NETSCOUT

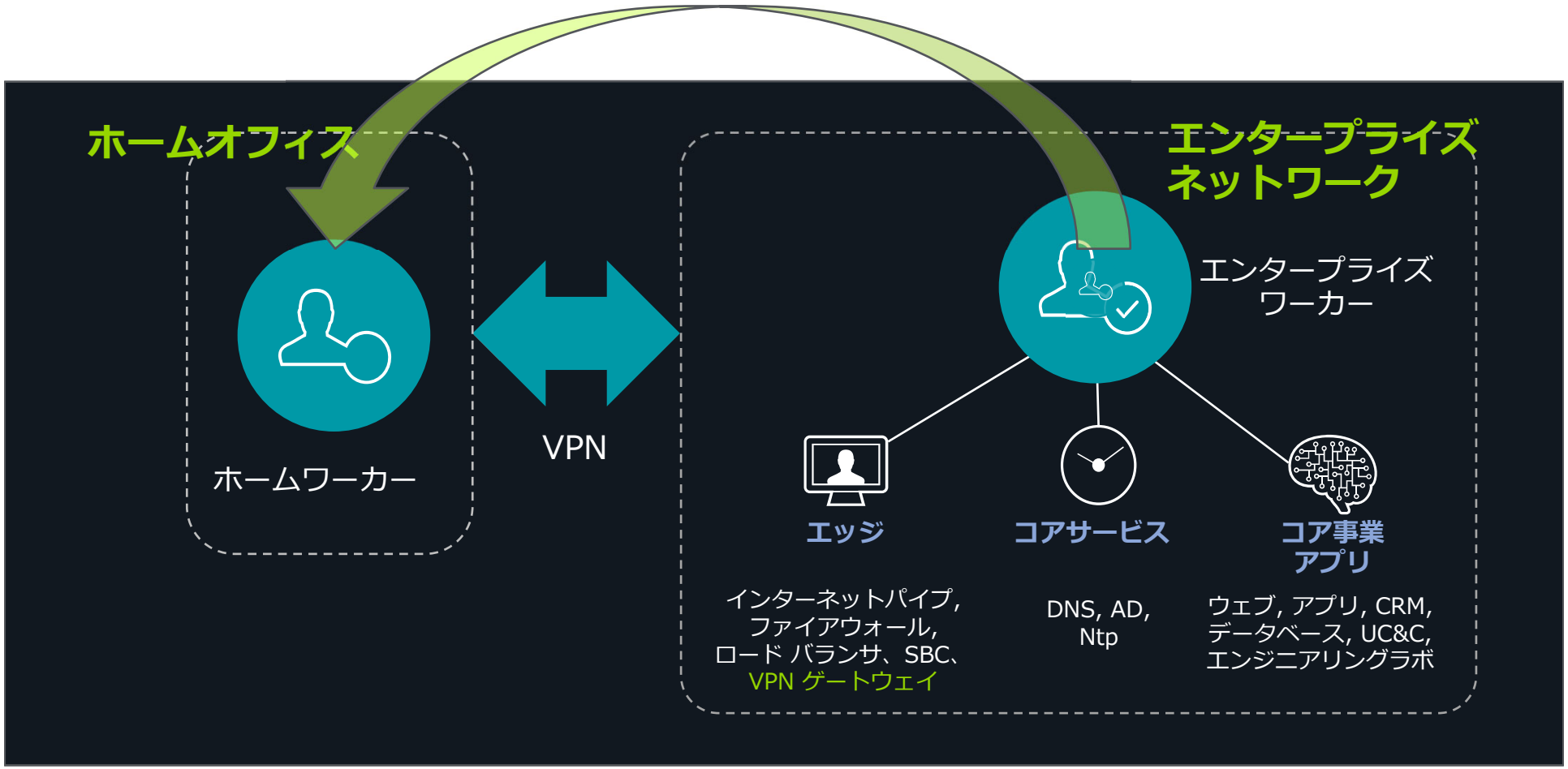
VPN を使用したテレワークへの移行とビジネス継続性確保

ユースケース

2020/07/27

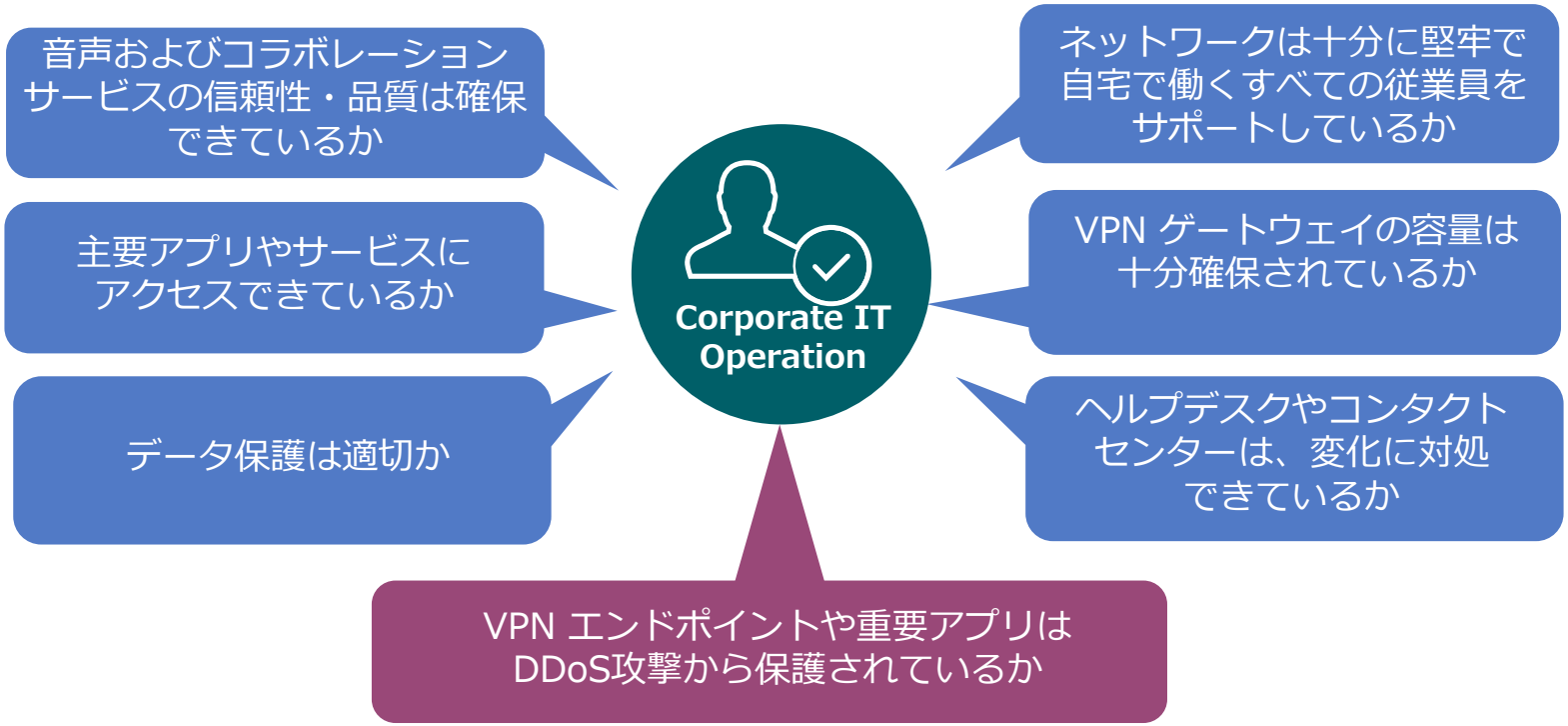
ネットスカウト・システムズ・ジャパン株式会社

企業ネットワークの劇的な変化



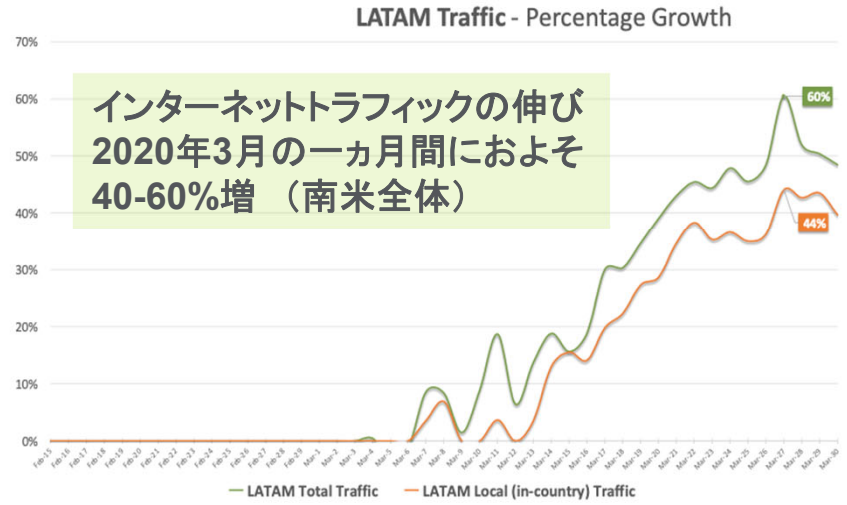
企業ネットワークが直面する新たな課題

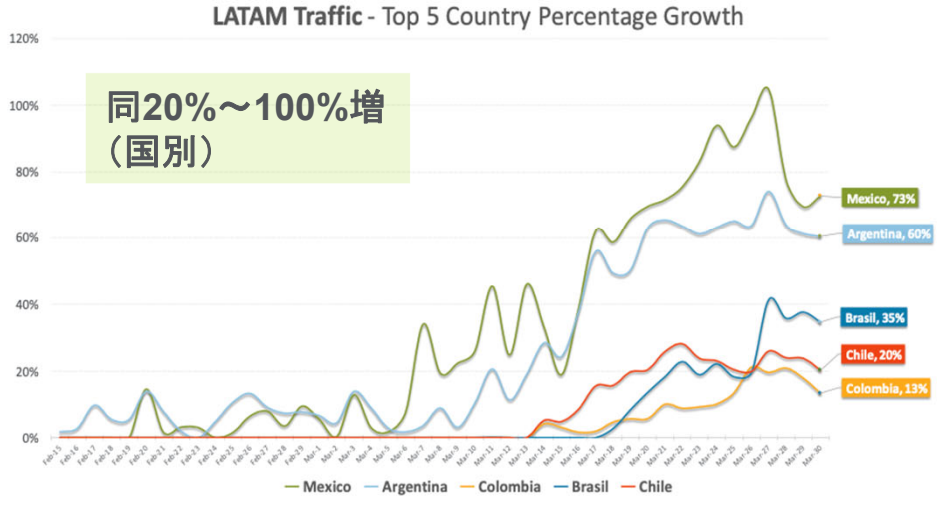
テレワークが企業の生産性を維持していることを確認する必要がある



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)

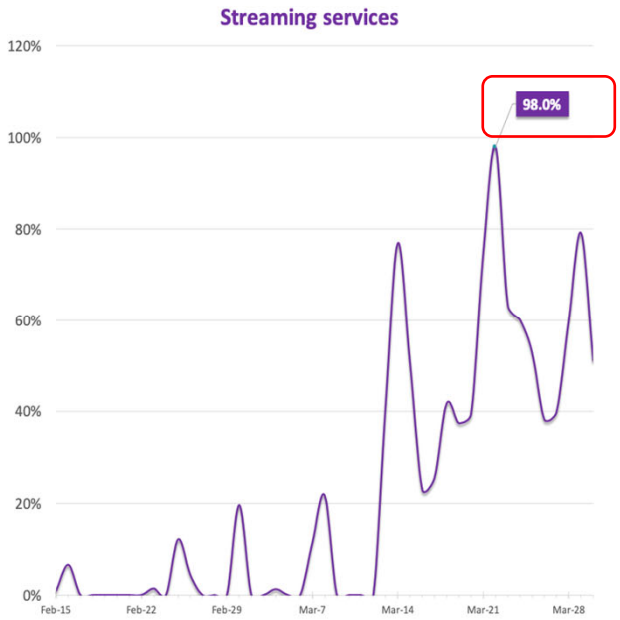
Traffic volume observed in LATAM region before and during COVID-19 contingency.





