トピックス

デジタル時代の消費者情報管理

企業のデジタルによる変化はとどまるところがない。しかし、企業は消費者のデータを活用する攻めのマーケティング戦略を進めるだけでなく、不正アクセスや情報漏えいなどのリスクに備えた守りの戦略も忘れてはいけない。本稿では、企業が消費者のデータを適切に管理し、ビジネスに活用するための「アイデンティティ管理」について、必要な要件と実現のポイントを紹介する。

NRIセキュアテクノロジーズ ソリューションビジネス一部
主任セキュリティエンジニア
柏木（かしわぎ） 希美（のぞみ）
専門はIDセキュリティソリューションに関するシステムの企画・開発

求められる消費者情報の管理

企業が消費者と接点を持つチャネルは、実際の店舗や従来型のWebだけでなく、スマートフォンやIoTデバイス（ゲーム機やスマートウォッチ、自動車）など、今後ますます多岐にわたることが予想される。このような状況の中で、企業が他社と差別化し、ブランド価値を高めるためには、デジタル技術を利用して消費者に新たな価値を提供するだけでなく、ユーザーエクスペリエンスについてもすべてのチャネルで一貫して提供するべきである。

また、企業が長期的に消費者との接点を維持・促進していくには、消費者を正しく把握することが求められる。従来の消費者の情報は用途ごと、システムごとに分散し、互いに関連付けられていなかったため、消費者の情報を総合的に把握することが難しかった。しかし企業が管理する情報がすべて電子化され、業務プロセスの自動化・効率化が進みつつある現代において、消費者のユーザーエクスペリエンス向上や、企業のマーケティング活動を効率的に行うためには、分散した消費者のデータ（年齢、住所などの基本的な属性情報や、嗜好（しこう）情報、購買履歴などを含む）を関連付け、一元的に管理する必要がある。加えて、分散していたデータをシステム間でやりとりするには、プライバシーの観点から消費者に同意を得る必要もある。

以上のことから、これまでシステムや用途ごとに実施していたユーザー管理だけでは、企業のニーズを満たすことが難しくなっている。そこでいま消費者の情報を総合的に管理し、アクセスを適切に行えるようにするための総合的な情報管理、つまり「アイデンティティ管理」を実現する技術としてCIAM（Consumer Identity and Access Management）と呼ばれる分野が注目されている。2017年5月、ドイツにてEuropean Identity & Cloud Conference 2017が開催されたが、ここでもCIAMソリューションは大きな話題となり、基調講演を行った同国のクピンガーコール社（アイデンティティ管理やアクセス管理の市場分析を行っている）によると、2020年頃までに市場規模は200億ユーロに達するとの推定が示された。

表1　EIAMとCIAMの要件の比較

大分類	小分類	EIAMの要件	CIAMの要件
機能面	登録	・組織の管理者がユーザーを登録する ・ユーザーの身元を組織が保証することが可能	・ユーザーが自分自身で登録する ・ユーザーの身元を確認する機能が必要
	ログイン	・複数のシステムがある場合、シームレスにログインできるよう、SSO（シングルサインオン）が必要	・ソーシャルメディアのIDでログイン可能であれば、ユーザーの利便性が高まる
	ユーザー管理	・組織の管理者が管理する	・ユーザーが自分自身でユーザー情報を変更・管理する機能が必要
	プライバシー管理	・組織で管理されるため、ユーザーが個別にプライバシー管理を行うケースは少ない	・ユーザー情報の収集・使用方法や組織外への提供などについて、ユーザーがコントロールできる機能が必要
	アクセス統制	・ユーザーの権限に基づくロール管理や上長承認によるアクセス制御などの機能が必要 ・定期的な監査が行われる	・アクセス統制の機能が求められることは少ない
アーキテクチャ要素	UX（ユーザーエクスペリエンス）	・重要度は高くない	・CIAMで最も重視される
	可用性	・組織の営業時間内など、限られた時間にシステムが利用できればよい	・24時間365日、利用可能であることが求められる
	規模	・一般的に数千から数十万人程度	・数百万人以上を想定する必要がある
	性能	・レスポンスが悪くてもある程度許容される	・レスポンスの悪さは許容されない ・季節やキャンペーンなどによっては、同時にアクセスするユーザー数が増えることがあるため、ユーザー数の急激な増加に対応できる必要がある
	相互運用性	・既存のデータストレージやマネジメントツールなどと連携する場合がある	・ソーシャルメディアを含むさまざまなシステムと連携できることが必要 ・ID連携の標準仕様はサポートする必要がある
	マルチデバイスサポート	・業務で利用するデバイスのみ、サポートすればよい	・さまざまなデバイスからのアクセスを考慮し、デバイスに依存しないサポートが必要

