【論文】

ネットワークサーバ機群の安全な維持管理に関する研究

大島　義智[*1]　松本　勝哉[*2]

Research on Secure System Maintenance for Network Server Machines

Yoshitomo Oshima[*1], Katsuya Matsumoto[*2]

Abstract: In these several years, it reached the situation we can easily get information through Internet on a worldwide scale. The various servers were installed even in our laboratory, and the information system environment that is adjusted to this kind of circumstance was improved for our laboratory students. Adjustment of the system was delicate, then it became the circumstance where often the server is unstable and/or suddenly had stopped. Our aim is simple that responsibility of the system manager to be little and confusion of plural manager to be little too. In this paper, we present the new system proposal for maintenance of server machine group through the VPN encoding communication method that can be controlled safely with remote manipulation. In supervision of the server machine group system, we use Mac OS X server supervisory tool and software "Webmin" to be able to manage basically with GUI. The result after the improvement was satisfactory, the supervision of the actual dynamic time of the server machine group became easier than before. It is future topic concerning the maintenance of the system that covers long term.

Keyword: Secure System, Maintenance, VPN, GUI

1. はじめに

近年、世界中でインターネットを介して様々な情報を容易に入手でき、便利な各種サービスを受けることが日常的な時代となった。日本において2005年2月に行われた調査によるとインターネット人口は7千万人に達成したとされている[1]。我が研究室内においても、年々、自宅でPC（Personal Computer）を使ってインターネットを利用している学生が増加している。2005年4月に研究室内でアンケートを実施した結果では、自宅にPCを10人中全員が保有しており、全員がインターネットを利用していたことに加えて、10人中5人がノート型PCを保有し、無線LAN（Local Area Network）を導入していたことが得られた。このような結果から家庭内や研究室内でも、ネットワークを介した各種情報サービスを提供できるシステムが必要不可欠であると考えられた。

これまでに、研究室内ではネットワークのサブネット化を行い、学生個人のデータ領域を確保することで、ネットワーク上でファイルを共有できるようにしてきた。さらに、研究室内に無線LANを導入することによって、学生が持参したノート型PCでインターネットを利用できるようにもした。このように、研究室内でも、独立したネットワーク上でメールを除く各種情報サービスを提供できるようにサーバの構築を進めてきた。

しかしながら、研究室内LANを利用する際に、システムの障害によりインターネットに接続できない、ファイルを共有することができない、研究室のPCが利用できないなどの問題が発生することもあり、必ずしも安定したサービスを提供する状況にはなかった。頻繁に小さな問題が発生していることや、システムの復旧が長期に及ぶ状況を回避するためには、管理者がネットワークやシステムの状態を常時監視し、問題発生時は迅速な対応できることが望まれるが、そのためには管理者に負担がかからないシ

*1 工学研究科電気工学専攻博士課程前期2学年
*2 電気工学科

ステムの構築が必要である。

そこで、本研究では各種サーバ機群の GUI（Graphical User Interface）による管理・監視と第三者からの盗聴や改ざんを防ぐ VPN（Virtual Private Network）暗号化通信を組み合わせて行い、大学の研究室程度の小規模 LAN 上でネットワークサーバ機群を安全にかつ管理者に負担の少ない維持管理システムを提案している。

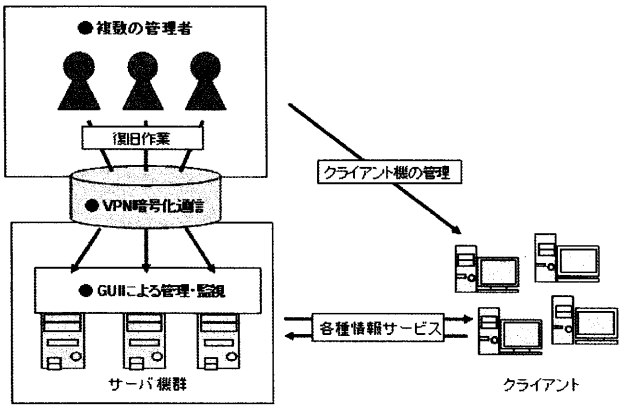

図 1 システムの構成

2. 研究室内 LAN

研究室内 LAN は 2003 年 4 月の時点から 2005 年 12 月までに大きく改善された。

2.1 サブネット化された研究室内 LAN[2][3]

サブネット化によって、メインネットワーク上の無駄なトラフィックを軽減され、PC の台数の増加で研究室に与えられたグローバル IP アドレスの不足をプライベート IP アドレスで補うことで、研究室内の PC はすべてインターネットを利用することができた。サブネット化されたネットワークを管理するサーバ機にファイルサーバなど導入することで、学生個人のデータ領域を確保し、ネットワーク上でファイルを共有できるようにもなった。

