第12版

ローカルブレイクアウト機能説明資料

2024年9月

古河電気工業株式会社
古河ネットワークソリューション株式会社

更新履歴

本説明資料の更新履歴

- 初版　2020年2月　新規作成
- 第2版　2020年6月　ProxyDNS機能を併用可能としたことにより更新
- 第3版　2020年8月　ローカルブレイクアウト機能の対応バージョンの情報を更新
- 第4版　2021年1月　全体的に見直し修正
- 第5版　2021年6月　HTTP snooping（Proxy環境下におけるLBO）の説明、
  コンフィグ例、アプリケーション動作確認実績を追加
  既存のLBOの説明をDNS snoopingの括りで再構成
- 第6版　2021年8月　全体を再構成
- 第7版　2021年11月　アプリケーション動作確認実績等を更新
- 第8版　2022年2月　アプリケーション動作確認実績にBoxを追加
- 第9版　2022年6月　LBO方式比較表、アプリケーション動作確認実績等を更新、機能補足のページを追加
- 第10版　2022年8月　アプリケーション毎統計情報対応を追加
  アプリケーション動作確認実績を更新
- 第11版　2023年9月　対応機種（vFX/vFX-S）追加、LBO+Fらくねっと®ソリューション追加、
  LBOマルチパス追加、動画ページのご案内を追加
- 第12版　2024年9月　対応機種（F225/F310）追加、TEAMSを使用する場合の設定について補足を追加、
  CLIに関して、app-profile 等を使うコマンドに修正
  Fらくねっとを利用したトラフィック可視化サービスの情報を追加

機種/バージョン毎のローカルブレイクアウト機能対応状況

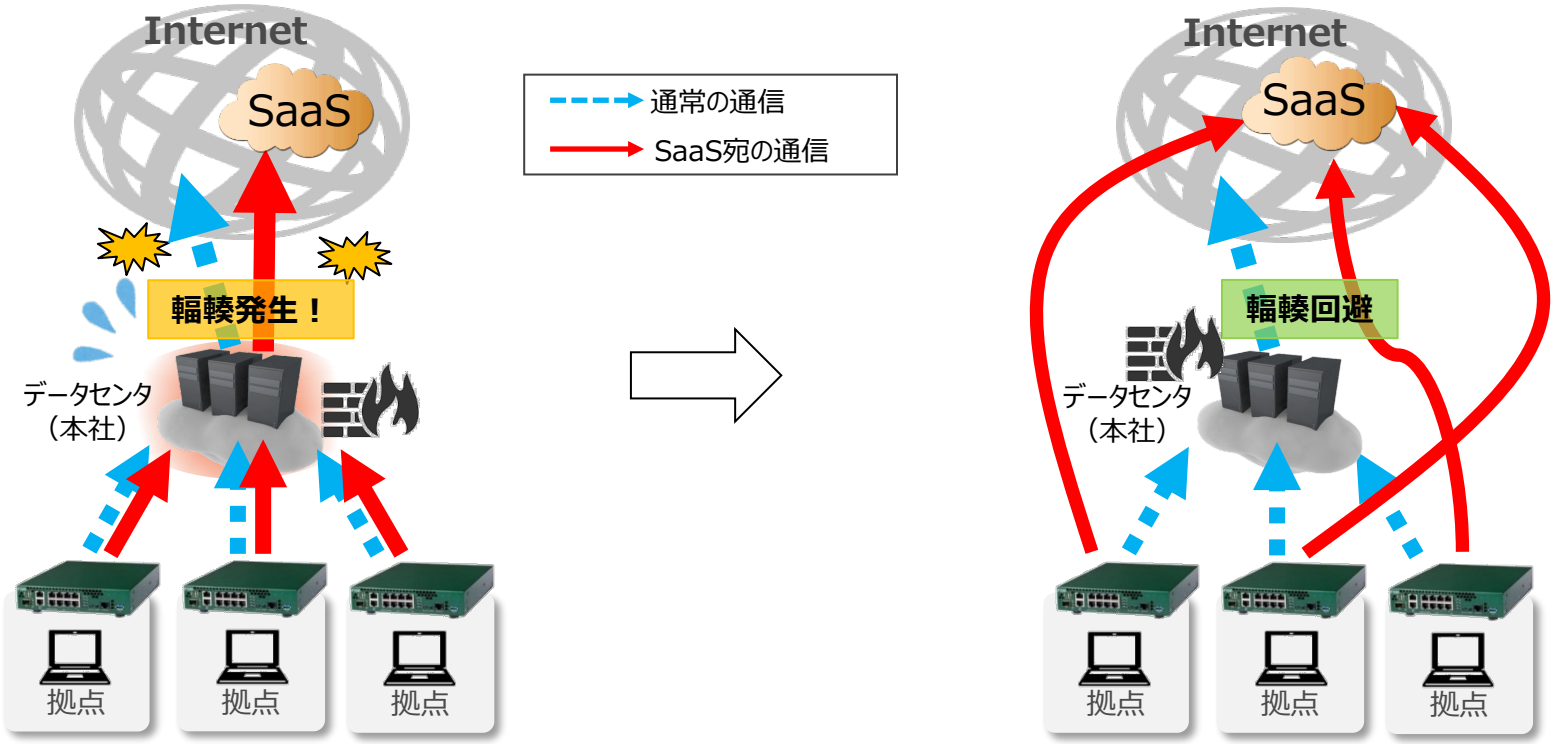
- 次の各機種にてローカルブレイクアウト機能に対応しています。
  - F70/F71
  - F220/F221
  - F220 EX/F221 EX
  - F225
  - F310
  - vFX/vFX-S

- 機能の対応状況は、ファームウェアバージョン毎に異なりますので、ご注意ください
  - F70/F71、F220/F221、F225、F310については、LBO方式比較表ページの注釈をご参照ください。
  - F220 EX/F221 EX、vFX/vFX-S については、弊社までお問い合わせください。

