SecuritySaaSの連携による ZTNA（Zero Trust Network Access）の実現

Realizing Zero Trust Network Access (ZTNA) through SecuritySaaS Integration

越　渡　俊　幸

要　約　従来の企業ネットワークは，トラフィックを一度データセンターに集約させた後，用途に応じて適切な場所やデバイスに分散させる設計で運用されてきた．社会情勢の影響や利便性・効率化への追求に伴い，業務システム及び情報資源はクラウドへシフトする方向に進んでいる．クラウドシフトや業務多様性に対応したセキュリティ対策として，守るべき対象がさまざまな場所に点在しても防御できる「ゼロトラスト」に基づいたセキュリティ対策が求められる．ユニアデックス株式会社は，クラウドセキュリティ対策に必要な機能を，認証，検知・防御，可視化，分析と定義して，Uniadex CloudPasをリリースした．

Abstract　Traditional corporate networks have been designed to aggregate traffic once in a data center and then distribute it to appropriate locations and devices according to the application. With the influence of social conditions and the pursuit of convenience and efficiency, business systems and information resources are shifting to the cloud. As a security measure corresponding to cloud shift and business diversity, security measures based on “Zero Trust” that can protect even if the objects to be protected are scattered in various places are required. Uniadex Co., Ltd. has released Uniadex CloudPas, defining the functions required for cloud security measures as authentication, detection / prevention, visualization, and analysis.

1. はじめに

従来のリモートワークはオンプレミス前提で考えられてきた．新型コロナウイルス感染症（COVID-19）によりテレワークが加速し，今後，ニューノーマルな勤務スタイルに合わせて，業務システムのクラウドシフトが進めば，セキュリティ対策のさらなる変革が求められる．クラウド環境下では情報資源を利用する端末が不特定多数になる．資源の保管場所が社内から社外へと広がればセキュリティ対策の範囲も広がる．これからは場所に捕われないセキュリティ対策が求められている．クラウド利用時のセキュリティに不可欠な機能として，『認証』，『検知/防御』，『可視化/分析』がある．また，クラウドセキュリティの新たな考え方としてSASE（Secure Access Service Edge）やZTNA（Zero Trust Network Access）という新しい概念がある．

本稿では，SASEの理解とZTNAの概念を深掘し，ゼロトラストモデルの実現に向けた最新動向について述べる．最後に，ユニアデックス株式会社（以下，ユニアデックス）の経験と知識をまとめたベストプラクティスとなる「Uniadex CloudPas」サービスを紹介する．

まず2章でSASEの概要，3章でZTNAの概要を説明して，4章でZTNAが登場した背景，5章でIaaSベンダーの取り組みを紹介した後，6章でゼロトラストモデルの実現に向けた最新動向，7章でUniadex CloudPasと統合管理の展望を述べる．

2. SASE（Secure Access Service Edge）とは

SASE（Secure Access Service Edge「サシー」と発音）とは，ネットワーク/セキュリティ機能を包括的にクラウドから提供することで，いつでもどこでもアプリケーションやサービスにセキュアにアクセスするための新しいフレームワークである．SASE は，ZTNA（Zero Trust Network Access）の概念をもった IDaaS（Identity as a Service），SWG（Secure Web Gateway），CASB（Cloud Access Security Broker），MDM（Mobile Device Management）のようなサービスをクラウド上で統合し，必要な機能をエッジに対して提供する．

SASE は，ガートナーが 2019 年 8 月に発表したレポート『The Future of Network Security is in the Cloud』で初めて提唱した次世代のセキュリティ対策の概念である．ガートナーは，この SASE に関する市場動向レポートの中で，「顧客は，インターネットのエッジネットワークセキュリティ市場において，シンプルさ，スケーラビリティ，柔軟性を兼ね備え，遅延の少ない広範なセキュリティ機能が提供されることを求めている」と述べている．

3. ZTNA（Zero Trust Network Access）について

ZTNA（Zero Trust Network Access）ゼロトラストネットワークアクセスとは，「全てのアクセスを信頼しない」というゼロトラストの考え方を取り入れた，セキュリティモデルである[1]．データファイルやアプリへのアクセス制御を一元的に管理するため，組織におけるセキュリティレベルのばらつきを防ぐことができる．システムやサービスに対して，すべてのトラフィックを信頼しないことを前提として，トラフィックをセキュリティゲートウェイに集約し，検査（アクセスコントロール）とログ分析を行う．認証と暗号化はエンドツーエンドで行い，デバイス情報やトラフィックを常に監視することがポイントである．