2.2 研究室内に無線 LAN を導入[4]

無線 LAN の存在は、2000 年春頃から低価格な無線ルータの製品が続々と登場することで、ここ数年間で身近な存在となり、一般家庭や企業内で導入しているケースも増加している。さらに、研究室でも持参のノート型 PC を使用することも多くなってきた。このような状況により、研究室内に無線 LAN の必要性があると考えられたので導入を行った。また、無線 LAN でもサブネット化した研究室内 LAN のファイルサーバなどのサービスを受けることも可能とし、無線の暗号化には WEP（Wired Equivalent Privacy）を利用して安全な通信を行っている。

2.3 研究室内 LAN の安全な維持管理

学部生が研究室内 LAN を実際に利用することで、システムの障害によりインターネットに接続できない、ファイルの共有が利用できない、研究室の PC が利用できないなどの問題が発生した。システムの障害は復旧するまでに数日かかることがあり、要因としてシステムの障害の原因がわからない、システムの障害の原因はわかるが改善に時間を要する、管理者が不在の場合があった。システムの障害が発生してから、システムの復旧が長期に及ぶことや、頻繁に問題が発生するような状態では、研究室内 LAN が安定な状態ではなく、ネットワークを経由して効率的な利便性のあるシステムを提供しているとは言えない。このような状況を回避するためには、管理者がネットワークやシステムの状態を常時監視し、問題発生時には迅速な対応できることが必要であると考えられる。

しかしながら、これまで研究室の管理者は 1 人であることが多く、常に対応できる状態とは限らず、問題が複数生じると対応が困難になった。その結果、研究室の管理者を増員することを考えたが、システムの設定がどのようになっているか即座に理解させるのが難しいためできなかった。また、問題発生時には迅速な対応するためにサーバの監視や管理をネットワーク経由で行うことは便利だが、第三者に盗聴や改ざんされることなど危険性もある。

本研究のシステムを導入して改善された研究室内 LAN の構成を図 2 に示す。

3. 研究室内のサーバ機群

図 2 で示すように研究室内 LAN は、松本研究室学部生室のサブネット化された LAN（サーバ機名が Blue で、以下 Blue と呼ぶ）、研究室内無線 LAN（サーバ機名が Fedora で、以下 Fedora と呼ぶ）、Web システム（サーバ機名が Brazil で、以下 Braizil と呼ぶ）、院生室のサブネット化された LAN（サーバ機名が mmacx で、以下 mmacx と呼ぶ）の主に 4 つのサーバ機群のシステムで構成されている。

3.1 システムの提供範囲

研究室内 LAN のシステムは、研究室内、学内（研究室内除く）、学外の 3 箇所の提供範囲がある。サーバ機群のシステムの提供範囲を表 1 に示す。

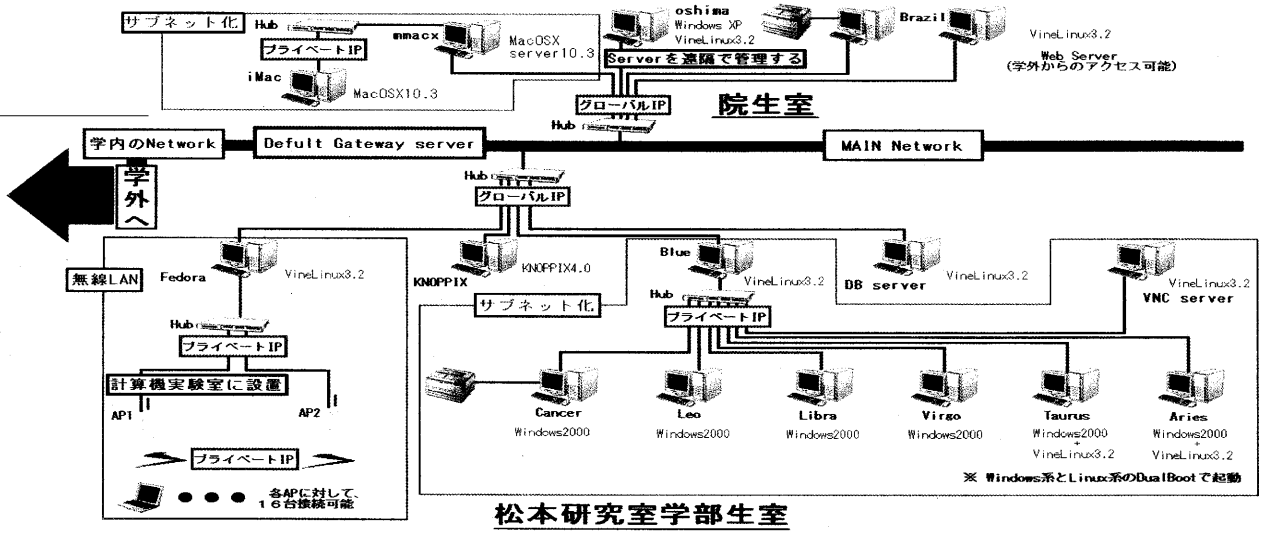

図 2 2005 年 12 月 時点の研究室内 LAN の構造

表 1 システムの提供範囲

	システムの提供範囲		
PC 名	研究室内	学内（研究室除く）	学外
Blue	○	△	×
Fedora	○	○	×
Brazil	○	○	○
mmacx	○	△	×

