「標的型メール攻撃」と「脱PPAP」に有効なソリューション

2023年2月27日

株式会社クオリティア
佐々木　泰

QUALITIA

CONTENTS

私たち「クオリティア」について

QUALITIA

TransWARE　DEEPSoft

社　名　株式会社クオリティア

本　社　東京都中央区日本橋茅場町 3-11-10

設　立　1993年10月

資本金　8,500万円

代　表　松田　賢

QUALITY MAKES FUTURE

- メッセージング関連ソリューションの開発・販売
- 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
- クラウド型サービス・オンプレミス型ソフトウェアで提供

QUALITIA

02　「標的型メール攻撃」に有効なソリューション

日本年金機構の標的型メール攻撃の被害事例

2015年、日本年金機構が標的型メール攻撃により、年金加入者の氏名や
基礎年金番号など約125万人の個人情報が流出

原因：職員がメールを開封してウイルスに感染
メール件名：『厚生年金基金制度の見直しについて（試案）』に関する意見

ばらまき型

メールが受信者に関係のない内容、添付ファイルを
開くと感染し、感染したことに気づきやすい

標的型攻撃

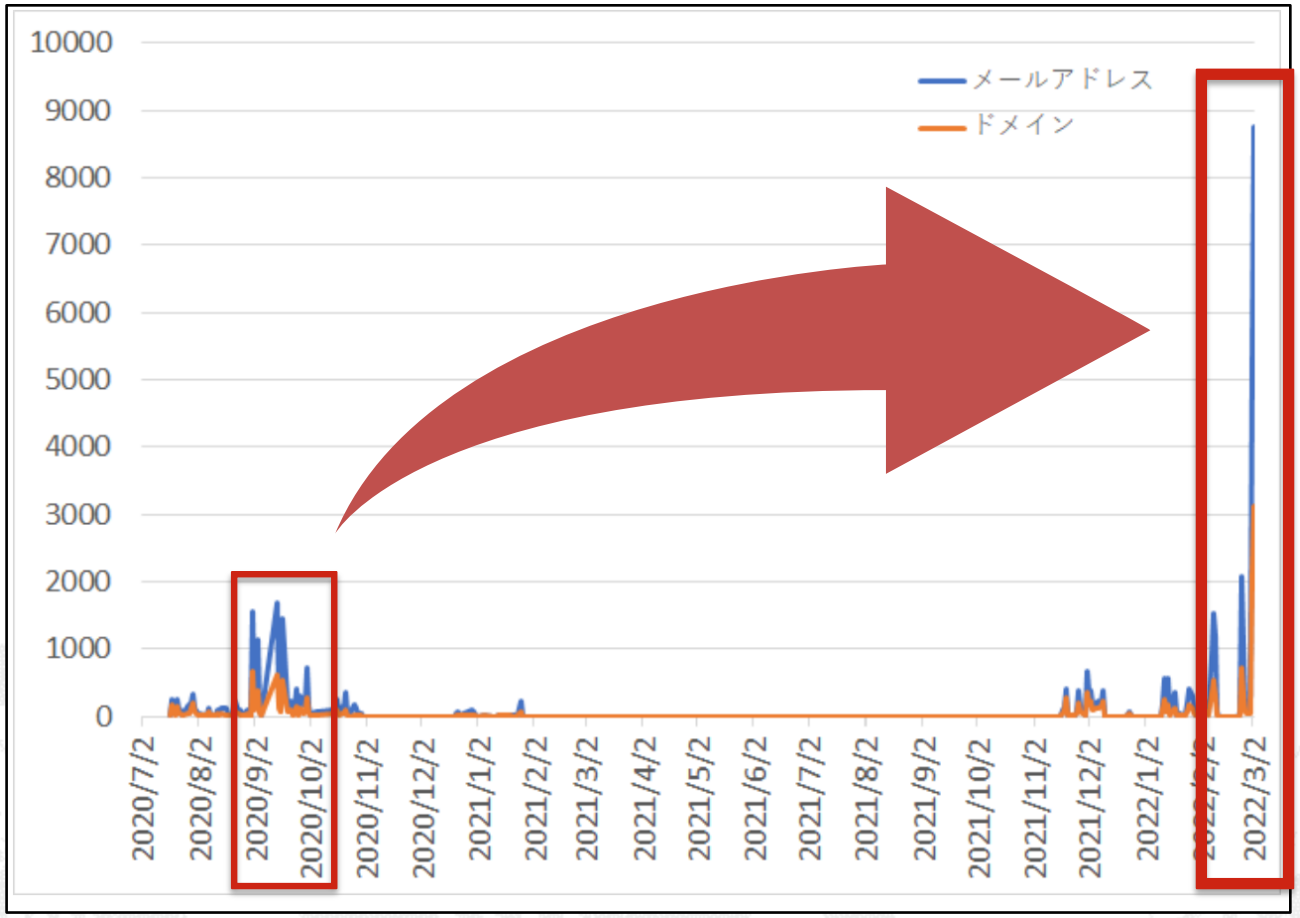
特定の企業や団体などを狙い、巧妙な偽装メールを送付
（数が出回らないので、パターンファイルにマッチしない）