ローカルブレイクアウト（LBO）が必要な理由

- 近年Microsoft 365などSaaSアクセス増大により、企業ネットワークのWAN圧迫が発生
- SaaSアクセスなど特定のトラフィックを直接インターネットに通すブレイクアウト技術で解決
- FITELnetは、次の2つの方式に対応
  - ① DNS snooping方式（Proxyサーバを利用しない企業ネットワーク）
  - ② HTTP snooping方式（Proxyサーバを利用する企業ネットワーク）

特許取得済



ローカルブレイクアウト導入前　　ローカルブレイクアウト導入後

FITELnetのLBOの特長

- **Proxyサーバ有無どちらのケースにも対応！**
  - 端末ごとにProxyサーバ利用有無が混在するケースも可能
- **LBOしたアプリケーションへの通信パフォーマンス影響少！**
- **端末の設定やPACファイル*が不要！**
  - LBO対象をProxy除外するための設定追加やPACファイル配布の必要なし
- **ファーストパケット問題**なし！**
- **各種アプリケーションに対応！**
  - オプションライセンス無しで、CLI設定のみで各種アプリに対応
  - 複雑な定義ファイルの作成は不要
  - 当社クラウドサービス「Fらくねっと」により、複数拠点への一括設定や自動更新、アプリケーション毎の統計情報可視化に対応

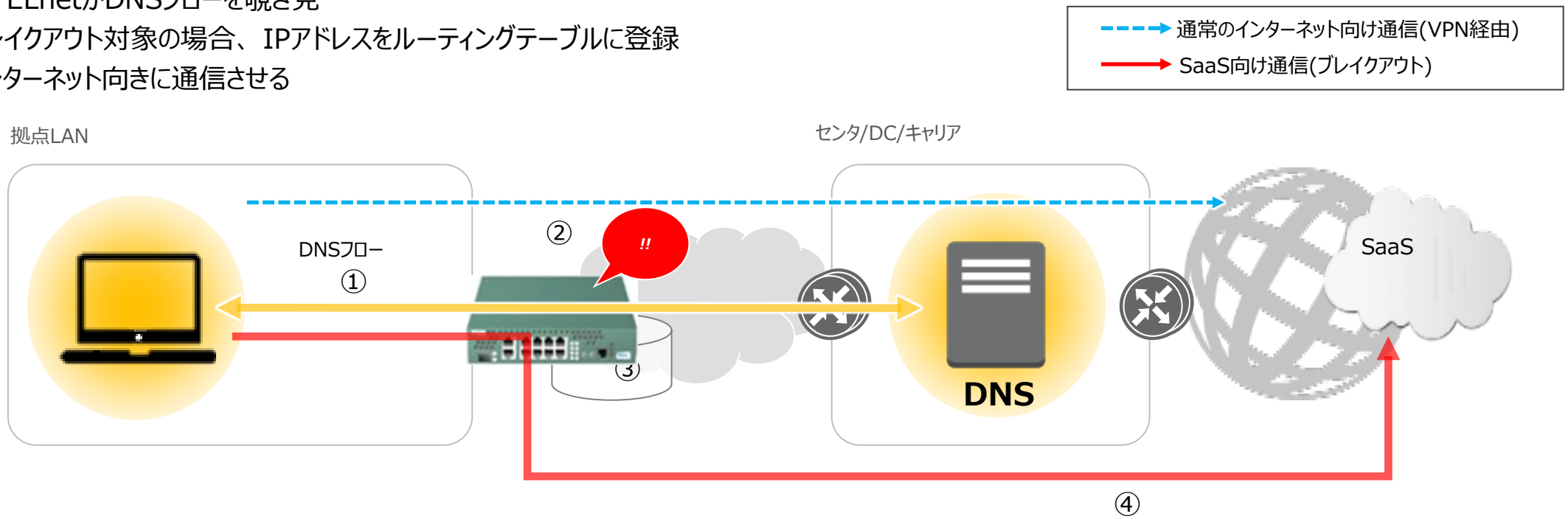
* PACファイル：URL毎にProxyサーバの利用有無等を定義したファイル

** ファーストパケット問題：ローカルブレイクアウトの最初のパケットがブレイクアウトせずにデータセンターを経由する問題

LBO方式①　DNS snooping方式

Proxyサーバを利用されないお客様にご提案

①端末からIPアドレス問い合わせのためのDNSフローが流れる
②FITELnetがDNSフローを覗き見
③ブレイクアウト対象の場合、IPアドレスをルーティングテーブルに登録
④インターネット向きに通信させる

