



AWS クラウドにおける顧客ライフサイクル管理のためのバンキングモダライゼーション戦略

AWS 規範ガイドンス



AWS 規範ガイド: AWS クラウドにおける顧客ライフサイクル管理のためのバンキングモダナイゼーション戦略

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

序章	1
モダナイゼーションの課題	2
変化する期待とネオバンク	2
業務の問題	2
顧客ライフサイクルの管理	3
顧客オンボーディング	4
オンボーディングジャーニー	5
サーバーレスオンボーディング	6
オンボーディングソリューション	6
セキュリティとコンプライアンス	8
よくある質問	10
AWS サービスが個人データを保存しないようにするにはどうすればよいですか?	10
アーキテクチャは GDPR に準拠していますか?	10
適切なデータの機密性を確保するにはどうすればよいですか?	10
AWS バンキングモダナイゼーションソリューションをレガシーバンキングシステムと統合で きますか?	10
オンボーディングダイアログはカスタマイズできますか?	10
次の手順	11
リソース	12
ドキュメント履歴	13
.....	xiv

AWS クラウドでのクライアントライフサイクル管理のための バンキングモダナイゼーション戦略

Patrick Rotzetter、Florent Batard (Amazon Web Services (AWS))

2022 年 6 月 ([ドキュメント履歴](#))

金融サービス (FS) 業界は大きな混乱に直面しています。金融テクノロジー企業 (フィンテック) やネオバンク (物理的な支店をもたないデジタル専用銀行) が小売顧客のオンボーディングプロセスの一環として提供している、完全デジタルセルフバンキングサービスを期待し、選択する顧客がますます増加しています。従来型金融機関は、フィンテックやネオバンクに追いつくことができません。これは、ほとんどの従来型金融機関のバンキングプロセスが、依然として手動または半自動で行われているためです。

従来型のバンキングプロセスはすべての金融機関に共通していますが、これらのプロセスを実装するための標準フレームワークはありません。このような標準フレームワークの欠如が、イノベーションを妨げています。例えば、従来型金融機関は、バンキングの最新トレンドの 1 つであるエンベデッドファイナンスを活用することができません。つまり、ノンバンクが提供する銀行のようなサービスを活用することができないのです。詳細については、McKinsey & Company の「[What the embedded-finance and banking-as-a-service trends mean for financial services](#)」を参照してください。従来型金融機関がエンベデッドファイナンスを活用するには、自社の事業能力を他の事業にシームレスに公開する必要があります。

この戦略は、AWS クラウドサービス上に構築された API 指向のサーバーレスアーキテクチャを使用して、スケーラブルで安全な標準バンキングプロセスを実装するためのモダナイゼーションアプローチを定義します。このアプローチの課題と機会を説明するために、この戦略では、顧客ライフサイクル管理 (CLM) のケーススタディに焦点を当てていきます。この戦略の対象者には、リテールバンキングおよびウェルスマネジメント業界のCEO、CFO、CIO、上級管理者が含まれます。

バンキングモダナイゼーションの課題

変化する顧客の期待とネオバンクの台頭

金融業界は大きな変化に直面しています。顧客は、完全なデジタルジャーニーだけでなく、パーソナライズされたエクスペリエンスも期待しています。こうした顧客の期待に応え、ネオバンクと競争するために、従来型の金融機関はスピード、アジリティ、イノベーションを必要とする大規模な変革を遂げる必要があります。この変革に際して、従来型の金融機関は短期的に次のような課題を克服する必要があります。

1. 従来型の銀行は、技術的負債やプロセスの負債がなく、本質的により俊敏性の高いネオバンクと歩調を合わせる必要があります。
2. 従来型の金融機関は、バンキングアズアサービス (BaaS) を通じて組み込みバンキングサービスを開発し、提供する必要があります。
3. 従来型の金融機関は、機械学習モデルを迅速かつ費用対効果の高い方法で統合する、カスタマイズ可能で柔軟な顧客エクスペリエンスを開発し、実現する必要があります。

今後数年間に検討すべき重要な戦略的要因は、組み込みのクラウドサービスを活用することと、サービスプロバイダーとのコラボレーションや俊敏な変革によって実現する市場投入時間短縮のメリットを生み出すことです。

