［さようなら，意味のない暗号化 ZIP 添付メール］

3 我々はなぜ PPAP するようになってしまったのか

上原哲太郎 | 立命館大学

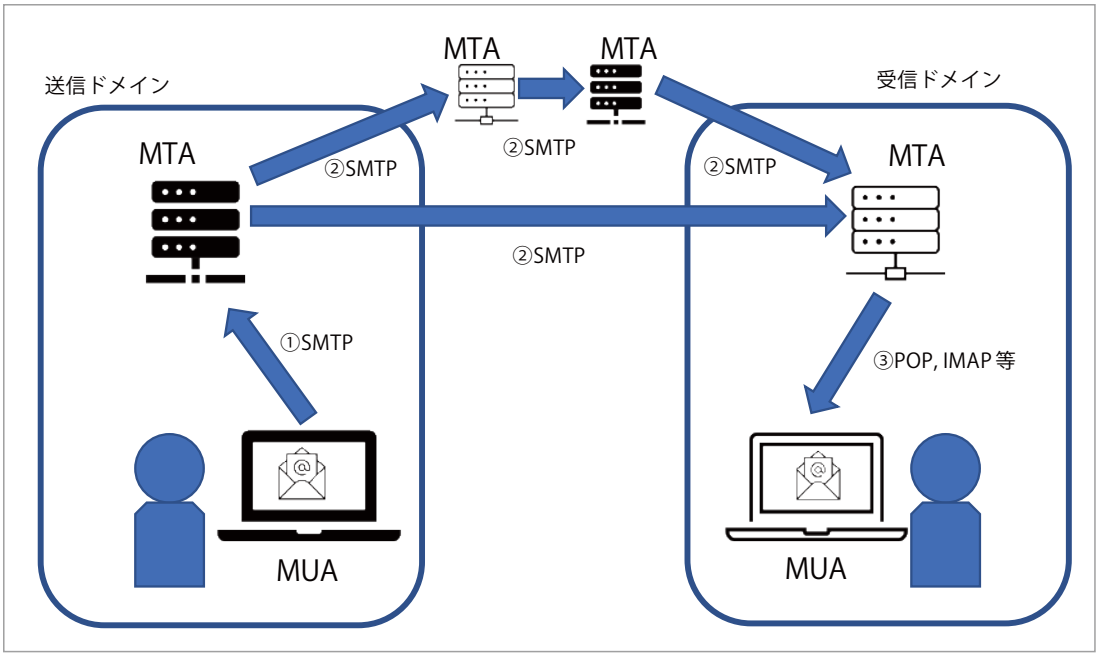
PPAP はなぜ生まれたか

情報システムのセキュリティ確保には技術的対策は欠かせないが，技術を運用するのは人だ．人に頼る限りは技術的に見て誤った対策でも広く使われるようになってしまうことがある．その最たるものがPPAP，すなわちパスワードにより暗号化されたファイルとそのパスワードを同経路で送ってしまうことであろうと思う．PPAP の定義については名付け親たる大泰司氏の別稿に譲るとして，ここでは「なぜ PPAP が生まれ，ここまで普及したのか」を論じよう．

電子メールは，そもそもセキュリティ上とても悩ましい存在である．インターネットがまったくの性善説で運営されていたころに生まれた電子メールは，そもそも認証や暗号化の仕組みに乏しい．電子メールは図 -1 にあるように，送信側の組織（送信ドメイン）と受信側の組織（受信ドメイン）に分かれた組織が協調して送受信を行う．その手順は，大きく分けて以下のような 3 段階からなる．

①送信者の MUA (Mail User Agent，いわゆるメーラと呼ばれるクライアントプログラム）から送信側の組織の MTA(Mail Transfer Agent, SMTP サーバ）に SMTP でメールを送信する．この際，利用者認証である SMTP AUTH や，SSL/TLS を用いた暗号化とサーバ認証である SMTPS の利用は必須とされていない．

②送信ドメインの MTA から，受信ドメインの MTA に SMTP で，直接または他の MTA を経由して送信する．この際，SSL/TLS を利用して受信側 MTA を



■図 -1
電子メール伝送の仕組み
How e-mails are transferred

認証し暗号化するSMTPSは必須とされていない．

③受信ドメインでMTAのメールボックス内に格納された電子メールを，受信者のMUAがPOPまたはIMAP経由で受信する．この場合はメールボックスに対する利用者認証は行われるが，やはり暗号化は必須とされていない．

