White Paper

Empowered by Innovation NEC

CLUSTERPRO XによるVMware vSphere 5 仮想化環境の可用性向上

CLUSTERPRO

http://www.nec.co.jp/clusterpro/

1. はじめに

仮想化環境の導入によりサーバが集中化した環境では、万が一の障害でサーバがダウンした場合、仮想マシン上の全ての業務は停止してしまうため、仮想化環境における可用性の向上は、業務の継続性を保つ上で重要な要素となります。

VMware vSphere™5(以降vSphere 5)にはvSphere HA、vSphere FTといった可用性機能が存在するものの、監視対象が限定されており、例えば仮想マシン上の業務アプリケーションの障害には対応できません。そこで本稿では、vSphere 5環境にクラスタリングソフトウェアCLUSTERPRO X(以降、図表中ではCLP)、及び、シングルサーバの可用性向上ソフトウェアCLUSTERPRO X Single Server Safe (以降SSS)を導入することでさらなる高可用性を実現する方法について検証します。

本稿では、vSphere HAを基本構成とし、その各レイヤ(管理用OS※1、ゲストOS)にCLUSTERPROを導入します。vSphere HA基本構成とCLUSTERPRO導入構成を可用性観点で比較検証を行い、CLUSERPRO導入による具体的なメリットについて述べます。

検証する構成A~Eを以下に示します。

(A) vSphere HA基本構成
(B) 管理用OSへCLUSTERPRO Xを導入
(C) ゲストOSへCLUSTERPRO X SSSを導入
(D) ゲストOSへCLUSTERPRO Xを導入
(E) 管理用OS/ゲストOSへCLUSTERPRO Xを導入
【推奨】

2. vSphere HAとの比較検証

物理サーバレベルと仮想マシンレベルの障害発生時における業務継続性についてvSphere HAとCLUSTERPROを導入した各構成の比較検証を行います。想定する障害を下記に示します。

- 物理サーバレベル
  - ネットワーク障害
  - ディスク障害
- 仮想マシンレベル
  - ゲストOS負荷ストール
  - ゲストOS停止※2
  - 業務アプリケーション異常

2.1. (A) vSphere HA 基本構成

vSphere HA機能は下記2つです。本稿ではこれら機能を全て有効にした環境で検証を行います。

ESXiホスト監視	管理ネットワークや共有ディスクを使用してESXiホスト間及びESXiホスト-vCenterサーバ間のネットワーク/ディスクハートビートを行い、ESXiホストを死活監視する。ESXiホストダウン時には、同ホスト上の仮想マシンを健全な別ESXiホストで再起動(以降、仮想マシンのフェイルオーバ)を行う。
仮想マシン監視	ESXiホスト-ゲストOS(VMware Tools)間でハートビートを行い、ゲストOS停止時には、同ホスト上で仮想マシンの再起動を行う。

vSphere HA基本構成の全体概要を図1に示します。ネットワーク構成、及び、ディスク構成の詳細について、図2、図3にそれぞれ記載します。詳細図ではESXiホスト1台分のみ記載していますが、2台目も同様の構成となります。

