5Gで変わる高速・大容量 ネットワークサービスとセキュリティ

A10ネットワークス株式会社
高木　真吾

A10

Always Secure. Always Available.

A10ネットワークスについて

A10 Networks, Inc. (NYSE: ATEN)

- 設立：2004年9月
- 代表者：Dhrupad Trivedi (CEO)
- 本社所在地：米国カリフォルニア州サンノゼ
- 2014年 ニューヨーク証券取引所（NYSE）に上場

A10ネットワークス株式会社

- 設立：2009年4月
- 代表者：川口 亨
  (日本法人代表兼社長 米国本社ヴァイス プレジデント兼務)
- 拠点：東京、大阪、名古屋

シリコンバレー発
グローバル企業

拠点のある国
27

従業員数
800(日本: 70+)

世界のリーディング企業で採用

製品・サポート提供先の国
117+

導入社数
8,000+

ハイパフォーマンスなネットワークアプライアンス製品により
セキュリティ・アプリケーション配信機能等を提供

A10のお客様

Microsoft社の大規模サービスを支える技術

135,000,000 ユーザー

6,000,000 組織
40データセンター
36グローバルリージョン

48,000,000 ユーザー

圧倒的なスケールでセキュリティを確保

A10製品について

Always Secure. Always Available.

5

A10の独自OS：ACOS <エイコス>

(Advanced Core Operating System)

- マルチコアCPUによる完全並列処理で高いパフォーマンスを実現
- 共有メモリアーキテクチャにより大量のセッションを制御可能

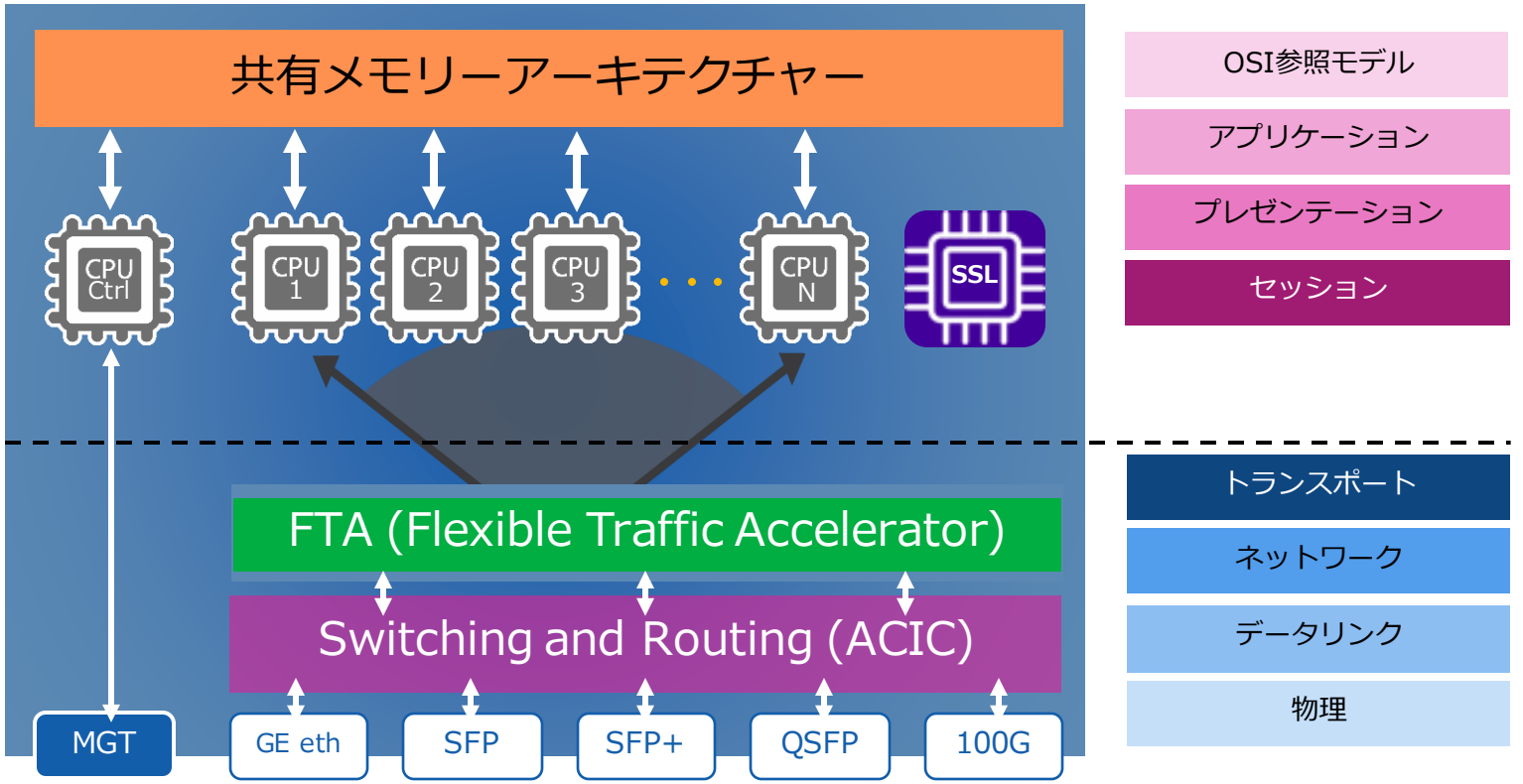
共有メモリアーキテクチャ
複数のCPUコアがメモリ空間を共有。
CPU間通信をゼロにすることによりCPUの性能を最大化

迅速な拡張性への約束 (HW依存関係なし)
汎用CPUを利用したソフトウェアプラットフォームにより、修正や新機能の実装が容易

CPU制御処理の分離
コントロールとデータ処理を完全分離することによる信頼性向上、データ処理能力の最大化

SSL処理 (CPU負荷軽減)
最新の暗号化処理専用ハードウェアにより、業界最高速のSSL/TLS処理性能を実現し、CPUの負荷をオフロード

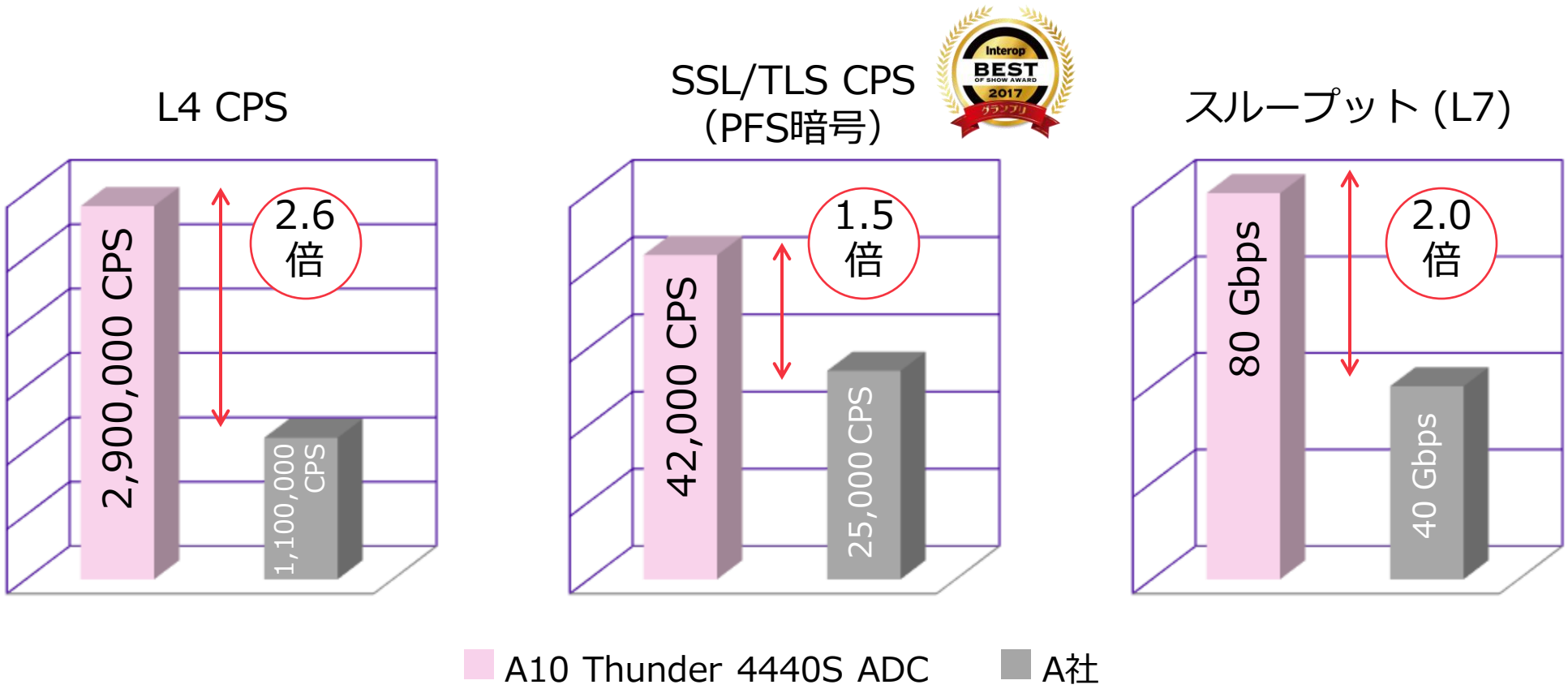
ASIC/FPGAによる処理 (CPU処理効率化)
レイヤ2/3/4の処理やDDoS防御等のセキュリティ機能を複数の専用ASIC/FPGAにオフロードし、CPUをアプリケーショントラフィック処理に集中



5Gに必須な「高速大容量」「高信頼・低遅延通信」「多数同時接続」に最適

※同価格帯の他社製品と比較

ACOSによる高いパフォーマンス



余裕のあるパフォーマンスによりピーク時トラフィックにも対応可能

ACOSを搭載したThunderシリーズ

サーバー負荷分散	IPv4枯渇対策(CGNAT)	DDoS防御	SSL可視化
サイト間冗長/負荷分散	IPv6 移行機能	WAF	IPレピュテーション
回線負荷分散	Gi/SGi FW	Webプロキシ	IPSec VPN
SSLアクセラレーション	GTP FW	ステートフルFW	O365高速化
IPv4 –v6負荷分散	VxLAN/NVGRE GW	URLフィルタリング	認証プロキシ

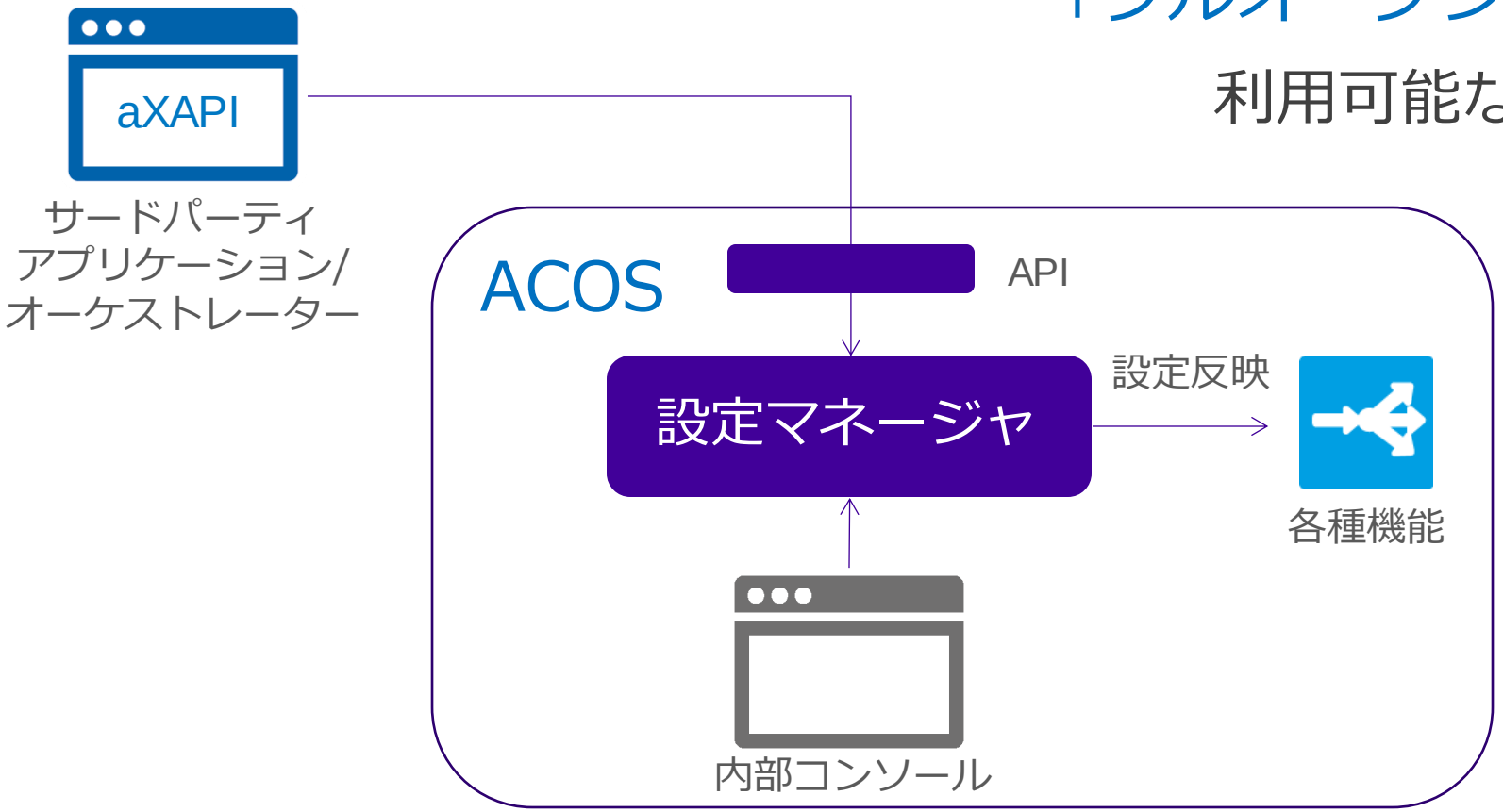
Thunderシリーズ

豊富なアプリ制御 / ネットワーク / セキュリティ機能を
１ボックス・１ライセンスで提供

ACOSのAPI機能– プログラマビリティ

「フルオープンAPI」

利用可能な機能を外部から操作可能



より多くの機能を対象に自動化を実装可能・SDN環境に最適

A10ソリューションの提供形態

あらゆるクラウド

プレイベートクラウド

ORACLE CLOUD

Microsoft Azure

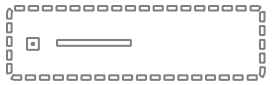
Google Cloud Platform

aws

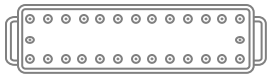
IBM Cloud

あらゆるプラットフォーム

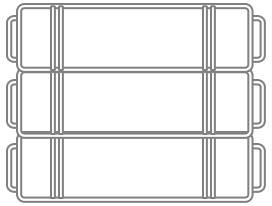
アプライアンス



仮想アプライアンス



ベアメタル



コンテナ

あらゆるライセンスモデル

- サブスクリプションライセンス
- パーペチュアルライセンス
- FlexPool™ライセンス

あらゆる環境・運用に対応できる柔軟な提供形態を実現

A10の製品ポートフォリオ

aGalaxy
(TPSの管理)

Harmony Controller
(マルチクラウド, マルチサービスのトラフィック可視化と管理)

セキュリティ

Thunder TPS

- DDoS防御
- DDoS検知
- 高度な
  レポーティング
- 脅威
  インテリジェンス
- 機械学習による
  防御

Thunder CFW

- ADC/CGNの全機能
- SSL通信の可視化と
  多様なセキュリティ
  製品との連携
- URL
  フィルタリング
- 脅威インテリジェンス
- L4/L7
  ファイアウォール
- Gi/SGi
  ファイアウォール
- GTP/SCTP
  ファイアウォール
- IPsec-VPN

アプリケーション配信

Thunder ADC

- 高度な負荷分散
- SSLオフロード
- 広域負荷分散
- WAF/DNS防御
- セキュア
  サービスメッシュ
- DNS防御/DoH/DoT
- フォワードプロキシ

Thunder CGN

- キャリアグレード
  NAT
- IPv4枯渇対策
- 多様なIPv6移行
  技術への対応

通信事業者様向けソリューション

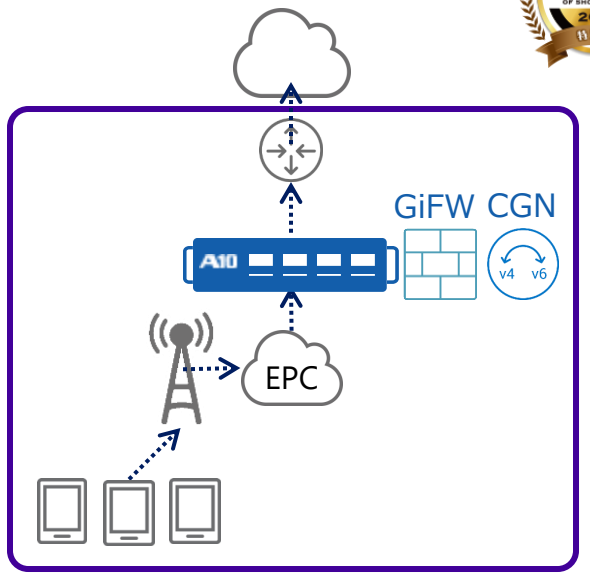
Always Secure. Always Available.

