仮想化技術を用いたセキュアクライアントの提案

山本 一樹† 安井 浩之† 横山 孝典†

†東京都市大学
158-8557 東京都世田谷区玉堤 1-28-1

あらまし 近年，セキュリティ対策や総所有コスト(TCO)を削減するために，シンクライアントを導入する事例が増えている．しかし，シンクライアントの導入には専用の端末や高性能なサーバを必要とすることが多く，資金的制約の大きい中小企業や教育機関などでは導入が困難である．そこで本報告では，仮想化技術を用いて，既に導入されているクライアント PC 上に，ネットワークブート方式の仮想的なシンクライアント端末を作り出すことで，導入コストを抑えるシステムを提案する．本システムでは，クライアント PC 上に構築してあった既存の環境もシンクライアント環境と同時に起動・実行可能であり，従来のシンクライアントにはない利便性も実現する．

Proposal of Secure Client System using Virtualization Technology

Kazuki Yamamoto† Hiroyuki Yasui† Takanori Yokoyama†

†Tokyo City University
1-28-1 Tamazutsumi, Setagaya-ku, Tokyo 158-8557

Abstract Currently, introduction of a thin client system is increased for security measures and for reducing Total Cost of Ownership (TCO). However, it is difficult for minor enterprises and schools to introduce a thin client system with economical restriction, because it requires dedicated terminals and high-end servers in most cases. Therefore, this research proposes a system that virtual thin client terminal of network boot type is realized on existing client PC using virtualization technology for reducing introduction cost. Furthermore, this system also realizes to boot an environment that was constructed on existing client PC and a thin client environment simultaneously. This convenience has not been realized with existing thin client system.

1. はじめに

近年，情報漏洩問題が多発し，社会的な問題にまで発展している．情報漏洩の大きな原因として挙げられるのが，クライアント PC の盗難・紛失である[1]．またワームやウィルスへの感染や，不正な情報の持ち出しによる被害も少なくない．その根底には，「重要な情報をユーザの管理するクライアント PC 上に保存している」という問題が存在する．

現在，この問題への対策として注目を集め，既に多くの企業や自治体，教育機関などで導入が進んでいるのがシンクライアントと呼ばれるシステムである．

2. シンクライアント

シンクライアントはもともと，PC 自体が高価であった時

代に，1 台のコンピュータをより多くのユーザで利用するために考えられたシステムである．ユーザはそれぞれ「ハードディスクなどの高価なハードウェアを搭載しない安価な端末（シンクライアント端末）」を用いてサーバに接続し，処理を実行させ，その結果をクライアント側のディスプレイで受け取る．

PC の低価格化が進んだことで，シンクライアントはあまり利用されなくなっていったが，情報漏洩が大きな問題となったことで，クライアント側に情報が残ることのない安全な仕組みとして，再び注目を集めることになった．さらに，情報がサーバ側に集約されることで一元管理が可能になり，TCO 削減にも効果的であることから，今後も市場の拡大が予測されている[2].

現在，様々な方式のシンクライアントが存在するが，リモート実行型とローカル実行型に大別することができる．

2.1 リモート実行型

リモート実行型は，旧来のシンクライアントと同様に，実際の処理は全てサーバ側で実行し，クライアント側では画面情報の表示と操作のみを行う方式である（図 1）.

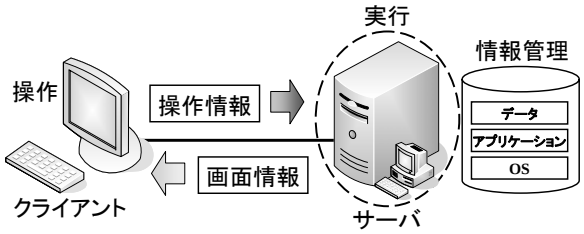

図 1 リモート実行型シンクライアント

サーバ

- 処理が集中するので，システムを安定して運用するには高い処理能力が必要

クライアント

- 入力情報の送信や画面の描画などの最低限の処理を行うだけで良いので安価な物を利用可能
- クライアントのハードウェア構成と，サーバ上で動作するOSやアプリケーションには依存関係がないため，異なるクライアントからでも同一のシンクライアント環境が利用可能

アプリケーション

- サーバに接続するユーザが共有して操作を行うため，マルチユーザ環境への対応が必要
- 画面情報はネットワークを経由するため画面遷移の激しいアプリケーションには不適

ネットワーク

- ネットワークを流れる画面情報は圧縮可能であるため，低速なネットワーク環境でも利用可能

2.2 ローカル実行型

ローカル実行型では，端末起動時にサーバ上に保存されている OS をネットワーク経由で取得して起動する. また，アプリケーション実行時には，必要な情報をネットワーク経由で取得し，クライアント側の CPU やメモリを用いて処理を実行させ，情報の保存はサーバ側で行う（図 2）.