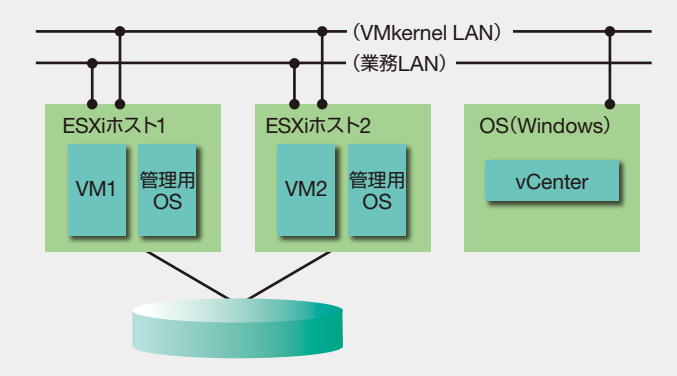

図1: vSphere HA基本構成

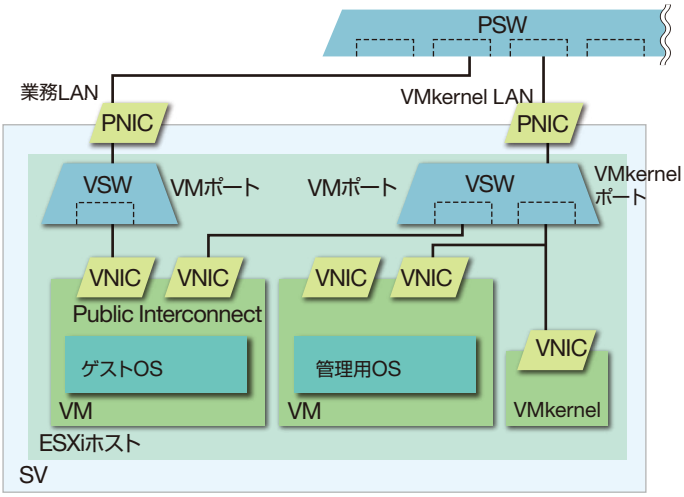

図2: ネットワーク構成

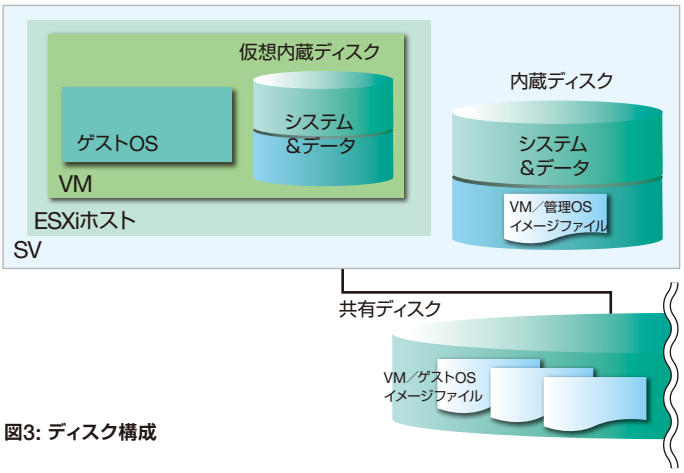

図3: ディスク構成

図中の略語は次のとおりです。

SV	物理サーバ	VNIC	仮想NIC
VM	仮想マシン	PSW	物理スイッチ
PNIC	物理NIC	VSW	仮想スイッチ

※1: CLUSTERPRO XはESXiを管理するために管理用OSを使用します。
CLUSTERPRO Xは管理用OSとしてVMware vSphere Management Assistant (vMA)とRed Hat Enterprise Linux 5.6をサポートしています。
※2: Windowsではブルースクリーン、LinuxではKernelパニックを想定します。

本検証ではCLUSTERPROからESXiホストを監視するために管理用OS間クラスタを構築します。管理用OS間クラスタを構築しない場合には管理用OSは使用しません。

ネットワーク構成については、仮想化環境における可用性や性能を考慮して、VMkernelポート、仮想マシンポート(ゲストOS上の業務アプリケーションが使用、図2ではPublicと表記)をそれぞれ別系統の物理NICへ割り当てるように構成します。以降では、各ポートに繋がる物理NICが構成するLANをそれぞれVMkernel LAN、業務LANと呼びます。

なお、ゲストOSへCLUSTERPRO Xを導入する構成のために、VMkernel LAN配下に仮想マシンポートの仮想NICを(Interconnectと表記)を追加しています。これは、ゲストOS間クラスタを構成する際のInterconnect LAN として使用します。ゲストOS間クラスタを構成しない場合は、使用しません。

ディスク構成については、vSphere HAを使用するため、仮想マシン(及び、仮想マシンが使用する仮想ディスク)、ゲストOSがアクセスするファイルは共有ディスク上に格納します。また管理用OSイメージはESXiホストの内蔵ディスクに格納します。

本環境はvMotion、vSphere DRSの併用が可能な構成※3にしています。

vSphere HA構成における各種障害発生時のシステムの挙動に関して検証結果を以下の表にまとめます。本表が以降の比較検証のベースになります。

障害区分	障害箇所	検証結果
物理サーバ	(a)VMkernel LAN	検出不可
	(b)業務LAN	ESXiの監視機能により検出可能 →ESXiホストのシャットダウン※4による仮想マシンのフェイルオーバ
	(c)共有ディスク※5	vSphere HAの仮想マシン監視により検出可能 →vSphere HAによるゲストOSのリセット
	(d)内蔵ディスク※6	ESXiの監視機能により検出可能 →ESXiホストのシャットダウンによる仮想マシンのフェイルオーバ
仮想マシン	(e)OS負荷ストール	ESXiの監視機能により検出可能 →ゲストOSの再起動※4
	(f)OS停止	vSphere HAの仮想マシン監視で検出可能 →仮想マシン再起動
	(g)業務アプリケーション	検出不可

