Cloud Protection
By WithSecure

Cloud Protection for Salesforce

Administrator's Guide

目次

1 ソリューション概要 5
1.1 機能 5
2 導入 9
2.1 Salesforceの対応エディション 9
2.2 前提条件 9
2.2.1 Chatter 機能を有効にします 9
2.2.2 Chatter 設定で、投稿とコメントの編集を許可します 10
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 10
2.2.4 他の言語を設定する 10
2.3 アプリケーションをインストールする 11
2.4 権限セットとライセンスの指定 12
2.4.1 Cloud Protection User 権限セットを指定する 12
2.4.2 Cloud Protection Admin 権限セットを指定する 13
2.4.3 Cloud Protection ライセンスを指定する 13
2.5 アプリケーションをアップグレードする 15
3 アプリケーションの設定 17
3.1 アラートと通知の受信者を構成する 17
3.2 セキュリティアラートと警告メッセージを構成する 17
3.3 ファイル保護を設定する 18
3.3.1 リスクの高いファイルのサポート 21
3.4 URL 保護を設定する 22
3.5 手動スキャンとスケジュールスキャンの設定を変更する 23
3.6 マニュアルスキャンの権限セットを作成する 25
3.7 製品の自動更新を設定する 25
3.8 プライバシー設定を変更する 26
3.9 アップグレード前の選択リスト値の有効化 27
3.10 URL スキャンにおける Salesforce の制限への対応 27
3.11 ファイルスキャンにおける Salesforce の制限への対応 29
4 アプリケーションを使用する 31
4.1 コンテンツの分析 31
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 31
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 32
4.1.3 スキャンからファイルを除外する 32
4.1.4 誤検知と誤検知の報告 33
4.1.5 隔離機能を使用する 34
4.1.6 スキャン結果のキャッシュを消去する 34
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 35
4.2 Cloud Protection 接続アプリの使用 35
4.2.1 接続済みアプリのユーザー アカウントの作成 35
4.2.2 組織内での Connected App のローカルインストール 37
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 37
4.2.4 接続されたアプリへの権限の割り当て 38

4.2.5 Cloud Protection Connected App の使用 39
4.2.6 Connectedアプリのインストール 39
4.3 クリック時の URL 保護の構成 40
4.4 高度な脅威分析を構成する 40
4.5 QRコードスキャン 41
4.6 カスタマイズされたオブジェクトスキャンを作成 41
4.7 警告の表示と検索 43
4.8 視覚フィルターの使用 44
4.9 レポートの表示と編集 45
4.10 製品のライセンス情報を表示する 47
4.11 データ処理領域を構成する 47
5 個人情報保護の概要 49
5.1 Salesforce 組織で Identity Protection を有効にする方法 49
5.1.1 侵害モニタリングを有効にする 50
5.1.2 ユーザーアクセスおよび権限スキャンを有効にする 50
5.2 Identity Protection スキャンのスケジュール 51
5.2.1 侵害スキャンをスケジュールする 51
5.2.2 ユーザーアクセスおよび権限スキャンをスケジュールする 51
5.3 リスクにさらされている ID の監視 51
5.4 Salesforce ユーザーの ID イベントの監視 52
5.5 個人情報漏洩アラートの監視 53
5.6 ユーザーの危険な権限を監視する 53
6 アプリケーションの動作を確認する 55
6.1 ファイル保護の動作を確認する 55
6.2 URL 保護の動作を確認する 55
7 アンインストール 57
7.1 権限セットの指定を削除する 57
7.2 アプリケーションをアンインストールする 57

第 1 章 ソリューション概要

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統合・拡張するため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。

Cloud Protection for Salesforce は、Salesforce クラウドに入出力され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、貴社、パートナー、またはお客様に対するサイバー攻撃に使用されないように保護します。

本ソリューションは、Salesforce アプリケーションと WithSecure Security Cloud で構成されています。WithSecure Security Cloud は、ファイルおよび 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。Cloud Protection for Salesforce アプリケーションは、貴社が使用している Salesforce Sales Cloud、Service Cloud、または Experience Cloud（旧 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、デジタル脅威の高度なデータベースを構築しています。このデータベースにより、グローバルなサイバー脅威のリアルタイムなビューが提供されます。

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な脅威状況の変化に迅速に対応します。例えば、当社のヒューリスティックおよび振る舞い分析が新しいゼロデイ攻撃を検出すると、この情報がすべてのお客様と共有されます。これにより、高度な攻撃が最初に検出されてから短時間で無効化することができます。

本ソリューションは遅延を削減するように設計されており、Salesforce の利用に影響を与えません。ファイルやコンテンツを分析する際、本ソリューションは WithSecure Security Cloud を活用したマルチステージ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。例えば、ゼロデイマルウェアやその他の高度な脅威による攻撃を防ぐために設計された Cloud Sandboxing テクノロジーによる詳細な分析は、ハイリスクファイルのみに対して実行されます。

1.1 機能

Cloud Protection for Salesforce は、共有責任モデルのもとでセキュリティの責任範囲を果たすための理想的なソリューションです。単なるウイルス対策ソフトウェア以上の機能を提供します。本ソリューションは Salesforce とシームレスに統合され、ミドルウェアを必要としません。

ファイル保護	本ソリューションは、Salesforce 内のファイルに対して高度な保護を提供します。マルウェア、ランサムウェア、エクスプロイト、および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ーエクスペリエンスへの影響を最小限に抑えながら、アップロードおよびダウンロードされたファイルを自動的にスキャンします。 本ソリューションは、Salesforce プラットフォームにアップロードされたファイル内の添付ファイル内に隠されている可能性のある悪意あるリンクを検出してブロックすることで、セキュリティを向上させます。

	注：ファイル内の悪意あるリンクの検出を機能させるには、高度な脅威分析（ATA）を有効にする必要があります。
URL 保護	本ソリューションは、悪意ある URL がネットワークを侵害する前に、そのアクセスを分析してブロックします。分析はゼロレイテンシで行われ、非常に少ないリソースしか消費しません。 URL 保護は、Salesforce の標準項目やオブジェクトを超えて拡張され、テキスト、テキストエリア（ロングおよびリッチの両方）、URL 項目を含むカスタム設定にも対応しています。
短縮URL内の脅威を防止	短縮 URL はセキュリティ対策を回避するためにしばしば使用されます。本ソリューションは、その中に隠された脅威を特定して無効化します。これは URL 保護機能にシームレスに統合されています。
アイデンティティ保護	本ソリューションは、Salesforce ユーザーのアイデンティティリスクを監視します。サードパーティのデータ侵害に晒されたユーザーを特定し、不適切な権限割り当てや認証の弱点（多要素認証（MFA）やシングルサインオン（SSO）の欠如など）を検出することで、侵害されたアカウントが悪用される前に手打つことができます。
脅威インテリジェンス チェック	数千万のセンサーから収集されたリアルタイムの脅威インテリジェンスを活用することで、発生から数分以内に新たな脅威や最新の脅威を特定し、常に進化する脅威に対して優れたセキュリティを保証します。
マルチエンジン高度ウイルス対策	Cloud Protection by WithSecueのテクノロジーは、振る舞い分析と複数のセキュリティ層を使用して、標的型攻撃で使用されるエクスプロイトや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	ハイリスクファイルが検出されると、Security Cloud内の WithSecure Cloud Sandboxing テクノロジーによってより詳細な分析が行われ、不必要な遅延を発生させることなくゼロデイマルウェアや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	セキュリティまたはコンプライアンスポリシーに従って許可されていない、危険なコンテンツや不適切なコンテンツの検出とブロックを可能にします。許可されていないファイルは、ファイルタイプまたは拡張子に基づいて除外フィルタリングできます。
オンデマンドおよびスケジュールスキャン	Salesforce のファイルおよび添付ファイルは、いつでも、あるいは事前に設定した間隔で、有害なコンテンツや許可されていないコンテンツがないかスキャンできます。作成日時や更新日時、ファイルタイプ、または場所に基づいて、スキャンするファイルを選択できます。
隔離管理	ファイル保護によって削除された有害なコンテンツや許可されていないコンテンツは、隔離管理ツールを使用して表示および復元できます。
アラートのファイル置換	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、置換ファイルのオブジェクト ID がアラートの詳細にレポートされます。

動的な分析とレポート	動的な分析とレポートにより、Salesforce コンテンツの全体的なセキュリティ概要が提供され、セキュリティ戦略を実践しながら追跡する機会が得られます。
アラート通知	豊富なレポート、高度なセキュリティ分析、および完全な監査ログにより、システム管理者は Salesforce 内の脅威に対応し、未知のソースからの攻撃を調査することができます。 管理者およびセキュリティ部門に送信される電子メールアラートにより、セキュリティインシデントのレポートを自動化できます。
自動更新	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	Cloud Protection by 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。
迅速かつ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

本セクションでは、Cloud Protection for Salesforce を組織に導入するための手順について説明します。

アプリケーションの導入には、以下のステップが含まれます:

- アプリケーションのインストール
- 権限セットとライセンスの割り当て
- アプリケーション設定の構成

以前のバージョンからアップグレードする場合は、2.5 アプリケーションをアップグレードするを参照してください。

2.1 サポートされている Salesforce エディション

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

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

- Enterprise
- Performance
- Unlimited
- Developer

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

2.2 前提条件

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

2.2.1 Chatter 機能を有効にする

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

Chatter 機能を有効にする手順:

1. システム管理者アカウントで Salesforce にログインします。
2. 組織の設定に移動し、[設定] を選択します。
3. [機能設定] > [Chatter] > [Chatter 設定] に移動します。
4. [編集] を選択して設定を変更します。
5. [Chatter 設定] の下にある [有効化] を選択し、[保存] を選択します。

2.2.2 Chatter 設定で投稿およびメンションの編集を許可する

Chatter の投稿やコメントでのユーザーメンションの破損を防ぐために、Chatter 設定で [ユーザーに投稿およびメンションの編集を許可] 設定を有効にすることを強くお勧めします。

この設定をSalesforceの組織でオンにするには

1. システム管理者アカウントで Salesforce にログインします
2. 組織の設定に移動し、[設定] を選択します。
3. [機能設定] > [Chatter] > [Chatter 設定] に移動します。
4. [編集] を選択して設定を変更します。
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 添付ファイルの Salesforce ファイルとしてのアップロードを許可する

ファイルを添付ファイルとして保存しており、Salesforce Classic ユーザーインターフェースを使用している場合は、[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、添付ファイルではなく Salesforce Files としてアップロードされます] 設定を有効にすることをお勧めします。

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

Salesforce 組織でこの設定を有効にする手順:

1. システム管理者アカウントで Salesforce にログインします。
2. 組織の設定に移動し、[設定] を選択します。
3. [機能設定] > [Salesforce Files] > [一般設定] に移動します。
4. [編集] を選択して設定を変更します。
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、添付ファイルではなく Salesforce Files としてアップロードされます] を選択し、[保存] を選択します。

2.2.4 その他の言語のアクティベート

Cloud Protection for Salesforce のデフォルト言語は英語ですが、サポートされている他の言語を有効にすることもできます。

Cloud Protection for Salesforceは現在次の言語をサポートしています。
Cloud Protection for Salesforce は、現在以下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
- ポーランド語

- 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、アラートのデフォルト言語として使用されます。

他の言語をアクティベートする手順:

1. システム管理者アカウントで Salesforce にログインします。
2. 組織の設定に移動し、[設定] を選択します。
3. メニューから [ユーザーインターフェース] > [トランスレーションワークベンチ] > [翻訳設定] を選択します。
4. 希望する言語の [有効] チェックボックスを選択します。

組織内のユーザーがアカウント設定の [設定] > [個人情報] > [言語とタイムゾーン] でその言語を選択している場合、アクティベートされた言語で Cloud Protection for Salesforce を使用できるようになります。

2.3 アプリケーションのインストール

Salesforce 組織にアプリケーションをインストールするには、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に移動し、Cloud Protection アプリケーションを検索して、[今すぐ入手 (Get It Now)] を選択してインストールを開始します。
   Cloud Protection は、Salesforce AppExchange のこちらに掲載されています: https://appexchangejp.salesforce.com/appxListingDetail?listingId=a0N3A00000EJGqnUAH

> 注：Cloud Protection for Salesforce アプリケーションのリリースプレビュー版またはベータ版をインストールする場合は、管理パッケージへの直接リンクが届きます。インストールを開始するには、Web ブラウザでそのリンクを開いてください。

> 注：アプリケーションのリリースプレビュー版またはベータ版が既にインストールされている場合は、新しいバージョンのアプリケーションをインストールする前にアンインストールしてください。

3. アプリケーションを本番用 Salesforce 組織またはサンドボックスのどちらにインストールするかに応じて、[本番環境にインストール] または [Sandbox にインストール] を選択します。
4. インストールの詳細を確認します。
5. [利用規約を読み、同意しました] 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. アプリケーションが WithSecure Security Cloud サービスに接続できるように、[はい、サードパーティ Web サイトにアクセスを許可します] を選択します。次に [続行] を選択します。インストールが完了するまで待ちます。
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りすぎているというメッセージが表示された場合は、アプリがインストールされた旨の確認メールが Salesforce から届くまでお待ちください。

> **重要**：アプリのインストールに時間がかかりすぎているというメッセージが表示された場合は、アプリがインストールされた旨の確認メールが Salesforce から届くまでお待ちください。

9. インストールが完了したら、[完了] を選択します。

Cloud Protection for Salesforce が正常にインストールされました。

2.4 権限セットとライセンスの割り当て

アプリケーションをインストールした後、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 Cloud Protection User 権限セットの割り当て

