様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　６ 月 １３ 日現在

機関番号：３２６７８
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１９４

研究課題名（和文）SNS利用におけるアプリケーション連携の認証誤用防止手法

研究課題名（英文）Authentication misuse prevention method on application cooperation in SNS use

研究代表者
関　良明（Seki, Yoshiaki）

東京都市大学・メディア情報学部・教授

研究者番号：７０７３５６４６

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：スマートフォンの急速な普及とソーシャル・ネットワーク・サービス（SNS）の世界的な拡大に伴い，インターネット技術を活用した簡便なツールが，情報リテラシーの乏しい利用者層へも浸透し始めている．本研究では，アプリケーション利用者の視点からユーザ認証に取り組んだ．具体的な事例として，友人関係が大学生のパスワード共有意識に与える影響を調査・分析し，モデルを構築した．また，ウェアラブルデバイスを用いたユーザ認証の手法を提案した．

研究成果の学術的意義や社会的意義
SNSは年代を問わず広い世代に普及し始めている．SNSの利用に際して，毎回のログイン操作を省略してアプリケーションを自動的に連携する認証機能は，利用者がその仕組みを十分に理解していないと，個人情報やプライバシーに関する情報を第三者に漏えいする危険性がある．これに対し，本研究では，認証機能のリスクアセスメント，誤用検知技術，安全対策技術を新たに研究開発することを目指して取り組んだ．研究成果は，査読有英語論文1件，査読有日本語論文１件と学会発表10件として発表した．

研究成果の概要（英文）：The rapid spread of smartphones and social network services (SNS) are expanding worldwide. Simple tools using Internet technology are beginning to penetrate even users with poor information literacy. In this research, we worked on user authentication from the viewpoint of application users. We investigated and analyzed the influence of friendship on the university students' consciousness of sharing passwords. Furthermore, we proposed user authentication using a wearable device.

研究分野：情報セキュリティ

キーワード：情報セキュリティ　アプリケーション連携　個人認証　ログイン認証

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

スマートフォンの急速な普及とソーシャル・ネットワーク・サービス（SNS）の世界的な拡大に伴い，インターネット技術を活用した簡便なツールが，情報リテラシーの乏しい利用者層へも浸透し始めている．特に，毎回のログイン操作を省略してアプリケーションを自動的に連携する認証機能は，利用者がその仕組みを十分に理解していないと，個人情報やプライバシーに関する情報を第三者に漏えいする危険性がある．

２．研究の目的

本研究では，認証機能のリスクアセスメント，誤用検知技術，安全対策技術を新たに研究開発することを目的として着手した．

３．研究の方法

(1) SSL/TLS，Cookie，OAuth 認証を誤用することで発生する，アプリケーション利用者，サービス提供者，第三者の被害（盗聴，不正アクセス）を，ユースケースの抽出によって顕在化させる．

(2) アプリケーション利用者の視点からユーザ認証の研究に取り組み，友人関係が大学生のパスワード共有意識に与える影響の調査・分析を実施し，ウェアラブルデバイスを用いたユーザ認証を提案する．

４．研究成果

(1) OAuth 認証を利用する SNS における認可のリスク[〔学会発表〕⑩]

① あらまし

毎回のログインを省略してアプリケーションを自動的に SNS と連携する認証機能は，利用者がその仕組みを十分に理解していないと，個人情報やプライバシーに関する情報を第三者に漏えいする危険性がある．このような認証技術の 1 つである OAuth 認証の認可に注目し，OAuth 認証における認証と認可の仕組みを整理し，アプリケーションが SNS と連携する際に，ユーザが不用意に認可してしまうことによるリスクを抽出した．リスクに対するサービス提供者およびユーザの現状の対策を述べ，リスクが起きる状況を認可の観点から考察した．

② 研究の背景と目的

SNS 提供者はユーザ獲得のために，SNS の機能を拡充するアプリケーションの開発を支援している．具体的には，SNS の機能の一部を利用できる権限を用意し，それを利用してアプリケーション開発者が SNS の機能を拡充するアプリケーションを開発している．アプリケーションには，企業などが提供する公式なアプリケーションと，個人が開発・提供する非公式のアプリケーションが存在する．

