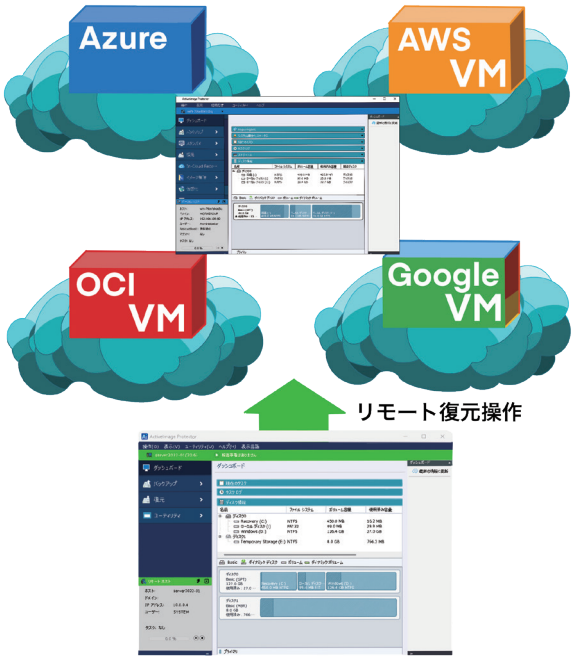
ActiveImage™ 2022
PROTECTOR

ActiveImage Protector ソリューションブック

Actiphy

ActiveImage™ 2022 PROTECTOR マルチクラウド環境への対応

Actiphy



ActiveImage Protector 2022 Cloudは、新たにマルチクラウド環境に対応しました。(Azure/AWS/OCI/Google)
各クラウドサービス上のコンピューターを、オンプレミスのサーバーOSと同様の操作でバックアップ/復元することができます。

マルチクラウド/オンプレミス/ハイブリッド環境において、エンジニアは環境を問わず同様の操作でバックアップ運用が可能なため、より身近に運用することが実現できます。

従来の専用アプライアンスを使用する方法と異なり、余分なコンピューターをクラウド上で起動する必要もなく、コストと使用ユーザー権限についての緩和も実現します。

・バックアップ運用方法
使用されているクラウドサービス上のコンピューターにActiveImage Protector 2022 Cloudをインストールして、コンソールを起動して、オンプレミス同様にバックアップタスクを作成して、バックアップを行います。

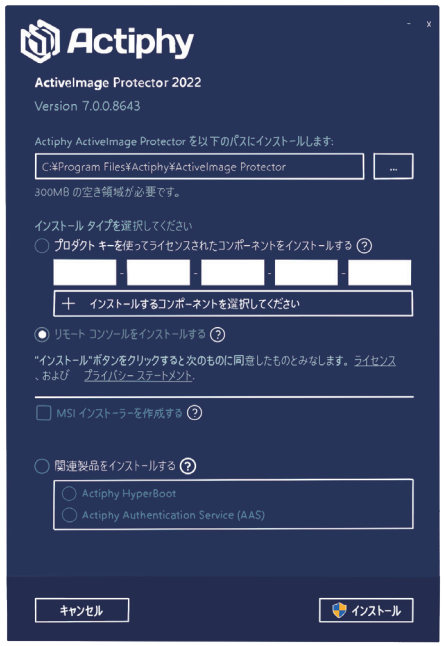
・復元環境の準備

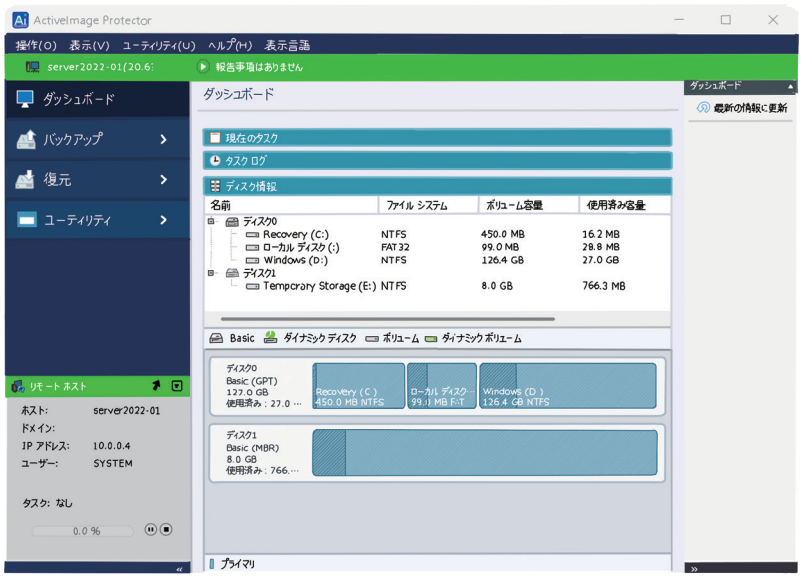
復元には、RescueBootを使用するため、コンソール上のRescueBootのスイッチをONにスライドします。後はクラウド上のコンピューター内に起動環境を自動作成します。

