2007－DSM－47 (5)
2007／9／21

PCクラスタによる認証スイッチの認証性能評価システム

近堂 徹　田島 浩一　岸場 清悟　西村 浩二　相原 玲二

広島大学情報メディア教育研究センター
〒739-8511 広島県東広島市鏡山1丁目4番2号

あらまし　近年，企業や大学などの情報ネットワーク利用において，一時利用者のみならず定常利用者を含む全利用者に対する利用者認証への要求が高まってきている．これらの運用においては，利用環境や運用ポリシーに応じて様々な性能要求条件が存在するため，目的に見合う性能を予め見極められることが必要である．本稿では，PC端末をクラスタ化することで多様なアクセスパターンを実現する検証環境の構築と，それを用いた認証スイッチの認証性能評価について報告する．

キーワード　PCクラスタ，ネットワーク認証スイッチ，利用者認証，性能評価

A Performance Evaluation System for the Network Authentication Switch using a PC Cluster

Tohru KONDO　Koichi TASHIMA　Seigo KISHIBA　Kouji NISHIMURA　Reiji AIBARA

Information Media Center, Hiroshima University
1-4-2, Kagamiyama, Higashi Hiroshima, Hiroshima 739-8511, JAPAN

Abstract　Network authentication is widely used in campus network to improve network security. Because there are various requirements for user environments and management policies, it is nessesary to test the performance previously for stable operation. In this paper, we show a performance evaluation system which can be generated various access patterns by a pc cluster, and report performance evaluation of the network authentication switch.

Key words　PC Cluster, Network Authentication Switch, User Authentication, Performance Evaluation

1　はじめに

PC端末の小型化・高性能化やネットワークの広帯域化に伴い，情報コンセントや無線アクセスポイントによるネットワーク接続サービスが広く提供されるようになってきた．大学などの教育機関においても，このようなサービスが導入されつつあり，大学構成員が自身の端末を持ち込んでネットワークを利用する場面も少なくない．持込み端末を組織内ネットワークで利用させる場合，ネットワークの入り口でセキュリティを確保することが必要となる．ネットワーク利用の制限や利用の記録保持の観点からも，固有情報を用いた利用者認証が行われるのが一般的となっている．

さらに上述の一時的な利用者だけでなく，大学の研究室や共同利用施設（演習用端末室）などでの日常的なネットワーク利用者に対する認証への要求も高まってきている．このようにネットワーク利用者認証をキャンパスワイドに展開しようとする場合，認証対象となる利用者や端末は飛躍的に増大するため，認証処理性能に対する要求条件も大きく変わることが予想される．継続的な認証要求や数十台・数百台単位での一斉認証要求など，認証要求も多様化するため，実利用に即した検証環境で評価することで，その性能を予め見極めることが必要である．

そこで本稿では，上述に対する解決策として，PC端末をクラスタ化することでネットワーク機器等の性能検証を実現する評価システムについて示し，その利用例として，ネットワーク利用者認証装置の性能評価について報告する．

2 ネットワーク機器の評価について

ここでは，ネットワーク機器の検証手法についてまとめ，本稿が対象とするネットワーク認証スイッチの概要とその評価手法について述べる．

2.1 ネットワーク機器の検証環境

何らかのネットワーク機器を実環境で運用しようとする場合，目的や要求条件に見合う性能を保持しているかどうかを予め検証できることが望ましい．これまでにも様々な検証手法が確立され，既に実用化されているものも多く存在する．例えば，Smartbit[1] や Iperf[2] に代表されるようなトラフィックジェネレータが存在する．これらは高精度のトラフィックを発生させることで対象機器のスループット計測を行うことが可能だが，特定のトラフィックしか取り扱うことができず適用範囲も限定される．

また実インターネット環境を模倣するために，StarBED を用いたサーバ負荷試験のフレームワークが提案されている [3]．これは，700 台規模の高性能サーバ群を利用し，多様なアクセスパターンを再現することでサーバ負荷の検証環境も実現するものである．StarBED は検証環境として有効的であるが，このような設備を自環境に構築するのは非常に困難である．

本稿では，大学等の教育研究機関で整備されている教育用端末や遊休資源を利活用することを念頭に置き，PC クラスタを構築することで，上述のようなネットワーク機器の検証環境を実現するためのシステムについて考える．

