

## 5.1 機器の構成

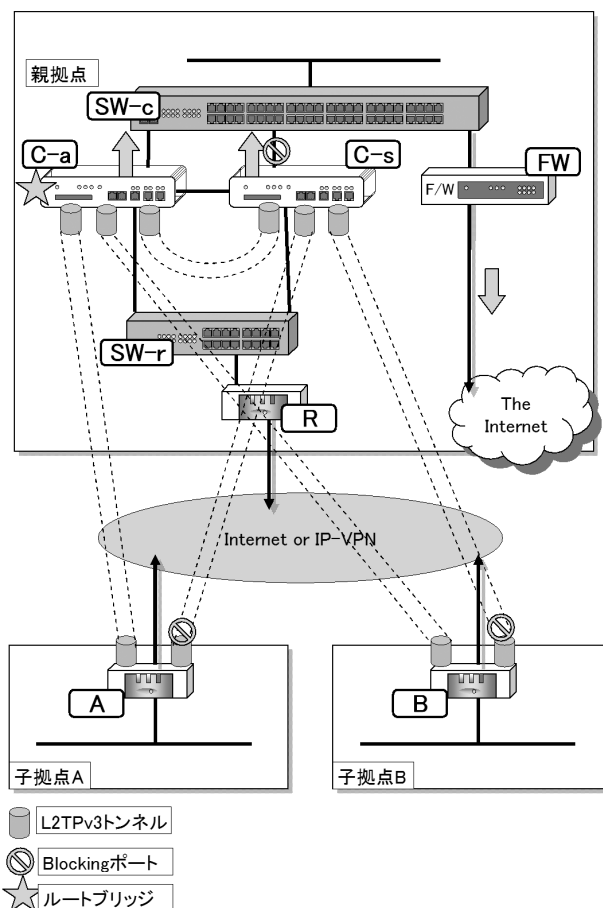
### 5.1.1 機器構成

デュアルハブ・シングルエッジ SEIL/L2-VPN は親拠点と子拠点の二種類の拠点から構成されます。子拠点は例として A,B の2 拠点を挙げていますが、設定すべき内容としては WAN 側（PPPoE）インターフェイスで使用するアカウント情報やグローバルアドレスを除いて同様となります。

本構成では各 VPN 装置において STP 機能を使用し、ブリッジの冗長リンクのループ制御を行います。そのため、VPN 装置と接続しネットワークを構成する各スイッチにおいては、BPDU を透過可能であるものを設置する必要があります。

図中の丸で囲んだアルファベット（例： X-x）は機器の識別子であり、第5章を通して使用します。

各拠点の機器構成を下図に示します。

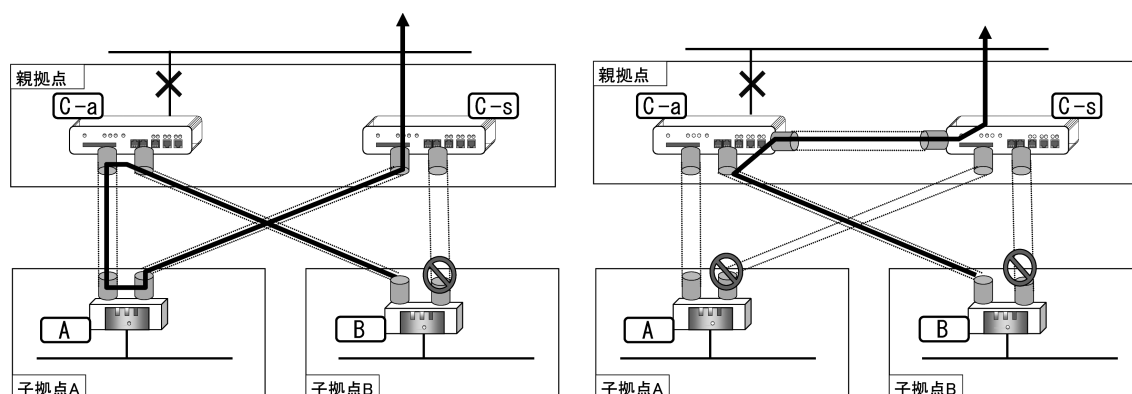


5.1. 機器の構成

5.1.2 VPN 親機間の L2TP トンネル形成について

本構成では、VPN 親機 (C-a)、(C-s) の OPTION ポート同士を接続<sup>\*1</sup>してプライベートネットワークを構築し、VPN 親機間で L2TP トンネルを形成しています。

