Cloud Protection for Salesforce

Administrator's Guide

目次

第 1 章： ソリューション概要 4

1.1 機能 5

第 2 章： 導入 7

2.1 Salesforceの対応エディション 8
2.2 前提条件 8
2.2.1 Chatter 機能を有効にします 8
2.2.2 Chatter 設定で、投稿とコメントの編集を許可します 8
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 8
2.2.4 他の言語を設定する 9
2.3 アプリケーションをインストールする 9
2.4 権限セットとライセンスの指定 10
2.4.1 WithSecure Cloud Protection User 権限セットを指定する 10
2.4.2 WithSecure Cloud Protection Admin 権限セットを指定する 11
2.4.3 WithSecure Cloud Protection ライセンスを指定する 11
2.5 アプリケーションをアップグレードする 12

第 3 章： アプリケーションの設定 13

3.1 警告と通知の送信先を設定する 14
3.2 セキュリティ警告と警告メッセージを設定する 14
3.3 ファイル保護を設定する 15
3.3.1 高リスクファイルのサポート 16
3.4 URL 保護を設定する 17
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 18
3.6 マニュアルスキャンの権限セットを作成する 19
3.7 製品の自動更新を設定する 20
3.8 プライバシー設定を変更する 20
3.9 更新前に選択リスト値を有効化する 21
3.10 URLスキャンにおけるSalesforceの制限事項への対応 21

第 4 章： アプリケーションを使用する 23

4.1 コンテンツの分析 24
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 24
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 24
4.1.3 スキャンからファイルを除外する 25
4.1.4 誤検知と誤検知の報告 25
4.1.5 隔離機能を使用する 26
4.1.6 スキャン結果のキャッシュを消去する 26
4.1.7 ゲストおよびコミュニティユーザー向けのファイル保護の高度なスキャン設定 27

4.2 WithSecure Cloud Protection 接続アプリの使用.....27
4.2.1 接続済みアプリのユーザー アカウントの作成.....27
4.2.2 組織内での WithSecure Connected App のローカルインストール.....28
4.2.3 新しい「アンインストールされた接続アプリの承認」権限セットを作成します.....29
4.2.4 接続されたアプリへの権限の割り当て.....29
4.2.5 WithSecure Cloud Protection Connected App の使用.....30
4.2.6 Connectedアプリのインストール.....31
4.3 クリック時の URL 保護の構成.....31
4.4 高度な脅威分析を構成する.....31
4.5 QRコードスキャン.....31
4.6 カスタマイズされたオブジェクトスキャンを作成.....32
4.7 警告の表示と検索.....33
4.8 視覚フィルターの使用.....34
4.9 レポートの表示と編集.....35
4.10 製品のライセンス情報を表示する.....37
4.11 データ処理領域を構成する.....37

第 5 章： 個人情報保護の概要.....38

5.1 Salesforce組織でIdentity Protectionを有効にする方法.....39
5.2 アイデンティティ保護スキャンのスケジュール設定.....39
5.3 リスクのあるIDの監視.....39
5.4 Salesforce ユーザーの ID イベントの監視.....40
5.5 個人情報漏洩アラートの監視.....41
5.6 ユーザーの危険な権限を監視する.....41

第 6 章： アプリケーションの動作を確認する.....42

6.1 ファイル保護の動作を確認する.....43
6.2 URL 保護の動作を確認する.....43

第 7 章： アンインストール.....44

7.1 権限セットの指定を削除する.....45
7.2 アプリケーションをアンインストールする.....45

第
1
章

ソリューション概要

トピック：

- 機能

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。 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。 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。 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。 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：

- Salesforceの対応エディション
- 前提条件
- 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
- アプリケーションをアップグレードする

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

Visualforceページにアクセスできる組織内のすべての有効ユーザーに [、WithSecure Cloud Protection User権限セット]を割り当てる必要があります。この権限セットには、WithSecureソフトウェアライセンスを持たないユーザーも対象としたダウンロード保護とURLクリック時保護が含まれます。WithSecure ***Cloud Protection User***バージョン3.1では、ライセンスの種類に応じてSalesforceユーザーに[WithSecure Cloud Protection for User]または [WithSecure Cloud Protection for guest user]権限セットを割り当てることができる、再設計された [ユーザー権限セット管理]ツールが導入されています。

注 : [ユーザー権限設定]ツールを使用する前に確認すべき事項:

- [WithSecure Cloud Protection ユーザー]権限は、ユーザーインターフェースを操作し、クリックタイム保護 (CTP) またはファイル ダウンロード保護を必要とするユーザーにのみ割り当てることをお勧めします。
- バッチ Apex に 200 人を超えるユーザーを挿入する場合は、自動割り当てを無効にし、権限セットツールを使用して権限セットを手動で割り当てることをお勧めします。
- 関連するすべてのユーザー グループで自動権限セットが有効になっていることを検証する必要があります。
- 新しい Salesforce ライセンスグループには、最初に手動で割り当てる必要があります。新しいユーザーを自動的にオンボーディングするには、ユーザーを作成する前に、グループの [自動割り当て] スイッチを有効にする必要があります。
- 統合ユーザーの割り当てを検証する必要があります。統合ユーザーに対しては自動割り当てが無効になっており、[WithSecure統合権限セットは]自動的に割り当てられません。
- このツールを使用しても、カスタム権限セットは移行されないことに注意してください。

