

# SINET6のサービス について

---

2022年12月6日/20日  
国立情報学研究所

# SINET6のサービス（赤字：新サービス）

- 利用機関様からのご要望を基に、共考共創で新サービスを開発し、ご提供していきます

サービスメニュー		備考
L3サービス	インターネット接続（IPdual）+ フルルート提供	
	IPマルチキャスト（+QoS）	
	アプリケーション毎QoS	
	L3VPN（+QoS）	
L2サービス	L2VPN/VPLS（+QoS）	
	仮想大学LAN	
	L2オンデマンド（基本、国際連携API：NSI、クラウド連携API：REST）	
アクセス回線冗長化対応	マルチホーミング	
	リンクアグリゲーション（同速度）	
	リングアグリゲーション（異速度）	
	冗長トランクグループサービス	
	データセンタ接続冗長化サービス	7月より開始
ネットワーク運用安定化	DDoS Mitigation機能	
	新DDoS Mitigationサービス	実網で動作評価中
	恒速ファイル転送	
	BGP Looking Glass	8月より開始
	時刻情報提供（NTP）	
	分散セカンダリDNS	
転送性能向上	パフォーマンス計測（Perfsoner）	8月より開始
	Pingチェックサイト	

# (継続サービス) 多様なVPNサービス

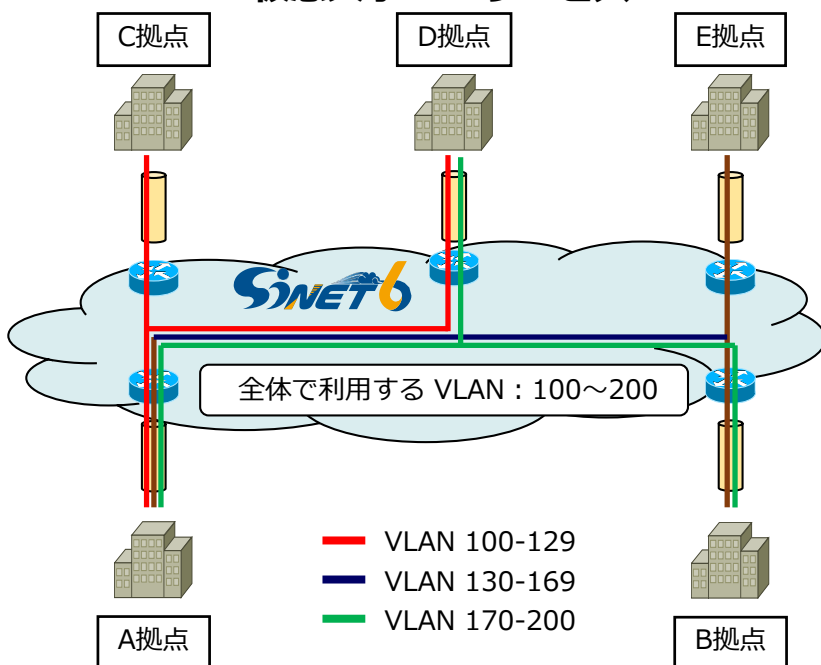
## ● 仮想大学LANサービス：

- 一度に100以上のレイヤ2 VPN設定が可能。複数対地間の同一VLAN間でVPNを構築
- 一部機関は1000VPN越えも

## ● レイヤ2 オンデマンドサービス：

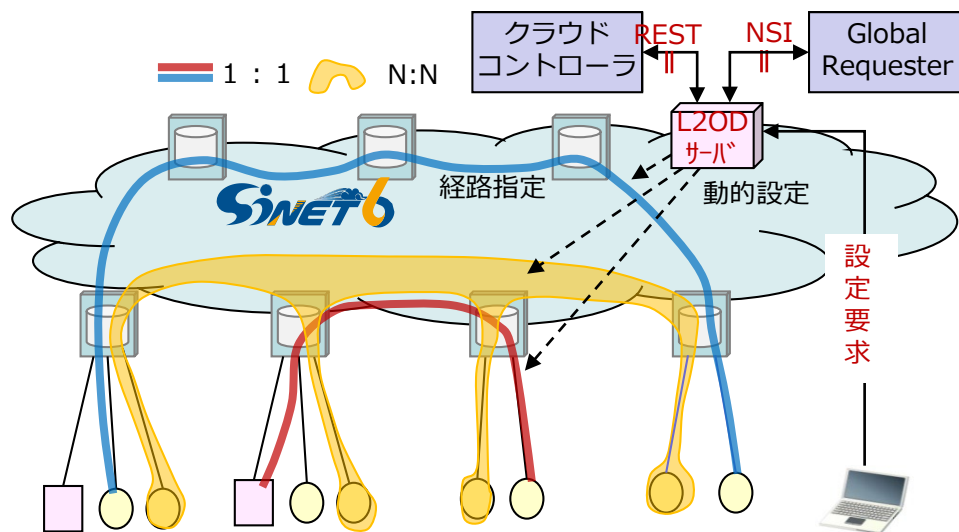
- 利用者自身でセルフプロビジョニングが可能。機関管理者にて任意のVLAN間でレイヤ2 VPNの設定／開放が可能

