カスタマー・アイデンティティ・アクセス管理（CIAM）プラットフォームの選定基準の例

Akamai

ベンダー評価の出発点

本書は、カスタマー・アイデンティティ・アクセス管理（CIAM）ソリューションの RFP の作成に役立つ質問集です。このガイドは、チームや関係者が自らの組織に固有の要件や優先事項を確認する際の出発点として使用することを意図しています。本書の質問は、CIAM ソリューションやベンダーを比較するための基本的な評価基準となります。

ベンダーの情報

1. 貴社の名称は何ですか？
2. オフィスの所在地と各オフィスの従業員数をすべて記載してください。
3. 貴社は創業何年ですか？
4. 貴社の沿革を簡単に説明してください。
5. 製品およびサービスポートフォリオの概要を説明してください。
6. 貴社のプラットフォームの世界規模での可用性について説明してください。
7. 他の組織との商業的または技術的パートナーシップについての情報を記載してください。
8. 貴社の財務状況の概要を説明してください。

経験と参考資料

1. CIAM ソリューションの提供に関する貴社の経験について説明してください。
2. 貴社のクライアント数はどれくらいですか？
3. 現在稼働しているプロジェクトの例を 5 つ以上挙げてください。
4. 貴社のクライアントのうち、規模や範囲が弊社と同等のクライアントの名前を挙げてください。
5. CIAM 領域における貴社のリーダーシップについて説明している、独立機関による調査報告書（アナリストレポートなど）を提出してください。
6. 貴社における CIAM 関連の発明的、革新的、または先進的な開発の事例について説明してください。

CIAM の機能

1. 貴社の CIAM ソリューションスイートについて、詳細に説明してください。
2. どのようなレジストレーション機能をサポートしていますか？（CAPTCHA、インライン検証、データ検証など）
3. 複数のソーシャルネットワークや ID プロバイダーによる認証をサポートしていますか？（Facebook、Google、Twitter、LinkedIn など）
4. クライアントは、ユーザー入力フォームをサイトのイメージと操作性に合うように簡単に設定できますか？また、その画面はどれくらい柔軟にカスタマイズできますか？
5. ユーザー入力フォームをクライアントのサイトに統合するプロセスについて説明してください。
6. 貴社のソリューションと連携できるデバイスについて、詳しく説明してください。説明には、モバイルデバイス、タブレット、IoT デバイス、コネクテッドデバイスを含めてください。
7. 応答性について詳しく説明してください。
8. どのソフトウェア開発キット（SDK）を標準プラットフォームとモバイルプラットフォームの両方に使用できますか？
9. 貴社のシステムは、多言語国家への対応として、すべてのフィールドで各種言語（UTF-8 や全角文字）をサポートしていますか？また、特殊文字（スペイン語の「ñ」、ドイツ語の「ö」、フランス語の「ç」など）を使用することはできますか？
10. 貴社のソリューションはオープンスタンダードですか？
11. 貴社のサービスには、詳細なレポート機能がありますか？
12. 貴社のプラットフォームの認証機能について説明してください。
13. 貴社のプラットフォームのアクセスコントロール機能およびアクセスポリシー管理機能について説明してください。
14. 貴社のプラットフォームの管理機能について説明してください。
15. クライアントは、デバイス、サブスクリプション、サブプロファイルなど、他のリソースを作成し、管理することができますか？
16. 消費者のユースケースにおいて、管理者の委任をどのようにサポートしているか説明してください。
17. 消費者は、友人や家族に代わってアカウントを作成したり、友人や家族を招待したりすることはできますか？
18. エンドユーザーに一元管理型の認証サービスを提供していますか？
19. 標準的なライブラリーを使って、ウェブアプリやモバイルアプリを貴社のプラットフォームに接続することはできますか？
20. 貴社のプラットフォームでは、どのように同意データが保管されますか？
21. 同意の監査履歴は、どれくらいの期間保管されますか？
22. 粗い同意ときめ細かい同意の両方をサポートしていますか？
23. エンドユーザーは同意データを完全に把握し、管理することができますか？
24. 必要に応じて、文脈の中で同意を得ることはできますか？

