神奈川工科大学

セキュリティ研究センター研究報告

第5巻

2017

神奈川工科大学

工学教育研究推進機構

セキュリティ研究センター
研究成果報告の発刊に際して

研究代表者　　情報ネットワーク・コミュニケーション学科　　岡崎 美蘭

企業のクラウドの活用が本格化し，あらゆるモノがネットワークでつながる「IoT 時代」．社会の様々な分野でビジネスの可能性が広がると共に，我々の日常生活と深く関係のある重要インフラを狙った新しいサイバー攻撃の可能性も高まっています．
最近，全世界を襲ったランサムウェアに見られるようにサイバー脅威が企業のビジネスの現場に与える影響は，日々大きくなってきています．そこで，このような新たな脅威とどのように向き合うべきか，そこで生じるリスクをどう管理するかが問われています．

本研究センターの特色は，情報セキュリティの基礎技術となるネットワークセキュリティ技術や個人認証技術，情報漏えい対策技術だけではなく，応用面での著作権保護技術及び電子透かし技術の研究，さらに組織における情報セキュリティマネジメントシステム（ISMS: Information Security Management System）の実施モデル構築手法の研究，危機管理やサイバー犯罪などのセキュリティと社会の研究を，統合的に行うことである．これにより，現代の安全・安心な情報化社会の実現に向けた将来ビジョンを世界に向けて展開することを目指す．

平成 28 年度は，学内重点配分研究として 2 つの研究テーマ「モバイルクラウドサービスを実現するための統合セキュリティ対策システムの開発」，「安全安心な社会を形成する危機管理とシステム監査を考慮した組織内情報セキュリティモデルの高度化」を実施した．そこで，覗き見耐性を持つ認証方式を用いたモバイルクラウドサービスの実現手法に関する研究，情報漏えい対策に向けた新たな認証方式の研究開発，情報ハイディングにおける埋め込み情報量の増加方法の検討，カード認証システムにおけるバイオメトリクス認証手法の検討，生体個人認証の基礎研究などを進め，特許出願及び学会発表など多くの成果を上げることができた．また，組織内の ISMS 構築モデル研究においては，組織内の情報価値の最大化と情報化投資の最小化を図り，一定のシステム監査基準に基づいてシステムを総合的に点検・評価するモデルの構築について検討した．さらに，セキュリティと社会・危機管理の研究においては，社会変動と人々の行動様式の変容に注目した，新たなセキュリティの概念の検討を行った．さらに，使いやすさと安全性を両立する認証方式を検討するためのセキュリティ意識の調査と解析を行った．

今後は，引き続き情報セキュリティ基礎基盤技術をより一層高深度化していくとともに，社会インフラの安心・安全の確保などへの適用を検討する．また，高度情報化社会で必要とされる様々な ICT システムへの実用化と応用システムの研究開発を進めて行く．

研究所メンバー

研究代表者

情報学部　　情報ネットワーク・コミュニケーション学科　　岡崎 美蘭

氏名	所属・職名	研究内容
岡崎　美蘭	情報ネットワーク・コミュニケーション学科・教授	覗き見耐性を持つ認証方式を用いたモバイルクラウドサービスの実現手法に関する研究
納富　一宏	情報工学科・教授	安全安心な社会を形成する危機管理と法制度を考慮した組織内情報セキュリティの高度化に関する研究
鳥井　秀幸	情報ネットワーク・コミュニケーション学科・教授	情報ハイディングに関する研究
岡本　学	情報ネットワーク・コミュニケーション学科・准教授	情報漏洩防止にむけての研究
岡本　剛	情報ネットワーク・コミュニケーション学科・准教授	不正アクセス対策技術に関する研究
松田　三知子	情報工学科・教授	組織内情報セキュリティのシステム監査に関する研究
西村　広光	情報メディア学科・准教授	カード認証システムにおけるバイオメトリクス情報の利用法に関する研究
上平　員丈	情報ネットワーク・コミュニケーション学科・教授	光による肖像権，著作権保護技術に関する研究
井上　哲理	情報ネットワーク・コミュニケーション学科・教授	没入型仮想環境でのヒューマンファクタの研究
須藤　康裕	情報工学科・准教授	組織内情報セキュリティのシステム設計に関する研究
山本　　聡	基礎教養教育センター　・教授	サイバー犯罪の実態と警察の捜査に関する研究
三浦　直子	基礎教養教育センター　・准教授	セキュリティと社会，危機管理に関する研究

セキュリティセンター研究報告
第 5 巻（2017）目次

モバイルクラウドサービスを実現するための
統合セキュリティ対策システムの開発

情報ネットワーク・コミュニケーション学科　　岡崎　美蘭

1.　研究の目的

本研究では，スマートフォンやタブレットなど従来のモバイル PC よりもモビリティ性能が高く，多機能な端末を用いたモバイルクラウドサービスを利用する際の情報流出防止対策を含む総合セキュリティ対策手法について検討する．特に，今まで研究開発してきた第三者による覗き見やカメラなどによる録画攻撃に耐性をもつ認証方式の**安全性**と**ユーザビリティ**の両立を確保できる新たな認証方式の研究開発を目指す．

そこで，利用者環境に応じた**「安全性満足度」**を最大にし，ユーザがどのような環境におかれても破られる可能性の極めて低い**「ネバー・ハック・パスワード」**を実現して，安全・安心なモバイルクラウドサービスを実現するための統合個人認証基盤技術を確立し，実用化に向けた実装・実験を行うことを目的とする．

2.　研究の必要性及び従来の研究

近年，企業内のネットワークなどの基本的なコンピューティングリソースやサービスプロバイダが提供するアプリケーションなどをクラウドサービス事業者が提供・管理するクラウドサービスモデルが注目を浴びている．また，スマートフォンやスマートタブレットなど，従来のモバイル PC よりもモビリティ性能が高く，多機能な端末などの登場により，画面処理や入力方法など，汎用的なコンピュータと同等な操作環境をモバイル端末上で実現することが可能となり，今後はこのような端末を用いたモバイルクラウドサービスが急速に伸びていくことが予想されている．

モバイルクラウドサービスの導入は，設備投資コストの軽減のみならず，データ管理の容易さや必要に応じた柔軟なシステムの構築ができる利便性を持つ．すなわち，スマートフォンやタブレットなどの高機能端末の業務への導入（BYOD：Bring Your Own Device）に伴う，営業活動や業務の効率化はもちろん，大規模な災害や事故発生時の事業継続計画（BCP：Business Continuity Plan）を実現可能になる．

一方，スマートフォンなどの携帯端末からクラウドを利用する際には，情報漏えいの脅威がさらに拡大されることが予想される．例えば，ユーザが PC やスマートタブレットなど多様な端末経由で保存したデータをクラウド上で集約出来ることは，クラウド利用のメリットとなる．しかし，スマートフォンやタブレットは PC に比べると紛失・盗難の危険性が高く，ボットウィルス感染などにより他者（攻撃者）の支配下に置かれると，簡単にクラウドへのアクセス認証が突破され，攻撃者によるクラウドへの不正アクセスやなりすまし

を可能にする端末として悪用される可能性がある．クラウドへの不正アクセスが発生すると，PC など他の端末から保存した画像や機密書類などすべての有価コンテンツ情報が漏えいし，不正コピーされる可能性もある．従って，ユーザの携帯端末からクラウドサービス利用時の情報漏えいを防止のための，安全・安心なアクセス制御技術の開発が必要になる．

現在多くのモバイル端末には，パスワードや PIN（Personal Identification Number）及びパターンなどを利用した画面ロックの解除認証が広く利用されている．しかし，これらの認証方法は，その認証動作を人の目にさらされた環境で使用するときに第三者に覗き見をされ，入力した認証情報が盗まれると，容易に秘匿情報が漏えいしてしまう問題がある．我々は，今までモバイル端末の個人認証における覗き見攻撃対策に対する様々な特許出願と研究を行ってきた．しかし，従来の覗き見耐性を持つユーザ認証方式は，利用者環境に関して十分考慮されておらず，入力方法の複雑化によるユーザビリティの低下や，認証動作の録画解析が可能な環境における安全性の低下などの課題が残されていることが判明した．そこで，本研究では周囲に人がいない安全な環境から，監視カメラが複数あり常に認証動作が録画されてしまう危険度の高い環境まで，様々な環境の変化に応じた認証方式を自律的に選択し利用できるようにした，利用者環境適応型モバイル端末認証のための基盤技術を確立するとともに，その有効性に関しても検証することを目的とする．

3. 期待される効果

従来の指紋認証などのように認証を行うために特別な機器を必要とせず，モバイル端末上での覗き見耐性とユーザビリティが高い個人認証を行う技術を開発することで，スマートフォンやスマートタブレットなどを利用したモバイルクラウドサービスのセキュリティに対する脅威を大きく低減できると考えられる．特に，カメラなどの録画機器などによる認証情報の機械的な解析対策を考慮した強度の高い認証技術を実用化することにより，様々な年代や職種での社会的需要と効果が期待できる．

4. 研究の経過及び結果

4.1 研究の経過

以前から我々は，スマートフォンやスマートタブレットなどの携帯端末の認証動作を他人に見られていても認証情報が漏洩しない覗き見耐性を持つ認証方式を提案するとともに，その有効性を実験とアンケートにより実証してきた．しかし，監視カメラなどの録画機器によって認証動作を複数回録画された場合，それらの記録を解析することで登録したパスワードが特定されてしまう危険性があることも分かった．

そこで，カメラなどの録画機器による録画攻撃対策の一つとして，リズム認証方式を提案するとともに，その有効性を実験とアンケートにより実証した．この認証方式では，ユーザが端末を見ることなく特定のリズムをタップすることにより認証を行う．リズムやタップする指の順番は，ユーザによって異なるため，これらの情報をパスワードとして扱うこ

とができる（図 1）．しかし，時間が経て慣れていくことによって同一のユーザが同一のリズムをタップしても，認証情報となるリズムが変わっていくことが分かった．

また，複数のユーザが同じ歌曲のリズムをタップする場合，タップする指のパターンだけで特定のユーザを絞り込むのは困難であることが分かった．

これに対し，今後は多人数向けの個人認証に対応するため，パスワード認証とリズム認証を組み合わせた認証方式について検討するとともに，ユーザビリティと安全性の向上を目指していくことが必要になることが分かった．

