JPAAWG Japan Anti-Abuse Working Group

JPAAWG 若手メールエンジニア向けメールセキュリティトレーニング

メールの送受信を見てみよう

メールアプリ・メールサーバ間通信の解説

JPAAWG

○講師紹介

森崎 聡

- 株式会社オプテージ
  - 技術本部プラットフォーム技術部サービスシステムチーム所属
  - 回線付帯のメールサービス、社内用メールリレーサーバ

○今日やること

- **メールアプリでメール送受信をしている際に**
  - **メールアプリと送信メールサーバ間**
  - **送信メールサーバと受信メールサーバ間**

  でどういったやりとり（通信）が行われているのかを実際に見てみる

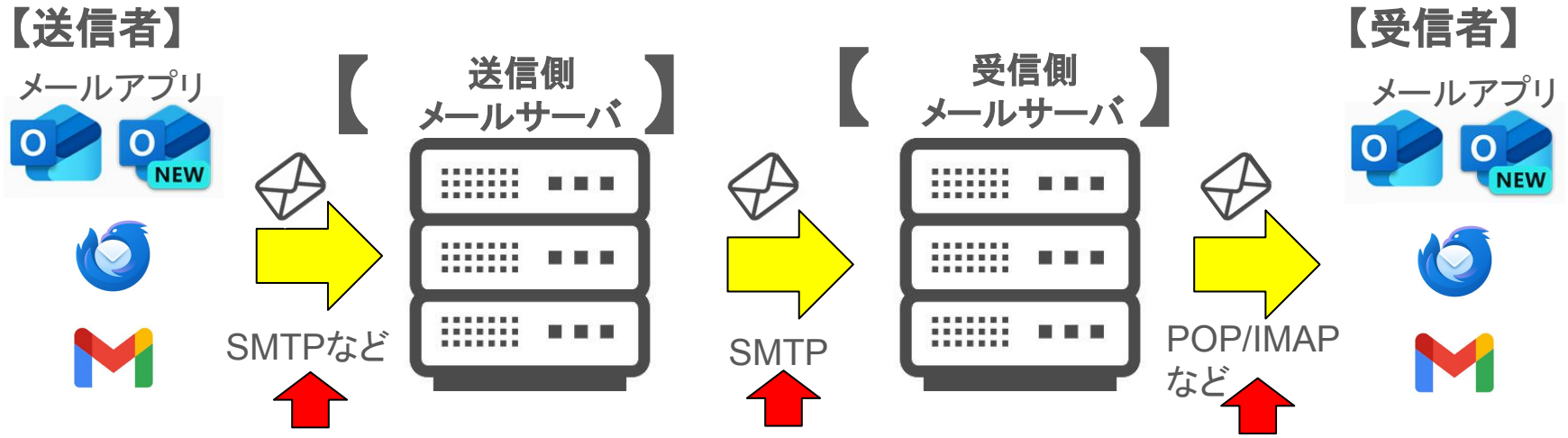
  メールアプリでメールを送受信してみて、その時の通信を傍受（パケットキャプチャ）して内容を確認する

