

salesforce

# Salesforce メールインテグレーションセキュリティガイド

Salesforce, Spring '24



本書の英語版と翻訳版で相違がある場合は英語版を優先するものとします。

© Copyright 2000–2024 Salesforce, Inc. All rights reserved. Salesforce およびその他の名称や商標は、Salesforce, Inc. の登録商標です。本ドキュメントに記載されたその他の商標は、各社に所有権があります。

# 目次

セキュリティガイドの概要	1
Outlook Integration	2
初回ユーザー認証ログインフロー	4
公開 EWS エンドポイントを使用する Outlook インテグレーション	6
設定要件	6
Web 版の Outlook の設定要件	7
添付ファイル付きメールの Salesforce フローへの記録	7
使用される API	9
Exchange Web サービス (EWS)	9
使用される EWS API	9
Gmail インテグレーション	11
設定要件	11
認証	11
Inbox ライセンスを使用する Outlook および Gmail インテグレーション	13
組織プロビジョニング	14
ネットワーク接続	14
Salesforce、Hyperforce、および Amazon Web Services (AWS) サーバーストレージ	16
Hyperforce データ保持	19
暗号化鍵管理	19
Inbox モバイルアプリケーションのデータストレージ	19
Inbox ライセンスを持つユーザーの後続のログイン	20
Gmail ガイドライン	21
Exchange Online (Office 365) ガイドライン	21
Microsoft Exchange 社内インスタンス	23
OAuth プロトコルについての詳細	23
Salesforce Hyperforce サーバー操作	25
モバイルデバイス管理とモバイルアプリケーション管理および Inbox	25
モバイルアプリケーションデータの削除	26



# セキュリティガイドの概要

Salesforce と Outlook および Gmail のインテグレーションにより、営業担当は作業を行う場所に関係なく、より効率的に販売を管理できます。SalesCloud では、Outlook および Gmail とのインテグレーションを無料で利用できません。

- ☑ **メモ:** 2023 年後半より、既存の Inbox のサービスとデータは Hyperforce に移行されます。Hyperforce は、パブリッククラウド用に構築された Salesforce クラウドネイティブインフラストラクチャアーキテクチャです。移行前は、一部の Inbox のサービスとデータはドイツまたは米国の Salesforce が管理するデータセンターに保存され、仮想プライベートクラウド (VPC) の背後にある Amazon Web Services (AWS) でホストされます。移行後は、Inbox のサービスとデータは Hyperforce 上に構築され、同じ地域内の新しい AWS のパブリッククラウドインフラストラクチャに保存されます。

このドキュメントでは、以下の技術およびセキュリティガイドラインについて説明します。

- Outlook および Gmail インテグレーション。
- Inbox ライセンスがあり、ユーザーに Inbox 権限が割り当てられている場合のデスクトップおよびモバイルソリューション。Inbox ライセンスは Sales Cloud Einstein と Sales Engagement でスタンドアロンライセンスとして使用できます。

Inbox ライセンスを追加すると、次の内容を実現できます。

- Outlook および Gmail インテグレーションでより多くの機能を使用できるようになり、Outlook や Gmail で作業しているときの営業担当の生産性が向上する。
- Lightning Experience のメールで厳選された Inbox 機能にアクセスできる。
- Inbox モバイルアプリケーションにアクセスできる。

設定手順、考慮事項、機能の詳細などの完全な情報は Salesforce ヘルプの「[Salesforce Inbox](#)」にあります。

Salesforce には、メールアカウントと Salesforce を統合する他の機能やソリューションが用意されており、Outlook および Gmail インテグレーションと Inbox 機能が補完されます。たとえば、Einstein 活動キャプチャや Lightning Sync を設定して、連絡先(取引先責任者)とカレンダーのイベント(行動)を Salesforce と同期します。また、Einstein 活動キャプチャで自動メールおよびイベント(行動)の記録を設定します。

セキュリティに関する考慮事項については、『[Einstein 活動キャプチャセキュリティガイド](#)』および『[Lightning Sync Design and Security Guide \(Lightning Sync の設計とセキュリティガイド\)](#)』を参照してください。

- ☑ **メモ:** Inbox ライセンスには、Einstein 活動キャプチャが含まれます。ただし、Einstein 活動キャプチャ機能を使用するかどうかに関係なく Inbox を有効にできます。また、Inbox を使用しても使用しなくても Einstein 活動キャプチャ機能を有効にできます。

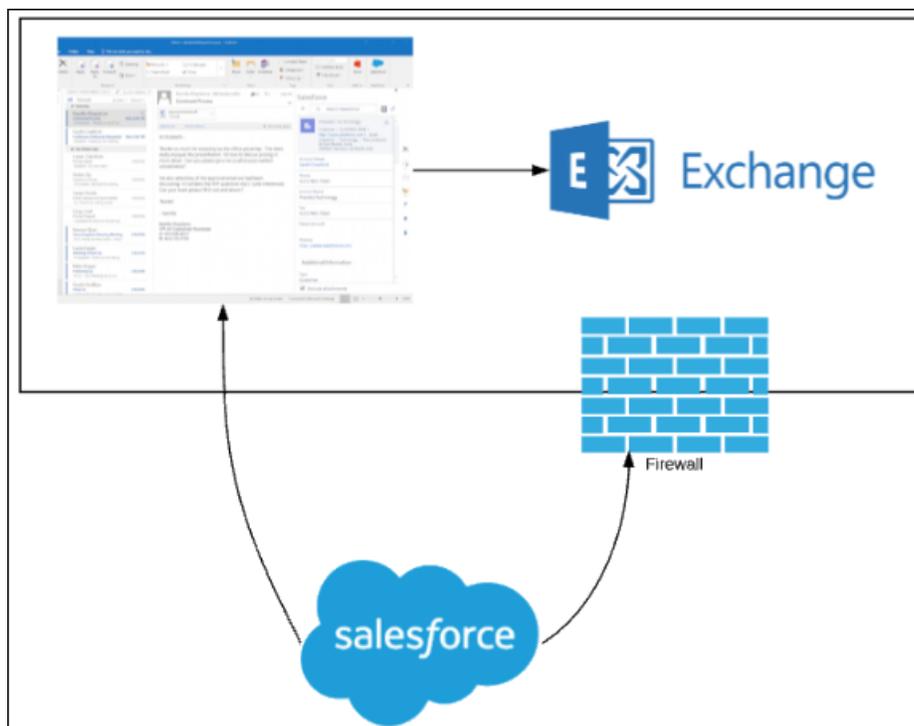
# Outlook Integration

Outlook インテグレーションに向けて適切に Exchange サーバーへのアクセス権を付与します。

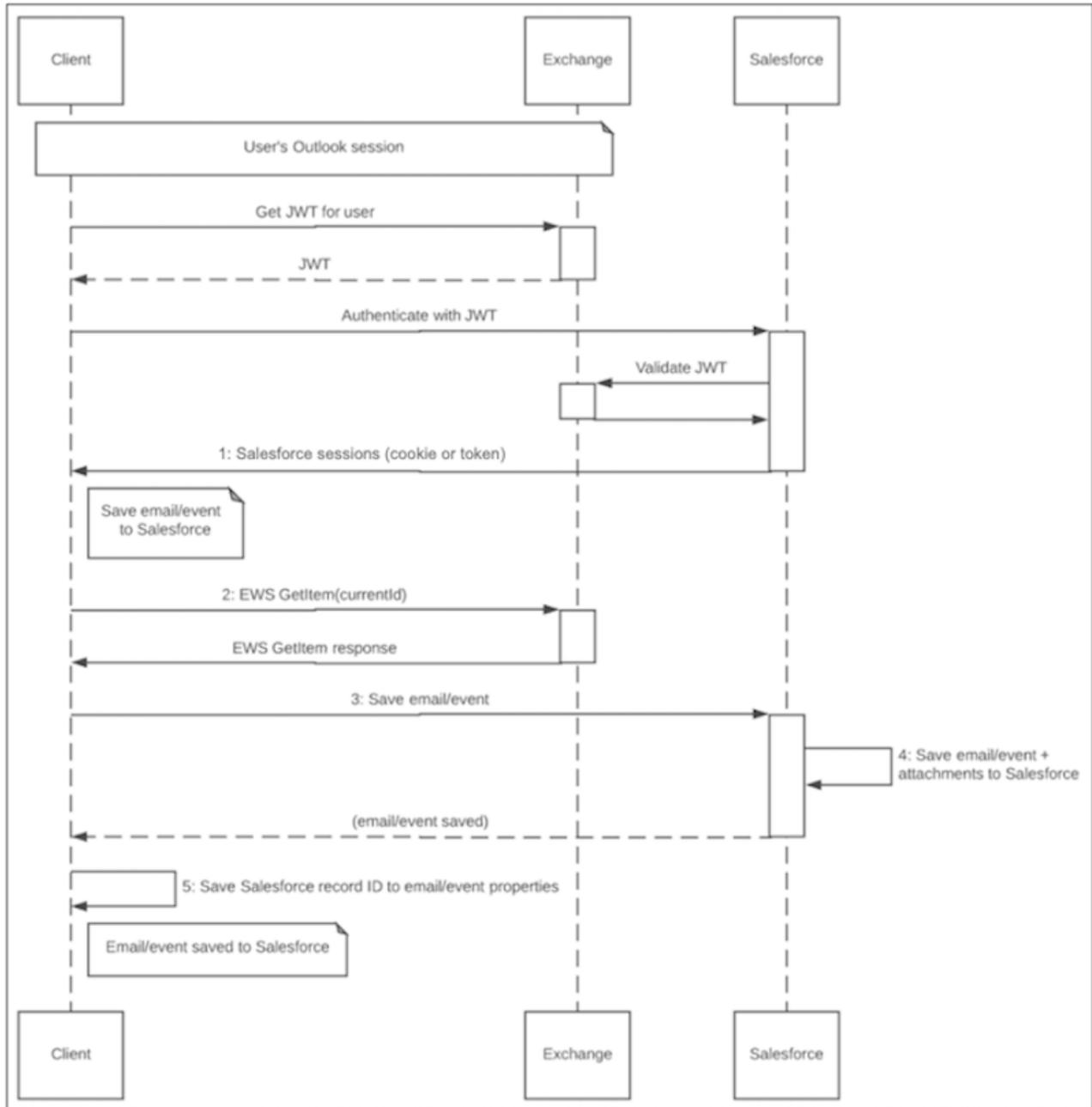
Outlook インテグレーションを設定するには、Exchange サーバーへのアクセス権が必要です。そのアクセス権を設定するための選択方法は、使用する Outlook のバージョン、社内のセキュリティポリシー、インテグレーション内で営業担当に必要な機能によって異なります。

