Deployment Guide

GIGA スクール構想対応ネットワーク ソリューション

学校からの広帯域通信のブレイクアウト（SD-WAN）設定ガイド

- NHK for School ビデオコンテンツ
- YouTube
- ビデオ会議システム (Zoom)

Version 1.01 2020 年 4 月

免責事項

目次

1.はじめに

この設定ガイドは、GIGA スクール構想において利用が想定されている広帯域通信(NHK for School・YouTube・ビデオ会議システム)を、インターネットブレイクアウトする方法について解説します。

インターネットブレイクアウトとは複数の WAN 回線を用意し、特定のトラフィックの通信経路を制御（例：特定のトラフィックのみ安価な WAN 回線を利用する、など）して、拠点から直接インターネットへ通信させる機能です。クラウドアプリケーションの利用による、ネットワークリソースのひっ迫を FortiGate の機能を用いて低減させることが目的で利用されます。本ガイドでも２つの WAN 回線が存在することを前提にしています。

1.1. 利用機器と OS/ソフトウェアバージョン

FortiGate	FortiGate-VM	Version 6.2.3
FortiGate	ISDB	Version 7.00702

1.2. 構成

物理構成

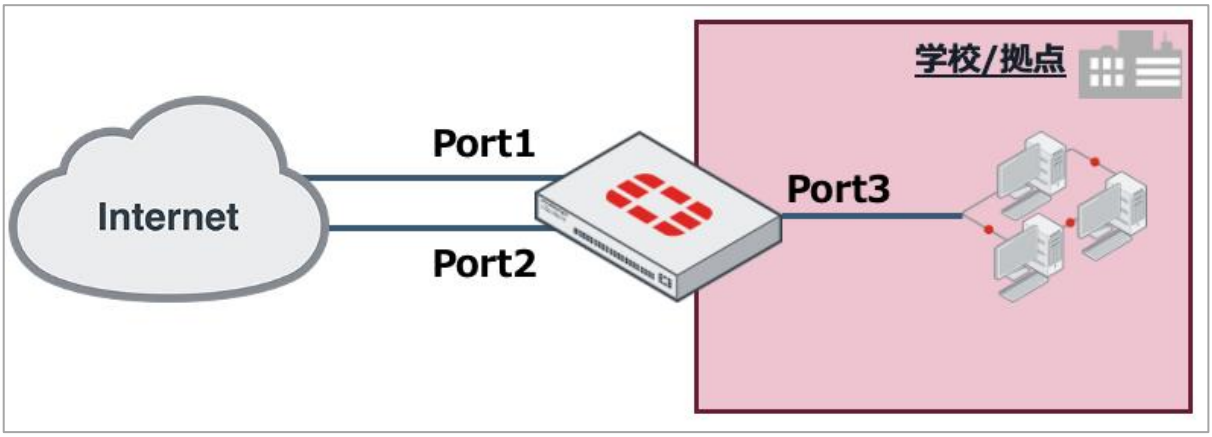

図 *1-1* 物理構成図

論理構成

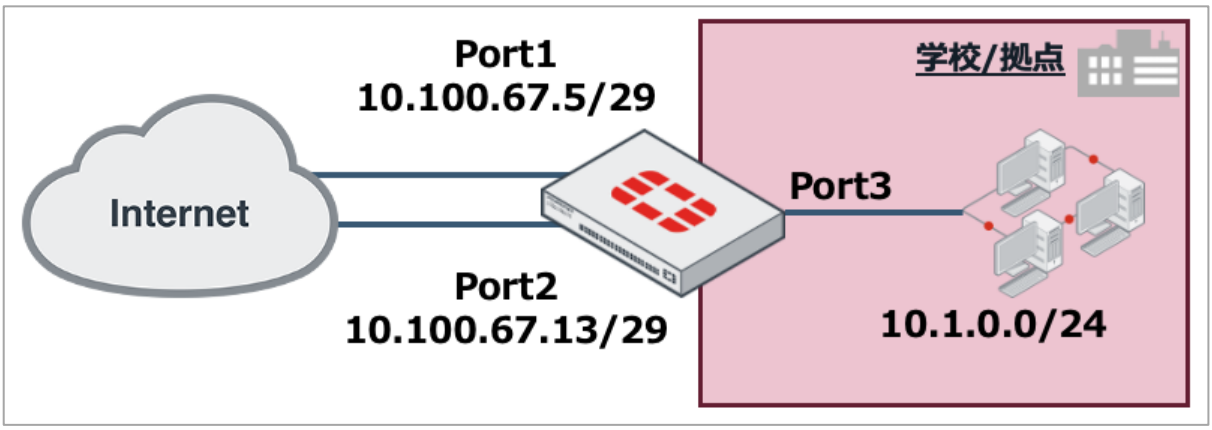

図 *1-2*　論理構成図

インターネットブレイクアウト構成

