

ローカルブレイクアウト機能説明資料

2023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

※本資料に記載の会社名、製品名、サービス名は、各社の商標または登録商標です。

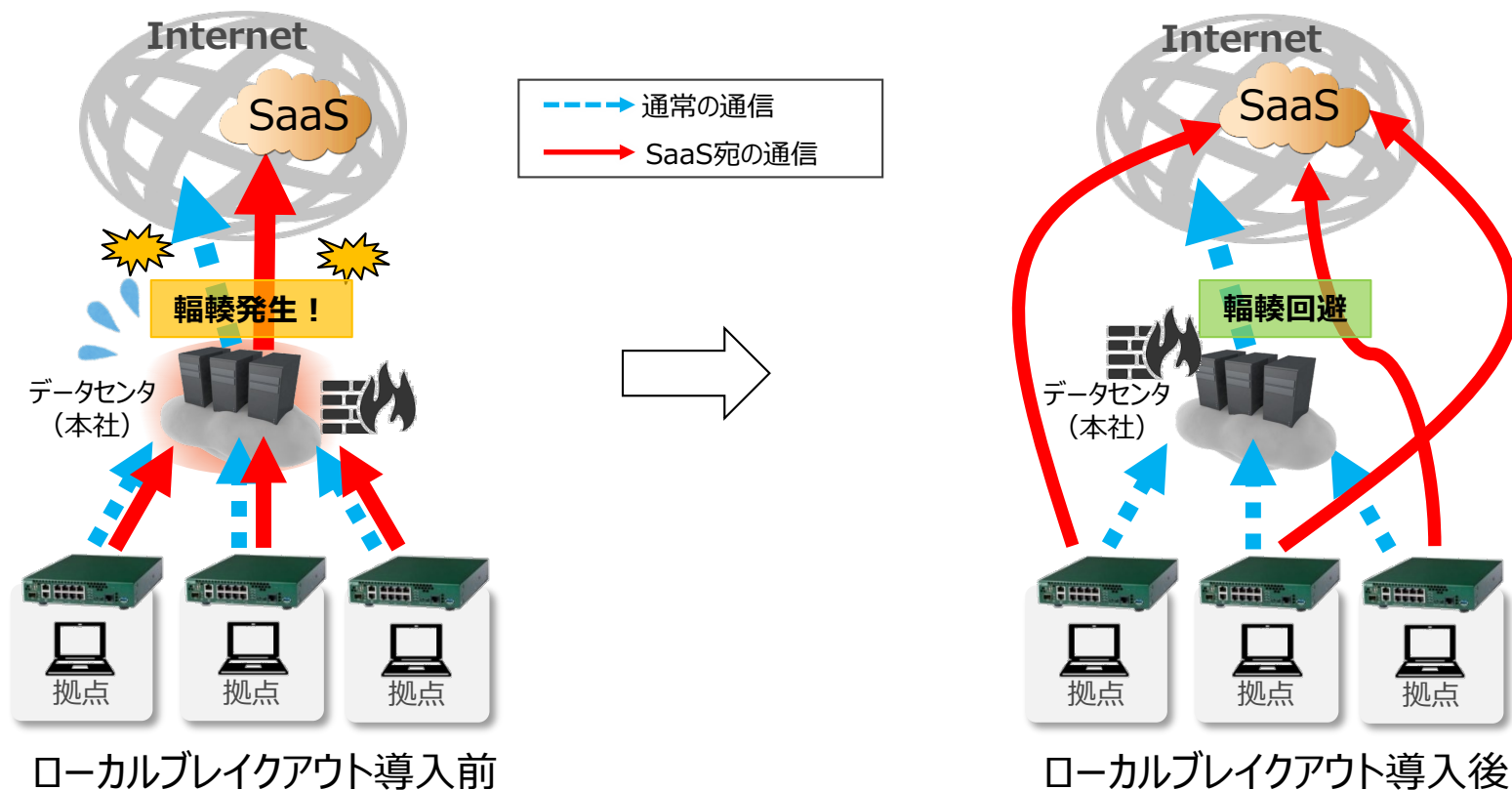
■ 本説明資料の更新履歴

- 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

- 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
 - 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**



