M-031

Kerberos を用いたネットワーク認証システム

Network Authentication Gateway System with Kerberized Firewall Controling Service

中島　麻衣子 [1]　　**原　元司** [1]

Maiko Nakashima　　Motoshi Hara

1. はじめに

近年，増加するネットワーク利用犯罪やプロバイダ責任制限法などの影響によって，多くの組織がネットワーク認証システムを導入している．このネットワーク認証システムの導入は，インターネット上でのユーザの活動を記録できる一方，組織内のユーザがインターネット上で行う不正行為やモラルハザードを抑制する効果が期待されている [1]〜[3].

一方，これまでに提案されているネットワーク認証システムはコストやユーザにとっての利便性の点で問題がある．そこで，本研究ではゲートウェイ型のネットワーク認証システムに着目し，Kerberos を活用したネットワーク認証システムの提案を行う．

2. ネットワーク認証システム

ネットワーク認証システムとは，ネットワークを利用するユーザの正当性を確認するシステムであり，コンピュータネットワーク上で安全性を確保するための重要な手段の一つである．ネットワーク認証システムが実現すべき機能として，認証，認可，監査といったものがある．これらの機能により，ネットワークを利用するユーザを特定し，そのユーザに基づいて特定のリソースへのアクセス権を与え，さらにユーザの活動記録を残すことができる．また，このネットワーク認証システムは，以下のように三種類に大別することができる．

(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

(1)〜(3) の中で，もっとも手軽にネットワーク全体を認証の対象とできるのは (1) の方式である．また，(2) の方式は一般に通常のハブよりも高価な VLAN 対応型のスイッチングハブを必要とするため，ネットワーク全体に導入するのは現実的ではない．

現在，松江高専では (1) のゲートウェイ認証システムの一種である Opengate を利用している [2]．この Opengate は無料配布されており，導入の際のコストを低く抑えることができる．また，C クラス程度のネットワークであれば，組織全体を認証の対象とすることも容易である．しかし，Opengate を含めてほぼすべてのネットワーク認証システムにおいて，OS での認証とネットワーク認証とが別であり，二重に認証を行う必要がある．

そこで本研究では，(1) の方式と (3) の Kerberos 認証の併用を行うネットワーク認証システムを構築し，より安全でしかも，シングルサインオンが可能なネットワーク認証システムを構築することにした．

[1]松江工業高等専門学校

3. Kerberos について

Kerberos は，チケットによるネットワーク認証システムの一種であり，通信系路上の安全が保障されていないインターネットなどのネットワークにおいて，サーバとクライアントの間で暗号化された通信を行う．これは，ユーザを安全でかつ効率的に認証することを目的として開発された．現在，Kerberos は多くの OS で標準化されており，UNIX 系 OS，Windows2000 以降，Mac OS 10.2 以降でサポートされている．

3.1 Kerberos の特徴

Kerberos の特徴を以下に示す [4].

1. 安全
   クライアントとサーバ間のすべての通信は，暗号化してやりとりされる．さらに，認証サーバ (AS) から発行される有効期限付きの交付チケット (TGT) を利用した認証方法により，より安全な認証が実現できる．

2. 認証情報の一元管理
   ネットワーク内に，AS とチケット発行サーバ (TGS) から構成される鍵配布センター (KDC) を配置し，そこですべての認証を集中化させる．

3. シングルサインオン
   クライアントは KDC で一度だけ認証を受け，正規のクライアントであることが確認されると，それ以降は，証明書となる TGT によりユーザは認証作業なしに複数のサービスが利用可能となる．

3.2 Kerberos 認証の流れ

Kerberos 認証の流れを図 1 に示し，その手順を説明する [5].

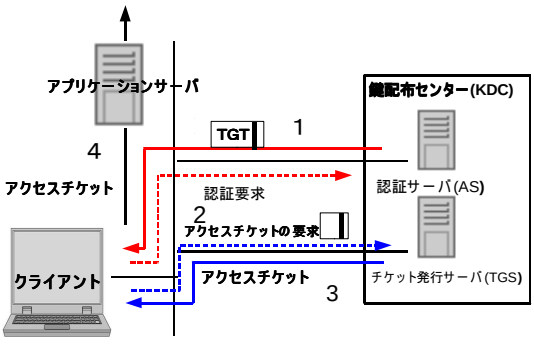

図 1: Kerberos の認証の流れ

1. クライアントは KDC の AS に Kerberos パスワードによる認証要求を行い，ユーザ自身のパスワー

ドで暗号化された TGT を受け取る．これを自身のパスワードで複合化することで，TGT を取得する．TGT を複合化して取得できるのは正規のユーザだけである．

2. 取得した TGT を KDC の TGS に提示し，アクセスしたいアプリケーションサーバへのアクセスチケットを要求する．TGT は期限を持っているが，その期限内であれば複数のアクセスチケットの要求が可能となる．

