

# テレワーク環境の改善 NetScoutソリューション

2020年5月

ユースケース1. DDoS 攻撃からのテレワークアクセス保護

ユースケース2. SSLVPN監視

ユースケース3. ビデオ会議システム監視[Webex事例]

ユースケース4. OTTトラフィックの可視化

# ビジネス継続性ソリューション

リモートベースのユーザー生産性の保護



## リモートユーザーのパフォーマンスと可用性のために NETSCOUTが可視性を実現します。

COVID-19の世界的な広がりには、私たちの日常生活を変えるだけでなく、私たちが働く方法と場所も変えました。社員の仕事のやり方が突然劇的な変化がおり、ビジネスを遂行するために必要なサービスを遠隔地から利用でき、信頼性が高いレベルで実行できるようにすることが、これまで以上に重要です。

# NetScoutソリューション



## 可用性を保護

現在、これまで以上に、インターネット回線、VPNゲートウェイ、ファイアウォール、内部アプリケーションの可用性は、リモートの従業員や学生の生産性を維持するために重要です。NETSCOUTからのArbor Smart DDoS保護が役立ちます。

### DDoS防御



## UC&Cの品質

UC&Cシステムは、従業員、顧客、学生のライフラインとなっています。全体にわたって最高品質のユニファイドコミュニケーションおよびコラボレーションサービスを保証する必要があります。NETSCOUTソリューションは、会社の最高品質の音声およびビデオサービスを維持するのに役立ちます。

### UCサービス



## パフォーマンスを確保

顧客や従業員が必要とする場所に、信頼性が高く、利用可能で応答性の高いアプリケーションとサービスを提供することが最優先事項です。ボーダーなしのNETSCOUTの可視性は、インターネットまたはVPNを介してアクセスされるクラウドおよびオンプレミスのアプリケーションに役立ちます。

### サービス保証プラットフォーム

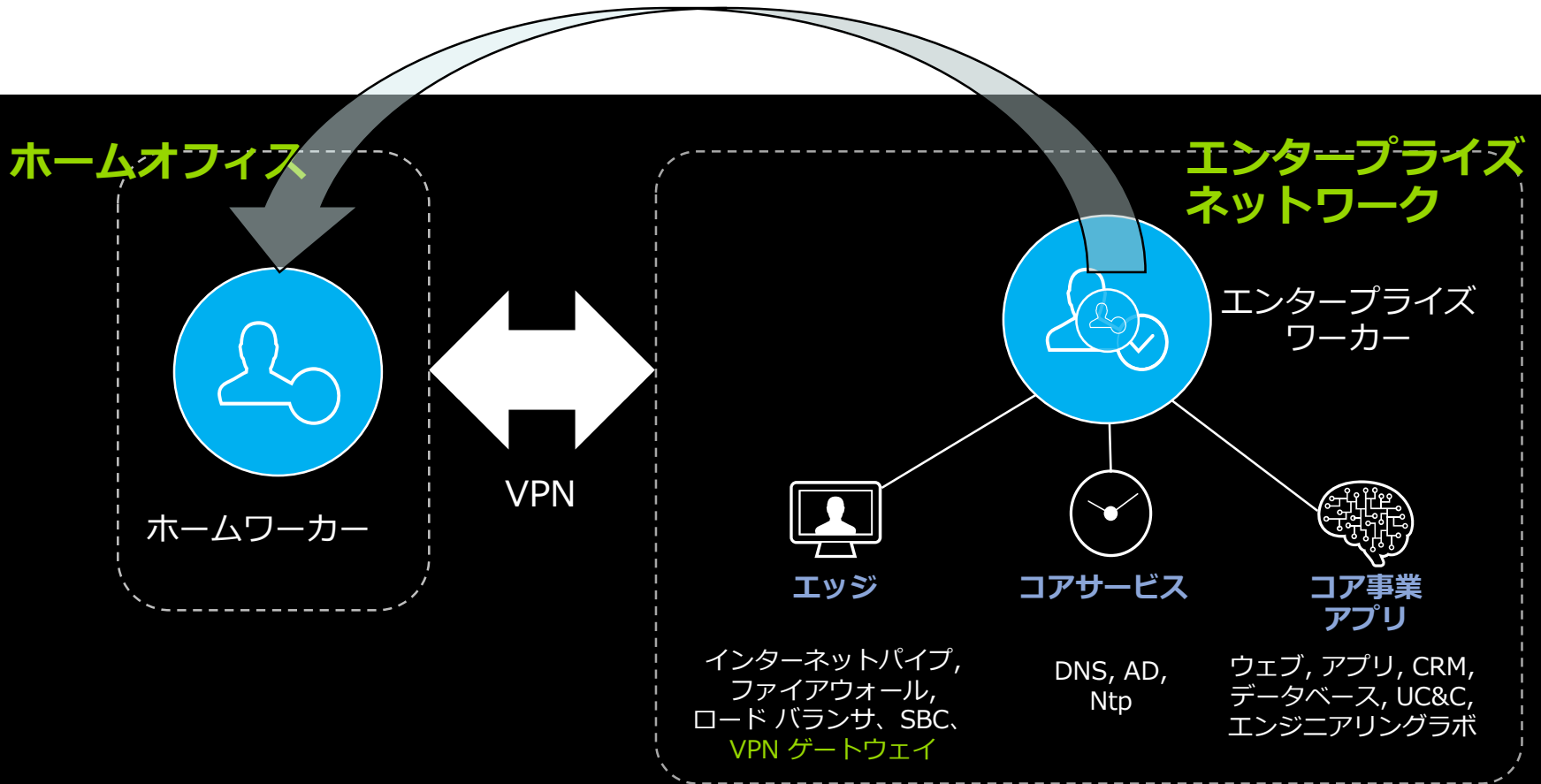


## コンタクトセンターエクスペリエンス

コンタクトセンターがお客様に製品やサービスを提供するための中心的な存在になるため、エクスペリエンスは鮮明で明確、かつ完全でなければなりません。NETSCOUTのソリューションを使用すると、コンタクトセンターを通じて高品質のカスタマーエクスペリエンスを提供できるようになります。

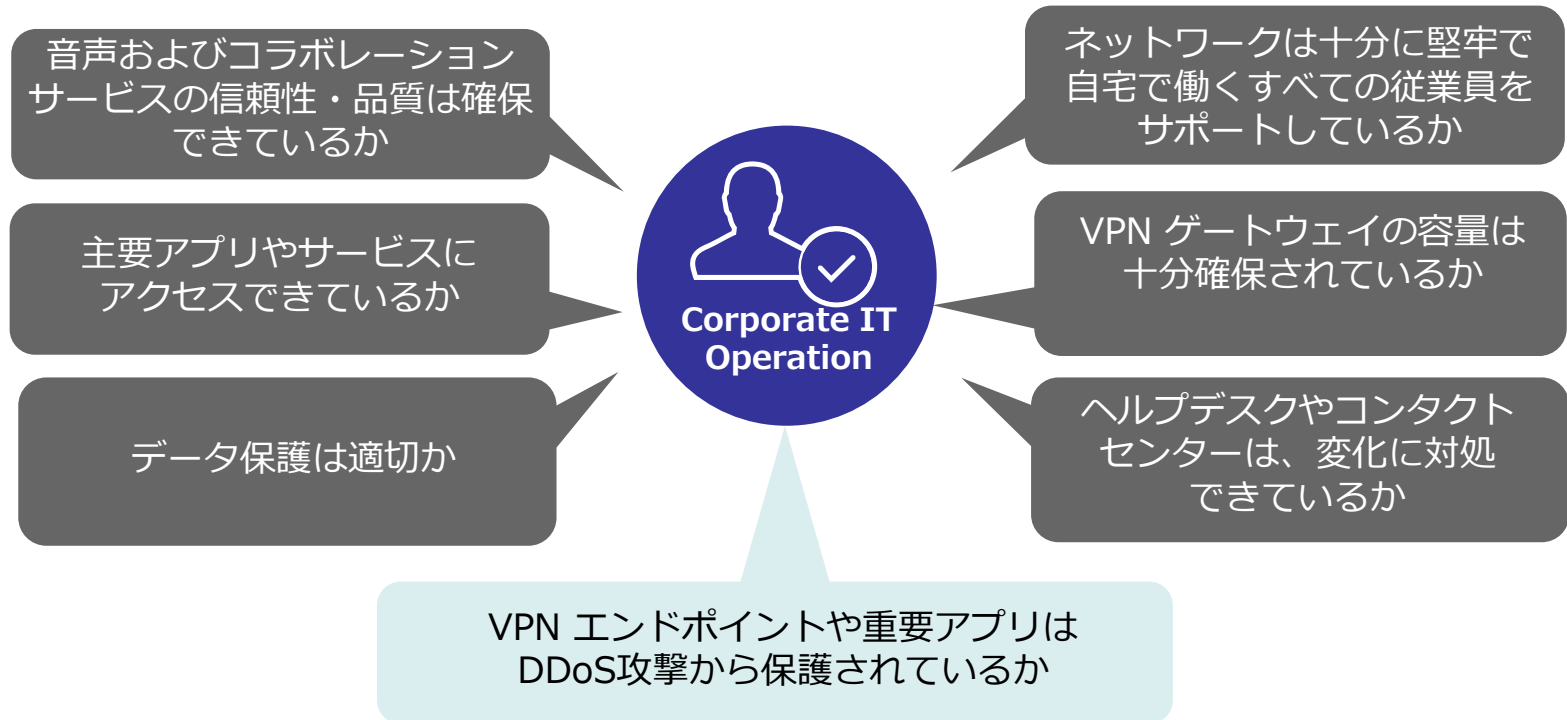
### あなたの基準を達成する

# 企業ネットワークの劇的な変化



# 企業ネットワークが直面する新たな課題

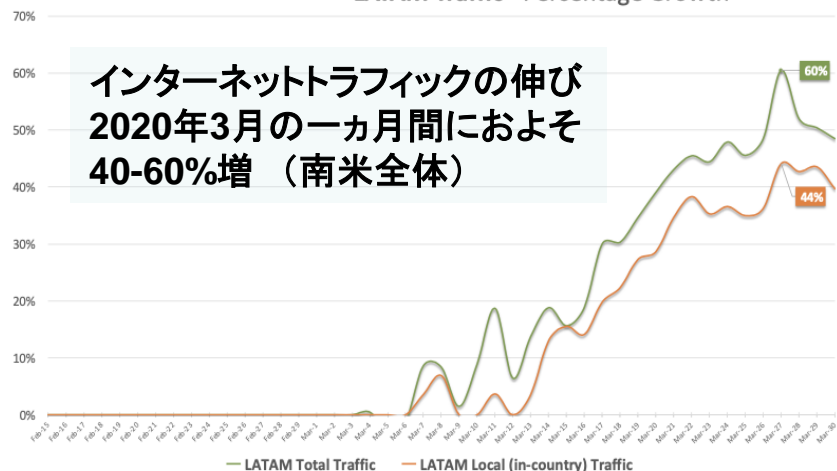
テレワークが企業の生産性を維持していることを確認する必要がある



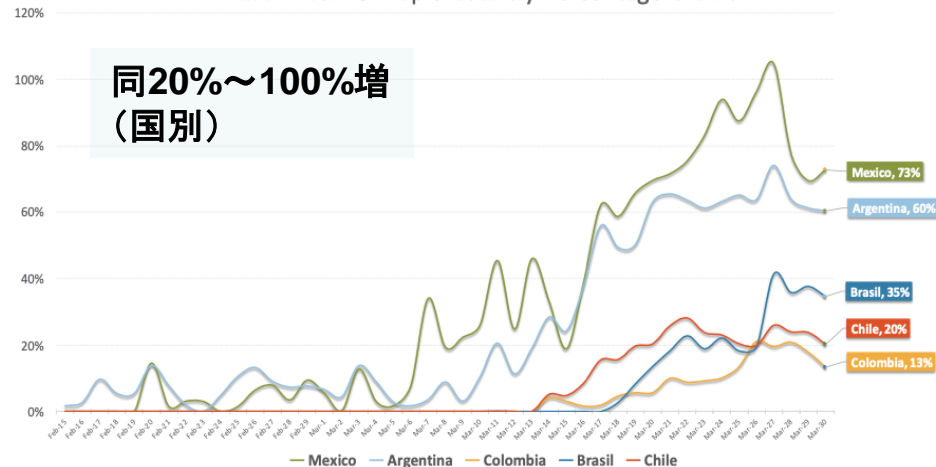
# 新型コロナウイルス感染症流行がインターネットに及ぼした影響(南米の例)

Traffic volume observed in LATAM region before and during COVID-19 contingency.

