データセキュリティにおける認証・認可技術の変遷と今後の展望

Changes in Authentication and Authorization Technologies in Data Security and Future Prospects

三宅 健，今泉直柔

要 約 デジタル化が進む現代社会では，データセキュリティの重要性が増している．データセキュリティとはデータを「機密性」，「完全性」，「可用性」の観点で保護することであり，これを実現するために様々な技術が存在している．「認証」や「認可」という技術はデータセキュリティの中でも特に「機密性」の確保において中心的な役割を担っている．パスワード認証や多要素認証，SSOといった技術やAIの活用，ITDR，ブロックチェーン，量子コンピューティングといった技術が不正アクセス防止に貢献している．BIPROGYグループは，これらの技術を用いて顧客に最適なセキュリティソリューションを提供している．安全で快適なデジタル生活を送るために，認証・認可技術の基本的な仕組みや重要性を理解し，利用環境や状況によって適切な技術を選択し活用していくことが重要である．

Abstract In today's increasingly digital society, the importance of data security is growing. Data security involves protecting data in terms of "confidentiality," "integrity," and "availability," and various technologies exist to achieve this. "Authentication" and "Authorization" technologies play a central role in data security, especially in ensuring confidentiality. Techniques like password authentication, multi-factor authentication, and single sign-on (SSO), as well as the use of AI, ITDR, blockchain, and quantum computing, contribute to preventing unauthorized access. The BIPROGY Group aims to provide optimal security solutions to customers using these technologies. In order to ensure a safe and comfortable digital life, it is essential to understand the fundamental mechanisms and importance of authentication and authorization technologies, and to select and utilize appropriate technologies based on the usage environment and situation.

1. はじめに

2020年の新型コロナウイルスによるパンデミックをきっかけに，社会のデジタル化が急速に進められ，様々なサービスがデジタル化されたやり取りによって提供される社会が形成されつつある．これは個人情報を含むあらゆる情報が「デジタルデータ」という形で取り扱われることを前提としている．これらの「データ」の重要度によって，求められるセキュリティの強度は変化する．サービスを提供する企業や組織はこれを念頭に適切なセキュリティ設定を行うことが求められている．中でも，「認証」や「認可」といった領域はデータを保護するための一連のセキュリティの出発点として位置づけられており，アクセスするユーザーが誰であり，どのような権限を持っているのかを確認する重要な要素である．

本稿ではこの「認証」や「認可」の仕組みについて，それぞれの特徴や利用方法を紹介したうえで，認証・認可技術の将来的な展望について考察していく．2章ではデータセキュリティおよび認証と認可の概要について説明し，3章ではすでに取り入れられている代表的な技術に

ついて説明する．4章では実際に技術を取り入れる際の注意すべき点とBIPROGYグループの具体的な取り組みについて説明し，5章では今後発展が見込まれる技術について推察する．

2. データセキュリティと認証・認可

本章では，現在の「データセキュリティ」の定義とその重要性，およびデータセキュリティの中で「認証」と「認可」がどこに位置づけられるかについて述べる．

2.1 データセキュリティの動向と重要性

2000年代初頭にインターネットが普及して以降，社会の仕組みのデジタル化は急速に進んできた．特に2020年に発生した新型コロナウイルスによる全世界規模のパンデミックを契機にして，リモートワークや様々なオンラインサービスの拡充，行政のデジタル化の推進など，社会のデジタル化はさらに加速している．日本国内においても，2016年に政府が提唱した「Society 5.0[*1]」や2021年に設立されたデジタル庁によるデジタル社会の推進など，社会のデジタル化に向けた取り組みが進められている．

これらの取り組みの根幹にあるのは，膨大なデータの蓄積と分析および利活用である．この中には，行政で利用するために個人の情報が記録されたデータや，企業がサービス改善のために利用する顧客データおよび業績データなど，厳重に取り扱うべきデータが多く含まれており，データを保護することの重要性は非常に高い．そのため，日本における個人情報保護法やEUにおけるGDPR（一般データ保護規則）[*2]といった個人データを扱うための様々な規則が整備されている．

このように，社会のデジタル化の推進に伴ってデータ量の増加や利用範囲の拡大は加速度的に進行しており，データの適切な保護は現代社会において必須である．

2.2 データセキュリティにおける認証・認可

データセキュリティとは，取り扱うデータを以下の三つの観点で保護する手段である．

- 「機密性」：許可されたものだけが情報にアクセスできること
- 「完全性」：情報が正確であり，改ざんされていないこと
- 「可用性」：必要な時に情報にアクセスできること

データセキュリティを適切に実現するためにはアクセス制御や暗号化，データに関する監査ログの管理，バックアップといった様々な手法がある．その中で，本稿では「機密性」に関連する「認証」および「認可」の技術について説明する．

