別紙 3

厚生労働科学研究費補助金
政策科学総合研究事業 (臨床研究等 ICT 基盤構築・人工知能実装研究事業)

分担研究報告書
クラウド上の医療 AI 利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言

研究代表者　岡村 浩司　国立成育医療研究センター 室長
研究分担者　松井 俊大　国立成育医療研究センター 医員

研究要旨

画像認識等 AI 技術の進歩は医療分野にも大きな可能性をもたらし、医療の質向上や効率化、地域格差の解消、医療従事者の負担軽減などを目指した取り組みが活発に進められている。国立成育医療研究センター(NCCHD)では、医療 AI サービスを開発、医療 AI プラットフォーム技術研究組合(HAIP)と連携し、国内多くの医療機関がクラウドから公開されるサービスを安全に使うことができる環境の整備を目指して研究を進めている。NCCHD では免疫不全患者や臓器移植後の免疫抑制剤投与患者など、感染症に対してハイリスクな患者を多数抱えており、グラム染色画像からの感染症起因菌同定支援システムの開発を進め、特許出願を行った。互いに異なる培養条件に対応する複数のモデルを構築し、判別対象菌の培養条件に応じて選択することで、外観が類似した菌種であっても高精度な判別を可能としている。また、ファブリー病のスクリーニングシステムでは、尿沈渣顕微鏡写真からマルベリー小体を自動検出する技術を実現した。早期発見により適切な治療が可能となるため、学校検尿との連携による効率的なスクリーニング実現を目指している。これらのサービスはコンテナ化しているが、使用頻度の変動に対応したコスト最適化と運用効率化を目的とし、サーバレスアーキテクチャへの移行を進めている。この過程で、電子カルテ端末からの安全な利用を実現するため、ゼロトラストセキュリティモデルの実装についての検討も行った。サーバレスアーキテクチャは、その特性上、従来のネットワーク境界に依存したセキュリティ対策ではなく、アイデンティティベースのアクセス制御を前提としており、ゼロトラストの実装に適している。さらに、医療機関のクラウド移行を支援するため、主要クラウドプロバイダのセキュリティサービスについて包括的な比較調査を実施した。セキュリティ監視、アクセス制御、データ保護、リスク管理の各領域において、プロバイダ間でのサービス機能の対応関係を体系的に整理し、要求に応じた最適なサービス選定の指針を提供した。本研究を通じて、医療 AI サービスの実用化に向けた技術的課題の解決とともに、セキュリティ面での実証を重ねることで、患者および市民の参画を促し、さらなる医療技術の発展につなげることを目指している。特に、電子カルテネットワークからの安全なアクセスの実現は今後の重要な課題であり、セキュリティ対策の実績を積みながら、管理者や患者、市民に対する分かりやすい説明を継続的に行っていく必要がある。

A. 研究目的

ディープラーニングによる画像認識の飛躍的な精度向上はその後の社会を大きく変えることとなった。皮膚がんの診断など医療における AI の有用性が示されて以来、医療の質や効率の向上、地域格差の解消、医療従事者の負担軽減などを目指した医療 AI の研究開発が盛んに進められている。自動車の自動運転や、世界最強棋士を破った囲碁プログラムで注目を浴びた強化学習についても、個別医療の最適化、手術に使われる医療ロボットの制御など、さまざまな活用が考えられている。これらの技術はハードウェアとソフトウェアの技術開発をも促進してきた。その結果、さまざまな実行環境がクラウドとオンプレミスで構築された複雑なシステムの上に組み合わされている状況を作り出し、一方で個人情報保護や患者不利益等への配慮が求められる時代背景にあって、ランサムウェアをはじめとするサイバー攻撃の危険性がますます高まっている。