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サービスの伸び
最大200% (3倍)以上



ストリーミングサービスの伸び
最大100% (2倍)

SNSの伸び
最大90% (1.9倍)

NETSCOUT

ユースケース

- SSLVPN監視
- ビデオ会議システム監視[Webex事例]
- DDoS 攻撃からのテレワークアクセス保護
- OTTトラフィックの可視化

NETSCOUT

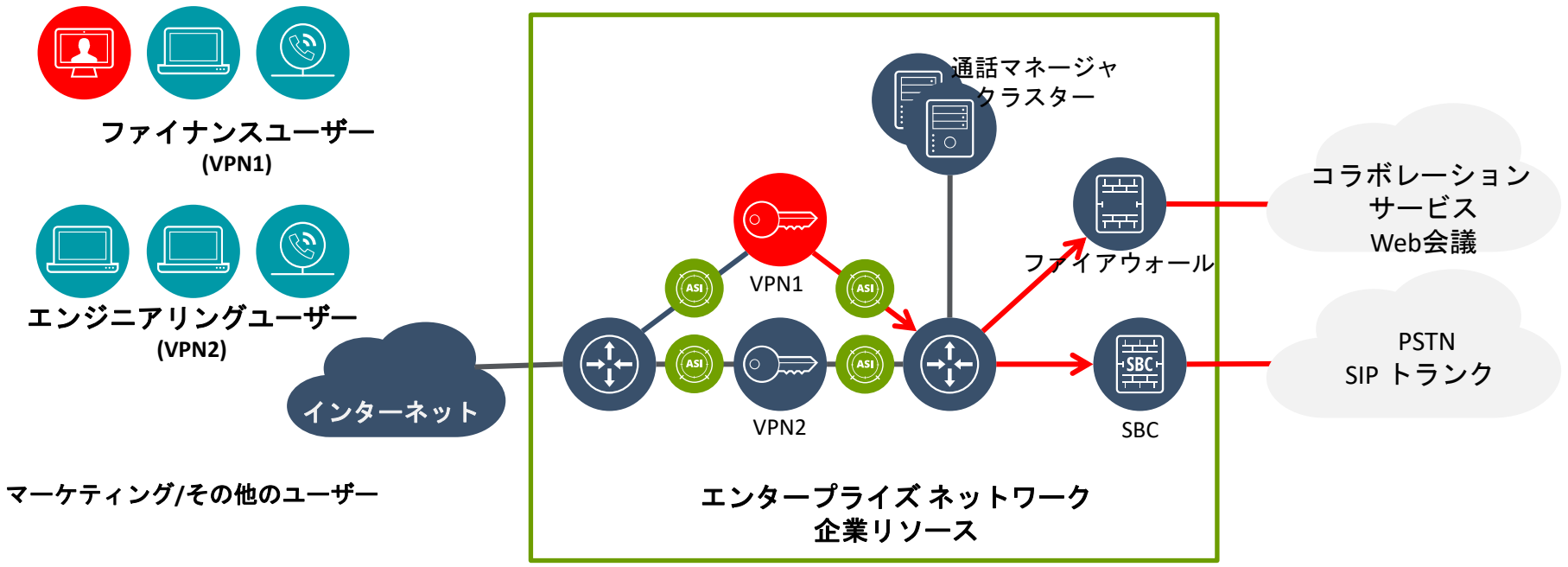
ユースケース 1

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

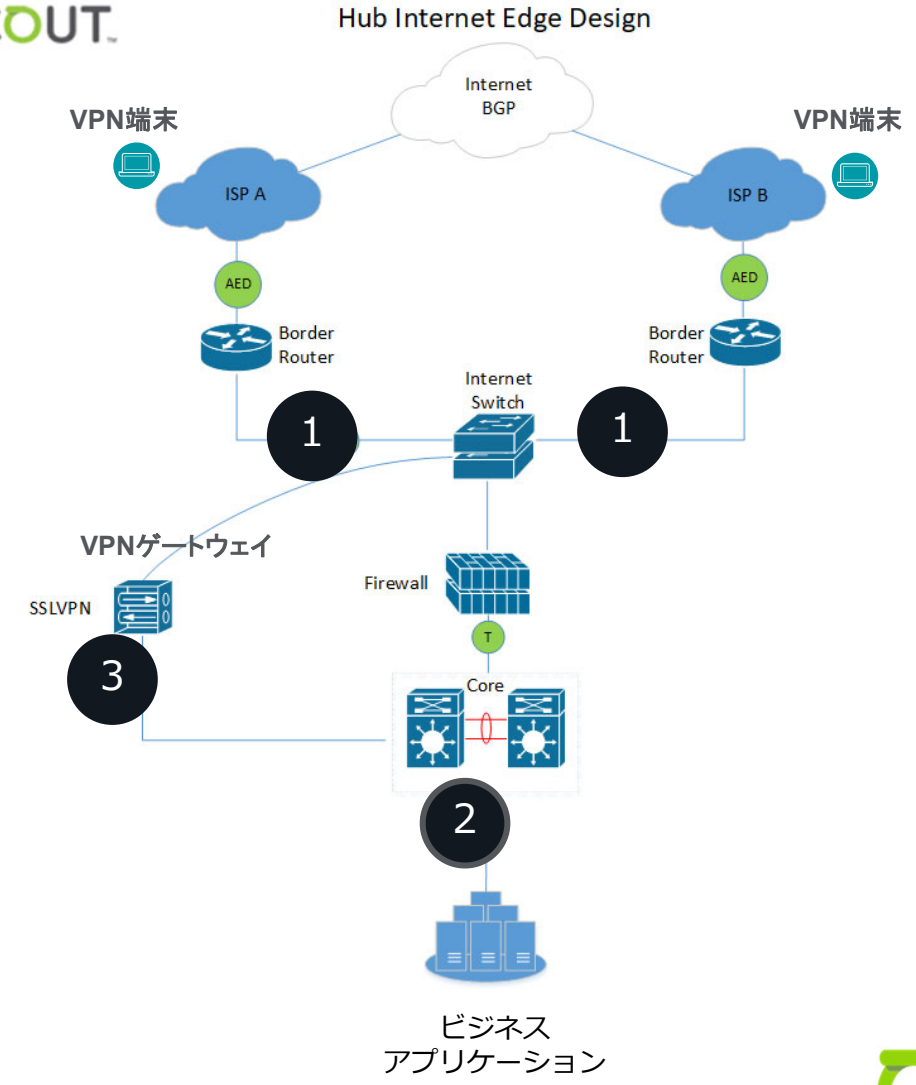
1

3

ビジネスサービス

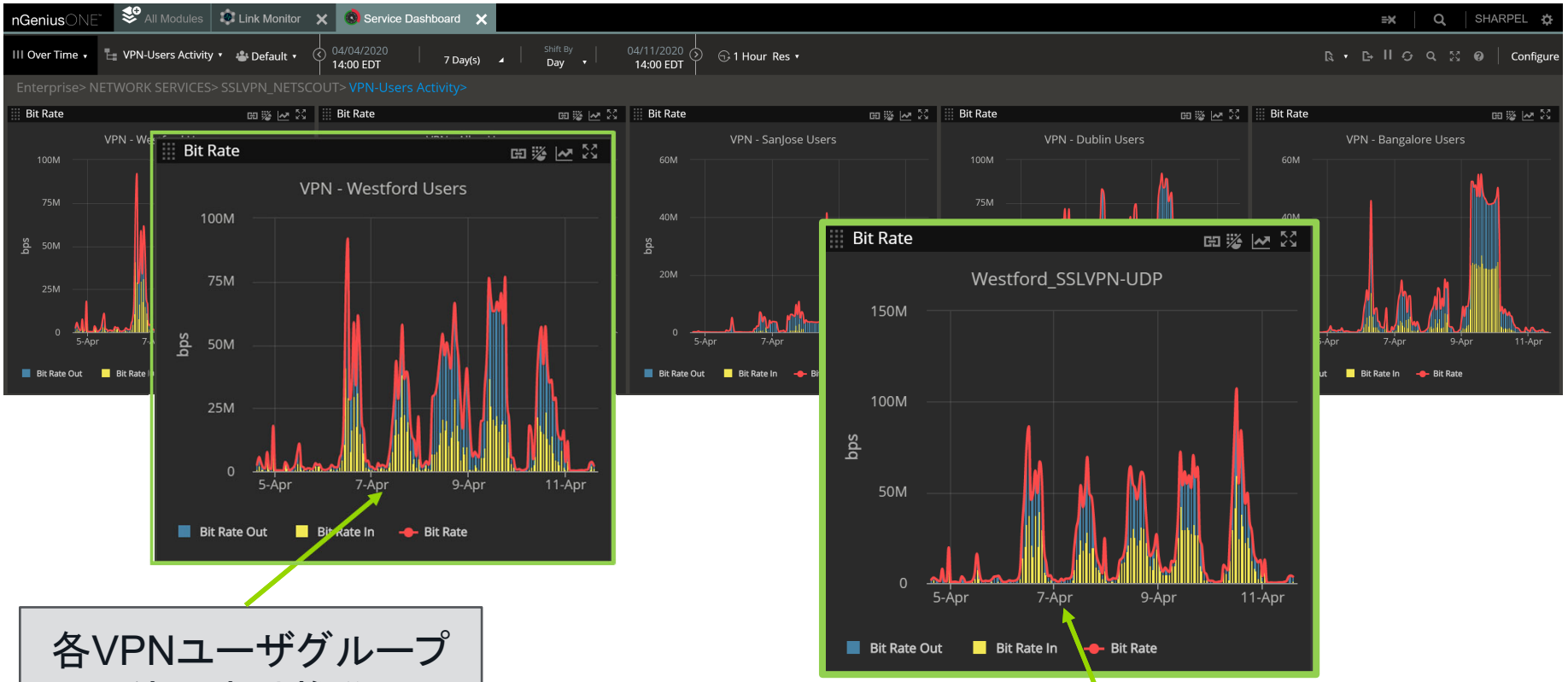
- ビジネス アプリケーションの正常性と使用状況
- VDI サービスの正常性
- 企業に出入りするメディア品質
- リモート ユーザーとのリンクに関する問題を特定する

