「クラウドストレージ」も「Webダウンロード」ももう不要
目からウロコのPPAP解決策
【TLS確認機能】のご紹介

GOLD SOPNSOR

株式会社クオリティア

脱PPAP宣言後の市場の動きは？

お手数お掛け致しますが何卒宜しくお願い致します。
--
【重要なお知らせ】

当社では2022年2月15日からマルウェア感染リスク低減のため

パスワード付き圧縮ファイル（zip等）が自動削除され受信できません。

大変申し訳ございませんが、ファイル単体へのPW設定をお願いいたします。

パスワードが掛かっていることが問題なのであって、パスワードZipと読み取りパスワードに違いはないのでは？

パスワード付きZipはダメだけど、パスワード付き7zipならいいの？

弊社からの注文書等配信方式変更のご連絡（再実施）

1．概要
弊社から配信される注文書、計上通知書等の暗号化方式が変更となります。
現在暗号化除外申請をいただいている場合においても全て下記形式となります。
・暗号化方式：7zip形式（識別子.zip）
・暗号化強度：AES256

2．変更日時
2022年6月22日(水)夕刻送信分より

3．お願い
（1）7zip形式（識別子.zip）の受信について
暗号化強度が強いために、解凍には復号化ツール（7zip）が必要です。
事前に用意くださいますようお願いいたします。
※7zip復号ツールURL　https://sevenzip.osdn.jp/download.html
詳細は添付資料（7zipインストール.pdf）をご参照ください。

（2）7zip形式（識別子.zip）の受信が不可能なことが判明した場合
下記「4．暗号化配信に関するお問合せ先」に至急連絡いただくようお願いいたします。

（3）6月22日以降パスワードメールのみが届いた場合
切り替え後、弊社からの注文書メール等がが届かずにパスワードメールのみが
届いた場合は弊社購買担当迄ご連絡ください。

4．暗号化配信に関するお問合せ先
[redacted]<[redacted]@[redacted].co.jp>
※本メールへ返信いただく形でご連絡ください。

以上

いや、だったらパスワードZipで送る場合も
別経路で伝えればいいのでは？

5. **今後の代替策について**

代替手段としては、次の優先順にて複数がございます。弊社希望は方法1となりますが、お客様でのご対応が困難なご事情等もあるかと存じますので、協議させて頂けますと幸いです。

【方法 1】クラウドサービスを使用したファイルの交換。
（Office365 の SharepointOnline の社外共有機能や、パブリッククラウドサービスの「Box」等）

【方法2】お客様準備のクラウドストレージ（ファイル授受）サービスの活用
（この場合は、お客様ご準備のサービスを弊社が利用可能か別途確認が必要となります）

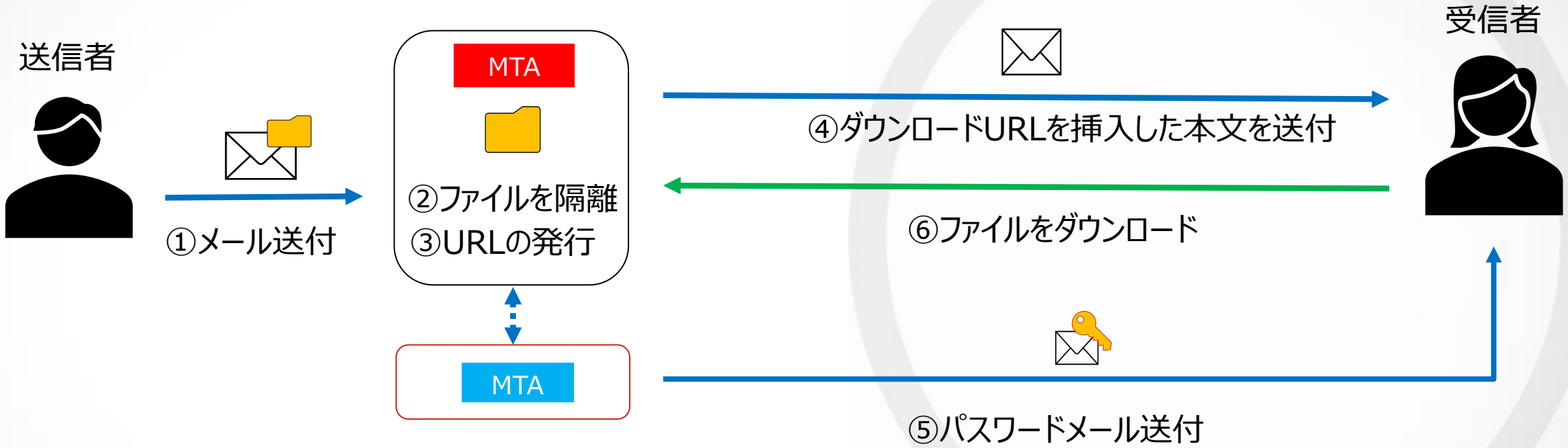
【方法3】以下の形式での暗号化ファイルでのメールやり取りに変更する。
この場合はパスワードを電話等メール以外の別経路にて連絡することになります（※）。
・ファイル形式「7zip」にてパスワード付き暗号化したファイル
・Office ファイル（Word や Excel）や PDF のパスワード付きファイル