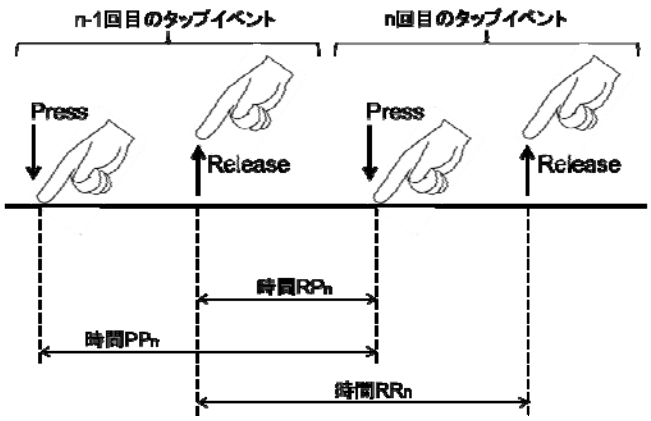


図 1．リズム認証におけるタップ時間

以下では，今年度の本研究の基本となる Random Forest による実用化に向けたリズム認証方式の実験評価について報告する．

4.2 RandomForest によるリズム認証の実験

リズム認証方式とは，連続した入力の時間差を認証情報として用いる認証方法であり，利用者個人の行動的特徴を活かしたバイオメトリクス認証の一つである．リズム認証を用いることにより，利用者は認証画面を見ずに，タッチスクリーンへのタップ入力によって認証を行うことができる．そのため，他人や監視カメラに認証画面を露呈することがなくなり，認証情報の漏洩を防ぐことが期待できる．しかし，現在のリズム認証の認証情報は入力の時間差のみであるため，FRR や FAR が増えやすく，認証精度が十分ではない．

本研究では，自己組織化マップ（Self-Organizing Maps，以下，SOM）を利用したリズム認証方式の認証精度の向上を目的として，タップのイベント時間だけでなく，タップした指の識別および指間の距離も認証情報に追加した認証方法について検討した．しかし，この SOM 作成にサーバが必要となる問題，利用者が少ないタップ数でリズム認証を行った場合は，得られる特徴量が減り，識別率が低下することが考えられる．そこで，今年度はリズム認証方式の実用化に向け，端末内だけで認証が行えるようになるシステムを検討した．また，利用者が少ないタップ数で認証を行った場合でも，識別に重要な特徴量を認証に使用することによって高い個人識別率を実現させることが可能かを実験で確認する．

本論文では，端末内で全ての処理を行えるようにするため，計算処理が高速な RandomForest を利用し，タップ情報で個人を識別する方式を提案する．また，RandomForest の特徴である，特徴量の重要度が計算できることを利用し，特徴量の重要度，MeanDecreaseGini を算出し，使用する特徴量を選択する際の目安とする．

RandomForest の識別性能を確認するため，被験者 24 名の方に，童謡「猫踏んじゃった」の冒頭 4 小節の 19 タップを 20 回入力してもらう．1 人 20 回の試行を行うのは，半分を学習用，残りを識別用のデータとして使用するためである．また，タップするリズムを童謡「猫踏んじゃった」の冒頭 4 小節としたのは，利用者同士が似たようなタップをした場合に，個人を識別可能かを確認するためである．

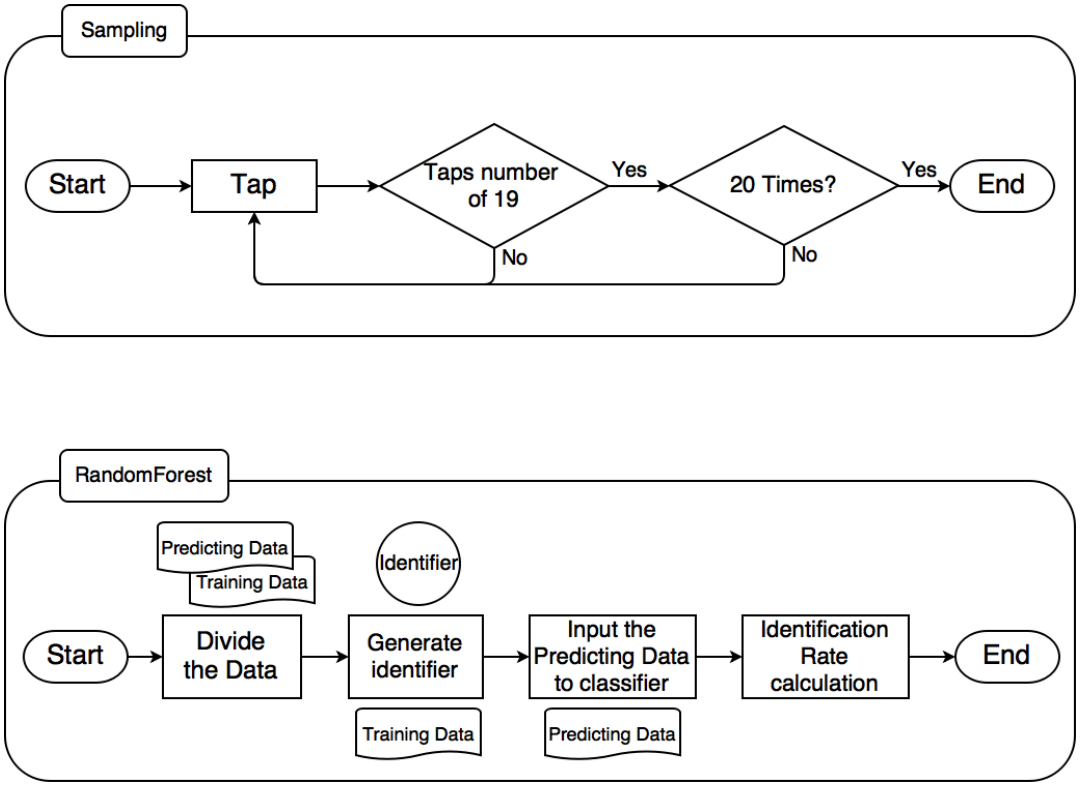


図 2. RandomForest による実験手順

4.2 実験結果

本提案手法の有用性と認証精度を評価するために，評価実験を行った．14 人の被験者にいくつかの条件を提示し，モバイル端末のタッチスクリーン上で童謡「猫踏んじゃった」の冒頭 4 小節をタップしてもらた．実験では，まず各被験者における特徴量の相対的標準偏差を求めた．相対的標準偏差の値が大きいほど，他人との差が大きい特徴となり，FAR を低減できる特徴であると考えられる．また，指 F，距離 D，時間 RR の 3 項目の値が大きいことから，これら 3 項目の特徴量を FAR 低減の特徴量とする．本研究では，認証判定の精度を高めるために，トーラス型 SOM を用いた．トーラス型 SOM は，マップ端の上下左右を結合したマップであり，近傍領域のばらつきがなく，ノード間のユークリッド距離を正確に導き出すことができる．本提案方式の有用性を確認するために，利用する特徴量の項目が異なる SOM ごとに FRR および FAR を計測し，認証精度を求めた．そこで，FAR は閾値が

最小のときでも 0 ではないことから，他人によるリズムの再現性が高いことも確認できた．さらに，指の識別や指間の距離が考慮されていないため，タップするリズムを他人に聞かれた場合，同じリズムでタップすると簡単にユーザ本人になりすますことができると考えられる．

5. 今後の計画

録画攻撃への対策として提案したリズム認証方式は，指の識別や指間の距離も認証情報として扱うことにより，マルチタッチ操作への応用を見込んでいる．この応用により，タップ入力のパターンを増やすことができるため，例えば，端末のスクリーンをタップする音によって他人にリズムを聞かれたとしても，認証情報が全て漏れることがなく，認証方式としての安全性を保つことができる．しかし，マルチタッチ操作によって操作が複雑化し，ユーザの誤操作や誤認証が発生することも考えられる．本提案方式では，認証判定に複数の SOM を利用しているため，SOM の作成時間が従来よりも SOM の枚数分長くなり，ユーザへの負担が大きくなることが課題として挙げられる．そのため，例えば FRR 低減 SOM および FAR 低減 SOM の 2 種類のみを用いたリズム認証方式など，SOM の作成方法や認証方法について改良していく必要がある．

また，覗き見されなくても偶然に認証を突破される確率的誤認証への対策なども考慮して，今後も安全性とユーザビリティを有する認証技術の研究を行っていく予定である．

6. 研究成果の発表

(1) 論文

[1] Y. Kita, K. Aburada, T. Katayama, M. Park, and N. Okazaki "Proposal of an Authentication Method using Two Types of Machine Learning and Mouse Operation Trajectory," The First International Symposium on BioComplexity 2016 (ISAROB, 2016), pp.346-349, 2016/1.

[2] K. Toyoda, M. Park, N. Okazaki, "Unsupervised SPITters Detection Scheme for Unbalanced Callers," The 30th IEEE International Conference on Advanced Information Networking and Applications Workshops (AINA-2016), pp.64-68, 2016.

[3] H. Yamaba, A. Kurogi, S. Kubota, T. Katayama, M. Park, N. Okazaki, "Evaluation of feature values of surface electromyograms for user authentication on mobile devices," Artificial Life and Robotics, 22(1), 108-112, 2017/01.

(2) 学会発表

[1] 堀 孝浩, 喜多 義弘, 朴 美娘, 岡崎 直宣, "Random Forest による実用化に向けたリズム認証の実験評価," 2017 Symposium on Cryptography and Information Security(SCIS2017), 1B2-1, 2017.01.