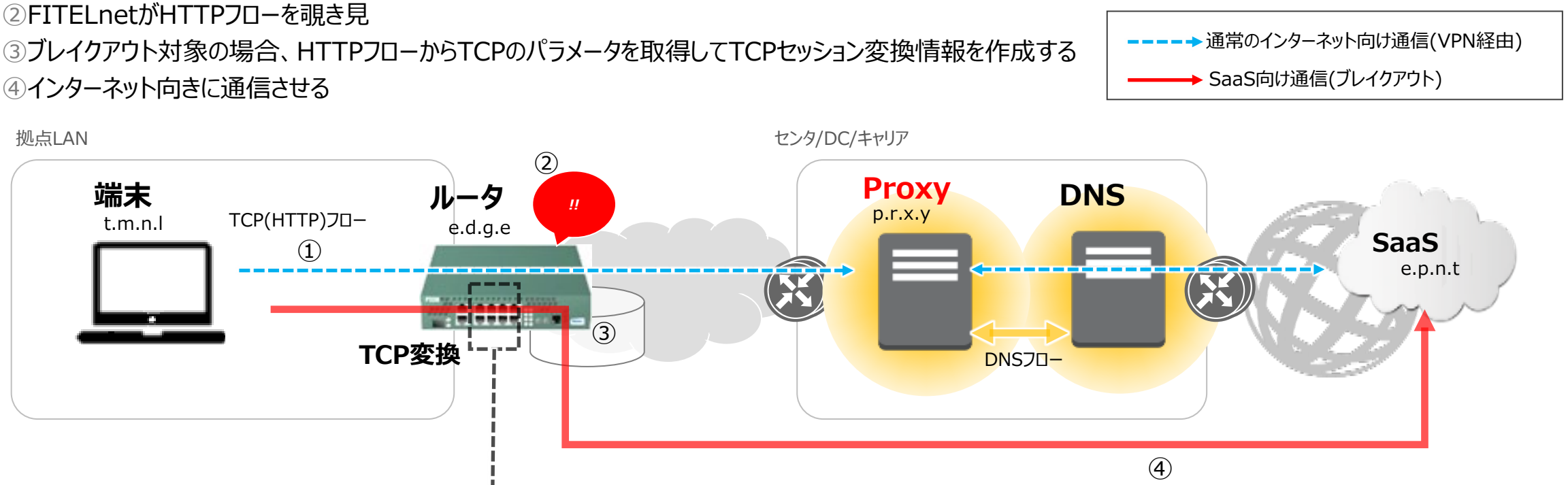


FITELnetルータにLBOしたいドメイン名を登録し、そのドメインに対するDNSフローを元にLBOする対象を決定

LBO方式②　HTTP snooping方式（1/2）

Proxyサーバを利用されるお客様にご提案

①端末からProxyサーバにHTTPフローを送信
②FITELnetがHTTPフローを覗き見
③ブレイクアウト対象の場合、HTTPフローからTCPのパラメータを取得してTCPセッション変換情報を作成する
④インターネット向きに通信させる