12

Thunder CFW (Convergent Firewall)

Gi/SGiファイアウォール（Gi/SGi FW）

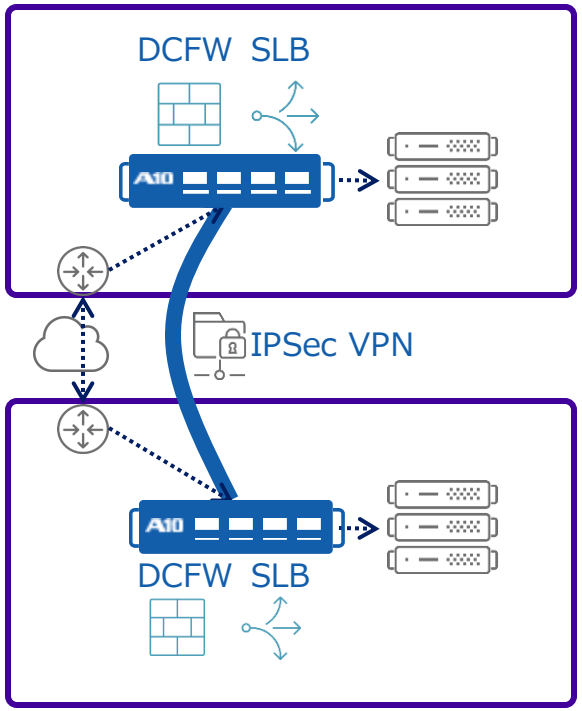
- CGNとFW機能を統合しモバイル通信事業者のNWを防御
- モバイル通信網とデータセンターを繋ぐ多様なソリューション提供を可能に



モバイル通信プラットフォーム

FWとADCをワンボックスに統合

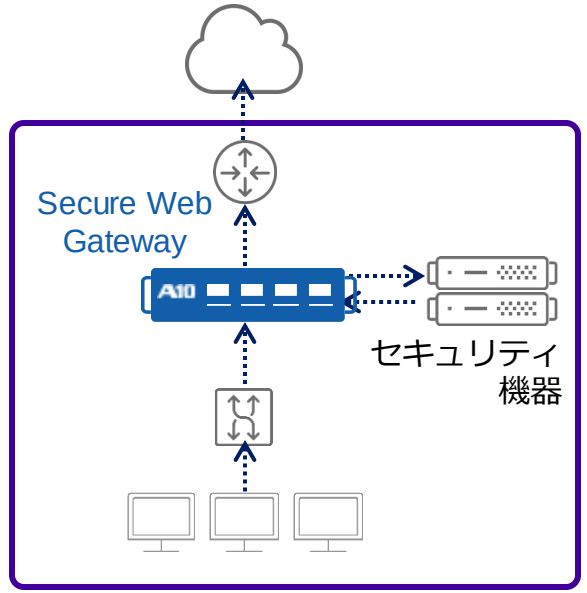
- 運用を効率化
- IPSec VPNによる拠点間接続



エンタープライズ/データセンター

セキュアWebゲートウェイ（SWG）

- FWやSSL可視化により
  エンタープライズのセキュリティを強化
- クラウドサービスの利用を円滑化
  （クラウドプロキシ）

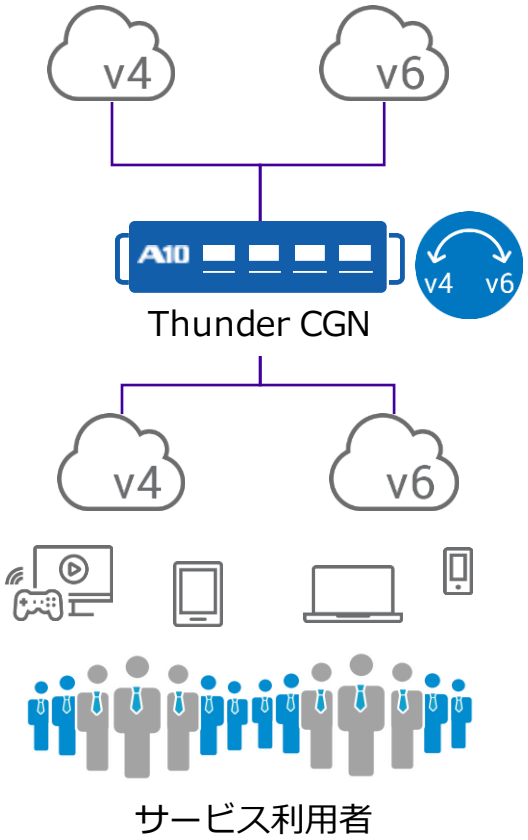


エンタープライズ

CGN・ADC・SSL可視化・FW機能を集約したセキュリティプラットフォーム

IPv4枯渇対策/IPv6移行

IPv4枯渇対策/IPv6移行を実現するキャリアグレードNATソリューション

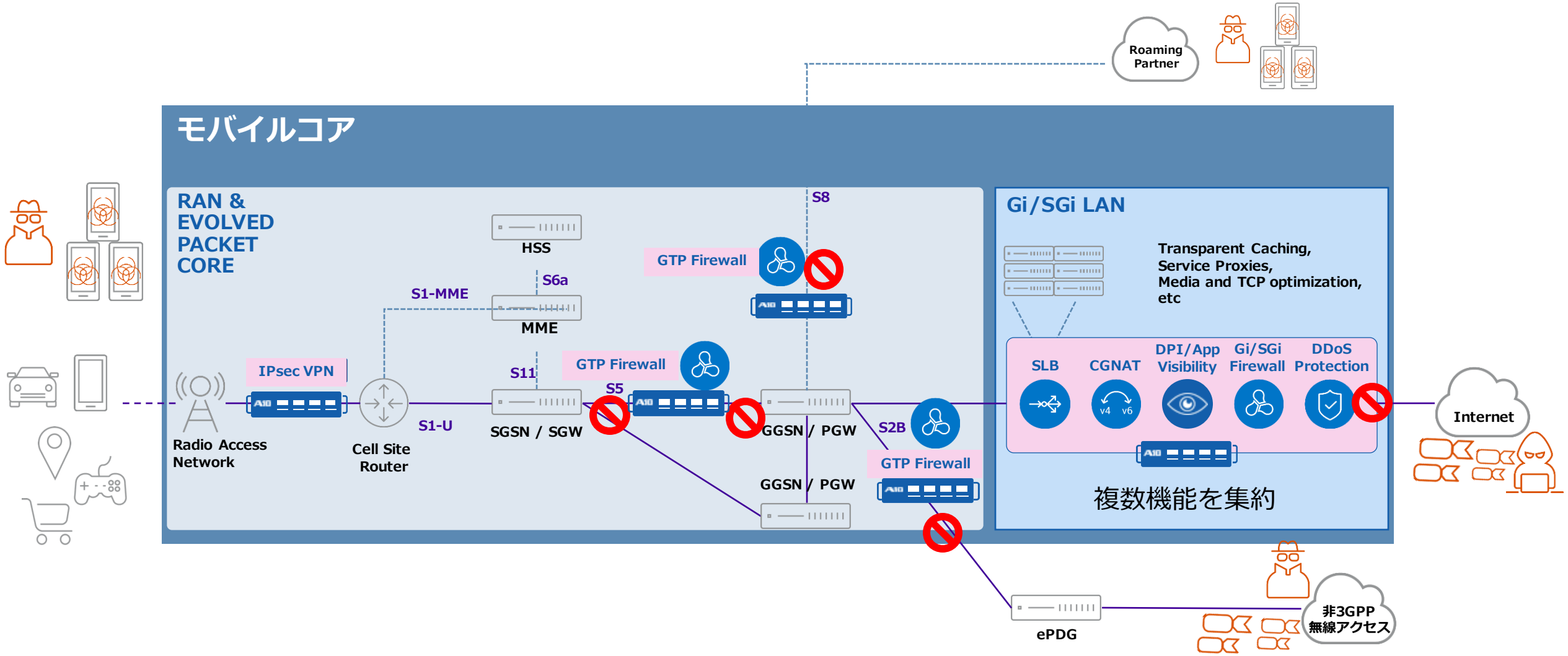


NAT44
6RD
NAT64/DNS64
DS-Lite
LW-4o6
MAP-E
MAP-T
464XLAT
CGNAT(LSN)

- 国内・海外における通信事業者の商用実績
- 圧倒的な大容量（最大同時接続数5億1200万）
- 多くのIPv6移行技術をサポート
- 不足しているIPv4アドレスあたりの加入者集約率を拡張 (CGNAT)
- 全機能標準搭載・同時使用可能
- 充実したグローバルIP宛のセキュリティ対策
- 高いコストパフォーマンス
- 他社と比べ2倍～4倍の性能と最大8倍の価格アドバンテージ

豊富な商用実績を持つ信頼性の高いCGNAT/IPv6移行実現

モバイルコア向けセキュリティ機能



セキュリティ・トラフィック制御機能を集約可能

Thunder CFWシリーズ（通信事業者様向け）

エントリ	ミッドレンジ	ハイエンド
		
Thunder 3040 | 30 Gbps	Thunder 5840 | 100 Gbps	Thunder 7650 | 370 Gbps, 100GbE
		
Thunder 1040 | 20 Gbps	Thunder 5440 | 90 Gbps	Thunder 14045 | 300 Gbps, 100 GbE
		
Thunder 940 | 5 Gbps	Thunder 4440 | 70 Gbps	Thunder 7440-11 | 220 Gbps, 100 GbE
		
vThunder | 200M - 100 Gbps		Thunder 6440 | 150 Gbps

通信事業者の5G用設備を支援

SAN JOSE, Calif. – August 15, 2018 – A10 Networks (NYSE: ATEN), a provider of intelligent and automated cybersecurity solutions, today announced a major Japanese mobile carrier has selected the A10 Thunder® Convergent Firewall (CFW) Gi/SGi firewall solution for their 5G pilot network, to complement the massive capacity demands of their existing mobile network and help lay the foundation for the mobile carrier's 5G production network, expected to become commercially available beginning in 2020.

A10 Networks has enjoyed a long-standing relationship with this customer, who has previously deployed our solutions to deliver a variety of security and networking services, such as application delivery, IPv4 preservation/IPv6 migration technologies, DDoS protection and Threat Intelligence. A10's expanded relationship includes the Thunder CFW Gi/SGi firewall 5G-GiLAN solution to scale and secure its GiLAN, and which will serve as the backbone network for data communication services of the carrier's 5G network.

"We continue to work very closely with global carriers to enable them to lead the way with their 5G rollouts. This is demonstrating our trusted partnership and continued leadership to help carriers accelerate network transformation to 5G," said Lee Chen, CEO of A10 Networks. "The A10 Thunder CFW provides service providers with a highly scalable, consolidated and secure 5G-GiLAN solution for a comprehensive network defense, with automation for improved business agility, faster network rollout and overall reduction of TCO".

The customer selected the A10 Thunder CFW 5G-GiLAN solution to accelerate its 5G pilot deployment due to

- Comprehensive 5G mobile core protection with the A10 Thunder CFW's GiFW and CGNAT
- Ease-of-use and simplified operations through [illegible] and intuitive management

SAN JOSE, Calif. – July 19, 2018 – A10 Networks (NYSE: ATEN), a provider of intelligent and automated cybersecurity solutions, today announced an Asian Tier-1 mobile service provider has selected the A10 5G-GiLAN™ solution for its next-gen 5G-ready network rollout. The service provider is leveraging the Gi/SGi firewall and advanced network translation components to provide the scale and security needed to meet the demands of its 5G infrastructure rollout and IoT adoption.

As the service provider plans to rapidly commercialize 5G services beginning early in 2019, they needed a consolidated security and networking solution to seamlessly integrate with its vEPC platform. It also required the solution to address rising IPv6 demands by supporting IPv4 to IPv6 network interoperability in their network.

"We are pleased to have been selected by the Tier-1 provider in a highly competitive bake-off. The fast-approaching rollout of 5G networks around the world represents a dramatic transformation in mobile services, including exciting new revenue opportunities for service providers," said Lee Chen, CEO of A10 Networks. "However, it will also elevate the breadth and sophistication of IP-based threats facing carriers and their customers. The A10 5G-GiLAN solution plays a major role in helping service providers simplify, scale and secure their 5G deployments. We are currently working with many Tier-1 providers who are seeking next-generation security and networking solutions for 5G."

The customer selected the A10 Thunder® CFW 5G-GiLAN solution to accelerate its 5G deployment with the following capabilities:

- Comprehensive 5G mobile core protection with the A10 Thunder CFW GiLAN consolidation of GiFW and CGNAT solution.
- Proven capabilities to enable CGNAT and GiFW, simultaneously with IPv6 migration technologies (NAT64, 464XLAT) on the same device, as well as advanced reliability and feature-rich ALG support.
- Sustained scalability, performance [illegible] two leading competitors, resulting in [illegible] of ownership (T[illegible]

既に複数の5G関連ネットワークプロジェクトで採用

5Gの用途

低遅延 (>1ms)

高密度(100x)

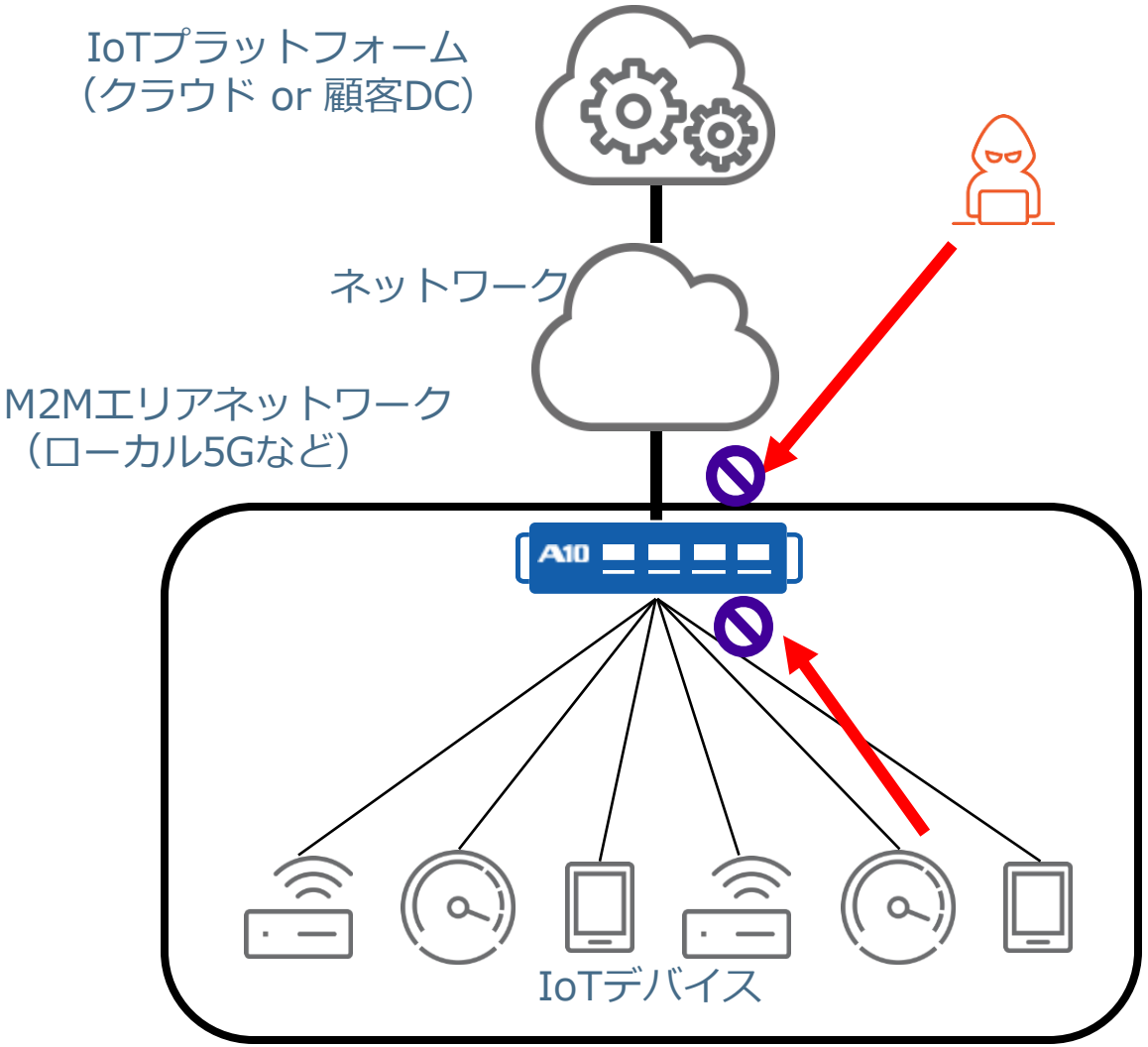
高帯域(20Gbps)

通信クライアントの主役は
人からモノへ

交通	産業	モビリティ	サービス
交通制御 自動運転 公共交通システム	スマート農業 スマートホーム スマートファクトリー	ウルトラハイスピード コネクティビティ イベントエクスペリエンス AR / VR	ヘルスケア 監視・モニタリング 公衆安全 緊急対応

通信インフラのセキュリティがますます重要になる

IoTデバイスのセキュリティリスク

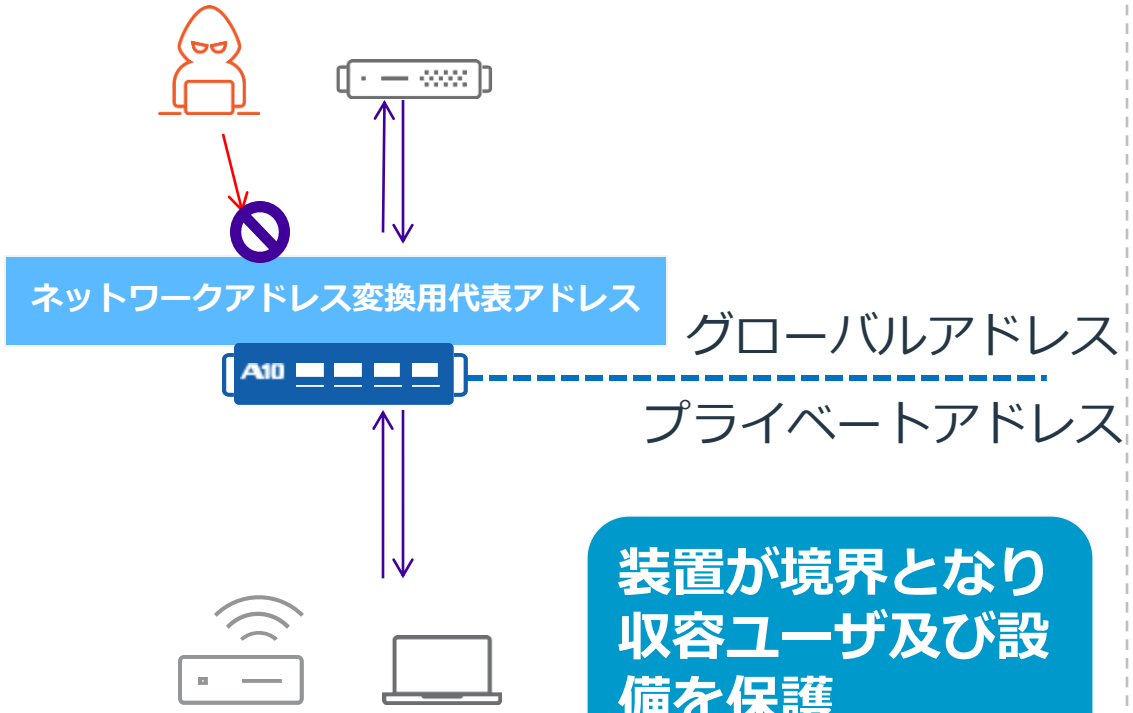


- 外部からのIoTデバイスへの侵入・DDoS攻撃からの防御
- マルウェア感染デバイスなどによる不正サーバへのデータ漏えい
- 暗号化通信による不正な活動の隠蔽

