[2021]九州大学情報統括本部年報 : 2021年度

出版情報：九州大学情報統括本部年報. 2021, pp.1-, 2022-10-01. Information Infrastructure Initiative, Kyushu University
バージョン：
権利関係：

第 3 章　先端サイバーネットワーク研究部門

3.1 スタッフ一覧

職 名	氏 名	研究キーワード
教授	岡村 耕二	インターネット、新世代ネットワーク、サイバーセキュリティ、マルウェア解析、教育
助教	笠原 義晃	計算機ネットワーク、インターネット運用技術、侵入検知、ネットワークセキュリティ

3.2 研究事例紹介

3.2.1「透過型 SMTP プロキシによるメール送信集約とキュー輻輳回避の検討」

小田 知央，廣川 優，近藤 宇智朗（GMO ペパボ株式会社），嶋吉 隆夫，笠原 義晃（九州大学）

はじめに

GMO ペパボ株式会社の研究開発組織「ペパボ研究所」と九州大学情報基盤研究開発センターは、2017 年 10 月 1 日より、ペパボ研究所が持つ軽量コンテナ技術を基盤に用いたクラウドホスティングに関する共同研究開発を進めている。現在は大規模高集積メールホスティング基盤に関する共同研究を進めている。

電子メールは古くから用いられている電子的メッセージ交換手段である。近年は電子メールを代替する様々なメッセージングツールが利用されているが、依然として電子メールは世界的に広く利用されている。その一方で、電子メールには迷惑メール対策やアカウント乗っ取りなどによる不正メール大量送信への対応など、セキュリティ的に対応しなければならない課題が多い。メールサービスには、これらの問題に対応しながらもメールが遅延しないような安定性やセキュリティの担保が求められる。

利用者にメールサービスを提供するメールホスティングでは、多数の利用者を同一システムに収容するマルチテナント型により集積率を高めることで、リソース効率を高めて、低コストでのサービスを実現している。なお、ここで「テナント」とは、ホスティングサービスの利用者（組織）に割り当てられる仮想的な領域であり、メールサービスの場合はメールドメインと、そのドメインで発行された多数のメールアカウントを含んでいる。メールホスティングにおいて、グローバル IPv4 アドレス数の制約や送信メールの集中監視といった要請から、外部にメールを送信するサーバは集約し、単一または少数の MTA (Message Transfer Agent)によりメール送信する構成が一般的である。

一方で、外部送信用メールサーバを集約する構成には課題がある。この構成では、送信サーバの送信メールキューがシステム全体で共有されることになるが、そのことに起因する問題が生じる。例えば正常に送信可能な範囲を超える大量のメールが利用者から外部に送信されるなどして、大量のメールが送信メールキューに滞留することがある。同じ事象は、送信先メールサーバにより、迷惑メール対策などを理由に送信サーバからの受信レートが制限された場合にも発生する。メールホスティングにおいて、送信メールキューの滞留は、システム全体でのメール送信の遅延につながる。この問題は、少数の送信サーバによる負荷分散だけでは、完全に解決することはできない。また、テナント間での IP アドレスの共有に起因

する課題もある。利用者による不正メール送信などによって、メール送信サーバの IP アドレスが拒否リストなどに掲載され、宛先サーバにより接続拒否や受信レート制限を受ける場合がある。その場合、同じ送信サーバを利用する善良な利用者のメールも受信拒否やレート制限の対象となる。もしホスティングのテナント別に送信サーバの IP アドレスを分離できればこの問題は解決できるが、大規模なメールホスティングで収容テナント数と同数のグローバル IPv4 アドレスを用意することは一般的に不可能である。

本稿では、マルチテナント型メールホスティングにおいて、不正メール送信による他の利用者への影響を限定的とする、メール送信サーバの構成方法に関する検討について述べる。提案する方法では、メール送信ゲートウェイとして透過型 SMTP プロキシを利用することで、メール送信の集約による集中管理と、利用者間でキューの分離によるキュー輻輳の回避を両立する。テナント別送信サーバからインターネットへのメール送信は、透過型 SMTP プロキシを経由して送信する。これにより、テナント別送信サーバでは既存のメール送信ソフトウェアに変更を加えることなく、送信サーバと宛先サーバ間での SMTP コマンド・応答を、ホスティングシステム全体で網羅的に収集、制御できる。また、透過型 SMTP プロキシはキューを持たないことから、コンテナにより送信キューをテナント分離することで、他テナントの影響でメールがキューに滞留することがなく、ホスティングシステム全体でのメールキューの輻輳を回避できる。

メールホスティングにおけるメール送信機能の課題

本章では、メールサーバ、特に集積度の高いメールホスティングが、他のメールサーバにメールを送信する際に考慮すべき課題について述べる。

大量メール送信

電子メールは、各組織が自分のメールドメインを持ち、自組織の利用者にメールアドレスを付与し、各ドメインのサーバ同士がメッセージを交換する分散運用が前提となっている。各メールサーバは DNS (Domain Name System)を利用して、MX レコードから宛先メールアドレスのドメインを担当するサーバを取得し、そのサーバに接続してメールを送信する。一般的に MTA には送信キューが用意されていて、送信すべきメールは一旦キューに入って順に送信処理される。DNS で宛先サーバの情報を取得できたとしても、そのサーバに常時接続できるとは限らず、配送できなかったメールはキューに残して一定時間後に再送を試みたり、長時間配送できなかったメールは破棄して送信元にエラーメッセージを返したりする。サーバが外部に配送するべきメールを受け付ける数が、実際に外部に配送できる数より多くなる状態が輻輳である。なんらかの理由により輻輳が発生すると、キュー長の増大によりメールがキューに滞留し、その MTA による全てのメール送信が遅延する。

