PaloAltoNetworks.NetSec-Architect.v2026-07-27.q24

試験コード：	NetSec-Architect
試験名称：	Palo Alto Networks Network Security Architect
認証ベンダー：	Palo Alto Networks
無料問題の数：	24
バージョン：	v2026-07-27
ページの閲覧量：	106
問題集の閲覧量：	270

https://www.jpnshiken.com/shiken/PaloAltoNetworks.NetSec-Architect.v2026-07-27.q24.html

質問: **1**
包括的なプロファイリングカバレッジを実現するには、IoTデバイスとどのインフラストラクチャコンポーネント間の経路にIoTセンサーを配置すべきでしょうか？
A. IoTゲートウェイ
B. DNSサーバー
C. SNMPコレクター
D. DHCPサーバー
正解: **(**正解を表示します**)**
DHCPトラフィックは、MACアドレス、ホスト名、ベンダークラス識別子、IPアドレス割り当てなど、IoTデバイスの正確なプロファイリングに不可欠な重要なデバイス識別属性を提供します。IoTセンサーをデバイスとDHCPサーバー間の経路に配置することで、初期ネットワーク接続時に包括的な可視性が確保され、信頼性の高い識別と分類が可能になります。

質問: **2**
ある組織は、すべてのセキュリティポリシーにおいて、IDおよびロールベースのアクセスグループ、デバイスセキュリティ、コンテンツ検査の活用に重点を置いたゼロトラストフレームワークを採用するよう指示を受けています。この目標を達成するために、高度な脅威対策、IoTセキュリティ、GlobalProtectを含むエンタープライズライセンス契約（ELA）が購入されました。
現在のセキュリティアーキテクチャでは、Panoramaを使用して60台の次世代ファイアウォール（NGFW）を管理しています。これらのNGFWは、PA-3240、PA-1410、PA-440が混在しています。PA-3240が設置されているサイトでは、プライベートアプリケーションリソースがトラストデータセンターゾーンにホストされています。すべてのサイトには、インターネットアクセス用のアントラストゾーンと、管理対象および管理対象外のエンドポイントデバイス用のユーザーゾーンがあります。PAN-OS SD-WANを介してサイト間接続を確立するために、トランジットメッシュゾーンが存在します。
プライベートホスト型アプリケーションには、Webサーバー、SMBおよびNFSファイルサーバー、ホスト型Active Directoryなどが含まれます。組織はこれらのプライベートアプ

リケーションにグループマッピング制限を導入する作業を進めており、グループは日々追加されています。また、データセンターを擁する大規模オフィスでホストされる、データチームの複雑なクエリ処理を支援するAIアプリケーションの構築も計画しており、パブリッククラウドでのホスティングも検討しています。
組織はオンプレミスのExchange、Dropbox、Zoom、ChatGPTを使用しています。さらに調査が必要な、いくつかのシャドウSaaSアプリケーションが存在します。ユーザーは、個人のログイン情報を使用してGoogleドライブ経由で機密ファイルを組織内にアップロードしていました。
ネットワーク上のIoTデバイスは、ユーザーゾーン上の専用VLANに接続されます。デバイスセキュリティ機能を使用することで、すべてのIoTデバイスは中程度または高信頼度の資産プロファイルに基づいて分類され、ポリシーセットがPanoramaにインポートされ、IoTネットワークに対してデフォルトの拒否設定が適用されます。
同組織はSSL復号化を導入し、コンテンツフィルタリングの大部分にURLカテゴリ分類を使用している。悪意のあるカテゴリ、未知のウェブサイト、高リスクのウェブサイトはブロックされ、残りのサイトは警告が表示されるように設定されている。
既存の技術を用いて、組織環境における機密ファイルの外部流出を制限するために、アーキテクトはどのような対策を推奨すべきでしょうか？
A. Prisma Browserで、アクセスセキュリティルールとデータセキュリティルールを作成し、許可されていないファイル共有アプリケーションによるファイルアップロードを防止します。
B. SaaSセキュリティを使用してテナント制限を有効にし、個人ログインによる不正アプリケーションの使用を防止します。
C. App-IDを使用して、GoogleドライブのWebアップロードを拒否するポリシーを作成します。
D. Enterprise DLPを使用して、機密データを通知するカスタムデータパターンを作成し、そのカスタムデータパターンがアップロードされないようにブロックします。
正解: **(**正解を表示します**)**
App-IDは、特定のGoogleドライブアップロード機能を識別し、既存の次世代ファイアウォール（NGFW）セキュリティポリシーを使用して、アーキテクトがファイルアップロードを直接ブロックできるようにします。組織は既にSSL復号化を導入しているため、ファイアウォールはこのアプリケーションの動作を正確に把握して制御でき、既に導入済みの技術を使用して機密ファイルの漏洩を防ぐ最も適切な方法となります。

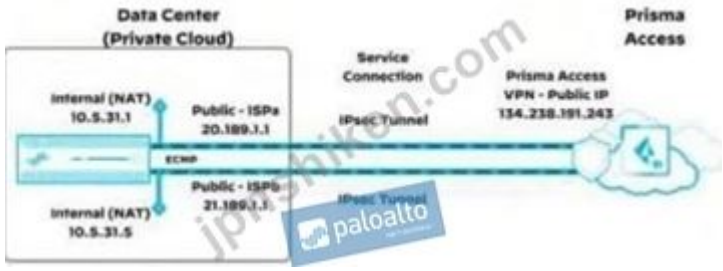
質問: **3**
あるグローバル企業は、モバイルワーカーとリモートオフィスのセキュリティを確保するためにPrisma Accessを全面的に導入し、ユーザーIDはOktaで管理しています。セキュリティチームは、ユーザーが自宅勤務かSD-WANデバイス経由で接続された支店勤務かに関わらず、ユーザーの所属部署に基づいて特定のSaaSアプリケーションへのアクセスを許可する、一貫性のあるセキュリティポリシーを作成したいと考えています。このユースケー

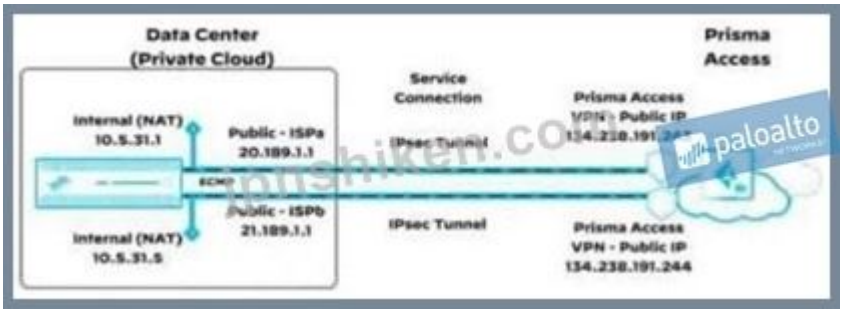
スにおいて、ポリシー適用に必要なユーザーとグループのマッピングをPrisma Accessで一貫して利用できるようにするには、どのようなアーキテクチャが最適でしょうか？
A. Palo Alto Networks User-IDエージェントをインストールし、OktaからPrisma Accessにユーザー情報を同期するように設定します。
B. PanoramaをデプロイしてPrisma Accessを管理し、Cloud Identity Engineを介してOktaからユーザーとグループ情報を取得するように設定します。
C. Prisma AccessとOkta間のSAMLフェデレーションを設定し、すべてのWebリクエストにユーザーIDを提供します。
D. 各リモートオフィスのSD-WANデバイスと各ユーザーのGlobalProtectクライアントを設定し、Oktaに直接ユーザー情報を問い合わせるようにします。
正解: **(**正解を表示します**)**
Panoramaが管理するPrisma Accessは、Cloud Identity Engineと連携して、モバイルユーザーとリモートネットワークの両方のユーザーおよびグループ情報を取得します。これにより、在宅勤務ユーザーと支店間で一貫したユーザーとグループのマッピングが可能になります。Cloud Identity EngineはIDソースとしてOktaをサポートしているため、Oktaの部門ベースのグループメンバーシップをPrisma Accessのポリシー適用に一元的に使用できます。

