appgate

Appgate SDP ゼロ・トラスト・ネットワーク・アクセス
を利用したアメリカ合衆国国防総省における戦術的エッジおよび拒否、劣化、断続、帯域幅制限（DDIL）環境での安全な運用

目次

要旨

アメリカ合衆国国防総省（DOD）は、陸、空、海、宇宙、サイバーなど、あらゆる領域にわたる作戦の安全を確保すると同時に、最も困難な環境においてもシームレスで回復力のある通信を確保するという複雑な課題に直面しています。統合全領域指揮統制(JADC2)構想はこの必要性を反映したもので、新たな脅威に対してより迅速で、より多くの情報に基づいた対応を可能にするために、軍の各部門にまたがる戦闘能力の統合を目指しています。作戦上の優位性を維持するために、国防総省は、特に従来の通信方法が信頼できない可能性がある拒否、劣化、断続的、限られた帯域幅（DDIL）環境において、堅牢で適応性のあるソリューションを必要としています。

戦術的エッジとDDIL環境における課題

DDIL環境は、以下のようなユニークな課題をもたらします:

- 中断のない指揮統制: 途絶えることのない指揮統制：通信チャネルが途絶えたにもかかわらず、指揮統制の継続性を維持すること。
- 安全で回復力のある通信: 通信の完全性を維持しながら、サイバー脅威から機密情報を保護します。
- 連合の相互運用性: 異なるツール、技術、セキュリティ標準を使用する連合パートナー間でのシームレスな情報共有を可能にします。
- 運用の柔軟性: Sインフラや接続性が限られた環境でのミッションの成功を支援します。

国防総省は、これらの課題に対処し、米軍と連合パートナー間の相互運用性を促進し、統一された安全な作戦態勢を確保するソリューションを必要としています。.

APPGATE SDP ゼロ・トラスト・ネットワーク・アクセス

Appgate SDP Universal ZTNA は、国防総省の特定のニーズに対応するのに適しています。具体的には、セキュリティに対する堅牢でデータ中心のアプローチ*を提供し、運用環境に関係なく、適切なユーザーが適切なタイミングで適切なデータにアクセスできるようにします。

主な機能は以下の通り::

- 動的アクセス制御: Appgate SDPは、ID属性、デバイスの遠隔測定、環境コンテキストを活用し、隔離された環境や競合環境であっても、動的にセキュリティポリシーを適用します。
- 弾力的な運用: Appgate SDPは、分散ダイレクトルートアーキテクチャ上に構築されているため、エンタープライズリソースとローカル戦術リソースの両方へのシームレスなアクセスが可能です。
- 環境を超えた統合アクセス: ユーザーは、同じZero Trust原則を使用して、戦術的リソースとエンタープライズリソースの両方にアクセスすることができ、すべての運用レベルで一貫したセキュリティ体制を確保できます。
- スケーラブルで軽量な展開: Appgate SDPは、小型のフォームファクタ・デバイスや仮想化環境内での展開をサポートし、前方展開や戦術的なエッジ・シナリオにおける柔軟性と拡張性を実現します。
- クロークド – シングルパケット認証（SPA**）により、Appgate SDPはネットワークを見えなくします。これにより、ネットワークエッジが隠蔽され、敵が保護されたリソースを特定し攻撃することが極めて困難になります。

**See 'Appgate SDP Understanding Single Packet Authorization (SPA) White Paper for a further understanding. [https://www.appgate.com/resources/appgate-sdp/single-packet-authorization-whitepaper] を参照

相互運用性の課題の解決

ユーザーアクセスを管理するために使用されるツールや技術が多様であるため、国防総省の各部署や連合パートナー間での相互運用性は重要な課題となっています。Appgate SDP Universal ZTNAは、以下を含む柔軟で包括的なアプローチにより、これらの課題に対処します:

- クライアントレスアクセス: 標準的なウェブブラウザ経由でセキュアなアクセスが提供されるため、迅速なオンボーディングと連合運用に最適です。
- セキュアなブラウザアクセス: ユーザーのローカル環境を保護するためにブラウジング・セッションを分離することで、制御の行き届かない環境でも安全なデータ・アクセスを実現します。
- ブラウザ拡張機能ベースのアクセス: クライアントを完全にインストールすることなくセキュアな接続を可能にすることで、ミッション・コンピュータのようなヘッドレス・クライアントでも、さまざまなセキュリティ・ツールで運用するユーザーに柔軟性を提供します。
- 既存のソリューションとの相互運用性: さまざまな環境でのシームレスな統合と統一されたポリシーの適用を促進することで、さまざまなテクノロジを使用しても一貫したセキュリティ体制を確保できます。

