様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　５　月　２２　日現在

機関番号：　１１３０１
研究種目：　若手研究(B)
研究期間：　2013～2014
課題番号：　２５８７００５３

研究課題名（和文）複数のクラウドを利用した高い安全性を実現するクラウド支援ソフトウェアの開発

研究課題名（英文）Developent of a Support Software for Making Cloud Storage Secure

研究代表者
長谷川　真吾（HASEGAWA, Shingo）

東北大学・教育情報基盤センター・助教

研究者番号：８０５６７２１４

交付決定額（研究期間全体）：（直接経費）　　1,200,000円

研究成果の概要（和文）：個人向けクラウドストレージに保存されるデータには、そのサービスの性質上、覗き見・消失・改ざん・漏洩といったリスクが存在する。本研究では、このようなリスクを克服するため、保存データを秘密分散共有技術により分割し、複数の異なるクラウドストレージに分散して保存するソフトウェアを開発し、その性能評価を行った。開発ソフトウェアはパスワードマネージャなど、高い安全性を要求されるアプリーケションへの利用が効果的である。また、基幹技術である秘密分散法をより強固にするパスワード付秘密分散法の開発も合わせて行った。

研究成果の概要（英文）：On the cloud storages for personal use, there are several risks about the stored data such as steal, loss, falsification and leak. In this research, in order to avoid such risks, we develop a software such that it divides data to multiple shares by using the secret sharing scheme and uploads them to different multiple cloud storages, and also evaluate the performance of it. The developed software is useful for applications which require high security, such as the password managers. We also develop the password-protected secret sharing schemes which are enhanced schemes of secret sharing schemes.

研究分野：　情報セキュリティ

キーワード：　セキュリティ　クラウドコンピューティング　秘密分散法

１．研究開始当初の背景

LTE などの高速通信や、BYOD と呼ばれる私的デバイスの業務利用の拡大に伴い、Dropbox や Google Drive などに代表されるクラウドストレージサービスの普及が急速に進んでいる。そのメリットとして、使用する端末やユーザーによらず、同じファイル、および作業環境を複数の環境で同期構築できることが挙げられる。しかしながら、クラウドストレージサービスの業務利用には保存データの秘匿性やサービスの安定性といった課題が存在する（図 1）。実際、2012 年 6 月に発生したファーストサーバ社の障害においては、長期間に渡りサービスが停止するだけでなく、その保存データのほとんどが失われるという事態に陥った。また、保存データの喪失を免れたとしても、クラウド上のデータを第三者に盗聴されないか、というリスクが存在する。例えば, Google 等はユーザサービス向上の名目でユーザーのデータを走査することを宣言しており、業務上の秘密がクラウド事業者の不正行為を通じて第三者に流出する危険が存在する。

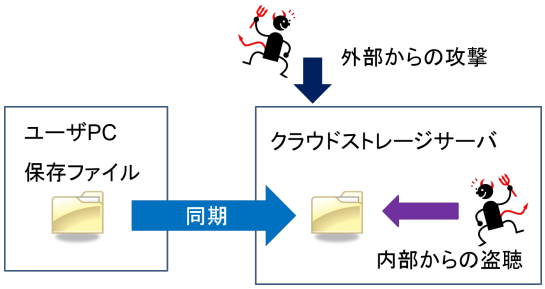

図 1 クラウドストレージのリスク

これらのリスクに対抗するための手段として、データに暗号化処理や秘密分散共有処理を施してからクラウド上に保存する仕組みが提案されている。前者については, Cloudfogger に代表されるクラウドストレージと連携した自動暗号化ソフトウェアがあり、 後者については、平成 22 年度産業技術研究開発委託費、次世代高信頼・省エネ型 IT 基盤技術開発事業として医療カルテ情報に秘密分散共有処理を施してからクラウド上に保存するというプロジェクトが進められている。しかしながら、これらの対策を採用しても、単一のクラウド事業者を利用している状況は変わっていないため、事業者のサービス安定性に関わるリスクや事業者内部の悪意ある第三者からの盗聴というリスクは解消されていなかった。