業務の問題

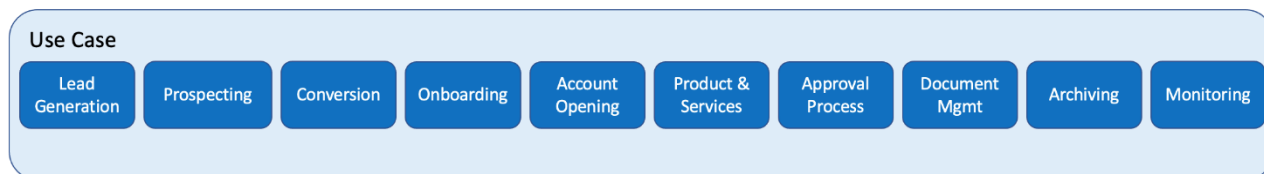
従来型の金融機関は、依然として手動または半自動のプロセスを採用しています。通常の銀行業務プロセスには業界標準は適用されません。ただし、これらのプロセスは同様の管轄区域のすべての金融機関で共通しています。これらの課題を克服するために、従来の金融機関は、AWS クラウドサービス上に構築されたサーバーレスアプローチを使用して、スケーラブルで安全な標準プロセスを実装できます。例えば、[Amazon Lex](#) や [Amazon Rekognition](#) は、強化されたカスタマージャーニーに統合できる、トレーニング済みの機械学習モデルを提供します。以前は、このようなイノベーションは複雑な統合とコストのかかる開発プロセスによって妨げられていましたが、現在では、API コールを通じて、顧客のアプリケーションで直接これらのイノベーションを利用できるようになっています。

AWS クラウドサービスは、さらなるイノベーションと統合速度を提供するだけでなく、最新のセキュリティ機能を活用してデータの機密性とプライバシーを確保します。ここでは、CLM 環境におけるバンキングモダナイゼーションのアプローチに焦点を当てていきます。顧客ライフサイクル

は、顧客との関係の中心です。そのため、ライフサイクルを早急にモダナイズし、さらにはデジタル化する必要があります。McKinsey & Company の「[What the embedded-finance and banking-as-a-service trends mean for financial services](#)」に示されているように、BaaS を提供する銀行はそれを機能させる必要があります。「BaaS は通常、API を介して顧客に提供され、エンベデッドファイナンスパートナーの強力なリスク管理とコンプライアンス管理が必要とされるため、BaaS を機能させるには新しいテクノロジーと機能が必要になります。」この戦略の「サーバーレスオンボーディング」セクションでは、このような戦略を機能させる方法について説明します。

顧客ライフサイクル管理のユースケース

CLM は、顧客とその金融機関または保険会社とのビジネス上のやり取りを定義する、緩やかな相互依存型の必須プロセスセットです。以下の図は、銀行および保険業界の CLM ステージの一般化された概要を示しています。



これらのプロセスは、顧客セグメントによって異なることを考慮してください。例えば、商用顧客のオンボーディングは小売顧客のオンボーディングとは異なります。また、プロセスは業界によって異なる場合があります。銀行顧客のオンボーディングは、保険顧客のオンボーディングとは異なります。この戦略は、銀行の小売顧客体験に焦点を当てています。

上の図では、すべてのボックス (プロスペクティングなど) がモダナイゼーションの候補を表しています。このような図を使用して、ユースケースを個別の独立したユースケースに分類できます。例えば、プロスペクティングユースケースは、構成要素のユースケースに分類できます。次に、独立した各ユースケースを、クラウドサービスプロバイダーまたは BaaS プロバイダーの既存の機能にマップできます。このマッピング作業により、銀行向けのドキュメントアーカイブなどは、それ自体が外部の第三者が提供するサービスである可能性が明らかになります。顧客ライフサイクル管理のユースケースを個別の独立したユースケースに分割することで、焦点を絞ったサービスの設計と開発が可能になります。

この戦略は、新しい銀行口座を開設するユースケースの例に焦点を当てています。これは多くの場合、顧客にとって時間がかかり、手作業が多く、エラーが発生しやすいプロセスであり、フラストレーションや不満が生じます。現在でも、オンボーディングのほとんどは電話や物理的なタッチポイントを通じて、依然として手動で行われています。しかし、調査によると、顧客はデジタルエクスペリエンスを好むことがわかっています。Open Research Europe の「[Digital onboarding in finance: a](#)

[novel model and related cybersecurity risks](#)」によると、顧客の 70% がデジタルによる商品契約を選んでいきます。

