

A10

A10 ネットワークス

総合カタログ



A10の4つの重点領域



企業やサービス事業者のマルチクラウド変革、そして5G対応 —「安全」で「止まらない」ビジネスクリティカルな アプリケーション配信を支えるのがA10です

A10 ネットワークスは2004年の創立以来、セキュアアプリケーションサービスのテクノロジーリーダーとして製品の開発、販売、サポートを世界各国で展開してきました。

常に最先端の技術を優れたコストパフォーマンスで提供できるよう努力を続けるA10 ネットワークスは、ネットワークを介してビジネスを推進する多くの皆様に認められています。

日本国内の市場に適したサポートを提供できるよう、2009年3月には日本法人を設立しました。日本に根差した経営を行ない、日本市場の特徴を理解し、その要望にお応えしていく — それがA10 ネットワークスの使命です。

A10 が提供するソリューション



DDoS 攻撃対策

- DDoS 緩和
- DDoS 検知
- 脅威インテリジェンス

詳しくは ▶ P4



トラフィック制御

- 帯域制御
- 公平制御
- プロキシ
- SSL/TLS 可視化 (SSLインサイト)

詳しくは ▶ P8



IPv6 移行、IPv4 枯渇対策

- キャリアグレード NAT (CGN)
- IPv6 移行

詳しくは ▶ P10

A10



インフラ/サービスの安定稼働

- アプリケーション配信コントローラー (ADC)
- 各種 DNS ソリューション

詳しくは ▶ P6



クラウド活用・DX 推進

- クラウドアクセスプロキシ
- データセンターブレイクアウト
- クラウドアクセスコントローラー

詳しくは ▶ P12

様々な提供形態



ハードウェア アプライアンス

ハイパフォーマンス
高いポート密度



仮想インスタンス

高いモビリティ



ベアメタル

ハードウェアの
共通化



コンテナ

クラウドネイティブ



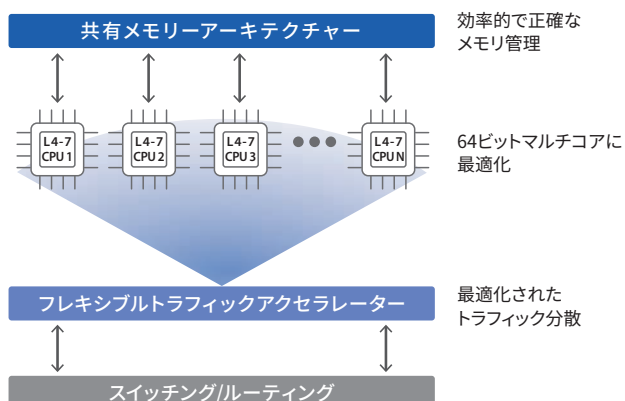
クラウド インスタンス

時間・月額サブスク
BYOL



Thunder シリーズのパフォーマンスを支える独自 OS、ACOS (Advanced Core Operating System)

ACOS プラットフォーム



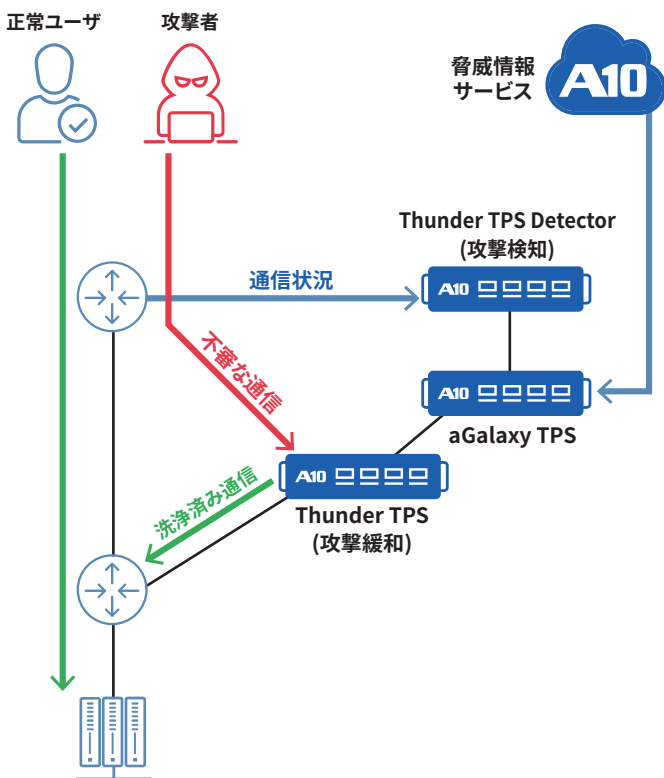
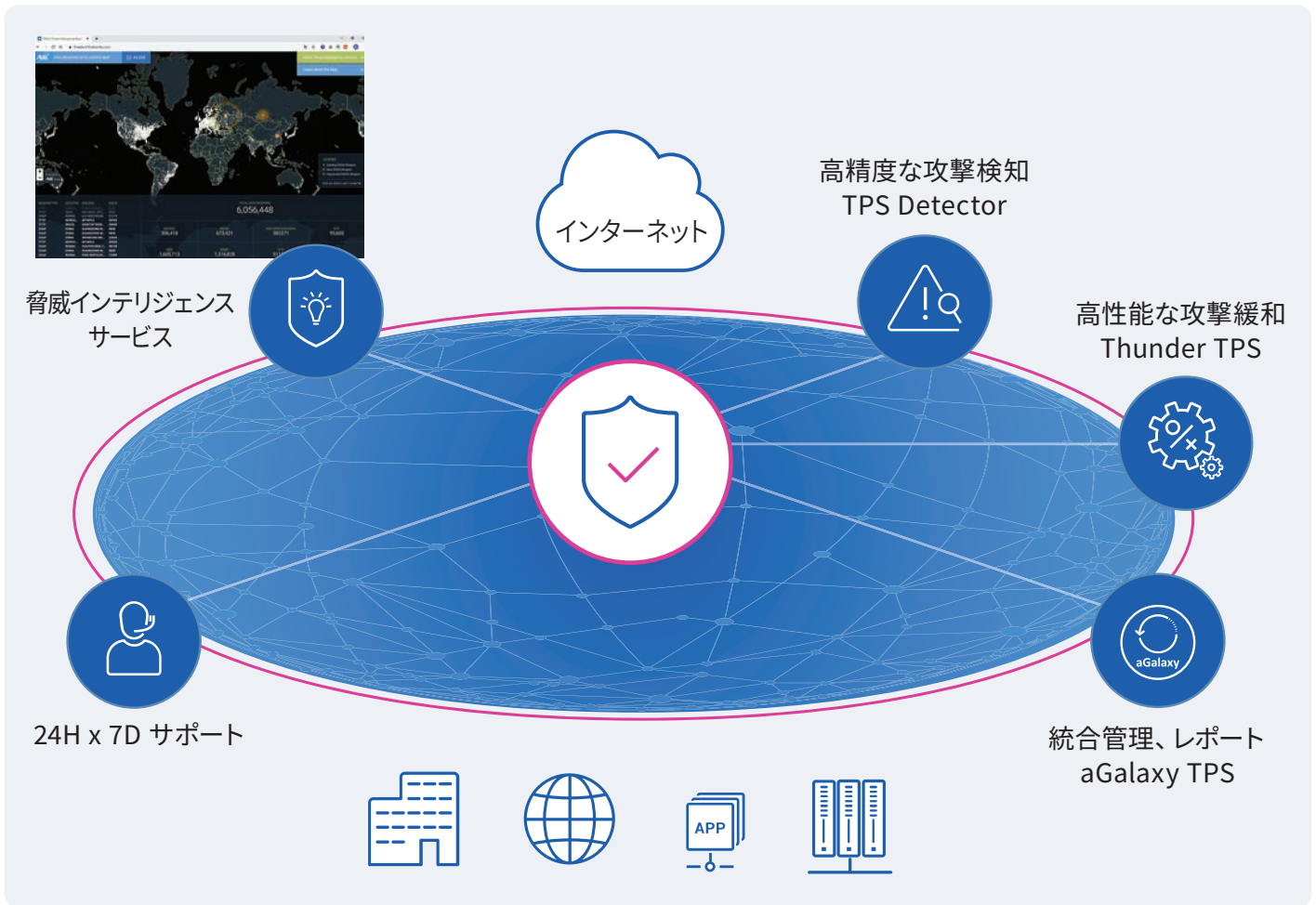
Thunder シリーズは、A10 ネットワークス独自の OS ACOS と 64ビット対応の専用ハードウェアにより業界最高峰のパフォーマンスを実現します。

ACOS は、マルチコア・マルチ CPU 構成で、各 CPU が完全に独立した並列処理を実現し、マルチコア CPU 特有の問題であるデータコピーやロッキングをなくすことにより、CPU のパフォーマンスを最大限に発揮させることを可能にしています。

ACOS プラットフォームの特徴

- アプリケーションの高速化
- 高度なセキュリティ機能
- アプリケーションサービスの可用性向上

DDoS 攻撃対策 Threat Protection System (TPS)



Thunder TPSシリーズ構成イメージ

A10のThunder TPSは、大手サービスプロバイダーやオンラインゲーム会社で多くの実績を持つDDoS攻撃対策ソリューションです。AI/機械学習を活用し、DDoS攻撃を検知・緩和することで、ネットワークを大規模なDDoS攻撃から保護します。

Thunder TPS:

DDoS攻撃を緩和して、サービス停止を阻止するアプライアンス製品です。専用ハードウェアと仮想アプライアンスにより、1Gbps～380Gbpsの防御パフォーマンスを実現します。

Thunder TPS Detector:

フローベースでDDoS攻撃を検知するアプライアンス製品です。NetFlow, sFlow, IPFIXなどのフロー情報を基に攻撃を検知します。

aGalaxy TPS:

Thunder TPSによるDDoS攻撃の検知・緩和を一元管理するアプライアンス製品です。TPSとDetectorとの連携管理や、攻撃状況の把握、レポートなどの機能を提供します。

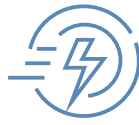
脅威情報サービス:

潜在的な攻撃元や脅威に関する情報を収集、分析、評価した結果得られたIPアドレス情報を提供するサービスです。重要な情報資産を守るために必要な事前の対処を支援します。

A10 のメリット



攻撃による被害や対応に
かかるコストを削減



正常通信を
可能な限り保護



攻撃状況を
リアルタイムで可視化

主な特長



AI/機械学習による自動防御

ボリウム攻撃を受けた際に、攻撃と思われる部分を AI が学習し、防御フィルタを自動生成することで、正常な通信のトラフィックへの影響を最小限に



先回り防御

将来 DDoS 攻撃に利用される可能性の高いデバイスの IP 情報を脅威インテリジェンス情報として利用することにより、攻撃が発生する前に防御設定が可能



あらゆる DDoS 攻撃に対応

ボリウム型攻撃だけでなく、アプリケーション層やネットワーク層などの高度な攻撃や暗号化されたトラフィックによる攻撃からもネットワークを保護



柔軟な構成

ネットワークの構成に合わせて、インライン、アウトオブパス構成など、自由にデプロイ可能で、他社の攻撃検知製品（フローコレクタなど）との連携実績も豊富



高いパフォーマンス

60 種類のよくある攻撃パターンを専用ハードウェアで検知・緩和し、マルチコアに最適化された独自 OS と組み合わせて、最大 5 億 pps の防御パフォーマンスを実現







