

# リソース融通のためのディスクレス型サーバ移送機構の提案

木場 雄一 福富 和弘 善明 晃由 木村 哲郎

(株) 東芝 研究開発センター

## 1 はじめに

企業内業務システムでは、滞りなく運用するために、最大負荷を想定し、それに合わせた冗長なシステムを構築しているものが多い。このように構築されたシステムでは、システムの平均負荷は数分の一と言われており、平時は余剰のリソースを抱えていることになる。

そこで、平時の動作に対応できるシステムを構築し、性能が不足する時に外部から計算機リソースを借用して補うことができれば、TCO(Total Cost of Ownership)の削減効果が期待できる。我々は、組織外から計算機リソースを調達し、そのリソースを自己の管理下で運用するためのリソース融通の研究を行っている。

本稿では、借用サーバのローカルディスクを用いないサーバ移送機構を提案する。

## 2 サーバ単位の企業間リソース融通

我々は、図1のような、データセンター内に共存するリソース貸出業者とユーザ企業間でのサーバの融通を想定している。サービスリクエストの集中による負荷等により計算機リソースが不足したユーザ企業は、リソース貸出業者にリソース要求を行う。要求を受けたリソース貸出業者は、ユーザ企業が持つ OS のブートイメージを利用して起動し、借用サーバをユーザ企業の管理下に置く。

我々はこの環境下でサーバ融通を実現するために、ユーザ企業が持つ OS イメージを借用サーバのローカルディスクに自動でインストールすることで実現するサーバ移送機構を提案している [1][2][3]。ユーザ企業が持つ OS のブートイメージは通常、貸出業者からは見えないので、LAN 環境で実現できるネットワークブートでは対応できない。そこで、提案したサーバ移送機構では汎用のブートイメージを貸出業者側で用意し、そのブートイメージで貸出対象サーバを起動する。次に、汎用ブートイメージに埋め込んである制御プログラムを介してユーザ企業の設定情報を入手した後、ユーザ企業の OS イメージを取得してから再度ブートするという一連の処理でサーバ移送を実現している。また、リソース融通では組織間で通信が発生するので、ユーザ

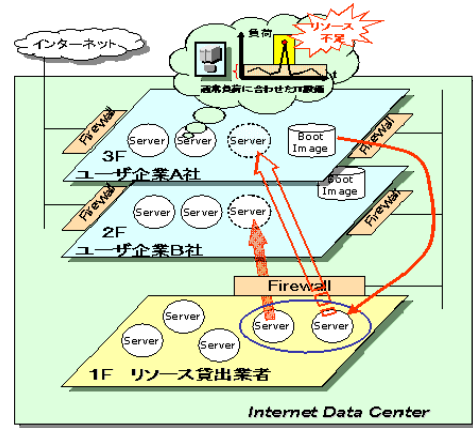


図 1: サーバ融通のイメージ

企業の秘密情報の漏洩を防ぐ必要がある。サーバ移送機構では、借用サーバとユーザ企業間で VPN を構築する。VPN 構築に必要な設定情報を借用サーバに送り、借用サーバ上で暗号化通信に必要な鍵を生成する。鍵は 1 回の融通のみに使われる使い捨ての鍵とする。サーバ移送機構では、移送並びに返却時における、組織を超えたブート処理やセキュアな通信を制御するために、ユーザ企業システム側を管理するマネージャ(借用側マネージャ)と、貸出業者システム側を管理するマネージャ(貸出側マネージャ)を設置して制御を行う。

OS の自動インストール方式によるリソース融通の場合、ユーザ企業の OS イメージのサイズが大きい程、インストールにかかる時間が長くなり、サーバ移送に要する時間が長くなる。また、リソース貸出業者が持つ借用サーバは、単一の企業に貸し出すとは限らないので、借用サーバのローカルディスクに書き込まれたユーザ企業 A の秘密情報が A 以外の他社に漏洩する危険性をはらむことになる。返却前にローカルディスク内を削除するプログラムを実行する等の対策はできるが、ディスク内の情報漏洩の危険性を完全に回避することはできない。そこで、本稿では OS の自動インストールによる方式とは別の方式として、ローカルディスクを用いずにサーバ移送を実現する方式(ディスクレス型サーバ移送方式)を提案する。

A Proposal of Diskless Type Server Transfer Mechanism for Resource Borrowing  
 Yuichi Koba, Kazuhiro Fukutomi, Teruyoshi Zenmyo and Tetsuro Kimura  
 Corporate Research & Development Center, Toshiba Corporation

### 3 ディスクレス型サーバ移送

ディスクレス型サーバ移送方式は、ユーザ企業側にあるファイルサーバ領域をルートファイルシステムとしてマウントし、借用サーバをユーザ企業の管理下で運用させることでサーバ移送を実現する。本稿では、借用サーバに Linux を入れ、ユーザ企業の NFS(Network File System) サーバにマウントさせるサーバ移送について述べる。