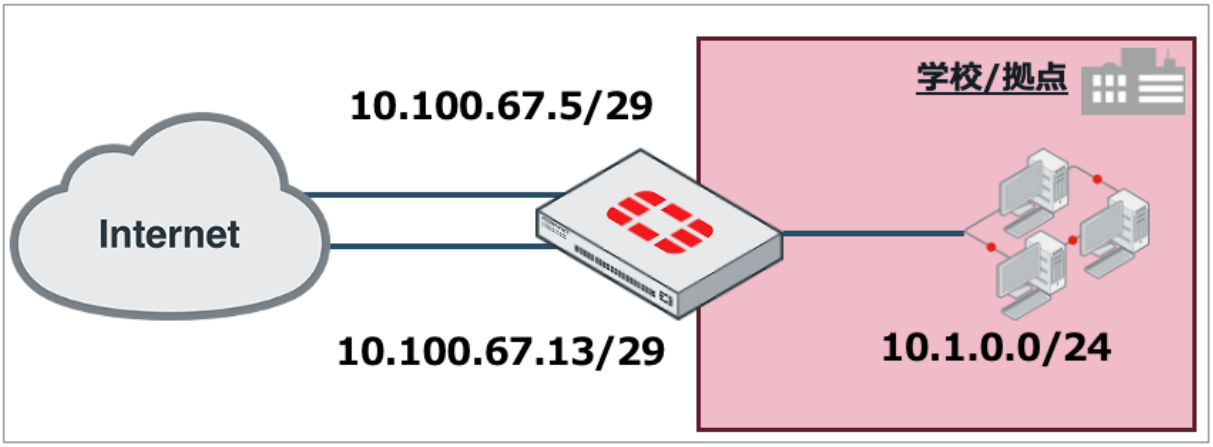

図 *1-3*　インターネットブレイクアウト構成図

1.3.　参照資料

本設定ガイドで紹介している設定は公式な設定ガイドに基づいています。より詳細な情報が必要な場合は以下も合わせてご参照ください。

FortiGate / FortiOS 6.2.3 Cookbook SD-WAN

https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/19246/sd-wan

2.インターネットブレイクアウト対象通信

本設定ガイドでは、GIGA スクール構想で使用される可能性が高い 3 つのトラフィックをインターネットブレイクアウトの対象とします。

1.1. NHK for School

NHK が提供する、学校放送番組やウェブサイトなど学校向けサービス。

1.2. YouTube

Google が提供する世界最大の動画共有サービス。

1.3. ビデオ会議システム（Zoom）

遠隔授業を実施するためのリアルタイムメッセージングとコンテンツ共有が可能なビデオ会議システム。

* 本ガイドでは代表例として Zoom の設定方法を記載します。

3. NHK for School ドメインの登録

NHK for School は FortiGate の ISDB（インターネットサービスデータベース：インターネット上のサービスと IP アドレス、ポート情報を紐付けた Fortinet 独自のデータベース）に登録されていないため、手動でアドレスオブジェクトを作成します。NHK for School のビデオコンテンツは以下をソースとしています。

