A10

A10 ネットワークス

総合カタログ

安全で可用性が高いミッションクリティカルなネットワークを実現
お客様のビジネスの成功を強くサポートします

A10 ネットワークスは、お客様のサービスが常に「最も安全でいつでも利用可能なデジタルエクスペリエンス」を提供することができるように、全力で支援いたします。

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す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。

A10 の注力分野

将来につなげるインフラ

- オンプレミス
- プライベートクラウド
- パブリッククラウド
  すべてをサポート

サイバーセキュリティ

- 重要なサービスを守る
  能動的サイバーセキュリティ

AI

- 生成 AI に対する脅威対策
- AI を悪用した脅威からの防御
- AI による障害の予兆検知と
  対策提案

A10 が提供するソリューション

A10 Control 詳しくは ▶ P5

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

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

ACOS (Advanced Core Operating System) 詳しくは ▶ P3

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、7,700 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)

詳細をWebで確認

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 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
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

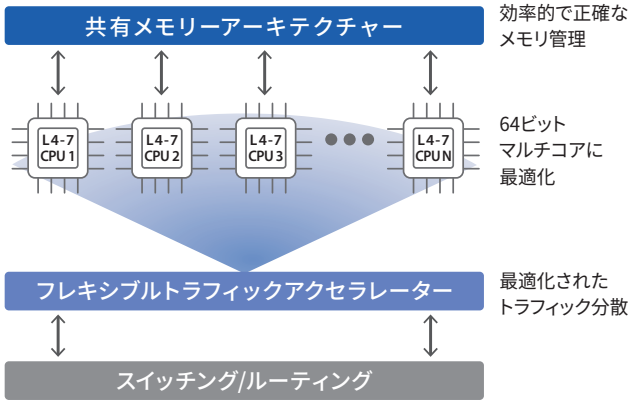
ヤフー株式会社
エキサイト株式会社

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

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

提供形態

ACOS は 多様なフォームファクタ に対して同一機能 を提供することができ、ユーザの導入コスト・学習コスト・運用コストを削減できます。

製品ラインナップ別プラットフォーム対応表はこちら

CLI / GUI / REST API での共通の操作・管理

仮想

独立したインスタンス
・KVM　・VMware ESXi

ベアメタル

最適なパフォーマンス

コンテナ

クラウドネイティブ
・Docker

クラウド

クラウドインスタンス
・AWS　・Google Cloud
・Microsoft Azure
・Oracle Cloud

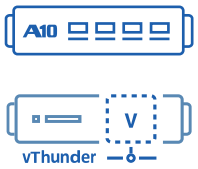
アプライアンス

ハイパフォーマンス

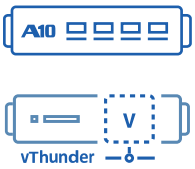
ライセンス体系

A10 製品のライセンスは、ユーザの将来のビジネス展開に対応可能な、様々なライセンス体系を提供しています。ランニングコストを抑える「買い切り型」、イニシャルコストを抑える「サブスクリプション型」、同一ハードウェアでモデルやサポート帯域を切り替えられる「モジュラー型」、帯域プールから必要に応じて払い出し可能な「帯域プール型」のライセンス形態があります。

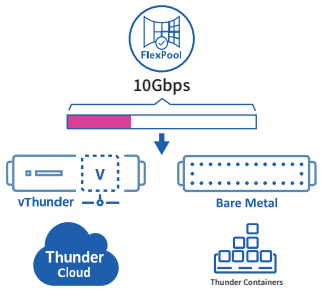
買い切り型



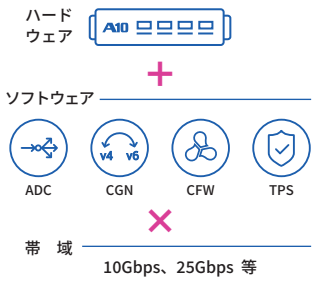
サブスクリプション型



帯域プール型



モジュラー型



金融

シンプレクス株式会社
株式会社保険見直し本舗

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

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

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

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

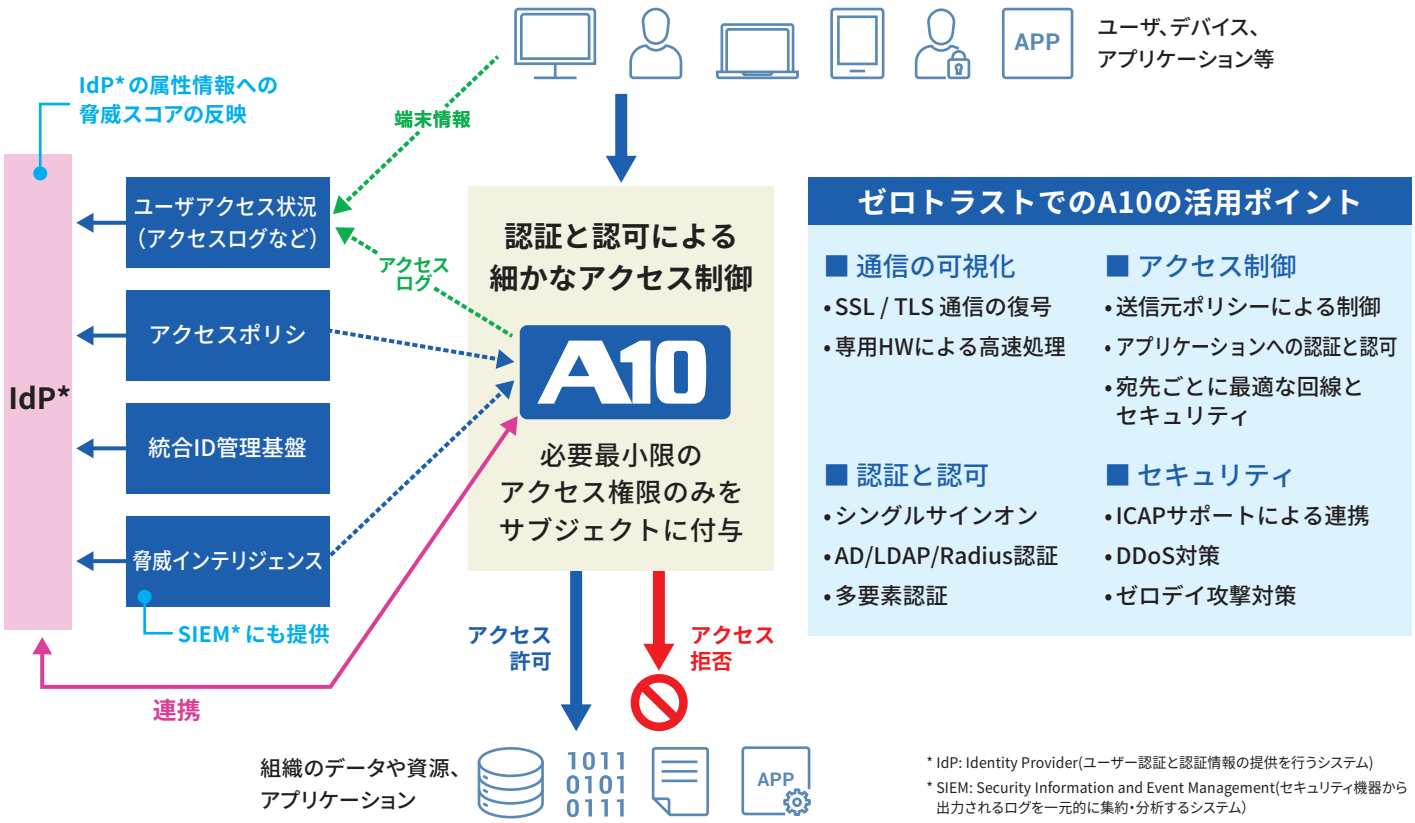
2025 年 6 月現在

ゼロトラストの実現を支えるA10のソリューション

ハイブリッド環境でのゼロトラストソリューション

詳細をWebで確認

デジタル技術の急速な進歩に伴い、従来の境界型セキュリティモデルのみでは現代のサイバー脅威に対応しきれなくなっています。
そこで注目を集めているのが「ゼロトラストセキュリティ」です。
多くの企業がSASEやSSEの採用によってこれを実現しようとしていますが、これらは「境界防御」をクラウドに押し上げただけであり、本質的な「ゼロトラスト」の役割を果たせていません。ゼロトラストはセキュリティ戦略であり、単一のソリューションで解決できるものではありません。企業全体のセキュリティを考慮し、既存のインフラと新しいアプローチを適切に組み合わせることが重要です。
A10ネットワークスは、ゼロトラストアーキテクチャを実現するための包括的なネットワークソリューションを提供しています。



ゼロトラストでのA10の活用ポイント

■ 通信の可視化
- SSL / TLS 通信の復号
- 専用HWによる高速処理

■ アクセス制御
- 送信元ポリシーによる制御
- アプリケーションへの認証と認可
- 宛先ごとに最適な回線とセキュリティ

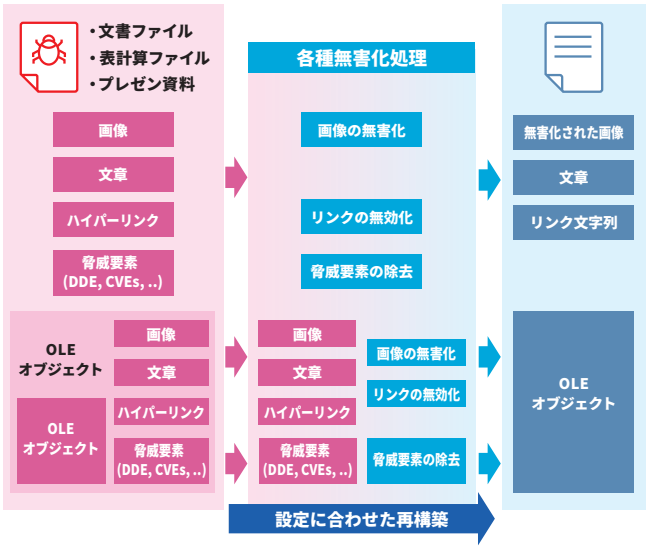
■ 認証と認可
- シングルサインオン
- AD/LDAP/Radius認証
- 多要素認証

■ セキュリティ
- ICAPサポートによる連携
- DDoS対策
- ゼロデイ攻撃対策

* IdP: Identity Provider(ユーザー認証と認証情報の提供を行うシステム)
* SIEM: Security Information and Event Management(セキュリティ機器から出力されるログを一元的に集約・分析するシステム)

暗号化通信も可視化し、脅威を確実に除去
無害化ソリューション

詳細をWebで確認



A10のSSL可視化技術とOPSWATのファイル無害化(MetaDefender)を組み合わせることで、ファイルから潜在的な脅威(マルウェアなど)を除去し、元のファイル形式で利用できるように再構築します。
A10の高速なSSL/TLS可視化技術により、暗号化されたファイルであっても、安全に閲覧可能です。