OAuth 認証以前の開発では，SNS の機能の一部をアプリケーションが取得する際，ユーザの ID とパスワードをアプリケーションが受け取って認証と認可を行う Basic 認証を利用していた．しかし，この方法ではアプリケーションがユーザの SNS に不正アクセスする危険性がある．そのため，ID とパスワードをアプリケーションに渡さずに認証と認可を行う OAuth 認証が現在用いられている．

OAuth 認証を使ってスマートフォン上で SNS と連携するアプリケーション(以下，AP と略す)は多数存在する．AP が取得できる権限は，Twitter で 3 種類，Facebook で 40 種類以上ある．この中から AP は，取得したい権限をユーザの同意を確認した上で取得することができる．ユーザがこれらの権限を悪意のある AP に対して不用意に認可するとリスクが発生することになる．

③ OAuth 認証の安全な運用への提言

認可における方式と粒度の現状を踏まえ，ユーザが悪意のある AP と連携してしまう問題の低減には，SNS 提供者の役割が重要となる．SNS 提供者が AP の事前審査を厳しくし，SNS 提供者の責任で悪意のある AP を排除し，そうでない AP を市場に出すべきである．悪意のある AP を排除できれば，悪意のある AP と連携するリスクを SNS 提供者がユーザに転嫁することもなくなる．API 仕様で AP 開発者が AP を開発しやすくするために権限をひとまとめにして，AP に余分な権限を与え，AP 開発者に悪用を助長させたとしても，AP の審査を厳しくすることで，悪意のある AP を事前に排除できる．審査を厳しくするにあたり，研究が進められているツールの利用なども有効と考える．例えば，アプリケーションプロトコルの apk ファイルから機能を，smali ファイルから動作やパーミッションを解析し，危険性を割り出し，種類ごとに区別する仕組みの提案などがある．

④ むすび

AP との連携で使用される OAuth 認証の認可に注目し，ユーザが悪意のある AP と連携する原因である認可の状況と解決案を考察した．OAuth2.0 でユーザが不用意に認可すると問題が発生すると考え，悪用例を挙げた．それに対して，現在 SNS 提供者，ユーザそれぞれ対策が行われていた．しかし悪意のある AP と連携するユーザも存在している．その原因の 1 つである認可の状況を挙げ，これらの状況を軽減する提言を試みた．

(2) 友人関係が情報セキュリティ行動に与える影響[〔雑誌論文〕②]

① あらまし

情報システムのユーザ認証に用いるパスワード等を学生間で共有する事例が散見される．大学生には ISMS による内部統制が効きにくいことが原因と考えられる．そこで，質問紙調査により，友人関係が情報セキュリティ行動に与える影響を調査した．

② 研究の背景と目的

企業や大学の情報システムは，パスワードに代表されるユーザ認証によって，不正利用者のシステム侵入を防いでいる．パソコンやスマートフォン等を利用するときのユーザ認証だけでなく，ネットワーク上の各種サービスを利用する際もパスワードは多用されている．パスワードは，端末やサービスの入口でシステムの情報セキュリティを守るもっとも重要な仕掛けの一つである．しかし，その管理は大半が個人に委ねられている．そのため，パスワードの設定や取り扱いは，所属組織のセキュリティポリシーなど ISMS（Information Security Management System）で規定されていることが多い．

IPA の意識調査によると，他人の ID とパスワードを使ったインターネットサービス利用の可能性が，20 代のスマートデバイス利用者で 23%以上あり，各年代で最も高い割合を示している．これは悪意をもって入手したパスワードの不正利用であるが，他人に依頼された不正利用も想定される．このような行動は，ユーザ認証の仕組みを脅かす悪質な行為である．

本研究では，大学生を対象に質問紙調査を行い，セキュリティポリシーに反して，他人の ID とパスワードを使う意識を明らかにする．更に，セキュリティの知識や意識の高低にかかわらず，ネット社会に関与している幅広いユーザの情報セキュリティに関する行動である情報セキュリティ行動に着目し，ISMS による内部統制が効きにくい大学生の友人関係が，情報セキュリティ行動モデルに及ぼす影響を考察する．

