Vol.2016-GN-99 No.13
Vol.2016-SPT-18 No.13
2016/5/13

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

緑川 達也[1,a)]　金岡 晃[1,b)]

概要：1999 年 Whitten と Tyger により「Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0」が発表された．この論文は，PGP 5.0 のユーザビリティについて検証を行った論文であるが，セキュリティとユーザビリティという分野に対して多くの先駆的な考え方を持ち込んだ論文でもある．その後，暗号化とユーザビリティについて多くの研究がなされた．また暗号化のみならずプライバシーやフィッシングなどセキュリティの全般でユーザビリティの研究が活性化するきっかけともなった．Whitten らの論文からどのように暗号化とユーザビリティの研究が進み，そして現在ではどういった段階にいるのかを調査する．そして調査した結果をふまえ，いくつかの考察を加えて今後暗号化とユーザビリティに関する研究がどの方向に向かうかを予測する．

Can't Johnny Still Encrypt?: A Survey of Encryption and Usability Studies

Tatsuya Midorikawa[1,a)]　Akira Kanaoka[1,b)]

Abstract: In 1999, Whitten and Tyger published a paper named "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0". While usability of PGP 5.0 is a main target of the paper, it brings several important factor to the study field of usability and security. Not just a lot of paper about encryption and usability follows the paper, a lot of paper about wider security feature like privacy and phishing, and usability follows the paper. In this paper, we survey how academic studies have been follows the Whitten's paper, and show where we stand now. Based on the survey, we add some consideration about future direction of encryption and usability.

1. はじめに

オンラインでのメッセージのやり取り，クラウドコンピューティング環境へのファイルの送受信や保存など，暗号化が求められている分野がいまあらためて注目されている．

Google が 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 [25]．そこでは 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）を用いて暗号化がされているかをいくつかの視点で報告がされている．また Google はそれに先立ち，Gmail のサービス上で，宛先アドレスと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に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 [31]．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がされていたものが 25%上昇したとした．

注意しなければいけない点がある．Web ブラウザでメールソフト（メーラ）が動くような Web サービス型の電子メールシステムを用いる場合，暗号化は 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環境とサービスを利用しているユーザの利用者環境間の通信の暗号化であり，もう 1 つはそこで送受信される電子メールそのものの暗号化の 2 つである．通信路の暗号化では，事業者と利用者以外の第 3 者は送受信される電

[1] 東邦大学
Toho University
[a)] 6516007m@nc.toho-u.ac.jp
[b)] akira.kanaoka@is.sci.toho-u.ac.jp

子メールの内容そのものを閲覧することを難しくするが，事業者が電子メールの内容を閲覧することは可能である．電子メールそのものの暗号化を送受信者間で行っている場合では，事業者は電子メールの内容を閲覧することが難しくなる．Google のレポートは前者の通信路暗号化についてのものであり，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）やその実装である GPG（GNU Privacy Guard），あるいは S/MIME (Secure / Multipurpose Internet Mail Extensions) といった仕様と実装が広範で利用可能となっている．PGP や S/MIME は電子メールの暗号化だけではなく，電子メールへの電子署名も行うことができる．PGP や S/MIME が多くの環境で利用可能になっている一方で，それらが普及しているとはいい難い．そこにはユーザビリティの問題があると指摘がされ，多くの研究がされてきた．1999 年に Whitten と Tyger により発表された「Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0」[50] は，電子メールの暗号化とそのユーザビリティの問題について焦点を当てた．この論文以前でも使い勝手に関する議論は存在した可能性があるが，この論文が発表されたことで暗号化とユーザビリティの関係について強い注目が向かい，その後 Whitten らの論文を参照として様々な研究が生まれた．

本論文では，Whitten らの論文により暗号化とユーザビリティの研究が本格的に始まったととらえ，Whitten らの論文からどのように暗号化とユーザビリティの研究が進み，そして現在ではどういった段階にいるのかを調査する．そして調査した結果をふまえ，いくつかの考察を加えて今後暗号化とユーザビリティに関する研究がどの方向に向かうかを予測する．

2. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

1999 年, Whitten と Tyger によって「Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0」[50] が発表された．この論文はセキュリティに焦点をあてた効果的なユーザインタフェースについて述べられた代表的な論文である．

ほとんどのコンピュータセキュリティにおける失敗の原因はユーザのエラーによるものだとし，その中でセキュリティのためのユーザインタフェースは扱いにくく混乱を招いたり，あるいはそもそも存在していないと指摘した．この問題に対して Whitten と Tyger は，単にセキュリティに標準的なユーザインタフェースデザイン技術を適用できなかったのではなく，逆に効果的なセキュリティは標準とは異なるユーザビリティが必要であり，他のタイプのソフトウェアに適したユーザインタフェースデザインでは解決されないと主張している．

