スパムがいっぱい！

～新メールゲートウェイの構築と運用～

○岩瀬雄祐、川田良文

情報通信技術支援室　情報基盤技術グループ

概要

名古屋大学では 2013 年より、全学的な迷惑メール判定システム（メールゲートウェイ）の正式運用を開始し、学外から大量に受信する迷惑メールに対してセキュリティチェックのサービスを提供し、危険な迷惑メールによって生じるセキュリティ事故の抑止に努めてきた。しかしながら、2020 年、ライセンス問題によって新メールゲートウェイを短期間で構築せざるを得なくなると共に、全国的な迷惑メールの急増によって大規模なメール配送遅延が発生する等、メールゲートウェイの運用についても厳しい状況となった。本発表では、新メールゲートウェイの構築と運用、運用のために開発したツール、全国的な迷惑メールの急増とその対応、ならびに名大独自のスパム削除フィルタの開発について報告する。

1　はじめに

名古屋大学では、全学の教職員向けの実験サービスとして、2011 年 4 月より、シマンテック社製 Symantec Messaging Gateway（SMG）[1]を用いた迷惑メール判定システム（メールゲートウェイ）を提供し、2013 年より、正式運用を開始し、危険な迷惑メールによって生じるセキュリティ事故の抑止に努めてきた[2]。しかしながら、2019 年 8 月にブロードコム社によってシマンテック社エンタープライズ向けセキュリティ事業の買収[3]が行われた後、SMG のライセンス更新ができない状況となった。そこで、2020 年 2 月に SMG の代替ソフトウェアとしてカスペルスキー社製 Kaspersky Security for Linux Mail Server（KLMS）[4]を採用し、1 ヵ月という短期間で構築、テスト、移行準備を進め、2020 年 4 月に KLMS によるメールゲートウェイサービスの正式運用を開始した。

2020 年はコロナ禍によりテレワークが普及すると共に、サイバー攻撃、フィッシングメールや不正アプリなどが増加しており、サイバーセキュリティ対策の必要性が高まった[5]。特に、全国的に迷惑メールが急増した [6]。本学においても 2020 年 5 月（ゴールデンウィークの前後）頃から同様の迷惑メールの急増を確認しているが、メールゲートウェイの運用ポリシーでは迷惑メールを遮断しないため、大量の迷惑メールが学内へ流入する状況が継続し、業務に支障が出る事態となっていた。また、2020 年 6 月にはウィルス付きメールが大量送付され、メールゲートウェイのメールキューが溢れ、大規模なメール配送遅延が発生してしまった。KLMS では特定の迷惑メールのみを抽出して削除することができなかったため、本学独自の迷惑メール削除フィルタの開発を進め、2020 年 10 月に迷惑メールの削除を開始した。

本発表では、新メールゲートウェイの構築と運用、運用のために開発したツール、全国的な迷惑メールの急増とその対応、ならびに名大独自のスパム削除フィルタの開発について報告する。

