責任者が確認後、全学システム管理責任者に提出する。
(III) 確認	全学システム管理責任者	• 提出された報告書の記入内容を確認する。

図5　アクセス記録の取得及び分析手順

表内容についての問い合わせが多数あった。

2.3 熊本大学のセキュリティポリシーと実施手順書への戦略

前節では、如何にして「実施手順書」を全学へ通したかについて述べたが、ここでは、実施手順書へ含めるべき内容について説明したい。

当総合情報基盤センターでは、ネットワークの管理･設計やセキュリティインシデント対応などで多忙であり、しばしばセキュリティインシデントのトリアージが問題となることがあった。そこでこのトリアージが円滑に取り行われるように実施手順書で、最低限必要な文書作成事項を盛り込む必要がある。

具体的に言えば、(1) 不正アクセス被害状況報告、(2) サーバ等アクセス記録の取得及び分析、それに (3) 新種のウィルス感染発見時の処理などが挙げられる（図4-6)。当熊本大学では、実施手順書における文書作成はこの3点に絞っているところが最大の特徴である。このことによって雛形ベースの原案に大量にあった文書作成事項を減らすことがで

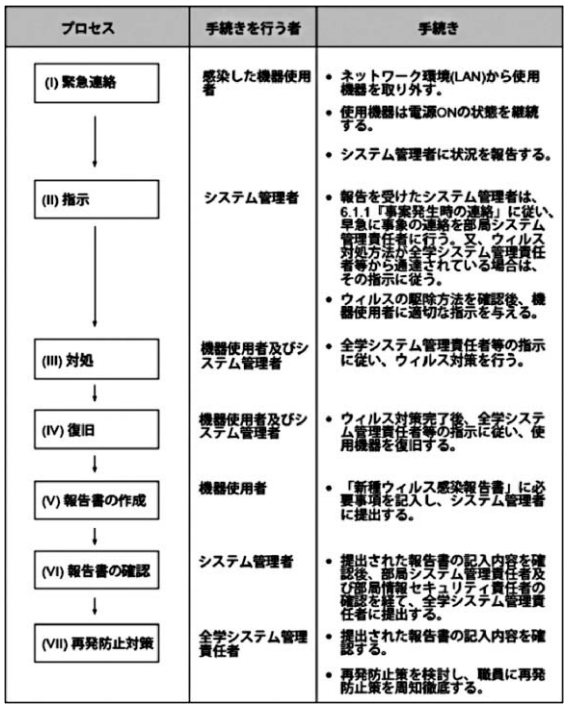

図6　新種のウィルス感染発見時の処理

き、結果的に実施手順書を圧縮するために大きく貢献した。当然であるが、実施手順書を作成した段階では不足する事項もあると考えられる。その場合は、当該事項についての予防対策を吟味して、そのための対応マニュアルを策定し、追加していけば良いとした。

ところで大学で大きな被害がでそうなセキュリティインシデントと言えば、サーバの乗っ取りと新種ウィルス感染拡大などが挙げられる。新種ではない、すなわち既知のウィルスの感染については、いわゆるワクチンソフトを導入すれば解決する問題と考えられるため、全学のサーバ管理者やネットワーク管理者がそのウィルスの駆除などへ直接対処するのではなく、PCの所有者側で適切に対応してもらい、最終的にはセキュリティインシデントとしては取り扱わないとするのである。当然ながらこの様な割り切った考え方については反発があったものの、人的資源確保や事務手続きの増大を理由にして議論を進めた結果、適当なところで折り合って決着させた。

逆にサーバの乗っ取り事件や新種のウィルスなどの感染事件は、学内外への大きな被害が出ることが懸念されるため、重要なインシデントであると位置付けることにした。またデジタルフォレンジックからの要請に応えるための準備のため、利用者認証やサーバのログの保存や取得、解析などが可能となるように実施手順書に明示しておくことにした。これは裁判などで法廷への電磁証拠の提出が日常となっており、そのためログなどの活動記録の保全や解析などは、当大学総合情報基盤センターの重要な業務となっているためである。

このように戦略的に実施手順書を構成することで、いつおこるかわからないセキュリティインシデントに備えることができると考えている。すなわち次に述べる「メールサーバにおけるスパム対策」において、このセキュリティポリシーがあったおかげでいろいろなインシデントの調査や対策の提案、実施運用など、またいわゆるインシデント対応が円滑に行えていると考える。また筆者は、いろいろな意味で、全学へ情報セキュリティポリシーを導入して良かったと感じている。

