Deloitte.
デロイト トーマツ

AI搭載の5Gエッジネットワークにおける セキュリティとコンプライアンス

2024年2月

目次

概要

コネクテッドエッジネットワークによって可能になるユースケースでは、アプリケーション、コネクテッドデバイス、機械学習モデル、有線および無線のアクセス、そしてデータを保護するためのサイバーセキュリティ対策が必要です。また、リアルタイムで脅威を検出して対応するために、ネットワークの完全な可視性を実現する必要があります。

特にAI搭載の5Gコネクテッドエッジネットワークに見られるような高度なコネクティビティの進化により、サイバーセキュリティと規制遵守のためのリーディングプラクティスが形成されつつあります。エッジユースケースの採用は、容易さ、スピード、利便性を通じて顧客体験を向上させることを目的としています。このホワイトペーパーでは、様々なサイバーセキュリティ戦略を調査して、脅威の状況を説明するとともに、エッジネットワークのセキュリティアーキテクチャを形成するベクトルについて述べます。

デロイトは、進化する規制の状況やサイバーセキュリティ標準、業界固有のフレームワークに組織が対応できるように支援するため、決済カード業界データセキュリティ基準（PCI DSS）や消費者のプライバシーに関する法律の遵守、およびゼロトラストアーキテクチャの採用に役立つリーディングプラクティスを提案しています。エッジでのセキュリティ制御を実装するには、適切なネットワークセグメンテーション、モノのインターネット（IoT）セキュリティ、有線および無線のセキュアなアクセス、アプリケーションのセキュリティ、高度なネットワークセキュリティが必要です。また、セキュリティリスクの軽減とセキュリティ脅威への対応のために実装できる適切なネットワーク構成の原則を明確にするために、セキュアソフトウェア開発ライフサイクル、サプライチェーン、AIワークロードについて述べています。

コネクテッドエッジのユースケース

小売業などの業界で採用されるエッジコンピューティングやAIの技術は、効果的でパーソナライズされた顧客体験の実現と従業員のための業務改善を通じて価値を引き出すことを目的としています。

小売業の上位2,000社のうち90%が店舗でのデータを利用するために2026年までにエッジコンピューティングを活用すると予想されています[1]。デロイトのコネクテッドエッジイニシアティブは、容易さ、スピード、利便性を通じて消費者体験を向上させるという目標を含め、小売業界全体の喫緊の課題に対応しています。消費者の行動が変化しているのと同時に、市場の競争が激しいため、店舗経営では自動化を取り入れ、従業員が自分の職務において優れた結果を出せるように、新しいスキル、能力、および機会を提供することを迫られています。主要な小売業者は、需要に応え、変化に適応するために、便利かつ効率的で顧客中心のサービスアプローチに移行しています。

これは、デロイトの「2023 Retail Industry Outlook」[2]で概説されている特定のトレンドにも見られます。具体的には、(1) 盗難や破損の可能性を正確に検出して低減するためのカメラ分析やセンサーへの投資 、(2) 個人の好みに基づいて製品やサービスをカスタマイズすることによる個人レベルの顧客エンゲージメントの醸成、(3) レジでの顧客の待ち時間や行列の短縮を目的としたプロセスの合理化、(4) リアルタイムでのタスクの優先順位付けと割り当ての自動化などが挙げられます。

図1に示すコネクテッドエッジに対するデロイトのアプローチは、シュリンク（紛失や盗難などによる在庫損失）の削減、ハイパーパーソナライゼーション、オムニチャネル在庫管理、店舗と販売の最適化、従業員管理の自動化、レジの変革など、非常に革新的な6つのユースケースを通じて、ほぼリアルタイムの運用を実現するように構築されています。

カメラやセンサーなどの様々なデータソースから得られる洞察によって、企業は遅延が起きてから対応するリアクティブなスタンスから、より予測的でプロアクティブなアプローチへと移行できます。データはAIモデルによって安全に処理され、リアルタイムの分析と洞察が可能になるため、従業員は自分の仕事をより効果的に遂行できるようになります。

