PPAP 廃止のための RPA を用いた S/MIME 利用の自動化・効率化

芹澤玲哉 [1,*]　佐々木良一 [1]　齊藤泰一 [1]

概要：現在は様々な場面でメールが使用されており，機密な情報をメールを用いて送る際に，メールに，パスワードが必要な圧縮をした資料を添付し，別のメールでそのパスワードを送る PPAP が広く用いられている．しかしそれは安全性に欠けるうえに，使い勝手も悪いという問題がある．その代替案としてメール本文を暗号化し，認証する機能を持つ S/MIME がある．だが現在は，暗号化に使用する証明書の導入の困難性などから普及していない. 本研究では, そのような S/MIME に対して利用しやすくする方法として RPA（Robotic Process Automation）を用いた自動化を試みたので，その方法と効果に関する検討結果を報告する．

キーワード：メールセキュリティ，S/MIME，RPA

Automation and efficiency improvement of S / MIME usage using RPA for the abolition of PPAP

Serizawa, Reiya[1,*]　Sasaki, Ryoichi [1]　Saito, Taiichi[1]

Abstract: Currently, email is used in various situations.When sending confidential information by e-mail, PPAP is widely used, in which a compressed document that requires a password is attached to the e-mail and the password is sent by another email.However, it is insecure.In addition, there is a problem that it is not easy to use.As an alternative, there is S/MIME that has the function of encrypting and authenticating the e-mail body.However, at present, it is not widely used due to the difficulty of introducing certificates used for encryption.In this study, we attempted automation using RPA (Robotic Process Automation) as a method to make it easier to use for such S/MIME, and report the method and the results of examining the effects of that method.

Keywords: Mail Security，S/MIME，RPA

1. はじめに

現在は様々な場面でメールが使用されており，機密な情報をメールを用いて送る際に, メールに, パスワードが必要な圧縮をした資料を添付し，別のメールでそのパスワードを送る PPAP が広く用いられていた. しかしそれは安全性に欠けるうえに, 使い勝手も悪いという問題がある. このため, 平井卓也デジタル改革担当大臣は 2020 年 11 月 24 日の記者会見で, 通称「PPAP」を内閣府と内閣官房で 11 月 26 日に廃止すると発表している[1].

・　メールの安全な暗号化と，デジタル署名のためには，S/MIME （Secure / Multipurpose Internet Mail Extensions）という方式が決められている．S/MIME にはメール暗号化のための S/MIME 暗号化の機能と S/MIME 署名の機能を持つ．S/MIME の方式を用いるには，送信者と受信者側との両方が S/MIME に対応する電子メールソフトを使用している必要があるが，Microsoft 社の Outlook や iPhone・iPad のメールソフトなど多くのメールソフトが対応している．したがって，S/MIME はメールの暗号化のための本命であるといえる．メールサーバ間やメールサーバと PC 間で，TLS などを用いて暗号化する方式はいろいろあるが（例えば, STARTTLS）, これらは, S/MIME のように, 送信用 PC と受信用 PC 間の END-END での暗号化ではない．したがって，メールサーバ運用者による不正のメール閲覧などを防止できない．

・　しかし, 情報処理について専門知識を持たない一般の人も含めて多くの人が，S/MIME を用いて暗号と電子署名を行おうとすると次のような課題が生じる．

（課題１）S/MIME ソフトを導入するのが初心者には難しい

（課題２）電子証明書の導入が初心者にはむつかしい

（課題３）電子証明書が高額

（課題４）使っている暗号方式の安全性が疑問

（課題５）異なるメールソフトでの互換性が疑問

（課題３）－（課題５）については，初期調査で比較的簡単に解決しうることが分かったが，（課題１）（課題２）の解決は簡単でないことが分かった．そこで，わかりやすいマニュアルを用意するだけでなく，RPA(Robotic Process Automation)を用いて，操作の自動化効率化を行い（課題１）（課題２）の解決を図ることとした．本稿では，これらの解決法案と，現在までに実装し，明確になった事項を報告する．

なお，S/MIME に関する研究（例えば[2]-[4]）や RPA(Robotic Process Automation)に関する研究（例えば[5]）はあるが，Google Scalar に（S/MIME AND Robotic Process Automation）を入力して検索した結果ヒットするものはなかった．

