【講演レポート】JIPDECセミナー

基調講演 「PPAP廃止に関する動向と対策案の検討」

東京電機大学研究推進社会連携センター
顧問・客員教授　佐々木　良一氏

PPAPの動向と問題点

PPAPとは

PPAPとは、パスワード付きZIPファイルとパスワードを別々のメールで送付する手法で、一時、ファイルを安全に相手へ送信する方法として普及しました。
メリットとして、ファイル添付メールとパスワードのどちらかを誤送信しても情報が流出しない誤送信対策があげられます。また、盗聴防止効果やファイル圧縮・解凍ソフトの相互運用性の高さなど利便性の良さ等があげられますが、どれも効果が高いとは言い切れないのが現状です。

PPAPの問題点

問題点としては、セキュリティ向上の効果があまり期待できないにも関わらず、パスワードが記載されたメールを探す、同一人物からの複数のメールを受信した際のパスワード記載メールとメール本文の照合など、手間がかかることを強制的にやる必要がある点があげられます。さらに、Emotetなどマルウェア検出を回避し拡散されるなど、マルウェア攻撃に悪用されるケースも見受けられます。
上記のような懸念点を踏まえ、2020年11月には当時のデジタル改革担当　平井大臣が内閣府、内閣官房によるPPAPの廃止を発表、その後も他官庁や企業などが廃止を宣言するなど話題となりました。

PPAPの代替方法は何か

PPAP廃止の流れがある一方、安全なデータのやりとりに必要な最適な方法に関しては確立していないのが現状です。
そこで今回は、考えうる対応策の比較を行い、PPAPに代わる最良の方法は何か？について考えていきたいと思います。
まずは、５つの対策案と評価指標を設け検証しました（図１）。対策案のうち、３つはメールベース、2つがストレージサーバの利用を想定し、安全性や使い勝手を評価指標としています。

対策案の比較

対策案 / 評価指標		①暗号化なし	PPAP 現状版	PPAP ②SMSで鍵配送	③S/MIME署名 組み合わせ	③S/MIME暗号化 組み合わせ	④CS利用（ACなし）	⑤CS利用（ACあり）
メールベースか		Yes	Yes	Yes	Yes	Yes	No	No
安全性	暗号強度	X	△	△	ー	○	ー	ー
安全性	鍵配送の安全性	ー	X	△	ー	○	ー	ー
安全性	認証機能	X	X	X	○	ー	X	○
ウイルスチェックが可能		○	X	X	○	○	○	○
使い勝手（ユーザの手間）		○	△	△	△自分の公開鍵証明書の入手のみ	X受信者側の公開鍵入手が困難	○	△

CS：Cloud Server　クラウドサーバ　　AC：Access Controlアクセス制御

図1．PPAPに代わる対策案の比較

メール利用を前提に考えた場合、使い勝手という意味では暗号化なしで送る、パスワードをSMSで別送する方法などがあります。特にSMS等別ルートで解凍用パスワードを送信する方法は、独立性の高さから不正の発生確率は各段に下がると考えられ、ある程度の安全性は確保できるでしょう。また、暗号化なしと同様、使い勝手もそうハードルが高いわけではありません。ただし、ウイルスチェックが行われない点などは課題として残っており、最適な策とは言えません。

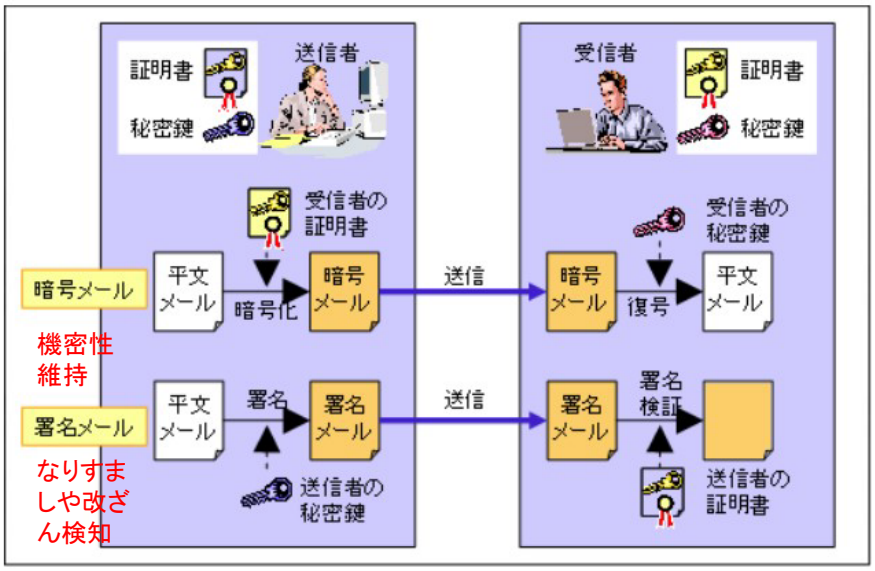
S/MIME（エスマイム）の利用

メールベースの対策案の一つとして、電子メールのセキュリティを向上する暗号化方式S/MIMEがあります。電子証明書を用いてメールの暗号化とメールへの電子署名を行う方法で、利用（図2）する前提として送信者、受信者ともに事前に認証局から証明書と後述する電子証明書（公開鍵証明書）を入手し保持していること、また双方がS/MIMEに対応した電子メールソフトを使用している必要があります。S/MIMEでは、以下のとおり、メールの暗号化（暗号メール）とデジタル署名の付与（署名メール）が実現可能です。