【ゴール】メールの送受信についての理解を深める

○セットアップ

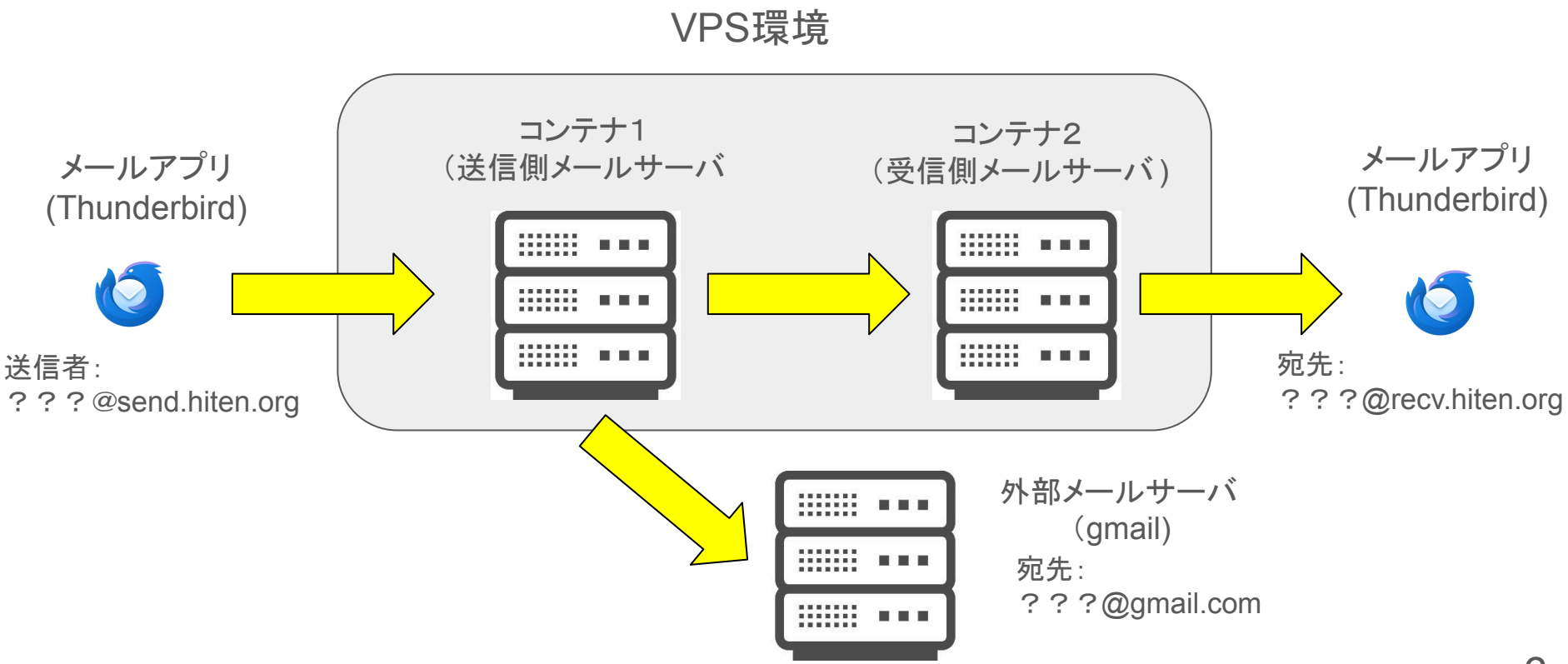
- メール送受信の基本説明
- 本日の実験環境のご紹介
- 本日やること一覧

○メール送受信の基本（超おおざっぱに）



本日は ⬆ の部分の通信を見ていきます

○本セッションの環境構成



○セッションの進め方

○ 資料で説明

○ メールアプリ(Thunderbird)の設定確認・送受信

○ 通信を取得（キャプチャー）して表示・説明

今から、ちゃんと表示されるか（見れるか）のテストします

○お品書き

- **メールの送受信基本**
  - SMTP
  - POP
  - IMAP
- **認証と暗号化**
  - SMTP認証
  - 暗号化（overSSL、StartTLS、エンドツーエンド暗号）
- **メール送信時のセキュリティ機構**
  - HELO/EHLO
  - From詐称