ゲートウェイ装置によるセキュリティ機能を有効活用

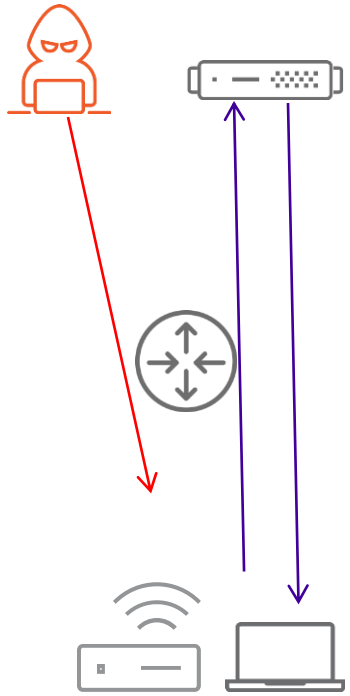
IoT機器のセキュリティリスク – IPv6

IPv4ネットワークの場合



装置が境界となり収容ユーザ及び設備を保護

IPv６ネットワークの場合

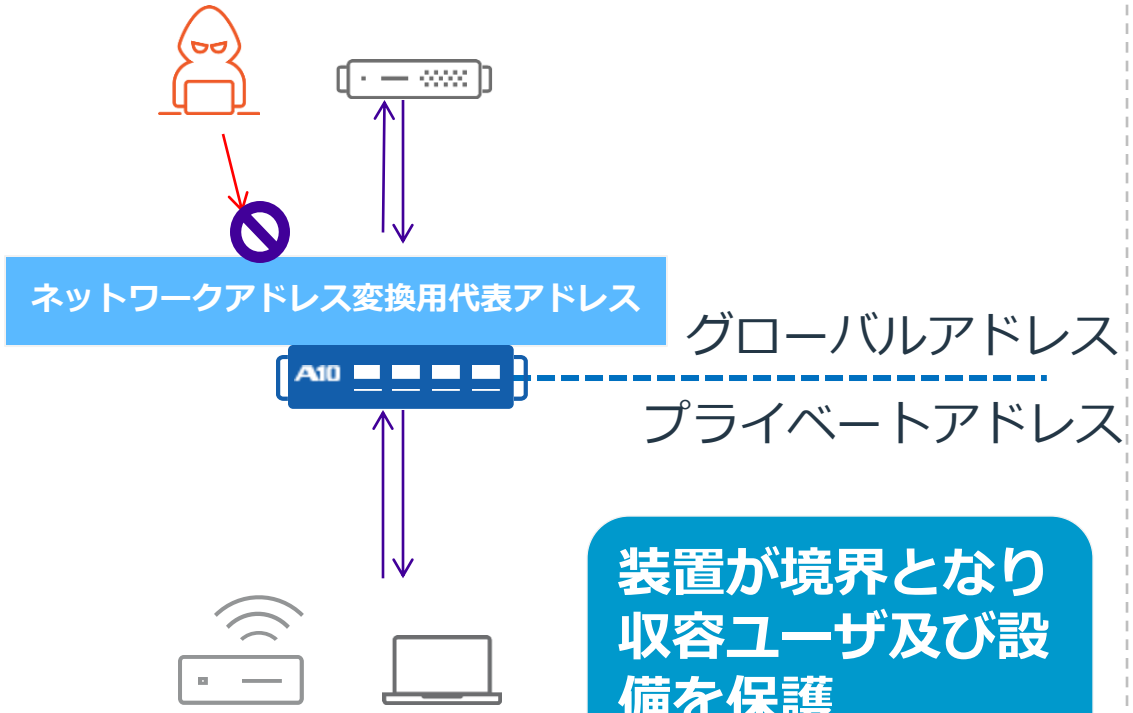


境界がないため外部からの悪意のあるトラフィックを通してしまう可能性がある

IPv6 Firewallによるセキュリティの確保が必要

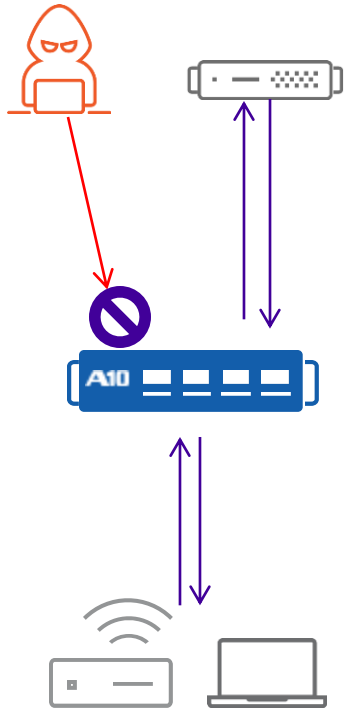
IoT機器のセキュリティリスク – IPv6通信制御

IPv4ネットワークの場合



装置が境界となり収容ユーザ及び設備を保護

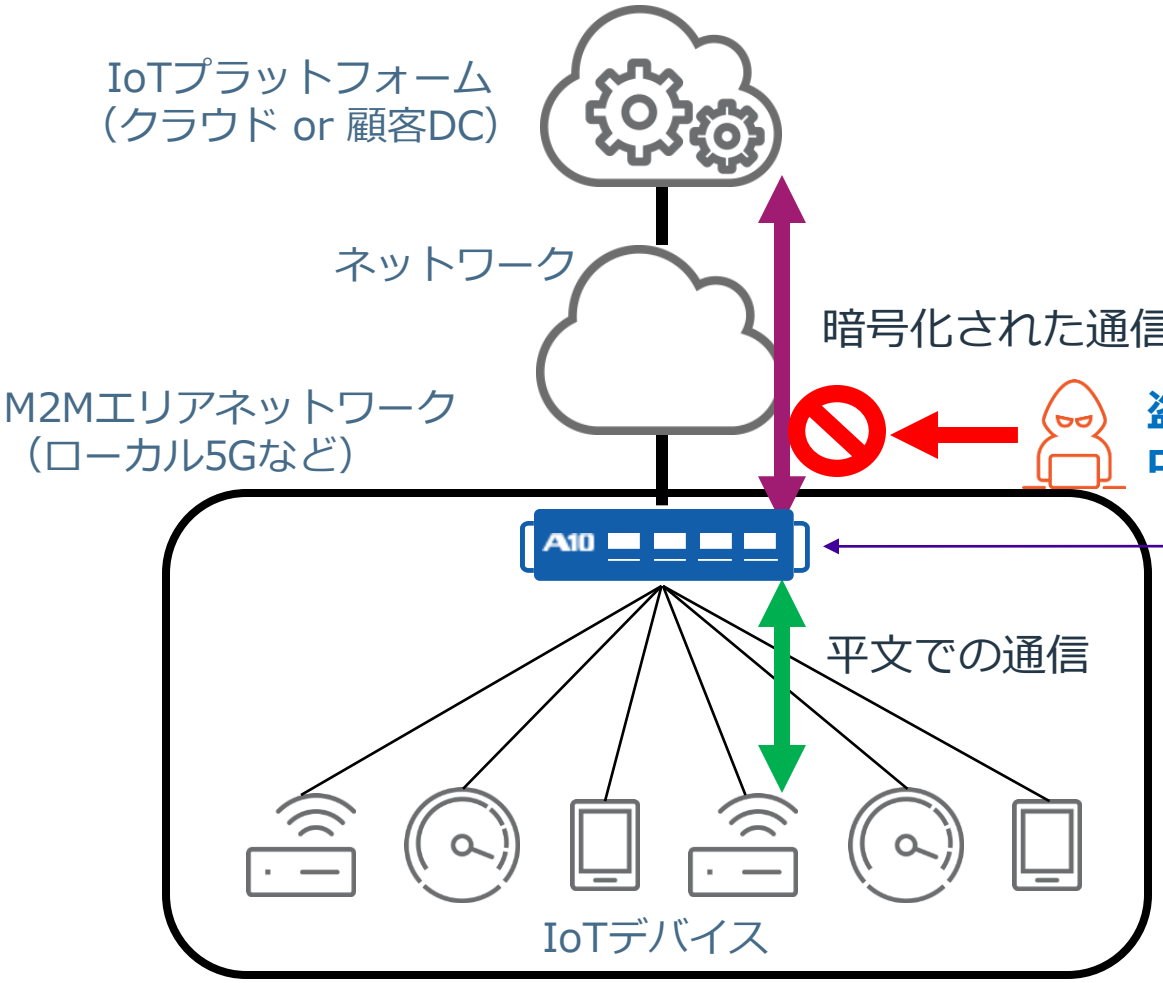
IPv6ネットワークの場合



通信状況をモニタし、内部から発信された通信のみ許可

IPv6でもIPv4と同じセキュリティレベルを提供

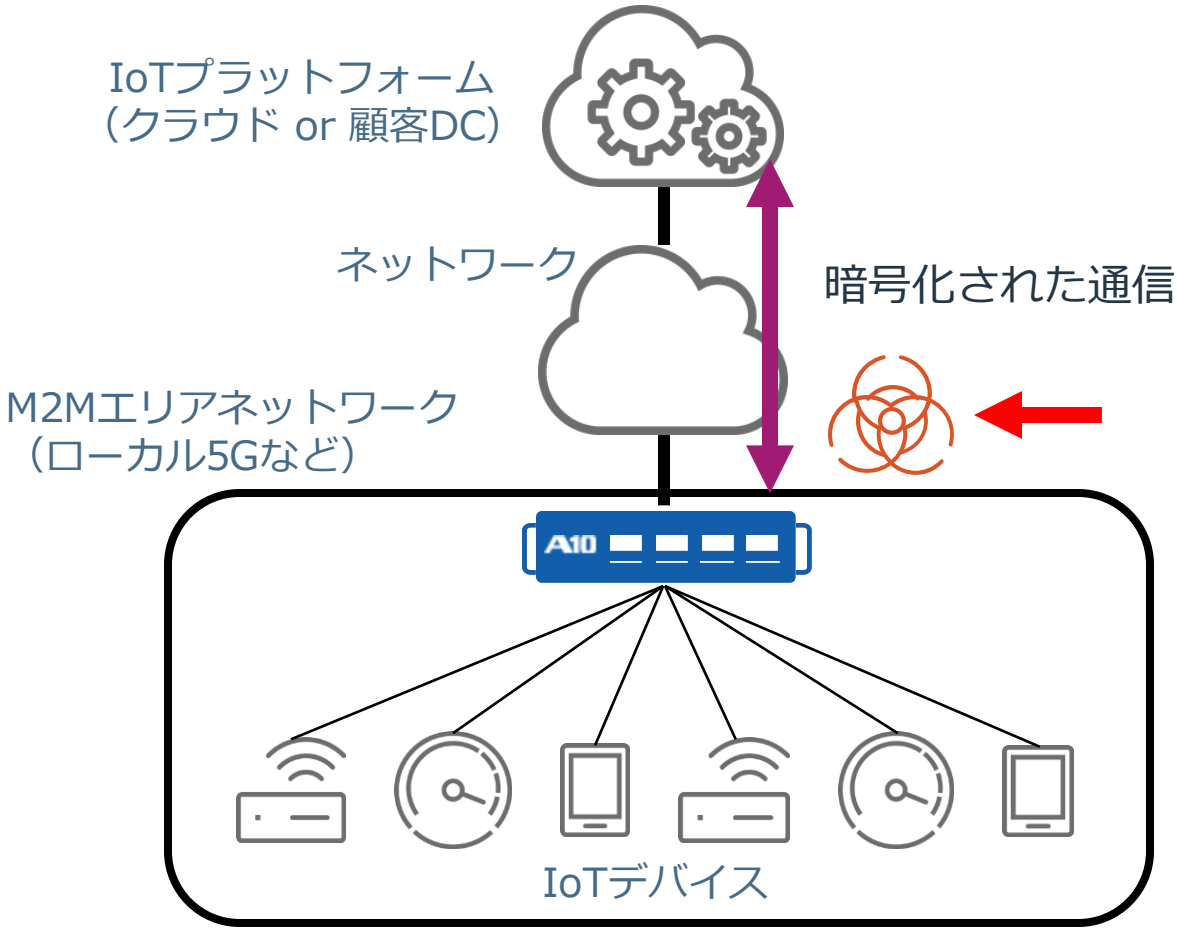
通信データの暗号化によるセキュリティ強化



- SSL/TLSやIPSec-VPNによる通信データの暗号化

IoTデバイスに安全な通信環境を提供

暗号化通信に隠れた脅威



通信のほとんどを占める暗号化通信により、
隠蔽された脅威

暗号化通信の可視化ソリューションの検討

政府機関向けのセキュリティ対策として「データの復号」が必要に

内閣サイバーセキュリティセンター(NISC) サイバーセキュリティ戦略本部
政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）
https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf

(2) 情報システムのセキュリティ要件の策定

(a) 情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否を判断した上で、以下の事項を含む情報システムのセキュリティ要件を策定すること。

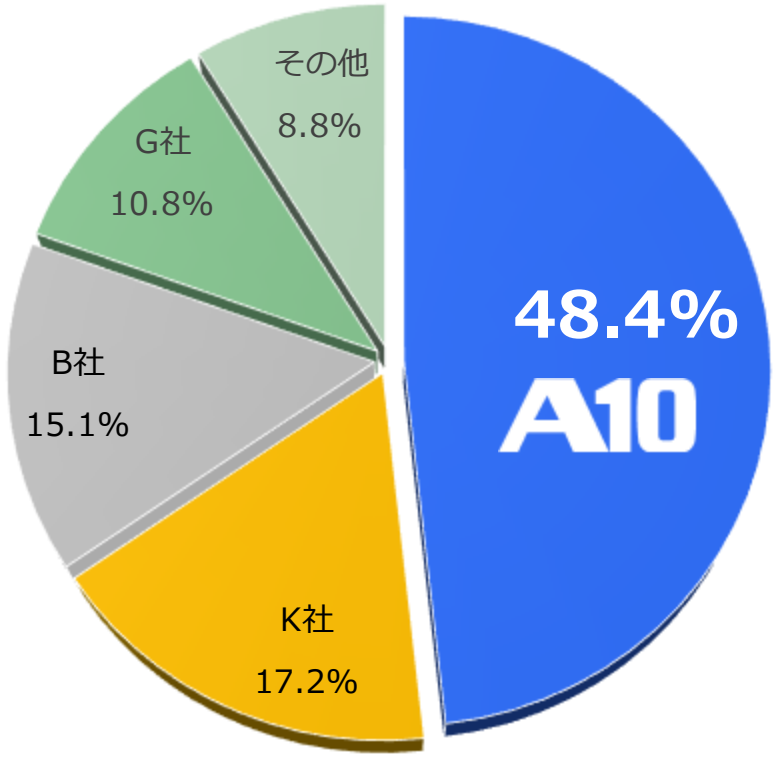
(ア) 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件

(イ) 情報システム運用時の監視等の運用管理機能要件(監視するデータが暗号化されている場合は、必要に応じて復号すること)

(ウ) 情報システムに関連する脆弱性についての対策要件

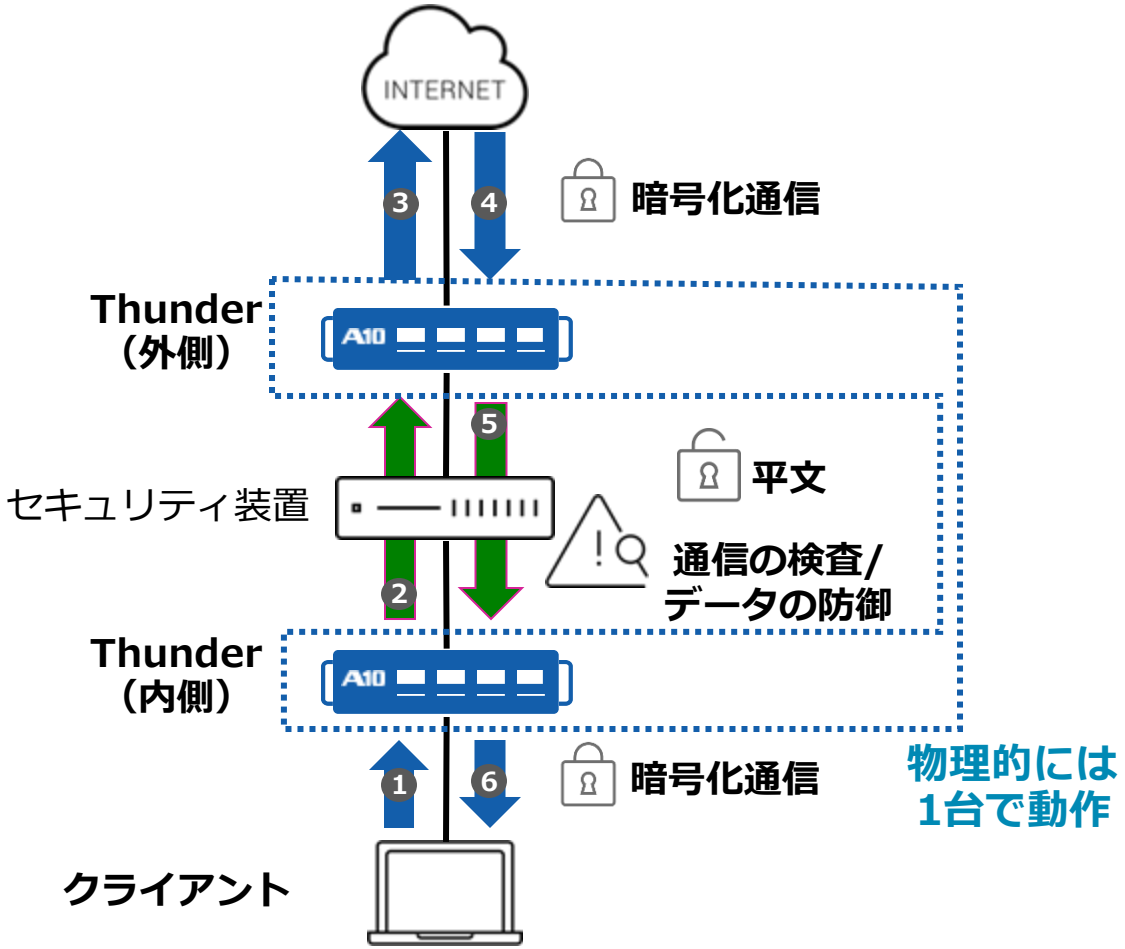
マーケットシェア (SSL可視化市場)

