


# インターネットVPN(H/W) サービス仕様書



1.7 版

2020 年 6 月 15 日

富士通クラウドテクノロジーズ株式会社

## 目次

はじめに.....	1.
1. サービス概要.....	1.
2. サービス詳細.....	3.
3. サービスの申込みと解約.....	7.
4. お問い合わせ先.....	8.
別紙1. プライベート LAN でのネットワーク設定例.....	9.

## はじめに

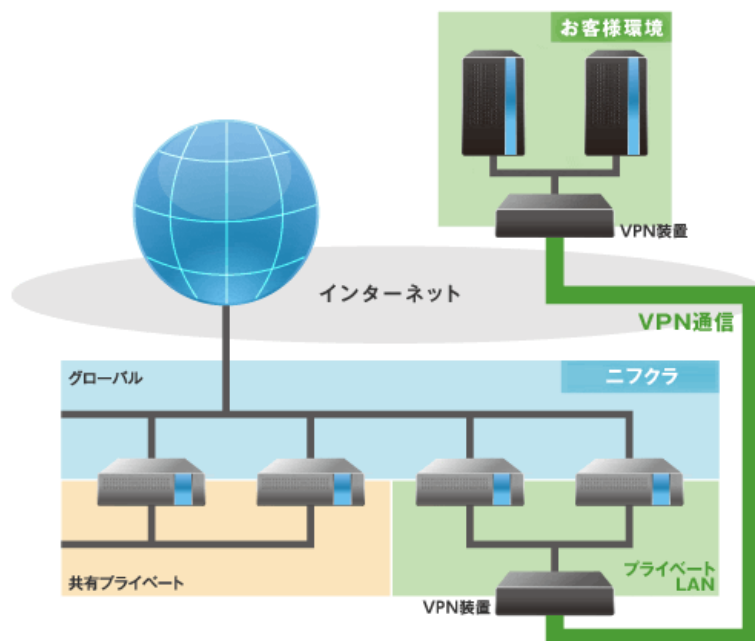
本サービス仕様書は、ニフクラユーザー（以下「お客様」という）に対して富士通クラウドテクノロジーズ株式会社（以下「当社」という）が提供するVPN接続サービスの内容を定めるものです。

## 1. サービス概要

ニフクラ内に当社がVPN装置およびVPN接続環境をご用意いたします。

ニフクラ内のお客様サーバーを共用ネットワークから隔離し、独立したネットワーク環境を構築します。サブネットごとに環境が隔離されるため、サーバーに対して自由にプライベートIPアドレスを振ることができます。

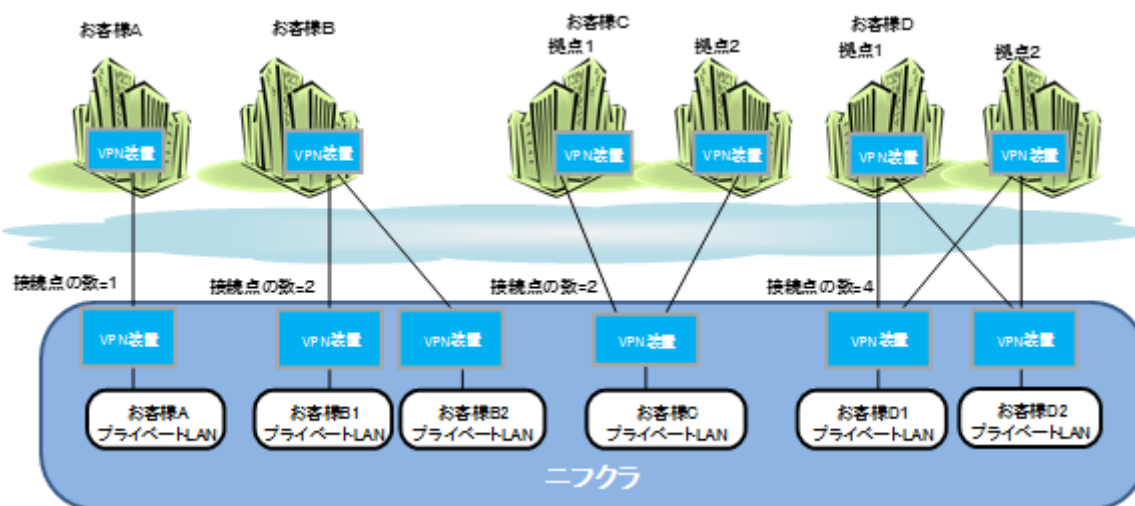
また、お客様社内／拠点のVPN装置からニフクラ内にインターネットVPN (IPsec-VPN) で接続することでニフクラとお客様社内サーバーをセキュアでシームレスに通信することが可能となり、ニフクラをお客様社内環境の延長として扱うことができますようになります。



