平成25年度卒業論文

論文題目

オンラインストレージでの利便性、安全性双方を求めたシステムの提案

神奈川大学　工学部 電子情報フロンティア学科
学籍番号　201002719
鈴川　朗広

指導担当者　木下宏揚　教授

目 次

図 目 次

第1章　序論

1.1　背景

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。

1.2 著作権

インターネット上での著作権問題は非常に難しく、解決は困難とされている。そもそも著作権とは、思想または感情を創作的に表現したものであって、文芸、学術、美術または音楽の範囲に属するもの。とされているが、インターネット上でディジタル化されたデータはパソコンひとつあれば複製品を製作できてしまうし、インターネットを利用してディジタルデータをパソコンを通して世界中に向けて発信することもできる。誰でも容易に製作者になりえて、誰でも容易にその複製などを行える為、今では著作権に関しての法律が追いついていないという状況にある。
インターネット時代の都合に合わせて、今では製作者の意図に従えばコンテンツの二次利用が利用者に一任されるようなものもある。しかし、それでも製作者と利用者の距離を縮めるにはまだ難しく、例えば利用者が製作者の考えや意図を理解したつもりでいても、製作者側が実はそれを認めていなかったなどの事例も数多い。

1.3 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の 1 つに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だ。インターネットにつながる環境があれば、時間、場所関係なく行うことができる。さらには、自分のパソコンに問題が起こった場合でもデータを失うことはなく、これは便利でもあり、また注意しなければならない問題でもある。
オンラインストレージが使われる背景の例に、自組織で情報システムを維持するより他組織での情報システムを利用したほうがピーク時の負荷によって設計を行う必要があり初期費用、運用費が高くな

るという理由がある。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。

1.4 問題に対する研究

オンラインストレージサービス等に関する問題として、これまでユーザの手元のパソコンで行われてきた行為を著作権法がどこまで許容するかどうかの問題、サービス提供内容の違いによって管理者の責任が不明確である問題、私的使用をどこまで許容するかの問題、公衆送信の範囲をどのように解釈するかという問題、などの問題として整理することができる
第 3 者が運営、利用するクラウド上では、機密情報などのデータを管理することは難しい。そこで、クラウドの持つ拡張性やシステム利用者や、またその負荷に応じた柔軟性を活かし、且つ慎重、安全を求めたシステムがあるといいと思う。これらを踏まえた上で、オンラインストレージ上での安全性と利便性の双方を追求し、クラウド技術の利点を活かしつつ、高い安全性を確保するためのソリューションとして、インテックでは安全なオンラインストレージシステム Sola について着目する。

第2章　予備知識

2.1　ディジタルコンテンツによる著作権の問題点

まず、ディジタルコンテンツによる著作権の問題点として、複製、流通が誰でも非常に簡単に行われてしまうことがあがり、さらには加工、改変も簡単に行えるという問題がある。

2.1.1　DRM

DRM（Digital Rights Management）とは、ディジタル著作権管理のことであり、ディジタルデータとして表現されたコンテンツの著作権を保護し、その利用や複製を制御、制限する技術の総称。これはコピーなどを制限する関係上、私的複製なども阻害してしまう可能性が発生する。

2.1.2　既存のオンラインストレージシステム例

ユーザインターフェイスと暗号化機能により、いくつかの型に分類できるものとして、
・OS統合型、暗号化なし
・専用ソフト型、暗号化なし
・OS統合型、サーバ型で暗号化
・専用ソフト型、サーバ側で暗号化
・OS統合型、クライアント側で暗号化
・専用ソフト型、クライアント側で暗号化
がある。

その中の、OS 統合型、クライアント側で暗号化とは、OS 標準の機能を用いクライアント側で暗号化を行うものである。クラウド上のサーバ側にファイルを送信する前にクライアントが保持する鍵を用いて暗号化を行う。サーバ側には暗号文のみ保持する。鍵はクライント側のみに存在しネットワーク上には送信しない。
このとき、クラウド上のサーバが不正アクセスを受けた場合情報漏えいするのは暗号文のみになる。つまり鍵が保持されている限りファイルの中身にアクセスすることはできない。
今回着目しているSolaとはこの、OS 統合型、クライアント側で暗号化で行う方式を採用している。

2.1.3 Sola

Solaとは、高い安全性を確保するためのソリューションとしてのオンラインストレージでの提案システムの 1 つである。Sola はクラウド技術と暗号を活用することで、仮想的なストレージ領域を安全に提供するシステムで。また、OS 統合型のクライアントソフトウェアとして動作し、クライアント側で暗号化および復号の処理を行うことで、暗号化のための鍵やファイルの中身などの秘密の情報がいっさいネットワーク上に漏洩しない点に特徴があるオンラインストレージシステム。
OS 統合型のクライアントソフトウェアとして動作し、クライアント側で暗号化、複合の処理を行うことにより、暗号化のための鍵やファイルの中身などの秘密の情報がネットワーク上漏洩しない.。

図 2.1: Sola の概要

2.1.4 クラウド鍵管理型暗号技術

クラウドに復号処理をアウトソースさせる技術であり，利用者は復号鍵を管理することなくデータを保護することが可能。復号処理をクラウドに委託して制御することによりいったん流通した暗号データの読み取りも、後から必要に応じて許可・禁止することが可能。