[2] 堀 孝浩, 朴 美娘, 岡崎 直宣, "Wi-Fi の受信信号強度を用いた近接検出による認証方式に関する一検討," 情報処理学会第 79 回全国大会, 3W-4, 20170317
[3] 堀 孝浩, 喜多 義弘, 豊田 健太郎, 朴 美娘, 岡崎 直宣, "テンポ感を特徴量に取り入れたリズム認証の評価," 情報処理学会第 78 回全国大会, 1W-3, 20160310
[4] 日隈光基, 喜多義弘, 山場久昭, 久保田真一郎, 朴美娘, 岡崎直宣 “パズル型認証方式の録画攻撃耐性の一検討”, IPSJ 火の国シンポジウム 2016, 20160302

(3) 特許

[1] 特願 2015-165962「個人認証装置及びプログラム 」
発明者：岡崎 美蘭
出願者：学校法人 幾徳学園

[2] 特願 2015-183574「個人認証装置及びプログラム 」
発明者：岡崎 美蘭
出願者：学校法人 幾徳学園

(4) 助成金採択

[1] 平成 26 年～平成 28 年度 文部科学省科学研究費補助金 基盤（C）
「覗き見耐性とユーザビリティを有するモバイル端末向けユーザ認証方式」
研究代表者：岡崎 美蘭

カードをかざす動作を用いた個人認証技術の改良

情報メディア学科　　西村広光

１．研究の目的

ユーザ認証技術はさまざまに開発され普及している。そのなかでも、カード認証技術は、クレジットカードや社員証、ホテルのカードキーなど幅広い用途で利用されている。しかし、普及している多くの技術は、4 ケタ暗証番号のように組み合わせ数が少なく十分な堅牢性の実現が難しいものや、指紋認証などのように唯一無二の個人情報である生体情報を登録することの心的負担が大きいとう問題がある。そこで本研究では、カード認証において心的負担の少ないバイオメトリクス情報を利用して認証の堅牢性を高める技術を検討することを目的とした。

28 年度の課題としては、これまでに案し特許出願し性能評価・改良を重ねてきた基盤システムをより幅広い用途で利用できるようにするための技術開発であった。当初計画では複数カメラの画像を利用したカード位置の高精度検出であったが、単体カメラでの位置検出精度をさらに高める技術検討を優先して行った。具体的には、遺伝的アルゴリズムをカード位置検出システムに導入し、高精度化を実現した。

さらに、さらなる高精度な認証技術を確立するため、紫外線画像による金属表面の傷画像分析技術を構築し、コピーして作成した金属鍵をマスターキーと区別できる基盤技術を構築した。

２．研究の必要性及び従来の研究

カード認証に関する従来研究としては、カード情報の読み取り装置に IC や磁気のカードをかざすことで個体認証番号を読み取って認証を行うものが普及している。暗証番号を利用する場合には、認証サーバに登録番号と認証番号との照会を行う必要があり、堅牢なネットワークを利用して行われる必要がある。

高い認証精度を実現している他の研究としては、静脈認証技術がある。静脈認証は、指を透過する近赤外光を照射し、指の静脈のみの画像を取得し、人体固有情報として登録情報と照合することで認証を行う方式である。この他にも指紋認証のように、人体固有の情報を直接的に利用する方法は、複製や偽造することはできないため堅牢な認証を実現することが可能であり、盗難に対し極めて堅牢である。しかし、生体情報を採取することに対して、利用者の心的負担が大きいことが問題といえる。また、静脈認証方式を導入する場合には、専用の大規模な機器を追加導入する必要があり、導入コストが高い。そのため、静脈認証方式が銀行 ATM で採用され

ているものの、対応機器が未だ全 ATM に導入されておらず、普及が進んでいない。

そこで、本研究では、心的負担の少ない意図的なバイオメトリクス情報としては、意図的な行動情報を利用することとした。具体的には、近年普及が進む非接触のカード認証を想定し、密着型でも近接型でも、近傍型でも利用可能な認証性能を向上させる方式として、カードをかざす動作をカメラで取得し認証に利用する方式に絞り検討を進めることとした。提案方式では、近赤外線の照明と安価な Web カメラ程度の機材で、カードをかざす動作を利用して認証を行うため、導入コストも安価に抑えることができる。

これまでに基礎技術を構築してきたが、極近距離でしか認証をおこなうことができない課題を克服するため、通路に設置した監視カメラ程度の撮影距離で認証用カードを高精度に位置検出する技術開発をすすめた。これは本提案技術を一般的なセキュリティーゲートなどで幅広く利用するためには欠くことのできない技術である。1 台のカメラを利用して遠距離からのカード位置の高精度検出技術を本年度確立した。次年度以降はさらに複数カメラに拡張し、本研究成果が適用可能な場面を増やして汎用性を高めていく。

さらに本年度は、金属鍵のような所有物による認証を高精度に行う技術についても検討をすすめた。具体的には、紫外線画像によって鍵の金属表面を撮影することで、金属成型時の微細な傷を画像処理でとらえることができ、それを利用して複製した金属鍵の個体それぞれを識別できる基礎技術を確立した。この技術を先のカード認証と合わせて利用した統合的な高精度認証技術を確立していく計画である。

３．期待される効果

本研究で提案するカードをかざす動作によるカード認証技術は、従来のカード認証システムに追加導入可能な方式といえる。そのため、提案方式を導入することで、既存認証システムの認証精度を高めることができる。

加えて、提案方式で利用する機器は、カメラと照明程度の機材でカードをかざす動作を利用して認証を行うため、既存システムへの追加導入が容易であり、汎用性にすぐれた認証方式であるといえる。

また昨年度基盤機技術を確立した紫外線による金属表面画像を利用した鍵認証技術は、3 次元スキャナと 3 次元プリンタで数年後鍵複製が容易になる時代を見越した新しい鍵認証技術であり、今後極めて高いニーズが生まれる研究といえる。

これまでに、基盤認証方式を確立し、実験を通して理想架橋での性能確認を行ってきた。今後は実際の利用状況を構築し、より実用に即した実験データを整え、評価をすすめながら、本技術の応用についての検討をすすめていく。

以上のことより、本研究の提案方式を拡張して幅広い利用状況に対応させていくことは、カード認証が利用されるあらゆる場面での高精度化につなげることができ

る技術開発であるといえ、その社会的な効果も非常に大きいといえる。

４．研究の経過及び結果

24 年度に新しい認証方式を考案し、TAMA-TLO を通して、2013 年 5 月 30 日付で、「特願 2013-114443」として特許出願に至った。

25 年度は、50 人の被験者を集め、多様な状況下における提案認証法の評価実験用データベースを構築した。構築したデータベースを用いて、カード盗難に対する堅牢性を評価する実験をおこなったところ、高精度に盗難されたカードでもカード利用登録された所有者を認証することができることを実証した。

26 年度は、提案認証方式を実用化させるためで大きな課題になると考えられるカメラとカードの位置制約条件の緩和を試み、従来よりも広角な映像からカード位置を非常に高精度に検出する手法を確立することができた。加えて、照明条件の検討を深め、従来の近赤外線に加え、紫外線情報を利用することでこれまで取得できなかった精度でカード等の物体表面の傷の情報を取得できることを確認し、今後の新しい認証方式の拡張に向けた大きな足がかりを得ることができた。

27 年度は、物体移動を高精度にとらえる技術としてオプティカルフローを高精度に取得する技術を新しく開発し基礎実験を通して有効性を確認した。さらに、紫外線による傷画像認証について、金属鍵の傷画像を利用した認証方式の有効性確認実験を進め、平面的な位置ずれが起きても正しく認証できることを確認した。

28 年度は､遺伝的アルゴリズムを利用したカード位置の高精度検出法を確立し、1 台のカメラでの高精度なカード位置検出を実現した。さらに、紫外線を利用した金属鍵の表面画像による高精度認証の基盤技術を確立し、実験により有効性を確認した。

５．今後の計画

複数監視カメラ画像が利用できる状況を想定し、複数画像を利用した高精度なカード位置検出法を確立する。これにより、広範囲に移動する人物が持つカードを高精度に認証する技術を実現することができ、開発してきたカード認証技術が応用できる状況を拡大する計画である。

加えて、紫外線画像による傷を利用した真贋認証技術を、実際のシリンダ鍵に組み込んだシステムを構築する。これにより、すぐに実用化できる認証方式として国内外に広く発表していく。。

６．研究成果の発表

本研究に関連して、これまでに下記の成果を発表した。

H28 年度

- Nami Tanaka, Hiromitsu Nishimura
  Correction of Optical Flow Calculations Using Color Balance Change
  2016 年　18th International Conference on Human-Computer Interaction
  プロシーディング有り、ポスター発表
- 田中 菜実, 西村 広光
  「高精度オプティカルフローによる位置推定とＧＡを用いた動的なカード型物体の輪郭推定法の一検討」
  2017 年　電子情報通信学会総合大会
- 流 凌太, 宇都宮 彼方, 西村 広光
  「紫外線画像による個体識別に関する一検討」
  2017 年　電子情報通信学会　総合大会　ISS「学生ポスターセッション」
- TBS「未来の起源」で「紫外線を利用した認証技術の開発」（学生：流凌太）の研究が紹介された。

H27 年度

- 田中 菜実, 西村 広光
  「複数の画像情報を利用したオプティカルフロー補正の検討」
  2016 年　電子情報通信学会　総合大会　ISS「学生ポスターセッション」

H26 年度

- Hiromitsu Nishimura
  「Proposal of a User Authentication Method using Near-Infrared Card Images」
  2014 年　16th International Conference on Human-Computer Interaction
  プロシーディング有り、ポスター発表
- 田中 菜実, 吉野 愛李, 島先 康貴, 西村 広光
  「カメラ画像からの高精度なカード位置検出法の検討」
  2015 年　電子情報通信学会　総合大会　ISS「学生ポスターセッション」
- 吉野 愛李, 田中 菜実, 西村 広光
  「紫外線画像からの傷検出による所有者の検討」
  2015 年　電子情報通信学会　総合大会　ISS「学生ポスターセッション」

H25 年度

- 及川祐希，西村広光
  「近赤外情報を利用したカード認証方式の性能評価に関する検討」
  2014 年　電子情報通信学会　総合大会　ISS「学生ポスターセッション」

H24 年度

- 神庭侑太，櫻井惠介，西村広光
  「カード認証に向けた高精度カード検出の検討」
  2013 年　電子情報通信学会　総合大会　ISS「学生ポスターセッション」
- 櫻井惠介・神庭侑太・西村広光
  「赤外線透過フィルタを利用したカード認証システムの検討」
  2013 年　電子情報通信学会総合大会
- 西村広光，櫻井惠介，神庭侑太
  「個人認証方法及び個人認証システム」
  特願 2013-114443