米国国立標準技術研究所（NIST）[*3]では「認証」および「認可」を以下のように定義している．

- 「認証」（Authentication）：ユーザー，プロセス，またはデバイスの身元を確認すること．多くの場合，システム内のリソースへのアクセスを許可するための前提条件となる．
- 「認可」（Authorization）：ユーザー，プログラム，プロセスに与えられるアクセス権限，またはその権限を与える行為．

これらの定義を踏まえると，「認証」とは「行ったのは誰か」を確認するプロセスであり，「認可」とは「その人は何ができるのか，しても良いのか」を確認するプロセスである．「認証」および「認可」の技術を適切に利用することで，データへのアクセス主体を特定し，アクセス

している状況から適切な範囲の権限を付与できる．認証や認可の分野では様々な技術が存在しており，それらを要件や状況によって適切に組み合わせて利用することで，データを適切に保護することができる．

3. データセキュリティで活用される認証・認可技術

本章では，データセキュリティで活用されている認証および認可の技術について代表的なものを取り上げ，それらの仕組みや特徴について述べる．

3.1 従来活用されてきた認証・認可の技術

本節で取り上げる技術は，既に多くの企業やサービスにおいて利用されており，十分に成熟している．そのため，これらの技術は認証や認可に関係する担当者がイメージしやすく，活用実績も多い．一方で，それぞれの技術に対する攻撃手法や脆弱性に関する情報も確認しやすいため，利用にあたっては十分に注意すべきである．

3.1.1 パスワード認証

多くの人が「認証」というキーワードから連想する技術として「パスワード認証」がある．パスワードは現在も多くのサービスで利用されており，デジタル化が進む現代社会において，パスワードを使わずに生活することは困難である．

パスワードの特徴としては「導入のしやすさ」が挙げられる．パスワードを利用することはサービスの利用者にとって広く一般的なものであるため，利用者が対応するためのハードルが低い．また，パスワードを設定するための特別な道具や環境も不要なため，導入コストも低く，サービス開発において迅速に実装できる．

一方で，パスワードの利用には様々なリスクがある．パスワードの持つリスクについては大きく分けて「漏洩」と「解読」という二つのパターンがある．

「漏洩」するという点では，フィッシングサイトなどによるパスワードの流出に加えて，PCにパスワードを書いたメモを貼っていたところを盗み見られるなど，ユーザー自身の管理方法が要因となることもある．また，パスワードの使いまわしによって，一つのパスワードの漏洩が複数のサービスの認証突破につながってしまうパターンも存在する．

「解読」されるという点では，辞書攻撃やブルートフォース攻撃など様々な手法によってユーザーのパスワードを解読されるリスクが挙げられる．機器性能の向上や AI の発展によって，パスワードが解読されるまでの時間は年々短縮されている．米国のサイバーセキュリティ企業である Home Security Heroes が公表している結果によると，自社開発によるパスワード予測 AI「PassGAN」によって，パスワードが英字（大文字と小文字の両方），数字，記号を全て利用している環境であっても，8 桁のパスワードが約 7 時間という短時間で解読できるとされている．

また，「人間がパスワードを忘れてしまう」というリスクもある．このリスクに対応するために，覚えやすいようにパスワードを使いまわしたり，自身が記憶しやすい単語に紐づけたりしたことによって，他者に「解読」される場合がある．

情報処理推進機構（IPA）[*4] が公開している「情報セキュリティ 10 大脅威 2025[1]」では個人向けの脅威に関して「インターネット上のサービスへの不正ログイン」の項目が 10 年連続で

ランクインしている．こうした現状を踏まえてIPAでは「セキュリティ対策の基本と共通対策[2]」でパスワードの適切な管理方法を公開している．

こうした背景から，認証にパスワードのみを使用することは現代において極めて高いリスクを伴う手法であると言える．

3. 1. 2　多要素認証（MFA（Multi-Factor Authentication））

3. 1. 1項で挙げたようなパスワードのみの認証でのリスクを回避する一つの手段として，多要素認証（以下，MFA）がある．多要素認証とはユーザーの認証を強固にするため複数の要素による認証を要求する方法である．ここでの複数の要素とは，表1に示す3種類に分類される．

表1　多要素認証の各要素

要素	利用できる認証	代表例
知識要素	ユーザーが知っている情報による認証	パスワード，秘密の質問
所持要素	ユーザーが所有している物による認証	SMS，メール OTP，IC カード
生体要素	ユーザーの身体的特徴に紐づく認証	指紋，顔

