

# 電子メールの柔軟な処理を可能とする IMAP エージェント

横木 健太<sup>1</sup> 山井 成良<sup>1</sup> 王 建人<sup>1,†1</sup> 北川 直哉<sup>1</sup>

## 概要：

電子メールにおいて利用者が新たな検査・処理機能を追加する場合、サーバ側への追加は困難なため、端末側へのプラグイン等の追加が一般的である。しかし、IMAP (Internet Message Access Protocol) サーバや Web メールのように電子メールサーバ上でメッセージを管理する形態では、たとえば発信国に基づくスコアリングや分類をメッセージの電子メールサーバへの到着時に行うことはできない。そこで本稿では電子メールサーバに常時接続する IMAP エージェントによりこれらの問題を解決する方法を提案する。

## IMAP Agent for Flexible Email Message Processing

Kenta Yokogi<sup>1</sup> Nariyoshi Yamai<sup>1</sup> Kento Ou<sup>1,†1</sup> Naoya Kitagawa<sup>1</sup>

### 1. はじめに

電子メールは社会活動を支える重要なコミュニケーション手段の1つであり、必要不可欠な存在となっている。一方、電子メールは不特定多数のユーザとメッセージをやり取りできることからセキュリティ上多くの問題を抱えており、特に広告、フィッシング詐欺、マルウェア配布などを目的に不特定多数のアドレス宛に一方的に送りつけられる迷惑メールの蔓延は大きな社会問題となっている。このような迷惑メールに対抗するために、電子メールサービス事業者はメール受信時にメッセージの内容を検査し、検査結果に基づいて分類、隔離、削除、転送等の処理（以下、検査・処理）を行う製品やプログラムを導入している [1], [2].

一般的には、電子メールサーバに導入された上記の製品やプログラムにユーザが新たな検査・処理機能を追加することは困難である。一方、ユーザは MUA (Mail User Agent) にプログラムを導入したり、POP (Post Office Protocol) [5] プロキシを用いたりすることで検査・処理を行うことは可能である。たとえば文献 [3] では POP プロキシを用いて DMARC (Domain-based Message Authentication, Reporting, and Conformance) [4] による送信ドメイン認証を

行うシステムが述べられている。

しかし、IMAP (Internet Message Access Protocol) [6] サーバや Web メールのように電子メールサーバ上でメッセージを管理する形態では、メッセージを実際に取得するまで MUA ではメッセージの内容を検査することができず、検査・処理が遅れることが問題となる。たとえば、発信国に基づくスコアリングや分類をメッセージの電子メールサーバへの到着時に行うことはできない。また、ユーザが複数の端末を用いて1つのサーバにアクセスする利用形態が増えてきている現状では、各端末に検査・処理を行う機能を追加することは利用者の負担が大きい。さらに、バッテリー駆動の端末にこのような機能を追加できたとしても、多数のメッセージに対する検査・処理により電力消費が増大して端末の利用可能時間が短くなってしまいうことも問題となる。また、特に Web メールでは、ヘッダ情報など必要な情報が端末で取得できるとは限らないため、端末側でメッセージの内容に基づく検査・処理を行うことは困難である。

そこで本稿では電子メールサーバに常時接続する IMAP エージェントによりこれらの問題を解決する方法を提案する。この IMAP エージェントはメッセージが電子メールサーバに到着すると直ちにその内容を取得し、検査を実施したり内容に基づいた処理を実行したりすることができる。また、IMAP エージェントを端末以外のホスト上で動作さ

<sup>1</sup> 東京農工大学  
Tokyo University of Agriculture and Technology  
<sup>†1</sup> 現在、SCSK 株式会社  
Presently with SCSK Corporation

表 1 POP3 と IMAP4 の比較

比較項目	POP3	IMAP4
メッセージの管理	MUA 側で管理	MRA 側で管理
MRA 内メールボックスの容量	少ない (通常は新着メッセージのみ保存)	多い (全メッセージを保存)
複数の端末	基本的には考慮せず	プロトコル設計時に考慮
オフラインでの利用	MUA 内のメッセージは常時利用可	ローカルコピーがあるメッセージのみ利用可
メッセージの一部取得	TOP コマンド (オプション) で限定的に可能	かなり自由 (マルチパートで各パート個別アクセス可)

