# Cloud Protection for Salesforce

## Administrator's Guide

# 目次

第
1
章

# ソリューション概要

トピック：



WithSecure Cloud Protection for Salesforceは、Salesforceプラットフォームの既存のセキュリティ機能を強化および拡張するように設計されたクラウドベースのセキュリティソリューションです。

WithSecure Cloud Protection for Salesforceは、Salesforce Cloudに出入りするコンテンツを分析します。これにより、Salesforce組織からアップロードまたはダウンロードされるファイルやURLが、会社、パートナー、顧客に対するサイバー攻撃に使用されることがなくなります。

このソリューションには、SalesforceアプリケーションとWithSecure Security Cloudが含まれています。WithSecure Security Cloud. WithSecure Security Cloudは、ファイルとWebサイトのレピュテーションとセキュリティサービスを提供します。WithSecure Cloud Protection for Salesforceアプリケーションは、会社が使用しているSalesforce Sales、Service、またはExperience Cloud（旧名「Community Cloud」）にインストールされます。他のソフトウェアをインストールしたり、ネットワーク構成を変更したりする必要はありません。

WithSecure Security Cloudは、脅威を分析して対応するためのクラウドベースのシステムです。数百万のセンサー ノードから脅威インテリジェンスを収集し、デジタル脅威の大規模なデータベースを作成します。このデータベースは、世界的なサイバー脅威をリアルタイムで表示します。

WithSecure Cloud Protection for Salesforceは、このデータを使用して、グローバルまたはローカルの脅威状況の変化に迅速に対応します。たとえば、当社のヒューリスティック分析と動作分析によって新たなゼロデイ攻撃が検出された場合、当社はこの情報をすべての顧客と共有します。これにより、高度な攻撃が最初に検出された直後に無効化することができます。

このソリューションは遅延を短縮するように設計されており、Salesforceの使用には影響しません。ファイルまたはコンテンツを分析する際、このソリューションはWithSecure Security Cloudを利用する多段階プロセスを使用します。このプロセス内のステップは、コンテンツのリスクプロファイルに基づいてアクティブ化されます。たとえば、ゼロデイ マルウェアやその他の高度な脅威を使用した攻撃を防ぐように設計されたCloud Sandboxingテクノロジーを使用して、リスクの高いファイルのみがより徹底的な分析を受けます。

## 1.1 機能

WithSecure Cloud Protection for Salesforceは、共有責任モデルでのセキュリティ対応に最適なソリューションです。ウイルス対策ソフト以上の機能を提供するこのソリューションは、ミドルウェアを必要とすることなく、Salesforce とシームレスに統合します

| | |
|---|---|
| ファイル保護 | このソリューションは、Salesforce 内のファイルを高度に保護します。マルウェア、ランサムウェア、脆弱性の悪用やその他の高度な脅威からファイルを保護します。パフォーマンスやユーザエクスペリエンスへの影響を最小限にとどめながら自動的にアップロード、ダウンロードされたファイルをスキャンします。<br>このソリューションは、Salesforceプラットフォームにアップロードされるファイル内の添付ファイルに隠された有害なリンクを検出し、ブロックすることで、セキュリティを向上させます。<br>注：ファイル内で有害なリンクの検出を機能させるには、高度な脅威分析（ATA）をオンにする必要があります。 |
| **URL** 保護 | このソリューションは、URL を分析し、悪意のある URL がネットワークに危害を及ぼす前にアクセスをブロックします。ゼロレイテンシーで実施される分析は、リソースもほとんど必要としません。<br>URL保護は、Salesforceの標準フィールドやオブジェクトだけでなく、***Text***、***TextArea***（***Long***および***Rich***）、および***URL***フィールドなどのカスタム設定にも拡張されています。 |
| 短縮**URL**の脅威を防ぐ | 短縮URLはセキュリティ対策を回避するためによく使われます。このソリューションは、それらに隠された脅威を特定し、無害化します。これはURL保護機能にシームレスに統合されています。 |
| 脅威インテリジェンスチェック | 数千万にものぼるセンサーから収集された脅威インテリジェンスをリアルタイムで活用して、新たに出現した脅威を発生直後から特定することができ、絶えず進化し続ける脅威に対する非常に優れたセキュリティを確実に提供します。 |
| マルチエンジン ウイルス対策 | WithSecureの一流の技術は、行動分析と、複数のセキュリティレイヤを使い、脆弱性の悪用や、標的型攻撃に使用される未知のマルウェアを検出します。 |
| クラウドサンドボックス | 高リスク ファイルが検出された場合には、Security Cloud内のWithSecure Cloud Sandboxingテクノロジーがより詳細な分析を行い、不要な遅延を起こすことなくゼロデイ マルウェアと高度な脅威をブロックします。 |
| コンテンツフィルタリング | 本ソリューションでは、セキュリティポリシーやコンプライアンスポリシーに基づいて許可されていない、危険で不適切なコンテンツを検出し、ブロックすることができます。許可されないファイルは、ファイルタイプやファイル拡張子に基づいてフィルタリングすることができます。 |
| オンデマンドおよびスケジュールスキャン | Salesforceのファイルと添付ファイルは、いつでも、または事前定義された間隔で、有害で許可されていないコンテンツをスキャンできます。作成日や更新日、ファイルの種類や場所に応じて、スキャンするファイルを選択することができます。 |
| 隔離管理 | ファイル保護で削除された有害なコンテンツや禁止されているコンテンツは、隔離管理ツールを使用して閲覧· 復元することができます。 |
| アラート詳細のファイル置換 | 有害なコンテンツが削除され、テキストファイルに置き換えられた場合、置き換えられたファイルのオブジェクトIDがアラートの詳細に報告されます。 |
| ダイナミックなアナリティクスとレポート | Salesforce コンテンツのセキュリティ保護状態の概要を包括的に表示するダイナミックなアナリティクス(分析)とレポートで、稼働中のセキュリティ対策を把握することができます。<br>充実したレポート機能、高度なセキュリティアナリティクスと完全な監査証跡は、システム管理者がSalesforceへの脅威に対応する場合や、未知のソースからの攻撃の調査に役立ちます。 |

| | |
|---|---|
| 警告 | セキュリティインシデントのレポートを、管理者やセキュリティ部門に送信されるメール警告で自動化することができます。 |
| 自動アップデート | 設定に基づいて、サンドボックスや本番組織に新しいバージョンのアプリを自動的に受け取ることができます。 |
| スキャン ページのカスタマイズ | スキャンページに表示される製品バナーをカスタマイズすることができます。また、有害なコンテンツや、禁止されたコンテンツがブロックされた際にエンドユーザに表示されるメッセージも変更できます。 |
| スケーラブルなライセンス | WithSecureは、実際のネットワークトラフィックに基づいて、予測可能なライセンスモデルを提供します。 |
| ライセンスの自動割り当て | アプリケーションのライセンスは、ユーザープロファイルやその他の条件に基づいて、Salesforceのユーザーに標準ユーザー、コミュニティユーザー、コミュニティログインユーザーライセンスとして自動的に割り当てることができます。 |
| 迅速で簡単なインストール | Salesforce AppExchange から数分でインストールすることができます。エンドユーザのデバイス上のソフトウェアのインストール、プロキシの展開や、MX の変更などをする必要がありません。 |
| **Lightning** 対応 | このアプリケーションは、Salesforce Classical と、Lightning Experience ユーザ インターフェースの双方に対応しています。 |

第
2
章

# 導入

トピック：



このセクションでは、WithSecure Cloud Protection for Salesforceを組織に導入する手順について説明します。

アプリケーションの導入には次のステップがあります:

- アプリケーションをインストールする
- 権限セットとライセンスの指定
- アプリケーションの設定

以前のバージョンからアップグレードする場合は、アプリケーションをアップグレードする（12ページ）を参照してください。

## 2.1 Salesforceの対応エディション

WithSecure Cloud Protection for Salesforceアプリケーションは、Salesforce ClassicとLightning Experienceの両方のユーザインターフェースで使用できます。

WithSecure Cloud Protection for Salesforceアプリケーションは、次のSalesforceエディションと互換性があります。

- Enterprise
- パフォーマンス
- Unlimited
- デベロッパー

注: アプリケーションを運用環境にインストールする前に、サンドボックスでテストすることを強くお勧めします。

## 2.2 前提条件

***WithSecure Cloud Protection for Salesforce***のインストールを開始する前に、ここでSalesforce設定を確認してください。

### 2.2.1 Chatter 機能を有効にします

WithSecure Cloud Protection for Salesforceをインストールして使用するには、Salesforce組織内でChatter機能が有効になっている必要があります。

Chatter 機能を有効にするには

1. システム管理者のアカウントでSalesforceにログインします。
2. 環境設定を開き、[設定] を選択します。
3. 機能設定 > **Chatter** > **Chatter** 設定 を開きます。
4. 設定を変更するために [編集] を選択します。
5. **Chatter** 設定の下の [有効化] を選択し、[保存] を選択します。

### 2.2.2 Chatter 設定で、投稿とコメントの編集を許可します

Chatterの投稿とコメントでユーザーの言及が問題が発生することを阻止するためにChatter設定の [ユーザに投稿とコメントの編集を許可] 設定を有効にすることを強く推奨します。

