キャンパスネットワークに対する SMTP Flood による DDoS 攻撃への対策と効果

原口 直大 [1)]

1) 大阪大学情報推進部

odins-room@odins.osaka-u.ac.jp

Design, Implemenatation and Evaluation of Mitigation Method against SMTP DDoS Attacks to the Campus Network

Naohiro Haraguchi[1)]

1) Department of Information and Communications Technology Services, Osaka Univ.

概要

大阪大学総合情報通信システム（Osaka Daigaku Information Network System: ODINS）は，大阪大学におけるキャンパスネットワークであり，学内の教育研究活動を支える ICT 基盤である．2015 年 11 月から ODINS に対して SMTP Flood による DDoS 攻撃が頻繁に発生しており，大量のスパム受信や透過型メールゲートウェイの SMTP セッション占有に伴うメール遅延の被害が発生している．本稿では，SMTP Flood による DDoS 攻撃の詳細，運用上の対応，及び ODINS が抱える問題点について説明する．また，本サイバー攻撃への対策実施とその効果について報告すると共に，恒久的対策について議論する．

1 はじめに

大阪大学総合情報通信システム（Osaka Daigaku Information Network System: ODINS）は，大阪大学のキャンパスネットワークであり，2016 年 5 月現在で教職員 10,056 人，学生 23,371 人を抱える大学の教育研究活動を支えている [1]．ODINS ではネットワークインフラに関する環境整備だけではなく，セキュリティ強化装置の運用や大阪大学のサーバ管理者等を対象とした情報処理技術向上を目的とする講習会を開催し，ネットワークを安全に保つための取り組みを行っている [2]．

大阪大学では，2015 年 11 月頃から SMTP Flood による DDoS 攻撃によって全学的なメール遅延が発生しており，教育研究活動に支障をきたしている．本攻撃は ODINS が現在保有しているセキュリティ強化装置では防ぎきれず，メール遅延の影響が長時間に及ぶこともあった．

本稿では，前提条件となる大阪大学における情報セキュリティに関する組織体制とシステム構成及び運用体制について説明し，SMTP Flood による DDoS 攻撃の影響と対策について述べる．加えて，本攻撃に対する対策の内容とその効果を報告し，対策に伴い発生した運用上の問題点を挙げると共に，今後の展望について議論する．

2 大阪大学における情報セキュリティに関する体制

本節では，大阪大学における情報セキュリティに関する組織構成と，ODINS で整備しているセキュリティ強化装置の構成と役割について説明する．

2.1 組織体制

大阪大学では，情報セキュリティの維持及び向上に関し必要な事項について定められた大阪大学情報セキュリティ対策規程をはじめとする諸規程等に準じて組織体制を整えている [3]．特に，情報セキュリティインシデントが発生した際に緊急対応としてネットワーク回線の遮断等が必要となる場合は，本規程に定められた CERT（学内の情報セキュリティに関する専門知識及び経験を有する教職員のうち，情報を担当する理事が担当する最高情報セキュリティ責任者により任命された者により構成される）による判断を経た上で実施している．ただし，一刻を争う状況であるが本稿に示す SMTP Flood による DDoS 攻撃対策のように判断基準が明確であり，対処内容を含めて問題ないと判断された事象については CERT の判断を経たものと