異常発生後のシステムの動作(特に業務アプリケーション観点)について次に示します。

- 業務継続可能

  (b)については、ESXiホストをシャットダウンすることで、vSphere HAによる仮想マシンのフェイルオーバ後に業務継続可能となります。ただし、障害発生ネットワークの特定ができないため、業務LANが複数存在する場合は障害の発生していない業務LANを使用する仮想マシンもフェイルオーバしてしまいます。

  (e)については、ESXiホストのCPU監視機能による仮想マシンの再起動後、業務継続可能になります。

  (f)については、vSphere HAの監視機能による仮想マシンの再起動後、業務継続可能となります。

- 制限付で業務継続可能

  (a)については、業務アプリケーションへの影響はありませんが、vCenter Serverからの仮想マシンの管理やvMotionが実行できなくなります。

- 業務継続不可

  (c)、(d)については、ESXiホストで検出可能ですが、ディスクにアクセスできないことによるESXiホストの動作不全により、ESXiホストのシャットダウン処理中やゲストOSのリセット処理中にストール状態となり業務継続できません。(g)については、vSphere HAの監視対象外のため業務継続できません。

なお、VMkernel LANと共有ディスクに同時に障害が発生した場合は、vSphere HAのハートビート監視異常による仮想マシンのフェイルオーバで業務継続が可能です。本検証では、単一障害時の動作についてのみ検証し2重障害についての検証は省略します。

2.2. (B) 管理用OSへCLUSTERPRO Xの導入

vSphere HA基本構成(図1)において管理用OSへCLUSTERPRO Xを導入し、物理サーバレベルの監視機能を強化します。

構成の概要を図4に記載します。

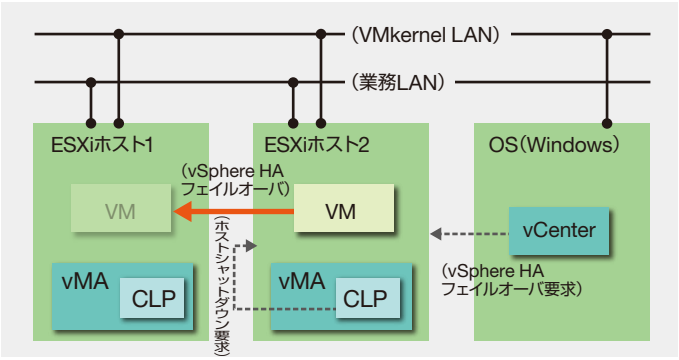

図4: vSphere HA+管理用OS間クラスタ構成

※3: ご利用のvSphere 5のパッケージにvMotion、vSphere DRSが含まれている必要があります。
※4: ESXiのアラームのアクションとして別途設定する必要があります。
※5: 障害箇所が1つのESXiホストになるものを想定します。
障害が複数個所にわたる2重障害は、今回は対象外とします。
※6: ESXiホストのインストール先のディスクを想定します。

本構成の検証結果について以下の表にまとめます。
vSphere HAと比較して異なる部分を色文字で示します。なお、仮想マシンレベルの障害については管理用OS上のCLUSTERPRO Xでは監視不可であり、検証結果はvSphere HA基本構成と同等となるため省略します。

障害区分	障害箇所	検証結果
物理サーバ	(a)VMkernel LAN	管理用OS上のCLPによるリモートネットワーク監視※7、NIC LinkUp／Down監視で検出可能 →異常時アクションとして仮想マシンのフェイルオーバなどが可能
	(b)業務LAN	(a)VMKernel LANと同様の検出が可能 →異常時アクションとして仮想マシンの無停止フェイルオーバなどが可能
	(c)共有ディスク※8	管理OS上のCLPによるリモートディスク監視で検出可能 →パスの片系障害の場合、異常時アクションとして仮想マシンの無停止フェイルオーバなどが可能 パスの両系障害またはディスク障害の場合、異常時アクションとして、ESXiホストのリセットによる仮想マシンのフェイルオーバが可能※9
	(d)内蔵ディスク※10	管理OS上のCLPによるリモートディスク監視で検出可能 →異常時アクションとしてESXiホストのリセットによる仮想マシンのフェイルオーバが可能

以下の点においてメリットがあります。

● NIC障害

リモートネットワーク監視により異常を検出し、異常時アクションとしてESXiホストの再起動や、仮想マシンのフェイルオーバを実行することで、可用性を向上させることが可能です。NIC単位での監視が可能となるため業務継続困難な仮想マシンだけフェイルオーバすることが可能です。
また、業務LANの障害の場合は仮想マシンの無停止フェイルオーバを実行することで、業務停止時間の短縮が可能です。

