DX時代に求められるID管理パラダイム

西谷昌紀

CONTENTS

要 約

1　デジタルビジネスとは、①自社のコアとなる価値を②ダイレクトなチャネルを通して③顧客個人に届けること、である。その実現には、まず自社のコアとなる価値の再定義が必要となる。

2　顧客とのダイレクトなコミュニケーションチャネルを確立するためには、自社サービスへの囲い込みを図るのではなく、API公開を通して既存プラットフォーマーのエコシステム内にコア価値を組み込んでいくことが重要である。

3　顧客個人を識別し、関係を築くための基礎となるID管理技術は、認証技術の進歩とプライバシー規制の広がりによって大きな変化の時を迎えている。一度の認証で状態を切り替えるのではなく、認証レベルを継続的に管理する「継続的認証」などの新しいモデルが必要となっている。

4　API公開や認証を含むID管理については、ツールを活用することで比較的容易に現時点でのベストプラクティスを実現できるが、そのためには先の三点について、明確なポリシーの定義付けが前提となる。

Ⅰ デジタルビジネスにおける三つの観点

DX（デジタルトランスフォーメーション）の急速な進展により、企業は、事業をデジタルビジネスに転換することを求められている。デジタルビジネスの旗手として知られるのがNetflixである。市場の破壊者（Disruptor）と呼ばれる同社の成長とともに、レンタルビジネス大手のBlockbuster社は倒産を余儀なくされた。Netflixは今や既存のメディアの強力な競争相手となっている。

デジタルビジネスとは何か、既存ビジネスとは何が異なるのか、さまざまな角度からの分析や解説がなされているが、ここでは以下の三点による定義を用いたい。

DXによるデジタルビジネスの特徴
①自社のコアとなる価値を
②ダイレクトなチャネルを通して
③顧客個人に届ける

デジタルビジネスを成功に導くためには、この三つの観点それぞれに関して、現在のビジネスでの状況からいったん離れ、スクラッチ（最初）から方針を考えることが必要となる。

Ⅱ コア価値の再定義がスタート地点

まず、最も基本となる「①自社のコアとなる価値」について考えたい。デジタルビジネスにおいては、DXによる社会環境の変化の中で、企業は自らが提供する価値とは何かを再定義する必要がしばしば生じる。たとえば、Uberに代表されるシェアリングエコノミーの進展と、自動運転技術の発達により、消費者の自動車に対するかかわり方が「所有」から「利用」に大きく変化している。このような状況の中で、自動車メーカーが自身のコアとなる価値を「高品質な自動車の製造・販売」から「安全に人・モノを移動させること」と捉え直し、MaaS（Mobility as a Service：サービスとしての移動）に参入しようとする動きはこの代表例であろう。

コアとなる価値とは一体何か。時には企業理念や文化に立ち返ることも有効な手段となる。化粧品メーカーが、「自分が美しいと思う姿を実現する」ことをコアの価値として定義するのであれば、物理的な肌から離れ、「ビデオ会議などで外見を自分の望むように変化させるサービス」を提供することも不思議ではない。このように、既存事業から大きく離れた価値を「再発見」することも、デジタルビジネスの特徴だろう。

Ⅲ API公開によってエコシステムの一部に

再定義したコア価値をどのように顧客に届けるか。「②ダイレクトなチャネルを通して」届けるというのがデジタルビジネスにおけるやり方だが、これは必ずしも、顧客とのコミュニケーションチャネルを自社で支配すべきだ、ということを意味しない。

確かに、企業がプラットフォーマーとしてチャネルを支配することが収益につながる、という考え方が広まった時代もあった。自社独自のネットショップ、自社独自のスマート

フォンアプリ、自社独自のSNSなどにより、自社の世界に消費者を囲い込むモデルである。しかし、GAFA（Google、Amazon、Facebook、Appleの米国の4大IT企業）というメガプラットフォーマーの支配力が強まり、プラットフォーム争いは勝敗が決したといえよう。今では、GAFAと通信キャリアやLINE、TikTokのような特定領域におけるチャンピオン企業が、多層的でオープンなエコシステム（複数企業がパートナーシップを組み、共存共栄していく仕組み）を作り上げている。このような現状においては、多くのチャネルから適切なものを選び出し、迅速に利用できるようにすることが重要である。

そのための基盤がAPI（Application Programming Interface：ソフトウエアの機能を一部公開して、外部のソフトウエアと機能を共有すること）である。APIを提供するとはすなわち、コア価値をどのように提供するか、その形式をオープンかつ明確に宣言するものである。APIによって、さまざまなコミュニケーションチャンネルにコア価値を組み込んでいくことができる。また、たとえば人気スマートフォンアプリの開発者が、自分のアプリにサービスを組み込んでくれることもあるだろう。APIを通して、自社のデジタルビジネスがエコシステムの中に組み込まれていくのだ。