パターンファイルマッチング型
AntiVirus

サンドボックス型 AntiVirus

QUALITIA

Emotet（エモテット）の感染被害が再拡大



2022年３月に入り、
Emotetに感染しメール送信に
悪用される可能性のある『.jp』の
メールアドレス数が2020年の
感染ピーク時から約5倍以上に急増

出典元： Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数の新規観測の推移（外部からの提供観測情報）
https://www.jpcert.or.jp/at/2022/at220006.html

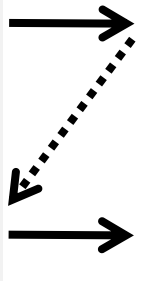
QUALITIA

「攻撃」と「防御」のイタチごっこ

ばらまき型
(メールが受信者に関係のない内容、添付ファイルを開くと感染し、感染したことに気づきやすい)

標的型攻撃
(大量に出回らないのでパターンファイルにマッチしない)

添付ファイル暗号化型(Emotet)
(パスワード付き添付ファイルで信憑性が高くつい開いてしまい感染、最新の脅威で深刻な被害が懸念)



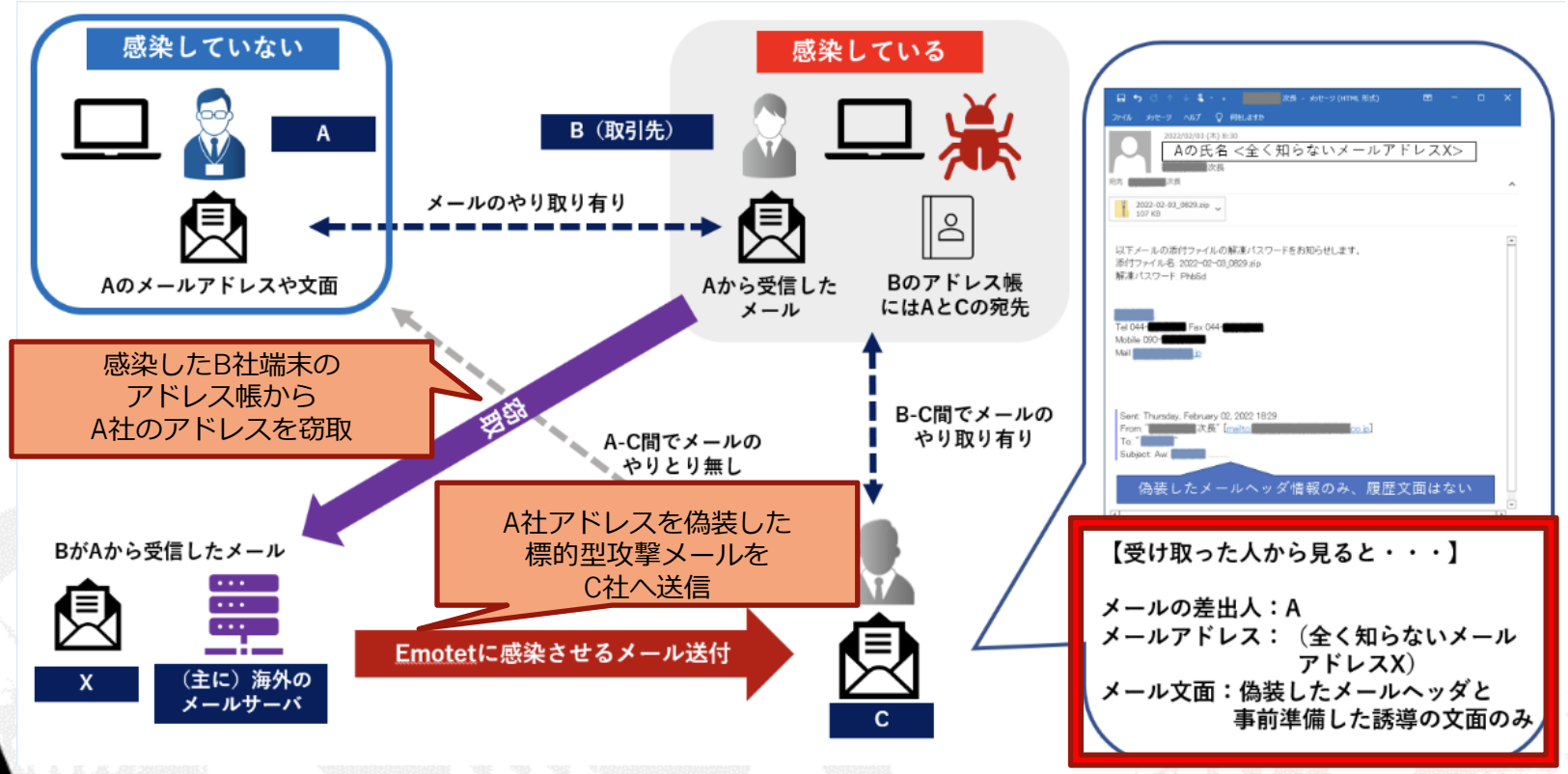
パターンファイルマッチング型
AntiVirus

サンドボックス型 AntiVirus

QUALITIA

Emotetの最新事例

取引先がEmotetに感染し、なりすましメールが配信されるケース



メールの差出人：実在する企業名や人名
メールアドレス：攻撃者のアドレス
→更にメールの巧妙性が増している

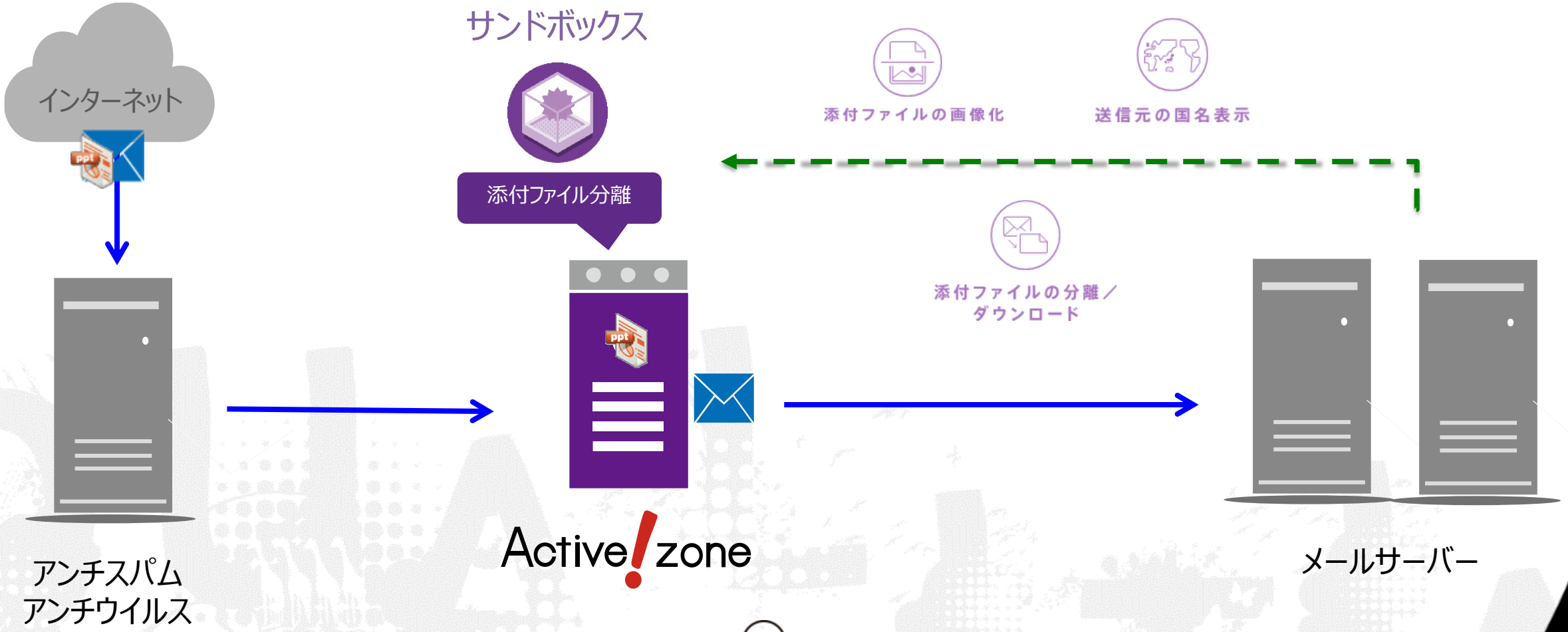
2022年7月中旬より、Emotetの感染に至るメールは国内では確認されず

しかし、11月初旬より再度確認
→忘れた頃を狙って再攻撃が始まる

出典元： マルウェアEmotetの感染再拡大に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220006.html

QUALITIA

Emotetなどの標的型メール攻撃に有効なソリューション



Zipパスワード付きファイルも検知

一目でわかる判定結果

Safe	アンチウイルスエンジンまたはサンドボックスにより無害と判定されたファイル。
Danger	アンチウイルスエンジンまたはサンドボックスによりウイルスと判定されたファイル。変換なども含めて一切のダウンロードが不可。
Unsupported	Active! zoneが暗号化を解除できないファイル。ウイルスチェックが行われていないため、原本のままダウンロードする場合は要注意。
Error	内部処理でエラーが発生。ウイルスチェックが行われていないため、原本のままダウンロードする場合は要注意。

Active!zone の特長

- ✓ 添付ファイル分離／ダウンロード＋サンドボックス、添付ファイル画像化、送信元の国名表示などの機能を持つ標的型メール攻撃対策ソリューション
- ✓ 1,741の自治体の内、400以上の自治体が採用
- ✓ 大手プロバイダー（I社）のメール無害化エンジンとして採用
- ✓ Emotet対応として国内で初めてリリースされたソリューション
- ✓ Emotetの検知・ブロックに多数の実績があり