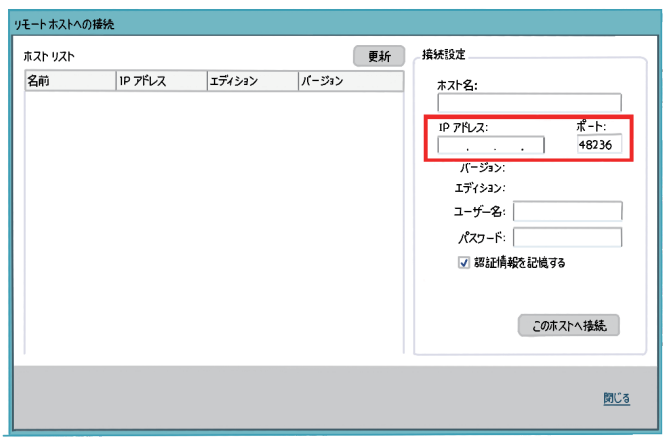
バックアップ対象としたマルチクラウド環境上の、コンピューターのポート番号48236を空けることにより、ActiveImage Protectorのリモートコンソールから容易に復元環境を操作することができます。

ActiveImage Protector のリモートコンソールは、インストーラーの"リモートコンソールをインストールする"を選択してインストールすることができます。

復元を行う場合、バックアップ対象のマルチクラウド上のコンピューター上で、RescueBootをタスクトレイより選択して実行します。
その後、当該環境へアクセス可能なコンピューターへインストールしたリモートコンソールを起動して、IPアドレスを入力するだけで、ActiveImage Protectorのリカバリーモードとなったマルチクラウド環境上のコンピューターへ、シンプルに接続することができます。
操作はオンプレミスのActiveImage Protector同様に、日本語のUIで表示されるため、簡単に行うことができます。



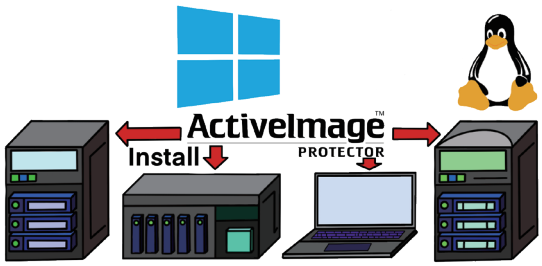




ActiveImage Protector は、システム環境/保護対象/運用方法/コストなどのバックアップポリシーに合わせた導入を行うことができるハイブリッドセキュリティーバックアップソリューションです。
今後増加する電子データからシステム全体までを、ハードウェア障害/ヒューマンエラー/ランサムウェア含むサイバー攻撃/災害などから保護することが、社会インフラを守ることに繋がります。
ActiveImage Protectorでは、BCP/DR/セキュリティー/人員不足からシステムを正常化することを実現できます。本書では様々な導入方法によるパターンについて解説しています。インフラエンジニアの方々のご参考になれば幸いです。

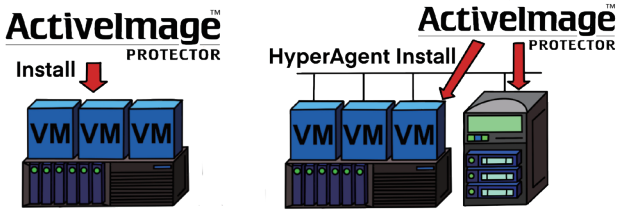
・物理サーバーの保護

Windows OSの物理サーバー/ネットワークストレージサーバー/パソコンとLinux OSの物理サーバーの場合、物理マシンに実装されるOSに直接ActiveImage Protectorのインストールを行って使用します。
ActiveImage Protectorの設定はインストールした各マシンで個別に行うことができます。