2.2 ネットワーク認証スイッチの評価要素について

ネットワーク利用者認証システムは，UNIX 系システムに認証機能を備えたゲートウェイ型認証システム [4] や独自認証認証を実装したスイッチを利用するシステム [5] などが提案，実運用されている．これらの認証方式としては，Web ブラウザによる認証や MAC アドレスによる認証，IEEE802.1x 認証の 3 つが一般的となっている．

これらはそれぞれにメリット・デメリットがあり，運用規模や運用方針に応じて使い分けを考える必要があるといえる．キャンパスネットワークでの利用を考えると，異なる OS が混在する環境においても同一のセキュリティプラットフォームを導入できる必要があり，また，既に点在しているスイッチ等 (いわゆる島ハブ) を含む既存ネットワークシステムとの親和性などを考慮する必要もある．このような場合，IEEE802.1x 認証機能を提供することは運用面でも大きな負担となるため，利用者の環境を選ばない Web ブラウザを利用した利用者認証への需要が高まる．

しかしながら，このようなネットワーク認証機器は http/https プロトコルの差異や SSL 認証鍵の長さ，同時接続セッション数によって，その性能が大きく変動することが予想される．本稿では，Web ブラウザを利用した http/https プロトコルによる認証方式に焦点を絞った性能評価について述べる．

3 PC クラスタによる認証スイッチ評価システム

本章では，構築した PC クラスタを用いた認証スイッチ評価システムの概要について述べた後，その基本的性能について示す．

3.1 システム構成

図 1 に今回構築したシステムの構成，表 1 に使用した機器のスペックを示す．本システムはトラフィックを発生させるクライアントノード群（以下，実行ノードとよぶ）と，それを管理するサーバ群で構成される．サーバ群は，実行ノードのディスクイメージを管理するディスク管理サーバと NFS サーバ，クラスタを制御するポータルサーバからなる．今回のシステムでは実行ノードは 34 台でクラスタを構成している．各端末のインターコネクトには 1000base-T を利用し，スイッチ間は 1000base-T を 4 回線利用して 4Gbps にて接続している．これにより，http や ftp のような TCP トラフィックや UDP を利用したストリームトラフィックなどの多様なトラフィックパターンを模倣するのに効果的な構成としている．

実行ノードは管理コストを考慮しディスクレス OS で構成している．ノードのブート時に共通のカーネルイメージを取得して起動し，ホームディレクトリやアプリケーションディレクトリは NFS サーバをマウントするように設定している．これにより，各実行ノードの設定情報や処理結果は NFS サーバに集約され一元的に管理できる．

なお，今回はディスクレスブート環境としてミントウェーブ社の VID システム [6] を用いたが，Debian/GNU Linux3.1r4 をベースに PXE ブートを用いて構築した Linux ディスクレス環境でも同様の機能を有するシステムが実現できることを確認している．

このように，本システムの利点は各実行ノードがディスクレス環境で動作する点にある．これによって，端末のハードディスク領域を変更することなく活用することができるため，大学等に存在する遊休資源を用いることで同様のシステムを構築することが可能になる．

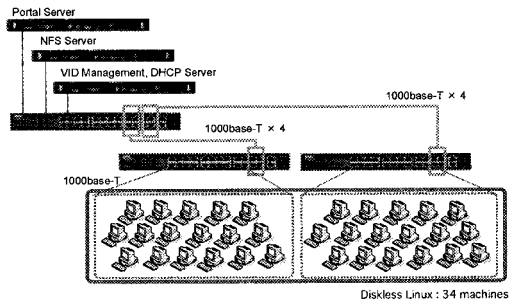

図 1: 基本システム構成

表 1: システム使用機器

	管理サーバ (VID, NFS, Portal)	実行ノード
CPU	P4-3.06GHz	P4-2.66GHz
memory	1024Mbyte	
NIC	1000base-T	
OS	RedHat Linux 9	
Kernel	2.4.20-20.9	