我が国では内閣府が主導する戦略的イノベーション創造プログラムにより AI ホスピタルの取り組みが 2018 年から始まり、国立成育医療研究センター(NCCHD)は、医療 AI プラットフォーム技術研究組合(HAIP)とともに採択され、医療データを共有し、一体となって AI 開発を進めてきた。国内多くの医療機関が、このようなサービスを、安全に、安価に利用できる環境を提供することを目的に、共同で調査等も行っている。いずれ、カルテ端末、さらには患者を含めた一般市民の端末からも利用されることを目指すには、どのような対策が必要かを考る必要がある。

現在、HAIP サービス事業基盤において、感染症起因菌同定支援、腎細胞がん病理画像のグレーディング支援、ファイブリー病スクリーニングの 3 つの医療 AI サービスがコンテナとして実装されており、公開範囲は限定されているものの、利用できる状況にある。ここでは、感染症起因菌同定支援、ファイブリー病スクリーニングについて報告する。また、近年の生成 AI の医療への活用は無視できるものではなく、NCCHD では医療的ケア児の支援体制、遺伝カウンセリング支援について開発を進めており、以下では後者について現状を報告する。

これらのサービスは Linux サーバにおいてウェブアプリケーションとして開発され、開発効率の向上、運用コストの削減、運用管理の簡素化、柔軟性の向上などを目的としてコンテナ化を行い、さらに、医療データを扱うという観点からセキュリティを強化するためにデスクトップ仮想化(VDI)を行ってクラウドから公開されている。現在、それぞれに対し、サーバレス環境への移行を進めており、その際にゼロトラストセキュリティモデルを実装し、電子カルテ端末からの利用、また一般ユーザからの安全な利用と普及を目指している。現在の AI 技術は教師あり学習に基づいており、実用化においては質と量の両方を伴ったビッグデータの収集が不可欠である。個人情報保護の観点からの制約により、思うように研究開発が進んでいない面もあるが、安全なシステムの実証により患者および市民の参画(PPI)を促し、さらなる医療技術の発展へと繋げることができると考えている。

B. 研究方法

顕微鏡画像からの教師データ作成には Microsoft VoTT を用いた。ラベルと位置情報を JSON 形式で出力し、画像分類のための切り出しや、物体検出のための YOLO 形式への出力を Python スクリプトで行った。

感染症起因菌同定支援では、まず

TensorFlow を利用して画像の分類を試みた。データ拡張には Keras を利用した。ImageNet で訓練された Inception V3 の転移学習を Hitachi SR24000/DL1 を用いて実行した。物体検出については、Microsoft Azure コンピューティング インスタンスのサイズ Standard_NC12s_v3 を利用して構築された HAIP の AI 開発基盤を利用した。アルゴリズムは、PyTorch を基盤とする YOLOv5 を採用した。CentOS 7 に設定した YOLOv5 を用いて訓練を行い、物体検出モデルを作成した。

ファブリー病スクリーニングでは、Amazon EC2 のインスタンスタイプ g4dn.xlarge を利用した。Amazon Linux 2 に設定した YOLOv8 を用いて訓練を行い、物体検出モデルを作成した。

コンテナ作成は、CentOS 7 に設定した Docker にて行い、デプロイ確認は Minikube を利用した。ウェブアプリケーションとしての公開は Amazon ECS を利用し、また、HAIP ラボ基盤、およびサービス事業基盤からの公開は Azure Kubernetes Service を利用した。VDI クライアントは Microsoft Remote Desktop、サーバは Azure Virtual Desktop でクラウドの Windows にアクセスし、そのブラウザから HAIP ラボ基盤、およびサービス事業基盤にデプロイされているコンテナにアクセスさせた。ウェブカメラの制御は JavaScript のメディアストリーム API に含まれている getUserMedia を利用し、クラウドの Windows に接続されているデバイスを動作させた。

遺伝カウンセリング支援は、Amazon SageMaker から AWS SDK for Python を利用して Amazon Bedrock を利用する環境を構築し、オレゴンリージョンの Anthropic Claude 3 Sonnet および Claude 3.5 Sonnet を利用して比較を行った。サービス間のアクセス許可は AWS IAM のロール作成にて行った。RAG は最初は Amazon Kendra にて構築したが、後に Amazon Bedrock Knowledge Bases の利用に移行した。