・仮想サーバーの保護

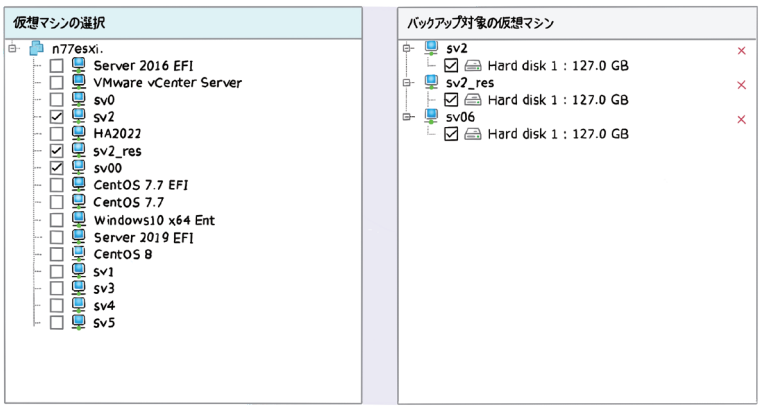
仮想環境の場合には、各仮想マシンにActiveImage Protectorをインストールしてバックアップ運用する方式と、Hyper-V/ESXiの場合には、HyperAgentを用意した、エージェントレスバックアップ方式より選択することができます。
KVMなどの仮想環境はエージェント方式のみ対応しています。

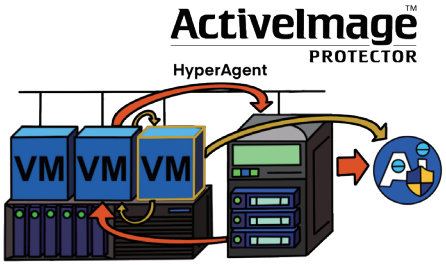


・HyperAgentとは

HyperAgentは、ActiveImage Protector 2022 Virtualを購入した場合に、納品されるHyperAgentキーを使用して、ActiveImage Protector 2022をインストールしたマシンへ、物理/仮想問わずに実装される機能のことです。
各仮想マシンにインストールを行って、エージェントバックアップする場合には、HyperAgentの設定を行う必要はありません。

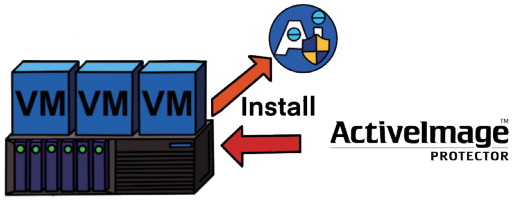
HyperAgentでは仮想ホストを登録することにより、登録された仮想ホスト上の仮想マシンを選択して、バックアップを実行することができます。
この方法では、バックアップ対象の仮想マシンには、何もインストールを行う必要はありません。HyperAgentとして使用するマシンは仮想/物理マシンは問いません。バックアップ対象の仮想ホストとネットワークで接続している必要があります。HyperAgentを実装する場合の留意点として、バックアップが動作した場合、全てのバックアップのパケットは必ず使用したHyperAgentを通過します。
このため、大量な仮想マシン/複数の仮想ホストをバックアップ対象とする場合には、HyperAgentを複数用意することにより、パケットの分散化を行うことができます。
また、HyperAgentはバックアップ保存先として使用するサーバーなどにインストールして使用することが一般的ですが、前提としてハードウェアスペックがある程度必要となります。