せることにより端末の利用可能時間短縮の問題も解決できる。さらに多くの Web メールサービスでは同時に IMAP サーバも利用可能であることから、Webメールの利用者に対しても検査・処理機能を追加することが可能である。

以下、2 節では IMAP の現行バージョンである IMAP4 について概説する。次に 3 節では提案する IMAP エージェントの動作について説明する。また、4 節では試作した IMAP エージェントを用いた簡単な検査例を示す。最後に 5 節で本稿をまとめる。

## 2. IMAP4 の概要

IMAP (Internet Message Access Protocol) [6] はメールサーバ (正確には MRA: Mail Retrieval Agent) 内のメールボックスに格納されているメッセージを MUA がアクセスする際に用いられるプロトコルである。現行のプロトコルは Version 4rev1 であり、現在では平文通信 (143/TCP を使用) の代わりに暗号化通信を行う IMAP4S (IMAP over SSL/TLS, 993/TCP を使用) の利用が推奨されている [7]。

IMAP4 と同様に MUA が MRA にアクセスする際に用いられる代表的なプロトコルに POP3 (Post Office Protocol - Version 3) がある。POP3 と IMAP4 の最も大きな違いは、メッセージを MUA 側、MRA 側のどちらで管理するかにある。POP3 では原則として MRA のメールボックスに到着したメッセージを全て MUA に転送し、MUA 側で管理する。MRA 内には基本的にはメッセージは残らない。そのため、大容量記憶装置を持つ端末 1 台だけでメールを送受信する場合によく利用される。一方、IMAP4 では MRA 側でメッセージを管理し、原則としてメッセージを実際に読む場合のみメッセージを MUA に転送する。転送されたメッセージは MRA 内に引き続き残り、同じメッセージを他の端末で読むことも可能である。そのため、複数の端末を使用したり、スマートフォンなど記憶容量が比較的小さい端末を利用する場合によく利用される。POP3 と IMAP4 の主な違いを表 1 に示す。

次に、IMAP4 で用いられるコマンドのうち、本稿に関連するものを以下で説明する。

- **FETCH** メッセージ 取得データ種類  
指定したメッセージの指定した種類のデータを取り出す。たとえば、「FETCH 1 RFC822」では 1 番目のメッセージ全体を RFC822 形式で取り出すことを意味

する。

- **STORE** メッセージ 変更方法 フラグ名  
指定したメッセージのフラグ状態を変更する。たとえば「STORE 2 +FLAG \Deleted」では 2 番目のメッセージのフラグに \Deleted を追加することを意味する。
- **APPEND** メールボックス [フラグ] [日時] { サイズ }  
指定されたメールボックスに指定されたサイズのメッセージを追加する。メッセージ本体はこのコマンドに続けて送る。
- **EXPUNGE**  
削除のマーク (\Deleted フラグ) があるメッセージを実際に削除する。
- **NOOP**  
何も行わないコマンドであるが、タイムアウトを起こさないようにセッションを維持し、またサーバのステータス更新通知を受信することができる。
- **IDLE**  
RFC2177[8] で規定されるオプションコマンドで、たとえば EXISTS、EXPUNGE などサーバ側のステータス更新通知応答を直ちに受信することができる。クライアントがこのコマンドを終了したい場合には DONE コマンドを送信する。

## 3. IMAP エージェントによる検査・処理機能の追加

### 3.1 提案システムの構成

提案方式では IMAP エージェントを独立型、プロキシ型の 2 種類の構成で実現することを想定している。独立型の構成を図 1 に、プロキシ型の構成を図 2 に示す。

いずれの構成においても IMAP エージェントはメールサーバとの間で常時 IMAP セッションを維持しており、メールサーバに新しいメッセージが到着すると直ちにそれを全文取得し、内容に基づいて検査・処理を実施する。検査・処理の内容にも依存するが、たとえば 1 節で例示した発信国の検査を行う場合、送信元 IP アドレスをヘッダ内から取り出し、その IP アドレスに基づいて GeoIP[9] などのサービスを用いて発信国を特定し、得られた発信国をヘッダ中に記録するようにする。その際、検査結果を記録したメッセージは APPEND コマンドにより新規メッセージとして追加し、元のメッセージを削除するようにする。