LATAM Traffic - Percentage Growth



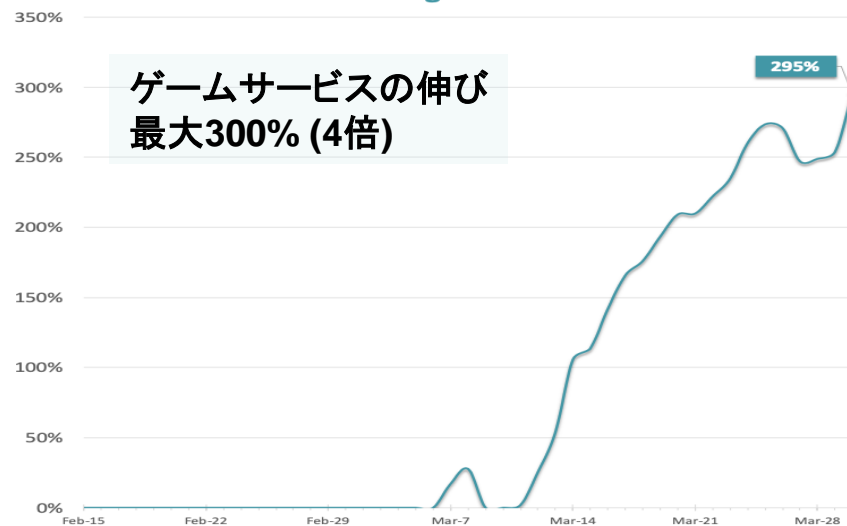
LATAM Traffic - Top 5 Country Percentage Growth



Video-conferencing services

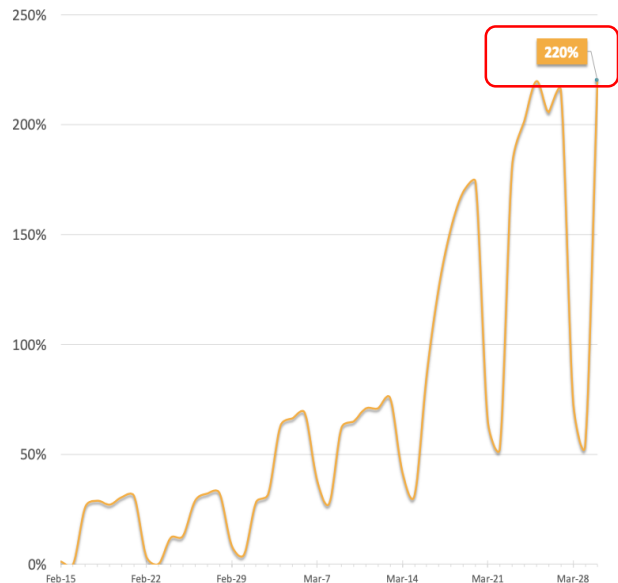


Gaming services



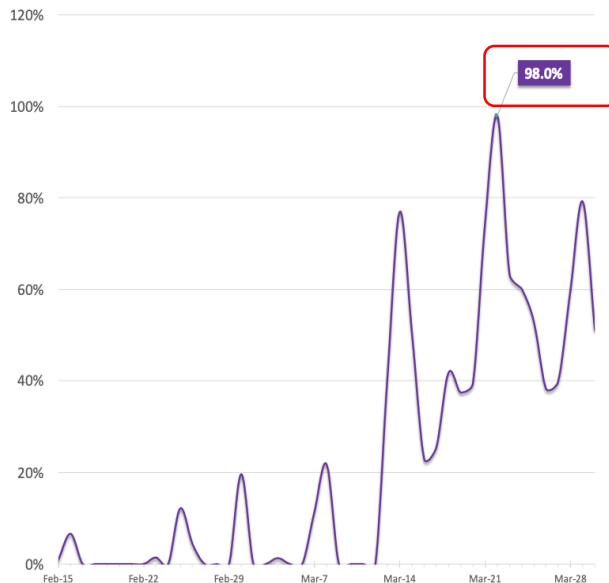
# 新型コロナウイルス感染症流行がインターネットに及ぼした影響(南米の例)

VPN services



VPNサービスの伸び  
最大200% (3倍)以上

Streaming services



ストリーミングサービスの伸び  
最大100% (2倍)

Social networks



SNSの伸び  
最大90% (1.9倍)