して取り扱い緊急対応を行っている．図 1 に，CERT による緊急対応判断フローを示す．

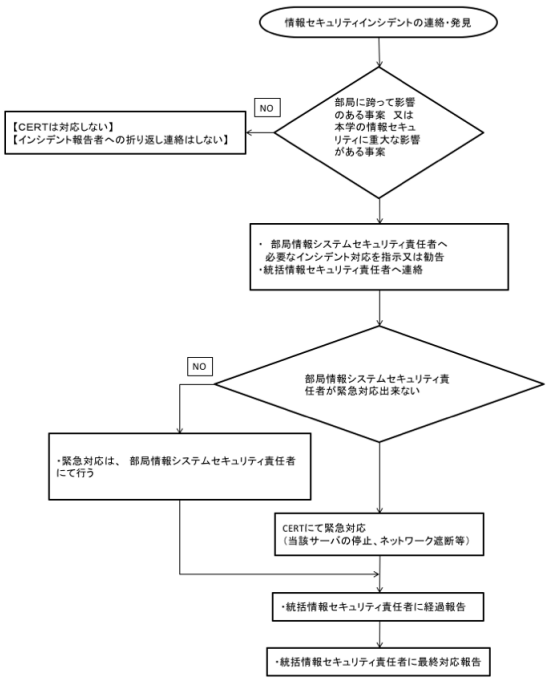

図 1　CERT 緊急対応判断フロー

2.2　システム構成及び運用体制

ODINS は，大阪大学全体のネットワーク環境を保護する情報セキュリティ対策機器群を有している．具体的には，ネットワーク侵入防止装置（Intrusion Prevention System: IPS），ネットワーク侵入検知装置（Intrusion Detection System: IDS），迷惑メール対策装置，及び学内通信監視装置により構成される．図 2 に，ODINS のネットワーク論理構成を示す．

IPS では，指定した IP アドレスを持つサーバに対する送受信を制限する設定を行う．また，外部へ業務委託している ODINS 外部監視担当が IPS 及び IDS を通過するデータを分析することで，より精度の高い監視と危険な通信を判断し，ODINS 事務担当と連携して対応を行っている．迷惑メール対策装置として，透過型メールゲートウェイを採用しており，ウイルスチェックや IP アドレスの危険度判定を行い，結果をメールヘッダに付与する役割を担っている．現在，ODINS では統一されたイントラネットワーク環境の構築と移行を計画しており，学内通信監視装置はイントラネットワーク環境を保護するために導入している．IPS 及び IDS による学内外通信の監視に加えて，学内通信であるイントラネットワーク環境の通信を監視する役割を果たしている．

ODINS では，情報セキュリティ対策装置を含めて機器の保守運用業務を外部業者（以降，ODINS 保守運用担当と呼ぶ）へ委託している．ネットワーク障害や情報セキュリティインシデント等の問題が発生した場合は，ODINS 保守運用担当，ODINS 外部監視担当，及び ODINS 事務担当と連携し対処する．

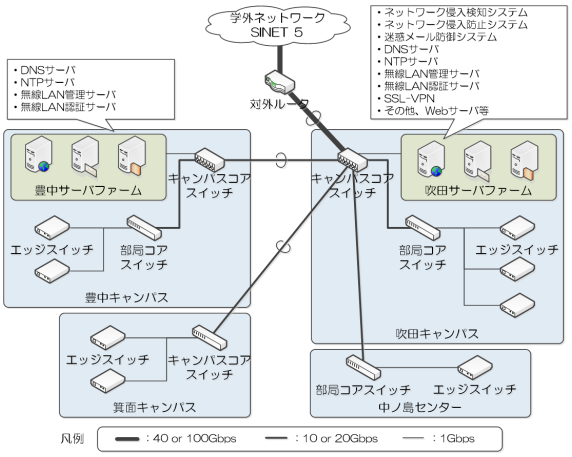

図 2　ODINS ネットワーク論理構成図

3　SMTP Flood による DDoS 攻撃

3.1　攻撃内容と被害状況

2015 年 11 月から大阪大学に対して SMTP Flood による DDoS 攻撃が頻繁に発生しており，全学的なメール遅延の影響を受けている．攻撃の傾向は把握出来ている範囲で 5 種類あり，表 3.1 にその傾向と概要を示す．

SMTP を利用した DoS 攻撃は攻撃元が少なく，通常の運用で観測される挙動と異なることから，特定が容易である．よって，ODINS 保守運用担当及び ODINS 担当が在室中であれば，問題なく対応可能である．ただし，DoS 攻撃に特化した監視体制を取っていないため攻撃発生直後に認知することは困難であるが，通常 1 時間以内に認知及び対処を行っている．

スローポスト型 DoS 攻撃は，少数からのアクセスであれば全学的なメール遅延は発生せず，影響は最小限となるため通常運用ではリスク受容している攻撃手法である．しかしながら，本攻撃手法は DDoS 攻撃との複合で行われることが多く，DDoS 攻撃によるメール遅延で SMTP セッション占有時間が長くなっている

