

A10

A10 ネットワークス

総合カタログ

ビジネスクリティカルなアプリケーション配信を支え、最新のセキュリティを様々なプラットフォームに

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。

ISP/通信事業者



Webサービス企業



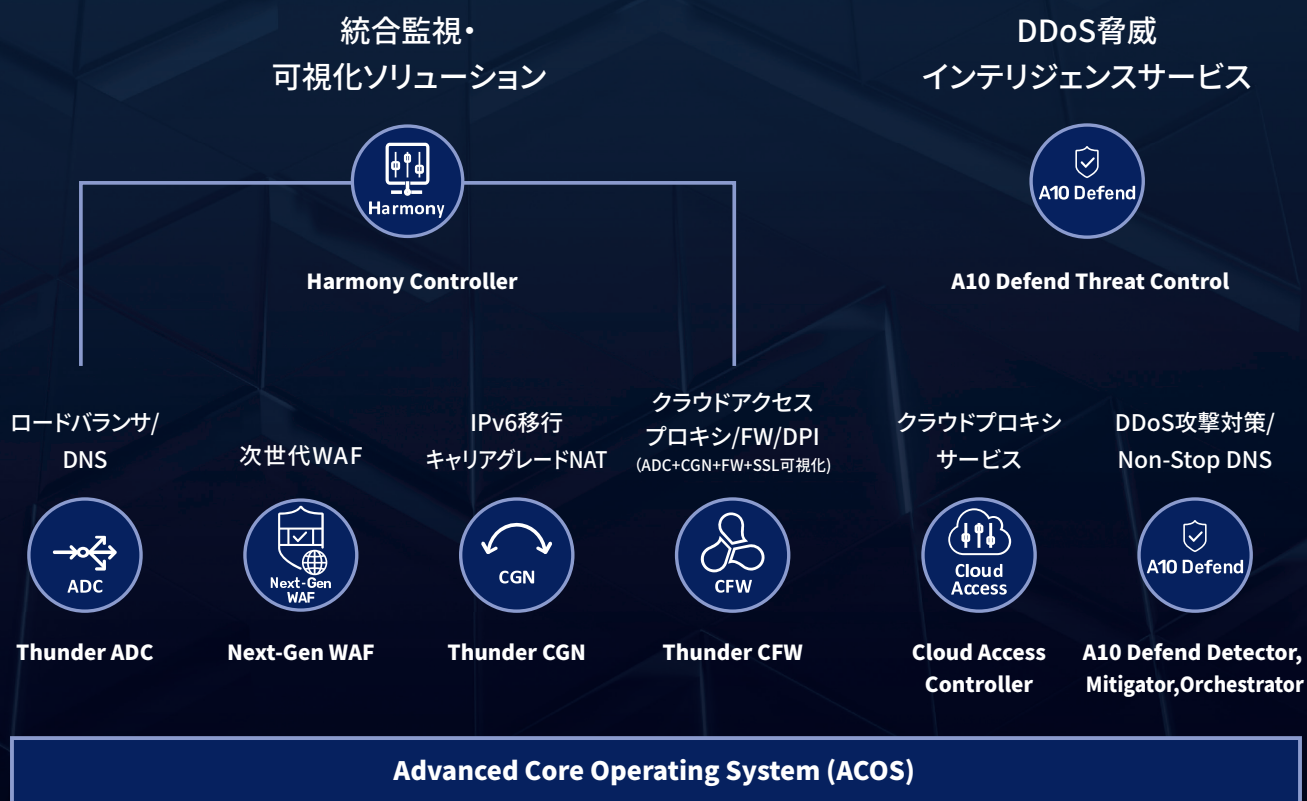
企業・自治体



データセンター



A10 の製品ラインナップ



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 ▶ P8

サーバー負荷分散・アプリケーション配信



- ・サーバーロードバランス
- ・グローバルサーバーロードバランス
- ・キャッシュ DNS

詳しくは ▶ P10

帯域制御・公平制御



- ・DPI
- ・公平制御

詳しくは ▶ P12

A10

プロキシ



- ・セキュア Web ゲートウェイ
- ・SSL/TLS 可視化

詳しくは ▶ P13

IPv6 移行・IPv4 枯渇対策



- ・キャリアグレード NAT (CGNAT)
- ・IPv6 移行技術

詳しくは ▶ P14

ローカルブレイクアウト・クラウドアクセスプロキシ



- ・トラフィック振り分け
- ・テナント制御

詳しくは ▶ P16

様々なライセンス体系・提供形態

製品ラインナップ別プラットフォーム対応表はこちら



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・ クラウドインスタンス



クラウドでもオンプレでも
使える高いモビリティ

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

FlexPool



帯域プール
ライセンス

モジュラー ライセンス



帯域やモデルを
自由に変更

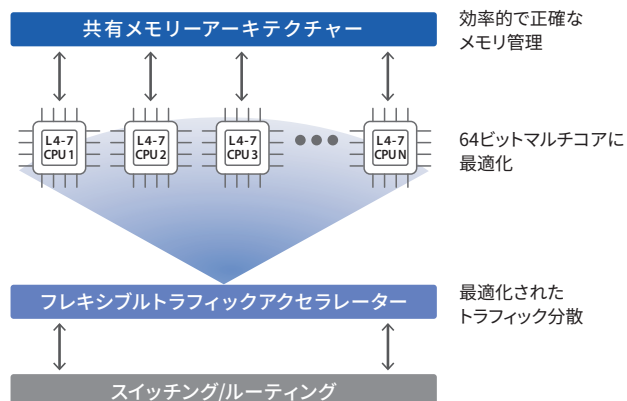
セキュリティオプション(追加ライセンス)

- ・URL フィルタリング/URL レビューション
- ・アプリケーション識別 L7 ファイアウォール
- ・IP アドレスレビューション
- ・ファイルセキュリティ (アンチマルウェア、コンテンツ無害化、データ損失防止など)
- ・A10 Next-Gen WAF, Powered by Fastly



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

注目のソリューション

自社サービスで使用している IP アドレスが
DDoS 攻撃に悪用されていないか監視できるクラウドサービス

A10 Defend Threat Control

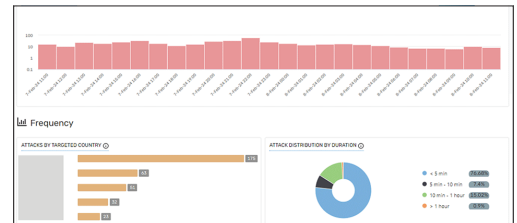


詳細を
Webで確認

予め登録した自社サービスの IP を監視

- ・ 攻撃に加担する可能性があるのか？
- ・ 攻撃を受けているのか？
- ・ 攻撃をしてしまっているのか？

これらを把握することで攻撃リスクを軽減



世界の DDoS 攻撃状況を表示



世界中のサービスプロバイダに提供している
DDoS 対策技術をベースとした脅威インテリジェンス



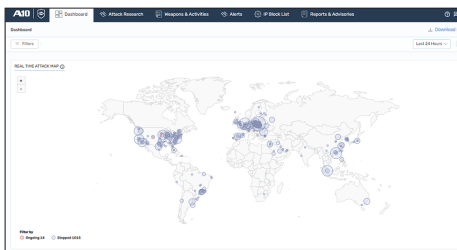
独自のスキャナー

- ・ 攻撃ツール化されたデバイスのスキャン
- ・ 攻撃インフラの分析

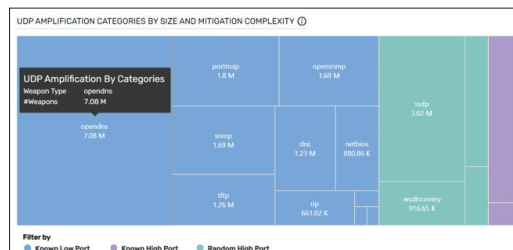
独自のセンサーネットワーク

- ・ 悪意のある活動の監視
- ・ 攻撃傾向の把握

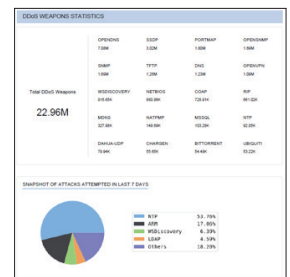
A10 Defend Threat Control の画面例



ポータル画面 (ダッシュボード)



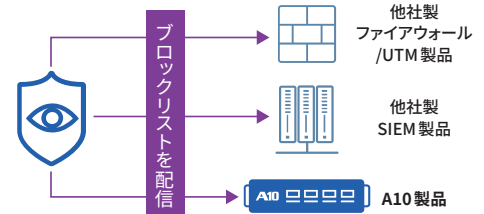
プロトコル毎の UDP アンプ攻撃ツール数



プロトコル毎のリフレクタ数

DDoS 攻撃に特化した精度の高いブロックリストで 既存のセキュリティ機器と連携可能

- ・ 各種ブロックリストを提供 (Bot ネット・リフレクタ・C2 サーバ等)
- ・ 他社製ファイアウォールや SIEM 製品にインポート可能
- ・ ブロックリストのサイズはカスタマイズ可能
- ・ A10 製品であればサイズを気にせずインポート可能



世界中で発生している DDoS 攻撃の傾向も確認可能 アドバイザリやレポートなどで防御計画の立案を支援

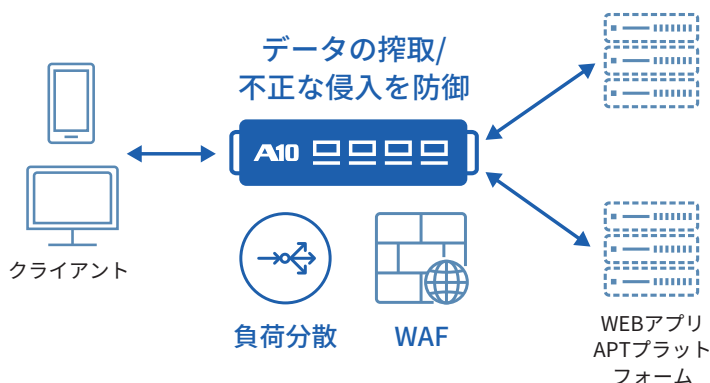
- ・ 専用ポータルからいつでも脅威の状況を把握
- ・ アドバイザリやレポートでプロアクティブな防御を支援
- ・ 攻撃ツール化されたデバイスや被害 IP を検索可能
- ・ クラウドサービスだから新規の設備導入やインテグレーションは不要
- ・ 世界中で発生している DDoS 攻撃の傾向を把握