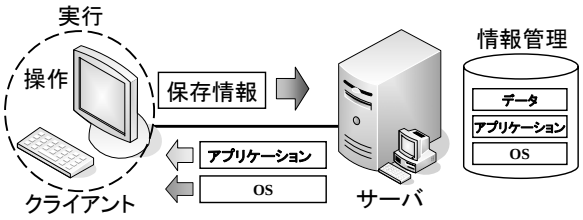

図 2 ローカル実行型シンクライアント

サーバ

- リモート実行型ほどの高い処理能力は不要

クライアント

- 通常のクライアント PC と同等の性能が必要
- クライアントのハードウェア構成と，サーバ上に存在する OS には依存関係があるため，クライアント側はハードウェア構成を揃えることが必要

アプリケーション

- アプリケーションをユーザが専有できるので，マルチユーザ環境への対応は不要
- ローカルで実行するので，画面遷移の激しいアプリケーションにも対応可能

ネットワーク

- OS やアプリケーションなど容量の大きな情報が流れるので，高速なネットワークが必要

2.4 問題点

セキュリティ対策や TCO 削減を目的として導入が進んでいるシンクライアントであるが，次のような問題点もある.

2.4.1 導入コスト

シンクライアントを導入する際に，最も大きな障害となっているのが導入コストである．

特にシンクライアント端末を導入する場合，端末自体の費用も負担となるが，既に導入済みのクライアントPCを置き換えなければならない点も問題となる．

加えて，リモート実行型ではサーバに高い性能が要求され，冗長化の検討も必要であることから，大きな負担となる．また，サーバの導入には安定した運用のために綿密な調査を必要とし，アプリケーションのマルチユーザ環境への対応など，費用以外にも導入のために多くの時間的コストがかかる．

一方，ローカル実行型では，サーバやアプリケーションのためのコストはそれほど大きくないが，高速なネットワークが必要となるため，既存のネットワーク構成によっては再構築が必要な場合がある．

2.4.2 ユーザの利便性

シンクライアントではOSやアプリケーションが一元的に管理されるため，ユーザが自分の扱いやすいように設定を変更したり，独自にアプリケーションを導入することが困難である．したがって，今まで使い慣れた環境で作業できなくなり，利便性が損なわれてしまう場合が多い．

2.5 既存の解決方法

2.5.1 既存 PC のシンクライアント端末化

既存のPCに搭載されているハードディスク（ローカルディスク）を，OSやアプリケーションの機能を用いて強制的に書込み禁止にし，情報を端末に残すことができないようにする方法である．CDやDVD，USBメモリなどの外部デバイスの利用を禁止することで，情報の持ち込みや持ち出しも制限可能である．

最近では，USBメモリなどに専用のOSと，サーバとやり取りを行うアプリケーションを入れ，起動時に読み込ませることで手軽に既存PCをシンクライアント端末化させる製品も増えてきている[3]．しかし，既存PCの場合，全てのハードウェア構成が統一されているとは限らないため，ほとんどがリモート実行型のシンクライアント端末としてしか利用されていない．したがって，リモート実行型で必要とされる，サーバの導入は避けられず，導入コストの削減には限界があるのが現状である．

2.5.2 複数台サーバによるユーザ環境の提供

サーバ側にユーザと同数のサーバを置き，ユーザに割り当てることで，ユーザは独自の環境を構築可能になる．ユーザがサーバを占有して使用できるため，アプリケーションがマルチユーザ環境に対応する必要がない．

サーバ側をブレードPCで構築する方式をブレードPC方式，仮想化技術を用いて1台のサーバ上に複数のサーバを稼動させる方式を仮想PC方式と呼ぶ．

しかし，ブレードPCは一般的に高価であり，仮想PCを利用する場合もサーバに高い性能が要求されるため，導入コストは増大してしまう．また，ユーザ独自の環境を構築可能ということは，ユーザの数だけ環境が存在することになり，管理コストもそれに比例して増えてしまう．さらにセキュリティリスクも高まることから，もともとの運用管理体制が十分な環境以外での導入は難しいといえる．