モバイルクラウドサービスを実現するための統合セキュリティ対策システムの開発（相関利用型情報ハイディング技術）

研究者名：情報ネットワーク・コミュニケーション学科　　鳥井　秀幸

１．研究の目的

近年、著作権侵害に関する社会的関心が高まっており、著作権保護技術の一つである電子透かしが注目を集めている。電子透かしやステガノグラフィなどのディジタルデータに特定の情報を隠蔽する技術は、情報ハイディングと呼ばれており、各種の応用が盛んに研究されている状況である。情報ハイディングが対象とするディジタルデータは、画像・動画・音声および音楽など、様々なものが存在するが、本研究では画像および音楽に対する情報ハイディングを研究対象とする。また、情報ハイディングを実現する方式としても様々なものが存在するが、本研究では周波数領域利用型かつ相関利用型の情報ハイディング技術を利用する。周波数領域利用型の情報ハイディングとは、画像（音楽）に対して離散フーリエ変換（DFT)、離散コサイン変換（DCT)、離散ウェーブレット変換（DWT）等の周波数変換を施し、周波数領域で透かし情報を埋め込んだ後、逆変換により透かし情報入り画像（音楽）を得る手法である。相関利用型の情報ハイディングは、通信分野におけるスペクトル拡散方式を応用したものであり、通信分野と同様に、その性能は使用する拡散系列の特性に依存する。一般に、情報ハイディングの研究では、情報ハイディングのアルゴリズムに対する研究が主に行われており、各種の周波数変換間の得失に関しては、ほとんど研究が行われていない。そこで、本研究では周波数変換として DFT、DCT、DWT を用いた周波数利用型かつ相関利用型の画像用情報ハイディングについて定量的な性能評価を行い、得られた結果を互いに比較することにより、周波数変換の違いによる得失を明らかにすることを目的とする。また、周波数領域利用型の画像用情報ハイディングでは、周波数領域で情報を埋め込んだ後に逆変換を行って透かし入り画像を得るが、同じ強度で情報を埋め込めば理論的には周波数変換の種類には依存せず同一のエネルギーを持つ透かし入り画像が得られるはずである。しかし、実数から整数への変換、0 未満の画素値を 0 へ変換、256 以上の画素値を 255 へ変換などの操作があるため、周波数変換の種類によって透かし入り画像のエネルギーに差が出る可能性がある。そこで、透かし入り画像と元画像のエネルギーの差についても検証を行う。さらに、周波数変換として DFT および DCT を用いた周波数利用型かつ相関利用型の音楽用情報ハイディングについても定量的な性能評価を行い、得られた結果を互いに比較することにより、周波数変換の違いによる得失を明らかにすることも目的とする。また、音楽に関しても、実数から整数への変換、-65563 未満の振幅値を-65536 へ変換、65536 以上の振幅値を 65535 へ変換などの操作があるため、周波数変換の種類によって透かし入り音楽のエネルギーに差が出る可能性がある。そこで、透かし入

り音楽と元音楽のエネルギーの差についても検証を行う。

２．研究の必要性及び従来の研究

一般に、画像（音楽）用情報ハイディングには大きく分けて、空間（時間）領域利用型と周波数領域利用型の 2 種類に分類することができる。空間（時間）領域利用型は処理が簡単であるが改変等の攻撃に弱く、周波数領域利用型は処理が複雑であるが改変等の攻撃に強いという特徴があり、従来からそれぞれの得失を考慮した様々な情報ハイディング技術が研究・提案されている。同様に、情報の埋め込み方式においても、様々な技術が研究・提案されている。本研究では、周波数変換を利用し、情報の埋め込みに拡散系列を使用する周波数領域利用型かつ相関利用型の情報ハイディング技術を対象としている。従来の情報ハイディングの研究は、情報ハイディングのアルゴリズムに対する研究が主に行われており、同一の埋め込み方式に対する各種の周波数変換間の得失に関しては、ほとんど研究が行われていない。そこで、本研究が対象とする周波数領域利用型かつ相関利用型の情報ハイディングにおいても、特に画質（音質）劣化を最小限に抑えるという観点から、周波数変換としてどの変換が最も適したものであるのかを明らかにする必要がある。

３．期待される効果

相関利用型の情報ハイディングでは、拡散系列を用いて情報を埋め込む際に、強度と呼ばれる係数を拡散系列全体に乗算することが必要となる。この強度が小さいと、透かし入りの画像（音楽）から情報を復元した際に、復元した情報に誤りが発生してしまう。したがって、この観点からは、強度は大きい方が良いということができる。しかし、画像（音楽）に埋め込む拡散系列は、元の画像（音楽）にとってはノイズとして作用するため、画質（音質）劣化の原因となる。強度が大きい程、この画質（音質）劣化も大きくなる。したがって、画質（音質）の観点からは、強度は小さい方が良いということができる。この様に、誤り率と画質（音質）は強度に対して、互いにトレードオフの関係にあるため、情報を埋め込む際には、誤りが発生しない必要最小限の強度を使用することが重要である。しかし、使用する画像（音楽）、拡散系列、情報が同一の場合であっても、周波数変換が異なれば、必要最小限の強度に違いが発生する可能性が極めて高い。どの周波数変換を用いれば埋め込みに必要な強度が最小となるかは、対象となる画像（音楽）にも依存する可能性が高く、絶対的に優れている周波数変換というものは存在しない可能性がある。そこで、他の条件を全て同一にした場合において、どの周波数変換が必要最小限の強度を平均的に最も小さくすることができるかを明らかにする。すなわち、どの周波数変換が平均的に最も画質（音質）劣化を抑えることがきるかが明らかになると期待される。

４．研究の経過及び結果

まず、画像用情報ハイディングに関して、対象画像として縦横 256 画素のビットマップ

画像を 10 種類、拡散系列として縦横 32、16、8 の大きさのものをそれぞれ 3 種類、埋め込む情報としてランダムに発生させた 960bit、240bit、60bit の乱数をそれぞれ 3 種類使用した。これらの条件を同一にし、周波数変換として DFT、DCT、DWT を用いた場合に、必要最小限の強度の違いを検証した。なお、周波数変換の次元は、256 次とした。また、透かし入り画像と元画像のエネルギーの差についても検証を行った。なお、ある程度の画質を維持するため、周波数変換後に画像のエネルギーが集中する全体の 1/16 に相当する低周波領域には透かし情報を埋め込まないものとした。検証の結果、強度に関しては DWT、DCT、DFT の順で必要最小限の強度の値が低いことが判明した。これより、周波数領域利用型かつ相関利用型の画像用情報ハイディングにおいては、画質劣化という観点から考えると、DWT、DCT、DFT の順で適しているということが推測される。エネルギーの差については、強度で見られたような周波数変換に依存した明確な大小関係は見られなかった。理論的には、埋め込み強度が大きいほどエネルギーの差も大きくなるはずであるが、そのような結果にはならなった。これは、実数から整数への変換、0 未満の画素値を 0 へ変換、256 以上の画素値を 255 へ変換などの操作があるため、周波数変換の種類によって埋め込んだ情報のエネルギーの表れ方が異なるためだと考えられる。

さらに、音楽用情報ハイディングに関して、再生時間が 3～4 分程度の WAV 形式の音楽を 3 種類、周波数変換の次元を 256、512、1024 の 3 種類、拡散系列として 64、128、256 の長さのものをそれぞれ 2 種類、埋め込む情報としてランダムに発生させた 1024bit の乱数を 2 種類使用した。これらの条件を同一にし、周波数変換として DFT および DCT を用いた場合に、必要最小限の強度の違いを検証した。また、透かし入り音楽と元音楽のエネルギーの差についても検証を行った。なお、ある程度の音質を維持するため、周波数変換後に音楽のエネルギーが集中する全体の 1/4 に相当する低周波領域には透かし情報を埋め込まないものとした。検証の結果、強度に関しては DCT の方が DFT よりも必要最小限の強度の値が低いことが判明した。これより、周波数領域利用型かつ相関利用型の音楽用情報ハイディングにおいては、音質劣化という観点から考えると、DCT の方が DFT よりも適しているということが推測される。エネルギーの差については、画像の場合と同様に、強度で見られたような周波数変換に依存した明確な大小関係は見られなかった。音楽においても、実数から整数への変換、-65563 未満の振幅値を-65536 へ変換、65536 以上の振幅値を 65535 へ変換など操作があるため、周波数変換の種類によって埋め込んだ情報のエネルギーの表れ方が異なるためだと考えられる。

５．今後の計画

画像に対する検証を行った際に、周波数変換の種類によって、同じ強度で情報を埋め込んだ場合でも透かし入り画像におけるノイズの表れ方がかなり異なっていることが明らかとなった。したがって、単純に必要最小限の強度のみで画質の優劣を比較するのが適切ではない場合もあることが推測される。そこで、画質の劣化を強度のみで判定するのではな

く、人間の感覚によってどのように認識されるのかという観点から検証を行う必要があると考えられる。これは音楽に対しても同様であると推測される。また、ディジタル画像や音楽は圧縮されて用いられることが多いため、JPEG や MP3 などの圧縮形式で使用した場合においても、今回の検証結果と同様の優劣が存在するのかについても検証を行う必要がある。

６．研究成果の発表

特になし。

社会的要請に基づいた組織内情報セキュリティのための ICT プラットフォーム構築に向けた基盤研究

研究者名：情報工学科　　納富　一宏，　松田　三知子

１．研究の目的

現在，様々な組織により構成された情報システムが社会において利用されている．各システムのセキュリティは，各々の組織内のポリシーにしたがってシステムに反映されているが，今後ますます守るべきデータは多くなると考えられる．本研究では，安全安心なインターネット社会構築に資する情報管理・監査手段を基盤とした組織内情報セキュリティシステムの構築を目的としている．具体的には，高度な情報セキュリティモデルに基づいた情報セキュリティプラットフォーム構築に必要な基盤技術の提供を目標とする．H28 年度は，これまでの研究で得た情報セキュリティモデルに対する考え方をベースに，プラットフォーム構築につながる情報セキュリティモデルを構成し高度化を図ることを目的とした．具体的には，社会的要請に対してシステム的な見方を導入して，技術的な要求が見える形で情報セキュリティモデルをまとめることを目標とした．

２．研究の必要性及び従来の研究

一般に，分野毎の技術統合を図りシステム化を図る場合，水平的なシステム化が主流であるが，本研究では，「セキュリティと社会」の観点で社会システム全体から情報セキュリティを俯瞰した上で，これをシステム的に考えるために「セキュリティ管理手法」を考察し，「情報漏洩防止」という重要な観点に焦点を絞り，さらにそれを実現する有望な技術面での観点「生体個人認証」について掘り下げるという，全体から実現技術までを統合して情報セキュリティモデルを作り，それをベースに情報セキュリティプラットフォームを中心として「全体システム設計」をするという垂直的なアプローチをとっている．これにより，より堅牢な情報セキュリティシステムの構築が可能になる．実現に向け，人文社会系と理工学系の研究者が障壁をなくし，学際的・横断的な研究の進め方をしている．

