ジョニーが検索するのを助ける：Webメールにおける対称型検索可能暗号の透過的適用

緑川 達也[1]　立川 彰宏[1]　金岡 晃[1]

概要：現在，オンラインでのメッセージのやり取りが一般的となっている．しかし，これらのサービスは便利である一方，データの漏えいというリスクが存在する．近年では，データを暗号化しているサービスもあるが，サービス事業者はデータを閲覧することが可能である．この問題の解決策としてユーザ側での暗号化が考えられ，電子メールを暗号化する仕様や実装は存在するが，どれも普及しているとは言い難い．それらの要因として，ユーザビリティの問題が考えられ，暗号化とユーザビリティに関する様々な研究が行われてきた．しかし，暗号化とユーザビリティについて議論はされているが，ユーティリティににについて言及している論文はない．我々は，ユーザビリティの向上にはユーティリティも大きく影響していると考える．本研究では、ユーティリティの中でも検索に焦点を当て、暗号化したまま検索することが可能な検索可能暗号を用いたシステムを実装し、実用性評価を行う．

キーワード：UWS，検索可能暗号，電子メールセキュリティ, End to End 暗号化, ユーザビリティ評価

1. はじめに

現在，オンラインでのメッセージのやり取りやクラウド環境へのデータのが保存が一般的となっている．しかし，これらのサービスは便利である一方データの漏えいというリスクが存在する．近年では，データを暗号化しているサービスもあり，サービス事業者とユーザ以外の第三者からデータの内容を閲覧することを難しくしているサービスもある．

Google は，Gmail に関する暗号化レポート「より安全なメール」を発表した [2]．このレポートでは Gmail のサーバを介して行う各サーバとの通信において，TLS (Transport Layer Security) を用いて暗号化されているかをいくつかの視点で報告している．また，Google はそれに先立ち Gmail のサービス上で宛先アドレスの電子メールサーバ間での通信に TLS がサポートされていない場合，赤く鍵がかかっていない状態を示した錠前のアイコンを表示するようにした [3]．Google はこのアイコンによる効果として，44 日間で受信したメールのうち暗号化通信されていたものが 25% 上昇したと発表した。

ここで注意しなければいけない点は，Web メールサービスにおける暗号化を考えた場合，2 つのポイントで行われることが考えられる．1 つは，サービスを提供している事業者のサーバとサービスを利用しているユーザとの間の通信の暗号化である．もう 1 つは，送受信される電子メールそのものの暗号化である．通信路の暗号化では，サービス事業者とユーザ以外の第三者が電子メールの内容を閲覧することを難しくしている．しかし，通信の暗号化の場合サービス事業者は電子メールの内容の閲覧が可能である．送受信者間でメール内容の暗号化を行っている場合，事業者もメール内容の閲覧が難しくなる．Google のレポートで言及されているのは前者であり，電子メールそのものの暗号化ではない．

電子メールそのものの暗号化としては PGP (Pretty Good Privacy) や GPG (GNU Privacy Guard)，S/MIME といった仕様や実装などがある．PGP や S/MIME は電子メールの暗号化だけでなく，電子メールへの電子署名も可能である．PGP や S/MIME は広く利用可能であるが，普及しているとは言い難い．その要因としてユーザビリティの問題が指摘され，多くの研究が行われてきた．1999 年,, Whitten と Tyger により発表された「Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0」[13] は，電子メールの暗号化とユーザビリティに焦点をあてた論文であり，この論文の発表以降，暗号化とユーザビリティの関係に強い注目が集まり，Whitten らの論文を参照した様々な研究が行われた．

[1] 東邦大学
Toho University

2013 年，Ruoti らにより「Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes」[7] が発表された．この論文では，Gmail のような既存 Web メールと緊密に統合するためにオーバーレイを用いるようなセキュアな Web メールシステムである Pwm (Private Webmail) が提案され，被験者実験が行われた．その後も Ruoti らは Pwm の改良版を用いた実験の論文を発表発表している [8], [9]．その他にも Web メールの暗号化とユーザビリティに関する多くの研究が行われてきた．これらの論文ではユーザビリティについては議論されているが，検索機能やソート機能についての議論はされていない．しかし，我々はユーザビリティを考える上でユーティリティも大きな影響を及ぼすと考えた．