3.2 ミドルウェア構成

次にミドルウェア構成について示す．本システムでは，PC のクラスタリングツールとして SCore を利用している．SCore[7] は PC クラスタコンソーシアム（旧新情報処理開発機構）で開発された統合型のクラスタリングツールであり，ノード間通信のための独自軽量プロトコルや，効率的なジョブスケジューリング機能，また，ノードの冗長機能等を実装しており，運用面も含めて高性能で高機能な PC クラスタを構築することができる．また台数の増加に対しても，管理コストを損なうことなく運用することもできる．

本システムでは高度な機能は利用することはないが，管理運用の効率化を図るために SCore を利用した．これにより，ポータルサーバから一元的に各クライアントの挙動を制御することができ，さらに台数の増加に対するスケーラビリティも容易に確保することができる．ポータルと実行ノード間の通信には rsh を利用し，複数ノードに対して rsh を実行するために SCore パッケージに同梱されている rsh-all コマンドを利用する．

評価で利用するアプリケーションプロトコルは，Linux で動作可能なアプリケーションであれば容易にインストールすることができる．例えば，http/https や ftp トラフィックであれば wget，UDP トラフィックであれば Iperf を用いることができ，さらに独自に開発したプロトコル等も利用することが可能である．インストールはマスタとなる NFS サーバ上の領域にインストールだけで全実行ノードで利用可能となるため，導入に対するコストも低いと考えられる．

3.3 システムの実行処理手順

図 2 に本システムの実行処理フローを示す．利用者はフロントエンドとなるポータルサーバ上でのみ一連の操作を行う．ここでは，ある Web サーバに対して http による同時アクセスを実現する場合を例に説明する．

まず始めにユーザは，各実行ノードがマウントしているディレクトリに実行ノードが処理する内容を記述したスクリプトファイルを保存する．スクリプトファイルの書式は以下に示すように、通常の UNIX コマンドを sh スクリプトにて記述する．この例では，あるホストに対して https を用いたアクセスを実施した時の応答時間を出力させる処理を表している．

```
#!/bin/sh
hostname='hostname';
logdir="/home/test/result";
(time wget -q -O $logdir/wgetlog-$hostname.$$ \
https://192.168.0.1/cgi-bin/index.cgi) 1> \
$logdirlog-$hostname.$$ 2>&1
```

次に，各実行ノードの挙動をポータルサーバ上で制御する．ポータルサーバ上では，スクリプトファイルで記述した処理をどのノードで起動させるかを指定する．この方法として，rsh-all コマンドにより対象とする実行ノードを直接指定して実行させる方法のほか，引数で与えるノード数から自動的に実行ノードリストを生成し rsh-all コマンドを実行することができる．つまり 1 台から 34 台までの任意の数で実行ノードを指定することができる．同じ処理を台数を変えて実行する場合は，ループ処理にてノード数を変更して実行すればよい．

このように，実行ノード処理の記述とポータルサーバ上での操作の 2 ステップの操作を経て，本システムを利用した評価実験を行うことができる．コマンドは通常の UNIX コマンドをそのまま利用することができるため，UNIX 経験者であれば操作性を損なうことなく本システムを利用することができる．しかしながら，一般利用者に対しては現状では不十分であると考えられ，対話型インタフェースやシナリオを記述したテンプレート読み込みなど，よりユーザ利便性を考慮したフロントエンドの実装は今後の課題である．

3.4 基本性能実験

本節では，構築したシステムの基本性能として，実行ノードからの一斉同時アクセスに対する時間精度につい

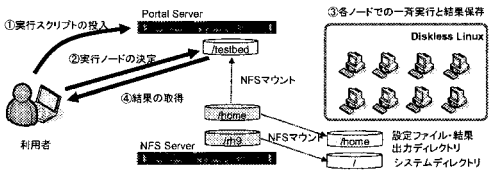

図 2: 実行処理フロー

て述べる．実験では，図 1 に示す環境で LAN スイッチとサーバを接続し，ポータル上での操作により，各クライアントから対象サーバへの一斉同時 http アクセスを実行させる．この時，サーバ側で TCP SYN パケットをキャプチャすることで，同時一斉アクセスに対する時間精度を求める．

