ホワイトペーパー

デジタルアイデンティティのセキュリティ保証：

顧客データのセキュリティを維持する方法

Akamai

エグゼクティブサマリー

デジタルアイデンティティと顧客プロファイルの管理は、あらゆる企業にとってデジタル変革の要と言えます。お客様のアイデンティティとそれに関連する個人データは、あらゆる組織の最も重要かつ貴重な資産です。このようなデジタルアイデンティティを登録からその後の顧客関係に至るまで保護し、関連データから継続的にビジネス上の価値を確保することは、企業の成功にとって不可欠です。

企業がデジタルアイデンティティを管理し、消費者の信頼を構築するためには、最高レベルのセキュリティ対策を適用して自社とそのお客様を保護する必要があります。最悪のケースでは、お客様がアイデンティティ窃盗の被害者となり、経済的、職業的、身体的な安全に深刻な影響を受けることもあります。これらのすべては、信頼の喪失につながる可能性があるだけでなく、その企業への賠償請求や集団訴訟の原因になる場合もあります。

さらに、EU の General Data Protection Regulation（一般データ保護規則、GDPR）[1]、California Consumer Privacy Act（カリフォルニア州消費者プライバシー法、CCPA）[2]、カナダの Personal Information Protection and Electronic Documents Act（個人情報保護および電子文書法、PIPEDA）[3] などの国際的なプライバシー規則、および医療情報のセキュリティに関するプライバシー法などの業界固有の規則を遵守するために、企業は厳格な個人情報保護対策を実施する必要があります。

このホワイトペーパーでは次のことについて説明しています。

- **カスタマー・アイデンティティ・アクセス管理（CIAM）とセキュアかつ堅牢なインフラストラクチャで消費者のアイデンティティを保護する必要性**
- **範囲を限定したアクセスなどの高度で柔軟なセキュリティ機能の必要性**
- **エッジネットワーク保護の重要性**
- **増え続ける国際的なプライバシー規則**
- **消費者の信頼の構築方法**
- **クラウドベース CIAM の利点**

そして最後に、データプライバシー規則が増え続ける中で、世界大手の製薬会社がクラス最高のセキュアな CIAM ソリューションを導入して、同社のヘルスケアプロバイダーを支援している実例を簡潔にご紹介します。

お客様のアイデンティティの保護

お客様のデジタルアイデンティティは貴重なアセットです。企業では、お客様の嗜好やふるまい、人口統計に基づいて顧客体験をパーソナライズするために、ますますアイデンティティデータを使用するようになっています。体験をパーソナライズするためにアイデンティティデータを収集することは、企業と消費者の両方にメリットをもたらしますが、データ漏えいのリスクも高まります。データ漏えいが発生すると、ブランドイメージが低下し、対応に高額な費用が必要となります。

IBM Security と Ponemon Institute が実施した調査、2019 Cost of a Data Breach Study（2019 データ漏えいのコストに関するレポート）では、対象組織の 48% がデータ漏えいの根本原因は悪意のある攻撃または犯罪者による攻撃であるとし、漏えいしたアイデンティティレコードあたりの平均コストは約 157 ドルであることがわかりました [4]。お客様の個人情報の漏えいレコード数は数十万に上ることも多く（数百万規模もあります）、これによるコストは企業に深刻な影響を及ぼす可能性があります。しかもこのコストには、評判やお客様からの信頼が損なわれることによる収益損失は含まれていません。

お客様のデータの取得と保存および認証情報や個人情報の保持と処理は、企業や組織にとって違反や不履行が許されない注意義務事項です。また、追加の指令として、各国政府はお客様の個人を特定できる情報（PII）を保護する法律を施行しています。EU の GDPR、カリフォルニア州の CCPA、カナダの PIPEDA や、そのほかにも多数のデータプライバシー規則が世界中で制定されています。

グローバルブランドが、さまざまな地域のデータプライバシー規則の微妙な差異を遵守するためには、適用される法律に従って PII を詳細に収集、処理、保存するための戦略を策定する必要があります。または、世界中の規則を遵守するために、データプライバシー戦略を全面的に見直すことを検討する必要があります。

お客様個人のアイデンティティを保護することに加えて、基盤となる IT インフラストラクチャ自体を、分散型サービス妨害攻撃（DDoS）などの脅威から保護する必要があります。さもないとダウンタイムやパフォーマンスの低下、消費者の信頼の喪失、潜在的な経済的損失がもたらされることになります。実際、特定の顧客データの収集はインフラストラクチャの保護に役立ちます。たとえば、詐欺行為を防止するために、お客様が使用する IP アドレスを記録し、ブラックリストに照らしてチェックすることが可能です。GDPR などの最近のデータプライバシー規則の多くでは、IP アドレスを個人情報として捉えていますが、セキュリティを目的とした場合に限り、そのようなデータの収集と処理を認めています。

