情報処理学会論文誌 Vol.59 No.12 2120–2131 (Dec. 2018)

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)]

受付日 2018年3月12日, 採録日 2018年9月7日

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．また暗号化だけでなくプライバシ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．

キーワード：ユーザビリティ，ユーザブルセキュリティ，暗号

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

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

Received: March 12, 2018, Accepted: September 7, 2018

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.

Keywords: usability, usable security, encryption, cryptography

1. はじめに

2010 年代後半に入り，メッセージの送受信者自身による暗号化（エンドツーエンド暗号化, End-to-End Encryption, 以後 E2E 暗号化）の重要性が増している．Facebook Messenger や WhatsApp，LINE といったメッセージングツールや，Web サイトへのアクセスすべてを Transport Layer Security（TLS）で暗号化を行う総 HTTPS 化（Always on SSL，AOSSL）など，近年での代表的な E2E 暗号化の例がある．

重要性が増した 1 つの理由として，Edward Snowden による告発があげられる．2013 年，Edward Snowden は米国 NSA が通信監視プログラムにより複数の Web サービスに対する情報を収集していることを告発した．その後，いくつかの企業は依頼により情報提供や対応などを行っていたことを明らかにし，大きな社会問題となった．2014 年に電

[1] 東邦大学
Toho University, Funabashi, Chiba 274–8510, Japan
[a)] 6516007m@nc.toho-u.ac.jp
[b)] akira.kanaoka@is.sci.toho-u.ac.jp

子フロンティア財団（Electronic Frontier Foundation）が代表的なメッセージングツールのE2E暗号化対応やその周辺の項目についての調査と評価を行ったSecure Messaging Scorecard [24] が公開され，E2E暗号化に向けた促進運動が始まった．さらに2016年になり，先述したメッセージングツールがE2E暗号化対応を行い，Let's Encryptプロジェクトにより無償のTLS証明書が正式に配布されるようになるなど，E2E暗号化は広まりを見せている．

暗号化がエンドユーザにとって必要になり，より身近になる一方で，適切な暗号を施すことの難しさがある．暗号技術そのものが破られるのではなく，暗号の不適切な利用により情報が漏えいする危険性がいくつも指摘されている．Heningerらの調査では，インストール時に初期設定の鍵が設定されていてそのままソフトウェアを利用してしまっているケースが多く存在することが明らかにされている [41]．またFahlら [27] やUS-CERTの調査 [19] ではAndroidアプリケーションの多くにWebサーバ証明書の検証不備が見つかっていることが示されている．前者はソフトウェアの利用者が適切に暗号を扱えなかった事例であり，後者はソフトウェア開発者が適切に暗号を扱えていない事例である．

E2E暗号化が促進される一方で，利用者や開発者が不適切な暗号を施すなど暗号の適切な利用の難しさがあり強いギャップが生じている．暗号を適切に使い情報を守ることの重要性は今あらためて考えなければならない課題となっており，そのギャップを埋める暗号化とユーザビリティに関する研究が注目されている．

暗号化とユーザビリティに関する研究は，電子メールに対する暗号化を対象に進められてきた．電子メールに対する暗号化は広く整備されてきており，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多くの環境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にくい．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Tygarにより発表された「Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0」[74] 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とTygarの論文を参照としてさまざまな研究が生まれた．

WhittenとTygarによる論文では，セキュリティにおけるユーザインタフェースは従来のユーザインタフェースと異なる設計が必要であることや，セキュリティにおけるユーザビリティの定義などを行い，電子メールの暗号化とユーザビリティの問題を明らかにしただけでなく，後に続くユーザブルセキュリティやユーザブルプライバシの研究に対し先駆的な考え方をいくつも持ち込んだ．

この論文が発表されてから20年近くが経とうとしている今，時代背景の変化もあり暗号化のユーザビリティはさらに重要な課題となっている．一方で，先述したように暗号が適切に扱われていないケースがまだ存在している．著者らは，いまここであらためて暗号化とユーザビリティの問題点と現状を整理し，その解決に向けたアプローチを再考する必要があると考えた．そこで本論文では，暗号化とユーザビリティの問題点の解決に向けた材料として整理された情報の提供を行うことを目的とし，WhittenとTygarの論文以降どのように暗号化とユーザビリティの研究が進み現在ではどういった段階にあるかを調査し整理を行う．そしてその解決に向けたアプローチはどうあるべきかを考察していく，

本論文の構成は以下のとおりである．まず2章でこの分野に先鞭をつけたWhittenとTygarの論文を紹介する．3章では，エンドユーザ向けの暗号化とそのユーザビリティについて研究されてきた分野を取り上げ，整理を行う．そして4章では開発者に向けた暗号化とユーザビリティについての研究分野を述べる．5章ではこれまであげたそれぞれの研究対象に共通する領域として鍵管理について述べる．6章では暗号化とユーザビリティに関連するその他の事項について紹介をし，7章では今後の予測を考察する．最後に8章でまとめる．

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

1999年，WhittenとTygarによって発表された論文はセキュリティに関して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 [74]．

WhittenとTygarは，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，そのなか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かったりすると指摘した．この問題に対して，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た．

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がされた．公開鍵暗号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ことがユーザインタフェース上の欠陥として指摘された．そして，テスト参加者のほとんどが PGP 5.0 を用いて署名とメッセージ暗号化を行う作業を 90 分間以内にはできないことを実証した．

Whitten と Tygar による論文は，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，しかし後世により影響を与えているのは，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点である．上述したようにセキュリティにおけ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，さまざま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多く存在する．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」，「鍵管理」，「その他」に分けて紹介をしていく．