メールホスティング環境において、メール配信の遅延はサービス品質に関わる大きな問題である。ネットワークやサーバの能力がアカウント数やメール流量に対して不足することによる輻輳であれば、送信サーバを複数用意して負荷分散することで、輻輳を軽減できる。しかし、アカウントの不正利用による迷惑メール送信では一時的に数万～数十万通のメールが投入されるような場合があり、通常の負荷分散で完全に輻輳を解決することは困難である。アカウントの不正利用については 1 アカウントが単位時間に送信できるメール数を制限するといった入口対策も重要だが、送信キューの輻輳は様々な理由で起こりうるため、出口側の対策も必要である。

送信キュー輻輳によるメール遅延は、原理的にはテナント毎に送信キューを分離する事で影響範囲を特定のテナント内に限定できる。利用者の MUA (Mail User Agent)からの送信メールを受け付ける MSA

(Message Submission Agent)については内部的にテナント分離される場合もある。しかし、不正メール送信への対策やメール送信状況の集中管理などの要請などから、メールを外部に送信する MTA を集約し、送信キューがテナント間で共有される構成が一般的である。我々が過去に提案した高集積マルチアカウント型メール基盤においても、MSA は軽量コンテナにより高集積とテナント分離を両立させる構成となっていたが、送信メールのウイルス検査や、ホスティング全体の送信メールについて網羅的・集中的に情報を収集して不正メール送信対策等を行う必要性から、送信メールはテナント間で共有のメール送信ゲートウェイコンテナから外部に送信する設計を採用しており、送信キューは集約されていた。送信キューが集約されるメールホスティング環境において、送信キュー輻輳は、高集積であればあるほど、影響範囲が拡大する。

IP アドレスによる配送制限

電子メールはインターネット上の任意のホストから配信されうることが前提であるため、外部からメールを受信するメールサーバはインターネット全体からの接続を受け付ける必要がある。一方、電子メールはフィッシングやマルウェアの配布など、悪意を持った目的での利用も多く、インターネット上には悪意を持ったサーバやクライアントも多く存在する。そのようなホストからの迷惑メールや不正利用を防ぐために、SMTP セッションの接続元 IP アドレスに基づいてメール受信を制限する技術が多くのメールサーバで利用されている。それらの技術は、メールを受信する側のセキュリティ向上のために必要な一方で、メールサービス自体には悪意がない場合でも不正利用や誤判定により制限の対象となることで、正常なメールの配送に影響を受けることがある。

悪質なホストが利用する IP アドレスを登録したリストを用いて、登録 IP アドレスからの接続やメール受信を拒否する方法は広く用いられている。サーバに静的な拒否リストを用意して手動で IP アドレスを登録する方法も用いられるが、手動での拒否リスト管理は煩雑でコストが高いことから、ログの出力を元に一定期間接続を拒否するようなソフトウェアを利用することもある。また、複数のサーバや監視システムで収集した情報に基づいて拒否すべき IP アドレスの一覧を作成し、それを講読者に提供するサービスもあり、単一サーバでの情報収集には限界があることから、サービスとして提供されている拒否リストを購読してメールサーバで利用する例は多い。拒否リストは IP アドレスやネットワーク単位であるため、メールホスティングで送信に利用しているグローバル IP アドレスが特定の拒否リストに含まれると、そのリストを利用しているサーバにはメールを配送できなくなる。拒否リストでメール受信を拒否する場合には、リストから除外する方法を提供することが推奨されており、SMTP の応答メッセージなどにその情報を含めて返すのが一般的である。

また、許可・拒否の二択ではなく、レピュテーション（評判）に基づいてメール受信を制御する方法も用いられる。レピュテーションのしきい値を決めて拒否したり、レピュテーションの値に応じて単位時間に受け取るメールの流量を制限したりする。メールサーバに対するレピュテーションを提供するサービスでは一般的に、長くインターネット上に存在し正常なメールを送出している IP アドレスは評判がよく、悪意のあるメールの送信元としてセキュリティ対策機器で検知された IP アドレスが評判が悪くなっていく。

また、あるメールサービスにとってなじみのない IP アドレスからのメールには受信レート制御をするという、IP スロットリングという仕組みを導入しているサービスやサーバ製品もある。例えば、Microsoft Exchange Online では、今まで Exchange Online にメールを送信したことがない IP アドレスからのメール

には強い送信レート制限が課せられる。IP スロットリングを実装しているメールサービスに対し、新しい IP アドレスから継続的にメールを送信したい場合には、最初に低レートでメールを送信し、だんだん流量を増やす（ウォームアップする）必要がある。レート制御の詳細は、攻撃者によって回避されるとを防ぐため非公開となっており、メール受信を拒否されてはじめてスロットリング対象になっていることがわかる。筆者らの所属する九州大学では、全学のメールサービスを Exchange Online に移行した直後、学内の他のサーバからの転送メールや、安否確認のための一斉送信サービスからのメールがスロットリング対象となったことがある。

このように、現状の電子メールシステムでは迷惑メール対策などのセキュリティ対策として、送信元の IP アドレスに基づいて受信側でさまざまな制限が行われている。メールホスティングでは、送信サーバの IP アドレスが制限対象になると、利用者に多大な影響がある。メール送信側から見ると、受信側でどのような受信制限を行っているかは一般的に分からない。また、実際に接続拒否や一時的なメール受信拒否をされるまでは、制限対象になったことも分からない。管理者は、送信先で受信制限を受けているかをエラーメールやログ、利用者からの問合せなどから抽出し、拒否リストからの除外依頼などの対応を行なう必要がある。サービス品質に大きな影響を与えるため、速やかな検知と迅速な対応が必要である。もしテナントごとに別個のグローバル IP アドレスを割り当てることができれば、ある IP アドレスが制限対象になっても他のテナントには影響しない。しかし、近年はグローバル IPv4 アドレスの確保が困難で高コストであることから、高集積なメールホスティングサービスでグローバル IPv4 アドレスをテナントと同数用意して完全なテナント分離を実現することは事実上不可能である。現実的には、メール送信に利用する複数のグローバル IP アドレスのプールを用意し、テナント間で共有する方法がとられる。状況により特定 IP アドレスの利用を一時的に止めたり、新しい IP アドレスをプールに追加する際に事前にウォームアップしたりするなど、限られた IP アドレスをやりくりして運用する必要がある。例えば Exchange Online では拒否リストに入ってもいい高リスク配送プールを別に用意する運用をしている。