仮想大学LANサービス



申請した範囲内のVLANで自由に通信可能

レイヤ2 オンデマンドサービス



事前登録した回線間に自由にVPNを設定可能

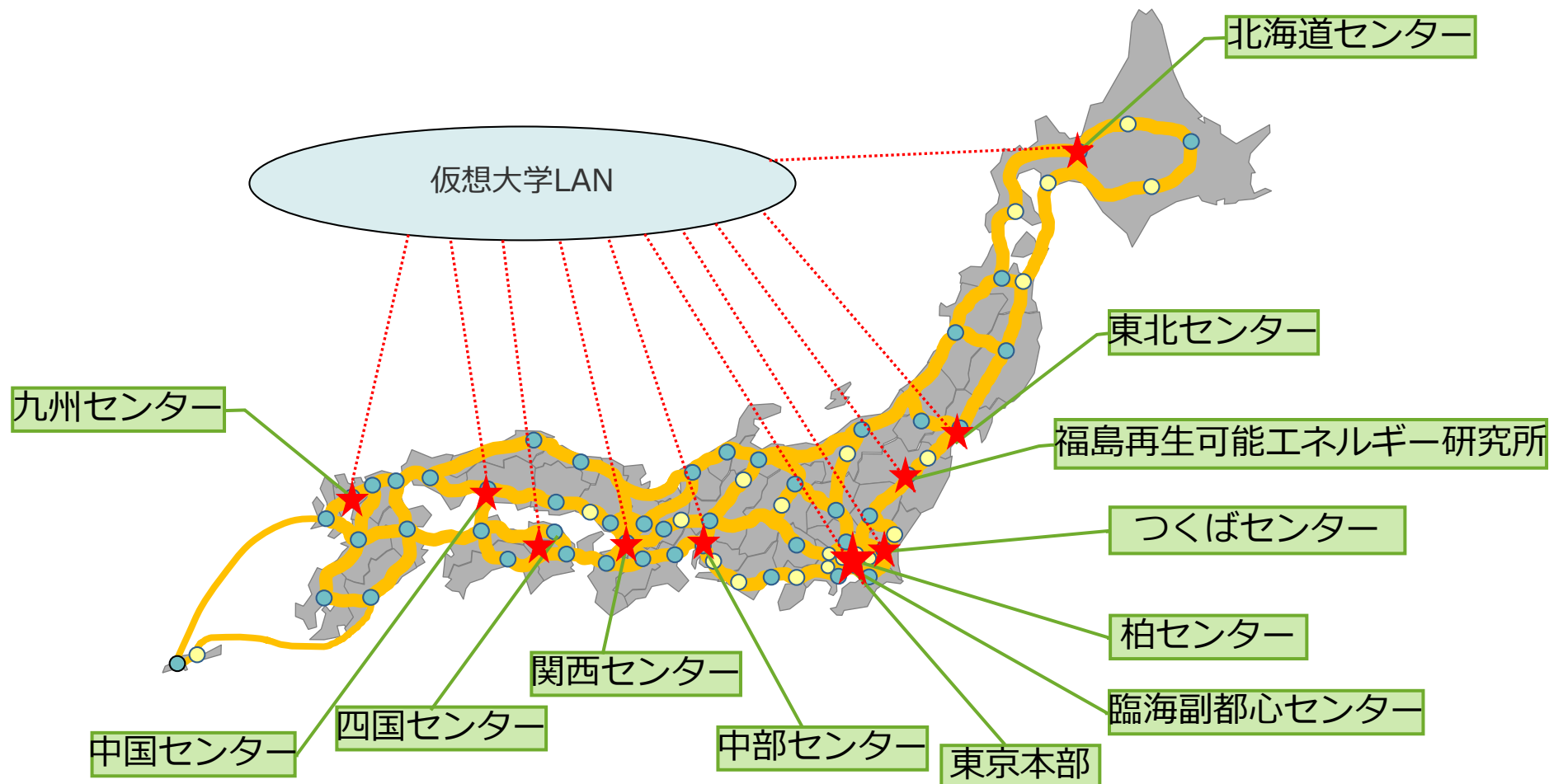
# VPNサービスの比較

	L2VPN/VPLS	L2オンデマンド	仮想大学LAN
VPNの構成メンバー	単一機関や他機関とも可能	同左	単一機関を想定
VPNの安全性	VLAN論理分割、暗号化なし	同左	同左
利用VLAN数目安	数個程度	10個程度	100個程度
利用可能なVLAN番号	2～4094	同左	同左
VLAN番号の調整	不要（SINET機器でVLAN変換、各拠点任意のVLAN番号で接続）	同左	必要（SINET内でVLAN変換不可、使用するVLAN番号を全拠点で揃える）
VLAN番号の指定	1個ずつ指定	範囲で指定	範囲で指定
利用申請	2段階申請（VPN利用開始申請、サービス利用申請）	2段階申請（L2ODサーバ登録申請、L2ODサービス申請）	仮想大学LAN申請の1通のみ
VLANの設定作業	SINETオペセンが設定	利用者がWeb操作で設定	VLANを自動認識
VLANの変更申請	必要（変更の都度必要）	不要（申請時の範囲内なら不要）	同左
QoS／経路制御	低廃棄、高廃棄	低廃棄、高廃棄、優先制御、帯域指定、経路制御	なし
クラウド接続サービスとの併用	可能	同左	利用したいサービスを提供するクラウド事業者に要確認

# 仮想大学LANの利用例

## • 産総研による仮想大学LANサービスの利用例

- 10以上の拠点間をSINETに接続し、仮想大学LANで接続
- 拠点を意識しないシームレスな通信環境を実現

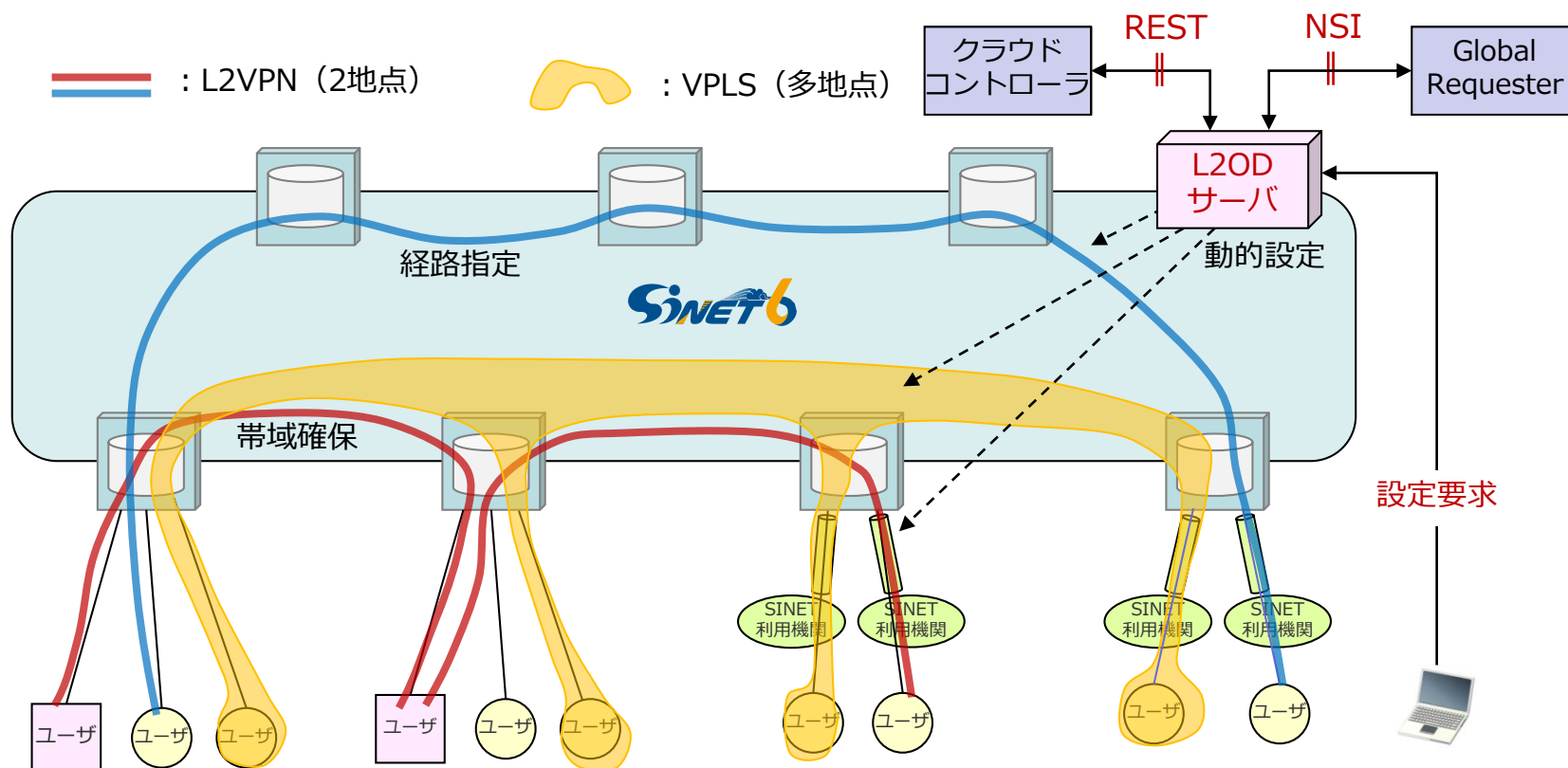


# L2オンデマンド（L2OD）サービス

- 簡単な操作でレイヤ2 VPNのセルフプロビジョニングが可能です

- レイヤ2 VPN（L2VPN/VPLS）の設定を行う候補拠点（2箇所以上）をSINETへ申請いただきます
- 機関様にて、L2ODサーバを介してVPN設定予約（※）を行います  
→設定予約に基づきレイヤ2 VPNが設定され、地点間での通信が可能となります