情報通信技術（ICT）の進歩は日進月歩であり，それを利用する人々の意識との間に生じるタイムラグは，新たなリスクや社会問題をもたらす．このセキュリティをめぐるズレは社会の至る所に偏在し，技術者・開発者と，組織の管理者・運用者，末端の利用者・ユーザとの間にも認識のズレが生じている．例えば，セキュリティに関する意識・知識・行動は多様であるにもかかわらず，標準化された利用者像を前提としたセキュリティ対策が講じられがちである．加えて，現在進行形で変化・発展するハッキングの手口を事前に予測することの困難さ，現場の人々の心理につけ込むソーシャル・エンジニアリングへの対策

の困難さが指摘されて久しい．そこで，このような「セキュリティと社会」の状況を考慮に入れた「セキュリティ管理手法」を検討し，特に，「情報漏洩防止」に注目して有効な手段である「生体個人認証」技術を積極的に取りいれた形で，組織内セキュリティモデルに基づいて「全体システム設計」を行う．共有可能な情報セキュリティプラットフォームを提案し（図 1 参照），各組織が情報システムをプラットフォーム上に構成することでセキュリティを保障する．

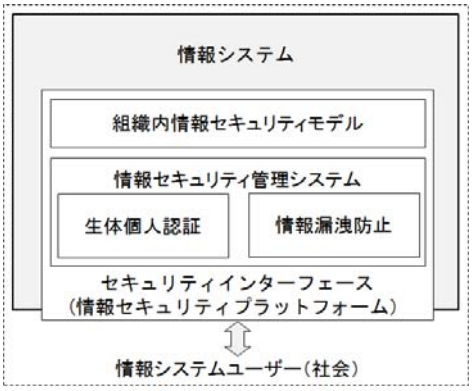


図 1．提案システムイメージ

以下，本報告書では，生体個人認証およびシステム監査に関する部分を中心に記述する．

3．期待される効果

組織内情報セキュリティにおいて，社会的にも重要課題である情報漏洩の防止策として，生体個人認証の技術をベースとした情報セキュリティモデルを構成し，それに基づいてシステムの情報セキュリティを保障する情報セキュリティ管理システムを提案し，各分担研究成果を共有プラットフォーム構築の基盤技術提供に繋げる．情報システムにおける個人認証は，盗聴・盗難や漏洩の危険性が存在することから，常になりすましへの対策を考慮しなければならない．また，システムへの不正侵入や情報の改ざんなどサイバー攻撃の脅威を低減することが重要である．さらに，超高齢化社会における認証時情報の忘却・盗難防止の検討が望まれている．これらへの対策として指紋や掌指形状，顔，虹彩パターン，声紋といった生体情報をキーとする生体個人認証（バイオメトリクス認証）技術が注目されており，さらにその発展が期待されている（図 2 参照）．そこで，生体情報の計測において，特別な計測装置等のハードウェアを必要としない手法の確立を目指す．機械学習型のバイオメトリクス認証方式を採用した認証システムの開発を実施する．また，特に各種センサを搭載したスマートフォンやタブレット PC など近年，身近となったモバイルデバイスを対象とすることで，個人識別に用いる特徴量計測を行い，提案手法の適用可能性に係る，実運用を意識した検証実験によりシステム評価を実施する．

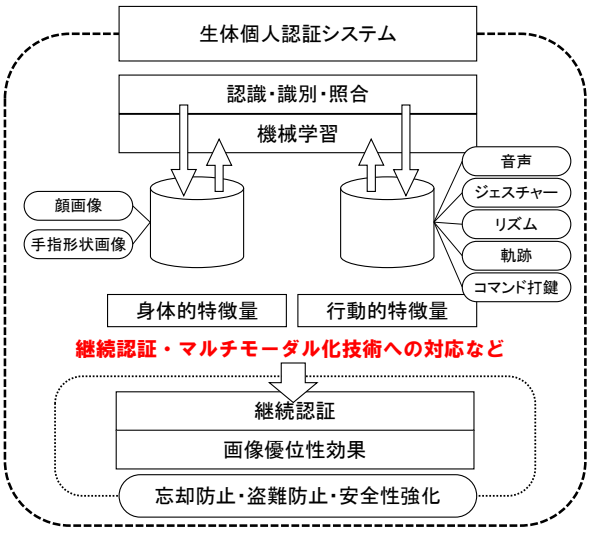


図 2．生体個人認証システムの拡張

４．研究の経過及び結果

情報システムにおける生体個人認証手法の開発と様々な状況下における検証実験に基づく精度評価を継続的に行った．特に，身体的特徴量および行動的特徴量はともに実際に認証を行う状況に応じた計測が必要であった．H28 年度に実験および評価を行った特徴量としては，声紋，コマンド操作時の打鍵動作，タッチ動作，デバイス保持動作であり，いずれも行動的特徴量をベースとしており，概ね 70～95%程度の認証精度が得られた．また，環状配置画像選択方式という新たな認証方式を提案したことで，行動的特徴量との２要素による統合認証が可能となった．また，一連のコマンド操作において連続的な打鍵タイミング情報を用いることで継続認証実現への可能性が開けた.

H27 年度までの身体的特徴量をベースとする方式に比べて認証精度は，条件によっては若干低下の低下が認められたが，それ以外の条件については同程度であった．認証精度の低下条件については，個人の特徴量の安定度が問題となるケースが多く，利用者個別に分散値の少ない情報を特徴量として取得することが課題となる．これらについては最初の登録時にチェックすることが重要である点を確認した．H28 年度の研究成果としては，複数の認証方式との統合が可能となったこと，および継続認証の可能性が開けたことにより，より安全・安心な環境の実現が期待できる.

今後は，ユーザ操作が容易でかつ個人認証精度が高い認証方式の確立が望まれるが，今回の研究により得られた，認証のマルチモーダル化と継続認証の可能性をさらに発展させ，実用レベルまで引き上げるための研究が必須である.

これらいずれも識別手法としては，ニューラルネットワークモデルのひとつである自己組織化マップ（Self-Organizing Maps）による機械学習を用いた統一的な手法に基づいているため，複数の特徴量による生体個人認証を複合的に搭載した情報システムの設計が可能であることが実証されつつある．これまでの研究で培ってきた成果をさらに発展させて研究を進めていきたい.

今後はクラウド・サーバにより一元管理されたデータベースに，各個人がモバイル端末からアクセスしてデータを利用する形式がさらに進むこと，その際にその個人を確実に特定する方策がセキュリティ上は重要であり，情報漏洩の防止策としても指紋，顔，声紋などを使った生体個人認証が個人への負担も少なく有用であることなどがわかった．なお，クラウド・サーバ上に生体認証用のデリケートなデータを蓄積することの議論・考察は十二分に尽くされたとは言い難いのが現状である．しかしながら，情報セキュリティ技術の発展のためには具体的なモデルを用いた検証および実証実験による検討は必要不可欠である．これらについては，具体的な個別事例を調査し，知見を増やしていく必要がある.

５．今後の計画

これまでの研究活動において試みてきたソフトコンピューティングを活用した生体個人認証（バイオメトリクス認証）のうち，①スマートフォン操作における「フリック」「スワ

イプ」「シェイク」などの操作時特徴量をキーとした「操作情報認証」，②キーボード上に置かれた手指形状を認識する「手指形状認証」，③スマートフォンに搭載されている各種センサからの入力情報とタッチパネルからの軌跡情報を複合化した「手書きパターン認証」，④画像優位性効果を活用した画像認証技術との併用による「忘却防止・盗難防止」，に加えて，⑤コマンド操作時の連続打鍵情報による「継続認証」の５つの検討項目を発展・高度化し，さらなる認証精度の向上を目指す．また，「高齢化社会へ受容される生体個人認証のあり方」という観点による考察を加える．さらに，これまで検証してきた個別要素による生体個人認証だけではなく，複数要素を用いたマルチモーダル認証方式のバリエーションを検討すると共に，システム使用中の連続操作に着目した継続的な認証方式の精度向上により，さらなるセキュリティの向上を目指す．ここで，ユーザ操作の妨害やユーザビリティの低減などを招かないような配慮と，アクセシビリティの確保を確実に行うための方策について，実証実験に基づいた検討・考察を行って行きたい．

最後に，本研究を進めるための方略について述べる．深層学習（Deep Learning）技術の発展に伴い，様々なライブラリ，ミドルウェア，フレームワークなどが世界的な企業や研究機関から豊富な研究用リソースが提供されている．また，プログラミングを補助するための数値計算ツールとして定評のある MATLAB やそのオープンソースソフトウェア（OSS）版である GNU Octave, 数値計算ライブラリ拡張を装備した Python 言語などが広く活用されてきている．これまで，独自プログラム開発を行って研究を進めてきているが，最近注目されているこうしたツールなども適宜取り入れていくことも重要である．これらを踏まえて安定した研究推進を図るためには，研究分担する教員間の密な情報共有が大切である．分担した分野ごとの共同研究を進めると共に，共通の技術理解を目的とした勉強会の実施なども充実させていきたい．

６．研究成果の発表

[1] 河合博之*, 納富一宏, 斎藤恵一:"画像選択および音声発話の二要素による個人認証システムの開発", バイオメディカル・ファジィ・システム学会誌, Vol.19, No.1, pp.??-?? (7pages), (2017.06 発刊予定) [採録決定 2017.2.2].

[2] 梶原　礼*, 河合博之*, 納富一宏:"サーバ操作時の打鍵情報による継続的な個人認証手法の検討", 情報処理学会 第 79 回全国大会講演論文集 第 3 分冊, 3W-03, pp.569-570, (2017.03).

[3] 河合博之*, 納富一宏, 斎藤恵一:"環状配置画像と音声発話の二要素による個人認証システムの開発と評価", バイオメディカル・ファジィ・システム学会 第 29 回年次大会講演論文集, pp.83-86, (2016.11).