nhks-vh.akamaihd.net

nhk-vh.akamaihd.net

この二つの FQDN を登録し、アドレスリストやスタティックルートに表示されるように設定します。

* 上記は 2020/4/1 時点の情報をもとに作成しています。

3.1. nhks-vh.akamaihd.net の設定

左メニュー「ポリシー＆オブジェクト」→「アドレス」をクリックし、「新規作成」→「アドレス」をクリックし、ドメイン情報を入力します。

名前：NHK1

カラー：任意

タイプ：FQDN

FQDN：nhks-vh.akamaihd.net

インターフェース：any

Show in address list：有効

Static route configuration：有効

コメント：任意

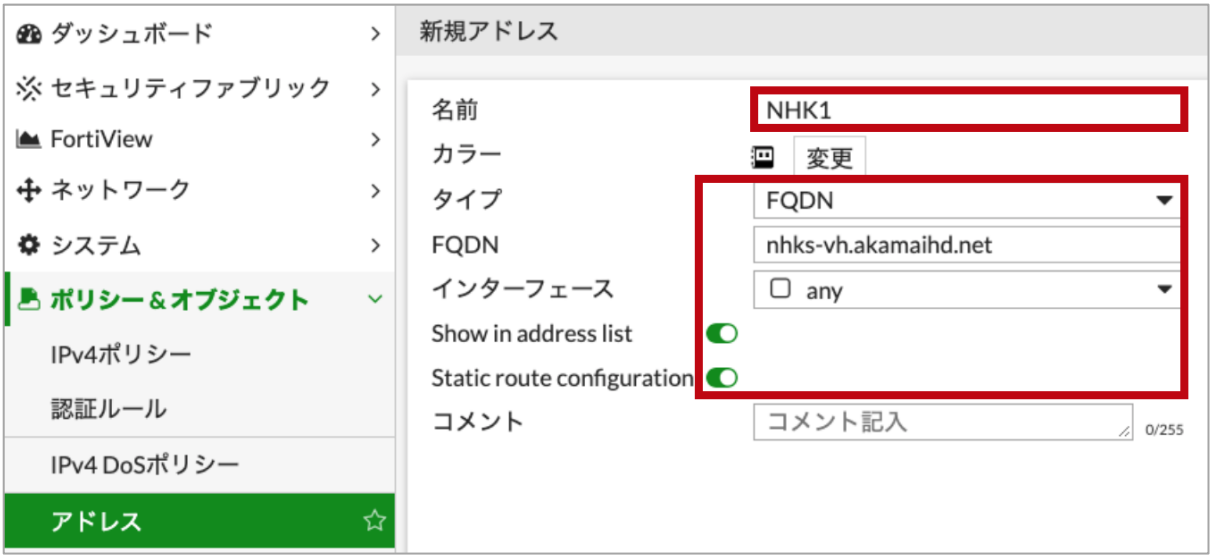

図 *3-1　nhks-vh.akamaihd.net* 設定

3.2. nhk-vh.akamaihd.net の設定

左メニュー「ポリシー＆オブジェクト」→「アドレス」をクリックし、「新規作成」→「アドレス」をクリックし、ドメイン情報を入力します。

名前：NHK2

カラー：任意

タイプ：FQDN

FQDN：nhk-vh.akamaihd.net

インターフェース：any

Show in address list：有効

Static route configuration：有効

コメント：任意

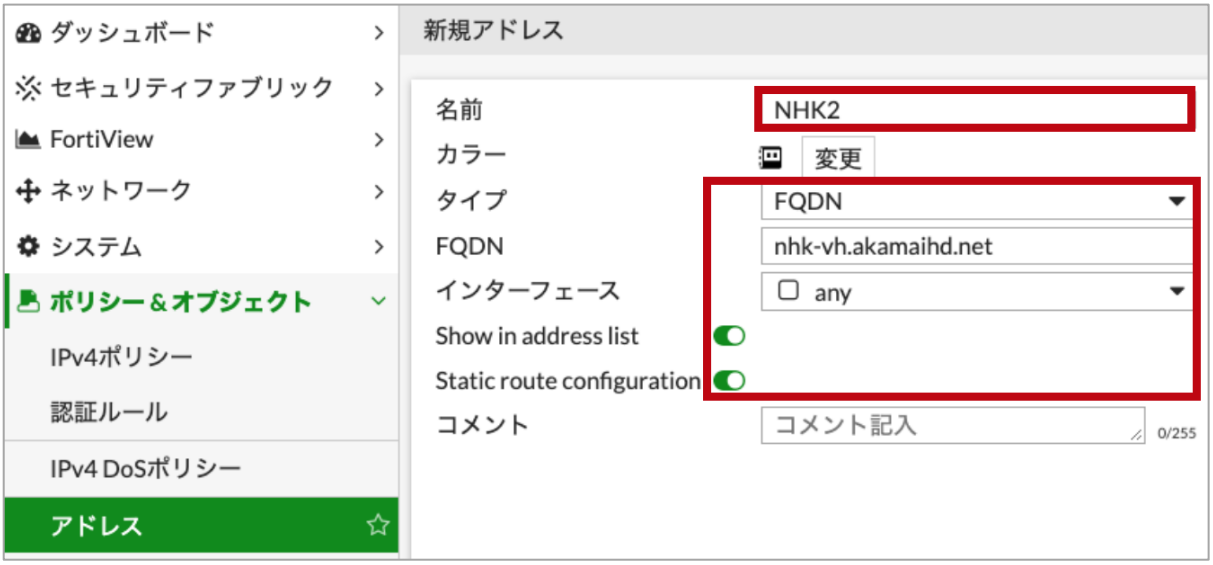

図 *3-2　nhk-vh.akamaihd.net* 設定

3.3. 確認

左メニュー「ポリシー＆オブジェクト」→「アドレス」をクリックします。作成したアドレスにマウスオーバーすることで FQDN から引いた IP アドレスを確認可能です。

* 正引きされる IP アドレスは環境やタイミングにより変わる可能性があります。GUI に表示されている IP アドレスは一例であり、必ずしも同一の IP アドレスになるわけではありません。

