Cloud Protection for Salesforce

Agentforce Extension

Agentforce 拡張パッケージマニュアル

目 次

第1章 Agentforce拡張機能の概要 5
1.1 Cloud Protection for Agentforce のユースケース 5
第2章 Cloud Protection for Agentforce の展開 7
2.1 前提条件 7
2.2 AgentExchange Marketplace を使用した Cloud Protection for Agentforce のインストール 8
2.3 Salesforce ポータルを使用した Cloud Protection for Agentforce のインストール 9
2.4 URLスキャン機能の設定 9
2.5 エージェントアクションの構成 10
2.6 エージェントへのトピックの割り当て 10
2.7 トピックの設定 11
2.8 権限セットの割り当て 11
第3章 高度なエージェントトピックの設定 13
3.1 変数の設定 13
3.2 フィルターの設定 13
3.3 出力変数のマッピング 14
第4章 Agentforceアクションアラート通知 15
4.1 Agentforceアクションのメール通知設定 15

第 1 章 Agentforce拡張機能の概要

Salesforce は、生成 AI、Data Cloud、大規模言語モデル（LLM）などの最先端技術を活用し、Agentforce アプリケーション開発に投資することで、プラットフォームを戦略的に進化させています。これらの革新は、インテリジェントエージェントがユーザーとのやり取りに基づいてコンテキストを認識したアクションを実行できるようにすることで、Service Cloud、Marketing Cloud、Experience Cloud を含む Salesforce の主要製品全体の自動化を強化することを目的としています。

この変革の一環として、Agentforce アクションを使用すると、AI エージェントはカスタムワークフローを呼び出すことでユーザーのプロンプトに応答できます。これらのワークフローでは、Salesforce レコードの更新や操作に使用される URL を取得するために、内部システムまたは外部システムへの REST API 呼び出しを行うことがよくあります。これらのやり取りの動的な性質を考慮すると、取得された URL が安全で、害がなく、許可されていないカテゴリに属していないことを確認することが非常に重要です。

このニーズに対応するため、Cloud Protection for Agentforce は、URL が処理される前に検証する保護層を導入しています。これは、Salesforce の Service Cloud と統合された機能である Agentforce チャットによって有効になるリアルタイムコミュニケーションのシナリオにおいて特に重要です。Agentforce チャットは顧客とのライブ会話を促進し、ケース、取引先責任者、または取引先にリンクされる可能性のあるトランスクリプトレコードを保存します。

AI 駆動の会話において、ユーザーは、ケースレコードの変更やトランスクリプトへの悪意のあるコンテンツの挿入など、機密データを操作しようとする URL を不注意または悪意を持って提供する可能性があります。適切な検証が行われない場合、これらのアクションによってデータの整合性が損なわれ、セキュリティ上のリスクが生じる可能性があります。

Cloud Protection for Agentforce は、Agentforce アクションを通じて取得されたすべての URL が徹底的にチェックされることを保証し、Salesforce 管理者が AI エージェントによる強力な自動化を実現しながら、安全な環境を維持できるように支援します。

1.1 Cloud Protection for Agentforce のユースケース

本章では、Cloud Protection for Agentforce パッケージが Salesforce 環境内のセキュリティと運用効率を向上させる主要なシナリオの概要を説明します。AI パワードワークフローにリアルタイムの URL スキャンを統合することで、このエクステンションは、悪意のあるコンテンツが内部データや顧客とのやり取りを損なうのを防ぐのに役立ちます。

内部運用のための AI アシスタンス

課題:

Einsteinチャットは、レコードの作成、更新、変更を支援することで、従業員の効率を大幅に向上させます。ただし、内部ユーザーが不注意で外部ソースからの URL を AI チャットに貼り付けるリスクがあります。これらの URL が悪意のあるものであり、Salesforce レコードに保存された場合、プラットフォームに対するセキュリティ上の脅威となる可能性があります。

解決策:

Cloud Protection for Agentforce は、Einstein AI チャット内でリアルタイムの URL スキャンを提供します。これにより、悪意のあるリンクを検知してブロックすることで、内部運用を保護します。

Salesforce 管理者は、Cloud Protection for Agentforce パッケージを次のように設定できます：

- 安全でない URL リストをブロックする。

- 許可しない URL リストを定義する。
- 脅威が検知されたときにアラートを受信する。

サービスエージェントによるサポート

課題:

