AUTOMATION ANYWHERE

RPAのための エンタープライズレベルの セキュリティ

はじめに

ビジネスプロセスのオートメーションテクノロジーに対する投資は 20 年以上も行われてきているにもかかわらず、なぜ、自動化されたタスクは 20% 未満なのでしょう？最たる理由は、企業のシステムの 85% で十分に定義された API が欠如しているためです。その結果、事業部門からの IT 統合のリクエストに対して、バックログが増加しています。

ロボティックプロセスオートメーション (RPA) は、人間のように企業のシステムとやりとりできるソフトウェア Bot をビジネスユーザーが作成できるようにという構想のもと開発されました。RPA Bot は人間のように認証情報を使用してエンタープライズアプリケーションにログインし、API のないレガシーアプリケーションを含めたエンタープライズアプリケーションのタスクを自動化します。請求処理、融資手続き、口座照合、請求書の作成/提出、レポートの生成は、さまざまなビジネス分野で考えられる自動化のうち、ほんの数例に過ぎません。

RPA を使用することで、かなりの時間とコストを節約でき、お客様満足度が向上し、従業員の士気が上がり、競合他社を凌いで圧倒的優位な立場に立てる可能性は大いにあります。しかし、これらを完全に実現するには、エンタープライズレベルのソリューションが必要です。

堅実な信頼性、スケーラビリティ、適用性と使い勝手を最大化する多様な機能は、オートメーションの基準として必要不可欠です。しかし、これらの要素は企業の最も重要な要件である「エンド・ツー・エンドのセキュリティ」を網羅してはいません。関連する極めて重要なアプリと機密データをエンド・ツー・エンドで保護しながら、最小限の特権や責任の分離などの基本的な原則を完全に支援できる機能を備えた、堅牢なセキュリティアーキテクチャーが必要不可欠です。

本書では、市場をリードするデジタルワークフォースプラットフォームである Automation Anywhere Enterprise が実証する、業界最高水準のエンタープライズレベルのセキュリティの概要について説明します。

RPA を使用することで、かなりの時間とコストを節約でき、お客様満足度が向上し、従業員の士気が上がり、競合他社を凌いで圧倒的優位な立場に立てる可能性は大いにあります。しかし、これらを完全に実現するには、エンタープライズレベルのソリューションが必要です。

アーキテクチャーとオペレーション

エンタープライズレベルの RPA の実装に必要なセキュリティコントロールを理解する上で、ソリューションとオペレーションを構成する要素を理解することが求められます。

主要な要素

図 1に示すように、Automation Anywhere Enterprise を構成する中核は Control Room、Bot Creator、Bot Runner です。

Control Room

Control Room はオートメーション環境で頭脳の役割を果たします。これは Windows Server ベースの管理システムであり、システムアドミニストレーション全体を一元的に表示する不可欠なデータベースを備えています。Control Room では RPA のオペレータがデジタルワークフォースを統合管理します。つまり、ここで組織の Bot オペレーションのスケジュール設定、展開、実行、監視、管理を行います。さらに、バージョン管理の機能 (Apache Subversion Server) で、変更管理のベストプラクティスを実施しつつ、本番環境で利用可能な Bot の中央レポジトリを構築し、複数ユーザーによる共同作業を促進します。

Bot Creator

Bot Creator は Bot の作成に使用されます。これは、ワークステーションまたはバーチャルマシンで実行する Windows 版デスクトップアプリです。Bot Creator は、ビジネスプロセスの専門家が自動化作業を作成しテストする際に使用します。Bot は Bot Editor を使用して作成します。一方、テスト (ローカルの非本番テストデータとアプリインスタンスを使用) は Bot Runner で実施されます。テスト (パフォーマンス、データの整合性、セキュリティなど) が無事終了すると、Bot は Control Room レポジトリに送られ、本番環境での展開が可能になります。

Bot Runner

Bot Runner が Bot を実行させます。Bot Creator と同じアプリケーションコードを、異なるライセンスキーと共に使用することで、Bot Runner が本番環境で Bot を実行します。その際、対象のアプリケーションと本番データストアの本番インスタンスを活用します。実際、Bot Runner にできるのは Bot を実行することだけで、機能の作成や編集を行うことはできません。また、非常に信頼性が高く、大規模なオペレーションを行うために、Bot Runner をプールして利用可能にするのにも対応します。