4. ZTNA（Zero Trust Network Access）が必要とされる背景

従来の企業ネットワークは，トラフィックを一度データセンターに集約させた後，用途に応じて適切な場所やデバイスに分散させる設計で運用されてきた．つまりデータセンターの外部は危険であり，内部だけ保護すれば安心というポリシーであった．現在のネットワーク環境と業務システムの利用状況を図 1 に示す．縦軸はセキュリティの信頼性の高/低を，横軸はネッ

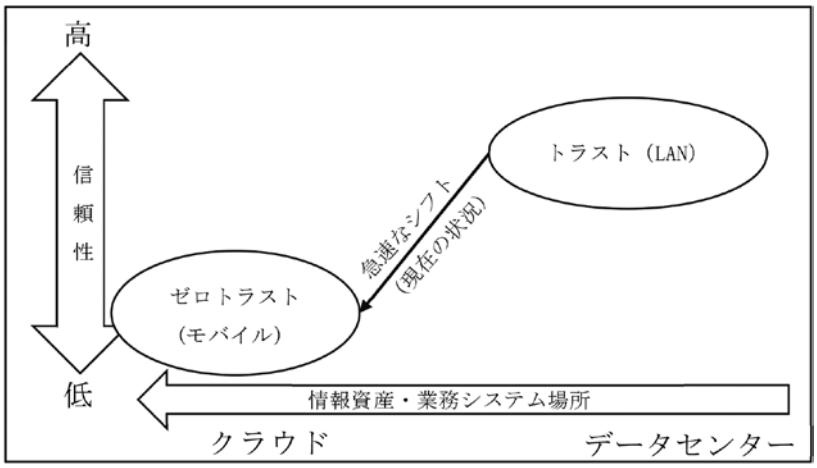

図 1　クラウドシフトとゼロトラストの関係性

トワークの利用状況を表している．右上に行くほど安全領域であるが，現在の社会情勢の影響や利便性・効率化への追求に伴い，業務システム及び情報資源はクラウドへシフトする方向に進んでいる．

アプリケーションがクラウドにシフトすることで，従来のような，データセンター集約型の運用では対応できない新たな課題が見えてきた．

4.1　クラウドシフトによるリスクの増加

SaaS などのクラウドアプリケーションをデータセンター経由で利用する場合，アプリケーションごとに異なるポリシーを適用するため，管理コストの増大やネットワークの帯域増加，大きな遅延が発生し，効率性と生産性に大きな影響を及ぼす[2]．

4.2　業務の多様化による従来型運用の崩壊

新型コロナウイルス対策によるリモートワークが加速する中，従来型のオンプレミス型での固定したセキュリティ境界を用いた防御では，外出先・リモート環境でのリスク対策の実現は困難であった．ユーザの利用環境や時間に依存せず，クラウドベースのアプリケーションやデータ（ビジネスクリティカルなアプリケーションやデータなど）に安全にストレスなくアクセスできる環境づくりが求められる．

4.3　ある企業での課題

クラウドシフトが進む中，クラウドのみでシステムを運用していく企業も出てきている．本節では，デジタル化を急速に進める企業の課題を紹介する．この企業では，急速な事業拡大に伴い「従業員やシステム増加」「パートナーとの業務連携」が急速に進んでいた．業務の拡大と多様化に対応するため「フルクラウド」で業務を行える環境を整備していた．システム担当者には，時間・場所・組織に捉われずセキュリティポリシーを確実に遵守して安全に外部ネットワークから業務を行える環境整備が，求められていた．クラウドを中心とした情報基盤には，まず外部からクラウドへ許可されたユーザだけが安全に利用できる ID 管理基盤が不可欠と考えたが，導入には表 1 のような課題があった．

