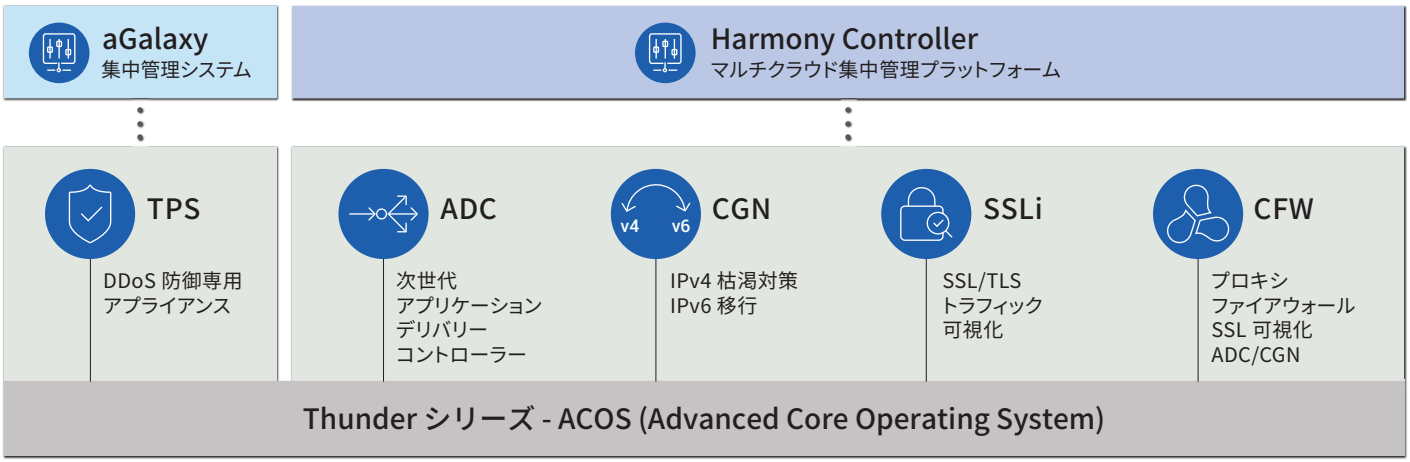
Product Overview

A10 ネットワークス
総合カタログ 2021

A10



A10 ネットワークスの製品群は、高速なトラフィック処理や大容量のセッション管理が求められるアプリケーションネットワーキングにおいて威力を発揮します。

Thunder シリーズは、全てのモデルにおいて CPU の性能を最大限引き出す A10 の独自 OS、ACOS を基盤としており、高速なサーバー負荷分散・アプリケーション配信を実現する Thunder ADC や、クラウドアクセスプロキシやファイアウォール機能を搭載したハイパフォーマンスセキュリティプラットフォーム Thunder CFW、IPv4 枯渇対策と IPv6 移行機能に特化した Thunder CGN、DDoS 防御専用アプライアンス Thunder TPS などの製品ラインナップを提供しています。

A10 ネットワークスは最先端技術で
日本のアプリケーションデリバリーの課題を解決します

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。

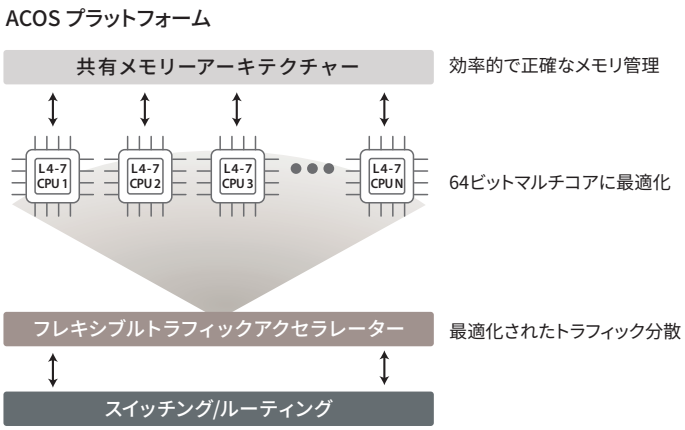
日本国内の市場に適したサポートを提供できるよう、2009 年 3 月には日本法人を設立しました。日本に根差した経営を行ない、日本市場の特徴を理解し、その要望にお応えしていく ― それが A10 ネットワークスの使命です。

A10 の強み：日本に特化した協力なサポート体制

A10 ネットワークスの強みは、日本国内に専用の検証環境や品質管理体制 / 技術開発部門をもっていることです。

営業 /SE/ サポートチームが一丸となり、導入から運用まで手厚くサポートしています。日本からの要望や機能開発においても密接に連携し、日本のお客様の要望や意見を積極的に製品開発に取り入れています。

Thunderシリーズのパフォーマンスを支える独自OS ACOS



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

Thunderシリーズの特徴

高いパフォーマンス
最大370 Gbps以上のスループットを実現する高いパフォーマンス

日本語GUI
完全に日本語化されたブラウザーによる操作画面

省スペース、省電力
コンパクトな筐体と高効率な電源を採用

オールインワンライセンス
全機能が標準で提供されており、追加のライセンス費用が不要

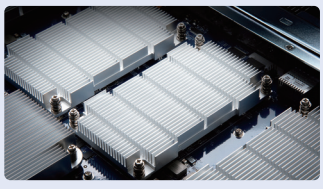
業界標準CLI
Ciscoライクなコマンドラインインターフェースを採用

キャリアクラスのハードウェア
冗長化電源やSSDを採用した信頼性の高いハードウェア

用途、ビジネス規模に応じて選べる豊富なラインナップ

PFS/ATSに対応したSSL高速化ハードウェアを搭載したハードウェアモデルや、VMwareやKVM上で動作する仮想アプライアンスモデルなど、環境や規模に応じたモデルを選択可能です。

そのほかにも汎用サーバを活用できるベアメタルライセンスや、Azure、AWS、GCP、Oracle Cloudなどで購入できるインスタンスライセンス、ハイブリッド・マルチクラウドに対応したコンテナ版も提供されており、これらは同じ機能を利用可能なため、従来のデータセンターとマルチクラウド環境にまたがって一貫した運用が可能です。