時間の許す限り見ていきます（最後まで行けなかったらごめんなさい）

○ちなみに余談ですが・・・

今回は通信の当事者による盗聴？傍受？のぞき見？ですが

第三者間の通信についてキャプチャを行うと『通信の秘密を侵害』する行為となります。

違法性があるかどうかは「通信当事者の同意がある」「違法性除却事由にあたる」など、正当な理由があるかどうかが問われます。

※詳細は別の機会にやるかもしれない（やらないかもしれない）

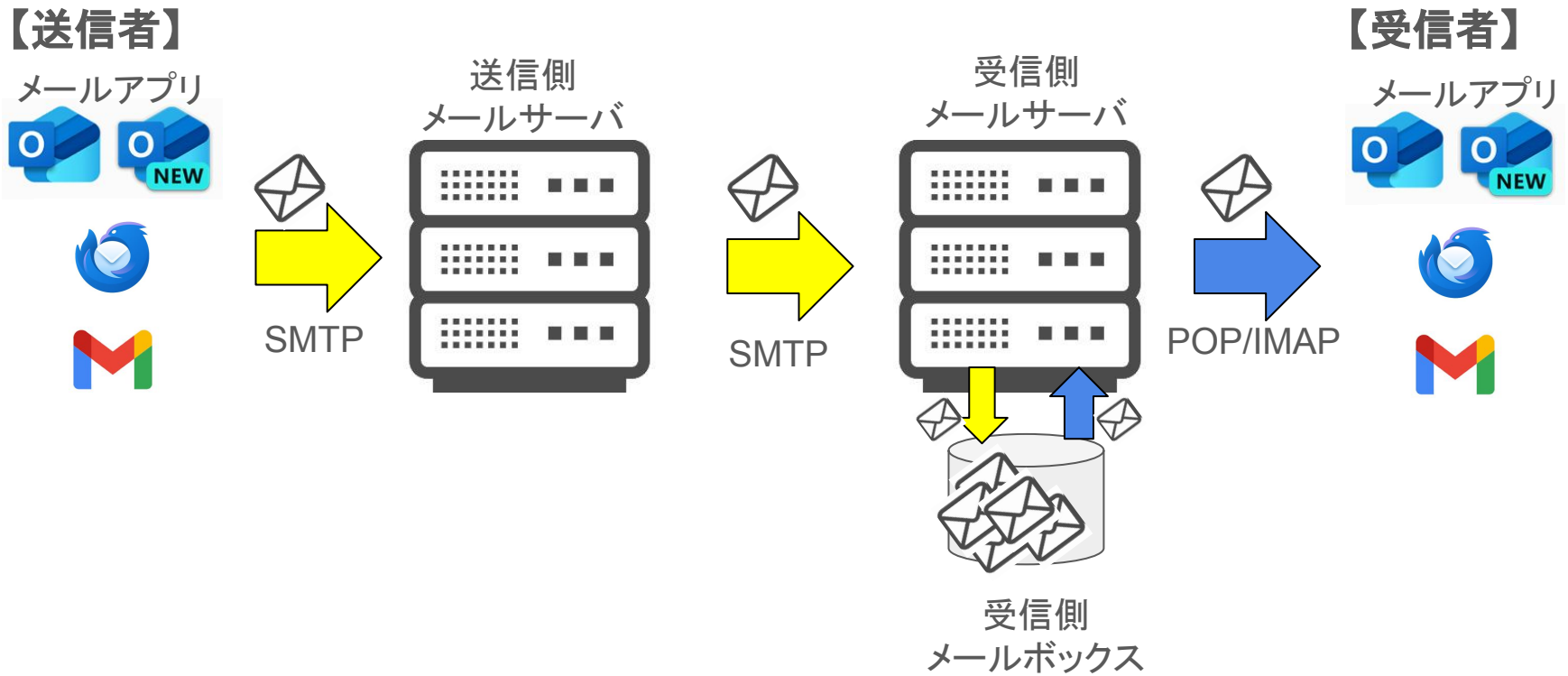
○実際やってみる

○SMTP、POP、IMAP

基本のメールプロトコル (通信方式)

- メールを送る
  - SMTP (Simple Mail Transfer Protocol）Port 25
- 届いたメールを取り込む
  - POP3 (Post Office Protocol ver3) Port 110
- メールボックスを操作する
  - IMAP4 (Internet Message Agent Protocol ver4) Port 143

