オンラインストレージサービスに対するクライアント側暗号化と検索可能暗号のユーザビリティ評価

立川　彰宏[1]　緑川　達也[1]　金岡　晃[1]

概要：近年普及が進んでいるオンラインストレージサービスは通信路や保存の際にサーバ側でデータを暗号化しているものも多く、第三者からの攻撃に対しては安全になってきているがデータ内容はサービス提供者に閲覧できる状態にある。問題の解決策としてファイルをアップロードする際に利用者側でデータの暗号化を行うことが挙げられる。しかし暗号化を行うだけでは検索機能やソート機能等のサービス提供者側で提供されているサービスが受けられなくなり、利便性の低下が起こってしまう。本研究では低下する利便性の中でも検索機能に焦点を当て、検索可能暗号を用いた Android アプリケーションとして実装し、実用性を被験者実験によって評価した。

キーワード：UWS, 検索可能暗号, オンラインストレージサービス, End to End 暗号化, ユーザビリティ評価

1. はじめに

近年普及が進んでいるオンラインストレージサービスは通信路や保存の際にサーバ側でデータを暗号化しているものも多く、第三者からの攻撃に対しては安全になってきているがデータ内容はサービス提供者に閲覧できる状態にある。

実際にサービス提供者側からのデータ閲覧が可能であることが確認された例として、2016 年 12 月 15 日にオンラインストレージサービスの 1 種である「Evernote」を提供する Evernote 社が、サービス向上のためという名目で、一部社員にユーザーコンテンツへのアクセスを可能とさせるプライバシーポリシーへの変更を発表した。そして実際に、サービス提供者側からのデータ閲覧が可能であることが確認された。また、Evernote 社はプライバシーポリシー変更を発表した翌日、多くのユーザからの懸念の声によりプライバシーポリシー変更の見直しを発表した [1]。この記事から、たとえサービス提供者であろうとデータを閲覧されたくないと考える一般ユーザが多数存在することが伺えた。

サービス提供者側へのデータ秘匿の方法として、クライアント側でのデータ暗号化が挙げられる。しかし暗号化を行うことで、オンラインストレージサービス側で提供されているソーティングや検索のサービスが受けられなくなり、利便性の低下を引き起こすことが考えられる。

本研究では低下する利便性の中でも検索機能に焦点を当て、対称型検索可能暗号（Symmetric Searchable Encryption、以後 SSE）を用いた Android アプリケーションとして実装し、そのユーザビリティを System Usability Scale（以後 SUS）と SUS でのアンケート回答に対しての半構造化インタビューを軸とした被験者実験を行い、Grounded Theory Approach（以後 GTA）を用いて評価した。実験の結果、SSE を適用したアプリへの評価は他の比較用のアプリへの評価と比較して特筆すべき差異は見られず、SSE の適用やファイルに対しての暗号化の適用はユーザビリティの面で大きな障害となるものではないことが示された。

2. 関連研究

2.1 電子フロンティア財団による「Secure Messaging Scorecard」

Secure Messaging Scorecard は、電子フロンティア財団（Electronic Frontier Foundation）によるメッセージングツールのクライアント間での暗号化状況について整理して公開したものである [2]。37 のツール・サービスが 7 つの項目を満たしているかについての調査結果が示されている。それらの項目は送信時の暗号化や、サービス事業者の閲覧から保護されているか、といった項目を含んでいる。7 項目すべてを満たすツール・サービスは 7 あり、サービス事業者にデータ閲覧がされないような暗号化がさているものは 21 あった。

[1] 東邦大学
Toho University

2.2 Curtmola らの SSE 手法

Curtmola らは、2006 年に共通鍵暗号の利用をベースにした対称型の検索可能暗号方式を提案した。対称型検索可能暗号は Curtmola らの提案後多くの研究が行われており、現在では基点となっている手法であると言える。Curtmola の SSE は以下の 4 つのアルゴリズムからなるシステムである。

- **Keygen**(1^k) : ユーザが、セキュリティパラメータ k を入力として受け取り、鍵 K を生成するアルゴリズム。
- **BuildIndex**$(K, \mathcal{D}, \Delta)$: ユーザが、**Keygen** で生成された鍵 K とドキュメント群 $\mathcal{D}$ 及び辞書 Δ を入力として受け取り、インデックス $\mathcal{I}$ を生成するアルゴリズム。生成された $\mathcal{I}$ は、暗号化ドキュメント群 $\mathcal{C}$ と共にユーザからサーバへ渡され、サーバは $\mathcal{I}$,$\mathcal{C}$ を保管する。
- **Trapdoor**(K, w) : ユーザが、**Keygen** で生成された鍵 K と検索キーワード w を入力として受け取り、w に対する検索クエリ T_w を生成するアルゴリズム。
- **Search**$(\mathcal{I}, T_w)$: サーバが、**BuildIndex** で生成されたインデックス $\mathcal{I}$ と **Trapdoor** で生成された検索クエリ T_w を入力として受け取り、検索結果 $\mathcal{D}(w)$ を出力するアルゴリズム。