アプリケーション配信+次世代型 WAF
誤検知が少なくブロッキングモードで使用可能

A10 Next-Gen WAF, Powered by Fastly



詳細を
Webで確認



誤検知を最小化

ブロッキングモードで使用可能

誤検知を最小化する実用的なソリューション

- 実環境でもフルブロッキングモードで使用でき、運用負荷を大幅に軽減
- クラウドでの情報収集・分析に加え、先進的な技術によって誤検知を最小化
- TLS オフロードや DDoS 対策などの機能も同時に提供し、ユーザ体験の向上と安全な運用環境を実現

「A10 Next-Gen WAF, Powered by Fastly」は、A10 のアプリケーション配信・負荷分散+Fastly 社の次世代型 WAF を統合したソリューションです。仮想マシンやハードウェアなど、さまざまなフォームファクタで利用可能です。誤検知を最小化する実用的なソリューションとして、Web サービスを守ります。

複数の A10 製品を一元管理するプラットフォーム

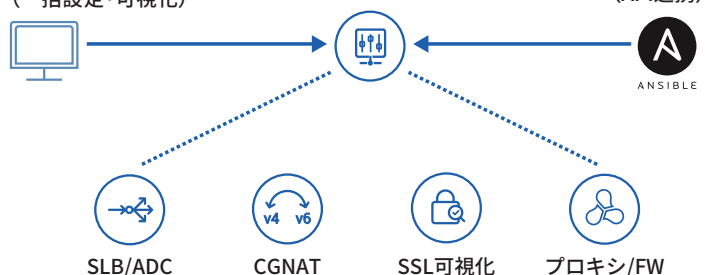
A10 Harmony Controller



詳細を
Webで確認

シングルパネルから
複数のデバイスを一元管理
(一括設定・可視化)

設定の自動化
(API連携)



LB / ADC のサービス状況を見える化

The screenshot shows the A10 Harmony Controller interface. It displays a table with columns for 'Client', 'Server', and 'Request Info'. The table contains data for a specific request, including client IP, location, device, OS, browser, server IP, server port, start/end times, request length, response code, and cache status.

Client	Server	Request Info
Client IP: 41.32.191.222	Server IP: 192.168.100.14	Request: GET /api/v1/...
Location: US	Server Port: 80	Response Code: 200
Device: UNKNOWN	Start Time at ADC: 04/09/21 02:56	Cache: hit
OS: MacOS	End Time at ADC: 04/09/21 02:56	
Browser: Safari		
Avg Transfer Rate: 0		

シングルパネルから複数のデバイスを一元管理 (一括設定・可視化)

マルチクラウド対応



データセンターやプライベートクラウド、パブリッククラウド、ハイブリッドクラウドなどのあらゆるインフラストラクチャに導入された A10 製品の一元管理、自動化、分析機能を提供します。

Thunder ADC、CGN、SSLi、CFW、A10 Defend など複数の A10 製品に対して、アプリケーションの設定やポリシー管理を実現する一元管理機能と分析機能を提供します。

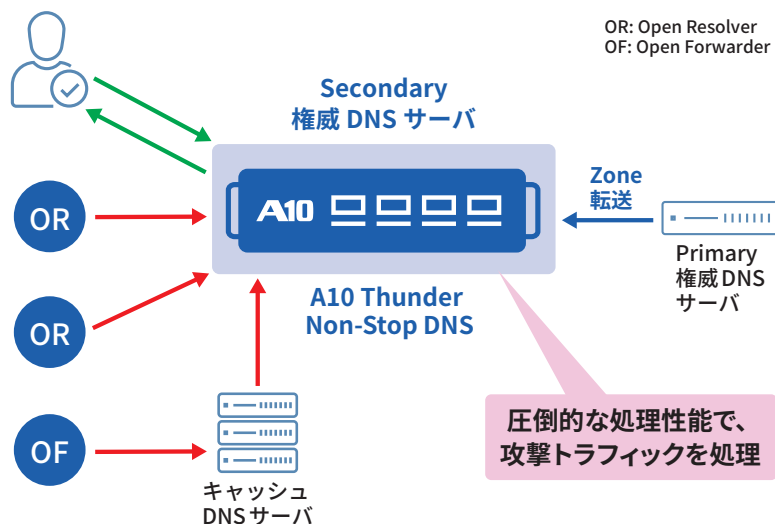
注目のソリューション

ランダムサブドメイン攻撃 (水責め攻撃) から権威 DNS サーバーを守る

Non-Stop DNS



詳細を
Webで確認



■ 既存の権威 DNS サーバの前段に Non-STOP DNS を導入

圧倒的な DNS 処理性能により、攻撃を受けても問題なく正常な DNS サービスの継続が可能

■ クライアントからの全ての DNS クエリには Non-STOP DNS が応答

既存の権威 DNS サーバはプライマリ権威 DNS サーバとして Zone 情報の管理目的で運用 (Hidden Primary DNS 構成)

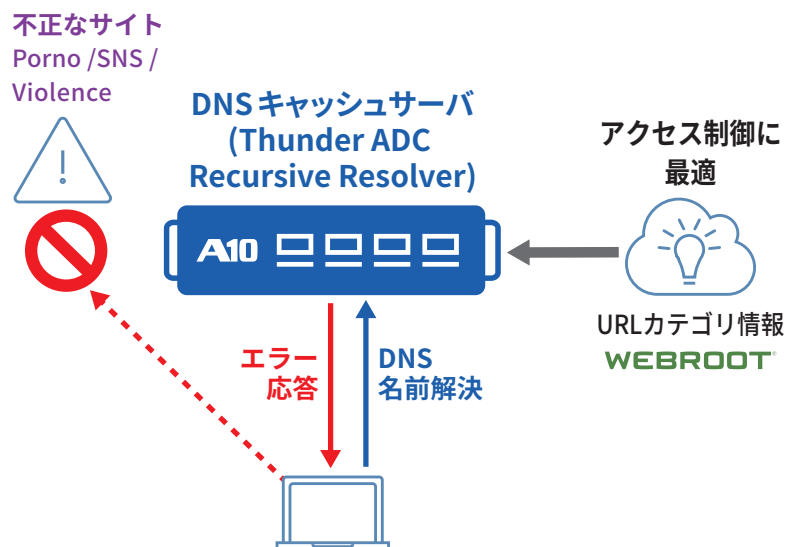
Non-stop DNS は、A10 Defend Mitigator (旧 A10 Thunder TPS シリーズ) が提供する機能で、大容量のセカンダリ権威 DNS サーバとして動作します。水責めの攻撃 (Water Torture) を受けても応答し続け、もしプライマリの権威 DNS サーバが停止しても、復旧するまでサービスを提供し続けます。

DNS を使ったセキュリティ対策を実現

DNS フィルタリング



詳細を
Webで確認



■ DNS によるアクセス制御

URL フィルタと同様のカテゴリ情報により名前解決時にアクセス制御

✓ URL フィルタと同等のアクセス制御を、よりシンプルに実現

A10 の DNS フィルタリングは、DNS ベースでアクセス制御を行う機能です。A10 が DNS サーバとして動作し、特定のカテゴリに属するサイトへのアクセスを制限します。

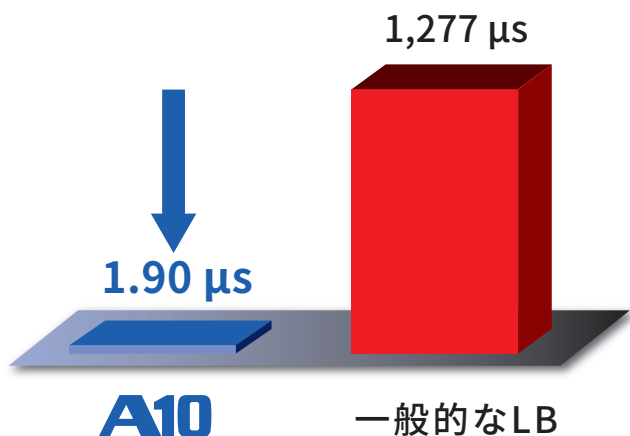
TCPトラフィックを超低遅延で負荷分散

超低遅延負荷分散



詳細を
Webで確認

一般的なLBとの遅延の比較



独自のアーキテクチャで
超低遅延を実現



A10 Thunder Ultra Low Latency モデル

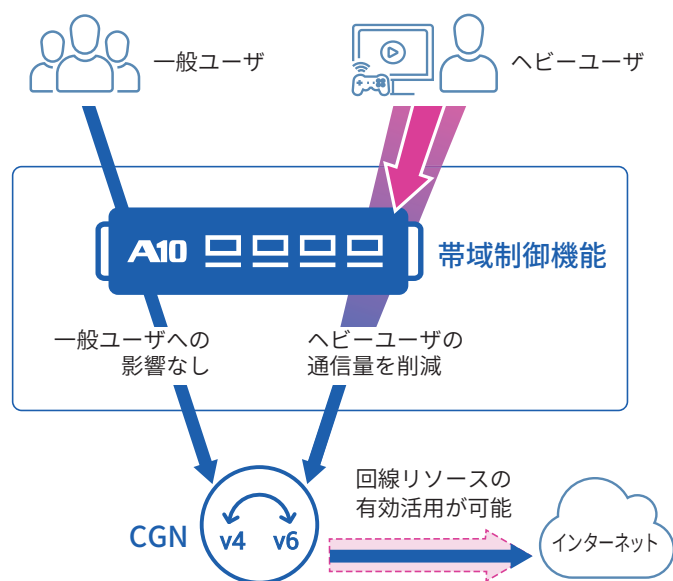
A10 Thunder Ultra Low Latency モデルは、独自のアーキテクチャにより、一般的なTCP通信を超低遅延・低ジッターでロードバランスすることができます。超高速取引などの低遅延が求められるアプリケーションにおいて高速で安定したサービスをより多く提供できるようになります。