送信元（端末）		宛先（Proxy）	
IPアドレス	Port	IPアドレス	Port
t.m.n.l	50000	p.r.x.y	58888

送信元（ルータ）		宛先（SaaS）	
IPアドレス	Port	IPアドレス	Port
e.d.g.e	60000	e.p.n.t	443

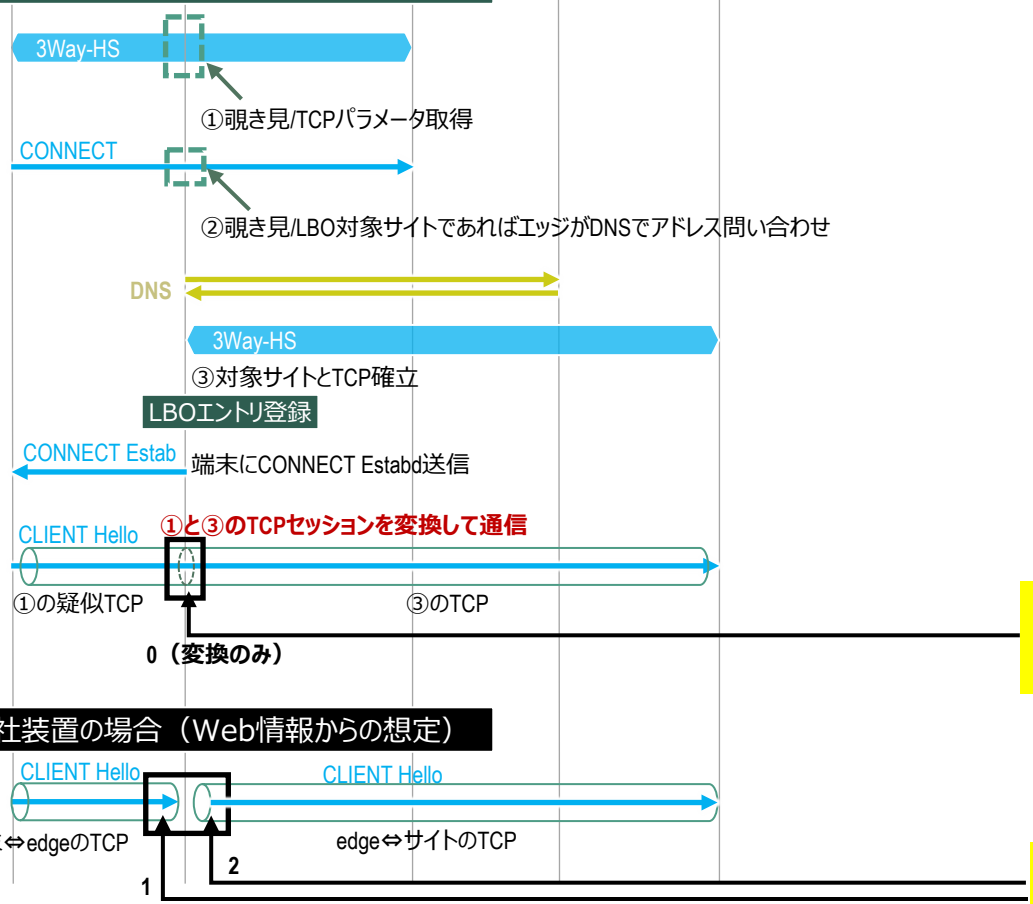
特許取得済

FITELnetルータにLBOしたいドメイン名を登録し、そのドメインに対するProxyサーバ経由の通信をLBO実施

LBO方式②　HTTP snooping方式（2/2）

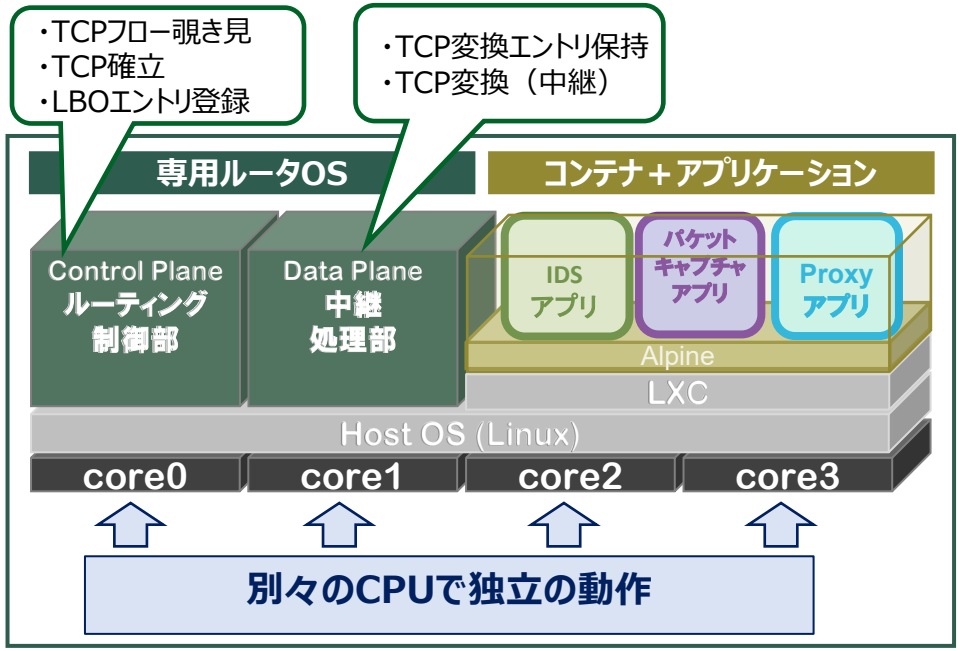
LBO対象フローの動作

FITELnetの場合



他社装置の場合（Web情報からの想定）

edgeがProxyサーバとして動作する仕組みのLBOと比較して、LBOしたアプリケーションの通信パフォーマンスへの影響少！



★ここがポイント
edgeはTCPセッションの変換のみを行う（TCPセッション0本を終端）

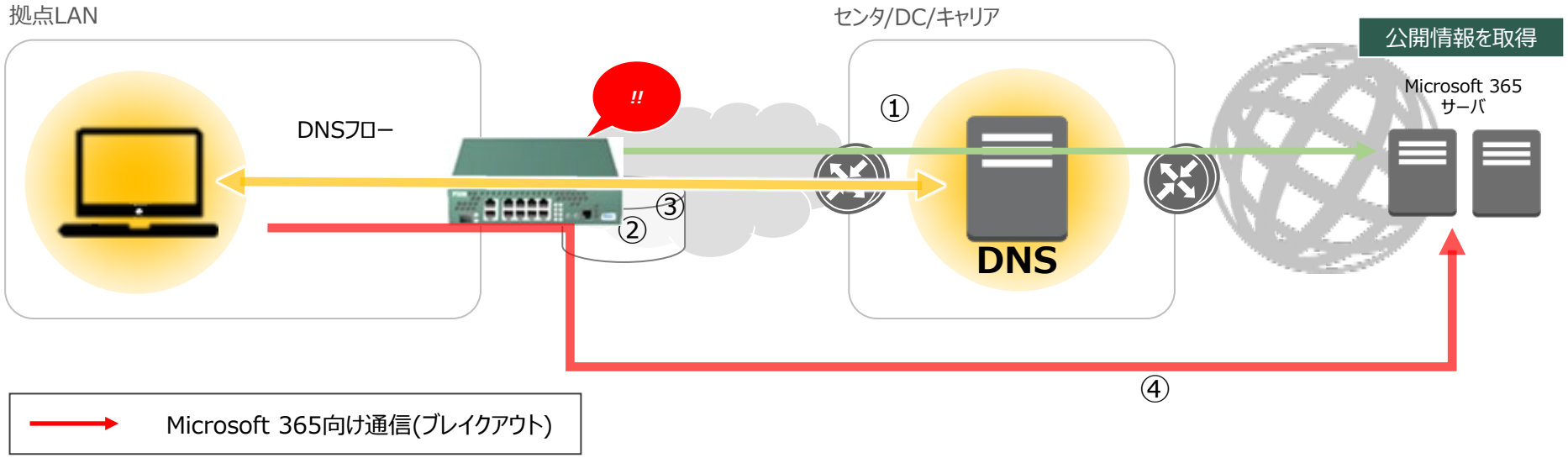
以後、同じTCPセッションのフローは、変換テーブルを利用して通信
（DNS問い合わせやHTTP CONNECTを行わない）

edgeはProxyとして、TCPセッション2本を終端

簡単設定　Microsoft 365 を使用する場合

Microsoft 365 をLBOする場合はドメイン名を設定しなくても、下記の一行の設定のみで可能
（DNS snooping/HTTP snooping共に対応）
o365 enable

Microsoft 365のLBO



MicrosoftのWeb公開情報(一部抜粋)

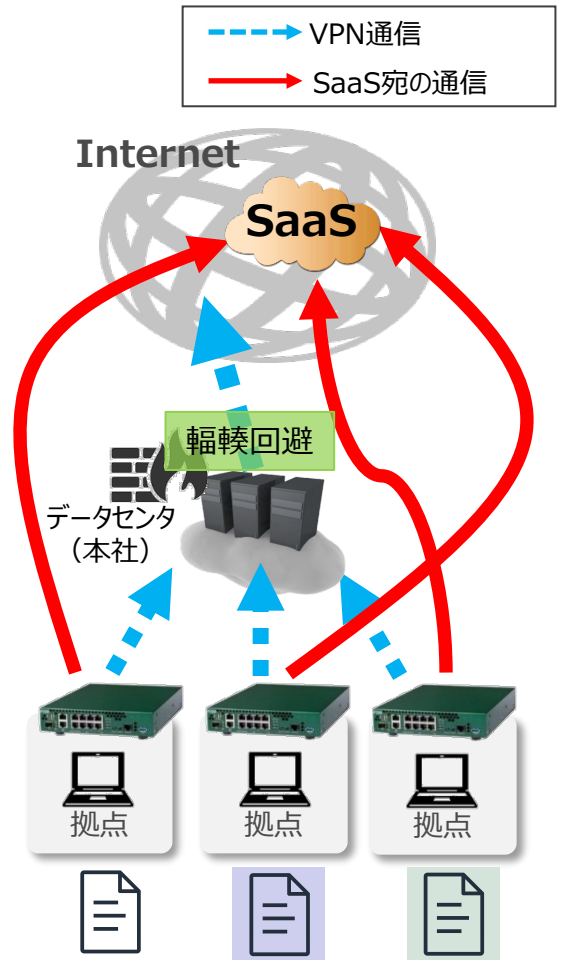

```
[
  {
    "id": 1,
    "serviceArea": "Exchange",
    "serviceAreaDisplayName": "Exchange Online",
    "urls": [
      "outlook.office.com",
      "outlook.office365.com"
    ],
    "ips": [
      "13.107.6.152/31",
      "13.107.18.10/31",
      "13.107.128.0/22",
      "23.103.160.0/20",
      "40.96.0.0/13",
      "40.104.0.0/15",
      "52.96.0.0/14",
      "131.253.33.215/32",
      "132.245.0.0/16",
      "150.171.32.0/22",
      "191.234.140.0/22",
      "204.79.197.215/32",
      "2603:1006::/40",
      "2603:1016::/40",
      "2603:1026::/40",
      "2603:1026:200::/39",
      "2603:1026:400::/39",
      "2603:1026:600::/44",
      "2603:1026:620::/44",
      "2603:1026:800::/44",
```