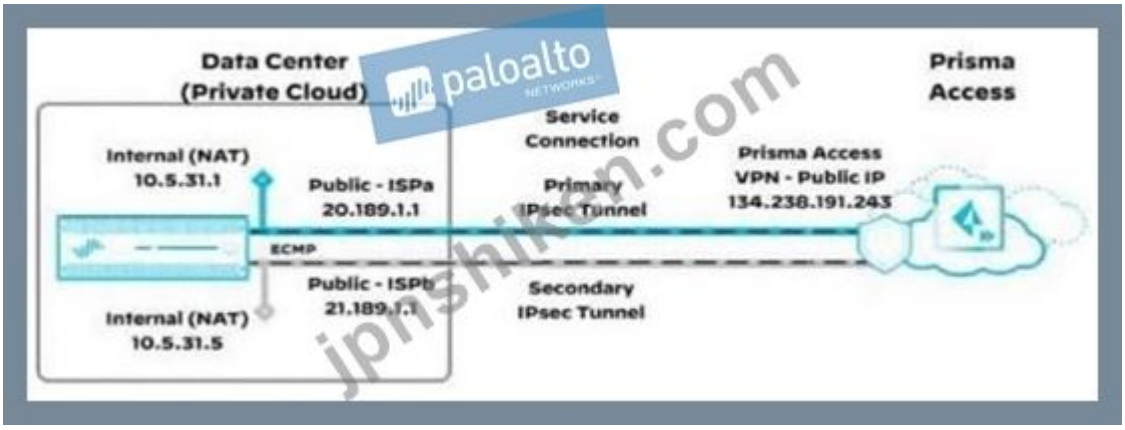
質問: **4**
企業は、データ漏洩を防ぎつつ、SaaSアプリケーションの利用を安全に可能にする必要がある。
このソリューションは、アプリケーションのトラフィックを可視化し、きめ細かな制御を可能にする必要があります。どのようなソリューションを使用すべきでしょうか？
A. URLフィルタリングのみ
B. データフィルタリング機能付きApp-ID
C. NATポリシー
D. スタティックルーティング
正解: **(**正解を表示します**)**
App-IDはポートやプロトコルに関係なくアプリケーションを識別し、データフィルタリングは機密データの漏洩を防ぎます。この組み合わせにより、可視性と制御の両方が実現します。URLフィルタリングだけでは、アプリケーション層のデータを詳細に検査してデータ保護要件を徹底することはできません。

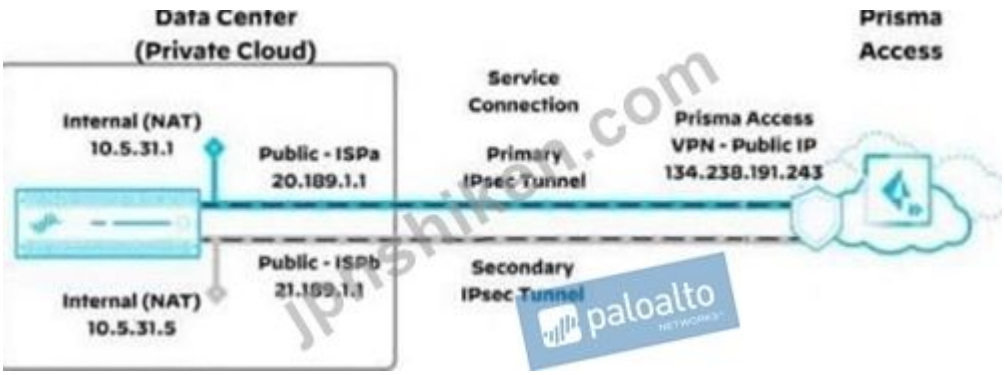
質問: **5**
グローバル製造企業は、合併・買収による急速な成長を目指す戦略計画を策定している。同社が購入したいくつかのコンポーネントは、親会社と競合する既存のIPアドレス体系と割り当てを持つ大規模な展開とみなされている。製造企業は、IPアドレスの再編計画を完了する前に、これらのリソースへのアクセスを確保する必要がある。

すべての展開にはさまざまなIoTデバイスが含まれており、経営陣は脆弱な資産の保護と、IoTデバイスに関連する既知のCVEの特定を求めています。ガバナンス、リスク、コンプライアンス（GRC）チームは、強制的な修復のために「重大（90以上）」のCVEスコアを報告するすべてのIoTデバイスを特定するために、包括的で否認不可能なログを必要としています。
スループットは現在の1Gbpsという傾向的な速度を上回る必要があり、予想される成長に伴い、間もなく5Gbpsにまで拡大するだろう。
セグメンテーションは必須要件であり、地域、デバイスの種類、機能に基づいてエンクレーブを構築する必要があります。
監査目的で、この詳細なリスクデータのIoTストレージ、整合性、および否認防止を保証するアーキテクチャコンポーネントはどれですか？
A. マスターキーで暗号化されたNGFWのセッションテーブル
B. セキュリティログとデバイステレメトリをクラウドに保存するためのStrata Logging Service
C. デバイスの状態を収集し、すべての重大な CVE スコアをローカルにログ記録する GlobalProtect エージェント
D. Panoramaログコレクターは、90日間の保持ポリシーを持つローカルデータベースを使用します。
正解: **B** (コメントを発表する)
Strata Logging Serviceは、整合性と否認防止を保証する集中型クラウドベースのログストレージを提供し、IoTテレメトリおよびセキュリティログが監査のために確実に保存されるようにします。
高スループット環境に対応できるよう拡張性があり、大規模な分散展開環境において重要なCVEスコアを持つデバイスを追跡するために必要な、長期的なデータ保持と分析をサポートします。

質問: **6**
ある組織が、自社のデータセンター向けにPrisma Accessサービス接続を設計しています。各データセンターは、インターネットへの10Gbpsの冗長リンクを備えています。各データセンターは、Prisma Accessに接続されたユーザーおよび支店からの最低1.5Gbpsのスループットをサポートする必要があります。このユースケースの要件を満たすソリューションを示す図はどれですか？
A.