# ユースケース1

## DDoS 攻撃からのテレワークアクセス保護

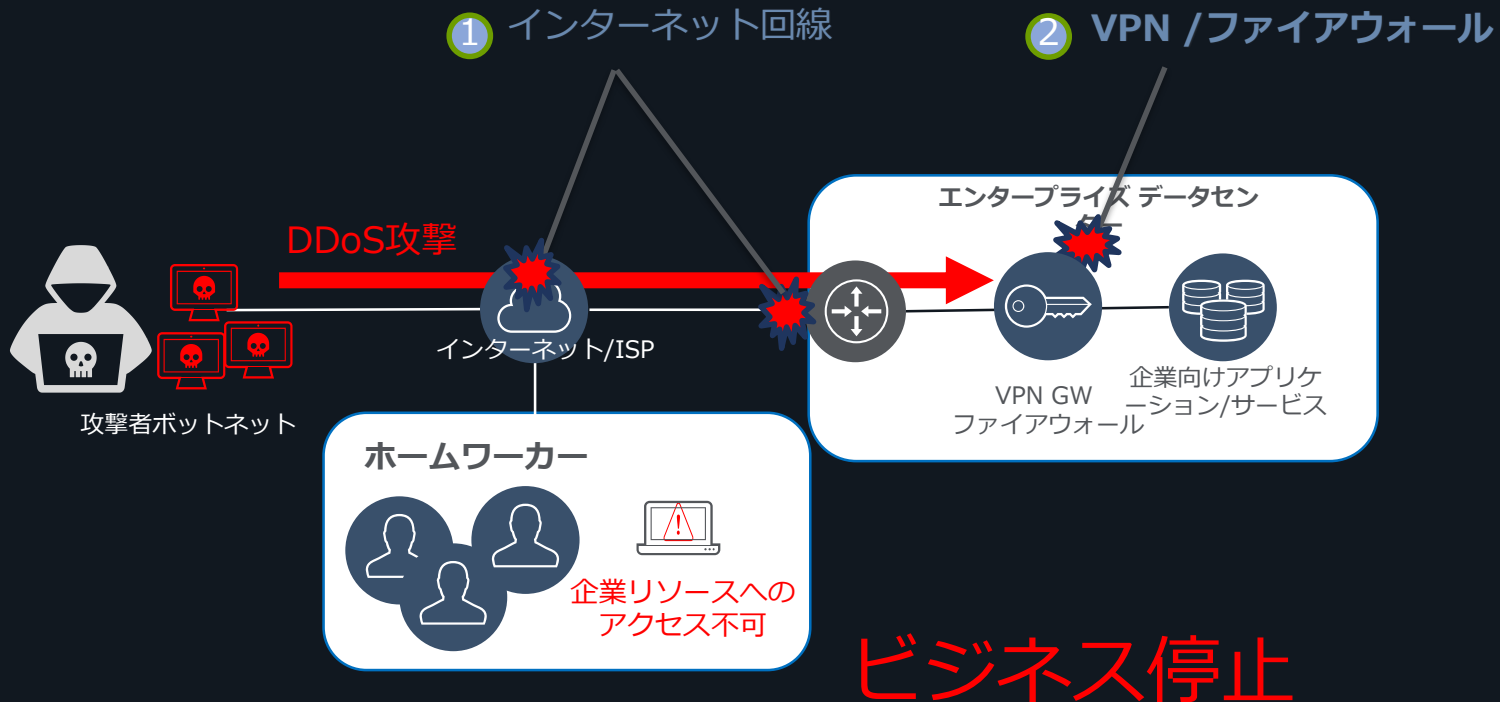


# DDoS攻撃対象の変化

従来の主な攻撃対象は、顧客向けアプリケーションサービス

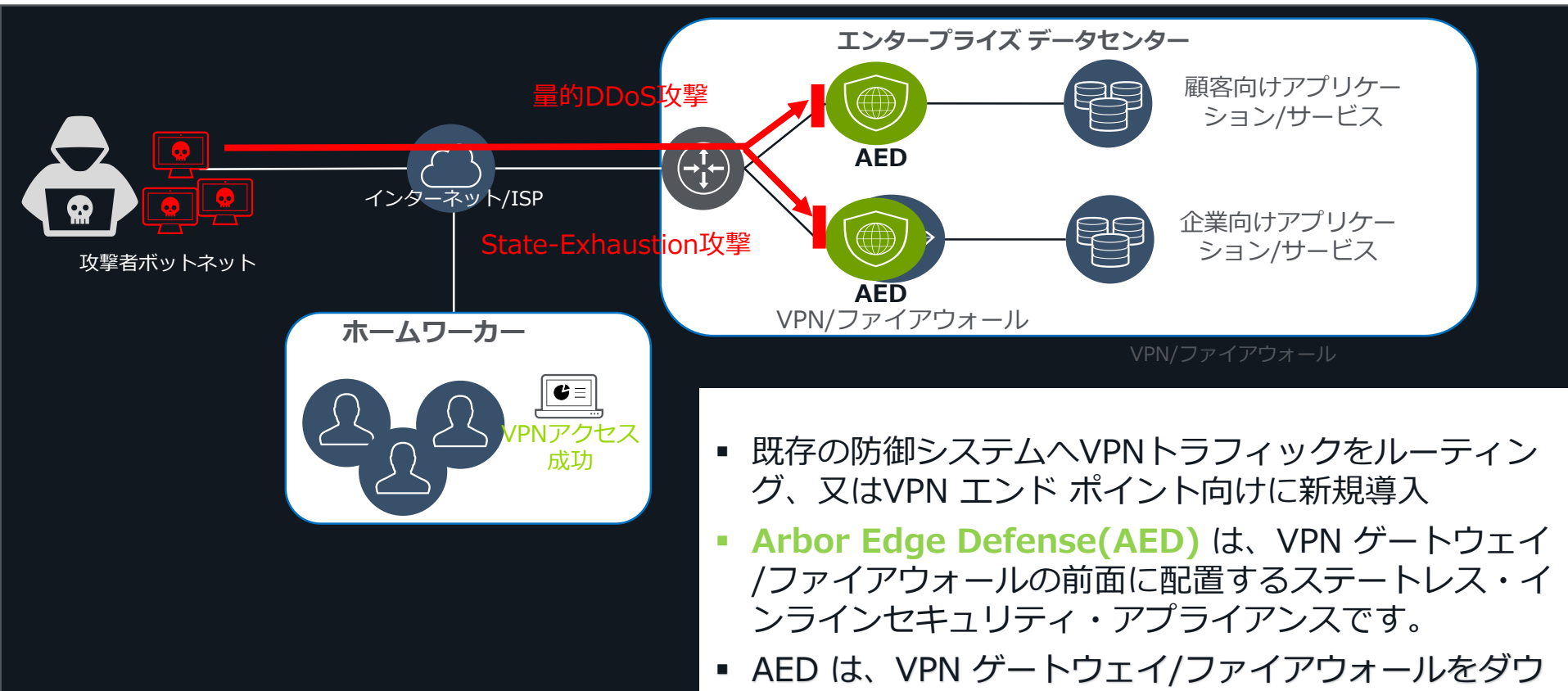


企業リソースへのホームワーカーアクセスが新たな攻撃対象



# 企業のためのスマートDDoS保護 Arbor Edge Defense(AED)

企業リソースへのホームワーカーアクセスの可用性を確保



- 既存の防御システムへVPNトラフィックをルーティング、又はVPN エンドポイント向けに新規導入
- **Arbor Edge Defense(AED)** は、VPN ゲートウェイ/ファイアウォールの前面に配置するステートレス・インラインセキュリティ・アプライアンスです。
- AED は、VPN ゲートウェイ/ファイアウォールをダウンさせるように設計されたすべてのタイプの DDoS 攻撃を自動的に検出し、軽減します。

- リアルタイムでトラフィックを瞬時に可視化、すべての攻撃を検出し軽減
- 常にトラフィックを監視し、良好なトラフィックを実現し、誤検知なしで正確な保護を提供
- インライン・オンプレミスであるため、インターネット上のルーティング変更は不要
- 単一のUIを使用した迅速な問題解決
- アプライアンス、仮想アプライアンス
- インバウンドだけでなくアウトバウンド方向の脅威検出・ブロック

# 既にDDoSサービスを利用している場合・・・

- **キャリア/ISP、CDNなど第三者からDDoS対策サービスを提供されている場合**
  - 常にDDoSチェックを行う「Always On」モードでは、企業のトラフィックはすべて「不自然」に第三者を経由する
    - 攻撃を受けている間、企業はトラフィックの制御性を失い、或いは遅延の可能性がある
    - 高価である
  - 攻撃時のみ防御を依頼する「オンデマンド」モードでは、第三者は正常トラフィックのベースライン（通常の間や変動）を知らない
    - オーバーストッピングや誤検知の可能性
  - VPN ゲートウェイに対する効果的な攻撃には大規模な攻撃は不要であるが、これまでは“攻撃者”と“被攻撃者”のどちらにとってもそれほど興味を引く問題ではなかった。多くの非VPNのケースと同様に、これからは大きな問題となり得る。
- AEDのオンプレミス導入が唯一の実行可能なソリューション

# ユースケース 2

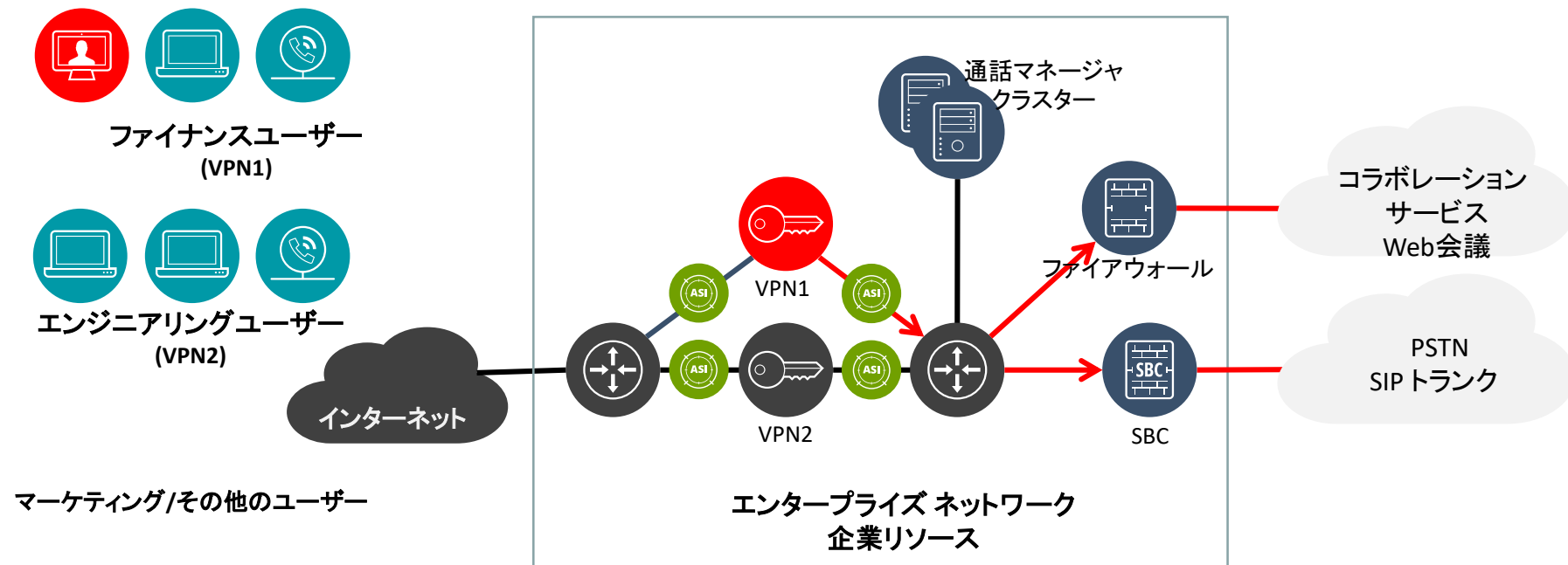
## SSLVPN監視

# VPNゲートウェイの飽和：原因と影響の把握

これまで企業ネットワーク内に終始していたトラフィックが、テレワークの増加に伴いインターネット経由に移行



インターネット向け回線、VPNゲートウェイの容量・品質に大きなインパクト



# ネットワーク構成例と監視事例

NETSCOUT.

## インターネット トラフィック

- ゲートウェイの時間経過に伴う使用パターン分析
- ビジー状態の間にリンクの飽和状態を特定する
- パケット損失などの着信トラフィックの問題の存在を検出する

1

## VPN トラフィック

- ユーザーグループ別のビジネスサービスの使用分析
- 使用状況に応じてユーザーグループまたはVIP/パワーユーザーを再割り当て
- VPN 経由のビジネスネットワークの不適切な使用を特定する
- ゲートウェイリソースの不足・枯渇によるトラフィック劣化検出

1

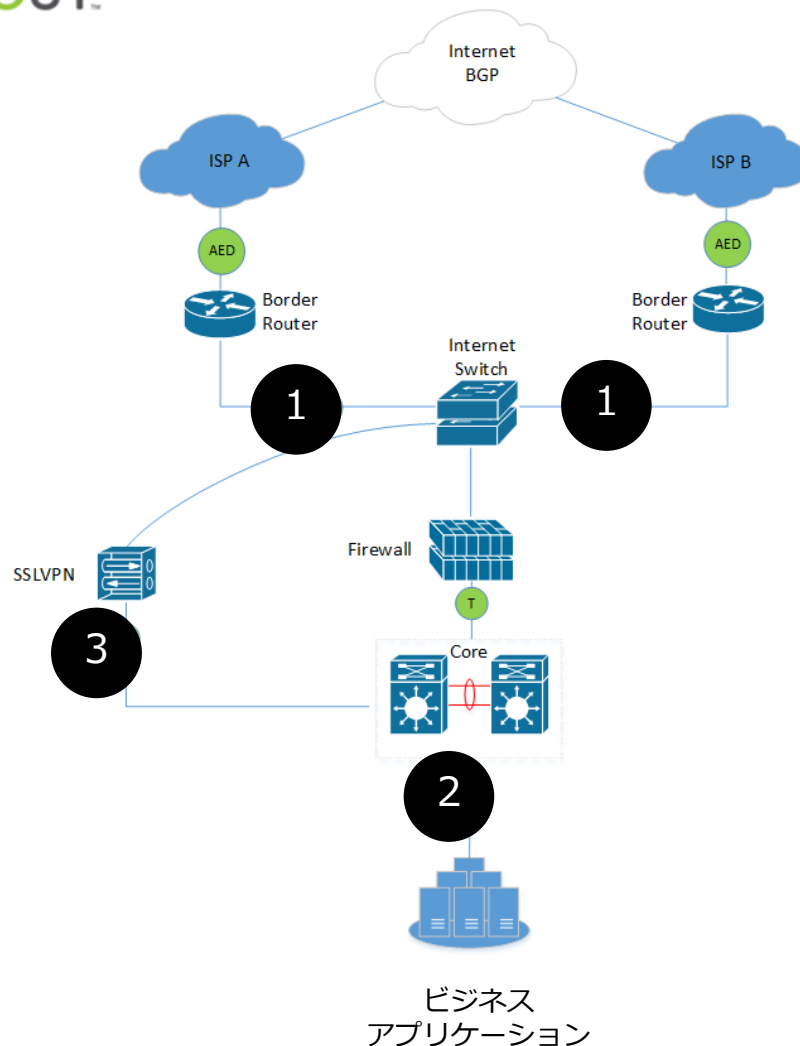
3

## ビジネスサービス

- ビジネス アプリケーションの正常性と使用状況
- VDI サービスの正常性
- 企業に出入りするメディア品質
- リモート ユーザーとのリンクに関する問題を特定する