透過型 SMTP プロキシ

メールホスティングにおいて、メール送信の集中管理や情報収集機能を維持しつつ前述の問題に対処する方法として、メール送信集約用の透過型 SMTP プロキシを提案する。

透過型プロキシとは、クライアントとサーバ間のネットワーク経路に設置され、クライアントとサーバはお互い直接通信しているように見せつつ、セッションに対する付加処理を行うことができるプロキシである。クライアント・サーバ間の通信内容を収集・改変したり、ウェブプロキシであれば通常のウェブキャッシュのようにサーバコンテンツをキャッシュしたり、暗号通信をプロキシで終端することによって平文に戻し、通信内容を検査したりすることができる。SMTP 通信を検査する際に透過モードを利用可能なセキュリティ製品がある。

透過型 SMTP プロキシの動作

透過型 SMTP プロキシによるメール送信部の構成を図 1 に示す。「MSA」は、利用者が MUA から送信するメールを受け付けるメールサーバである。従来の一般的なメールホスティング環境の構成（図 2）では、外部への送信メールは、MSA から「送信用 MTA」に転送されてキューに格納されたのち、送信用 MTA から「宛先 MX サーバ」に送信される。一方、提案する構成では、MSA がメールを外部に送信する際に、通常通り DNS で宛先ドメインの MX レコードから「宛先 MX サーバ」の IP アドレスを取得し、SMTP セッションを開始する。しかし、実際にはそのパケットは「透過型 SMTP プロキシ」で一旦受け取る。透過型

SMTP プロキシは、ここで SMTP のコマンドメッセージの内容に対して検査や情報収集などの必要な処理を行う。その後、MSA からのコマンドメッセージを、場合によっては改変を伴って、透過型 SMTP プロキシがバインドする SMTP 送信用 IP アドレスから本来の宛先サーバへと送信する。宛先サーバからの応答メッセージは透過型 SMTP プロキシの SMTP 送信用 IP アドレス宛に送られるので、コマンドメッセージと同様に情報収集や改変などののちに、本来の送信元である MSA に転送する。

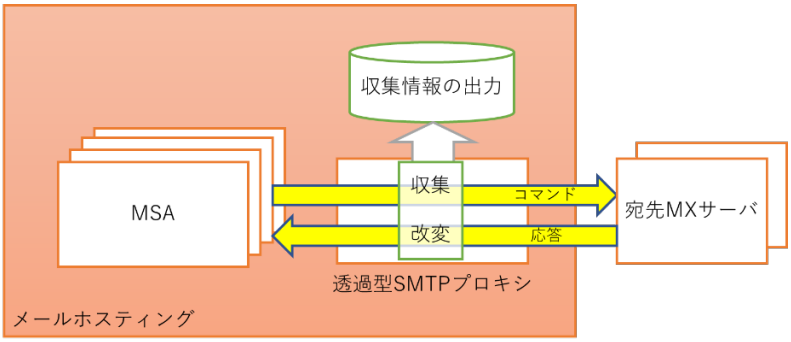

図 1 透過型 SMTP プロキシによるメール送信部の構成

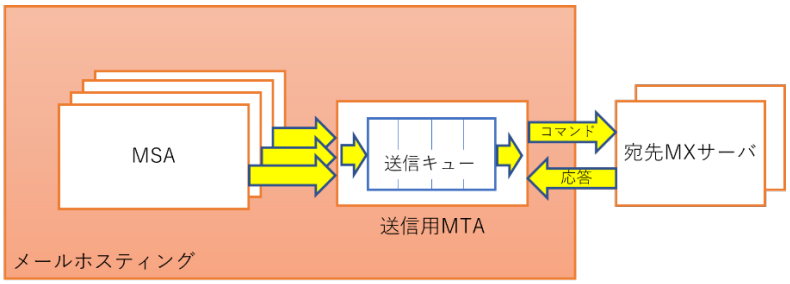

図 2 従来のメールホスティング環境の一般的構成

最近では、MTA 間の SMTP 通信についても、インターネット上での盗聴を防ぐ目的などから、STARTTLS コマンドによる TLS 暗号化が一般的になっている。暗号化が送信サーバと宛先サーバで終端されている場合、経路上でセッションの内容を取得することができない。つまり、MSA が宛先 MX サーバに対して STARTTLS コマンドを発行すると、それ以降のコマンド・応答メッセージは TLS 暗号化されることになり、透過型 SMTP プロキシでは内容を確認できない。しかし、本提案では、TCP セッション情報だけでなく、SMTP コマンド・応答メッセージの内容も情報収集・検査の対象とすることを考えている。そこで、透過型プロキシにより TLS 暗号化を制御することとした。具体的には、宛先 MX サーバからの EHLO コマンド応答に「TLS 暗号化通信可能」を意味する STARTTLS の提示があった場合、宛先 MX サーバとの TLS セッション確立は透過型 SMTP プロキシが行い、TLS 通信を透過型 SMTP プロキシで終端する。これにより、インターネット上の SMTP 通信は暗号化で保護しつつ、MSA からの送信メール情報を一元的に収集できる。このとき、MSA と透過型 SMTP プロキシとの間で暗号化が不要であれば、透過型 SMTP プロキシで EHLO コマンド応答から STARTTLS を削除して MSA に返すことで、透過型 SMTP プロキシと MSA との間は平文で SMTP セッションを開始できる。MSA と透過型 SMTP プロキシとの間も暗号化したい場合は、MSA において任意のホストに対して透過型 SMTP プロキシのサーバ証明書を許可するように設定することで実現できる。