### ・提供サービス

メニュー	サービス内容	契約単位
初期導入設定	<ul style="list-style-type: none"><li>・ニフクラ内に VPN 装置を用意し、お客様のニフクラプライベート LAN とニフクラ内 VPN 装置の接続設定を行います。</li><li>・ニフクラ内にお客様のプライベート LAN の設定を行います。</li><li>・ニフクラ内の VPN 装置にお客様拠点から接続するためのお客様専用のグローバル IP アドレスを 1 個提供します。</li><li>・お客様社内システムの VPN 装置に設定する情報とプライベート LAN に設定する情報を提供します。</li><li>・導入時の Q&amp;A に対応します。</li></ul>	/拠点数
月額利用サービス	<ul style="list-style-type: none"><li>・VPN 接続サービスを月額固定料金で提供します。</li><li>・サービス運用時の Q&amp;A に対応します。</li><li>・ニフクラ内の VPN 装置の障害、メンテナンス情報等を通知します。</li></ul>	/拠点数

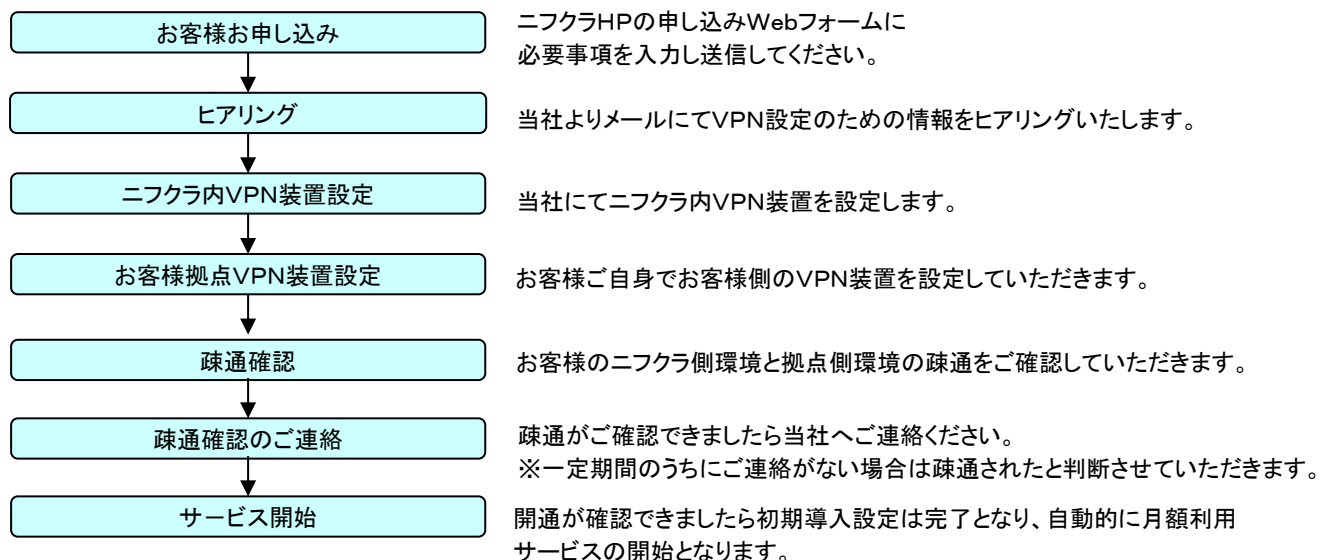