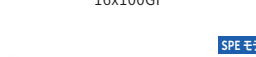







様々な提供形態

専用の物理アプライアンスから、仮想アプライアンス、Azure などのパブリッククラウド上での使用など、容量や使用場所によって適切なモデルを選択

対応製品

2023 年 3 月現在

DDoS 攻撃緩和装置（モード変更で検知装置へ変更可能）			仮想アプライアンス
～ 10Gbps	100 ～ 220Gbps	300Gbps～	
 <p>Thunder 3350-E 10Gbps 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF</p>	 <p>Thunder 7445 220Gbps 48x1/10GF, 4x100GF</p>	 <p>Thunder 7655S 380Gbps 16x100GF</p>	 <p>aGalaxy-VA 仮想アプライアンス</p>
 <p>Thunder 1040 5Gbps 5x1GC, 4x10GF ハードウェアバイパスオプション</p>	 <p>Thunder 5845 100Gbps 48x1/10GF, 4x100GF</p>	 <p>Thunder 14045 300Gbps 4x40GF, 4x100GFs</p>	 <p>サブスクリバードポータル (VM)</p>
 <p>vThunder TPS 仮想アプライアンス 1～5Gbps</p>	 <p>vThunder TPS 仮想アプライアンス 10 - 100Gbps</p>		
 <p>Thunder TPS for Azure 5Gbps</p>			
			 <p>vThunder TPS Detector 仮想アプライアンス</p>

*SPE モデル：セキュリティポリシーの適用を高速化するハードウェアである SPE(Security and Policy Engine) を搭載したモデル

最新情報または詳細は、
右記の web ページをご覧ください。

詳細情報

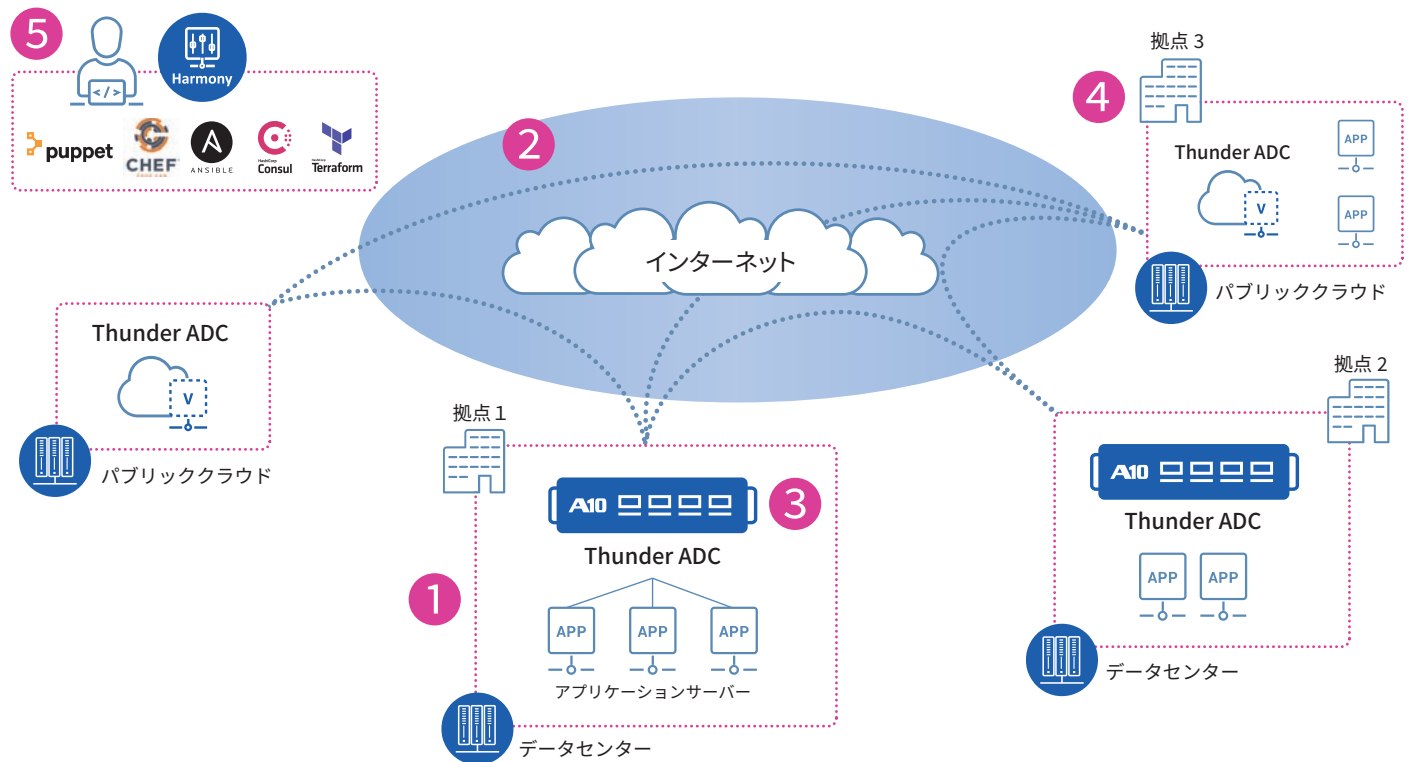


データシート



インフラ・サービスの安定稼働

ビジネスに不可欠なアプリケーションをセキュアに提供



1 サーバー負荷分散

- サービスの可用性向上
- 迅速な応答のための負荷分散

2 Global Server Load Balancing(GSLB)

- グローバル サイト全体での高可用性
- コンテンツのローカリゼーション、規制遵守

3 アプリケーションセキュリティ

- Web Application Firewall (WAF)
- DNS Application Firewall
- アプリケーションアクセス管理
- 統合 DDoS 防御

リダンダンシ/ クラスタリング

- VRRP-a
- aVCS
- Scale-out

4 柔軟な提供形態

- ハードウェアアプライアンス
- ソフトウェア (VM, パブリッククラウド, Bare Metal, コンテナ)
- FlexPool ライセンス

5 一元管理と分析

- ポリシーの集中的な実施
- リアルタイムのアプリ解析と可視化
- オーケストレーションと自動化

A10のメリット



アプリケーションの可用性を向上

- 複数データセンタ、マルチクラウド環境下での高速・高信頼アプリケーション配信を実現
- ネットワーク遅延やダウンタイムを最小化し、ユーザエクスペリエンスを向上



包括的なアプリケーションセキュリティ

- 高度な SSL/TLS オフロード
- シングル サインオン (SSO)
- DDoS 攻撃からの防御
- Web アプリケーション ファイアウォール (WAF)



アプリケーションの可視性

- A10の Harmony Controllerと連携することにより、アプリケーション毎に提供状況を可視化
- オンプレミス、パブリッククラウドも含めたマルチクラウド環境でサービスの管理・制御も可能

主な機能



高度なサーバー負荷分散

- 俊敏なトラフィック制御、カスタマイズ可能なサービスヘルスチェック、aFlex スクリプトを活用したフルプロキシ L4-L7 負荷分散により、アプリケーションの可用性を確保
- ラックスペースの効率的利用を実現



マルチテナント対応のソフトウェア

- カスタマイズ可能なポリシー、ロールベースのアクセス制御 (RBAC) により、強固に分離された最高密度のマルチテナントソリューションをサポート



任意のクラウドへ展開

- ハードウェア、仮想、クラウド、ベアメタル、およびコンテナのフォームファクターで展開
- FlexPool による、マルチクラウド全体でのライセンスポータビリティ



アプリケーションパフォーマンスの高速化

- キャッシュ、TCP 最適化によるコンテンツ転送の高速化
- 最新の ECC 暗号に対応した TLS/SSL オフロード



Web と DNS の保護

- シングルサインオン、CAPTCHA、Web および DNS ファイアウォール、DDoS 保護などの統合セキュリティ



アプリケーションごとの分析

- A10 Harmony Controller と統合し、ユーザーエクスペリエンス、トラフィックプロファイル、ヘルスチェックを可視化し、パフォーマンスを監視



Rest ベースのプログラマビリティ

- 100% の API カバレッジ
- 多くの DevOps、自動化管理ツールへネイティブな統合が可能



グローバルサーバーロードバランシング (GSLB)

- グローバルに負荷分散を拡張。高速なサーバーレスポンスを可能に
- マルチクラウド環境でのビジネス継続性を実現



DevOps ツール

- Terraform、Ansible などの自動化ツールを使用した CI/CD パイプラインへの統合



自動サービス検出

- Thunder Kubernetes Connector (TKC)、または HashiCorp NIA with Consul などのサードパーティツールを使用し、Kubernetes 環境での自動サービス検出



分析とイベント監視

- Prometheus/Grafana および内蔵の Prometheus エクスポートによるネットワークの可視化、イベント監視、アラートを一元化

対応製品

2023年3月現在

仮想アプライアンス	~ 20Gbps	~ 100Gbps	~ 200Gbps	200Gbps ~
 vThunder ADC for Cloud Microsoft Azure, AWS: 最大 10 Gbps まで Oracle Cloud: 最大 24Gbps まで	 Thunder 1040 20 Gbps 5x1GC, 4x1/10GF	 Thunder 4440 78 Gbps 24x1/10GF, 4x40GF	 Thunder 6440 150Gbps 48x1/10GF, 4x40GF	 Thunder 7655S <small>SPE モデル</small> 370 Gbps 16x100GF
 vThunder ADC 仮想アプライアンス 最大 100 Gbps まで	 Thunder 940 10 Gbps 5x1GC, 4x1/10GF	 Thunder 3350S 50Gbps 6x1GC, 2x1GF, 8x1/10GF, 4x10GF	 Thunder 5840 115 Gbps 24x1/10GF, 4x40GF	 Thunder 7440 220 Gbps 48x1/10GF, 4x40GF
 Thunder ADC for Container (Docker) 最大 100 Gbps まで		 Thunder 3350 40Gbps 6x1GC, 2x1GF, 4x25GF, 4x40GF, 4x10GF	 Thunder 5840-11 115 Gbps 24x1/10GF, 4x100GF	 Thunder 7440-11 220 Gbps 48x1/10GF, 4x100GF
ベアメタル		 Thunder 3350 -E 30Gbps 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF	 Thunder 5440 100 Gbps 24x1/10GF, 4x40GF	

