クラウドサービスの認証連携における課題と解決方法

Problems and Solutions for Federated Cloud Service

小 倉 俊 弘，新 原 英 樹

要 約 クラウドの普及は企業のICT環境や情報資産を「内」から「外」へとシフトさせている．また，働き方改革によるAny Device Anywhereの波はスマートフォンやタブレットをはじめとしたICT端末のビジネス利用を急速に拡大させた．これからは，時代の要求として，「内側」と「外側」という従来型のネットワーク境界防御からアイデンティティによる境界防御という新たなセキュリティモデルへとシフトする．

そのキーソリューションとなるのがID管理をクラウドサービスとして提供するIDaaS（Identity as a Service）である．これまでのActive DirectoryやLDAPをはじめとした企業内のID管理基盤では，頻繁に増加するクラウドの認証に対応することが難しい．IDaaSはクラウド・社内外を問わず共通のアクセスポリシーでシングルサインオンを可能にするハイブリッド統合認証基盤を実現することができる．さらにIDaaSはクラウドファーストの時代で求められる，利用者の利便性向上と企業ガバナンス強化の双方を満たすことができる．

Abstract The spread of the cloud is shifting the ICT environment and information assets of companies from “inside” to “outside”. In addition, the trend of Any Device Anywhere due to work style reform has rapidly expanded the business use of ICT terminals such as smartphones and tablets. From now on, as the demands of the times, we will shift from the conventional network boundary defense of “inside” and “outside” to a new security model of boundary defense by identity.

The key solution is IDaaS (Identity as a Service), which provides ID management as a cloud service. It is difficult for the existing ID management infrastructure in a company such as Active Directory and LDAP to support the frequently increasing cloud authentication. IDaaS can realize a hybrid integrated authentication platform that enables single sign-on with a common access policy regardless of cloud or in-house. Furthermore, IDaaS makes it possible to satisfy both the improvement of user convenience and the strengthening of corporate governance required in the cloud-first era.

1. はじめに

企業のクラウド利用は飛躍的に増加している．また，スマートフォンのビジネス利用が当たり前の時代となったことは，企業が従業員やパートナーに対して，デバイス/場所/ネットワーク環境に依存することなくセキュリティが担保された安全なアクセス環境を実現しなければならないことを意味している．情報資産やITリソースが企業の「外側」と「内側」に存在する環境になったことにより，「外側」と「内側」をファイアウォールで区別する従来型の企業ネットワークではセキュリティを担保することができない状態となった．

働き方改革によるAny Device Anywhereの波や2020年の新型コロナウイルス（COVID-19）パンデミックによるテレワークの増加は従来型の企業ネットワーク構成をますます淘汰していくだろう．企業内部と外部のセキュリティ境界線が曖昧になりつつある状況において安全なセ

キュリティ環境を実現するために，従来型のセキュリティ概念からアイデンティティ（ID）によるアクセス制御が新たな境界線となる時代が到来しつつある．

本稿では，ID 管理をクラウドサービスとして提供する IDaaS（Identity as a Service）製品の有効性，適用時の課題について述べ，マーケットリーダー「Okta」の機能，適用事例を紹介する．2 章と 3 章でクラウドサービスのセキュリティと認証基盤の課題を挙げ，4 章で求められる認証基盤，5 章で IDaaS 製品の概要を述べる．6 章で Okta を紹介し，7 章で導入事例を挙げる．

Okta を利用した次世代型のセキュリティ境界線を構築することで，企業の情報資産，IT リソースに対して安全なアクセス環境を実現することができる．

2. クラウドサービスの普及に伴うセキュリティの課題

企業におけるクラウドサービスの利活用が当たり前の時代になりつつある．総務省の「情報通信白書令和元年版[1]」によると，2018 年の調査時点でクラウドサービスを一部でも利用している企業の割合は 58.7％となっており，2014 年時点の 38.7％からわずか 4 年で 20％増加している．政府においても，2018 年 6 月に「クラウド・バイ・デフォルト原則[*1][2]」を発表した．政府系情報システムの構築や行政サービスはクラウド利用を第一候補とするクラウド・バイ・デフォルトの原則に加え，デジタル技術・デジタル情報と社会を高度に融合させた未来のあるべき日本社会として提唱された「Society 5.0[*2][3][4]」は，企業だけでなく社会全体のクラウド利用をますます促進させることになるだろう．このような環境においては，企業の情報資産，IT リソースは「外側」と「内側」に存在し，あらゆるデバイス・あらゆる場所からアクセスされる状況になっている．そのため，従来の「外側」と「内側」の境界線で守るというセキュリティ対策の有効性は損なわれ，新たなセキュリティの概念を念頭に置いた対策が望まれる．

その新たな概念とは「ゼロトラストネットワーク」である．2009 年に Forrester Research, Inc. により提唱されたもので，「全て信頼できない（ゼロトラスト）ことを前提として，全てのデバイスのトラフィックの検査やログの取得を行う」という概念であり，「信頼された」内部ネットワークと「信頼されていない」外部ネットワーク，というネットワークの境界線の概念を捨てるべく生まれたセキュリティ対策の考え方である．クラウドシフトにより「外側」と「内側」に IT リソースが存在する環境となりつつある今日の状況においては，従来型の「ネットワーク境界防御モデル」では万全なセキュリティ維持が困難になっている．従来型のネットワークの境界線に代わる概念が，企業ネットワークと情報資産へのアクセス権を持つアイデンティティの管理と制御を柱とした「アイデンティティによる境界線」という新たなセキュリティの考え方である．

3. クラウドサービスの普及に伴う認証基盤の課題

SalesForce，Office365，Box などのクラウドサービスの普及，ICT 端末の活用やテレワークによる労働環境の多様化によって，社内システムや情報資産は境界外部へと広がっている．クラウド上の情報資産やリソースは不特定多数の人とデバイスと場所からアクセス可能なインターネット上にあるため，そのセキュリティは適切な人と適切な権限を根拠としたアクセス制御をアイデンティティ認証により実現することが現時点で最も有効な方法となっている．このような考え方から，ゼロトラストネットワークにおけるセキュリティ対策として認証によるア

クセス制御が次世代のセキュリティ境界防御に位置づけられた.「外側」と「内側」の区別が希薄になった企業の ICT 環境では，アイデンティティ認証によるアクセス制御が「企業のリソース・ユーザー」を区分する境界となる.