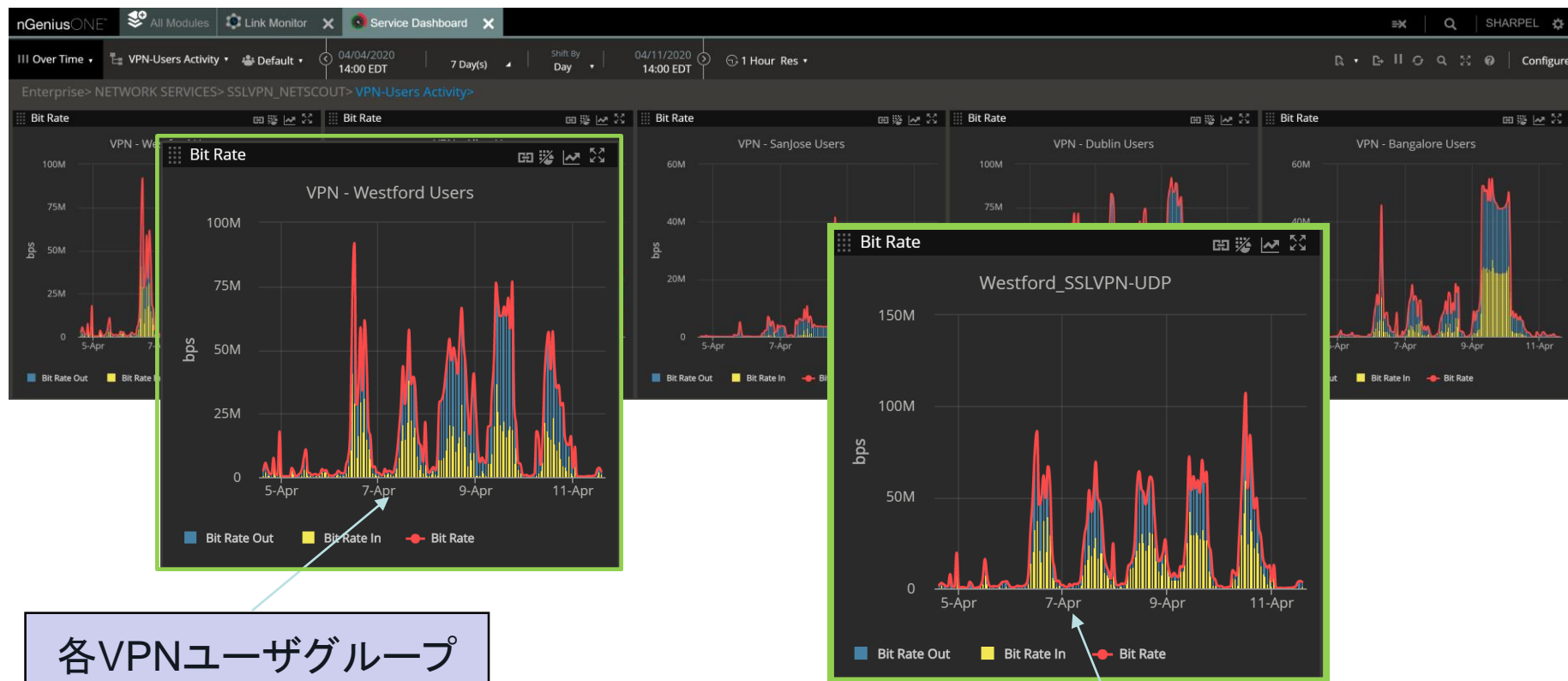
2

## Hub Internet Edge Design



ビジネス  
アプリケーション

## nGeniusONE – VPNユーザグループ毎の使用帯域推移 (Up/Down)



各VPNユーザグループ  
使用帯域推移

各VPNユーザグループ  
SSLVPN-UDP(ストリーミング向け)  
使用帯域推移



## nGeniusONE – VPNユーザグループ毎の使用アプリケーション分析

VPNゲートウェイ及びユーザグループの識別

1	<input checked="" type="checkbox"/>	IS	WST-NG1:WSTINF07:SSL_VPN	Not Defined
2	<input type="checkbox"/>	IS	WST-NG1:WSTINF08:Silverpeak	Westford VPN_Users
3	<input type="checkbox"/>	IS	WST-NG1:ALLEN_INF01:SilverPeak	Westford VPN_Users
4	<input type="checkbox"/>	IS	WST-NG1:EQX_USA_ISNG:if5	Westford VPN_Users
5	<input type="checkbox"/>	IS	WST-NG1:SJC_INF01:Sil	
6	<input type="checkbox"/>	IS	WST-NG1:ARBOR:Silver	
7	<input type="checkbox"/>	IS	DUB-NG1:DUBINF01:Sil	

Packets (K)	% Utilization	Bit Rate (Kbps)	Packet Rate (pps)
Total	Total	Total	Total
1,837,181.84	0.03	13,744.70	3,037.67
306,402.27	0.10	2,926.89	506.62
149,324.27	0.06	2,036.72	246.90
33,891.12	0.01	300.51	56.04
16,157.48	0.00	145.40	26.72

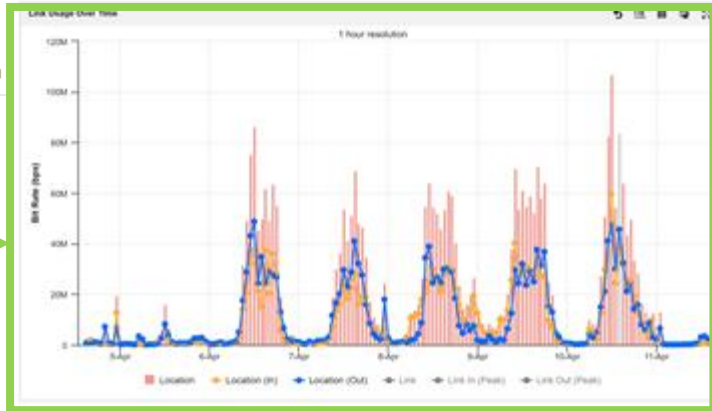
  

Traffic Distribution by Application

Top 10 Application by Bit Rate (bps)

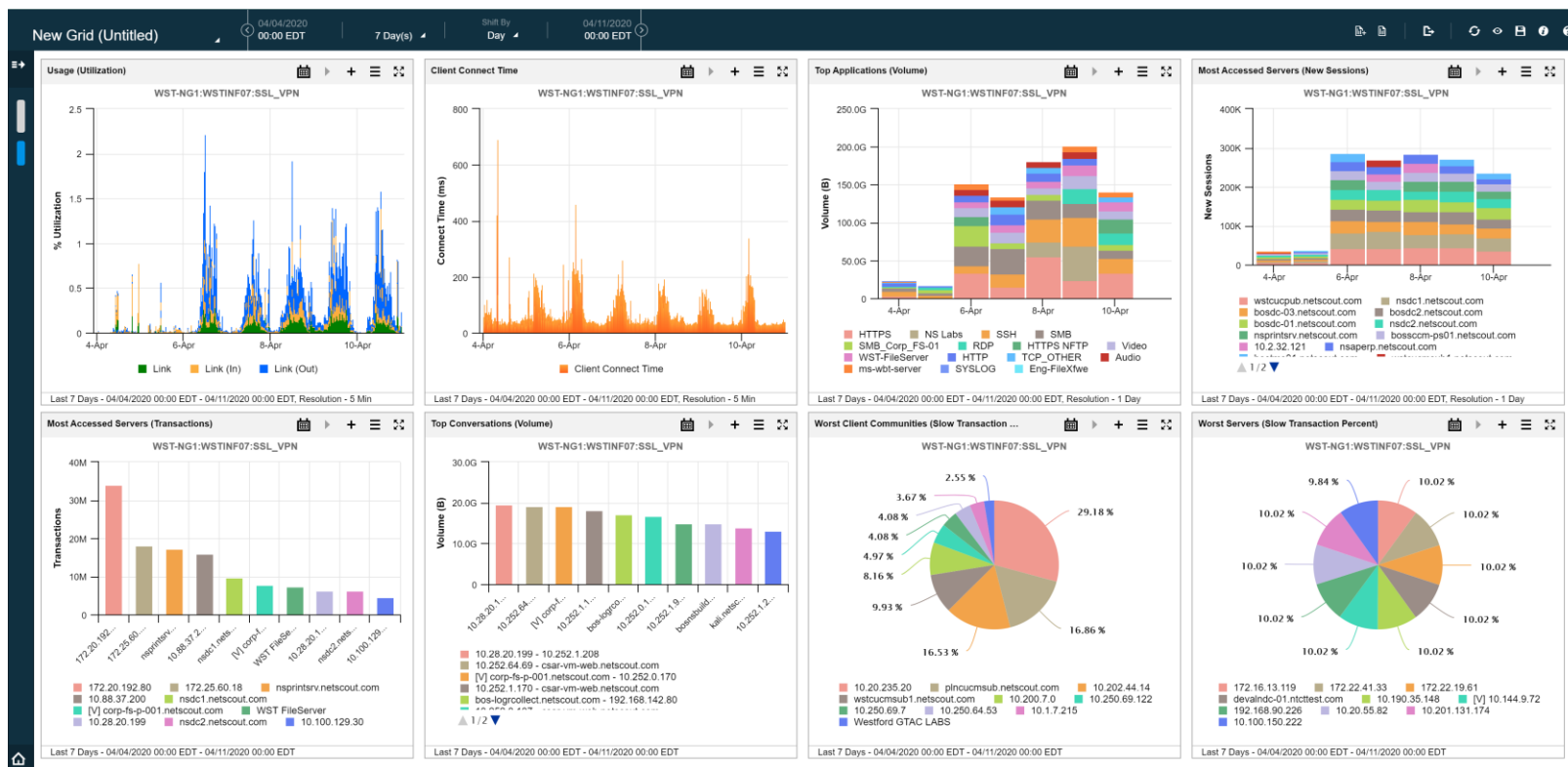
トラフィックのアプリケーション内訳

トラフィックのアプリケーション毎推移



## nGeniusONE – VPN 向けグリッド

- トラフィック推移、応答時間推移
- TopNアプリケーション、TopNユーザグループ
- TopNクライアント、TopNサーバ、TopNカンバセーション etc.