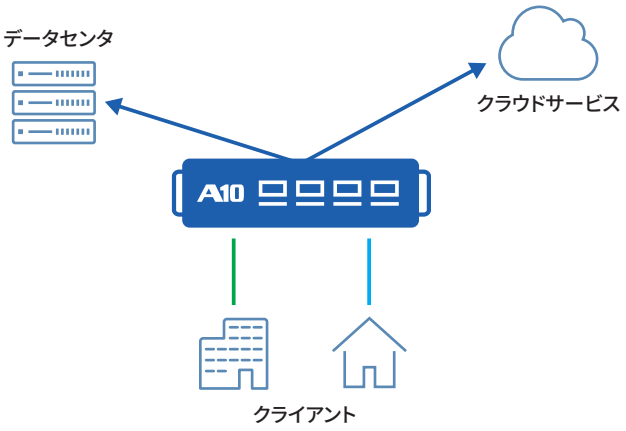
SSL可視化: 専用ハードウェアで高速に暗号通信を復号、再暗号化
Deep CDR: ファイル形式を変更せずにコンテンツを無害化

- 180種類以上の一般的なファイル形式に対応(MS-Excel, Word等)
- 検知回避型マルウェアや既知・未知の脅威を除去
- 機密情報やファイルの脆弱性など、電子ファイル内に潜む様々な脅威に対応

快適で安全なクラウドサービス活用のためのネットワーク

ローカルブレイクアウト（クラウドアクセスプロキシ）

詳細をWebで確認



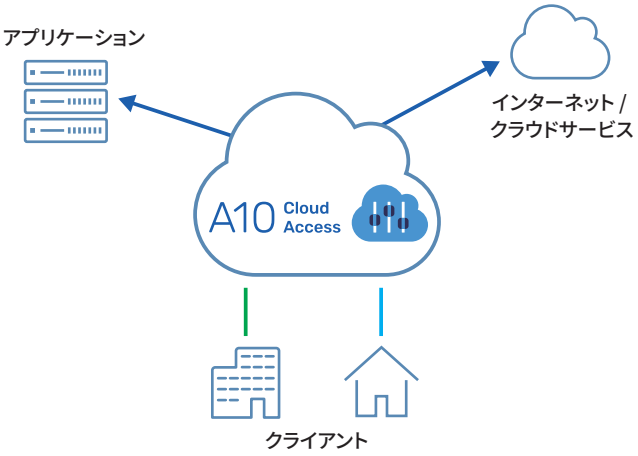
特定のクラウドサービスへの通信を自動で判別して、本社やデータセンターを経由せずに、拠点やリモートサイトから直接インターネットにアクセスできるようにするソリューションです。
クラウドサービスの利用増に伴うネットワーク・プロキシの負荷軽減や、自治体や医療機関・金融機関などで利用される閉域網から、特定の宛先向け通信だけを許可するなどの制御を可能にします。

- 宛先ドメイン名による正確な振り分け
- Microsoft 365 や Google Workspace など各種サービスに対応
- 個人アカウント利用の制限機能
- 10万クライアント以上でも利用可能な高い性能
- 国内数百社以上の商用実績

アプリケーションやインターネット向けのアクセスを制御・管理できる A10 のクラウドサービス

Cloud Access Controller

詳細をWebで確認



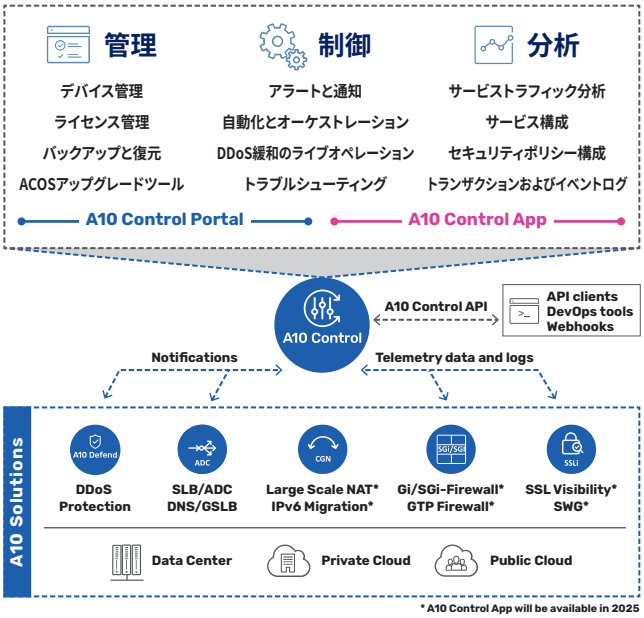
Cloud Access Controller は、組織のセキュリティポリシーに基づき、ユーザー単位でアプリケーションやインターネット向けの通信を制御・管理できるクラウドサービスです。
オンプレミスの A10 Thunder シリーズとの併用で、一貫したセキュリティポリシーを提供するハイブリット構成も可能です。

- 認証・認可によるユーザー毎のアクセス制御
- 接続元・接続先に応じた適切なトラフィックの振り分け
- 特定アプリ向けの通信と外部向け通信を同時に制御可能
- URL フィルタリングなどの各種セキュリティ機能を提供
- セキュアな IPsec による VPN 機能をサポート
- 手軽に導入できる SaaS 型サービス
- アクセス状況を監視できるログを提供

A10 製品の一元管理とトラフィック可視化

A10 Control

詳細をWebで確認



A10 Control は、A10 ソリューション向けの次世代統合管理・分析プラットフォームです。オンプレミス、クラウド、ハイブリッドなど多様な環境に分散した A10 製品を一元管理し、アプリケーションやサービストラフィックの可視化・分析を実現します。これにより、迅速なキャパシティプランニングやスケーリング対応が可能となり、運用効率とセキュリティの向上に貢献します。

- 多拠点・マルチクラウド環境に分散した A10 デバイスを一元管理し、運用負荷を大幅に軽減
- アプリケーションやサービスのトラフィックを収集・分析・可視化し、異常検知やトラブルシューティングを効率化

AI時代のサイバー攻撃から自社ネットワークとサービスを守る

サイバー攻撃の手口は巧妙化の一途を辿り、特にAI技術を悪用した新たな脅威も出現しています。
このような状況下で、自社のWebサイトをいかにして守り抜くかが、企業にとって喫緊の課題となっています。
A10 Defendは、システムやサーバーを狙うDDoS攻撃だけでなくアプリやAPIへを狙う巧妙な攻撃を包括的に防御するセキュリティソリューションです。オンプレミスでもクラウドでも使用可能で、フルマネージドのSOCサービスも利用できます。

詳細をWebで確認

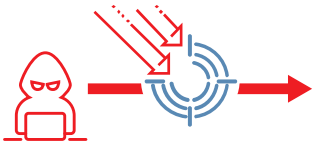
A10 Defend

Webアプリへの攻撃

AIによる攻撃の進化

DDoS 攻撃

システム、サーバへの攻撃
ネットワーク層を利用した攻撃



AIによる攻撃の進化

A10 Defend Next-Gen WAF
次世代WAF
詳しくは▶P7

ThreatX by A10 Networks
WAAP・API防御
詳しくは▶P6

A10 Defend Threat Control
DDoS脅威情報
詳しくは▶P8

A10 Defend DDoS Mitigator
DDoS緩和装置
詳しくは▶P8

A10 Defend DDoS Detector
DDoS検知装置
詳しくは▶P8

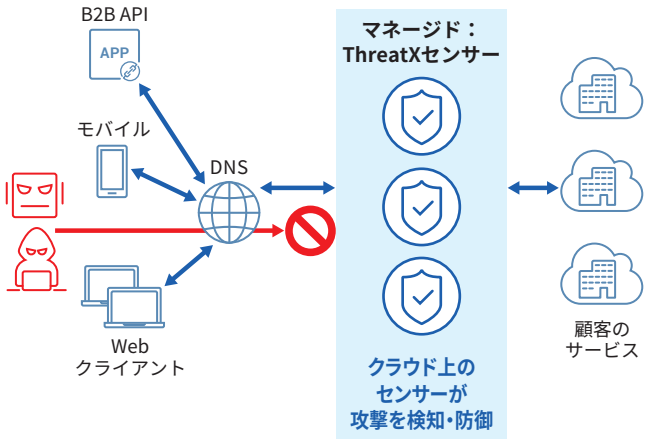
防御対象

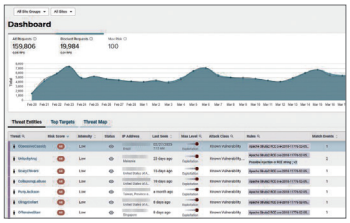
- Webアプリ
- API
- AI
- システム / サーバ
  - DNSサーバ
  - Webサーバ
  - APIサーバ
  - AIサーバ
  - など
- ネットワーク

API防御、WAF、L7 DDoS防御、ボット対策がフルセットで利用可能なクラウド型WAAP

ThreatX by A10 Networks

詳細をWebで確認





ThreatXは、Webアプリケーションと APIを包括的に保護するクラウドネイティブ WAAP（Web Application and API Protection）です。WAF、APIセキュリティ、L7 DDoS対策、ボット対策を統合し、独自の行動解析とリスクスコアリングによる検知、防御機能で巧妙な攻撃からサービスを保護します。

- 行動解析と脅威インテリジェンスにより、シグネチャベースよりも高い精度で攻撃を阻止。
- リスクスコアに基づく自動ブロックで、誤検知を減らし運用負荷を軽減。
- クラウドネイティブなアーキテクチャにより、クラウド、オンプレミス、ハイブリッドなど、あらゆる環境で素早く導入可能

リスクベースの自動ブロッキング
Protection-as-a-Service
わずか15分でサイトに設置可能

- 行動解析とリスクスコアによる防御
- オールインワンセキュリティ
- SOCチームによるサポート
- クラウドネイティブ対応による迅速な導入

DDoS 攻撃からWebアプリを守る、精密な最初の防御層

A10 Defend Threat Control

詳細をWebで確認

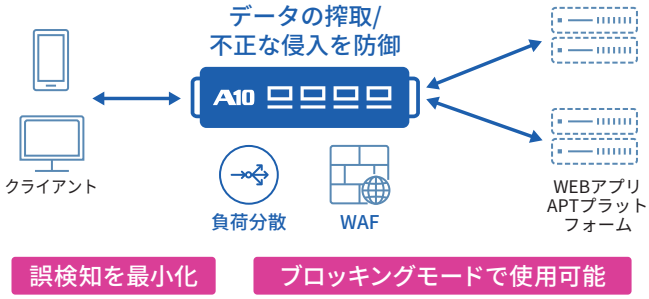
A10 Defend Threat Controlは、能動的なDDoS防御を可能とするDDoS特化の脅威インテリジェンスです。A10の専門チームにより収集・調査・分析されたデータはSaaSとして提供され、攻撃検知より前の先回り防御を可能にします。

