「PPAP」から脱却！
安全なファイル送受信を実現するには？

見積書や契約書、個人情報が含まれる名簿――日本のビジネスシーンでは、こうした重要ファイルのやり取りにおいて、パスワード付きZIPファイルをメールに添付し、後からメールでパスワードを送る、いわゆる「**PPAP**」が慣習となっています。汎用性の高さから官民問わず浸透していたこの慣習が昨今にわかに注目を集め、その問題点が広く認識されるようになりました。

PPAPは何が問題なのか？　その代わりに何を使えばいいのか？　ここではとある企業の座談会形式でお届けします。

P	パスワード付きのZIPファイルを送付
P	パスワードの送付
A	暗号化
P	プロトコル

座談会参加メンバー

A：営業
IT企業の営業として、ITツールは何でも使いこなしているという自負を持つ。口癖は「ビジネスマナー…」

B：情シス
社内ITの導入推進だけでなく、セキュリティ統制も兼ねる。口癖は「保守がまだ残ってるので…」

C：SE
Webシステムの開発系SE。セキュリティには強い関心を持つ。口癖は「そもそも…」

D：企画
経営企画部門で事業計画策定などにも関わり、知識と視野を広げてスキルアップに邁進中。口癖は「変わらなくちゃ!」

「PPAP」の問題点とは？

―みなさんお集りいただきありがとうございます。本日は昨今話題になっている「PPAP」について語っていただきます。
それではさっそく、AさんはPPAPについてどのようにとらえておられますか？

［A：営業］知ってますよ。う～ッ、ってやつですよね！？

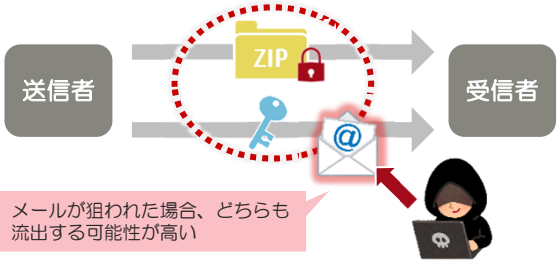
（一同沈黙…）

［A：営業］やだな、冗談ですよ。知ってますよ。添付ファイルをパスワード付きZIP化してメールで送ることですよね。
ツールが全社導入されたときは「なんで必要なの？」と思いましたけど、今は社外に添付ファイル送るときは常に使ってますよ。それって、ビジネスマナーですね、もはや（ドヤ）。時々パスワードが先に送られてくるのは愛嬌ってやつです。
…あれっ？　使ってはいけなかったですか？

―Aさん、いきなりのボケありがとうございます。導入部門のBさんはいかがですか？

［B：情シス］うーん…導入を推進した部門としては突っ込みづらいな～（苦笑）。ボケは別ですけど。
まだ保守が残っているので、切れるまではきっちり使ってはいただきたいんですが…。ツール導入当初とは状況が変わって、今はパスワード付きZIPファイルを添付してメール、別メールでパスワードを送ることについて、気になってはいます。すでに運用が形骸化して、セキュリティの強度的にもどうなの？　ってとことも言われ始めていて…。
ビジネスマナーっていうか、世間の認識とは乖離したセキュリティ対策になってしまった面もあるかと思います（汗）。

［C：SE］そもそも「暗号化ZIPファイルとパスワードを同じ経路で送付して意味あるのか？」って言いたいね、僕は。そもそものセキュリティ対策として、さ。



［D：企画］これまでのやり方が、今の時代にはそぐわなくなってきているってことよね。見直すべき時期ってことじゃないの？　変わらなくちゃ、てことなのかな？

［A：営業］え～っ、導入の時の説明会で「添付ファイル持ち出しの際に意図せず流出しても、パスワードが一緒じゃなければ復号されない」って言ってた気がするんですけど。

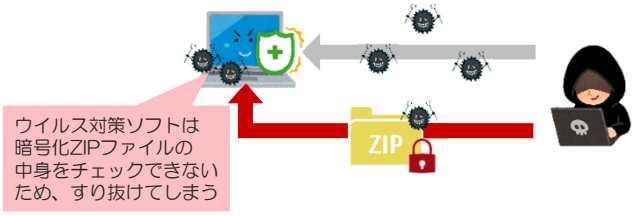
Copyright 2021 Fujitsu Japan Limited

―ZIPパスワードの解析ツールなんてものが、忘却時のお助けツールとしてネットで出回っている、なんて話も聞きますよね。そうすると…解析されてしまったりするんでしょうか？