電子メールがSMTPで配送されるようになった初期には，これらのいずれも段階においても通信は暗号化されておらず，その規格すらなかった．現在③は，認証に使われるパスワードを保護する観点からSSL/TLSで暗号化されることが多い．①においては主に迷惑メール送信を抑止する観点から暗号化や利用者認証を行う例が増えてきた．しかし②のMTA間通信については，暗号化はまだまだ十分ではない．仮に暗号化されていたとしても，複数のMTAを中継した通信である場合には，その中間のMTAにおいて盗聴等が行われない保証はない．何より利用者にとって送信前にその電子メールがどのようなMTAを辿って相手まで届けられ，またその通信や間で暗号化されるか確かめる手段はない．受信者にとっても（ヘッダから類推は一応できるものの）途中経路で盗聴されなかったか確かめる手段もない．

これらのことから，電子メールの送受信の仕組みだけ見れば，どこかに盗聴やなりすましの可能性が残っている．そもそも電子メールはその到達性も保証されていない，まさにベストエフォートなサービスである．しかしその緩さ故に利用や運用のコストを低く抑えることができ，それが電子メールの広い普及を支えてきたとも言える．

その後，次第にインターネットがインフラとしての重要性を増し，セキュリティ上の脅威が認識されるにつれ，インターネット上のどこかでの盗聴の脅威に備えて何らかの暗号化が必要であるという認識は広まった．この問題の解決には，メール本文や添付ファイルを暗号化する必要がある．そのため公開鍵暗号を用いたエンド・トゥ・エンド(E2E)での暗号化と電子署名による送信者認証を可能とするメール暗号化方式として，PGPやS/MIMEが提案され規格化された．しかし，HTTPSなどの通信路暗号化方式がサーバ側に公開鍵と秘密鍵のペアを持ちさえすればよいのに比べ，メールの場合はすべての利用者がそのメールアドレスに対応する公開鍵と秘密鍵を個別に持って管理する必要があり，この鍵の管理の煩雑さやコスト（特にS/MIME用の電子証明書コスト）が嫌われ，メールの標準的な暗号化は普及しなかった．

この状況でひねり出されたのが「添付ファイルをパスワードによる共通鍵で暗号化する電子メール」である．その暗号化も，当初は専用のソフトウェアが用いられる例もあったが，汎用性がありパスワードによる暗号化が可能なZIP形式が次第に主流となった．重要なファイルをZIPで圧縮しつつパスワードを用いて暗号化してから添付ファイルとして送付し，パスワードについては文書やFAXなどの別の手段で共有する手法が広まった．さらに，PマークやISMSなどのセキュリティ認証取得に際して「重要な情報を含むメールは暗号化すること」が求められたことにより，このようなパスワードによる暗号化をセキュリティ対策として認める動きが広がった．

しかしこのパスワードの伝達を電子メール以外の手段で行うことはきわめて煩雑であり，運用コストが高い．そこで，苦肉の策として「パスワードを別メールで送付する」という規定で運用する組織や企業が現れ，PPAPが誕生したのだろうと考えている．さらに，このような方式が各組織においてセキュリティ対策として認められてしまったことや，その疑わしい有効性に対して「メールによる情報漏えいの主なリスクは盗聴ではなく誤送信であり，その対策として一定の効果がある」という理屈がひねり出されたことにより，一気に普及が加速したように感じている．

このPPAPの普及にはもう1つ要因があるので

はないだろうか．一般にセキュリティ対策はシステムの利用者に負担を強いる．PPAP はまさに利用者にとって「余計な一手間」であって，本来ならこのような運用負荷を増すセキュリティ対策は受け入れられなかったかもしれない．しかし，特に技術的知識が十分ではないホワイトカラーの人々にとっては，パスワードはきわめて身近で分かりやすいセキュリティ対策である．ZIP ファイルを作成してパスワードを設定するという手間が，まさにセキュリティ対策をしているという実感，満足感を生んでしまうがために，PPAP はセキュリティ対策として広く受け入れられるようになったのではないだろうか．

PPAP に意味はあるか

現在では多くの企業や組織が添付ファイルの外部送信の際の PPAP を内規で義務づけたり，果ては PPAP を自動で行うシステムを導入している．しかし PPAP にセキュリティの観点からは効果がないことは明らかだ．暗号化されたファイルと，その復号に必要なパスワードを同一経路で送る限り，片方を入手できる攻撃者は他方も入手できるからである．

では実際にそのようなメールの読み取りは行われているのだろうか．最近被害が多いビジネスメール詐欺（Business E-mail Compromise : BEC）では，実際の取引でやりとりされているメールに突然割り込む形で，別の銀行口座への振込先変更などの指示をメールで送りつけ，金銭を奪取する手口が知られている．このようなことが可能なのは，その取引に関するメールをずっと覗き見られているからである[1]．その読み取りはマルウェアによって端末の制御をまるごと奪ったり，電子メールの読み出しに必要なアカウント（ID とパスワード）をフィッシング手法などによって奪ったりすることが先に行われているからだと考えられている．つまり電子メールの盗聴は攻撃の前段階として，きわめて広く行われると考えてよい．電子メールのアカウントそのものが奪われている状況では，すべての電子メールは攻撃者に読み取られるわけだから，PPAP はセキュリティ対策としてまったく役に立たない．