この設定をSalesforceの組織でオンにするには

1. システム管理者のアカウントでSalesforceにログインします。
2. 環境設定を開き、[設定] を選択します。
3. 機能設定 > **Chatter** > **Chatter** 設定 を開きます。
4. 設定を変更するために [編集] を選択します。
5. [投稿とコメントの変更] で [ユーザに投稿とコメントの編集を許可] を選択して、[保存] を選択します。

### 2.2.3 添付ファイルを Salesforce ファイルのアップロードとして許可する

ファイルを添付ファイルとして保存し、Salesforce Classicのユーザーインターフェイスを使用する場合は、添付ファイルの設定ではなく、[**Salesforce Files**としてアップロードされたレコードの添付ファイル関連のファイル] の設定を有効にすることを推奨します。

この設定をオンにすると、添付ファイルとしてアップロードされたファイルは、アップロードまたはダウンロード時にSalesforceファイルに変換され、WithSecure Cloud Protection for Salesforceによってスキャンされます。

この設定をSalesforceの組織でオンにするには

1. システム管理者のアカウントでSalesforceにログインします。

2. 環境設定を開き、[設定] を選択します。
3. 機能設定 > **Salesforce Files** > 一般設定 を選択します。
4. 設定を変更するために [編集] を選択します。
5. [レコードの [添付ファイル] 関連リストにアップロードされたファイルは、添付ファイルとしてではなく **Salesforce Files** としてアップロードされます] を選択して、[保存] を選択します。

### 2.2.4 他の言語を設定する

WithSecure Cloud Protection for Salesforceのデフォルト言語は英語ですが、他の言語を設定できます。

WithSecure Cloud Protection for Salesforceは現在次の言語をサポートしています。

- 中国語 ( 簡体字 )
- 中国語 ( 繁体字 )
- チェコ語
- 英語
- フランス語
- ドイツ語
- ハンガリー語
- イタリア語
- 日本語
- 韓国語
- 研磨
- ポルトガル語
- ロシア語
- スロバキア
- スペイン語
- タイ語
- トルコ語

注 : インストール時に管理者が選択した言語が警告の表示言語になります。

他の言語を設定するには

1. システム管理者のアカウントでSalesforceにログインします。
2. 環境設定を開き、[設定] を選択します。
3. メニューから ユーザ インターフェース > 翻訳ワークベンチ > 翻訳設定 を選択します。
4. 有効にする言語の [アクティブ] チェックボックスを選択します。

WithSecure Cloud Protection for Salesforceで有効にした言語をアカウント設定の 設定 > 個人情報 > 言語とタイム ゾーン から選択できるようになります。

## 2.3 アプリケーションをインストールする

次の方法でアプリケーションを Salesforce 環境にインストールできます。

1. システム管理者のアカウントでSalesforceにログインします。
2. ***Salesforce AppExchange*** マーケットプレイスを開き、WithSecure Cloud Protection アプリケーションを探し、[今すぐ入手] を選択してインストールを開始します。

   WithSecure Cloud Protection は ***Salesforce AppExchange*** から入手できます。
   https://appexchangejp.salesforce.com/appxListingDetail?listingId=a0N3A00000EJGqnUAH

   注 : WithSecure Cloud Protection for Salesforceのリリース プレビューまたはベータ版をインストールする場合、管理インストール パッケージへのダイレクト リンクが提供されます。インストールを開始するには Web ブラウザでリンクを開いてください。

   注: すでにリリースプレビュー版やベータ版のアプリケーションがインストールされている場合は、それをアンインストールしてから新しいバージョンのアプリケーションをインストールしてください。

3. アプリケーションのインストール先 (Salesforce プロダクション環境またはサンドボックス) に応じて [本番組織にインストール] または [**Sandbox にインストール**] を選択し、使用条件に同意します。
4. インストールの詳細をクリックします。
5. [私は契約条件を理解し、同意します] を選択し、[確認してインストール] を選択します。
6. [管理者のみのインストール] を選択し、[インストール] を選択します。
7. [はい、これらのサードパーティ **Web** サイトにアクセスを許可します] を選択して、アプリケーションが WithSecure Security Cloud サービスに接続することを許可します。[次へ] を選択します。
8. インストールが完了するまで待ちます。

   重要 : アプリのインストールに時間がかかっているメッセージが届く場合、Salesforce からアプリがインストールが完了したメールが届くまでお待ちください。

9. インストールが完了したら、[**OK**] をクリックします。

WithSecure Cloud Protection for Salesforceがインストールされ、使用できます。

## 2.4 権限セットとライセンスの指定

アプリケーションをインストールした後、WithSecure Cloud Protection for Salesforceの権限セットとライセンスを割り当てる必要があります。

### 2.4.1 WithSecure Cloud Protection User 権限セットを指定する

WithSecure のソフトウェアライセンスを購入していない場合でも、組織内のすべてのアクティブ ユーザーに***WithSecure Cloud Protection User***の権限セットを割り当てる必要があります。

次の方法で ***WithSecure Cloud Protection User***の権限セットを指定できます。

1. システム管理者のアカウントで Salesforce にログインします。
2. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
3. 管理 > ツール を開き、「ユーザ権限セットの管理」で [指定] を選択します。

   Salesforce 組織内のアクティブ ユーザに***WithSecure Cloud Protection User***の権限セットが割り当てられます。

   注 : 権限セットは、バックグラウンドでアクティブユーザーに割り当てられます。

4. 管理 > ツール で、[有効化] を選択すると、***WithSecure Cloud Protection User***権限セットの自動割り当てが有効になり、WithSecureアプリケーションのインストール後にSalesforce組織に追加される新しいユーザに権限セットが自動的に割り当てられます。

   ヒント : このオプションを有効にしておくことを推奨します。

タスクがアクティブ化されて完了すると、アプリは情報アラートを作成します。

WithSecure権限セットの割り当てに失敗した場合、アプリは権限セットを受け取らなかったユーザIDのリストを含むエラー警告を生成します。

### 2.4.2 WithSecure Cloud Protection Admin 権限セットを指定する

アプリケーションの設定、アナリティクス (分析)、およびレポートにアクセスすることが許可されるユーザに、***WithSecure Cloud Protection Admin*** (管理者) 権限を割り当てる必要があります。

次の方法で ***WithSecure Cloud Protection Admin*** ユーザの権限セットを指定できます。

1. システム管理者のアカウントで Salesforce にログインします。
2. 環境設定を開き、[設定] を選択します。
3. ユーザ > 権限セット > **WithSecure Cloud Protection 管理** を選択します。
4. [割り当ての管理] をクリックします。
5. [割り当てを追加] をクリックします。
6. WithSecure Cloud Protection for Salesforceアプリケーション、分析、およびレポートにアクセスする必要があるすべてのユーザを選択し、[割り当てを追加]を選択します。

## 2.4.3 WithSecure Cloud Protection ライセンスを指定する

WithSecure Cloud Protection for Salesforceのライセンスは、アプリケーションを管理するすべてのユーザ、または有害かつ禁止コンテンツに関連するセキュリティ脅威から保護されているすべてのユーザに指定する必要があります。

注：WithSecure ライセンスが指定されていないユーザは、WithSecure Cloud Protection for Salesforce によって保護されません。Salesforce組織に侵入する可能性のある有害なコンテンツや禁止コンテンツにアクセスする危険性があります

次の方法で、WithSecure Cloud Protection for Salesforceライセンスをユーザに指定できます。

1. システム管理者のアカウントで Salesforce にログインします。
2. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
3. 管理 > ライセンスを開きます。
4. 購入したライセンスの数に応じて、次のいずれかを実行します。
   - 限られた数のユーザに対してWithSecureのライセンスを購入した場合、ライセンスモードを[選択したユーザ] に設定し、[保存] を選択して次の手順に進みます。
   - すべてのユーザに対してWithSecureライセンスを購入した場合、ライセンスモードを[すべてのユーザ] に設定し、[保存] を選択して次の手順に進みます。
5. [ライセンス ユーザを選択] リンクを選択します。
   「ライセンスを指定」ウィンドウが開きます。
6. ユーザ名、プロフィール、部門別に検索するか、リストをスクロールして、ライセンスが必要なユーザを探します。
7. [操作] 列の [指定] を選択して、選択したユーザにライセンスを指定します。[すべて指定]を選択して、検索で取得したユーザのリストに***WithSecure Cloud Protection for Salesforce***ライセンスを指定することもできます。
8. 設定が完了したら [閉じる] を選択します。
   ユーザープロファイルまたはその他の基準で自動ライセンス割り当てをオンにすることを検討できます。
   a) [ライセンスの自動割り当てを管理します] をクリックします。
   b) 新しいライセンスの自動割り当てルールを追加するための検索条件を定義します。
      検索条件には、名前、プロファイル、役割、メールアドレス、会社、部門、およびライセンスの値を使用できます。検索ボックスは、部分一致と完全一致をサポートしています。
      - `Profile=System`は、プロファイル名に`System`（`System Administrator`など）を含むユーザーを検索します。
      - `Profile="System"`は、「`System`」という名前のプロファイルを持つユーザのみを検索します。
      - パーセント記号をワイルドカードとして使用して、任意の文字に一致させることができます。たとえば、`Profile=S%A`は、`System Administrator`だけでなく、`Standard User`などのプロファイルを持つユーザも検索します。
   c) [追加] をクリックします。
      ルールがテーブルに追加され、必要に応じてさらにルールを追加できます。