Outlook インテグレーションアドインは、[Microsoft Office](#) アドインフレームワークに基づいて構築されています。そのフレームワーク内で特に Outlook から Salesforce へのメールを記録するというエンドユーザーアクションでは、Salesforce は Exchange サーバーに対してコールを実行する必要があります。

一般的な社内の Exchange 設定では、ファイアウォールでインターネットからのアクセスをブロックします。



Outlook インテグレーションでは Exchange API を利用して、Salesforce アプリケーションサーバーから Exchange Web サービス (EWS) コールを実行します。これまで、アドインコールは Exchange 自体で提供される URL と JSON Web トークン (JWT) を使用して EWS を介して実行されてきました。JWT コールでは、EWS エンドポイントを公開する必要がありました (古いバージョンの Exchange および Outlook では引き続き必要)。



最新バージョンの Outlook および Exchange の最近の機能強化により、歴史的な EWS サーバーコールを Outlook で提供される Office.js API のクライアントコールにすることができるようになりました。適切なバージョンの Outlook および Exchange では、EWS エンドポイントを公開することなく、Outlook インテグレーションのほぼすべての機能を使用できます。ただし、Outlook と Exchange 間のローカル EWS 接続や Exchange メタデータ URL は引き続き公開する必要があります。

Exchange および Outlook で JavaScript API v1.8 以降が実行されている場合は、EWS エンドポイントを公開することなく、標準の Outlook インテグレーション機能を使用できます。ただし、Outlook と Exchange 間のローカル EWS 接続や Exchange メタデータ URL は引き続き公開する必要があります。設定のこの変更は、Summer '21 からローリ

ング方式で既存のユーザーに適用されます。タイミングと対象資格についての詳細は、Salesforce アカウント担当者にお問い合わせください。

Exchange Online の最新のビルドでは、JavaScript API v1.8 以降が実行されます。Outlook クライアントで JavaScript API v1.8 以降が使用されているかどうかを確認するには、Microsoft ドキュメントの「[Outlook JavaScript API の要件セット](#)」を参照してください。

**❗ 重要:** Inbox ライセンスで使用できる機能 ([対応可能時間を挿入] や [後で送信] など) では、Outlook または Exchange API のバージョンに関係なく、Exchange サーバーへのアクセス権が必要になります。Inbox ライセンスがある場合は、「[公開 EWS エンドポイントを使用する Outlook インテグレーション](#)」(ページ 6)および「[Inbox ライセンスを使用する Outlook および Gmail インテグレーション](#)」(ページ 13)を参照してください。

Exchange サーバーまたは Outlook バージョンで JavaScript AP バージョン 1.4 ~ 1.7 がサポートされている場合でも、公開 EWS を使用せずに Exchange を設定することはできます。ただし、ユーザーは次の機能にアクセスできなくなります。

- Outlook から直接添付ファイルを記録する。ユーザーは Salesforce で記録済みのメールに添付ファイルを追加でき、Salesforce に記録されたメールやイベント (行動) の場合、[Salesforce に記録済み] と表示されます。
- Inbox 生産性機能。

### 初回ユーザー認証ログインフロー

Salesforce は Exchange に接続して、メタデータ URL でユーザーを認証します。これは、EWS とは異なる考慮事項です。

#### 公開 EWS エンドポイントを使用する Outlook インテグレーション

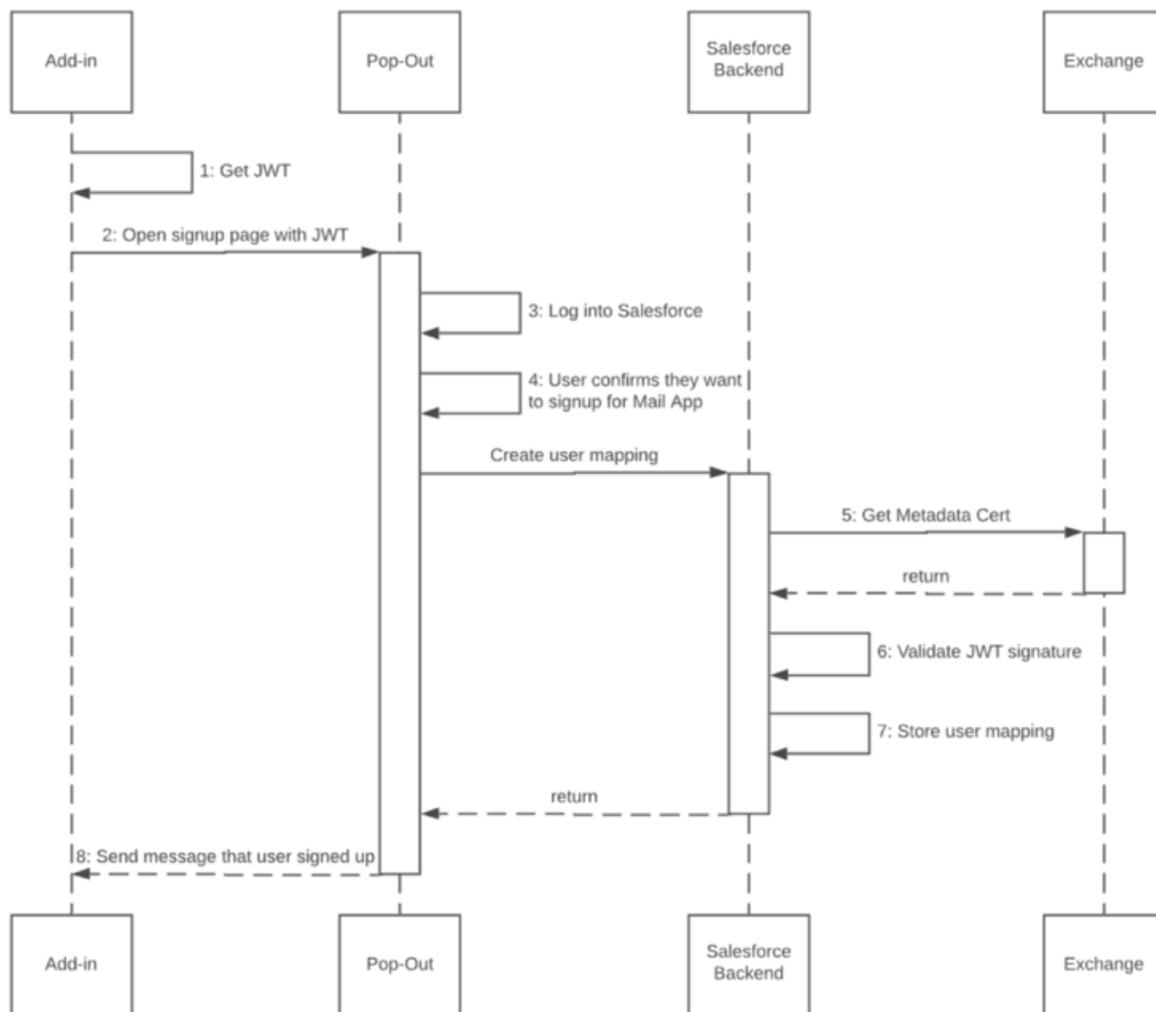
Outlook インテグレーションアドインでは、いくつかのシナリオで認証されたコールを使用します。

