

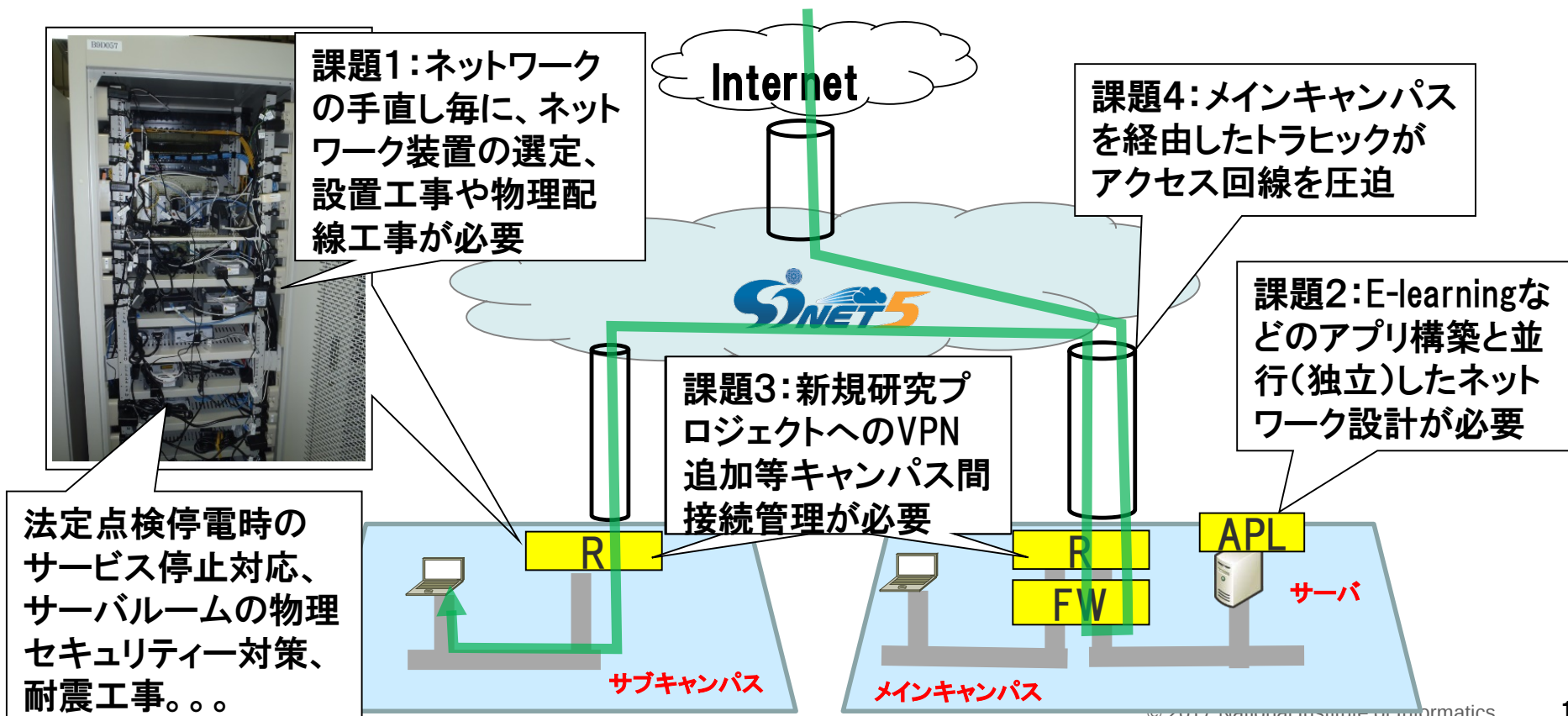
ネットワーク機能仮想化と 活用への取り組み

平成29年6月8日
国立情報学研究所

はじめに： ネットワーク設計上の課題について

◆こんな課題で困っていませんか？

- 課題1: ネットワーク装置の選定、設置工事、物理配線工事などが必要。
- 課題2: サーバー設計とネットワーク設計が独立しており連携設定に時間がかかる
- 課題3: 学内のネットワーク接続管理に手間がかかる。
- 課題4: メインキャンパスに集約するとアクセス回線がボトルネックとなる

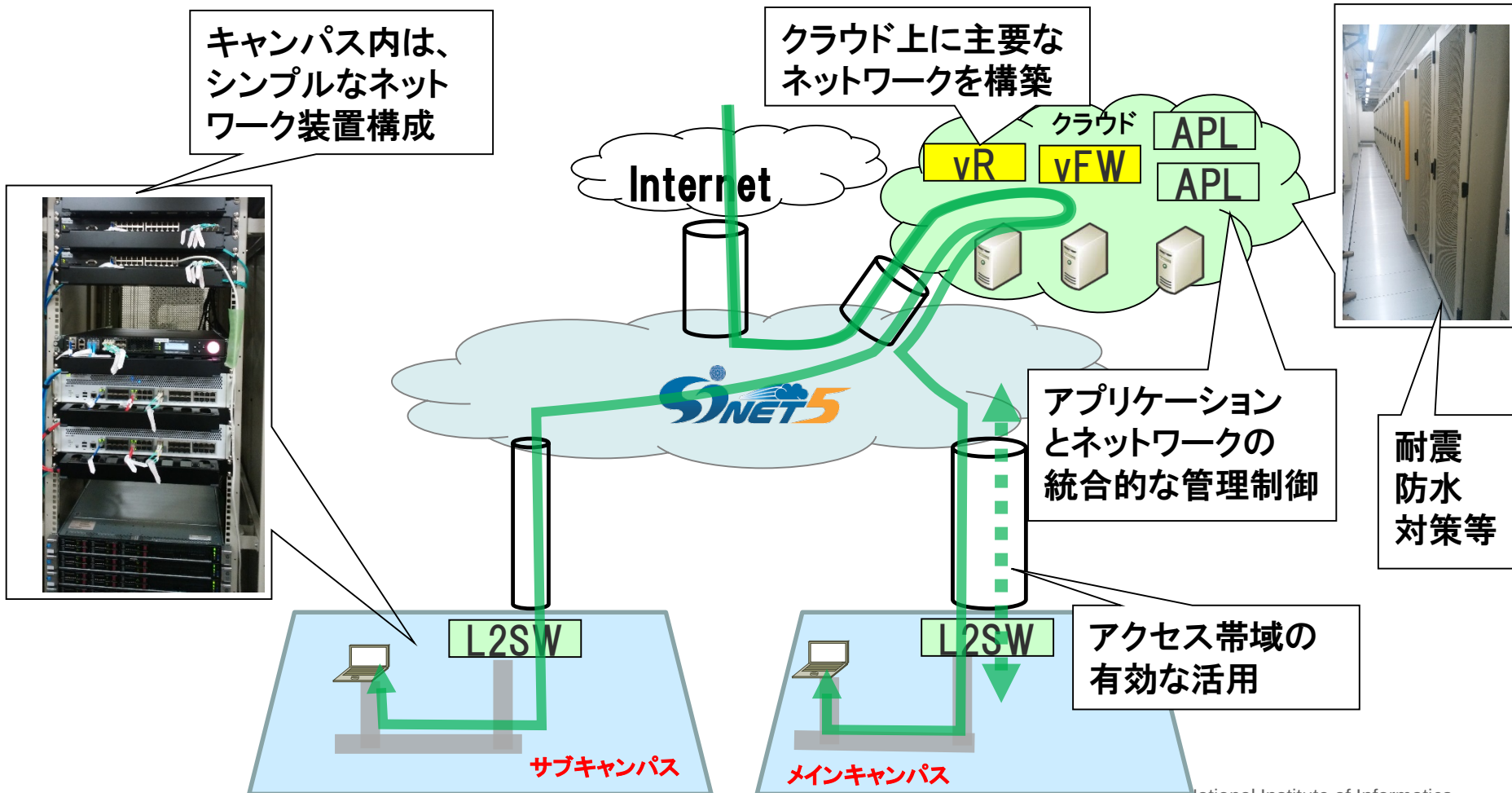


ネットワーク機能仮想化の活用イメージ

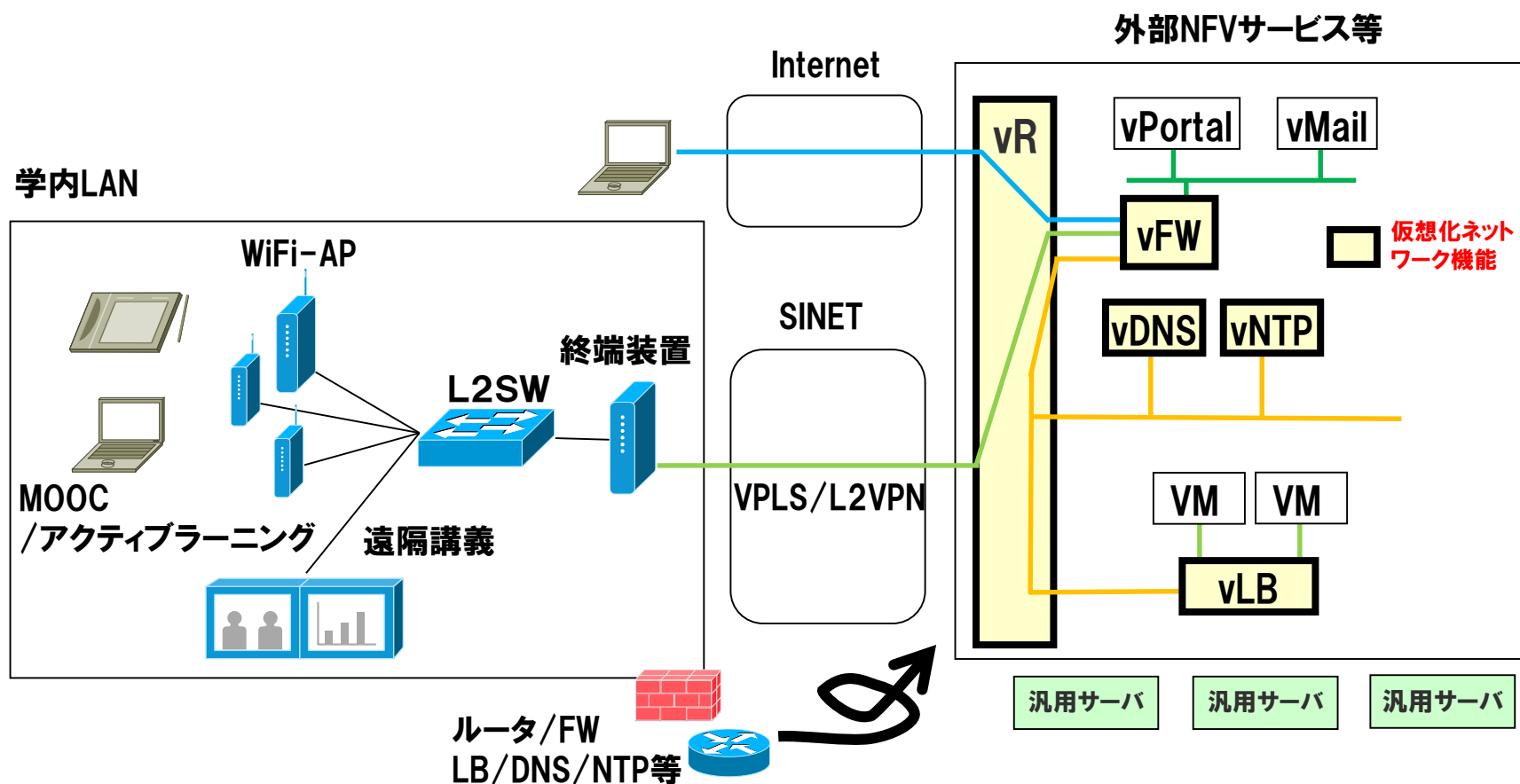
◆ネットワーク機能仮想化を活用することで課題解決を目指しています。

**ポイント1: ネットワーク機器をクラウドに移行しキャンパス内はすっきり。
ネットワークは遠隔から自動設定！**

ポイント2: アプリケーションとあわせネットワーク機能を含めた統合的な管理・制御を実現!