いずれの三社も
- **一部上場**
- **社員数10,000人以上**
- **IT系･･･(ノД`)･゜･。**

脱PPAP宣言後の各社の対応は？

比較サービス①　A社

- ファイルの授受にはWebダウンロード方式



【特徴】 URL付きのメールが発送されるMTAとパスワードを記載したメールが発送されるMTAが異なる

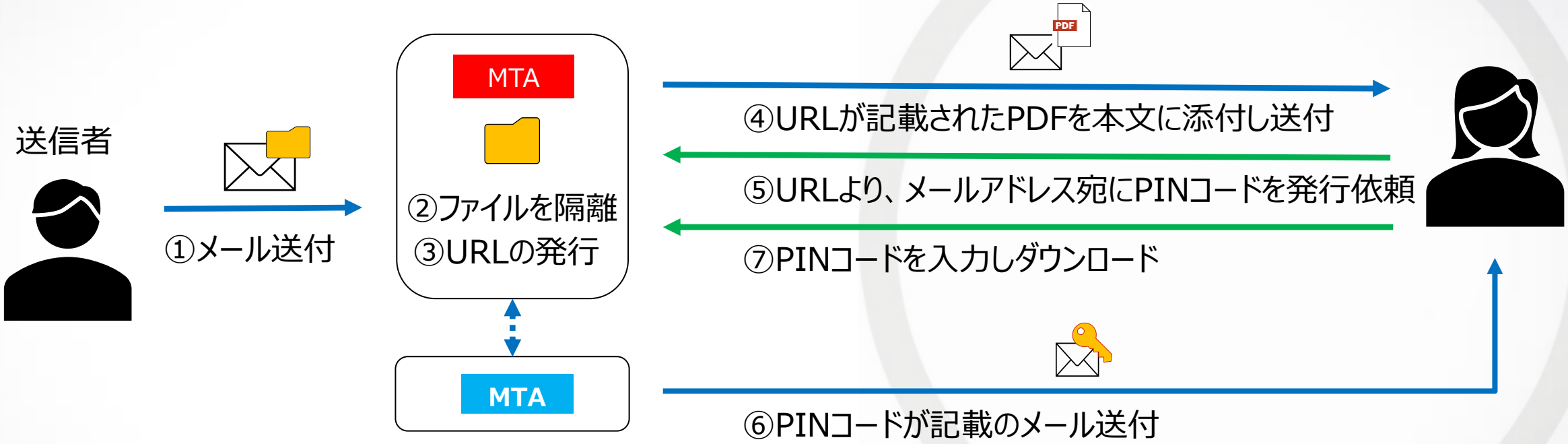
比較サービス①　A社

【懸念点】

・元メールとパスワード通知メールの配送サーバーを分けたとしても
受信メールサーバー側で盗聴されている場合は、
結果、盗聴されてしまうのではないか？

比較サービス②　B社

- ファイルの授受にはWebダウンロード方式
- PINコード(ワンタイムパスワード)を使ってダウンロードさせる



【特徴】

・URLが記載されているPDFファイルを元メールに添付し送信

・受信側によるパスワード発行の仕組みを搭載※自動別送ではない（待ち伏せ盗聴に対するシビレ切らせ効果）

・PDF付き元メールとPINコード通知メールの配送サーバーは異なる

比較サービス②　B社

【懸念点】

・PDFではセキュリティ的観点では特に意味がない…？

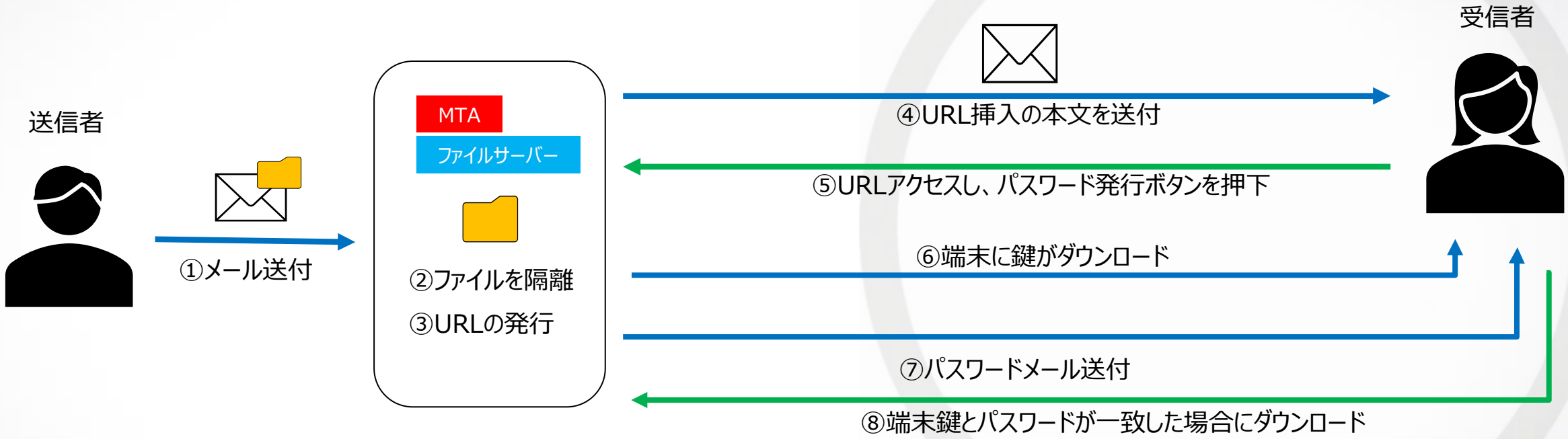
・そもそものURLと鍵を盗聴者に取られたらそこはあきらめる

・元メールとPINコード通知メールの配送サーバーを分けたとしても、
受信メールサーバー側で盗聴されている場合は、結果、
盗聴されてしまうのではないか？

・利用する為には、別途有償で別プランへの移行が必要

比較サービス③　C社

- ファイルの授受にはWebダウンロード方式
- ダウンロードには端末へ保管される鍵と別送パスワードの二要素による認証が必要



【特徴】

・端末鍵を持っていない端末からのアクセス時は不正アクセスとみなしロックを掛ける

・盗聴被害に備え、盗聴者より先に正規受信者がロックすることが可能

比較サービス③　C社

【懸念点】

・そもそものURLと鍵を盗聴者に取られたらそこはあきらめる

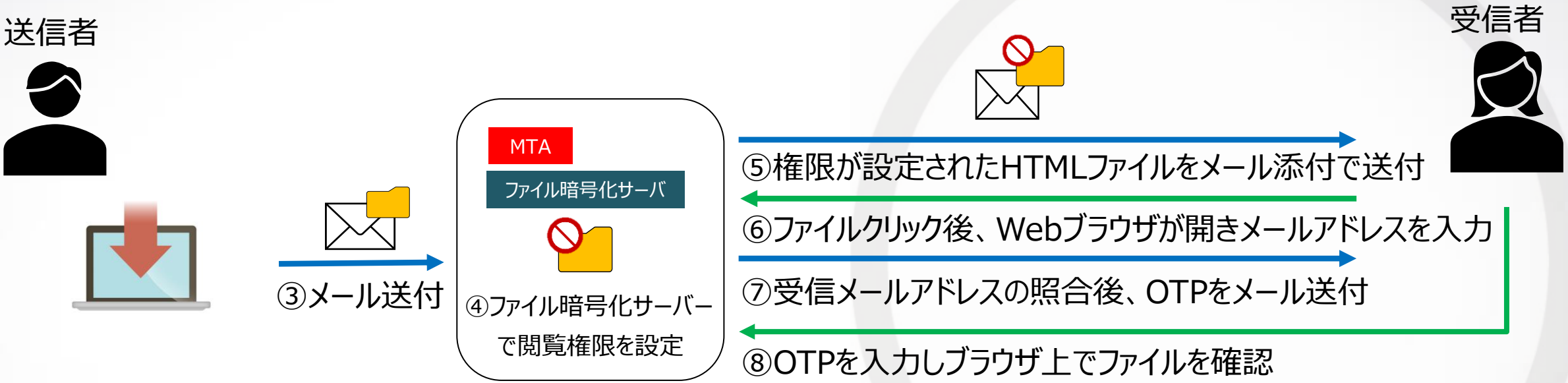
・メーリングリストやグループアドレス宛に送付したファイルは、
いち早くアクセスしたユーザー1名のみがファイルを取得できる為、
その後の社内展開が必要となるのでは…？

