RPA が必要とする
ログ管理とは？

Robotic Process Automation 2.0

RPA とログ

RPA を構築すれば、ソフトウェアロボットが業務を代行してくれます。
そのロボットが正しく業務を行ったという証明はできますか？
もし、残念にもロボットが停止してしまった場合、どうやって原因を調べますか？
もっとたくさんの業務をロボットにやらせたい場合、どのロボットにやらせたらよいかわかりますか？

こうしたことを判断するためには、ロボットに関する様々な情報を記録しておくことが必要です。つまり、いろいろな目的を達成するための判断材料として、多くのログが必要だということです。
ロボットに関係するログがなければ、処理結果の合否も、障害の原因追及も、ロボットの容態さえもわかりません。

- 業務の品質確認
- ロボットのヘルスチェック
- セキュリティ対策
- 障害時の原因分析
- 障害対応策の判断材料
- キャパシティプランニング
- ライフサイクル管理　　…etc

ロボットを本番業務で使用するためには、セキュリティリスク回避のためだけでなく、人を採用するのと同じく、様々な管理をするための元データとして、多くの種類のログが必要です。

ログの多様化

取得すべきログは、これだけあれば十分だと限定できるものではありません。
昔の車には、ドライブレコーダーはついていませんが、今では珍しくありません。
以前はなかったのに、今では街のいたるところに監視カメラが設置されています。
環境のみならず、その時代の要請と、技術の進歩によって、必要とされるログの種類も、目的も、使用法も変化します。

RPA のロボットの適用業務については、今後ますます複雑化します。
バックオフィス業務のみならず、様々な業種、様々な分野でロボットが活躍し、そして進化しているため、ログの取り扱いも多様化せざるを得ません。
単純な動きしかしないロボットであれば、チェックすべきポイントも少なくてすみますが、稼働する範囲が広がり、処理する内容が複雑になればなるほど、取得すべきログも増えていきます。
ログの取得については、ログ量の増加に伴ってリソースへの影響が懸念されますが、それについては技術の進歩によって、ストレージとネットワークが、大容量化および高速化されていくおかげで対応が可能になります。

そして当然、そのログを分析する CPU パワーもますます必要になりますが、こちらもビッグデータを扱う GPU や TPU などの高速化によって、ログ解析にディープラーニングなどの AI を利用することにより、効率化できるようになります。

つまり、今後ロボットが活躍すればするほど、ログの需要は高まり、ロボットの進化と共に、ログの多様性も高まります。
但し、ログの種類や量が増えても、人間が作業できる時間には限りがあるため、このログを管理するのもロボットに頼って自動化することになるでしょう。

このように、ログ管理も進化するため、日々の変化に対応できるように、ログ管理システムは、柔軟性、拡張性に優れていることが最重要ポイントです。

取得すべきログ

ログを取得する目的を明確にすることで、取得すべきログが決まります。ログ管理をするためにログを取得しているわけではないので、管理が目的になっていては、必要となるログが取得できていないという場合もあり、見直しが必要です。
たとえば、RPA ツールの導入で、ロボットの実行ログが自動的に取得されているので、それで管理ができていると安心してしまうケースなどが、これに当たります。

ログ管理をする上で、まず初めにすべきことは、RPA で使用するロボットが正常稼働し続けるために必要な情報は何か、を洗い出すことです。
たとえば、以下のようなものです。

(1) 業務が正常終了したという証明
- 処理エラーはないという情報
- インプットは必要なデータを全件読み込んでいるという情報
- アウトプットは期待したものが生成されているという情報

(2) ロボットが正常に働いたという証明
- 予定通りの業務をしたという情報
- 予定時間に実行できたという情報
- 処理ステップごとにエラーはなかったという情報