Curtmola らは、非適応的攻撃に対して安全な方式である Efficient SSE Construction（SSE1）と適応的攻撃に対して安全な方式である Adaptive Secure Construction（SSE2）の 2 つの SSE 方式を提案している [3]。

2.3 尾形らによる改良方式

尾形らは Curtmola らの方式をベースとして Simple-SSE を提案した [4]。Simple-SSE は、安全性を考慮していない検索方式から直接的に導出できる SSE 方式であり、暗号化していない通常のインデクス内のキーワードをランダムな文字列に置き換えたものを秘匿処理されたインデクスとする。また、Curtmola らと同様に、**Keygen**、**BuildIndex**、**Trapdoor**、**Search** の 4 つのアルゴリズムにより構成される。

2.4 緑川らによる暗号化とユーザビリティに関する研究の調査

緑川らの論文 [5] は、暗号化とユーザビリティの研究をテーマとした論文について、計 52 本をまとめ、その動向や将来を議論したものである。この論文では、エンド間での通信を行う際に通信路の暗号化だけでは不十分であると述べている。

3. オンラインストレージサービスにおける脅威のモデル

本研究では、利用者の意図しない情報漏えいに焦点を当ててオンラインストレージサービスの脅威を検討する。

オンラインストレージサービスでは、サービスの利用者とサービスの事業者、そしてサービスに関係のない第 3 者の 3 つのプレーヤーを想定する。そして、利用者の意図しない情報漏えいの発生として、以下の 2 つを情報漏えいの脅威と考える。

- 第 3 者に対する情報の漏えい（第 3 者による意図的な情報詐取を含む）
- サービス事業者に対する情報の漏えい（サービス事業者による意図的な情報取得を含む）

第 3 者に対する情報の漏えいとしては、サービス事業者とサービス利用者間の通信路における情報の保護と、サービス事業者側によるデータの保護の 2 種類で対応が可能である。

サービス事業者に対する情報の漏えいについては、サービス事業者側によるデータの保護だけでは対応できず、サービス利用者側での保護機能利用を行わなければならない。

4. 既存オンラインストレージサービスの調査

4.1 調査対象となるオンラインストレージサービスの選定

既存サービスの調査として、調査対象となるオンラインストレージサービスの選定を行った。オンラインストレージサービスには、日本語に対応しているサービスだけでも Dropbox（Dropbox）、Google ドライブ（Google）、OneDrive（Microsoft）など、複数の種類のサービスが存在する。

その中で、Dropbox は後述するようにサーバ側での暗号化対応が明言されていることに加え API を提供していることから、本研究では Dropbox を評価の土台として採用した。

Google ドライブ、OneDrive については、事業者が提供する情報からはその暗号化の有無を含めた詳細は得られなかったため、今回の評価には採用しなかった。

4.2 Dropbox の暗号化状況

Dropbox では通信路の保護とサーバ側のファイル暗号化については以下の方式が採用されている [6]。

- ファイル保存には 256 ビット鍵の AES を利用
- サーバとクライアント間の通信には TLS を利用し、128 ビット以上の鍵サイズを持つ AES で保護されている

なお、ファイル暗号化の実施と暗号鍵の管理はサービス提供者である Dropbox 社が保持しており、Dropbox 社は利用者のデータの閲覧が可能な状態となっている。3 章で示した脅威モデルと比較した場合、Dropbox、Google ドライブ、OneDrive は「サービス事業者に対する情報の漏えい」が発生している状況となる。しかしこれは悪意のあるものではなく、安価なオンラインストレージサービス利用における対価の 1 つとして利用者が合意したものであるこ

とに注意が必要である。

5. クライアント側暗号化を行うオンラインストレージのシステムモデルと研究の目的

後者のサービス事業者に対する情報漏えいを防ぐためには、クライアント側での情報保護が必要となる。本研究ではオンラインストレージアプリケーションによる暗号化と復号で実現する。

サービス事業者にデータをアップロードするときに拡張子を含むファイル名とファイルのデータを暗号化して送信し、暗号化されたファイル名とファイルデータをダウンロードしてクライアント側アプリケーションで復号をして表示を行うことで、サービス事業者に対する情報漏えいから守る。ファイル名とファイル内容の暗号化をここでは1つにまとめて「コンテンツ暗号化」と呼ぶとする。

単純にコンテンツ暗号化をした場合、オンラインストレージとしてのいくつかの機能が暗号化データを考慮したものでなければならなくなる。利用者は多くのファイルの中から求めたファイルを見つけるために、ファイル名や更新日時、ファイルタイプでのソーティングや、コンテンツに含まれる文字列を検索する。