・鍵、、、とはメーカー独自のプログラム？受信者側のEndPointセキュリティで
Alertは出ない？

・ 鍵、、、という独自プログラムを相手側（受信者）に扱わせることで、
無用の警戒心を抱かせるのでは？

比較サービス④　D社

- 独自のアプリを使ってファイルを共有
- 端末上のアプリ間では独自プロトコルを使ってファイルの授受を行う



①端末にアプリをインストール

②アプリ上で受信者登録＆権限設定を実施

【特徴】

- 受信者側のファイルを送信者側から削除する操作も可能
- 独自プロトコルなので盗聴の懸念なし

比較サービス④　D社

【懸念点】

・ファイルをアプリ内からOS上の領域へ保存すると、送信者側では削除できない

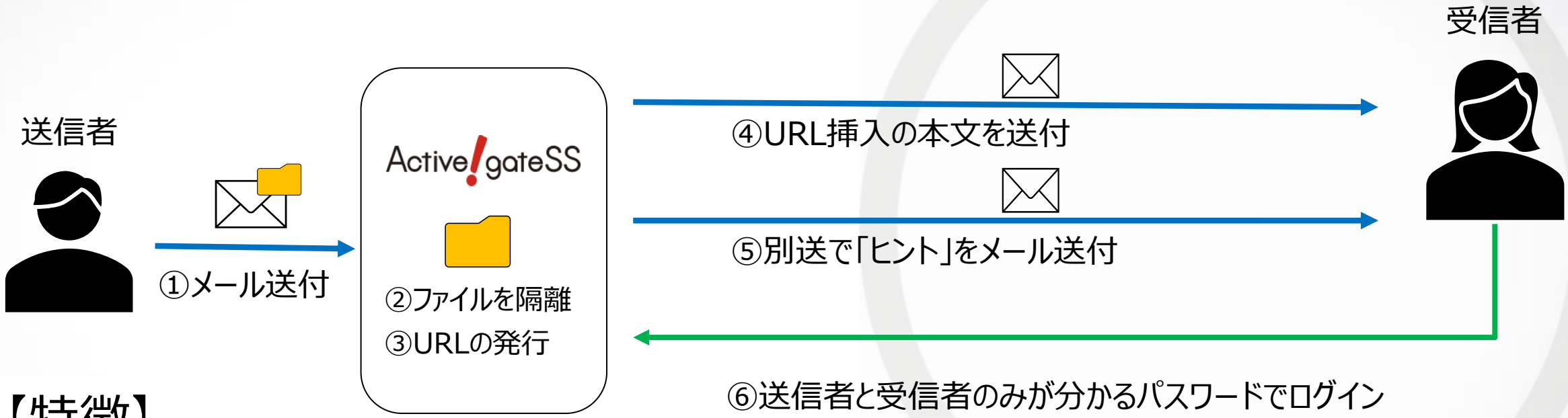
・使えるファイルは限定される
（容量が大きくなりがちな動画ファイルは使用できない）

・HTMLファイル付きメールが盗聴された場合は、あきらめるしかない

・HTMLファイルは日常でのやり取りが少ないので相手側（受信者）に
無用の警戒心を抱かせるのでは？

当社サービス(ActiveGateSS)

- **ファイルの授受にはWebダウンロード方式**
- **固定パスワードを付与し、パスワード通知メールへは「ヒント」のみを記載**



【特徴】

・パスワード自体は通知メールに記載されていない為、パスワードの盗聴が不可能
・別送パスワードメールを待つ必要がなく、決められたパスワードでファイルの取得ができる
・ダウンロード期限を設けることで、ファイル奪取のリスクを低減

【懸念点】

- 初めて送る相手に対してはパスワードをヒントで伝える方式でのやり取りが現実的ではない

サービス比較まとめ

	A社	B社	C社	D社	当社
ファイルの送信方法	WebDL方式	WebDL方式	WebDL方式	WebDL方式	WebDL方式
パスワード通知メール 配送方式	自動送付	受信者発行	受信者発行	受信者発行	自動送付 (ヒントを記載)
一見さんへの汎用性	○	○	○	△ (送信者側での受信者登録処理が必要)	×
盗聴防止策	× (別MTAからのパスワード通知)	△ (PINコードを別MTAから通知)	○ (端末鍵とパスワードで認証)	○ (OTPでの認証)	◎ (パスワードを通知しない為、漏洩リスク無)
待ち伏せ盗聴者への対策	× (短時間で自動配送されてくるため)	△ (受信者のタイミングで配送)	△ (受信者のタイミングで配送)	△ (受信者のタイミングで配送)	◎ (パスワードを通知しない為、漏洩リスク無)
一通目の盗聴による 漏洩リスク	×	×	×	×	○
オンプレでの提供可否	×	×	○	○	○
追加オプションは不要か？	不要	要	不要	要	不要

