2007－DSM－44 (2)
2007／3／9

デスクトップPCの遠隔管理サーバーの構築と評価

柴田章博[a]、佐々木節[a]、金子敏明[a]、平川貴之[b]、坂爪孝行[c]
[a]KEK 計算科学センター、[b]日立情報システムズ、[c]日本IBM

概要：キャンパスLANに接続されたデスクトップPCの資産やソフトウエア構成の管理のコストは膨大なものとなってきている。さらに、インターネット接続するPCは、セキュリティー対策のため最新のセキュリティー対策をされた環境を維持する必要もあり、必ずしも十分な知識を有しないエンドユーザにとってPCの管理作業は負担となる。LANに散在するデスクトップPCの資源の有効利用と管理コストの軽減のため、PCのソフトウエア構成管理を遠隔支援する「PC構成サーバ」を構築した。また、PC管理データベースを作成しPC管理ソフトウエアを連携させることで、PCの構成情報の収集、ソフトウエアのインストール及びOSのパッチを含むのソフトウエアのアップデートの自動化及びライセンスの管理を統合することで多様なPCのソフトウエア構成に対応できる。

Construction of PC remote management servers and its evaluation

A.Shibata[a], T.Sasaki[a], T.Kaneko[a], T.Hirakawa[b], T.Sakadume[c]
[a]Computing Research Center, KEK, [b]Hitatchi Information Systems,[c]IBM Japan

Abstract: Desktop PCs are indispensable for research and official work in university and research institute. Most of staffs have own desktop PC on their desk, which are connected to the Internet. While, increasing the number of PCs connected to the campus LAN drive up management cost of PCs. The further fact that PCs connected to the Internet need well-maintained security measure weight on end-users, who do not always have sufficient skills for computer. We have constructed the remote management server for PCs that supports the administration of PCs through network. This server provide the assistant for sufficient use of PCs and reduction of administration cost. To support the variety of PCs, we also develop the database system which integrate administration jobs such as collecting the inventory, delivery and installation of software, update the software including OS, and license assignments.

1 はじめに

大学や研究所の業務や研究においてさまざまな処理が電子化されWebや電子メイルなどが不可欠となった。ほぼ一人1台の割合で、PCがキャンパスLANに接続され、デスクトップPCは数百に達しPC資源の管理やセキュリティー対策には膨大なコストがかかる。また、エンドユーザの中には、PCのセットアップに関して必ずしも精通しているわではないためPCのセキュリティー対策は負担であり、運用コストの軽減が望まれる。

大学の情報処理演習や事務系の計算機システムの計算機に関連するPCは、キャンパスLANの中に独自のファイアーウォールの中のネットワークにおかれ、ハードウエアおよびソフトウエアの一元管理が行われる。これらのPCは管理されたネットワークの中でのみ利用が認められ、中央集約的な管理サーバの配下で一様なソフトウエア構成による管理によって、運用コストを抑えることができる。一方、研究室や研究系に事務室でLANに接続されたデスクトップPCやノートPC（モバイルPC）は、研究室もしくは個人の単位でPCの管理がされている。また、ネットワークのセキュリティーに対する方針や運用も様々であるため、中央集約型のPCの管理方式を適用することはデスクトップPCの利用の自由度を落とすとともに、セキュリティー

の確保を困難にする。

中央集約な構成管理方式の問題点を検討し、個別管理されているデスクトップPCに対してソフトウエアの構成管理をネットワーク経由で遠隔支援するプロトタイプシステムを構築しその評価を行う。プロトタイプシステムは、広く利用されているMS Windowsを対象とし、PCの構成情報の収集、ソフトウエアのインストール及びセットアップ、OSパッチを含むソフトウエアのアップデート、ソフトウエアのライセンス管理を行うものを検討する。

2 PC構成サーバの構築

LANに点在するPCを対象とし資源の有効利用や管理コストの軽減を図るため、ソフトウエア構成管理を遠隔支援するサーバーの用件について検討を行う。その際、対象とするPCはさまざまなグループや個人の単位で管理され、ネットワークセキュリティのポリシーやネットワークアクセスの設定がさまざまであり、PC構成サーバの役割や管理者権限とネットワークアクセスの方法などの管理方式が重要な検討項目となる。