接続点の数え方の例を示します。



注)お客様拠点のVPN装置はすべてシングル構成で示しています。

## ・お申し込みからサービス開始までの流れ

### (1) 基本サービス



### (注意)

ヒアリングにおいて本サービスが適用出来ないと当社が判断した場合、本サービスのお申し込みはキャンセルされます。

## 2. サービス詳細

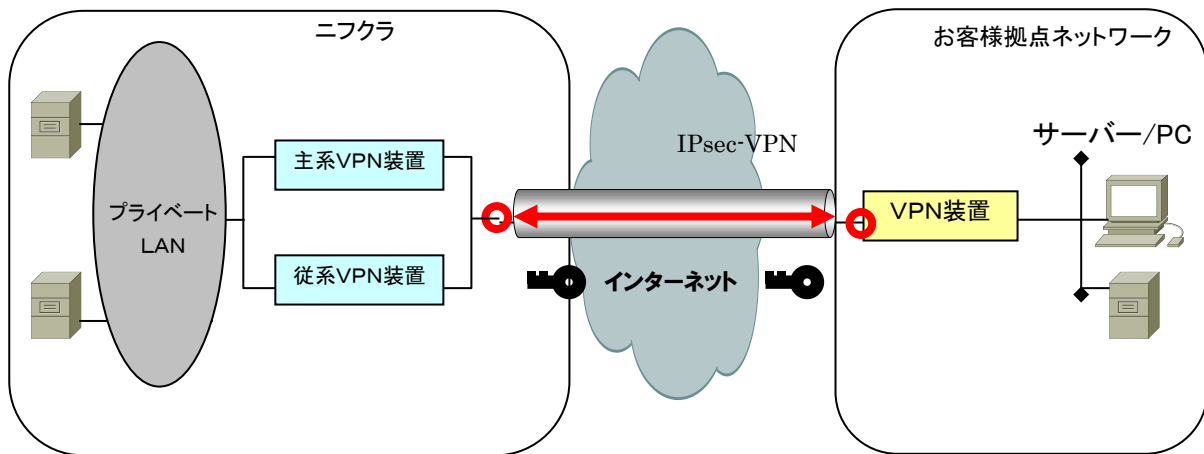
### 2. 1. サービス仕様

#### (1) 接続イメージ

本サービスが対応する一般的なお客様拠点の構成として以下の2タイプを想定しています。

##### A) インライン型構成

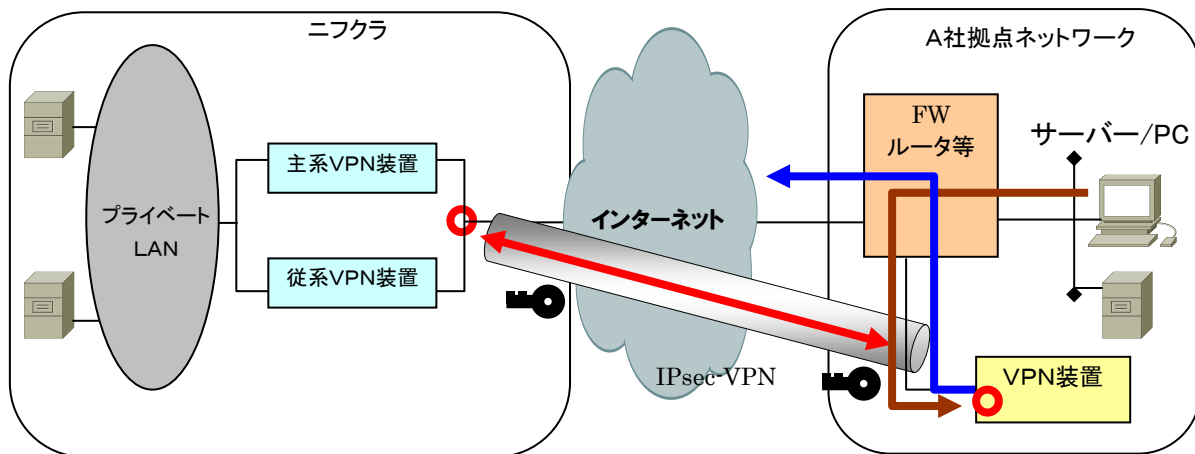
一般的な接続で、通信している経路の途中にVPN装置が設置されている構成となります。



##### B) ワンアーム型構成

VPN装置をDMZに設置する場合やインタフェースが1口しか空いていない装置などに使用します。

以下の構成では、A社PCは必ずFW／ルータを経由して対向VPN装置にPeerを張り、対向サーバーに接続します。この時、A社PCはIPsec VPNを張らずに直接FW装置から接続することはできません。

