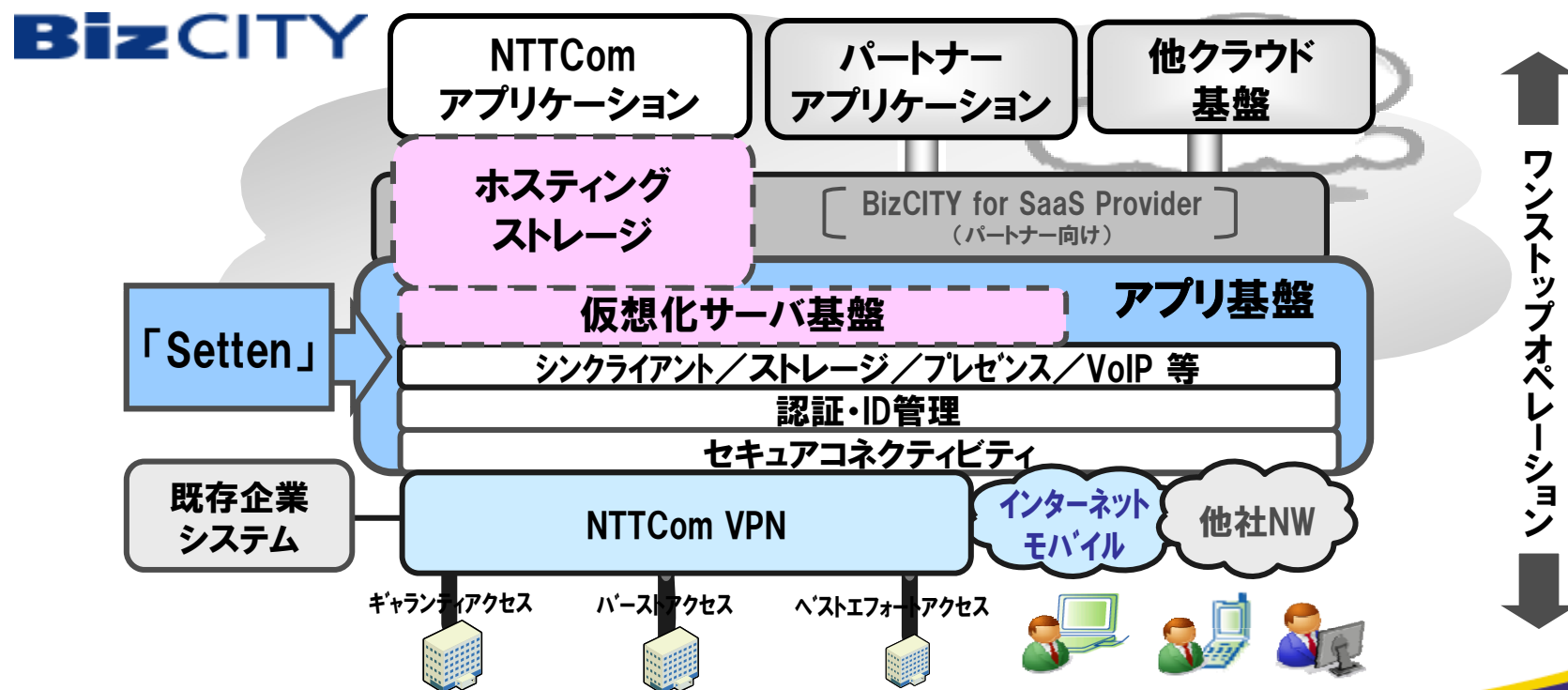


NTTコミュニケーションズの クラウド戦略

2009年12月3日
NTTコミュニケーションズ株式会社
ビジネスネットワークサービス事業部
村上 守
高橋 健太

NTTコミュニケーションズのBizCITY戦略

- ユビキタスなオフィス環境をセキュア・高品質に実現する「BizCITY」サービスの開発を推進中
 - ・ 既存のICT環境と各サービスをシームレスにつなげる
 - ・ あらゆるネットワーク（インターネット、VPN、モバイル）を介し、セキュアにサービスが使える
 - ・ 様々なデバイス・端末においても、同じユーザーインターフェースで使える
 - ・ SaaS等パートナーと連携し、様々なアプリケーションを準備



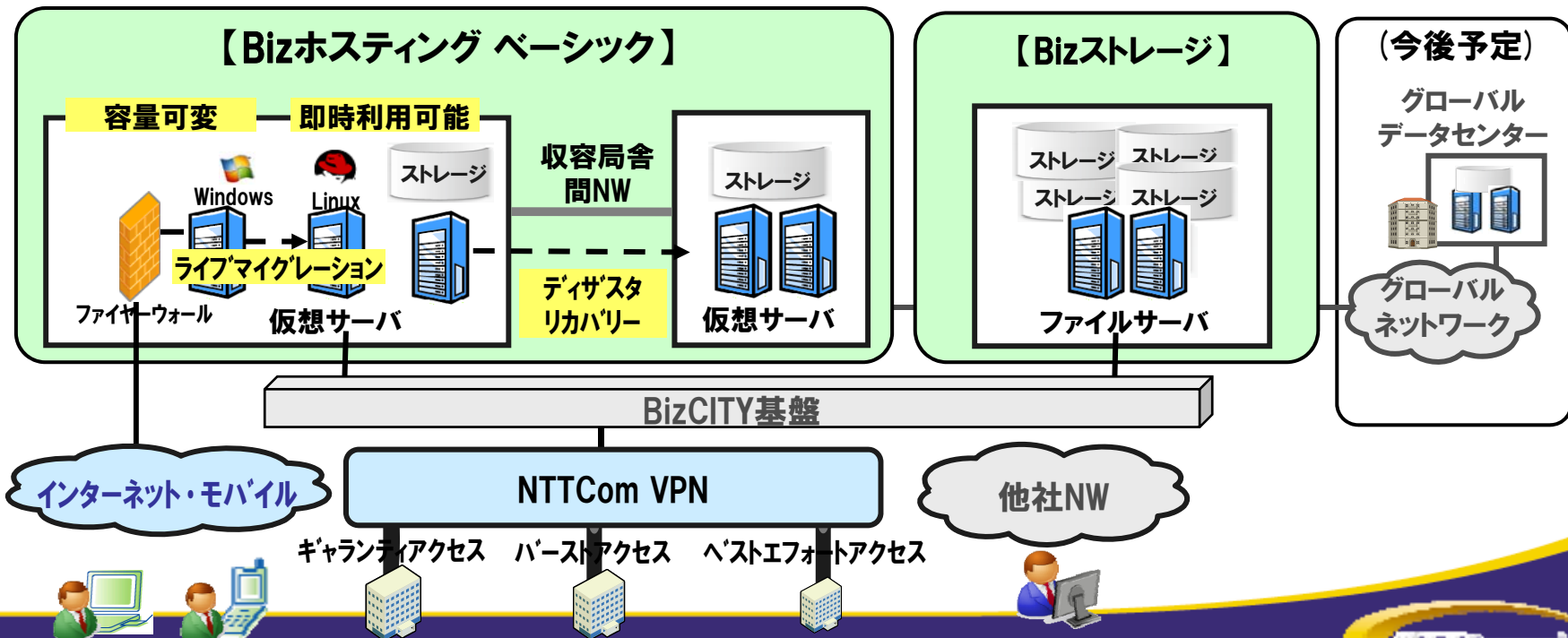
ホスティング・ストレージサービスの概要・特徴

Bizホスティング ベーシック

- ◆ ネットワークと一体で利用できる仮想化技術を用いたホスティングサービス
 - 必要な時・必要なだけオンデマンドでサーバリソースを低コストで利用可能
 - セキュアなVPN上で、障害や災害時の対策も確保し安全・安心に利用可能
- ◆ BizCITYアプリケーションのサーバ基盤としても活用