暗号メール：送信者は受信者側の証明書でメールを暗号化。受信者側は自分の秘密鍵でメールを復号。通信路に暗号がかかっているため、機密性が維持される。

署名メール：送信者は自分の秘密鍵でメールに署名を付与。受信者は送信者の証明書で署名の検証を行う。これによってなりすましやメール内容の改ざん検知が可能になる。

S/MIME利用のイメージ



7

図1：S/MIMEの利用イメージ（出典：IPA「情報セキュリティ - S/MIME」）

図2. S/MIMEの利用イメージ（出典：IPA　S/MIME概要）

電子証明書（公開鍵証明書）の入手、設定

S/MIMEの利用に必要な電子証明書とは、ある公開鍵、記載された者が保有することを証明する電子的文書のことを言います。

電子証明書の入手は認証局から無料で発行することも可能ですが、入手後の操作として自身の電子メールソフトへの設定等、さまざまな操作、処理が必要なことから、個人で設定する場合など慣れない人には容易ではないかもしれません。ただし、一度設定が完了してしまえば、都度のメール送信時の署名・暗号化処理は比較的容易になっています。

参考：電子証明書の申込みから取得まで（JIPDEC　デジタルトラスト評価センター）

S/MIMEのメリット

PPAPの代替策として、S/MIME利用のメリットとして以下の2点があげられます。

①S/MIME暗号は公開鍵暗号を利用しており、End-End（PCからPC）への鍵の配送が容易。たとえ運用者であっても内容を知ることをできないこと。

②S/MIME署名によって、本人性と通信文の非改ざん性が確保できることで標的型攻撃の防止が期待できること。

①S/MIME暗号と②S/MIME署名を組み合わせることで、非常に高い安全性を確保できると考えられており、PPAPに代わる対応策としてS/MIMEが非常に効果的と言えるでしょう。

S/MIMEの現状の問題点と評価

ここまでお話したとおり、S/MIME利用のメリットは大きいと考えています。一方、電子証明書を入手する際のコストが大きいことや、現状の各種メーラーとの互換性がない点、そもそもWebメールでは利用できるものが少ないなど解決すべき点も多くあります。現状ではメールベースの対策案として、S/MIMEが最適と考えられますが、今後使い勝手など細かい見直しは必要となるでしょう。

メールに代わるコミュニケーション手段とセキュリティ対策

クラウドストレージサービスでの代替

昨今はコミュニケーション手段として、メールに加え、クラウドストレージやビジネスチャット、WEB会議システムなどが充実しメールを利用しないビジネスシーンでのコミュニケーション手段も普及しています。
そこで、続いてはPPAPの代替策としてクラウドストレージの利用を想定したメリットや課題を考えてみましょう。

クラウドストレージ：アクセス制御機能のないサービスを利用する場合

送信者はファイルをクラウドストレージ上にアップし、アップ先のURLを受信者に知らせます。受信者はURLをクリックするだけで情報をダウンロード（閲覧）することができるので、とても使い勝手はよい反面、送信中のメールにタッピングされれば簡単に不正アクセスされる可能性もあり、機密性の高い文書等のやりとりには適しません。

クラウドストレージ：アクセス制御機能があるサービスを利用する場合

受信者側がファイルがアップされたクラウドストレージサービスへのアクセス権限（パスワード）を持っていることが前提になります。送信者が該当のクラウドにファイルをアップロードした旨を伝達すると、受信者は事前に登録したパスワードでログインし、ファイルをダウンロード（閲覧）することができます。この方法であれば、不正者が送信中のメールにタッピングを行っても閲覧用のパスワードを知られることもなく、安全性、使い勝手の両面で望ましい方法の一つと言えます。
ただしリスクもあり、受信者側がパスワードなどの認証手段を確立していない段階でメールをタッピングされた場合、不正者によって先にパスワードを発行され、不正アクセスされることも考えられます。送信者は、受信者が該当のクラウドサービス上でパスワード設定が完了しているか確認する、など運用面でのフォローも必要となってくるでしょう。

S/MIMEに期待するものと要改善点

PPAPに代わる手段として、メールベース、クラウドストレージサービスを使った対応策を紹介してきましたが、利用頻度やユーザーの数を鑑みた結果、現状のビジネスの中心的なコミュニケーション手段と言えるメールベースでの対応策についてより考えていく必要があると私は考えています。

そのためには、S/MIMEをより安全性が高く利便性も高いものにしていかなければなりません。

上記でも述べた電子証明書の入手方法の難しさや、転送時や有効期限切れの際の使い勝手の悪さなど問題点はいくつかあります。しかし、利用者増による低コスト化や申請時の猥雑さの解決、証明書の半自動入手機能の実装を進めていくことなどが実現すれば、より使い勝手のよい対策として機能していくでしょう。より安全で使いやすいS/MIMEの実装と普及を目指して、今後も支援を行ってまいりたいと思います。

東京電機大学　研究推進社会連携センター
顧問・客員教授　佐々木良一氏

1971年日立製作所に入社。システム開発研究所にてシステム高信頼化技術やセキュリティ技術などの研究に従事。1981年工学博士（論文博士）。2001年より東京電機大学教授。2020年より現職。日本セキュリティ・マネジメント学会会長、内閣官房サイバーセキュリティ補佐官等を歴任。

本内容は、2022年2月18日に開催されたJIPDECセミナー「S/MIME最前線「なりすましメール対策の現状と課題－S/MIMEを活用したなりすまし対策事例紹介」」講演内容を取りまとめたものです。