表 1　SMTP Flood による攻撃の種類と概要

攻撃の種類	概要
SMTP を利用した DoS 攻撃	学内のサーバへ集中的にメールを送り続ける．
スローポスト型 DoS 攻撃	SMTP セッションを確立後，可能な限りセッションを占有しリソースを枯渇させる．
メールサーバに限定しない学内サーバに対する DoS 攻撃	大量の 421 エラーコードのログ出力及びログを溢れさせ，セッションも占有されリソースを枯渇させる．
SMTP を利用した DDoS 攻撃	多数の攻撃元サーバから学内のサーバへ集中的にメールを送り続ける．
各種攻撃の複合型	DoS/DDoS，スローポスト含め，様々な組み合わせで攻撃を行う．

場合と，攻撃の意図がありSMTP セッションを占有している場合の区別がつかず，攻撃元を特定することが困難である．また，対処するためにはログを分析する必要があり，アクセス遮断候補の選定に多くの時間を割くこととなり，分析時間中はメール遅延が継続した．ログの分析は，攻撃を認知してから平均で 2 時間以上要しており，メール遅延は攻撃の対処成功，または攻撃の自然収束まで継続した．

SMTP を利用した DDoS 攻撃の場合は，数が多いが攻撃元の特定は容易であるため，順次アクセス遮断を行った．メール遅延も SMTP を利用した DoS 攻撃と同様に，通常 1 時間以内に認知及び対処を行った．

メールサーバに限定しない学内サーバに対する DoS 攻撃は，迷惑メール対策装置のログに 421 エラーコードとして大量に記録されていたため特定は容易であった．本攻撃も SMTP を利用した DoS 攻撃と同様に，認知から 1 時間以内に対処を行なっており，長時間に渡るメール遅延は発生していない．

各種攻撃の複合型は，確認されている攻撃手法を複数組み合わせたパターンの攻撃である．大量のログ及び攻撃元が存在しており，一切の特定ができなかった．メール遅延は 6 時間以上継続していたこともあり，最も被害が大きい攻撃手法であった．

攻撃対象となる学内サーバの傾向として，取り扱うドメインが多いメールサーバが集中的に攻撃受けることが挙げられる．特に大阪大学におけるキャンパスクラウドサービスで提供しているキャンパスメールサーバが頻繁に攻撃対象となった．その結果，キャンパスメールサーバのリソース枯渇が発生し，キャンパスメールサーバから迷惑メール対策装置に対して発信されるエラーメッセージによる SMTP セッション占有が発生するため，迷惑メール対策装置のリソース枯渇が連動し全学的なメール遅延の原因となった．全学的な影響を最小限に抑えるため，学内サーバ 1 台あたりの同時接続数を，迷惑メール対策装置のリソース上限の 25% とした．全学的なメール遅延の発生頻度は緩和されたが，キャンパスメールサーバの被害は継続しており，メールを利用した学内業務の妨げとなった．

3.2　攻撃への対応経緯

ODINS 保守運用担当による攻撃への対処は業務時間帯に限られており，土日祝日を含め，勤務時間外の時間帯は攻撃の認知を含め一切対処ができなかった．加えて，ODINS の情報セキュリティ対策装置軍は SMTP Flood を想定した構成ではなかったため，効果的かつ適応的な対処を行うことが出来なかった．そのため，状況を改善するための暫定策として，ODINS 事務担当によるログ分析及びプログラム開発により対処を行なった．また，被害を最小限に抑えるため，攻撃の予兆を観測した場合は，休日，夜間を含め ODINS 事務担当が臨時出勤し対処を行なっていた．対処が長期化していたこともあり，ODINS 事務担当の業務負担は膨大となり，通常業務を圧迫した．

SMTP Flood による DDoS 攻撃に対応は，以下の 3 段階で行った．

1. ODINS 運用保守担当の業務契約範囲で調査及び対応
2. ODINS 事務担当によるログ分析及び攻撃検知体制の確立
3. ODINS 事務担当によるプログラム開発

システムの稼働率の監視や過負荷の解消は ODINS 保守運用業務の一環であるため，SMTP Flood による DDoS 攻撃を発見した場合は，ODINS 保守運用担当から ODINS 事務担当への連絡と対処可能な範囲の改善策の提示を行う体制とした．しかしながら，ODINS 保守運用担当で可能な提案は，SMTP Flood による DDoS 攻撃発生の事実と被害状況の報告，及び明らかに不審と判断可能な DoS 攻撃を行うメールサーバの