本論文では，ユーティリティの中でも検索機能に焦点をあて，データを暗号化した状態で検索を行うことができる検索可能暗号を用いることで，ユーザビリティの低下の軽減を考えた．これを，Gmail に検索可能暗号を適用するための Chrome Extension を作成し，そのユーザビリティを System Usability Scale と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 を用いて評価した．実験の結果，すべての被験者からこのサービスを利用したい，使いやすいという回答があり，一定以上のユーザビリティがあることががわかった．

2. 関連研究

2.1 電子メールのユーザビリティに関する研究

1999 年, Whitten と Tyger によって「Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0」[13] が発表された．この論文は，はじめてセキュアな電子メールシステムのユーザビリティにおけるユーザ実験が行われた．この論文が発表されて以降，電子メール暗号化とユーザビリティに関する様々な研究が行われている．

また、Whitten と Tyger の論文の後、多くの研究が電子メールの暗号化におけるユーザビリティについて行われてきた [15], [16], [17], [18], [19]。前章で紹介した Ruoti らの Pwm はその中でも近年特に電子メール暗号化のユーザビリティに力を入れて研究がされている。

2.2 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 [10]。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。それらの項目に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 であり、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 であった。

3. 検索システムの危険性

本章では，メールソフトの Thunderbird と Outlook で検索インデクスがどのように実装されており，どのような危険性が存在するかについて言及する．また, 検索可能対称暗号を実装する際の検索インデクスの扱いについても言及する．

Mozilla が提供しているメールソフトの Thunderbird では，検索システム”Gloda”で検索を行っている [5]．Gloda は，Thunderbird ”global database” の略であり，SQLite を用いて実装されている．

> *Thunderbird includes a new message indexing and search system (gloda) that improves search performance, provides sophisticated full-text search capabilities and categorized search results.*

Microsoft が提供している Outlook では，Windows の検索システムを使っている．

検索可能対称暗号を適用したシステムを実装する場合，Search サーバが必要となる．そこで注目すべき点は、インデクスファイルの暗号化による保護である．インデクスファイルを平文のまま保存してしまうとインデクスファイルから情報が漏えいする危険性がある．また、断片的なインデクスの情報からメール本文の内容が推測でき，場合によっては完全な状態のメールを復元することも可能である．

例えば Java で実装されているオープンソース全文検索ソフトウェアである Apache Lucene の場合，公式サイトにインデクスファイルの内容が詳細に記載されており [4]，インデクスファイルと公式サイトの情報をもとにメールの内容を復元することが可能である．

このような点から検索可能対称暗号を適用したシステムを構築し第三者に Search サーバを委託する場合，メール本文だけでなくインデクスファイルも暗号化することが必要不可欠である．

4. システム構成

4.1 Web メールシステムへの検索可能暗号適用

Web メールシステムへ検索可能暗号を適用する場合，Web メールシステムそのものに検索可能暗号を適用する方法と既存サービスに上乗せするアドオン型の方法の 2 通りの方法が考えられる．将来的には、Web メールサービスを提供している企業やオープンソースの Web メールシステムに検索可能暗号を組み込むことで，Web メールサービスにおいて検索可能暗号が利用できることが理想的である．しかし、本研究では既存 Web メールサービスと検索可能暗号を適用した Web メールサービスとのユーザビリティの比較評価を行うため，前者は適していない．

そこで本研究では，アドオン型のサービスとして検索可能暗号を適用する方法を選択する．検索可能暗号の適用にあたっては，Curtmola らが提案した検索可能対称暗号の 1 つである Efficient SSE Constructure (以下，SSE1) を選択する．SSE1 は，検索可能暗号の代表的な手法であり，検索可能対称暗号の機能を明確に 4 つに分けていることなど，SSE を実装する際の基本的な構成であるため，本研究では SSE1 を採用した．