      注：追加したルールは、行間の「OR」（または）を使用して読み込まれます。つまり、ルールは、テーブル内のルールのいずれかに一致する新規ユーザにのみ、ライセンスが自動的に割り当てられることを意味します。「AND」（および）条件を定義するには、検索条件を同じ行に記述します。
   d) 指定したルールを使用するには、[自動ライセンス割り当て] をオンにします。

WithSecureライセンスが多数のユーザーに割り当てられている場合、アプリはこれらのライセンスをバックグラウンドで割り当て、ステータスまたはエラーをアラートとして報告します。

## 2.5 アプリケーションをアップグレードする

WithSecure Cloud Protection for Salesforceの最新バージョンは Salesforce AppExchangeで常に利用できます。アップグレードしても、既存の設定と分析データはすべて保持されます。

注 : アプリケーションのリリースプレビューまたはベータ版からアップグレードすることはできません。以前のバージョンをアンインストールしてから、新しいバージョンのアプリケーションをインストールしてください。

1. システム管理者のアカウントでSalesforceにログインします。
2. **Salesforce AppExchange** マーケットプレイスを開き、**WithSecure Cloud Protection** アプリケーションを探し、[今すぐ入手] をクリックしてインストールを開始します。

   WithSecure Cloud Protection は **Salesforce AppExchange** から入手できます。
   https://appexchangejp.salesforce.com/appxListingDetail?listingId=a0N3A00000EJGqnUAH
3. アプリケーションのインストール先 (Salesforceプロダクション環境またはサンドボックス) に応じて [本番組織にインストール] または [**Sandbox** にインストール] を選択し、使用条件に同意します。
4. インストールの詳細をクリックします。
5. [私は契約条件を理解し、同意します] を選択し、[確認してインストール] を選択します。
6. [管理者のみのインストール] を選択し、[アップグレード] を選択します。
7. [はい、これらのサードパーティ **Web** サイトにアクセスを許可します] を選択して、アプリケーションが WithSecure Security Cloud サービスに接続することを許可します。[次へ] を選択します。
8. インストールが完了するまで待ちます。

   重要 : アプリのインストールに時間がかかっているメッセージが届く場合、Salesforce からアプリがインストールが完了したメールが届くまでお待ちください。
9. インストールが完了したら、[**OK**] をクリックします。

WithSecure Cloud Protection for Salesforceがアップグレードされました。

第
3
章

# アプリケーションの設定

トピック：



ここでは、インストール後に確認および設定が必要なアプリケーションの設定について説明します。

## 3.1 警告と通知の送信先を設定する

WithSecure Cloud Protection はセキュリティ警告とユーザ通知をメールで送信します。

セキュリティ警告は、WithSecure Cloud Protection の管理者 (Admins) グループに送信されます。ユーザ通知は、Salesforce組織内の社内ユーザに送信されます。セキュリティ警告とユーザ通知を送信するために使用されるメール アドレスを作成する必要があります。

注: セキュリティ警告とユーザ通知に使用されるメールアドレスは有効である必要があります。Salesforce で使用できるようにするには、メール アドレスを確認する必要があります。

次の方法で、WithSecure Cloud Protection とメール アドレスを設定して、セキュリティ警告とユーザ通知を送信できます。

1. システム管理者のアカウントでSalesforceにログインします。
2. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
3. 管理 > 一般 タブを開きます。
4. [通知] パネルを開きます。
5. [**WithSecure Cloud Protection Admins**] リンクを選択します。
6. [編集] を選択し、WithSecure Cloud Protectionからセキュリティ警告を受けるユーザを追加して、[保存] を選択します。
7. 管理 > 一般 に戻り、通知パネルから [会社全体のメール アドレスを設定する...] を選択します。
8. [ユーザが選択できる会社全体のメールアドレス] の横にある [追加] を選択します。
9. 表示名とメールアドレスを指定し、[保存] を選択します。
10. 管理 > 一般設定 > 一般 を開きます。
11. 「通知」で、[このアドレスからメール通知を送る] で作成したメールアドレスを選択します。
12. [保存] をクリックして、変更を保存します。

## 3.2 セキュリティ警告と警告メッセージを設定する

次の方法で、管理者とユーザに警告を送るタイミングを設定して、警告メッセージも変更できます。

1. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
2. 管理 > ファイル保護 タブを開きます。
3. [通知] を開き、ファイル保護の警告とメッセージを設定します。
   - [危険なコンテンツの検出時にセキュリティ警告を送る] を有効にすると、Salesforce クラウドに危険なコンテンツがアップロード/ダウンロードされたときに管理者へ警告が送られます。
   - [許可されていないコンテンツの検出時にセキュリティ警告を送る] を有効にすると、Salesforce クラウドに許可されていないコンテンツがアップロード/ダウンロードされたときに管理者へ警告が送られます。
   - [危険なコンテンツをアップロードした内部ユーザにセキュリティ警告を送る] を選択すると、Salesforce クラウドに悪質なコンテンツがアップロードされたときにユーザへ警告が送られます。
   - [許可されていないコンテンツをアップロードした内部ユーザにセキュリティ警告を送る] を選択すると、Salesforce クラウドに許可されていないコンテンツがアップロードされたときにユーザへ警告が送られます。
   - [コンテンツの評価が変更したときにセキュリティ警告を送る] を選択すると、ファイルの評価が変更されたときに管理者へ警告が送られます。

   スキャン検出時に危険たは許可されていないファイルを取り除くように選択した場合、[取り除いた危険なコンテンツをテキストファイルに置き換える] または [取り除いた許可されていないコンテンツをテキストファイルに置き換える] を有効することで取り除いたファイルのプレースホルダーにテキストファイルを使用できます。[ファイルの置き換えを設定] をクリックすると、ファイルを変更できます。
4. 管理 > **URL 保護** タブを開きます。
5. [通知] を開き、URL 保護の警告とメッセージを設定します。

- [危険な URL の検出時にセキュリティ警告を送る] を選択すると、Salesforce クラウドに危険な Web リンクが発行されたときに管理者へ警告が送られます。
- [許可していない URL の検出時にセキュリティ警告を送る] を選択すると、Salesforce クラウドに許可していない Web リンクが発行されたときに管理者へ警告が送られます。
- [危険な URL をアップロードした内部ユーザにセキュリティ警告を送る] を選択すると、Salesforce クラウドに危険な Web リンクが発行されたときにユーザへ警告が送られます。
- [許可していない URL をアップロードした内部ユーザにセキュリティ警告を送る] を選択すると、Salesforce クラウドに許可していない Web リンクが発行されたときにユーザへ警告が送られます。
- [URL 評価が変更したときにセキュリティ警告を送る] を選択すると、Salesforce クラウドへ発行された Web リンクの評価が変更されたときに管理者へ警告が送られます。

## 3.3 ファイル保護を設定する

ここでは、ファイル保護スキャンを設定する方法について説明します。

次の方法で Salesforce にアップロードされたファイルおよび Salesforce からダウンロードファイルをスキャンできます。

1. システム管理者のアカウントでSalesforceにログインします。
2. [アプリケーション ランチャー] から [Cloud Protection] を開きます。
3. 管理 > ファイル保護 を開きます。
4. チェックするコンテンツの保存方法に応じて、[Salesforce の添付ファイルとして保存されたコンテンツをスキャンする]、[Salesforce ファイルとして保存されたコンテンツをスキャンする] のいずれか、または両方をオンにします。
5. 添付ファイルをスキャンする場合は、[対象ロケーションの設定] を選択して、確認するコンテンツのソースを指定します。
   - [選択したオブジェクト] を選択し、チェック対象のソースを選択します。
   - すべての添付ファイルを対象にチェックする場合は、[すべてのオブジェクト] を選択します。
6. [確定] をクリックします。
7. [アップロード時に危険なコンテンツをスキャンする] と [ダウンロード時に危険なコンテンツをスキャンする] を有効にします。
8. 危険なコンテンツを検出したときの処理を選択します。
   - [アクセスを許可] - スキャン中に検出された危険なファイルのアクセスを許可します。
   - [ファイルを取り除く] - スキャン中に検出された危険なファイルを隔離します。
   - [アクセスをブロック] - 危険なファイルのアクセスをブロックしますが、ファイルは取り除かれません。
9. 必要に応じて、スキャンするファイルタイプまたはファイル拡張子を変更します。
   a) [除外されるファイルを除く] または [含むファイルのみ] を選択します。
   b) [除外されたファイルの種類と拡張子を構成する] または [含まれるファイルの種類と拡張子を構成する] を選択します。
   c) 関連するファイルタイプまたは拡張子のリストを指定します。
      ファイルタイプまたはファイル拡張子を使用します ( 例 : `WORD_X` または `docx` ) 。

      注: ファイルタイプの識別は、Salesforceにリストされているタイプに基づいて行われます。ファイルタイプの例を見るには、アナリティクス > ファイルイベント ページにリストされているファイルの詳細を見ることができます。
   d) 必要なタイプまたは拡張子がリストにない場合は、テキストフィールドに入力して、[追加] を選択します。
   e) [保存] を選択します。
10. WithSecure Cloud Protection for Salesforceが、Salesforce ユーザによってアップロードまたはダウンロードされた禁止コンテンツを検出した際に WithSecure Cloud Protection の動作を設定できます。
    a) 管理 > ファイル保護 を開きます。

b) [アップロード時に禁止コンテンツをスキャンする]と[ダウンロード時に禁止コンテンツをスキャンする] を有効にします。
c) 危険なコンテンツを検出したときの処理を選択します。
- [アクセスを許可] - スキャン中に検出された禁止ファイルのアクセスを許可します。
- [ファイルを取り除く] - スキャン中に検出された禁止ファイルを隔離します。
- [アクセスをブロック] - 禁止ファイルのアクセスをブロックしますが、ファイルは取り除かれません。

