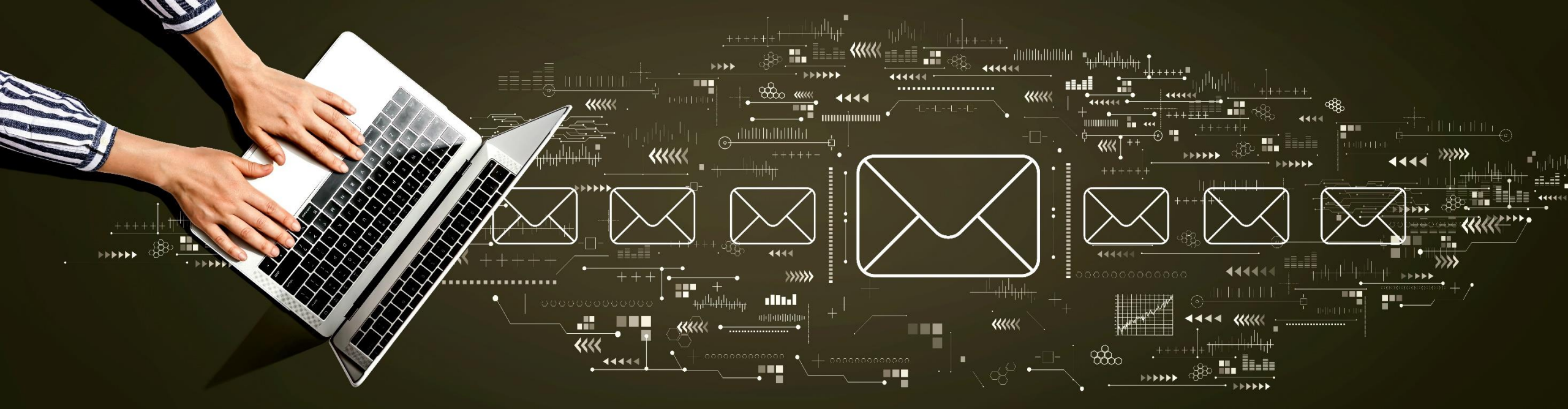

３分でわかる
PPAP対策の最適解

2022年

01 PPAPの問題点とは

02 代替策の種類と特徴

03 PPAP代替策を選ぶポイント

04 PPAP代替策の比較

01 PPAPの問題点とは

2020年11月、デジタル改革担当大臣により、メール添付ファイルZIP暗号化（PPAP）の中央省庁での利用を廃止する方針が発表されました。日本国内では、PPAPはその安全性に問題はありながらも、メール添付で簡単にファイル交換ができる誤送信対策として普及してきました。

PPAPとは

メールで添付ファイルを送信する際に、
添付ファイルを暗号化し、パスワードを送信する一連の流れ

P：　Passwordが必要なZIPファイルを送付
P：　Passwordを送付
A：　暗号化
P：　プロトコル

PPAP 4 つの問題点

1 攻撃者による悪用

暗号化ZIPファイルは、ウイルス検疫システムをすり抜ける可能性があるため悪用されやすく、ZIPファイルを受取拒否する企業も出てきました

2 パスワードの盗聴

パスワードは平文で送信されるため、パスワードの盗聴リスクがあります

3 送受信の手間

送信者のパスワード発行・別送付の手間や、受信者解凍作業の手間が都度かかります

4 モバイル非対応

モバイル端末で受信する場合、ZIPファイルが解凍できないことも

PPAPの本来の目的は、
誤送信防止
利用廃止と言われても・・・。

02 代替策の種類と特徴

代替策に正解はありません。
ご利用にあった選択が必要です。

一般的な代替手段と概要

	添付ファイル ダウンロードリンク化	ファイル転送サービス	オンラインストレージ
概要	メールの添付ファイルをクラウドストレージに自動アップロードし、受信者はメール本文のリンクからダウンロード	送信者はWebサイトにファイルをアップロードし、受信者は発行されたURLからダウンロード	クラウドに共有フォルダーを設置し、データやファイルをやり取りする方法
送信の手段	メールの添付	Webアップロード	Webアップロード
ファイル送付の安全性 （経路の暗号化）	HTTPS(暗号化)	HTTPS(暗号化)	HTTPS(暗号化)
ファイルの保護 （暗号化や権限管理）	なし	なし	ファイル権限設定が可能 暗号化可能
ダウンロード認証	ワンタイムパスワード ソーシャルログイン	ワンタイムパスワード	利用アカウントによる認証 ワンタイムパスワード
向いている 利用シーン	メールを利用したビジネス上のやり取りでのファイル送付	大容量ファイルの共有	プロジェクトごとなど特定者とのファイル共有
向いている ファイル	不特定な相手先への情報含む、 見積書/提案書など	動画制作物や写真データなど容量の大きいファイルなど	決まった相手先との共同編集や 頻繁に更新するプロジェクト計画など
考慮点	メールのアーカイブなど追加対策が望ましい	版管理や履歴管理がログのみ	受信者登録の手間 ファイル権限設定の手間と管理