Bizストレージ

- ◆ ネットワークサービスと一体で利用できるファイルサーバホスティング(ストレージ)サービス
- ◆ 増加し続けるデータ量に対応するためのファイルサーバを自社設置せずアウトソースが可能
 - データ量の増加に応じて、低コスト・オンデマンドで拡張可能(テラバイトを越える大容量にも対応)
 - セキュアなVPN上で、安全・安心に利用可能



Bizホスティングベーシックサービスの 開発・運用について

目次

- Bizホスティングベーシックサービスのご紹介
- 良かったこと
- **困ったこと**
- 今後の予定

Bizホスティング ベーシック サービス概要

1. オンデマンドにリソースを提供

- ・仮想サーバー (VM) 単位での提供
(リソースによる月額料金/台)
- ・リソース: CPU/メモリ/ディスク を指定
- ・OS : Windows Server 2003/2008
Linux RHEL4/5 から選択可
- ・複数仮想サーバ構成可能

2. セキュアなサーバ環境

- ・VPN接続
サーバに接続可能なVPNは
お客さま指定の1VPNに限定
- ・インターネット接続
FWIによるフィルタ機能を提供
- ・DMZ構成
VPN、インターネット両方から
接続可能

3. 運用サポート

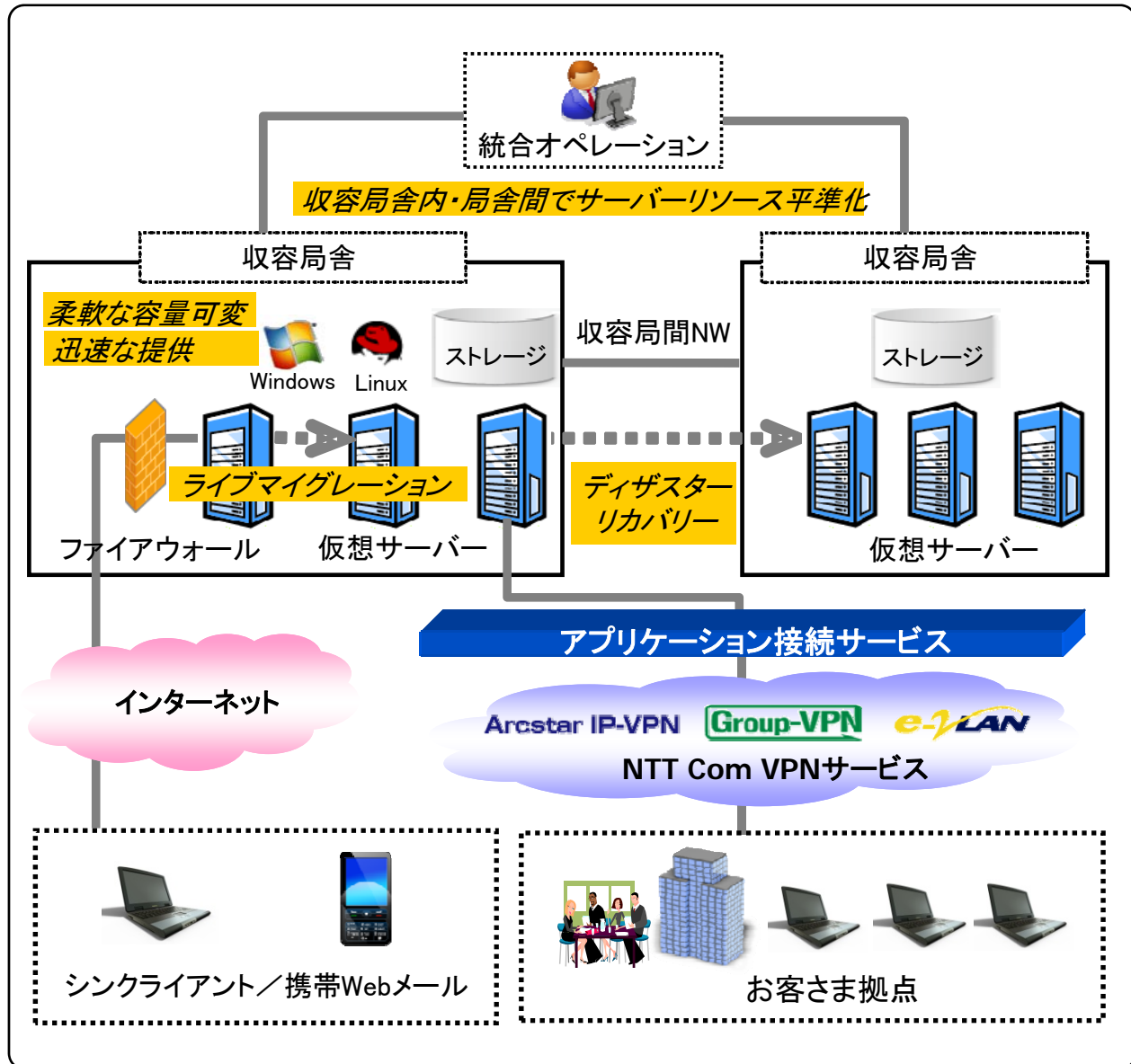
- ・仮想サーバ (VM) OSレベルの保守

4 次世代仮想化ソフト

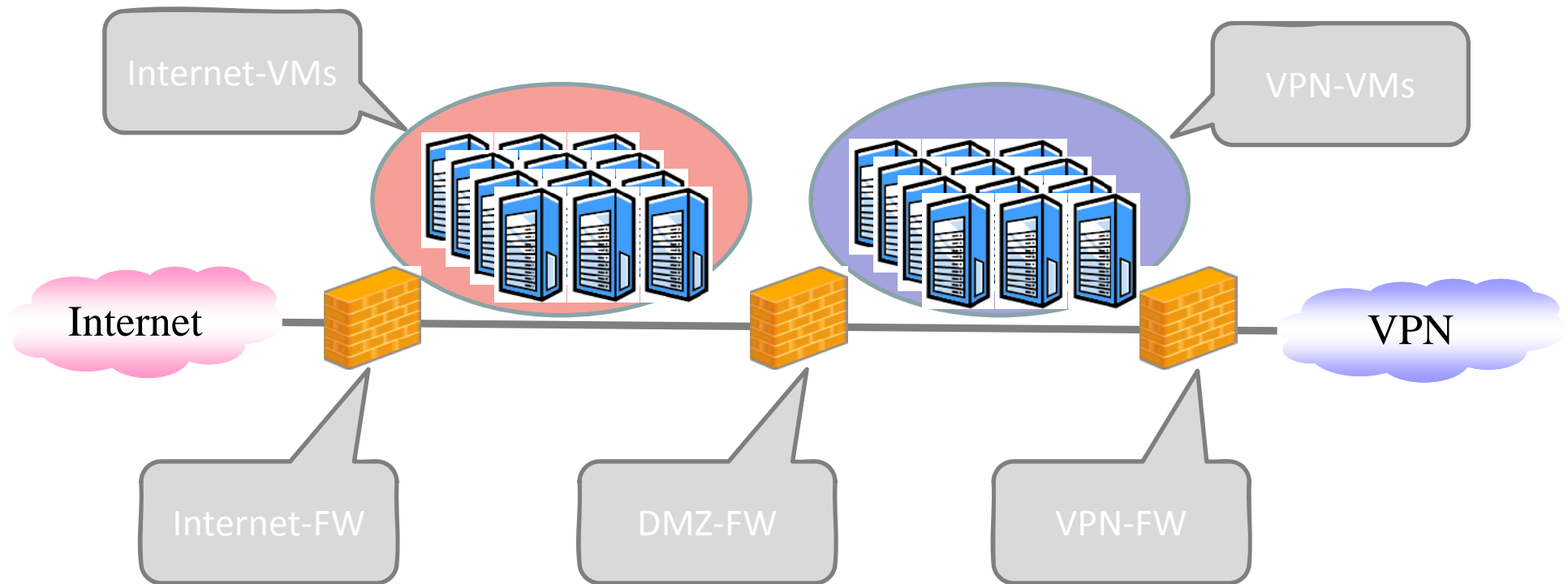
- ・KVM

※「KVM」とは

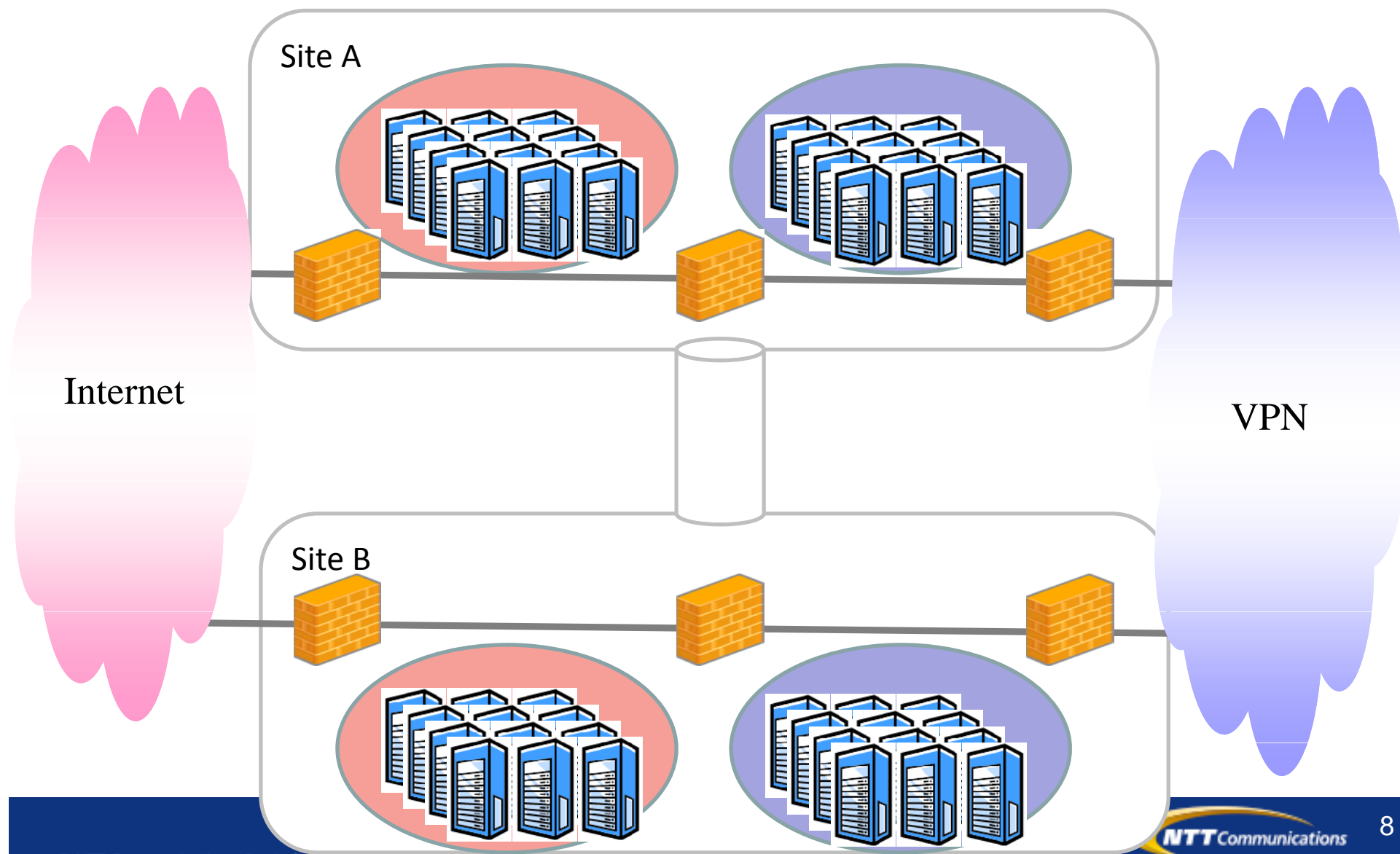