- Microsoft 365トラフィックについては、MicrosoftのWeb公開情報に記載されているMicrosoft 365エンドポイント情報を用いることで、LBOを実現します。
  （https://endpoints.office.com/endpoints/worldwide）
- 「o365 enable」を設定することにより、上記URLに対し、FITELnetがMicrosoft 365エンドポイント情報を取得しにいきます。

※TEAMSをご使用する際には、ポリシールーティングの設定も必要となります。下記URLの設定例をご参照ください。
https://www.furukawa.co.jp/fitelnet/setting/lbo/

LBO＋ Fらくねっと®ソリューション（1/2）

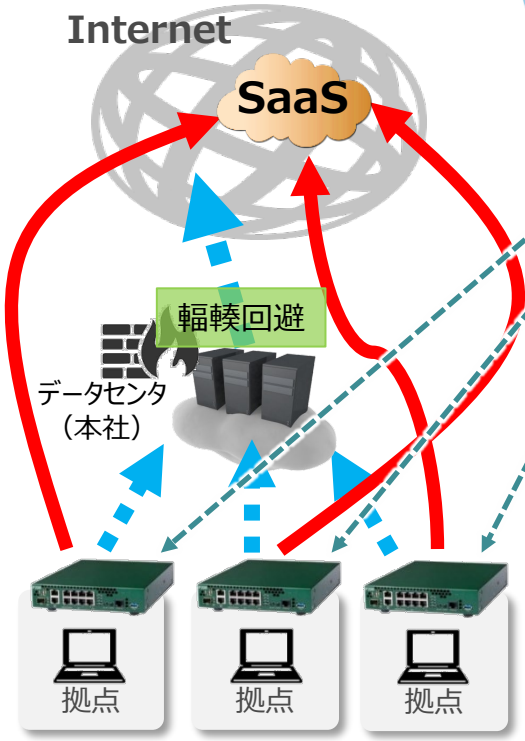
Fらくねっと® 導入前



・機器ごとにドメイン設定をつくることが必要
・SaaSのドメインリスト更新に追従できない

Fらくねっと® 導入後

★SaaSトラフィックをインターネット回線へブレイクアウト



Fらくねっと®

★Fらくねっと® からLBOポリシーを制御
SaaSの宛先変更等に追従

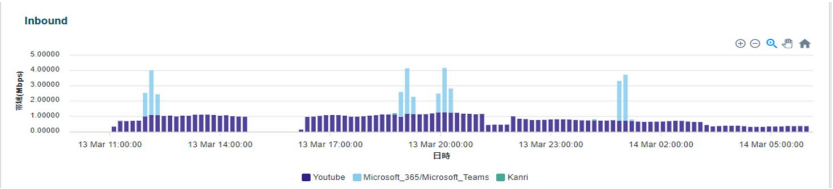
チェックのみでOK！

- ☑ Microsoft 365
- ☑ Zoom
- ☐ Webex
- ☐ Box
- ・・・

★SaaS毎の統計情報確認

トラフィック累計値の多い順に確認可（LBO非対象トラフィック含む）

時系列で確認可



トラフィック可視化サービスを利用して、送信元のIPアドレスを確認可
↓以下をご参照ください。
https://docs.f-rakunet.jp/docs/gaiyou_kinou/gaiyou_page/gaiyou6