- ◆ 加入機関様のロケ内に配備がなされていた各種ネットワーク装置を、外部NFVサービスにアウトソーシング化する。(構内LANはシンプルな機器を中心に配備し、運用管理を簡易化)
- ◆ 特定の機能に対する突発的な需要増減や、構成変更への柔軟な対応、リソース集約／共用によるコスト削減などが期待できます



ネットワーク機能仮想化の流れ

◆サーバの高性能化

一般サーバのCPU性能の価格性能比(30年で約3000倍)、バス速度はPCIからPCIe3.0で500倍

◆WANの低廉化・高速化

・ISDN(64kbps)から光アクセス(1Gbps)へ15600倍

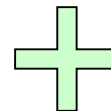
◆Software Defined Network(SDN)の登場: ネットワーク設計・設定をソフト的に簡易に実現

◆Network Function Virtualization(NFV)の登場: ネットワーク機器が汎用サーバ上で動作

サーバの高性能化

WANの低廉化・高速化

データセンタに設置されたサーバを、
ネットワーク越しで共有するクラウドの登場



ネットワークの設計・設定は、
物理作業・論理設定と大変

SDN: ネットワーク設計・設定をソフト的に簡易に

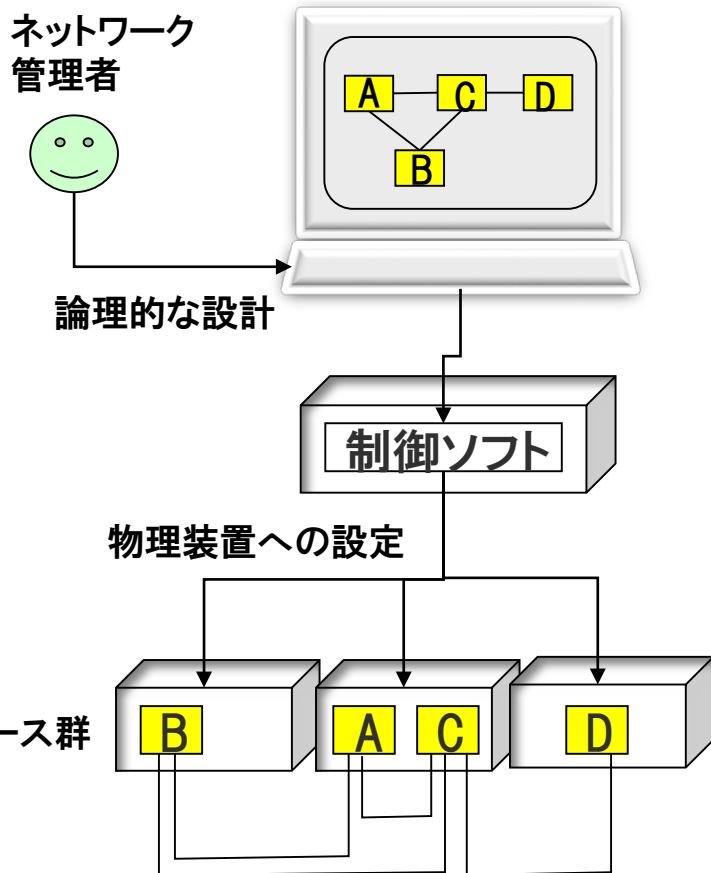
ネットワーク機器は
専用のハードウェア
管理・運用が大変

NFV: ネットワーク機器が汎用サーバ上で動作

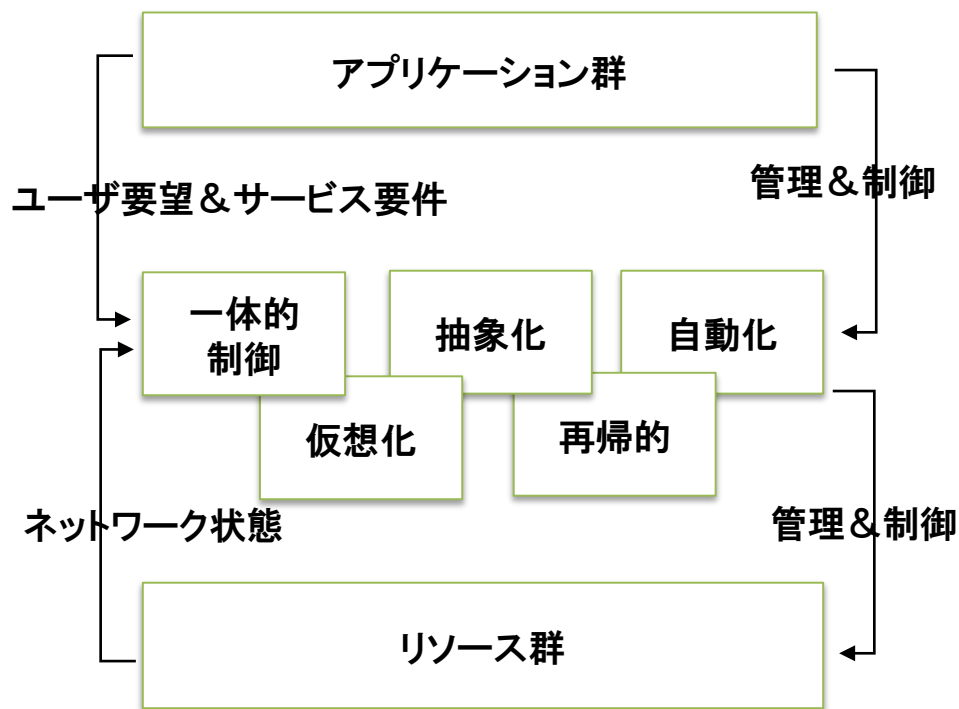
SDN (Software-Defined Networking)とは

◆SDNは、ソフトウェアを用いてネットワークを設定／制御可能とすることで、コスト削減、自動化によるネットワーク設定の簡易化を目指します。

利用イメージ



SDNアーキテクチャ



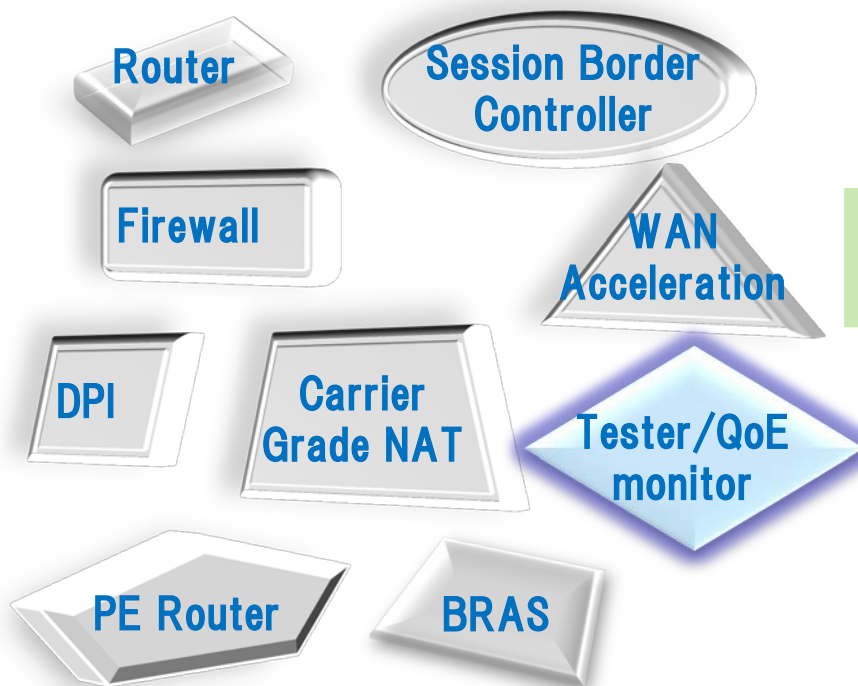
※参照：<https://www.opennetworking.org/sdn-resources/sdn-definition>

NFV (Network Function Virtualization)とは

◆NFVは、汎用のハードウェア上に、ソフトウェア化したネットワーク機能を動作させることで、個々の専用ハードウェアを不要とし、柔軟にネットワーク機能を実現することを目指します。