3.　メールサーバでのスパム対策

3.1　スパムメール対策

筆者はスパムメールを、平日で数百通から数千通、祝休日で数百通程度受信している。最近のスパムメールは、フィッシングメールが主で、怪しげなサイトへのリンクがメール本体へ張り込んであり、それをクリックすることで詐欺サイトへ誘導するものや、またウィルスそのものを埋め込んであるものが多くなっている。

メールサーバ側でのスパムメール対策としては、(1) スパムメールを受信しない対策と、(2) スパムメールを送信しない対策がある。また最近のスパムメールの発信は、(3) ウィルスやワームなどで乗っ取られたPCを悪用する、いわゆるボットによる発信が主流であり、そのボットと化したPCを検知して駆除していく対策がある。

3.2　スパムメールを受信しない対策技術

スパムメールをメールサーバ側で可能な限り受信しないためには下記の示すような、対策技術が知られている。

(1) ホワイトまたはブラックリストモデル
(2) コンテンツフィルタ
(3) 実装の際を利用したspam判定
(4) 遅延･通信流量制限
(5) 経験則による判定
(6) DNS経由の送信側MTAの正当性確認

まず（1）では、メールサーバのアクセス制御リスト（ACL）やリアルタイムブラックリスト（RBL）などのホワイトまたはブラックリストと呼ばれる、送信元MTA（Mail Transfer Agent：電子メールサーバ機能を持つプログラムなどを指す）のドメイン名や送信元IPアドレス（またはネットワークアドレス）単位で通信制御を行う対策技術が利用される。この対策技術は非常に単純な方式であるため、利用者にも管理者にも判りやすい、説明しやすい利点のある対策技術といえる。ただし、この対策技術では、メールサーバと認証管理（IDM）システムとの適切な連携がなければ、手動で管理することになるため、管理者に負荷がかかりやすい。またRBLは有効であるものの、政治的な圧力によって潰されるなどして、よく自然消滅するため、サーバ側の設定変更が必要となる。しかもこの自然消滅について管理者が迅速にそれを知る方法が現時点ではない。

（2）では、電子メールのメールヘッダ部分や本文の内容でスパムか否か判断する対策技術が用いられる。例えば、

- キーワードによる単純フィルタ技術：Spammassasin [6]
- 単語の生起確率によるベイジアン型学習フィルタ技術：Bogofilter [7] やBsfilter [8]
- URI Black Listを利用するフィルタ技術：URIBL [9]、Vipul's Razor [10]
- 利用者情報型公開データベースを利用するフィルタ技術：Web Mailer（Gmail等）

などがある。これらのフィルタ技術において特徴的なのは、その処理が高速であるということである。ただしコンテンツフィルタの大きな欠点は、スパムではないメールをスパムと誤判定する、いわゆるファルスポジティブの問題がある。このファルスポジティブの問題は最悪の場合政治的問題へ発展しやすく、その実装には利用者への徹底した周知や教育が必要となる。また最近では、メール本文を画像化してそれを添付することで、コンテンツフィルタを回避するスパムメールなどが出現しており、またそれらは増加傾向にあるため、それをスパムと判定できない、いわゆるファルスネガティブ（見逃すこと）も増加している。

（3）では、ボットなどスパムメールを送信するMTAはメールの再送処理、MXフォールバック判定やプロトコル違反によるメール再送処理にうまく対応できないと仮定してフィルタする技術が用いられる。例えば、

- 再送処理型対策技術：Greylisting [11]、お馴染みさん方式または一見さんお断り方式 [12]、S25R方式 [13]とも言われる対策技術
- MXリソースレコード処理型対策技術：MXフォールバック判定 [14]、Unlisting [15]、Nolisting [16]、GION [17]
- プロトコル違反型対策技術：Greeting pause、EHLO、HELOへのフォールバックチェック [18]

などがある。これらの対策技術の長所は、メール配送時の初期段階で、つまりSMTPエンベロープの段階で対策処理が可能なことである。SMTPエンベロープで処理できれば、メールサーバのメモリ資源やディスク資源を無駄に消費することがないからである。この対策技術が公表された当時は、単純なスパムボットのMTAには効果が大きかった。しかしながら、RFCの実装が甘いが、でも正当であるMTAをスパム検知の対象外として除外する設定作業が必要であるが、それらの設定作業を手動で行う必要があること、再送処理によって利用者へ好ましくない遅延が度々発生することを強制すること、再送処理を適切処理するスパムボットMTAが増えてきたこと、組織内の脆弱性のあるローカルであり、かつ正当なMTAを経由するスパムボットMTAが出現してきたことなどにより、現時点では事実上、これらの対策技術は、もはや過去のものになってきたと言える。