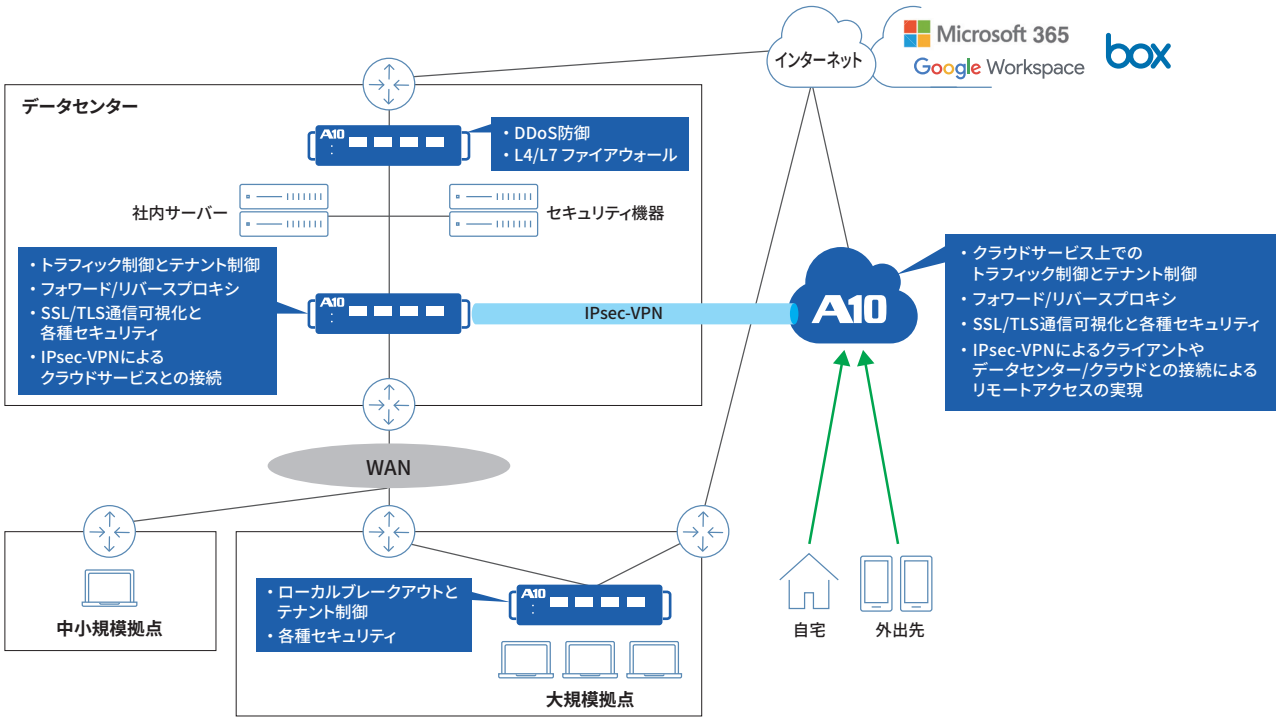
圧倒的なパフォーマンスを提供する専用ハードウェアを搭載

Thunderシリーズの上位モデルには、特定の処理を高速に処理することができる専用のハードウェアが複数搭載されています。PFS/ATS/ECCに対応したSSL高速化ハードウェアやDDoS攻撃防御を高速化するFTA(Flexible Traffic ASIC)などが搭載されており、ACOSがこれらを効率よくCPUと連携させることによって、圧倒的なパフォーマンスを実現します。

企業・自治体情報セキュリティ対策向けソリューション

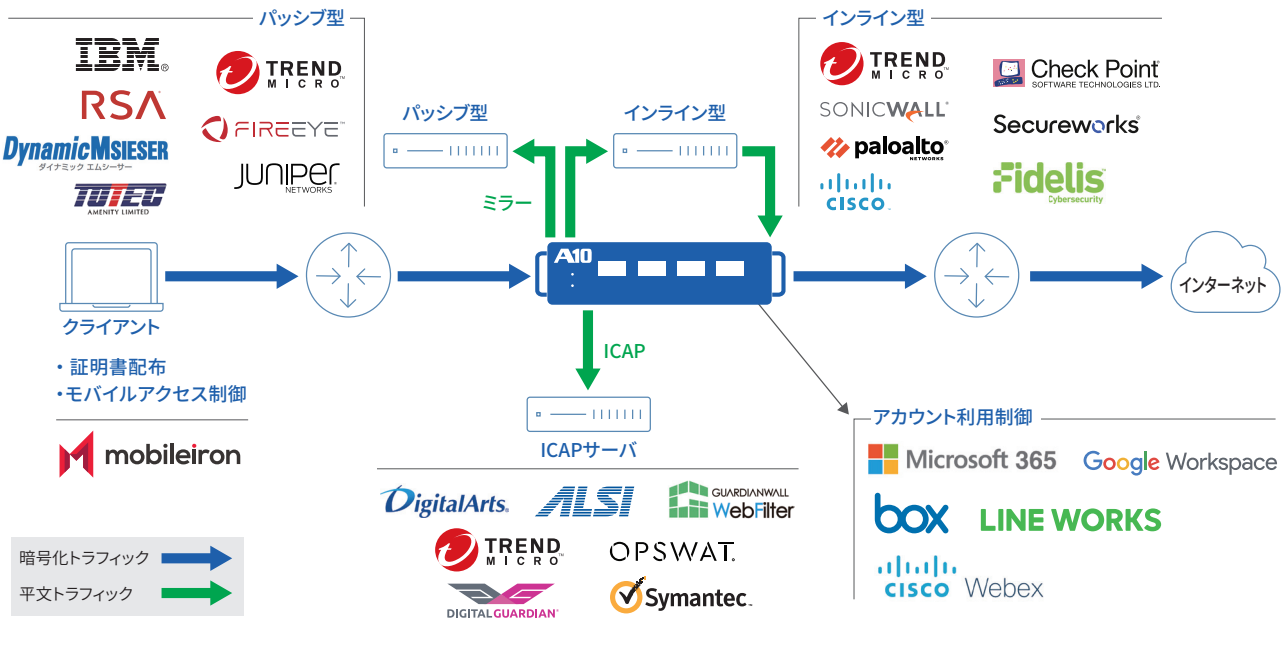
エンタープライズネットワーク向けソリューションマップ

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



企業・自治体情報セキュリティ対策向けソリューション

快適なクラウドサービス利用と利用アカウント制御

A10 のクラウドアクセスプロキシソリューションにより、Microsoft 365 や Box などの SaaS を始めとするクラウドサービスの快適な利用を実現できます。SaaS の利用を開始すると、これまで組織内で閉じていた通信が全てインターネットに流れることから必要な通信セッション数が増大し、既存のプロキシサーバーやファイアウォールなどが通信のボトルネックとなり、十分な帯域があってもクラウドサービスの動作に影響を与えます。

Thunder CFW シリーズを導入しフォワードプロキシとして利用することで、クラウドサービスのトラフィックを識別して、ボトルネックとなる箇所をバイパスできます。クラウドサービスは基本的にドメイン名で定義されており、IP アドレスは頻繁に変化することからルーターやファイアウォール等でのトラフィック制御は困難ですが、Thunder CFW ではトラフィックに含まれるドメイン名を識別して通信を振り分けるため、適切にトラフィックを制御できます。データセンターと拠点を繋ぐ WAN がボトルネックになった場合には、拠点に Thunder シリーズを導入することで、クラウドサービス向け通信を直接インターネットに振り分けるローカルブレークアウトも実現できます。

また、情報漏えい防止の観点などから、組織内から個人アカウント等でクラウドサービスを利用されることを防ぐために、利用アカウントの制御（テナント制御）を行うことができます。SaaS 側でテナント制御の機能を提供しているものだけでなく、SSL/TLS 通信可視化を利用することで多様なクラウドサービスのテナント制御を実現できます。

認証・認可に基づく適切なアクセス制御

Thunder ADC/CFW シリーズは、リバースプロキシまたはフォワードプロキシとして動作し、Active Directory や LDAP 等との連携による認証・認可だけでなく、SAML2.0 や OpenID Connect、OAuth2.0 に対応した認証・認可、CAPTCHA を利用した認証などを行えます。ユーザー情報や属性情報に応じてきめ細かくリソースへのアクセス制御を実現し、ユーザー情報を含めたアクセスログを記録できます。