デロイトのコネクテッドエッジイニシアティブは、15社を超える小売テクノロジーベンダーによる多様なエコシステムを結集して、相互運用可能かつ統合された成果を提供します。統合プラットフォームでは多様なアプリケーションを実行し、次のものを強化します。

- 最先端のエッジコンピューティング
- 5GとWi-Fiの高度なコネクティビティ
- コンピュータビジョンと複数のセンサーによるAIアクセラレーション
- オンサイトでのデータ処理

センサーとカメラを活用して小売店の商品棚からデータを収集する店内処理により、瞬時の分析と洞察が可能になるため、労働力の効率性、生産性、有効性を向上させることができます。

デロイトのコネクテッドエッジイニシアティブは、特にセキュリティとコンプライアンスに重点を置いて設計された、AI搭載の5Gエッジネットワークの一例です。以下のセクションでは、業界標準や規制を遵守しながら、図1に示すエッジインフラストラクチャと、そのAI搭載アプリケーションの安全性を確保する方法について説明します。

図1：デロイトのコネクテッドエッジアーキテクチャ

セキュリティガバナンス

AIを搭載した無線の次世代エッジテクノロジーを活用するために、企業は新たな法規制や業界固有のガイダンス、先進的なサイバーセキュリティ標準を遵守する必要があります。

コネクティビティの標準化に関する主要団体や国のサイバーセキュリティグループによるガイドライン、および業界固有のガイドラインを活用するには、コスト効率の高い調和されたセキュリティとプライバシーの枠組みにより、企業がコネクテッドエッジの変革を乗り切れるようにすることが必要です。

エッジネットワークの安全性を確保するには基本方針とリーディングプラクティスを調和させることが必要であり、ガバナンスやマルチテナント環境内のサービスレベルアグリーメント（SLA）のほか、様々な標準や規制を業界固有の制御に結び付けるゼロトラスト（ZT）フレームワークの採用に着手しなければなりません。5Gのコネクテッドエッジネットワークの複雑なエコシステムには、通信事業者、マルチクラウド、エッジ、AI/ML、そしてIoTのベンダーのセキュリティ境界、責任、説明責任をマッピングするハイブリッドなガバナンスモデルが必要です。

特定のミッションクリティカルなユースケースでは、プライベート5Gネットワークのデプロイメントなどの高度なコネクティビティが必要となるため、最高情報セキュリティ責任者（CISO）にとっては、ネットワークのセキュリティとパフォーマンスに関するSLAと契約条件が非常に重要になります[3]。コンテナ化された、または仮想化されたデプロイメントで実行されているシステムでは、アクセス制御、イベントロギング、検査、構成管理、サプライチェーンリスク管理、個人を特定できる情報の処理、データの透明性など、チーム間で交差する無数の責任が存在します。

5Gとコネクテッドエッジのセキュリティに関連するサイバーセキュリティ標準とリーディングプラクティスは、業界固有の組織、国の組織、国際的な組織によって推進され、進化を続けています。

いくつか例を挙げると、次世代のAI搭載デバイス、無線通信、およびエッジテクノロジーについては、アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁（CISA）、米国国立標準技術研究所（NIST）、米国家安全保障局（NSA）、国際標準化機構（ISO）、決済カード業界データセキュリティ基準（PCI DSS）、GSMアソシエーション（GSMA：グローバルの携帯電話事業者による業界団体）、第三世代携帯電話システム標準化プロジェクト（3GPP）などの団体によって確立された高度な標準や規制の遵守が必要です。