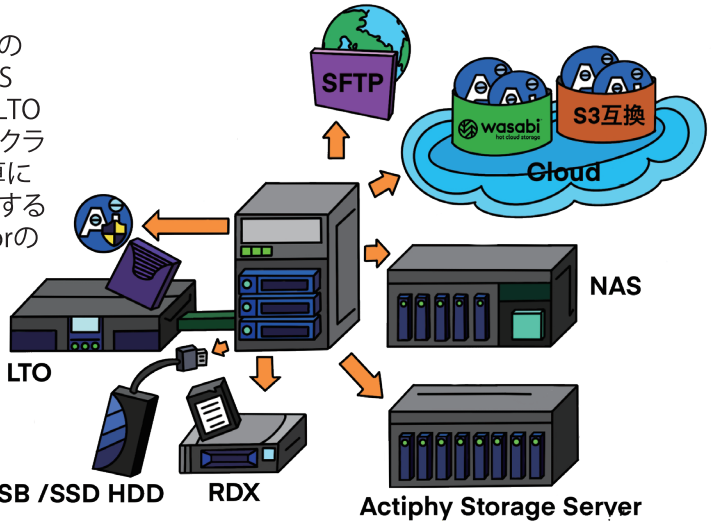
・Hyper-Vのバックアップについて

Hyper-V環境の場合には、仮想ホストはWindows OSとなるため、HyperAgentとしてインストールを行って、Hyper-Vホスト全体のバックアップを行うことで、仮想マシンは実質エージェントレスでバックアップすることもできます。
バックアップファイルはHyper-Vホスト全体の1ファイルのバックアップファイルとなりますが、ReZoom It!を使用することにより、仮想マシン単体毎の復元をすることもできます。



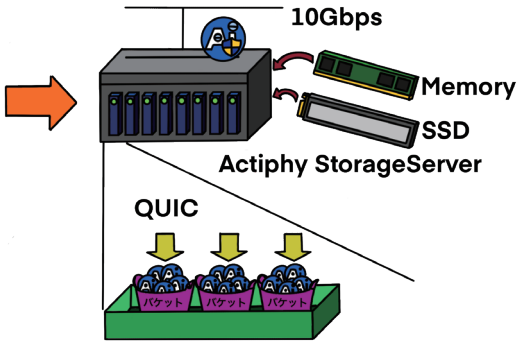
ActiveImage Protectorを使用してバックアップファイルを保存出来るデバイス

保存先として幅広いデバイスに対応しています。例えば物理サーバーのバックアップを行う場合、よく使用されるネットワークストレージのNAS(Windowsベース、Linuxベース)から、ローカル接続のデバイスとしてLTO/USB機器/RDX/ローカルディスク、そしてインターネット接続先となるクラウドサービス上のS3互換のストレージ/SFTPなど、お客様の環境、予算に合わせて使用することができます。また複数の保存先を使用して運用することもできます。またActiphy Storage ServerはActiveImage Protectorのバックアップ専用ストレージとして使用することができます。
※仮想マシンはLTOへの直接のバックアップを行えません。

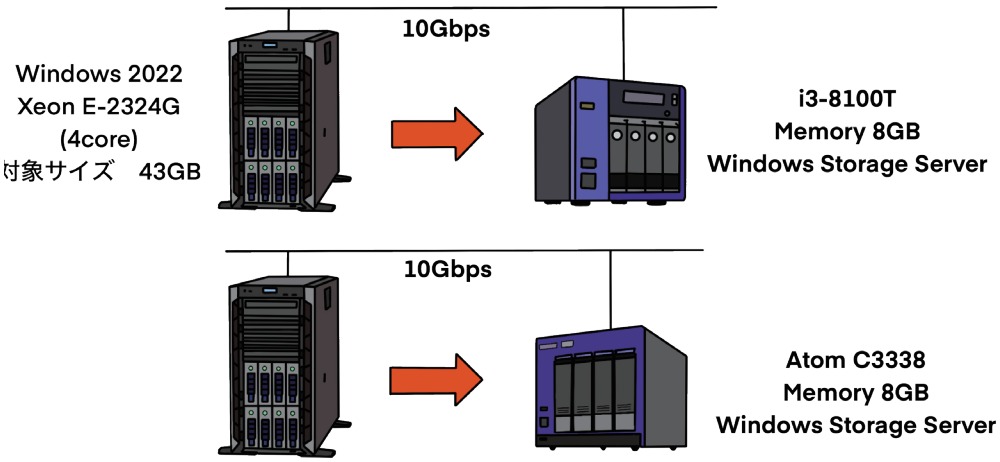


Actiphy StorageServerのメリット

Actiphy StorageServerは、Windows/Linux/Docker環境に導入することができます。バックアップ対象からの通信はQUICプロトコルを使用します。バックアップLANとして10Gbpsの回線でバックアップ対象とActiphy StorageServerを接続することにより、保存先側のメモリの70%をキャッシュとして利用するデフォルト設定においても、高速なデータ転送を実現します。キャッシュサイズは必要に応じてメモリ/SSDを追加することにより設定することができます。SSDのキャッシュはUSB接続でも効果が期待できます。