・Kernel-based Virtual Machineの略
Linuxカーネルの標準機能として組み
込まれており、今後仮想化技術の主流
となることが予想されています。



Bizホスティング ベーシック ネットワーク構成図



Bizホスティング ベーシック ネットワーク構成図



まとめ - Bizホスティングベーシックサービスとは

- クラウド/IaaS型サーバホスティングサービス
 - 仮想サーバ基盤にLinux KVMを採用
 - RedHat Enterprise Linuxを採用
 - 保守運用でLive Migrationをサポート
 - 高可用性 & 高メンテナンス性
- 複数データセンタからお客様が拠点を選択(予定)
 - 容易にActive-Active、Active-Standby構成がとれる
 - 業務継続、災害対策を容易に実現



良かったこと

- Linux KVMのこの時期の採用は割と話題にしていた
だけだったかも？
 - 各種ニュースサイトにリリースの記事
 - @ITで自分が参考に使っていた連載で言及されてた



- 知って見るみるKVM

<http://www.atmarkit.co.jp/flinux/rensai/kvm04/kvm04a.html>

- Live Migrationのサポートでメンテナンスが簡単に

困ったこと

- 市販ツールがない
 - Linux KVM を採用してしまったがために。。
- VPN/VLAN構成
 - 仮想スイッチ群の構成がえらいことに。。
- SANストレージの使い方
 - NFSみたいなものだと思ってたらエライことに。。