## 初回ユーザー認証ログインフロー

---

Salesforce は Exchange に接続して、メタデータ URL でユーザーを認証します。これは、EWS とは異なる考慮事項です。

次の図は、ユーザーが初めて Outlook インテグレーションアドインを読み込んだときに Exchange メールが対応する Salesforce ユーザーにどのように対応付けられるのかについての詳細なフローを示しています。このフローは、JavaScript API のバージョンに関係なく、すべてのバージョンの Outlook および Exchange に適用されます。



1. Outlook アドインは、簡単な JavaScript メソッドを使用して ID トークンを取得します。

```
Office.context.mailbox.getUserIdentityTokenAsync(callback, userContext);
```

JavaScript メソッドは、Exchange サーバーに対して Exchange ユーザー ID トークン (JSON Web トークンまたは JWT) を要求します。アドインは、Salesforce でホストされるウィンドウでサインアップページを開きます。

2. ユーザーは、Salesforce ログイン情報を使用して認証を行います。
3. Salesforce は、(ID トークンで指定された) ユーザーの Exchange アカウントを認証済み Salesforce ユーザーに接続するように求めます。
4. ユーザーはプロンプトをクリックし、サインインすることを確認します。
5. Salesforce サーバーは、Exchange トークンコンテンツを検証して、メタデータ URL の公開証明書を取得します。Salesforce では、EWS エンドポイントに有効な証明書が含まれていることが想定されています。サポートされている SSL 証明書については、[Salesforce ヘルプ](#)を参照してください。
6. Salesforce は、Exchange サーバーの認証メタデータドキュメントの公開署名鍵にアクセスして、ID トークン署名を検証します。

Exchange サーバーは、初めて JSON トークンをアドインに提供するときに以下を指定します。

- トークン自体のペイロード部分の Exchange メタデータエンドポイント URL
- Salesforce アドイン

アドインは、定義されたメタデータ URL に要求を送信して、署名を検証します。Exchange メタデータ URL は、ユーザーの ID トークンを検証できるように公開されている必要があります。

トークンの検証についての詳細は、[Microsoft ドキュメント](#)を参照してください。

7. その後、Exchange から Salesforce ユーザーへの対応付けは、ユーザーの Salesforce 組織データ内に保存されません。

## 公開 EWS エンドポイントを使用する Outlook インテグレーション

Outlook インテグレーションアドインでは、いくつかのシナリオで認証されたコールを使用します。

- Outlook バージョンで JavaScript API 1.7 以前が実行されている。「[Outlook JavaScript API の要件セット](#)」で、Outlook アプリケーションで実行される API のバージョンを確認します。
- [対応可能時間を挿入]、[後で送信]、[テキストショートカット]、[メール追跡]などの機能を有効にする Inbox ライセンスを追加している。これらの機能を使用するには、Exchange サーバーへのアクセス権が必要です。このガイドの「[Inbox ライセンスを使用する Outlook および Gmail インテグレーション](#)」(ページ 13)も確認してください。上記のセクションには、このセクションで説明されていないセキュリティと実装の考慮事項が記載されています。

- ❗ 重要:** これらのシナリオで公開 EWS エンドポイントがない場合、インテグレーションユーザーはインテグレーションから添付ファイルを記録したり、Inbox 生産性機能を使用したりできません。

### 設定要件

Outlook インテグレーションが正しく設定されていることを確認します。

#### Web 版の Outlook の設定要件

一部の設定は、営業担当が Web 版の Outlook で Salesforce インテグレーションを使用する場合に適用されません。

#### 添付ファイル付きメールの Salesforce フローへの記録

選択した Outlook メールメッセージと添付ファイルを手動で Salesforce に記録します。

#### 使用される API

API コールと Exchange Web サービス (EWS) コールについて説明します。

#### Exchange Web サービス (EWS)

Exchange Web サービス要求は正しい形式である必要があります。

#### 使用される EWS API

Exchange Web サービスコールについて詳しく説明します。

## 設定要件

Outlook インテグレーションが正しく設定されていることを確認します。

Outlook インテグレーションを設定するには、URL を公開する必要があります。

- 認証されていない HTTP アクセスを許可する Exchange メタデータ URL。 [「初回ユーザー認証ログインフロー」](#) (ページ 4) を参照してください。
- Exchange Web サービス URL

## Web 版の Outlook の設定要件

一部の設定は、営業担当が Web 版の Outlook で Salesforce インテグレーションを使用する場合に適用されます。

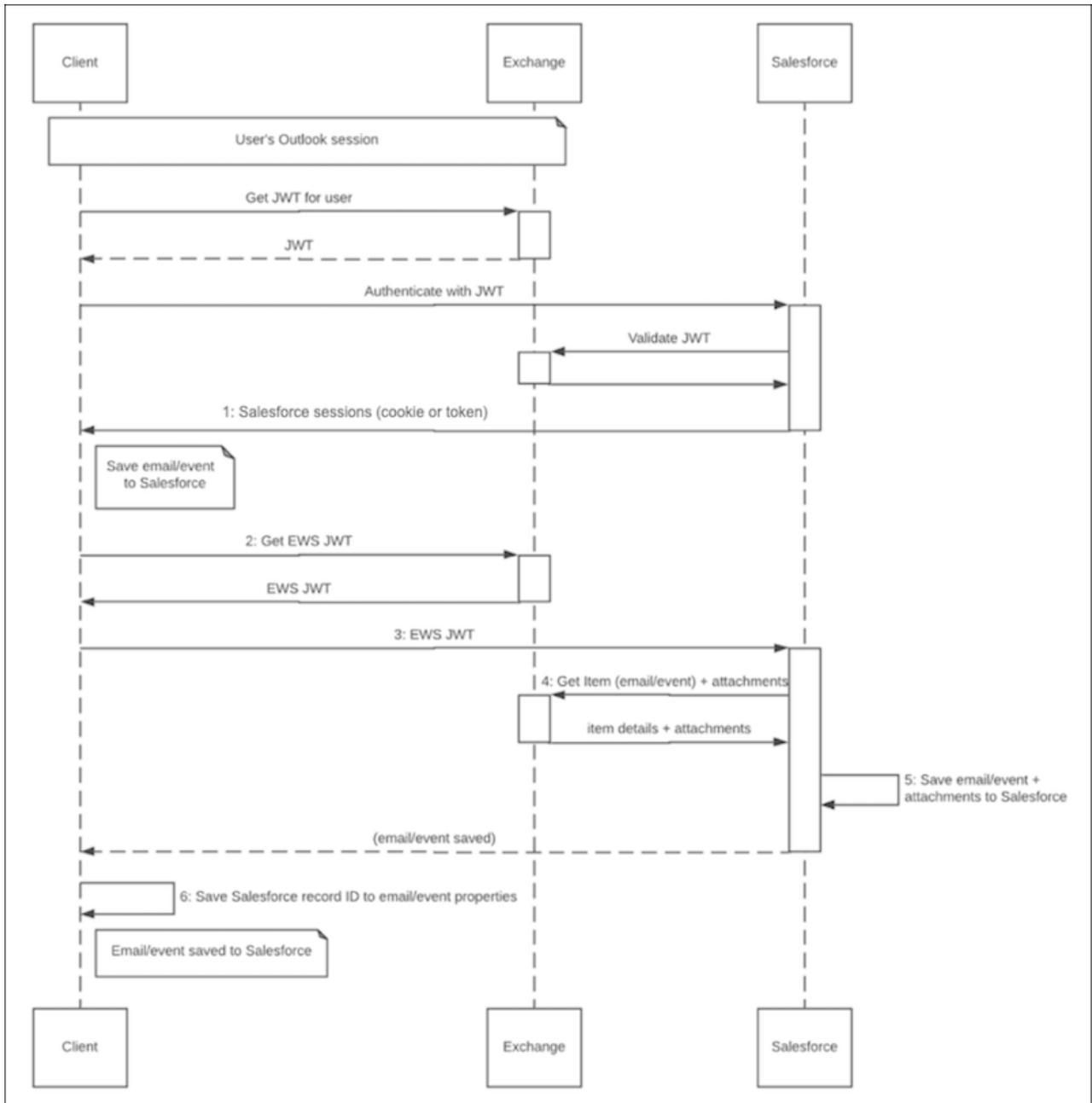
Salesforce は、Exchange エンドポイントに対して送信コールを実行するため、各エンドポイント URL には有効な SSL 証明書が必要です。 [Salesforce でサポートされるすべての SSL 証明書についての詳細をご確認ください](#)。