しかし，認証によるクラウド利用を制御する上で大きな問題がある．それは利用するクラウドが増えるたびに，IT 担当者/利用者の双方で管理すべき ID/パスワード情報が増えてしまうことである．単一のクラウド利用であれば大きな問題にはならないが，日々新しいクラウドが誕生している現代においては利用するクラウドも増えていく．ID 管理の煩雑さはクラウドそのものの利便性を低下させる．また，クラウド毎に ID 作成を行うことで運用コストの増大を，クラウド毎に権限設定・認証ポリシーが異なることでガバナンスの低下を招く．これまでは企業内に設置された Active Directory（AD）や LDAP をはじめとした従来型の認証基盤だけで完結していたが，今後は境界外部のクラウドサービスの認証も考慮しなければならない.

4. ゼロトラストネットワークに求められる認証基盤

前章の課題を解決する方法に IDaaS がある．IDaaS とは Identity as a Service の略称で，アイデンティティ（Identity）の管理機能と認証機能を SaaS（Software as a Service）や IaaS（Infrastructure as a Service）などと同じくクラウドで提供するサービスである．AD や LDAP などの従来型のオンプレミスで実現していた ID 管理システムの機能をクラウドで提供する SaaS と位置付けることができる．IDaaS は従来のオンプレミス型にはない以下の三つの特徴を持つ.

1) クラウドアプリケーションへのシングルサインオン環境を容易に実現

従来の認証システムは企業の情報システム部門が社内ネットワーク内のみに限定した認証基盤を構築し業務システムや人事 DB へのシングルサインオンを実現させていた．しかし，Office365 や Box などのクラウドサービスへのログインは，各クラウドサービスへの認証を要するため，従来型の社内認証基盤ではシングルサインオン環境を実現することは難しい[*3]. IDaaS の場合，事前に統合された数多くのクラウドとのコネクタが用意されており，短期間かつ容易に各クラウドへのシングルサインオン環境を実現することができる.

2) クラウドアプリケーションとオンプレミスアプリケーションに対するハイブリッドな統合認証基盤

IDaaS を利用すれば，増え続けるクラウドサービスに対して IT 担当者・従業員は複数の ID/パスワードの管理から解放される．また，自社独自の ERP や勤怠管理などのアプリケーションも IDaaS に登録することで，社内アプリケーションに対するシングルサインオンも可能となる．更に IDaaS は世界中からアクセスできるため，オンプレミスの AD/LDAP を使用しているグループ企業や，グローバルでバラバラだった認証基盤を容易に統合でき，異なる組織間でも ID を集中管理することでガバナンスを向上させることができる[*4].

3) スマートフォンやタブレットとの親和性

IDaaS は認証基盤の機能に加え，条件に応じたアクセス制限や多要素認証の機能を追加することができる．これにより，社内からのアクセスでは ID/パスワード認証を，社外からの

アクセスはパスワードにもうひとつの認証要素を加えることで本人認証を強化することができる．例えば，スマートフォンにインストールした認証アプリケーションをタップするとIDaaSにリダイレクトし，ID/パスワードに加えコードの入力やiPhoneのTouchIDまたはFaceIDの生体認証を要求する，などである．

このような特徴から，IDaaSは，増え続けるクラウドアプリケーションへの対応，働き方改革への対応，グループ，グローバル，M&Aへの対応，という時代の要求にマッチした統合認証基盤なのである．

5. IDaaS製品の構成と機能

本章では，IDaaS製品の主要な構成要素である認証連携と，IDaaS製品選定のポイントについて説明する．

5. 1 IDaaS製品の認証連携

IDaaSとクラウド/企業内アプリケーションとの認証連携は，SAMLという規格に沿って実装されるのが主流となっている．SAMLについて以下に説明する．

複数のウェブサイトやクラウドサービスを利用する際に，別システムで認証されているため再度認証画面を表示しないで連携する仕組みが「フェデレーション（認証連携）」である．フェデレーションにより複数のサービスで認証情報を共有することで，一度のユーザー認証で複数のサービスを利用することができる．

それぞれ個別に認証機能を持つクラウドやサイト間のフェデレーションでは，認証情報を交換し信用することにより，連携した別サイトにアクセスする際にも認証される．ユーザーID，パスワードや属性情報などのユーザーの認証情報（アサーション）を登録し管理しているサイト（IDP：Identity Provider）とサービスを提供するサイト（SP：Service Provider）間で信頼関係を締結する．ユーザーがIDPにログインすると，IDPがSPにそのユーザーが認証済みであることを伝達する．SPはそれを受け，ユーザーのログインを許可する．これによりユーザーはSPへのログイン時にIDやパスワードの入力を省ける．また，IDPがSPに伝達する際に，パスワードなど重要なユーザー認証情報がネットワーク上に流れることはない（図1）．

この仕組みを実現しているのが「SAML」である．SAMLはシングルサインオンやフェデレーションを実現する仕組みのひとつであり，標準化団体のOASIS（Organization for the Advancement of Structured Information Standards）によって策定された[5]*5．

SAMLを使うことで，異なるクラウドサービス同士，異なるインターネットドメイン間であっても，ユーザーID，パスワードや属性情報などのユーザーの認証情報（アサーション）をやりとりすることができる．利用するシステムがSAMLに対応していれば，シングルサインオンやフェデレーションを実現できることからシステムを横断的に利用できる．例えば，社内システムとクラウドとの間でSAMLを利用すれば，社内システムにログインするだけで，クラウドにもアクセスできる．