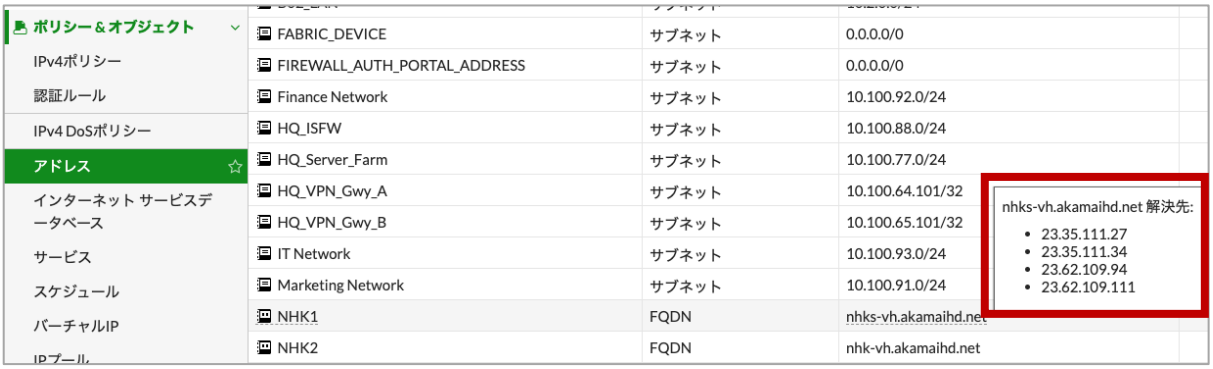

図 *3-3　nhks-vh.akamaihd.net の IP アドレス確認*

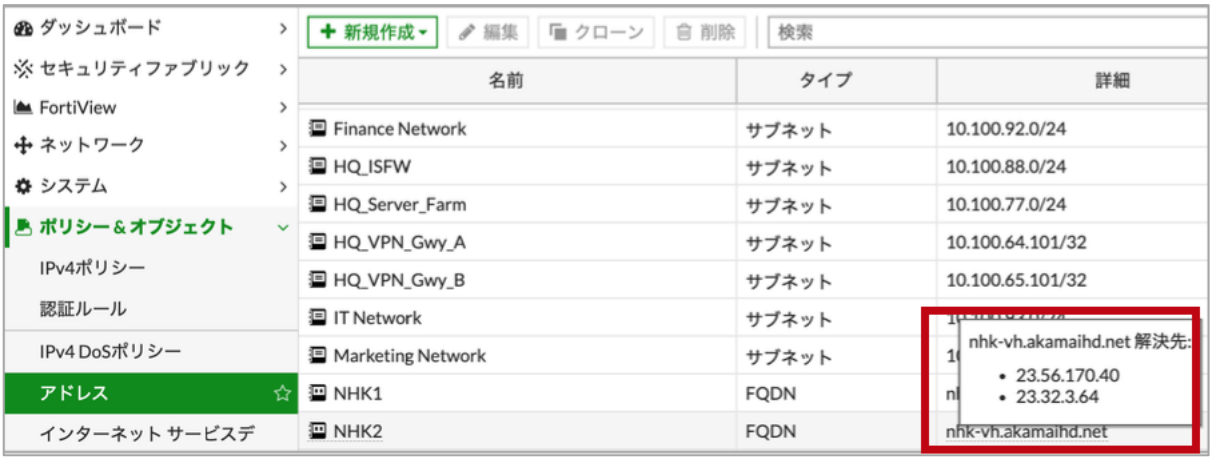

図 *3-4　nhk-vh.akamaihd.net の IP アドレス確認*

4. SD-WAN ルールによるインターネットブレイクアウト

4.1. SD-WAN インターフェースの設定

左メニュー「ネットワーク」→「SD-WAN」をクリックし、「有効」をクリックします。

図 *4-1　SD-WAN* 設定

次に「新規作成」をクリックし、SD-WAN インターフェースメンバーの設定を行います。

インターフェース：port1

ゲートウェイ：0.0.0.0

* 動的にデフォルトゲートウェイを取得する場合は 0.0.0.0 を設定します。

コスト：任意　　（例. 0）

ステータス：有効

図 *4-2　SD-WAN* 設定 *(port1)*

続いて、2 つ目のインターフェースの設定を行います。

インターフェース：port2
ゲートウェイ：0.0.0.0
* 動的にデフォルトゲートウェイを取得する場合は 0.0.0.0 を設定します。
コスト：任意　　（例. 0）
ステータス：有効

図 *4-3　SD-WAN* 設定 *(port2)*

2 つのインターフェースを登録できたことを確認し、「適用」をクリックします。

4.2. NHK for School の SD-WAN ルールの設定

左メニュー「ネットワーク」→「SD-WAN ルール」をクリックし、「新規作成」をクリックします。

名前：GIGA_School_NHK
送信元アドレス：all
ユーザグループ：選択しない
アドレス：NHK1, NHK2
プロトコル番号：ANY
インターネットサービス：選択しない
アプリケーション：選択しない
ストラテジー：マニュアル
　→基本的に優先するインターフェースでのみ通信を行います。優先するインターフェースがダウンした場合は、他の SD-WAN インターフェースで通信を行います。