Actiphy StorageServerとアイ・オー・データ機器製の実践データの参考数値



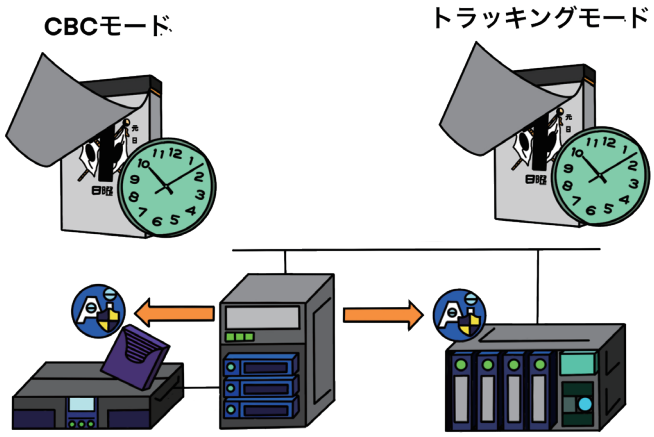
Atom NAS			
Copy	ActiveImage Protector		
CIFS	ASS	+SSD	CIFS
20分29秒	6分44秒	6分32秒	9分29秒
core i3 NAS			
Copy	ActiveImage Protector		
CIFS	ASS	+SSD	CIFS
6分28秒	6分８秒	5分6秒	9分5秒

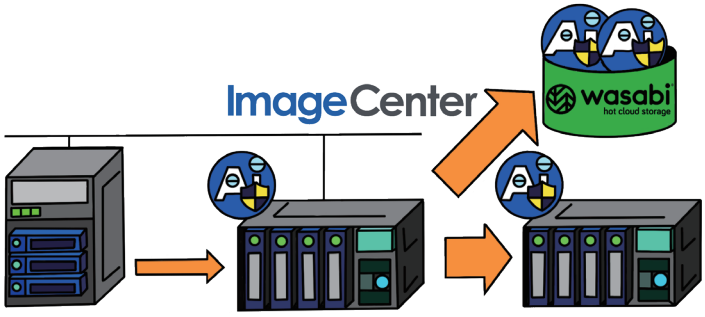
左の表では各書込み動作にかかった時間を比較しています。
CopyのCIFS=WindowsのCopyコマンドで同一サイズファイルをコピー
ActiveImageでバックアップを行った方法を下記のように表しています。
CIFS=TCP/IPで通常のCIFSにバックアップ
ASS=NASのMemoryのみをディスクキャッシュに使用
+SSD=ASSを使用してディスクキャッシュにMemoryとSSDを使用

ASSを使用して、デフォルト設定の70%のMemoryをディスクキャッシュにするだけで、約半分の時間でバックアップを完了することができます。
より短い時間でのバックアップ運用を行う場合には、i3モデルにSSDを追加キャッシュとすることで、実現できます。

分散型バックアップ運用について

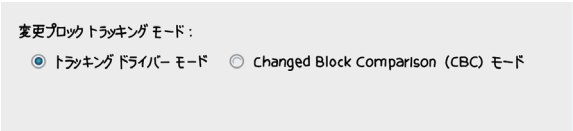
システムの運用に不可欠なバックアップの運用ですが、最近では2箇所以上の保存先を使用しての運用が増えています。
基本的には日々の運用の利便性の高いNAS(Windows/Linux)を使用して、追加でもう１箇所以上を使用します。
ActiveImage Protectorでは、複数のバックアップタスクの運用を行うことができます。日々のバックアップを行うNASにはトラッキングドライバーモードでバックアップタスクを作成します。また週/月/年などの単位で、2次保存先にベースバックアップを行うスケジュールには、CBCモードを使用してバックアップタスクを作成することにより、分散化されたバックアップ運用を行うことができます。





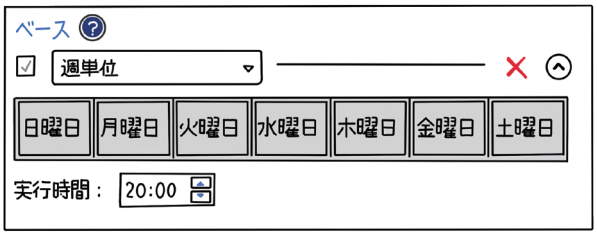
また、１次保存先(Windows)に付属のImageCenterをインストールすることにより、バックアップファイルをレプリケーションすることができます。遠隔地の拠点/S3互換のオブジェクトストレージなどに転送が可能です。レプリケーションはバックアップ対象側で実行することもできますが、保存先へImageCenterをインストールすることにより、バックアップ対象のリソースを使用しません。