SSL可視化市場売上金額ベース 2016～2019年度
4年連続　マーケットシェア　No. 1を獲得
(2016-2018年度実績。2019年度予測。 Thunder SSLi/CFWが対象)



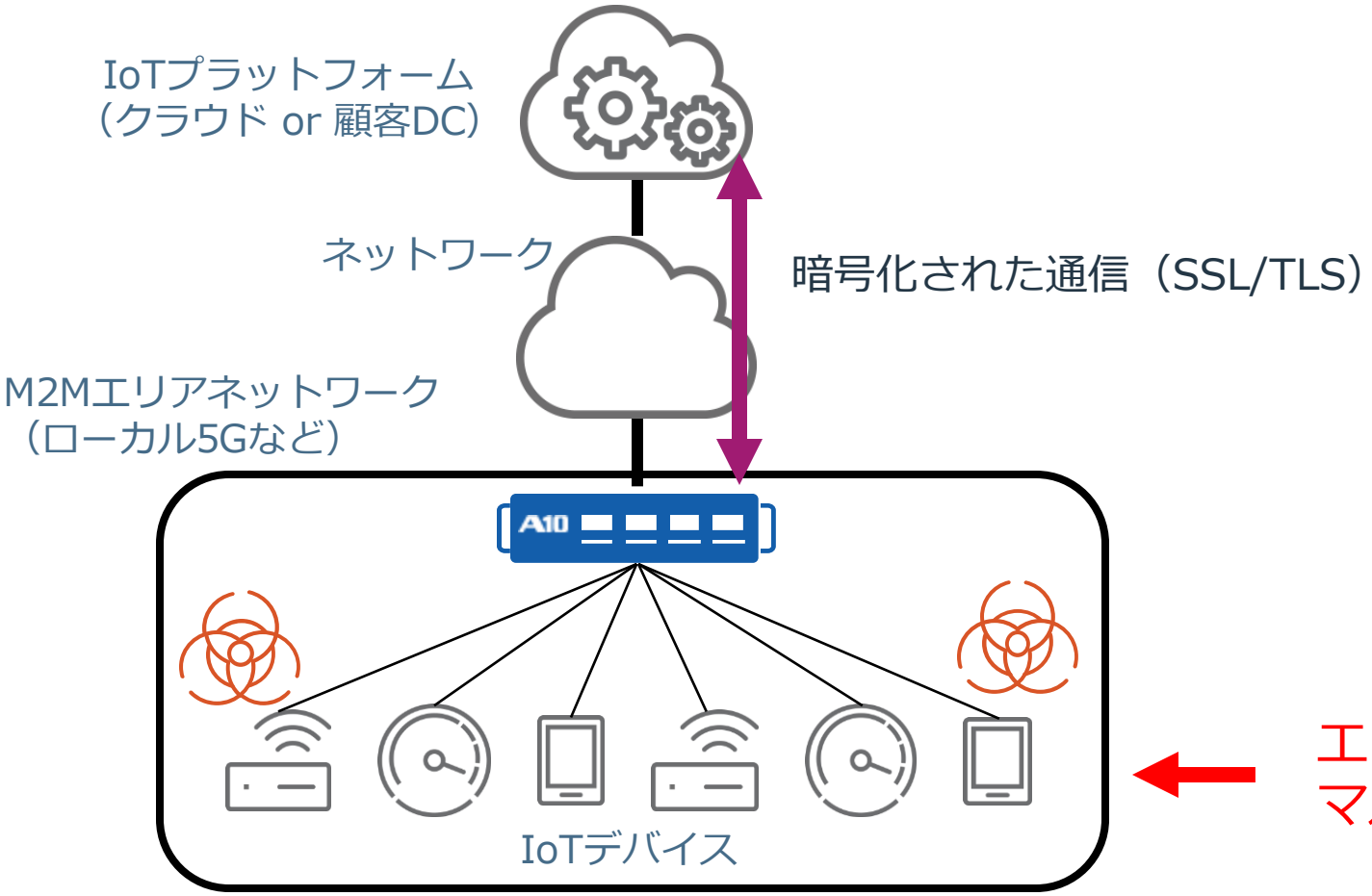
SSL可視化市場 2019年度予測
Source: ITR「ITR Market View：サイバー・セキュリティ対策市場2020」

SSL可視化ソリューション



1. クライアント側Thunderで外向けSSL/TLS通信を復号（URLカテゴリ等でバイパスも可能）
2. セキュリティ装置により平文を検査
3. 回線側Thunderにおいて再暗号化し、SSL/TLS通信を外部サーバーへ送信
4. 回線側Thunderでサーバーからの応答トラフィックを復号
5. セキュリティ装置により平文を検査
6. クライアント側Thunderにおいて通信を再暗号化し、クライアントへ送信

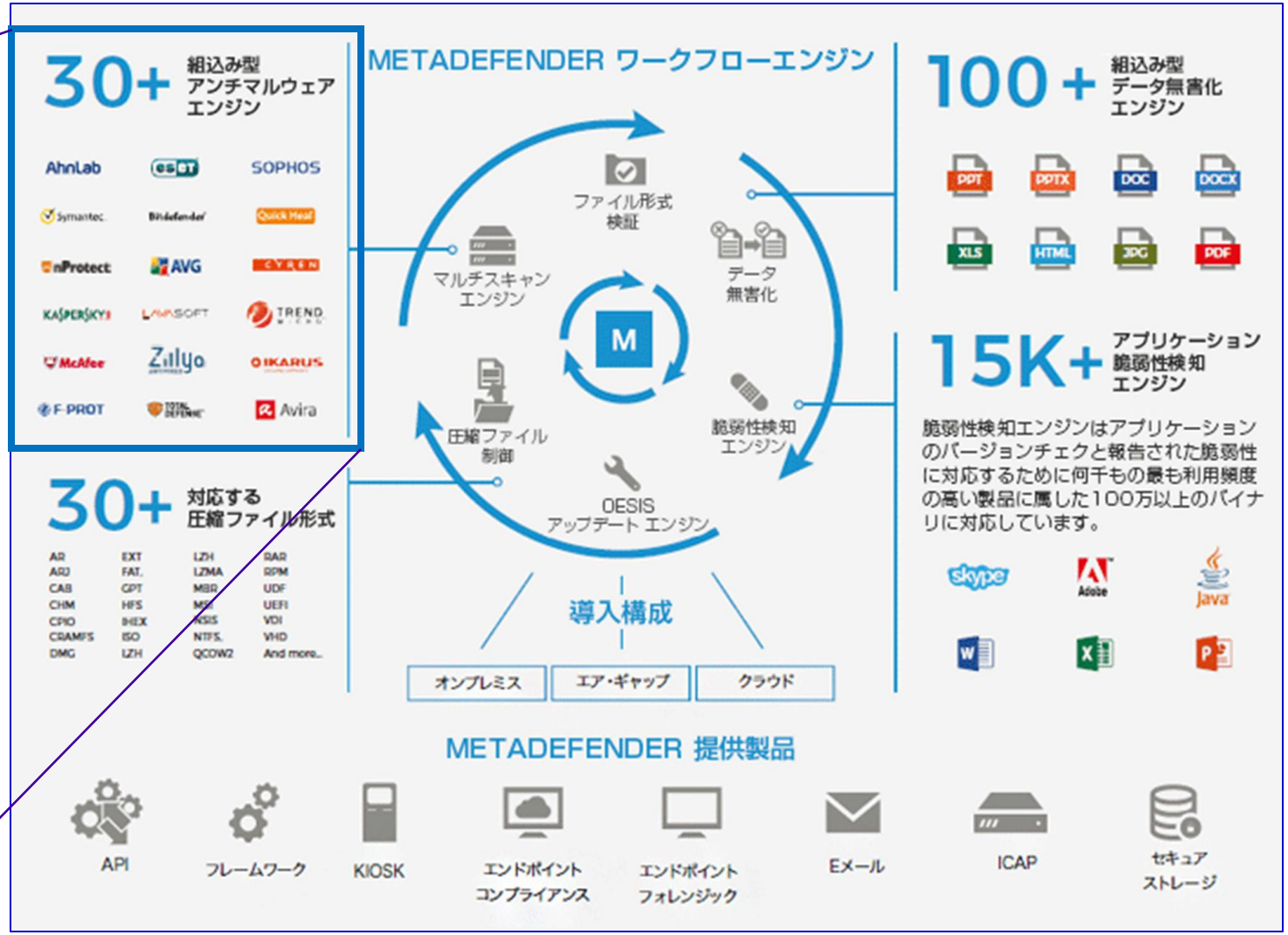
IoTデバイスのマルウェア対策



エンドポイントにおける
マルウェア対策などが難しい機器類

ゲートウェイ型のマルウェア対策の検討

OPSWAT MetaDefenderとの連携



３０種類以上のウイルスソフトによるマルチエンジン型のマルウェア検知を実現

重要インフラにおける情報セキュリティ確保のために「マルチスキャン」が重要に

内閣サイバーセキュリティセンター(NISC) サイバーセキュリティ戦略本部
重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版；令和元年5月23日改定）
https://www.nisc.go.jp/active/infra/pdf/shishin5rev.pdf

●マルウェアからの保護

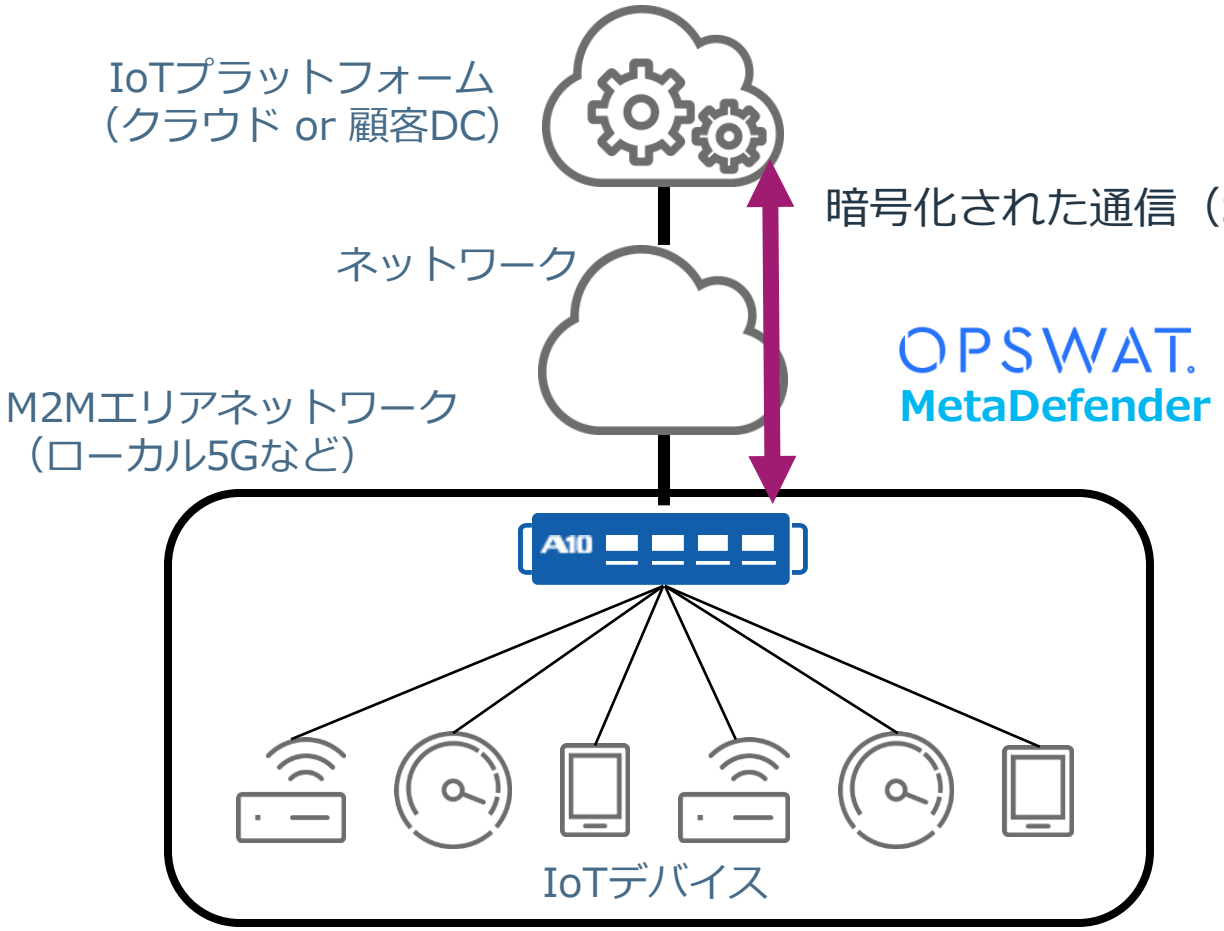
標的型攻撃メールや USB メモリ等から情報システムに感染するマルウェアが重要インフラサービス障害を引き起こす可能性が考えられるため、マルウェアを検出及び予防する仕組みをあらかじめ整備しておくとともに、万が一マルウェアに感染した場合でも早期回復を図るための対策及び手順を確立する。なお、重要インフラ事業者等が直接管理することが困難である、委託先等が持ち込む PC やデバイスがマルウェア感染している可能性も考慮する。

また、優先度の高い重要システムにおいては、マルウェアの検知率向上が期待されるマルチエンジン型のマルウェア検知ソフトや、システム負荷を抑えつつ、未知の脅威に対応できることを特徴とするホワイトリスト型のマルウェア無効化機能の活用も検討することが期待される。

マルチエンジン型マルウェア検知の効果

複数ウイルス対策エンジンによる検知率の向上

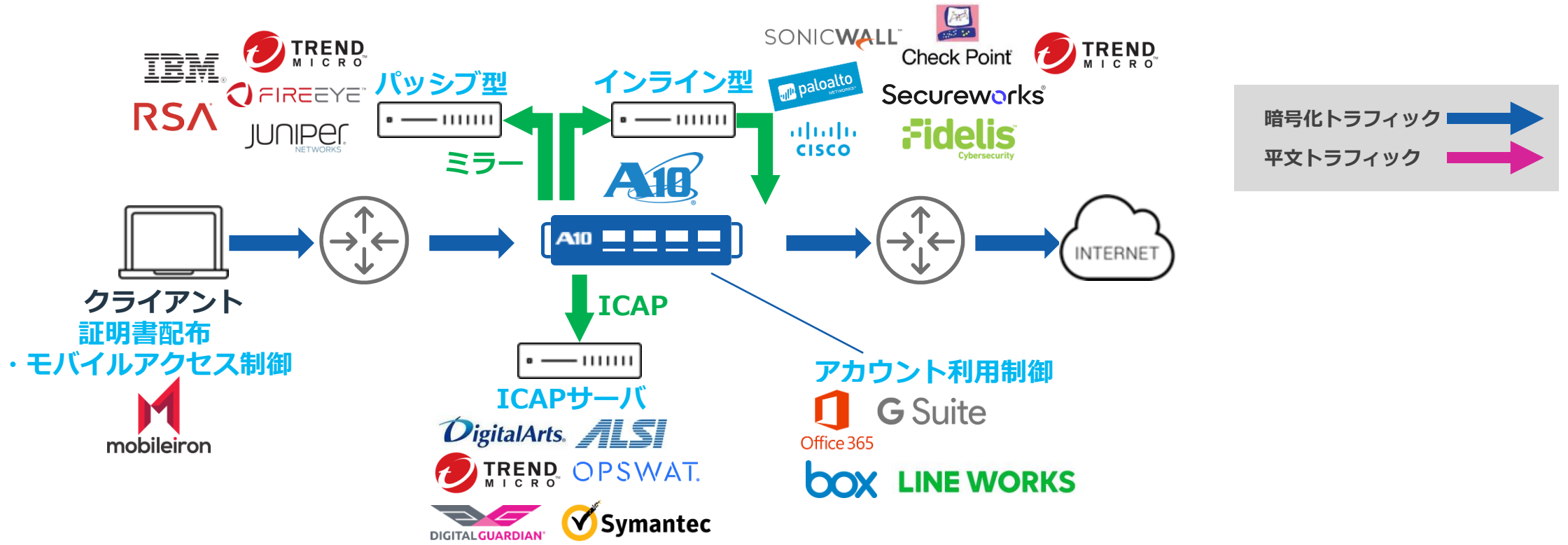
IoTデバイスのマルウェア対策



- OPSWAT社のMetaDefenderと連携
- 暗号化通信を含む全通信のマルウェアを検査

ゲートウェイでマルチエンジン型のマルウェア検知を実現

SSL/TLS可視化：連携ソリューション一覧

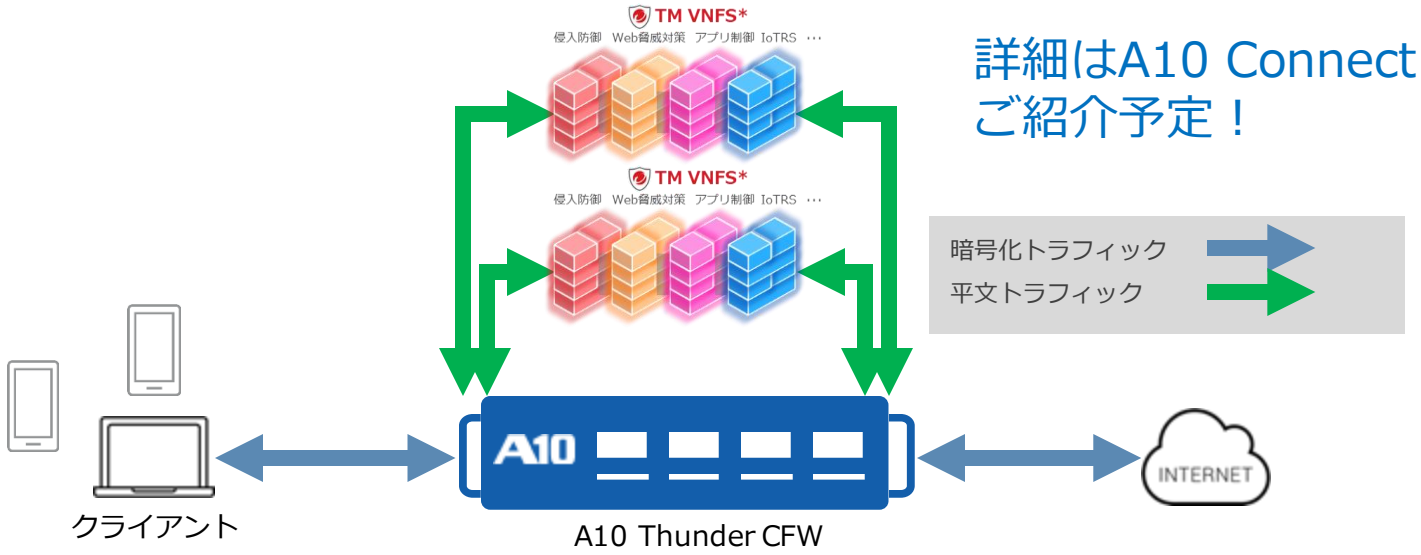


- 一筐体でSSLインサイトを提供、明示型・透過型プロキシとしての動作も可能
- セキュリティ装置の配置形態に柔軟に対応
- お客様環境に最適なセキュリティ装置・ソリューションの構築に寄与