JADC2目標との整合

Appgate SDP Universal ZTNAは、安全で動的なアクセス制御を可能にし、マルチドメイン運用をサポートすることで、JADC2の目的と密接に連携しています。JADC2のミッションの成功には、競合環境において弾力性のあるオペレーションを維持し、さまざまなテクノロジーやパートナーとの相互運用性を確保するプラットフォームの能力が不可欠です。

実証済みのセキュリティ

Appgate SDP Universal ZTNAは、国防総省が要求する最高のセキュリティ基準を満たすために、厳格なテストと認証を受けています:

- 複数の運用許可（ATO)(IL2-IL6): 非機密環境から機密環境まで、すべてのセキュリティ・ドメインにわたる安全なアクセスをサポートします。
- コモンクライテリアEAL認証: 情報技術（IT）製品やシステムのセキュリティを評価・認証するための国際基準を提供します。
- NIAPプロテクション・プロファイル（進行中): Appgateは、米国政府のセキュリティ要件を満たす複数のプロテクション・プロファイル認証を受けており、機密および戦術的なネットワーク展開をサポートしています。
- DISAカテゴリ保証リスト（CAL）承認: 国防総省の厳しいセキュリティおよび相互運用性基準を満たしています。

国防総省がゼロ・トラスト戦略を推進する中、Appgate SDP Universal ZTNAは、最も困難な戦術的エッジやDDIL環境においても、すべてのドメインにわたって安全で弾力性のある運用を保証する強力で適応性のあるソリューションを提供します。シームレスな通信、クローキング、ダイナミックなアクセス制御、相互運用性を促進することで、Appgate SDPは、今日の複雑で競争の激しいグローバルな状況において、国防総省のミッションの成功をサポートする独自の地位を確立しています。

戦術的エッジと拒否、劣化、断続、帯域制限（DDIL）環境におけるゼロトラスト・ネットワーク・アクセス

現代の防衛・軍事作戦では、特に戦術的エッジ環境において、安全で回復力のある通信・情報共有能力が必要とされます。敵対勢力との交戦には、従来の通信方法が危殆化するか、存在しないような、拒否され、劣化し、断続的で、帯域幅が制限された（DDIL）能力が必要であり、堅牢で適応性のある通信ソリューションが必要となります。国防総省（DOD）は、特殊作戦部隊から通常兵科に至るまで、すべての作戦部隊がこのような複雑なシナリオで効果的に活動できるよう、ニアピアの敵からの脅威に対処することを優先しています。

DDIL環境は、さまざまな軍事作戦にまたがる独自の課題を提示します。これには、DODの指揮統制センター（通常、C2、C4、C5と呼ばれ、それぞれの特殊能力に基づいています）の枠組みが示すように、中断のない指揮統制、通信、コンピュータ、サイバー防御の確保が含まれます。

さらに、DDIL 環境はしばしば次のような複雑な事態を引き起こします:

- 限られた状況認識
- 安全でない通信
- 連合軍の相互運用性
- 中断されたデータ共有
- デバイスとシステムの非互換性
- インフラの制約
- 断片的なコラボレーション
- 物理的フットプリント

米特殊作戦司令部（SOCOM）や米戦闘司令部（COCOM）など、国防総省のさまざまな組織に共通する要件は、DDIL環境の制約や課題に適応できる弾力性のある通信ソリューションの必要性です。

軍事作戦には、多様なプラットフォーム、技術、セキュリティ・プロトコルを介して情報を安全に共有する必要のあるミッション・パートナーや連合パートナーが関与することが増えているため、このような環境では相互運用性が特に重要になります。各パートナーが異なるツールを使用するため、互換性の問題が生じ、作戦の有効性が妨げられる可能性があります。

このような多様なシステム間でシームレスな通信を確保し、DDIL 条件下でも安全な情報共有を行うことは、ミッションの成功に不可欠です。DDIL環境で活動するもう一つの重要な側面は、物理的脅威とサイバー脅威の両方に耐えることができる安全で弾力性のあるインフラの必要性です。その結果、国防総省は紛争環境でも運用でき、高度なサイバー脅威から保護できるソリューションを配備しなければなりません。これには、データの暗号化、アクセス制御、攻撃を受けても中核機能を維持できるよう設計されたシステムの確保などが含まれます。

米本土や海外から戦術的な端まで、国防総省の企業には、ABMS（Advanced Battle Management System）（米空軍）、Project Convergence（米陸軍）、NOA（U.S. Naval Operational Architecture）、Force Design（米海兵隊）など、すべての軍部からの戦争遂行能力を統合するJADC2（Joint All-Domain Command and Control）のようなプログラムが必要です。この統合により、シームレスでマルチドメインな作戦が可能になり、空、陸、海、宇宙、サイバーの各ドメインにまたがるコミュニケーションと調整が強化されます。しかし、これらのプログラムの成功は、DDIL環境における作戦即応性に大きく依存しています。