（※）VPN情報を登録先のメールに通知します



# L2VPN方式とVPLS方式の違い

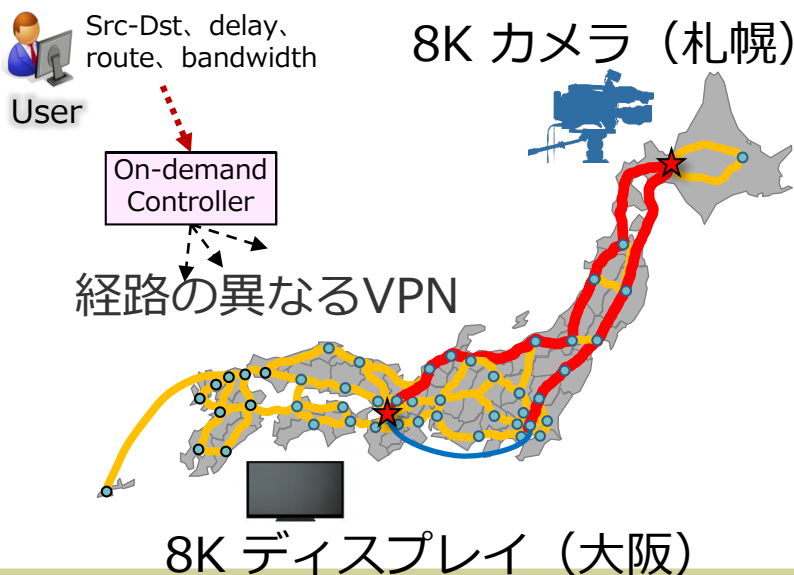
- L2VPN方式とVPLS方式で利用できる機能に違いがあります。
  - 経路指定や優先的なQoS制御指定・帯域指定のオプションを必要とする場合はL2VPN方式になります。
  - 3拠点以上でVPNを張る場合はVPLS方式になります。

	L2VPN	VPLS
接続地点数	2地点のみ	2地点以上可能
経路指定	可能 (指定しない場合は最短経路)	不可、最短経路
QoS制御	低廃棄、高廃棄 転送クラスによる優先的なQoS制御指定 と帯域指定も可能	低廃棄、高廃棄のいずれか
長期間予約	可能 (優先的なQoS制御指定と帯域指定は利 用不可)	可能
その他		接続対地の追加・削除が可能

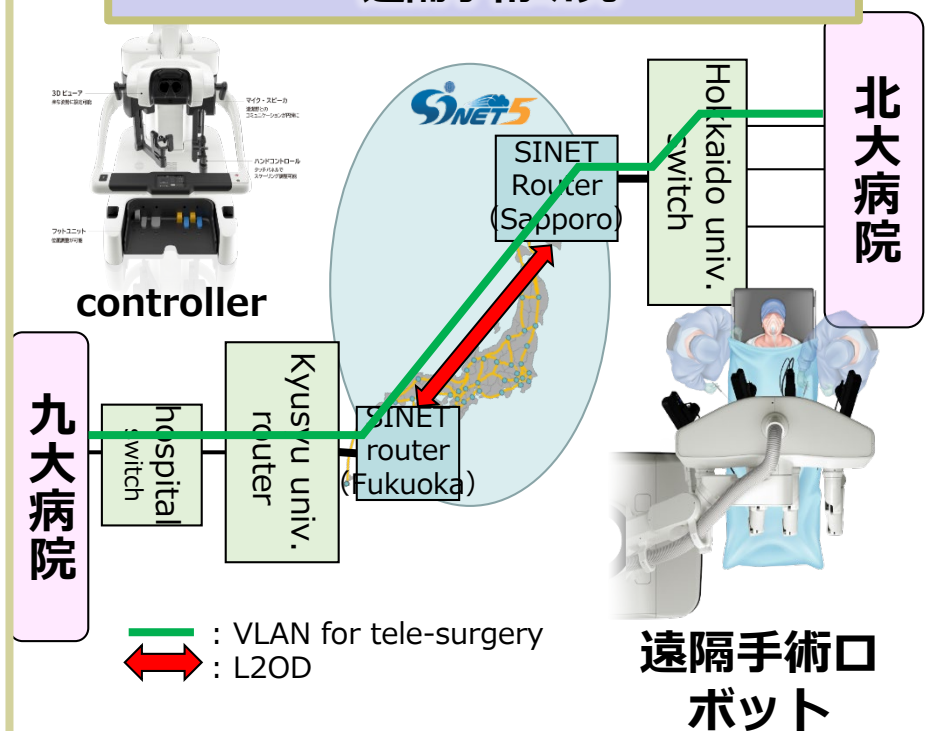
- 100Gbps超の高精細8K 映像転送技術の実証
  - 2つのVPNを異なる経路を用いて設定し、100G超転送を実現
- 遠隔手術において、通信速度が操作性に与える影響を評価
  - 帯域指定VPNを設定することで、多様な通信速度を模擬

## 100Gbps超の8K 映像伝送研究

110 Gbps の映像を2つの異なる経路を通るVPNを用いて転送



## 遠隔手術研究





# L20DサービスのGUI画面

## ・4ステップの操作で設定を行います

https://nwcs6.sinet.ad.jp/nwcs/faces/app/nwcsLo...

### ログイン画面

NWCS

ユーザID  
demouser

パスワード  
\*\*\*\*\*

ログイン

[パスワードをリセット](#)

[学術認証でのご利用はこちら](#)

English demouser

### ステップ1 研究グループ選択

VPN管理 > VPN設定 > VPNグループ選択

1 VPNグループ選択 2 VPN選択 3 ポート選択 4 予約

グループ 研究プロジェクト 加入機関サイト VPI

☐ test-v test-vpn-P 仙台サイト 0

<< < 1 > >>

次へ

English demouser

### ステップ3 VPN拠点の選択

VPN管理 > VPN設定 > VPNグループ選択 > VPN選択 > ポート選択

1 VPNグループ選択 2 VPN選択 3 ポート選択 (VPN作成) 4 予約

グループ名 test-vpn-G  
研究プロジェクト test-vpn-P  
VPN名  
種別 ☒ VPLS ☐ L2VPN

加入機関サイト	VLAN
<input type="checkbox"/> 仙台サイト	3001
<input type="checkbox"/> 新潟サイト	3007
<input type="checkbox"/> 大阪サイト	3003
<input type="checkbox"/> 広島サイト	3001