サーバレスコンピューティングは、AWS Lambda に加え、Amazon API Gateway、Amazon S3、Amazon CloudFront、AWS WAF を用いて基本的なウェブサービスを構築し、必要に応じて Amazon Bedrock などを組み込んだ。サービス間のアクセス許可については AWS IAM を利用した。

C. 研究結果

小児科として高度先進医療を提供する NCCHD は、免疫不全、臓器移植後に免疫抑制剤の投与を受けているなど、感染症に関してハイリスクな患者を多数抱えている。適切な抗生物質の選択など治療方針の決定は患者の予後に直結し、また不必要な抗生物質の使用は耐性菌の問題もあり、責任ある対応が求められている。そこで菌血症患者の検体の顕微鏡写真から起因菌を迅速に同定する医療 AI の開発を行なった。

小児の菌血症患者の血液培養からグラム染色を行なって得られた顕微鏡写真に、生化学反応や質量分析によって決定された細菌や真菌の種類を正解ラベルとして教師データを作成した。まず、10 μm 四方のクロップ

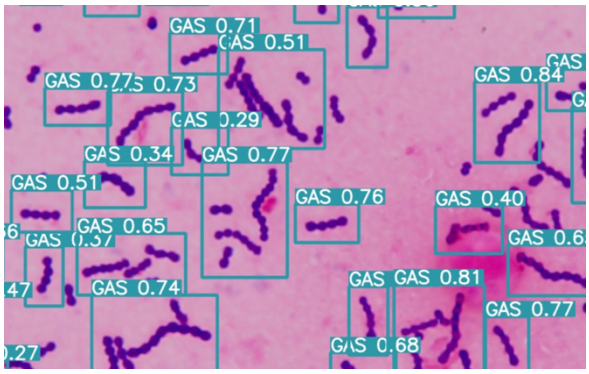

図 1 人食いバクテリア、化膿レンサ球菌の検出

に対してアノテーションを行い、グラム陽性桿菌、グラム陰性桿菌、グラム陽性球菌、グラム陰性球菌、それから背景の 5 分類を試みた。Inception V3 の転移学習により訓練を行ったモデルに対し、ランダムに切り出した 10 μm 四方のクロップでテストを行った。多数のクロップに対する結果のうち、背景を除いた多数決を取ることで良好な結果が得られることを確認した。

感染症起因菌をより詳しく同定するため、15 細菌および 1 真菌を物体検出により区別するアノテーションを行なった。内訳は、腸内細菌科、緑膿菌、エンテロコッカス属、コアグラーゼ陰性ブドウ球菌、バシラス属、黄色ブドウ球菌、B 群 β 溶血性レンサ球菌、レンサ球菌属、ヘモフィルス属、肺炎レンサ球菌、化膿レンサ球菌、リステリア、シュードモナス属、コリネバクテリウム、グラム陰性球菌、カンジダであり、これらに赤血球を加えた 17 ラベル、23,753 枚の写真から 347,234 クロップの切り出しで訓練を行なった。モデルは YOLOv5x を採用し、V100 を搭載する HAIP の AI 開発基盤で、150 エポック 34 時間をかけて独自モデルを完成させた(図 1)。本システムでは、互いに異なる培養条件に対応する複数の学習済みモデルを構築し、判別対象菌の培養条件に応じたモデルを選択して解析を行うことで、外観が類似した菌種であっても高精度な判別を可能としており、この点については特許を出願した。

図 2 VDI でクラウドのウェブカメラを利用

扱う医療データを安全にやり取りする目的で、コンテナを VDI 環境で公開している。ユーザはリモートデスクトップクライアントを利用して、クラウドのブラウザにアクセスし、デスクトップ画像の通信で利用する形態である。顕微鏡写真はデータをアップロードすることもできるが、顕微鏡に接続されたコンピュータからの簡易的な利用を見据え、ディスプレイに表示された画像をウェブカメラで撮影して検出できるように設計されている(図 2)。その際には、ユーザが手元で操作するウェブカメラからのリアルタイム入力は、VDI によりクラウド側に存在するウェブカメラと直結している。