表 1　ID 管理基盤導入の課題

課　題	内　　容
ID 管理による課題と要望	・自社に認証基盤がないため，各システム側でのユーザ ID 管理が煩雑（一つの ID に対して利用システムの数分の登録や管理）．部署異動に伴う従業員の増減，協力会社へのアクセス権の付与有無等により管理が複雑化しており，設定不備等のリスクを軽減したい． ・クラウド（SaaS）との属性連携や，各グループのドメインを限定せずに ID 管理を行いたい．
インターネット接続課題	時間・場所・組織に捉われない環境で，セキュリティポリシーを遵守し，外部から安全にインターネットアクセスを行える仕組みが不可欠である．

これらの課題を解決するため，クラウドシフトや業務多様性に対応したセキュリティ対策が急務であった．すべてのネットワークを「信頼しない」とした上で，情報資源を保護するため，

『認証』『検知・防御』『可視化・分析』といったセキュリティ対策を施し，端末から情報資源への接続に対するリスクを排除する必要がある．さらに，業務の拡大・多様性を損なわせないため利便性やパフォーマンスの確保と運用の効率化に対しても，考慮する必要があった．

デジタルイノベーションが加速していくことで，ネットワークやクラウド利用が広がる中，攻撃対象領域は急速に拡大する．従来型のセキュリティソリューションでは，組織やユーザが求めるスピード，パフォーマンスを向上させながらセキュリティレベルを維持することが困難になっている．従来の社内ネットワークのように閉じた環境を守る境界線防御ではなく，守るべき対象がさまざまな場所に点在しても防御できる「ゼロトラスト」に基づいたセキュリティ対策が求められる．ZTNA の概念に基づいたセキュリティサービスが多くリリースされ実装例も増えている．5 章で ZTNA のソリューションをいくつか紹介する．

5. 各 IaaS ベンダーにおける ZTNA への取り組み

大手 IaaS ベンダー（Google/Microsoft/Amazon）の現状の ZTNA の取り組みについて，以下に整理する．

5. 1 Google

Google では，ゼロトラストの概念に基づいた『BeyondCorp[3]』という，独自の概念に基づき自社のセキュリティシステムに 2011 年から取り組んでいる（Google が考える ZTNA イコール BeyondCorp を提唱している）．概要としては，ネットワークアクセスのセキュリティ境界線を各端末で持つという設計思想に基づき，リモートアクセス VPN を利用せずとも，場所や環境に依存せず，ユーザ/契約業者は企業データに安全にアクセスできる仕組みである．ソリューションの中核となる機能としては，リバースプロキシを経由した，GCP/Gsuite/オンプレミスへアクセスする方式である．これにより，さまざまなデバイスからのタイムカードや勤怠システムといった業務アプリケーションへのアクセスや，特定 OS を利用している端末のみセキュリティチェックを実施し，問題ないと判断された端末のみアクセス可能としている．例として，GCP へのアクセスのシステム構成を表 2 と図 2 に示す．

表 2　GCP の場合（各コンポーネント説明）

コンポーネント	ファンクション
Cloud Identity	ユーザ識別（誰が）
Endpoint Verification	接続環境（どの端末）
Cloud Identity-Aware Proxy	リスク判断，アクセスコントロール
Cloud Interconnect	クラウド/社内接続システムコントローラー
Access Context Manager	通信に対するリスク判断（トラフィック制御）