3. エンドユーザ向けの暗号化とユーザビリティ

3.1 電子メール暗号化と電子署名

電子メールの暗号化は Whitten と Tygar が対象にしたように，暗号化とユーザビリティの研究では初期に大きく注目されていた分野であり，充実した研究がされている．暗号化だけではなく，電子メールへの電子署名についてもユーザビリティの観点から研究されている論文も多い．本節では，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．

Garfinkel らにより 2005 年に発表された論文 [36] 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 を主著として書かれた別の論文 [33] では，Whitten らの論文 [74] と同様のアプローチで対象を S/MIME に変えて電子メール暗号化に関するユーザ実験を行った．その結果，Whitten の指摘と同様な問題が存在することを示した，

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，知人などを偽装するような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，未知メールアドレスからメールが届くタイプの攻撃がまだ有効であることも示された．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 Sheng らにより発表された論文 [68] では，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あげられる．それらに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．その結果，公開鍵の検証や電子メールの暗号化は引き続き問題点が残ることを示したことに加え，電子署名の付与に関しては PGP5 よりも悪化していることが指摘された．

1999 年より電子メールにおける暗号化や電子署名の標準的な技術を対象にユーザビリティがいくつも研究されていたが，2000 年代後半になりそれらの研究がいったん落ち着きを見せた．2010 年代に入り，改めて電子メールの暗号化とユーザビリティについて焦点を当てたのは Ruoti らの研究チームである．2013 年になり，Ruoti らが 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レイを用いるセキュアな Web メールシステム Pwm（Private WebMail）を提案した [62]．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，誤って平文の電子

メールを送信することを防止し，多くの被験者がPwmへの信頼を示した．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もう1つ行われた実験である．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．WhittenとTygarの論文，またそれに続くGarfinkelらの論文がターゲットにしていた標準的な技術から一歩先に進んだ独自技術による透過的な暗号化は，暗号化とユーザビリティの研究に新たな焦点を当てることとなった．

そのほかにも電子メールの暗号化とユーザビリティに関する論文は複数存在する．ここではそれらを簡単に紹介する．

Straubらによって2004年に発表された論文 [71] 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論文 [60] 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．そこではさらに可視化とインタラクション技術によりユーザに送受信メールの状態を伝える手法も提案されている．実験結果により鍵の検証にPKIとは別の手段を用いたほうが経済的である可能性を指摘している点が興味深い．

Garfinkelらにより2005年に発表された論文 [34] 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．さらに同じくGarfinkelらが上記の論文 [34] より先に2003年に発表した論文 [35] 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年に発表された論文 [39] では，電子メールを暗号化するかの意思決定および暗号化タイミング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年に発表された論文 [56] 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年に発表された論文 [9] 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とTygarの論文を参照しており，論文の影響を受けて開始した，あるいは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．

3.2 メッセージ暗号化

暗号化とユーザビリティの研究は電子メールを端緒に開始されたが，時代が進むにつれ，Web技術をもとに電子メールよりも手軽に利用可能なメッセージングツールが普及してきた．このメッセージングツールで送られるメッセージについてもデータの秘匿やプライバシなどの問題が潜んでおり，同じく暗号化とユーザビリティに焦点があてられることとなった．電子メールも広くメッセージングツールと考えることも可能であるが，より手軽に利用可能なプラットフォームとして電子メールとは異なる視点も必要なものがあるなど，研究としての広まりがある．本節では，それらの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年に発表した論文 [26] 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」の重要性をあげ，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論文 [67] 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

焦点を当てて調査を行った．

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アプリケーションが多く市場に投入されていた時期であった．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．それは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特徴を持っていた．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，またアカウントのハイジャックやユーザのなりすましなど主要なセキュリティ上の欠陥が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いえる一方で，メッセージングの暗号化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[22]．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いっており，今後さらに注目が浴びられることが予想される．

E2E暗号化がさまざまなプラットフォーム，アプリケーションにおいて適用が進んでいる一方で，それらの安全性は必ずしも十分ではないケースが多い．たとえばAppleによるE2E暗号化アプリケーションであるiMessageでは，Garmanらにより暗号化や署名での問題が指摘された[38]．Facebook Messengerをはじめ，欧州でのシェアが高いWhatsAppなどで採用されているSignalについても暗号学的な安全性について問題点が指摘されている[15], [17], [61]．日本およびアジア各国で広く利用されているLINEでは，独自に開発したE2E暗号化方式Letter Sealingが採用されており，ユーザ同士のメッセージ交換だけでなくグループ内でのメッセージ交換も暗号化がされている．Letter Sealingの仕様は2016年に発表されたホワイトペーパー[52]に記載されているが，2018年にIsobeらによって発表された論文[46]でLINEのE2E暗号化の安全性解析が行われ，具体的な複数の問題点が指摘された．代表的なメッセージングアプリではE2E暗号化が高いユーザビリティを目指して進んでいるものの，脆弱性が次々と指摘されておりその難しさを示している．脆弱性の指摘や安全性の議論は技術仕様が公開されているからこそ可能なものであり，E2E暗号化仕様が公開されていることは高く評価したい．

4. 開発者向けの暗号化とユーザビリティ

2章および3章であげていた研究は実際のサービスやソフトウェアを利用するエンドユーザのユーザビリティを議論し研究されたものであった．2010年代後半に入り，ユーザビリティとセキュリティ・プライバシを扱う研究分野に大きな転換訪れた．それがエンドユーザを広く対象にした研究から，よりユーザ属性に特化した研究への移行である．たとえばユーザ属性を特殊な業務に携わるユーザと特化して行った研究[18], [72]や，年齢層を特化した研究[48]，身体的な特徴を持つユーザに特化した研究[20]などがあげられる．そのなかで注目すべきは，開発者というユーザ特性に特化したユーザブルセキュリティの研究である．