サービス加入者間で公平な帯域利用を実現

帯域制御・公平制御



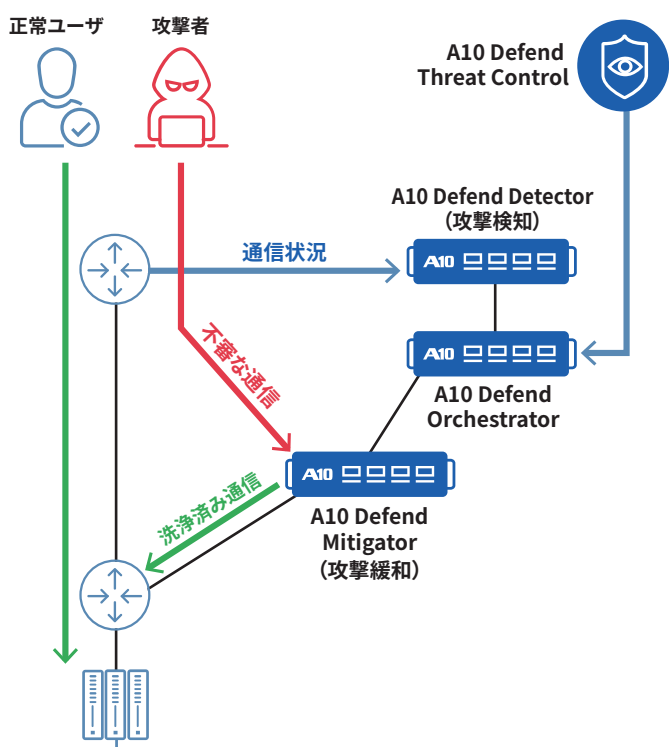
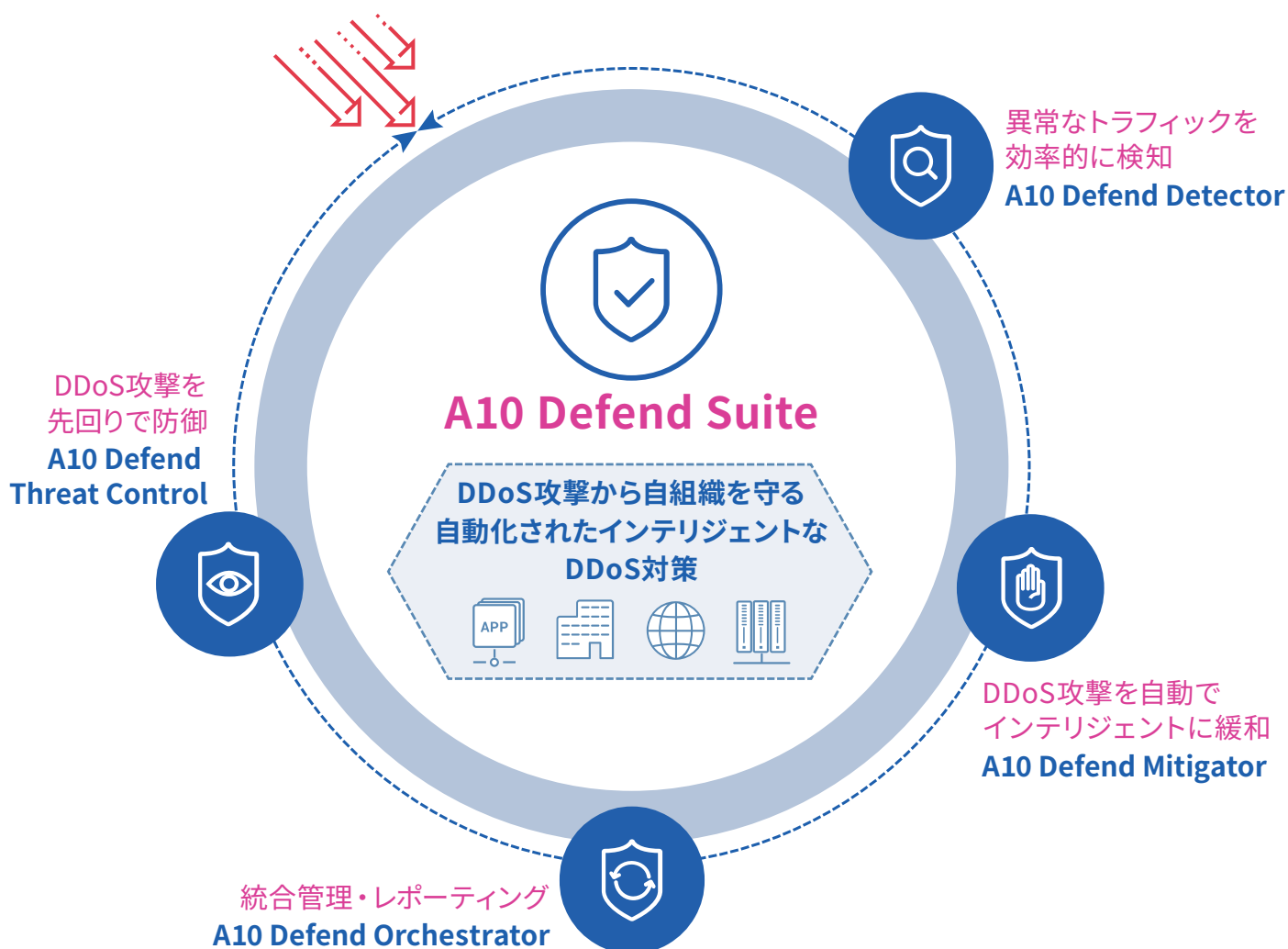
詳細を
Webで確認



- ソースIPアドレスや、アプリケーション種別に基づき、通信帯域や秒間パケット数、秒間コネクション数、同時コネクション数を制限することが可能
- ファイアウォールの一部として提供され、CGNAT・ADC機能との併用も可能
- ハードウェア、仮想、ベアメタル、コンテナなど幅広いA10 Thunderフォームファクタで利用可能

ヘビーユーザの帯域を制限することで、サービス加入者間で公平な帯域利用を実現します。グループ分けした加入者に階層的に制御をかけることも可能です。

A10 Defend Suite: DDoS攻撃対策統合ソリューション



A10 Defend Suite 活用例

A10 Defend Suite 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。

A10 Defend Mitigator :

DDoS 攻撃を緩和して、サービス停止を阻止。

A10 Defend Detector :

フローベースで DDoS 攻撃を検知。

NetFlow, sFlow, IPFIX などのフロー情報を基に攻撃を検知。

A10 Defend Orchestrator :

Detector, Mitigator による DDoS 攻撃の検知・緩和を一元管理。

Mitigator 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。

A10 Defend Threat Control :

DDoS 攻撃対策の要綱。

A10 の専門チームによる収集・調査・分析。

アタックサーフェス (攻撃対象領域) の現状把握と対策立案に。

ロバストな最初の防御層として先回り防御を実現。

脅威情報の分析・提供。

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



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



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



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



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



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

2024 年 10 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）			管理ソフトウェア
～ 20 Gbps	10 G ～ 100 Gbps	100 Gbps～	
モジュラーライセンス  Thunder 1060S 5G, 10G, 20 Gbps 7x1GC, 4x1/10GF, 2x10/25GF  Thunder 3350-E 10 Gbps 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF  Mitigator VA 1 ～ 5 Gbps  Mitigator VA for Cloud Microsoft Azure: 5 Gbps	SPE モデル  Thunder 5845 100 Gbps 48x1/10GF, 4x100GF SPE モデル  Thunder 5845-40G 40 Gbps 48x1/10GF, 4x100GF  Mitigator VA 10 ～ 100 Gbps VMware ESXi (SR-IOV) FlexPool Licensing	SPE モデル  Thunder 8665S 550 Gbps 12 x 400GF SPE モデル  Thunder 7655S 380 Gbps 16x100GF SPE モデル  Thunder 7445 220 Gbps 48x1/10GF, 4x100GF	 Orchestrator VA  Subscriber Portal VA DDoS 検知専用  Detector VA Standalone Detector 150 K – 1.5 Million fps

*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 *VA:Virtual Appliance(仮想アプライアンス)

*モジュラーライセンス:ソフトウェアとハードウェアを分離し、同一ハードウェアであっても帯域やその他のスペックによってカバーする領域を分けて提供する形態

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

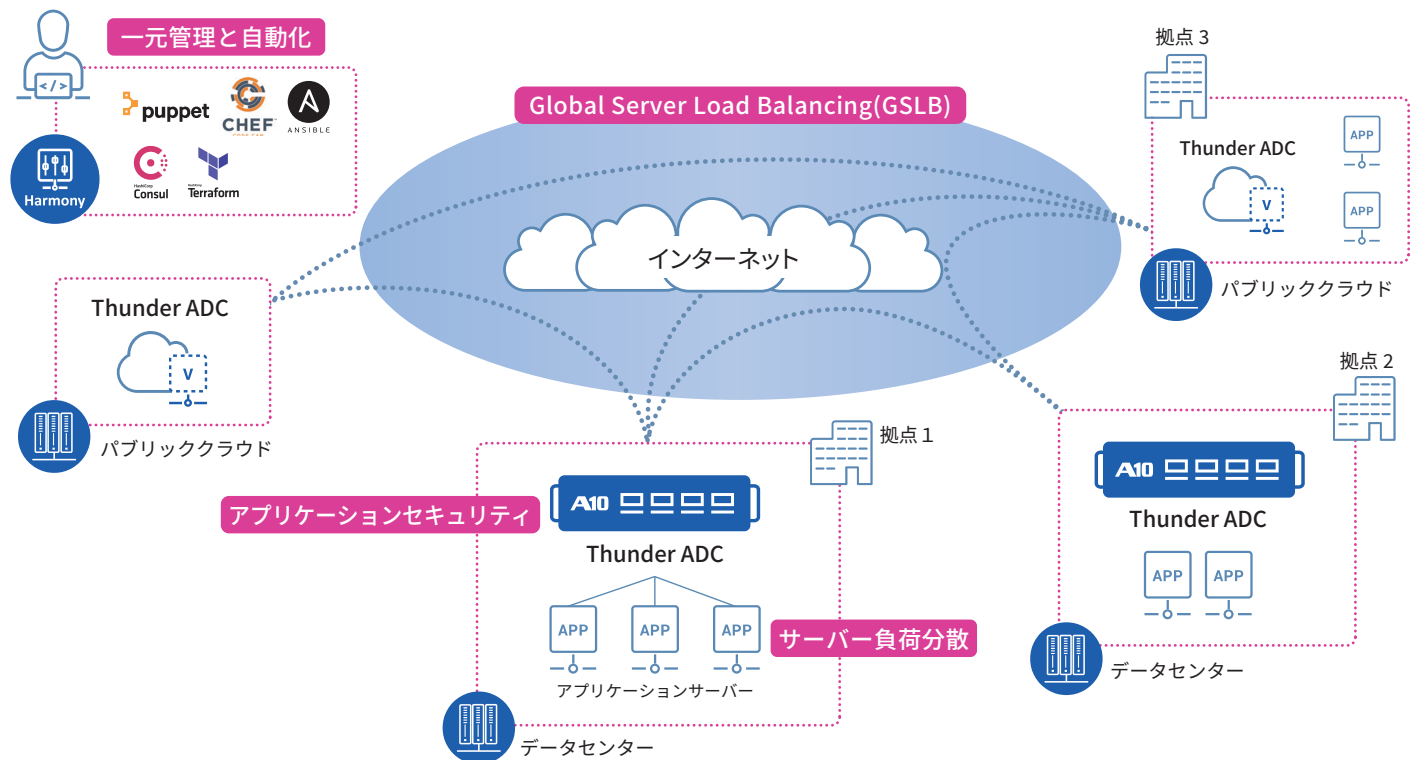


データシート



サーバー負荷分散・アプリケーション配信(ロードバランサー・ADC)