[4] 河合博之*, 納富一宏, 斎藤恵一:"画像を用いた音声認証システムの実装：画像選択時におけるなりすまし耐性の評価", 情報処理学会 第 15 回情報科学技術フォーラム (FIT2016)講演論文集, 第 4 分冊, L-019, pp.147-148, (2016.09).

（*：発表当時，本学学生）

以上

情報漏洩防止に向けての研究

研究者名：所属学科 情報ネットワーク・コミュニケーション　　氏名 岡本学

１．研究の目的

近年，個人情報の漏洩が問題となっており，特にパスワードが流出した場合には簡単になりすましが発生してしまう可能性がある．パスワード以上に「強い認証」を実現するための認証手段として，ワンタイム・パスワードや生体認証，PKI 認証等があり，更にそれらを複数組み合わせて利用するマルチサインオン技術も存在する．ただしそれら各技術に対応する設備環境を取りそろえるのはサービス提供側にとって負担が大きく，利用者にとっても認証手段を使い分ける面倒が生じる．そこで Web サイト訪問履歴を利用した追加認証方式を研究する．本方式では通常のパスワード認証に加えて，ユーザが事前に登録した順番通りに特定 Web サイトを訪問したかどうかで追加の本人確認を行う．サイトの訪問履歴はクライアント端末に保存されるものを利用せず，アイデンティティ・プロバイダ(IdP)と呼ばれる認証サーバから各サイトが画像取得する際に記録されるログを用いるため，ユーザは特別な機器や追加ソフトウェアを必要とせず，簡易にいつでもどこでも利用できる方式であり，ユビキタス社会における新たな安全安心を実現する技術である．

２．研究の必要性及び従来の研究

ユーザがブラウザを立ち上げてネットサーフィンを行う際，毎回ほぼ同じ順序で各サービスサイトを訪問することが多い．例えば，ツイッターで友人関係のつぶやきをまずチェックし, Instagram と Facebook で更に近況をチェックしたうえで最後はニュースサイトをみる，といった具合である．これら一連の動作は本人が意識的に行っているというよりは，一種の個人的な癖として行っている場合がほとんどである．

そこで本研究では，ユーザが自分があらかじめ決めておいた順番で特定のサイトを訪問した「Web サイト訪問履歴」をもって自身の本人確認に利用させる方式を提案する．具体的にはサイト１→サイト２→サイト３と自身が登録した順番通りに正しく該当サイトを訪問することで本人確認を受ける方式である．

従来の研究においては，パスワード方式以外の認証方式としては生体認証やワンタイム・パスワード，PKI 認証等があるが，これら認証方式を実現するにはサービス側においては様々な設備環境の構築に負担がかかることが課題であった．ハードウェアや証明書が必要であればそれらの送付・発行といった費用や手間がかかるし，ユーザからの問い合わせ対処も必要となり，保守管理の負担も馬鹿にならない．一方ユーザにとっても記憶だけで済むパスワード方式とは異なり，例えば生体認証の指紋認証であれば指紋読み取り装置が必要であるし，ワンタイム・パスワードであればパスワード発生装置の所持が必要であ

り，PKI 認証の場合は証明書や鍵の保持が必要となる．常にそれら機器・情報を持ち歩かなければならないのはユーザにとって負担となる場合があるし，例えば出張先ホテルのビジネスルーム共有 PC からでは必要設備が揃わず利用が難しい場合がある．

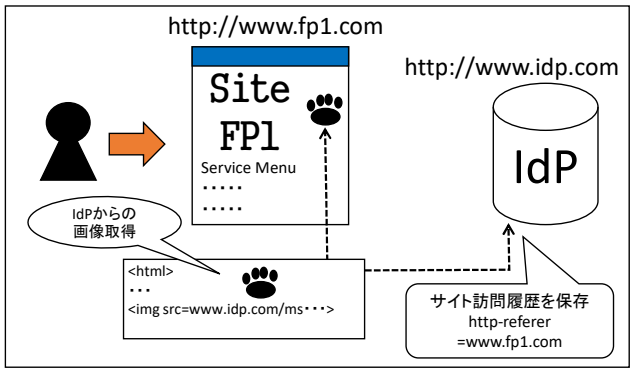
３．期待される効果

本研究では「Web サイトを決められた順番に訪問した」という「Web サイト訪問履歴」を用いて認証を行うことでこれら特別な道具・情報と必要とせず，更にいつでもどこでも利用できる認証方式として実現できる．特に，Web サイト訪問履歴の取得方法として，各 Web サイトから認証サーバ（Identity Provider）への画像取得依頼の際のログを用いることで，ユーザ・クライアント端末側の情報を用いない方式をとる．つまり特定の訪問履歴以外は記録・蓄積・利用されないため，ユーザのプライバシーを守ることが可能な方式である．

４．研究の経過及び結果

ユーザの「行動履歴」を用いて本人確認を行うことを目的とする技術提案はこれまでも様々行われてきている．特に近年ではこれら情報を「ライフログ」と呼び，その利活用方式が注目されている．更にライフログ認証の一種として，普段と異なった行動が判断された場合に追加認証を行う「リスクベース認証」技術があり実際に銀行等で利用されている．

そこで本研究ではライフログとして Web サイトの訪問履歴を利用する．訪問するサイトの順番が事前登録した順番と同じでなければ本人として認めない追加認証方式であり，リスクベース認証の一種としても利用可能である．Web サイト訪問についてはあくまで認証行為を目的として意識的に巡回して本人性を示してもよいが，恣意的に振舞って，結果的には「普段どおりの行動」としての Web サーフィンとなり，自然と「いつも通りの Web サイト訪問の順番」となることで認証が完了してもよい．



参考図：Web サイト訪問履歴を用いた認証方式

例えば「追加パスワード」方式や「秘密の質問」方式であればその回答を意識的かつ永続的に記憶しておく必要があり，しかもそれらの質問・回答の確認行為がずっと行われな

い場合はその質問・回答を本人自身も忘れてしまう課題があるが，Web サイトの訪問であれば「いつも通りの行動」を行えばこれに対応でき，覚えやすさの点において優位性が期待できる点を狙う．

なお 28 年度は本方式の基本案を下記発表文献[1]にて発表した．本論文では，認証情報通知にシングルサインオン・プロトコルを利用したうえで，FP と呼ばれる訪問記録サイトに IdP と呼ばれる認証サーバからの画像取得タグを含めることにより IdP に FP 訪問履歴情報を蓄積させ，それらユーザの「Web サイト訪問履歴情報」が事前にユーザが登録していたものと一致することでユーザを追加認証する方式を提案した．履歴と登録情報が一致すれば IdP は結果をシングルサインオン・プロトコルの認証結果応答通知として SP と呼ばれるサービス提供サイトに対し発行し，それにより SP はユーザを単純な ID・パスワード以上のセキュリティ強度で本人確認ができる．

５．　今後の計画

今後の課題としては，どの程度の数の訪問記録サイトを準備すれば，更には各ユーザが Web サイト訪問履歴の正答数としてどの程度のサイト数を登録すれば，より利便性が高まり安全性を守ることができるかをユーザ試験を通して見極めることが必要となる．また本方式以外のライフログを用いた認証方式，あるいは「強い認証方式」についても合わせて研究を行うものとする．

６．　研究成果の発表

[1] 熊澤祐紀,伊藤茜，岡本学,"Web 履歴認証方式の提案",2017 年暗号と情報セキュリティシンポジウム(SCIS2017)，　2017 年 1 月,沖縄.

研究課題名「セキュリティと社会」

研究者名：基礎・教養教育センター　三浦直子

１．研究の目的

本研究は、組織内情報セキュリティの高度化に向けて、人々の実際の情報通信技術（以下、ICT）の利用状況について社会調査を実施し、得られた調査結果を踏まえて人文社会科学の分野（情報社会論、社会学理論）から研究枠組みを提供することを目的としている。それはまた、文理融合の立場から、既存の情報セキュリティの盲点への対策を検討するものでもある。

本研究は、文系・理系の研究領域の分断がもたらす２つの盲点に注目する。１つ目の盲点とは、技術開発者と実際の利用者との認識の「ずれ」である。日進月歩する ICT の開発状況（開発スピード）と、それを利用する人々のセキュリティ意識・知識・行動の変化（対応スピード）との間にはタイムラグが生じ、この「ずれ」が情報セキュリティ上の大きなリスクとなってきた。いわば、時間軸における「ずれ」の社会的効果に対する注目である。加えて注意すべきは、技術開発時に「利用者」として想定されてきた人々が、決して均質的で一枚岩な社会集団ではなく、セキュリティ意識・知識・行動の面で多様性を有しているという点である。いわば、現実の利用者空間（利用者集団）という、空間軸における「ずれ」の社会的効果への注目と位置づけることができよう。社会学では、時間軸や空間軸において多様である人々の認知図式・行動様式を、「ハビトゥス」概念を用いて理論化してきた。そこで、ハビトゥス論を踏まえた社会調査を実施することで、情報社会に特有のハビトゥスについて分析し、情報セキュリティのための研究枠組みを提供する。

２つ目の盲点は、情報セキュリティに関する今日的リスクが、まさに文系・理系の研究領域の分断・棲み分けによってもたらされているという側面である。これまで、人々のプライベートな SNS 利用に関しては、情報セキュリティ（理工系）というよりも、むしろ情報モラル（人文社会系）の側面として注意喚起されることが多かった。例えば、「ネット炎上を起こさないように、社員としての自覚をもって投稿内容に注意しよう」と言われるように、企業の社会的イメージを傷つけないように振る舞うべきとして、ネット上での交流マナーの問題として捉えられがちであった。しかし今日では、下記「2. 研究の必要性及び従来の研究」にて詳細を確認するように、SNS への投稿画像から情報セキュリティの認証に必要な生体情報の読み取りが技術上可能となったり、公私でパスワードを使い回していたため大規模な個人情報漏洩によって組織の攻撃リスクが高まったり、プライベートな投稿内容に依拠したソーシャル・エンジニアリングによる標的型攻撃などが登場したりしている。すなわち、「SNS の利用は情報モラルの対象であって、セキュリティ技術の開発とは無関係」と見なしがちな専門分化した既存の視点では対応できない情報セキュリティ上の盲点が、今日的な新しいリスクの源泉となっていると言えよう。