次にファブリー病であるが、この疾患は分解酵素の欠失や活性の低下により不必要な糖脂質が細胞内に蓄積し、年月を経て体全体に障害を与える先天性の代謝異常症である。10 歳頃になって手足の痛みなどの症状が現れるが、診断は難しく、原因が判明した頃には心臓や腎臓などの損傷が進み、40 歳頃に亡くなるケースが多々見られる。酵素補充療法などの治療が確立しているので、患者や家族にとっては早期に発見することがきわめて重要となる。

患者の尿には、糖脂質が蓄積した糸球体上皮細胞由来の特異的な形状の物体が観察されることが報告されていて、マルベリー小体と呼ばれている。NCCHD では独自にサンプルを収集し、顕微鏡写真にマルベリー小体が写っているか否かを判別できる医療 AI モデルを開発し発表した。わずか 240 枚の写真しかないが、尿に含まれるマルベリー小体、マルベリー小体様物質、赤血球、白血球、扁平上皮細胞、精子、細菌、結晶に加え、その他の計 9 種類を識別する物体検出モデルを作り、ブラウザから利用できるようにした(図 3)。

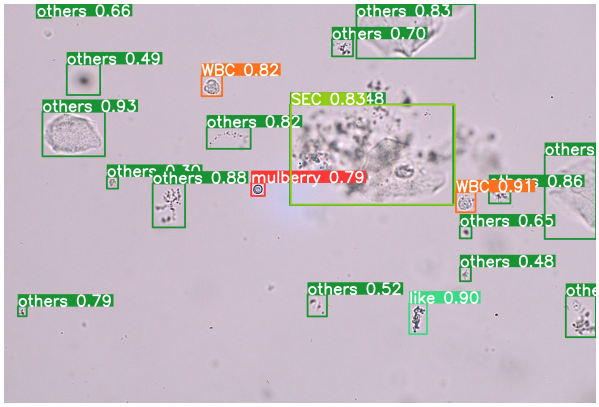

図 3 尿沈渣顕微鏡写真からのマルベリー小体検出

日本人における頻度は欧米人と比べて高く、7000 人に 1 人と言われている。7000 検体に 1 検体、マルベリー小体が存在するか否かを医師や臨床検査技師が手作業で調べることはきわめて苦痛で困難であり、見落としも多くなると考えられる。マルベリー小体はあったとしても、多数確認されるわけでもない。この物体検出は動画にも対応しており、実際には、大量の写真あるいは動画を自動的に撮影し、自動的に検出するスクリーニングとしての開発を進めており、毎年各学年で行われる学校検尿と結びつけた社会実装を目指している。

最後に、遺伝カウンセリングを生成 AI で代替する試みであるが、まず、日本遺伝カウンセリング学会と日本人類遺伝学会が実施している認定遺伝カウンセラーの認定試験でどれほどの点数を取ることができるのか確認してみた。大規模言語モデルは Amazon Bedrock から API を介して Claude 3 Sonnet を利用し、2020 年度の基礎問題全 26 問の日本語原文をプロンプトとして入力したところ、正解率は 48%であった。選択肢を正解まで絞り切れていない回答が 11 問あり、これらには半分の点数を与えて計算しているが、合格レベルにはない状況である。2024 年 6 月末、Claude 3.5 Sonnet が発表されたので改めて試したところ、正解率は 85%で合格レベルまで跳ね上がった。試験問題を解答するようシステムプロンプトとして指示を与えているだけでこのような結果が得られ、最近では基盤モデルとも呼ばれる大規模言語モデルは日進月歩の改良が進められていることがよく分かる。正解が得られなかった点については、関連情報を含むウェブページの HTML を集め、RAG(検索拡張生成)の構築により正解を出力できるよう改変することができた。

