The bridge to possible

ハイブリッドクラウド産業用 DMZ

産業のデジタル化を大規模に推進

産業用緩衝ゾーン（IDMZ）は、産業オペレーション環境でエンドツーエンドの包括的なセキュリティ戦略を実現するための重要なレイヤとなっていますが、オンサイト専用の IDMZ にはいくつかの課題があります。たとえば産業用 IoT（IIoT）や IT/OT/ クラウドの統合が進むにつれて新しい機能が求められるようになっていますが、オンサイト専用の iDMZ にはそうした今後の需要を満たすだけの十分な能力がありません。また、オペレーションスタッフが複数の拠点で IDMZ の一貫性を維持し、一貫したセキュリティポリシーを提供するのも難しいことがあります。

そうした課題を解決できるのが、ハイブリッドクラウド IDMZ モデルです。オンプレミスで展開した IDMZ のように包括的なセキュリティ戦略を実現できるだけでなく、リソースとアセットの共有が可能なので、再現しやすく一貫性の高いアーキテクチャを構築できるほか、運用のオーバーヘッドと複雑さも緩和されます。また、一部の産業組織、特に世界規模で展開している組織では ROC（地域オペレーションセンター）が重要になっていますが、ハイブリッドクラウド IDMZ はこの概念に沿ったものとなっています。

The bridge to possible

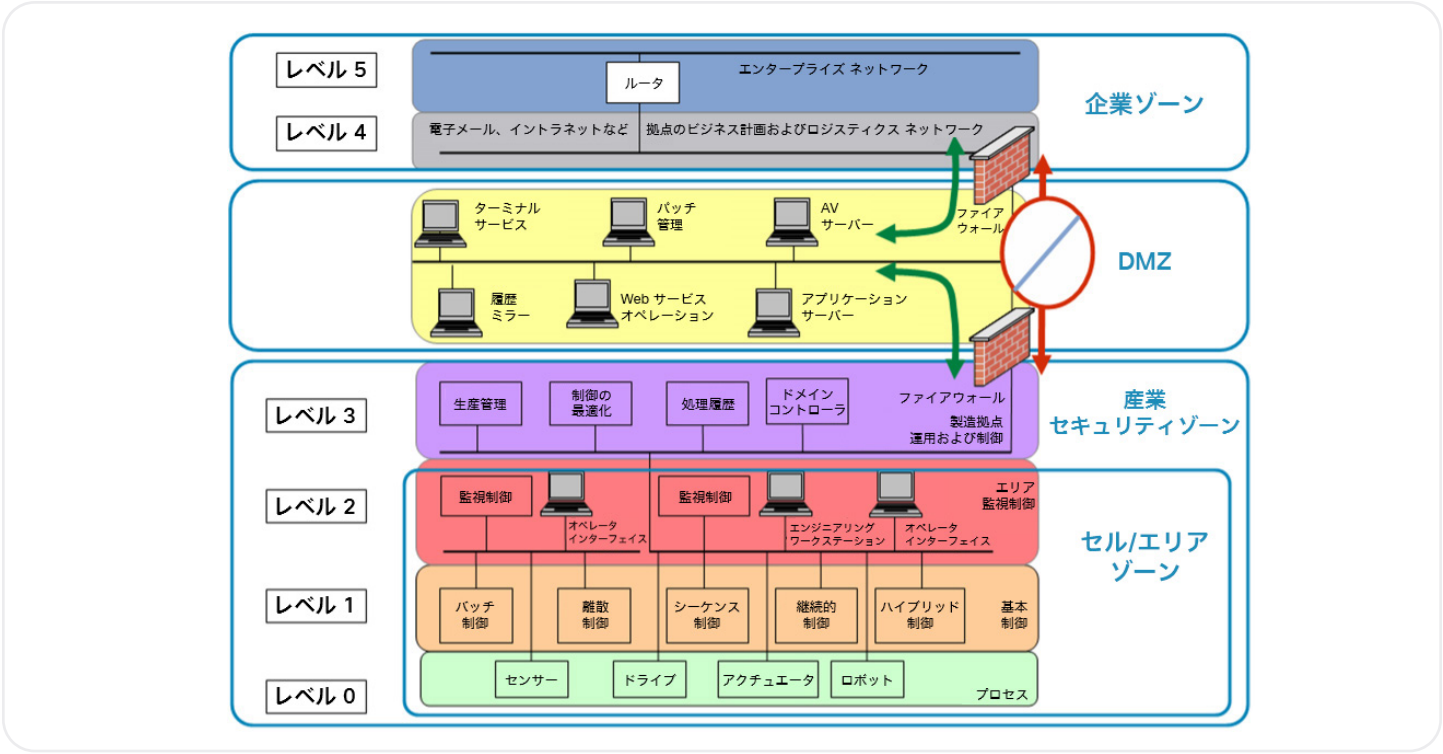
進化する要件と産業用 DMZ

産業事業者や企業はさまざまな課題に直面しています。いくつか例を挙げると、生産性、スキルの保持、コスト削減、競争圧力に関連する課題があります。これらすべてに関わっているのが、そうした問題に対処しやすくなる高度なテクノロジーを展開するという技術的な課題です。たとえば、コラボレーション テクノロジーを展開して「Expert on Demand」（XoD）と一般に呼ばれているリモートエキスパート機能を提供することで、スキル不足に関連する懸念を解決することができます。インダストリー 4.0 の成否を決めるのは、オペレーションデータへのアクセスを確保し、複数のドメイン（さらには複数の地域）からそれらのデータを取り込み、データ分析によって洞察を獲得して予知保全に役立てることができるかどうかです。この文脈では、セキュリティ（とそのすべての派生物）をいかに確保するかが最も重要になります。基本的に、セキュリティを適切に展開して構成することで、生産性の向上、コラボレーション、コストの削減が可能になります。

産業環境に関するあらゆる議論と同様に、ISA95 および ISA99 標準で規定されている Purdue 参照モデルは、全体像を把握するのに役立ちます。DHS、NIST、NERC では、同様のアーキテクチャや参照モデル、特に産業用緩衝ゾーン（IDMZ）の役割に関連するガイダンスが提供されています。このモデルでは 6 つの機能レイヤ（レベル）が記述されていますが、産業サポートオペレーションは次の 3 つの主要な領域に分けられています。

