

VPN系サービス・技術・利用例

平成29年6月8日
国立情報学研究所

- ◆ SINETのVPNサービスとは
 - ・ VLANの設定の仕方
 - ・ L2VPNの接続構成
 - ・ L3VPN
 - ・ VPN利用申請手続き
 - ・ タグVLAN接続への変更申請
- ◆ 仮想大学LANサービス
- ◆ L2オンデマンドサービス

ネットワークサービス

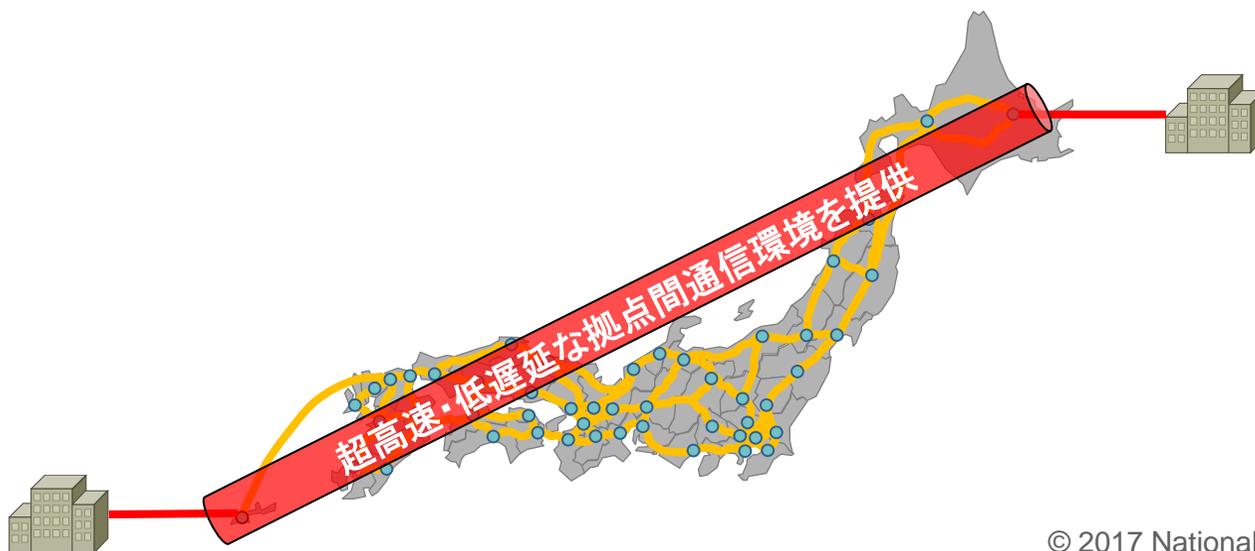
	サービスメニュー	SINET5	SINET4
L3 サービス	インターネット接続 (IPv4&IPv6)	○	○
	[オプション] QoS	○	○
	[オプション] フルルート提供	○	○
	[オプション] マルチホーミング	○	○
	[オプション] IPv6 トンネル接続	△*1	○
L2 サービス	IPマルチキャスト (IPv4&IPv6)	○	○
	[オプション] QoS	○	○
	L3VPN*2	○	○
	[オプション] QoS	○	○
	[オプション] VXLANアクセス New	予定	×
L2 サービス	L2VPN/VPLS	○	○
	[オプション] QoS	○	○
	[オプション] VXLANアクセス New	予定	×
	L2オンデマンド	○	Trial
L1 サービス	仮想大学LAN New	○	×
	L1オンデマンド	×*3	○
	波長専用線 New	○*4	×

*1: 新規受付は終了し、SINET5期間内に廃止予定。
IPv4/IPv6デュアル接続への移行をご検討ください。
*2: L3VPNでのIPマルチキャスト利用は、ご相談ください。

