L-012

クラウド上における秘密分散法の実装
Implementation of Secret Sharing Scheme in the Cloud

井上 開斗† 坂﨑 尚生†
Kaito Inoue Hisao Sakazaki

1. はじめに

近年では、データを保存する方法としてクラウドストレージが注目されている[6]。主なクラウドサービスには、Google が提供している Google Drive やマイクロソフト社が提供している OneDrive 等がある。このようなクラウドを利用することで業務の効率化が期待できる。

利便性や運用効率の向上を目指す企業にとっては、クラウド利用は選択肢の一つとなっている。特に会社の機密情報などの重要なデータもオンプレミスからクラウドへ移行する企業は年々増加している。但し、機密情報を扱う為、十分にセキュリティについて考慮する必要がある。

そこで、日本では新たな情報セキュリティの概念として、ゼロトラストの導入を推進している[7]。従来のセキュリティでは境界内部を信用し、境界外部を信用しないという考え方であった。それに対してゼロトラストは、社内外のネットワーク環境における、従来の境界の概念を捨て去り、守るべき情報資産にアクセスするものはすべて信用せずにその安全性を検証することで、情報資産への脅威を防ぐという、セキュリティの新しい考え方である。ゼロトラストの考えを基にクラウドの運用を行うことにより、クラウド上での機密情報管理も安全に行うことができる。

一方、クラウドを利用する場合、ユーザがアップロードしたデータはクラウドの運営側が管理している。すなわち、クラウドの運営側は、理論上、ストレージに保存してある機密情報をいつでもアクセスできる状態にある。ゆえに、クラウドに重要な機密情報を保存する場合は、データの暗号化などを考慮する必要がある。データの機密性を担保する技術として暗号化[4][5]や秘密分散法[1][2][3]などが存在する。尚、主な暗号方式は、計算量的安全性に基づいて構成されているゆえ、計算機能力の向上によっては、いずれ解読される可能性がある。

一方、秘密分散法は、1979 年に Blakley[1]と Shamir[2]により独立に発表された情報保護技術である。基本方式である Shamir の(k,n)閾値法を例にとると、Shamir 法は、秘密情報をn個の分散情報に分割し、n個の分散情報の中から任意のk個集めれば元の秘密情報が復元できるが、$k-1$個以下の分散情報からでは元の秘密情報に関する情報がまったく得られないという特徴がある[2]。また、情報理論的安全性に基づいて構成されている為、計算機能力の向上によって解読されることがない。加えて、データのバックアップとしても利用することができる。

Shamir 法は代表的な秘密分散法であるが、秘密情報の分散及び復元において k-1 次多項式の計算を行う必要がある。それに対して藤井らは排他的論理和を用いた(2, n)秘密分散法を提案した[3]．藤井らの方式は，XOR 演算のみを用いる為，非常に高速に処理できる．

秘密分散法をクラウド上に実装することで、データの機密性を向上させることができる。しかし、主なクラウドサービスでは、秘密分散法は実装されていない。その理由として、以下のことが考えられる。

1. クラウド運営側が秘密分散法の必要性を説くことは、クラウドの機密性が運営側によって損なわれている可能性があると言っているようなものである。
2. クラウド運営側からデータの機密性を担保する為には、秘密分散法は同一運営内で行っても意味がない。それ故、複数の異なるクラウドで協力して秘密分散法を実装する必要がある。しかし、顧客の囲い込み等、運営側の利益追求を考慮すると競合他社との協力は難しい。

これらの理由から、クラウド運営側が秘密分散法を自社サービスに適用することは、難しいと考える。

上記状況に鑑み、本研究では、クラウド運営側でなく、クライアント側で簡単にクラウド上での秘密分散法を実現ですることが重要と考え、クライアント側設定による秘密分散システムを設計しプロトタイプシステムを開発した。