PCI DSSは、クレジットカード情報の受け入れ、処理、保存、または送信を行う企業が安全な環境を維持しているかどうかを判断するために設計された**一連のセキュリティ標準**です。2022年3月31日にリリースされた最新版PCI DSS 4.0[4]に従って、カード所有者データの受け入れ、送信、または保存を行う組織に対して、その規模やトランザクション数に関係なくPCI DSSが適用されます。決済カード情報を管理する企業は、機密データの安全性を保護し、データ漏洩のリスクを軽減するために、PCI DSSを遵守し、それを維持する必要があります。遵守することは継続的なプロセスであり、1回限りのものではありません。したがって、企業は遵守状況を定期的に評価し、検査しなければなりません。PCI DSSは、ネットワークセキュリティ、アクセス制御、データ暗号化、定期的なテスト、監視などの分野を網羅していますが、コネクテッドエッジのユースケースでは、2つのセキュリティドメインが際立っています。最初のドメインは、決済情報の保存、処理、または転送を行うエッジノードとクラスタのID管理とアクセス管理（IAM）です。2つ目のドメインでは、保存時、転送中、処理中の3つの過程でデータに触れます。また、個人を特定できる情報が、既存または新規に設置されたカメラによって偶発的に入手される可能性がないことを判断するために、物理的評価が必要となる場合があります。同様に、Kubernetesなどのコンテナ化されたデプロイメントでは、PCI DSSを遵守したアーキテクチャを設計するために、仮想ネットワークのセグメント化、名前空間の分離、およびシステム管理者の様々な資格情報のプロビジョニングが必要になる場合があります。

これにより、個人を特定できる情報の要求を処理するPodを、AI/MLモデルに使用される画像処理Podから分離して、エッジユースケースを使用できるようになります。

一方、モバイルネットワーク事業者は、5Gネットワークスライシングの設計、デプロイメント、メンテナンスに関するセキュリティ上の考慮事項についてNSAとCISAが発表した最新のガイダンス[5]の内容を取り込んだ店舗内アプリケーションを実現するために、**5G専用**のエンドツーエンドネットワークスライスの**提供を計画しています**。企業の観点からは、各ネットワークスライス／サービスタイプ（SST）のサービス品質とセキュリティポリシールールを評価することで、企業は新しい5Gベースのエッジユースケースを導入する際に、コンプライアンスの維持に不可欠な信頼性と確信を得ることができます。5Gネットワークスライシングの安全性確保については、次のセクションで説明します。

規制遵守には、日本の個人情報保護法のみならず欧州連合の一般データ保護規則（GDPR）やカリフォルニア州消費者プライバシー法（CCPA）などの**プライバシー関連法規制も含まれます**。特に、消費者の活動や購買行動をモニタリングするカメラを使ってビデオ監視や分析を行う場合にこれが該当します。消費者のプライバシーの尊重を図りつつ、消費者から明示的な同意を得ることは、プライバシー関連法の遵守における主要な要件です。日本においても、個人情報保護委員会から生成AIサービスの利用に関する注意喚起等が発行されていることや、総務省公表の日米豪印「Open RANセキュリティ報告書」にてAI及びマシーンラーニングへのセキュリティ、また、プライバシーへの言及があることから、国内外で規制遵守への対応が不可欠です。このような遵守には、機密性、完全性、可用性などのデータに関するサイバーセキュリティ要件を維持しながら、プライバシー関連法に従うというバランスのとれたアプローチが必要です。

コネクテッドエッジのセキュリティ

5GやWi-Fi接続を利用する分散型エッジネットワークでコンピュータビジョンのユースケースの安全性を確保するには、リアルタイムのトラフィック可視性、高度な脅威相関、自動化されたセキュリティの適用が必要です。

エッジコンピューティングでは、データ処理とアプリケーションの実行がエンドユーザーに比較的近い場所で行われます。一元化されたクラウドサービスを使用する代わりに、負荷は分散化され、組織のネットワークの「エッジ」で処理されます。小売店の例では、様々なコネクテッドデバイスからのデータのストレージと処理は、専用の処理装置（CPU）とグラフィックス処理装置（GPU）、ネットワーキング、およびストレージ要件を備えた店舗のローカルネットワークで行われます。これにより、AIモデルの処理遅延が低くなり、処理速度が向上します。

他のユースケースと同様に、エッジでの小売店の安全性確保は、ユーザーやデバイスにとどまらず、クラウドとアプリケーションファブリックにも及びます。ワークロードに対してクラウドネイティブなセキュリティを実装し、次世代ファイアウォールを統合することで、既知および未知のインバウンドおよびアウトバウンドの脅威からの保護、データ流出の防止、個々のデバイスの保護、アプリケーション間およびネットワーク内のラテラルムーブメント（攻撃者がシステムやデバイスに侵入した後に、ネットワーク内を横移動し、他のシステムやデータの偵察や、資格の窃盗を行うことで、攻撃範囲の拡大を試みる行為）の防止を図るのです[6]。