多要素認証は，これらのうち少なくとも2種類以上の要素の組み合わせによって認証を行うことを前提としており，それぞれの要素の中でもさまざまな認証を利用することができる．中には，Okta[*5]社が提供している「Okta Verify」やMicrosoft社が提供している「MS Authenticator」といった独自のアプリケーションを利用することで，プッシュ認証や生体認証，アプリケーションから取得できるデバイス状態などの様々な条件を複合的に加味した高度な認証手段も存在する．

多要素認証の大きなメリットはセキュリティの向上にある．パスワードにおけるリスクのように，仮にいずれかの要素が漏洩した場合でも，別の要素による認証が要求されるため，不正アクセスを防御できる．また，この追加の認証が要求されたという通知によって，ユーザーが自身のアカウントへの不正アクセスを発見するきっかけにもなる．

一方で，多要素認証はユーザーの利便性とコスト面での課題が存在する．利便性に関する課題としては，複数の要素による認証が求められるため，ユーザーの手間が増えることが挙げられる．また，これを悪用した「多要素認証疲労攻撃」（MFA Fatigue Attack）という攻撃手法も存在している．これは漏洩しているユーザー情報をもとに何度も繰り返しMFAの要求を行うことで，ユーザーの誤操作，あるいは誤認識を誘って認証を突破するという手法である．

コスト面での課題としては，所持要素や生体要素を利用した認証を行うために，生体情報を読み取ることができる機器など，個別に機器を調達しなければならないことが挙げられる．加えて，採用した認証方法がユーザーにとって馴染みがない方法であった場合，適切な教育をしなければならないこともある．

Okta社が提供する「The Secure Sign-in Trends Report[3]」では日本のユーザーのMFA導入率は54%という結果となっており，諸外国と比べても低い水準にある．この結果から，特に日本ではこれまで利用されてこなかった機器や手法を利用すること，あるいはそれらへコストをかけることへの抵抗感が強いことが考察できる．多要素認証を取り入れることの重要性と

ともに，多要素認証のメリット，デメリットを丁寧に説明し，ユーザーが納得して利用できる状況を作り出していかなければならない．

3.1.3　パスワードレス認証

パスワードレス認証は，名前の通りパスワードを利用せずに他の方法で認証を行うプロセスを指す．これによってパスワードに関するリスクを回避すると同時に，ユーザーのパスワードを管理する手間も省くことができる．

手段としては，3.1.2 項の多要素認証の要素として挙げた所持要素，生体要素のそれぞれの手法がある．両方を認証時に確認することで多要素認証を満たすこともできるが，その場合は多要素認証と同様に専用の機器やそれを利用するための教育といったコスト面での課題が発生する．

パスワードレス認証の推進を目的とした業界団体である FIDO アライアンスでは，このパスワードレス認証の標準的な規格である「FIDO」や「パスキー」といった仕様開発を続けており，サインインにかかる時間の短縮や成功率の向上，攻撃頻度の低下などパスワードレス認証による様々なメリットを統計情報と併せて提供している．

3.1.4　Single Sign On（SSO）

Single Sign On（以下，SSO）は 3 章でこれまで挙げてきた認証の手法とは異なり，ユーザーが複数のサービスを利用することを前提に認証頻度を下げることで利便性を向上する仕組みである．関連するシステムが共通の SSO の規格に従うことを前提に，特定のサービスで初めに認証を行った情報を他サービスでも流用することで認証のプロセスをスキップできる．

SSO にはいくつかの方式が存在するが，中でも主流となってきているのは認証プロトコルを利用する方法である．これらは主にインターネット上で通信する Web アプリケーションで利用されており，プロトコルの仕様に従い十分に確認した認証情報（トークン）を利用することで安全に，かつベンダーの独自仕様などに依存しない標準化した方式での SSO を実現できる．

認証頻度の低減以外の SSO のメリットとして，利用するサービス全体での認証強度の統一が挙げられる．SSO のプロセスの中で最初の認証を十分に強力な状態にすることで，各サービスが個別に認証方法を実装できない場合においても，高水準の認証が保証される．

一方で，SSO にはいくつかの大きなリスクが存在する．その一つは，単一障害点になり得ることである．SSO を提供するサービスは複数のサービスでの認証を肩代わりできる状態であるため，仮に SSO を提供するサービスが何らかの理由によって停止してしまった場合，関連するすべてのサービスにアクセスできなくなってしまう．このため，SSO を提供するサービスは可用性を十分に考慮しておくことが必須である．

また，SSO に利用する認証情報が漏洩した場合に，他サービスへの不正アクセスができるようになってしまうというリスクも存在する．このため，SAML のようなプロトコルにおいては，認証プロセスの中で適切に暗号化やデジタル署名による検証を行うなど，認証情報を厳密に取り扱っている．また，各アプリケーションの認証を SSO によってスキップする際には，アクセス時のユーザーの状況や前回認証を行ってからの経過時間によって再度認証を要求するなど，複数の条件を用いて認証頻度を設定し，利便性とセキュリティのバランスを見ながら最適な認証制御を検討すべきである．