顧客オンボーディングの機会

新型コロナウイルス感染症の危機が収束した今、銀行や金融機関の顧客は、煩雑で複雑なプロセスに直面しています。実際のところ、現在、モバイル端末から当座預金口座開設の全プロセスを完了できる顧客はほとんどいません。大多数の顧客は、次のような手動による銀行口座開設のオンボーディングプロセスに従う必要があります。

1. 顧客またはエンドユーザーは、身分証明書、法的身分証明書、およびその他のさまざまなデータポイントを提出する必要があります。多くの場合、これらのデータポイントには、住所や雇用証明などのドキュメントが含まれます。顧客は支店に行ってこれらの情報を提供するか、通常の郵便で銀行に送付する必要があります。
2. 顧客は、銀行口座を利用する前に複数の紙の書類を受け取ります。その後、書類に署名して銀行に返送する必要があります (つまり、個人口座、共同口座、取引口座、電子バンキング、クレジットカード、セキュリティコードなど、銀行の商品ごとに単一の契約書が必要です)。
3. 銀行は、署名された書類をすべてデジタル化し、「進行中」の口座にリンクさせて、口座を運用できるようにします。
4. 顧客セグメントや申請者のリスク評価に応じて、銀行はこのプロセスの一部または全部を定期的に繰り返す必要があります。
5. 顧客の住所、民法上の身分、または「状況の変更」とみなされるその他のデータが更新されると、プロセスは再開されます。

このプロセスの完了には数日から数週間かかることがあり、多くの場合、異なる部署の複数の銀行員による介入と承認が必要になります。

オンボーディングカスタマージャーニー

口座開設のためのモダナイズされたカスタマージャーニーには、以下の特徴と機能が含まれている必要があります。

- 顧客が、インターネットウェブサイト、仮想アシスタント、コールセンターを通じてオンボーディングサービスにアクセスできる。仮想アシスタントはテキスト指向のチャットボットでも音声指向のチャットボットでもよく、ウェブページ、または Messenger や Telegram などのメッセージングアプリケーションに統合します。
- 仮想アシスタントは、事前定義されたインテントを使用して顧客のニーズや背景を把握し、顧客とやり取りできます。例えば、仮想アシスタントは、興味を共有してもらうように顧客に依頼したり、個人情報共有して口座を開いたり、ID をスキャンして自撮りをしたり、顧客が口座開設を続けるかどうかを確認したりできます。
- チャットボットは多言語対応になります。
- 顧客は、音声またはテキストを使用してチャットボットと対話できます。
- 顧客から必要な情報をすべて収集したら、その情報を銀行に送信して、口座開設プロセスを開始できます。顧客には、プロセスが開始されたことを確認する E メール通知が届きます。
- 口座開設後は、ダイアログを閉じることができます。
- 顧客情報をクラウドに保存することは避けてください。この情報は一時的なものである必要があり、顧客との契約期間中にのみ存在する必要があります。口座開設プロセスが完了したら、データを削除し、可能であれば、削除の証拠を提出する必要があります。ダイアログが中断された場合でも、すべての個人データが削除されている (キャッシュされない) ことを確認する必要があります。
- 個人を特定できる情報 (PII) のログを保存することは避けてください。
- PII データは保存されないため、顧客は安心できます。使用するサービスがサーバーレスの場合、個人データを含むデータやログは残りません。

サーバーレスオンボーディング

このセクションでは、顧客オンボーディングのユースケースに焦点を当てています。サーバーレスパターンを再利用して、主要なカスタマージャーニーをモダナイズする方法の一例をご紹介します。