優先するインターフェース：port2
ステータス：有効

図 *4-4　SD-WAN ルール設定 (NHK for School)*

4.3. Zoom、YouTube の SD-WAN ルールの設定

左メニュー「ネットワーク」→「SD-WAN ルール」をクリックし、「新規作成」をクリックします。

名前：GIGA_School_Zoom_YouTube
送信元アドレス：all
ユーザグループ：選択しない
アドレス：選択しない
インターネットサービス：”Zoom.us-Zoom.Meeting”
　→Zoom の他のサービスもブレイクアウトしたい場合は、該当サービスを選択します。
　* ISDB のバージョンによっては、インターネットサービスで指定するオブジェクトが変更になる場合があります。本設定ガイドでは ISDB Version 7.00702 を利用しているため”Zoom.us-Zoom.Meeting”を指定します。
アプリケーション：”YouTube”
　→YouTube の全ての通信をブレイクアウトさせる場合は”YouTube”を選択します。
ストラテジー：マニュアル
　→基本的に優先するインターフェースでのみ通信を行います。優先するインターフェースがダウンした場合は、他の SD-WAN インターフェースで通信を行います。
優先するインターフェース：port2
ステータス：有効

図 *4-5　SD-WAN* ルール設定 *(Zoom、YouTube)*

4.4. 通常トラフィックの SD-WAN ルールの設定

左メニュー「ネットワーク」→「SD-WAN ルール」をクリックし、「新規作成」をクリックします。

名前：All
送信元アドレス：all
ユーザグループ：選択しない
アドレス：all
インターネットサービス：選択しない
アプリケーション：選択しない
ストラテジー：マニュアル
　→基本的に優先するインターフェースでのみ通信を行います。優先するインターフェースがダウンした場合は、他の SD-WAN インターフェースで通信を行います。
優先するインターフェース：port1
ステータス：有効