◆全社共通してWebダウンロード形式を採用

◆パスワード送付方法に各社工夫がみられる

ところが、1通目を取られたらどのサービスもOUT

じゃあクラウドストレージ使う？

■Dropbox　　■Google ドライブ
■Box　　■OneDrive　　など

●PPAPだけの用途を検討するとコスト高

●受信者側でアーカイブが取れない

●過去メールからファイルの確認が困難

（去年の見積ってどれだっけ？）

●PPAPでのメール送付ではないが、結局はURL通知、PW通知が同一経路となる

そもそもPPAP問題とは？

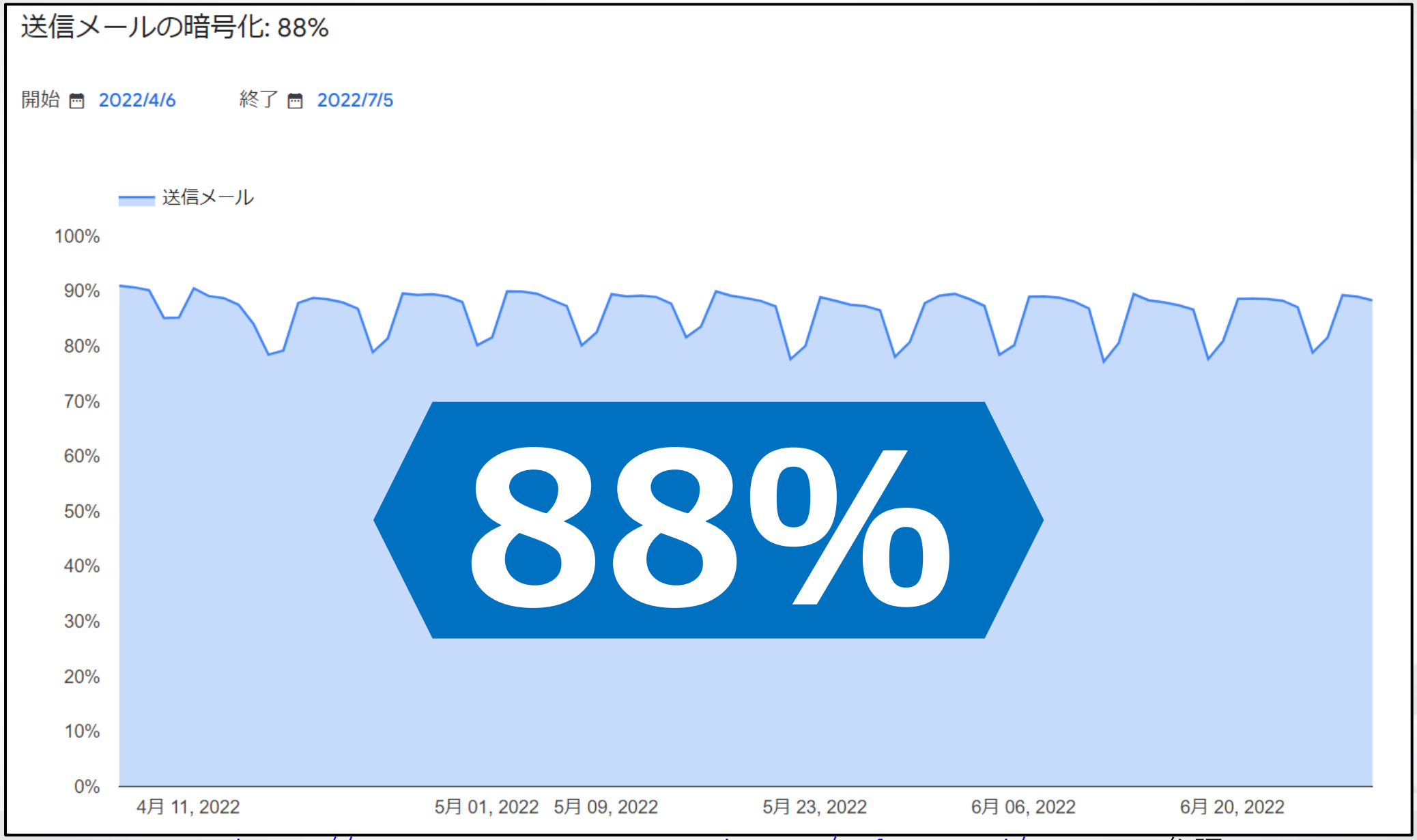
- 盗聴リスクがある（ファイルとPWの同一経路問題）
- ウイルス検知できない（PWファイルのセキュリティスルー問題）
- 利便性が悪い（スマホで見れない問題）

では、ここで考えてみましょう。

今日現在、Internetを飛び交っている
メールの何割が暗号化されているのか？

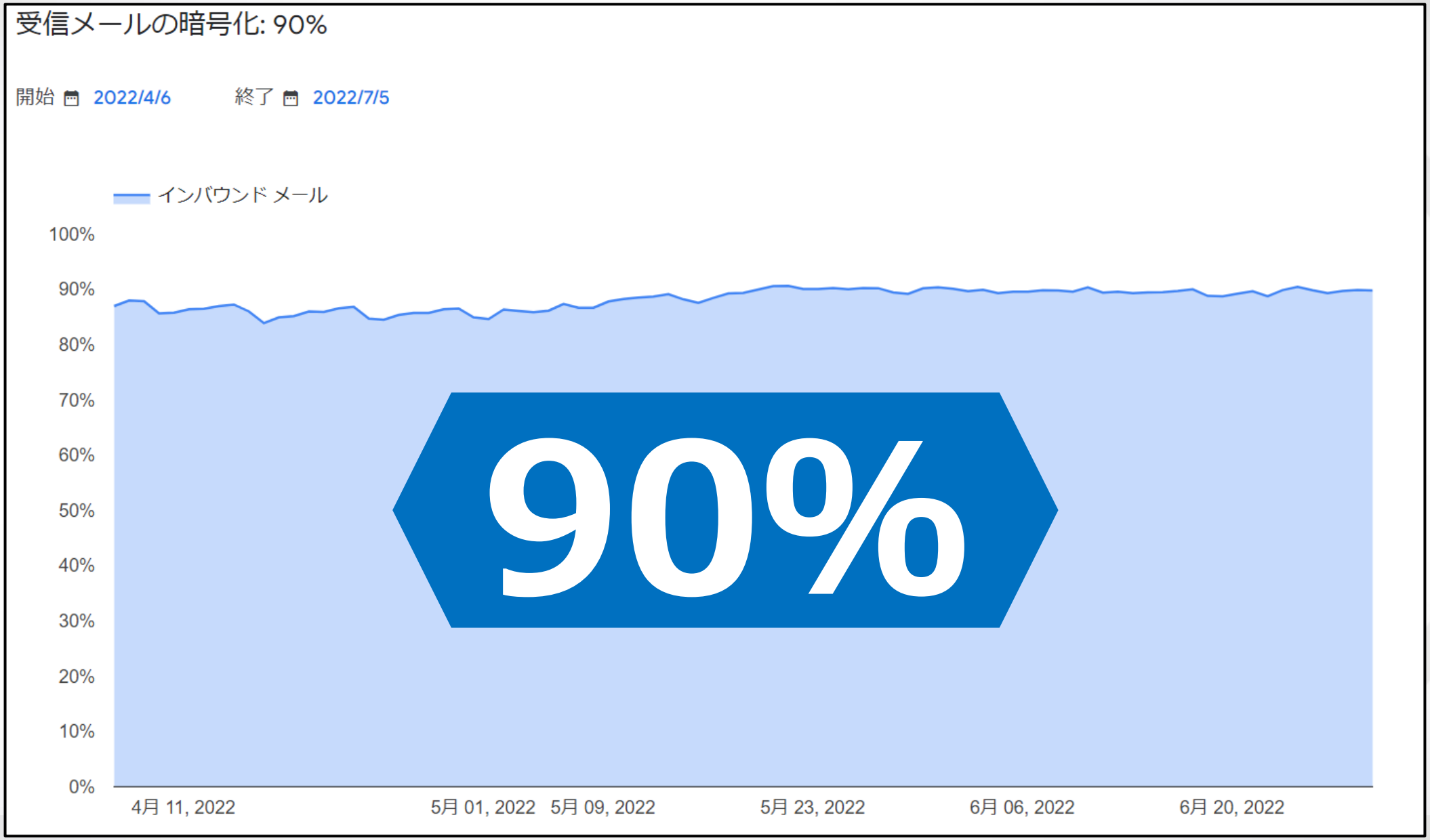
盗聴リスクがあると言うけれど、今までその手法で
盗聴されて情報漏洩えいが明るみになった事故って
ありますか？