営業担当が Web 版の Outlook (Outlook Web App (OWA) とも呼ばれる) を使用する場合、Salesforce の [設定] の [Outlook インテグレーション] 設定でカスタム OWA URL (Office 365 以外の URL など) を指定します。Web 版の Outlook にアクセスする必要があるのはクライアントブラウザのみであるため、カスタム URL を公開する必要はありません。

## 添付ファイル付きメールの Salesforce フローへの記録

選択した Outlook メールメッセージと添付ファイルを手動で Salesforce に記録します。

Outlook インテグレーションから、ユーザーは選択した Outlook メールメッセージとその添付ファイルを手動で Salesforce に記録できます。アドインでは、次のフローを使用して記録を実行します。



1. Salesforce で認証します (詳細は、「ログインフロー」を参照)。
2. Outlook アドインに提供される API を介して、認証されたコールを Exchange Web サービス (EWS) に対して実行します。これで、記録する現在のメールまたはイベント (行動) を Salesforce サーバーで取得できます。 [Microsoft Office API ドキュメント](#) を参照してください。
3. 現在のメールまたはイベント (行動) とその添付ファイルに対して EWS 操作 EWS GetItem + GetAttachment(s) を実行します。
4. メールまたはイベント (行動) および添付ファイルを Salesforce に保存し、選択した Salesforce レコードに両方を関連付けます。

- Exchange オブジェクトの拡張プロパティに Salesforce レコード ID が含まれるように、Exchange のメールまたはイベントを変更します。

## 使用される API

API コールと Exchange Web サービス (EWS) コールについて説明します。

クライアント側 API コールは、Office.js およびサーバー EWS コールを介して実行されますが、GetItem 操作と GetAttachment 操作に制限されます。実行される EWS コールは、クライアント側と Salesforce アプリケーションサーバーから開始されます。これらのコールは、特定のメールまたはイベント(行動)のコンテキストで、ユーザーアクションによってトリガーされます。Salesforce アプリケーションサーバーから EWS URL へのコールは、公開された IP アドレス範囲から取得されます。

Outlook インテグレーションでは、メールまたはイベント(行動)とその添付ファイルを読み取ることできるように ReadWriteMailbox が指定されます。更新アクセスは、Office.js API で実行される EWS コールを介して Salesforce の ToDoID または行動ID を Exchange レコードに書き戻すためのものです。EWS コールを実行するための設定要件についての詳細は、Office.js ドキュメントを参照してください。

## Exchange Web サービス (EWS)

Exchange Web サービス要求は正しい形式である必要があります。

EWS 要求には、次の要素が含まれます。

- HTTP ヘッダー
  - 認証: (Office.js getCallbackTokenAsync からの) ベアラートークン
  - ユーザーエージェント: ExchangeServicesClient/0.0.0.0
- SOAP リクエストボディの XML

## 使用される EWS API

Exchange Web サービスコールについて詳しく説明します。

EWS を介して次のコールが実行されて、メールまたはイベント(行動)および添付ファイルが取得されます。また、Salesforce レコード ID が Exchange 項目のプロパティに書き込まれます。特定のコールについては、Microsoft ドキュメントのリンクをクリックしてください。

- [GetItem](#) (クライアント側とサーバー側): Salesforce レコードを保存するときに [AdditionalProperties](#) と現在のメールメッセージのコンテンツを取得および設定します。
- [GetAttachment](#) (サーバー側): Exchange から添付ファイルを取得し、(Salesforce メールメッセージ表現に関連付けられた) Salesforce レコードに追加します。
- [UpdateItem](#) (クライアント側)
- [GetFolder](#) (クライアント側): ドラフトフォルダーを取得します。
- [CreateItem](#) (クライアント側): ドラフトメッセージを作成するために使用します。

「クライアント側」は、Office.js API `makeEwsRequestAsync` を介して実行されるコールです。「サーバー側」は、Salesforce アプリケーションサーバーから EWS エンドポイントに対して実行されるコールです。これらのサーバー側コールでは、[getCallbackTokenAsync](#) の 5 分間のトークンが使用されます。

# Gmail インテグレーション

このセクションでは、Gmail インテグレーション Chrome 拡張機能で使用されるログイン認証と認証されたコールについて説明します。

メールインテグレーションにInboxが含まれる場合は、このガイドの「[Inbox ライセンスを使用する Outlook および Gmail インテグレーション](#)」セクションも参照してください。

## 設定要件

Gmail とのインテグレーションを行う前に、システムが次の要件を満たしていることを確認します。

## 認証

Salesforce が Gmail インテグレーションで使用する認証方法について説明します。

## 設定要件

---

Gmail とのインテグレーションを行う前に、システムが次の要件を満たしていることを確認します。

Gmail とのインテグレーションを設定するには、Salesforce ヘルプの「[Gmail とのインテグレーションの設定](#)」でシステム要件およびその他の考慮事項を確認してください。

## 認証

---

Salesforce が Gmail インテグレーションで使用する認証方法について説明します。

## OAuth 2.0

Salesforce では、OAuth 2.0 プロトコルを使用して、ユーザーの Google アカウントに接続します。Salesforce サーバーは、Google に対して要求を実行するための OAuth 更新トークンとアクセストークンを取得および保存します。このトークンは、そのユーザーの Gmail アカウントへのアクセス権を提供するシングルユーザートークンです。このトークンは、Chrome 拡張機能で直接使用されません。これは、接続された Salesforce 組織内に保存され、顧客データとして処理されます。

## 認証プロバイダー

Gmail インテグレーションでは、Salesforce プラットフォーム機能の認証プロバイダーを使用して、Google アクセストークンを保存および管理します。認証プロバイダーを使用すると、Apex でアクセストークンを取得して更新できます。詳細は、Salesforce ヘルプの「[認証プロバイダー](#)」を参照してください

## Gmail と Salesforce の接続の維持

Google を使用したログインを維持するには、Salesforce の [設定] の [Gmail インテグレーションおよび同期] ページにある [Gmail と Salesforce の接続を維持] 設定を有効にします。この設定により、ユーザーは Google ID に基づいて Salesforce セッションを取得できます。Salesforce セッションは、Salesforce 内で設定された有効期限や他のルール (使用できる IP 範囲など) に従います。Salesforce セッションの有効期限が切れた場合、ユーザーは Google ID に基づいて新しいセッションを確立できます。この設定では、ユーザーのブラウザで Google アカウントにログインする必要があります。この設定が無効になっている場合、ユーザーは Salesforce Desktop と同じ方法でログインします。システム管理者によって制御されるセッションと同じルールが適用されます。Salesforce セッションの有効期限が切れた場合、ユーザーは再度ログインする必要があります。

# Inbox ライセンスを使用する Outlook および Gmail インテグレーション

Inbox ライセンスを追加すると、Outlook および Gmail インテグレーション内で営業担当の生産性を向上させる機能を使用できるようになります。また、営業担当は Lightning Experience のメールでより多くの機能にアクセスしたり、Inbox モバイルアプリケーションにアクセスしたりできます。

**重要:** この章の内容は、Salesforce Inbox がある場合にのみ適用されます。Inbox ライセンスがない場合や、Inbox 権限が割り当てられているユーザーがいない場合、この章をスキップできます。

この章では、Inbox ライセンスがあり、ユーザーに Inbox 権限が割り当てられている場合の接続、データストレージ、データ保持の詳細について説明します。

## 組織プロビジョニング

Inbox データが保存される場所について説明します。

## ネットワーク接続

Salesforce と接続アプリケーション間のネットワークコールについて説明します。

## Salesforce、Hyperforce、および Amazon Web Services (AWS) サーバーストレージ

Inbox ライセンスが有効になっていると、サーバーおよびデータベースは Hyperforce でホストされ、Amazon Web Services (AWS) などのパブリッククラウドインフラストラクチャで構築されます。

## Hyperforce データ保持

Inbox では、一部のデータが Salesforce Hyperforce インフラストラクチャを使用して保存されます。

## 暗号化鍵管理

デフォルトでは、Salesforce はクラウドプロバイダーが提供する機能を使用して、Hyperforce の保存時の顧客データをすべてインフラストラクチャレイヤーで暗号化します。