Visualforce ページへのアクセス権を持つ組織内のすべてのアクティブユーザーに、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、Cloud Protection by WithSecure ソフトウェアライセンスを保有していないユーザーに対しても、ダウンロード保護および URL クリック時保護が含まれています。Cloud Protection User のバージョン 3.1 では、ライセンスタイプに基づいて Salesforce ユーザーに Cloud Protection for User または Cloud Protection for guest user 権限セットを割り当てるための、再設計された「ユーザー権限セット管理 (Manage user permission set)」ツールが導入されています。

> 注：ユーザー権限セット管理ツールを使用する前に確認すべき事項:
>
> - ユーザーインターフェースを操作し、クリック時保護 (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、Cloud Protection User 権限を割り当てることが推奨されます。
> - バッチ Apex で 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手動で権限セットを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は、初期状態では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、ユーザーが作成される前にグループの自動割り当てトグルが有効になっている必要があります。
> - 統合ユーザーの割り当てを検証する必要があります。統合ユーザーの自動割り当ては無効になっており、Integration 権限セットは自動的に割り当てられません。
> - 作成されたカスタム権限セットは、このツールを使用して移行されないことに注意してください。

Cloud Protection User および Cloud Protection Guest user 権限セットを割り当てるには、以下の手順に従ってください。

1. システム管理者アカウントで Salesforce にログインします。
2. アプリケーションランチャーに移動し、[Cloud Protection] を開きます。
3. [管理] > [ツール] > [管理ツールを開く] に移動し、[ユーザー権限セット管理] の下にある [割り当て] を選択します。[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タイプ、総ユーザー数、権限セットを持つユーザー、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の [すべて割り当て] / [すべての割り当てを解除]、およびグローバルに権限セットを削除するための [すべての割り当てを解除] がリスト表示されます。

- ユーザーライセンスは、総ユーザー数の降順で並べ替えられます。
- 自動割り当ては、ユーザーの再有効化およびユーザーのオンボーディング変更中にのみ発生します。
- デフォルトでは、新規インストールの場合、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維持されます。
- 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、および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対象外のライセンスタイプが特定された場合、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用意されています。

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。

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

作成された当社の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ず、これまでも考慮されていませんでした。

アップグレード時、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（ユーザーの再有効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 Cloud Protection Admin 権限セットの割り当て

アプリケーションの設定、分析、およびレポートへのアクセスが許可されているユーザーに、Cloud Protection Admin 権限セットを割り当てる必要があります。

Cloud Protection Admin 権限セットを割り当てる手順:

1. システム管理者アカウントで Salesforce にログインします。
2. 組織の設定に移動し、[設定] を選択します。
3. [ユーザー] > [権限セット] > [Cloud Protection Admin] を選択します。
4. [割り当ての管理] を選択します。
5. [割り当てを追加] を選択します。
6. Cloud Protection for Salesforce アプリケーション、分析、およびレポートへのアクセスが必要なすべてのユーザーを選択し、[割り当てを追加] を選択します。

2.4.3 Cloud Protection ライセンスの割り当て

Cloud Protection for Salesforce ライセンスは、アプリケーションを管理する、あるいは有害または許可されていないコンテンツに関連するセキュリティ脅威から保護されるすべてのユーザーに割り当てる必要があります。

> 注：Cloud Protection by WithSecure ライセンスが割り当てられていないユーザーは、WithSecure Cloud Protection for Salesforce によって保護されません。これらユーザーは、Salesforce 組織に入り込む可能性のある有害または許可されていないコンテンツにアクセスするリスクに晒されます。

Cloud Protection for Salesforce ライセンスをユーザーに割り当てるには、以下の手順に従ってください:

1. システム管理者アカウントで Salesforce にログインします。
2. アプリケーションランチャーに移動し、[Cloud Protection] を開きます

3. [管理] > [ライセンス] に移動します。
4. 購入したライセンスの数に応じて、以下のいずれかを実行します:
   - 限定された人数のユーザー向けに Cloud Protection by WithSecure ライセンスを購入した場合は、[ライセンスを所有する
     ユーザーを手動で選択] オプションを選択し、[保存] をクリックして、次のステップに進みます。
   - 組織内のすべてのユーザー向けに Cloud Protection by WithSecure ライセンスを購入した場合は、[すべてのユーザーにラ
     イセンスを自動的に割り当てる] オプションを選択し、[保存] をクリックします。
5. [ユーザーとライセンス割り当てルールの管理] リンクをクリックします。
   [ユーザーとライセンス割り当てルール] ウィンドウが開きます。
6. ユーザー名、プロファイル、または部署で検索するか、リストをスクロールしてライセンスが必要なユーザーを見つけます。
7. プラス (+) アイコンの付いたボタンをクリックして、ライセンスを割り当てるユーザーを選択します。検索によって取得されたユーザーのリスト全体に Cloud Protection for Salesforce ライセンスを割り当てるには、[すべて割り当て] をクリックすることもできます。
8. 完了したら [保存] をクリックします。
   ユーザープロファイルプロファイルやその他の基準に基づいて、ライセンスの自動割り当てを有効にすることを検討できます:
   a) [ユーザーとライセンス割り当てルールの管理] リンクをクリックし、[自動割り当てルール] タブに移動します。
   b) 製品の他の場所と同じ項目ベースの構文（Name, Profile, Role, Email, Company, Division, LICENSED, または UNLICENSED）を使用して、入力フィールドにテキストとしてルールを入力します。ワイルドカードとして * を使用できます。例えば、Profile System* と指定すると、"System" で始まる任意のプロファイル名に一致します。
   c) [ルールを追加] をクリックします。
      ルールが検索ボックスの下のリストに追加されます。さらにルールを追加したり、リストから既存のルールを削除したりできます。

      > 注：ルールはルール間で "OR" 論理で評価され、いずれか 1 つのルールに一致するユーザーが含まれます。

   d) [自動ライセンス割り当てを有効化] トグルをオンにします。
   e) 完了したら [保存] をクリックします。

Cloud Protection by WithSecure ライセンスが多数のユーザーに割り当てられると、アプリはバックグラウンドでこれらのライセンスを割り当て、ステータスやエラーをアラートとしてレポートします。

2.5 アプリケーションのアップグレード

Cloud Protection for Salesforce アプリケーションの最新バージョンは、Salesforce AppExchange で常に利用可能です。以前のバージョンからアプリケーションをアップグレードすると、既存のすべての設定と分析データが保持されます。

> 注 :リリースプレビュー版またはベータ版のアプリケーションからはアップグレードできません。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に移動し、Cloud Protection アプリケーションを検索して、[今すぐ入手 (Get It Now)] を選択してインストールを開始します。
   Cloud Protection は、Salesforce AppExchange のこちらに掲載されています:https://appexchangejp.salesforce.com/appxListingDetail?listingId=a0N3A00000EJGqnUAH
3. アプリケーションを本番用 Salesforce 組織またはサンドボックスのどちらにインストールするかに応じて、[本番環境にインストール] または [Sandbox にインストール] を選択します。
4. インストールの詳細を確認します。
5. [利用規約を読み、同意しました] 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. [アプリケーションが WithSecure Security Cloud サービスに接続できるように、[はい、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、[続行] を選択します。インストールが完了するまで待ちます。
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りすぎているというメッセージが表示された場合は、アプリがインストールされた旨の確認メールが Salesforce から届くまでお待ちください。

9. インストールが完了したら、[完了] を選択します。

Cloud Protection for Salesforce が正常に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

本セクションでは、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設定について説明します。

3.1 アラートと通知の送信先の設定

Cloud Protection は、セキュリティアラートとユーザー通知を電子メールで送信します。

セキュリティアラートは Cloud Protection Admins グループに送信されます。ユーザー通知はSalesforce 組織内の内部ユーザーに送信されます。セキュリティアラートおよびユーザー通知の送信元となる組織全体のメールアドレスを作成する必要があります。

> 注：セキュリティアラートとユーザー通知に使用するメールアドレスは、存在しており有効である必要があります。Salesforce が使用を許可する前に、メールアドレスを検証する必要があります。

セキュリティアラートとユーザー通知を送信するための Cloud Protection Admins およびメールアドレスを設定するには、以下の手順に従ってください。

1. システム管理者アカウント、または Cloud Protection Admin 権限セットが割り当てられているユーザーで Salesforce にログインします。
2. アプリケーションランチャーに移動し、[Cloud Protection] を開きます。
3. [管理] > [通知] に移動します。
4. [管理者向けメール通知] の下の [このグループに電子メール通知を送信] の横にある [Cloud Protection Admins] リンクをクリックして、Cloud Protection Admins グループを開きます。
5. [編集] を選択し、Cloud Protection からセキュリティアラートを受信するユーザーを追加して、[保存] を選択します。
6. [管理] > [通知] に戻り、[組織全体のメールアドレスを参照] をクリックします。
7. [ユーザーが選択可能な組織全体のメールアドレス] の横にある [追加] を選択します。
8. 表示名とメールアドレスを指定し、[保存] を選択します。
9. [管理] > [通知] に戻ります。
10. [組織全体のメールアドレスを参照] の横で、以前に作成したメールアドレスを選択します。
11. [保存] をクリックして変更を保存します。

3.2 セキュリティアラートと警告メッセージの設定

管理者およびユーザーにアラートを送信するタイミングを選択し、警告メッセージを編集するには、以下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に移動し、[Cloud Protection] を開きます。
2. [管理] > [通知] に移動します。
3. [管理者向けメール通知] > [ファイル保護] の下で、ファイル保護アラートを設定します:
   - [Salesforce クラウドから有害な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には、[有害なファイルを検出] をオンにします。

- Salesforce クラウドからハイリスクな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には、[ハイリスクファイルを検出] をオンにします。
- [ファイルの実際のタイプがその拡張子と一致しない場合に管理者にアラートを送信するには、[不一致のファイルタイプを検出] をオンにします。
- Salesforce クラウドから許可されていない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には、[許可されていないファイルを検出] をオンにします。
- [ファイルのレピュテーションが変更されたときに管理者にアラートを送信するには、[ファイルのレピュテーション変更] をオンにします。

4. [管理者向けメール通知] > [URL保護] の下で、URL 保護アラートを設定します:
   - [Salesforce クラウド上で悪意ある Web リンクが公開されたかクリックされたときに管理者にアラートを送信するには、[有害な URL を検出] をオンにします。
   - Agentforce エージェントアクションで悪意ある URL が検出されたときに管理者にアラートを送信するには、[エージェントアクションからの有害な URL を検出] をオンにします。
   - Salesforce クラウド上で許可されていない Web リンクが公開されたかクリックされたときに管理者にアラートを送信するには、[許可されていない URL を検出] をオンにします。
   - Agentforce エージェントアクションで許可されていない URL が検出されたときに管理者にアラートを送信するには、[エージェントアクションからの許可されていない URL を検出] をオンにします。
   - 公開された Web リンクのレピュテーションが変更されたときに管理者にアラートを送信するには、[URL のレピュテーション/判定の変更] をオンにします。
5. [内部ユーザー向けメール通知] > [ファイル保護] の下で、ユーザーに送信される警告メッセージを設定します:
   - ユーザーが Salesforce クラウドに悪意あるコンテンツをアップロードしたときに警告を送信するには、[有害なファイルのアップロード] をオンにします。
   - [許可されていない URL の投稿] を有効にすると、ユーザーが許可されていない Web リンクを Salesforce クラウドに公開したときに警告が送信されます。
6. [内部ユーザー向けメール通知] > [URL保護] の下で、ユーザーに送信される警告メッセージを設定します:
   - ユーザーが Salesforce クラウドに悪意ある Web リンクを投稿したときに警告を送信するには、[有害な URL の投稿] をオンにします。
   - ユーザーが Salesforce クラウドに許可されていない Web リンクを投稿したときに警告を送信するには、[許可されていない URL の投稿] をオンにします。

3.3 ファイル保護の設定

本セクションでは、基本的なファイル保護スキャン設定のセットアップ方法について説明します。

Salesforce からアップロードおよびダウンロードされるファイルをスキャンする方法を設定するには、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に移動し、[Cloud Protection] を開きます。
3. [管理] > [ファイル保護] に移動します。

チェックしたいコンテンツの保存方法に応じて、[Salesforce 添付ファイルのファイル保護]、[Salesforce Files のファイル保護]、またはその両方を切り替えて有効にします。

5. 添付ファイルをスキャンする場合は、[オブジェクトの設定] を選択してチェック対象のコンテンツソースを指定します。
   - チェックするオブジェクトを選択するか、利用可能なすべての添付ファイルをチェックする場合は [すべてのオブジェクトでスキャン] を選択します。
6. [有害なファイルのスキャン] の下で:
   - 必要に応じて、有害なコンテンツとしてスキャンされるファイルタイプまたはファイル拡張子を変更します:
     - [除外されたもの以外のすべて] または [含まれるもののみ] を選択します。
     - [除外されたファイルタイプと拡張子の設定] または [含まれるファイルタイプと拡張子の設定] を選択します。

       ル該当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 や 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きます。ファイルタイプの例を確認するには、[分析] > [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参照してください。

     - 目的の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。
     - [保存] を選択します。
   - アップロード時に有害なコンテンツが見つかった場合の処理を選択します:
   - アップロード時に有害なコンテンツが見つかった場合の動作を選択します:
     - [アクセスを許可、レポートのみ] は、スキャン中に見つかった有害なファイルをブロックも削除もしません。
     - [ファイルを削除] は、スキャン中に見つかった有害なファイルを隔離に移動します。
   - [ハイリスクファイルが検出された場合のアクション（アップロード）] の横にある [ハイリスクファイルのタイプとアクションの設定] を選択します。詳細については「3.3.1 ハイリスクファイルのサポート」を参照してください。
   - [ダウンロード時にファイルをスキャン] をオンにします。
   - ダウンロード時に有害なコンテンツが見つかった場合の処理を選択します:
     - [アクセスを許可、レポートのみ] は、スキャン中に見つかった有害なファイルをブロックも削除もしません。
     - [アクセスをブロック] は、有害なファイルへのすべてのアクセスをブロックしますが、削除はしません。
     - [ファイルを削除] は、スキャン中に見つかった有害なファイルを隔離に移動します。
   - [ハイリスクファイルが検出された場合のアクション（ダウンロード）] の横にある [ハイリスクファイルのタイプとアクションの設定] を選択します。詳細については「3.3.1 ハイリスクファイルのサポート」を参照してください。
7. [許可されていないファイルのフィルタリング] の下で:
   - 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:
     - [禁止のみ] または [許可されたもの以外のすべて] を選択します。
     - [禁止されたファイルタイプと拡張子の設定] または [許可されたファイルタイプと拡張子の設定] を選択します。

