6R-3

セキュリティゲートウェイの構築

黒羽 秀一† 初谷 良輔†† 齋藤 孝道††
† 東京工科大学 †† 明治大学

1 はじめに

Web サーバで SSL (Secure Socket Layer)[1] を利用する場合，暗号処理が高い負荷をかけ Web サーバ全体の処理能力が低下する．そのため，Web サーバから SSL の処理を分離し，SSL リバースプロキシとバックエンド Web サーバからシステムを構成することがある．しかしながら，アプリケーションによってはユーザを識別したいことがある．そのような場合に，SSL リバースプロキシがクライアント認証モードで動作していると，SSL リバースプロキシとアプリケーションの２つのレベルでの認証をクライアント（ユーザ）に強いることになる．

さらに，Apache などが提供するアクセス制御モデルでは，階層構造にあるファイルやディレクトリに対して，きめ細かなアクセス制御ポリシーを設定することが困難な場合がある．また，バックエンドに複数存在する Web サーバのリソースの管理も煩雑になる．

そこで，本論文では，SSL リバースプロキシ内で認証情報を制御する仕組みを導入し，バックエンドサーバとの透過的な認証を実現することで二重の認証を解決し，さらに，複数のバックエンド Web サーバに対して柔軟なアクセス制御を実現するセキュリティゲートウェイ (Security Gate Way, 以下 SGW) を提案する．

2 準備

本論文を通して用いる用語について記述する．

Basic 認証の認証情報

Web サーバがユーザを識別するために必要なユーザ ID とパスワード．

認証リスト

認証リストの要素は，X.509 クライアント証明書の CN(Common Name) と Basic 認証の認証情報の対である．認証リストは SGW がクライアントの代わりに Web サーバと認証をするときに利用される．ただし，本論文では CN は一意であると仮定する．CN と Basic 認証の認証情報の対応を以下に示す．

認証リスト = $\{CN, id, password\}$

ACL (Access Control List)

ACL は SGW が保持している．ACL はクライアントが Web サーバのどのリソースに対してどのような権限を持つのかを記述したリストである．

3 提案システム

ここでは，提案システムの概要について述べる．

SGW は，クライアント[1] と 1 台以上からなる Web サーバ[2] との間に位置するゲートウェイである．SGW は認証フェーズとアクセス制御フェーズから構成されている．認証フェーズはクライアントに代わってパスワードの管理と Web サーバとの透過的な認証をおこなうフェーズである．アクセス制御フェーズは複数台の Web サーバに代わってアクセス制御をおこなうフェーズである．本論文では，ファイルシステムのアクセス制御を例としている．

3.1 認証フェーズ

SGW の認証フェーズでは，認証リストに登録された Basic 認証の認証情報を使用して，クライアントの代わりに Web サーバと 認証をおこなう．

この認証フェーズには２つのパターンがある．SGW が認証リストに Basic 認証の認証情報を登録するパターン (以降，パターン 1) と SGW が認証リストを利用して Web サーバと Basic 認証をおこなうパターン (以降，パターン 2) がある．パターン 1 は，クライアントが SGW にはじめてアクセスした場合を想定している．今回は，事前に SGW に CN と Basic 認証の認証情報が登録されていることを前提とし，パターン 2 について述べる．

認証リストを利用して Web サーバと Basic 認証をおこなう手順を図 1 示す．

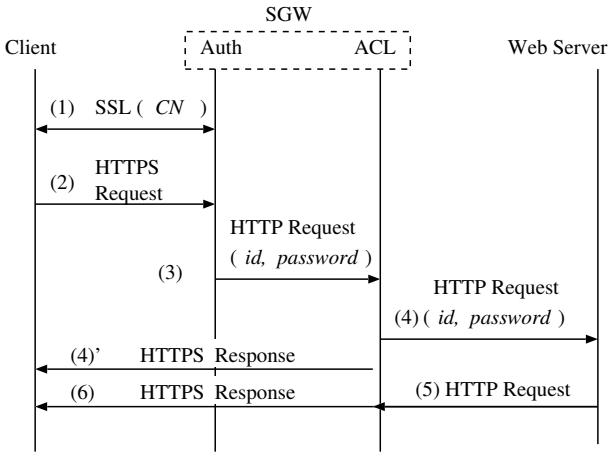

図 1: パターン 2

(1) クライアントは SSL クライアント認証モードで SGW を相互に認証をおこなう．これによって，SSL 接続が確立する．このとき，X.509 クライアント証明書に含まれる CN と対応する Basic 認証の認証情報を認証リストから取得する．

(2) クライアントは SGW にファイルの取得要求をおこなう．

(3) 認証フェーズでクライアントからファイル取得要求の通報を受信すると，その通報に取得した Basic 認証の認証情報を付加する．その後アクセス制御フェーズに移る．

(4) アクセス制御フェーズで ACL を確認し，クライアントにファイルに対するアクセスが許可されている場合，Basic 認証の認証情報を付加したファイル取得要求の通報を Web サーバに送信する．

† Shuuichi KUROBA (b0206914@ess.teu.ac.jp)
†† Ryosuke HATSUGAI (hatsugai@cs.meiji.ac.jp)
†† Takamichi SAITO (saito@cs.meiji.ac.jp)
Tokyo University of Technology(†)
Meiji University(††)