２．研究の必要性及び従来の研究

本研究では、日々進展する ICT の技術革新がもたらした新しい今日的なリスクについて、言い換えれば、専門分化された文系・理系領域の分断によって既存のセキュリティ研究の「盲点」となってきた、技術革新にともなう人々のセキュリティに関する知識・意識・行動のずれを、また ICT をめぐる人々の認知図式や行動様式の特徴を、社会学のハビトゥス論の視座から解明する。それはまた、文理融合の視点から、実際の ICT 利用状況を調査し、人々の時間軸・空間軸におけるハビトゥスのずれが、情報セキュリティにどのような影響を及ぼしているのかについて、調査・検討するものである。

今年（2017 年）1 月、指紋の盗撮防止技術を開発した国立情報学研究所は、SNS 等に投稿されたスナップ写真（ピースサインをした画像）から、指紋や瞳の虹彩など情報セキュリティの生体認証に関わる個人情報が漏洩しうる危険性を指摘し、社会に広く警戒を呼びかけた。同研究所の実験では、3 メートル離れて撮影した画像からも指紋を読み取ることが可能であったという。このように、日進月歩の技術革新によって（例えば、高解像度カメラを搭載したスマートフォンの普及など）、情報セキュリティに関する現実の危険性は、人々のセキュリティ意識や想定していたリスクを凌駕しつつある。

写真から指紋認証に必要な情報を読み取る技術は、さらに 2 年ほど遡った 2014 年 12 月、ホワイトハッカー集団 Chaos Computer Club（以下、CCC）のハンブルク大会にて、既に公開されていた。大会では、ドイツ国防大臣の記者会見写真から親指の指紋を読み取り、市販のソフトウェア（指紋読み取りソフト「VeriFinger」）を用いて指紋認証システムを通過できる水準での指紋複製が可能であることが実演された。その際、指紋のついたコップなどを物理的に入手する必要がなくなったことが指摘され、政治家に対して公的な場で手袋を着用することが提案された（なお、今年 1 月に国立情報学研究所が発表した盗撮防止技術も、指先に着用する読み取り防止フィルムであり、CCC と同様の提案といえよう）。CCC の実演からわずか 2 年で、報道記者が撮影した会見写真から、一般の人々による Web 上の投稿画像へと、生体認証に関する指紋複製の対象が拡大したのは、目を見張るスピードと言えよう。さらに CCC は、今年 5 月、Samsung 社の最新スマートフォンに搭載された虹彩認証機能についても、所有者をデジタルカメラの夜間撮影モードで 5 メートル離れた場所から撮影し、瞳を実物大に拡大して印刷したものにコンタクトレンズを載せることで偽装できると動画で発表した。これもまた、技術革新にともない近い将来、Web 上の投稿画像への加工から複製が可能となるかもしれない。

加えて日本社会においては、富士通が 2015 年 1 月に行ったビジネスマンに対する全国調査によると、業務ごとに使い分けるよう指導しているパスワードを、プライベートまたは別の業務で使い回しているビジネスマンの割合が 93%にものぼり、また 60%が類似パスワードを使用していることが判明した。企業や組織がいくら「注意喚起」を促しても、「覚えきれない」「面倒」といった理由から、パスワードの使い回し防止など人々のセキュリティ行動にはほとんど効果がなく、それゆえ、別のルートからプライベートのパスワード（仕

事でも使い回しているパスワード）が漏洩すれば、企業への攻撃に悪用されるリスクが懸念されている。

さらに、昨今の標的型攻撃で用いられるソーシャル・エンジニアリングの手法には、SNSに投稿された個人情報が参照されているとも指摘されて久しい（例えば、犬好きを公言する社員に愛犬家を装った書き込みで近づき、飼い犬自慢の画像に偽装して添付したマルウェアを開封させる等)。このように、人々のプライベートなSNS利用（投稿画像、IDやパスワードの使い回し、投稿内容等）が、今日では企業や組織の情報セキュリティにリスクをもたらす新たな要因ともなっていると言えよう。

３．期待される効果

本研究において期待される効果は、上述してきたような、今日の高度に専門分化された研究状況、すなわち文系と理系の研究領域の分断状況においては「盲点」となってきたセキュリティ上のリスクの現状を調査データに基づいて客観的に分析し、時間軸・空間軸における「ずれ」を把握できる研究枠組みを提供することで、組織内の情報セキュリティにおける新たな対策を提案することである。他方でそれは、情報社会における人々のハビトゥス（社会的位置に由来する認識図式や行動様式）の特徴や変化を実証するものであり、社会学的研究におけるハビトゥス論（理論）の実証研究への展開の試みとしても位置付けられる。それゆえ、文理融合によって、情報セキュリティ技術の運用に関する提案という実際の効果と、情報社会論における社会学理論の実証的展開を促す学術的な効果とが期待される。

４．研究の経過及び結果

本研究では、利用者の情報セキュリティに関して、大学生を対象とした社会調査を実施してきた。文系大学（人文学科・社会学科）と理系大学（工学系学科・情報系学科)、および理系大学単独（バイオ系学科・工学系学科・情報系学科）で調査を実施したところ、セキュリティに関する知識、意識、行動を尋ねる質問項目相互の間には、いずれの調査においても統計的有意差が、すなわち相関関係が算出されなかった。むしろ、セキュリティに関する知識や意識には、学科や性別といった回答者の「属性」が大きくかかわっており、また、セキュリティに関する実際の被害や加害に関しては、ネット上での「慣習行動」（習慣、すなわち意識に上らない日常的な実践）が関係していることが判明した。

以上の調査結果から、情報セキュリティ対策には、これまで一般的に想定されていたような「講演によって知識を与える研修」だけでは行動に結びつかないことが明らかとなった。喩えるならば、運動不足が健康に良くないと理解しており（知識があり)、実際に健康診断の数値も悪くなって焦っている（意識している）にもかかわらず、忙しさや不規則な生活時間などにより普段から運動する習慣のない人々は、なかなか運動不足を改善できない（行動に結びつかない）という状況と同様であると言えよう。そのような人々が、研修

によって「運動不足が健康に良くない」「病気のリスクを高める」という講演を聞いても、改善は難しい。

ここで注目すべきは、属性による意識の相違であろう。学生にとっての学科だけでなく、社会人にとっての職場という日常的な所属の場においても、意識は共有されると想定しうる。そこで、意識を共有する職場単位で慣習行動を促すような「実践」を取り入れれば、行動も定着しやすくなると考える。具体的には、避難訓練と同様の「体験型」研修の導入である。避難訓練もまた、どれほど気を付けていても（意識しているにもかかわらず)、避けられない震災や不慮の事故で生じてしまった火災に対する「体験型」研修である。これは、事前の予防（防災の知識や意識の涵養）はもちろんのこと、事後の対策について経験しておくことで、実際の被害を最小限に留める効果があり、情報セキュリティ対策においても避難訓練をモデルとした「体験型」研修には大きな効果が期待できると言えよう。

５．今後の計画

これまで、予算や時間面での制約から、大学生を対象とした予備的な社会調査を実施してきた。しかし、そこから得られた知見は情報セキュリティにとって重要な示唆を与えるものであった。そこで今後は調査対象を広げ、企業や組織に勤務する現役世代に対する全国調査の実施を計画している。その際、ハビトゥス論を用いて、どのような社会的属性が人々のセキュリティ意識・知識・行動にどれほど影響しているのかを分析することで、組織内情報セキュリティの高度化のためのより正確な現状分析と対策の提案を行う。

まず今年の前期から夏休みにかけて、これまでの調査結果を改めて精査し、質問票（アンケート用紙の質問項目）を精緻化する。秋から冬には、情報セキュリティ（セキュリティ意識・知識・行動の実態）に関するインターネットでの全国調査の実施を予定している（現在、伊藤忠系シンクタンクを親会社にもち、企業や大学、官公庁とも取引実績をもつインターネット調査会社「マイボイスコム株式会社」と相談中)。今年の冬から来年の春にかけて、調査結果を踏まえて明らかとなった社会学的知見をまとめて、情報セキュリティ技術の開発と運用に対する提案を行う。また、これらの研究成果を来年度の査読付き国際学会（国際社会学会や情報処理学会など）で発表することも検討している。

６．研究成果の発表

［1］三浦直子：「ネットワークコミュニケーションにおける情報モラル」，神奈川県総合教育センター（2016,08,02），神奈川工科大学（国内研修での招聘講義）.

［2］三浦直子「情報通信技術がもたらす社会変動とリスク：ネット炎上を考える」，春日清孝他編著『〈社会のセキュリティ〉を生きる:「安全」「安心」と「幸福」との関係』pp.67-91，学文社，2017.04.1（学術図書）.

使いやすさと安全性を両立する認証方式を検討するための セキュリティ意識の調査と解析（2）

研究者名：情報工学科　須藤康裕

１．研究の目的

本研究の目的は，「強い認証」であることを維持した上で，ユーザの IT リテラシに依存しない認証方式の検討を行うために必要な調査と解析である．認証強度と利便性は基本的にトレードオフにあるが，認証方式が複雑になりすぎると利用に支障が出るユーザも増加する．そこで，現在認証手段として広く利用されているパスワード方式に対して，ユーザのセキュリティ意識を解析した結果，定期的にパスワードの変更を実行しているユーザが極めて少数であることが明らかになった．本稿では，ユーザが自ら認証方式を選択することができるシステムを試作する準備として，システム利用者に対して調査を行った結果を報告する．

２．研究の必要性及び従来の研究

情報漏洩防止のための仕組みとして，現在通常に認証手段として用いられているのはパスワード方式であるが，パスワードはフィッシング詐欺やキーロガーによる搾取等で，盗まれたり漏洩したりすることが多い．一方でマトリクス認証やワンタイムパスワードなどの導入は，認証手続きが煩雑になることでユーザからは敬遠されやすい傾向にある．これらの認証手段は，理想的には保護しなければならない情報の機密度を考慮に入れた上で適切な方式を選択すべきであるが，必ずしもシステムがそのように設計されていないのが現状である．また，システム提供者とユーザの間でセキュリティ意識が乖離しているケースもしばしば見受けられる．すなわち，機密度のそれほど高くない情報に対して過分な認証を求めたり，機密度の重要な情報に対して突破されやすい認証を用いていたりする場合がある．この点についての調査も，認証方式の検討には欠かせないものと考える．