2



SSLVPN監視例

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

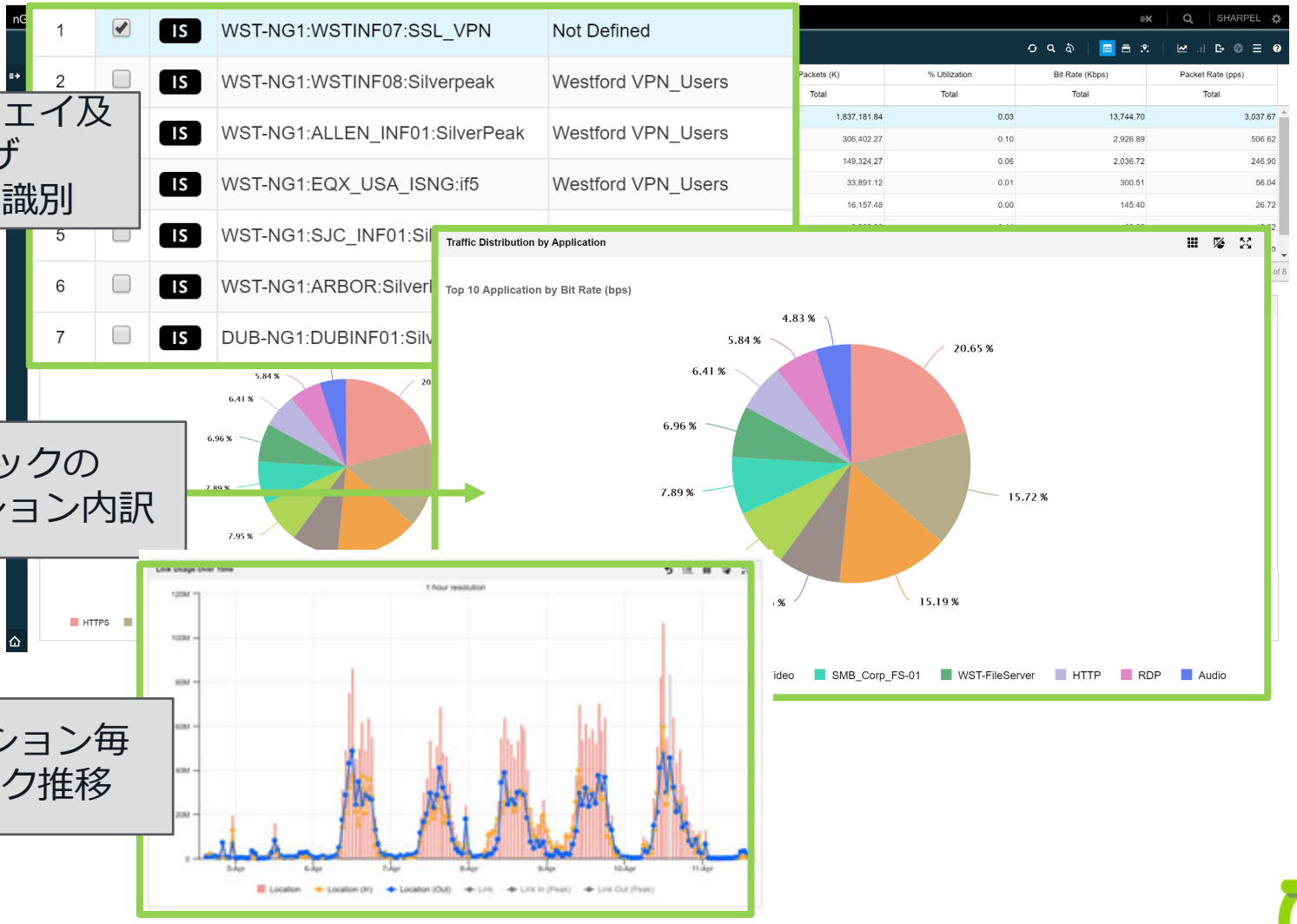
SSLVPN監視例

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

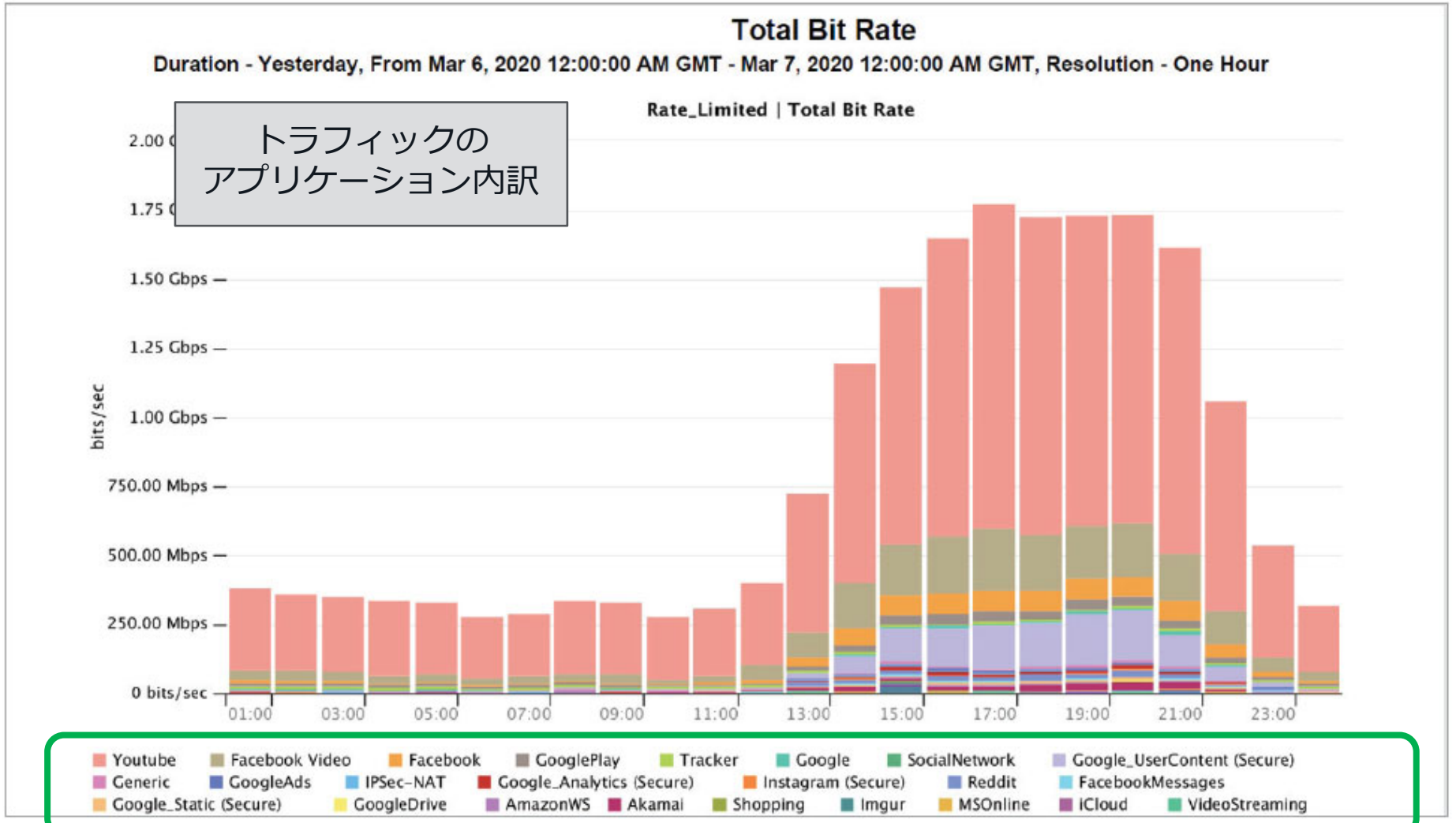
トラフィックのアプリケーション内訳

アプリケーション毎トラフィック推移



SSLVPN監視例

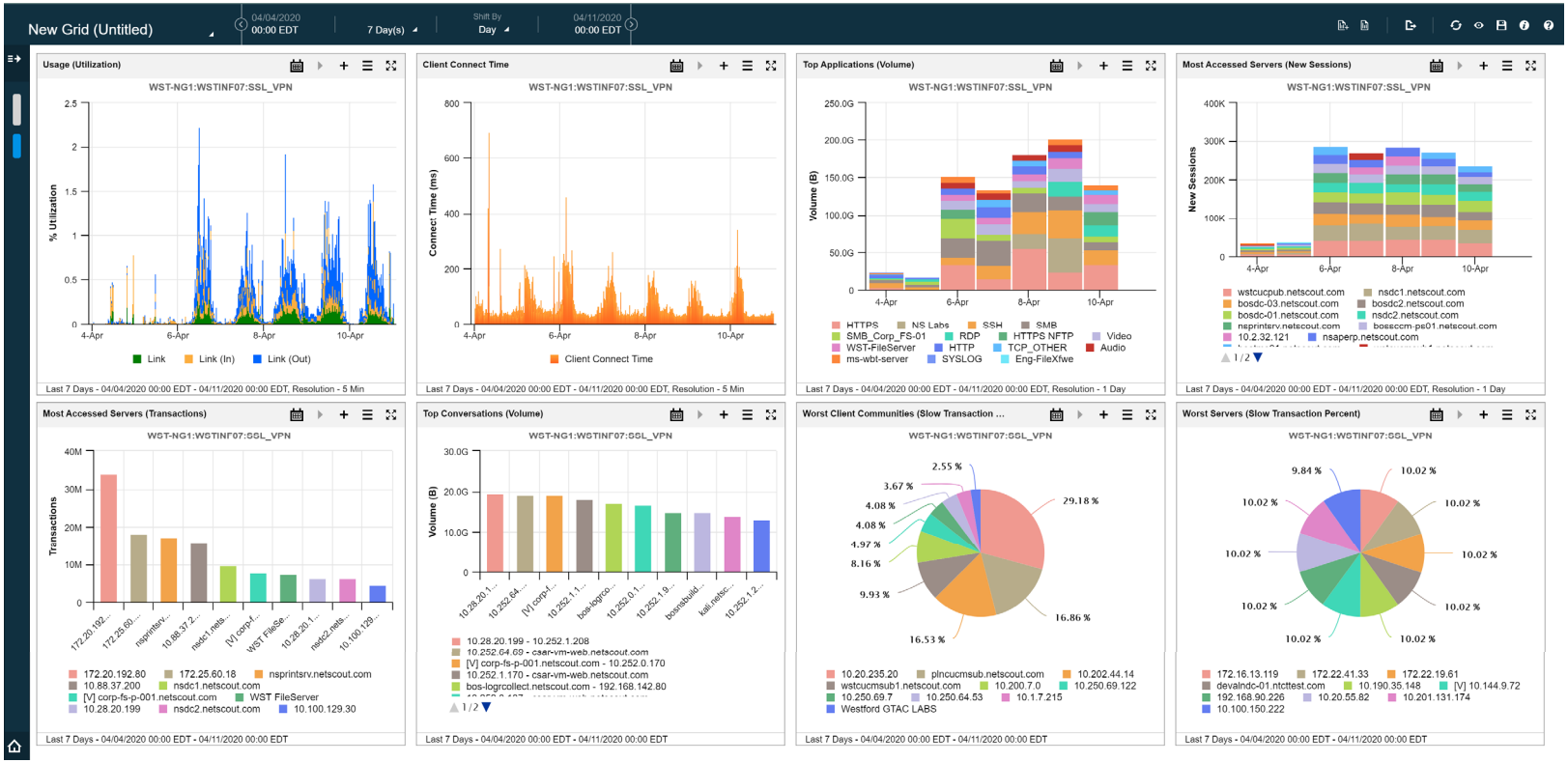
nGeniusONE –VPN上の使用アプリケーション分析



SSLVPN監視例

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.