- **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

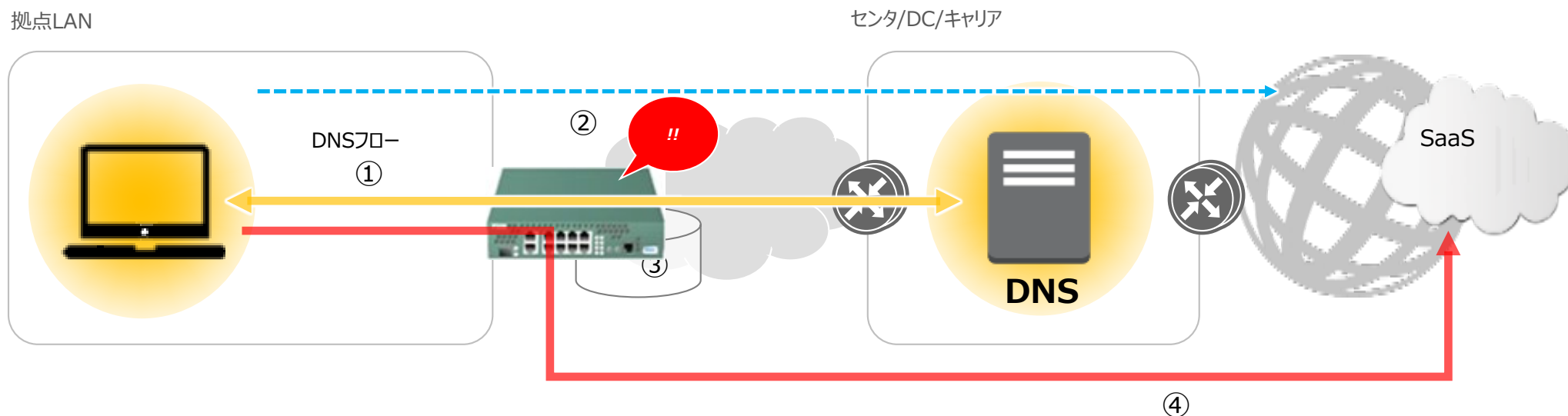
* PACファイル：URL毎にProxyサーバの利用有無等を定義したファイル

** 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

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
- ② FITELnet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

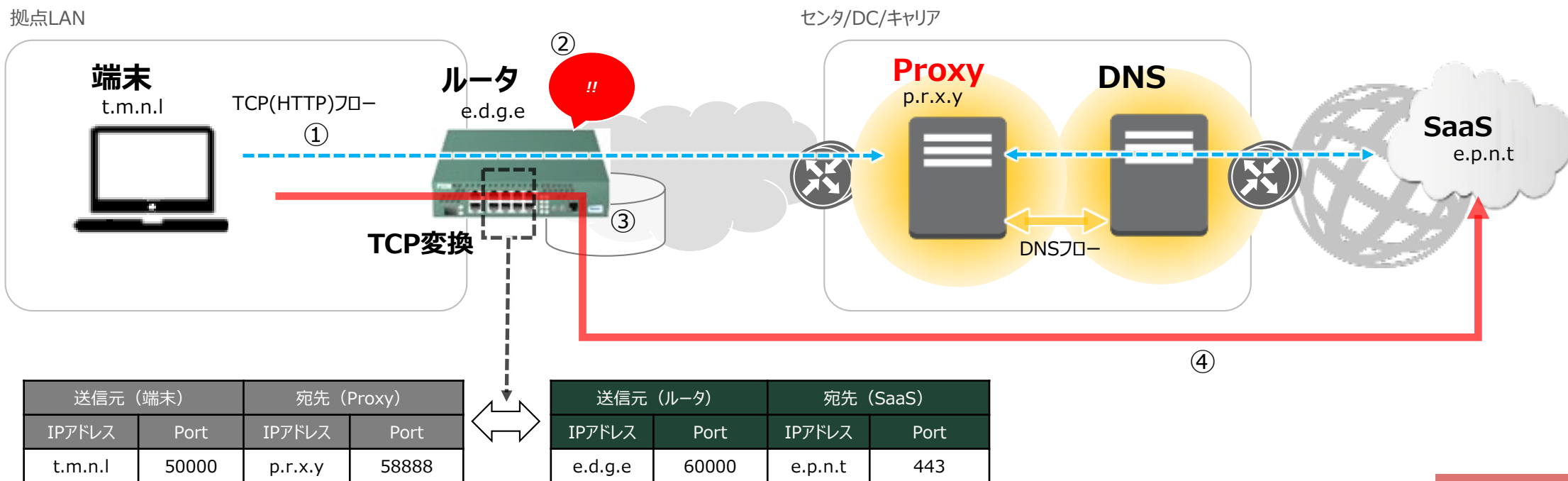
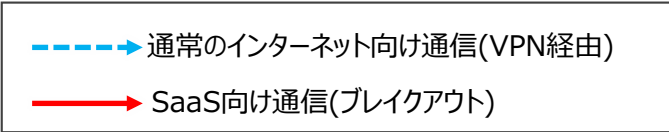
---> 通常のインターネット向け通信(VPN経由)
-> SaaS向け通信(ブレイクアウト)