- 自組織のIPがDDoS攻撃に加担しそうな場合、早期アラートで安全性を確保
- 信頼性の高いIPブロックリストを提供し、既存セキュリティ機器と連携した防御が可能
- 専用機器不要のSaaS型で、導入コストや運用負担を削減

アプリケーション配信＋誤検知を最小化した次世代WAF

A10 Defend Next-Gen WAF, Powered by Fastly

詳細をWebで確認



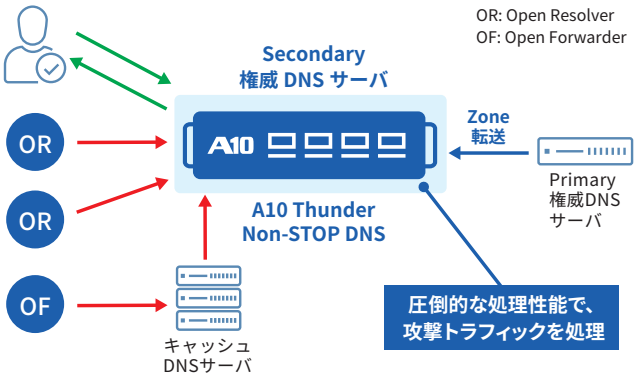
A10 Defend Next-Gen WAF, Powered by Fastlyは、A10のアプリケーション配信・負荷分散＋Fastly社の次世代型WAFを統合したソリューションです。仮想マシンやハードウェアなど、さまざまなフォームファクタで利用可能です。誤検知を最小化する実用的なソリューションとして、Webサービスを守ります。

- 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

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



Non-STOP DNSは、A10 Defend DDoS Mitigator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。

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

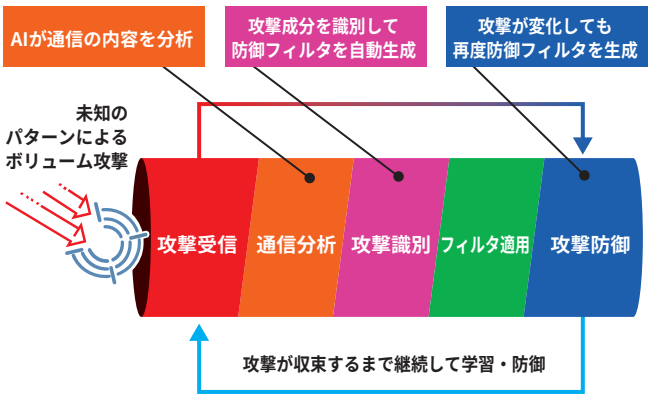
クライアントからの全てのDNSクエリにはNon-STOP DNSが応答

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)

AIで強化したボリューム型攻撃に対抗するための自動フィルタ生成機能

ZAPR(Zero-day Attack Pattern Recognition)

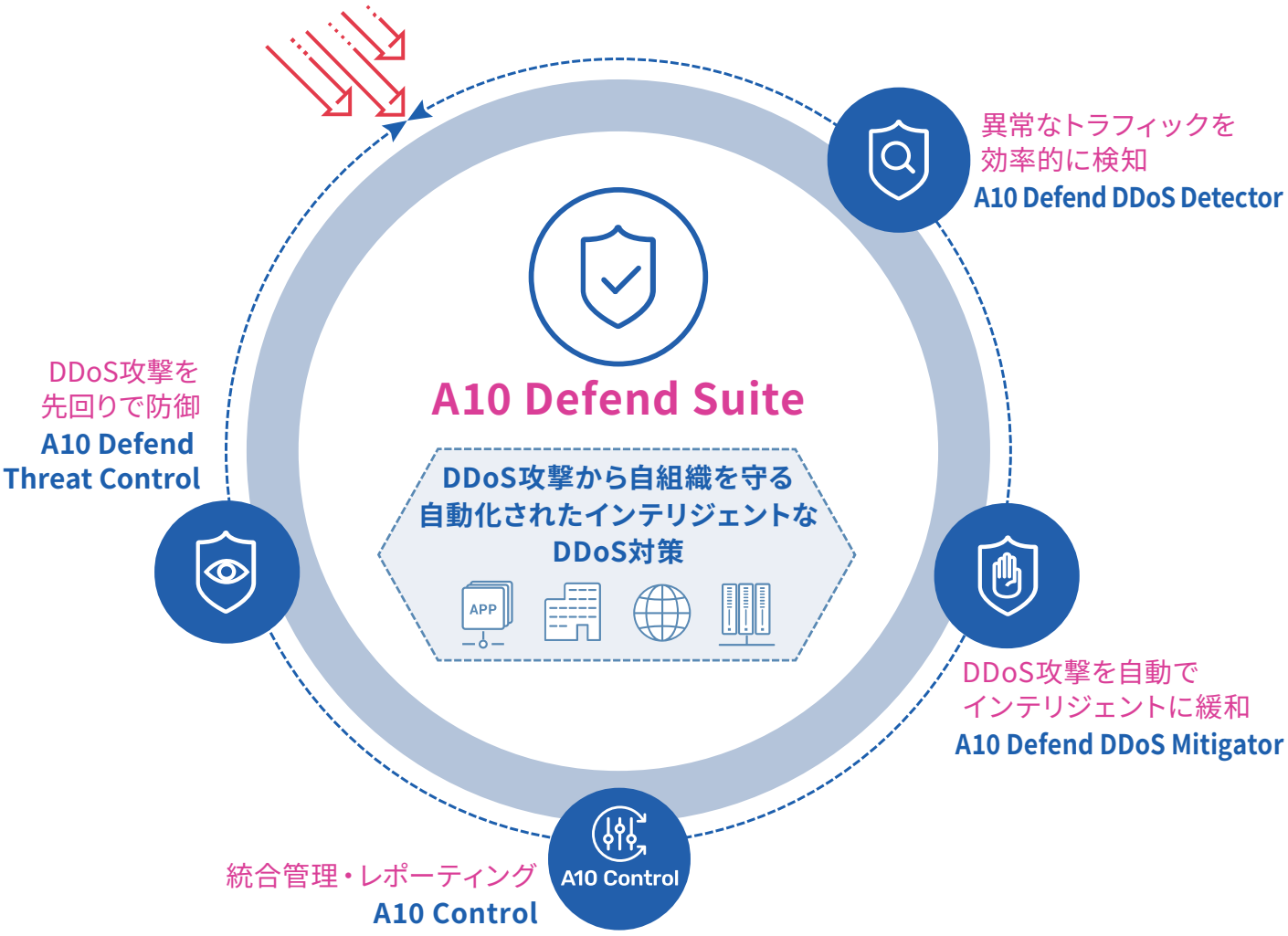
詳細をWebで確認

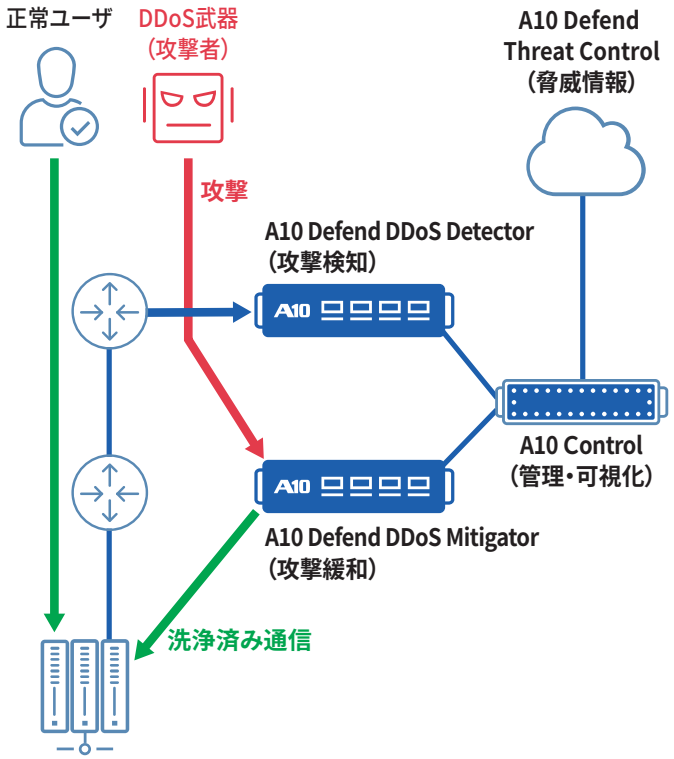


ゼロデイ攻撃パターン認識(ZAPR)エンジンは、機械学習を活用してDDoS攻撃の特徴を自動的に識別し、動的に緩和フィルターを適用します。

- ゼロデイ攻撃や新たな攻撃パターンにも迅速かつ自動的に対応可能
- 事前の高度な設定や手動による介入不要
- 攻撃緩和の精度を向上

A10 Defend DDoS Suite:DDoS攻撃対策統合ソリューション





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 DDoS Mitigator :
DDoS 攻撃を緩和して、サービス停止を阻止

A10 Defend DDoS 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 Control :
Detector, Mitigator による DDoS 攻撃の検知・緩和を一元管理
Mitigator と Detector の連携により、攻撃の詳細なレポーティングと分析を実現

A10 Defend Threat Control :
DDoS 攻撃対策の監視調査分析
A10 の専門チームによる 24 時間 365 日のアタックサポートを提供
ログストレージ、分析、レポート作成、脅威情報の分析 共有を行う

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

ボリュー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

ボリュー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

2025年6月現在

緩和装置：A10 Defend DDoS Mitigator

～10 Gbps

モジュラーライセンス

Thunder 1060S
5G, 10G, 20Gbps
7x1GC, 4x1/10GF, 2x10/25GF

Thunder 3350-E
10Gbps
6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF

Mitigator VA
1～5Gbp
Virtual Appliance

Mitigator VA for Cloud
5Gbps
Microsoft Azure

10G～100Gbps

SPEモデル

Thunder 5845
100Gbps
48x1/10GF, 4x100GF

SPEモデル

Thunder 5845-40G
40Gbps
48x1/10GF, 4x100GF

Mitigator VA
10～100Gbps
VMware ESXi (SR-IOV)
FlexPool Licensing

100Gbps~

SPEモデル

Thunder 8665S
550Gbps
12 x 400GF

SPEモデル

Thunder 7655S
380Gbps
16x100GF

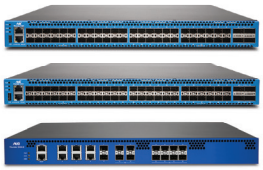
SPEモデル

Thunder 7445
220Gbps
48x1/10GF, 4x100GF

管理ソフトウェア

A10 Defend DDoS Orchestrator on A10 Control

検知装置



A10 Defend DDoS Detector Thunder 3350-E, 5845, 7445
Standalone Detector
1 – 6 Million fps