2.5.3 課題

シンクライアントを導入する際の問題点を解決するため，様々な方法が採られているが，中小企業は大企業に比べて導入が進んでいないのが現状である[4]．これは，既存PCのシンクライアント端末化だけでは導入コストの削減が不十分であることや，運用管理体制を十分に整える余裕がないことが原因であると考えられる．

そこで本報告では，資金的制約によって導入が困難であり，運用管理にもコストをかけることができない中小企業や教育機関でも導入が可能なシステムを提案する．

3. 提案するシステムの概要

3.1 仮想シンクライアント端末

提案するシステムでは，仮想化技術を用いて既存PC上に仮想的なシンクライアント端末を動作させる．この仮想シンクライアント端末は，ローカルディスクを割り当てず，外部デバイスの認識を制限することで，シンクライアント専用端末と同様の機能を実現する．

ここまでは，OSやアプリケーションによる既存PCのシンクライアント端末化と同等であるが，既存の方法と大きく異なるのが，仮想シンクライアント端末をローカル実行型であるネットワークブート方式の端末として利用できる点である．既存の製品にも，クライアントPCのハードウェア構成の数だけ，シンクライアント環境を用意するこ

とで，ローカル実行型の端末として利用できるもの[5]もあるが，管理する環境が増えれば管理コストの増大は避けられない．一方，提案するシステムでは，仮想化技術によってクライアント PC のハードウェア構成が抽象化されるため，どのようなクライアント PC 上でも同一のハードウェア構成を実現することができ，管理コストも抑えることが可能である．

ローカル実行型であるので，導入コストの大きな要因であった高性能なサーバを導入する必要がなくなり，既存の方法よりも大幅に導入コストを削減可能である．

また，本提案のもうひとつの特徴が，ローカルディスクに構築してあった既存のユーザ環境を，シンクライアント環境と同時に利用できる点である．これは仮想化技術が 1 台の物理マシン上で複数台の論理的マシン（仮想マシン）を同時に実行することが可能であることを利用し，既存環境も仮想マシン上で実行させることによって実現する．

仮想マシン同士は同一の物理マシン上で動作していても直接干渉することができないため，シンクライアント環境上にある情報が直接既存環境側に漏れることはない．したがって，重要な情報は全てシンクライアント環境で扱うようにすることで，情報漏洩のリスクを避けることができ，既存環境ではユーザが使い慣れたアプリケーション環境で作業することが可能になる．

しかし，この仮想シンクライアント端末を用いるだけでセキュアな環境を構築できるわけではない．

3.2 システム構成

シンクライアント環境の情報が既存環境へと直接漏れることはないと述べたが，ネットワークを経由して情報が漏れたり，マルウェアに感染するリスクは存在する．そこで，このリスクを避けるため既存環境のネットワークとシンクライアント環境のネットワークを分離する．また，ネットワークの盗聴を避けるためシンクライアント環境とサーバ間の通信に暗号化を施す．

さらに，不正な仮想化ソフトウェアによって仮想マシン間でデータ共有が行われたり，共通のネットワークを割り当てられる危険性を回避するため，シンクライアント環境の起動時にはサーバ側で仮想化ソフトウェアの正当性を検証し，認証を行う．

4. 仮想化技術

仮想化を実現する仮想化ソフトウェアは，実装形態によってホスト型とハイパーバイザ型に分類できる．

4.1 ホスト型

ホスト型は仮想化ソフトウェアを動かす OS（ホスト OS）が存在する．仮想化ソフトウェアはホスト OS 上でアプリケーションのひとつとして実行され，さらにその上で仮想マシンが動作する（図 4）．

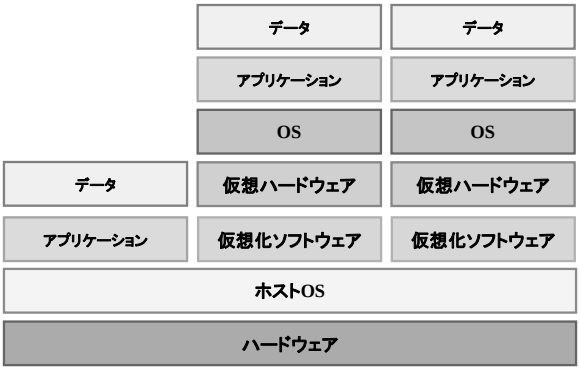

図 4 ホスト型

仮想化ソフトウェアがアプリケーションとして動作するので，その他のアプリケーションの影響を受けてパフォーマンスが低下したり，トラブルによって仮想化ソフトウェアがクラッシュしてしまう可能性も存在する．また，ホスト OS がキーロガーなどのマルウェアに感染してしまった場合，間接的に仮想マシン上の情報を奪われてしまう危険性がある．