組織内向けサービスの高速な配信と可用性の向上

さらに、Thunder ADC/CFW シリーズにより、データセンター内の組織内向けサービスなどのサーバー負荷分散や TLS オフロードなどのアプリケーション配信最適化を実現できます。HTTP/2 のサーバー負荷分散や TLS1.3 のオフロードにも対応し、高速なアプリケーション配信を実現するとともに高いサービスの可用性を実現します。Web アプリケーションファイアウォールや L4 ファイアウォールによるセキュリティの強化も実現できます。Harmony Controller を用いることでアプリケーションの利用状況やレイテンシも可視化でき、サービスの問題点などへの迅速で効率的な対処を可能にします。

暗号化された通信に対するセキュリティの強化

ネットワークトラフィックの大部分が HTTPS を始めとする SSL/TLS を用いた暗号化通信となっている一方で、多くのサイバー攻撃でも不正ファイルのダウンロードや情報の窃取に SSL/TLS 通信が利用されています。Thunder CFW シリーズで利用できる SSL/TLS 可視化（SSL インサイト）ソリューションにより、暗号化通信を高速に復号し、セキュリティ機器での高速な検査を実現できます。一度復号することでインライン型（ファイアウォールや IPS など）・パッシブ型（サンドボックスや標的型攻撃防御製品、SIEM、フォレンジック製品など）・ICAP 連携型（URL フィルタリングやウィルススキャン / コンテンツ無害化 / データ損失防止など）のセキュリティ機器で並行した検査ができ、通信遅延も最小に抑えることができます。SSL/TLS 可視化により、サブディレクトリ以下の情報やペイロードも含めた詳細なアクセスログの取得も可能です。

IPsec-VPN によるセキュアな通信の実現

Thunder CFW シリーズでは標準で IPsec-VPN を利用でき、PC 端末やモバイル端末の OS の標準機能である IPsec-VPN クライアント機能を利用することでリモートアクセス／リモートワークの環境を実現したり（Client-to-Site IPsec VPN）、データセンター間や IaaS などのクラウドサービスとの間を広帯域な IPsec-VPN で接続（Site-to-Site IPsec VPN）することができます。接続時にユーザーと端末の双方が認証され、低レイヤでの通信暗号化により、通信プロトコルを問わないセキュアな通信が実現できます。

ネットワークセキュリティの強化

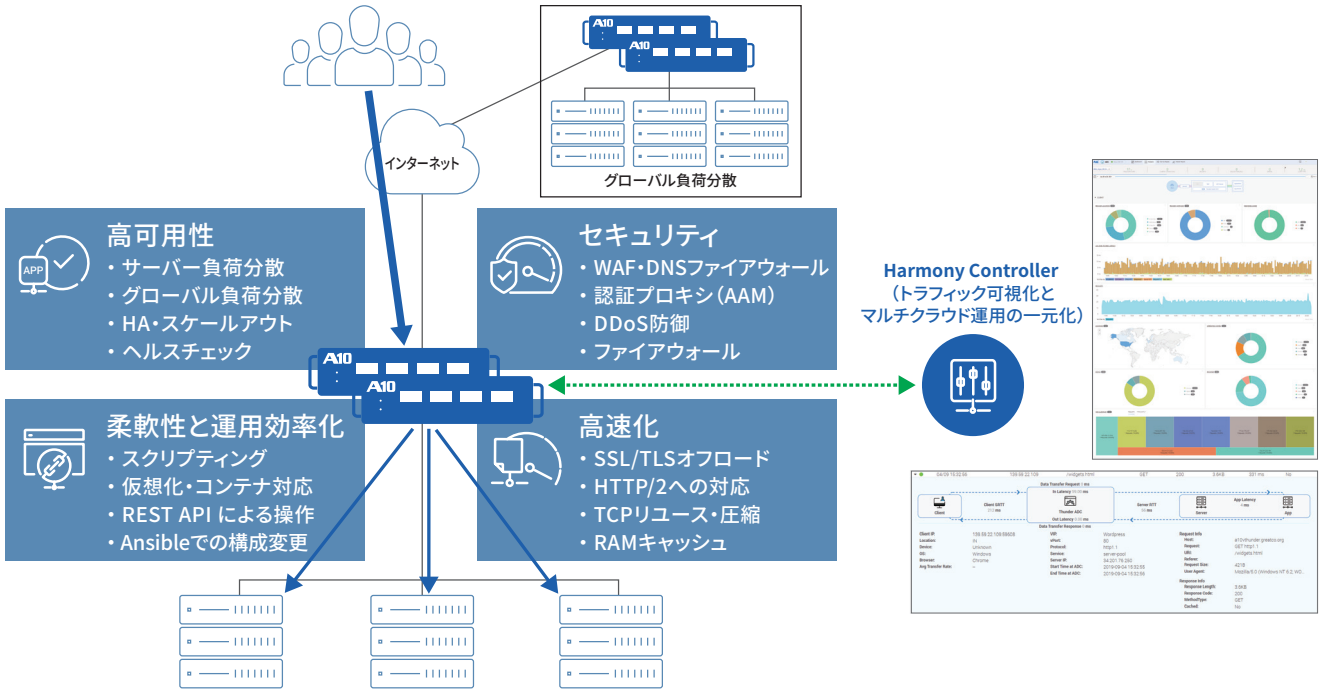
Thunder CFW シリーズでは標準で高性能な L4 ステートフルファイアウォールを利用できます。また、パケットを検査することでアプリケーションを識別してトラフィック制御を行うことも可能です。送信元 / 宛先の情報やアプリケーションの情報に基づいた帯域制御やレートリミットも適用できます。また、URL のカテゴリを指定して通信トラフィックの制御（フォワードプロキシの制御や SSL/TLS 可視化の実施可否などの制御）を行ったり、URL レピュテーションスコアや IP アドレスレピュテーションに基づくトラフィック制御を行うことも可能です。

また、Thunder TPS シリーズを利用することで、ネットワーク層からアプリケーション層までのマルチレイヤーに渡る DDoS 攻撃（マルチベクトル DDoS 攻撃）を検知・防御して正常通信のみを通すことができます。インターネットの出口に通常設置されるファイアウォールは帯域の大きくない DDoS 攻撃でも容易に停止させることができ、組織内からクラウドサービスの利用等が出来なくなってしまいます。オンプレミスでの DDoS 攻撃防御を行うことで、このような攻撃にも有効な防御を実現できます。