セッション数の増加に対する全アクセス時間の変化を実験結果を図 3 に示す．本結果は各測定点において，3 回測定した平均値を代表値としている．本結果から，セッション数の増加に従いアクセス時間も増加しているが，340 セッション（各ホスト 10 セッション× 34 台）の場合でも 1 秒以下で全てのアクセスを生成できていることが分かる．

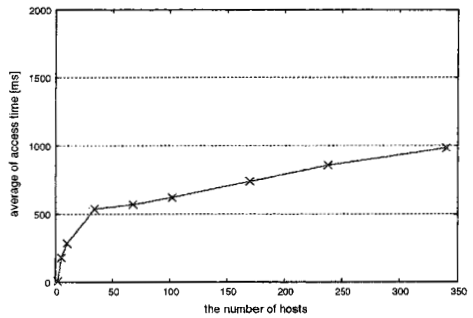

図 3: セッション数に対する http アクセス生成時間

4 認証スイッチの性能評価

認証スイッチの認証性能は，http や https プロトコルの違いや SSL 認証鍵の長さ，同時接続セッション数によって変動することが予想される．本章では構築したシステムを用いてこの傾向を明らかにすると共に，認証スイッチの実用性について検証する．

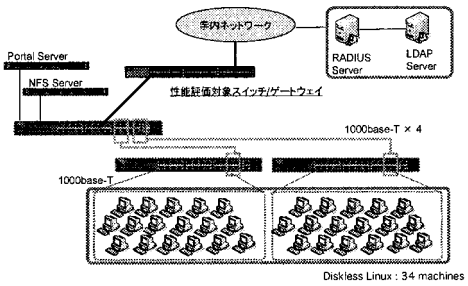

図 4: 実験構成図

4.1 実験内容

実験構成図を図 4 に示す．本稿では評価対象の認証装置として，認証ゲートウェイ型にネットスプリングの Micro FEREC（以下 FEREC），認証スイッチ型に日立電線の Apresia 2124GT-SS（以下 Apresia）を用いた．それぞれの仕様を表 2 に示す[1]．認証データについては，アカウント情報を学内に設置してある LDAP サーバに 100 名分登録した．認証装置からは RADIUS プロトコルで RADIUS サーバに認証問い合わせを行い，LDAP 内の登録情報との照合により認証処理が行われる．

実験では 2 つの機器について

- 同時セッション数および SSL 認証鍵の長さに対する認証可能セッション数
- 同時セッション数および SSL 認証鍵の長さに対する認証時間

について調べることで，同時接続に対する認証スイッチの性能評価を行った．ここで認証可能セッション数とは認証処理に成功したセッション数，認証時間は成功したセッションに関する認証処理時間と定義する．

表 2: 実験機器のスペック

サーバ	ハードスペック / OS / ソフトウェア
LDAP サーバ	Ultra Sparc IIIi 750MHz 512MB / Solaris8 / iPlanet (LDAP)
RADIUS サーバ	Ultra Sparc IIi 440MHz 512MB / Solaris 10 / FreeRADIUS, OpenLDAP
認証装置	ファームウェアバージョン
Apresia 2124GT-SS	6.15.02
micro FEREC	1.5

[1] この仕様は本実験に用いた機器のものであり，現在は変更されている可能性がある点に注意が必要である

4.2 実験結果と考察

4.2.1 認証可能セッション数に関する実験結果

図 5 に Apresia，図 6 に FEREC の認証可能セッション数に関する実験結果を示す．横軸は生成セッション数で，縦軸が成功セッション数を表している．各測定点において，3 回測定した平均値を代表値としている．

この結果より，15 台程度までは同じような挙動であるのに対し，それ以上になると各々で異なる特性を示していることが分かる．Apresia の場合は，SSL 暗号化通信を行うことで極端な性能低下が見られ，鍵長が長くなることでより性能が低下する点が特徴的となっている．SSL 通信を利用しない場合は 80 セッション程度まで性能を維持できていることから，SSL 通信を利用した同時接続の処理負荷がボトルネックになっていると考えることができる．一方，FEREC の場合は，SSL 通信の有無に関わらず，セッション数の増加に従い徐々に性能が低下しているのが分かる．このことから，SSL 暗号化処理以外の要因でボトルネックが生じていることが分かる．考えられる要因としては，Web サーバの性能などが挙げられる．

