アジア太平洋地域における アイデンティティの現状 - 2022年

はじめに

2021年は、インテリジェントな自動化技術によるバックオフィス業務の変革はもちろん、新しい顧客エクスペリエンスの提供に向けて、企業におけるデジタルトランスフォーメーション(DX)への取り組みが大幅に加速した。デジタル成熟度の高い企業は、この業務環境にいち早く適応し、ビジネスのあらゆる場面で「デジタルファースト」のアプローチを採用している。デジタルファーストエコノミーでは、長期に渡り、AI(Artificial Intelligence:人工知能)とパーベイシブコンピューティングで強化されたソフトウェア機能によって、新しい目的、イノベーション、持続可能性が推進されるという認識に基づいている。

2022年末にはアジア太平洋地域の経済活動の半分が、デジタル技術を使うか、あるいはそれから強い影響を受けたものになるとIDCでは予測している。その結果、この地域の企業はデジタル技術を高度に活用し、急速に進化しつつある働き方のニーズ(すなわち、ハイブリッドファースト)に対応することになり、デジタルとリアルの両方のチャネルにまたがって一貫性のある顧客エクスペリエンスを提供し、業務の自動化を進め、インテリジェントエンタープライズへと変化することが期待される。

しかし、ハイブリッドワークモデルへの移行と共に、サイバー攻撃への露出性や関連するリスクが着実に増加しており、アジア太平洋地域の企業においては、セキュリティへの投資がより重視されるようになっている。オンプレミスとクラウド環境の両方を確実に保護する必要性が第一の目標である。脅威が拡大し増殖を続ける環境において、データ、ネットワーク、そしてユーザーをいかに保護するかが、今日の企業が抱える最大の課題である。

地域を超えて広がるデータ関連規制や法律も、セキュリティ導入を促進する重要な要因である。しかし、地域によってばらつきがあり、統一されたな基準が存在しない。オーストラリア、ニュージーランド、シンガポール、さらに香港などの市場では、データプライバシーと侵害通知に関する比較的厳しい法律が施行されているが、その他の地域では、ほとんど制定されていないか、あっても限定的である。昨年、認証および承認プロセスを容易にする共通の基準とフレームワークを使用してアクセス認証を強化するため、フェデレーション方式のアイデンティティおよび特権管理に回帰する動きがIDCの調査で見られたが、この傾向は、これまで長期に渡り調査を継続してきたなかで初めてのことである。このトレンドは2022年も続くと予測される。

アイデンティティ管理の現状

アイデンティティ管理ソリューションは、顧客アイデンティティをより適切に管理するための基盤になっている。2021年にアジア太平洋地域の企業879社を対象にIDCが実施した調査「Asia/Pacific(AP) Security Services Survey」では、アイデンティティセキュリティが最大の焦点であると、調査参加企業の40%以上が回答している。ほとんどの企業がすでに多要素認証など、導入が容易で採用が広がっているテクノロジーを実装しているにもかかわらず、IDCが2021年12月に実施した調査「Future Enterprise Resiliency and Spending(FERS) Wave Survey」では、約80%の企業が、2022年も引き続き、高度な認証／多要素認証への支出を維持するか増額する意向である。

アイデンティティセキュリティが最大の焦点分野だと考えている企業の割合

高度認証への支出を続けると回答した企業の割合

コンテキスト(振るまい)ベースのアクセス制御(例:パスワードに依存しないソリューション)などのテクノロジーと、アナリティクス、AI、MLの組み合せを利用し、ユーザー、デバイス、アプリケーション、インフラストラクチャの不自然な挙動を検知することによって、さらに大きな効果が得られるであろう。アイデンティティガバナンスと特権アクセス管理は、アイデンティティ管理の健全性を維持する上で不可欠と考えられている。

さらにIDCは、企業と従業員、企業と企業、企業と消費者(B2E、B2B、B2C)のすべてのアイデンティティに関連するセグメントにおいて、バイオメトリクス認証(生体認証)技術の採用が進むと予測している。政府、企業、ユーザーにとって、レスポンスの速さ、ユーザー認証、全体的なエクスペリエンスの改善に役立つためである。ただし、パンデミックの中で特に注目され始めたのは、B2Cにおけるアイデンティティ管理であり、2021年の前半期にAPJ全体で31.4%という極めて高い成長率を示した。