    - 該当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 や docx）。
    - 目的の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。
    - [[保存] を選択します。
  - [アップロード時にファイルをフィルタリング] をオンにします。
  - アップロード時に許可されていないコンテンツが見つかった場合の処理を選択します:
    - [アクセスを許可、レポートのみ] は、スキャン中に見つかった許可されていないファイルをブロックも削除もしません。
    - [ファイルを削除] は、スキャン中に見つかった許可されていないファイルを隔離に移動します。
  - [ダウンロード時にファイルをフィルタリング] をオンにします。
  - ダウンロード時に許可されていないコンテンツが見つかった場合の処理を選択します:
    - [アクセスを許可、レポートのみ] は、スキャン中に見つかった許可されていないファイルをブロックも削除もしません。
    - [アクセスをブロック] は、許可されていないファイルへのすべてのアクセスをブロックしますが、削除はしません。
    - [ファイルを削除] は、スキャン中に見つかった許可されていないファイルを隔離に移動します。

8. 削除されたファイルを単に削除するのではなくプレースホルダーテキストファイルに置き換えるかどうかを選択するには、削除したファイルを (単に削除するのではなく) プレースホルダーのテキストファイルで置き換えるかどうかを選択するには、[削除されたファイルをテキストファイルで置換] の下で [有害なファイル]、[ハイリスクファイル]、または [許可されていないファイル] をオンにして、削除された各ファイルタイプの代わりにプレースホルダーテキストファイルを残します。[置換ファイルの設定] を選択して、プレースホルダーのコンテンツを編集します。

9. [詳細設定] の下で、以下の設定を行います:

   - [外部ダウンロードのファイルスキャン – 公開リンクや MIAW チャット経由で共有されたファイルがどのようにスキャンされるかを制御します。これらのダウンロードは未認証の公開ユーザーとして実行されるため、ライセンスモードが「選択済み」に設定されている場合でも、ファイルスキャン使用量としてカウントされます。以下から 1 つ選択します:
     ・ファイルのスキャンが完了するまでダウンロードを保留する – 最大限の保護。ダウンロード前にファイルがスキャンされるため、不安全なファイルが受信者に到達することはありませんが、ダウンロードに時間がかかる場合があります。
     ・[即座にダウンロードを許可し、バックグラウンドで非同期にファイルをスキャンする – ダウンロードは即座に完了しますが、スキャンが終了する前に不安全なファイルが受信者に到達する可能性があります。
     ・外部ダウンロードをスキャンしない – 最もリソース使用量が少ないですが、悪意あるファイルは検出・ブロックされません。
   - Salesforce から送信されるメール内の添付ファイルをスキャンするには、[送信メール内のファイルをスキャン] をオンにします。
   - ゲストユーザーがスキャン完了前にファイルをダウンロードできるようにするには、[スキャンが完了する前にゲストユーザーによるファイルのダウンロードを許可] をオンにします。
   - 内部ユーザーがスキャン完了前に画像ファイルをダウンロードできるようにするには、[スキャンが完了する前に内部ユーザーによる画像のダウンロードを許可] をオンにします。

> 注 :右記のファイル拡張子が画像として分類されます: jpg, png, gif。

- [「不明」なファイルレピュテーションの扱い] の下で、[安全] または [不安全] を選択して、既知のレピュテーションを持たないファイルをどのように処理するかを決定します。

> 注：一部のファイルには既知のレピュテーションがありません。それらを「不安全」として扱うと、偽陽性（誤検知）が発生する可能性があります。

- [ゲストおよびコミュニティユーザーのファイルスキャン遅延] の下で、遅延時間を 遅延なし, 1 分, 3 分, 5 分, または 10 分 から選択します。

3.3.1 ハイリスクファイルのサポート

攻撃者はパスワード保護されたファイル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。Cloud Protection for Salesforce バージョン 3.0 では、アップロードおよびダウンロード中のこれらのハイリスクファイル（パスワード保護されたファイル）の取り扱いに関する設定可能なオプションが導入されました。

3 つのハイリスクファイルタイプは以下の通りです:

- パスワード保護されたアーカイブファイル
- パスワード保護された Microsoft Office ファイル
- パスワード保護された PDF ファイル

ハイリスクファイルの取り扱い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、Cloud Protection Connected App を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に移動し、[Cloud Protection] を開きます。
3. [管理] > [ファイル保護] に移動します。
4. [有害なファイルのスキャン] の下のアップロード設定で、[ハイリスクファイルが検出された場合のアクション] に移動し、[ハイリスクファイルのタイプとアクションの設定] を選択します。
   - 3 つのハイリスクファイルタイプのそれぞれについて、保護のオン/オフを切り替え、以下からアクションを選択します:
     - [アクセスを許可、レポートのみ]
     - [ファイルを削除]
     - [保存] を選択します。
5. [有害なファイルのスキャン] の下のダウンロード設定で、[ハイリスクファイルが検出された場合のアクション] に移動し、[ハイリスクファイルのタイプとアクションの設定] を選択します。
   - 3 つのハイリスクファイルタイプのそれぞれについて、保護のオン/オフを切り替え、以下からアクションを選択します:
     - [アクセスを許可、レポートのみ]
     - [ファイルを削除]
     - [アクセスをブロック]
     - [保存] を選択します。

> 注：デフォルトでは:

- 新規インストール: 3 つのハイリスクファイルタイプすべてで保護がオンになっており、アップロードおよびダウンロードの両方でアクションが「アクセスを許可、レポートのみ」に設定されています。
- バージョン 2.6 から 2.9.x からのアップグレード: パスワード保護されたアーカイブファイルは、以前に設定されていたアクションを維持します。パスワード保護された Microsoft Office および PDF ファイルはこのリリースで新しく追加されたものであり、アップロードおよびダウンロードの両方でアクションのデフォルトは「ファイルを削除」ですが、保護はデフォルトでオフになっているため、手動でオンにする必要があります。
- バージョン 2.5 以前からのアップグレード: 3 つのハイリスクファイルタイプすべてがアップロードおよびダウンロードの両方でデフォルトで「ファイルを削除」に設定されますが、保護はデフォルトでオフになっているため、手動でオンにする必要があります。

重要 : 2 つの設定がハイリスクファイルの通知とファイル処理を制御します:

- [管理] > [通知] の下の [ハイリスクファイルを検出] は、ハイリスクコンテンツが検出、ブロック、または削除されたときに管理者アラートを送信します。新規インストールの場合はデフォルトでオフになっています。
- [管理 > ファイル保護 > 削除したファイルをテキストファイルで置き換える] にある [リスクの高いファイル] は、削除されたリスクの高いファイルをプレースホルダーのテキストファイルで置き換えます。デフォルトでオンになっています。

メール通知設定に関する詳細なガイダンスについては、「3.1 アラートと通知の送信先の設定」および「3.2 セキュリティアラートと警告メッセージの設定」を参照してください。

3.4 URL 保護の設定

本セクションでは、URL 保護のスキャン設定を設定する方法について説明します。

1. アプリケーションランチャーに移動し、[Cloud Protection] を開きます。
2. [管理] > [URL保護] に移動します。
3. [全般] の下で、[URL 保護] がオンになっていることを確認します。
4. [オブジェクトの設定] を選択し、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。

5. クリック時保護を使用するには、オブジェクトを選択して [項目の設定] を選択します。各 URL 項目について、[クリック時保護] のオン/オフを切り替えます。
6. 特定の Web サイトへのアクセスを許可するには、[ドメイン、URL、TLD の除外] をオンにし、[除外するドメイン、URL、TLD の設定] を選択して、ブロックしない Web サイトを指定します。
7. [リッチリンクプレビューをサポートするドメインの除外] をオンにし、[ドメインの設定] を選択して、埋め込まれた動画、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。
8. 悪意ある Web サイトへのアクセスをブロックするには:
   a) [有害な URL のスキャン] の下で、[URL をスキャン] をオンにします。
   b) [有害な URL が検出された場合のアクション] で、[アクセスをブロック], [アクセスを許可、レポートのみ], または [URL を削除] を選択します。
9. 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) [許可されていない URL のフィルタリング] の下で、[URL をフィルタリング] をオンにします。
b) [[許可されていない URL カテゴリ] で、[許可されていない URL カテゴリの設定] を選択し、ブロックしたいコンテンツを選択します。
c) [許可されていない URL が検出された場合のアクション] で、[アクセスをブロック], [アクセスを許可、レポートのみ], または [URL を削除] を選択します。

10. 新規登録ドメインをブロックするには、[許可されていない URL のドメイン経過日数] でブロックするURL の経過日数を選択します。新規登録ドメイン (NRD) はフィッシング攻撃でよく使用されます。これらのドメインをブロックすることで、システムをそのような脅威から保護できます。[すべてのドメイン経過日数を許可], または 7, 14, 30, 60, または 90 日以下を選択できます。

> 注：デフォルトでは、新規インストールの場合は 30 日以下の URL がブロックされ、製品アップグレードの場合はすべての経過日数が許可されます。

11. ブロックされたリンクの代わりに表示されるプレースホルダーテキストをカスタマイズするには、[URL 置換テキスト] に移動し、[有害な URL の置換テキスト] または [許可されていない URL の置換テキスト] をオンにして、[置換テキストの設定] を選択します。
12. [詳細設定] セクションに移動します。
13. [投稿やコメントを処理するためのカスタム Chatter 統合を有効化] をオンにして、Cloud Protection が Salesforce の Connect API を介して Chatter フィード項目やコメント（メンションやリッチHTML リンクを含む投稿）を処理できるようにします。これは新規インストールの場合はデフォルトでオヱ、製品アップグレードの場合はデフォルトでオフになっています。
14. 分析レポートに除外された URL を表示したくない場合は、[除外された URL を分析でレポート] をオフにします。
15. リンク内やブロック/削除ページに元の URL を表示したくない場合は、[クリック時保護リンク内に元の URL を表示] および [ブロックおよび削除されたページに元の URL を表示] をオフにします。
16. 変更を行った場合は、[保存] をクリックしてすべての変更を保存します。

3.5 手動およびスケジュールスキャンの設定変更

手動スキャンとスケジュールスキャンの両方で、スキャン対象、検出時の処理、送信される通知に関する同じ共有設定が使用されます。

1. アプリケーションランチャーに移動し、[Cloud Protection] を開きます。
2. [管理] > [手動スキャン] に移動します。
3. スキャンを即座に実行するには:
   a) [手動ファイルスキャンの開始] の下で、[期間] を設定し、[作成日] または [更新日] を選択してから、開始日と終了日を選択します。
   b) [スキャンする最大ファイル数] を設定します。
   c) [今すぐスキャン] を選択します。すでにスキャンが実行中の場合、このボタンは [スキャンを中止] に変わります
4. 定期的なスキャンを管理するには、[スケジュール済みジョブの管理] の下で、[新規作成] を選択してスケジュールを設定するか、[削除] を選択して既存のスケジュール済みジョブを削除します。[すべてのスケジュール済みジョブを表示] を選択して、Salesforce の設定画面で表示します。
5. [スキャン設定] の下で、チェックしたいコンテンツの保存方法に応じて、[Salesforce 添付ファイルとして保存されたファイルをスキャン]、[Salesforce Files として保存されたファイルをスキャン]、またはその両方を切り替えて有効にします。添付ファイルをスキャンする場合は、[オブジェクトを選択] をクリックして、含める添付ファイルオブジェクトを選択します。

6. [有害なファイルのスキャン] の下で、[有害なファイルのスキャン] をオンにします。
   a) [有害なコンテンツが見つかった場合のアクション] で、[アクセスを許可、レポートのみ] または [ファイルを削除] を選択します。
   b) [有害なコンテンツをスキャンするファイル] の下で、[除外されたもの以外のすべて] または [含まれるもののみ] を選択します。
      1. [除外されたファイルタイプと拡張子の設定] または [含まれるファイルタイプと拡張子の設定] を選択します。
      2. 該当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 や 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きます。ファイルタイプの例を確認するには、[分析] > [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参照してください。

      3. 目的の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。
      4. [保存] を選択します。
7. 特定の種類のコンテンツもチェックしたい場合は、[許可されていないファイルのフィルタリング] をオンにします。
   a) [許可されていないコンテンツが見つかった場合のアクション] で、[アクセスを許可、レポートのみ] または [ファイルを削除] を選択します。
   b) [許可されていないコンテンツとして扱うファイル] の下で、[禁止のみ] または [許可されたもの以外のすべて] を選択します。
      1. [禁止されたファイルタイプと拡張子の設定] または [許可されたファイルタイプと拡張子の設定] を選択します。
      2. 上記の有害なファイルのスキャンと同様の方法で、該当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。
      3. [保存] を選択します。
8. [削除されたファイルをテキストファイルで置換] の下で、[有害なファイル] または [許可されていないファイル] をオンにして、削除された各ファイルタイプの代わりにプレースホルダーテキストファイルを残します。[置換ファイルの設定] を選択してそのコンテンツを編集します。
9. [管理者向けメール通知] の下で、[有害なファイルを検出] または [許可されていないファイルを検出] をオンにして管理者にアラートを送信し、[メールテンプレートの設定] を選択してメッセージを編集します。