次に，SSO を実現するための代表的な認証プロトコルである SAML と OIDC について，また OIDC のベースとなった認可プロトコルである Oauth 2.0 について，その概要を紹介する．

1）Security Assertion Markup Language（SAML）

SAML は主に SSO を実現する際に利用される認証のプロトコルである．XML ベースの情報を利用して，ユーザーの特定やユーザーが持つ属性情報を適切にアプリケーションへ提供できる．また，情報をやり取りする際のプロセスにおいては，暗号化やデジタル署名の仕組みを利用し，データの改ざんや盗聴を防止することが考慮されている．

SAML を利用することで安全な SSO 環境を構成することができるが，その仕様の複雑さや実装難易度の高さから，主に企業の社内システムでの利用が中心となっている．

2）Oauth 2.0 / Open ID Connect（OIDC）

Oauth 2.0 は認可に対するフレームワークを提供するプロトコルである．「スコープ」と呼ばれる情報でアクセスできる範囲を定義し，アクセスしてきた主体が持つトークンの情報から割り当てられたスコープの範囲内での認可を行う．API で情報を取得する際の権限を確認するなど，主に Web アプリケーション同士の認可制御を行うことができる仕組みである．

また，Oauth 2.0 のフレームを流用し，これにユーザーの身元確認プロセスを加えて拡張した認証プロトコルが OIDC である．Oauth 2.0 のフレームを流用しているため，OIDC は SSO の機能を提供するのと同時に，Oauth 2.0 による認可の仕組みを提供できる．また，SAML と比較して，やり取りする情報の構造が JSON をベースとしている点や Restful API との親和性が高いという特徴から，比較的新しい Web アプリケーションやモバイル向けのアプリケーションで利用されている．

3. 1. 5　認可コントロールの仕組み

ユーザーに対するアクセス許可を制御する認可コントロールの仕組みとして代表的なものを三つ取り上げる．これらを適切に組み合わせて設定することで，ユーザーが必要以上にデータにアクセスしてしまうことを防止できる．

1）ロールベースのアクセス制御（RBAC（Role-Based Access Control））

RBAC は組織における役割（ロール）を定義し，それぞれの役割でアクセスできる範囲を設定する制御方法である．例えば「管理者の役割を与えられたユーザーは A アプリケーションにアクセスできる」というような制御を実現する．

この役割は組織の構造や業務内容などに紐づけて定義する．これによって，それぞれの役割に必要最低限のアクセス許可を設定してユーザーに提供し，不正なアクセスを防ぐ．また，ユーザーの組織変更や新規追加などが発生した際にも，それに紐づく役割を管理者が変更するだけで適切なアクセス制御を行える．裏を返せば，RBAC は役割の定義とアクセス範囲の設定が適切に行われていることを前提としている．

2）属性ベースのアクセス制御（ABAC（Attribute-Based Access Control））

ABAC は対象ユーザーやリソース，アクセス環境などの情報に基づいてアクセス制御を行う方法である．例えば「ユーザーの部署が営業であり，役職がマネージャーである場合は B アプリケーションにアクセスできる」というような制御を実現する．

定義する属性によって静的，動的の両方で判断できるため，RBAC と比べて柔軟にアクセスを制御できる．一方で，動的な属性の定義をニーズに応じて確認しなければならないなど，

管理者の負担が大きいという側面を持つ.

3）コンテキストベースのアクセス制御（CBAC（Context-Based Access Control））

CBAC はユーザーの行動やアクセス時間，場所といったコンテキスト（状況）によってアクセス制御を行う方法である．例えば「C アプリケーションにオフィス外からアクセスできるのは特定の時間帯のみとする」というような制御を実現する.

よりリアルタイムに判断できるため，特にセキュリティを重要視するリソースに対するアクセス制御として有用である．一方で，定義の仕方によってはデバイスの制限やネットワーク状態などユーザーがアクセスしている環境全体を考慮した判断基準を検討しなければならないため，システムの複雑さが増す可能性がある.

これらの認可コントロールの仕組みに共通する課題として，定義が複雑になりやすいという点がある．ユーザーが必要以上にアクセス許可を得ることを防ぐためには，組織の構造やアクセス状況に応じて適切な範囲で権限設定を行い，かつそれらを定期的に見直すことが求められる．RBAC，ABAC，CBAC のそれぞれの特徴を生かし，管理負荷とのバランスを考慮しながら適切に権限を設計しなければならない.