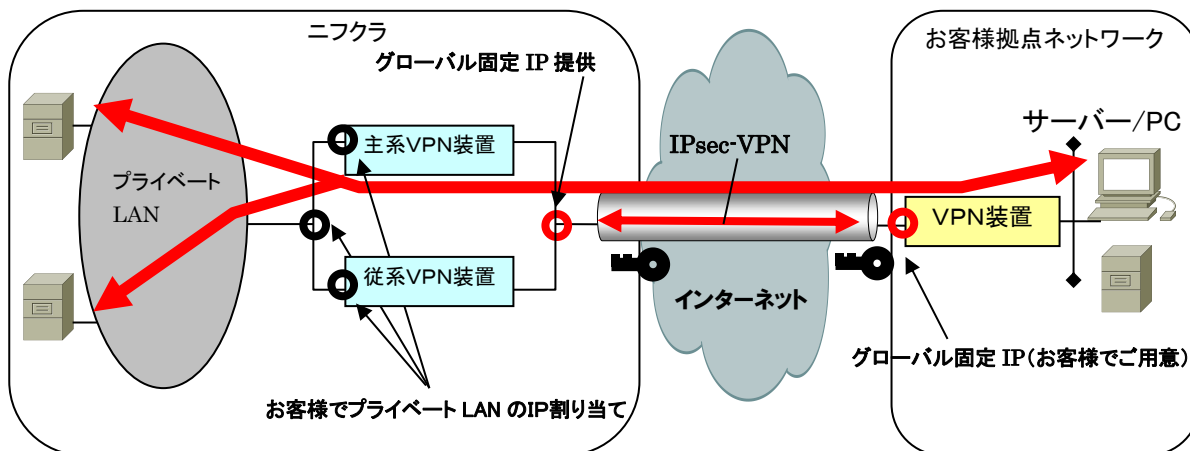


## (2) ニフクラ内VPN装置との接続

お客様のニフクラプライベートLAN(以降、「プライベートLAN」という)と拠点ネットワークをVPN接続するためには、ニフクラ内VPN装置をプライベートLANとお客様拠点のVPN装置に接続する必要があります。

プライベートLANとニフクラ内VPN装置との接続を行うには、VPN装置にプライベートLAN内のIPアドレスを3つ割り当てる必要があり、お客様よりIPアドレスをご指定頂きます。

ニフクラ内VPN装置とお客様拠点内VPN装置の接続を行うため、クラウド内VPN装置のインターネット側のグローバルIPアドレスをお客様専用IPアドレス(固定)として提供します。



## (3) VPN接続仕様

以下にVPN装置設定情報およびお客様拠点のネットワークに設定する情報を示します。

### A) ニフクラ内 VPN 装置 IP アドレス

IP アドレス	設定値
グローバル IP アドレス※	お申込み時に通知
プライベート LAN アドレス	お客様で指定

※IPv4アドレスを1個提供します。IPv6アドレスは提供できません。

### B) ニフクラ側VPN装置 IPsec の仕様

IPsecのISAKMP SA(IKE Phase1)パラメータ仕様を以下に示します。

ISAKMP SA のパラメータ	設定値
Encryption(暗号化アルゴリズム)	aes (128bit)
Hash(ハッシュアルゴリズム)	sha
ISAKMP SA Lifetime	86400 /秒
Authentication(認証方式)	pre-share
パスフレーズキー	お申込み時に通知
VPN Peer アドレス	お申込み時に通知
Group(DH グループ)	Group2 (1024bit)
Keep Alive(生存確認)	有効※

※極力短い間隔での設定を推奨します。

IPsecのIPSEC SA(IKE Phase2)のパラメータ仕様を以下に示します。

IPSEC SA のパラメータ	設定値
Transform Type(ESP 暗号化トランスフォーム)	esp-aes (128bit)
Transform Type(ESP 認証トランスフォーム)	esp-sha-hmac
IPsec 通信モード	tunnel mode
VPN Peer アドレス	お申込み時に通知
PFS	Group2 (1024bit)
IPsec SA Lifetime	3600 /秒
セレクト(通信元/通信先サブネット)	お客様にて指定