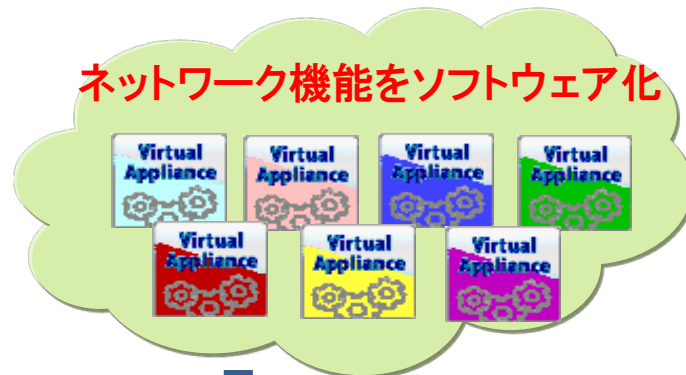
従来のネットワークアプライアンス
のアプローチ

↓
機能ごとに専用ハードウェアを使用



NFVのアプローチ

ネットワーク機能をソフトウェア化

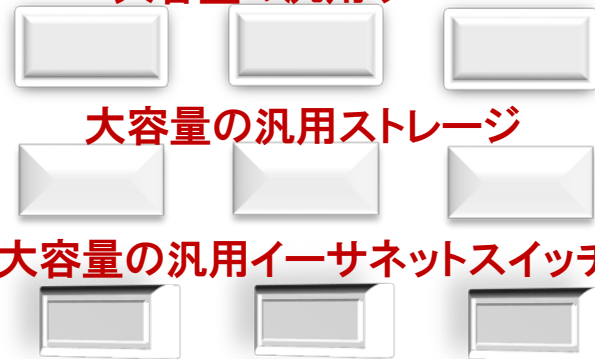


汎用のハード上で動作

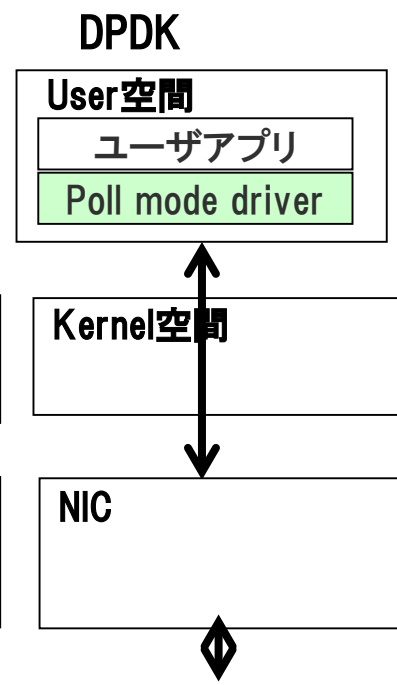
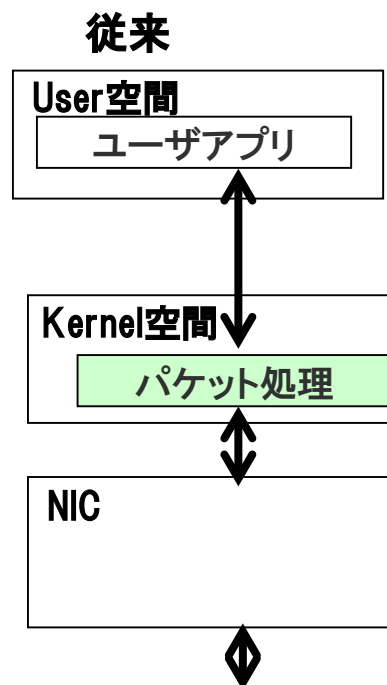
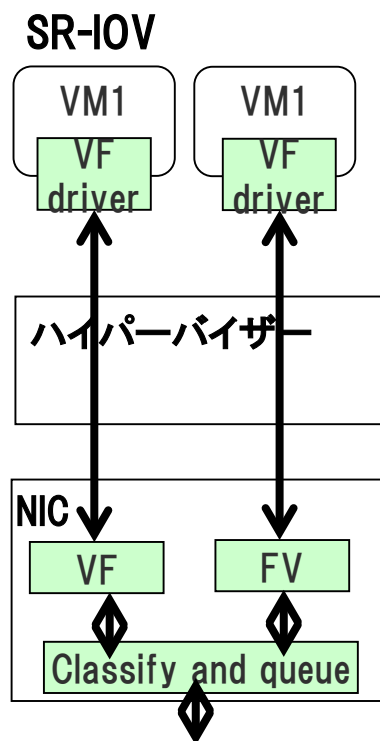
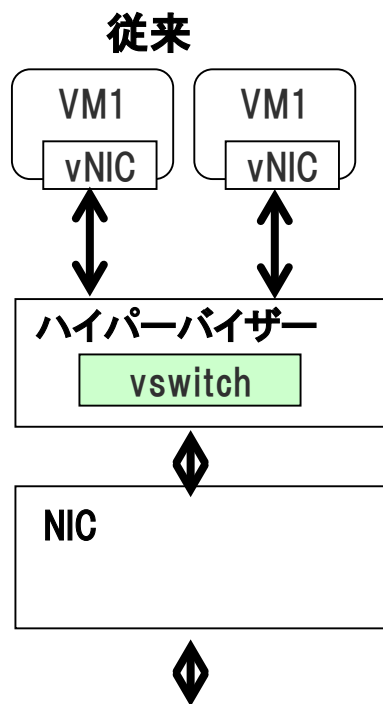
大容量の汎用サーバ

大容量の汎用ストレージ

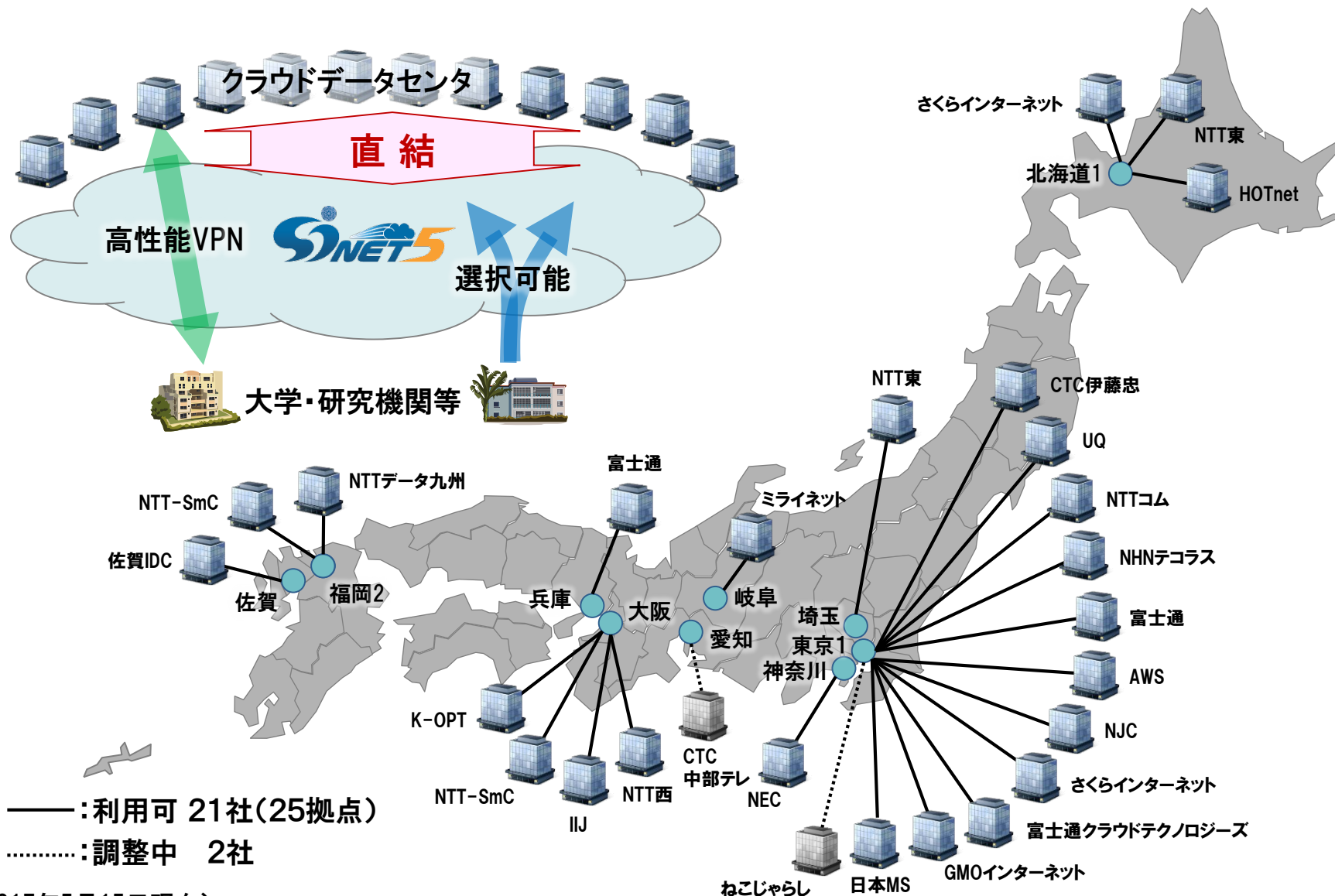
大容量の汎用イーサネットスイッチ



- ◆仮想マシンにおけるパケット処理技術が向上し、単純処理ならば10Gbps～も可能に！
- ◆従来はNICからのパケットはKernel(ハイパーバイザ)が一旦受信し、パケット解析後にユーザ空間のアプリケーションへ転送を行っていたため、パケット処理性能が低下
- ◆直接NICからVM/ユーザ空間へパケットを渡すことで性能を向上
 - ・ SR-IOV: VMからはVFドライバで直接NIC内のVF(仮想化PCI)から読みだすことで高速化
 - ・ DPDK: User空間NOアプリケーションから、直接NICのパケットを読み出すことで高速化

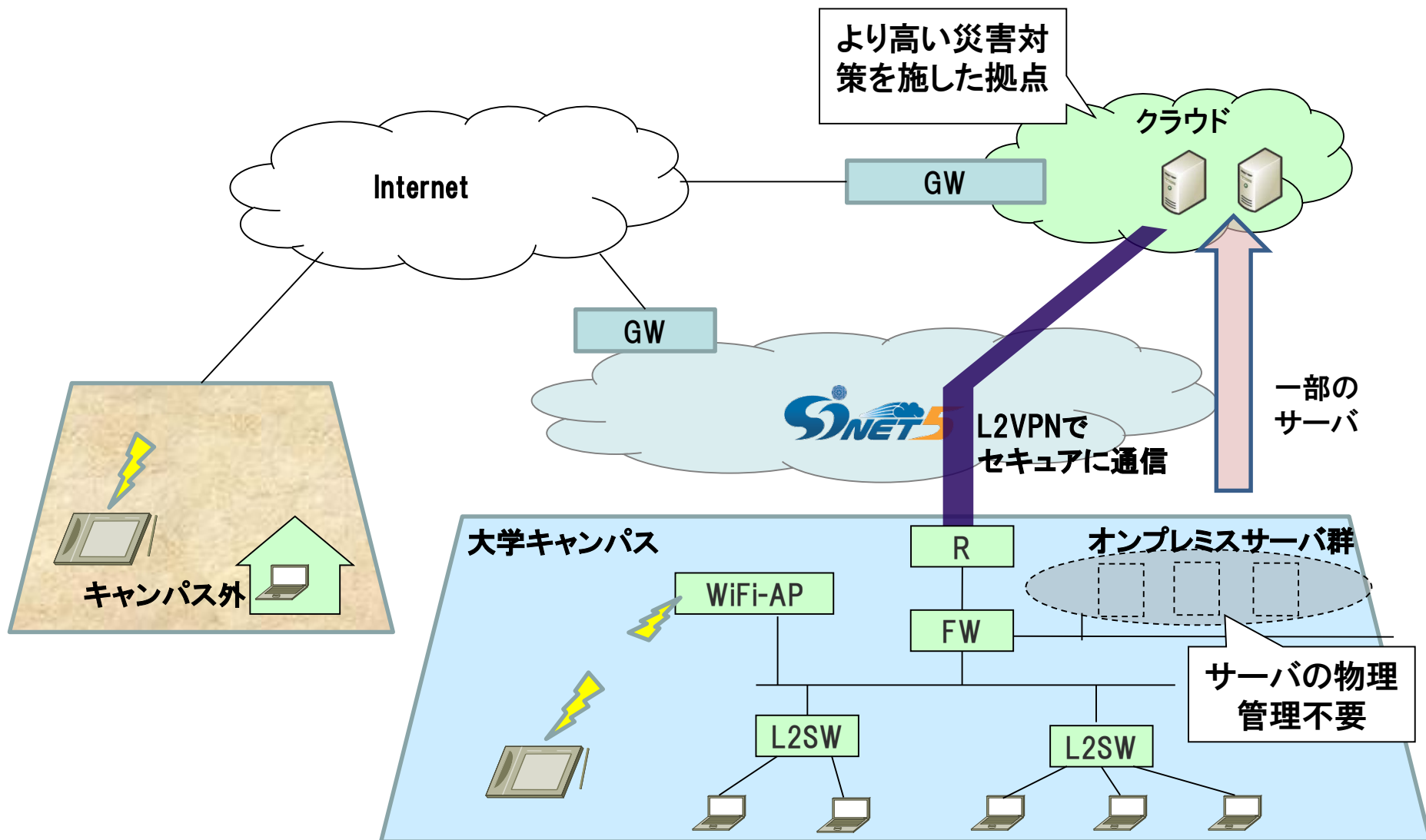


◆ SINETに直結した商用クラウド事業者数は21へ(80以上の加入機関に提供中)