示されている例が複雑であるため、ゼロトラストアーキテクチャ（ZTA）の実装は、ID、ワークロード、データ、ネットワーク、デバイスという5つの基本的な柱にわたって、強力な基本的機能を基に構築されるモデルが必要となる困難なタスクになります。テレメトリ＆アナリティクス、自動化とオーケストレーションが、上述の5つの柱と交わり、脅威の監視、分析、プロアクティブな対応を行います。

エッジロケーションでアクセス要件を適用する必要があるため、プロビジョニング時に適切なアクセス制御を使用してクラウドのリソースを設計する必要があります。また、チームは、セキュリティ侵害を防ぐために　、　厳格なアクセスポリシーを備えたInfrastructure as Code（IaC）メソッドを使用する必要があります。ZTAとIaCを採用するメリットは次のとおりです。

- 攻撃対象領域の最小化、けん制、人的なエラーにつながる手動のデプロイメントの削減。
- サイバー攻撃の特定、けん制、防止のための継続的な監視、およびリソースに対する最小権限アクセスの実施[7]。
- コネクテッドエッジの承認ユーザーリストに対するアクセスのプロビジョニングと取り消しを含む、最小権限アクセスの管理および監視、様々なPCIタグ付きアプリケーションに対する個別の資格情報の維持。
- 店舗内の管理者数の最小化、最小権限アクセスの流動的付与（必要な場合にのみ）により、管理者権限を長期間行使するユーザーを削減。

