5D-3

Web 上の機密情報漏洩防止システム

桐畑　康裕　　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

企業内で共有される情報として、人事情報や顧客情報等の機密情報があるが、そのような機密情報の格納されているデータベースに Web サーバ経由でアクセスできるようなシステムを構築することは、業務の効率化を図る上で有用である。

しかし、Client に送信された機密情報が外部に漏洩されることを禁止するシステムは数少ないのが現状であり、動的に機密データが生成されるシステムに対応するものは現在のところ考案されていない。

本稿では、Web サーバ経由で機密情報を閲覧できるが、機密情報を外部に漏洩することのできないシステムを提案し、その実装方法について検討する。

2. 機密情報漏洩防止システムの概要

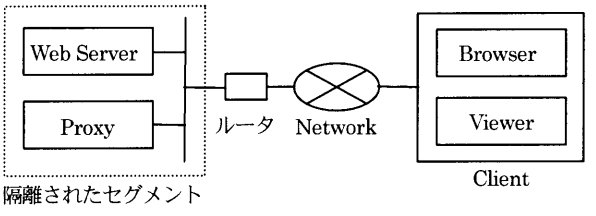

図 1　機密情報漏洩防止システムの構成図

本稿で提案する Web Server 上の機密情報漏洩防止システムの構成図を図 1 に示す。Proxy と Web Server は隔離されたセグメントに配置され、通信は SSL 等により安全であると仮定する。また、ルータの設定により、Client から Web Server へのアクセスは Proxy を経由して行われるものとする。Web Server は Proxy を認証し、Web Server 上の機密情報には Proxy しかアクセスできないように設定する。Viewer は Proxy で暗号化され送信された機密情報を復号して表示する。Viewer を用いることにより、Client にダウンロードされた機密情報の漏洩を防止する。

3. Viewerの設計

Client に送信された機密情報の漏洩を防止するために、Viewer は以下の機能を備える必要がある。

(1) Viewer に表示されたデータのコピー禁止
(2) Viewer 起動中のハードコピー禁止
(3) ダウンロードした機密情報を暗号化して保存

ネットワーク上で盗聴されることを防ぐために、Proxy でユーザごとに用意された鍵を用いて暗号化する。Viewer は Proxy で暗号化された機密情報を、復号表示する。これより送信された機密情報は、平文のまま他のファイルにコピーできないので、Client 外部に持ち出すことができない。また、機密情報は暗号化されて保存されるため、Viewer のない環境では機密情報を閲覧することができない。

4. Proxy の設計

Proxy は Client と Web Server を中継する位置にあり、Web Server へのアクセスは Proxy 経由でアクセ

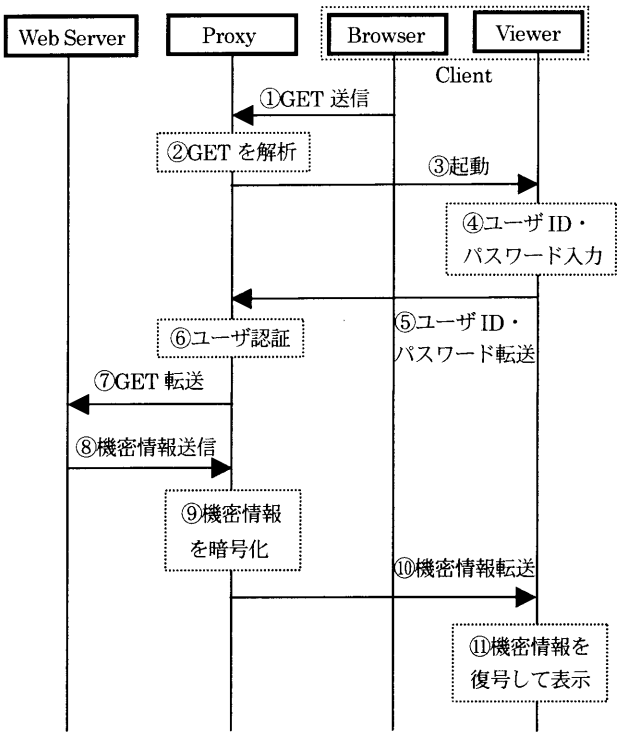

図 2　機密情報アクセスの際の Proxy における処理

A Web-based system for the prevention of the information leakage
Yasuhiro Kirihata, Hitachi Software Engineering Co.,Ltd.
Yoshiki Sameshima, Hitachi Software Engineering Co.,Ltd.