*SPE モデル：セキュリティポリシーの適用を高速化するハードウェアである SPE(Security and Policy Engine) を搭載したモデル

最新情報または詳細は、
右記の web ページをご覧ください。

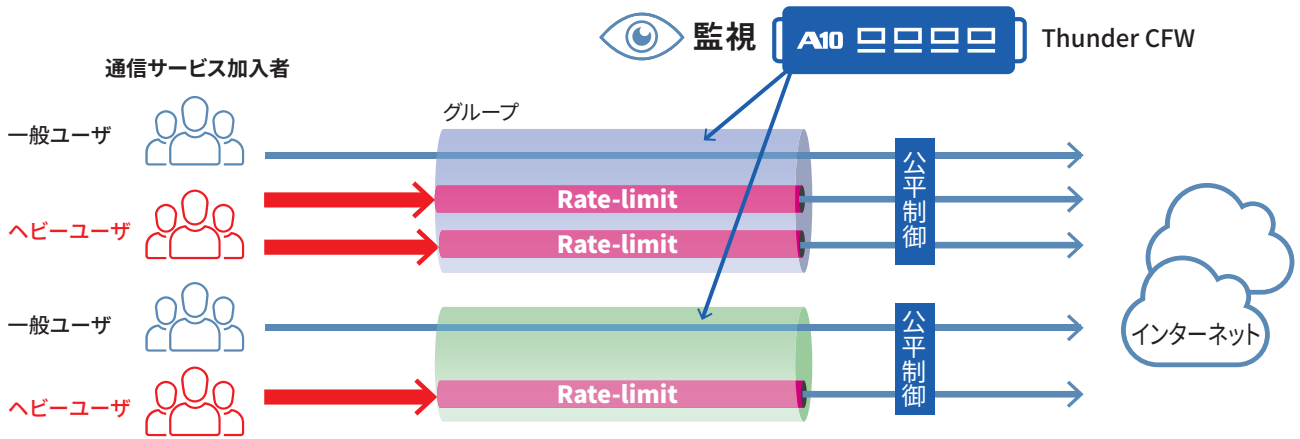
ソリューション詳細



データシート



トラフィック制御（帯域制御）

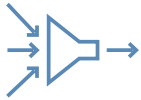


A10の帯域制御ソリューションを用いることで、ヘビーユーザーの過剰な帯域の利用を抑制することができ、公平かつ有効な通信帯域の利用を実現できます。送信元・送信先IPアドレス等や、DPIを利用して識別したアプリケーション種別を指定し、上り下りの通信帯域やコネクション数などを制限できます。

帯域制御機能はファイアウォール機能の一部として搭載されており、公平制御以外にもCGNAT機能・ADC機能と併せて利用することも可能です。

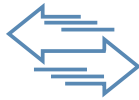
大容量の専用ハードウェア製品に加えて、ベアメタルソフトウェアや、仮想ソフトウェア、コンテナでも本機能を利用できます。

A10のメリット



階層的な公平制御

トラフィックピーク時にヘビーユーザーの帯域を制限することで公平な帯域の利用を実現し、通信事業者が通信サービス加入者の満足度を高めることが可能。グループに分けたサービス加入者に階層的に制御をかけることも可能



ネットワーク資源の有効活用

通信帯域やセッション数、秒間パケット数などを上り・下り合計で制御し、ネットワーク資源を有効活用可能に



アプリケーション識別と制御

Deep Packet Inspectionにより通信のアプリケーションを識別し、利用アプリケーションを可視化し利用されているアプリケーションの状況を確認したり、アプリケーション毎の帯域制御や通信制御が実現可能に



CGNAT機能等との併用

キャリアグレードNATやファイアウォール、負荷分散・回線分散やフォワードプロキシ機能など、A10 Thunderの持つ機能をトラフィック制御と併せて同一筐体で利用可能

対応製品

2023年3月現在

仮想アプライアンス	～ 100 Gbps*		～ 200 Gbps*	200Gbps* ～
 vThunder CFW for Cloud vThunder 仮想アプライアンス Thunder for Container (Docker) ベアメタル Thunder for Bare Metal	 Thunder 4440S 24x1/10GF, 4x40GF	 Thunder 5840 24x1/10GF, 4x40GF Thunder 5840-11 24x1/10GF, 4x100GF	 Thunder 7440 220 Gbps 48x1/10GF, 4x40GF Thunder 7440-11 48x1/10GF, 4x100GF	 Thunder 7650 16x100GF
	 Thunder 3350S 6x1GC, 2x1GF, 8x1/10GF, 4x10GF	 Thunder 5440 24x1/10GF, 4x40GF	 Thunder 6440S 48x1/10GF, 4x40GF	

* 公平制御が必要となるスループットの目安

最新情報または詳細は、右記のwebページをご覧ください。

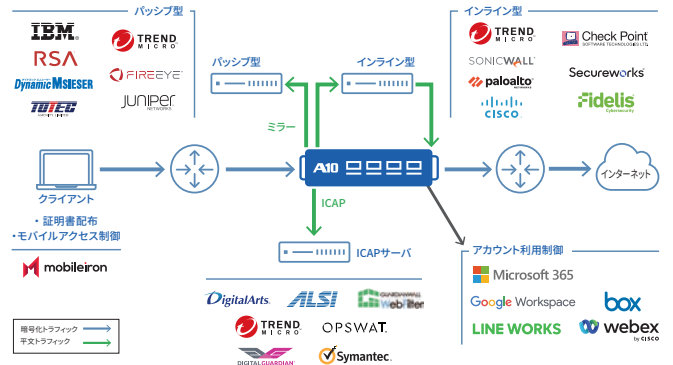
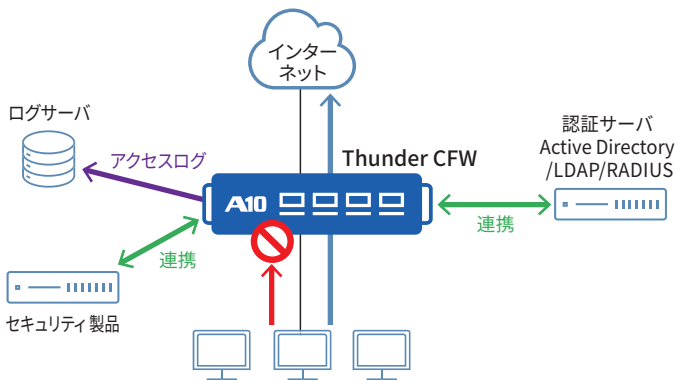
ソリューション詳細



データシート



トラフィック制御 (プロキシ)



A10のThunderシリーズはWebのフォワードプロキシとして動作します。クラウドサービスの活用により生じるインターネット向けの大規模な通信セッション処理にも十分対応できる、高いセッション処理性能を有します。上位プロキシへのプロキシチェーンやクラウドサービス向けトラフィックのバイパス、回線分散など、多様なトラフィック制御を行うことができます。

各種認証サーバ/認証サービスと連携し、ユーザーやグループを指定しての認証・認可に基づくアクセス制御を行うことで、企業や組織のゼロトラストセキュリティの実現に寄与します。

SSL/TLS通信の可視化を行い詳細なユーザーの振る舞いを記録するとともに、各種セキュリティ製品と連携して暗号化通信に隠れた脅威に対応できます。URLフィルタ・URLレピュテーション・IPアドレスレピュテーションなどの脅威インテリジェンスによる日々変化する脅威への防御も実現できます。L4ファイアウォールやアプリケーションファイアウォールの機能による通信制御も可能です。

複数のアンチマルウェアエンジンを利用して検知率を向上するマルスキャンや、ゼロデイ攻撃に対応するコンテンツ無害化、機密情報の漏洩を防ぐデータ損失防止などもプロキシ機能と併せてご利用頂けます。

A10のメリット



セキュアで快適なクラウドサービス利用環境の実現

大規模トラフィックの振り分けや回線分散による通信のボトルネック回避と、IDベースセキュリティを実現するテナント制御



ゼロトラストセキュリティの実現

認証・認可基盤と連携し、リソースおよびインターネットへのアクセスを柔軟に制御



振る舞いの追跡

暗号化通信の可視化により、セキュリティ製品と連携した隠れた脅威からの防御と詳細なアクセスログの取得が可能となり、攻撃の痕跡や従業員の振る舞いを確実に追跡



不正アクセス防止

脅威インテリジェンスとの連携により、不正なサイトへのアクセスや攻撃者からのアクセスを防止し、セキュリティを強化

対応製品

2023年3月現在

仮想アプライアンス	~ 5,000 クライアント	~ 20,000 クライアント	~ 50,000 クライアント	50,000 クライアント~	
vThunder CFW for Cloud vThunder 仮想アプライアンス Thunder for Container (Docker)	Thunder 1040S 1.5Gbps* 5x1GC, 4x1/10GF	Thunder 3350 3Gbps* 6x1GC, 2x1GF, 4x25GF, 4x40GF, 4x10GF	Thunder 5440S 15Gbps* 24x1/10GF, 4x40GF	Thunder 5840S 25Gbps* 24x1/10GF, 4x40GF	Thunder 7655S 72Gbps* 16x100GF
	Thunder 940 0.5Gbps* 5x1GC, 4x1/10GF	Thunder 3350-E 3Gbps* 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF	Thunder 4440S 8Gbps* 24x1/10GF, 4x40GF	Thunder 5840S-11 25Gbps* 24x1/10GF, 4x100GF	Thunder 7440S 25Gbps* 48x1/10GF, 4x40GF
bare metal Thunder for Bare Metal			Thunder 3350S 5.5Gbps* 6x1GC, 2x1GF, 8x1/10GF, 4x10GF	Thunder 6440S 22Gbps* 48x1/10GF, 4x40GF	

