Automation Anywhere クラウドに根ざす 顧客データの「プライバシー ファースト」

Automation Anywhere® のクラウド ポートフォリオは、ホスト型のサービス配信プラットフォームです。クラウド ポートフォリオには、クラウド上でホストされる統合型 Control Room と Bot 作成機能、そして顧客のインフラストラクチャ上でクラウド接続型 Bot Runner ノードを実行する機能が含まれています。IQ Bot™ など、他の製品は、クラウドでホストすることもできます。

クラウドのサービスは、データのプライバシーを確保するように設計されており、GDPR およびその他のデータ プライバシーの原則とガイドラインに従っています。

データ セキュリティ

導入アーキテクチャでは、お客様のデータとインフラストラクチャを保護するための「プライバシー ファースト」アプローチを採用しています。

顧客ネットワーク上の Bot Runner とクラウドに存在する Control Room 間のデータ接続は暗号化されます。HTTPS や TLS 1.2 などの安全な暗号化プロトコルが、移動中のデータの暗号化に使用されます。クラウドに格納されているデータの場合は、保存データ用の暗号化 (AES 256 ビットなど) が使用されます。

クラウド サービスが展開されているクラウドの運用、暗号化テクノロジー、および環境のネットワーク セキュリティをカバーする完全なセキュリティに対する姿勢については、こちら <insert URL> のクラウド セキュリティ運用ガイドに説明されています。

データ収集

導入モデルには、クラウド上で Bot を構築し、クラウドの Control Room から Bot の導入を管理するユーザーが含まれます。Bot が構築されると、ユーザー自身のコンピューティング インフラストラクチャで実行できるようにテストおよび展開されます。

次の表は、Automation Anywhere クラウド ポートフォリオで収集されたデータを示しています。この表は、自然人の特定に使用できる可能性のあるデータに関するガイダンスを提供します。

データ項目	データ カテゴリ	内容
ユーザー名	個人	電子メール、姓と名、優先名、タイム ゾーン、最後のログイン、パスワード、質問セット、AD ドメイン
ユーザー パスワード	個人	
パスワード セキュリティ キー	個人	Credential Vault パスワード セキュリティ キー
Bot Runner デバイス アクセス	個人	デバイスのユーザー名とアクセス資格情報
ロールの定義	個人	管理者、作成者など
ユーザー、デバイス、リソースにマップされたロール	個人	ユーザー ロール
Bot デバイス IP / FQDN	個人	一人のユーザーに紐付け可能なデバイス IP アドレスまたは FQDN
Bot 定義 (リポジトリ)	メタデータ	Bot の定義の一部として格納されるデータ
Bot アプリケーションの資格情報	個人	アプリケーション ユーザー、URL、公開キー、ルーティング名
Control Room の Bot スケジュール	メタデータ	Bot 管理、Bot を実行するタイミングと場所
WLM ワークフロー定義	メタデータ	Bot を実行するタイミングと場所、およびシーケンス
監査ログ	個人	識別子が含まれる場合あり : デバイス メッセージ ログ、導入メッセージ ログ、E メール メッセージ ログ、ジョブ実行ログ : (開始 / 終了時刻、ユーザー ID、スケジュール、自動化名、導入 ID。デバイス名、Bot 名、ユーザー名)、 ユーザー管理編集ログ、 Credential Vault メッセージ ログ、 サーバーとデータベースの変更ログ
エラー ログ	個人	識別子が含まれる場合あり
オペレーショナル アナリティクス	メタデータ	サービス ステータス
使用状況データ	メタデータ	機能の使用状況、有効なライセンス、個人 / ユーザーのデータ識別子なしで集計されます。 IQ Bot の場合 : インスタンス、ドメイン、運用統計、検証の変更、アップロードされたドキュメント、および抽出結果を学習するユーザー。
使用状況データ	個人 / メタデータ	インスタンス、ドメイン、運用統計、検証の変更、ユーザーがアップロードしたドキュメント、および抽出結果を学習するユーザー。

データの使用

運用とサポート

クラウド運用では、サービス SLA <link here> に従ってサービスを運用、拡張、およびサポートするために、導入システムと運用パフォーマンスを監視します。オートメーション・エニウェアは、一般に、上記に記載された顧客データを見ることはできません。

サポート サービスがトラブルシューティングや問題解決のためにアクセスする必要がある場合は、サポート担当者が適切な顧客の許可を得たうえでのみ、これらの情報にアクセスします。

オートメーション・エニウェアでは製品を改善するために次のことを行います。

- 製品の改善を目的とした機能の使用状況データの分析 (例: 機能の使用状況を把握するためのテレメトリーの追加)。これは、オートメーション・エニウェアによる製品の優先順位付けや改善の追加に役立ちます。その例には次のようなものがあります。
    - Excel コマンドの使用頻度をレビューして、今後のリリースに追加するコマンドの優先順位付けに役立てます。
    - 運用上のベスト プラクティスに関する推奨事項を提供します。
    - 更新、セキュリティ保護、およびトラブルシューティングのために使用されるサポート サービスを提供します。
    - 製品をカスタマイズし、推奨事項を作成します。
    - IQ Bot では、顧客データを使用して AI 学習スキルの品質向上を図ります。

オートメーション・エニウェアのデータ プライバシー ポリシーに関する詳細情報については、次の資料 (英語) を参照してください。https://www.automationanywhere.com/in/privacy