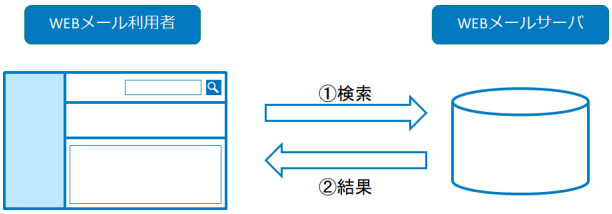

図 1　検索可能暗号適用前のシステム構成

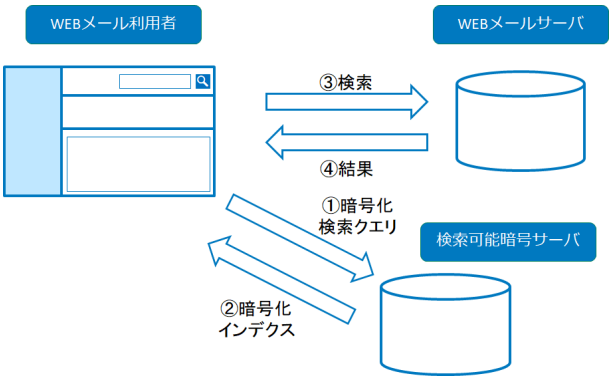

図 2　検索可能暗号適用後のシステム構成

検索可能の適用は，以下の流れで行う．

(1) 検索可能暗号サーバを用意
(2) 検索クエリを取得し検索可能暗号サーバへ送信
(3) 検索可能暗号サーバから返ってきた結果を Web メールサービスで検索
(4) 対象メール（群）を取得

4.2　Gmail への検索可能暗号適用

2013 年，Ruoti らが発表した論文 [7] において，Gmail に対し透過的に E2E 暗号化を適用する Extension の Pwm (Private Webmail) が提案された．本研究においても，既存 Web メールシステムとして Gmail を対象とし Chrome Extension を作成し検索可能暗号を適用することで Pwm に沿う形での実現を目指した．

提案システムはクライアント側の Chrome Extension は JavaScript で実装し，暗号化部分は CryptoJS を利用した．クライアント側では，SSE1 における Trapdoor の機能を組み込んでおり，入力されたキーワードに対する検索クエリ (Trapdoor) を作成し，Search サーバへ送信する．その後，Search サーバから受信した結果を Gmail で検索する．

サーバ側は Java で実装を行った．サーバ側では，SSE1 における Search の機能を組み込んでおり，クライアント側から送信された Trapdoor を受信することで，検索を行い検索キーワードを含んだメールの ID を回答する仕組みとなっている．

検索キーワードの入力から結果の出力までの一連の流れは，図 3 となっている．

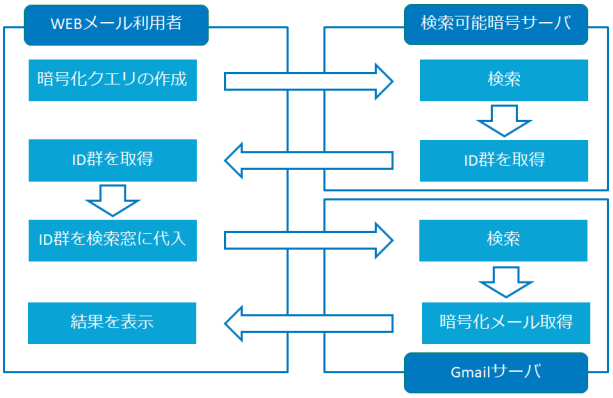

図 3　検索可能暗号適用後の検索フロー

5.　ユーザビリティ評価

本研究では，量的研究と質的研究の 2 つのアプローチから被験者実験を行う．実験結果の分析は，System Usability Scale (以下 SUS) の質問を行い，得られた結果をスコアリングすることで量的な分析を行う．また，SUS の回答と前提知識などに関する半構造化インタビュー結果と，実験中の行動を動画撮影した動画の内容から Grounded Theory Approach (以下 GTA) を行うことで質的な分析を行う．

5.1　実験情報

被験者の募集は，2017 年 7 月 18 日～2017 年 8 月 25 日に大学の Web メールと学内掲示板において行った．合計 4 人の被験者から応募があり，実験を行った．実験時間は 30 分であり，報酬は 500 円分の図書カードである．500 円という報酬については，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 時間あたり 10 ドル程度であった [7] が，最低賃金が 15 ドルへ引き上げられて以降 15～20 ドルへと変化しており [8], [9], [12]，その国の 1 時間あ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．その点から，本学がある千葉県の最低賃金が時給 842 円 (2017 年 7 月 18 日現在)[1] ，大学でアルバイトを行った際の賃金が時給 900 円であり，実験時間が 30 分であることから報酬は 500 円 (時給 1000 円) が妥当であると考えられる．