2. 関連技術

2.1 排他的論理和型秘密分散法（XOR 法）

代表的な秘密分散法として、Shamir 法[2]と XOR 法[3]が存在する。このうち Shamir 法は、処理の過程で$k-1$次多項式を処理する必要がある。一方 XOR 法は、ビット毎の XOR のみで処理を行うことができる為、Shamir 法と比べて高速処理が可能である。

本研究では、様々な企業データをクラウド上で管理することを想定している為、高速処理が可能な XOR 法の適用を検討した。以下では、XOR 法について説明する。

XOR 法は、アルゴリズムが単純であり、ビット毎の排他的論理和のみで秘密分散法を実現することができる。その為、大容量データを処理するのに適している。

ここでは簡単の為、(2,3)閾値法を例として説明する。藤井らの(2,3)閾値法では、秘密情報 M を 2 個に分割する$(\mathrm{M}=\{\mathrm{M}_1,\mathrm{M}_2\})$。また別途$M_0=0$を用意する。

次に 2 個の乱数$(\mathrm{R}_0,\mathrm{R}_1)$を独立かつランダムに選び、3 つの分散情報（以降 Share と呼ぶ）S_0,S_1,S_2を以下のように計算する。

$$S_0=\{S_{00}=\mathrm{M}_0\oplus R_0\ ,S_{01}=M_2\oplus R_1\}$$
$$S_1=\{S_{10}=\mathrm{M}_1\oplus R_0\ ,S_{11}=M_0\oplus R_1\}$$
$$S_2=\{S_{20}=\mathrm{M}_2\oplus R_0\ ,S_{21}=M_1\oplus R_1\}$$

復元においては、例えばS_0とS_1から以下のようにして元の秘密情報Mを復元する。

$$M=\{M_1=S_{00}\oplus S_{10},M_2=S_{01}\oplus S_{11}\}$$

また、S_0とS_2の場合、以下で復元できる。

† 玉川大学 Tamagawa University

$$M = \{M_2 = S_{00} \oplus S_{20}, M_1 = S_{01} \oplus S_{21} \oplus M_2\}$$

また、S_1とS_2の場合以下で復元できる。

$$M = \{M_1 = S_{11} \oplus S_{21}, M_2 = S_{10} \oplus S_{20} \oplus M_1\}$$

2.2 クラウドストレージ

クラウドストレージは、オンライン上でファイル共有を行うことができるサービスのことである[6]。従来のように、ローカルな PC にデータを保存する代わりに、インターネット上のサーバなどにデータを保存することができる。また、インターネット上の保存場所には複数のデバイスでアクセスすることができる為、必要なときにどこからでもデータをダウンロードすることができる。クラウドストレージは種類によって異なる容量や料金体系を持っている。したがって、利用目的やニーズに応じて利用するサービスを選択することが重要である。

以下では、代表的なクラウドストレージについて簡単に説明する。

2.2.1 Google Drive

Google Drive は、Google 社が提供するクラウドストレージである[8]。このサービスは Gmail などといった他の Google サービスと深く連携している為、幅広い利用ができる。また、Google のセキュリティ機能とプライバシー保護機能が組み込まれている為、高い安全性を提供している。データの暗号化や二要素認証などの機能も備えており、情報の保護に対する信頼性も高い。また、データのバックアップと復元を自動的に行うことも可能である。

Google Drive の容量は、無料プランでも 15GB を使用することができ、有料プランではさらに追加の容量を利用することができる。

モバイルアプリからも簡単に利用することができ、共有リンクの作成も可能である。その為、ファイルやフォルダの共有及び同期をスムーズに行うことができる。Google Drive は利用しやすく信頼性の高いクラウドストレージであり、多くのユーザに利用されている。

利用するには、Google アカウントを作成して Google Drive にログインする必要がある。アカウント作成後は、Google Drive の Web ページかローカルの G ドライブからサービスを利用することができる。