暗号化とユーザビリティの問題は，1章でも指摘したように，エンドユーザ側で起こる問題とともに，開発時に起きてしまう問題も抱えている．開発者の本来の開発モチベーションはそのソフトウェアやサービスが実施したい本来目的に強く向いており，セキュリティやプライバシはそのソフトウェアやサービスが本来実施したいものではないことが一般的になる．ハードウェアやソフトウェアライブラリの高度化により，ソフトウェアやサービスが可能にすることも多く多岐にわたるようになり，充実したユーザエクスペリエンスを提供できるようになった．一方で，高度化に応じたリスクの増大から暗号化が果たす役割も大きくなりその適切な実施が重要になってきた．開発者はハードウェアやソフトウェアライブラリの高度化に応じた新たな知識獲得に注力する一方で適切な暗号化を求められることになった．そのなかで，開発段階で暗号利用に問題があるケースが多く報告されることになってきた．Androidの多くのアプリでTLS証明書の検証に不備がある問題では，一部のアプリは検証時に無条件に検証成功とだすケースが示され，中間者攻撃が容易に実現してしまうリスクが顕在化していた[19], [27]．また銀行が提供するアプリにおいて，独自暗号が適用されているケースや暗号鍵がソフトウェアにそのまま記載されている，いわゆるハードコーディングがされているケースも見つかっている[58]．

Acarらは開発段階で暗号利用に問題がある点に注目し，暗号ライブラリのユーザビリティやそのあり方についての研究を行っている．2016年のSecDev2016における論文では，開発者側のユーザブルセキュリティに注目し研究対象の整理が行われており[1]，その後暗号利用やTLSの脆弱性につながる開発者の行動や感覚などを調査し明らかにしてきた[2], [3]．先述したAndroidの不適切な検証においては，1つの可能性として開発者たちによるQ&A Webサービスの影響が指摘された．Q&Aサービスではソースコー

ドの一部を記載することが可能であり，開発者はそれらのコードを再利用して活用していたが，その掲載コードが脆弱であるケースが明らかにされた．コード再利用については，Fischer らにより Q&A サイト Stack Overflow の Android アプリケーションへの影響についての調査が行われ，開発者側に存在するセキュリティ技術適用の問題がさらに明らかにされている [32]．Imai らはその影響についての調査を時系列を含めて解析し，その問題をさらに明確化した [45]．

5. 鍵管理

本章では鍵管理について書かれた論文の紹介と現状について言及する．鍵管理は大きく分けてユーザに鍵管理を任せる鍵交換モデル（Key Exchange Model）と鍵の発行や管理などを鍵管理サーバに任せる鍵登録モデル（Key Registration Model）の 2 種類がある．

鍵交換モデルの代表的なものは，1991 年にジマーマンによって開発された Pretty Good Privacy（PGP）や 1995 年に多数のセキュリティベンダによって開発された S/MIME などがある．このモデルは 1990 年代～2000 年代に開発されたものが多く従来型のモデルといえる．

鍵登録モデルの代表的なものには，Apple 社が提供している iMessage や WhatsApp 社が提供している WhatsApp Messenger，Facebook 社が提供している Facebook Messanger，LINE 社が提供している LINE などのメッセージアプリがある．これらのアプリやサービスは，複数デバイスでの利用などの用途をふまえて鍵管理をより容易にすべくサービス側で鍵管理を行いエンドユーザは意識せずに利用できる．Ruoti らによって開発された Pwm [62] もこの方式を採用している．このモデルは 2010 年以降に普及したものが多く比較的新しいモデルといえ，近年鍵登録モデルを採用するサービスが増えてきている．

2016 年に Bai らによって発表された論文 [6] において，この両モデルを対象にセキュリティのレベルやユーザの認識について研究がされた．エンドユーザ側とすれば，鍵管理を意識せずに行うことが可能な鍵登録モデルにユーザビリティの高さを感じる一方で，暗号鍵管理を委託することのリスクを認識していないことが容易に予想された．しかし被験者は鍵登録モデルの潜在的な危険性を理解し，鍵交換モデルの方が安全であることを認識したうえで，日常的な目的では鍵登録モデルで十分であるとする回答が半数を超えた．この結果は非常に興味深いものである．2013 年に Ruoti らの研究で提案された Pwm は，暗号化を自動的に行うことでユーザに透過性のある暗号化を実現していた．そのユーザビリティを評価する目的で Ruoti らは同じ機能を手動で暗号化操作を行う Message Protector（MP）を用意し，両者に対してユーザ実験を行った [62]．その結果，Pwm よりも MP がユーザの満足度と信頼性の高さを示す結果となり，完全に透過的な暗号化は逆にエンドユーザの信頼を増やすことにはつながらず煩雑とも思える作業を経ることで信頼が高まることが示された．

2016 年の Bai らの結果は 2013 年の Ruoti らの結果の逆を示すものであり，3 年間という短い期間でありながらもで鍵登録モデルが急速に受け入れられるようになり，ユーザの意識が変わった可能性がうかがえた．

6. その他

3 章から 5 章であげた論文とは分類としては異なるものの，Whitten らが書いた論文を参照して書かれた論文であり，暗号技術やセキュリティに関連す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 暗号技術に関連する論文

Whitten らの論文 [74] 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 [14] や Shin らにより 2011 年に発表された論文 [69]，Egele らにより 2013 年に発表された [21] がある．いずれも直接的にユーザビリティについて提案など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 [14] はタイトルも Whitten のものを踏襲している．

