神奈川工科大学

セキュリティ研究センター

研究報告

第 7 巻

2018 年度

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

世界は今，サイバー空間とフィジカル空間を高度に融合させることにより，人々に様々な高度でかつきめ細かなサービスを提供可能にする「Society 5.0」へシフトしている．例えば，工場や農業といったフィジカル空間上に設置されたセンサなどの IoT デバイスによって種々のデータが観測・収集され，ネットワークを介してサイバー空間上のクラウドに集められて AI により分析・予測され新しいサービスがどんどん登場している． 一方で，個人情報をはじめとした生活に関わるあらゆる情報がネットワーク上に流通して計算機上で管理・処理されるようになり，機密情報や個人情報などを目的としたサイバー攻撃もその手口が多様化・高度化している．

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 30 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」,「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」を実施した．そこで，環境適応型モバイル端末認証手法に関する研究，サーバアプリケーションのセキュリティ強化方式の研究開発，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，不可視画像処理を利用した認証手法の検討などを進め，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，組織内の情報セキュリティシステムの構築モデル研究においては，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，技術普及段階の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，さらなる高度化と汎用化を図ることについて検討した．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	安全性と利便性を考慮した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	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
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	情報ハイディング技術に関する研究
岡本　学	情報ネットワーク・コミュニケーション学科・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・教授	サーバアプリケーションのセキュリティ強化に関する研究
西村　広光	情報メディア学科・教授	不可視画像処理を利用した認証技術の研究
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	使いやすさと安全性を両立する認証方式に関する研究
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
佐藤　史緒	教職教育センター	セキュリティと教育に関する調査研究

目次

基礎・教養教育センター　三浦直子

環境適応型モバイル端末認証手法に関する研究

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，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として,モバイル端末とサーバの安全性の高い相互認証手法について検討する．特に,モバイル端末が無線 LAN を利用してサーバに接続する際の中間者攻撃による不正アクセス防止対策として,サーバでカメラという視覚的なチャンネルを用いてデバイスを認証できる新たな認証方式の研究開発を目指す.

そこで，今年度の研究では，スマートフォンやタブレットのようなモバイル端末とカメラが備え付けられた PC サーバを想定し,カメラに映る範囲内に存在するデバイスのみが認証されるセキュアデバイスペアリング方式を提案し,その有効性について検討することを目的とする.

2.　研究の必要性及び従来の研究

近年，Wi-Fi，Bluetooth や NFC(Near-Field-Communication)などの無線技術の進歩により，スマートフォン，タブレット，IoT 機器などのデバイスが相互に通信する機会が多くなっている．特に，最近ではモバイル端末の GPS 情報と無線 LAN のアクセスポイント情報によるコンテンツの配布が注目されており，端末の近接情報に基づきクーポンの配布などが行われる．しかし，このような無線を用いた近接検出技術は精密に空間を区切ることはできないため，第三者による通信の盗聴や中間者攻撃などの問題が考えられる．例えば，会議中にプレゼンターが参加者に無線で資料を配布するシーンを想定した場合，部屋外にいる盗聴者も会議資料を受け取ることができる問題がある.

本研究では，以上のような無線通信によるコンテンツの配布を行う前にセキュアな無線通信を確立するためのデバイス同士で鍵を共有するプロセスを，セキュアなデバイスペアリングと定義する.

通常，モバイル端末同士もしくは機器同士のペアリングを行う一つの方法として，キーとなる情報やパスワードをデバイスに手動で入力することにより相互認証を行う方法がある．しかし，これからの機器同士のペアリングを行う機会が多くなれば，逐一手動で相互認証を行うことは手間のかかる作業となる．よって，即時的で手軽であり，加えて空間的に精密に分けることができるペアリング手法が必要となる.

関連研究として，距離画像を取得できる赤外線カメラを備え付けたサーバと加速度センサを備え付けられたデバイスをペアリングする方式が研究されている．カメラを備え付けたサーバでデバイスを持っている人の手の動きを検出し，端末側で端末自体の加速度デー

タを取得する．その加速度をサーバに無線で送信し，手の動きのデータと加速度データを比較することでペアリングを行う手法である．この手法を用いると部屋単位やパーテーション区切りでペアリング可能空間を分けることが可能となる．しかし，カメラで取得した手の動きから端末の傾きを認識することは困難であるため，カメラの範囲外にいる盗聴者が正規の端末と同じ動きを行えば，盗聴者が不正にペアリングを行える問題が考えられる．また，広範囲を認識できる赤外線カメラは一般的に普及しておらず導入する際のコストを考えると実用的とは言えない．

3. 期待される効果

従来のような特殊なカメラを必要とせず，安価な通常の機器を用いることにより，増加するペアリング機器のコストを削減できると考えられる．また，ペアリング機器同士を高精度に認識できる手法を実現することでより安全な端末認証を行うことができると期待される．

4. 研究の経過及び結果

現在まで，本研究では特殊なカメラを用いず，通常のカメラを備え付けた PC と加速度センサを備え付けたモバイル端末を安全にペアリングする手法を提案し，その評価実験を行なった．以下に本研究の提案方式についての説明と実験結果を報告する．

4.1 カメラと加速度センサを用いたデバイスペアリング方式の提案

通常のカメラを搭載したサーバーと，加速度センサを搭載したモバイル端末をペアリングする手法を紹介する．この手法を用いればユーザがモバイル端末をカメラに向けて振るだけでペアリングを行うことができる．この手法の特徴は，マーカーと呼ぶカメラが認識しやすい画像の動きでデバイスの動きを代替することで，デバイスの認証精度を高めている点である．

図１に本提案方式におけるペアリング手順について示す．まず，デバイス側でマーカーをモバイル端末画面上に表示する．次にユーザはモバイル端末を動かし，端末で取得される加速度情報をサーバーに無線で送信する．この時，モバイル端末の画面上に表示されるマーカーの種類が一定時間ごとに変化する．同時に，サーバ側のカメラではマーカーの種類と動きを取得し，カメラ画像上での端末の変位情報を取得する．その後に，変位情報を微分，加速度情報を積分して速度情報に変換する．最後に，カメラが読み取ったマーカーの種類の列とデバイスから送信されたマーカーの種類の列の類似度と，変換された二つの速度情報の類似度を算出し，一定の閾値以上の値を得ることができればペアリング完了である．

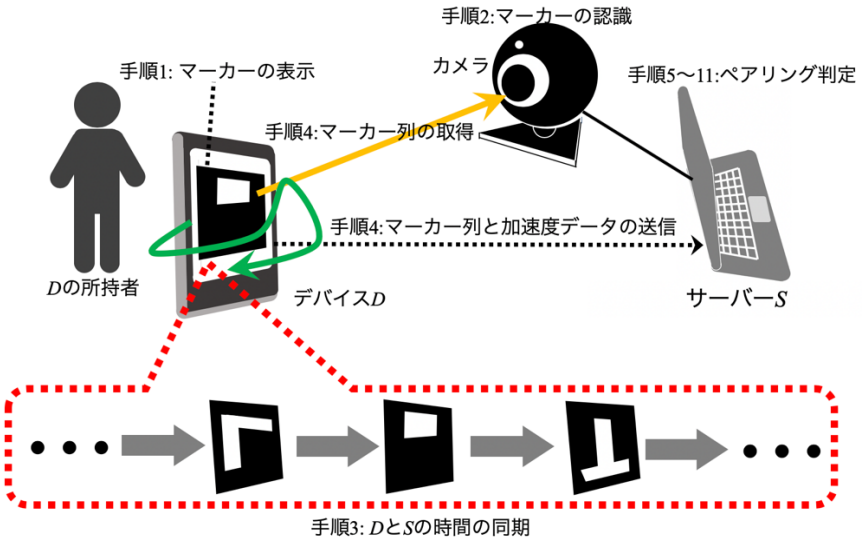


図１．提案手法のペアリング手順

4.2 実験結果

提案手法の有用性を確かめるために，マーカーの種類を一種類のみに限定した提案手法において，サーバ側を MacBookPro 15inch，デバイス側を Nexus 5X として実装し，速度データの類似度を確認する実験と，カメラの範囲外から正規のユーザになりすましてペアリングを行うことができるかどうかという 2 つの評価実験を行なった．類似度の確認実験の結果として，カメラとデバイスの距離と，デバイスのモーションによって類似度が大きく変化しないことが確認できた．また，なりすましの実験の結果として，相関係数を用いて類似度算出を行えば，他の類似度算出方法を使ったときよりもペアリングの成功率が一番高いことが確認できた．また，類似度の平均を見ると，なりすまし者の平均類似度より正規ユーザの平均類似度の方が大きくなることがわかり，ペアリングを行う際の閾値を設定できることがわかった．しかし，類似度の標準偏差が大きくなってしまったため，安定したペアリングができないこともわかった．

次に提案手法において，デバイスを動かす際マーカーの種類が変化するようにしたとき，前述した実験と同様にマーカー列の類似度と速度データの類似度を確認する実験と，カメラに映る範囲外のなりすまし者がペアリングを行うことができるかという実験を行なった．加えて，3 人同時にペアリングを行えるかどうかの実験を行なった．類似度の算出方法としては，前述した実験により相関係数のみを算出した．類似度の確認実験の結果として，マーカーの類似度は高い値を算出でき，速度の類似度は前述した実験より高い値を確認できた．なりすましの実験では，マーカーの類似度と速度の類似度両方において平均的に見れば正規のユーザとなりすまし者を分けることができた．同時にペアリングを行う実験の結果として，約 70%で 3 つのマーカーの変位データからそれぞれの変異データに分けることが確認できた．しかし，速度データの類似度の平均が 1 台の

み用いた実験のときの平均類似度より小さくなった.