NETSCOUT

ユースケース 2

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

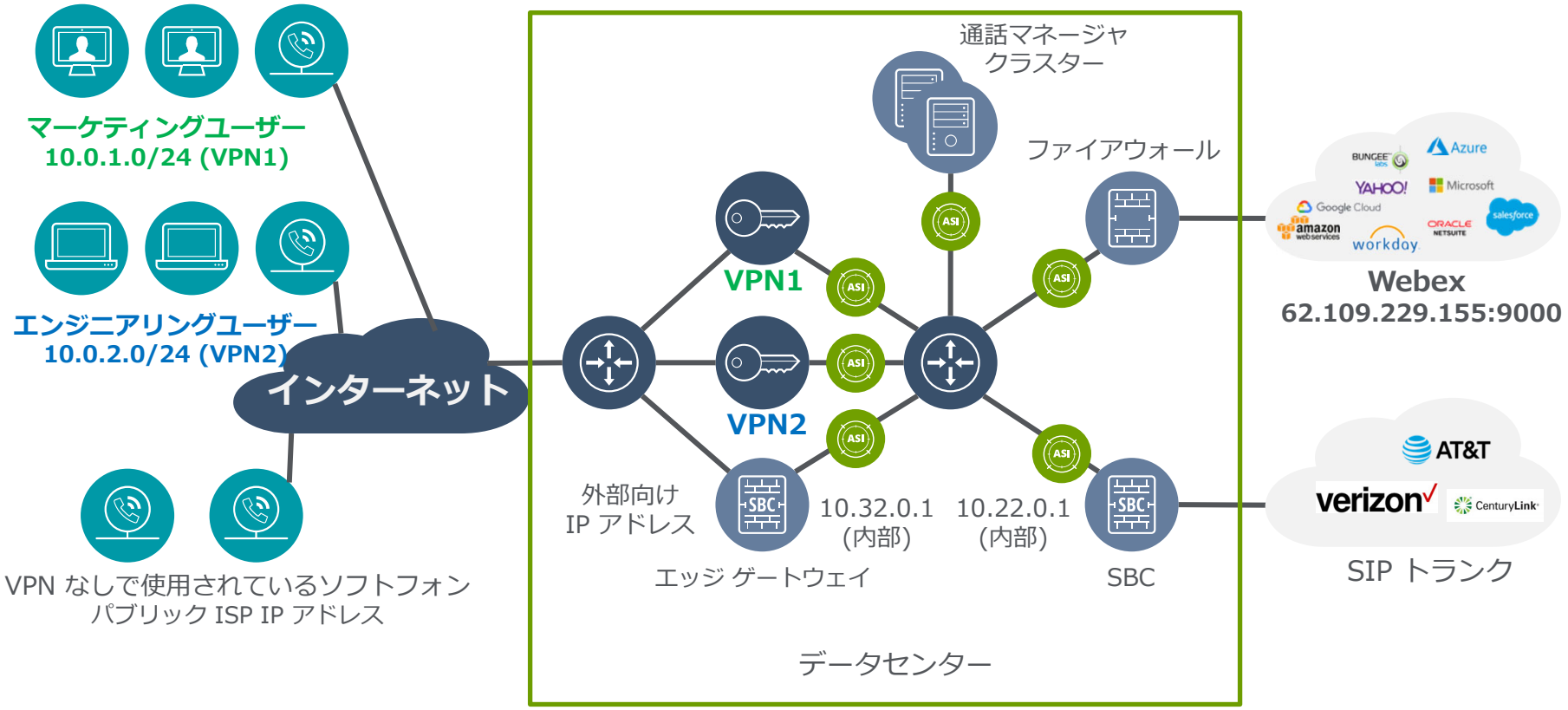
[VPN・WebEX環境]

- 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]

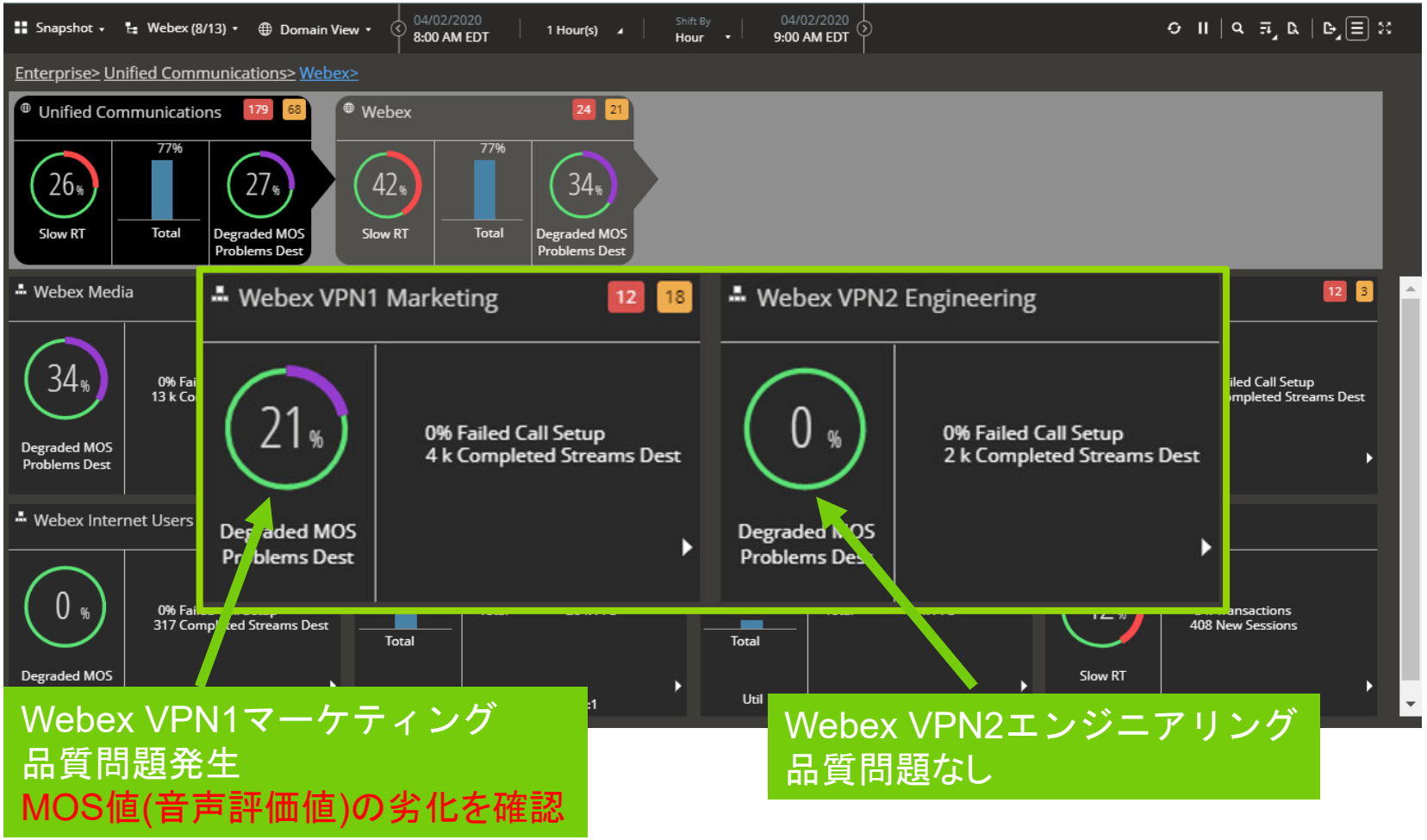
- マーケティングユーザーが使用するVPN1は、営業時間時、特にピーク時(午前9時から午前11時EDT)で飽和状態
- パケットがドロップされ、マーケティングチームのWebEx 会議や音声およびビデオの品質低下を数値で確認
- マーケティングチームのビデオ使用により、一部のVPNゲートウェイが過負荷となっていることを確認