［B：情シス］（ドキッ）いや…一定の防御効果はあるというか…。

［C：SE］そもそも、流出するのは送信経路か受信端末ってことになるんだけど、受信メールを一度にガサーっと持って行かれて、パスワードのメールだけたまたま無事でしたとかめったにないでしょ、てか、あるの？

そもそも、現在猛威をふるっているウイルスのEmotetなんかは、ウイルス対策ソフトをすり抜けるためにPPAPで送られてくるって言うじゃないですか？　いつも「不審メールに注意」とか呼び掛けていますもんねぇ（ニヤニヤ）。



［D：企画］「注意してください」って個人に依存した対策って、無理っぽい。変わらなくちゃいけないタイミングじゃない！？

―Bさん、かなりやり込められていますね（笑）。

ところで、誤送信についてはどなたも触れておりませんが、この点についてみなさんのお考えは？？？

（一同沈黙…）

―なるほど、誤送信については言うまでもないということで…ビジネスマンとしてありえません、と（汗）。

これまでの議論をまとめると、PPAPはセキュリティ対策といいながら、以下の3つの問題点があるということがわかりました。

1. 暗号化ZIPファイルとパスワードが同一経路で送付されるためまとめて流出する可能性が高い。
2. 暗号化ZIPファイルだけが流出しても、パスワード解読ツールで比較的簡単に復号化される可能性がある。
3. ウイルスの侵入経路としてPPAPが悪用される場合がある。

PPAPの代替ツール

―それでは、ここからはPPAPに替わるセキュリティ対策ツールの本命について語っていただきます。Aさん、営業として外部の方とやり取りされる場面が多いと思われますが、何か新しい動きがありましたらお話しいただきたいのですが。

［A：営業］そうですね。メール添付で送れない大容量のファイルの受け渡しを行う「○○便」みたいなツールを使われるお客様が増えている気がします。ファイルはWebからダウンロード、パスワードはメールで来るので、同一経路ではないという点ではクリアできている気がします。操作はひと手間増えますが、割と新しいビジネスマナー的な感じで、いいかなって…。

［C：SE］そもそも、セキュリティ対策って色々あるんですけど、まぁセキュリティ機能が充実しているファイル伝送の専用ツールが狙い目かと思います。

そもそも暗号化方式でAES-256の実装やサーバ上でのウイルスチェックなんてものは必須の機能ですね。あと、送信後の取消（取戻）やファイル送信の承認ワークフローなどがあると、誤送信対策や自宅PCへの不正な持ち出し防止という観点でも安心です。それから利用者認証だけだけでなく送信端末の認証もできると、なりすまし防止もできるかと。

―なるほど、PPAPの問題点をクリアできそうですね。ただ、使い勝手という面ではいかがでしょうか。操作系がWebとメールに分かれますが。

［D：企画］メール送信時に自動的に添付ファイルを分離して、Webにアップロードしてくれるなんて欲張り過ぎ？　なんかありそうな気がするけど…。

［C：SE］送る方は便利だね。これまでの操作とあまり変わらないし。そもそも、そんなのあったらトライアルやってみたいね。

［B：情シス］ちょっとちょっと、勝手に話しを進めないでくださいよ（汗）。こちらでは自社ファイルサーバからオンラインストレージサービスへの移行に合わせて、このサービスを使って社外とのファイルのやり取りをうまく実現できないかってのを検討中なんですよ…。まだサーバの保守が残っているけど…。

