L-029

柔軟なアクセス制御を実現する認証ゲートウェイに関する研究

Authentication Gateway System with Flexible Access Policies

立石　直樹[1]　Naoki Tateishi
原　元司[1]　Motoshi Hara

1. はじめに

大学や会社などのネットワーク環境の多くでは組織内のユーザによるネットワークの活動記録や不正利用を監視するため，ネットワーク認証システムが導入されている．しかし，これらの認証システムはユーザ，グループ，端末などの単位で異なったアクセス制御を行うことは難しい．

そこで，本研究では，端末の情報と利用者情報を組み合わせることで制御条件を設定可能にする認証ゲートウェイの構築を考えた．本研究では多様なアクセス制御を実現するために，LDAP[1] サーバと Opengate[2] を基盤とした認証ゲートウェイを提案する．

2. 認証ゲートウェイ

2.1 ネットワーク認証システム

ユーザがネットワークを利用する際，そのユーザが本人かどうか確認するシステムがネットワーク認証システムである．ネットワーク認証システムは，大きく分類して

1) ゲートウェイ認証システム
2)VLAN による認証システム
3) チケットによる認証システム

の 3 種類がある．特に，ゲートウェイ認証システムは，ネットワークの出入り口であるゲートウェイ部で認証を行うことでネットワーク全体をネットワーク認証の対象とする．一般的に，認証ゲートウェイは，ユーザのネットワーク認証の完了と同時に通信路を開き，利用の終了と同時に通信路を閉じるようなシステムである．ゲートウェイ認証システムは，上述の 2)，3) の方式に比べて実装面やコスト面で利点を有する．

2.2 Opengate

Opengate は佐賀大学で開発されたオープンソースのゲートウェイ認証システムであり，不特定多数のユーザが多様な端末を接続利用するネットワーク環境を想定している．Opengate の特徴は，汎用の技術を組み合わせることで運用・管理を比較的容易にしている点にある．また，Opengate は利用者認証に web ブラウザを用いるため，特別な申請やクライアント側のソフトウェアの追加なしにネットワーク認証を行うことができる，という利点がある．以下に Opengate の動作の概要を示す．

Step 1:ゲートウェイのファイアウォールは閉鎖状態を標準とする

Step 2:利用者が公開端末や持参 PC で任意の Web サイトへアクセスする．また，ゲートウェイはこの通信を横取りし，ユーザ ID とパスワードを要求する Web ページを返す

Step 3:利用者が入力した情報を受取ったゲートウェイは，認証サーバに問い合わせ，認証が得られれば当該端末に対してファイアウォールを開放する．同時に Java スクリプトまたは javaApplet を端末側に送り利用終了を監視する．監視中には定期的に，端末とのメッセージ交換を行い利用継続をチェックする

Step 4:上記監視が不可能な場合は，指定時間経過時や MAC アドレス変化時，無パケット期間検出時にファイアウォールを閉鎖する．また，利用者が Web ブラウザを終了すると，ファイアウォールを閉鎖する，また，ユーザ ID 等をログに記録する

本研究では，ネットワーク認証システムのプラットホームとしてこの Opengate を活用することにした．

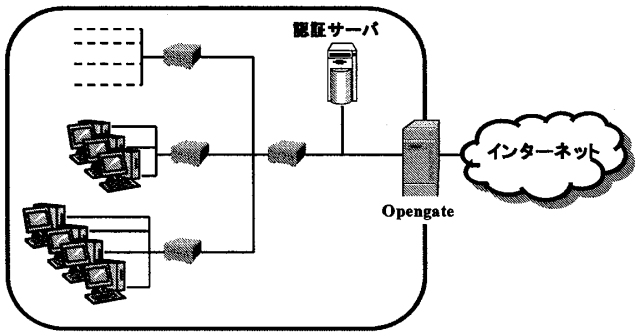

図 1: Opengate のハードウェア構成

3. LDAP と SNMP

本研究ではユーザ，グループ，端末，情報コンセントといった条件でアクセス制御を実現する．この所望の機能を実現するために，LDAP(Lightweight Directory Access Protocol) と SNMP(Simple Network Management Protocol) の両プロトコルを利用する．

3.1 LDAP

LDAP はディレクトリサービスを提供する木構造のデータベースである．ディレクトリサービスとは，ネットワークを利用するユーザ名，パスワード，コンピュータ名，ネットワークデバイス，アプリケーションといったネットワークリソースのさまざまな情報を管理するためのサービスであり，一般的にユーザ名などのキーとなる値からさまざまな情報を検索することが可能である．ディレクトリサービスの身近な例に，ドメイン名と IP アドレスの関係を知るための DNS(Domain Name System) や UNIX のアカウントや機器の情報を提供するための NIS(Network Information Service) がある．オープンソースソフトウェアである OpenLDAP はスキーマと呼ばれるデータによって LDAP 内で多様なデータを扱える．

[1]松江工業高等専門学校

本研究では OpenLDAP を用いて，利用者情報と端末情報，アクセスポリシーなどを格納したデータベースを作成する．OpenLDAP には SDK が含まれており，C 言語の API が用意されている．

