秘密分散法構築におけるユーザフレンドリーなUIの提案・評価・考察

三浦 夢生
（木更津工業高等専門学校 専攻科 制御・情報システム工学専攻）

Proposal, Evaluation and Discussion of user-friendly UI for Secret Sharing scheme construction

Yu Miura
(Advanced Control and Information Engineering Course, National Institute of Technology, Kisarazu College)

In modern society, spreads cloud or online service and a lot of important information (e.g. personal data) is transmitted and received. Cyber-attacks against companies and organizations are increasing year by year, and the damage caused by ransomware, one of them, is expanding. In this study, I deals with a scheme called secret sharing. By using this scheme, we can reduce the risk of loss or theft of the secret. and allows managers to adjust discretion per role by using hierarchical one. The purpose is designing intuitive and user-friendly UI for people who don't know too much about secret sharing and proposing easy to use secret sharing tool even individuals. In an evaluation, I ask testers to use the proposed UI and the conventional CLI-based UI, and conduct a questionnaire survey and analysis of whether the UI is "visually easy to understand", "easy to operate", and "time required to build a secret sharing system".

Keywords: Secret Sharing, cryptgraphy, Shamir's Secret Sharing, User Interface

1 まえがき

近年, クラウド及びオンラインサービスが企業や一般家庭において広く普及し [1], [2], 個人情報などの多くの重要な情報がやり取りされており，実際, 重要な情報へのアクセスに対してセキュリティ対策を施す企業は増加している [3]．その中で企業・団体等に対するサイバー攻撃は年々増加しており, その中の一つであるランサムウェアによる被害は拡大している [4]．IPA の情報セキュリティ 10 大脅威においても，機密情報を狙った攻撃は大きな影響を与えるとされる [5]．これらは機密情報やアクセス権の集中管理によって攻撃を受けた際のリスクが高まるためであり，最小限の適切なアクセス管理が重要である．しかし，無闇な機密情報のコピーや，アクセス権限の厳重化ではかえってリスクが高まる [6].

これらのリスク低減のため機密情報の分散管理及びアクセス権限の柔軟な付与ができる「秘密分散 [7]」という技術を用いる．秘密分散によって情報の漏洩・紛失のリスクを低減し，またこれを階層化することによって管理者の役割ごとの裁量を調節できる手法を UI のバックエンドに採用する．フロントエンドサイドでは，秘密分散を詳しく知らないユーザでも直感的に利用しやすい UI の設計をする．本研究では個人で気軽に利用できるような秘密分散ツールの設計・提案を行い，UI によってどの程度秘密分散ツールが利用しやすくなったかアンケート調査し，提案 UI の有用性や改善点について考察することを目的とする．

実装には，ユーザの環境を選ばずブラウザで動作する Javascript と，そのフレームワークである React.js を主として用いる．React.js は GUI 作成に特化した Javascript フレームワークであり，SPA(Single Page Application) を作成しやすい画面遷移のない実装が可能となり，ユーザ側での画面読み込みや通信負荷を減らすことができる．

アンケート調査ではコマンドラインライクな UI と木構造を模した提案 UI を用意し，それぞれファイルを秘密分散する課題を遂行してもらい，それにかかった時間の計測，使用感に関する質問への回答を求める．

2 Shamir の秘密分散法

秘密分散法とは，まず対象となる秘密情報をあるアルゴリズムを用いてシェアと呼ばれる分散情報を作成し，そのシェアを管理する人・端末に配布し管理・保管する手法である．元の秘密情報を得る際には，管理されたシェアを必要な数だけ集め，復元アルゴリズムによって復元する．

いくつかある秘密分散法のうち，本節では

Shamir の秘密分散法 [8] について述べるこの手法は (k, n) しきい値秘密分散法とも呼ばれ，シェアを n 個生成し，k 個のシェアを集めることで秘密情報の復元が可能であるが，$(k-1)$ 個以下のシェアからは復元は不可能である．