## ユースケース 3

# ビデオ会議システム監視[Webex事例]

# WebEx監視シナリオの背景と環境

## [在宅勤務移行後、問題が発生]

- 2部門の社員が在宅勤務に移行した際に、特定部門VPNを経由したWebEx回線の品質が昼間時間帯に劣化

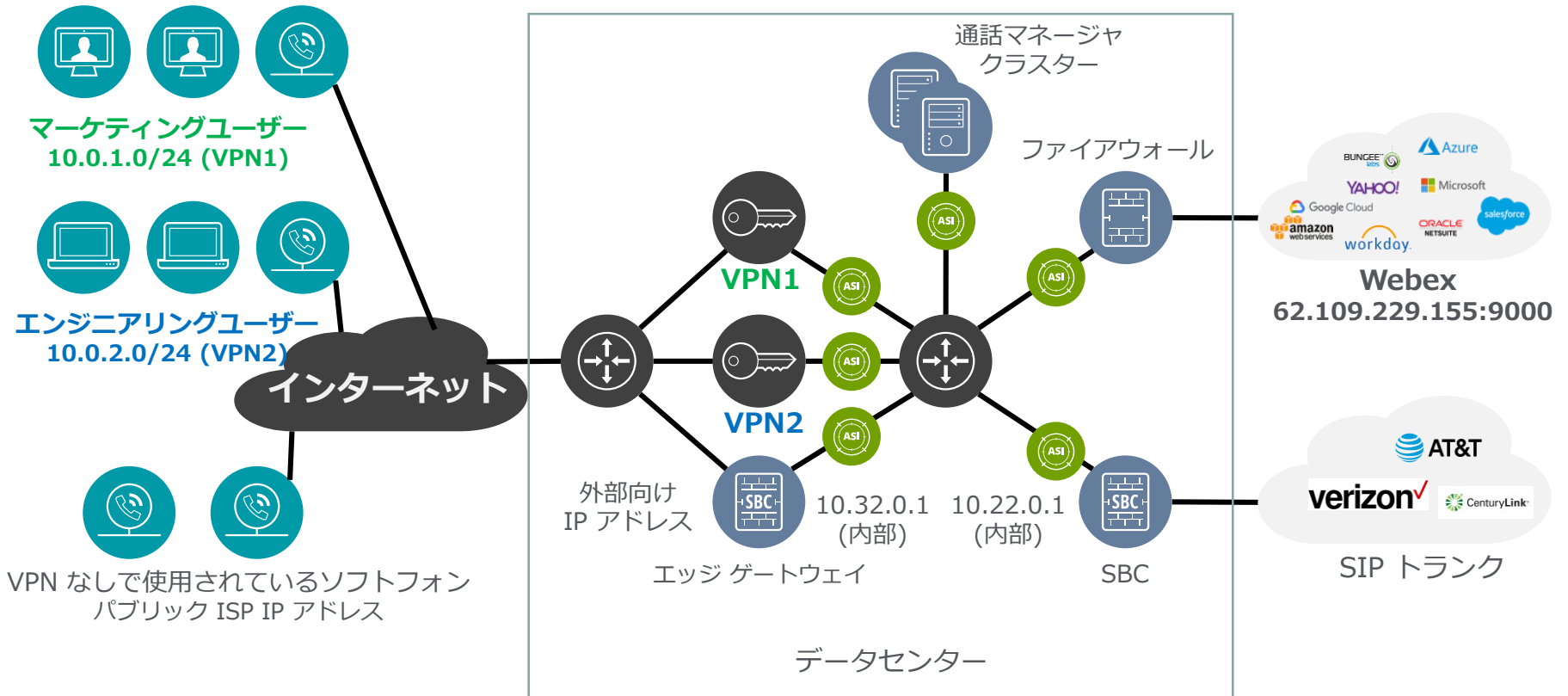
## [VPN・WebEX環境]

- エンジニアリングとマーケティングの従業員が、VPNを使用して企業リソースに接続
- マーケティングのユーザーのラップトップはVPN1に接続、エンジニアリングのユーザーはVPN2に接続
- エンジニアリング部門はWebEx会議でのビデオ使用が不可
- マーケティング部門ではWebEx会議でのビデオ使用が自由

## [nGeniusONEによる調査・分析]

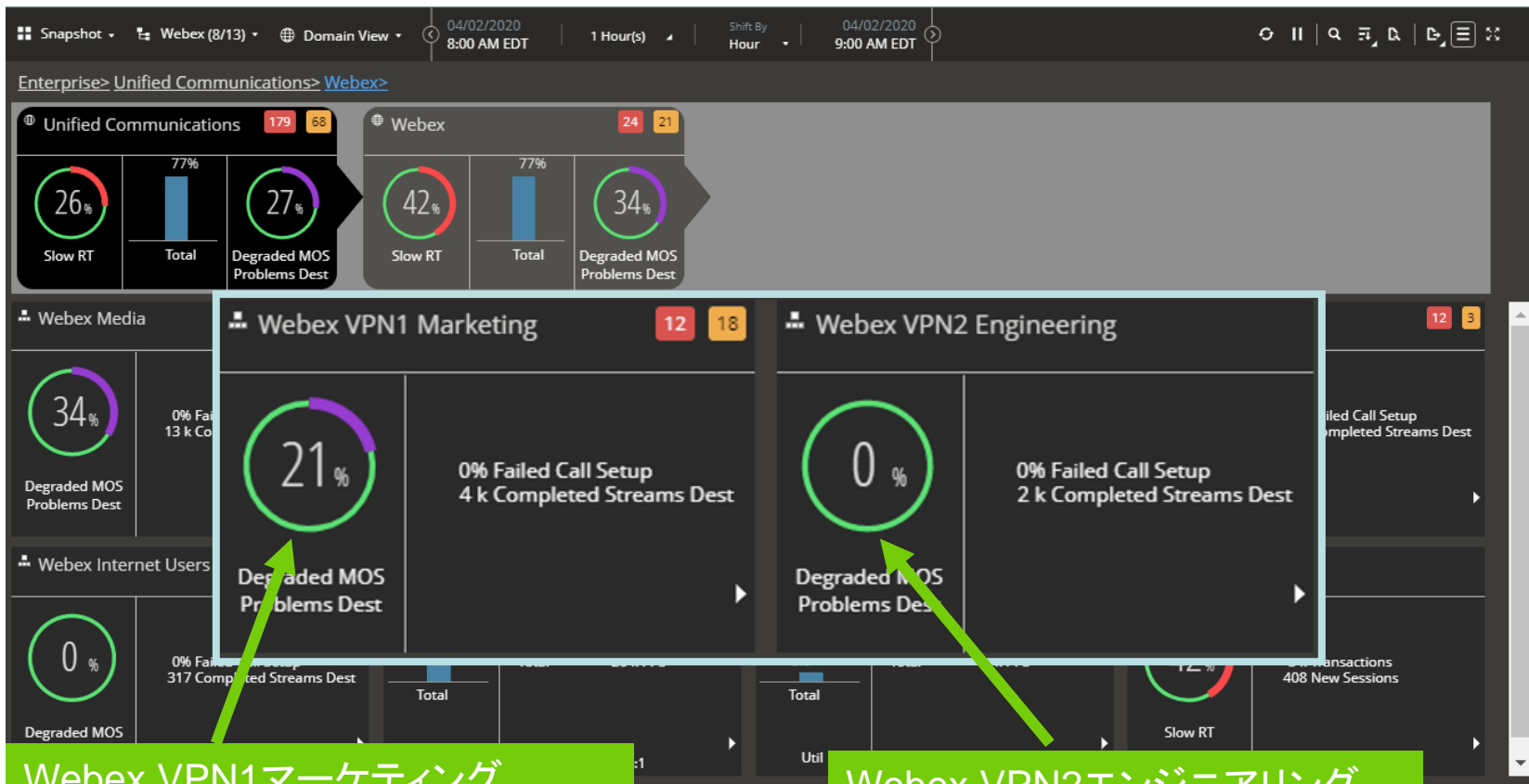
- マーケティングユーザーが使用するVPN1は、営業時間時、特にピーク時(午前9時から午前11時EDT)で飽和状態
- パケットがドロップされ、マーケティングチームのWebEx会議や音声およびビデオの品質低下を数値で確認
- マーケティングチームのビデオ使用により、一部のVPNゲートウェイが過負荷となっていることを確認

# ネットワーク アーキテクチャ



# サービス ダッシュボード

- 品質の劣化を視覚的に確認
- VPNゲートウェイ毎に状況が異なることを容易に切り分け

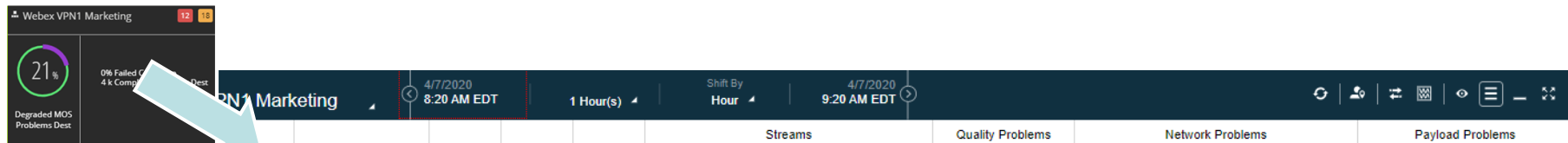


Webex VPN1マーケティング  
品質問題発生  
MOS値(音声評価値)の劣化を確認

Webex VPN2エンジニアリング  
品質問題なし

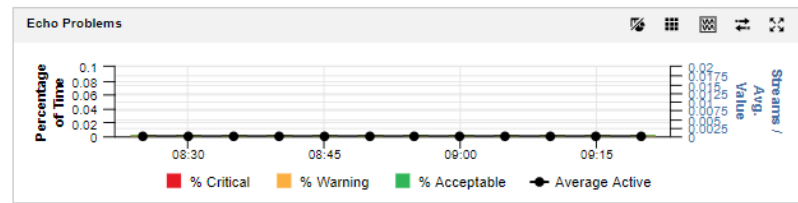
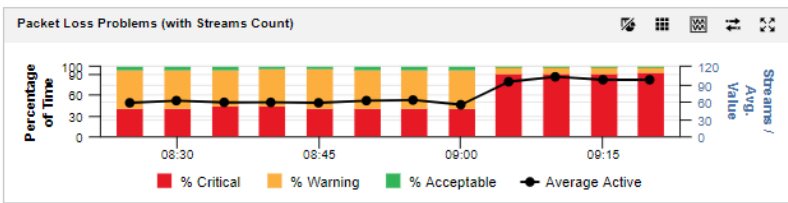
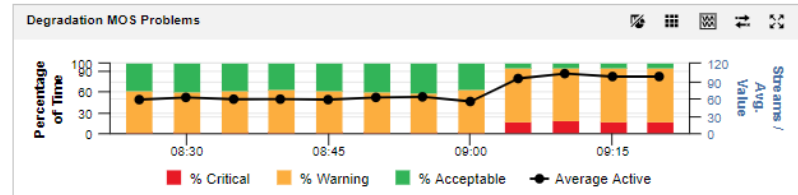
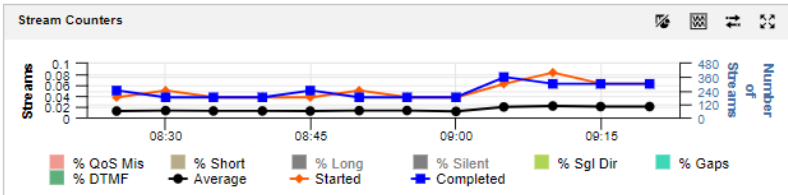
# VPN1マーケティング - メディアモニター

- アプリケーション（WebEx音声、 WebEx映像、 非WebEx VoIP） 毎に各種の品質指標を確認
- 品質推移を任意の時間帯で切り取って確認



1. オーディオ - 非-Webex ソフトクライアントとのコール,コーデック = G.711  
 2. Webex-RTP - Webex ビデオ, コーデック= H.264  
 3. Webex-RTP - Webex 音声, コーデック=オーパス