1 東京電機大学
Tokyo Denki University
* 21kmc09@ms.dendai.ac.jp

2. PPAP の問題点と S/MIME の利用

2.1 PPAP の問題点

PPAP とは，パスワード付きの暗号化した zip ファイルとパスワードをそれぞれメールで送信することで悪意のある第 3 者からの攻撃を防ぐセキュリティ方式である．メールの暗号化添付ファイルの送信方法として，次のようにして送付する．

① Password 付きZIP 暗号化ファイルを送ります
② Password を送ります
③ A ん号化（暗号化）
④ Protocol

PPAP は，数年前にヒットした「ペンパイナッポーアッポーペン（Pen-Pineapple-Apple-Pen）」の略称にかけた造語であり，命名したのは日本情報経済社会推進協会（JIPDEC）を経て「PPAP 総研」を設立した大泰司章氏であるといわれている．

しかし，同じ経路で zip ファイルとパスワードを送信することになるため，悪意のある第 3 者がその経路からメールを奪えるならそのどちらについても手に入れることができてしまうため安全性が低いことが指摘されている[6]．zip ファイルとパスワードのどちらかを誤送信しても両方がないと解凍できないので読み取られることのないというメリットについても，利用者が宛先を間違えて記憶しているなら無意味である[6].

以上のことから，送信した zip ファイルとパスワードにそれぞれアクセスされる可能性がほぼ等しいことから何もせずメールで送信する場合と効果があまり変わらず，セキュリティとしては意味のない方法となっている．そのような用法をすることは無駄手間に等しく，反対に zip ファイルの特性からマルウェア攻撃に使用される危険がある．

現在では以上のような問題点が共有され使用を控えるようになっている．現在メールセキュリティを向上する場合は複数の方法があるが，初期設定後の使い勝手と安全性の両方について高品質に達成できるものに S/MIME が存在する．

2.2 S/MIME の概要

メールに署名や暗号化する方法はいくつかあり，メールの送信経路を暗号化する SSL や TLS とメール本文を暗号化する OpenPGP と S/MIME がある．前者については，エンドツーエンドの暗号化は実現できず，また，メールの認証機能を持たない．また直前のバージョンについて脆弱性が確認されており，これだけに頼るメールは将来的に安全とは言えなくなる危険がある．後者について，その 2 つは署名や暗号化の方法は同じだが，公開鍵の正当性を証明する方法が異なる．今回は公的に信用されている認証局(CA)を利用して公開鍵を信頼してもらう S/MIME を用いる．メールを送りあう同士で証明書の認証を行う OpenPGP より一般に信頼性が高いためである．S/MIME のメール通信については図 1 のとおり行う．

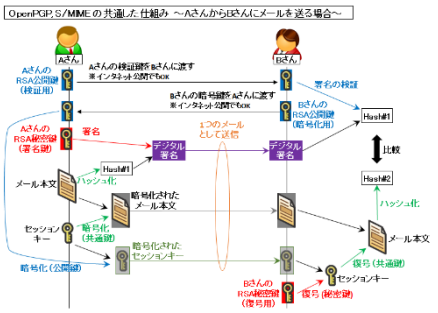

図 1　S/MIME のメール通信

出典：https://milestone-of-se.nesuke.com/sv-advanced/digicert/openpgp-smime-tls/amp/

まず以下の 3 つを作成し，それをまとめてメールとして受信者に送信する．

① メール本文をハッシュ化した値を自身の秘密鍵で暗号化して署名したもの
② メール本文をセッションキーで暗号化したもの
③ セッションキーを受信者の公開鍵で暗号化したもの

受信者はそのメールについて，暗号化されたセッションキー(= ③)を自分の秘密鍵で復号しセッションキーで暗号化されたメール本文(=②)を復号する．最後にメールに添付した本文のハッシュ値と復号した本文をハッシュ値化したものを比較しそれが等しいとメールに改編が含まれる危険のない安全な送信が正しく行われたと判断する[7] ．

以上より，S/MIME は，暗号技術を高度に使った方式であり，エンドツーエンドの暗号化や，電子署名を実現しており，安全性が高い方式であるといえる．また，一度初期設定を終えれば，以下に示すような操作をするだけなので初心者でも使いやすいといえる．