このトンネルを設定することにより、VPN 親機 (C-a) の LAN0 (LAN 側) インターフェイスがダウンした際に、STP の動作原理によって子拠点 B からの親拠点向けトラフィックが子拠点 A の VPN 子機 (A) を経由するのを防ぐことができます。



・ VPN 親機間で L2TP トンネルを形成しない構成の場合

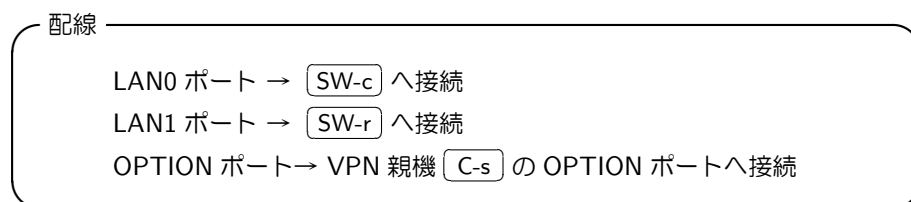
・ 本書で紹介する構成の場合

5.1.3 装置解説

親拠点

(C-a) Active 系 VPN 親機 : SEIL/Turbo

- 親拠点の VPN 親機 (C-s) とプライベート環境で L2TP トンネルを確立し、子拠点の VPN 子機 (A, B) と VPN トンネルを確立します



<sup>\*1</sup> 直接繋ぐ場合はクロスケーブルを使用します

## 5.1. 機器の構成

**C-s** Standby系 VPN 親機 : SEIL/Turbo

- 親拠点の VPN 親機 **C-a** との L2TP トンネル及び、子拠点の VPN 子機 (**A** , **B**) と VPN トンネルを確立します

配線

LAN0 ポート → **SW-c** へ接続  
 LAN1 ポート → **SW-r** へ接続  
 OPTION ポート → **C-a** の OPTION ポートへ接続

**R** インターネット接続ルータ

- 親拠点のインターネット接続（または IP-VPN 接続）のゲートウェイとなります
- グローバルセグメントを LAN 側に作成します

**SW-c** Layer-3 スイッチ

- 親拠点の LAN 内ネットワークとの接続ゲートウェイとなります
- 必要に応じて設置します

**SW-r** Layer-2 スイッチ

- VPN 親機を複数設置する必要がある場合に設置します

**FW** ファイアウォール

- VPN 親機では NAT、セキュリティコントロールは実施しません
- インターネットへの接続がある場合に、ゲートウェイとして必要に応じて設置します

## 子拠点 A

**A** VPN 子機 : SEIL/Plus

- 平常時に利用する Active 系の VPN トンネルを親拠点の VPN 親機 **C-a** と、Active 系の障害時に利用する Standby 系の VPN トンネルを親拠点の VPN 親機 **C-s** と確立します
- ブリッジと同じ挙動をするため、LAN 側ネットワーク向けの IP アドレスは付与しません
- 親拠点 LAN 側セグメントやインターネットへは **SW-c** を介してアクセスします

配線

LAN0 ポート → LAN 側ネットワークへ接続  
 LAN1 ポート → モデム/メディアコンバータへ接続

## 5.1. 機器の構成

## 子拠点 B

B VPN 子機 : SEIL/Plus

- A と同様に、親拠点の VPN 親機 ( C-a , C-s ) との VPN トンネルを確立します
- ブリッジと同じ挙動をするため、LAN 側ネットワーク向けの IP アドレスは付与しません

配線

LAN0 ポート → LAN 側ネットワークへ接続

LAN1 ポート → モデム/メディアコンバータへ接続

## その他のホスト

## NTP サーバ

I/F	Address	備考
—	10.123.0.1	インターネット上の NTP サーバのアドレス

## 遠隔保守管理ホスト

I/F	Address	備考
—	10.100.0.1	管理ホスト A のアドレス
—	10.100.1.1	管理ホスト B のアドレス

## 5.2 IP アドレス設計

各機器への IP アドレスの設定例を以下に示します。

各アドレスは、実際のネットワーク環境に合わせて適宜変更してご利用ください。

## 親拠点

## C-a Active 系 VPN 親機

I/F	Address	備考
lan0	なし	ブリッジ動作するため IP アドレスは無し
lan1	10.0.0.2/29	VPN 親機 C-a の WAN 側グローバルアドレス
lan2	172.16.0.1/24	VPN 親機 C-s との L2TP トンネル形成用アドレス
l2tp0	なし	VPN 親機 C-s との L2TP トンネルインターフェイス
l2tp1	なし	VPN 子機 A との L2TP トンネルインターフェイス
l2tp2	なし	VPN 子機 B との L2TP トンネルインターフェイス