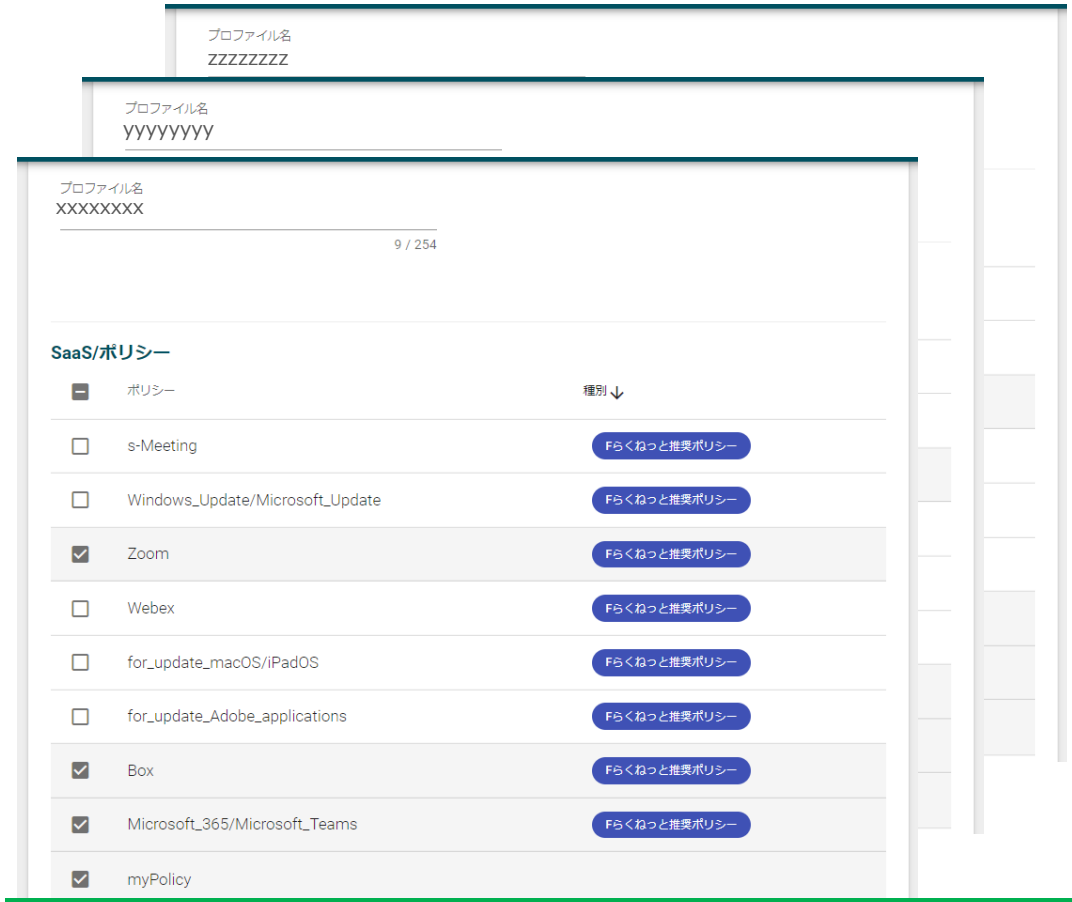
LBO＋ Fらくねっと®ソリューション（2/2）

ローカルブレイクアウト (LBO) を導入したいけど…

```
lbo-profile zzzzzzzz
  dns-snooping enable
lbo-profile yyyyyyyy
  dns-snooping enable
lbo-profile xxxxxxxx
  o365 enable                    ← Microsoft 365
  dns-snooping enable
  domain *zoom.us                ← Zoomのドメイン
  domain *.box.com               ┐
  domain *.box.net               │
  domain *.boxcdn.net            │
  domain *.boxcloud.com          ← Boxのドメイン
  domain *.cdn.office.net        │
  domain excel.officeapps.live.com
  domain fs.microsoft.com        ┘
  domain *.example.com           ┐
  domain *furukawa*              │
  domain fnsc.com                ← myPolicyのドメイン
  domain furu.kawa               │
  domain upload.fnsc.com         ┘
exit
!
```

・機器ごとにドメイン設定をつくることが必要
・SaaSのドメインリスト更新に追従できない

Fらくねっと® があれば…



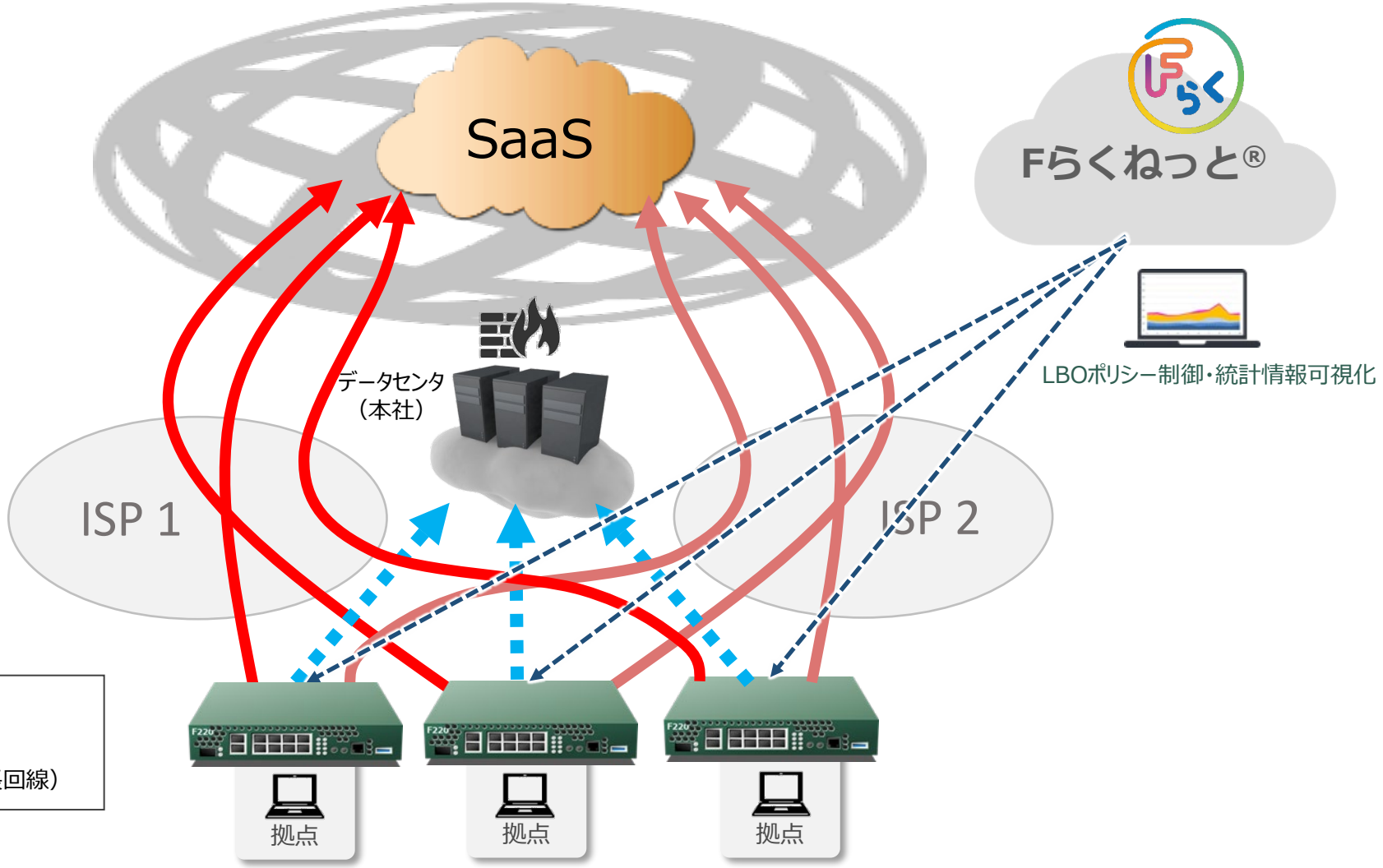
・SaaSのチェックだけでLBOできる！
・SaaSのドメインリスト更新に追従可(マイポリシー除く)

※当社にてSaaSのドメインリスト定期見直し/DB更新したタイミングで追従

Fらくねっと®ドキュメントページの「LBO管理サービス」をご参照ください
https://docs.f-rakunet.jp/docs/user/NW/lbo/

LBOマルチパス

- LBOの帯域拡張や通信安定性向上のため、異なる2つの回線にてLBOの分散や冗長を行うための、マルチパス機能を開発
- DNS snooping, HTTP snooping どちらも対応