マルチモーダルであるため、家系図を理解することもでき、関連する論文を PDF のまま読み込んで患者向けに分かりやすい情報提供を行うこともできる。実際のカウンセリングにおいても、役に立つ情報を引き出せて

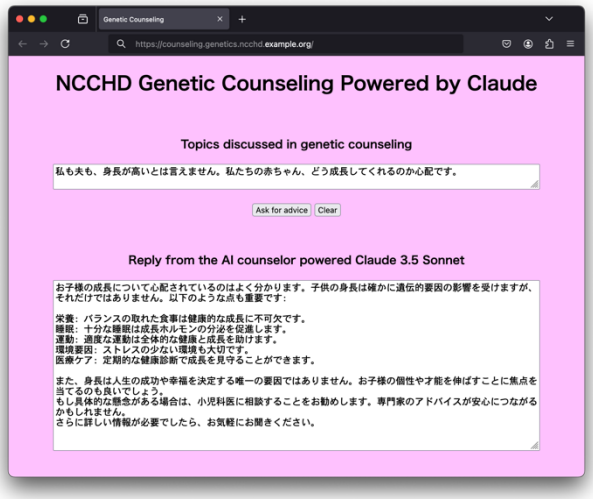

図 4 遺伝カウンセリングを生成 AI で代替

いるが(図 4)、そもそも医師の指導のもとに行われなければならず、ハルシネーションやプライバシーの問題など解決しなければならない問題が多く残っている。

これら医療 AI サービスは開発段階ということもあるが、そうでなくとも使用頻度が高いとは言えず、クラウドの仮想マシンやコンテナとしての運用では、24 時間 365 日の連続稼働となり、ほとんど使われていないのに課金される状態が続くことになる。これに対し、サーバレスアーキテクチャを採用した場合は必要最小限のリソースで、API のコール数とデータ転送量に対してのみ課金が発生するため、コストを大幅に下げることが可能である。サーバーのセットアップ、メインテナンス、スケーリングといったインフラ管理からも解放される。各コンポーネントには自動的に復旧される仕組みも備わり、耐障害性の高い仕組みを作り上げることができ、作業を進めている(図 5)。

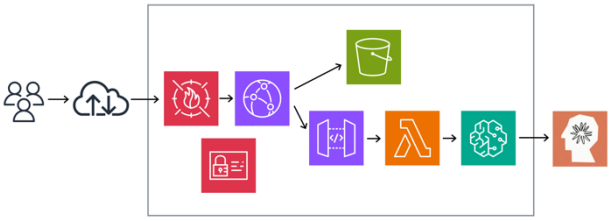

図 5 サーバレスのビルディングブロック例

最後に、医療機関のクラウド移行におけるセキュリティサービス選定を支援するため、主要クラウドプロバイダのセキュリティサービス群に関する比較調査研究を実施した。各社が提供する有償・無償セキュリティサービスについて、サービス名称の相違による選定困難性の課題に着目し、機能要件に基づく対応関係の分析を行った(資料)。調査により、セキュリティ監視、アクセス制御、データ保護、リスク管理の各領域において、プロバイダ間でのサービス機能対応を体系化し、組織のセキュリティ要求に応じた最適なクラウドセキュリティサービス選定のための実践的指針を提供した。

D. 考察

従来のクラウドコンピューティングでは、1 つの仮想マシンに数多くのサービスや機能を持たせ、運用を行っていたが、スケーラビリティ、独立性、柔軟性、コスト効率、開発速度などの点からクラウドプロバイダ自体がマイクロサービスアーキテクチャに移行し、クラウドユーザに対して各種多様なサービスを提供している。これらがサーバレスのビルディングブロックとなり(図 5)、仮想マシンが不要となる。クラウド上でサーバが不要になるわけではなく、ユーザが用意する仮想マシンが不要になることがサーバレスである。