２．研究の目的

本研究では、上記のリスクを抜本的に解決するため、複数のクラウドサービスを複合的に使用することで保存データの完全な秘匿性、および安定性を実現するソフトウェアの開発、およびそれを応用したアプリケーションの開発を目的とする。

具体的には、ハードディスクにおける RAID 技術を参考にし、１つのクラウドストレージを１つのディスクと見立て、大容量のクラウドストレージを仮想的に構築する、またそれを実現するソフトウェア（図 2）の開発が目的である。

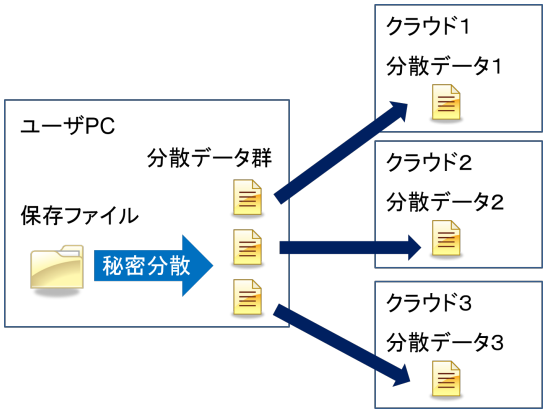

図 2 複数クラウドを利用したデータ保存

秘密分散共有技術は情報理論的に安全であることが示されているため、個々の分散データの秘匿性が脅かされても元データの情報が得られることはなく、また秘密分散共有の冗長性によりいくつかの事業者のサービスが滞ってもユーザーの利便性に影響を与えることはない。さらに副次的な効果として、容量が様々である複数のクラウドストレージを一括利用することでストレージ領域の利用効率向上が見込める。

開発するソフトウェアでは、上記の処理とクラウドとの通信を全てバックグラウンドで実行しユーザーが意識することなくデータの安全、安定な保管が可能になる。

また、この開発ソフトウェアを部品モジュールとして組み込んだ応用アプリケーションの開発を行う。アプリケーションとして、パスワードマネージャを開発対象とする。パスワードマネージャはパスワードという機密性の非常に高い情報を取り扱うため、高い安全性が求められるが、これは情報理論的安全性を持つ秘密分散共有技術の特性で保証できる。また、パスワードを一括管理することにより、パスワードマネージャが使用できないと他全てのサービス利用に影響を及ぼすことになるため、対故障性をを持つことも求められるが、これは複数のクラウドストレージを使用するという開発ソフトウェアの特性による冗長性により実現できる。

３．研究の方法

(1)秘密分散共有処理と分散データの自動同期を行うソフトェアの開発

基幹処理部である秘密分散共有処理を行なうモジュール、および処理結果の分散データを自動的に各クラウドストレージサービスに転送するモジュールを開発し、それらを統合したソフトウェアを開発する（図 3)。

使用する秘密分散共有のアルゴリズムはシャミア法および XOR 法とする。またソフト

ウェアの開発言語は、ユーザインタフェース部分に関するライブラリの豊富さや他プラットフォームへの移植のしやすさなどを踏まえ C#とする。 オブジェクト指向言語の特性により、秘密分散共有処理部とデータ転送部はそれぞれモジュール化し、ユーザーが用途に合わせてアルゴリズムを選択できるよう利便性を向上させるほか、新しいアルゴリズムを追加・拡張しやすいよう設計を行う。