シェアを生成するアルゴリズムは，まず Eq.1 のような秘密情報 S を定数項とするランダムな $k-1$ 次多項式を定める．

$$f(x) = S + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \tag{1}$$

管理に参加する人や端末の数 i に対し，$f(1), f(2), \ldots, f(i)$ を計算し，配布する．

復元の際は，k 個のシェア $(j, f(j))$ を集めて k 個の式を立て，連立方程式を解くことで秘密情報 S を得る．k 個のシェアは同じ多項式から生成されたものであればよく，任意のものを用いればよい．

またこのときラグランジュ補間を用い，Eq.2, Eq.3 において $x = 0$ の場合を計算することで，多項式のうち定数項のみ，つまり元の秘密情報を得ることができる．

$$L(x) = \sum_{i=0}^{k} y_i l_i(x) \tag{2}$$

$$l_i(x) = \prod_{j=0, j\neq i}^{k} \frac{x - x_j}{x_i - x_j} \tag{3}$$

3　先行事例

秘密分散を行うツール・ソフトウェアはいくつか存在している．

グラフィカルな UI では，エスロジカル社の “マル秘分散”[9] が挙げられる．ダウンロードして利用する PC ソフト版と Web 版を提供しており，PC ソフト版においてはコマンドラインモードも存在する．このソフトは，暗号化・復号，2/2 分散．2/3 分散が利用可能であり，暗号化については 2 種類のプロトコル，3 種類のビット長の計 6 種類が利用可能である．また複数ファイル，複数フォルダの一括処理をすることもできる．メール・FTP や，CD-R 郵送などの記録メディア運搬時に用いることが主な目的で，比較的小規模な利用での秘密分散が想定されている．

コマンドラインで利用可能なものでは，Jon Frisby 氏の “ssss”[10] が挙げられる．これは先述の Shamir の秘密分散に基づいて秘密分散を行っており，最大で 128 文字の ASCII 文字を処理することができる．GPLv2 のライセンスで公開されており，誰でも利用可能であるが，ソースコードをダウンロードし，ビルドする必要がある．このツールは前者とは違い，ファイル・フォルダ単位での処理はできないが，秘密分散に用いるパラメータは自由であり，より柔軟な秘密分散が可能である．限られた文字のみ処理できることから，パスワードを管理する際に主に用いられる．

4　提案 UI

本研究では感覚的に階層化された秘密分散法を構築できる GUI を提案する．階層化された秘密分散において，各階層の分散情報を頂点とし，分散情報と，その上位の分散情報を線で結び，それを辺とおくことで木構造として表現できる．このとき，元となる機密情報を最上位ノードとし，それから生成された分散情報を子ノード，その各分散情報から生成された分散情報を子孫ノードとして定義し，パラメータ設定及び描画を行う．

5　実装

ブラウザ上で動作するアプリケーションによって，ユーザの環境に依存せず動作する実装を行う．

提案 UI との比較のためコマンドライン型 UI の実装も行う．

5.1 提案 UI

各ノードを，ノード名．パラメータ・子ノードを持つオブジェクトとして定義する．オブジェクトはすべてのノードを含む単一の木構造となる．

Fig.1. Tree structure type UI.

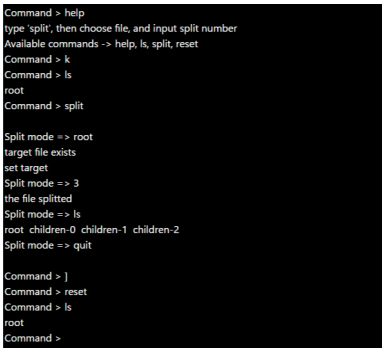

Fig.2. CLI type UI.

Fig.1 のように，初期状態から存在する最上位ノードにパラメータを入力し，分散情報を表す子ノードを動的に生成する．

パラメータが入力されたと同時に対応するノードのパラメータが変更され，Comfirm ボタンが押下されると対応するノードの子ノードがパラメータの数だけ生成され，オブジェクトの状態が更新される．パラメータの変更及びオブジェクトの更新がされるたびにオブジェクトを参照し，再帰的に木構造を描画する．

5.2 コマンドライン型 UI

提案する UI と比較するためのコマンドラインを模した UI を Fig.2 に示す．

この UI は文字及び Enter キーの入力のみ受け付けており，あらかじめ用意された文字列入力があった場合にのみ出力が変化する．またオプション等はなく，スペースで区切られていない単語の入力が可能となっている．