<< < 1 > >>

次へ

English demouser

### ステップ2 VPNの種類選択

VPN管理 > VPN設定 > VPNグループ選択 > VPN選択

1 VPNグループ選択 2 VPN選択 3 ポート選択 4 予約

グループ名 test-vpn-G  
研究プロジェクト test-vpn-P

VPN名	種別	加入機関サイト	VLAN	状態
	選択			選択

レコードがありません

<< < > >>

VPLS追加 L2VPN追加 更新

English demouser

### ステップ4 VPN利用期間の設定

VPN管理 > VPN設定 > VPNグループ選択 > VPN選択 > ポート選択 > 予約

1 VPNグループ選択 2 VPN選択 3 ポート選択 4 予約 (VPN作成)

グループ名 test-vpn-G  
研究プロジェクト test-vpn-P  
VPN名 test-vpn  
種別 ☒ VPLS ☐ L2VPN

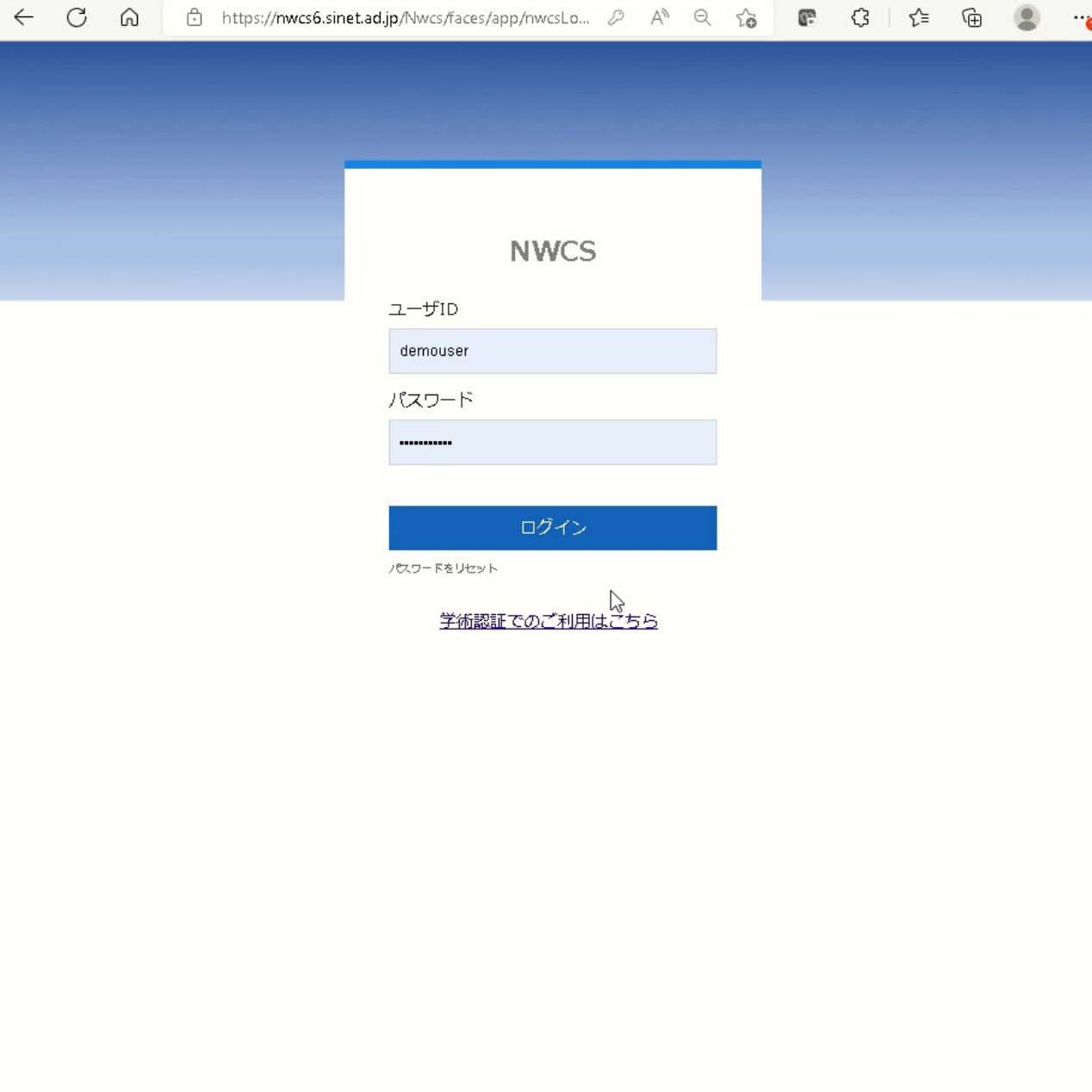
開始日時 ☐ 2022/08/22 12:39  
終了日時 2022/08/22 12:40  
転送クラス ☒ BE (標準) ☐ BE (高遅延)

加入機関サイト	VLAN
仙台サイト	3001
新潟サイト	3007

<< < 1 > >>

予約

# L20DサービスのGUI操作例



← ↻ 🏠 🔒 https://nwcs6.sinet.ad.jp/Nwcs/faces/app/nwcsLo... 🔍 ☆ 🗑️ ⚙️ | ☆ 🗑️ 👤 ...

## NWCS

ユーザID

demouser

パスワード

\*\*\*\*\*

ログイン

[パスワードをリセット](#)

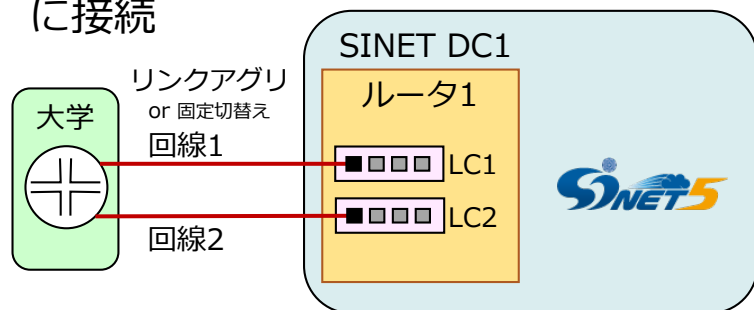
[学術認証でのご利用はこちら](#)