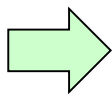
クラウド直結サービスによるサーバ移行

◆オンプレミスで管理していたサーバをクラウド化することで、物理的なサーバ管理が不要に！！



◆物理障害・物理セキュリティ・災害耐性を高める物理的な対策として以下があげられます。

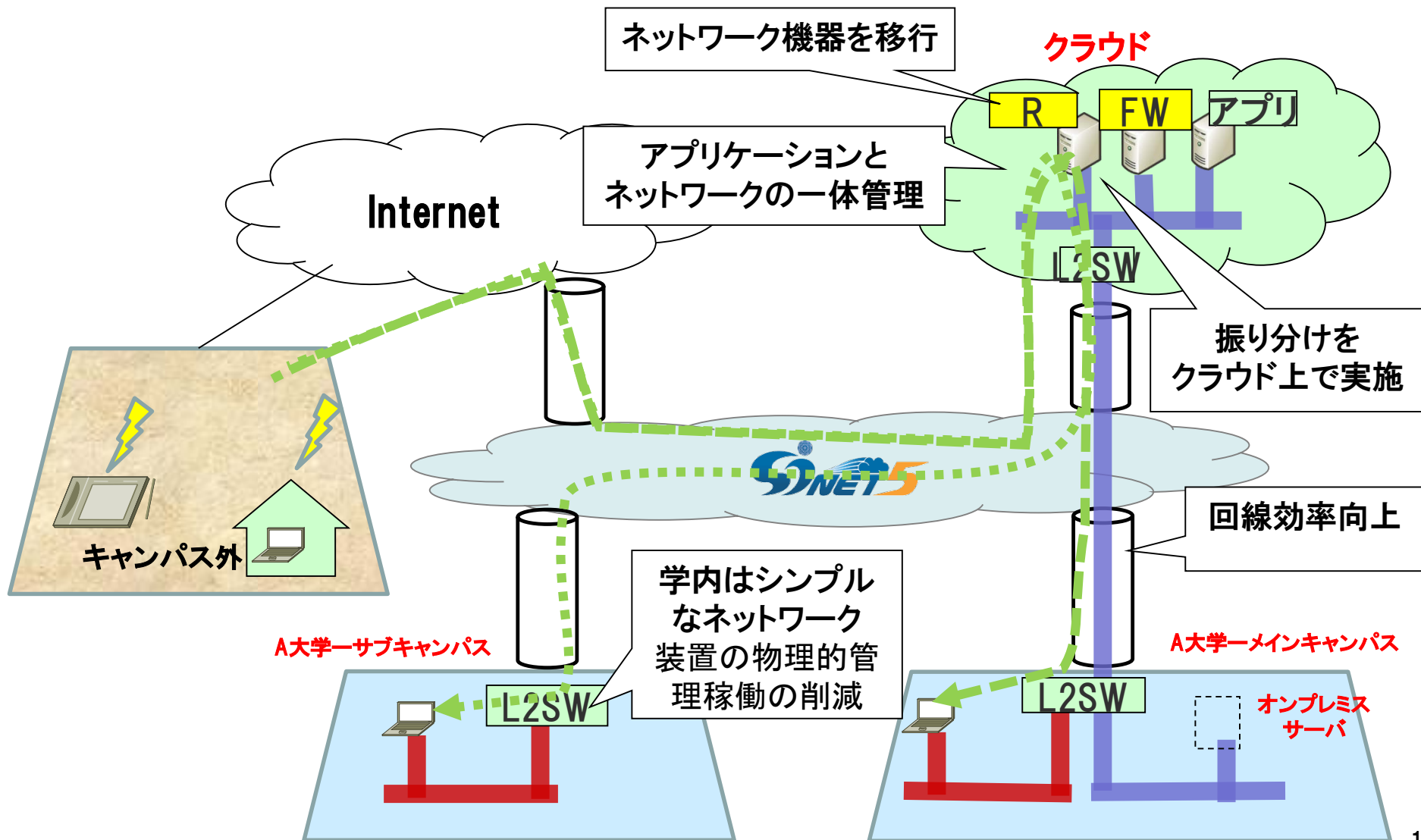
- ・ UPSの導入
 - ・ 電源断においても、バッテリーにより電源供給ルートを継続
 - ・ 万一の停電時は自家発電も組み合わせ電力を供給
- ・ 物理的セキュリティ
 - ・ 入館管理とラック施錠管理
 - ・ 生体認証や監視カメラによる監視
- ・ 耐震設備の導入
 - ・ 2重床による免震構造 → 設置機器へのダメージを抑制
- ・ ネットワーク接続の堅牢化
 - ・ 堅牢性の高い物理ネットワーク接続
 - ・ とう道 > 管路 > 架空



高い障害対策が施されたデータセンタ上のクラウド活用も一つの解決策

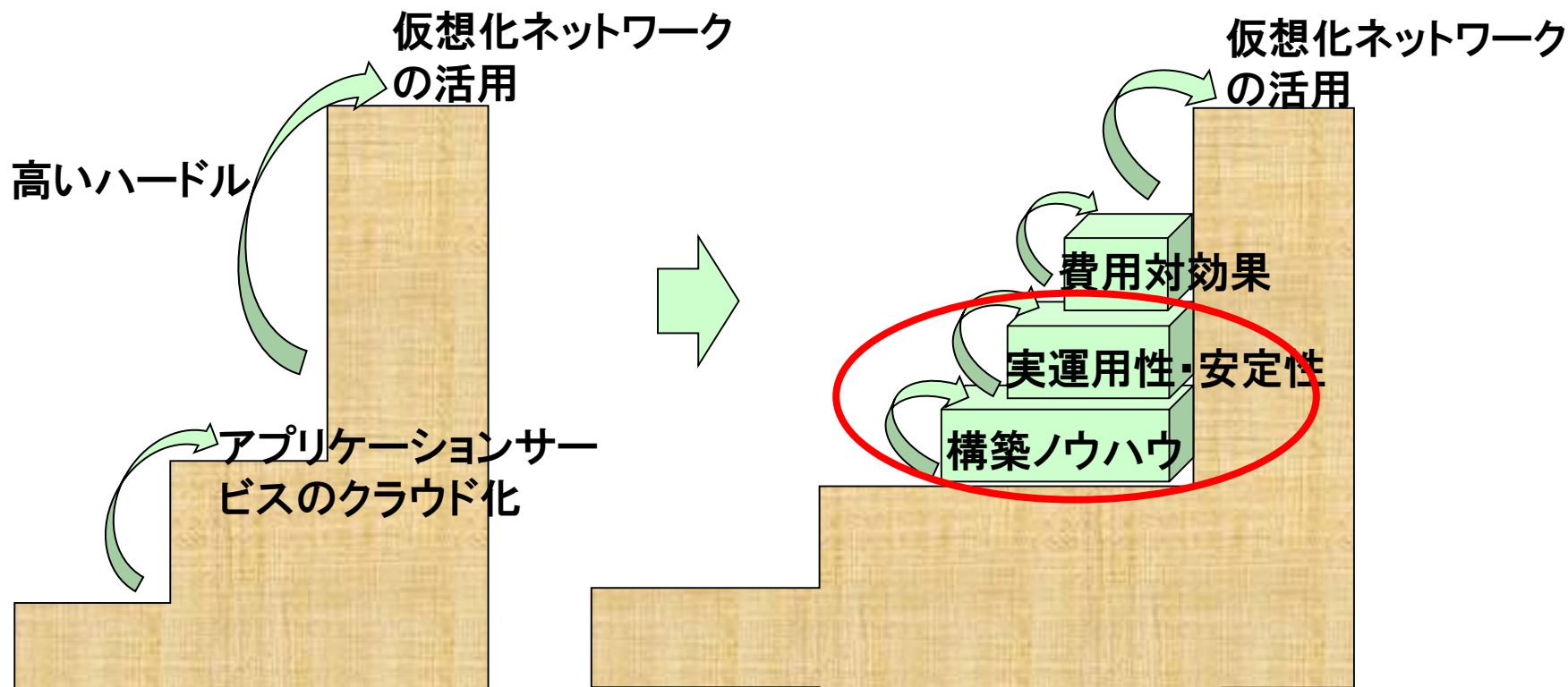
ネットワーク機器のクラウドへの移行イメージ

◆ネットワーク機器の仮想化を行いクラウド上のサーバに移行しアプリケーションとネットワークを一体的に管理・制御することで、運用の効率化が期待されます。



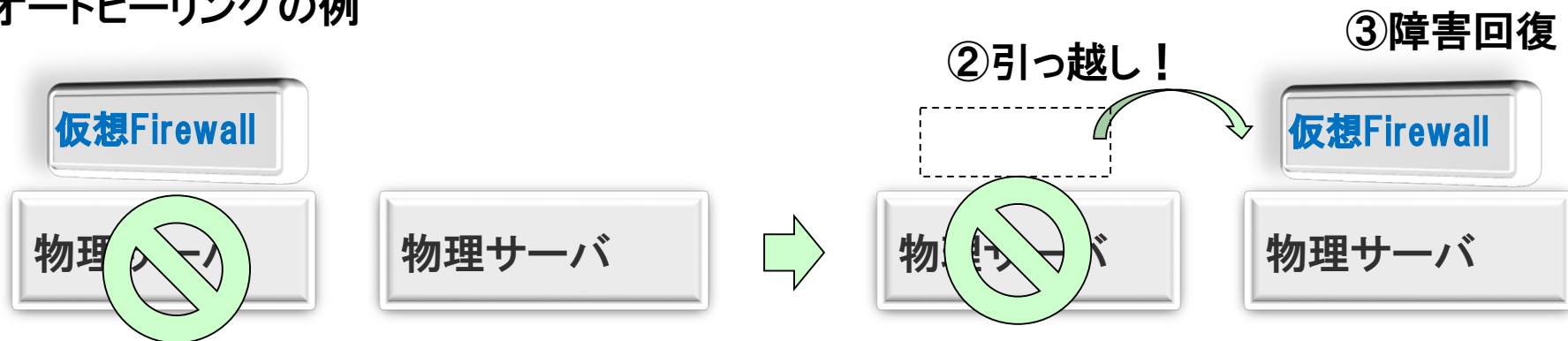
ネットワーク機能仮想化技術に関する取組み

- ◆ ネットワーク機能仮想化技術は運用面・性能面など未知の面があるため、新しい技術を実利用するためのノウハウ蓄積、運用性／安定性評価を進めております。



- ◆ より安定的にネットワークサービスを実現するための機能として、オートヒーリング機能、オートスケーリング機能の実現が期待されています。
- ◆ オートヒーリング：
 - ・ 仮想ネットワーク機器が稼働しているホストサーバに物理障害が発生した際、他の物理サーバにVMを移動することで、早急に障害回復を実現します
- ◆ オートスケーリング：
 - ・ 仮想ネットワーク機器の処理負荷が許容値を超えたときに、新たに仮想ネットワーク機器を追加することで処理負荷を分散し対応します