25. エンドユーザーは、自身のデータのコピーをダウンロードできますか？
26. エンドユーザーのデータは、要求に応じて削除することができますか？
27. 貴社のソリューションには、設定可能な認証機能がありますか？
28. 貴社の認証機能は、どれくらいの粒度に対応していますか？（RBAC、ABAC など）
29. 貴社のソリューションは、ポリシー属性の動的ルックアップをサポートしていますか？
30. 貴社のソリューションは、複数の ID プロバイダーのポリシーをサポートしていますか？
31. 貴社のソリューションでは、認証判断の監査ログを提供していますか？また、そのログでは、機微な情報を自動で暗号化することはできますか？
32. ポリシーはどのように作成されますか？（ポリシー作成のためのビジュアルツールはありますか？それとも、ポリシーはテキストやコードの設定で作成されますか？）
33. 貴社のポリシーの妥当性、完全性、影響の分析を行うために、どのようなツールを提供していますか？
34. 貴社のソリューションには、ポリシーの作成者、変更者、削除者を管理する機能はありますか？

統合

1. 貴社のプラットフォームは、どのブラウザーに対応していますか？以下の中から選択してください。
    - 1.1 Firefox
    - 1.2 Google Chrome
    - 1.3 Apple Safari
    - 1.4 Microsoft Edge
    - 1.5 Microsoft Internet Explorer
    - 1.6 Android ブラウザー
2. 以下のカテゴリーについて（ただしそれらに限定せずに）、サードパーティー製プラットフォームとの統合をどのようにサポートしているか説明してください。
    - 2.1 CRM ソリューション
    - 2.2 電子メール・マーケティング・プラットフォームおよびサービス
    - 2.3 その他のデジタル・マーケティング・プラットフォーム
    - 2.4 E コマースプラットフォーム
    - 2.5 CMS ソリューション
    - 2.6 BI および分析ソリューション
    - 2.7 SIEM およびログ・モニタリング・ソリューション

3. 貴社のプラットフォームは、バッチ統合とリアルタイム統合の両方のパターンをサポートしていますか?
4. 貴社のプラットフォームから取得されるプロファイルデータのフォーマットのオプションについて説明してください。
5. イベントデータは、フィードの一部として使用できますか？使用できるイベントをすべて記載してください。
6. 認証および同意されたデータのみが下流システムに送られるようにするために導入されている管理方法について説明してください。

API

1. 貴社のプラットフォームの以下のアプリケーション・プログラム・インタフェース（API）について説明してください。
    - 1.1 登録 API（クライアント側およびサーバー側）
    - 1.2 認証 API（クライアント側およびサーバー側）
    - 1.3 アカウント更新 API（クライアント側およびサーバー側）
    - 1.4 管理 API
    - 1.5 クエリー API

プラットフォームアーキテクチャ、データストレージ、インフラストラクチャ

1. 貴社のプラットフォームアーキテクチャとデータ取得方法について説明してください。
2. 認証プロセス中にユーザーのプロファイルデータを収集するために、リアルタイムのクエリー可能な構造データベースを提供していますか？
3. 貴社のデータスキーマの柔軟性について説明してください。データフィールドの追加や削除、任意フィールドから必須フィールド（または必須フィールドから任意フィールド）への変更はできますか?
4. ユーザーレコードからデータ項目を削除する機能（法的な理由で要求された場合など）について説明してください。また、貴社のソリューション内で、データ・アクセス・セキュリティのルールに則ってそれを行う方法について説明してください。
5. ユーザーが貴社のソリューションからアカウントを削除した場合、何が起こるか説明してください。
6. 貴社のソリューションでは、どのようにユーザーに自身のプロファイルデータの変更を許可しているか説明してください。
7. データの複製、耐障害性、インフラストラクチャの可用性に関して、ソリューションの詳細を説明してください。
8. 貴社のデータおよびバックアップストレージ設備の技術的な詳細（地理的位置、関連する物理的および論理的セキュリティフレームワーク、バックアップ手順など）を説明してください。
9. 目安として、最大でどれくらいの量のユーザーレコードを記録できますか？
10. 顧客はどのようにシステム可用性をモニタリングできますか？
11. 貴社はどの程度のシステム可用性を保証しますか？また、そのレベルに満たない場合、信用回復のためにどのような財務的措置が講じられますか？

12. 技術上または運用上の重大な混乱が生じた場合のビジネス継続性計画案の概要を説明してください。これには、災害復旧プロセスなどが含まれます。

13. 貴社のソリューションは、要求に応じて（大規模なユーザー向けプロモーションを行う場合など）動的に拡張することができますか？できない場合、予想されるトラフィックの急増に対処するためには、どれくらい事前に通知する必要がありますか？これに対応できるインフラストラクチャをすでに配備していますか？

14. または、貴社のソリューションでは、このような要求に対応できるだけの十分な余裕のある大容量データベースを使用していますか？

15. 独立した機関によるパフォーマンスベンチマークはどのようなものを行いましたか？ベンチマークの結果を提示してください。

16. 貴社のプラットフォームでは、コンポーネントを独立して拡張するためにマイクロサービスアーキテクチャを使用しますか？

17. 貴社のプラットフォームでは、カスタマープロファイルとウェブイベントのレポジトリは異なりますか?