困ったこと1: 市販ツールがない

- Xenならたくさんあった



- VMWareももちろんあった

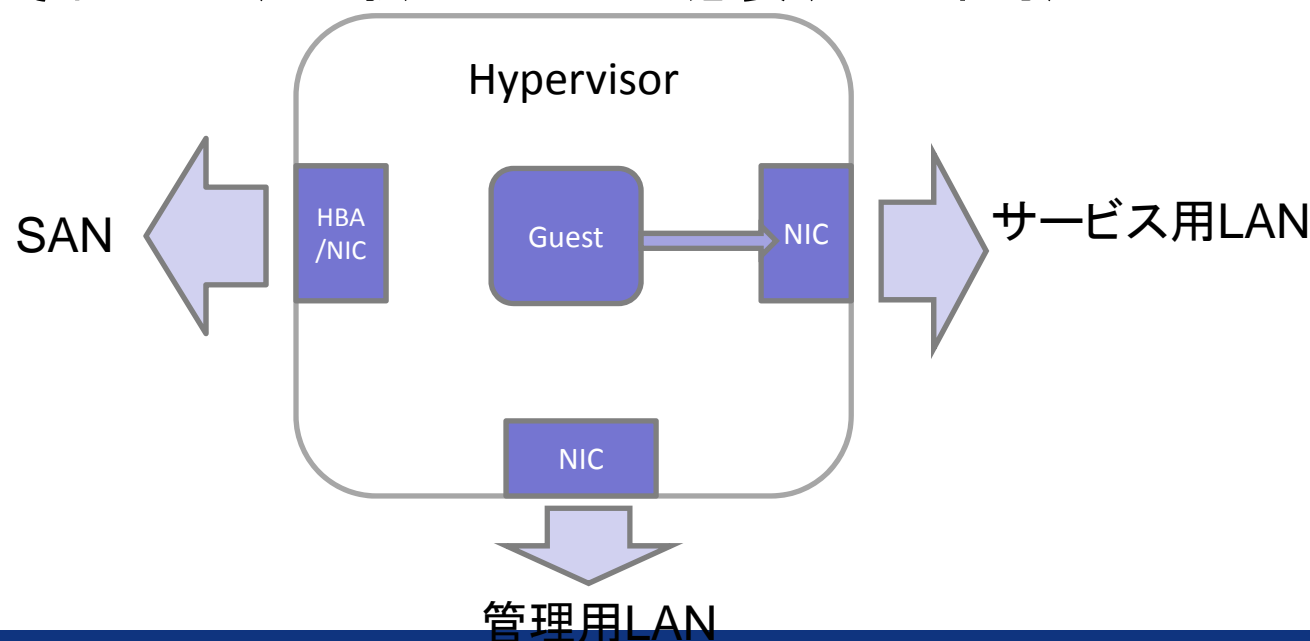


困ったこと1: 市販ツールがない

- でもLinux KVMになった
 - 理由は
 - 将来性？
 - Kernelのコミュニティの勢い
 - Redhatの標準仮想化ツールとしての採用
 - 話題性？
 - ~~自分たちで作るのが面白そうだから！？~~
 - 1VMは通常のLinuxの1プロセスとなり、特別な扱い不要
 - 市販ツールを採用しなかったはっきりした理由の1つ
 - 市販ツールはNetwork設計に自由度がなかった

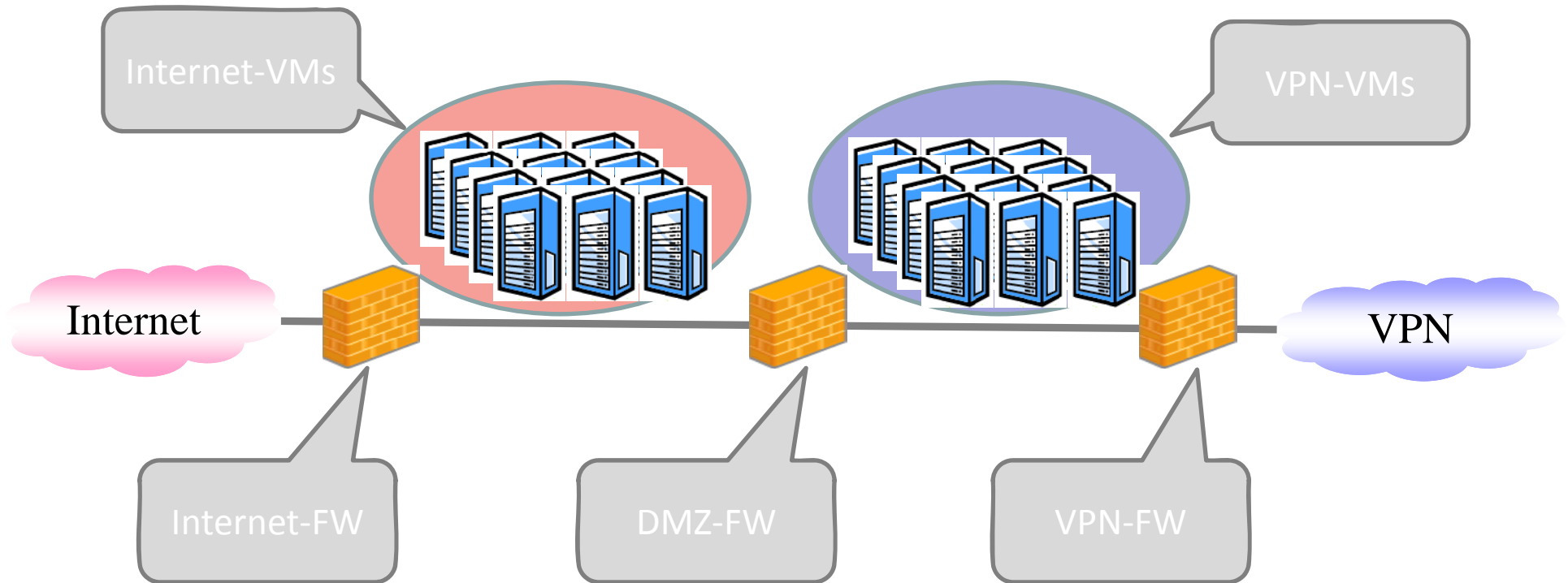
困ったこと1: 市販ツールがない

- 市販仮想化ツールによくあるNetwork構成の制限
 - ストレージ用LANは管理用と兼ねるものもある
 - Guestはサービス用のLANにしかつなげられない
 - サービス用LANは1つだけのことが多い
 - それぞれのLAN用に独立したNICが必要 (VLAN不可)

