

ThousandEyes

テクニカル ワークショップ

後編

サウザンドアイズ



ThousandEyes

ThousandEyes is
now part of Cisco. 

本日の内容

- Enterprise エージェント
- ネットワークテスト
- Webプロキシ環境の可視化
- オンラインビデオ会議の監視
- DNSサービスの監視
- インターネットにあるサービスの経路監視 (BGP)*
- ThousandEyes API *
- Q&A

Enterprise エージェント (社内エージェント)



Enterprise エージェント

- ユーザーの選んだ場所にインストールできる「マイ・エージェント」
- 仮想システムや物理サーバーで動作可能
 - 仮想アプライアンスは ESXi, Hyper-V, QEMU/KVM, Virtualbox などをサポート
 - Linux サーバーのパッケージ (RHEL/CentOS, Ubuntu)、Linuxコンテナ (Docker)
 - 物理アプライアンスは Intel NUCとRaspberry Pi 4 を正式サポート
- Cisco ハードウェア (2020/03)
 - Cisco 1000 ASR
 - Cisco 4000 ISR
 - Cisco Cat 9000
 - Cisco Cat 9300 (OSに組み込み)
- Enterpriseエージェントの機能はCloudエージェントと同じ



Enterprise エージェントのインストール : アプライアンス

The screenshot shows the 'Add New Enterprise Agent' window with the following sections:

- Appliance** (selected): Account Group Token (nx6v2qa9x1c0l6q...), Copy
- Virtual Appliance**: Virtualization Software with OVA/OVF support, VMWare (ESXi, Workstation, or Player), Oracle VirtualBox. Download - OVA, Installation Guide
- Hyper-V Appliance**: Hyper-V Manager, Microsoft Windows Server 2008, Microsoft Windows Server 2012. Download - OVA, Installation Guide
- Physical Appliance Installer**: Intel NUC. Download - ISO, Installation Guide
- Raspberry Pi 4**: * Browser tests are not supported. Download - IMG, Installation Guide
- Juniper Junos OS Container**: Juniper Cloud CPE, Juniper NFX250 Router. Download - QCOW2, Installation Guide

アカウントのトークン
エージェントをこのアカウントに紐付ける

仮想アプライアンス
□ メンテナンスのエージェント
ESXi, QEMU/KVM,
Hyper-V, Player, Virtualbox

物理アプライアンス
□ メンテナンスのエージェント
Intel NUC, Raspberry Pi 4
(RasPi はBrowser系の監視テスト :
Pageload, Transactionテストをサポートしません)

Enterprise エージェントのインストール : Linux のパッケージ

Appliance Custom Appliance Cisco Application Hosting **Linux Package** Docker IaaS Marketplaces

Installation Instructions

Ubuntu LTS 16.04, 18.04, 20.04
Red Hat Enterprise Linux 7.7+, 8.1+
CentOS 7.7+, 8.1+
Amazon Linux 2

curl is required for installation

Copy and run the following commands:

```
curl -0s https://downloads.thousandeyes.com/agent/install_thousandeyes.sh
chmod +x install_thousandeyes.sh
sudo ./install_thousandeyes.sh -b nx6v2qa9x1c0l6qkxwzqt:uiff5yb2gjf
```

Install BrowserBot At least 2GB of RAM required to run browser tests (BrowserBot)

Show Advanced Options

Linux のパッケージ
Ubuntu, RHEL, CentOS のサーバー
に
エージェントをインストール

アカウントのトークン

エージェントの動作環境は
アプライアンスと同じ :

vCPU x 2

エージェント用メモリ 2GB

エージェント用ストレージ 20GB

- Linuxの設定でインターフェイスやVRFを複数使うことが可能
- サーバーOSのメンテナンスとハードニングはお客様が担当

Enterprise エージェントのインストール : Linux コンテナ

Appliance Custom Appliance Cisco Application Hosting Linux Package **Docker** IaaS Marketplaces

Usage Instructions

Name
Tokyo_DC1

Docker Version
Docker 1.10.0 or later

Host Vol. Agent Directory ⓘ
/var

Proxy Type
None Static PAC

Install with BrowserBot support curl is required

Copy and run the following commands:

```
docker pull thousandeyes/enterprise-agent > /dev/null 2>&1
docker stop 'Tokyo_DC1' > /dev/null 2>&1
docker rm 'Tokyo_DC1' > /dev/null 2>&1
docker run \
  --hostname='Tokyo_DC1' \
  --memory=2g \
  --memory-swap=2g \
  --detach=true \
  --tty=true \
  --shm-size=512M \
  -e TEAGENT_ACCOUNT_TOKEN=nx6v2qa9x1c0l6q6awrqds0f5yb2gjf \
  -e TEAGENT_INET=4 \
  -v '/var/thousandeyes/Tokyo_DC1/te-agent':/var/lib/te-agent \
  -v '/var/thousandeyes/Tokyo_DC1/te-browserbot':/var/lib/te-browserbot \
  -v '/var/thousandeyes/Tokyo_DC1/log':/var/log/agent \
  --cap-add=NET_ADMIN \
  --cap-add=SYS_ADMIN \
  --name 'Tokyo_DC1' \
  --restart=unless-stopped \
  thousandeyes/enterprise-agent /sbin/my_init
```

Docker を使ったインストール
LinuxのDistributionの制限は無し
(サーバーOSのメンテナンスとハードニングはお客様が担当)

エージェントの動作環境は同じ :

vCPU x 2
エージェント用メモリ 2GB
エージェント用ストレージ 20GB

Enterprise エージェントのインストール : Cisco ルーター

Appliance Custom Appliance **Cisco Application Hosting** Linux Package Docker IaaS Marketplaces

Cisco IOS XE Docker Appliance
Catalyst 9000 Series Switches [Download - TAR](#)
* Browser tests are not currently supported. SSD not required.
[Installation Guide](#)

Copy, adapt, and run the following commands:

```
Device> enable
Device# app-hosting install appid DESIRED_APP_ID package https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-3.0.cat9k.tar
Device# configure terminal
Device(config)# app-hosting appid DESIRED_APP_ID
Device(config-app-hosting)# app-vnic AppGigabitEthernet trunk
Device(config-config-app-hosting-trunk)# vlan DESIRED_VLAN guest-interface 0
Device(config-config-app-hosting-vlan-access-ip)# guest-ipaddress DESIRED_IP netmask DESIRED_NETMASK
Device(config-config-app-hosting-vlan-access-ip)# exit
Device(config-config-app-hosting-trunk)# exit
Device(config-app-hosting)# app-default-gateway GATEWAY_IP guest-interface 0
Device(config-app-hosting)# name-server0 NAMESERVER1_IP
Device(config-app-hosting)# name-server1 NAMESERVER2_IP
Device(config-app-hosting)# app-resource docker
Device(config-app-hosting-docker)# prepend-pkg-opts
Device(config-app-hosting-docker)# run-opts 1 "-e TEAGENT_ACCOUNT_TOKEN=nx6v2qa9xc0l6q6awrqdts0f5yb2gjf"
Device(config-app-hosting-docker)# run-opts 2 "--hostname DESIRED_AGENT_HOSTNAME"
Device(config-app-hosting-docker)# exit
Device(config-app-hosting)# exit
Device(config)# exit
Device# write memory
Device# app-hosting activate appid DESIRED_APP_ID
Device# app-hosting start appid DESIRED_APP_ID
Device#
```

Cisco IOS XE KVM Appliance
Integrated Services Router (ISR)
Aggregation Services Router (ASR) [Download - Cisco OVA](#)
[Installation Guide](#)

Catalyst 9000 Series Switches [Download - TAR](#)
* Full test suite supported. SSD required.
[Installation Guide](#)



現在のサポート状況

- ISR 4000
- ASR 1000
- Catalyst 9000
- Catalyst 9300
- Catalyst 9400 (2021/4 予定)
- Catalyst 9500 (2021/8 予定)
- Catalyst 9600 (2021/8 予定)
- Catalyst 8200 (2021/8 予定)
- Catalyst 8300 (2021/8 予定)



Enterprise エージェントの起動 (アプライアンス型)

- 仮想アプライアンスの電源をON
- 起動後、エージェントを設定をするURLとログイン情報が表示

ThousandEyes Virtual Appliance

To configure your ThousandEyes Virtual Appliance, please point your browser to <http://192.168.1.148/>.
Username is 'admin', default password is 'welcome'.

Press N if you need to change the network configuration.
Press R to reset the appliance password.

Press Enter to update this screen.

コンソール画面表示内容 :

- WebUIのURL
- ユーザー名 (admin)
パスワード (welcome)
- ネットワークの設定
- パスワードリセット

Enterprise エージェントの初期設定 (アプライアンス型)

1. Self-signed デジタル証明書の警告は無視 😊
2. デフォルトのパスワードの変更
3. アカウントに紐付けるトークンを設定
4. Status 状態の確認
5. 追加設定 (optional) :
 - DNS サーバー
 - Proxy サーバー
 - Proxy 用のデジタル証明書のインストール
 - ソフトウェアのアップデートに使う Proxy サーバーの設定
 - クラウドアプリから設定の仕上げ

Enterprise エージェントの設定確認画面

ThousandEyes
Virtual Appliance
0.190

Network
Time
Appliance Access
Agent
Review

Review Log Out

Run Diagnostics

Appliance Status Last updated just now

- Agent is running. Restart Download Log
- Browserbot is running. Restart Download Log

Diagnostics

- Gateway is pingable 15 seconds ago Check Now
- DNS resolvers working 15 seconds ago Check Now
- NTP servers are contactable 15 seconds ago Check Now
- ThousandEyes collector is contactable 15 seconds ago Check Now
- ThousandEyes data ingress is contactable 15 seconds ago Check Now
- ThousandEyes API is contactable 15 seconds ago Check Now
- Account group token is valid 15 seconds ago Check Now
- ThousandEyes Apt repository is contactable 15 seconds ago Check Now
- Web interface password has been changed from default 15 seconds ago Check Now

この画面の項目が
全て緑色になればエージェントの設定完了

クラウドアプリからエージェントの設定

The screenshot displays the configuration page for a ThousandEyes agent named 'thousandeyes-va'. The interface is divided into several sections:

- Basic Configuration:** Fields for Agent Name (thousandeyes-va), Country (Japan), Region/City (Tōkyō), Account Groups (1 of 19 selected), Tests (Select item(s)), and Enable agent notifications (checked).
- Advanced Settings:** Includes Labels and Cluster options.
- Agent Statistics:** Shows Status: Online, Last Contact: 1 minute ago, Virtual Appliance Version (0.190), and Browserbot Version (1.128).
- General Information:** Lists system details such as Primary Account Group (Online Seminar), Created date (Wed, Nov 25, 2020), IP addresses, Operating System (Ubuntu 16.04.6 LTS), and Agent Version (1.104.1).

Red circles and lines highlight specific configuration elements: the Agent Name field, the Account Groups dropdown, the Tests dropdown, the Cluster dropdown, and the Agent Name field in the General Information section.

デフォルトの仮想エージェント名
(もっと分かりやすい名前に変更)

このエージェントを使える
アカウントグループを指定

新しいエージェントを
設定済みの監視テストに追加

Enterprise エージェントを別のアカウントで使うには

ThousandEyes
Virtual Appliance
0.198

Advanced Settings

Reboot Log Out

Setup Wizard Run Setup Wizard

Result Cache Clear Result Cache

This clears the cached state of the agent. Note that this clears test results that haven't been sent back to the ThousandEyes platform.

Agent State Reset Agent State

This resets the state of the agent and allows it to be used as if it was a newly set up agent. This should only be performed if you know what you are doing.

Logs

Browserbot Log
Agent Log
Web Server Log
System Log
Shell Log
Web Log

エージェントを
現在のアカウントから削除
(ネットワーク設定は残ります)

エージェントのトラブルシュー트에
役立つログがここから取得できます

Enterprise エージェントに関する資料

- [物理サーバーへのインストール（日本語）](#)
- [仮想サーバーへのインストール（日本語）](#)
- [仮想サーバーへのインストール \(mp4 ビデオ, 2MB\)](#)
- [Enterprise エージェントの設定方法（日本語）](#)
- [Enterprise Agent に関するオンラインマニュアル](#)

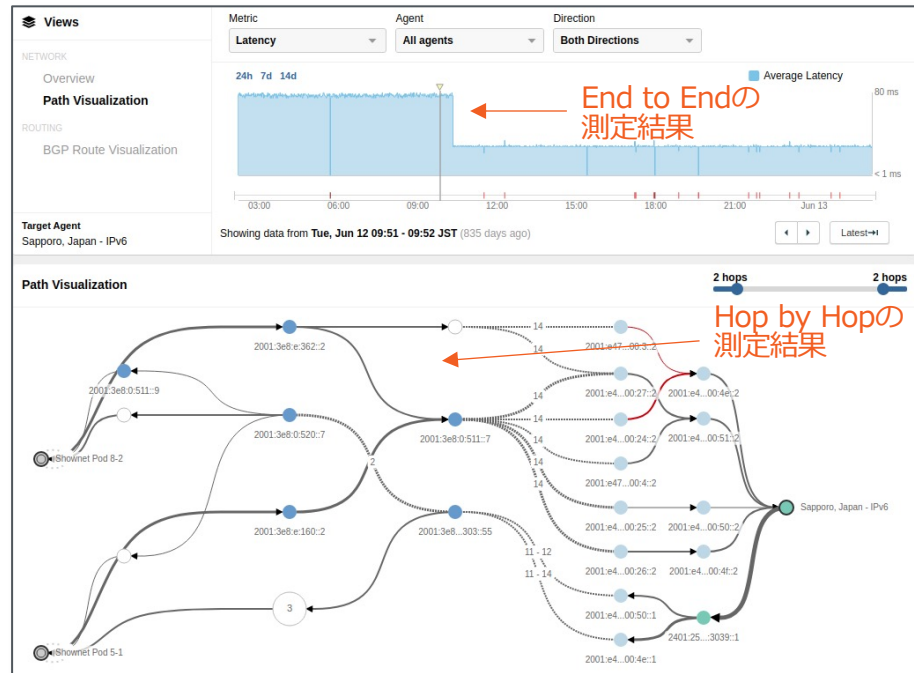
ネットワークテスト

Agent to Server テスト
エージェントとサービス間の可視化



ネットワークテストとは？

- アプリケーションサービスとエージェント間の可視化と品質測定
- ネットワークパスの可視化
 - マルチパスの検知
- ネットワークパスの品質測定
 - End to End
 - Hop by Hop
 - 双方向 (上り+下り)
- アプリケーションの死活監視



Agent to Server テスト

- **Server**とは TCP/ICMP に応答する送信先ホスト
 - TCP : imap/pop, rdp, proxy のポート など
 - ICMP : TCPに反応しないIPインターフェイス
- **Agent**は Cloud、Enterprise、Endpoint エージェント
- **任意のTCPポート**、ICMPをテストに使用可能
- ICMPよりも**TCPが優れた可視性を提供 (マルチパスの検知)**

Agent to Server テスト設定

New Test

Layer: Routing, **Network**, DNS, Web, Voice

Test Type: **Agent to Server**, Agent to Agent

Test Name: 10.1.1.1:3389

Test Description: Optional

Basic Configuration | Advanced Settings

Target: 10.1.1.1

Protocol: TCP | Port: 3389

Probing Mode: **Prefer SACK**, Force SACK, Force SYN

Path Trace Mode: In Session

Interval: 2 minutes

Agents: 2 of 3 selected

Alerts: Enable
2 of 2 alert rules selected | Edit Alert Rules

ターゲット (IP,ドメイン名)

TCP/ポート番号、ICMP

「tracerouteを止めるFirewall」対策

テストの実行間隔

テストを実行するエージェント

Agent to Server テスト設定

Basic Configuration | **Advanced Settings**

NETWORK

Data Collection Perform bandwidth measurements
 Perform MTU measurements
 Collect BGP data

Ping Payload Size **Auto** | Manual

Transmission Rate Enforce fixed packet rate
10 pps

No. of Path Traces Default (3)

DSCP Best Effort (DSCP 0)

ターゲットの
経路データの取得

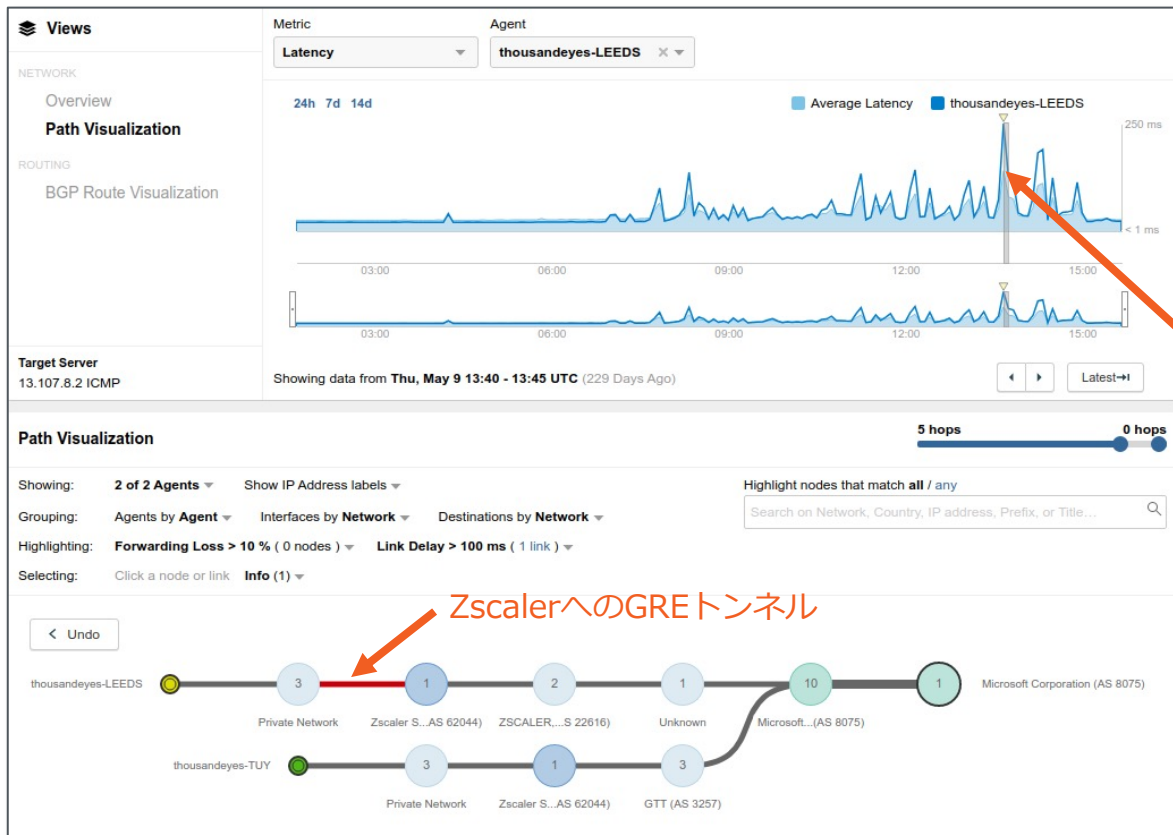
End-to-End
トラフィックの
送信レート

検出する
マルチパスの数

DSCPの値を設定

監視例 (1) : Zscalerを経由するMS Skypeへのパス

スナップショット



最大100msのRTTが推奨される
MS Skypeのトラフィックに
250ms以上の遅延が発生

監視テストはICMPを使った
Agent to Server テスト

ネットワークテスト

Agent to Agent テスト
エージェント間の可視化



Agent to Agent テスト

- エージェント間（ネットワーク間）のネットワーク測定
- 双方向のネットワークパスの品質測定と可視化
- 任意のTCP/UDPポートをテスト用に使用可能
- ICMPよりもTCPが優れた可視性を提供（マルチパスを検知）
- 環境によってはネットワークの設定変更が必要
 - 双方向テストではFirewallに外部から社内エージェント宛のルールを追加
 - 社内エージェント宛のNAT設定の変更
- ★ Endpointエージェントを使った Agent-to-Agent テストは不可