○・・・提供している、△・・・一部提供している
×・・・提供していない

表 1 より学外へシステムを提供しているのは、Web システム（Brazil）だけである。これは不正なアクセスやサーバ機を踏み台にして学内に進入される危険性などの安全面を考慮して、学外からの遠隔管理やファイルサーバでの研究室内のデータは公開しないようにしている。しかし、学内からの遠隔管理やファイルサーバの利用に関して研究室内のデータは公開している。表 1 中の△印で表している「一部提供している」は、学内からの遠隔管理や研究室内のデータを公開している意味である。

3.2 サーバの種類[5]

研究室内のサーバ機のシステムは、各種情報サービスを提供できるようにするために、様々なサーバを導入している。サーバ機と各種サーバの対応表を表 3 に示す。

3.3 サーバ機の各種サーバを統合した管理

表 2 で示した各種サーバを容易に設定できるよ

表 2 サーバ機群のシステムと各種サーバの対応表

	サーバ機名			
サーバの種類	Blue	Fedora	Brazil	mmacx
DHCP	○	○	×	○
NIS	○	×	×	×
NFS	○	×	×	○
Samba	○	×	×	○
FTP	×	×	○	○
VNC	○	○	×	○
SSH	○	○	○	○
Web	○	×	○	○
DB	×	×	○	×

○・・・導入している、×・・・導入していない

に、GUI で統合した管理を行えるように、「サーバ管理」と「Webmin」のソフトウェアを導入した。

「サーバ管理」のソフトウェアは、Mac OS X サーバ 10.2 以降であるなら、デフォルトでハードディスクのアプリケーションで Server のフォルダにある。Mac OS X 10.2 以降のクライアントは、Apple 社の公式サイトより AdminTools.dmg のファイルを取得することができる。

動作画面はサーバ機で mmacx の local 情報が表示され、左部のカテゴリにはサーバ機のネットワーク名と各種サーバ名、右部のカテゴリ内には選択された情報、下部にはその詳細な情報や設定を表示できる項目がある。