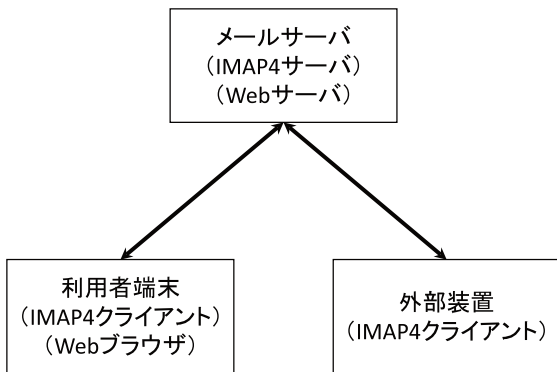


図 1 IMAP エージェントの構成 (独立型)

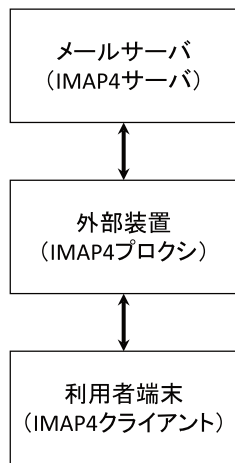


図 2 IMAP エージェントの構成 (プロキシ型)

IMAP4 では複数の端末が存在することを想定してプロトコルが設計されているため、図 1 の構成でも問題ないと思われるが、その場合、他の端末が先に新着メッセージにアクセスして IMAP エージェントが新着メッセージの検査・処理を行えない可能性がある。そのような可能性がある場合、図 2 の構成を用いて全ての端末が IMAP エージェント経由でメールサーバにアクセスするようにし、IMAP エージェントが必ず先に新着メッセージにアクセスするようにすればよい。

### 3.2 提案システムの動作

説明を分かりやすくするため、本節では図 1 の構成に基づき、新着メッセージを検査してその結果をヘッダ中に反映させることを想定して IMAP エージェントの動作を説明する。なお、IMAP エージェントによるメールサーバとの IMAP セッションの確立など、全ての IMAP クライアントに共通する動作は説明を省略する。また、IMAP エージェントが発行する各コマンドの引数についても詳細な説明は省略する。

(1) IMAP エージェントはメールサーバに IDLE コマンドを送信し、メールサーバ上で inbox メールボックスのメッセージ数が更新されるのを待つ。具体的には IDLE コマンドの応答として EXISTS が返されるのを

待つ。

- (2) メールサーバから EXISTS 応答が返されると、IMAP エージェントはこの応答が新着メッセージによるものかどうかを確認する。新着メッセージによるものでなければステップ 1 に戻る。
- (3) IMAP エージェントは新着メッセージを 1 つ選び、その全体を FETCH コマンドで読み出す。
- (4) IMAP エージェントは新着メッセージの検査を実行する。その結果、既に検査を行ったメッセージなど、特にメッセージを変更する必要がなければステップ 1 に戻る。
- (5) IMAP エージェントは検査結果を新着メッセージのヘッダ中に追加した、新たなメッセージを作成する。その際、このメッセージを再び検査しないように、検査結果に一種のフラグを含める。
- (6) IMAP エージェントは APPEND コマンドを用いて新たなメッセージを inbox メールボックスに追加する。
- (7) APPEND コマンドが成功すると、IMAP エージェントは STORE コマンドを用いて元のメッセージに削除フラグ (\Deleted) をセットする。さらに IMAP エージェントは元のメッセージを完全に削除するために EXPUNGE コマンドを発行する。
- (8) IMAP エージェントは他に新着メッセージがあればステップ 3 に戻る。そうでなければステップ 1 に戻る。

なお、IDLE コマンドはオプションコマンドであるため、全ての IMAP サーバで利用できるとは限らない。もし IMAP サーバが IDLE コマンドをサポートしていないものであれば、図 2 の構成を採用し、NOOP コマンドを十分短い間隔 (たとえば 1 分間隔) で実行することにより同様の機能を実現できる。