Thunderbird の場合は図 2 のようにメール作成時に「セキュリティ」右の矢印を押して，「このメッセージにデジタル署名」にチェックを入れるとデジタル署名を，「暗号が必要」に「・」をつけてメールを送信する．

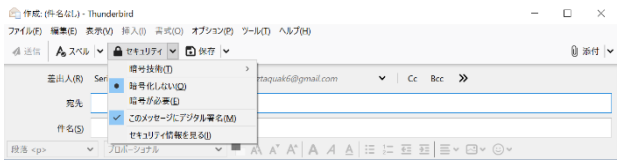

図 2　Thunderbird のメール作成画面

Outlook では図 3 のようにリボンにある「オプション」をクリックし，「暗号化」にある署名をクリックするとデジタル署名を，暗号化をクリックしてから送信すれば暗号化したメールを送信することができる．

図 3　Outlook のメール作成画面

しかし，次節に示すような解決すべき課題も考えられる．

2.3 S/MIME 適用上の問題

S/MIME 適用上の課題として次のようなものがあ

る．

（課題１）S/MIME ソフトを導入するのが初心者には難しい

（課題２）電子証明書の導入が初心者には難しい

（課題３）電子証明書が高額

（課題４）使っている暗号方式の安全性が疑問

（課題５）異なるメールソフトでの互換性が疑問

調査の結果（課題３）の電子証明書が高額な点については，イタリアのサイトである Actalis を利用すれば無料で S/MIME の電子証明書を手に入れることができる．（課題４）についてはこの証明書は Version3 に対応しており，ハッシュ関数は SHA256，公開鍵暗号は 2048bit 鍵長の RSA を採用するなど，暗号の現時点での安全性は高い．

（課題５）のメールソフトでの互換性については Outlook と Thunderbird の間では本文や添付ファイルに異常は見られなかった．今後，他の組み合わせについても今後検討していく予定である．

したがって，（課題１）と（課題２）の解決が必要となる．導入するのが難しい課題について，導入をわかりやすくするために証明書を入手するためのマニュアルを作成し，できるだけ詳しくない人でもわかりやすくなるように努めた．これ以外に RPA(Robotic Process Automation)を用いて自動化を行い，利用者の手間を最小限にする方法の実装を試みた．

3. RPA を用いた S/MIME の公開鍵証明書入手の効率化法

3.1 RPA の概要

RPA(Robotic Process Automation)はパソコンを使って人間が行っていた様々な作業を機械的に代行することができるようにする仕組みである ．

RPA 用のシステムにはいろいろなものがあるが，ここでは無料で使える Microsoft の RPA「Power Automate Desktop」を使用して S/MIME の証明書を利用しやすくするために自動化を試みた．Microsoft Power Automate Desktop を導入することで，Excel への入力作業やコピー，業務システムへの転記作業など，アプリケーションをまたいだ操作もプログラミングの専門知識なしに自動化できるとされている．

使用方法としては，RPA のフロー作成ツールに対して命令を記述する．「MicrosoftEdge の起動」であれば，URL を開くか既に開いているものを扱うか決める．URL を開く場合はそれを指定する．変数が生成されるが，これは対象の Web ページの操作に必要となるインスタンスである．基本的な使い方について，詳しくは文献[7]を参照願いたい．

3.2 RPA を用いた S/MIME のための公開鍵証明書入手の自動化・効率化の構想

自動化を試みる対象としては当初，次のようなものがあった．

（１）S/MIME ソフトの自動インストール

（２）S/MIME 用電子証明書の自動入手とインストール

以下では，（２）の方法について記述する．

S/MIME 用電子証明書の入手とインストールのためには次のような作業が必要となる．

手順１　証明書発行機関にアクセスし（今回はイタリアのサイトである Actalis），証明発行用画面を表示する

手順２　上記画面のメールアドレス欄に自分のメールアドレスを入力して確認メールを明書発行機関に送信する

手順３　送られてきた確認メールを識別し，メール本文にある確認コードを入手する

手順４　要項にチェックを入れフォームを証明書発行機関に送信する

手順５　署名付きメールから証明書を手に入れる

手順６　証明書をインストールする

RPA は，それらをできるだけ自動化することを目指す．

4. RPA を用いたシステムの試作と評価

4.1 システムの試作結果

RPA の設定を行い，次のような作業の自動化を可能とした．

（手順１）　証明書発行機関 Actalis にアクセスし，図 4 に示すような証明書発行用画面を表示する.PRA に MicrosoftEdge で任意のサイトを開くフローが存在するためそれを使用してサイトを開くようにした．