11. 必要に応じて、許可または禁止するファイルタイプまたはファイル拡張子を変更します。
a) [許可されていない ] または [許可されているもの以外] を選択します。
b) [禁止するファイルタイプを設定する] または [許可するファイル タイプを設定する] を選択します。
c) 関連するファイルの種類または拡張子のリストを指定します。WORD_Xやdocxのように、ファイルの種類や拡張子を使用します。
d) 必要なタイプまたは拡張子がリストにない場合は、テキストフィールドに入力して、[追加] を選択します。
e) [保存] を選択します。

### 3.3.1 パスワード保護されたアーカイブファイルの削除

攻撃者はパスワードで保護されたアーカイブを使用してマルウェアを配信し、従来の検出メカニズムを回避します。

注 : [高度な脅威分析]がオンになっており、WithSecure Cloud Protection Connected App使用していることを確認してください。

1. システム管理者のアカウントでSalesforceにログインします。
2. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
3. 管理 > ファイル保護 を開きます。
4. [パスワードで保護されたアーカイブが見つかった場合]、ファイルを許可するか、削除するか、ブロックするかを選択します。

   注 : デフォルトでは、パスワードで保護されたアーカイブは新規インストールでは削除され、製品のアップグレードではアップロードされたファイルでは許可され、ダウンロードされたファイルではブロックされます。

## 3.4 URL 保護を設定する

ここでは、URL 保護スキャンを設定する方法について説明します。

次の方法で Salesforce 上で危険なコンテンツと禁止リンクをブロックできます。

1. システム管理者のアカウントでSalesforceにログインします。
2. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
3. 管理 > **URL保護**を開きます。
4. [一般で] で、[標準オブジェクトの**URL**をスキャン] がオンになっていることを確認します。
5. [オブジェクトの構成] で、スキャンするオブジェクトを選択します。

   注 : リストからすべてのオブジェクトを選択することをお勧めします。

6. 危険なWebサイトのアクセスをブロックするには
a) [設定] で、[**URL**の評価を確認] をオンにします。
b) [**URL** が「危険」と評価されているときに] で [アクセスをブロック] を選択します。
7. 許可されていないコンテンツを含むWebサイトをブロックするには
a) [設定] で、[**URL**のカテゴリを確認] をオンにします。
b) [禁止カテゴリを選択] リストでブロックするカテゴリを選択します。
c) [禁止 **URL** の検出時に] で [アクセスをブロック] を選択します。

8. 新しく登録されたドメインをブロックするには、[許可しないURLの経過期間を選択する] でブロックするURLの経過期間を選択します。

   フィッシング攻撃では、新規登録ドメイン（NRD）がよく使用されます。これらのドメインをブロックすると、システムをそのような脅威から保護するのに役立ちます。7日以内のURLと90日以内のURLを選択できます。経過期間に基づいてURLをブロックしない場合は、[すべての経過期間を許可] を選択します。

   注：デフォルトでは、新規インストールの場合は30日以内のURLがブロックされ、製品のアップグレードの場合はすべての期間の URL が許可されます。

9. クリック時間保護を使用するには
   a) [URL保護] > [一般] > [オブジェクトの構成]に移動し、[URLをクリックで置き換える] をオンにします。
   b) [オブジェクトの構成] を選択し、クリック時保護に含めるオブジェクトを選択します。

      注：リストからすべてのオブジェクトを選択することをお勧めします。

10. 指定したWebサイトへのアクセスを許可するには
    a) [除外] を選択します。
    b) [信頼できるドメイン、ホスト、URL] をオンにします。
    c) [信頼済みのドメイン、ホスト、URLを開く] を選択して、アクセスを可能にするWebサイトを指定します。
    d) [リンクのリッチプレビューに対応しているドメインを除外] を有効にし、[ドメインの一覧を開く] を選択して、埋め込みビデオ、画像、記事のプレビューを許可するWebサイトを指定します。
11. [詳細設定] を選択します。
12. [投稿とコメントを処理するためのカスタムChatter統合] をオンにして、***WithSecure Cloud Protection Edit Chatter Posts***権限セットを作成します。[WithSecure Cloud Protection User 権限セットの割り当て] セクションで説明されているように、この権限セットを***WithSecure Cloud Protection User***権限セットとともにすべてのユーザに割り当てます。
13. アナリティクスレポートで除外されたURLを表示したくない場合は、[アナリティクスで除外されたURLをレポートする] をオフにします。
14. リンクに元のURLを表示したくない場合は、[リダイレクトリンクに元のURLを表示する] をオフにします。
15. [保存] を選択して、変更を保存します。

## 3.5 マニュアルスキャンとスケジュールスキャンの設定を変更する

マニュアルスキャンとスケジュールスキャンは、スキャンされるコンテンツ、検出の処理方法、通知の送信方法に同じ共有設定を使用します。

1. システム管理者のアカウントでSalesforceにログインします。
2. [アプリケーション ランチャー] から [Cloud Protection] を開きます。
3. 管理 > マニュアルスキャン.
4. [設定] で、[危険なコンテンツをスキャンする] をオンにします。

   スキャンするファイルの種類を設定するには
   a) [除外されるファイルを除く] または [含むファイルのみ] を選択します。
   b) [除外されたファイルの種類と拡張子を構成する] または [含まれるファイルの種類と拡張子を構成する] を選択します。
   c) 関連するファイルタイプまたは拡張子のリストを指定します。

      ファイルタイプまたはファイル拡張子を使用します（例：WORDXまたはdocx）。

      注：ファイルタイプの識別は、Salesforceにリストされているタイプに基づいて行われます。ファイルタイプの例を見るには、アナリティクス > ファイルイベントページにリストされているファイルの詳細を見ることができます。

   d) 必要なタイプまたは拡張子がリストにない場合は、テキストフィールドに入力して、[追加] を選択します。

e) [保存] を選択します。

5. 特定のタイプのコンテンツもチェックする場合は、[禁止コンテンツをスキャンする] をオンにします。

   許可されないファイルタイプを設定するには

   a) [許可されていない] または [許可されているもの以外] を選択します。
   b) [禁止するファイルタイプを設定する] または [許可するファイル タイプを設定する] を選択します。
   c) 関連するファイルタイプまたは拡張子のリストを指定します。
      ファイルタイプまたはファイル拡張子を使用します（例：WORDXまたはdocx）。
   d) 必要なタイプまたは拡張子がリストにない場合は、テキストフィールドに入力して、[追加] を選択します。
   e) [保存] を選択します。

6. 製品が有害または許可されていないコンテンツを検出した場合の動作を選択します。

   - [レポートのみ] はレポートと通知の検出を含みますが、ファイルには何もしません。
   - [ファイルの削除] はファイルを隔離し、レポートと通知に検出を含めます。

7. スキャンの通知を設定します。

   管理 > 一般 > 通知で設定した受信者に通知を送信します。

   通知テンプレートを編集するには、[セキュリティ警告メッセージを設定] または [ファイル置換を設定] をクリックします。

8. [詳細] を選択して、設定を確認します。

   - スキャン結果にクリーン（安全）なファイルまたは除外されたファイルを表示したくない場合は、[有害または許可されていないコンテンツを報告] をオンにします。
   - スキャンされたファイルのファイル変更タイムスタンプを更新する場合は、[スキャンされたファイルのハッシュチェックサムを更新する] をオンにします。スキャンされたファイルのSHA値が更新され、ファイルの最新の変更時刻も設定されます。
   - 1つのバッチで処理されるファイルの数を定義する場合は、[バッチあたりの最大ファイル数] をオンにします。

     注：通常、この設定を変更する必要はありません。ただし、「最大時間超過」エラーが表示された場合は、この設定で定義された値を減らすことをお勧めします。

## 3.6 マニュアルスキャンの権限セットを作成する

WithSecure Cloud Protection for Salesforceによるマニュアルスキャンとスケジュールスキャンでは、Salesforce内のすべてのファイルの処理を許可する特別な権限が必要です。

必要な権限のセットを作成するには

1. システム管理者のアカウントでSalesforceにログインします。
2. 環境設定を開き、[設定] を選択します。
3. 管理 > ユーザ > 権限セット に移動します。
4. [新規] をクリックして、新しい権限セットを作成します。
5. 新しい権限セットの [ラベル] および [API名] を入力します。
   たとえば、「WithSecure Cloud Protection Manual Scan」と入力し、自動生成されたAPI名（FSecureCloudProtectionManualScan）を使用します。
6. [保存] をクリックします。
7. 新しく作成された権限セットのあるページで、[アプリ] セクションの [アプリ権限] をクリックします。
8. [アプリ権限] ページで、[編集] をクリックします。
9. [コンテンツ] で、[すべてのファイルをクエリ] を選択します。
10. [保存] をクリックします。

11. [権限の変更確認] ダイアログで [保存] をクリックすると、追加されたシステムやオブジェクトの権限が有効になります
新しい権限セットが作成されます。
12. [割り当ての管理] をクリックし、マニュアルスキャンまたはスケジュールスキャンを実行する必要があるユーザに新しい権限を割り当てます。