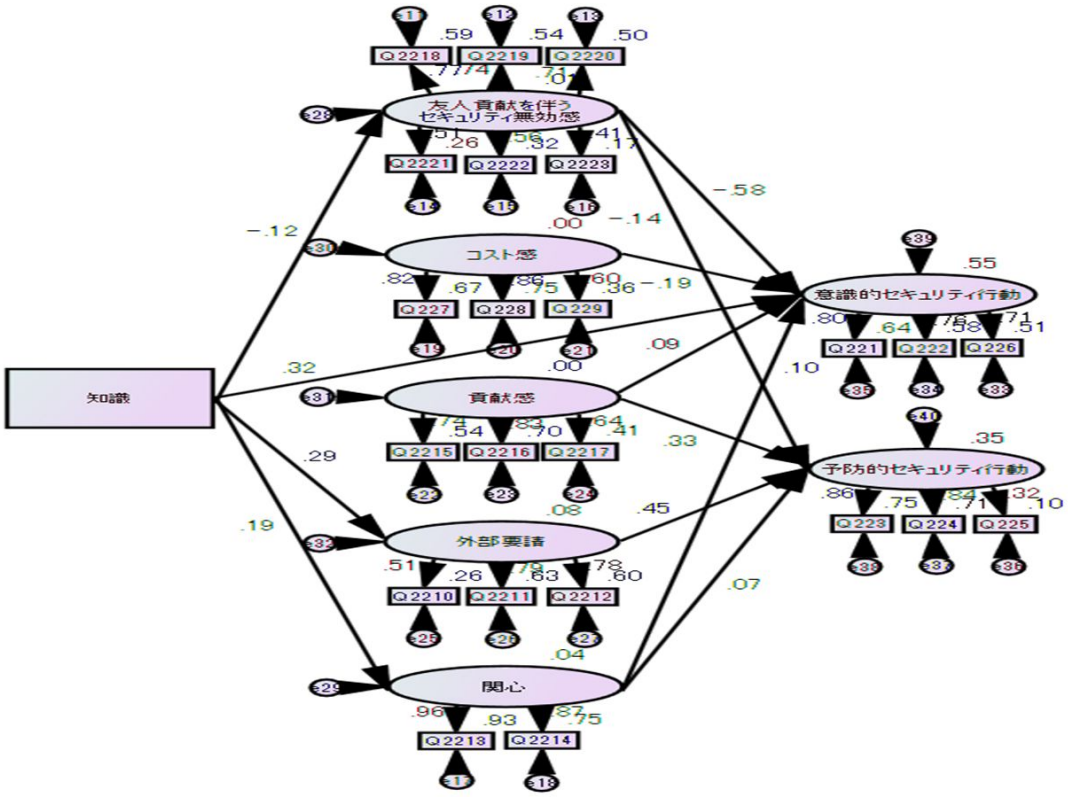

図１　情報セキュリティ行動モデル

③ 調査の新規性・有用性と限界

管理の大半が個人に委ねられているパスワードに着目し，ISMS による内部統制が効きにくい大学を対象に質問紙調査を実施した．他人の ID とパスワードを使う意識を情報セキュリティ行動モデルと友人関係を考慮した分析・考察は新たな試みである．

情報セキュリティ行動モデルは，個人ユーザの一般的な行動をモデル化しているが，友人関係の考慮が十分ではなかった．本調査では，友人関係を考慮した事例を設定して，情報セキュリティ行動モデルを再検証している点（図１参照）の有用性が高い．

パスワードはインターネットサービスでも多用されているため，インターネットを使った質問紙調査との親和性が高く，サンプルの偏りは小さいと考えられる．本調査では，経験と意識を区別した質問により，大学生の本音を明らかにしていると考えられる．しかし，
今回再検証した情報セキュリティ行動モデルは，パスワードを聞こうと思う意識に特化しているため，一般化するためには，更なる検証が必要である．