顧客データの保護

顧客データを保護し、消費者の信頼を維持するために、企業はクラス最高の CIAM ソリューションの使用を開始して、強力な暗号化と範囲を限定したアクセスによる制御によってユーザーデータや認証情報を保護する必要があります。CIAM ソリューションを社内で構築する場合でも、プロフェッショナルグレードの商用ソリューションを展開する場合でも、組織はそのアイデンティティ管理ソリューションで次のことが可能かどうかを確認する必要があります。

- **伝送時と保存時の強力な暗号化により顧客データのセキュリティを確保する**

- **データとアプリケーションの両方に対して範囲を限定したアクセスによる制御を提供する。アクセス制御は個々のデータ・レコード・フィールドのレベル（「無しか全部か」のみが可能なシステムレベルではなく）、およびロールや属性まで制御可能なことが推奨されます**
- **ステップアップやワンタイムパスワード（OTP）による認証、および CAPTCHA チャレンジレスポンス方式のサポートによる強力なユーザー認証方法で顧客アカウントを不正利用から保護する**
- **重要なアプリケーションに到達してサービスの停止やパフォーマンスの低下、コンピューティングコストの増大が引き起こされる前に、攻撃トラフィックを阻止する**
- **International Organization for Standardization（国際標準化機構、ISO）27001:2013 および 27018:2014、Service Organization Control（SOC）2 Type II、Cloud Security Alliance（CSA）STAR レベル 2 などのセキュリティ保護認定および認証を遵守する**
- **GDPR、CCPA、PIPEDA、その他多数の業界固有の規則およびヘルスケア規則を含む、さまざまな地域のデータプライバシー規則を完全に遵守する**

範囲を限定したアクセスによる制御

お客様のアイデンティティ情報を保護するためには、きめ細かい許可レベルを提供する CIAM ソリューションを採用し、どの個人やアプリケーションが情報にアクセスし操作できるかを、その役割と責任に基づいて完全に制御する必要があります。

データの列、行、フィールドまでのきめ細かいアクセス制御を適用できることが推奨されます。たとえば、開発者に顧客データへのアクセスを許可することなく、それらの開発者がアプリケーション管理タスクを実行できるように役割を定義できる必要があります。

さらに、CIAM ソリューションは、典型的な管理業務に基づき、最小権限の原則に従って事前に役割を設定し、それらの役割を使用できるように提供する必要があります。たとえば、管理権限を持たない状態で顧客データにアクセスできるという、カスタマーサービス担当者用の役割などです。

このような範囲を限定したアクセスは、会社の従業員、業務委託先や、組織の営業およびマーケティングアプリケーションに対して設定できる必要があります。この機能は、有害なデータの拡散の防止に非常に役立ちます。たとえば、ユーザーがメールコミュニケーションの受信をオプトアウトした場合、範囲を限定したアクセス機能を持つ CIAM ソリューションは自動的に、マーケティング・オートメーション・システムやその他の機能がそれらの人々のメールアドレスにアクセスすることをブロックできます。

エッジでの保護

デジタルアイデンティティのセキュリティにおいて重要なコンポーネントは、エッジネットワークの保護です。エンタープライズグレードの CIAM ソリューションは、機会をうかがっている高度な不正行為から DDoS 攻撃や悪意のあるアプリケーション・プログラミング・インタフェース（API）による呼び出しに至るまで、ますます複雑で高度化する脅威から登録エンドポイントを保護する必要があります。

保護レイヤーを配置してネットワークエッジでアイデンティティエンドポイントを保護することで、悪意のあるアクティビティや攻撃者（およびそれらが引き起こす可能性のある大規模な攻撃トラフィック）を検知し、それらが実際のサイトやアプリケーションに到達しないように阻止することができます。

アイデンティティ体験のパフォーマンスを促進するために、エンタープライズソリューションはインテリジェントなキャッシングテクノロジーも採用する必要があります。これにより、データとユーザー体験をエンドユーザーの近くで維持および処理できます。