CIAMに必要とされるもの

CIAMのIAM（Identity and Access Management）は、ユーザーを認証し、本人に関連するデジタルリソースへのアクセスや利用の範囲を許可し、アクセス履歴や画面遷移など追跡するためのID情報の保持、またIDのライフサイクル管理およびアクセス権の管理などを指す。これを消費者の管理に利用するものが、CIAM（Consumer IAM）である。

従来のIAMソリューションは主に企業内の従業員管理に利用されており、これをEIAM（Enterprise IAM）と呼ぶ。EIAMもCIAMも必要となる主要な機能は、ユーザー情報の登録・検証・管理、ユーザー情報ストレージ、認証、認可である。これらはどちらにも共通する必要な機能であるが、実装の要件は異なる（表1）。

例えば企業の従業員はシステムの使い勝手が悪いことを理由にシステムの利用を中断することはない。しかし消費者向けのサービスでは、どのサービスを利用するかの判断は消費者に委ねられており、登録や認証のプロセスが煩雑だった場合、途中でサービスの利用を中断してしまいかねない。そのため、ソーシャルメディアとの認証連携やSSO（Single Sign On）機能を活用し、プロセスを簡素化する必要がある。また消費者はサービスが常に利用可能であることを期待しており、レスポンスに時間がかかることを許容しない。そのためEIAMと比べ高い可用性および性能が必要となる。反対にCIAMでは、EIAMでよく利用される職務権限に基づいた細かなロール管理や上長承認によるアクセス制御などを含むアクセス統制へのニーズはほとんどない。

CIAM導入のポイント

前述のとおり、消費者向けシステムではユーザビリティの低下は消費者離れに直結する。実際に、米国Janrain社（CIAMソリューションのプロバイダー）によると、ID／パスワードを忘れた際に再設定の手続きを取らずサービスの利用を止めたことのある人は、全体の92％に及ぶ。そのため、CIAMはEIAM

表2　振る舞い分析による不正アクセス検知の例

不正検知に利用可能な属性	不正アクセス疑いの判定条件
端末識別子 （アクセス元端末のOS/ブラウザのバージョン、言語設定など）	・特定端末から大量のログイン試行 ・特定端末から大量のユーザーのログインに成功している ・過去の不正アクセスや他サービスの不正アクセスに使用されたのと同じ端末からのアクセス ・該当ユーザーが通常利用していない端末からのアクセス
IPアドレス	・同一IPアドレスから大量のログイン試行 ・同一IPアドレスから大量のユーザーのログインに成功している ・該当ユーザーが通常利用しないネットワークからのアクセス
地理情報 （IPアドレスから検出できる国／地域情報、あるいは端末GPSなどから取得できる位置情報）	・該当ユーザーが通常は利用しない国/地域からのアクセス ・該当ユーザーの前回アクセス時からの位置の変化で計算される移動速度が異常 （例：東京からアクセスのあった1時間後に東欧からログイン）
ページ遷移／入力操作	・人間では不可能な速度でのフォーム入力やページ遷移（ボットによるアクセスの疑い） ・スパイダリング（情報抽出目的の機械巡回）が疑われる画面遷移
曜日／時間帯	・該当ユーザーが通常は利用しない曜日や時間帯におけるアクセス
取引パターン	・該当ユーザーが通常行わない種別の取引の実施 ・該当ユーザーが通常行う金額の範囲を超える取引の実施 ・取引実行前のメール・電話番号などの属性情報変更（本人通知が行われるのを防ぐ疑い） ・取引実行後の即時退会

よりもユーザビリティを重要視すべきである。一方でセキュリティとプライバシーの問題も重要であり、いかにこれらのバランスを取るかがCIAMソリューション導入の大きなポイントといえる。

一般的にユーザビリティとセキュリティはトレードオフの関係にある。ユーザーは煩雑な認証は避けたいと考えるが、企業は不正アクセス防止のために強固な認証手段を利用したい。この相反した要件を実現するために、ユーザーの振る舞いを分析し、リスク判定することで、ユーザーエクスペリエンスとセキュリティのバランスをコントロールする考え方が注目されている。