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

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
- ② FITELnet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

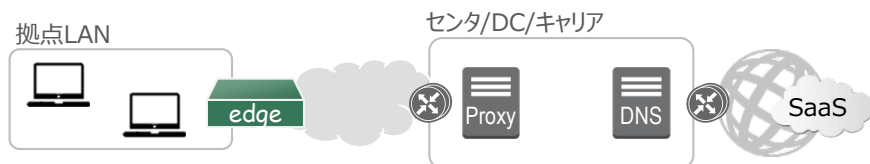


特許取得済

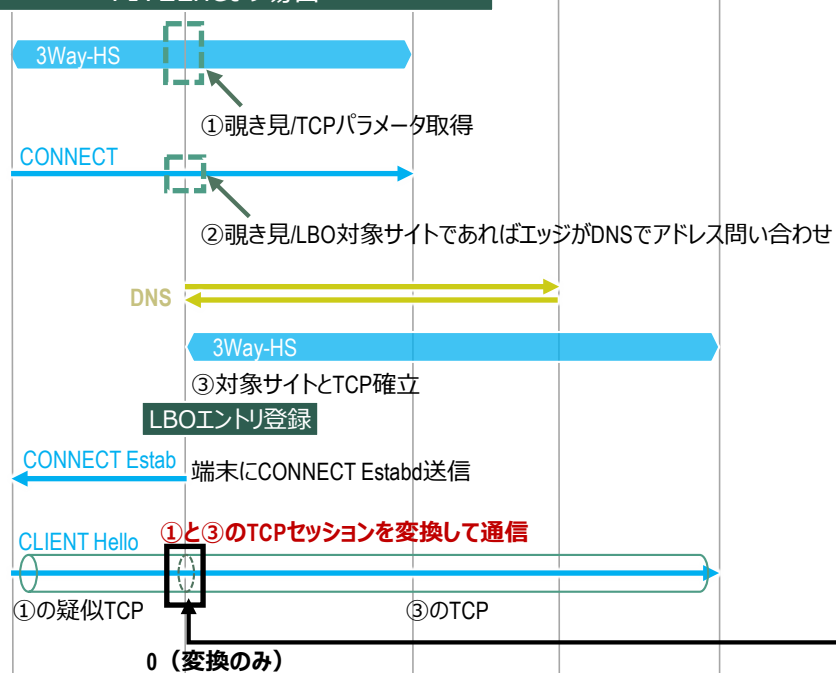
FITELnetルータにLBOしたいドメイン名を登録し、そのドメインに対するProxyサーバ経由の通信をLBO実施

LBO方式② HTTP snooping方式 (2/2)