1. **企業ゾーン**は工場あるいは IT が管理する環境を表しており、企業のデータセンター、LAN、WAN、ビジネスアプリケーションのホスティングなどが含まれます。
2. **産業用緩衝ゾーン（IDMZ）**は、重要な環境または製造現場システムとエンタープライズ ネットワークの間のバッファです。産業ゾーンと企業ゾーンの間の共有サービスはすべて IDMZ に配置されます。
3. **産業セキュリティゾーン**には重要なオペレーションシステムが配置されます。このゾーンには、低遅延またはリアルタイムの通信が頻繁に行われるセル / エリアゾーンが含まれます。本書は主に IDMZ を取り扱っているため、セル / エリアゾーンの詳細な説明は割愛します。

図 1. Purdue 参照モデルのレイヤ



さまざまなゾーンの厳格なセキュリティ要件、セキュリティテクノロジーの制限、異なるデータアクセス要件、ベンダーアクセス要件、環境の重要性を考えると、IDMZ は IT/OT の統合において最も重要な領域になっています。

モノのインターネット（IoT）によって軽量のセンサーと軽量の通信プロトコルが登場しており、大量のデータを取得してデータセンターやクラウドに送信し、詳細な分析を行うことが必要になっています。また、次世代の産業機器とアセットが高度化していることや、プロセス最適化が広範に採用されるようになったことで、メンテナンスやパフォーマンスサービスのために環境に OEM アクセスできることも必要になっています。こうした要因が相まって、IDMZ においてより高いレベルの柔軟性、シンプルさ、確定的で一貫したセキュリティが求められるようになってきています。産業ゾーンと企業ゾーン、サードパーティベンダー、エコシステムパートナーの間のデータ移動をサポートしながら、本当に必要とされている管理機能を実現しようとしているのです。

またデータセンターにおいても、製造実行サービス（MES）、エンタープライズ リソース プランニング（ERP）アプリケーション、（オペレーションからの）大量のデータ収集を処理し、柔軟性を向上させ、リーチを拡大し、コストを削減することが求められるようになっており、結果として IT 部門は重要なデータ管理の取り組みをクラウドに移行させています。いくつかの最新の統計によると、クラウドの勢いは増す一方であり、経費節減と高度な計算機能の両面で企業に価値を提供しています。またクラウド事業者は、リーチをエッジまで拡大してアクセスを改善することで、低遅延と最適化されたパフォーマンスの両方を実現しています。重要なビジネスアプリケーションをプライベートにホストしている場合やエンタープライズ データセンターでホストしている場合と比べ、パフォーマンスが勝ることさえあるのです。

IDMZ は、ハイブリッド インフラストラクチャで運用することで多大なメリットを得られます

このような論拠から、ハイブリッド クラウド ソリューションは IDMZ（および最終的に産業オペレーション）に多大なメリットをもたらすとシスコでは考えています。

クラウドに対する誤解

企業のお客様の多くはクラウドサービスやクラウド機能を活用するために積極的に取り組んでいますが、産業事業者の間ではクラウドテクノロジーの採用が遅れています。その大きな理由になっていると思われるのが、産業オペレーションを WAN にさらすと攻撃対象領域が広がる可能性があるという懸念です。この 10 年間メディアで取り上げられてきたように、状況によっては、外部に接続することでオペレーションの侵害を招くことがあります。そうした事例から、産業ゾーンを十分に保護するのは不可能であるといったクラウドに対するさまざまな誤解や懸念が生じています。その代表例を以下に示します。

クラウドを利用するのであれば、すべてのサービスとアプリケーションをクラウドプロバイダーに一気に移行する必要があり、部分的に移行することはできない。今日の世界では、単一のクラウドというものは存在しません。世界はマルチクラウドでできており、組織は複数のプロバイダーの複数のクラウドサービスを使用しています。ハイブリッドクラウドとは、オンプレミスのプライベートクラウドとパブリッククラウドなど、2 つ以上のクラウドのインフラストラクチャを組み合わせたものであり、集中管理によってさまざまなユースケースで相互運用性を実現できます。クラウド移行戦略では、データとアプリケーションをオンプレミスアーキテクチャからクラウドに徐々に移行していくように調整することができます。ワークロードによっては、クラウドベースのインフラストラクチャで実行してもメリットが得られないことがありますが、IDMZ は大きなメリットを得られます。

ハイブリッドクラウド環境でホストされているデータとアプリケーションを完全に保護することはできない。いくつものパブリック クラウド プロバイダーが世界中でサービスを提供しているので、オンプレミスで維持するものとクラウドに配置するものを自由に選択できます。このような各種のクラウドに接続するのは簡単ですが、さまざまな環境の管理は複雑化する可能性があります。シスコでは多層防御のアプローチを使用して、ビジネスのあらゆるレイヤに保護を追加しています。シスコセキュリティでは、Cisco® Cyber Vision による産業の可視化、Cisco Secure Firewall によるセグメンテーション、Cisco Secure Workload によるアプリケーション保護など、マルチクラウドの世界に対応した効果的なセキュリティソリューションを幅広く提供しています。

クラウドの恩恵を受けるのは主に IT 部門であり、産業オペレーションにはほとんどメリットがない。ハイブリッドクラウドやハイブリッド IT アーキテクチャの構築が推進されている重要な要因となっているのが、パブリッククラウドサービスへのアクセスです。組織は、自社のオンプレミス環境をパブリッククラウドに拡張して、開発チームがプラットフォームサービスのメリットを享受してアプリケーション構築までの時間を短縮できるようにしています。産業オペレーションをマルチクラウドエコシステムに組み込むと、産業オペレーションのイノベーション速度が大幅に向上します。

クラウドでホストすると、アプリケーションおよびサービスレベル契約（SLA）を適用および維持することができなくなる。Cisco AppDynamics®、ThousandEyes、Cisco Secure Cloud Analytics などのクラウドおよびアプリケーション モニタリング ツールは、オンプレミスとハイブリッドで並行してリアルタイムで機能します。これによってハイブリッドクラウド、プライベートクラウド、パブリッククラウドのサービス間でアプリケーションやネットワークレイヤのパフォーマンスを測定し、視覚化することができます。これらのツールを活用することで、分散した場所にある大量のデータを統合し、異常と根本原因を特定し、潜在的リスクや生産停止を予測することができます。