検索の手法としては、利用者が検索を行うたびに全文を文字列検索する逐次検索と、あらかじめコンテンツが持っている情報を検索用に準備するインデクス型の検索とに大別される。インデクス型検索はあらかじめ検索用語と結果を保持しているため効率が良い一方で、保護される対象であるコンテンツの情報がインデクス内に解析可能な形で保存される可能性がある。オープンソースの検索エンジンとして代表的な Apache Lucene では、インデクスのデータフォーマットの仕様が公開されており、キーワードやその検索結果が平文のまま保管されており、インデクス情報からコンテンツの内容が類推できる仕様となっている。本研究ではインデクス保護を実現可能かつ検索効率のよい対称型検索可能暗号を採用し、そのユーザビリティを測ることを目的とした。

6. 検索可能暗号を適用したアプリケーションの実装概要

6.1 アプリケーションの概要

本実験で使用するために作成したアプリケーションは、クライアント側でファイルの暗号化を行い Dropbox と連携し、SSE によって検索インデクスの暗号化を行った Android アプリケーションである。

ファイルの暗号化には AES を利用し、SSE では Curtmola らが提案した SSE を利用する。

6.2 基本的な処理性能とアプリの動き

本実験で使用する Android 端末および作成したアプリケーションの基本性能を表 1 に示す。

OS	Android 4.3
対応 CPU	インテル Atom プロセッサー Z2560 1.6 GHz
対応メモリ	1GB
ストレージ機能	eMMC：16GB

表 1 本実験で使用する Android 端末の基本性能

作成したアプリケーションの基本的な動きを示す。アプリを開くとファイルの一覧と検索窓が表示される。ファイル名は暗号化されているため表示する際に復号している。そしてアプリ利用者がファイル一覧からファイルのアイコンをタップすることで Dropbox からファイルがダウンロードされる。ダウンロードされた暗号化ファイルを端末側で復号し、ファイルを開く仕様となっている。検索窓の動きとしては、検索キーワードを入力し検索ボタンを押すと SSE1 の Trapdoor を作成し、インデクスを使用して検索を行う。検索結果に対応するファイル ID を取得し、ファイル ID に対応した暗号化されたファイル名で Dropbox に対して検索を行う。検索結果を受け取り、ファイル名の復号の処理を行って検索結果を表示するという流れとなっている。

アプリケーションの基本性能として、ファイル表示に必要な時間と検索待ち時間を測定した。ファイル表示はユーザによりファイル選択された時点から、ダウンロードと復号を経て表示されるまでの時間を測定し、検索待ち時間は検索開始のボタンを押下された時点から検索結果が返ってくるまでの時間を測定した。その結果、ファイル表示は平均で 1096.68ms、検索待ち時間は平均 1974.33ms となった。

7. 被験者実験

7.1 実験目的

本研究では 5 章で示したオンラインストレージシステムのモデルのユーザビリティ評価を行うことを目的としている。そのため、実験では 5 章で示したオンラインストレージシステムを含めて複数のアプリケーション実装し比較をすることでそのユーザビリティを議論する。

7.2 実験に使用するアプリケーション

本実験では、機能の異なる 4 つの Android アプリケーションを用意し、それぞれのユーザビリティを測定し、機能の違いによるユーザビリティ変化かを観測する。4 つの Android アプリケーションの外観については、検索機能の有無に従い検索窓の有無が異なるが、他の部分の外観は同一である。実験に使用する 4 種類の Android アプリケーションについての情報を表 2 にまとめた。以後それぞれのアプリケーションを参照する際はアプリ ID を参照する。

app1「Normal」については、現在 Dropbox 社が提供している Dropbox のアプリケーションを意識し、機能面におい

アプリ ID	アプリ名称	検索機能	ファイル暗号化	インデクス暗号化
app1	Normal	○	×	×
app2	E2E 暗号化 (検索なし)	×	○	−
app3	E2E 暗号化 (逐次復号+検索)	○	○	−
app4	E2E 暗号化 (SSE 利用)	○	○	○

表 2 実験に使用するアプリケーションについて

てほぼ同等のアプリケーションとなっている。app2「E2E 暗号化（検索なし）」については、コンテンツ暗号化・復号のみを行い検索機能がないアプリケーションとなっている。app3「E2E 暗号化（逐次復号＋検索）」では検索機能が与えられているがインデクスを使用しておらず、Dropbox 内の暗号化ファイルを全てダウンロードし、全ファイルに対して復号の処理を行った後に、全文の文字列一致により検索を行うものとなっている。app4「E2E 暗号化（SSE 利用）」はコンテンツ暗号化に加え検索機能を SSE1 で提供するアプリケーションとなっている。