*3: 100Gbps化に伴い、L2オンデマンドに統合。
*4: 利用機関の費用負担で提供。1波長は100Gbps。

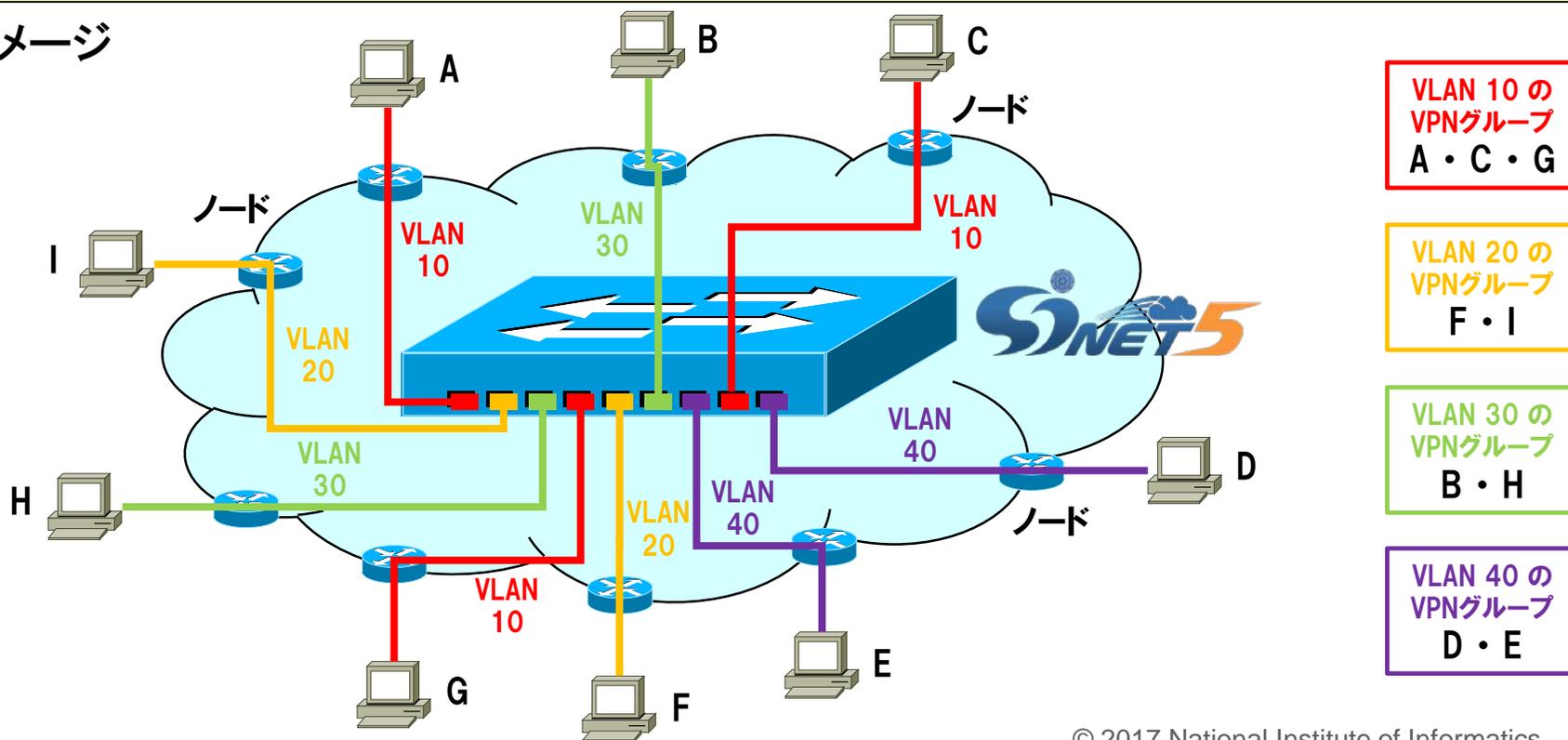
SINETのL2VPNサービスとは

- ◆ L2VPNサービスは拠点間を同一のセグメント(レイヤ2)で閉域網を提供する接続サービスです。
- ◆ インターネットから分離されたネットワークを提供しますので安全です。
- ◆ 共同研究等による複数の加入機関間VPNや、複数のキャンパス(遠隔地にあるオフィス等も対象)を持つ加入機関のキャンパス間通信や、SINETクラウド接続サービス等、様々な場面で利用されています。
- ◆ SINET5の全国100Gフルメッシュで超高速・低遅延な回線を利用したVPN接続が経済的に実現できます(広域イーサネットだと高額、インターネットVPNだと低速、・・)。
- ◆ L2 (レイヤ2)サービスなので、TCP/IP以外のプロトコルも利用可能ですが、現在のところ、スパンニングツリープロトコル(STP)は利用できません。



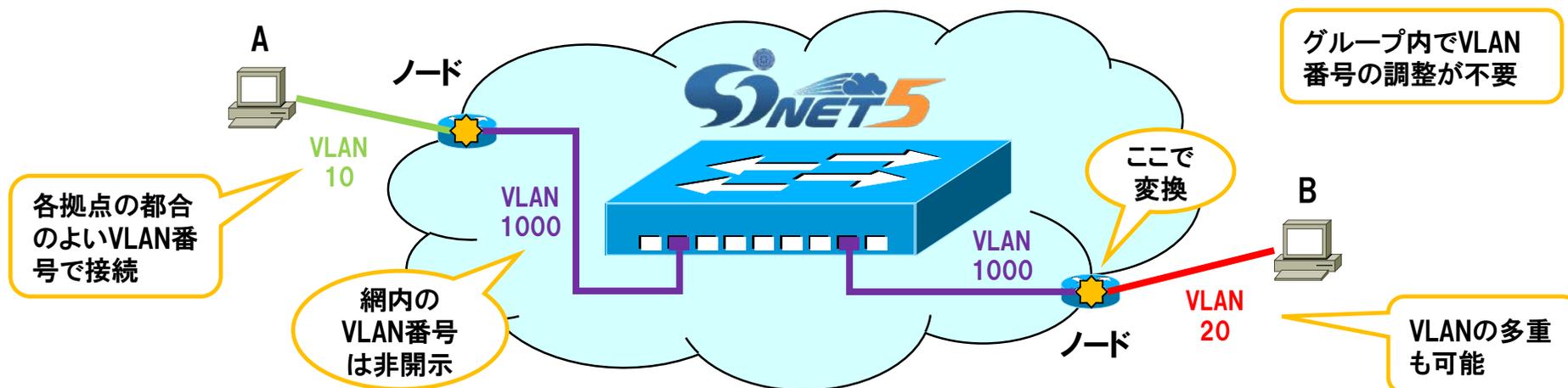
- ◆ SINETを巨大なレイヤ2スイッチ(L2SW)だとイメージしてください。
- ◆ L2SWなので同じVLAN番号に属するグループ間でしか通信できません(安全)。
- ◆ VLANによる論理分割なので、VPN装置は不要です。暗号化はされませんが、速度の低下がありません(高速)。
- ◆ L2(レイヤ2)サービスなのでSINET機器からping等による疎通確認が難しい点にはご注意ください(MACアドレスの確認は可能)。

L2VPNのイメージ



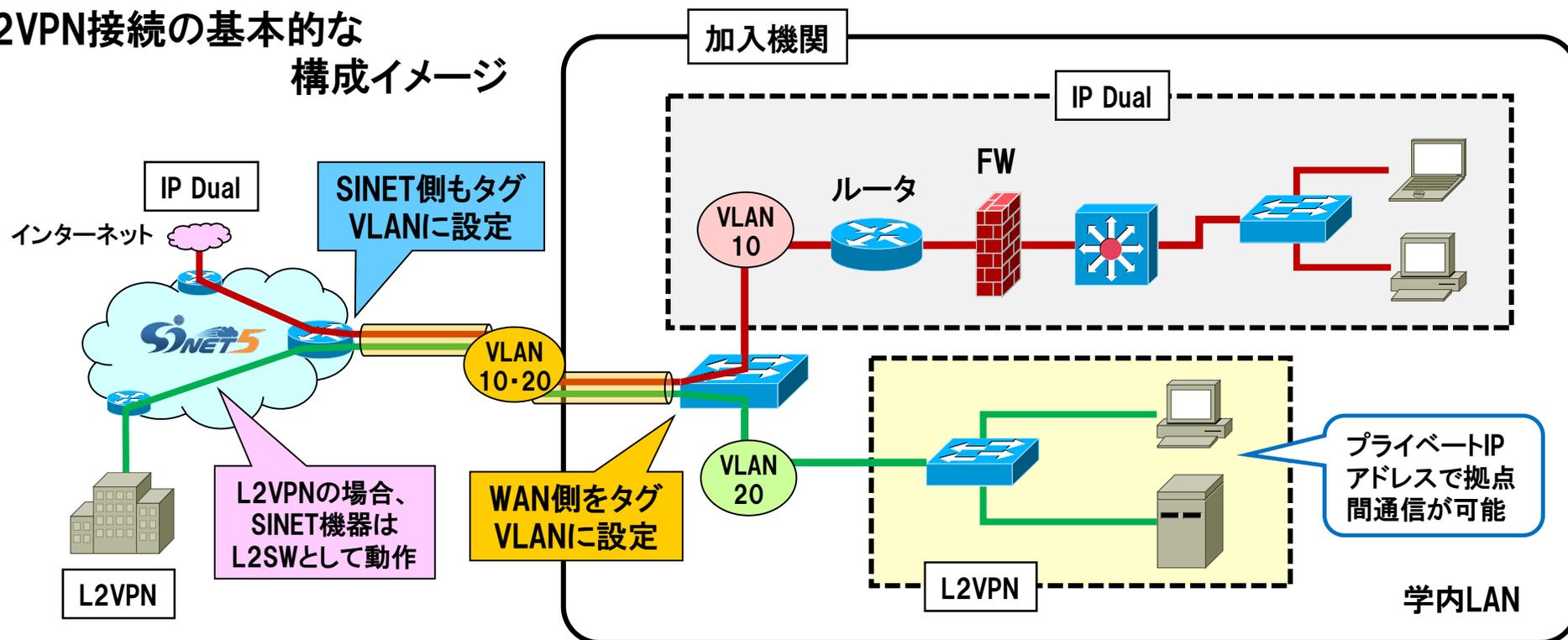
- ◆ SINET網内でVLAN変換をしますので、各拠点から異なるVLAN番号でSINETに接続することが可能です(VLAN番号の統一不要)。
- ◆ 他拠点を気にせずに、自拠点のネットワークの都合でVLAN番号を決めることができます。
- ◆ VLAN番号は2～4094の範囲で自由に指定できます(デフォルトVLANは不可)。
- ◆ VLANの変換はノードのSINET機器で行いますので、SINET網内の設定は気にしないでください。(SINET網内情報は非開示)。
- ◆ 1本の物理回線に複数のVLANを多重することも勿論可能です。