18. 貴社のインフラストラクチャは、顧客のプロファイルとウェブアクティビティを統合しますか？

19. 貴社のインフラストラクチャには、データ・ウェアハウス・レポートのためにデータを照合、変換、適合させるデータパイプラインはありますか？

サイバーセキュリティおよびデータ保護

セキュリティ全般

1. Standardized Information Gathering（SIG）Questionnaire を作成し、提出してください。

2. 貴社のセキュリティアーキテクチャについて説明してください。これには、ネットワーク、データベース、アプリケーションレイヤーのセキュリティが含まれます。

3. セキュリティおよびプライバシーの概要書はありますか？

セキュリティプログラム

1. 情報セキュリティ管理プログラム（ISMP）はありますか？ある場合、どの程度の有効性があると評価されていますか？

2. リスクプログラムはありますか？

   2.1 既知のリスクの追跡方法と管理方法を説明してください。

   2.2 正式なリスク評価をどのように行っているか説明してください。それはどれくらいの頻度で行われますか？また、その範囲について説明してください。

3. ウイルス対策をどのように管理していますか？

アクセス制御

1. 従業員によるプロダクションシステムへのアクセスをどのように管理していますか？

2. 多要素認証を使用していますか？

変更管理

1. 変更管理ポリシーはありますか？
2. 変更管理手順を順守するために、どのような措置が講じられていますか？
3. コア製品の技術開発中、どのように変更管理を実施していますか？
4. クライアントのアプリケーション設定の変更管理プロセスについて説明してください。
5. クライアントのカスタマイズの変更管理プロセスについて説明してください。
6. メンテナンスやパッチについて、どのようにクライアントに通知していますか？
7. 製品リリースについて、どのようにクライアントに通知していますか？

データ保護

1. 保管データを暗号化していますか？また、その方法について詳しく説明してください。
2. データを送信する際、暗号化していますか？また、その方法について詳しく説明してください。
3. 貴社のソリューションでは、他のシステム、ウェブサイト、モバイルサイト、外部関係者がどのフィールドを閲覧、確認、修正、削除できるかをクライアントがコントロールできるよう、個別のデータフィールドに細かいセキュリティ・アクセス・コントロールを設けていますか？
4. 貴社のソリューションでは、アプリケーションや人による保管データへのアクセスに対して、複数のセキュリティレベルを設けていますか？それらのセキュリティレベルは、アプリケーション別またはロール別に適用することができますか？
5. どのような侵入検知メカニズムを使用していますか？

キー管理

1. 暗号化キーをどのように管理していますか？
2. 顧客は独自の暗号化キーを使用することはできますか？

パスワード管理

1. パスワードをハッシュ化しますか？
2. ハッシュ化アルゴリズムにどのようなコストファクターを使用していますか？
3. 各エンドユーザーに個別のソルトを付与していますか？
4. パスワードをリセットする際、どのようにソルトを処理していますか？
5. クライアントは独自のパスワード規則（独自のパスワード正規表現）を選択することができますか？

耐久性

1. クライアントデータのストレージはどれくらいの耐久性がありますか？

モニタリング

1. 24 時間 /365 日体制でモニタリングしていますか？
2. プラットフォームの状態について顧客にリアルタイムで通知していますか？
3. クライアントアプリケーションの傾向をモニタリングしていますか？
4. 高度な持続的分散攻撃にどのように対処していますか？
5. サービス妨害（DoS）攻撃にどのように対処していますか？
6. IP をブロックすることはできますか？
7. 貴社のソリューションは、セキュリティイベントをセキュリティ管理または SIEM プラットフォームにエクスポートすることができますか？

ネットワーク保護

1. 貴社のファイアウォールについて説明してください。
2. セキュリティグループを使用していますか？
3. 仮想プライベートクラウド（VPC）を使用していますか？
4. 貴社のソリューションはゼロトラスト設計ですか？
5. 何の要素を強化していますか？