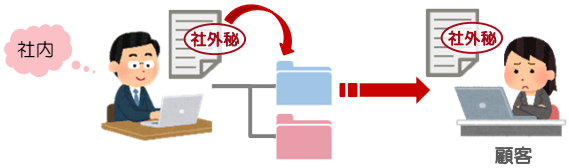
［A：営業］あっ、それプライベートで使ってます！　仲間内で動画ファイルとか共有するのに便利なんですよ。スマホでチャチャっとやれて。もちろん、業務では使ってませんよ、ビジネスマナー的にどうかなって感じで…。

［C：SE］私もプライベートでは使っているけど、業務用で使うのは少し抵抗あるな～。

そもそも、共有の設定って最初はいいんですけど、使っているうちに異動・離職とかでだんだん管理がずさんになって行くんですよね。あと、そもそもファイルサーバ移行って、容量問題やアクセス権や不要ファイル削除のための棚卸しだったりしませんか？　つけてはいけないアクセス権がついていた例もあったんじゃないですか？

なので、そもそもファイルサーバ的なツールを使って、外部とファイル共有するのってコワい気がするんですよね。

［D：企画］社内共有フォルダだと思ってファイルを置いたら、実は顧客との共有用だった、とかありそうじゃないかしら。そういえば、実際にある地方自治体で、共有グループへの招待メールを第三者に誤送信してしまった事例も発生していたような…。



［C：SE］でしょでしょ。そもそもヤバいと思っていたんですよ。

PPAPで「経路が同一」っていう弱点があるように、社内外のファイルのやり取りにおいては「ツール（あるいは利用空間）を同一に」すべきではないんですよ。

Copyright 2021 Fujitsu Japan Limited

［A：営業］フェイルセーフって考え方ですよね。これもビジネスマナーっていうか…。

［D：企画］昔からある設計思想ね。（ビジネスマナーとちゃうわ！）時代が変わっても変わらないもの、あるわね。

［B：情シス］ムムム、また追い込まれてしまった…。では、こうしましょう。
ファイルサーバ移行はすでに進んでいるプロジェクトなので、その延長で外部とのやり取りを試行してみます。ファイル伝送ツールに関しては、いくつか候補をあげて同じ評価軸、特にセキュリティ面を重視して検証してみましょう。

―使い勝手は企業や組織の業務特性やITリテラシーにも依存しますし、事前検証は必要ですね。セキュリティレベルが高くても使いづらく、別の意味で形骸化してしまっては元も子もありません。

［A：営業］もしいいのが見つかったら、お試しで使って、そのまま採用しちゃってもいいんじゃありません？

［C：SE］そもそもクラウド前提だし、お試し、行けちゃうよね！

［D：企画］そういうスピード感、大事よね！　そういうところは、変わらなくちゃね！

［B：情シス］ちょ、ちょ、待ってください、どんなサービスがあるのかこれから調べないと…。「まだ雲の中」なんですよ～、クラウドだけに（笑）。

―…えー、なんというか、以上で終わりたいと思います。ありがとうございました…。

（A、C、D、会議室退席）

［B：情シス］え～、みなさーん…

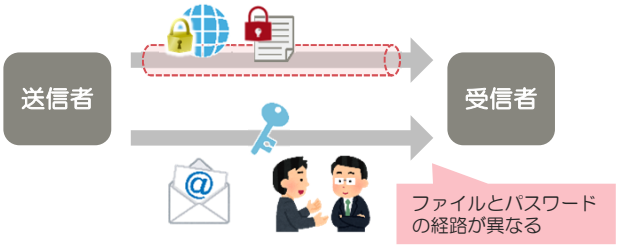
Confidential PostingでPPAP問題を解決！

さて、途方に暮れているBさんのために、ここからは富士通Japanの暗号化ファイル伝送ツール「Confidential Posting」を利用したPPAP問題の解決方法をご紹介します。