オンボーディングソリューション

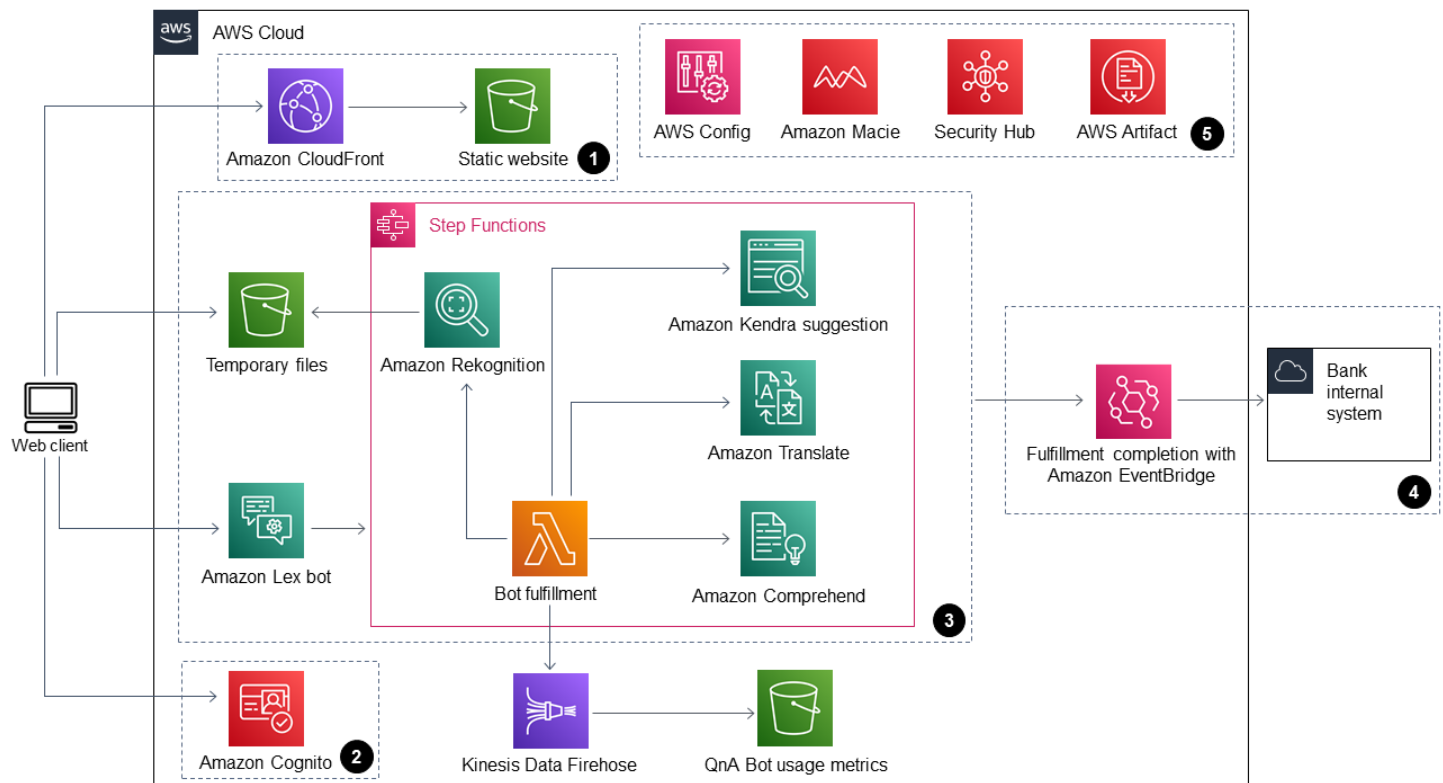
オンボーディングソリューションは通常、単独で提供されるわけではなく、より大きな全体像の一部として提供されます。統合に必要なコンポーネントとサービスには以下が含まれます。

1. リードジェネレーション (CRM システム)
2. デューデリジェンス (AML、リスク、コンプライアンス)
3. 中央クライアントデータファイル (コアバンキングシステム)
4. デジタル署名管理 (DocuSign などのサードパーティツールを使用)
5. バイオメトリクス検証
6. デジタル契約管理ライフサイクル
7. プロセスと運用モデルの自動化

メモ

これらのコンポーネントを外部アプリケーションに統合することは、この戦略の範囲外です。

次の図は、AWS クラウド内のチャットボットを通じて顧客とやり取りするためのサーバーレスアーキテクチャを示しています。



メモ

アーキテクチャは、QnA Bot on AWS ソリューションと Amazon Rekognition の更新に基づいています。詳細については、AWS「ソリューションライブラリ」の「[QnA Bot AWS](#)」および AWS Machine Learning Blog の「[Amazon Rekognition が顔の検出、分析、認識機能の更新を発表しました](#)」。[Amazon Rekognition](#)

この図表は、次のワークフローを示しています：

- 顧客はフロントエンドコンポーネントにアクセスして、ボットとやり取りします。この場合、フロントエンドライブラリをさまざまな方法で、既存のアセットに含めることができます。例えば、これらのコンポーネントを企業のウェブサイト統合したり、主要なチャットアプリにリンクさせたりできます。これらのコンポーネントは JavaScript で配信され、Amazon Simple Storage Service (Amazon S3) と Amazon CloudFront を使用した静的アセット管理を通じて提供されます。
- フロントエンドコンポーネントは、Amazon Cognito を介して認証情報を検証するために、バックエンドコンポーネントへの接続を埋め込みます。承認されると、顧客サービスはオンボーディングソリューションのサービスと通信できます。