4.2 ハイパーバイザ型

ハイパーバイザ型にはホスト OS という存在がなく，ハードウェア上で直接仮想化ソフトウェアが動作する（図 5）．

図 5 ハイパーバイザ型

ホストOSが存在しないため，ひとつの仮想マシンのトラブルがその他の仮想マシンへ影響を与えることがなく，マルウェアによる情報漏洩の危険性もない．

5. 実装方法

5.1 仮想化ソフトウェア

提案するシステムでは，シンクライアント環境上の情報を保護するために，ハイパーバイザ型の仮想化ソフトウェアを用いる必要がある．また，仮想環境の正当性を保証するためにハイパーバイザのチェックを行う必要があるので，仮想化ソフトウェア自体に手を加えることができるオープンソースソフトウェアであることが望ましい．

そこで提案するシステムでは，この条件を満たすXen[6]を用いて実装を行う．

5.2 シンクライアント環境

仮想マシンをシンクライアント端末として扱うために，以下のような設定を行い，仮想マシンを作成する．

・ローカルディスクを搭載しない
・CD/DVDドライブやUSBポートなどを搭載しない
・起動デバイスをLAN上に設定

5.3 既存環境

既存環境ではシンクライアント環境とは異なり，ユーザが自由に環境を構築できるように，以下のような設定の仮想マシンを作成する．

・ローカルディスク全体を仮想マシンに接続
・CD/DVDドライブやUSBポートを仮想マシンに接続
・起動デバイスをローカルディスクに設定

5.4 管理OS環境

5.4.1 管理OS環境の保護

Xenでは，管理OSが動作する仮想マシンをDomain0と呼び，その他の仮想マシンをDomainUと呼ぶ．Domain0ではクライアントPCの実ハードウェアを制御しており，仮想マシンの作成や設定変更もDomain0上から行われる．したがって，Domain0がセキュアに保てなければ，クライアント全体のセキュリティが保証できなくなってしまう．

そのため提案するシステムでは，Domain0上で動作させるプログラムをXenの動作に関わるものに限定し，実ハードウェアの制御や仮想マシンの制御だけを行える状態にする．また，この状態を維持するため，外部（ネットワーク）や内部（ユーザ）から管理OS環境が改変されないようにする．

外部からDomain0に対して脅威になるのが，マルウェアへの感染であるが，これらはDomain0にIPアドレスを与えないことで，進入する経路自体を塞ぐことが可能である．

一方，内部からDomain0に対して脅威になるのが，ユーザ自身が管理OS環境を改変してしまうケースである．この場合ユーザがDomain0にアクセスできないようにすれば，防ぐことが可能であるが，Xenではは DomainU を操作するには，Domain0から内部の仮想ネットワークを経由してリモート操作をする必要があるため，この経路を塞ぐことができない．

そこで，ユーザがDomain0へアクセスしても，管理OS環境に変更を加えられないように，Domain0では，DomainUを操作するためのアプリケーションのみをフォアグラウンドで動作させ，ユーザがバックグラウンドへ命令を送るためのコンソールを与えないことで，この経路を塞ぐ．

ただし，この状態では仮想マシンの起動・停止といった命令も実行できないため，「普段は既存環境だけを起動して，必要なときにシンクライアント環境を起動する」といった使い方ができなくなってしまう．そこで，提案するシステムを運用する上で最低限必要な命令を絞り込み，それを実行可能な専用のアプリケーションを管理OS環境上で動作させる．

5.4.2 ネットワークの分離

シンクライアント環境と既存環境のネットワークを分離するための機能は，パケットにタグと呼ばれる識別IDを付けて仮想的にネットワークを分割するタグVLAN[7]を，管理OS環境に実装することで実現する．

タグVLANは，実際のNICに対してVLANインタフェイスと呼ばれる仮想的なネットワークインタフェイスを作成し，そこを通過するパケットに自身のIDをタグとして付ける．タグ付きのパケットを受け取ったNICはIDを確認し，該当するVLANインタフェイスのみに送ることでネットワークを分離する．

提案するシステムではIDの異なるVLANインタフェイスをシンクライアント環境と既存環境にそれぞれ割り当てることで分離を実現する．

5.5 システム構成

全体のシステム構成を図 6 に示す.