そこでこの仮説を検証するために，当時セキュリティに関するツールの中では良いユーザインタフェースを持っていると評された PGP 5.0 を対象にケーススタディが行われた．ケーススタディでは，PGP 5.0 が有効な電子メールセキュリティを実現するために暗号化初心者が使用できるかどうか評価するための実験室実験（Lab Study）と認知的ウォークスルーによる分析が行われた．この論文では，セキュリティにおけるユーザビリティを以下のように定義した．

- 利用者がやるべきセキュリティの作業を確かに（Reliably）認識する
- 利用者がそれらの作業をうまく（Successfully）実施する方法を理解可能である
- 利用者が危険なエラーを起こさない
- 利用者がそのインタフェースを継続して使うことを十分に快適に感じる（Comfortable）

定義されたユーザビリティと実験結果から，PGP 5.0 にはいくつかのユーザインタフェース上の欠陥があると指摘した．公開鍵のモデルを理解していない被験者への理解醸成が難しいことや，モデルを理解した被験者でも鍵を取得して暗号化することが難しいこと，また暗号化の作業と誤解して誤って自身の秘密鍵（Private Key）を送る被験者もいた．そして，テスト参加者のほとんどが 90 分間で PGP 5.0 を用いて署名とメッセージ暗号化ができないことを実証した．

この論文は，PGP 5.0 のユーザビリティについて検証を行った論文であるが，セキュリティとユーザビリティという分野に対して多くの先駆的な考え方を持ち込んだ論文でもある．上述した求められるユーザビリティについての定義だけでなく，ユーザビリティを考える際に必要となるセキュリティに関連する特性についてのリストアップ，評価としてのユーザ実験方法など，与えた影響は大きい．この論文以降，様々な論文で暗号化とユーザビリティについて発表がされている．また暗号分野以外においても，セキュリティの広範囲の分野でユーザビリティ研究のきっかけになっており，似たタイトルであるが別分野の研究もおおく存在する．3 章以降ではこれらを「電子メール暗号化と電子署名」「メッセージ暗号化」「ファイル暗号化」「その他」に分けて紹介をしていく．

ちなみに，この論文のタイトルは 1955 年に Rudolph Flesh によって書かれた書籍"Why Johnny Can't Read: And What You Can Do about It"[18] を元にしたものである．この書籍は，子供に対してどうやって国語 (英語) を家庭で教えるかについて書かれており，その後このタイトルを元にしたさまざまな文章が生まれている．多くは元の書籍の"read"を変形した形になっており，Whitten らの論文もそれにあたる．Google で"why johnny can't"

と検索すると，Whitten らの論文をはじめ，”program”，”think”，”code”，”write”などが結果に表れる．

3. 電子メール暗号化と電子署名

本章では，電子メール暗号化と電子署名について書かれた論文について紹介する．

「How to Make Secure Email Easier To Use」[22] は 2005 年に Garfinkel らにより発表された．この論文では，暗号化や電子署名の方式である PEM，PGP，S/MIME の 3 つをターゲットとし，Amazon.com で品物を販売している 470 人に対してアンケートを実施し分析を行った．その結果，被験者の大多数が電子署名された電子メールを利用できることを主張した．

2005 年に同じく Garfinkel を主著として「Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express」[19] が発表された．Garfinkel らはこの論文において Whitten らの論文 [50] と同様のアプローチで電子メール暗号化に関するユーザ実験を行った．ただし，対象は異なっている．Whitten らの論文では電子メール暗号化と電子署名として PGP を対象にしていたが Garfinkel らの論文では S/MIME が対象となっていた．Garfinkel らは論文中で「Whitten らが示した点は PGP 5.0 にとどまらない問題である」としてユーザビリティに関する Whitten らの視点は広範にあてはまるものだと指摘した．

Garfinkel らの論文では，S/MIME における署名を簡略にするために提案されていた KCM（Key Continuite Management）を用い，KCM に対する初めてのユーザ実験を行った．ユーザ実験は Whitten らの論文に沿った形で行われたため彼らはその実験を「Johnny 2」と呼んでいる．

ユーザ実験は，以前に S/MIME などのセキュアな電子メールを使用したことがない先入感のない被験者に対して行われた．提案されたセキュアな電子メールのインタフェースは，ソーシャルエンジニアリング攻撃の影響は著しく受けにくくなるが，受信者が知らないメールアドレスからの新しいアイデンティティにによる攻撃はまだ有効であったとした．提案システムでは，すでにメッセージを送信したことがある相手などに対してのインタフェースが付与されていたことが大きな点だと考えられる．そして Whitten らの論文では指摘がなかった新たな視点として「フィッシングの危険性」を示した．

