



オフィス®  
宅ふあいる便

ファイル誤送信のリスク対策に重要なStep  
～オフィス宅ふあいる便の有効活用に向けて～

**Daigas**  
Group

 オージス総研



# 目次

• 昨今、問題になっている「PPAP」の危険性とは？	3
• 安全な手段を準備するだけではリスクは減らない	4
• ファイル誤送信のリスク対策に向けたStep	5
• ファイル誤送信対策を進める上での問題点	6
• オフィス宅ふぁいる便でファイル誤送信対策を	7
• オフィス宅ふぁいる便の「多重の誤送信対策」	8
• オフィス宅ふぁいる便で手間をかけずに安心して送信	9
• シャドーIT対策（クライアントセキュリティ管理のご提案）	10

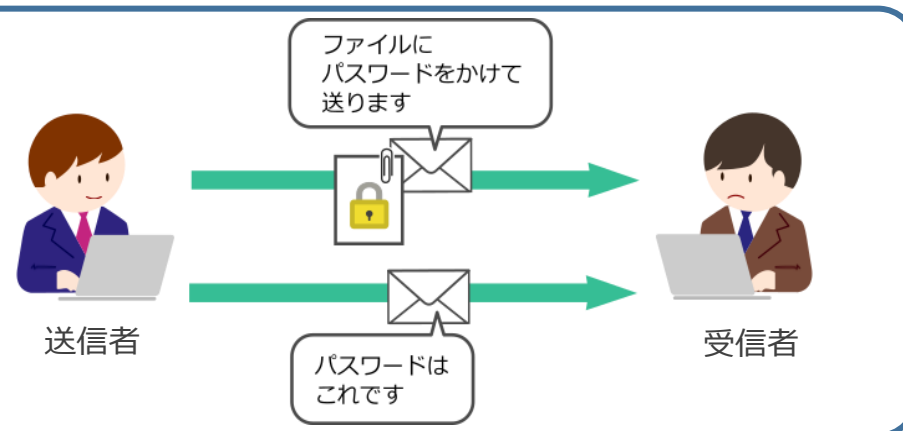


# 昨今、問題になっている「PPAP」の危険性とは？

## ？ そもそも「PPAP」って何？

PPAPとは、パスワード付きzip形式の添付ファイルと、暗号化解除用のパスワードをメールで送信すること  
下記の頭文字をとってPPAPと略称されています

- P** assword付きzip暗号化ファイルを送ります
- P** asswordを送ります
- A** (あ)ん号化 (暗号化) します
- P** rotocol (プロトコル=手順)



## PPAPで発生しうる問題

- ① 送信先アドレスの指定ミスなどで発生する誤送信
- ② 悪意のある第三者による盗聴(添付ファイル・パスワード)
- ③ 添付ファイルの暗号化によりウイルス感染が検知できず受信者に送信されてしまう

上記のような問題があることから、近年は「PPAP」を禁止する企業が増加している



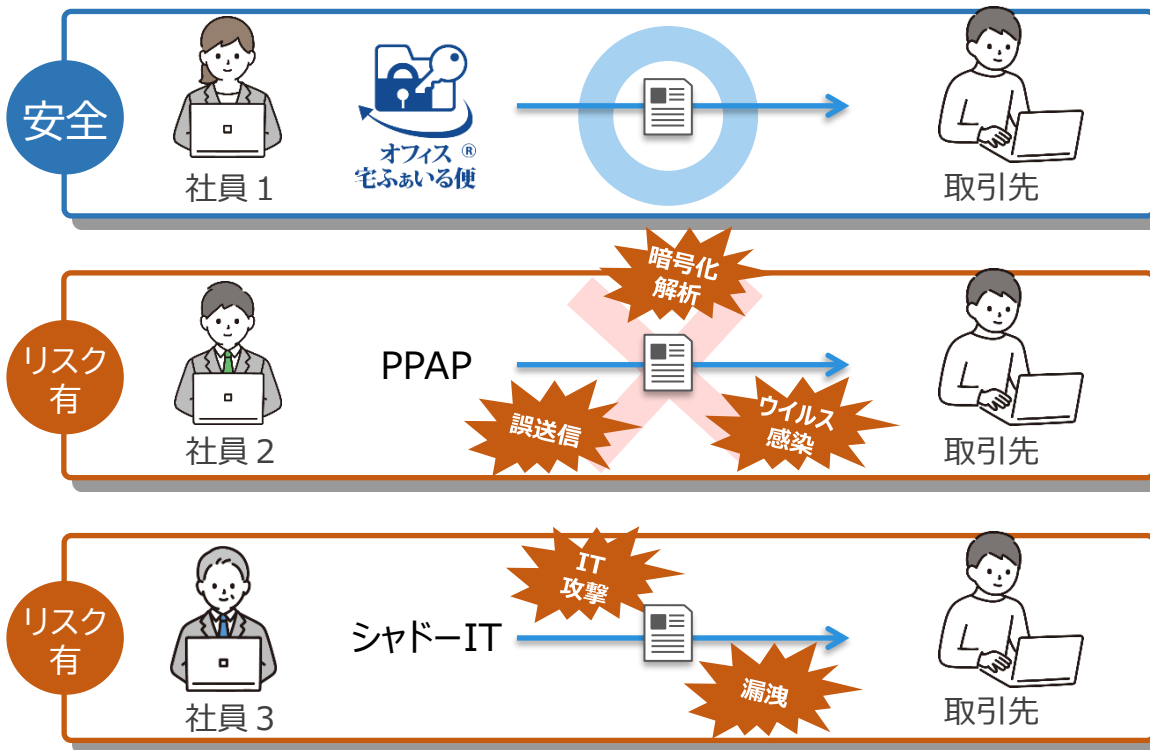
# 安全な手段を準備するだけではリスクは減らない

社外へのファイル送信に安全な手段を準備しても、それまでの送信方法が利用可能なままでは社員は自分が便利と思う方法を使い続けるため、一向にリスクは減らない  
リスクコントロールが難しい送信方法は可能な限り利用制限することが望ましい

リスクの恐れがあるものは、制限していかないとキリがない



セキュリティ統括



例えば..

メールへのファイル添付禁止、もしくはフィルタリング(特定のアドレスのみ許可)など

例えば..

- Webフィルタリング
- USB制限(利用禁止)
- ローカル管理者権限の剥奪



# ファイル誤送信のリスク対策に向けたStep

Step

①

Step

②

Step

③

ファイル持出・送信の規定

- 原則、オフィス宅ふぁいる便のみ利用
- 重大な業務影響がない限り、ファイル送信は原則としてオフィス宅ふぁいる便のみを利用する
- 利用は極力排除
- ルール違反が発生した場合に、その違反の検知と影響範囲を追跡できる準備

運用トライアル

- Webラーニングなどで社員啓蒙
- 期限内に業務上の影響を申告して

本格運用の開始

- ファイル送信は原則としてオフィス宅ふぁいる便のみを利用する
- シャドーITを制限しイレギュラーを排除することで違反行動の監視範囲を絞り込むことが重要

この資料にご興味をお持ちいただけましたら、是非ダウンロードをお申し込みください。

一度お申し込みいただくと、オフィス宅ふぁいる便に関連したすべての掲載資料をダウンロードいただけます。

お申し込み

この期間を円滑に進めるため、オフィス宅ふぁいる便は最大2カ月の無償トライアル期間を設けています