5.2 被験者情報

被験者は男性 1 人，女性 3 人の合計 4 人である．学科は情報系の学生 1 人，生物系の学生が 3 人である．

表 1 被験者情報

	性別	学年	学科
P1	女性	学部 4 年	生物分子科学科
P2	女性	学部 4 年	生物分子科学科
P3	男性	学部 4 年	情報科学科
P4	女性	学部 4 年	生物分子科学科

5.3 実験目的

本研究では，暗号化したまま検索することが可能な検索可能暗号を Chrome Extension により適用した Gmail と，検索可能暗号を適用していない通常の Gmail を比較し，検索機能のユーザビリティの評価を行う．

5.4 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．

5.5 実験で使用するアプリケーション

本実験では，検索可能暗号を適用していない通常の Gmail または Chrome Extension により検索可能暗号を適用した Gmail のいずれかを利用してもらい，それぞれのユーザビリティを評価し，検索可能暗号を適用した場合としていない場合のユーザビリティの比較を行う．検索可能暗号を適用した場合としていない場合の外観の差は，検索ボタンの虫眼鏡アイコンの有無と Google のお知らせの部分は異なるが，他の部分の外観は同一である．実験で使用する Gmail は表 2 となっている．

表 2 実験で使用する Gmail 情報

アプリケーション ID	内容
1	通常の Gmail
2	検索可能暗号を適用した Gmail

5.6 実験シナリオ

本実験では，被験者は東邦大学理学部の学生としてロールプレイを行う．

この学生は，大学の Web メールシステムであり履修情報や連絡事項、案内事項が掲載せれる ActiveAcademy から送られて来ているすべての案内メールを Gmail に転送設定している．普段のメールの利用は Gmail で行っており，過去に受け取った案内メールを調べる必要があり，メールの検索を行い必要な情報を探し出すタスクを行ってもらう．

5.7 実験方法

本実験では，より深く被験者の意識や行動を知るためにアンケートの回答に対するインタビューを行った．SUS の回答に対しその数値を選んだ根拠と事前知識や実験中の行動，システムに対する意見についてインタビューと作業の録画を行うことにより，被験者が利用した Gmail に対してどのように感じたかをより深く観察することが可能であると考えた．このことを踏まえ，実験の手順は以下となっている．

(1) 実験目的の説明
はじめに本研究の目的を説明し，その後作成したサービスと本実験の必要性を説明

(2) 実験内容の説明
実験内容の説明の前に前提の説明を行い，その後実際に行う作業の説明を行う．実際の内容は以下となっている．
前提：ActiveAcademy (大学の Web メールシステム) から送られて来ているすべての案内メールを Gmail に転送設定しており，普段のメールの利用は Gmail で行っている．
作業：過去に受け取った案内メールの中から指定の内容を含んだメールを探し出し，結果を回答用紙に記入する．探し出す内容は 5 つあり，問題はすべて回答用紙に記載している．

(3) 作業

(4) SUS アンケートの記入

(5) SUS アンケートと事前知識, 実験に関するインタビュー
インタビューの内容は，SUS アンケートの項目に対してその数値を選択した根拠を伺う．事前知識，実験に関するインタビューは，事前知識に関する内容が 5 つと実験に関する内容が 3 つである．また，その回答に対し追加で質問を行う場合もある．前提知識に関する質問は，以下である．
(a)「Gmail の利用経験はありますか？」
「利用頻度はどれくらいですか？」
(b)「メール本文が暗号化しているか気にしたことはありますか？」
(c)「LINE や Facebook メッセンジャーのメッセージが暗号化しているか気にしたことはありますか？」
(d)「LINE や Facebook メッセンジャーは，初期設定でメッセージ本文が暗号化されていることはご存知ですか？」
(e)「Web メールから情報が漏えいするとしたら，どこから漏えいすると思いますか？」
実験に関する質問は，以下である．
(a)「メールを検索することにストレスを感じましたか？」
If Yes 「ストレスを感じた要因はどこにあると感