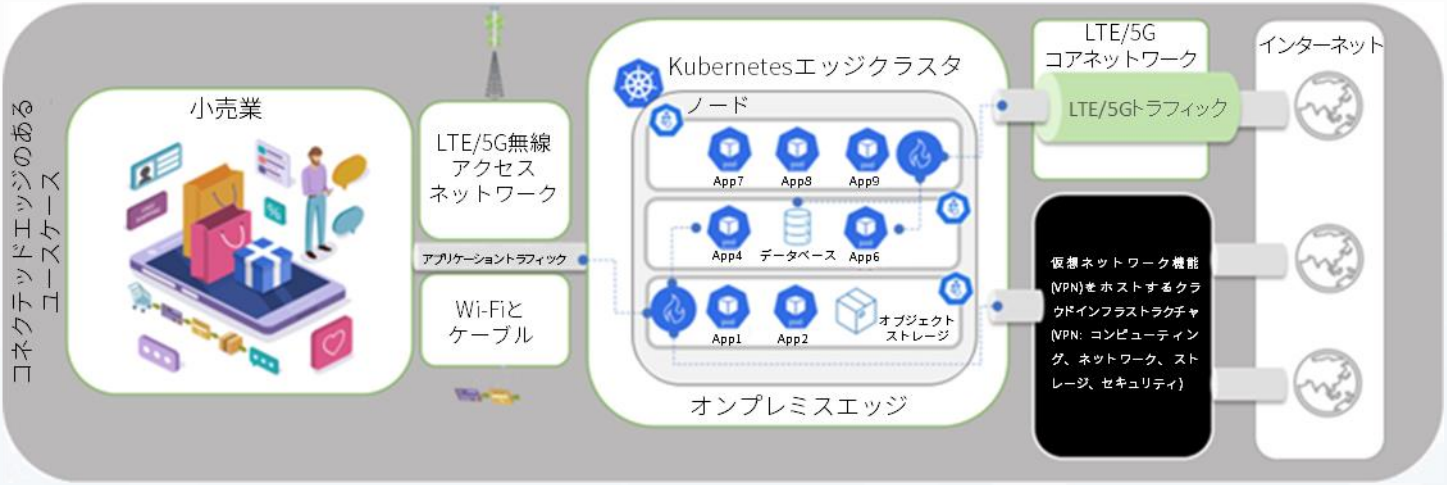

図2.：コンテナ化されたエッジアーキテクチャ

小売店のユースケースでは通常、商品補充、QRコードスキャナー、様々な温度や湿度のセンサーに対して、セキュリティ、請求、および在庫のチェックポイント（棚の上）に配置されたカメラなど、**幅広い種類のデバイスを使用します**。図2に表示されている店舗のインフラストラクチャには、オンプレミスのサーバー、販売時点情報管理（POS）システム、Kubernetesクラスタを実行する最新のエッジインフラストラクチャも含まれる場合があり、Kubernetesクラスタには、それぞれのデータパイプラインまたはその他のコネクテッドサービス、ネットワーキングデバイス、インターネット接続があります。事業の拡大に合わせて、これらのデバイスとアプリケーションを無数に組み合わせたインフラストラクチャへと拡張することが可能です。これらのデバイスの大半に共通する要件の1つは、ソフトウェアの継続的な更新とパッチの適用であり、ソフトウェアとハードウェアのサプライチェーンが安全でない場合は大きなリスクがあることを意味します。

次世代ファイアウォールとゼロトラストネットワークセグメンテーションのエージェントが、インターネットとのデバイスアクセスとデバイス間接続の監視と制御を行うことで、コードインジェクション攻撃やコマンド＆コントロール攻撃を減らすことができます。高度なAI/MLモデルを使用したIoT資産プロファイリングは 、リスクの高いポートの既知の脆弱性や、コネクテッドデバイスの暗号化されていない通信の防止に役立ちます。

ネットワークの観点からは、特にクラウドネイティブのKubernetesクラスタでは、様々な部分を保護する必要があります。ネットワークセキュリティの複雑さは、南北および東西のトラフィック、Pod内およびPod間の通信、IoTおよびカメラのクラスタとの通信、クラウドまたはエンタープライズネットワークへのクラスタの外部通信など、多数の脅威ベクトルから生じます。

名前空間の分離を含むアプリケーションと資産の間の仮想および物理ネットワークセグメンテーションの実装は、ラテラルムーブメントを防ぎ、攻撃の影響範囲を縮小するようなエッジクラスタを設計する際に採用すべき主要な設計原則の1つです。

さらに、コンテナベースの次世代ファイアウォールを統合することで、(1) 既知および未知のインバウンドおよびアウトバウンドの脅威からの保護、(2) データ流出の防止、(3) アプリケーション間およびネットワーク内でのラテラルムーブメントの阻止に役立ちます。

リアルタイムのトラフィック可視性とIoT資産のプロファイリングにより、ネットワークセキュリティポリシーとゼロトラスト制御を強化する手段が提供されます。これは、ゼロデイなどの脆弱性の修正、ウェブとDNS保護の強化、コマンド＆コントロールを使用した攻撃の防止に役立ちます。