ノベルティをお受け取りください

QUALITIA

03　「脱PPAP」に有効なソリューション

平井元デジタル改革担当相の「脱パスワード付きZip宣言」とは？

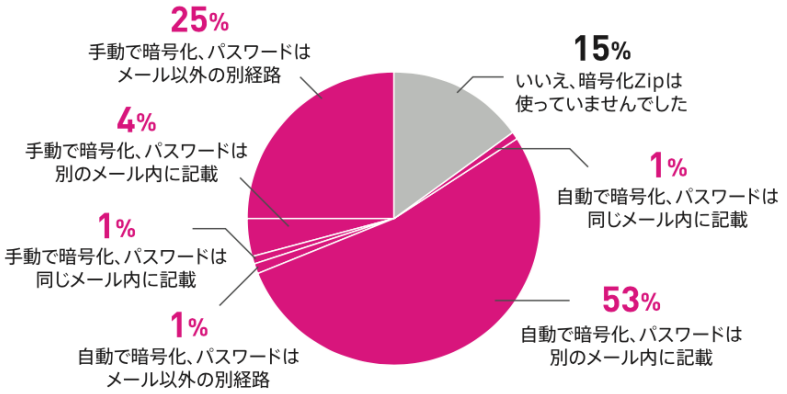
Passwordつきzip暗号化ファイルを送ります
Passwordを送ります
Aん号化
Protocol

- ✓ 2020年11月17日の定例会見で当時の平井デジタル改革担当相が、官庁職員が文書などのデータをメール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に（同月26日から実施）
- ✓ 廃止の理由
  - 受け取り側の利便性が低い（スマートフォンで見れない）
  - セキュリティレベルを担保するため、という理由が薄弱

PPAPの現状と指摘されるリスクとは？

PPAP運営の現状

以下は当社のお客様（有効回答数 514件）に2021年2月4日～15日の期間で実施したアンケートの結果です。
実にPPAPの利用は85%、パスワードをメールで送っていたお客様は59%に達していたことがわかります。



2020年11月以前において、
添付ファイルの暗号化Zipを利用してメールを送っていましたか？

情報漏えいのリスクがあるPPAP

広く普及していたPPAPですが、昨今では以下の2点の情報漏えいリスクが指摘されています。

暗号化した添付ファイルとパスワードを同一経路で送信している

▼

添付ファイルを盗聴されるリスク

暗号化したファイルをメールに添付して送り、同一経路で後追いパスワードを受信者に伝えることは、その経路上を第三者に盗聴されていたとしたらパスワードまで傍受されるため暗号化の意味がありません。

ファイルを暗号化してメール添付すると
ゲートウェイでのウイルスチェックができない

▼

標的型メール攻撃を受けるリスク

Emotet、IcedIDなどのマルウェア（ウイルス）は暗号化したファイルをメール添付で送ってきます。一般のセキュリティソフトでは検出が困難で、ウイルスチェックやサンドボックスチェックをすり抜けてしまいます。

QUALITIA

検討された当面の代替策

現時点での代替手段

PPAPの代替手段は現状いくつかの方法が考えられます。しかし、受信者側のセキュリティ性を担保しつつ同時に送信者の利便性も維持することを念頭に置くと、残念ながらどの手段も完全な解決策と言えません。

01 STARTTLS、MTA-STSZ (TLS1.2以上)、DANEなどのメールサーバー間のセキュリティ対策を利用する

課題

- 送信者及び受信者はメールサーバー間の暗号化通信に対応しているか確認する手段がない

02 クラウドストレージを利用する

課題

- URLとパスワードを同一経路で送るとZip暗号化と同じことになってしまう
- 過去のメールから検索し、当時配送されていたファイルを確認しようとしてもメールとファイルが分かれている、どのファイルが見つけたいものなのかわからない

03 S／MINE、PGPなどの電子署名と暗号化の仕組みを利用する

課題

- 証明書や鍵の管理が容易ではなく、またゲートウェイでのウイルスチェックができない
- 利用可能なメールクライアントが限定され、送受信を行うには相手にも高度なナレッジを求めることになる

