神奈川工科大学

セキュリティ研究センター
研究報告

第6巻

2017（平成29年度）

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

「アレクサ、明日の天気は？」「音楽かけて」「電気消して」など人間と会話ができる AI のクラウドサービスが本格化してきた．あらゆるモノがインターネットにつながることに よって，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．例えば， 自動車システムの遠隔操作可能な脆弱性により，攻撃者がスマホで他車のドアを開閉でき，我々の命まで奪われる惨事なってきています．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 29 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，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，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	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・准教授	クラウドサービスの強靭化に関する研究
西村　広光	情報メディア学科・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	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

セキュリティ研究センター研究報告
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，今年度の研究では，公共の場で持ち込みのノート PC のロックを解除したり，設置してある公共の PC を用いてサービスにログインしたりする際に覗き見攻撃に十分な耐性を持つ個人認証方式について検討する．特に，手軽でほとんどのデスクトップ PC に備え付けられている機器を入力デバイスとした個人認証方式を提案する．そこで，従来のキーボードを用いた認証に対して，不特定多数の人が認証を行うことを視野に入れ，操作の単純性やユーザビリティを考慮した安全な認証方式の提案を目的とする．

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．

その中で，不特定多数の人が存在する公共の場で個人認証を行う場面が増加している．現在の認証方法には，主にパスワード方式が利用されているが，第三者による覗き見によって，パスワードが漏洩する問題がある．よって，公共のパソコンで使用でき，かつ老若男女誰でも直感的に使用できる認証方式が必要となる．

従来のデスクトップ PC における個人認証方式では，例えばマトリックス上の座標をキーボードで入力する方式が存在する．このような文字の記憶ではなく，場所の記憶による認証はユーザが覚えやすい利点があるが，キーボードで認証情報を直接入力する方式であるため，キーボードを見ることによる覗き見攻撃に弱い欠点がある．またキーボードを使わない方式として，マトリックス上におけるマウスの軌跡上の座標を認証情報とした方式も

存在するが，画面上の軌跡を覗き見されると認証情報が漏洩する．よって，不特定多数の人がいる公共の場では，直接認証情報を入力しその入力デバイスが第三者に見える状況で認証を行う方式では，覗き見攻撃に弱くなる．

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．

また，操作が簡単なマウスを利用した認証方式として，認証画面だけを見ても入力情報が漏洩しないようにすることで，覗き見に対する耐性を持つ方式が期待できる．更に，マウスは簡単に机の下などに隠せるため，認証する際の環境状況に応じて覗き見耐性の強さを変更できる方式となる．このように，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

公共の場で有用な覗き見耐性を持つ個人認証方式の提案をするとともに，そのユーザビリティ評価と覗き見耐性の有無を実証した．提案した方式では，ほとんどのデスクトップ PC に備え付けられておりかつ操作が簡便なマウスを用いて認証を行う．以下にマウス認証についての説明とその実験結果を報告する．

4.2 マウス操作を用いた認証方式

マウス認証方式は，入力インタフェースとしてマウスの左右クリックと上下ホイル回転，ホイルクリックを用い，出力インタフェースとして N×N のマトリックスを用いた認証方式であり，N×N のマトリックス上の座標を認証情報とする．図 1 にマウス認証における認証情報の登録手順について示す．最初にマトリックス上にランダムで初期位置が配置され，ユーザは登録したい座標にマウス操作を用いて移動を行う．操作と座標移動の対応は直感的で，例えば右クリックを押せば現在位置が一つ右に移動し，上ホイル回転を行えば一つ上に移動する．ホイルクリックで座標を登録すると再びランダムに初期位置が表示され，二つ目の登録したい座標に移動を行う．

次に，図 2 に認証手順について示す．基本的な操作は登録手順と同じであるが，ユーザは初期位置から現在位置が見えない状態で登録した場所を指定する．そうすることにより，画面を見ることによる覗き見攻撃を防ぐことができる．

提案方式の有効性を確認するために実験行い，ユーザビリティの評価として認証成功率や認証にかかった時間を測り，アンケートを実施した．結果として，マウスの発する音を聞くことによる覗き見攻撃に対する耐性が十分に備わっていることを示した．さらに，提案手法のバリエーションとして二つの新たな手法を提案し，そのユーザビリティを確かめる実験を行った．一つ目のバリエーションとしては，数字と色をマトリックス上にランダムに表示し，それを指定することで数字と色の組み合わせを認証情報として登録する手法であり，二つ目はマウス操作の組み合わせで直接マトリックス上の座標を指定する方法である．結果として，操作の組み合わせを用いたバリエーションが提案手法の中で一番のユーザビリティを持つことが分かった．