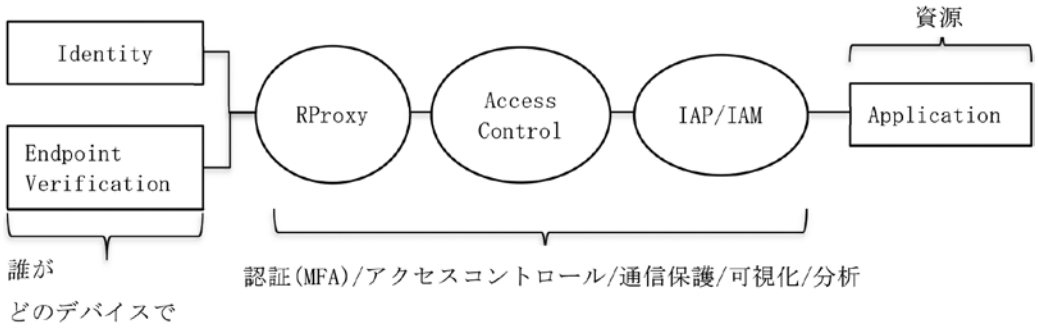

図 2　GCP の場合（各コンポーネント説明）

5. 2　Microsoft

Microsoft 社[4]では，「Active Directory」「Azure AD」と「Azure Sentinel」を核とした，ID 管理に注力した ZTNA を提唱している（表 3）．サービスの中心としては，やはり「Azure Active Directory（AD）」となっている．Azure AD は，各種のクラウドサービスやアプリケーションのアカウントに対する認証基盤の役割を果たすクラウドサービスである．「AWS（Amazon Web Services）」や「Box」をはじめとして，他社が提供するクラウドサービスと認証を連携させることができる．このため，一度のサインインで全てのサービスやアプリケーションが利用できるようになる．企業のディレクトリーサービスとして事実上の標準となった，オンプレミスの AD とアカウント情報を統合できることも大きな特徴である．オンプレミスの AD と連携する形で Azure AD を導入すれば，クラウド環境のために別途の ID を管理する作業は不要になる，といったシングルサインオンを中心としたソリューションを打ち出している．

表 3　Microsoft の場合（各コンポーネント説明）

コンポーネント	ファンクション
Active Directory	Active Directory（アクティブディレクトリ）とはマイクロソフトによって開発されたオンプレミスにおけるディレクトリ・サービス・システムであり，Windows 2000 Server から導入された，ユーザとコンピュータリソースを管理するコンポーネント群の総称である．なお，クラウドコンピューティングにおけるディレクトリ・サービス・システムである Azure Active Directory と区別する場合，オンプレミス Active Directory と表記することもある．
Azure AD	Azure Active Directory（Azure AD）は Microsoft が提供するクラウドベースの ID およびアクセス管理サービスであり，サービスへのサインインとアクセスを支援する（図 3）．
Azure Sentinel	「Azure Sentinel」は，クラウドと AI（人工知能）を活用した企業のセキュリティ運用ソリューションである．企業内で収集したさまざまなイベントログを統合管理し，相関関係を分析して，サイバー攻撃による被害を未然に防いでシステムを保護．セキュリティ関連で重視されているソリューションに「SIEM」がある．

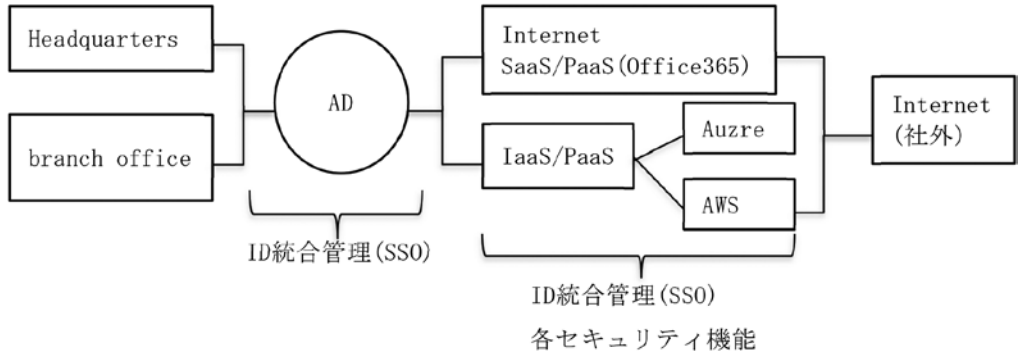

図 3　Active Directory の ID 管理・権限概要

5. 3　AWS（Amazon Web Services）

AWS[5]では，ベストプラクティスアーキテクチャとして，AWS 上で Well-Architected なアプリケーションを設計するための基礎となるフレームワークのツールを提供している．AWS Well-Architected Framework は，AWS のベストプラクティスとワークロードを比較し，安定的かつ効率的なシステムを構築するためのガイダンスを得る戦略を紹介している．Well-Architected Framework には，セキュリティを含む五つの明確な柱が含まれており．このフレームワークを基に，ゼロトラストを AWS アーキテクチャに適用したモデルがある．Amazon では，マイクロソフトが提唱している『STRIDE』の脅威分析モデル（表 4）を基にゼロトラスト（図 4）を組み立てている．