B. 

C. 

D. 

正解: (正解を表示します)

この設計では、冗長なISPリンクと複数のアクティブなIPsecトンネルを介してECMPを使用し、トラフィックの負荷分散と集約を可能にします。これにより、必要なスループット（1.5Gbps以上）を確保しつつ、高い可用性と耐障害性を実現し、Prisma Accessサービス接続のベストプラクティスに準拠します。

質問: 7

ネットワークが検査を回避する暗号化された脅威にさらされている。最適な対策は何か？

A. すべてのHTTPSをブロックする

B. SSL復号化を有効にする

C. ログ記録を無効にする

D. 静的ルートを使用する

正解: (正解を表示します)

SSL復号化により暗号化されたトラフィックを検査し、隠れた脅威を明らかにすることができます。HTTPSをブロックすることは現実的ではなく、ログ記録を無効にしたりルーティングを調整したりしても、暗号化された脅威の可視性は確保されません。

質問: **8**
世界中にオフィスを持つ組織は、すべてのトラフィックを中央のデータセンターにバックホールするSD-WANソリューションを導入しています。多くのオフィスにはIoT/OTデバイスが設置されています。セキュリティアーキテクトは、この組織のセキュリティアーキテクチャを進化させるのに役立つゼロトラストネットワークソリューションを決定する際に、どのIoTセキュリティ要件を考慮する必要がありますか？
A. 正確な IoT / OT 検出には、Prisma SD-WAN ION または NGFW デバイスのいずれかが必要です。
B. ローカルセンサーは、DHCPサーバー上のエージェントとして、または仮想インフラストラクチャ上のコンテナとしてデプロイする必要があります。
C. IoT / OT 検出のため、すべての DHCP リクエストは Prisma SD-WAN ファブリックを経由する必要があります。
D. 組織は、執行のためにローカルのNGFWを用意する必要があります。
正解: **(**正解を表示します**)**
正確なIoT/OT検出には、デバイス間の通信が行われるローカルネットワークトラフィックを直接可視化する必要があります。これは、Prisma SD-WAN IONまたは次世代ファイアウォールを現場に導入することで実現でき、観測されたトラフィックとネットワーク動作に基づいて適切なデバイス識別とプロファイリングが可能になります。

質問: **9**
ある大規模組織では、Microsoft Azureの複数の可用性ゾーンに展開されたPalo Alto Networks VM-Seriesファイアウォールを使用しています。これらはAzure仮想マシンスケールセット（VMSS）によって管理され、トランジットVNet内での高可用性（HA）トラフィック検査のためにAzureロードバランサーと統合されています。
セキュリティチームは、アプリケーションのダウンタイムを最小限に抑えつつ、ファイアウォール群全体にわたって重要なPAN-OSソフトウェアのアップグレードを実施する必要があります。
Palo Alto Networksの高可用性クラウド展開に関するベストプラクティスに従って、ダウンタイムを最小限に抑えつつ、このソフトウェアアップグレードを安全に実行するための推奨されるアプローチは何ですか？
A. Azure VMSS のイメージを更新してから、インスタンスのアップグレードを開始します。
B. アップグレード中のヘルスチェックのフェールオーバーを処理するようにAzure Load Balancerプローブを構成する
C. 新しいPAN-OSバージョンを使用して新しい並列VMSSをプロビジョニングし、検証を行い、古いVMSSから新しいVMSSにトラフィックをリダイレクトします。
D. スケジュールされたメンテナンス期間中に、Azure Update Manager を使用して PAN-OS アップグレード パッケージをすべてのファイアウォール インスタンスに同時に直接プッシュします。

正解: **(**正解を表示します**)**
最も安全でダウンタイムが最小限に抑えられる方法は、ブルー/グリーン方式の置き換えです。ターゲットのPAN-OSバージョンを実行する新しい並列VMSSを構築し、完全に検証した後、古いスケールセットから新しいスケールセットにトラフィックをリダイレクトします。Palo Alto Networksのドキュメントでは、デプロイするPAN-OSバージョンに合わせてカスタムAzure VM-Seriesイメージを作成する方法が説明されており、アクティブな検査パスをその場でアップグレードするのではなく、検証済みの別のフリートを立ち上げることをサポートしています。Azureヘルスプローブは、更新中にインスタンスの健全性を判断するのに役立ちますが、稼働中のフリートをその場でアップグレードすることによるサービスの中断リスクを排除するものではありません。

質問: **10**
ある組織は、すべてのセキュリティポリシーにおいて、IDおよびロールベースのアクセスグループ、デバイスセキュリティ、コンテンツ検査の活用に重点を置いたゼロトラストフレームワークを採用するよう指示を受けています。この目標を達成するために、高度な脅威対策、IoTセキュリティ、GlobalProtectを含むエンタープライズライセンス契約（ELA）が購入されました。
現在のセキュリティアーキテクチャでは、Panoramaを使用して60台の次世代ファイアウォール（NGFW）を管理しています。これらのNGFWは、PA-3240、PA-1410、PA-440が混在しています。PA-3240が設置されているサイトでは、プライベートアプリケーションリソースがトラストデータセンターゾーンにホストされています。すべてのサイトには、インターネットアクセス用のアントラストゾーンと、管理対象および管理対象外のエンドポイントデバイス用のユーザーゾーンがあります。PAN-OS SD-WANを介してサイト間接続を確立するために、トランジットメッシュゾーンが存在します。
プライベートホスト型アプリケーションには、Webサーバー、SMBおよびNFSファイルサーバー、ホスト型Active Directoryなどが含まれます。組織はこれらのプライベートアプリケーションにグループマッピング制限を導入する作業を進めており、グループは日々追加されています。また、データセンターを擁する大規模オフィスでホストされる、データチームの複雑なクエリ処理を支援するAIアプリケーションの構築も計画しており、パブリッククラウドでのホスティングも検討しています。
組織はオンプレミスのExchange、Dropbox、Zoom、ChatGPTを使用しています。さらに調査が必要な、いくつかのシャドウSaaSアプリケーションが存在します。ユーザーは、個人のログイン情報を使用してGoogleドライブ経由で機密ファイルを組織内にアップロードしていました。
ネットワーク上のIoTデバイスは、ユーザーゾーン上の専用VLANに接続されます。デバイスセキュリティ機能を使用することで、すべてのIoTデバイスは中程度または高信頼度の資産プロファイルに基づいて分類され、ポリシーセットがPanoramaにインポートされ、IoTネットワークに対してデフォルトの拒否設定が適用されます。