## Inbox モバイルアプリケーションのデータストレージ

Inbox モバイルアプリケーションで保存される情報を確認します。

## Inbox ライセンスを持つユーザーの後続のログイン

OAuth アクセストークンと更新トークンを使用してユーザーログインを管理します。

## Gmail ガイドライン

Gmail アカウントに接続するときは、次の考慮事項を念頭に置いてください。

## Exchange Online (Office 365) ガイドライン

Exchange Online (Office 365) の認証ガイドラインを確認します。

## Microsoft Exchange 社内インスタンス

社内の Microsoft Exchange インスタンスには、考慮すべき重要な要件があります。

## OAuth プロトコルについての詳細

Salesforce では OAuth 2.0 認証フレームワークを使用して外部サービスに接続します。

## Salesforce Hyperforce サーバー操作

Salesforce Hyperforce インフラストラクチャには Inbox データが保存され、さまざまな操作が実行されます。

### モバイルデバイス管理とモバイルアプリケーション管理および Inbox

Inbox モバイルアプリケーションでは、モバイルデバイス管理(MDM)とモバイルアプリケーション管理(MAM)が制限付きでサポートされます。

### モバイルアプリケーションデータの削除

Salesforce システム管理者は、いつでも特定のユーザーの Salesforce または Salesforce Inbox ライセンスを削除できます。

## 組織プロビジョニング

Inbox データが保存される場所について説明します。

**メモ:** Hyperforce は Salesforce インフラストラクチャアーキテクチャであり、Amazon Web Services (AWS) などのパブリッククラウドプロバイダーで使用するために構築されています。Hyperforce は、Salesforce プラットフォームおよびアプリケーションを迅速かつ確実に世界中の場所に配信できるように、ハードウェアではなくコードで構成されています。Salesforce アプリケーションにコンプライアンス、セキュリティ、プライバシー、俊敏性、スケーラビリティを提供し、お客様にデータレジデンシーに関するより多くの選択肢や制御を提供します。

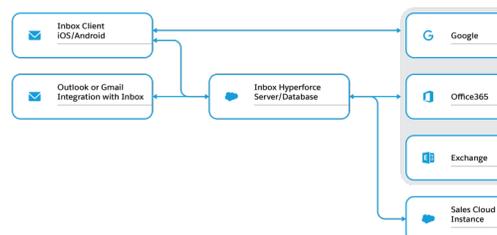
Salesforce 組織で Inbox が有効になると、Salesforce の Hyperforce サーバー上に対応する組織が作成されます。ユーザーに Inbox を使用してメールボックスを Salesforce に接続する権限がある場合、メールボックスは Hyperforce に接続されます。この接続により、Salesforce Hyperforce サーバーは、Google、Microsoft Exchange、または Office 365 に対してネットワークコールを実行するように求められます。Hyperforce データセンター内でアプリケーションは、関連するデータを関連するユーザーに提供するために鍵と ID を使用します。

Inbox で使用する Einstein プラットフォームのセキュリティとアーキテクチャについての詳細は、[Einstein プラットフォームの信頼とコンプライアンスに関するドキュメント](#)を参照してください。

## ネットワーク接続

Salesforce と接続アプリケーション間のネットワークコールについて説明します。

Inbox モバイルアプリケーションおよびデスクトップクライアントは、Salesforce Hyperforce サーバーに対してネットワークコールを実行します。その後、サーバーが Microsoft Exchange、Office 365、Google に対して直接ネットワークコールを実行します。



Inbox ライセンスを使用する Outlook および Gmail インテグレーションから Salesforce Hyperforce サーバー AES-128 暗号化を使用する HTTPS TLS 1.2 接続。この接続は、ログインと Inbox 固有のタスクの実行で使用されます。

**Salesforce Hyperforce サーバーから Google**

AES-256 暗号化を使用する HTTPS TLS 1.2 接続。この接続では、Gmail API プロトコルと OAuth 2.0 認証が使用されます。

**Salesforce Hyperforce サーバーから Office 365 (Exchange Online)**

AES-256 暗号化を使用する HTTPS TLS 1.2 接続。この接続では、EWS プロトコルと OAuth 2.0 認証が使用されます。

**Salesforce Hyperforce サーバーから社内の Exchange (2019、2016、2013)**

HTTPS TLS 1.2 接続 (Exchange サーバーが TLS バージョンおよび暗号化を決定)。この接続では、EWS プロトコルと、ユーザー名およびパスワードによる基本認証が使用されます。IP または VPN によって EWS エンドポイントが制限されている場合、アドレスの許可リストに次のアドレスを追加します。

**ⓘ 重要:** Hyperforce への移行前は、一部のデータが仮想プライベートクラウド (VPC) の背後にある AWS サーバーおよびデータベースに保存されます。Inbox のサービスやデータへのアクセスが中断されないように、両方の IP アドレスのセットを許可リストに追加してください。

	Salesforce インスタンスがヨーロッパ外にある場合	Salesforce インスタンスがヨーロッパ内にある場合
Hyperforce	<ul style="list-style-type: none"> <li>• 44.242.15.232</li> <li>• 44.236.183.129</li> <li>• 100.21.196.196</li> <li>• 54.200.249.136</li> <li>• 44.228.8.56</li> <li>• 35.165.2.200</li> </ul>	<ul style="list-style-type: none"> <li>• 18.158.21.76</li> <li>• 3.76.67.243</li> <li>• 18.158.241.92</li> <li>• 3.76.75.66</li> <li>• 52.57.103.81</li> <li>• 3.72.121.255</li> </ul>
Hyperforce への移行前	<ul style="list-style-type: none"> <li>• 54.200.130.205</li> <li>• 54.218.59.121</li> <li>• 34.210.91.105</li> <li>• 34.210.91.103</li> <li>• 44.224.62.36</li> <li>• 52.35.129.120</li> <li>• 54.71.145.62</li> <li>• 35.166.120.106</li> <li>• 44.224.71.98</li> <li>• 52.35.232.62</li> <li>• 54.68.117.123</li> <li>• 52.26.6.102</li> <li>• 35.163.187.73</li> <li>• 52.36.92.175</li> <li>• 34.210.91.106</li> <li>• 34.210.91.104</li> <li>• 35.166.17.212</li> </ul>	<ul style="list-style-type: none"> <li>• 52.59.28.245</li> <li>• 52.28.30.206</li> <li>• 52.57.191.228</li> <li>• 18.194.116.65</li> <li>• 52.57.191.229</li> <li>• 18.184.19.133</li> <li>• 52.57.191.226</li> <li>• 52.57.191.224</li> <li>• 52.57.191.227</li> <li>• 18.197.233.154</li> <li>• 18.196.51.181</li> <li>• 3.124.138.13</li> <li>• 3.124.208.146</li> <li>• 3.124.224.62</li> <li>• 3.124.238.55</li> </ul>

	Salesforce インスタンスがヨーロッパ外にある場合	Salesforce インスタンスがヨーロッパ内にある場合
	<ul style="list-style-type: none"> <li>34.216.184.173</li> <li>34.210.91.108</li> <li>34.210.91.107</li> </ul>	

EWS または Inbox に固有でない Salesforce IP アドレスについては、こちらの[ナレッジ記事](#)を参照してください。

Exchange の発信接続の制限がある場合、表で示すとおりに発信アクセスを許可してください。その後、Exchange に新しいメールとイベント (行動) が届くと、プッシュ通知が Salesforce に送信されます。Einstein 活動キャプチャのサービスやデータへのアクセスが中断されないように、両方の Web フックエンドポイントのセットを組織に追加してください。

	Salesforce インスタンスがヨーロッパ外にある場合	Salesforce インスタンスがヨーロッパ内にある場合
Hyperforce	apiq-ews-webhook-c01.sfdc-lywfpd.svc.sfdcfc.net	apiq-ews-webhook-c01.sfdc-yzvd4.svc.sfdcfc.net
Hyperforce への移行前	ews-webhook-us1-prod.salesforceiq.com	ews-webhook-eu1-prod.salesforceiq.com

### iOS および Android Inbox アプリケーションから Google

AES-256 暗号化を使用する HTTPS TLS 1.2 接続。この接続では、Gmail API プロトコルと OAuth 2.0 認証が使用されます。

### iOS および Android Inbox アプリケーションから Office 365 (Exchange Online)

AES-256 暗号化を使用する HTTPS TLS 1.2 接続。この接続では、Exchange ActiveSync (EAS) または Office 365 API プロトコルが使用されます (それぞれで OAuth 2.0 認証が使用される)。

### iOS および Android Inbox アプリケーションから社内の Exchange (2019、2016、2013)

HTTPS TLS 1.2 接続。Exchange サーバーが TLS バージョンおよび暗号化を決定します。この接続では、Exchange ActiveSync (EAS) プロトコルと、ユーザー名およびパスワードによる基本認証が使用されます。

## Salesforce、Hyperforce、および Amazon Web Services (AWS) サーバーストレージ

Inbox ライセンスが有効になっていると、サーバーおよびデータベースは Hyperforce でホストされ、Amazon Web Services (AWS) などのパブリッククラウドインフラストラクチャで構築されます。

**重要:** Inbox ライセンスには、Einstein 活動キャプチャが付属しています。ただし、Einstein 活動キャプチャ機能を有効にするかどうかに関係なく Inbox を有効にできます。両方の機能で同じデータが使用されるため、Einstein 活動キャプチャが有効になっているかどうかに関係なく、データは Hyperforce に保存されません。