Agent to Agent テストの設定

Basic Configuration | **Advanced Settings**

Test Name: 社内 WAN 双方向テスト

Target Agent: HQ 1 × ▼ ● 監視テストのターゲットとなるエージェント (1台)

Interval: 2 minutes ▼ ● ターゲットのエージェントとネットワークの測定をするエージェント (複数)

Agents: 11 of 391 selected ▼ ●

Direction: Both Directions ▼ ● 測定トラフィックの方向

Protocol: TCP ▼ ● TCP/UDP

Enable Throughput

Path Trace Mode: In Session ● TCPのセッション内でtracerouteを実行するモード (IPS/FW 対策)

Agent to Agent テストの設定

Basic Configuration | **Advanced Settings**

NETWORK

Server Port

MSS bytes

Collect BGP data

Transmission Rate Enforce fixed packet rate
 10 pps

No. of Path Traces Default (3)

DSCP

TCP/UDP 受信ポート

ターゲットの経路情報の取得
プライベートIPでは必要なし

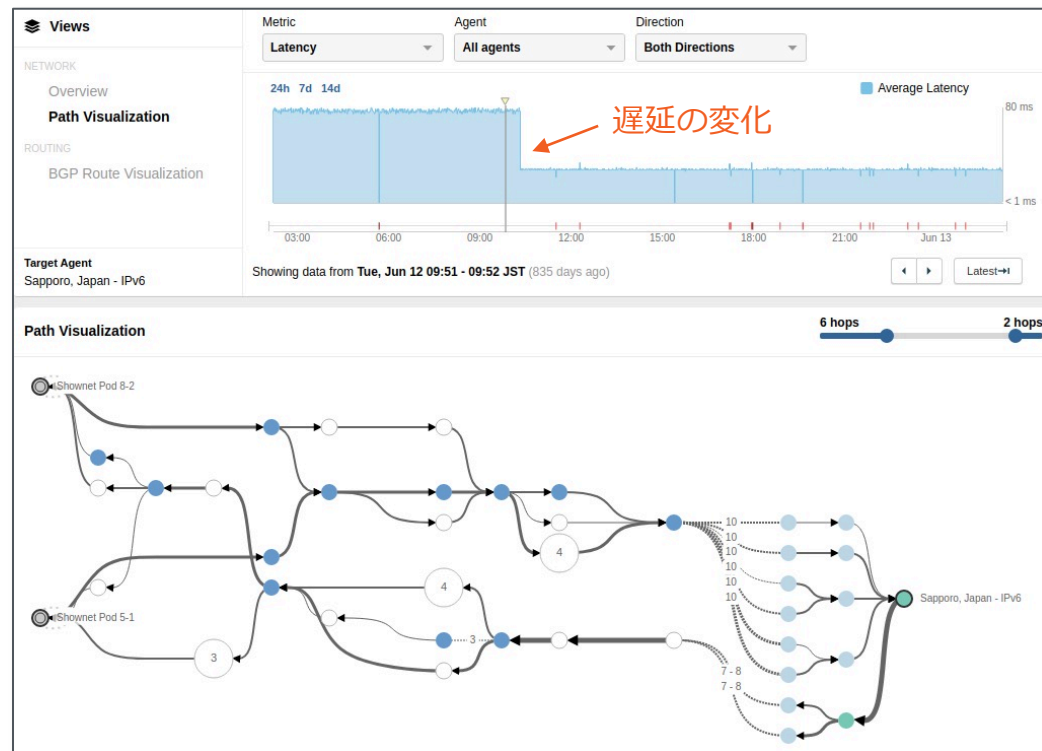
測定トラフィックの速度

検知するマルチパスの数

DSCPの設定
(ルーターホップ毎にDSCPが見える)

Agent to Agent の監視テスト例 (1)

Agent to Agent テストを使った支店・本社WANの双方向品質監視
ISPのピアリングが変更して、ネットワークの遅延が大きく変わる

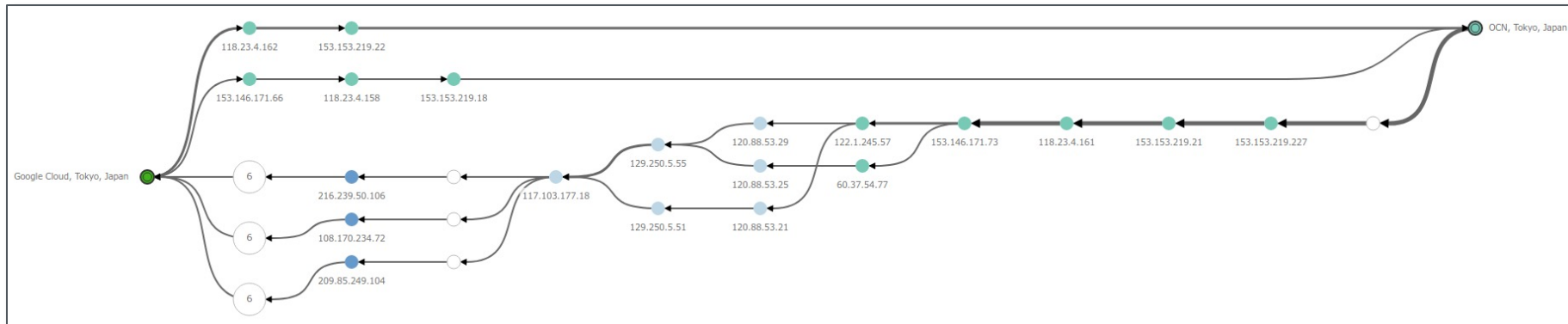


[共有リンク](#)

Agent to Agent の監視テスト例 (2)

上りと下りの経路が異なるネットワークパス

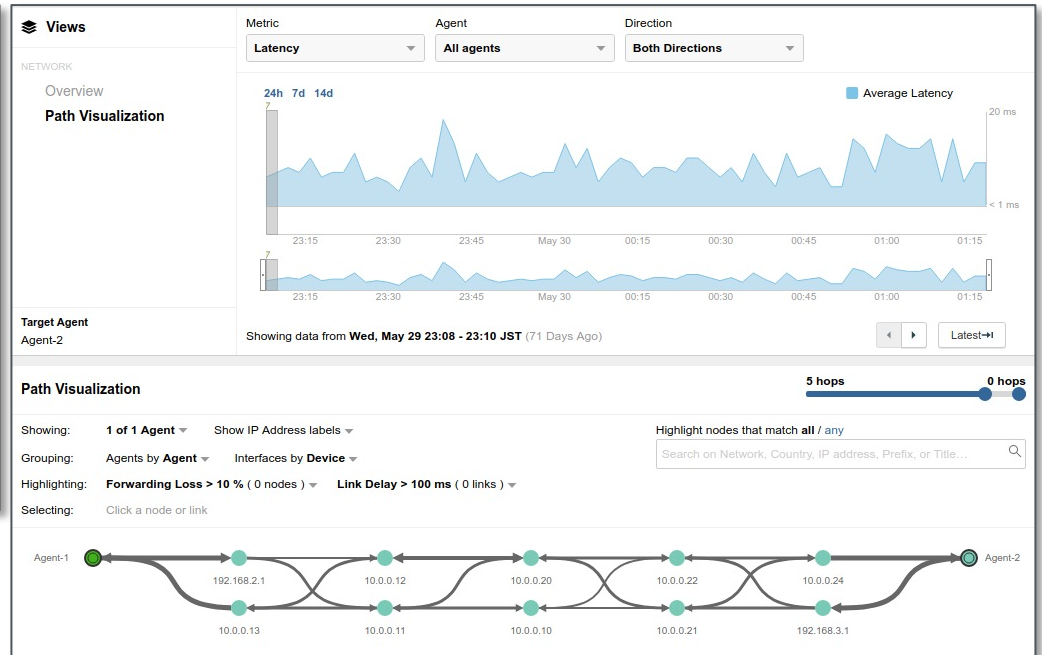
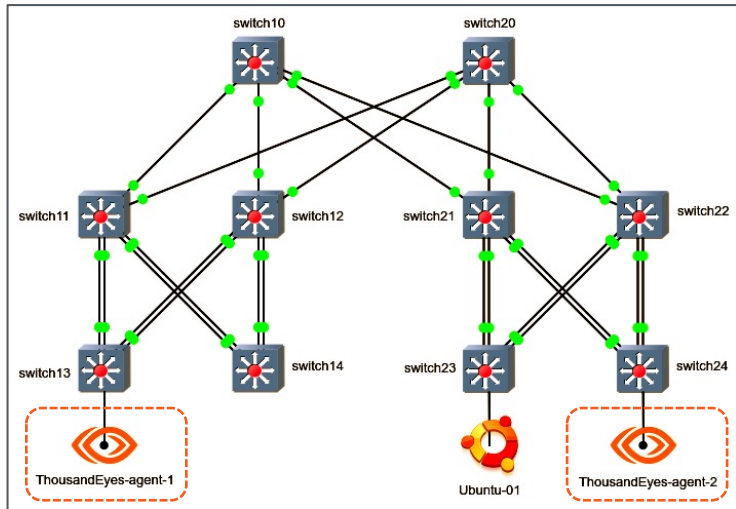
双方向の監視テストを実行して分かる 非対称ルーティング



共有リンク

監視例 (3) : データセンターLANの監視

IP/Clos ネットワークのアプリケーションパスの可視化
Agent-to-Agentの双方向テストを使い多数のパスのある
ネットワークのアプリケーションパスを可視化



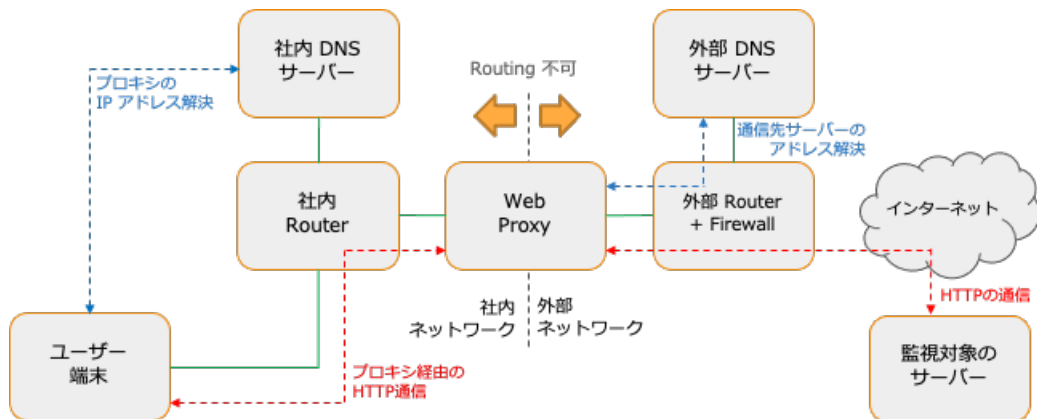
スナップショットの共有リンク

Web プロキシ環境の可視化

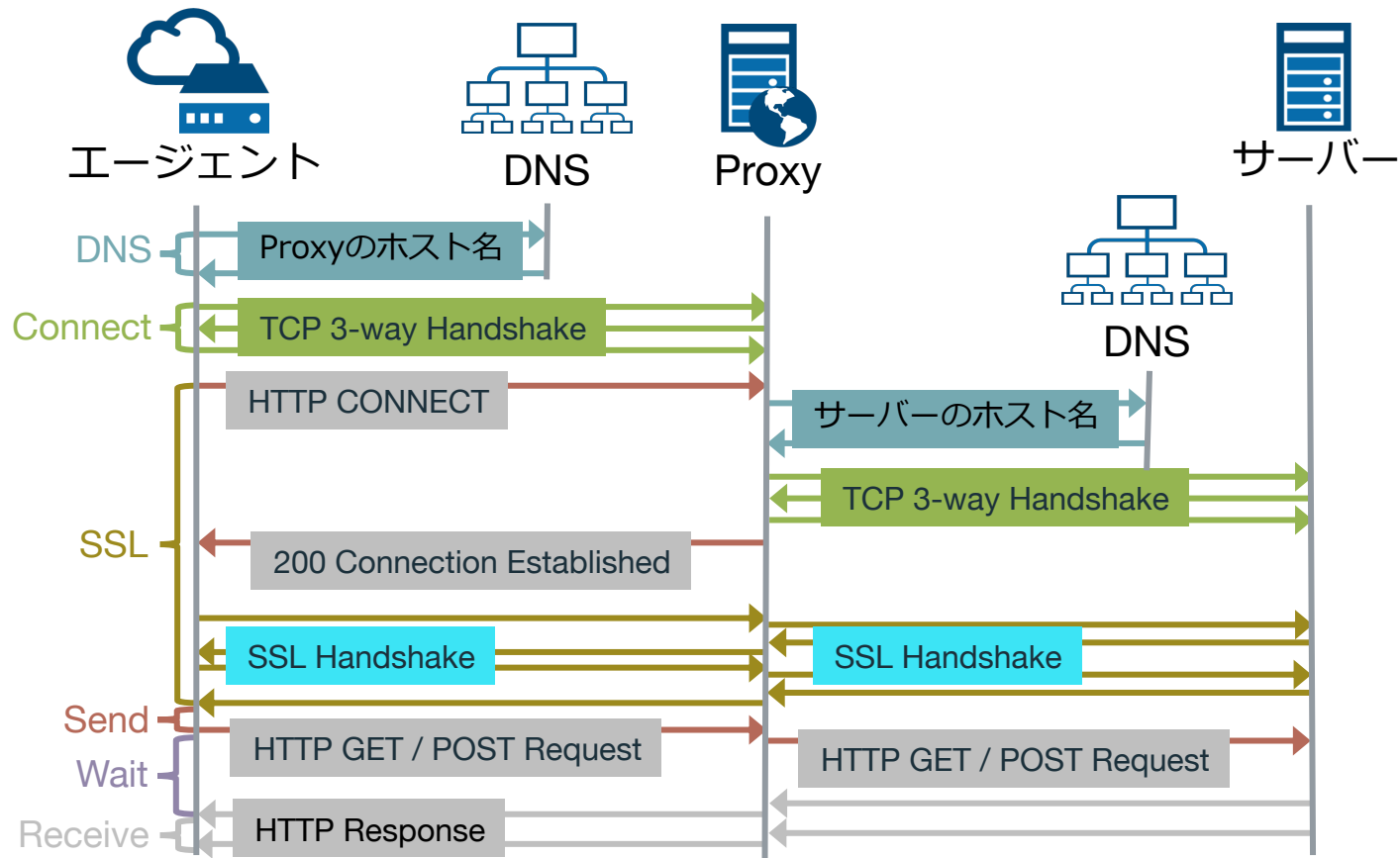


Web プロキシ

1. 社内ネットワークからインターネットへのWeb アプリのトラフィック制御を実行
2. Web プロキシの種類：
 - a. ユーザー端末にプロキシの設定をする **Explicit** 構成（最も一般的構成）
 - b. プロキシ指定をしていないクライアントのトラフィックを外部デバイスがプロキシにリダイレクトする **Transparent** 構成
 - a. 社内ネットワークと外部ネットワークの通信は全てプロキシを経由する構成（下の図）