* 全通信をSSL/TLS可視化した際の最大スループット

最新情報または詳細は、右記のwebページをご覧ください。

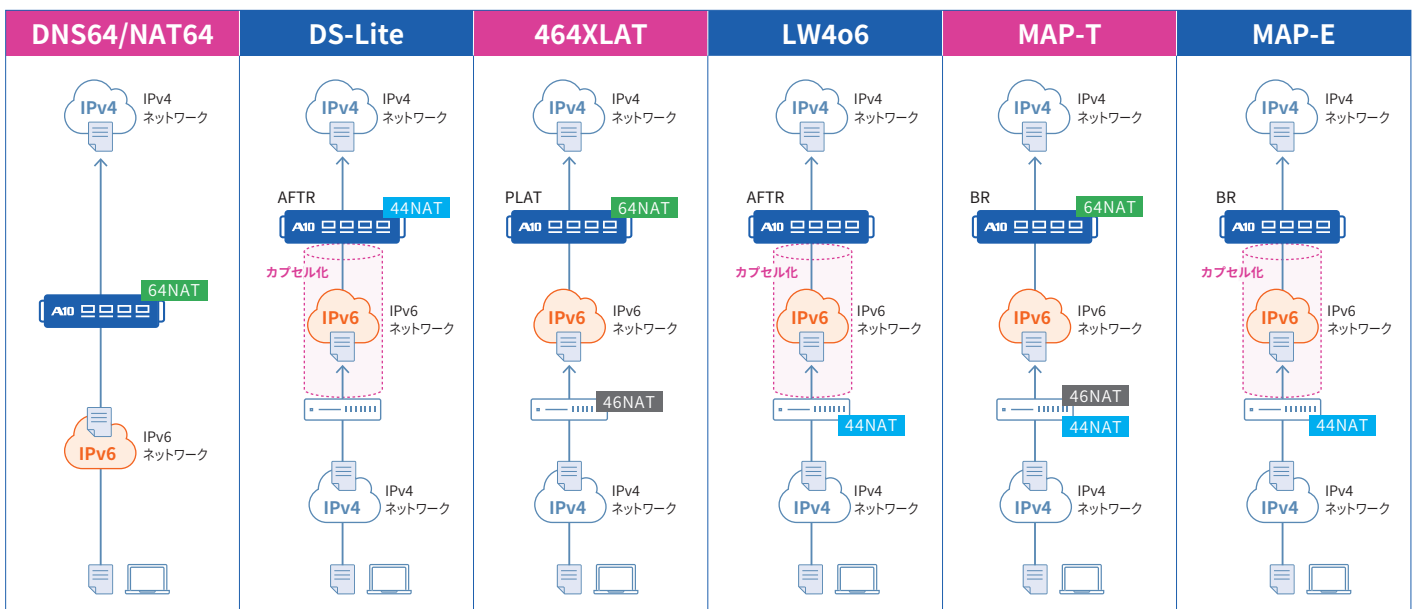
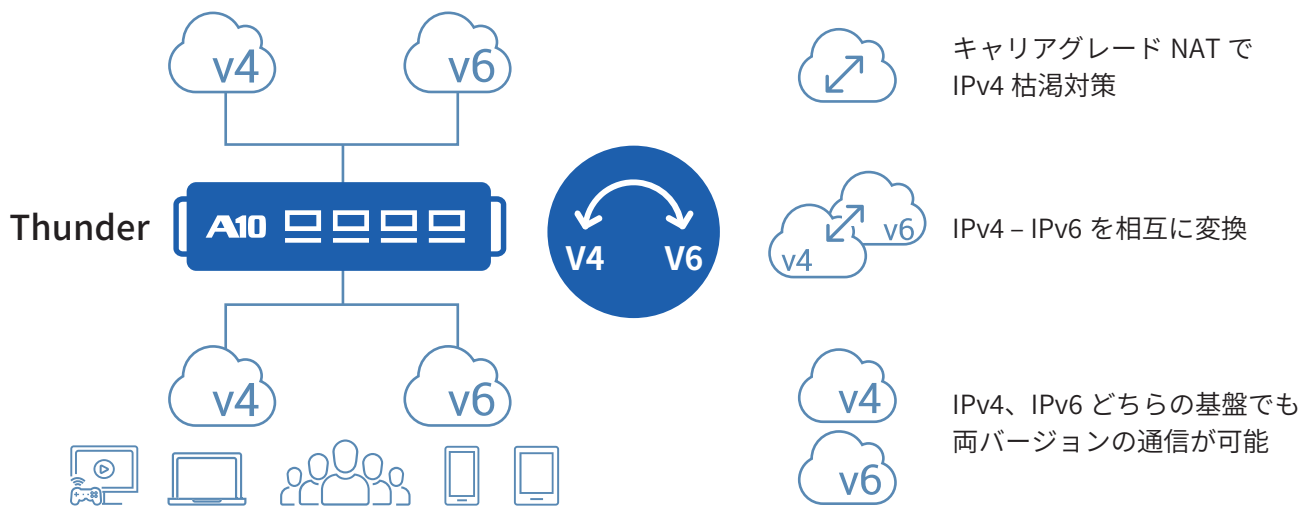
ソリューション詳細



データシート



IPv6 移行、IPv4 枯渇対策



A10のIPv4枯渇対策・IPv6移行ソリューションは、新規入手が困難なIPv4アドレスの加入者収容効率を上げて、サービスを延命することができるCGNAT機能と、あらゆるネットワーク基盤上で、IPv4、IPv6サービス両方のサービス提供を低コストで実現するトンネリングや、プロトコル変換機能を提供します。

A10のCGNATとIPv6移行技術は、過去10数年以上、国内、海外含めた多くの通信事業者で商用実績がある信頼性の高いソリューションです。

Thunder CFWモデルを利用すれば、CGNATとIPv6移行に加えて、DPIを使用した帯域制御も可能です。

大容量の専用ハードウェア製品に加えて、ベアメタルソフトウェアや、仮想ソフトウェア、コンテナでも利用できるため、ハードウェアなどの基盤設備を共通化した構成も可能です。

A10のメリット



IPアドレス購入にかかるコストを削減



IPv4、IPv6基盤の共通化で運用コストを削減



加入者通信の制御やセキュリティ機能を提供可能

主な特長



豊富な商用実績

- 国内・海外の大手通信事業者において、CGNAT及びIPv6移行の豊富な商用稼働実績を持った信頼性の高いソリューション



あらゆるIPv6移行技術に対応

- 商用で使用されているほぼ全てのIPv6移行技術に対応しているため、既存設備や投資計画に合わせた柔軟な構成を取ることが可能



大容量

- 最大同時接続数5億1200万の大容量をサポートしているため、加入者数の多い大手事業者においても高い収容効率でサービスを構成することが可能



全機能標準搭載

- サービス提供に必要な全ての機能が標準で搭載されているため、機能毎にライセンスを購入するような追加のコスト不要。また、論理パーティションを使用することで、CGNATや複数の移行技術を並行して利用することが可能



柔軟な構成

- 既存の設備がIPv4、IPv6のどちらをベースにしているか、トンネリングや変換機能を利用することで、両バージョンのサービスを提供することが可能















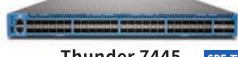



様々な提供形態

- 専用の物理アプライアンスから、仮想アプライアンス、ベアメタルソフトウェアなど、容量や使用場所によって適切なモデルを選択可能

対応製品

2023年3月現在

	～ 100Gbps	～ 200Gbps	200Gbps ～
仮想アプライアンス  vThunder 仮想アプライアンス  Thunder CGN for Container (Docker) 最大 180Gbps まで	 Thunder 4440 78 Gbps 24x1/10GF, 4x40GF	 Thunder 6440 48x1/10GF, 4x40GF	 Thunder 7655S <small>SPEモデル</small> 370 Gbps 16x100GF
	 Thunder 3350S 50Gbps 6x1GC, 2x1GF, 8x1/10GF, 4x10GF	 Thunder 5845 <small>SPEモデル</small> 115 Gbps 48x1/10GF, 4x100GF	 Thunder 7650 370 Gbps 16x100GF
	 Thunder 3350 40Gbps 6x1GC, 2x1GF, 4x25GF, 4x40GF, 4x10GF	 Thunder 5840 115 Gbps 24x1/10GF, 4x40GF Thunder 5840-11 115 Gbps 24x1/10GF, 4x100GF	 Thunder 14045 <small>SPEモデル</small> 300 Gbps 4x40GF, 4x100GF
ベアメタル  Thunder CGN for Bare Metal	 Thunder 3350 -E 30Gbps 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF	 Thunder 5440 100 Gbps 24x1/10GF, 4x40GF	 Thunder 7445 <small>SPEモデル</small> 220 Gbps 48x1/10GF, 4x100GF  Thunder 7440 220 Gbps 48x1/10GF, 4x40GF Thunder 7440-11 220 Gbps 48x1/10GF, 4x100GF

*SPEモデル：セキュリティポリシーの適用を高速化するハードウェアであるSPE(Security and Policy Engine)を搭載したモデル

最新情報または詳細は、
右記のwebページをご覧ください。

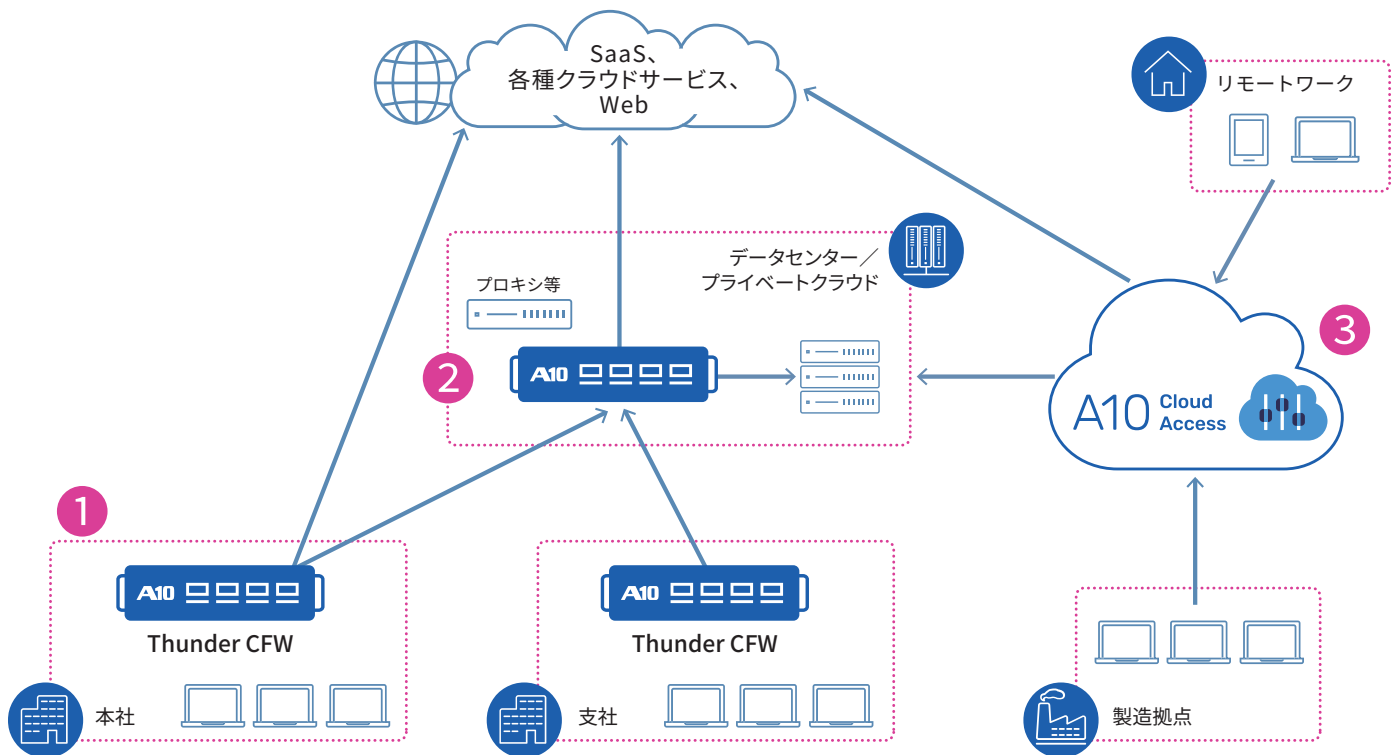
ソリューション詳細



データシート



クラウド活用・DX推進



1 クラウドアクセスプロキシ

- ローカルブレイクアウト
- テナント制御
- プロキシなどネットワーク機器の負荷軽減
- シャドー ITの監視
- アプリケーションごとの接続監視
- ファイアウォール等、各種セキュリティ

2 データセンターブレイクアウト

- 信頼できる SaaS へはプロキシを迂回させる等、ネットワーク機器の負荷軽減
- フォワードプロキシ、リバースプロキシ
- SSL/TLS 通信の可視化
- 各種セキュリティ

3 Cloud Access Controller

- A10 が提供するクラウドサービス
- トラフィック制御+アクセス制御+セキュリティをクラウド上で
- シンプルなライセンス体系
- 様々なセキュリティ機能との連携
- 上位の SaaS・SASE ソリューション等と連携して、トータルコストの抑制に
- Zero Trust Network Access (ZTNA)
- Secure Web Gateway