5. 今後の計画

今回の実験では，速度データの類似度に関して，ばらつき(標準偏差)が大きくなり安定したペアリングができないことがわかった.この理由の一つとしてカメラの解像度が低いことが挙げられる.今後は提案手法の実用化を目指すため，解像度の高い外付けのカメラを使い，これまで行なった実験の再実験を行う予定である.また，さらに速度データの類似度のばらつきを減らすための方式を提案する.加えて，今後即時性や安全性を有するアドホックな機器同士のペアリング手法の研究と実験実証を行っていく予定である.さらに，これらの研究成果と実験結果をまとめて情報処理学会論文誌に投稿できるよう，執筆を行う予定である.

6. 研究成果の発表

(1) 論文

[1] Makoto Nagatomo, Kentaro Aburada, Naonobu Okazaki and Mirang Park, “An Examination of Pairing Method with Camera and Acceleration Sensor,” The 11th International Conference on Mobile Computing and Ubiquitous Networking(ICMU2018), 4 pages,2018.

[2] Makoto Nagatomo, Kentaro Aburada, Naonobu Okazaki and Mirang Park, “Proposal and Evaluation of Secure Device Pairing Method with Camera and Accelerometer,” The 6th International Symosium on Computing and Networking(CANDAR), pp. 310-315, Nov. 2018.

[3] H. Yamaba, S. Usuzaki, K. Aburada, M.Mukunoki, M. Park, N. Okazaki, ″A proposal of new reading text CAPTCHA using random dot patterns,″ Proceedings of 2018 Sixth International Symposium on Computing and Networking (CANDAR2018), 5B-3, pp.1-6, Nov. 2018.

[4] K. Sakamoto, M. Nagatomo, N. Okazaki, and M. Park, ″Examination of personal authentication method achieving shoulder-surfing resistance by combining mouse operation and number matrix,″ IEICE ComEX, Vol.8, No.3, pp.61-66, 2019.

(2) 学会発表

[1] 長友 誠, 油田 健太郎, 岡崎 直宣, 朴 美娘,″カメラと加速度センサを用いたデバイスペアリング方式の提案とその評価,″ マルチメディア，分散，協調とモバイルシンポジウム (DICOMO2018) 論文集，pp.172-178，2018.

[2] 坂本 憲理、長友 誠、岡崎 直宣、朴 美娘,“覗き見耐性を持つマウス操作と数字盤を組み合わせた個人認証方式の提案と評価,” コンピュータセキュリティシンポジウム

（CSS2018）論文集， pp.165-172, Oct. 2018.

[3] 渡辺 一樹、長友 誠、油田 健太郎、岡崎 直宣、朴 美娘,“スマートフォンとウェアラブル端末の加速度センサを用いたスマートロックにおける歩行認証,” コンピュータセキュリティシンポジウム（CSS2018）論文集， pp.173-178, Oct. 2018.

[4] 長友 誠、渡辺 一樹、油田 健太郎、朴 美娘、岡崎 直宣、 ″覗き見耐性を持つ小型タッチスクリーン端末における個人認証方式の提案,″ 2019 Symposium on Cryptography and Information Security(SCIS2019), 3E4-2, 2019.01

(3) 特許

[1] 特願 2014-046134 「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 2015-165962 「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

[3] 特願 2015-183574 「個人認証用プログラム 」
発明者：岡崎 美蘭
出願者：学校法人 幾徳学園

[4] 特願 2018-036579 「加速度センサを搭載したモバイル端末を正規の通信相手として認証する方法および認証装置」
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

[2] 平成 29 年～平成 31 年度 文部科学省科学研究費補助金 基盤（C）
「安全な IoT サービスを実現するためのセキュリティ技術に関する研究」
研究代表者：岡崎 美蘭

サーバアプリケーションのセキュリティ強化

研究者名：情報学部　情報ネットワーク・コミュニケーション学科　岡本　剛

１．研究の目的

本研究は、既存のサーバアプリケーションに手を加えずに、脆弱性に対するサイバー攻撃からサーバアプリケーションを保護するセキュリティモジュールを開発する。一般に、未知の脆弱性に対する攻撃を予測することが困難であり、最初の攻撃を検知することが難しい現状を踏まえて、免疫的なアプローチ（最初の攻撃は防止できないが、2 回目以降の攻撃は検知・防止できる仕組み）により、適応的に攻撃を検知する仕組みを開発することがメインテーマである。適応的に攻撃を検知する仕組みであるので、事前に大量の学習データを必要としない利点がある。平成 30 年度は、これまで設計・実装してきた技術を、世界で広く利用されているサーバアプリケーションに適用して、その実用性を評価することが目的である。

また、上述の研究と並行して、サーバの可用性を向上するレジリエントサーバシステムを開発することも本研究に含まれる。レジリエントサーバシステムは、サーバ OS やサーバアプリケーションの実装の多様性により、サイバー攻撃を緩和するシステムである。従来の同一構成（多様性のない構成）の冗長化システムと比べた有効性を示すため、これまで開発してきたレジリエントサーバシステムを多角的に評価することが目的である。

２．研究の必要性及び従来の研究

脆弱性に対するサイバー攻撃からサーバを保護するセキュリティ技術には、主に、パターンマッチング検知、ヒューリスティック検知、機械学習による検知がある。これらの技術は、水際対策であり、検知をすり抜けた攻撃による被害（サービス不能など）からサーバを回復させることはできない。サーバの回復には、サーバ管理者の対応が必要であり、数分から数時間のダウンタイムが発生する。人手を介さずに、迅速にサービスを回復させる技術が求められている。

従来の手法で課題を解決することが難しいとき、ニューラルネットワークのように、生物学的な知見が課題解決のブレークスルーとなることがある。本研究では、サーバのレジリエンスを強化するために、免疫系の戦略を参考にする。脊椎動物の免疫系は、自然免疫系と獲得免疫系から構成され、病原体が自然免疫系をすり抜けても、獲得免疫系が適応的に検知・防止する。セキュリティ技術では、水際対策の技術が自然免疫系に対応するが、獲得免疫系に対応する技術がない。そこで、自然免疫系と獲得免疫系が果たす機能をサーバに組み込むことにより、未知の脆弱性に対する攻撃が従来の水際対策をすり抜けたとしても、攻撃によ

る被害から攻撃を検知して、その攻撃を学習することにより、攻撃に対するレジリエンス（回復力）を強化できる。

３．期待される効果

既存のサーバアプリケーションに手を加えずに、サイバー攻撃に対するサーバアプリケーションを保護できる。特に、未知のサイバー攻撃に対して、セキュリティパッチが提供されていないが、サービスを継続しなければならない状況において、適応的にサイバー攻撃を学習して、検知・防止できることが本技術の強みである。この強みは、セキュリティ強化のみならず、人手を要さないという点において、サーバの管理・運用にかかるコストの削減を期待できる。

また、本研究と並行して開発するレジリエントサーバシステムも、人手を介さずに、サーバの可用性を向上させることができる。レジリエントサーバシステムは、ハードウェアの冗長化も含むため、故障など偶発的な障害にも強い。

４．研究の経過及び結果

本研究では、これまで、オリジナルのウェブサーバアプリケーションに特化したセキュリティモジュールを実装してきたが、平成 30 年度は、セキュリティモジュールの汎用性と実用性を評価するため、世界で広く利用されているサーバアプリケーションの 1 つとして、DNS サーバの実装である ISC BIND9 を選び、このサーバアプリケーションのセキュリティモジュールを実装した。

これまでの研究で、試作モジュールは、入力データのファジーハッシュ化が原因で特定の攻撃を誤検知しやすいことがわかっていた。そこで、ファジーハッシュ化を行わない仕様に変更にすることによって、10%程度の検出精度を改善できた。実用性を評価するため、実在する脆弱性（CVE-2015-5477 と CVE-2016-2776）とそれに対する攻撃を行って検出精度とオーバーヘッドを評価した。その結果、過去最高の検出精度（97%）を得られた。モジュールのオーバーヘッドは 11%であった。

サーバの可用性を向上させる研究では、これまで開発してきたレジリエントサーバシステムに対して、様々な評価尺度により性能評価を行い、従来の同一構成の冗長化システムより、多様性のあるレジリエントサーバシステムの方がサイバー攻撃に対して頑健であることを確認した。

５． 今後の計画

実用化において、セキュリティモジュールのオーバーヘッドが無視できない大きさであると考えられるので、オーバーヘッドの削減を試みる。削減するアプローチとして、

機械学習アルゴリズムの変更と GPU による機械学習の高速化を予定している。

想定より早い段階でオーバーヘッドを削減できたら、他のサービスに展開することを検討する。現在、IoT 機器のセキュリティが問題になっているため、IoT 機器を対象にしたサービスのセキュリティモジュールを開発する。

６. 研究成果の発表

1. Winarno, Idris, Yoshiteru Ishida, Takeshi Okamoto, “A Performance Evaluation of Resilient Server with a Self-Repair Network Model,” Mobile Networks and Applications (ACM/SIGMOBILE), DOI:10.1007/s11036-018-1103-2, 2018. （査読有）