透過型 SMTP プロキシの特徴

メールホスティングにおいて、前述した大量メール送信による影響を最小限に留めるには、キューをテナントごとに分離し、そのキューから直接外部にメールを送信する必要がある。一方、テナントごとに別の IP アドレスを付与するのは現実的でないため、送信 IP アドレスは集約する必要がある。

送信用 MTA ではなく透過型 SMTP プロキシを用いることで、キューを持つことなく、少ないグローバル IP アドレスで集約してメールを送信可能である。送信 IP アドレスを集約するだけであれば、SNAT (Source Network Address Translation)でパケットの送信アドレスを付け替えることでも実現可能だが、送信メールの集中管理には別の仕組みが必要となる。

さらに、送信キューは MSA ごとに持つ構成となるため、先行研究のように MSA をテナントごとに分離すれば、あるテナントが大量にメールを送信したとしても、キュー長の増大が他のテナントに影響を与えることがない。透過型 SMTP プロキシで収集する情報に基づいて、不正利用が疑われるテナントやアカウントからのメール送信には、透過型 SMTP プロキシで通信レートを制御するなどの対応も可能である。

透過型 SMTP プロキシでは、送信に利用する IP アドレスを集中的に管理するだけでなく、宛先 MX サーバからの SMTP 応答も集中管理できる。このことから、例えばある送信用 IP アドレスが拒否リストに登録されたり、スロットリングの対象となったときに、応答メッセージや応答タイミングなどを分析することでこれを検知可能である。例えば、複数の送信用 MTA を用意して別個の送信用 IP アドレスを用いる構成においてある送信用 IP アドレスが拒否リストに登録された場合、当該 MTA のキューにメールが滞留することになり、キュー内のメールは送信用 IP アドレスを付け替えるまで送信できず、アドレス付け替え後に順次送信されるのを待つ必要がある。しかし、透過型 SMTP プロキシは自身がキューを持たないことから、透過型 SMTP プロキシでのメール送信遅延は発生しない。さらには、透過型 SMTP プロキシに複数の送信用 IP アドレスを設定しておけば、拒否リストに登録された IP アドレスの使用を停止するだけで、メール送信が継続できる。

概念実証

予備実験

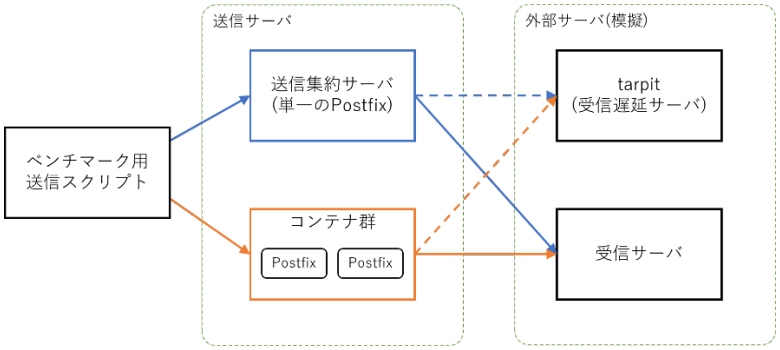

図 3 実験の構成

予備実験として、送信キューの分離によってキュー輻輳時の影響範囲が限定される効果を確認するための実験を行った。実験の構成を図 3 に示す。実験は、Ubuntu 20。04 LTS 上で実施した。「ベンチマーク用送信スクリプト」は、多数の利用者からのメール送信を模擬するスクリプトである。従来法では送信用 MTA サーバでキューが共有されることから、ベンチマーク用送信スクリプトは単一の Postfix 経由でメ

ールを送信する（キュー共有）。一方、提案手法の模擬構成（キュー分離）では、MSA 別にキューが分離されることになるので、コンテナを利用して複数の Postfix を MSA として起動し、ベンチマーク用送信スクリプトは複数 MSA 経由でメールを送信する。

送信キューでの輻輳を発生させることを目的に、本実験では送信先の 2 ドメインのうち 1 つを tarpit として動作させる。tarpit は迷惑メール対策の 1 つで、相手が悪意のあるサーバと判定した場合などにセッションは切断せずに応答の送出を極端に遅らせ、送信サーバによるメール送信の完了を遅延させる仕組みである。本実験では、tarpit サーバとして mxtarpit を使用した。なお、本実装では標準で SMTP 応答を 1 文字につき 3 秒かけて返す設定となっていたが、実験にかかる時間を考慮し 0.25 秒に変更している。これにより、tarpit 宛のメール送信には通常以上に時間を要することとなり、結果的にメール送信レートが低下することでキューの輻輳が発生する。また、tarpit の影響を明確に可視化するため、実験開始 5 分後に受信遅延サーバ宛メールを 80 通送信している。キュー分離構成では、あるテナントが不正メールを送信している状況を想定し、通常のメールと受信遅延サーバ宛メールはベンチマーク用送信スクリプトから別の MSA へと送信する。