同組織はSSL復号化を導入し、コンテンツフィルタリングの大部分にURLカテゴリ分類を使用している。悪意のあるカテゴリ、未知のウェブサイト、高リスクのウェブサイトはブロックされ、残りのサイトは警告が表示されるように設定されている。
アーキテクトは、ユーザーIDベースのルールを有効にし、アクセスを可能な限りソースに近い場所で制限または許可しつつ、運用上のオーバーヘッドを最小限に抑えるために、どの導入方法を提案すべきでしょうか？
A. データ再配布用のパノラマデバイステンプレート。プライマリおよびセカンダリパノラマをユーザーIDエージェントとして参照します。
B. ファイアウォールでのグループ更新時間を短縮するために、グループ許可リストを含むグループマッピングプロファイルを備えたPanoramaデバイステンプレート
C. SCIM を介したクラウド ディレクトリを使用して、ユーザー グループをクラウド アイデンティティ エンジンおよびファイアウォールに同期します。
D. クラウドアイデンティティエージェントがユーザーグループをクラウドアイデンティティエンジンおよびファイアウォールに同期します。
正解: **(**正解を表示します**)**
Cloud Identity Engineは、オンプレミスディレクトリ向けに軽量なCloud Identity Agentを使用し、SCIMはクラウドネイティブのIDプロバイダー向けです。この環境では、組織はオンプレミスでActive Directoryをホストしており、運用上のオーバーヘッドを抑えつつ、多数のファイアウォール間で拡張性と集中性を備えたユーザーおよびグループの同期を必要としています。そのため、Cloud Identity Agentを導入してユーザーグループをCloud Identity Engineとファイアウォールに同期させるのが最適です。

質問: **11**
ある企業が、社内ネットワーク内で横方向移動攻撃を受けました。このリスクを軽減するのに役立つ機能はどれですか？
A. NATルール
B. NGFWによる内部セグメンテーション
C. 静的ルート
D. QoSポリシー
正解: **(**正解を表示します**)**
次世代ファイアウォール（NGFW）を用いた内部セグメンテーションは、内部ゾーン間でセキュリティポリシーを適用し、横方向の移動を制限します。このアプローチは、セキュリティの強制機能を持たないNATやルーティングとは異なり、ネットワーク内部での検査とアクセス制御を実現します。

質問: **12**
ある小売企業は、在庫管理のために特定のサードパーティ製SaaS型AIアプリケーションの使用を承認したいと考えています。このアプリケーションは、機密情報がDMZ内で厳重に保護されている組織の内部サプライチェーンデータベースへのネットワーク層データアクセスを必要とします。CISOは、承認されたサードパーティ製AIアプリケーションが侵害さ

れ、内部データベースから顧客のPHデータが不正に持ち出される可能性があることを懸念しているため、実装が遅れています。CISOの懸念を解消できるソリューションはどれでしょうか？
A. 不正アクセス試行を監視するためにデータベースサーバーにAIエージェントをデプロイしたPrisma AIRS
B. Prisma AIRSとAI Securityのコンテンツアップデートにより、モデルの動作を検査し、異常なデータベースクエリをブロックします。
C. App-IDクラウドエンジンサブスクリプションによるアクセスセキュリティで、在庫管理アプリケーションを正確に識別し、完全にブロックします。
D. AIアクセスセキュリティとエンタープライズDLPサブスクリプションにより、SaaSアプリケーションとの間のトラフィック内の個人情報（PII）を識別してブロックします。
正解: **(**正解を表示します**)**
AIアクセスセキュリティと統合されたエンタープライズDLPは、SaaSアプリケーションとの間のトラフィックを検査し、顧客の個人情報などの機密データを検出できます。アプリケーションが侵害された場合でもデータ漏洩を防ぐポリシーを適用することで、組織は機密データを保護しながらAIアプリケーションを安全に承認できます。

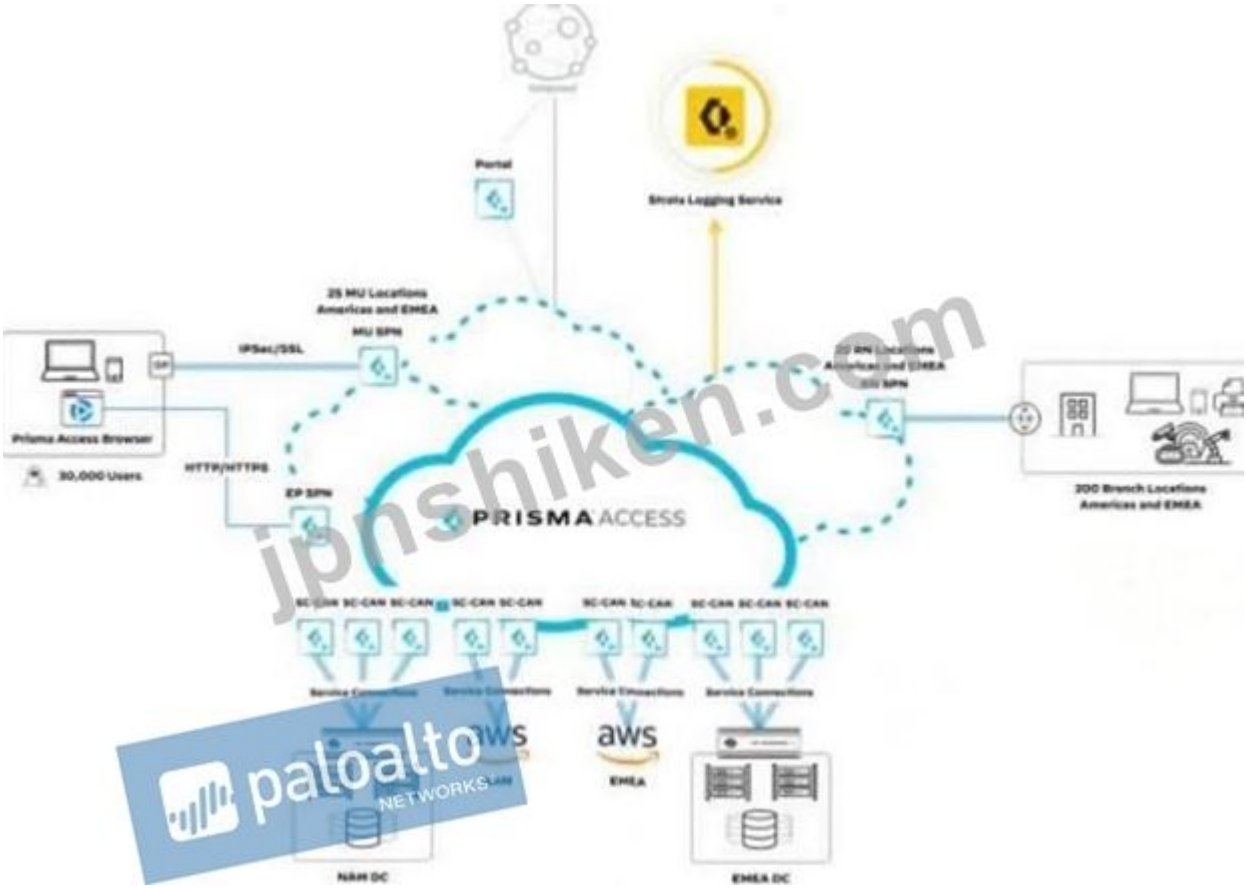
質問: **13**
あるグローバル企業がデータセンターとプライベートクラウドのインフラストラクチャを近代化している。その環境は以下の通りである。
- 重要な東西アプリケーションワークロードをホストするNutanix AHVクラスタ
- 高スループットワークロード（≥10 Gbps）をサポートする、マルチソケットホストを備えたVMware ESXiクラスタ
- 境界セキュリティを強化し、暗号化されたトラフィックの検査を大規模に処理するための新しいPA-5450ファイアウォール2台
南北方向と東西方向の両方のトラフィックフローに対して厳格なパフォーマンスサービスレベル契約（SLA）が適用され、TLS 1.3とIPSecに大きく依存している。
- KVM 上のネットワーク機能仮想化 (NFV) 環境は、パケット スループットを最大化し、レイテンシを最小化する高性能セキュリティ サービスを提供します。チーフ アーキテクトは、ファイアウォール設計がハイパーバイザの競合を回避し、非均一メモリ アクセス (NUMA) を最適化し、暗号化されたトラフィックにハードウェア機能を使用することを保証する責任を負います。
Nutanix AHV 上の VM シリーズ - リソース割り当て
Nutanixクラスタは既に高い負荷で使用されているため、アーキテクトの主な懸念事項は、仮想ファイアウォールのパフォーマンス低下を防ぐことです。シンプロビジョニングやバルーニングを行うと、レイテンシや予測不能性が発生する可能性があり、セキュリティに敏感なワークロードにとっては許容できません。
VMware ESXi 上の VM-Series - NUMA および vCPU の配置
VMware ESXi環境において、アーキテクトは10Gbpsを超えるワークロード向けにVM-Seriesを導入しています。NUMAノード間でvCPUを割り当てたり、コアを過剰に割り当て