(3) 障害発生時の対応
- 障害やエラー時のロボットの状態の詳細情報
- 処理に使用したリソース側のアクセス情報
- 障害時の稼働環境の情報

(4) リスク回避
- セキュリティ対策ツールからの情報
- 使用するリソースの稼働状態の情報
- 予兆検知のための累積データや知識ベースの情報

(5) ロボットのライフサイクル
- キャパシティプランニングのための情報
- ロボットのバージョン適用履歴の情報

ログの出力分類

ソフトウェアロボットをどんな業務に使用するかで、ログの取得方法も千差万別ですが、ロボット管理で必要な出力されるログは大きくは５つの分類されます。

① ロボット自身が任意に出力
- 作業ステップごとのログ
- エラー時のコンディションログ

② 稼働 PC のシステムが出力
- Windows のイベントログやセキュリティログなど

③ RPA ツールが出力
- RPA ツールが持っているロボット管理のためのログ

④ リソース側のシステムやアプリが出力
- DB や、ファイルサーバなどのアクセスログ
- アプリケーションが出力しているログ

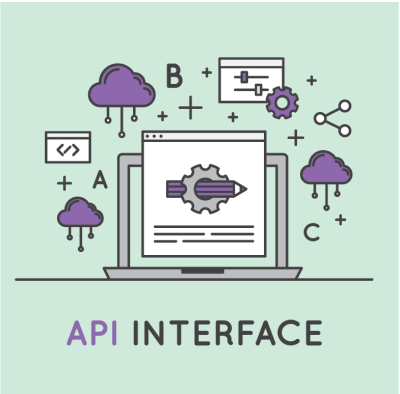
⑤ セキュリティ対策ツールや、運用ツールが出力
- マルウェア対策や、ネットワーク監視などのログ
- ジョブスケジューラなどの運用管理ログ

既存のシステムでも、出力はされていても活用されていないログはたくさんあります。よって、まずは必要最小限から始めて、徐々に管理対象を模索しながら拡大してくという考えもあります。
しかしながら、管理するシステムの構築は後回しにしたとしても、どんなログが必要なのかを最初に洗い出し、情報として必要なログは、正しく出力されて、保存されているかを、RPA 導入当初から確認すべきです。
特に、ロボットに組み込んで出力すべきログは、ロボット開発時に組み込まないと、障害対応などができないため、コーディングに入る前に具体的に洗い出しておかなければなりません。そうでなければ、障害などの異常事態にどう対処したらよいのか判断する情報がなく、危険なのでロボットを動かすことができません。

① ロボット開発時に組み込むログ

何かの原因でロボット停止などの障害等が発生した場合は、ロボットが行った作業についてリカバリーが必要となりますが、そのまま、ロボットを再起動すればよいケースばかりだとは限りません。リカバリーをするには、同じ処理を再実行しても大丈夫という判断が下せる情報が必要であり、そのためにもロボットが行った作業の節目ごとに、その状況を記録しておくことが必須となります。
ロボットが実行したコマンドレベルの内容であれば、RPA ツール側でその詳細を確認できる場合がありますが、業務によっては、中間ワークのデータをどこまで書き込んだかとか、例外データを読み込んでいた場合、どのような処理をしたのかなどを記録しておかないと、正しい再実行方法の判断ができず困ってしまいます。

ロボットの業務作業に関わるログは、ステップ毎に適宜必要な情報を記録できるよう事前にプログラミングしておくことが大切です。そのため、ロボット開発をする時点で、エラーハンドリングなどの処理を入れることと同様に、適切なログを残す処理を組み込むことが必要です。
手順としては、ロボットに実行させる業務のステップごとにリカバリーポイントを設け、処理結果の情報をアプリケーションログとして出力していきます。それ以外にも、エラーハンドリングのルーチンに追加して、エラーとみなされる状況に陥った場合に、リカバリーに役立ちそうな情報すべてをログとして出力していくとよいでしょう。当初から、リカバリーポイントを設けてログを残すことは、ロボットの動きをテスト検証する際にも、とても役立ちます。



想定できる例外データでテストができれば、その時ロボットが行った対処を記録しておくことにより、リスク軽減の確認もでき、結果的には業務品質の向上にも貢献します。
ログを生成するためのコーディングには、そのログのレコード毎にタイムスタンプを入れておくことも効果的です。そうすれば、他のログとの関連を調べる時に、発生時刻で検索でき、とても役立ちます。

②システムのログ

Windows などのシステムが出力しているイベントログ等は、この情報を上手く管理することで、ロボットが決められた時間、決められた環境以外で、不正に使用されていないかなどをチェックできます。
RPA ツール側でも、通常はロボットの操作ログ等を出力しているため、その確認は可能ですが、万が一ロボットが乗っ取られて不正使用されている場合などは、犯罪者が痕跡を残さないようにするのは当たり前なので、そのロボットのログも削除や改ざんがされている可能性があり、当てにできません。