指揮統制センター

指揮統制センターは、軍事・統合作戦やサイバーセキュリティ作戦における作戦、意思決定、資源管理を支援するために、重要な情報を収集・処理する重要な役割を担っています。

それぞれの機能の内訳は以下の通りです:

- **C2 -** 指揮・統制: 任務遂行のために指揮官が部隊に対して行使する権限と調整を指します。
- **C4 -** 指揮・統制・通信・コンピューター: 意思決定と状況認識を強化するため、通信システムとコンピュータネットワークを組み込んでC2を構築します。
- **C5 -** 指揮・統制・通信・コンピューター・サイバーセキュリティ：サイバーセキュリティを重視し、サイバー能力を防衛・攻撃作戦に活用することにより、サイバー作戦を追加してC4を拡張します。

Appgate SDP の機能

Appgate SDP Universal Zero Trust Network Access (ZTNA)は、すべての運用環境において、国防総省（DOD）特有の進化するニーズに効果的に対応し、適切なユーザーが適切なタイミングで適切なデータにアクセスできるようにします。Appgate SDPは、ID属性、デバイスの遠隔測定、およびコンテキスト要素を活用することで、運用上のニーズに沿ったリアルタイムの動的なアクセス決定を可能にします。この機能は、企業ネットワーク、前方展開ユニット、戦術的エッジオペレーション、OTおよびIoTデバイス、SIPRNet（Secret Internet Protocol Router Network）などのエアギャップ／機密環境、JWICS（Joint Worldwide Intelligence Communication System）など、さまざまな環境に拡張されます。

Appgate SDPは、データ中心のアプローチを採用し、基盤となるデータ管理の改善は本質的に、より優れた、より安全なユーザー／ID管理につながることを認識しています。これにより、Appgateは、各ユーザーとシステムの特定のニーズに合わせた正確で動的なアクセス制御を提供することができます。このプラットフォームは、タグとラベルを活用して、リアルタイムの状況に適応するきめ細かなアクセス・ポリシーを定義し、実施します。この機能は、国防総省が2023年6月27日付で発表した「データ、アナリティクス、人工知能の採用戦略」で説明されているように、国防総省のデータ検索・発見分類戦略に直接合致します。国防総省は、「...改良の対象となるデータセットは、データ検索と発見を可能にするメタデータに基づいて構築され、関連性と任務価値のために優先順位付けされます」と述べています。

堅牢なZTNAソリューションにこれらのコンセプトを組み込むことで、国防総省は多様で競争の激しい戦場で作戦の成功を収めることができ、「国防総省ゼロ・トラスト・オーバーレイ」（2024年2月）および「DODゼロトラスト戦略、v1」（2022年10月）などの文書で国防総省CIOが定めたゼロ・トラスト・フレームワークの目標に確実に準拠することができます。Appgate SDPは、ユーザとシステムが明示的に許可されたデータのみにアクセスできることを保証し、すべてのDOD業務にわたって重要な情報を保護します。この適応性は、従来の任務から機密性の高い任務まで、あらゆるシナリオにおいてセキュリティと作戦の有効性を維持するために極めて重要です。

Appgate SDPは、競合環境で効果的に動作するユニークな能力と、基礎となるインフラ全体（すなわち、リソースとアプリケーション）を敵に発見されないようにする高度なクローキング機能によって実証されているように、ミッション優先のアプローチにとって理想的なソリューションです。Appgate SDPは、重要なリソースを無許可のユーザーから見えないようにすることで、サイバー攻撃の標的を劇的に減らします。このアプローチは、国防総省の多様な任務要件に沿うように設計されており、エンタープライズから戦術的なエッジ環境に至るまで、あらゆるレベルの運用において比類のないセキュリティと柔軟性を提供します。

データ中心のセキュリティ: Appgate が国防総省でゼロトラストを実現する方法

Appgate SDPの主な機能はゼロトラストネットワークアクセス（ZTNA）を提供することですが、その真の強みは、アクセスポリシーを実施するために使用されるデータ中心のアプローチにあります。ネットワークへのアクセス許可だけに焦点を当てるのではなく、Appgate SDPのポリシーエンジンは、ワークロード、アプリケーション、またはデータがどのようにタグ付けまたはラベル付けされているかに基づいて決定を下すように設計されています。.