### C) アクセス制御方式

お客様拠点のネットワークに以下の通信プロトコルを許可する設定を行う必要があります。  
詳細はお申し込み時に通知いたします。

#### ・インライン型構成

送信元	送信先	プロトコル	許可／禁止
ニフクラ内 VPN 装置	お客様 VPN 装置	icmp	許可
同上	同上	ESP (Protocol: 50)	許可
同上	同上	AH (Protocol: 51)	許可
同上	同上	isakmp(500/udp)	許可

#### ・ワンアーム型構成

送信元	送信先	プロトコル	許可／禁止
ニフクラ内 VPN 装置	お客様 VPN 装置	icmp	許可
同上	同上	ESP (Protocol: 50)	許可
同上	同上	AH (Protocol: 51)	許可
同上	同上	isakmp (500/udp)	許可
お客様拠点内部セグメント	ニフクラ プライベート LAN セグメント	お客様指定	許可

(注意)ワンアーム型VPN装置の上位装置にて、プライベートLANセグメント向けの  
ルーティング設定をワンアーム型VPN装置に向けていただく必要があります。

#### (4) お客様拠点でご使用になられるVPN装置について

お客様拠点でご使用されるVPN装置については特に制限はございません。但しすべての装置の接続を保証するものではありません。

#### (5) プライベート LAN について

プライベート LAN は、クラウドのプライベート側ネットワークにて、お客様のサーバーを共用ネットワークから隔離し、独立したネットワーク環境とするための設定です。サブネットごとに環境が隔離されるため、プライベート LAN 内のサーバーに対して自由にプライベート IP アドレスを振ることができます。

VPN通信を行うためには、当社がプライベートLANを設定後、お客様ご自身でプライベートIPの設定、プライベートインタフェースのルーティング設定、プライベートインタフェースのファイアウォール設定を行って頂く必要があります。  
※別紙1に設定例を添付しておりますのでご参照ください。

#### (6) サービス利用上の前提条件

- ・インターネット回線はお客様でご用意ください。また、お客様の拠点WAN側IPは固定IPでのみ対応します。
- ・本サービスの申し込み時に、「プライベート LAN ID」をご指定いただきます。ご指定の ID のプライベート LAN に対して接続を行います。また、プライベート LAN に追加するサーバーの指定は、コントロールパネルから行うことができます。  
※本サービスの申し込み時に指定したプライベート LAN は、本サービスのご利用中は削除できません。  
(本サービス解除後に、削除可能です)
- ・プライベート LAN 内のサーバーのプライベート IP を手動で設定している場合、サーバーをコピーすると、コピー元のサーバーのプライベート IP 設定もコピーされるためアドレスの衝突が発生します。  
コピーされたサーバーにログインし、プライベート IP アドレスを変更して、アドレスの衝突を解消してください。
- ・ニフクラサービスをお申し込みになられた時期によっては準備期間が必要な場合があります。
- ・リモートアクセスVPN機能は提供しておりません。LAN間接続VPN機能となります。
- ・VPN通信帯域はベストエフォートで30Mbpsを上限とします。30Mbps以上を希望される場合は、別途ご相談ください。
- ・ご利用可能なプロトコルは、IPプロトコルのみとなります。
- ・共用ネットワーク環境での IP アドレス変更は禁止です。
- ・お客様環境内のネットワーク装置で設定変更(ルーティング設定等)が必要な場合は、お客様にて変更いただく必要があります。

## 2. 2. サービス内容

### (1) 初期導入設定

- ・VPN設定情報の決定  
お客様と設定情報を決定します。連絡は原則メールにて行うものとします。
- ・ニフクラ側VPN環境、プライベートLAN環境の設定作業  
決定した情報をもとにニフクラ側の設定を実施します。
- ・お客様設定に関するQ&A対応  
お客様環境のVPN設定に関するお問合せに回答します。  
※装置固有のご質問、VPN設定、プライベートLAN設定以外のお客様環境個別のご質問は対象外となります。  
※お客様環境の設定ならびにオンサイトでの作業は含みません。
- ・設定情報の追加および変更時は本サービスの再契約が必要となります。

### (2) 月額利用サービス

- ・インターネットVPN(H/W)環境の提供

サービスレベル	内容
サービス時間	24 時間 365 日(計画停止を除く) セキュリティ改善やシステム影響があると判断した場合は事前に通知の上、メンテナンスを実施します
メンテナンス通知	通信影響が有る場合、1ヶ月前にメールにて告知 通信影響が無い場合、2週間前にメールにて告知 緊急の場合、事前、事後にメールにて告知
メンテナンス方針	当社判断のもと実施するものとします。
障害通知	監視検出の後、メールにて通知します