● ディスク障害

リモートディスク監視(ディスクとHBAの監視)により共有ディスクパスの片系障害や両系障害、または共有ディスク・内蔵ディスクのディスク障害を検出します。
パスの片系障害の場合、異常時アクションとして、仮想マシンの無停止フェイルオーバなどが可能です。パスの両系障害またはディスク障害の場合、異常時アクションとして、ESXiホストのシャットダウン及びBMCによるリセットを行うことで、ゲストOSが中途半端にストールしている状態で業務が継続してしまう現象や回復動作としてのシャットダウン中にストールしてしまう現象を回避できます。シャットダウン後は、vSphere HAのESXiホスト監視機能でサーバダウンを検出し、仮想マシンをフェイルオーバします。

2.3. (C) ゲストOS へCLUSTERPRO X SSSの導入

vSphere HA基本構成(図1)においてゲストOSへCLUSTERPRO X SSSを導入し、仮想マシンレベルの監視機能を強化します。また、物理サーバレベルの監視について仮想マシンレベルの監視により間接的に行うことができます。

構成の概要を図5に記載します。

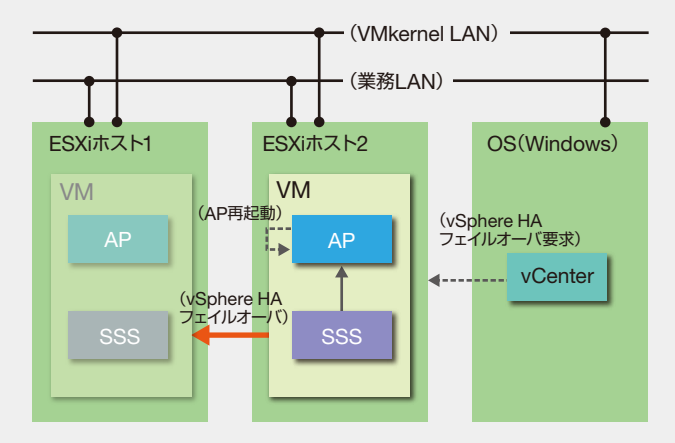

図 5 : vSphere HA+ ゲストSSS 構成

※7: 管理用OSからのリモート監視にはvSphere Command-Line Interfaceを使用します。
※8: 障害箇所が1つのESXiホストになるものを想定します。
障害が複数個所にわたる2重障害は、今回は対象外とします。
※9: ディスク障害発生時はシャットダウン途中で無応答になるケースがあるため、
BMCによるホストのリセットを実行しています。
※10: ESXiホストのインストール先のディスクを想定します。

本構成の検証結果について以下の表にまとめます。
vSphere HAと比較して異なる部分を色文字で示します。

障害区分	障害箇所	検証結果
物理サーバ	(a)VMkernel LAN	検出不可
	(b)業務LAN	ゲストOS上SSSのIP監視で間接的に検出可能 →異常時アクションとして有効なアクションがない
	(c)共有ディスク	(Linux版のみ)ユーザ空間監視で間接的に検出可能 →異常時アクションとして仮想マシンをリセットし、業務を停止可能
	(d) 内蔵ディスク	検出不可
仮想マシン	(e)OS負荷ストール	監視Agent※11、(Linux版)ユーザ空間監視／(Windows版)ディスクRW監視で検出可能 →ゲストOSの再起動
	(f)OS停止	vSphere HAの仮想マシン監視で検出可能 →仮想マシン再起動
	(g)業務アプリケーション	プロセス死活監視や監視Agentで検出可能 →異常時アクションとして、アプリケーションの再起動などが可能

vSphere HAと比較して、仮想マシンレベルでの障害発生時に、ゲストOSや業務アプリケーションを再起動させることができ、仮想マシンレベルの可用性を向上させることができます。メリットを下記にまとめます。

- 共有ディスク障害(Linux版のみ)
  SSSのユーザ空間監視にて異常を検出し、異常時アクションとして、仮想マシンのリセットを行うことで、ゲストOSが中途半端にストールしている状態で業務が継続してしまう現象を回避できます。
  ゲストOSがWindows版の場合は、vSphere HA構成と同様に業務アプリケーションが不安定な状態で継続してしまう可能性があります※12。

- 仮想マシンレベルの障害
  (e),(f)について、SSSとvSphere HAでOSのストール／停止への監視機能を補完できます。
  (e)についてはCPU、メモリ以外のOSリソースの枯渇によるOSストールも未然に検出可能です。
  (g)について、vSphere HAでは未対応の業務アプリケーションの監視が可能です。