2. Takeshi Okamoto, Mitsunobu Tarao, “An artificial immunity-enhancing module for internet servers against cyberattacks,” Artificial Life and Robotics, Vol. 23, No. 3, pp. 292-297,2018. （査読有）

3. Takeshi Okamoto, Mitsunobu Tarao, “Implementation and evaluation of an immunity-enhancing module for ISC BIND9,” Proc. of the 22th International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, Procedia Computer Science, Vol. 126, No. 2018, pp. 1405-1414, 2018. （査読有）

安全・安心な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構築技術に関する研究
～不可視画像処理を利用した認証技術の研究～

情報メディア学科　　西村　広光

１．研究の目的

高度なセキュリティ技術構築に向けて、不可視画像処理を利用した認証技術の研究を進めてきている。具体的に 2 つの新しい技術構築に向け、検討・実験・実証をこれまでに進め、更なる応用技術についての検討を進めていく。

一つ目の技術は、赤外線を利用したカードを利用した個人認証技術における新しい技術開発である。カード形状の所有物認証は、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これまでに開発し、特許出願や学会発表をおこなってきた。

もう一つの技術は、金属鍵のセキュリティを高める新技術の開発である。高精度な監視カメラがどこにでも設置されるようになり、画像からの 3 次元形状推定技術の精度が非常に高くなってきている。このままでは、非常に近い将来、複雑な形状の金属鍵であっても、カメラ映像から 3 次元形状推定を行い、3 次元プリンタで出力することで金属鍵の複製が極めて容易になってしまう可能性が高い。しかし、従来から利用している金属鍵の利用を社会が辞めることは難しい。そこで本研究では、高精細な映像取得が可能な紫外線画像処理を利用して、金属鍵の表面の微細な傷画像を取得し、形状が同じくシリンダ鍵として開錠できる鍵であっても、あらかじめ登録した鍵とそれいがいを識別する技術の開発を進め，基礎技術を確立してきた。

これら技術を認証に利用する基礎技術はこれまでに確立し、公開してきた。今年度は考案技術をさらに幅広く応用していくことに関して検討を深めることとした。

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。

本研究のカード認証技術は、心的負担の少ない「意図的なバイオメトリクス情報」の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、30cm 程度の極近距離でしか認証ができない課題が残っていた。この課題を克服すれば、通路に設置した監視カメラ程度の撮影距離で提案技術を利用することができ、一般的なセキュリティーゲートなどで幅広く利用可能とできる。

金属鍵の複製に堅牢な認証方式の実現は、今後の社会に不可欠な技術といえる。これまでに、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捉えることができることを確認し、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。この技術は未だ類似技術として報告例がない技術である。この技術をシリンダ鍵内部に埋め込むことができるかの技術検討を行うこと、摩耗劣化によって提案技術にどのような影響があるかを調査することは、本技術の実用可能性をはかる上で必要不可欠といえる。

加えて、本研究で確立させてきた可視光以外の画像処理によって個体識別を行う偽技術は可視光以外での物体状態分析に応用できる技術として利用できるものであり、確立させてきた技術を幅広く転用させていく意義は大きいと考える。

３．期待される効果

本研究で提案する 2 つの技術は、どちらも将来の高度セキュリティ社会実現に不可欠な技術となる。

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、紫外線による金属表面画像を利用した金属鍵認証技術は、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。

双方の技術に関して、これまでに、基盤認証方式を確立し、実験を通して理想環境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進める。

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、近い将来の社会に不可欠な技術になると考えられ、本技術確立による社会的な効果も極めて大きいといえる。

４．研究の経過及び結果

24 年度にカード認証法の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、考案カード認証法の性能評価のため、50 人の被験者を集め、多様な状況下における評価実験用データベースを構築した。構築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実験で実証した。

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した。加えて、可視光・不可視光の条件検討を深め、従来の近赤外線に加え、紫外線情報を利用する新しい認証方式の可能性を発見した。

27 年度は、カード認証を広く実用化させるための技術である物体移動を高精度にとらえる技術の基礎技術を構築した。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た。

28 年度は、カード認証技術を実用的にするために、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、視野角の広い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、実験により提案技術の有効性を確認した。

29 年度は、カード認証のカード位置推定技術の高精度化、高速化に取り組み、成果を報告した。紫外線による金属鍵認証に関しては、鍵メーカから特殊加工したシリンダ鍵を借用して実験を進め、鍵形状によってはシリンダ挿入状態でも紫外線鍵認証できる可能性を確認した。加えて、鍵の摩耗劣化情報を領して、さらなる高度な紫外線金属鍵認証ができる可能性を確認した。

30 年度は、これまで構築した認証技術がノイズに対して堅牢であるかの検討を行い、実験規模を拡大して実証を進めた。さらに、可視光以外での物体の画像分析技術とし

ての応用を考え、印刷メーカのエラー検出技術への応用や、工事現場での状態分析技術への応用について検討を始め、企業からのデータ提供を頂き分析を進めている。

５．今後の計画

これまでに構築した技術を、実用的な認識システムに落とし込んでいくことが課題の一つである。実験規模をさらに拡大し、高度な認証性能を発揮できる技術であることを示しながら、改良とシステムのダウンサイズ化を進めていく計画である。

さらに、物体の表面分析として応用できる技術の応用シーンを広め、産学共同研究として多くの技術転用を検討していく計画である。

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。

H30 年度

企業からのデータ提供を頂き、分析を進めている段階で、30 年度中の段階では外部公開できない情報が多く外部発表を行っていない。現在、2 つの企業との連携を工学教育研究推進機構の紹介で進めており、今後産学連携を進めながら成果公開を目指していく。

H29 年度

- TBS「未来の起源」平成 29 年 5 月 28 日放送で「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。
- TBS「未来の起源」平成 29 年 7 月 9 日放送で「高精度カード位置検出法の検討」（学生：田中菜実）の研究が紹介された。
- 田中菜実，西村広光
  リアルタイム処理に向けた GA とオプティカルフローを用いた動的な黒いカードの輪郭推定法の検討
  2018 年　電子情報通信学会総合大会
- 流　凌太，西村広光
  「分割画像の連結を利用した紫外線による鍵認証技術の検討」
  2018 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」

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」

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

安全・安心な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構築技術に関する研究（相関利用型情報ハイディング）

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、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。また、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、一昨年度の研究において、周波数変換として DFT、DCT、DWT を用いた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ついて定量的な性能評価を行い、DWT、DCT、DFT の順で必要最小限の強度の値が低いという結果を得た。これにより、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。また、周波数変換として DFT および DCT を用いた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ついても定量的な性能評価を行い、DCT の方が DFT よりも必要最小限の強度の値が低いという結果を得た。これより、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。一方、昨年度の研究において、画質（音質）劣化が人間の感覚によってどのように認識されるのかという点を明らかにするために、被験者を用いた主観的評価を行った。その結果、画質劣化に関しては、DWT が最も認知されやすく、DCT と DFT では違いが明確には認知されにくいという結果を得た。また、音質劣化に関しては、DFT と DCT との違いがあまり認知できないという結果を得た。このように、画質劣化においても音質劣化においても、強度による客観的評価と被験者による主観的評価が大きく異なる結果となった。そこで本年度の研究においては、客観的評価と主観的評価が異なる原因を検証するこ

とを目的とする。この原因はいくつか考えられるが、本研究では透かし入り画像（音楽）における雑音エネルギーに着目し、客観的評価と主観的評価が異なる原因を説明可能であるか検証を行う。

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。一昨年度の研究においては、強度を尺度とした定量的な評価により各種周波数変換間の優劣について検証を行った。また、昨年度の研究においては、被験者による画質（音質）の主観的評価を行った。両者を比較すると、客観的評価と主観的評価では明らかに結果が異なっている。どの周波数変換が最も適したものであるのかを明らかにするためには、この原因について検証を行う必要がある。

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）にとっては雑音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。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）にも依存するため、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が、他の条件を全て同一にした検証により、画像用情報ハイディングについては DWT、DCT、DFT の順で平均的に必要最小限の強度の値が低くなり、音楽用情報ハイディングについては DCT、DFT の順で平均的に必要最小限の強度の値が低くなることが明らかとなっている。一方、必要最小限の強度で情報を埋め込んだ画像（音楽）を被験者によって主観的に評価してもらったところ、画質においては DWT が最も画質劣化が激しく、DCT と DFT では明確な違いが無いという結果を、音質劣化においては DCT と DFT において大きな違いが無いという結果を得た。本研究では、透かし情報を埋め込んだ際の雑音エネルギーに着目することで、両者の結果が異なる原因を明らかにすることを目的としている。これにより、各種周波数変換の優劣を明らかにすることにつながると期待される。