A10 Defend DDoS 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

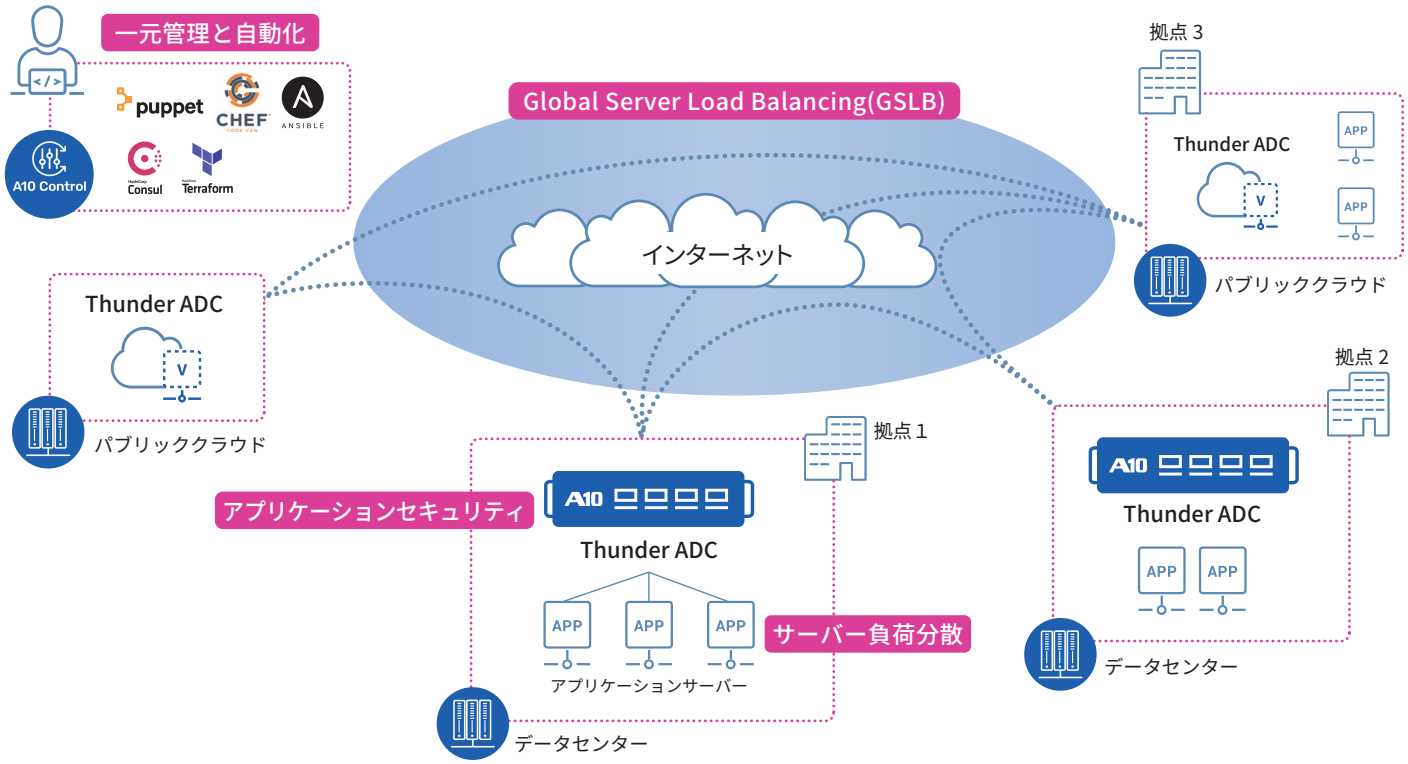
最新情報または詳細は、
右記のwebページをご覧下さい。

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リゼーション、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 Control 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 Control 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 エクスポータ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

2025 年 6 月現在

仮想アプライアンス

vThunder ADC for Cloud
Microsoft Azure, AWS:
最大 10 Gbps まで
Oracle Cloud: 最大 24Gbps まで

vThunder ADC 仮想アプライアンス
最大 100 Gbps まで

Thunder ADC for Container (Docker)
最大 100 Gbps まで

ベアメタル

Thunder ADC for Bare Metal

～ 25 Gbps

モジュラーライセンス
Thunder 1060S
25 Gbps
7x1GC, 4x1/10GF, 2x10/25GF

モジュラーライセンス
Thunder 1060S
10 Gbps
7x1GC, 4x1/10GF, 2x10/25GF

～ 100 Gbps

Thunder 4440
78 Gbps
24x1/10GF, 4x40GF

Thunder 3350S
50 Gbps
6x1GC, 2x1GF, 8x1/10GF, 4x10GF

Thunder 3350
40 Gbps
6x1GC, 2x1GF, 4x25GF, 4x40GF, 4x10GF

Thunder 3350 -E
30 Gbps
6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF

～ 200 Gbps

Thunder 6440
150 Gbps
48x1/10GF, 4x40GF

Thunder 5840
115 Gbps
24x1/10GF, 4x40GF
Thunder 5840-11
115 Gbps
24x1/10GF, 4x100GF

Thunder 5440
100 Gbps
24x1/10GF, 4x40GF

SPE モデル

Thunder 6655S
185 Gbps
16x100GF

200 Gbps ～

SPE モデル

Thunder 7655S
370 Gbps
16x100GF

Thunder 7440
220 Gbps
48x1/10GF, 4x40GF
Thunder 7440-11
220 Gbps
48x1/10GF, 4x100GF

超低遅延モデル

Thunder 3745
4 x 10GE

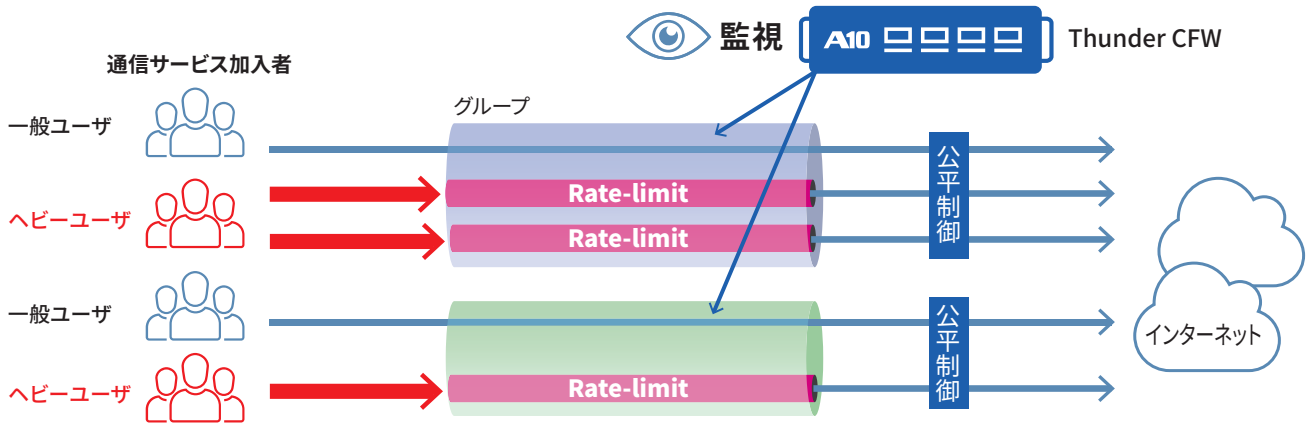
*SPE モデル：セキュリティポリシーの適用を高速化するハードウェアである SPE(Security and Policy Engine) を搭載したモデル
*モジュラーライセンス：ソフトウェアとハードウェアを分離し、同一ハードウェアであっても帯域やその他のスペックによってカバーする領域を分けて提供する形態

最新情報または詳細は、
右記の web ページをご覧下さい。

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

2025 年 6 月現在

仮想アプライアンス

- 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

～ 100 Gbps*	～ 200 Gbps*	200 Gbps* ～
Thunder 4440S 24x1/10GF, 4x40GF	**Thunder 7440** 48x1/10GF, 4x40GF **Thunder 7440-11** 48x1/10GF, 4x100GF	**Thunder 8665S** 12 x 400GF
Thunder 5840 24x1/10GF, 4x40GF **Thunder 5840-11** 24x1/10GF, 4x100GF		**Thunder 7655S** 16x100GF
Thunder 3350S 6x1GC, 2x1GF, 8x1/10GF, 4x10GF	**Thunder 6440S** 48x1/10GF, 4x40GF	**Thunder 7650** 16x100GF
Thunder 5440 24x1/10GF, 4x40GF		

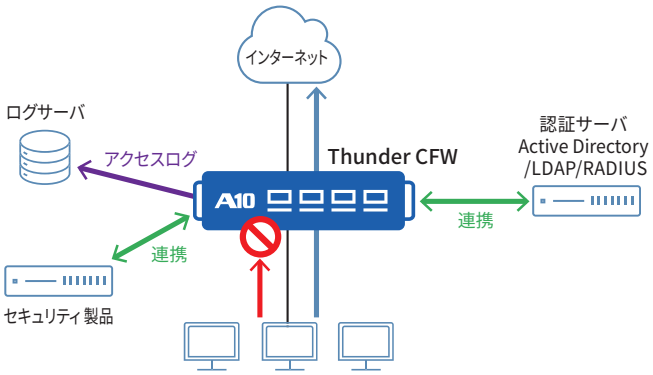
* 公平制御で必要となるスループットの目安

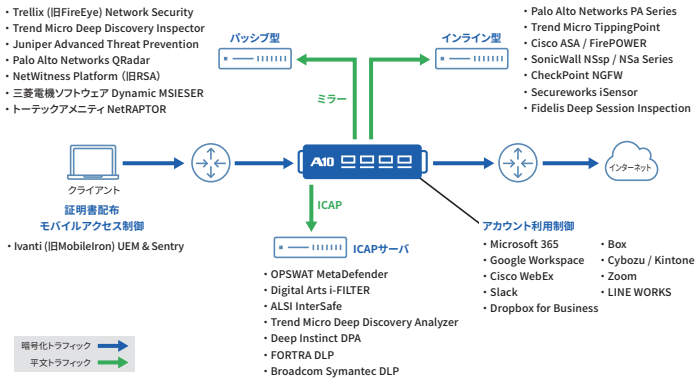
最新情報または詳細は、
右記の web ページをご覧下さい。

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チスキャンや、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

2025 年 6 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～
モジュラーライセンス **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
モジュラーライセンス **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 7440S-11** 25 Gbps* 48x1/10GF, 4x100GF	**Thunder 5840S** 25 Gbps* 24x1/10GF, 4x40GF **Thunder 5840S-11** 25 Gbps* 24x1/10GF, 4x100GF
		Thunder 3350S 5.5 Gbps* 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF		