   > 注：これらのアラートの送信先は [管理] > [通知] で設定します。

10. [詳細設定] を選択し、そこでの設定を確認します:
    - スキャン結果にクリーンなファイルや除外されたファイルを表示させたくない場合は、[有害または許可されていないコンテンツのみレポート] をオンにします。
    - まだ SHA 値と更新タイムスタンプがないスキャン済みファイルについて、それらを更新したい場合は [スキャン済みファイルのハッシュチェックサムを更新] をオンにします。
    - [バッチあたりの最大ファイル数] を設定して、1 つのバッチで処理されるファイルの数を定義します（デフォルトは 40、10 ～ 50 の間で設定可能）。

> 注：通常、この設定を変更する必要はありません。ただし、「最大時間を超えました（Exceeded maximum time）」エラーが表示される場合は、この設定で定義されている値を減らすことをお勧めします。

3.6 手動スキャン用権限セットの作成

Cloud Protection for Salesforce による手動スキャンおよびスケジュールスキャンには、Salesforce 内のすべてのファイルを処理できるように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. システム管理者アカウントで Salesforce にログインします。
2. 組織の設定に移動し、[設定] を選択します。
3. [管理] > [ユーザー] > [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表示ラベルと API 名を入力します。
   例えば、表示ラベルに Cloud Protection Manual Scan と入力し、自動生成される API 名 Cloud_Protection_Manual_Scan 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ページで、[アプリケーション] セクションの下にある [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] の下で、[すべてのファイルをクエリ（Query All Files）] を選択します。
10. [保存] をクリックします。
11. [権限変更の確認] ダイアログで [保存] をクリックして、追加のシステム権限およびオブジェクト権限を有効にします。
    これで新しい権限セットが作成されました。
12. [割り当ての管理] をクリックし、手動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ーに新しい権限セットを割り当てます。

3.7 製品の自動更新の設定

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確認されると、Salesforce AppExchange に公開されます。

1. アプリケーションランチャーに移動し、[Cloud Protection] を開きます。
2. [全般] タブに移動します。
3. [自動更新 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] をオンにします。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. [アップデートをインストールする希望の曜日と時間] で、Salesforce 組織環境に新しいバージョンをインストールしたい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るため、希望の時間にすぐに反映されない場合があります。Salesforce 組織にアップデートが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依存します。製品ライフサイクルポリシーに従い、Cloud Protection by WithSecureは自動アップデート設定にかかわらず、製品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か確認するには、[分析] > [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 Cloud Protection Admins グループに追加されたユーザーに電子メール通知を送信します。

3.8 プライバシー設定の変更

WithSecure Security Cloud にどの情報を提供するかを選択するには、以下の手順に従ってください。

WithSecure Security Cloud は、マルウェアやその他のさまざまなデジタル脅威のための分析エンジンであり情報リポジトリです。Security Cloud のレピュテーションサービスは、既知の安全なオブジェクトや悪意あるオブジェクトを迅速に特定する方法を提供し、疑わしいオブジェクトの自動分析および手動分析の両方を実行でき、保護精度を高めるためにオブジェクトに関する情報を世界規模で集約します。

当社は厳格なプライバシー原則を適用して機密性の高い個人データの収集を回避し、必要な技術データのみが当社のサーバーに届くようにしています。

1. [アプリケーションランチャー]に移動し、[Cloud Protection] を開きます。
2. [管理] > [全般] タブに移動します。
3. [スキャン設定] の下で、以下の設定を変更します:
   a) Cloud Protection for Salesforce は、主にファイルのハッシュを使用して WithSecure Security Cloud にクエリを実行します。ハッシュだけでなくファイル全体を送信して分析するには、[マルウェアおよび高度な脅威スキャンのためにファイル全体を送信] をオンにします。Cloud Protection for Salesforce が高度な脅威や複雑なマルウェアを可能な限り迅速に検出できるように、このオプションをオンにしておくことをお勧めします。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) [脅威分析のために Cloud Protection by WithSecure が使用するサードパーティサービスへのファイル関連データの送信を許可] の下で、ファイルが検知を引き起こした際に、サードパーティサービスと共有を許可するデータを選択します:
      - すべてのコンテンツ: ファイルを共有できます。
      - メタデータのみ: ファイルのメタデータのみを共有できます。
      - 許可しない: サードパーティサービスとデータは共有されません。
   c) URL 脅威分析についても同様に URL データの共有を許可したい場合は、[脅威分析のためにCloud Protection by WithSecure が使用するサードパーティサービスへの URL の送信を許可] をオンにします
4. [分析] の下で、より詳細な分析のために未知のファイルを送信するには、[Cloud Protection by WithSecureによる分析用の疑わしいファイルの収集と保存を許可] をオンにします。Cloud Protection by WithSecure に送信されるデータは常に匿名化されており、個人のユーザーに紐付けることは決してできません。

> 注：組織がプライバシー設定を指定のプライバシー管理者に制限している場合、その権限がない限り [マルウェアおよび高度な脅威スキャンのためにファイル全体を送信] および[Cloud Protection by WithSecure による分析用の疑わしいファイルの収集と保存を許可] は無効（グレーアウト）表示されることがあります。

3.9 アップグレード前の選択リスト値のアクティベート

Cloud Protection for Salesforce の新リリース（2.9.1）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。これらの値が利用可能で機能することを確認するために、管理パッケージに新しく導入された選択リスト値をアクティベートしてください。この手順は、アップグレードプロセス中の自動アクティベーションを妨げるプラットフォームの制限のために必要です。

Cloud Protection for Salesforce を新規インストールする場合は、このセクションをスキップできます。

> 重要：この作業は、Salesforce 組織でのアップグレードプロセスの後ではなく、「前」に行う必要があります。

Salesforce 組織の管理者は、以下の選択リスト値を手動でアクティベートする必要があります: ：

- オブジェクト: URL Scan (AFSC__FS_URL_Scan_Log__c)
- 項目: Action (AFSC__Action__c)
- 値: Removed

管理パッケージに新しく導入された選択リスト値をアクティベートするには、以下の手順に従ってください:

1. [設定] 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. [URL Scan] を選択します。
4. [項目とリレーション] をクリックします。
5. [Action] を選択します。。
6. [非アクティブな値] セクションの下に値 Removed がリストされているか確認します。
   - 値が存在する場合は、アクティベートします。
   - 値 Removed が完全に存在しない場合は、新しい選択リストエントリを作成します: [値] セクションに移動し、[新規] をクリックして、値 Removed を追加し、[保存] をクリックします。

新しい値 Removed がアクティベートされました。

3.10 URL スキャンの Salesforce 制限への対処

Cloud Protection for Salesforce バージョン 3.1 では、特に Salesforce のガバナ制限に達した際の URL イベント障害の処理が改善されました。

これは以下のようなシナリオで発生する可能性があります:

- バッチ処理でのメール送信時: カスタマーコードが 1 回の呼び出しで複数のメールを送信（またはタスクを作成）し、Salesforce トリガーが複数回呼び出されてガバナ制限を超える可能性がある。
- フロー経由でメールメッセージが送信される場合: バッチメールと同様に、これらはメールとタスクのスキャンを必要とし、future メソッドが呼び出される場合もある。1 つの queueable と 50 の future で不十分な場合、Salesforce はエラーをスローする。

コ200 レコードを超えるバッチでスキャンが必要なオブジェクトを作成する場合: これにより 200 レコードごとのチャンク処理がトリガーされ、最初のチャンクは queueable ジョブを使用するが、2 番目のチャンクは起動できない。

- デフォルトでは、そのようなカスタム設定は組織に存在しません — 手動で作成するまで、以下の詳細設定はいずれも適用されず、ガバナ制限に達したときにアラートのみが作成されます。

これらの課題に対処するため、Salesforce ガバナ制限に達した際に 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. [設定] > [カスタム設定] > [新規] に移動します。
2. 表示ラベルを Advanced Settings に設定します。
3. API 名を FS_AdvancedSettings__c に設定します。
4. 種別(Visibility)を Public に設定して [保存] します。
5. [新規] を選択して、以下のカスタム項目を作成します:

項目表示ラベル	API 名	データ型
Defer URL Scan When Resources Limited	DeferURLScanWhenResourcesLimited__c	チェックボックス
Is Allowed To Start Delayed Deferred URL Scan	isAllowedToStartDelayedDeferredUrlScan__c	チェックボックス
Is Hourly Deferred URL Scan Enabled	isHourlyDeferredUrlScanEnabled__c	チェックボックス
URL Deferred Scan Schedule Delay In Minutes	URLDeferredScanScheduleDelayInMinutes__c	数値、デフォルト 10

推奨設定:

API 名	推奨値	役割・機能
DeferURLScanWhenResourcesLimited__c	True(必須のマスターマススイッチ。オフの場合、以下のいずれの延期パスもアクティブ化できません)	全体的な遅延 URL スキャン動作を有効にします。
isAllowedToStartDelayedDeferredUrlScan__c	True(推奨されるプライマリパス)	queueable/future の制限に達した際、この設定によりほぼリアルタイムで遅延ジョブが作成されます。これが推奨されるパスです。以下の毎時設定は代替のフォールバックであり、追加の要件ではありません。
isHourlyDeferredUrlScanEnabled__c	True	isAllowedToStartDelayedDeferredUrlScan_c がオフの場合にのみ効果があります。使い果たされたクォータは、代わりに毎時プロセッサ用の遅延レコードを作成します。
URLDeferredScanScheduleDelayInMinutes__c	10 (デフォルト)	isAllowedToStartDelayedDeferredUrlScan_c と連携して動作します。遅延 URL スキャンジョブが queueable ジョブとして将来どれくらい先で実行されるかを決定します。最大 10 分に制限されています(Salesforce プラットフォームの queueable ジョブの最大遅延時間)。

> 重要： 上記のシナリオは、一括メール内の URL スキャンのみを処理します。添付ファイルが存在する場合は、[管理] > [ファイル保護] > [詳細設定] の下の [送信メール内のファイルをスキャン] を無効にし、これらの高度な設定を使用して URL スキャンを適切に処理することをお勧めします。

3.11 ファイルスキャンの Salesforce 制限への対処

Cloud Protection for Salesforce バージョン 3.3 では、Salesforce プラットフォームの制限に達した際（例えば、多数のファイルが同時にアップロードされ、すべてをスキャンする前に Salesforce が処理制限に達した場合など）に、ファイルスキャンを延期する機能が追加されました。

デフォルトでは、これらの制限に達すると Salesforce はアラートを作成しますが、ファイルはスキャンされません。

リソースが利用可能になるまでファイルスキャンを延期するには、遅延 URL スキャンで使用されるものと同じ FS_AdvancedSettings_c カスタム設定で高度な設定を行います（「3.10 URL スキャンの Salesforce 制限への対処」を参照）。これにはシステム管理者アクセス権が必要です。

1. [設定] に移動し、[カスタム設定] を検索します。
2. `FS_AdvancedSettings__c` カスタム設定が組織にまだ存在しない場合 (たとえば、延期 URL スキャンを設定していない場合) は、[ラベル] を [Advanced Settings] に、[オブジェクト名] を `FS_AdvancedSettings` に設定して作成します。
3. [新規] を選択して、以下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
Defer File Scan When Resources Limited	`DeferFileScanWhenResourcesLimited__c`	チェックボックス
Allow Delayed Deferred File Scan	`isAllowedToStartDelayedDeferredFileScan__c`	チェックボックス
Is Hourly Deferred File Scan Enabled	`isHourlyDeferredFileScanEnabled__c`	チェックボックス
File Scan Schedule Delay (Minutes)	`FileDeferredScanScheduleDelayInMinutes__c`	数値、デフォルト 10

推奨設定:

API 名	推奨値	機能
`DeferFileScanWhenResourcesLimited__c`	True (必須 — マスタースイッチ)	True の場合、延期ジョブが作成されます。False の場合、制限に達したときにアラートのみが作成されます。
`isAllowedToStartDelayedDeferredFileScan__c`	True (推奨されるプライマリパス)	True の場合、延期ジョブが作成され、構成された遅延でスケジュール済みジョブまたはキュー可能ジョブが実行されます。これが推奨されるパスです。以下の毎時設定は代替のフォールバックであり、追加要件ではありません。
`isHourlyDeferredFileScanEnabled__c`	True	`isAllowedToStartDelayedDeferredFileScan__c` がオフの場合にのみ有効になります。延期ジョブは代わりに毎時ジョブによって取得され、スキャンされます。

API 名	推奨値	機能
FileDeferredScanSchedule DelayInMinutes__c	10	isAllowedToStartDelayedDeferred FileScan__c と連携して動作します。延期ファイルスキャンジョブがキュー可能ジョブとして将来どのくらい先に実行されるかを決定します。10 分が上限です。これは Salesforce プラットフォームのキュー可能ジョブの最大遅延です。

第 4 章 アプリケーションの使用

本セクションでは、Cloud Protection for Salesforce の日常的な運用に関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、 Cloud Protection for Salesforce は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組織内の有害コンテンツの手動スキャン

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の自動チェックに加えて、製品を使用し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できます。