3. 2　近年注目を集める認証・認可の技術

本節では，2020 年以降特に注目を集めている認証・認可の技術について記載する．これらの技術は有用性が評価されつつある一方で，運用するにあたってのノウハウなどが成熟しておらず，利用実績もまだ多くない.

3. 2. 1　認証・認可の分野における AI 活用

認証・認可の分野での AI 活用が注目されている．生体認証における精度向上などに利用されているケースもあるが，本項では以下の二つの例を取り上げる.

1）AI によるリスクベース認証

ユーザーの過去のログイン履歴やアクティビティ，ログインを行った際の場所や時間，利用する要素など，過去と現在の様々な情報を AI で分析し，AI によるリスクを評価する方法である．AI により算出されたリスクのスコアに基づいてアクセスを拒否したり，認証強度を変えたりすることができるため，よりリアルタイムな挙動から判断することができる．AI によるリスク評価はユーザーが認証を行うたびに算出され，ユーザーの認証試行回数が増えるほど，リスク評価の精度が向上していく.

基本的にリスク評価のロジックはサービスごとに異なり，また脅威対策の観点から公開されていないことが多い．このため，リスク評価の結果が安定するまで時間がかかる点や，誤検知の可能性がある点などを考慮しておかなければならない．段階的に認証強度を上げるなど，注意しながら運用に組み込むべきである.

2）AI による行動分析

SSO やログ連携などでユーザーの認証行為が一か所で確認できる場合，これらの監視および分析によってユーザーの行動分析を行うことができる．これによって異常な行動パターンを検知し，不正アクセスの兆候を発見し迅速に対処することができる.

特に，3. 1. 4 項で挙げたような SAML や OIDC のように SSO を行う際のセッションが漏洩

してしまうと，一度に複数のサービスに対して不正アクセスできるようになってしまう．AIによる行動分析を活用し，セッション漏洩時に不審な行動を検知することで，このような被害をリアルタイムで防止できる．また，仮に検知された行動がユーザーの正常な操作であった場合においても，不審な行動と誤解されるような操作方法があることを把握できるため，管理者はこれらに対する対策を検討できる．

ただし，これらの行動分析においても誤検知のリスクや，蓄積できるデータ量によっては活用が難しい場合もある．これらの機能を運用に組み込む場合は，長期的に継続して使用することが重要となる．

3. 2. 2　Identity Threat Detection and Response（ITDR）

ITDRとは，ユーザーのアカウントなどのデジタルアイデンティティ情報に関する脅威を検出し，対応する技術のことを指す．3. 2. 1項で挙げたAIによる行動分析やリスク判断もITDRに関連した技術である．ITDRは「アイデンティティに関する侵害は発生する」ことを前提として，迅速な検知と対応を主軸に置く仕組みである．

本稿で述べてきた認証・認可の技術は，それ自体のデメリットや攻撃手法の多様化などによって，侵害されるリスクが常に存在する．より強固なセキュリティを保つためには，リソースへのアクセスの入り口での確認と共に，アクセスした後の挙動についても常に監視するなど，認証・認可のリスクに対応できる環境を作り出すことが重要である．こうした背景から，ITDRへの期待は大きく，MarketsandMarkets[*6]が2024年に発行した市場予測によると，世界のITDRの市場規模は2024年の128億米ドルから2029年には356億米ドルに成長すると予測されている．

4.　認証・認可技術の利活用とBIPROGYグループでの取り組み

本章では3章で触れてきた様々な認証・認可の技術について，実際に活用するにあたってどのような観点や課題があるかについて説明する．また，BIPROGYグループにおける認証・認可技術への取り組みについても併せて説明する．

4. 1　認証・認可技術の利活用

認証・認可技術を実際に運用へ取り入れる際には，サービス提供者である企業や団体が留意すべき重要なポイントがいくつか存在する．加えて，組織自体の環境の制約なども加味して実装を計画し，運用していかなければならない．セキュリティ全般に関わる利活用については「NIST SP800-64 Security Considerations in the System Development Life Cycle」を代表とした様々な文献でまとめられているため，ここでは割愛する．本節では特に「認証」および「認可」の分野に着目して確認すべき点を記載する．

それは，「認証」および「認可」はユーザー操作に直結しており，セキュリティと利便性のバランスがユーザー体験において顕著に表れるという点である．多要素認証は仕組みとしてユーザーに複数の要素による認証を要求するため，セキュリティの強度が向上する一方で，場合によっては2回以上の認証操作が求められるなど，ユーザーにとっての利便性は低減する．さらに，多要素認証を行うための機器の紛失など，サービスの利用や業務遂行が不可能な状況になってしまう可能性もある．認証要素の選定は慎重に行い，ユーザーの教育やサポートも適