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



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

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ライゼーション、規制遵守

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

一元管理と自動化

- 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

キャッシュ DNS

- DNS フルサービスリゾルバ
- DNS ロードバランス

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と、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

2024 年 10 月現在

仮想アプライアンス	～ 25 Gbps	～ 100 Gbps	～ 200 Gbps	200 Gbps ～	超低遅延モデル
 vThunder ADC for Cloud Microsoft Azure, AWS: 最大 10 Gbps まで Oracle Cloud: 最大 24 Gbps まで	 Thunder 1060S 25 Gbps 7x1GC, 4x1/10GF, 2x10/25GF	 Thunder 4440 78 Gbps 24x1/10GF, 4x40GF	 Thunder 6440 150 Gbps 48x1/10GF, 4x40GF	 Thunder 7655S 370 Gbps 16x100GF	 Thunder 3745 4 x 10GE
 vThunder ADC 仮想アプライアンス 最大 100 Gbps まで	 Thunder 1060S 10 Gbps 7x1GC, 4x1/10GF, 2x10/25GF	 Thunder 3350S 50 Gbps 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 40 Gbps 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 30 Gbps 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF	 Thunder 5440 100 Gbps 24x1/10GF, 4x40GF		
 Thunder ADC for Bare Metal			 Thunder 6655S 185 Gbps 16x100GF		

*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

*モジュールライセンス：ソフトウェアとハードウェアを分離し、同一ハードウェアであっても帯域やその他のスペックによってカバーする領域を分けて提供する形態

最新情報または詳細は、
右記の web ページをご覧ください。

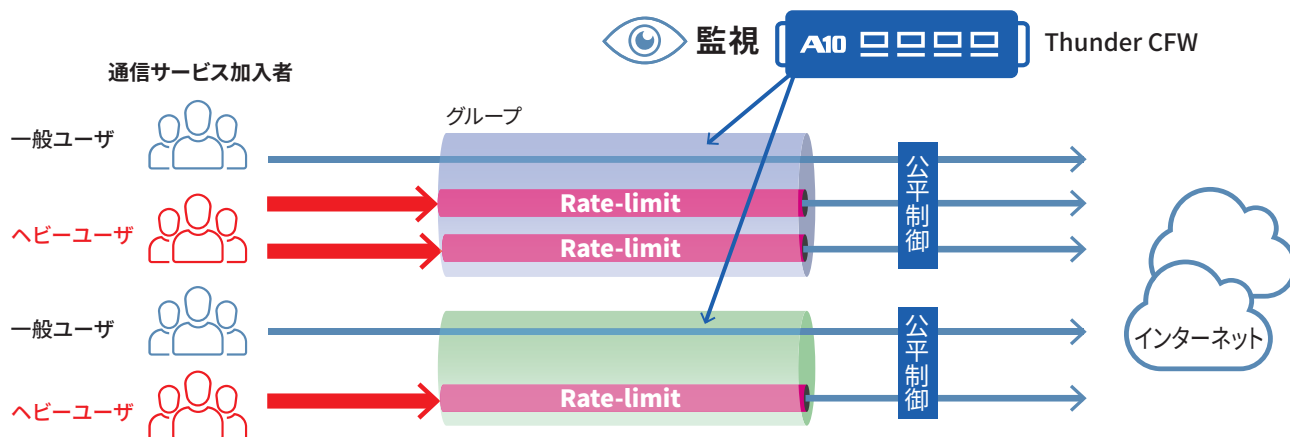
ソリューション詳細



データシート



帯域制御・公平制御

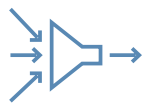


A10の帯域制御ソリューションを用いることで、ヘビーユーザーの過剰な帯域の利用を抑制することができ、公平かつ有効な通信帯域の利用を実現できます。送信元・送信先IPアドレス等や、DPIを利用して識別したアプリケーション種別を指定し、上り下りの通信帯域やコネクション数などを制限できます。

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

2024年10月現在

仮想アプライアンス	～ 100 Gbps*		～ 200 Gbps*	200 Gbps* ～
 vThunder CFW for Cloud	 Thunder 4440S 24x1/10GF, 4x40GF		 Thunder 7440 48x1/10GF, 4x40GF	 Thunder 8665S 12 x 400GF
 vThunder 仮想アプライアンス	 Thunder 5840 24x1/10GF, 4x40GF		 Thunder 7440-11 48x1/10GF, 4x100GF	
 Thunder for Container (Docker)	 Thunder 3350S 6x1GC, 2x1GF, 8x1/10GF, 4x10GF		 Thunder 6440S 48x1/10GF, 4x40GF	 Thunder 7655S 16x100GF
 ベアメタル	 Thunder 5440 24x1/10GF, 4x40GF			 Thunder 7650 16x100GF
 Thunder for Bare Metal				

* 公平制御で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。

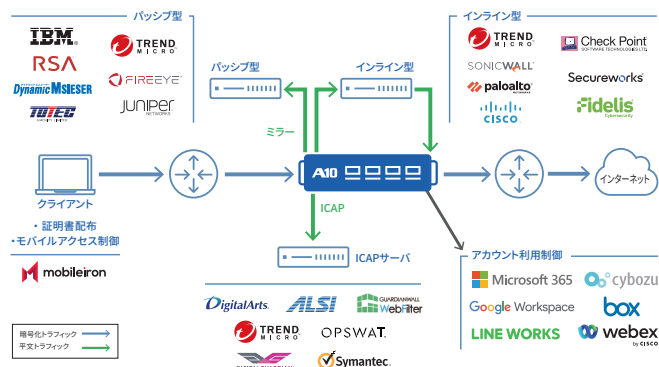
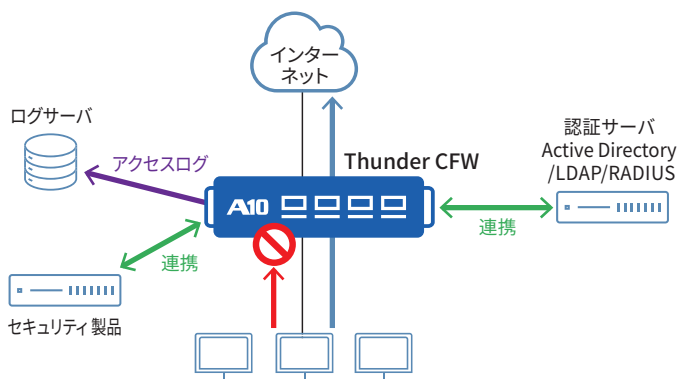
ソリューション詳細



データシート



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イ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

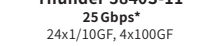


不正アクセス防止

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

2024年10月現在

～ 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～	
 Thunder 1060S 25G 2 Gbps* 7x1GC, 4x1/10GF, 2x10/25GF	 Thunder 3350 3 Gbps* 6x1GC, 2x1GF, 4x25GF, 4x40GF, 4x10GF	 Thunder 5440S 15 Gbps* 24x1/10GF, 4x40GF	 Thunder 7655S 72 Gbps* 16x100GF	 Thunder 6440S 22 Gbps* 48x1/10GF, 4x40GF
 Thunder 1060S 10G 1 Gbps* 7x1GC, 4x1/10GF, 2x10/25GF	 Thunder 3350-E 3 Gbps* 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF	 Thunder 4440S 8 Gbps* 24x1/10GF, 4x40GF	 Thunder 7440S 25 Gbps* 48x1/10GF, 4x40GF	 Thunder 5840S 25 Gbps* 24x1/10GF, 4x40GF
		 Thunder 3350S 5.5 Gbps* 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF	 Thunder 7440S-11 25 Gbps* 48x1/10GF, 4x100GF	 Thunder 5840S-11 25 Gbps* 24x1/10GF, 4x100GF

*全通信をSSL/TLS可視化した際の最大スループット *モジュラー：モジュラーライセンス。ソフトウェアとハードウェアを分離し、同一ハードウェアであっても帯域やその他のスペックによってカバーする領域を分けて提供する形態