クラウドサービスを使用してオペレーションをサポートすることにためらいを感じるかもしれませんが、クラウドは産業オペレーションにも確実にメリットをもたらします。

クラウドのメリット

クラウドには次のようなメリットがあります。

弾力性、スケーラビリティ、クラウドバースティング。クラウドサービスはスケーラブルで弾力性があるため、リアルタイムの需要に基づいてアプリケーションとサービスを簡単に拡張したり縮小したりできます。これはクラウドバースティングと呼ばれています。細かな例外はありますが、さまざまなクラウドプロバイダーが提供しているサービスは世界中で利用でき、需要の変動に応じてスケーリングできるため、一貫性のあるエクスペリエンスが得られ、統一された方法でそれらのサービスを利用することが可能です。

クラウドを利用すれば、復元力のある可用性の高いサービスを世界中で迅速に展開できます

効率性。クラウドを活用すれば、クラウド環境内でアクセスできる堅牢で冗長性のあるツールとリソースに基づいて、復元力のある可用性の高いサービスとアプリケーションを迅速に展開できます。物理的なハードウェアや基盤となるインフラストラクチャに対して責任を追ったりメンテナンスを実施したりする必要がないため、アプリケーションや階層型サービスの展開を簡単にスクリプト化して自動化できます。これによって、運用のオーバーヘッドを最小限に抑え、効率を高めながら、ビジネスの進化する需要や新しい要件に素早く対処することができます。

グローバルで利用可能。いくつものパブリック クラウド プロバイダーが類似する各種のサービスを提供しています。それぞれのクラウドプロバイダーは世界中で事業を展開しており、Americas、EMEAR、APJC のそれぞれの主要地域において一貫したメニューやサービスのセットを提供しています。たとえば、オフィスがドイツにあっても米国にあっても同じサービスを利用できるので、オペレーション全体で一貫性を保つことができます。クラウドプロバイダーは、一貫性のあるサービスのセットを世界中で提供しているだけでなく、クラウドエッジの近くにサービスを分散させることもできます。これによって、アプリケーションとコンテンツをエンドユーザー / 消費者に近づけることができ、効率的かつ適切にデータを移動して配信できます。

クラウドテクノロジーの一般的なメリットに加えて、産業事業者が享受できる独自のメリットがあります。

オンサイト要員の削減。就業中やオンサイトでの安全が何よりも優先される産業事業者にとって、危険な領域に要員を近づけないことは重要な関心事となっています。

まず、オンサイトでホストされている重要でないアプリケーションとサービスを減らし、それらをクラウドに移行することで、設備投資を削減できます。事業者は拠点ごとに設置するハードウェアの規模を減らすことができます。また、一部の業界の事業者にとって非常に困難で制約のある課題となっている電力、冷却、スペースの要件も緩和できます。

さらに、オンサイトのハードウェアとアプリケーションをメンテナンスする要員を地域のオペレーションセンターなどの遠隔地に配置転換できるので、オンサイトでオペレーションを担当する要員を減らすことができます。たとえば、機械や車両のテレメトリデータを取得して予知保全やプロセスの最適化に利用している事業者の中には、オンサイトに要員を配置してこれらのアクティビティを実施し、データ分析や、バックエンドシステムとデータリポジトリのメンテナンスを行っている事業者もあります。しかし、テレメトリサービスをクラウドに移行すれば、担当要員が拠点にいる必要がなくなり、より重要で不可欠な任務を負う要員のみを拠点に配置することができます。

IDMZ をクラウドに移行すれば、通信が合理化され、オペレーションのダウンタイムが短縮されます

エコシステムパートナーとサプライチェーンとのより効率的な連携。IDMZ をクラウドに移行して、アセット、コンピューティングリソース、接続をオペレーションでより直接的に制御できるようになると、エコシステムパートナーとの直接接続を確立して安全に管理することが可能になります。それらのエコシステムパートナーが提供するサービスを利用すれば、オペレーションのパフォーマンス効率を高めることができ、独力では得られなかったような洞察まで得られるかもしれません。

たとえば前述の例において車両や機械のデータを分析したい場合、従来であればそのデータを保存するためのサーバーを追加する必要があり、ハードウェア、電力、冷却、訓練された要員といったコストがかさんでいました。産業環境内のオンプレミスに機器が配置されているケースでは、アクセスするために付き添いと追加の安全トレーニングが必要になることもありました。

こうしたアクティビティをクラウドに移行すれば、クラウドの弾力性とスケーラビリティを活用できるようになり、ハードウェアのメンテナンスが不要になります。また通信が合理化され、予防保全などのアプリケーションのためにパートナーと情報を簡単に共有できるようになります。さらに、Software as a Service（SaaS）などの新しいサービスを利用してオペレーションにメリットをもたらすことも可能になります。

エンタープライズ ネットワークからの独立。一部の産業事業者の間ではオペレーションが時間とともに有機的に拡大しており、IT と OT で環境が共有されて制御もポリシーの適用も行き届かなくなり、IT/OT アセットとオペレーションの間の境界が不明確になってきています。

エンタープライズ データセンターにおいて明確なアーキテクチャ、アセットの共有、OT アセットのテナントが欠如していたり、複数のロケーションや施設でポリシーの適用方法に一貫性がなかったりすると、オペレーションにおけるリスクと課題が増大する可能性があります。また、メンテナンスのスケジュールや管理責任にも不整合や分断が生じる可能性があります。そのような状況では、オペレーションにおいて不要なダウンタイムが発生する可能性があります。24 時間無休で稼働している場合は特にその可能性が高くなります。また、IT 部門が開発したオペレーションのニーズに合わないセキュリティ管理を回避するためにバックドアの脆弱性が導入されかねません。