プロバイダ側の利点は、そのままユーザ側の利点ともなる。セキュリティの観点では、攻撃範囲の限定、範囲が狭いことによる迅速な脆弱性対応、動的な実行環境による攻撃対象からの回避、細粒度必要最小限の権限付与によるリスクの低減、ブロックに特化した対策に集中、監視ログの細分化による問題特定の容易化、そしてセキュリティ技術の入れ替えも細分化されていればその一つ一つは決して困難ではない。このような状況では、従来のネットワーク境界に依存したセキュリティ対策は成り立たず、マイクロサービスアーキテクチャの欠点のようにも見えてしまうが、アイデンティティによるアクセス制御、つまり ID ベースのアクセス制御が必要になる。これは、ゼロトラストと盛んに言われる以前から、クラウドプロバイダ側には当然の対策であった。イベント駆動型のサーバレスコンピューティングサービスの中で最も歴

史が長く、機能も充実していると思われる AWS Lambda では、SigV4 というリクエスト署名によるクライアント認証により、実行権限のある正当なユーザから出された改竄されていないリクエスであることが確認される。ユーザー管理、グループ管理、ロールベースのアクセス制御、ポリシー管理は AWS IAM によって行われ、Microsoft Azure や Google Cloud では、それぞれ、Microsoft Entra ID、Google Cloud IAM が対応する。そしてサーバレス環境では、データの保存や転送時の暗号化が標準的に行われている。サーバレスを採用することでそのままゼロトラストセキュリティモデルを実現することができるわけではないが、見通し良くある程度のセキュリティを確保できそうである。

このような状況でも、実際の電子カルテネットワークから医療 AI サービスへのアクセスは許されておらず、現状インターネット側に出て行けるのは、NTP サーバとの同期、MDM サーバの認証のみとのことで、逆向きに、サービス側からのアクセスは言うまでもなく許されていない。

E. 結論

開発を行った医療 AI サービスに対し、運用コストの面からサーバレスへの移行を進めているが、マイクロサービスアーキテクチャはゼロトラストの実装を容易にする特性を多く持っており、掴みどころがないように思われたゼロトラスに対する理解を深めることができた。一方、ゼロトラストを謳う統合的なサービスの仕様を眺めると、やはり複雑で分かりにくく、必要性が不明な高機能、それに付随する高価格を目にすれば、気安く導入できるようなものではない。実際、目標とする電子カルテからのアクセスは実現できておらず、ゼロトラストの言葉をもって管理者、患者や市民に安心を与えられるわけではない。ゼロトラストセキュリティは開発者側を鼓舞する上で便利な言葉ではあるものの、ユーザ側を納得させ、医療 AI サービスのより広範な活用を図るためには、セキュリティ対策の実績を積むとともに、分かりやすい説明を続けるという地道な作業が必要であるように思われる。

F. 健康危惧情報

総括研究報告書に記載

G. 研究発表

岡村 浩司, 松井 俊大. 電子カルテ端末からの利用を見据えた医療 AI サービスの開発. *医療情報学*, 2024, **44(Suppl.)**, 354-357

岡村 浩司. 医療×AI: AWS の生成 AI サービスと切り拓く医療の新時代 —遺伝カウンセリングへの活用に向けて—. *ITvision*, 2024, **52**, 19

H. 知的財産権の出願

松井 俊大, 岡村 浩司. 菌種判別装置、菌種判別方法および菌種判別プログラム. 特願 2025-018598 (2025 年 2 月 6 日)