FITELnetのLBOの特長とメリット

＊	特長	メリット
①	Proxyサーバ有無 どちらにも対応！	・Proxyサーバを本社などに配置した企業ネットワークの環境でも拠点にてLBOを実現！ ・端末ごとにProxyサーバ有無が混在するケースも対応可能！
②	DPI方式のLBOと 比較して、 パフォーマンスへの 影響少！	・TCPセッションの変換のみをData Planeで実施する(TCPを終端しない)ことで、中継性能への影響が少ない ・DPI方式と比較して中継性能が良い(Proxy使用時) FITELnet F70/F71 最大1.9Gbps、 F220/F221/F225 最大3.0Gbps、 FITELnet F310 最大8.9Gbps、他社(カタログ値) 1.0Gbps ・スケーラビリティ面で有利、下記のTCPセッション変換可能 F70/F71/F310 20,000、 F220/F221/F225 60,000
③	お客様の端末の 設定や PACファイルが 不要！	・お客様の端末にてProxyサーバアドレス、ポート番号以外のProxy関連の設定は不要 ・お客様の端末にPACファイルの配布が不要 →PACファイルの運用を禁止しているお客様環境に対応 ・LBO環境移行時の端末の設定変更の必要なし
④	ファーストパケット 問題なし！	・DPI方式のローカルブレークアウトで課題となっている、ファーストパケット問題が発生しない。 ファーストパケットからLBO可能
⑤	各種 アプリケーションに 対応！	・オプションライセンス無しで、ルータのコマンド(domain)のみでオンライン会議やクラウドストレージサービス、 動画配信サービスなど、各種アプリケーションに対応 ・「Fらくねっと®」LBOサービスにより、複数拠点への一括設定や自動更新、アプリケーション毎の統計情報 可視化に対応 ・複雑な定義ファイルの作成は不要

LBOの設定

DNS snooping方式の設定

```
app enable
local-breakout enable
local-breakout A tunnel 1        … LBO先を指定
app-profile A
  o365 enable                    … Microsoft 365のLBO
  dns-snooping enable            … DNS snoopingを行うための設定
  domain *example*
  domain *.xxx.com               …一般的なサイトのLBO「*」でまとめて指定可能
exit
!
interface Tunnel 2
  description WAN-default
  dns-snooping enable            … DNS snoopingをこの回線で行うための設定
exit
```

設定が簡単！

①ルータのCLI設定のみで様々なアプリケーションに対応

②Microsoft 365は一行のみ（o365 enable）
　※TEAMSを使用する場合は「簡単設定　Microsoft 365を使用する場合」もご参照ください

③定義ファイルやスクリプトは必要なし

Fらくねっと®があればさらに簡単！

HTTP snooping方式の設定

```
ip name-server <DNSサーバ>              … DNS問い合わせ先を設定
!
app enable
local-breakout enable
local-breakout proxy-server ip any port <ポート番号>   … プロキシ宛通信のLBO対象のポート番号を指定
local-breakout A tunnel 1               … LBO先を指定
app-profile A
  o365 enable                           … Microsoft 365のLBO
  http-snooping enable with-route       … HTTP snoopingを行うための設定。with-routeオプションにより宛先アドレスを経路情報として登録するので、TCP以外のLBOが可能
  domain *example*
  domain *.xxx.com                      … 一般的なサイトのLBO：「*」でまとめて指定可能
exit
!
interface Port-channel 1
  description LAN
  ip address 192.168.10.1 255.255.255.0
  http-snooping enable                  … HTTP snoopingを設定
  mss 1300                              … mssを指定　※LAN回線のMSSをLBO回線よりも小さい値に設定する
exit
```

LBO確認コマンド（1/2）

- 下記の情報表示コマンドがございます（★：HTTP snoopingにて使用）

show local-breakout:	LBO動作状況を確認可能
show ip route, show ipv6 route:	LBO経路登録状況を確認可能
show app session★:	HTTP snoopingによりLBOしたTCPセッションを確認可能
show app session no-match★:	HTTP snoopingでdomain情報と一致せず、LBO対象外となったTCPセッションを確認可能
show app statistics:	LBOの統計情報を確認可能
show app traffic:	アプリケーション毎（app-tag単位）の統計情報を確認可能 ※Microsoft 365の場合はサービス単位で確認可能

- show ip route, show ipv6 routeについて
  - LBO経路については、先頭に「L ＞」が表示されます。

```
#show ip route
（中略）
L ＞ * xxx.xxx.xxx.xxx/32 [0/0] is directly connected, Tunnel1
```

  - パケットの宛先が先頭「L ＞」の経路に包含される場合に、当該パケットはブレイクアウトします。
  - HTTP snoopingの場合は、with-routeオプションを設定した場合のみ先頭「L＞」の経路が確認されます（with-routeなしの場合は、TCPパケットのみ、次ページに示すshow app sessionの変換テーブルにしたがってブレイクアウトします）。

LBO確認コマンド（2/2）

- show app sessionについて
  - HTTP snoopingによりLBOしたTCPセッション情報（変換前と変換後）を表示します。

```
#show app session

http snooping:
（中略）
  List of active session:
  Local network
      Breakout network
  Server
  192.168.10.42:60870 192.168.20.2:58888        #変換前の送信元アドレス:ポート番号　宛先アドレス:ポート番号
      192.168.30.11:60870 xxx.xxx.xxx.xxx:443    #変換後の送信元アドレス:ポート番号　宛先アドレス:ポート番号
  www.fnsc.co.jp                                #宛先サイトのURL情報
  192.168.10.42:60932 192.168.20.2:58888
      192.168.30.11:60932 xxx.xxx.xxx.xxx:443
  test.fnsc.co.jp
```

- show app session no-matchについて
  - domain設定と一致せず、LBO対象外となったTCPセッション情報を表示します。

```
#show app session no-match

no- match list:
（中略）
  List of no match session:
  Local network                                 Server
  192.168.10.42:62083 192.168.20.2:58888   www.furukawa.co.jp
                              #送信元アドレス:ポート番号　宛先アドレス:ポート番号　宛先サイトのURL情報を表示
```