拠点側とSINET網内のVLANのイメージ



- ◆ IP Dual(インターネット)接続用とL2VPN接続用のVLANを分けて同一の物理回線で両サービスを利用できます(経済的)。
- ◆ 加入機関のWAN側にL2SW等を設置し、タグVLANでSINETと接続します。
- ◆ SINETとアンタグで接続している場合は、まず初めにタグVLAN接続に変更します。
- ◆ また、インターネットとの通信がありませんので、プライベートIPアドレスが使用できます。

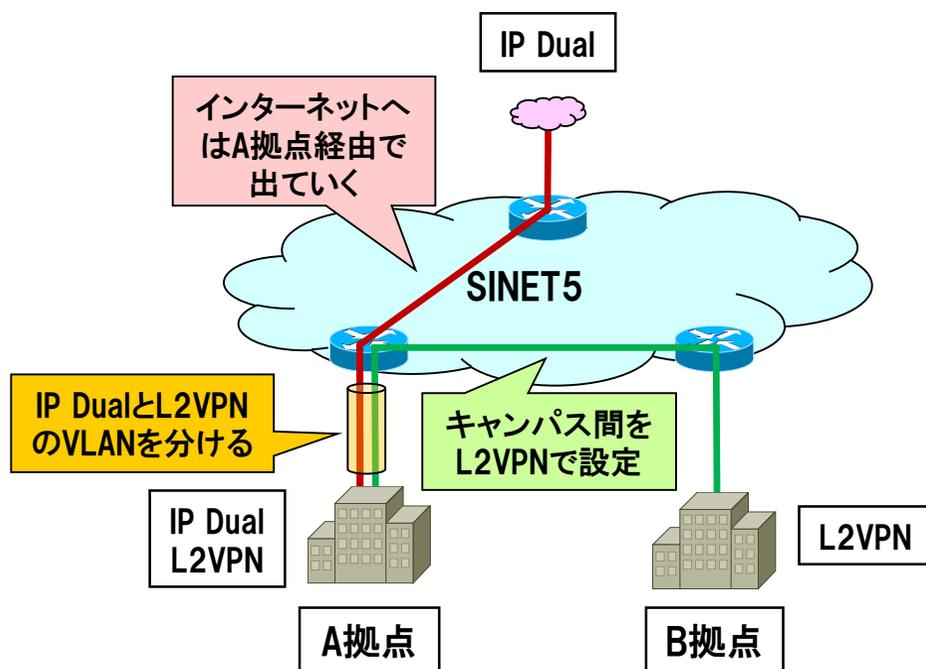
L2VPN接続の基本的な構成イメージ



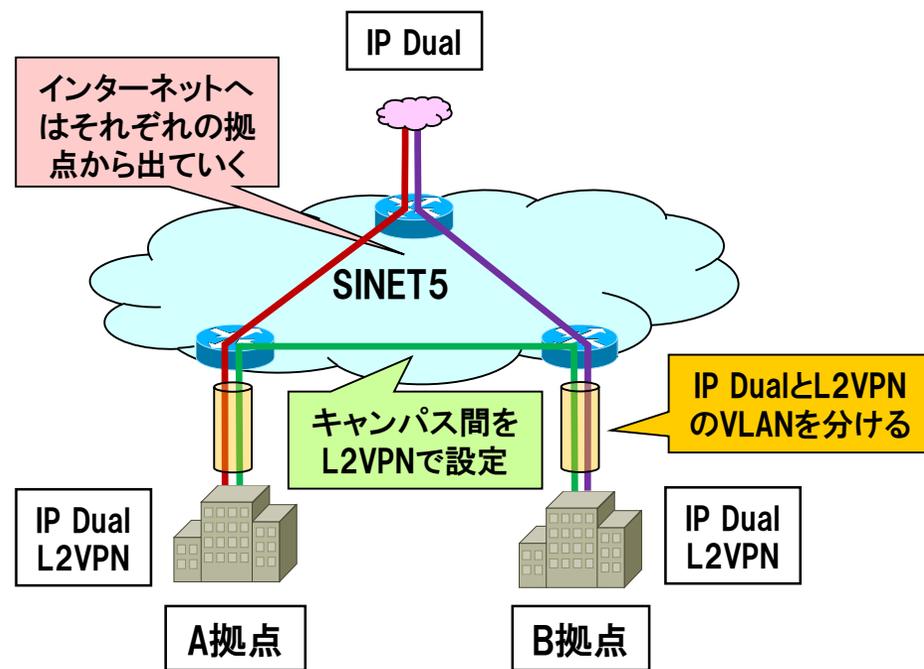
L2VPN接続の構成例

◆ 複数のキャンパスからそれぞれSINETへ接続し、キャンパス間通信をSINET経由のL2VPNで構築する。

例1) キャンパス間をL2VPNで接続し、インターネットへの出口をA拠点に集約する

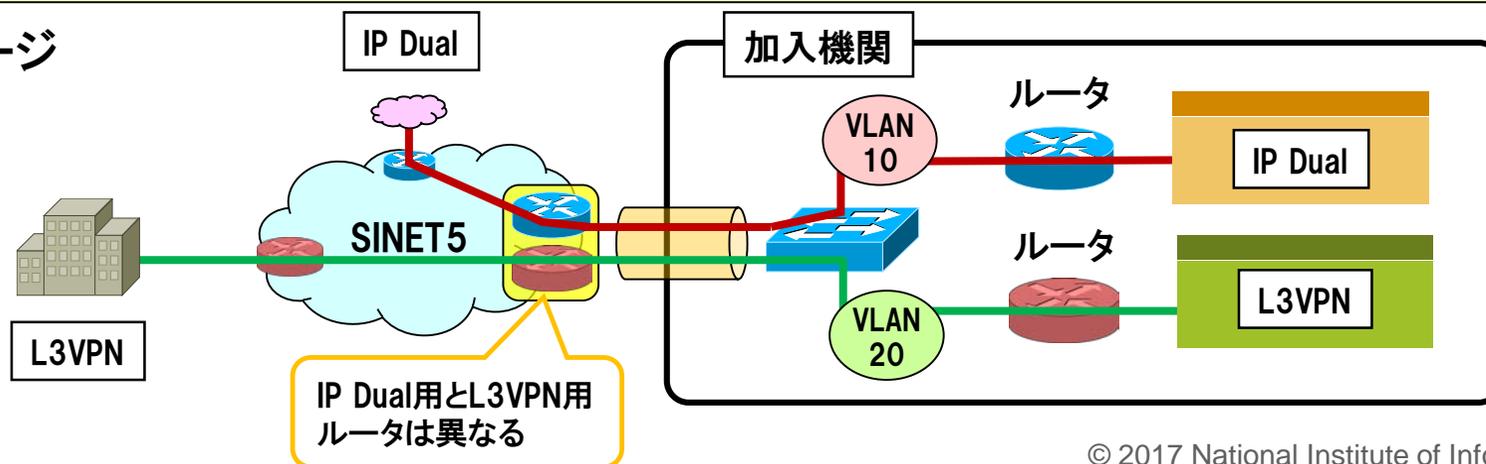


例2) キャンパス間をL2VPNで接続し、インターネットへの出口は拠点ごとに別々にする



- ◆ 各拠点の接続ポリシーが異なる等の事情でレイヤ3で拠点間VPNを構築したいときは、L3VPNサービスが利用できます。
- ◆ SINET機器でルーティングしますが、インターネット接続用のルータとは論理的に分離されていますので安全です。
- ◆ L2VPNと同様に、VLANによる論理分割なので、暗号化はされません。
- ◆ 利用可能なプロトコルは、TCP/IP(IPv4/IPv6)に限定されます。
- ◆ L3(レイヤ3)サービスなのでSINET機器からping等による疎通確認が可能です。
- ◆ L2VPNと違って、ブロードキャストストーム等の障害が発生しても、SINETルータがあるためグループ全体への波及を防ぎます。
- ◆ L3VPNの場合は、SINETから接続セグメント用IPアドレス(150.99.xxx.zzz)の払い出しはありません。拠点ごとに接続用IP(ルーティング)アドレスを決めてください。