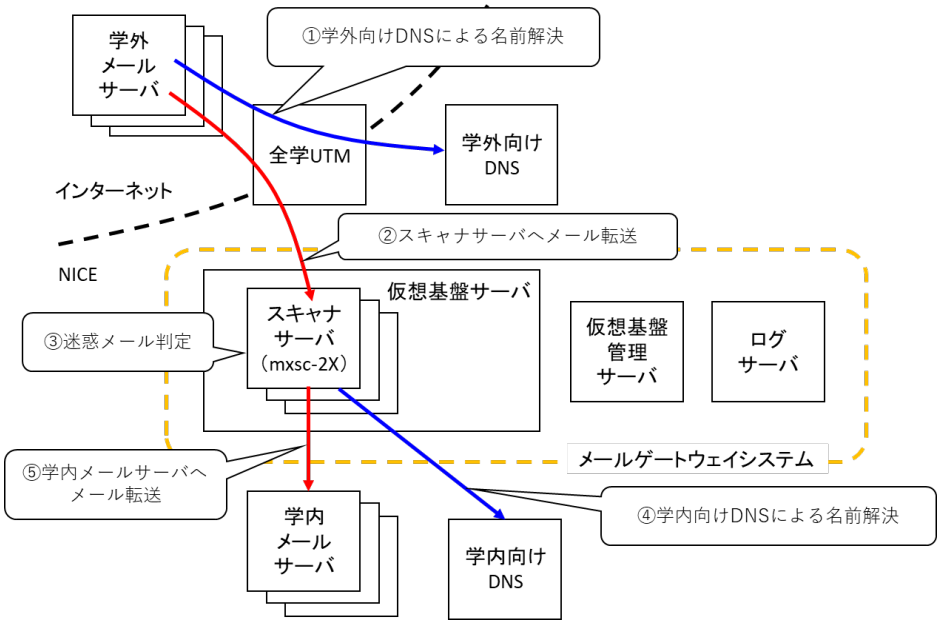

図 1. メールゲートウェイのシステム構成と迷惑メール判定の流れ

2　新メールゲートウェイの構築と運用

2.1　システム構成と迷惑メール判定の流れ

新メールゲートウェイは、迷惑メールを判定するスキャナサーバ（mxsc-2X、仮想サーバ）6 台、スキャナサーバが稼働する仮想基盤サーバ（VMware ESXi）3 台、仮想基盤の管理サーバ（VMware vCenter Server）1 台、ログサーバ 1 台によって構成される。スキャナとログサーバは Linux（CentOS）によって構築されている（図 1）。スキャナサーバはメール転送エージェントの Postfix、内部キャッシュ DNS の BIND、迷惑メール判定を行う KLMS がインストールされており、IPv6 のアドレスによるメール転送が可能で、メール転送を暗号によって保護できる SMTPS にも新対応した。SMG による旧システムの仮想基盤を流用しており、サーバ台数に変更はないが、KLMS のスキャナの動作が軽く、仮想基盤のリソースの消費が少なくなった。

本学では学外向けと学内向けの 2 種類の基幹 DNS を運用している。メールゲートウェイの利用登録を行った学内メールサーバは学外向け DNS の MX レコードがスキャナサーバへ置換される。学外から学内へメールを送信する場合、学外メールサーバは学外向け DNS による名前解決を行い（図 1—①）、スキャナサーバへメール転送する（図 1—②）。スキャナサーバは迷惑メール判定を行い（図 1—③）、学内向け DNS による名前解決を行い（図 1—④）、学内メールサーバへメール転送する（図 1—⑤）。スキャナによってスパムと判定されたメールは件名とメールヘッダへ文字列を追加され、ウィルスと判定されたメールは添付ファイルを削除して学内へ転送される。また、フィッシングとワーム（人手を介さずに拡散するウィルスの一部）と判定されたメールはメールゲートウェイ上で削除される。

2.2　システム移行とサーバ負荷の調整

学外向け DNS で置換される MX レコードに指定するスキャナサーバを変更することにより、新メールゲートウェイへの移行とサーバ負荷の調整を行っている。2020 年 3 月に新メールゲートウェイを構築し、本学の情報連携推進本部が管理するドメインについて、MX レコードを新スキャナサーバへ変更し、動作テストを行った。その後 4 月に、メールゲートウェイを利用する全ドメインについて、MX レコードへ新スキャナサーバを追加して並行運用した後、MX レコードから旧スキャナサーバを削除し、システム移行を完了した。

新旧システムが並行運用することによって仮想基盤が過負荷となる懸念があったため、新スキャナサーバは 4 台のみを本番運用とし、2 台はテスト（待機）運用としていた。

新メールゲートウェイの運用が安定した 11 月に、本番スキャナサーバを 5 台へ増やしたところ（1 台をテスト運用として残す）、IPv4 アドレスしか持たない学外メールサーバの一部において、IPv6 アドレスでメールゲートウェイへ接続しようとして失敗し、本学へメール転送できない現象が発生した。この現象は同年 10 月末の CentOS 6 のサポート終了によって CentOS をバージョンアップしたメールサーバの一部において、Postfix のバージョンが上がってデフォルトで IPv6 の MX レコードが優先的に選択されるようになったことが原因と推測される。問題となる学外メールサーバは IPv4 の IP アドレスしか持たず、CentOS バージョンアップの際に Postfix で使用する IP アドレスを IPv4 に限定する設定（inet_protocols = ipv4）を忘れ、本学の本番スキャナサーバの IPv6 の MX レコードを（Postfix のデフォルトとなる）5 つだけ参照して接続できなくなったとみられる。これは前年まで旧システムでは露見していなかった問題であり、Postfix の正しい設定が普及するのには時間を要すると判断し、メールゲートウェイのスキャナサーバについて、本番運用を 4 台、テスト運用を 2 台へ戻した。

