データシート

A10 Control

アジャイルな運用と自動化を実現する
統合管理・制御・分析プラットフォーム

オンプレミス、クラウド、ハイブリッド環境など、
様々な場所に展開される
A10 ソリューションを集中管理・分析するプラットフォーム

アジャイル管理と インテリジェント分析

ネットワークインフラやセキュリティインフラは複雑さを増し、AI とクラウドテクノロジの急速な導入が進む今日、組織はミッションクリティカルなサービスとビジネスを管理およびサポートする必要に迫られていますが、そこには大きな課題が生じています。

様々な地理的場所や複数のクラウドにネットワークインフラが分散していると、サービスステータスを把握・追跡することが複雑になり時間を要します。AI 駆動のアプリやアプリケーションサービス インフラは、トラフィックとトランザクション量が多く、レイテンシの影響を非常に受けやすいため、正確なキャパシティプランニングと、スケーリング需要へ迅速に対応できることが必要です。そのために管理者は、アジャイル管理とインテリジェント分析を活用して、効率的な運用と管理のワークフローを確立するべきです。

A10 Control は、従来の A10 Harmony Controller と aGalaxy の機能を統合した、A10 ソリューション向けの次世代の管理・分析プラットフォームです。A10 Control は、あらゆるネットワーク環境／クラウド環境に導入されている Application delivery、DNS、CGNAT、SSL Insight、Gi-firewall、DDoS 防御などの A10 Security ソリューションと A10 infrastructure ソリューションを一元管理します。

一元化されたプラットフォームは、A10 アプライアンスを通過するアプリケーションおよびサービストラフィックを収集し、インテリジェントな分析によってサービスとセキュリティの状態を可視化します。

プラットフォーム

Software/VM

関連製品

ADC

A10 Defend
DDoS Protection

CFW

CGN

SSLi

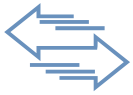
お問い合わせ

https://info.a10networks.com/JP-WebContactUs.html

得られる価値

リアルタイムのインテリジェント分析と可観測性を実現

組織は、サービスの常時稼働を保証する必要があります。サービスの状態を把握し、可観測性を確保することは、運用チームにとって重要なタスクです。A10 Control は、A10 の Advanced Core Operating System（ACOS）を搭載した A10 デバイスを通過するサービストラフィックのメトリクスデータとトランザクションログを収集し、サービスとネットワークインフラで何が起こっているかを詳細に可視化します。インテリジェント分析とカスタマイズ可能なアラートにより、エンドユーザに影響を与える前に潜在的な問題を特定します。コンテキスト化されたトラフィックデータとログにアクセスしてプロアクティブなトラブルシューティングを可能にします。



業務効率の向上

組織はワークフローを合理化し、プロセスを自動化することで、運用チームのアジリティと効率を向上させることができます。バックアップ、ヘルスチェック、ソフトウェアアップグレード、インベントリ、ライセンス管理といったデバイスのライフサイクル管理は、煩雑で時間のかかる作業になりがちです。A10 Control のインテリジェントな自動化機能とツールは、データセンタからクラウドまで、様々な基盤インフラに展開された多数のアプライアンスとサービスを効率的に管理することが可能です。包括的な API により、一般的な DevOps、Infrastructure as Code、オブザーバビリティツールチェーン、そして主要なパブリッククラウドおよびプライベートクラウドインフラとの容易に統合できます。

サービスとセキュリティの管理を簡素化

あらゆる A10 ソリューションを単一のプラットフォームで管理します。A10 の技術的優位性の一つは、プラットフォームやフォームファクタを問わず、すべての A10 ソリューションが共通の OS（ACOS）上で動作することです。A10 Control は、A10 Harmony Controller と aGalaxy の機能を統合することで、管理者にとって唯一の管理プラットフォームとなりました。A10 Control は、豊富なインテリジェント分析機能と組み込みの自動化ワークフローツールを活用し、IT 運用を効率化し、サービスの稼働率を向上させます。