2.2.2 OneDrive

OneDrive は、Microsoft 社が提供するクラウドストレージである[9]。OneDrive は、Windows OS や他の Microsoft Office サービスと連携している。ファイルの同期機能を備えており、複数のデバイス間でファイルを自動的に同期することができる。また、バックアップが行われる為、データの保護も行われる。モバイルアプリからのアクセスも可能である為、時と場所を選ばずにデータにアクセスすることができる。

容量は、無料プランでは 5GB のストレージを利用することができる。有料プランでは追加のストレージとして 1TB までのストレージを利用することができる。

利用するには Microsoft アカウントの作成が必要である。アカウント作成後、OneDrive にログインすることで、OneDrive の web ページか C ドライブの User にアクセスすることで利用することができる。

2.2.3 Dropbox

Dropbox は、Dropbox 社が提供するクラウドストレージである[10]。デスクトップアプリケーションやモバイルアプリからのアクセスが可能であり、ファイルへのアクセスと同期をスムーズに行うことができる。データの暗号化、二要素認証に加えてリンクのパスワード保護を行うことができる為、セキュリティ機能が充実している。Slack や Zoom といった他のツールとの同期をすることもできる。

容量は、無料プランでは 2GB のストレージを利用することができる。また、有料プランでは更なる追加ストレージを利用することができる。

利用するには、Dropbox アカウントを作成する必要があり、アカウント作成後、公式 Dropbox の Web ページにログインすることでサービスを利用することができる。また、C ドライブの User にアクセスしても Dropbox を利用することができる。

2.2.4 Amazon Simple Storage Service (Amazon S3)

Amazon S3 は、Amazon Web Service（AWS）が提供するクラウドストレージである[11]。オブジェクトストレージと呼ばれる形式でデータを保存している。オブジェクトストレージは、データをオブジェクトという単位で扱う記憶装置のことである。メリットとして、データの検索性が高いことや OS への依存性が低いことがあげられる。

容量は、12 か月間の無料枠として 5GB が用意されている。有料プランでは更なる追加ストレージを利用することができる。特に、企業向けの大容量データの保存やバックアップに利用される。

しかし、無料プランでも支払い情報を入力する必要がある為、普段使いの間隔で利用するには敷居が高い。

利用するには、AWS アカウントを作成後、AWS にサインインする必要がある。その後、支払い情報等を登録することで、クラウドサービスを利用することができる。

3. 設計と実装

本研究では、Google Drive、OneDrive、Dropbox の 3 つのクラウドストレージと XOR 型による(2,3)閾値法を利用し、クライアント側設定によるクラウド上で簡単に秘密分散法を実現する仕組みを開発した。また、開発方針として以下の 4 つを定めた。

① クライアント側だけで 簡単に秘密分散の環境設定ができること。
② 簡単に分散処理を行うことができること。
③ 簡単に再構築処理を行うことができること。
④ 閾値以上の Share から正しく元のファイルを復元できること。

本システムは、分散フェーズと再構築フェーズの 2 つのフェーズに分かれている。分散フェーズでは、ファイルの秘密分散を行い、Share を各クラウドに保存する。再構築フェーズでは、各クラウドから Share を取得し、正しく取得できた 2 つの Share を用いてファイルの復元を行う。

図 1 は、本システムのディレクトリ構造を示した図である。C ドライブの下には秘密分散を利用する為の SSS（Secret Sharing Scheme）フォルダを設置した。SSS フォル

ダは、実行ファイルが格納されている bin フォルダ、プログラム実行中の一時ファイルを格納する temp フォルダ、秘密情報を保存する SSSDrive フォルダの 3 つのフォルダから成る。bin フォルダ内には分散プログラムである SSSDist.java と復元プログラムである SSSRest.java が格納されている。temp フォルダは、分散及び復号の際に生成される一時ファイルの格納場所である。ユーザは、作業領域である SSSDrive フォルダにデータを保存することで、クラウド上での秘密分散を行うことができる。なお、One Drive と Dropbox は C/User の下にあり、Google Drive は G ドライブの直下に設定した。