Ⅳ データ分析の基盤となる「ID管理」

デジタルビジネス三要素の最後となる「③顧客個人に届ける」。これは、価値を届ける相手を集団（マス）ではなく、個人と捉え、その相手との間で一対一の、いわば「名前で呼び合うような」関係を構築する、ということを意味している。その実現を担う技術がID管理（Identity Management）である。

注意すべきは、ここでいうIDが、ログインIDのようなユーザーを特定するための識別子（Identifier）ではなく、ユーザーの属性や行動履歴といった、ユーザーに帰属するすべてのデータを含む、いわばネット上でのその人自身（Identity）を指す概念であることだ。つまり、ユーザーのデータすべてを管理するID管理は、デジタルビジネスの中核をなすデータ分析（アナリティクス）の基盤でもある。さらに、ID自体に帰属するデータだけでなく、ID作成から削除までのライフサイクル管理、ID登録時のユーザーの本人確認[注]の実現方法、顧客がそのIDの本人であることを証明するプロセスである認証機能を含んで考える。

このID管理においても、技術や社会環境の変化に伴う考え方の変化が起きつつある。先に述べたように、かつて、顧客の情報をなるべく多く収集し、自分の手の内に囲い込むことが価値につながるという風潮があった時代では、ユーザーのログインIDやパスワードも囲い込むべき情報の重要な一つであり、ログイン後のポータル画面を支配することが重視されていた。しかし現在、このような考え方は、OpenIDやOAuthといったID連携（フェデレーション：管理主体の異なるサービス間で識別情報を共通して行えるようにする連携方法）規格の普及と、FacebookやTwitterでのログイン情報を利用するソーシャルログインの流行によってほぼ廃れた。そしてさらに近年、認証とプライバシーという

二つの分野における変化により、ID管理のパラダイムはさらに進化しつつある。

V 多様性をサポートする認証モデルの活用を

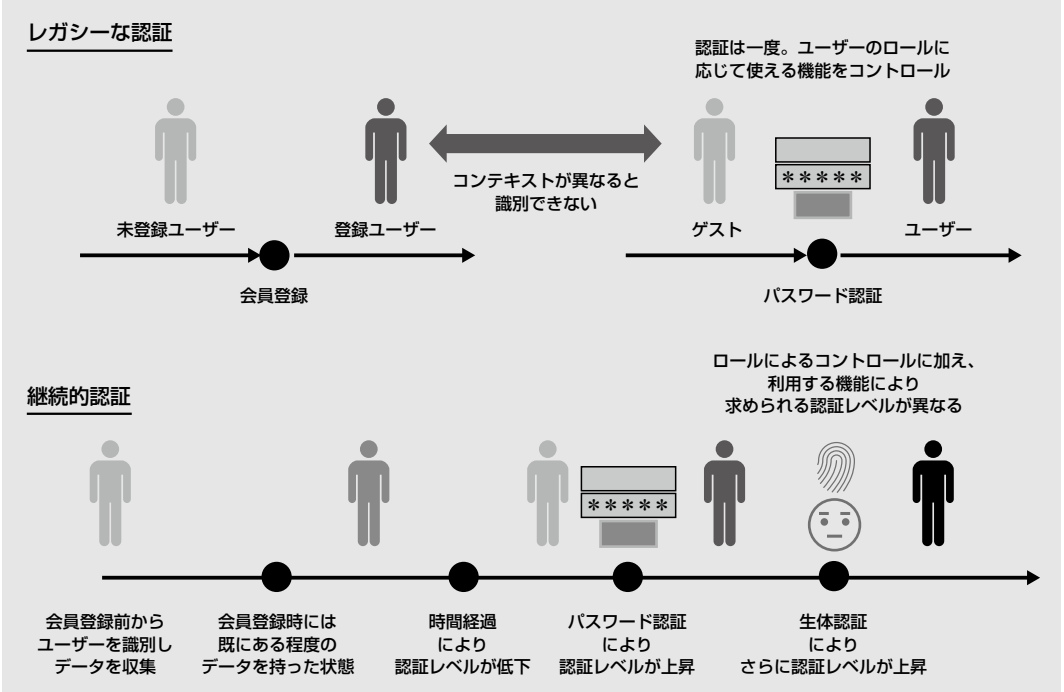
認証分野における変化とは、認証方式の多様化である。スマートフォンの普及により、スマートフォンアプリを利用したワンタイムパスワードによる二段階認証はもはや一般化しつつある。また、指紋認証や顔認証といった生体認証も手軽に利用できるようになり、FIDO（Fast IDentity Online：指紋による生体認証などパスワードに代わる認証方式）による規格化が進んだことにより、今後一層の普及が予想されている。