資料　クラウドプロバイダのセキュリティサービスの比較

ユースケース	A社	費用	O社	費用
ID とサービスおよびリソースへのアクセスを安全に管理	AWS Identity and Access Management (IAM)	無償	IAM Identity Domains	無償/有償
複数のアカウントやアプリケーションへのワークフォースのアクセスを一元管理	AWS IAM アイデンティティセンター (SSO の後	無償	IAM Identity Domains	無償/有償
安全でフリクションレスなカスタマー ID およびアクセス管理の実装と拡張	Amazon Cognito	有償	IAM Identity Domains	無償/有償
カスタムアプリケーション内できめ細かい権限と承認を管理	Amazon Verified Permissions (プレビュー)	有償	IAM Identity Domains	無償/有償
フルマネージドのマイクロソフトアクティブディレクトリサービスで効率化	AWS Directory Service	有償	-	-
複数のアカウント間でリソースを簡単かつ安全に共有	AWS Resource Access Manager	無償	OCI（built-in）	-
リソースをスケーリングする際に、環境を一元管理	AWS Organizations	無償	OCI（built-in）	-
セキュリティチェックの自動化とセキュリティアラートの一元化	AWS Security Hub	有償	Cloud Guard	無償
インテリジェントな脅威検出でアカウントを保護	Amazon GuardDuty	有償	Cloud Guard /Threat Intelligence	無償
大規模な自動化された継続的な脆弱性管理	Amazon Inspector	有償	Vulnerability Scanning	無償
数ステップでセキュリティデータを自動的に一元化	Amazon Security Lake	有償	Observability & Management Logging/Logging Analytics	有償
リソースの設定を評価、監査、評価する	AWS Config	有償	Cloud Guard	無償
オンプレミスおよびクラウド上のリソースとアプリケーションを観察および監視	Amazon CloudWatch	無償/有償	Observability & Management	有償
ユーザーアクティビティと API 使用状況の追跡	AWS CloudTrail	無償/有償	Cloud Guard /Threat Intelligence	無償
			Observability & Management Logging/Logging Analytics	有償
IoT デバイスとフリート全体のセキュリティ管理	AWS IoT Device Defender	有償	-	-
アカウント全体のファイアウォールルールを一元的に構成および管理	AWS Firewall Manager	有償	VCN, Security List, etc	無償
VPC 全体に Network Firewall セキュリティをデプロイ	AWS Network Firewall	有償	Network Firewall	有償
マネージド DDoS 保護でアプリケーションの可用性と応答性を最大化	AWS Shield	無償/有償	OCI（built-in） Layer3,4	
VPN なしで企業アプリケーションに安全にアクセス	AWS Verified Access	有償	IAM Identity Domains	無償/有償
一般的な攻撃からウェブアプリケーションを保護	AWS Web Application Firewall (WAF)	有償	Web Application Firewall	有償
VPC のアウトバウンド DNS トラフィックのフィルターと制御	Amazon Route 53 Resolver DNS Firewall	有償	-	-
大規模な機密データを検出して保護する	Amazon Macie	有償	Data Safe	無償
データを暗号化またはデジタル署名するためのキーを作成および管理	AWS Key Management Service (AWS KMS)	有償	Vault	無償/有償
シングルテナントのハードウェアセキュリティモジュール (HSM) の管理	AWS CloudHSM	有償	Vault	無償/有償
サービスと接続されたリソースを使用した SSL/TLS 証明書のプロビジョニングと管理	AWS Certificate Manager	無償	Certificates	無償
リソースを識別してデータを保護するためのプライベート証明書を作成	AWS Private Certificate Authority	有償	Certificates	無償
シークレットのライフサイクルを一元的に管理	AWS Secrets Manager	有償	Vault	無償/有償
セキュリティデータを分析および視覚化して、潜在的なセキュリティ問題を調査	Amazon Detective	有償	Cloud Guard	無償
			Logging Analytics（OCI Auditログ, VCN Flowログ）	有償
スケーラブルでコスト効率性に優れたアプリケーションの復旧	AWS Elastic Disaster Recovery	有償	OCI（built-in）	-
コンプライアンスレポートにオンデマンドでアクセスできるセルフサービスポータル	AWS Artifact	-	Oracle Cloud Compliance	-
使用状況を継続的に監査して、リスクとコンプライアンスの評価を簡素化	AWS Audit Manager	有償	Cloud Guard	無償