横浜国立大学「認証ネットワーク」：運用管理方法の改良

Authentication Network in Yokohama National University : Improvement for Operation and Management method

志村　俊也†，　徐　浩源†
Toshiya Shimura†，　Haoyuan Xu†

tshimura@ynu.ac.jp,　haoyuan@ynu.ac.jp

†横浜国立大学総合情報処理センター
240-8501　横浜市保土ヶ谷区常盤台 79-5

† Information Processing Center, Yokohama National University
Tokiwadai 79-5,　Hodogaya-ku Yokohama,　240-8501

概要

2003 年 4 月に運用を開始した本学の「認証ネットワーク」について、これまでに行ってきた「運用管理面での改良事項」および「認証スイッチを用いた新しい形の認証方法」について報告する。

キーワード

認証ネットワーク, 運用管理, IP アドレス指定接続

1. はじめに

本学は日立電線製レイヤ 2 認証スイッチ(NASW)を用いた認証ネットワークの構築を全学的に展開している(2006 年 8 月現在、28 建物 57 台)。導入に至った経緯、構築当初の様子・システム構成・問題点は、2003 年度情報処理研究会[1]で報告している。本報告では、2003 年 4 月の運用開始から現在までの約 3 年半の間に行ってきた運用管理面での改良事項全般について説明する。

2.　認証サーバとの接続方法の改良の推移

2.1.　2003 年 4 月- 2004 年 3 月

構築当初(2003 年 4 月～2004 年 3 月)における構成を図-1 に示す。NIS で認証データの管理を行っている認証サーバ(NIS master)と、NASW からの RADIUS 認証要求を受け、NIS client として NIS master に認証要求を行う RADIUS サーバで構成されている。認証サーバの仕様は、ハードウェア：Sun Microsystems / Enterprise 10000 (Star Fire)，OS ： Solaris 8 であり、全学メールサーバ、アプリケーションサーバを兼ねた汎用レンタルサーバである。RADIUS サーバの仕様は、ハードウェア ： DELL /

PowerEdge350 [CPU Pentium III 1GHz, RAM 512MB], OS：Redhat Linux 7.3, RADIUS サーバソフトウェア：Cistron RADIUS Server (フリーソフトウェア) である。

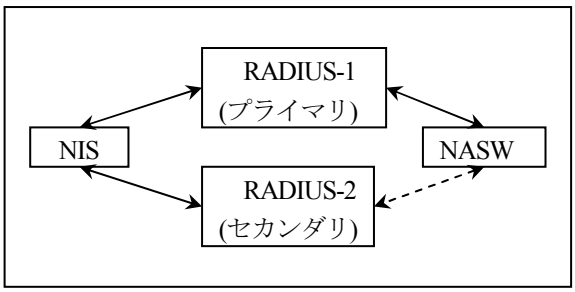

図-1. 2003 年 4 月-2004 年 3 月の間における、NIS サーバ、RADIUS サーバ、認証スイッチ間の連携図。実線が active 系、点線が standby 系である。

2.2. 2004 年 4 月-2006 年 2 月

認証ネットワークの運用開始後まもなくして、認証データを保有する第 2 認証サーバを新規に構築し、RADIUS サーバは、認証サーバではなく第 2 認証サーバに認証の問い合わせを行わせた方が運用上好ましいということになった。NIS master⇔第 2 認証サーバ⇔RADIUS サーバ間の認証データの同期方法に関しては、NIS master は汎用サーバであるため、極力設定変更作業は行なうべきではないとの判断から、NIS master⇔第 2 認証サーバ間の同期はこれまでどおり NIS で行うこととし、第 2 認証サーバ⇔RADIUS サーバにおける同期は、拡張性・柔軟性の面で NIS より優れている LDAP を採用することにした。

第 2 認証サーバ(LDAP サーバ)導入後の認証ネットワークの構成を図-2 に示す。LDAP サーバの仕様は、ハードウェア： Sun Microsystems / Sun Fire V240 [CPU UltraSPARC IIIi 1GHz, RAM 1GB] 、OS ： Solaris 9、 ディレクトリサービス ： Sun One Directory Server 5.2 (OS 標準装備)であり、マスターとレプリカの冗長構成である。NIS master⇔LDAP サーバ⇔RADIUS サーバ間の認証データの同期の具体的な方法は以下の通りである。