このように、今やパスワードは、認証手段の唯一どころか最初の選択肢でもなくなりつつあり、さまざまな認証方法を使い分ける、あるいは組み合わせて使うということが当たり前に受け入れられつつある。

また、リスクベース認証とIdentity（ID）Proofingの概念についても、認証方法の多様化という観点から触れておくべきであろう。誤解を恐れず簡単に表現するなら、リスクベース認証とは、ユーザーのアクセス元やアクセス方法に関する情報、行動パターンなどを分析し、本人以外の（不正な）アクセスであるというリスクを数値的に評価する技術である。Identity Proofingは、たとえユーザーが登録や認証を行う前（すなわちアクセスしてきているユーザーに名前がついていない状態）であっても、ユーザーの行動履歴や取引活動の記録を基に、そのユーザーがどんな人物であり、どの程度信用できるかを検証する行為である。

これらの変化に対応して、NRIセキュアテクノロジーズが推奨しているのが、継続的認証（Continuous Authentication）という考え方だ（図）。これまでは、認証状態を「認証

図　レガシーな認証と継続的認証のプロセス



済の特定ユーザー／未認証の誰でもない状態」の二値で管理し、一回の認証プロセスでそれを切り替えていた。継続的認証では、認証プロセスの実行後も、ユーザーの振る舞いを検証し、常に同じユーザーが使い続けているかを検証し続けるとともに、必要に応じて再認証・追加認証を求めることにより、不正アクセスに対抗する。

筆者は、さらにこの継続的認証に、リスクベース認証やID Proofingの考え方を取り入れ、ユーザーがどの程度信頼できるのか、どの程度本人らしいかを継続的に管理し続ける「確率的認証（Quantum Authentication）」を提唱したい（「Quantum」は厳密には「確率的」という意味ではないが、量子状態が固定ではなく確率分布になることから採用した）。

ユーザーの行動、アクセス環境、そして実行した認証プロセスによって、そのユーザーが信頼できる確率を「信頼度」として計算し、その信頼度によって、ユーザーに何ができるのか、サービスとして何を提供するかを判定する。明示的に認証しなくとも、自分のスマートフォンでアクセスするとおすすめ情報が表示される、送金時には生体認証が必要、出張先のホテルからのアクセス時は二段階認証が必要、などはこの確率的認証の考え方に包含できる。

Ⅵ プライバシー意識の高まりがもたらす変化

プライバシーの分野では、プライバシー意識の高まりとGAFAによるデータ支配への懸念から、欧州でGDPR（EU一般データ保護規則）が施行されるなど、顧客のデータを持つことが、リスクにもなり得る、ということが認知されつつある。GDPRをはじめとする各国のレギュレーション（規制・規則）を遵守し、プライバシーを守りながらデータの収集と分析を行うためには、ユーザーとの真摯なコミュニケーションが必要となる。すなわち、収集するデータの内容、利用目的、取り扱い方法を可能な限り詳細かつ分かりやすく提示し、ユーザーの了承を得なくてはならない。

その前提として、当然のことながらユーザーからどのようなデータを集め、何の目的でどんな分析を行うのか、明確に定義できている必要がある。つまり、データ分析に関して、あらかじめある程度の見通しを立てておくことが望ましい。

Ⅶ 明確なポリシーを定めた上でツールの活用を

最新の認証手法やプライバシー保護制度に対応し、かつサイバー攻撃に対抗できる安全なサービスを実現するには、多くの考慮すべきポイントがある。技術や環境の変化が急速な分野でもあるため、その分野に関するノウハウや経験なしに徒手空拳で挑めば大きなコストを覚悟せざるを得ないだろう。

しかし、幸いにして、APIやID管理の分野では、ベストプラクティスというべき標準的な手法が整備されつつある。また、APIを実装するためのAPIゲートウェイや、消費者向けのID管理システムであるCIAM（Consumer Identity and Access Management）など、ベストプラクティスを迅速に実装するための

ツールも登場し、これらの活用により、DXにふさわしい速度でセキュアな仕組みを提供することが可能となる

ただし、これらのツールの利用にあたっても、当然にこれまでに述べたような戦略が前提として必要となる。実効性のあるDXのための最初のステップは、①何を②どのように③誰に提供するのか、を明確化し、必要に応じて再定義するという「当たり前」の作業であることを、あらためて強調しておきたい。

注

金融業においては特にKYC（Know Your Customer）と表現される

著者

西谷昌紀（にしたにまさき）
NRIセキュアテクノロジーズDXセキュリティ事業本部DevSecOps事業部長
専門はID管理・認証技術、ソフトウエア開発プロセスにおけるセキュリティ