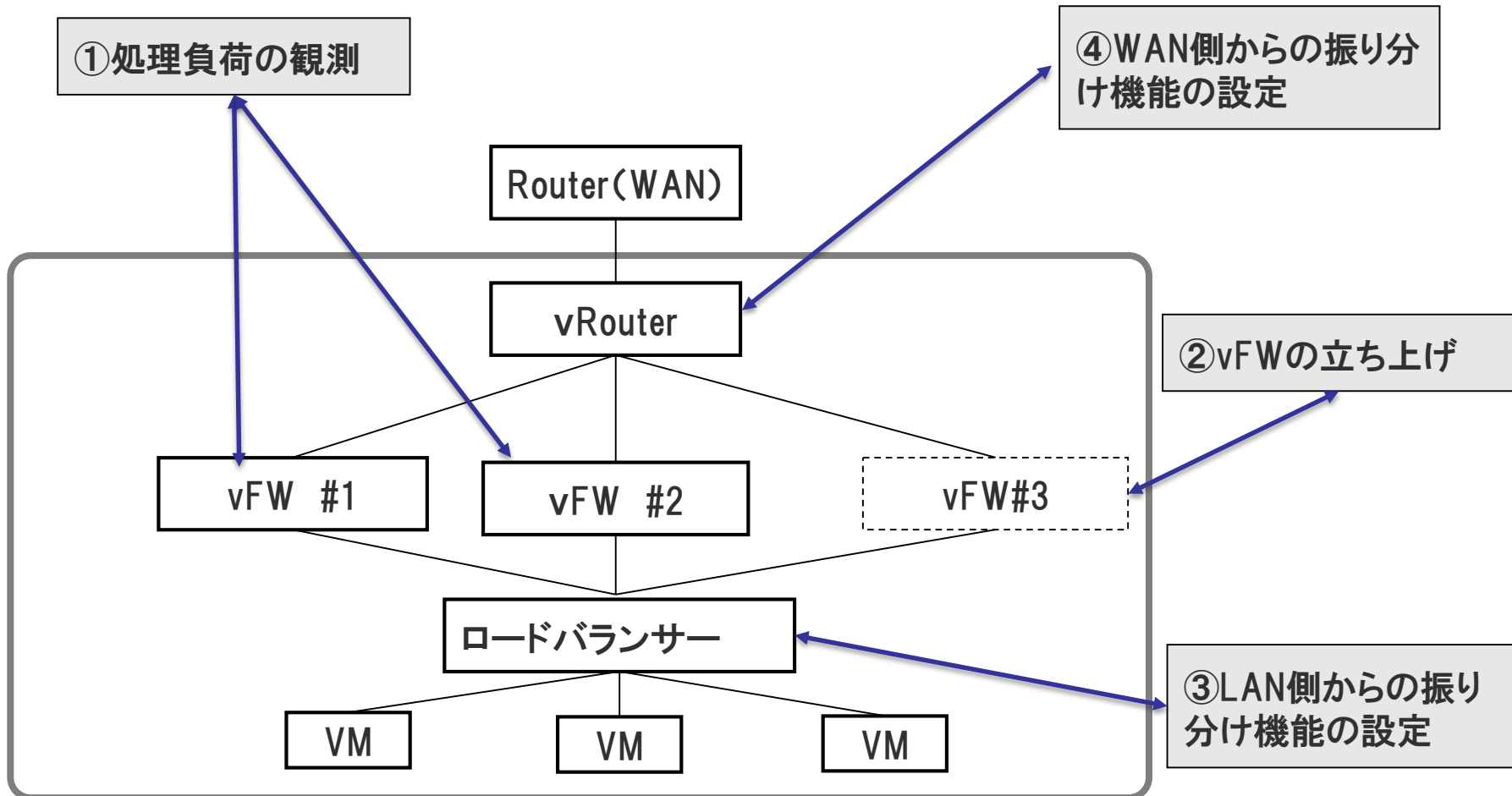
オートヒーリングの例



①物理サーバの障害＝仮想ネットワーク機器の障害

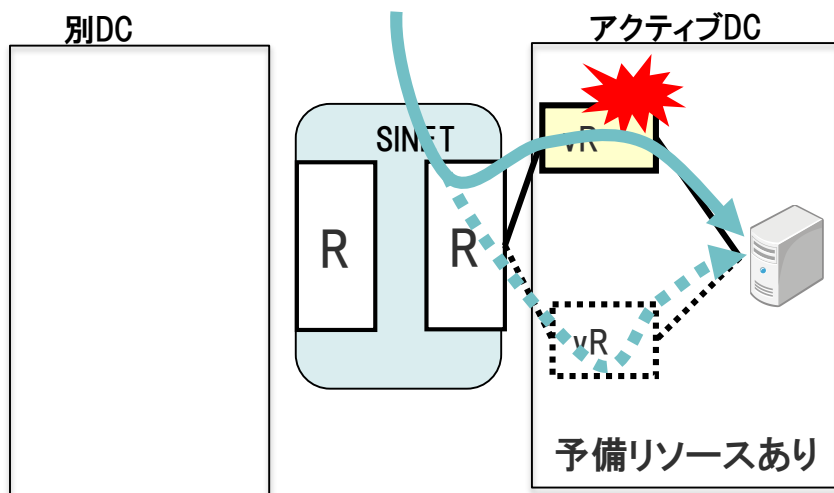
仮想FWのオートスケーリング例

- ◆ 仮想FWの負荷を観測し、負荷が所定の範囲を超えた際に、自動的に仮想FWの追加を行います。その際に必要な振り分けを行うために必要な周辺機能への設定も同時に行います。

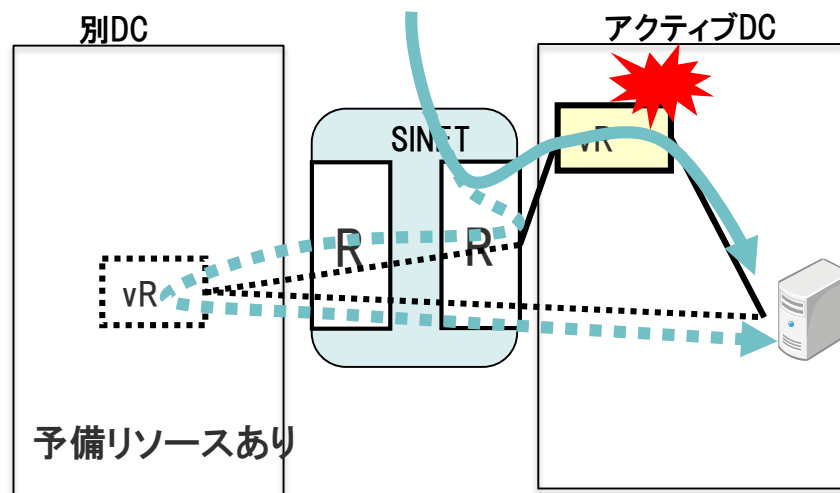


- ◆ DC内でのオートヒーリングに加えDC間を跨いだvRouterオートヒーリングも評価しています。DC間でのオートヒーリングは、同一のDC内に必要な予備リソースをDC内に確保できないケースを想定し行っています。

DC内オートヒーリング



DC間オートヒーリング



R WAN側ルータ

vR vRouter(仮想化ルータ)

vR

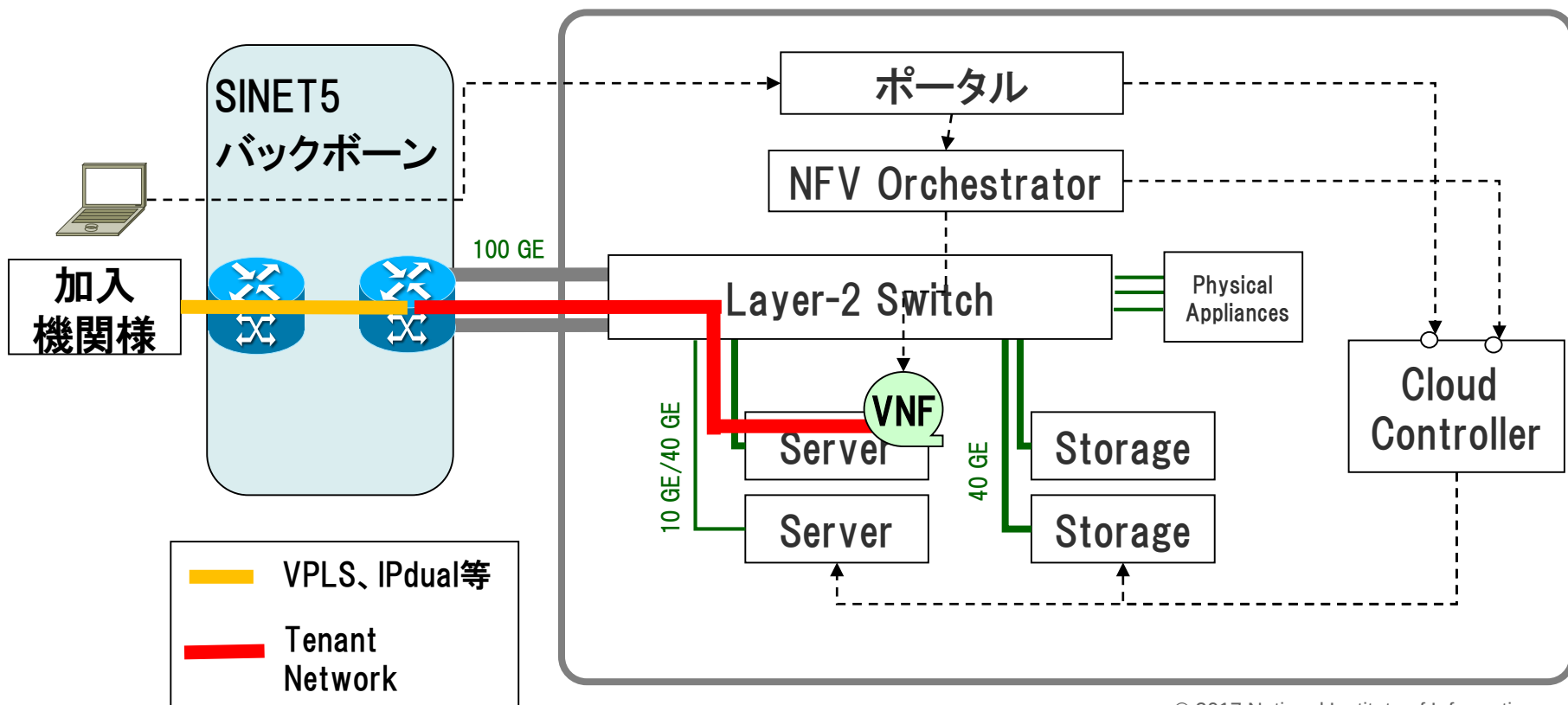
オートヒーリング後のvRouter



VM(Webサーバ等)