① LDAP マスターが 1 時間に一度、NIS client として ypcat を実行して、NIS master の全アカウント情報を取得する。
② 前回(1 時間前)取得したアカウント情報と比較して、新規登録、更新、削除の３つを抽出し、それぞれの差分を LDIF 形式に変換した上で、新規・更新に対しては ldapmodify を、削除に関しては ldapdelete を実行し、ディレクトリサービスに反映させる。
③ レプリケーション機能を用いて LDAP マスター⇔LDAP レプリカ間で認証データの複製を行う。
④ LDAP マスターが障害等で停止した場合は、LDAP レプリカの設定を手動で変更し、LDAP マスターに昇格させる。
⑤ RADIUS サーバは、LDAP client として、LDAP サーバに認証要求を行う。

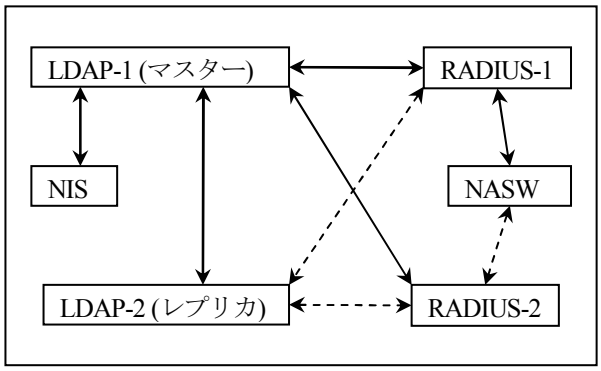

図-2. 2004 年 4 月-2006 年 2 月の間における、NIS サーバ、LDAP サーバ、RADIUS サーバ、認証スイッチ間の連携図。実線が active 系、点線が standby 系である。

RADIUS サーバを NIS client から LDAP client へ変更する際、2 台の LDAP サーバを登録可能な LDAP client 機能を備えた Linux 上で動く Radius サーバソフトウェアを見つけられなかったため、OS を Windows2000 サーバへ、RADIUS サーバソフトウェアを Soliton RADDBY 2.6 (LDAP 版) に変更した。

2.3. 2006 年 3 月- 現在

2006 年 3 月、NIS master のレンタル終了にともない、認証サーバを更新した。更新後の構成を図-3 に示す。

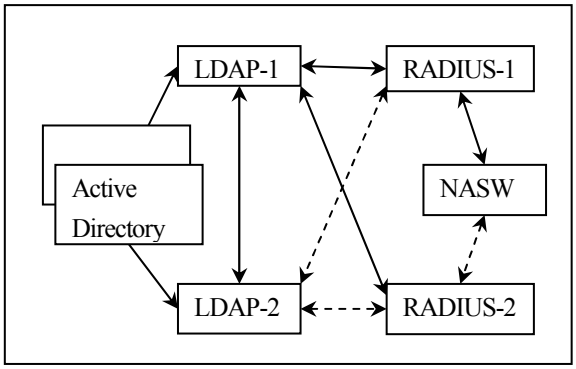

図-3. 2006 年 3 月以降の認証サーバ(Active Directory)、LDAP サーバ、RADIUS サーバ、認証スイッチ間の連携。

新認証サーバは認証専用機であり、その仕様は、ハードウェア：富士通 / PRIMERGY TX200FT S2 [CPU Xeon 3.2GHz×2(dual processor), RAM 4GB]、OS：Windows

Server 2003 Enterprise Edition 、認証データは Active Directory＋富士通製「ICAssist」で管理されている。本認証サーバは、フォルトトレラントシステムであり 2 台で一式の冗長構成となっている。認証データ同期は、Active Directory 上で 認証データの更新が行われると ICAssist がそれを検知し、リアルタイムで 2 台の LDAP サーバに反映させる仕組みとなっている。

3. その他、運用面での改良

3.1. 接続端末管理の廃止

認証ネットワークの運用に際して、認証ネットワークから離脱した利用者の登録情報を NASW 上から速やかに削除するという目的から、NASW の標準装備である「接続端末確認 ：NASW から接続登録端末に対して 1 分に 1 回の割合で ping polling を行い、5 分間に一度も応答がない端末を強制ログアウト」を使用して、正式なログアウト手続きを実行せずにネットワークから離脱した端末の認証登録を自動的に削除するということを実施していた。