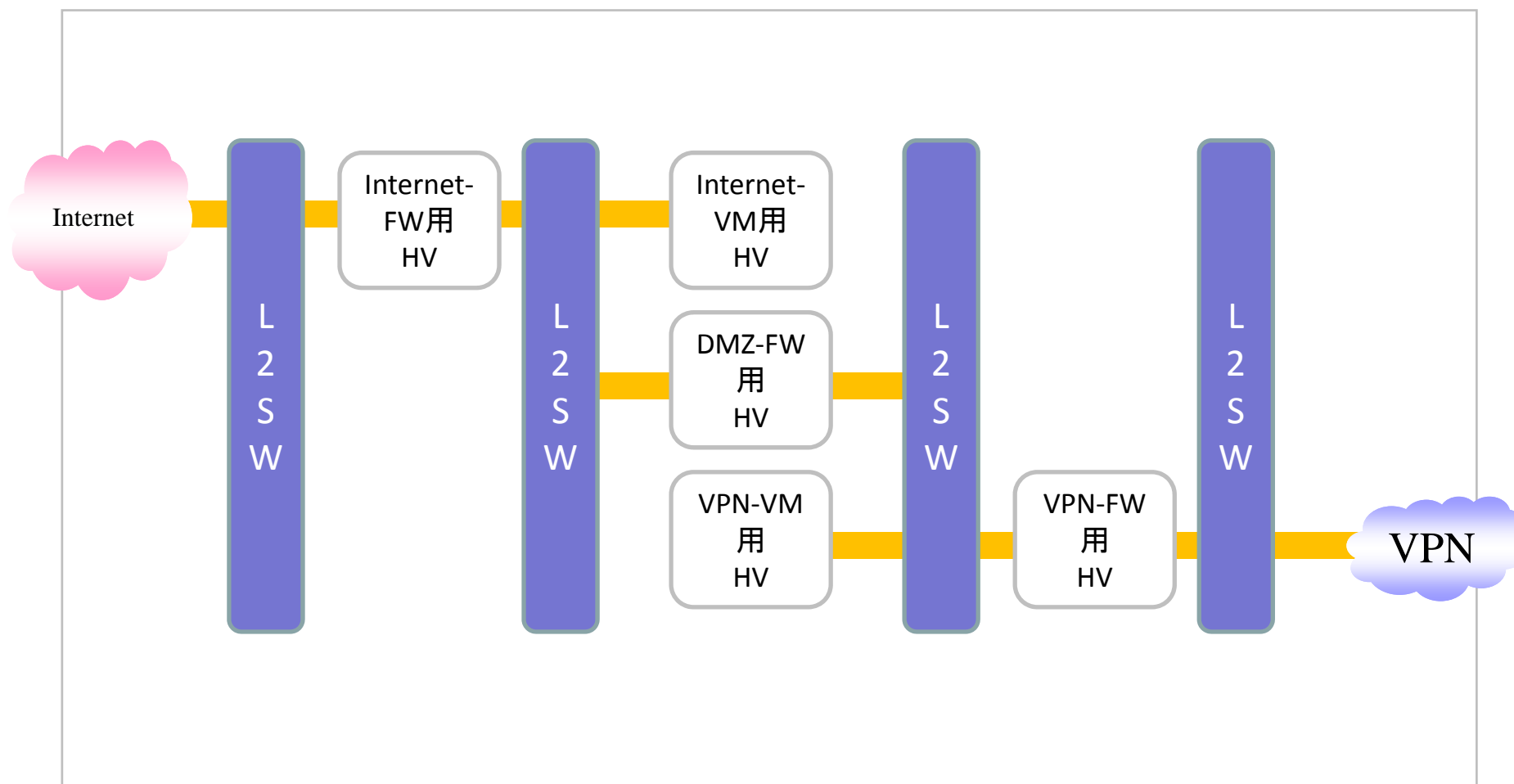


Bizホスティング ベーシック ネットワーク構成図

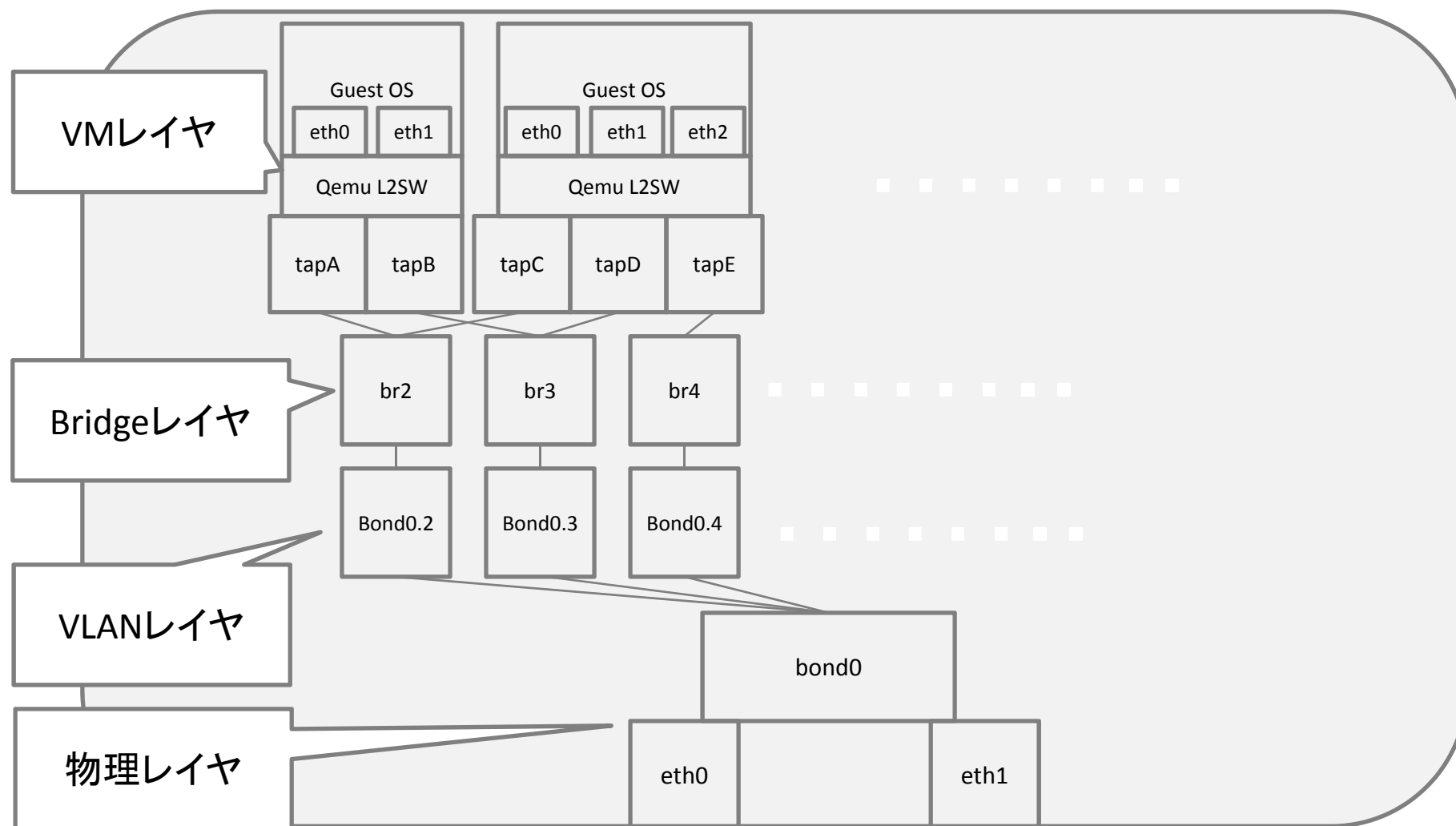
- この構成を実現するためには...