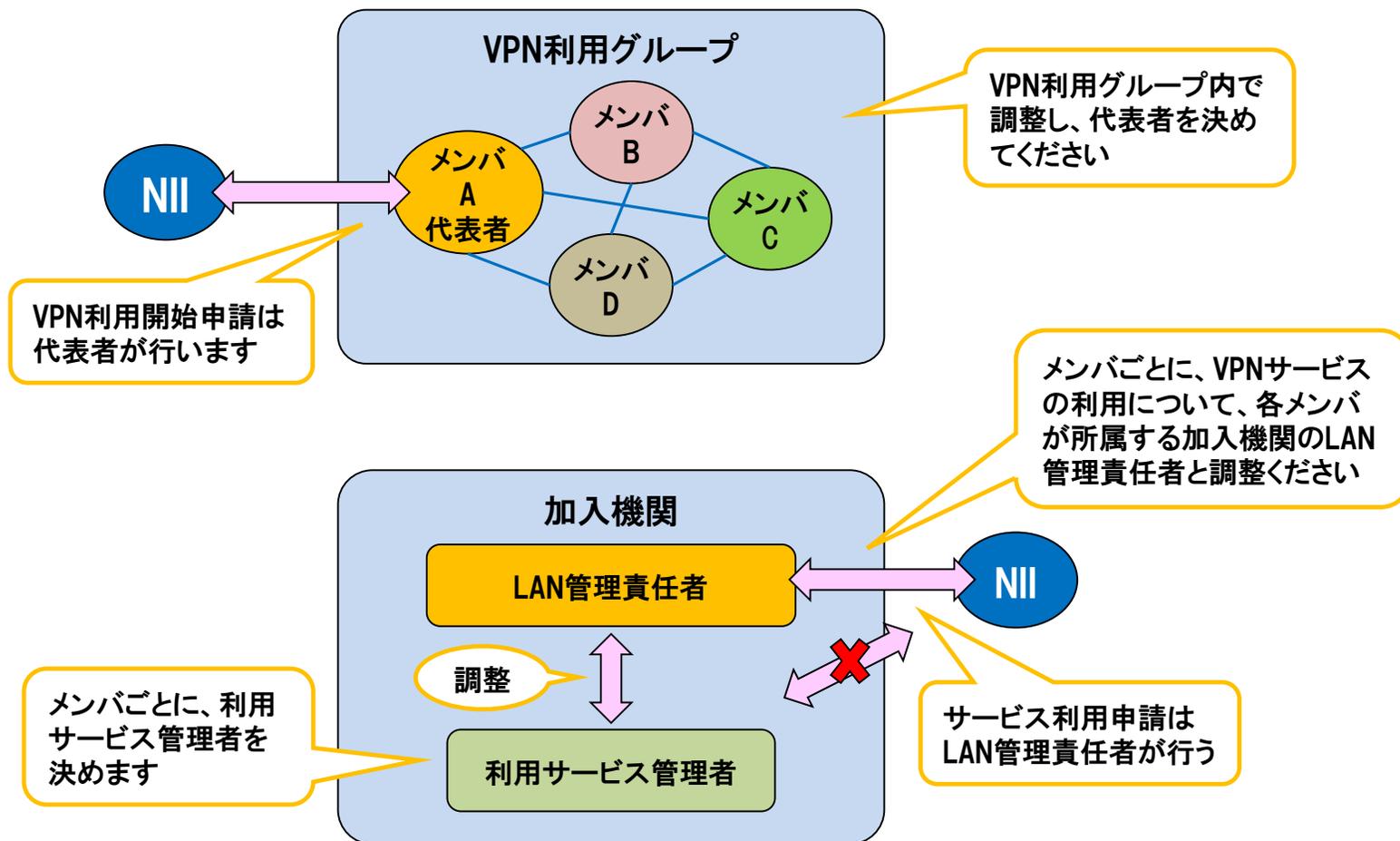
L3VPNのイメージ



VPN利用手続きについて(1)

◆ VPNサービスを利用するには、2段階の申請が必要です。

- ① VPN利用開始申請
- ② サービス利用申請



① VPN利用開始申請

■ VPN利用グループ代表者 → NII

- ・ VPN利用グループ内で各種調整が済みましたら、VPN利用グループ代表者がNIIにVPN利用開始申請を行います。
- ・ 承認に**1週間程度**かかります。
- ・ 無事承認されますと「**申請用ID**」を発行します。
- ・ 申請用IDが記載された**VPN利用開始承認書**をVPN利用グループ代表者に郵送します。
- ・ 承認書が手許に届くまでサービス利用申請が行えませんのでご注意ください。