また、(b)について、業務LANは仮想マシンの仮想NICに割り当てているため、SSSのIP監視※13で間接的に検出可能ですが、SSSは仮想マシン上のゲストOSで動作しているため、物理サーバレベルの障害に対する有効なアクションが取れません。ただし、ネットワークが使用できないまま業務を継続させたく無い場合に業務を停止させることが可能です。

2.4. (D) ゲストOSへCLUSTERPRO Xの導入

vSphere HA基本構成(図1)においてゲストOSへCLUSTERPRO Xを導入し、仮想マシンレベルの監視機能を強化し、ゲストOS間でクラスタを構成します。構成C(2.3)のメリットを引き継ぎつつ、クラスタ構成により業務のダウンタイムを削減できます。業務ダウンタイムに関しては、5.1を参照してください。
構成の概要を図6に記載します。なお、検証したゲストOS間クラスタはミラーディスク型です※14。

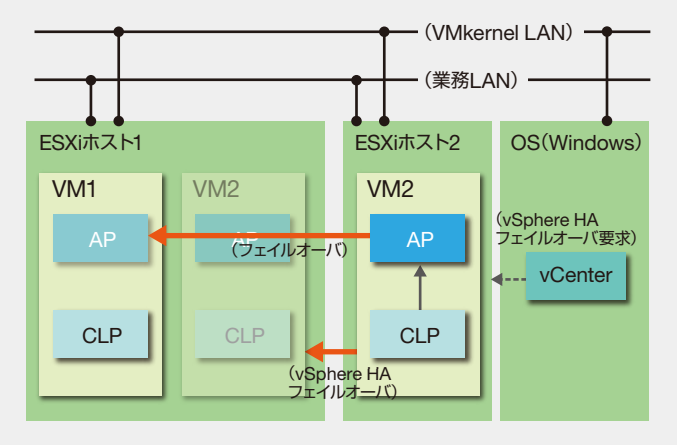

図6: vSphere HA+ゲストOS間クラスタ構成

本構成の検証結果について以下の表にまとめます。
vSphere HAと比較して異なる部分を色文字で示します。

障害区分	障害箇所	検証結果
物理サーバ	(a)VMkernel LAN	検出不可
	(b)業務LAN	ゲストOS上CLPのIP監視で間接的に検出可能 →異常時アクションとして業務アプリケーションのフェイルオーバが可能
	(c)共有ディスク	(Linux版のみ)ユーザ空間監視で間接的に検出可能 →異常時アクションとして仮想マシンをリセット 仮想マシンのリセットの間、業務アプリケーションのフェイルオーバが可能
	(d)内蔵ディスク	検出不可

※11: 特定アプリケーションに特化した監視を実行し、アプリケーションのハングアップや結果異常を検出することができます。CLUSTERPRO Xのオプション製品となります。
※12: 共有ディスク障害時のゲストOSストールの検出はWindows版ディスクRW監視では不可能のためです。
※13: 監視対象としてはゲストOS上で使用する業務LANのデフォルトゲートウェイのIPアドレスなどのシステム外部のアドレスを指定します。
※14: 共有ディスク型の場合、vMotion、vSphere DRSは利用できません。VMwareの仕様により、仮想マシンのSCSIコントローラの「SCSIバスの共有」設定を「なし」以外にする(仮想マシン間でディスクを共有する)とvMotionが利用できなくなるためです。

障害区分	障害箇所	検証結果
仮想マシン	(e)OS負荷ストール	監視Agent、(Linux版)ユーザ空間監視／(Windows版)ディスクRW監視で検出可能 →異常時アクションとして仮想マシンをリセットし、ゲストOSを再起動 ゲストOS再起動の間、業務アプリケーションのフェイルオーバが可能
	(f)OS停止	vSphere HAの仮想マシン監視で検出可能 →仮想マシン再起動 仮想マシン再起動の間、業務アプリケーションのフェイルオーバが可能
	(g)業務アプリケーション	プロセス死活監視や監視Agentで検出可能 →異常時アクションとして、業務アプリケーションのフェイルオーバが可能

vSphere HAと比較して、仮想マシンレベルでの障害発生時に、業務アプリケーションをフェイルオーバさせることができ、業務のダウンタイムを削減できます。メリットを下記にまとめます。

- 業務LANのNIC障害

  構成C(2.3)と同様にゲストOS上CLUSTERPRO XのIP監視で間接的に検出可能です。加えてその異常時アクションとして待機系ゲストOSへ業務アプリケーションをフェイルオーバできます。

- 共有ディスク障害(Linux版のみ)