表 4　脅威モデル

STRIDE 脅威モデル	対　　策	説　　明
Spoofing	AmazonMFA SSL/TLS	ユーザ ID のなりすまし対策
Tampering	AWS AIDE	データの改ざん対策
Repudiation	CloudWatch	ソースの否認対策
Information Disclosure	Cloud Automator	情報漏洩
Denial of Service	AWS Shield	サービス停止
Elevation of Privilege	IAM	特権の昇格

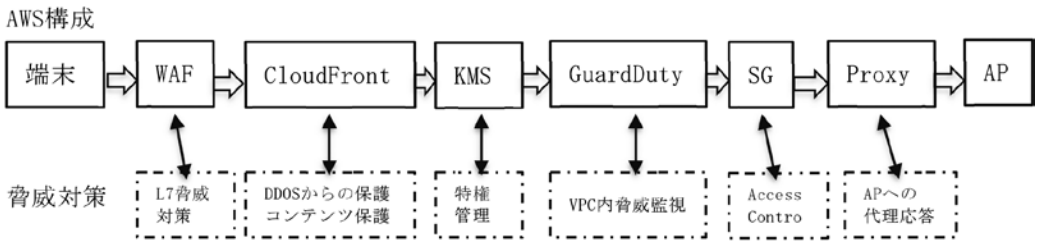

図 4　AWS ゼロトラストモデルケース

6.　ゼロトラストモデル実現に向けた最新動向

本章では，現在の動向として，ZTNA の機能に対するサービスや実現方法（表 5）について整理する．

表 5　ZTNA 実現モデル

機　　能	サービス	実現方法
認証	IDaaS	Okta/AzureAD
検知・防御	WebSecureGateWay	Zscaler
可視化	CASB	MVSION
分析	SIEM	Sumo Logic

6. 1　IDaaS（Identity as a Service）分析

IDaaS とは Identity as a Service の略称で，アイデンティティ（Identity）の管理を SaaS や IaaS などと同じくクラウドにて管理するサービスである．IDaaS の市場では 4 年連続で okta[6]がリーダー的地位である．Microsoft や Ping Identity もリーダークラスの実力で評価されているが，okta は，SSO アプリケーションの対応数や各 SaaS との親和性（プロビジョニング），MFA（種類の豊富さ），API アクセス管理，UX において一歩リードしている．

IDaaS を選定する際は，クラウド・オンプレミスシステムとの接続性と制御できる範囲を考慮する．Okta や AzureAD は，接続性と制御機能が豊富であるため候補になることが多い．IDaaS は，退職や異動による権限の変更/削除のオペレーションミスを防ぐ有効な手段である．また，成りすましを防ぎ，本人を厳格に承認するための多要素認証や，利用者の負担を軽減するシングルサインオンなど，クラウドサービスへ安全にアクセスするために不可欠な機能を備えている．以下に利用が増えている「Okta」の特徴と優位性を紹介する．

6. 1. 1　実績

Okta は世界で数千社，国内でも 100 社以上と，IDaaS 市場では十分な導入実績がある．また，Gartner 社からリーダーとして評価されている．

6. 1. 2　連携対応 SaaS

IDaaS の実力を測る基準として，連携できるアプリケーションの数も重要なファクターである．Okta は約 6,000 以上のアプリケーションを連携できる．また，認証方式として，SAML は当然ながら，Active Directory/LDAP/Radius 等とも連携できる．SAML 未対応のレガシーなアプリには，ID/Password の自動入力による連携方式を採れる．

6. 1. 3　MFA（Multi-Factor Authentication）

MFA は，認証機能の必須要件となる多要素認証である．okta は二段階目の認証として，『秘密のパスワード』『ワンタイムパスワード』『承認機能』『生体認証（FIDO2.0）』『生体認証』といった多彩なバリエーションを持っている．FIDO を利用することによりパスワードレスが実現されていく見通しである．

6. 2　SWG（Secure Web Gateway）

SWG とは，URL フィルタやアプリケーションフィルタ，アンチウイルス，サンドボックスなどの機能を，クラウド型で提供するサービスである．ZTNA/SASE を実現するために必須のセキュリティ対策であり，クラウドを利用するうえで接続先の URL アクセスコントロールや通信の安全性をスキャンし，悪意あるコードやスクリプト，マルウエア等をチェックし，脅威と判定した場合に通信を遮断する機能を持っている．