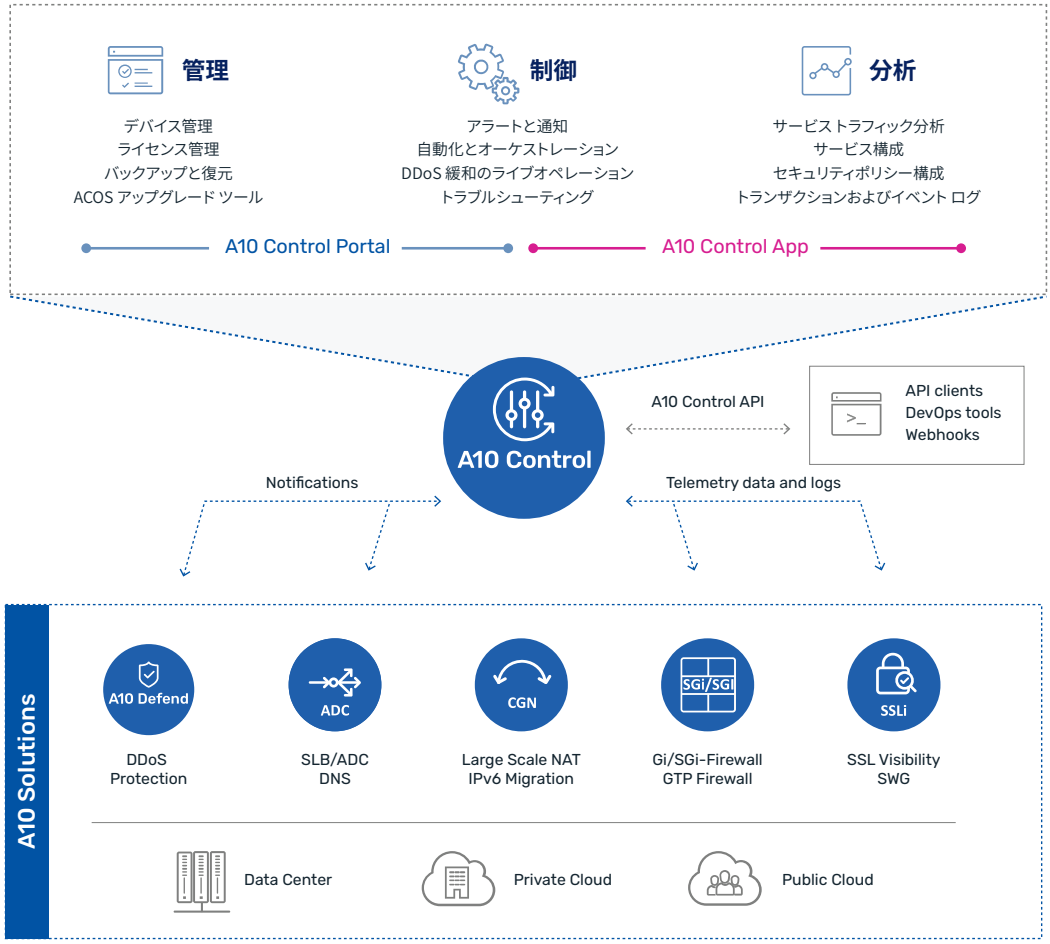


図 1：A10 Control：A10 のインフラ向けソリューションや、A10 のセキュリティソリューションを集中管理および運用するプラットフォーム

機能

集中管理

デバイスライフサイクル管理

A10ハードウェアおよび仮想アプライアンス（パブリック、プライベートクラウド、ベアメタルを含む）のデバイスライフサイクルを一元管理します。複数のA10 ThunderおよびA10 Defend DDoSアプライアンスのインベントリとライセンスを直感的に管理できます。バックアップ、インベントリレポートなどの定型タスクを自動化し、自動ソフトウェアアップグレードのスケジュール設定も可能です。

デバイス分析

地理的に異なる場所にある様々なネットワークおよびクラウド環境に展開されたA10デバイスについて、デバイスレベルでの詳細分析が可能です。デバイスヘルスモニタとダッシュボードは、システムリソースの使用状況、デバイスの位置情報、トラフィックと接続のメトリクス、トランザクションログ、イベント情報を提供します。

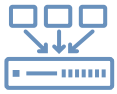
アラートとレポート

A10デバイスから収集されたメトリクスとログは、ユーザ定義のルールに基づいて相関分析・評価され、異常なイベントが発生した場合にアラートを発報します。これらのアラートは、メール通知またはWebhook経由で配信され、SlackやMicrosoft Teamsなどのコラボレーションツールを用いた自動アクションに活用されます。

サービス運用

サービスとポリシーを管理

セントラルコンソールから、様々な地理的な場所に展開されたA10 デバイスのクラスリストや IP リストなどの共有リソースを使用して構成を変更し、セキュリティ ポリシーを更新します。



マルチテナント

柔軟なマルチテナントアーキテクチャとロールベースのアクセス制御により、各アプリケーションチームとサービスオーナーは、organization-unitと呼ばれる独自のテナントワークスペースを使用して、サービスと運用を管理することができます。テナントの割り当ては、複数のA10デバイスクラスタをテナント内に配置できる柔軟性から、A10デバイスのL3V/ADPパーティションごとにテナントを割り当てるきめ細かな設定まで可能です。

API駆動型の自動化とと統合

包括的なA10 Control APIにより、Ansible、Chef、Jenkinsなどの DevOps ツール チェーンを使用した統合が可能になります。A10 Controlを介して A10デバイスの構成管理を自動化し、管理対象のA10ソリューションの監視と運用のワークフローを合理化できます。

証明書の管理と自動更新

証明書管理ユーティリティを使用すると、管理者は証明書を効果的に管理し、証明書のステータス（アクティブ、期限切れ、失効）を確認することができます。特定の証明書プロバイダとの更新プロセスを自動化することも可能です。

アーキテクチャとシステム

高信頼 コントローラプラットフォーム

A10 Control は、Kubernetes を使用したマイクロサービスアーキテクチャを備えた堅牢な RHEL 基盤上に構築されています。コントローラの可用性を最大化し、最新の業界標準のためのコンプライアンスを遵守します。コントローラは、A10 デバイスからさまざまな種類のテレメトリデータを安全な方法で収集して処理します。A10 デバイスのデータプレーンを通過するサービストラフィックを処理することはありません。このアーキテクチャにより、コントローラと A10 デバイス間の接続がダウンした場合でも、サービストラフィックが中断されることはありません。

セキュリティと保守性の向上

A10 は、Harmony Controller を含む A10 製品としてマイクロサービスアーキテクチャを使用する長年の経験と専門知識を有しています。A10 Control は、最新の RHEL ソフトウェアと次世代アーキテクチャで使用できるように設計されています。このことにより、特にセキュリティと CVE パッチに関して、システムのセキュリティと保守性が強化されています。

安定性と パフォーマンスのための新設計

A10 Control は、製品構築に使用される全てのコンポーネント、フレームワーク、テクノロジをアップグレードし、安定性とパフォーマンスを向上させました。A10 Control は、Harmony Controller とは異なるデータベースシステムを使用して、簡素化された低遅延のデータ操作と、ユーザ認証管理用の新しいテクノロジを採用しています。

高可用性

コントローラは、サイト内の単一ノードまたは複数ノードの高可用性（HA）展開において、セルフマネージドソフトウェアソリューションとしてインストールできます。

A10 Control は、地理的に分散したサイト間の高可用性アーキテクチャ（アクティブ / パッシブ）向けに設計されたディザスタリカバリもサポートしており、スタンバイシステムを事前にプロビジョニングし、プロアクティブなヘルスチェックを実行してビジネス継続性を確保します。

A10 Control をインストールするためのシステム要件と前提条件の詳細については、最新の製品ドキュメントを参照、あるいは A10 の営業担当者にお問い合わせください。

柔軟な導入オプション

A10 Control は、あらゆる規模の組織のニーズに応える柔軟な導入オプションを提供します。

- **A10 Control Standard**：最大 200 台の管理対象デバイスをサポートし、高い可用性と拡張性を求める大規模企業やサービスプロバイダ向けに設計されています。
- **A10 Control Lite**：小規模な導入に最適で、インフラとリソース要件を抑えながら、基本的な管理機能を提供します。

A10 Control Apps

ソリューションベースの包括的な分析、構成、サービス運用ツールはすべて、アプリとして A10 Control に組み込まれています。

Application Deliver Controller (ADC) App

単一または複数サイトの ADC および DNS を集中管理するためのコンフィグツールと可視性を提供します。豊富な分析機能とコンテキスト化されたログにより、アプリとトラフィックに関する優れたインサイトを獲得し、必要に応じてトラブルシューティングワークフローを簡素化できます。