Gmailから送信されるメールの通信の暗号化がされている割合



https://transparencyreport.google.com/safer-email/overview参照

Gmailで受信するメールの通信の暗号化がされている割合



https://transparencyreport.google.com/safer-email/overview参照

Active! gate SSのTLS通信割合は？

弊社サービスActive! gate SSを利用いただいているお客様の暗号化通信(TLS通信)の割合は？

90.8%

盗聴リスクがあると言うけれど、今までその手法で盗聴されて情報漏えいが明るみになった事件ってあるのか？

- 少なくとも当社では聞いたことはない
- スノーデンレポートのこと言ってますか？
- 国内のISPってお国の言うillegalなことに黙って従いますか？

そもそもあるかどうかもわかんないリスクに踊らされ過ぎ

PPAPって言い出した人間の罪は重い

当社の考えについて

暗号化(STARTTLS)通信が確立できるメール配送先へは
単純なZipでの送付、もしくは、何もせずに送れば良いのでは？

暗号化(STARTTLS)通信が担保されるか否かを
Active! gate SS で判断し配送ができれば良いのでは？

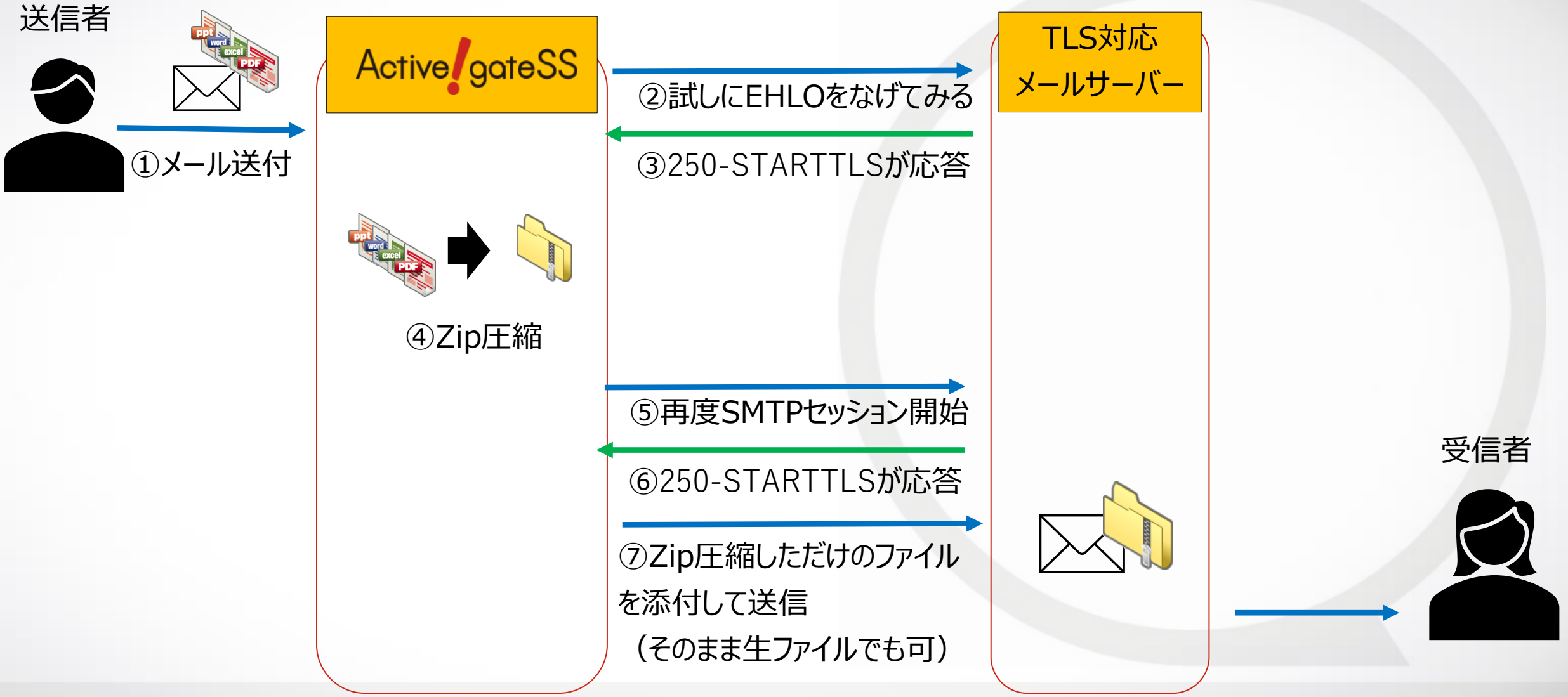
STARTTLS通信の確認はどのように行うか

```
# telnet 172.16.**.** 25
Trying 172.16.**.**...