たりすると、ソケット間のメモリアクセスやスケジューリングの遅延によりレイテンシが発生します。同様に、論理ハイパースレッドを専用化しても、必要な決定論的なデータプレーンのパフォーマンスは得られません。
運用統合と高可用性
適切なハイパーバイザーとハードウェアのプロビジョニングによってパフォーマンスが保証されるだけでなく、アーキテクトは高可用性（HA）も考慮に入れています。VM-SeriesペアはNutanixおよびVMwareクラスタ全体でアクティブ/パッシブHA構成で展開され、PA-5450はデータセンターの南北方向のセキュアな境界を構成します。これにより、不要な東西方向の検査ボトルネックを発生させることなく、耐障害性が確保されます。
推奨事項は、企業のSLAおよびCISOの暗号化トラフィックに関する懸念事項に合致した、拡張性と高性能を備えたファイアウォール導入案でなければならない。
PAN-OSのどの機能が、CISOが求める南北方向のトラフィック検査のニーズを満たすでしょうか？
A. 柔軟なネットワーク接続を実現する高密度DAC/QSFPポート
B. 管理トラフィックとデータトラフィックを分離するための専用アウトオブバンド管理ポート
C. HA（高可用性のための二重冗長ホットスワップ電源
D. SSL/TLS復号化およびIPSec処理をオフロードするための専用ハードウェア暗号エンジン
正解: **(**正解を表示します**)**
PA-5450に搭載された専用ハードウェア暗号化エンジンは、SSL/TLS復号化とIPSec処理をメインCPUからオフロードすることで、暗号化された南北トラフィックの高性能な検査を可能にします。これにより、ファイアウォールはTLS 1.3およびIPSecの負荷の高いワークロードを効率的に処理しながら、厳格なSLAを満たすことができます。

質問: **14**
建築家は、ユーザー向けに安全なリモートアクセスを設計する必要があります。最も適切なソリューションはどれでしょうか？
A. NATのみ
B. グローバルプロテクト
C. スタティックルーティング
D. VLANセグメンテーション
正解: **(**正解を表示します**)**
GlobalProtectは、ユーザー認証、デバイスの状態チェック、ポリシー適用機能を備えた安全なリモートアクセスを提供します。これにより、基本的なネットワーク構成と比較して、より安全な接続が保証されます。

質問: **15**
ある組織は、クラウドファーストのネットワークインフラストラクチャの構築を進めています。改訂されたアーキテクチャの一部として、以下の図に示すようにPrisma Accessが導

入されています。この組織は、データセンターおよびパブリッククラウド環境に展開されているPrisma Accessと次世代ファイアウォール（NGFW）の管理方法として、Strata Cloud Manager（SCM）を選択しました。サービス接続の終端、ネットワークのセグメント化、データセンターおよびパブリッククラウドのリソース保護のために、150台のNGFWが稼働しています。



耐障害性に関する要件の一つは、NGFWおよびPrisma Accessの導入環境において、高可用性のディレクトリサービスと認証機能を提供することである。
このシナリオにおいて、設計要件と顧客要件を満たす構成はどれですか？（2つ選択してください。）

A. LDAPサーバーに接続されたファイアウォールと、ディレクトリサービス用のLDAPサーバーへの接続を備えたクラウドアイデンティティエンジンに接続されたPrisma Access
B. RADIUS認証によるモバイルユーザー向けファイアウォールおよびPrisma Access
C. ファイアウォールと Prisma Access は、ディレクトリ サービス用の Entra ID に接続され、Cloud Identity Engine に接続されています。
D. SAML認証で構成されたモバイルユーザー向けのファイアウォールとPrisma Access

正解: **C,D** (コメントを発表する)

Entra IDに接続されたCloud Identity Engineは、次世代ファイアウォール（NGFW）とPrisma Accessの両方に対して、集中管理された高可用性のディレクトリサービスを提供します。これは、クラウドファースト設計とStrata Cloud Managerベースの運用に合致しています。SAML認証は、Prisma Accessモバイルユーザー向けに堅牢で最新のIDベース認証を提供し、クラウドIDプロバイダーとの連携も良好で、環境全体における高可用性認証の要件をサポートします。

質問: **16**
あるグローバル企業は、クラウドファースト設計への移行を進めながら、クラウドベースの移行中に重要なアプリケーションのセキュリティを確保する作業を進めており、現在、CRMや製品の知的財産／設計システムといった最も重要なアプリケーションをAzureクラウドへ移行する既存システム移行（ブラウンフィールド移行）を実施しています。同社は既に、複数のゾーンを持つアクティブ／パッシブ型の高可用性（HA）次世代ファイアウォール（NGFW）をデータセンターに導入しており、その設計を既存のAzure HA環境にも再現しています。
組織は、重要なワークロードがデータセンターから移行し、ユーザーがどこからでも接続するようになるにつれて、セキュリティ体制を近代化する必要性を認識しています。そのセキュリティモデルは、従来型の「ハードシェル、ソフトセンター」アプローチによって定義されています。
信頼のギャップをゼロに
現在のネットワークセグメンテーションは境界型である。組織は、クラウド環境とオンプレミス環境の両方にゼロトラストの原則を拡大したいと考えている。
- このネットワークは、主にオフィス所在地と大まかな部門グループごとに区分された、VLANとIPアドレスベースのアクセス制御リスト（ACL）に大きく依存しています。従業員が社内ネットワーク（つまり「境界内」）に入ると、比較的広い範囲にアクセスできるようになります。
攻撃者が単一のエンドポイントを侵害した場合（例えば、フィッシングメールを介して）、容易に横方向に移動して、価値の高いターゲットをスキャンすることができます。
雲の死角
- 当該組織は、本番環境にAzureを使用しており、機密性の高い顧客データを含むアプリケーションをホストしている。
クラウドにおけるセキュリティ制御は、オンプレミスネットワークとは独立して管理されることが多い。
アクセス権限は、ユーザーのリアルタイムの状況やアプリケーションの状態ではなく、リソースに基づいて、過度に寛容なIDおよびアクセス管理（IAM）の役割とキーによって付与されることが多い。
リモートユーザーアクセス
- 多くのリモートユーザーは、インターネットやSaaSリソースにアクセスするためだけに、依然として企業のデータセンターを経由する接続経路を使用しており、遅延や非効率性を引き起こしている。
- 従来型のVPNは、リモートワークを行う従業員に利用されています。
VPNは内部ネットワークセグメント全体へのアクセスを許可するため、リモートエンドポイントが新たな、より脆弱な境界となります。最初の接続後、ユーザーデバイスの状態を継続的に監視する機能はありません。
可視性とログ記録