４．研究の経過及び結果

画像用情報ハイディングに関しては、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 8、16、32 の大きさのものを 2 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 2 種類使用した。なお、周波数変換としては DFT、DCT、DWT を使用し、周波数変換の次元は、256 次とした。また、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。全ての周波数変換において、強度を 5、10、15 に固定して透かし情報を埋め込んだ画像を作成し、雑音エネルギー（透かし入り画像と元画像のエネルギーの差）の大きさについて検証を行った。検証の結果、どの強度においても、DFT、DCT、DWT の順に雑音エネルギーが小さいことが明らかとなった。さらに、音楽用情報ハイディングに関しては、再生時間が 3～4 分程度の WAV 形式の音楽を 5 種類、周波数変換の次元を 256、512、1024 次、拡散系列として 64、128、256 の長さのものを 2 種類、埋め込む情報としてランダムに発生させた 768bit の乱数を 2 種類使用した。なお、周波数変換としては DFT および DCT を使用した。また、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。両方の周波数変換において、強度を 1000、2000、3000 に固定して透かし情報を埋め込んだ音楽を作成し、雑音エネルギーの大きさについて検証を行った。検証の結果、どの強度においても、DFT が DCT よりも雑音エネルギーが小さいことが明らかとなった。画像用情報ハイディングにおいても音楽用情報ハイディングにおいても、誤りが発生しない必要最小限の強度が小さくなる周波数変換の優劣と同じ強度において雑音エネルギーが小さくなる周波数変換の優劣とが全く逆になっていることが明らかとなった。この両者の相互作用によって、主観的評価の結果が説明できる可能性が高いと考えられる。

５．今後の計画

今回の検証では、画像および音楽において、埋め込む強度を固定して検証を行った。今後は、誤りが発生しない必要最小限の強度で埋め込んだ場合における雑音エネルギーの大きさについて調査する必要があると考えられる。また、雑音エネルギー以外に主観的評価に影響を与える要素についても検証が必要である。さらに、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ける検証も必要である。

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

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．特にこれら情報システムの構築においては，人工知能（AI）技術や IoT 技術の導入も行われており，より広範囲に渡る情報セキュリティ確保が重要視されている．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情報資産の構成要素となる重要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．H30 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，技術普及段階の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，さらなる高度化と汎用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統合的な見方を導入することで，技術的な要求の視覚化が可能となるよう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

分野毎の技術統合を図ることで，全体のシステム化を目指す場合，一般に，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．これらの実現に向け，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．

多方面にわたる情報通信技術（ICT）の進歩は日進月歩であり，それら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．

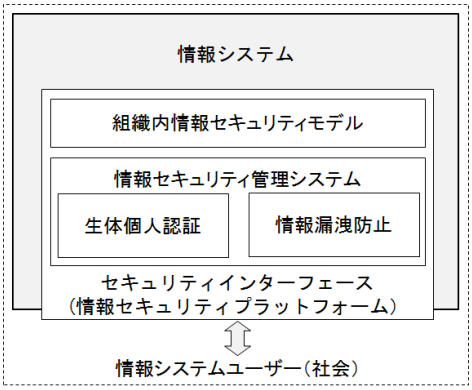


図 1．提案システムイメージ

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：Biometrics Authentication）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

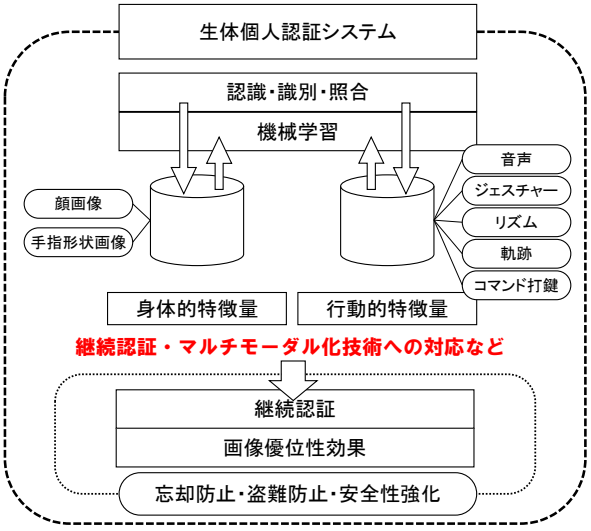


図 2．生体個人認証システムの拡張

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.

４．研究の経過及び結果

H29 年度の取り組みにおいては，重要なデータが蓄積されるサーバ操作に着目し，管理者のパスワードが奪取された場合を想定し，キーボード操作者の打鍵情報をリアルタイムに分析することで，“なりすまし”発見につながる本人認証手法を開発・提案した．正規ユーザとしての登録者に限定した判別において，最大 85%程度の認証精度の実現を達成することができた.

これを踏まえて，H30 年度の研究結果では，前年度の提案手法の拡張を目的として，特徴量判定のパラメータ調整を施すことにより登録者以外の判別を行う新たな手法開発と提案を行った．また実験によりパラメータ調整の有効性を明らかにした．登録者以外の判別においても平均 82%以上の認証精度の実現を達成することができた．このことにより，サーバ操作中の継続的な認証可能性が示唆されるとともに，バイオメトリクス認証のマルチモーダル化と継続認証の実現にさらに近づくことが期待される.

なお，これまでの研究では，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てきた．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．H29 年度まで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，H28 年度に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傾向が認められたが，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.

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，これまで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手段の導入と試行をさらに発展させ，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が，従前通り示唆された．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継続的に調査し，知見をさらに増やしていく必要がある．

５．今後の計画

開発技術の普及段階を意識すると共に，従来の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」等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サーバ操作時の「打鍵情報に基づく継続認証」の５つの検討項目を発展・高度化し，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．さらに生体個人認証における複数要素を用いたマルチモーダル認証方式と共に，システム使用中の継続的な認証方式の高度化により，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・考察を行っていく．

全体システム設計としては，平成 30 年度までに洗い出した問題点を補完する方策を提示して，情報セキュリティモデルの高度化を行なう．さらに，情報セキュリティモデルに基づいた情報セキュリティ管理システムの構成を検討する．

本研究を進めるための方略として，これまでに掲げたことは，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点に着目することであった．特に，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いるが，現時点では，初期検討にとどまっており，導入まで至っていない．今後は本格的な導入を図りたい．

６．研究成果の発表

[1] 滝本将司*, 納富一宏 : "継続的打鍵情報を用いたサーバ操作中のなりすまし検出", 情報処理学会 第 81 回全国大会講演論文集 第 3 分冊, 5ZA-07, pp.465-466, (2019.03) **[学生奨励賞]**.

[2] 滝本将司*, 納富一宏 : "継続的個人認証を用いたサーバ操作中の不正侵入検出手法", バイオメディカル・ファジィ・システム学会 第 31 回年次大会講演論文集, pp.53-56, (2018.11).

（* : 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

情報セキュリティにおける情報漏えい問題は，情報の所有者ではない第三者が勝手に情報にアクセスすることで始まる．これら不正を防止するには，各種情報において，その情報が誰の所有であり誰のアクセスを許すかを決め，さらには決められたユーザ以外はアクセスできなくすることが重要である．特に近年ではサーバ側に情報を保存するクラウド方式がとられているため，これらクラウド上情報群へのアクセス制御が大きな課題となってきている．

アクセス制御において最も重要な技術は認証技術である．認証とはアクセス権があるユーザかどうかを確認する技術であり，現状では認証方式としてパスワード方式が用いられる場合が多いが，パスワード方式には盗聴や推測など問題点も多いため，今後はパスワード方式以外の様々な認証方式の取り揃えが必要となる．

当然ながら安全性を高めるためには「強い認証」を実現することが重要となるが，一方で認証の安全性を高めるとユーザ側の準備や操作が煩雑になる課題がある．例えば指紋認証を導入すれば安全性は高まるが，指紋読み取り装置の準備やユーザの登録作業が必要となる．また複数の認証方式を用いて安全性を高める方式もあり，例えば複数のパスワードを要求する形にすれば安全性は当然上がるが，ユーザは複数のパスワードを記憶し，かつそれを毎回入力する必要があり，面倒で時間がかかる．一方ですべての情報に高度な認証が必要かというとそうではない．クレジットカード番号などの機密性が高い情報については多少のユーザ負担があっても高い安全性を保つべきだが，機密性が低い情報については簡単な認証でかまわない．そこでアクセスするコンテンツ毎に異なるアクセス要件を設けて，「強い認証」から「簡単な認証」まで様々な認証方式を取りそろえる必要がある． さらに言えば，最近利用が一般的になった SNS を用いたりすることでユーザに使いやすい認証方式も選択肢に入れていく必要がある．

２．研究の必要性及び従来の研究

「強い認証」の方式はこれまでも様々提案されている．これまでは PKI を用いた証明書認証方式や，所有物認証である IC カード認証，顔や指紋を用いた生体認証などが提案され利用されている．しかしこれら従来技術には課題もある．生体認証には読取装置の配備が必要であり費用もかかる．所有物認証も同様で物理的な IC カードを用いるならそれらカードの購入・配布の費用がかかる．証明書等，電子的な所有物で認証を行う場合，それらは主に認証行為にしか用いないため，結局は端末が限定されたり日常の所持が不便だったり

する場合がある．そこでSNS等，普段日常的に別の要件に頻繁に用いているものを使用して認証を実行させることでユーザにとっても利便性の高い方式を実現できる．ただしSNSは元々はある種オープン性のあるサービスであるため，安全に認証行為に利用するには注意が必要である．よってSNSを用いながら，複数の他のユーザの許可を必要とする方式をとることで安全性を高める提案を行う．ICカード認証や指紋認証はユーザ自身がそれを実施すれば認証が完了する「自己完結型」であった．一方提案方式では，第三者の許可を必要とすることで安全性を高める「第三者介在型」をとることでSNSを利用しても高い安全性にて認証が実現できる．