WEB事業者様向けソリューション

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

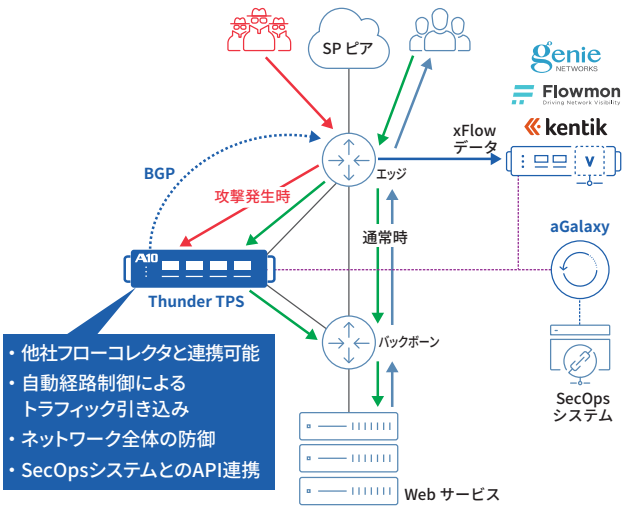
負荷分散と配信高速化、各種セキュリティ機能を集約。トラフィック可視化と運用自動化も実現



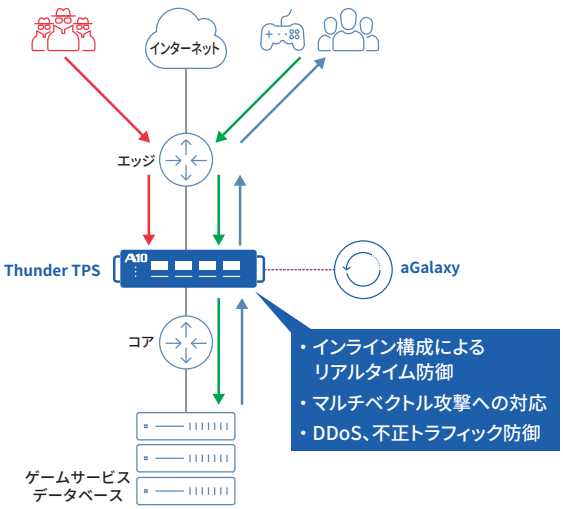
DDoS攻撃からの防御

多様なネットワークレイヤーでの攻撃から構成されるマルチベクトルDDoS攻撃からネットワークを防御

Webサービス：インフラの防御



ゲーム：プレイヤー体験の向上



WEB事業者様向けソリューション

アプリケーション配信の最適化とセキュリティ強化

Thunder ADC/CFWシリーズを利用することで、データセンター／プライベートクラウドやパブリッククラウド上の自社サービスのサーバー負荷分散やTLSオフロードなどのアプリケーション配信最適化を実現できます。1Uの専用ハードウェアアプライアンス1台で最大220Gbpsのスループット、1,050万秒間コネクション、2億5,600万同時コネクションを処理できる高い性能を有します。Thunderそのものの冗長化やスケールアウトも可能です。

HTTP/2のサーバー負荷分散やTLS1.3のオフロードにも対応し、高速なアプリケーション配信を実現するとともに高いサービスの可用性を実現したり、Webアプリケーションファイアウォールや統合されたL4ファイアウォールによるセキュリティの強化を実現できます。

Thunder CFWシリーズではアプリケーション配信機能にL4ファイアウォール機能が一元化されていることから、処理の高速化やラックスペースの効率的利用を実現します。

グローバル負荷分散の機能を標準で搭載しており、マルチクラウドに渡る災害対策やクライアントに最も近いサーバーからのコンテンツ配信なども可能です。サーバー負荷分散においてはスクリプティングにも対応し、トラフィックの中身に基づいたきめ細かなトラフィック制御を行えます。

DNSサーバーの前段に配置してDNS over HTTPSやDNS over TLSを容易に実現したり、DNSリクエストに対するアプリケーションファイアウォール機能によるセキュリティ強化も実現できます。

ユーザー認証プロキシとしてはActive DirectoryやLDAP等との連携による認証・認可だけでなく、SAML2.0やOpenID Connect、OAuth2.0に対応した認証・認可、CAPTCHAを利用した認証なども実現できます。アプリケーションレベルでのDDoS攻撃に対する防御も実現できます。

トラフィックの可視化と運用の効率化

管理ソリューションであるHarmony Controllerを用いることで、Thunder ADC/CFWを通過するWebサービスの利用状況やサーバー負荷分散を中心とした各トラフィックのレイテンシの詳細な内訳（クライアントとThunder間のレイテンシ、Thunder内部の処理時間、Thunderとアプリケーションサーバー間のレイテンシ、アプリケーションサーバー内での処理時間など）を可視化でき、Webサービスの問題点に対する迅速で効率的な対処を可能にします。

Harmony ControllerはマルチクラウドにIaaSや仮想化プラットフォーム、コンテナプラットフォームへのThunderシリーズのデプロイやライセンスの割り当て、構成変更、トラフィック可視化とアラート設定を一元的に実施できます。アラートの設定は多様なメトリクスに基づきEメールやWeb hookでの通知が可能で、状況に応じて自動的に特定のスクリプトを実行する等、運用の自動化や効率化を行うことができます。

ThunderシリーズはフォームファクタにかかわらずREST APIによるほぼ全ての機能の設定が可能であり、各種の運用ツールに容易に組み込むことができます。Ansibleのモジュールも多数提供しており、Ansibleを利用した構成変更も行うことができます

ネットワーク仮想化 / コンテナ化への対応

Thunderシリーズは専用ハードウェアアプライアンスだけでなく、サーバー仮想化プラットフォームでの利用やベアメタルでのインストール、コンテナプラットフォームでの利用、各種パブリッククラウドでの利用にも対応しています。仮想版でも1インスタンスあたり最大100Gbps、コンテナ版では最大180Gbpsのスループットに対応します。また、必要な帯域をプールで購入し、通信トラフィックに応じて帯域を柔軟にインスタンスに割り当てることができるライセンス体系も提供しており、ネットワーク機能の配置を最適化できます。

また、アプリケーションをKubernetesを利用したプラットフォームで提供する場合に、外部にあるThunderアプライアンスと連携するためのA10 Kubernetes Connectorのソリューションも提供しています。このソリューションを利用すると、A10 Kubernetes Connectorが、Kubernetes Cluster内のサービスを発見し、外部にあるThunderのサーバー負荷分散設定を自動的に更新することができます。