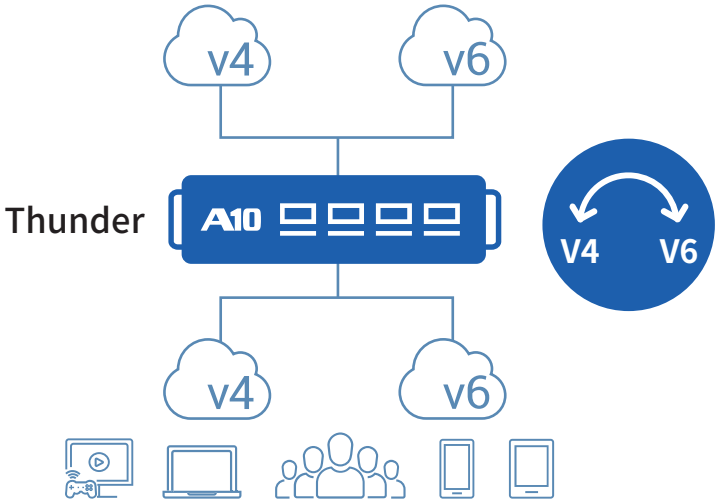
*全通信をSSL/TLS可視化した際の最大スループット *モジュラー：モジュラーライセンス。ソフトウェアとハードウェアを分離し、同一ハードウェアであっても帯域やその他のスペックによってカバーする領域を分けて提供する形態

最新情報または詳細は、
右記の web ページをご覧下さい。

ソリューション詳細

データシート

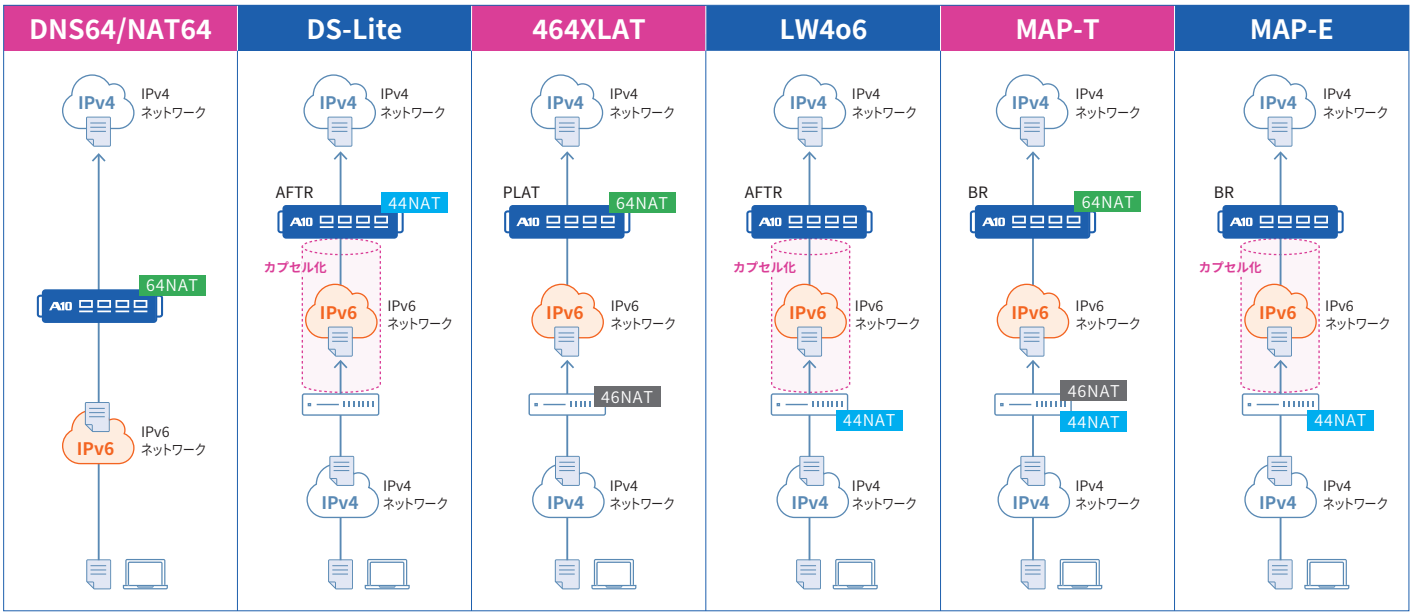
IPv6 移行、IPv4 枯渇対策



キャリアグレード NAT で
IPv4 枯渇対策

IPv4 – IPv6 を相互に変換

IPv4、IPv6 どちらの基盤でも
両バージョンの通信が可能



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

2025年6月現在

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

～100 Gbps

Thunder 4440
78 Gbps
24x1/10GF, 4x40GF

Thunder 3350S
50 Gbps
6x1GC, 2x1GF, 8x1/10GF, 4x10GF

Thunder 3350
40 Gbps
6x1GC, 2x1GF, 4x25GF, 4x40GF, 4x10GF

Thunder 3350 -E
30 Gbps
6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF

～200 Gbps

Thunder 6440
48x1/10GF, 4x40GF

SPE モデル

Thunder 5845
115 Gbps
48x1/10GF, 4x100GF

Thunder 5840
115 Gbps
24x1/10GF, 4x40GF

Thunder 5840-11
115 Gbps
24x1/10GF, 4x100GF

Thunder 5440
100 Gbps
24x1/10GF, 4x40GF

200 Gbps～

SPE モデル

Thunder 8665S
550 Gbps
12 x 400GF

SPE モデル

Thunder 7655S
370 Gbps
16x100GF

Thunder 7650
370 Gbps
16x100GF

SPE モデル

Thunder 7445
220 Gbps
48x1/10GF, 4x100GF

Thunder 7440
220 Gbps
48x1/10GF, 4x40GF

Thunder 7440-11
220 Gbps
48x1/10GF, 4x100GF

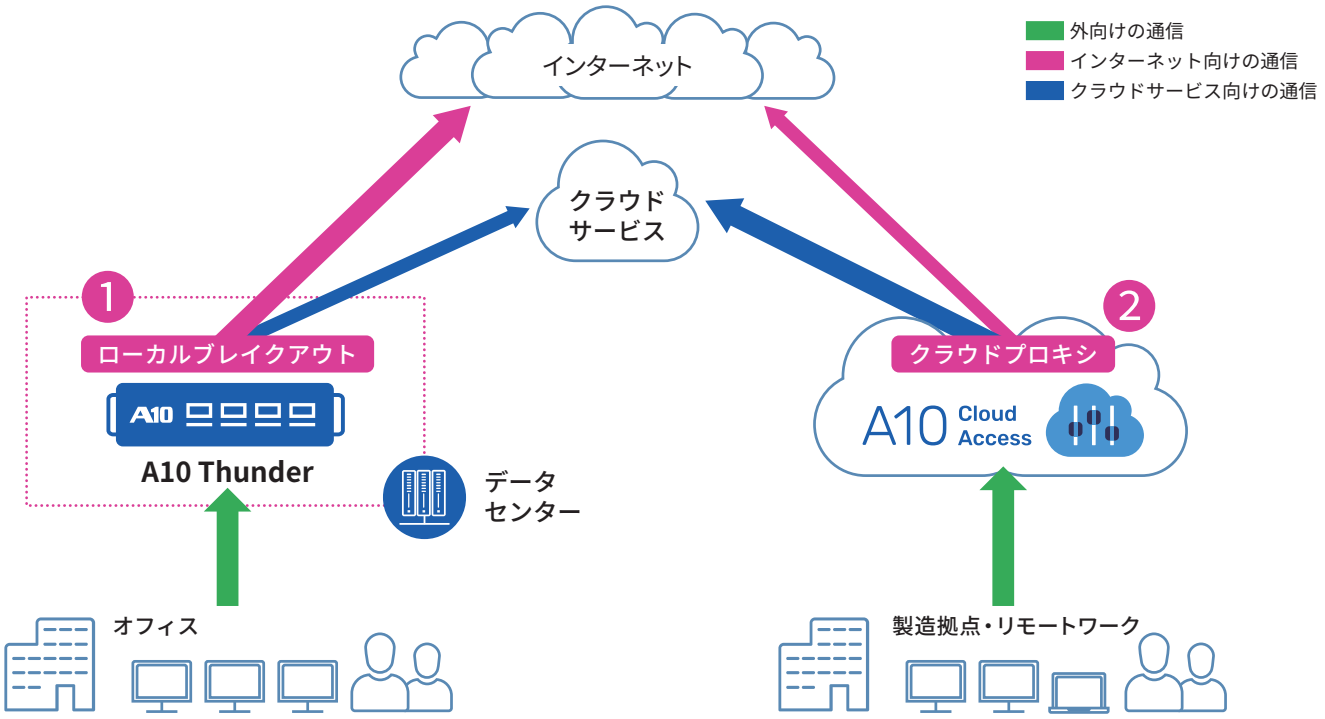
*SPE モデル：セキュリティポリシーの適用を高速化するハードウェアである SPE(Security and Policy Engine) を搭載したモデル

最新情報または詳細は、
右記の web ページをご覧下さい。

ソリューション詳細

データシート

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 ページをご覧下さい。

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

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

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

対応製品

2025 年 6 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～
モジュラーライセンス  **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
モジュラーライセンス  **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 7440S-11** 25 Gbps* 48x1/10GF, 4x100GF	 **Thunder 5840S** 25 Gbps* 24x1/10GF, 4x40GF **Thunder 5840S-11** 25 Gbps* 24x1/10GF, 4x100GF
		 **Thunder 3350S** 5.5 Gbps* 6x1GC, 2x1/10GF, 8x1/10GF, 4x10GF		