３．期待される効果

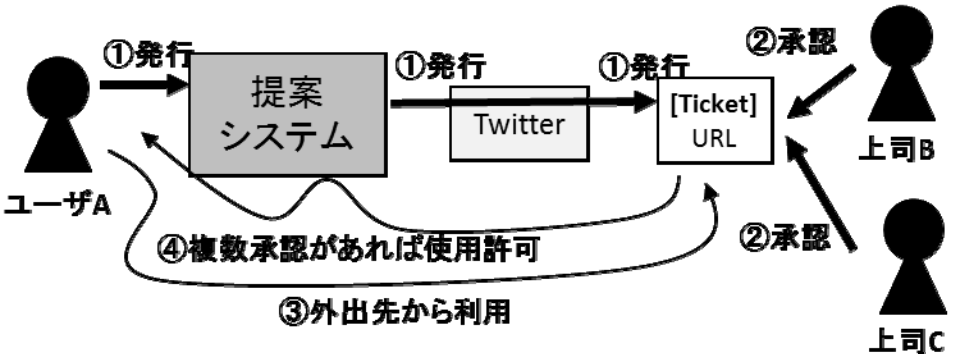
SNSを用いることでユーザには利便性の高い認証方式を提供できる一方で，システム提供側としては無料でSNSのシステムを利用できるためコスト削減が可能になる．例えば代表的なSNSであるTwitterを利用すれば，ユーザは無料で利用できるし，普段よくTwitterを使うユーザであれば親和性も高い．一方で，システム側もユーザ認証の一部にTwitterを利用すればTwitterのセキュリティ機能（https や鍵アカウント）を利用できる一方で，無料で利用できるので開発費用を大幅に削減できる．

４．研究の経過及び結果

本研究では「Twitter チケット認証」方式の研究を行った． SNS として広く普及しているミニブログサービス「Twitter」を用い，複数人による「強い認証」方式を実現した．以下に提案方式を説明する．

ユーザ A は会社のシステムを普段は会社の中で利用しているが，出張先でも同様に利用したいと考えている．しかしシステム側としては会社の中からのアクセスであれば通常のID・パスワードによる認証でかまわないが，出張先からのアクセスの場合はなりすましが懸念されるためそれ以上の高いセキュリティを要求したい．そこで本提案方式ではユーザAが出張にあたり社内にいるときにシステムにログインして出張先で使えるように事前に「Twitterチケットの発行」を行う．ここでユーザAはチケットに対応した一時パスワードを決めておく．チケットはユーザ A の Twitter アカウントにつぶやきとして送信される．つぶやき内容はシステムへの接続URLとなっている．次に複数の上司B，Cに対してチケット承認をもらう．ユーザAは上司B，Cに対し一次パスワードを教え，自身のつぶやきを参照してクリックしてもらいチケット承認の依頼をする．上司B，CはユーザAのTwitterのつぶやき上にある「Twitterチケット」のつぶやきとして書かれているURLをクリックする．するとシステムに接続されそこで一時パスワードを入力するとそのチケットを承認したことになる.ユーザAは複数の上司に承認を受けた上で出張に赴き,出張先では自身のTwitterのつぶやきであるTwitterチケットのURLをクリックしてシステムに出張先から接続する．ここでは普段の ID・パスワードに加えて，Twitter チケット番号と一時パスワードを入力

し，さらにすでにその Twitter チケットが複数の上司に承認されていれば認証が完了しシステムが出張先からでも使えるようになる．



参考図：Twitter チケット認証方式

本研究では提案システムとして XAMPP を用いてプロトタイプ・システムを作成し，利便性を検証した．Twitter は鍵アカウントといってフォローワ以外にはツイート情報を見ることができない機能があり，それを用いればチケットそのものを他人に見られることはないため安全に認証が実現できる．加えてチケットそのものを見られてクリックされたとしても一時パスワードが必要であるため第三者には簡単には利用されない．加えて複数の上司からのチケット承認が必要となるのでその点においても安全性を高めることができる．

５．　今後の計画

今後の課題としては，「強い認証」ばかりでなく，「簡単な認証方式」の取り揃えも検討する．特に「幼児向け認証方式」と題して，ゲームのような感覚でアルファベットを理解しない程度の幼児においても本人確認のための認証が可能な方式の検討を行う．大人にとっては面倒でしかない時間のかかる認証方式ではあるが，幼児であれば単純なゲームでも楽しんで繰り返し実施できるため，例えばインベーダーゲームのようなもので決まった色の敵を順番にやっつけることを秘密情報にして認証を行う方式などが考えられる．

６．　研究成果の発表

昨年度学会誌での論文発表を行ったため今年度は発表を行わなかったが，成果については今後学会等での発表を検討したい．

使いやすさと安全性を両立する認証方式を試行するための装置開発

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を目指し，システムと分離した設計を検討することである．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．これまでに，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わかっている．その一方でユーザが望む認証方式としても,パスワード方式が非常に好まれていることがこれまでの調査でわかってきた．

その要因の一つに，web を介するサービス・システムにおいては，認証のためのデバイス的な制約が多い点が挙げられる．すなわち，バイオメトリクス認証などを実現するための特殊な装置をユーザの手元に準備することができないという根本的な問題を解決せねばならない．そこで本稿では，web を介する必要のない入室認証における，様々な認証方式を試行するための仕組みについて報告する．

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．その一方で，虹彩や静脈の模様を利用したバイオメトリクス認証は簡単に精度よく管理ができる利点がある反面，特別なスキャニング装置を用意しなければならなかったり，直接触れることに対して嫌悪感を示すユーザも存在する．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．そのため，どのような認証方法を採用するべきであるかといった点についての調査も，認証方式の検討には欠かすことはできず，様々な認証方式を試行するための仕組みが必要不可欠である．

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

4.1　ソフトウェア工房におけるこれまでの取り組み

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．

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．2019 年度よりシステムを刷新し，現在は機密情報をサーバ内に保持しなくなったため，認証方式の実験ができなくなっている．

4.2　パスワード変更の状況と認証方式の選択に関する意識調査

2015 年度以降は RMS 利用者のパスワード変更に関する調査を行ってきている．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．

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．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１）．

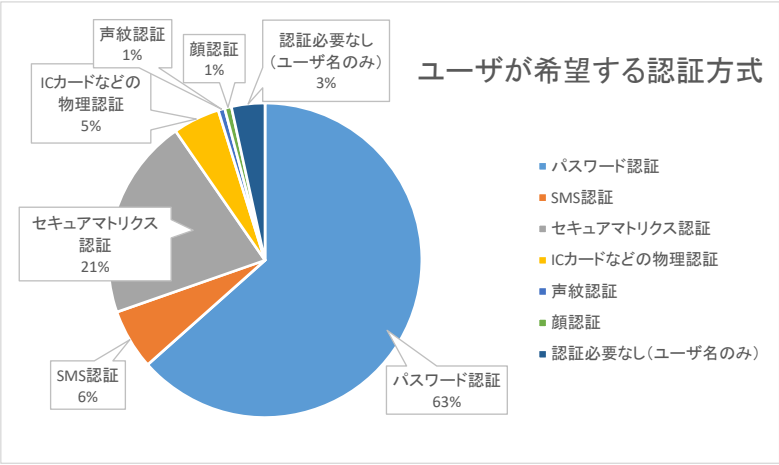


図　１　ユーザが希望する認証方式（全ユーザ）

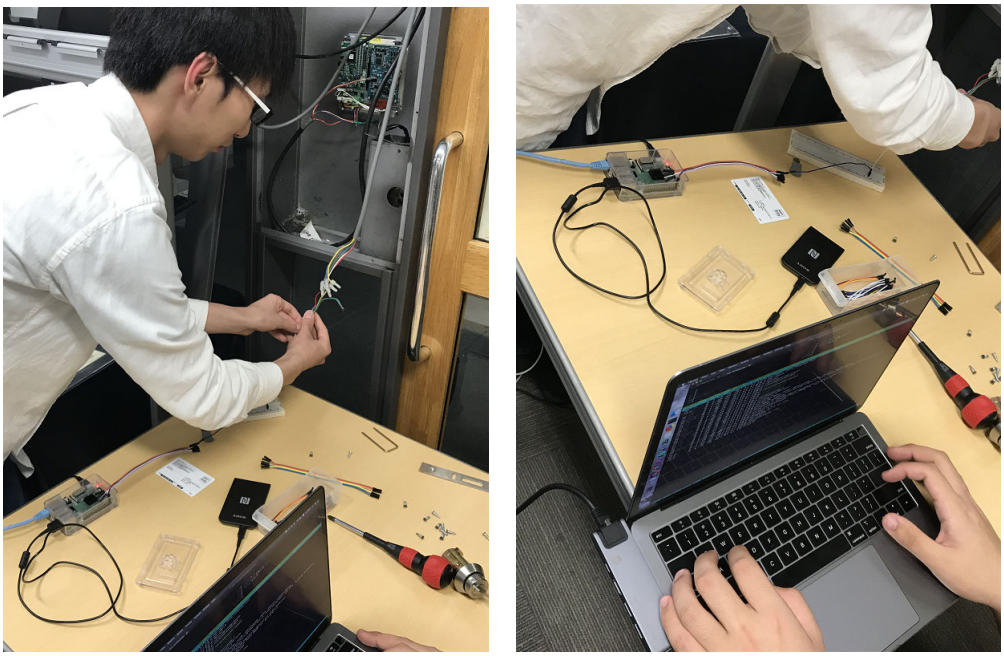


図 2　IC カードリーダーと電動シリンダの制御

4.3　新認証方式の試験運用のための仕組み提案と今後の計画

RMS のログインにおいては，web を介したサービスという前提のため，これまでに多く提案されてきているバイオメトリクス方式や IC カード方式といった認証システムを組み合わせるような実験が事実上不可能であった．そこでソフトウェア工房において新しく学生プロジェクトを立ち上げ，入室管理のための電子錠に対する認証として，新しく提案された様々な認証方式を組み込むことができる装置を開発中である．図 2 は，かつて本学情報学部棟にて運用されていた電子錠システムを，管財課の協力のもと再利用するための実験風景である．Raspberry pi と非接触カードリーダーを組み合わせて電動シリンダを動作しているが，今後は顔認証や様々な新方式を実験するための場として利用可能である．ユーザの利用する端末に依存しない認証の試験運用やデータ取得のための仕組みに留まることなく，オープンキャンパスなどで一般の高校生などに新方式をデモしたり，情報漏洩防止意識を高めてもらうといった副次的な効果も大きく期待できる．