IP アドレスを特定のみとなるため，全ての攻撃には対処しきれなかった．そのため，暫定策として，毎時 0 分の迷惑メール対策装置の SMTP セッション占有率を通知する仕組みを導入し，継続して不審な攻撃を行うメールサーバの IP アドレスを特定することとした．特定した IP アドレスについて CERT にブロック（接続拒否）の可否を伺い，IPS へブロック登録を行うこととした．また SMTP セッション占有率が 40% を超えた場合，ODINS 保守運用担当の業務対象外の時間帯（土日祝日及び 17:15 - 翌 8:30 である場合）には，ODINS 事務担当が大阪大学内の管理系ネットワークへアクセス可能な端末設置場所へ移動し，対処することとした．

次に，迷惑メール対策装置のログを分析し，攻撃を行うメールサーバの IP アドレスの特定を試みた．ログ分析は ODINS 保守運用業務には含まれていないため，ODINS 事務担当が行った．全学のサーバ全てを対象として分析を行うことは困難であったため，攻撃が集中し，かつ影響が大きいキャンパスメールサーバを中心に対応を行い，キャンパスメールサーバ運用担当と連携し，接続拒否の候補となる不審な IP アドレスの特定を行った．不審な IP アドレス候補を抽出後は，不審な挙動を行うメールサーバと共通する特徴を分析した．分析の結果，迷惑メール対策装置が付与するメールサーバが持つ IP アドレスに対する危険度判定結果でスパムと判定（90% 以上となった場合）された IP アドレスのうち，95% 以上の値を示す IP アドレスを持つメールサーバから DDoS 攻撃と思われる挙動が多く確認されたこと，接続時間が 300 秒以上となる場合が多いことがわかった．加えて，迷惑メール対策装置の開発メーカによるログ分析結果によると，20 秒以上 SMTP セッションを保持している IP アドレスの危険度判定結果では 95% 以上の評価となる割合が高いとあった．また，開発メーカの基準では，危険度判定結果で 95% 以上の評価が誤判定となる確率は 100 万分の 1 とのことであった．よって，この条件に合致する IP アドレスを持つメールサーバは攻撃元と判断して良いことがわかった．

これらの条件を参考に，さらに正常な通信を行う IP アドレスを持つメールサーバを誤ってブロックする確率を減らすため，攻撃元候補となったメールサーバが持つ IP アドレスの名前解決を行い，日本のドメイン以外をブロックする IP アドレスとして取り扱うこととした．しかし，このようなブロック条件に合致するか否かを確認するために必要となる，ログの取得及び分析には 1 回あたり 2 時間以上を要するため，即効性のある対策とはならなかった．

次に，ブロックする IP アドレスを持つメールサーバの候補を機械的に選定するために，SMTP Flood による DDoS 攻撃対策用プログラムを開発した．このプログラムでは，ブロック対象となる IP アドレスを持つメールサーバの抽出及び IP アドレスの名前解決までを自動化している．プログラムへの入力となるログの取得，及びプログラムが出力した IP アドレスを IPS へブロック登録する作業は自動化することができていない．そのため，大幅な運用負担軽減には至っていない．また，プログラムによるログ分析には最短 10 分以上を要するため，攻撃を行うメールサーバの IP アドレスをブロックするまでには依然として多くの時間を要している．しかし，プログラム開発を行う時間と通常業務のバランスを鑑みて，プログラムの実行速度は向上させず運用することとなった．

また，ログを取得するためには ODINS の管理系プライベートネットワークへアクセスする必要があるが，遠隔地からネットワークを介して外部から管理系プライベートネットワークへアクセスする手段がなく，管理系ネットワークへアクセス可能な端末が設置されている学内へ移動しなければならなかった．そのため，ODINS 事務担当の業務負担は大きくは軽減されず，心身ともに大きな負担となっていた．