# データセンタ接続冗長化サービス

- データセンタ接続冗長化サービスをご用意頂くことにより、通信環境の信頼化が可能です

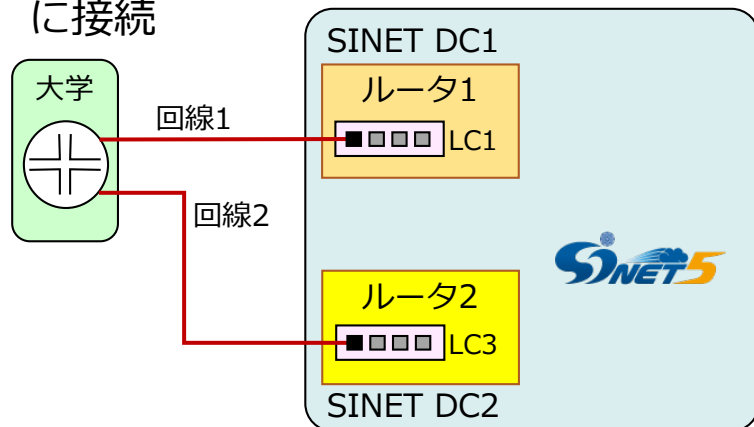
## 方式1：ルータの異なるラインカードに収容

- 2本のアクセス回線を SINET DC1 に接続



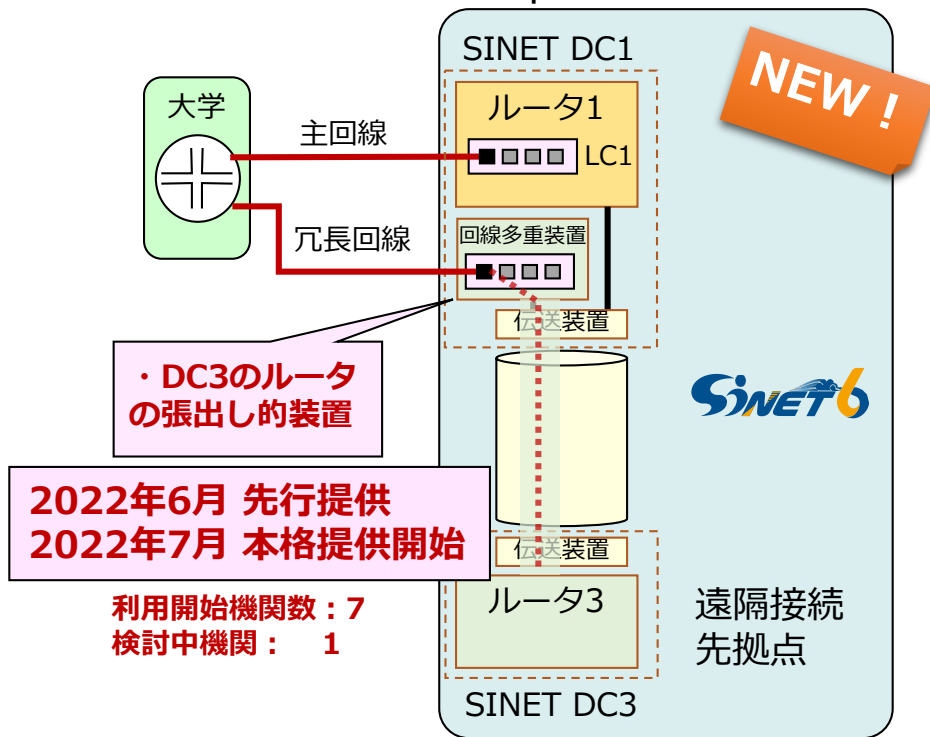
## 方式2：異なるDCのルータに収容

- 2本のアクセス回線を SINET DC1とDC2 に接続



## NEW: データセンタ接続冗長化サービス

- 2本のアクセス回線を SINET DC1 に接続
- 冗長回線をSINET DC1経由で別DCのルータに収容
- 冗長回線は原則10Gbpsまで



# 異なるDCのルータへの収容

- 遠隔接続先拠点としてエリアごとに1ないし2拠点を設け、各拠点毎に決められた遠隔接続先拠点へ接続します

遠隔接続先拠点：

○ エリアの接続拠点

北海道エリア（室蘭）

東北エリア（福島、新潟）

関東エリア（千葉、甲府）

中部エリア（浜松）

近畿エリア（奈良、大津）

中国エリア（岡山）

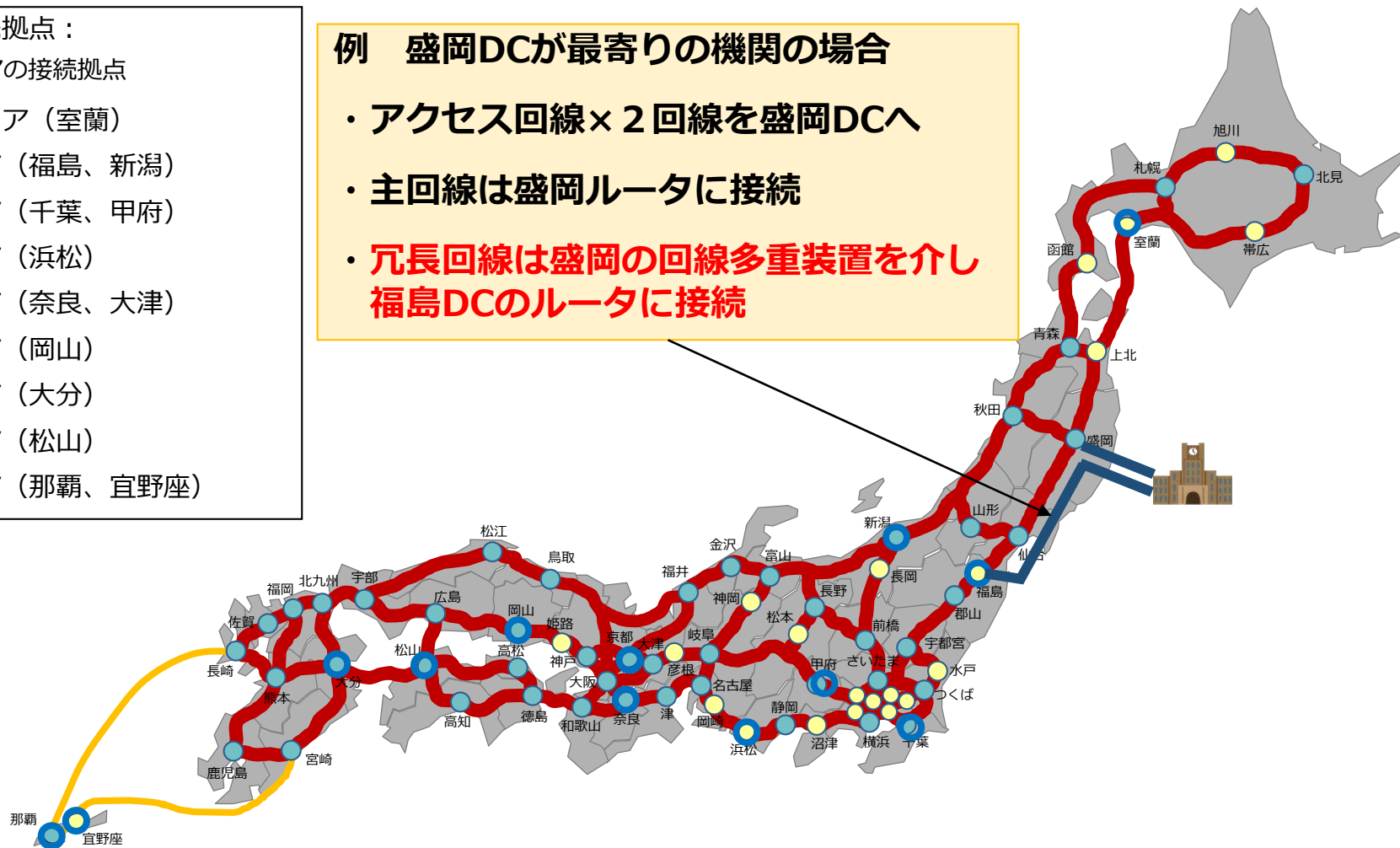
九州エリア（大分）

四国エリア（松山）

沖縄エリア（那覇、宜野座）

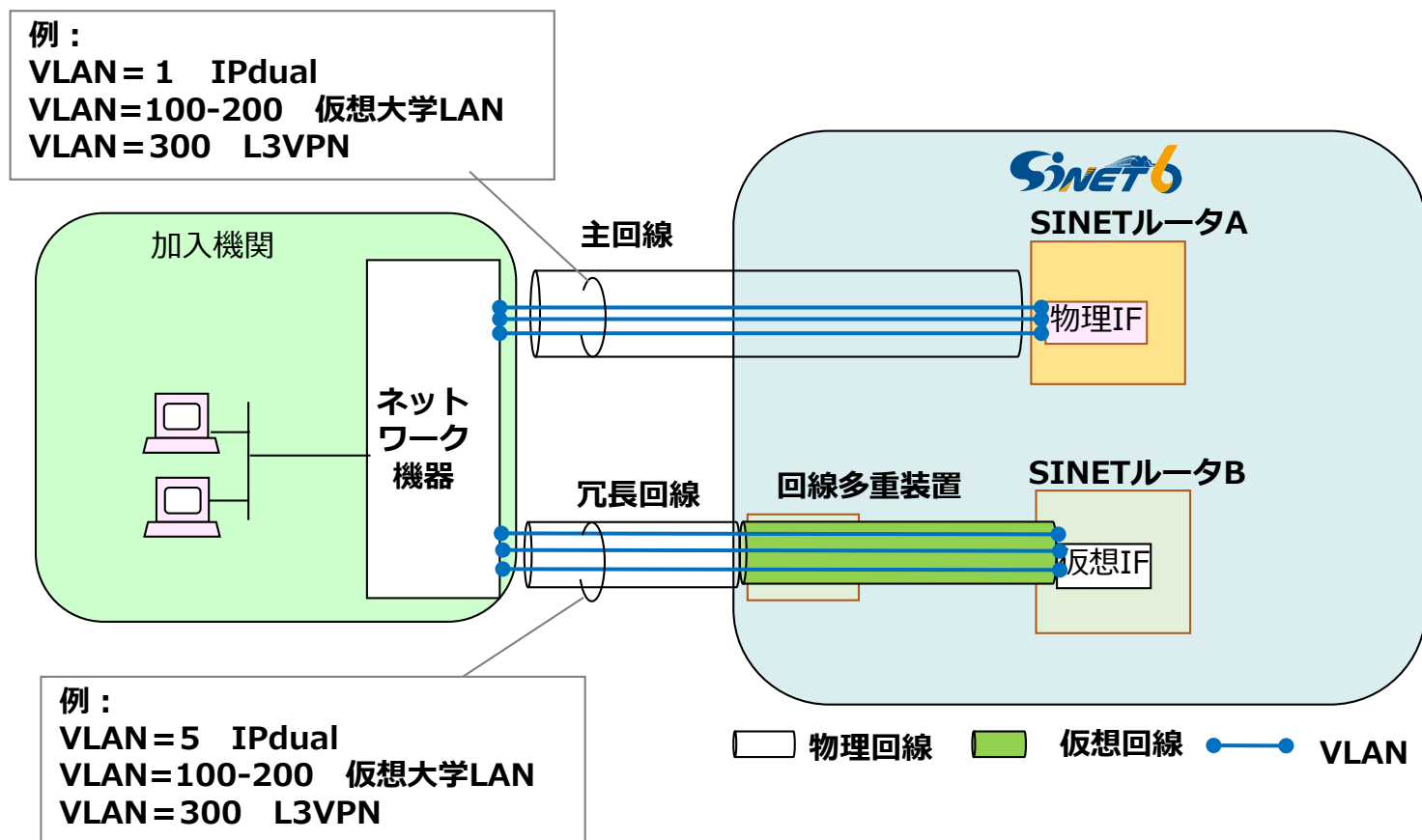
## 例 盛岡DCが最寄りの機関の場合

- アクセス回線×2回線を盛岡DCへ
- 主回線は盛岡ルータに接続
- 冗長回線は盛岡の回線多重装置を介し福島DCのルータに接続



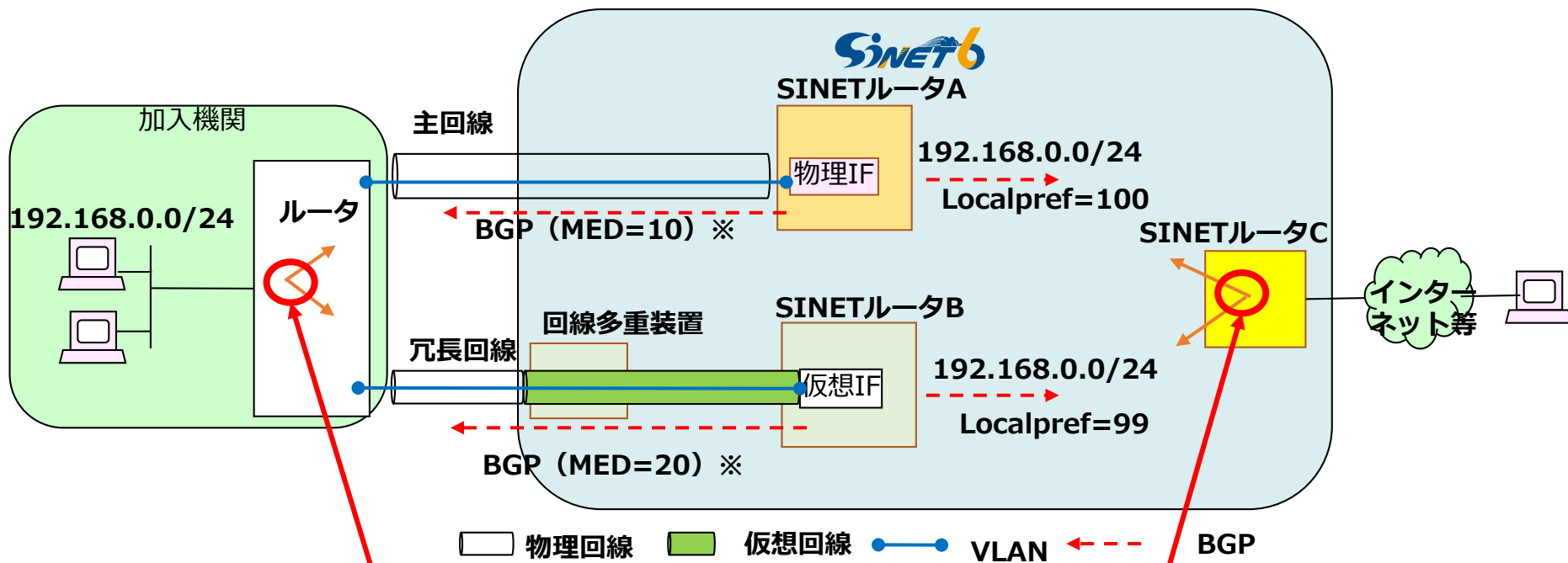