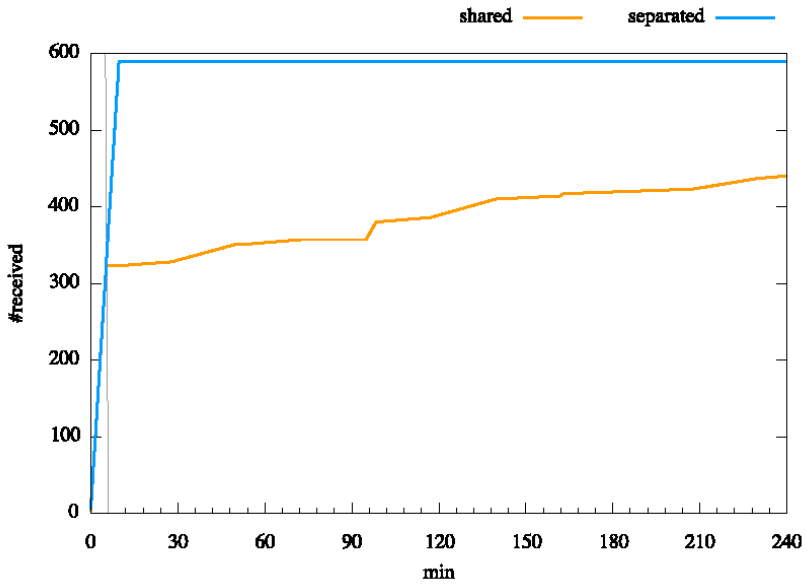

図 4 メール配信数の時間経過

本実験でのメール配信数のグラフを図 4 に示す。横軸は実験開始からの時間（分）であり、青がキュー分離の構成で配信完了した通常メールの積算通数、黄がキュー共有の構成で配信完了した通常メールの積算通数である。tapirt 宛メールの送信開始時点を灰色縦線で示している。キュー分離構成では、tarpit 宛メールの送信開始前後でレート変化なくメールが受信できていることが分かる。一方、キュー共有構成では、tarpit 宛メールの送信開始後には配信レートが著しく低下しており、大きな配信遅延が生じていることが分かる。これは、tarpit へのメール送信に大きく時間が掛かることから、Postfix の送信キューにメールが滞留し、さらには Postfix でのメール受理が不能になり、送信スクリプトからのメール送信にも遅れが生じたことによる。この結果から、送信キューを分離することで、メール送信遅延の影響範囲が限定されることが確認できた。

プロトタイプ実装

提案する透過型 SMTP プロキシが実現可能であることを示すため、プロトタイプを開発した。実装言語は go 言語である。なお、本実装では、TLS 対応を簡略化するために、MSA と透過型 SMTP プロキシを同一ホスト上で動作させることを前提とし、宛先 MX サーバと透過型 SMTP プロキシとの間だけで TLS 通信を行い、MSA と透過型 SMTP プロキシとの間は平文で通信する実装とした。また、収集した情報はログとして出力する実装としている。

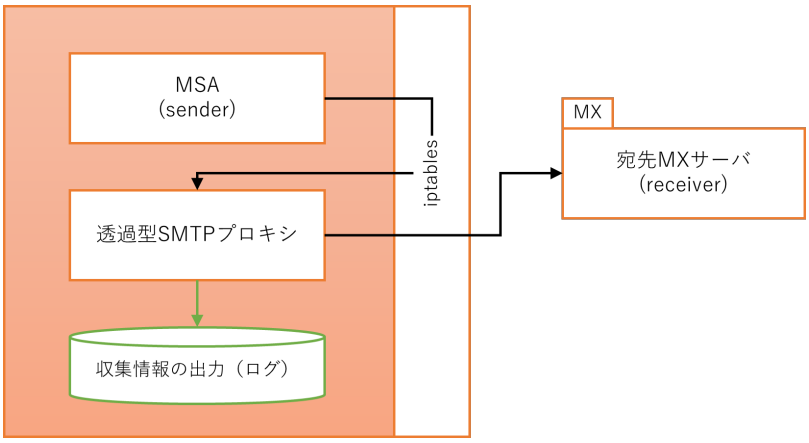

図 5 プロトタイプ検証環境の構成

本プロトタイプの動作確認実験を行った模擬環境の構成を図 5 に示す。MSA からのパケットを透過型 SMTP プロキシプロセスにリダイレクトするために Linux の iptables を使用している。

透過型 SMTP プロキシを起動し、MSA (sender)から宛先 MX サーバ(receiver)にメールを送信した際のプロキシでのセッションログの例を図 6 に示す。時刻情報に続く「<-」は sender に送信された応答（プロキシで改変されたものを含む)、「->」は receiver に送信されたメッセージ（プロキシで改変されたものを含む)、「|<」は receiver から送信されプロキシで終端された応答、「|>」はプロキシから receiver に送信されたメッセージ、「>|」は sender から送信されプロキシで終端されたメッセージである。

図 6 の 1、2 行目で平文での SMTP 接続を開始している。5 行目で receiver からの応答には TLS による暗号通信の開始が可能であることを示す「STARTTLS」が含まれているが、6 行目で sender に返す際にはその行を削除することで、sender は平文のまま SMTP 通信を続ける。7 行目で sender とは独立にプロキシから STARTTLS コマンドを発行し、TLS セッションを確立するとともに、10 行目で再び EHLO コマンドを送る事で SMTP セッションを再開する。その応答である 12 行目は sender に返す必要がないため破棄している。8 行目で sender から受け取ったメール送信のためのコマンドは一旦プロキシで保持しておき、TLS セッションが確立した後に 14 行目で receiver に送信している。なお、実際にはこれらのメッセージは暗号化されて送信される。その後も、引き続き通常の SMTP セッションを継続することで、メール送信を完了している。

