盗聴は本当に可能なのか？
「脱PPAP」を現実的な視点で考えてみる

株式会社クオリティア

2023年11月7日

@JPAAWG 6th General Meeting

会社概要

株式会社クオリティアは、

メッセージング関連ソリューションの開発・システム構築などを中心とした事業を展開しています。

コミュニケーションの効率化とセキュリティの強化を支援するさまざまなメッセージング関連

ソリューションをソフトウェア・クラウド型サービスで提供しています。

会　社　名	： 株式会社クオリティア
事 業 内 容	： メッセージング関連ソリューションの開発・システム構築など
主要導入先	：一般企業、ISP、文教、公共など　累計1,300万アカウント以上
所　在　地	： 東京都中央区日本橋茅場町3-11-10　PMO日本橋茅場町
設　　立	：1993年10月　有限会社トランスウエア設立 1997年8月　株式会社トランスウエアに改組 2003年1月　ディープソフト有限会社設立 2005年4月　ディープソフト株式会社設立 2015年10月　両社の合併により株式会社クオリティア設立

許認可・資格・認証

- 電気通信事業　届出番号A-22-11059
- 日本語ドメイン取り扱い事業者
- ISO/IEC 27001（情報セキュリティマネジメントシステム：IS 586579）
- ISO/IEC 27017（ISMSクラウドセキュリティ認証：CLOUD 681574）
- ISO/IEC 27018（パブリッククラウド上の個人情報保護：PII 681575）
- ISO/IEC 27701（プライバシー情報マネージメントシステム：PM 757678）

Active!gateSS
メール誤送信防止サービス

Active world
メール統合サービス

Active!vaultSS
メールアーカイブサービス

Active!zoneSS
標的型メール攻撃
対策サービス

Introduction①

その昔、2020年11月24日に 平井デジタル担当大臣（当時）の 脱パスワード付きZipファイル宣言がありました

- 2020年11月17日の定例会見で、職員が添付ファイルをメールで送信する際に使う**パスワード付きzipファイルを廃止**する方針を明らかにしたこと
- 廃止の理由
  - 受け取り側の利便性が低い（スマホで見れない）
  - セキュリティ対策の観点から適切ではない（かえって危険性が高い）
- 「**脱PPAP**」「**PPAP対策** 」とワードが広まるきっかけになった

引用：https://www.cao.go.jp/minister/2009_t_hirai/kaiken/20201124kaiken.html

Introduction②

- 「PPAP」提唱者を探してみた
    - 2016年、当時JIPDECに所属していたO氏（現・PPAP総研）
- 脱PPAPと言い出した理由
    - 効率が悪い
    - 受信側のマルウェアフィルタをすり抜ける
    - **2通目に同じ経路でパスワードを送るのであれば秘匿性がない**

PPAPという言い方があまり気に食わないのは わたしだけでしょうか

二つの宣言を比較

	脱PPAP宣言	脱パスワード付きZipファイル宣言
宣言時期	2016年	2020年
理由	① 効率が悪い ② 受信側のマルウェアフィルタをすり抜ける ③ 2通目に同じ経路でパスワードを送るのであれば秘匿性がない	① 受け取り側の利便性が低い（スマホで見れない） ② セキュリティ対策の観点から適切ではない（かえって危険性が高い）

政府はあえて
「盗聴対策にはなっていない」
と言わなかった

この差異についての考察

- 仮に「盗聴対策になっていない」と政府が言うと、、、

  そもそも盗聴って現実的にできないはずなのでそんな突拍子もないことは言えない

  or

  政府が「盗聴の事実を認識している」ことを認めることになる

  のいずれかではないかと推測

確かに以前からSMTPは盗聴し放題とは言われてきた

都市伝説が
都市伝説じゃなくなった
出来事

スノーデンレポートによる暴露（2013年）

- 米国内大手メールプロバイダーがNSA（国家安全保障局）の要請に従って、PRISMを自社サイトに仕掛け、フィルタリングした情報を渡していた
- NSAがデンマークのインターネット・ケーブルを盗聴し、複数の各国政府高官のテキストメールを盗聴
- NSAが極秘の情報監視システムを日本側に供与し、**日本政府が**個人の**メール**や通話などの**大量監視を行える状態**にあることを示唆