Salesforce のお客様は以前、パーソナライズされた顧客対応をサポートするために、ウェブチャット、MIAW、ライブチャットなどのツールを使用していました。現在、Agentforce と Einstein AI エージェントの導入により、このやり取りの多くが自動化され、場合によっては人間のエージェントと AI エージェントが連携して機能しています。これらの AI エージェントは、Experience Cloud やサードパーティアプリケーションに埋め込まれた外部ユーザーを介してゲストユーザーとやり取りします。ただし、組み込みのコンテンツスキャン機能がないため、これらのやり取りを通じて悪意のある URL が Salesforce に導入されるリスクが高まります。

解決策:

Cloud Protection for Agentforce は、AI を活用したサービス対応中に URL のリアルタイムスキャンを可能にします。AI エージェントが問題を解決できず、人間のエージェントにエスカレーションした場合、このエクステンションは、AI エージェントと共有された可能性のある有害または許可されていない URL をクリックしないようにエージェントに警告する安全装置として機能します。

管理者は、Cloud Protection for Agentforce パッケージを次のように設定できます :

- 悪意のある URL をブロックする。
- 許可しない URL カテゴリを定義する。
- 脅威が検知されたときにアラートを受信する。

このユースケースにより、安全な顧客コミュニケーションが確保され、エージェントが安全でないコンテンツとやり取りするのを防ぎます。

第2章 Cloud Protection for Agentforce の展開

本セクションでは、Salesforce 組織に Agentforce アクションエクステンションパッケージを展開およびセットアップするための手順を提供します。

Cloud Protection for Agentforce の展開には、以下の手順が含まれます:

- Cloud Protection for Agentforce のインストール
- Agentforce アクションでの URL スキャンのセットアップ

2.1 前提条件

Cloud Protection for Agentforce パッケージを展開する前に、以下の条件が満たされていることを確認してください。

Cloud Protection for Salesforce がインストールされていること

> **重要** : Cloud Protection for Agentforce パッケージをインストールする前に、Cloud Protection for Salesforce アプリケーションのバージョン 2.9.1 以上がインストールされていることを確認してください。Cloud Protection for Agentforce エクステンションは、メインアプリケーションによって提供されるコアコンポーネントに依存しています。

> **注** : Cloud Protection for Salesforce アプリケーションをアップグレードする必要がある場合は、更新前に選択リスト値を有効化してください (更新前に選択リスト値を有効化)。

> **注** : Cloud Protection for Salesforce をインストールしていない場合は、AgentExchange からダウンロードできます。
>
> - グローバルのAgentExchange
> - 日本語版 のAgentExchange
>
> Cloud Protection for Salesforce アプリケーションをインストールおよび設定するには、こちらで利用可能な手順を使用してください: Cloud Protection for Salesforce アプリケーションのインストール。アプリケーションをインストールするには、Salesforce 組織への管理者権限が必要です。

Cloud Protection for Agentforce パッケージがインストールされていること。

Cloud Protection for Salesforce アプリケーションがインストールされたら、Cloud Protection for Agentforce エクステンションをインストールする必要があります。

> **注** : 新しいエクステンションをインストールする方法は2つあります。
>
> 1. Agentforce の AI Agent Marketplace（AgentExchange）から Cloud Protection for Agentforce パッケージを直接ダウンロードできます。
> 2. Salesforce ポータルから Cloud Protection for Agentforce を直接ダウンロードできます（この2番目のオプションについては、本章の次のセクションで説明する手順を使用してください）。

> **重要：**ソリューションをインストールするには、Salesforce 組織に Agentforce クレジットが必要です。

Agentforce アクション設定が有効になっていること

Cloud Protection for Salesforce アプリケーション（バージョン 2.9.1 以上）および Cloud Protection for Agentforce エクステンションがインストールされたら、以下の構成設定を有効にする必要があります：

- **有害なURLスキャン**
- **許可されていない URL スキャン**

> **注：**提案された設定を有効にするには、「URL スキャンのセットアップ」セクションで説明されている手順に従ってください。

> **重要：**これらの設定は、Cloud Protection for Agentforce パッケージがインストールされた後にのみ有効になります。エクステンションが存在しない場合、Cloud Protection for Salesforce アプリケーションでこれらのオプションを有効にしても、機能上の影響はありません。

2.2 AgentExchange Marketplace を使用した Cloud Protection for Agentforce のインストール

本セクションでは、AgentExchange Marketplace から直接 Cloud Protection for Agentforce パッケージをインストールするための手順を提供します。