この実験により、宛先 MX サーバとの間で TLS 暗号化通信を行う場合でも、透過型 SMTP プロキシで SMTP セッションの情報を収集・検査可能であることが確認できた。

```
2021/02/06 14:50:48 connected from 192.168.30.40:57493
2021/02/06 14:50:48 connected to 192.168.30.50:25
2021/02/06 14:50:48 <- 220 receiver ESMTP Postfix (Ubuntu)¥r¥n
2021/02/06 14:50:48 -> EHLO sender¥r¥n
2021/02/06 14:50:48 |< 250-receiver¥r¥n250-PIPELINING¥r¥n250-SIZE 10240000¥r¥n250-VRFY¥r¥n250-ETRN¥r¥n250-S
TARTTLS¥r¥n250-ENHANCEDSTATUSCODES¥r¥n250-8BITMIME¥r¥n250-DSN¥r¥n250-SMTPUTF8¥r¥n250 CHUNKING¥r¥n
2021/02/06 14:50:48 <- 250-receiver¥r¥n250-PIPELINING¥r¥n250-SIZE 10240000¥r¥n250-VRFY¥r¥n250-ETRN¥r¥n250-E
NHANCEDSTATUSCODES¥r¥n250-8BITMIME¥r¥n250-DSN¥r¥n250-SMTPUTF8¥r¥n250 CHUNKING¥r¥n
2021/02/06 14:50:48 |> STARTTLS¥r¥n
2021/02/06 14:50:48 >| MAIL FROM:<root@sender> SIZE=327¥r¥nRCPT TO:<root@receiver> ORCPT=rfc822;root@receiv
er¥r¥nDATA¥r¥n
2021/02/06 14:50:48 |< 220 2.0.0 Ready to start TLS¥r¥n
2021/02/06 14:50:48 |> EHLO sender¥r¥n
2021/02/06 14:50:48 pipe locked for tls connection
2021/02/06 14:50:48 |< 250-receiver¥r¥n250-PIPELINING¥r¥n250-SIZE 10240000¥r¥n250-VRFY¥r¥n250-ETRN¥r¥n250-E
NHANCEDSTATUSCODES¥r¥n250-8BITMIME¥r¥n250-DSN¥r¥n250-SMTPUTF8¥r¥n250 CHUNKING¥r¥n
2021/02/06 14:50:48 tls connected, to pipe unlocked
2021/02/06 14:50:48 -> MAIL FROM:<root@sender> SIZE=327¥r¥nRCPT TO:<root@receiver> ORCPT=rfc822;root@receiv
er¥r¥nDATA¥r¥n
2021/02/06 14:50:48 <- 250 2.1.0 Ok¥r¥n250 2.1.5 Ok¥r¥n354 End data with <CR><LF>.<CR><LF>¥r¥n
2021/02/06 14:50:48 -> Received: from sender (localhost [127.0.0.1])¥r¥n        by sender (Postfix) with SMT
P id 45B113EA9B¥r¥n for <root@receiver>; Sat,  6 Feb 2021 14:50:48 +0000 (UTC)¥r¥nFrom: <root@sender>¥r¥nTo:
 <root@receiver>¥r¥nDate: Sat,  6 Feb 2021 14:50:48 +0000 (UTC)¥r¥nMessage-Id: <a77e.0003.0000@sender>¥r¥nS
ubject: Hi, Receiver from Sender¥r¥n¥r¥nXXXXXXXXXX¥r¥n.¥r¥nQUIT¥r¥n
2021/02/06 14:50:48 <- 250 2.0.0 Ok: queued as 76DAD4113D¥r¥n221 2.0.0 Bye¥r¥n
2021/02/06 14:50:48 connections closed
```

図 6 プロキシでのセッションログ

まとめ

本研究では、高集積マルチテナント型メールホスティングにおけるメール送信機能で解決すべき課題を述べ、その解決方法としてメール送信集約用の透過型 SMTP プロキシを提案し、キュー分離によるメール送信遅延の問題回避を確認する予備実験、および、プロトタイプ実装と動作検証を行った。これらの実験により、提案手法の概念が実証できた。

今回実装した透過型 SMTP プロキシのプロトタイプは機能が限られているが、今後、実装を改良していく予定である。例えば、透過型 SMTP プロキシでは、宛先 MX サーバからの応答を収集できるだけでなく、各 SMTP コマンド・応答メッセージの送受信に掛かった時間などの情報も出力できる。
これにより、受信拒否や一時受信不能による明示的な受信制限だけでなく、tarpit やそれに類する通信レートによる受信制限も検知可能だと予想している。また、アカウント、テナントや宛先 MX サーバ、送信メールの疑わしさなどによって送信用 IP アドレスを使い分けること、拒否リストの掲載を理由に受信拒否したという応答メッセージを受け取った場合に当該 IP アドレスを自動的に利用停止するなどといった機能拡張が考えられる。

さらに、本研究では送信用 MTA の代わりに透過型 SMTP プロキシを用いる方法を提案しているが、透過型 SMTP プロキシは既存のシステムにも容易に追加できることから、例えば、既存の送信用 MTA と同一ホスト上で透過型 SMTP プロキシを動作させて情報収集に利用することも可能である。今後、ホスティングサービスの実運用に影響を与えない範囲で透過型 SMTP プロキシを導入し、実際の SMTP コマ

ンド・応答の情報を収集し、受信制限の自動検知や不正メール送信の自動防止のために分析を進めていくことを検討している。

3.3 研究内容紹介

3.3.1 岡村 耕二

研究内容

私は、1988 年に九州大学工学部で卒業研究を行って以来、三菱電機株式会社、奈良先端科学技術大学院大学、神戸大学、九州大学において、20 年以上にわたって、コンピュータ・ネットワークに関わる研究や仕事、また、学生への教育をしてまいりました。九州大学の助教授に着任しました 1998 年以降の約 12 年間の教育や研究内容について、1) 基礎技術的な内容のもの、2) 応用・実践的あるいは国際的な内容のものに分けて紹介いたします。

1) 基礎技術的な内容の教育・研究

インターネットに関する基礎的な内容の教育・研究は、学術振興会・未来開拓研究「知的で動的なネットワーキング」（コアメンバー）、総務省通信総合研究所（現在の情報通信研究機構）と取り組んだ「新世代モバイル通信技術」、韓国の大学・研究機関との総合的な共同研究である学術振興会・日韓拠点大学プロジェクト、国立情報学研究所とともに取り組んでいる CSI (Cyber Science Infrastructure)プロジェクトそして、最近では新世代ネットワークの研究などを通じて行ってきました。