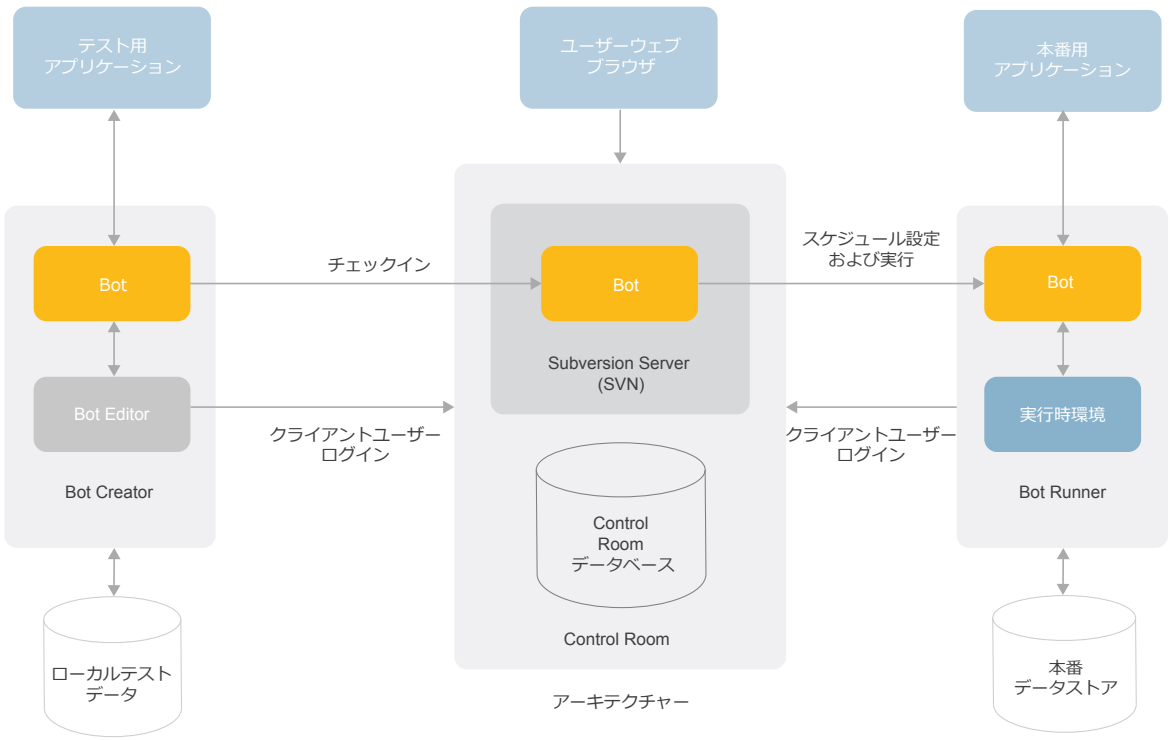

図 1: Automation Anywhere Enterprise アーキテクチャー

その他のエンタープライズレベルの要素

大規模なオペレーションを検討する場合、エンタープライズレベルの展開を進める組織にとって大切になってくる重要な RPA ソリューションが 2 つあります。オンデマンドの拡張性と Bot Insight です。

オンデマンドの拡張性

パブリッククラウドの Amazon Web Services (AWS) を活用することで、Automation Anywhere Enterprise はすべての付帯機能と共に RPA-as-a-service を効率的に提供します。付帯機能には、Bot Runner インフラストラクチャーの柔軟な拡張/縮小、利用量に基づく計測、制限のない水平展開が可能な拡張性、継続的なモニタリング、監査ログの記録などが挙げられます。その結果、たとえオートメーションの作業負荷の振れ幅が大きくても、マルチノードによる高可用性により、SLA 主導のパフォーマンスとビジネスの継続性を実現します。

Bot Insight

Control Room 内で完全に統合されたサブシステムである Bot Insight が、Bot のオペレーションと業務プロセスデータの分析をほぼリアルタイムで実施します。Bot Insight は、各 Bot 特有の高度なアルゴリズムを使用して、カスタマイズ可能なダッシュボードを自動的に作成します。Bot Insight が提供する詳細度は、Bot オペレーションのきめ細かいイベントログに基づいており、微妙な変更、アドホックの発見、双方向性のドリルダウン、経時的な分析、オペレーショナルプロセスや業務プロセスの総合的な洞察を可能にします。また、さらに詳細な分析、調査、レポート作成のためのセキュリティ情報イベント管理 (SIEM) ログとしてすべてのデータをエクスポートできます。

Bot の実行: 2 種類の自動化方法

最後にひとつ、Automation Anywhere Enterprise の高度なセキュリティ機能を展開させる前に明確にしておくべきことがあります。自動化の方法は基本的に 2 種類あるということです。それは、Attended (クライアントで実行を指示する) と Unattended (サーバーから実行を指示する) です。

Attended の自動化の場合、ユーザーは Bot Runner マシンでログインし、Bot の実行を積極的に監視します。ユーザーが対応する理由は、Bot が彼らの業務を支援する実用的な作業を行っている、あるいは、ユーザーによる定期的な入力や状況に応じた指示が必要なバッチタイプの作業を実施しているためです。Attended の自動化は、フロントオフィスオートメーションとも呼ばれます。