*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

2025 年 6 月現在

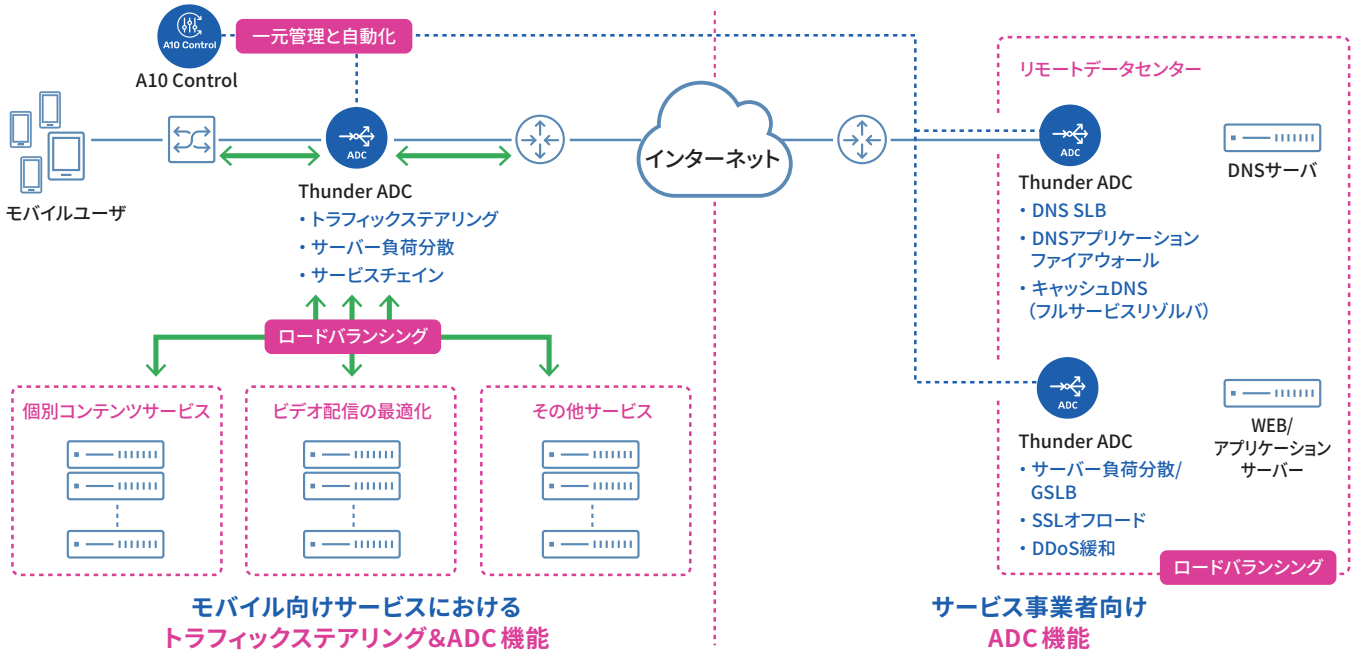
- **Basic、Standard、Advanced の包括ライセンスのみ**
  - 追加オプション有
- **クライアント数での課金**
  - 課金単位：50 クライアント
    （最小利用：50 クライアントより）
- **期間：1 年単位（最小契約：1 年）**
  - フリートライアル：有（1 か月）
- **アクセスログは最大 3 か月保管**
  - （ログは Web API 経由で取得可能）

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

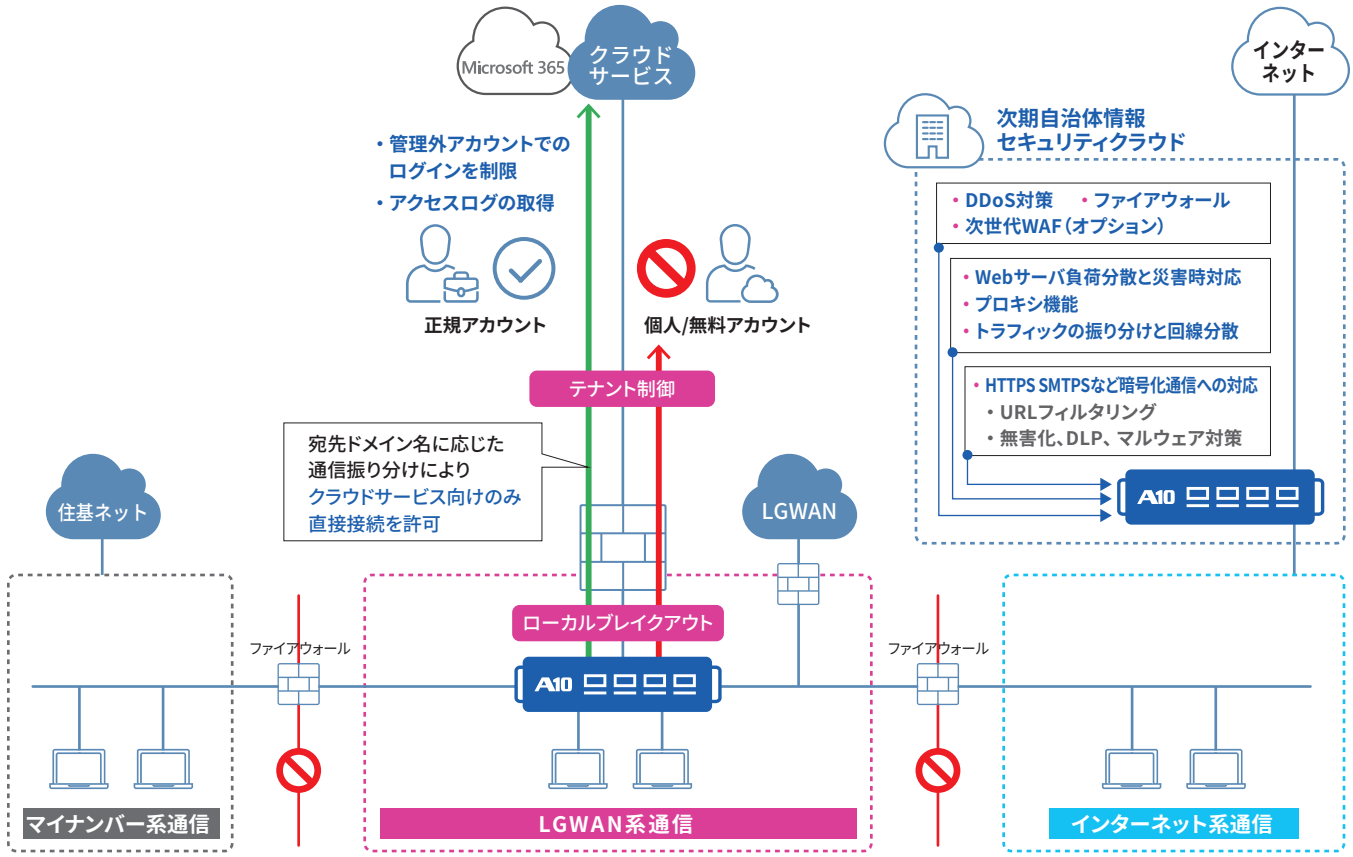
Web事業者

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



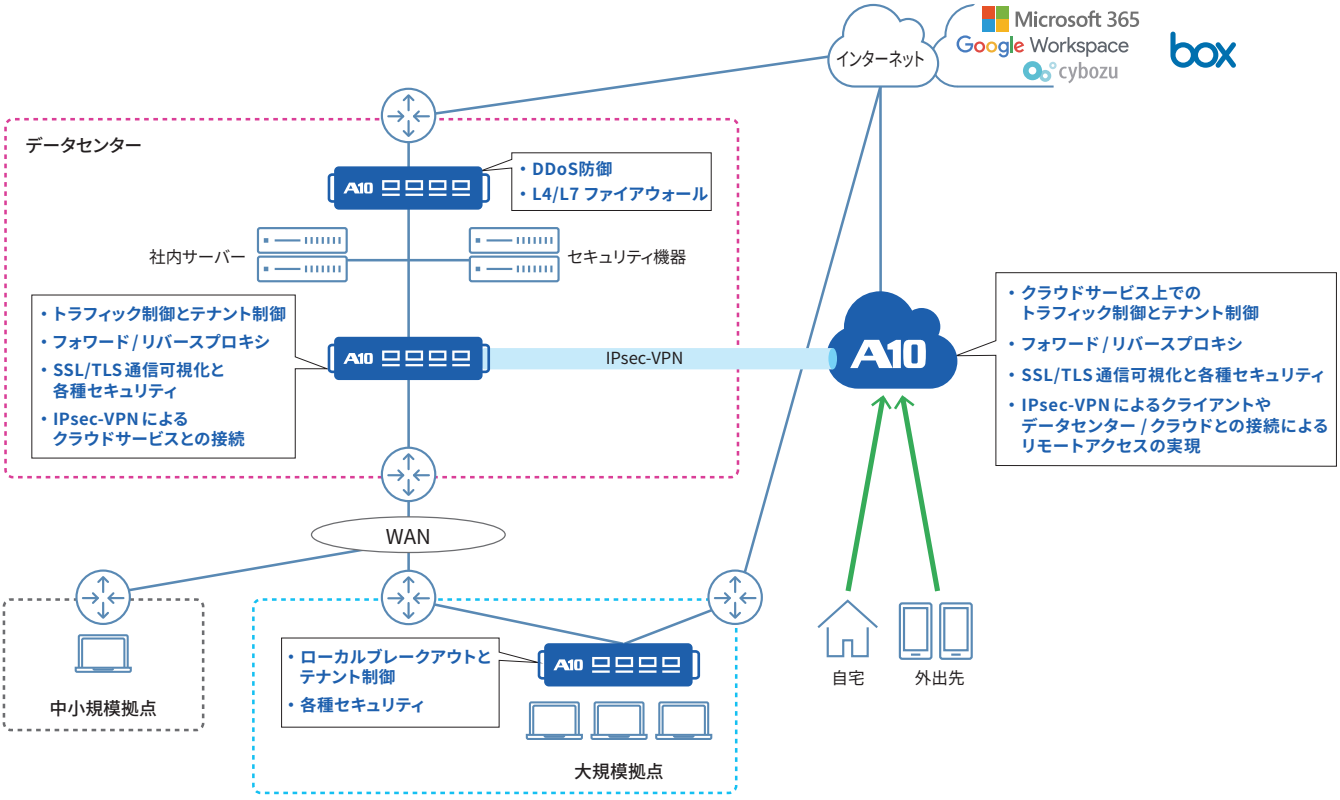
自治体

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

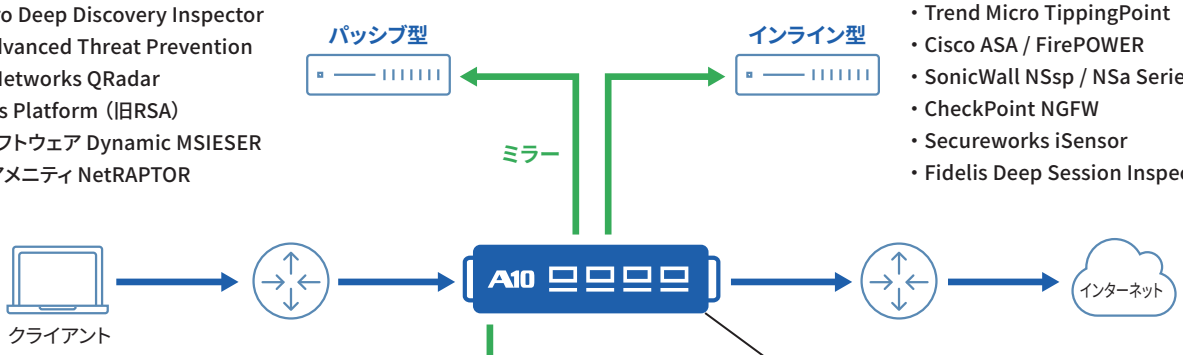


SSL/TLS通信可視化と連携ソリューション

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

- Trellix (旧FireEye) Network Security
- Trend Micro Deep Discovery Inspector
- Juniper Advanced Threat Prevention
- Palo Alto Networks QRadar
- NetWitness Platform（旧RSA）
- 三菱電機ソフトウェア Dynamic MSIESER
- トーテックアメニティ NetRAPTOR