すべてのアプリケーションサービスでパケット損失とMOS低下を観測



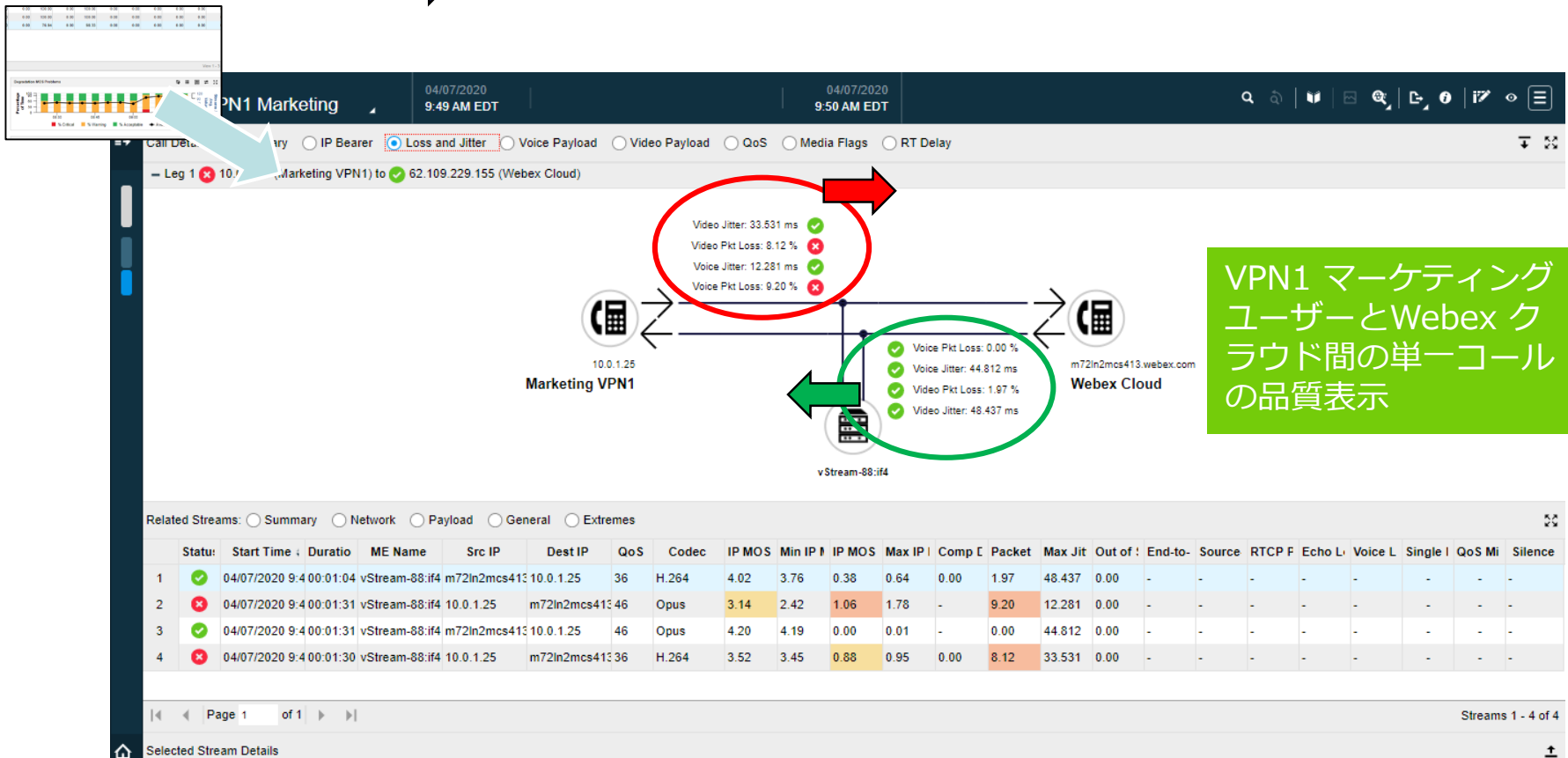




# VPN1 マーケティング - シングルコールビュー

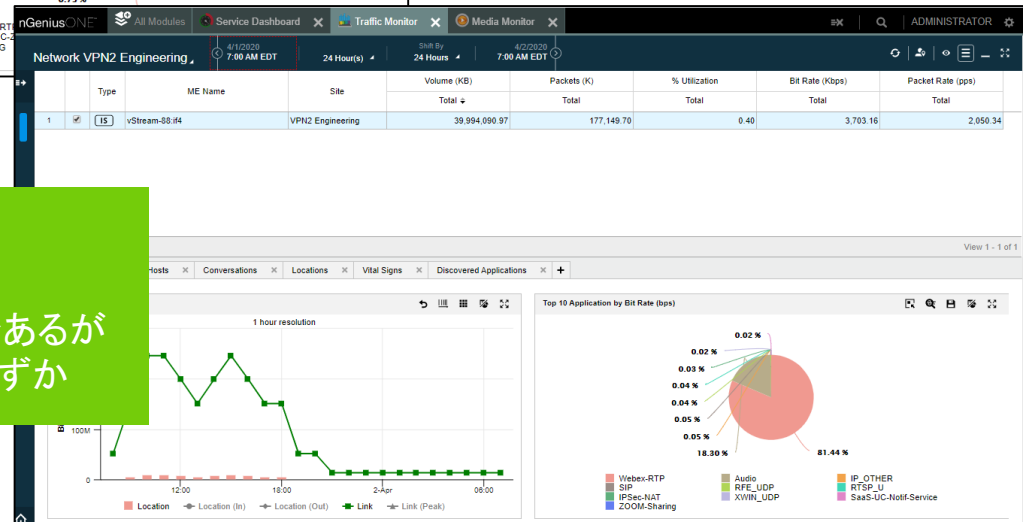
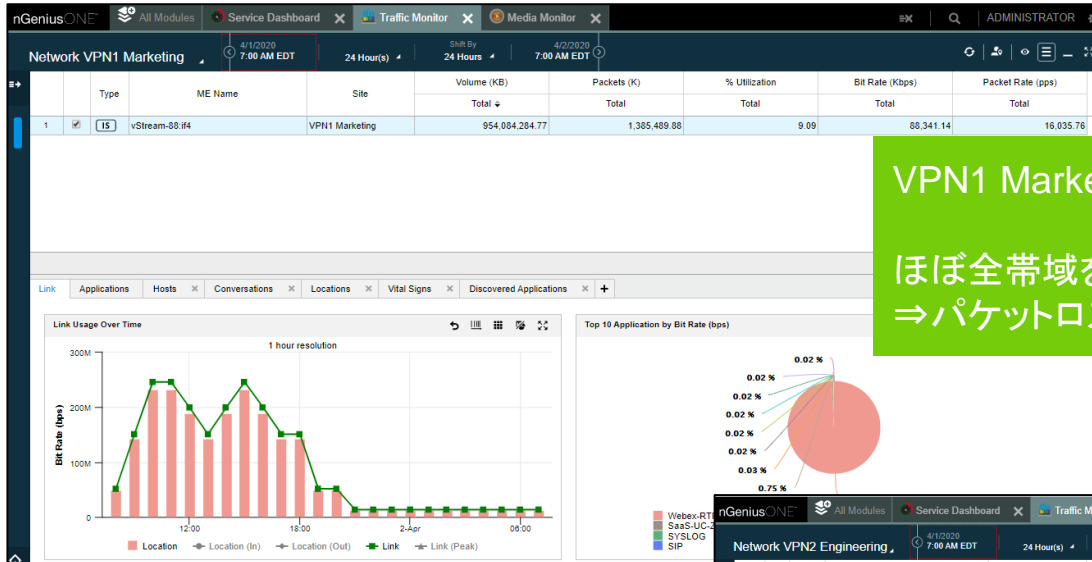
- 「単一回線」の品質状態を分析
- クライアント⇒クラウド方向の劣化のみ発生していることを確認