５．研究成果の発表

とくになし．

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高度 ICT プラットフォーム構築に向けた基盤研究
－　セキュリティと教育に関する調査　－

研究者名：教職教育センター　　氏名：佐藤　史緒

１．研究の目的

本研究は、「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」を目的とした研究の一環である。特に次代を担う子どもの情報セキュリティに対する認知と実際のセキュリティ対策行動を検討するために、学校現場においてどのような情報モラル教育が行われているかを把握することを目的として行われた。

ICT の普及とともに学校現場においても積極的な ICT 活用が求められている。2009 年 4 月には「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」が施行され、青少年がインターネットを適切に活用できるような環境を整備することが求められている。2018 年度「青少年のインターネット利用環境実態調査」（内閣府）によると、満 10 歳から満 17 歳までの青少年におけるインターネットの利用状況は 93.2%であり、年々増加傾向にある。特に、高校生においては、99.0%がインターネットを利用しており、主にスマートフォンを使用している（93.4%）。インターネットの利用内容については、高校生はコミュニケーションが最も多く（89.7%）、次いで動画視聴（87.4%）、音楽視聴（80.6%）である。中学生においては、動画視聴（80.9%）、ゲーム（74.1%）、コミュニケーション（68.2%）にインターネットを使用しており、小学生においても、ゲーム（81.5%）、動画視聴（66.1）があげられている。また、勉強・学習・知育アプリやサービスの利用も増えてきている。特に、低年齢層については、学習用タブレットを用いたインターネット利用の割合が高く、学校や自宅での学習において、ICT 教育が用いられていることが背景に考えられる。学習用タブレットの利用は今後さらに増加することが予想される。インターネットの利用時間においても年齢とともに増加傾向にある（平均利用時間 168.5 分）。この状況により、青少年におけるインターネットの利用は日常生活の中で不可欠になっており、早期から情報社会に関する知識やマナーを習得することが必要であると考えられる。

学習指導要領（中学校学習指導要領解説, H29 年告示）において、「情報モラル」は、「情報社会で適正な活動を行うための基となる考え方と態度」とされており、各教科指導の中で身につけさせることをめざしてカリキュラムが組まれている。また、2009 年より「教育の情報化に関する手引」作成検討会（文部科学省）において、「第 5 章　学校における情報モラル教育と家庭・地域との連携」として、情報モラル教育の必要性や具体的な指導について明記されている。情報モラル教育は学校を挙げて体型的に取り組む活動のひとつであり、発達段階に合わせた具体的な指導の必要性について示されている。

青少年のインターネットに関する啓発や学習の経験については、学校種が上がるほど割合が高くなっており、その主な機会は学校においてである（97.6%）（「青少年のインターネット利用環境実態調査」（内閣府））。では、実際に学校現場ではどのような情報モラル教育が行われているのか。まず、情報モラル教育を行う教員が、情報社会の特性を理解し、子どもたちに実践を意識した指導をする必要がある。そこで、学校における情報モラル教育の現状を把握することを目的として、情報モラルを扱っている教科書の内容について検討した。

２．研究の必要性及び従来の研究

本研究課題は、情報に関する知識の乏しい者にも利用可能な、高度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である。そこに、理工系研究者の視点による情報工学の技術だけでなく、社会システム全体から情報セキュリティを俯瞰的に捉えようとする人文社会系の視点を取り入れることにより、より社会的要求に基づいた提案をすることが可能となる。これまでの大学生や一般社会人に対する研究において、情報セキュリティ対策行動は、セキュリティに対する意識や知識だけでなく、利用者の社会的環境や所属する組織・集団によっても異なることが明らかにされた。そこに、子どものセキュリティに対する意識も加えることにより、より幅広いインターネット利用者を対象としたセキュリティ技術の提案が可能になる。

３．期待される効果

現在のインターネットの利用状況を考慮し、早期に情報セキュリティに対するリスク等を理解することによって、セキュリティ対策行動に対する意識を高める可能性が考えられる。そこで、学校現場における情報モラル教育の課題を、情報セキュリティモデルに反映させることにより、より現実場面に即した ICT プラットフォーム構築の提案が可能になると考えられる。

４．研究の経過及び結果

学校種ごとに、情報モラル教育を扱っている教科の教科書を用いて、情報セキュリティに関してどのような内容の呈示をしているかを検討した。なお、情報モラル教育の中でも、本研究課題で対象としている「情報セキュリティ」に関連した内容に着目した報告を行う。

小学校では、主に「道徳」（日本文教出版）と「社会」（東京書籍）の中で情報モラルを扱っている。小学校 1・2 年生の道徳の教科書には、「パソコンやインターネットをつかってさらにがくしゅうをふかめましょう」という ICT 機器の活用についての呈示はあるが、実際にはその使い方等についての説明はみられなかった。また、小学校 3・4 年生では、情報モラルを扱った内容としてパソコンやメールを用いたストーリーであるが、そこで児童が考える学習内容は、約束を守ることや学級意識についてであり、実際には

情報セキュリティ意識を高めるような内容ではなかった。小学校 5 年生では、携帯メールについて取り上げており、インターネットを利用したコミュニケーションに関するトラブルについて学習する内容になっていた。6 年生になると、さらに携帯電話の利用の仕方について考える内容であり、児童が情報モラル理解度を確かめる「情報モラルチェックシート」が呈示されていた（例：日本文教出版「小学道徳　生きる力」）。また、小学校 5 年生の「社会」の中では、情報化社会の特性を理解する単元があるが、インターネット利用における問題については、2/42 ページ程度の扱いであった。小学生のインターネット利用状況は、増加傾向（2017 年度 65.4%、2018 年度 85.6%）にあることから、小学校において教科書のみでは情報セキュリティについての知識は十分に扱うことができていない可能性が高く、補助教材の使用や、教員の工夫が必要であることが考えられる。

中学校においては、情報分野の学習は、主に「技術」科目での扱いである（教科書：東京書籍、教育図書、開隆堂）。小学校の内容に加えて、ネットワークのしくみやパソコン技術の紹介が主であり、図や絵、写真を用いて大変わかりやすく説明されていた。「情報セキュリティ」の内容は、言葉の説明がほとんどであり、調べる課題等も少なく、「覚えるモラル教育」になってしまっている可能性が考えられる。日常生活の中でとるべき具体的な対策について、特に中学生の利用内容を意識したトラブルを授業の中で扱う等が必要である。また、スマートフォンの利用が多くなっていることを踏まえると、スマートフォンにおけるセキュリティ対策や SNS によるコミュニケーションのトラブル等については教科書での扱いがほとんどみられなかったため、授業の中で現実のトラブルを知る機会を設ける等、情報セキュリティの必要性を意識させる工夫が求められる。

高校においては、「情報」科目が設けられており（教科書：東京書籍、実教出版、開隆堂、教研出版、日本文教出版、第一学習社）、情報の活用や ICT と仕事の関係、また情報社会における法律等、幅広く学習できる内容であった。特に、「情報セキュリティ」については、「調べ学習課題」や「確認問題」の呈示が多く、知識の習得だけでなく、具体的にどのように対策をするべきかを生徒自身が考える内容になっていた。情報セキュリティを高める方法の理解だけでなく、利用者として意識を向上させる工夫がみられた。

これらの情報モラル教育を扱っている教科書の内容から、特に小学生や中学生の授業においては、教科書のみでは具体的な対策行動には繋がらない可能性が示唆された。また教員の工夫が求められ、補助教材等の利用や新聞記事等による実際のトラブルの呈示も必要であると考えられる。例えば、文部科学省が選定する情報モラルについての視覚教材も作成されている。それらの内容と教科書の内容によって、子どもたちがどの程度情報モラルの知識を習得でき、実際のセキュリティ対策行動に繋げることが可能なのかどうかについて、さらに検討を進めてく必要がある。

５．今後の計画

実際に子どもたちがどの程度情報モラルの知識を習得しているのかを検討していく必要がある。現在使用されている教科書による情報モラル教育の実態は把握できたが、学校現場では、その他にどのような補助教材を利用しながら教育を進めているのか。教科書の他に使用している資料等について検討することにより、例えば、より知識の理解を深めさせるための教材等、学校現場で使いやすい情報モラル教育の提案ができるのではないかと考えている。さらに、情報担当の教員への調査等を検討し、情報モラル教育を行う教員のリスク認知とセキュリティ対策行動との関連を分析することを考えている。早期の情報モラル教育を積極的に進めていくために、教員自身の意識を高めていくことも必要である。今後は、子どもたちへの情報モラル教育と、教員のモラル教育の見直しも考えていく必要があるのではないかと考えている。