続く 2006 年には Sheng らにより「Why Johnny Still Can’t Encrypt: Evaluating the Usability of Email Encryption Software」[45] が発表された．この論文では特に，Whitten らの論文で扱われた PGP5 に対して，論文発表時での PGP9 との比較を行った．調査対象の作業行為としては，鍵ペアの生成，公開鍵の取得・検証，電子メールの暗号化・復号，電子署名の付与と検証，そして公開鍵と秘密鍵のバックアップの保存が挙げられる．それらについて存在する問題を見つけるためにパイロット研究が行われた．

2013 年になり，Ruoti らが「Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes」[40] を発表した．この論文では，Gmail のような既存の 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) が提案された．Pwm では，鍵管理と暗号化の自動化を含めほとんどが透過的 (transparent) に行われる．Pwm による自動化の効果により，多くの被験者が誤って平文の電子メールを送信することの防止や，Pwn への信頼をすることを示した．Pwm への信頼を示さなかった被験者は，その透過性ゆえに信頼が得られなかったと結論づけている．

この論文で最も注目すべきは別の実験である．これは Ruoti らも指摘しているが，続いての実験として暗号化を行うにあたり利用者に一定の作業が必要となるようにカスタマイズした Pwm（Ruoti らはこれを Message Protector（MP）と呼んだ）でユーザ実験を行ったところ，暗号文などを切り取り貼り付けるような余分なステップを被験者らが受け入れ，そしてより高い信頼を得たという結果を示した．

Ruoti らにより示された透明性の削減とより大きな信頼を得る方法としての手動暗号化の意味はシステム設計を再考する必要性があることを示唆した．

Straub らによって 2004 年に発表された「A Framework for Evaluating the Usability and the Utility of PKI-enabled Applications」[48] では，PKI 対応アプリケーションのユーザビリティとユーティリティを評価するための汎用的なフレームワークが提示された．また Roth らにより発表された「Security and Usability Engineering with Particular Attention to Electronic Mail」[39] では，ユーザに透過的に動作するベストエフォートな鍵交換と鍵維持方式が考案されている．非侵入型の方法でユーザに送受信メールの状態を伝える補完的な可視化およびインタラションな技術も記述されている．実用評価のため，結果を表示するユーザのメール挙動の定量分析の結果，個々の非商業的ユーザのために，鍵のアウトオブバウンドの検証が第三者が発行した公開鍵証明書の信頼を確立するより経済的かもしれないと主張している．Garfinkel らに 2005 年に発表された「View, Reaction and Impact of Digitally-Signed Mail in e-Commerce」[20] では，Amazon.com 出品者の経験，知識および電子署名された電子メールの認証に関して調査が行われた．調査の結果，インターネットベースの出品者は，”ベストプラクティス”として電子署名された電子メールを送るべきであると結論付けられた．本論文は Garfinkel らによる他の論文 [22] と類似した内容となっているが別の論文となっている．さらに同じく Garfinkel らが

上記のものより先に 2003 年に発表しあた「Enabling Email Confidentiality through the use of Opportunistic Encryption[21] では，Opportunistic Encryption とセキュリティプロキシを使った電子メールセキュリティへの新しいアプローチが提案されている．

Gaw らにより 2006 年に発表された「Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-Mail」[24] では，電子メールを暗号化するかどうかおよび時期についてユーザ決定の背後にある社会的コンテキストについて考察している．一般的に，暗号化に関する決定はユーザビリティなどの技術的問題だけでなく，社会的要因によっても起こる．社会的要因を理解することがより広く採用される暗号化技術デザインには必要であると主張している．そして Perlman らにより 2008 年に発表された「User-centric PKI」[36] では，インターネットブラウザから Web サイトへ認証する方式と認証が列挙され，Bobba らにより 2009 年に発表された「Usable Secure Mailling Lists with Untrusted Servers」[5] では，ソフトウェアシステムのユーザビリティを高め，SELS に関する経験について説明されている．

これらのいずれの論文も Whitten らの論文を参照しており，いずれも Whitten らの論文の影響を大きて開始した，あるいは Whitten らのアプローチを別角度からとらえて進めた研究のアプローチとなっている．