３．期待される効果

本研究で得られる情報は，それぞれの認証方式を適切な場面で導入するための指標とすることができるようになる．さらに，これまで実現が難しかった「強くて使いやすい」新しい認証方式を設計するための解を導く．また，ユーザサイドからみた，直感的な使いやすさと認証強度の相関には例外があるため，ユーザが認証方式を選択して使うシステムが考えられる．これはシステムと，その利用に関する認証の仕組みの分離も意味し，そのための API 設計についての指標ともなり得る．

４．研究の経過及び結果

本稿では，情報工学科ソフトウェア工房によって開発運用されている「履修管理システム」のアーキテクチャと直近の運用状況，アンケート調査による利用者のセキュリティ意識の解析結果を示す．

4.1　履修管理システム

大学生が，これまでに積み重ねた単位と，今後修得する単位を総合して長期的な学習プランを設計するためのソフトウェアシステムとして，視覚的・直感的な操作とシラバス等の授業情報を連携した履修マネジメントシステムを開発してきている．履修管理システム（RMS: Registration Management System）の最大の特色は，時間割とカリキュラムツリーを連動することにある．

RMS は 2013 年 4 月より正式にサービス提供を開始しており，現在も稼働中である．RMS は Web アプリケーションとして運用し，ユーザは web ブラウザからシステムにログインして利用する（図１）．システムの基本構成は，時間割画面・科目リスト画面・卒業要件画面・ツリー画面・オプション画面から成る．時間割画面は本システムの中心的画面であり，履修可能な科目とその基本情報が曜日・時限ごとに表示され，履修したい科目を選択することで履修計画を行う．科目リスト画面や卒業要件画面，ツリー画面は，履修済科目の選択や要件の集計・比較，科目間の関係の可視化などにより，時間割画面での履修計画をサポートしている．　https://rms.cs.kanagawa-it.ac.jp/

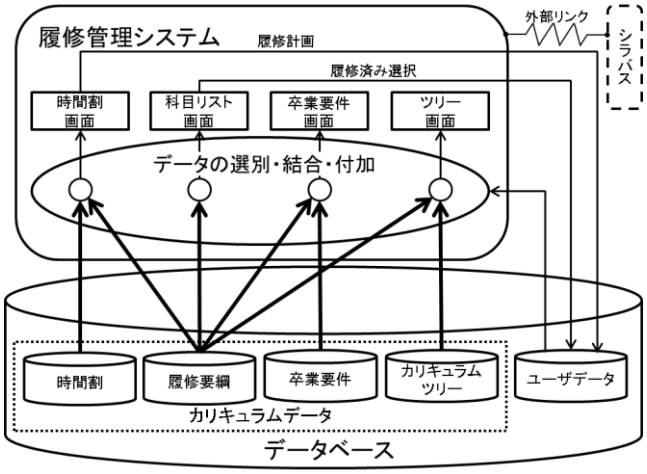


図１　履修管理システム構成図

ユーザデータのうち，機密となるデータは「履修中の科目」と「単位取得済み科目」であり，成績評価や電話番号，住所などの情報は扱っていない．しかしながら通信中の暗号化方式には SSL/TLS を用い，ユーザデータはサーバ内部で SHA-521 を利用して暗号化し，厳格に管理している．

4.2　2017 年度前期における利用者数の推移

2017 年度の履修登録期間は 4 月 8 日～14 日であり，利用者数のピークは 4 月 11 日の 125 名であった．近年のアクセスログから推測できることは，履修キャンセルのためにシステムを用いるユーザは多くないということと，キャンセル期間が過ぎても一定のユーザがシステムを日常的に利用しているということである．

ユーザログインにはパスワードによる認証を行っており，定期的な変更を促しているが，2015 年 1 月 1 日から 2015 年 12 月 31 までの一年間にパスワードの変更を行ったユーザ数を集計した結果，全体の 6.9%（26/376）に留まっているということが判明した（パスワード忘れによるものを除く）．ユーザの多くが情報学部学生ということからいっても，パスワードの定期的な変更に対する認識がきわめて低いことが明らかになった．

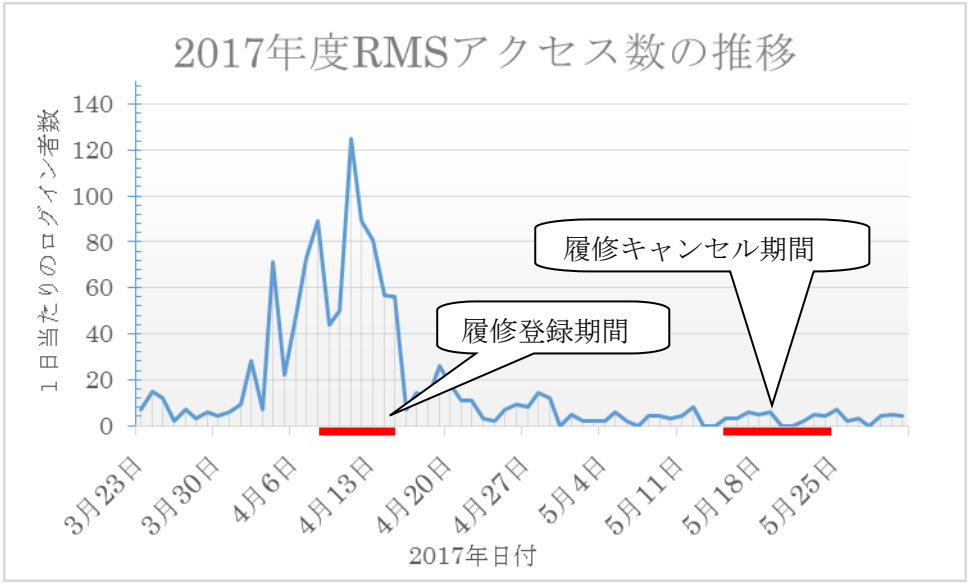


図２　ＲＭＳのユーザログイン数（13～15 年度）

4.3　認証方式の選択に関する意識調査

2017 年度はシステム利用者に対して，もし認証方式を自由に組み合わせることが出来たら何を選択するかアンケート調査を実施し，110 名のユーザから回答を得た．図３はユーザが利用を望んだ認証方式の数（複数回答可）である．

最も多い回答はパスワード方式で，次いで KAIT Walker で使い慣れているマトリクス認証が選ばれる傾向が見られた．携帯などの SMS による認証と IC カード等の物理認証も数%のユーザが希望した．図４はセキュリティ意識が比較的高いであろうと思われる N 科学生のみの回答結果である．認証必要なしの回答がなくなっており，マトリクス認証の比率が高まっている．SMS による認証方式が敬遠されている原因をさらに追跡調査すれば，興味深い結果が得られる可能性が示された．

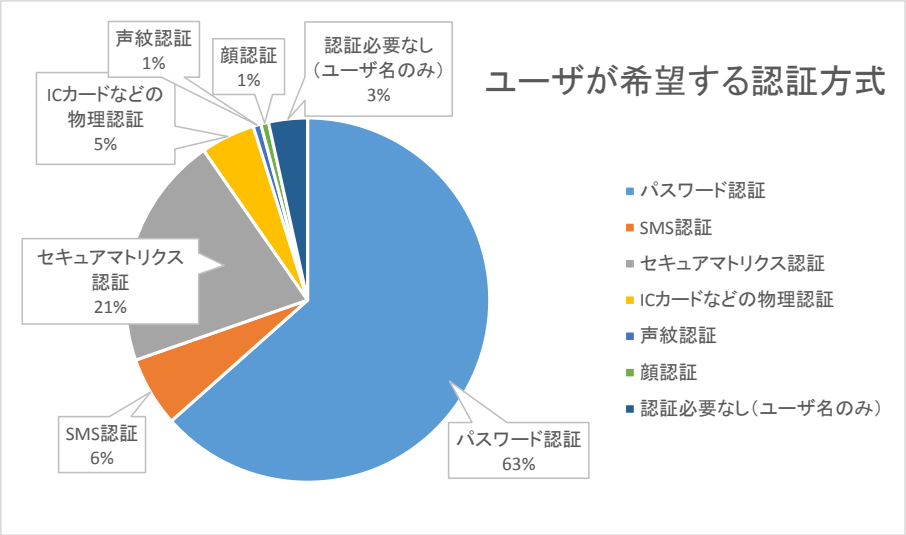


図３　ユーザが希望する認証方式（全ユーザ）

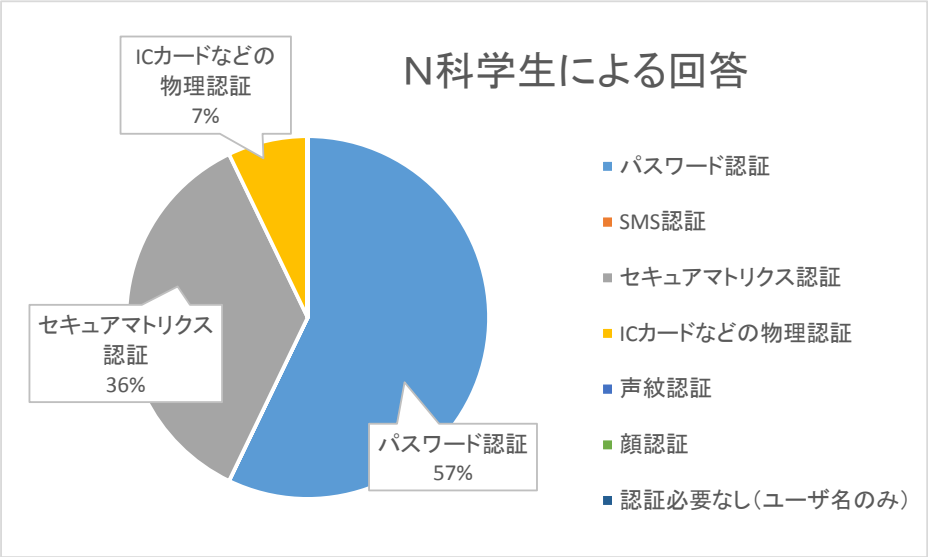


図４　情報ネットワークコミュニケーション学科学生の回答

５．今後の計画

RMS プロジェクトでは，認証方式を複数候補からユーザが選択できる方式を導入予定である．これにより，ユーザがどのような認証方式を望んでいるのかといった傾向を実際に調査することが可能になる．さらに，ユーザが複数の認証方式を選択して自由に組み合わせることが可能な認証システムを検討中であり，これによりさらに認証強度を高めることが可能になる．

６．研究成果の発表

とくになし．