2.1 管理方式の検討

PCのソフトウエアの構成管理を行うには、PCの管理者権限を操作を行うプロセスに付与する仕組みが必要である。またネットワーク越しに遠隔管理を実現するためには、管理サーバとデスクトップPCのセキュアなネットワーク接続と操作の方式を定める必要がある。キャンパスLANに点在するPCを対象とするため、ネットワークセキュリティの確保に十分配慮されなければならない。デスクトップPCの遠隔管理方式には、PCの管理者権限の移譲の有無やネットワークアクセスの方法の観点から、「中央集約型」と「ユーザ要求型」に大きく分けることができる。

「中央集約型」は、デスクトップPCの管理者権限及び操作をPC管理サーバに集約する。PCの管理者権限をPC管理サーバに委譲し、PCの管理者は管理ワークステーションを介してリモートログインやリモートシェル、RPCなどのうえに、様々な操作を実装する。各デスクトップPCには、遠隔操作を待ち受けるエージェント（サーバ）が稼働し、リモートアクセスを受け付ける必要がある。この方式を実現するために分散システムのミドルウエアを導入するのが一般的で、MS Windowsでは、Active Directoryが使われる。分散システムもミドルウエアを利用するためには、管理サーバーとでデスクトップPCの間で様々なクライアント・サーバの通信を確保する必要があり、システム全体のセキュリティーの確保が課題となる。分散システム全体を同一のファイアウォールの中にいれて管理するのが一般的である。また、デスクトップPCの管理コストを抑えるために多くの場合、thin-clientが用いられる。

中央集約型は、デスクトップのデバイスの使用をコントロールし、デスクトップPC経由での情報漏えいの対策を実施する場合などに効果的な方法である。しかしながら、管理者権限の移譲が必要であるため、デスクトップPCのユーザ側でさまざまな利用形態を選択する自由度を持たせることには困難である。また、管理操作を行う際に管理サーバ及びデスクトップPCとの安全な通信路確保する必要があり、LANに点在するディスクトップの管理には不向きである。

「ユーザ要求型」は、デスクトップPCの管理者権限を委譲することなくPCの構成管理を遠隔支援する。PCの管理作業を管理者権限を持って実行できるよう、ネットワーク接続の手順を逆転させ、デスクトップPCからサーバへ管理操作を訪ねる方式をとる。デスクトップPCの管理者権限をもったプロセスが、管理サーバから指示された管理操作を実行するため、PCの遠隔操作の指示を受けるためのサーバ・プロセスの起動や管理者権限の委譲が不要となる。PC管理サーバとデスクトップPCの間の安全な通信が確保されればよい。デスクトップPCがパーソナルファイアウォール内に存在しても、NATやプロキシー経由でサーバーと接続できれば必要なサービスを受けることができる。デスクトップPC上での管理操作の実行は、管理者権限をもつユーザでログインして要求手動で要求を送る他、管理者権限をもったエージェント・プロセスを常駐させ、ユーザのログイン時や決められた時刻にPC管理サーバーに対して要求を送る方法などが考えられる。これらの方法は、Windows Updateやウイルス対策ソフトのパターンファイルの更新などの目的のために利用されている。

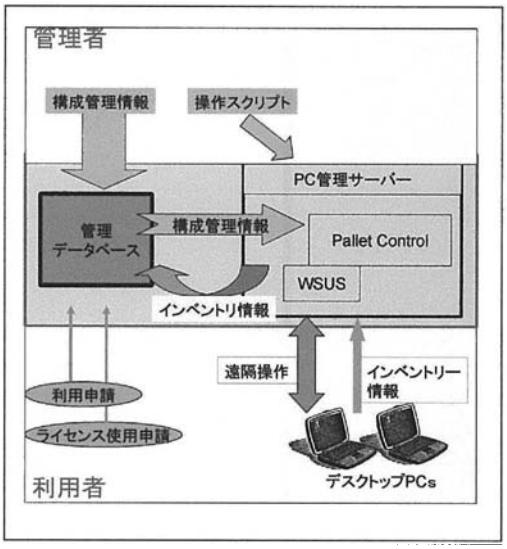
2.2 PC管理サーバの要件

PC構成サーバーは、キャンパスLANに点在するデスクトップPCを対象に、次の機能を有するソフトウエア構成管理を遠隔支援するシステムとする。そのために実現べき要件として、次のものが挙げられる。1)TCP/IP通信によるユーザ要求型の遠隔管理ができること、2)PCのハードウエア資源情報とソフトウエア構成情報の取得と管理ができること、3)有償ソフトウエアのライセンス管理ができること、4)ソフトウエアのインストールや設定作業の自動実行と選択的実行ができること、5)OSのパッチを含むソフトウエアのアップデート支援。これらを実装において、LANに接続されたPCのセキュリティーの確立と、多様なデスクトップPCの構成に対応できるよう配慮されることが望まれる。