確かに以前からSMTPは盗聴し放題とは言われてきた

しかし、それって私的な興味とかで高度なスキルを持ってる人たちならできるよ、とかそういう立場にいる人ならできちゃうよ、という話かと思ってた。

再度、政府のこの理由についての考察

- 仮に「盗聴対策になっていない」と政府が言うと、、、

  そもそも盗聴って現実的にできないはずなのでそんな突拍子もないことは言えない

  or

  政府が「盗聴の事実を認識している」ことを認めることになる

  のいずれかではないかと推測

後者・・・、かな。
「盗聴してるかどうかは別にして、メール盗聴はできるものだ」
との認識を持っていることを認めることになる

ここから本題

- そもそも国内においてメール盗聴って本当に可能なのでしょうか？

① 国家権力系

米国政府のように国家権力がメールプロバイダーに指示する

② 個人犯罪系

xSP、データセンター事業者の従業員による不正

③ 高等技術系

DNSハック等によりMXレコードを書き換え、自分が管理するMTAを経由

皆さんにお聞きしたい。
どれが現実的にあり得そうでしょうか？

①国家権力系（国家権力がメールプロバイダーに指示）

- フィルタツール仕込め、logを出せ、アーカイブデータ提出しろ、など言われたことありますか？
- 実際にやってますか？

ですよね、「言えないよ」ね・・・

②個人犯罪系（xSP、データセンター事業者の従業員による不正）

- 皆さんは盗聴したい人です。現実的に考えてみましょう。

事業者名は分かるけど、DCがどこか？ってなかなか難しい

まぁDNS見りゃ一発ですね

標的とする企業の利用メールシステムを突き止める

↓

SaaSならDCを突き止める（オンプレならサーバルームの場所）

↓

そのラックに近づける人にピンポイントでコンタクトしないといけません

だいたい本社ビルの中ですかね
違うケースもあるよね

従業員にコンタクトする

↓

大容量のストレージを持ち込ませて

Portが埋まった、SSHで入った、Wiresharkが動いてるとか監視網って潜り抜けられる？

スイッチつながせてパケットキャプチャ取らせる

↓

最近のDCって荷物チェック、監視カメラ、ID確認など物理チェック厳しい

持ち出させる

非現実的な匂いしかしてこない・・・

③高等技術系（DNSハック等によりMXレコードを書き換え、自分が管理するMTAを経由）

こまかいことは言うなかれ

皆さんを前にして思うことは

（これが一番現実的かも・・・）

現実的なメール盗聴の可能性

① 国家権力系

国家権力が秘密裏にメール盗聴したいとししたらテロや組織犯罪対策なので、BtoCのメールが対象だろうと思われる。したがって、脱PPAPはBtoBでの利用シーンがメインとなり、想定する盗聴者は国家ではないのでこの可能性は一旦排除する

② 個人犯罪系

5年10年まで迄は最も確実な方法だったと思われるが、NW的にも物理的にも心理的にもセキュリティレベルが上がったこの令和の時代に最も不確実な方法になった

③ 高等技術系

DNSハックによるMX切り替えは、TLS通信も解凍できるし全部自分の手元を流れるので、どうにでもできる。あと、MXレコードが変更されたってそんなに気づかないのでは？