7.3 実験と分析の概要

本研究では、検索可能暗号を採用した暗号化オンラインストレージサービスのユーザビリティ評価のために、System Usability Scale（SUS）と SUS でのアンケート回答に対しての半構造化インタビューを軸とした被験者実験を行う。SUS の回答をスコアリングすることで実験結果を量的に分析し、実験中の行動を動画撮影しインタビュー内容と動画内容からグラウンデッド・セオリー・アプローチ（Grounded Theory Approach、GTA）を行うことで質的な分析を行う。SUS の質問項目、SUS の原文の 10 項目を和訳したものを使用した。

本来の研究目的を伝えることで偏ったユーザ行動が観察されてしまうことを避けるために、本来の研究目的とは異なる仮の実験目的を立て、被験者の意識を実験用の Android アプリケーションそのものから逸らせることとした。今回の実験では、実施母体である研究室が実施して違和感がなく、またオンラインストレージを利用することが目的に沿うように「新しいパスワードリマインダ機能の有効性調査」として仮の目的を立てた。

実験の手順は以下の通りである。

(1) 仮の実験目的の説明
(2) 被験者による作業内容の説明を行い、被験者に実際に作成した Android アプリケーションを利用してもらう
作業内容は以下の通りである。
「利用者の方がパスワードによってロックをかけたフォルダが存在するが、利用者の方がそのパスワードを忘れてしまったので、本人確認を行うために 4 桁の数値を入力しなければならない」と仮定し、被験者に本人確認を以下の手順で行ってもらう。1. 本人確認を行うための 4 つの単語が画面に表示される
2. Dropbox 内のファイル群の中から、与えられた単語が含まれているファイルの数を求める
3. 与えられた単語が含まれるファイル数を順に並べて出来上がった 4 桁の数値をパスワードリマインダ情報として入力する
(3) 本来の実験目的の説明
(4) 本来の実験目的で実験結果を利用することに対しての同意取得。同意が得られない場合は、録画した映像の消去など実験で得られたものの破棄を行い、参加報酬を渡す。
(5) SUS アンケートへの回答と、インタビューの実施
(6) 被験者からの実験についての質問・感想を伺う

インタビューでは、SUS 項目の各回答の理由を問い、またアプリ利用におけるストレスの実感と要因、検索の効率、オンラインサービス利用におけるセキュリティの意識をヒアリングした。

実験で利用する検索対象のファイルには、被験者がファイルの中身を見た際に目視で単語を見つけ出すことが難しくなるような文章にするために、[7] で紹介されていた 10 種類の英語の童話を用意した。

また、本人確認を行う際の与えられた 4 つの単語については、一般的な用語であり、選出した童話にも少なからず出現する可能性を考慮して、色についての単語を選択し、その中から 4 種類を選出した。

7.3.1 被験者について

被験者の募集は、2017 年 6 月 5 日〜2017 年 8 月 25 日に大学の履修システムと学内掲示板にて行った。今回の実験において集まった被験者の情報は表 3 に記載した。なお、表 3 には後述する SUS のスコアも付記している。

いくつかの被験者実験を行っている論文を見る限り、米国の論文では報酬が 1 時間当たり 10 ドル程度であったが [8]、米国では最低賃金が 15 ドルへ引き上げられた [9] 後から 15〜20 ドルへと変化しており [10], [11], [12]、その国の 1 時間当たりの最低賃金を基準とした報酬額であることが見て取れた。そのため、千葉県の最低賃金が時間給 842 円であり [13]、実験予定時間が 30 分であったため、最低賃金の時間給の半分に近い 500 円が妥当であると考え、500 円分の図書カードを報酬とした。

7.4 生命倫理審査委員会の承認

本実験を行うにあたり学内の生命倫理審査委員会に承認を得て実験を行った。

8. 実験結果

8.1 SUS スコアの集計結果

各被験者から得られたスコアは表 3 に示されている。本

被験者 ID	学科	性別	利用アプリ番号	SUS 合計点
P1	情報科学科	女性	app1	62.5
P2	情報科学科	女性	app2	60
P3	情報科学科	男性	app3	67.5
P4	情報科学科	男性	app2	92.5
P5	情報科学科	女性	app4	92.5
P6	情報科学科	女性	app1	87.5
P7	情報科学科	女性	app1	60
P8	情報科学科	女性	app4	72.5
P9	情報科学科	男性	app3	77.5
P10	化学科	男性	app4	45
P11	化学科	男性	app2	82.5

表 3 被験者情報

実験で得られた SUS のスコアと各アプリごとに平均を取った結果、app1 は 70、app2 は 78.33、app3 は 72.5、app4 は 70 となった。

8.2 GTA を行ったうえで分類された概念の考察

実験で得られたアンケート回答・実験行動（総数：188（重複含む））を基に GTA を行い、計 16 の概念に分類を行った。それぞれの概念において特徴的なものを分析した結果を示す。

8.2.1 矛盾

4 種類のアプリ全ての利用者が、「特に矛盾は感じなかった」「矛盾が良く分からなかった」という意見を出していることから、アプリケーションに矛盾を感じていないことが見て取れる。