Unattended の自動化は、その名のとおり、ビジネスユーザーやオペレータの介入を必要とすることなく操作を実行します。Unattended の自動化は、通常、Bot、自動化されているアプリケーション、自動化の目的について若干の知識があるオペレータが実行します。ビジネス部門と協力して、オペレータは Bot Runner で Bot を実行するスケジュールを設定します。Bot の実行中、オペレータは CPU、メモリ、ストレージの使用量といった実行 Bot の稼働状況を監視し、エラーや例外が発生することなく実行されていることを確認します。Control Room ダッシュボードには、実行中の Bot の稼働状況がすべて詳細に表示されます。エラーにより Unattended の自動化作業が完了しない場合は、オペレータは自動化作業を修正して再開するためのプロシージャの実装が必要な場合があります。または、RPA チームかビジネス部門にエスカレーションして、問題を診断および修正する必要があります。

多層エンタープライズ RPA セキュリティと多要素の本人確認および多要素認証

Automation Anywhere Enterprise セキュリティアーキテクチャーの最も重要な理念は、関連部門の事前認証なしではアクセスもアクションも許可されないというものです。これは、人間にも Bot にも同様に適用されます。そのため、Attended および Unattended 両方の自動化に、多要素認証のプロセスを導入しています。

誰が誰か:一般的なエンタープライズ認証

認証情報とペルソナは多層化することができます。単純なエンタープライズ認証を見てみましょう (**図 2** 参照)。エンタープライズのユーザーであるアリスが Windows ワークステーションの認証を行います。次にアリスは、ワークステーションにある有効なチケットに基づき Windows Domain Active Directory ログインまたは Kerberos 認証を行いながら、リモートで実行中のアプリケーションにログインします。このシナリオでは、一連の認証に一人のユーザーとその認証情報が必要です。

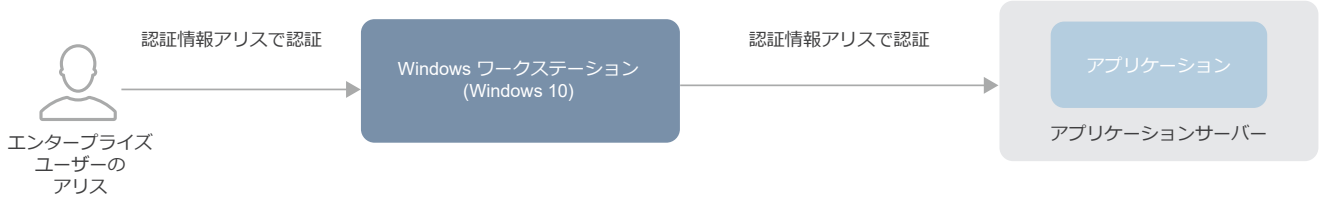

図 2: 一般的なエンタープライズ認証

次に、図 3 に示す、Attended の自動化のシナリオを見てみましょう。この場合、ユーザーであるボブは、自分の日常業務の一環として、Bot のテストまたは Attended の自動化の実行のいずれかを実施します。ステップ 1 で、ボブは彼個人の認証情報を使用して Bot Runner ワークステーションの認証を行います (上記のアリス同様)。ステップ 2 で、ボブは Automation Anywhere Enterprise クライアントを起動させ、自分の Control Room ユーザー ID とパスワードを入力することで、Control Room のクライアントソフトウェアを認証します。ステップ 3 で、今度は、認証が必要なアプリケーションにアクセスする Bot を実行します。このステップで Bot が使用する認証情報は、Enterprise Credential Vault に保存されており実行時に Bot が取得可能であるか、ボブ個人の認証情報のパススルーであるかのいずれかです (ワークステーションとアプリケーションサーバーが同じドメイン内にある)。いずれにせよ、結果的として合計 3 層で識別と認証を行います。

図 4 では、Unattended のシナリオに 3 層認証が使用されています。これに少しひねりを加えます。この場合、ユーザーであるチャールズは Control Room への認証から開始します。それにより、Bot を選択して、即座にまたは指定した時間に実行することができます。

ステップ 2 で、Bot の実行開始時刻になると、Control Room は BotRunnerUser 認証情報を使用して Bot Runner ワークステーションに自動的にログインします。Bot がローカルの Player 機能にダウンロードされ (ステップ 3)、実行を開始すると、BotApplicationUser 認証情報を使用して対象アプリケーションに対する認証を開始します (ステップ 4)。Attended のシナリオ同様、 BotApplicationUser 認証情報は、Credential Vault から取得されたものか、BotRunnerUser 認証情報のパススルーです。