この接続端末管理で問題となったのは、セキュリティ対策ソフト(トレンドマイクロ社のウィルスバスター等)のパーソナルファイアウォール機能や、Windows XP–SP2 の Windows ファイアウォール機能が標準で ping をブロックしてしまうため、利用者側でブロック解除の設定を行なわない限り、接続が 5 分で切断されてしまうという点である。当然のことながら利用者にとっては大変不便なシステムであったが、当センターでは利用者からの不満の声に耳を貸すことなくこの接続端末確認を続けていた。そういった状況の中、2006 年 4 月に総合情報処理センター長が交代し、早々に「セキュリティも大切だが、使い勝手とのバランスが重要である。接続端末管理が本当に必要かどうかきちんと再度検討してほしい」との指示を受けた。当センター内で真剣に検討した結果「接続端末管理はあまり意味がない」という結論となり、2006 年 5 月に「接続端末管理」を廃止した。

3.2. NASW 配下に NAT 機器を接続した場合に発生するセキュリティホールの解決

初期の NASW には、「認証ポートにブロードバンドルータ等の NAT 機器を接続した場合、プライベートネットワーク側の任意の一人が認証許可されると、その後は全利用者が認証なしに接続可能となる」というセキュリティホールが存在した。これでは認証ネットワーク自体が成り立たなくなるので、NAT 機器を経由する接続をすべて拒否する仕様に変更をするよう日立電線に申し入れた。日立電線は、端末が発信するパケットの TTL 値は、NAT 機器を通過後 1 だけ減少することに注目し、TTL 値がデフォルト値以外の値を持つパケットを NASW で全て破棄する設定ができるようにファームウェアを改良することでこの問題を解決した。端末側が発信するパケットの TTL のデフォルト値は OS・アプリケーションソフトウェアによって異なるが、調査の結果、64, 128, 255 以外のデフォルト値は見つからなかったため、この 3 つの TTL 値をもつパケットのみ通信を許可することにより NAT 機器を経由した接続の遮断を実現している。

3.3. 接続ログ管理・解析システム

認証ネットワークの構築当初、接続認証のログは全て RADIUS サーバ上に保管していた(RADIUS サーバが Syslog サーバを兼ねていた)。ログ解析を行う際は、RADIUS サーバにリモートログインし、収集されているログを検索・解析していたのだが、膨大なログを手動で解析するのはあまりに効率が悪いので、認証ネットワーク専用のログ管理･解析システムを 2004 年 3 月に構築した。ログ管理・解析システムは、ダブルマスターの冗長構成であり、仕様は、ハードウェア : 富士通 / PRIMERGY RX300 (CPU Xeon2.4GHz, RAM 1GB, HD 293GB), OS : Redhat Linux 9 (その後 Fedora Core 5 に変更)、ログ管理ソフトウェア：日立電線「NALogManager」(本学用にカスタマイズしたもの) である。

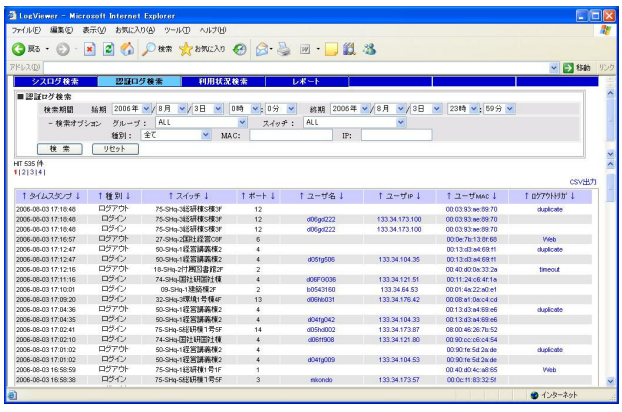

図-4　ログ解析画面の一例

このシステムを使用した接続ログ検索画面の一部を図-4 に示す。解析インターフェースがウェブブラウザであるため、作業効率が劇的に向上した。認証スイッチ単位、認証スイッチのグループ単位、クライアントの IP アドレス、MAC アドレス、接続ユーザ名、期間指定等、様々な項目で接続状況を解析することができ、検索したデータを CSV 形式でダウンロードすることも可能である。また、認証ネットワークの接続障害調査ツールとしても役立っている。さらに、このシステムは接続認証ログだけでなく、NASW の動作に関する通常の Syslog も受信する