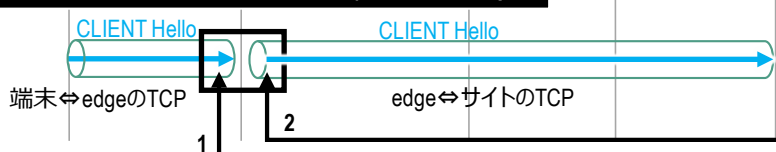
LBO対象フローの動作



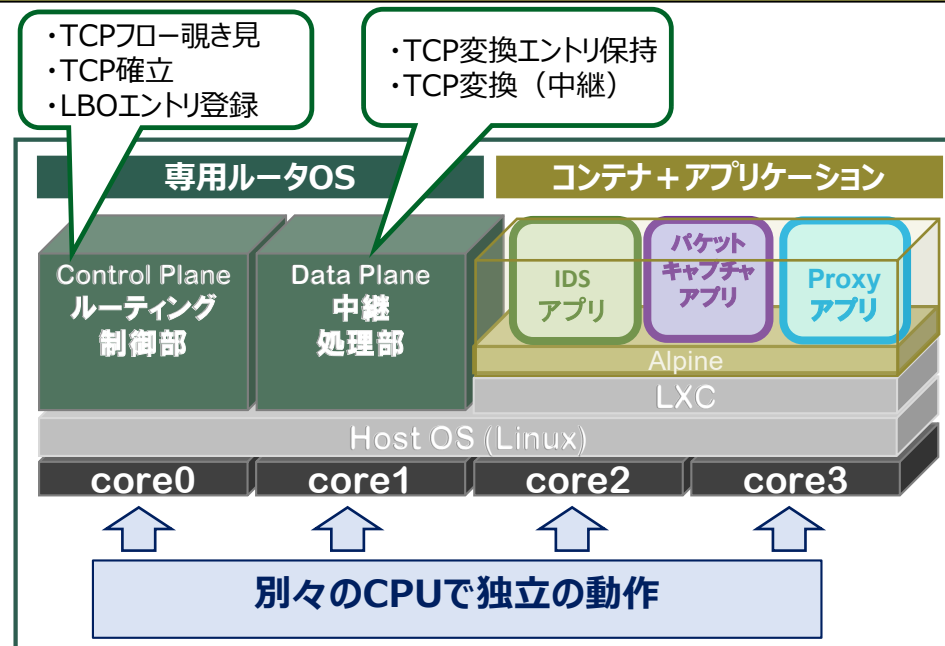
FITELnetの場合



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

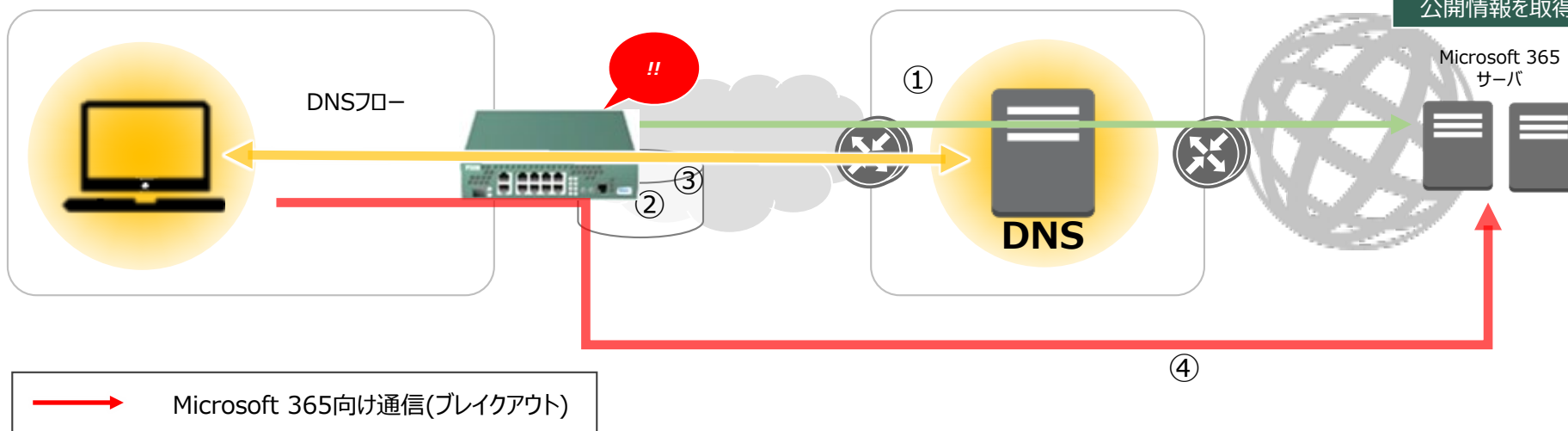
Microsoft 365 をLBOする場合はドメイン名を設定しなくても、下記の一行の設定のみで可能
(DNS snooping/HTTP snooping共に対応)