直接 Whitten の論文を参照していないもののなかでも，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 [25]，2009 年に Lin らにより発表された論文 [51]，2013 年に Clark らにより発表された論文 [13]，2006 年に Cagalj らにより発表された論文 [10]，2008 年に Chen らにより発表された論文 [11] がある．

6.2 Web の HTTPS 化

メッセージの暗号化とは異なるが，エンド側暗号化の 1 つの事例として 2010 年代に入り大きく進んでいるのが Web の HTTPS 化である．ユーザビリティの面では特にユーザインタフェースに関する研究と改良が Google 社の Chrome ブラウザを中心に活発に行われている．

Web で提供されるサービスでは，ユーザ ID とパスワードの入力を行うログイン画面や個人の情報を入力する画面，決済に関連する作業を行う画面など，限られた場所で HTTPS が利用されサービスのトップ画面や検索画面といった部分には HTTPS は用いられることは少なかった．2010 年代より，サイトすべてを HTTPS 化するという動きが目立ってきた．それを後押しした 1 つは Let's Encrypt に代表される安価ないしは無料で取得可能な Web サーバ証明書であろう．その進展については Felt らが調査結果を発表しており，そこでは各国における HTTPS の対応状況などが示されている [29]．

総HTTPS化はGoogle社が特に推進をしている様子がブラウザにおけるURLのバー表示にも表れている．Googleが提供しているブラウザChromeでは2018年7月に公開されるChrome68以降httpのページを開いた際に新たに「Not Secure」の文言が表示されるようになることが発表されている[66]．Chromeは証明書の状態表示方法や文言，フィッシングサイトやマルウェア配布サイトの遮断表示方法など，ユーザインタフェースに関して暗号化という観点だけでなくより広い視点からユーザビリティに取り組んでおり[30], [31]，それらの取り組みの1つとしてE2E暗号化にかかわる表示が行われている．

通信のTLS適用に関しては，電子メールの送受信でのTLS適用にも注目したい，2016年にGoogleが発表したGmailに関する暗号化レポート「より安全なメール」[40]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[50]．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．

このように，Webなどの通信路暗号化としてのE2E暗号化がTLSによりけん引されており，エンドユーザに向けた施策が研究レベルではなく実運用レベルで行われている．そしてエンドユーザに対する暗号関連の表示方法も時代に応じて変化している様子も分かる．

6.3 ファイル暗号化

電子メールやメッセージングツールのようにエンドユーザとしての送受信者がいるわけではないが，電子ファイルをクラウド事業者などに預けるサービスやソフトウェアも一般化してきており，そのなかでエンド側でのファイル暗号化が議論されるようになってきた．本節では，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論文[76]では，ファイルシステムの暗号化について焦点を当て，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，Whittenらの論文[74]を参照していた．また，ファイル暗号化と完全性を議論したOpreaらによる2007年の論文[54]やファイル暗号化と分散ストレージファイルシステム実現を議論したPeltkaらによる2006年の論文[57]では直接のユーザビリティの議論はないもののWhittenらの論文が参照されている．

Stanekらにより2014年に発表された論文[70]ではファイル暗号化による重複除外（Deduplication）への対策が議論されたが，そのなかでユーザビリティに言及されており，暗号化とユーザビリティに関してFahlらの論文[26]が参照されていた．

ファイル暗号化についてはユーザビリティ研究がさかんとはいえないが，これまでの暗号化とユーザビリティの研究への言及や参照がされており，今後はこの分野でのユーザビリティ研究が進むことが考えられる．

7. 今後の予測

本論文では，3章でエンドユーザ向けの暗号化とユーザビリティについて，電子メールの暗号化と電子署名，そしてメッセージ暗号化の研究について言及をしてきた．4章では開発者向けの暗号化とユーザビリティの研究の進展について触れ，5章では暗号化のユーザビリティの面で暗号化と復号とともに重要となる鍵管理における研究状況について触れた．そして6章ではユーザビリティとそのほかの暗号技術やセキュリティに関連する研究について概観をした．

その結果，暗号化とユーザビリティについてはユーザビリティを求めるなかで透過的な暗号化が進展しており，鍵管理のユーザ感覚が2010年代後半に入り大きな変化を迎えている様子が分かった．また，電子メールを中心に研究されてきた暗号化とユーザビリティは，メッセージングやそのほかのアプリケーションに研究の裾野を広げてきていることもうかがえた．

これらをふまえて，本章では今後の暗号化とユーザビリティ研究の方向性を考察する．

7.1 暗号化とユーザビリティ

長らく研究が行われてきた暗号化とユーザビリティは，自動的に暗号化や復号を行うことを透過的と呼びRuotiらが始めた研究[62]や，各メッセージングツールの透過的な暗号化により，暗号化や復号の作業をエンドユーザが意識せずに行うことが広まりを見せている．そして暗号化と復号の作業の自動化により，鍵管理も透過的に行われることが増えた．2013年のRuotiらの研究では，過度の透過性はユーザの信頼を損なう恐れがあるとした一方で，2016年にBaiらの研究[6]の結果は，ユーザは鍵管理の透過性にリスクがあることを認識したうえで信頼している状況を示しており，この数年でエンドユーザの認識に大きな差が生まれることとなった．

E2E暗号化はエンド間だけが情報を知りサービス事業者などの第3者が内容を見ることができないことに意味があり，鍵管理の透過性を実現している鍵登録モデルではそのサービス事業者に暗号鍵を預けていることからE2E暗号化の意味が一部失われることになる．サービス事業者を信