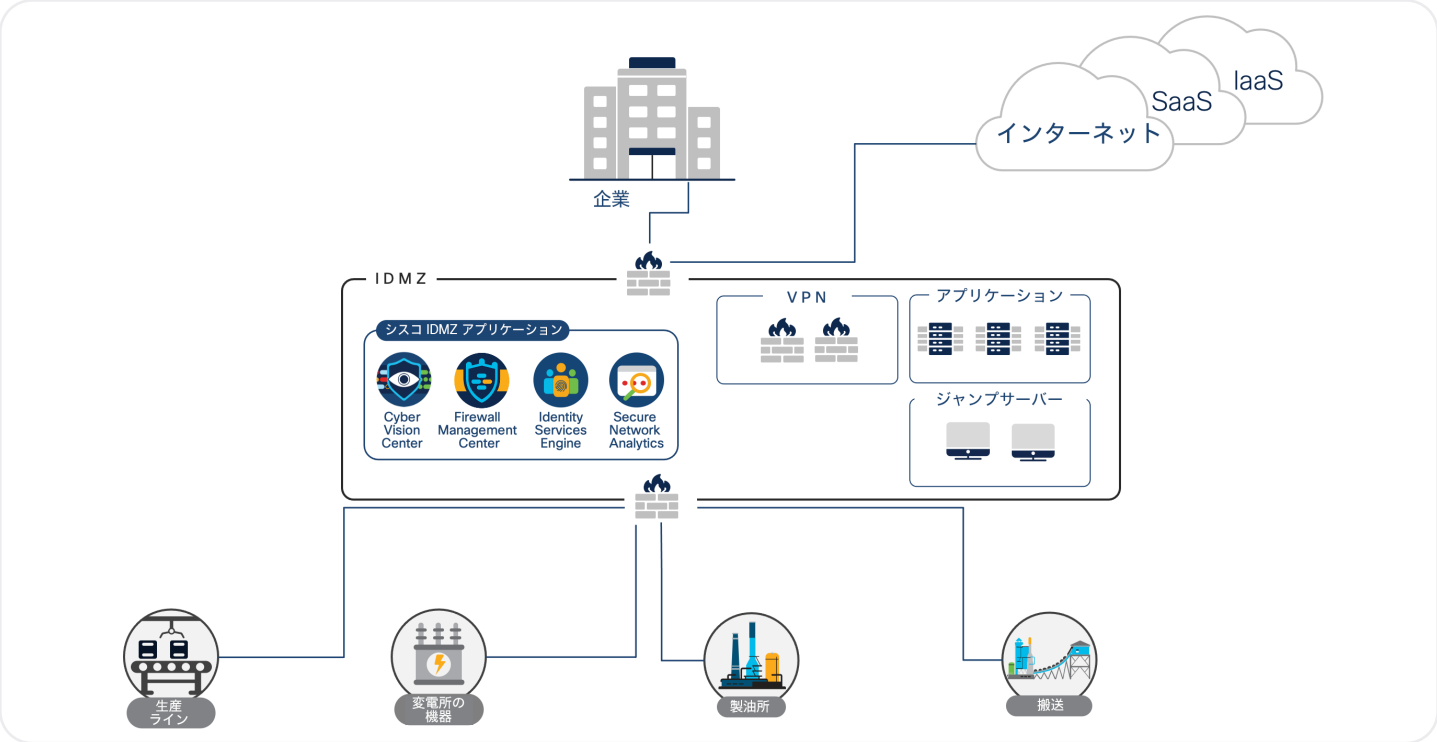
クラウドにサービスを移行すれば、IT アセットと OT アセットの分離が促進され、オペレーションをサポートするアセットやそれらのアセットのメンテナンスをオペレーションが詳細に制御できるようになります。また、ビジネスニーズに合った一元化されたセキュリティポリシーも確立できます。これによって、最終的に OT を IT 部門からある程度独立させることができます。OT が自身のコンピューティングリソース、アプリケーション、アセットを管理できるようになるだけでなく、OT スタッフもオペレーションの都合に合ったスケジュールとルーチンでメンテナンスタスクや管理タスクを行えるようになります。

また、WAN サービスと接続を OT が管理できるようになる場合もあります。それによって、ビジネス運営により適合したポリシーを OT が開発したり、独自の WAN 接続を管理して SaaS オファーを利用したりできるようになります。また、リモート接続を使用してリモートエキスパートなどを活用することも、OEM などのエコシステムパートナーと緊密に連携してそれらのパートナーがクラウドでホストしている独自のサービスやアプリケーションを利用することも可能になります。最後に、オンプレミスの IDMZ を使用して企業からオペレーション施設に専用回線を直接引く代わりに、クラウド IDMZ を使用して同じ接続を実現することができます。その場合、企業は基本的に他の XaaS プロバイダーやアプリケーション プロバイダーと同様に扱われて、製造実行システム（MES）やエンタープライズ リソース プランニング（ERP）などのアプリケーションが一般的に共有されます。

ハイブリッドクラウド IDMZ

クラウドサービスをオペレーションで活用する機会を探っている産業事業者にとって、IDMZ のクラウド展開は検討する価値があります。

図 2. IDMZ をクラウドに展開



IDMZ でホストするサービスは、企業のオペレーションに不可欠なサービスではない。産業用ネットワークではオペレーションの確定性と継続性が重要になります。オペレーションチームの管理が及ばない可能性があるリソースとアプリケーションに対して依存関係を確立することは避けられる傾向があります。産業ゾーン（Purdue モデルのレベル 0 ～ 3）にあるアプリケーションとオペレーションは企業のオペレーションに不可欠であり、オンプレミスに保持することが必要になる可能性があります。それに対して、企業ゾーン（Purdue モデルのレベル 4 および 5）は IT 部門がメンテナンスしており、オペレーションから離れた企業内の場所に配置できます。

したがって、セキュリティイベントや接続の中断が発生した場合には、外部との接続を切断した上で、オペレーションを遂行する能力を維持することができます。IDMZ でホストするアプリケーションやサービスの多くは、オペレーション全体にとって重要ではありますが、厳格な SLA はなく、遅延やリアルタイムの要件もないため、それらのサービスやアプリケーションを展開できる場所には柔軟性があります。

リモート拠点間で一貫性のあるポリシー。これまで、IDMZ はリモート施設ごとに導入されるのが一般的でした。IDMZ を中央に配置すれば効率が向上し、規模の経済の恩恵が得られます。同じ地域に複数の施設や設備を持つ加工業者や製造業者が、各施設を独立したものと見なして、それぞれ固有のオンプレミス IDMZ セキュリティスタックを使用していることがあります。