このような若干複雑な構成を取らざるを得なかった

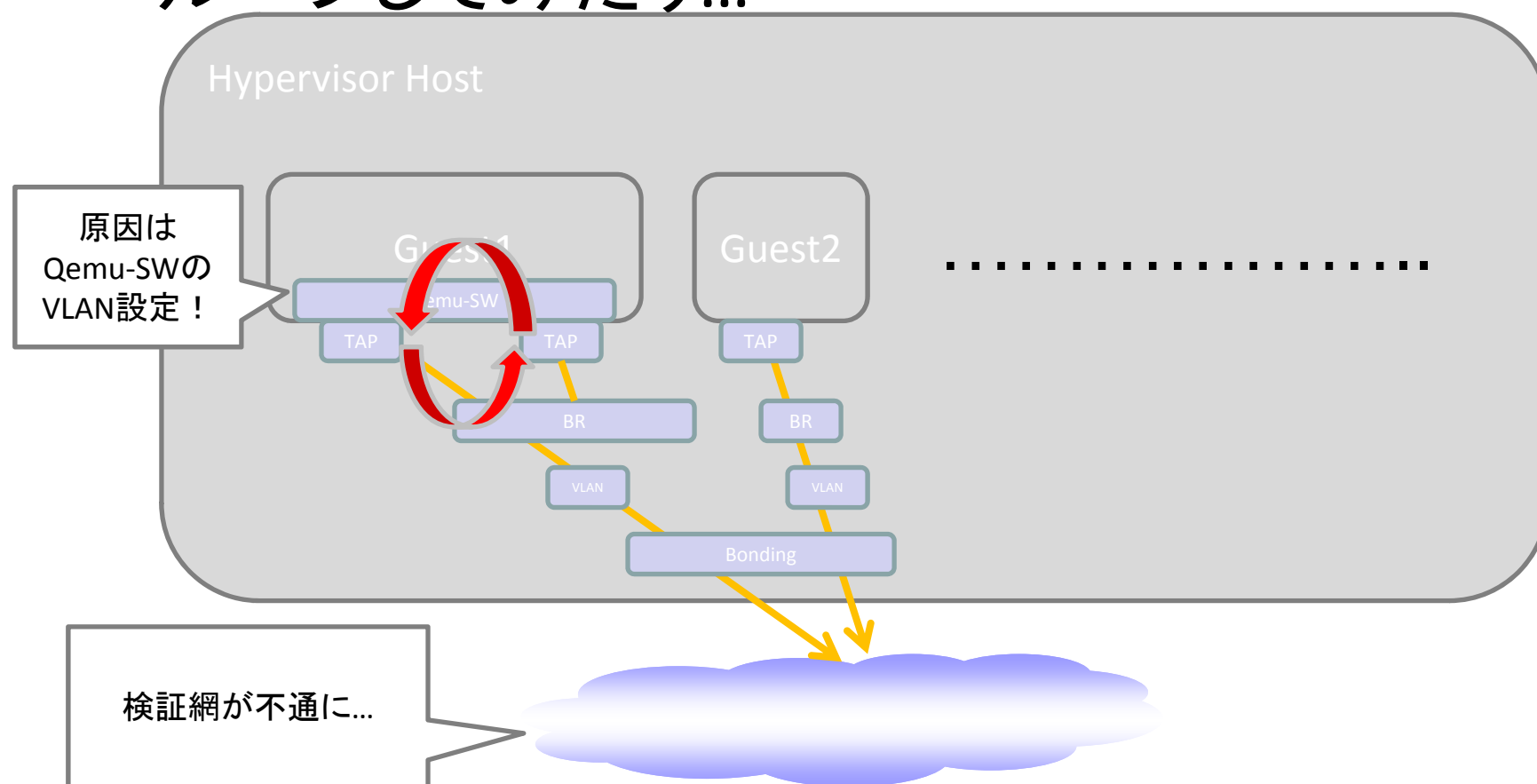


Hypervisor機の内Network構成



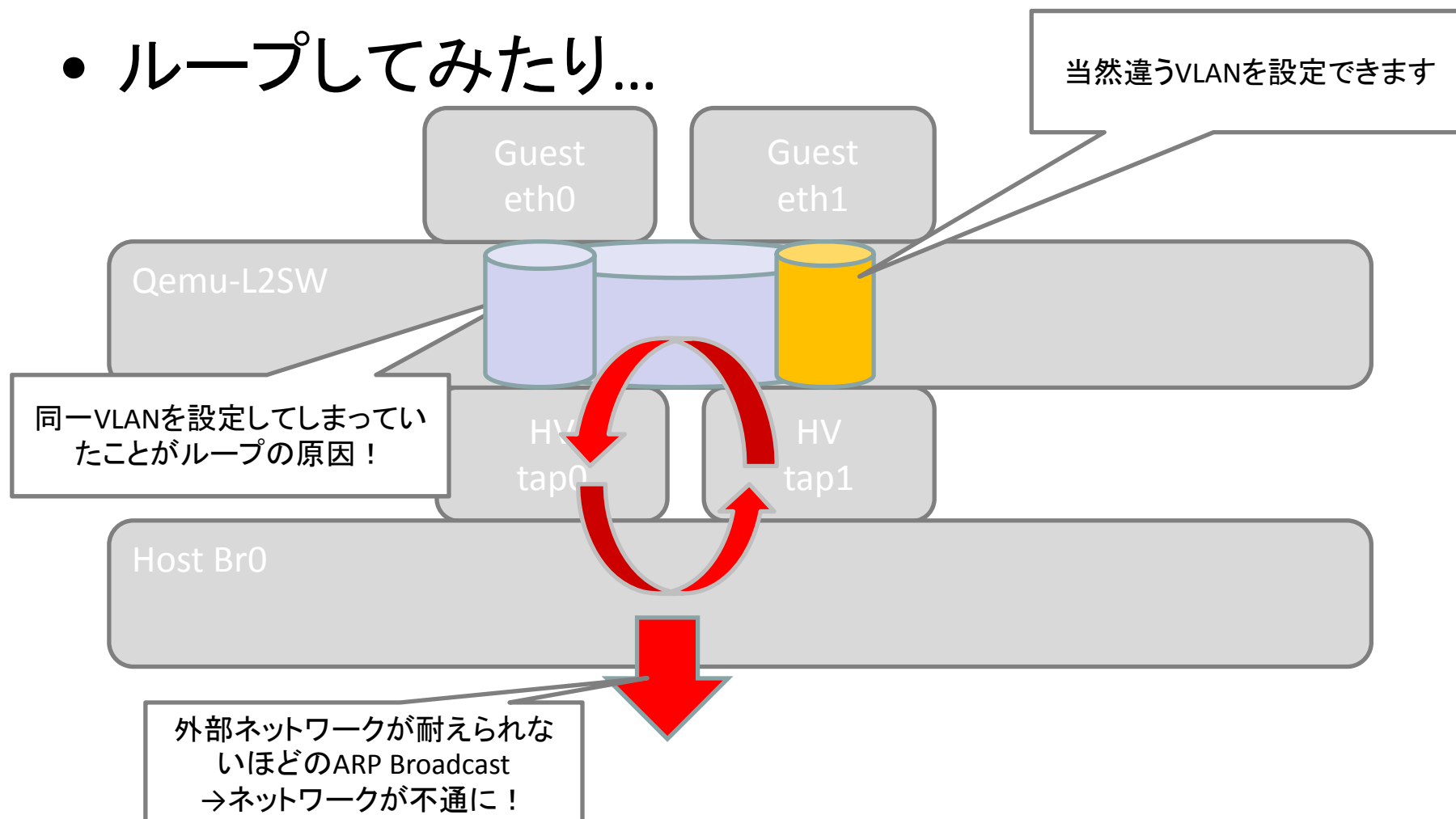
困ったこと2: Network構成

- ループしてみたり...



