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いる．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 [3]．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 [4]．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 [5]．

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 [6]」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 前提知識

2.1 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，本研究では Shamir の秘密分散法 [10] を用いている．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　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．

4　実装

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

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．同時に木構造全体の状態を保持するオブジェクトが更新され，そのオブジェクトを参照し，再帰的に木構造を描画する．

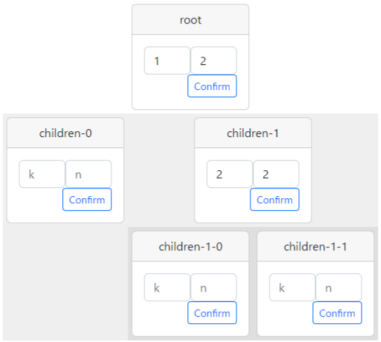

Fig.1. Tree structure type UI.

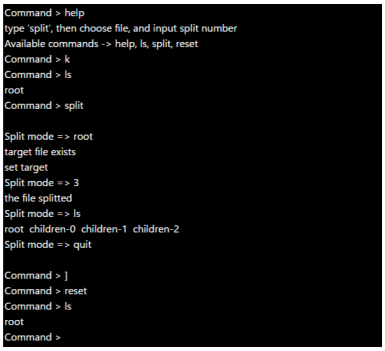

Fig.2. CLI type UI.

5　アンケート調査

アンケート調査は提案する UI と比較するため，Fig.2 に示すようなコマンドラインを模した UI を用意した．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 のを説明を行い，② GUI，CUI 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における UI の提示順は，参加者を二つのグループに分け一方は GUI，CUI の順，他方は CUI,GUI の順にすることでカウンターバランスを取った．

6　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 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．

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

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

くなったと考える．使いやすさに関して，

7　まとめ

8　今後の展望

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) 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.
(4) 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.
(5) 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.
(6) 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.
(7) 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.
(8) 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.
(9) Jon Frisby, “ssss”, https://github.com/MrJoy/ssss, 閲覧日Dec 2021.
(10) A Shamir, “How to share a secret”, Communications of ACM, Vol.22, pp.612-613, April 1979.
(11) 野崎昭宏, “納得する群・環・体”, 講談社, 第1版, pp.136-137, May 2016.
(12) 汐崎陽, “情報・符号理論の基礎”, オーム社, 第2版, pp.90-91, May 2019.
(13) 野崎昭宏, “納得する群・環・体”, 講談社, 第1版, pp.160-176, May 2016.
(14) 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.
(15) 青野成俊, 岩村惠一, “実用観点からみた秘密分散法に関する一考察”, 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.