加えて，多くの場合はパスワードを用いて暗号化された ZIP ファイルの解読はそれほど困難ではないから，実は攻撃者にとっては，パスワードを知ることさえ必要がない．暗号化 ZIP ファイルの解読はオフラインでの総当たり攻撃が可能であるので，相当複雑なパスワードでない限り解読が可能である．少し古いデータであるが，文献 2）によると 2012 年当時の 1 台のパソコンで ZIP パスワードを 1 秒間に 45 億回試行可能であった．2020 年の現在，仮に 1 秒間に 100 億回のパスワード試行が可能なパソコンを用いると，英小文字と数字の組合せ 8 桁のパスワード全試行は 282 秒しかかからない．これに文字種として英大文字を加えたとしても，総当たりに要する時間は 6 時間ほどでしかない．オフライン攻撃に耐え得るパスワードは十分な文字種の複雑さと長さを要するが，文書など別の手段でこのパスワードを受信者に伝え，正しく入力してもらうのはきわめて繁雑な作業になってしまう．

このように，パスワードに頼ったファイル暗号化は，セキュリティを保つためにはきわめて煩雑な作業を受信者に強いることとなり，労働生産性に少なからぬ悪影響を与えていると思われる．ところが PPAP 方式を採る限り，普通の平文メールに比べてセキュリティ的なリスクが下がっているかはきわめて疑わしい．さらに，現在のメールを用いた業務で最も注意すべき標的型メール攻撃に対して，暗号化 ZIP ファイルは受信側 MTA でのマルウェア対策を無効化してしまうため，かえって受信者のセキュリティリスクを高めている恐れがある．このように，PPAP はセキュリティ向上には事実上役に立っておらず，生産性の低下とマルウェア混入リスクを高めるだけの存在ではないだろうか．

PPAP の代替手段はあるか

ここで原点に戻って，そもそも電子メールのセキュリティはどうあるべきで，PPAP に代わるセキュリティ対策はどうあるべきなのかを考察する．

ここでは，電子メールのセキュリティ対策として

①通信経路における盗聴のリスク

②メール送信者を詐称したメールを受信するリスク

③メール送信時に誤った受信者を指定し，内容を読み取られるリスク

上記 3 つのリスクを軽減することを考える．PPAP は本来①を軽減するために考えだされたものと思われるが，実際にはすでに述べたように盗聴防止としては役立たない．②はマルウェアや BEC 対策として重要だが，PPAP では対策できず，むしろマルウェア対策には有害である．③に関しては，すでに述べたように PPAP が一定の防止策となるという意見があるが，それは暗号化したファイルを送信してからパスワード送信までに誤送信に気づく可能性がある，という主張であり，少なくとも自動化された PPAP ではリスク軽減に役立たない．

では，このようなリスクを軽減するべくファイルを送信するにはどうしたらよいのだろうか．

(1) 最優先で考えるべきは，やはり S/MIME や PGP といった，E2E での暗号化を実現する技術の利用である．これらの技術は上記リスクの①と②を軽減することができる．ただし，③については，送信アドレスを誤って指定し，かつ送信先の公開鍵を保有していた場合には防止できないのでリスク軽減は難しい．また，S/MIME や PGP はその運用コストが嫌われてきた歴史があり，限られた組織や利用者を除いては今後も普及する見込みは薄いと思われる．

(2) そこで代替案として考えられるのが，既存の電子メール基盤の強化である，すでに述べた通り PPAP が生まれる原因となった電子メールのリスクは上記①，より具体的には MTA 間の通信の暗号化と相互認証が保証されていないことである．しかし現在はメールの転送トポロジは単純になってきており，送受信ドメイン以外に属する MTA が配送に介在する可能性は低い．さらに転送経路の SSL/TLS 暗号化も進んでおり，受信ドメインの MTA が TLS 対応であることを広報したり，TLS 以外での受信をしないことを宣言できる MTA-STS（MTA Strict Transport Security）という規格の普及も始まっている（RFC 8461）．よって，現在は MTA 間通信における盗聴のリスクはかなり小さくなっている．ここで不足しているのは，電子メールの送信者が，この MTA 間通信が安全に保護されていることを事前に知る手段である．ここは適切なツールが提供され，MUA と統合されることが今後求められてくると思う．これさえ提供されれば，送信者はそれを用いて経路の安全性を確認できれば，ファイルを暗号化せずに電子メールに添付し送信できるようになるはずである．