4. メッセージ暗号化

本章では，メッセージ暗号化について書かれた論文について紹介する．

Fahl らが 2012 年に発表した「Helping Jonny 2.0 to Encrypt His Facebook Conversations」[15] では，電子メールでのユーザビリティに関する研究がされている一方で，Facebook のメッセージセキュリティやその関連分野での研究がほとんどされていないことを指摘した．

Fahl らはまず Facebook 上のプライベートメッセージを保護するために明確な意欲を示した 514 人に対して，スクリーニング調査を行った．そこでは，個人的な Facebook メッセージは Facebook 社が閲覧可能であることを知っているかどうかや，それを気にしているか，などが質問された．そこでは 324 人 (66.53%) の被験者が気にしていることが示された．そしてその時点で Facebook のメッセージが暗号化できるソリューション群などを考慮して，暗号化のユーザインタフェースと鍵管理オプションという 2 つの特徴に焦点を当て，プロトタイプを作成してさらなるユーザ実験を行った．そこでさらに 2 つの発見として「鍵管理の自動化」と「鍵リカバリ機能」の重要性を挙げ，それに従いサービスを開発して最終的な実験を行った．

その結果，すべての被験者が提案されたサービスを使用した場合，エラーなく正常に Facebook のメッセージを暗号化でき，提案されたメカニズムが有用であることが示された．

2012 年に Schrittwieser らにより発表された「Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Aplications」[44] では，モバイル環境でのメッセージングや VoiP アプリケーションが増加したことを受けそれらのアプリケーションに焦点をあてて調査を行った．

調査では 9 つの人気モバイルメッセージングと VoIP アプリケーションを認証メカニズムに焦点を当てて分析し，それらのセキュリティモバイルの評価を行った．Schrittwieser が論文発表を行った 2012 年のころは，スマートフォン用のモバイルメッセージングや VoIP アプリケーションの新しいものが多く市場に投入されていた．これらのサービスは，他の加入者に無料の通話やテキストメッセージを提供する．そして SMS，MMS や音声通話のようなセルラーネットワークのキャリアによって管理される従来の通信方式に代わるインターネットベースの手段を提供していることも特徴である．調査分析の結果，調べたアプリケーションのほとんどは，アカウントを識別するための一意のトークンとしてユーザの電話番号を使用していることを見つけ，また主要なセキュリティ上の欠陥がテストしたアプリケーションのほとんどで存在することを示した．さらに，攻撃者がアカウントを乗っ取り送信者 ID を騙したりすることも可能であることも示した．

ユーザビリティの実験としては電子メールに比べてまだ日が浅いと言える一方で，これらの分野は大きく近年盛り上がりを見せている．1 つの原動力は EFF（電子フロンティア財団，Electronic Frontier Foundation）が整備した”Secure Messaging Scoreacard”であろう [12]．そこでは 30 を超えるさまざまツールに対して，「送信時の暗号化」や「事業者が読めないような暗号化が施してあるか」など 7 つの項目について評価を行っている．また EFF はこれらは Secure & Usable Crypto という新しい EFF キャンペーンの最初のフェーズであることを言っており，今後さらに注目が浴びられることが予想される．

5. ファイル暗号化

本章では，ファイル暗号化について書かれた論文について紹介する．

2003 年に Wright らにより発表された「Cryptographic File Systems Performance: What You Don't Know Can Hurt You」[52] では，ファイルシステムの暗号化について焦点をあて，従来問題になるだろうと思われていたパフォーマンスを実装により評価を行い，パフォーマンスが問題ないものであることを示した．パフォーマンスを中心にした暗号化ファイルシステムの実用性に関しての論文であり，ユーザビリティの評価は主なトピックではないが，

暗号化ファイルシステムを実現するにあたり示された 5 つの技術群である「ブロックベースのシステム」「ディスクベースのファイルシステム」「ネットワークループバックベースのシステム」「スタック可能なファイルシステム」「アプリケーション」として示されたうちの「アプリケーション」内に，ファイルアクセスの都度の暗号化や復号により引き起こされる問題点について指摘しており，そこで Whitten らの論文 [50] を参照している．

Stanek らにより 2014 年に発表された「A Secure Data Deduplication Scheme for Cloud Storage」[47] では，クラウドコンピューティング環境においてデータ漏洩が問題視され，それに伴いエンド間での暗号化が求められるようになった背景について説明をした．そしてファイル暗号化により起きうるクラウドコンピューティング側としての重複除外（Deduplication）の問題についての対応として，ポピュラーなファイルについては暗号化を行わず，ポピュラーでないファイルについては暗号化で保護する仕組みを提案し，その安全性をランダムオラクルモデルで示し，またベンチマークとシミュレーションで性能評価を行った．ユーザビリティについては直接の研究テーマではないが，提案している仕組みの中で必要となる信頼される第 3 者（Trusted Thrid Party, TTP）の実現において，実際にはユーザビリティを確保することを考えた場合は TTP の実現そのものがセキュリティの目的となることがあるとしてユーザビリティについて言及している．またその際に参照している論文は Fahl らの論文 [15] であった．