ビジネス継続性および災害復旧（BCDR）

1. ビジネス継続性に関するポリシーはありますか？詳細に説明してください。
2. 定期的に BCDR 計画の訓練を行っていますか？
3. クライアントデータを別のデータセンターに同時に書き込んでいますか？
4. クライアントデータのバックアップをいくつ作成していますか？
5. コアプラットフォームのバックアップをいくつ作成していますか？
6. バックアップからの復元をテストしていますか？している場合、どれくらいの頻度で行っていますか？また、外部監査機関による検証を受けていますか？
7. 実際に災害復旧計画やビジネス継続性計画を実施したことはありますか？ある場合、詳しく説明してください。

侵入および脆弱性テスト

1. どれくらいの頻度でネットワーク侵入テストを行っていますか？

コンプライアンス

1. 以下のうちどのコンプライアンス認証を外部の認定監査機関から取得していますか？

    1.1 SOC 2 Type 2 Security（Common Criteria）— この認証を取得している場合、レポートを提出してください。

    1.2 SOC 2 Type 2 Availability — この認証を取得している場合、レポートを提出してください。

    1.3 SOC 2 Type 2 Confidentiality — この認証を取得している場合、レポートを提出してください。

    1.4 SOC 2 Type 2 Processing Integrity

    1.5 SOC 2 Type 2 Privacy

    1.6 ISO 27001:2013 — この認証を取得している場合、レポートを提出してください。

    1.7 ISO 27018:2014 — この認証を取得している場合、証明書のリンクを提示してください。

    1.8 HIPAA — この認証を取得している場合、レポートを提出してください。

    1.9 HITECH — この認証を取得している場合、レポートを提出してください。

    1.10 CSA Star Level 2 認証 — この認証を取得している場合、証明書のリンクと認証レポートを提出してください。

    1.11 Privacy Practices — この認証を取得している場合、評価証明書を提出してください。

    1.12 Privacy Shield — この認証を取得している場合、評価証明書を提出してください。

EU 一般データ保護規則（GDPR）

1. 貴社のソリューションには、GDPR に基づいたデータ主体の要求に対応するためのワークフローがありますか？
2. 国境を越えて個人データを転送する場合に貴社が転送の合法性を維持するために順守または規定できる転送メカニズムを提示してください（Privacy Shield 認証、拘束的企業規則（BCR）、標準的契約条項など）。
3. どのような GDPR トレーニングを行っていますか？
4. 情報セキュリティマネージャーはいますか？
5. 個人情報保護担当の副社長または統括責任者はいますか？
6. 貴社のソリューションには、同意管理機能はありますか？

サポートとサービス

1. 貴社のソリューションの導入プロセス、導入中にクライアントが利用できるサポート機能、市場投入までの平均時間の概要を説明してください。
2. 貴社のテクニカル・サポート・サービス（24 時間 /365 日年中無休オプション、SLA など）について説明してください。
3. 貴社が提供する戦略サービスおよびコンサルティングサービスについて説明してください。
   - 3.1 貴社には、サードパーティー製ソリューションとの統合やエンタープライズアーキテクチャのベストプラクティスについての専門知識がありますか？
4. 貴社が提供するトレーニングサービスやトレーニングプログラムについて説明してください。
5. テクニカル・サポート・エンジニアの採用基準は何ですか？
6. テクニカル・サポート・チームの所在地はどこですか？
7. テクニカル・サポート・チームはどのようなトレーニングを受けていますか？
8. チケットの品質について、テクニカル･サポート･チームはどのように評価や指導を受けていますか？
9. テクニカル・サポート・チームはどのようにして成功を測定していますか？
10. テクニカルサポートとエンジニアはどのような関係ですか？
11. 起こり得る設定ミスから顧客を保護するために、テクニカル・サポート・チームはどのようなプロセスを実施していますか？
12. 不正な設定リクエストや設定変更から、どのように顧客を保護しますか？
13. 毎月または四半期ごとに、テクニカル・サポート・チームは顧客にどのようなデータを提供していますか？
14. テクニカルサポート上の問題について、どのようなエスカレーションプロセスが設けられていますか?
15. 既存顧客に対する SLA の順守状況について説明してください。
16. テクニカル・サポート・チケットに関する顧客満足度をどのように測定していますか？
17. ソリューションアーキテクチャに関するコンサルティングを行っていますか？
    - 17.1 そのコンサルティングには、顧客の既存の情報エコシステム内でのアイデンティティ管理の統合（データ取得、マーケティングの自動化、運用レポート、ビジネス分析、その他の IT プロセスなど）に関するアドバイスが含まれていますか？