機能紹介（1/2）

LBO対象外ドメイン指定（bypassオプション）：

「*」指定によりLBO対象ドメインに含まれた一部のドメインを、LBO対象外として、デフォルト回線、もしくは他の回線に中継させる場合に指定

```
app-profile A
  dns-snooping enable
  domain *.example.com                 …LBO対象
  domain *.spl.example.com bypass      …LBO対象外
  …
exit
```

bypassオプションにより、Proxy環境下で、Microsoft 365のテナント制限とLBOの併用動作が可能です。
https://www.furukawa.co.jp/fitelnet/setting/lbo/ProxyLBO_Microsoft365_Tenant-restrictions.pdf

破棄対象ドメイン指定（中継先をnullインタフェースに指定）：

特定のドメイン宛のパケットを破棄する場合に指定（あらかじめアクセス制限したいドメインがわかっている場合に有効）

```
local-breakout A tunnel 1          … LBO対象
local-breakout B null 0            … 破棄対象
!
app-profile A
  dns-snooping enable
  domain *.example1.com            … LBO対象のドメインを指定
  …
exit
!
app-profile B
  dns-snooping enable
  domain *.example2.com            … 破棄対象のドメインを指定
  …
exit
```

機能紹介（2/2）

アプリケーションごとの統計情報表示（app-tagオプション）：

アプリケーション毎、もしくはサービス毎に統計情報を表示する場合に指定

```
app-profile A
  o365 enable                                  …Microsoft 365はサービス（Exchange, Teams, etc）毎に
                                                  統計情報を記録。app-tag設定は不要
  dns-snooping enable
  domain *.example.com app-tag S1          …サービス：S1として統計情報を記録
  domain *.spl.example.com app-tag S1      …サービス：S1として統計情報を記録
  domain *.spl2.example.com app-tag S1     …サービス：S2として統計情報を記録
  …
exit
```

・アプリケーション毎/サービス毎の統計情報はshow app trafficコマンドにより確認可能
・Fらくねっと®にて統計情報の可視化も可能

Fらくねっと®連携：

以下、Fらくねっと®ドキュメントページをご参照ください
LBOポリシー制御：https://docs.f-rakunet.jp/docs/user/NW/lbo/　⇒ domain設定が不要となります
トラフィック可視化：https://docs.f-rakunet.jp/docs/user/NW/visualizing/traffic_visualizing_config
⇒LBO対象/非対象SaaSのどちらも確認可。SaaS毎に送信元IPアドレスの情報が確認できます。

LBOマルチパス：

異なる2つの回線にて、LBOの分散や冗長を行う場合に指定

```
local-breakout A tunnel 1                    … LBO中継先：主回線（distance 0）
local-breakout A dhcp port-channel 2 10      … LBO中継先：冗長回線（distance 10）
!
app-profile A
  dns-snooping enable
  domain *.example1.com          … LBO対象のドメインを指定
  …
exit
```

LBO方式比較表

項目		DNS snooping	HTTP snooping
動作環境		Proxyサーバなし	Proxyサーバ配下
スケーラビリティ		下記のLBO経路の 登録が可能	下記のTCP変換テーブルの 登録が可能
	F70/F71/F310	10,000経路	20,000セッション
	F220/F221/F225 F220 EX/F221 EX vFX/vFX-S	10,000経路	60,000セッション
便利 機能	DNS snooping/ HTTP snooping 共通	・複数lbo-profile指定（lbo-profile毎に中継先を指定） ・LBO経路のdistance値指定 ・LBO中継先にnullインタフェースを指定（特定のdomain宛パケットを破棄対象とする） ・LBO対象外ドメイン指定（bypassオプション） ・Fらくねっと®連携（Fらくねっと®を利用したLBOサービス：vFX/vFX-Sは未対応） ・アプリケーション毎の統計情報表示 ・LBOマルチパス	
	DNS snooping/ HTTP snooping 個別	・ProxyDNS併用動作 ・LBO経路登録上限数設定 ・LBO経路有効期間指定	・LBO対象外エントリの表示 （キャッシュエントリ数指定可） ・無通信監視時間指定
中継性能		通常のルーティングと同等	NAT利用時と同等

アプリケーションのLBO動作確認実績

Fらくねっと®でも利用可！

FURUKAWA ELECTRIC GROUP

■ 弊社にて下記の通り、アプリケーションのLBO動作確認実績がございます（○：動作確認済、 △：動作確認中、 －：動作確認未実施）

アプリケーション		DNS snooping	HTTP snooping
動画配信サービス※1		○	○
Microsoft 365		○	○
ソフトウェア・アップデート	Windows Update/Microsoft Update	○	○
	for update macOS/iPadOS	○	－
	for update Adobe applications	○	－
オンライン会議システム	Microsoft Teams	○	○
	Zoom	○	○
	Webex®	○	○
	s-Meeting	－	○
クラウドストレージサービス：Box		○	○

※1：アプリケーション名については弊社にお問い合わせください。
・Windows, Microsoft 365, Microsoft Teams は、Microsoft Corporation およびグループ会社の米国およびその他の国における商標です。
・macOS, iPadOS は、Apple inc.の商標です。
・Adobeは、アドビシステムズ社の商標です。
・Zoomは、Zoom Video Communications, Inc.の米国およびその他の国における登録商標または商標です。
・Webex®は、Cisco Systems, Inc.の米国およびその他の国における登録商標または商標です。
・「s-Meeting」は、ドコモ・システムズの登録商標です。
・Boxは、Boxの米国あるいはその他の国における登録商標または商標です。

■ 以下に設定例がございます。設定例や動作確認実績の無いアプリケーションについてはご相談ください
https://www.furukawa.co.jp/fitelnet/product/setting/lbo-list.html ローカルブレイクアウト機能を使う

動画ページのご案内

- LBO機能について、動画にてご説明します。視聴を希望されるお客様は、以下のページにて必要事項をご記入ください。
  https://www.furukawa.co.jp/fitelnet/member/form_lbo.html

Bound to Innovate