ここで開発した Java プログラムの詳細を説明する。

SSSDist.java は、ファイル読込、分散処理、ファイル出力、bat ファイル生成機能から成る。ファイル読込機能は、引数として入力したファイルを SSSDrive フォルダから読み込む機能である。また、分散処理は、入力したファイルに対して秘密分散を行い Share に変換する。ファイル出力機能は、生成した Share を各クラウドに出力する。bat ファイル生成機能は、“再構築プログラムを起動する為の AAA.docx.bat”を SSSDrive フォルダに生成する。また同時に“元ファイルを SSSDrive 上から削除する DistDel.bat”、“再構築処理後、再構築したファイルを自動的に画面に表示する Activation.bat”、“不要な一次ファイル等を削除する DeleteAllShare.bat”を temp フォルダに生成する。また、SSSRest.java は、ファイル読込、再構築処理、ファイルの出力から成る。ファイル読込は、各クラウド上の Share を temp フォルダにコピーし、その Share を読み込む。再構築処理は、読み込んだ Share を用いて元ファイルの再構築を行う。ファイル出力では、復号したファイルを SSSDrive フォルダに出力し、SSSDist.java で生成した Activation.bat、DeleteAllShare.bat を実行させる。

以下では、簡単の為に AAA.docx という名前のワードファイルを本システムに適用した場合の流れを、順を追って説明する（図 2 参照）。

＜分散フェーズ＞

(1) ユーザは作業領域 SSSDrive フォルダにて作業を行い、秘密分散したいファイルを保存する。
(2) コマンドプロンプトを立ち上げ、bin フォルダ内の SSSDist.java を起動する。その際、ファイル名を引数とする。
(3) 引数に入力したファイルが存在した場合には分散プログラムが実行される。
(4) 分散処理が行われ、元のファイルから 3 つの Share がメモリ上で生成される。
(5) 生成された 3 つの Share はそれぞれ Google Drive, OneDrive, Dropbox の 3 つのクラウドストレージに保存される。
(6) 再構築プログラム起動用の bat ファイルを生成し、SSSDrive 内に保存する。この時、bat ファイルは、元ファイルの名前を引き継ぐ。例. AAA.docx.bat
(7) 最後に DistDel.bat が起動し、元ファイル（AAA.docx）が SSSDrive 上から消去する。

＜再構築フェーズ＞

(1) SSSDrive 内の bat ファイル（AAA.docx.bat）をダブルクリックする。bat ファイルにより再構築処理である SSSRest.java が起動する。