A10 のメリット



トラフィック分離

- ローカルブレイクアウト、データセンターブレイクアウト時に宛先ドメインでの分離
- SSL/TLS 通信の可視化
- 自治体ネットワークの三層分離に対応



アクセス制御

- ID ベースのアクセス制御
- テナント制御
- 特定サイト以外へのアクセスのブロック
- URL フィルタ
- アクセスログの取得



セキュリティ

- ブレイクアウト後のトラフィックへのセキュリティ
- マルチスキャン、無害化、データ漏洩防止などの各種セキュリティ機能を利用可能

最新情報または詳細は、
右記の web ページをご覧ください。

A10 Cloud Access Proxy
ブレイクアウトソリューション詳細



A10 Cloud Access Controller
ソリューション詳細



データシート



主な機能



様々なセキュリティ機能

- URL フィルタリング
- IPレピュテーション
- 認証基盤との連携
- アプリケーションファイアウォール
- レイヤ3, レイヤ4ファイアウォール
- レートリミット機能
- マルチスキャンエンジン
- ファイル無害化 (CDR)
- データ損失防止 (DLP)
- SSL/TLS 復号
- アクセスログ取得



トラフィック振り分け

- A10 Thunder CFWをプロキシとして導入することにより、SaaS 導入後の既存プロキシへの負荷を軽減
- 不定期に変更される Microsoft 365 のドメイン名の自動更新も可能



回線オフロード

- 例えば、SaaS へのアクセスはプロキシを経由せず直接 SaaS 専用回線へ振り分け、SaaS 向け通信以外は、既存プロキシサーバへ振り分け
- 回線のひっ迫を回避しながら安全性も担保



Secure Web Gateway

- 明示型 / 透過型プロキシとして動作
- URL フィルタリング、アプリケーション可視化・制御、脅威インテリジェンスなどの機能によりリスクを軽減。ユーザーレベルのきめ細かい制御を実現
- SIEM 製品との連携、高速ロギングなどにより、プライバシー標準に準拠したコンプライアンスを実現
- SSL/TLS 可視化機能



テナント制限

- 指定した法人アカウントのみクラウドサービスへのログインを許可することで個人アカウントや無料アカウントの使用を制限し、機密情報が漏洩するリスクを低減

対応製品

2023年3月現在

仮想アプライアンス	～ 5,000 クライアント	～ 20,000 クライアント	～ 50,000 クライアント	50,000 クライアント～	
 vThunder CFW for Cloud vThunder 仮想アプライアンス Thunder for Container (Docker)	 Thunder 1040S 1.5Gbps* 5x1GC, 4x1/10GF	 Thunder 3350 3Gbps* 6x1GC, 2x1GF, 4x25GF, 4x40GF, 4x10GF	 Thunder 5440S 15Gbps* 24x1/10GF, 4x40GF	 Thunder 5840S 25Gbps* 24x1/10GF, 4x40GF Thunder 5840S-11 25Gbps* 24x1/10GF, 4x100GF	 Thunder 7655S 72Gbps* 16x100GF
	 Thunder 940 0.5Gbps* 5x1GC, 4x1/10GF	 Thunder 3350-E 3Gbps* 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF	 Thunder 4440S 8Gbps* 24x1/10GF, 4x40GF	 Thunder 6440S 22Gbps* 48x1/10GF, 4x40GF	 Thunder 7440S 25Gbps* 48x1/10GF, 4x40GF Thunder 7440S-11 25Gbps* 48x1/10GF, 4x100GF
 Thunder for Bare Metal		 Thunder 3350S 5.5Gbps* 6x1GC, 2x1GF, 8x1/10GF, 4x10GF			

* 全通信を SSL/TLS 可視化した際の最大スループット

Cloud Access Controller ライセンス体系 A10 Cloud Access

2023年3月現在

Basic、Standard、Advanced の包括ライセンスのみ

- 追加オプション有

クライアント数での課金

- 課金単位：100 クライアント
(最小利用：100 クライアントより)

期間：1年単位 (最小契約：1年)

- フリートライアル：有 (1か月)

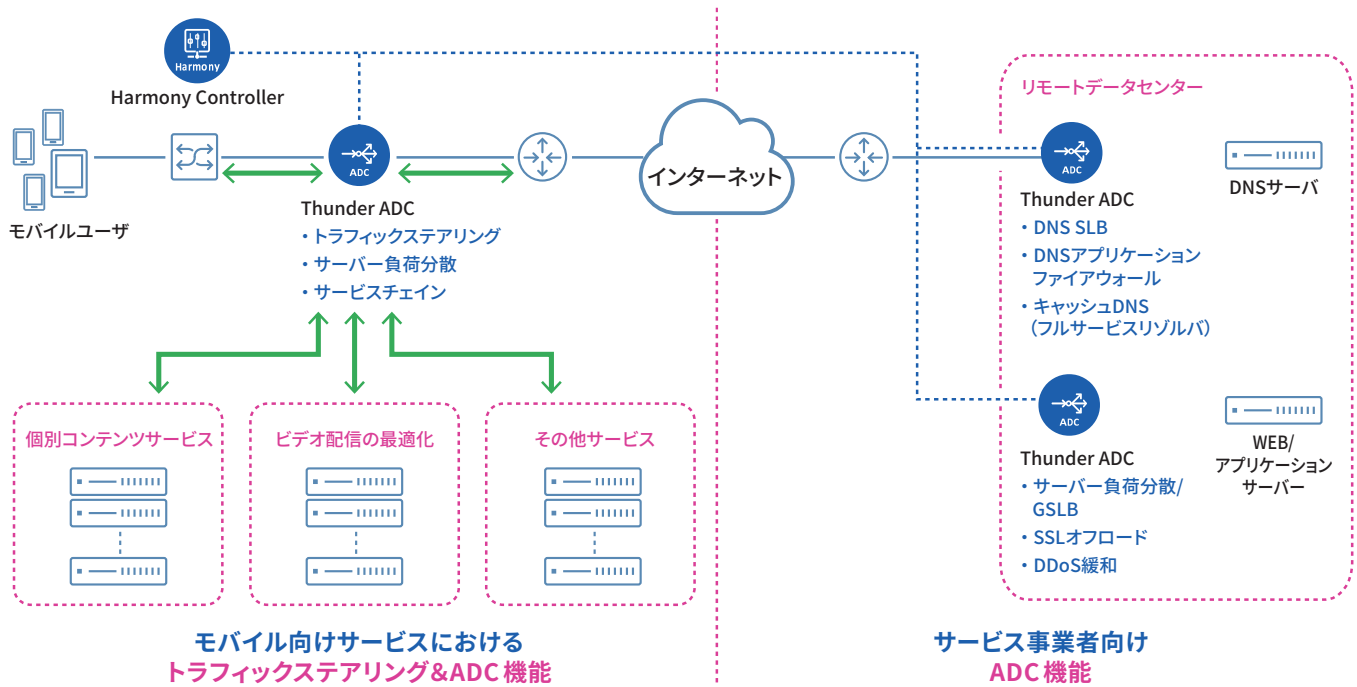
アクセスログは最大3か月保管

- (ログは Web API 経由で取得可能)

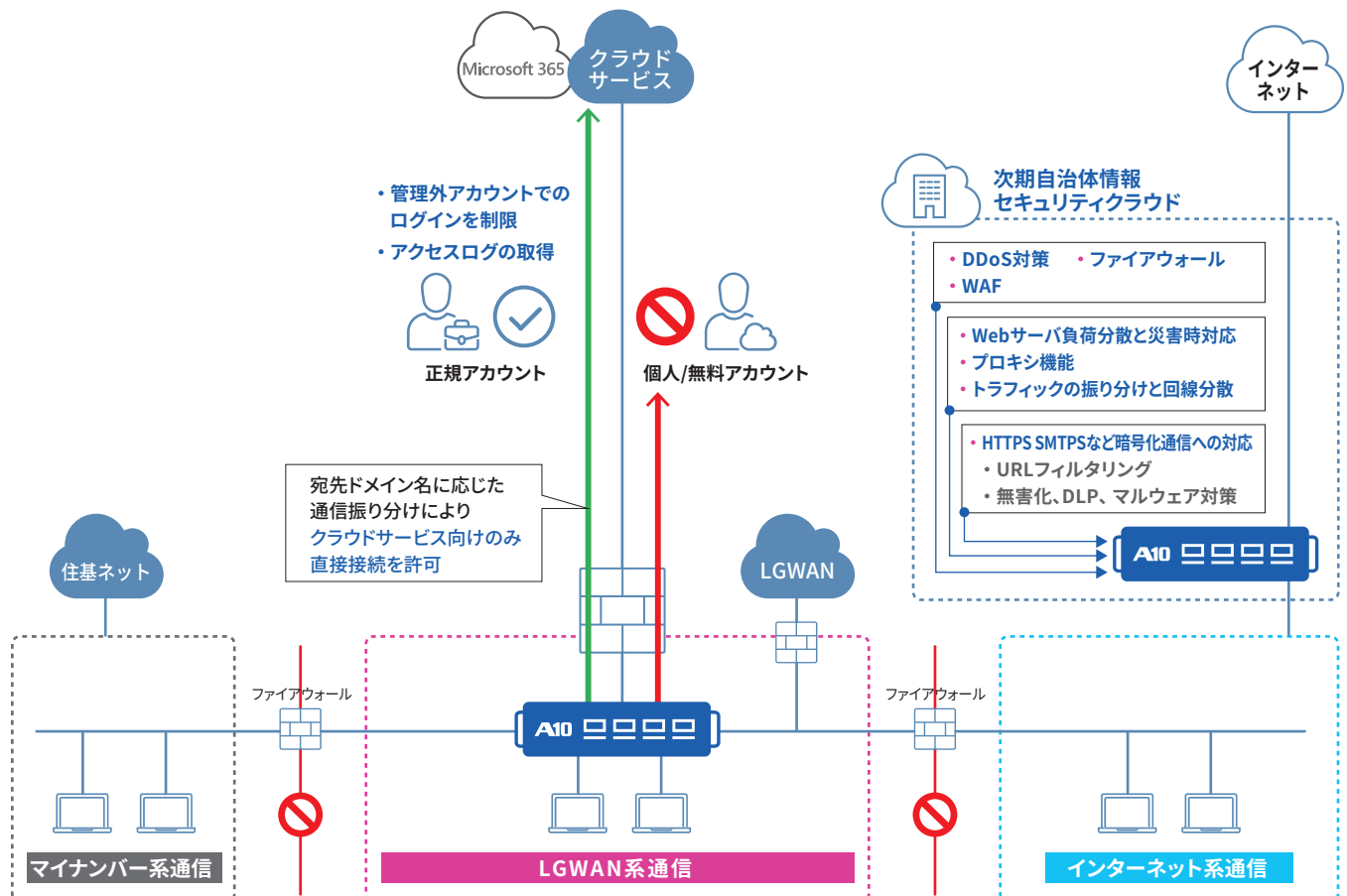
機能	ライセンス種別			
	Basic	Standard	Advanced	追加オプション
フォワードプロキシ	○	○	○	
リバースプロキシ	○	○	○	
トラフィック制御機能	○	○	○	
認証基盤連携	○	○	○	
アクセスログ保管	○	○	○	
URL フィルタリング	○	○	○	
SSL/TLS 復号		○	○	○
SaaS サービスのテナント制御		○	○	○
IP アドレスレピュテーション			○	○
アプリケーション可視化と制御			○	○
アンチマルウェア				○
コンテンツ無害化				○
データ損失防止				○
Site-to-Site IPsec VPN による接続				○