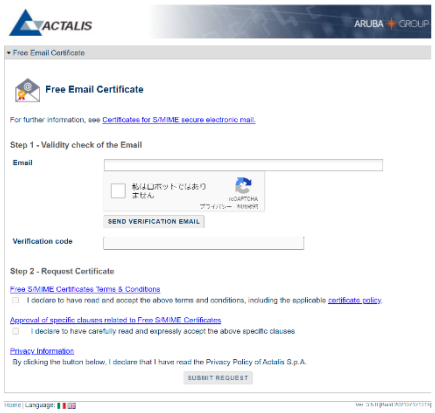

図 4　証明書の入手フォームの画面

（手順２）　上記画面のメールアドレス欄に自分のメールアドレスを自動入力して確認メールを証明書発行機関に送信する

RPA を用いて MicrosoftEdge を立ち上げると，証明書の入力フォームが表示され，メールアドレスと証明書の保存先の入力フォームが表示される．

利用者は入力ダイアログを使用してメールアドレスを図 5 に示すように入力する．これを変数に使用し，あとでメールを受け取った際のアドレスとして使用する．

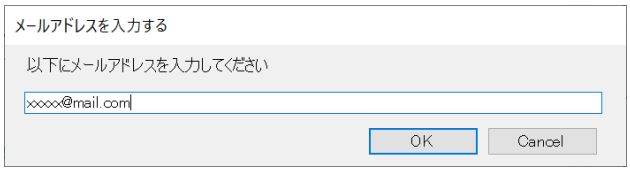

図 5　メールアドレスの入力

利用者は図 6 に示すようにフォルダ選択ダイアログを使用し証明書の保存先を指定する．RPA の実行後にここに証明書が入り，一時的に使用するテキストファイルの保存先でもある．

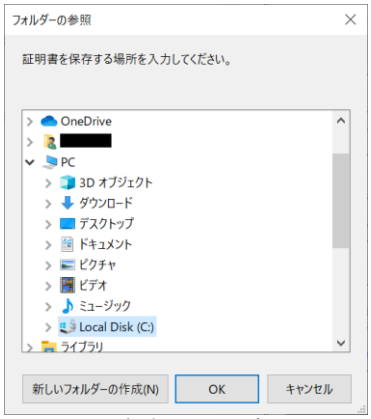

図 6　保存先フォルダの選択

それを入力すると前述した Actalis の証明書を入手するページにメールアドレスが入力される．具体的には，Web 内のテキストフィールドへの入力フローに，メールアカウントをフロー変数から RPA の機能を用いて自動入力し，自動的にクリックボタンを押して確認メールを送信する．そうすると確認メールがメールアドレスに送信される．

(手順３)利用者に送られてきた確認メールを識別し，メール本文にある確認コードを自動的に入手する

証明書の入手のためには，確認コードを受け取り，それを入力フォームへ入力する必要がある．RPA は Outlook を起動しメールメッセージを入手する．ループを使用して該当メールが取得できるまで行う．送られてきたメールについてはメールの識別にはメールタイトルなど使用する．メールを取得するとメール取得の際のカウントが 0 ではなくなるためそれを条件にする．メールに書かれた確認コードを抽出するため，メールメッセージをテキストファイルに書き出してからテキストの内容をフローで読み込み変数にする．これにより，変数の配列を指定すると任意の行を読み込むことができる．確認コードの指定を行で指定するが，条件による処理ができないか検討の余地がある．現状本文にある確認コードについては直接メールから抽出できないため，メールメッセージをテキストファイルに保存してそれを読み取り，本文の行を指定してテキストフィールドに入力する．書き出しに使用したテキストファイルは使用しないため削除する．