最新情報または詳細は、
右記の web ページをご覧ください。

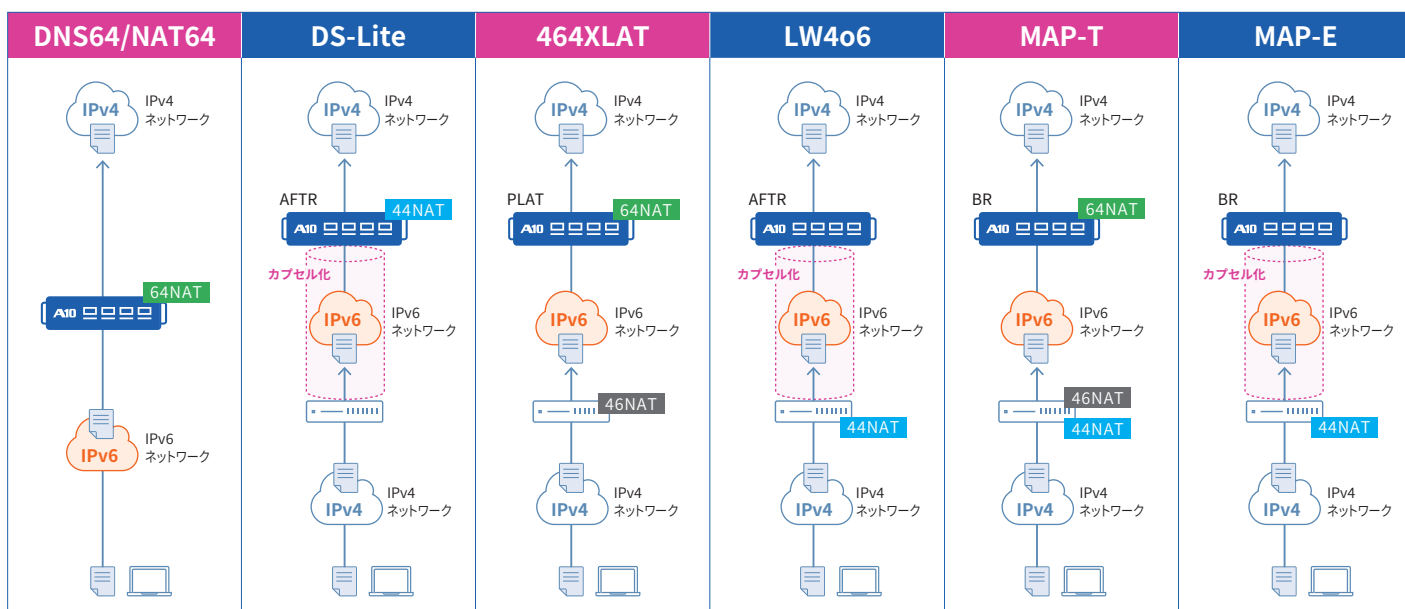
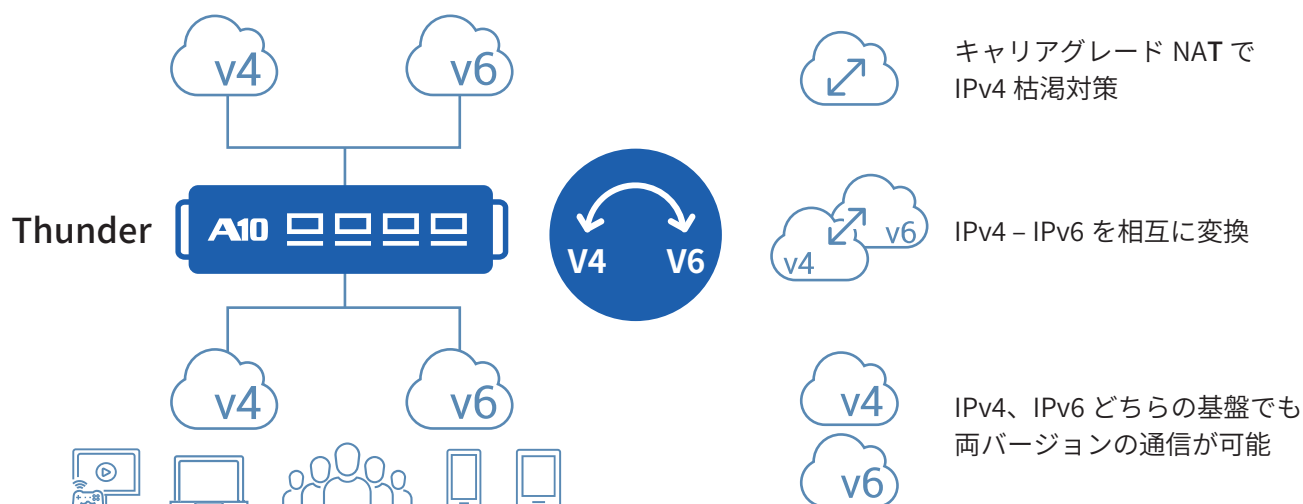
ソリューション詳細



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も、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

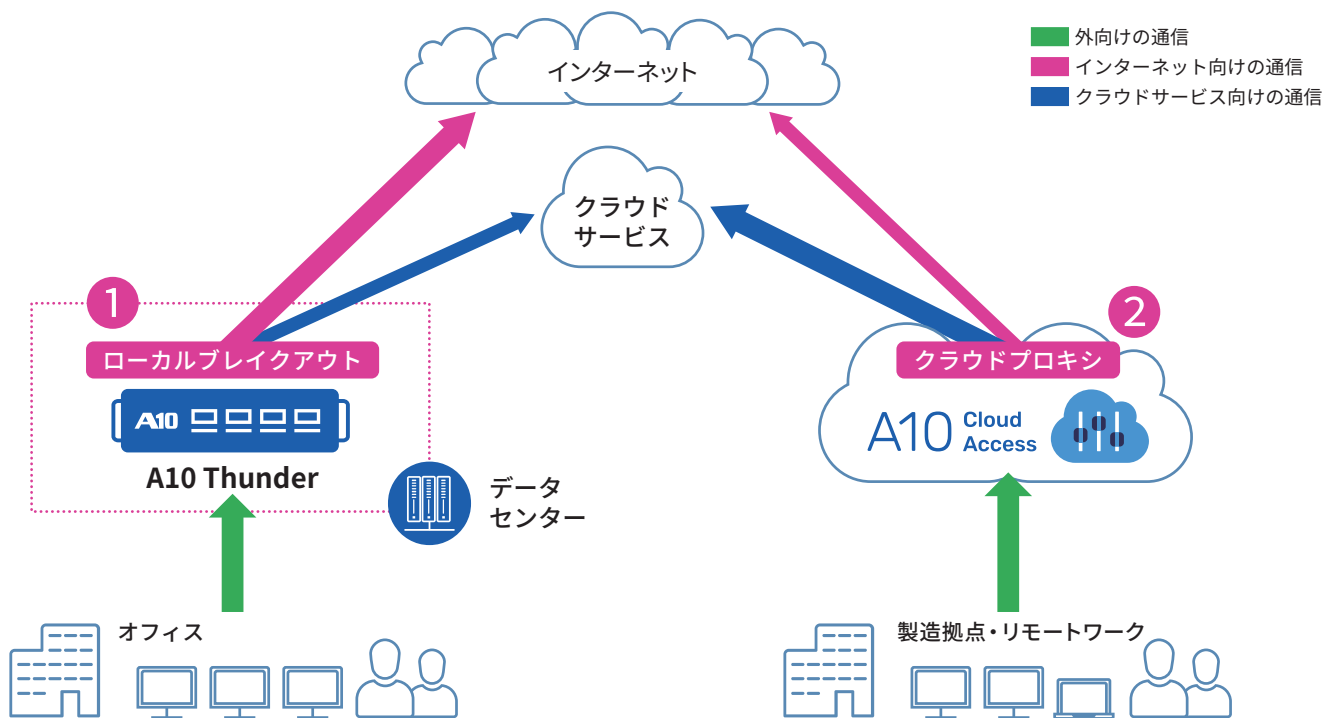
2024年10月現在

	～ 100 Gbps	～ 200 Gbps	200 Gbps ～
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 180 Gbps まで			
ベアメタル			
 Thunder CGN for Bare Metal			
	 Thunder 4440 78 Gbps 24x1/10GF, 4x40GF	 Thunder 6440 48x1/10GF, 4x40GF	 Thunder 8665S 550 Gbps 12 x 400GF
	 Thunder 3350S 50 Gbps 6x1GC, 2x1GF, 8x1/10GF, 4x10GF	 Thunder 5845 115 Gbps 48x1/10GF, 4x100GF	 Thunder 7655S 370 Gbps 16x100GF
	 Thunder 3350 40 Gbps 6x1GC, 2x1GF, 4x25GF, 4x40GF, 4x10GF	 Thunder 5840 115 Gbps 24x1/10GF, 4x40GF	 Thunder 7650 370 Gbps 16x100GF
	 Thunder 3350-E 30 Gbps 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF	 Thunder 5840-11 115 Gbps 24x1/10GF, 4x100GF	 Thunder 7445 220 Gbps 48x1/10GF, 4x100GF
		 Thunder 5440 100 Gbps 24x1/10GF, 4x40GF	 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



ローカルブレイクアウト・クラウドアクセスプロキシ



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 クラウドプロキシ (A10 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



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

2024 年 10 月現在

～ 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～	
 Thunder 1060S 25G 2 Gbps* 7x1GC, 4x1/10GF, 2x10/25GF	 Thunder 3350 3 Gbps* 6x1GC, 2x1GF, 4x25GF, 4x40GF, 4x10GF	 Thunder 5440S 15 Gbps* 24x1/10GF, 4x40GF	 Thunder 7655S 72 Gbps* 16x100GF	 Thunder 6440S 22 Gbps* 48x1/10GF, 4x40GF
 Thunder 1060S 10G 1 Gbps* 7x1GC, 4x1/10GF, 2x10/25GF	 Thunder 3350-E 3 Gbps* 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF	 Thunder 4440S 8 Gbps* 24x1/10GF, 4x40GF	 Thunder 7440S 25 Gbps* 48x1/10GF, 4x40GF	 Thunder 5840S 25 Gbps* 24x1/10GF, 4x40GF
		 Thunder 3350S 5.5 Gbps* 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF	 Thunder 7440S-11 25 Gbps* 48x1/10GF, 4x100GF	 Thunder 5840S-11 25 Gbps* 24x1/10GF, 4x100GF

*全通信をSSL/TLS可視化した際の最大スループット *モジュラー：モジュラーライセンス。ソフトウェアとハードウェアを分離し、同一ハードウェアであっても帯域やその他のスペックによってカバーする領域を分けて提供する形態

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



2024 年 10 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：50 クライアント
(最小利用：50 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

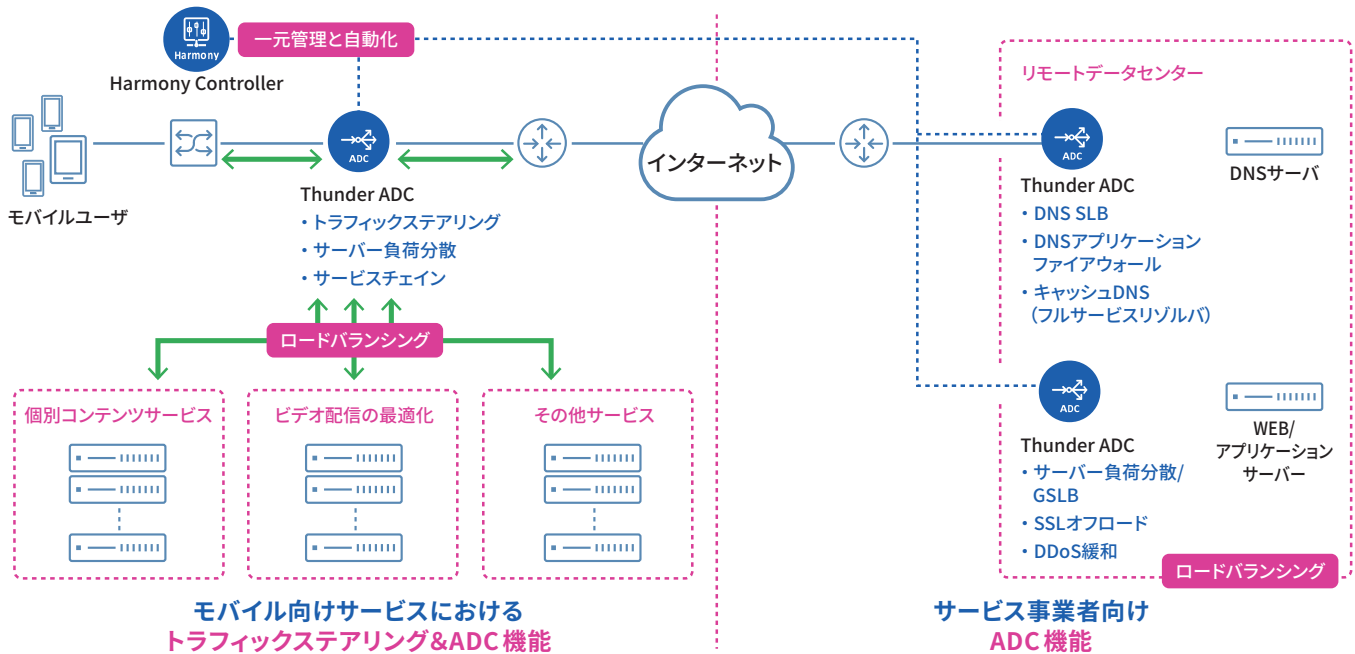
- (ログは Web API 経由で取得可能)