3.3 恒久的対策とその結果

ログの分析とプログラムの構築により課題と自動化のための条件が明らかになったため，恒久的対策を実施することとなった．解決すべき課題として，次の項目として整理した．

1. 学外環境から ODINS 管理系プライベートネットワークへのリモートアクセス環境構築
2. SMTP Flood による DDoS 攻撃対策用プログラムの計算速度向上と定期稼働
3. IPS への自動登録

1 つ目の課題を解決するために，ODINS が所有する SSL-VPN 機能を使用することとした．この機能を用いて ODINS 管理系プライベートネットワーク環境へアクセスするため設定変更を行い対処した．2 つ目及び 3 つ目の課題を解決するために，プログラム開発費用を確保し外部機関へ発注することとした．発注したプログラムのアルゴリズムを図 3 に示す．また，プログラムの動作条件となる閾値を表 2 に示す．

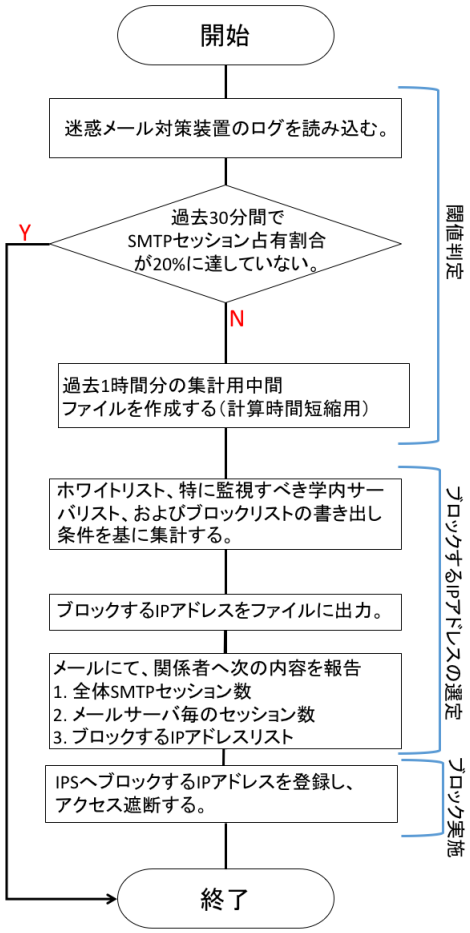

図 3　SMTP Flood による DDoS 攻撃対策プログラムのアルゴリズム

表 2　ブロック対象とする IP アドレスを持つメールサーバの抽出条件

ブロック条件	セッション占有時間	アクセス回数	危険度判定結果
条件 1	20 秒	40 回	95% 以上
条件 2	200 秒	1 回	95% 以上
条件 3	0 秒	300 回	0% 以上

閾値は ODINS の迷惑メール対策装置固有の値となるため，本稿では汎用化するため危険度判定結果を割合で示している．迷惑メール対策装置において攻撃を受けていない状況下での SMTP セッション占有率は 13% 程度であるため，20% 以上の占有率となった場合に攻撃が発生したと判断しプログラムを動作させることとした．具体的には，30 分に 1 回 SMTP セッション数の占有率を確認し，20% を超える場合にブロックする IP アドレスを持つメールサーバを選定する．加えて，学内の主要メールサーバの被害状況を把握するため，指定した主要メールサーバの SMTP セッション占有率を取得するように設計した．選定されたブロックする IP アドレスを持つメールサーバは，IPS の機能により 1 時間に 1 回自動的に更新する設定とした．なお，条件 1 の閾値は開発時点で 50 回以上のアクセスとしていたが，条件 1 に合致する攻撃が長期化する際に早期解決させるため，2016 年 4 月 5 日に閾値を 40 に変更した．また，条件 2 に合致する攻撃も同様に，攻撃を早期解決させるため，2016 年 4 月 5 日に閾値を 300 秒から 200 秒へ変更した．条件 3 は，アクセス回数を 1,000 回以上かつ危険度判定結果が 95% 以上としていたが，攻撃に対応仕切れなかったため 2016 年 7 月 25 日にアクセス回数を 300 回，危険度判定結果を 0% 以上とした．危険度判定結果の閾値を大幅に下げた理由は，学内全体に不特定多数のアクセスを行う接続元は一律で不審な通信と判断したためである．