プライバシー規則と信頼

デジタルアイデンティティのセキュリティの概念と密接に関連しているのが、消費者のプライバシー保証の概念です。付属のホワイトペーパー「GDPR、CCPA、さらなる規制：コンプライアンスとお客様の信頼向上に役立つアイデンティティガバナンス」で説明したように、データ漏えいや ID の窃盗、それらに関するスキャンダルが広く報じられることによって、GDPR や CCPA など、ますます多くのプライバシー規則が世界中で急速に制定されています[5]。米国だけでも 10 州が、広範囲にわたるビジネス上の義務を課す法案を施行または可決しています[6]。これらは PII に関して、より高い透明性と制御権を消費者に与えるよう規定されています。

企業がこれらの新しいプライバシー法や規制を無視することは許されません。金銭面だけを見ても、GDPR 施行後の最初の 12 か月の間は中程度の規模の罰金が科されることはありましたが、今でははるかに大きな罰金を科されるケースが発生しています。その最大規模の例は、ある世界大手のホスピタリティ企業です。3 億 8,000 万人のホテル滞在者の個人情報をハッキングされたことによって科された罰金は、1 億 2,300 万ドルでした[7]。このような罰金は今後も増え続けることは間違いなく、その GDPR 法令上の上限は該当企業の全世界における年間売上高の 4% と定められています。

しかし、グローバル企業にとっての代償は金銭面だけに留まりません。消費者からの信頼もリスクにさらされます。今日の企業が個人データを処理するためには、個人から明示的な同意を得ることが必要です。そのような同意を得るには信頼が必須です。信頼がなければ、誰も同意しません。同意がなければ、データは得られません。データがないと、営業やマーケティングキャンペーンが非効率となります。

セキュリティとプライバシーの尊重は、コンプライアンス上の課題になるだけではなく、ビジネスにとって主要な利点にもなります。セキュリティ、プライバシー、およびアイデンティティガバナンスは、企業がユーザーやお客様と深い関係を構築するのに役立ち、ロイヤルティを高め、ビジネス収益を増大させる可能性もあります。

最新の CIAM に関する要件

GDPR やその他のプライバシー法の規定では、個人データを処理する組織には、データを不正アクセスから保護することが求められています。GDPR のもとでは、「適切」で「最新」のセキュリティ対策が効果的にデータを保護していることを示せることが不可欠です。

しかし、「適切なセキュリティ対策」とは何でしょうか。また、どのような証拠が期待されているのでしょうか。GDPR によると、適切なセキュリティ対策とは、「最新性」、実施コスト、適用範囲、状況、処理目的を考慮し、それらを個人の権利や自由に対するリスクや影響と勘案して策定されたバランスのよいセキュリティ対策です。つまり、組織は何が適切でバランスがとれているかを判断する必要があり、そのため業界のベストプラクティスをガイドとして参考にする必要があります。

適切なバランスを判断するための 1 つのツールとして、Data Protection Impact Assessment（データ保護影響評価、DPIA）があります[8]。GDPR の遵守には、データ処理操作の影響の可能性を判断するために、このプロセスが必要になる場合があります。組織が DPIA を実施する際には、以下のようないくつかの点について詳細な文書を作成する必要があります。

- **想定されるデータ処理操作**
- **それらの操作の必要性と比率**
- **操作に関連したデータ漏えいリスクの評価**
- **これらのリスクに対応するために想定されている対策（予防やセキュリティ対策、および個人データを確実に保護するためのメカニズムなど）**

GDPR やその他の規則に対応するためには、リスクベースのデータ保護対策が不可欠です。データセキュリティの義務事項をただ果たせばよいというものではなく、各処理がその対象データの持ち主である個人に及ぼす可能性のあるリスクを完全に分析し理解したうえで、それに基づいて策定することが求められています。

このようなアプローチでは、コスト、システムアーキテクチャ、関連要因を考慮して妥当な対策を柔軟に適用できなければなりません。また、個人データを使用する活動すべての費用効果とリスクを綿密に検証することも必要です。

リスク緩和の効果を示す十分な証拠を適切に示せるかどうかは、関連するプライバシーリスクをどれだけ正確に把握できるか、そしてそのリスクへの対応策として選択する「最新」のデータ管理およびセキュリティ手段の強度をどれだけ理解しているかによって左右されます。

クラウドの利点

このホワイトペーパーで説明しているデジタルアイデンティティのセキュリティの概念、プロセス、テクノロジーを実装しようとする企業は、2 つの基本的な選択肢に直面します。それは、CIAM を社内で開発するか、CIAM に特化したベンダーからエンタープライズグレードのソリューションを購入するかという選択です。

ホワイトペーパー「構築か購入か？カスタマー・アイデンティティ・アクセス管理（CIAM）ガイド」で詳細に分析したように、市販のクラウドベースのソリューションは通常、ほとんどの企業にとって、それぞれの目標、ニーズ、リソースに適した望ましい選択肢です[9]。特に、当初の実装だけでなく、長期的