どのデータが取得されて保存され、そのデータがどのように使用されるかの詳細を確認します。

Hyperforce によって取得および保 存される内容	追加の詳細	データの使用方法
カレンダーのイベント (行動)	<p>カレンダーのイベント (行動)には、ユーザーの接続済みMicrosoft アカウントまたは Google アカウントから取得されたすべてのイベント (行動) データが含まれます。イベント (行動) の添付ファイルは含まれません。</p>	<p>Einstein 活動キャプチャではこのデータを使用して Salesforce カレンダーの活動タイムラインに行動が表示されます。</p> <p>Inbox では [対応可能時間を挿入] 機能と [推奨コネクション] 機能にこのデータが使用されます。</p>
取引先責任者の詳細	<p>詳細には、連絡先(取引先責任者)のプロファイル画面 (Gmail、Exchange、Sales Cloud) に表示されるデータから取得された取引先責任者データが含まれます。</p>	<p>取引先責任者データは他の Salesforce 機能 (Einstein メールインサイトなど) で使用されます。</p>
メールアカウント	<p>情報には、メールアドレス、サーバー、ドメインなど、ユーザーの接続済みMicrosoft アカウントまたは Google アカウントに関する詳細が含まれます。</p>	<p>Einstein 活動キャプチャと Inbox では、このデータを使用してユーザーのメールアカウントが Salesforce に接続されます。</p>
メールの添付ファイル	<p>メールの添付ファイルのメタデータが含まれます。Einstein 活動キャプチャの場合、添付ファイル自体は保存されず、活動タイムラインにも表示されません。</p> <p>Inbox の場合、[後で送信] 機能を使用するとメールが送信されるまで添付ファイルが保存されます。</p> <p>Inbox のメール送信アクション中、Google サーバーまたは Exchange サーバーにメールメッセージ ID を渡して添付ファイルをメールの添付ファイルとして動的に取得できます。</p>	<p>現在、Einstein 活動キャプチャでは添付ファイルメタデータは使用されていません。</p> <p>Inbox では添付ファイルとメタデータは [後で送信] 機能に使用されます。</p>
メールヘッダーとメタデータ	<p>メールメッセージはユーザーの接続済み Microsoft アカウントまたは Google アカウントから取得されます。保存されるメール要素には、件名、送信者、宛先、CC、送信日が含まれます。</p>	<p>Einstein 活動キャプチャではこのデータを使用して Salesforce の関連レコードの活動タイムラインにメールが追加されます。</p> <p>Inbox と Einstein 活動キャプチャで使用可能なメールインサイトでは、このデータを使用して分類が作成されます。</p>

Hyperforce によって取得および保 存される内容	追加の詳細	データの使用方法
		Inbox と Einstein 活動キャプチャで使用可能な推奨コネクションでは、このデータを使用して提案が生成されます。
メール HTML 本文		Einstein 活動キャプチャではこのデータを使用して Salesforce にメールが表示されます。また、このデータはメールインサイトの生成にも使用されます。
パスワードと OAuth トークン	<p>OAuth の更新トークンとアクセストークンは、ユーザーの Google アカウントまたは Microsoft アカウントを Salesforce に接続するために使用されます。</p> <p>ユーザーが OAuth 2.0 を使用してアカウントを Salesforce に接続すると、ユーザーのパスワードは保存されません。そのため、アカウントを Salesforce に接続した後にユーザーがメールのパスワードを変更しても Google または Microsoft に対して再認証する必要はありません。</p> <p>ユーザーがオンプレミスの Exchange メールアカウントを使用していて、パスワード認証が使用されている場合は、ユーザーのパスワードが保存されます。</p>	
Salesforce レコード	<p>レコードには、取引先責任者、リード、商談などのレコードのメタデータ、権限、項目、ページレイアウトなども含まれます。</p> <p>Inbox では、レコードのメタデータが最大24時間保存されます。Einstein 活動キャプチャでは、Salesforce のデータを削除するまで、レコードのメタデータが保存されます。</p> <p>Salesforce のレコードデータを削除すると、そのデータは Hyperforce サーバーからも削除されます。</p>	<p>Inbox モバイルアプリケーションでは、このデータを使用して、メールや行動に関連するレコードを参照するときのパフォーマンスが改善されます。</p> <p>メールに関連する Salesforce レコードに関連付けるため、Einstein 活動キャプチャでは、取引先責任者レコードやリードレコードからメールアドレスがコピーされて Hyperforce サーバーに保存されます。</p>

Hyperforce によって取得および保 存される内容	追加の詳細	データの使用方法
ユーザーの設定	ユーザーの設定には、Inbox または Einstein 活動キャプチャから取得されるユーザーの個人設定が含まれます。	

## Hyperforce データ保持

Inbox では、一部のデータが Salesforce Hyperforce インフラストラクチャを使用して保存されます。

新しいメールアカウントが接続されると、Salesforce Hyperforce サーバーは過去 6 か月または 180 日分のメールメッセージをダウンロードします。それ以降、サーバーは Gmail、Exchange、または Office 365 の通知登録を使用して、新しいメールメッセージのダウンロードをトリガーします。デフォルトでは、メールメッセージは 2 年間保持されてから削除されます。保持期間は、30 日～5 年に設定できます。

## 暗号化鍵管理

デフォルトでは、Salesforce はクラウドプロバイダーが提供する機能を使用して、Hyperforce の保存時の顧客データをすべてインフラストラクチャレイヤーで暗号化します。

すべてのデータは保存時と移行時に暗号化され、Salesforce がデータを暗号化するための鍵を所有します。Hyperforce 鍵は組織固有ではありません。

データベースのメールメタデータとカレンダーデータは、ディスクレベルの暗号化を使用して暗号化されません。

## Inbox モバイルアプリケーションのデータストレージ

Inbox モバイルアプリケーションで保存される情報を確認します。

対象	詳細
Inbox ユーザー設定	<p>個人ユーザー設定は、デバイスの SQLite データベースとアプリケーション設定に保存されます。</p> <ul style="list-style-type: none"> <li>• iOS の NSUserDefaults</li> <li>• Android の SharedPreferences</li> </ul> <p>次のようなユーザー設定が保存されます。</p> <ul style="list-style-type: none"> <li>• Salesforce 設定 (応答画面でメール記録を要求)</li> <li>• ユーザーが設定した作業時間</li> <li>• メール設定 (スワイプ方向、メッセージに表示される行数、スレッドによる整理、バッジ数種別など)</li> </ul>

対象	詳細
	<ul style="list-style-type: none"> <li>• カレンダー設定 (不参加や表示される日数など)</li> </ul>
メールメッセージ	Inbox モバイルアプリケーションは、最近のメールメッセージ (メール本文を含む) を保存します。メールメッセージは、SQLite データベースに保存されます。iOS の場合、データベースは AES-256 暗号化を使用する SQLCipher で暗号化されます。Android の場合、データベースは暗号化されません。
行動	Inbox モバイルアプリケーションは、カレンダーのイベント (行動) を SQLite データベースに保存します。iOS の場合、データベースは AES-256 暗号化を使用する SQLCipher で暗号化されます。Android の場合、カレンダーのイベント (行動) はデフォルトの共有カレンダープロバイダストレージに保存されます。カレンダーについての詳細は、 <a href="#">Android 開発者向けドキュメント</a> を参照してください。
パスワードと OAuth トークン	メールやカレンダーのイベント (行動) を Google、Office 365、Exchange から直接取得するために、Inbox モバイルアプリケーションは Google および Office 365 の OAuth アクセストークンを保存します。また、Exchange のパスワードも保存します。これらのトークンやパスワードは、iOS キーチェーンまたは Android アカウントマネージャー (それぞれのデバイスのデフォルトの暗号化領域) に保存されます。
iOS キーチェーン	<a href="#">キーチェーンサービスの概念</a> については、Apple 開発者向けガイドを参照してください。
Android アカウントマネージャー	<a href="#">アカウントマネージャープロバイダー</a> については、Android 開発者向けガイドを参照してください。

## Inbox ライセンスを持つユーザーの後続のログイン

OAuth アクセストークンと更新トークンを使用してユーザーログインを管理します。

初回ログイン後、Inbox ライセンスを持つユーザーは、引き続き認証を行って、メールボックスを Salesforce Hyperforce サーバーに接続します。この認証により、Salesforce に対して要求を実行するための OAuth 更新トークンとアクセストークンが取得および保存されます。このトークンは、ユーザーの Salesforce アカウントに関連付けられます。