導入例

Web 事業者

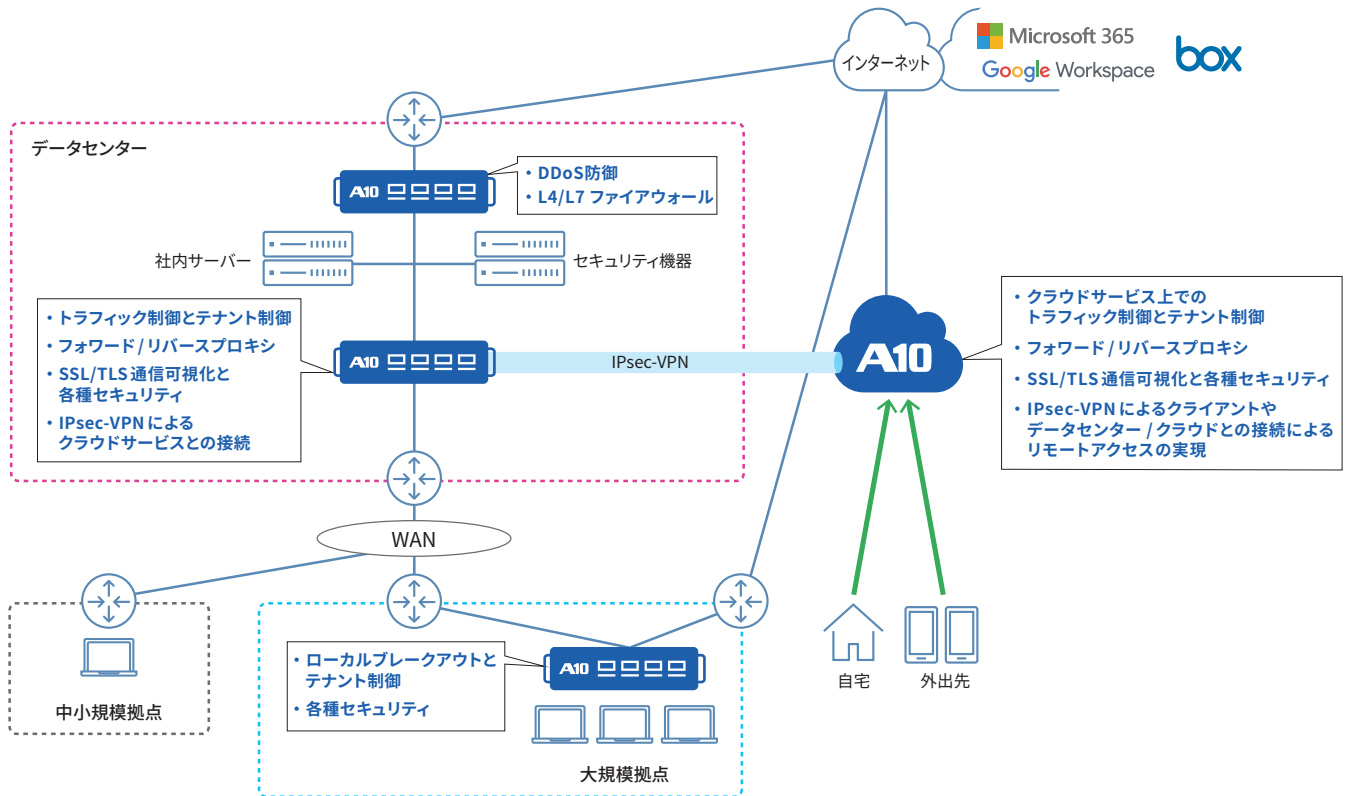


自治体



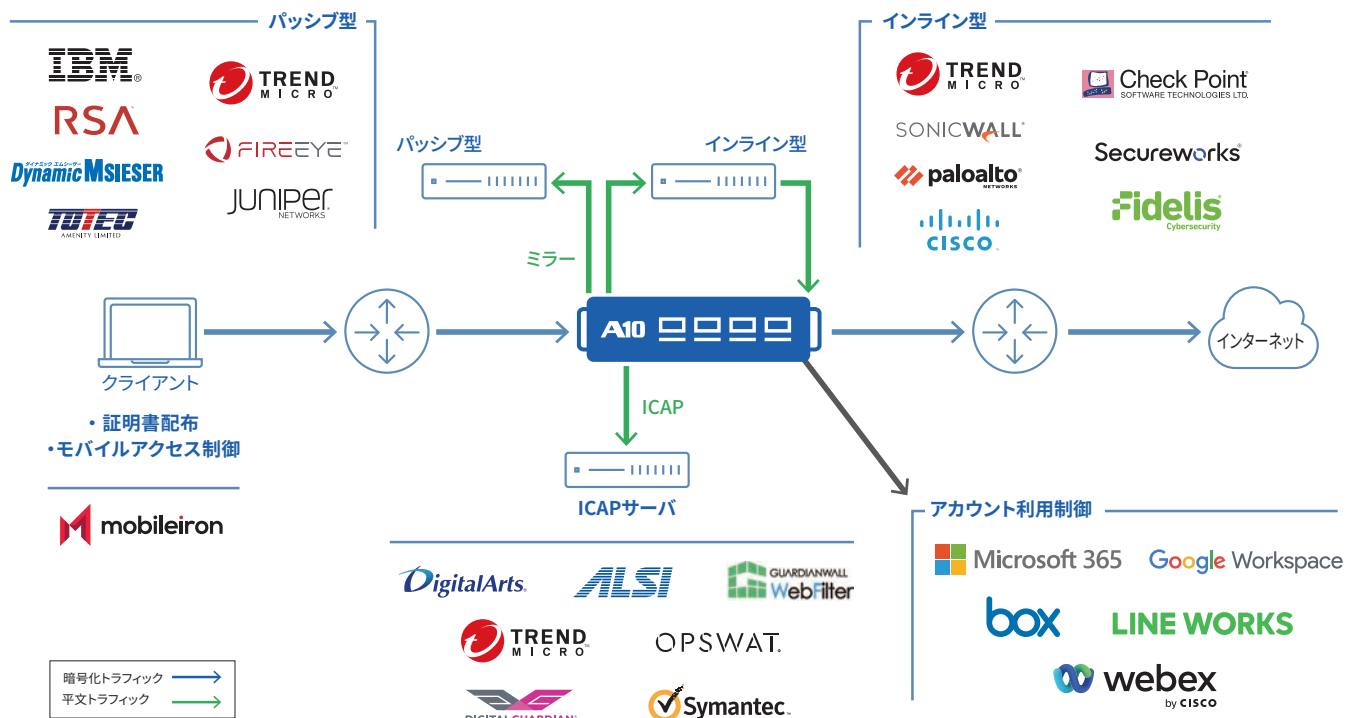
エンタープライズネットワーク向けソリューションマップ

データセンター／拠点／クラウドの各ポイントで通信トラフィックを最適化しセキュリティを強化



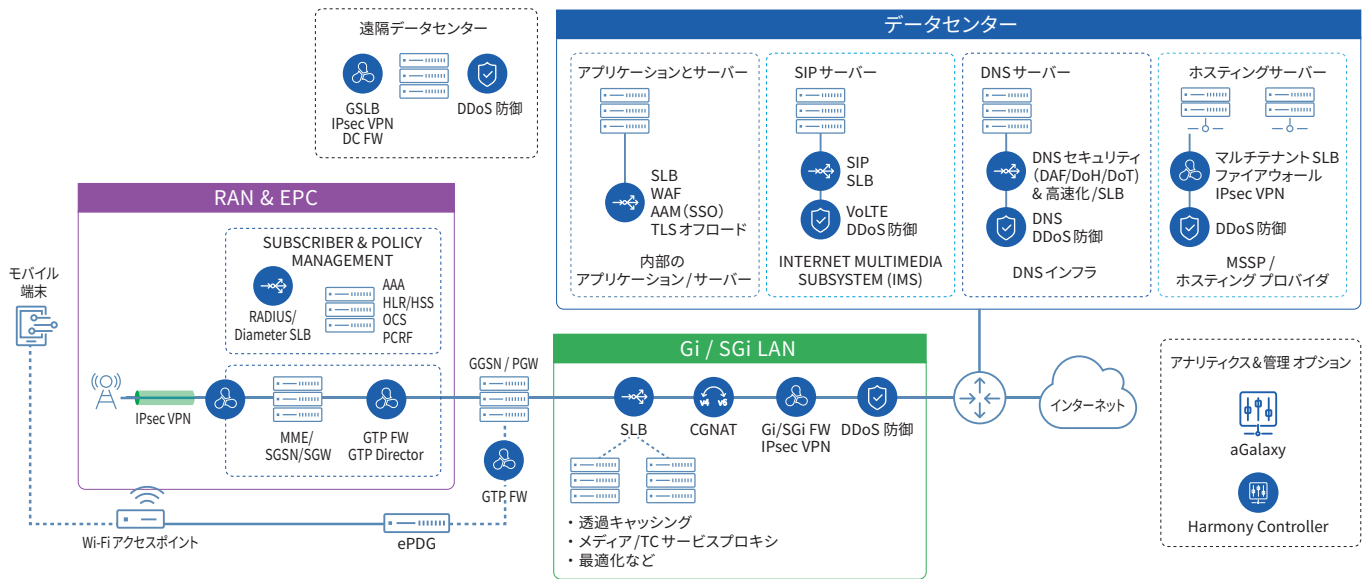
SSL/TLS 通信可視化と連携ソリューション

SSL/TLS 通信を高速に復号し多様なセキュリティ製品と連携、暗号化通信に隠れた脅威を検知し防御

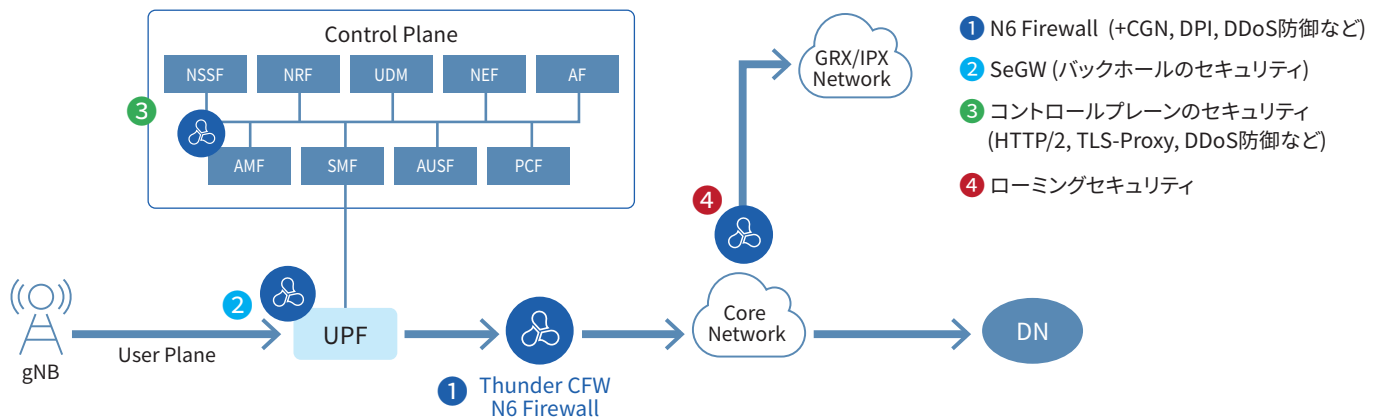


導入例

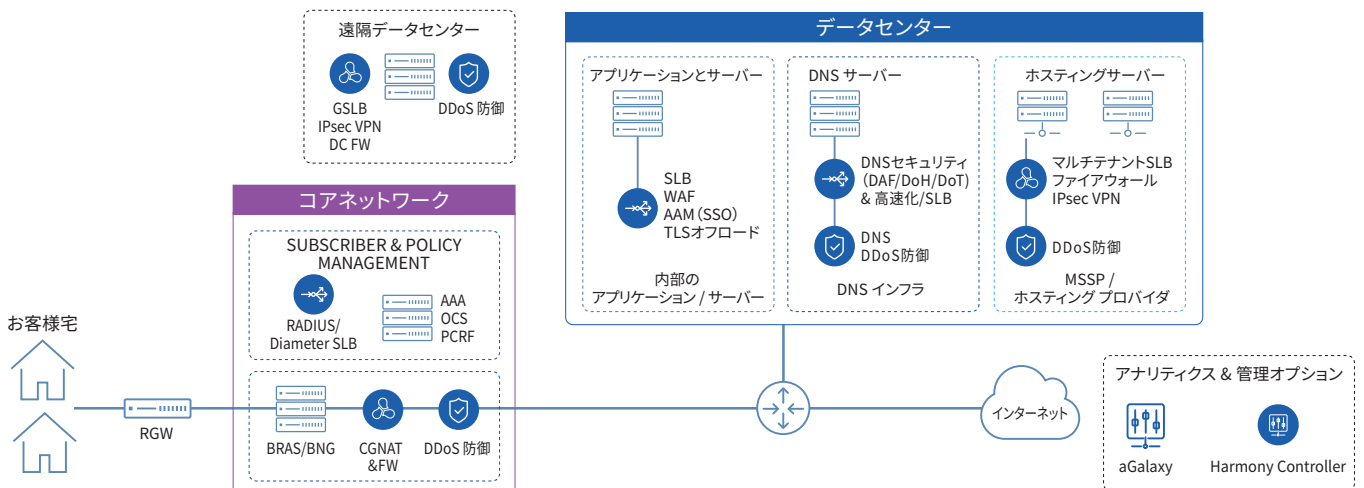
モバイル事業者様向けソリューションマップ (LTE/5G-NSA 向け)



モバイル事業者様向けソリューションマップ (5G-SA 向け)



ISP/CATV 事業者様向けソリューションマップ

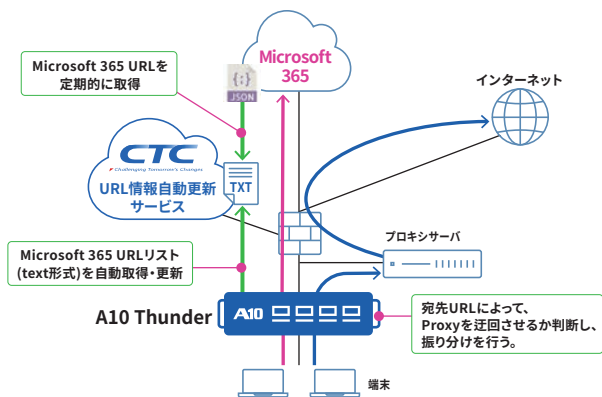


パートナーソリューション

Microsoft 365ドメイン情報自動更新ソリューション

Microsoft 365のドメイン情報は定期的に更新があり、手動で更新する場合には運用負荷が増大します。そこで、A10が提供するAPIやA10の販売パートナーが提供するソリューションを利用することにより、振り分けに必要な設定更新を完全に自動化することができます。

各ソリューションの詳細は、A10 ネットワークまでお問い合わせください。a10networks.co.jp/contact



伊藤忠テクノソリューションズ株式会社

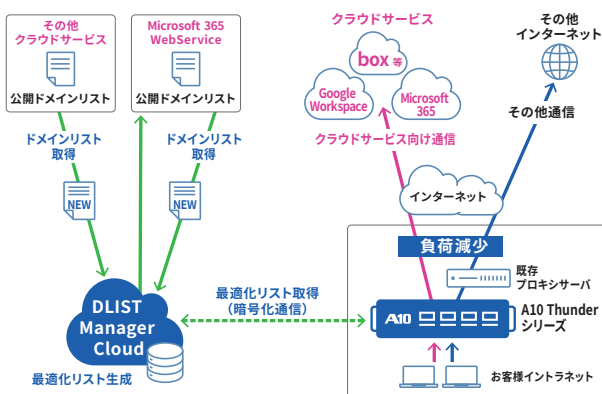
Microsoft 365 利用時における Proxy 負荷軽減ソリューション クラウドアクセスプロキシ向け URL 情報自動更新サービス

Microsoft 365 を利用する企業が増加しています。Microsoft 365 の利用を開始すると、Proxy サーバに対するアクセスが増加し負荷が高くなり、Proxy サーバのパフォーマンス不足の問題が発生します。

Proxy サーバの負荷軽減を行うためにロードバランサを導入し、Microsoft 365 向けの通信を迂回させます。宛先が変更されても、ロードバランサが宛先情報を自動取得し、反映させることで運用負荷軽減を図ります。

お問い合わせ: 情報通信事業グループ 情報通信事業企画室
a10-info@ctc-g.co.jp

Webサイト: https://www.ctc-g.co.jp/solutions/a10_axthunder/

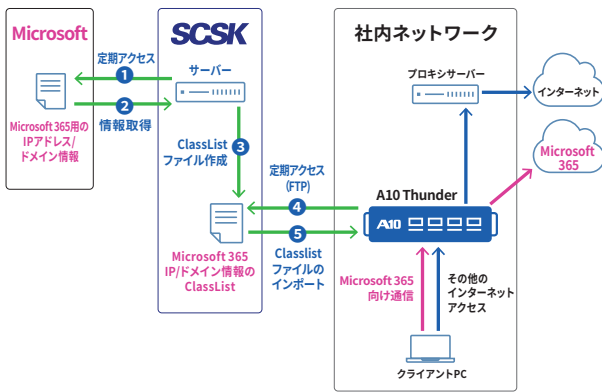


富士通ネットワークソリューションズ株式会社

運用の自動化による業務の安定稼働を実現 FUJITSU Network DLIST Manager Cloud サービス

本サービスは、A10 製品を新規または更新でご導入頂く際には無償でバンドルしてご提供しており、Microsoft365をはじめ、WindowsUpdateや複数のクラウドサービス(Box、Google Workspace、Webex Meetings、Zoom)の公開ドメインリスト情報を自動で取得しA10に適用することで、常に最新のリスト情報でA10の振り分けが可能となります。さらに、「個別指定リスト機能」や「除外リスト機能」を有し、リストの個別カスタマイズが可能のため、お客様のネットワーク環境に合わせてきめ細やかな運用を行うことができます。