■ VPN利用グループ代表者 → 各拠点の利用サービス管理者

- ・ 申請用IDを各拠点の利用サービス管理者に通知します。
- ・ サービス利用申請の際に申請用IDが必要です。

(詳細) https://www.sinet.ad.jp/application_procedures/form-vpnreg

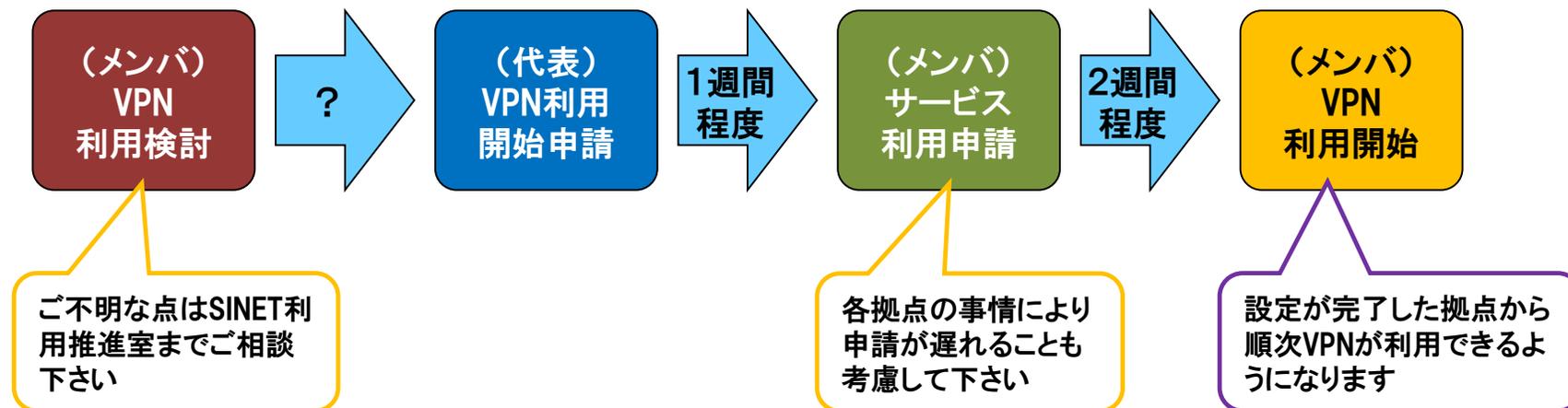
② サービス利用申請

■ 各拠点のLAN管理責任者 → NII

- ・ サービス利用申請書はグループメンバーごとに作成して下さい。
- ・ 利用サービス管理者はLAN管理責任者と申請内容について調整します。
- ・ 各拠点のLAN管理責任者からNIIにサービス利用申請を行います。
- ・ 申請書は利用開始予定日時の**2週間前**までにNIIに提出して下さい。

(詳細) https://www.sinet.ad.jp/application_procedures/form-vpncon

全体の流れ



タグVLAN接続への変更申請(1)

- ◆ アンタグからタグVLAN接続に変更は、VPN利用開始時に同時に行うことも、インターネット接続をまずタグVLAN化してから、後からVPNを利用開始することも可能です。加入機関の都合に合わせてご検討下さい。
- ◆ インターネット接続の変更申請はIPv4/IPv6 Dualサービス申請書をお使い下さい。
(詳細) https://www.sinet.ad.jp/application_procedures/form-ipdual
- ◆ アンタグからタグVLAN接続に変更の際には通常短時間(数分から10分程度)の通信断が発生します。
- ◆ タグVLAN化以降のVLANの追加や削除では通信断は発生しません。
- ◆ 加入機関側機器で対応可能であれば、新規接続の際に、当面はインターネット接続しか利用の予定がなくてもタグVLANで接続するのがよいかと思います。最初からタグVLANにしておけば将来VPNサービス利用時に通信断が発生せずに済みます。

タグVLAN接続への変更申請(2)

◆ 変更届 https://www.sinet.ad.jp/application_procedures/form-ipdual

基本情報

申請区分 新規 変更 終了

VLANの利用 する(tag) しない(untag)

* 必須 物理接続の同時変更申請 する しない

利用既存物理接続種別 ノード接続
 広域LAN(UNO)接続
 既存接続機関経由接続
 地域学術NW等経由接続

オプション

BGP 利用する 利用しない

QoS 利用する 利用しない

■ QoS情報
 使用しない

■ VLAN情報
 ・ VLAN ID:

ここにインターネット接続用のVLAN番号を記入

■ 加入機関側接続元拠点情報
 ・ 接続元拠点名: (キャンパス名等)
 ・ 接続元拠点住所:
 ・ 接続元拠点郵便番号:

■ 既存物理接続情報
 ノード接続
 ・ 接続先ノード:
 ・ パッチパネルポート番号:

SINET5利用変更届(IP-VLAN Dual)
 FORM-SINET5-IPDUAL-136

国立情報学研究所 学術基盤情報部
 予約管理課 宛

作成 年 月 日

学術情報ネットワークの利用に係る事項の変更について、次々とおり届出をします。

種別名:

変更内容:
 ※旧登録や取消等の詳細は「備考」へ記述

■ 申請種別(LAN管理責任者)
 ・ 管理責任: SA
 ・ 所属:
 ・ 氏名:

■ 利用サービス管理者
 ・ 所属: (必須記載したのちが記述)
 ・ 所属:
 ・ 氏名:
 ・ フリガナ:
 ・ 郵便番号:
 ・ 住所:
 ・ E-mail:
 ・ TEL:
 ・ FAX:

■ 申請担当者
 ・ 所属:
 ・ 氏名:
 ・ フリガナ:
 ・ 郵便番号:
 ・ 住所:
 ・ E-mail:
 ・ TEL:
 ・ FAX:

■ 通信先情報
 ・ 運用連絡用メールアドレス:
 ・ 障害連絡用FAX電話番号:

■ 利用時間
 ・ 利用変更希望日時: (平日 9:00~18:00 の間で対応)
 ・ 利用終了予定日:

■ レーティング情報
 ・ レーティングアドレス:

■ BGP情報
 使用しない

■ QoS情報
 使用しない

■ VLAN情報
 ・ VLAN ID:

■ 加入機関側接続元拠点情報
 ・ 接続元拠点名: (キャンパス名等)
 ・ 接続元拠点住所:
 ・ 接続元拠点郵便番号:

■ 既存物理接続情報
 ノード接続
 ・ 接続先ノード:
 ・ パッチパネルポート番号:

■ 備考 (特記事項などがあれば記入)

※ 会員登録完了日時が経過した場合、SINET5から登録取り消し届出を推奨
 いたします。届出後変更の申請をすることがあります。なお、SINET5が登録
 した届出の日時を超過することはありません。ご了承ください。