Connected to 172.16.**.**.
Escape character is '^]'.
        220 receive.qualitia.co.jp ESMTP Service ready
EHLO hoge
        250-receive.qualitia.co.jp Hello [172.16.**.**], pleased to meet you
        250-8bitmime
        250-STARTTLS
        250 help
MAIL FROM: <sender@qualitia.co.jp>
        250 sender@qualitia.co.jp... Sender
RCPT TO: <receiver@example.com>
        250 receiver@example.com... Recipient OK
data
        354 Enter mail, end with "." on a line by itself
<省略>
.
        250 Message queued for delivery as 468c1ec829
quit
        221 Bye...
Connection closed by foreign host.
```

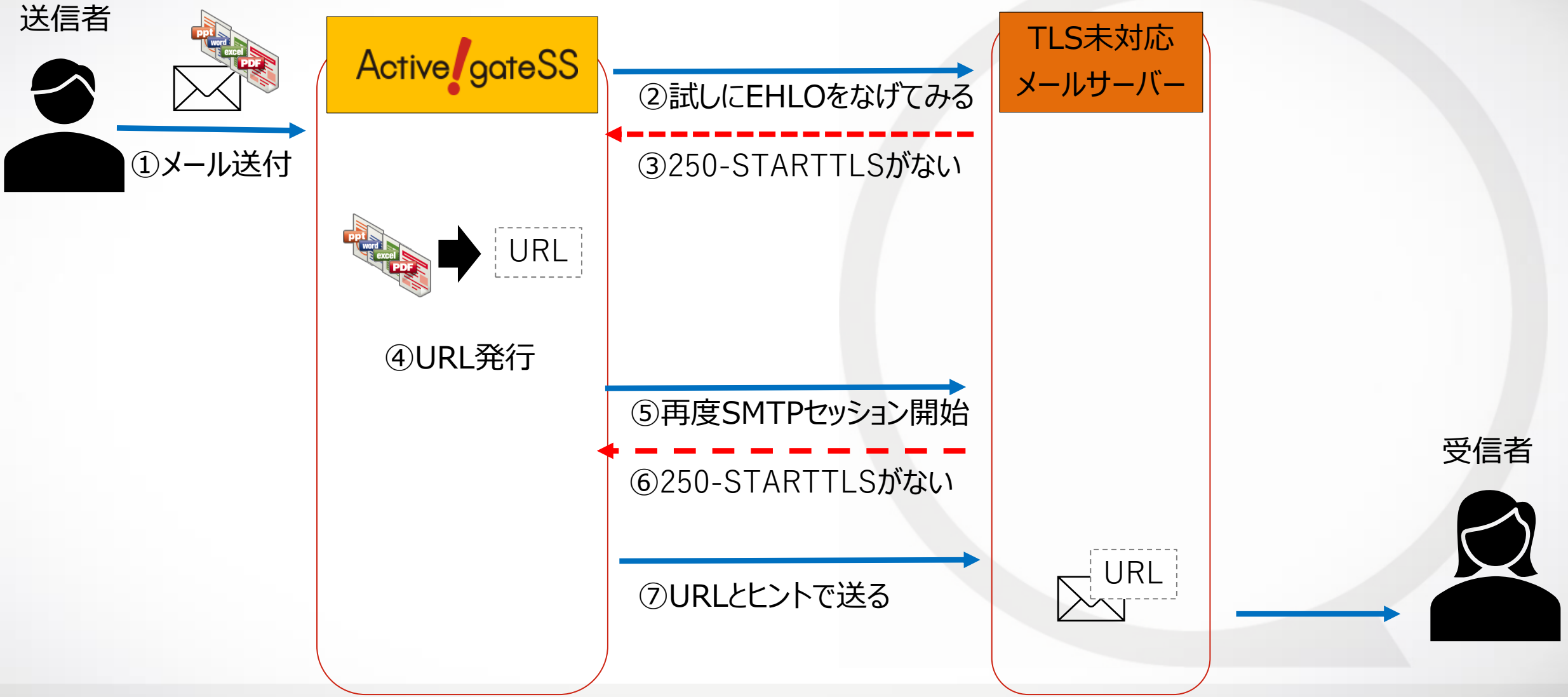
送信する方がEHLOを宣言した後、受信する方の応答でTLSが話せる相手かどうかわかる