(3) いま現実に利用可能な策としては，Google Drive や OneDrive，Dropbox といったクラウドストレージの利用が考えられる．電子メールにファイルを添付する代わりに，これらのストレージを参照するための URL を電子メールに記述する方法である．これらクラウドストレージは通常 HTTPS を用いているので，上記①のリスクは相当低減される．受信者も同じクラウドストレージにアカウントを所有していれば，送信者も受信者を確実に指定できるし，受信者も送信者を確認しやすいので，上記②や③のリスクも低減できる．仮に送信者が受信者を間違って指定してしまったら，気づいた時点でファイルの共有を無効にすればよい．

この種のクラウドストレージによるリスクとして残るのは，クラウドストレージ事業者自身によりファイルを読み取られるリスクである．このリスクの低減には，そもそもクラウドストレージ上に置くファイルを ZIP 等でパスワード暗号化しておいて，メールでそのパスワードを伝える方法がある．もちろんこの場合も電子メール盗聴によるリスクは残るが，クラウドストレージ側でも送受信者双方が利用者認証されているという前

提であれば問題にならない．

なお，このようなファイル授受に特化したクラウドストレージとして Firefox Send がある．このシステムは以下のような特徴を持っている．

(a) ファイル送信者は Web ブラウザを用いてファイルをクラウド上に登録するが，その際にブラウザ内で暗号鍵が生成され，ファイルが暗号化されてアップロードされる．その暗号鍵はクラウド側には伝わらないので，クラウドストレージの運営者もそのファイルを復号することができない．その暗号鍵はブラウザで生成される受信用 URL 内に含まれている．この URL をメールで送信する．

(b) 送信者はファイルをクラウドに登録する際に，ファイルの有効期限を指定できる．その長さは最長 7 日であり，これを越えたファイルは削除されるため，漏えいリスクが軽減されている．さらに，ファイルのダウンロード回数も指定でき，これも最大 100 回である．さらに，ダウンロード URL がメール誤送信等で漏えいした場合でも直ちに URL を無効にすることで，ファイル自体の漏えいのリスクを最小にすることができる．

(c) 受信者はメール内に含まれる URL をクリックすることで，ファイルをダウンロードすることができる．この際，URL 内に含まれる暗号鍵によりファイルはブラウザ内で自動的に復号される．

このように Firefox Send はクラウドストレージにおける E2E 暗号化をほぼ実現しており，その意味で優れたファイル送信手段であると言える．ただし，厳密には受信時に暗号鍵を含む URL が一瞬クラウドに伝わってしまうため，厳密にはそこでクラウド事業者にファイルを復号されてしまう恐れがある．そこでオプションとして，ファイルアップロード時にブラウザ上でパスワードを入力することができる．このパスワードはファイル暗号化にも併用されており，かつ URL には含まれていないので，このパスワードをメールで受信者に送信することでクラウドの運営者にファイルを復号されるリスクも排除でき，完全な E2E 暗号化を実現できる．

もちろん基本的なこととして，電子メールのセキュリティにはその送受信用のアカウントを保護することや，マルウェア対策を行うことは欠かせない．また，上記リスク②に対応するための送信ドメイン認証（DKIM や SPF（RFC 7208）など）も重要である．電子メールがその送受信時に DNS を利用することから，DNSSEC など DNS の信頼性を上げる技術の利用も必要である．逆に言えばそれらを前提とすれば現在，すでに述べた通りメールの通信路における盗聴リスクはかなり下がっているため，添付ファイルをわざわざ暗号化する意味は失われつつあると思われる．この認知が広がれば，PPAP のように単に手間を増やすだけの，役に立たないセキュリティ対策はやめて，単にファイルをそのまま電子メールに添付した方がましという空気感が醸成できるのではないかと思っているのだが，それは楽観にすぎるだろうか．

参考文献

1) （独）情報処理推進機構，ビジネスメール詐欺「BEC」に関する事例と注意喚起（2017）．
2) （株）ディ・アイ・ティ：パスワードの最大解読時間測定，セキュリティ調査レポート Vol.3（2012）．

（2020 年 5 月 16 日受付）

■上原哲太郎（正会員） t-uehara@fc.ritsumei.ac.jp

和歌山大学，京都大学，総務省を経て 2013 年より立命館大学情報理工学部教授．専門はサイバーセキュリティ，システム管理，ディジタル・フォレンジック．入力しにくいだけの Excel 帳票や無駄な押印の撲滅にも興味を持つ．