5Gネットワークスライシングは、コネクテッドエッジユースケースで使用される場合がある5Gネットワークに限定された機能です。

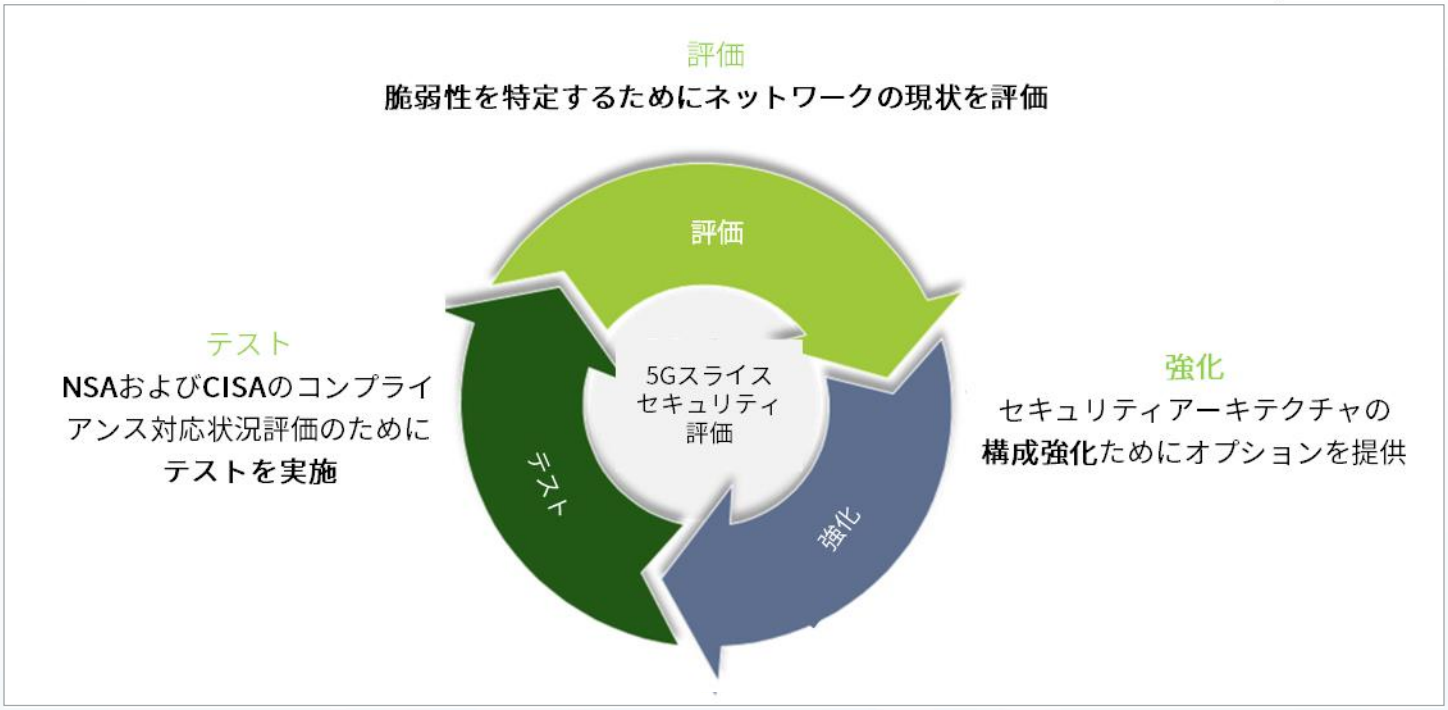

図3：デロイトの5Gセキュリティ評価

デロイトは、図3に示すように、ネットワークスライスのセキュリティを評価するために、評価、強化、テストの3段階アプローチを開発しました。これは、5Gネットワークとスライスのセキュリティに対するアプローチの加速と合理化を行う150を超えるセキュリティ制御で構成されています[8]。デロイトは、NSAとCISAが開発した取り組みに発想を得て、ユーザー機器、データネットワーキング、仮想化など、様々なネットワークプレーンにおけるサイバーセキュリティの問題に対処するリーディングプラクティスを説明した例示的なチェックリストを提供しています。

オンプレミスのエッジインフラストラクチャでは、多くの場合、アプリケーションプログラミングインターフェイス（API）を使用して、IoTアプリケーションが様々なアプリケーションに接続し、ワークロード、データベース、データレイク、その他のストレージテクノロジー間でデータを転送できるようにします。 APIは非常に重要であり、サイバー攻撃を防ぐための認証、トークン、暗号化、および安全な通信の適切な使用について、これを評価することが必要です。デバイス、エンドポイント、Podの通信をリアルタイムで把握し、ネットワークトラフィックについて完全な可視性を得ることにより、悪意あるアクティビティや異常な動作の綿密な監視と防止が可能になります。

アプリケーションとAIのセキュリティ

アプリケーションとAIワークロードを保護するには、アプリケーションに対する最小権限アクセスの継続的なリスク評価と、AIモデルのデータ完全性チェックが必要です。

データが不正にアクセスされていないことの確認や、マルウェアの検出強化のために、エッジアプリケーションに対するコンテンツ検査と制御を導入する必要があります。ソフトウェア開発においては、安全かつ継続的な統合/開発（CI/CD）のためのパイプラインを構築し従うことにより、開発中における適応戦略を可能にし、新旧の攻撃から保護するための、より優れた機能をネットワークに適時投入する必要があります。

AIの使用は、アプリケーションの様々な領域で**標準になりつつ**あり、現代におけるエッジトランスフォーメーションの取り組みの基礎になっています[9]。

AIを使用することで、ビジネスに大きなメリットがもたらされますが、当然ながら、対処が必要な独自の脆弱性やセキュリティ上の懸念ももたらします。通常、AIエンジンは、データフィードを行うためのモデルに基づいて動作し、新しい入力データが来たときの微調整のために、追加のトレーニングデータを必要とします。

