Vol.2013-SPT-7 No.5
2013/11/11

"Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes" の紹介

宮嵜仁志[†1]　白石善明[†2]　岩田彰[†1]

Report of "Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes"

HITOSHI MIYAZAKI[†1]　YOSHIAKI SHIRAISHI[†2]　AKIRA IWATA[†1]

安全な電子メールの実現方法は存在するが，広く受け入れられるには至っていない．文献[1][2]ではこの一因としてユーザビリティの問題が指摘されており，とりわけ鍵の管理と携帯性に関しての問題があるとされている．ユーザは Web メールには高いユーザビリティと携帯性を期待するため，これらは安全な Web メールシステムを構築する上で重要な問題となっている．Routi らは，ユーザは慣れ親しんだユーザビリティと利便性を維持されることを期待するため，既存の Web メールシステムと密に統合されている場合に，安全な Web メールシステムが受け入れられると考えている．安全であってもユーザの負担になれば，ユーザは安全な Web メールシステムを受け入れず，第一目的である電子メールの送受信を容易にできるようなシステムを選択する．

紹介論文[3]で Routi らは Gmail，Hotmail，Yahoo! Mail などの既存の Web メールシステムを，端末間での暗号化機能を持ち，メッセージの完全性を満たすよう拡張した Pwm(Private Webmail)を作成し，Pwm についてのユーザビリティの調査結果を報告している．Pwm のセキュリティはユーザにほとんど意識させず透過的であり，鍵管理の細部や暗号文はユーザから見えないよう秘匿されている．Pwm はユーザに受け入れられやすいよう新しいシステムを利用する際の操作を習得する負担を減らすため，セキュリティオーバーレイを用いて元の Web メールのインターフェースと密に統合している．

紹介論文[3]における 1 つ目の調査は，Pwm の既存の Web メールシステムとの密な統合と透過的な暗号化機能がユーザビリティにどのような影響を与えるかについてである．Routi らがユーザ実験を行ったところ，ほぼ全ての参加者は，事前の操作の習得や説明なしに，自分宛の暗号化されたメッセージを復号することができた．

しかしながら，このユーザ実験は 2 つの興味深い事実を明らかにした．1 つ目は，鍵の管理や暗号化などのセキュリティについての詳細な機能が透過的であり，どのように動いているのかがわからないため，システムを信用出来ないユーザもいるということである．2 つめは少数ながらセンシティブなメッセージをやりとりする際に，暗号化せずにメッセージを送ってしまうユーザもいたことである．メッセージを送る際のユーザの操作手順が暗号化データと送る場合と非暗号化データを送る場合とで非常に似ているため，ユーザはセンシティブなメッセージを Pwm のセキュリティ機能を有効にしないで送ってしまいやすくなっている[4].

これらの事実を受けて，Routi らはセキュリティの詳細をユーザに秘匿することについて再考した．紹介論文[3]における 2 つめの調査は，ブラウザとは別のアプリケーションで手動で暗号化することで，センシティブなメッセージをする際に暗号化せずに送ってしまう失敗を防ぐことができるかについてである．また Pwm とユーザビリティの観点から比較し，ユーザにセキュリティの詳細を見せることで，ユーザのシステムに対する大きな信用が得られることも期待できるとしていた．これらを確かめるため，Routi らはブラウザと別のアプリケーションでの手動の暗号化の機能を含む試作品として Message Protector(MP)を作成した．

Routi らは MP を使ってさらに 2 つのユーザ実験を行った．その結果，驚くべきことにユーザは手動で暗号化しなければならない MP に Pwm と同程度のユーザビリティがあると評価した．また，ユーザは Pwm より MP を信用し，センシティブなメッセージを暗号化せずに送ってしまう失敗を避けることができた．しかしながら，ユーザはセキュリティシステムがブラウザに密に統合されている Pwm をより好んだ．このように，安全とユーザビリティのバランスを取るなかで，暗号化に関する機能の一部分をユーザに見せ，かつ既存のシステムと密な統合をすることで，ユーザが信用し，ユーザが失敗せずに安全にデータを取り扱う助けになるシステムを実現できると Routi らは主張している．

参考文献

1) Whitten, A., Tygar, J.D.: Why Jonny can't encrypt: A usability evaluation of PGP 5.0, In 8th USENIX Security Symposium (1999).
2) Sheng, S., Broderick, L.,Koranda, C.A, and Hyland, J.J.: Why johnnystill can't encrypt: evaluating the usability of email encryption software, In 2006 Symposium On Usable Privacy and Security – Poster Session (2006).
3) Ruoti, S., Kim, N., Burgon, B., Horst, V.D.T, and Seamons, K.: Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes, In 2013 Symposium On Usable Privacy and Security (2013).
4) Cialdini, B.R.: Influence : Science and practice, Vol.4, Allyn and Bacon Boston (2001).

†1 名古屋工業大学
Nagoya Institute of Technology
†2 神戸大学
Kobe University