Peltka らにより 2006 年に発表された「Cryptographic Security for a High-Performance Distributed File System」[37] では，ファイル暗号化システムと分散ストレージエリアネットワーク (SAN) ファイルシステムの実現のための一般的なデザインの説明，実装が行われている．今日ストレージシステムは，ますます攻撃対象となっている．ファイル暗号化システムは，クライアントが暗号化および完全性保護，E2E でのセキュリティ保証をすることでデータをさらす危険性が軽減される．実装は，ハッシュ木を通してファイル暗号化と完全性保護のサポートがされている．2 つの技術は，クライアントのファイルシステムドライバに実装されている．この論文では先述した Wright らの論文 [52] を参照しているものの，論文中にユーザビリティについて言及はされていない．

Opera らにより 2007 年に発表された「Integrity Checking in Cryptographic File Systems with Constant Trusted Storage」[34] も Peltka らの論文と同様，Wright らの論文 [52] を参照しているものの，論文中にユーザビリティについて言及はされていない．

いずれもユーザビリティを直接扱った論文ではなく，別の暗号化のアプリケーション分野で問題視されているユーザビリティについて触れたものとなっている．

6. その他

3 章から 5 章で挙げた論文とは分類としては異なるものの，Whitten らが書いた「Johnny」をもとに書かれたと思われる論文はまだ多く存在する．本章ではこれらを紹介していく．

6.1 暗号系

Whitten らの論文 [50] を参照している論文としては，Clark らにより 2011 年に発表された論文 [10] や Shin らにより 2011 年に発表された論文 [46]，Egele らにより 2013 年に発表された [11] がある．いずれも直接的にユーザビリティについて提案等をしたものではなくすでに広まっている対象に対してユーザビリティの視点をもって調査を行ったものとなっている．特に Clark らの論文 [10] はタイトルも Whitten のものを踏襲している．

また，直接 Whitten の論文を参照していないものの中でも，Whitten の論文を参照した論文を参照している，いわば孫論文のようなものも多く存在しており，暗号に関連した論文では，2015 年に Eskandari らにより発表された論文 [14], 2009 年に Lin らにより発表された論文 [32], 2013 年に Clark らにより発表された論文 [9], 2006 年に Cagalj らにより発表された論文 [6], 2008 年に Chen らにより発表された論文 [7] がある．

6.2 ”Johnny”という名称利用

Whitten らが名付けた「Johnny」は他の研究者の琴線を刺激したのか，多くの論文がそれを踏襲するなどしてユーモアのある論文タイトルを見ることができる．その中でも 2010 年に Kumaraguru らにより発表された論文 [29] と 2009 年に Amir Herzberg により発表された論文 [26] と 2011 年に Atzeni らにより発表された論文 [2] はいずれもフィッシングに関連した研究となっており、フィッシングも 1 つのユーザビリティとセキュリティという分野における大きなテーマ領域であることがわかる．

それ以外にも多く存在している [1], [3], [4], [28], [30], [35], [41], [42], [43], [51]．興味深いのが Ruoti らによる [43] である．[43] 自身はタイトルに Johnny を含まないが，彼らはこの論文の当初の版を arXiv.org に掲載しており，その際のタイトルは「Johnny and Jane: Analyzing Secure Email Using Two Novice Users」となっていた．

7. 今後の予測

本章では，前章までの調査を踏まえ，今後の予測をする．

7.1 ユーザビリティと暗号

暗号とユーザビリティについての根本的な問題は解決されたとは言い難い．解決は基礎研究，応用研究，実装と実

社会への展開といくつもの段階で考えうるものであるが，まだいずれの段階でも解決できていないのではないかと考える．基礎研究として要素技術を 1 つ注目すると解決しているように思えるが，それらを応用研究などで実証を踏まえようとすると多くのものが新たな課題に面することになるだろう．

なによりそれが，Whitten らがその論文で Introduction の最初に語られている以下の文章について，解決したと言い切れないところが如実に現在の状況を示しているのではないかと考える．

> *Security mechanisms are only effective when used correctly. Strong cryptography, provably correct protocols, and bug-free code will not provide security if the people who use the software forget to click on the encrypt button when they need privacy, give up on a communication protocol because they are too confused about which cryptographic keys they need to use, or accidentally configure their access control mechanisms to make their private data world-readable.*