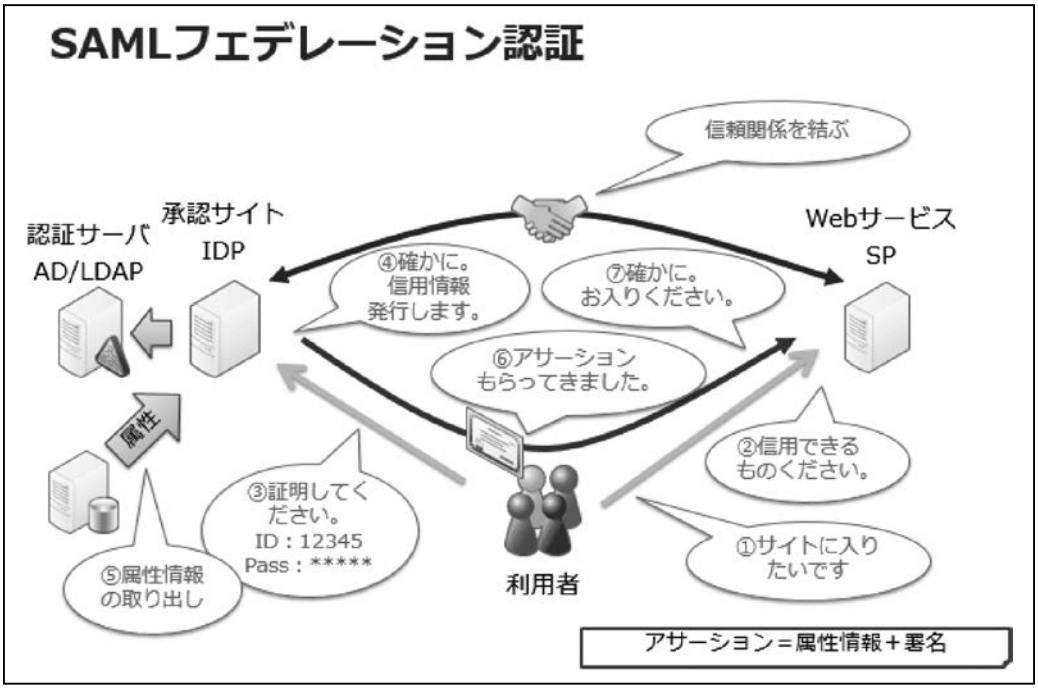

図 1　SAML フェデレーションの仕組み

5. 2　製品選定のポイント

ゼロトラストベースネットワーク，セキュリティの境界は認証，という新しいセキュリティ概念におけるキーソリューションとなる次期認証基盤は，課題に対し図 2 に示す対策が講じられたものでなければならない．そのための要件を表 1 に挙げる．この次期認証基盤を具体化したものが IDaaS による統合認証基盤である（図 3）．

IDaaS を活用し，ID 管理をクラウドへと移行することで，IT 担当者は利用しているクラウドサービスのユーザー ID を統合管理できるようになる．一方で，ユーザーは一組の ID とパスワードを憶えておくだけで，複数のサービスへシングルサインオンができるようになり，クラウド利用の利便性が飛躍的に高まる．また社内で使用している AD と連携することで，オンプレミスとクラウドを統合したハイブリッドな認証基盤も実現できる．これによりユーザー ID の管理を 1 カ所で集中的に行えるようになり IT 担当者の負担は大幅に軽減する．

また，インターネットに接続できれば，社内ネットワークへアクセスすることなく企業ポリシーに沿った認証を実現できる．例えば，IDaaS でユーザー情報ディレクトリの一元管理を行うことでユーザー ID の管理がより容易となるため，休眠アカウントの不正利用等を回避できるようになる．特定端末での利用のみを許可する，特定の場所からのみアクセスを許可する，といったアクセス制御機能や多要素認証機能（MFA：Multi-Factor Authentication）を提供するものもあり，これらの機能を活用すれば，社内ポリシーに合わせたきめ細かい利用制限をかけることも容易となる．

このようなメリットを最大限に活かすには，十分な機能を持ち，幅広いクラウドサービスに対応した IDaaS を選択することが重要である．

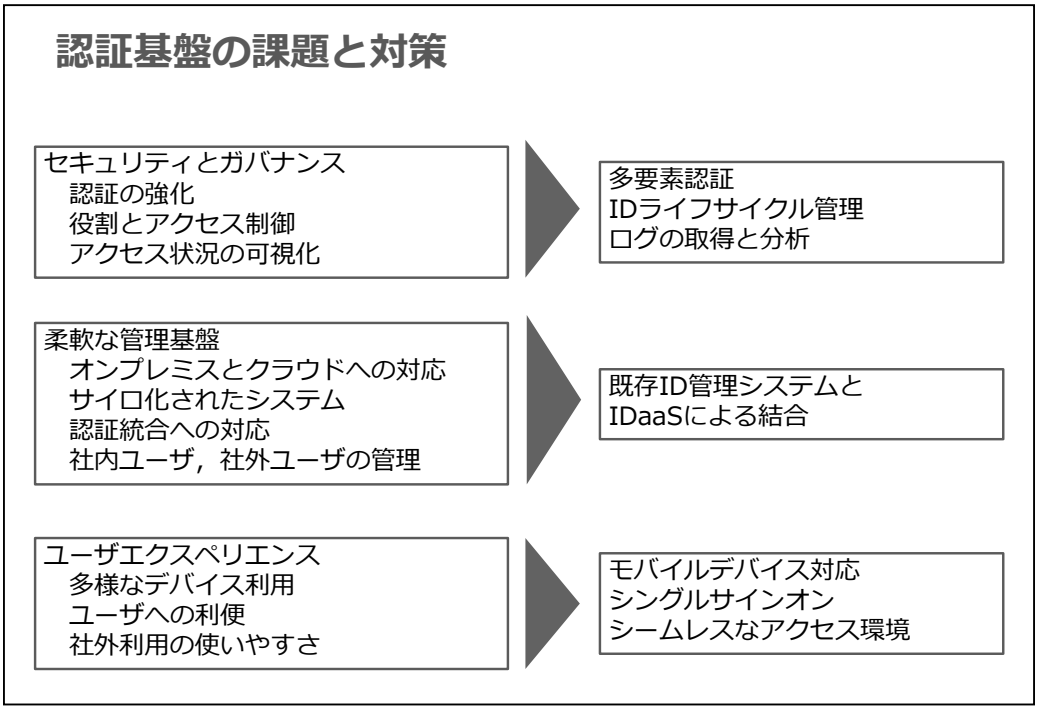

図 2　認証基盤の課題（左）と対策（右）

表 1　次期認証基盤の要件

要件	要素	既存認証基盤	次期認証基盤
ユーザ情報 グループ情報	人事データをベースに属性情報生成し格納する場所を提供する	データベースやAD，LDAPサーバで管理	**クラウド化と既存のハイブリッド**
パスワード	生成ポリシー，期限を管理し、変更後配信する	ADやLDAPサーバ 各アプリケーションが保持している	**一箇所に集約し，アプリケーションにパスワードを渡さない**
認証	パスワード照合	パスワード照合	**SAMLやOIDCによるフェデレーション**
シングルサインオン	パスワードの入力を１回にする仕組み	統合Windows認証やリバースプロキシー、代行入力型がある	**SAMLやOIDCによるフェデレーション**
多要素認証	記憶、持ち物，生体の要素を２つ以上組み合わせる．情報の価値やリスクの高さで必要性を判断する	社外からのアクセスや機密情報へのアクセス時にワンタイムパスワードやICカード，生体認証，デバイス証明書が利用される	**一つのシステムで集約できることが望ましい。ユーザやアプリケーション，接続元などの条件で必要に応じて追加認証を求める．**
アクセス制御	ユーザが利用できるリソースを制御する．	ADによるファイルサーバ利用制限．アプリ側でグループ情報ロール情報を持ち利用可能なメニューを表示する．	**認証のタイミングでソースIPやデバイス種別で利用できるアプリを制限する．また認証時にグループ情報を引き渡しアプリ側で表示メニューを変更する**
社外、グループ企業	グループ全社で一つのクラウドサービスを利用したいが認証基盤がバラバラで集約困難	AD統合を目指すが，制約が多く難しく，断念している	**フェデレーションによる認証により統合しなくても，各社の認証基盤を利用して連携が可能**
デバイス管理	OS設定，アプリの制限を行う	WindowsはADのグループポリシー，モバイルはMDMで対応	**EMMによりWindows10，MacOS，iOS，Androidが管理できるようになり，アプリ配信やデバイス利用制限が可能に**