8.2.2 使いやすい・便利

使いやすかったという意見は全てのアプリ利用者から出ており、全体を通して使いやすいアプリになっており、検索の有無や検索手法の違いで使いやすさに強い差異を生じさせていないことが伺える。

「アプリの検索機能が自分が普段使うときに便利だと思った。中身がごちゃごちゃになったときに便利そう」（P3、app3）「効率よく探すことが出来ていたと感じた。アプリ内の検索機能でファイルの中身に単語があるかどうかの検索が出来たので便利だった」（P5、app4）「検索をすると検索結果の件数が表示されるので使いやすかった」（P7、app1）以上のようにアプリ内の検索機能が便利だったという意見が出ており、アプリ内の検索機能の有用性が見て取れる。

アプリ内の検索機能が実装されていない app2 のアプリの利用者の意見は、アプリが使いやすかった、暗号化されているから便利・使いたい、オンラインストレージ自体が便利という意見が見られた。P11 からは「そこまで利用するかはわからないが、暗号化されているので普通の暗号化されていないものよりかは使いたいと思う」（P4、app2）とあり、暗号化されていることで安心感が生まれているであろうことが見て取れるが、言及は 1 名のみのため全体の傾向とは言い切れない。

「そんなに必要ないと思ったので。あれば便利だと思うが自分があまりファイルをいじらないので必要ないと思った」（P6、app1）「ファイルの数が増えたときに便利だと思った（オンラインストレージ自体が）オンラインストレージは普段利用しない。今後、データの共有のために利用するかも」（P11、app2）一方以上のようにオンラインストレージ自体にあまり興味がない、利用しないという被験者からも便利、使う機会があれば利用するといった肯定的な意見が出ている。

8.2.3 ストレス

P8（app4 利用）以外の被験者の意見が分類された。

多くの回答は「特にストレスは感じなかった」といった回答であり、基本的には 4 種類ともストレスを感じないアプリになっていることがわかる。

app2 利用の被験者 2 名より「検索ワードのうち「pink」と「purple」の頭文字の「p」が同じだったので押し間違えることがあったので頭文字が別々の方が検索がしやすいのかなと思う。検索ワードがシンプルだったので検索は簡単だった。ファイル内で検索をすると単語が水色でマーキングされたので視覚的にも分かりやすかった。ファイルが増えていくと検索を行うのにストレスを感じるかもしれない」（P4、app2）「10 個のファイルしかなかったのでそんなに感じなかったけど、ファイルが増えたりするとファイルを開く手間だったりファイルの開き忘れ等があると思う。1 つ 1 つ開いて検索ワードを入力しないといけないのが面倒」（P2、app2）という意見が出ており、ファイル数が増えると 1 つ 1 つ開いて検索ワードを入力することにストレスを感じる可能性があることを指摘している。

一方で、「最初、検索機能を知らなかったのでちょっと感じた。説明書を読んで、検索機能を使ってからは特に感じなかった」（P5、app4）と、検索機能を利用したことによりストレスを軽減できたということが確認され、検索機能の有用性が伺える。

8.2.4 効率が良い

app2 のアプリ利用者以外の全被験者（P1, P3, P5, P6, P7, P8, P9, P10）が分類された。分類された回答は全て実問 2 に対する回答であった。分類された被験者を見るに、app2 のアプリを利用した被験者は効率が良いと感じていなかったことが伺える。

8.2.5 面倒ではない

4 種類全てのアプリが分類された。検索機能を持たない app2 の被験者においても同様の傾向を示していることが特徴的である。「特に面倒だと思わなかった。ファイル内検索で引っかかった検索ワードが画面端に表示されていて見にくかったのがいくつかあったのでそれはちょっと気になった。」（P11、app2）

8.2.6 面倒・大変・手間・複雑

面倒であることや、それに近い「大変」「手間」「複雑」というキーワードで回答をしていたものについてもあった。こちらもアプリの種類にかかわらず分類がされていた。

検索機能を持たない app2 に対して、被験者からこの概念に属する回答が多く寄せられた。「ファイルを開く前から検索機能があるわけではなくて、いちいちファイルを開かないと検索出来ないから手間がかかり不便」（P2、app2）「効率は良くなかったと思う。1 つ 1 つ調べないといけなかったので」（P2、app2）といったように、いちいちファイルを開くのが不便、ファイルを開く前から検索機能が欲しいというピンポイントでアプリ内検索を欲する意見や、「効率はそんなに良くはないかもと思った。同時に複数検索が出来ると便利だと思う」（P11、app2）

8.2.7 難しい・分からない

4 種類全てのアプリが分類された。分類された回答に目立った偏りは見られなかった。

難しさの言及については、被験者自身は利用可能であったが、老人等の他の被験者であったら難しさが生じるかもしれない、という意見があった。「Android を使い慣れていない人はサポートが必要かもしれない」（P1、app1）「ケータイのアプリ等を利用している人なら使えると思うけど、年齢層が高い人が使うと使いにくいと思ったから 2」（ P2、app2）「ファイルとかに触れていない人からするとサポートが必要かもしれないから 3」（P7、app1）