  CLUSTERPRO Xのユーザ空間監視にて異常を検出し、異常時アクションとして、仮想マシンのリセットを行うことで、ゲストOSが中途半端にストールしている状態で業務が継続してしまう現象を回避できます。仮想マシンのリセット後、ゲストOS間クラスタでハートビートタイムアウトを検出し、業務アプリケーションをフェイルオーバします。ただし、CLUSTERPRO Xの設定について注意点(本節最後に記載)があります。ゲストOSがWindowsの場合、ゲストOSの中途半端にストールした状態が解消されないため、業務アプリケーションは現用系／待機系ゲストOSで両系活性状態となり最終的に業務停止してしまう場合があります※15。そのため、ゲストOSがWindowsである場合、本障害に対応するためには管理用OS間クラスタを導入し(構成E(2.5))、障害発生時にESXiホストをシャットダウンさせる必要があります。

- 仮想マシンレベルの障害

  (e),(f)について、構成C(2.3)ではゲストOSの再起動に留まりますが、本構成ではゲストOS再起動後、ゲストOS間クラスタにおけるハートビートタイムアウトによって待機系ゲストOSへ業務アプリケーションをフェイルオーバできます。

  (g)については、業務アプリケーションの異常を検出後、速やかにフェイルオーバします。

共有ディスク障害のCLUSTERPRO X注意事項

ユーザ空間監視による仮想マシンリセットの完了前に、業務アプリケーションのフェイルオーバ処理が実行された場合、フェイルオーバに失敗します。ただし、業務アプリケーションが属するフェイルオーバグループにフローティングIPリソースが含まれる場合に限られます。

これは、共有ディスク障害時におけるゲストOSの中途半端ストール状態で、障害発生元ゲストOSがpingに応答するためです。フローティングIPリソースは二重活性を防止するために、フェイルオーバ開始時に該当フローティングIPアドレスが既に使用中であった場合(ping応答がある場合)、フェイルオーバを失敗させる仕様となっています。

上記の理由により、CLUSTERPRO Xの設定を下記の方法で調整し、ユーザ空間監視による仮想マシンリセットのタイミングをフェイルオーバよりも早くする必要があります。