国内ベンダーを含めて２０社以上のセキュリティ機器と連携・可視化

通信事業者様向け連携ソリューション（A10のSSL可視化とTrend Micro VNFS連携）

- Trend Micro VNFS: 通信事業者様向けIPS/IDSソリューション
- Thunder CFW: SSL可視化（複合・最暗号化）してVNFSに転送
  - SSL/TLS通信の場合は復号してTrend Micro VNFSで検査
  - 平文の通信はそのままTrend Micro VNFSで検査



詳細はA10 Connect 別セッションでご紹介予定！

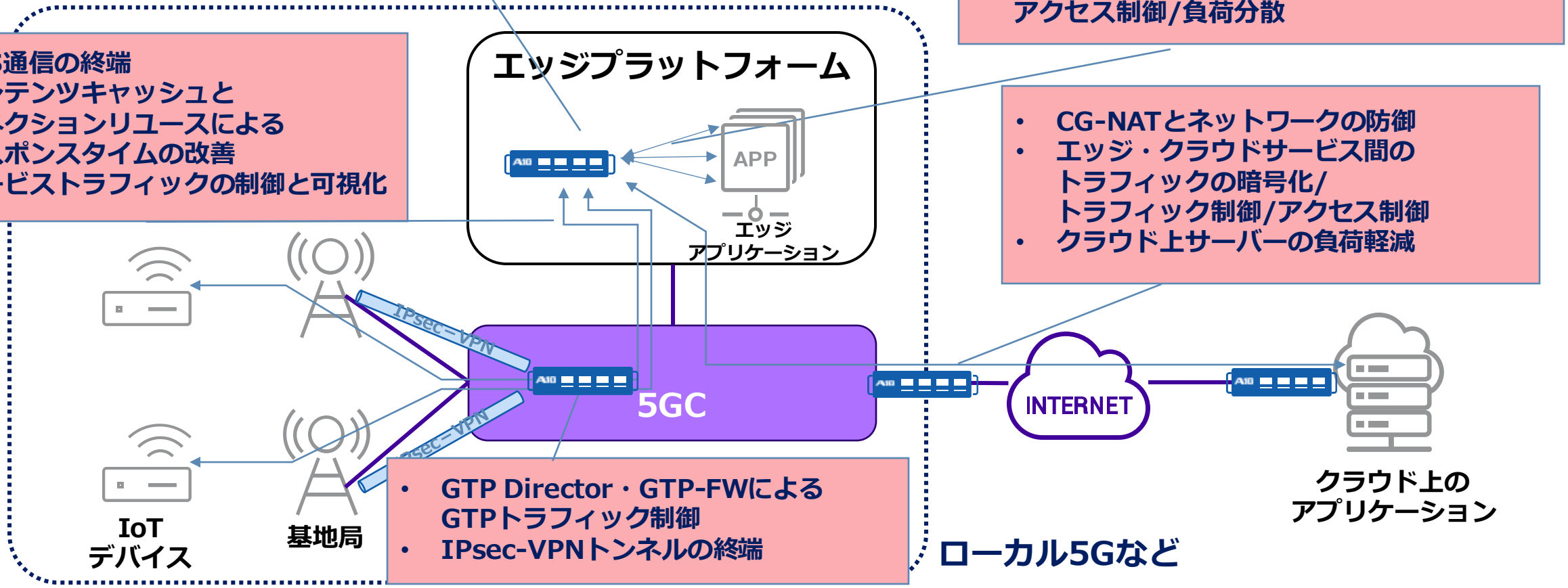
SSL/TLS通信に隠れた問題の検知やブロックもVNFSで実現

エッジプラットフォームでのA10活用

- 各種リバースプロキシ機能
- アプリケーションセキュリティ機能の提供
  （DDoS防御、各種FW、脅威インテリジェンス、可視化など）

- セキュアサービスメッシュ：
  エッジサービス間のトラフィック制御/暗号化/
  アクセス制御/負荷分散

- TLS通信の終端
- コンテンツキャッシュと
  コネクションリユースによる
  レスポンスタイムの改善
- サービストラフィックの制御と可視化



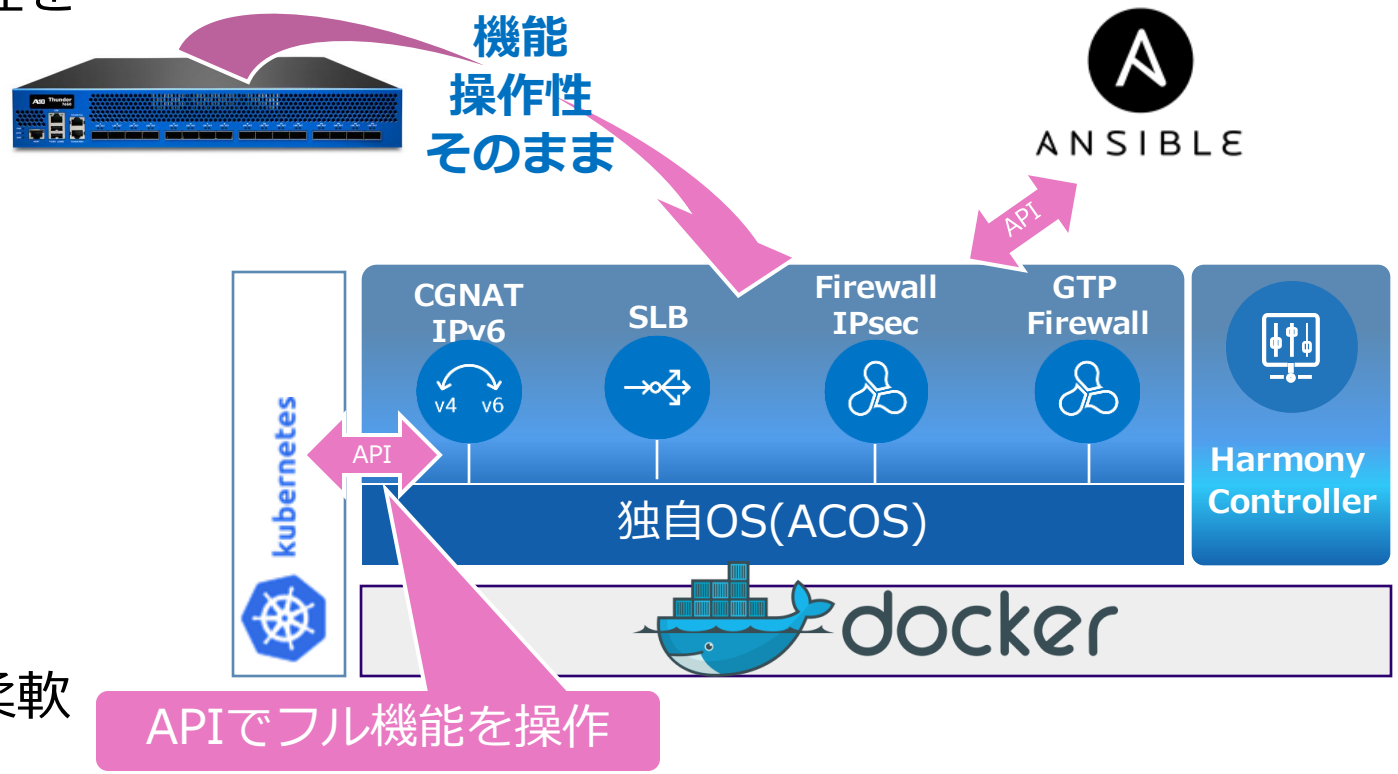
- CG-NATとネットワークの防御
- エッジ・クラウドサービス間の
  トラフィックの暗号化/
  トラフィック制御/アクセス制御
- クラウド上サーバーの負荷軽減

- GTP Director・GTP-FWによる
  GTPトラフィック制御
- IPsec-VPNトンネルの終端

エッジエリアでのトラフィック制御・セキュリティを提供

Thunderのコンテナ対応

- 既存のThunderシリーズの機能や操作性をそのままにコンテナ化
- CFWの機能を利用可能
- 最大180Gbpsのパフォーマンス
- Dockerコンテナとして動作
- RESTベースのAPIで連携可能
- Ansibleとの連携による自動化に対応(RedHat OpenShiftと連携)
- Kubarnetesとの連携も可能
- スケールアウト機能を利用することで柔軟な容量拡張が可能

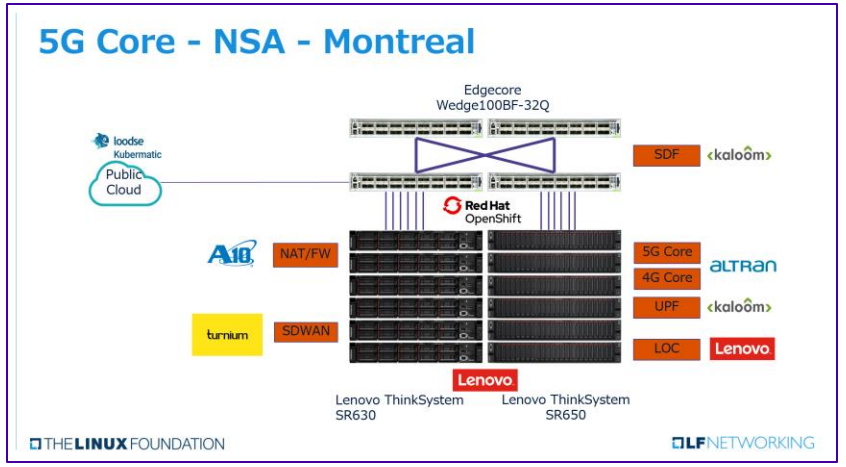


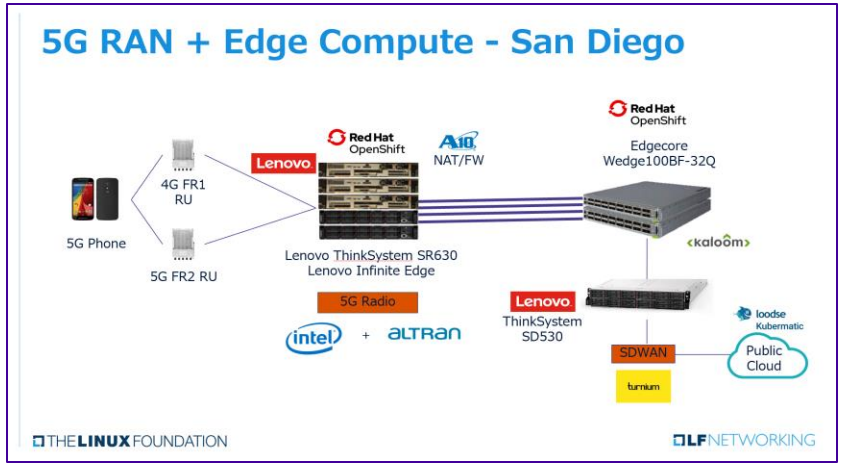
従来からの機能や操作性をそのままにコンテナ環境で利用可能

A10 KubeCon 2019 5Gコンテナ化PoCに参加

- OPNFV / Linux Foundationが協賛するライブ5G環境デモに参加
  - 5G Virtual Central Office デモ (VCO 3.0)

- A10：5Gコンテナ型ファイアウォールを5Gコアの中でデモ
  - L4/7 ステートフルFW＋CGNAT
  - Kubernetes / OpenShift 環境で連携
  - Lenovo社製サーバを使用
  - ポリシ設定でアプリケーションの使用を制御するデモを公開





Kubernetes / Red Hat OpenShiftと連携してセキュリティ機能を提供

AnsibleによるA10 Thunder ADCの設定自動化

36 lines (26 sloc) | 2.03 KB — Raw | Blame | History

Ansible Training - A10 Thunder ADC Workshop

このドキュメントはA10 Thunder/vThunder　ADCの構成管理をAnsibleで自動化するためのハンズオントレーニングの内容を示しています。

Section 1 - A10 Thunder ADCのAnsibleによる自動構成　基本演習（ネットワーク設定とHTTP仮想サーバの構築）

- 演習 1.0 - サーバ負荷分散の基礎と演習環境の確認
- 演習 1.1 - VLANの設定とデータポートの割り当て
- 演習 1.2 - データポートのenable
- 演習 1.3 - Serverの追加
- 演習 1.4 - Service-Groupの構成
- 演習 1.5 - NATプールの設定
- 演習 1.6 - HTTPのVirtual-Serverの構成
- 演習 1.7 - Serverの切り離しと切り戻し

Section 2 - A10 Thunder ADCのAnsibleによる自動構成　応用演習（HTTPS仮想サーバの構築）

ここでは変数 `a10_host` として、vThunderの管理用ポートのIPアドレスを指定しています。

次に、Playbook内で実行する処理を `tasks` として記述します。

```
---
- hosts: 10.255.0.1
  connection: local
  gather_facts: no

  vars:
    a10_host: "10.255.0.1"
  tasks:
  - name: Create VLAN
    a10_network_vlan:
      a10_host: "{{ a10_host }}"
      a10_port: "{{ a10_port }}"
      a10_username: "{{ a10_username }}"
      a10_password: "{{ a10_password }}"
      vlan_num: "10"
      untagged_eth_list:
        - untagged_ethernet_start: "1"
          untagged_ethernet_end: "1"
      ve: "10"
      state: present
      partition: shared
```

- `name: Create VLAN` は、タスクの説明文で、Playbook実行時にこの内容が表示されます。
- `a10_network_vlan:` は、タスクで使用されるモジュール名を示しています。これはvThunderに対しVLANの設定を行うモジュールです。
- `a10_host: "{{ a10_host }}"` は、モジュールのパラメーターで、モジュールがどのvThunderのIPアドレスに接続するかを指定します。ここでは上記の `vars` で定義された `a10_host` を参照しています。
- `a10_port: "{{ a10_port }}"` は、モジュールのパラメーターで、モジュールが接続するvThunderのポートを指定します。ここではインベントリ（hostsファイル）で定義された `a10_port` を参照しています。
- `a10_username: "{{ a10_username }}"` は、モジュールのパラメーターで、vThunderのaXAPIを実行するユーザー名を指定します。ここではインベントリ（hostsファイル）で定義された `a10_username` を参照しています。
- `a10_password: "{{ a10_password }}"` は、モジュールのパラメーターで、vThunderのaXAPIを実行するユーザーに対応したパスワードを指定します。ここではインベントリ（hostsファイル）で定義された `a10_password` を参照しています。
- `vlan_num: "10"` は、モジュールのパラメーターで、 `a10_network_vlan` で設定するVLANのID番号を指定します。
- `untagged_eth_list:` は、リスト形式のモジュールのパラメーターで、 `a10_network_vlan` で設定するVLANに対応したethernetの番号を、 `untagged_ethernet_start` と `untagged_ethernet_end` で開始番号と終了番号を指定して設定しま

205 lines (149 sloc) | 10.7 KB — Raw | Blame | History

演習 1.0 - サーバ負荷分散の基礎と演習環境の確認

この演習では、ADCによる負荷分散の基礎について紹介し、演習で利用する環境の事前準備を実施します。

目次

Thunder用Ansibleモジュールについて

A10 Thunder用のAnsibleモジュールは、以下のGitHubにあります。 ほぼ全ての機能の構成管理に対応する1,400以上のモジュールが用意されています。

Click here to A10 Ansible Modules on GitHub

現状このAnsibleモジュールをGitHubからCloneした場合、モジュールの一部を修正する必要があります。 修正点などを記述したスタートアップガイドは以下にあります。本演習で利用する環境では、この修正は適用済みです。