④ むすび

ISMS による内部統制が効きにくい大学生のパスワード共有に着目して，質問紙調査により，友人関係が情報セキュリティ行動に与える影響を調査した．共分散構造分析により，友人貢献を伴うセキュリティ無効感が意識的セキュリティ行動に負の影響を強く与えることが判明した．また，パスワードを聞こうと思う大学生の予備群の抽出には，パスワードに関する質問と群れ志向に関する質問が有効であることが考察できた．

(3) 腕時計型デバイスを用いたスマートフォンの盗難防止手法[〔雑誌論文〕①]

① あらまし

所有者が居眠りした時のスマートフォンの盗難防止手法を提案する．スマートフォンの所有者は，加速度センサと振動モードを備えた腕時計型デバイスを装着し，所有者が居眠りしたことを検出する．スマートフォンの加速度センサが居眠り中に異常を検知すると，デバイスが振動する機能を実装し，その有用性を確認した．

② 研究の背景と目的

スマートフォンの紛失・盗難による不正利用が重大な問題である．日本のスマートフォン所有者の 23% がスマートフォンの紛失・盗難を経験している．スマートフォンは 常時起動状態で，日常的に携帯され，機密性の高い情報を格納している スマートフォンの不正利用は比較的容易で，生じる被害は極めて大きいと推測される．スマートフォンの不正利用に繋がるリスクの１つに居眠り時の盗難が存在する． スマートフォンを放置して ユーザが居眠りをすると，第三者がスマートフォンを置き引きできるリスクである．

本研究では，進歩と普及が著しいウェアラブルデバイスである腕時計型デバイスに注目し，これを用いたスマートフォンの盗難警報ソフトウェアを提案する．両端末の加速度センサで，ユーザの居眠りとスマートフォンの盗難を検知することによりスマートフォンの盗難を防止する．

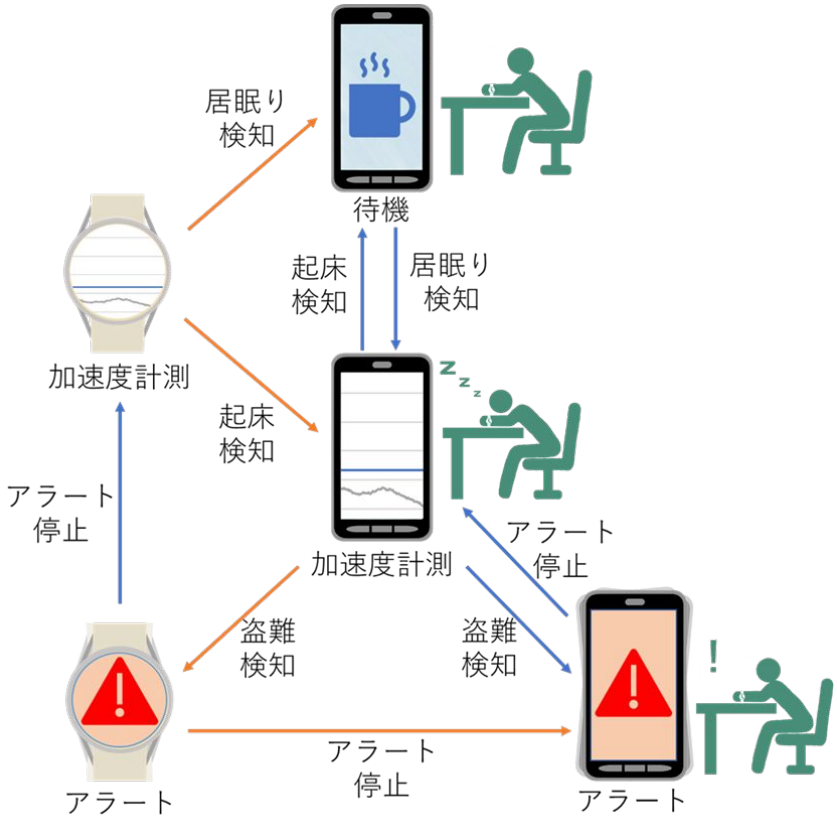

図 2　提案ソフトウェアの概要図

③ 考察

腕時計型デバイスでユーザの居眠りを検知し，スマートフォンで盗難を検知することにより，スマートフォンの盗難を防止できる（図 2 参照）．腕時計型デバイスでユーザの居眠りを検知しない場合，ユーザは覚醒状態と見なし，スマートフォンは問題なく操作できる．ユーザの居眠り検知に居眠り判定フェイズを実装し，誤検知なくユーザの居眠りを検知できる．提案ソフトウェアは他ソフトウェアや他サービスと連携せず動作するため，スマートフォンと腕時計型デバイスの他機能を妨げることなく利用できる．