振る舞い分析による不正アクセス検知に利用できる代表的な属性情報と、不正アクセスと疑われる振る舞いの条件の例を表2に示す。例えば通常は日本からアクセスしていたユーザーが海外からログインした場合、不正アクセスの疑いがあると判定できる。しかし実際に正当なユーザーが出張などで海外からアクセスしている可能性もあり、ひとつの条件に当てはまっただけで不正アクセスとは断定できない。そこでそれぞれの条件に、あらかじめ「不正疑いスコア」を割り当てておく。より合計スコアが高いほど、不正アクセスの疑いが高いとシステムで判断する。

さらに「不正疑いの合計スコア」だけでなく、アクセスした人が実行しようとしている「トランザクション（業務上の処理）の重要度」も考慮し、ユーザビリティのコントロールに利用すると良い。金銭やポイントなどを扱うトランザクションは最も重要度が高く、住所などの変更は次に重要度が高い。ログインを試みられてもそれが失敗したり、また成功してもニックネームなど機密性の低い情報の閲覧だけで大きな被害はなく、これらは重要度の低いトランザクションと言える。

このように「不正疑いの合計スコア」と「トランザクションごとの重要度」に応じてリスクランクを判定し、リスクランクが高い場合にのみ、追加認証を要求したり、処理を実行不可にしたりするなどの対応をとる。この手法のメリットは、すべての検証はバックエンドで行われるため、ユーザーには何も意識させないという点にある。正当なユーザーのユーザビリティの低下を防ぎつつ、不正アクセスに対するセキュリティ強化が可能である。

制度面での消費者保護も視野に

CIAM導入は単なるユーザー管理やセキュリティ対策にとどまらず、その先にビジネスへの活用がある。デジタルによる市場や消費者の変化が進むにつれて、消費者に関連するアイデンティティデータとマーケティングデータ、営業やサポート活動に利用するデータは爆発的に広がっていく。これらの多くの消費者の情報を一元的に管理することで、クロスセル・アップセルなどの効果的なマーケティングが可能になるだけでなく、製品やサービスの改善計画にも利用できる。またCIAM導入により、登録プロセスが消費者にとって簡単なもの（よいユーザーエクスペリエンスを提供している状態）になれば、登録の離脱率が低減し、より多く消費者と接する機会を得ることが可能となる。つまりユーザーエクスペリエンスは、いまや他社との差別化要因のひとつなのである。

また、消費者保護を目的とした法整備が進んでいることも、CIAM導入を考える上で重要な要素である。近年、欧州で整備が進んでいる、GDPR（General Data Protection Regulation：EU一般データ保護規則）やPSD2（Directive on Payment Services 2：改正EU決済サービス指令）などである。IoTやFinTechなどの技術面の発展と並行して、こうした側面も意識しておく必要がある。

例えばPSD2は決済サービスに関する規制で、2017年中にはEU加盟国内で法制化される見込みである。規制の一例として、決済サービスのログインには二段階認証などの強固な認証を求めている。しかし先に述べた「振る舞い分析」などの機能により、リスクが低いトランザクションと判断できる場合は例外とすることが認められている。つまりCIAM導入により、セキュリティ要件は満たしつつ、ユーザーエクスペリエンスを維持できると考えられているのである。

このように、技術面だけでなく、制度面からも拡大する要件に対応するのは、個々の企業では困難になりつつある。そのため欧州や北米では、これらの要件を満たすものがCIAMソリューションという形で急成長している。

日本でもIoT、FinTechなどを筆頭に新たな技術を用いたデジタルビジネスは今後も拡大し、関連する制度の整備も欧州同様に進むと考えられる。2017年5月には、日本でも個人情報保護法と銀行法が改正され、個人情報利用用途の明確化や銀行にAPI公開の努力義務を課すなど、改革が進んでいる。今後、消費者情報のビジネスへの活用と適切な管理・保護を両立できるアクセスマネジメントシステムを構築することが、各企業には求められる。

しかし大規模なシステムを長期間かけて構築していては、昨今のビジネスのスピード感とは合わない。既存のシステムやソーシャルメディアなどと相互に連携し、対応を進めていくことが必要だろう。ただし、他のシステムと相互に連携する場合、取り扱うデータの種類や構造、ユーザーの認可などの要件が複雑になる。またデジタル化に伴いユーザー登録やサービス利用契約といった手続きを全てオンラインで実施可能とするためには、オンラインでのKYC（Know Your Customer：本人の身元確認）プロセスの構築も重要な要素になると考えられる。今後、中長期的なデジタルビジネス戦略を立案する際には、制度対応も同時に検討し、要件を満たすCIAMソリューションを積極的に採用すべきだろう。■