一方、ロボットが稼働する PC などのシステムのログは、ロボットの動きを第三者的に監視するためにもとても有効です。但し、業務担当者は、普段システムのイベントログ等にはなじみはないし、そのログは独特なレコードフォーマットであるため見てもよくわからないでしょう。
こうした状況を解決するために、RPA のロボットも、情報システムの監視対象に加えてもらうことが必要です。そうした体制が不十分であれば、システムのログを理解し易いようにフォーマット変換して、エラーが発見されれば自動的に通知してくれるようなログ管理ツールを導入することも効率的です。

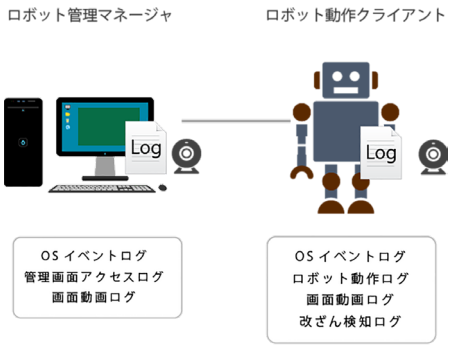
システムのログは、OS 側が把握しているロボットの詳細な動きなので、障害時の原因分析にも、多くの有益な情報となります。
ロボット内部では問題のない動きであっても、OS 側で記録した各プロセスの処理時間やアクセスログにより、その時、ネットワークの障害があったとか、他に負荷のかかるプロセスが動いていて遅くなっていたなど、外的要因により不具合が発生していた場合の重要な手がかりになります。
システムのログがロボットにとっても必要となる理由は、RPA ツールが出す情報だけでは、ネットワーク障害など外的要因によるトラブルは原因追及できないということも大きいです。

環境依存によるトラブルは、コンピュータにとっては避けられません。ロボットの内側と外側からの情報を連携してはじめて、ロボットの動きが正確に把握できるようになります。

③ RPA ツールのログ

RPA ツールには、ロボット側で取得できる様々なログを出力する機能が標準で搭載されています。高価なツールでは、そのログによってロボットの実行管理やセキュリティ管理、監査などを可能にしています。
もちろん、こうした RPA ツールが搭載しているログ管理機能は、とても役に立ち日々のロボット運用の助けになります。しかしながら、パッケージソフト同様、標準的なガバナンスや、セキュリティポリシーを元に管理システムが作成されているため、導入する企業が、その企業のガバナンス基準に準拠しているかどうかは、確認が必要です。
たとえば、ロボットの実行権限やアクセス権の承認方法が、その企業のポリシーに合っていなかったり、そのログの原本管理方法の違いで、ログ保存先をセキュアな改ざんできない場所に指定していないような場合など、注意が必要です。

いずれにせよ、RPA ツールのログ管理方法を把握して、うまく運用に組み込むことが大切ですが、多くの RPA ツールが持つログ管理のツールは、独自サーバにログインして取り扱う必要があるため、その管理者は、その管理ツールの使用方法を覚える必要があります。RPA ツールのログ管理は、ロボット管理の一環で行われるものですから、ロボットの実行権限を持つかなり高いレベルの権限が要求され、その管理者の責任も重大となります。
意外とこのロボット管理用 ID が、セキュリティ管理上のウィークポイントとなります。提供元の RPA ベンダーに知られないよう、導入時のパスワードは運用開始前に変更することをお勧めします。間違っても、ベンダー担当者しか、ログ管理方法がわからないということがないように、管理者の方はベンダーよりスキルトランスファーを受けて、責任を持って管理することが必要です。



そうした RPA ツールの管理だけではリスクを感じられる場合は、ロボット起動もその企業標準のスケジューラに登録して、その企業の統一したログ管理システムにロボットのログも取り入れてしまう方法もあります。但し、この場合は、ログのフォーマット変換や、ログの原本をコピーして消されない仕組みを作ることが必要になるかもしれません。

④ リソース側のログ

ロボットで行った業務の品質を確保するためには、その業務で使用するデータのリソース側の情報が必要です。
具体的には、どのデータベースからインプットしたデータなのか、あるいはどのファイルサーバにいつ、どの ID で書き込んだかなど、監査の面でも、リソース側で取得した情報のログが必要です。
こうした情報なしでは、ロボット側で正常終了したと通知されている業務についても、本当に期待していたアウトプットが作成されたのかどうかが確証できません。