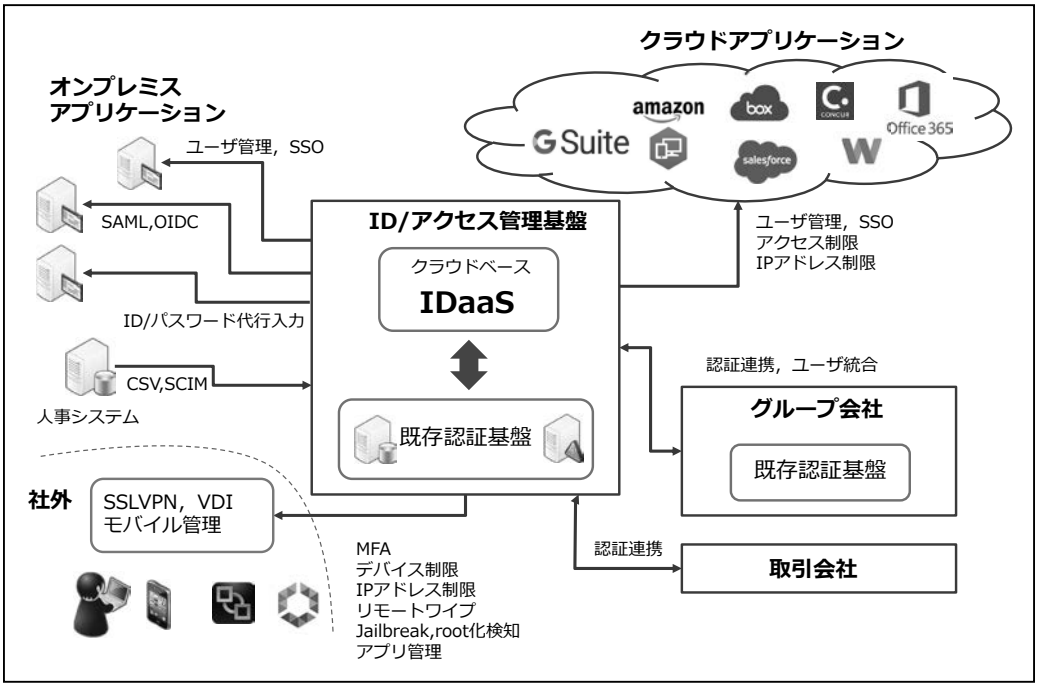

図 3　次期認証基盤のイメージ

6.　Okta について

ユニアデックス株式会社（以降，ユニアデックス）では，IDaaS 製品のマーケットリーダーである Okta についての技術検証や顧客導入に取り組んできた．本章では Okta を選択した背景，Okta のアーキテクチャー，実現機能について説明する．

6. 1　Okta を選択した背景

本節ではユニアデックスが IDaaS 製品として Okta を選択した理由となる背景を説明する．Okta, Inc. は 2009 年に設立され，2017 年 4 月に Nasdaq に上場した．2020 年時点で，20th Century Fox，JetBlue，Nordstrom，Slack，Teach for America，Twilio をはじめとする 8,400 以上の企業が Okta を導入しており，日本企業へも 50 社以上の導入実績がある．また，Gartner[6]，Forrester Research, Inc.[7]のアナリストレポートにおいて，IDaaS 市場における「リーダー」ポジションを獲得している唯一のベンダーである．

2019 年 1 月，Okta の CEO は，同社の登録ユーザーが 1 億人を超えたと発表した[8]．このように，Okta は IDaaS 業界において導入実績，市場評価ともに No.1 となっている．第三者機関によるセキュリティ評価においても，ISO 27001，ISO 27018，SOC 2，CSA STAR，FedRAMP，HIPAA などを取得しており，グローバル最高水準のセキュリティ基準をクリアしている．

6. 2　Okta のアーキテクチャー

Okta のサービスは 100％クラウドで提供されており，そのプラットフォームは Amazon Web Services（以下 AWS）に構築されている[9]．全てのシステムを AWS 上に構築すること

により，Okta はスケーラブルで可用性の高いオンデマンドなサービスを提供している．アメリカ大陸の東西のデータセンターにおいて 3 重化のシステムを運用しており，ヨーロッパ東西にもアメリカと同じ高可用性で構築されたシステムが存在している．2019 年 5 月には日本を含む APAC 域内向けとしてオーストラリアのシドニーのデータセンターでシステム運用が開始された．また，APAC 域内におけるディザスターリカバリー対策として，シンガポールに災害復旧用のシステムを構築している．それぞれのリージョン内の顧客データはそれぞれの域内のみで保全されており，他リージョンのデータセンターへレプリケーションやバックアップされることはない．

Okta のテナントは全てのユーザーが同じ基本環境を共有するマルチテナントモデルとなっている．そのシステムは，プロキシロードバランサーを含むフロントエンド層，ファイアウォールやソフトウェアが主に実行されるアプリケーション層，そしてデータベース層の 3 階層で構成されている．その全ての要素が複数の地理的に離れたデータセンターに跨って AWS 上で実行されることにより，大規模で高スループット，かつ高可用性を実現するように設計されている（図 4）．