## 3.7 製品の自動更新を設定する

自動更新を設定するには、次の手順に従ってください。

アプリケーションの新しいバージョンが内部で検証され、Salesforceセキュリティチームによってレビューされた後、SalesforceAppExchangeで公開されます。

1. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
2. [一般 ] タブに移動します。
3. [自動アップデート] を開きます。
4. アプリの新しいバージョンを自動的に受信するには、[製品アップデートを自動的にインストールする] をオンにします。
5. [アップデートのインストールを希望する曜日と時間] で、Salesforce組織環境に新しいバージョンをインストールする曜日と時間を選択します。

   注 : アップデートは Salesforce 内でキューに入れられ、希望するタイミングですぐに反映されるとは限りません。アップデートがSalesforceorgにインストールされる正確な時間は、アップグレードキューによって異なります。製品のライフサイクルポリシーに基づき、WithSecure™は自動アップデートの設定に関わらず、製品のアップデートをプッシュする権利を留保します。

6. アップデートが正常にインストールされたことを確認するには、アナリティクス > アラートに移動します。

   注 : 新しいバージョンがインストールされると、アプリはWithSecure Cloud Protection Adminsグループに追加されたユーザーにメール通知を送信します。

## 3.8 プライバシー設定を変更する

次の方法でWithSecure Security Cloudに提供する情報を選択できます。

WithSecure Security Cloudは、マルウェアや多様なデジタル脅威の分析エンジンかつ情報レポジトリです。Security Cloud の評価サービスは、安全なオブジェクトや悪意のあるオブジェクトを迅速に判定する方法を提供し、疑わしいオブジェクトの分析(自動・ 手動両方)を行い、保護の精度を上げるためにオブジェクトに関する情報を世界中から集積します。

当社は、敏感な個人データの収集を避け、不可欠なテクニカル データのみが当社サーバに確実に届くよう、厳密なプライバシー原則を適用しています。

1. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
2. 管理 > 一般 タブを開きます。
3. [プライバシー] の下で設定を変更します。
   a) WithSecure Cloud Protection for Salesforceはファイルのハッシュと一緒にWithSecure Security Cloudへクエリを実行することがあります。[完全なファイルをマルウェアと高度なスキャンに送る] を有効にすると、分析用にハッシュだけではなく、完全なファイルを送信できます。このオプションをオンにしておくと、WithSecure Cloud Protection for Salesforceが高度な脅威や複雑なマルウェアをできるだけ早く検出できるようになります。高度な脅威スキャンのために送信されたファイルは、処理後すぐに削除されます。
   b) [分析用に実行可能ファイルの収集を **WithSecure** ラボに許可] を有効にすると、実行可能ファイルを分析用に送信できます。

      Flash、Silverlightなどの解釈済みコードやスクリプトも実行可能ファイルとして処理できる場合があります。

   c) [分析用に不審・ 非実行ファイルの収集を **WithSecure** ラボに許可] を有効にすると、危険性のあるデータ ファイルをより深い分析を行うために送信できます。

d) ファイルが脅威分析を検出したときに、サードパーティのサービスとの共有を許可するデータを選択します。

- 許可しない：サードパーティのサービスとデータを共有しません。
- メタデータのみ：ファイルメタデータのみを共有できます。
- コンテンツ全体：ファイルを共有できます。

第
4
章

# アプリケーションを使用する

トピック：



ここでは、***WithSecure Cloud Protection for Salesforce***の通常の使用に関連するさまざまなタスクについて説明します。

## 4.1 コンテンツの分析

デフォルトでは、WithSecure Cloud Protection for Salesforce組織内でアップロード、ダウンロード、またはアクセスされるコンテンツを自動的にチェックします。

### 4.1.1 Salesforce組織内の有害なコンテンツを手動でスキャンする

組織内にアップロード、ダウンロード、アクセスされたコンテンツを自動的にチェックするだけでなく、本製品を使って組織内に保存されているコンテンツを手動でチェックすることもできます。

注: マニュアルスキャンやスケジュールスキャンを使用するには、ユーザアカウントに特別な権限を割り当てる必要があります。

1. システム管理者のアカウントでSalesforceにログインします。
2. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
3. 管理 > マニュアルスキャン.
4. チェックするコンテンツの保存方法に応じて、[**Salesforce**の添付ファイルとして保存されたコンテンツをスキャンする]、[**Salesforce** ファイルとして保存されたコンテンツをスキャンする] のいずれか、または両方をオンにします。
5. 添付ファイルをスキャンする場合は、[対象ロケーションの設定] を選択して、確認するコンテンツのソースを指定します。
   - [選択したオブジェクト] を選択し、チェック対象のソースを選択します。
   - すべての添付ファイルを対象にチェックする場合は、[すべてのオブジェクト] を選択します。
6. [確定] をクリックします。
7. チェックするコンテンツの日付範囲を設定し、コンテンツが作成された日を基準にしているのか、最後に修正された日を基準にしているのかを設定します。
8. [スキャンするファイルの最大数] を設定します。
9. [今すぐスキャン] をクリックします。
   [スキャン ジョブ開始済み] の通知が表示されます。

スキャン結果の個別のレポートはありませんが、 アナリティクス > ファイルイベント ページには、スキャン中に処理されたファイルが表示されます。[方向] 列には、マニュアルスキャンとスケジュールスキャンに関連するイベントの [スキャンジョブ] が表示されます。

関連タスク

マニュアルスキャンの権限セットを作成する（18ページ）

WithSecure Cloud Protection for Salesforceによるマニュアルスキャンとスケジュールスキャンでは、Salesforce内のすべてのファイルの処理を許可する特別な権限が必要です。

### 4.1.2 設定された時間に有害なコンテンツをスキャンする

スケジュールされたスキャンタスクは、WithSecure Cloud Protection for Salesforce特定の時間に組織のコンテンツを確認します。

注: マニュアルスキャンやスケジュールスキャンを使用するには、ユーザアカウントに特別な権限を割り当てる必要があります。

新しいスケジュールスキャンタスクを作成するには

1. システム管理者のアカウントでSalesforceにログインします。
2. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
3. 管理 > マニュアルスキャン.
4. [スケジュールスキャン] を選択し、[作成] をクリックします。
   これにより、[スケジュール**Apex**] ビューが開き、スケジュールされたタスクを設定できます。
5. [ジョブ名] を編集します。
6. 頻度に、[毎週] または [毎月] を選択します。
7. タスクの繰り返しを設定します。
8. タスクの [開始] と [終了] の日付を設定します。

9. [優先開始時間] を選択します。
10. [保存] をクリックします。

スキャン結果の個別のレポートはありませんが、 アナリティクス > ファイルイベント ページには、スキャン中に処理されたファイルが表示されます。[方向] 列には、マニュアルスキャンとスケジュールスキャンに関連するイベントの [スキャンジョブ] が表示されます。

スケジュールタスクを後で編集するには、[スケジュール スキャン] の下にある [スケジュール ジョブを表示する] をクリックして、[スケジュールApex] ビューを開き、タスクの [管理] をクリックします。

関連タスク

マニュアルスキャンの権限セットを作成する（18ページ）

WithSecure Cloud Protection for Salesforceによるマニュアルスキャンとスケジュールスキャンでは、Salesforce内のすべてのファイルの処理を許可する特別な権限が必要です。

## 4.1.3 スキャンからファイルを除外する....

場合によっては、特定のファイル タイプまたは特定のファイル拡張子をスキャンしたくない場合があります。除外されたファイルは、除外リストから削除しない限りスキャンされません。

スキャンからファイルの種類またはファイル拡張子を削除するには:

1. [アプリケーション ランチャー] から [Cloud Protection] を開きます。
2. 除外するファイル タイプまたは拡張子を検索するには
   a) アナリティクス > ファイル イベント を開きます。
   b) スキャンしたくないファイルのイベント行の最後にある [表示]を選択します。
   「ファイル拡張子」と「ファイル タイプ」は「ファイル名」の横にある「ファイル イベント履歴」ビューで表示されます。
3. 管理 > ファイル保護 タブを開きます。
4. 除外を開いて、ファイルの種類または拡張子に基づいて [スキャンから]ファイルを除外します。
   - [ファイルの種類別にファイルを除外する]をオンにし、[ファイルの種類の一覧を開く] を選択して、スキャンしないファイルの種類を指定します。
   - [ファイル拡張子でファイルを除外する]をオンにし、[ファイル拡張子のリストを開く] を選択して、スキャンしないファイル拡張子を指定します。

## 4.1.4 誤検知と誤検知の報告

スキャン エンジンが、ファイルまたは Web サイトを悪意のあるものまたは安全なものとして誤って識別することがあります。それらを報告すると、検出の精度が向上し、実際の脅威からユーザーを保護することができます。

誤って識別されたファイルまたは Web サイトを報告するには:

1. システム管理者のアカウントでSalesforceにログインします。
2. [アプリケーション ランチャー] から [Cloud Protection] を開きます。
3. ファイルを報告するには [Analytics] > [ファイル イベント]に移動し、Web サイトを報告するには [Analytics] > [URL イベント]に移動します。
4. レポートするファイルまたは URL を選択します。
   選択すると、イベントの詳細ビューが開きます。
   - 誤って安全でないと識別された、または不正確に分類された安全なファイルまたは Web サイトを報告するには、[誤検知として報告]を選択します。
   - 誤って安全であると識別された、または不正確に分類された悪意のあるファイルまたは Web サイトを報告するには、[偽陰性として報告]を選択します。
5. 開いた確認ダイアログで [レポート]を選択します。
   URL を報告する場合、URL を再分析する理由を選択します。
   - 安全な Web サイトが有害であると識別された場合、[無害な URL を選択するとブロックされます]。

- 安全であると識別されたWebサイトが有害である場合、[有害なURLを選択してもブロックされません]。
- ウェブサイトが誤って分類されたためにブロックされている場合は、[許可されたURLがブロックされます]を選択します。
- ウェブサイトが誤って分類されているためブロックされていない場合は、[許可されていないURLはブロックされません]を選択します。

ヒント：ファイルが有害である、またはファイルやWebサイトが誤って検出され評価されていると疑われる場合は、いつでも「サンプルWebサイトの送信」を使用して分析のために送信できます。

### 4.1.5 隔離機能を使用する

WithSecure Cloud Protection for Salesforce検出された有害なファイルを隔離領域に移動して、組織にさらなるリスクをもたらさないようにします。

注：隔離の設定はSalesforceのごみ箱に基づいているため、保存されたコンテンツは、組織のごみ箱の設定に基づいて完全に削除されます。有害なファイルのアラートを受信したら、必要に応じて完全に削除される前にできるだけ早く隔離を確認してください。

隔離されたコンテンツを表示するには

1. システム管理者のアカウントでSalesforceにログインします。
2. [アプリケーション ランチャー] から [Cloud Protection] を開きます。
3. 管理 > 隔離に移動します。
   ファイルの詳細を表示するには、[表示] をクリックします。
   ファイルを完全に削除するには
   a) 削除するファイルを選択します。
   b) [削除] をクリックします。
   c) [確定] をクリックします。
   隔離されたファイルを復元するには
   a) 復元するファイルを選択します。
   b) [復元] をクリックします。
   選択したファイルを元の場所に戻し、再度アクセスできるようにします。

### 4.1.6 スキャン結果のキャッシュを消去する

WithSecure Cloud Protection はスキャン結果をキャッシュに保存して、パフォーマンスを最適化します。キャッシュは定期的に消去されますが、手動で消去することもできます。

1. [アプリケーション ランチャー] から [Cloud Protection] を開きます。
2. 管理 > ツール タブを開きます。
3. [スキャン結果のキャッシュを消去] で [開始] をクリックします。
4. スキャン結果がキャッシュに保存される時間を設定するには
   a) 管理 > 一般 > 詳細 タブを開きます。
   b) [キャッシュにあるスキャン結果の有効時間 (TTL)] でスキャン結果がキャッシュに残る時間を選択します。

## 4.2 WithSecure Cloud Protection 接続アプリの使用

Connected AppWithSecure Cloud Protection for Salesforceスキャン機能が強化され、現在および将来にわたってビジネスクリティカルなプラットフォームをより効果的に保護します。

WithSecure Cloud Protection for Salesforce通常、Salesforce 環境への外部データ アクセスを必要としない統合ソリューションです。ただし、大量のデータを処理する場合、Salesforceプラットフォームの実行制限によりパフォーマンスの問題が発生することがあります。WithSecure WithSecure Cloud Protection Connected Appこのような状況でも Salesforce のパフォーマンスへの影響を最小限に抑えながら、最適なセキュリティを保証します。

Connected AppによりWithSecure Cloud Protection for Salesforce包括的な脅威分析を実行し、新たに発見された脆弱性や高度な悪意のあるソフトウェアに対して、発生時に完全な防御を提供します。非同期処理を使用することで、Salesforceのパフォーマンスへの影響を最小限に抑え、集中的なセキュリティ操作中でもプラットフォームがシームレスに機能できるようにします。

Connected Appの使用は必須ではありませんが、特にSalesforce環境内に大きなファイルを保存する場合は、使用することを強くお勧めします。

### 4.2.1 接続済みアプリのユーザー アカウントの作成

WithSecure Cloud Protection Connected App使用する前に、Salesforce でユーザー アカウントを設定し、必要な権限を割り当てる必要があります。

WithSecure Cloud Protection for Salesforce統合を有効にするアカウントで Salesforce 組織にアクセスします。このアカウントでは、通常のユーザー アカウントとは異なるレベルの Salesforce データおよび機能へのアクセスが必要です。Connected App専用のユーザーアカウントを作成し、そのアカウントに必要な権限のみを割り当てることを強くお勧めします。

別の統合アカウントを作成すると、Salesforceデータの監査証跡とアクセス管理が向上します。たとえば、トラブルシューティングの際に、別のアカウントを使用すると、問題の原因となっているユーザーアカウントを特定する代わりに、統合の問題を特定のアカウントまで簡単に追跡できます。

WithSecure Cloud Protection Connected Appの新しい統合ユーザーを作成するには、次の手順に従います。

1. **Salesforce** セットアップインターフェースを開きます。
2. [管理] > [ユーザー] > [ユーザー]に移動します。
3. 新しいユーザーを作成するには、[新しいユーザー]を選択します。
4. 必要に応じて、新しいユーザーアカウントの[姓]、[エイリアス]、[電子メール]、[ユーザー名]、その他の詳細を入力します。
   - [ユーザーライセンス]の場合は、***Salesforce*** を選択します。
   - [プロファイル]には、*標準ユーザー*を選択します。
5. [保存] を選択します。
   新しいユーザーが作成され、[電子メール]で指定された電子メール アドレスに電子メール メッセージが送信されます。
6. 新しいユーザーアカウントでログインしてログインパスワードを設定し、アカウントの作成を完了します。
   強力なパスワードを使用して統合アカウントを保護し、不審なアクティビティの兆候がないかアカウントを定期的に監視することを忘れないでください。

### 4.2.2 接続されたアプリへの権限の割り当て

アプリの権限セットを作成し、Salesforce 環境内で Connected App使用および管理するために、統合ユーザーに適切な権限セットを割り当てます。

次の手順に従って、必要な権限を持つ新しい権限セットを作成します。

1. **Salesforce** セットアップインターフェースを開きます。
2. [管理] > [ユーザー] > [権限セット]に移動します。
3. 新しい権限セットを作成するには、[新規]を選択します。
4. 新しい権限セットの [ラベル]と [**API** 名]を入力します。たとえば、ラベルは `WithSecure Cloud Protection Connected App`で、自動生成された API 名は `WithSecure_Cloud_Protection_Connected_App`になります。
5. [保存] を選択します。
6. 新しく作成された権限セットのあるページで、[システム権限]を選択します。
7. 「システム権限」ページで、[編集]を選択します。
8. システムセクションで、[**API** 有効]と [すべてのデータを表示の]チェックボックスを選択します。
9. [保存] を選択します。

10. 追加のシステムおよびオブジェクトの権限を有効にするには、権限の変更確認ダイアログで [保存] を選択します。
    新しい権限セットが作成されます。
11. Salesforce セットアップインターフェースで、[管理] > [ユーザー] > []に移動し、専用ユーザーの権限を設定します。
12. WithSecure Cloud Protection Connected App用に作成したユーザー アカウントを選択します。
13. [権限セットの割り当て]を選択し、[割り当ての編集」を]選択します。
14. [使用可能な権限セット]のリストで、「*WithSecure Cloud Protection 管理者*」と、以前に WithSecure Cloud Protection Connected App用に作成した権限セットを選択します。
15. [保存] を選択します。

### 4.2.3 WithSecure Cloud Protection Connected App の使用

Connected Appアプリで WithSecure Cloud Protection for Salesforceを使用する方法の説明。

1. WithSecure Cloud Protection Connected App用に作成したアカウントを使用して Salesforce にログインします。
2. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
3. [管理] > [ツール]に移動します。
4. [接続されたアプリの管理]で [接続]を選択します。
5. 「**Secure Cloud Protection** に接続」ダイアログで [接続]を選択します。
6. [アクセスを許可]ダイアログで、要求された権限を確認し、[許可]を選択します。
7. [ウィンドウを閉じる]を]選択します。
8. [管理] > [ツール]ページでステータスを確認し、WithSecure Cloud Protection Connected Appが接続されていることを確認します。

## 4.3 クリック時の URL 保護の構成

URLは、アップロードされた時点では安全に見えても、時間の経過とともに、無害に見えるリンクから危険なペイロードに変化する可能性があります。クリック時保護を使用すると、URLがクリックされたときにリアルタイムでその安全性を検証できます。これにより、ユーザーが以前は非アクティブだった罠に陥るのを防ぎ、潜在的なデータ侵害やシステム侵害から組織を保護します。

好みに応じて、選択した Salesforce オブジェクトにクリック時 URL 保護 (CTP) を使用できます。たとえば、Chatter 投稿にクリック時URL保護を適用して内部ユーザーに最高レベルのセキュリティを提供し、外部の顧客に送信される送信メールにはクリック時 URL 保護をオフにしておくことができます。

次の手順に従って、クリック時 URL 保護を有効にし、セキュリティ要件に合わせて調整します。

1. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
2. 管理 > **URL保護**を開きます。
3. [**URL** 保護] > [一般] > [オブジェクトの構成]に移動し、[オブジェクトの選択] モーダルで歯車アイコンを選択して、必要なフィールドの [**URL** をクリック時間保護リンクに置き換える] を]オンにします。