2.1.5 暗号化

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い。現代の情報化社会には無くてはならないものである。

2.1.6 2段階認証

2段階認証とは、情報漏洩によりパスワードが漏れた場合でも、アカウントの不正利用を防止できることができるものである。仕組みとしてはまずPCによりパスワードの入力を行い、それにより使用端末にメールなどで送られたコードを受け取り入力を行う。このように、自分が保管したパスワードと携帯電話などの端末2回のプロセスを行うことでセキュリティ面を強くすることができる。しかしその反面手間がかかることになり利便性が損なわれることになる。

2.1.7 TrueCrypt

TrueCrypeとは、暗号化された仮想ディスクの作成、利用を無料で使用できる暗号ソフトである。仮想ディスクはファイルとして作成するだけでなく、パーティション自体も対象にできる。Windows版TrueCrypt ではシステムドライブ自体も暗号化することが出来る。パソコンを紛失し、万が一ハードディスクからデータを引き出されそうになっても、暗号化されていることで防止することができる。また、マウントした仮想ドライブへアクセスすると、自動で暗号化・復号を行うので、ユーザは暗号化／復号を意識する必要がなく暗号化ソフト初心者に最適である。

2.1.8 Xythos

神奈川大学でも導入されている情報系システムであり、学内情報の共有・活用をしているWeBSt@tionでこのXythosが使用されている。LDAPやActive Directoryなどのディレクトリと連携したユーザー認証とアクセス制御が可能であり、学内外で情報共有できる環境下でユーザーごとにアクセス権限を設定できるXythosが選ばれている。「限られたリソースで運用していくことも考え合わせると、サーバ側で添付ファイルの一括管理ができれば、ファイルサーバの容量削減やメールサーバの負荷軽減、クライアント端末のディスク容量節減にもつなげられている。

2.1.9 チケット機能

Xythosなどのオンラインストレージでアカウントの無いユーザに対して、一時的なアクセス権を発行する機能。これを使用することで顧客、依頼者などに営業資料の配布や外注先からの納品物の受け取り等で、自分が所属する組織外のユーザとファイルを授受するなどの一時的な取引の場合、そチケット機能を利用することで一時的なアカウントをユーザ自身が発行する事が可能です。アクセス権としては、チケット作成画面にて、ファイル/フォルダへのアクセス権として 読み取り専用または読み取り/書き込み/削除のいずれかの選択を要求され、 この情報がファイル/フォルダのアクセス権画面に格納される。また、チケットを作成する時パスワードを設定することができる。 パスワードを設定するとパスワードで保護されたチケットリンクが送信され、 パスワードのないチケットリンクは送信されない。チケット機能には有効期間を設けるのが基本であり、設定されたチケットの有効期間が経過すると、チケットでアクセスしていたユーザは対象のファイル/フォルダへアクセスすることができなくなる。これらによって情報漏洩防止に繋げているのだが、情報を一時的とはいえ外部に漏らすことになるため完全な安心を得られるとは言い難いものである。

2.1.10 検索可能暗号

データを暗号化したまま検索する暗号技術。検索対象データだけではなく検索キーワードも暗号化したまま処理できることで、クラウド上のデータを安全且つ利便性にも優れたものとして注目されている。

第3章　提案システム

3.1　提案

Sola を参考に、
・情報同期プラットフォームの確立。
・共有内共同作業でのアクセス制御。
・検索可能暗号。などを絡めたさらなる利便性を向上させたシステムを提案したい。

3.1.1　課題

チケット使用時の情報漏洩ポイントを理解し、セキュリティの改善を行いたい。
データセンターに預ける利点・難点を理解し双方の情報漏洩発生の危険箇所、またその改善ができるかの検討を行いたい。
オンラインストレージでのさらなる安全性・利便性を求められるところを見つけ、改善できるかの検討を行いたい。

第4章　質疑応答

Q 1
チケット使用時のセキュリティ保護に着目に、改善していきたいと言っていたが具体的な案はあるのか？
A1
今現在具体的な案は無いので、今後の研究でチケット使用時の情報漏洩ポイントを見つけそこから改善点を見つけていくつもりです。
Q2
データセンターからの情報漏洩の危険性を防ぐ方法としてSolaを利用するかどうかと言っていたが、Sola以外の方法は今現在考えているのか？
A2
今後の研究で見つけていくつもりです。

関連図書

[1] 野尻祐亮， 金井遵， 並木美太
オンラインストレージを用いた分散仮想ディスクの開発 (分散ファイル・システム)

[2] 永見健一， 伊波源太， 笹川浩， 脇谷康宏
セキュアなオンラインストレージシステムの提案

[3] 山口　誉央
著作権管理のための Bee-gent による仲介システム

[4] 川村隆浩， 田原康之， 長谷川哲夫， 大須賀昭彦
Bee-gent:移動型仲介エージェントによる既存システムの柔軟な活用を目的としたマルチエージェントフレームワーク

[5] 桑名栄二
NTT 情報流通プラットフォーム研究所　所長
変化する環境とサイバーセキュリティ]

[6] IISEC（情報セキュリティ大学院大学、学長：田中 英彦）暗号技術の導入による機密情報の適切な保護方式の研究～グローバル社会における持続的な経済発展のための基盤技術として～

[7] 後藤めぐ美, 大東俊博, 西村浩二, 相原玲二
属性ベース暗号を利用したファイル名暗号化ファイル共有サービス

[8] On THE Security of Cloud Storage Services