このような要件を満たすシステムの概要を「PC構成サーバ概念図」に示す。デスクトップPC上では、管理者権限を持ったマネージメントプロセスを稼働させインベントリー情報を収集し、サーバーに送信する仕組みが必要となる。インベントリー情報は、収集するインベントリー情報は、CPU、メモリー及びディスク容量などのハードウエア構成やOSを含むソフトウエア構成とバージョンやライセンス番号などの情報が含まれる。インベントリーの収集は、デスクトップPCのログイン時や決められた時刻に送信され、それと同時にPC管理サーバで準備された操作コマンドが実行される。一方、サーバ側では、収集れたインベントリー情報はデスクトップPC毎にして保存管理され、インベントリーのビューアを用いて情報を検索・表示する機能を有する。収集されたインベントリ情報はPC固有の管理番号PCIDとともにサーバのデータベースで保持され検索や操作を行えることが必要である。

PC管理サーバで、計画したPCの操作を実行するため、デスクトップPCで操作コマンドを実行する環境が必要である。操作をスクリプトとして記述し、インベントリ情報の収集時に自動実行されるようにすることで、PCの遠隔操作を実現する。また、デスクトップ管理者がスクリプトを選択的に実行できるようにする。さまざまなソフトウエアの自動インストールを実現するために、セットアッププログラムの実行時に必要なマウスやキーボードの操作をエミュレーションする機能も必要である。

一方、ユーザ情報やソフトウエアのライセンスとPCの構成情報の統一的な管理を行うためのPC管理データベースが必要である。データベース上で管理された情報は、PC管理サーバの制御パラメータとして反映され、PC毎に異なる管理操作を実行できるような構成とする必要がある。この機能を用いて、特定のPCにおいて、ライセンスが付与されたソフトウエアのインストールを可能としたり、インベントリー情報に基づく設定変更が可能となる。



PC構成サーバ概念図

2.3 PC管理ツールの導入の検討

インベントリー情報の収集とPCのソフトウエアを配布する市販のパッケージ・ソフトエアが多数存在する。要件を満たす管理ツールを基礎部分から作成するのではなく市販されているパッケージを核として、必要な機能を拡充することでPC構成サーバを構築する。PC管理ツールの主要な機能であるPCそれぞれに固有のID（PCID）を付与やインベントリーの収集機能やソフトウエアの配布機能などの機能は、ほぼ実装されている。しかしながら、多くのパッケージはすべてのPCの一様な構成を行うには十分であるが、多くの場合、PCそれぞれを識別して固有の処理をおこなうような設定をするには機能拡張を行う必要である。ま

た、ソフトウエアの配布機能も、ブラインドインストールやバイナリーイメージの配布はあるが、インストー時のセットアッププログラムの操作エミュレートしインストールを代行するためのスクリプト言語を提供しているものは多くない。多様なPCの構成管理を行うためには展開イメージを送信するのではなく、セットアッププログラムをここのPCで実行する必要があるの。したがって、フリーソフトウエアを含む多種なソフトウエアのインストール操作を記述できる機能があらかじめ備わっていることが望まれる。

ライセンス管理を行うために、PC管理データベースとの連携が必要である。市販されるPC管理ソフトウエアにあるライセンス管理機能はインベントリー情報として使用されているライセンスを管理する方式のものが多い。しかしながら、本PC構成サーバで必要なライセンス管理機能は、一般のソフトウエアにたいしてライセンスの付与を管理とインストールの可否を制御できるものであり、新たにPC管理データベースを構築しPC管理データベースとのインストールプログラムが連携する連携機能を作りこむ必要がある。