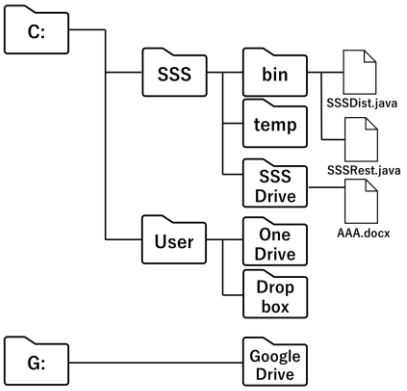

図 1. ディレクトリ構造

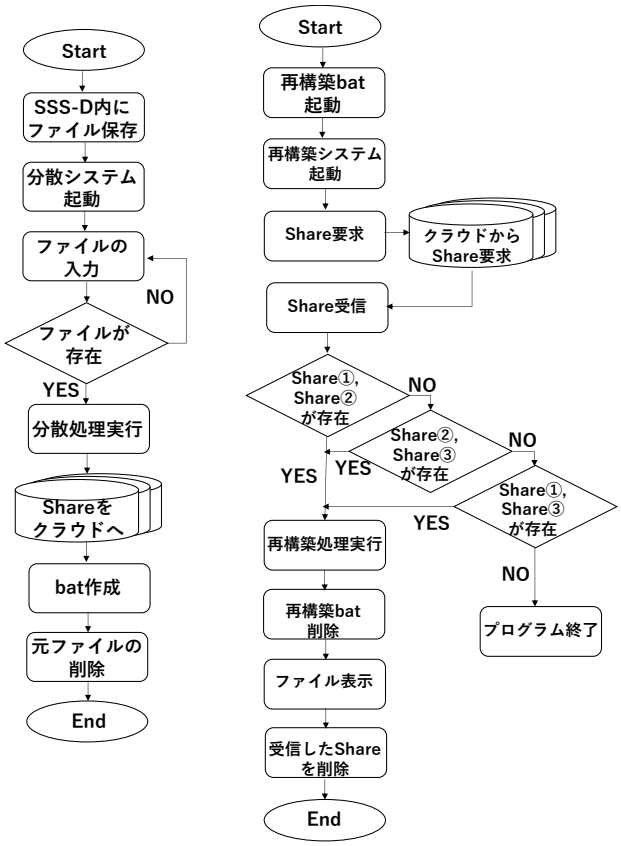

図 2a. 分散フェーズ　　図 2b. 再構築フェーズ

図 2. アクティビティ図

(2) 再構築処理では、3 つのクラウドにアクセスし、3 つの Share を temp フォルダ内にコピーする。
(3) まず、Share1 と Share2 のペアを用いて再構築処理を試みる Share1 または Share2 が存在しなかった場合、Share2 と Share3 のペアを用いて再構築処理を試みる。Share2 と Share3 のペアが存在しなかった場合、Share1 と Share3 で再構築処理を試みる。尚、3 つの Share のうち、2 つ以上の Share が存在しない場合は、再構築失敗とし、例外処理を行う。
(4) SSSRest.java は 2 つの Share より元ファイル（AAA.docx）を SSSDrive に復元する。

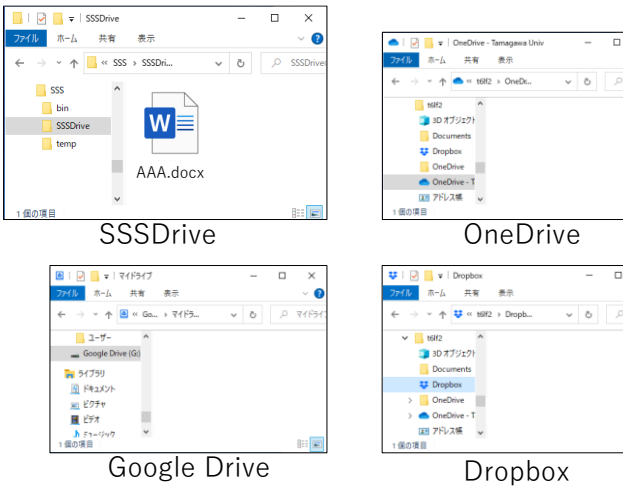

図 3．各ストレージ（分散前）

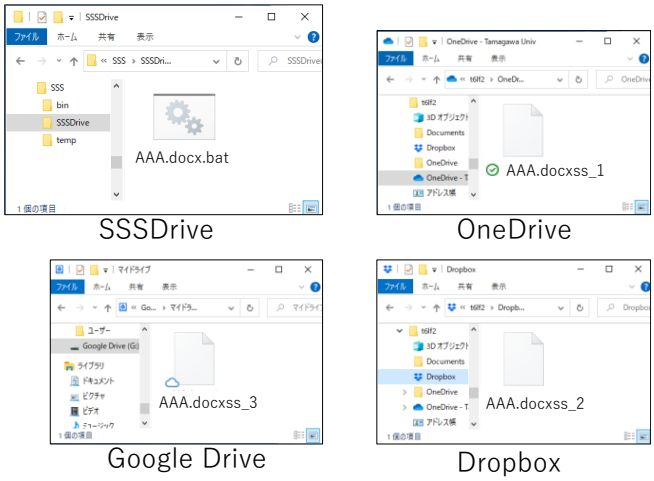

図 4．各ストレージ（分散後）

(5) 元ファイル復元後、SSSDrive から復元用の bat ファイル（AAA.docx.bat）を削除する。
(6) 再構築処理後は、Activation.bat を起動し復元したファイル AAA.docx を画面に表示する。
(7) 最後に DeleteAllShare.bat を起動し、temp フォルダの Share を削除し、処理を終了する。