- Palo Alto Networks PA Series
- Trend Micro TippingPoint
- Cisco ASA / FirePOWER
- SonicWall NSsp / NSa Series
- CheckPoint NGFW
- Secureworks iSensor
- Fidelis Deep Session Inspection



証明書配布
モバイルアクセス制御

- Ivanti (旧MobileIron) UEM & Sentry

ICAPサーバ

- OPSWAT MetaDefender
- Digital Arts i-FILTER
- ALSI InterSafe
- Trend Micro Deep Discovery Analyzer
- Deep Instinct DPA
- FORTRA DLP
- Broadcom Symantec DLP

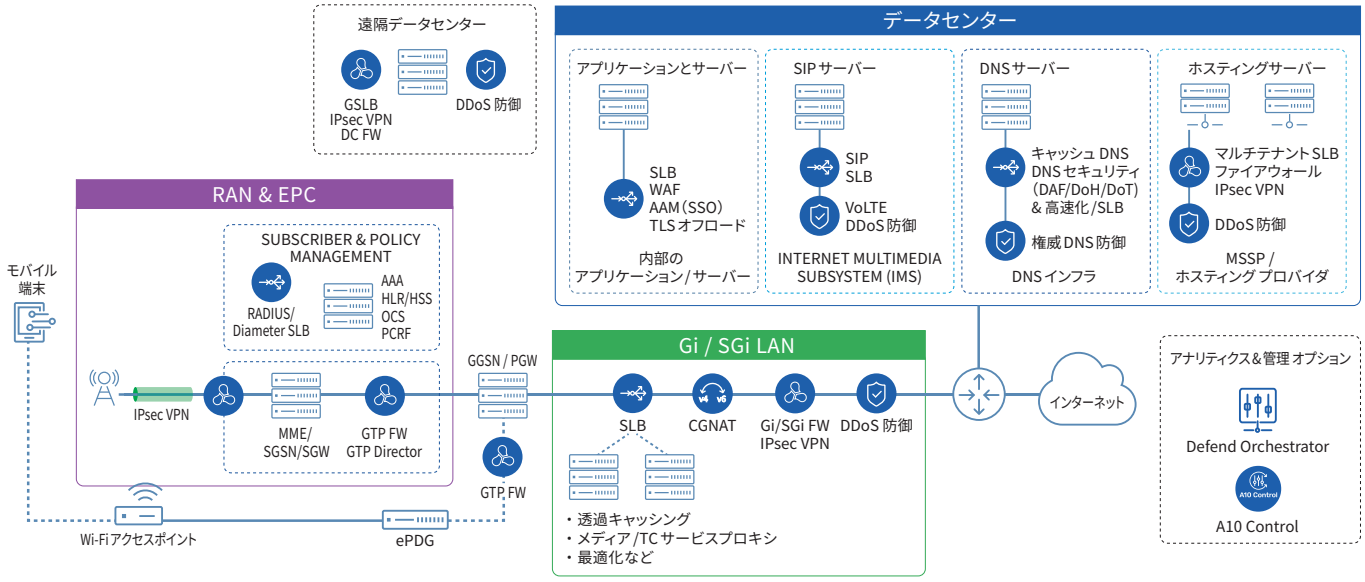
アカウント利用制御

- Microsoft 365
- Google Workspace
- Cisco WebEx
- Slack
- Dropbox for Business
- Box
- Cybozu / Kintone
- Zoom
- LINE WORKS

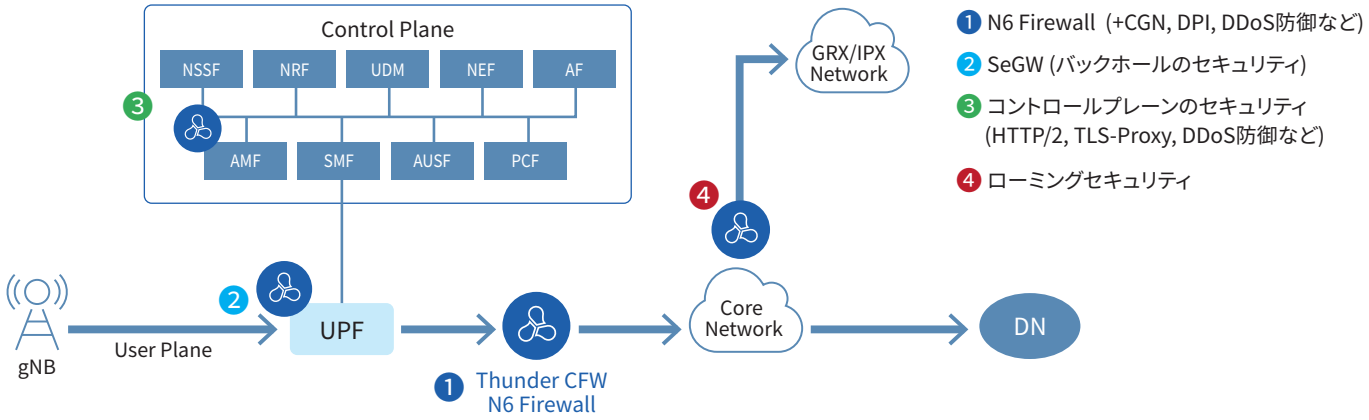
暗号化トラフィック
平文トラフィック

導入例

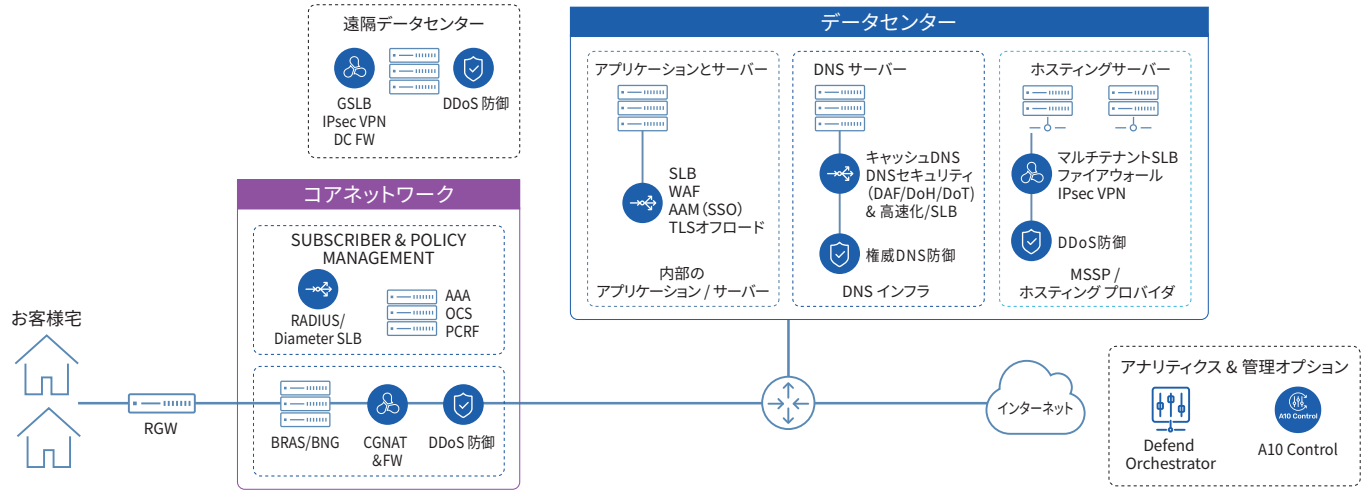
モバイル事業者様向けソリューションマップ（LTE/5G-NSA向け）



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

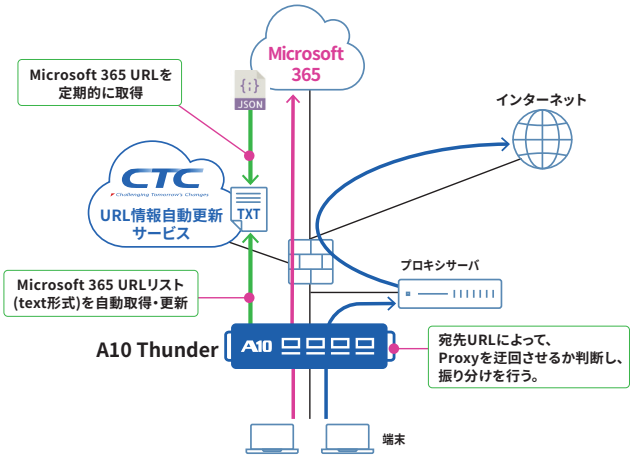


パートナーソリューション

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



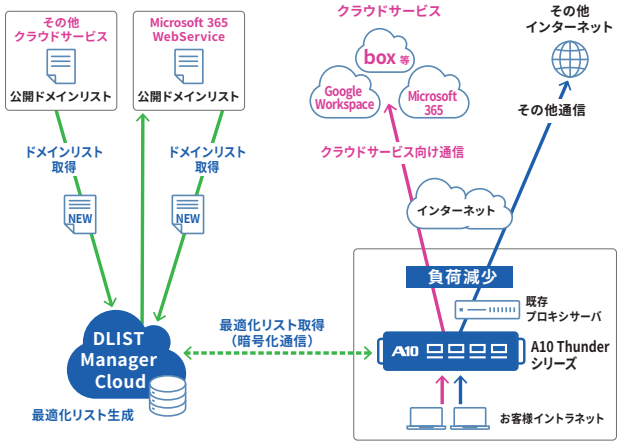
伊藤忠テクノソリューションズ株式会社

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 サーバの負荷低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/



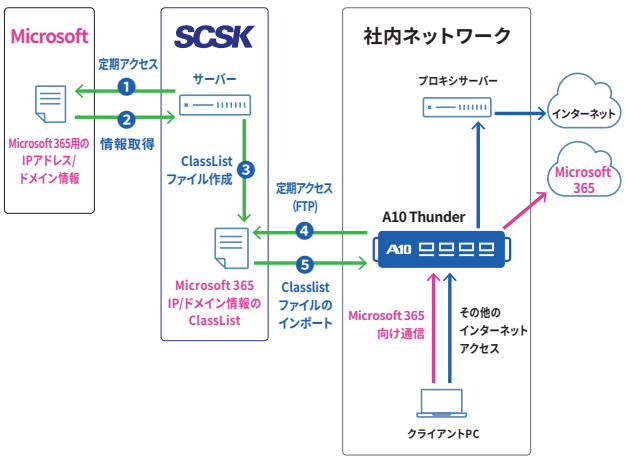
富士通ネットワークソリューションズ株式会社

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、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なため、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