６．研究成果の発表

今年度学会等で発表する予定である。

研究課題名：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高度 ICT プラットフォーム構築に向けた基盤研究（「セキュリティと社会」担当）

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、セキュリティと社会に関する社会調査やケーススタディ――具体的には人々の情報通信技術（以下、ICT）の利用実態に関する全国調査の結果や情報セキュリティに関する社会問題となった実際の事例――の分析を踏まえて、人文社会科学（情報社会論、社会学理論）の立場から独自の研究枠組みを提供することを目的としている。

情報通信技術（ICT）の進歩は日進月歩である。同様に、組織を標的としたサイバー犯罪もまたグローバル化と先端技術によって次々と新しい手口を開発し、被害が多発・深刻化するなど社会問題としても注目を集め、より高度な組織内セキュリティ対策が急務とされる。しかし、ICT は既に社会的インフラとして広く浸透しており、ICT を日常的に利用する私たちの情報セキュリティに関する意識・知識・行動と、最新の技術的動向との間に生じるタイムラグ（時間的な「ずれ」）は、新たなリスクとなっている。こうした情報セキュリティをめぐる「ずれ」はまた、社会の至る所に偏在し（社会集団内の「ずれ」＝空間的な「ずれ」）、例えばセキュリティ上のリスクの認識についても、技術者・開発者と、組織の管理者・運営者、また末端の利用者・ユーザ同士の間に「ずれ」と多様性が生じている。このように、情報セキュリティに関する人々の意識・知識・慣習行動は多様であり、一人ひとりの属性や社会的環境に応じて異なるにもかかわらず、既存の情報セキュリティ研究では「標準化された利用者像」を前提として（利用者の意識・知識・行動に詳細に踏み込むことなく）技術的対策が講じられがちであった。しかし、昨今のソーシャル・エンジニアリングを用いた標的型攻撃による組織被害（2018 年 1 月に、日本国内で起きた、大手仮想通貨交換会社コインチェックへの不正アクセスと仮想通貨 580 億円相当の流出事件等）に顕著なように、「合理的で効果的なセキュリティ技術」への傾注によって、人文社会科学が主に扱ってきた「必ずしも合理的でない生身の人間」の弱さ（脆弱性・盲点）が、情報セキュリティ研究で見過ごされてきたのではないか。

そこで本研究では、時間と空間の「ずれ」を認識する研究枠組みを、社会学理論の「ハビトゥス」概念をもとに考察することで社会学的知見と接合し、また全国調査で明らかとなった人々の利用実態を踏まえて、今日的状況や社会的環境を十分に考慮した社会的要請に基づく組織内情報セキュリティ研究という視点から人文社会科学的基盤の提供を目指す。

２．研究の必要性及び従来の研究

情報処理推進機構（IPA）は 2019 年 4 月、最新のサイバーセキュリティ 10 大脅威につい

て発表した。組織を標的とした脅威では、1 位に（前述したソーシャル・エンジニアリング等を用いた）標的型攻撃による被害、2 位にビジネスメール詐欺による被害（2017 年に日本航空が 3 億 8000 万円を詐取された事件等）が挙がっている。ビジネスメール詐欺は、上司や取引先を騙ったメールで振込先や連絡先の変更を伝えるもので、高額な金銭被害や情報漏洩が発生しやすい。2018 年度から日本語メールの事例が国内で確認され始めたが、従来型のセキュリティ対策ソフトでは識別が難しいことが指摘されている。ウィルスメールとは異なりファイルを添付しておらず、またフィッシング詐欺のような不正なウェブサイトへ誘導するリンクも文中に記載されないためである。IPA は、これらの情報セキュリティ対策には、人々が脅威や手口を知る必要性を強調しているが、他方で巧妙化して拡大する「オレオレ詐欺」被害のように、手口が知られていても（知識が普及していても）「まさか自社で起きるはずはない」と意識や行動が伴わずに被害が進行しているのが現状である（昨年度順位も 1 位と 3 位で、いずれも上位を占めている）。また、2019 年に新たにランクインしたのが 4 位のサプライチェーン（供給網）の弱点を悪用した攻撃の高まりである。これは、情報セキュリティの甘い業務委託先組織が攻撃の足がかりとして狙われるもので、2018 年度だけでも、2 月にポルシェジャパン、4 月に三菱地所、6 月にはプリンスホテルなど国内大手企業の顧客・会員情報が流出している。いずれも、危機意識が甘く予算や人員の面でセキュリティ対策（行動）に限界のある中小企業を狙っており、大企業との格差を突いた攻撃といえよう。また、2019 年 2 月 8 日の日本経済新聞では、東京五輪開催を前に日本が標的となる可能性に備えて、総務省が 2019 年 2 月 20 日から IoT 機器の安全性を確かめるために企業・個人向けに異例の調査を開始すると報道した。これまでセキュリティ対策といえば、パソコンやスマートフォン経由で被害を受けないよう注意が払われてきたが、ICT の進歩により IoT 機器が乗っ取られると、サイバー攻撃（加害）に使われてしまう。ルーター・センサー・監視カメラなどを、人々が「セキュリティ対策の不要なもの」と見なし、出荷時の安易なパスワードのままネット接続していることにつけこんだ手口である。

このように、近年のサイバー攻撃は、技術的なセキュリティ対策をすり抜けるべく、個々人や中小企業の情報セキュリティに関する知識・意識・行動の多様性・格差を突いた組織攻撃が主流となりつつある。情報セキュリティに関する既存研究では、こうした人々の多様性への認識を欠いており、それが組織内セキュリティの盲点となってきていることから、文系・理系の研究領域を横断する視座を持った学際的な研究が必要である。

３．期待される効果

本研究では、ICT の進展が人々の情報への接し方やリスクへの対応の仕方（認識図式や行動様式：ハビトゥス）をどのように変容させるのか調査し分析する。その際、社会学の知見を応用し、時間軸（事前予防から事後対策への注目）と空間軸（人々の格差と対応の多様性）の両側面から考察し、危機管理の今日的枠組みを検討する。時間軸の「ずれ」に注目すると、どれほど新しい知識を学んでも、現在進行中の技術的進歩と手口の変化がもた

らす将来のリスクまで正確に見通すことは困難であることが分かる。また、昨今のソーシャル・エンジニアリングの手法は、怪しいメールを疑うといった個人の主観に依拠した「事前の対策」だけでは、もはや組織内セキュリティを守ることは困難であり、攻撃を受け不正アクセスがなされることを前提として、そこから先に、情報流出や金銭的被害に至らないよう、被害を抑える「事後の対策」を講じる必要があると注意喚起されている。言い換えれば、人々の知識や意識の「ずれ」を突いたサイバー攻撃に対しては、組織的な管理体制や事後対応を検討することが要請されている。

そのために本研究では、利用者間に見られるセキュリティに関する知識・意識・行動の差異に注目し、その諸要因を調査・研究する。既存のセキュリティ対策では、一律に研修を行い、知識を増やすことに重点が置かれてきた。しかし、実感の伴わない知識は必ずしも行動に結びつかず，そこで、所属する組織や集団の慣習行動や行動規範を研究する社会学的知見（ハビトゥス論）と接合することで、事後対応の周知徹底の方法等、より効果的な組織内セキュリティの提案へとつなげる。他方でまた、調査から明らかとなった新たな知見をハビトゥス論に内包することで、社会学理論として新しい水準に展開していくことができる。こうして、文系と理系の学問領域を横断した研究を目指すだけでなく、そこで得られた知見をそれぞれの領域へフィードバックすることで、安心安全なインターネット社会の構築に資する情報セキュリティへの提案と新規課題の発見とを通じて、検討・精緻化を行い、深い水準で研究を展開していくことができると期待される。

４．研究の経過及び結果

本研究においては、2017 年度（2017 年 11～12 月）と 2018 年度（2019 年 2～3 月）に情報セキュリティの実態に関するインターネット全国調査を実施し、多くの知見を得ることができた。これらの調査・研究は、本学のヒト倫理審査委員会で承認されたもの（承認番号 20171212-17 および 20190318-30）である。

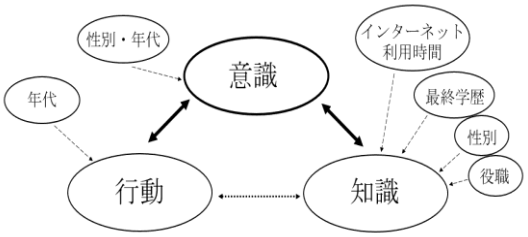


図 1. セキュリティ意識･知識･行動の関連図

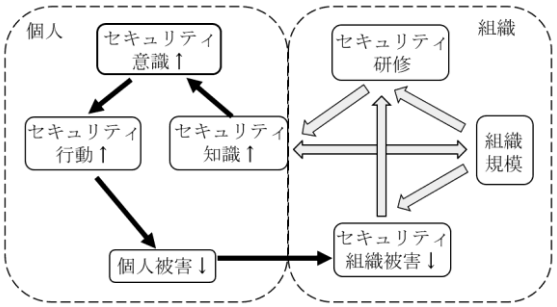


図 2. 個人と組織の情報セキュリティ関連図

2017 年度に実施したインターネット全国調査では、組織に所属する人々（会社員・公務員）2,000 人に対して、情報セキュリティに関する意識・知識・行動を尋ねると共に、組織内および自宅での ICT の取り扱いや情報セキュリティ対策の実態を調査した。調査結果を