Web プロキシを使ったHTTPの動作



エージェントに3種類のプロキシ設定が可能

1. エージェントのWebUIから固定・PACファイルの設定

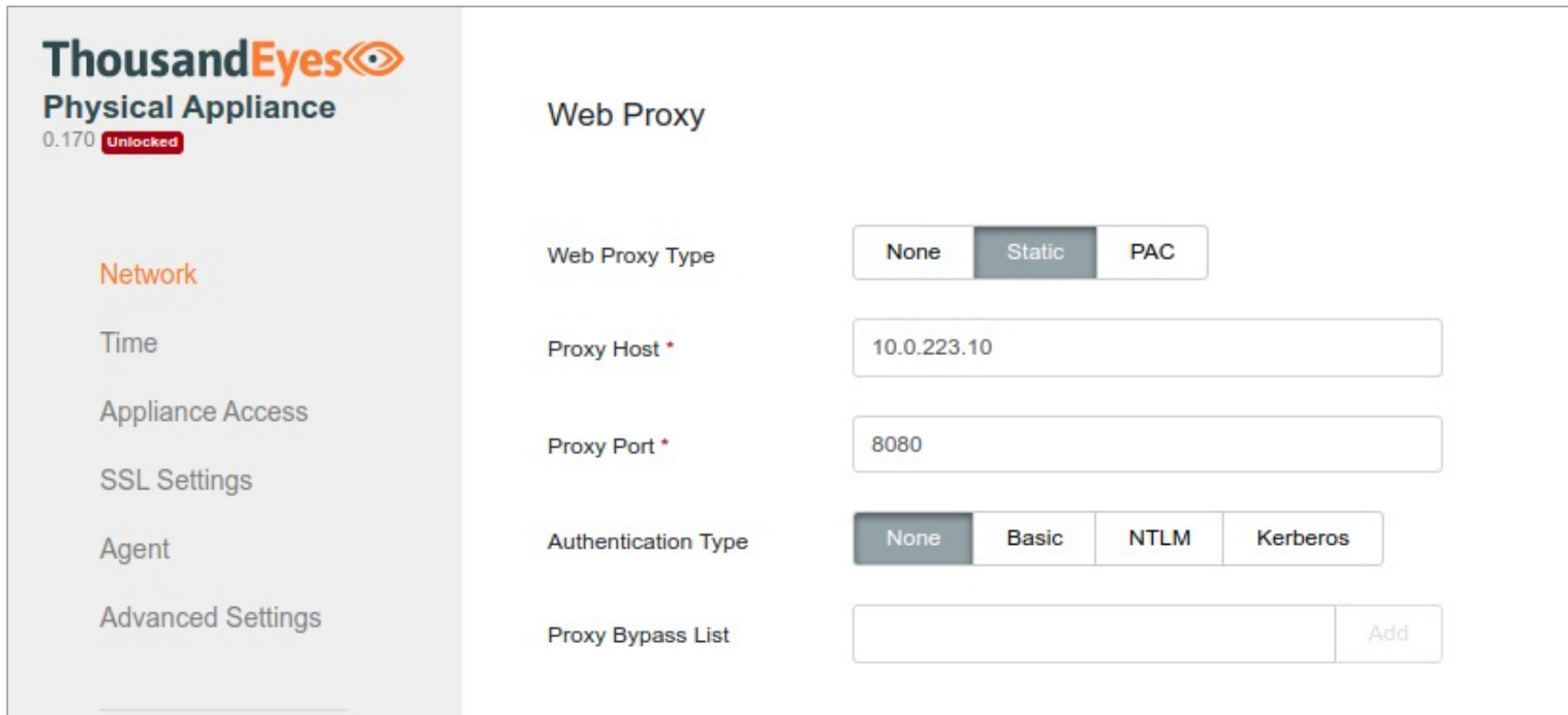
- 監視テスト内でプロキシ設定を変更しない限り**すべての通信** (監視テスト、ThousandEyesとの通信) は**プロキシ経由**で実行
- **プロキシを経由**しないと**インターネットに抜けられない**環境ではエージェントのWebUIから初期設定の際にプロキシを設定

2. ThousandEyesのクラウドアプリからプロキシの設定

3. 監視テスト毎のプロキシ設定

- テスト毎に異なる**プロキシ**有り・無しの実行が可能
- 但しThousandEyesとの通信は**1**と**2**で設定したプロキシを経由する

1. エージェントのWebUIからWebプロキシの設定



The screenshot displays the configuration interface for the Web Proxy on a ThousandEyes Physical Appliance. The left sidebar shows the navigation menu with 'Network' selected. The main content area is titled 'Web Proxy' and contains the following settings:

- Web Proxy Type:** A radio button group with three options: 'None', 'Static' (selected), and 'PAC'.
- Proxy Host *:** A text input field containing the IP address '10.0.223.10'.
- Proxy Port *:** A text input field containing the port number '8080'.
- Authentication Type:** A radio button group with four options: 'None' (selected), 'Basic', 'NTLM', and 'Kerberos'.
- Proxy Bypass List:** A text input field with an 'Add' button to its right.

ThousandEyes Physical Appliance
0.170 Unlocked

Network
Time
Appliance Access
SSL Settings
Agent
Advanced Settings

2.クラウドアプリのUIからWebプロキシの設定

Cloud & Enterprise Agents > Agent Settings > Proxy Settings

Add New Proxy Configuration ✕

Proxy Configuration Name
internal proxy

Authentication Type
None

Type
Static PAC

Host Port
10.0.200.23 8888

Bypass List
Separate list items by pressing "Enter"/"Return"

Enterprise Agents
0 of 0 selected

このプロキシ構成の名前

認証の設定

固定プロキシ・PACファイルの選択

固定プロキシの設定

プロキシを経由しないターゲット

このプロキシ設定を使うエージェント

3. 監視テストのプロキシ設定

HTTP / Page Load / Transaction テストの設定画面の Advanced Setting から

- a) 監視テストが使用するプロキシの選択と
- b) エージェント ⇄ プロキシ間のネットワーク品質測定の設定が可能



The screenshot shows the 'PROXY SETTINGS' section of a configuration interface. It includes a 'Proxy Option' dropdown menu currently set to 'Enterprise Agent's proxy configuration' and a checked checkbox labeled 'Perform network measurements to the proxy'. Two red lines with circular endpoints point from the text annotations to these specific UI elements.

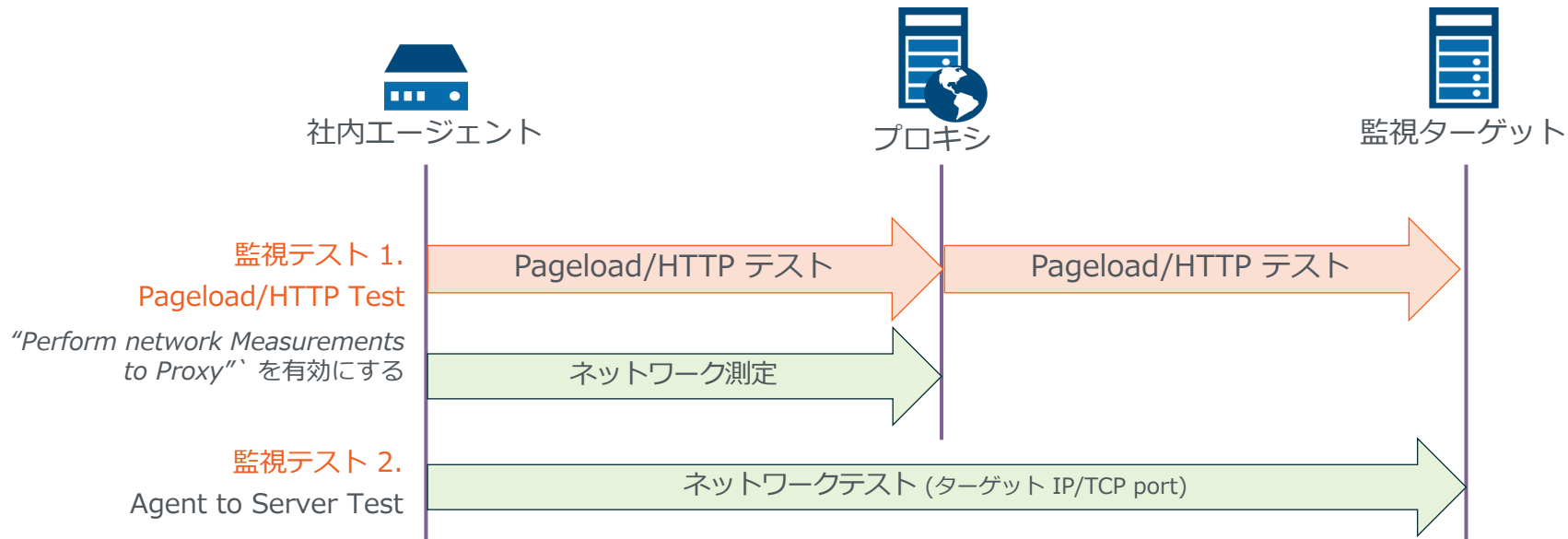
監視テストの実行に使われる Proxyサーバーの選択

エージェントとProxyサーバー間のネットワーク品質測定を実行する

- c) 特定の監視テストだけプロキシをバイパスする設定も可能

Webプロキシを使ったパスの可視化

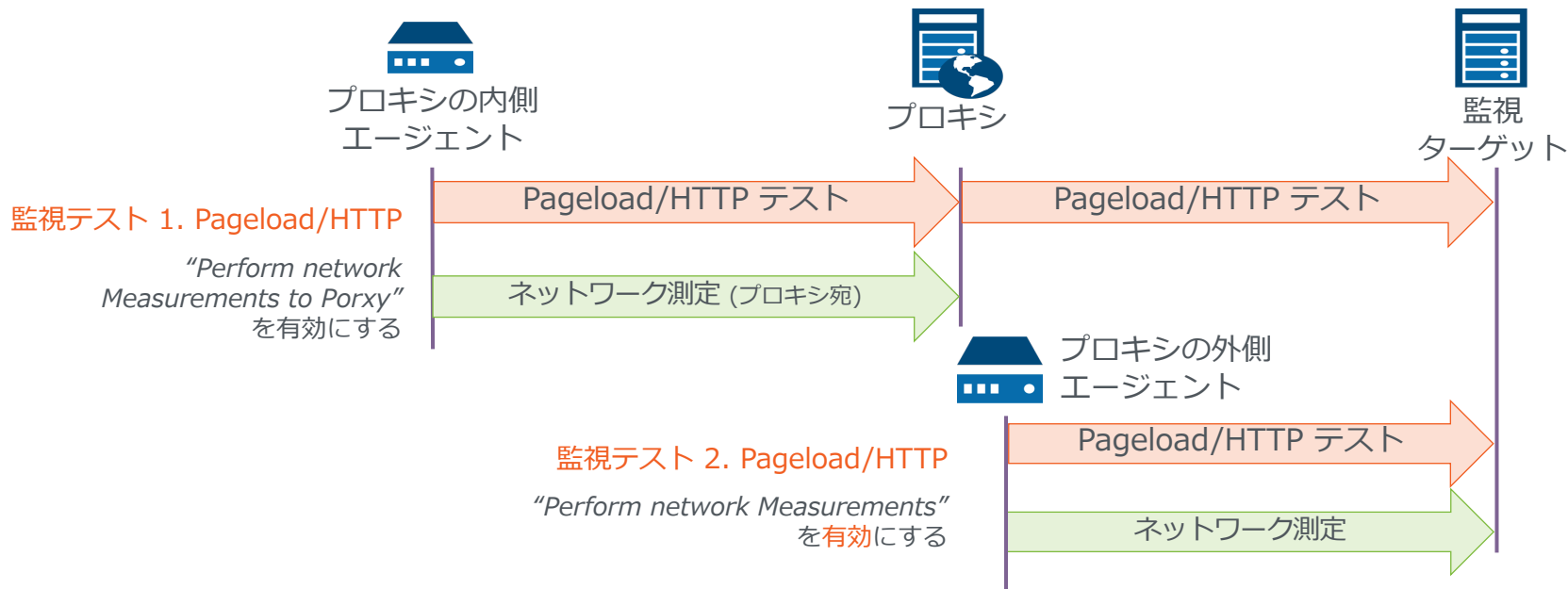
(監視ターゲットにエージェントからtracerouteが可能な場合)



1. プロキシを経由するWebアプリのレスポンスとプロキシまでのネットワークパスの品質測定をする **HTTP/PageLoad テスト**
2. エージェントと監視対象のサーバー間のネットワークの可視化と品質を直接測定する **Agent to Server ネットワークテスト**

Webプロキシを使ったパスの可視化

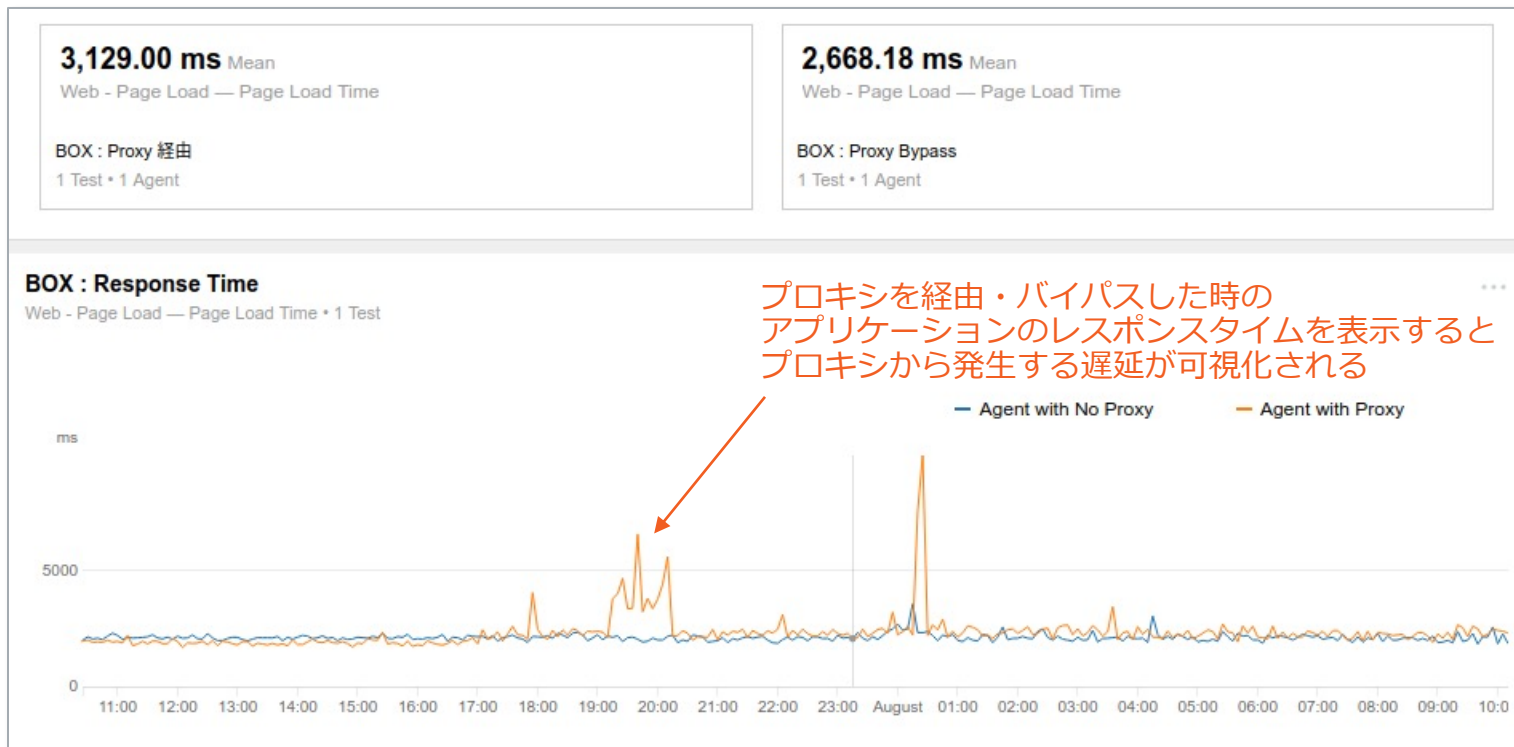
(監視ターゲットにエージェントからtracerouteが不可能な場合)



- Proxy経由以外は外部ネットワークに通信不可であるネットワークでは、プロキシを境界線として、プロキシの両側を別に測定する。
- 一般的にはこの方法の監視テストを推奨します。

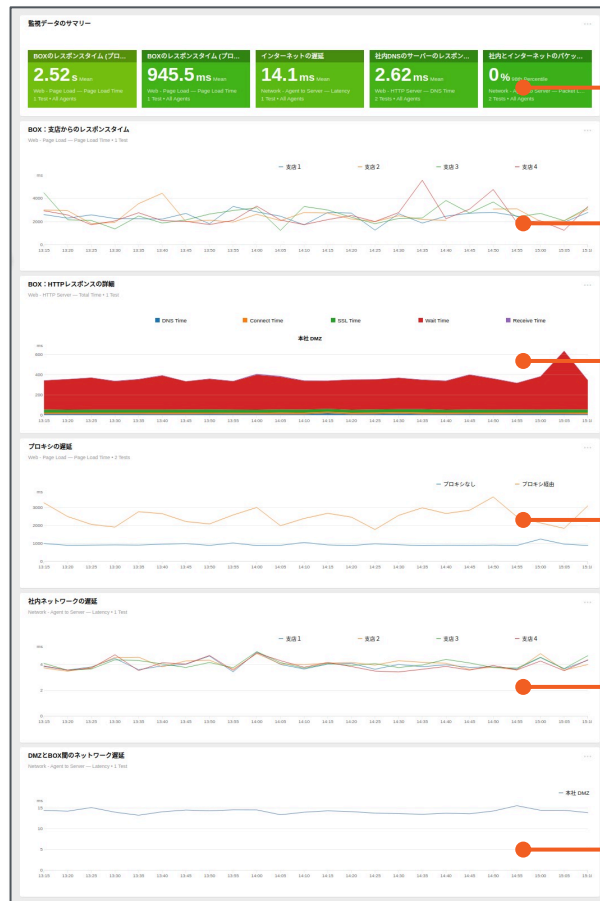
Webプロキシの負荷を監視

レポートやマルチテストViewの機能を使い、プロキシから発生する遅延を監視



Webプロキシ環境の監視レポート

[共有リンク](#)



全体のステータス

支店のアプリのレスポンス

レスポンスタイムの詳細

プロキシから発生した遅延

プロキシへの遅延

プロキシの外側から
Webアプリのレスポンス

関係資料

[HTTPプロキシを使用したパフォーマンスの測定](#)

[Zscaler Web Secure Gatewayの監視](#)

[Installing Enterprise Agents in Proxy Environments](#)

[Configuring an Enterprise Agent to Use a Proxy Server](#)

[Measuring Performance with HTTP Proxies](#)