問題1

暗号化ZIPファイルとパスワードが同一経路で送付されるためまとめて流出する可能性が高い。

Confidential Postingでは、暗号化されたファイルをWebからダウンロードします。通信も暗号化（TLS1.2）されており、さらにネットワークアドレスや端末のMACアドレスによって、送受信環境を制限することも可能です。
復元パスワードは、メールで自動通知する方法と、通知しない方法を送信者が指定することができます。後者の場合、電話等の別の手段でパスワードを伝える、定期的にやり取りをする取引先であればあらかじめパスワードのルールを決めておく（毎回個別にパスワードを通知しない）、といった対応を取ることになります。



このように、ファイルとパスワードの経路を分けることで、情報流出のリスクを低減します。

問題2

暗号化ZIPファイルだけが流出しても、パスワード解読ツールで比較的簡単に復号化される可能性がある。

Confidential Postingは、サーバ内でファイルやパスワードをAES-256で暗号化して保管しています。AESは、総務省および経済産業省が策定した「電子政府における調達のために参照すべき暗号のリスト」にも掲載されている、信頼性の高い暗号化方式です。万が一サイバー攻撃を受け、サーバから暗号化ファイルが流出したとしても、解読は困難と言えます。
受信者が端末にダウンロードしたファイルは、実行形式の暗号化ファイル（拡張子変更可）となっています。復元回数の上限が定められているため、パスワードを複数回試行して無理やり復元することは不可能です。また、ダウンロード時だけでなく復元時の操作ログもサーバに残ります。

問題3

ウイルスの侵入経路としてPPAPが悪用される場合がある。

PPAPでは、ウイルス対策ソフトが暗号化ZIPファイルの中身をチェックできないことから、ウイルスが混入されていても検出されずにすり抜けてしまうことが問題でした。
Confidential Postingは、サーバで必ずウイルスチェックを行ってからファイルを暗号化しますので、受信者は安全にファイルを受け取ることができます。

その他の便利な使い方

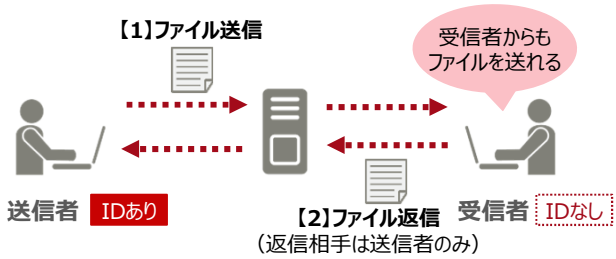
（1）ファイルの送信対策は万全！　では受け取りは？

相手にファイルを送信するだけでなく、逆に相手からファイルを受け取りたいが、メールではちょっと…という場面はありませんか？　そんなときはConfidential Postingの「**返信機能**」が便利です。

例えばこんなシーン
- 顧客から、動画ファイルや膨大なログデータ等、業務上必要な大容量データを受け取る
- 取引先から機密情報が含まれるファイルを受け取る
- 顧客に所定の書式を送り、個人情報を記入して返信してもらう

Copyright 2021 Fujitsu Japan Limited

返信機能は、IDを持っていない受信者でも、送信者に対してファイルを返信することができる機能です。返信するファイルは、元の送信ファイルとは関係なく何でもOK。返信においてもファイル送信時と同様のセキュリティ対策が実施されるため、相手が特別なツールを導入していなくても、安全にファイルを受け取ることができます。



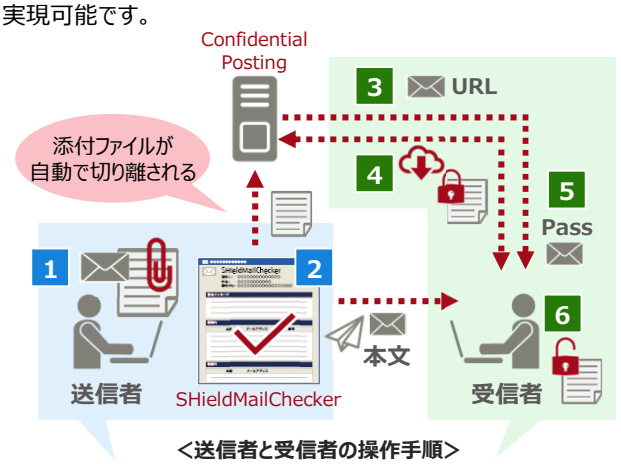
（2）メール誤送信防止ツール × Confidential Posting

座談会では、Dさんからこんな話が出ていました。

> **メール送信時に自動的に添付ファイルを分離して、Webにアップロード**してくれるなんて欲張り過ぎ？
> なんかありそうな気がするけど…。

この方法なら、「メールにファイルを添付する」という標準的な運用と大きく変わらないためユーザビリティが高く、セキュリティ面の強化だけでなく業務効率化のメリットもあると言えそうですね。