Cliech here to A10 Ansible Modules Startup Guide

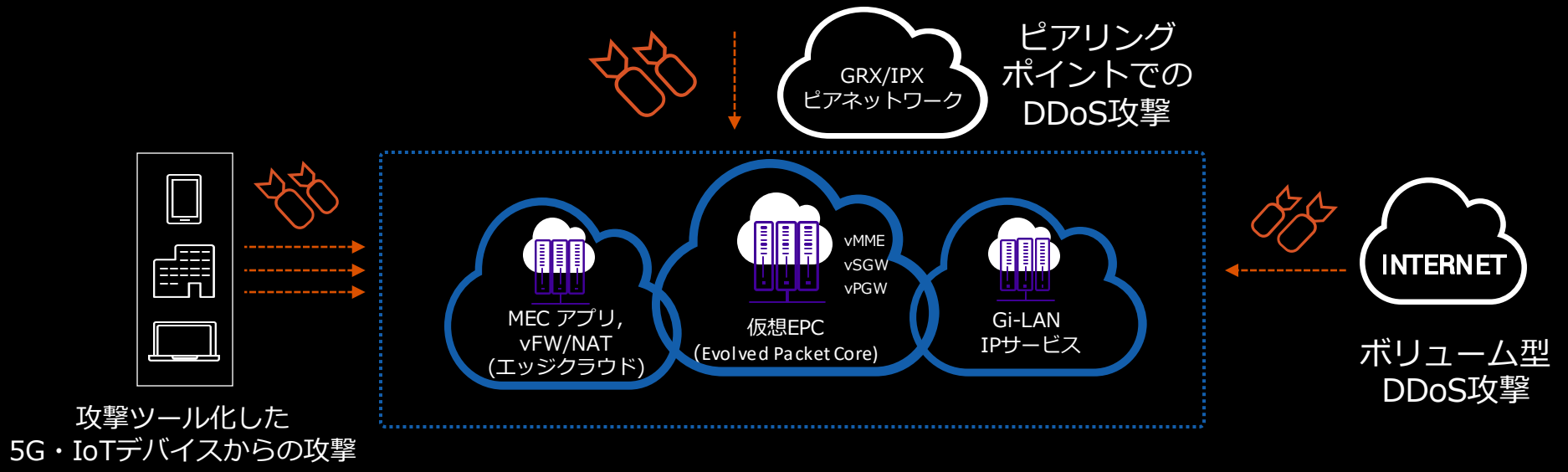
このAnsibleモジュールではA10 Thunderの提供するREST APIであるaXAPIを利用しています。 Ansibleモジュールを実行する際は、Ansible Coreが動作しているサーバにSSHし、ローカルでモジュールを実行することで、aXAPIを通じた構成変更が行われます。

a10_*モジュールを利用した場合の基本動作

管理者

https://github.com/kishizuka4989/ansible_training_a10_thuner_adc/blob/master/README.ja.md

A10によるハンズオントレーニングもご提供



5Gによりセキュリティ脅威が増加

4X

2年間にわたる
DDoS攻撃サイズの平均*

12M

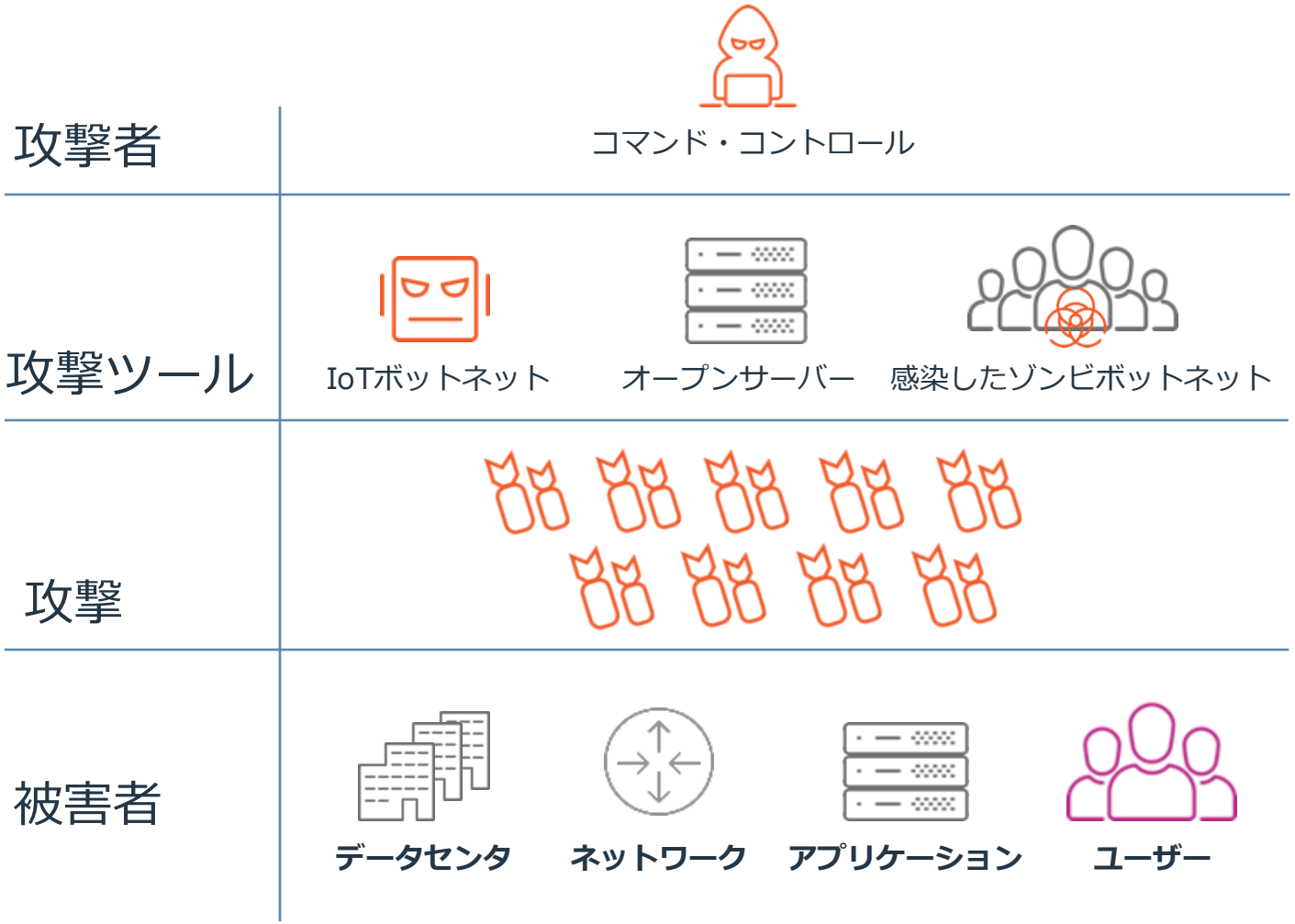
5Gインフラを攻撃できる
DDoS攻撃ツールの数*

62%

5GにおいてDDoS攻撃
防御が最も重要*

*出典: SecurityIntelligence.com, SC Magazine, IHS Markit

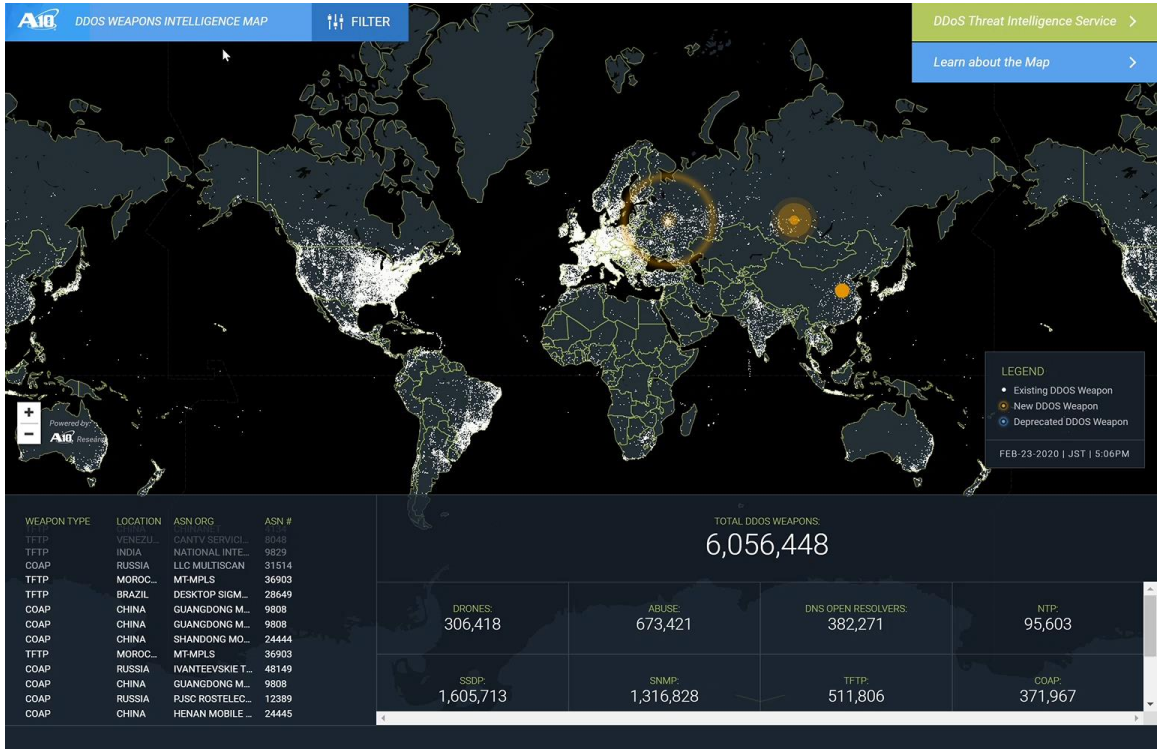
DDoSによるサイバー攻撃とは？



攻撃者が、
様々な攻撃ツールを用いて、攻撃対象のサービスを利用できなくなるようにする
サイバー攻撃

海外ではライフラインに関わるインフラに対する攻撃も発生

A10 脅威インテリジェンスサービスについて



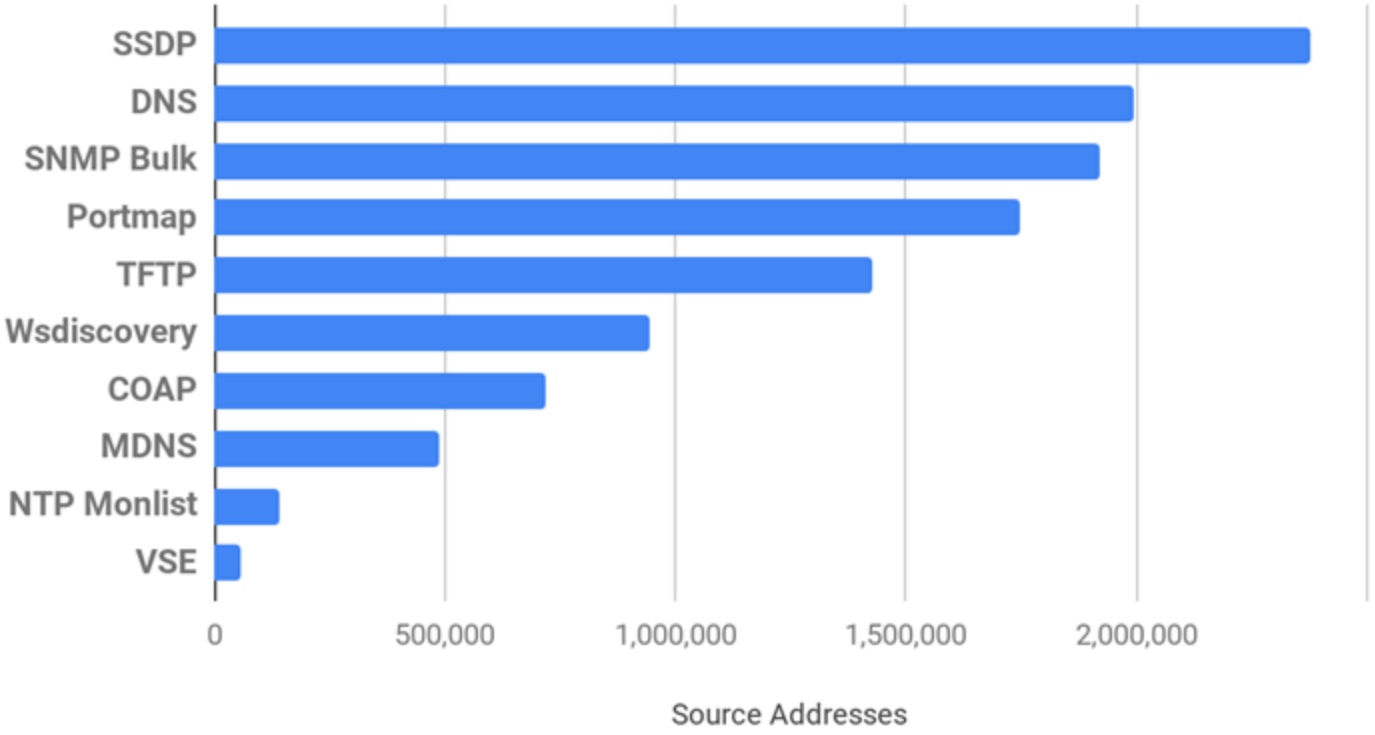
A10グローバルDDoS脅威インテリジェンスマップ
https://threats.a10networks.com/

- 独自開発の脅威インテリジェンスデータソースによるレピュテーションデータ
- リアルタイムの脅威検知
- シグネチャの自動検出
- 攻撃エージェントとして繰り返し利用されているIP
- 脆弱性のあるIPとホストに関する知見
- AS番号毎のDDoS攻撃ツール数に関するデータ
- DDoSリスクアセスメントサービス（カスタマイズされた調査が可能）

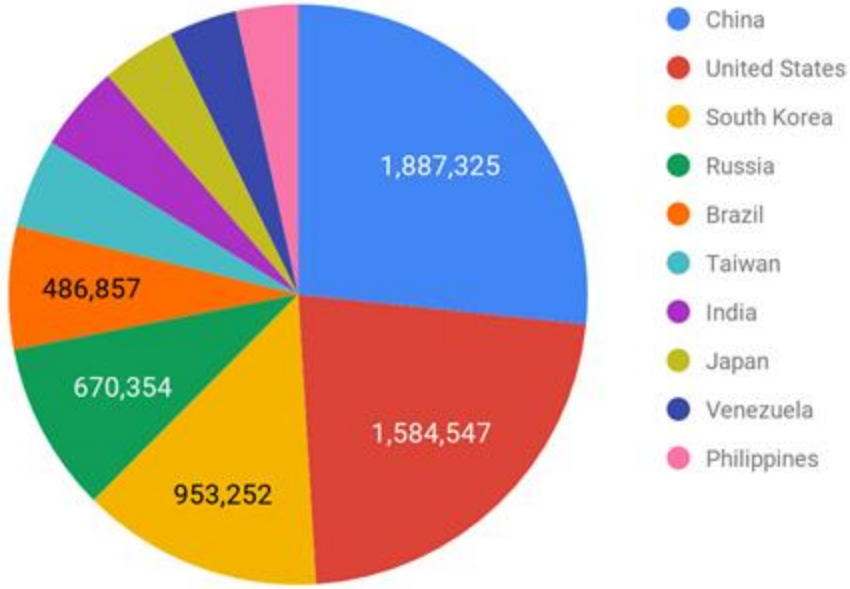
攻撃を防御するためのプロアクティブなアプローチを支援

アンプ攻撃ツールのデータ
（2020年8月：グローバル）

UDPアンプ攻撃ツールトップ１０（ソースアドレス数）



アンプ攻撃ツール数トップ10（国別）

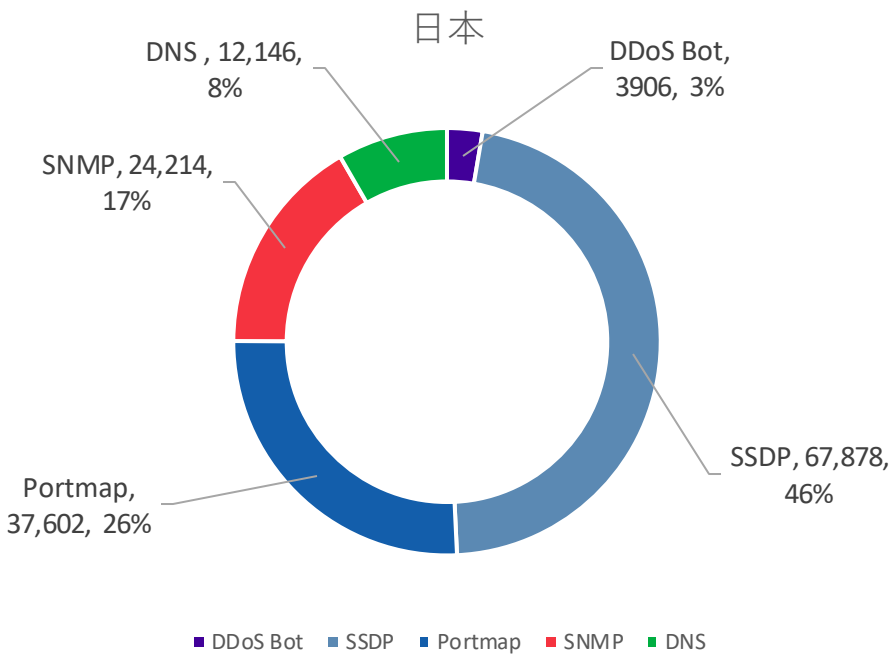


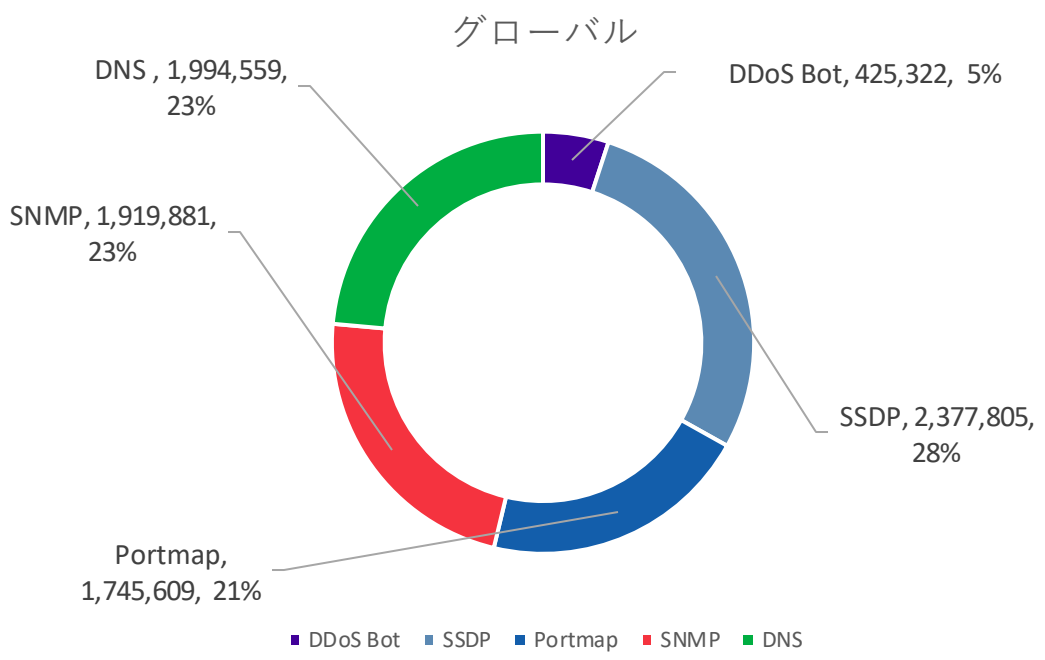
Organization	Unique Sources
China Unicom	700,127
China Telecom	679,491
Korea Telecom	643,091
Chungwha Telecom	255,944
CANTV Servicios, Venezuela	255,022
PLDT	220,287
Guangdong Mobile	213,706
Rostelecom	198,845
OVH SAS	133,780
Charter Communications Inc	123,779