（4）では、設定時間当たりでスパムの通信量を減らす対策技術が用いられる（牛歩戦術）。例えば、

- 時間当たりの全体の送信量を減らす対策技術：Spamd (Open BSD) [19], Symantec Mail Security 8100 [20]
- スパムと判定されたホストに対して実行する対策技術： Spamd [19], Symantec Mail Security 8100 [20]

などが知られている。これらの対策技術の良いところは、スパムの流量を減らし、下流のサーバの負荷を軽減でき、スパム配送業者の作業効率を下げることが可能なことである。しかしながら、現在のところ対応できるMTAやOSが限られており、あるいは専用のハードウェアが必要となるという問題点がある。

（5）では、スパムがどこから送られて来るかを注意深く観察するなどスパム対策を講じて来た結果や経験をベースにしてスパムと判定する対策技術が用いられる。例えば、

・逆引きが不可能なMTAを拒否･制限する対策技術
・逆引きホスト名が動的IPアドレスに基づく等特定のルールに当てはまる場合を拒否･制限する対策技術

などがある。一般的なスパムから特定のアカウントやホストを狙ったスパムに対して細やかに対応できるという利点がある一方で、相当な経験を積んだ人材確保の必要な点が課題と言える。

（6）では、正当な送信側MTAのIPアドレスに関する情報をDNSサーバに登録し、受信側でそれを確認して判定する対策技術である。例えば、

・DNSサーバに正当なMTAを登録する対策技術：SPF（Sender Policy Framework）[21]
・DNSサーバに公開鍵を登録する対策技術：DKIM（Domain Key Identifier Mailed）[22]
・SPF対策技術をSMTPエンベロープではなく、メッセージヘッダで処理する対策技術：Sender ID [23]

などがある。SPFやDKIMはSMTPエンベロープ段階でチェックできる。またSender IDではどのような経路からメールが転送されて来たことを知ることが可能となる利点がある。しかし、DKIMではメーリングリストサーバで再送時に公開鍵を書き換える必要があり、またSPFとSender IDは似ていそうでまったく別物であるため、実際には誤実装が多くて有効に使えているとは、いえない現状がある。更に、スパムが正当なMTAを介して発信された来た場合は、それを防ぐ方法を別に実装する必要がある。

3.3 スパムメールを送信しない対策技術

スパムメールをメールサーバ側で送信させないためには下記の示すような対策技術が用いられる。

（1）OP25B（Outbound Port 25 Blocking）[24]

（2）送信者ユーザの認証（SMTP AUTH）[25]

（1）のOP25Bでは、スパムボットからのスパム送信やメール型ウィルスの送信をブロックする方式である。具体的には、 L3スイッチ（ルータ）やFW（ファイアーウォール）などで、指定したMTA以外からの組織外へのSMTP送信をブロックする（図7）。この対策技術では、スパムボットなどの正当でないMTAから犠牲ホストへの直接的なメール送信を阻止する。しかしながら、組織内から見ればオープンリレーであることにかわりはないため、組織内の不要となったメールサーバを整理する必要がある。OP25Bを所属組織に適用する場合は、組織外のメールサーバを組織内LANから利用することができなくなるため、利用者の反発が出る可能性がある。そのため、OP25Bの導入は、十分な周知徹底を行い、政治的な問題に発展しないようにする必要がある。

