

飯田 恭弘 佐藤 直之 花木 三良

NTT 情報流通プラットフォーム研究所

1. はじめに

近年、インターネットへ接続し、Web ブラウザを使用してネットワーク上に置かれている資源を利用する事が一般的になりつつある。その際、ユーザの認証はユーザ識別子とパスワードを照合し、ユーザを特定することで行う場合が多い。しかし、本来、認証の目的は資源を利用できるかどうかの権利を確認することであり、ユーザ個人を特定することではない。認証時にユーザを必要と特定することはプライバシ保護の面からも好ましいとは言えない。

このような背景から、著者らはユーザが個人情報を開示せずに権利を行使できる方式（これを匿名認証方式と呼ぶ）を提案してきた[1,2]。また、Web 環境に本方式を適用し、その有効性を確認してきた[3]。

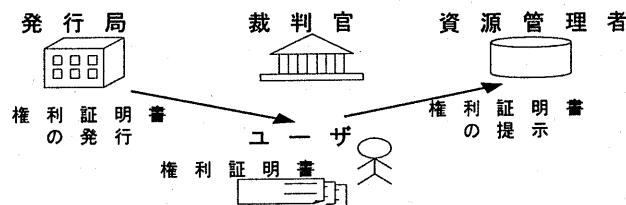
本稿では、Web 環境にさらに適した形で匿名認証方式を適用する方法を報告する。また、本方式をインターネットへのダイヤルアップ接続に適用する方法も併せて報告する。

2. 匿名認証方式

著者らが提案してきた匿名認証方式では、以下に述べる 4 種類の主体を考える。また、ユーザを特定することなく権利のみを保証する特殊な証明書（これを権利証明書と呼ぶ）を利用する（図 1）。

- ・発行局：権利証明書を発行する主体
- ・資源管理者：権利証明書を検証し資源を提供する主体
- ・ユーザ：権利証明書を用いて資源を利用する主体
- ・裁判官：ユーザを特定し権利証明書を無効にできる唯一の主体

本方式では、ユーザは同一の権利証明書を何度も使用できる。また、資源管理者はもちろん、権利証明書の発行局でさえも証明書自体からその証明対象であるユーザを識別できないという特徴がある。



3. Web 環境への適用

匿名認証方式を Web 環境に適用し、Web サーバがユーザを識別することなく、ユーザがアクセス制限の設けられた Web ページを閲覧できるシステムを実現する。本システムでは、Web サーバは匿名認証方式における資源管理者の役割を果たす（図 2）。

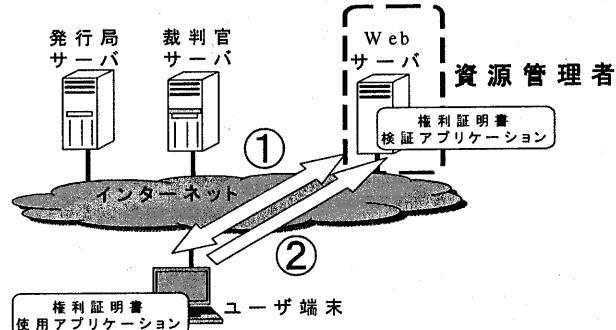


図 2 Web 環境における匿名認証方式

匿名認証方式を実現するため、Web サーバに権利証明書検証アプリケーションを、ユーザ端末に権利証明書使用アプリケーションを導入する。ユーザがアクセス制限の設けられた Web ページを閲覧するためには、Web サーバは①権利証明書の検証、②Web ページ閲覧の許可、の 2 段階の処理を行う。

① 権利証明書の検証

- ・権利証明書の送信：Web サーバはユーザの要求を受けて、ユーザ端末へ権利証明書使用アプリケーションに関連付けられた設定ファイルを送信する。ユーザ端末がこの設定ファイルを受信すると、Web ブラウザはユーザ端末上で権利証明書使用アプリケーションを起動する。このとき、ユーザは使用する権利証明書を選択し、Web サーバへ送信する。

- ・発行局の署名の確認：Web サーバは権利証明書に含まれる発行局の署名を CGI にて検証する。

- ・ユーザの正当性の確認：Web サーバはユーザが権利証明書の正当な使用者であることをチャレンジレスポンス

ンスを行い、検証する。

- ・Cookie の発行：上記二つの処理に成功したとき、Web サーバはアクセスの許可を証明する Cookie を CGI にて作成し、ユーザ端末へ発行する。この Cookie は権利証明書の内容を含む。また、Cookie の作成には、Cookie の偽造防止のために Web サーバの秘密鍵を用いたハッシュ値（署名）を利用している。