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				○
Client-to-Site IPsec VPN による接続				○

導入例

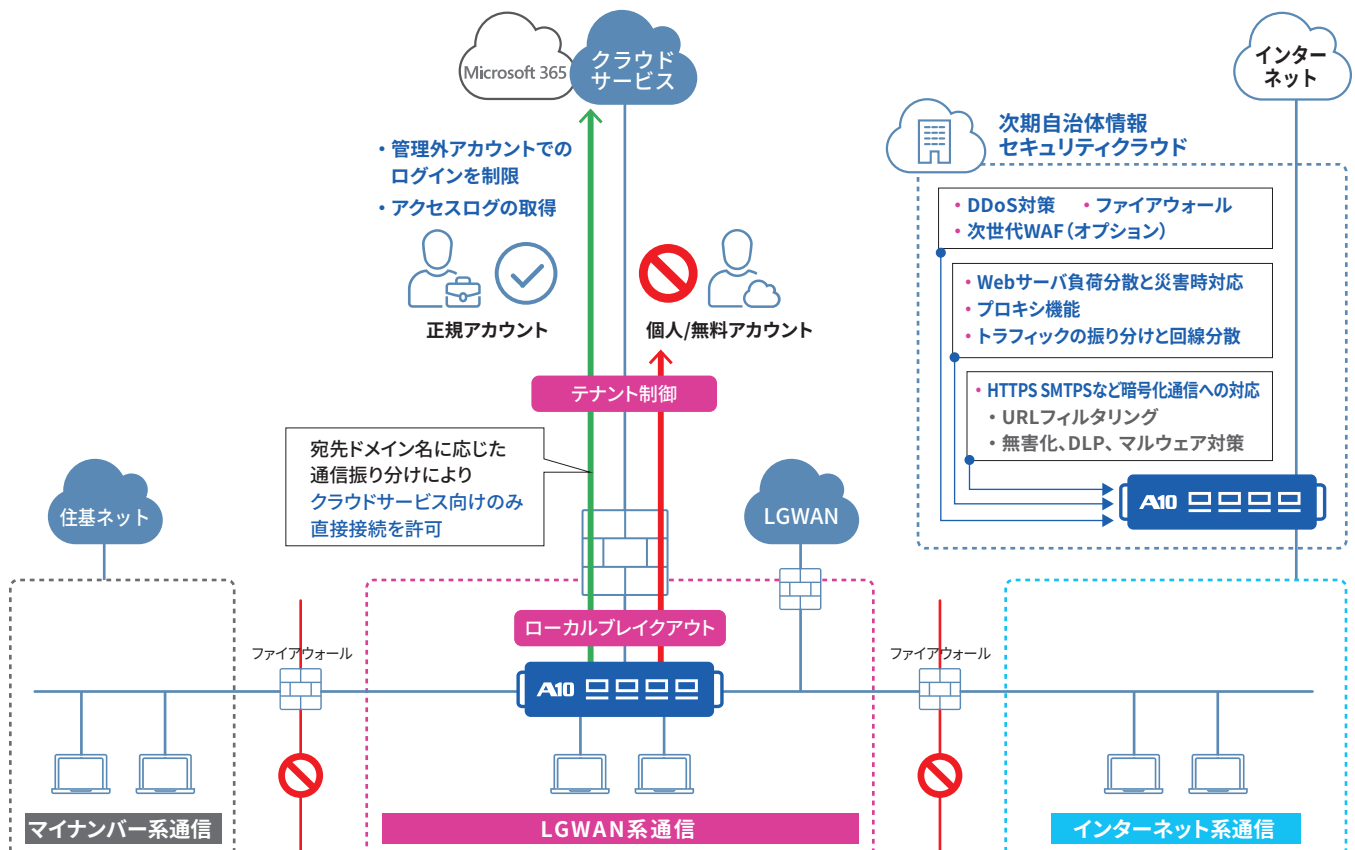
Web 事業者

マルチクラウドでのアプリケーション配信の最適化とセキュリティ強化・運用の効率化により、高品質・高信頼のWeb サービスを実現



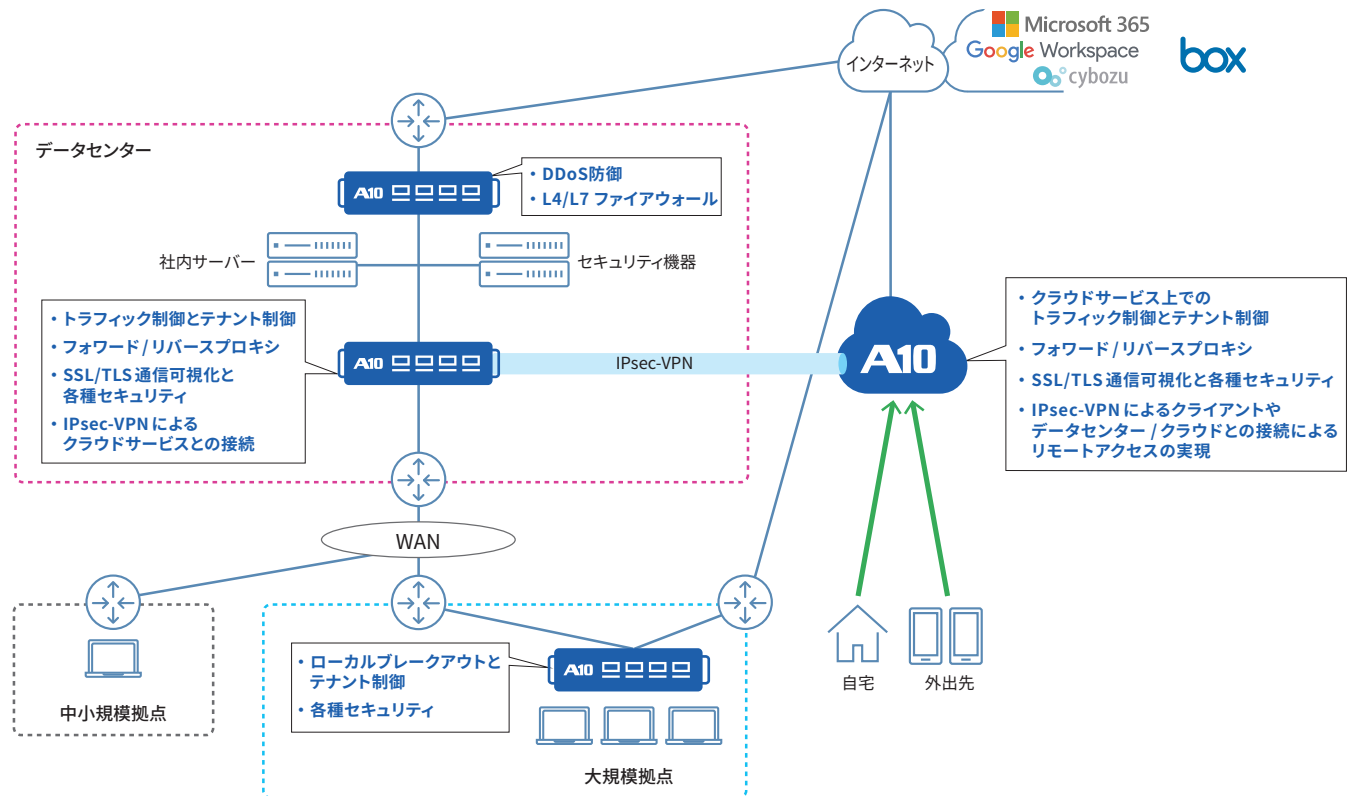
自治体

α'モデルに対応。LGWAN系端末からMicrosoft 365等の特定通信を接続可能にするローカルブレイクアウトとテナント制御を提供



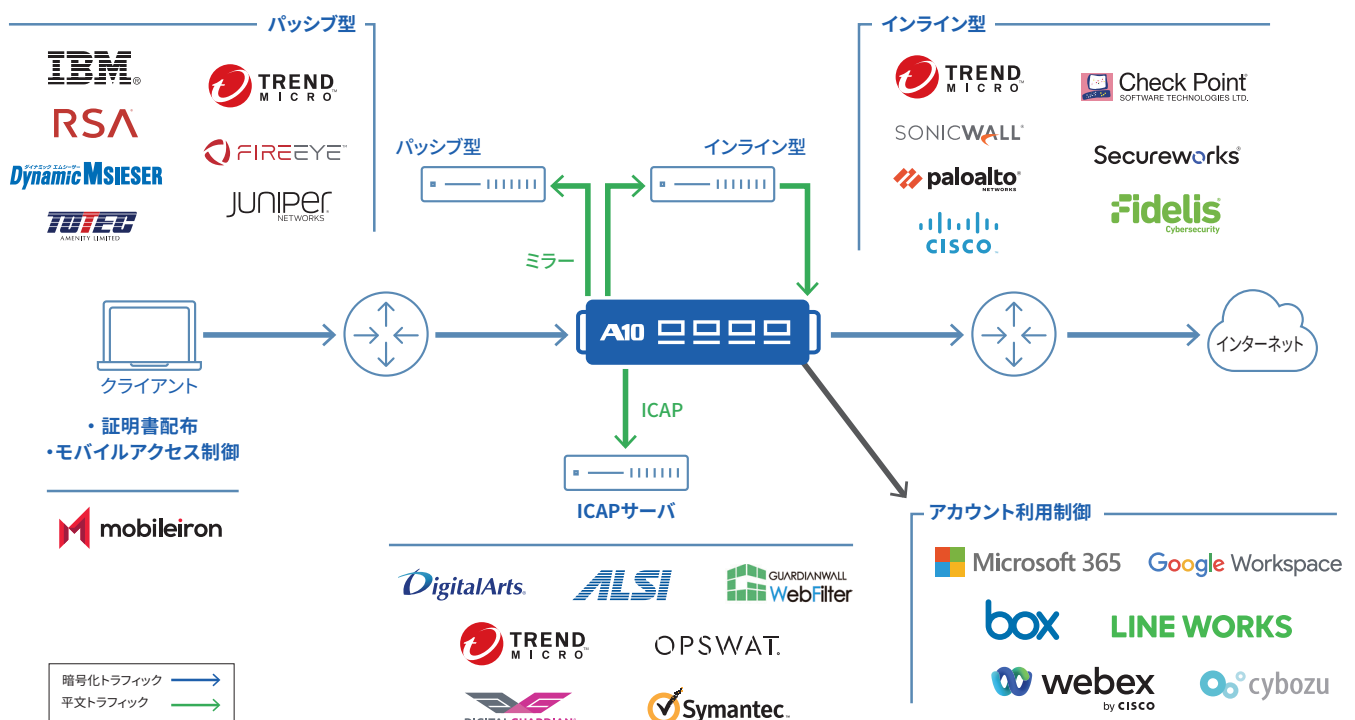
エンタープライズネットワーク向けソリューションマップ

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

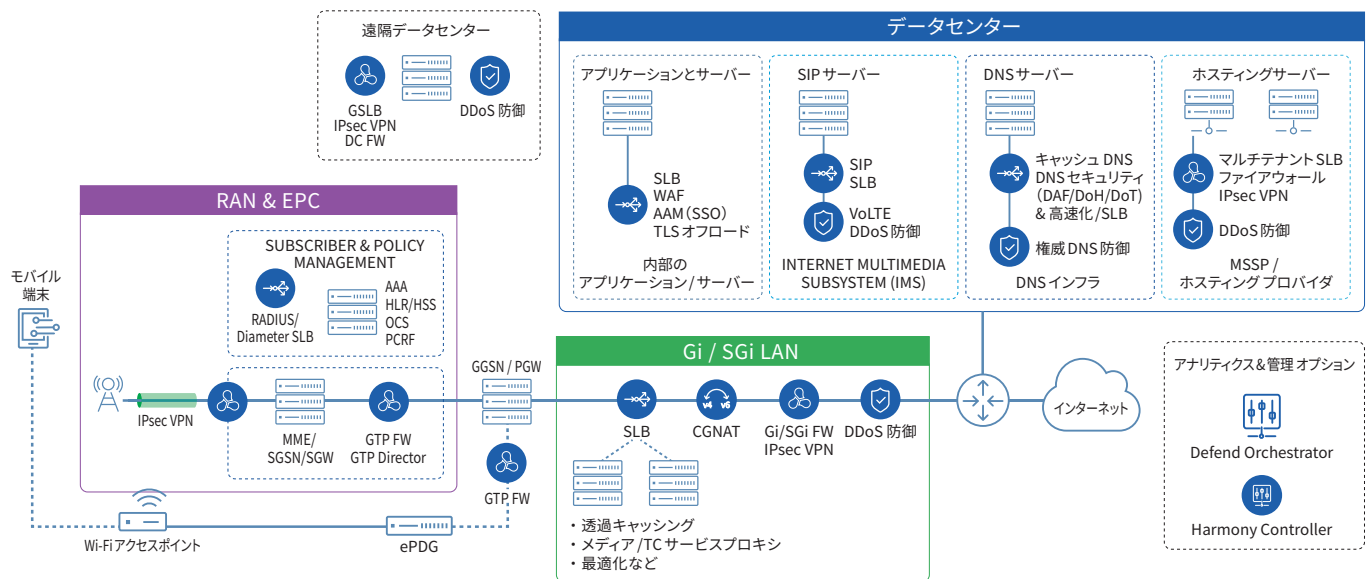


SSL/TLS 通信可視化と連携ソリューション

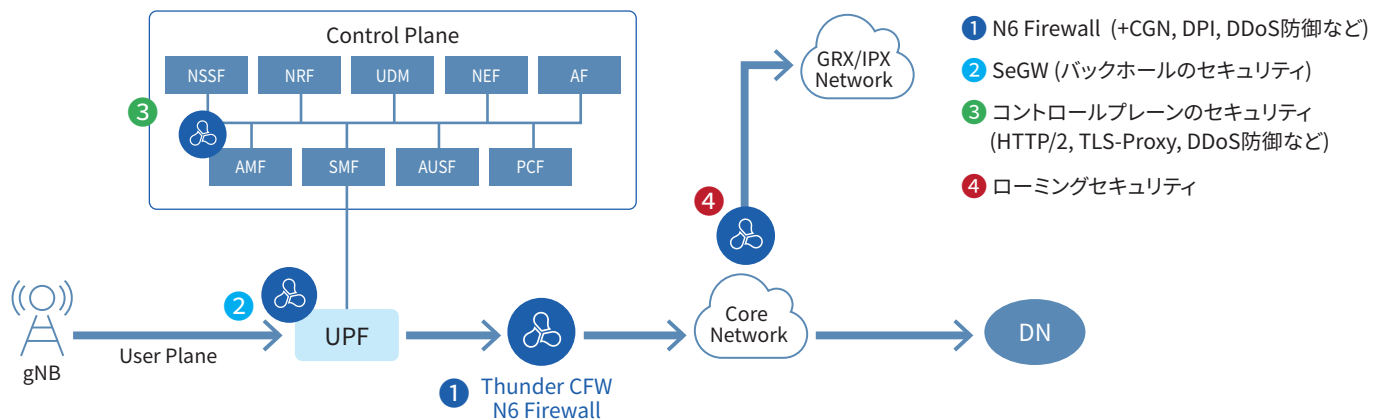
SSL/TLS 通信を高速に復号し多様なセキュリティ製品と連携、暗号化通信に隠れた脅威を検知し防御



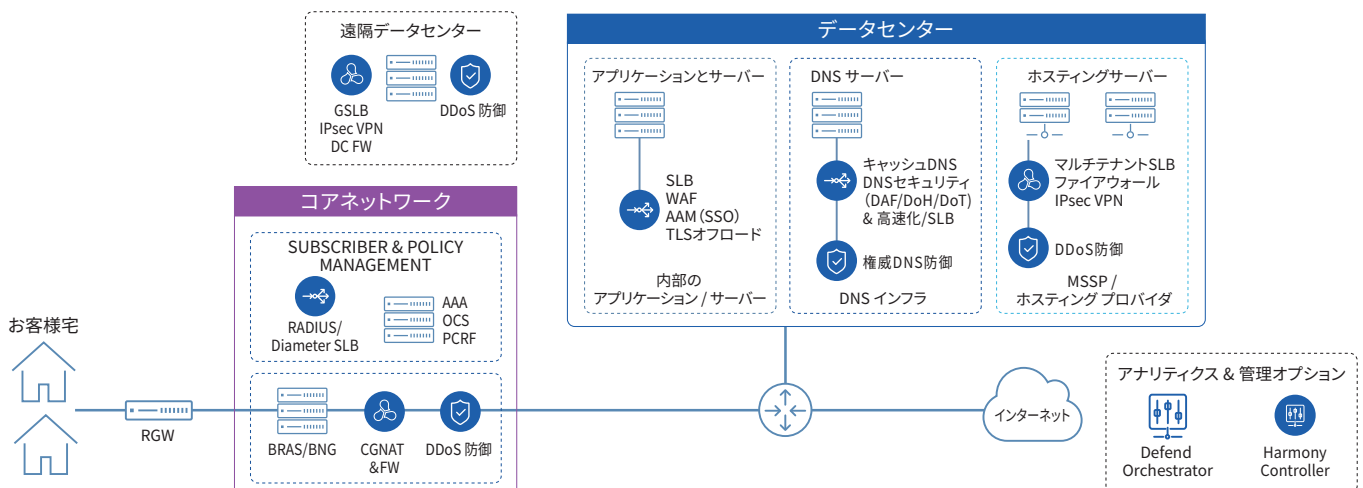