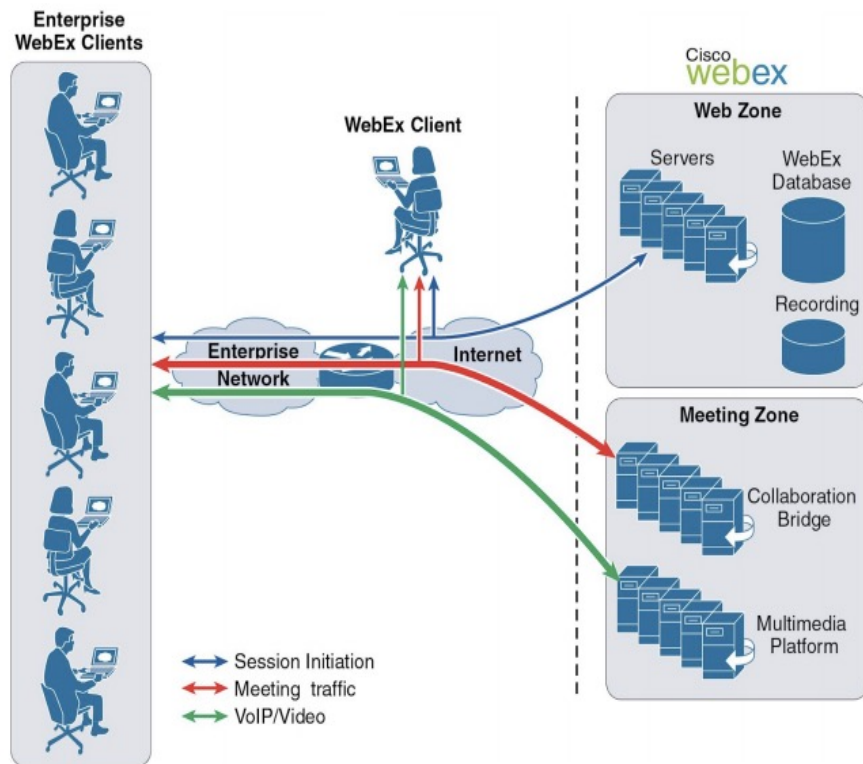
オンラインビデオ会議の監視

Webex

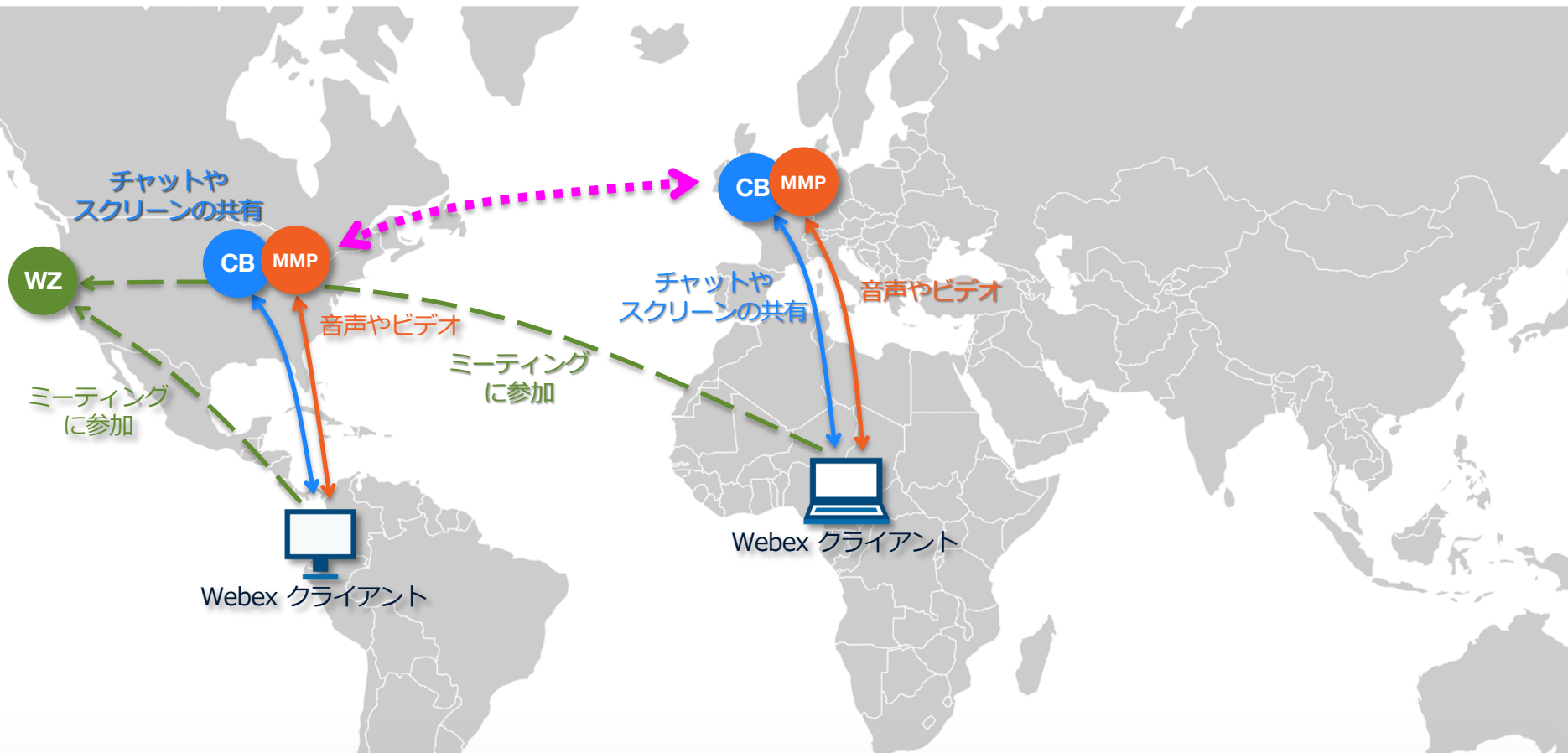


Webex のアーキテクチャ

1. Webexデータセンターは、Webゾーンと Meetingゾーンに分割
2. ユーザーは**初めにWebゾーンに接続**。Webゾーンは認証、スケジューリング、課金、レポート、レコーディングなどのタスクを処理
3. Meetingゾーンには**チャットやデスクトップ共有**などの通信処理をするコラボレーションブリッジ (CB)、会議の**音声やビデオストリーム**の処理するマルチメディアプラットフォーム (MMP)がある
4. WebゾーンのDCはお客様の本社に近いロケーション、**会議ゾーンは接続するユーザーに近いDC**が選択される



グローバルに分散された会議



Webexの監視ターゲット

1. MMPやCBは共に数が10,000ノードを超える (2020/4月)
2. Webexのクライアントが接続するMMP/CBは動的に選択されるため、事前に監視ターゲットを選択することは難しい
3. 何処のDCのCB/MMPが選択されるかはパケットキャプチャやDNSのリクエストから確認

CB/MMPのドメイン名:

- *cb*.webex.com のホスト名が Collaboration Bridge、
- *mcs*.webex.com のホスト名が Multimedia Platform

監視テストのターゲットをキャプチャ

No.	Time	Protocol	Info
6733	13.927676	DNS	Standard query 0xad5c A ed1lncbmm60.webex.com
6734	13.928045	DNS	Standard query 0x1871 A ed1chcbmm100.webex.com
6735	13.936995	DNS	Standard query response 0xb90c A ed1txcbmm80.webex.com A 209.197.222.159
6736	13.937640	DNS	Standard query response 0x2161 A ed1sgcbmm10.webex.com A 114.29.213.212
6739	13.938757	DNS	Standard query response 0xf96f A ed1sycbmm90.webex.com A 69.26.183.22
6740	13.939076	DNS	Standard query response 0xad5c A ed1lncbmm60.webex.com A 62.109.231.3
6743	13.939721	DNS	Standard query response 0x6006 A eaccbmm10.webex.com A 66.114.168.168
6745	13.940490	DNS	Standard query response 0x1871 A ed1chcbmm100.webex.com A 173.243.4.76
7117	14.393513	DNS	Standard query 0xeb8c A global-tsa3.webex.com
7419	14.517573	DNS	Standard query response 0xeb8c A global-tsa3.webex.com A 64.68.120.47
104...	15.595583	DNS	Standard query 0x1b8b A ed1sgcb25901.webex.com
104...	15.609424	DNS	Standard query response 0x1b8b A ed1sgcb25901.webex.com CNAME ed1sgcb259.webex.com A 150.253.208.155
112...	16.096072	DNS	Standard query 0xb1f4 A msj6mcccl01.webex.com
115...	16.259791	DNS	Standard query response 0xb1f4 A msj6mcccl01.webex.com CNAME global-msj6mcccl01.webex.com A 66.114.169.71
118...	16.405647	DNS	Standard query 0xfeef A dnszombie.cisco.com
118...	16.406967	DNS	Standard query response 0xfeef No such name A dnszombie.cisco.com
118...	16.407210	DNS	Standard query 0xbeef TXT debug.opendns.com OPT
118...	16.415839	DNS	Standard query response 0xbeef TXT debug.opendns.com SOA auth1.opendns.com OPT
124...	16.797082	DNS	Standard query 0xdc04 A m06sgmcs101.webex.com
125...	16.816818	DNS	Standard query response 0xdc04 A m06sgmcs101.webex.com A 114.29.210.131
137...	17.771764	DNS	Standard query 0x631b PTR 183.1.168.192.in-addr.arpa
137...	17.773189	DNS	Standard query response 0x631b PTR 183.1.168.192.in-addr.arpa PTR MARTYN1-M-V5B4.lan

Collaboration Bridge (cb) : ed1sgcb259.webex.com

Multimedia Platform (mmp) : m06sgmcs101.webex.com

監視テストに使える 日本国内Webex DCの監視ターゲット

パケットキャプチャやDNSのログにアクセスできない場合、
以下の日本国内にあるWebEx DC内のサーバー宛に監視テストを設定

サービスの種類	ドメイン名のフォーマット	ドメイン名
Multimedia Platform	*jpmcs*.webex.com	m06jpmcs113.webex.com m06jpmcs201.webex.com m06jpmcs212.webex.com
Collaboration Bridge	*jp2cb*.webex.com	ed1jp2cb53201.webex.com ed1jp2cb52202.webex.com

Webexの監視テストの設定例

テストの種類	ターゲット	エージェント	間隔	パラメーター
DNS Server (ローカル DNS サーバー)	<会社名>.webex.com IN,A	Enterprise	5分間	Path Trace : In Session No. of Path Traces : 5 Transmission Rate : 10 pps Send recursive queries : ENABLE
HTTP テスト (WebZone)	https://<会社名>.webex.com	Enterprise + Cloud	2-5分間隔	HTTP interval : 2 min No. of Path Traces : 5 Path Trace : In Session Transmission Rate : 10 pps
HTTP Server * (Collaboration Bridge)	https://ed1jp2cb53201.webex.com + https://ed1jp2cb52202.webex.com	Enterprise エージェント + Cloud エージェント	2分間	No. of Path Traces : 5 Path Trace : In Session Transmission Rate : 10 pps
Agent to Server * (Multimedia Platform)	m06jpmcs113.webex.com + m06jpmcs201.webex.com	Enterprise エージェント + Cloud エージェント	1-2分間	TCP port 5004 Path Trace : In Session No. of Path Traces : 5 Transmission Rate : 10 pps DSCP : EF (DSCP 46)

* CBとMMPの監視テストは、傷害の際にサーバーとネットワーク問題の切り分けのために**2台ずつ**監視テストを設定します

Webex監視テストの設定例

- Webex監視に必要な監視テストの一覧

The screenshot displays the 'Test Settings' page in the Cisco Cloud & Enterprise Agents interface. The left sidebar contains navigation options such as 'Views', 'Test Settings', 'Agent Settings', 'BGP Monitors', 'Endpoint Agents', 'Devices', 'Internet Insights', 'Dashboards', 'Alerts', 'Reports', 'Sharing', and 'Account Settings'. The main content area is titled 'Tests' and includes an 'Add New Test' button and a search filter. Below the search bar is a table listing the configured tests.

Test Name ▲	Type	Target	Alerts	Enabled	
▶ ThousandEyes WebEx	Web - HTTP Server	https://thousandeyes.webex.com	✓	✓	...
▶ WebEx CB JP #1	Web - HTTP Server	https://ed1jp2cb53201.webex.com	✓	✓	...
▶ WebEx CB JP #2	Web - HTTP Server	https://ed1jp2cb52202.webex.com	✓	✓	...
▶ WebEx DNS	DNS Server	thousandeyes.webex.com A · UDP	✓	✓	...
▶ WebEx Media Server JP #1	Network - Agent to Server	m06jpmcs201.webex.com:5004	✓	✓	...
▶ WebEx Media Server JP #2	Network - Agent to Server	m06jpmcs113.webex.com:5004	✓	✓	...

Webex監視テストの設定例：DNSサーバー

- DNSサーバーテストの基本設定

The screenshot displays the 'Basic Configuration' tab of a Webex monitoring test setup. The fields are as follows:

- Test Name:** WebEx DNS
- Test Description:** DNS lookup for WebEx to local DNS servers
- Domain:** thousandeyes.webex.com
- Interval:** 5 minutes
- Agents:** 1 of 391 selected
- DNS Servers:** 192.168.1.8, 192.168.1.17

Red lines connect the following fields to labels on the right:

- Domain dropdown (IN/A) to: お客様にアサインされた Webex URL
- Agents dropdown to: 社内Enterpriseエージェント
- DNS Servers input field to: 社内DNSサーバー

お客様にアサインされた
Webex URL

社内Enterpriseエージェント

社内DNSサーバー

Webex監視テストの設定例：DNSサーバー

- DNSサーバーテストのアドバンス設定

Basic Configuration | **Advanced Settings**

NETWORK

Data Collection Perform network measurements

- Perform bandwidth measurements
- Perform MTU measurements
- Collect BGP data

All public BGP monitors will be included

Protocol **TCP**

Probing Mode **Prefer SACK** Force SACK Force SYN

Path Trace Mode In Session

Transmission Rate Enforce fixed packet rate

10 pps

No. of Path Traces Default (1)

DNS

Send recursive queries

Transport **UDP**

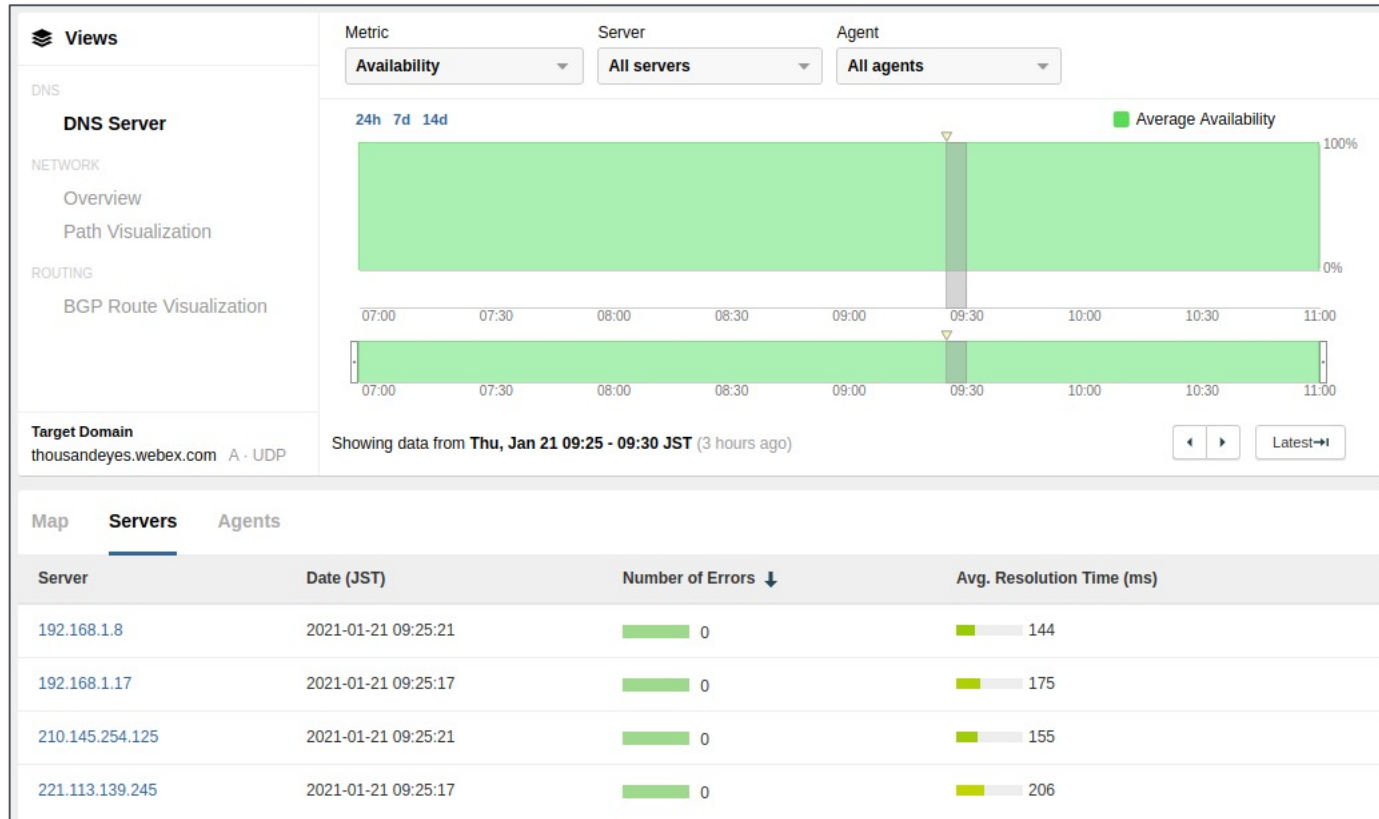
サーバーと接続したTCPセッション内での
End to Endのネットワーク品質測定を実行

サーバーに優しい送信レート

IPアドレスを解決するまで
DNSクエリを続けるように設定

Webex : ローカルDNSサーバーの監視例

[共有リンク](#)



Webex監視テストの設定例：WebZone

- HTTPサーバーテストの基本設定

The screenshot displays the 'Basic Configuration' tab of a test configuration interface. It includes the following fields:

- Test Name:** ThousandEyes WebEx
- Test Description:** WebEx launch/control server for ThousandEyes
- URL:** https://thousandeyes.webex.com. A red dot is positioned at the end of the URL field, with a red line extending to the right towards the explanatory text.
- Interval:** 5 minutes (selected from a dropdown menu)
- Agents:** 3 of 391 selected. A red dot is positioned at the end of the agents field, with a red line extending to the right towards the explanatory text.

Below the URL field, a note states: "Editing this field will require test credentials to be reentered".

- 1) お客様のWebex URL
- 2) Collaboration Bridge

社内Enterpriseエージェント
+ Cloud エージェント

Webex監視テストの設定例：WebZone

- HTTPサーバーテストのアドバンス設定

The screenshot shows the 'Advanced Settings' tab for an HTTP server test. It is divided into two sections: 'HTTP SERVER TIMING' and 'NETWORK'. In the 'HTTP SERVER TIMING' section, there are two sliders: 'Timeout' set to 5 s and 'Target Response Time' set to 1000 ms. The 'NETWORK' section includes a 'Data Collection' section with four checkboxes: 'Perform network measurements' (checked), 'Perform bandwidth measurements' (unchecked), 'Perform MTU measurements' (unchecked), and 'Collect BGP data' (checked). Below this, it states 'All public BGP monitors will be included'. There is a 'Protocol' dropdown menu set to 'TCP'. The 'Probing Mode' section has three buttons: 'Prefer SACK' (selected), 'Force SACK', and 'Force SYN'. The 'Path Trace Mode' section has a checked checkbox for 'In Session'. The 'Transmission Rate' section has a checked checkbox for 'Enforce fixed packet rate' and a slider set to 10 pps. The 'No. of Path Traces' section has a checked checkbox for 'Default (3)'.