○SMTP、POP、IMAPの基本的な関係



SMTPのポイント3つ

- SMTPの特徴はいろいろあるが、セキュリティという切り口で考えると

  - 認証の仕組みがない
  - 平文である
  - 差出人(From)、宛先(To)の書き方

○SMTP認証

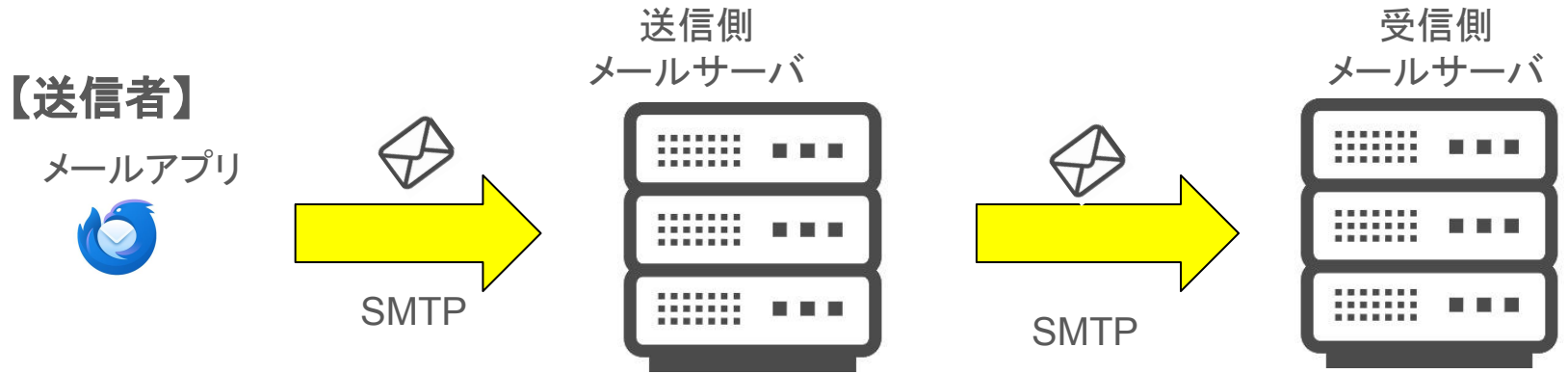
POP/IMAPにはあるが、SMTPは認証機構がない（誰でもメールが送信可能）

ID/Passwordを用いた認証を行ってメールを送信する方式が開発

＝**SMTP認証(SMTP Authentication、SMTP-Auth）**

利用Portは一般的に587番(SubmissionPort)を利用

SMTP認証の効果



○暗号化（overSSL）

基本的にSMTPでは平文テキストでデータを送受信する

途中の経路で第三者に盗聴される危険 ⇒ **暗号化**

ウェブのHTTPSなどと同じように、メールアプリとサーバ間で暗号化する方式

- **SMTP over SSL**
- **POP over SSL**
- **IMAP over SSL**

○暗号化（startTLS）

SMTP over SSLには以下の課題がある。

- SSL(TLS)に対応していない相手と通信できない
- （上記理由により）メールサーバ間で利用できない

SMTPセッション内で、暗号化に対応しているかどうかを事前に確認する仕組みが登場⇒
startTLS

- 暗号化で対応している相手とは暗号化通信
- 暗号化に対応していない相手とは平文通信

利用者からは、サーバ間通信が暗号化されているのかどうかはわからない

※gmailでは受信したメールが暗号化されて送信されたものかを確認できる

○暗号化 (エンドツーエンド暗号化)

overSSLもstartTLSも、ユーザ端末-サーバ間、あるいはサーバ-サーバ間の暗号化で、細切れに暗号・復号を繰り返している（＝平文になる瞬間がある）

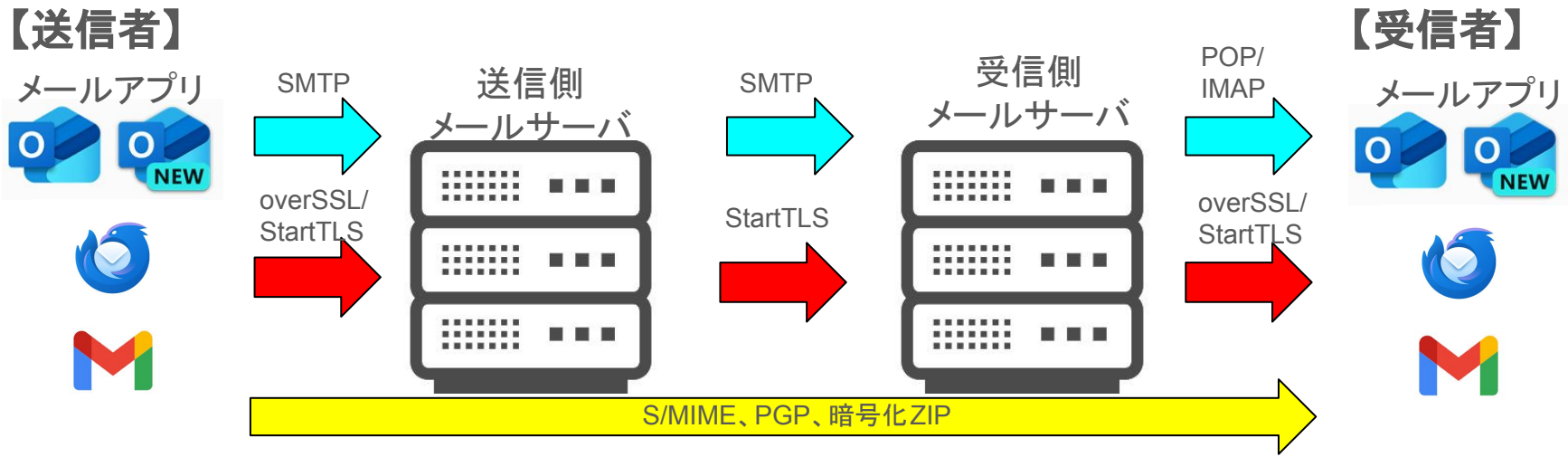
⇒送信者と受信者の間で一貫して暗号化できる方式として、S/MIME、PGP、暗号化zipなどがある

- 本日は**S/MIME（Secure/Multipurpose Internet Mail Extensions）**を紹介

やってること：メール本文の暗号化と電子署名（なりすましや改ざんの検出）

- エンド ツーエンドで暗号化が可能（サーバで復号化できない）
- 暗号化は本文のみで、やり取りの存在そのものは対象外
- 送受信者の間であらかじめ鍵のやり取りをしておく必要がある

○暗号化まとめ



- メールアプリには、overSSL/StartTLSを設定
- (商談相手など)特定の相手とはエンドツーエンドの暗号化を実施
  ※メールではなくクラウドストレージなどでの受け渡しでもいい

メール送信時に働くセキュリティ機構

○

最後に／実運用において

- 本日のセッションでは、メールの送受信時の様子を見ていただくことによってメール配送に関する理解を深めていただいた

- 実際の運用では、パケットを取得しての調査、解析は殆ど行わない（最後の手段に近い）
- 実際の運用では、エラーメールの確認、メールログの確認が状況把握・原因特定のための第１歩
- エラーメールやメールログを読んで、意味がわかるようになってほしい
  - 需要があれば別の機会に・・・