図 3 中の左部のカテゴリには、各種サーバ名と動作状況が表示されている。各種サーバの設定を行う

には、サーバ名を選択し右部のカテゴリ内の設定の項目を選択すればよい。例として DHCP サーバの状況画面を図 4 に示す。

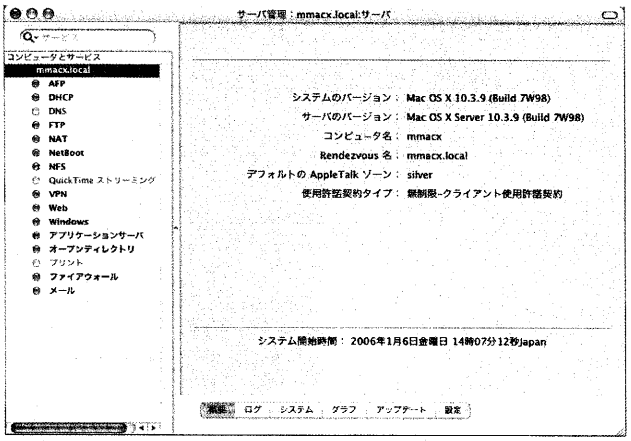

図 3 「サーバ管理」の起動画面

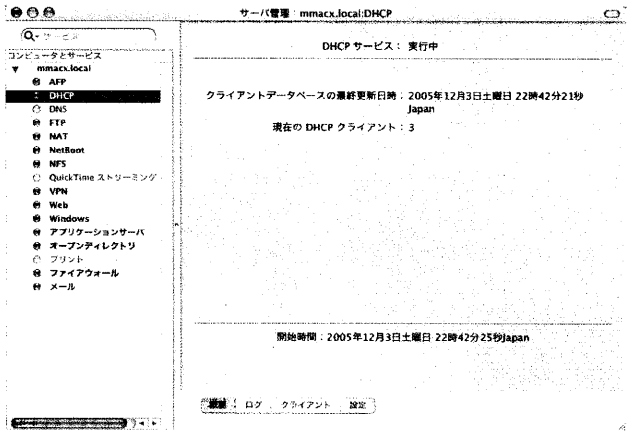

図 4 DHCP サーバの状況画面（サーバ管理）

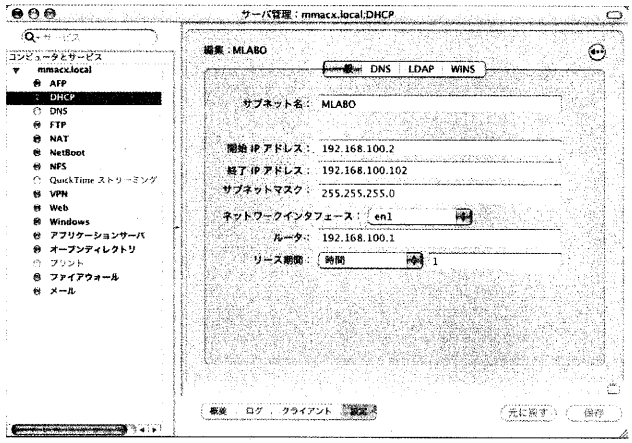

図 5 DHCP サーバの設定画面（サーバ管理）

選択した最初の画面は、サービスの状態、現在のクライアントの接続数、開始時間など DHCP サーバの概要が表示されている。下部に DHCP サーバのログ、クライアント、設定の詳細な情報が選択できる。

図 5 より GUI で表示されているため、DHCP サーバでどのような設定がされているか理解しやすい。サブネット名の MLABO が存在し、IP アドレスやインターフェースなど設定していることが容易に理解できる。

Webmin は、多数のモジュールが組み込まれており、GUI で各種設定を管理でき、Perl 5 で記述された CGI プログラム群で構成されているので、Linux だけではなく FreeBSD や Mac OS X、Solaris など多様な OS で利用できる。操作は Web ブラウザを利用してアドレスに https://localhost:10000 と記述することで表示されるので容易に扱える。また、https は Net_SSLeay モジュールによって SSL 機能を有効化しているので暗号化されて安全に通信ができる。

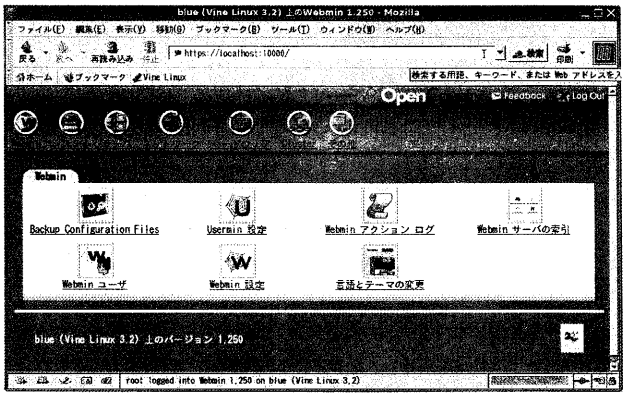

図 6 Webmin の設定画面

最初の動作画面は、図 6 のように Webmin の設定画面になり、上部にカテゴリアイコン、下部にカテゴリ内に各種アイコンが表示され、Web ブラウザによって設定を変更した場合でも、ディレクトリの構造や設定ファイルは反映されている。

図 7 中の上部のカテゴリアイコンは、Webmin は Webmin の設定、システムは Linux 各種の設定、サーバは各種サーバの設定、ネットワークはネットワークで通信するための設定、ハードウェアは Linux の起動とプリンタやハードディスクの管理などの設定、その他、Cluster の 7 つのカテゴリアイコンが表示されている。本研究では、容易に各種サーバの設定するためにサーバのカテゴリアイコンを利用した。

例として、DHCP サーバの設定を挙げている。図 8 より GUI で表示されているため、DHCP サーバでどのような設定がされているか理解しやすい。サブネットにおいて MATSUMOTO という共有ネットワークが存在し、各クライアントのホスト名とプライ