04 チャットやSNSなどを利用する

課題

- 送信者、受信者ともに同一のアプリケーションを利用している必要性があり汎用性が低い

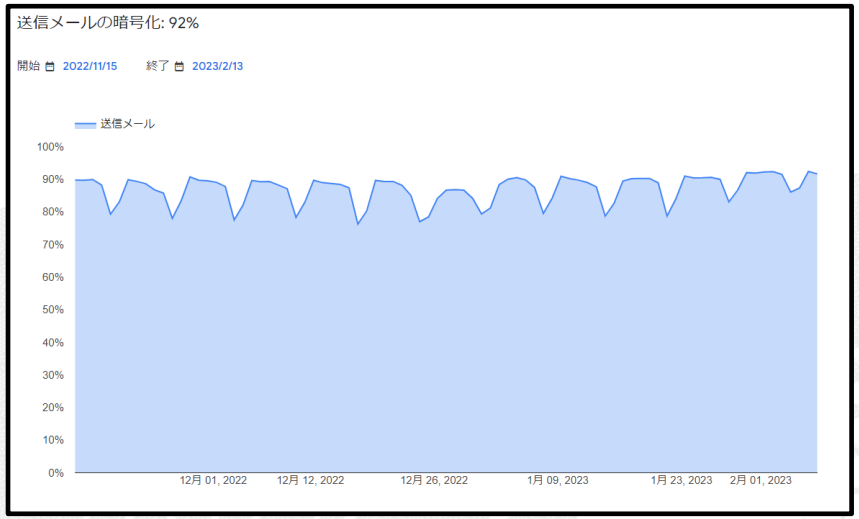
QUALITIA

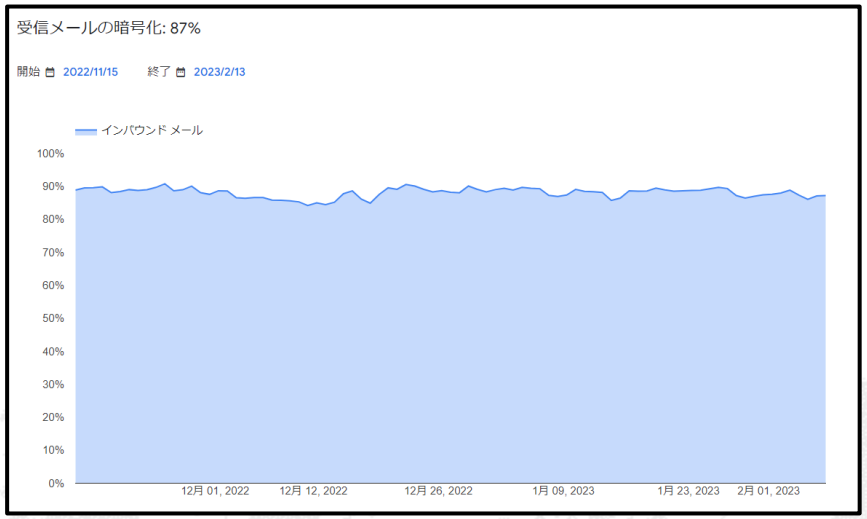
各メーカー推奨の「添付ファイルのWebダウンロード」方式

	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

そこで当社はメールの通信経路に着目しました

- ✓ Gmailから送信されるメールの通信が暗号化されている割合 → 92%
- ✓ Gmailで受信するメールの通信が暗号化されている割合 → 87%
- ✓ 当社サービスのメールの通信が暗号化されている割合 → 送信 90.8%、受信 88.7%