利用可能なコマンドは “help”，“ls”，“split”，“reset” の 4 つである．help コマンドは利用可能なコマンド，split コマンドの簡単な説明を表示する．ls コマンドは現在存在するファイルを列挙する．擬似的に “root” という秘密分散用ファイルを用意し初期状態ではこれのみ表示される．split コマンドは，“Command >” から “Split =>” という表記に変化し，視覚的に秘密分散を行う状態へ移行したことを示す．移行後は，対象とするファイル名の入力をした後，分散したい数を入力すると，分散後のファイルが追加される．移行後に"quit"と入力すると通常状態へと戻ることができる．reset コマンドは秘密分散の進捗を初期状態に戻すコマンドである．どれだけファイルが存在しても，初期状態の root のみになる．

6 アンケート調査

アンケートの内容は，概要を説明できるほど秘密分散を知っているか，UI の使用感，秘密分散を施すイメージを掴めたか，実用を想定した際に選択肢の一つとなるか，その他感じたことについて回答を求めた．

実験参加者には①秘密分散・評価項目・UI の説明を行い，②木構造型 UI，コマンドライン型 UI の順にデモンストレーションを交えて説明し，③同様の順でそれぞれの UI を用いた課題に取り組み，④それぞれの UI に関するアンケートへの回答を求めた．②③④においては，参加者を二つのグループに分け一方は木構造型 UI，コマンドライン型 UI の順，他方はコマンドライン型 UI，木構造型 UI の順に説明し，課題に取り組むことでカウンターバランスを取った．

7 結果・考察

参加者 6 名に回答を求め，得られた結果の平均値を Table.1 に示す．評点は 1 から 5 の 5 段階で，数字が大きいほどポジティブなイメージを示す．6 名全員が秘密分散の概要を知らなかった．

Table1. Average of survey results.

	木構造型 UI	コマンドライン型 UI
秘密分散のイメージがしやすいか	3.5	3.3
使いやすいか	4.3	3.5
実用を想定した際に選択肢となるか	4.3	3.3

全体として木構造型 UI における平均値が高い結果となったが，イメージのしやすさはほとんど変わらなかった．これは事前説明の段階で秘密分散の概要を説明し，デモンストレーションを交えながら実際にその過程を見せたことで，その差がなくなったと考える．使いやすさに関して，コマンドライン型 UI はあくまでコマンドラインを模したものであり，それを想像した上で操作すると不自由に感じると考えられる．また CUI の特性上，操作量が多くなってしまい，そこからくる煩わしさも結果に表れたと考える．実用を想定した際に選択肢になりうるかについても使用感が大きく影響したと考える．

自由記述回答ではコマンドライン型 UI は多少の慣れが必要で，文字のみだと戸惑うという意見があり，コマンドラインを利用したことがない人にとっては利用しづらさがあることがわかった．また，通常のコマンドラインのようなオプションを交えた利用法ができず，普段通りの運用とは勝手が違うことが不自由に感じるとの意見もあった．反対に，コマンドラインを利用したことがある人にとっては，慣れれば強力なツールとなることもわかった．

木構造型 UI は使いやすく，直感的な操作ができ，利用しやすいという意見が多く，コマンドライン利用経験の有無によらない運用が可能なことがわかった．

8 まとめ

本研究では，機密情報を分散管理でき，柔軟なアクセス権限付与が可能な階層化された秘密分散に着目し，その構築において視覚的なサポートする木構造型の UI を提案・実装した．また提案した UI の評価を行うため従来のようなコマンドライン

型の UI を用意し，アンケート調査を行った．その結果について考察し，それぞれの UI の実装や，評価項目そのものにおける課題を明らかにした．

調査結果から，秘密分散構築プロセスのイメージしづらさは，事前説明によって取り除くことができ，UI による差異がほとんどない可能性が示唆された．

自由記述でいただいた意見から，コマンドライン型 UI の評価は，用意した UI の操作性や，機能性の不充分さに起因するものが多く，UI の機能改善によって評価が変化することも示唆された．