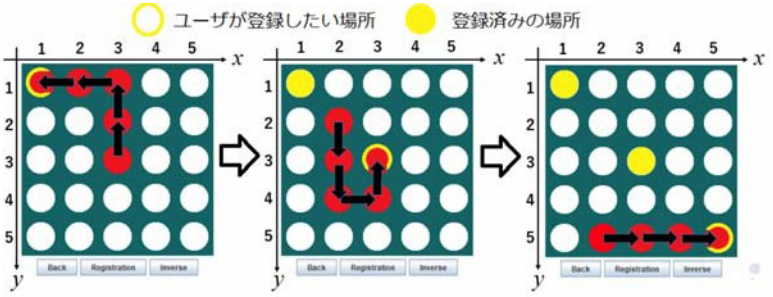


図 1. 登録手順

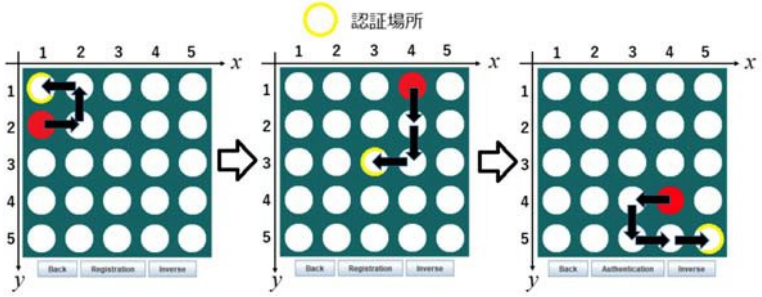


図 2. 認証手順

5. 今後の計画

公共の場や企業などで利用することが多いデスクトップ PC の覗き見対策として提案したマウス認証方式は，新たなデバイスを導入することなく，環境に応じて簡単な操作でだれでも使うことができることが分かった．今後は，提案手法のバリエーションの覗き見耐性

の実験い，安全性とユーザビリティを向上するための検証を行っていく予定である．さらに，これらの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] M. Nagatomo,Y. Kita, K. Aburada, N. Okazaki and M. Park, " Implementation and user testing of personal authentication having shoulder surfing resistance with mouse operations," IEICE ComEX, Vol.7, No.3, pp.77-82,January 11, 2018.

[2] M. Nagatomo, Y. Kita, K. Aburada, N. Okazaki, and M. Park, "Evaluation of Mouse Operation Authentication Method Having Shoulder Surfing Resistance," Advances in Internet, Data & Web Technologies, Lecture Notes on Data Engineering and Communications Technologies, Springer, Vol.17, pp.979-989, 20180315.

[3] H. Yamaba, T. Kurogi, K. Aburada, S. Kubota, T. Katayama, M. Park and N. Okazaki, "On applying support vector machines to a user authentication method using surface electromyogram signals," Artificial Life and Robotics, Vol.23, pp.87-93

(2) 学会発表

[1] 長友 誠，喜多 義弘，油田 健太郎，岡崎 直宣，朴 美娘，“マウス操作を用いた個人認証方式のユーザビリティと覗き見耐性の実験と評価，”コンピュータセキュリティシンポジウム（CSS2017）論文集，pp.1521-1526, (2017.10.23).

[2] 長友 誠, 朴 美娘, 岡崎 直宣, "覗き見耐性を持つマウス操作を用いた個人認証方式の提案," IPSJ CSEC/SPT 研究報告, No.29, 20170714

[3] 堀 孝浩, 朴 美娘, 岡崎 直宣 “受信信号強度を用いたデバイス認証における異常値除去手法に関する検討”，マルチメディア，分散，協調とモバイルシンポジウム（ DICOMO2017）論文集，pp.217-222, Jun 2017.

[4] 油田 健太郎, 山場 久昭, 朴 美娘, 岡崎 直宣 “DPI を用いたIoT 機器向け不正侵入検知システムの検討”，マルチメディア，分散， 協調とモバイルシンポジウム（ DICOMO2017）論文集，pp.1627-1634, Jun 2017.