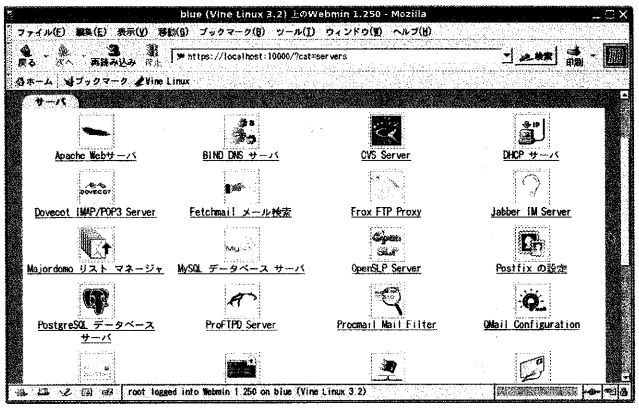

図 7　各種サーバの設定画面（Webmin）

ベート IP アドレスを設定していることが容易に理解でき、各 PC に対して詳細な設定も行える。

「サーバ管理」と「Webmin」どちらのソフトウェアもサーバに関する仕組みの知識を得ている人であれば、GUI により各種サーバの容易に設定でき、サーバの状態を確認し管理することができる。サーバ機に導入しやすさを比較すると多様な OS で利用できる面で「Webmin」が優れている。また、「サーバ管理」は、各種サーバの設定項目が少数なので、新規にサーバを導入しても GUI で管理することができなくサーバ機の拡張が難しい。しかし、項目が少数な面「サーバ管理」は、各種サーバのサービスの状態を確認でき、簡易的なグラフやログがあることでサーバを監視し問題発生時には対処しやすい。

各種サーバの GUI 設定で便利性と扱いやすさを考えるなら「サーバ管理」であり、サーバ機に拡張性を考えるなら「Webmin」を導入することがよい。

4. VPN 暗号化通信による安全な管理

近年、外出先などからインターネットを介して安全に社内へアクセスしたり、特定のビジネスパートナーに対して安全に情報提供したりするニーズが高まっている。以前は、このようなニーズに対して専用線か、Web ベースでの暗号化接続を提供する SSL（Secure Sockets Layer）やメールの暗号化という方法が主流であった。

しかし、サービスが多様化するにつれて、利用するアプリケーションを意識することなく暗号化したいというニーズが高まり、そうした環境に対して、VPN は最も有効な手段となり急速に広まってきた。このようなことから、研究室単位でも VPN を導入することで、安全にネットワークを介して GUI によるサーバの管理や監視を行うことで、複数の管理者でも理解しやすく安全な維持管理ができると考えた。

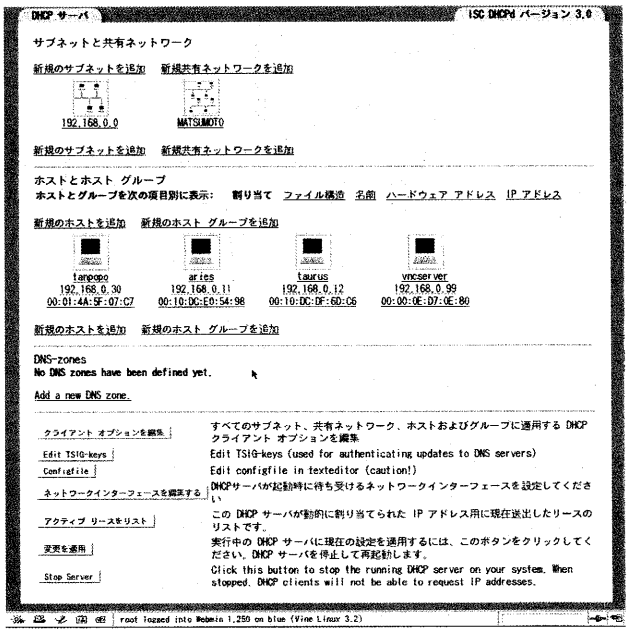

図 8　DHCP サーバの設定画面（Webmin）

4.1 VPN 暗号化通信[6]

VPN（Virtual Private Network）とは、公衆回線を介して、私的な LAN 同士および私的な LAN と端末機器が相互通信するために、仮想的に構築される私的な LAN のことである。公衆回線とは、一般電話網やインターネットに代表される公衆回線網のことで、私的な LAN とは、社内 LAN に代表される私有回線網である。

現在では、インターネットや通信事業者が用意した IP ベースの広域 IP 網を利用する VPN をまとめて IP-VPN（IP Based VPN）と呼ばれている。IP-VPN では、多くの LAN で利用されている IP の通信プロトコルをベースとした技術を使って、ユーザが保有する遠隔地の LAN 間の接続、あるいは遠隔地のコンピュータからの LAN への接続を実現している。

4.2 IP-VPN を実現するためのプロトコル

図 9 で示すように、IP-VPN の機能は、ネットワーク上に専用の通信路を確保する「トンネリング」と送信データが外部から見えないようにする「通信パケットを暗号化」で大きく分けられる。トンネリングの機能は、パケットに新たなヘッダを付加することで、カプセル化して通信を行っている。ユーザはデータを送信する側、受信する側も、トンネリングされていることを意識しないで、使用中のシステムの設定を変更することなく利用でき、プライベートアドレスやマルチプロトコル通信を実現する VPN の最も重要な機能である。通信パケットを暗号化す