o365 enable

Microsoft 365のLBO

拠点LAN

センタ/DC/キャリア

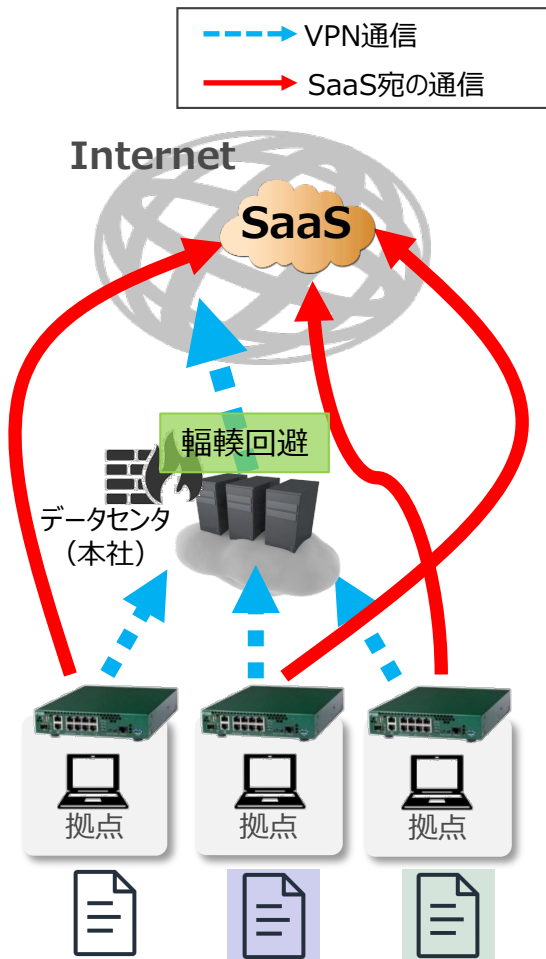


MicrosoftのWeb公開情報(一部抜粋)

```
[
{
  "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。

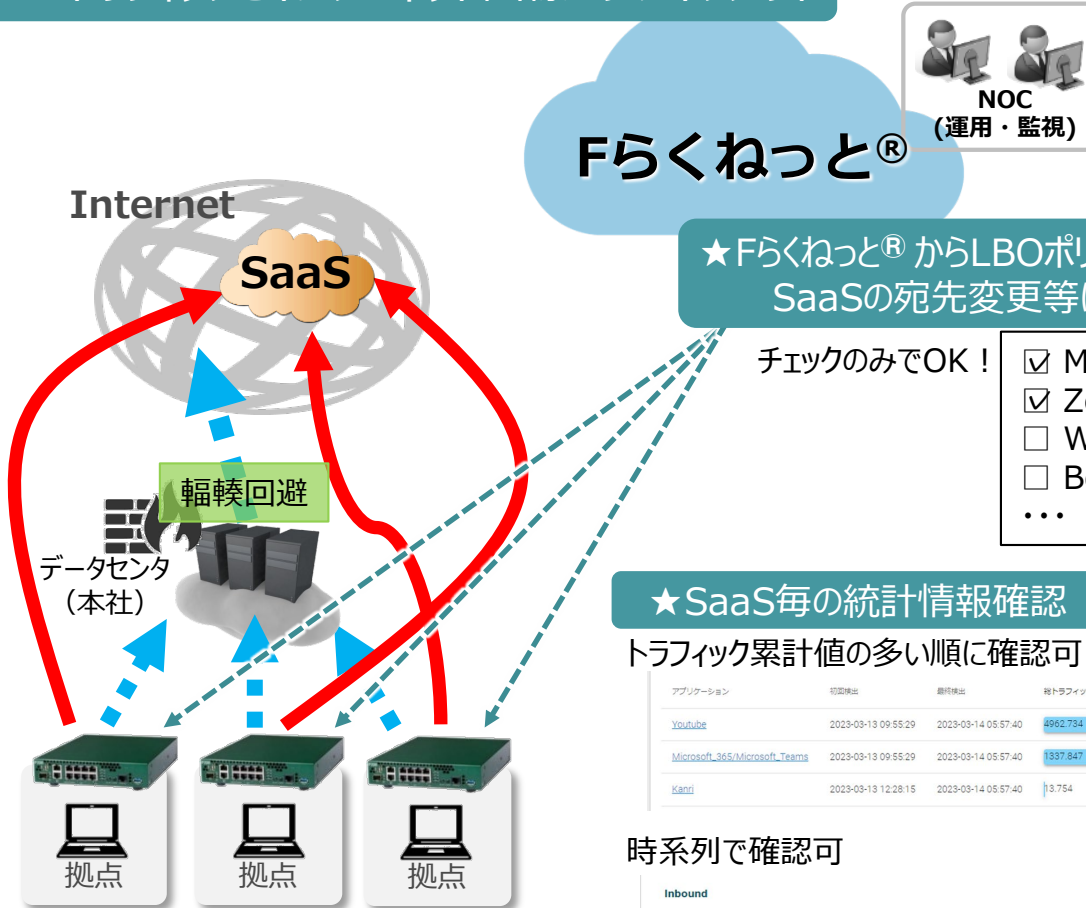
Fらくねっと® 導入前



- ・機器ごとにドメイン設定をつくらなければならない
- ・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® 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!

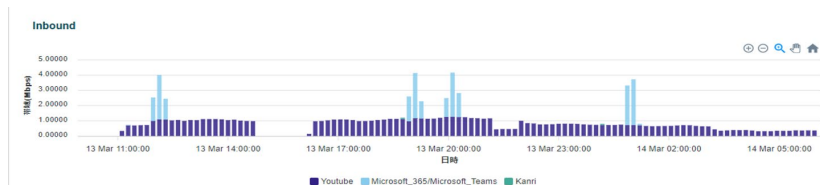
- Microsoft 365
- Zoom
- Webex
- Box
- ...

★ SaaS毎の統計情報確認

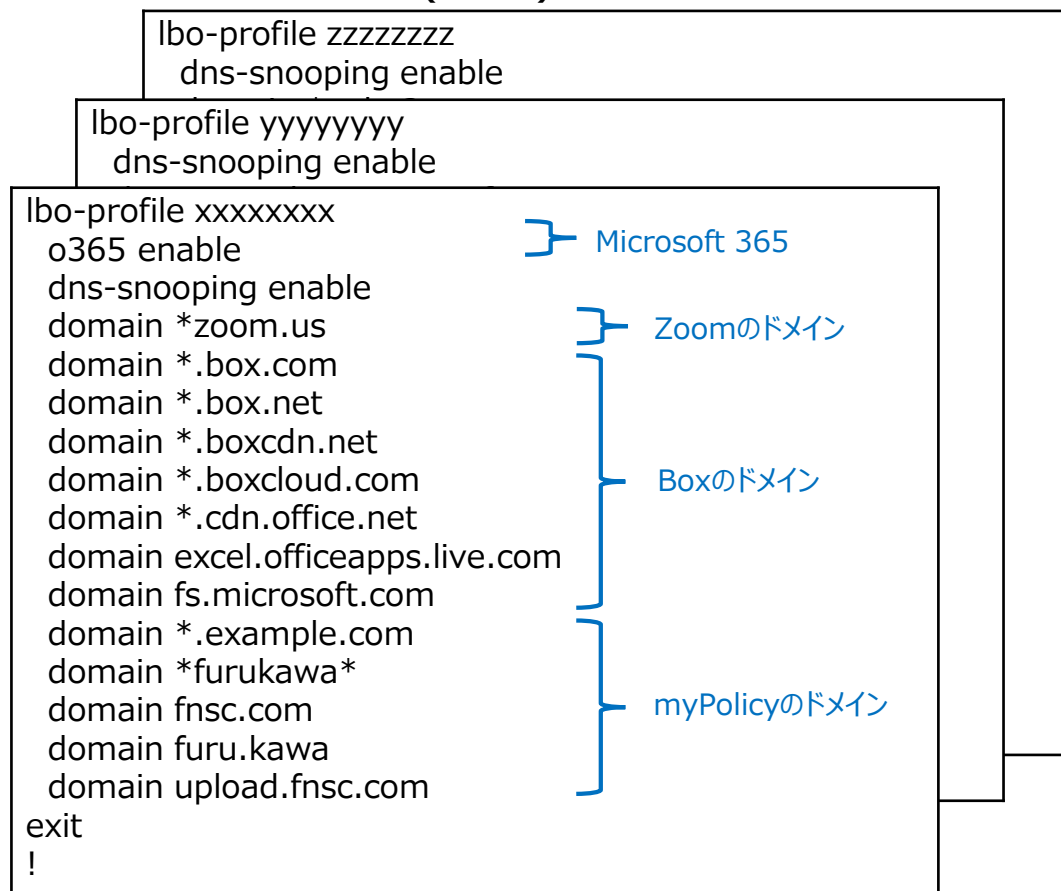
トラフィック累計値の多い順に確認可

アプリケーション	初回検出	最終検出	総トラフィック (MB/週) ↓