NFVプラットフォーム構成イメージ

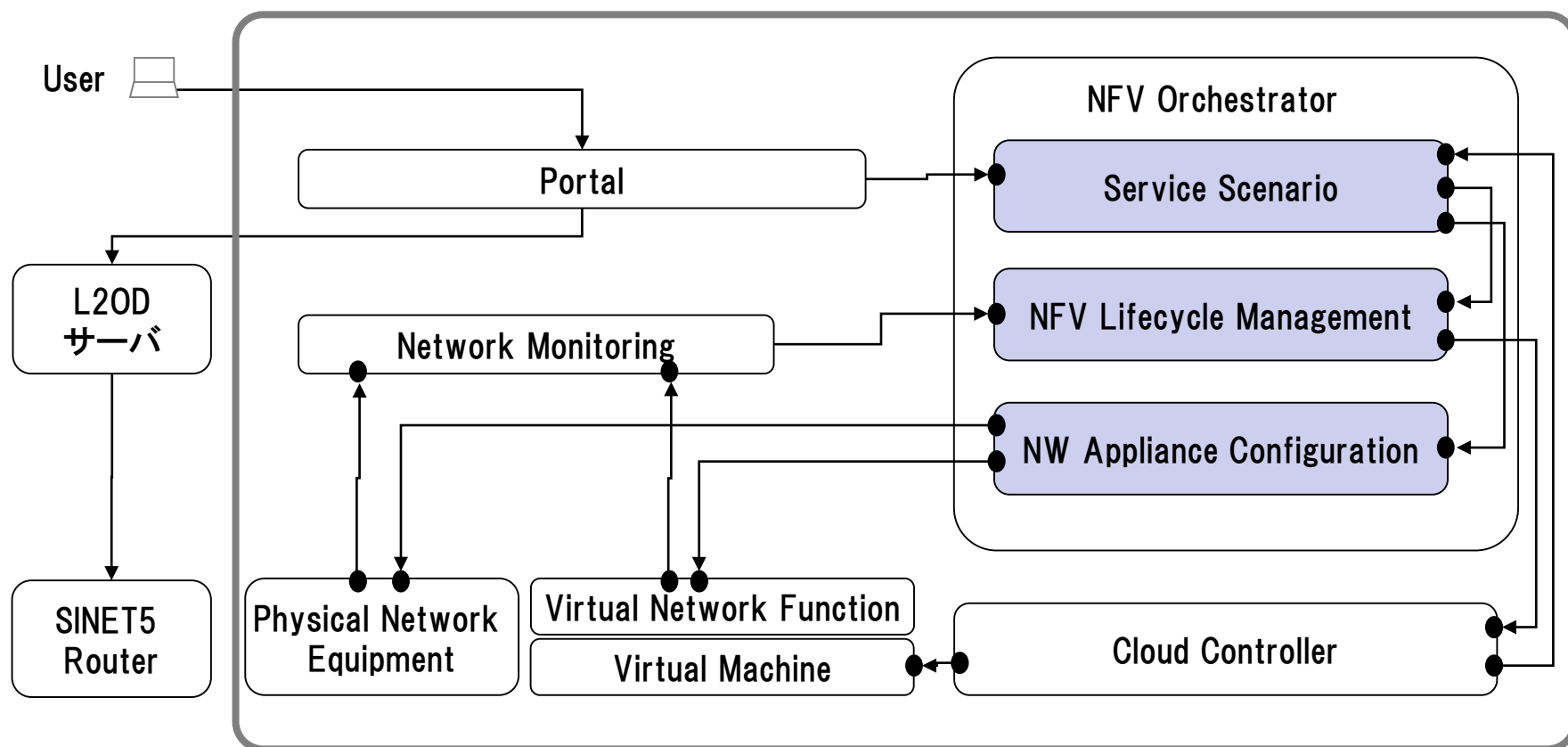
- ◆ データセンタ内にL2SWを配備し、SINET5とサーバ・ストレージを接続します。
- ◆ NFVオーケストレータ+クラウドコントローラで、仮想ルータ(vRouter)、仮想ファイヤーウォール(vFW)等の仮想化ネットワーク機能(VNF)をサーバ上に構成します。
- ◆ SINETとデータセンタ間をVPN等で接続することで、VNFにアクセスが可能となります。



NFVオーケストレータ構成

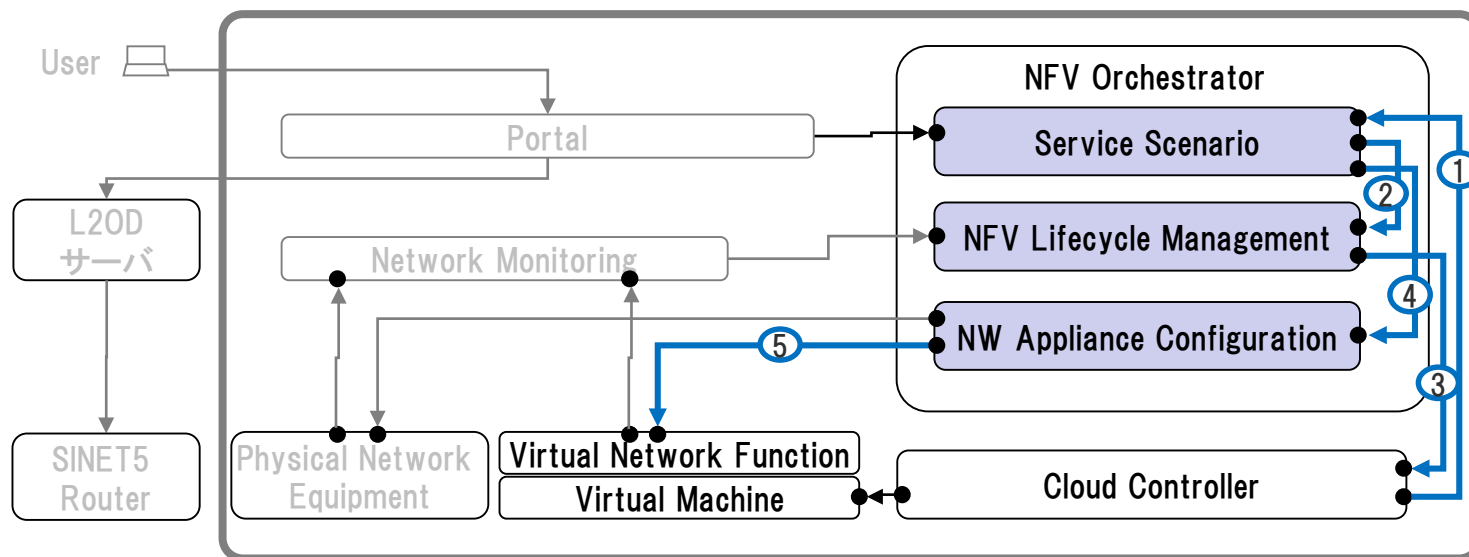
◆ NFVオーケストレータは3つの機能要素から構成されています。

- ・ サービスシナリオ(Service Scenario)
- ・ ライフサイクル管理(NFV Lifecycle Management)
- ・ NW装置設定(NW Appliance Configuration)



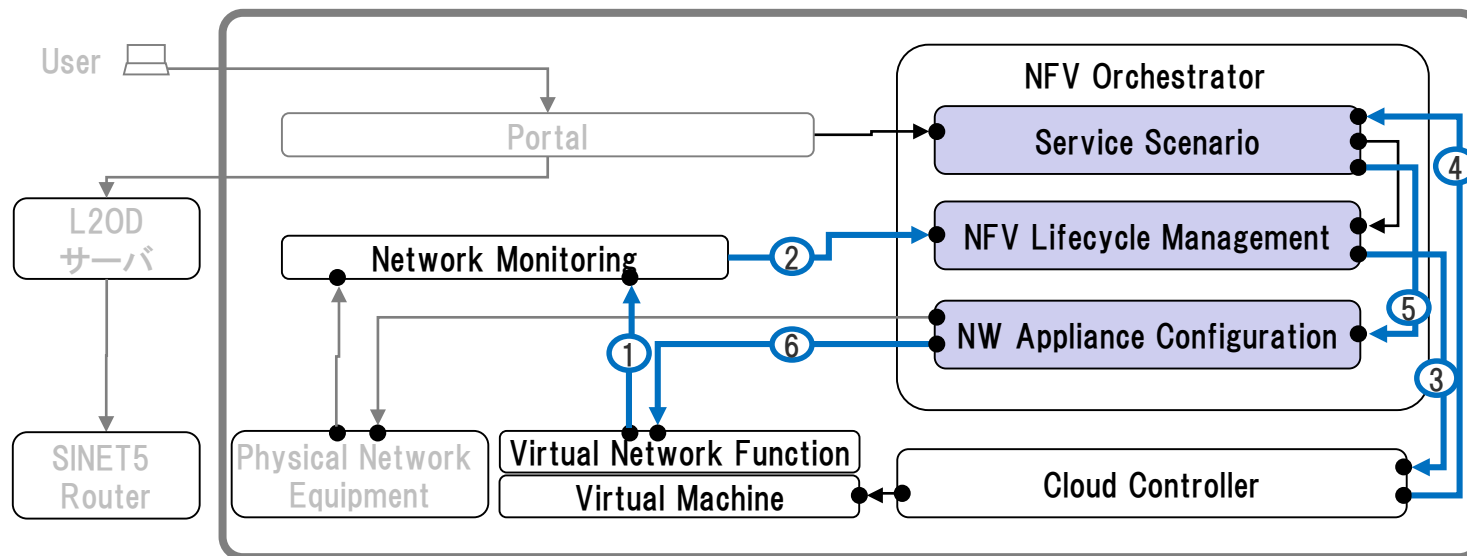
vFW オートスケーリング シナリオ動作

- ① Cloud Controllerが各VMのCPU負荷を定期的に監視。
閾値を一定回数(N回)連続で超過をトリガーにService Scenarioを起動
- ② Service Scenario部は事前に設定したシナリオに沿って動作。
vFWを追加するためにNFV Lifecycle Management部にVM起動を指示
- ③ NFV Lifecycle Management部は、Cloud ControllerにVM起動を指示
- ④ Service Scenario部はVMの起動完了を待ち受け。起動完了の信号受信後、NW Appliance Configuration部へvFWのセットアップを指示
- ⑤ NW Appliance Configuration部は、vFWのコンフィグを投入しFW機能を起動