頼できる組織として認識し，そのほかを信頼できないものとするモデルとなり，これまでの「通信にかかわる 2 者」と「それ以外」という 3 者のモデルから「通信にかかわる 2 者」「通信サービスを提供するサービス事業者」「それ以外」という 4 者のモデルに移行をしてきていることを示している．一方で，Bai らの研究 [6] では 3 者モデルから 4 者モデルへの移行についての考察やモデルの違いについてのエンドユーザの認識は調査されておらず，「通信サービスを提供するサービス事業者」を信頼するモデルがどういったリスクを持つかについては，まだエンドユーザの認識をより明らかに調査していく必要がある．社会的影響の大きいインシデントの発生によりエンドユーザ認識がさらに大きく変化することも十分考えられるため，引き続いてエンドユーザの認識を調査することも重要になると思われる．セキュリティとプライバシのユーザビリティ研究をリードする国際会議である SOUPS でも，これまでに行われた研究を母集団や時期を変えてあらためて調査することでその違いを議論する Replication の研究が勧められていることから，継続的な研究が進んでいくものと考えられる．

7.2 暗号技術全般とユーザビリティ

暗号化は暗号技術の 1 つであり，そのほかにもさまざまなプロトコルや技術が存在する．暗号技術全般とユーザビリティについても暗号化と同様に深めていかなければならない重要な課題であり，そもそもの Whitten と Tygar の論文でも，電子署名に関する議論もされていた．

暗号技術のユーザビリティの解決は基礎研究，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ふ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．暗号技術で最も普及をしていると考えられる Web サーバ証明書では証明書の扱いはまだ完全には至らず，近年急速に広まっている Bitcoin に代表される暗号通貨（Crypto Currency，あるいは仮想通貨とも呼ばれる）でも鍵管理に起因すると思われる問題が複数発生しており，金銭的な損害という実害につながっているなど，暗号とユーザビリティの問題はますます現実的な問題として対処されなければならないものとなってきた．

なによりそれが，Whitten らがその論文で Introduction の最初に語っている以下の文章について，解決したとい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.*

これらを解決する動きとして，開発者向けの暗号化とユーザビリティの研究が進展しつつある状況は，ますます加速するものと考えられる．暗号技術のソフトウェアライブラリや API の高いユーザビリティや，開発環境における暗号技術適用の支援技術など，開発者向けの研究がさらに細分化され進んでいくことが予想される．

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と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．

サービス事業者からもメッセージを秘匿しなければならないという目的から，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んできた．その点は EFF の Secure Messaging Scorecard における評価項目の 1 つとなっている．

一方で，エンド間で暗号化をする場合には，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暗号化がされてしまうために受けられなくなる，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．検索機能やソーティング機能，フィルタリング機能など，E2E 暗号の適用アプリケーションによってさまざまな機能がかかわってくると考えられる．

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，電子メールのアプリケーションや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クスもエンド側環境で保持することは考えにくい．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クスが存在し，そしてそのインデクスからは情報が漏れない，ということが求められる．

Web での HTTPS 化などでは，エンド側以外では通信内容を確認できないことがリスク増大につながる可能性もある．現在のインターネット接続環境では，クライアント端末がインターネットに接続する際にプロキシサーバを介して接続をさせるケースが企業を中心に一般的に行われている．プロキシサーバはローカルなネットワークからのアクセスを代替する役割をするとともに，現在では危険な Web サイトへのアクセスの遮断や危険なアプリケーションのダウンロードを防ぐセキュリティの役割も担っている．HTTPS によりエンド間で暗号化がなされると，通常のプロキシサーバではこれらの機能が利用不可能となり，エンド側でのより高いセキュリティが求められることになる．

暗号技術としてこれらを実現する方式は提案されている，インデクスの暗号化によりインデクス自身からの情報漏えいや検索時の情報漏えいを防ぐ検索可能暗号や，秘密分散技術などを応用して情報を秘匿したまま計算を行える秘密計算（マルチパーティ計算）技術，文字列マッチングや統計処理といった特定計算を行う秘匿計算技術など広く研究開発が進んでいる．しかし，このユーザビリティについては現時点ではまったくといっていいほど考慮されていない．

今後は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，それを実現することができる技術要素である高機能な暗号技術自身のユーザビリティの研究も進んでいくであろう．

8. まとめ

本論文では，暗号化とユーザビリティに関する研究に焦点を当て，研究の現状を調査と整理を行い，その結果得られた知見から考察を行った．

暗号化とユーザビリティに関する研究は 1999 年に Whitten と Tygar らにより拓かれた後，多くの研究がされてきた．この論文が発表されてから 20 年近くが経とうとしている今，時代背景の変化もあり暗号化のユーザビリティはさらに重要な課題となっている．一方で，暗号が適切に扱われていないケースは多く存在しており，E2E 暗号化の用途が進むにつれて適切に扱われる難しさも増すことが十分に考えられる．著者らは，いまここであらためて暗号化とユーザビリティの問題点と現状を整理し，その解決に向けたアプローチを再考する必要があると考えた．

多くの研究を調査した結果，当初はエンドユーザ向けの暗号化に対してユーザビリティの調査や向上の研究が行われ，その後さらに対象が詳細化されユーザ属性を絞った研究がさかんになってきたことが分かった．近年では特に開発者向けの暗号化とユーザビリティについての研究が注目されていた．それをふまえ，本論文ではこれまでの研究をエンドユーザ向けの暗号化とユーザビリティと，開発者向けの暗号化とユーザビリティに大別してそれぞれの研究分野やアプローチの特徴を示した．また両者に共通する点として鍵管理の問題を取り上げ，それを別の章として示した．

さらに今後の予測として暗号化とユーザビリティ研究の継続性や開発者向けの研究の拡大，メッセージなどの暗号化により利用不可能になる可能性のあるユーティリティ機能についての考察を行い，今後の進む方向性を考察した．

E2E 暗号化の急激な広まりは暗号技術を適切に利用させる機会であると同時に不適切なまま広まりリスクが逆に高まる脅威でもある．暗号化に関するユーザビリティは暗号技術利用を適切にさせる強力な要素になることができ，今後さらに重要になる研究分野になってくるであろう．

参考文献

[1] Acar, Y., Fahl, S. and Mazurek, M.: You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users, *2016 IEEE Cybersecurity Development* (*SecDev*) (2016).

