ロールベースアクセス可能なオンラインストレージ

木下研究室　鈴川　朗広 (201002719)

1　はじめに

近年ではパソコンとインターネットの普及に伴い、数多くのディジタルコンテンツが多くの製作者によって作成されている。製作者は企業から一個人まで幅広く、製作されているコンテンツも数多く存在している。そんな時代の中それらのコンテンツを配信、利用するにあたり著作権の保護や利用の制限をどう取り扱うか、どのように制御していくのかが現代での大きな問題となっている。そこで、改善策の 1 つとして暗号化というものが行われている。暗号化とは通信内容や保管書類を読み取られないようにパスワードや鍵を掛けることによって、第三者からはそれらを解かなければ中の内容を見ることが出来なくなる。暗号化は現代の情報化社会には無くてはならないものである。その中でも本研究では属性ベース暗号を用いたシステムの提案を行う。

2　オンラインストレージ

近年多様されるようになり、注目されているものとしてオンラインストレージがある。これは文書、画像、動画などの様々なデータを保存し、他者に公開、共有することができるというものである。メールに添付できないような大容量ファイルも公開、共有することが可能であり、インターネットにつながる環境があれば時間、場所関係なく使用することができる。しかし、その一方でクラウドの利用者が保持する個人情報や顧客情報などの機密情報を扱うことが難しいという課題も発生している。

3　Xythos

Xythos とは、オンラインストレージの代表的な物の 1 つである。この Xythos のような共通のファイルで作業をするツールでは、共有されるドキュメントへのアクセスに対して、そのアクセス可能なメンバー全員に同じ権利が与えられている。これにより誤った編集、削除などから保護されないという問題点が起こることになる。Xythos は読み取り、書き込み、削除、管理の 4 種類のアクセス権で全てを管理している。

4　属性ベース暗号

属性ベース暗号とは個人の属性情報を利用して情報を保護する暗号方式である。例えばファイル作成時に「工学部のみ」、「4 年生のみ」といった公開範囲を指定して暗号化を行い、その指定された属性を持つ者のみがそのファイルを復号して閲覧できるという仕組みである。この方式はまず秘密鍵、公開鍵をペア作成し、公開鍵は公開し秘密鍵は自分で管理する。これにより、ある 1 つの暗号文に対して復号可能な利用者が複数存在できることにより、企業など大規模なクラウド上でのファイル共有システムへのアクセス制御等への応用が可能になる。

5　公開鍵暗号

公開鍵暗号とは暗号化に使用する鍵と復号に使用する鍵がそれぞれ違う鍵を使う方式であり、片方の鍵を相手に公開する暗号化システムである。これにより、1 つの鍵を公開しておけば誰にでもその鍵を使ってもらうことができるので、他数の相手とのやりとりを行うとき秘密鍵を管理しておくだけで済む。さらに公開鍵をどんなに調べても秘密鍵がどうなっているか分からず、秘密鍵で暗号化した文書は公開鍵でないと元に戻せない。 逆に公開鍵で暗号化することもできるけれどもそれは秘密鍵でないと元に戻せない。

6　提案

属性ベース暗号

7　まとめ

本稿では、属性ベース暗号をオンラインストレージの 1 つ Xythos の暗号化に取り入れたシステムの提案をした。