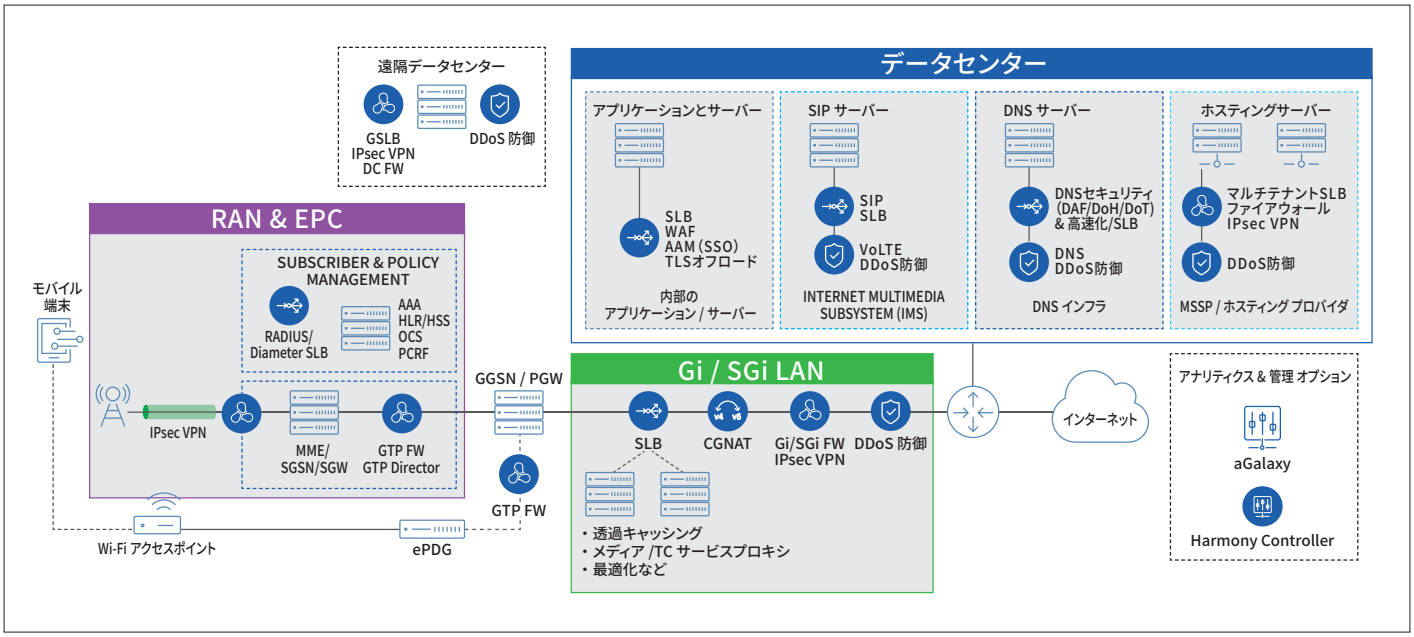
DDoS攻撃からの防御

Thunder TPSシリーズを利用することで、ネットワーク層からアプリケーション層までのマルチレイヤーに渡るDDoS攻撃（マルチベクトルDDoS攻撃）を検知・防御して正常通信のみを通すことができます。ネットワークの外部からの攻撃だけでなく、内部からの攻撃にも対応できます。管理ソリューションであるaGalaxyと連携することで、フローデータからDDoS攻撃を検知し、自動的に防御設定を変更できます。他社のフローコレクタとの連携も可能です。攻撃内容を分析するためのダッシュボードや高度なレポーティング機能も搭載されており、攻撃の状況を確認しながら対策を変更できます。

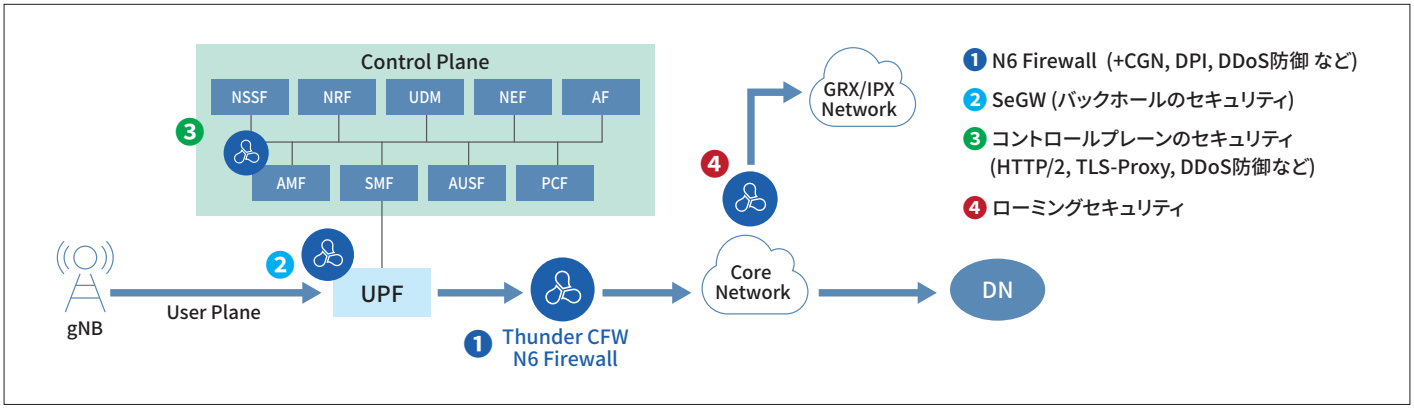
Thunder TPSは、機械学習を用いてボリューム型DDoS攻撃の内容を分析し、自動的に緩和フィルターを適用できるZAP（Zero-day Automated Protection <ゼロデイ自動保護>）機能が搭載されており、手動での作業なく迅速な防御を実現できます。不正なIPアドレスからの攻撃を防ぐために、50以上の提携セキュリティ機関から集めた3,100万以上の脅威IP情報を相関分析することにより、高い検知率でありながら誤検知が少なく、リアルタイムに更新されるIPレピュテーション情報も利用できます。

通信事業者様向けソリューション

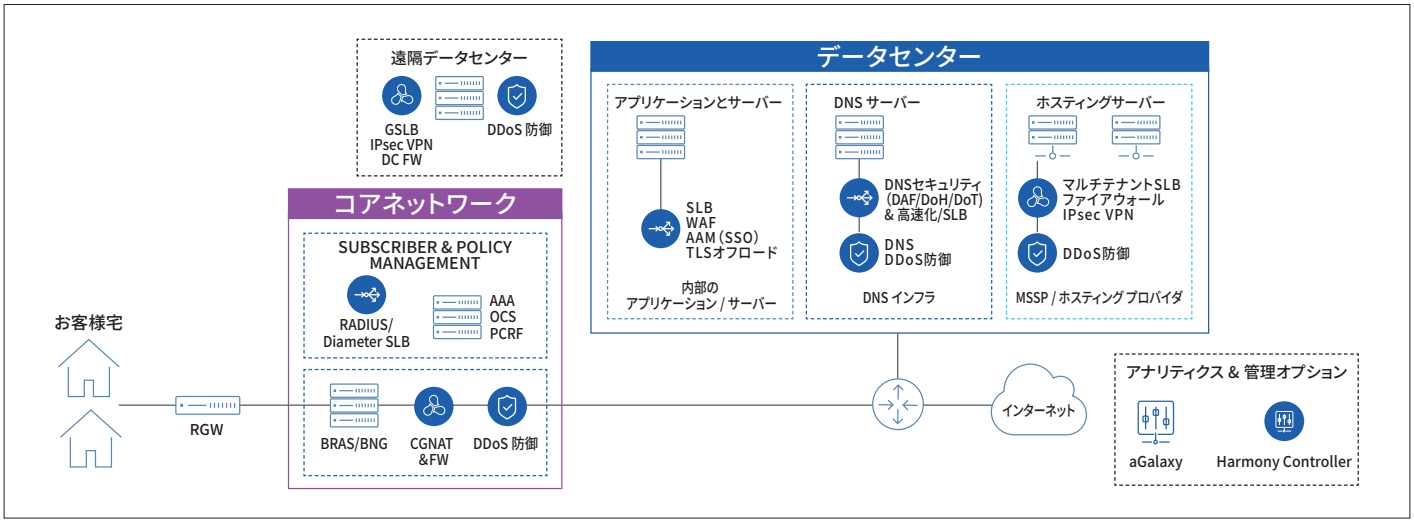
モバイル事業者様向けソリューションマップ（LTE/5G-NSA 向け）



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



通信事業者様向けソリューション

IPv4 枯渇対策とIPv6 移行

A10 のキャリアグレードNAT（CGN）ソリューションを利用することにより、IPv4 アドレスの枯渇に対応しつつ、IPv6 への移行を進めることができます。Thunder CGN シリーズは、パフォーマンスに優れたトランスペアレントなアドレス・プロトコル変換を提供するキャリアグレードのネットワークゲートウェイであり、1.5U の専用ハードウェアアプライアンス 1 台で最大 370Gbps 以上のスループットを実現できます。