「わたしはロボットではありません」については，ＲＰＡを利用してメッセージボックスを表示し，実行者が手動でチェックをしてからメッセージボックスの OK をクリックするよう指示する．この箇所のみ自動化を行わなかったのは機械ではないことの証明であるため自動化することには問題があるためである．

(手順 4)　要項にチェックを入れフォームを証明書発行機関に送信する

入力するとページが変わるため，RPA は MicrosoftEdge の新しいインスタンスを取得する．Web の自動ページクリックで証明書の規約をクリックとフォームを送信を行う．UI オートメーションを使用し画像認識を行う．

(手順 5)　証明書付きメールから証明書を手に入れる

フォームの送信を行うと証明書の添付されたメールが送信される．メールの取得フローでは添付ファイルの取得が可能なため RPA は Outlook を起動して再び取得する．ファイルは圧縮されているため RPA で自動解凍を行う．先ほど取得したファイルとあらかじめ入力してある保存先に解凍した証明書を移動させる．

（手順 6）　証明書をインストールする

証明書の導入についても自動化を検討したが，Outlook などの RPA での動作は難易度が高く正常に動かすには検証が足りず，現状は実現できなかった．

また，その他の部分について，メールアカウントが正しくないときのエラー処理を充実させたかった．例えば，何も書かれてないとメールアカウントの入力を再表示するなどである．確認メールの取得について Outlook 以外(Thunderbird など)での取得も検討したい．どれを選ぶかをラジオボタンで選択できるようにしたい．

4.2　試作結果に対する考察

S/MIME の電子証明書自動取得については一通り実装ができた．これにより，利用者の作業が大幅に低減できると予想できる．しかし，システムとしては完全とは言えずエラー処理の調整が完璧とは言えない．それに加え，証明書を実際に使用する場合にはメールソフトで使用するための設定が必要である．その自動化については今後の課題となる．

今後としては Outlook などのメールソフトへ証明書を導入するところまでの自動化を完成するとともに性能評価のため複数人に使用してもらいアンケートで使い勝手を評価してもらう予定である．

5.　おわりに

今回の自動化では証明書の入手をするところまでの実装を行った．Outlook などのメールソフトに証明書を導入するところまで RPA を完成させるとより簡単に S/MIME が使用できると思われる．

今後の課題としては，現状完成しているシステムのエラー処理などの調整とメールで使用できるようにするためのシステムの完成や，そのシステムを使用することでの使い勝手の評価があげられる．

これらを RPA で自動的に実装する努力を行うとともに，実装がむつかしい部分については，わかりやすいマニュアルとのリンクなどの対応も検討していきたい．

6.　参考文献

[1]パスワード付き zip、内閣府と内閣官房で 26 日から廃止へ

https://www.itmedia.co.jp/news/articles/2011/24/news097.html
[2] Adrian Reuter, Ahmed Abdelmaksoud, Karima Boudaoud ,and Marco Winckler(2021) Usability of End-to-End Encryption in E-Mail Communication, NCBI
[3] Kunal Meher, Divya Midhunchakkaravarthy(2020), The State-of-the-art Cryptographic Algorithms, Journal of University of Shanghai for Science and Technology、Vol.22 ,No,142-145
[4] Jörg Schwenk, Marcus Brinkmann, Damian Poddebniak, Jens Müller, Juraj Somorovsky, Sebastian Schinzel, *Mitigation of Attacks on Email End-to-End Encryption*, CCS '20: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security
[5]Akshay P N1 , Nisarga Kalagi2 , Deeksha Shetty3 , Ramalingam H M 4(2020), EMAIL CLIENT AUTOMATION WITH RPA, JOURNAL OF CRITICAL REVIEWS, Vol.7, No, 787-795
[6] 佐々木良一(2021),「脱ハンコ」と「ＰＰＡＰ廃止」に関する動向の分析と対策の考察, SCIS2021
[7]【図解】OpenPGP と S/MIME の仕組みと違い ~メール暗号化と署名，ssl/tls との違い~
https://milestone-of-se.nesuke.com/sv-advanced/digicert/openpgp-smime-tls/amp/
[8]タダで使える Windows 用業務自動化ツールを活用! Microsoft「Power Automate Desktop」の使い方