図 *4-6　SD-WAN* 設定 *(*通常トラフィック*)*

4.5. SD-WAN インターフェース向けスタティックルートの設定

左メニュー「ネットワーク」→「スタティックルート」をクリックし、「新規作成」をクリックします。

ダイナミックゲートウェイ：無効

宛先：サブネット → 0.0.0.0/0.0.0.0

インターフェース：SD-WAN

アドミニストレーティブ・ディスタンス：10

＊ 10 を設定すると、SD-WAN インターフェースではアドミニストレーティブ・ディスタンス値は 1 が設定されます。

コメント：任意

ステータス：有効化済み

図 *4-7　SD-WAN* インターフェース向けスタティックルート設定

4.6. IPv4 ポリシーの設定

左メニュー「ポリシー＆オブジェクト」→「IPv4 ポリシー」をクリックし、「新規作成」をクリックします。

名前：GIGA_School
着信インターフェース：port3
発信インターフェース：SD-WAN
送信元：all
宛先：all
スケジュール：always
サービス：ALL
アクション ACCEPT
インスペクションモード：任意　（例. フローベース）
NAT：任意　（例. 有効）
IP プール設定：任意　（例. 発信インターフェースのアドレスを使用）
送信元ポートの保持：任意　（例. 無効）
プロトコルオプション：default
アンチウイルス：任意　（例. 無効）
Web フィルタ：任意　（例. 無効）
DNS フィルタ：任意　（例. 無効）
アプリケーションコントロール：有効 → default
　→デフォルトのプロファイルは全アプリケーションがモニタの設定です。YouTube アプリケーションを検出する必要があるため、ここではデフォルトプロファイルを使用します。
IPS：任意　（例. 無効）
SSL インスペクション：certificate-inspection
許可トラフィックをログ：任意　（例、有効 → すべてのセッション）
セッション開始時にログを生成：任意　（例、無効）
パケットをキャプチャ：任意　（例、無効）
このポリシーを有効化：有効

図 *4-8　IPv4* ポリシー設定

4.7. 動作確認

左メニュー「ログ＆レポート」→「転送トラフィック」をクリックします。通常トラフィックが port1 経由での通信となっていることを確認することができます。

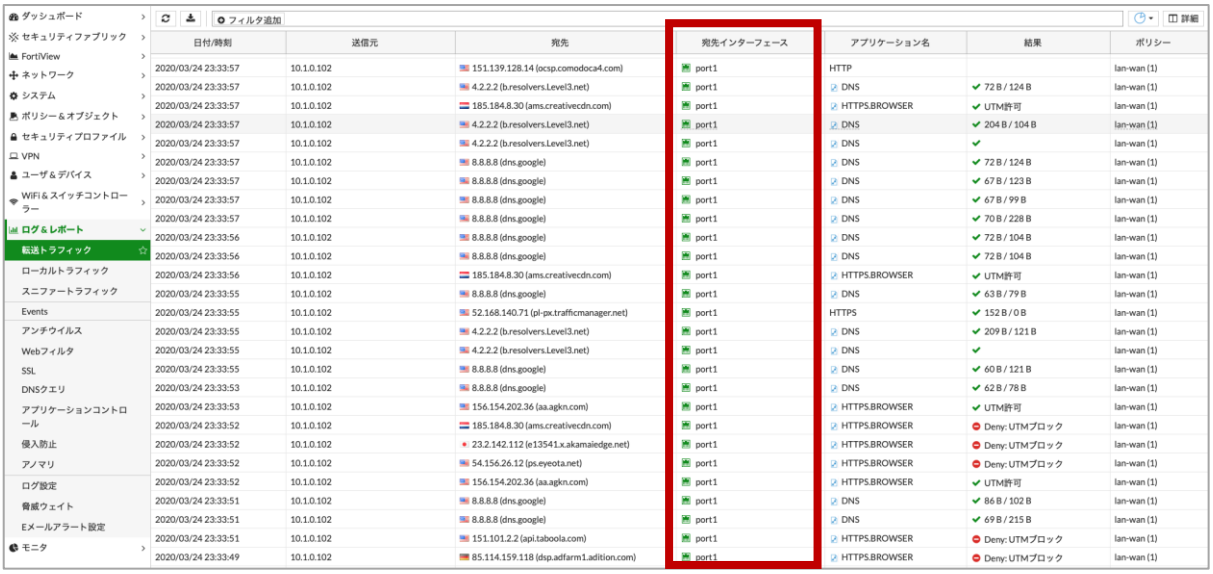

図 *4-9*　動作確認 *(*通常トラフィック*)*

検索ボックス内の「フィルタ追加」をクリックし、宛先をクリックします。先ほど登録した nhks-vh.akamaihd.net の IP アドレスを入力し、ログにフィルタをかけます。NHK for School トラフィックが port2 経由での通信となっていることを確認することができます。