Thunder CGN　は、CGN、DS-Lite、NAT64/DNS64、6rd、464XLAT、LW4o6、MAP-T、MAP-E などの様々なIPv6 移行技術を標準で提供し、NAT プールに対するDDoS 防御機能も持ちます。

CGN 機能などに各種セキュリティ機能が統合されたThunder CFW シリーズでは、IPv4/IPv6 双方の通信セッションに対するファイアウォール機能を提供するGi/SGi ファイアウォール機能などを利用でき、インターネットからの攻撃からモバイルネットワークや加入者を防御したり、加入者のIPv6 端末間での攻撃や不正アクセスを防御することもできます。

パケットコアの防御やGTP トラフィックの制御

Thunder CFW シリーズでは、GTP/SCTP ファイアウォール機能を標準で利用できます。不正なGTP/SCTP 通信の検査やレートリミットなどが可能で、不正なローミング先や端末からのGTP/SCTP を悪用した攻撃からモバイル事業者のネットワークを防御します。また、GTP トラフィックの内容に基づき通信を適切なゲートウェイに振り分けるためのGTP Director の機能を併せ持ち、モバイルネットワークのスライシングなどに利用できます。

広帯域のIPsec-VPN 機能により、バックホールの通信暗号化も実現できます。

DDoS 攻撃からの防御

Thunder TPS シリーズを利用することで、ネットワーク層からアプリケーション層までのマルチレイヤーに渡るDDoS 攻撃（マルチベクトルDDoS 攻撃）を検知・防御して正常通信のみを通すことができます。ネットワークの外部からの攻撃だけでなく、内部からの攻撃にも対応できます。

管理ソリューションであるaGalaxy と連携することで、フローデータからDDoS 攻撃を検知し、自動的に防御設定を変更できます。攻撃内容を分析するためのダッシュボードや高度なレポーティング機能も搭載されており、攻撃の状況を確認しながら対策を変更できます。

Thunder TPS は、機械学習を用いてボリューム型DDoS 攻撃の内容を分析し、自動的に緩和フィルターを適用できるZAP（Zero-day Automated Protection <ゼロデイ自動保護>）機能が搭載されており、手動での作業なく迅速な防御を実現できます。不正なIP アドレスからの攻撃を防ぐために、50 以上の提携セキュリティ機関から集めた3,100 万以上の脅威IP 情報を相関分析することにより、高い検知率でありながら誤検知が少なく、リアルタイムに更新されるIP レピュテーション情報も利用できます。

トラフィック制御と帯域制御

Thunder CFW シリーズを利用することで、通信トラフィックを適切なネットワークサービスにチェインするためのトラフィック制御を行ったり、送信元 / 宛先やアプリケーションの種別に応じた帯域制御やレートリミットを通信トラフィックに適用できます。利用者に応じて提供するネットワークサービスへ適切にトラフィックを振り分けることが可能です。

帯域制御 / レートリミット機能を用いると、P2P アプリケーションやトラフィック量の多い利用者に対するトラフィック制御を行ったり、ネットワーク攻撃を防御することができます。

アプリケーション配信の最適化

Thunder ADC/CFW シリーズを利用することで、データセンター内の自社サービス、DNS サーバー、ホスティングサーバーなどのサーバー負荷分散やTLS オフロードなどのアプリケーション配信最適化を実現できます。

HTTP/2 のサーバー負荷分散やTLS1.3 のオフロードにも対応し、高速なアプリケーション配信を実現するとともに高いサービスの可用性を実現したり、Web アプリケーションファイアウォールやL4/L7 ファイアウォールによるセキュリティの強化を実現できます。

DNS サーバーの前段に配置してDNS over HTTPS やDNS over TLS を容易に実現したり、DNS リクエストに対するアプリケーションファイアウォール機能によるセキュリティ強化も実現できます。

ユーザー認証プロキシとしてはLDAP 等との連携による認証・認可だけでなく、SAML2.0 やOpenID Connect、OAuth2.0 に対応した認証・認可、CAPTCHA を利用した認証なども実現できます。

ネットワーク仮想化 / コンテナ化への対応

Thunder シリーズは専用ハードウェアアプライアンスだけでなく、サーバー仮想化プラットフォームでの利用やベアメタルでのインストール、コンテナプラットフォームでの利用、各種パブリッククラウドでの利用にも対応しています。

仮想版でも 1 インスタンスあたり最大 100Gbps、コンテナ版では最大 180Gbps のスループットに対応し、キャリアグレードの性能を提供します。また、必要な帯域をプールで購入し、通信トラフィックに応じて帯域を柔軟にインスタンスに割り当てることができるライセンス体系も提供しており、ネットワーク機能の配置を最適化できます。

製品ラインナップ

		アプリケーション配信 Thunder ADC	IPv4枯渇対策/IPv6移行 Thunder CGN	DDoS防御 Thunder TPS	SSL可視化 Thunder SSLi	プロキシ/ファイアウォール Thunder CFW	DDoS対策管理 aGalaxy	マルチクラウド管理/可視化 Harmony Controller
ハードウェアアプライアンス	Thunder	●	●	●	●	●	●	
仮想アプライアンス	vThunder	●	●	●		●	●	●（ソフトウェア版）
ベアメタル	Bare Metal	●	●					
クラウドインスタンス	Public Cloud	●						●
コンテナ	Docker	●	●			●		

Thunder ADC/CGN

高速なサーバ負荷分散機能に加えてSSLアクセラレーションやセキュリティ機能を提供する製品です。
Thunder CGNは、IPv4枯渇問題を解決し、アドレスの延命とIPv6へのスムーズな移行を優れたコストパフォーマンスで実現します。

Thunder TPSシリーズ

1台で最大300Gbps, 440Mpps、クラスタ構成で最大2.4Tbpsまでの攻撃に対応し、大規模なマルチベクトル型DDoS攻撃からネットワークを防御する製品です。DDoS攻撃トラフィックを検知して、攻撃トラフィックを緩和し、正常トラフィックのみを通常ネットワークに転送する機能を持ち、様々な他社製フローコレクター製品とAPIで連携可能です。

Thunder SSLiシリーズ

SSL/TLSで暗号化されたトラフィックを高速に複合して、他社セキュリティ製品に転送し、再び暗号化してから宛先に転送することにより、SSLに隠れた脅威を検知しやすくすることができる「SSL可視化」機能に特化した専用アプライアンスです。