ログは主にオンプレミス環境に保存され、その後ローカルのセキュリティ情報およびイベント管理（SIEM）ソリューションに転送されます。アプリケーションがAzureに移行すると、クラウドトラフィックとユーザー行動の可視性が断片化されます。
データセキュリティに関する懸念
製品設計ファイルを含む機密データは、今後SaaSおよびクラウド環境に保存されることになります。組織は、情報漏洩を防ぎ、コンプライアンスを徹底するために、データセキュリティ対策を講じる必要があります。
侵入セキュリティ
・第三者パートナーやサプライヤーはデータセンターやクラウドアプリケーションへのアクセスを必要とするため、アクセスポイントでリスクが生じる。
このシナリオにおいて、回復力を向上させ、運用コストを削減できるソリューションはどれでしょうか？
A. 既存のHAソリューションを、新しいアプリケーションに対応できる十分な容量で垂直方向に拡張する。
B. 既存の仮想ネットワーク（VNet）設計にクラウドNGFWを統合
C. 既存の仮想ネットワーク（VNet）に導入された集中型VMシリーズNGFW
D. 新しい仮想ネットワーク（VNet）における分散型VMシリーズNGFW
正解: **(**正解を表示します**)**
既存のVNet設計に統合されたクラウドNGFWは、顧客がVMベースのファイアウォールインフラストラクチャを運用・拡張する必要なく、Azure VNetトラフィックに対して管理されたクラウドネイティブなファイアウォール保護を直接提供するため、耐障害性を向上させ、運用オーバーヘッドを削減します。Palo Alto Networksは、Azure向けクラウドNGFWについて、集中管理されたルールスタックを通じてAzure仮想ネットワークトラフィックを保護すると説明しており、これは、拡大するクラウドファースト環境をサポートしながら、よりシンプルな運用へのニーズに合致しています。

質問: **17**
従業員5万人を擁し、35カ国に拠点を置くグローバル製造企業は、高度な産業機器を設計し、重要な知的財産を保有している。同社は競争の激しい市場で事業を展開しており、企業秘密の保護は市場優位性を維持するために不可欠である。

過去18か月間、CISOは組織全体で従業員が生産性向上のために数百ものGenAIアプリケーションを導入していることを発見した。エンジニアはAIコーディングアシスタントを使って製品開発を加速させ、営業チームはAIツールを使って提案書を作成し、カスタマーサービス担当者はチャットボットを使って返信文を作成している。こうした導入はイノベーションを促進した一方で、重大なセキュリティリスクも生み出している。
セキュリティ監査により、画像生成サービスにアップロードされた機密性の高いCADファイル、公開されているコーディングアシスタントと共有された独自のソースコード、プロンプトで使用された機密性の高い顧客情報が明らかになった。監査では、300種類以上のGenAIアプリケーションが使用されていることが判明したが、そのほとんどは正式な審査や承認を受けていなかった。
カスタマーサービス部門は、クラウド型大規模言語モデル（LLM）プラットフォーム上に構築されたカスタマーサービス・コパイロット、社内知識管理アシスタント、コードレビューツールなど、社内AIアプリケーションの開発も進めている。これらの社内アプリケーションは、機密性の高いデータベース、顧客記録、社内APIにアクセスするため、悪用や不正使用に関するセキュリティ上の懸念がさらに高まる。
組織は分散型の労働力構成を採用しており、従業員の60%がリモートワークまたはハイブリッド勤務で、管理対象デバイスと非管理対象デバイスを使用して様々な場所から企業リソースやAIアプリケーションにアクセスしている。既存のネットワークセキュリティインフラには、AIに特化したセキュリティ機能が不足している。
組織の経営陣は、包括的なセキュリティ対策を実施しながら、AIを活用したイノベーションを推進したいと考えています。CISOは、生産性を阻害することなく機密資産を保護する、組織全体を対象としたGenAIガバナンスプログラムの開発を任されています。このプログラムは、従業員が使用する外部AIアプリケーションと、IT部門が開発する内部AIアプリケーションの両方に対応する必要があります。
組織の戦略目標であるAIイノベーションの実現と機密資産の保護に最も合致するアーキテクチャアプローチはどれか？
A. AIトラフィックに対して標準的なURLフィルタリングとデータ損失防止（DLP）ポリシーを適用する既存の境界ファイアウォールとVPNコンセントレータに依存する。
B. 各データセンター内でネットワークゾーンをセグメント化し、AIワークロードを重要なIPアドレスリポジトリから分離し、東西トラフィックを監視する。
C. AI対応制御機能とIDおよびデバイス状態を統合したクラウドベースのセキュリティプラットフォームを導入する
D. ファイアウォールで外部のGenAIアプリケーションをブロックし、従業員が社内で開発されたAIアプリケーションを使用できるようにします。
正解: **C** (コメントを発表する)
AI対応の制御機能を備えたクラウドベースのセキュリティプラットフォームは、ユーザーの場所やデバイスに関係なく、承認済みおよび未承認のAIアプリケーション全体にわたって、一元的な可視性とポリシー適用を提供します。IDとデバイスの状態を統合することで、きめ細かなゼロトラストアクセスを実現し、機密データの外部流出を防ぎ、イノベーショ

ンを阻害することなく、外部開発および内部開発のAIアプリケーションの両方を保護します。

質問: **18**
ある企業は、強力なセキュリティを維持しながら、脅威検出における誤検知を減らしたいと考えている。
彼らはどうすべきだろうか？
A. セキュリティプロファイルを無効にする
B. セキュリティプロファイルと例外を調整する
C. すべてのトラフィックを許可する
D. ログ記録を削除
正解: **(**正解を表示します**)**
セキュリティプロファイルを調整し、例外を作成することで、保護を維持しながら誤検知を減らすことができます。プロファイルを無効にしたり、すべてのトラフィックを許可したりすると、セキュリティが損なわれます。