2.3 スパム誤判定の対応

迷惑メール判定ソフトウェアは、セキュリティ的に問題のあるメールサーバの IP アドレスをブラックリストに登録してメールサーバを評価する。クラウドサービスを利用する機関が増えている一方、ブラックリストに登録されたメールサーバを偶発的に利用してしまうことで、スパムメールと誤判定されることが少なからず発生している。

SMG によるメールゲートウェイを運用していた当時、シマンテック社のブラックリストに登録されることで、メールゲートウェイからメール受信拒否をされる学外メールサーバが問題となった。しかし、シマンテック社は公開サイトにてブラックリストの確認と修正依頼が可能なため、メールゲートウェイ担当者にて原因特定した後、学外メールサーバの管理者ならびにメール受信者へスパム誤判定の解除を委ねることができた。

KLMS によるメールゲートウェイでは、スパム誤判定の増加が問題となった。カスペルスキー社は契約者から提出された誤判定メール（検体）を解析し、迷惑メール誤判定を解除する。メールゲートウェイ担当者はカスペルスキー社とメール受信者を仲立ちし、メール受信者におけるメールソフトからのエクスポート作業等（検体採取）をサポートする必要がある。解除手順の煩雑さは、スパム誤判定の増加によってメールゲートウェイ担当者を苦しめた。そこで、スパム誤判定の解除手順を見直し、検体採取の手順をドキュメントとして準備すると共にスパム誤判定の解除申請方法を Web サイトにまとめ、カスペルスキー社への検体提出と受理までを管理し、誤判定の解除結果の確認はメール受信者の判断に委ねることにした。

3 運用のために開発したツール

KLMS は SMG に存在したコントローラに相当する機能がなく、複数台のスキャナサーバを統合的に管理するための仕組みを自前で準備する必要があった。そこで、KLMS に完備されているユーティリティコマンド等を利用して、設定同期、統計データ収集、健全性チェックといったスキャナサーバの統合管理ツール（Python スクリプト）を開発していった。

3.1 設定同期

KLMS の設定変更は KLMS 独自の Web ユーザインタフェース（ダッシュボード）を用いて行う。スキャ

ナサーバの 1 台において KLMS の設定を変更した後、設定同期スクリプトを実行し、メールゲートウェイを構成する全てのスキャナサーバにおける KLMS の設定を変更する。設定同期スクリプトはユーティリティコマンドを用いて KLMS 設定を XML ファイルとしてエクスポートし、XML ファイルを各スキャナに合わせて微調整した後、各スキャナのユーティリティコマンドを用いて XML ファイルをインポートする。

3.2 統計データ収集

各スキャナサーバにおけるメールの流量や迷惑メール判定の状況は、KLMS のダッシュボードを用いて確認できる。しかしながら、メールゲートウェイの運用には全てのスキャナサーバを合算した統計データが必要となるため、ダッシュボードの集計・集約化スクリプトを定期的に実行している。集計・集約化スクリプトは、各スキャナサーバのユーティリティコマンドを用いてダッシュボードのデータを CSV ファイルとして取得し、全てのスキャナサーバの CSV ファイルの値を集計し、1 つの CSV ファイルにまとめ、ログサーバに保存している。

3.3 健全性チェック

迷惑メールのバースト（急増）によってメールキューが溢れてしまったこと（後述）を教訓として、健全性チェックスクリプトを定期的に実行し、各スキャナサーバにおける Postfix と KLMS に滞留しているメールの量を、メールゲートウェイ担当者へ定期的にメールで通知するようにした。迷惑メールのバーストでは、転送できなかったメールを通知するバウンスメールによって Postfix のキューが溢れてしまったため、MailerDaemon（メールサーバからの通知）のメール数もカウントして通知メールに加えている。