お問い合わせ: 総合受付窓口
0120-20-7430 | <https://www.fujitsu.com/jp/group/fnets/contact/>
Webサイト: <https://www.fujitsu.com/jp/group/fnets/solutions/network/a10/>



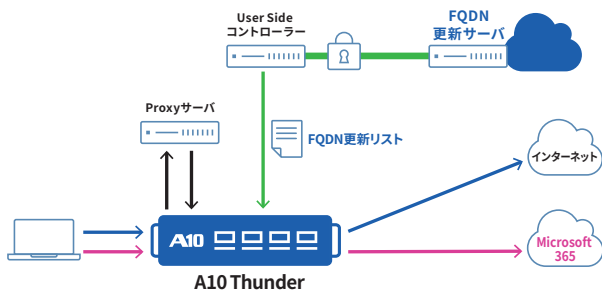
SCSK 株式会社

クラウドプロキシのA10 運用負荷軽減無償サービス A10 機器向け Classlist ファイル自動更新サービス

Microsoft 365 の IP/ドメイン情報は定期的に変更されることがあり、その都度設定を変更する必要があります。本ソリューションは、最新の IP/ドメイン情報を SCSSK が提供することで、運用の手間を軽減する無償のソリューションです。SCSK が Microsoft 365 や関連サービスで利用される最新の IP/ドメイン情報を Microsoft より取得し、Classlist ファイルを生成します。お客様側では、簡単な A10 機器の設定を行うだけで、SCSK から Classlist ファイルを定期的に取得することができます。

お問い合わせ: ネットワークセキュリティ事業本部 ネットワークプロダクト第二部
a10-info@scsk.jp

Webサイト: https://www.scsk.jp/product/common/a10networks/cloud_access_controller.html



三井情報株式会社

ボトルネックを解消し、快適なクラウドアクセス環境を実現 クラウドサービスアクセス時の Proxy 環境改善

通信回線、インフラ構築、保守運用をワンストップで提供する三井情報のマネージドサービス「M-ANVO」のCloud Proxyサービス「M-ANVO Proxy」では、クラウドサービスのFQDNが変更されても自動で更新する「FQDN自動更新サービス」をオプションで提供しています。クラウドサービスの仕様変更に対応することや、セキュリティを考慮し外部から直接A10 Thunderを操作させないことを目的として、User Sideコントローラーをお客様サイトに設置します。コントローラーはHTTPSを用いて、クラウド上にある弊社システムからFQDN更新リストをダウンロードし、Thunderに自動的に更新を反映することで、システム管理者様の負荷を軽減します。

お問い合わせ: ホームページよりお問い合わせください
Webサイト: <https://www.mki.co.jp/>

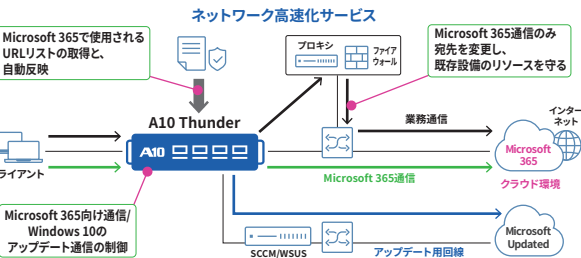
- お客様導入メリット
- ✓クラウドサービスのスムーズな導入を実現
 - ✓クラウドサービスの通信経路の最適化
 - ✓運用者の負荷を軽減するFQDN自動更新サービス

パートナーソリューション

各ソリューションの詳細は、A10 ネットワークスまでお問い合わせください。a10networks.co.jp/contact

「NEC 365」サービスラインナップ

セキュリティ	運用	利便性向上	利活用促進
シングルサインオン 認証サービス	運用代行 トラフィック可視化	ネットワーク高速化サービス	クラウドバックアップ サービス
ファイル暗号化 サービス	サポートデスク データ管理 ソリューション	専用型アドレス簿	Microsoft 365 ニュース
会議室3密検知 ソリューション	会議室3密検知 ソリューション	認証型PCセキュリティサービス	エンドユーザー 教育サービス
		認証型PCセキュリティサービス	メールアーカイブ サービス