モバイル事業者様向けソリューションマップ（LTE/5G-NSA 向け）



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

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

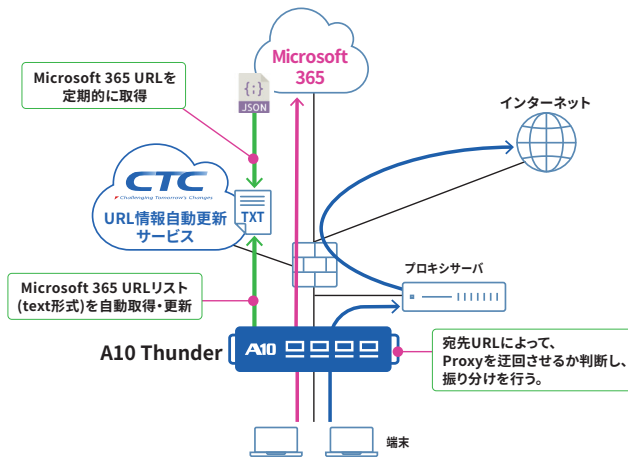
Microsoft 365 を利用する企業が増加しています。Microsoft 365 の利用を開始すると、Proxy サーバに対するアクセスが増加し負荷が高くなり、Proxy サーバのパフォーマンス不足の問題が発生します。

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/



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

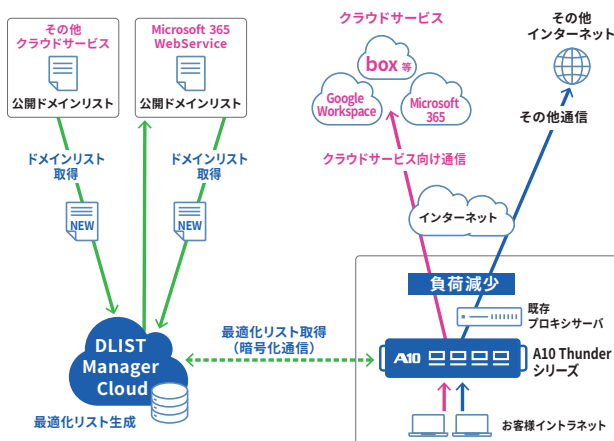
本サービスは、A10 製品を新規または更新でご導入頂く際には無償でバンドルしてご提供しており、Microsoft 365をはじめ、Windows Update や複数のクラウドサービス (Box、Google Workspace、Webex Meetings、Zoom) の公開ドメインリスト情報を自動で取得し A10 に適用することで、常に最新のリスト情報で A10 の振り分けが可能となります。