サブスクリプションの終了後のデータ保持

オートメーション・エニウェアは、顧客データ、構成 (Bot)、IQ Bot データ、およびほとんどのログを、顧客のサブスクリプション終了後 30 日間保持します。一部のログは、お客様のサブスクリプション終了後、最大 180 日間まで保持されることがあります。

データ処理補足契約書およびデータ保存ポリシーの全詳細については、次の資料 (英語) をご覧ください。https://www.automationanywhere.com/support/DPA.pdf

データ保護

Automation Anywhere は広範囲にわたるセキュリティ機能を備えており、データ保護を自動的に提供することも、設計に基づいて構成して提供することもできます。すべてのエンタープライズ アプリケーションと同様に、セキュリティ制御の一貫した適切な活用は、このエンタープライズ アプリケーションを使用する組織に委ねられます。ユーザーの承認は IT 管理者が担います。IT 管理者は承認された担当者のみがアクセスできるように制御を実装する必要があります。

データ所有者は、ビジネス ニーズを持つ権限のある担当者のみがサービスにアクセスできるよう徹底する必要があります。アクセス権を持つ企業ユーザーには、ロール ベース アクセス制御 (RBAC) を使用してきめ細かなアクセス制御 (RBAC) を付与できます。RBAC モデルは、運用環境内での二重制御と役割の分離を保証します。アクセス許可は、資格情報、Bot、Bot Runner、Bot Creator、Bot のスケジュール、IQ Bot 学習インスタンス、監査ログ アクセス、ワークロード管理キュー、プールなど、製品運用のすべての側面で実装できます。

Automation Anywhere は、すべてのユーザー アクションがプラットフォーム内で監査される完全監査機能を持ち、運用担当者が実行したすべてのアクセスとアクションの記録を提供します。監査は、NIST AC-6 で定義されているベスト プラクティスに準拠するために、すべての特権ロールおよび非特権ロールに対して自動化されています。

Bot は顧客のビジネス専門家が開発するソフトウェア プログラムのため、必要とされる最先端の安全なソフトウェア開発ライフサイクル (SDLC) プロセスは顧客によって実装される必要があります。そのため、Automation Anywhere は、前述のように個々の導入と RBAC を組み合わせることで、開発、テスト、および本番環境の分離をサポートします。

仮名化

GDPR には、データを保護するための適切な技術的手段として、仮名化が明示されています。仮名化では、データを人為的な識別子に変換します。これにより、コントローラーおよびプロセッサーに、別に管理されている追加情報なしにはデータを使用して自然人を特定することができない、データの処理方法が提供されます。トークン化は、後で参照できるようにデータを変換するもう 1 つのアプローチですが、トークン化されたデータは自然人の特定には使用できません。

オートメーション・エニウェアでは、開発環境およびテスト環境でのデータの仮名化をお勧めしています。IQ Bot の場合、本番環境にあるドキュメントや画像は実際のユーザー情報で処理されます。これらのドキュメントを自動的に仮名化し、IQ Bot を使用することは技術的に可能ではありません。

Control Room でのデータ残存

Control Room をサポートするデータベース内にデータが保存されている場合があります。具体的には、ワークロード管理、IQ Bot および Bot Insight™ (将来リリース) を使用する場合です。Control Room でのデータ残存に関するすべての場合において、仮名化とトークン化は GDPR に準拠するためのコントローラーおよびプロセッサーの労力を削減します。また、デバッギング情報のログを有効にする場合、ユーザー名 (プラットフォームのユーザー) などがログに保持されます。

ワークロード管理とキュー

ワークロード管理 (将来リリース) を利用して複数の Bot を同じオートメーションに導入する場合、キューに配置された作業項目は Control Room のデータベースに保存されます。Control Room のユーザー インターフェースを使用することで、すべての作業項目は照会、確認、および削除できます。作業項目で個人データを処理する場合は、キューを定期的に削除することができます。

ユーザー資格情報は、適切なロールによって設定された適切な権限を持つ任意の管理者によって、追加および削除を行うことができます。Control Room では、あらゆる資格情報の照会、確認、削除を常時行うことができます。

Control Room は、適切な RBAC でユーザー アカウントを設定および削除する手段を提供します。組織の管理者は、ユーザーとリソースへの適切なアクセスを提供する責任があります。管理者は、企業およびユーザー データのプライバシーに関するガイドラインに準拠して、必要なレベルのアクセス権を持つポリシーを作成する必要があります。個々のユーザーが個人情報へのアクセスまたは制限を要求する場合は、個々のユーザーが顧客の管理者に問い合わせる必要があります。顧客の管理者は、Control Room で該当するユーザーのアカウントを削除できます。

GDPR データのプライバシーに関するお問い合わせおよび個人データのコピーに関する詳細は、オートメーション・エニウェアのデータ主体アクセス権要求フォームをご利用ください。

まとめ

今日のクラウドベースのビジネス クリティカルなサービスでは、アクセス セキュリティとデータ プライバシーを根本から最優先事項として備えた製品を提供することが当然と考えられています。

オートメーション・エニウェアのクラウド ポートフォリオは、厳しい運用ガイドラインを満たし、それを超えるように設計されています。その根幹にあるのは、お客様に自動化を提供する際、お客様のプライバシーとセキュリティの保護に真剣に取り組むという考え方です。

オートメーション・エニウェアの画期的なクラウド ソリューションの詳細については、クラウド ページをご覧ください。