リソース側で、ロボットが使用したレコードのアクセス履歴等を把握することで、トラブル時の原因分析に有効な情報を得ることもできます。また、特にリカバリーのために再実行をする場合、どのポイントまで戻ってやり直しを行うのかを決定するためには、このリソース側の情報は欠かせません。
どのデータをどれだけの量作成できているのかは、こちらのリソース側の情報がなければ、ロボット側で出力したと判断している件数のデータも、実際にデータベース等に書き込まれたレコード数が同じでなければ、最終的に正常に生成できているとは判断できません。アウトプットされた業務データは、データベースなどのリソース側に保存されていなければ、そのデータを利用することができないからです。
インプットするデータについても同じことが言えます。ロボットは、指定されたことしか実行しないので、データベース側でリードエラーがあったとしても、そのまま処理を続行してしまうかもしれません。

リソース側のログには、使用する業務各種のアプリケーションのログもあります。これが、業務の正常終了を確認できる有効な情報です。
アプリケーションのログからは、適切な権限で、そのアプリケーションがアクセスされ、業務レベルで期待通りの処理が行われたかどうかの情報が得られます。

これらのログには、独自に作成された業務アプリの他に、ERP や CRM、市販のパッケージソフト、クラウド上のアプリなどもあります。業務として使用するシステムが出力しているログは、全てが有益な情報となります。

⑤ セキュリティツールのログ

ロボットには、社内での不正利用はもちろん、外部からの悪意を持った第三者のロボットの乗っ取りなど、数多くのセキュリティリスクがあります。
よって、セキュリティ対策のために RPA のロボットも対象システムに組み入れ、監視が必要です。こうしたセキュリティツールが出力する情報は、ロボットが業務に与える影響を最小限にするためにも有益であるため、活用すべきです。

たとえば、マルウェアに感染した情報を見逃して、ロボットをそのまま動かし続けたらどうなるでしょう。バックドアを設置され重要なデータが漏洩してしまうリスクや、システムがロボットによって破壊されてしまうリスクを、このセキュリティ対策ツールからの情報で、未然に防ぐことが可能となるかもしれません。

ロボットがいろんな仕事を行うためには、ロボットにも様々な業務のリソースにアクセスできるよう特別な権限を与えることになります。そのため、システム管理者の特権 ID 管理と同様に、定められた手続きに従って承認された権限を持った人だけが、ロボットを実行でき、そのロボットを動かす指示さえも、いつどのように行われたかの履歴を残し、不正が行われていないかどうか、必要であればそのオペレーションを動画で残すぐらい徹底できると安心です。
また、SIEM（Security Information and Event Management ）が、構築されている企業では、ロボットの管理も組み込むことで、ロボットに影響しそうな兆候を入手でき、迅速にロボットを停止させるなどして、未然にインシデントの発生を食い止めることができるかもしれません。

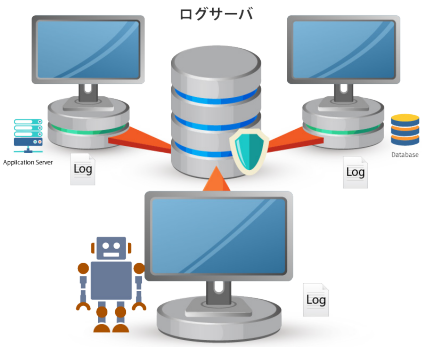
ログの収集と保存

システムや、アプリケーションなどから出力されたログは、必要に応じて収集され、保存されます。重要度にもよりますが、ログは通常一定期間を過ぎると上書きされてしまうため、改ざんできないディスク装置などで、決められた期間保存されているのが理想です。
昔であれば、大量なログもコスト面から磁気テープなどにアーカイブして保存していましたが、現在はハードディスクも大容量となり安くなったため、できればオンラインでアクセスできるディスクにて保存してある方が、いざというときの分析には高速処理ができて便利です。

とはいえ、無作為にあらゆるログをすべて集めていたのでは、分析にも時間がかかり、処理にかかる負荷やリソースを維持するためのコストも増え続けてしまいます。
そのため、一定期間が過ぎたログは、圧縮したり、必要な部分だけを抜き出して、コンパクトにしてセキュアに保存した方が、管理も活用もし易くなります。