SSL Insight (SSLi) App

ウィザードベースの設定、ガイド付きトラブルシューティングツール、そして SSL インサイトやセキュア Web ゲートウェイの導入に役立つ TLS/SSL 暗号化トラフィックの包括的なオブザーバビリティを提供します。

A10 Defend Orchestrator (ADO) App

以前は aGalaxy と呼んでいた機能が、ADO アプリとして利用可能になりました。DDoS Detector と Mitigator 向けの集中的な保護設定とリアルタイム監視を提供します。DDoS インシデントが発生した場合、ライブ緩和コンソールを使用してアクションをオーケストレーションし、ワークフローを効率化します。

Carrier Grade NAT (CGN) App

CGNAT の設定ツール、管理機能、そして加入者トラフィックと NAT プールの利用状況に関する詳細な分析情報を提供します。ユーザーセッションログを含む豊富なサービス分析機能により、運用効率が向上し、将来の計画策定に役立ちます。

Gi/SGi Firewall (Gi-FW) App

ファイアウォール ルールベースの分析、CGNAT 分析、アプリカテゴリベースの分類など、CFW-CGN デバイスを通過するユーザトラフィックに関する詳細な分析情報を提供します。

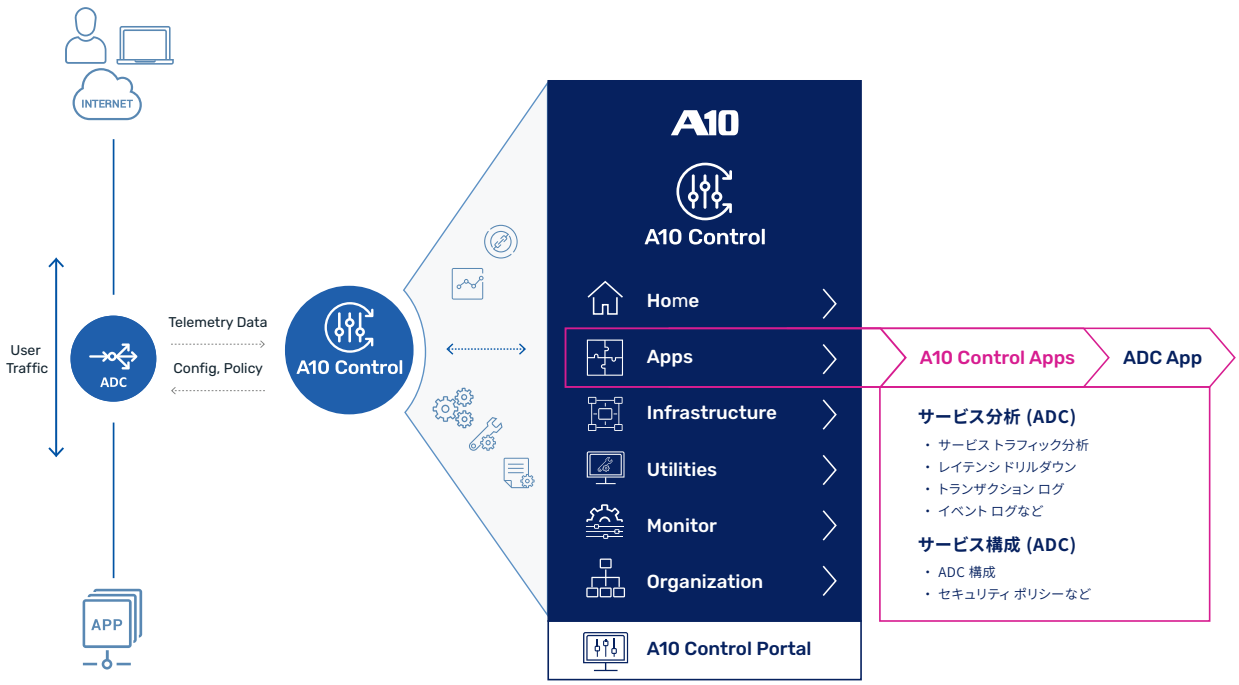


図2：A10 Control は、コントロールプレーンを介して A10 デバイスからテレメトリを収集し、サービス固有の A10 Control アプリを使用して分析と制御を提供

Use Cases

サポート対象 A10 ソリューション

アプリケーション配信

アプリケーションの高可用性、高速化、セキュリティを実現する高性能な負荷分散ソリューション。ハードウェア、ハイパーバイザベースのソフトウェア、ベアメタル、コンテナ、ハイブリッドおよびマルチクラウド環境など、あらゆるフォームファクタで A10 Thunder ADC または Thunder CFW-ADC を使用して導入

SSL Insight

包括的な TLS/SSL 復号ソリューションにより、暗号化されたトラフィックをセキュリティデバイスが分析できるようになり、統合されたセキュア Web ゲートウェイ機能によりセキュリティ体制をさらに強化できます。あらゆるフォームファクタで A10 Thunder CFW-ADC と連携して導入できます。

DNS

スケーラブルで安全な DNS 負荷分散およびキャッシュソリューションにより、DNS インフラの回復力と効率が向上します。A10 Thunder ADC または Thunder CFW-ADC を使用して、あらゆるフォームファクタと環境に導入できます。

DDoS 防御

拡張性、経済性、正確性、インテリジェンスを備えた包括的な DDoS 防御ソリューションにより、企業はサービス稼働時間をより長く確保できます。A10 Defend DDoS Detector と Mitigator により導入できます。

CGNAT と Gi/SGi-Firewall

A10 Thunder CGN を導入することで、拡張性と効率性に優れた NAT ソリューションを実現できます。サービスプロバイダや企業は、IPv4 接続を拡張しながら、IPv6 インフラへのスムーズな移行を実現できます。A10 Thunder CFW-CGN と組み合わせることで、CGNAT、Gi/SGI ファイアウォール、アプリケーション可視化といったネットワーク機能を統合し、効率的な Gi-LAN とモバイルコアセキュリティを実現します。