スする以外にはアクセスできない。このネットワーク構成により、Web Server への不正アクセスを防止する。

図2に Client から Web Server への機密情報アクセスの際の、Proxy における処理の流れを示す。これは、ユーザが機密情報を閲覧する際に、Web Server・Proxy ・Browser 及び Viewer の間で行われる一連の処理を時系列で表した図である。

Proxy には予め機密情報の URL を登録しておく。CGI 等で動的に機密情報が生成される場合には、機密情報が生成されるディレクトリに対応する URL を登録する。Proxy は、Browser から Web Server へ送信された GET リクエストを解析して、アクセス要求先の URL と予め登録されている機密情報の URL を比較し、機密情報へのアクセスか否かを判定する。機密情報へのアクセスの場合にはユーザ認証を行う。ユーザが認証されれば、Proxy は GET リクエストを Web Server に転送し、Web Server から機密情報をダウンロードする。そして、ダウンロードした機密情報を暗号化して Viewer に転送する。機密情報へのアクセスでない場合は、Web Server からダウンロードしたデータをそのまま Browser に送信する。

5. 機密情報漏洩防止システムの実装

5.1 Viewer の実装

Viewer での HTML の構文解析と表示には、既存の WebBrowser コントロール[1]を使用した。また、Viewer に表示された機密情報のコピー防止のために、Viewer にはコピー機能は実装せず、ハイライト選択も禁止した。ハイライト選択の禁止により、選択した表示データのドラッグ&ドロップによる他のファイルへのコピーを防止する。

5.2 Proxy の実装

Client からの GET リクエスト受付用のポート P1、及び Client からユーザ ID とパスワードを受付けてアクセス要求先の機密ファイルをダウンロードして暗号化し、Viewer に送信するためのポート P2 を生成する。Client からアクセス要求を受けると、Proxy は GET リクエストの記述された Viewer のファイルを送信し、Viewer を起動してユーザ認証ダイアログを表示させる。入力されたユーザ ID とパスワード、及び GET リクエストは P2 に送信され、ユーザ認証後機密情報が暗号化されダウンロードされる。

5.3 セキュアな通信の確保

Proxy と Client 間の通信を安全に保つために、Proxy で機密情報の暗号を行うが、暗号化に用いる鍵の管理スキームについて説明する。

予め、Viewer にはユーザ固有の秘密鍵、Proxy にはユーザ固有の公開鍵を登録しておく。最初のセッションでは、Proxy で生成されたセッション鍵を暗号化するための共通鍵は、Viewer の公開鍵を用いて暗号化され、Viewer に送信される。暗号化され、送信された共通鍵は、Viewer で秘密鍵を用いて復号化され、その後一定時間 Viewer に保管される。セッションが開始し、機密情報が送信されるごとに、機密情報に対応したセッション鍵を Proxy で生成し、そのセッション鍵を用いて暗号化して Client に送信する。暗号化に使用したセッション鍵もセッション開始時に生成した共通鍵を用いて暗号化し、Viewer に送信する。Viewer では保管されている共通鍵を用いてセッション鍵を復号し、復号されたセッション鍵を用いて機密情報を復号する。セッション鍵を暗号化するための共通鍵は一定時間後に消去される。消去された後に再びセッションを開始するときには、再び共通鍵の生成から始まって同様の処理を繰り返す。

6. 結論

本稿では、Web 上の機密情報閲覧システムを提案した。このシステムではデータベース等で動的に機密情報が生成される場合にも対応できる。また、Viewer・Proxy の実装を検討し、機密情報防止システムが構築可能であることを確認した。今後の課題としては、キャプチャツールによる画像コピーへの対応、HTML 以外の機密ファイルへ対応するための Viewer の機能拡張等が挙げられる。

参考文献

[1] D.Chappell, Understanding ActiveX and OLE, 1997.