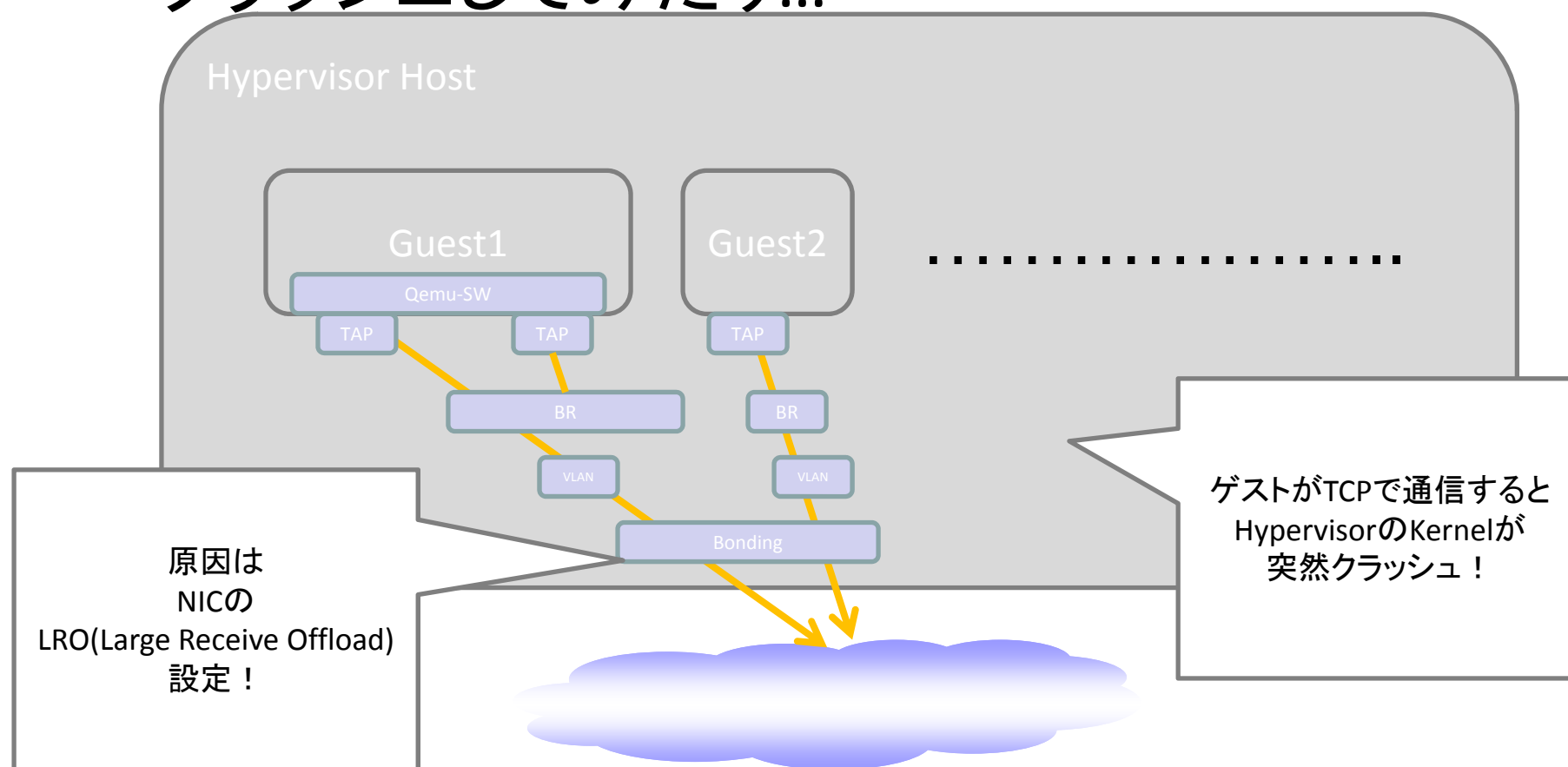
困ったこと2: Network構成

- ループしてみたり...



困ったこと2: Network構成

- クラッシュしてみたり...

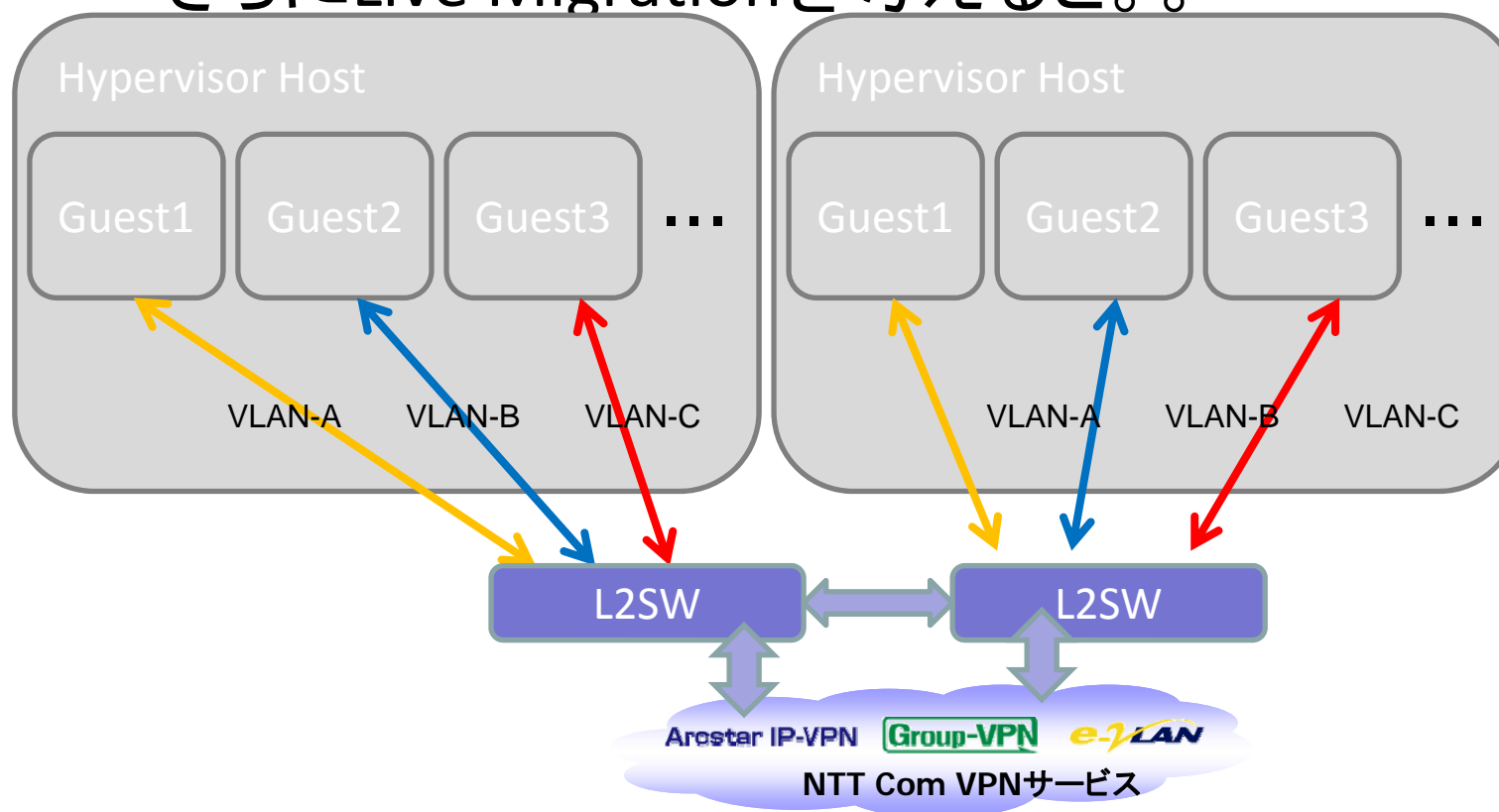


困ったこと2: Network構成

- LRO(Large Receive Offload)とは？
 - 高速に大量のTCPパケットを受信するたびに割り込みをかけるのでは処理効率が落ちるため、いくつかのTCPパケットをまとめ上げてから割り込みをする方式
 - http://en.wikipedia.org/wiki/Large_receive_offload
- 今回のKernel Crashの原因は？
 - RHSA-2009:1455-1
 - <http://rhn.redhat.com/errata/RHSA-2009-1455.html>
 - Linux BridgeとTAPインターフェースとの間でLROパケットをうまく処理できていなかった
 - 現在のカーネルもLROパケットを破棄してクラッシュはしない、という処置を行っている
 - Redhatのサポートによると、基本的に仮想化を使うときはオフロード機能は使わないで、とのこと