[2] Acar, Y., Backes, M., Fahl, S., Kim, D., Mazurek, M.L. and Stransky, C.: You Get Where You're Looking For: The Impact Of Information Sources On Code Security, *37th IEEE Symposium on Security and Privacy* (*S&P '16*), IEEE (2016).

[3] Acar, Y., Backes, M., Fahl, S., Garfinkel, S., Kim, D., Mazurek, M. and Stransky, C.: Comparing the Usability of Cryptographic APIs, *38th IEEE Symposium on Security and Privacy* (*S&P '17*) (2017).

[4] Atwater, E., Bocovich, C., Hengartner, U., Lank, E. and Goldberg, I.: Leading Johnny to Water: Designing for Usability and Trust, *Symposium on Usable Privacy and Security* (*SOUPS*) (2015).

[5] Atzeni, A., Cameroni, C., Faily, S., Lyle, J. and Flechais, I.: Here's Johnny: A Methodology for Developing Attacker Personas, *The 6th International Conference on Availability, Reliability and Security* (*ARES*) (2011).

[6] Bai, W., Kim, D., Namara, M., Qian, Y., Kelley, P.G. and Mazurek, M.L.: An Inconvenient Trust: User Attitudes Toward Security and Usability Tradeoffs for Key-Directory Encryption Systems, *Symposium on Usable Privacy and Security* (*SOUPS*) (2016).

[7] Beneson, Z., Lenzini, G., Oliveira, D., Parkin, S. and Uebelacker, S.: Maybe Poor Johnny Really Cannot Encrypt – The Case for a Complexity Theory for Usable Security, *New Security Paradigms Workshop* (*NSPW*) (2015).

[8] Bicakci, K., Atalay, N.B. and Kiziloz, H.E.: Johnny in Internet Cafe: User Study and Exploration of Password Autocomplete in Web Browsers, *7th ACM Workshop on Digital Identity Management* (*DIM '11*) (2011).

[9] Bobba, R., Muggli, J., Pant, M., Basney, J. and Khurana, H.: Usable Secure Mailing Lists with Untrusted Servers, *8th Symposium on Identity and Trust on the Internet* (*IDtrust '09*) (2009).

[10] Cagalj, M., Capkun, S. and Hubaux, J.-P.: Key Agreement in Peer-to-Peer Wireless Networks, *Proc. IEEE*, Vol.94, No.2, pp.467–478 (2006).

[11] Chen, C.-H., Chen, C.-W., Kuo, C., Lai, Y.-H., McCune, J.M., Studer, A., Perring, A., Yang, B.-Y. and Wu, T.-C.: GAnGS: Gather, Authenticate'n Groups Securely, *14th Mobile Computing and Network* (*MobiCom '08*) (2008).