※ 届出項目「〇」が記載されている項目については、該当する情報の
 「〇」を「■」に記入いただくか、該当しない項目を削除して下さい。

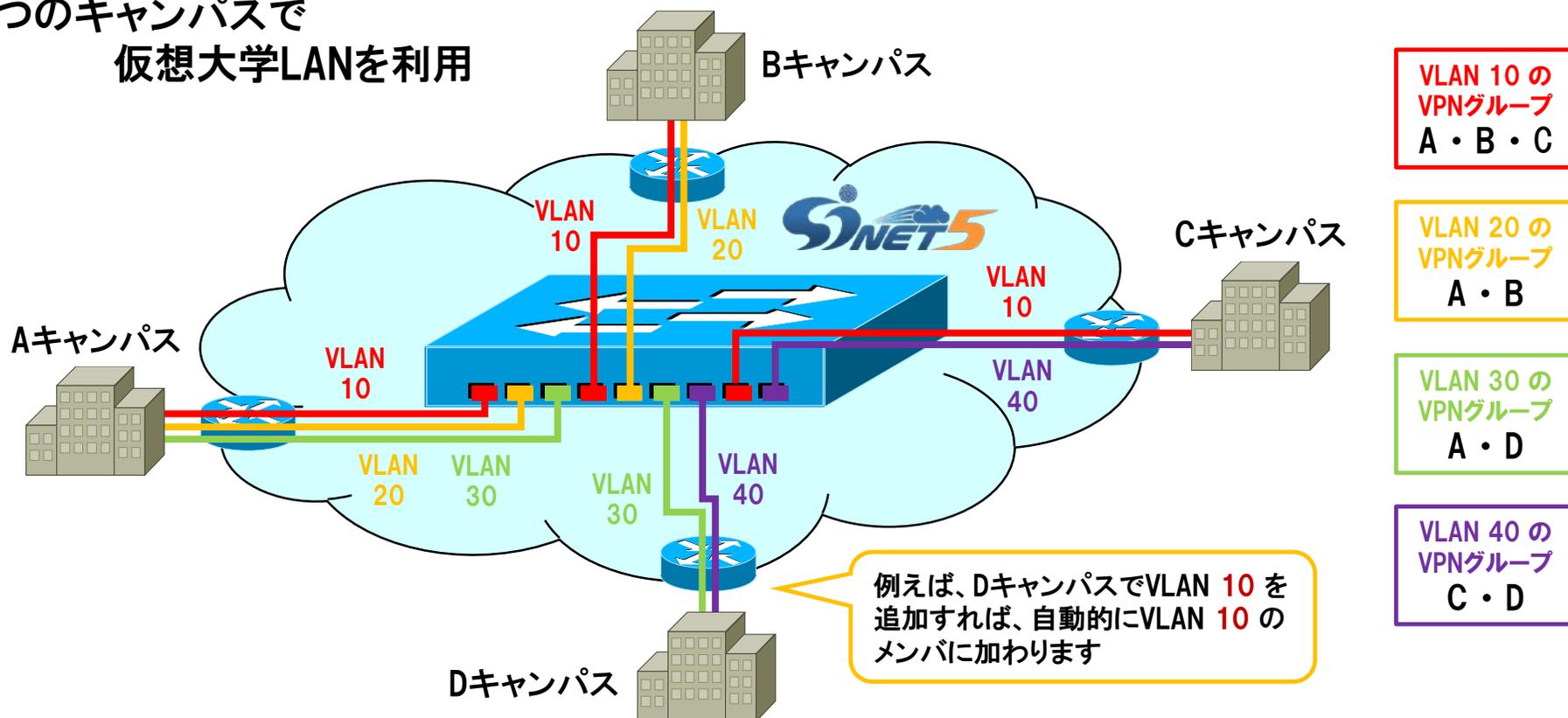
クリップボードにコピー ダウンロード

- ◆ SINET5からの新サービスです。
- ◆ VLANの取り扱いがL2VPNより柔軟です。
 - ・ 申請時にVLAN番号を範囲(上限100個を目安)で指定できます。
 - ・ 同一のVLAN番号の拠点間でVPNを自動的に構築します。
 - ・ 初回申請時に指定したVLANの範囲内であれば、設定変更に申請は不要です。
- ◆ キャンパス間で使用するVLANが非常に多い場合や、VPNの構成変更が比較的頻繁に発生するような加入機関に向いています。
- ◆ 注意点
 - ・ 複数の拠点を持つ**単一の加入機関**に特化したサービスになりますのでご注意ください。
 - ・ SINET機器側にストーム制御の機能がありません。
 - ・ ループしないような構成にしてください。
 - ・ 加入機関側機器でブロードキャストストームを抑止してください。
 - ・ SINET機器でのVLAN変換はできません。

仮想大学LANサービスのイメージ

- ◆ 各拠点のVLAN番号がそのままSINET網内に入ってきます。
- ◆ SINET機器がVLAN番号を自動認識し、同じVLAN番号の拠点間を通信可能にします。
- ◆ 最初の利用申請時に予め指定したVLAN番号の範囲内であれば、NIIへ申請せずにVLANの設定変更が自由にできます。

例) 4つのキャンパスで
仮想大学LANを利用



仮想大学LANとL2VPNの比較

◆ L2VPNと仮想大学LANの主な違いと共通部分を以下に示します。

	L2VPN	仮想大学LAN
VPNの構成メンバ	単一機関や他機関とも可能	単一機関に限定
VPNの安全性	VLANで論理分割、暗号化なし	同左
利用可能なVLAN番号	2～4094	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）	必要（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
利用申請	2段階申請（VPN利用開始申請、サービス利用申請）	仮想大学LAN申請の1通のみ
VLANの変更申請	必要（変更がある度に）	不要（申請時の範囲内なら）
クラウド接続サービスとの併用	可能	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

- ◆ L2VPNと異なり、グループ代表者を決めたり、利用開始の承認を得るといった手続きはありません。利用開始予定日時の**2週間前**までにご提出ください。
- ◆ 仮想大学LAN申請に必要な接続拠点情報と、別紙表(エクセル)に使用予定のVLAN番号を列挙して申請します。

(詳細) https://www.sinet.ad.jp/application_procedures/form-vsw

TOP > 申請手続き > 仮想大学LAN申請

仮想大学LAN申請

申請フォーム

- 以下のフォームに情報を正確に記入してください。
- 申請の受付メールアドレスは「apply@sinet.ad.jp」です。
- 利用開始予定日時の約2週間前までにご提出ください。
- 別紙表は [こちら](#)よりダウンロードしてご記入ください。

SINET5 利用申請書 (仮想大学LAN)
 国立情報学研究所 学術基盤推進部
 学術基盤課長 殿

平成 年 月 日

「国立情報学研究所学術情報ネットワーク加入細則」を遵守し、次のとおり申請します。

当該ガイドラインを 承諾する 承諾しない

機関名：
 接続概要：
 ※設定値や図表等の詳細は「備考」または資料を添付する

◆申請者 (LAN管理責任者)

- 管理者ID：
- 所属：
- 氏名：

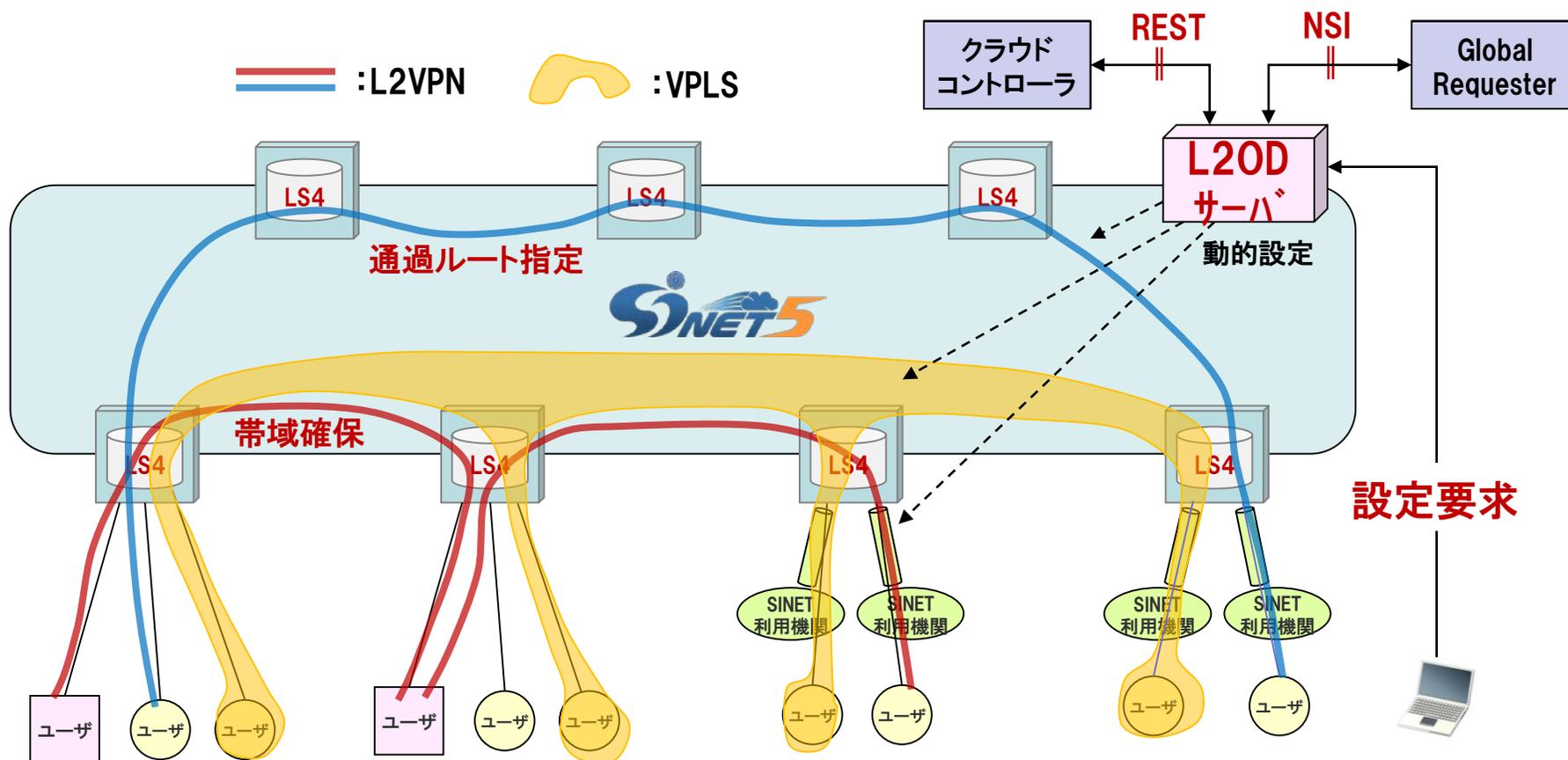
The screenshot shows a detailed application form with a table for listing connection points and VLAN numbers. The table has columns for '接続拠点名' (Connection Point Name), '接続先IP' (Destination IP), '接続先ポート' (Destination Port), and 'VLAN番号' (VLAN Number). There are also sections for '備考' (Remarks) and '申請者' (Applicant).