Thunder CFWシリーズ

A10が提供するADCやCGN、SSL可視化機能に加えて、ファイアウォール（以下FW）機能が搭載されたセキュリティアプライアンス製品です。
ADCやCGNにファイアウォール機能が統合されているため、管理ノードの削減を実現します。
ADCとFWを統合したDC FW機能と、CGN/IPv6とFWを統合したGi/SGi FW機能、セキュアWebゲートウェイ機能をサポートします。
Office 365などのクラウドアプリケーションを最適化するクラウドアクセスプロキシ機能や、SSL可視化機能もサポートしています。

aGalaxyシリーズ

DDoS攻撃の検知や、その攻撃内容に応じた適切な防御設定、攻撃状況の監視、レポーティングを行う管理アプライアンス製品です。
他社製品からのフロー情報やA10製品からの情報を基にDDoS攻撃を検知してThunder TPSに自動的に設定を投入し、攻撃を防御します。

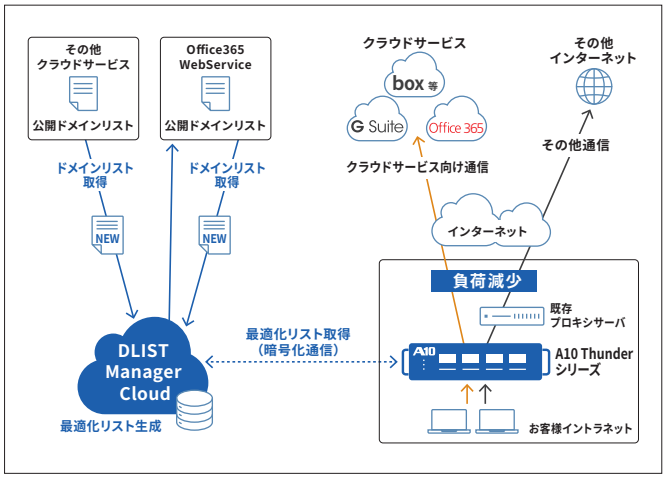
Harmony Controller

アプリケーション、セキュリティ、分析機能を一元管理できる、ハイブリッド・マルチクラウドに対応したソリューションです。
Thunderシリーズを管理可能です。

パートナーソリューション

Office 365ドメイン情報自動更新ソリューション

Office 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



富士通ネットワークソリューションズ株式会社

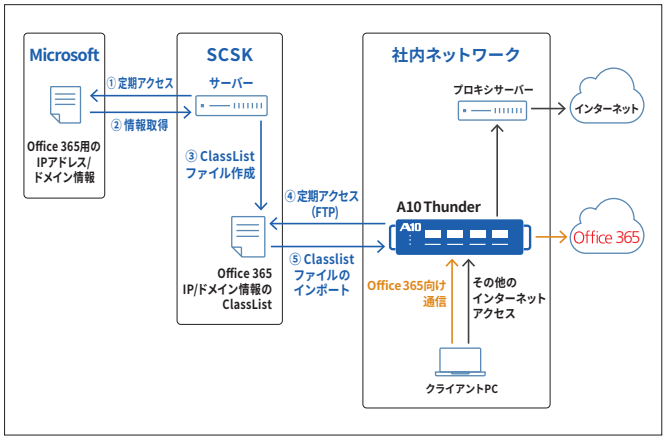
マルチクラウド時代のネットワーク最適化を実現

FUJITSU Network DLIST Manager Cloudサービス

クラウドサービスの活用は加速し、Office365といった情報系システムに加え、業務・基幹システムなど様々なクラウドサービスを活用するマルチクラウド時代に突入しています。複数のクラウドサービスの活用とセキュリティを両立するためには、トラフィックを適切にコントロールしていくことが必要不可欠です。

Fujitsu Network DLIST Manager Cloud サービスは、ドメインリスト自動更新によるOffice365トラフィックの振り分けに加え、Box、G suite、Windows updateなど複数のクラウドサービスに対応した他、お客様固有のクラウドサービスについても振り分けする機能を実装しました。さらに、ExpressRoute、サービス毎や3rd Partyサービス除外の振り分けにも対応し、IPのリストの提供も可能なため、クラウドサービスへの通信を、きめ細かくコントロールできます。

Fujitsu Network DLIST Manager Cloudで、お客様のマルチクラウド活用を、強力にサポートします。



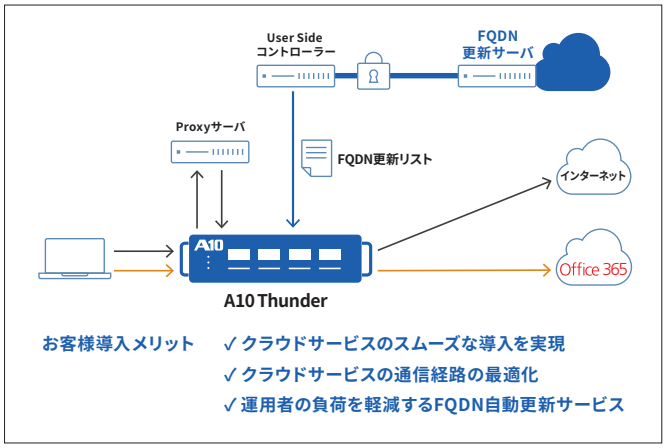
SCSK株式会社

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

Office 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Office365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。



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

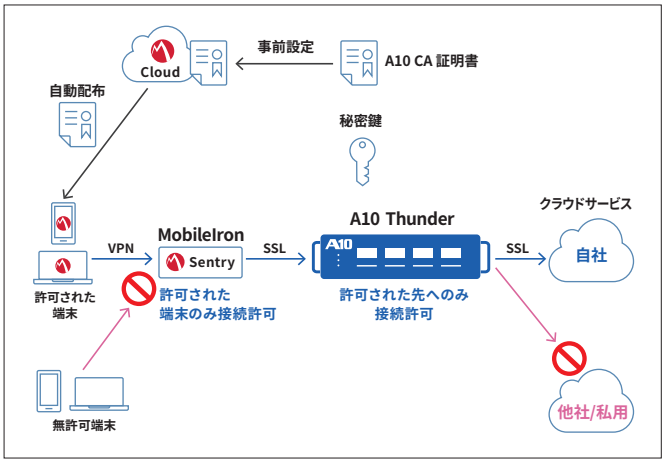
クラウドサービスアクセス時のProxy環境改善

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柔軟に対応することや、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。

パートナーソリューション

A10 の販売パートナーが提供するソリューションを紹介します。 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