日本電気株式会社

Microsoft365をより快適にするサービス「NEC365」

ネットワーク高速化サービス

「快適にMicrosoft 365を利用するには、アプリケーションの導入検討だけでは足りません」Microsoft 365やWindows 10を快適に利用するには、アプリケーションのメリットを十分に享受するネットワーク環境の検討や運用者の負担軽減などを考慮した導入/運用コストの最適化という様な課題解決が必要となります。

NECの導入支援サービス「ネットワーク高速化サービス」では、豊富な導入実績とノウハウを集約し、少ないコストでURL自動更新サービスを含む快適なMicrosoft 365の利用を実現します。

お問い合わせ: 各 NEC 担当営業の窓口までご連絡ください

SCSK 株式会社

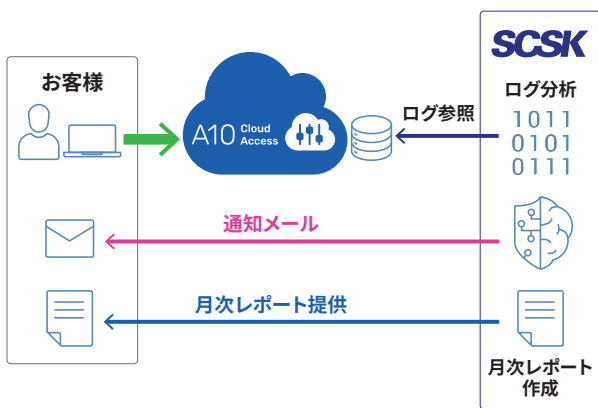
Cloud Access Controller 向け簡易SOCサービス

Cloud Access Controller セキュリティレポートサービス

Cloud Access Controller から検出したログをもとに、緊急性の高い不正アクセスを検知した場合にメールで通知、重要度の高い事象とその他の事象に関してはアクセス分析結果と推奨される対策について月次レポートとして提供します。セキュリティリスクの高いWebサイトへのアクセスやレピュテーションスコアの低い(ハイリスク)サイトへのアクセス、制限サイトへのアクセスや全Webアクセスのカテゴリ分析など、ユーザの利用実態をご確認いただき、推奨される対策案をご案内するサービスです。*2023年夏稼働予定

お問い合わせ: ネットワークセキュリティ事業本部 ネットワークプロダクト第二部
a10-info@scsk.jp

Webサイト: https://www.scsk.jp/product/common/a10networks/cloud_access_controller.html



株式会社日立ソリューションズ

Menlo Security と A10 Thunder を連携させることで、安全 / 快適な Web 利用環境を実現

安全 Web 閲覧ソリューション

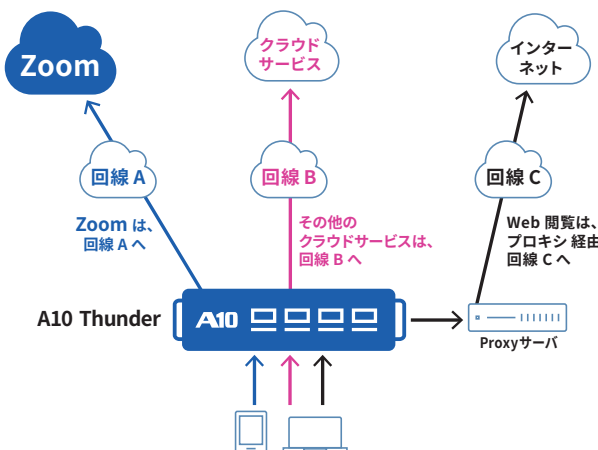
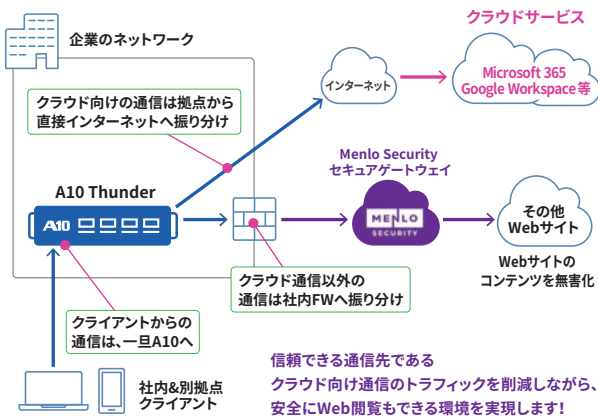
リモートワークやクラウド (Microsoft 365 等) の利用拡大、悪意のあるコンテンツが増加している昨今、安全・快適に Web が利用できないという声は上がっていませんか
⇒ この問題は Menlo Security と A10 Thunder を組合せることで解決可能です。

① 【Menlo Security】コンテンツをクラウド上の隔離された環境で実行、表示のみをクライアントに送信し、デバイス・OS・ブラウザの種類を問わず、悪意あるコンテンツからクライアントを防御 (エージェントレス)

② 【A10 Thunder】クラウドアクセスプロキシ機能で安全な通信を直接 Web にブレイクアウトさせることにより、ネットワークの負荷を軽減

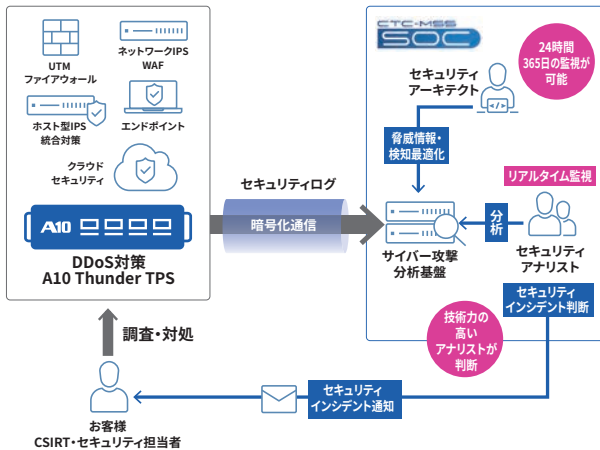
お問い合わせ: ネットワーク・サイバーセキュリティソリューション部
hs-a10@ml3.hitachi-solutions.com

Webサイト: <https://www.hitachi-solutions.co.jp/a10/>



パートナーソリューション

各ソリューションの詳細は、A10 ネットワークスまでお問い合わせください。a10networks.co.jp/contact



伊藤忠テクノソリューションズ株式会社

Thunder TPS で検知した DDoS 攻撃を 24 時間 365 日監視するサービス CTC-SOC for A10 Thunder TPS

DDoS 攻撃は現在も多くの被害を及ぼしています。

本サービスは、A10 ネットワークス Thunder TPS で検知した DDoS 攻撃を、CTC-SOC の技術力の高いセキュリティアナリストが 24 時間 365 日監視するサービスです。検知内容を分析して緊急度に合わせて通知し、お客様の DDoS 対策の運用をサポートします。お客様環境のインシデント状況については可視化できるポータルサイトをご用意し、月次で当月の検知状況を確認できるレポートもご提供します。

Thunder TPS の導入を検討中、あるいは運用監視に課題をお持ちの際は、「CTC-SOC for A10 Thunder TPS」をご検討ください。

お問合せ：情報通信事業グループ 情報通信事業企画室
a10-info@ctc-g.co.jp

Web サイト： https://www.ctc-g.co.jp/solutions/a10_axthunder/

世界で 7,800 社を超える導入実績

A10 ネットワークスの提供する製品群は、世界中のあらゆる分野のリーダー企業、7,800 社以上でご利用いただいています。

特に Web コンテンツプロバイダーや、サービスプロバイダーなど、高い信頼性・耐障害性・可用性が求められるシステムにおいて多数の実績があります。(以下ご導入企業例：順不同)

2023 年 3 月現在

■ 通信事業者

KDDI 株式会社
ソフトバンク株式会社
株式会社ワイヤ・アンド・ワイヤレス
ひまわりネットワーク株式会社
株式会社日本ネットワークサービス
株式会社ケーブルネット鈴鹿
株式会社 NTT ぷらら
ケーブルテレビ株式会社

■ データセンター

株式会社 IDC フロンティア
ビットアイル・エクイニクス株式会社
株式会社エヌ・ティ・ティ・データ
さくらインターネット 株式会社
Fujitsu Asia Pte Ltd
株式会社リンク
株式会社 ODK ソリューションズ
日本電気株式会社
株式会社クララオンライン
株式会社シナジー

■ 教育

福岡大学
琉球大学
京都産業大学
東京造形大学
京都工業繊維大学

■ ポータルサイト

ヤフー株式会社
エキサイト株式会社

■ ゲーム・コンテンツ配信

株式会社セガ
株式会社ゲームオン
株式会社スクエア・エニックス
株式会社ドワンゴ

■ サービスプロバイダ/メディア

株式会社サイバーエージェント
バリューコマース株式会社
株式会社 DMM.Com ラボ
株式会社テレビ東京コミュニケーションズ
GMO インターネット株式会社
松竹株式会社
株式会社 IT コア

■ 金融

シンプレクス株式会社
株式会社保険見直し本舗

■ 製造業

カシオ計算機株式会社
株式会社寺岡製鋼
清水建設株式会社

■ 官公庁・自治体

山口県
八代市
北本市
岐阜市
由利本荘市
鳥取市
南アルプス市

■ IT サービス

伊藤忠テクノソリューションズ株式会社
三井情報株式会社

基本設定や操作感をお試しいただける、無料のハンズオンセミナーや、無料のトライアル版をご提供しております。

A10を今すぐ試すには

https://www.a10networks.co.jp/download/resources_try-a10.html



無料ハンズオンセミナー

Thunderシリーズの操作に必要な基礎的な内容をハンズオン演習を交えて受講可能な無料のセミナーです。
<http://www.a10networks.co.jp/training/hands-on/hands-on.html>



無料トライアル

Thunderシリーズの仮想版を、トライアル期間内は制限なしでご利用いただけます。
<https://www.a10networks.co.jp/download/free-trial/>



簡単スタートアップマニュアル

Thunderシリーズをこれからご利用になるお客様に最適な簡単マニュアルです。
<http://www.a10networks.co.jp/download/startupmanual/>



無料オンライントレーニング

Thunderシリーズの操作に必要な基礎的な内容をオンラインで学ぶことができます。
<https://www.a10networks.co.jp/download/e-learning/>



A10 Networks / A10 ネットワークス株式会社について

A10 Networks (NYSE: ATEN)は、サービス事業者やクラウド事業者および企業で利用される5Gネットワークやマルチクラウドアプリケーションのセキュリティを確保します。高度な分析や機械学習、インテリジェントな自動化機能により、ミッションクリティカルなアプリケーションを保護し、信頼性と可用性を担保します。A10 Networks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拠地を置き、世界117か国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ク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。

www.a10networks.co.jp/

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

©2023 A10 Networks, Inc. All rights reserved. A10 ロゴ、A10 Networks は米国およびその他の各国におけるA10 Networks, Inc. の商標または登録商標です。その他上記の全ての商品およびサービスの名称はそれら各社の商標です。A10 Networks は本書の誤りに関して責任を負いません。A10 Networks は、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。商標について詳しくはホームページをご覧ください。 www.a10networks.com/a10-trademarks

Part Number: A10-Product Overview _2 APR 2023