➡ クライアント～VPNゲートウェイ間のネットワークで問題発生



VPN1 マーケティング  
ユーザーとWebex ク  
ラウド間の単一回線  
の品質表示

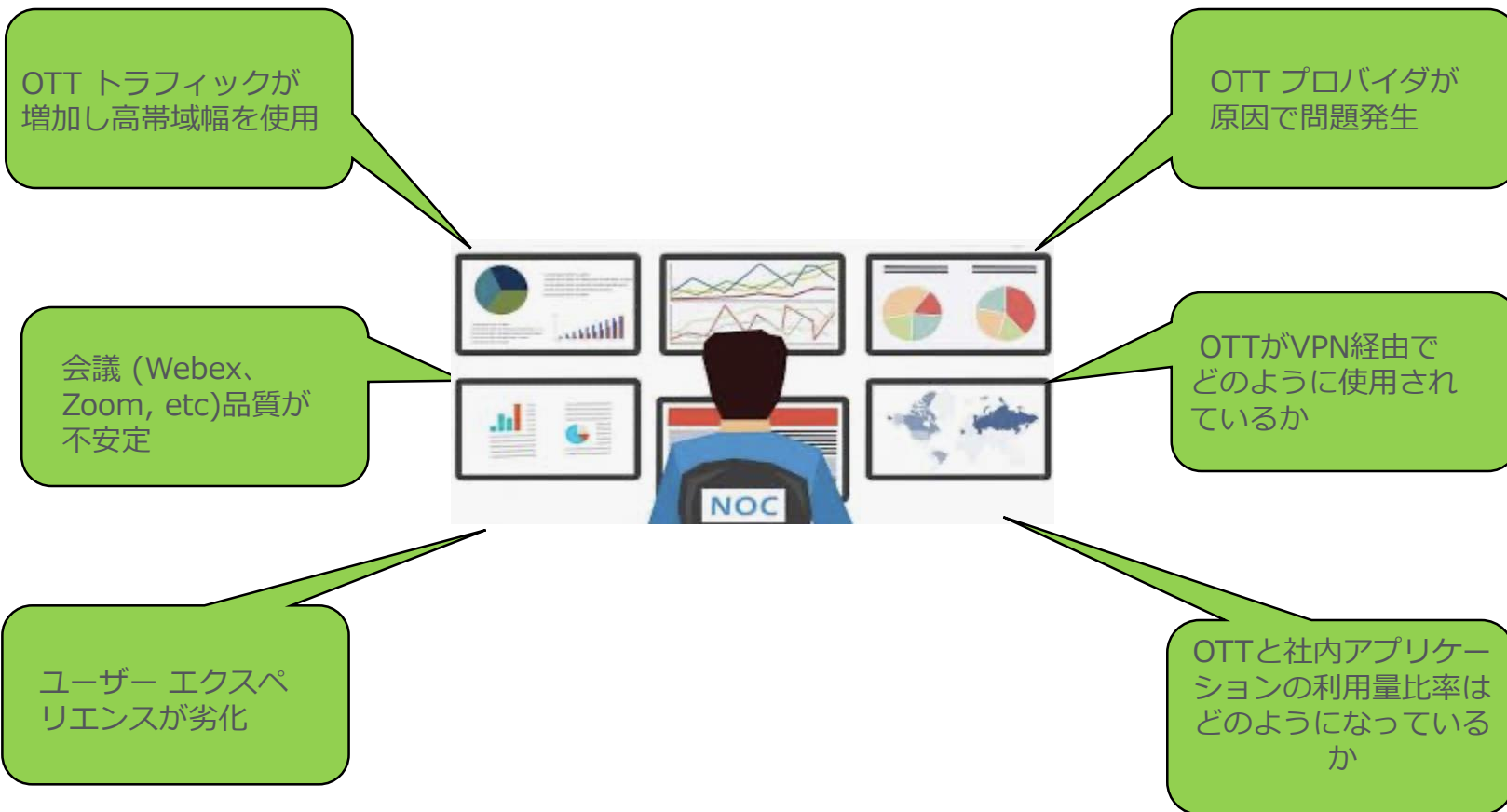
# トラフィックモニター



## ユースケース4

# OTT トラフィックの可視化

# テレワークが直面するOTTに関わる新たな課題



## AIFとは

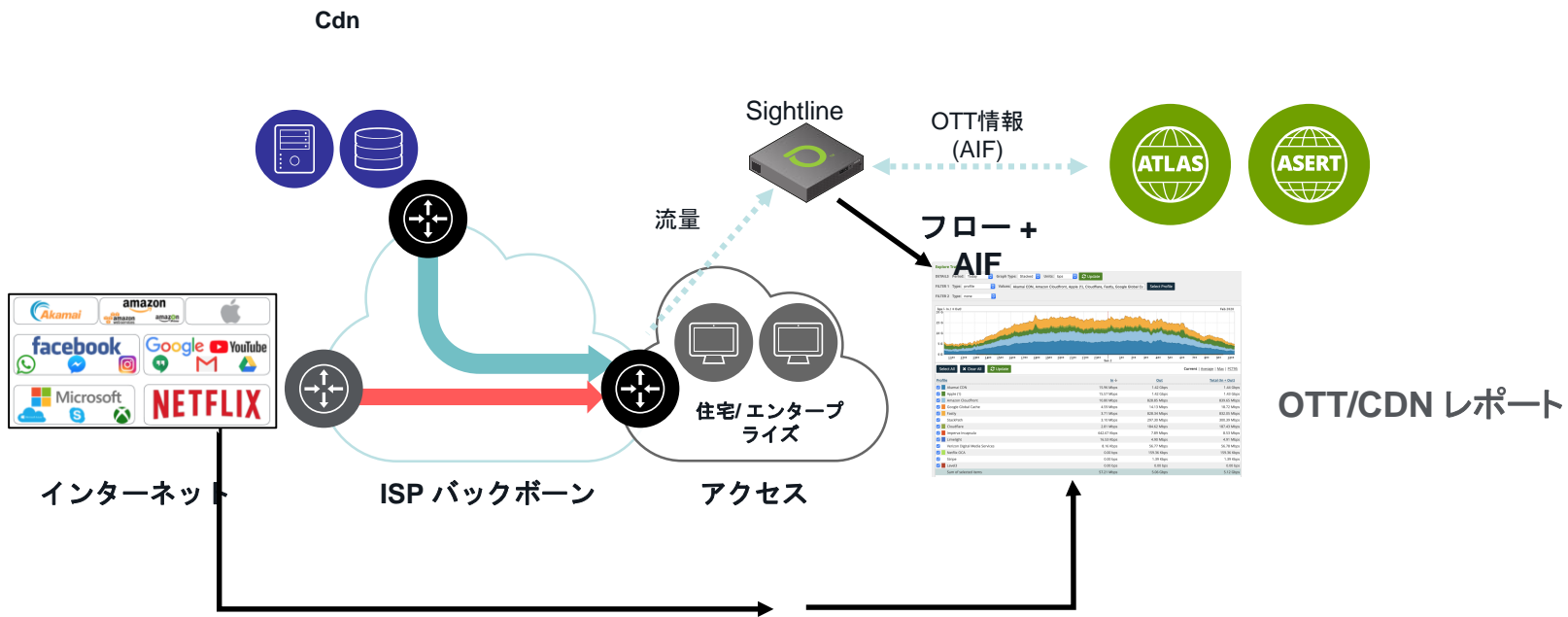
- Sightline、AEDなどのNETSCOUTセキュリティアプライアンスに対して、脅威情報やOTT情報をオンラインで配信するサービス

## AIFによるOTT可視化

- OTT が企業ネットワークに与えている影響を理解
- 企業活動の一環で使用しているOTTの状態を把握
- ネットワークの輻輳が始まる前にルーティング変更やOTTの利用抑制などを行う手助けをする
- どのような OTT が企業活動に価値あるものかを理解
- ネットワーク容量計画の支援

# OTT/CDN を使用した AIF 署名

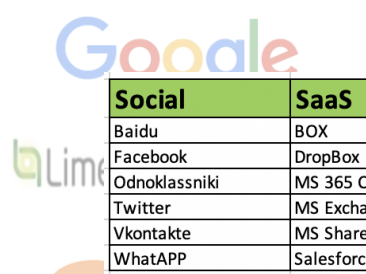
- NETSCOUT ASERTによりIPアドレスレンジなどのOTT情報を収集
- AIF加入者機器に対してOTT情報をフィード



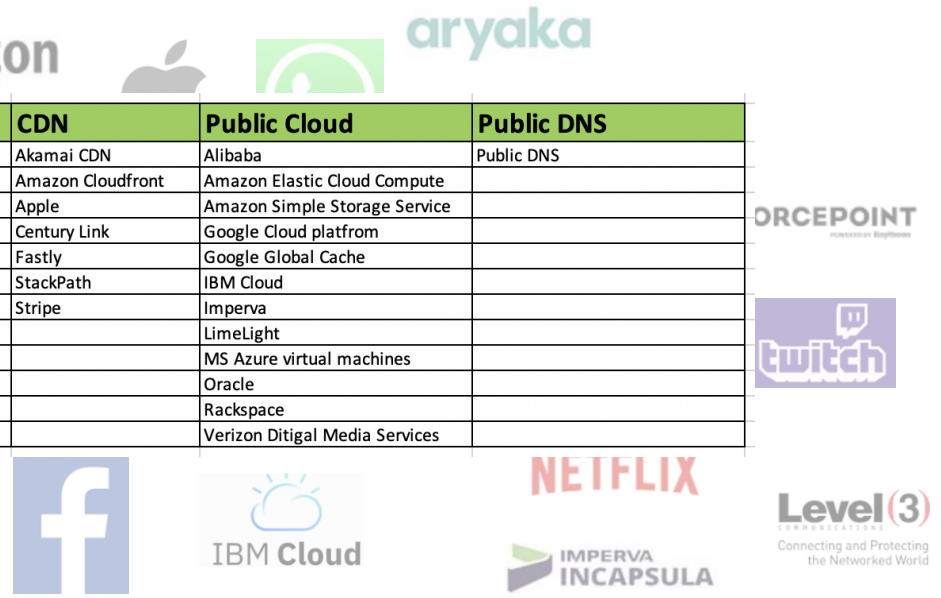
# AIF-OTT – 管理対象OTT



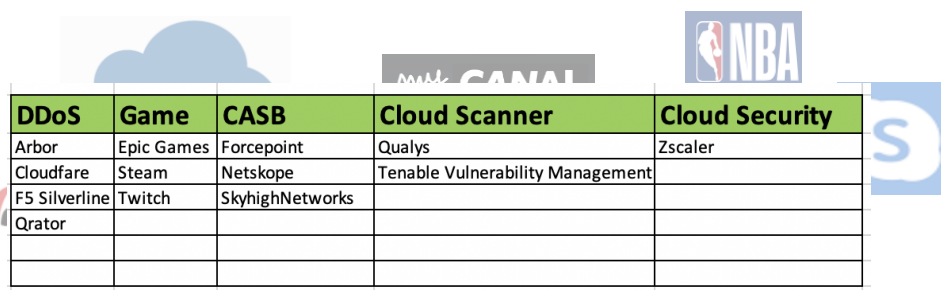
Streaming	Collaboration	CDN	Public Cloud	Public DNS
AfreecaTV	Dialpad	Akamai CDN	Alibaba	Public DNS
Bild	Google Hangouts Meet	Amazon Cloudfront	Amazon Elastic Cloud Compute	
Disney	RingCentral	Apple	Amazon Simple Storage Service	
ESPN	Skype for Business Online and MS Team	Century Link	Google Cloud platform	
HBO	Webex	Fastly	Google Global Cache	
Hulu	Zoom	StackPath	IBM Cloud	
iQIYI		Stripe	Imperva	
myCANAL			LimeLight	
NBA			MS Azure virtual machines	
Netflix			Oracle	
			Rackspace	
			Verizon Digital Media Services	



Social	SaaS	SD-WAN
Baidu	BOX	Aryaka
Facebook	DropBox	Meraki
Odnoklassniki	MS 365 Common and Office Online	VeloCloud
Twitter	MS Exchange oNLINE	
Vkontakte	MS Sharepoint Online and One Drive	
WhatsApp	Salesforce	



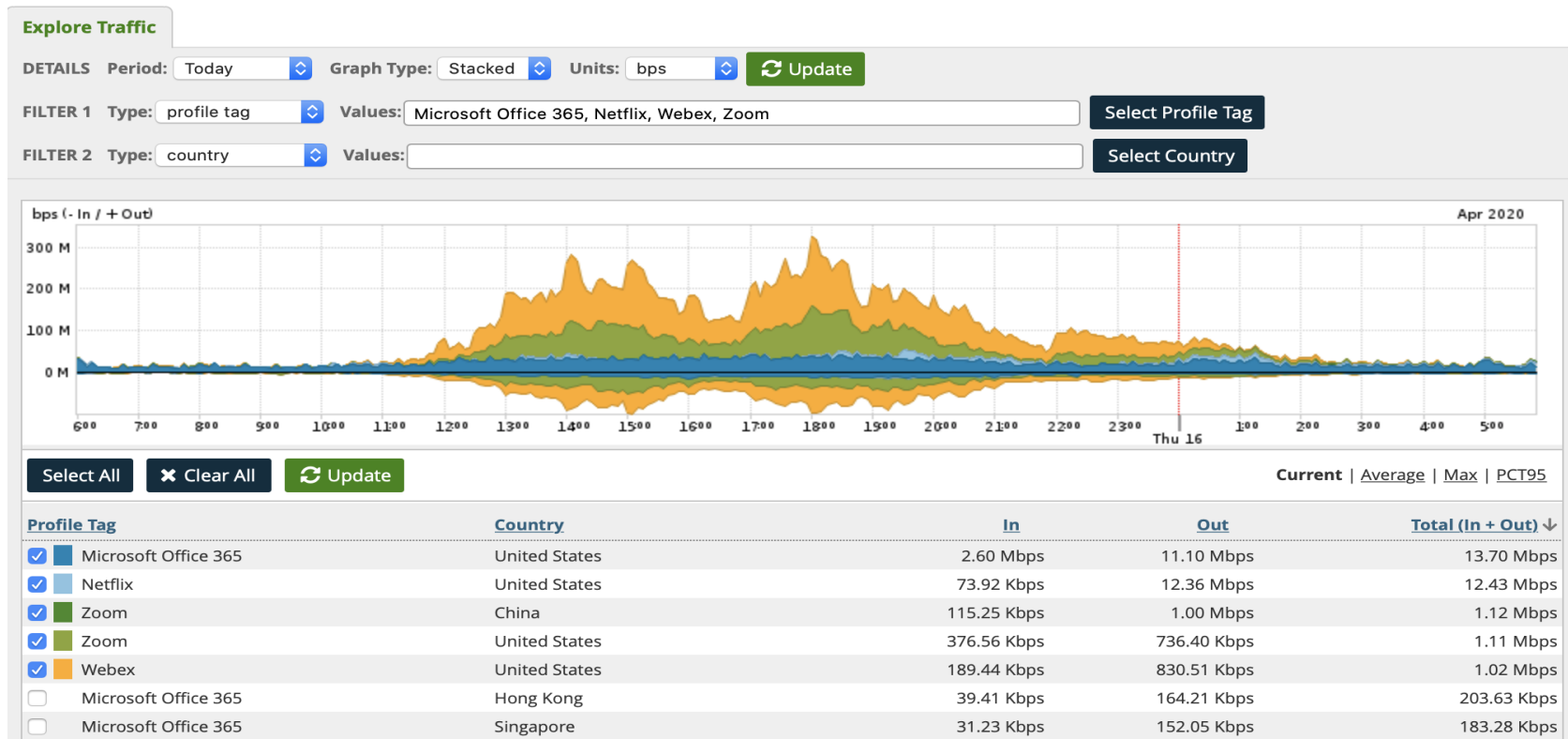
DDoS	Game	CASB	Cloud Scanner	Cloud Security
Arbor	Epic Games	Forcepoint	Qualys	Zscaler
Cloudfare	Steam	Netskope	Tenable Vulnerability Management	
F5 Silverline	Twitch	SkyhighNetworks		
Qrator				