結論：DNSのセキュリティをしっかりやろう

となると、、、

DNSのセキュリティってメール屋のすべき
ことではない

受信者側の責任で対策してもらわないといけない

脱PPAPを論じるうえで、
メール屋が盗聴を懸念することはなくなった

脱PPAP宣言後の各メール屋の対応は？

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

つまり盗聴対策に一生懸命になってる

盗聴対策は受信者側の責任であるにもかかわらず

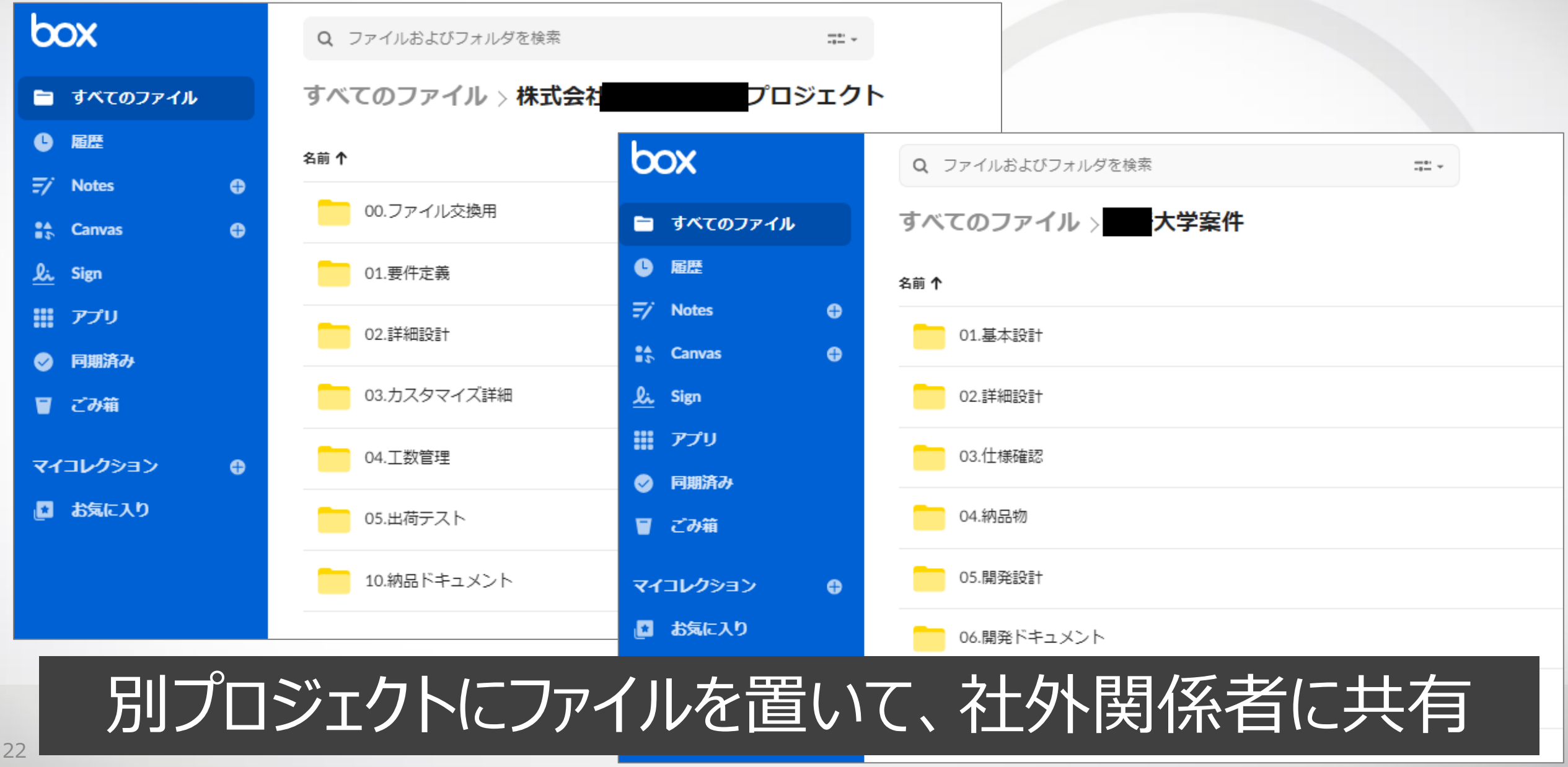
じゃあクラウドストレージ使う？

■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？）
- 社員に利用を強制させられない
- 誤送信ならぬ、**誤配置**が頻発しているという事実

クラウドストレージの誤配置とは？

クラウドストレージの誤配置とは？



別プロジェクトにファイルを置いて、社外関係者に共有

クラウドストレージの誤配置問題

社員に利用を強制させられない

⇩

管理者の影響が及ばない

⇩

管理者が誤配置に気づけない

⇩

会社が知らない間に情報漏洩が発生している

QUALITIA

そもそもPPAP問題とは？

- 利便性が悪い（スマホで見れない問題）
- 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）
- 盗聴リスクがある（ファイルとPWの同一経路問題）