7.2 ID ベース暗号

暗号とユーザビリティを議論するにあたり，大きな課題となるのが公開鍵暗号の取り扱いである．公開鍵による暗号化や検証鍵による署名検証を行う際の鍵はどうやって取得しどうその情報を信頼するのか，など，現実的な展開を考慮すると，ユーザビリティの議論対象となるエンドユーザにとっては技術的な知識への障壁が大きいのは否めない．

ID ベース暗号は ID 情報をはじめとした任意の情報を公開鍵として設定可能であるため，公開鍵暗号で多く利用されている PKI（Public Key Infrastructure，公開鍵基盤）で行われている鍵所有者と鍵情報の結びつきの保証が必要ないことで期待されている技術ではあるが，ID ベース暗号を現在広く利用されている公開鍵暗号である RSA 暗号や ECDSA 署名，ECDH 鍵交換などと共に広くオープンな世界で利用するとなると，やはり「提供された ID 情報の確認」と「提供者の信頼」が必要になるなど，PKI と同じ仕組みが求められてしまい，本質的な解決とはならない．利用範囲や用途などが限定された範囲内では，PKI による仕組みの多くがすでに同意されているものとして省略可能とできるために，そういったケースでは ID ベース暗号が有効になるであろう．しかしそういったケースでユーザビリティの問題はこれまでの暗号化とユーザビリティの問題と併せて議論すればよいかは疑問である。多くの研究対象が敷いている前提であるオープン性とは大きく異なる点に注意が必要だ。

7.3 メッセージ暗号化のユーティリティ

2 者間でメッセージが暗号化される場合，暗号化には 2 種類あることにまず注意が必要である．1 つはメッセージをやり取りする通信路の暗号化であり，もう 1 つはメッセージそのものの暗号化である．通信路の暗号化は重要な 1 つの要素ではあるが，クラウドコンピューティング環境をはじめとしたサービス事業者にはメッセージデータが平文で手に入ることになるため，見知らぬエンティティから覗き見られることを防ぐことはできるが，本来エンド間でしか見えないものと期待されているメッセージはエンド間の 2 者だけでなくサービス事業者も見ることができる．

そのため，メッセージそのものの暗号化によるメッセージ暗号化が進むと考えられる．その点は EFF の Secure Messaging Scorecard における評価項目の 1 つとなっており，今後注目すべき動きであると言えよう．

一方で，エンド間で暗号化をする場合には，暗号化がされてしまうがためにサービス事業者によって提供される数々の便利な付随サービスが受けられなくなる，あるいは受けることにコストがかかる，ということが予想される．もっとも身近なものは検索機能であろう．過去に大量に蓄積されたメッセージから検索により特定のメッセージを探しだすことは，メッセージングツールであれば当然備えている機能である．大量に蓄積されたメッセージは現在の状況ではエンド側の環境（クライアント環境）に保持することは考えづらく，同じく検索のためのインデックスもエンド側環境で保持することは考えづらい．蓄積されたメッセージが大量であればあるほど，検索のためのインデックスも巨大になり，それをエンド側が保持することは現実的ではなくなる．そうなると検索ができ，かつ，サービス事業者側に検索のためのインデックスが存在し，そしてそのインデックスからは情報が漏れない，ということが求められる．

検索可能暗号はそれを解消する技術として十分に期待され，対称型の検索可能暗号はパフォーマンスとしても十分に期待できるレベルに現時点で達していると言ってよい．しかし，このユーザビリティについては現時点では全くといっていいほど考慮されていない．今後は検索機能を中心とした，こういったメッセージ暗号化により阻害されうるユーティリティ機能についてユーザビリティの研究として焦点が当てられていくであろう．

参考文献

[1] Erinn Atwater, Cecylia Bocovich, Urs Hengartner, Ed Lank, Ian Goldberg: Leading Johnny to Water: Designing for Usability and Trust, Symposium On Usable Privacy and Security(SOUPS)(2015).