AgentExchange Marketplace から Cloud Protection for Agentforce を直接インストールするには、以下の手順に従います。

1. Agentforce の AI エージェント マーケットプレイス（AgentExchange）にアクセスします。
2. Cloud Protection for Agentforce拡張機能を検索して開きます。
3. [Get It Now]（今すぐ入手）をクリックします。

> **重要：**Salesforce 組織に Cloud Protection for Salesforce バージョン 2.9.1 以上がインストールされていることを確認してください。Cloud Protection for Agentforce パッケージは、Cloud Protection for Salesforce アプリケーションによって提供されるコアコンポーネントに依存しています。

> **注：**Cloud Protection for Salesforce パッケージをインストールするには、Cloud Protection for Salesforce ユーザーガイドマニュアルで利用可能な手順を参照してください。

Cloud Protection for Agentforce パッケージが正常にインストールされました。

2.3 Salesforce ポータルを使用した Cloud Protection for Agentforce のインストール

本セクションでは、Salesforce ポータルから直接 Cloud Protection for Agentforce パッケージをインストールする手順を説明します。

Salesforce ポータルから Cloud Protection for Agentforceパッケージを直接インストールするには、次の手順に従ってください。

1. [Topics] (トピック) に移動します。
2. [New] (新規) → [Add from AgentExchange] を開きます。
3. Cloud Protection for Agentforce パッケージを選択します。
4. パッケージをインストールします。

   エクステンションパッケージがすでにインストールされている場合は、[Add from Asset Library] から直接エージェントアクションを追加してください。

> **重要** :Salesforce 組織に Cloud Protection for Salesforce アプリケーションバージョン 2.9.1 以上がインストールされていることを確認してください。Cloud Protection for Salesforce アプリケーションをインストールするには、ユーザーガイドマニュアルの指示を参照してください。Cloud Protection for Agentforce パッケージは、Cloud Protection for Salesforce アプリケーションによって提供されるコアコンポーネントに依存しています。

これで Cloud Protection for Agentforce パッケージのインストールは正常に完了です。

2.4 URLスキャン機能の設定

Cloud Protection for Agentforce パッケージをインストールした後、Agentforce Actions の URL スキャンを設定する必要があります。

Agentforce アクションの URL スキャンを設定するには、以下の手順に従ってください。

1. [Administration] (管理) に移動し、[URL Protection] (URL保護) を開きます。
2. [General] (全般) セクションにある [Scan URLs] トグルを有効にします。
3. [Settings] (設定) の下にある以下の設定を有効にします。
   - エージェントアクションからの URL を有害な URL スキャンに含める。
   - エージェントアクションからの URL を許可されていない URL スキャンに含める。

> **重要** : これらの設定は、Cloud Protection for Agentforce パッケージがインストールされた後にのみ有効になります。エクステンションが存在しない場合、Cloud Protection for Salesforce アプリケーションでこれらのオプションを有効にしても、機能上の影響はありません。

2.5 エージェントアクションの設定

本セクションでは、Service Agent で使用する Agent Actions を設定するための情報を提供します。

エージェント アクションを構成するには、次の手順に従ってください。

1. [Setup] (設定) に移動し、Agentforce Studio を検索します。
2. [Agentforce Studio の下にある [Agentforce Agents] を開きます。
3. 悪意のあるコンテンツに対して保護する必要のあるエージェントのタイプを選択します。
4. 下向き矢印をクリックして、[Open in Builder] オプションを選択します。
5. Salesforce が推奨するように、設定が調整されるまでエージェントを無効化します(エージェントの有効化または無効化)。

2.6 エージェントへのトピックの割り当て

エージェントに割り当てるトピックを選択する必要があります。

> 事前確認 : 変更を行うには、Salesforceの推奨に従い、設定が調整されるまでエージェントを無効にしてください。(エージェントの有効化または無効化)

エージェントに割り当てられたトピックを選択するには、以下の手順に従います。

1. [Topics] (トピック) に移動します。
2. 要件に応じて Topic Label を作成します。
3. Topic Action を選択します

   (参考として、ここでは Customer Experience Support というトピックラベルを作成しました。)
4. [This topic's Actions] に移動します。
5. [New] をクリックし、[Add from Asset Library] を選択します。
6. Scan URLs トピックアクションを選択します。

> 注 : Cloud Protection for Agentforce パッケージがインストールされていない場合は、[Add from AgentExchange] を選択してパッケージをインストールできます。エクステンションパッケージがインストールされると、アセットライブラリに Scan Url アクションが表示されます。