※スライド投影のみ

日本における脅威状況の比較

DDoS攻撃ツール化したサーバーの数（2020年９月第一週のデータ）

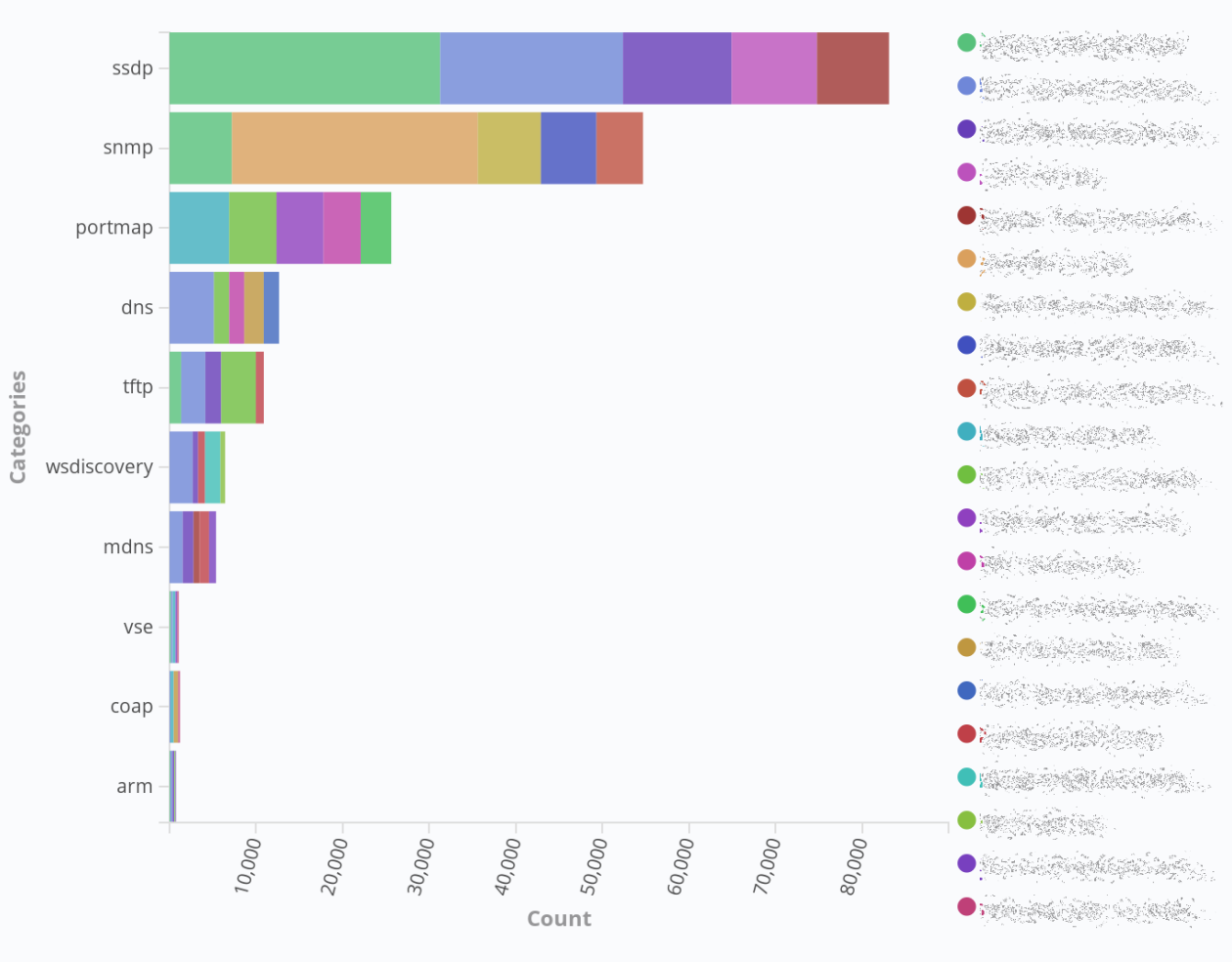




日本は、DNSの割合が少なく、SSDPの割合が多い

※スライド投影のみ

日本の組織毎の脅威状況



日本の各組織でどのDDoS攻撃ツールが何台あるかのデータ

※スライド投影のみ

日本の組織毎の脅威状況

Category	Organizations	Cities	Unique Sources
ssdp	[redacted]	Hiroshima	180
ssdp	[redacted]	Koto	95
ssdp	[redacted]	Kashiwa	84
ssdp	[redacted]	Machida	59
ssdp	[redacted]	Sagamihara	33
ssdp	[redacted]	Osaka	568
ssdp	[redacted]	Yokohama	566
ssdp	[redacted]	Tokyo	323
ssdp	[redacted]	Saitama	266
ssdp	[redacted]	Nagoya	246
ssdp	[redacted]	Yokohama	540
ssdp	[redacted]	Tokyo	358
ssdp	[redacted]	Osaka	343
ssdp	[redacted]	Koto	158
ssdp	[redacted]	Nagoya	152
ssdp	[redacted]	Osaka	924

日本の各組織の地域毎でどのDDoS攻撃ツールが何台あるかのデータ

A10のDDoS防御ソリューション – Thunder TPS

Thunder TPS　シリーズ

DDoS攻撃防御の効率化

機械学習を用いたゼロデイ攻撃防御

フルオート

の自動DDoS緩和ポリシー

- 自動で攻撃内容に応じた防御ポリシーを適用
- 手動による操作、実行に要する時間を削減

プロアクティブ

に実行可能な
DDoS脅威インテリジェンス

他社と比較して**48倍のブラックリストを保有**

高い投資効率

他社より 2倍

マルチコアに最適化された独自OSにより
業界最高レベルのパフォーマンス
1台で **300 Gbps/440 Mpps**
(仮想アプライアンス：100Gbps)

2倍 **省スペース化**
1U*で最大*220Gbps

10倍 **保護対象ホスト収容率**

1台あたりの収容率を向上 CAPEXとラックの省スペース化を実現

物理・仮想環境でハイパフォーマンスな防御環境を構築可能

Thunder TPS ラインナップ

DDoS攻撃緩和装置（モード変更で検知装置へ変更可能）

エントリ

Thunder 3040S
10 Gbps

Thunder 1040
5 Gbps,
ハードウェアバイパスオプション

vThunder TPS
仮想アプライアンス
1~ 5 Gbps

ミドルレンジ

Thunder 5845
100 Gbps

Thunder 5435
77 Gbps

Thunder 4435
38 Gbps

ハイエンド

Thunder 14045
300 Gbps, 100 GbE ports

Thunder 7445
220 Gbps, 100 GbE ports

Thunder 6635(S)
152 Gbps, 100 GbE ports

Thunder 6435(S)
152 Gbps

統合管理・DDoS検知

aGalaxy 5000
ハードウェア
アプライアンス

aGalaxy-VA
仮想アプライアンス

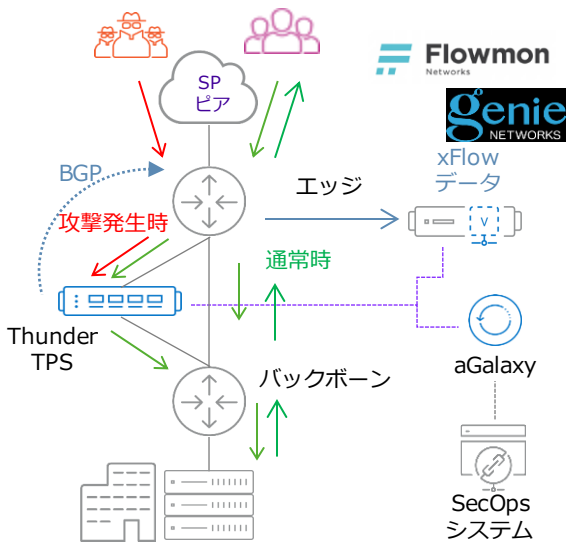
DDoS検知専用

vThunder TPS Detector
仮想アプライアンス

防御帯域、ポート構成などで様々なモデルを選択可能

Thunder TPSのユースケース

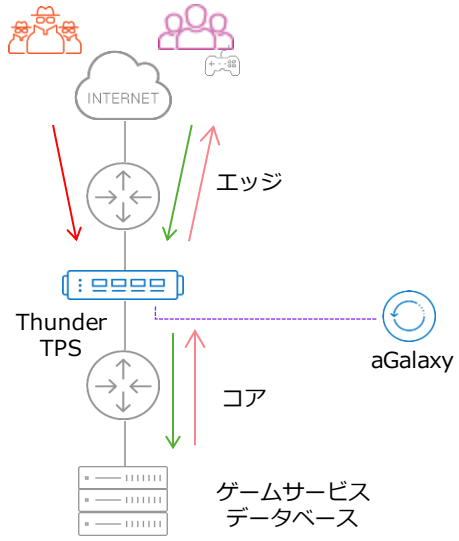
サービスプロバイダ



- 他社フローコレクタと連携可能
- ネットワーク全体の防御
- 自動経路制御
- SecOpsシステムとのAPI連携

インフラの防御

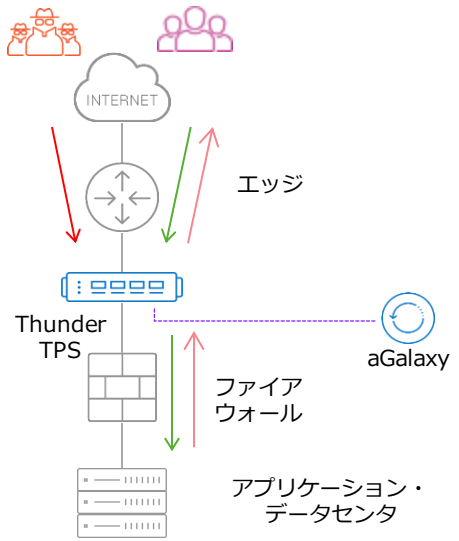
ゲーム



- リアルタイム防御
- インライン構成
- マルチベクタ
- DDOS、不正トラフィック防御

プレイヤー体験を向上

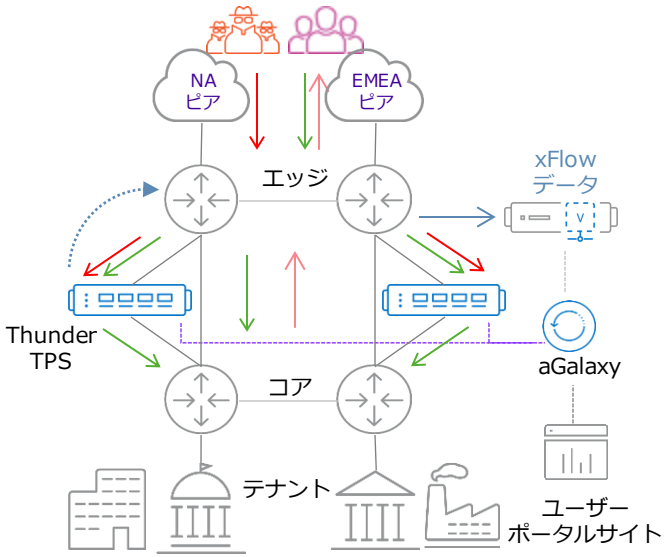
企業



- DDoS攻撃に弱いFWを防御
- アプリケーションの可用性確保

FWプロテクション

MSSP

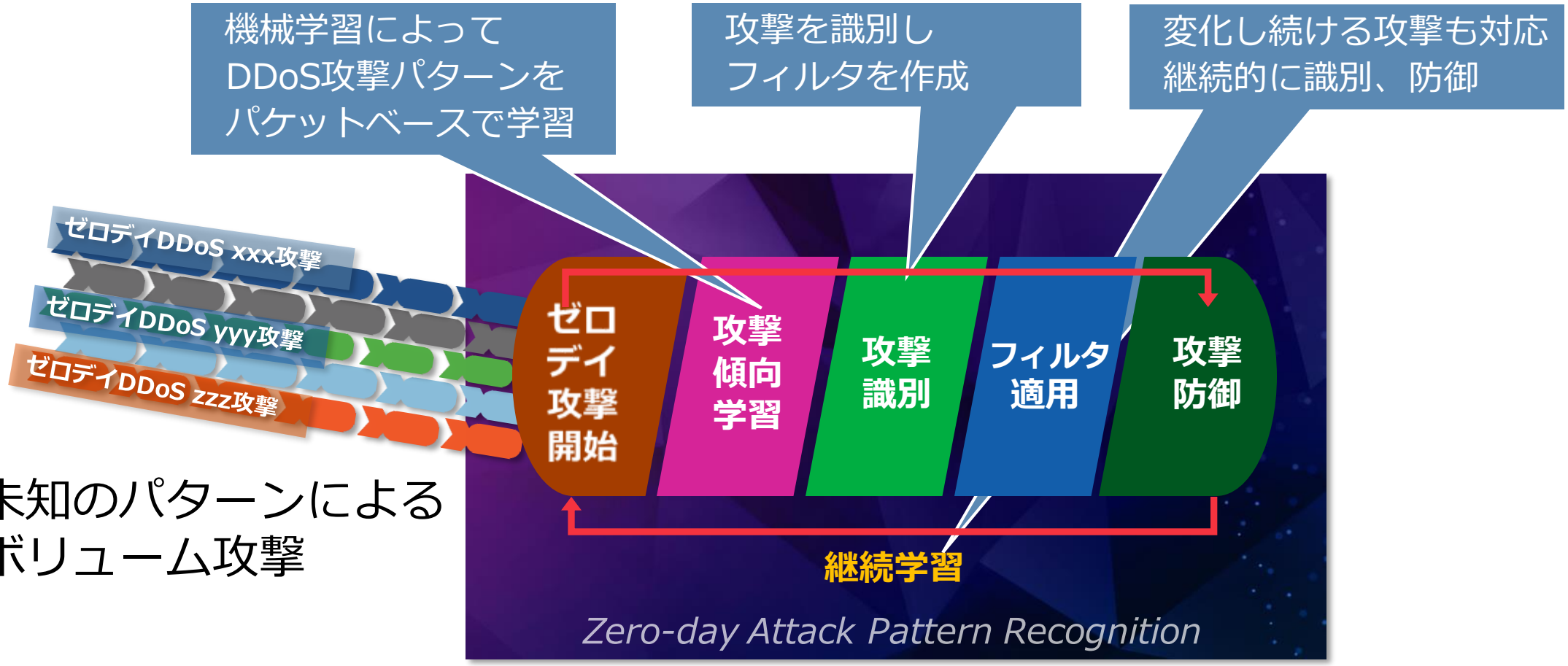


- テナントの防御
- テナント毎のレポーティング
- サブスクライバーポータル

マルチテナントサービス

あらゆるネットワーク構成に対応

A10の機械学習による防御機能（ZAPR）



未知のパターンによる
ボリューム攻撃

攻撃パターンを学習して防御ポリシを自動生成・攻撃が変化しても再学習して防御

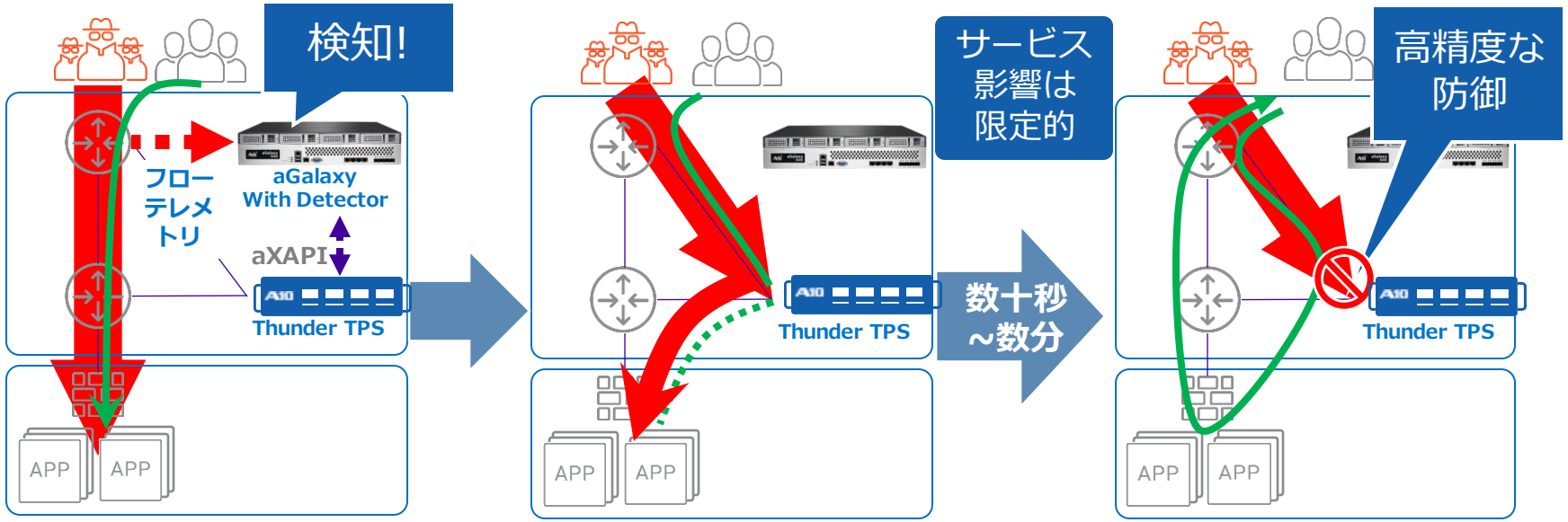
[従来]未知のDDoS攻撃パターンの防御フロー

1. 設定済みのポリシなどで緩和（複数回）
2. 攻撃パターンが変化してポリシで防御不能、ベースラインを超過
3. 最終的にレートリミットが起動してトラフィックを制限