別紙表

L2オンデマンドサービス概要

◆ ユーザから接続対地や開始・終了時間等を指定して、VPN設定や帯域確保が可能

- ・ L2VPN (1対1): 「帯域確保」や「通過ルート指定」も可能
- ・ VPLS (多対多): 「接続対地の追加や削除」も可能
- ・ 外部連携: クラウド連携等のためのRESTや国際連携のためのNSIも実装



◆ L2オンデマンド利用のイメージ

- ① 事前申請:VPNグループ情報等の登録(VPNに属する拠点・回線の登録、VLAN範囲の申請)
- ② 事前予約:Web画面からVPN予約を設定
- ③ 利用時刻:パス確立～利用～パス解放 →設定、解放実施のメール通知

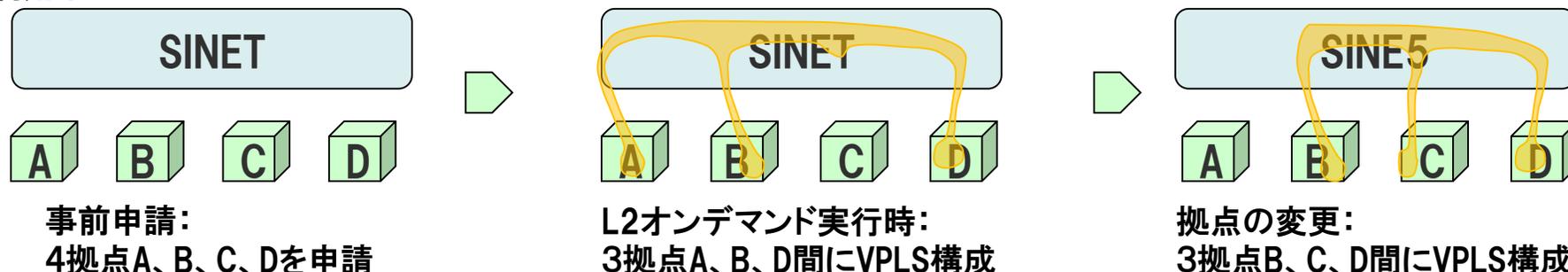
◆ L2VPN (PtoP接続)オプション

- ◆ 帯域指定も可。帯域の範囲内で優先パケットとしてSINET内を転送。
優先帯域が容量超過した場合は抽選で利用者を決定。(抽選結果はメール通知)
- ◆ 即時利用(最短5分後からの開始予約)も可能。即時利用の場合は帯域指定は不可
- ◆ 経路指定も可能。(通常は最短経路)

◆ VPLS (MPtoMP接続)オプション

- ・ VPNグループに登録した複数拠点の中から、任意の拠点を選択し日時を予約することで、選択した拠点間に予定の日時にVPNを構成
- ・ VPNへの対地の追加・削除が可能。