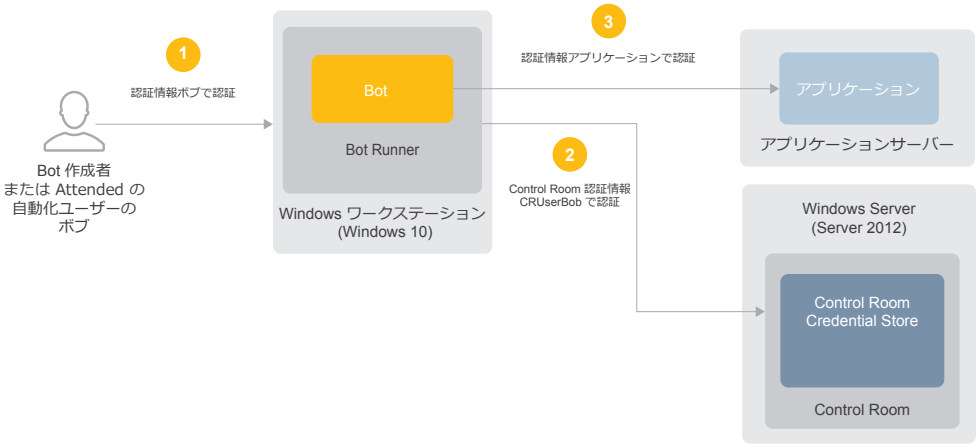

図 3: Attended の自動化の認証プロセスのシナリオ

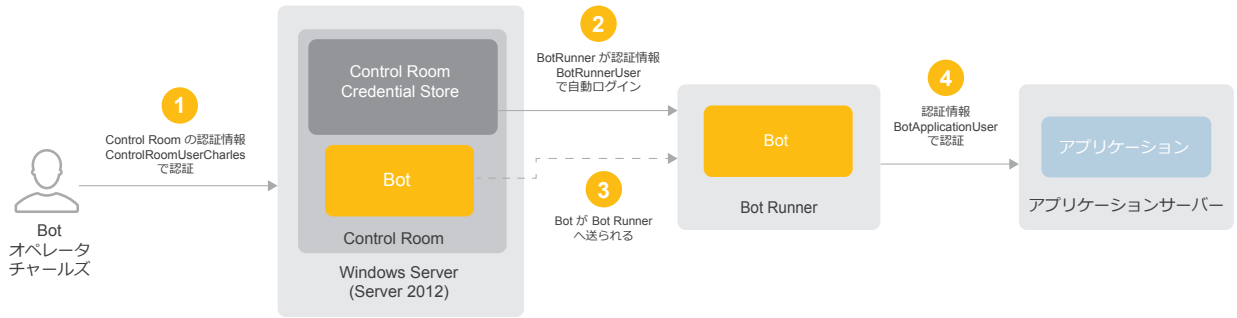

図 4: Unattended の自動化の認証プロセスのシナリオ

認証オプションと IAM の統合

Control Room 認証のオプションとして、LDAP 使用の Active Directory、Kerberos 使用の Active Directory、組み込みの Credential Vault 使用のローカル認証 (後続のセクションで説明) がサポートされています。

エンタープライズの展開で利用可能なその他の ID およびアクセス管理オプションには以下のようなものがあります。

+ SAML 2.0 ベースのシングルサインオンのサポート
+ サードパーティ製の特権/認証情報の管理ソリューション (CyberArk、One Identity、Thycotic など) との統合

総合的なロールベースアクセス制御 (RBAC)

認証の成功は、Automation Anywhere Enterprise のセキュリティアーキテクチャーが提供する必須のアクセス制御実装では初歩レベルにすぎません。特に、最小限の特権と役割分担というコア原則に従うのであれば、同等に重要なのはきめ細かいロールベースアクセス制御 (RBAC) です。

RPA プラットフォームの基本アーキテクチャーと主要機能では、検討すべき役割 (**表 1** 参照) が明確に 5 つに分けられています。BotBuilders は Bot Creator を利用して業務ロジックを捉え、自動化作業を作成します。BotBuilders はテストアプリケーションとデータセットで作業を行います。これにより、開発段階で本番システムが影響を受けることはありません。開発当初だけでなく、関連業務プロセスや対象アプリケーションがアップデートされると、通常、各 Bot に多種多様な反復とバージョンが作成されます。BotTesters はまた、各 Bot が安全な方法で想定どおり動作するか確認しながら、Bot Creator と共に Bot のパフォーマンス、データ整合性、セキュリティをテストします。BotTesters は、Bot を本番データとアプリケーションで実行する前の第二段階の認証の役割を果たします。

Bot がテストされ、セキュリティ検査を通過すると、BotPromoter が BotBuilders や BotTester と連携して、本番システムで使用する Bot のバージョンを指定します。このバージョンが、ビジネス部門と協業して Bot のスケジュールを設定して実行する BotOperator に表示される唯一の Bot のバージョンです。BotOperator にはまた、実行時に発生する問題のトラブルシューティングなど、Control Room での Bot のパフォーマンスを監視する役目もあります。最後に、コンポーネント、インタフェース、すべての役割/許可の設定を含め、プラットフォームの全般的な管理は RPA Admin の責任となります。