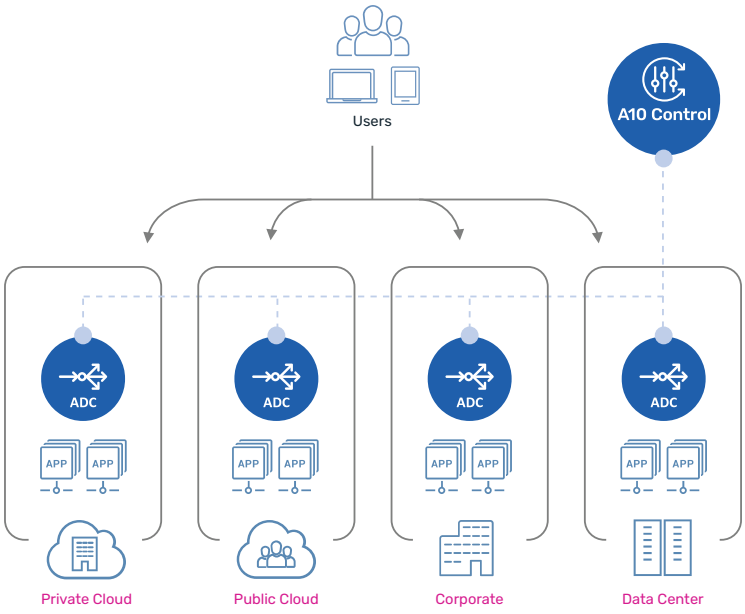


図 3：ユースケース：マルチクラウド ADC

マルチクラウド アプリケーション配信の展開

A10 Control は、ハイブリッドまたはマルチクラウド環境に展開されたアプリケーション配信サービスの管理と制御を一元化し、次の機能を提供します。

- ADC 分析
- ADC およびセキュリティポリシーの適用
- ADC デバイスと構成の管理など

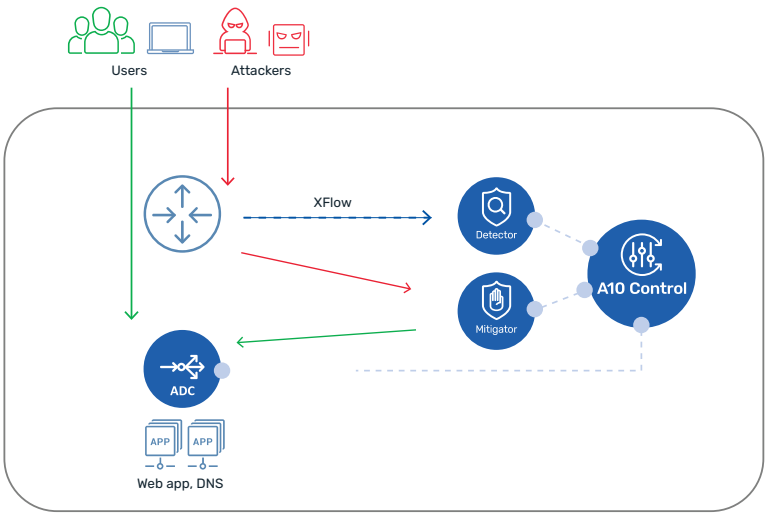


図 4：ユースケース：DDoS 防御

Web アプリと DNS への DDoS 防御

A10 Control 上で実行される A10 Defend DDoS Orchestrator（ADO）は、Mitigator および Detector と連携して、アプリケーションサービスやネットワークインフラを標的とする今日の DDoS 攻撃に対するインテリジェントな自動保護を実現します。

ADO アプリは以下を提供します：

- DDoS 防御オーケストレーションと自動化
- DDoS 緩和コンソール
- DDoS 防御ポリシー構成
- インシデント レポートなど

A10 ADC が複数のアプリケーションサービスで利用されている場合、同一の A10 Control で管理および制御することもできます。

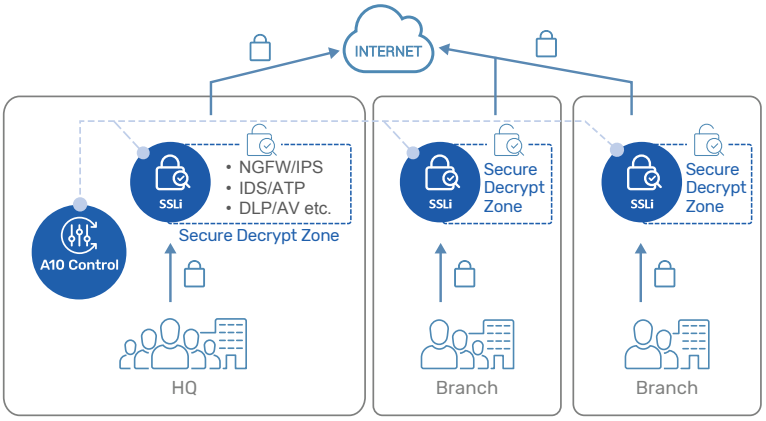


図 5：ユースケース：SSL インサイト

SSLi / セキュア Web ゲートウェイで企業の境界を保護

A10 Control は、組織の境界保護のために、複数の拠点や支社にまたがる SSL インサイト /Secure Web Gateway の導入を一元管理します。