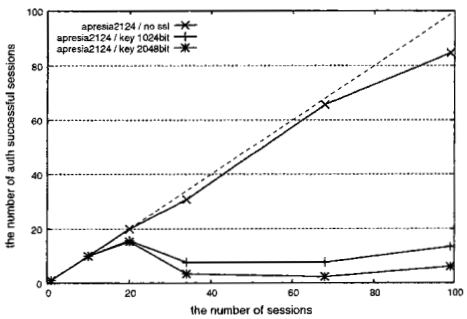

図 5: 認証可能セッション数 (Apresia の場合)

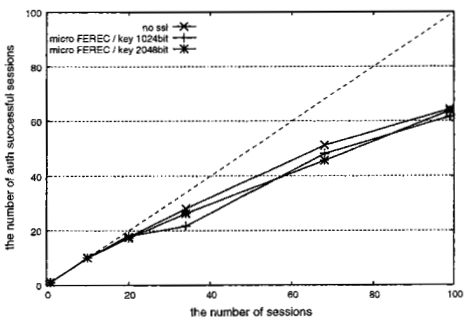

図 6: 認証可能セッション数 (FEREC の場合)

4.2.2 認証時間に関する実験結果

次に，認証時間に関する実験結果について示す．図 7 - 8 は Apresia の測定結果，図 9 - 10 は FEREC の測定結果であり，それぞれ http 接続および https (鍵長 1024 ビット) の結果を示している．測定では，認証成功した全セッションの最小/平均/最大認証時間を求め，各測定点において 3 回測定した平均値を代表値としている．例えば，図 7 の横軸 99 の場合は，99 セッションの同時接続に対する，認証可能セッション数 83 (図 5) の認証時間の最小値/平均値/最大値が 5 秒/29 秒/56 秒であることを示している．

これらの結果より，Apresia，FEREC ともに同時認証セッション数の増加および SSL 通信の利用によって認証時間が増加していることが分かる．特に Apresia の場合は，SSL 利用による性能の変動が顕著に表れている．

同時接続に対する認証可能セッション数と認証時間の測定結果より認証機器の特性について考察する．Apresia2124 は，SSL を利用した場合は認証可能セッション数も少なく認証時間も増加する傾向にあることが分かる．このことから，暗号化処理による負荷が機器性能全体を低下させ，新規セッションに対する処理も困難になっていると考えることができる．一方 FEREC の場合は，SSL を利用することでの認証成功セッション数の変動はほとんどなかったが，認証時間は約 2 倍増加していることが分かる．これは，認証セッションの受付バッファは十分に確保されているが SSL 暗号化処理に時間がかかったために，このような結果になったと考えられる．

5 本評価システムの応用について

本稿では，ネットワーク認証スイッチに焦点を当てて，評価システムの構築と実際の検証結果について示した．本システムの基本動作としては，各実行ノードから様々なアクセスパターンやトラフィックを生成することが可能である．よって，帯域の制限はあるものの，利用方法によっては様々な検証実験に適用することが可能になると考えている．例えば，ファイアウォールのセッション処理に対する性能評価や CGI プログラムの性能評価などにも活用できると考えている．

本評価システムは，各々の組織に存在する遊休資源を活用し環境を構築することを前提に考えている．各組織でこのような検証環境が構築できることで，既存ネットワークに関する評価や，新しいサービスを導入する際の指標評価にも活用できる．本稿で示した認証スイッチの性能評価のような，広帯域のトラフィックを必要としない検証ならば，比較的容易に PC クラスタを構成する端末を用意することができる．

また構築にあたっては，既存環境に変更を加えずに実現できる必要があるため，本稿ではディスクレスブート

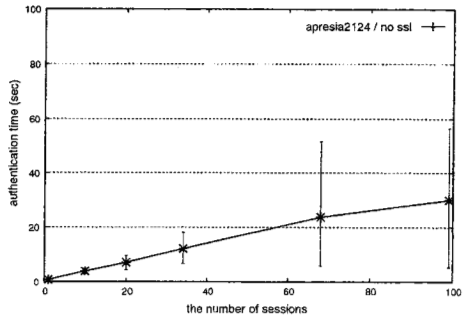

図 7: http による認証時間 (Apresia の場合)