切に行わなければならない．このようなユーザーの利便性低減への対策として，パスワードレスや SSO といった利便性向上の技術を取り入れることが検討できる．

ただし，認証対象によってはあえてユーザーに認証操作を求めることで「重要な情報にアクセスしている」意識を促すという考え方もある．認証・認可の技術を導入する際にはその認証対象やユーザーの環境などから慎重に設計を行い，十分な試験期間を用意して，ユーザーへの教育を行いながら導入することが求められる．

4. 2　BIPROGY グループでの取り組み

本節では，BIPROGY グループでの認証・認可技術への取り組みについて紹介する．

企業の DX 推進やクラウドシフトへの支援として，ユニアデックスではゼロトラストの概念をベースとしたセキュリティアーキテクチャとして「CloudPas」を提唱している．図 1 に示すように「CloudPas」では SWG[*7] や CASB[*8]，EDR[*9] といった様々なセキュリティアーキテクチャを複合的に活用することで企業の情報資産を適切に守る解決策を提供する．

認証・認可の分野では IDaaS である Okta を利用している．Okta は本稿で取り上げてきた認証・認可技術を網羅的に提供しており，これらを複合的に組み合わせた「ポリシー」を構成して認証・認可の制御を行う．これにより，企業や組織ごとにそれぞれの環境で，セキュリティと利便性を加味した柔軟な構成を実現することができる．また，Okta はアイデンティティに関連した運用自動化機能（Workflows）を提供しており，これによって管理者の負荷を低減できる．こうした Okta の機能を最大限に活用することで，4. 1 節で挙げたようなセキュリティと利便性のバランスを考慮した最適解の実現を支援する．

さらに，Okta は IDaaS としてクラウドで管理できる ID 管理基盤と認証・認可制御だけでなく，CloudPas の製品である Zscaler や CrowdStrike といった製品との連携も提供している．特に EDR 製品である CrowdStrike との連携により，デバイスの詳細な状態を加味した認証・認可制御を実現することができる．製品単体での機能と併せて，各製品を適切に連携させることでゼロトラストモデルを実現できることが CloudPas の強みである．

また，BIPROGY グループでは企業におけるセキュリティの導入計画や運用における課題を支援するサービス「iSECURE」を提供している．「iSECURE」では顧客の現状を把握しアセ

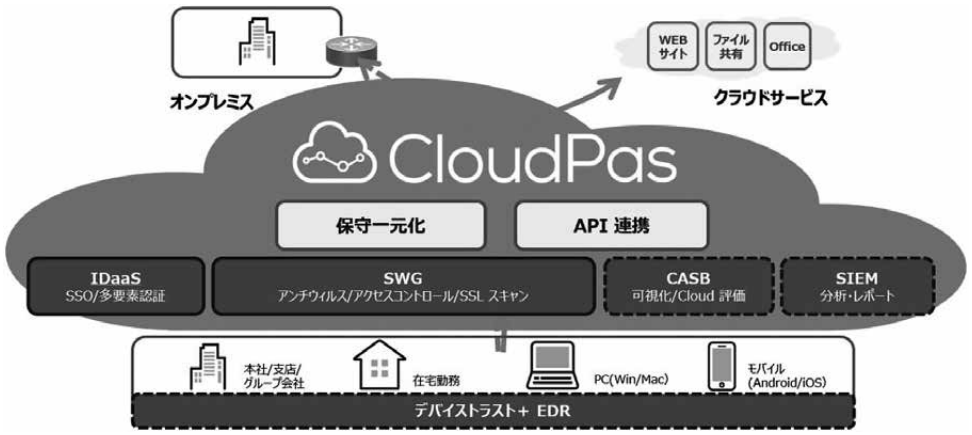

図 1　CloudPas ソリューション構成

スメントを行うといったコンサルティングサービスに加えて，セキュリティサービス導入後の運用監視，インシデント対応といった運用面での支援サービスも提供する．

今後も，BIPROGY グループは時代の変遷とともに多様化する攻撃手法とそれに対抗するセキュリティサービスや技術に追随し，セキュリティと利便性の両方の観点で顧客の環境に合わせた最適解を提供する．

5. 認証・認可技術の今後

本章では，本稿で触れてきた技術や活用方法を踏まえて，認証・認可の技術に関する今後の展望を考察する．

5.1 将来的な活用が見込まれる技術

考察の前に，現時点では活用事例が少ないものの，将来的な活用が見込まれている技術について説明する．

5.1.1 分散型アイデンティティ

分散型アイデンティティは，ブロックチェーンの技術を用いたアイデンティティ情報管理の新しい仕組みである．従来の中央集権型でのアイデンティティ管理と異なり，ユーザー自身が各自の情報を管理し適切な範囲で共有することができる．認証や認可の行為に直接は関連しないが，密接する技術である．