高度な役割分担

これらの中核的な役割は RBAC では基本中の基本です。Automation Anywhere Enterprise プラットフォームでは、さらに優れた役割分担が可能です。内蔵の役割作成ウィザードを使用して、管理者は容易に役割をカスタマイズして定義できます。ユーザー管理、ライセンス発行、Credential Vault、数組の Bot Runner、Bot のスケジュール設定、Bot のオペレーション/ダッシュボード、監査ログなど、Control Room のオブジェクトや機能一式を構成する特権や許可を設定できます。権限を選択すると、それぞれに対し、ウィザードが付随または派生する権限に動的にステップを追加します。

たとえば、BOTS (Bot) > View my bots (マイ Bot を表示)> Run My bots privileges (マイ Bot 権限を実行) を選択すると (**図 5** 参照)、アクセスを許可された特定の Bot Folders (数組の Bot) を示すステップがワークフローに追加されます。最終的に、厳重で安全なだけでなく、コンプライアンス規制のある環境ニーズの大部分を満たすには十分である、きめ細かくアクセス制御された非常に忠実な役割を作成することができます。

役割	説明
RPA Admin	システムの管理者 (コンポーネント、役割、インタフェースを設定)
BotBuilder	Task Editor を使用して Bot を作成し、基本的な機能テストを実施する業務プロセスのエキスパート
BotTester	機能的精度、パフォーマンス、セキュリティについて Bot をレビューする品質保証テスター
BotPromoter	Bot を承認し、開発、テスト、本番ステージ間を移動させる管理者
RPAOperator	Bot のスケジュール設定、実行、パフォーマンスを監視するオペレータ

表 1: Automation Anywhere Enterprise における RPA の主な役割

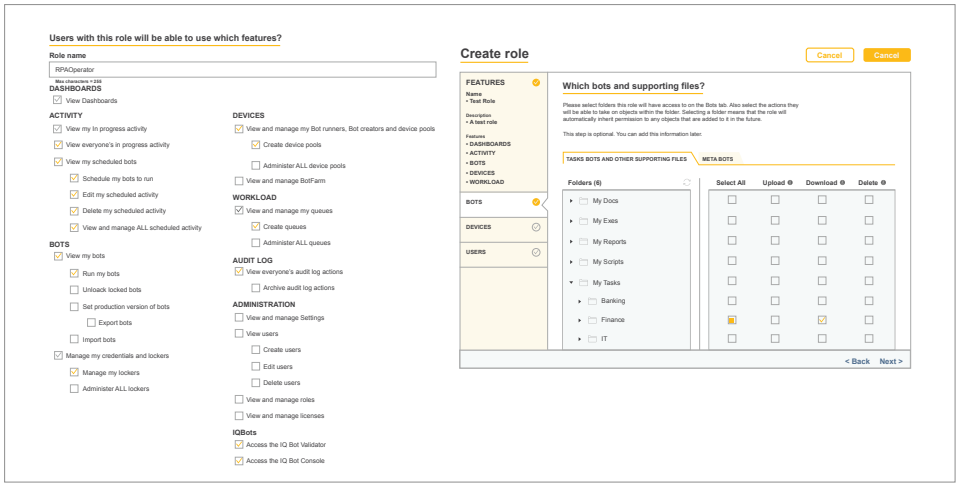

図 5: きめ細かい認証が可能な役割作成

独立した制御レベル

広範な RBAC 機能に加え、Automation Anywhere Enterprise では、Bot の開発と Bot の実行というタスクを完全に分離するアーキテクチャーを採用することで、役割の論理的な分担を本質的に提供しています。

Bot Creator は、Control Room 内のバージョンコントロールシステムへの Bot のアップロードまたはダウンロードしかできません。同様に、Bot Runner は Bot の実行しかできません。Bot の作成やテスト機能へのアクセス権はありません。構造的に役割分担を強制することで、アメリカ国立標準技術研究所 (NIST) のベストプラクティスに一致する二重認証を構成します。このベストプラクティスでは、(最低でも) 開発者とビジネスユーザー双方が最終的には業務プロセスの自動化を実施できることを求めています。

独立したプロセスドメイン

特に大規模なエンタープライズの場合、プラットフォームの RBAC 機能の効果的な使用事例は独立したプロセスドメインの構築です (**図 6** 参照)。これは、Control Room 内の対応フォルダーの最適なドメインごとに Bot を厳密に整理および保存することで実現できます。

代表的な例: 経理アプリケーションに関連する Bot は経理フォルダーに、人事アプリケーションに関連する Bot は人事フォルダーに保存されます。経理部の Bot オペレータには経理用の Bot と Bot Runner に対する特権だけが割り当てられます。一方、人事部の Bot オペレータには人事用の Bot と Bot Runner に対する特権だけが割り当てられます。その他のプロセスドメインやオートメーションドメインも同様です (**図 6** 参照)。

最終的に、さらに役割が分担され、関連するアプリケーションとデータが分離され (ここでは組織ユニットレベル/ドメインレベル)、各オペレータは自分たちのドメイン以外の Bot を見たり操作したりすることができません。