***WithSecure Cloud Protection** ユーザーと **WithSecure Cloud Protection** ゲスト ユーザー*権限セットを割り当てるには、以下の手順に従います。

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] > [ツール] > [管理ツール] を開いて]、[ユーザー権限セットの管理]の [割り当て]を選択します。

   このツールには、すべての Salesforce ユーザー ライセンスの種類、合計ユーザー数、権限セットを持つユーザー数、自動割り当てを有効/無効にするオプション、ライセンスレベルですべて割り当て/すべて割り当て解除、権限セットをグローバルに削除するすべて割り当て解除が一覧表示されます。

   - ユーザー ライセンスは、ユーザー総数に基づいて降順に並べられます。
   - 自動割り当ては、ユーザーの再アクティブ化とユーザーのオンボーディングの変更時にのみ発生します。
   - デフォルトでは、新規インストールでは自動割り当てはオフになっています。アップグレードでは以前の設定が保持されます。

- このツールは、権限セットの割り当ておよび削除中にトースト通知、アラート、イベントを表示します。検証により、権限セットの割り当てに適さないライセンスタイプが特定された場合は、トースト通知のみが表示されます。
- 権限セットの割り当てが失敗した場合に電子メール通知を送信するオプションが提供されます。

アップグレード シナリオでは、現在のライセンスのスナップショットが考慮されます。

自動アップグレードが有効になっている場合、アップグレード後の自動割り当ては、現在 WithSecure User または WithSecure Guest 権限セットに割り当てられているライセンスにのみ適用されます。

作成された権限セットのカスタム クローンはこの移行プロセスでは考慮されておらず、これまで考慮されたこともありません。

アップグレード時に、システムは既存のユーザーに権限セットを割り当てます。ユーザーエンティティが変更された場合 (ユーザーの再アクティブ化またはオンボーディング) 、自動権限セットルールが呼び出されます。

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 に口グインします。
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 に口グインします。
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：

- 警告と通知の送信先を設定する
- セキュリティ警告と警告メッセージを設定する
- ファイル保護を設定する
- URL 保護を設定する
- 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の権限セットを作成する
- 製品の自動更新を設定する
- プライバシー設定を変更する
- 更新前に選択リスト値を有効化する
- URLスキャンにおけるSalesforceの制限事項への対応

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。
   - [高リスクコンテンツが検出されたときにセキュリティアラートを送信する設定は、] Salesforce クラウドから高リスクコンテンツがアップロードまたはダウンロードされたときに、管理者にアラートを送信するものです。
   - [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。

   スキャンで有害ファイルや許可されていないファイルが見つかった場合に削除するように選択した場合は、[削除された有害コンテンツをテキストファイルに置き換える」、[削除され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]、または [削除された高リスクコンテンツをテキストファイルに置き換える」をオンにして、削除されたファイルの代わりにプレースホルダーテキ

ストファイルを使用します。ファイルを編集するには、[ファイルの置き換えを設定]をクリックします。

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 高リスクファイルのサポート

攻撃者はパスワードで保護されたファイルを利用してマルウェアを拡散し、従来の検出メカニズムを回避します。WithSecure WithSecure Cloud Protection for Salesforceバージョン3.0では、パスワードで保護されたアーカイブファイルの検出、削除、ブロックに加え、PDFファイルやMicrosoft Officeファイルのアップロードおよびダウンロード時に高リスクファイルを処理するための設定可能なオプションが導入されています。

高リスクファイルの処理オプションを設定するには、以下の手順に従ってください。

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. [有害なコンテンツまたはアップロードをスキャンします (ファイル/添付ファイル)]:
    a) [有害なコンテンツが見つかった場合]に移動し、ドロップダウンリストからファイルの許可、削除、またはブロックを選択します。
    b) [高リスクコンテンツが見つかった場合] → [高リスクファイルのタイプとアップロード時のアクションを設定]に移動し、ファイルの種類ごとにアクションの種類を選択します。選択できるアクションの種類は以下のとおりです。

    - アクセスを許可、レポートのみ
    - ファイルを取り除く

    注 : 適切なアクションを選択したら、変更を [保存して]ください。

5. [ダウンロードファイル内の有害コンテンツをスキャン]する
    a) [有害なコンテンツが見つかった場合]に移動し、ドロップダウンリストからファイルを許可する、削除する、またはブロックするかを選択します。
    b) [高リスクコンテンツが見つかった場合」→[高リスクファイルの種類とダウンロード時のアクションの設定]に移動し、ファイルの種類ごとにアクションの種類を選択します。選択できるアクションの種類は以下のとおりです。