図 3 および図 4 は、分散処理前後の SSSDrive フォルダ、および 3 つのクラウドストレージの内部を示した図である。図 3 では、SSSDrive フォルダ内に分散したいファイルである AAA.docx が入っている。分散処理終了後では、AAA.docx は Share に変換され、各クラウドに移動する。代わりに SSSDrive 内には AAA.docx.bat という bat ファイルが保存される（図 4）。ファイルを復元する際には、SSSDrive 内の bat ファイルを立ち上げることによって、再構築処理が実行され、元のファイルを復元することができる。

4. システム評価

ここでは、プロトタイプシステムの評価を行う。先に示した通り、本システムは以下の 4 つの開発方針に従って実装した。

① クライアント側だけで 簡単に秘密分散の環境設定ができること。
② 簡単に分散処理を行うことができること。
③ 簡単に再構築処理を行うことができること。
④ 閾値以上の Share から正しく元のファイルを復元できること。

環境設定は、java の動作と各クラウドを利用できることが必要である。クラウドは先に示した利用方法に基づいてアカウント作成を行うことで利用することができる。これらの設定は、秘密分散環境としてクラウド運営側にお願いすることなく、クライアント側で簡単に設定できる。

プロトタイプにおいては、分散フェーズにおいて 1 度のコマンド入力のみで元ファイルの分散処理が可能である。プロトタイプでは、コマンドプロンプトによるコマンド入力を必要としたが、ファイル保存と同期したり、定期的に SSSDist.java と連携したりして、分散処理の起動を簡略化することも考え得る。

再構築処理では、SSSDrive にある bat ファイルをダブルクリックするだけで元ファイルを復元することができ、また復元されたファイルが自動起動される。これにより、ユーザは秘密分散を意識することなく、通常のファイル操作と同様にファイルの閲覧・更新等が可能になる。

また、3 つの Share のうち、2 つ以上の Share が存在する場合、元ファイルを復元することも確認した。

5. おわりに

本論文では、クラウドストレージのユーザ側で簡単に秘密分散法を行うことができるサービスを開発した。ユーザは分散時に 1 度のコマンド入力が必要であるものの、比較的簡単に秘密分散法を利用することができる。

今後、すべての操作においてコマンド入力が必要とならないよう、サービスの UI 化などを行う予定である。

参考文献

[1] G. Blakley, “Safeguarding cryptographickeys”, Proc. AFIPS, vol. 48, pp.313 317, 1979.
[2] A. Shamir, “How to share a secret”, Commun. ACM, 22 (11), pp.612 - 613, 1979.
[3] 藤井ら“高速な (2, n) 閾値法の構成法とシステムへの応用”, CSS2005, 8C 2, 2005.
[4] R. L. Rivest, A. Shamir and L. Adleman, “A Method for Obtaining Digital Signature and Public-Key Cryptosystems,” Communications of the ACM, Vol. 21, No. 2, 1978, pp. 120-126.
[5] NIST, Announcing the ADVANCED ENCRYPTION STANDARD (AES), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
[6] 平成 30 年度版情報通信白書, 総務省, https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/pdf/30honpen.pdf
[7] ゼロトラストアーキテクチャ適用方針, デジタル庁, https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5efa5c3b/20220630_resources_standard_guidelines_guidelines_04.pdf
[8] Google Drive, Google, https://www.google.com/intl/ja/drive/
[9] OneDrive, Microsoft, https://www.microsoft.com/ja-jp/microsoft-365/onedrive/online-cloud-storage
[10] Dropbox, Dropbox, https://www.dropbox.com/
[11] AmazonS3, Amazon https://aws.amazon.com/jp/s3/