3. 顧客は Amazon Lex ボットを使用してサービスとやり取りします。オンボーディングの事前定義されたシナリオは、AWS Step Functions を使用して必要なサービスを呼び出し、プロセスを完了することによって実行されます。このシナリオは、バンキングシステムのニーズ (写真撮影の要件、多言語での翻訳、顧客の意図に合わせた自然言語処理など) に合わせてカスタマイズできます。AWS Lambda 関数を使用して、Amazon Lex ボットのアクションを実行し、オンボーディングステージに応じて サービスを呼び出すことができます。
4. Step 関数の出力は、Amazon EventBridge を介して銀行の内部システムに一括送信されます。Amazon EventBridge は、任意の方法で銀行の内部システムに接続できます。この通信は、別の AWS アカウントへのピア接続、または仮想プライベートネットワーク (VPN) を介した銀行システムへのネットワークピア接続のいずれかで処理できます。
5. アーキテクチャ全体は AWS Config、Amazon Macie AWS Artifact、および を使用してセキュリティとコンプライアンスを実現するように設計されています AWS Security Hub CSPM。

セキュリティとコンプライアンスに関する考慮事項

セキュリティの維持と機密情報の処理は、サーバーレスオンボーディングアプローチの中心です。サーバーレスオンボーディングはステートレスになるよう設計されており、PII や重要なビジネスデータは保存されません。セキュリティとコンプライアンスを継続的に確保するには、以下のサービスを導入し、正しく設定する必要があります。

- AWS AppConfig は、コンプライアンスに合わせてカスタマイズされたルールを通じて、サービスの整合性と機密性を確保します。実行される制御により、全体的なコンプライアンスが検証され、設定のドリフトが阻止されます。
- Macie はプロセス全体を通じてあらゆる PII を検出し、タグ付けします。
- Security Hub CSPM は、すべてのサービスがセキュリティ範囲内で定義および使用されるようにします。
- AWS Artifact は、AWS サービスのコンプライアンスに関する監査証拠を提供します。

トランザクションや非否認の証拠は、カスタマーマネージドキーまたは監査目的で封印された専用のハードウェアセキュリティモジュール (HSM) を使用して、保存および暗号化されます。Amazon Glacier を使用して、整合性とセキュリティを確保しながら、低コストでデータをシールすることもできます。

 Note

Amazon Glacier (元のスタンドアロンのポールドベースのサービス) は、2025 年 12 月 15 日以降、新規のお客様を受け入れなくなります。既存のお客様に影響はありません。

Amazon Glacier は、ポールドにデータを保存する独自の API を備えたスタンドアロンサービスであり、Amazon S3 および Amazon S3 Glacier ストレージクラスとは異なります。既存のデータは Amazon Glacier で無期限に安全性が確保され、引き続きアクセス可能です。移行は必要ありません。低コストの長期アーカイブストレージの場合、は [Amazon S3 Glacier ストレージクラス](#) AWS を推奨します。これにより、S3 バケットベースの APIs、低コスト、AWS のサービス 統合で優れたカスタマーエクスペリエンスを実現できます。AWS リージョン 拡張機能が必要な場合は、[Amazon Glacier ポールドから Amazon S3 Glacier ストレージクラスにデータを転送するためのAWS ソリューションガイド](#)を使用し、Amazon S3 Glacier ストレージクラスへの移行を検討してください。

環境へのアクセスは、運用チームのみに許可する必要があります。開発アクティビティは、自動化された継続的デリバリーによって合理化し、本番環境への人間のアクセスを阻止する必要があります。プラットフォーム上のアーティファクトとコンプライアンスレポートにアクセスするための追加のルールを、監査のためにプロビジョニングする必要があります。

AWS は、規制およびコンプライアンスの基準を満たすのに役立ちます。詳細については、AWS ドキュメントの「FINMA ISAE 3000 Type 2 Report」を参照してください。FINMA Circular 2008/21 AWS Artifact、FINMA ISAE 3000 Type 2、FINMA Circular 2018/03、Global Financial Services Regulatory Principles など、関連するバンキングアーティファクトを から直接ダウンロードすることもできます。