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

QUALITIA

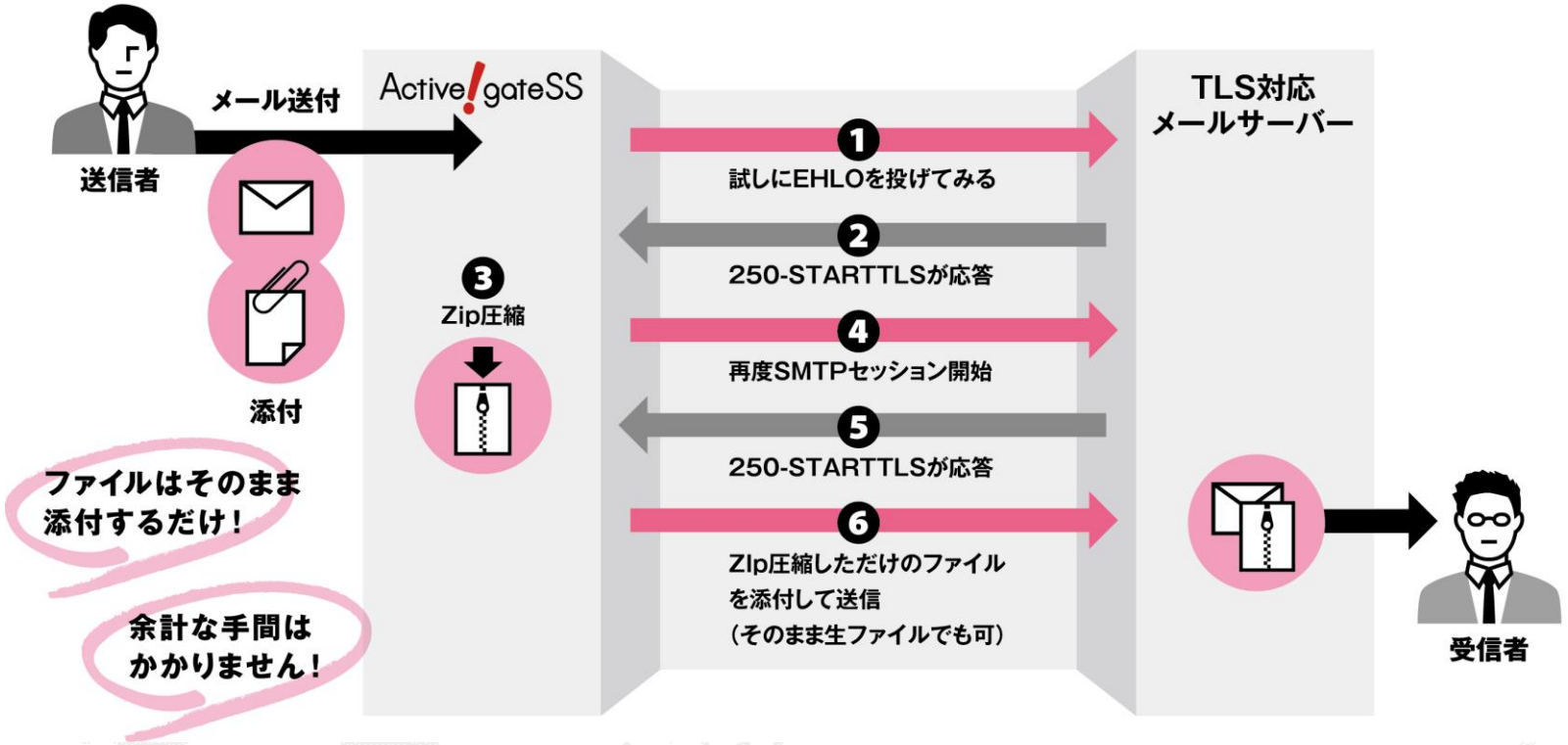
STARTTLS通信の確認はどのように行うか

```
# 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 OK
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.
```

送信する側がEHLOを宣言した後、受信する側の応答でTLSが話せる相手かどうかがわかる

応答に
　250-STARTTLS
がなければ、TLSで受けられないという意味

Active!gateSS のTLS確認機能



- 配送先のメールサーバーがTLSに対応しているかメール送信前に確認を行い、対応している場合はTLS暗号化通信で送信します。
- ファイルはそのまま添付されるか、パスワードなしのZipに圧縮化されて添付されます。
- 配送先のメールサーバーがTLS対応していない場合は「Webダウンロード」などに自動的に切り替えます。

QUALITIA

TLS確認機能のノベルティを制作中です

QUALITIA

04 Q&A

ご清聴ありがとうございました！