こうした、レコードのフィルタリング処理などは、プログラムを作成すればある程度自動化できますが、ログ管理のツールを使用した方が、安心で効率的な場合も多くなります。その際、フォーマット変換やレコードの抜き出し等に ETL ツールなどを使用するのも効率的です。また、貯まる一方のログを、どのタイミングで上書きするのかを自動的に判断して実行するような仕組みや、自動アーカイブの仕組みも作らないと、運用負荷も増え、リソースの無駄遣いにもなりかねません。

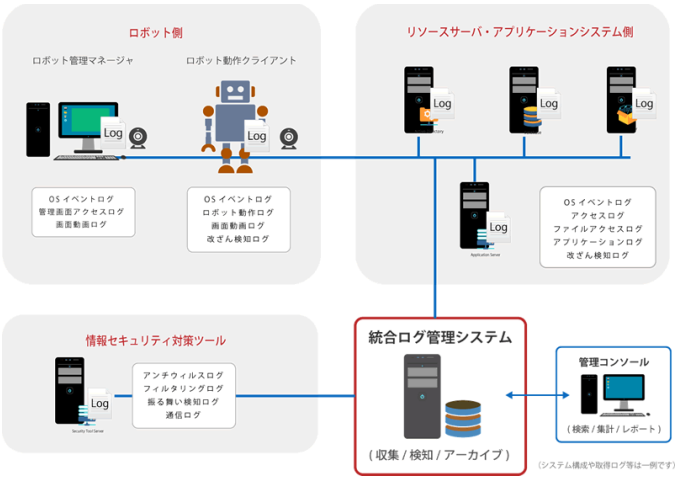
ログにもライフサイクルがあり、法律で規定されている年数などによって、適切に削除もしていかないと、個人情報などの秘密情報を不当に保持してしまうリスクも出ます。そうした仕組みも、ツールを使うか、ロボットにやらせる方が楽でしょう。



ログの統合管理

たとえば、ロボットが突然停止し業務自体が続行できなくなってしまった場合、それを復旧させるために、ロボットが停止した原因を調べなければいけません。
ロボットのバグであれば、まずロボットの実行ログを調べ、どこまで正常に動いていたかを見つけて、その部分のロボットのプログラムソースをチェックするでしょう。
コーディングしたロジックに問題がなければ、インプットに使用したデータが間違っていないかを、データベースなどのリソース側のログを調べます。想定外の例外データが来た時に、ロボットは何も対処できず止まってしまうことがあるからです。
データに問題がなさそうでであれば、アプリケーション側のログを調べます。パスワード期限切れでアクセスできなかったり、画面レイアウト変更によりクリックできなかったなど、些細なことでもロボットは停止することがあります。
こちらも問題なさそうであれば、その時点でネットワーク障害はなかったかとか、CPU パワーは不足していなかったかなど、システム側の動きも確認します。
それも関係ない場合、マルウェアなどの感染を疑ったり、リモート操作の可能性など、セキュリティ対策ツールのログや、監視ツールのログも調べることになります。

こうした一連の調査を効率よく行うためには、関係するログを一ヵ所に集め、タイムスタンプ等をキーにして、横串検索によって複数のログを横断して分析し易くする統合ログ管理システムの構築が望まれます。



ログの活用

ログ管理というと、セキュリティ強化のためのイメージが強いですが、多種多様なログはそれ以外にも有益であるため、最大限利用すべきです。
多くのログは、いざというときの障害対応などの情報として活躍しますが、ログを有効利用できれば、障害を起こさないための予兆検知や、ロボットのヘルスチェック、さらには、将来のロボット増強の参考になるキャパシティプランニングなどにも活用できます。

従来、ログは万が一必要になるかもしれないからと溜めておいて、保管期間を守ることだけで管理しているつもりになっている企業が、多数あるようです。
ログの活用なんて、それより優先したい仕事がたくさんあるので、おろそかになってしまっている面も少なからずあるでしょう。

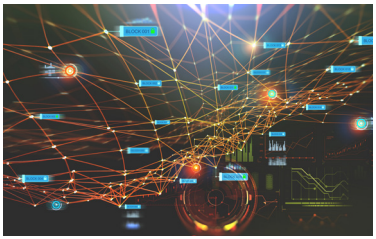
しかし、このログを上手く活用できれば、業務の成果物の品質も向上し、生産性も上がり、ひいては、季節変動の予測や、生産計画、投資計画なども効率的に行えるようになります。
重要なログを知識ベースに蓄積することにより、既知の障害は未然に防ぐ対策をとることもでき、エラー率、障害率の削減も可能になります。

