6C-3

リソース融通のためのセキュアなサーバ移送機構

善明 晃由　木場 雄一　木村 哲郎　吉田 英樹　崎山 伸夫
株式会社 東芝 研究開発センター

1　はじめに

一般的に企業情報システムは、想定される最大負荷に合わせて構築される。多くの場合、システムにかかる平均負荷は最大負荷の数分の一である。このため、最大負荷に合わせて構築された企業情報システムは、余剰コンピューティング資源を大量に抱えることになり、TCO(Total Cost of Ownership) の増加につながる。

TCO 削減のためには、状況に応じて必要な計算機リソースを外部から調達することが有効である。そこで、我々は、企業情報システムが外部から計算機リソースを調達し、それを自己の管理下で運用するためのリソース融通の研究開発を行なっている。

リソース融通は、借用側企業の運用するサービスを貸出用サーバ上で運用可能にすることを目的とする。そのためには、借用側企業の持つ OS イメージで貸出用サーバをブートする必要がある [1]。この時、借用側企業が持つ OS やサービスの実行イメージを、セキュアに貸出用サーバに移送する必要がある。

本稿では、IPsec を用いて OS やサービスの実行イメージをセキュアに移送する方法を提案する。

2　リソース融通の概要

我々は、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。

例えば、スパイク的な負荷などにより、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を要求する。リソース貸出業者は、ユーザ企業からの要求を受けると、貸出用サーバをユーザ企業の持つ OS のブートイメージを利用して起動し、貸出用サーバをユーザ企業の管理下に置く。

図 1 に、リソース融通の概要 [1] を示す。ここで、ユーザ企業システム内で、リソースの調達を管理するマネージャを Procurement Organizer と呼び、貸出業者システム内で、貸出用サーバを管理するマネージャを Lease Manager と呼ぶ。

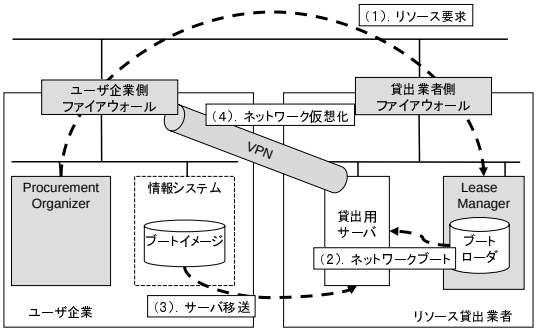

図 1: リソース融通の概要

リソースの借入れを要求するユーザ企業の Procurement Organizer は、貸出業者の Lease Manager にリソースを要求する (図 1(1))。要求を受けた Lease Manager は、自分の管理する貸出用サーバの中で貸出可能なものを起動させる (図 1(2))。起動された貸出用サーバは、ユーザ企業情報システム内のブートイメージを自身にインストールする (図 1(3))。これをサーバ移送と呼ぶ。ここで、ブートイメージとは、貸出用サーバが、ユーザ企業が要求するサーバとしてブートするためのイメージのことである。ブートイメージには、OS やサービスの実行イメージなどが含まれる。サーバ移送が終了すると、貸出用サーバは、ユーザ企業情報システムとの間に VPN を構築し、ユーザ企業の管理下にはいる (図 1(4))。

ユーザ企業の持つブートイメージを貸出用サーバに移送することにより、ユーザ企業の運用するサービスを、貸出用サーバで運用することが可能となる。

ブートイメージを移送する際には、ブートイメージに対するセキュリティを確保する必要がある。ブートイメージが、例えば、OS イメージといった、借用側企業の機密情報を含んでいるためである。

3　セキュアなサーバ移送機構

本節では、リソース融通におけるサーバ移送の際の課題とその解決法について述べる。

3.1　サーバ移送の際の課題

サーバ移送の際の課題として、以下の 2 点がある。

Secure Server Transfer Mechanism for Resource Borrowing

Teruyoshi Zenmyo , Yuichi Koba , Tetsuro Kimura , Hideki Yoshida and Nobuo Sakiyama
Corporate Research & Development Center, Toshiba Corporation
{zenmyo, koba, kimura, hideki, nobuo}@isl.rdc.toshiba.co.jp