- フローティングIPリソースのPingリトライ回数、Pingインターバルを大きくする
- ユーザ空間監視の監視タイムアウト値を小さくする

2.5. (E) 管理用OS／ゲストOSへCLUSTERPRO Xの導入【推奨】

vSphere HA基本構成(図1)において管理用OSとゲストOSへCLUSTERPRO Xを導入し、物理マシン／仮想マシンレベルの両面で監視機能を強化します。

構成B(2.2)、構成D(2.4)のメリットがあります。

構成の概要を図7に記載します。検証したゲストOS間クラスタはミラーディスク型です。

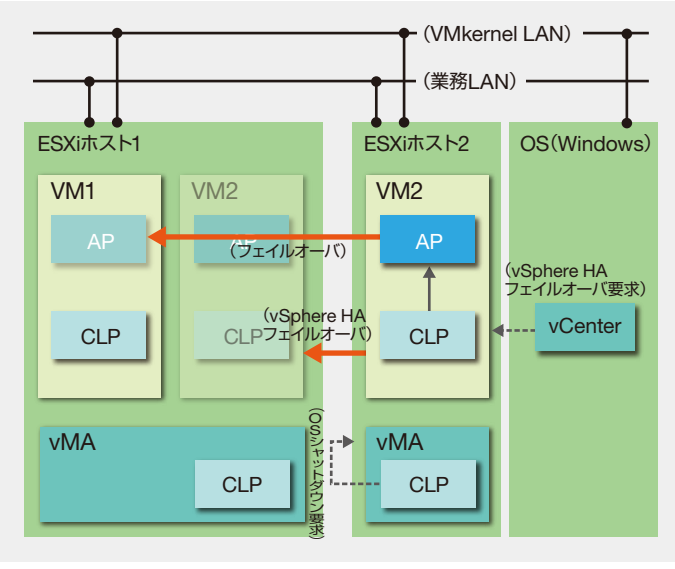

図7: vSphere HA+管理用OS・ゲストOS間クラスタの組み合わせ構成

※15: CLUSTERPROは、業務の両系活性時、リソース排他制御によるデータ保護の観点から、両サーバとも緊急シャットダウンを行う仕様です。

本構成の検証結果について以下の表にまとめます。
vSphere HAと比較して異なる部分を色文字で示します。

障害区分	障害箇所	検証結果
物理サーバ	(a)VMkernel LAN	管理用OS上のCLPによるリモートネットワーク監視、NIC Link Up／Down監視で検出可能 →異常時アクションとしてESXiホストの再起動などが可能 ESXiホスト再起動の間、業務アプリケーションはフェイルオーバが可能
	(b)業務LAN	(a)VMKernel LANと同様の検出が可能 →異常時アクションとして仮想マシンの無停止フェイルオーバなどが可能
	(c)共有ディスク	管理OS上のCLPによるリモートディスク監視で検出可能 →パスの片系障害の場合、異常時アクションとして仮想マシンの無停止フェイルオーバなどが可能 パスの両系障害またはディスク故障の場合、異常時アクションとしてESXiホストのシャットダウン／リセットによる仮想マシンのフェイルオーバが可能 ESXiが停止中は業務アプリケーションのフェイルオーバが可能
	(d)内蔵ディスク	管理OS上のCLPによるリモートディスク監視で検出可能 →異常時アクションとしてESXiホストのリセットによる仮想マシンのフェイルオーバが可能
仮想マシン	(e)OS負荷ストール	ゲストOS上CLPの監視Agent、(Linux版)ユーザ空間監視／(Windows版)ディスクRW監視で検出可能 →異常時アクションとして仮想マシンをリセットし、ゲストOSを再起動 仮想マシンのリセットの間、業務アプリケーションのフェイルオーバが可能
	(f)OS停止	vSphere HAの仮想マシン監視で検出可能 →仮想マシン再起動 仮想マシン再起動の間、業務アプリケーションのフェイルオーバが可能
	(g)業務アプリケーション	ゲストOS上CLPのプロセス死活監視や監視Agentで検出可能 →異常時アクションとして、業務アプリケーションのフェイルオーバが可能

vSphere HAと比較して、物理マシン／仮想マシンレベルの両面で監視が可能であり、障害発生時は業務アプリケーションをフェイルオーバすることにより、業務のダウンタイムを削減できます。メリットを下記にまとめます。

- ディスク障害
  ゲストOSの種別によらず、業務アプリケーションのフェイルオーバが可能となり業務継続できます。
- 物理サーバ／仮想サーバレベルの障害
  構成B(2.2)、構成D(2.4)と同じ可用性があります。

管理用OSにCLUSTERPROを導入するメリット

管理用OSにCLUSTERPROを導入し管理OS間クラスタを導入することにより以下のメリットがあります。

- 仮想マシン上のCLUSTERPROからESXiホストの物理資源の監視を行うより、管理OS上のCLUSTERPROから一元的に監視を行うほうが効率的です。また、ディスクやネットワークの片パス障害、内蔵ディスクの障害やVMkernel LANの障害を検出することが可能になります。
- ディスクやネットワークの片パス障害時や業務LAN障害時に無停止フェイルオーバが可能なため業務の停止時間が短くなります
- ディスク障害などでESXiホストが正常に停止できない場合(停止中のストールなど)、待機系ESXiホストの管理OS上で動作するCLUSTERPROからBMC経由で現用系ESXiホストを停止することにより待機系ESXiホスト上で仮想マシンの起動が可能になります。
- CLUSTERPRO Xにより仮想マシンのフェイルオーバポリシが設定できます。フェイルオーバポリシによって仮想マシンのフェイルオーバ先のESXiホストに優先順位をつけることが可能です。

2.6. 検証結果まとめ

構成A～Eについて、可用性の検証結果を表1へまとめます。構成A、B、C、D、Eの順番で可用性は向上します。
推奨構成は、ゲストOS上の業務アプリケーションの可用性が高く、物理サーバの共有ディスク障害をはじめとした物理サーバレベルの障害へ対応できるという理由から構成Eとしています。ただし、導入コストも大きくなるため(図8)、用途に合わせて、ベストな構成を選択していくことが必要です。

表1：各構成における可用性

障害区分	障害箇所	A	B	C	D	E
物理サーバ	VMkernel LAN	△	○	△	△	◎
	業務LAN	×	○	×	◎	◎
	内蔵ディスク	×	○	×	×	◎
	共有ディスク	×	○	×	*	◎
仮想マシン	OS負荷ストール	○	○	○	◎	◎
	OS停止	○	○	○	◎	◎
	業務アプリケーション	×	×	◎	◎	◎

表中の記号は可用性を以下の観点で評価したものです。

◎	障害検出可能かつ業務継続可能(ダウンタイムにOS起動時間を含まない)
○	障害検出可能かつ業務継続可能(ダウンタイムにOS起動時間を含む)
△	障害検出不可だが制限付で業務継続可能
×	業務継続不可
*	ゲストOSによって異なる Linuxは◎、Windowsは×