Appgate SDPによるタグ、ラベル、メタデータの活用方法

Appgate SDPはさまざまなソースと統合し、タグ、ラベル、その他のコンテキストに富んだメタデータを消費して、リアルタイムのセキュリティポリシーを適用します。このアプローチにより、動的なアクセス制御が可能になり、機密データやミッションクリティカルなシステムのきめ細かな保護が実現します。

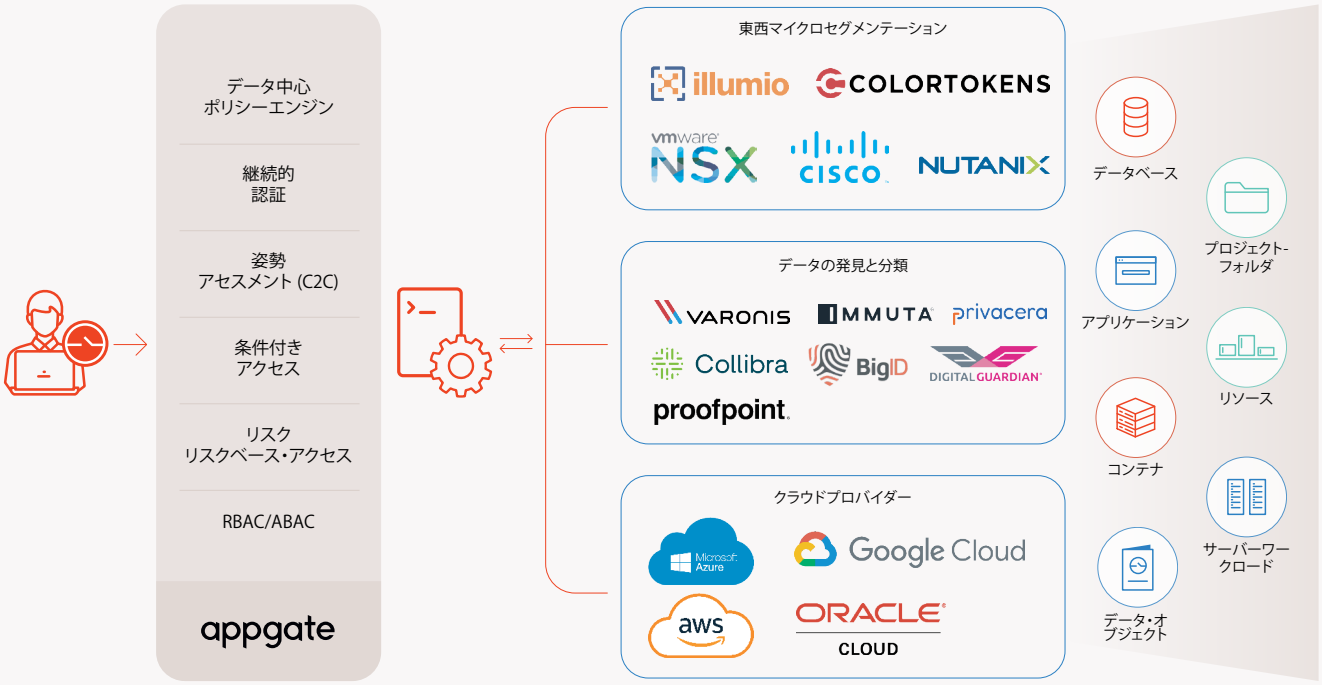
主な機能:

- マイクロセグメンテーションオーバーレイ/アンダーレイ: Appgate SDPは、マイクロセグメンテーションツールからタグとラベルを消費し、ネットワーク内のトラフィックのセグメンテーションに基づいて動的なアクセス制御を実施します。
- データ発見、分類、ガバナンス: Appgate SDPは、例えば NOFORN、FVEY、CUI、HIPAA、 PIIなどのツールと統合して、データの機密性や分類レベルを表すタグを消費して、データを分類し、ラベル付けします。
- インフラプロバイダー（クラウドおよびハイパーバイザー）: Appgate SDPは、クラウドプラットフォーム（AWS、Azure、GCP）やハイパーバイザのようなインフラストラクチャプロバイダからタグを取得し、IL4/IL5分類のようなワークロード属性、DevとProdのような環境タイプ、または特定のプロジェクトやプログラムに基づいたポリシーを適用します。
- データ損失防止（DLP）ツール: Appgate SDPはDLPツールのタグを活用し、データのラベル付け方法と関連するリスクレベルに基づいてセキュリティポリシーを適用します。
- DODオペレーションにおける適応性: Appgate SDPのデータ中心のアプローチは、国防総省が直面する独自のセキュリティ課題に対応するように設計されています。Appgate SDPは、進化するミッション要件、セキュリティ分類、運用ニーズに動的に対応する、柔軟なタグおよびラベル駆動型システムを提供します。メタデータに基づいてアクセス・ポリシーを継続的に調整することにより、Appgateは、適切な個人が適切なタイミングで適切なリソースにアクセスできるようにします。