構築したプログラムは 2016 年 3 月 24 日から稼働させている．図 4 に稼働効果を示す．図の棒グラフは，毎時 0 分に通知される SMTP セッション占有率の値が 40% を超えた回数（ODINS 事務担当が緊急対応する必要がある条件）を月単位でまとめており，線グラフは月単位でブロックした IP アドレスを持つメールサーバ数を示す．なお，2015 年 11 月と 12 月のデータは，毎時 0 分の SMTP セッション占有率を計測できていなかったため，メール遅延が発生した回数（SMTP セッション占有率 100%）としている．プログラムを投入したのは 3 月末であったため 3 月はあまり効果を得られなかったが，4 月からは SMTP セッション占有率が 40% を超える回数が減少していることが確認出来る．6 月はキャンパスメールサーバが集中的に攻撃対象となったため，SMTP セッション占有率は高くなっているが，メール遅延はほとんど発生していない．ブロックした IP アドレスの IPS への登録間隔は，開発時に 1 時間に 1 回のブロックする IP アドレスリストの更新頻度としていたが，定期的な登録によるシステム負荷も許容範囲であったことから 7 月 15 日から 30 分に 1 回に変更した．その結果，SMTP セッション占有率が高くなる前に攻撃をブロックすることができており，非常に安定した運用となった．9 月はキャンパスメールサーバに加えて，複数の学内サーバを対象にした攻撃が多く発生していたため，SMTP セッション占有率が高くなっているが，攻撃ブロックサイクルが早まったこともあり，SMTP セッション占有率は 7 月より低く，ブロックする IP アドレスを持つメールサーバ数も多くなっている．また，ODINS 事務担当が ODINS 保守運用担当の業務対象外の時間帯

に対応することがなくなったことからも，プログラムは効果的であると考える．

本プログラム稼働と並行して，新たな攻撃手法に備え継続的にログ分析も継続して行っている．本分析では，新たな攻撃手法対策だけでなく，本学のメールサーバから発信される異常な数のメールやエラーメッセージ等も発見することもあり，情報セキュリティインシデントに繋がる挙動もより早く認知することができるようになった．よって，本学全体のメールに関する情報セキュリティ対策水準は大幅に向上したと考えている．

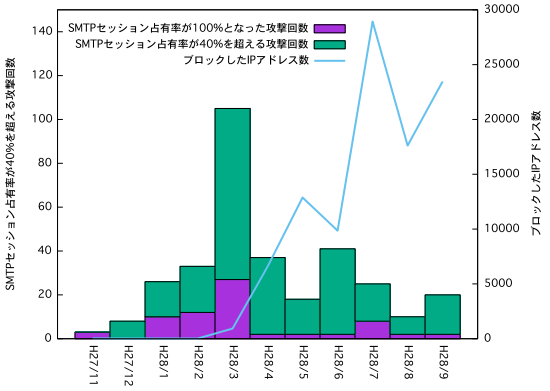

図 4　SMTP Flood による DDoS 攻撃回数とブロックした IP アドレスを持つメールサーバ数の推移

4　その他課題と今後の展望

4.1　運用上の問題点

SMTP Flood による DDoS 攻撃対策プログラムは開発発注時点で把握している条件を基に作成しており，想定外の多様な攻撃には対応仕切れない．また，本プログラムの開発予算は臨時で確保したものであるため，今後の継続的な開発発注は，予算確保の観点から困難である．加えて，プログラムの閾値変更をする必要がある場合，変更内容を適切と判断するための基準がないため本番環境で実験的に判断することしかできない．そのほか，本学内で SMTP Flood による DDoS 攻撃及びログ分析に関するサポートや助言を得ることに限界があるため，ログ分析品質は ODINS 事務担当者個人の能力に依存している．そのほか，ブロックした IP アドレスを持つメールサーバが誤検知である可能性があるが，明確な誤検知判定方法が定まっていない．現在は ODINS 事務担当が whois 情報の参照や FQDN の取得を行いブロックした IP アドレスを持つメールサーバを管理する機関を調査し，大学や出版社等の教育研究活動に必要と思われる IP アドレスを持つメールサーバを個別に確認しホワイトリストへ登録している．しかしながら，誤検知対策を施してもホワイトリスト登録から漏れた IP アドレスの使用者等から大阪大学へ問い合わせがあることから，運用負担の高さと対処精度が伴わない状況である．現状より，ODINS のセキュリティ対策装置で防御しきれないサイバー攻撃に対する継続的な対策体制が整備されていないことが明確になった．