VNF オートヒーリングシナリオ動作

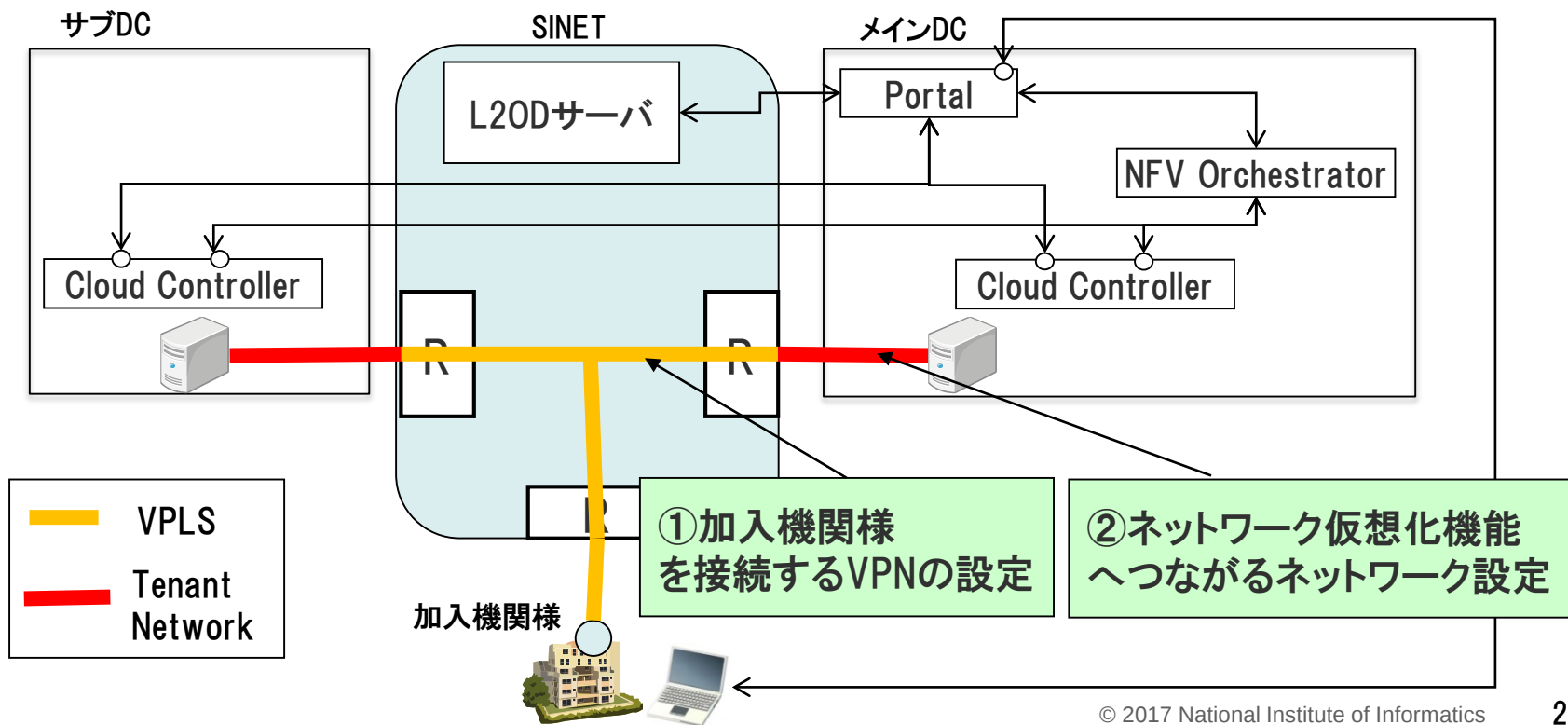
- ① Network Monitoring部が定期的にVNFの障害を監視
- ② 一定時間VNFの動作が確認できない場合、NFV Lifecycle Management部に通知
- ③ NFV Lifecycle Management部は、Cloud ControllerにVM削除、新規VM作成を指示
- ④ Cloud ControllerからService Scenario部にVMの起動完了を通知。
- ⑤ NW Appliance Configuration部へVNFのセットアップを指示
- ⑥ NW Appliance Configuration部は、VNFのコンフィグを投入しVNFを起動



SINETとクラウドDC間の連携機能

◆ SINET内のVPN(VPLS)と、NFV-DCに構成したネットワーク仮想化機能とを、自動的に接続するための機能の検討を行っています。

- ① 加入機関様からNFV-DC間のVPNを設定
- ② ネットワーク仮想化機能はオーケストレータ/クラウドコントローラで設定
- ③ 上記、①と②を接続



-

◆ Web画面からVPNの設定(VPNグループ選択、予約時刻、経路指定等)が可能

ログイン画面

ネットワーク制御システム

ユーザID

パスワード

ログイン

新規登録の方は[こちらをクリックしてください](#)

NWCS VPNグループ選択画面

ホーム

ユーザ情報
登録内容更新
利用履歴

VPN管理
VPN設定
VPN予約一覧

VPNグループ選択

VPNグループ選択 > VPN選択 > VPNポート選択 > VPN予約

VPNグループを選択してください

研究プロジェクト	VPN-G名	VPN	加入機関サイト	選択
大プロジェクト	test1VPN	無	大学KのABCキャンパス aaa 大学KのXYZキャンパス 大学の地方キャンパスの食堂	☐
小プロジェクト	test100	無	大学B 大学A	☒

次へ

NWCS VPN予約時刻等の設定画面

ホーム

ユーザ情報
登録内容更新
利用履歴

VPN管理
VPN設定
VPN予約一覧

VPN予約

VPNグループ選択 > VPN選択 > VPNポート選択 > VPN予約

利用する期間と帯域を入力してください

VPN-G名	test100
種別	L2VPN
VPN名	L2VPN-test4

加入機関サイト	VLAN	日時	転送クラス	設定帯域	経路指定
大学B 大学A	66 80	2016/03/28 15:26 - 2016/03/28 15:27	BE(低廃棄)	0 Gbps	未指定