ゼロ・トラスト・フレームワークにおけるデータ中心のセキュリティk

従来のセキュリティモデルでは、アクセスは通常、IPアドレスベースのアクセス制御リスト（ACL）などの静的なパラメータによって管理されていました。このアプローチはかつては効果的でしたが、DODのダイナミックでリスクの高いオペレーションには段々と不十分になってきています。ACLの静的な性質は管理を困難にし、時間の経過とともに継続的に追加されますが、重要なシステムが壊れることを恐れてほとんど削除されないからです。その結果、これらのリストは古くなり、古い項目で肥大化し、運用と維持に多大な人手を必要とします。

Appgate SDPのデータ中心モデルは、ワークロード、アプリケーション、データに関連するタグやラベルに焦点を当てることで、このような課題を克服しています。静的なルールに依存するのではなく、タグとラベルに基づいてリアルタイムでポリシーを動的に調整することで、運用のオーバーヘッドを削減し、セキュリティ体制を強化します。



データ中心のセキュリティモデル。

戦術エッジとDDIL環境におけるAPPGATE SDP

Appgate SDPは、企業へのDDILネットワーク接続がある環境であっても、戦術的エッジユーザが企業とローカル／前方に配置された戦術的リソースの両方にシームレスにアクセスできるようにします。堅牢で適応可能なゼロトラスト・アプローチを実装することで、Appgate SDPは接続状況に関係なく、一貫してセキュリティ・ポリシーを実施します。

タクティカルエッジでは、Appgate SDP Universal ZTNAは、ローカルおよびエンタープライズからの重要なリソースへの並列アクセスを可能にします。その分散アーキテクチャは、リソースへの直接接続をサポートするため、ユーザーは集中型のクラウドベースのネットワークに依存することなく、運用効率を維持することができます。これにより、ローカルの戦術システムであれ、エンタープライズ・アプリケーションであれ、ゼロ・トラスト原則の一貫した適用が実証されます。

- 環境を超えた統合アクセス: ユーザーは、同じZero Trust原則を使用して、戦術的リソースとエンタープライズ・リソースの両方にアクセスすることができ、すべての運用レベルで一貫したセキュリティ体制を確保できます。
- 自律的な運用: エンタープライズから切り離された場合でも、Appgate SDPはローカルでZero Trustポリシーを適用し続けるため、妥協することなくセキュリティを維持できます。
- 運用の維持-ローカル管理: 連合軍のオンボーディング、アクセスのプロビジョニング、Zero Trustポリシーの適用はすべて、企業の接続性とは無関係に、戦術的なエッジで管理できます。
- 容易な同期: 接続性が回復すると、Appgate SDPはローカル環境とエンタープライズ環境をシームレスに同期し、必要に応じてバージョン管理とロールバックを適用します。これは時間に依存しません。

さまざまな連合パートナーを含む共同作戦では、強固なセキュリティ態勢を維持することはさらに困難になります。Appgate SDPは、DDIL環境であっても、このようなパートナーの迅速かつ安全なオンボーディングを可能にします。

たとえば、遠隔地で連合軍と活動する米軍特殊作戦チームは、Appgate SDPを使用して、新たに到着した連合軍部隊のミッションクリティカルなシステムへのアクセスを許可することができます。企業ネットワークから切り離されているにもかかわらず、Appgate SDPのローカルインスタンスは、新しいユーザーアカウントのシームレスな作成、アクセスのプロビジョニング、厳格なZero Trust制御の適用を可能にします。これにより、新規ユーザが導入されてもセキュリティ体制が維持され、不正アクセスが防止されます。さらに、これらのユーザーはエッジで遮蔽され、その存在が効果的に見えなくなります。

たとえ「プライベート・クラウド」として販売されているものであっても、真のオンプレミス・ソリューションとクラウドベースの製品を区別することが重要です。自社のプライベート・クラウドが戦術的な設定においてオンプレミスと同等であると主張する企業は、誤解を招きやすいです。プライベートクラウドにはいくつかの利点があるかもしれませんが、基本的に自社のインフラへの接続に依存していることに変わりはありません。対照的に、Appgate SDPはDDIL運用のために構築されています。すべての外部通信が失われたとしても、ローカルのAppgate SDPインスタンスは機能し続け、中断のないアクセス制御とセキュリティを確保します。