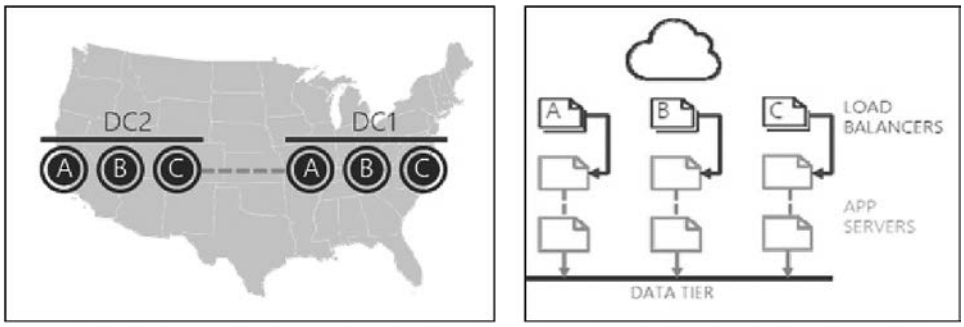

図 4　Okta のアーキテクチャー

この高可用性により，Okta は 99.99％のサービスレベルアグリーメント（SLA）を保証しており，計画停止やメンテナンス停止のないアーキテクチャーを実現している．なお，Okta の稼働状況は Web ページ（https://trust.okta.com/）でリアルタイムに確認することができる．

また，セキュリティ対策として，Okta は保存されているデータとネットワーク上のデータを保護するための堅牢な暗号化機能を提供している．暗号化以外にも，DDoS 攻撃，クロスサイトスクリプティング，SQL インジェクションなどのアタックへの対策，そして第三者のセキュリティ調査会社による脆弱性評価と BugCrowd（重大なバグを見つけると報酬が得られる）を利用するなど，数多くの対策を行うことで強固なセキュリティ基盤を実現しており，これまで情報漏洩などのセキュリティインシデント発生の事例はない．

6. 3　Okta でできること

Okta は認証における様々な機能を提供しているが，セキュリティとコンプライアンスの強化，およびビジネスの効率化という観点で大別すると，以下三つの機能的な特徴がある．本節の各項で説明する．

1）柔軟なシングルサインオン

2）企業間連携
3）強力な本人認証機能

6. 3. 1.　柔軟なシングルサインオン

・クラウドも社内もシングルサインオン

一度の認証で様々なサービスへのログインができるシングルサインオン機能は，ユーザーのサービス利便性の向上とともに，ID・パスワードの使いまわしによる情報漏洩のリスクを抑えることができる．Okta には 2020 年 6 月時点で業界トップの 6,500 以上のクラウド，オンプレミス，モバイルのアプリケーションへのシングルサインオン用コネクタが予め用意されており，簡易な設定で SAML/OIDC などによるシングルサインオンが実現できる．

また，Okta のカスタムアプリケーションである「Okta Active Directory Agent」をオンプレミスに配置すれば社内 AD との連携も可能となり，社内から Okta テナントへのアウトバウンド通信のみでユーザー情報の同期やパスワード認証ができる．この機能により，Okta Active Directory Agent を経由して AD からアカウント情報を取得，パスワードを照合，Okta から AD へのプロビジョニング（ID 同期：自動的に他のシステムやサービスで ID の整合性を取るよう管理する機能）を実現する（図 5）．

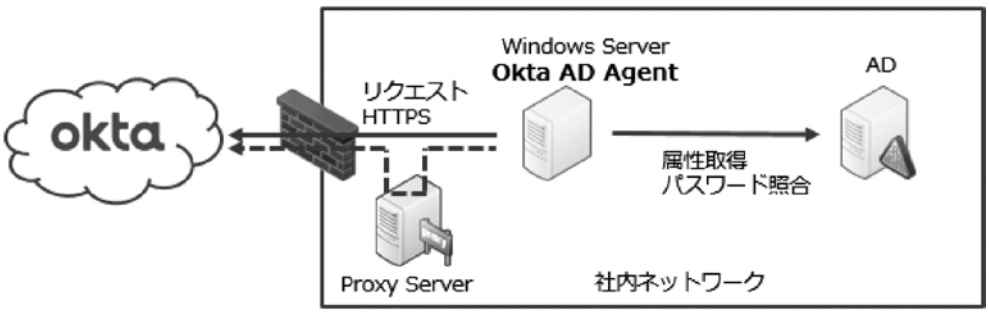

図 5　AD 連携アーキテクチャー

その他，Okta のカスタムアプリケーションである「Okta IWA Web Agent」をオンプレミスに配置すれば，Windows ドメインログオンと連動して Okta への認証を完了することができ，ユーザーの利便性を更に高めることができる（統合 Windows 認証（デスクトップ SSO））．

・Secure Web Authentication

これは Okta のブラウザ拡張機能による ID とパスワードの自動代行入力機能である．SAML 未対応アプリケーションには，アプリケーションへのログイン画面で ID/パスワードを Okta が自動で代行入力することでユーザー側の ID/パスワード入力を省略することができる．

・ID のライフサイクル管理

Okta の管理画面上で外部アプリケーションのユーザー情報を一元管理する機能である．2020 年 6 月時点でプロビジョニング可能なアプリケーション数は 130 に上り業界トップであ

る．プロビジョニング機能を使用することにより，クラウドへのログイン用のアカウント作成，更新，および無効化や，ユーザー属性，グループメンバーシップの管理を Okta から一括してできるようになる．また，オンプレミスの AD や LDAP からのプロビジョニングができる．オンプレミスの社内アプリケーションについても，アイデンティティ・プロビジョニングプロトコル SCIM（System for Cross-domain Identity Management：複数ドメイン間でユーザー ID 情報のやり取りを自動化するための規格）によるプロビジョニングができる．

6. 3. 2.　企業間連携

・グループ＆グローバル統合 ID 基盤

グループ会社との認証基盤の統合や，業務提携，M&A により認証基盤を連携する場合，オンプレミス環境では AD 統合による認証基盤の結合作業に多くの費用と労力を費やすこととなる．Okta を利用すれば，Okta 内にユーザー情報を格納できるため，異なる企業のユーザーでもまとめて ID 情報を管理することができる．Okta AD Agent によるオンプレミス AD との連携により，各社のユーザー情報を収集，管理し，クラウドをはじめとした共用すべきアプリケーションの認証基盤を Okta で提供することで，AD 統合よりはるかに簡易に認証基盤を統合できる．

・人事 SaaS 連携

Workday などのクラウドの人事（Human Resource（HR））システムとの連携により，AD やアプリケーションのアカウント管理を自動化でき，入社や退職に合わせたアカウントの追加，編集，削除などができる．