企業の理想的なリモートワーク環境である，インターネットからの脅威に対するセキュリティ対策を実現するためには，場所や接続環境を選ばずにセキュリティポリシーを適用できる，SWG（クラウド型プロキシ）を利用することが求められる．

ZTNA を実現するうえで最初のステップとなる SWG 市場において，Zscaler 社[7]の Zscaler Internet Access（ZIA）の適用事例が増えている．実績や機能の豊富さ，可用性の高さ，パフォーマンスにおいて優位性が高い，Zscaler Internet Access の特徴を紹介する．

6. 2. 1　実績

Zscaler は 10 年にわたり，Secure Web Gateway サービス提供を行っている，長きにわたり培ったノウハウ・テクノロジーに関しては，他社と比べて一歩リードしている．また，Forbes Global 2000 の 400 以上の企業がこの Zscaler Internet Access を採用しており，クラウドシフトや働き方の多様化により，国内外で導入を検討する企業が急増している．

6. 2. 2　可用性

Zscaler Internet Access は，全世界 150 カ国にデータセンターを保有しており，端末は自動的に，最寄りの DC へ接続するため，仮に利用している DC がダウンしても，隣国の DC を利用することにより業務を継続できる．また SLA に関しても，ISO 27001 認定を取得しており，99.999％の可用性を保証し，レイテンシとセキュリティについては別途 SLA を定めている．

6. 2. 3　パフォーマンス

ZscalerCloud のパフォーマンスについては，2019 年度の実績値として，SLA を維持した状態で，全世界で 1,000 億件のトランザクションの処理実績があり，パフォーマンスが高い．また，リソースが不足する場合は，クラウドの強みであるオートスケーリングの機能を活用することで，ユーザはストレスなくインターネットを利用できる．

6. 2. 4　セキュリティ

Zscaler セキュリティエンジンは，実績値として，1 日あたり約 12 万件に及ぶセキュリティ対策のアップデートの実績があり，1 億件以上を検知する脅威データベースを保有している．この数値から，インターネットの脅威に対して迅速に対応できることがわかる．また，個人情報保護関連法のコンプライアンスを遵守しており，代表的な例として，GDPR（一般データ保護規則）や Privacy Shield，国内では APPI（Act on the Protection of Personal Information）に準拠している．

6. 3　CASB（Cloud Access Security Broker）

Cloud Access Security Broker は，クラウドサービスユーザとクラウドアプリケーションの間に位置し，すべてのアクティビティを監視してセキュリティポリシーを適用するオンプレミスまたはクラウドベースのソフトウェアである．シャドー IT やクラウドリスクのレーティングに基づきポリシーを作成し，企業ガバナンスを維持するシステムである．クラウドを安全に利用するための運用管理の視点からも，無数にあるクラウドサービスの中で，どのサービスが安全であるかの判断は非常に難しい．こうしたリスク分析の専門家の評価を活用することで，企業のコンプライアンス維持とユーザがポリシーに合った振る舞いであるかをチェック・制御して情報漏洩を抑止できる．

CASB としての導入実績が増えている McAfee 社の MVISION を紹介する．

6. 3. 1　実績

CASB は，ZTNA に不可欠な機能である．CASB の市場として，まだ，国内では導入実績が少ないが，今後はクラウドへのシフトが進むと考えられており，シャドー IT の可視化や，クラウドのレーティング（リスク）や情報漏洩対策を把握できるサービスとなる．

6. 3. 2　SaaS への対応

連携対応の SaaS として，全世界では 30,000 以上のクラウドサービスのリスクプロフィールに対応している．また，日本国内利用時の強みとして，日本のクラウドサービスに対して，400 種類以上に対応できる．

6. 3. 3　データ保護

データ保護機能については，Knock-Knock 攻撃によるアカウント乗っ取りや，ポリシー違反のファイル共有，フィッシングによるアカウント乗っ取り，ストレージサービスの設定ミス等に対応した機能を有する．この機能により，データ侵害に関するリスクを回避することで，クラウドデータを保護する．