YouTube	2023-03-13 09:55:29	2023-03-14 05:57:40	4962,734
Microsoft_365/Microsoft_Teams	2023-03-13 09:55:29	2023-03-14 05:57:40	1337,847
Kanri	2023-03-13 12:28:15	2023-03-14 05:57:40	13,754

時系列で確認可

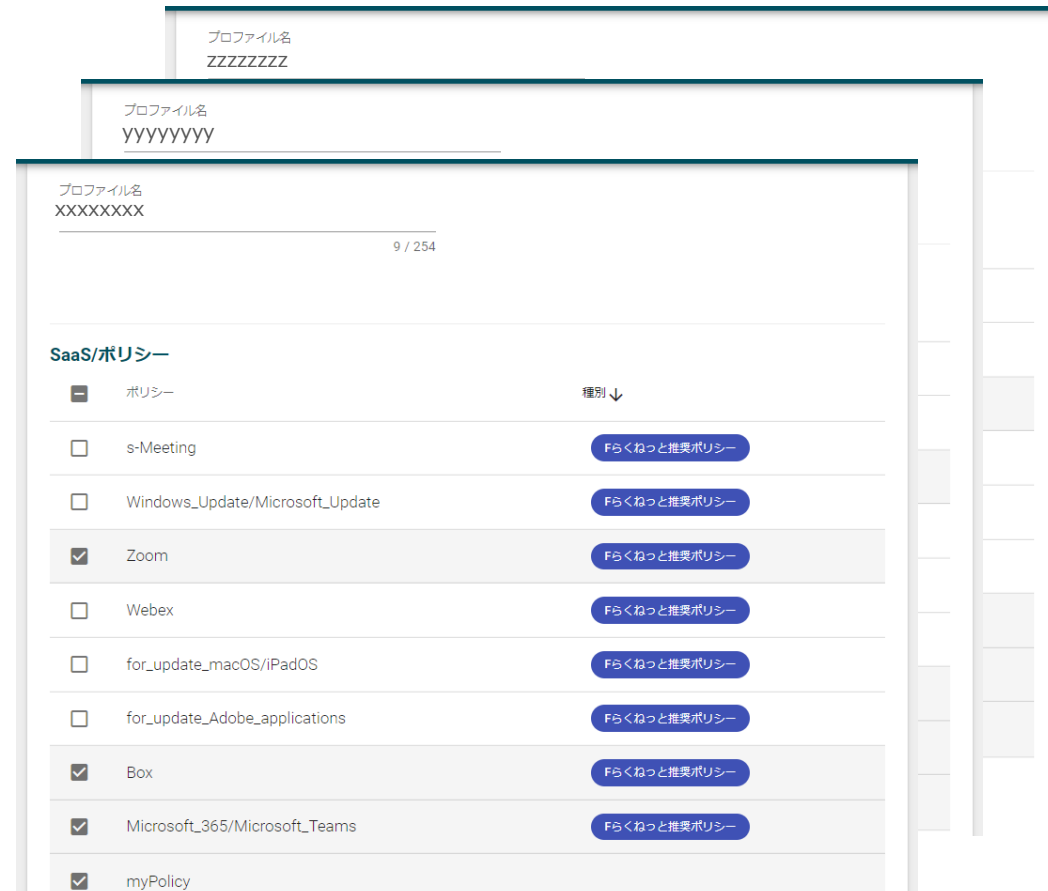


ローカルブレイクアウト (LBO) を導入したいけど…



- ・機器ごとにドメイン設定をつくる必要がある
- ・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…

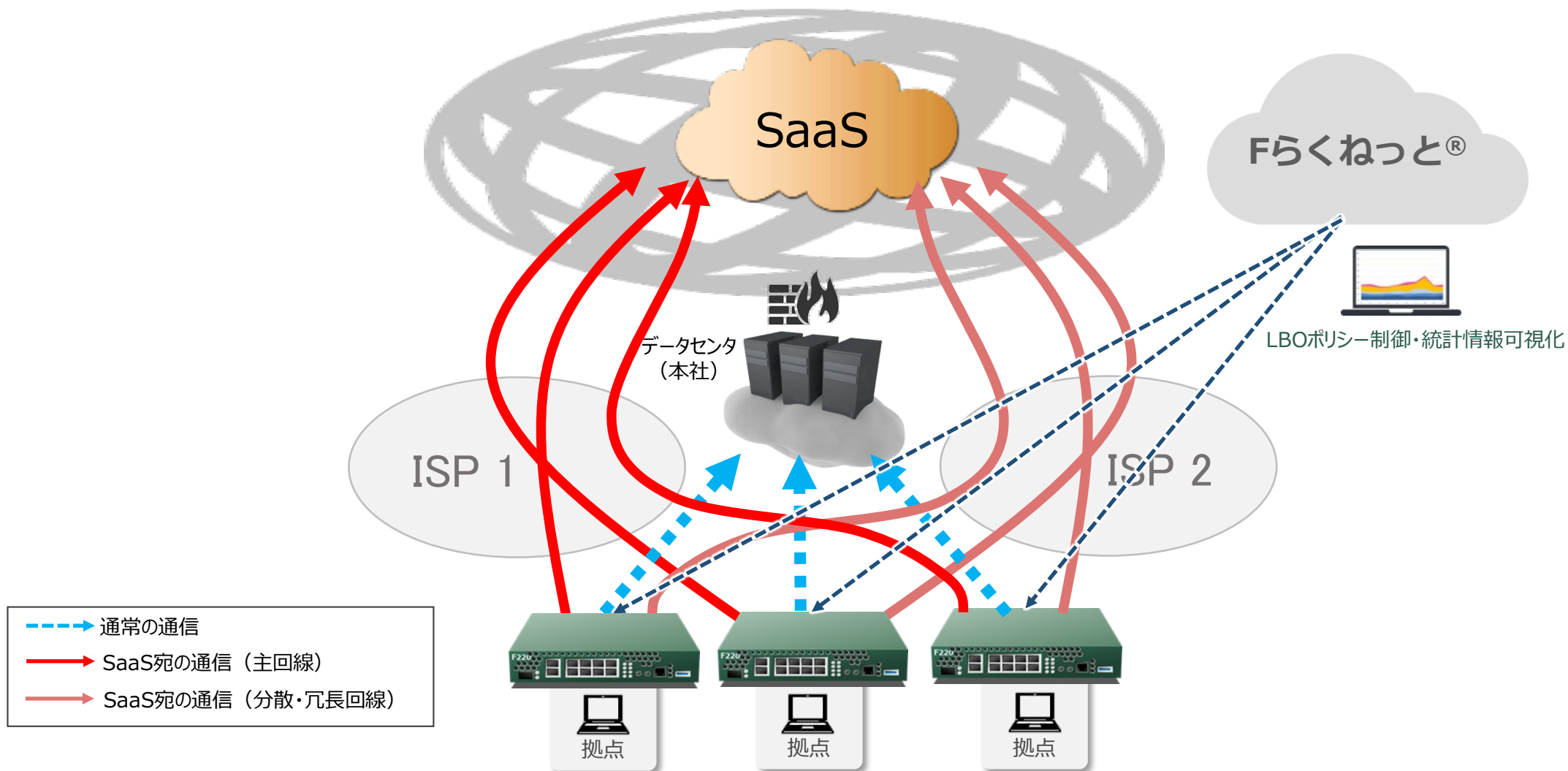


- ・SaaSのチェックだけでLBOできる！
- ・SaaSのドメインリスト更新に追従可(マイポリシー除く)

※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



*	特長	メリット
①	Proxyサーバ有無どちらにも対応！	<ul style="list-style-type: none"> • 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！	<ul style="list-style-type: none"> • 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 1.9Gbps、 F220/F221 3.0Gbps、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 20,000、 F220/F221 60,000
③	お客様の端末の設定やPACファイルが不要！	<ul style="list-style-type: none"> • 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！	<ul style="list-style-type: none"> • DPI方式のローカルブレイ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！	<ul style="list-style-type: none"> • 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

DNS snooping方式の設定