適切なログ管理の実施が、同業他社よりも高い生産性と安全性をもたらし、そしてさらに業務効率が高まることが理解できれば、ログ管理が無駄な時間や費用の投資であると思わないでしょう。
ログを活用できる企業こそが、安心安全で快適なロボット社会をいち早く実現できます。

ログ管理の未来

ログを取得する目的の一つにロボット管理があります。
ロボットが進化して、企業に浸透すればするほど、管理は複雑になり難しくなるでしょう。そんな中で正確性、安全性を求めるのは、至難の業です。
しかしながら、技術の進歩は、人々の暮らしを楽にしてきました。
ログ管理も、将来はきっと人手に頼らず、ロボットにより自動化されて、知識ベースも自動的に蓄えられ、ログ量が爆発的に増えていくにも拘わらず、それらを元にディープラーニング等の技術で次々と最適化されるはずです。

ログを管理するには、従来通り一元管理をする方が簡単です。しかし、それでは、今はよくても、今後は管理者に権力が集中し、責任とリスクも増大し、監視体制もシビアになっていくでしょう。
一方で、ブロックチェーンの技術を元にした非中央集権型で分散管理ができる手法もいろいろな分野で採用され始めました。ブロックチェーンのような技術は、暗号化され改ざんできず、利便性のよい強固なシステムなので、情報セキュリティの３要素の機密性、完全性、可用性の実現に、きっと貢献していくことでしょう。
ロボットの適用範囲が増えれば増えるほど、ロボット管理も複雑さが増すので、管理者の負荷も、責任も大きくなってしまうのですが、ログの改ざん防止を担保できるブロックチェーンであれば、一度仕組みを作れば拡張性もあり安心でしょう。
将来は、プルーフ・オブ・ワーク (POW) などの手法によって、ロボットを使用した分だけ、トークンを支払う仕組みも同時に確立できることが想定されるので、クラウドサービスなどを利用して、あらゆる場所で、様々な分野でロボットを適用でき、使用した分だけ自動的に適切に支払われる環境が作られていくでしょう。
世界中のロボットを、暗号資産のトークンのスマートコントラクトを使用できるようになれば、ロボットの使用の支払いに仲介業者を介入させる必要なくなり、それでいてトレーサビリティも確保できるので、世の中はかなり様変わりすることが予想されます。



まさしくロボットによる働き方改革だといえますが、その際には、ブロックチェーンによって改ざんされないよう保護されるログが、ますます重要な役割を果たします。

今必要なログ管理

RPA でロボットを安心安全に運用していくためには、ログ管理が必須です。
ログ管理は、どこまで行うべきか、それは時代とともに移り変わります。
よって、今現在のログ管理に重要なことは、柔軟性があること、拡張性があることです。今後増えるであろうロボットに対して、適切な管理が継続して行われる仕組みが求められています。
この前提に、セキュリティの機密性、完全性、可用性は保証されるべきです。
企業のポリシーの準拠したセキュリティ対策のガイドラインに沿って、収集、分析、アーカイブなど統一されたログ管理が出来ることが安心につながります。

導入効果ばかりに目が行き、とりあえずロボットを動かすことを優先してしまった企業が今やるべきことは、ログ管理を中心としたロボットの運用管理に力をいれることです。
この部分をおろそかに考えると、必ず RPA は失敗します。後悔しないロボット導入を進めるのであれば、ロボット管理のための一貫した統一的なログ管理は、最重要課題です。

ロボットは、人の採用と同様、会社の発展を目指し、共に歩んでいく仲間です。
PoC による一時的な効果ばかりでなく、運用管理に目を向け、ログを有効活用することにより、将来に夢のあるロボット社会を迎えましょう。

（編集：春日井）

CCS 株式会社シーイーシーカスタマサービス
■お問合せ　ESECinfo@cec-ltd.co.jp
〒150-0022 東京都渋谷区恵比寿南 1-5-5 JR 恵比寿ビル 8F
TEL：03（5789）2443 FAX：03（5789）2575

（2019年5月10日公開の情報です）