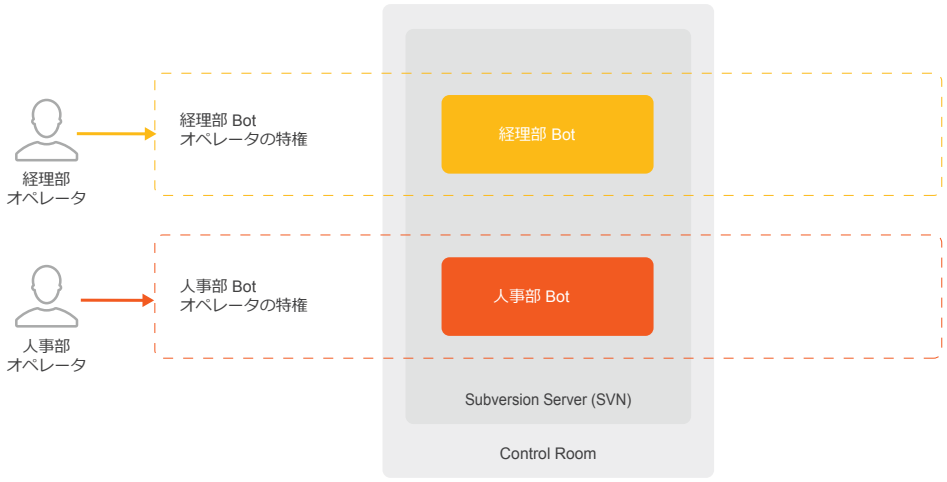

図 6: 独立したプロセスドメインをサポート

エンド・ツー・エンドのデータ保護

きめ細かなアクセス制御と多層認証は、厳しい管理下にある環境では必要不可欠です。同様に、エンド・ツー・エンドのデータ保護も、業務に不可欠なプロセス、機密データ、関連秘密情報 (認証情報など) の機密性と整合性を維持するために必要です。

Automation Anywhere Enterprise プラットフォームに組み込まれた Credential Vault 機能がこの必要性に対応し、 保存されたおよび転送中のデータを保護するだけでなく、各システムで使用中のデータも保護する種々の保護対策を提供しています。

暗号化キーと Credential Vault

図 7 ではプラットフォームで使用される主要な暗号化キーと Credential Vault との関係性を示しています。暗号化はすべて、FIPS140-2 のレベル 1 で検証された暗号化モジュールを用いて行われます。

インストールの際 (**図 7** の左側) 、システムは RSA 2048 ビットのパブリックキー/プライベートキーのペアと AES 256 ビットキーを生成します。RSA 2048 ペアのプライベートキーはマスターキーと呼ばれ、AES 256 キーはデータキーと呼ばれます。マスターキーは、システム外部の安全なロケーションで保護されるようインストール管理者に提示されます。パブリックキーはデータキーの暗号化に使用します。パブリックキーと暗号化されたデータキーは、その後、データベースに保存されます。使用中は、すべてのキーと暗号化されたデータは Microsoft Data Protection API (DPAPI) を使用して暗号化された安全なメモリに保存されます。

Control Room の起動または再起動の際 (**図 7** の右側)、管理者はマスターキーを入力するよう指示されます。暗号化されたデータキーがデータベースから取得され、マスターキーを使用して復号化されます。これでデータキーが使用できる状態になります。システムがデータを保存して Credential Vault から取得する間、データキーがデータの暗号化と復号化に使用されます。

Credential Vault は、システム管理の認証情報と重要なシステム設定データをすべて保存するために使用します。また、組織の自動化作業で使用するそれ以外の機密データ (名称と値の組み合わせなど) を保存するためにも使用します。その結果、BotBuilders が自動化作業の中で認証情報やその他の機密データや引数をハードコーディングしてしまう危険性を回避できます。

保存されたデータの保護

ローカルの認証情報の暗号化と Bot が使用する実行中データの選択に加え、Credential Vault は、不可欠なバージョンコントロールとメールサービスに関連する機密の設定パラメータと詳細を安全に保存します。

転送中データの保護

クライアントのすべてのネットワークサービスと Control Room は、トランスポート・レイヤー・セキュリティ (TLS) 1.2 を使用して、コンポーネント間で転送する際のデータの安全性と整合性を確保します。

Control Room への認証で Bot Creator と Bot Runner が使用する認証情報は、TLS で保護された接続で送信される前に暗号化されます。暗号化にもう一層加えることで、ネットワークのスタック問題 (Heartbleed など) から保護するだけでなく、フロントエンドのロードバランサーで外層の TLS 接続が切断された場合に、実装用の認証情報が危険にさらされるのを防ぎます。