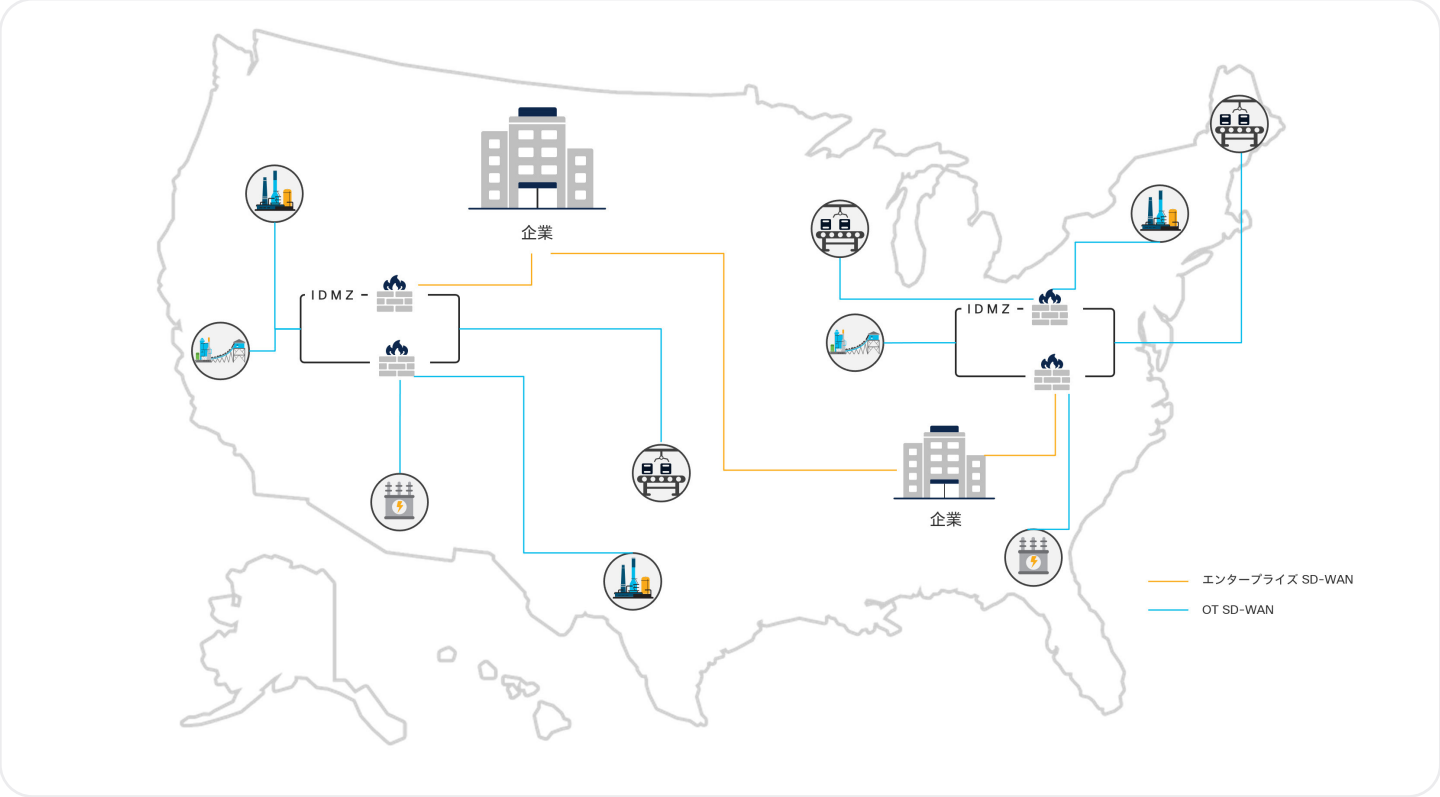
物理ハードウェアの観点からは、同じ規模の物理ハードウェアをすべての場所に一貫して設置することが可能です。しかし、テクノロジーに関する決定は各拠点のマネージャに委任されていることが多く、拠点間で大きく異なるハードウェア構成が採用される可能性があります。さらに、同じポリシーのセットがすべての場所で採用される保証はなく、セキュリティ戦略全体にギャップが生じる可能性があります。一元化された単一の IDMZ ソリューションを地域ごとに導入すれば、均一で統一されたセキュリティ展開を簡単に実現できるだけでなく、同じポリシーのセットを複数の拠点に簡単に適用できるようになります。

一元化された IDMZ ソリューションを導入すれば、同じポリシーのセットを複数の拠点に簡単に適用できるようになります

地域オペレーションセンター。地域オペレーションセンター（ROC）は、地域内の複数の拠点や施設にわたる広範な可視性を提供します。ROC によって拠点の人員が削減されるため、拠点の全体的な安全性が向上して一部のコストが削減されます。フライイン / フライアウト（シフト体制を組んで遠隔地の現場まで飛行機で移動する勤務形態）の場合は特にこの効果が大きくなります。クラウドに IDMZ を移行する取り組みは、多面的な階層化セキュリティのアプローチを活用し、特定の地域にある拠点間で IDMZ を共有するという点において ROC モデルの概念に沿ったものとなっています。

ハイブリッドクラウド IDMZ に展開したリソースは地域のセキュリティチームによって管理されます。これによってポリシーの開発と適用の観点で一貫性が促進され、地域の IDMZ に属するさまざまな拠点が送受信するトラフィックを把握できるようになります。またクラウド インフラストラクチャの弾力性のあるサービスと機能を活用できるようになります。

図 3. 地域の IDMZ



ここで強調しておきたいのは、提示されている展開モデルが特定の地域の中央ハブに焦点を当てており、パブリック クラウド プロバイダーが提供するクラウドサービスのグローバルな可用性を活用していることです。地域モデルのサイズとスケーリングを定義するためにさまざまな戦略を策定することができます。世界中に施設を持つ事業者の場合、各地域において地域ハブの概念が同じように適用され、複数の施設から成るグループが最も近い地域ハブの場所に所属します。また、地域の IDMZ が可用性の高い構成（アクティブ / スタンバイまたはアクティブ / アクティブ）で展開されることも注目に値します。

特定のパートナーや OEM 専用の IDMZ 内に、適切な仮想化とセキュリティ管理を備えた環境を構築できます。これによってパートナーとベンダーは独自の仮想スペースを管理して、共有データを管理および分析したり、特定のサービスをオペレーションにホストしたりできます。これらの仮想環境では、データレイクを作成して、データの収集と分析を促進することができます。複数の施設からデータが集約されるので、地域レベルと個々の施設の両方で独自の洞察が得られます。地域の観点で言えば、IDMZ はさまざまなタイプの施設にサービスを提供する場合があるため、さまざまなパートナーや機械 / 機器ベンダーを利用する場合があります。さらに、各地域が準拠しなければならない規制とコンプライアンス要件は異なる可能性があります。地域の IDMZ レベルでカスタマイズを行うことで、地域の規制と要件に準拠することができます。