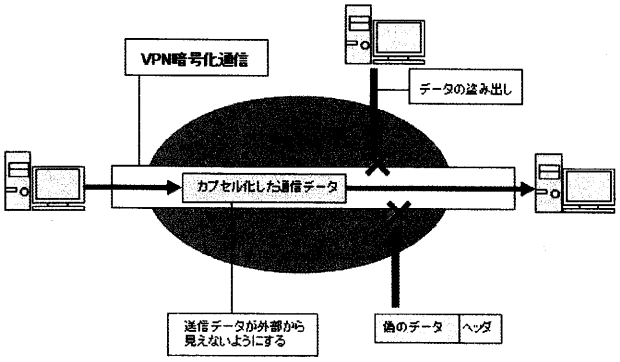

図 9 VPN 暗号化通信

る機能は、トンネリングだけでは通信しているデータの内容が見えてしまう。トンネリングされたパケットの盗聴や改ざんなどを防止するために、パケットを暗号化して伝送するための仕組みが必要になる。

IP-VPN で使用されているプロトコルは、PPTP（Point to Point Tunneling Protocol）、L2TP（Layer 2 Tunneling Protocol）、IPsec などそれぞれ独自の技術がある。本研究では、「サーバ管理」と「Webmin」のソフトウェアを利用して、VPN を容易にサーバの設定や管理が可能であるため、「L2TP」と「PPTP」のシステムを導入した。

4.3 VPN と VNC による安全なサーバ管理[7]

VNC（Virtual Network Computing）とは、リモートマシンのデスクトップをローカルマシンの画面上に GUI で遠隔操作できる。このようなことから GUI で扱えるため容易に操作し、遠隔で同時に複数のリモートマシンを操作できるメリットがある。

デメリットとしては、通信の遅延が発生すること、VNC の通信では暗号化されていないため第三者に盗聴や改ざんされる危険性があることが挙げられる。通信の遅延に関しては、近年、ネットワークの通信速度が向上している点もあり、サーバ機の設定や管理する程度なら問題なく扱える。また、VNC の通信の暗号化は、前述で説明した VPN 技術を利用することで安全な通信を確立した。

VNC を利用することでサーバの設定を変更しようとサーバ機の前で操作しなくともローカルマシン上でサーバ機を管理することができる。さらに、サーバ機が複数存在する場合でも同時にサーバ機を容易に操作し設定できるので、サーバ機群の連携が取りやすく、システムの障害が発生したときでも迅速に対応ができるようになる。

図 10 は OS が Windows XP のクライアント機により、OS が Linux 系と Mac OS X のサーバ機を操作し

図 10 VNC で複数のサーバ機を管理

サーバを管理している。VNC と VPN を利用することでサーバとクライアント間を安全な通信、GUI で容易なサーバ機の設定、ローカルマシンで同時に複数のサーバ機を管理、遠隔通信なので管理者が複数人でも同時にサーバ機を操作できる。さらに、パケットフィルタリングは VPN を許可することで、多様なアプリケーションを VPN 間で通信できるので、既存のファイアウォールの設定変更が容易である。

5. サーバ機群の統合された運用監視

サーバ機群の運用監視する目的は、システムの障害発生やその予兆をいち早く発見することで、できるだけ早く障害の復旧できることや、障害の発生を未然に防ぐことである。

5.1 監視する項目[8]

コンピュータシステムの運用監視を行うときは用いられる監視項目はさまざまなものが考えられる。しかし、管理者が少人数の場合すべてを監視することが難しく、監視項目が多数あると反対に混乱を招く場合がある。そこで、表 3 のような項目で監視を考えることとした。

Linux 系の OS の場合、表 3 中の各監視項目を CUI（Character-based User Interface）よる確認方法を利用して、実際に管理者が監視を行うと図 11 のように小さな文字が大量に出力される画面だらけになり、どのウィンドウがどのようなことを監視しているのか混乱を招く。しかもシステムの障害はいつ発生するかわからないので、この画面を常時監視するには効率的とはいない。これでは、実際にシステムを運用するには難しく、さらに監視対象の数が増加すると対処できなくなってしまう。

表 3　監視する項目

分類	監視項目
リソース監視	CPU 使用率、ディスク I/O、ディスク空き容量などを監視
ログ監視	OS や Web サーバなどミドルウェア、アプリケーションが出力するログの内容を監視
ネットワーク監視	ネットワークの死活状況や監視対象ネットワークインターフェースのトラフィックを監視
サービス監視	Web サーバや VNC サーバ、SSH デーモンなどネットワークアプリケーションが利用可能か監視
ハードウェア監視	HDD やメモリ、電源、冷却装置、温度に異常が発生していないか監視