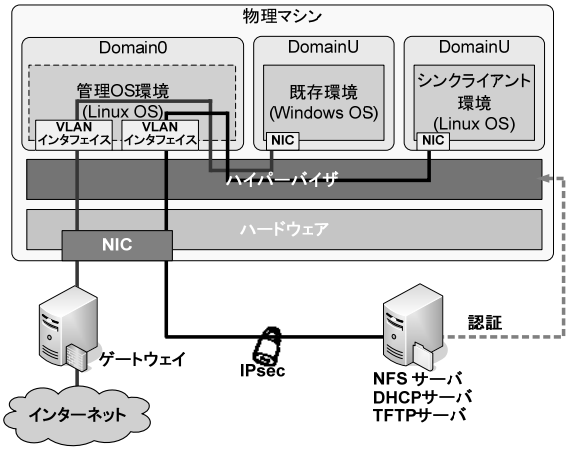

図 6 システム構成

ネットワークブート方式を実現するために, PXE(Preboot eXecution Environment)[8]というネットワークブートの規格を用いる. 仮想シンクライアント端末は起動時に, DHCP サーバによって IP アドレスが割り当てられ, TFTP サーバの IP アドレスを指定される. 指定された TFTP サーバでネットワークブート用のプログラムと設定ファイルを受け取り, 設定ファイルに従って, NFS サーバ上の OS を取得する.

提案するシステムでは, NFS サーバで OS を配布する前にハイパーバイザと通信を行うことによって正当性の確認を行い, セキュアでない仮想環境上でシンクライアント環境が動作しないことを保証する.

また, 仮想シンクライアント端末と NFS サーバ間では重要な情報が流れるので, IPsec[9]のトランスポートモードによる暗号化を実装することで盗聴を防ぐ.

6. まとめ

シンクラインを導入する際の問題として挙げられる導入コストと利便性に対して, 仮想化技術の持つ, 「ハードウェアの抽象化」と「仮想マシンの同時実行」という特徴を用いて解決する方法を提案した.

導入コストの面では, 「既存 PC の活用」と「高性能なサーバの導入を行わない」ことを同時に実現させることが可能であることを示し, 利便性の面では, 「重要な情報はシンクライアント環境上で取り扱い, それ以外の情報は使い慣れた既存の環境上で扱うことができる」という考え方を示した. これにより, 重要な情報とそれ以外の情報を切り分けることのできる環境であれば, 本システムの特徴である, 導入コストと利便性の両面でメリットが受けられると考えられる. たとえば, 教育機関では, 「成績などの個人情報はシンクライアント環境で取り扱い, 授業の資料は自分の環境で作成できる」という利用形態が想定できる.

今回は, シンクライアント環境上の情報がどのような経路から漏洩してしまうかに着目をし, その経路を塞いでいく方法をとった. しかし, 想定している経路以外からも情報が漏れる可能性が考えられるため, 更なる検証が必要である. 特に, 提案したシステムでは, 仮想マシン同士が仮想化ソフトウェアによって完全に隔離可能であることを前提にセキュリティを保証しているため, 仮想化ソフトウェア自体の脆弱性によるリスク[10]も考える必要がある. 他にも管理 OS 環境上で動かす最低限のプログラム構成や, Xen に命令を送る専用アプリケーションの機能なども十分検討しなければならないと考える. 今後は, 上記の点を検討しつつ, 実装を進めていく.

参考文献

[1] NPO 日本ネットワークセキュリティ協会, "2008 年情報セキュリティインシデントに関する調査報告書", 2009.

[2] 株式会社ミック経済研究所, "シンクライアント& デスクトップ仮想化市場の現状と将来の展望 2009", 2009.

[3] Resalio Lynx, http://www.mptech.co.jp/solution/lynx/lynx.html

[4]株式会社ノークリサーチ, "2008 年版 中堅・中小企業市場のサーバ・クライアント管理実態と展望 サーバ統合とシンクライアントの将来", 2008.

[5] Phantosys, http://www.wasay.co.jp/pdt/phantosys_1.htm

[6]Xen.org, http://xen.org/

[7]IEEE Std. 802.1Q-2005, Virtual Bridged Local Area Networks, http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf

[8]Intel and Systemsoft, Preboot Execution Environment (PXE) Specification, http://www.pix.net/software/pxeboot/archive/pxespec.pdf

[9]RFC 2401, http://www.rfc-editor.org/rfc/rfc2401.txt

[10]藤澤 一樹, 橋本 正樹, 宮元 久仁男, 金 美羅, 辻 秀則, 田中 英彦, "仮想マシンモニタにおけるデバイスドライバ安全性向上に関する提案", 情報処理学会論文誌 Vol.47 No.4, Apr.2006.