SSLi アプリは以下の機能を提供します：

- SSLi 分析
- 一元的なセキュリティとポリシー適用
- トラブルシューティングツール
- 導入ウィザード

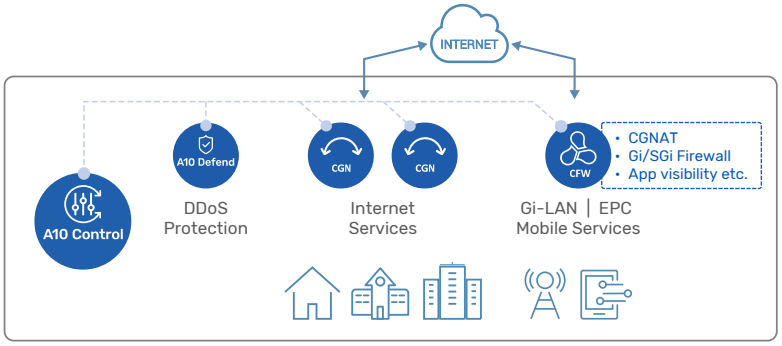


図 6：ユースケース：モバイルおよびサービスプロバイダソリューション

モバイル /SP ネットワーク向けネットワークおよびセキュリティソリューション

CGNAT および GiFW サービスは A10 Control によって一元管理可能です

- CGNAT 設定とセキュリティポリシー適用の一元管理
- デバイス管理の統合
- CGNAT およびファイアウォールの詳細な分析

さらに、DDoS 防御ソリューションも同じ A10 Control で管理可能

機能詳細

A10 Control ポータル

デバイス管理と分析	
デバイス管理ダッシュボード	完全なデバイスインベントリは、個々のデバイスとクラスタビュー（単一ノード、VRRP ペアなど）で一般的なシステムとネットワーク情報を提供し、システムリソースの使用状況とトラフィック統計の詳細な分析を提供します。
デバイス管理と分析	A10 デバイスでは、システムおよびネットワーク情報、システム リソースの使用状況とトラフィック統計の分析など、詳細なクラスターおよびデバイス レベルの分析が利用できます。
デバイスバックアップとレストア	A10 デバイスのコンフィグは定期的にバックアップされ、A10 Control に保存されます。 バックアップは、必要に応じてデバイスを復元するために使用できます。
ACOS イメージのアップグレード	アップグレード前後のチェック機能を備えたイメージアップグレードユーティリティは、登録された A10 デバイスに対して、手動およびスケジュール方式の両方で、直感的で信頼性の高い ACOS イメージのアップグレードプロセスを提供します。すべてのアップグレード操作ログと記録は、履歴ビューで利用可能です。
モニタリングとアラート	
サービスレベルヘルスモニタとアラート	サービスのトラフィックと状態は、様座なサービス レベルのメトリックと閾値を使用して、カスタムトリガ ルールで監視できます。アラートは電子メールと Webhook 経由で送信できるため、既存の監視システムとの統合が容易になります。
デバイスレベルヘルスモニタとアラート	インフラストラクチャ / デバイスのリソース使用量、デバイスレベルのトラフィックベースの閾値、システム ログに基づいて、詳細なデバイスレベルのトリガルールを設定できます。アラートは電子メールと Webhook 経由で送信できるため、既存の監視システムとの統合が容易になります。
レポーティング	包括的なインベントリレポートとサービスごとの運用レポートは、オンデマンドで生成することも、スケジュールを設定して自動配信することもできます。レポートは PDF 形式でのダウンロード、あるいは、メールで配信されます。
イベントログ、監査ログ	イベント ビューアは、登録されているすべての A10 デバイスからの統合されたシステムおよびサービスイベントログを提供します。監査ビューアは、A10 コントローラからの監査ログ、および登録されているすべての Thunder およびライセンス管理アクティビティログへのアクセスを提供します。詳細なログ フィルタが利用可能で、ログは CVS 形式でダウンロードできます。
管理およびユーティリティ	
マルチテナンシ管理	マルチテナント機能は、アプリケーション チームとサービス所有者に対して、きめ細かなロールベースのアクセスを提供します。各テナント（組織単位）は、A10 デバイスのパーティション（ADP/L3V）レベルでマッピングできます。
CLI コマンド	単一またはバッチの CLI コマンドを複数のデバイス パーティションで同時にリモート実行できます。
共有設定リソースツール	クラス リスト、許可リスト・拒否リスト、SLB テンプレート、セキュリティテンプレート、TLS/SSL 証明書などの共通の構成リソース / テンプレートは、共有リソースとして作成でき、サービスタイプに関係なく、登録されているすべての A10 デバイスで使用できます。
証明書管理	ADC および SSLi サービスの TLS/SSL 証明書と鍵は A10 Control で管理でき、組織管理者は証明書の保存、プロビジョニング、更新、ステータス（有効、期限切れ、失効）の監視を行うことができます。Venafi などの証明書プロバイダとの連携により、自動更新を含む証明書ライフサイクル管理の完全自動化が可能になります。
ライセンス管理	A10 Control はエンタープライズ ライセンスマネージャとして機能し、登録された A10 デバイスの FlexPool 容量ライセンスを管理および制御できます。
ユーザ管理	ロールベースのアクセス制御により、柔軟なユーザー管理が可能になります。たとえば、アクセス領域は組織、テナント、デバイス、または特定のサービス / パーティションで設定でき、権限レベルは管理者、オペレータ、または特定の操作を含むカスタムルールとすることができます。
認証管理	ローカル認証に加えて、外部認証とシングル サインオン（SSO）用に、Azure、Okta、LDAP などの ID プロバイダー（IdP）を選択できます。

A10 Control Apps

アプリケーション配信	
ADC App ホーム	• テナント（org-unit）下の仮想サーバ（VIP）のステータスとデプロイメントマップを統合 • 主要な仮想サーバ • イベントとアラートを表示するダッシュボード
分析	• Orgniazation Unit の各仮想サービスに対する ADC サービス分析 • トラフィック情報、エラー率、レイテンシなどのリアルタイム ADC サービスレベル KPI • ユーザインサイト（位置情報、ブラウザ）、Top-K、リクエストインサイト、時系列レイテンシなどを含む、ユーザトラフィックベースの分析 • 一般的なプロトコル（HTTP/S、SSL、HTTP2）に対する ADC サービス分析 • リソース使用状況に関するインサイトを得るための ADC クラスタ分析 • 詳細なアプリサービス状況と傾向を得るためのアプリケーションサービス分析 • サーバの健全性とステータスに関するアプリケーションサーバ分析 • End-to-End レイテンシとリクエストレスポンスサイクルに関する、レイテンシ情報のドリルダウンと分析
トランザクションログのビューア	• クライアント、パケット、プロトコル、リクエストヘッダ、レイテンシ情報などを含む詳細なセッションログ（HTTP/TCP） • ADC システムログからのイベントビュー • カスタム監視およびアラートルールに基づくアラートビューア
コンフィグツール	• サービスオブジェクト（VIP、サービスグループ、サーバ）および共有オブジェクト（テンプレート、aFleX、ヘルスモニタなど）の ADC 一元設定 • 自動最適化（ブラウンフィールド デプロイメント）とコンフィグの同期