```
local-breakout enable
local-breakout A tunnel 1    … LBO先を指定
lbo-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)
- ③定義ファイルやスクリプトは必要なし

HTTP snooping方式の設定

```
ip name-server <DNSサーバ>    … DNS問い合わせ先を設定
!
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
!
Lbo-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
```

Fらくねっと®があればさらに簡単！

■ 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 break-out: 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 local-breakout session★: HTTP snoopingによりLBOしたTCPセッションを確認可能
- show local-breakout 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 local-breakout statistics: LBOの統計情報を確認可能
- show local-breakout 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 >」の経路に含まれる場合に、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 local-breakout sessionの変換テーブルにしたがってブレイクアウトします)。

■ show local-breakout 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 local-breakout 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 local-breakout 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 local-breakout 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
```


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

```
lbo-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/product/setting/pdf/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
!
lbo-profile A
dns-snooping enable
domain *.example1.com        ... LBO対象のドメインを指定
...
exit
!
lbo-profile B
dns-snooping enable
domain *.example2.com        ... 破棄対象のドメインを指定
...
exit
```

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

```
lbo-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 S2 ...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 local-breakout 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 :

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)
!
lbo-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	10,000経路	20,000セッション
	F220/F221 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	<ul style="list-style-type: none"> •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	<ul style="list-style-type: none"> •ProxyDNS併用動作 •LBO経路登録上限数設定 •LBO経路有効期間指定 	<ul style="list-style-type: none"> •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

- 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> □-カルブレイクアウト機能を使う

- 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*