6. 3. 3.　強力な本人認証機能

・多要素認証

多要素認証（以下 MFA）とは，本人確認のため，パスワードの他に別の認証要素を加える機能である．Okta はスマートフォンのアプリケーションである「Okta Verify」を使用した MFA の他に，メールやモバイルの SMS に送信されるセキュリティコード入力による MFA，FIDO 1.0/2.0 に準拠した U2F and WebAuthn による生体認証による MFA，セキュリティコード入力や FIDO 1.0/2.0 に準拠した生体認証も可能な USB 型の Yubikey による MFA などの認証要素を加えることができる．

・アクセス制限

Okta へのログインや，アプリケーションの利用を制限するポリシーを設定する機能である．例えば，社内ネットワークと会社承認の外部ネットワークからのみ接続を許可したいポリシーを設定する場合のソース IP 制限や，地域の限定，不審な IP アドレスの接続制限，MDM との連携によるデバイストラスト，AD や LDAP のグループやユーザー属性でクラウドへのアクセスを制限，などのポリシーを設定することができる．

6. 4　Okta とクラウドベースのセキュリティ製品との相互連携

前節で述べた Okta の認証機能を起点として，Okta とクラウドプロキシ，CASB，クラウド

型 SIEM などを相互に連携させることで，次世代型の総合的なインターネットセキュリティソリューションを実現できる．

ユニアデックスでは，クラウド時代における総合的なインターネットセキュリティソリューションとして，「クラウドセキュリティプラットフォーム：CloudPas」構想の実現をアピールしている（図 6）．これは，Okta，クラウドプロキシ，CASB，SIEM 等のクラウドベースのセキュリティ製品を相互に連携させプラットフォーム化することで，世界中どこにいても，社内/社外問わず同一のセキュリティーポリシーでインターネットアクセスを実現，制御，可視化する次世代型のセキュリティスキーマである．

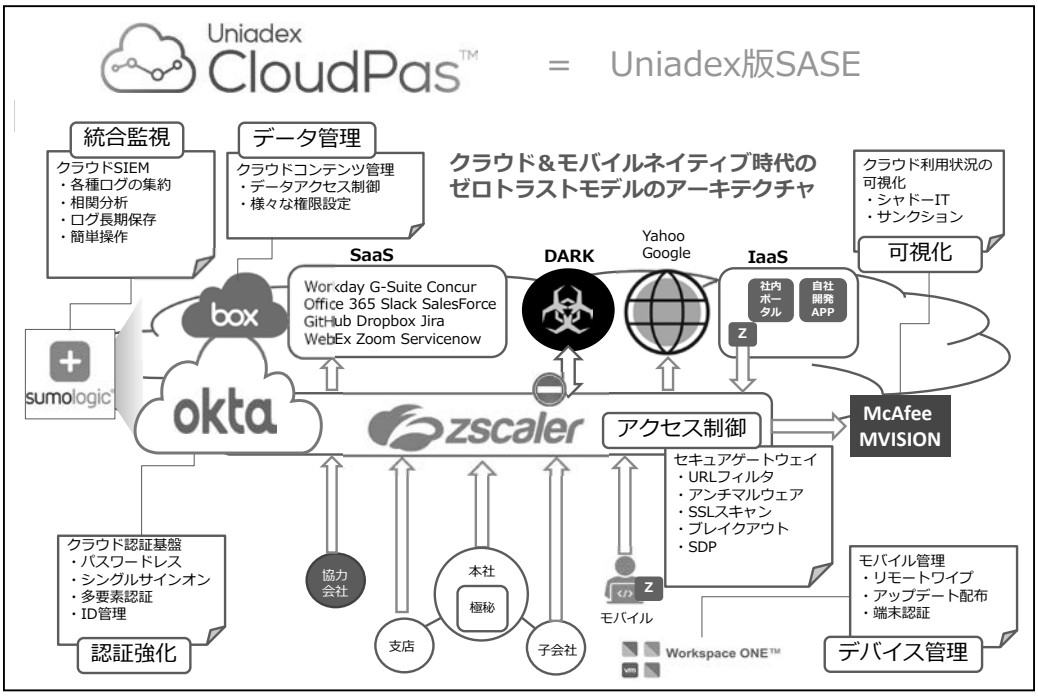

図 6　次世代型の総合的なインターネットセキュリティソリューション

インターネット利用時は，クラウドプロキシ製品の Zscaler や，各クラウドアプリケーションを Okta と認証連携させることで，統合認証基盤としてシングルサインオンやアクセス制御を実現する．社内や外出先からオープンなインターネットやクラウドを利用する際は，国や場所を問わず，Zscaler の URL フィルタリングやアプリケーションコントロールで通信制御を行い，合わせてマルウェアやフィッシングなどへの脅威防御を実装することができる．Zscaler の Web アクセスログを CASB 製品の MVISION Cloud へ転送することで，企業が利用を認めていないシャドー IT クラウドの利用状況を可視化，および利用クラウドのリスク評価を行い，API 連携により Zscaler 側で危険なシャドー IT クラウドへの通信を制御することもできる．Okta，Zscaler，MVISION Cloud，およびオンプレミスのネットワーク，サーバ，クライアント機器，クラウドの IaaS，PaaS，SaaS のログをクラウド型 SIEM 製品の sumo logic へ転送し，リアルタイムでログを分析することで，アノマリや脅威などの不正な通信を可視化し，機械学習による相関分析ができる．

これらのクラウド製品を相互に連携させることで，デバイスやアクセス場所を問わず，安全なインターネット利用，クラウド利用の促進，および全世界で統一のアクセスポリシーを実現することができる．これは 2019 年 8 月に Gartner が発表した Secure Access Service Edge＝SASE（サッシーと発音）の概念に基づくゼロトラストモデルのアーキテクチャーとなっており，企業の動的なセキュアアクセスニーズをサポートする，オールインワンの統合されたクラウドセキュリティを実現するものである．

7. Okta の導入事例

Okta は管理者向けのユーザー・インターフェースが優れているため，顧客自身でシステムを導入できるケースは多いと思われる．しかし，実際に Okta を導入して自社運用に適用すると課題が発生するケースも多い．本章では，ユニアデックスで対応した導入事例から，メリットと課題を説明する．

7. 1　自社アカウント管理システムを持たない顧客のケース

自社アカウント管理システムを持たない顧客 A は，サービスごとにアカウント管理を行っていたため運用管理負荷が高かった．またサービスの利用についても，ログイン処理やパスワード管理をサービスごとに行うなど，利用者の利便性も低かった．この 2 点の課題について，Okta を導入することで解決した（図 7）．