   注：クリック時の保護は、100 文字を超えるフィールドにのみ適用されます。100 文字未満の場合は、N/Aと表示されます。

4. [確認]を選択します。
5. [保存] をクリックして、変更を保存します。

## 4.4 高度な脅威分析を構成する

高度な脅威分析では、クラウドサンドボックスなどの高度な検出機能を利用して、アップロードされたファイルを徹底的にスキャンします。

高度な脅威分析では、最初のファイルスキャンと比較して、より徹底的なスキャンが行われます。 サンドボックス環境でファイルをスキャンします。時間はかかりますが、悪意のあるファイルをより確実に識別します。

注：高度な脅威分析を使用するには、WithSecure Cloud Protection Connected Appを使用する必要があります。

ヒント：セキュリティを強化するには、高度な脅威分析中にファイルのダウンロードをブロックします。 これにより、ファイルアクセスの待ち時間が長くなる可能性があります。

1. [アプリケーション ランチャー] から [Cloud Protection] を開きます。
2. 管理 > ファイル保護 を開きます。
3. [設定] で、[高度な脅威分析] をオンにします。
4. [保存] をクリックして、変更を保存します。

## 4.5 QRコードスキャン

QR コード スキャンは、Salesforce の電子メールと Chatter メッセージからすべての QR コードを識別して抽出します。

QR コードのスキャンを有効にするには、次の手順に従ってください。

1. 管理 > ファイル保護 を開きます。
2. [設定]で [高度な脅威分析]がオンになっていることを確認します。
   QR コードのスキャンが機能するには、高度な脅威分析が必要です。
3. [管理] > [ファイル保護] > [除外するファイルの種類と拡張子を構成する]に移動します。
4. QR コードスキャンに必要な画像形式がスキャンから除外されていないことを確認してください。
   QR コード スキャンは、JPEG、PNG、GIF、BMP など、すべての主要な画像形式をサポートしています。

   注：現在、QR コード スキャンでは、ファイル内の QR コードや短い URL としてフォーマットされた QR コードのスキャンはサポートされていません。

QR コード画像は、[ファイル保護]および [ファイル イベント]で `Malicious:Network/QR`として報告され、画像に悪意のあるコンテンツが含まれていることが示されます。

## 4.6 カスタマイズされたオブジェクトスキャンを作成

独自のカスタム設定により、URL保護をSalesforceの標準フィールドやオブジェクト以外にも拡張できます。

カスタマイズされたスキャンを作成するには

1. [アプリケーション ランチャー] から [Cloud Protection] を開きます。
2. [管理] > [URL保護] > [一般] > [オブジェクトの構成]に移動します。
   デフォルトでは、すべての標準オブジェクト（***Case***、 ***CaseComment***、 ***Lead***、 ***Task***、 ***EmailMessage***、***FeedItem***、および***FeedComment***オブジェクト）とそのフィールドが選択されます。

   注：メール スキャンは***EmailMessage***（*受信*）と***EmailMessage***（*送信*）に分割されており、単一のカスタマイズルールで設定することはできません。

3. スキャンするオブジェクトを選択します。
   検索を使用して、スキャンする標準オブジェクトまたはカスタム オブジェクトを見つけ、検索結果からオブジェクトを選択します。

4. URLスキャンのオブジェクトを選択したら、行の末尾にある歯車アイコンを選択して、スキャンするフィールドとクリック時間保護を使用するかどうかを選択します。

   注：クリック時間保護は、100文字を超えるフィールドでのみ機能します。

   注：最大5つのフィールドを選択できます。

5. [保存] を選択します。
   Secure Cloud Protectionでは、選択したオブジェクトのトリガーを設定するように通知されます。
6. オブジェクトマネージャーで、選択したオブジェクトのトリガーを作成します。

   注：標準オブジェクトの場合、トリガーはすでに含まれているため、設定する必要はありません。

   選択したオブジェクトのトリガーがすでに存在する場合は、必要な操作タイプがすべて揃っていることを確認して、トリガーを保存します。

   a) [オブジェクトのセットアップ] ページの [トリガー] に移動します。
   b) 新しいトリガーを作成します。
   c) オブジェクトの詳細に従って、次のコードを編集し、トリガーとして貼り付けます。

```
trigger [TRIGGERNAME] on [OBJECTAPINAME] (before insert, before
 update, after insert) { AFSC.FS_CommonURLChecker.scanURLS(); }
```

   括弧 ([]) 内のセクションを変更します。

   - `[TRIGGERNAME]`

     標準オブジェクト：`Object API name + Trigger`

     カスタムオブジェクト:オブジェクトAPI名 ( `__c + Trigger`を除く )

   - [OBJECTAPINAME]：オブジェクトAPIの名前。

   d) トリガーを保存します。
   e) サンドボックス環境でトリガーをテストします。
      「テストクラスの追加 ( salesforce.com ) 」の手順に従って、トリガーコードをカバーするオブジェクトレコードを挿入します。
      テスト後、 *変更セット* またはその他のデプロイ方法を使用して、トリガーとテストクラスを実稼働環境に移動します。詳細については、「変更の開発および展開のためのツールの選択 (salesforce.com)」を参照してください。

   トリガーが設定されると、[オブジェクトの選択]ウィンドウのステータスが「トリガーの設定」から「含まれるフィールド」に変わります。

実稼働環境で使用する前に、カスタムオブジェクトのスキャンをテストします。悪意のあるURLイベントは、[分析] セクションで報告されます。

スキャンからオブジェクトを削除するには、[オブジェクトの選択]ウィンドウに移動し、歯車アイコンを選択して、**[オブジェクトの削除]** を選択します。

注：カスタムURLスキャンのオブジェクトを構成するには、ユーザーにWithSecure Cloud Protection管理者権限セットを割り当てる必要があります。

## 4.7 警告の表示と検索

次の方法でセキュリティ警告を表示できます。

1. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
2. 「アナリティクス」タブを開きます。

   - 「警告」ビューすべてのセキュリティ警告が表示されます。
   - 「ファイル イベント」ビューではファイル スキャンで発生したすべてのイベントがされます。
   - 「**URL** イベント」ビューでは Web リンクの評価· カテゴリ チェックで発生したすべてのイベントが表示されます。

3. 警告の終わりにある [表示] またはイベント行をクリックすると、警告/イベント履歴の詳細を確認できます。
4. 検索値を使用して結果を絞り込めます。
   - 「警告」ビューで使用できる値: TIME / SEVERITY / SOURCE / USER / REASON
   - 「ファイル イベント」ビューで使用できる値: TIME / ACTION, VERDICT / FILENAME / FILETYPE / DIRECTION / LOCATION / SHA1 / USER / IPADDRESS
   - 「URL イベント」ビューで使用できる値: TIME / ACTION / VERDICT / URL / DIRECTION / LOCATION / USER / IPADDRESS / CATEGORY
   - 特定の日時に発生したイベントを検索する場合、現在のロケールにもとづいた日時を使用してください。検索機能はに Salesforce SOQL データ リテラルすべて使用できます。

   検索例:

   - 「警告」ビューで、ファイル保護に関連する重大な警告を検索する: `SEVERITY=Critical, SOURCE=File Protection`
   - 「ファイル イベント」イベントでブロックしたアップロード ファイルを検索する: `ACTION=Blocked, DIRECTION=Upload`
   - 「ファイル イベント」ビューにある `Sales Report.xlsx` に対してブロックされたダウンロード試行を検索する: `ACTION=Blocked, DIRECTION=Download, FILENAME=Sales Report.xlsx`
   - 「URL イベント」ビューで、ユーザから投稿され、ブロックされたすべての URL: `ACTION=Blocked, DIRECTION=Post`
   - 「URL イベント」ビューで 192.168.0.1 の IP アドレスから開かれたすべての URL を検索する: `DIRECTION=Open, IPADDRESS=192.168.0.1`

   日時の検索例 (ロケール: 英語 (英国))

   - `TIME=31/12/2016 12:00`
   - `TIME=31/12/2016 12:00...12/12/2016 14:00`
   - `STARTTIME=31/12/2016 12:00`
   - `ENDTIME=31/12/2016 12:00`
   - `TIME=31/12/2016>5d`
   - `TIME=31/12/2016 12:00>5h`
   - `TIME=YESTERDAY`

## 4.8 レポートの表示と編集

WithSecure Cloud Protection のレポート機能は、保護ステータスの確認および攻撃の原因を調べるため、あるいは対応するために便利な情報を提供します。

情報の報告には、発見された感染やその発生元(ソース)などの感染関連の統計情報、安全および安全でないファイル間のトレンド比較、ならびに保護されているファイルの数が含まれます。***WithSecure Cloud Protection for Salesforce***は、最も一般的に使われるファイル タイプ、最も頻繁の発生元ソース、および最もアクティブなユーザも報告します

次の方法で***WithSecure Cloud Protection for Salesforce***でレポートを表示できます。

1. [アプリケーション ランチャー] から [Cloud Protection] を開きます。
2. 「概要」タブを開きます。

   「概要」ビューではスキャンしたファイル、ブロックした URL、発生した警告数の統計情報を確認できます。

   注: 特に「重大」「重要」と記載されているアラートの数を監視することを推奨します。これらのアラートの数が急激に増加した場合は、組織内のセキュリティ問題を示している可能性があります。
3. 特定のアラートタイプをフィルタリングされたビューで表示するには、[アラート] テーブルの対応する番号をクリックします。
4. [レポートをもっと表示する] ドロップダウンをクリックし、レポートを選択すると、保護されているコンテンツの分析情報およびファイルと URL 保護の詳細を確認できます。