    - アクセスを許可、レポートのみ
    - ファイルを取り除く

- [ブロックファイル]

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。
- 新規インストールの場合、設定は [アクセスを許可」と「レポートのみ]です。
- バージョン **2.6**以降からのアップグレードの場合: Microsoft Office および PDF ファイルはアップロードとダウンロードの両方で [削除のみ]に設定され、アーカイブ ファイルの設定は既存の構成に従います。
- **2.6** より前のバージョンからのアップグレードの場合: デフォルトはダウンロード時に [ファイルを削除]です。

重要：

[管理]→[ファイル保護]→[通知]に進むと、高リスクファイルに関連する 2 つの新しい設定があることがわかります。

- [高リスクコンテンツが検出された場合、セキュリティアラートを送信します]。これはデフォルトでは無効になっています。ただし、設定された内容に基づいてアラートとイベントが生成され、高リスクコンテンツが検出、ブロック、または削除されたタイミングとファイルの種類情報が通知されます。
- [削除された高リスクコンテンツを、デフォルトで有効になっているテキスト ファイルに置き換えます]。

メール通知設定の詳細については、以下を参照してください。警告と通知の送信先を設定する（14 ページ）そして セキュリティ警告と警告メッセージを設定する（14ページ）。

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 : `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。
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 : `WORD_X`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、Salesforce AppExchange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。

3.9 更新前に選択リスト値を有効化する

WithSecure Cloud Protection for Salesforceの新リリースでは、管理パッケージ内の既存の項目に新しい選択リスト値が導入されています。これらの値を確実に利用し、機能させるには、管理パッケージ内で新しく導入された選択リスト値を有効化してください。この手順は、プラットフォームの制限により、アップグレードプロセス中に自動的に有効化されないため必須です。

重要: このアクティビティは、Salesforce 組織でアップグレード後ではなく、アップグレードプロセスの前に実行する必要があります。

Salesforce 組織管理者は、次の選択リスト値を手動で有効化する必要があります。

- [フィールド:]AFSC_URL_Scan_Log_c.Action_c。
- [値:]削除されました。

管理パッケージで新しく導入された選択リスト値を有効にするには、次の手順に従います。

1. [セットアップ]に移動します。
2. [オブジェクト マネージャー]に移動します。
3. FS_URL_Scan_log_cを選択します。
4. [フィールドと関係]をクリックします。
5. [Action_c]を選択します。
6. 非アクティブな値のセクションに Removed の値がリストされているかどうかを確認します。
   - 値が存在する場合は、値 Removedをアクティブにします。
   - 値 Removedが欠落している場合は、新しい選択リスト エントリを作成します。

     注 : 新しい選択リスト エントリを作成するには、[値]セクションに移動 > [新規]をクリック > [広告値 が削除されました] > [保存]をクリックします。

新しい値「削除」が有効になります。

3.10 URLスキャンにおけるSalesforceの制限事項への対応

WithSecure Cloud Protection for Salesforceバージョン 3.1 では、特に Salesforce の管理制限に達した場合の URL イベント障害の処理が改善されました。

これは次のシナリオで発生する可能性があります。

- 電子メールを一括送信する際、顧客コードは 1 回の呼び出しで複数の電子メールを送信 (またはタスクを作成) し、Salesforce トリガーを複数回トリガーして、管理制限を超える可能性があります。
- メールメッセージはフロー経由で送信されます。バッチメールと同様に、メールとタスクのスキャンが必要です。また、Futures が呼び出される場合もあります。キュー可能オブジェクトが1つとFuturesが50個では不足する場合、Salesforce はエラーをスローします。
- 200 件を超えるレコードを一括でスキャンする必要があるオブジェクトを作成しているとき: これにより、レコードの処理が 200 件ごとにトリガーされます。最初のチャンクは Queueable を使用しますが、2 番目のチャンクは起動できません。
- デフォルトでは、すべての詳細設定がオフになっており、管理制限に達した場合にのみアラートが作成されます。

これらの課題に対処するため、Salesforce のガバナンス制限に達した場合に URL スキャンを延期する高度な設定を 3.1 リリースで導入しました。カスタム設定を作成するには、以下の手順に従ってください。

1. [セットアップ] > [カスタム設定] > [新規]に移動します。
2. [ラベル]として [詳細設定]を選択します。
3. [API 名を][FS_AdvancedSettings_c]に設定します。
4. 表示設定で [公開]を選択し、[保存」します]。
5. [新規]を選択して、次のカスタム フィールドを作成します。

フィールドラベル	[**API**名]	データ型
リソース制限時にURLスキャンを延期する	リソース制限時にURLスキャンを延期する	チェックボックス
遅延URLスキャンの開始が許可される	遅延URLスキャンの開始が許可される	チェックボックス
isHourlyDeferredUrlScanEnabled	isHourlyDeferredUrlScanEnabled	チェックボックス
URL遅延スキャンスケジュールの遅延（分）	URL遅延スキャンスケジュールの遅延（分）	数値とデフォルトは10

注：推奨設定:

- [**DeferURLScanWhenResourcesLimited__c**]: True（必須）; この設定は、遅延動作に使用されます。ブール型データ型です。
- [**isAllowedToStartDelayedDeferredUrlScan__c**]: True (必須); キュー可能/将来の制限に達すると、この設定により延期されたジョブが作成されます。ブール型データ型。
- [**isHourlyDeferredUrlScanEnabled__c**]: True ですが、メタデータ情報は管理者名に設定されます。これは、[**isAllowedToStartDelayedDeferredUrlScan__c**]設定がオフの場合にのみ機能します。クォータが使い果たされると、時間単位プロセッサの遅延レコードが作成されます。ブール型。
- [**URLDeferredScanScheduleDelayInMinutes__c**]: [**isAllowedToStartDelayedDeferredUrlScan__c**]設定と連動します。スケジュールされたジョブは設定に従って動作しますが、保留中のレコードがキュー可能なジョブで処理される場合、最大遅延時間は10分です。この設定は、新しくスケジュールされた遅延ジョブをどのくらい先まで実行するかを決定します（デフォルト：10分）。数値データ型は数値です。

重要：上記のシナリオでは、一括メール内のURLスキャンのみが対象となります。添付ファイルがある場合は、[管理] > [ファイル保護] > [] →「詳細設定」→ [送信メール内のファイルをスキャン]を無効にし、これらの詳細設定を使用してURLスキャンを適切に処理することをお勧めします。

第
4
章

アプリケーションを使用する

トピック：

- コンテンツの分析
- WithSecure Cloud Protection 接続アプリの使用
- クリック時の URL 保護の構成
- 高度な脅威分析を構成する
- QRコードスキャン
- カスタマイズされたオブジェクトスキャンを作成
- 警告の表示と検索
- 視覚フィルターの使用
- レポートの表示と編集
- 製品のライセンス情報を表示する
- データ処理領域を構成する

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（19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（19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、またはファイルやウェブサイトが誤って検出・評価されていると思われる場合は、いつでも「サンプルを送信」ウェブサイトを使用して分析のために送信できます。サンプル送信の受理基準については、以下をご確認ください。

アプリが動作しないケース (接続されたアプリがない、ファイルサイズが12MBを超えるなど) に関する情報を追加してください。ファイルの内容と提出理由を簡単に説明してください。可能であれば、検証のためにファイルハッシュまたはサンプルIDも記載してください。

注: エンタープライズサポートをご利用の場合は、カスタマーサクセスマネージャーにご連絡いただき、Withsecureのマルウェアアナリストによる分析を受けてください。

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。

4.1.7 ゲストおよびコミュニティユーザー向けのファイル保護の高度なスキャン設定

Secure Cloud Protection for Salesforce バージョン 3.1 では、ゲストおよびコミュニティ ユーザー向けのファイル保護スキャン設定が導入されました。

組織内で新しい設定を有効にするには、以下の手順に従ってください。

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. [アプリランチャー]を開き、[クラウド保護を開きます。]
3. 次の操作を行うには、[管理] > [ファイル保護] > [詳細設定]に移動します。
   - ゲストユーザーとコミュニティユーザーのファイルスキャンの遅延時間を選択します。遅延時間は1分、3分、5分、10分から選択できます[。また、デフォルトで設定されている「遅延なし]を選択することもできます。
   - [コンテンツスキャンが完了する前にゲストユーザーがファイルをダウンロードできるよう]にする設定をオンにすることができます。この設定はデフォルトではオフになっています。
   - [コンテンツスキャンが完了する前に、内部ユーザーが画像ファイル（**.jpg**、**.png**、**.gif**）をダウンロードできるよう]にする設定をオンにすることができます。この設定はデフォルトではオフになっています。

   注：この設定が構成されたゲスト ユーザーと内部ユーザーの両方に、WithSecure Cloud Protection for User 権限セットが割り当てられていることを確認します。

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。

注：WithSecure Cloud Protection Connected App初めてインストールする場合は、**Salesforce** 管理者プロファイルを使用してすべての手順を実行することをお勧めします。接続アプリが正常にインストールされ、ローカルにリンクされたら、アプリを管理するための専用の統合プロファイルを割り当てることができます。

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 Integration***を選択します。
   - [プロファイル]の場合は、***Minimum Access - API Only Integrations***または同じライセンスを持つ他のプロファイル/カスタム プロファイルを選択します。

     注 : 統合ユーザーライセンスは、UIアクセスなしで外部システムからSalesforceに接続するためのものです。Salesforce統合ユーザーライセンスはUIアクセスを許可せず、システム間統合向けに特別に設計されています。バックエンドからSalesforceと通信するには、アプリケーションに[すべてのファイルのクエリ]（Salesforceヘルプ）および[すべて表示」（Salesforceヘルプ）権限が必要です。

