オフラインで利用可能なセキュア・オンラインストレージの開発
ー 簡単操作でサーバからの情報漏洩を防止します ー

１．背景

企業においてオンラインストレージや Web 上の文書サーバを使う場合、社外にデータが持ち出されることや、内部犯行によるサーバ側からの情報漏洩が問題とされています。また、オンラインストレージはネットワークがなければ利用できないため、ちょっとした外出先で欲しいデータが手に入らないという不自由な場面にも遭遇します。

２．目的

このような問題を解決し、機密性、利便性、操作性、の３つを兼ね備えた次世代のオンラインストレージを開発します。具体的には、ユーザ側で暗号化と鍵管理の自動化を行いサーバ側からの根本的な情報漏洩対策を可能にします。また、ネットワークの接続を自動で検知しローカルとリモートを同期することでネットワークのないオフラインの環境でもオンラインストレージを利用可能にします。

３．開発の内容

図１は開発したソフトウェアの基本アーキテクチャ、図２はソフトウェアの画面キャプチャを表しています。

Web ブラウザのプラグインとして実装することで、アプリケーションのインストールの手間を短縮し、ActiveX を用いることで AES による高速な暗号化と、ドラッグ＆ドロップによる直感的なアップロード・ダウンロードを実現しています。

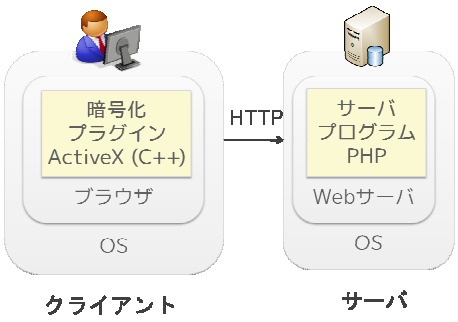

図１．基本アーキテクチャ

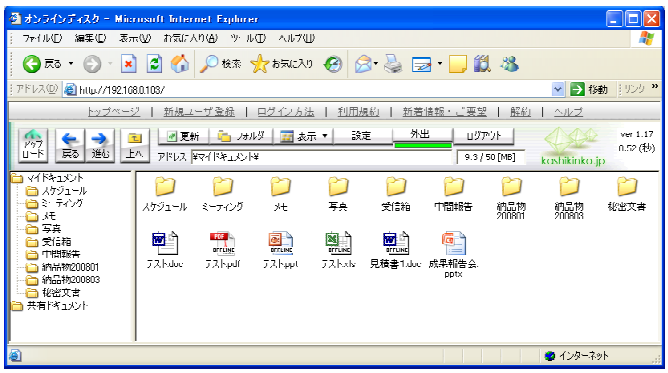

図２．画面キャプチャ図

３.１　暗号化機能

サーバ側で暗号化を行うのではなく、クライアント側で暗号化を行います。そのため、サーバ側からのデータが漏洩したとしても、ファイルはユーザの鍵で暗号化されているため、情報の中身の漏洩を防止することができます。また、暗号鍵はユーザのパスワードと乱数を元に自動で生成されるため、ユーザは面倒な鍵の管理は不要です。

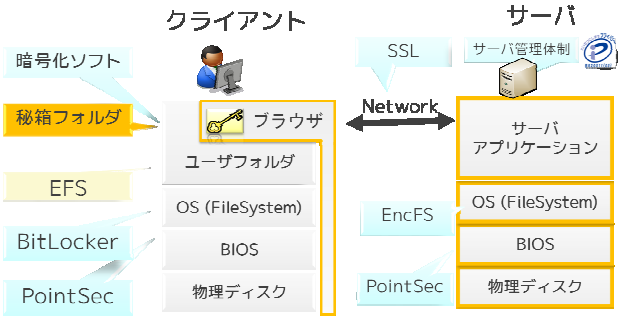

図３．暗号化レイヤ図

３.２　オフライン機能

従来は、ユーザがオンラインとオフラインを明示的に切り替える必要がありましたが、定期的なポーリング処理によって、自動でネットワーク状態を判断し同期を行うことが可能です。

また、図４の状態遷移を用いることで、通信エラーによるオフライン状態への自動移行だけでなく、ユーザは外出前に明示的にオフライン状態へ移行しローカルキャッシュを保持することもできます。

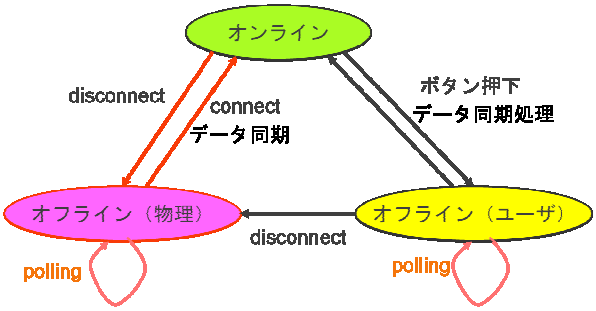

図４．オフライン・オンライン状態遷移図

４．従来の技術（または機能）との相違

・ ユーザ側でファイルの暗号化を行うことで、サーバの運用体制、ポリシーに依存せずに、サーバ側からの情報漏洩を根本的に防止します。
例えば、提案するソフトウェアを使用することで、信頼できないホスティング業者やサーバ管理者がいたとしても、安全にオンラインストレージを利用できるよ

うになります。

・ 次世代の技術として Google の「Google Gears」、Adobe の「AIR」等の「Web アプリのオフライン化」の注目を集めていますが、初の「Web オンラインストレージのオフライン化」を実現しました。自動でネットワークの接続／切断を検知し、サーバと同期を行います。

・ RIA (リッチインターネットアプリケーション) の技術を用いることで、Web ブラウザへドラッグ＆ドロップ等の直観的な操作性を持つオンラインストレージを実現しました。

5．期待される効果

・ 企業内における文書サーバ（オンラインストレージ）は、日常的に使うものであり業種を問わず汎用性が高く、特に企業間やプロジェクトの文書サーバなど、サーバ側からの情報漏洩リスクが高いため導入効果が高いと考えられます。

・ 提案するソフトウェアを公開することで、情報漏洩の可能性のあるホスティング業者や悪意あるサーバ管理者に対して、ファイルは利用者側で自動的に暗号化されてアップロードされるため、安全にオンラインストレージを利用できると考えられます。これは、サーバ運用における情報漏洩対策コストを下げることにもつながり、オンラインストレージ利用者の拡大による市場の活性化につながることも考えられます。

・ RIA（リッチインターネットアプリケーション）と呼ばれる Web ブラウザを使ったリッチクライアント環境でオンラインストレージが実現できたという実例となり、今後 RIA 技術の適用領域が拡大していくと考えられます。

6．普及（または活用）の見通し

・ 公開できる機能から順に随時下記サイトにて公開中。現時点での利用者数は約 1000 ユーザを突破。

7．開発者名（所属）

松本義秀（奈良先端科学技術大学院大学）

（参考）http://kashikinko.jp