8.2.8 理解・自信（簡単）

4 種類全てのアプリが分類されていた。分類された回答に目立った偏りは見られず、ほぼ全ての質問が分類されていた。4 種類全てのアプリ利用者から「分かりやすかった」、「利用できる自信がある」、「理解できた」、「複雑でない」、「特に必要な知識はない」といった意見があった。このことから、4 種全てのアプリが使いやすく、理解されやすいアプリになっていたと取れる。この概念に分類された回答は 48 回答と、他の概念と比べ圧倒的に多く、全体（188（重複含む））の 4 分の 1 近い回答が分類されている。また、被験者全員の回答が 1 回答以上分類されていることから、全ての被験者が今回の実験で使用したアプリに対してプラスの印象を持っていることが分かる。

「説明書が分かりやすかったので分かると思う」（P4、app2、一部抜粋）「説明書を読んで検索の仕方が分かった」（P6、app1、一部抜粋）「アプリの説明書が分かりやすかったので簡単に操作できた」（P7、app1、一部抜粋）上記のような説明書が分かりやすかった・説明書があれば理解できるという回答が見られ、上の 2 名は説明書があればサポートが要らないという回答だった（問 4）。

8.2.9 暗号

app1 以外の 3 種類のアプリが分類された。多かったアプリは app2（9 回答中 4 回答）であった。

「そこまで利用するかはわからないが、暗号化されているので普通の暗号化されていないものよりかは使いたいと思う」（P4、app2）「あんまり自分がこのアプリを使う姿が想像できない。他人に見られることを想定していなかったので特に暗号化が必要だと思わない。」（P8、app4）「他の色々なアプリと比べ、性能の差を感じないので他と特に変わらないと思うので 3。暗号化している点についてはどちらでもないというよりは、分からない方の 3」（P9、app3）といった回答で、三者とも違う回答をしている。（利用したい、必要だと思わない、分からない）利用したいと解答した被験者も、「普段 Dropbox を利用しているがパスワード等がもれなければ特に問題はないと思っている」と回答していることから、暗号化されていないよりは暗号化されているほうがいいといった回答であることが見て取れる。

また、「検索がまったく出来ないと不便だと思うが、ファイルのページにいけば検索は出来るので暗号化とうまくメリットをとって統合できていると思った」（P4、app2）「暗号化の処理が目に見えていない時点で、上手く統合されていると思った」（P9、app3）「他のアプリと比べて暗号化されている分、うまく統合されていると思った。（途中で 3 にした理由：検索機能だけでは特に秀でているわけではないのでどちらでもない）」（P11、app4）といったように、暗号化されていることがアプリ利用者にとって好印象であることが見て取れる。

加えて、「検索の仕方は他の色々なものと同じなので特に無いと思う。暗号化については暗号化しないとどこが危険なのかは知っておいたほうがいいかも。このアプリを利用する上では特に暗号化について知る必要はない」（P4、app2）「暗号化についての知識などを理解していたらスムーズに利用できると思う」（P11、app4）といったように、暗号化についての知識は必須ではないにしろ、あったほうがアプリ利用の際にスムーズに利用できると回答している。また、「特に学ぶことはないと思う。暗号化に関しても特に学ぶ必要はないと思う。」（P12、app2）のように、暗号化についてまったく知らなくても利用できるという回答もあり、透過的な暗号の利用に対する肯定的な意見が複数あった。

8.2.10 安全・セキュリティの意識

セキュリティや安全についての意識に対しては、アプリの種類を問わず、意識していないことを示している被験者が多くいた。

その中で、意識をしている被験者の中に「基本的にネットに預けるのは信用していない。セキュリティがしっかりしているのかの信用が出来ない。大事なデータは手元にとっておきたい」（P1、app1）といったようにインターネット（オンラインストレージ）に対する信頼があまり無く、大事なデータはネットに上げずに手元に取っておきたいという意見もあった。脅威モデルとして我々が示した 2 つ目の脅

威に対しての意識があることが示されている。

8.2.11 説明書を読む／読まない

説明書に関連する概念として「読む」「読まない」の 2 つが抽出された。表 4 は、被験者ごとの使用アプリ、実験の説明者から開始が支持されたあとに実際に端末操作を始めるまでの操作開始時間、実験実施時間、SUS 合計点をまとめたものである。表の被験者 P3、P5、P12 の被験者は説明書を読まないに分類されている被験者である。