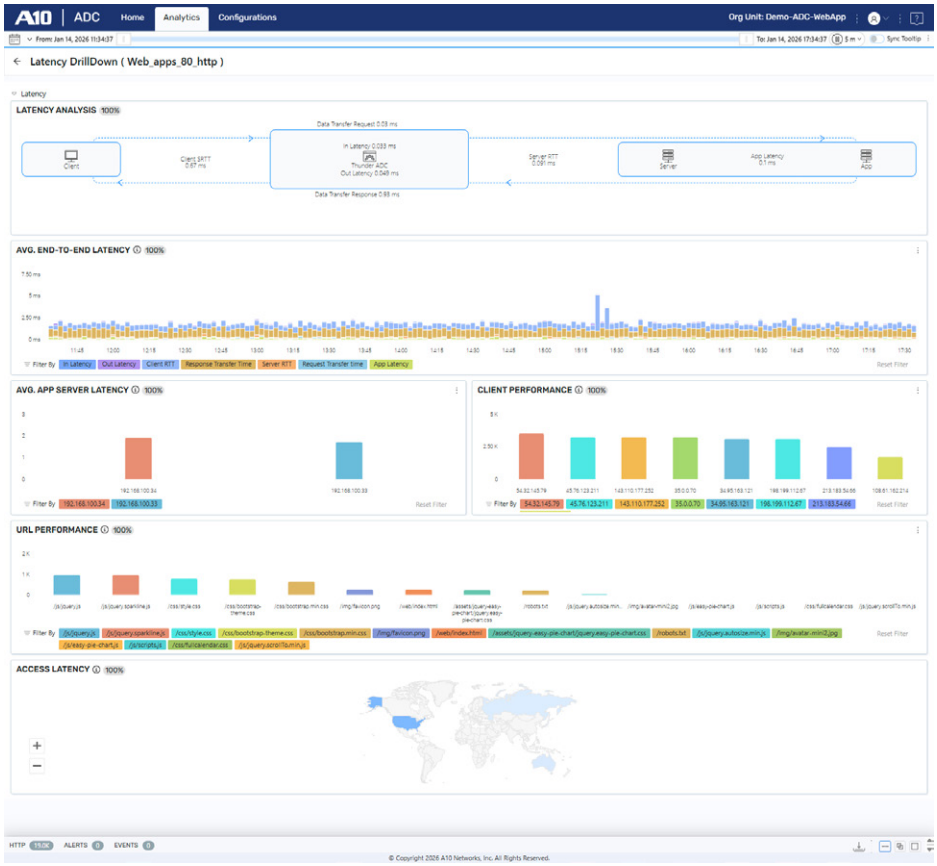


図 7：レイテンシ詳細情報のための ADC 分析

Defend Orchestrator	
保護ワークフロー オーケストレーション	• 検知から緩和、レポートまで、シームレスで自動化された DDoS 防御を実現 • 攻撃終了後の DDoS インシデントレポートを自動生成
オーケストレータ ダッシュボード	• DDoS インシデントとアクティビティの概要 • DDoS 防御のステータスとアクティビティの概要 • サービス保護の健全性、緩和のための集約トラフィックを表示するダッシュボード • 攻撃の種類、攻撃元、攻撃対象 / 攻撃先などに関する攻撃傾向の分析情報（Top-K）
DDoS インシデントコンソール	• DDoS 防御の監視とライブオペレーションのための緩和コンソール（サービスポートレベルまでドリルダウン可能） • 対策に基づいたパケットレート、ボリューム、トラフィック指標、パケットドロップチャートを含むライブトラフィックチャート • Top-k（送信元と宛先）、インシデントおよびイベントログ、アラートビューア、グローバルおよびサービスポートレベルの緩和統計情報 • カスタム緩和ポリシーへの手動介入
モニタリング	• 監視対象ゾーン / オブジェクトのリアルタイムトラフィックチャートと統計情報 • 攻撃対象と送信元（Top-K）の詳細な IP アドレスの可視性と分析情報 • リモートトリガー型パケットキャプチャツール（オンデマンドまたは自動） • DDoS インシデント、保護対象ゾーン、デバイスインベントリなどのオンデマンドおよびスケジュールレポート
コンフィグツール	• DDoS 防御プロファイルと運用ポリシーの一元設定 • 再利用可能な定義済みテンプレート、防御プロファイル、運用ポリシーによる直感的な設定 • BGP ベースのトラフィックリダイレクト（リアクティブ展開）、RTBH、Flowspec をサポート • DDoS 防御固有のデバイス管理（Mitigator と Detector の設定）