3. TGS は，クライアントが要求したアプリケーションサーバへのアクセス権限をあると確認すると，そのアプリケーションサーバへのアクセスチケットをクライアントに発行する．

4. クライアントは，入手したアクセスチケットをアプリケーションサーバに提出して，自信が正規のネットワークユーザであり，アクセス権を持っていることを通知し，サービスの利用を開始する．アクセスチケットのやり取りには共有鍵暗号方式がが使われており，安全性が保障されている．

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，KDC，Kerberos クライアント，Firewall の三者で構成される．今回，KDC と Kerberos クライアントの実装を Kerberos に対応した PC-UNIX(FreeBSD) 上で行った．本研究の最終目標は，Kerberos によるログイン認証を完了したユーザに対し，ユーザ名，パスワードの情報を再入力することなくインターネットの利用を開始させることである．今回，Firewall 上に telnet ログインを利用したシングルサインオン型のネットワーク認証を実現した．本システムの構成図を図 2 に示す．

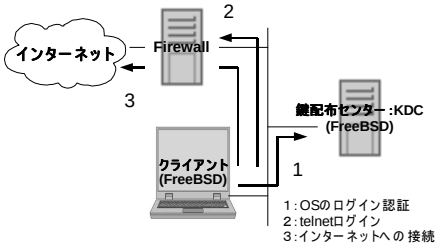

図 2: 提案システムの構成図

4.2 提案システムの動作

現時点で，本システムは KDC とクライアントの設定を終え [6]，KDC に登録されたクライアントがネットワーク認証を行うホストにパスワード入力なしで telnet ログイン可能となっている．この telnet 認証を行った際に，Firewall の通過許可および切断を指示するための認証プログラムを作成し，ユーザ名，パスワードの再入力を必要としないネットワーク認証システムのプロトタイプを実現した．

この認証プログラムは，/var/run/utmp ファイルを利用し，クライアントのホスト名，ユーザ名のセットからクライアントのログイン，ログアウトを監視するものである．また，ログイン，ログアンを行ったクライアントのホスト名から IP アドレスを取得する機能を有しており，ここで取得した IP アドレスにより，Firewall の通過と切断の制御を行うパケットフィルタリングコマンドの発行を行っている．

なお，本システムではネットワーク認証の終了は telnet ログアウト，あるいは一定時間 Firewall を通過するパケットがない場合で判定する．

4.3 提案システムの拡張

本提案システムでは，Kerberos におけるサービスチケットを提示する手段として telnet ログインによるシングルサインオンを実現した．しかし，インターネット利用として利用頻度の高い Web ブラウザとは別に，telnet コマンドを実行する作業が余計にかかってしまう．このため，Web ブラウザの起動がサービスチケットの提示となるようなシステムの拡張を検討している．

具体的には，Firewall 上で Kerberos 化した WWW サーバプログラムを起動させ，ネットワーク認証が完了していないユーザからのパケットをその WWW サーバに forward を行う．この作業により，サービスチケットを WWW サーバに提示し，認証を完了する．このシステムの場合，サービスチケットの有効期限を短くすることで，telnet 利用時と同様なタイムアウト処理が可能になる．

5. まとめ

本研究では，OS のログイン認証を Kerberos で行い，telnet ログインによる Firewall の通過・切断を行うネットワーク認証システムを作成した．今後は Web ブラウザベースのネットワーク認証システムへの拡張を行い，実際に運用実験を行いたい．

参考文献

[1] 原　元司，他：情報倫理教育に適したネットワーク認証システム，論文集「高専教育」第 26 号，pp.781-786(2004).

[2] 渡辺　義明，他：利用と管理が容易で適用範囲の広い利用者認証ゲートウェイシステムの開発，情報処理学会論文誌，vol.42,No.12,pp.2802-2809(2001)

[3] 石橋　勇人，他：利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式，情報処理学会論文誌，vol.42,No.1,pp.79-88(2001)

[4] Jason Garman(桑村潤 訳)：Kerberos，オイラリー・ジャパン (2004).

[5] @IT「Kerberos」：
http://www.atmarkit.co.jp/icd/root/11/87736911.html

[6] 佐藤広生：FreeBSD で作る Kerberos 認証システムオープンソースマガジン,Vol.14,No.12,pp.133-139(2005).