質問: **19**
グローバル製造企業は、合併・買収による急速な成長を目指す戦略計画を策定している。同社が購入したいくつかのコンポーネントは、親会社と競合する既存のIPアドレス体系と割り当てを持つ大規模な展開とみなされている。製造企業は、IPアドレスの再編計画を完了する前に、これらのリソースへのアクセスを確保する必要がある。
すべての展開にはさまざまなIoTデバイスが含まれており、経営陣は脆弱な資産の保護と、IoTデバイスに関連する既知のCVEの特定を求めています。ガバナンス、リスク、コンプライアンス（GRC）チームは、強制的な修復のために「重大（90以上）」のCVEスコアを報告するすべてのIoTデバイスを特定するために、包括的で否認不可能なログを必要としています。
スループットは現在の1Gbpsという傾向的な速度を上回る必要があり、予想される成長に伴い、間もなく5Gbpsにまで拡大するだろう。
セグメンテーションは必須要件であり、地域、デバイスの種類、機能に基づいてエンクレーブを構築する必要があります。
組織の要件を満たすために、建築家はどの出口ルートを推奨すべきでしょうか？
A. ZTNAコネクタ
B. サービス接続
C. GCPネットワーククラウドコネクタ
D. コロコネクト
正解: **D (**コメントを発表する**)**
Colo-Connectは、Prisma Accessとオンプレミス環境またはデータセンター環境との間で、高スループットのプライベート接続を提供し、マルチギガビット要件（1Gbpsを超えて5Gbpsまで拡張可能）をサポートします。大規模かつ高性能な環境向けに設計されてお

り、IPアドレスの再設定を即座に行うことなく、セグメンテーションとセキュアアクセスをサポートするため、このシナリオに最適です。

質問: **20**
ある企業は、検出された脅威に対して自動的に対応することを望んでいます。どのような対策を講じるべきでしょうか？
A. 手動応答
B. SOAR統合
C. 静的ルールのみ
D. アラートを無効にする
正解: **B** (コメントを発表する)
SOARは、検出と修復のワークフローを統合することで、インシデント対応の自動化を実現します。
これにより、手作業によるプロセスと比較して、応答時間が短縮され、一貫性が向上します。

質問: **21**
あるグローバル企業は、クラウドファースト設計への移行を進めながら、クラウドベースの移行中に重要なアプリケーションのセキュリティを確保する作業を進めており、現在、CRMや製品の知的財産／設計システムといった最も重要なアプリケーションをAzureクラウドへ移行する既存システム移行（ブラウンフィールド移行）を実施しています。同社は既に、複数のゾーンを持つアクティブ／パッシブ型の高可用性（HA）次世代ファイアウォール（NGFW）をデータセンターに導入しており、その設計を既存のAzure HA環境にも再現しています。
組織は、重要なワークロードがデータセンターから移行し、ユーザーがどこからでも接続するようになるにつれて、セキュリティ体制を近代化する必要性を認識しています。そのセキュリティモデルは、従来型の「ハードシェル、ソフトセンター」アプローチによって定義されています。
信頼のギャップをゼロに
現在のネットワークセグメンテーションは境界型である。組織は、クラウド環境とオンプレミス環境の両方にゼロトラストの原則を拡大したいと考えている。
- このネットワークは、主にオフィス所在地と大まかな部門グループごとに区分された、VLANとIPアドレスベースのアクセス制御リスト（ACL）に大きく依存しています。
従業員が社内ネットワーク（つまり「境界内」）に入ると、比較的広い範囲にアクセスできるようになります。
攻撃者が単一のエンドポイントを侵害した場合（例えば、フィッシングメールを介して）、容易に横方向に移動して、価値の高いターゲットをスキャンすることができます。
雲の死角

- 当該組織は、本番環境にAzureを使用しており、機密性の高い顧客データを含むアプリケーションをホストしている。
クラウドにおけるセキュリティ制御は、オンプレミスネットワークとは独立して管理されることが多い。
アクセス権限は、ユーザーのリアルタイムの状況やアプリケーションの状態ではなく、リソースに基づいて、過度に寛容なIDおよびアクセス管理（IAM）の役割とキーによって付与されることが多い。
リモートユーザーアクセス
- 多くのリモートユーザーは、インターネットやSaaSリソースにアクセスするためだけに、依然として企業のデータセンターを経由する接続経路を使用しており、遅延や非効率性を引き起こしている。
- 従来型のVPNは、リモートワークを行う従業員に利用されています。
VPNは内部ネットワークセグメント全体へのアクセスを許可するため、リモートエンドポイントが新たな、より脆弱な境界となります。最初の接続後、ユーザーデバイスの状態を継続的に監視する機能はありません。
可視性とログ記録
ログは主にオンプレミス環境に保存され、その後ローカルのセキュリティ情報およびイベント管理（SIEM）ソリューションに転送されます。アプリケーションがAzureに移行すると、クラウドトラフィックとユーザー行動の可視性が断片化されます。
データセキュリティに関する懸念
製品設計ファイルを含む機密データは、今後SaaSおよびクラウド環境に保存されることになります。組織は、情報漏洩を防ぎ、コンプライアンスを徹底するために、データセキュリティ対策を講じる必要があります。
侵入セキュリティ
- 第三者パートナーやサプライヤーはデータセンターやクラウドアプリケーションへのアクセスを必要とするため、アクセスポイントでリスクが生じる。
現在のMicrosoft Azure NGFWアーキテクチャでは、移行される新しいアプリケーションに伴うトラフィック増加に対応できません。
拡張性の高い検査を実現するアーキテクチャソリューションはどれでしょうか？
A. ファイアウォールペアを廃止し、Azure VPNゲートウェイのマルチリージョン展開を使用してVNet間接続を管理します。
B. ユーザー定義ルート (UDR) を使用してトラフィックを複数の同時ファイアウォールインスタンスに送り、検査を行うロードバランサーベースのオートスケーリングファイアウォールクラスタに移行します。
C. アクティブ/パッシブファイアウォールは南北方向のトラフィックのみに使用し、東西方向のトラフィック検査はAzureネットワークセキュリティグループ（NSG）に完全に依存します。

D. Azureのアクティブ/パッシブ設計を維持し、Azureスケールセットを使用してファイアウォールのサイズを垂直方向に拡張し、現在および将来予想されるすべての東西トラフィックを処理します。
正解: **(**正解を表示します**)**
VM-Series向けの拡張性の高いAzure設計では、固定のアクティブ/パッシブペアではなく、複数のアクティブなファイアウォールインスタンスを備えたロードバランサーを使用します。Palo Alto Networksは、ロードバランサーを使用してトラフィックを同時実行されるファイアウォールインスタンスに分散する高可用性Azureデプロイメントについてドキュメント化しており、VM-SeriesへのAzureルーティングは、ユーザー定義ルートを使用してトラフィックを検査パスに誘導します。そのため、ロードバランサーベースの自動スケーリングファイアウォールクラスタは、クラウド移行トラフィックの増加と拡張性の高い検査に適したアーキテクチャと言えます。