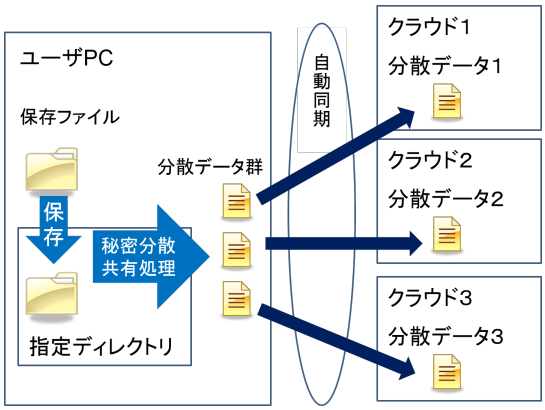

図 3 開発ソフトェアの基本設計

(2)秘密分散ソフトウェアを組み込んだパスワードマネージャの開発

上記(1)で開発を行う、秘密分散共有処理、およびクラウドストレージとの通信を行う基本ソフトウェアの応用アプリケーションとして、クラウドサーバとスマートフォンを補助デバイスとして利用するパスワードマネージャの開発を行う。

開発にあたっては、McCarney らが開発したスマートフォンを補助デバイスとして利用するパスワードマネージャをベースとし、(1)で開発した基本ソフトウェア、およびクラウドサーバを組み込む（図 4)。

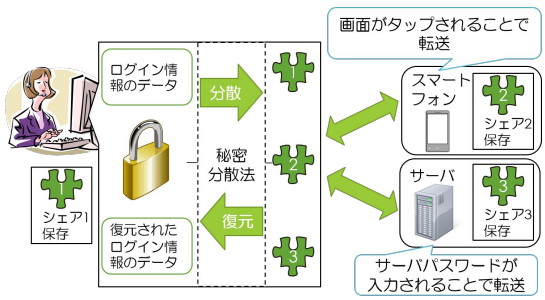

図 4 パスワードマネージャの基本設計

対象とするスマートフォンの OS は iOS および Android OS とする。このとき、基本ソフトウェアのスマートフォン用コードを作成する必要があるが、それぞれの OS 向けのネイティブコードを作成するのではなく、Mono プロジェクトによる開発キットを利用し、C#で記述されたコードを変換することで作業の効率化を図る。

(3)高い安全性を持つパスワード付秘密分散法の開発

秘密分散共有技術によりクラウドストレージを安全に利用する基本ソフトウェア、およびそれを応用したパスワードマネージャについて、より高い安全性を実現するため、根幹技術である秘密分散共有技術の安全性を高める、パスワード付秘密分散法の開発を行う（図 5)。

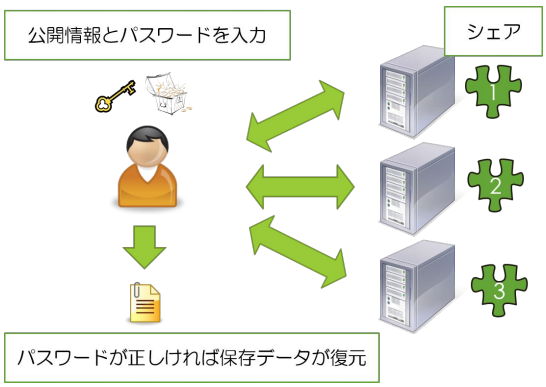

図 5 パスワード付秘密分散法の基本設計

開発にあたっては既存のパスワード付秘密分散法をベースに、構成要素として使用されている暗号プロトコルをより強度の高いものに変更する形で開発する。具体的には、既存方式で使用されている ElGamal 暗号を、標準モデルにおいて高い安全性を持つ暗号方式に置き換えることで目的を実現する。また、構成した方式には別途安全性証明を行うことでその安全性を保証する。

4．研究成果

(1)秘密分散共有処理と分散データの自動同期を行うソフトェアの開発

複数のクラウドストレージを利用し、秘密分散共有技術を用いることで、ユーザーが自身のデータを安全に保管することが可能なソフトウェアの開発を行った（図 6)。開発ソフトウェアは Dropbox や Onedrive といった広く知られているクラウドストレージサービスに対応しており、ユーザーは簡単な初期設定を行うだけで複雑な操作を必要とすることなく開発ソフトウェアを利用することができる。開発ソフトウェアはシャミア式、ランプ式、XOR 式の３つの秘密分散共有方式に対応しており、ユーザーは保存容量や処理速度など、自身の利用目的に合わせた方式を