ネットワーク アーキテクチャ



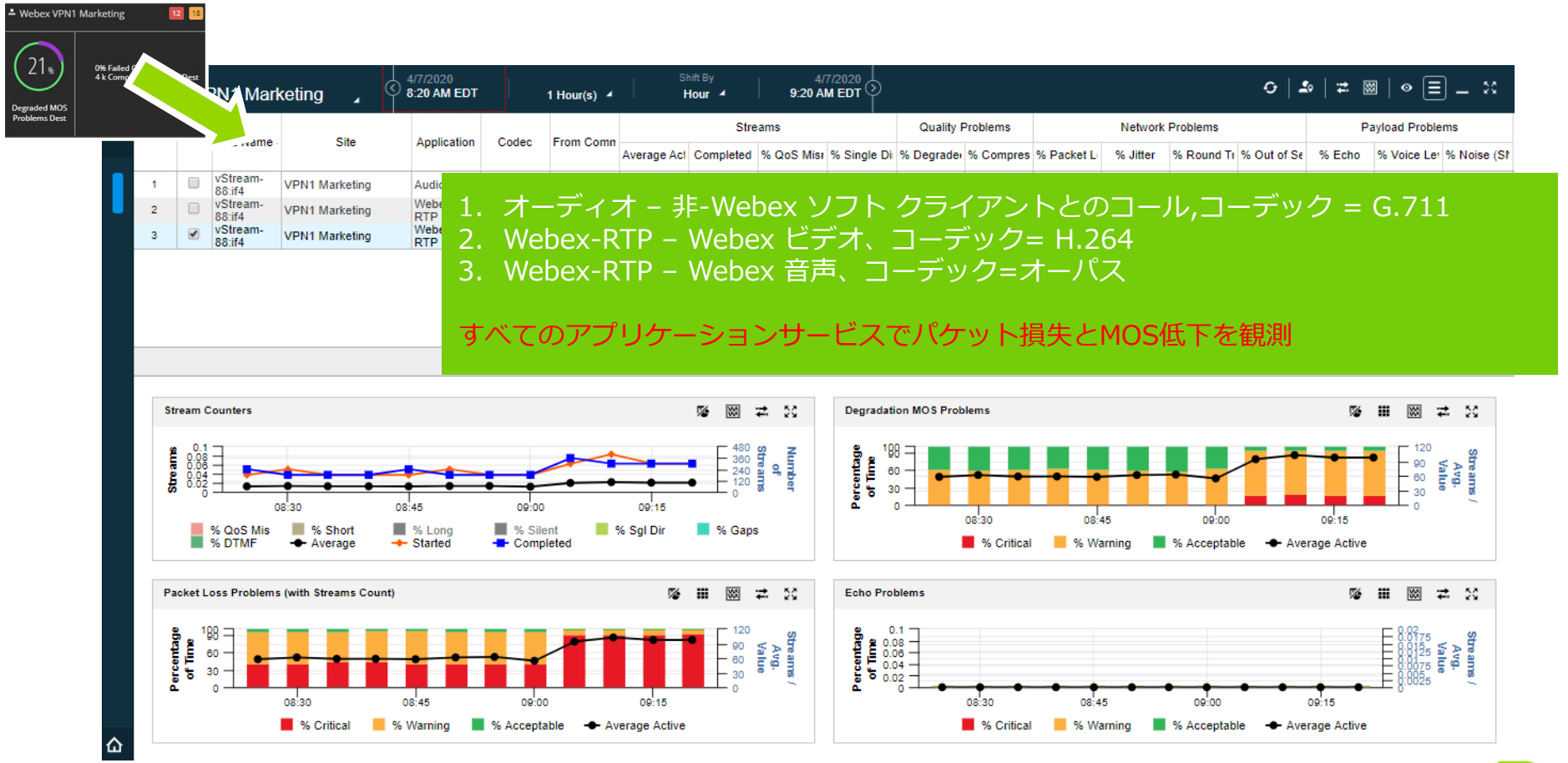
サービス ダッシュボード

- 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



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



VPN1マーケティング - メディアモニター

過去 24 時間

営業時間内のトラフィック量と品質問題を確認

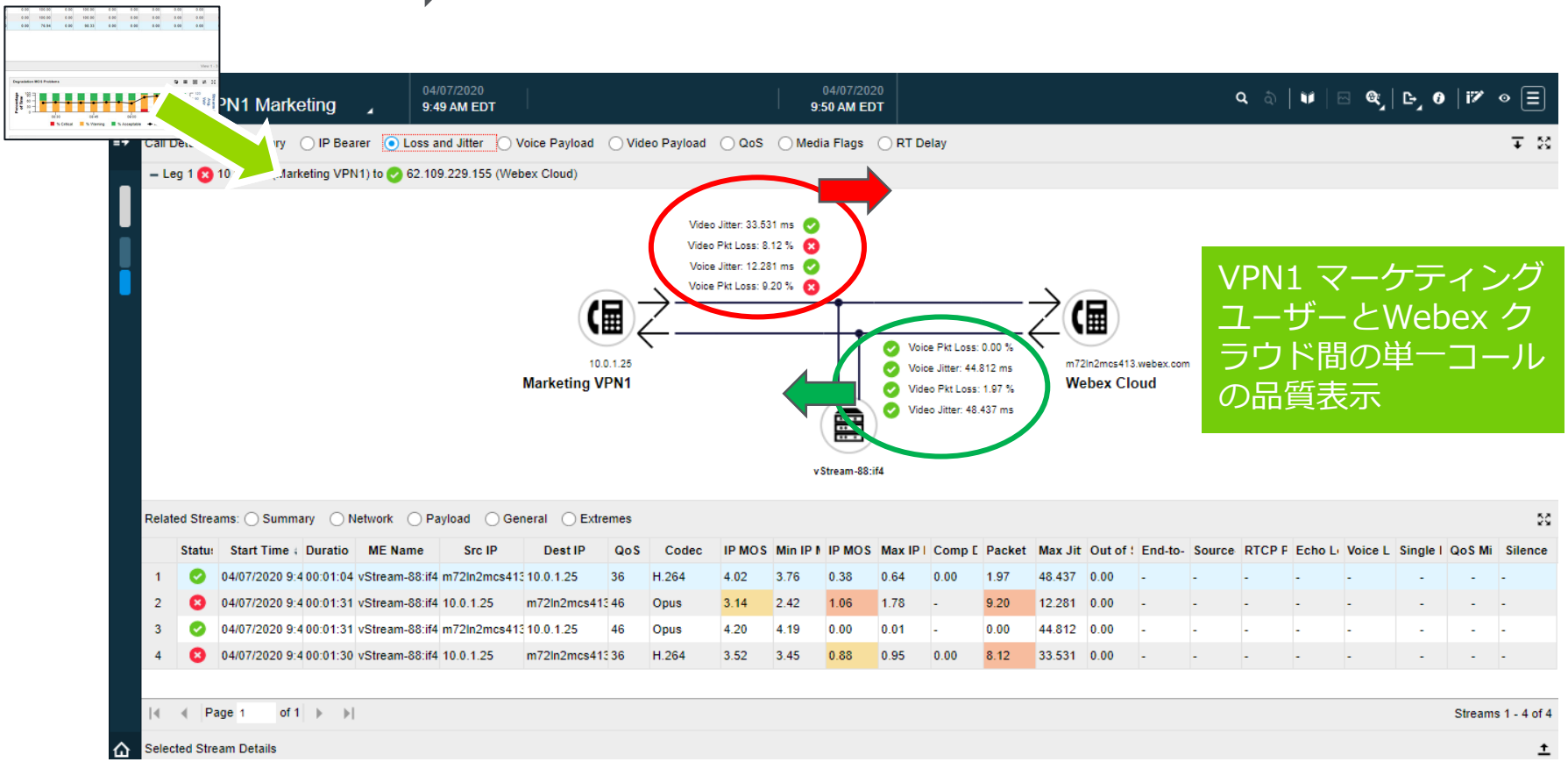
午前 6 時から正午

セッション数と品質劣化の完全な関連を確認

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

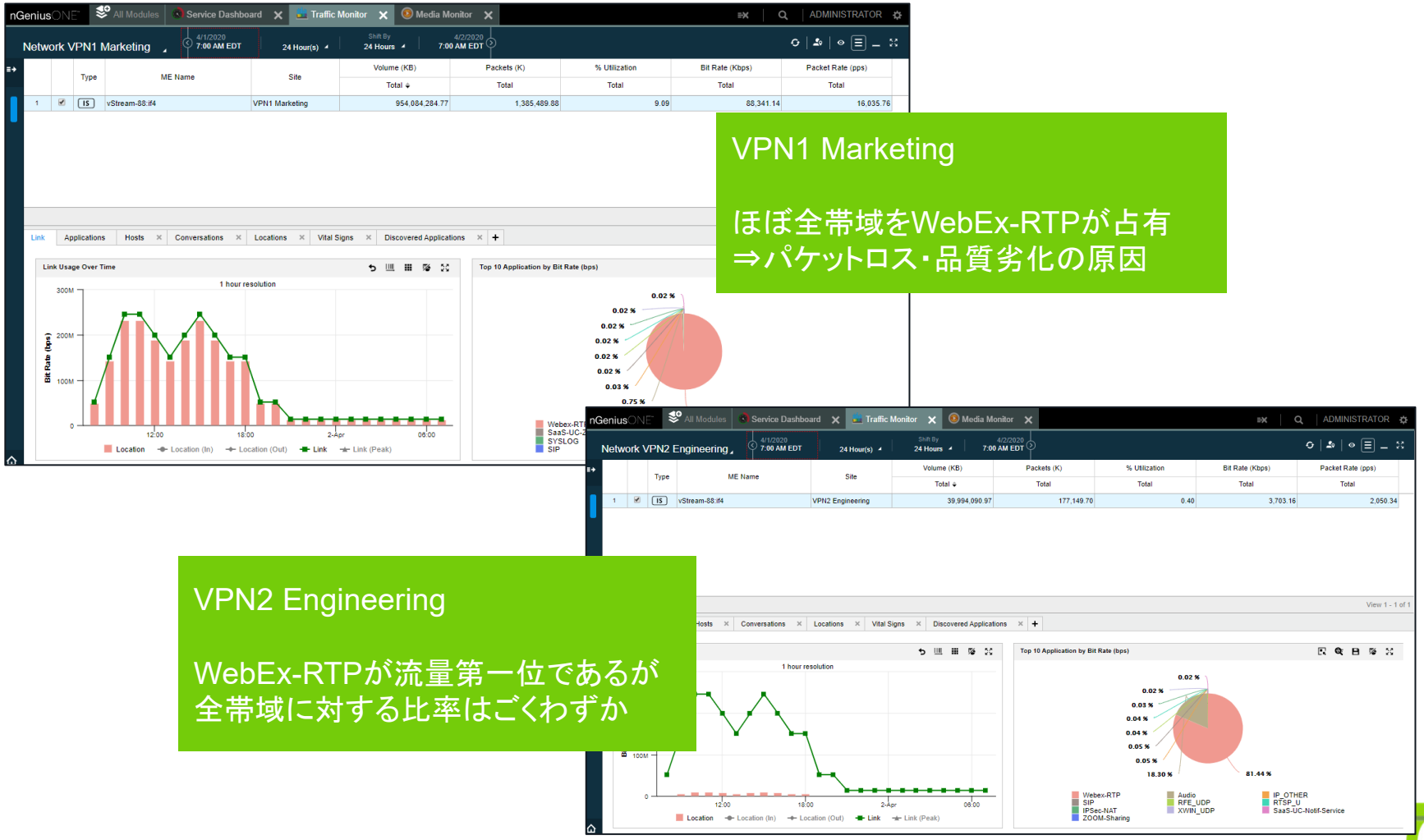
➡ クライアント～VPNゲートウェイ間のネットワークで問題発生



	Statu	Start Time	Duratio	ME Name	Src IP	Dest IP	QoS	Codec	IP MOS	Min IP M	IP MOS	Max IP I	Comp D	Packet	Max Jit	Out of S	End-to-	Source	RTCP F	Echo L	Voice L	Single I	QoS Mi	Silence
1	✓	04/07/2020 9:4	00:01:04	vStream-88:if4	m72ln2mcs413	10.0.1.25	36	H.264	4.02	3.76	0.38	0.64	0.00	1.97	48.437	0.00	-	-	-	-	-	-	-	-
2	✗	04/07/2020 9:4	00:01:31	vStream-88:if4	10.0.1.25	m72ln2mcs413	46	Opus	3.14	2.42	1.06	1.78	-	9.20	12.281	0.00	-	-	-	-	-	-	-	-
3	✓	04/07/2020 9:4	00:01:31	vStream-88:if4	m72ln2mcs413	10.0.1.25	46	Opus	4.20	4.19	0.00	0.01	-	0.00	44.812	0.00	-	-	-	-	-	-	-	-
4	✗	04/07/2020 9:4	00:01:30	vStream-88:if4	10.0.1.25	m72ln2mcs413	36	H.264	3.52	3.45	0.88	0.95	0.00	8.12	33.531	0.00	-	-	-	-	-	-	-	-