4.2　技術的な問題点

現在，ODINS 事務担当の一人のみがプログラムの改修を行う能力を有しており，また，改修するための着眼点といったノウハウも共有できていない状況である．対策として，ODINS 事務担当全体の技術力向上，SMTP Flood 対策業務を外注するための予算確保，新たな攻撃に対応するためのプログラム改修，及び改修するための判断基準の明文化等が必要となる．加えて，開発に使用しているプログラミング言語の理解と記述方法の習得も必要であるため，どのようにして技術継承を行うべきか課題が残る．

迷惑メール対策装置は全学的なセキュリティ対策装置の一つであるが，キャンパスメールや一部のメールサーバへの攻撃が集中していることに伴い，迷惑メール対策装置の SMTP セッション占有率が高くな流ことによって，大学全体のメール遅延が引き起こされている．そのため，ODINS だけでなく，学内のメールサーバに適用すべき対策についての検討が必要である．また，学内のサーバ管理者も能力差があり，部署によっては ODINS が提示する対処方法を実現できないことも考えられる．一方で，ODINS でどの水準までの対応を行うべきかという判断基準もないため，対応要求に際限がないことも問題である．

また，技術や知識についても得られるサポートに限界があるため，適宜学んだことをフィードバックする以上の向上が望めず，ブレイクスルーとなる改善には至っていない．

4.3　今後の展望

有効な対策であると考えられる迷惑メール送信規制（Outbound Port 25 Blocking）や送信ドメイン認証技術（Sender ID，Sender Policy Framework: SPF，Domainkeys Identified Mail: DKIM，Domain Message Authentication Reporting & Conformance: DMARC）については検討が不足しており，また大阪大学全体で導入した際の影響も想定仕切れていない．将来的に，現在の対策方法で不十分になることを想

定し，プログラムの改修だけでなく，大阪大学全体のメールサーバ運用体制も見直す必要があると考える．また，今後の ODINS で導入する機器は，本稿で対象としたような攻撃に動的に対処可能であることを要件としたい．そのほか，情報セキュリティに関する技術や知識をどのように学び，業務へ還元していくべきかについてのノウハウがないため，今後も継続して情報収集を行い，知識と技術を担当者を中心に還元していきたい．

5　おわりに

本稿で取り扱った SMTP Flood による DDoS 攻撃対策は，大阪大学固有の環境に特化したものである．ただし，全てのメール通信を観測するポイントに透過型アンチスパムアプライアンスを設置している場合は，対策指針の一つになりうると考える．また，同様の攻撃の被害にあった機関であれば，情報連携することでより精度の高いサイバー攻撃対策基盤構築に繋がると期待している．

今回の取り組みは経験則を機械処理へ落とし込むアプローチであったが，本対応方法は担当者の能力と抱える業務量により，品質に大きな差が生じてしまう．よって，品質の担保のためにも専属のセキュリティ担当を用意し教育するか，外注による一定品質以上のセキュリティ対策環境を確保する必要がある．

参考文献

[1] 大阪大学，大阪大学プロフィール（http://www.osaka-u.ac.jp/ja/guide/about/profile/files/profile2016.pdf），pp.4-4，2016.

[2] 原口直大，南吉英，大阪大学におけるネットワーク環境の構築とその運用，大学 ICT 推進協議会 2013 年度年次大会論文集 W1E-5，pp.1-1，2013.

[3] 大阪大学，大阪大学情報セキュリティ対策規程（http://www.osaka-u.ac.jp/jp/about/kitei/reiki_honbun/u035RG00000784.html），2016.