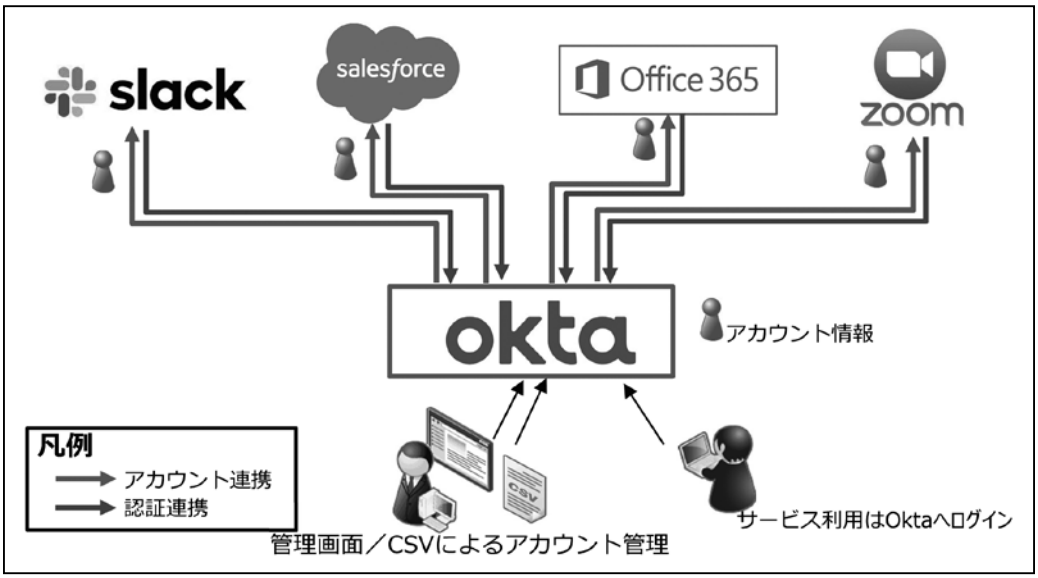

図 7　Okta 連携後のシステム構成図

この案件では，Okta を導入することにより，以下のような利点が享受できた．

1）　アカウント管理の一元化

Okta から各サービスに対してプロビジョニングを行うことで，アカウント管理の一元化を実現した．利用者のパスワード管理も Okta 上のアカウントだけとなり，システムが増えるほど発生する利用者のパスワード忘れなどの運用負荷を軽減できた．

2) ログインの集約
各サービスのログインを Okta に集約したため，Okta のログインを多要素認証で強化することで各サービスの機能に依存せずに認証を強化することができた．

注意事項として，アカウント管理の一元化については，全てのサービスが Okta とのプロビジョニングに対応している訳ではないため，対応していないシステムは今まで通りサービス上でアカウント管理を行わなければならず，案件開始前の事前確認が重要である．

7.2 アカウント運用が複雑な顧客のケース

顧客 B において，図 8 に示す構成で Okta のシステム構築を行った．

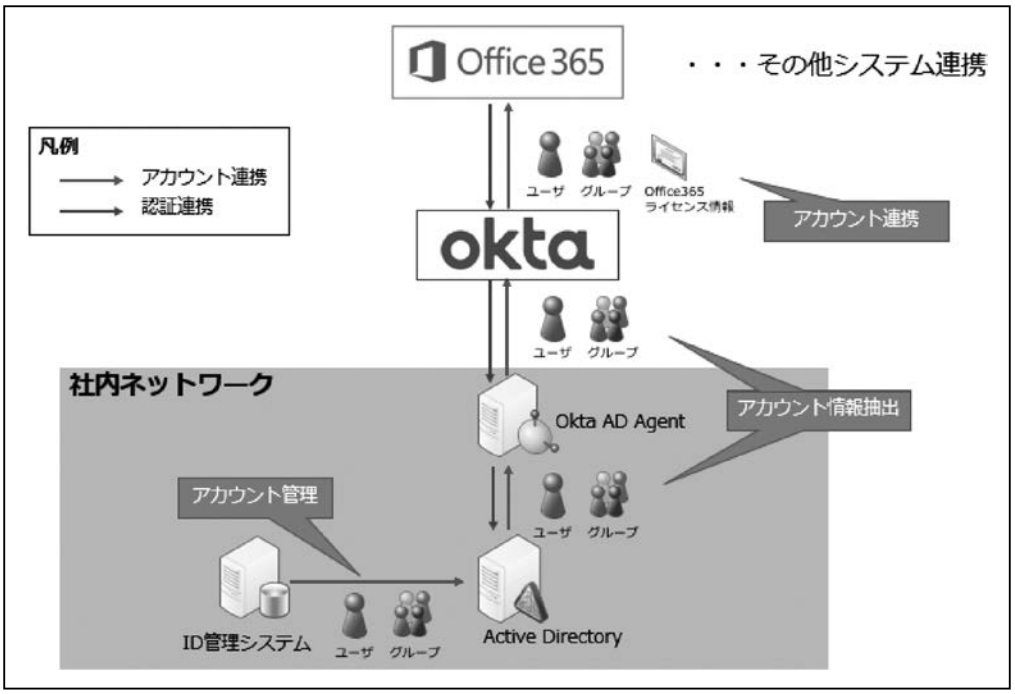

図 8　AD をアカウント源泉としたシステム構成

ID 管理システムでアカウント管理された Active Directory が存在し，Okta は Active Directory からユーザーアカウントやグループアカウントを取得して，Office365 や他サービスへの認証連携やアカウント連携を行う要件であった．本件では以下のような課題に直面した．

1) 自社のアカウント運用が複雑
自社に構築されていた ID 管理システムで行われるアカウント運用は，アカウントの一次凍結，一定期間未利用アカウントの削除，削除ユーザーが同名のアカウントで再作成されることがある，など独自の運用が行われていた．

2) Office365 への連携要件が複雑
Office365 上のユーザーアカウントは外部から連携すると，Office365 の管理画面からユーザー情報の直接管理ができなくなる仕様である．Office365 ユーザーアカウントは

一般的なユーザー属性だけではなく，Office365 ライセンス情報やロール情報など多岐にわたる情報を持っているが，アカウント連携を行うとその全ての情報を Okta 経由で管理する構成になる．

Okta のような SaaS として提供されているサービスは短い期間で運用開始できる反面，一から構築するフルスクラッチのシステムとは異なり，提供される機能は予め決まっている．そのため自社の ID 管理システムの運用や，連携するサービスが提供するアカウント連携の機能内容によって，システム連携の難易度は増減する．本案件は Okta の標準機能で顧客 B の要件を満たすことができず，Okta の機能と併せて顧客 B の ID 管理システムの運用を一部変更することによってシステム構成を行った．