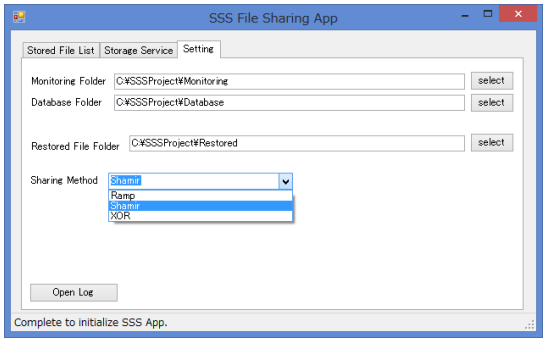

図 6 開発ソフトウェア

選択することができる。
　また、開発ソフトウェアについて数値実験を行った。開発ソフトウェアが対応している３つの秘密分散共有方式についてその性能評価を行い、ランプ式、XOR 式がその処理時間において優れていることが確認された（図 7）。

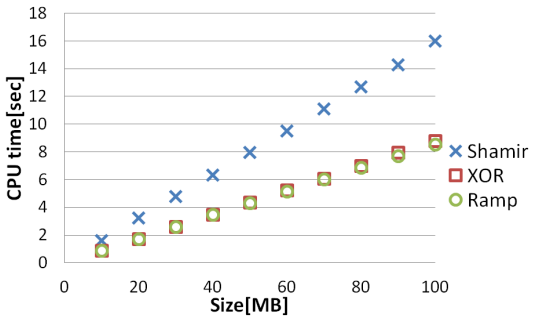

図 7 アルゴリズム毎の処理時間

開発ソフトウェア全体の処理性能については、秘密分散共有処理にかかる時間と処理後のデータを各クラウドストレージにアップロードする時間を計測し、アップロード時間が圧倒的に大きいことが確認された。これについて、クラウドストレージへのアップロード時間をより詳細に調査したところ、使用するアルゴリズムとクラウドストレージにより、処理時間が変化することが明らかになった（図 8）。

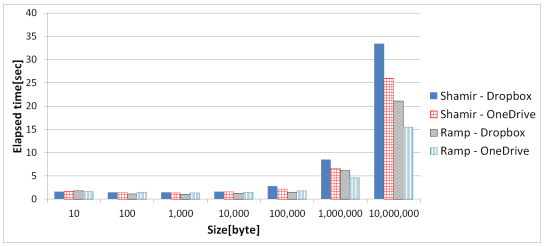

図 8 処理時間の詳細

(2)秘密分散ソフトウェアを組み込んだパスワードマネージャの開発
　上記(1)で開発した基本ソフトウェアの応用アプリケーションとして、クラウドサーバとスマートフォンを補助デバイスとして利用するパスワードマネージャの開発を行った（図 9）。開発したパスワードマネージャは補助トークンとしてスマートフォンを利用することで、パスワード管理におけるトークン管理の問題を解決し利便性を向上させているだけでなく、個別パスワードの保管にあたり秘密分散共有技術を用いているため高い安全性を実現している。

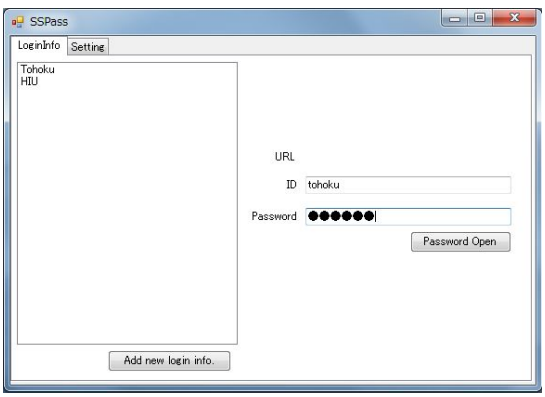

図 9 開発パスワードマネージャ

　また、開発したパスワードマネージャの性能評価として、Web における認証技術の総合評価フレームワークである UDS フレームワークを用いて評価を行った。その結果、開発のベースとした方式よりも複数の項目で性能が向上していることが確認された（図 10）。