> 注：手動スキャンおよびスケジュールスキャンを使用するには、ユーザーアカウントに特別な権限が割り当てられている必要があります。

1. システム管理者アカウントでSalesforceにログインします。
2. アプリケーションランチャーに移動し、Cloud Protection を開きます。
3. [設定] (Administration) > [手動スキャン] (Manual Scan) に移動します。
4. チェック対象のコンテンツの保存方法に応じて、[Salesforce 添付ファイルとして保存されたコンテンツをスキャン] (Scan content stored as Salesforce Attachments)、[Salesforce ファイルとして保存されたコンテンツをスキャン] (Scan content stored as Salesforce Files)、またはその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、[場所の設定] (Configure locations) を選択して、チェック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] (Selected objects) を選択し、チェックするソースを選択します。
   - 利用可能なすべての添付ファイルをチェックする場合は、[すべてのオブジェクト] (All objects) を選択します。
6. [確認] (Confirm) 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と、日付の基準をコンテンツの作成日時（作成日）とするか最終更新日時（最終更新日）とするかを設定します。
8. [スキャンする最大ファイル数] (Maximum number of files to scan) を設定します。
9. [今すぐスキャン] (Scan now) をクリックします。
   [ス[スキャンジョブが開始されました] (Scan Job Started) 通知が表示されます。

スキャン結果の個別レポートはありませんが、[アナリティクス] (Analytics) > [ファイルイベント] (File Events) ページにスキャン中に処理されたファイルが表示されます。[方向] (Direction) 列には、手動スキャンおよびスケジュールスキャンに関連するイベントに対して Scan Job と表示されます。

関連タスク:

3.6 手動スキャン用の権限セットの作成

Cloud Protection for Salesforce での手動スキャンおよびスケジュールスキャンには、Salesforce内のすべてのファイルを処理できるようにする特別な権限が必要です。

4.1.2 指定日時での有害コンテンツのスキャン

Cloud Protection for Salesforce でスケジュールスキャンタスクを設定して、特定の時間に組織のコンテンツをチェックできます。

> 注：手動スキャンおよびスケジュールスキャンを使用するには、ユーザーアカウントに特別な権限が割り当てられている必要があります。

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に移動し、Cloud Protection を開きます。
3. [設定] (Administration) > [手動スキャン] (Manual Scan) に移動します。
4. [スケジュールスキャン] (Scheduled Scanning) を選択し、[作成] (Create) をクリックします。
   これにより、[Apex をスケジュール] (Schedule Apex) ビューが開き、スケジュールタスクを設定できます。
5. [ジョブ名] (Job Name) を編集します。
6. 頻度として [毎週] (Weekly) または [毎月] (Monthly) を選択します。
7. タスクの繰り返し条件を設定します。
8. タスクの [開始日] (Start) と [終了日] (End) を設定します。
9. [希望開始時間] (Preferred Start Time) を選択します。
10. [保存] (Save) をクリックします。

スキャン結果の個別レポートはありませんが、[アナリティクス] (Analytics) > [ファイルイベント] (File Events) ページにスキャン中に処理されたファイルが表示されます。[方向] (Direction) 列には、手動スキャンおよびスケジュールスキャンに関連するイベントに対して Scan Job と表示されます。

後でスケジュールタスクを編集するには、[スケジュールスキャン] (Scheduled Scanning) の下にある [スケジュールされたジョブの表示] (View scheduled jobs) をクリックして [Apex をスケジュール] (Schedule Apex) ビューを開き、該当するタスクの [管理] (Manage) をクリックします。

関連タスク:

3.6 手動スキャン用の権限セットの作成

Cloud Protection for Salesforce での手動スキャンおよびスケジュールスキャンには、Salesforce内のすべてのファイルを処理できるようにする特別な権限が必要です。

4.1.3 スキャンからのファイルの除外

特定のファイルタイプや特定の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タイプまたはファイル拡張子を削除（除外設定）するには:

1. アプリケーションランチャーに移動し、Cloud Protection を開きます。
2. 除外するファイルタイプまたはファイル拡張子を確認します:
   a) [アナリティクス] (Analytics) > [ファイルイベント] (File Events) に移動します。
   b) スキャンしたくないファイルのイベント行の末尾にある [表示] (View) を選択します。
      [ファイル拡張子] (File Extension) と [ファイルタイプ] (File Type) は、[ファイル名] (File Name) の横の [ファイルイベント履歴] (File Event History) ビューに一覧表示されます。
3. [設定] (Administration) > [ファイル保護] (File Protection) タブに移動します。
4. [除外] (Exclusions) を開き、タイプまたは拡張子のいずれかに基づいてスキャンからファイルを除外します。

- [ファイルタイプ別にファイルを除外] (Exclude files by file type) をオンにし、[ファイルタイプのリストを開く] (Open the list of file types) を選択して、スキャンしないファイルタイプを指定します。
- [[ファイル拡張子別にファイルを除外] (Exclude files by file extension) をオンにし、[ファイル拡張子のリストを開く] (Open the list of file extensions) 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 偽陽性(誤検知)および偽陰性(検知漏れ)の報告

スキャンエンジンがファイルまたはウェブサイトを悪意がある、または安全であると誤って判定する場合があります。これらを報告していただくことで、検知精度の向上と実際の脅威からの保護に役立ちます。

誤って判定されたファイルまたはウェブサイトを報告するには:

1. システム管理者アカウントでSalesforceにログインします。
2. [アプリケーションランチャー]に移動し、Cloud Protection を開きます。
3. ファイルを報告する場合は [アナリティクス] (Analytics) > [ファイルイベント] (File Events) に、ウェブサイトを報告する場合は [アナリティクス] (Analytics) > [URLイベント] (URL Events) に移動します。
4. 報告したいファイルまたはURLを選択します。

   選択後、イベント詳細ビューが開きます。

   選択すると、イベントの詳

   - 誤って不安全と判定された、または不正確に分類された安全なファイルやウェブサイトを報告するには、[偽陽性として報告] (Report as false positive) を選択します。
   - 誤って安全と判定された、または不正確に分類された悪意のあるファイルやウェブサイトを報告するには、[偽陰性として報告] (Report as false negative) を選択します。
5. 表示される確認ダイアログで [報告] (Report) を選択します。

   URLを報告する場合は、URLの再分析をリクエストする理由を選択します:

   - 安全なウェブサイトが有害であると判定された場合は、[安全なURLがブロックされている] (Harmless URL is blocked) を選択します。
   - 安全と判定されたウェブサイトが有害である場合は、[有害なURLがブロックされていない] (Harmful URL is not blocked) を選択します
   - ウェブサイトが不正確に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がブロックされている] (Allowed URL is blocked) 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。
   - ウェブサイトが不正確に分類されたためにブロックされていない場合は、[不許可のURLがブロックされていない] (Disallowed URL is not blocked) を選択します。

ヒント: ファイルが有害であると疑われる場合、またはファイルやウェブサイトが誤って検知・評価されたと思われる場合は、サンプルの送信ウェブサイト(Submit a sample website)を使用して、いつでも分析のために送信できます。以下のサンプル送信の承認基準を確認してください:

接続アプリケーションがない、またはファイルサイズが12MBを超えているなど、アプリが機能しないケースに関する情報を追加する必要があります。ファイルが何であるか、なぜ送信されるのかについての簡単な説明を含めてください。利用可能な場合は、検証用にファイルハッシュまたはサンプルIDも含めてください。

注 : Enterprise Supportをご契約の場合は、Cloud Protection by WithSecure のマルウェアアナリストによる分析を受けるため、カスタマーサクセスマネージャーにお問い合わせください

4.1.5 隔離機能の使用

Cloud Protection for Salesforce は、検知された有害なファイルを隔離に移動し、組織に対するそれ以上のリスクを防ぎます。

> 注：: 隔離は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ごみ箱の組織設定に基づいて永久に削除されます。有害なファイルのアラートを受信した後は、永久に削除される前に必要に応じてファイルを確認できるよう、できるだけ早く隔離を確認してください。

隔離リストは、無限スクロールのページネーションによる検索とフィルタリング（日時、理由、ファイル名、オブジェクトタイプ、またはユーザー別）もサポートしており、[理由] (Reason) と [オブジェクトタイプ] (Object Type) の2つの追加列が含まれています。

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]に移動し、Cloud Protection を開きます。
3. [設定] (Administration) > [隔離] (Quarantine) に移動します。
   ファイルの表示詳細を確認するには、[表示] (View) をクリックします。

   ファイルを永久に削除するには:

   a) ファイルの行にある [表示] (View) の横のドロップダウンボタンを選択し、[削除] (Delete) を選択します。

   ファイルを完全に削除するには (一括):

   a) 削除したいファイルを選択します。

   b) [アクション] (Actions) > [削除] (Delete) を選択します。

   ファイルを復元するには:

   a) ファイルの行にある [表示] (View) の横のドロップダウンボタンを選択し、[復元] (Restore) を選択します。

   隔離されたファイルを復元するには (一括):

   a) 復元したいファイルを選択します。

   b) [アクション] (Actions) > [復元] (Restore) を選択します。
   これにより、選択したファイルが元の場所に戻り、再びアクセスできるようになります。

4.1.6 スキャン結果キャッシュの消去

Cloud Protection は、パフォーマンスを最適化するためにスキャン結果をスキャン結果キャッシュに保存します。このキャッシュは定期的にクリーンアップされますが、製品のテスト中などに、キャッシュからすべてのスキャン結果を手動で削除したい場合があります。

1. アプリケーションランチャーに移動し、Cloud Protection を開きます。
2. [設定] (Administration) > [ツール] (Tools) タブに移動します。
3. [スキャン結果キャッシュのクリーンアップ] (Clean up scan result cache) の下にある [開始] (Start) をクリックします。
4. または、[自動キャッシュクリーンアップ] (Automatic cache cleanup) をオンにして、手動で [開始] (Start) を実行する代わりに、スケジュールされたジョブでキャッシュを自動的にクリーンアップします。
5. スキャン結果がキャッシュに保存される期間を設定するには:
   a) [設定] (Administration) > [一般] (General) > [詳細] (Advanced) タブに移動します。
   b) [キャッシュ内のスキャン結果の有効期間 (TTL)] (Expiration time (TTL) for scan results in the cache) で、スキャン結果をキャッシュに保存する期間を選択します。

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高度スキャン設定

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に移動し、Cloud Protection を開きます。
3. [設定] (Administration) > [ファイル保護] (File Protection) > [詳細] (Advanced) に移動して、以下を行います:
   - 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

> 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、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 Cloud Protection 接続アプリの使用

Cloud Protection for Salesforce 接続アプリ(Connected App)を使用すると、スキャン機能が向上し、現在および将来にわたってビジネスに不可欠なプラットフォームに対してより効果的な保護が提供されます。

Cloud Protection for Salesforce は統合型のソリューションであり、通常は Salesforce 環境への外部データアクセスを必要としません。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。Cloud Protection 接続アプリは、このような場合でも Salesforce のパフォーマンスへの影響を最小限に抑え、最適なセキュリティを確保します。

接続アプリを使用することで、Cloud Protection for Salesforce は包括的な脅威分析を実行し、新しく発見された脆弱性や高度な悪意のあるソフトウェアが発生した直後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あってもプラットフォームがシームレスに機能するようにします。

接続アプリの使用は必須ではありませんが、Salesforce 環境内に大きなファイルを保存している場合は特に使用することを強くお勧めします。

4.2.1 接続アプリ用ユーザーアカウントの作成

Cloud Protection 接続アプリを使用する前に、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。

Cloud Protection for Salesforce は、統合を有効にするアカウントの下で Salesforce 組織にアクセスします。このアカウントには、通常のユーザーアカウントと比較して、Salesforce データおよび機能への異なるアクセスレベルが必要です。接続アプリ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。

専用の統合アカウントを作成すると、Salesforce データの監査ログ（Audit Trail）およびアクセス管理が向上します。例えば、トラブルシューティングの際、専用アカウントを使用することで、問題を発生させているユーザーアカウントを特定しようとする代わりに、統合の問題を特定のアカウントに簡単に追跡できます。

> 注：Cloud Protection 接続アプリを初めてインストールする場合は、すべてのステップをSalesforce システム管理者 プロファイルを使用して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。

以下の手順に従って、Cloud Protection 接続アプリの新しい統合ユーザーを作成します。

1. Salesforce の [設定] (Setup) 画面を開きます。
2. [管理] (Administration) > [ユーザー] (Users) > [ユーザー] (Users) に移動します。
3. [新規ユーザー (New User)] を選択して、新しいユーザーを作成します。
4. 新しいユーザーアカウントの [姓], [別名], [メール], [ユーザー名] およびその他の詳細を適宜入力します。
   - [ユーザーライセンス] で Salesforce Integration を選択します。
   - [プロファイル] で 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：Salesforce Integration 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 に接続することを意図しています。Salesforce Integration ユーザーライセンスは UI アクセスを許可しておらず、システム間統合専用に設計されています。アプリケーションがバックエンドから Salesforce と通信するには、Query All Files (Salesforce ヘルプ) および View All (Salesforce ヘルプ) 権限が必要です。
5. [保存 (Save)] を選択します。
   新しいユーザーが作成され、[メール] で指定されたメールアドレスに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。
   強力なパスワードで統合アカウントを保護し、疑わしいアクティビティの兆候がないか定期的にアカウントを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 Cloud Protection for Salesforce アプリケーションのバージョンを確認してください。

- インストールされている Cloud Protection for Salesforce アプリのバージョンが 2.5 以上 の場合、統合ユーザーに Cloud Protection Integration User 権限セットを割り当てます。
- 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:
  1. Cloud Protection Admin 権限セットを複製し、複製した権限セットで Visualforce ページのアクセス権を削除します。
  2. 複製した権限セットと Cloud Protection Connected App を統合ユーザーに割り当てます。

4.2.2 組織内への Cloud Protection by WithSecure 接続アプリのローカルインストール

以下の手順に従って、Cloud Protection for Salesforce アプリをローカルにインストールします。

1. 必要な新しい権限セットを作成します（4.2.3 新しい「未インストールの接続アプリを承認」権限セットの作成を参照）。
2. 管理者または Salesforce ライセンスを持つユーザーに権限セットを割り当てます（4.2.1 接続アプリ用ユーザーアカウントの作成 & 4.2.4 接続アプリへの権限の割り当て を参照）。
3. 接続アプリを接続します（4.2.5 Cloud Protection 接続アプリの使用開始 を参照）。
4. 接続アプリをインストールします（4.2.6 接続アプリのインストール を参照）。