[12] Cheswick, W.: Johnny Can Obfuscate: Beyond Mother's Maiden Name, *USENIX Workshop on Hot Topics in Security* (*HotSec*) (2006).
[13] Clark, J. and van Oorschot P.C.: SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements, *34th IEEE Symposium on Security and Privacy* (2013).
[14] Clark, S., Goodspeed, T., Metzger, P., Wasserman, Z., Xu, K. and Blaze, M.: 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).
[15] Cohn-Gordon, K., Cremers, C.J.F., Dowling, B., Garratt, L. and Stebila, D.: A formal security analysis of the signal messaging protocol, *2017 IEEE European Symposium on Security and Privacy* (*EuroS&P 2017*), pp.451–466, IEEE (2017).
[16] Cohn-Gordon, K., Cremers, C.J.F. and Garratt, L.: On post-compromise security, *IEEE 29th Computer Security Foundations Symposium* (*CSF 2016*), pp.164–178, IEEE Computer Society (2016).
[17] Cohn-Gordon, K., Cremers, C., Garratt, L., Millican, J. and Milner, K.: On Ends-to-Ends Encryption: Asynchronous Group Messaging with Strong Security Guarantees, Cryptology ePrint Archive, Report 2017/666 (2017), available from ⟨http://eprint.iacr.org/2017/666⟩.
[18] Conway, D., Taib, R., Harris, M., Yu, K., Berkovsky, S. and Chen, F.: A Qualitative Investigation of Bank Employee Experiences of Information Security and Phishing, *13th Symposium on Usable Privacy and Security* (*SOUPS 2017*) (2017).
[19] Dormann, W.: Finding Android SSL Vulnerabilities with CERT Tapioca, CERT/CC Blog (2014).
[20] Dosono, B., Hayes, J. and Wang, Y.: "I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication, *11th Symposium on Usable Privacy and Security* (*SOUPS 2015*) (2015).
[21] Egele, M., Brumley, D., Fratantonio, Y. and Kruegel, C.: An Empirical Study of Cryptographic Misuse in Andoroid Applications, *20th ACM Conference on Computer and Communications Security* (2013).
[22] Electoronic Frontier Foundation: Secure Messaging Scorecard, available from ⟨https://www.eff.org/secure-messaging-scorecard⟩.
[23] Elison, C. and Dohrmann, S.: Publick-key support for group collaboration, *ACM Trans. Information and System Security* (*TISSEC*) (2003).
[24] Electronic Frontier Foundation: Secure Messaging Scorecard (2014), available from ⟨https://www.eff.org/node/82654⟩ (accessed 2018-02-27).
[25] Eskandari, S., Barrera, D., Stobert, E. and Clark, J.: A First Look at the Usability of Bitcoin Key Management, *The Network and Distributed System Security Symposium* (*NDSS*) (2015).
[26] Fahl, S., Harbach, M., Muders, T., Smith, M. and Sander, U.: Helping Johnny 2.0 to Encrypt His Facebook Conversations, *Symposium on Usable Privacy and Security* (*SOUP*) (2012).
[27] Fahl, S., Harbach, M., Muders, T., Smith, M., Baumgarther, L. and Freisleben, B.: Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security, *22nd ACM Conference on Computer and Communications Security* (*CSS*) (2012).
[28] Fahl, S., Harbach, M., Muders, T. and Smith, M.,: Confidentiality as a Service–Usable Security for the Cloud, *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* (*TrustCom*) (2012).
[29] Felt, A.P., Barnes, R., King, A., Palmer, C., Bentzel, C. and Tabriz, P.: Measuring HTTPS Adoption on the Web, *26th USENIX Security Symposium* (2017).
[30] Felt, A.P., Ainslie, A., Reeder, R.W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H. and Grimes, J.: Improving SSL Warnings: Comprehension and Adherence, *Proc. Conference on Human Factors and Computing Systems* (*CHI 2015*) (2015).
[31] Felt, A.P., Reeder, R.W., Ainslie, A., Harris, H., Walker, M., Thompson, C., Acer, M.E., Morant, E. and Consolvo, S.: Rethinking Connection Security Indicators, *12th Symposium on Usable Privacy and Security* (*SOUPS 2016*) (2016).
[32] Fischer, F., Böttinger, K., Xiao, H., Stransky, C., Acar, Y., Backes, M. and Fahl, S.: Stack Overflow Considered Harmful? The Impact of Copy & Paste on Android Application Security, *38th IEEE Symposium on Security and Privacy* (*S&P '17*) (2017).
[33] Garfinkel, S.L. and Miller, R.C.: Johnnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express, *Symposium on Usable Privacy and Security* (*SOUPS*) (2005).
[34] Garfinkel, S.L., Schiller, J.I., Nordlander, E., Margrave, D. and Miller, R.C.: Views, Reactions and Impact of Digitally-Signed Mail in e-Commerce, *Financial Cryptography and Data Security* (*FC '05*) (2005).
[35] Garfinkel, S.L.: Enabling Email Confidentiality through the use of Opportunistic Encryption, *The Annual National Conference on Digital Government Research* (*DG.O '03*) (2003).
[36] Garfinkel, S.L., Margrave, D., Schiller, J.I., Nordlander, E. and Miller, R.C.: How to Make Secure Email Easier To Use, *SIGCHI Conference on Human Factors in Computing* (*CHI '05*) (2005).
[37] Garfinkel, S.L. and Miller, R.C.: The Johnny 2 Standardized Secure Messaging Scenario, *Symposium on Usable Privacy and Security* (*SOUPS*) (2005).
[38] Garman, C., Green, M., Kaptchuk, G., Miers, I. and Rushanan, M.: Dancing on the lip of the volcano: Chosen ciphertext attacks on Apple imessage, *25th USENIX Security Symposium* (*USENIX Security '16*), pp.655–672, USENIX Association (2016).
[39] Gaw, S., Felten, E.W. and Fernandez-Kelly, P.: Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-Mail, *SIGCHI Conference on Human Factors in Computing* (*CHI '06*) (2006).
[40] Google：より安全なメール透明性レポート Google (2016), 入手先 ⟨https://www.google.com/transparencyreport/saferemail/⟩.
[41] Heninger, N., Durumeric, Z., Wustrow, E. and Halderman, J.A.: Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices, *Proc. 21st USENIX Security Symposium* (2012).
[42] Herzberg, A.: Why Johnny can't surf (safely)? Attacks and defenses for web users, *Journal of Computers & Security* (2009).
[43] Herzberg, A. and Margulies, R.: Training Johnny to Authenticate (Safely), *33th IEEE Security & Privacy* (2012).
[44] Herzberg, A. and Margulies, R.: 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).
[45] Imai, H. and Kanaoka, A.: Time Series Analysis of Copy&Paste Impact on Android Application Security, *13th Asia Joint Conference on Information Security* (*AsiaJCIS 2018*) (2018).