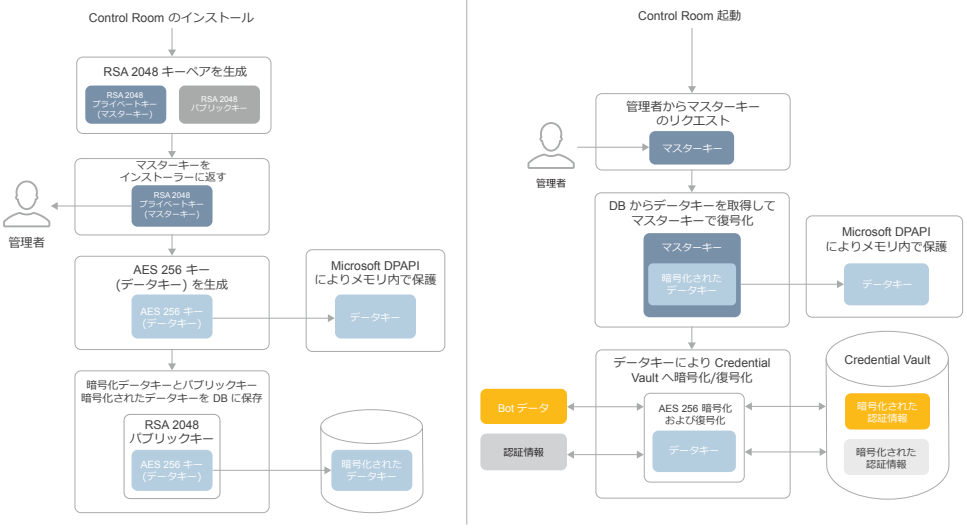

図 7: Automation Anywhere Enterprise の暗号化アーキテクチャー

使用中データの保護

実行時のセキュリティは分散型の認証情報を保護することから始めます。具体的に言うと、Bot Runner にはローカルの認証情報ストレージがありません。自動化作業で使用するために Credential Vault から動的に取得した認証情報と他のデータは、揮発性メモリに暗号化されたフォーマットのみで保持されます。その後、関連 Bot の実行が終了すると一掃されます。

機密情報への不正なアクセス (データ漏えいなど) や実行中の Bot の改ざん防止機能や設定のオプションとして、他には以下のようなものがあります。

+ Stealth mode (ステルスモード) – ローカル画面にプログラムウィンドウが何も表示されておらず、ログイン中のユーザーに Bot Creator や Bot Runner でのイメージキャプチャを無効にするオプションがある場合、画面上に表示されている機密情報が Bot に保存されることを防ぐ
+ Input lock (入力ロック) – 自動化作業を実行している場合、マウスやキーボードの端末側での操作を無効にする機能
+ Time limit (タイムリミット) – 実行が終了しなかった場合、自動化作業を打ち切る時間制限を設定する機能
+ Central control (中央コントロール) – Control Room でリモートで実行している自動化作業の操作を集中的にコントロール (一時停止、再開、停止など) する機能

ソフトウェア開発ライフサイクル (SDLC) の安全なサポート

自動化環境に置かれた制御と保護機能を最大化するため、前述の基本的な展開シナリオを「拡張」して、FISMA、FedRamp、PCI DSS などが求めるソフトウェア開発ライフサイクル (SDLC) のベストプラクティスにより近付けることが可能です。それに基づく結果としての高度な展開モデルでは、 開発、ユーザー受け入れテスト (UAT)、本番 (**図** 8 参照) の 3 つの明確な RPA ゾーンを提供します。ゾーンはそれぞれ、重要な役割と特権を付与された異なるユーザーグループで論理的に分割 (分離) されています。縦の点線はネットワークセグメントとファイアウォールを表しています。

基本的な展開モデルのように、 Bot のライフサイクルは開発から始まります。BotBuilders が開発した Bot に満足すると、UAT BotPromoters が Bot を開発バージョニングレポジトリ (SVN) から UAT レポジトリへ移します。UAT ゾーンの唯一の目的は、 Bot の精度、パフォーマンス、セキュリティをテストすることです。Bot が受け入れテストを通過すると、本番 BotPromoter が Bot を本番ゾーンに移します。この時点で、Bot は本番ステータスに達し、RPAOperators が本番アプリケーションで使用することが可能になります。プロセスのステップごとに、さまざまな役割と特権を持った異なる管理者によってチェックと認証が実施されます。厳格な役割分担と多層制御が設計段階で組み込まれているため、デジタルワークフォースの信頼性、スケーラビリティ、効率、安全性、コンプライアンスが確保されます。

