「製品を入れれば解決」がID管理で通じないのはなぜか

IBM Security

当たり前のように使っている「ID」と「パスワード」だが、個人を特定する情報を整合性ある形で設計し、どのように管理・運用するかを改めて問い直すべき時期に来ている。

経営のグローバル化や法令順守からも求められるID管理

従来、IDは「システムに付随する要素」「アプリケーションを使うときに必要な要素」として個別に設計され、深く考えることなく何となく払い出されてきた。これまではそれでよかったかもしれないが、徐々にこうした行動が生み出す“ひずみ”が大きくなっている。

“ひずみ”が顕在化するきっかけの一つは、企業経営のグローバル化だ。世界各地の拠点や工場を結び付けたり、パートナーやサプライチェーンにまたがってシステムを共通化したりすることを考えると、途端に話がややこしくなる。例えば新たなコラボレーションツールを採用するとき、あるいはクラウドサービスを導入するとき、どのIDでログインさせればいいのか。あるいは本社側の会計システムに、子会社の課長はどの程度アクセスできるようにすべきなのか……。

経営がグローバル化すれば、それに伴って順守すべき各種法令も増える。欧州連合のGDPR（一般データ保護規則）はその典型だ。GDPRでは、個人データの侵害が発生した場合には、72時間以内に関係当局に報告する義務が課せられる。

日本アイ・ビー・エム（以下、日本IBM）のシニア・マネージング・セキュリティ・コンサルタント、竹内和弘（セキュリティー事業本部アイデンティティ・アンド・アクセス・マネジメント）は「企業全体にまたがるID管理が実現できていない状態では、セキュリティログの相関分析ができず、結局一つ一つ付き合わせる作業が必要になる」と語る。

せっかく最新の製品／サービスを導入しても、個別に「Microsoft Excel」で作った台帳と付き合わせたり、「それは別の人に聞いて」とたらい回しされたりすることになり、想像以上に手間と時間がかかってしまうという。

こうした背景から、改めて企業としてIDをどのように管理し、ガバナンスを効かせていくかを根本的に考え直す時期に来ていると竹内は言う。

日本IBM　**竹内和弘**

パスワードだけに頼る認証の時代は終わりに向かう

竹内は「ユーザーの本人性を確認する『認証』、どのユーザーにどのシステムやアプリケーション、データの利用をいつまで許すのかを定める『ID管理』、そのルールに基づいてアクセスを制御する『アクセス管理』の3つはセキュリティの根幹。人とシステムを結び付けるベースがこの3つだからだ」と言う。

竹内によると、ID管理と密接に結び付いている「認証」の在り方に大きな変化が訪れようとしているという。

これまで数十年にわたって、IDを入力した人間が確かに本人であることを示す「本人性」を確認する手段として最も広く使われてきたのがパスワードだ。それ故にパスワードは、不正ログインやなりすましをもくろむ攻撃者のターゲットになり、常に狙われてきた。

認証という行為の持つ重みを踏まえ、米NIST（National Institute of Standards and Technology：米国国立標準技術研究所）は2017年6月に「電子認証に関するガイドライン」（NIST SP 800-63）を改訂した。この改訂では、実際に漏えいした場合を除いて「パスワードの定期変更を強制すべきではない」と指摘した一文が注目を集めているが「パスワードの強度についての調査もされており、そこにも興味深い内容がある」と竹内は言う。

パスワードの強度を決めるのは「長さ」「複雑性」「ユーザーが扱う数」「更新頻度」という要素だ。複雑性を高めようとしても、人間が作る以上どうしても似たり寄ったりのものになりがちで、あまり効果は望めない。唯一有効なのはパスワード長を長くすることだが、長くしたところで情報を保管している場所（リポジトリ）そのものが不正アクセスされ、情報が使われてしまうと効果がない。

「パスワードだけに頼るのは、もはや良い方法とはいえない。『IDとパスワードによる認証の時代はもう終わり』だとガイドラインは示している」（竹内）。

デジタルネイティブ世代に学ぶ新しい認証

いわゆるブラックマーケットで売買されているIDの数は、世界全体の人口を優に上回る90億個ともいわれている。「漏えいが起こり得ることを前提にしなければいけない中、本人性をパスワードのみで確認する方法はナンセンスだ」と竹内は指摘する。

デジタルネイティブ世代が増えるにつれ、IDとパスワードだけの認証はますます時代からずれていくだろう。代わって注目されるのが、スマートフォンなどのデバイスが搭載している生体（バイオメトリクス）認証やワンタイムパスワードだ。入手しやすく、スマートフォン「iPhone」の「TouchID」などの認証機能がスマートフォンに搭載されたことで自然に使えるようになってきた。こうした新たな認証技術は、パスワードを補う形で広がっていくだろう。

まず「ID」をどう扱うかの整理を

認証の強化によってなりすましを防ぎ、同時にシングルサインオン（SSO）製品などユーザーの負荷を減らす製品を導入することも大事だが、それ以前にまず考えなければいけないことがあると竹内は言う。それはID管理だ。