社内 IT と比較した場合、商用の CIAM ソリューションには、継続的な R&D から SLA の保証に至るまで、いくつかの大きな利点があります。クラウドソリューションは、柔軟な拡張性、マルチリージョンのフェイルオーバーと災害復旧を実現し、さらに、社内チームでは到達できないレベルのセキュリティを提供します。

にソリューションを運用し維持していく労力も考慮すると、なおさら市販のソリューションが有利となります。変わり続けるテクノロジー、消費者、市場、規制に対応する必要があるからです。特に、GDPR などの規制法の最新の条項を遵守するためには、プロフェッショナルグレードのサードパーティソリューションが最も優れています。

商用の CIAM ソリューションには、重要な利点がいくつかあり、社内の IT 部門が独自に構築しようとする場合よりも有利です。サードパーティベンダーを利用すれば、グローバルな可用性や拡張性からサービスレベル契約（SLA）による保証やセキュリティ認定まで、商用の CIAM ソリューションによって大きな能力とリソースを得ることができ、継続的な調査と開発も可能となります。これにより、社内の IT チームはビジネスに重要な他の計画に注力できます。

最新のクラウドの機能を活用したリソースの共有、柔軟な拡張性の提供、セキュリティの確保、マルチリージョンのフェイルオーバーや災害復旧への対応が可能な CIAM ソリューションは、多彩な機能を備えたサービスとしてのアイデンティティ（IDaaS）を提供し、社内開発では実現が困難なレベルのセキュリティを達成できます。同時に、データセンターの設備やハードウェアを所有し運用する必要性もなくなります。

アイデンティティ管理の自社構築は実現可能なように思えるかもしれません。しかし、市場の要件や消費者の期待の変化に対応しながら、ソリューションをサポートし、維持し、進化させるには、かなりの労力や資金、そして長期的な社内リソースと専門知識が必要となります。こうした要件を過小評価するリスクがあるのです。

商用 CIAM ベンダーは、テクノロジー、消費者、市場、規制による変化への対応では有利な立場にいます。なぜなら、提供する商品の競争力、関連性、準拠を維持し、販売できるものにするためには、サービスを進化させざるを得ないからです。それらのベンダーは、1 人のクライアントのためだけではなく多数のクライアントのためにソリューションを開発しているため、ソリューションを社内で構築した場合には獲得できない「規模の経済」によるメリットを実現できます。

ヘルスケアプロバイダーを支援するためにセキュアなアイデンティティ管理ソリューションを導入した世界的な製薬会社

課題

この大手の製薬会社は、世界各地でヘルスケアプロフェッショナル（HCP）、政府、地域団体と協力し、信頼できる低料金のヘルスケアのサポートと拡大に取り組んでいます。しかし、各地域には HCP への商品やサービスの販促に関するコンプライアンス規制が複数あり、市場に迅速に処方薬を提供するという同社の目標に影響を及ぼしていました。同社は、各国の規制へのコンプライアンスを維持しながら、HCP が同社の専門的な Web サイトにシームレスかつ安全にアクセスし、処方薬のプロモーションを活用することができるアイデンティティ管理ソリューションを必要としていました。こうしたニーズに対応するため、同社はエンタープライズグレードの最新の CIAM ソリューションを求めていました。

解決策

同社は Akamai Identity Cloud を選択しました。この製品は、ログインワークフロー、シングルサインオン、認証、パスワード管理、アカウント作成フロー、フィールド検証などの機能があり、同社の専門的な Web サイト向けのセキュアで全面的にブランディングできるアカウント登録ソリューションとして機能します。そのプロファイル管理機能により、プロファイル情報を簡単に編集できるようになりました。また、プロファイルデータの保存機能により、HCP のデータはセキュアで柔軟性の高い統一クラウドデータベースに自動的に収集され保存されます。

Identity Cloud プラットフォームは、同社の以前のソリューションより 9 倍高速です。これにより、さまざまな地域のセキュリティおよびコンプライアンス基準に対応しながら、HCP に世界のどこでも同じように規制医療リソースへのセキュアなアクセス権を付与できるようになりました。HCP はセキュアな Web サイトを通じてオンラインでサンプル薬品を注文できるようになり、これまで数週間かかっていた薬品入手が数日に短縮されました。これにより患者の治療が改善され、生活の質が向上しています。同社の代表者は、薬品サンプルやその他のリソースを提供するために HCP のオフィスを訪問する必要性が減ったため、生産性の向上を実感しています。