6. 4　SIEM（Security Information and Event Management）/Analytics

セキュリティ情報とイベント管理は，コンピュータセキュリティの分野のサブセクションであり，ソフトウェア製品とサービスは，セキュリティ情報管理とセキュリティイベント管理を組み合わせている．アプリケーションやネットワークハードウェアによって生成されたセキュリティアラートのリアルタイム分析を提供する．リーダーとしては，Splunk や IBM がリーダークラスである．今後のクラウドシフトの流れにより，各クラウドサービスとの親和性の高い Sumo Logic に注目したい．

Sumo Logic は，自社が利用する様々なクラウドサービス内部に記録される監査ログを収集し，ログデータだけでは分かりにくい証跡を可視化することができる．クラウドサービスを対象としたセキュリティ分析[8]として SIEM のカテゴリに位置づけられている．

7. Uniadex CloudPas

ユニアデックスは，ZTNA を実現する最適なコンポーネントを提供するため，クラウド事業者の ZTNA への取り組みや，経済産業省発行のサイバーセキュリティガイドライン 2.0 等，最新の脅威やトレンド等を参考に，「Uniadex CloudPas®（以降，CloudPas）」をリリースした．CloudPas は，ZTNA の『認証』『検知/防御』『可視化』『分析』を一元管理できるワンストップ型のクラウドセキュリティサービスである．CloudPas の構成要素を表 6 と図 5 に示す．我々は，CloudPas をアーキテクチャとしたサービスを普及するため活動を続けている．

表 6　CloudPas の構成要素

機　能	目　　的	構成要素
認証	本人認証 適正な権限の割当て 特定のデバイスからのアクセスコントロール	SSO MFA Device Trust ライフサイクル管理（プロビジョニング）
検知・防御	通信に対する脅威対策 通信のアクセスコントロール 通信の保護 ガバナンス維持	SSL インスペクション Antivirus/Sandbox/IPS/Firewall/URL フィルタリング
可視化	脅威の可視化 クラウド利用判定 データ保護	API クラウドレーティング
分析	ロギング，脅威分析	テレメトリ，メトリクス
運用負荷軽減	運用負荷軽減（一元管理）	各 SaaS へ API コントロール

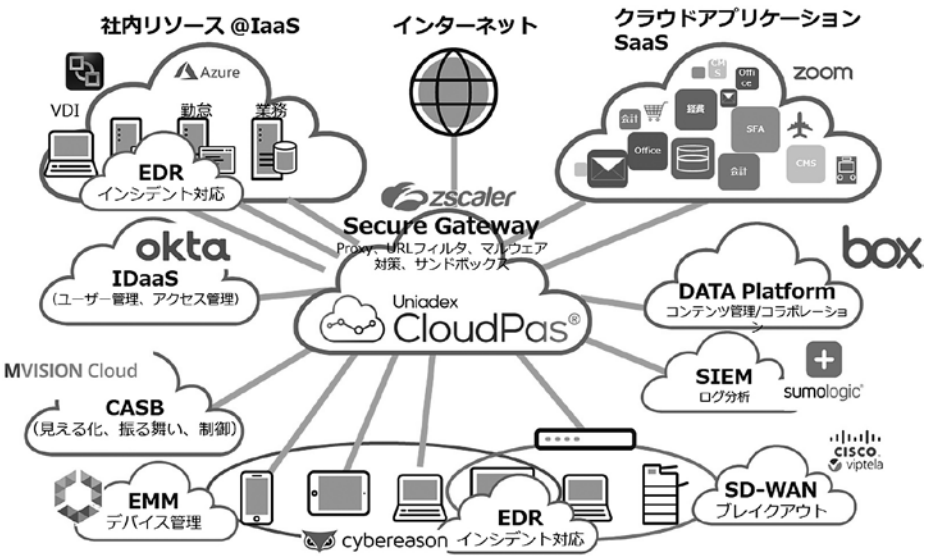

図 5　CloudPas ソリューション構成

クラウドサービスへのセキュリティの脅威から貴重な資産や情報を守り，ゼロトラストモデルを実現するには，いくつかの機能やサービスを組み合わせて対策を施すことが重要である．ZTNA サービスを活用して実装することは理想であるが，逆にシステムが複雑となり運用負荷が増大する恐れがあった．運用負荷の増大は，設定ミス等のリスクを誘発する恐れがある．そこで，各サービスに実装されている API を活用し，統合されたサービスを利用することで運用負荷を解消できると考え，新たな開発「CloudPas Operation（仮）」を進めている．