4 全国的な迷惑メールの急増とその対応

4.1 メール流量の推移

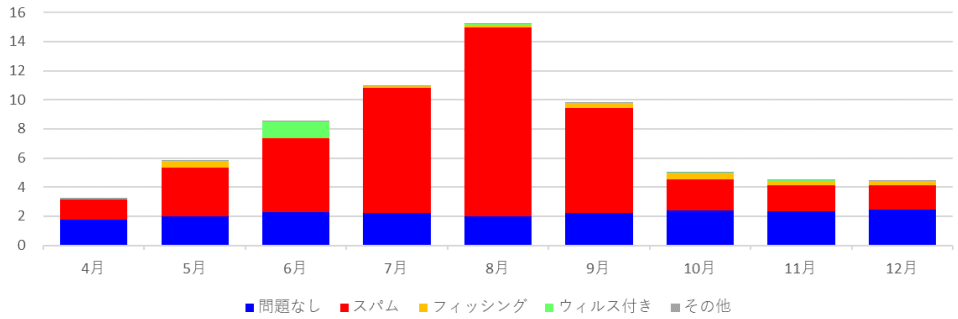

図 2. 新メールゲートウェイのメール流量（2020 年 4 月～12 月、月次、縦軸の単位は非公開）

新メールゲートウェイにおける 2020 年 4 月から 12 月までのメール流量を図 1 に示す。問題なしメールは月次で大きく変化せず、3 月から 4 月のシステム移行においても大きく変化していない。迷惑メールは、旧メールゲートウェイでは問題なしメールの 2 倍程度存在していたが、新メールゲートウェイでは本番運用を開始した 4 月に大きく減少した。これはメールゲートウェイの IP アドレスが変わったことにより、一時的に学外からの攻撃を逸らすことができたためとみられる。

迷惑メールはスパム、フィッシング、ウィルス付きに大別される。スパムメールは、ある特定のスパムの発生が原因となり、5 月から急増し、8 月まで増加の一途をたどり、9 月の中旬に急減した。スパムメールは最終的に学内へ転送されるため、スパムメールの急増によって大量スパムの受信者も発生し、大学の業務に支障が出る事態となっていた。フィッシングメールとウィルス付きメールは迷惑メール全体からみると少な

い。しかし、ウィルス付きメールは 6 月に大量発生した日があり、メールキューが溢れ、学外からのメール受信ができなくなり、大規模なメール配送遅延を生じる被害が出た。

4.2 「ホットな」メールの増加

Carenza
ホットな女の子と女性をお探しですか？
今夜セックスしたい、毎日新しいマンコが欲しい？
（以下省略）

図 3. 「ホットな」メールの本文の例

2020 年 5 月のゴールデンウイーク前後付近から、図 3 のようなスパムメール（本学では「ホットな」メールと呼ぶ、「出会えない系メール」とも呼ばれる[6]）が届くようになった。図 3 は文字参照によって一部が文字番号で記載されているが、「ホットな女の子と女性をお探しですか」「ここであなたは〇〇〇〇の女の子を見つけることができます」等、通常の大学業務において使用する可能性が極めて低い文字列を含んでいる。標準で HTML メールを表示するメールソフトウェアでは、文字番号が実際の文字へ変換された上、本文に類する画像まで表示されていた。「卑猥なメールが大量に届いているのでどうにかしてほしい」といった苦情が寄せられて返答に窮したが、有効な手立てが打てないまま、9 月 16 日を最後にスパムが急減して自然収束した。

この「ホットな」メールは、送信元のメールアドレスや IP アドレスに共通性がなく、KLMS のフィルタ機能では削除できなかった。さらに、新メールゲートウェイにおけるスパム誤判定が多く、スパムメールを削除する運用ポリシーへ変更することもできなかった。学内メールサーバには、大量のスパムによって機能不全となるサーバが発生する一方、送信元のメールアドレスに含まれるドメインと IP アドレスが対応しないメールを拒否する設定で「ホットな」メールを受信拒否するものがあったが、スパム送信サーバがバウンスメールを受け付けないことにより、メールゲートウェイのキューにバウンスメールが滞留することで、該当するドメインにメール転送の遅れが発生していた。

4.3 ウィルス付きメールによる大規模なメール配送遅延

新メールゲートウェイにおける 2020 年 6 月のメール流量を図 4 に示す。2020 年 6 月 9 日にウィルス付きメールが大量発生した。このウィルス付きメールは、送信元のメールアドレスが「{英語の人名のような文字列}{4 桁の数字}@{4 桁の数字}.com」、タイトルが英語の文章、本文が「;)」のみといったものであった。ウィルス感染によるセキュリティ事故は発生していないが、学外からメールが半日以上届かない事態となっていた。

大規模なメール配送遅延の原因はスキャナサーバの Postfix のキューが溢れたことによる。そこで、Postfix のキューのサイズを増やすと共に、一時的に、KLMS によるウィルス付きメールの扱いを（メール転送を行う）ウィルス駆除から（メール転送を行わない）メール削除へ変更、さらに、MailerDaemon からのバウンスメールを cron で定期的に削除することとした。一連の対応によって、新メールゲートウェイの機能は徐々に