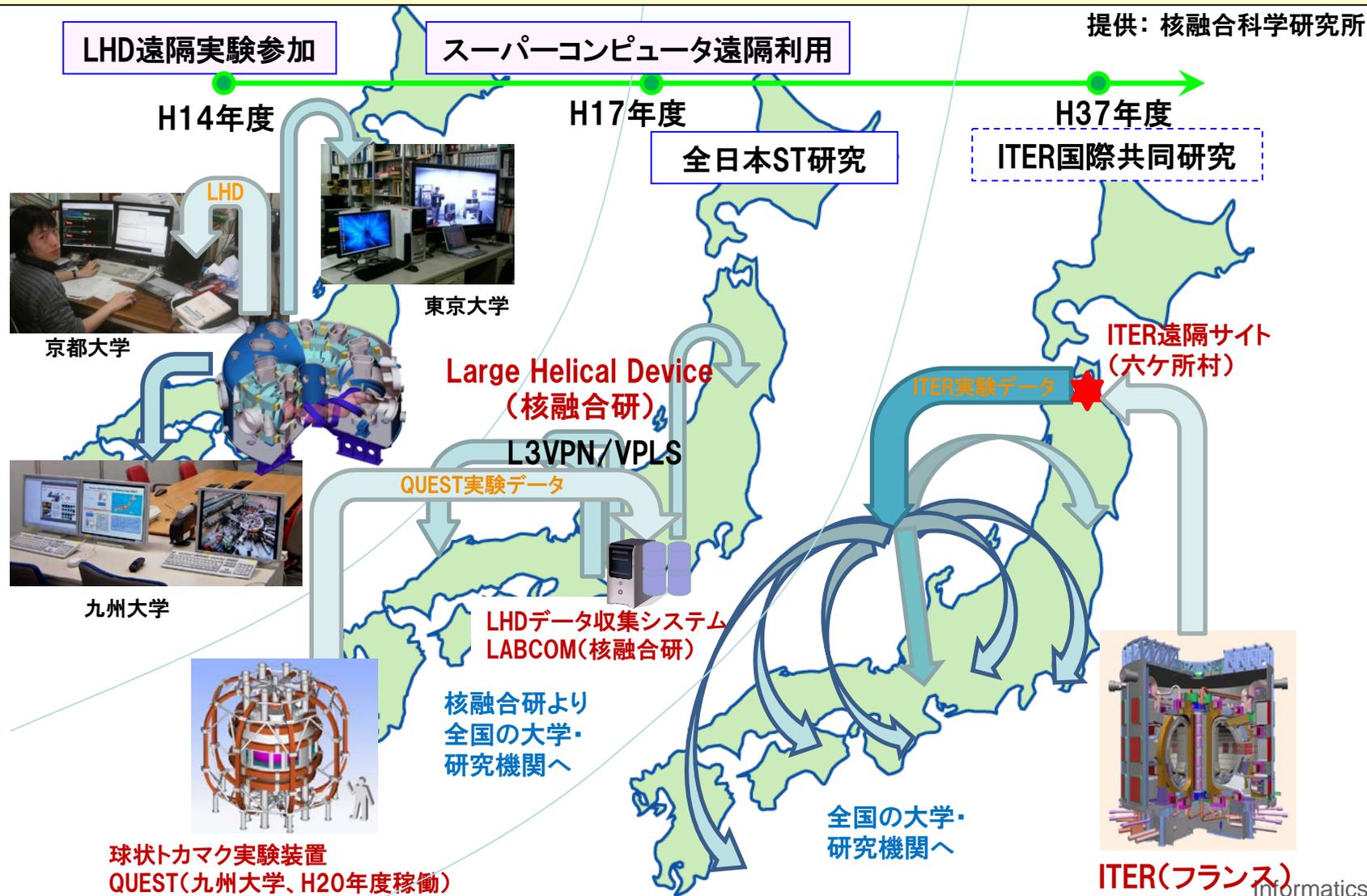
利用イメージ



SINET利用例

SINET利用例 — 核融合研究

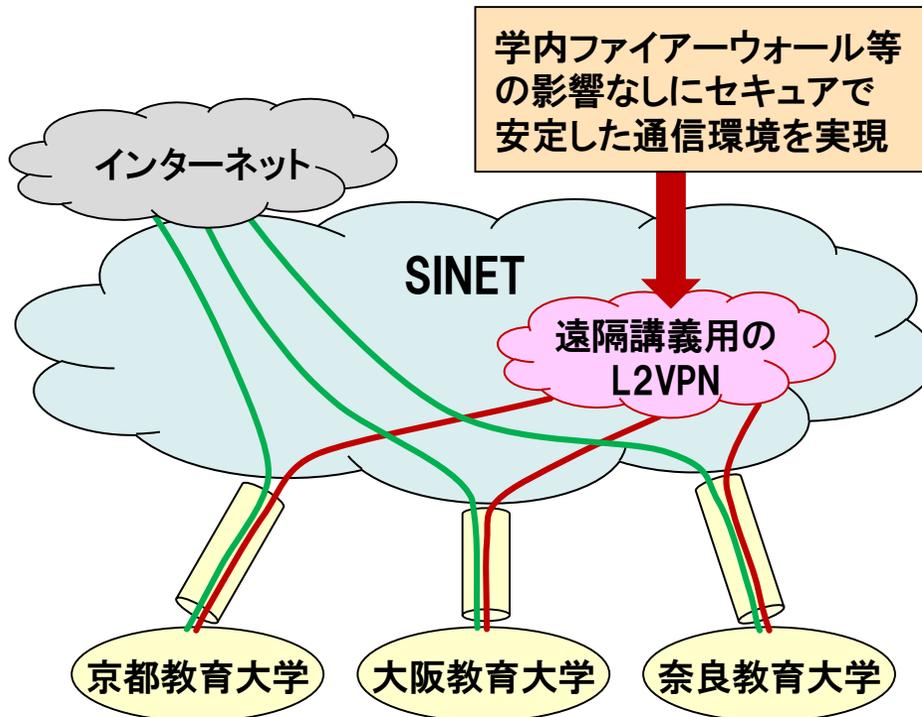
- ◆ 大型ヘリカル実験装置(LHD)や球状トカマク実験装置(QUEST)等からのデータをセキュアに転送
- ◆ ITER遠隔サイト(六ヶ所村)に設置のスパコン(EUファンド)の国際利用をサポート



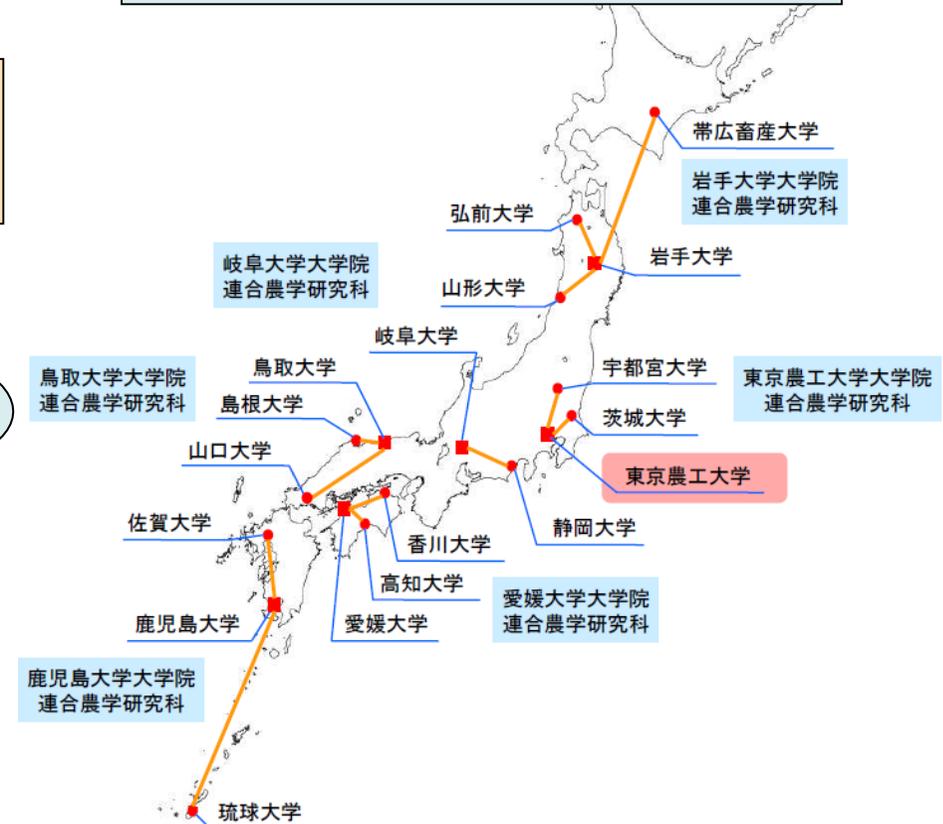
SINET利用例 — 遠隔講義例

- ◆ 関西の3教育大学(京都教育大学、大阪教育大学、奈良教育大学)にまたがる双方向の遠隔講義環境を、SINETのL2VPNを活用して構築
- ◆ 北海道から沖縄までの全国18の国立大学(23拠点)にまたがる連合農学研究科を結ぶ遠隔講義環境を実現 等

3教育大学にまたがる遠隔講義環境



連合農学研究科を結ぶ遠隔講義環境



SINET利用例 — 医療情報バックアップ

- ◆ 全国の42国立大学46病院の災害時用データをL2VPNでセキュアにバックアップ
- ◆ SS-MIX2(診療情報の国際標準仕様)データを東西2カ所のデータセンターに保管

SS-MIX: Standard Structured Medical Information Exchange

提供: 東京大学医学部附属病院

SS-MIXは2か所へ、フルバックアップは遠い方1か所へ