「CloudPas Operation（仮）」では，Web 画面から，日々の運用で実行するセキュリティポリシー単位（1 回の操作）で，複数のサービスや機能への設定を同時に行う，運用利便性を追求したオリジナルサービスの開発を目指している（図 6）．

図 6　開発中の CloudPas Operation Web 画面イメージ

サービスの活用例として，新しい社員が入社した際に，基本的なパラメータ（氏名/所属部署/初期パスワード等）を設定するだけで，適正なアプリケーション接続やネットワークのアクセスコントロールを，API を用いて自動的にプロビジョニングする機能が挙げられる．

今後，クラウドシフトが進む中，他ベンダー間の API での連携は不可欠である．主要な SaaS ベンダーの機能は既に API が実装されているものが多く，その API を活用することで各サービスの特異性を活かしながら各サービス間を疎結合し，保守運用性を高めて，最新技術へ追従していけるようになるだろう．

8. お　わ　り　に

本稿では，ZTNA の概念や各ベンダーの取り組み，分析といった順序で述べてきた．改めて ZTNA（Zero Trust Network Access）について整理した．

Forrester Research が 2010 年に提唱した ZTNA は 10 年の歴史の経過し，ZTNA の多くの機能は，プロキシモデルを中核としたゲートウェイを利用し，情報資産の保護を行い，アプリケーションアクセスの認証強化，証跡管理といったセキュリティ対策を提唱している．最後に，ソリューションが劇的に進化を遂げる中，AI による脅威分析や運用自動化も進んでいるが，これを使いこなせる（考える力を持つ）セキュリティ人材育成も急務である．

現在，筆者は CloudPas の企画に従事している．チームメンバーとともに，顧客にとってクラウドセキュリティ対策＝ユニアデックスという存在になれるよう，日々努力したい．

参考文献
［1］ Evan Gilman/Doug Barth 著，鈴木研吾監訳，「ゼロトラストネットワーク　境界防御の限界を超えるためのセキュアなシステム設計」，オライリー・ジャパン，2019 年 10 月
［2］ 金丸浩二/河野省二/久保田朋秀/仲山昌宏/吉井和明/吉田雄哉/渡辺一宏著，「クラウドセキュリティ　クラウド活用のためのリスクマネージメント入門」，株式会社　翔泳社，2014 年 5 月
［3］「BeyondCorp ゼロトラスト企業セキュリティ」，Google，https://cloud.google.com/beyondcorp?hl=ja
［4］「マルチクラウド本格活用で改めて見直すべきセキュリティ対策」，株式会社　日経 BP，https://special.nikkeibp.co.jp/atclh/NXT/19/microsoft0930_2/vol2/
［5］「AWS 上でどのようにゼロトラストアーキテクチャを考えていくか」，Amazon Web Services ブログ，2020 年 6 月 5 日，Amazon，https://aws.amazon.com/jp/blogs/news/how-to-think-about-zero-trust-architectures-on-aws/
［6］「エンタープライズアイデンティティの統合」，Okta，https://www.okta.com/jp/projects/customer-identity/integrate-enterprise-identities/
［7］「セキュアインターネットゲートウェイ Zscaler Internet Access」，Zscaler，https://www.zscaler.jp/products/zscaler-internet-access
［8］「Cloud SIEM」，Sumo Logic，https://www.sumologic.jp/solutions/cloud-siem-enterprise/

※　上記参考文献に含まれる URL のリンク先は，2021 年 2 月 25 日時点での存在を確認.

執筆者紹介　越　渡　俊　幸（Toshiyuki Koito）
2000 年ネットマークス入社，2005 年ユニアデックス株式会社へ転籍.
Cisco，Juniper 設計構築，文教，金融，キャリアの基盤ネットワークの設計・構築に従事.
現在，ユニアデックス(株) DX イノベーション統括部に所属 .