[2] Andrea Atzeni, Cesare Cameroni, Shamal Faily, John Lyle, Ivan Flechais: Here's Johnny: a Methodology for Developing Attacker Personas, The 6th Interna-

tional Conference on Availability, Reliability and Security(ARES)(2011).
[3] Zinaida Beneson, Gabriele Lenzini, Daniela Oliveira, Simon Parkin: Sven Uebelacker, Maybe Poor Johnny Really Cannot Encrypt - The Case for a Complexity Theory for Usable Security, New Security Paradigms Workshop(NSPW)(2015).
[4] Kemal Bicakci, Nart bedin Atalay, Hakan Ezgi Kiziloz: Johnny in Internet Cafe: User Study and Exploration of Password Autocomplete in Web Browsers, The 7th ACM workshop on Digital identity management(DIM'11)(2011).
[5] Rakesh Bobba, Joe Muggli, Meenal Pant, Jim Basney, Himanshu Khurana: Usable Secure Mailing Lists with Untrusted Servers, The 8th Symposium on Identity and Trust on the Internet(IDtrust'09)(2009).
[6] Mario Cagalj, Srdjan Capkun, Jean-Pierre Hubaux: Key Agreement in Peer-to-Peer Wireless Networks, Proc. of the IEEE, Vol.94, Issue. 2, pp 467-478, (2006).
[7] Chia-Hsin Chen, Chung-Wei Chen, Cynthia Kuo, Yan-Hao Lai, Jonathan M.McCune, Ahren Studer, Adrian Perring, Bo-Yin Yang, Tzong-Chen Wu: GAnGS: Gather, Authenticate'n Groups Securely, The 14th Mobile Computing and Network(MobiCom'08)(2008).
[8] Wiliam Cheswick: Johnny Can Obfuscate: Beyond Mother's Maiden Name, USENIX Workshop on Hot Topics in Security(HotSec)(2006).
[9] Jeremy Clark, Paul C.van Oorschot: SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements, 34th IEEE Symposium on Security and Privacy(2013).
[10] Sandy Clark, Travis Goodspeed, Perry Metzger, Zachary Wasserman, Kevin Xu, Matt Blaze: Why(Special Agent)Johnny(Still)Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System 20th USENIX Security Symposium(2011).
[11] Manuel Egele, David Brumley, Yanick Fratantonio, Chistopher Kruegel: An Empirical Study of Cryptographic Misuse in Andoroid Applications, 20th ACM Conference on Computer and Communications Security(2013).
[12] Electoronic Froutier Foundation, "Secure Messaging Scorecard", https://www.eff.org/secure-messaging-scorecard.
[13] Carl Elison, Steve Dohrmann: Publick-key support for group collaboration, ACM Transactions on Information and System Security(TISSEC)(2003).
[14] Shayan Eskandari, David Barrera, Elizabeth Stobert, Jeremy Clark: A First Look at the Usability of Bitcoin Key Management, The Network and Distributed System Security Symposium(NDSS)(2015).
[15] Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, Uwe Sander: Helping Johnny 2.0 to Encrypt His Facebook Conversations, Symposium On Usable Privacy and Security(SOUP)(2012).
[16] Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, Lars Baumgarther, Bernd Freisleben: Why Eve and Mallory Love Android: An Analysis of Android SSL(In)Security, 22nd ACM conference on Computer and Communications Security(CSS)(2012).
[17] Sascha Fahl, Marian Harbach, Thomas muders, Matthew Smith: Confidentiality as a Service–Usable Security for the Cloud, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications(TrustCom)(2012).
[18] Rudolph Flesch: Why Johnny Can't Read: And What You Can Do about It, Harper, 1995.
[19] 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).
[20] 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).
[21] Simson L.Garfinkel: Enabling Email Confidentiality through the use of Opportunistic Encryption, The annual national conference on Digital government research(dg.o'03)(2003).
[22] 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).
[23] Simson L.Garfinkel, Robert C.Miller: The Johnny 2 Standardized Secure Messaging Scenario, Symposium On Usable Privacy and Security(SOUPS)(2005).
[24] Shirley Gaw, Edward W.Felten, Patricia Fernandez-Kelly: Secrecy,Flagging, and Paranoia: Adoption Criteria in Encrypted E-Mail, the SIGCHI Conference on Human Factors in Computing(CHI'06)(2006).
[25] Google: より安全なメール透明性レポート Google, 2016, https://www.google.com/transparencyreport/saferemail/
[26] Amir Herzberg: Why Johnny can't surf(safely)? Attacks and defenses for web users, Journal of Computers & Security(2009).
[27] Amir Herzberg, Ronen Margulies: Training Johnny to Authenticate(Safely), 33th IEEE Security & Privacy(2012).
[28] Amir Herzberg, Ronen Margulies: Forcing Johnny to Login Safely Long-Term User Study of Forcing and Training Login Mechanisms, 16th European Symposium on Research in Computer Security(ESORICS)(2011).
[29] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong: Teaching Johnny Not to Fall for Phish, ACM Transactions on Internet Technology(TOIT)(2010).
[30] Pedro G.Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, YangWang: Why Johnny Can't opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising, the SIGCHI Conference on Human Factor in Computing Systems(CHI'12)(2012).
[31] Nicolas Lidzborski, Jonathan Pevarnek, "More Encryption, More Noti
cations, More Email Security", Google Security Blog, 2016, https://security.googleblog.com/2016/03/more-ncryption-more-noti
cations-more.html
[32] Yue-Hsun Lin, Ahren Studer, Hsu-Chun Hsiao, Jonathan M.McCune, King-Hang Wang, Maxwell Krohn, Phen-Lan Lin, Adrian Perring, Hung-Min Sun, Bo-Yin Yang: SPATE: Small-group PKI-less Authenticated Trust Establishment, The 7th Mobile System,Applications,and Services(MobiSys 2009), 2009.
[33] Greg Norcie, Jim Blythe, Kelly Caine, L Jean Camp: Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems, The 2014 Network and Distributed System Security Symposium(NDSS)(2014).
[34] Alina Oprea, Michael K.Reiter: Integrity Checking in Cryptographic File Sytems with Constant Trusted Stor-