03 PPAP代替策を選ぶポイント

ポイント1 誤送信・誤共有対策

PPAPはパスワードを別送付する手続き中に**宛先違い**や**添付間違い**を発見し、誤送信を防ぐことを目的としています。
代替手段についても、宛先や添付ファイルをチェックする仕組みがあることが選択のポイントとなります。

ポイント2 誤送信発覚時の対応

誤送信が発生した場合、影響範囲の特定、被害拡大の防止、再発防止の策定と実施が必要になります。
そのため、影響範囲を確認するためのログの有無や、
共有後の取り消し機能の有無も選択のポイントです。

ポイント3 経路の安全性

メールの送信手順であるSMTPでは、経路が暗号化されないため、盗聴リスクが問題となりました。代替手段の検討では、 Web通信の暗号化（HTTPS）など、経路の暗号化の確認が必要です。

ポイント4 パスワードの授受

パスワードは、暗号ファイルの復号や、ダウンロード認証などに必要となります。盗聴を防ぐための手段はさまざまです。パスワード通知経路の分離やパスワード授受が発生しないソーシャル認証、受信側の事前利用登録など手段はさまざまです。安全性や利用の手間を考慮して、選択する必要があります。

ポイント5 ファイルの種類と共有手段

企業で取り扱うファイルはさまざまです。ファイルの種類や共有目的によって共有手段の使い分けが必要です。
プロジェクトなど特定相手と共同編集するような書類では、オンラインストレージのような手段が適しています。
見積書や提案書など、相手先情報を含む書類をやりとりする場合は、メールのような双方向性があり、時系列がわかりやすい手段が適しています。また、動画制作物など大容量のファイルの場合はファイル交換サービスなど、利用にあった選択が必要です。

ポイント6 利用者のつかいやすさ

複雑な操作や面倒な利用登録など、利用者負担の大きい対策では長続きしない可能性があります。利用者視点のわかりやすさは重要なポイントです。

ポイント7 統制と利便性

利用者の裁量にまかせた運用は望ましくありません。
全社員に適用させるか、利用者に利用の有無をまかせるかなど、導入方針を決定し、対応可能な手段の選択が必要です。
端末インストール型やゲートウェイ型、Webアップロード型などで導入形態により統制の取り方や監視の仕方が異なってきます。

ポイント8 導入・運用の容易性

管理者の導入のしやすさや、運用のしやすさも利用継続の点で重要です。利用者への導入説明や教育などの容易性もポイントです。

04 PPAP代替策の比較

一般的な比較です。ベンダー毎にさまざま工夫や安全のための対策がとられています。
実際には、各選択ポイントに基づき、ベンダー評価利用を実施し比較されることをお勧めします。

選択ポイント		添付ファイルDLリンク化			ファイル転送サービス	オンラインストレージ
		ゲートウェイ型※1	クライアント型	Outlookアドイン型※1		
ポイント1	誤送信・誤共有対策	○ 送信チェック	○ 送信チェック	○ 送信チェック	△	△
ポイント2	誤送信発覚時の対応	○ ログ・ファイル公開取消	△	○ ファイル公開取消	○ ファイル公開取消	○ ファイル公開取消 ファイル権限削除
ポイント3	経路の安全性	HTTPS	HTTPS	HTTPS	HTTPS	HTTPS
ポイント4	パスワードの授受	△ワンタイム認証 ○ソーシャル認証	△	△ワンタイム認証 ○ソーシャル認証	△	○ 事前登録
ポイント5	ファイルの種類と共有手段	メール添付 自動分離でのWebアップロード			Webアップロード	Webアップロード
ポイント6	利用者のつかいやすさ	○メールの利便性を活かせる			○大容量ファイル △送信の手間	△事前登録の手間 ○版管理や共同編集
ポイント7	統制と利便性	○ゲートウェイでの出口対策可能	△	△	△ （監視必要）	△ （監視必要）
ポイント8	導入・運用の容易性	△メール経路変更	×クライアント配布	○アドイン配布設定	△利用登録	△利用登録

※1：キヤノンマーケティングジャパン株式会社のGUARDIANWALL　Mailセキュリティ・クラウドでの比較
ゲートウェイ型　：　MailConvert on Cloud ベーシック／プレミアム
Outlookアドイン型：　Outbound Security for Microsoft 365

GUARDIANWALL

製品情報　https://cweb.canon.jp/it-sec/solution/guardianwall/

お問い合せ　https://cweb.canon.jp/it-sec/solution/guardianwall/contact/

キヤノンマーケティングジャパン株式会社