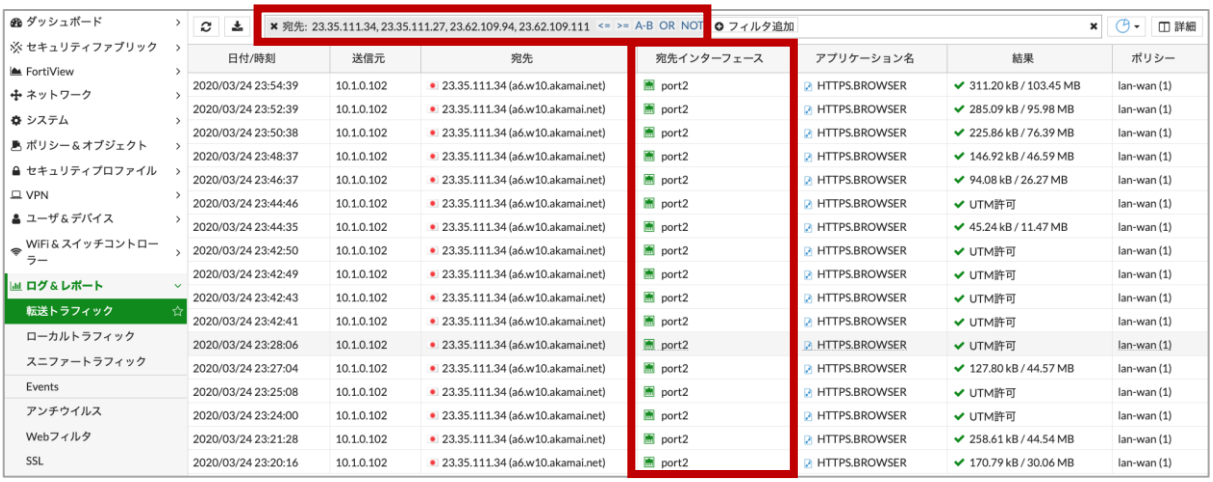

図 *4-10*　動作確認 *(NHK for School)*

* YouTube 通信はトラフィック検出時に動的に ISDB を作成します。そのため、各宛先の 2 度目の通信以降ブレイクアウトを行うことが可能です。

5. Appendix: スタティックルートによるインターネットブレイクアウト

NHK for School トラフィックは、「SD-WAN ルールによるインターネットブレイクアウト」の代わりにスタティックルート設定でもインターネットブレイクアウトが実現可能です。設定方法を記載します。

5.1. スタティックルートの設定

左メニュー「ネットワーク」→「スタティックルート」をクリックし、「新規作成」をクリックします。

ダイナミックゲートウェイ：有効
宛先：名前付きアドレス　→　NHK1
インターフェース：port2
ゲートウェイアドレス：ダイナミック
アドミニストレーティブ・ディスタンス：10
コメント：任意
ステータス：有効化済み

図 *5-1*　スタティックルートの設定 *1*

同じ手順でもう一つのドメインの設定を行います。

ダイナミックゲートウェイ：有効
宛先：名前付きアドレス　→　NHK2
インターフェース：port2
ゲートウェイアドレス：ダイナミック
アドミニストレーティブ・ディスタンス：10
コメント：任意
ステータス：有効化済み

図 *5-2*　スタティックルートの設定 *2*

5.2.　IPv4 ポリシーの設定

「SD-WAN ルールによるインターネットブレイクアウト」と同様の設定です。

5.3.　動作確認

「SD-WAN ルールによるインターネットブレイクアウト」と同様の方法で確認可能です。

改定履歴

バージョン	リリース日	改定履歴
1.0.0	2020.4	初版発行
1.0.1	2020.4	「IPv4 ポリシー設定」の修正、「SD-WAN 向けインターフェーススタティックルートの設定」を追記、その他文言修正
1.0.2	2020.5	ISDB 更新に伴う修正