# 切り替え可能なSiNETサービス

- 本サービスでは、主回線にて利用されているサービスをまとめて冗長回線に切り替えることが可能です
  - インターネット接続サービス (IPdual)、L3サービス (L3VPN)
  - L2サービス (VPLS、仮想大学LAN)



# インターネット接続/L3サービス

- インターネット接続サービス (IPdual)、L3サービス (L3VPN) では、機関側ルータとSINETルータの間で通信プロトコル (BGP) を設定することで故障時に自動切替が可能です

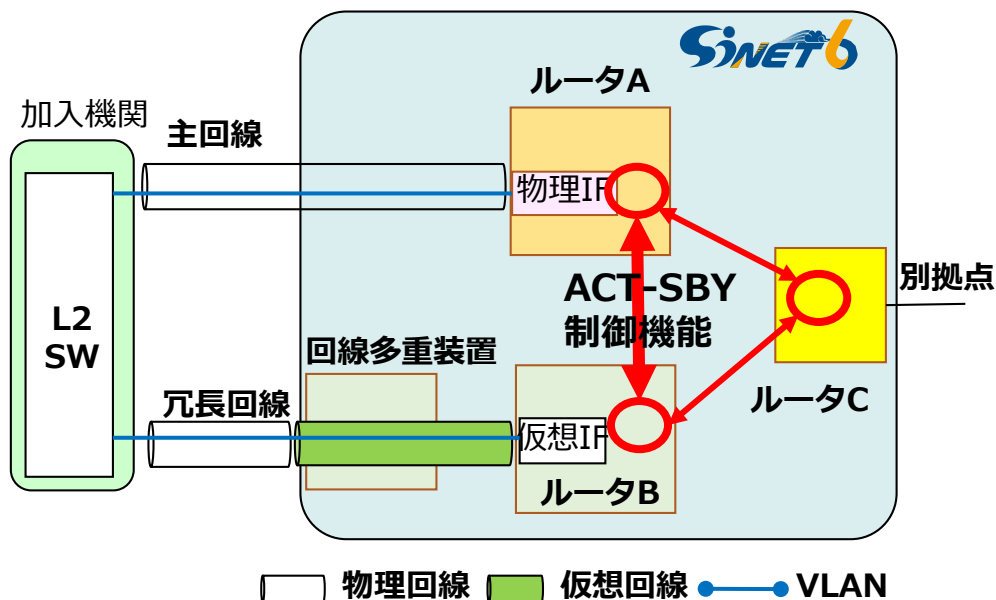


加入機関からSINET向けトラフィックは、主回線を優先的に選定  
※BGPのMED値を参照することも可

SINETから加入機関向けトラフィックは、BGPのlocalpref値を参照し経路選択

# L2サービス

- L2サービス（VPLS／仮想大学LAN）では、SINET内にAct-Standby制御機能を適用し運用します
- 加入機関装置とSINET装置間に通信プロトコル（STP等）は不要です
- 切替が遅くなる特殊なケース（※）でのご利用の場合はご注意ください



## Act-Standby制御の動作

- SINET内で拠点間の死活をチェック
- 正常時：ルータAに転送
- ルータA障害時：ルータBに切替て転送

## ※特殊なケース

- 加入機関から別拠点に対して片方向でパケット送信を行っている場合
- 加入機関L2SWのMAC学習のExpireタイマーが切れるまで、切り替わらない可能性があります。
- このような利用ケースの場合、双方向通信を行うことで直ちに切り替わります