- ・Q&A対応  
インターネットVPN(H/W)に関するご質問、VPN接続状態の確認に対しお答えします。  
24時間365日メールにて受付。対応は当社営業時間内(年末年始・土日・祝祭日除く)となります。  
※お客様側の装置に関する質問は対象外とします。



### 3. サービスの申込と解約

#### 3.1 サービスの申込

(1) 申込方法

以下 URL のWeb申請フォームより必要事項を入力してください。

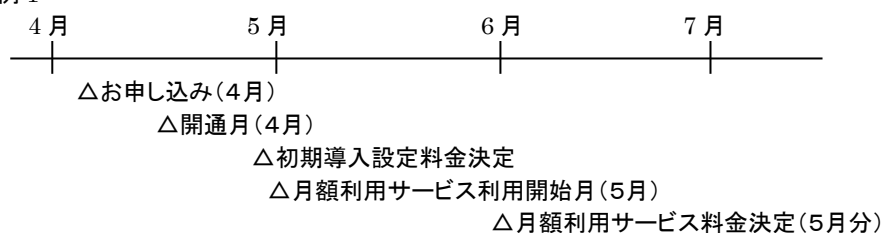
[https://inquiry.nifcloud.com/webeq/pub/cloud/vpn\\_hw\\_auth](https://inquiry.nifcloud.com/webeq/pub/cloud/vpn_hw_auth)

(2) 料金の発生とご請求について

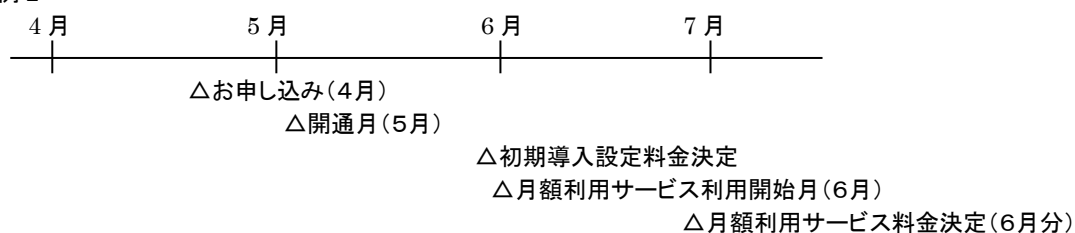
初期導入設定の料金は、ニフクラ内お客様プライベートLAN環境とお客様拠点との通信が確認できた月（開通月）の月末に料金が決定します。

月額利用サービスの料金は、開通月は無料とし、開通月の翌月を利用開始月とし翌月末に料金を決定します。いずれも日割り計算はいたしません。

例 1



例 2



(3) 月額利用サービスの最低利用期間について

最低利用期間は、1ヶ月とします。

※同時に20接続点以上のご利用をご希望される場合はお問合せ窓口にご相談ください。

### 3.2 サービスの解約

#### (1) 解約方法

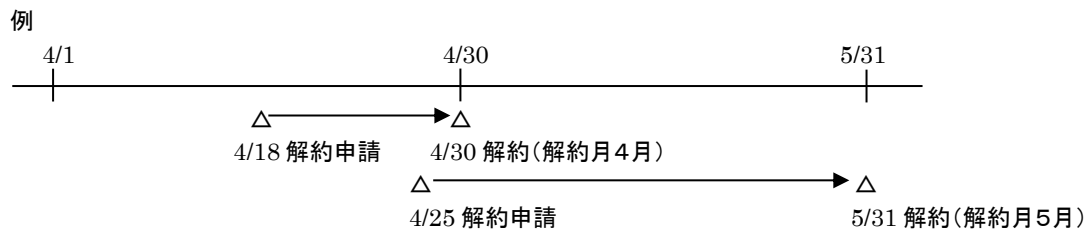
申込と同様に以下 URL のWeb申請フォームより必要事項を入力してください。

[https://inquiry.nifcloud.com/webeq/pub/cloud/vpn\\_hw\\_auth](https://inquiry.nifcloud.com/webeq/pub/cloud/vpn_hw_auth)