最も重要なことは、ユーザーエクスペリエンスが中断されないことです。企業ネットワークが利用できなくても、チームは何も変更する必要はありません。Appgate SDPは、利用可能なリソースに応じてアクセスを自動的に調整し、継続的で透過的な運用を保証します。ネットワークが再接続されると、新規ユーザーのオンボーディングやポリシーの調整を含むすべてのローカル変更が、時間制限なしにエンタープライズ環境に同期されます。この同期化プロセスにはバージョン管理が含まれており、必要に応じて変更を見直し、ロールバックすることができます。この機能により、最も困難な作戦環境においても、連合軍はミッション全体の完全性を損なうことなく、安全かつ効率的に共同作業を行うことができます。

軍部、国防総省、連合軍環境にわたる相互運用性の課題の解決

ユーザー・アクセスを管理するためのツール、テクノロジー、ポリシーは、軍部や国防機関によって多種多様であるため、DOD 内では相互運用性が依然として大きな課題となっています。この課題は、パートナーがDODゼロトラスト・プロトコルに直接合致しない異なるセキュリティ基準やシステムを持つ可能性のある連合環境において増幅されます。このようなさまざまな環境でシームレスな運用と安全なデータアクセスを確保することは、特に複雑な前方展開の戦術的シナリオにおいて、ミッションの成功に不可欠です。

Appgate SDPは、DDIL環境でのセキュアなアクセスを保証する柔軟で包括的なZero Trustソリューションにより、これらの相互運用性の課題に対処します:

1. クライアントレスアクセス: Appgate SDP Universal ZTNAには、堅牢なクライアントレスアクセスポータルが含まれており、ユーザーは標準的なWebブラウザを使用してリソースに安全に接続できます。これは、連合作戦や迅速なオンボーディングが必要な場合など、すべてのデバイスにエージェントを配備することが現実的でない場合に最適です。エンドポイントデバイスに大掛かりなソフトウェアをインストールすることなく、安全なアクセスを保証します。
2. セキュアなブラウザアクセス: 潜在的な脅威からユーザーのローカル環境を保護するために、セキュアなブラウザベースのアクセスと分離ブラウジングセッションを提供します。mTLSをベースとするこの方法は、ブラウザ内で直接セキュリティポリシーを実施することにより、Zero Trustアーキテクチャをサポートし、機密データへのセキュアなアクセスを保証し、連合作戦や劇場内作戦のような統制の取れていない環境でもリソースに安全にアクセスできるようにします。
3. ブラウザ拡張機能ベースのアクセス: Appgate SDPのブラウザ拡張機能により、クライアントを完全にインストールすることなく、セキュアなリソースアクセスが可能になります。この機能は、ユーザーがさまざまなセキュリティツールや、特殊な兵器システムやヘッドレスクライアントなど、フルクライアントをサポートできないデバイスで操作する場合に特に便利です。Appgate SDPは、さまざまな軍事部門、国防総省機関、および連合パートナーの多様な運用ニーズに対応する、柔軟かつセキュアなアクセスソリューションを提供します。

4. 既存のZTソリューションとの相互運用性: Appgate SDP Universal ZTNAは、さまざまな支社や連合パートナーがすでに使用している他のZero Trustソリューションとの相互運用性を促進します。この機能により、さまざまな環境でシームレスな統合と統一されたポリシーの適用が可能になり、多様なテクノロジを使用してもセキュリティを確保できます。このアプローチは、ミッション要件が進化し、新たなパートナーが運用フレームワークに加わる際に不可欠であり、一貫したゼロ・トラスト・ポリシーを適用し、効率的に管理することを可能にします。
5. クローク – シングルパケット認証により、Appgate SDPはネットワークを不可視化します。これにより、ネットワークエッジを隠蔽することができ、敵が保護されたリソースを特定し攻撃することが極めて困難になります。