OAuth 更新トークンおよびアクセストークンは、Salesforce Hyperforce サーバーに保存されます。接続されると、API コールが実行されて、OAuth アクセストークンが取得されます。デフォルトでは、アクセストークンの有効期限は 1 時間で切れます。Salesforce システム管理者は、有効期限を設定できます。たとえば、システム管理者は 7 日ごとに有効期限が切れるように OAuth 更新トークンを設定できます。

デフォルトのトークンの有効期限を変更するには、Salesforce の [設定] から、[クイック検索] ボックスに「[接続アプリケーション](#)」と入力し、[\[接続アプリケーションを管理する\]](#)を選択します。次に、[\[SalesforceIQ\]>\[編集\]>\[更新トークンポリシー\]](#)を選択します。

ユーザーの Salesforce パスワードは、Outlook インテグレーション、Gmail インテグレーション、または Salesforce Hyperforce サーバーに保存されません。Salesforce Hyperforce サーバーで認証するための個別のトークンが取得されます。このトークンは、HTTPS 認証ヘッダーに渡される個別のベアラートークンです。

Salesforce Hyperforce サーバーに対するネットワークコールは、すべて TLS 1.2 を介して実行されます。

Salesforce システム管理者は、いつでも OAuth アクセスをブロックできます。Salesforce の [設定] から、[クイック検索] ボックスに「接続アプリケーション」と入力し、[接続アプリケーションの OAuth の利用状況] を選択します。

個人ユーザーは、各自の Salesforce OAuth トークンを取り消すことができます。Salesforce システム管理者も、任意のユーザーの OAuth トークンを取り消すことができます。OAuth トークンは、個人設定の [接続] に表示されます。

## Gmail ガイドライン

---

Gmail アカウントに接続するときは、次の考慮事項を念頭に置いてください。

ユーザーに Inbox ライセンスがある場合、Inbox インテグレーションでは、OAuth 2.0 プロトコルを使用して Gmail アカウントを接続します。Chrome 拡張機能およびモバイルアプリケーションは、Salesforce アカウントにログインするためのページを開きます。この初回ログインが完了すると、Salesforce Hyperforce サーバーは、Google に対して要求を実行するための OAuth 更新トークンとアクセストークンを取得および保存します。このトークンは、そのユーザーの Gmail アカウントへのアクセス権を提供するシングルユーザートークンです。Chrome 拡張機能および Salesforce Hyperforce サーバーは、ユーザーの Google パスワードを使用したり保存したりしません。

Inbox モバイルアプリケーションはメールアプリケーションとカレンダーアプリケーションで構成されるため、Google メールとカレンダーに対する参照および更新のフルアクセス権が必要です。また、Google ドライブからメールへのファイル添付をサポートするには、Google ドライブに対する参照のみのアクセス権も必要になります。Inbox モバイルアプリケーションでは、次の Google OAuth 権限が必要です。

- <https://mail.google.com/>
- <https://www.google.com/m8/feeds/>
- <https://www.googleapis.com/auth/userinfo.profile>
- <https://www.googleapis.com/auth/userinfo.email>
- <https://www.googleapis.com/auth/calendar>
- <https://www.googleapis.com/auth/drive.readonly>

ユーザーは、Google アカウントユーザー設定でサードパーティアプリケーションに移動して、いつでも Google OAuth トークンを取り消すことができます。サードパーティアプリケーションの削除についての詳細は、[Google ヘルプ](#)を参照してください。

Google に対するネットワークコールは、すべて TLS 1.2 AES-256 暗号化を使用して実行されます。Inbox では、Google の 2 つのプロトコルが使用されます。

- [Gmail API](#)
- [Google カレンダー API](#)

## Exchange Online (Office 365) ガイドライン

---

Exchange Online (Office 365) の認証ガイドラインを確認します。

ユーザーに Inbox ライセンスがある場合、Outlook インテグレーションでは、このガイドに記載されている OAuth 2.0 プロトコルを使用して Office 365 アカウントを接続します。Outlook アドインおよびモバイルアプリケーション

ンは、Salesforce アカウントにログインするためのページを開きます。この初回ログインが完了すると、Salesforce Hyperforce サーバーは Office 365 に対して要求を実行するための OAuth 更新トークンとアクセストークンを取得および保存します。このトークンは、そのユーザーの Office 365 アカウントへのアクセス権を提供するシングルユーザートークンです。Salesforce は、ユーザーの Office 365 パスワードを使用または保存しません。

Inbox モバイルアプリケーションは、メールアプリケーションとカレンダーアプリケーションであるため、Office 365 メールとカレンダーに対する参照および更新のフルアクセス権が必要です。Inbox モバイルアプリケーションでは、次の Office 365 権限が必要です。

- 特定のユーザーとしてメールを送信する
- ユーザーのカレンダーを参照および更新する
- ユーザーの連絡先を参照および更新する
- ユーザーのプロファイルを参照する
- EWS を介してログイン済みユーザーとしてメールボックスにアクセスする
- ユーザーのメールを参照および更新する

ユーザーは、いつでも Office 365 OAuth トークンを取り消すことができます。Office 365 に移動し、[マイアカウント]と[アプリの権限]を選択します。

Microsoft Azure システム管理者は、[Microsoft Azure Active Directory](#) で、Office 365 OAuth 更新トークンの有効期限を MaxAgeSingleFactor および MaxAgeMultiFactor に設定して変更できます。

Outlook アドインまたは Inbox モバイルアプリケーションと Office 365 間のネットワークコールは、すべて TLS1.2 を介して実行されます。

Salesforce は、次のプロトコルを使用して、Office 365 のメールおよびカレンダーにアクセスします。

対象	プロトコル	認証	メモ
Salesforce Hyperforce サーバー	EWS	OAuth 2.0 認証	EWS は、Windows および Mac の Microsoft Outlook デスクトップで使用する SOAP ベースのプロトコルです。Salesforce Hyperforce サーバーは、定期的ではなく通知に基づいてデータをポーリングします。詳細は、 <a href="#">Office 開発センターの「Exchange の通知サブスクリプション、メールボックスイベント、および EWS」</a> を参照してください。
Inbox モバイルアプリケーション	<a href="#">Exchange ActiveSync (EAS)</a> または <a href="#">Office 365 REST API</a>	EAS では、ユーザー名、ドメイン、パスワードを使用した認証がサポートされません。  Office 365 REST API では、OAuth 2.0 アクセストークンが使用されます。	Exchange ActiveSync (EAS) は、モバイルアプリケーションを対象とした XML ベースのバイナリプロトコルです。ネイティブ iOS メールアプリケーションおよび Android Exchange メールアプリケーションでは、EAS プロトコルが使用されます。iOS 用 Exchange ActiveSync についての詳細は、 <a href="#">Apple サポートトピック</a> を参照してください。  Microsoft には、 <a href="#">Microsoft Graph API</a> や Office 365 REST API と呼ばれる新しい API があります。iOS および Android 用 Microsoft Outlook アプリケーションで Microsoft Graph API を使用して、メールやカレンダーのイベント (行

対象	プロトコル	認証	メモ
			<p>動)を読み取りおよび書き込みできるようになりました。</p> <p>Inbox モバイルアプリケーションでは、IMAP プロトコルは使用されません。</p>

## Microsoft Exchange 社内インスタンス

社内の Microsoft Exchange インスタンスには、考慮すべき重要な要件があります。

社内の Exchange インスタンス (2013、2016、2019) との接続では、ユーザー名、パスワード、ドメインに基づく従来の認証が使用されます。この場合、Salesforce Hyperforce サーバーと Inbox モバイルアプリケーションが Exchange パスワードを保存します。パスワードは、AES-256 暗号化を使用して保存時に暗号化されます。

Exchange でのネットワークコールは、TLS 1.1 または TLS 1.2 を使用して実行されます。Exchange サーバーでサポートされている最上位の TLS プロトコルによって、使用される TLS プロトコルが決定されます。

Salesforce は、次の 2 つのプロトコルを使用して、Exchange のメールおよびカレンダーにアクセスします。

対象	プロトコル	メモ
Salesforce Hyperforce サーバー	EWS	EWS は、Microsoft Outlook デスクトップで使用される SOAP ベースのプロトコルです。
Inbox モバイルアプリケーション	Exchange ActiveSync (EAS) または Office 365 REST API	Exchange ActiveSync (EAS) は、モバイルアプリケーションを対象とした XML ベースのバイナリプロトコルです。ネイティブ iOS メールアプリケーションおよび Android Exchange メールアプリケーションでは、EAS プロトコルが使用されます。