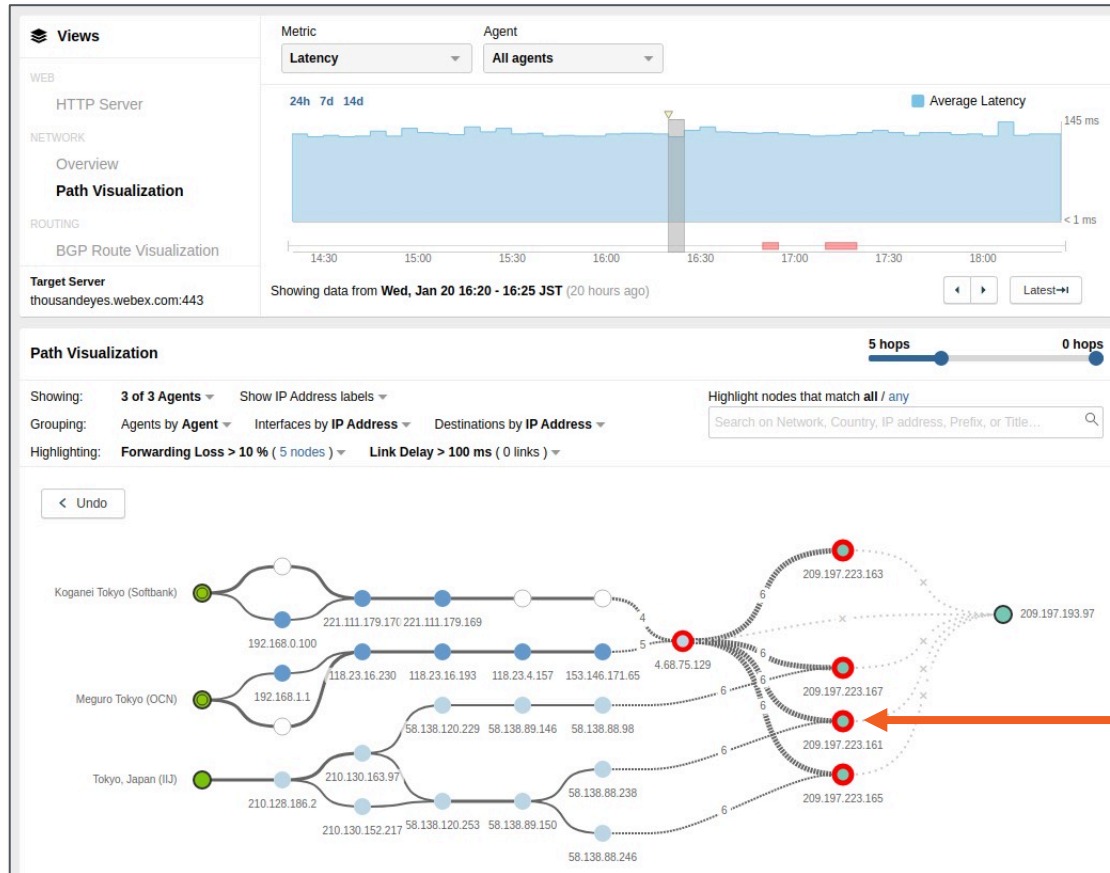
BGPの経路データを取得する

サーバーと接続したTCPセッション内での
End to Endのネットワーク品質測定を実行

サーバーに優しい送信レート

Webex WebZone の監視例

[共有リンク](#)

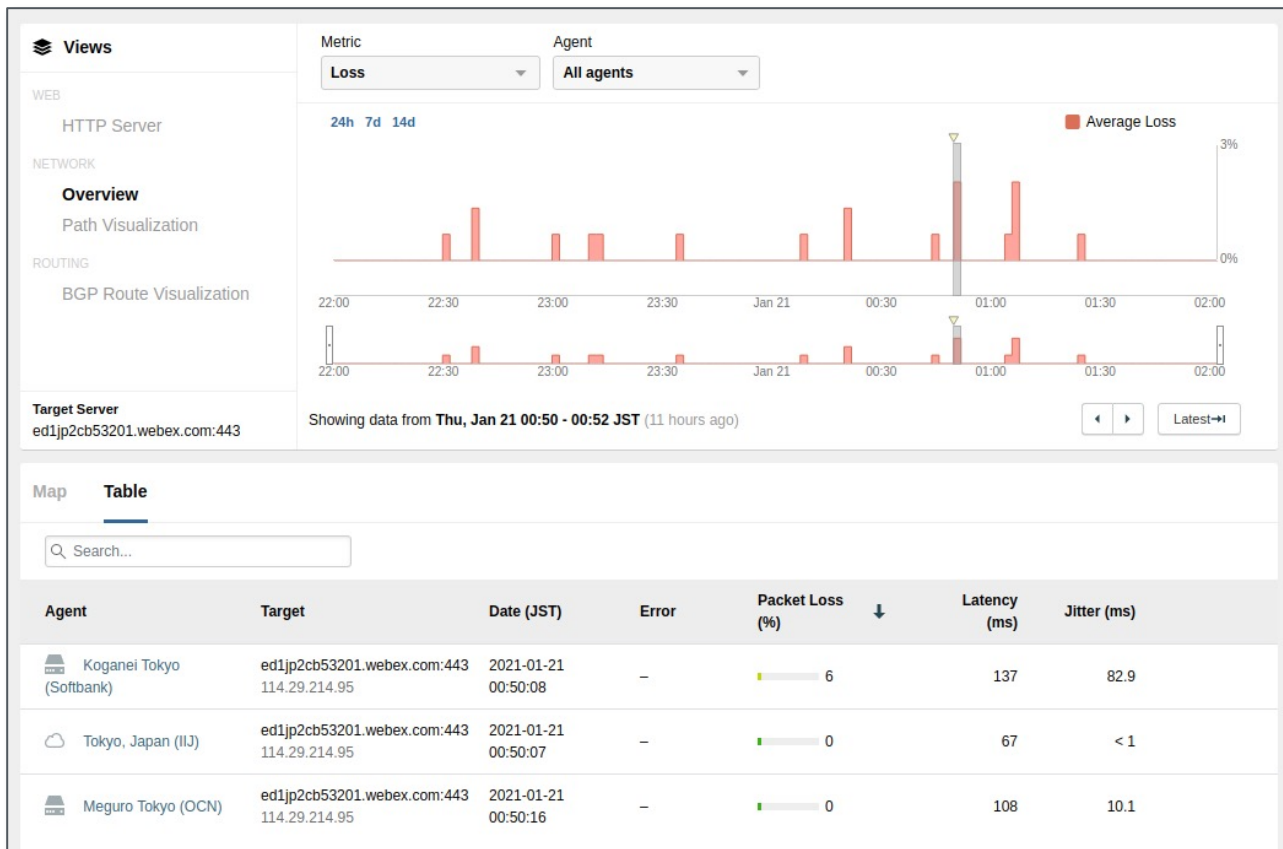


Webex DC内では
ICMPパケット
がブロックされている



国内 Collaboration Bridge の監視例

[共有リンク](#)



Webex監視テストの設定例：Multimediaサーバー

- メディアサーバーへのネットワークテストの基本設定

New Test

Layer: Routing Network DNS Web Voice

Test Type: Agent to Server Agent to Agent

Test Name: WebEx Media Server JP

Basic Configuration / Advanced Settings

Target: m06jpmcs201.webex.com

Protocol: TCP Port: 5004

Probing Mode: Prefer SACK Force SACK Force SYN

Path Trace Mode: In Session

Interval: 1 minute

Agents: 2 of 391 selected

監視対象のメディアサーバーのドメイン名

TCP ポート 5004

サーバーと接続したTCPセッション内での
End to Endのネットワーク品質測定を実行

社内Enterpriseエージェント+ Cloud エージェント

Webex監視テストの設定例：Multimediaサーバー

- メディアサーバーへのネットワークテストのアドバンス設定

The screenshot shows the 'Advanced Settings' tab for a network test configuration. It includes sections for 'Data Collection', 'Ping Payload Size', 'Transmission Rate', 'No. of Path Traces', and 'DSCP'. Red lines connect specific settings to explanatory text on the right.

Setting	Value / State	Annotation
Perform bandwidth measurements	<input type="checkbox"/>	
Perform MTU measurements	<input checked="" type="checkbox"/>	
Collect BGP data	<input checked="" type="checkbox"/>	BGPの経路データを取得する
Enforce fixed packet rate	<input checked="" type="checkbox"/>	サーバーに優しい送信レート
Transmission Rate	10 pps	
No. of Path Traces	5	
DSCP	EF (DSCP 46)	DSCPの設定 (EF, DSCP 46)

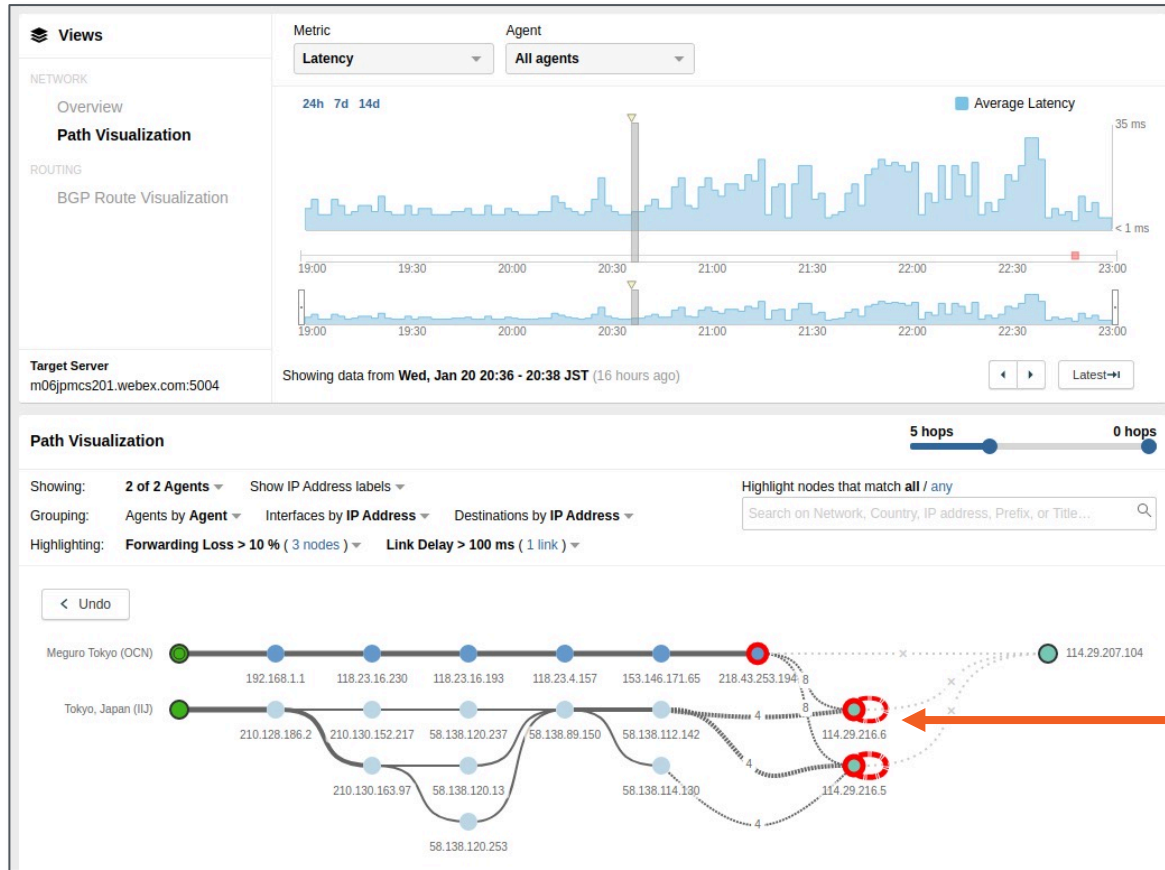
BGPの経路データを取得する

サーバーに優しい送信レート

DSCPの設定 (EF, DSCP 46)

国内 Multimedia サーバーの監視例

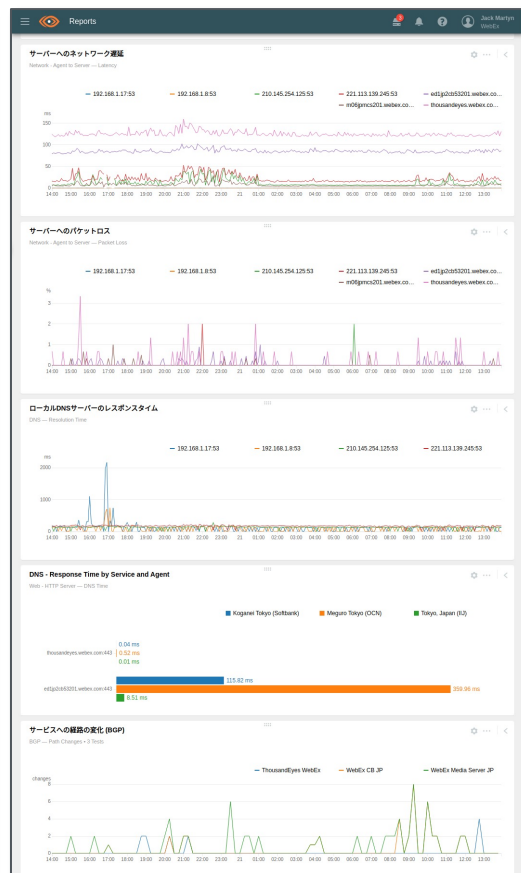
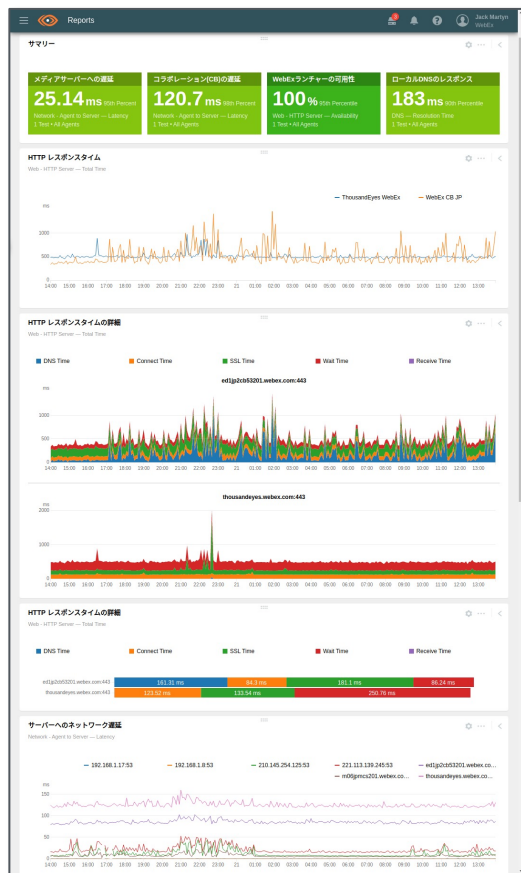
[共有リンク](#)



WebEx DCがICMPパケットをブロックしている

Webexの監視レポート例

共有リンク



オンラインビデオ会議の監視 Microsoft Teams





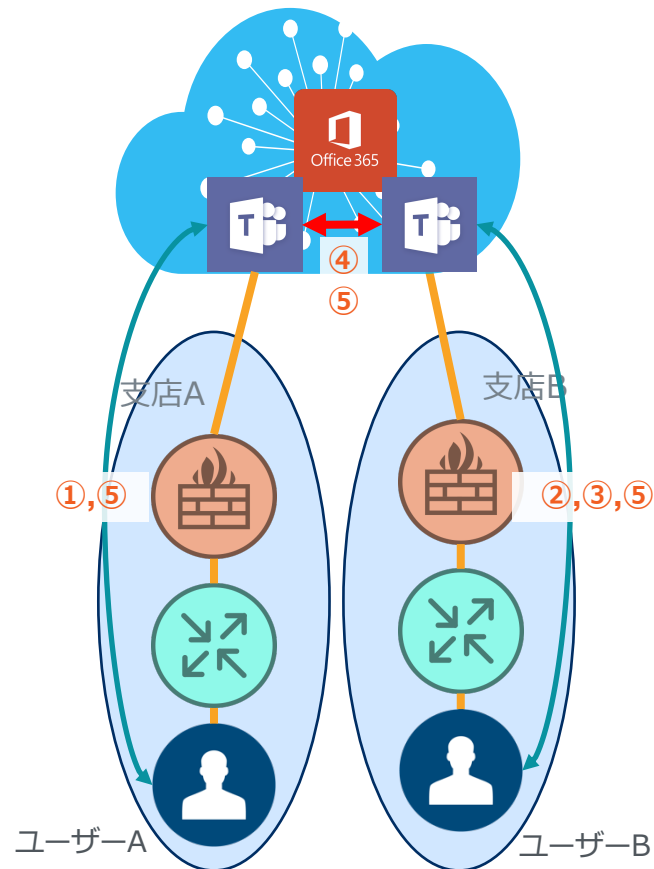
Microsoft Teams

- Teamsに対するMicrosoft社の推奨環境：
 1. プロキシやDPIなど遅延に影響する機器はバイパスする
 2. 自社ネットワークに一番近いMicrosoftエッジへのパスを使う
 3. ボイスやビデオのトラフィックにはUDPを使う
 4. DNSはローカルのネットワークで解決する
 5. 事前にOffice 365への遅延、ロス、ジッターや必要になる帯域などを測定・計算する

Teamsのコールフロー

• コールフロー

1. 社員AがOffice365のTeamsに接続 (TCP/443)、社員Bへの**通話の招待状**を送信
2. Office365のTeamsが社員Bに社員Aからの**通話招待**を通知
3. 社員BがOffice365のTeamsに接続 (TCP/443)、**通話の招待に回答**
4. 社員Aと社員BのTeamsが**直接接続の通信は不可**であることを検知、Office 365のTeamsの**トランスポートリレー**を使い接続する
5. Office 365のTeamsのトランスポートリレーを使った**会話の開始**