認証やアクセス制御は、正式に本人であると認められた人に対して、その権限で許される情報に正しくアクセスできるようにする仕組みだ。どのような認証方式が良いか、どのような製品が必要かを考えることも大切だが、その前に「誰に対して、どのような権限でどのアプリケーションやシステム、情報を使わせるのか、それもアプリケーション単位か、データベース単位か、もっと細かく制御するのかといった事柄をきちんと整理しなければいけない」（竹内）。その設計、つまり土台が曖昧なままでは、どれだけ認証を強化したところで意味がなくなってしまう、と竹内は警鐘を鳴らす。

これは、想像以上に大変で手間のかかる作業だ。「アクセス権はこのように与えるべきだ」という統一された基準やガイドラインがあるわけではない。企業ごとに異なる組織形態や業務プロセス、意思決定の在り方などを踏まえ、それぞれの実情に合わせて、時に人事部や総務部、現場の各部門と調整しながらルールを決めていかなければならない。グローバル展開する企業では、ヒアリングや調整は一層大変になる。

身近な例として、働き方改革の流れの中で「リモートワークの従業員にどのような権限を与えるか」「産休・育休や介護休暇を取得している従業員のアクセス権はどうするか」といった事柄一つを考えるだけで、社内からさまざまな意見が出て紛糾する。この実情を考えても、IDの在り方を決める作業が一筋縄ではいかないことは容易に分かるだろう。

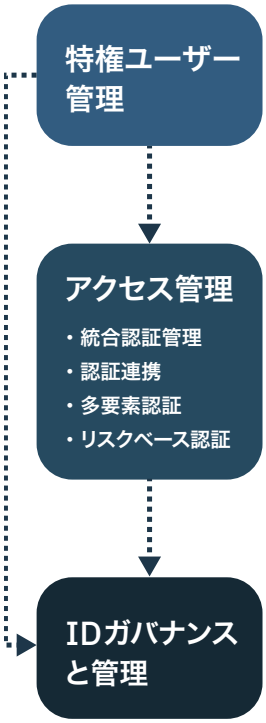
豊富な経験とコンサルティングで支援

長年にわたって認証やSSO、ID管理を支援する製品群を提供してきた日本IBMは、こうした面倒な部分を、欧米で広がり始めている「IDガバナンス」という考え方を取り入れつつ支援しようとしている。

IDガバナンスとは、作成から利用、変更、廃棄に至るまでのライフサイクル全体でIDを考えるとともに「ロール」(役割)と組み合わせ「どのIDがどのように利用されているか、アクセスコントロールの部分も含めて可視化し、一元的に監視し、ルール違反を発見できるようにする仕組みのこと」(竹内)。ITシステムの観点ではなく、ビジネス視点で分かりやすく示すことが大きな違いだ。(図1)

実はIBMも、CISO(最高情報セキュリティ責任者)の下に「アイデンティティー管理ディレクター」という担当者を置き、グローバルのIDガバナンスを実現している。竹内によると「米国の大手企業ではこうした専任の担当者を置き、中規模以下でもCSO(最高セキュリティ責任者)がIAM(IDとアクセス管理の仕組み)を構築、運用するための予算を確保し、IDガバナンスを決めるケースが増えている」といい、そうした先進事例のノウハウも紹介するという。

(図1) IBMが提供するIdentity and Access Management (IAM - IDとアクセス管理の仕組み) 製品一覧



サービス	IBM 製品	IDaaS	エコシステム
・IAMに関する	・IBM Privileged Identity Manager (PIM) ・IBM Secret Server		・CyberArk
✓アセスメント / コンサルティング ✓構想策定支援 ✓アーキテクチャ策定支援	<統合認証管理> ・IBM Security Access Manager (ISAM) <拡張認証機能> ・ISAM with Advanced Access Control (AAC)	IBM Cloud Identity	
✓プロセス構築支援 ✓システム構築支援	・IBM Identity Governance & Intelligence (IGI) ・IBM Security Identity Manager (ISIM)	IBM Cloud Identity Govern	

製品導入だけでは「あるべきIDガバナンス」は実現できない

竹内は「ただ製品を導入しただけでは、IDガバナンスは実現できない」と述べ、現状の洗い出しから社内のルールや標準作り、実装と運用に至るまでの一連の作業を、コンサルティングサービスとID関連の製品群を通じて手助けするという。「どこまでやるかを決めるのは顧客次第だが、ID専門のコンサルティングサービスを通じて一気通貫で支援する」（竹内）

システムやアプリケーションを使う以上、IDは縁を切ろうにも切れない要素だ。しかもこの先、IoT（モノのインターネット）を活用して情報を集約し、業務改善に役立てるといったデジタルトランスフォーメーションに向けた取り組みを考えると、IDが付与される対象は「ヒト」だけでなく「モノ」にも広がっていくことだろう。これまでとは桁違いの数のIDを管理し、ガバナンスを効かせていかなければならない時代を前に「理想像」「あるべき姿」に行き着くすべを、コンサルティング／構想策定から実装まで日本IBMは支援するという。

この冊子は、Tech Targetに2018年7月に掲載されたコンテンツを再構成したものです
http://members.techtarget.itmedia.co.jp/tt/members/1807/25/news01.html