VPN1 マーケティングユーザーとWebex クラウド間の単一コールの品質表示

トラフィックモニター



VPN1 Marketing

ほぼ全帯域をWebEx-RTPが占有
⇒パケットロス・品質劣化の原因

VPN2 Engineering

WebEx-RTPが流量第一位であるが
全帯域に対する比率はごくわずか

NETSCOUT

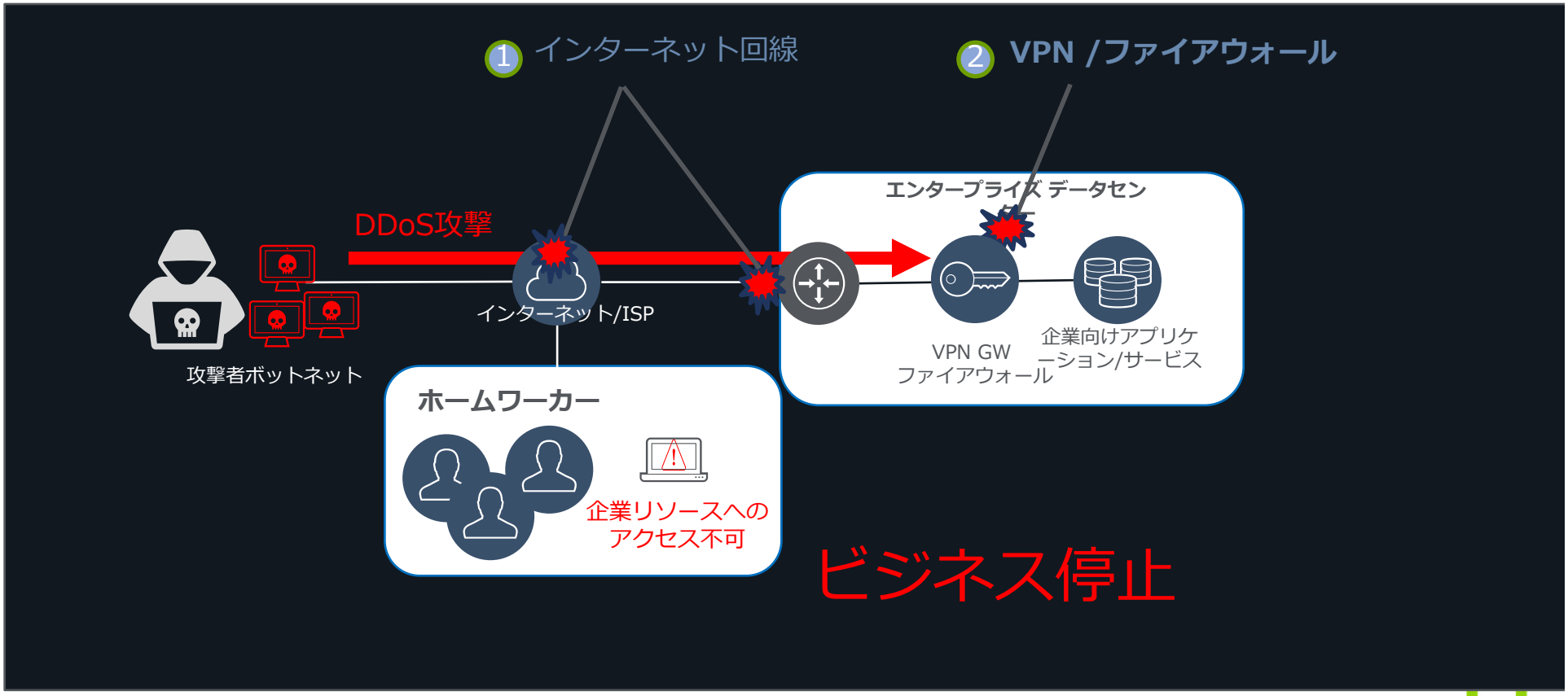
ユースケース3

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

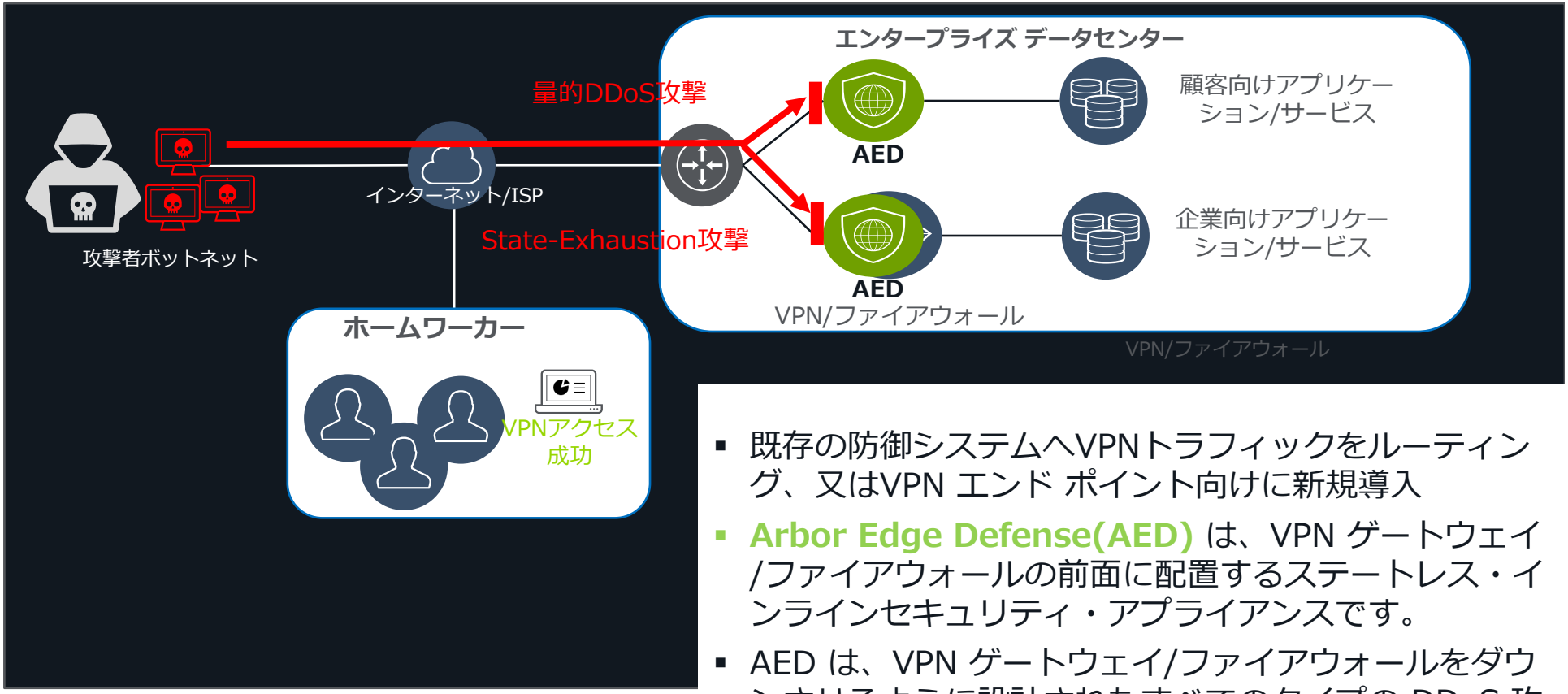
従来の主な攻撃対象は、顧客向けアプリケーションサービス

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)

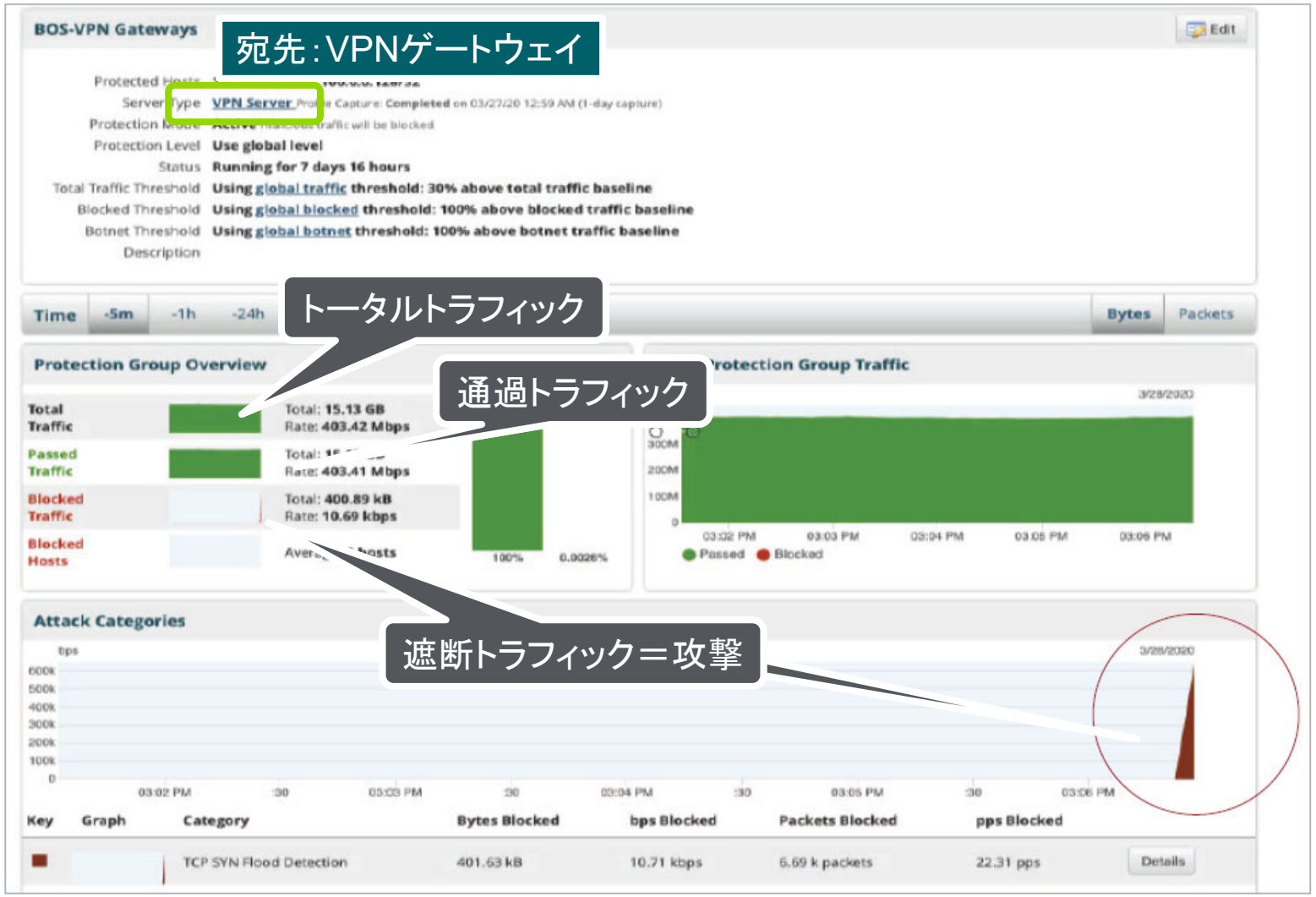
企業リソースへのホームワーカーアクセスの可用性を確保



- 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。

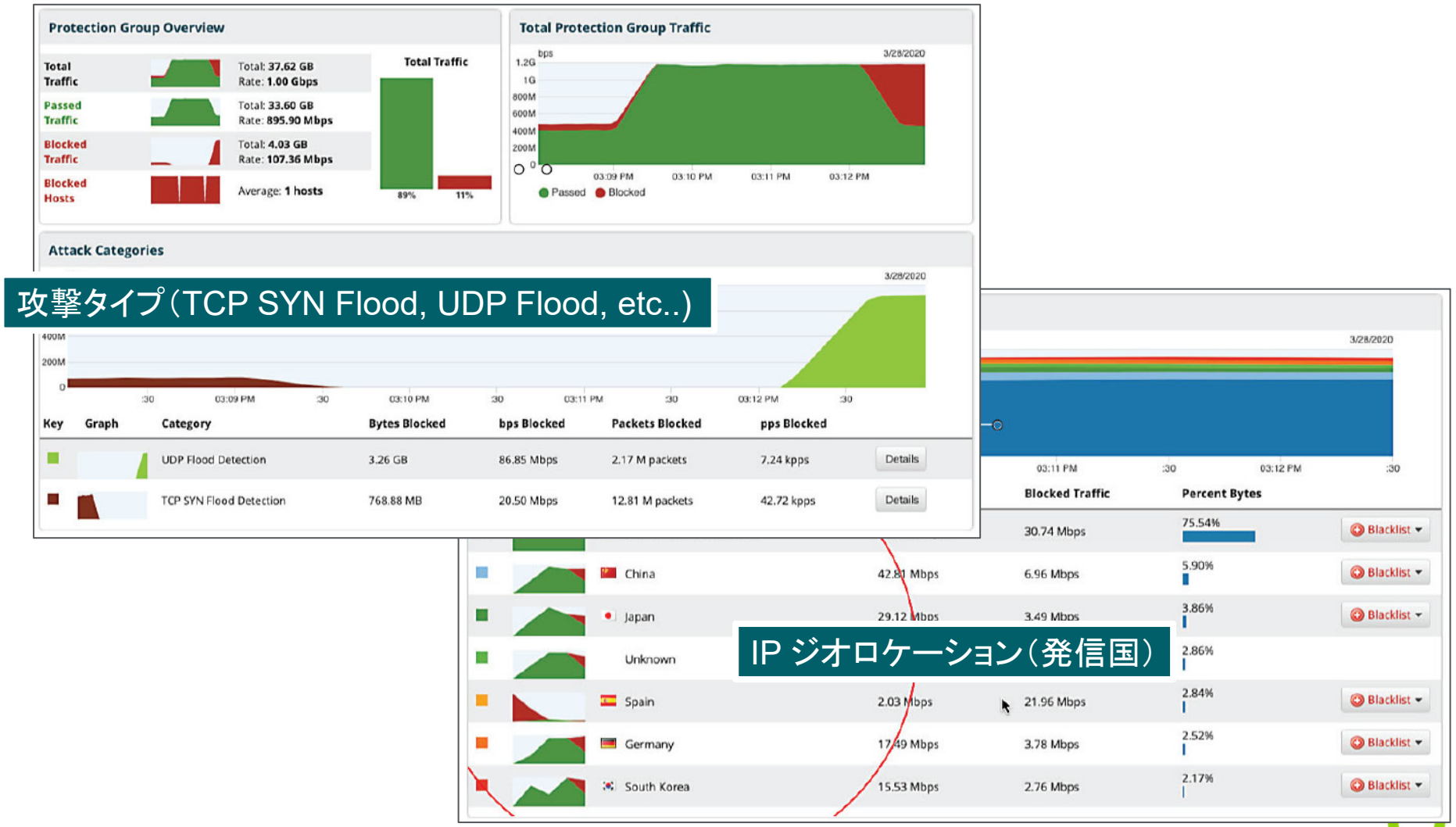
企業のためのスマートDDoS保護
Arbor Edge Defense(AED)

VPNゲートウェイへの攻撃検知、攻撃トラフィックと正規トラフィックの可視化



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

VPNゲートウェイへの攻撃の可視化と高度な分析



AED – VPN エンドポイントのスマート DDOS 保護

- 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、COTS、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（通常の量や変動）を知らない
    - オーバーブロッキ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