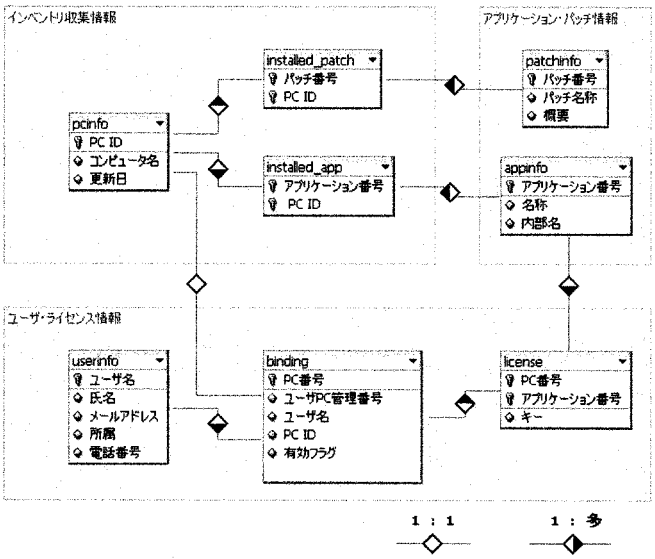


図 1: 管理データベース関係図

2.4 管理データベース

インベントリー情報とユーザ情報及びライセンス管理を統一的に管理するため、PC管理データベースを構築する。このことにより、多様なソフトウエア構成のPCの個別の操作などが可能となる。管理データベースを独自に構築することによって、ソフトウエアのライセンスの付与とインストールを統一的に管理する。さらに、ソフトウエアのインストールスクリプトの実行権を管理データベースと連携させることで、ライセンスを付与されたPCにのみソフトウエアがインストールできる仕組みを構築できる。また、クエリーを自在に組むことができるため、ユーザ情報などと連携させたさまざまな条件で検索や処理を行うことができる。条件にマッチするPCのユーザをリストアップしたり、注意喚起のメイルを送ることができる。

PC管理データベースは、次の機能を有する。1）PC構成サーバで管理するPC及びユーザの管理簿の機能を提供する。2）ユーザ情報とソフトウエアのライセンの情報を保持する。3）PC個々の収集したインベントリー情報とユーザを関連付ける、4）PC構成サーバーから配布されたソフトウエアとそれぞれのPCで

の構成情報を管理する、5）ソフトウエアのライセンスとPCへのインストールを管理する、6）データベースの情報をもとにPC管理サーバへ管理情報を設定をする。

PC管理データベースは、PC構成サーバーに収集されたPCIDをキーとするインベントリー情報とPC構成サーバーを利用するユーザ情報及びソフトウエアのライセンス情報を管理する。(図1参照). PC管理データベースのインベントリ情報はPCIDを識別子として収集されたインベントリ情報をもとに収集される。このインベントリー情報はさまざまなものが収集できるが、PC構成サーバの運用上必要とされるデータのみ格納し、最新の構成情報を保持するように設計する。PC構成サーバで、サポートするソフトウエアや配布するパッチ情報に関してもPC管理データベースで管理される。インベントリー情報に含まれる、アプリケーション番号やパッチ番号と関連づけることによって、インストールされたソフトウエアの情報及びパッチの適用状況を把握できる。一方、ユーザ及びライセンス情報は、ユーザ申請に基づくデータベースへの登録によって行われる。PCの資源情報は、userinfo と PCID とを関連づける binding によって行う。また、ライセンスの付与は、ライセンス管理データとPCの情報を対応付けることで管理する。また、PC管理データベースの管理情報とソフトウエアの配布サーバと連携することで、PCごとに配布するソフトウエアを設定する。

3 プロトタイプシステム

これまで検討をもとにPC構成サーバのプロトタイプを構築した。PC管理ツールとして、Pallet Control[2]を導入した。Pallet Controlは、ユーザ要求型のPC管理を行うソフトウエアであり、メニュー形式のソフトウエアのインストールツールを有する。PC管理データベース管理はPostgreSQLを用いて構築した。収集したインベンと情報のデータベースへの書き込みはPerlを用いた。また、ユーザ情報やライセンスの登録は、Webベースの作業を行うことができるようApacheとPHPを用いて実装し、運用管理の作業を委託できるようなシステム構成とした。また、デスクトップPCの参照構成を定め、試験環境を準備し提供するサービスのテストを行っている。

3.1 PCの管理

PC構成サーバの管理者は、PC構成サーバで配布するソフトウエアや設定を行うスクリプトを作成し、PC構成サーバに登録することでデスクトップPCの管理を行う。登録したスクリプトは、Pallet Controlのクライアントがインベントリー情報をサーバに送信したときに自動実行されるものと、マイクロインストーラによるユーザによる対話的な実行をするメニューとして登録することによって、自動実行や選択的な実行をコントロールすることができる。

プロトタイプシステムでは、PC管理サーバに登録された情報をもとに、PCごとに実行されるスクリプトを制御する機構をプログラムすることで、PCID毎に異なる操作を実行できるようにした。この機能を用いて、OSやインストールされたプログラムによって適用するパッチを切り分けたり、ライセンスの付与を設定したPCにのみ有償ソフトウエアをインストールできる仕組みをPC管理データベーすと連携して実行できるよう実装した。インストールできるソフトウエアは管理者があらかじめスクリプトを作成し、PC構成サーバーに登録されいる。インストールの可否は、PC管理データベースを通じてPCID毎にフラッグが設定され、インストーラのメニューでの選択が制御される。