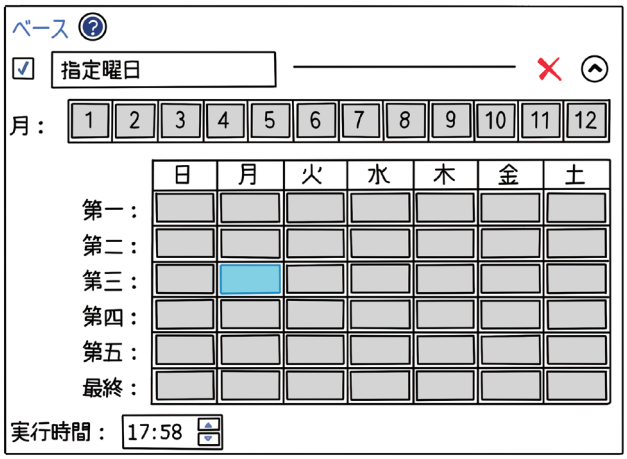
トラッキングドライバーモード/CBCモードのバックアップタスクの切替は、高度な設定内の下記で切替を行います。



バックアップタスクのスケジュール

もっともベーシックなバックアップのスケジュールは、週1ベースバックアップを行い、平日は増分バックアップを行い世代管理を行って運用します。
この場合、1世代は1週間分のバックアップとなります。

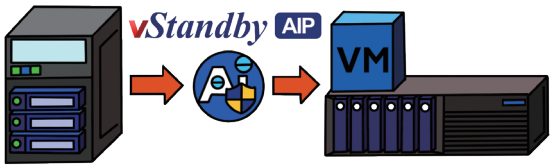


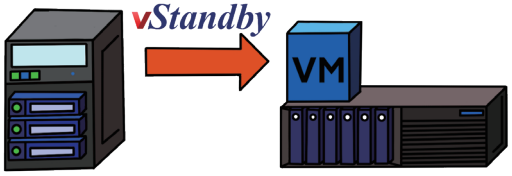


日本企業の業務に合わせやすい、第何何曜日といったタイミングでベースバックアップを行う月1ベースのバックアップ設定が行えます。
分散型バックアップを行いたい場合、例えば、ベースバックアップを月1回、それ以外は増分バックアップと設定し、1か月を1世代として1次保存先へバックアップを実行、別途2次保存先へ月1回ベースバックアップを実行するなど、自由にスケジュールを作成することができます。
世代管理はスケジュール作成後に設定を行います。必要容量は設定世代数+1世代分となります。

ダウンタイムを短くするシンプルな冗長化機能

ActiveImage Protectorではシンプルな冗長化の機能が2つ実装されています。
バックアップファイルを作成しないで、ダイレクトに仮想マシンにスタンバイマシンを作成するvStandbyと、作成されたバックアップファイルからスタンバイマシンを作成するHyperStandbyがあります。設定したスケジュールに沿ってスタンバイマシンを作成するため、一般的なHA/FTのように操作ミス/ウィルス感染の場合などでも、直ぐに反映されないシンプルな冗長化の機能です。緊急時には、仮想マシンの電源を投入するだけで、システムを稼働させることができるため、短時間での復旧を実現します。また物理マシンから仮想マシン、または異なる仮想ホスト間で仮想マシンの移行を行う場合、ダウンタイムの短い移行に利用することができます。