予約

◆ L20Dで設定するVPNと、NFVで設定するネットワークとを連携して設定します

①L20Dで設定するVPN情報の投入

VPNグループ選択

VPNグループ名 SINETS-L20D-PROJECT

VPNグループ A
VPNグループ B
VPNグループ C
VPNグループ D

2017-03-27 18:32 ~ 2017-04-03 18:32

次へ 戻る

©2017-Copyright

OpenStackプロジェクト選択

プロジェクト名

admin
all_demo
demo

次へ 戻る

©2017-Copyright

③L20D-クラウドそれぞれの情報を突合し、
設定可能なVPN情報としてまとめて表示
→この画面からVPN設定を実施

VPN接続予約ポータル 予約登録・更新

再取得

VPNグループ名 SINETS-L20D-PROJECT ステータス

VPN名

NFV-DCサイト

☐ 北海道1-SiteH-1000
☐ 東京1-SiteT-1000
☐ 大阪-SiteO-1000
☐ 福岡2-SiteF-1000

接続VM参照
接続VM参照
接続VM参照
接続VM参照

NFV-DC外サイト

☐ 静岡-SiteS
☐ 富山-SiteM
☐ 石川-SiteI
☐ 千葉-SiteC

2001
2002
2003
2004

VPN接続日時 2017-03-27 18:45 ~ 2017-04-03 18:45

QoS設定 BPS制限

VPN種別 VPLS

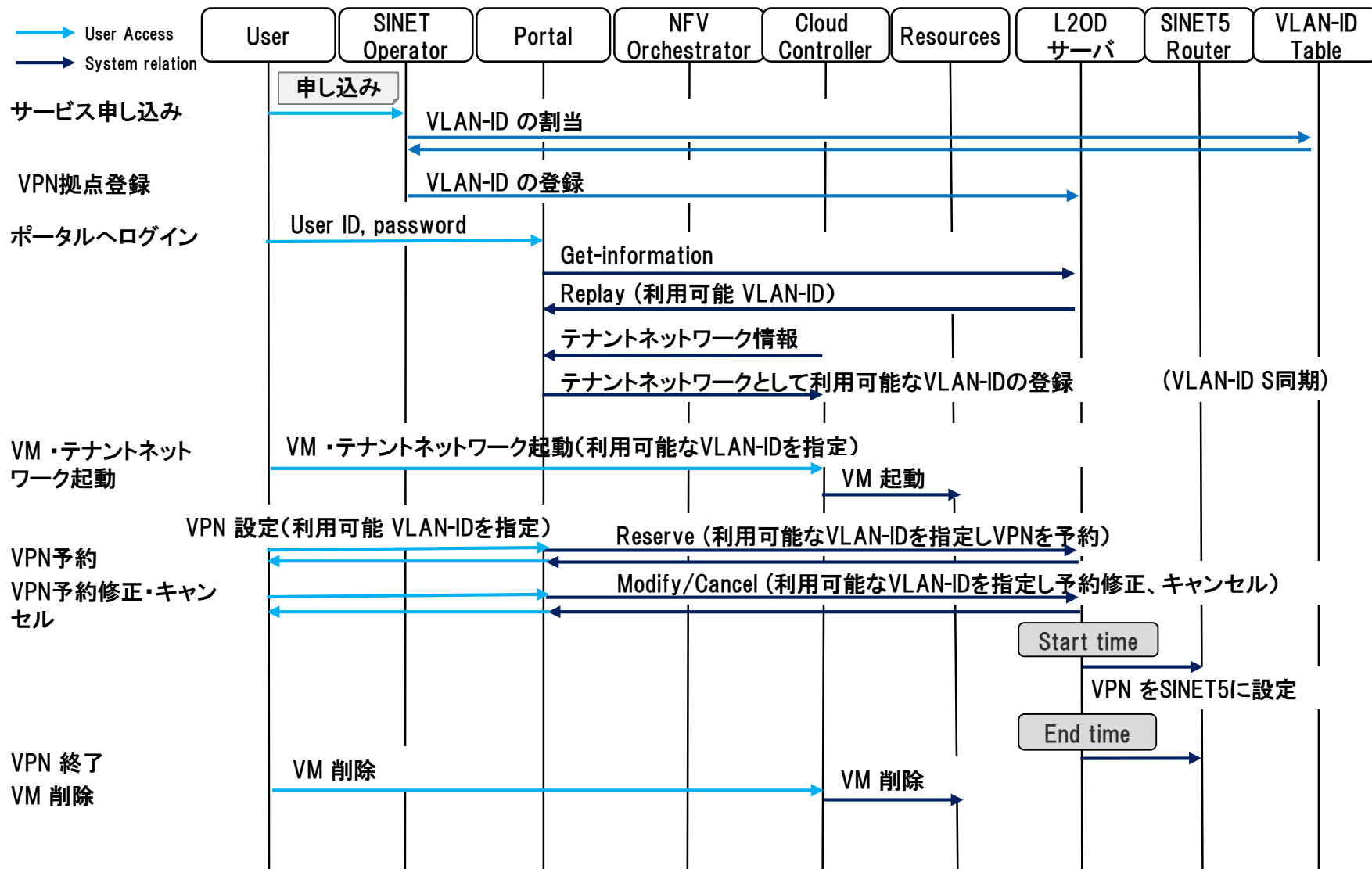
予約・更新 戻る

©2017-Copyright

②クラウドで設定するプロジェクト情報の投入

(参考) L20DサーバとNFVの連携機能

◆ L20Dサーバにて設定を行うVPNと、NFVを接続する機能を検討しております



- ◆ 先般、表記Webアンケートにご協力いただき、誠にありがとうございます。
- ◆ webアンケート結果概要について御報告させていただきます。

件名

新サービスに関するwebアンケートについて

主旨

NFVサービスに関する需要があるかの調査目的のため、2項目についてwebアンケートを実施。

調査項目

「ネットワーク機能仮想化サービストライアル」

「VPN Exchange Pointサービス」

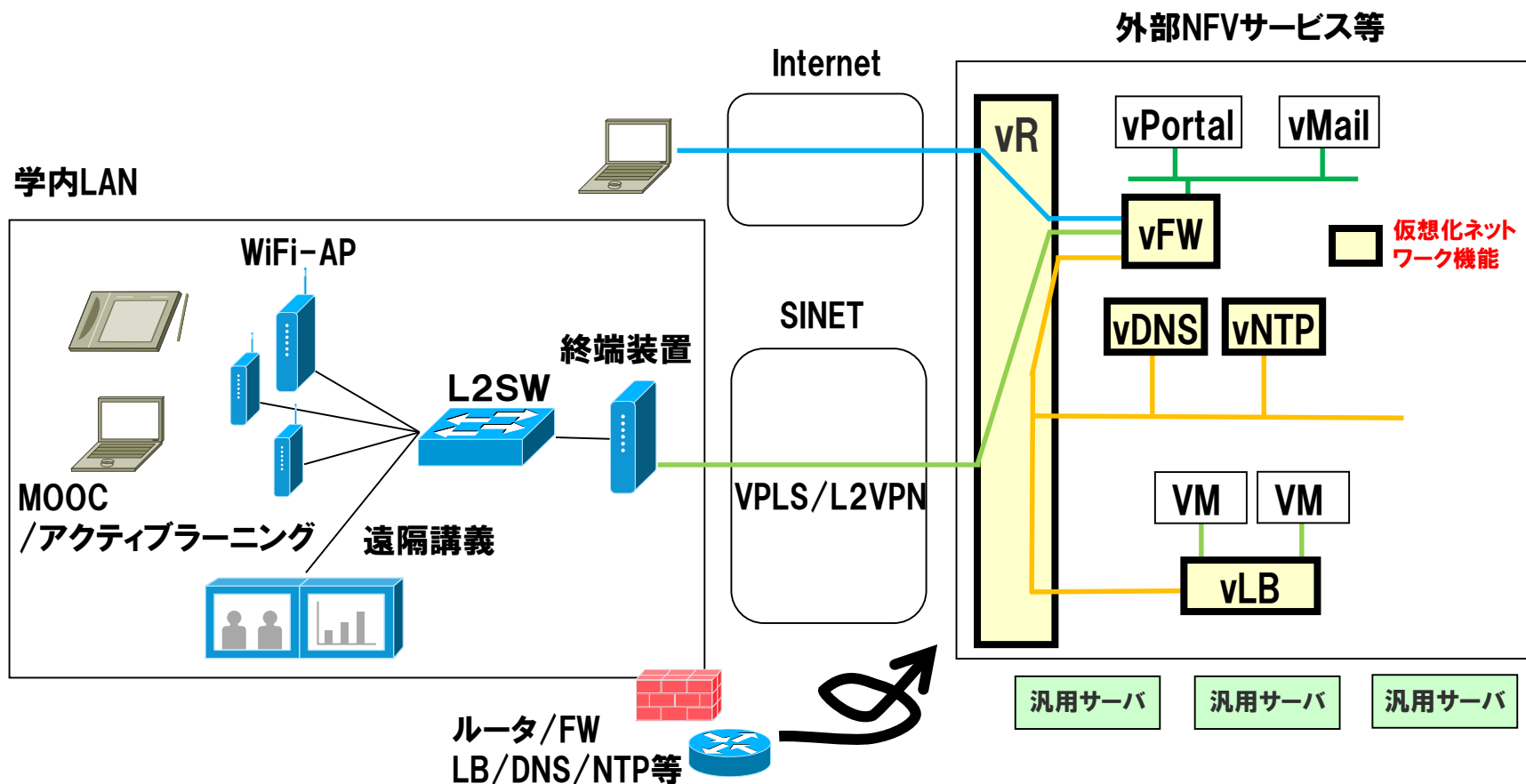
期間

2016/8/1～2016/10/末

アンケート実施対象

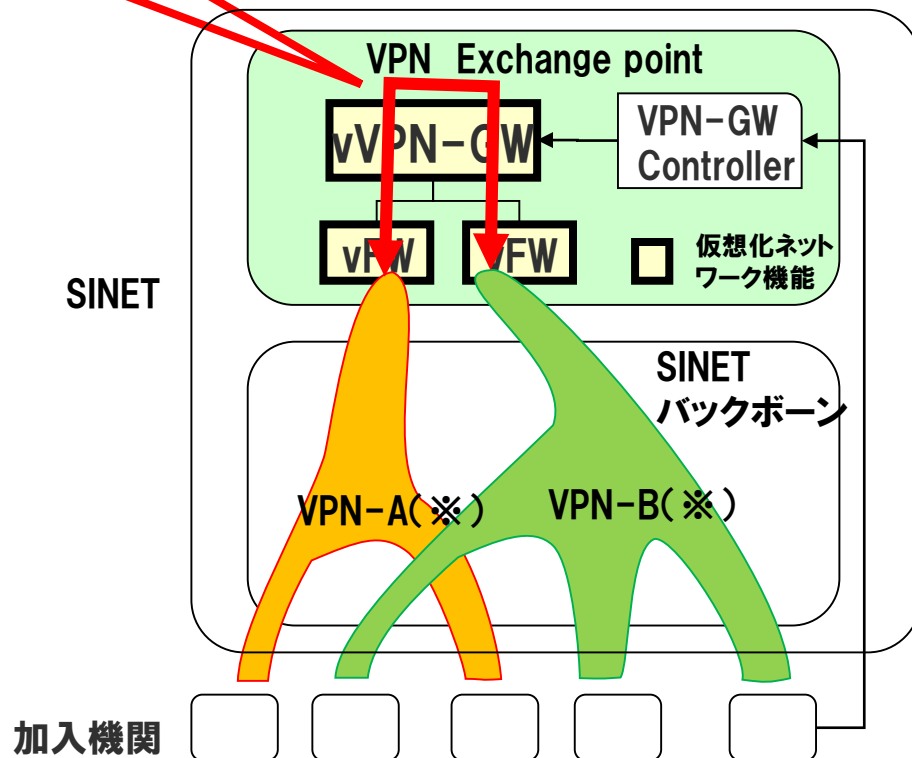
SINET加入機関、回線の登録者

- ◆ 加入機関様のロケ内に配備がなされていた各種ネットワーク装置を、外部NFVサービスにアウトソーシング化する。(構内LANはシンプルな機器を中心に配備し、運用管理を簡易化)
- ◆ 特定の機能に対する突発的な需要増減や、構成変更への柔軟な対応、リソース集約／共用によるコスト削減などが期待できます



- ◆ 加入機関様の異なるVPN(図はVPN-AとVPN-B)間を、NFVサイトに配備する仮想化ネットワーク機能を介して接続を行います。

異なるVPN間で
トラフィックを疎通



- (※)SINET-VPNサービス
- ・L2VPN/VPLS
 - ・L3VPN
 - ・仮想大学LAN
 - ・L2オンデマンド

- ◆ 166の機関から回答をいただいた。1割強の機関は具体的にNFV検討を進めており、9割以上の組織が関心を持たれている。
- ◆ 5割弱の機関からネットワーク機能仮想化サービストライアルに興味ありとご回答をいただいた

質問事項

回答(有効回答数 166/対象数 約800)

Q1 特定のネットワーク機能に対する、突発的な需要増減や構成変更への柔軟な対応が望めますか？	Yes 60 (36%) / No 106 (64%)
Q2 Q1がYesの場合、いずれのネットワーク機器が対象となりますか？(複数選択可)	ファイヤウォール 54 (90%) 、 ルータ 41 (68%) ロードバランサー 27 (48%) 、 その他(※1)
Q3 Q1がYesの場合、NFVは候補となりますか？(複数回答可能)	候補として検討中 12 (20%) 時間があつたらNFVを検討したい 43 (73%) NFV以外で検討中 8 (13%)
Q4 貴機関では、ネットワーク整備のためのコスト削減を進めていますか？	Yes 107 (64%) / No 59 (36%)
Q5 Q4がYesの場合、NFVは候補となりますか？	候補として検討中 14 (13%) 時間があつたらNFVを検討したい 62 (58%) NFV以外で検討中 27 (25%)
Q7 貴機関では、学内ネットワーク更改(※2)を予定していますか？	予定している 94 (56%) 予定していない 29 (17%) 未定 53 (27%)
Q8 NFVテストベッドに興味がありますか？	Yes 86 (52%) / No 80 (48%)

※1 L2スイッチ、無線LAN-AP、DNS、SSL VPN-GW、IDS/IDC、Webサーバ、MLサーバ、ドメイン認証サーバ、事務局システム・就職支援システム

※2 ここでのネットワーク更改とは、学内LANなどの大掛かりなもの、NFV化の対象となるネットワーク機器(ゲートウェイルータ、基幹ルータ、FW/DNS等)などの機器の更改を対象としています。

- ◆ 「VPN間接続に対する需要あり」と、3割弱の機関からご回答いただいた。
- ◆ VPN間接続の利用用途は、自組織内VPNが9割、他機関VPN接続も4割弱あるとの結果。
- ◆ また、数分以内でのVPN接続といった、即応性についても需要があるとの回答をいただいた。

質問事項		アンケート対象数 約800	有効回答数 166
Q1 VPN間の接続を行う必要がありますか？	☐ Yes ☐ No	47 (28%) 119 (72%)	
Q2 VPN間の接続を行うのは、どのような利用用途のVPNですか(複数回答可)	☐ 情報システム接続用VPN ☐ 研究用途VPN ☐ その他(自由記載:)	33 (70%) 31 (66%) 6 (13%)	
Q3 接続先のVPN候補の責任機関は？(複数回答可)	☐ 自機関内のVPN ☐ 他機関のVPN ☐ その他(自由記載:)	42 (89%) 18 (38%) 1 (2%)	
Q4 VPN間接続にかかる時間として望まれるのは？	☐ 数分以内 ☐ 数時間以内 ☐ 数日以内	20 (43%) 18 (38%) 15 (32%)	
Q5 VPN間接続のために必要と考えるネットワーク機器は？(複数回答可)	☐ ルータ ☐ ファイアウォール ☐ その他(自由記載:)	36 (77%) 18 (38%) 4 (9%)	