7. [Topics] セクションに移動します。
8. トピックラベル Customer Experience Support を選択します。
9. [This Topic's Actions] の下で Scan URLs アクションを選択します。
10. [Finish] をクリックします。

2.7 トピックの設定

本セクションでは、トピックに指示を追加するための手順の概要を説明します。

トピックに指示を含めるには、以下の手順に従います。

1. [Topic] → [Topic Details] に移動します。
2. [Topic Configuration] の下に指示を追加します。

> 注 :指示は、組織の要件に応じてカスタマイズして追加する必要があります。

> ヒント : 以下は、悪意のある URL をスキャンするための指示の例です。
>
> 1. ユーザー入力を常に Apex アクション Scan_Urls に渡します。このアクションは、最優先事項として、他のどのアクションよりも前に実行する必要があります。応答は、リッチテキスト出力を持つ ″message″ コンポーネントを使用してユーザーチャットウィンドウに表示する必要があります。出力が空の場合は、URL スキャンに関連する内容をユーザーに伝えずに、次のアクションに進みます。
>
> > **重要 :**
> >
> > 出力には、有害な URL と許可されていない URL を2つの別々のセクションに明確に表示する必要があります。これは優先度の高いタスクであり、一貫して適用する必要があります。
> > これは優先度の高いタスクであり、一貫して適用する必要があります。
>
> 2. Scan_Urls が実行され、その応答がユーザーに表示されるまで、他のアクションは実行されません。
> 3. 変更を保存し、エージェントを有効化します。

2.8 権限セットの割り当て

本セクションでは、Agent ユーザーへの権限セット割り当て手順を説明します。URL スキャンの呼び出しには Agentforce 権限セットが必須です。

エージェントユーザーに権限セットを割り当てるには、以下の手順に従います。

1. Agent Builder の [Settings] セクションに移動し、エージェントユーザー（例: Agentforce Service Agent (ASA)）を特定します。
2. 以下の権限セットを割り当てます。
   - 社内ユーザー向けの場合:
     - Cloud Protection User 権限セットが割り当てられている場合は、Cloud Protection Agent User – Extension のみを割り当てます
     - Cloud Protection User 権限セットが割り当てられていない場合は、Cloud Protection Agent User と Cloud Protection Agent User – Extension の両方の権限セットを割り当てます。

- Einstein Agent User プロファイルを持つ Agentforce Service Agents (ASA) の場合:

  - Cloud Protection Agent User と Cloud Protection Agent User – Extension の両方の権限セットを割り当てます。

> 重要: 必要なコンテンツ保護を確保するため、以下の両方の権限セットを社内ユーザーおよびサービスエージェントユーザーに割り当てる必要があります。
>
> - Cloud Protection Agent User
> - Cloud Protection Agent User – Extension

上記の設定が完了したら、以下の手順を行います。

1. エージェントを有効化します(エージェントの有効化または無効化)
2. [Conversation Preview]を更新します。
3. Cloud Protection for Salesforceアプリケーションで構成された設定に従ってエージェントをテストします。

第3章 高度なエージェントトピックの設定

本章では、エージェントトピックの高度な設定を行うための手順の概要を説明します。

高度なエージェントトピックの設定には、以下のコンポーネントが含まれます。

- 変数の設定
- フィルターの設定
- 出力変数のマッピング

3.1 変数の設定

変数は、トピックおよびアクションの選択に対する決定論的なロジックと安全なデータ処理を提供することで、エージェントの動作を制御および強化する重要なコンポーネントです。

1. [Context] セクションに移動し、[Variables] を確認します。
2. [New Variable] をクリックします。
3. 以下を入力します：
   - **API name**
   - **Description**
   - **Data type: Boolean**

> 注：[カスタム変数]の下に、2つの Boolean 変数の例があります：
>
> - API 名が Has_Harmful_Content でデータ型が Boolean の Has Harmful Content。
> - API 名が Has_Disallowed_Content でデータ型が Boolean の Has Disallowed Content。
>
> 変数 Has Harmful Content は有害な URL から保護し、
>
> 変数 Has Disallowed Content は許可されていない URL カテゴリから保護します。

4. 「Has Harmful Content」および 「Has Disallowed Content」、または作成した変数名を選択ください。

> **注：**[Allow value to be set by API] または [Allow LLM to use value] は選択しないでください。
> [Allow LLM to use value] を選択すると、AI が判断や出力にその値を使用できるようになります。