ので、機器の状態変化、例えば、各スイッチの各ポートの LINK 状態の変化、NTP サーバとの同期状態、プライマリ RADIUS サーバへの接続状態など機器動作確認ツールとしても活用している。

3.4. ウェブアクセスログの収集

本学が認証ネットワークを導入すると同時に、ウェブアクセス関連の問題(学外掲示板サイトへの学内からの不正投稿等)が発生した際に追跡調査ができるよう、認証ネットワーク利用者のウェブアクセス記録の強制収集を開始した。方法としては、基幹 L3 スイッチで認証サブネットから他ネットワークへの 80 番ポートへのアクセスを遮断して、利用者自身がウェブブラウザに PROXY サーバの設定をしなければウェブアクセスができないという利用者側に不便を強いるものであった。この不便さを解消するため、2006 年 3 月に基幹系ファイアウォール(FW)の更新に合わせて、ウェブアクセスログの収集を PROXY サーバから FW で行うこととした。これにより、利用者側が PROXY サーバの設定を行なわなくても済むようになり、認証ネットワークの利用環境がさらに改善された。

新 FW の機種は、Nokia / IPO380 (スループット 1.5Gbps, RAM 1GB)、フィルタリングソフトは Check Point Software Technologies 製 Firewall-1 であり、基幹ネットワークに Active-Active の冗長化構成で設置されている.

取得されるウェブアクセスログは、FW 本体に保管するのではなく、syslog 機能を使って FW 管理専用サーバに送信しているため、FW にかかる負荷はほとんどない(図-5)。取得されるウェブアクセスログの量は、一日当たり約 500MB(平日)で、土日祝日はその約 1/3 であり、ログ解析は、Check Point Software Technologies 製 SmartView Tracker で行なっている。

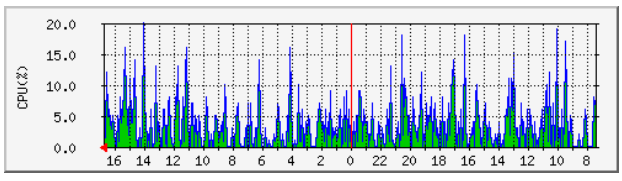

図-5　基幹ネットワークに接続されている 2 台の FW の内の 1 台のロードアベレージ。

4. IP アドレス指定接続 - 新しい認証方式

認証ネットワーク配下において、端末に対する IP アドレス割当ては、DHCP による自動割当てが基本である。接続時間に関しては、一度の認証で可能な接続時間を 12 時間に制限してある。そのため、固定 IP アドレスで常時接続が必要なサーバ機器を認証ネットワーク配下に収容するのは原理的に無理である。従って、固定 IP アドレスで常時接続が必要とされる機器は非認証ネットワークに収容することになるのだが、そういった機器に対しても何らかの形で認証、あるいは同様な接続管理ができないものか当センターで考えた結果、NASW の Packet-filter 機能を使って接続元 IP アドレスを制限するという方式を考案した。具体的には、フロアスイッチの各非認証ポートに対して接続可能な IP アドレスを指定し、接続 IP アドレス⇔接続ポートを一対一で対応させるというものである。各ポートに接続する LAN ケーブルの敷設先の部屋名、そしてその部屋の入居者氏名はわかっているので事実上の認証と同じことになる。この「IP アドレス指定接続方式」は、「認証」という目的以外にも、他者に割当てた IP アドレスを勝手に使う IP アドレスの盗用や、未割当ての IP アドレスの勝手な使用といった IP アドレスの乱用を防ぐといった利点も含むためネットワークの安定運用の面でも役立っている。ただし、この IP アドレス指定接続を実施するには、該当サブネットが組まれている全てのフロアスイッチを NASW に置き換える必要があるため全学規模での展開には至っておらず、現時点では、総合研究棟 S, E の 2 建物のみの導入となっている。

5. おわりに

本報告は、本学がこれまで行ってきた認証ネットワークの改良事項全般の記録を「研究発表」という形で残しておきたいという全くもって身勝手な思いから行なったものである。内容的にみても、斬新と思えるほどのものではないが、本報告が少しでも他大学の参考になれば幸いである。

参考文献

[1] 徐　浩源、古門　麻貴：L2 認証スイッチを用いたネットワークの構築と運用、学術情報処理研究、No.7, 2003, P69