> 注：ンストール後、必要に応じて、接続された管理者ユーザーを統合ユーザーに切り替えることができます。あるいは、管理者が切断し、接続アプリ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、接続アプリ用の専用ユーザーを作成し、この専用ユーザーに必要な権限セットを割り当てる方法について説明します。

> 注：なぜ組織内に Cloud Protection by WithSecure 接続アプリをローカルにインストールする必要があるのですか？
>
> 025年9月初旬より、Salesforce は未インストールの接続アプリの使用制限を開始します。この使用制限により、エンドユーザーは未インストールの接続アプリを使用できなくなります。
>
> 環境で API アクセス制御（API Management）が有効になっている場合、接続アプリを有効にしようとすると Salesforce 組織で OAuth エラーが表示され始めます。エラーメッセージは以下のようになります:
>
> 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。後で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、組織自体に Cloud Protection by WithSecure 接続アプリをインストールすることで回避できます。接続アプリをインストールするには、以下のセクションの手順を確認してください。

4.2.3 新しい「未インストールの接続アプリを承認」権限セットの作成

以下の手順に従って、新しい [未インストールの接続アプリを承認] (Approve Uninstalled Connected Apps) 権限セットを作成します。

1. [[設定] (Home) に移動し、[ユーザー] (Users) →[権限セット] (Permission Sets) を検索します。
2. Approve Uninstalled Connected Apps 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. [システム管理者権限] (System Permissions) に移動し、[編集] (Edit) をクリックして、[未インストールの接続アプリを承認] (Approve Uninstalled Connected Apps) 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. [権限セット] (Permission Sets) > [Approve Uninstalled Connected Apps] > [システム管理者権限] (System Permissions) > [編集] (Edit) に移動し、[API 参照のみのユーザー] (Use Any API Client) チェックボックスをオンにします。

> 重要：API アクセス制御（API Access Control）が有効になっている場合のみ、このステップを実行してください。有効になっていない場合は、次のステップに進んで継続してください。
> API アクセス制御が有効になっており、以下のいずれかがチェックされている場合にこのステップを実行します:

- 管理者が承認したユーザーについて、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する
- または、顧客およびパートナーについて、API アクセスをインストール済み接続アプリのみに制限する

7. [割り当ての管理] (Manage Assignments) 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 環境内で接続アプリを使用および管理するための適切な権限セットを統合ユーザーに割り当てます。

以下の手順に従って、必要な権限を持つ新しい権限セットを作成します。

1. Salesforce の [設定] (Setup) 画面を開きます。
2. [管理] (Administration) > [ユーザー] (Users) > [権限セット] (Permission Sets) に移動します。
3. [新規] (New) を選択して、新しい権限セットを作成します。
4. 新しい権限セットの [表示ラベル] と [API 参照名] を入力します。例えば、表示ラベルを Cloud Protection Connected App とし、自動生成される API 参照名 Cloud_Protection_Connected_App を使用します。
5. [保存 (Save)] を選択します。
6. 新しく作成された権限セットのページで、[システム管理者権限] (System Permissions) を選択します。
7. [システム管理者権限] ページで、[編集 (Edit)] を選択します。
8. [システム] セクションで、[API の有効化] (API Enabled) および [すべてのデータの参照] (View All Data) 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 統合ユーザーである場合、この設定はすでに有効になっています。それ以外のすべてのユーザーについては、[API の有効化] 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 (Save)] を選択します。
10. [アプリケーション] セクションの [アプリ権限] (App Permissions) を開き、[すべてのファイルのクエリ] (Query All Files) をチェックします。
11. [権限変更の確認] ダイアログで [保存 (Save)] を選択して、追加のシステム権限およびオブジェクト権限を有効にします。新しい権限セットが作成されました。
12. Salesforce の [設定] 画面で、[管理] (Administration) > [ユーザー] (Users) > [ユーザー] (Users) に移動して、専用ユーザーの権限を設定します。
13. Cloud Protection 接続アプリ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] (Permission Set Assignments) を選択し、次に [割り当ての編集] (Edit Assignments) を選択します。

    ス[有効な権限セット] のリストから、Cloud Protection Integration User と、前に Cloud Protection 接続アプリ用に作成した権限セット、および Approve Uninstalled Connected Appsの権限セットを選択します。統合ユーザーから Cloud Protection for Salesforce ユーザーインターフェースへのアクセス権を削除する必要がある場合は、Cloud Protection Admin 権限セットを複製して新しい権限セットを作成し、Cloud Protection Admin の代わりにそれをユーザーに割り当てます。

16. [保存 (Save)] を選択します。

4.2.5 Cloud Protection 接続アプリの使用開始

Cloud Protection for Salesforce アプリで接続アプリを使用開始する方法に関する手順です。

1. Cloud Protection 接続アプリ用に作成したアカウントで Salesforce にログインします。
2. アプリケーションランチャー(App Launcher)に移動し、[Cloud Protection] を開きます。
3. [管理 (Administration)] > [ツール (Tools)] に移動します。
4. [接続アプリの管理 (Manage connected app)] の下にある [接続 (Connect)] を選択します。
5. [Cloud Protection の接続] ダイアログで [接続 (Connect)] を選択します。
6. [アクセス許可] ダイアログで、要求された権限を確認し、[許可 (Allow)] を選択します。
7. [ウィンドウを閉じる (Close window)] を選択します。
8. [管理 (Administration)] > [ツール (Tools)] ページでステータスを確認し、Cloud Protection 接続アプリが接続されていることを確認します。
   それでも接続されていない場合は、トラブルシューティングセクションを確認し、プロファイルのログイン IP アドレス制限範囲(Login IP Ranges)を追加して、上記の手順をもう一度試してください。

> 注： 組織によって IP 制限が実装されている場合のみ、以下のステップが適用されることに注意してください。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。
>
> 1. これら両方(使用されている場合)で Cloud Protection の IP アドレスが許可されていることを確認します:
>   - [設定] (Setup) > [セキュリティ] (Security) > [ネットワークアクセス] (Network Access) > [許可された IP アドレス範囲]
>   - [設定] (Setup) > [ユーザー] (Users) > [プロファイル] (Profiles) > [Cloud Protection Integration ユーザーが使用するプロファイル] > [ログイン IP アドレス制限範囲 (Login IP Ranges)]
>
>   > **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。
>
> 2. バックエンド IP アドレスを許可リスト(allowlist)に追加した後、すべてが正常に動作するはずです。再度接続を試みることができます。
> 3. 情報アラートが作成され、[アナリティクス (Analytics)] > [アラート (Alerts)] で確認できます。
> 4. これで、組織への接続アプリのインストールに進むことができます (4.2.6 接続アプリのインストール)

4.2.6 接続アプリのインストール

以下の手順に従って接続アプリをインストールします。

[設定] (Setup) > [接続アプリの OAuth 利用状況 (Connected Apps OAuth Usage)] に移動し、Cloud Protection アプリの横にある [インストール (Install)] ボタンをクリックします。

> 注：これにより、組織内にアプリが自動的にインストールされます。確認するには、[設定] (Setup) > [接続アプリ (Connected App)] に移動し、Cloud Protection アプリがそこに表示されていることを確認します。

4.3 クリック時 URL 保護の設定

URL は、アップロードされた時点で安全に見えても、時間の経過とともに害のないリンクから危険なペイロードに変化することがあります。クリック時保護（Click-time Protection）を使用すると、ユーザーが URL をクリックし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トラップに落ちるのを防ぎ、潜在的なデータ侵害やシステムの侵害から組織を保護します。

好みに応じて、選択した Salesforce オブジェクトに対してクリック時 URL 保護（CTP）を使用できます。例えば、Chatter の投稿にクリック時 URL 保護を適用して内部ユーザーが最高レベルのセキュリティを持てるようにし、外部の顧客に送信される送信メールではオフにすることができます。

以下の手順に従って、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カスタマイズします。

1. アプリケーションランチャーに移動し、[Cloud Protection] を開きます。
2. [管理 (Administration)] > [URL 保護 (URL Protection)] に移動します。
3. [URL 保護] > [全般 (General)] > [オブジェクトの設定 (Configure Objects)] 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、必要な項目に対して [クリック時保護リンクで URL を置換 (Replace URLs with click time protection links)] をオンにします。

> 注：クリック時保護は、100 文字を超える項目にのみ適用されます。100 文字未満の場合、N/A と表示されます。

4. [確認 (Confirm)] を選択します。
5. [保存 (Save)] を選択して変更を保存します。

4.4 高度な脅威分析の設定

高度な脅威分析（Advanced Threat Analysis）は、クラウドサンドボックスなどの高度な検知機能を利用して、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。

高度な脅威分析は、初期ファイルスキャンと比較して、より徹底的なスキャンを提供します。サンドボックス環境でファイルをスキャンするため、時間はかかりますが、悪意のあるファイルをより確実に特定できます。

> 注：高度な脅威分析を使用するには、Cloud Protection 接続アプリを使用する必要があります。

> ヒント：セキュリティを高めるため、高度な脅威分析中はファイルのダウンロードをブロックします。これにより、ファイルアクセスへ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に移動し、[Cloud Protection] を開きます。

2. [管理 (Administration)] > [ファイル保護 (File Protection)] に移動します。
3. [設定 (Settings)] の下で、[高度な脅威分析 (Advanced threat analysis)] をオンにします。
4. [保存 (Save)] を選択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 のメールおよび Chatter メッセージからすべての QR コードを特定し、抽出します。

この機能強化は、以下の新しい機能と連携して動作します:

- 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 の特定。

> 注 : この機能は QR コード内の URL を抽出し、URL レピュテーションを確認します。ファイル内のこれらの QR コードスキャンに対してアラートおよびイベントが生成されます。

- QR コード画像内の短縮 URL 保護。QR コード画像内の短縮 URL 保護。

> 注 : この機能は主要なすべての短縮 URL プロバイダーをサポートし、再帰的分析を実行して URL レピュテーションを提供します。

QR コードスキャンを有効にするには、以下の手順に従ってください:

1. [管理 (Administration)] > [ファイル保護 (File Protection)] に移動します。
2. [設定 (Settings)] の下で [高度な脅威分析 (Advanced threat analysis)] がオンになっていることを確認します。
   QR コード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 (Administration)] > [ファイル保護 (File Protection)] > [除外するファイルタイプと拡張子の設定 (Configure excluded file types and extensions)] に移動します。
4. QR コードスキャンに必要な画像フォーマットがスキャンから除外されていないことを確認します。
   QR コードスキャンは、JPEG、PNG、GIF、BMP を含む主要なすべての画像フォーマット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を示します。

4.6 カスタマイズされたオブジェクトスキャンの作成

独自のカスタム設定を使用すると、Salesforce の標準項目や標準オブジェクトを超えて URL 保護を拡張できます。

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に移動し、[Cloud Protection] を開きます。
2. [管理 (Administration)] > [URL 保護 (URL Protection)] > [全般 (General)] > [オブジェクトの設定 (Configure Objects)] 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、FeedComment オブジェクト)とその項目が選択されています。

> 注：メールのスキャンは EmailMessage（受信）と EmailMessage（送信）に分かれており、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したい標準オブジェクトまたはカスタムオブジェクトを検索し、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後、行の最後にある歯車アイコンを選択して、スキャンする項目を選択し、クリック時保護を使用するかどうかを選択します。

> 注：クリック時保護は、100 文字を超える項目でのみ機能します。

> 注：最大 5 つの項目を選択できます。

5. [保存 (Save)] を選択します。
   Cloud Protection から、選択したオブジェクトのトリガーを設定するよう通知されます。
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、必要なすべての操作タイプが配置されていることを確認し、トリガーを保存します。