困ったこと2: VPN/VLAN構成

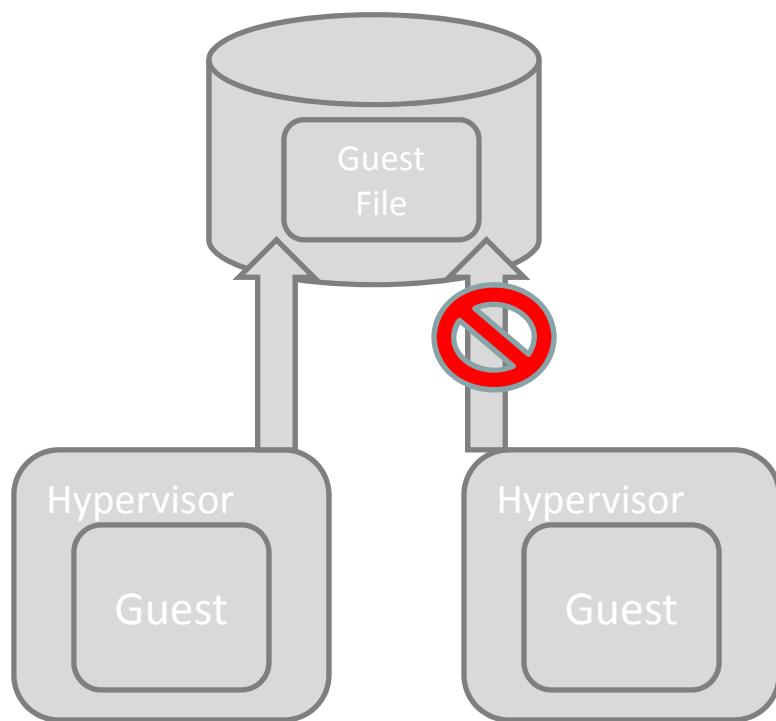
- 複数台あるとさらに面倒なことに。。
 - さらにLive Migrationを考えると。。



困ったこと3: SANストレージの使い方

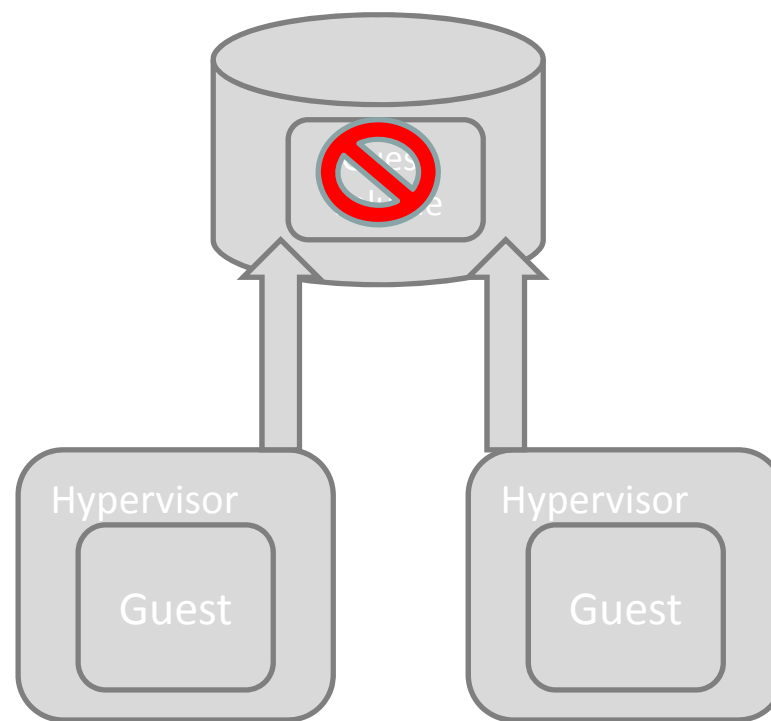
NFSの場合

- 自動で排他制御される



SANストレージ(FC,iSCSIなど)の場合

- ただのSCSIディスクなので排他を意識しないと平気でVolumeが壊れる



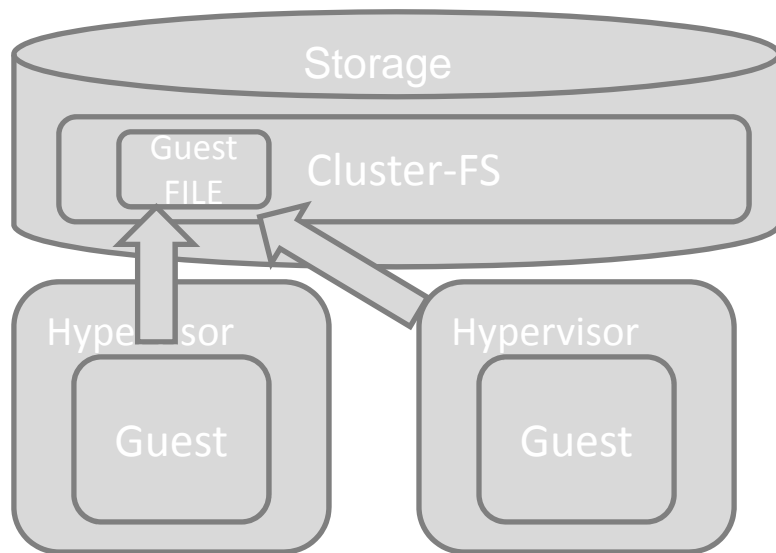
困ったこと3: SANストレージの使い方

- ファイルシステム型
 - クラスタファイルシステムを使う
 - NFSライクにロックや排他制御を自動でしてくれる
 - VMWareはVMFS, CitrixXenも独自のクラスタFSを使用している模様
 - Open SourceなものではOCFS2, GFSなど
- ブロックデバイス型
 - Diskのつかみ方を工夫して、排他が必要無いように使う
 - 1つのボリュームは常に1つのGuestのみが掴むようにする、など

困ったこと3: SANストレージの使い方

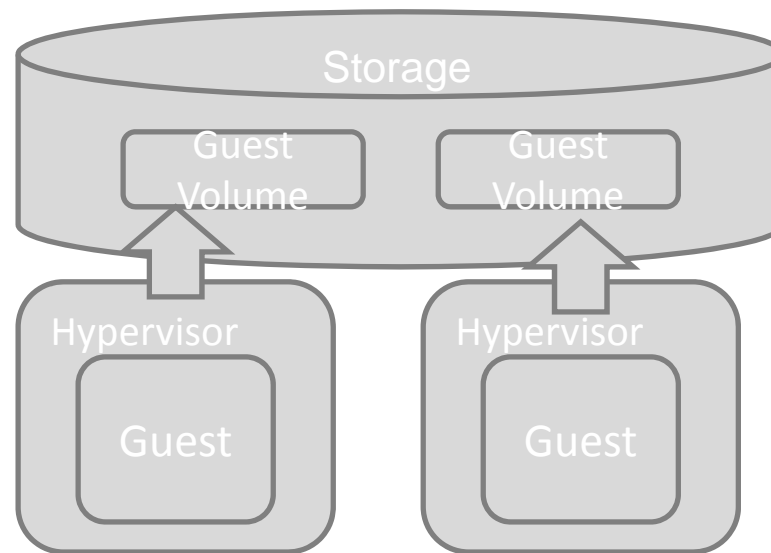
クラスタFS型

- NFSライクに使える
 - 一部専用サービスやサーバが必要なFSもある
 - ファイル単位アクセスで管理も簡単だが性能はブロックデバイスには負ける



ブロックデバイス使い分け

- 1つのボリュームは1人からしかアクセスさせない
 - 性能はFS経由よりも良いが管理が煩雑



今後の方向性

- リソース制限の粒度
 - Disk I/O制御
 - dm-ioband
 - cgroups
- ゲスト監視
 - 契約ごとにVLANが異なる
 - 直接保守網からゲストへアクセス不可
 - 監視エージェント導入？
- バックアップ
 - オンラインバックアップ