1999 年からコアメンバーとして参加した学術振興会・未来開拓研究「知的で動的なネットワーキング」プロジェクトでは、専門家以外には難解なネットワークの設定について、その自動化をめざし、最終的にはネットワークの構成要素が変化してもネットワークがその変化に追随して最適なネットワーク環境が自動的に構成されることを目標にした研究に取り組みました。この研究の一部は当時の学生の修士研究としても進められましたが、その成果は最終的に情報処理学会の論文誌に掲載することができました。2003 年から、韓国の主要な大学・研究機関と日本の間の総合的な共同研究を行う、日韓拠点大学方式の総括責任者として、本プロジェクトを遂行するとともに、自分自身も韓国の研究機関と共同研究を行ってきました。私の主たるテーマは、国際的なネットワーク運用と、遠隔医療などの国際応用技術に関するものです。国際的なネットワークの運用のための技術として、私の研究室で行ってきた、蓄積されたネットワークのトラフィック・経路情報の統計処理技術と、韓国の実践的な解析技術を融合させることに成功し、2007 年末に発生しました台湾南沖地震で発生した日本と中国の間の光ファイバ切断がインターネットに与えた影響を、私の研究室と韓国の先生と共同で解析し、災害に対する現在のインターネット運用技術の課題をまとめることができました。これは当時の学生の修士研究、博士研究の一部として取り組み、この成果は、情報処理学会、電気通信学会のそれぞれの論文誌に掲載されました。さらに、次世代ネットワーク技術について着目した研究では、韓国人の博士課程の学生と韓国で一足先に始まった、次世代ネットワーク網のデータ解析を行い、それを日本に提言することができました。この成果も情報処理学会論文誌に掲載されております。また、最近では新世代ネットワークにおける仮想ネットワーク技術、新しいデータ交換技術、省電力運用技術に着目した研究を行い、すでにいくつかの国際会議にその成果を投稿し、発表しております。

2) 応用・実践的、国際な内容の教育・研究

応用・実践的、国際な教育・研究として、総務省・情報通信研究機構が提供する JGN (Japan Giga Network) に関連する公募によるもの、日韓光ファイバに関連するもの、国際遠隔医療に関するものなどに取り組んできました。JGN を用いた研究として、高精細動画像伝送に関わる研究、IPv6 に関する研究、次世代型インターネット拠点のアーキテクチャに関する研究に取り組んできました。次世代型インターネット拠点のアーキテクチャに関する研究では、福岡に設立された九州ギガポッププロジェクト (QGPOP) の主要なメンバーとして研究活動を行い、このプロジェクトで培った高度なネットワーク運用技術はのちの実証実験で活用されています。日韓光ファイバに関する研究では、九州・山口経済連合が導入した福岡と釜山の間の光ファイバの利活用について、産官学非常に多くのさまざまな方々と玄海プロジェクトを 2001 年に設立させ、2003 年にはインターネットとしての利用に成功、さらに、総務省からそのネットワークを利用した 5 年後の IT 社会を模索する研究 (e! プロジェクト) を委託され、国際的な近未来的な遠隔講義、遠隔医療の実証実験に取り組みました。さらに、この活動が評価され、学術振興会による日韓拠点事業が認められました。この事業は 8 年にわたって行われ、私はその総括責任者として日韓で 200 名以上の研究者の代表として事業を成し遂げました。国際遠隔医療は、2002 年から九州大学病院と構想を練り始め、2003 年から韓国と実施をはじめ、以降、九州大学の P&P や学術振興会・アジアコアプログラムの支援などを利用してアジアの各国、オセアニア、米国、欧州などの共同研究医療機関を開拓し、現在では約 20 カ国、世界中の約 90 の医療機関と高精細動画像を用いた遠隔医療の先進的な事例実験に成功しています。この遠隔医療の実証研究の成果・評価の一つとして、九州大学病院にアジア遠隔医療センター (TEMDEC) の設置への貢献をあげることができます。遠隔医療に関する学術的な研究成果は九州大学病院の教員と共著で多くの国際会議などで発表し、高い評価を得ております。

以上のように私は、コンピュータ・ネットワーク技術について、基礎的な内容での教育・研究活動を継続して行い、その成果を論文誌、国際会議論文誌また学会誌に残してきています。また、この延長で、いままで主査として2名の学生に博士号（大学院　システム情報科学府）を授与させることができました。応用・実践的、国際的な教育・研究の推進で、企業や省庁、自治体と連携した実用的な研究活動や、海外の多くの研究機関とも連携した国際的な研究活動を行い、研究室の学生に国際的な共同研究の機会も与えるとともに、対外的に九州大学のプレゼンスをあげ、その研究活動で得た最新の技術を九州大学のキャンパスネットワークなどの IT インフラや九州大学病院の活動に還元してきました。

所属学会名

IEEE，教育システム情報学会 ，電子情報通信学会 ，情報処理学会

主な研究テーマ

・　新世代ネットワークに関する研究
　　キーワード：新世代ネットワーク，2010.04～

- 省電力化を考慮した先進的なネットワーク運用
  キーワード：グリーン IT，省電力，先進的ネットワーク運用，2010.04～
- サイバーセキュリティ
  キーワード：サイバーセキュリティ，2014.03～
- 国際的インターネット実証研究
  キーワード：イーサイエンス，2013.04～
- 日韓およびアジア次世代インターネットおよびその応用に関する研究
  キーワード：インターネット技術、インターネット応用，韓国，アジア，2001.05～

研究プロジェクト

- 日米の超高齢社会支援に IoT 技術を適用する際のデジタルギャップの解消と、異文化の壁を超え国際的普及に資する為の研究
  2020.04～2022.03，代表者：岡村耕二，日本，アメリカ
- 安全な IoT サイバー空間の実現
  2016.11～2022.03，代表者：岡村耕二，インド工科大学デリー校
- 成長分野を支える情報技術人材の育成拠点の形成(enPiT)セキュリティ分野
  2016.10～2021.09，代表者：岡村耕二
- サイバーセキュリティ
  2014.04～，代表者：岡村耕二，メリーランド大学 ボルチモア校
- 九州大学　サイバーセキュリティ
  2013.03～，代表者：岡村耕二
- 九州ギガポップ プロジェクト
  2000.04～，代表者：岡村耕二，九州大学 情報基盤研究開発センター
- 日韓およびアジア地域次世代インターネットプロジェクト
  2001.07～，日本，韓国，タイ，シンガポール
  日韓およびアジアでの次世代インターネットのリーダーシップをとる