[1] IE や Netscape といった一般的な Web ブラウザが利用可能なマシンである．

[2] このマシン上では Apache-2.0.52 が稼動している．

(4)' アクセス制御フェーズで ACL を確認し，クライアントがファイルに対するアクセスが許可されていない場合，エラーの通報をクライアントに送信する．

(5)(6) SGW から Basic 認証の認証情報を受信し，これを確認した後，ユーザの認証に成功した場合，リクエストに対応するレスポンスをクライアントに送信する．

3.2 アクセス制御フェーズ

アクセス制御フェーズはクライアントのファイル取得要求の通報を受信した後におこなわれる．アクセス制御は ACL を利用して実現する．ACL はユーザが所有するディレクトリおよびファイルの構造と同じ階層構造で示されるデータベーステーブルで記述される．データベースのテーブルフィールドを図 2 に示し，各フィールドの役割を以下で記述する：

File	Allow	Deny	Delegate

図 2: ACL テーブル

File： ファイル名または下位へのディレクトリ名である．

Allow： このフィールドに記述されたユーザは，File フィールドのファイルまたはディレクトリに対するアクセス権限がある．また，Allow フィールドはフラグ表記 rw によって権限の詳細を記述できる．フラグ r が記述されているときは読み込み許可を示し，フラグ w が記述されているときは書き込みの許可を示す．

Deny： このフィールドに記述されたユーザは，File フィールドのファイルまたはディレクトリに対するアクセス権限がない．また，Deny フィールドはフラグ表記 rw によって権限の詳細を記述できる．フラグ r が記述されているときは読み込み不可を示し，フラグ w が記述されているときは書き込み不可を示す．

Delegate： このフィールドに記述されたユーザは，ACL の アクセス制御を自由に設定することができる．

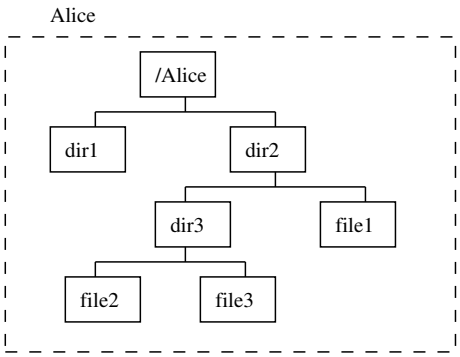

図 3: Alice の所有するディレクトリの階層構造

3.3 アクセス制御の一例

Bob が Alice の所有するファイル file3，file2 にアクセスした場合を例に，アクセス制御フェーズの動作を示す．

Alice が図 3 の破線で囲まれたディレクトリ階層を所有しているとする．さらに，Alice は図 4 に示す ACL の階層構造を持つアクセス制御ポリシーを作成していると仮定する．また，図 4 中の ALL はすべてのユーザを示す．

3.3.1 アクセス権限の有無

Bob が file3 にアクセスする場合，SGW は Alice が作成した アクセス制御ポリシーの階層を上位にある ACL から順番にアクセス権限を確認する．この場合，リクエストに含まれる URL は /Alice/dir2/dir3/file3 である．したがって，dir2，dir3，file3 の 順に ACL に記述されたアクセス権限を確認する．

dir2 と dir3 の ACL を確認するとすべてのユーザがアクセス可能であることがわかる．次に， file3 の ACL を確認すると Deny フィールドに Bob:w と記述されていることがわかる．このフラグは，Bob が file3 に対する読み込み権限は認められているが，書き込み権限が認められていないことを示す．

3.3.2 アクセス権限の委譲

Bob が file2 にアクセスする場合，dir2，dir3，file2 の順に ACL に記述されたアクセス権限を確認する．dir2，dir3 の ACL に記述されたアクセス権限を確認するところまでは，file3 にアクセスした場合と同様である．SGW が file2 の ACL に記述されたアクセス制御を確認すると，Delegate フィールドに Bob と記述されていることがわかる．これは，file2 の owner 権限が Bob に委譲されているということである．つまり，Bob は file2 のアクセス制御を自由に設定することができる．

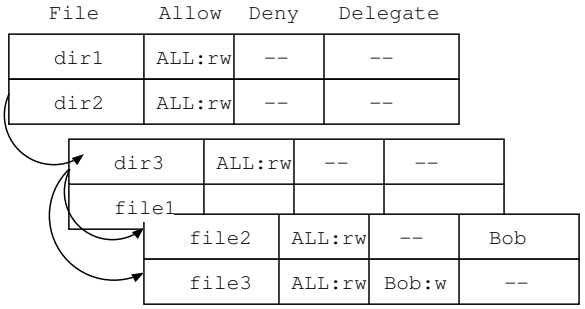

図 4: ACL の階層構造

4 まとめ

SSL リバースプロキシを利用した Web システムにおいて，SSL クライアント認証モードと Basic 認証を利用すると，クライアントに二重の認証を強いることになる．本論文では，SGW によって SSL による認証とパスワードによる認証の二重の認証を解決する方法を示した．さらに，ACL を利用して Web サーバに依存しない柔軟なアクセス制御を実現できることを示した．今後の課題には，ACL の記述をおこなうためのインタフェースの設計と権限を委譲した場合にそれをユーザに通達するためのインタフェースの設計がある．

参考文献

[1] A.Freier, P.Kocher, and P.Kaltorn, "The SSL Protocol Version 3.0 draft", March 1996.