(3) 特許

[1] 特願 2014-046134「個人認証装置及びプログラム 」
発明者口岡崎 美蘭
出願者口学校法人 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

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・実証を進めてきている。

一つ目の技術は、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。29 年度の課題は、構築したカード認証技術は、認識用カメラから 30cm 以内に近づけないと利用することができなかった問題を解決するため、2-3m 離れた距離で高速にカードを検出する技術開発であった。

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たかい。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てきた。29 年度の課題は、鍵をシリンダ内部に挿入した状況で、カメラ撮影用の穴を特殊加工した状況で、鍵識別が高精度に行えるかの検討することであった。加えて、金属鍵の抜き差しによる摩耗劣化が検討している認証技術にどのような影響を与えるかについて検討することも課題であった。

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。

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。

５．今後の計画

カード認証においては、実用的な実験環境を構築し、これまでに構築した技術を融合した実証システムの構築を試みる。加えて、より大規模実験を行い、提案手法の有効性・堅牢性を実証していく計画である。

紫外線画像による金属鍵認証に関しては、実際に複製した鍵での性能評価実験をすすめる。加えて、摩耗劣化していく過程を利用した新しい認証技術を構築する。

双方の成果を広く国内外に発信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。

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

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、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、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、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。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、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。しかし、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は、周波数変換の種類によってかなり 異なる。そこで本研究では、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、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。同様に、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も、同じ強度で情報を埋め込んだ場合でも透かし入り音楽におけるノイズの表れ方は、周波数変換の種類によって異なる。そこで、音楽用情報ハイディングについても同様の検証を行う。

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。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。しかし、周波数変換が異なれば、画質（音質）に影響を与えるノイズの表れ方も異なる。したがって、人間の視覚（聴覚）によって画質（音質）劣化を評価する必要がある。

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。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。しかし、周波数変換が異なれば、画質（音質）に影響を与えるノイズの表れ方も異なる。そこで、人間の視覚（聴覚）によって画質（音質）劣化を評価することにより、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各種周波数変換の優劣が明らかになることが期待される。

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 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 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。まず、全ての周波数変換において、強度を 20 に固定して透かし情報を埋め込んだ画像を作成し、5 人の被験者に評価を行ってもらった。検証の結果、同一の強度においては、DFT、DCT、DWT の順に画質劣化が小さいと認知されることが明らかとなった。この結果は、昨年度に行った強度を尺度とした定量的な検証の結果 と真逆である。そこで、両者を同時に評価する検証として、それぞれの周波数変換におい て、誤りが発生しない必要最小限の強度で透かし情報を埋め込んだ画像を作成し、5 人の被験者に評価を行ってもらった。検証の結果、DWT が最も画質劣化が認識されやすいこと、DFT と DCT については、一概にどちらが優れているか判定できな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 3 種類、周波数変換の次元を 1024 次、拡散系列として 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 1536bit 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。まず、両方の周波数変換において、強度を 3000 に固定して透かし情報を埋め込んだ音楽を作成し、5 人の被験者に評価を行ってもらった。検証の結果、同一の強度においては、DCT の方が DFT よりも音質劣化が小さいと認知されることが明らかとなった。この結果は、昨年度に行った強度を尺度とした定量的な検証の結果と同じ である。次に、両方の周波数変換において、誤りが発生しない必要最小限の強度で透かし 情報を埋め込んだ音楽を作成し、5 人の被験者に評価を行ってもらった。検証の結果、同一の強度を使用した場合と同様に、DCT の方が DFT よりも音質劣化が小さいと認知されることが明らかとなった。ただし、同一の強度を使用した場合と比較すると、DFT の方が音

質劣化が小さいと感じる割合や両者に違いがないと感じる割合が増加した。これは、強度を必要最小限としたため、音質劣化が小さく抑えられた結果、両者の違いを聞き分けるのが困難になったためであると考えられる。

５．今後の計画

今回の検証では、画像および音楽において、拡散系列の大きさは 1 種類のみを使用した。今後は、異なる大きさの拡散系列を用いた検証を行い、今回得られた結果が、どのような 条件下でも同様なのか詳しく調査する必要がある。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。

クラウドサービスの強靱化

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、故障などの偶発的な障害だけでなく、サイバー攻撃に対しても耐性のある高可用性サーバを実現することを目的とする。この研究目的を実現するために、次の 2 つの研究開発を進めてきた。

