5W-5

XFW:アドレス偽造を防止した オープンスペース用ネットワークアクセスサービスの運用と評価

氏　名† 福田 浩章　　氏　名† 山本 喜一
所　属† 慶應義塾大学　所　属† 慶應義塾大学

1．はじめに

現在コンピュータ(端末)の小型化や低価格化に伴い，端末を持ち歩くユーザが急速に増加している．また，それらの端末をネットワーク接続させるために無線 LAN を代表とするネットワークインフラも整備されつつある．しかし，無差別にネットワーク接続を許可する場合，不正利用の温床になることは容易に想像できる．したがって，あらかじめ登録された正規ユーザが利用する正規端末だけ接続を許可し，かつ IP アドレスや MAC アドレスの偽造による不正端末のネットワーク接続を防止する必要がある．

そこで本論文では，一般的なウェブブラウザだけを使って正規ユーザの識別および，IP アドレスや MAC アドレスを偽造した不正端末を使ったネットワークの利用を防止するシステム XFW を構築し，実際に運用した結果と評価を報告する．

2. ネットワーク接続方式

本節では，XFW を用いた接続方式，および認証方式を述べる．

2.1 接続方式

多数のユーザをネットワークに接続させる場合，図 1 に示すようなプライベートネットワークを利用することが一般的である．この場合，プライベートネットワークに接続した端末は，NATBOX と呼ばれるサーバを経由してグローバルネットワークに接続することができる．NATBOX では一般的に DHCP,NAT,Firewall,DNS といった機能を提供している．XFW はこの NATBOX 上で動作してユーザ認証を行い，Firewall の機能を利用して正規端末だけのネットワーク接続を許可する．また，ユーザ認証情報は Radius や LDAP といった外部認証システムを利用する．

2.2 認証方式

ユーザは図 2 に示す手順で認証処理を行う．

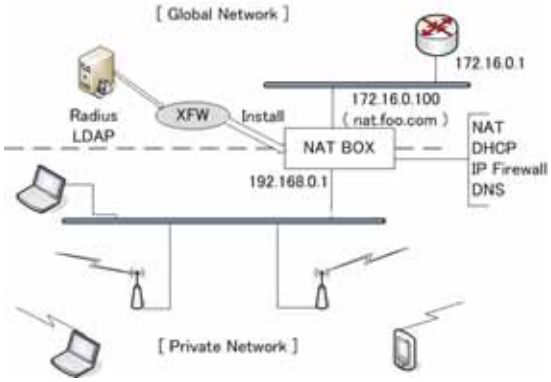

図 1 ネットワーク接続方式

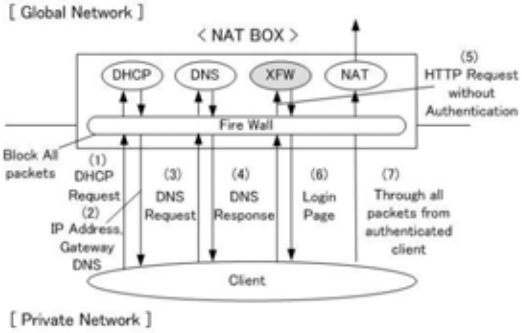

図 2 認証方式

(1) 端末をプライベートネットワークの情報コンセントに接続するか，無線の電波を受信し，DHCP リクエストを送信する．

(2) DHCP サーバが IP アドレスを提供する．
(3) ユーザがブラウザを起動し，ブラウザが DNS リクエストを送信する．
(4) DNS サーバから IP アドレス情報を受信する．
(5) ブラウザが HTTP リクエストを送信する．Firewall 機能によって HTTP リクエストを強制的に XFW にフォワードする．
(6) XFW は無条件に認証用コンテンツを送信する．
(7) ユーザが ID とパスワードを入力し送信する．認証に成功すると XFW はその端末が正規端末であると認識し，その端末が送信するパケットを通過させるために Firewall の設定を変更する．その結果，正規端末からのパケットだけが Firewall を通過する．

XFW: An evaluation against address spoofing for open network access service
† Keio University

3. アドレス偽造防止法

2.2 節で示した方法で正規端末の接続を許可した後，ユーザが利用を止めたとき，端末の切断を検知する必要がある．しかし，端末の識別子として用いられる IP アドレスや MAC アドレスは容易に偽造できるため，それらを識別子として利用するだけでは不正利用の危険性は免れない．
そこで XFW では，認証時に XFW から端末に発行するセッション ID を端末から定期的に送信させ，かつ送信するたびにセッション ID を変更することでアドレス偽造を検知する．

