ユーザ属性情報を利用したセキュアイントラネットの構築

1Ｔ－7

宮崎 博　　鮫島 吉喜
日立ソフトウェアエンジニアリング(株)

1.はじめに

インターネットを利用した企業内情報交換が普及するにつれ、情報漏洩などに対するセキュリティ導入の必要性が高まっている。その対策として暗号技術の導入が進んでいるが、従来のような個人単位の復号可能者指定方式では、復号可能な者の指定が個人単位になっており、企業における所属部署や役職の指定による情報の送付・開示形式にそぐわない。そこで我々は、暗号する際に復号可能な者の条件として、氏名のようなＩＤだけでなく所属部署や役職といったユーザ属性情報を指定できる暗号方式を提案してきた[1]。これにより、情報の漏洩防止、ユーザ認証、アクセス制御を兼ね備えたセキュリティシステムの構築が可能となる。本稿では、この暗号方式を利用した暗号・アクセス制御のWWWへの適用について報告する。

2.WWWのアクセス制御の問題点

WWWでは、そのプロトコルであるＨＴＴＰでパスワード方式によるアクセス制御方式を提供している。そのため、WWWを企業内の情報公開に使った場合、課長以上のみ閲覧可能というようなアクセス制御を行うと、パスワード管理が煩雑になってしまう。

3.秘密鍵証明書と属性証明書

本稿で述べるシステムでは秘密鍵証明書と属性証明書を導入し、秘密鍵暗号方式による暗号化とユーザ属性の認証、およびアクセス制御を実現している。

秘密鍵証明書はユーザの秘密鍵を保護するもので、その発行元であるＫＤＣ(Key Distribution Center)の秘密鍵で暗号化と署名をしている。したがって秘密鍵証明書は自由に配布可能である。

属性証明書はユーザの属性を保護するもので、ＫＤＣの秘密鍵で署名してあり、秘密鍵証明書と同様に自由に配布可能である。属性には、氏名・所属部署・役職・担当業務などがあり、例えば「役職＝課長」というように、属性型「役職」と属性値「課長」からなる。

これらの秘密鍵証明書および属性証明書は予めユーザやWWWサーバに対して発行し、配布しておく。

4.暗号化・アクセス制御手順

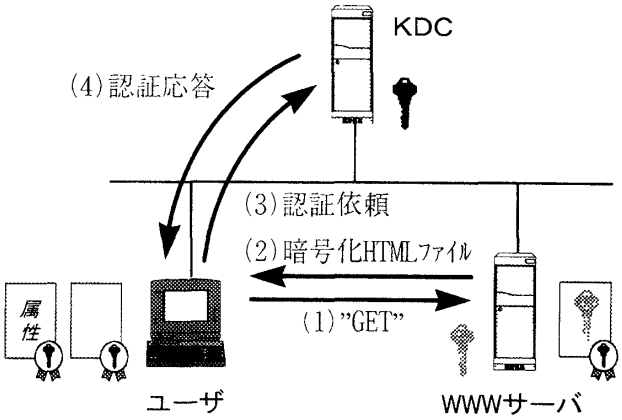

図 システム概要

図は、ユーザ属性情報を利用した暗号・アクセス制御を適用したWWWシステムの概要である。図に示したように、ＫＤＣ、WWWサーバ、ユーザはそれぞれ秘密鍵をローカルに保存している。また、WWWサーバとユーザはそれぞれ、ＫＤＣの秘密鍵で暗号化・署名されている秘密鍵証明書を所有している。さらにユーザは、ＫＤＣの秘密鍵で署名されている属性証明書を持っている。

Secure Intranet with user attribute
Hiroshi Miyazaki, Yoshiki Sameshima
Hitachi Software Engineering Co., Ltd.

以下に、WWWサーバ上のＨＴＭＬファイルの暗号化とアクセス制御の仕組みを示す。

4.1 暗号化・アクセス制御の準備

WWWサーバ側では、前もってＨＴＭＬファイルの暗号化とアクセス制御情報の生成をしておく。

まず、セッション鍵をランダムに生成し、この鍵でＨＴＭＬファイルを暗号化する。次に、閲覧を許可する属性とセッション鍵をWWWサーバの秘密鍵で暗号化し、アクセス制御情報を生成する。そして、これらの暗号化したＨＴＭＬファイルとアクセス制御情報、WWWサーバの秘密鍵証明書を、ユーザからの一回のアクセスでダウンロードできるように一つのファイルにまとめておく。

4.2 動作手順

ユーザは、以下のような手順でWWWサーバ、ＫＤＣと通信し、平文のＨＴＭＬファイルを得てブラウザに内容を表示する。

(1)WWWサーバへのアクセス

(2)暗号化したＨＴＭＬファイルのダウンロード

(3)認証依頼

ユーザ側では暗号化ＨＴＭＬファイルを得た後、まず、受信したファイルからアクセス制御情報とWWWサーバの秘密鍵証明書を取り出す。続いて、これらにユーザの秘密鍵証明書と属性証明書を付け加えて認証依頼を作成し、ＫＤＣに送る。

(4)認証応答

ＫＤＣはまず、受信した認証依頼に含まれるWWWサーバの秘密鍵証明書とユーザの秘密鍵証明書をＫＤＣの秘密鍵で復号し、WWWサーバの秘密鍵とユーザの秘密鍵を得る。次に、WWWの秘密鍵を使ってアクセス制御情報を復号し、閲覧許可属性とセッション鍵を取り出す。そして、この閲覧許可属性をユーザの属性証明書に含まれる属性が満たしていれば、セッション鍵をユーザの秘密鍵で暗号化して認証応答を作成する。満たしていなければ、エラー情報を暗号化して認証応答を作成する。最後に、この作成した認証応答をユーザに送る。

(5)暗号化ＨＴＭＬの復号

ユーザは、受け取った認証応答を自分の秘密鍵で復号する。認証に成功していた場合には、取り出したセッション鍵を使って暗号化したＨＴＭＬファイルを復号し、ブラウザに表示する。ユーザがWWWサーバの指定した属性を持っておらず認証に失敗した場合には、その旨のエラーメッセージを表示する。

4.3 実装方法

本システムのユーザ側の機能は、WWWブラウザのプラグインとして実装した。プラグインは、ダウンロードしたファイルのＭＩＭＥタイプごとに特定の処理を行わせる機能である。プラグインをサポートしているブラウザであれば、上記のアクセス制御機能を新規にブラウザを作成することなく容易に組み込むことができる。

5. まとめ

本報告では、秘密鍵暗号を用いたWWWの暗号化とアクセス制御について報告した。この暗号方式では、各ファイルに閲覧を許可する属性を指定し、ＫＤＣがユーザの属性を認証することでアクセス制御を実現している。そのため、企業における所属部署や役職の指定による情報の送付・開示形式に即しており、イントラネットでの使用に適している。

6. 参考文献

[1] 鮫島、宮崎：秘密鍵証明書・属性証明書を利用した暗号電子メールシステム：マルチメディア通信と分散処理ワークショップ論文集、情報処理学会、pp.85-92（1995）