これらの各レポートには、組織の保護ステータスの詳細を提供する多数のチャートやグラフが含まれています。必要に応じて、レポートを編集し、カスタマイズされた新しいレポートとして保存することができます。

レポートのメール配信をスケジュールするには

a) [サブスクライブ] をクリックします。
b) レポートを送信する頻度と時間を設定します。
c) [受信者を編集] をクリックし、レポートを受信する必要がある他のユーザを追加します。
d) [保存] をクリックします。

利用可能な属性を使用して新しいレポートを作成するには

a) [サブスクライブ ] の横にあるドロップダウンアイコンをクリックし、[新規ダッシュボード] を選択します。
b) レポートの名前と説明を入力し、フォルダを選択して、[作成] をクリックします。
c) ツールバーの [コンポーネント] および [フィルタ] オプションを使用して、レポートに含めるものを選択します。
d) [保存] をクリックします。
e) レポートの編集が終了したら、[完了] をクリックします。

ファイルレポートの属性：

- 作成者：フルネーム
- 作成日
- 日時
- ファイル拡張子
- ファイル名
- ファイルスキャンID
- ファイルサイズ
- ファイルタイプ
- IPアドレス
- 最終更新者：フルネーム
- 最終更新日
- 名前
- 所有者：フルネーム
- レコードID
- スキャンタイプ
- SHA1
- ロケーション
- ユーザ：フルネーム
- 評決
- 所有者 ( 名、フルネーム、姓、所有者ID、電話、プロファイル：名前、ルール：名前、タイトル、ユーザ名、メールアドレス、エイリアス、アクティブ )
- 理由
- ファイルの普及度
- ファイルレピュテーション評価

URLレポートの属性：

- URLスキャン：ID
- URLスキャン：名前
- アクション
- カテゴリ
- 日時
- 方向
- IPアドレス
- ロケーション
- 理由
- 評判
- 評判の説明

- URL
- ユーザ
- 評決
- 所有者名
- 所有者エイリアス
- 所有者ロール
- 作成者
- 作成されたエイリアス
- 作成日
- 最終更新者
- 最終更新エイリアス
- 最終更新日

## 4.9 製品のライセンス情報を表示する

WithSecure Cloud Protection for Salesforceの [ライセンス] ページには、ライセンスのステータスと使用法の詳細が含まれています。

1. システム管理者のアカウントでSalesforceにログインします。
2. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
3. 管理 > ライセンスページを開きます。
   このページでは、ライセンスのステータスと有効期限、およびライセンスの使用状況やスキャンの使用統計に関する情報が表示されます。

関連タスク

WithSecure Cloud Protection ライセンスを指定する（11ページ）
WithSecure Cloud Protection for Salesforceのライセンスは、アプリケーションを管理するすべてのユーザ、または有害かつ禁止コンテンツに関連するセキュリティ脅威から保護されているすべてのユーザに指定する必要があります。

## 4.10 データ処理領域を構成する

データが処理される地理的地域を選択できます。

デフォルトでは、WithSecure Cloud Protection for Salesforceは最も近いデータ処理リージョンを自動的に選択します。コンプライアンス、パフォーマンス、またはデータの所在地に関する要件があり、データ処理のための地理的な場所を選択する必要がある場合は、次の手順に従ってください。

1. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
2. 管理 > 一般 タブを開きます。
3. [詳細] の下で、 [データ処理地域] ドロップダウンメニューを開き、新しい地域を選択します。
   注 : [自動] を選択すると、最も近いアクティブな地域が自動的に選択されます。
4. [保存] をクリックして、変更を保存します。
   リモートサイトがまだ設定されていないため、新しいリモートサイト設定を作成することを促す通知が開きます。
5. 通知からURLアドレスをコピーします。
6. Salesforceを開き、[設定] に移動し、[リモートサイト設定] を参照します。
   [リモートサイト設定] セットアップビューが開きます。
7. [新しいリモートサイト] を選択します。
   a) サイトの名前を [リモート サイト名] に入力します。
   b) コピーしたURLを [リモートサイト**URL**] に貼り付けます。
   c) [保存] を選択します。
8. **Cloud Protection**アプリを再度開きます。
9. 管理 > 一般 タブを開きます。

10. [詳細] の下で、 [データ処理地域] ドロップダウンメニューを開き、新しい地域を再度選択します。
11. [保存] をクリックして、変更を保存します。
    新しい設定が保存されたことを通知する通知が表示されます。

データは選択した場所で処理されます。

第
5
章

# アプリケーションの動作を確認する

トピック：



WithSecure Cloud Protection for Salesforceアプリケーションをインストール・設定した後、ファイル保護とURL保護が動作していることを確認してください。

## 5.1 ファイル保護の動作を確認する

次の方法で Eicar テスト ファイルを使用してファイル保護の動作を確認できます。

1. `Eicar.com`テスト ファイルをhttps://www.eicar.org/?page_id=3950からダウンロードして、ファイル名を`Example_MaliciousFile.docx`に変更します。

   注: `Eicar.com` は実際に脅威がないファイルですが、検証用にマルウェアとして認識されます。マルウェア対策ソフトがファイルをブロックした場合、特定のフォルダをリアルタイム スキャンから除外して `Eicar.com` ファイルをフォルダに入れてください。

2. `Example_MaliciousFile.docx` および安全なファイル を Salesforce *ファイル*または ***Chatter*** にアップロードします。
3. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
4. アナリティクス > ファイル イベント タブを開きます。
   安全なファイルとブロックしたファイルが1ファイルずつあることが示されます。
5. 両方のファイルをダウンロードできるか試します。
   安全なファイルはダウンロードできますが、悪質なファイルはブロックされています。
6. アナリティクス > ファイル イベント タブに戻り、ダウンロード イベントを確認します。
7. [表示] をクリックするとイベント履歴を確認できます。
   選択したファイルに対するアップロード・ダウンロードのアクティビティが表示されます。

## 5.2 URL 保護の動作を確認する

次の方法でテスト ドメインを使用して URL 保護の動作を確認できます。

1. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
2. 管理 > **URL 保護** タブを開きます。
3. このテストでは、[許可していない カテゴリを選択] で [*ギャンブル*] が選択されていることを確認してください。
4. 次の2つの URL `unsafe.fstestdomain.com` と `gambling.fstestdomain.info` を Salesforce ***Chatter*** に投稿します。
5. ***Chatter*** を開き、URL がある2つの新しい投稿を表示します。
6. **WithSecure Cloud Protection** に戻り、アナリティクス > **URL イベント** タブを開きます。
   ***Chatter*** の新規投稿が2つあります。
7. ***Chatter***に戻り、両方のリンクを開けるか試します。「***Web*** *サイトをブロックしました*」および「*許可していない* ***Web*** *サイトをブロックしました*」のブロック ページが表示されます。
8. **WithSecure Cloud Protection** に戻り、アナリティクス > **URL イベント** タブをもう一度開きます。
   URL を開いたイベントが2つ表示されます。
9. [表示] をクリックするとイベント履歴を確認できます。
   選択した URL に対するアクティビティ (投稿とリンクのアクセス) が表示されます。

第
6
章

# アンインストール

トピック：



このセクションでは、削除手順を説明します。WithSecure Cloud Protection for Salesforceあなたの組織から。

アプリケーションの削除には次の手順があります。

- 権限セットの指定削除
- アプリケーションのアンインストール

## 6.1 権限セットの指定を削除する

アンインストールする前にWithSecure Cloud Protection for Salesforceアプリケーションを削除するには、Salesforce組織内のユーザーに割り当てた ***WithSecure Cloud Protection*** ユーザーおよび ***WithSecure Cloud Protection*** *管理者*権限セットを削除する必要があります。

権限セットを削除するには

1. システム管理者のアカウントでSalesforceにログインします。
2. [アプリケーション ランチャー] から [**Cloud Protection**] を開きます。
3. 管理 > ツールを開き、「ユーザの権限を管理する」で [削除] を選択します。
4. 環境設定を開き、[設定] を選択します。
5. ユーザ > 権限セット > **WithSecure Cloud Protection** 管理 を選択します。
6. [割り当ての管理] をクリックします。
7. [**Remove Assignments (指定の取り除き)**]
8. [**OK**] をクリックしてユーザの削除を確定します。

## 6.2 アプリケーションをアンインストールする

すべてのユーザ権限を取り除いた後、WithSecure Cloud Protection を削除する必要があります。

次の方法で WithSecure Cloud Protection をアンインストールできます。

1. システム管理者のアカウントで Salesforce に口グインします。
2. 環境設定を開き、[設定] を選択します。
3. アプリケーション > インストール済みパッケージ を開きます。
4. [WithSecure Cloud Protection] の横にある [アンインストール] を選択します。
5. 「パッケージのアンインストール」ページで、下にスクロールして [はい、このパッケージをアンインストールして、すべての関連コンポーネントを永久に削除します] を選択します。

**WithSecure Cloud Protection** がアンインストールされると、メール通知が届きます。