[46] Isobe, T. and Minematsu, K.: Breaking Message Integrity of an End-to-End Encryption Scheme of LINE, *23th European Symposium on Research in Computer Security* (*ESORICS 2018*) (2018).
[47] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F. and Hong, J.: Teaching Johnny Not to Fall for Phish, *ACM Trans. Internet Technology* (*TOIT*) (2010).
[48] Lastdrager, E., Gallardo, I.C., Hartel, P. and Junger, M.: How Effective is Anti-Phishing Training for Children?, *13th Symposium on Usable Privacy and Security* (*SOUPS 2017*) (2017).
[49] Leon, P.G., Ur, B., Balebako, R., Cranor, L.F., Shay, R. and Wang, Y.: Why Johnny Can't opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising, *SIGCHI Conference on Human Factor in Computing Systems* (*CHI '12*) (2012).
[50] Lidzborski, N. and Pevarnek, J.: More Encryption, More Notifications, More Email Security, Google Security Blog (2016), available from ⟨https://security.googleblog.com/2016/03/more-encryption-more-notifications-more.html⟩.
[51] Lin, Y.-H., Studer, A., Hsiao, H.-C., McCune, J.M., Wang, K.-H., Krohn, M., Lin, P.-L., Perring, A., Sun, H.-M. and Yang, B.-Y.: SPATE: Small-group PKI-less Authenticated Trust Establishment, *7th Mobile System, Applications, and Services* (*MobiSys 2009*) (2009).
[52] LINE Corporation: LINE Encryption Overview (2016).
[53] Norcie, G., Blythe, J., Caine, K. and Camp, L.J.: Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems, *2014 Network and Distributed System Security Symposium* (*NDSS*) (2014).
[54] Oprea, A. and Reiter, M.K.: Integrity Checking in Cryptographic File Sytems with Constant Trusted Storage, *16th USENIX Security Symposium* (2007).
[55] Orman, H.: Why Won't Johnny Encrypt?, *IEEE Internet Computing* (2015).
[56] Perlman, R. and Kaufman, C.: User-centric PKI, *7th Symposium on Identity and Trust on the Internet* (*IDtrust '08*) (2008).
[57] Pletka, R. and Cachin, C.: Cryptographic Security for a High-Performance Distributed File System, *24th IEEE Conference on Mass Storage Systems and Technologies* (*MSST*) (2006).
[58] Reaves, B., Scaife, N., Bates, A., Traynor, P. and Butler, K.R.B.: Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World, *24th USENIX Security Symposium* (2015).
[59] Renaud, K., Volkamer, M. and Renkema-Padmos, A.: Why Doesn't Jane Protect Her Privacy?, *Performance Evaluation of Tracking and Surveillance* (*PETS '14*) (2014).
[60] Roth, V., Straub, T. and Richter, K.: Security and Usability Engineering with Particular Attention to Electronic Mail, *International Journal of Human-Computer Studies* (2005).
[61] Rsler, P., Mainka, C. and Schwenk, J.: More is Less: How Group Chats Weaken the Security of Instant Messengers Signal, WhatsApp, and Threema, Cryptology ePrint Archive, Report 2017/713 (2017), available from ⟨http://eprint.iacr.org/2017/713⟩.
[62] Ruoti, S., Kim, N., Burgon, B., van der Horst, T. and Seamons, K.: Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes, *Symposium on Usable Privacy and Security* (*SOUPS*) (2013).
[63] Ruoti, S., Andersen, J., Zappala, D. and Seamons, K.: Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client, arXiv.org (2015), available from ⟨http://arxiv.org/abs/1510.08555⟩.
[64] Ruoti, S., Andersen, J., Hendershot, T., Zappala, D. and Seamons, K.: Helping Johnny Understand and Avoid Mistakes: Comparison of Automatic and Manual Encryption in Email, arXiv.org (2015), available from ⟨http://arxiv.org/abs/1510.08435⟩.
[65] Ruoti, S., Andersen, J., Heidbrink, S., O'Neil, 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, *Special Internet Group on Computer-Human Interaction* (*SIGCHI*) (2016).
[66] Schechter, E.: A secure web is here to stay, Google Security Blog (2018), available from ⟨https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html⟩.
[67] Schrittwieser, S., Fruhwirt, P., Kieseberg, P., Leithner, M., Mulazzani, M., Huber, M. and Weippl, E.: Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications, *The Network and Distributed System Security Symposium* (*NDSS*) (2012).
[68] Sheng, S., Broderick, L. and Koranda, C.A.: Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software, *Symposium on Usable Privacy and Security* (*SOUPS*) (2006).
[69] Shin, D. and Lopes, R.: An Empirical Study of Visual Security Cues to Prevent the SSLstripping Attack, *27th Annual Computer Security Applications Conference* (*ACSAC '11*) (2011).
[70] Stanek, J., Sorniotti, A., Androulaki, E. and Kencl, L.: A Secure Data Deduplication Scheme for Cloud Storage, *Financial Cryptography and Data Security* (*FC 2014*) (2014).
[71] Straub, T. and Baier, H.: A Framework for Evaluating the Usability and the Utility of PKI-enabled Applications, *1st EuroPKI* (2004).
[72] Sundaramurthy, S.C., McHugh, J., Ou, X., Wesch, M., Bardas, A.G. and Rajagopalan, S.R.: Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations, *12th Symposium on Usable Privacy and Security* (*SOUPS 2016*) (2016).
[73] Tong, W., Gold, S., Gichohi, S., Roman, M. and Frankle, J.: Why King George III Can Encrypt (2014), available from ⟨http://randomwalker.info/teaching/spring-2014-privacy-technologies/king-george-iii-encrypt.pdf⟩.
[74] Whitten, A. and Tyger, J.D.: Why Johnny Encrypt: A Usability Evaluation of PGP 5.0, *8th USENIX Security Symposium* (1999).
[75] Wilbur, P.F. and Deshane, T.: Johnny can drag and drop: Determining user intent through traditional interactions to improve desktop security, *4th Symposium on Computer Human Interaction for the Management of Information* (*CHiMiT '10*) (2010).
[76] Wright, C.P., Dave, J. and Zadok, E.: Cryptographic File Systems Performance: What You Don't Know Can Hurt You, *2003 IEEE Security in Storage Workshop*

(*SISW '03*) (2003).

緑川 達也

2016 年東邦大学理学部情報科学科卒業．2018 年同大学大学院修士課程修了．セキュリティとユーザビリティの研究に従事．現在は株式会社アイオスに所属．2017 年情報処理学会山下記念賞受賞

金岡 晃 （正会員）

1998 年東邦大学理学部情報科学科卒業．2000 年同大学大学院修士課程修了．2004 年筑波大学大学院博士課程システム情報工学研究科修了．同年セコム（株）入社．筑波大学大学院システム情報工学研究科研究員，同助教を経て 2013 年東邦大学理学部講師．2017 年同准教授．セキュリティとプライバシのユーザビリティ，暗号技術の応用に関する研究に従事．2014 年情報処理学会山下記念賞受賞．