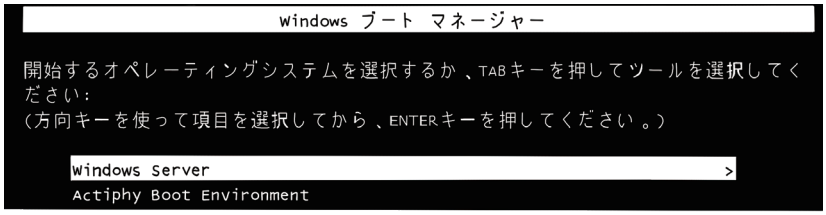
復元時の起動媒体起動のバリエーション

ActiveImage Protectorでディザスタリカバリーを実行する時に使用する、起動メディアでの起動方法は下記の通りです。

・ISO/DVD/USBデバイスを使用して、マシンを起動
従来通りのサーバー復旧方法です。Windowsベース／Linuxベースの起動メディアを用意することができます。作成は、Actiphy Boot Environment Builderを使用して行います。
仮想環境の場合などでは、ISOを作成するのが一般的となり、データストレージに保存を行い、各仮想マシン上でISOを接続しておきます。
またパソコンなどで使用される方法としては、USB SSDなどを起動媒体として、空き領域にバックアップを行うこともできます。。
基本的にWindows OSで使用する場合は、Windowsベース、Linux OSで使用する場合はLinuxベースの起動メディアを使用します。
またこの起動媒体を使用してコールドバックアップを実行することもできます。
Windowsベースの起動媒体の作成は、Windows ADKをインストールして使用することもできますが、ほとんどのマシンではWindows RE領域を使用して、起動媒体を作成することができます。

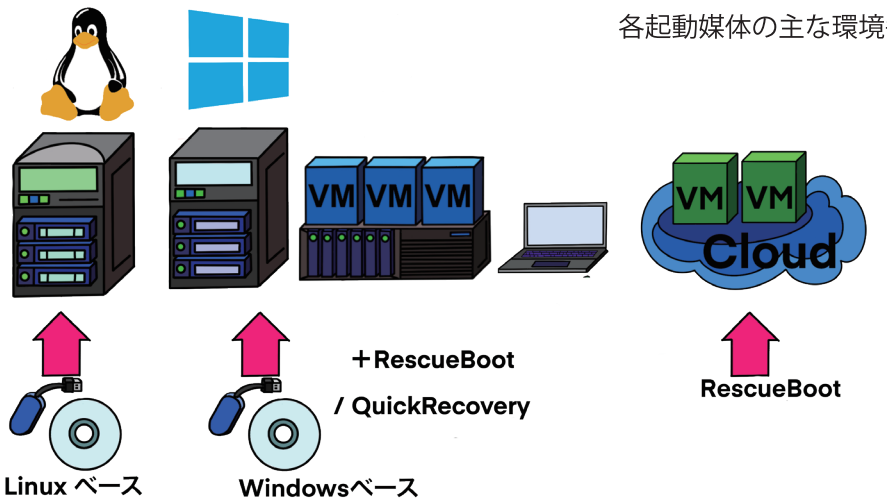
・RescueBootを使用してディスク内リカバリーで起動
設定は非常にシンプルで、ActiveImage Protectorのコンソールのダッシュボードより「システム健全性ステータス」タブの下記の部分をスライドするだけで、自動的にディスク内に起動メディアのイメージが組み込まれます。

組み込み完了後は、OS起動時に下記のようにWindowsブートマネージャーが表示されるようになり、いつでも起動媒体から起動することができます。基本的には、ディスクなどの故障などが発生しいない限りこの方法で起動を行い、ディザスタリカバリーを実行することができます。またRescueBootは次回マシン起動時に強制的に起動させる事もできます。



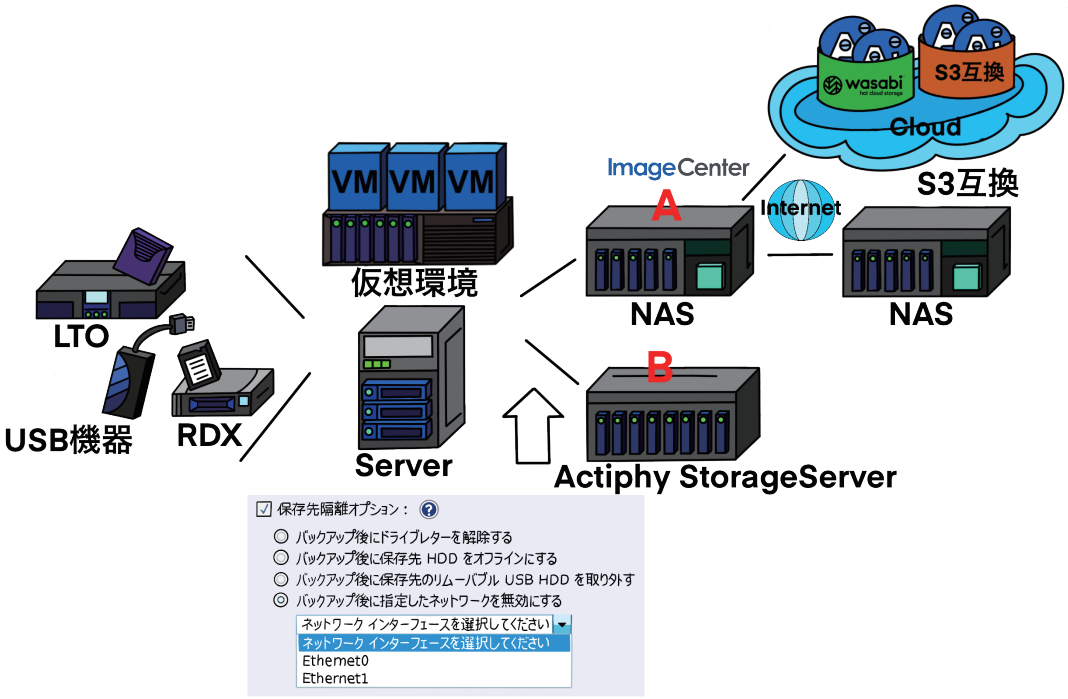
また、Rescuebootに予めバックアップタスクを紐づけしておくことにより、2クリックでディザスタリカバリー可能な、QuickRecoveryといった方法で復元する事もできます。RescueBoot/QuickRecoveryはActiveImage Protectorのタスクトレイアイコンよりメニューを表示させて実行することができます。