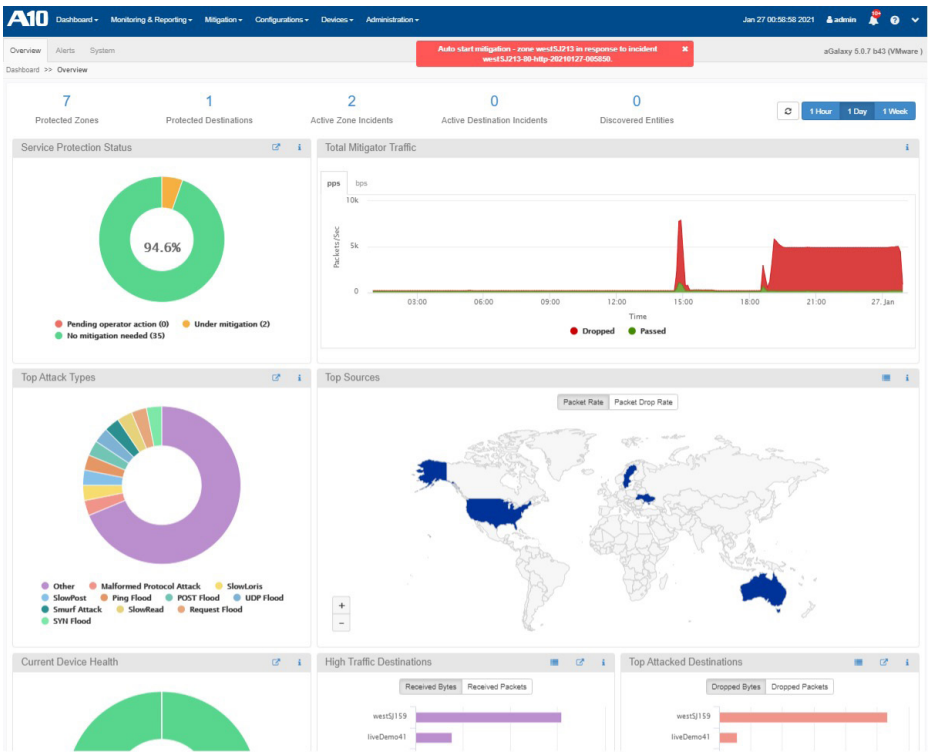


図 8：A10 Defend Orchestrator ダッシュボード：リアルタイムの攻撃統計、DDoS インシデントの概要

SSL Insight	
デプロイメント ウィザード	• SSLi およびセキュア Web ゲートウェイ向けの、ガイド付きまたはガイドなしのワークフローオプションを備えた直感的な構成ウィザード • 推奨セキュリティポリシーに基づき、あらゆる導入オプション（単一アプライアンスまたはデュアルアプライアンス、高可用性、透過的 / 明示的プロキシ、サービスチェイニング、L2/L3/ 仮想ワイヤなど）において、グリーンフィールドとブラウンフィールドの両方の導入をサポート • 新規サイトの導入、特定のサイトまたはデバイスのポリシーまたは構成変更のために、グローバル（サイトグループ）、サイトレベル、またはデバイスレベルの構成に迅速にアクセス • コンフィグ差分を使用した構成変更のレビューとロールバックをサポート
コンフィグの集中管理	• ACL、ポリシーテンプレート、SSL プロファイル、証明書管理、URL フィルタリング、ICAP、AAM、SAML、G-Suites、Office 365 など、さまざまな SSLi 設定を共有オブジェクトとして保存・管理 • タグマネージャーは、物理インターフェースと論理インターフェース、および接続属性を定義・管理
SSLi 分析	• サイトグループを対象とする SSL インサイト分析。接続数とレート、復号率、エラー率、ポリシー違反率などのリアルタイム KPI を提供 • TLS トラフィックの観測と分析：復号済みトラフィックの Top-K（送信元 / 宛先）、TLS と証明書の詳細、キャッシュされた証明書など • URL カテゴリ、アプリケーションカテゴリ、脅威インテリジェンスに基づくセキュリティ関連分析。接続数とトラフィック量の観点からトラフィックの傾向とパターンを提供し、各エリアのリスクの高いアクセスや不審なアクセスを可視化 • ウォッチリスト機能により、管理者は URL とアプリケーションのカスタムカテゴリリストを作成し、リアルタイムのトラフィック監視と分析が可能。
トラブルシューティングツール	• SSL Insight によるシステム、リソース、エンドツーエンド通信の検証のための、ガイド付きのステップバイステップテスト • 同一デバイスの異なる KPI を比較したり、異なるデバイスの同じ KPI を比較したりするためのメトリクス相関
トランザクションログビューア	• SSLi トランザクション、エラー、ファイアウォールイベントログの拡張表示および検索機能を提供し、トラブルシューティングと分析を支援 • 豊富な検索フィルタ（IP、TLS、URL/ アプリカテゴリ、サイズ、ステータスなど）による詳細なセッションドリルダウンと、Webroot による脅威調査機能（Threat Investigator ルックアップ）を搭載

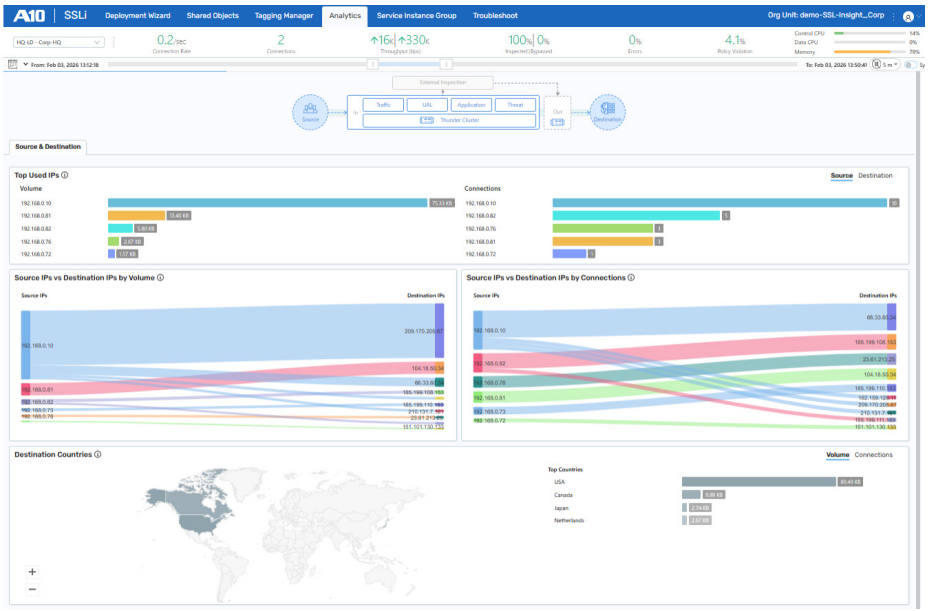


図 9：送信元と宛先の IP 相関分析用の SSLi アプリ

Carrier-grade NAT	
CGN App ホーム	• テナント（組織単位）下の CGNAT 導入情報を統合的に表示 • LSN/Fixed-NAT/1:1 NAT/DS-Lite/NAT64/NAT46 ステートレステクノロジーの CGNAT サービスステータスの内訳 • イベントとアラートのダッシュボード
分析	• 組織単位（OU）下の各 CGN テクノロジ（LSN/Fixed-NAT/1:1 NAT/DS-Lite/NAT64/NAT46 ステートレス）の CGNAT サービス分析 • トラフィックおよびセッション情報、NAT プールの使用状況などを含む、CGNAT サービスレベルのリアルタイム KPI • トラフィック、セッション、ポートマッピング、ドロップされたトラフィックとエラー、リンクプローブ、CGN システムに関する CGNAT サービスの分析情報 • 詳細な CGNAT テクノロジーベースの分析情報（セッション、Top-K、ユーザクォータなどのトラフィック分析情報、ポートマッピング、プールの使用状況と不正行為などの CGN サービスの分析情報、アプリケーションカテゴリの分析情報） • 統合 DDoS 防御、拒否リストに登録された IP などに関するセキュリティ分析
トランザクションログビューア	• CGN セッションとトランザクションの詳細なビューを提供。IP: ポートマッピング、加入者情報（MSISDN、IMSI など）、セッションステータス、カスタムフィールドなどが含まれる • 豊富な検索フィルタと加入者トレース機能を備えた詳細なセッションドリルダウン機能 • CGN エラーログ、システムイベント、アラートを表示するイベントビューア
コンフィグツール	• 集中管理された CGNAT 構成 (LSN/NAT64/DNS64)、共有オブジェクト (NAT プール、クラスリスト、EIM/EIF、ALG)、統合された DDoS 保護、ログ テンプレートなど

