連載

5分で分かる!? 有名論文ナナメ読み

金岡　晃（東邦大学）

Alma Whitten and J. D. Tygar : Why Johnny Can't Encrypt : A Usability Evaluation of PGP 5.0

The 8th USENIX Security Symposium (1999)

暗号技術の適切な利用とユーザビリティ

今や多くの利用者がインターネットを介して情報の取得やメッセージの送受信を行っている．2010年代後半を迎えた現在，それらの通信が送受信側で暗号化されることが増えてきた．メッセージの送受信者による暗号化はエンドツーエンド暗号化（End-to-End Encryption，以後E2E暗号化）と呼ばれており，身近な例としてはLINEやFacebook Messenger，WhatsApp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）などが代表的なE2E暗号化として挙げられる．

2010年代前半よりインターネットにおける通信にE2E暗号化が重要であることが注目され，2014年には電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を公開し，E2E暗号化に向けた促進運動が始まった．2016年になり先述したメッセージングツールにE2E暗号化対応が行われ，Let's Encryptプロジェクトにより無償のTLSサーバ証明書が正式に配布されるようになるなど，E2E暗号化は大きな広まりを見せている．

暗号化の広まりにより利用者の環境はより安全になるが，そこには1つ重要な仮定が必要となる．それが「暗号が適切に利用されていること」である．暗号の技術としては十分に安全なものであるが，その利用が適切でない場合，守られるべき情報などは期待される安全性を満たさなくなる．だからこそ実際にツールを利用する一般利用者だけでなく，ツールを開発・運用する開発者も適切に暗号技術を利用する必要がある．たとえばTLSサーバ証明書を利用するツールでは，その証明書が信頼できるものかどうかを利用時に毎回検証する必要がある．ツールの実装でその検証部分に適切な検証を行わず，常に「検証O.K.」としてしまう場合，故意・事故を問わず不適切な証明書を利用しているサーバへのアクセスが遮断されず，安全とはいえない通信が行われてしまう．別の例としては，暗号化通信ツールに使う公開鍵暗号の鍵ペアに初期設定で固定の鍵が使われており，その鍵を更新することなく利用可能になってしまっている場合，多くの一般利用者がその危険性に気づかずに利用を続けてしまうこともある．いずれの例も開発者側が適切な利用を施していれば一般利用者にリスクを生じさせずに済むものであった．

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利用の難しさがあり，求められている時代背景と提供されている実際の技術の間に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技術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がたい．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」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．この論文以前でも電子メール暗号化の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集まり，その後この論文を参照してさまざまな研究が生まれた．

この論文では，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．さらに，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．

ジョニーはなぜ暗号化できない？

この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．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くか，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，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，ほか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．

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ていた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，暗号初心者がPGP5.0を用いて有効な電子メールセキュリティを実現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）実施する方法が理解可能である
- 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．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．

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だった．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．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た．この論文はこの20年間のセキュリティとプライバシの研究分野の発展を語るにあたって欠かせない論文であることは間違いない．

（2018年4月23日受付）

金岡　晃（正会員）akira.kanaoka@is.sci.toho-u.ac.jp

2004年筑波大学大学院修了．博士（工学）．セコム（株），筑波大学を経て2013年より東邦大学．セキュリティとプライバシのユーザビリティを中心に，暗号技術の応用やモバイルセキュリティ，ネットワークセキュリティの研究に従事．