回復し、翌日にはシステムを正常化できた。

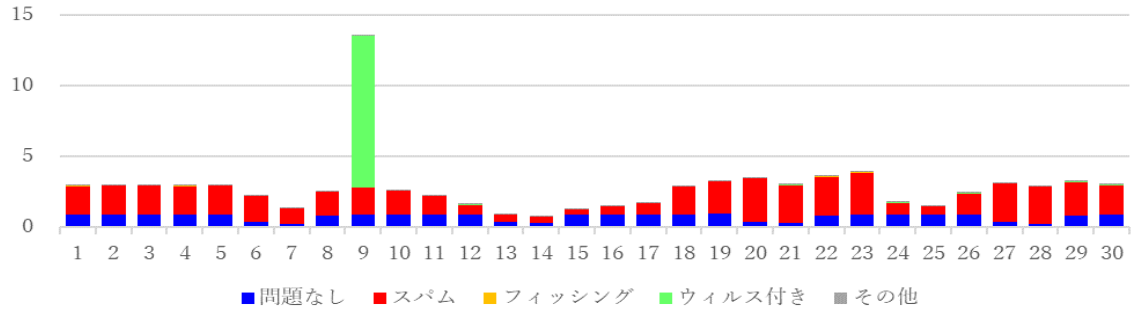

図 4. 新メールゲートウェイのメール流量（2020 年 6 月、日次、縦軸の単位は非公開）

5　名大独自のスパム削除フィルタの開発

大量スパムによる攻撃から本学のメールシステムを守るため、名大独自のスパム削除フィルタ（nu-milter）を導入した。nu-milter は、KLMS でスパムと判定されたメールについて、本文中に特定の文字列を含むメールを削除する。導入時に削除対象としたスパムメールは 4.2 節の「ホットな」メールである。学内では業務に必要なメールが届かなくなると誤認される場合もあったが、削除対象となる一部のスパムメール以外にフィルタ導入による影響はほとんどない（学内のメール受信者からメールゲートウェイの利用中止を示唆されることもあったが、「ホットな」メールをどうしても受信したいならばしかたないとの旨を回答している）。フィルタ設定は人手で行っているが、「ホットな」メールの削除は判定に利用できる特徴的な文字列を含んでいたために過ぎず、オンラインストアや銀行を詐称するスパムメール等、削除したいスパムは多いものの、実際に削除できるスパムメールのパターンは少ない。

nu-milter は Perl スクリプトで、Sendmail::PMilter ライブラリ[7]を利用して開発し、KLMS と同様に、スキャナサーバの Postfix へメールフィルタ（milter アプリケーション）としてインストールし、サービスとして起動し、スパム削除判定を行う。nu-milter は以下の手順でスパム削除判定を行う。

(1) KLMS にてスパム判定されたメールのみを処理対象とする。
(2) 対象メールの本文について、先頭から一定サイズを抽出、Base64 の場合はデコードも行う。
(3) 対象メールに特定の文字列（「ホットな」メールに含まれる特徴的な文字列等）が含まれる場合、削除対象とする。

削除対象となるメールは最終的に Postfix 上で discard（受信者に配信したふりをして、破棄）する。スパム送信者はメール受信できない場合が多く、Postfix のキューが MailerDaemon のメールで溢れてしまうため、Postfix で reject（受信を拒否し、送信者へメールを返信）しない。当初、Postfix でパターンマッチングによりフィルタを行う header_checks や body_checks 設定の利用を検討したが、Base64 に非対応で、エンコードされた文字列について削除対象となる文字列を指定することも困難なため、milter アプリケーションの開発に至った。nu-milter の機能はシンプルであるが、メールゲートウェイ上のサービスとして安定運用を可能とし、大量メールを処理できる性能とするために開発期間を要した。

2020 年 10 月下旬において、一時的に「ホットな」メールが再発した。nu-milter の導入によって削除されたスパムの量を図 5、6 に示す。2020 年 10 月 21 日～23 日において nu-milter が削除したスパムメールを除けば、メール流量は平時のレベルを維持しており（図 5）、スパムメールの急増に対して本学のメールシステムを守る効果があったと考えられる。また、スパムメールが最大となった 10 月 22 日には（図 6）、2 倍以上に