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。

   注 : インストールされている WithSecure Cloud Protection for Salesforceアプリケーションのバージョンを確認します。
   - インストールされている **WithSecure Cloud Protection for Salesforce** アプリのバージョンが **2.5**以上の場合は、[**WithSecure Cloud Protection** 統合ユーザー]権限セットを統合ユーザーに割り当てます。
   - インストールされているアプリのバージョンが **2.4.1** 以下の場合は、以下の手順に従ってください。
     a. **WithSecure Cloud Protection** 管理者権限セットを複製し、複製した権限セットでVisualforceページへのアクセスを削除します。
     b. 複製された権限セットと **WithSecure Cloud Protection** 接続アプリケーションを統合ユーザーに割り当てます。

4.2.2 組織内での WithSecure Connected App のローカルインストール

Cloud Protection for Salesforce アプリをローカルにインストールするには、以下の手順に従います。

1. 必要な新しい権限セットを作成します（アンインストールされた接続アプリケーションの承認新しい「アンインストールされた接続アプリの承認」権限セットを作成します（29ページ））
2. 権限セットを管理者またはSalesforceライセンスを持つユーザーに割り当てます(接続済みアプリのユーザーアカウントの作成（27ページ）& 接続されたアプリへの権限の割り当て（29ページ）&）
3. 接続されたアプリを接続する（WithSecure Cloud Protection Connected App の使用（30ページ））
4. 接続されたアプリをインストールします（Connectedアプリのインストール（31ページ））

注: インストール後、必要に応じて、接続済みの管理ユーザーを統合ユーザーに切り替えることができます。また、管理者は接続を切断し、接続済みアプリケーション用に作成された専用ユーザーが切断後に再接続することもできます。以下の手順では、接続済みアプリケーション用の専用ユーザーを作成し、必要な権限セットをこの専用ユーザーに割り当てる方法について説明します。

注 : **WithSecure** 接続アプリを組織内でローカルにインストールする必要があるのはなぜですか?

Salesforceは2025年9月上旬より、アンインストールされた接続アプリケーションの使用を制限します。この使用制限により、エンドユーザーはアンインストールされた接続アプリケーションを使用できなくなります。

Salesforce組織でAPI管理が有効になっている環境で接続アプリケーションを有効化しようとすると、OAuthエラーが表示されるようになります。エラーメッセージは次のようになります。

OAuthエラーのため、認証できません。詳細については、Salesforce管理者にお問い合わせください。OAUTH_APPROVAL_ERROR_GENERIC: 認証中に予期しないエラーが発生しました。しばらくしてからもう一度お試しください。

または OAUTH_APP_BLOCKEDおよび error_description=this+app+is+blocked+by+admin。

これは、**WithSecure** 接続アプリケーションを組織自体にインストールすることで回避できます。接続アプリケーションのインストールについては、以下のセクションの手順をご確認ください。

4.2.3 新しい「アンインストールされた接続アプリの承認」権限セットを作成します

以下の手順に従って、新しい[アンインストールされた接続アプリの]承認」権限セットを作成します。

1. [ホーム]に移動し、[ユーザー] → [権限セット]を検索します。
2. [アンインストールされた接続アプリを承認]という名前の権限セットを作成します。
3. ライセンスとして [**Salesforce**]を選択します
4. [システム権限]に移動して [編集]をクリックし、[アンインストールされた接続アプリを承認]チェックボックスをオンにします。
5. 変更を保存します。
6. 重要: APIアクセス制御が有効になっている場合にのみこの手順を実行し、そうでない場合は次の手順に進んで続行します。

   [**API** アクセス制御]が有効になっており、次のいずれかの場合:

   - 管理者が承認したユーザーの場合、API アクセスを許可リストに登録された接続アプリのみに制限します。

     または

   - 顧客とパートナーに対して、API アクセスをインストール済みの接続アプリのみに制限します

   チェックが入っている場合は、次の手順を実行してください。

   [権限セット] > [アンインストールされた接続アプリケーションの承認] > [システム権限の] > [編集]に移動して、[任意の **API** クライアントを使用する]チェックボックスをオンにします。
7. [割り当ての管理]をクリックし、ユーザー([システム管理者]または [**Salesforce**]ライセンスを持つ他のユーザー) を選択します。

4.2.4 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] > [者ユーザー] > [権限セット]に移動します。
3. 新しいアクセス許可セットを作成するには、[新規]を選択してください。
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。

   注: ユーザーが [システム管理者]または [**Salesforce API**統合ユーザーの]場合、この設定はすでに有効になっています。その他のユーザーの場合は、[**API**有効]オプションが選択されていることを確認してください。
9. [保存] を選択します。

10. アプリセクションで [アプリの権限]を開き、[すべてのファイルを照会するをチェックします。]
11. 権限変更確認ダイアログで [保存]を選択すると、追加のシステム権限とオブジェクト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. 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。
13. 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。
14. [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。
15. [使用可能な権限セット]のリストで、***WithSecure Cloud Protection Integration User***と、前に **WithSecure Cloud Protection** 接続アプリケーション用に作成した権限セット、および 「アンインストールされた接続アプリケーションの承認」用の権限セットを選択します。