被験者 ID	利用アプリ番号	操作開始時間	実験実施時間	SUS スコア
P1	app1	1:50	4:33	62.5
P2	app2	0:30	8:32	60
P3	app3	0:03	12:24	67.5
P4	app2	1:28	8:57	92.5
P5	app4	-0:05	6:42	92.5
P6	app1	0:22	6:38	87.5
P7	app1	0:34	2:32	60
P8	app4	1:28	3:47	72.5
P9	app3	1:06	3:55	77.5
P10	app4	1:04	5:13	45
P11	app2	0:04	16:08	82.5

表 4 被験者ごとの実験結果

表の操作開始時間の部分に注目すると、実験開始を支持してから端末を触るまでの時間が 1 分を超えている被験者がこの概念に分類された半数を超えていることが分かる（8 人中 5 人）。この時間帯に被験者はアプリの説明書を読んでいることを示している。実験実施時間に注目すると、実験実施時間が 5 分を切っている被験者が半数いることが分かる。（8 人中 4 人）。実験が 5 分未満で終了している被験者 4 名のうち、3 名が説明書を 1 分以上読んでいる被験者であることから、実験を開始してから 1 分以上説明書を読んだ被験者はアプリの利用方法の理解が早いことが伺える。実験実施時間が一番短い P7 の被験者は、実験説明の途中から説明書を読んでいたため、操作開始時間より長い間説明書を読んでいたことになる。

一方、SUS のスコアと操作実施時間、実験開始時間への相関は見られなかった。

全被験者のうち、実験実施時間が短かった被験者の下位 2 名（P3（12 分 24 秒）、P11（16 分 08 秒））が説明書を読んでおらず、最初に説明書を読まない場合は実験実施時間が長くなる可能性が考えられる。

説明書を読まなかった 3 名全員の共通点として、実験中に質問を行っていた。

9. Discussion and Limitation

9.1 実験から得られたこと

脅威モデルとして脅威のうち 2 つ目である「サービス事業者に対する情報の漏えい」への保護実現として、クライアント側暗号化と検索可能暗号利用可能なオンラインストレージアプリケーションを作り、そのユーザビリティ評価を目的として実験を行ってきた。

その結果、SSE を適用したアプリへの評価は、他のアプリとの評価と SUS のスコアを見ても、GTA 分析をした結果を見ても、特筆すべき差異はなかった。SSE1 の適用についてはユーザビリティの問題点は確認されなかったと言える。

一方で、暗号化の必要性については、脅威として認識している被験者の存在や、暗号化されているのであれば使いたいという意見などがあり、ユーザビリティが高くあれば暗号処理を受け入れる意見も複数あり、SSE の適用やコンテンツ暗号化の適用はユーザビリティの面で大きな障害となるものではないことが示されたと言えよう。

9.2 インデクス情報の保管

今回実験に利用したアプリケーションではインデクスは端末側に保管がされていた。オンラインストレージサービスとして利用した Dropbox が SSE に対応しておらず、また SSE をサーバ側で実用可能な高い柔軟性は持っていなかったためである。

SSE ではインデクスはサーバ側とクライアント側のいずれも持つことが可能である。サーバ側で SSE のインデクスを持つ場合は、サービス事業者への情報漏えいを防ぐことが可能になり、クライアント側で SSE のインデクスを持つ場合は、他のアプリケーションからの閲覧や端末紛失時の望まない閲覧からの保護が可能となる。今回検討した脅威モデルでは、第三者への情報漏えい対策として他のアプリケーションや紛失時を脅威としては設定していなかったものの、さらに脅威モデルを広げて検討した場合、クライアント側で SSE のインデクスを持つことが有効な手段となる。ただし、一般的に SSE のインデクスは暗号化をしていないインデクスより巨大なサイズとなるために、処理速度面ではなく容量面での不利な点を踏まえた利用が必要となる。

9.3 他の SSE 手法の適用

今回の実験では SSE1 を利用した。SSE1 は、KeyGen、BuildIndex、Trapdoor、Search の 4 つの関数が定義されている。このうち今回の実験で用いたものは、検索のキー生成となる Trapdoor 関数と、暗号化インデクスから Trapdoor を用いて検索結果を得る Search 関数の 2 つのみであった。

SSE 方式は一般的にこの 4 つの関数は定義されているため、本研究の実験は SSE1 に限定したものではなく他の SSE 方式でも実施可能である。

9.4 鍵管理

今回のアプリケーションで志向したことの 1 つは暗号

の透過的な利用であった。透過性に関しては Ruoti らの研究により、透過的すぎることが逆にユーザの混乱を招きユーザビリティを下げることが示唆されていたものの、その後 Bai らの研究により、鍵のディレクトリモデルと交換（Exchange）モデルの比較と利用者のユーザビリティ評価をして行われた。ディレクトリモデルはこの透過的な暗号化を実現する鍵管理モデルであり、Bai らの結果ではディレクトリモデルの利用に関してユーザビリティ低下がほとんどないことが示されている。