関連する点として、すべてのパートナーや請負業者が IDMZ に仮想プレゼンスを持つとは限らないため、クラウド IDMZ 環境はリモート接続を管理するためのスケーラブルなソリューションとなります。そのようなリモート接続には、リモートエキスパートのための VPN 接続や、SaaS などのサービスを提供する OEM やサードパーティ事業者のための直接インターフェイスポイントなどがあります。これらの接続も ROC 担当者が一元的に監視して管理できます。ROC 担当者は、展開している地域の関係と要件に基づいてソリューションをカスタマイズできます。

ハイブリッドクラウド IDMZ は優れた柔軟性と復元力を提供します

すべての接続がハイブリッドクラウド IDMZ を経由するので、サードパーティや外部の接続およびサービスを管理できるだけでなく、企業の接続、アプリケーション、データの共有方法もオペレーションが制御できます。これによって、接続元に関係なく明確で簡潔なセキュリティ戦略を策定でき、セキュリティ管理が回避される危険性があるバックドア接続の可能性を最小限に抑えることができます。

最後に、ハイブリッドクラウド IDMZ はソフトウェアベースのソリューションであるため、優れた柔軟性と復元力を提供します。まず、施設を外部から隔離する必要がある場合は、IDMZ への接続を無効にすることで迅速に隔離できます。ミッションクリティカルなリアルタイム機能は引き続きオンプレミスに存在するので、アウトバウンド接続を切断しても実際のオペレーションが中断されることはありません。問題が解決されたら接続を復元できます。壊滅的な出来事の影響を受けて IDMZ が機能しなくなる極端なケースにおいても、IDMZ は物理的な場所やハードウェアのセットに依存していないので、自動化の支援を受けながら侵害された IDMZ を排除し、新しい IDMZ を迅速にインスタンス化して接続の継続性を維持し、ダウンタイムを最小限に抑え、サービスを素早く復元することができます。

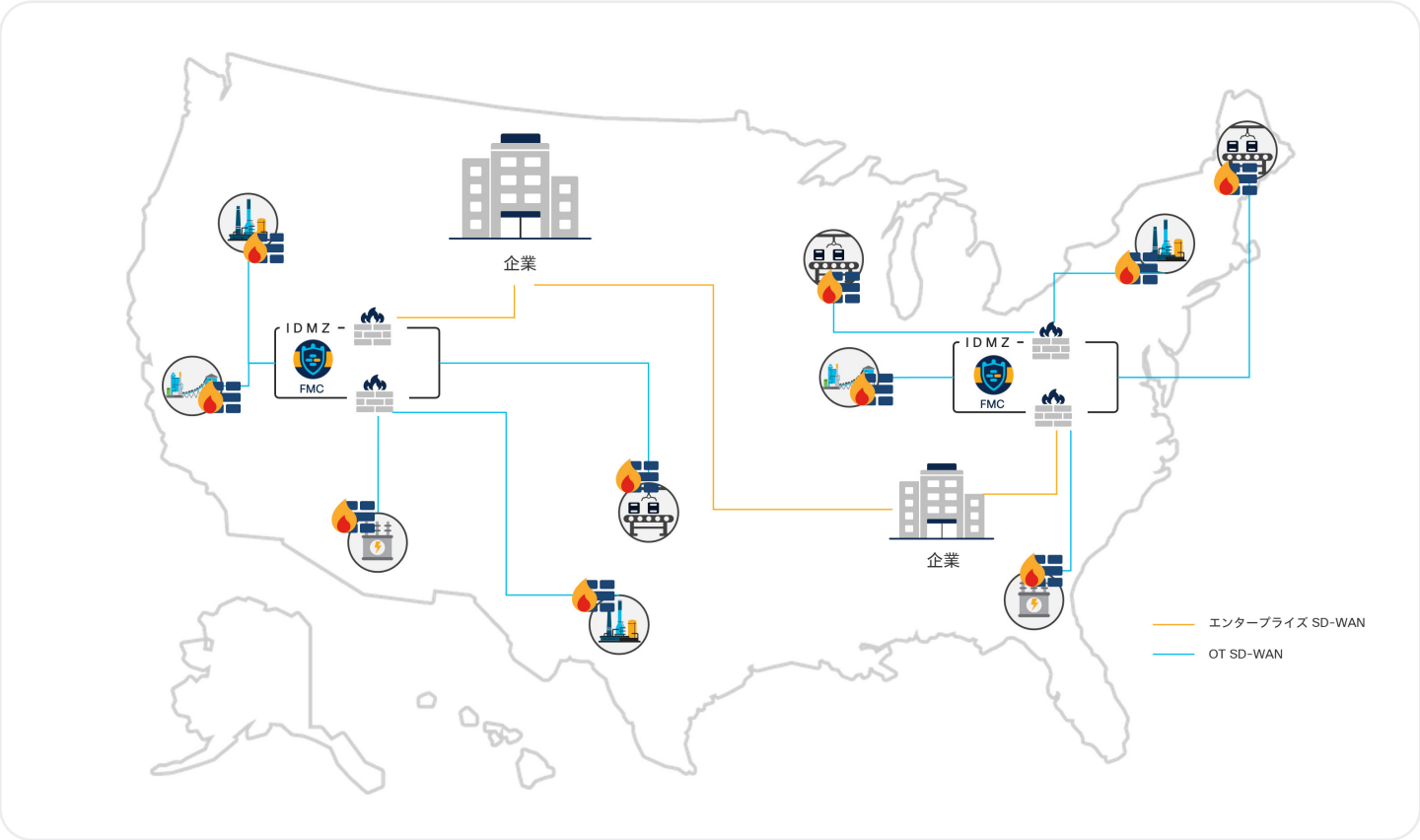
ROC モデルは、一貫性と運用効率を向上させるためのさまざまな機会を提供します。ハイブリッドクラウド IDMZ を利用すれば、複数の拠点からデータを集約して分析と予知保全に役立てることができます。また、複数の拠点で一貫したポリシーを維持し、十分な情報に基づいて意思決定を行い、予期しない課題を回避し、ビジネスニーズにより正確に集中できます。

ハイブリッドクラウド IDMZ の実践

1 つの製品、テクノロジー、方法論で産業自動化制御システム（IACS）のアプリケーションを完全に保護するのは不可能です。IACS のアセットを保護するには、内部および外部のセキュリティ脅威に対処する多層防御のセキュリティアプローチが必要になります。シスコと Rockwell Automation 社が開発した Converged Plantwide Ethernet（CPwE）ガイドをはじめとするさまざまな設計ガイドや実装ガイドでは、産業ゾーンと企業ゾーンの間のアプリケーション トラバーサルを物理 IDMZ で認識するための推奨事項が説明されていますが、最新のネットワークではクラウドを活用できる新しいアプローチが必要です。