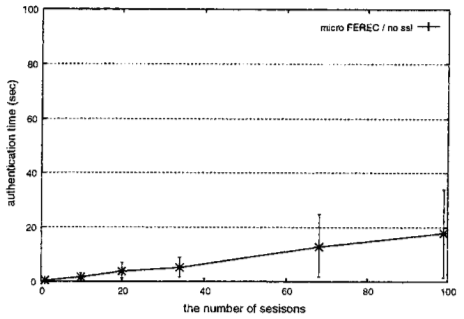

図 9: http による認証時間 (FEREC の場合)

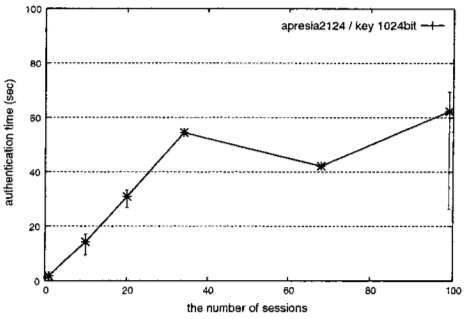

図 8: https (1024bit) による認証時間 (Apresia の場合)

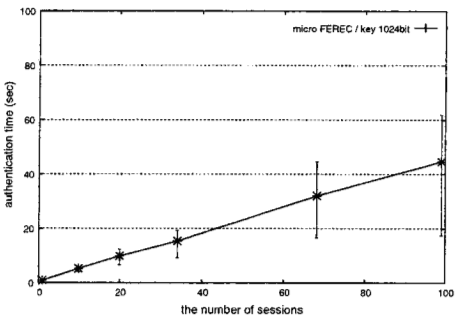

図 10: https (1024bit) による認証時間 (FEREC の場合)

環境を構築する手法を採用した．今後は，ネットワークブートに対応していない端末等の利用も考慮し，1CD Linux を使ったシステム構築なども考えていく必要がある．また，より汎用的な環境として利用するために，用途に応じた機能の提供行うユーザインタフェースの提供やシステムの改良についても今後の課題である．

6 まとめ

本稿では，PC 端末をクラスタ化することで多様なアクセスパターンを実現するネットワーク機器の評価システムについて示し，これを用いたネットワーク認証スイッチの性能評価について報告した．ディスクレス技術を用いで PC 端末をクラスタ化することで，様々な実運用における要求条件を擬似的に作り出すことが可能になり，多人数を動員した動作検証や負荷テストに取って代わることができ，定量的かつ客観的な評価が容易となった．

本大学では，大学の教育用端末群を活用した PC クラスタ/グリッドサービス [8] も行っており，多数のノードを統一的に管理運用する基盤が整っている．本システムで用いた端末管理手法もこれをベースに考えたものである．今後は大学でサービスしている PC クラスタ/グリッド基盤を利用した検証システムの展開も考えたい．また，本システムが提供するサーバ機能の 1CD Linux 化や操作性の向上など，ユーザが容易に利用できるようにシステムへの改良も行っていく必要があると考えている．

参考文献

[1] Spirent Communications, Smartbit, *http://www.spirentcom.com*
[2] A. Tirumala, F. Qin, J. Dugan, J. Ferguson, and L. Gibbs, "Iperf: The TCP/UDP bandwidth measurement tool", *http://dast.nlanr.net/Projects/Iperf/*, 1999.
[3] 野中 雄太, 知念 賢一, 宇多 仁, 宮地 利幸, 篠田 陽一, "StarBED を用いたサーバ負荷試験の実現,"DICOMO 2007 シンポジウム論文集, pp.199–204, 2007.
[4] (株) ネットスプリング, FEREC, *http://www.ferec.jp.*
[5] 日立電線株式会社, Apresia, *http://www.apresia.jp.*
[6] ミントウェーブ社, VID システム, *http://www.mintwave.co.jp*
[7] PC Cluster Consortium, SCore, *http://www.pccluster.org*
[8] 近堂徹:"教育用端末を利用した HPC クラスタシステムの省電力化手法とその評価", 情報処理学会 マルチメディア・分散・協調とモバイル (DICOMO) シンポジウム 2007 論文集, pp.1059–1064, Jul.5 (2007)