分散型アイデンティティのメリットは二つある．一つは，ブロックチェーン技術によるデータの改ざん防止である．ブロックチェーンの仕組みによりブロック間やシステム全体での相互の監査機構が働くため，データの改ざんが非常に困難となる．もう一つは，攻撃対象を分散できる点である．従来の中央集権型の場合，アイデンティティ情報は一か所にまとめられるため，侵害が発生してしまった場合には集約されるすべてのアイデンティティ情報に影響が及ぶが，分散型アイデンティティではこれを回避することができる．

一方で，分散型アイデンティティには課題点も複数ある．分散型アイデンティティを支えるためのインフラやシステムの整備などの環境面での制約も挙げられるが，特徴的な課題として現代のプライバシー保護関連法案に違反しかねないというリスクが存在する．各国のプライバシーに関する法案上での所有権や管理責任をブロックチェーンによる情報分散した形に合わせていかなければならない．

分散型アイデンティティの普及にはこうした技術的および立法的なハードルが存在しており，現時点で仕組みはそこまで浸透していない．とはいえ，分散型アイデンティティが普及すれば，ユーザーが自身のデジタルアイデンティティを主体的に管理し，異なるサービス間や国境を越えた標準的な仕組みの実現につながる可能性がある．

5.1.2 量子コンピュータと認証

量子コンピュータの台頭により様々な観点で計算技術の飛躍的な向上が確認されている．これらは技術的な発展をもたらす一方で，セキュリティへの攻撃手法の進化にもつながっている．

特に暗号化技術の分野において影響が大きい．現在主流の暗号化技術は「計算の難易度が非常に高い」ということを担保としている仕組みであるため，計算能力が向上した量子コン

ピュータにおいては従来の方法で暗号化した情報は簡単に解読できるからである．量子コンピュータによる暗号解読への対策として，耐量子計算機暗号（PQC）と呼ばれる暗号方式の開発，普及が進んでいる．

もちろん，量子計算の仕組みを応用したセキュリティの技術発展もある．量子暗号通信はその代表例であり，これは量子通信を行う際に利用する「光子」の「第三者の観測によって状態が変化する」特性を利用して，暗号化のための鍵を安全に共有するという仕組みである．こうした量子暗号通信の技術は，個人の情報を利用する認証行為とは切り離せない重要な仕組みになることが予想される．また，量子暗号通信と同様に「光子」の性質を利用した認証要素の開発や，量子ビットと呼ばれる量子コンピュータにおける特性を利用した多要素認証の開発など，量子計算の技術が直接利用された認証技術の研究も進められている．

現在はこうした技術を利用するための機器などが普及していないため，限定された範囲での活用にとどまっているが，将来的にこうした量子コンピュータや量子計算による技術を活用した認証の仕組みが一般化されることも十分にあり得る．

5.2　認証・認可技術の技術的課題と今後

本稿では様々な認証・認可の技術について，それらの特徴や課題を紹介してきた．認証や認可の技術は社会のデジタル化が急速に進む現代において，すべての人が安心して情報やサービスを受けるために必要不可欠な技術である．認証・認可という仕組みは情報を保護するための一連のセキュリティ対策の中で最初の門番とも言える部分であり，これが侵害されることの影響は非常に大きい．

一方で，認証・認可の仕組みはユーザーにとっても意識して触れる機会が多い部分である．パスワードや生体認証といった「ユーザーの確からしさ」を確認するためのアクションはユーザー自身が行う行為であり，この操作の難易度がサービスの利便性に直結する．

すなわち，認証および認可という技術は，より堅牢で，かつより便利であることが常に求められる領域である．あらゆる物事がデジタル化された社会で，ユーザーが意識せずとも安全にそのサービスを享受するために，認証・認可技術の継続的な進化や多様化するセキュリティ攻撃への対策を行っていくことが，現代において世界中が一丸となって取り組むべき活動である．また，技術の発展とともに，それぞれの技術における特徴やメリット，課題点，利用方法を逐次整理し，状況に合わせて適切な活用方法を検討し続けることが，デジタル上でのサービスを提供する企業や団体にとっても必要不可欠である．

認証・認可の技術に対する新たな仕組みを研究，開発する面でも同様のことが言える．日々高度化する攻撃への対処に加えて，ユーザーが安心して利用できる環境を整えることが重要である．このためには，仕組み自体のユーザービリティの向上に加えて，業界全体で標準化した仕組みの開発や継続した啓蒙活動などが有用である．情報技術の分野に精通していないユーザーが運用するためのノウハウを十分に理解して安心して利用できる状況を作り出すことが求められる．