NETSCOUT

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

OTT トラフィックが増加し高帯域幅を使用

会議 (Webex、Zoom, etc)品質が不安定

ユーザー エクスペリエンスが劣化

OTT プロバイダが原因で問題発生

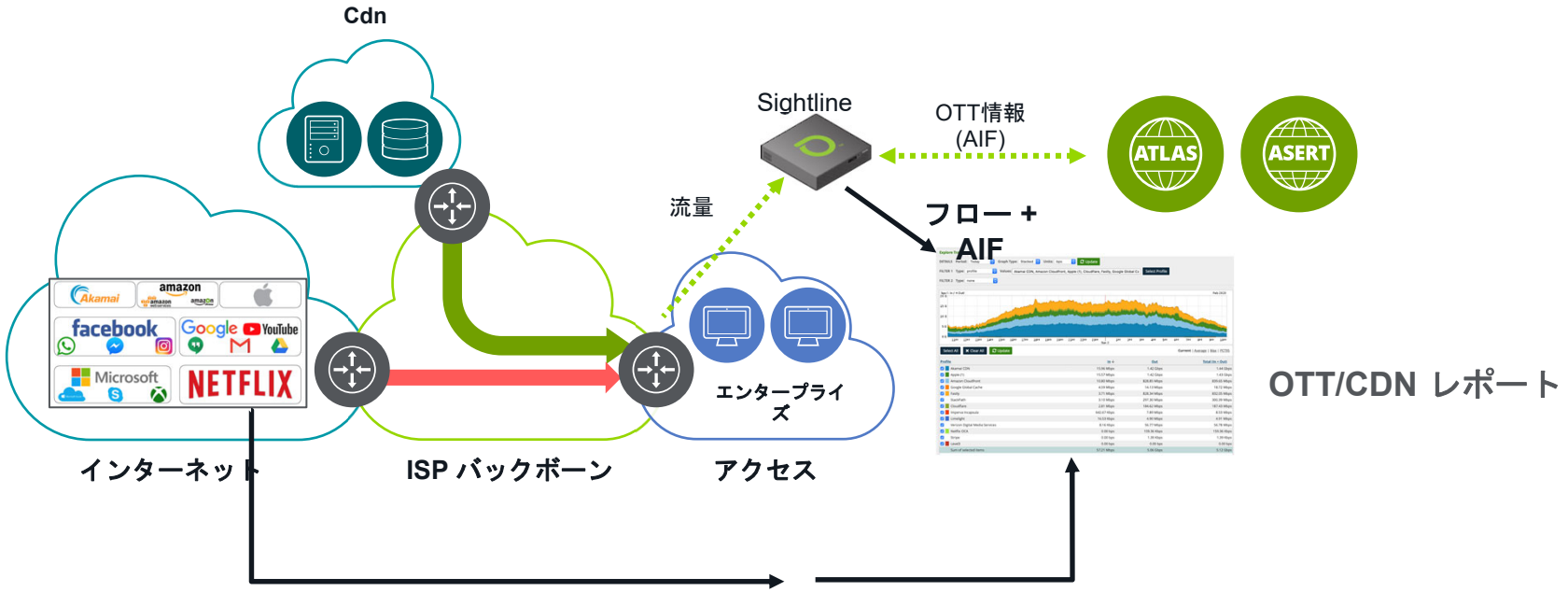
OTTがVPN経由でどのように使用されているか

OTTと社内アプリケーションの利用量比率はどのようになっているか

AIFシグネチャを使用したOTT/CDNレポート

OTT可視化

- 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(ATLAS Intelligent Feed)-OTTの可視化

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

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 platfrom	
HBO	Webex	Fastly	Google Global Cache	
Hulu	Zoom	StackPath	IBM Cloud	
iQIYI		Stripe	Imperva	
myCANAL			LimeLight	
NBA			MS Azure virtual machines	
Netlfix			Oracle	
			Rackspace	
			Verizon Ditigal Media Services	

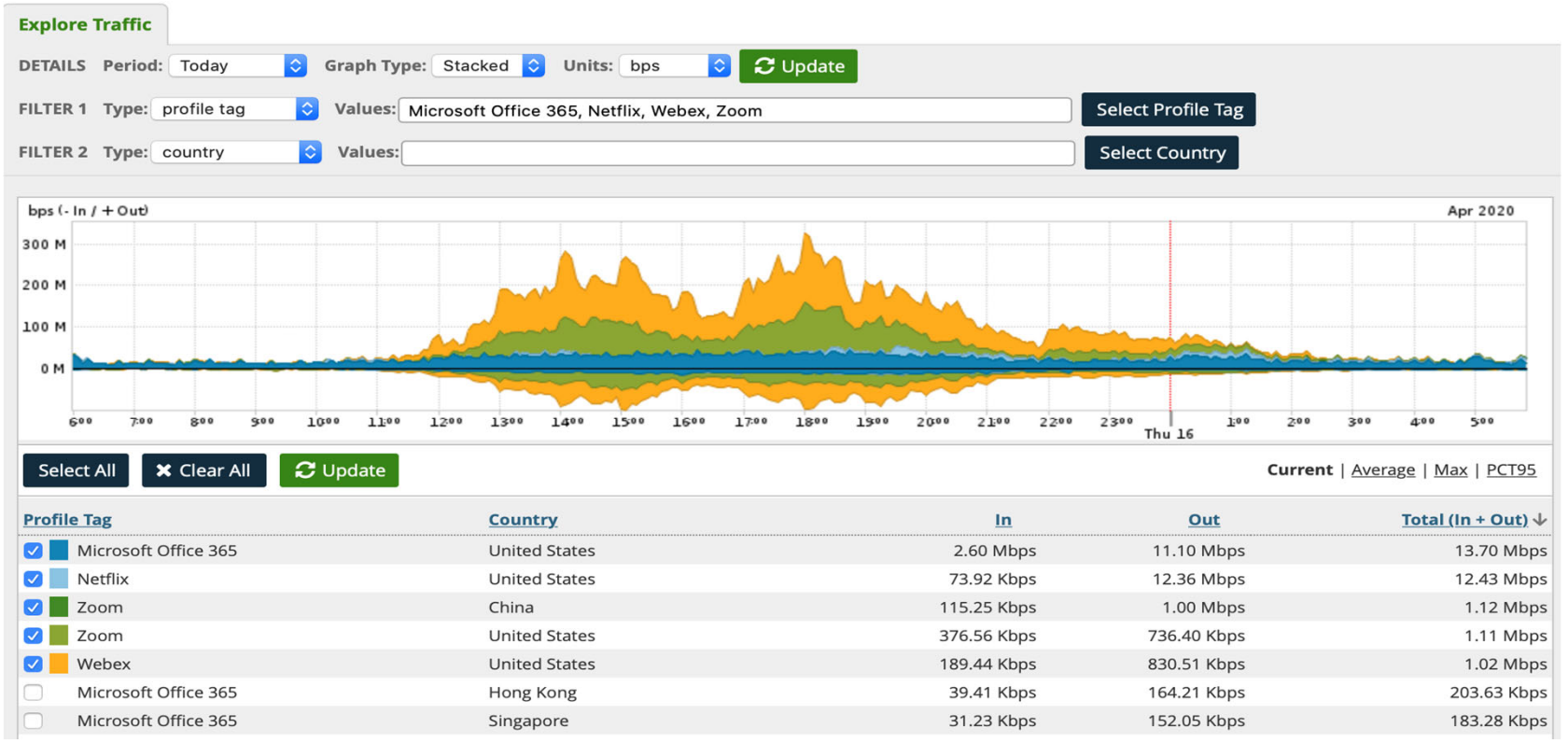
Social	SaaS	SD-WAN
Baidu	BOX	Aryaka
Facebook	DropBox	Meraki
Odnoklassniki	MS 365 Common and Office Online	VeloCloud
Twitter	MS Exchange oNLINE	
Vkontakte	MS Sharepoint Online and One Drive	
WhatAPP	Salesforce	

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・・・）

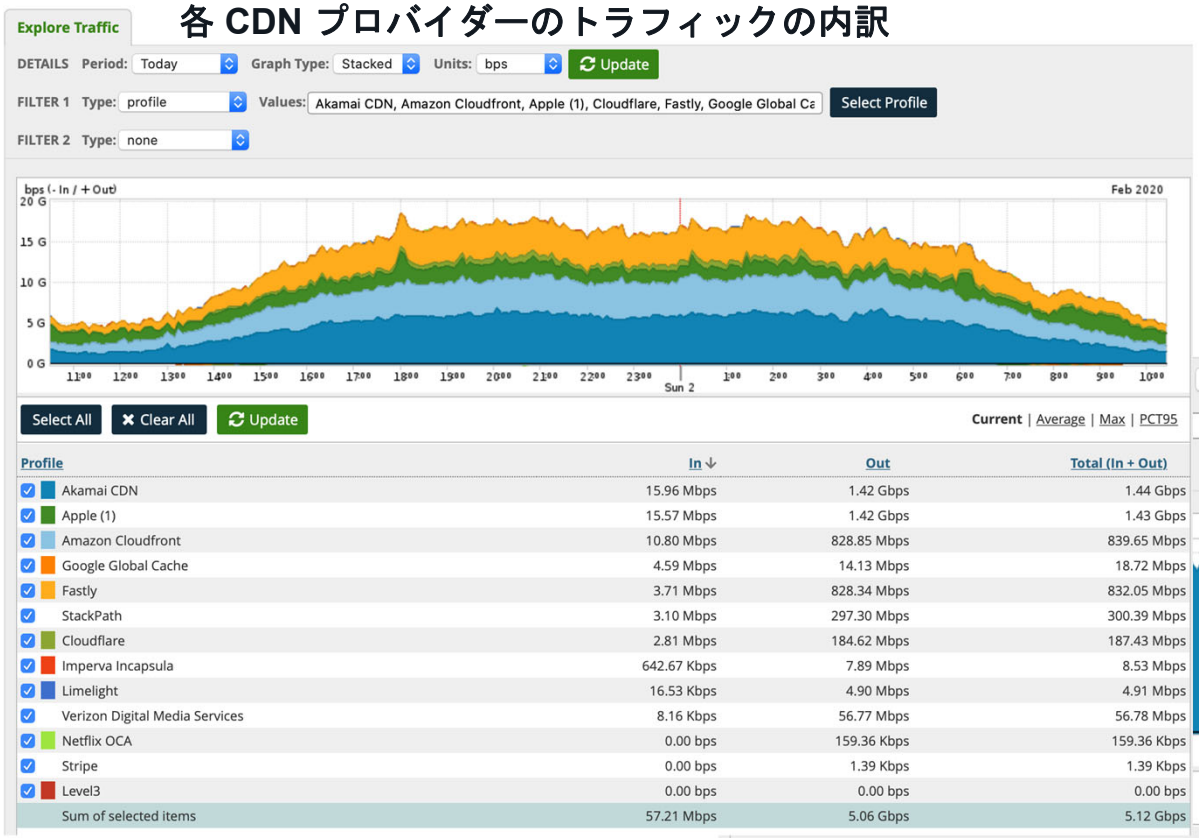
Office365, WebEx, Zoomの可視化事例



Profile Tag	Country	In	Out	Total (In + Out)
Microsoft Office 365	United States	2.60 Mbps	11.10 Mbps	13.70 Mbps
Netflix	United States	73.92 Kbps	12.36 Mbps	12.43 Mbps
Zoom	China	115.25 Kbps	1.00 Mbps	1.12 Mbps
Zoom	United States	376.56 Kbps	736.40 Kbps	1.11 Mbps
Webex	United States	189.44 Kbps	830.51 Kbps	1.02 Mbps
Microsoft Office 365	Hong Kong	39.41 Kbps	164.21 Kbps	203.63 Kbps
Microsoft Office 365	Singapore	31.23 Kbps	152.05 Kbps	183.28 Kbps