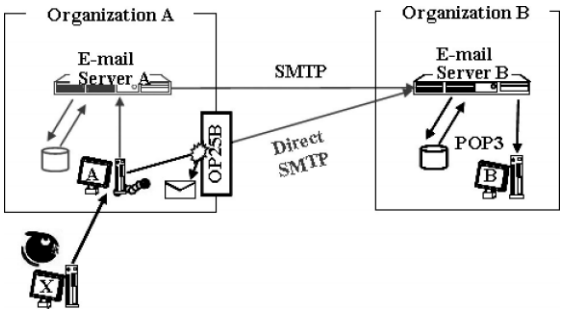

図7　Outbound Port 25 Blocking（OP25B）

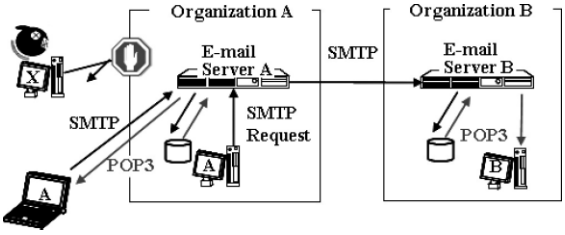

図8　送信者ユーザの認証（SMTP AUTH）

（2）の対策技術は、スパムボットからのスパム送信やメール型ウィルスの投稿をブロックする技術である（図8）。具体的には、送信側MTAの投稿･配送ポートをTCP 25番から、例えば、TCP 587番など、別のポートへ変更する。また組織外からメールを送信する場合には、POP before SMTP over SSLとSMTP AUTHを併用して投稿するようにする。後者をInbound Port 25 Blocking（IP25B）

と呼ぶ。この対策技術では、スパムボットなどの正当でないMTAから次の犠牲となるメールサーバへの、直接なメール送信を阻止することが可能である。OP25B [24] やIP25B [25] の問題点は、投稿ポートの設定に対応しかつSMTP AUTHに対応できるMUAを利用者が使用する必要があるということである。

何度も言っても申し訳ないが、OP25BやIP25Bを導入する場合は、必ず事前に投稿ポートなどの情報を利用者へ周知徹底させる。またOP25BやSMTP AUTH（IP25B）に対応していないMUAの利用者へ、IP25B/OP25B対応済みのMUAへの切り換えを強く促していく必要がある。

3.4 スパムボットの検知と対策

現在、スパムメールの発信は、大半がスパムボットMTAを利用していることが知られている。したがってスパムボットMTAを検知し、駆除していく対策技術は必要でありかつ重要である。現在下記のスパムボット検知技術が知られている。

（1）メールサーバやIDSでの検知
（2）DNSベースのスパムボットの検知

（1）の対策技術では、メールサーバのログやIDS/IPS等で組織内外へのSMTP関連のチェックをすることで、スパムボットになっているPCの検知を行うものである。実際には、メールサーバの/var/log/maillogなどからスパム関連の行を抜き出して統計処理などを行い、組織内の送信元IPアドレスを探索する。またIDS/IPSなどでも同様の作業を行い組織内の怪しいPCのIPアドレスを調査する（図9）。

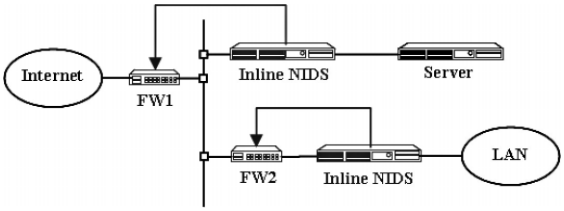

図9　Intrusion Detection System（IDS）

比較的小規模な組織内のメールサーバを経由するスパムメールやIDSの検知ログを調査することでスパムボットのIPアドレスは容易に判る。

しかし、メールサーバを経由しないスパムメールは、当然であるがメールサーバ側では検知できない。また膨大な通信流量を処理するIDS/IPSでもその検知が難しい場合が多い。実際筆者の大学のIDSで採取されるログは、ポートスキャンだけで一日あたり400MB以上であり、それにSMTPまで設定すると、データの取りこぼしなど性能低下が起こり、中･大規模な組織では現実的に、事実上不可能に近いことが判っている。

（2）の対策技術では、組織内のPC端末や組織外のC&CサーバやIDSセンサーからのDNSサーバへのDNSクエリパケット流量を監視して、組織内のセキュリティインシデントを検知する（図10）。特にスパムボットMTA活動を行っているPCからのDNSクエリパケット流量には特徴があることが確認されており、組織内におけるスパムボットと化していると疑いのあるPCを、すなわちスパムボット候補のIPアドレスを検出するのに有効である [26]。

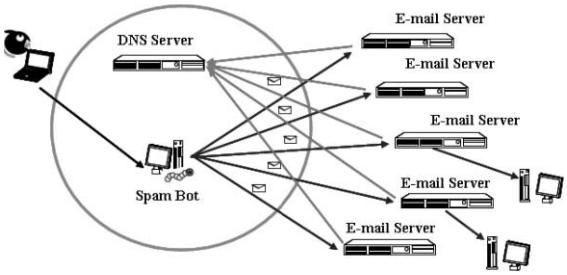

図10　DNSによるスパムボットの検知

このDNSアクセスを利用した対策技術は、中･大規模組織内の新種のトロイ等スパムボット活動を行っているPC端末などの早期発見が可能であり、そのことによって迅速に次の段階の対策を打てる可能性がある。