利便性のこと忘れてませんか？

スマホで見させてあげて、
ウイルス検知させてあげませんか？

ここで再度整理します。

DNSハックによる盗聴対策は、受信者の責任

送信者の責任は、
安全な通信でメールを送りだすこと
と
受信者の利便性

メール通信のTLS普及率

約90%

※クオリティアサービス利用者　送信時 90.8%　受信時88.6%　22年5月調査
※Google公表　Gmailの暗号化率　送信時 82% 受信時 96%

10社に1社がTLS非対応

脱PPAPのジレンマ

STARTTLSで送付

非対応の1社の
セキュリティを
確保ができない

Webダウンロードで送付

TLS対応済みの9社に
不要な手間がかかる

**セキュリティ性と利便性の
トレードオフが発生してしまう**

クオリティアの考えとは

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

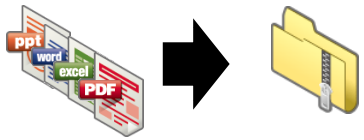
送信者

①メール送付

Active!gateSS

②試しにEHLOをなげてみる

③250-STARTTLSが応答



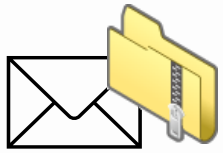
④Zip圧縮

⑤再度SMTPセッション開始

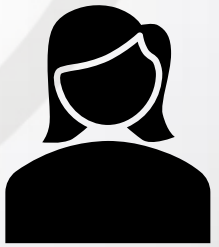
⑥250-STARTTLSが応答

⑦Zip圧縮しただけのファイル
を添付して送信
（そのまま生ファイルでも可）

TLS対応
メールサーバー

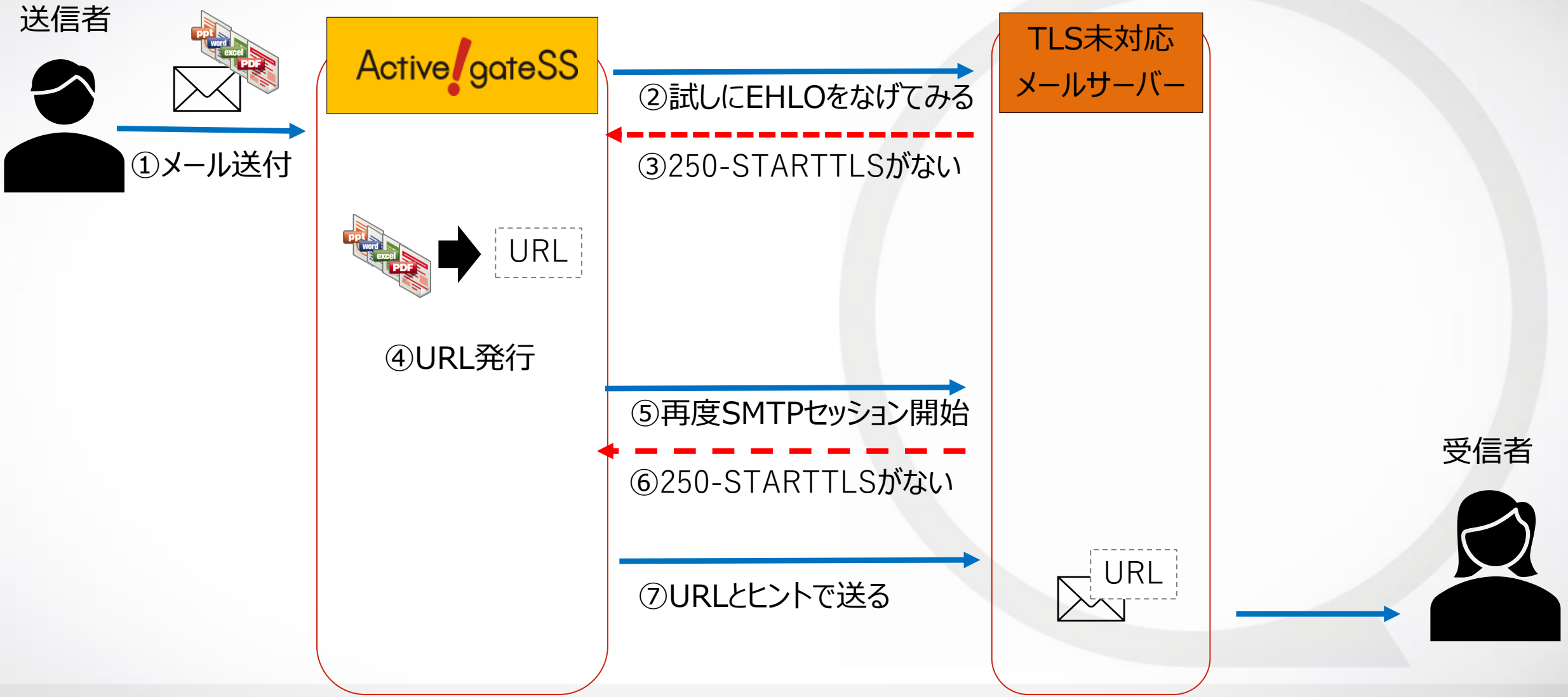


受信者

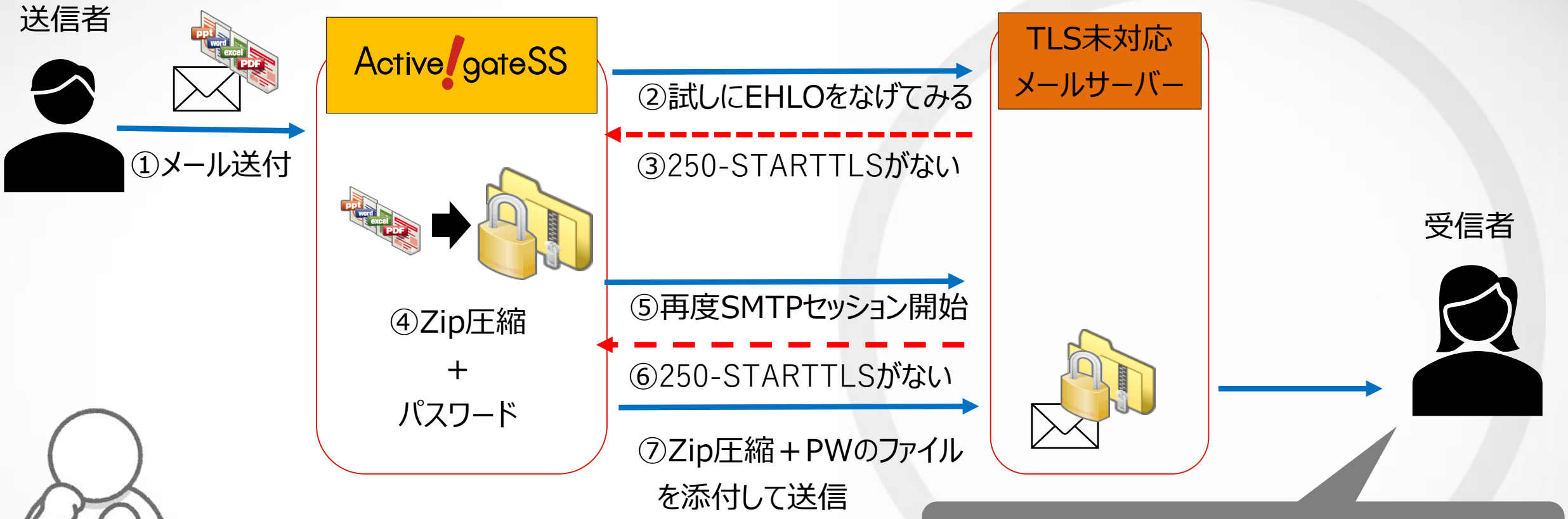


QUALITIA

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

※当社調べ（2022年6月21日～2023年6月21日までの新規／既存顧客 累計利用社数）

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

ホスティング事業者の方へ

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
でサービス提供いかがですか？

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