研究資金

● 競争的資金

1. 2016 年度～2021 年度，JST 戦略的国際共同研究プログラム，代表，安全な IoT サイバー空間の実現

教育活動

● 担当授業科目

1. 2021 年度・春学期，サイバーセキュリティ基礎論
2. 2021 年度・夏学期，企業から見たサイバーセキュリティＡ
3. 2021 年度・夏学期，ソフトウェア技術を利用したシステム構築のための技術論Ⅰ
4. 2021 年度・冬学期，企業から見たサイバーセキュリティＢ
5. 2021 年度・冬学期，警察実務から安全な生活について学ぶ
6. 2021 年度・冬学期，ソフトウェア技術を利用した創造的サービス構築論Ⅰ
7. 2021 年度・前期，サイバーセキュリティ演習
8. 2021 年度・後期，サイバーセキュリティ演習
9. 2021 年度・前期，ソフトウェア技術を利用したシステム構築のための技術論Ⅱ
10. 2021 年度・後期，ソフトウェア技術を利用した創造的サービス構築論Ⅱ
11. 2021 年度・秋学期，通信工学通論 A
12. 2021 年度・冬学期，通信工学通論 B
13. 2021 年度・後期，サイバーセキュリティ
14. 2021 年度・冬学期，情報ネットワーク特論
15. 2021 年度・通年，セキュリティエンジニアリング演習

社会貢献・国際連携等

● 社会貢献・国際連携活動概要

1. 通信・放送機構 委託研究評価委員
2. 北九州ギガビットラボ 利用促進部長
3. 北九州 IT 研究開発基盤利用促進協議会 会長
4. 福岡県 ギガビットハイウェイ 構想委員

大学運営

● 学内運営に関わる各種委員・役職等

1. 2020.10～，副学長
2. 2020.10～，CISO（最高情報セキュリティ責任者）
3. 2014.12～，サイバーセキュリティセンター センター長
4. 2012.04～，全国共同利用運営委員会
5. 2007.04～，全学情報環境利用委員会
6. 2003.04～，セキュリティ専門委員会

3.3.2 笠原 義晃

研究内容

・ 安定した情報サービスのためのサーバ品質の監視・異常検知・品質改善

インターネットではさまざまな種類の情報サービスが提供されている。九州大学でも構成員に向けてさまざまなサービスを提供している。サービスを提供する機器（サーバ等）の増加により、管理は複雑さを増しており、期待される性能が出ていなかったり、異常が発生していても迅速に対応できない場合が増えている。仮想化技術の進展により仮想計算機によるサービス構築も容易になったが、仮想化レイヤが増加することにより障害対応はより複雑になった。
本研究では、実サービスの運用管理を通して、仮想化システムも視野に入れた、統一されていない多数のサーバによるサービス提供環境において、管理者の負荷を低減し効率的に管理・運用が可能な手法の構築を目指す。

・ ネットワークトラフィック監視に基づく侵入検知・裏口検出に関する研究

インターネットを利用した計算機への不正アクセスや、ウィルス・ワーム・ボット等の自動化された侵入・拡散ソフトウェアによる被害は年々増加し、また手口も巧妙化している。これに対抗するには、ホストレベルからネットワークレベルに到る多層的な対策が必要となる。
本研究では、このうち特にネットワークでの対策に重点をおき、組織の基幹ネットワーク管理者の立場から組織内ネットワークでの不正な活動などを監視・検出する手法を研究・開発する。具体的には、ネットワークトラフィックを受動的に収集し、パターンによらない分類手法や、プロトコルの特徴を利用した異常検知手法について検討している。これにより、既存のパターン検出型侵入検知システムでの検知が難しい活動を発見する事を目指している。

・ その他の活動

九州大学の学内ネットワークである総合情報伝達システム（KITE）の管理・運用に参加し、学内外向け各種サーバの管理・運用、新規サービスの開発等を行っている。
また、管理者向け講習会の実施、管理者や利用者からの質問への対応、侵入検知システム等の監視による学内ネットワークの保全等、安定したネットワークを維持するための活動を続けている。

所属学会名

Association for Computing Machinery (ACM)，情報処理学会，電子情報通信学会

主な研究テーマ

・ 安定した情報サービスのためのサーバ品質の監視・異常検知・品質改善
キーワード：情報システム，サーバ管理・運用，仮想化，2012.04～.

・　ネットワーク監視に基づく侵入検知・異常検知
キーワード：インターネット，ネットワーク管理運用，侵入検知，ネットワークセキュリティ，2001.04～.

研究業績

● 原著論文

1. Yoshiaki Kasahara, Takao Shimayoshi, Our Design and Implementation of Multi-Factor Authentication Deployment for Microsoft 365 in Kyushu University, 2022 ACM SIGUCCS Annual Conference (SIGUCCS '22), https://doi.org/10.1145/3501292.3511569, 56-61, 2022.03.

● 学会発表

1. 小田 知央，廣川 優，近藤 宇智朗，嶋吉 隆夫，笠原 義晃，透過型 SMTP プロキシによるメール送信集約とキュー輻輳回避の検討，マルチメディア，分散，協調とモバイル(DICOMO2021)シンポジウム，2021.07.

研究資金

● 科学研究費補助金

1. 2020 年度～2022 年度，基盤研究(C)，代表，軽量コンテナによる大規模高集積メールホスティング基盤における送信機能の高機能化

● 共同研究、受託研究

1. 2017.10～2023.03，代表，軽量コンテナに基づく柔軟なホスティング・クラウド基盤の研究開発と大規模・高負荷テスト環境の構築

教育活動

● 担当授業科目

1. 2021 年度・春学期，サイバーセキュリティ基礎論
2. 2021 年度・春学期，サイバーセキュリティ基礎論

3. 2021 年度・秋学期，情報処理概論（24 クラス）

大学運営

● 学内運営に関わる各種委員・役職等

1. 2016.10～，ウエストゾーン安全衛生部会 委員
2. 2014.04～，情報基盤研究開発センター安全衛生部会 委員
3. 2013.04～，九州大学病院情報基盤専門委員会 委員
4. 2012.04～，生涯メール運営会議 構成員