3.2 SNMP

SNMP は，TCP/IP ネットワークにおいて，ルータやコンピュータ，端末など，ネットワークに接続された通信機器をネットワーク経由で監視・制御するためのプロトコルである．SNMP の機能を用いることで，監視対象である SNMP エージェントからホスト名，ルーティングテーブル，ARP テーブル，トラフィック数といった情報を取得することができる．

本研究では，オープンソースソフトウェアである Net-SNMP を用い，ルータ L3 スイッチと L2 スイッチを SNMP エージェントとする．

4. 提案システム

4.1 提案システムの概要

本提案システムは，クライアント，Opengate，LDAP サーバ，SNMP 機能対応ルータ，SNMP 機能対応 L2 スイッチで構成される．LDAP サーバには，ユーザ ID をキー値とした利用者情報と MAC アドレスをキー値とした端末情報，アクセスポリシーなどが格納されている．システムが正常に動作するための条件として

1) 認証ゲートウェイ下のネットワーク内で NAT の機能を使用しない

2) ルータの IP アドレスと MAC アドレスが予めわかっている

3)L2 スイッチの管理用 IP アドレスと MAC アドレスが予めわかっている

4)L2 スイッチの接続形態が予めわかっている

という 4 項目がある．

提案システムの構成を図 2 に示す．

4.2 提案システムの動作

クライアントが外部ネットワークを利用する手順を以下に示す．

Step 1:ゲートウェイのファイアウォールは閉鎖状態を標準とする

Step 2:利用者が公開端末や持参 PC で任意の Web サイトへアクセスする．また，ゲートウェイはこの通信を横取りし，ユーザの IP アドレスを取得し，ユーザ ID とパスワードを要求する Web ページを返す

Step 3:利用者が入力した情報を受取ったゲートウェイは，ユーザの IP アドレスからユーザのネットワークのルータを特定し，SNMP の機能を用いて ARP テーブルを調査し，ユーザの MAC アドレスを得る．

Step 4: ゲートウェイは，ユーザの IP アドレスからユーザのネットワークの L2 スイッチ群を特定し，L2 スイッチの MAC テーブルを調査することでユーザが利用している端末がどの L2 スイッチのどのポートに接続されているか特定する．

Step 5 : ゲートウェイは LDAP サーバに対し，ユーザ ID をキー値とした検索と MAC アドレスをキー値とした検索を行い，利用端末の位置，端末の所有者などの情報によって認証条件を生成し，照らし合わせる．

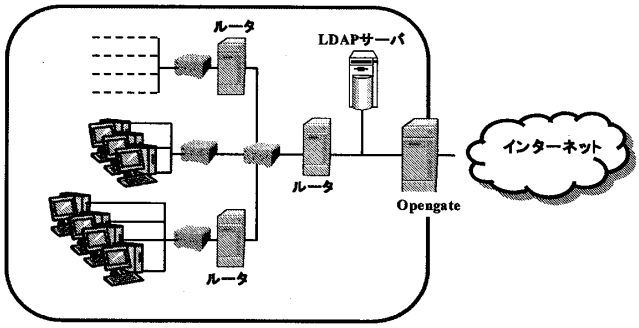

図 2: 提案システムの構成例

Step 6:認証が得られれば当該端末に対してファイアウォールを開放する同時に Java スクリプトまたは javaApplet を端末側に送り利用終了を監視する．監視中には定期的に，端末とのメッセージ交換を行い利用継続をチェックする

Step 7 : 利用端末の MAC アドレスが登録されていないときは，Opengate の通常の認証を行う．

Step 8 : ファイアウォールの開放と閉鎖時には，ユーザ ID 等をログに記録する

現在，Opengate と LDAP サーバ，SNMP の連携部分を実装中である．

5. まとめ

本研究では，端末情報と利用者情報を組み合わせ，柔軟なアクセス制御を可能にする利用者認証ゲートウェイを提案した．しかし，LDAP サーバ内のデータスキーマを詳細に定義し，利用者情報と端末の情報を組み合わせて柔軟なアクセス制御を行うことは未だ実現できていない．

今後は端末の情報と利用者情報を組み合わせることで制御条件をどのように設定するかを決め，LDAP サーバ内のデータに基づくアクセス制御を実現したい．また，LDAP 内で扱う各種データを簡単に管理する方法についても検討したい．

参考文献

[1] 稲地　稔，”OpenLDAP 入門”，技術評論社，2003.

[2] 渡辺義明，渡辺健次，江藤博文，只木進一， 大谷誠， “HTTP コネクションの監視により利用終了検知を行うネットワーク利用者認証システムの開発とその円滑な導入 ”，情報処理学会論文誌，Vol. 50, No. 3, pp. 1-11, 2009.

[3] 串間竜治, 長野一樹, 最所圭三 ，“ レイヤ 2 スイッチを用いた不正パケット遮断システムの研究” 平成 18 年度 電気関係学会四国支部連合大会論文集，p.250, 2006.9.