応答に
250-STARTTLS
がなければTLSで受けられないという意味

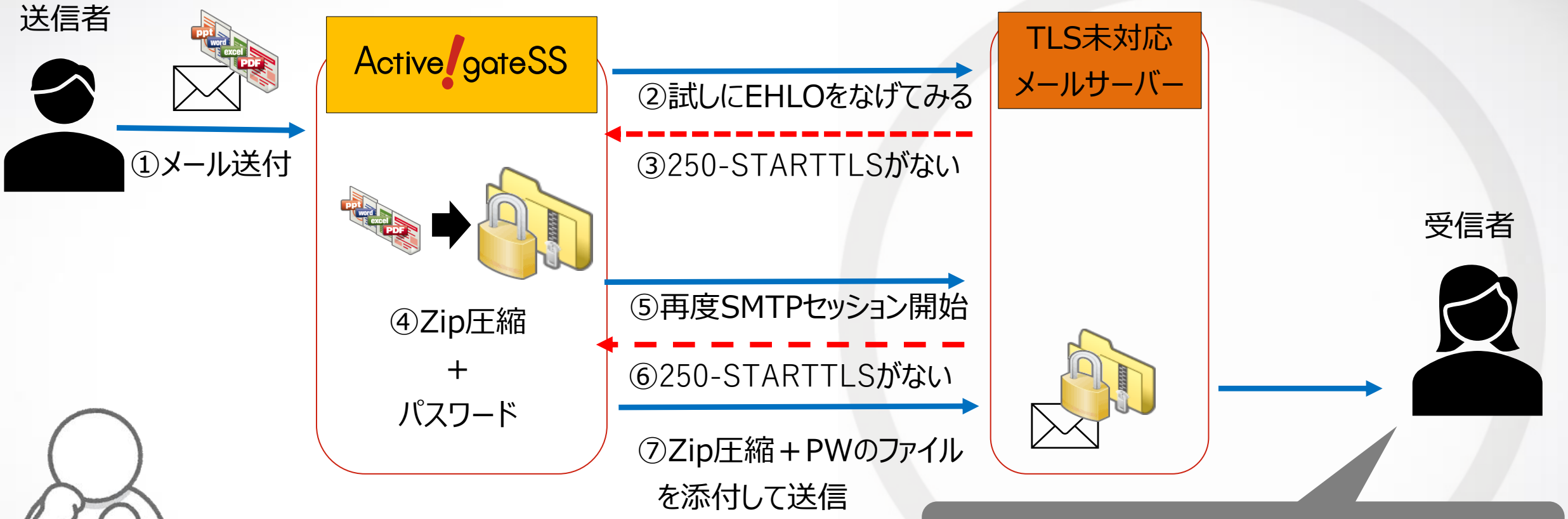
つまり、、、暗号化通信が使える相手なら



では、逆に使えない相手なら？



もっと過激なことをいうと、、、



どうして未だにZipPW？

受信のTLSに対応してください

まとめ

- PPAP（ZipPW）が悪いとされているところ
  - ◆ 盗聴されるリスク？
    - 実害があったかどうかは不明
    - でも各社ともに盗聴防止に躍起になっている
  - ◆ 相手側のセキュリティシステムをすり抜ける
    - Emotetなどの被害の原因に
  - ◆ スマホで見れない
    - 確かに利便性が悪い

生で送っても90%は盗聴されません

生で送ればしっかりウイルスチェック掛かります

クラウドストレージ使っても利便性は上がりません。

まとめ-2

暗号化（STARTTLS）通信は約90%の割合で確立している

➡たった残りの一割のために、ファイル共有サービスを利用すべきか再検討しましょう

➡本来、暗号化通信(TLS)で送っていい相手先にも

- Webダウンロード方式で送ってしまい、アーカイブを取らせてません
- 一年前の見積もりなどを過去メールから検索させず、運用の手間を掛けさせてます

クオリティア社としてのご提案

利便性を落とさず、セキュリティ性を担保し、
現行の運用を変えずに済むのは

メール専業メーカーである当社だからこそできる

TLS確認機能付き
Active! gate SS
へのご利用に切り替えること

TLSに対応してる相手かどうかを具体的に知りたい

https://www.qualitia.co.jp/product/ag/tls-check.html