じましたか？」

(b)「メール本文が暗号化されていることの認識はありましたか？」

(c)「検索キーワードが暗号化されていることの認識はありましたか？」

本実験で使用するメールデータは，実際に大学から送られてきたメールの内容を実験用に変更した 100 通のメールを用意した．また，作業の際に探し出す内容については実験用のデータと気づかれないようにオープンキャンパスや学園祭，ガイダンスなどの日時や場所など，通常の学生生活を送っている上で受け取る可能性のあるものを 5 つ選出した．

5.8 評価方法

本研究では，実験の評価方法として通常の Gmail または検索可能対称暗号を適用した Gmail のいずれかを利用してもらい，SUS のアンケートと事前知識や実験中の行動などに対するインタビューに回答してもらう．SUS アンケートから得られたスコアから量的な分析を行い，事前知識や実験中の行動などに対するインタビュー結果と録画映像から GTA を用いて質的な分析を行う．

6. 実験結果

6.1 System Usability Scale

本実験で得られた SUS スコアは，表 3 となっている．作業時間は、実際に作業に取り掛かってから作業が終了するまでの時間を示している。

表 3 SUS スコア

	利用サービス	SUS スコア	作業時間
P1	2	80	5:44
P2	1	95	5:01
P3	2	67.5	5:34
P4	1	85	3:55

6.2 使いやすさへの言及

使いやすさに対する質問に対しては, すべての被験者が普段とかわらないという回答であった．しかし，以下の意見があった．

P1 : 利用するのにソフトなどをインストールしなきゃいけないとなったらちょっと…．あんまりパソコン詳しくないので．

このことから，サービスの使いやすさだけでなくインストールのしやすさなども使いやさに影響を与えることが考えられる．

特に興味深い行動が，P3 のブラウザの検索機能を用いたことである．この検索は今回の実験の対象外ではある．しかし，興味深い指摘である．我々が検討した脅威では，検索に関連するキーワードやインデクスも守らねばならない，という脅威モデルを検討したが，ブラウザ内検索は脅威モデルでの検討外であった。ブラウザ内の検索が脅威となるケースは、最終的に復号されたコンテンツが画面上に表示されたときに漏えいするケースであり、マルウェア感染によるメモリ内容の不正閲覧や、ショルダーハッキングによる覗き見など、暗号化では対応できないものとなっている。

6.3 ストレス

サービスを使用した際のストレスについては，検索可能暗号を適用した場合としていない場合ともに多くの被験者が「使用する際にストレス感じなかった.」と回答した．

P3 : 1 個だけあるのが，オープンキャンパスで検索したときに入っていないのも引っかかる．そこくらい．

P3 が感じたストレスは検索可能暗号を適用したことに対するストレスではなく，Web メールのインデクス作成時のインデクス内容に起因に対するストレスである．

6.4 Gmail の利用経験

Gmail の利用経験については，被験者全員が利用経験があると回答た．2 人は，Web サイトからの利用ではなくアプリからの利用であった．多くの利用者がショッピングサイトの会員登録などに利用しダイレクトメールを受信する程度で，日常的に利用しており利用方法を熟知しているとは言えない．

6.5 情報漏えいへの言及

ヒアリングの回答として被験者全員が情報漏えいへの言及を行っていた．しかし、そこでの回答は本研究の目的とは異なる面での言及であった．被験者全員が、電子メールに関連する情報漏えいとなると、自身の電子メールアドレスの漏えいが意識されている様子であり、いずれも電子メール本文などのメールコンテンツの漏えいへの言及はしていなかった。

P1 : ニュースなどを見ていると，メールの機能を提供している企業や個人でインターネットでウイルスなどに感染して漏えいしているのかなーと思います．

P2 : サイト．例えばネットなどで検索をしているときにウイルスにかかってそこから．

また，情報漏えいの経路に関する質問に対しては，システムの問題ではなくフィッシングサイトのようなサイトやウイルスに感染することによる漏えいという意見がすべてであった．この要因として考えられることは，P1 の回答にあるようにニュースの報道が大きいと考えられる．