Teamsのエッジノード

- Teams の制御ノード
 - Teamsクライアントとコールのシグナリングを処理
 - <https://teams.microsoft.com>
 - IP Anycastで運用 (現在 52.113.194.131)
 - Office365のバックエンドとのコミュニケーション
- トランスポートリレー
 - world.tr.teams.microsoft.com, IP Anycast (現在 13.107.64.2)
 - カンファレンスのメディア通信を複数のユーザーにリレーする
 - UDP/3479 (音声), UDP/3480 (ビデオ), UDP/3481 (画面)
 - UDPの通信が最適。不可の場合はTCP/443にフォールバック
 - UDP/TCPやIPv4/IPv6のクライアントをブリッジ接続できる！

監視テストの内容

1. Teamsのエッジノードの監視

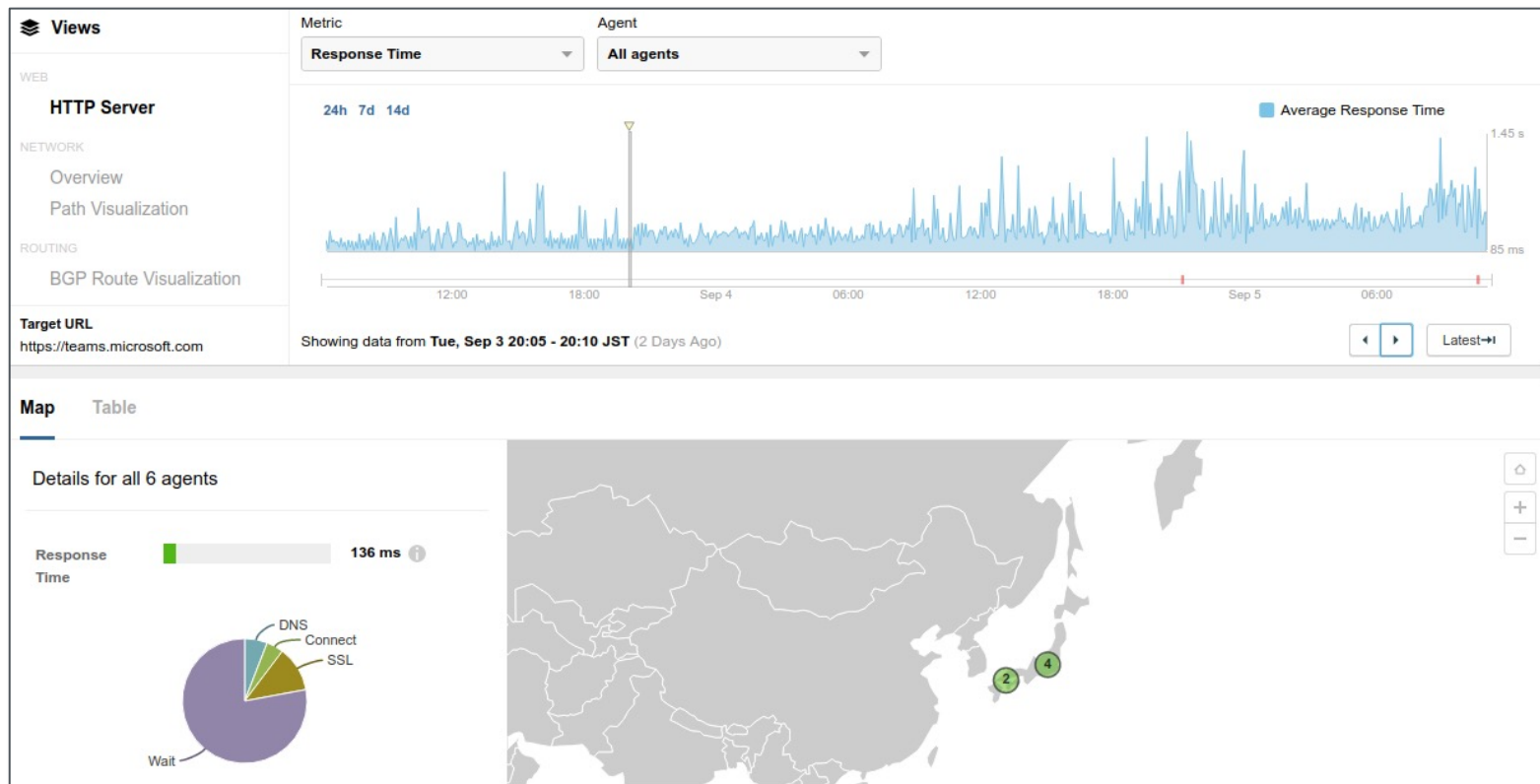
- 社内EnterpriseエージェントとCloudエージェントからHTTPテストを実行
- ターゲットは **https://teams.microsoft.com**
- テスト間隔は5分以内

2. トランスポートリレーの監視

- 社内EnterpriseエージェントとCloudエージェントからAgent to Server テストを実行
- ターゲットは **world.tr.teams.microsoft.com**、tcp/443
- テスト間隔は2分以内、DSCPの設定：音声は 46、ビデオなら 34

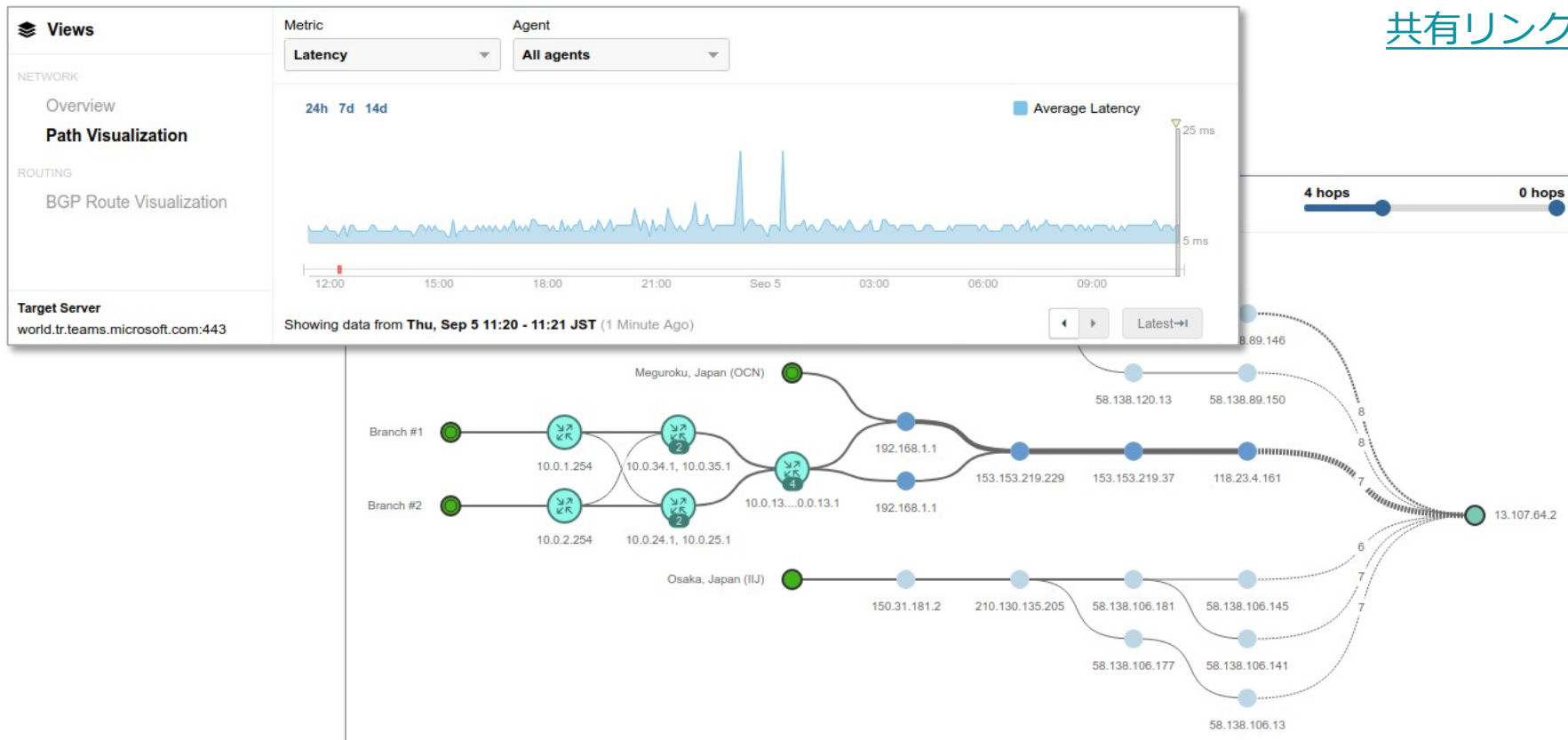
監視テストの実行例：Teamsのエッジノード

[共有リンク](#)



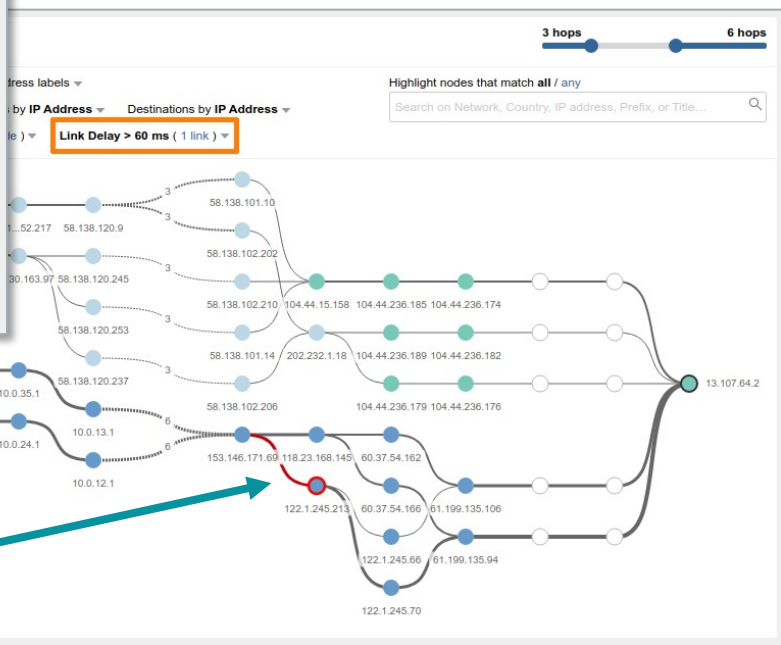
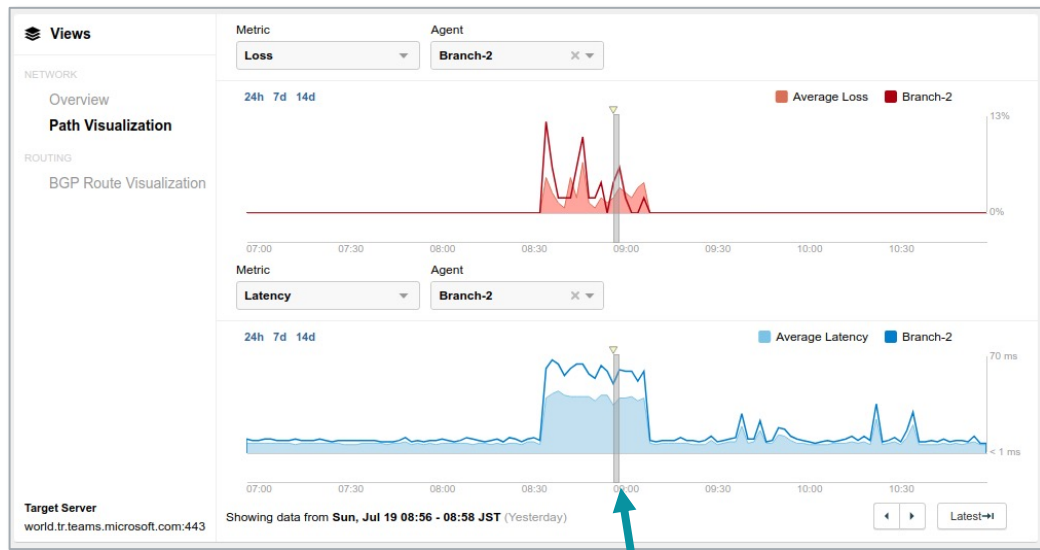
監視テストの実行例：トランスポートリレー (1)

[共有リンク](#)



監視テストの実行例：トランスポートリレーの障害 (2)

[共有リンク](#)



トランスポートリレーへの
ネットワークパス上のルーターにて
大きな遅延とロスが発生

MS Teams のアラート設定

- Teamsが正常に動作するためのネットワーク環境：

<https://docs.microsoft.com/ja-jp/microsoftteams/prepare-network>

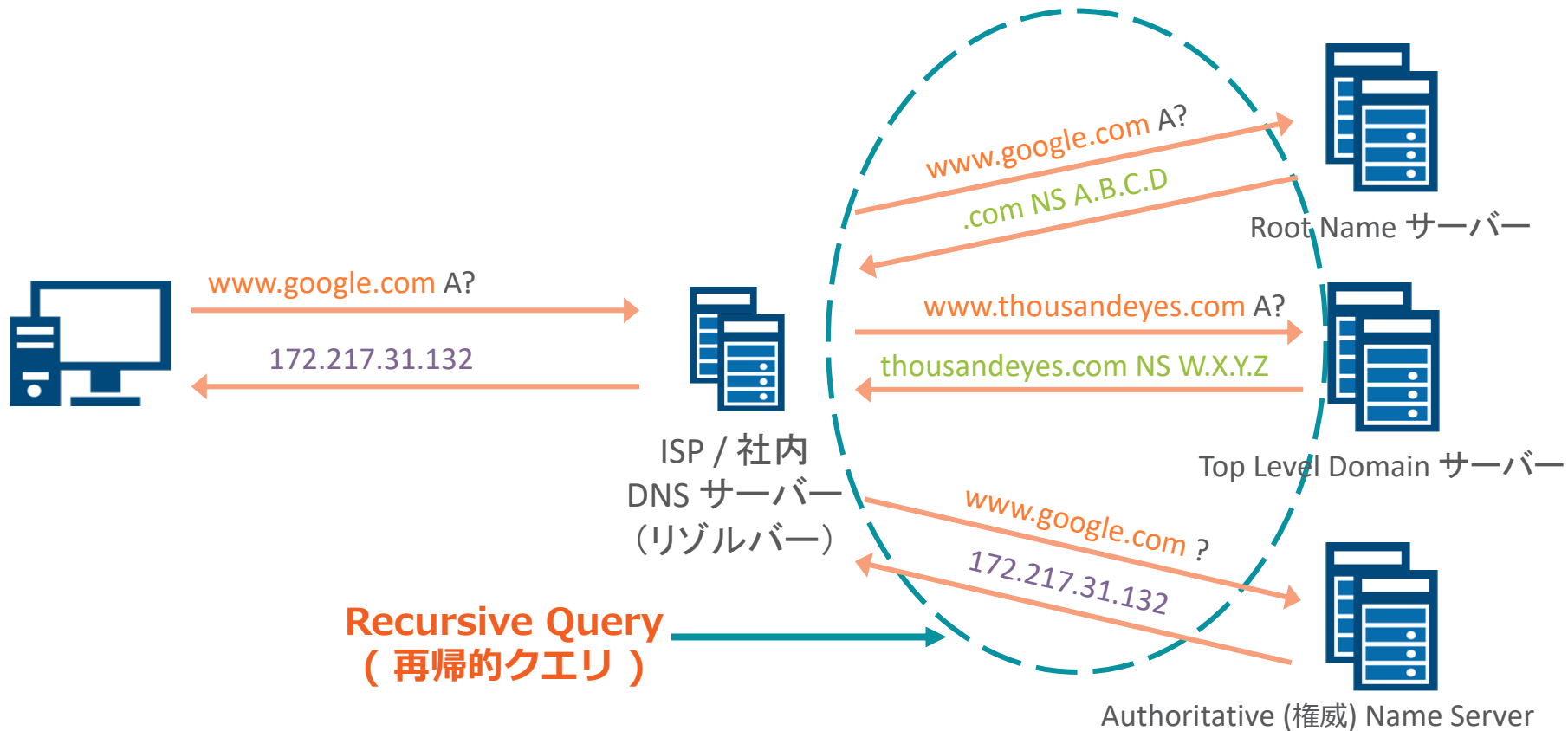
- 下のMicrosoftの推奨値を使い、**トランスポートリレー**の監視テストにアラートを設定：

監視データ	ThousandEyes のアラート設定	推奨値
遅延 (往復時間)	Network Latency	100 ミリ秒以下
パケット損失	Network Packet Loss	1% 以下
パケット到着間ジッター	Network Jitter	30 ミリ秒以下

DNS サービスの監視



DNSの基礎知識



DNS レコード

DNSに格納されている情報を「レコード」と呼ぶ。
レコードは格納する情報によって種類が分類分けされている。

監視テストによく使うDNSレコード：

Aレコード	ドメイン名からIPv4アドレス
AAAAレコード	ドメイン名からIPv6アドレス
PTRレコード	IPアドレスからドメイン名
NSレコード	DNSサーバーのドメイン名
MXレコード	メールサーバーのドメイン名
CNAMEレコード	ドメイン名の別名

DNSのアドレス解決 (Mac OS, Linux)

```
$ dig @8.8.8.8 outlook.office.com
```

8.8.8.8 (Google) のDNSリゾルバーに outlook.office.comのアドレス解決をリクエスト、以下はサーバーからのレスポンス

```
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 23367
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; QUESTION SECTION:
outlook.office.com. IN A
```

```
;; ANSWER SECTION:
```

```
outlook.office.com.      8      IN      CNAME   substrate.office.com.
substrate.office.com.   205    IN      CNAME   substrate.ms-acdc.office.com.
substrate.ms-acdc.office.com.  8      IN      CNAME   afd-k.office.com.
afd-k.office.com.      54     IN      CNAME   outlook-office-com.k-0002.k-
msedge.net.
outlook-office-com.k-0002.k-msedge.net.  48     IN      CNAME   k-0002.k-msedge.net.
k-0002.k-msedge.net.   48     IN      A       13.107.18.11
```

qr : サーバーからの回答

rd : 再帰的クエリの要求

ra : サーバーは再帰的クエリをサポート

DNS 監視テストのユースケース

サーバーの可用性 とレスポンスタイム

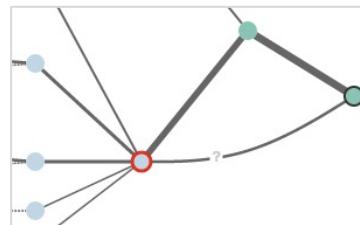
Details for ns1.google.com. from Cairo, Egypt