よくある質問

AWS サービスが個人データを保存しないようにするにはどうすればよいですか？

AWS Config を使用して、Macie と組み合わせてアーキテクチャコンポーネントのコンプライアンスをチェックし、検出された個人データを検出して修復できます。

アーキテクチャは GDPR に準拠していますか？

はい。「GDPR」の第 2 章、[第 5 条](#)に記載されているように、このアーキテクチャは、ユーザーに関連するデータを長期的には保持せず、プロセス PII に関連するデータのみを保持するように設計されています。これは、継続的なコンプライアンスメカニズムによって保証されています。さらに、Macie は GDPR コンプライアンスを危険にさらす可能性のある、PII データのタグ付けと分類を確実に行います。

適切なデータの機密性を確保するにはどうすればよいですか？

機密性は、Security Hub CSPM、および Macie を使用して AWS Config、継続的なコンプライアンスとセキュリティパターンを通じて確保されます。機密性違反は直ちに検出、修正、エスカレートされます。デプロイ段階でガードレールを追加することもお勧めします。ガードレールは、機密性を危険にさらす可能性のある重大な変更がアーキテクチャにプッシュされるのを防ぎます。

AWS バンキングモダナイゼーションソリューションをレガシーバンキングシステムと統合できますか？

このソリューションは高い適応性を備えているため、標準の API コールを受け入れることができるレガシーバンキングシステムと統合できます。

オンボーディングダイアログはカスタマイズできますか？

はい。チャットボットのダイアログは、ユースケースや対象となるダイアログのシーケンスに合わせてカスタマイズできます。詳細については、「AWS ソリューションライブラリ」の [「の QnA Bot AWS」](#) を参照してください。

次の手順

クライアントオンボーディング以外にも CLM ユースケースがあり、これらのユースケースは組み込み AWS クラウド サービスでモダナイズできます。以下のシナリオでは、モダナイゼーションの潜在的なユースケースをいくつか検討しています。

1. [Amazon Personalize](#) またはその他のカスタムメイドのレコメンデーションを使用して、製品のレコメンデーションをバンキング製品やサービスに組み込んでください。FS 製品は小売製品とは異なりますが、The Financial Brand の「[Industry Leaders Predict Massive Changes in Banking by 2025](#)」によると、2025 年までに高い度合いのパーソナライゼーションが起こると予測されています。顧客は、高度にパーソナライズされたコンテキストサービスにもっと料金を支払うことを厭わないかもしれません。これは、機械学習をベースにしたよりスマートなソリューションによって初めて実現できます。
2. アカウントのモニタリングには、機械学習に基づくオンライン不正検出機能である [Amazon Fraud Detector](#) を使用できます。他の組み込みアルゴリズムをカスタマイズ (異常検出を使用するなど) して、標準化されたアカウントモニタリングサービスを提供することもできます。

Note

Amazon Fraud Detector は、2025 年 11 月 7 日をもって新規顧客に公開されなくなりました。Amazon Fraud Detector と同様の機能については、Amazon SageMaker、AutoGluon、および [AWS WAF](#) を参照してください。詳細については、「[Amazon Fraud Detector の可用性の変更](#)」を参照してください。

3. Amazon Lex と、最新の自然言語モデルに基づくチャットボットを使用することで、スマートアシスタントが顧客と直接やり取りできるようになります。

クリエイティブなソリューションに制限はありませんが、これらのソリューションを大規模かつ迅速に統合し、デプロイする必要があります。

リソース

- [What the embedded-finance and banking-as-a-service trends mean for financial services](#) (McKinsey & Company)
- [Digital onboarding in finance: a novel model and related cybersecurity risks](#) (Open Research Europe)
- [Industry Leaders Predict Massive Changes in Banking by 2,025](#) (The Financial Brand)
- [AWS スイスの金融サービス規制とガイドラインに関するユーザーガイドおよび FINMA ワークブックの出版物](#) (AWS セキュリティブログ)
- [FSI サービススポットライト: 特 AWS Lambda](#)集 (AWS ブログ記事)
- [Amazon Rekognition が顔の検出、分析、認識機能の更新を発表](#) (AWS Machine Learning ブログ)
- [での QnA ボット AWS](#) (AWS ソリューションライブラリ)

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、[RSS フィード](#) をサブスクライブできます。

変更	説明	日付
初版発行	—	2022 年 6 月 8 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。