## C-s Standby 系 VPN 親機

I/F	Address	備考
lan0	なし	ブリッジ動作するため IP アドレスは無し
lan1	10.1.0.2/29	VPN 親機 C-s の WAN 側グローバルアドレス
lan2	172.16.0.2/24	VPN 親機 C-a との L2TP トンネル形成用アドレス
l2tp0	なし	VPN 親機 C-a との L2TP トンネルインターフェイス
l2tp1	なし	VPN 子機 A との L2TP トンネルインターフェイス
l2tp2	なし	VPN 子機 B との L2TP トンネルインターフェイス

## R インターネット接続ルータ

I/F	Address	備考
lan0	10.0.0.1/29	インターネットへのゲートウェイ
pppoe0	unnumbered	接続サービスに依存して設定

## SW-c センタ LAN 内へ接続される L3 スイッチ

I/F	Address	備考
—	192.168.1.1/24	親拠点 LAN 側 L3 スイッチ

## 子拠点 A

## A VPN 子機

I/F	Address	備考
lan0	なし	ブリッジ動作するため IP アドレスは無し
pppoe0	10.0.1.1/32	VPN 子機 A の WAN 側グローバルアドレス
l2tp0	なし	VPN 親機 C-a との L2TP トンネルインターフェイス
l2tp1	なし	VPN 親機 C-s との L2TP トンネルインターフェイス

## 子拠点 B

## B VPN 子機

I/F	Address	備考
lan0	なし	ブリッジ動作するため IP アドレスは無し
pppoe0	10.0.2.1/32	VPN 子機 B の WAN 側グローバルアドレス
l2tp0	なし	VPN 親機 C-a との L2TP トンネルインターフェイス
l2tp1	なし	VPN 親機 C-s との L2TP トンネルインターフェイス

## その他のホスト

## NTP サーバ

I/F	Address	備考
—	10.123.0.1	インターネット上の NTP サーバのアドレス

## 遠隔保守管理ホスト

I/F	Address	備考
—	10.100.0.1	管理ホスト A のアドレス
—	10.100.1.1	管理ホスト B のアドレス

## 5.3 コンフィグと解説

ここでは各機器の設定内容について、実際のコンフィグを例として解説します。

Index :

<b>C-a</b>	親拠点-Active 系 VPN 親機	コンフィグ : Page.72	/	解説 : Page.76
<b>C-s</b>	親拠点-Standby 系 VPN 親機	コンフィグ : Page.81	/	解説 : Page.85
<b>A</b>	子拠点 A-VPN 子機	コンフィグ : Page.90	/	解説 : Page.94
<b>B</b>	子拠点 B-VPN 子機	コンフィグ : Page.99	/	解説 : Page.103

## 5.3.1 親拠点-Active 系 VPN 親機 : コンフィグ

コンフィグファイル : DualHub\_Ca.cfg

```

hostname "C-a"
timezone "Japan"
environment login-timer 300
Ca:1 l2tp hostname C-a
Ca:2 l2tp router-id 10.0.0.2
Ca:3 l2tp add to_C-s hostname C-s router-id 10.1.0.2 cookie off retry 5
      hello-interval 30 password L2TP-PASSWD
      l2tp add to_A hostname A router-id 10.0.1.1 cookie off retry 5
      hello-interval 30 password L2TP-PASSWD
      l2tp add to_B hostname B router-id 10.0.2.1 cookie off retry 5
      hello-interval 30 password L2TP-PASSWD
Ca:4 interface lan0 media auto
      interface lan1 media auto
      interface lan1 queue normal
      interface lan1 add 10.0.0.2/29
      interface lan2 media auto
      interface lan2 add 172.16.0.1/24
Ca:5 interface l2tp0 tunnel 172.16.0.1 172.16.0.2
      interface l2tp0 l2tp to_C-s remote-end-id C-a_C-s
      interface l2tp1 tunnel 10.0.0.2 10.0.1.1
      interface l2tp1 l2tp to_A remote-end-id C-a_A
      interface l2tp2 tunnel 10.0.0.2 10.0.2.1
      interface l2tp2 l2tp to_B remote-end-id C-a_B
Ca:6 bridge group add BG00 stp on priority 1000
      bridge interface lan0 group BG00 stp on
      bridge interface l2tp0 group BG00 stp on
      bridge interface l2tp1 group BG00 stp on
      bridge interface l2tp2 group BG00 stp on

```