これらの結果から，コンテンツの暗号化の必要性，ある

いは脅威モデルとして我々が設定したものに関しての脅威は意識していないと考えられる．

6.6 暗号化機能の知識

前提知識に関する質問に対しすべての被験者が, メールや LINE，Facebook メッセンジャーの本文やメッセージが暗号化されているか気にしていないという回答であった．また，LINE や Facebook メッセンジャーが初期設定でメッセージ本文が暗号化されているということをほとんどの被験者が知らなかった．

> P2：暗号化．LINE の本文を保存したいときに暗号化というキーワードがでてきて暗号化っていうシステムみたいなものはあるんだなっていうのは知ってました．

P2 は，暗号化というシステムがあることは知っていたがどの情報が暗号化されているかなどの詳しい情報まで知らなかった．

提案システムでは，メール本文と検索キーワードが暗号化されていたことの認識に対しては，1 人は認識がなかった．通常の Gmail では，1 人は認識がなく，もう 1 人は事前説明を受けたことにより暗号化されているという認識はあったが，使用している段階での認識はなかったという回答であった．

P3 は，検索キーワードの入っていないメールが検索結果に入っているということから，なんらかの処理が行われているという認識はあった．しかし，この問題はメールに対するインデクス作成で利用し Apache Lucene の問題であり検索可能対称暗号の本質的な問題ではない．ここで考えなくてはいけないことは検索の挙動がおかしいことに気付いたのが，新しい機能を適用したという説明を行ったことによるかどうかである．仮に，説明したことによるものだとすると透過的に適用することで解決するかである．この問題については，2013 年 Ruoti らにより発表された論文 [7] で言及されている．この論文では透過的にするとユーザは混乱を招くと述べられている．しかし，2016 年 Wai らに発表された論文 [12] で言及された鍵管理モデルのことから透過的にすることにより検索可能対称暗号のユーザビリティが向上することは十分に考えられる．

7. Discussion and Limitation

7.1 被験者の人数

本研究では，被験者数が 4 人と少なく量的分析を行うためには不十分であった．半構造化インタビューと GTA の結果から属性による傾向とみられる結果は得られたものの，属性によるものと断定させるにはデータ量が不十分であった．そのため今後より大規模な被験者実験を行う必要がある．

7.2 検索システムとしての性能

「メールを検索することにストレスを感じましたか？」という質問に対し，P3 の「検索キーワードが入っていないメールも検索結果に表示されていた」という回答は，今後実験を行う上で興味深い回答であった．検索キーワードの入っていないメールが表示されたことは，インデクスを作成した際に利用した Lucene の問題であり検索可能暗号の本質的な問題ではないものの，今後改善すべき課題である．この回答から考えなくてはいけないことは，なぜ検索キーワードが含まれていないメールが表示されていることに気付いたかである．

7.3 OR 検索の必要性

検索可能暗号を適用する場合，検索可能暗号サーバから返ってきた ID を既存システム検索するため検索結果が複数であると OR 検索できることが必須条件である．しかし，OR 検索のできる Web メールシステムを調査した結果，既存サービスでは Gmail と Yahoo!メール，オープンソースの Web メールシステムでは Zimbra の 3 種類のみであった．

また，本研究で使用した SSE1 では単一キーワードでの検索しかできず，Gmail や Yahoo!メールのように複数キーワードでの検索ができない．今後よりユーザビリティの高いサービスを実装するためには複数キーワード検索や部分一致検索のできる方式の採用を検討しなくてはいけない．

7.4 鍵管理

鍵管理の問題も今後の大きな課題である．Ruoti ら Pwm ではプライベート鍵の発行をサーバで行い，その鍵を受け取る形となっている．2016 年 Bai らによって発表された論文 [12] でこの問題について言及している．この論文では，利用者同士で鍵管理を行う Exchange model と鍵を登録しておく Registration model のユーザビリティの比較実験が行われている．この実験の興味深い結果が，被験者は Registration model の潜在的な危険性を理解し，Exchange model の方が安全であることを認識したうえで，日常的な目的では Registration model で十分と回答したてんである．このことから，今後サービスを実装するうえで Registration model のサービスが考えられる．