Status ■ **Error** Could not reach name server

データの正確性

Mapping not in dsn1.espn.com dsn2.espn.com

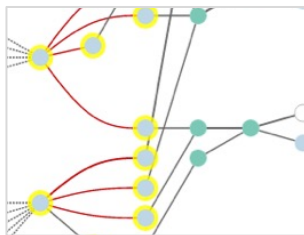
DNSサーバーへの ネットワークの品質



クエリーのトレース

Madrid, Spain	2016-01-11 10:30:03	■ Dead end for bairiki-monitor.coconutwireless.ki A
San Diego, CA	2016-01-11 10:30:29	■ Dead end for bairiki-monitor.coconutwireless.ki A
St. Louis, MO	2016-01-11 10:30:19	■ Dead end for bairiki-monitor.coconutwireless.ki A
Sydney, Australia	2016-01-11 10:30:02	■ Dead end for bairiki-monitor.coconutwireless.ki A
Philadelphia, PA	2016-01-11 10:30:30	■ Dead end for bairiki-monitor.coconutwireless.ki A

CDN/DNSの動作確認



DNSSECバリデーション

```
DNSKEY 257 3 8 AwEAAgAIIK1VZrj
3fLjwBd0YI0EzrAcQqBGCzh/RStIo08
96M/QZxkjf5/Efucp2gaDX6RS6CXpoY
2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sG
AmRLKBP1dfwhYB4N7knNnu1qQxA+Uk
```

DNSの運用管理者

DNSサーバーの種類	運用・管理者	監視の必要
ルートサーバー	VeriSign, NASA, Internet Systems Consortium, US Defence Agency, ICANN, WIDE Project, JPRS	X
トップレベルドメイン	ICANN/IANAとその配下の公式レジストラ	X
権威DNSサーバー	SaaS、IaaSや 自社のWebアプリ管理者	DNS Server テスト
社内DNSサーバー (ローカル IP アドレス、 DNS キャッシュ)	社内IT	DNS Server テスト

監視する必要あり

権威 DNS サーバーの監視



DNS サーバーの監視

- **権威DNSサーバーの監視内容**
 - **権威DNSサーバーの可用性**
 - 名前解決のレスポンスタイムの監視
 - 権威DNSサーバーへのネットワークパスの品質監視
 - 正しいIPアドレスのマッピングの確認（セキュリティ）
- **社内DNSサーバー**
 - 社内サーバーの可用性
 - **ユーザーが体験しているレスポンスタイムの監視**
 - ユーザーからDNSサーバーへのネットワークパスの品質監視
 - 正しいIPアドレスのマッピングの確認（セキュリティ）

権威DNSサーバーテストの設定

監視するドメイン名

Domain

e.g. google.com

実行間隔 (5~10分)

Interval

5 minutes

エージェント

Agents

0 of 136 agents selected

監視対象DNSサーバー

DNS Servers

ns2.google.com. x

ns1.google.com. x

2 more x

Lookup Servers

Alerts Enable

3 of 3 alert rules selected

Edit Alert Rules

Lookup Servers

を押すと、ターゲットドメイン名の
権威 DNS サーバーが自動入力される

レコードタイプ

A

AAAA

ANY

CNAME

DNSKEY

DS

MX

NS

NSE

NULL

PTR

RRSIG

SOA

TXT

権威DNSサーバーテストの設定

Basic Configuration | **Advanced Settings**

NETWORK

Data Collection Perform network measurements

- Perform bandwidth measurements
- Perform MTU measurements
- Collect BGP data

All public BGP monitors will be included

Protocol: TCP

Probing Mode: **Prefer SACK** | Force SACK | Force SYN

No. of Path Traces: Default (1)

Send recursive queries

DNSサーバーへのBGPの経路データの取得

再帰クエリ

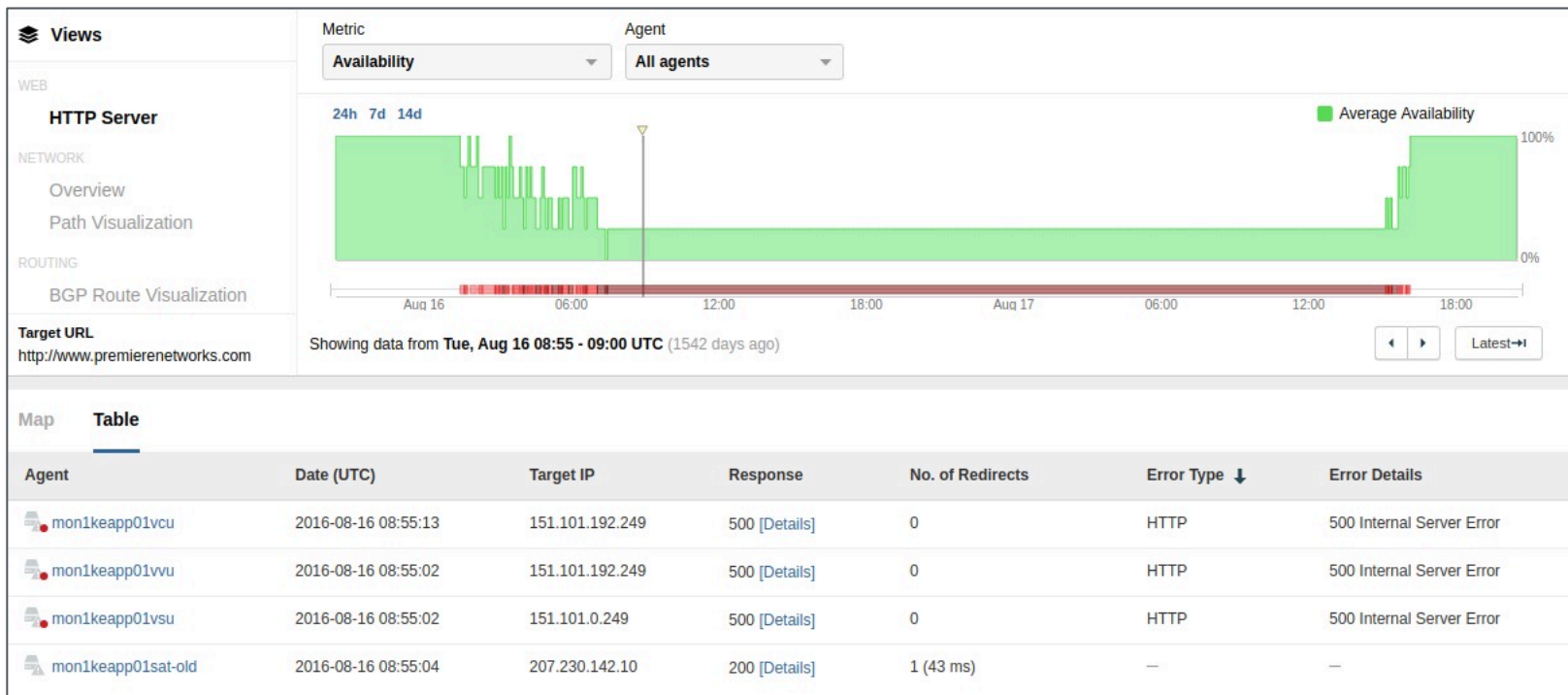
権威サーバーのテストでは無効に設定

権威DNSサーバーの監視例 (1)

CDNへのステアリングに問題

[共有リンク](#)

DNSを使いCDNに誘導された後、ホスティングされているべきWebサービスが無かった！

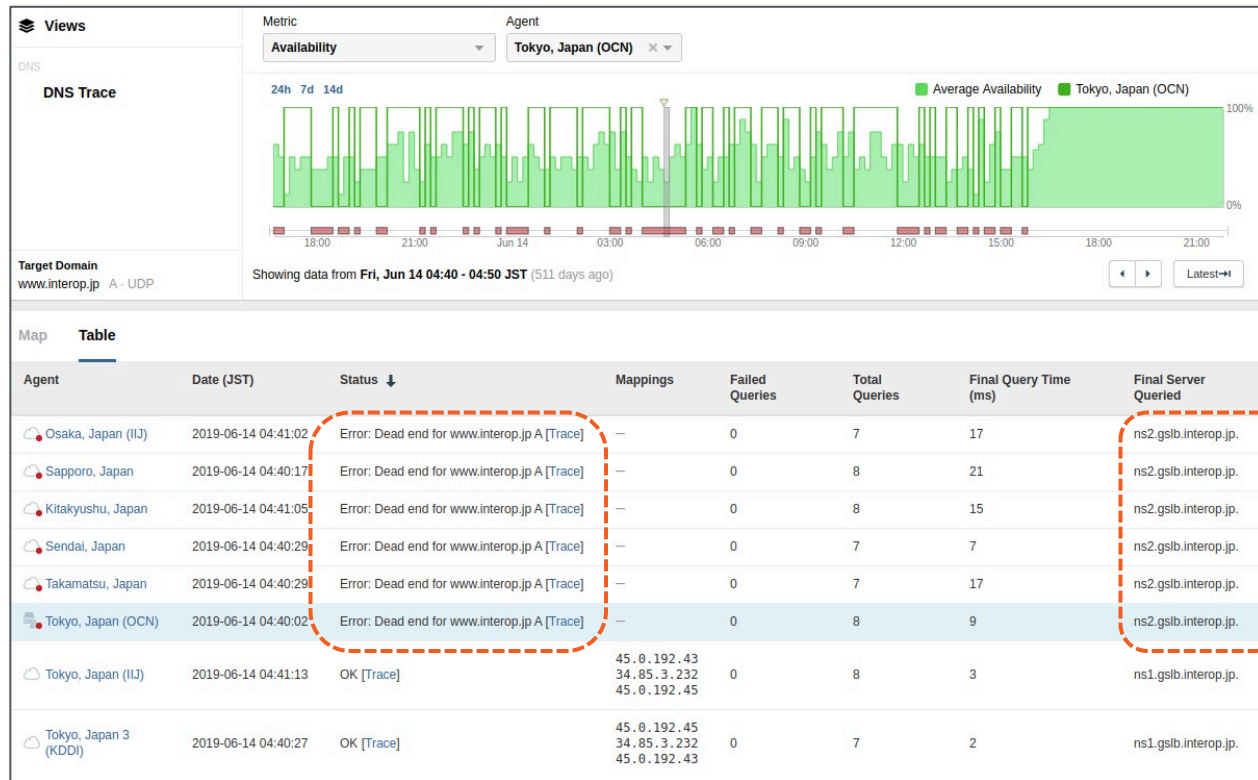


権威DNSサーバーの監視例 (2)

DNS Traceテストを使ったDNSサーバーの問題解析

[共有リンク](#)

ロードバランスされたDNSサーバーの1台 (ns2.gslb.interop.jp) の問題



社内 DNS サービスの監視



社内 DNS サーバーの設定

- 権威DNSサーバーの監視内容

- サーバーの可用性
- 名前解決のレスポンスタイムの監視
- サーバーへのネットワークパスの品質監視
- 正しいIPアドレスのマッピングの確認（セキュリティ）

- 社内DNSサーバー

- 社内サーバーの可用性
- ユーザーが体験しているレスポンスタイムの監視
- ユーザーからDNSサーバーへのネットワークパスの品質監視
- 正しいIPアドレスのマッピングの確認（セキュリティ）

Web アプリケーションの DNS 監視 社内 DNS サーバーテストの設定

監視するドメイン名

間隔 (2~5分)

社内Enterpriseエージェント

社内DNSサーバー

The screenshot shows a configuration interface with two tabs: "Basic Configuration" (active) and "Advanced Settings".

- Test Name:** Optional
- Domain:** ap0.salesforce.com, IN, A
- Interval:** 2 minutes
- Agents:** 8 of 326 agents selected
- DNS Servers:** 192.168.1.17 x, Q Lookup Servers
- Alerts:** Enable, 3 of 11 alert rules selected, Edit Alert Rules

Buttons at the bottom: Cancel, Run Once (i), Save Changes

DNSサーバーテストの設定

The screenshot shows the 'Advanced Settings' tab for a network configuration interface. Under the 'NETWORK' section, the 'Data Collection' area has several options: 'Perform network measurements' (checked), 'Perform bandwidth measurements' (unchecked), 'Perform MTU measurements' (checked), and 'Collect BGP data' (checked). Below these is the note 'All public BGP monitors will be included'. The 'Protocol' is set to 'TCP'. The 'Probing Mode' has three buttons: 'Prefer SACK' (selected), 'Force SACK', and 'Force SYN'. The 'No. of Path Traces' is set to 'Default (1)'. At the bottom, 'Send recursive queries' is checked.

DNSサーバーへのBGPの経路データ
社内サーバーのテストでは無効

再帰クエリ
DNSサーバーがリゾルバーなら有効

DNSのアラート設定

- 可用性とレスポンスタイム
 - サーバーの問題やレスポンスの劣化はアラートでリアルタイムに通知
- DNSハイジャックの検知
 - アタッカーがDNSのレスポンスに偽りのリソースレコードを埋め込む
 - 正常でないIPアドレスの解決を管理者にアラート

ALERT CONDITIONS

At least agent meets of the following conditions time in a row:

The screenshot shows a configuration window for alert conditions. The title is 'ALERT CONDITIONS'. The main text reads 'At least 1 agent meets all of the following conditions 1 time in a row:'. Below this, there is a list of conditions. The first condition is 'Mapping not in 10.0.10.10'. Each condition is in a separate box with a dropdown arrow on the left and a close button (x) on the right.

- DNSサーバーへのネットワークパス上のパケットロスを通知
- BGPのアラート：DNSサーバーへの経路の変化

DNSカスタムアラートの設定例

Settings Notifications

GENERAL

Rule Name

Tests

Agents

ALERT CONDITIONS

All conditions are met by at least agent of time in a row:

1回でもDNSのレスポンスが
AWSのIPブロックでなかったらアラートする

DNSサーバーからのレスポンスが3回に2回
1秒以上であったらアラートする

Settings Notifications

GENERAL

Rule Name

Tests

Agents

ALERT CONDITIONS

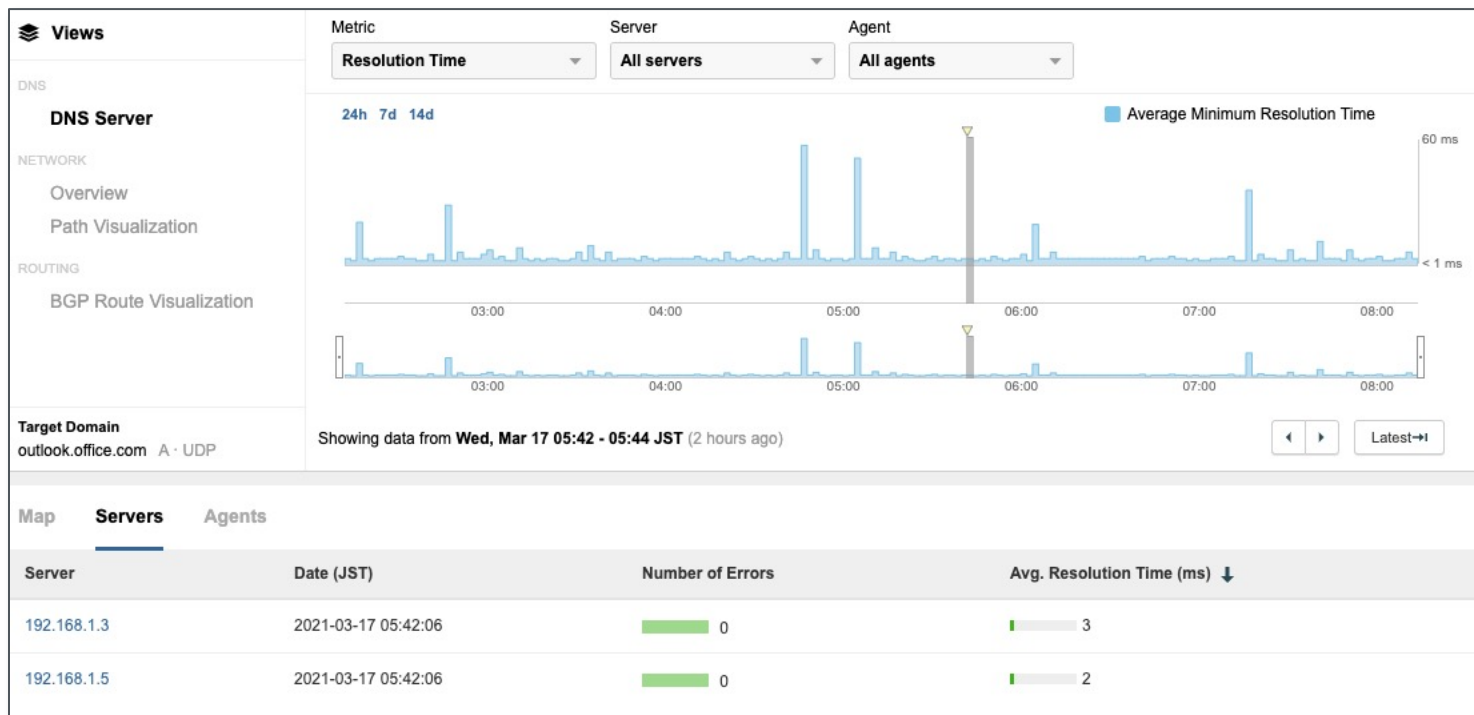
All conditions are met by at least agent of times in a row:

ms

社内DNSサーバーの監視例

社内DNSサーバーの可用性、レスポンスとネットワークパスの品質測定

[共有リンク](#)



インターネットにある サービスの経路監視 (BGP)



BGP 経路の可視化

- BGP Route Visualization は全ての監視テストの一部
- 監視テストのターゲットが属するIPプリフィックスがBGPでどのように変動しているか、世界100箇所以上のISPのルーティングテーブルデータから監視する。
 - 各ISPからのReachableであるか
 - インターネットのどこかでPath Changeが発生しているか
 - サービスのプリフィックスがハイジャックされてはいないか
 - サービスのプリフィックスがブラックホールされてはいないか
- 経路に異常があると管理者にアラートで通知
- BGPの経路データは Route Views Project から取得
 - <http://www.routeviews.org/routeviews/>