XFW では秘密鍵と MD5 ハッシュアルゴリズムを利用し，JavaScript が動作する一般的なブラウザだけでこの機能を実現している．したがって，ノート型端末だけでなく，PDA などの携帯端末でも新たなアプリケーションを導入することなくネットワークに接続することができる．

4. 運用実績と評価

XFW は，現在大学のキャンパスで運用しており，十分な効果を発揮している．図 3 と図 4 に 2005 年 12 月から 2006 年 12 月まで 1 日あたりの延べユーザ数，最大同時接続数の推移を示し，XFW を評価する．そして，運用時に発生した問題と解決法を述べる．

4.1 評価

図 3 に示すように，運用を開始してから 1 年後には 1 日あたりの延べユーザ数が約 2.5 倍に増加している．また，図 4 に示すように，1 日あたりの同時接続数も，運用開始から 1 年後には約 3 倍に増加している．キャンパスに出入りする教員や学生の数には大きな変化がないため，これらの結果から XFW が一般に広く浸透していると考えることができる．また，延べユーザ数，および同時接続数が増加したことによる性能の低下も認められていない．

一方， XFW 導入以前は SSH クライアントを利用したネットワーク接続サービスを展開していた．しかし，SSH クライアントのインストールや設定で混乱するユーザも多く，それらのサポートが必要であった．XFW では，一般的なウェブブラウザだけですべての処理を行うことができるため，新規にソフトウェアを導入する必要もなく，ユーザの混乱を避けることができた．

4.2 問題点と対策

3 節で述べたように，XFW ではセッション ID を用いて正規端末の接続や切断を確認している．しかし，無線環境で利用した場合，電波の状況によっては一時的にセッション ID が XFW に届かず，端末で送信するセッション ID と，XFW で管理するセッション ID のずれによって，正規端末であるにもかかわらず強制的に切断されるという現象が見受けられた．そこで，セッション ID が異なる場合，秘密鍵をもとにセッション ID を補正する処理を加えることにより解決している．

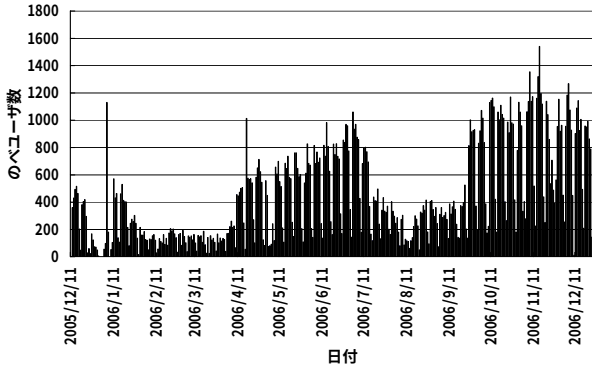

図 3　延べユーザ数の推移

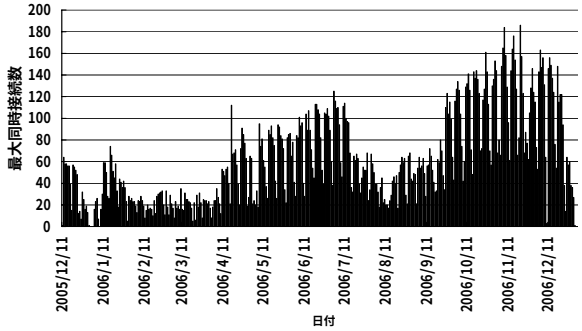

図 4　最大同時接続数の推移

5. まとめ

本論文では，多数のユーザが対象になる環境において，正規ユーザだけに接続を許可し，アドレス偽造による不正利用を防止するシステム，XFW の提案を行った．そして実際に大学のキャンパスで運用し，結果を示すとともに運用時の問題点と対策を示した．XFW を導入することによって，利用する権利を持ったユーザであれば認証処理を行った後，容易にネットワークを利用することができる．しかし，XFW では認証後に端末がやり取りするデータに関して暗号化などは行わないため，情報漏えいを防ぐためには SSL/TLS などの暗号化技術を導入する必要がある．