なったスパムメールから「ホットな」メールが削除され、業務影響を抑えることができたと考えられる。

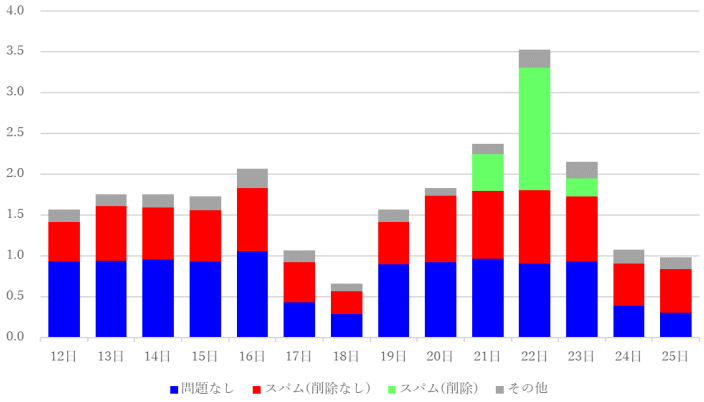

図 5. スパム削除フィルタで削除されるスパム
（2020 年 10 月 12 日～25 日、日次、
縦軸の単位は非公開）

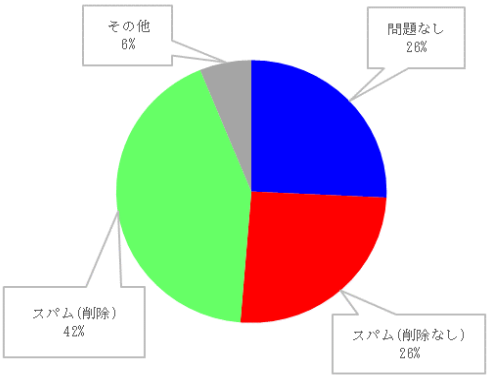

図 6. スパム削除の割合
（2020 年 10 月 22 日）

6　まとめ

新メールゲートウェイの構築と運用について報告した。セキュリティ担当教員から SMG のライセンス更新の断念を告げられた時には天を仰いだが、旧システムの仮想基盤を流用でき、KLMS のインストールが比較的容易だったことが功を奏し、1 ヵ月という短期間で新システムの運用を開始することができた（旧システムは 2018 年に物理サーバから仮想サーバへ移行したが、構築に 1 年程度要した）。スキャナサーバを複数台で運用するためには、スキャナサーバを統合的に管理するための仕組みが欠かせない。KLMS のバージョンアップによってコントローラ機能が追加されることを期待すると共に、運用改善の一環として統合管理用ダッシュボードを開発し、設定同期の実行と統計データの可視化を Web ユーザインタフェースで実現したいと考えている。

新メールゲートウェイの本番運用を開始して一息ついたのもつかの間、全国的な迷惑メールの急増によって大規模なメール配送遅延が発生する等、メールゲートウェイの運用についても厳しい状況となった。特に、2020 年 6 月 9 日は学外からの猛攻撃に晒され、消しても消しても消しても消えない MailerDaemon のメール、1 台ずつ倒れていくスキャナサーバにシビアな対応を迫られた。学外の攻撃からメールシステムを守るためには、運用ポリシーを踏襲しつつも、柔軟な対応が欠かせない。メールゲートウェイの安定運用に努めるとともに、スパム削除フィルタや健全性チェックの改善を進めたいと考える。

参考文献

[1] ブロードコム社、Symantec Messaging Gateway、
https://jp.broadcom.com/products/cyber-security/network/messaging/gateway（2020/12/17）

[2] 情報連携推進本部、“全学向けウィルスメール及び迷惑メール判定システムについて”、
http://www.icts.nagoya-u.ac.jp/nu-only/ja/services/nice/anti-spam.html（2020/12/17）

[3] Broadcom Inc., “Broadcom to Acquire Symantec Enterprise Security Business for $10.7 Billion in Cash” ,
https://www.broadcom.com/company/news/financial-releases/52511, Aug. 2019

[4] カスペルスキー社、Kaspersky Linux Mail Server Security、
https://www.kaspersky.co.jp/small-to-medium-business-security/linux-mail-server（2020/12/17）

[5] 総務省、“第 3 節　新型コロナウイルス感染症が社会にもたらす影響”、令和 2 年情報通信白書、2020 年 8 月

[6] 古賀 勇、“迷惑メールの量が急増中！ 2020/1Q 緊急レポート”、IIJ Engineers Blog
https://eng-blog.iij.ad.jp/archives/6231、2020 年 7 月

[7] Sendmail::PMilter、https://metacpan.org/pod/Sendmail::PMilter（2021/1/5）