a) オブジェクト設定ページの [トリガー (Triggers)] 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(); }
```

角括弧 ([]) 内のセクションを変更します:

- [TRIGGERNAME]

  標準オブジェクト: オブジェクト API 名 + Trigger
  カカスタムオブジェクト: 末尾の _c を除いたオブジェクト API 名 + Trigger
- [OBJECTAPINAME]:: オブジェクトの API 参照名。

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、オブジェクトレコードを挿入し、トリガーコードをカバーします。
   テスト後、 変更セット（Change Sets）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本番環境に移動します。詳細については、[変更の開発とデプロイを行うツールの選択] (salesforce.com) を参照してください。

トリガーが設定されると、ステータスが [トリガーの設定 (Set a trigger)] から [オブジェクトの選択] ウィンドウの [項目が含まれています (Fields included)] に変わります

本番環境で使用を開始する前に、カスタムオブジェクトのスキャンをテストしてください。悪意のある URL イベントは [アナリティクス (Analytics)] セクションに報告されます。

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 (Remove object)] を選択します。

> 注 : カスタム URL スキャン用のオブジェクトを設定するには、ユーザーに Cloud Protection Admin権限セットが割り当てられている必要があります。

4.7 アラートの表示と検索の使用

セキュリティアラートを表示するには、以下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に移動し、[Cloud Protection] を開きます。
2. [アナリティクス (Analytics)] タブに移動します。
   - [アラート (Alerts)] ビューにはすべてのセキュリティアラートが表示されます。
   - [ファイルイベント (File Events)] ビューにはファイルスキャンからのすべてのイベントが表示されます。
   - [URL イベント (URL Events)] ビューには Web リンクのレピュテーションおよびカテゴリチェックからのすべてのイベントが表示されます。
   - [ID イベント (Identity Events)] ビューには ID リスク監視に関連するすべてのイベントが表示されます。
3. アラートまたはイベントの行の最後にある [表示 (View)] をクリックして、アラートまたはイベント履歴の完全な詳細を表示します。
4. 検索値を使用して、表示される結果を絞り込みます。サポートされている検索値:
   - 「アラート (Alerts) ビュー: TIME, SEVERITY, SOURCE, USER, REASON
   - 「ファイルイベント (File Events) ビュー: TIME, ACTION, VERDICT, FILENAME, FILETYPE, DIRECTION, LOCATION, SHA1, USER, IPADDRESS
   - URL イベント (URL Events) ビュー: TIME, ACTION, VERDICT, URL, DIRECTION, LOCATION, USER, IPADDRESS, CATEGORY
   - ID イベント (Identity Events) ビュー: TIME, RISK, USER

特定の日時のイベントを検索するには、現在のロケールに基づいた日時値を使用します。検索はすべての Salesforce SOQL 日付リテラルをサポートしています。

検索例:

- [アラート] ビューでファイル保護に関連する重大なアラートを検索する:
  SEVERITY=Critical, SOURCE=File Protection
- [ファイルイベント] ビューでブロックされたすべての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] ビューで Sales Report.xlsx ファイルのブロックされたすべての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] ビューでユーザーによって投稿されたブロック済みのすべての URL を検索する:ACTION=Blocked, DIRECTION=Post
- [URL イベント] ビューで IP アドレス 192.168.0.1 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)の場合)

- 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 ビジュアルフィルターの使用

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ました。

ビジュアルフィルターを見つけて使用する方法については、以下の手順に従ってください。

1. [アナリティクス (Analytics)] に移動し、以下のいずれかを選択します:
   - [アラート (Alerts)]
   - [ファイルイベント (File Events)]
   - [URL イベント (URL Events)]
   - [ID イベント (Identity Events)]
   - [ID (Identities)]
2. [項目の選択 (Select Field)] 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 (Apply filter)] をクリックします。

> 注 : サポートされている演算子は Equal (等しい) です。

> 注 : 合計で最大 10 個のフィルターを適用できます。フィルターは [アナリティクス] ページにとどまっている間、有効なままになります。[アラート]、[ファイルイベント]、[URL イベント] の間で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 (Summary)]) 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
アラート (Alerts)	日時 (Date/time), 深刻度 (severity), 送信元 (source), 理由 (reason: テキストボックス、255文字), ユーザー (user: テキストボックス、255文字)	
ファイルイベント (File Events)	日時 (Date/time), アクション (Action: 選択リスト), 判定 (verdict), ファイルタイプ (File type: テキストボックス、255文字), 方向 (Direction), 場所 (Location: テキストボックス、255文字)	テAction (選択リスト) は翻訳サービスで未サポートです。
URL イベント (URL Events)	日時 (Date/time), アクション (Action), 判定 (Verdict), 方向 (Direction), 場所 (Location: テキストボックス、255文字)	Location はカスタムオブジェクトをサポートします。
IDイベント	日時 (Date/time), リスク (risk), ユーザー (user: テキストボックス、255文字)	

ID (Identities)	ユーザー (User: テキストボックス、255文字), 最高リスク (highest risk), 日時 (date/time), 侵害 (breaches), 役割 (role: テキストボックス、255文字), プロファイル (Profile: テキストボックス、255文字)	
D > 概要 (Identities > Overview)	ユーザー (User), メール侵害 (Email breaches), リスクのある権限 (Risky permissions), Cloud Protection ライセンス (Cloud Protection license)	
ID > リスクのある権限	ユーザー (User), リスク (Risk)	
ID > 未ライセンスユーザー	ユーザー (User), ユーザー種別 (User	type)

4.9 レポートの表示と編集

Cloud Protection のレポート機能は、保護ステータスの簡単な概要を取得する場合と、攻撃を調査または対応する場合の両方で役立つ情報を提供します。

レポート情報には、発見された感染とその発生源などの感染関連の統計、安全なファイルと安全でないファイルの傾向の比較、現在保護されているファイルの量が含まれます。Cloud Protection for Salesforce は、最もよく使用されるファイルタイプ、最も頻繁に発生するソース、および最もアクティブなユーザーもレポートします。

Cloud Protection for Salesforce のレポートを表示するには、以下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に移動し、[Cloud Protection] を開きます。
2. [サマリー (Summary)] タブに移動します。
   [サマリー] ビューには、スキャンされたファイルとブロックされた URL の全期間の統計、およびアラートの総数が表示されます。

> 注 : アラートの数、特に 重大 (Critical) および 重要 (Important) としてリストされているアラートの数を監視することをお勧めします。これら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. 特定のタイプのアラートの絞り込まれたビューを表示するには、[アラート] テーブルの対応する数字をクリックします。
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、新しいカスタマイズされたレポートとして保存できます。
   レレポートのメール配信をスケジュールするには:

   a) [登録 (Subscribe)] 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) [受信者の編集 (Edit Recipients)] をクリックし、レポートを受信する他のユーザーを追加します。
   d) [保存 (Save)] 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、フォルダーを選択して、[作成 (Create)] をクリックします。
c) ツールバーの [コンポーネント (Component)] と [フィルター (Filter)] オプションを使用して、レポートに含める内容を選択します。
d) [保存 (Save)] をクリックします。
e) レポートの編集が完了したら、[完了 (Done)] 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 (Created By: Full Name)
- 作成日 (Created Date)
- 日付/時間 (Date/Time)
- ファイル拡張子 (File Extension)
- ファイル名 (File Name)
- ファイルスキャン ID (File Scan ID)
- ファイルサイズ (File Size)
- ファイルタイプ (File Type)
- IP アドレス (IP Address)
- 最終更新者: フルネーム (Last Modified By: Full Name)
- 最終更新日 (Last Modified Date)
- 名前 (Name)
- 所有者: フルネーム (Owner: Full Name)
- レコード ID (Record Id)
- スキャンタイプ (Scan Type)
- SHA1
- 場所 (Location)
- ユーザー: フルネーム (User: Full Name)
- 判定 (Verdict)
- 所有者 (名、フルネーム、姓、所有者 ID、電話番号、プロファイル: 名前、ルール: 名前、役職、ユーザー名、メール、別名、アクティブ)理由
- 理由 (Reason)
- ファイル普及率 (File Prevalence)
- ファイルレピュテーション評価 (File Reputation Rating)

URLレポートの属性：

- URL スキャン: ID (URL Scan: ID)
- URL スキャン: 名前 (URL Scan: Name)
- アクション (Action)
- カテゴリ (Categories)
- 日付/時間 (Date/Time)
- 方向 (Direction)
- IP アドレス (IP Address)
- 場所 (Location)
- 理由 (Reason)
- レピュテーション (Reputation)
- レピュテーションの説明 (Reputation Description)
- URL
- ユーザー (User)
- 判定 (Verdict)

- 所有者名 (Owner Name)
- 所有者別名 (Owner Alias)
- 所有者の役割 (Owner Role)
- 作成者 (Created By)
- 作成者別名 (Created Alias)
- 作成日 (Created Date)
- 最終更新者 (Last Modified By)
- 最終更新者別名 (Last Modified Alias)
- 最終更新日 (Last Modified Date)

4.10 製品のライセンス情報の表示

Cloud Protection for Salesforce の [ライセンス (License)] ページには、ライセンスのステータスと使用状況に関する詳細が含まれています。

1. システム管理者アカウントで Salesforce にログインします。
2. アプリケーションランチャーに移動し、[Cloud Protection] を開きます。
3. [管理 (Administration)] > [ライセンス (License)] ページに移動します。

> 注：多数のユーザーに対して一度にライセンスを割り当てたり割り当て解除したりする作業はバックグラウンドジョブとして実行されます。ジョブの実行中はウィンドウに進行状況インジケーターが表示されます。

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。

> 注：ライセンス使用状況 (License Usage): ライセンスタイプごとに、利用可能なライセンス数、保護されているユーザーと保護されていないユーザーの数、および使用されているライセンスの割合を表示します。

> 注：スキャン使用状況 (Scan Usage): 現在および前回の請求期間について、スキャンされたファイル数、スキャンされた URL 数、総スキャン数、および使用されたスキャン許容量の割合を表示します。

関連タスク

Cloud Protection ライセンスを指定する

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 データ処理地域の設定

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、Cloud Protection for Salesforce は最も近いデータ処理地域を自動的に選択します。社内にデータの処理場所の地理的指定を必要とするコンプライアンス、パフォーマンス、またはデータ居住性の要件がある場合は、以下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に移動し、[Cloud Protection] を開きます。
2. [管理 (Administration)] > [全般 (General)] に移動します。
3. [スキャン設定 (Scan Configuration)] の下で、[データ処理地域 (Data processing region)] 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 : [自動選択 (Automatic selection)] は、最も近いアクティブな地域を自動的に選択します。

4. [保存 (Save)] を選択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よう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 (Setup)] に移動して、[リモートサイトの設定 (Remote Site Settings)] を参照します。[リモートサイトの設定] 画面が開きます。
7. [リモートサイトの設定] 画面が開きます。[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 アイデンティティ保護の概要

Cloud Protection for Salesforceのアイデンティティ保護（Identity Protection）機能は、侵害されたユーザーアカウントによるリスクを監視・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し、組織内フィッシングキャンペーン、ランサムウェア攻撃、なりすましなどを可能にします。これらの攻撃は正規の会社アカウントを使用するため、検知が困難です。単一の侵害されたアカウントが、Salesforce環境全体を危険に晒す可能性があります。

このニーズに対応するため、Cloud Protection Identity Protectionでは、Salesforceのメールアドレスを使用して、標準ユーザーおよびコミュニティユーザーの侵害状態を監視できます。本機能では、初期状態で過去12ヶ月間の侵害レコードが表示され、その後は直近の侵害が表示されます。新しい侵害レコード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ユーザーまでサポートしています。

アイデンティティ保護のスキャンをスケジュール設定できます。Cloud Protection for Salesforceは、SHA-256でハッシュ化された形式でメールアドレスを収集し、侵害レコードを検索して結果を返します。各侵害レコードには以下が含まれます：

- 公開日（Published date）
- 重要度（Criticality）
- ロケーション（Location）
- 漏えいたユーザー（Exposed user）
- ユーザーの役割およびプロファイル（User roles and profiles）
- 侵害の説明（Breach description）

Cloud Protection for Salesforceのアイデンティティ保護機能は、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ています。

侵害監視に加えて、Cloud Protection for Salesforceは独立した「ユーザーアクセスおよび権限スキャン（user access and permission scan）」を提供します。このスキャンは、標準ユーザー、コミュニティユーザー、およびコミュニティログインユーザーを対象に、リスクのある権限割当や認証の弱点（多要素認証（MFA）やシングルサインオン（SSO）の欠如など）をチェックします。侵害監視とユーザーアクセスおよび権限スキャンは、それぞれ独立して有効化、スケジュール設定、実行されますが、どちらも「5.3 リスクのあるアイデンティティの監視」で説明する［リスクのあるアイデンティティ］（Identities at risk）ページに統合されます。

アイデンティティ保護を有効にするには、以下を行う必要があります：

- 接続アプリケーション（Connected App）が有効になっていることを確認する。
- 有効なCloud Protection for Salesforceユーザーライセンス数が、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する。

5.1 Salesforce組織でアイデンティティ保護を有効にする方法

アイデンティティ保護には、個別に有効化する2つのスキャンが含まれます：「侵害監視（breach monitoring）」と「ユーザーアクセスおよび権限スキャン（user access and permission scan）」です。

対象としたいユーザータイプごとに各スキャンを有効にします。以下のセクションでは、侵害監視およびユーザーアクセスと権限スキャンの有効化手順について説明します。

5.1.1 侵害監視の有効化

Salesforce組織で侵害監視を有効にするには、以下の手順に従ってください。