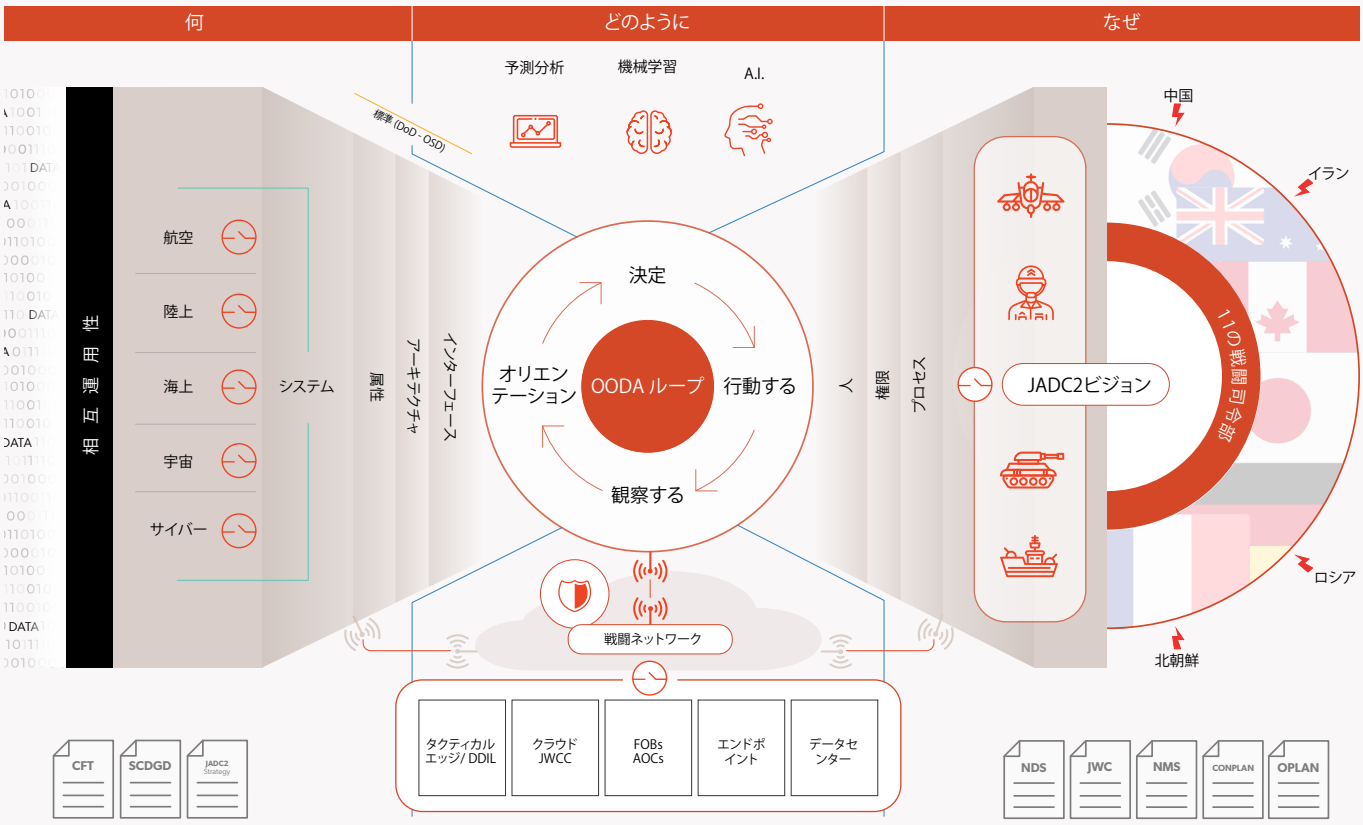
これらの機能は、国防総省の複雑で進化するミッション要件に対応する多用途で安全なゼロ・トラスト・ソリューションの提供というAppgateのコミットメントを強調するものです。Appgate SDPは、完全に接続された企業、戦術的なエッジシナリオ、またはさまざまなセキュリティ態勢を持つ連合作戦のいずれで運用されている場合でも、相互運用性の課題に対処するための堅牢で適応性の高いソリューションを保証します。

JADC2との連携

JADC2は、空、陸、海、宇宙、サイバーなど、すべての領域にわたるセンサー、戦闘員、指揮統制ノードを統合し、接続します。その目的は、戦場全体にわたるシームレスでリアルタイムのコミュニケーションと意思決定であり、新たな脅威に対してより迅速かつ情報に基づいた対応を可能にします。

Appgate SDPはJADC2の目標に密接に合致しており、特にドメイン間や連合パートナーとの安全でシームレスなコミュニケーションを促進します。その方法は次のとおりです:

1. セキュアでダイナミックなアクセス制御: Appgate SDP Universal ZTNAは、場所や運用ドメインに関係なく、適切なユーザが適切なタイミングで適切なデータにアクセスできるようにします。これは、あらゆる領域にわたる情報への迅速かつ安全なアクセスがミッションの成功に不可欠なJADC2にとって極めて重要です。
2. 相互運用性: Appgate SDPは、既存のさまざまなテクノロジやセキュリティフレームワークと統合できるため、JADC2の多様なニーズをサポートできます。Appgate SDPは、クライアントレス・アクセス・ポータル、セキュアなブラウザ・ベース・アクセス、他のZero Trustソリューションとの相互運用性のいずれを通じてであっても、軍のすべての部門、国防総省機関、連合パートナー間でのセキュアな通信と情報共有を保証します。
3. 競合環境における回復力のある作戦: DDIL環境など、通信リンクが劣化したり切断されたりするシナリオでは、Appgate SDPはZero Trustポリシーがローカルで実施されることを保証します。これにより、厳密なセキュリティプロトコルを守りながら部隊が独立して活動する必要があるJADC2作戦において、作戦上のセキュリティと有効性が維持されます。
4. マルチドメイン作戦のサポート: のJADC2の中心となるマルチドメインオペレーションへのサポートは、そのデータ中心アプローチによって強化されています。データの正確性、集中管理、適切な保護を保証することで、Appgate SDPは堅牢なアクセス制御を可能にし、複雑なマルチドメイン環境においても、データの保護と許可された個人によるアクセスのみを保証します。
5. セキュア: JADC2の主要なテナントは、悪意のある活動を抑止するための階層的なサイバー防御を提供することです。Appgate SDPは、Single Packet Authorization (SPA)を使用してネットワークを不可視化し、ネットワークとそのユーザーを隠蔽します。これにより、敵対者や国家攻撃者が保護されたリソースを特定することが非常に困難になります。Appgateは、競合環境において安全なC2（コマンド・アンド・コントロール）を実施するために必要な技術を提供します。.



Joint All-Domain Command and Control（JADC2）は、米軍全軍のデータ・センサー、射撃手、関連通信機器を接続する戦略的な戦争戦闘コンセプトです。

認可および認証

Appgate SDPは、厳格なテストが実施され、国防総省やその他の連邦政府機関によって要求される高いセキュリティ基準を満たすことが認定されています。その高度なセキュリティ態勢は、以下を通じて実証されています：

IL2～**IL6**にわたる複数の**ATO**: Appgate SDPは、非機密データから機密データまでをサポートする環境を含む、インパクトレベル2から6にわたる複数のATO（Authorization to Operateを取得しており、すべてのセキュリティドメインにわたる安全なアクセスを保証しています。

Common Criteria EAL認証: はAppgate SDPはCommon Criteria - Evaluation Assurance Level (EAL)の認証を受けており、国家安全保障システム(NSS)を扱うシステムにとって重要なコンピュータセキュリティ認証の国際的に認知された基準を提供しています。この認証により、AppgateのZTNAプラットフォームは、機密情報や機密扱いの厳しいセキュリティ要件を満たしていることが保証されます。

NIAPコモンクライテリア・プロテクション・プロファイル（処理中）: Appgateは、Protection Profile Functional Package TLS v1 および Protection Profile Application Software v1.4を満たすための認証を受けています。これらは米国政府のNSSセキュリティ要件を満たすものであり、機密および戦術的なネットワークの配備をサポートしています。

DISAカテゴリ保証リスト（**CAL**）承認済み: Appgate SDPは、国防総省情報システム局（DISA）のカテゴリ保証リストに含まれており、DODの厳格なセキュリティおよび相互運用性基準を満たしていることが確認されています。

結論

国防総省（DOD）とその連合パートナーが、複数のドメインにまたがり、さまざまな条件下で活動しなければならない今日の予測不可能な紛争環境では、弾力性があり、適応性があり、安全なソリューションの必要性が最も重要です。Appgate SDPユニバーサル・ゼロ・トラスト・ネットワーク・アクセスは、このような課題に対処することを目的として構築されており、戦術的エッジやDDIL環境での運用に不可欠な堅牢なセキュリティ、拡張性、柔軟性を提供します。

国防総省がゼロ・トラスト戦略を推進し続ける中、Appgateは最も要求の厳しい運用環境においてリソースを安全に接続、管理、保護することで、ミッションの成功をサポートする準備が整っています。これにより、戦術的なエッジオペレーションが、完全に接続されたエンタープライズ環境でのオペレーションと同様に安全かつ効果的であることを保証し、ミッションの成功に貢献します。

Appgate SDP Universal ZTNAが連邦政府機関のセキュリティニーズをどのようにサポートできるかについて詳しくは https://www.appgate.com/federal-division をご覧ください。

Appgateについて

Appgateは、組織の最も貴重な資産とアプリケーションを保護します。アップゲートは、ZTNA（Zero Trust Network Access）とオンライン詐欺防止におけるマーケットリーダーです。アップゲートの製品には、Appgate SDP for Universal ZTNAと360 Fraud Protectionがあります。アップゲートのサービスには、脅威アドバイザリ分析およびZTNA実装が含まれます。アップゲートは、世界中の企業や政府機関を保護しています。詳細は appgate.com をご覧ください。