3.2 日常の動作の設定

PC構成サーバのクライアントは、PCにログイン時または、決められた時刻にPC構成サーバにインベントリー情報をお送るように設定される。PC構成サーバで計画されている設定の変更は、Pallet Controlのインベントリー情報収集時に、計画されたスクリプトが自動実行され各ディスクトップPCの設定が反映される。プロトタイプシステムでは、セキュリティーに関連する緊急パッチの適用に限定して利用している。セキュリティーパッチの適用を管理することは、インターネットに接続しているPCの重要な管理作業のひとつであり、ユーザーの作業の軽減はPC構成サーバーの中核サービスの一つである。プロトタイプシステムでは、また、パッチ適用の状況の監視をPC管理データベースで行っている. また、ソフトウエア提供会社のアップデートサービスが利用できる場合は、それを活用

してソフトウエアのアップデートする方針とした。PC構成サーバでは、その運用のポリシーをすべてのPCに反映させ、インベントリ情報を監視することで、PCの管理を行う、プロトタイプシステムでは、Windows Update や Office Update については、WSUS [1] を導入して適用するパッチのレベルの設定やパッチ適用を実装した。

3.3 デスクトップPCのセットアップ

PC構成サーバのクライアントの設定は、申請時に配布する、スタートアップCDによるPallet Controlのクライアントソフトウエアをインストールすることで設定が完了する。スタートアップCDを挿入するとセットアップが自動実行され、ネットワークの接続のテストとIPアドレス設定を入力するとインストール作業は終了する。今後のPCの設定作業は、PC構成サーバを用いてネットワーク越しに行うことができる。PCの管理作業を行うために、ユーザ情報とPCの情報を関連づけるをデータベース上で行うとPC構成サーバの登録作業は完了する。最初のインベントリー情報を収集とともに初期設定のスクリプトが自動実行され、すべてのPCに共通の設定が施される。共通設定を行う項目は、PC構成サーバの管理者が、自動実行されるスクリプトを制御することでおこなうことで自在に設定ができるが、必修パッチの適用や、運用ポリシーのポリシーの設定などに活用している。

PC構成サーバのクライアントは、PC構成サーバーへの登録が完了すると、マイクロインストーラをもちいて必要なソフトウエアの選択的なインストールを行うことができる。有償ライセンスのソフトウエアは、申請を行うとライセンスが付与され、インストールメニューで選択できるようになる。提供するインストールのスクリプトは、インストールプログラムのキー入力を代行して自動インストールが実行されるようにプログラムされている。また、インストールのスクリプトを連続実行するすることで複数のソフトウエアを一括して自動インストールするメニューも準備されており、数ステップでPCの設定を行うことができる。

4 まとめと議論

Windowsのデスクトップを対象にPCソフトウエア構成の管理を遠隔支援するシステムを構築した。管理機能のトリガーをデスクトップPCからの要求に基づいて行うユーザー要求型のサーバを構築することで、管理者権限の委譲を行うことなくPCのソフトウエア構成管理を実現することができた。PC管理データベースを構築し、ユーザ情報とPCの構成情報及びライセンスを統一的に管理し、PCの構成管理の個別設定を実現した。選択的なPCソフトウエアの構成を自移送することで、多様なソフトウエア構成のPCに対してサービスの提供が可能となった。PC管理データベースと管理機能の連携を充実させることによって電子申請やオンラインでのPC管理オプションなどの変更などの機能を充実させることが可能である。現行の遠隔管理の方式は異種OSへの適用をすることが原理的に可能である。しかしながら、セットアップや管理作業をエミュレートするスクリプトの作成をプラットフォーム毎に作成する必要があり、管理サーバ管理者の負担である。また、より広範な管理サーバの構築には、セキュアネットワーク接続とセットアップスクリプトの安全性の保証の方法などが検討課題である。

参考文献

[1] Windows Server Update Services (WSUS) URL=http://www.microsoft.com/japan/windowsserversystem/updateservices/default.mspx

[2] Pallet Control； JAL Infomatic 社が提供す PC 管理ソフトウエア。URL=http://www.jalinfotec.co.jp/product/pallet/

[3] PostgreSQL URL=http://www.postgresql.jp/