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。

お問合せ： 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

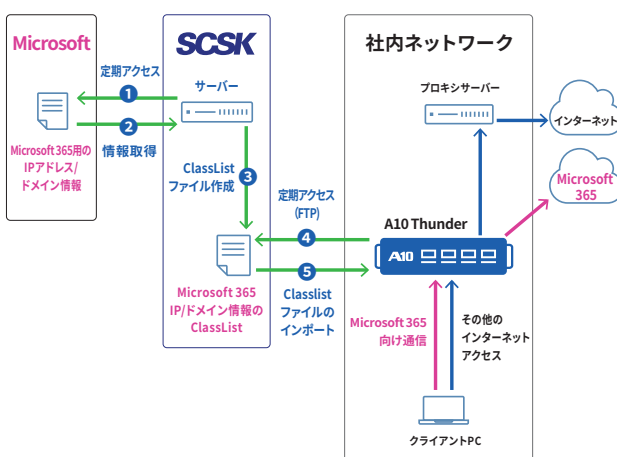
Microsoft 365 の IP/ドメイン情報は定期的に変更されることがあり、その都度設定を変更する必要があります。本ソリューションは、最新の IP/ドメイン情報を SCSK が提供することで、運用の手間を軽減する無償のソリューションです。SCSK が Microsoft 365 や関連サービスで利用される最新の IP/ドメイン情報を Microsoft より取得し、Classlist ファイルを生成します。

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。

お問合せ： 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



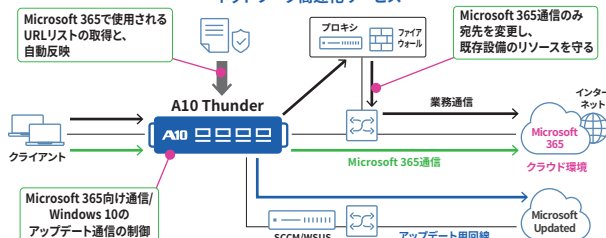
パートナーソリューション

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	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	Microsoft 365 ニュース
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	クラウドバックアップ サービス	Microsoft 365 エンドユーザー 教育サービス
金庫室3重検知 ソリューション		暗号化アドレス帳	メールアーカイブ サービス
		暗号化PCセキュリティサービス	
		暗号化の様々な業務を デジタル(AI)で支援	
導入	コンサルティング	Microsoft 365ライセンス	設計・構築

ネットワーク高速化サービス



日本電気株式会社

Microsoft 365 をより快適にするサービス「NEC 365」

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。

お問合せ: 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出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。*メール通知機能は、2024 年夏稼働予定。

お問合せ: 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

お問合せ: 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/>

NEC ネットズエスアイ株式会社

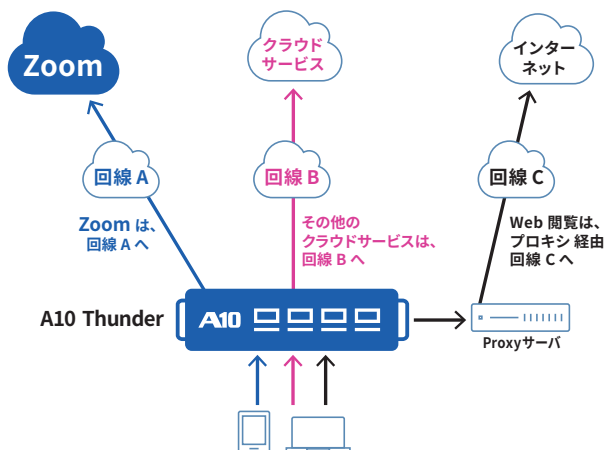
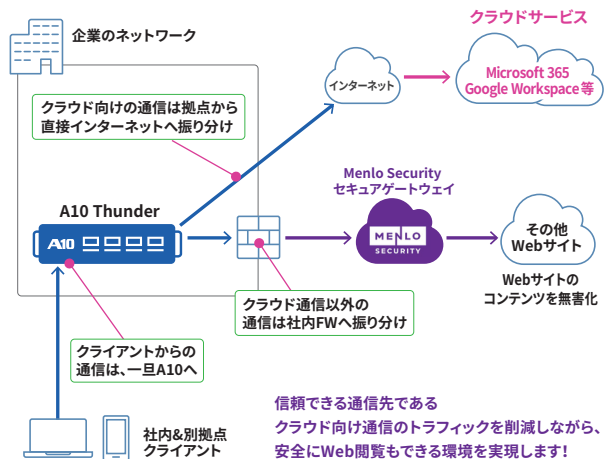
コミュニケーションサービスの音声や映像品質用の通信帯域維持を実現

Zoom トラフィック最適化ソリューション

音声 / ビデオ会議通信システムの提供で多くの実績を持つ NEC ネットズエスアイが提供する「Zoom トラフィック最適化ソリューション」は、インターネットアクセスの増加による通信回線ひっ迫の課題を解決し、Zoom の高い映像・音声コミュニケーション品質を維持することが可能なソリューションです。

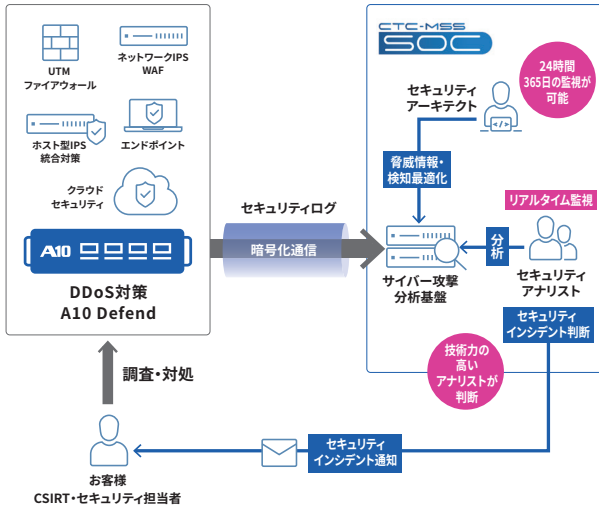
共創ワークソリューション Zoom と、A10 Thunder シリーズが提供するクラウドプロキシソリューションの組み合わせにより、Zoom の通信を帯域に余裕がある回線に振り分けたり、プロキシサーバーを迂回させたりすることで、より一層安定した映像・音声環境を提供します。

お問合せ: デジタルソリューション事業本部 オフィスソリューション事業部
マネージドセキュリティサービス部
a10-info@ml.nesic.com



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

A10 Defend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 Defend

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 Defend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。

A10 Defend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 Defend」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/

富士通ネットワークソリューションズ株式会社

不正通信の検知・遮断を自動化による安全な業務環境を実現

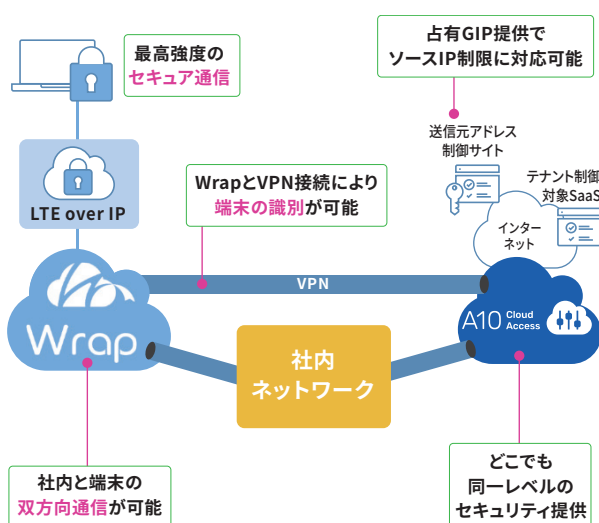
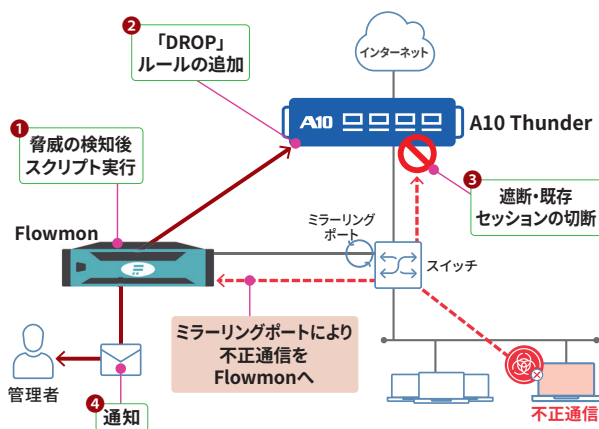
高度なサイバー攻撃に対応するNDRソリューション

サイバー攻撃は日々巧妙化しており、従来のセキュリティ対策だけでは不十分と言われています。また、攻撃を検知しても即座に対応できず、時間が経てば経つほど被害規模や深刻度が増していくため、早期発見・対応が必要とされています。

本ソリューションは、ネットワークトラフィックの可視化情報を元にA10製品が不正通信を自動でブロックします。自動ブロックを実施することで、万が一、マルウェアが侵入したとしても被害を最小限に留めることが可能です。また、運用サービスと合わせることで、監視・脅威の分析・改善対処まで一貫してお客様の運用をサポートすることも可能です。

お問合せ：

総合受付窓口：0120-20-7430 | <https://www.fujitsu.com/jp/group/fnets/contact/>



ユニアデックス株式会社

持ち出しPCにも社内と同じアクセス制御とセキュリティ

Wrap + A10 Cloud Access Controller

Wrap (ラップ) は、「モノ」「ヒト」「コト」をシームレスにつなぐために必要な全てを『ラッピングして』お届けする、ユニアデックスのクラウド型ネットワークサービスです。LTE over IP によるプライベートLTEを利用して、どこにいてもセキュアに企業ネットワークを利用することが可能です。

また、A10 Cloud Access ControllerをWrapと組み合わせることによって相乗効果を発揮します。Wrapによって常時安全にA10 CACと接続することで、持ち出しPCに対しても、いつでも、どこでも、社内にいるときと同じようにアクセス制御・セキュリティ機能を施すことができます。

お問合せ：TEL：03-5546-4900 (大代表)

promo_m@ml.uniadex.co.jp

Webサイト: <https://www.uniadex.co.jp/service/product/wrap.html>

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) 2024 年 11 月現在

■ 通信事業者

KDDI 株式会社
ソフトバンク株式会社
株式会社石川コンピュータ・センター
株式会社倉敷ケーブルテレビ
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 ぶらら
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
SCSK 株式会社
株式会社シナジー

■ 教育

福岡大学
琉球大学
群馬大学
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

鹿児島市	山口県
大分県	足利市
甲州市	北本市
三原市	岐阜市
竹富町	由利本荘市
有田市	鳥取市
輪島市	南アルプス市
名古屋市	日野市
舞鶴市	十津川村
長崎県	志免町
八代市	

■ 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/handson/handson.html>



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/>



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 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けており、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。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](https://www.a10networks.co.jp/contact)

A10 ネットワークス株式会社

www.a10networks.co.jp

©2024 A10 Networks, Inc. All rights reserved. A10 ロゴ、A10 Networks は米国およびその他の国における 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 NOV 2024