7. 3　既に利用済みのサービスへプロビジョニングを行うケース

顧客 C において，図 9 に示すシステム構成とした．

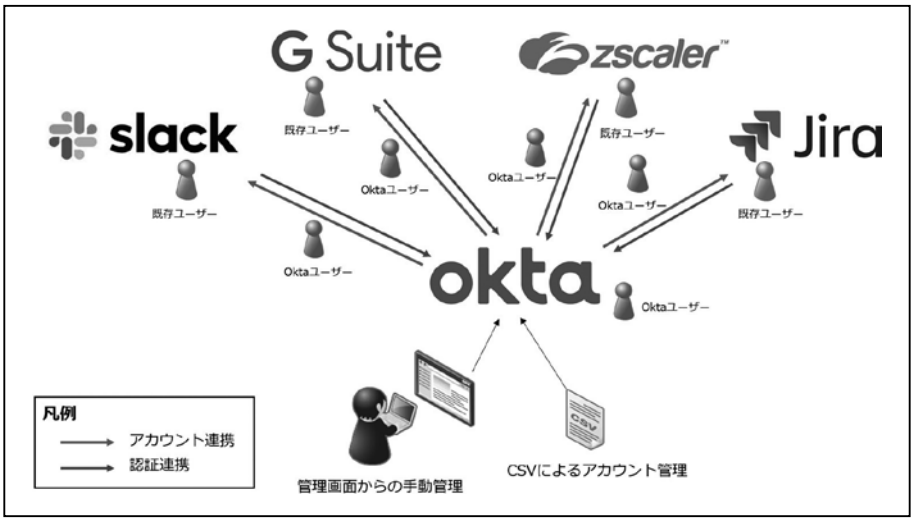

図 9　運用開始済みのサービスにおける Okta 関連システム構成図

この案件は，既に運用を開始しているサービスに対するアカウント連携が要件に含まれていた．運用開始済みのサービスにプロビジョニングを行う場合，連携のタイミングでサービスの既存アカウントへの上書きやデータの重複，消失などを防ぐ考慮をしなければならない．これは運用開始済みのサービスに依存するため，事前にサービス提供事業者への確認や事前検証を行わなければならなかった．

8. お　わ　り　に

マルチデバイス，マルチクラウド環境が今後ますます進んでいく中で，Okta を起点とした次世代型の Web 脅威対策＋ID 統合管理＋CASB＋分析基盤等のプラットフォーム化は時代の要求に応え得るものであり，インターネットアクセス，社内アクセスをより強靭なものにできると考えている．今後もクラウドセキュリティプラットフォームを推進し，企業のデジタルト

ランスフォーメーション（DX）とセキュリティガバナンスの両輪を支援していくために，高い技術力とサービス提供力で最適な次世代型クラウドセキュリティの環境作りに貢献していく所存である．

最後に，本稿の執筆にあたり助言頂いた関係者に深く感謝し，御礼を申し上げたい．

＊1　クラウド・バイ・デフォルト原則：2018年6月に政府が発表した政府情報システムにおけるクラウドサービスの利用に係る基本方針．

＊2　Society 5.0：政府が提唱する新たな未来社会の姿．2016年1月に閣議決定され，日本政府が策定した「第5期科学技術基本計画」の中で用いられている言葉．

＊3　AD環境の場合，Active Directory Federation Services（ADFS）を利用すればクラウドへのシングルサインオンに対応できるが，オンプレミス環境へのADFSサーバ，ADFSサーバファームと外部アプリケーションの間にインストールされるフェデレーションサービスプロキシ，ADFS構成データベースの三つのハードウェアコンポーネントを導入しなければならず，大規模な構成とメンテナンスを要する．

＊4　ここでポイントになるのが，既存のオンプレミスのAD/LDAPとの連携である．IDaaSの中には既存のAD/LDAPのID情報をIDaaSに連携することで，認証をAD/LDAPのまま，アカウント情報の統合をIDaaSで行う，ということも可能な製品がある．クラウドサービスと社内システムへのシングルサインオンが可能なハイブリッド統合認証基盤を実現できる．

＊5　SAMLはXMLをベースに2002年に策定され，2005年にバージョン2.0になっている．XMLにはフォーマット化されたメッセージとして，ユーザーID，パスワードや属性情報などのユーザーの認証情報が記述されおり，これをアサーションという．

参考文献　［1］「情報通信白書令和元年版」，総務省，https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd232140.html

［2］「政府情報システムにおけるクラウドサービスの利用に係る基本方針」，各府省情報化統括責任者（CIO）連絡会議決定，内閣官房情報通信技術（IT）総合戦略室，2018年6月，https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

［3］「Society 5.0」，内閣府，https://www8.cao.go.jp/cstp/society5_0/

［4］「成長戦略閣議決定（令和2年7月17日）」，首相官邸，2020年7月，https://www.kantei.go.jp/jp/headline/seicho_senryaku2013.html

［5］「Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0」，OASIS，2005年3月，http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

［6］「Magic Quadrant for Access Management」，Gartner，2019年8月，https://b2bsalescafe.files.wordpress.com/2019/09/gartner-magic-quadrant-for-access-management-august-2019.pdf

［7］「Okta Named Industry Leader by Forrester Research, Inc. for Identity as a Service for Enterprise.」，BeyondID，2019年7月，https://www.beyondid.com/okta-named-industry-leader-by-forrester-for-identity-as-a-service-for-enterprise/

［8］「Okta now has over 100 million registered users, says CEO」，CNBC，2019年1月，https://www.cnbc.com/2019/01/24/okta-ceo-we-now-have-over-100-million-registered-users.html

［9］「Okta Security Technical Whitepaper」，Okta，2020年5月，https://www.okta.com/resources/whitepaper/okta-security-technical-white-paper/

※　上記参考文献に含まれるURLのリンク先は，2020年10月19日現在での存在を確認．

執筆者紹介　小　倉　俊　弘（Toshihiro Ogura）

2000年日本ユニシス(株)入社．PingFederate，IceWall SSOなどのオンプレミスの認証基盤製品の主管業務に携わる．2017年よりSaaSの認証基盤であるOktaの提案，および設計，提供に従事．

新　原　英　樹（Hideki Shimbara）

2003年(株)ネットマークス入社．CheckPoint，Juniper，Fortinetなどのセキュリティ製品の導入およびカスタマーサポートに携わる．2017年よりMVISION Cloud，Okta，Zscalerをはじめとするクラウドセキュリティ領域の製品主管として，提案と設計およびサービス開発に従事．