本研究のユーザビリティ評価においては、暗号鍵の管理が透過的に行われていればよいことが要件となる。したがって、実験用に開発したアソフトウェアでは、ドキュメントとファイル名の暗号化に用いた AES の鍵と SSE の Trapdoor 作成に用いた AES 鍵の双方はプログラムに直接記載をした。実験用開発ソフトウェアでは柔軟な鍵管理は実現されていない。

提案したアプリケーションの実現において柔軟な鍵管理を実現するためには、ドキュメント暗号化用と SSE1 用の AES 鍵 2 種類を統合して管理する必要が出てくる。逆に言えば、アプリケーションは鍵管理のモデルを制限する仕様となっていないため、柔軟な鍵管理手法の適用が可能である。

9.5 今後の課題

今後の課題としてはまず、量的分析の質を上げるために被験者の数を増やすことがあげられる。今回の実験で集まった被験者数は 11 人と量的分析を行うには少ない人数であったため、SUS のスコアを基にした統計的な議論は行っていなかった。統計的に SUS のスコアを議論するために、より多い被験者数を確保することは欠かせない。

10. まとめ

本研究では、クライアント側暗号化と検索可能暗号利用可能なオンラインストレージアプリケーションを作り、そのユーザビリティ評価を行った。クライアント側暗号化と検索可能暗号の利用は、オンラインストレージサービスにおけるサービス事業者への情報の漏えいに対する保護実現と機能低下の防止という 2 つの観点から検討されたものであり、そのユーザビリティを評価することにより、安全かつ利用効率の高いシステムやアプリケーションが提供できることの議論が可能となる。

評価は、アプリケーションを複数用意して実験を行い、SUS のスコアと GTA により行われた。その結果、クライアント側暗号化と検索可能暗号利用について、未暗号化や検索可能暗号未利用などの他のアプリとの評価と SUS のスコアを見ても、GTA 分析をした結果を見ても、特筆すべき差異はなく、少なくとも SSE1 の適用についてはユーザビリティの問題点は確認されなかったと言える。

今回の実験により暗号化を適用してもオンラインストレージサービスのユーザビリティが低くないことが示されたことにより、より安全で快適なオンラインストレージ環境が実現できることが示された。

参考文献

[1] Evernote Japan 「お知らせ: Evernote プライバシーポリシーの変更を見直します」 EVERNOTE https://blog.evernote.com/jp/2016/12/16/55030

[2] Electronic Frontier Foundation「Secure Messaging Scorecard」 Electronic Frontier Foundation https://www.eff.org/node/82654

[3] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky; Searchable Symmetric Encryption:Improved Definitions and Efficient Constructions. the 13th ACM Conference on Computer and Communications Security (CCS 2006), pp.79-88, 2006.

[4] W. Ogata, K. Koiwa, A. Kanaoka, S. Matsuo. Toward Practical Searchable Symmetric Encryption.The 8th International Workshop on Security(IWSEC2013),2013

[5] 緑川達也, 金岡晃 ジョニーはまだ暗号化できない?：暗号化とユーザビリティに関する研究の調査（SPT2016）,2016

[6] Dropbox 「Dropbox のアーキテクチャ」 Dropbox Business https://www.dropbox.com/business/trust/security/architecture

[7] Richard Graham 「英会話上達：童話で英語学習」 元気イングリッシュ http://www.genkienglish.net/fairystoriesj.htm

[8] Ruoti, S., Kim, N., Burgon, B., Van Der Horst, T. and Seamons, K.: Confused Johnny: when automatic encryption leads to confusion and mistakes. In Proceedings of the Ninth Symposium on Usable Privacy and Security. ACM(2013).

[9] RACHEL FEINTZEIG, LAUREN WEBER「米最低賃金アップ、同時に高まる職場の緊張」THE WALL STREET JOURNAL http://jp.wsj.com/articles/SB12692037482832534161104582049733755391666

[10] Ruoti, S., Andersen, J., Heidbrink, S., O'Neill, M., Vaziripour, E., Wu, J., Zappala, D. and Seamons, K.: We're on the Same Page: A Usability Study of Secure Email Using Pairs of Novice Users. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 4298-4308). ACM(2016).

[11] Ruoti, S., Andersen, J., Hendershot, T., Zappala, D. and Seamons, K.: Private Webmail 2.0: Simple and easy-to-use secure email. In Proceedings of the 29th Annual Symposium on User Interface Software and Technology (pp. 461-472). ACM(2016).

[12] Wei Bai and Moses Namara and Yichen Qian and Patrick Gage Kelley and Michelle L. Mazurek and Doowon Kim.: An Inconvenient Trust: User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems. In Proceedings of the Ninth Symposium on Usable Privacy and Security. ACM(2016).

[13] 厚生労働省 千葉労働局 「最低賃金一覧表」 厚生労働省千葉労働局 http://chiba-roudoukyoku.jsite.mhlw.go.jp/jirei_toukei/chingin_kanairoudou/toukei/saitin/saitin01.html