ディスクレス型サーバ移送方式の場合、移送のための設定をメモリ上しか格納できず、リブート後の環境に VPN 設定をはじめとする各種設定情報を引き継がない。そのため、借用サーバからマウントすべきユーザ企業ネットワークにある NFS サーバに接続できない。また、VPN 構築のために必要な設定やファイル、プログラムなどは通常、ルートファイルシステム上に置かれている。そのため、ルートファイルシステムが、起動直後に仮のルートファイルシステムとなっているメモリ上から、NFS に切り替わった後にあるべき情報が存在しない状態に陥る。

そこで、我々はリブート後の環境に移送設定を渡すために kexec を用いた [4]。kexec は Linux カーネルで提供されている機能で、リブート時に BIOS の初期化を経由しない高速な再起動を可能にする。リブートのために指定する対象ブートイメージはメモリ上に格納して再起動を行うため、サーバ融通に必要な情報をローカルディスク等に退避させずに設定を引き継ぐことが可能になる。リブート時に発生する、ルートファイルシステム切り替えによる各種設定の格納場所の整合性は、ルートファイルシステム切替前に、NFS 側に暗号鍵 (秘密鍵) を始めとする VPN 設定情報を送り、切替前と切替後の設定に関連するディレクトリ構成を合わせる処理で対応する。

図 2 にディスクレス型サーバ移送の流れを示す。移送処理は以下の順序で行われる。

1. 貸出側マネージャによって借用サーバを起動し、ブートローダと、起動用ブートイメージ (図 2 中 `vmlinuz(A)`, `initrd(A)`) を取得する。
2. `initrd(A)` に格納させておいた鍵生成コマンドを利用して公開鍵と秘密鍵を生成する。貸出側マネージャから電子証明書の署名を取得し、借用側ネットワークに接続するための情報 (借用側ファイアウォールの IP アドレス等) を取得して、IPsecVPN を構築する。
3. 移送 OS 用のブートイメージ (図 2 中 `vmlinuz(B)`, `initrd(B)`) をユーザ企業から取得する。`initrd(B)` には VPN 構築に必要な情報がないので、設定情報の追加と、必要なプログラムの起動処理を行うように編集する。
4. 移送 OS 用ブートイメージをリブート対象として、`kexec` を実行する。リブート前の環境はクリアさ

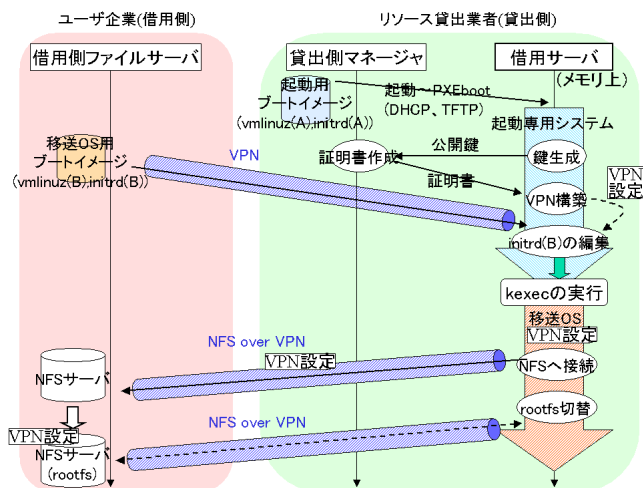


図 2: ディスクレス型サーバ移送の流れ

れるが、リブート対象の `vmlinuz(B)`, `initrd(B)` はメモリ上に維持されたままリブートが行われる。リブート処理開始直後は、メモリ上を仮のルートファイルシステムとして動作する。

5. IPsecVPN を確立し、NFS サーバの指定領域にマウントする。秘密鍵をはじめとする VPN 設定情報を NFS サーバにコピーし、仮のルートファイルシステムの構成に合わせて、NFS サーバ側のディレクトリ構成を調整する。
6. ルートファイルシステムを NFS 領域に切り替える。

これらの手順を踏むことでユーザ企業側の NFS をルートファイルシステムとした、借用サーバのディスクを使わないサーバ融通が可能となる。

### 4 まとめ

本稿では、リソース融通のためのサーバ移送方式として、借用対象サーバのローカルディスクを使用しないディスクレス型のサーバ移送機構を提案した。本方式や OS の自動インストール方式の他にも、移送方式のバリエーションを増やし、ユーザ企業の様々な要件に幅広く対応できるサーバ移送機構を目指す。

### 参考文献

- [1] 木場, 他, "リソース融通のためのサーバ移送機構の試作", 第 4 回情報科学技術フォーラム, 2005 年 9 月.
- [2] 木場, 他, "リソース融通のためのサーバ移送機構の概要", 情報処理学会第 67 回全国大会, 2005 年 3 月.
- [3] 善明, 他, "リソース融通のためのセキュアなサーバ移送機構", 情報処理学会第 67 回全国大会, 2005 年 3 月.
- [4] Andy Pfiffer, "Reducing System Reboot Time With kexec", [http://www.osdl.org/docs/reducing\\_system\\_reboot\\_time\\_with\\_kexec.pdf](http://www.osdl.org/docs/reducing_system_reboot_time_with_kexec.pdf), April 24, 2003.