# サンプル レポート (Sightline) – Web会議

- 企業ネットワークを介してアクセスされるWeb会議トラフィック
- OTT トラフィックがどこから来たか（国別、CDN別、AS別・・・）

## Office365, WebEx, Zoomの可視化事例



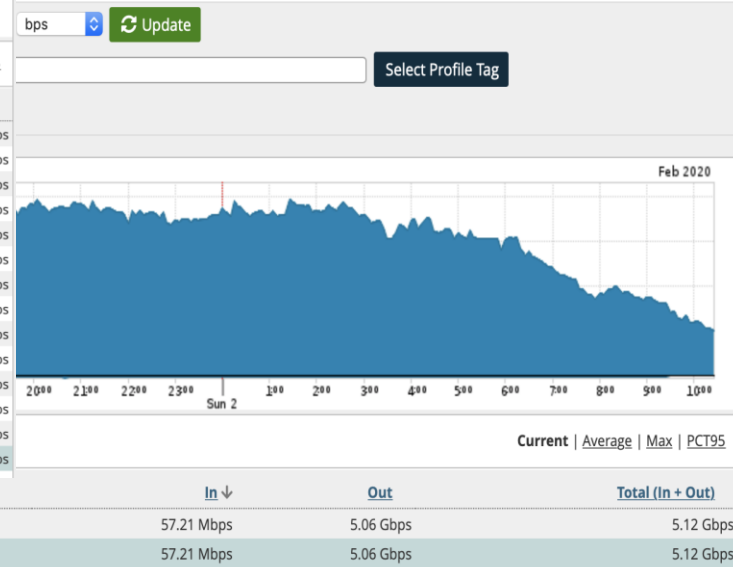


# サンプルレポート (Sightline) – CDN プロバイダー

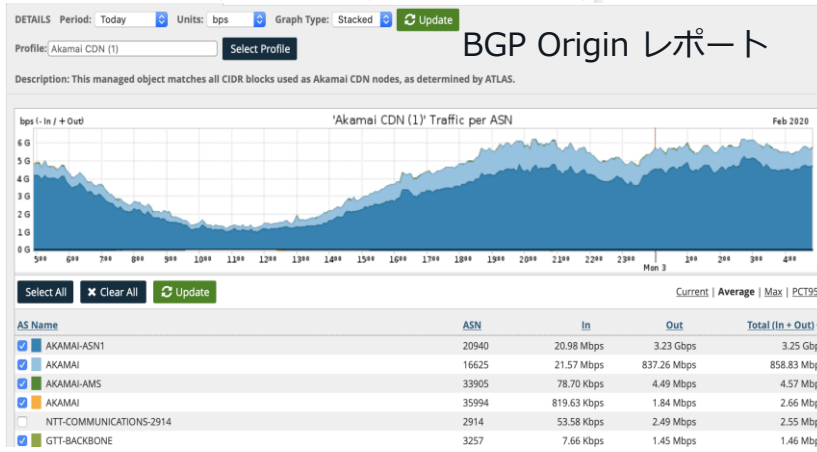
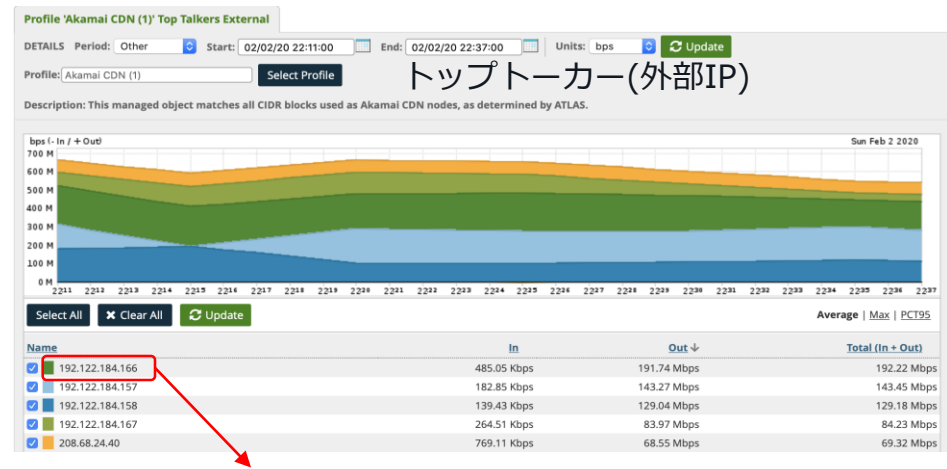
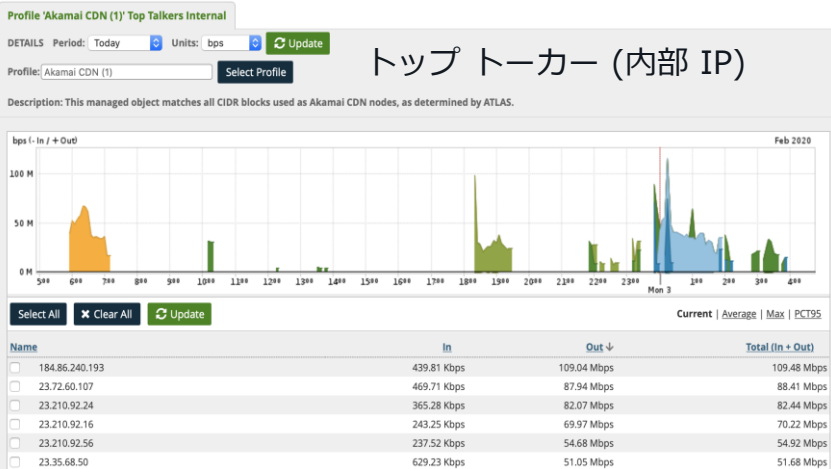
## 各 CDN プロバイダーのトラフィックの内訳



## CDN トラフィックの概要



# サンプル レポート (Sightline) Akamai CDNのトップトーカー&ASN Originレポート

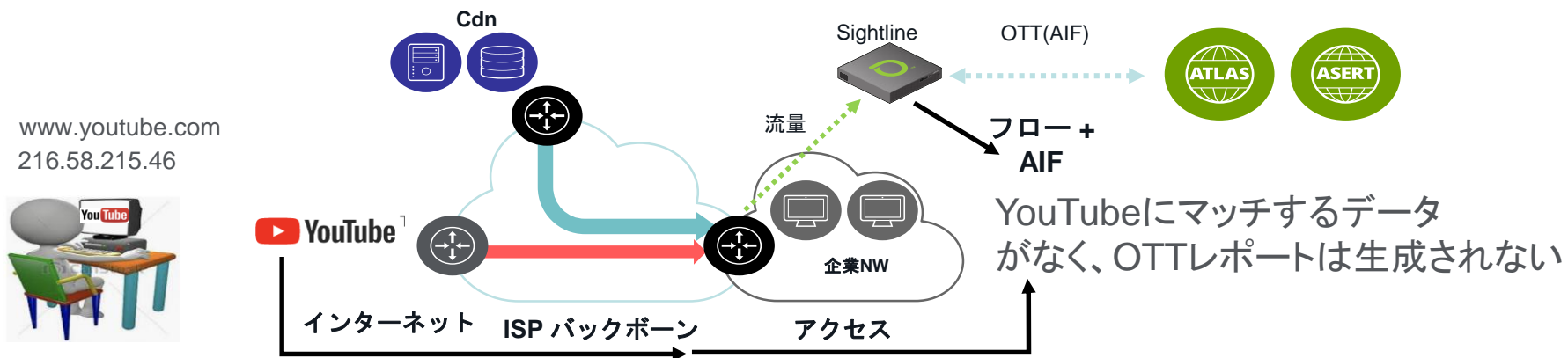


192.122.184.166 がほとんどのトラフィックを提供

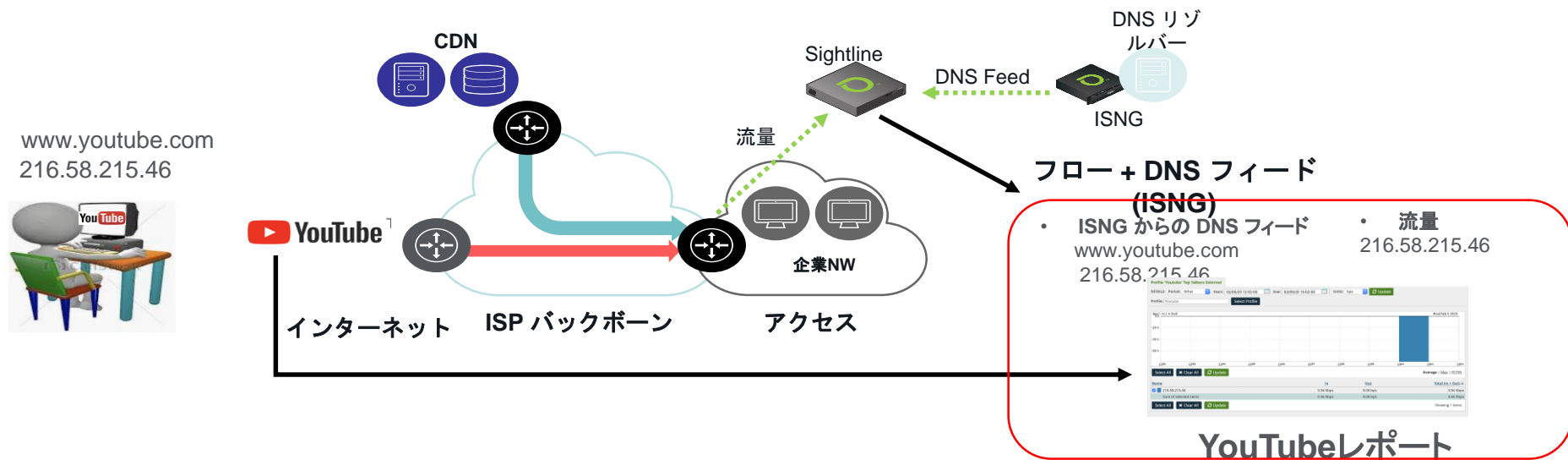
- トラフィックはどこへ送信されたか?
- トラフィックはどのルートでネットワークに入っているか?

# ISNGとAIFの連携 (Sightline Sentinel)

- Youtubeは人気のOTTプロバイダであるがAIF には含まれてない



- ISNGのURL検出機能を用いてAIFに含まれないOTTの可視化を実現



**SCSK**