そのため監視作業を自動化し、管理者の作業量をできるだけ減らし、見やすい GUI を利用することで、負担の軽減が必要である。たとえば、CPU 使用率やネットワークトラフィックなどはグラフで表示するようにし、監視対象で発生した障害やエラーなどをアラートやメールで管理者に通知することで、障害の履歴や対応の状況がわかり、常にリアルタイムに管理ができるようになる。監視作業の負担を軽減し、効率化するために統合された監視が必要不可欠である。本研究では、Mac OS X サーバに「サーバモニタ」、Linux 系 OS サーバに「HotSaNIC」のソフトウェアで統合した監視を行う。

5.2　統合された監視

サーバモニタは、「サーバ管理」と同様に Mac OS X 10.2 以降に導入された Mac OS X のサーバ管理用のソフトウェアである。また、Mac OS X を利用して SSH2（Secure SHell）の暗号化通信によるリモートで、Mac OS X サーバが構成するハードウェアの情報を GUI で監視することができる。さらに、監視対象のサーバ機にハードウェアの障害が発生した可能性がある場合には、設定していたユーザのメールアドレスにその状態の通知を送付する。

「サーバモニタ」のハードウェア情報の各項目を縦列で編集した画面を図 13 示す。図 11 と比較してもわかるように、各ハードウェアの詳細な情報とその状況をグラフや区別した項目で表示されているので容易に確認することができる。

これによって、リソース監視、ネットワーク監視、ハードウェア監視を GUI で統合して監視し、さらに

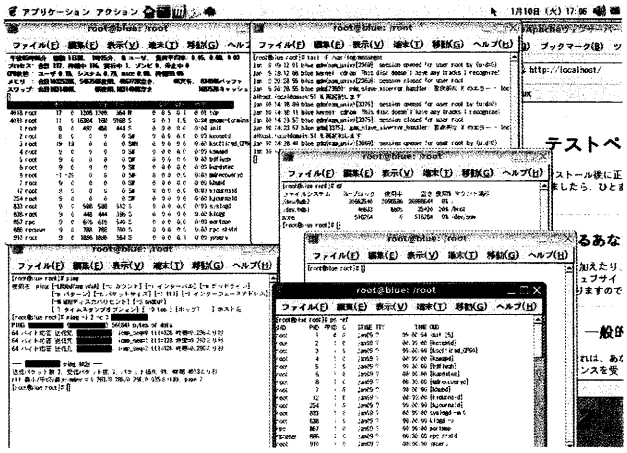

図 11　複雑な監視画面

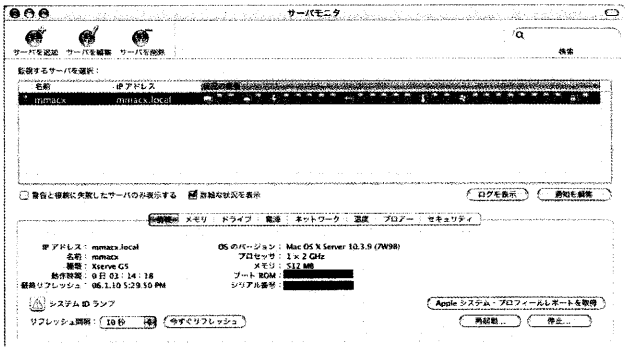

図 12　「サーバモニタ」の起動画面

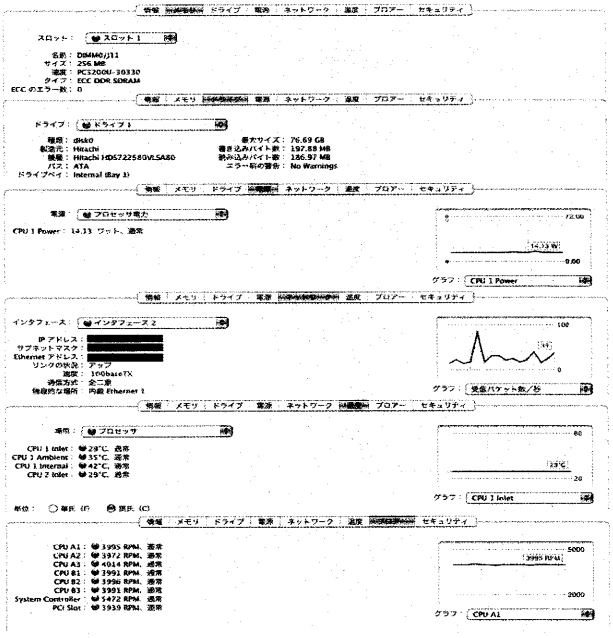

図 13　各項目を縦列に編集した画面

「サーバ管理」のソフトウェアも同時に利用することで、各種サーバのサービス監視とログ監視の監視

を行えるようになる。

しかし、欠点として OS が Mac OS X でしか GUI が利用できないため、監視できるサーバ機が限定されるので、多様な OS には利用できない。この問題を解決するために Linux、FreeBSD でも動作可能な「HotSaNIC」を Linux 系 OS サーバに導入した。