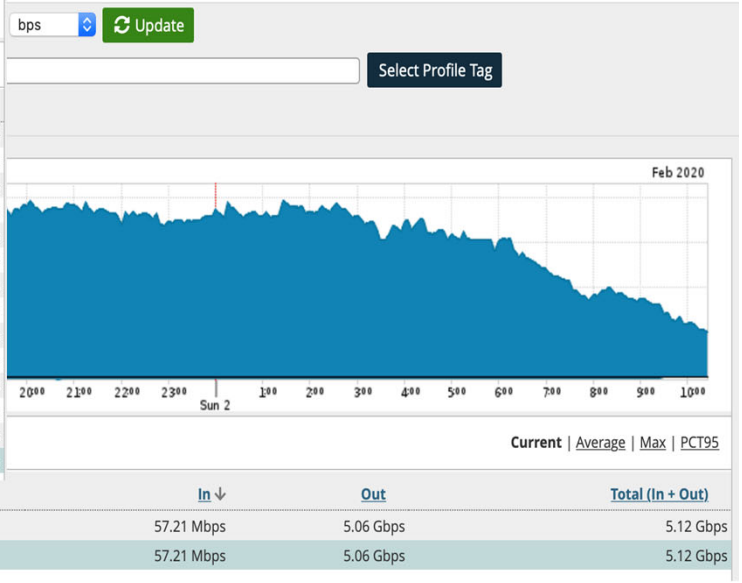
サンプルレポート (Sightline) – CDN プロバイダー

各 CDN プロバイダーのトラフィックの内訳



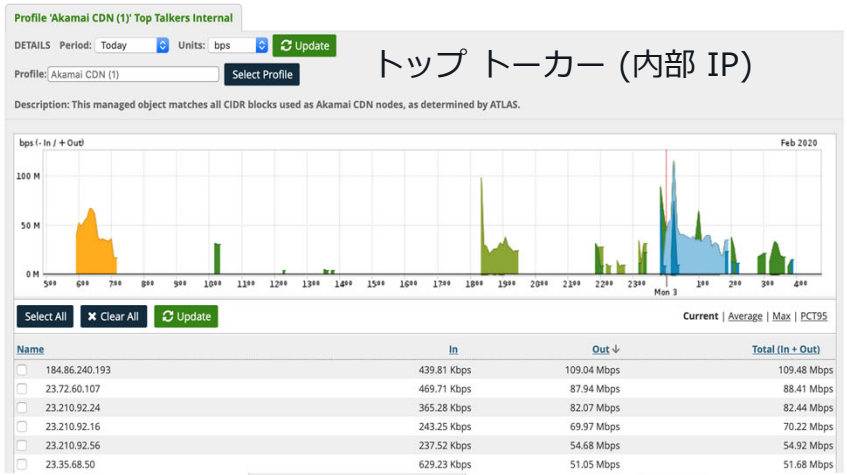
Profile	In	Out	Total (In + Out)
Akamai CDN	15.96 Mbps	1.42 Gbps	1.44 Gbps
Apple (1)	15.57 Mbps	1.42 Gbps	1.43 Gbps
Amazon Cloudfront	10.80 Mbps	828.85 Mbps	839.65 Mbps
Google Global Cache	4.59 Mbps	14.13 Mbps	18.72 Mbps
Fastly	3.71 Mbps	828.34 Mbps	832.05 Mbps
StackPath	3.10 Mbps	297.30 Mbps	300.39 Mbps
Cloudflare	2.81 Mbps	184.62 Mbps	187.43 Mbps
Imperva Incapsula	642.67 Kbps	7.89 Mbps	8.53 Mbps
Limelight	16.53 Kbps	4.90 Mbps	4.91 Mbps
Verizon Digital Media Services	8.16 Kbps	56.77 Mbps	56.78 Mbps
Netflix OCA	0.00 bps	159.36 Kbps	159.36 Kbps
Stripe	0.00 bps	1.39 Kbps	1.39 Kbps
Level3	0.00 bps	0.00 bps	0.00 bps
Sum of selected items	57.21 Mbps	5.06 Gbps	5.12 Gbps

CDN トラフィックの概要

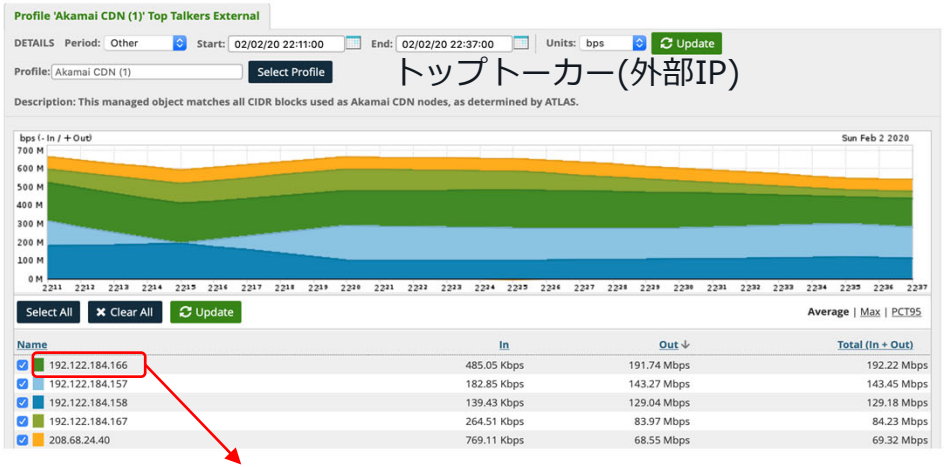


Profile Tag	In	Out	Total (In + Out)
CDN	57.21 Mbps	5.06 Gbps	5.12 Gbps
Sum of selected items	57.21 Mbps	5.06 Gbps	5.12 Gbps

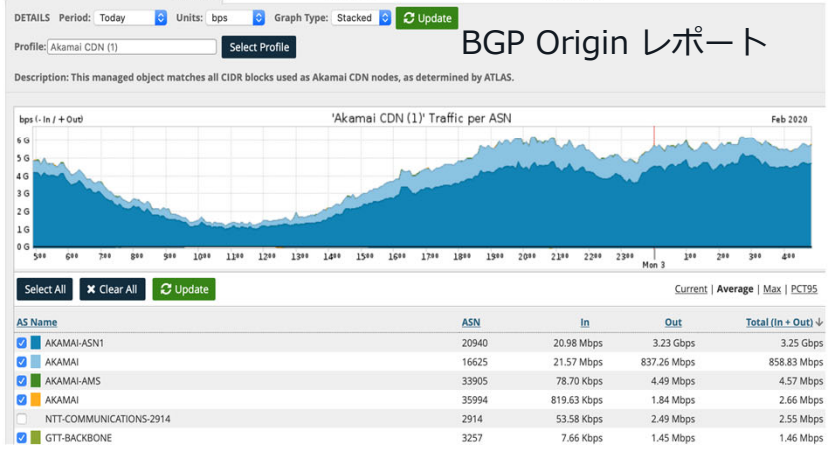
サンプル レポート (Sightline)
Akamai CDNのトップトーカー&ASN Originレポート



トップ トーカー (内部 IP)



トップトーカー(外部IP)



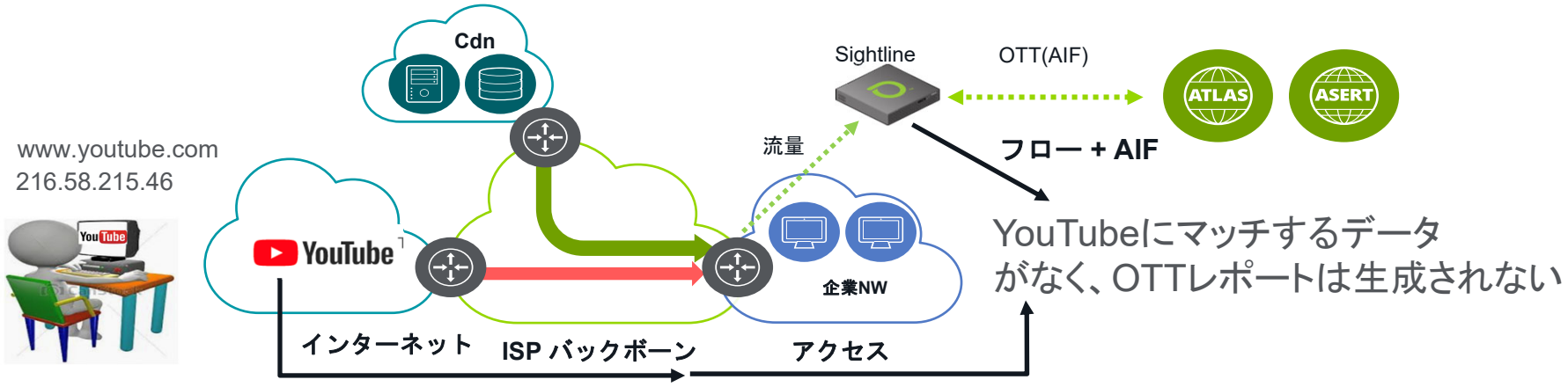
BGP Origin レポート

192.122.184.166 がほとんどのトラフィックを提供

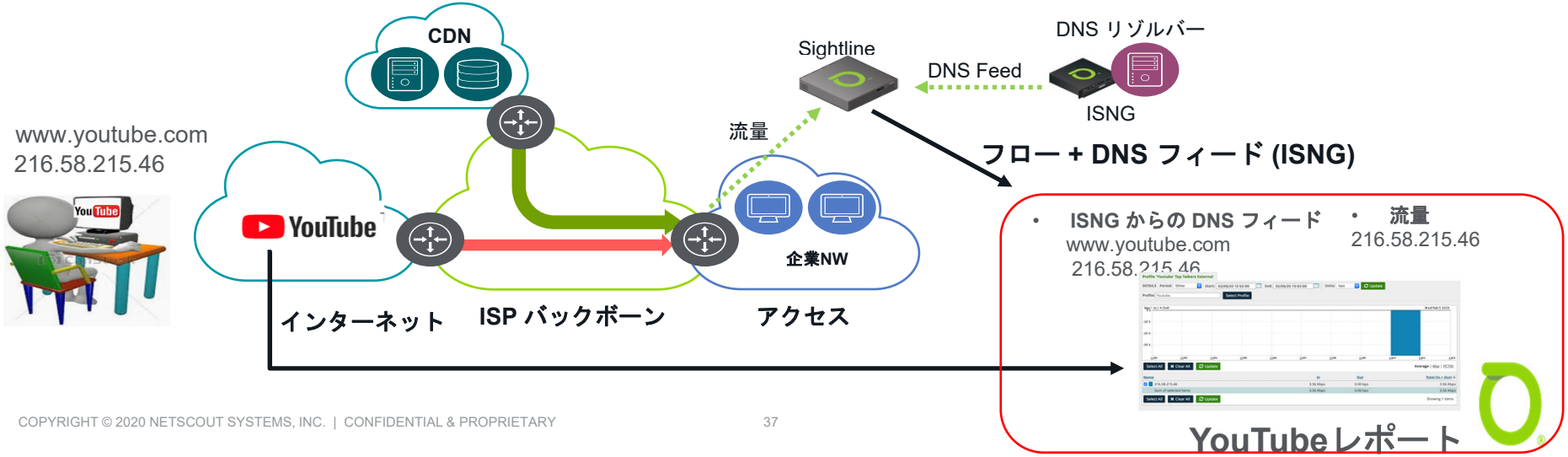
- トラフィックはどこへ送信されたか?
- トラフィックはどのルートでネットワークに入っているか?

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



NETSCOUT®

Guardians of the Connected World