しかし、あくまでも疑わしいIPアドレス候補が判るだけであるため、可能な限りの状況証拠や組織外での接続点、該当IPアドレスを持つPC端末とLAN間のパケットキャプチャリングが必要となる場合があり、また該当者PC所有者または利用者から協力を得る必要もあるなどの課題がある。

4. 結論

今回は、「セキュリティポリシーと電子メール」と題し、下記の項目について説明した。（1）熊本大学への情報セキュリティポリシーの導入について、特に基本ポリシー･対策基準および実施手順書の策定について説明した。また（2）メールサーバにおけるスパム

受信および送信対策について、また（3）スパムボットの検知･対策について説明した。

本稿の筆者は、スパムボットの検知を実際に行っているが、現在のところ利用者からの反発もなく円滑に調査できている。これは単なる思い込みまたは推測に過ぎないが、恐らく情報セキュリティポリシーの実施手順書に、「不正アクセスの被害状況の報告」、「サーバ等アクセス記録の取得及び分析」、および「新種のウィルス感染発見時の処理」の三つの項目を書き込んでいたおかげであると勝手ながらそう考えている。

謝辞

本稿を書く機会を与えてくださったCAUAの皆様方に感謝申し上げます。また執筆につきまして暖かい修正をしてくださり、そして辛抱強く私の原稿を待っていただいたCAUA事務局の高橋様に感謝申し上げます。

参考文献

［1］ 政府機関統一基準について：
http://www.nisc.go.jp/conference/seisaku/dai2/pdf/2siryou03.pdf
［2］ 高等教育機関の情報セキュリティ対策のためのサンプル規程集：
http://www.nii.ac.jp/csi/sp/
［3］ 長谷川･伊藤･井上･八巻，実践ISMS講座，静岡学術出版，ISBN978-4-903859-08-8
［4］ グリーンIT推進協議：http://www.greenit-pc.jp
［5］ 文部科学省･情報セキュリティセミナー：
http://www.nii.ac.jp/hrd/ja/security/h16sec_seminar.html
［6］ Spamassassin：http://spamassassin.apache.org/
［7］ Bogofilter：http://bogofilter.sourceforge.net/
［8］ Bsfilter：http://bsfilter.org/
［9］ URIBL：http://uribl.com/
［10］ Vipul's Razor：http://razor.sourceforge.net/
［11］ Greylisting：http://www.greylisting.org/
［12］ お馴染みさん方式：
http://www.tokai-ic.or.jp/spam/
［13］ S25R
http://www.gabacho-net.jp/anti-spam/anti-spam-system.html
［14］ MX Fallback
http://moin.qmail.jp/MX_20fallback_20_c8_bd_c4_ea
［15］ Unlisting：http://unlisting.org/
［16］ Nolisting：http://nolisting.org/
［17］ GION：http://www.reflection.co.jp/spam/
［18］ Tarpitting：
http://d.hatena.ne.jp/keyword/Tarpitting
［19］ spamd：
http://opentechpress.jp/developer/article.pl?sid=07/04/16/0122217&from=rss
［20］ Symantec Mail Security 8100：
http://www.symantec.com/ja/jp/business/products/overview.jsp?pcid=2242&pvid=852_1
［21］ SPF：
http://www.rbbtoday.com/column/spamadmin/20051109/
http://www.openspf.org/
http://www.vwnet.jp/mura/BookFollow/SPF.htm
http://itpro.nikkeibp.co.jp/free/ITPro/USNEWS/20050712/164467/
［22］ DKIM：http://www.dkim.jp/
［23］ SenderID：
http://www.atmarkit.co.jp/fsecurity/special/82senderid/sender101.html
http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx
http://suika.fam.cx/~wakaba/-temp/wiki/wiki?envelope%20from
［24］ OP25B：http://e-words.jp/w/OP25B.html
http://bb.watch.impress.co.jp/cda/special/14369.html
［25］ IP25B/OP25B
http://seclan.dll.jp/ccblk25.htm
http://itpro.nikkeibp.co.jp/article/COLUMN/20060523/238776/?SS=imgview&FD=-1369990986
［26］ D. A. Ludeña R., Y. Musashi, R. Matsuba, and K. Sugitani, Detection of Bot Worm-Infected PC Terminals, Information, Vol. 10, No. 5, pp. 673-686 (2007)