    統合ユーザーの WithSecure Cloud Protection for Salesforceユーザー インターフェース アクセスを削除する必要がある場合は、**WithSecure Cloud Protection** 管理者権限セットを複製して新しい [権限セット]を作成し、それを **WithSecure Cloud Protection** 管理者の代わりにユーザーに割り当てます。
16. [保存] を選択します。

4.2.5 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]に移動してください。
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。

   それでも接続されない場合は、トラブルシューティングのセクションを確認し、プロファイルの ログイン **IP** 範囲を追加して、上記の手順を試してください。

   注 :

   以下の手順は、組織によってIPアドレス制限が設定されている場合にのみ適用されます。IPアドレスに関する情報については、テクニカルアカウントマネージャーにお問い合わせください。

   a. クラウド保護 IP アドレスがこれら両方で許可されていることを確認します (使用中の場合)
      - [セキュリティ] > [ネットワーク アクセスの] > [許可された **IP** 範囲] > [を設定します]
      - [ユーザー] > [プロファイル] > [の設定。**Cloud**] > [**Protection Integration** ユーザーの] > [ログイン **IP** 範囲]。

        重要 : 以前から何らかの制限がある場合にのみこれを追加する必要があります。

   b. バックエンドIPアドレスを許可リストに登録すると、すべてが正常に動作するようになり、再度接続を試みることができます。
   c. 情報アラートが作成され、[**Analytics**] > [アラート]で確認できるようになります。
   d. これで、接続されたアプリケーションを組織にインストールする手順に進むことができます (Connectedアプリのインストール (31ページ))

4.2.6 Connectedアプリのインストール

Connected アプリをインストールするには、以下の手順に従ってください。

[接続アプリの **OAuth** 使用法の] > [セットアップ]に移動し [、**WithSecureTM Cloud Protection**]アプリの横にある [インストール]ボタンをクリックします。

注 : これにより、アプリが組織内に自動的にインストールされます。確認するには、[接続済みアプリケーションの] > [設定]に移動し、**WithSecureTM Cloud Protection** アプリが表示されていることを確認してください。

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。

この機能強化は、次の新機能と連携して機能します。

- ファイル (PDF および Microsoft Office スイート形式のファイル) 内に埋め込まれた悪意のある QR コード URL を識別します。

  注: この機能は、QRコード内のURLを抽出し、URLのレピュテーションをチェックします。ファイル内のQRコードスキャンに対して、アラートとイベントが生成されます。

- QR コード画像内の短縮 URL 保護。

  注: この機能は、すべての主要な短縮 URL プロバイダーをサポートし、再帰分析を実行して URL の評判を提供します。

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。

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。
   WithSecure 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、現在の口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 視覚フィルターの使用

WithSecure Cloud Protection for Salesforceバージョン 3.1 では [、アラート]、[ファイル イベント]、[URL イベント]、[ID イベント]、および [ID]ページにビジュアル フィルターが導入されています。

ビジュアル フィルターを見つけて、その使用方法を知るには、以下の手順に従ってください。

1. [アナリティクス]に移動し、次のいずれかを選択します。
   - 警告
   - ファイル イベント
   - URL イベント
   - IDイベント
   - ID
2. [フィールドの選択を]選択し、サポートされているフィルターを配置して、特定のフィルターを適用します。
3. サポートされているフィルターを選択したら、[フィルターの適用」をクリックします。]

   注 : サポート演算子は [Equal]です

   注 : フィルターは合計で最大10個まで適用できます。フィルターは、アナリティクスページを開いている間は有効なままです。[アラート]、[ファイルイベント、][URLイベント]を切り替えてもフィルターはリセットされません。ただし、別のメインページ (例 : [サマリー)]に切り替えると、すべてのフィルターがクリアされます。

   サポートされているフィルターのリストを以下に示します。

ページ	サポートされているフィルター	追加情報
警告	日付/時刻、重大度、ソース、理由 (テキストボックス、255文字) 、ユーザー (テキストボックス、255文字)	
ファイル イベント	日付/時刻、アクション (選択リスト) 、判定、ファイルタイプ (テキストボックス、255文字) 、方向、場所 (テキストボックス、255文字)	アクション (選択リスト) は翻訳サービスではサポートされていません。

URL イベント	日付/時刻、アクション、判定、方向、場所 (テキストボックス、255 文字)	場所はカスタム オブジェクトをサポートします。
IDイベント	日付/時刻、リスク、ユーザー (テキストボックス、255文字)	
ID	ユーザー (テキストボックス、255 文字)、最高リスク、日時、侵害、役割 (テキストボックス、255 文字)、プロフィール (テキストボックス、255 文字)、メール (テキストボックス、255 文字)	

4.9 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

4.10 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。

4.11 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

個人情報保護の概要

トピック：

- Salesforce組織でIdentity Protectionを有効にする方法
- アイデンティティ保護スキャンのスケジュール設定
- リスクのあるIDの監視
- Salesforce ユーザーの ID イベントの監視
- 個人情報漏洩アラートの監視
- ユーザーの危険な権限を監視する