デジタル化が一般化していく社会では，あらゆるサービスを自身のデジタルアイデンティティ情報を適切に守りながら利用しなければならない．すなわち，今後の社会においては，すべての人が認証・認可技術の基本的な仕組みや重要性を理解しておくことが，より安全で快適なデジタル生活を送るための前提条件になる．そのために「認証」「認可」の仕組みや技術動

向を継続して発信し，様々なリスクに備えておくことが，BIPROGY グループを含む IT 業界に携わる人々が共通して取り組むべき課題の一つである．

6. お わ り に

本稿では様々な認証・認可の技術の仕組みについて紹介した．ここで取り上げた技術以外にも，様々な企業，組織において多種多様な認証・認可の仕組みが存在している．それぞれの利用環境や状況などによって，適切な技術を選択し組み合わせて活用することが求められる．各技術の特徴を踏まえた活用を検討するにあたり，本稿がその一助になれば幸いである．

最後に本稿の執筆にあたり，ご支援いただいた皆様に深く感謝し，御礼を申し上げたい．

＊1 Society 5.0：IoT や AI といったテクノロジーを駆使してサイバー空間とフィジカル空間を高度に融合させ，経済発展と社会課題の解決を両立する人間中心の社会モデルの定義．日本政府によって提唱され，2016 年に閣議決定された．

＊2 GDPR（一般データ保護規則）：欧州連合（EU）が 2018 年 5 月 25 日に施行したデータ保護に関する規則．個人のプライバシーを保護し，個人データの取り扱いの権利や透明性を確保することを目的としている．

＊3 米国国立標準技術研究所（NIST）：アメリカ合衆国の連邦政府機関の一つであり，科学技術に関連する標準について研究を行う機関．NIST が発行するサイバーセキュリティに関するガイドラインである SP800 シリーズは日本においても参照されることの多い文書である．

＊4 情報処理推進機構（IPA）：日本の経済産業省で IT 政策実施を目的とした独立行政法人．情報セキュリティに関しても様々な情報を発信している．

＊5 Okta：ID 管理及び認証基盤の機能を有するクラウド型ソリューション，および同製品を提供する企業．2024 年 12 月時点で Gartner が提供する Magic Quadrant for Access Management にて 8 年連続リーダーポジションの認定を受けている．

＊6 MarketsandMarkets：グローバルな市場調査を行う調査出版会社．医療，化学，エネルギー，IT など様々な業界や分野での業界分析や市場予測を行う．

＊7 Secure Web Gateway（SWG）：URL フィルタリングやアプリケーションフィルタリング，アンチウィルスなどの機能によってインターネットへの通信の安全性を確認し，状況によって通信を遮断するなどの処理を行うクラウド型のプロキシソリューション．

＊8 Cloud Access Security Broker（CASB）：ユーザーが利用するクラウドサービスを監視し，意図せずに利用しているサービス（シャドー IT）の検出や利用中のサービスのリスク確認をもとに企業ガバナンスを維持するためのソリューション．

＊9 Endpoint Detection and Response（EDR）：ユーザーが利用している PC やサーバーといった機器（エンドポイント）における実行中の通信やプロセスを監視し，異常や不信な挙動など脅威に対する検知，調査，対応を行うソリューション．

＊10 Identity as a Service（IDaaS）：ID や認証情報をクラウド上に一元的に管理し，SSO などの認証基盤としての機能やアクセス管理の機能を提供するソリューション．

参考文献 ［1］ 情報セキュリティ 10 大脅威 2025，独立行政法人情報処理推進機構，2025 年 1 月，https://www.ipa.go.jp/security/10threats/10threats2025.html

［2］ セキュリティ対策の基本と共通対策 情報セキュリティ 10 大脅威 2025 版，独立行政法人情報処理推進機構，2025 年 2 月，https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kihontokyoutsuu_2025.pdf

［3］ The Secure Sign-in Trends Report，Okta，2023 年，https://www.okta.com/the-secure-sign-in-trends-report/

※ 上記参考文献に含まれる URL のリンク先は，2025 年 7 月 23 日時点での存在を確認．

執筆者紹介

三　宅　　健（Takeshi Miyake）

1999年日本ユニシス(株)入社．2004年ユニアデックス(株)に転籍．ストレージを用いたソリューションの金融系勘定システムへの適用など付加価値あるサービス提供に従事．2022年からクラウドセキュリティ，クラウドストレージのソリューション領域を担当している．

今　泉　直　柔（Naonari Imaizumi）

2017年ユニアデックス(株)入社．仮想化，HCI，ストレージ製品の設計および導入業務を経験後，2022年よりクラウドセキュリティソリューションであるCloudPasのデリバリー業務に従事．現在はIDaaSソリューションであるOktaの設計，導入を中心に担当している．