HotSaNIC (HTML overview to System and Network Information Center) は、Bernd Pissny 氏らのグループらが開発したグラフィカルなシステム統計情報を出力する Perl スクリプト群である。

HotSaNIC を導入すると、サーバ機のハードウェアとソフトウェアに関連するさまざまな情報を収集でき、他のマシンやネットワーク機器からも SNMP（Simple Network Management Protocol）を利用して情報を収集して画像グラフを作成できる。さらに、画像グラフは HTML 形式のデータとして出力されるので、ネットワークを介して監視できる特徴から導入することにした。これにより、ソース監視、ネットワーク監視、サービス監視、ハードウェア監視を GUI で統合した監視が行えるようになった。

5.3 データの保守

サーバ機を監視した場合でも、システムの障害は発生するものである。この障害によりサーバ機が起動しない状況に陥った場合、サーバ機のハードディスク内のデータを取り出せないなど問題が生じる。ハードディスク内のデータが重要であるほど常にデータの保守は必要不可欠で、クライアント機の場合でも状況は同じであるので、データを定期的にバックアップすることが重要である。

6. おわりに

本研究は、各種サーバ機群の GUI による管理・監視と第三者からの盗聴や改ざんを防ぐ VPN 暗号化通信を組み合わせて行うシステムを提案した。

従来の研究室ネットワーク環境では、独立した各種情報サービスを提供することを最優先に考えていたため、安定したサービスを提供できる状況とは必ずしもいえなかった。そこで、VPN 暗号化通信によりネットワークを介して複数の管理者でもサーバ機を安全に管理でき、サーバ機のシステムを GUI で統合して管理・監視することで、設定の誤りなど人為的な問題を防止し、管理者が常時監視しできることで安定した管理が行えた。また、システムの障害でデータが破損した場合でも、データの保守管理をしていることで、データを復旧しサービスの維持ができる。以上、大学の研究室程度の小規模 LAN 上で、

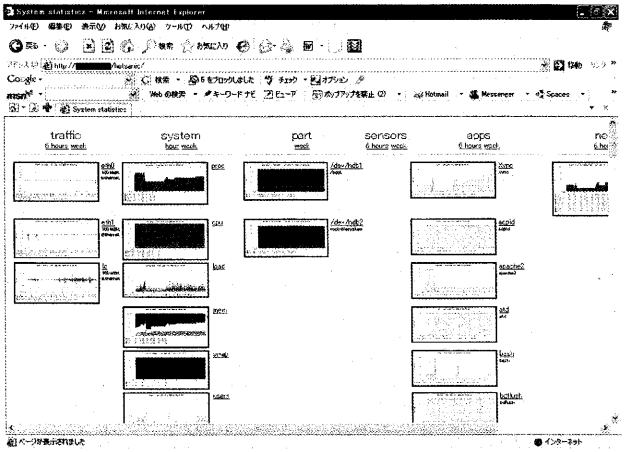

図 15 Web ブラウザによる HotSaNIC の起動画面

ネットワークサーバ機群を安全にかつ管理者に負担の少なく維持管理できる一システム提案ができたと考えられる。

現行では、監視出力データが長期間にわたって蓄積できず、過去の監視データと比較分析できない。ネットワークサーバ機群のより安全な維持管理のためには、これらの解決は重要であり、今後の課題としたい。

参考文献

[1] 財団法人インターネット協会：「インターネット白書 2005」、http://www.iajapan.org/iwp/ (2005-10 取得)、(株)インプレス

[2] 開 慶貴、帆秋 雄介、西依 祐之：「サブネット化によるトラフィック低減化に関する研究」、九州産業大学工学部平成 15 年度卒業論文(2004-4)

[3] 大島 義智、松本 勝哉：「研究室内のネットワーク環境と PC の管理」、COMMON Vol.24 pp.69-78 (2004)、九州産業大学総合情報基盤センター

[4] 藤枝 直記：「無線 LAN を用いた研究室内ネットワークの構築に関する研究」、九州産業大学大学院工学研究科電気工学専攻平成 16 年度修士論文 (2005-4)

[5] 松本 浩明、中村 新一郎：「よくわかるネットワークと最新サーバの基本と仕組み」、pp.99-138、(株)秀和システム(2001-1-15)

[6] 金城 俊哉：「よくわかる最新 IP-VPN の基本と仕組み」、pp.11-167、(株)秀和システム(2002-2-3)

[7] 大島 義智、川口高弘、武久正幸：「遠隔指導のための VNC と支援ツール」、九州産業大学工学部平成 15 年度卒業論文(2004-4)

[8] 片岡 巌：「Linux ソフトウェアアンテナ」、pp.120-128、(株)技術評論社(2005-10-25)