age, 16th USENIX Security Symposium(2007).
[35] Hilarie Orman: Why Won't Johnny Encrypt?, IEEE Internet Computing(2015).
[36] Radia Perlman, Charlie Kaufman: User-centric PKI, The 7th Symposium on Identity and Trust on the Internet(IDtrust'08)(2008).
[37] Roman Pletka, Christian Cachin: Cryptographic Security for a High-Performance Distributed File System, 24th IEEE Conference on Mass Storage Systems and Technologies(MSST)(2006).
[38] Karen Renaud, Melanie Volkamer, Arne Renkema-Padmos: Why Doesn't Jane Protect Her Privacy?, Performance Evaluation of Tracking and Surveillance(PETS'14)(2014).
[39] Volker Roth, Tobias Straub, Kai Richter: Security and Usability Engineering with Particular Attention to Electronic Mail, HCI International(2005).
[40] Scott Ruoti, Nathan Kim, Ben Burgon, Timothy van der Horst, Kent Seamons: Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes, Symposium On Usable Privacy and Security(SOUPS)(2013).
[41] Scott Ruoti, Jeff Andersen, Daniel Zappala, Kent Seamons: Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client, arXiv.org, http://arxiv.org/abs/1510.08555 (2015).
[42] Scott Ruoti, Jeff Andersen, Travis Hendershot, Daniel Zappala, Kent Seamons: Helping Johnny Understand and Avoid Mistakes: Comparison of Automatic and Manual Encryption in Email, arXiv.org, http://arxiv.org/abs/1510.08435 (2015).
[43] Scott Ruoti, Jeff Andersen, Scott Heidbrink, Mark O'Neil, Elham Vaziripour, Justin Wu, Daniel Zappala, Kent Seamons: "We're on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users, Special Internet Group on Computer-Human Interaction(SIGCHI)(2016).
[44] Sebastian Schrittwieser, Peter Fruhwirt, Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Markus Huber, Edgar Weippl: Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications, The Network and Distributed System Security Symposium(NDSS)(2012).
[45] 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).
[46] Dongwan Shin, Rodrigo Lopes: An Empirical Study of Visual Security Cues to Prevent the SSLstripping Attack, The 27th Annual Computer Security Applications Conference(ACSAC'11)(2011).
[47] Jan Stanek, Alessandro Sorniotti, Elli Androulaki, Lukas Kencl: A Secure Data Deduplication Scheme for Cloud Storage, Financial Cryptography and Data Security(FC 2014)(2014).
[48] Tobias Straub, Harald Baier: A Framework for Evaluating the Usability and the Utility of PKI-enabled Applications, 1st EuroPKI(2004).
[49] Wenley Tong, Sebastian Gold, Samuel Gichohi, Mihai Roman, Jonathan Frankle: Why King George III Can Encrypt, http://randomwalker.info/teaching/spring-2014-privacy-technologies/king-george-iii-encrypt.pdf, 2014.
[50] Alma Whitten, J.D.Tyger: Why Johnny Encrypt: A Usability Evaluation of PGP 5.0, 8th USENIX Security Symposium(1999).
[51] Patrick F.Wilbur, Todd Deshane: Johnny can drag and drop: determining user intent through traditional interactions to improve desktop security, the 4th Symposium on Computer Human Interaction for the Management of Information(CHiMiT'10)(2010).
[52] Charles P.Wrigjt, Jay Dave, Erez Zadok: Cryptographic File Systems Performance: What You Don't Know Can Hurt You, the 2003 IEEE Security in Storage Workshop(SISW'03)(2003).