#### (2) 解約のタイミングと料金について

毎月 20 日までに申請を受け付けたものは、当月末日をもって解約となります。

21 日以降に受け付けたものは翌月末日の解約となり、翌月分の月額利用サービス料金をご請求いたしますのでご注意ください。日割り計算はいたしません。



解約月の翌月にVPN通信を遮断し、VPN接続サービスのご利用を停止いたします。また、ニフクラ側VPN接続用固定グローバルIPは使用出来なくなります。解約後、再開をご希望される場合、新たに初期導入設定を申し込んでいただく必要があります。ニフクラを解約する場合、解約前までに本サービスの契約を解約いただく必要があります。

### 4. お問い合わせ先

お申し込み前のお問い合わせは、ニフクラホームページ「【法人サービス】ニフクラに関するお問い合わせ」にてお受けいたしております。

以上

## 別紙1. プライベート LAN でのネットワーク設定例

### (1) サーバーのプライベートIP設定例

```
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.xxx.xxx
NETMASK=255.255.255.0
```

※ネットワークアドレスには、10.0.0.0/8 以外を設定してください。

クラウド内のプライベート IP はお客様拠点のプライベート IP と違うアドレス体系を指定してください。  
本 VPN サービスはレイヤ 3 であるため、クラウド内サーバーとお客様拠点サーバーの IP アドレスは同じセグメントに設定できません。

例	お客様拠点	クラウド	
	192.168.1.0/24	192.168.1.0/24	×
	192.168.1.0/24	172.16.1.0/24	○

### (2) ルーティング設定例

#### 【手順】

クラウドサーバープライベートI/Fにクラウド側VPN装置の仮想アドレスから拠点ネットワークに向けたルーティングを設定します。

例えばクラウド側VPN装置の仮想アドレスが「172.16.1.3」、お客様拠点のプライベートネットワークセグメントが192.168.1.0/24であった場合、192.168.1.0/24 via 172.16.1.3 metric 4 等の記述を  
/etc/sysconfig/network-scripts/route-eth1に記述します。

---

#### 【ルーティング設定例】 Linux系サーバー

Editorで編集↓

```
# vi /etc/sysconfig/network-scripts/route-eth1
192.168.1.0/24 via 172.16.1.3 metric 4 ←記述
```

以下コマンドでインターフェースのリセットを行う必要があります。

```
# ifdown eth1
# ifup eth1
```

---

#### 【ルーティング設定例】 Windowsサーバー

コマンドプロンプトを管理者権限で実行し以下のコマンドを実行します。

```
route -p add 192.168.1.0 mask 255.255.255.0 172.16.1.3
                ↑                ↑                ↑
        拠点側ネットワークアドレス  拠点側ネットワークサブネット  クラウド側VPN装置仮想アドレス
```

### (3) ファイアーウォール設定例

お客様拠点のプライベートネットワークとニフクラ側サーバーのプライベートLANとの間で許可する通信を、ニフクラのファイアーウォール機能で設定してください。

iptablesでファイアーウォールを設定している場合も同様です。

⇒具体的にいきますと、例えば、お客様拠点のプライベートネットワークセグメントが192.168.1.0/24であった場合、192.168.1.0/24の通信と、ニフクラ内部セグメントの通信のみ許可、というような設定になります。

次に、VPN通信の確認のため一時的に、クラウド側VPN装置に割り当てたIPアドレスとping(ICMP)通信の送受信が可能となるようにファイアーウォールを設定してください。

※クラウド側VPN装置はファイアーウォールの外側に位置しています。

※VPN通信の疎通確認完了後は、ping送受信が出来ないように設定を戻して頂いて構いません。



#### 【プライベート LAN 仕様】（2013 年 6 月 4 日現在）

(1) プライベート LAN 環境を構築した後に、サーバーを新規作成した場合、プライベート LAN 内に作成されます。

(2) プライベート LAN 内に新規作成したサーバーは、お客様側でプライベート IP アドレスの割り当てが可能となります。

プライベート LAN 環境に存在しているサーバー、もしくは プライベート LAN 環境に存在しているサーバーのカスタマイズイメージからコピーしてサーバーを新規作成した場合も、プライベート LAN 環境にサーバーが作成されます。

※プライベート IP ごとコピーされるので、コピーにより新規作成したサーバーには、再び IP アドレスの割り当てを行ってください。

以上