株式会社日立ソリューションズ

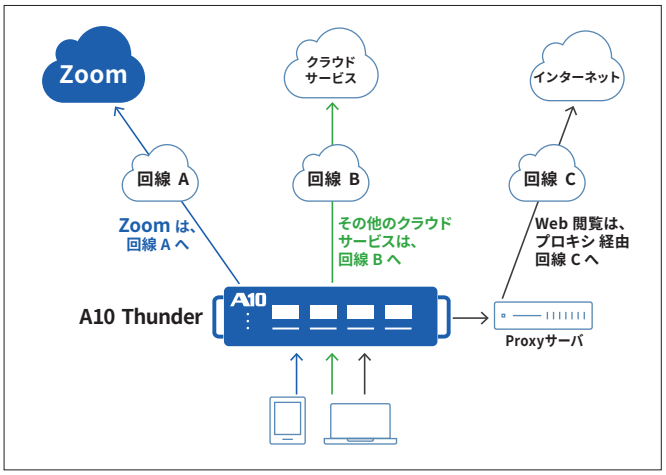
デバイス認証とアカウント認証の組み合わせによるクラウド内情報資産の漏えい防止

モバイルデバイスからクラウドサービスへのテナント制御の実現

MobileIronはデバイス認証によってPCやモバイルデバイスを使った社外からのアクセスを統制するMDM/EMM[*1]製品です。A10 Thunderとの組み合わせにより、社外からのアクセスに対してもクラウドサービスに対するテナント制御を適用し、情報漏えいを防ぐ強力なセキュリティを実現します。

MobileIronは、テナント制御時にA10のSSLインサイトで必要となるCA証明書をモバイルデバイスに自動配布する機能も備えており、運用の効率化にも力を発揮します。

[*1] MDM/EMM:Mobile Device Management/Enterprise Mobility Management



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。

ソリューション提供：

三井情報株式会社

〒105-6215 東京都港区愛宕2-5-1
愛宕グリーンヒルズMORIタワー
ソリューションURL:
https://www.mki.co.jp/solution/m-anvo.html

株式会社日立ソリューションズ

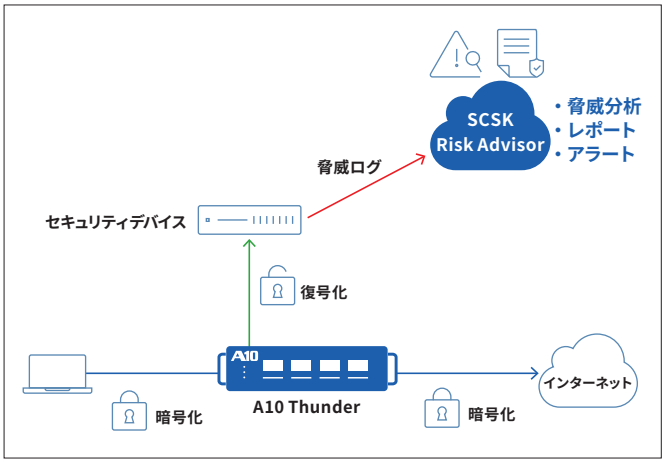
セキュリティソリューション第1部
〒140-0002 東京都品川区東品川4−12−7
日立ソリューションズタワーA
TEL: 03-5780-2273
hs-a10@ml3.hitachi-solutions.com
ソリューションURL:
https://www.hitachi-solutions.co.jp/a10/

NEC ネッツエスアイ株式会社

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

A10の販売パートナーが提供するソリューションを紹介します。 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



SCSK株式会社

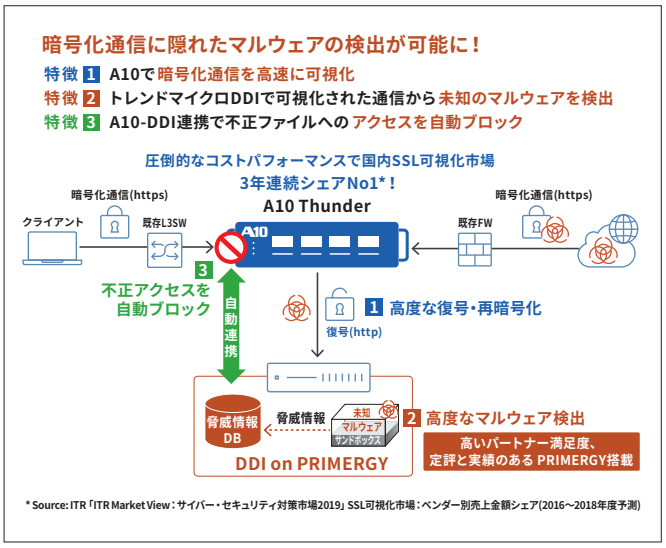
SSL可視化の効果を可視化するトライアルサービス

ASAS（A10 SSLインサイト・アセスメント・サービス）

常時SSL化が急速に進む中、SSLを復号しセキュリティ検査を行う「SSL可視化」の重要性が高まっており、A10 ThunderによるSSLインサイトソリューションの導入を検討する組織も急速に増加しています。一方で暗号化通信を可視化しないことでどれくらいの脅威を見逃しているのか、つまり可視化の効果が分かりづらいという顧客の声も数多く寄せられています。

SCSKが提供する「ASAS（A10 SSLインサイト・アセスメント・サービス）」は、SSL可視化の効果を可視化するトライアルサービスです。

本サービスでは、A10のSSLインサイトをトライアルで導入いただき、SCSKの簡易SOCサービス「Risk Adviser」にて脅威分析、レポーティングを実施することで、SSL可視化の前後を比較することが可能です。



富士通ネットワークソリューションズ株式会社

常時SSL化時代のセキュリティ運用を実現！

DDI on PRIMERGY 連携

インターネットWeb通信の安全性を担保する、常時暗号化時代に突入しています。一方で、正常な通信に見せかけた、悪意の攻撃者による通信も暗号化されており、従来のセキュリティ対策機能では検知することができません。

このような問題を『A10 Thunder』のSSLインサイト機能と、トレンドマイクロ社の『DDI(Deep Discovery™ Inspector)』による連携で解決します。

A10 Thunderで復号したWeb通信を、DDIの持つ高度脅威検出エンジンを用いて、未知の脅威までも検出します。更に、検出した脅威サイトへの自動ブロックまでを実現することで、運用負荷の軽減やマルウェアの拡散防止に効果を発揮します。

DDIのハードウエアには、2019年満足度No.1を獲得した信頼性の高い富士通サーバ(PRIMERGY)を採用し、ワンボックスモデル(DDI on PRIMERGY)として提供します。
安心の充実した運用サポートなど、ワンストップで、お客様の安心・安全なインターネット利活用をサポートします。

ソリューション提供：

SCSK株式会社

プラットフォームソリューション事業部門
ITプロダクト＆サービス事業本部
ネットワークセキュリティ部
〒135-8110 東京都江東区豊洲3-2-20 豊洲フロント
TEL: 03-5859-3037　FAX: 03-5859-3106
A10-info@ml.scsk.jp

富士通ネットワークソリューションズ株式会社

総合受付窓口 TEL:0120-20-7430
受付時間：9:00-17:00(※祝祭日・年末年始除く)
https://www.fujitsu.com/jp/fnets/contact/
ソリューションURL： DLIST Manager
https://www.fujitsu.com/jp/group/fnets/products/a10/a10-relation.html
ソリューションURL： DDI on PRIMERGY
https://www.fujitsu.com/jp/products/software/partners/partners/trendmicro/products/network/#DDI

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)

■ 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
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
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
南アルプス市
鳥取市

■ 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

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-leaning/

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。

www.a10networks.co.jp/
Facebook: http://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

©2021 A10 Networks, Inc. All rights reserved. A10 ロゴ、A10 Networksは米国およびその他各国における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 2021 APR 2021