そのため、トレーニングデータが汚染されていないこと、および悪意のある個人や組織からのインジェクション攻撃によってトレーニングステージが侵害されていないことを確認することが重要です。さらに、入力の観点からは、誤分類されたデータでモデルを混乱させてAIエンジンを騙す攻撃を防ぐことも必要です。

出力の観点からは、AIエンジンの成果が攻撃者によって取得されないこと、出力データがそのデータを入手すべきではないユーザーに公開されない（知る必要がある人にだけ知らせる）ことを評価することが求められます。設計の観点からは、AIエンジンの用途を限定し、目的を特定することが重要です。そうすることで、不要なデータがモデルのトレーニングに使用されることがなくなり、機密情報が適切に使用されるようになります。

そのうえで、AI開発のワークフローでは、従来のソフトウェアで使用されている従来のガイドラインとリーディングプラクティスに従う必要があります。そうすることが、バックドアなどの攻撃、資格情報の盗難、意図しないモデルの使用を防ぐことに役立ち、CI/CDパイプラインに寄与することになります。また、使用されるデータ（トレーニング用または単にモデルの入力用として）の完全性と、そのアクセス許可と使用範囲を確認することも、安全かつ規制を遵守したAI環境には同様に重要です。

総括

コネクテッドエッジコンピューティングと高度なコネクティビティにより、様々な業界でパーソナライズされた効果的な顧客体験と業務改善が可能になっています。AIワークロードを利用するコネクテッドエッジのユースケースの安全性確保には、ゼロトラスト原則を採用し、組織が規制、プライバシー法、業界固有のガイダンス、先進的なサイバーセキュリティ標準を遵守できるようにする広範なフレームワークが必要です。

サイバーセキュリティ対策の適切な実施では、アプリケーション、コネクテッドデバイス、機械学習モデル、有線および無線のアクセス、データを含めるとともに、脅威をリアルタイムで検出して対応するための完全なネットワーク可視性を実現する必要があります。さらに、AIワークロードのセキュリティには、MLモデルへの最小権限アクセスについての継続的なリスク評価と、トレーニング、テスト、リアルタイムデータの厳格なデータ完全性チェックが不可欠です。

著者

Frederico Macias
Partner
Deloitte Portugal LLC
fremacias@deloitte.pt

Ally Adnan
Managing Director
Deloitte & Touche LLP
allyadnan@deloitte.com

日本連絡先

プラサド アナンド ラガワ
Anand Raghawa Prasad
Partner
デロイト トーマツ サイバー合同会社
anandraghawa.prasad@tohmatsu.co.jp

北野 晴人
Partner
デロイト トーマツ サイバー合同会社
haruhito.kitano@tohmatsu.co.jp

松尾 正克
Managing Director
デロイト トーマツ サイバー合同会社
masakatsu.matsuo@tohmatsu.co.jp

参考資料

1. Deloitte, "Be out front - EDGE.AI accelerates store innovation," 2023.
2. Deloitte, "2023 Retail Industry Outlook," 2023.
3. Deloitte, "3 Critical Elements of Strong 5G Service Level Agreements," The Wall Street Journal, 2023.
4. PCI Security Standards Council, LLC, "Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0," 2022.
5. NSA and CISA, "5G Network Slicing: Security Considerations for Design, Deployment, and Maintenance," 2023.
6. Deloitte, "Connected Everything: Securing advanced connectivity use cases," 2023.
7. Deloitte, "Deloitte Cyber Threat Trends," 2023.
8. Deloitte, "5G Network Slicing: Security Considerations for Deign, Deployment and Maintenance," 2023.
9. Deloitte, "Emerging Technologies and Innovation: How 5G & IPv6 can enhance Edge AI solutions and shape the architecture of the future," 2023.

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ リスクアドバイザリー合同会社、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ グループ合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市に約2万人の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト、www.deloitte.com/jpをご覧ください。

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
http://www.bsigroup.com/clientDirectory

Member of
Deloitte Touche Tohmatsu Limited