7.5 電子メールシステムへの適用

Web メールのサービスに対する，ブラウザの Extension という方向性で実現したが，SSE 適用自体はこれを制限するものではない．Web メールシステムとしてコンテンツ暗号化と SSE を包含するシステムにすることも可能である。例えば，Web メールシステムとしての OSS である Squirell メールなどは先述のとおり OR 検索ができないので、直接適用はできない。

その部分についてはシステム内の検索に Include させることが重要である．またクライアント側での検索も適用は可能である．脅威モデルとして，ローカルからの盗難などによる漏えい保護として電子メールクライアントで利用される検索インデクスを暗号化して SSE 対応化させることも可能である。いずれもパフォーマンスに問題はないと思われる。

8. まとめ

被験者実験の結果，すべての被験者からこのサービスを利用したい，使いやすいという回答があった．また，「このサービスを利用できる自信がある」という質問に対しても「強くそう思う」「そう思う」という回答であり，検索可能暗号を適用した Gmail も通常の Gmail と同様に利用しやすく，わかりやすいサービスとなっていると言える．しかし，P3 の「検索キーワードが入っていないメールも検索結果に表示されていた」という回答から，このことに気付いた要因を考察した．仮に検索可能暗号を適用したことを説明したことにより気付いたとした場合，透過的に適用することで気付かないかもしれないという仮説を得た．この仮説を調査するためにもより大規模な調査が必要である．また，より使いやすいサービスとするために SSE1 以外の複数キーワード検索などのできるより機能が充実した検索可能暗号の採用を考える必要がある．

参考文献

[1] 千葉県最低賃金 http://chiba-roudoukyoku.jsite.mhlw.go.jp/jirei_toukei/chingin_kanairoudou/toukei/saitin/saitin01.html

[2] Google: より安全なメール透明性レポート Google, 2016, https://www.google.com/transparencyreport/saferemail/

[3] Nicolas Lidzborski, Jonathan Pevarnek, ”More Encryption, More Noti cations, More Email Security”, Google Security Blog, 2016, https://security.googleblog.com/2016/03/morencryption-more-noti cations-more.html

[4] Apache Lucene 公式サイト https://lucene.apache.org/core/6_6_0/core/org/apache/lucene/codecs/lucene62/package-summary.html

[5] Gloda https://developer.mozilla.org/en-US/docs/Mozilla/Thunderbird/gloda

[6] Herzberg, A. and Leibowitz, H.: Can Johnny Finally Encrypt? Evaluating E2E Encryption in Popular IM Applications. In ACM Workshop on Socio-Technical Aspects in Security and Trust (STAST)(2016).

[7] 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).

[8] 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).

[9] 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).

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

[11] Unger, N., Dechand, S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I. and Smith, M.: SoK: secure messaging. IEEE Symposium on Security and Privacy (SP). IEEE(2015).

[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] Alma Whitten, J.D.Tyger: Why Johnny Encrypt: A Usability Evaluation of PGP 5.0, 8th USENIX Security Symposium(1999).

[14] Simson L.Garfinkel, Robert C.Miller: Johnnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express, Symposium On Usable Privacy and Security(SOUPS)(2005).

[15] Simson L.Garfinkel, Jeffrey I.Schiller, Erik Nordlander, David Margrave, Robert C.Miller: Views,Reactions and Impact of Digitally-Signed Mail in e-Commerce, Financial Cryptography and Data Security(FC'05)(2005).

[16] Simson L.Garfinkel, David Margrave, Jeffrey I.Schiller, Erik Nordlander, Robert C.Miller: How to Make Secure Email Easier To Use, the SIGCHI Conference on Human Factors in Computing(CHI'05)(2005).

[17] Volker Roth, Tobias Straub, Kai Richter: Security and Usability Engineering with Particular Attention to Electronic Mail, HCI International(2005).

[18] Steve Sheng, Levi Broderick, Colleen Alison Koranda: Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software, Symposium On Usable Privacy and Security(SOUPS)(2006).

[19] Tobias Straub, Harald Baier: A Framework for Evaluating the Usability and the Utility of PKI-enabled Applications, 1st EuroPKI(2004).