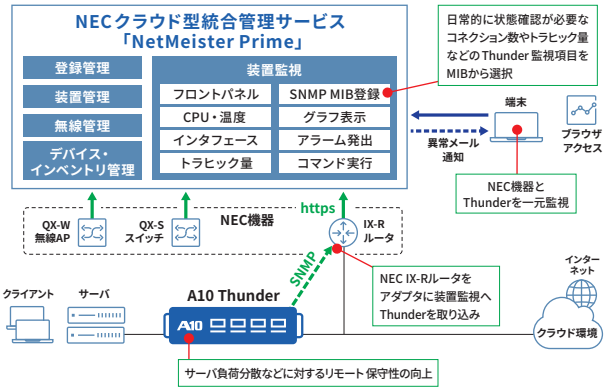
A10 機器向け Classlist ファイル自動更新サービス

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



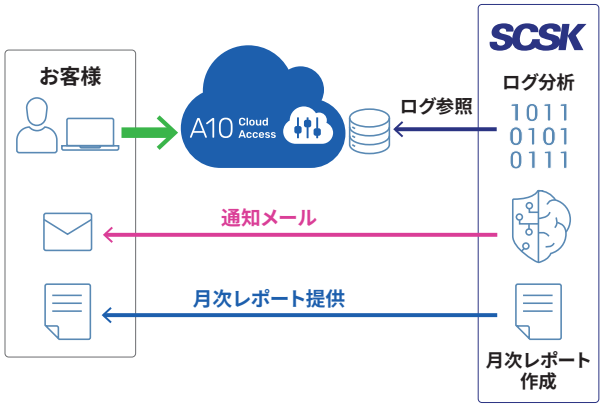
日本電気株式会社

クラウド型統合管理サービスによる一元監視

NetMeister 連携マルチベンダ管理ソリューション(A10 製品)

NEC が提供するクラウド型統合管理サービス「NetMeister (ネットマイスター)」との連携で、NEC ネットワーク機器 (IX/QX シリーズ) に加え A10 Thunder の装置監視を実現します。顧客ネットワーク内の多拠点、多数の装置を、NetMeister の一つの管理画面で一括可視化・リモート保守管理ができるようになります。A10 製品の CPU 使用率、インタフェース状態、サーバ負荷分散コネクション数、トラヒック量などの情報収集が可能になり、現地対応を最小限にして管理者の負担を大きく削減します。

お問合せ : 各 NEC 担当営業の窓口までご連絡ください



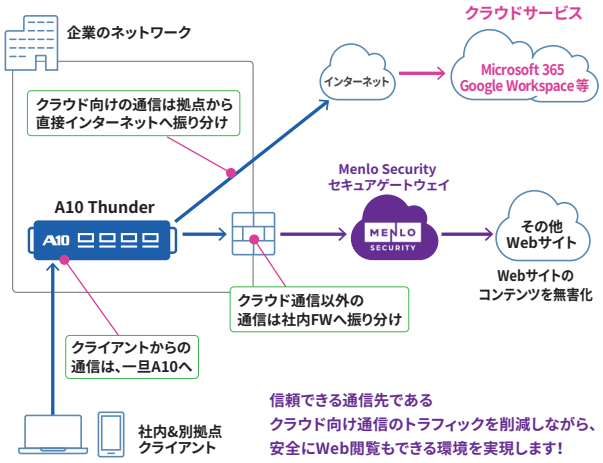
SCSK 株式会社

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。*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

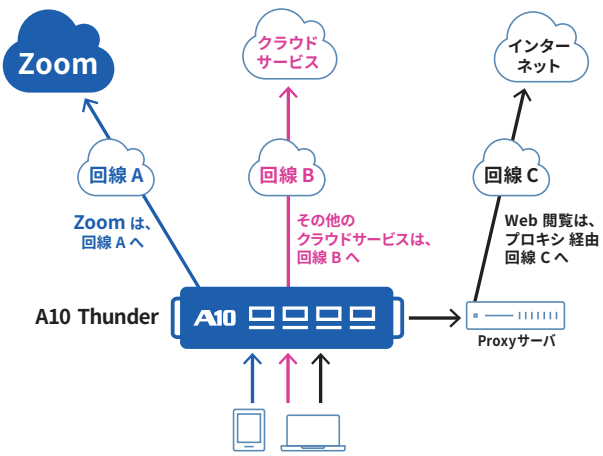
リモートワークやクラウド (Microsoft 365 等) の利用拡大、悪意のあるコンテンツが増加している昨今、安全・快適に Web が利用できないという声は上がっていませんでしょうか

⇒　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 にブレー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 ネッツエスアイ株式会社

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

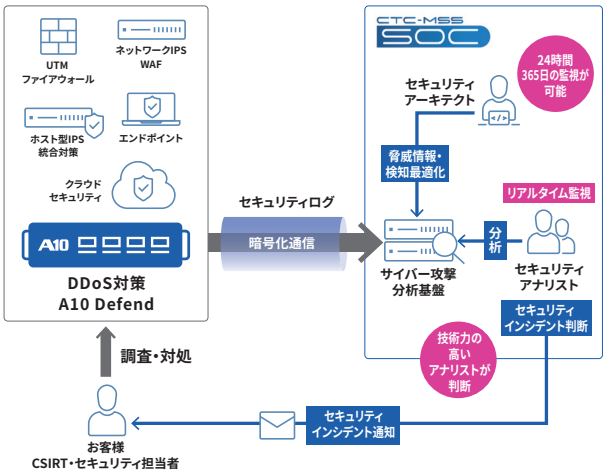
音声 / ビデオ会議通信システムの提供で多くの実績を持つ NEC ネッツエスアイが提供する「Zoom トラフィック最適化ソリューション」は、インターネットアクセスの増加による通信回線ひっ迫の課題を解決し、Zoom の高い映像・音声コミュニケーション品質を維持することが可能なソリューションです。

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

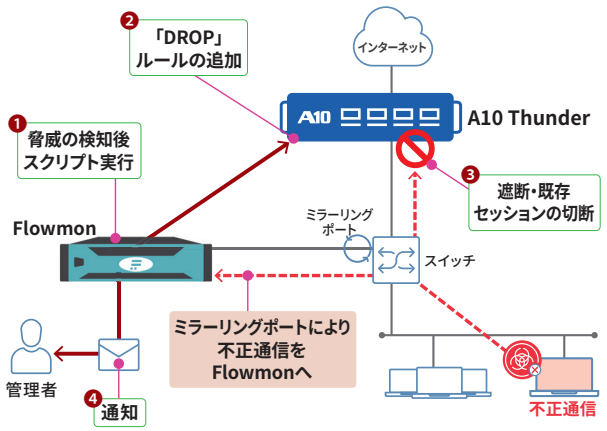
DDoS 攻撃は現在も多くの被害を及ぼしています。

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

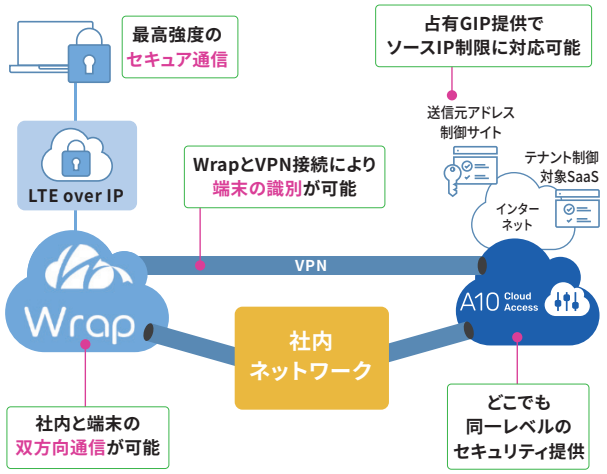
不正通信の検知・遮断を自動化による安全な業務環境を実現

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

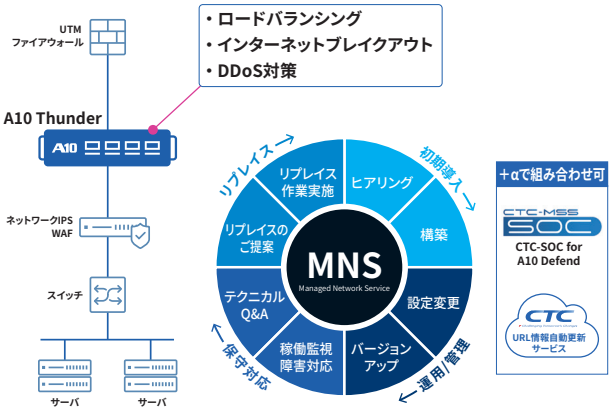
持ち出し PC にも社内と同じアクセス制御とセキュリティ

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



伊藤忠テクノソリューションズ株式会社

A10 トラフィックマネジメントの支援サービス

CTC マネージド ネットワーク サービス

本サービスは、A10 製品の運用を CTC が一括で担う、フルマネージド型の運用サービスです。設定変更、バージョンアップ、障害対応などの定常業務に加えて、「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」や「CTC-SOC for A10 Defend」といった CTC 独自のソリューションと組み合わせることで、単なる運用代行にとどまらず、セキュリティの強化まで一体的に支援します。

運用負荷の軽減とセキュリティ対策の両立を目指す企業に、最適なサービスです。

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/

A10 製品の導入をご検討中のお客様へ

A10 の販売パートナー

お問い合わせ先一覧　https://www.a10networks.co.jp/partner/affinity-partners/

詳細をWebで確認

Platinum Partner

プラチナ・パートナー

CTC Challenging Tomorrow's Changes
NEC \Orchestrating a brighter world
FUJITSU 富士通ネットワークソリューションズ株式会社
MKI

Platinum Indirect Distributor

プラチナ・インダイレクト・ディトリビューター

SCSK

Gold Partner

ゴールド・パートナー

- NTTデータ先端技術株式会社
- 株式会社日立システムズ
- ユニアデックス株式会社

Bronze Partner

ブロンズ・パートナー

- NECネッツエスアイ株式会社
- ジェイズコミュニケーション株式会社
- 双日テックイノベーション株式会社
- 日鉄ソリューションズ株式会社
- 株式会社日立ソリューションズ
- 富士通株式会社

Authorized Reseller

認定パートナー

- 株式会社インターネットイニシアティブ
- エイチ・シー・ネットワークス株式会社
- 株式会社エーピーコミュニケーションズ
- キヤノンITソリューションズ株式会社
- スターネット株式会社
- ソフトバンクコマース&サービス株式会社
- ソフトバンクテクノロジー株式会社
- 株式会社宝情報
- 株式会社ディ・アイ・システム
- デジタルテクノロジー株式会社
- トビラシステムズ株式会社
- 日信ITフィールドサービス株式会社
- 日本ビジネスシステムズ株式会社
- 株式会社ネットケアサービス
- エフサステクノロジーズ株式会社

2025 年 6 月現在

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。

https://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。

https://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/

A10 へのお問い合わせ

A10 製品やソリューション、導入に関するご不明点など、
お気軽にご質問ください。

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

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-Product Overview　JUN 2025