企業のエンジニアリングチームは複数の拠点をサポートするのが一般的です。今日では、拠点は個別に管理されている場合があり、アーキテクチャチームが拠点の実装方法のブループリントを提供し、オンサイトの要員がネットワークを実装してメンテナンスしています。要員が異動し、要件が変化するにつれて、拠点は意図された設計から逸脱し始めます。産業ゾーンからのノースバウンド通信に対するセキュリティ管理が定義されている例を見てみましょう。それらのポリシーは文書化されて個々の拠点に伝達されており、常駐のセキュリティ専門家によってローカルファイアウォールに実装されます。ファイアウォールログがセキュリティ情報イベント管理（SIEM）システムに送信されていても、これらのネットワークを完全に把握するには、セキュリティ オペレーション センター（SOC）が個々の拠点にアクセスして、実施されているセキュリティ対策を監査する必要があります。

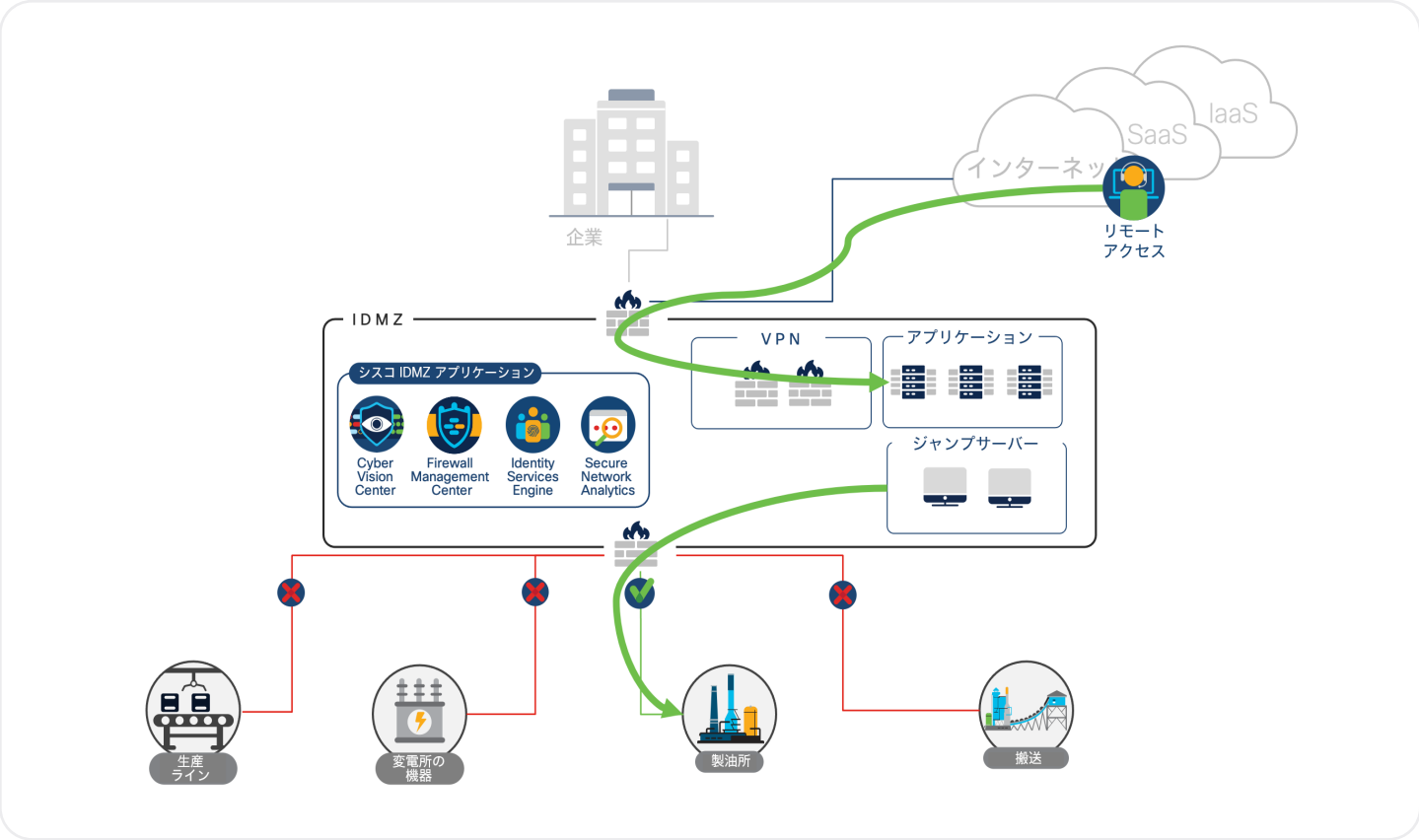
図 4. 一元化されたファイアウォール管理機能



一元化された IDMZ モデルにファイアウォール管理を移行すれば、管理対象のそれぞれの場所におけるあらゆるセキュリティアクティビティをセキュリティオペレータがまとめて確認できるようになります。ポリシーの変更をあらゆる場所に均一に展開でき、拠点固有の逸脱を単一の管理プラットフォームで追跡することができます。

ハイブリッドクラウド IDMZ のメリットを享受できる別のユースケースとして、安全なリモートアクセスがあります。IACS デバイスが停止したときや、高度なトラブルシューティングが必要になったときに、リモートエキスパートがデバイスにアクセスして詳細な分析を行うことが必要になる場合があります。