② Web ページ閲覧の許可

- ・Cookie の送信：ユーザは Web サーバに Cookie を送信する。
- ・Cookie の検証：Web サーバは Cookie の内容および偽造がなされてないことを検証し、これに成功すればユーザへ Web ページの閲覧を許可する。

上記のように、アクセスを許可する証明書（これをアクセス許可証と呼ぶ）として Cookie をユーザ端末へ発行する検証方法では、権利証明書の検証に一度成功すると、次回からは Cookie を検証するだけでよい。権利証明書の検証にかかる負荷は Cookie の検証に比べて非常に大きいため、今回、上記の検証方法を用いることで負荷の低いシステムを実現している。また、この手法では、権利証明書の使用時に権利証明書使用アプリケーションが Web ブラウザを 2 つ起動してしまうという従来手法[3]の操作上の欠点を解消している。

なお、権利証明書の発行処理及び裁判官サーバによる処理もネットワーク上で行っているが、本稿では説明を省略する。

4. ダイヤルアップ接続への適用

匿名認証方式をダイヤルアップ接続に適用し、アクセスサーバ及び Radius[4]サーバがユーザを識別することなく、ユーザがインターネットへ接続できるシステムを実現する。ここで、上記の二つのサーバは匿名認証方式における資源管理者の役割を果たす（図 3）。

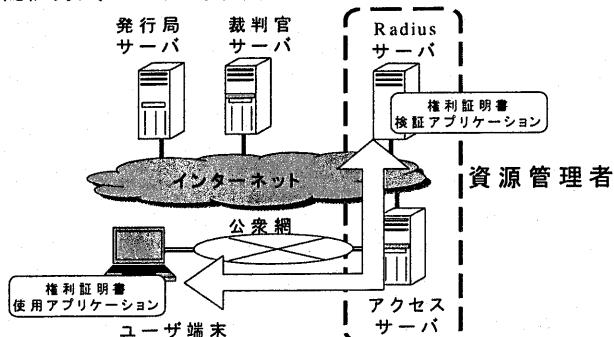


図3 ダイヤルアップ接続における匿名認証方式

匿名認証方式を実現するため、Radius サーバに権利

証明書検証アプリケーションを、ユーザ端末に権利証明書使用アプリケーションを導入する。また、アクセスサーバには、権利証明書をユーザ端末から Radius サーバへ受け渡せるように拡張を加えている。以下に、ダイヤルアップ接続確立までの処理を順に述べる。

- ・回線接続の確立：アクセスサーバはユーザ端末との間に電話回線の接続を確立する。
- ・権利証明書の取得：ユーザは使用する権利証明書を選択し、これをアクセスサーバ経由で Radius サーバへ送信する。通常、ダイヤルアップ接続の場合はパスワードによる認証を行う。しかし、本システムでは権利証明書による認証を行うため、権利証明書の送受信が発生する。そこで、アクセスサーバを介した Radius サーバとユーザ端末の通信には、証明書の送受に対応した PPP-EAP[5]及び Radius-EAP[6]を利用する。
- ・発行局の署名の確認：Radius サーバは権利証明書に含まれる発行局の署名を検証する。
- ・ユーザの正当性の確認：Radius サーバはユーザが権利証明書の正当な使用者であることを、アクセスサーバを介したユーザ端末とのチャレンジレスポンスによって検証する。
- ・PPP コネクションの確立：上記二つの処理に成功したとき、PPP コネクションを確立する。

5. まとめ

今回、匿名認証方式を Web 環境およびダイヤルアップ接続へ適用する方法を提案し、この有効性を確認した。Web 環境においては、Cookie をアクセス許可証としてすることで、従来の方法に比べて操作の利便性を改善することができた。今後はさらに効率のよい実装方法を検討するとともに、ftp や telnet 等における認証部分についても匿名認証方式を適用することを検討する予定である。

参考文献

- [1] 佐藤直之、鈴木英明，“匿名のままの権利行使を可能とした認証方式”，情報処理学会論文誌，Vol.41, No.8, 2000
- [2] 佐藤直之、鈴木英明，“耐タンパ個人端末を利用し個人情報の保護を可能とした認証方式”，情報処理学会論文誌，Vol.41, No.8, 2000
- [3] 飯田恭弘、佐藤直之、鈴木英明，“バイオメトリクスを用いたユーザを識別しない認証方式の実装”，第 61 回情報処理学会全国大会講演論文集，3F-3, 2000
- [4] C. Rigney, et.al.: “Remote Authentication Dial In User Service”, RFC2058, 1997
- [5] L. Blunk, et.al.: “PPP Extensible Authentication Protocol”, RFC2284, 1998
- [6] P. Calhoun, et.al.: “Extensible Authentication Protocol Support in RADIUS” RFC-draft, 1997