質問: **22**
従業員5万人を擁し、35カ国に拠点を置くグローバル製造企業は、高度な産業機器を設計し、重要な知的財産を保有している。同社は競争の激しい市場で事業を展開しており、企業秘密の保護は市場優位性を維持するために不可欠である。
過去18か月間、CISOは組織全体で従業員が生産性向上のために数百ものGenAIアプリケーションを導入していることを発見した。エンジニアはAIコーディングアシスタントを使って製品開発を加速させ、営業チームはAIツールを使って提案書を作成し、カスタマーサービス担当者はチャットボットを使って返信文を作成している。こうした導入はイノベーションを促進した一方で、重大なセキュリティリスクも生み出している。
セキュリティ監査により、画像生成サービスにアップロードされた機密性の高いCADファイル、公開されているコーディングアシスタントと共有された独自のソースコード、プロンプトで使用された機密性の高い顧客情報が明らかになった。監査では、300種類以上のGenAIアプリケーションが使用されていることが判明したが、そのほとんどは正式な審査や承認を受けていなかった。
カスタマーサービス部門は、クラウド型大規模言語モデル（LLM）プラットフォーム上に構築されたカスタマーサービス・コパイロット、社内知識管理アシスタント、コードレビューツールなど、社内AIアプリケーションの開発も進めている。これらの社内アプリケーションは、機密性の高いデータベース、顧客記録、社内APIにアクセスするため、悪用や不正使用に関するセキュリティ上の懸念がさらに高まる。
組織は分散型の労働力構成を採用しており、従業員の60%がリモートワークまたはハイブリッド勤務で、管理対象デバイスと非管理対象デバイスを使用して様々な場所から企業リソースやAIアプリケーションにアクセスしている。既存のネットワークセキュリティインフラには、AIに特化したセキュリティ機能が不足している。
組織の経営陣は、包括的なセキュリティ対策を実施しながら、AIを活用したイノベーションを推進したいと考えています。CISOは、生産性を阻害することなく機密資産を保護する、組織全体を対象としたGenAIガバナンスプログラムの開発を任されています。このプログ

ラムは、従業員が使用する外部AIアプリケーションと、IT部門が開発する内部AIアプリケーションの両方に対応する必要があります。
CISOは、GenAIのデータ漏洩を制御するために、どのような対策を推奨できますか？
A. Prisma AIRSを実装する
B. AIアクセスセキュリティの実装
C. 境界NGFWでUser-IDとApp-IDを設定する
D. Prisma AIRSを設定して、AIアプリケーションのプロンプト内でのデータ漏洩を監視する。
正解: **B** (コメントを発表する)
AIアクセスセキュリティは、外部のGenAIアプリケーションとのユーザーインタラクションを制御・管理するように設計されており、プロンプトとレスポンスの検査、機密データの漏洩を防ぐためのDLPポリシーの適用などが含まれます。分散ユーザー全体にわたるSaaSベースのAI利用に対してインラインで強制適用を行い、サードパーティのGenAIツールを通じて機密データが漏洩するリスクに直接対処します。

質問: **23**
グローバル製造企業は、合併・買収による急速な成長を目指す戦略計画を策定している。同社が購入したいくつかのコンポーネントは、親会社と競合する既存のIPアドレス体系と割り当てを持つ大規模な展開とみなされている。製造企業は、IPアドレスの再編計画を完了する前に、これらのリソースへのアクセスを確保する必要がある。
すべての展開にはさまざまなIoTデバイスが含まれており、経営陣は脆弱な資産の保護と、IoTデバイスに関連する既知のCVEの特定を求めています。ガバナンス、リスク、コンプライアンス（GRC）チームは、強制的な修復のために「重大（90以上）」のCVEスコアを報告するすべてのIoTデバイスを特定するために、包括的で否認不可能なログを必要としています。
スループットは現在の1Gbpsという傾向的な速度を上回る必要があり、予想される成長に伴い、間もなく5Gbpsにまで拡大するだろう。
セグメンテーションは必須要件であり、地域、デバイスの種類、機能に基づいてエンクレーブを構築する必要があります。
トラフィックの可視化とプロファイリングのために、ファイアウォールがタップモードで構成されています。プロファイリングにおいて、さまざまな動作が混在し、一貫性のない結果が観測されています。
その行動の根本原因として考えられるものを2つ挙げてください。（2つ選択してください。）
A. デバイスはNATデバイスの背後に配置されています
B. 非対称ルーティングは、TXトラフィックの可視性は提供するが、RXトラフィックの可視性は提供しない。
C. ハードコードされたMACアドレスは適切にプロファイリングできません
D. ネットワーク上でMACアドレスのなりすましが発生しています

正解: **(**正解を表示します**)**
デバイスがNATデバイスの背後にある場合、複数のエンドポイントが単一の送信元として認識される可能性があり、プロファイリングの精度が低下し、混在した動作や一貫性のない動作が誤って特定される可能性があります。非対称ルーティングも、ファイアウォールが通信の一方の側しか認識できないため、可視性が不完全になる原因となり、プロファイリングエンジンが正確な識別に必要なトラフィックパターン全体を観測できなくなる可能性があります。

質問: **24**
アーキテクトは、多数のアプリケーション仮想プライベートクラウド（VPC）を持つ大規模なAWS環境向けのセキュリティソリューションを設計しています。これらのアプリケーションは、多様で時には相反する受信セキュリティ要件を持っているため、単一の統一されたルールセットを作成および維持することは困難です。このソリューションは、異なるアプリケーショングループの受信トラフィックを保護すると同時に、AWS Transit Gatewayを介してすべての送信トラフィックと東西トラフィックを一元的に保護する必要があります。すべてのセキュリティ要件を満たしながら、受信トラフィックのルールの複雑さを軽減できる設計モデルはどれでしょうか？
A. トランジットゲートウェイモデルは、すべてのアプリケーションVPC間で直接ピアリング接続のフルメッシュを構築することにより、接続性を確立することに重点を置いています。
B. 論理アプリケーショングループ専用の受信NGFWと、東西トラフィックおよび送信トラフィック用の中央NGFWを組み合わせたモデル
C. アプリケーションVPCごとに個別の非接続セキュリティVPCをデプロイする分離モデル
D. すべての受信、送信、および東西トラフィックを単一の共有セキュリティVPC経由でルーティングすることにより、すべてのセキュリティ機能を統合する集中型モデル
正解: **(**正解を表示します**)**
複合モデルは、アプリケーショングループごとに受信要件が異なる環境向けに設計されています。このモデルでは、論理アプリケーショングループごとに専用の受信ファイアウォールを使用することで、受信ポリシーセットを簡素化し、管理を容易にします。一方、トランジットゲートウェイに接続された中央の次世代ファイアウォール（NGFW）が、送信トラフィックと東西トラフィックを一元的に保護します。パロアルトネットワークスは、この複合展開パターンについて、アプリケーションVPC側で受信セキュリティを使用し、トランジットゲートウェイを東西トラフィックと送信トラフィックのセキュリティのハブとして使用することを具体的に説明しています。