さらに、Identity Cloud には同社の既存のマーケティング・テクノロジー・プラットフォームとの統合機能もあるため、世界各地の HCP へのマーケティングをパーソナライズすることもできます。

Akamai Identity Cloud

Identity Cloud は CIAM 向けの Akamai ソリューションです。企業は Identity Cloud プラットフォームにより、お客様が個人アカウントを作成し、Web サイトやモバイルアプリ、IoT ベースのアプリケーションにセキュアにログインできるようにするために必要なものを、すべて得ることができます。Identity Cloud は、企業に安全性の高い顧客プロファイルリポジトリを提供すると同時に、プライバシー遵守のための作業を大幅に減らすことが可能なツールを提供します。これによって企業は、お客様の全体像を把握することができます。

Identity Cloud は、企業がセキュリティおよび規制の要件に対処できるように支援する特定の機能とユーザー体験を提供します。Identity Cloud のプライバシーおよび保護機能には、クライアント登録、ログイン、認証、シングルサインオン、範囲を限定したアクセスによる制御、設定および同意管理など、個人データの収集、管理、保護に必要なさまざまな機能が含まれています。

Identity Cloud を展開することで、企業や組織はエンタープライズグレードのアイデンティティ管理を迅速かつ柔軟な方法で実装できます。クラウドネイティブなアーキテクチャで設計されたこのソリューションは、トラフィックの急増に対応し、何億ものユーザーへの拡張性を提供するとともに、ビジネスクリティカルなアプリケーションのサポートに必要なセキュリティ、パフォーマンス、可用性を提供するために、アプリケーション容量のニーズに合わせてインテリジェントに拡張できます。Akamai Identity Cloud は、すべての地域やアプリケーションにわたってデータセキュリティを利用できるようにすることで、組織が国際的なセキュリティおよびプライバシー規則を遵守し、ブランドへの信頼を築き、クライアントデータを管理し、リスクを緩和できるように設計されています。

結論

データプライバシー規則が増え続けている中で、信頼性の高い強固なデジタルリレーションシップをお客様との間で構築したいと考えている組織にとっては、お客様のアイデンティティのセキュリティとプライバシーを保護することが不可欠です。個人データのセキュリティとプライバシー保護に対する消費者の期待は高まる一方です。データの悪用、漏えい、認証情報の窃盗などのケースが多数公表されている今、エンタープライズが個人データの信頼できる保管者とみなされるためには、高いハードルを超えなければなりません。組織にデータを保存する際、お客様はその組織を信頼して同意します。失ってしまった信頼を取り戻すことはきわめて困難です。

出典

1) European Union Data Protection Rules（EU のデータ保護規則）、https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
2) California Legislative Information（カリフォルニア州議会情報）: AB-375 Privacy、https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375
3) Personal Information Protection and Electronic Documents Act（個人情報保護および電子文書法、PIPEDA）、https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
4) IBM 2019 Cost of a Data Breach Report（IBM 2019 データ漏えいのコストに関するレポート）、https://www.ibm.com/security/data-breach
5) Akamai ホワイトペーパー：GDPR、CCPA、さらなる規制：コンプライアンスとお客様の信頼向上に役立つアイデンティティガバナンス、https://www.akamai.com/jp/ja/multimedia/documents/white-paper/gdpr-ccpa-and-beyond-white-paper.pdf
6) Davis Wright Tremaine：“Copycat CCPA” Bills Introduced in States Across Country（「CCPA を模倣した」法案が全米各州で施行）、https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou
7) ZDNet：Marriott Faces $123 Million GDPR Fine in the UK for Last Year's Data Breach（英国で昨年のデータ漏えいに関して 1 億 2,300 万ドルの罰金が GDPR に基づいて科された Marriott）、https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/
8) Data Protection Impact Assessment（データ保護影響評価、DPIA）：How to Conduct a Data Protection Impact Assessment（データ保護影響評価の実施方法）、https://gdpr.eu/data-protection-impact-assessment-template/
9) Akamai ホワイトペーパー：構築か購入か？カスタマー・アイデンティティ・アクセス管理（CIAM）ガイド、https://www.akamai.com/jp/ja/multimedia/documents/white-paper/build-vs-buy-a-guide-for-customer-identity-and-access-management.pdf

Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、ウェブ／モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日 /24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、www.akamai.com、blogs.akamai.com および Twitter の @Akamai でご紹介しています。全事業所の連絡先情報は、www.akamai.com/locations をご覧ください。公開日：2019 年 11 月。