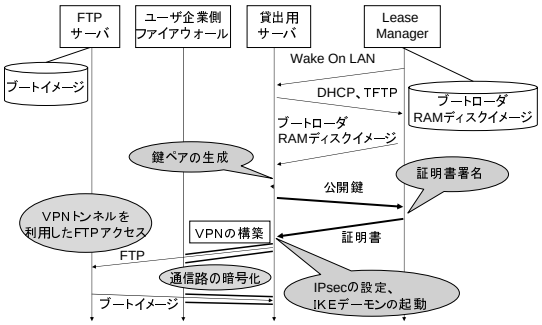

図 2: サーバ移送シーケンス

- 移送するデータの機密性の確保
  サーバ移送の際には、移送するデータが盗聴される可能性がある。これは、ユーザ企業と貸出業者間のネットワークが、データセンター内の他の企業とも共有されているためである。

- 移送するデータへの到達可能性
  移送する OS やサービスの実行イメージは、セキュリティ上の理由で、ファイアウォールなどによって保護された、外部から直接到達できない場所に配置されるべき場合がある。

3.2 IPsecVPN を利用したサーバ移送

3.1 節に示した課題を解決するために、サーバ移送の直前に貸出用サーバとユーザ企業間に IPsecVPN を構築することを考える。

IPsec のセキュリティプロトコルとして ESP [2] を利用することで、移送するデータの機密性を確保することができる。また、IPsec をトンネルモードで利用することによって、貸出用サーバとユーザ企業ネットワークを VPN で接続することが可能となる。

IPsec 通信を行なうためには、貸出用サーバに以下の機能が必要となる。

- 電子証明書の準備[1]
- セキュリティポリシーの設定 [3]
- IKE デーモン [4]

そこで、我々は、RAM ディスクイメージに上述の機能をもたせ、それを利用したサーバ移送機構を開発した。

図 2 に、IPsecVPN を利用したサーバ移送の流れを示す。サーバ移送は以下の順序でおこなわれる。

1. Lease Manager は、Wake On LAN などを利用して貸出用サーバを起動する。
2. 貸出用サーバは、DHCP、TFTP を利用して Lease Manager からブートローダと RAM ディスクイメージを取得する。
3. 貸出用サーバは、RAM ディスクイメージが持つ鍵生成コマンドを利用して、公開鍵と秘密鍵を生成する。また、生成した公開鍵を基に Lease Manager に電子証明書への署名を要求する。
4. Lease Manager は、署名した電子証明書を貸出用サーバに発行する。また、貸出用サーバにユーザ企業側ファイアウォールのアドレスを教える。
5. 貸出用サーバは、RAM ディスクイメージの機能を利用してセキュリティポリシーの設定を行ない、IKE デーモンを起動する。
6. 貸出用サーバは、ユーザ企業側ファイアウォールとの間に IPsecVPN を確立し、サーバ移送を開始する。

なお、ここで、ユーザ企業側ファイアウォールは、Lease Manager から署名された電子証明書を持っていることを前提としている。

ユーザ企業側ファイアウォールとの間に IPsecVPN を確立することで、移送するブートイメージの機密性を確保できる。また、ファイアウォールなどによって保護されたところにブートイメージが存在しても、貸出用サーバは、ユーザ企業側ファイアウォールとの間に構築された IPsecVPN を利用してブートイメージにアクセスできる。

4 まとめ

本稿では、リソース融通のための、OS やサービスの実行イメージの移送を、IPsecVPN を利用することでセキュアに行なう方法を提案した。

我々は、サーバ移送機構のプロトタイプを開発しており、今後は、試験運用などを通して提案手法の評価をおこなう予定である。

参考文献

[1] 木場雄一, 善明晃由, 木村哲郎, 吉田英樹, 崎山伸夫. 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.

[2] S. Kent and R. Atkinson. IP Encapsulating Security Payload. IETF RFC 2406, November 1998.

[3] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. IETF RFC 2401, November 1998.

[4] D. Harkins and D. Carrel. The Internet Key Exchange . IETF RFC 2409, November 1998.

[1] 認証用の鍵を利用することも考えられるが、セキュアに鍵を共有する方法が必要となる。