## 通常のケース

- 加入機関と別拠点間で双方向でパケットの送受を行っている場合
- 加入機関L2SWにてMAC学習が行われ、素早く（数100ms程度）で切り替わります

# 新DDoS Mitigationサービス

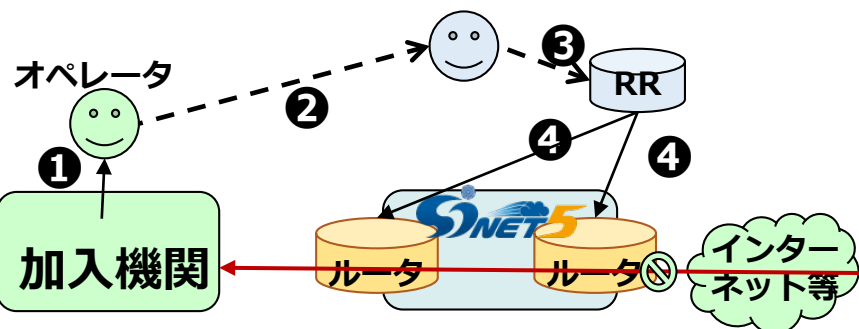
- DDoS攻撃に自動的に防御を行うための新サービス（実網で動作評価中）
  - SINET内にDDoS攻撃検知機能を配備
  - サービス申請に基づき検知対象IPアドレスを設定
  - DDoS攻撃検知後10秒程度でパケットフィルタを自動設定（モニタのみも選択可能）