デジタルトラストを達成するためには、クラウドベースのアイデンティティ管理が不可欠であるという点については、企業の運営を成功に導く上で重要度が高いことが認識されている。デジタルトラストとは、顧客、パートナー、サプライヤー、社内の関係者から構成される企業のエコシステム全体に渡る信頼性を構築することである。

従って、企業は包括的でセキュアな業務環境を提供するにあたり、ゼロトラストフレームワークの検討を進めている。ゼロトラスト方式では、すべてのユーザー、デバイス、ネットワークのアイデンティティを毎回認証し、アクセスを認可している。ゼロトラスト戦略を構築するにあたって、アイデンティティはセキュリティアーキテクチャ全体のコア(核)と位置づけるべきである。なぜなら、境界線がなくなる一方、ビジネス同士が繋がり合う世界において、アイデンティティはセキュリティ強度を高め、エコシステム全体に渡ってデジタルトラスト構築するからである。

勢いを増すIDaaS:主な要因

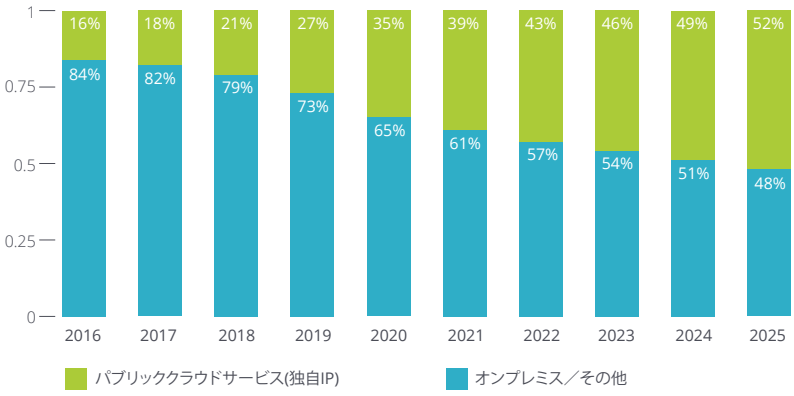
企業がクラウドあるいはモバイルファースト環境に移行するにつれ、業務のオペレーションを簡素にし、統一する必要性が出てきている。データ主権に関する要件、ハイブリッドデータセンター環境における集中型ディレクトリーの必要性、アイデンティティ管理に関するニーズの進化といった課題に対し、次のようなベネフィットを提供するIdentity as a Service(IDaaS)、すなわちクラウドベースの認証モデルの採用の動きが広がっている。

- コスト節約効果、業務効率、専門性を一つにまとめて提供
- アイデンティティソリューションの利用によるリードタイムの短縮
- Security Assertion Markup Language(SAML)、Open Authorisation(OAuth)などのアイデンティティを統一的に扱う規格によって、ユーザーは、一組の認証情報でアクセス可能となる
- すぐに利用できるシングルサインオンおよび多要素認証
- データ主権やプライバシーの関係で増加を続ける諸要件への対応が容易
- ハイブリッドデータセンター環境向けの集中型ディレクトリー

アイデンティティの未来:統一プラットフォームの構築

サービスとしてのセキュリティは、際立った機能性と管理性を提供する最善策であると、今や多くの企業が考えるようになった。アイデンティティおよびデジタルトラストソフトウェアに関するIDCの市場予測では、2025年にはインド、韓国、マレーシア、ニュージーランド、シンガポールなど多くの国で、IDaaSがオンプレミス環境でのソフトウェア利用を上回ると予測される。その理由は、コスト、柔軟性、実装の容易さなどがある。

アイデンティティおよびデジタルトラストソフトウェア市場予測、2020年–2025年



Source: IDC Semiannual Software Tracker, 2021H1 Forecast

IDaaSは、広範囲に及ぶユースケース、リモートアクセス、将来的に有力なクラウドサービスの統合が可能な一つのアイデンティティ管理プラットフォームによって、従来型のポイントソリューションがあまりにも多く存在するという問題の解決策となる。企業が成熟度を増すにつれ、アイデンティティ・アクセス管理ソリューションは、IT運用や他の管理ツールとの統合が進む可能性が高い。MDM、SIEM、自動化など、さまざまなセキュリティモジュールを使用して、より統一された能率的なセキュリティ運用システムを構築できる。そのため、オンプレミスとクラウドの両方を含むエンドツーエンドソリューションを提供するアイデンティティセキュリティプラットフォームを構築および提供できるベンダーが、今後のデジタルエンタープライズの優先的パートナーになると予測される。