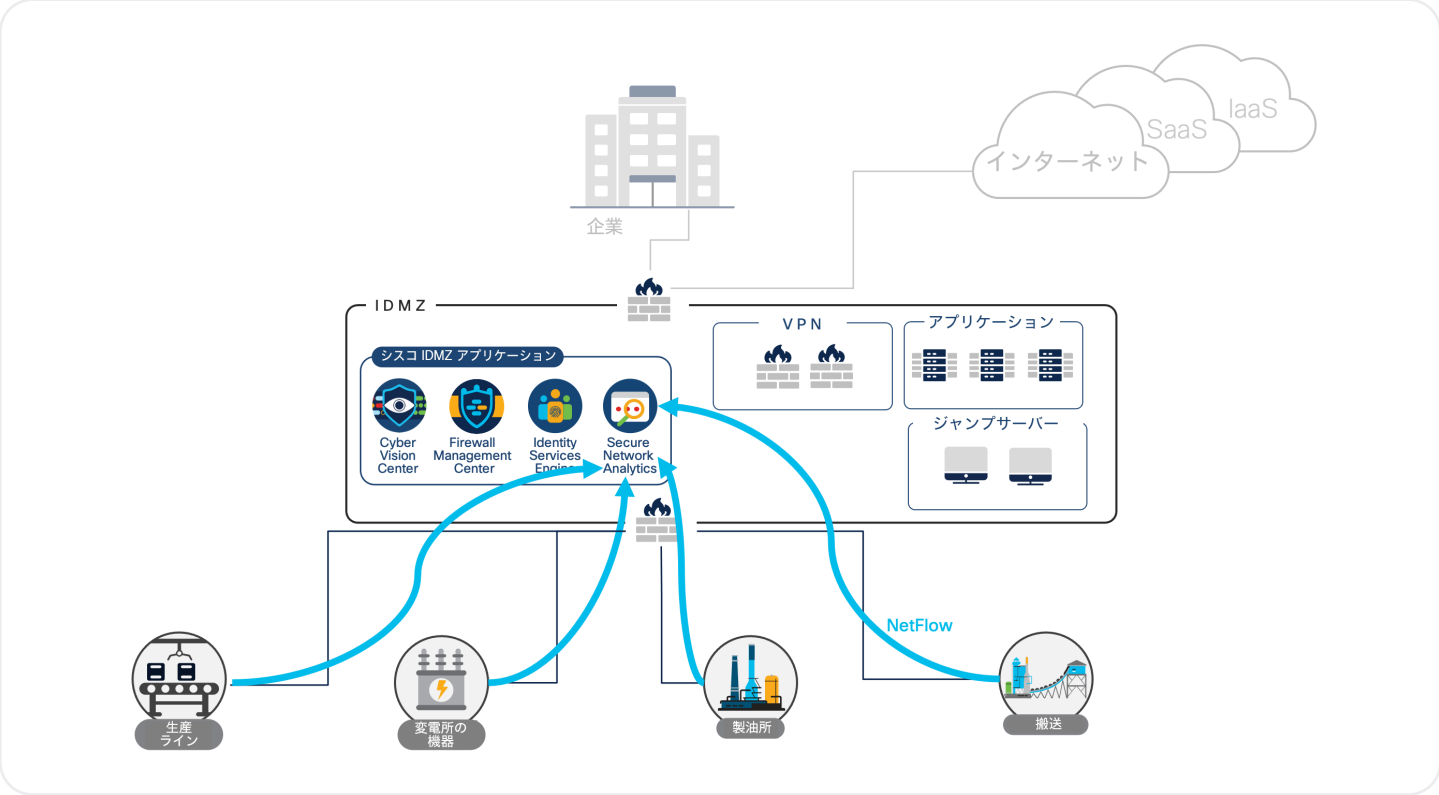
図 5. ハイブリッドクラウド IDMZ による安全なリモートアクセス



安全なリモートアクセスの原則はクラウドでも変わりません。つまり、VPN クライアントを使用してリモート アクセス ネットワークにアクセスし、多要素認証（MFA）を使用してユーザーの本人確認を行い、ジャンプサーバーを使用してリモートセッションでベンダーが使用するデバイスを制御します。ただし、ハイブリッドクラウド IDMZ を通じてアクセスを制御している場合には単一のアクセスポイントが提供されます。これによって、産業拠点をエンタープライズ ネットワークから独立させながら、そのアクセスポイントを通じてあらゆる接続試行を管理することができます。ユーザーがクラウドでのセッションを終了すると、ユーザーの本人確認が行われ、デバイスのポスチャが評価されます。それらの初期チェックに合格したら、ユーザーポリシーを通じてリモートエキスパートを目的のネットワークにリダイレクトできます。ユーザーの接続を終了すること、特定の産業用ネットワークへのアクセスを閉じることはいつでも可能です。

アウトバウンド通信でもこのメリットを享受できます。ネットワークの検出と対応（NDR）ソリューションは疑わしいネットワークアクティビティを検出するために使用されており、異常なトラフィックや悪意のあるトラフィックにチームが対応できるようになります。豊富なコンテキストを提供する NDR ツールを展開すれば、ネットワークアクティビティの全体像を把握でき、ネットワーク上のユーザー、対話しているデバイス、共有されているデータの種類に関する洞察が得られます。セキュリティチームはこの可視性によって脅威を検出できるだけでなく、脅威の発生源、伝播した可能性がある他の場所、侵害されたユーザーも特定できます。

図 6. ハイブリッドクラウド IDMZ を使用したテレメトリの集約と関連付け



ネットワーク全体でテレメトリを集約して関連付けることで、インシデント管理と脅威ハンティングを向上させることができます。Cisco Secure Network Analytics は、既存のネットワーク インフラストラクチャ全体にエージェントレスで展開でき、Cisco Identity Services Engine (ISE)、Cisco Cyber Vision（産業用ネットワーク専用の可視化を提供）、Cisco AnyConnect® からメタデータを取り込んでネットワークにおけるユーザー、デバイス、アプリケーションのコンテキストを把握できます。1 つの施設で悪意のあるアクティビティが検出された場合には、脅威を封じ込めるために迅速な措置を行いながら、同じツールを使用して他の施設を調査することができます。

まとめ

産業自動化制御システム（IACS）セキュリティおよびクラウドセキュリティのリーダーであるシスコは、IDMZ のクラウド移行戦略を強力に支援できます。クラウド導入プロセスには、コスト削減、人工知能や機械学習のツールキットへのアクセス、スケーラブルなインフラストラクチャの活用といったさまざまな段階がありますが、シスコはそれらのどの段階にあるお客様にも、ダウンタイムを最小限に抑えて課題を迅速に解決できるツールと専門知識を提供できます。

詳細および開始方法については、以下を参照してください。

- シスコの産業用セキュリティの Web ページ
- Cisco Secure Firewall ソリューションの詳細
- Zero Trust セキュリティの産業ネットワークへの拡張に関するホワイトペーパー
- 「IT と OT のサイバーセキュリティ：統合された組織と分断された組織」ホワイトペーパー
- お問い合わせ

C11-2980061-00 05/22