1. アプリケーションランチャーに移動し、[Cloud Protection] を開きます。
2. [設定] (Administration) に移動し、[アイデンティティ保護] (Identity Protection) を開きます。
3. [サードパーティのデータ侵害] (Third-party data breaches) の下で、[標準ユーザーのサードパーティデータ侵害を監視] (Monitor third-party data breaches for standard users) および/または [コミュニティユーザーのサードパーティデータ侵害を監視] (Monitor third-party data breaches for community users) のトグルを有効にします。

> 注： 組織が「すべてのユーザー」に設定されており、合計ユーザー数が購入済みのユーザーライセンス数以下である場合、標準ユーザー、コミュニティユーザー、またはその両方のタイプのユーザーのメールをスキャンできます。

> 注： 組織が「選択されたユーザー」モードであり、ライセンス保持ユーザー数が購入済みユーザー数以下である場合、標準ユーザー、コミュニティユーザー、またはその両方のタイプのユーザーのメールをスキャンできます。

> **重要**：統合ユーザーおよび自動化ユーザーはアイデンティティ保護の侵害スキャンから除外されるため、[設定] のライセンス数と不一致が生じます。

5.1.2 ユーザーアクセスおよび権限スキャンの有効化

Salesforce組織でユーザーアクセスおよび権限スキャンを有効にするには、以下の手順に従ってください。

1. アプリケーションランチャーに移動し、[Cloud Protection] を開きます。
2. [設定] (Administration) に移動し、[アイデンティティ保護] (Identity Protection) を開きます。
3. [ユーザーアクセスおよび権限スキャン] で、スキャンするユーザーの種類に応じてトグルを有効にします: [標準ユーザーのユーザーアクセスをモニタリング]、[コミュニティユーザーのユーザーアクセスをモニタリング]、および [コミュニティログインユーザーのユーザーアクセスをモニタリング]。[ユーザーアクセスおよび権限スキャン] (User access and permission scan) の下で、スキャンするユーザータイプのトグルを有効にします:[標準ユーザーのユーザーアクセスを監視] (Monitor user access for standard users)、[コミュニティユーザーのユーザーアクセスを監視] (Monitor user access for community users)、および/または [コミュニティログインユーザーのユーザーアクセスを監視] (Monitor user access for community login users)。

> 注： このスキャンは、侵害監視とは独立して権限セットの割り当てや認証設定(MFAやSSOの欠如など)を評価します。既知のメール侵害がないユーザーであっても、このスキャンによってフラグが立てられる場合があり、その逆も同様です。

> **注：ユーザーのリスクのある権限の監視(「5.6 ユーザーのリスクのある権限の監視」を参照)および [リスクのある権限] (Risky permissions) タブ(「5.3 リスクのあるアイデンティティの監視」を参照)は、このセクションの少なくとも1つのトグルが有効になってからデータが表示されます。**

> 注： トグルを初めて有効にするには、事前にスケジュール済みジョブを作成しておく必要があります。詳細は「5.2.2 ユーザーアクセスおよび権限スキャンのスケジュール設定」を参照してください。

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

侵害監視とユーザーアクセスおよび権限スキャンは、それぞれ独立してスケジュール設定されます。

侵害スキャンは希望する曜日と時間を使用するのに対し、ユーザーアクセスおよび権限スキャンはSalesforce標準の「Apexをスケジュール (Schedule Apex)」機能を使用してスケジュール設定します。以下のセクションでは、各スキャンのスケジュール設定手順について説明します。

5.2.1 侵害スキャンのスケジュール設定

侵害スキャンをスケジュール設定するには、以下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に移動し、[Cloud Protection] を開きます。
2. [設定] (Administration) に移動し、[アイデンティティ保護] (Identity Protection) を開きます。
3. [侵害] で、[侵害を確認する優先曜日と時刻] を設定します。[サードパーティのデータ侵害] (Third-party data breaches) の下で、侵害チェックを実行する [希望する曜日と時間] (Preferred week day and time) を設定します。

> 注：以下にご注意ください：
> - アイデンティティ保護の侵害ジョブが開始されると、完了までに3日かかります。つまり、次のスケジュール済みジョブは3日経過後にのみ実行できます。すべての侵害レコードは即座に確認可能ですが、アイデンティティ保護ジョブ完了アラートは3日後に発生します。
> - バッチの開始時および終了時に、Cloud Protection for Salesforceアプリケーション内にアラートが表示され、侵害ルックアップが進行中か完了したかを確認できます。
> - スケジュールされたスキャンが開始されてから3日以内に、アイデンティティ保護によって発見された侵害に関する更新が提供されます。

5.2.2 ユーザーアクセスおよび権限スキャンのスケジュール設定

Salesforce のネイティブな Schedule Apex 機能を使用して、ユーザーアクセスおよび権限スキャンをスケジュールします。

ユーザーアクセスおよび権限スキャンは、曜日・時間選択ツールを使用しません。代わりに、Salesforce標準の「Apexをスケジュール」機能を使用して設定します。

1. アプリケーションランチャーに移動し、[Cloud Protection] を開きます。
2. [設定] (Administration) に移動し、[アイデンティティ保護] (Identity Protection) を開きます。
3. [ユーザーアクセスおよび権限スキャン] (User access and permission scan) の下で、[新規作成] (Create new) を選択して正確なジョブ詳細があらかじめ入力された [Apexをスケジュール] ページを開き、希望するスケジュールを設定します。
4. [すべてのスケジュール済みジョブを表示] (Show all scheduled jobs) を選択すると、標準の [スケジュール済みジョブ] ページで既存のスケジュール実行を表示または管理できます。

5.3 リスクのあるアイデンティティの監視

Cloud Protection for Salesforceは、それぞれ異なるリスクシグナルをカバーする4つのタブを備えた [リスクのあるアイデンティティ] (Identities at risk) ページを提供します。

1. [アプリケーションランチャーに移動し、[Cloud Protection] を開きます。
2. [アイデンティティ] (Identities) に移動します。
3. 以下のいずれかのタブを選択します:
   - [概要] (Overview) – ユーザーごとにメール侵害、リスクのある権限、およびCloud Protectionライセンスのステータスを表示し、ユーザーのすべてのリスクシグナルを一目で確認できます。
   - [メール侵害] (Email breaches) – 既知のメール侵害があるユーザーを表示します:最高侵害リスク、最新侵害日、合計侵害数、役割、およびプロファイル。このタブは侵害監視の状況を反映します(「5.1.1侵害監視の有効化」を参照)。
   - [リスクのある権限] (Risky permissions) – 高リスクな権限が割り当てられているユーザーを表示します:最高リスク権限、合計リスク権限数、合計権限セット数、および合計権限セットグループ数。このタブはユーザーアクセスおよび権限スキャン(「5.1.2 ユーザーアクセスおよび権限スキャンの有効化」を参照)の状況を反映し、そのスキャンが有効化されている場合にのみデータを表示します。
   - [未ライセンスユーザー] (Unlicensed users) – Cloud Protectionライセンスを持っていないユーザー、そのライセンスステータス、およびユーザータイプ(標準、コミュニティ、またはコミュニティログイン)を表示します。
4. [検索] 項目を使用して結果を絞り込みます。サポートされる検索値はタブによって異なります:
   - 概要(Overview): USER, EMAIL_BREACHES, RISKY_PERMISSIONS, CLOUD_PROTECTION_LICENSE
   - メール侵害 (Email breaches): USER, HIGHEST_RISK, TIME, BREACHES, ROLE, PROFILE
   - リスクのある権限 (Risky permissions): USER, RISK
   - 未ライセンスユーザー (Unlicensed users): USER, USER_TYPE
5. 任意の行の [表示] (View) を選択すると、そのユーザーの [アイデンティティ詳細] (Identity Details) 画面が開き、以下が表示されます:
   - 一般情報 (General Information) – ライセンスステータス、SSO/MFAステータス、権限セット、権限セットグループ、およびキュー
   - 接続アプリケーション (Connected Apps) – 接続アプリケーション名、最終使用日、および使用回数
   - ファイルおよびURLイベントの概要 (File & URL Events Summary)
   - 侵害履歴 (Breach History) – 以下に記載する完全な侵害詳細
   - リスクのあるシステム権限 (Risky System Permissions) – 権限名および説明
   - ログイン履歴 (Login History)

   侵害履歴の詳細には、侵害日、タイトル、Webサイト、取得日、侵害カテゴリ、確信度、侵害メインカテゴリ、公開日、タイプ、レコード数、機密ソースフラグ、消費者カテゴリ、および侵害された組織が含まれます。

5.4 Salesforceユーザーのアイデンティティイベントの監視

Cloud Protection for Salesforce バージョン 3.0 では、Salesforceユーザーの侵害レコードを監視するための[アイデンティティイベント] (Identity events) が導入されました。

Salesforceユーザーの侵害レコードを監視するには、以下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に移動し、[Cloud Protection] を開きます。
2. [アナリティクス] (Analytics) に移動し、[アイデンティティイベント] (Identity Events) を開きます。
   各イベントには、侵害の日時、リスクタイプ、侵害理由、影響を受けたユーザー、およびその他の侵害情報が詳しく記載されています。[検索] 項目を使用して結果を絞り込むことができます。検索項目でサポートされている値は以下のとおりです:

- 時間（TIME）
- リスク（RISK）
- ユーザー（USER）

> 注：例えば、特定ユーザーのすべての重大な侵害を検索する場合：″RISK=Critical, USER=John Doe″ のように入力します。

5.5 アイデンティティ侵害アラートの監視

アイデンティティ保護の侵害ジョブはスケジュールされたスキャンの日時で実行されるため、アイデンティティ保護機能は、侵害チェックジョブが開始・完了した際や、ユーザーが新しい侵害に直面した際にアラートを生成します。

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. アプリケーションランチャーに移動し、[Cloud Protection] を開きます。
2. [アナリティクス] (Analytics) に移動し、[アラート] (Alerts) を開きます。
3. [表示] (View) をクリックして、特定のアラートに関する詳細情報を確認します。

> 注：アラート詳細モーダルには、侵害日時、重要度、理由、ソース、露出したユーザー、侵害における最高リスク、ユーザーあたりの合計侵害数、ユーザーの役割、ユーザーのプロファイル、および完全な侵害履歴を確認するためのアイデンティティセクションへのリンクが表示されます。

5.6 ユーザーのリスクのある権限の監視

アイデンティティ保護は、ユーザーに割り当てられている権限セットを評価し、高リスクなシステム権限が含まれているものにフラグを立てます。

ユーザーのリスクのある権限を表示するには、以下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に移動し、[Cloud Protection] を開きます。
2. [アイデンティティ] (Identities) に移動し、[リスクのある権限] (Risky permissions) を開きます。

   フラグが立てられた権限は、ユーザーごとに [リスクのある権限] タブおよび [概要] タブに表示されます。

   [リスクのある権限] タブには、ユーザーが保持している高リスクな権限と、それらの権限がどの権限セットおよび権限セットグループに属しているかが表示されます。

   [概要] タブには、メール侵害への露出やCloud Protection for Salesforceライセンスの欠如など、他のリスクシグナルとともにリスクのある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くなります。

第 6 章 アプリケーションのテスト

Cloud Protection for Salesforce アプリケーションのインストールと設定が完了したら、ファイル保護およびURL保護が正常に機能しているかをテストします。

6.1 ファイル保護のテスト

Eicarテストファイルを使用してファイル保護をテストするには、以下の手順に従ってください。

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

   > 注：有害ではありませんが、Eicar.com はテスト目的でマルウェアとして識別されます。アンチマルウェア保護によってファイルがブロックされる場合は、リアルタイムスキャンからフォルダを除外対象に設定し、そこに Eicar.com ファイルを配置してください。

2. Example_MaliciousFile.docx と任意のクリーン（安全な）ファイルを Salesforce Files 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に移動し、[Cloud Protection] を開きます。
4. [アナリティクス] (Analytics) > [ファイルイベント] (File Events) タブに移動します。
   クリーンファイルが1つと、ブロックされたファイルが1つ表示されます。
5. 両方のファイルをダウンロードしてみます。
   クリーンファイルはダウンロードできますが、悪意のあるファイルはブロックされます。
6. 再び [アナリティクス] (Analytics) > [ファイルイベント] (File Events) タブに戻り、ダウンロードイベントを確認します。
7. [表示] (View) をクリックして、完全なイベント履歴を確認します。
   選択したファイルに対するすべてのアップロードおよびダウンロードのアクションが表示されます。

6.2 URL保護のテスト

テスト用ドメインを使用してURL保護をテストするには、以下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に移動し、[Cloud Protection] を開きます。
2. [設定] (Administration) > [URL保護] (URL Protection) タブに移動します。
3. このテストでは、[許可されないカテゴリを選択] (Select disallowed categories) リストで [ギャンブル] (Gambling) が選択されていることを確認します。
4. 2つのサンプルURL unsafe.fstestdomain.com と gambling.fstestdomain.info を Salesforce Chatter に投稿します。
5. Chatter を開き、URLが書き換えられた2つの新しい投稿を確認します。
6. Cloud Protection に戻り、[アナリティクス] (Analytics) > [URLイベント] (URL Events) タブに移動します。
   2つの新しい Chatter 投稿が表示されます。
7. Chatter に戻り、両方のリンクを開こうとしてみます。[有害なWebサイトがブロックされました] (Harmful website blocked) および [許可されていないWebサイトがブロックされました] (Disallowed website blocked) というブロックページが表示されます。
8. 再び Cloud Protection に戻り、[アナリティクス] (Analytics) > [URLイベント] (URL Events) タブに移動します。

2つのURLオープンイベントが表示されます。。

9. [表示] (View) をクリックして、完全なイベント履歴を確認します。
選択したURLに対するすべての投稿およびアクセスの操作が表示されます。

第 7 章 アンインストール

本セクションでは、組織から Cloud Protection for Salesforce を削除する手順について説明します。

アプリケーションの削除には以下の手順が含まれます:

- 権限セットの割り当ての削除
- アプリケーションのアンインストール

7.1 権限セットの割り当ての削除

Cloud Protection for Salesforce アプリケーションをアンインストールする前に、Salesforce組織内のユーザーに割り当てた Cloud Protection User および Cloud Protection Admin 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に移動し、[Cloud Protection] を開きます。
3. [設定] (Administration) > [ツール] (Tools) > [詳細設定] (Advanced) セクションに移動し、[すべての権限セットの割り当てを解除] (Unassign all permission sets) をクリックします。開いた [すべての権限セットの割り当てを解除] ウィンドウで、[すべての権限セットの割り当てを解除] をクリックして確認します。
4. 組織の設定に移動し、[設定] (Setup) をクリックします。
5. [ユーザー] (Users) > [権限セット] (Permission Sets) > [Cloud Protection Admin] を選択します。
6. [割り当ての管理] (Manage Assignments) をクリックします。
7. すべてのユーザーを選択し、[割り当ての削除] (Remove Assignments) をクリックします。
8. [OK] をクリックして、すべてのユーザーを削除することを確認します。

7.2 アプリケーションのアンインストール

すべてのユーザー権限を削除した後、Cloud Protection アプリケーションをアンインストールする必要があります。

Cloud Protection アプリケーションをアンインストールするには、以下の手順に従ってください:

1. システム管理者アカウントで Salesforce にログインします。
2. 組織の設定に移動し、[設定] (Setup) を選択します。
3. [アプリ] (Apps) > [インストール済みパッケージ] (Installed Packages) に移動します。
4. Cloud Protection の横にある [アンインストール] (Uninstall) を選択します。
5. [パッケージのアンインストール] (Uninstalling a Package) ページで下にスクロールし、[はい、このパッケージをアンインストールして、関連するすべてのコンポーネントを永久に削除します] (Yes, I want to uninstall this package and permanently delete all associated components) を選択します。

Cloud Protection アプリケーションのアンインストールが完了すると、確認のメール通知が届きます。