	U1	U2	U3	U4	U5	U6	U7	U8
ID/Pass	なし	なし	●	なし	●	●	○	●
LastPass	○	●	○	○	●	●	●	○
MBCCO	●	●	○	○	●	○	●	なし
Ours	●：P ○：S	●	●：S ○：P	○：P なし：S	●	●：S ○：P	●	○

図 10 開発パスワードマネージャの性能評価

(3)安全性の高いパスワード付秘密分散法の開発
　上記(1)で開発した基本ソフトェア、および(2)で開発したパスワードマネージャの機関技術である秘密分散共有技術について、より安全性を高めた方式であるパスワード付秘密分散法の新方式を開発した（図 11）。
　まず、既存のパスワード付秘密分散法には大量のデータが流出した場合に安全性が損なわれる可能性があることを示した。この問題点を解決するため、パスワード付秘密分散法の新しい安全性概念として公開情報安全性を定義し、またそれを満たす方式の設計・開発を行いその安全性を証明した。さらに、これまでのパスワード付秘密分散法は、その安全性がランダムオラクルモデルと呼ばれる理想的な状況でのみ保証される方式のみであったため、現実世界の状況をより反映した標準モデル上で安全性が保証される方式の開発を行った。

	PPSS-secure & pparam-secure	PPSS-secure	PPSS-secure (UC framework)
RO モデル	本研究	[BJSL11]	[CLN12], [CLLN14]
標準モデル	本研究		未解決

図 11 開発パスワード付秘密分散法

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１件）

① Shingo HASEGAWA、Shuji ISOBE、Jun-ya IWAZAKI、Eisuke KOIZUMI、Hiroki SHIZUYA、A Strengthened Security

Notion for Password-Protected Secret Sharing Schemes、IEICE Transactions on Fundamentals of Electronics 、Communications and Computer Sciences、査読有、E98-A、203-212、2015 年、DOI:10.1587/transfun.E98.A.203

〔学会発表〕（計４件）

①福光正幸、長谷川真吾、岩崎淳也、酒井正夫、高橋大樹、秘密分散法とサーバアプリ、スマートフォンを用いたパスワードマネージャの UDS フレームワークによる性能評価、2015 年電子情報通信学会総合大会、査読無、2015 年 3 月 10 日、立命館大学（滋賀県・草津市）

② Shingo HASEGAWA、Shuji ISOBE、Jun-ya IWAZAKI、Eisuke KOIZUMI、Hiroki SHIZUYA、Password-Protected Secret-Sharing Schemes without Random Oracles、ISITA2014、査読有、579-583、2014 年 10 月 29 日、メルボルン（オーストラリア）

③福光正幸、長谷川真吾、岩崎淳也、酒井正夫、高橋大樹、秘密分散法とサーバアプリを用いた安全性と利便性を両立するパスワードマネージャの提案、コンピュータセキュリティシンポジウム 2014 年、査読無、2014 年 10 月 23 日、札幌コンベンションセンター（北海道札幌市）

④福光正幸、長谷川真吾、岩崎淳也、酒井正夫、高橋大樹、秘密分散法によりクラウドストレージを安全に活用する技術の実用化研究、2014 年暗号と情報セキュリティシンポジウム、査読無、2014 年 1 月 23 日、城山観光ホテル（鹿児島県鹿児島市）

６．研究組織

(1)研究代表者

長谷川　真吾（HASEGAWA, Shingo）
東北大学・教育情報基盤センター・助教
研究者番号：80567214