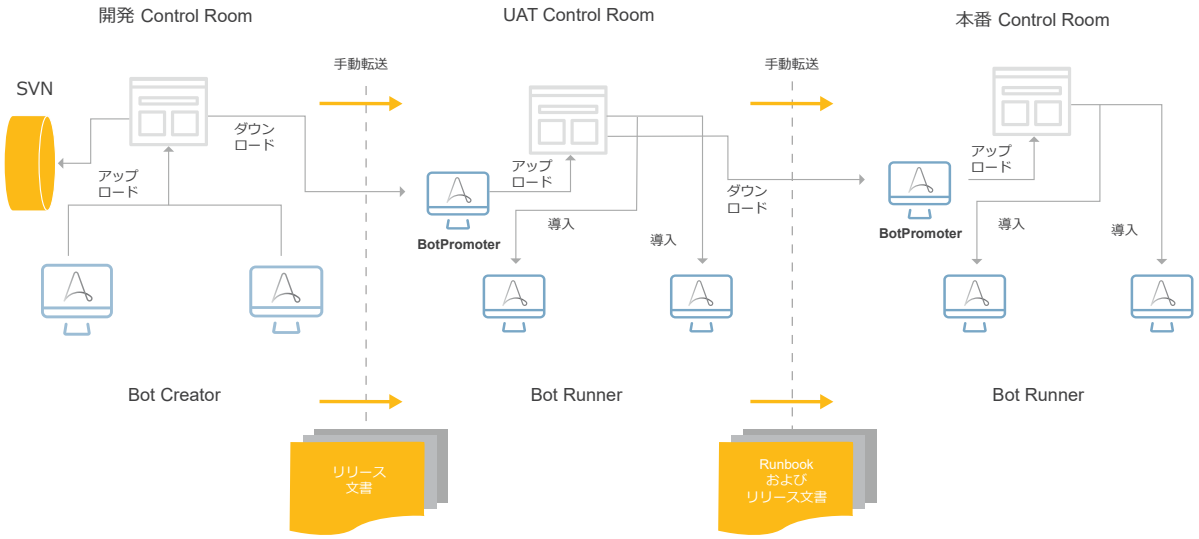

図 8: 完全な SDLC サポートの高度な展開モデル

ログの記録とモニタリング

包括的な監査ログの記録、モニタリング、レポートの生成機能は、主要な IT ソリューションのセキュリティアーキテクチャーにおいては必須の要素です。Automation Anywhere Enterprise も例外ではありません。

プラットフォーム全体で、ユーザー、 Bot、Bot Creator、Bot Runner の作成、変更、有効化、無効化、削除など、60 種以上のユーザー/エンティティのアクションについて、イベントの詳細 (誰が、何を、いつ、どこで、結果) を自動的にキャプチャします。自動キャプチャ、特定 ID に対する各アクティビティの結び付け、デフォルトの読み取り専用ポリシーの組み合わせにより、否認防止を実現します。また、RBAC を採用して、最初の段階で監査ログを閲覧できる役割はどれか厳格にコントロールすることができます。

モニタリングの観点からは、自動化ダッシュボードとレポートは Control Room 内でアクセスが可能なうえ、カスタマイズして異常なアクティビティ (または他の自動化やセキュリティ担当部門が関心を持った詳細) を特定して警告することができます。さらに、ログのエクスポート機能は、組織が既に使用している他の分析、レポート、インシデント調査/対応用のインフラストラクチャー (SIEM、UEBA、高度な分析ツール等) の使用をサポートしています。

その他のエンタープライズセキュリティと回復機能

Automation Anywhere Enterprise ではさらに、以下の要素によりエンタープライズセキュリティと回復機能をサポートしています。

+ 組織が使用している既存の高可用性とディザスターリカバリー (HA/DR) インフラストラクチャーとプロセスにシームレスに"適合する"分散型 (かつ柔軟な) コンポーネント型アーキテクチャー
+ プラットフォームの広範な RBAC 機能と併せて、極めて厳格な変更管理ポリシーとプロセスを実施および強化することができる、全体的なバージョンコントロールシステム (Apache Subversion)
+ プラットフォームコードの開発中に一般的な攻撃 (SQL Injection や Cross Site Scripting など) に対する脆弱性を取り除く Hibernate や ReactJS フレームワークなどのツール
+ ソフトウェアの脆弱性を検出して取り除くための継続的な複数のツールと多層のスキャニングが必要とされる、コード開発のためのセキュリティのプランやプロトコル

上記の詳細や Automation Anywhere Enterprise のその他の数々のコントロール、保護、セキュリティ機能については、こちらからご確認いただけます。Automation Anywhere Enterprise: https://www.automationanywhere.com/images/Enterprise-Architecture-ja.pdf

ロボティックプロセスオートメーションは、運用コストの削減、お客様満足度の向上、競争での優位性を求める現代の企業にとって非常に有望です。市場をリードするインテリジェントデジタルワークフォースプラットフォームとして、Automation Anywhere Enterprise は、成功に必要な信頼性、スケーラビリティ、使い勝手といった機能だけでなく、自動化環境全体の機密性、完全性、可用性の維持に求められるエンタープライズレベルのセキュリティを提供することで、上記以外にも多くの利点を最大限に享受できるよう支援します。

Automation Anywhere Enterprise の詳細については、こちらからご確認ください。
https://www.automationanywhere.com/jp/products/enterprise