分析結果に基づいた
フィルタを設定して防御

レートリミットでの防御のため正常トラフィックにも影響あり

[ZAPR]未知のDDoS攻撃パターンの防御フロー

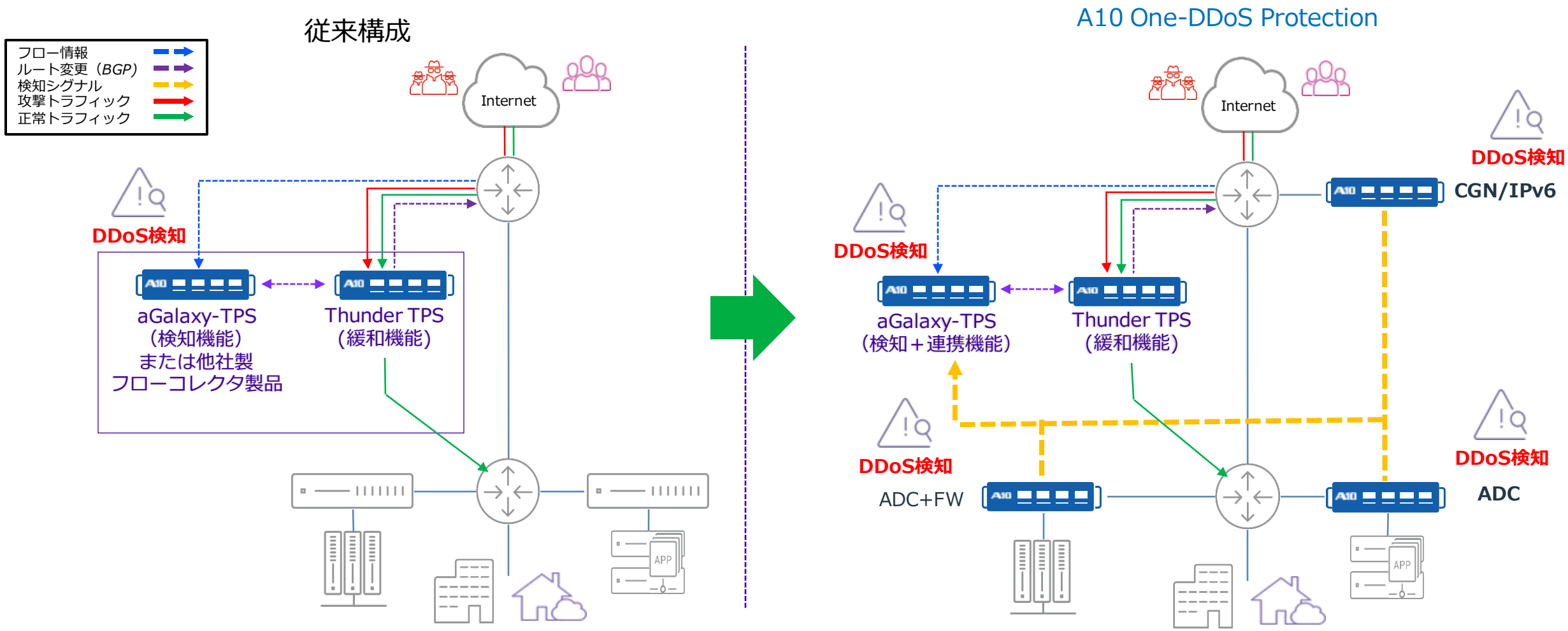


1. 設定済みのポリシなどで緩和（複数回）
2. 攻撃パターンが変化してポリシで防御不能、ベースラインを超過
3. レートリミットをトリガとしてZAPRが起動
4. ZAPRが全体トラフィックから攻撃成分のみをドロップ

- フィルタの効果を常時モニタ
- 一定の効果が得られないと判断した場合は、再学習
- 再作成したフィルタを適用

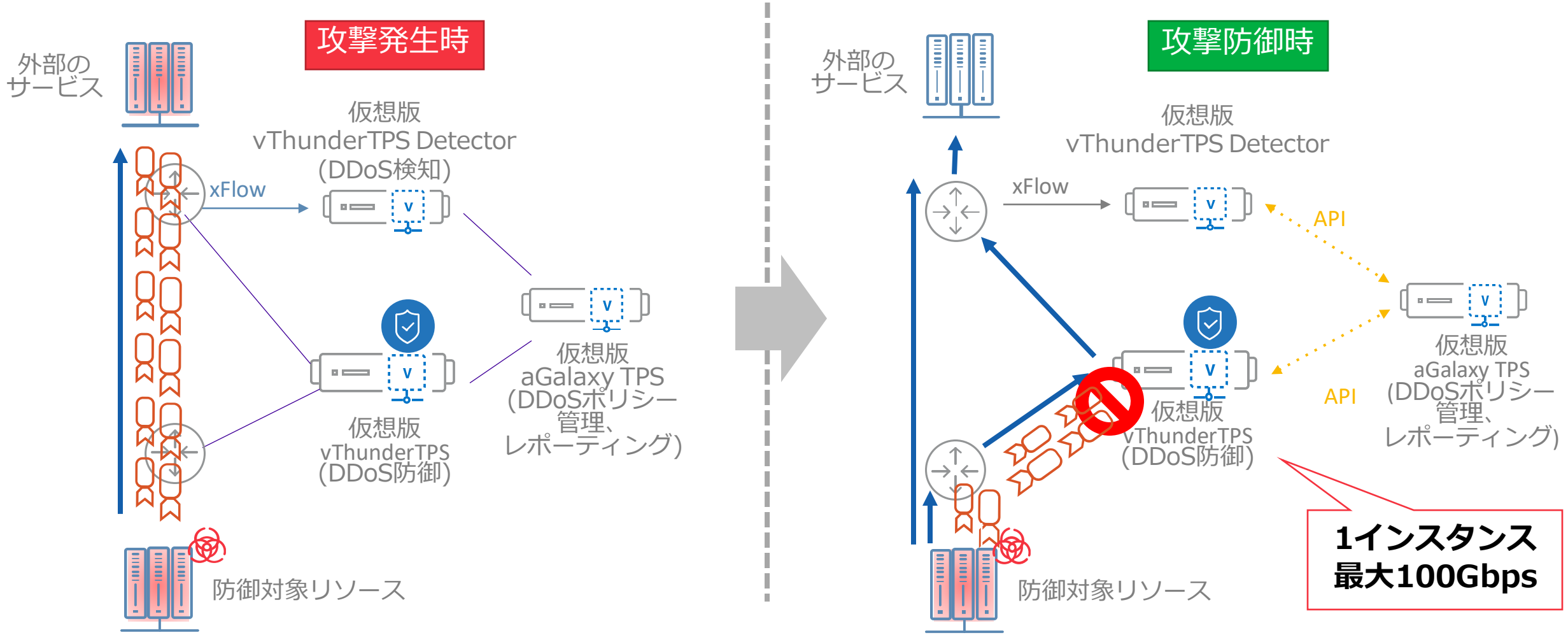
正常トラフィックへの影響を極力避けた緩和が可能

A10のOne-DDoSソリューション



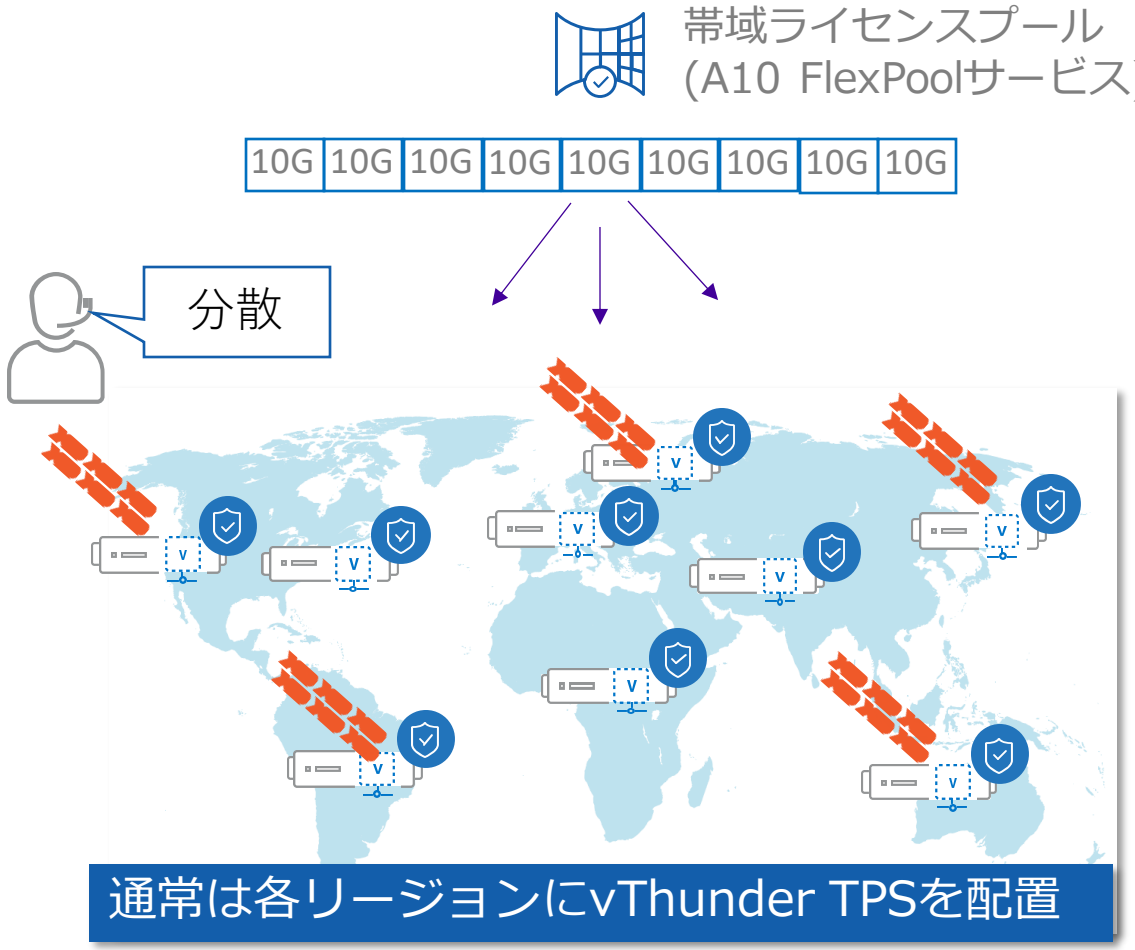
保護対象のサービス・アプリケーションに近いポイントで攻撃を検知

内部から外部へ向けての攻撃防御

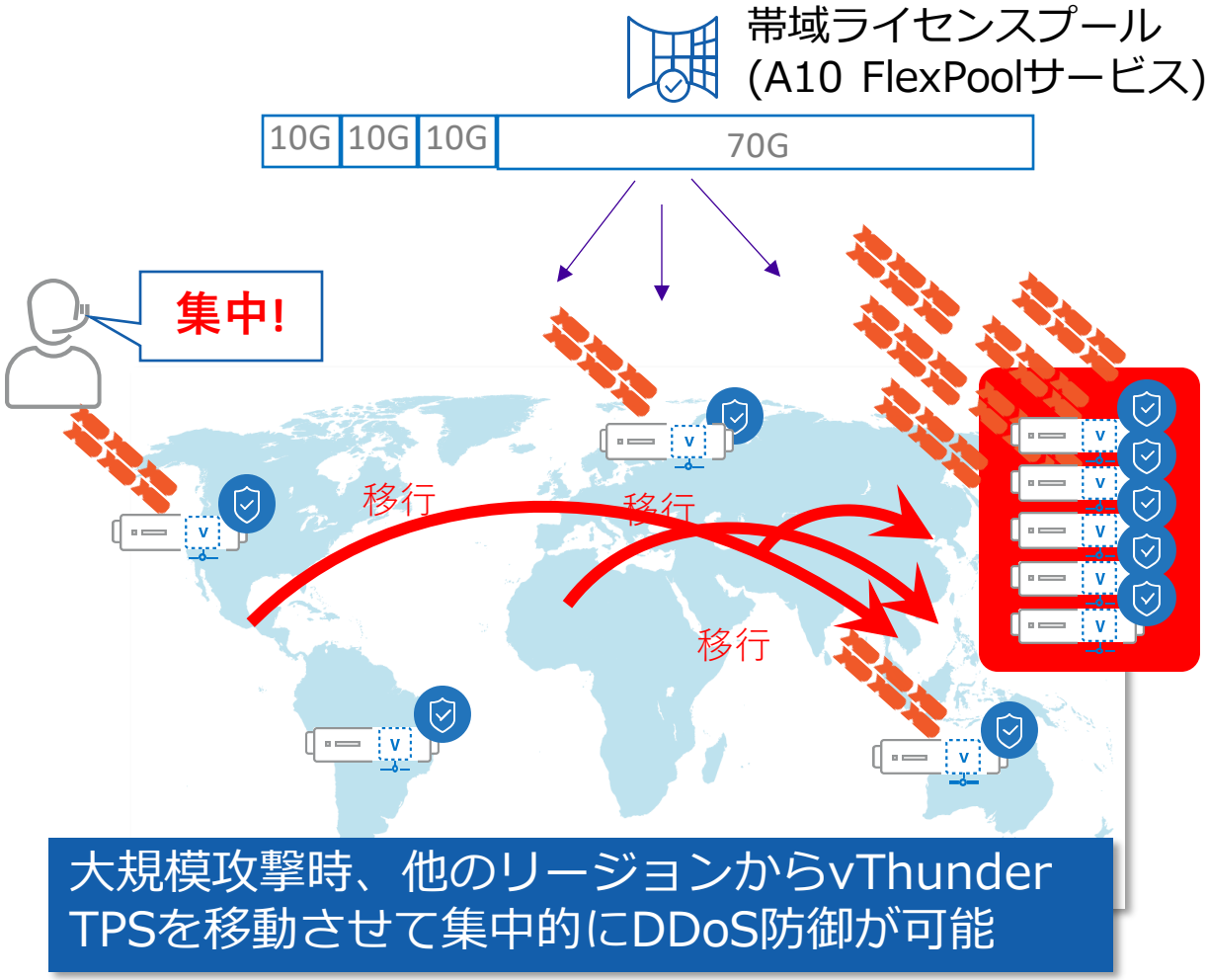


組織内部から外部に対する攻撃も大容量で防御し、組織のブランドを保護

A10 FlexPoolライセンスによる防御帯域制御



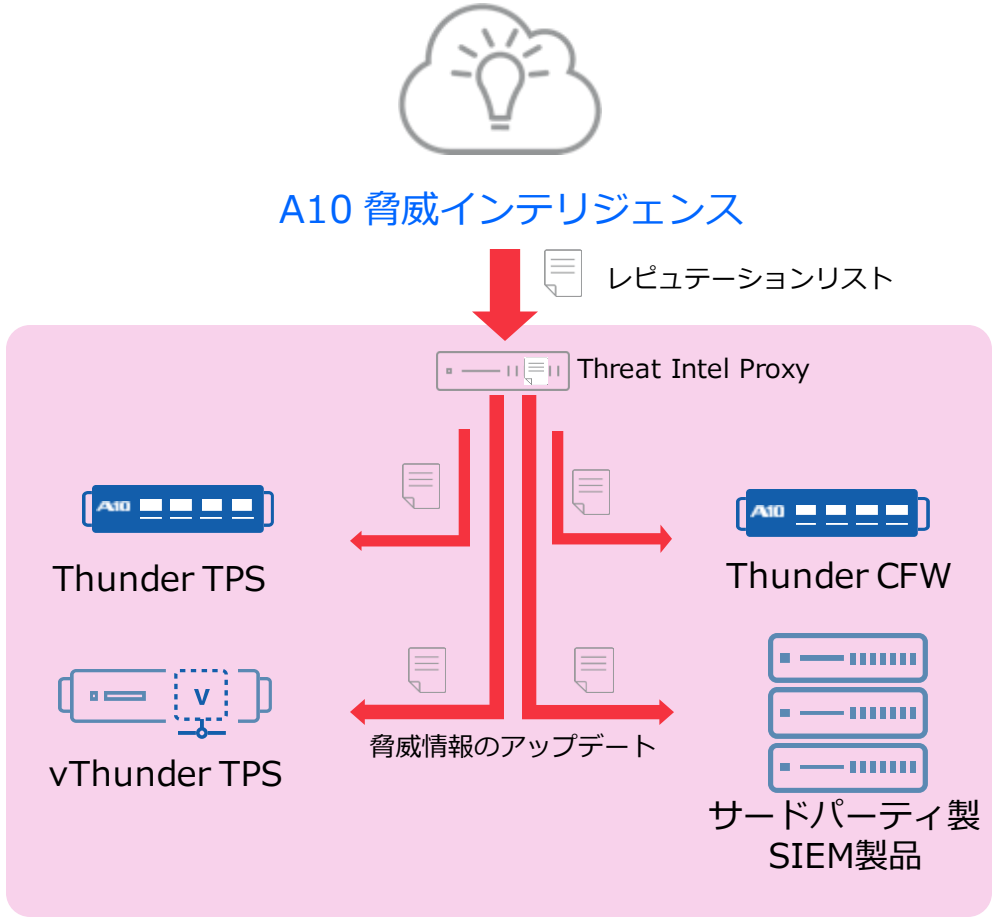
通常は各リージョンにvThunder TPSを配置



大規模攻撃時、他のリージョンからvThunder TPSを移動させて集中的にDDoS防御が可能

防御リソースを効果的に分散/集中配置しつつ迅速なデプロイを実現

脅威インテリジェンスサービスの活用



- 脅威インテリジェンスを利用した防御
- Thunder TPSや他のA10製品でも利用可能
- カスタマイズできるデータフィード
- プロキシ経由のデータ転送
- データのみの提供も可能
- サードパーティ製のSIEMデバイスなどで利用可能

他社製品でも使用可能・プロアクティブな防御環境を構築

まとめ

- サービス不能攻撃（DDoS攻撃）が増加する可能性がある

  ➡ DDoS攻撃対策や脅威情報を活用して対策を検討

- IoT機器向けのセキュリティ対策が必要になってくること

  ➡ ゲートウェイ型のセキュリティソリューションを検討

- 暗号化通信についての取り扱いについて見直しが必要

  ➡ 暗号化通信のリスクを検証して対策を検討

ネットワークにおけるセキュリティ対策をご検討ください

お問い合わせ：https://info.a10networks.com/JP-WebContactUs.html

Thank You

アンケートにご協力お願いします。
https://business.form-mailer.jp/fms/fef556b3137447

A10

Always Secure. Always Available.