各起動媒体の主な環境毎の使用例は下記の通りです。



ランサムウェア対策を考慮した構成例

ランサムウェアを考慮してバックアップファイルを保護するには、単純にAD環境などに接続されたNASへの保存はお勧めしません。企業のAD環境には属さない単体マシンとして保存先を設置することにより、VPNの脆弱性よりAdministratorグループのアカウントを作成され、セキュリティ製品のサービス停止をされて感染が進んだケースでも比較的感染までの時間を稼げる傾向があります。
また可能であれば、バックアップ専用LANを用意して、通常の業務LANとは分けることが重要です。
また、Backup専用LANをActiveImage Protectorの機能である隔離オプションを使用して、バックアップ実行時以外では、ネットワークを遮断しておく必要があります。また2次保存先として、取り外しデバイスに対して月次バックアップを行い、メディアをローテーションすることにより、ランサムウェアからの感染リスクを軽減することができます。仮想マシンのバックアップをエージェントレス方式で行う場合にはWindows OSにHyperAgentをインストールする必要があります。保存先NASに実装する場合にはある程度のマシンスペックが必要となります。



・1次保存先
NAS Aまたは、BのActiphy StorageServerのどちらかを選択肢とした場合、ある程度のメモリ実装と10GbpsのバックアップLANを用意可能な環境の場合であれば、B選択のメリットがあります。またBのActiphy StorageServerを実装するOSをAD環境から隔離したLinuxにすることにより、ランサムウェア感染を遅らせる可能性があります。災害対策も考慮して遠隔地またはS3互換のストレージサービスにバックアップファイルを転送する場合には、NAS AがWindows OSであれば、ImageCenterをインストールすることで、バックアップファイルのレプリケーションを行うことができます。

・取り外しデバイス
LTO/RDX/USB機器の取り外しデバイスの選択に関しては、予算と運用方法に合わせて選択できます。隔離オプションでは、RDX / USB機器のバックアップ後のイジェクトが可能ですが、次のバックアップ前までに手動で接続またはメディアのインサートが必要となります。

・遠隔地/S3互換ストレージサービス
ランサムウェア対策と合わせて災害対策になります。S3互換のストレージへのバックアップ対象から直接のバックアップも可能ですが、回線速度を考慮した場合、2次保存先としての利用の方が現実的ですが、ダイレクトコネクトの場合には、問題ありません。

実運用のサーバーを100%ランサムウェアから保護出来るセキュリティソリューションはありません。またインターネットに接続が必要なサーバーは100%守ることは不可能なため、バックアップ運用を行い、被害を軽減することが現在のシステム運用上不可欠となっています。バックアップファイルは取り外しデバイスなどにも退避できるため、複数保存することによりリスク低減を行うことが、システム運用上重要となります。

ランサムウェア感染時の復旧について

ランサムウェア感染が発生した場合、バックアップファイルをそのまま復元を行わずに、必ずバックアップファイルの感染がないか、確認を行った上で、システム復旧の作業を開始します。
ActiveImage Protectorでは付属のHyperBootを使用することにより、仮想環境上で、バックアップファイルを直接起動させることができます。
起動させた仮想マシンのLog、不明なユーザーが作成されていないか、エンドポイントの動作などを行い、感染がないか確認する必要があります。