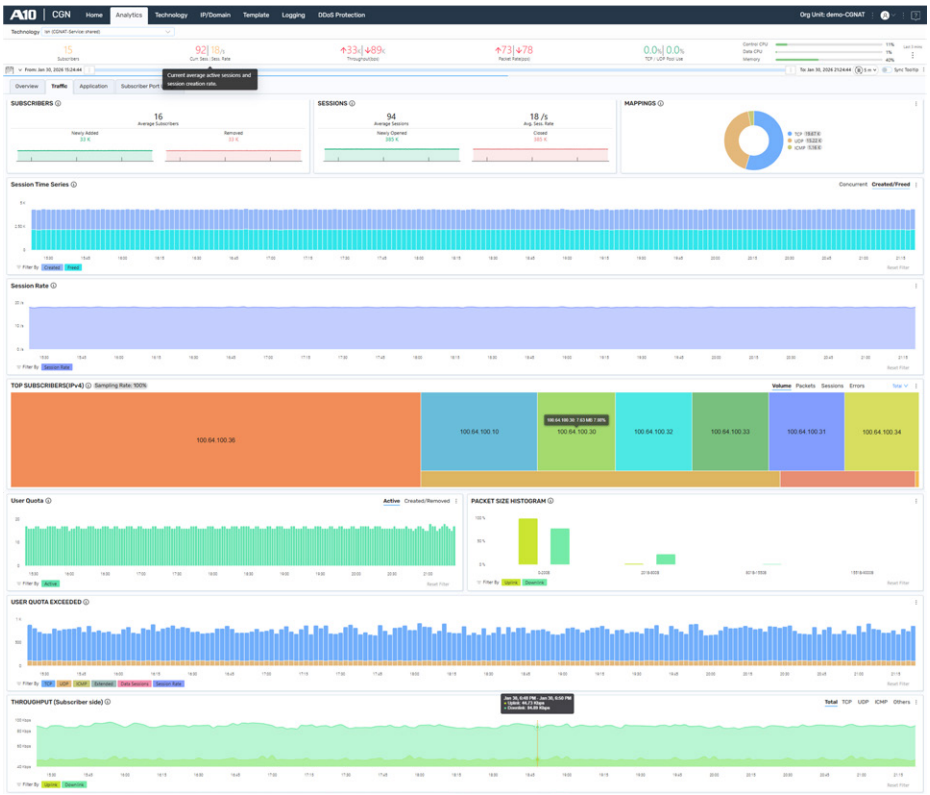


図 10：: LSN サービストラフィック分析のための CGN app

Gi/SGI Firewall	
Gi Firewall App ホーム	• テナント（org-unit）配下の Gi/SGi ファイアウォールのデプロイメント情報を統合的に表示 • イベントとアラートのダッシュボード
分析	• Organiaztion Unit に属する各ファイアウォールポリシールールセットの Gi ファイアウォールサービス分析 • トラフィックとセッション情報、ルールヒットカウンターなどを含む、リアルタイムの GiFW サービスレベル KPI • 詳細な GiFW サービス分析 - ルールパフォーマンス、古いルールのリスト、Top-K の加入者、CGNAT マッピングと使用率、アプリケーションカテゴリなどのトラフィック分析を含む、ファイアウォールルールベースの分析情報
トランザクションログビューア	• ファイアウォールセッションの詳細なビューを提供。ファイアウォールゾーンとインターフェース、関連ルールと加入者情報、IP とポートのマッピング、NAT されたトラフィックのトレースされたトランザクションなどが含まれる • 豊富な検索フィルターを備えた詳細なセッションドリルダウン • GiFW/CFW システムログからのイベントビューア • カスタム監視およびアラートルールに基づくアラートビューア

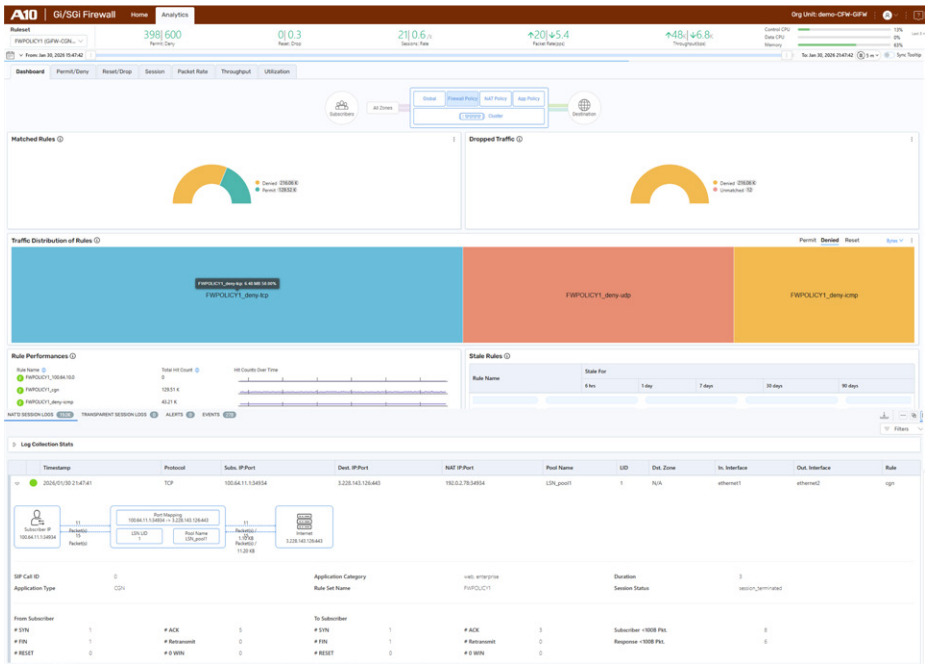


図 11：詳細なセッションビューアを備えたファイアウォール ポリシー分析用の Gi/SGi ファイアウォール アプリ

A10 Networks / A10 ネットワークス株式会社について

A10 Networks は、オンプレミス、ハイブリッドクラウド、エッジクラウド環境における、セキュリティ、インフラストラクチャの課題を解決するソリューションを提供しています。大手グローバル企業や通信、クラウド、Web サービス事業者まで 7000 社以上のお客様に導入いただいており、ビジネスに不可欠なアプリケーションやネットワークの安全性、可用性、効率性を高めています。A10 ネットワークスは 2004 年に設立されました。米国カリフォルニア州サンノゼに本社を置き、世界中のお客様にサービスを提供しています。

A10 ネットワークス株式会社は A10 Networks の日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。

詳しくはホームページをご覧ください。
- URL：https://www.a10networks.co.jp/
- X（旧 Twitter）：https://twitter.com/a10networksjp
- Facebook：https://www.facebook.com/A10networksjapan

Learn More
About A10 Networks

お問い合わせ
A10networks.co.jp/contact

A10ネットワークス株式会社
www.a10networks.co.jp

Part Number: A10-DS-15139-JA-03 MAR 2026