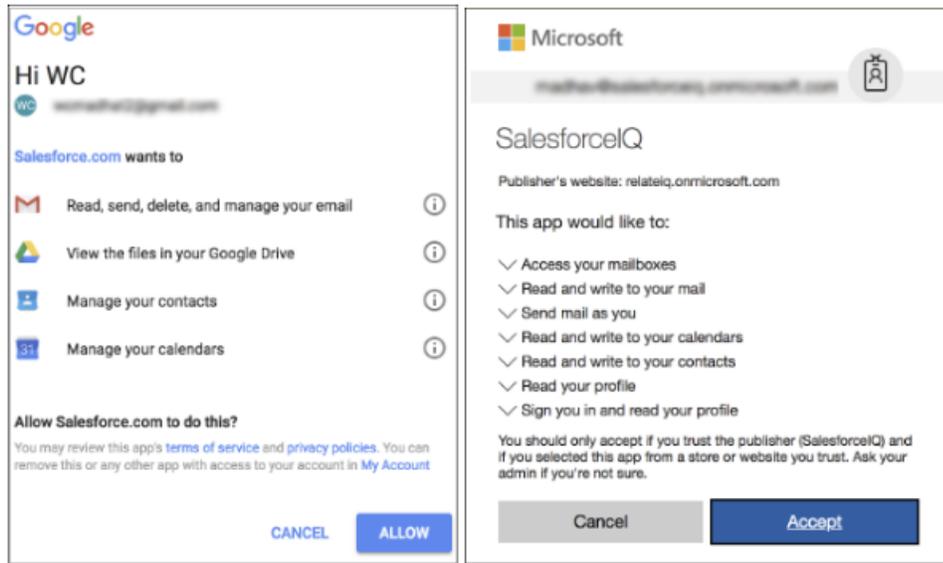
社内サーバーでは、OAuth 2.0 プロトコルはサポートされません。この接続では、代わりに NTLM Manager (NTLMv2) および基本認証がサポートされます。これらの認証では、ユーザー名、ドメイン、パスワードが必要になります。

Microsoft で [Microsoft Graph API](#) や Office 365 REST API と呼ばれる新しい API が最近導入されました。Office 365 上にない Exchange サーバーでは、新しい Office 365 REST API や Microsoft Graph API はサポートされません。

Office 365 API については、[Microsoft ドキュメント](#) を参照してください。

## OAuth プロトコルについての詳細

Salesforce では OAuth 2.0 認証フレームワークを使用して外部サービスに接続します。



Inbox ライセンスでプロビジョニングされる場合、ユーザーは Salesforce プラットフォームと各自のメールプロバイダーに接続できます。Gmail または Office 365 メールアカウントを持つモバイルユーザーは、OAuth 2.0 プロトコルを使用して接続されます。この初回ログインが完了すると、Salesforce Hyperforce サーバーは、サーバーに対して要求を実行するための OAuth 更新トークンとアクセストークンを取得および保存します。

OAuth 2.0 を使用すると、Gmail や Office 365 などのサービスにログインプロセスを委任している間、Salesforce などのサードパーティアプリケーションでそのようなサービスにアクセスできます。

ユーザーがサービスに接続すると、Salesforce はサービスのログインページにアクセスするための新しいページを開きます。このページは、次のようなサービスの独自のログイン Web ページになります。

- <https://login.salesforce.com/>
- <https://accounts.google.com>
- <https://login.microsoftonline.com>

ユーザーがログインすると、サードパーティアプリケーション(このケースでは Salesforce)に権限を付与するように求められます。次のような権限を付与します。

- メールに対する参照および更新のフルアクセス権。
- カレンダーに対する参照および更新のフルアクセス権。

ユーザーが権限を付与すると、サービスは Salesforce Hyperforce サーバーにリダイレクトされます。Salesforce Hyperforce サーバーは、サービスに接続して、以下を取得します。

- OAuth 更新トークン
- OAuth アクセストークン

OAuth アクセストークンは、サービスに対して認証済み要求(メールやカレンダーのイベント(行動)の取得など)を実行するために使用されます。これらのトークンの有効期限は1時間後に切れます。別のアクセストークンを取得するには、OAuth 更新トークンが使用されます。通常、更新トークンの有効期限は長い、期限がありません。

## Salesforce Hyperforce サーバー操作

---

Salesforce Hyperforce インフラストラクチャには Inbox データが保存され、さまざまな操作が実行されます。

Salesforce Hyperforce インフラストラクチャは、次のメールおよびカレンダー操作を実行します。

- メールボックスからメールヘッダーおよび HTML 本文を取得して保存する。
- 送信済みメールからメールヘッダーおよび HTML 本文を取得する。
- カレンダーのイベント (行動) を取得して保存する。
- [後で送信] 機能を使用してメールメッセージを送信する。
- [対応可能時間を挿入] を使用して被招集者が含まれるイベント (行動) を作成する。

Inbox モバイルアプリケーションには、メールとカレンダーに対する参照および更新のフルアクセス権があり、メールとカレンダーに対して次の操作を実行します。

- 添付ファイルが含まれるメールの読み取り、作成、送信を行う
- 既読としてマークしたり、フラグを付けたり、メールをフォルダー、アーカイブ、ごみ箱に移動したりする
- イベント (行動) を表示、作成、編集する
- イベント (行動) に RSVP を送信する

## モバイルデバイス管理とモバイルアプリケーション管理および Inbox

---

Inbox モバイルアプリケーションでは、モバイルデバイス管理 (MDM) とモバイルアプリケーション管理 (MAM) が制限付きでサポートされます。

Inbox モバイルでは、以下で MDM クライアント証明書がサポートされます。

- ユーザーの Salesforce ログイン。
- Office 365 メールアカウントへの接続。
- Google メールアカウントへの接続。

Inbox モバイルでは、Exchange 2013 または 2016 メールアカウントの MDM クライアント証明書はサポートされません。

特定のベンダーについては、次のようになります。

- Inbox モバイルでは、iOS デバイスで Inbox を使用する場合に Office 365 メールアカウントの Microsoft Intune MAM および MDM がサポートされます。
- Inbox モバイルでは、MobileIron や VMware Airwatch などの MDM ソリューションはサポートされません。

## iOS 用 Inbox モバイルの Microsoft Intune サポート

iOS 用 Inbox モバイルバージョン 8.6.0 以降、モバイルアプリケーション管理 (MAM) およびモバイルデータ管理 (MDM) のために iOS 用 Inbox モバイルを Microsoft Intune に追加できます。Inbox モバイルアプリケーションを Intune に追加して、Salesforce 組織が正しく設定されていることを確認するには、次のアクションを実行します。

アクション	詳細	リソース
Salesforce Inbox モバイルアプリケーションを Intune の管理アプリケーションとして追加する。	<a href="#">iOS アプリケーションを Intune に追加</a> する詳細な手順については、Microsoft ドキュメントを参照してください。	アプリケーションを Intune に追加するには、App Store リンクとバンドル ID が必要です。 <b>App Store リンク:</b> <a href="https://apps.apple.com/us/app/salesforce-inbox/id1208232122">https://apps.apple.com/us/app/salesforce-inbox/id1208232122</a> <b>iOS バンドル ID:</b> com.salesforce.inbox
Intune の Inbox モバイルアプリケーションエントリのアプリケーション保護ポリシーを作成する。	<a href="#">アプリケーション保護ポリシーの作成</a> については、Microsoft ドキュメントを参照してください。	
Azure Active Directory で、Office 365 の管理者の同意設定を定義する。	合理化された認証フローを実現するには、管理者の同意を Intune に提供します。 <ul style="list-style-type: none"><li>この URL に移動します。</li><li>Office365 アカウントにログインします。同意を付与するウィンドウが表示されます。</li><li>組織の代わりに管理者の同意権限を Salesforce Inbox 用 Intune に付与するには、[同意する]をクリックします。</li></ul>	<a href="#">管理者の同意についての詳細</a>
Salesforce で Intune のサポートを有効化する。	Inbox モバイルアプリケーション用 Intune を使用するように Salesforce を設定します。 <ol style="list-style-type: none"><li>Salesforce の [設定] の [クイック検索] ボックスに「Inbox」と入力し、[設定アシスタント]を選択します。</li><li>Microsoft Intune を有効化します。</li></ol>	

## モバイルアプリケーションデータの削除

Salesforce システム管理者は、いつでも特定のユーザーの Salesforce または Salesforce Inbox ライセンスを削除できます。

ライセンスを削除すると、ユーザーはアプリケーションにログインできなくなります。ユーザーがログインしようとする、アプリケーションからログアウトされ、ローカルに保存されているそのユーザーのすべてのデータが削除されます。

Exchange システム管理者は、Exchange ActiveSync リモートワイプを開始することもできます。

- Office 365 の場合、Office 365 設定に移動してデータをワイプします。
- 社内の Exchange サーバーの場合、Exchange 管理センターに移動してデータをワイプします。

データをワイプした後に、アプリケーションを開くと、アプリケーションはExchangeに接続されて、リモートワイプ応答を受信します。メールアカウントは無効としてマークされます。ユーザーはアプリケーションからログアウトされ、ローカルに保存されているそのユーザーのすべてのデータが削除されます。