監視テストのBGPデータ監視設定

NETWORK

Data Collection Perform network measurements

Perform bandwidth measurements

Perform MTU measurements

Collect BGP data

All public BGP monitors will be included

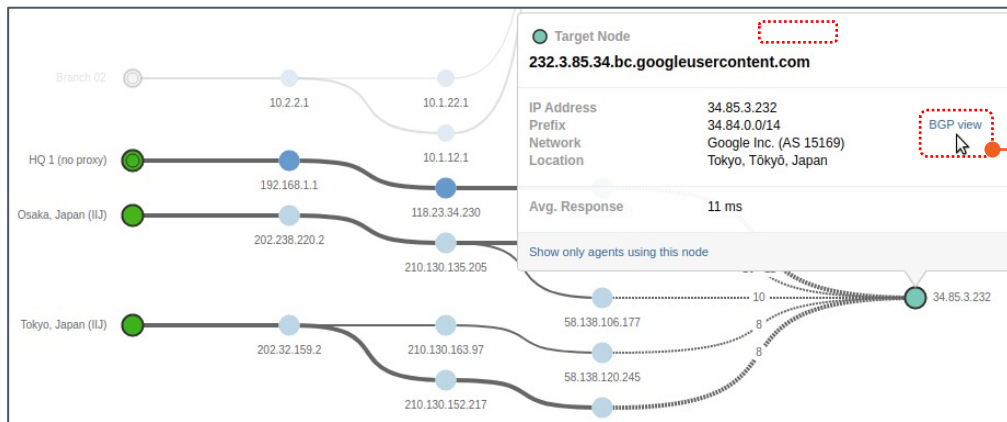
Protocol

Probing Mode

- 監視テストの [Advanced Settings > Collect BGP data](#) をチェックすれば監視しているサービスのIPプリフィックスが自動的に監視される。
- 設定した監視ターゲットがCDNのサービスを使うことで多数のIPアドレスにリゾルブされる場合、このオプションが外れることがあるが、強制的にチェックできる。

BGP 経路の可視化の使い方

- 監視ターゲットの経路を監視するサービスであり、巨大なIPアドレススペースを持つプロバイダーの経路を全て監視するような機能ではない。
- CDNを使ったサービスではロケーションによって異なるサーバー・IPにDNSで誘導される。正しいIPプリフィックスをUIで追いかけるには、Path Visualizationの画面からターゲットデータに表示される **BGP View** のリンクを使う：



ここをクリックすれば
追いかけやすい

(単独の) BGP 監視テスト

New Test

Layer **Routing** Network DNS Web Voice

Test Type **BGP**

Test Name

Test Description

Basic Configuration

Prefix

Include covered prefixes

All public BGP monitors will be included

Alerts Enable

1 of 1 alert rules selected

指定したプリフィックスに
含まれるサブネットの監視
(/19~/23 まで)

監視するプリフィックス
(CIDR表記)

アラートの設定

BGPの可視化：記号の意味



Public/Private BGP モニター
ターゲットの経路情報あり



視覚化のために簡略化されたパス。
数字は隠れたASホップを表す。
クリックしてパスを展開。



Public/Private BGP モニター
ターゲットの経路情報がない



BGPピアリングを通過する
経路の数を回線の太さで示す



トランジットAS
中央にASNを表示



ターゲットのプリフィックスが
消去された



ターゲットのOrigin AS
中央にASNを表示



ターゲットのプリフィックスが
新しくアナウンされた

ThousandEyesを使った Office 365 の (BGP) 障害解析例



2019年11月20日 障害発生

「Microsoft 365」で障害発生 「Teams」「Skype」 など利用しづらい状況 アップデートが影響か

2019年11月20日 12時15分公開

ITmedia



印刷



179



Share



5



米Microsoftは11月20日午前10時53分（日本時間）、「Microsoft 365」に含まれる複数のクラウドサービスが利用しづらい障害が発生していると発表した。最近行ったネットワークアップデートが影響している可能性があるという。

- 「Microsoft 365」の障害が解消 「Teams」など全サービス復旧

Microsoft 365 Status @MSFT365Status · 2019年11月20日
We're investigating an issue preventing access to Microsoft 365 services. We'll provide additional details shortly on status.office.com.

Microsoft 365 Status
@MSFT365Status

We've identified that multiple Microsoft 365 services are affected and we're actively looking for the swiftest means of restoring access. Please refer to status.office.com for details, or MO196220 in the admin portal, if accessible.

♡ 233 10:53 - 2019年11月20日

🗨️ 298人がこの話題について話しています

該当するサービスは「Exchange Online」「SharePoint Online」「Microsoft Teams」「Skype for Business」「Yammer」など。

Microsoft 365のユーザー管理や契約形態の変更ができる管理者向けツール「Microsoft 365 Admin Center」も利用しづらい状況になっている。

The screenshot shows the Microsoft 365 Service health status page. The title is "Microsoft 365 Service health status". The title of the issue is "Microsoft 365 admin center access issue". The start time is "November 20, 2019, at 1:26 AM UTC". The next update is scheduled for "November 20, 2019, at 4:00 AM UTC". The more info section states: "We've identified that users may intermittently experience this problem with the Microsoft 365 admin center, Exchange Online, SharePoint Online, Office Online, Microsoft Teams, Skype for Business, and Yammer." The current status section states: "We've identified that a recent networking update may have caused user traffic coming from the internet to fail intermittently before reaching Microsoft 365 services. We've reverted this update and are seeing some initial signs of mitigation. We're continuing to validate the cause of the problem while we monitor the environment for service recovery." There is a link to "View your Microsoft 365 Service health".

米Microsoftによる発表

同社は「最近のネットワークアップデートが、ユーザーのアクセス失敗に影響している可能性がある。当社はこの更新を元に戻したので、サービスは回復の傾向がみられる。今後も問題の原因を検証し続ける」と説明している。

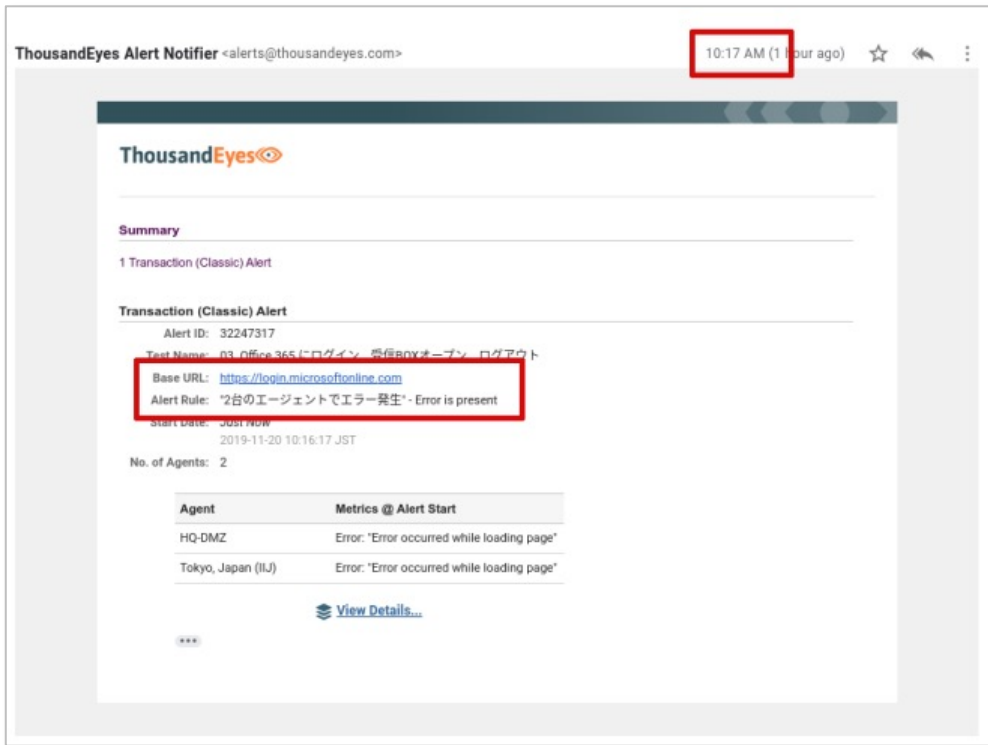
すでに復旧済みだが、19日には日本、インド、オーストラリアなどで「Office 365」のメール機能が利用しづらい障害が発生していた。

Copyright © ITmedia, Inc. All Rights Reserved.

<https://www.itmedia.co.jp/news/articles/1911/20/news088.html>

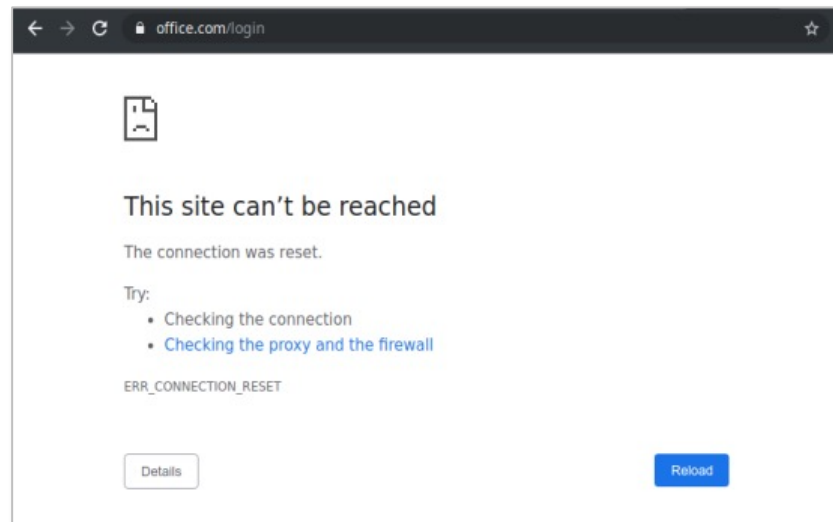


障害発生直後にアラート通知 (2019年11月20日)



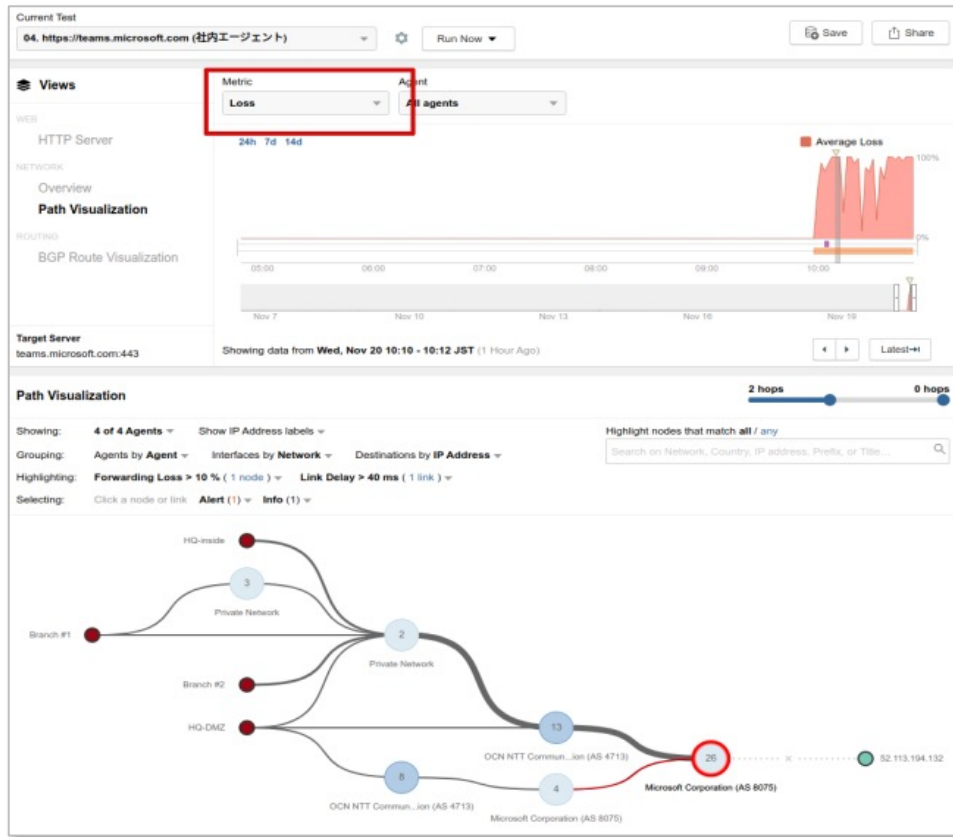
メールでアラート通知

[共有リンク](#)



実際ブラウザーのアクセスも不可

Office 365 の障害解析 (2019年11月20日)



10:00am

TeamsやOutlookへの通信でMicrosoft社のネットワーク内で**ほぼ100%のパケットロス**が発生

10:00am

障害が発生する直前に Microsoft社のサービスが属する複数のネットワークへの**経路の変動**を確認

11:30am

日本国内のTeamsへの経路と**サービスの復旧**

今回の障害は、Microsoft社のBGPルーティングの問題が原因で複数のサービスに影響を及ぼしたと考察

【共有リンク】

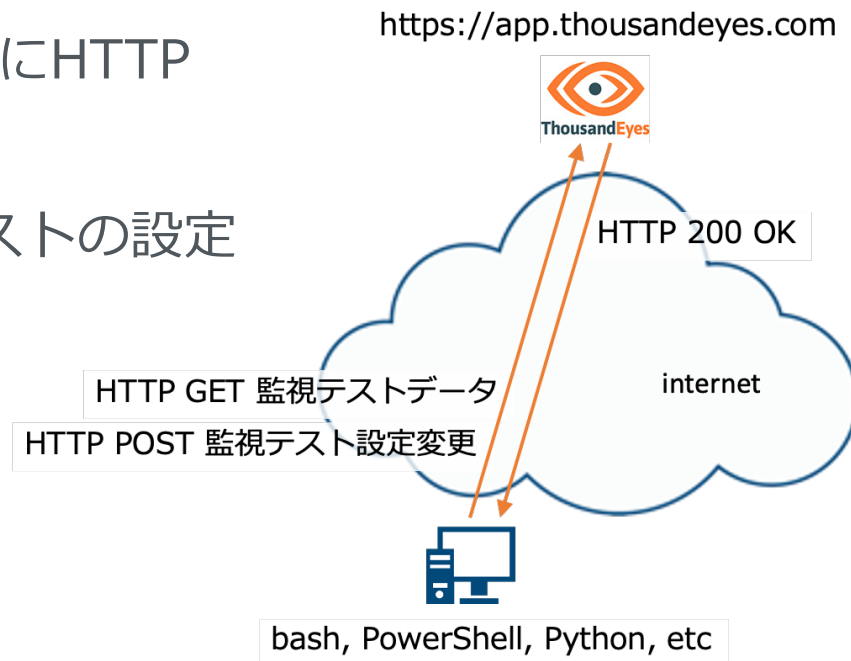
<https://cmkyaz.share.thousandeyes.com/>

ThousandEyes API



ThousandEyesのAPI

- RESTful API
- アプリケーションからAPIのURIにHTTP GET/POSTの通信を実行
- 監視データの読み取りや監視テストの設定変更が可能



ThousandEyes APIのユースケース

- 同じオペレーションを多数繰り返して実行する際
 - 監視ターゲットだけが違う監視テストをExcelファイルから数百個設定
 - APIを使いテンプレート化された複雑なレポートを自動設定
- 自動運用
 - アラートで障害を検知した時、自動にスナップショットを保存
 - 外部アプリと連携、監視テストの自動作成と設定変更

APIのオンラインマニュアル

<https://developer.thousandeyes.com/>

ThousandEyes

DEVELOPER REFERENCE

- Overview
- Instant tests
- Tests
 - Test list
 - Test list by type
 - Test details
 - Test metadata
 - Creating a test
 - Updating a test
 - Deleting a test
 - Saved events
- Test Data
- Credentials
- Endpoint Agents
- Endpoint Data
- Endpoint Scheduled Tests
- Endpoint Scheduled Test Data
- Endpoint Instant Tests

Example

Please note, test creation/modification/deletion is not allowed on the Sandbox API account, and will not work if attempted. The following example is presented for documentation and reference purposes only.

```
$ curl -i https://api.thousandeyes.com/v6/tests/agent-to-server/new.json \
-d '{ "interval": 300,
      "agents": [
        {"agentID": 113}
      ],
      "testName": "API agent-to-server test addition for www.thousandeyes.com",
      "server": "www.thousandeyes.com",
      "port": 80,
      "alertsEnabled": 0
    }' \
-H "Content-Type: application/json" \
-H "Accept: application/json" \
-u noreply@thousandeyes.com:g351mw5xqhvkmh1vq6zfm51c62wyzib2
```


Header

```
HTTP/1.1 201 CREATED
Server: nginx
Date: Mon, 09 May 2016 16:04:24 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Organization-Rate-Limit-Limit: 240
X-Organization-Rate-Limit-Remaining: 228
X-Organization-Rate-Limit-Reset: 1492608660
Strict-Transport-Security: max-age=31536000
X-Server-Name: 1-2
```

For more information on our HTTP response status codes, see the [response status codes documentation](#).

Updating a test **POST** /v6/tests/{testType}/{testId}/update

Updates a test in ThousandEyes, based on properties provided in the POST data. In order to edit a test, the user attempting the creation must be an Account Admin, and the target test cannot be a live share or saved event.

 © 1992–2020 Cisco Systems, Inc. All rights reserved.

100

APIとの認証に必要なデータ

Account Settings > Users and Roles

Profile Roles Users Account Groups

User Profile

Name Jack Martyn

Email **jmartyn+japan@thousandeyes.com**

YOUR ACCESS

Organization	Account Group	Roles
ThousandEyes Japan (Demo)	All Account Groups	Organization Adm

Login Account Group Google Meet

TIME ZONE

Web Interface Default (JST)

User API Tokens

The user tokens associated with the Jack Martyn (jmartyn+japan@thousandeyes.com) profile.

Basic Authentication Token **gadjv8yhw3r4[redacted]8zp4v7f4l**

This token should be used along with your username

ユーザー名
(ログインに使ったメールアドレス)

API トークン

Q&A タイム



ThousandEyes 

Thrive in a connected world™

ThousandEyes is
now part of Cisco.