3.2 フィルターの設定

フィルターの主な目的は、有害なコンテンツまたはブロックされたコンテンツが検知された場合に、指定された変数を使用してアクションが実行されないようにブロックすることです。

フィルターを設定するには、以下の手順に従ってください。

1. [Context] セクションの [Filters] に移動します。
2. [New] をクリックします。
3. 名前を入力し、フィルター条件を指定します。
4. [Resource] オプションで、前の手順で作成した変数を選択します。
5. Operator（演算子）と Value（値）を追加します。

設定例：

1. Filter1: Is Safe to Proceed (Harmful)
   - Resource → Has Harmful
   - Operator → Does Not Equal (次の値と等しくない)
   - Value → True

   これにより、エージェントでやり取りされた URL に有害なコンテンツがないかスキャンされ、Cloud Protection for Salesforce の設定に基づいてアクションが実行されます。

2. Filter2: Is Safe to Proceed (Disallowed)
   - Resource → Has Disallowed
   - Operator → Does Not Equal (次の値と等しくない)
   - Value → True

   これにより、Agent内で対話された禁止URL禁止コンテンツがスキャンされ、Cloud Protection for Salesforce アプリケーションの設定に基づいてアクションが実行されます。

3.3 出力変数のマッピング

Scan URLs アクションから正しく出力変数をマッピングする必要があります。

1. Scan URLs アクションから正しい出力変数をマッピングします。
   a) containsDisallowedUrl -> Has disallowed
   b) containsHarmfulUrl -> Has Harmful
   c) message Output Rendering -> Rich Text
2. 安全でないコンテンツまたは禁止されたコンテンツが検出された場合にアクションを制限するには、フィルターを使用します。

> 注：ブール値（Boolean）の Has Harmful Content および Has Disallowed Content を使用して、独自のフィルターを作成できます。フィルターは Scan URLs 以外の他のアクションに適用できます。

> 重要：これらのフィルターを Scan URLs Agent Action 自体には追加しないでください。

第 4 章 Agentforceアクションアラート通知

Agent Action エクステンションパッケージには、AI を活用したエージェントのやり取り中の視認性とセキュリティを向上させるために設計された、堅牢なアラートおよびイベント生成システムが含まれています。AI エージェントのやり取り中に検知されたセキュリティ上の脅威をタイムリーに把握できるように、Agent Action エクステンションパッケージには、有害な URL および許可されていない URL に対する設定可能なメール通知が含まれています。

主な機能:

1. すべての URL に対するイベント生成

   エージェントチャットに投稿されたすべての URL はイベントとしてログに記録されます。これにより、ユーザーインタラクションの完全な追跡可能性が確保されます。

2. 悪意のある URL または禁止された URL に対するアラート

   URLが悪意のあるものと判定された場合、または禁止カテゴリに属している場合、アラートが自動的に生成されます。これにより、潜在的な脅威に迅速に対応できます。

3. 設定と接続の問題に関するシステムアラート
   以下の場合にもアラートがトリガーされます

   - Agentforce スキャン設定が変更された場合
   - 拡張機能パッケージの接続が切断された場合
   - 拡張機能パッケージでエラーが検出された場合

4. 詳細なURLイベントメタデータ

   各 URL イベントには次の情報が含まれます。

   - 日時 (Date/Time)
   - 判定結果 (Verdict 例: 安全、悪質)
   - 実行されたアクション (Action taken)
   - 判定の理由 (Reason for the verdict)
   - URL
   - 方向 (Direction 例: インバウンド / アウトバウンド)
   - 場所 (Location 例: チャット、トランスクリプト)
   - ユーザー (User)
   - IP アドレス (IP Address)

4.1 Agentforceアクションのメール通知設定

本セクションでは、Agentforce Action のメール通知を設定する手順を説明します。

Agentforce Action の URL スキャンおよび禁止 URL に関するメール通知を設定するには、以下の手順に従ってください。

1. [Administration] (管理) に移動し、[URL Protection] (URL保護) を開きます。
2. [Notifications] (通知) セクションの下で、以下のトグルをオンにします。
   - エージェントアクションから有害な URL が検知されたときにセキュリティアラートを送信する
   - エージェントアクションから許可されていない URL が検知されたときにセキュリティアラートを送信する

これで Agentforce Actions のメール通知設定は正常に完了です。