Confidential Postingでは、メール誤送信防止ツールの「**SHieldMailChecker 誤送信防止**」と連携することで、これも実現可能です。



<送信者と受信者の操作手順>

1. メールにファイルを添付、送信ボタン
2. SHieldMail Checker起動
3. 宛先と添付ファイルの内容をチェック、送信
4. ダウンロードをメールでお知らせ

（*）自動通知しない方法も指定可能。

3. ダウンロードURL通知メール受信
4. 暗号化ファイルをWebからダウンロード
5. パスワード通知メールを受信（*）
6. ファイル復元

✓送信者側のメールサーバはExchange ServerまたはExchange Onlineで動作します。
✓クライアントにはOutlookが必要です。Webメールでは動作しません。

SHieldMailChecker 誤送信防止は、メール送信前に宛先や添付ファイルのチェックを促し、うっかりミスによる誤送信を防ぎます。組織独自のポリシーに合わせた警告表示や、過剰な警告を抑止するための自動学習ホワイトリストといった機能も搭載しています。

送信前のチェックで確実にメール誤送信を防止し、添付ファイルは暗号化してWeb経由で安全に相手へ。SHieldMailCheckerとConfidential Postingを組み合わせると、一歩進んだセキュアなファイル送受信が可能になります。

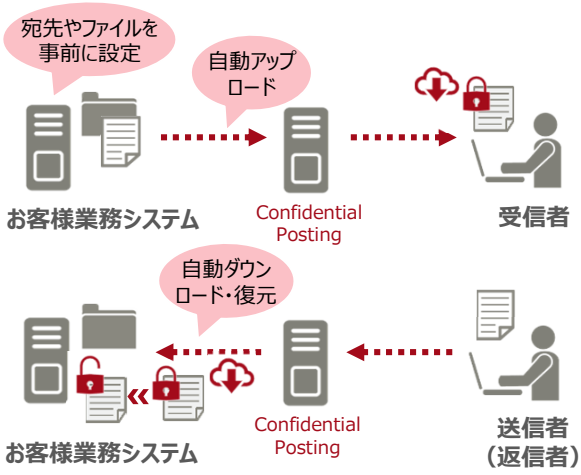
※「SHieldMailChecker 誤送信防止」は、株式会社富士通ソーシアルサイエンスラボラトリの製品です。

（3）システム連携でファイルを自動送受信

Confidential Postingには、お客様の業務システムと連携し、**ファイルを自動で送受信**する機能があります。取引先やグループ企業との定期的なファイル送受信にご利用いただくことで、手作業による送信業務の負荷を軽減します。また、帳票をFAXや郵送から電子化に切り替える場合にも活用いただけます。

例えばこんなシーン

- 集計データのファイルを日次でグループ企業に送る
- 請求書を郵送していたが、PDFファイルの送信に切り替える
- 取引先に毎月データの記入を依頼し、回答を受信する



PPAP問題が広まって以降、早速PPAPを廃止する企業が登場する等、ファイルのやり取りを見直す企業は増えています。

ファイル送信は必ず相手あってのもの。自社のセキュリティ対策を高めることが、送信相手からの信頼を得ることにもつながります。問題のある手法を使い続け、ビジネスの相手からの信頼を損なわないよう、ぜひこの機会に最適な解決方法を検討してみましょう。

富士通Japan株式会社
https://www.fujitsu.com/jp/fjj/

2021.03

Copyright 2021 Fujitsu Japan Limited