## DDoSミティゲーションサービス

申し込みから廃棄設定完了まで数時間以上

- ① DDoS検出
- ② ミティゲーション申請
- ③ RRにパケット廃棄設定
- ④ ルータのフィルタ設定

SINET受付

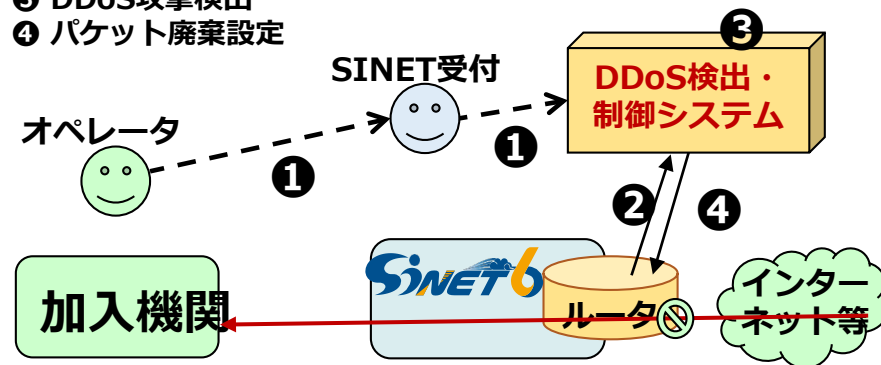


## 新DDoSミティゲーションサービス

検出から廃棄設定完了まで10秒程度

- ① サービス申請（DDoS対象アドレス登録）
- ② 情報収集
- ③ DDoS攻撃検出
- ④ パケット廃棄設定

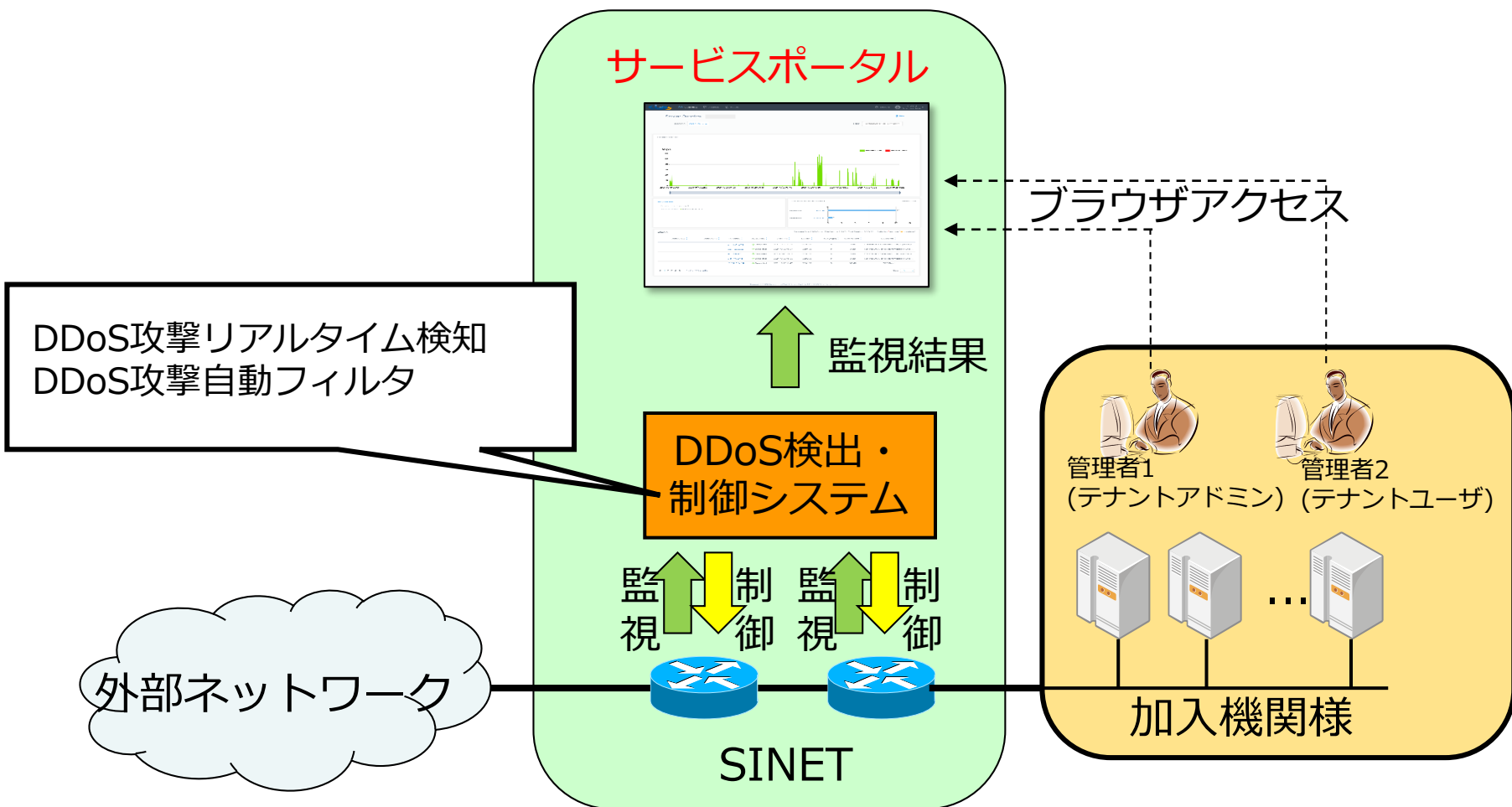
SINET受付





# 攻撃検知結果の確認について

- サービスポータルにアクセスすることで、新DDoS Mitigationサービスによる攻撃検知結果をお手元のブラウザにてリアルタイムにご確認いただけます



# サービスポータル概要

## • トラフィック量のグラフ表示

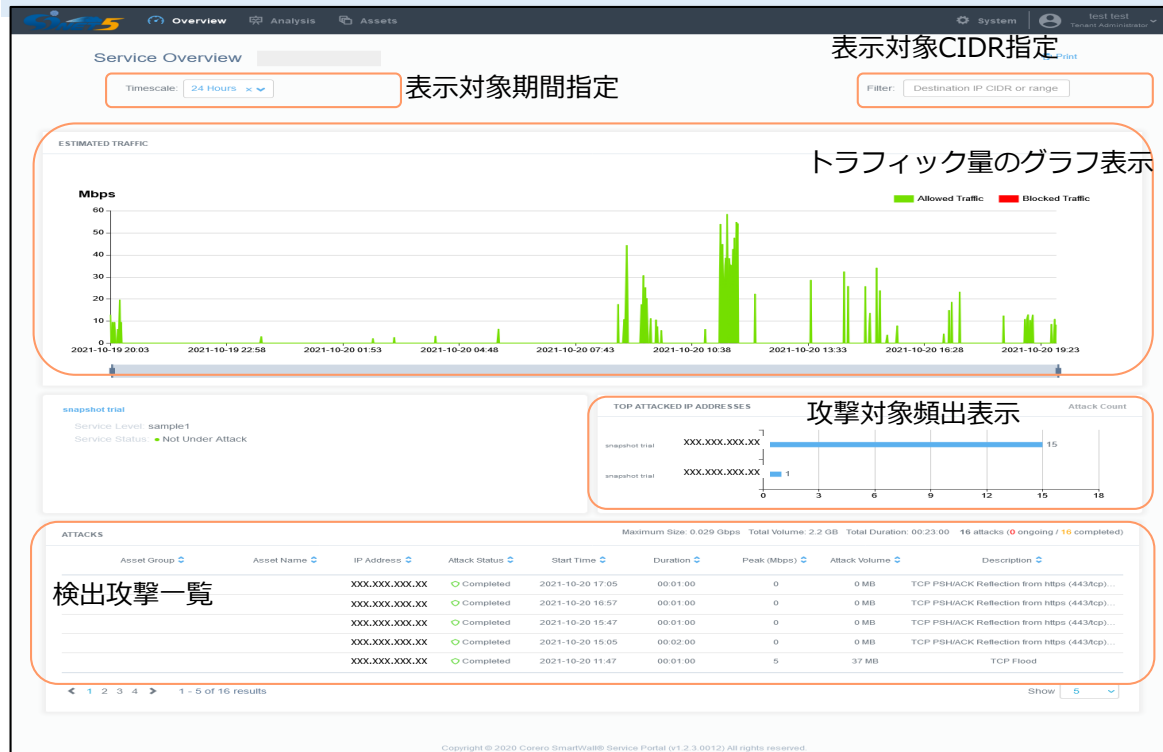
- 加入機関様ネットワークに入力するトラフィック量の時間推移グラフを表示
- 破棄したDDoS攻撃トラフィック量のグラフ表示も対応

## • 攻撃対象IPアドレス頻出表示

- 加入機関様ネットワークで攻撃対象となったIPアドレスの頻出ランキングを表示

## • 検出攻撃一覧

- 加入機関様ネットワークに対する攻撃検知の一覧を表示
  - 攻撃対象IPアドレス、検知期間、検出トラフィック量等



- ブラウザ表示
- メールレポート機能
- ログインユーザ管理

## 検出攻撃毎のグラフ表示

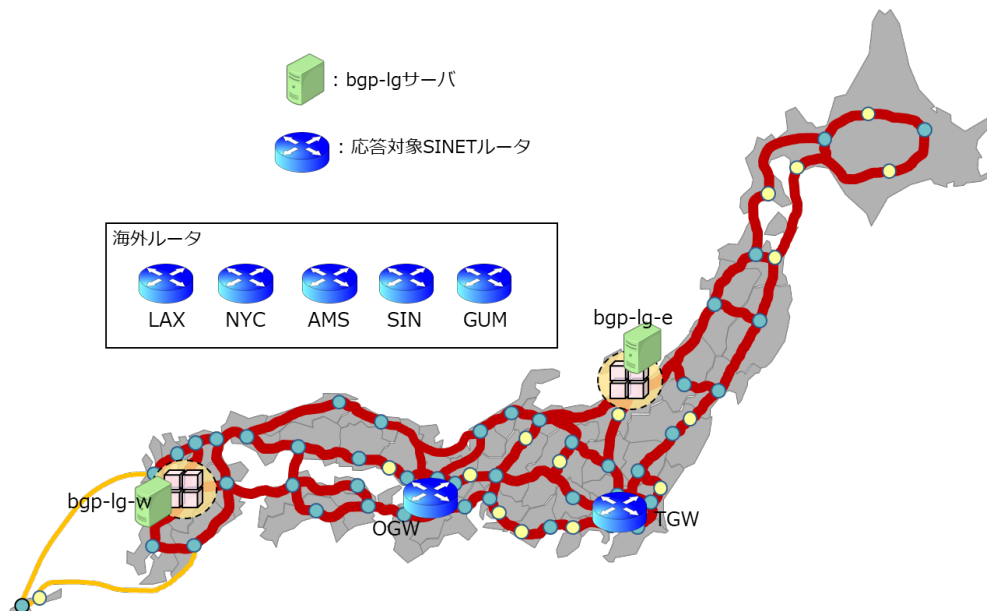


# BGP looking glass

- SINET加入機関（及びR&Eコミュニティ）にBGPルーティング情報を提供
  - URLは、<https://bgp-lg-e.sinet.ad.jp>, <https://bgp-lg-w.sinet.ad.jp>
  - 応答対象のルータ：海外5ルータと東京・大阪ゲートウェイの計7か所（下図参照）
  - サービス継続性の為、新潟・熊本に2台構成でサービス提供
  - BGPルーティング情報の提供に対応。
- ルーティング情報に興味のある研究者・学生の方に、使って頂きたい

NEW!

## SINET6 BGP looking glass 全体構成

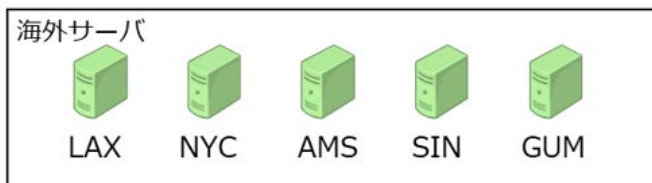
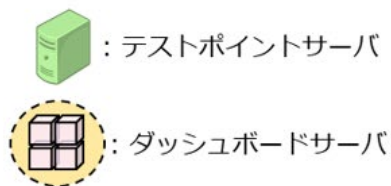


## SINET6 BGP looking glassの画面

# SINET6 PerfSONAR (Update)

- SINET加入機関（及びR&Eコミュニティ）にネットワーク性能計測サービスを提供
  - 計測（テストポイント）サーバ： 国内11カ所，海外5カ所（下図参照）

## SINET6 PerfSONAR全体構成



## SINET6 PerfSONARの特徴（S5比）

- 国内テストポイント100G化（S5は40G）
- 国内テストポイントが1カ所増（S5は10）

# SINET6 PerfSONARの特性

- ・ IPアドレスに基づき利用者を分類し、実施可能なテストを制限（下表参照）

## 利用者分類と実施可能テスト

分類	分類基準	実施可能テスト
優先利用者	ESNETが提供する学術教育機関（REN）一覧(*)に掲載されたIPアドレス（ <b>SINET加入機関は通常含まれる</b> ）	スループットテスト: テスト時間: 120秒まで, コネクション数: 20まで. UDP利用: 10Gbpsまで それ以外: "latency", "latencybg", "rtt", "trace", "clock", "dns", "simplestream"
利用禁止者	REN・SINET加入機関以外で悪質利用者とSINETで判定したIPアドレス（現在無し）	全て禁止
普通利用者	上記以外	スループットテスト: テスト時間: 60秒まで, コネクション数: 2まで. UDP利用不許可. それ以外: "latency", "latencybg", "rtt", "trace"

(\*) [http://stats.es.net/sample\\_configs/pscheduler/ren](http://stats.es.net/sample_configs/pscheduler/ren)

# 共考共創

ご清聴ありがとうございました！