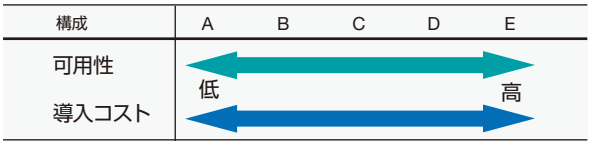

図8: 可用性と導入コストの関係

3. vMotion との比較検証

vMotionはESXiホスト間で仮想マシンを無停止移行でき運用面で高い利便性を持ちますが、可用性機能を持たないため、vMotionだけでは障害対策はできません。

そのため、可用性を重視するシステムでは、2で検証したCLUSTERPROを導入した構成が必要となります。

また、vMotionのメリットとして、物理サーバ(ESXiホスト)の計画メンテナンスが行える点があります。メンテナンス対象のESXiホスト上の仮想マシンを別ESXiホストへvMotionで退避させることによって、業務を継続したままESXiホストのアップデートや物理サーバのハードウェアの保守などが実施できます。しかしながら、vMotionでは、仮想マシン(ゲストOS)上の業務単位での移行はできないため、仮想マシン(ゲストOS)の計画メンテナンスには業務停止を伴います。

CLUSTERPROをゲストOSへ導入する構成D(2.4)、構成E(2.5)は業務単位での移行が可能なため、仮想マシン(ゲストOS)の計画メンテナンスは業務を継続したまま実施できます。この時の業務停止時間は業務の移行時間だけとなります。

また、構成D・Eにおいてもゲスト OS間クラスタをデータミラー型で構築することによって、vMotionが利用可能となります。

表2: 計画メンテナンス時の業務停止有無

構成	物理サーバ(ESXiホスト)	仮想マシン(ゲストOS)
vMotion	○	×
構成D・E	○	○

(○:業務停止なし×:業務停止あり)

4. おわりに

本稿では、VMware vSphere 5の仮想化環境においてCLUSTERPRO X／SSSを多様な構成で導入し、それぞれの構成について、vSphere HA基本構成と可用性の比較検証を行いました。その結果、全ての構成において仮想化環境へCLUSTERPROを導入することでvSphereの機能を補完し、可用性を向上できることが実証されました。具体的には大きく分けて以下の3点です。

- ゲストOS上業務アプリケーションの可用性向上
- 物理サーバ／仮想マシンレベルの障害に対する可用性向上
- 計画メンテナンスを業務継続で実施可能(ゲストOS間クラスタ構成のみ)

5. 付録

5.1. 業務ダウンタイムの比較

参考情報として、構成A、D、EについてOS停止障害時の業務ダウンタイム(障害発生から業務再開に掛かる時間)を比較したものを、図9に示します。構成Aは仮想マシンのフェイルオーバ・再起動において、ゲストOSの停止・起動時間を含むため、構成D、Eと比較してダウンタイムが大きくなります。

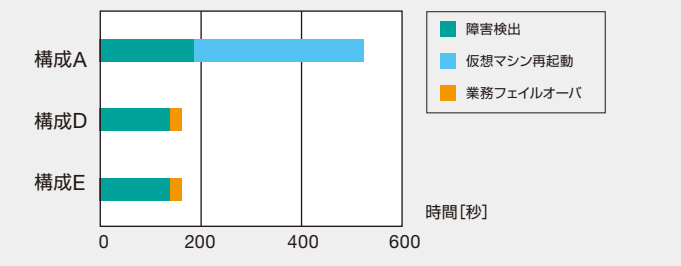

図9: 業務ダウンタイムの比較(OS停止)

図9の注意事項を下記に示します。

- 仮想マシンフェイルオーバ・再起動に掛かる時間は、ゲストOSの停止・起動を含むため、ゲストOSの種別に依存します。上記の業務ダウンタイムはゲストOSにRed Hat Enterprise Linux 5.7を使用しています。
- vSphere HAの仮想マシン監視とCLUSTERPROの各監視については、監視間隔やハートビートタイムアウト値を変更可能です。上記は全て既定値を使って評価しています。

5.2. 検証環境

本検証で用いた機材を以下に示します。

仮想化プラットフォーム	VMware vSphere ESXi 5 VMWare vCenter Server 5
クラスタリングソフトウェア	CLUSTERPRO X 3.1 CLUSTERPRO X SSS 3.1
管理用OS	vSphere Management Assistant 5
ゲストOS(Windows)	Windows2008 R2 Standard SP2
ゲストOS(Linux)	Red Hat Enterprise Linux 5.7
サーバ	Express5800 R120b-1 (N8100-1725)

NEC 第一ITソフトウェア事業部
CLUSTERPROグループ