またコマンドライン利用経験の有無が大きく評価に影響することも明らかとなり，アンケートの内容を精査する必要性も示された．

9 今後の展望

今後の展望として，まず各 UI の高機能化が挙げられる．木構造型 UI においてはパラメータ入力時の不具合特定・修正，ダミーのテキストファイルを実際に秘密分散し，実際に分散情報のファイルが生成される機能の実装をすることで，より実用に近い体験ができると考える．その場合，ブラウザによる描画処理だけでなく，ローカルに保存されているファイル操作処理が行われることとなり，大きなファイルを扱う場合にはユーザのマシンスペックに依存することになる．今回例としてあげた Shamir の秘密分散は，機密情報と同じサイズの分散情報が生成され，ファイルのサイズやパラメータによっては大きな記憶容量が必要とされることから，(k, L, n) ランプ型秘密分散法という手法を採用することも考えられる．この手法は新たに L というパラメータが利用でき，n 個のシェアを生成し，しきい値 k の数のシェアから復元が可能である．また，$k-L$ 個以下のシェアからは秘密情報に関する情報は一切得られず，$k-l(1 \leq l \leq L-1)$ 個のシェアからは秘密情報のどの部分も明確には得られない特徴をもつ．分散情報のサイズは $1/L$ となる性質をもつため，分散情報の容量が比較的小さくなることから，より実用的であるといえる．

コマンドライン型 UI においては，最低限必要なキー入力，作業をサポートするためのメッセージ表示の追加，オプション引数の実装などが考えられる．UI の機能を充実させることで機能面の差による使用感の評価を減らし，それぞれの UI の特性を正確に評価できると考える．

また，アンケートの内容及び，事前説明の内容の精査を行うことも挙げられる．GUI は CUI と比べて現在一般的に用いられており，CUI よりも使い慣れている人が多いと考える．また，CUI に触れたことがない人はまず CUI に慣れる必要があることから不便さを感じてしまうと考える．逆に CUI に触れたことがある人は使い勝手を知っており，事前知識の有無で評価に影響することが結果から示唆されている．

このことから，UI 提示前に事前知識の有無を問う質問を設けることが挙げられる．今回は秘密分散の事前知識のみについて回答を求めたが，CUI, GUI という言葉について知っているか，それぞれの UI を普段どの程度使うか，そもそも CUI を使ったことがあるかについての質問も設ける必要があると考える．それぞれの UI の利用経験を加味して評価を行うことで，両 UI における改善点もより明確になると考える．

参考文献

(1) 総務省, “デジタルで支える暮らしと経済”, 情報通信白書, pp.156-159, July 2020.
(2) 総務省, “デジタルで支える暮らしと経済”, 情報通信白書, pp.313-315, July 2020.
(3) 独立行政法人情報処理推進機構, “企業における営業秘密に関する実態調査2020”, 調査実態報告書, pp.44-47, March 2020.
(4) 警察庁, “令和3年におけるサイバー空間をめぐる脅威の情勢等について”, 警察庁 広報資料, pp.3-5, April 2022.
(5) 独立行政法人情報処理推進機構セキュリティセンター, “情報セキュリティ10大脅威”, 情報処理推進機構, pp.36-39, March 2022.
(6) 独立行政法人情報処理推進機構, “組織における内部不正防止ガイドライン”, 情報処理推進機構, pp.40-44, April 2022.
(7) 西川律子, “秘密分散法の概要”, 沖テクニカルレビュー 第205号, pp.70-71, January 2006.
(8) A Shamir, “How to share a secret”, Communications of ACM, Vol.22, pp.612-613, April 1979.
(9) 株式会社エスロジカル, “マル秘分散”, http://www.ma-bu.com/, 閲覧日Dec 2021.
(10) Jon Frisby, “ssss”, https://github.com/MrJoy/ssss, 閲覧日Dec 2021.
(11) 高荒亮, 岩村惠一, “XORを用いた高速な(k, L, n)ランプ型秘密分散法に関する研究”, コンピュータセキュリティシンポジウム2009(CS2009)論文集, Vol.2009, pp.1-6, October 2011.