WithSecure Cloud Protection for Salesforceの Identity Protection は、組織が侵害されたユーザー アカウントによるリスクを監視し、軽減するのに役立ちます。

侵害されたアカウントは、攻撃者に組織へのアクセスを許可し、社内フィッシング攻撃、ランサムウェア、なりすまし攻撃などを可能にします。これらの攻撃は、正規の企業アカウントが利用されるため、検知が困難です。たった1つのアカウントが侵害されると、Salesforce環境全体が危険にさらされる可能性があります。

このニーズに対応するため、WithSecure Cloud Protectionアイデンティティ保護では、Salesforceのメールアドレスを使用して、標準ユーザーとコミュニティユーザーの侵害を監視できます。この機能は、最初に過去12か月間の侵害記録を表示し、その後は最近の侵害記録を表示します。新しい侵害記録は毎週監視されます。アイデンティティ保護のフェーズ1では、最大50,000ユーザーをサポートします。

個人情報保護のためのスキャンをスケジュール設定できます。Salesforce WithSecure Cloud Protection for Salesforce、SHA-256ハッシュ形式でメールアドレスを収集し、侵害記録を検索して結果を返します。各侵害記録には以下の情報が含まれます。

- 公開日
- 臨界性
- 所在地
- 露出したユーザー
- ユーザーの役割とプロフィール
- 違反内容の説明

WithSecure Cloud Protection for Salesforceの Identity Protection 機能は、内部 (標準) ユーザーとコミュニティ ユーザーの両方をサポートします。

個人情報保護を有効にするには、次のことが必要です。

- 接続されているアプリが有効になっていることを確認します。
- アクティブな WithSecure Cloud Protection for Salesforce ユーザーライセンスが、侵害チェックの有効化を必要とするユーザータイプと一致していることを確認します。

5.1 Salesforce組織でIdentity Protectionを有効にする方法

Salesforce組織でID保護を有効にするには、以下の手順に従ってください。

1. アプリランチャーを開き、[クラウド保護を開きます。]
2. [管理]に移動して、[Identity Protection] を開きます。]
3. トグルをアクティブにして、[標準ユーザーの侵害を監視]および/または[コミュニティユーザーの侵害を監視]できるようにします。

   注：組織が [すべてのユーザー]に設定されており、ユーザーの合計数が購入したユーザー ライセンス数以下の場合は、標準またはコミュニティ、あるいは両方のタイプのユーザーの電子メールをスキャンできます。

   注：組織が [選択的ユーザー]モードであり、ユーザー ライセンスの数が購入したユーザー数以下の場合は、すべての標準ユーザーまたはコミュニティ ユーザー、または両方のタイプのユーザーの電子メールをスキャンできます。

   重要：統合および自動化ユーザーは、ID 保護侵害スキャンから除外されるため、管理ライセンスの数が一致しません。

5.2 アイデンティティ保護スキャンのスケジュール設定

Identity Protection スキャンをスケジュールするには、以下の手順に従ってください。

1. [アプリ起動]に移動して [クラウド保護]を開きます
2. [管理]に移動して、[アイデンティティ保護]を開きます
3. [違反をチェックする曜日と時間]を設定する

   注：以下の点にご注意ください:

   - Identity Protection の侵害ジョブは開始後、完了まで3日かかります。つまり、次のスケジュールされたジョブは3日後にしか実行できません。すべての侵害記録は表示されますが、IP ジョブ完了アラートは3日後にトリガーされます。
   - バッチの開始時と終了時に、Cloud Protection for Salesforce アプリケーション内にアラートが表示され、侵害の検索が進行中か完了しているかを把握できるようになります。
   - スケジュールされたスキャンの開始後3日以内に、ID保護は検出された侵害に関する更新情報を提供します。

5.3 リスクのあるIDの監視

WithSecure Cloud Protection for Salesforceバージョン 3.0 では、リスクのある ID を監視するための新しい[ID]セクションが導入されました。このセクションには、侵害の危険にさらされたユーザー、最も高い侵害リスク、最新の侵害日、侵害の総数、役割とプロファイル、侵害されたメール、そして詳細な侵害履歴に関する情報が表示されます。

危険にさらされている ID を監視し、侵害履歴を表示するには、以下の手順に従ってください。

1. [アプリ起動画面]を開き、[クラウド保護」を選択します。]
2. [アイデンティティ」へ移動します。]
   - [検索を]使用して結果を絞り込みます。

     注：サポートされる値は次のとおりです:

     - ユーザー
     - 最高リスク
     - 時間
     - 違反
     - 役割
     - プロフィール

- メール

  注：たとえば、標準ユーザーのすべての侵害を見つけることができます:"HIGHEST_RISK=Critical、PROFILE=Standard User。

- ユーザーの違反履歴を確認するには、[表示]をクリックします。

  重要：ユーザーの侵害履歴を開くと、次のようなメタデータを含む [詳細]も確認できます。

  - 違反が発生したと思われる日付を示す 違反日
  - 取り込まれた各侵害の タイトル。サードパーティのセキュリティ調査チームが侵害のタイトルを文書化するため、これは侵害の詳細を開示できる場合にのみ利用可能であり、そうでない場合は一般的なタイトルになります。
  - 侵害を受けた組織の **Web** サイト(利用可能な場合)。
  - 取得日。サードパーティのセキュリティ調査チームが侵害されたデータを最初に取得した日付です。
  - データが侵害された方法を分類する 侵害カテゴリ (*コンボリスト*、*流出*、*露出*、*情報窃盗*、*フィッシング*、*スクレイピング*、*または不明_**)
  - 信頼性は、侵害の発生源に対する信頼度を表す値です。使用可能な値は、***Low***、***Medium***、***High***です。
  - 侵害をコンボリスト、侵害、またはマルウェアに分類する 侵害の主なカテゴリ。
  - 公開日：この侵害が公表された日付を示します。通常、以下の ***media_urls***リストにメディアのURLが示されます。
  - タイプは、侵害が *公開か 非公開か*を示します。*公開*侵害はインターネット上で簡単に発見できるものであり、*非公開*侵害は多くの場合、サードパーティのデータベースプロバイダーのみが把握できるものです。
  - レコード数は、サードパーティのデータベースが解析し、この特定の侵害から取得したレコードの数を示します。この情報は、解析、正規化、重複排除の実行後に利用できます。
  - 機密ソースは、侵害ソースが機密であるかどうかを示します。
  - 消費者カテゴリは、消費者製品マッピングの分類を提供します。

5.4 Salesforce ユーザーの ID イベントの監視

WithSecure Cloud Protection for Salesforceバージョン 3.0 では、Salesforce ユーザーの侵害記録を監視するための [**ID イベント**]が導入されています。

Salesforce ユーザーの侵害記録を監視するには、以下の手順に従ってください。

1. [アプリ起動画面]を開き、[クラウド保護」を選択します。]
2. [**Analytics**]に移動し、[**Identity Events** を開きます。]

   各イベントには、侵害の日時、リスクの種類、侵害の理由、影響を受けたユーザー、その他の侵害情報の詳細が記載されています。[検索]フィールドを使用して結果を絞り込むことができます。検索フィールドでサポートされている値は次のとおりです。

   - 時間
   - リスク
   - 理由
   - ユーザー

     注：たとえば、特定のユーザーの重大な違反をすべて見つけることができます:「RISK=Critical、USER=John Doe」。

5.5 個人情報漏洩アラートの監視

アイデンティティ保護侵害ジョブはスケジュールされたスキャン日時に実行されるため、侵害チェックジョブが開始および完了したとき、またはユーザーが新しい侵害に直面したときに、アイデンティティ保護機能によってアラートが生成されます。

侵害アラートを監視するには、以下の手順に従ってください。

1. [アプリ起動画面]を開き、[クラウド保護」を選択します。]
2. [**Analytics**]に移動して、[アラート]を開きます。
3. 特定のアラートの詳細情報を確認するには、[表示]をクリックします。

   注：アラートの詳細モーダルには、侵害の日時、重大度、理由、ソース、侵害にさらされたユーザー、侵害の中で最も高いリスク、ユーザーごとの侵害の合計数、ユーザーの役割、ユーザープロファイル、および完全な侵害履歴のIDセクションへのリンクが表示されます。

5.6 ユーザーの危険な権限を監視する

ID保護機能は、ユーザーに割り当てられた権限セットを評価し、リスクの高いシステム権限を含む権限セットにフラグを立てます。

ユーザーの危険な権限を確認するには、以下の手順に従ってください。

1. [アプリランチャー]を開き、[クラウド保護を開きます。]
2. [**ID**]に移動し、[**Risky**のアクセス許可」を開きます。]

   フラグが立てられた権限は、ユーザーごとに [危険な権限]タブと [概要]タブに表示されます。

   [リスクの高い権限]タブには、ユーザーが保持しているリスクの高い権限と、それらの権限が属する権限セットおよび権限セットグループが表示されます。

   [概要]タブには、メール漏洩のリスクや WithSecure Cloud Protection for Salesforceライセンスの不足など、その他のリスクシグナルとともに、リスクの高い権限が表示されます。複数のリスクシグナルでフラグが立てられたユーザーは、単一のシグナルでフラグが立てられたユーザーよりも、全体的なリスクが高いと判断されます。

第
6
章

アプリケーションの動作を確認する

トピック：

- ファイル保護の動作を確認する
- URL 保護の動作を確認する

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。

6.1 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。

6.2 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、両方のリンクを開いてみてください。「有害なウェブサイトがブロックされました」と「許可されていないウェブサイトがブロックされました」という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
7
章

アンインストール

トピック：

- 権限セットの指定を削除する
- アプリケーションをアンインストールする

このセクションでは、削除の手順を説明します。WithSecure Cloud Protection for Salesforce貴社から。

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

7.1 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。

7.2 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 にログインします。
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。