### 3.3 試作システムの応用例

提案方式の応用例として、たとえば 1 節で示したように送信国の検査が挙げられる。これは MAXMIND 社提供の GeoIP[9] を用いて送信元 IP アドレスから送信国名を取得して、ヘッダに追加するものである。本節では Microsoft Outlook 2013 において送信国名を表示した例を示す。

Microsoft Outlook 2013 ではヘッダ中の Keywords フィールドに設定された文字列をメッセージの上部に表示する機能を有している。そこで IMAP エージェントを用いてたとえば「Keywords: sender country:Japan」のようなフィールドを発信国としてヘッダ中に追加する機能を実装した。なお、本実装では図 2 の構成を採用した。

IMAP エージェントにより送信国名を追加したメッセージを Microsoft Outlook 2013 で表示した例を図 3 に示す。この図により追加したヘッダ中の「sender country:Japan」が表示されていることが確認できる。これにより、試作した IMAP エージェントは想定した通りに動作していること

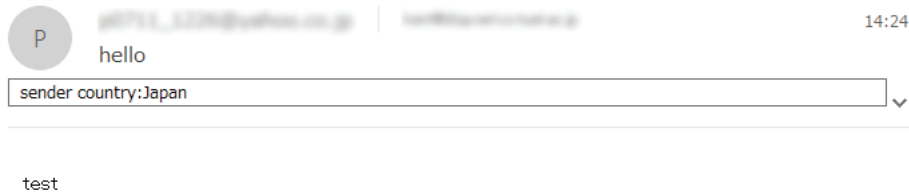


図 3 Microsoft Outlook 2013 での発信国表示例

が確認できた。

#### 4. まとめ

本稿ではメールサーバや端末に新たな機能を追加することなく柔軟な処理を追加可能な IMAP エージェントを提案した。また、IMAP エージェントにより Microsoft Outlook 2013 で送信国名を表示できることを確認した。

今後の課題としてはメッセージの条件に基づいた振り分けや転送など他の機能の実装が挙げられる。

**謝辞** 本研究の一部は国立研究開発法人科学技術振興機構平成 29 年度地域産学バリュープログラムの支援を受けている。ここに記して感謝する。

#### 参考文献

- [1] 日本データ通信協会: 迷惑メール対策 — 迷惑メール相談センター (オンライン), 入手先 (<https://www.dekyo.or.jp/soudan/contents/taisaku/index.html>) (参照 2018-05-14).
- [2] 迷惑メール対策推進協議会: 迷惑メール対策ハンドブック 2017 (オンライン), 入手先 ([https://www.dekyo.or.jp/soudan/data/anti\\_spam/h2017/HB17\\_0\\_all.pdf](https://www.dekyo.or.jp/soudan/data/anti_spam/h2017/HB17_0_all.pdf)) (参照 2018-05-14), 2017 年 11 月.
- [3] Naoya Kitagawa, Toshiki Tanaka, Masami Fukuyama, Nariyoshi Yamai: “Design and Implementation of a DMARC Verification Result Notification System”, *Proceedings of the 13th APAN Research Workshop 2016 (APAN-RW 2016)*, pp.8–14, Hong Kong, China, July 31 – August 5, 2016.
- [4] Kucherawy, M. and Zwicky, E. (Eds.): Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC7489, IETF, March 2015.
- [5] Myers, J. and Rose, M.: Post Office Protocol - Version 3, RFC1939, IETF, May 1996.
- [6] Crispin, M.: INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1, RFC3501, IETF, March 2003.
- [7] Moore, K. and Newman, C.: Cleartext Considered Obsolete: Use of Transport Layer Security (TLS) for Email Submission and Access, RFC8314, IETF, January 2018.
- [8] Leiba, B.: IMAP4 IDLE command, RFC2177, IETF, June 1997.
- [9] Maxmind Developer Site: “GeoIP Products << Maxmind Developer Site (online), available from (<http://dev.maxmind.com/geoip/>) (accessed 2018-05-14).