④ むすび

ユーザの居眠り時におけるスマートフォン盗難防止のため，腕時計型デバイスを用いたスマートフォンの盗難警報ソフトウェアを提案した．腕時計型デバイスの居眠り検知において，居眠り判定フェイズを導入することで，居眠りの誤検知を解消した．加速度計測を用いた検知手

法によってスマートフォンの盗難から警報までの許容時間を短縮した.

５．主な発表論文等

〔雑誌論文〕（計　２件）

① Kouhei Nagata, and Yoshiaki Seki: A Method for Smartphone Theft Prevention when the Owner Dozes off, IEICE Transactions on Information and Systems, DOI:10.1587/transinf.2018OFL0001 (2019.10.04) 査読有

② 熊谷 匠純，菊地 拓翔，澤 信吾，加藤 菜美絵，関 良明：友人関係が情報セキュリティ行動に与える影響 －大学生のパスワード共有調査－，電子情報通信学会論文誌，Vol.J101-D，No.10，pp.1438-1442，DOI:10.14923/transinfj.2017LIL0002 (2018.10.01) 査読有

〔学会発表〕（計　１０件）

① 澤 信吾，菊地 拓翔，関 良明：情報セキュリティリテラシー測定手法の提案，2018 年電子情報通信学会基礎・境界ソサイエティ/NOLTA ソサイエティ大会，2018

② 菊地 拓翔，澤 信吾，関 良明：クレジット決済の阻害要因を明らかにする質問紙設計，2018 年電子情報通信学会基礎・境界ソサイエティ/NOLTA ソサイエティ大会，2018

③ 澤 信吾，菊地 拓翔，熊谷 匠純，関 良明:大学生の情報セキュリティ意識に関する調査分析 －代理出席時のパスワード共有－，2018 年電子情報通信学会総合大会，2018

④ 菊地 拓翔，澤 信吾，熊谷 匠純，関 良明：大学生の友人関係とパスワード/学生証共有に関する調査分析，2018 年電子情報通信学会総合大会，2018

⑤ 熊谷 匠純，菊地 拓翔，澤 信吾，関 良明：大学生のパスワード共有に関する調査分析 －友人関係を考慮した情報セキュリティ行動モデル－，2018 年電子情報通信学会総合大会，2018

⑥ 永田 航平，関 良明：ウェアラブルデバイスを用いたキーガード自動制御，2018 年電子情報通信学会総合大会，2018

⑦ 熊谷 匠純，菊地 拓翔，澤 信吾，加藤 菜美絵，関 良明：大学生におけるパスワード管理の意識調査 ～友人関係を考慮した質問紙設計～，電子情報通信学会技術研究報告，2017

⑧ 松下 海央，永田 航平，関 良明:腕時計型デバイスを用いたユーザ認証維持手法の提案 ～加速度センサの活用～，電子情報通信学会技術研究報告，2017

⑨ 松下 海央，関 良明：腕時計型デバイスの取り外し検出手法の一考察,2017 年電子情報通信学会総合大会，2017

⑩ 吉田 達司，関 良明：OAuth 認証を利用する SNS における認可のリスク,電子情報通信学会技術研究報告，2016

〔図書〕（計　１件）

高橋 修(監修)，関 良明，河辺 義信，西垣 正勝，岡崎 直宣，岡崎 美蘭，本郷 節之，岡田 安功(著)：ネットワークセキュリティ，共立出版 (2017.09.25)

〔産業財産権〕

○出願状況（計　０件）

○取得状況（計　０件）

〔その他〕

ホームページ等

http://www.comm.tcu.ac.jp/seki_lab/achiev_list.html

６．研究組織

(1)研究分担者

なし

(2)研究協力者

なし