まとめたものが、図1と図2である。矢印はすべて、算出された統計的有意差を表す。図1から、組織に属する人々は一律ではなく、性別・年代・学歴といった属性、組織内での役職やネット利用時間などによって、情報セキュリティに関する知識・意識・行動が様々な水準にあることが分かる。また、セキュリティに関する知識と実際の行動との間に直接的な関連性は低く、他方でセキュリティ意識が両者と強く結びついているが分かる。図2は、個人と組織の関係性を示している。組織規模（従業員数）、セキュリティ研修の実施、組織被害の有無という三者の間には、互いに強い関連性が算出された（組織規模が大きいとサイバー攻撃の対象とされやすく、組織被害も多くなる：組織被害の経験があったり、組織規模が大きいほど、セキュリティ研修を実施している等）。しかし、組織に属する個人との関係で見てみると、セキュリティ知識と組織被害との間には関連性がない（統計的有意差を示す矢印が引かれていない）ことが分かる。ここから、組織内の研修で人々の知識を増やすように努めても、それだけでは人々の行動を変えることに直結しない実態が見て取れる。加えて、人々のセキュリティ意識を介在させることで、知識が行動に影響を与える可能性が示唆される。例えば、セキュリティ研修において、同業他社の被害事例を具体的に検討するなど、情報セキュリティへの対応は急務であり決して他人事でないという意識を一人ひとりに実感してもらえるような（セキュリティ意識の向上を促す）知識を紹介することで、人々の行動を効果的に改善することができるだろう。実際、組織規模にかかわらず、個人のセキュリティ行動は個人の被害経験の有無に、また個人の被害経験の有無は組織の被害経験の有無に、それぞれ統計的有意差が算出されている。組織内での研修は、ただちに組織被害を防ぐものではないが、セキュリティに関する知識を増やすことで人々の意識が向上し、それによって一人ひとりが納得してリスクの高い行動を避ける（慣習行動を改める）ようになり、個人の被害が減るだけでなく、安全性が高まることで組織被害の減少にもつながる。このように、組織内セキュリティを高める研修の効果（影響の伝播）について、大きく迂回するルートの存在を明らかにすることができた。

他方で、ICT利用の慣習行動が実際のセキュリティ状況を左右し、それらは社会的環境ごとに特徴的な傾向があること、また、利用者の性別や年齢、学歴、社会的環境（所属する組織の規模や職位、労働状況、生活水準等）によって、セキュリティ意識・知識・行動に差異が生じることが調査データから実証された。例えば、知識や関心領域に「性差」があることは、社会学における既存のジェンダー研究でも指摘されて久しい。しかし今回の調査では、回答者の性別は、知識に強い影響を、また意識に弱い影響を及ぼすのに対して、実際の行動にはほとんど影響が見られなかった（統計的有意差を示さなかった）。ここから、新しい社会学理論上の知見が得られる。既存研究にあるように、例えばインターネットの利用に関して、男性はゲーム依存、女性は SNS 依存になりやす傾向が知られているが、それはインターネットを利用した――ネット利用を「通じた」――社会慣例的な行動に現れる性差とみなすことができる。対して、ネット利用に「関する」情報セキュリティ行動といったメタ水準では、性別などの属性的要因よりも、社会的環境からの要因が大きいこと

が明らかになった。性差による行動様式の違いとして理論化されてきたハビトゥス概念の、水準の違いを考慮に入れた更なる精緻化の可能性が示唆されよう。

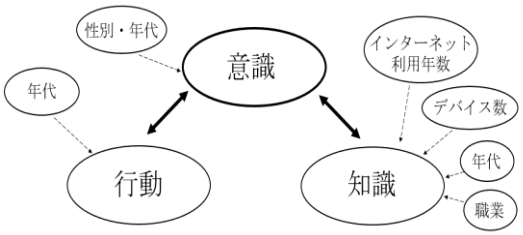


図 3. セキュリティ意識･知識･行動の関連図

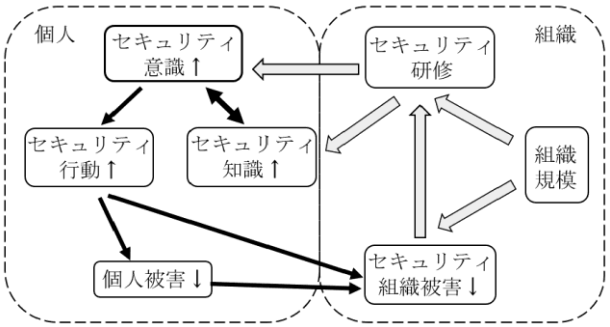


図 4. 個人と組織の情報セキュリティ関連図

次に、2018 年度に実施したインターネット全国調査では、より広範囲に非正規で組織に所属する人々も含めた 2,000 人（年代性別は均等割付）に対して、情報セキュリティに関する意識・知識・行動を尋ね、また情報セキュリティに関する知識の摂取方法（情報検索の仕方）についても調査を行った。調査結果をまとめたものが、図 3 と図 4 である。矢印はすべて、算出された統計的有意差を表す。図 3 から、前年度の調査（図 1）と同様に、情報セキュリティに関する知識・意識・行動が、人々の属性や社会的環境に応じて様々な水準にあることが分かった。今回の調査では、一方で、セキュリティに関する知識と実際の行動との間に関連性は見出されなかったが、他方で、知識に対して回答者の学歴の影響が薄れ、代わって新たに質問項目に加えたデバイス数の多さ（スマホだけでなく、ノート PC、ディスクトップ PC、タブレットなど情報検索への複数のアクセス）等が、正の相関をもつことが分かった。ここから、回答者の属性よりも、ICT 等の使いこなし方によって、セキュリティ知識に差が生じることが分かった（他にも、まとめサイトだけでなく、取材して書かれた解説記事を読むかどうか等、アクセスする情報の「質」と知識との間に強い関連が見られた)。図 4 の個人と組織の関連図では、前年度の調査（図 2）と同様に、セキュリティ研修が迂回して発揮するルートを確認することができたが、若干の変化が見られた。2018 年度の調査では、（個人の）学歴と知識に関するつながりが見出されなかったことに付随して、組織規模と（就労者の）知識の間の関連性も見出されなかった（非正規雇用の回答者が一定数いたためと想定される)。しかし新たに、研修を受講した人は、していない人よりもセキュリティ意識の面での向上が見られた（研修の受講が「業務」の一環であることを考慮すると、意識が高いから受講したという流れも否定できないものの、受講することによって人々の意識が高まったと見るのが妥当であろう)。また、意識と知識の間は強い相関が見られ、個人の日常生活において、意識の高まりが知識の吸収に向かい、知識の増加が意識の向上につながることも示唆された。加えて、前年度と同様に、知識の増加が直接的に安全な行動へと結びついてはいないが、意識を介在することで変化し得ること、また新

たに、個人の行動が個人の被害を減少させるだけでなく、直接的に組織被害の減少とも関連していることが抽出された。しかし、今日のサイバー攻撃はソーシャル・エンジニアリングを用いるなど巧妙になっており、個人的な注意だけでは防げないことも指摘されている。そこで、これらの調査結果を踏まえ、例えば、部署ごとの小規模なセキュリティ研修を実施して、「避難訓練」のように、実際に被害を受けてしまった場合にどのような対策を組織内で取るべきかを「行動ベース」で習得させることの効果が指摘できよう。目前の ICT の小さな異変を看過することで、その後に生じる被害の甚大さを実感したり、どの時点でどのような対処をすべきなのか、どのタイミングで組織内の誰に報告・相談するのかを追体験・グループ議論したりすることで、座学で新しい情報を得るだけではない研修の効果が得られると考える。こうした行動ベースの知識であれば、(最新の情報に基づいた行動を心がけて被害を未然に防ぐだけでなく) 万が一、サイバー攻撃を受けても被害を最小限に抑えることができ、組織内セキュリティを一層強固にすることができる。

５．　今後の計画

本研究の研究成果を、情報系・社会学系の学会にて発表する（論文発表や口頭発表を行う)。特に 2018 年度の全国調査は、2019 年 2～3 月に実施したこともあり、まだ十分には調査データを分析しきれていない。この調査では、情報へのアクセスルートや情報収集のハビトゥス（認知図式・行動様式）について詳細に質問しており、人々の情報セキュリティに関する知識の形成プロセスを明らかにすることで、知識の質や量が生み出す差異、および知識が意識や行動に与える影響や条件を抽出できるのではないかと期待している。それを踏まえて、より効果的な組織内セキュリティの在り方についても、検討していきたい。

６．　研究成果の発表

2018 年 3 月に、所属系列（基礎・教養教育センター人社系列）の専任教員が定年退職し、教員数が 3 名から 2 名へと減少した。そのため、2018 年度は増加した業務に追われてしまい、過労のため大学構内で倒れて救急搬送されたほどである。日々の教育と膨大な業務に追われて研究を後回しにせざるを得ず、結果として予定していた学会発表・論文投稿などが全くできなかった。(2019 年度は、自身の体調に配慮しつつ、研究成果の発表に努めたい。)

▼付記：昨年度（2017 年度）の報告書に記載を落としていた研究成果発表

[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』第 3 章として収録、学文社（2017,04）