① サイバー攻撃に耐性のあるサーバの運用技術の開発

② サーバアプリケーションそのものを強化するセキュリティモジュールの開発

研究①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運用技術を開発する。この技術では、異なるサーバ OS と異なるサーバアプリケーションを組み合わせて冗長化するが、プライマリサーバがダウンしてからセカンダリサーバへサービスを引き継ぐときに発生するダウンタイムを最小化することがメインテーマとなる。

研究②は、既存のサーバアプリケーションに手を加えずに、サーバアプリケーションの可用性を強化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。

２．研究の必要性及び従来の研究

インターネットの普及とともに可用性の高いサーバが求めれている。一般的に高可用性サーバといえば、同一構成の冗長化であるが、同一構成はサイバー攻撃に耐性がない。故障などの偶発的な障害だけでなく、サイバー攻撃などの意図的障害に対しても耐性のある高 可用性サーバを実現することが求められている。偶発的障害と意図的障害に対する可用性 を強化するために、多様性を有する冗長化があるが、多様性のある冗長化には、多くの物理リソースが必要であったり、数分程度のダウンタイムが発生したりするなどの課題がある。

サイバー攻撃を未然に防止することにより、可用性を維持する研究も盛んに行われている。最新のサイバー攻撃検知技術は、主に機械学習に基づく手法が大勢を占める。最新の研究成果は、高い検出精度と高速性を両立しているが、いずれも大量の学習データがあることが前提である。学習データは、正常データと攻撃データに分けられるが、いずれも大量の多様なデータを用意することが難しいケースが想定される。特にオリジナ

ルやカスタムされたサーバアプリケーションに対する攻撃データを事前に収集することが難しい。また、大量の正常データがある場合において、それらすべてが真に正常であることを保証することが難しいことがある。なお、これらの最新の手法はすべて実験の段階であり、実際の運用時の性能は明らかでない。

３．期待される効果

研究①により、偶発的障害と意図的障害に対する可用性を強化できる。ただし、研究①は、サーバアプリケーションの多様な実装が存在することが前提であるので、研究①が適用可能なサービスやプロトコルは、HTTP や DNS など主要なプロトコルに限定される。

研究②により、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可用性を強化できる。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、適応的に未知のサイバー攻撃を検知・防止できる点が研究②の強みである。

４．研究の経過及び結果

研究①では、1)オンプレミスの環境下でダウンタイムを最小化することと、2)クラウドプラットフォームの環境下でオンプレミス環境下と同等の機能を実現することを目標に研究を進めた。

研究①の 1 では、受動的冗長化と能動的冗長化を組み合わせることにより、物理リソースを最小化しつつ、ダウンタイムをゼロにする運用技術を提案した。プロトタイプを構築して、2 台の物理マシンだけでダウンタイムをゼロにできることを確認した。なお、プロトタイプが提供するサービスは、DNS である。

研究②の 2 では、まず、クラウドプラットフォームの仕様や機能の比較を行い、それらの機能制約に基づいて、クラウドプラットフォーム環境下でのプロトタイプの設計を行った。プロトタイプでは Kubernates によるコンテナオーケストレーションを活用することとした。Kubernates の動作を確認するため、オンプレミスで Kubernates によるサービス環境を構築して、サービスの可用性を評価した。その結果、障害発生時に 5 分程度のダウンタイムを要することを確認した。

研究②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部分的に実装していたが、2017 年度に最小構成の機能をすべて実装した。実験的な試みとして、機械学習の入力データを工夫することにより、検出精度を10%程度改善できることを確認した。さらに、モジュールのポータビリティを評価するため、世界でよく利用されているサーバアプリケーションの 1 つである ISC BIND9 に適用可能なモジュールを実装した。実在する脆弱性（CVE-2015-5477 と CVE-2016-2776）に対してサイバー攻撃を行って、検出精度を評価した結果、過去最高の

96.87 %を得た。しかし、モジュールの実装作業を通して、非同期入出力処理を行うサーバアプリケーションでは、モジュールがそのサーバアプリケーションの実装に強く依存し、サーバアプリケーションごとにモジュールの実装が必要であることを確認した。また、モジュールのオーバーヘッドが 126%程度あったことから、オーバーヘッドの削減が課題である。

5. 今後の計画

研究①では、クラウドプラットフォーム環境下での可用性強化に向けて、Kubernatesのオートヒーリング機能のリカバリ速度を改善する。これにより、クラウドプラットフォームにおけるサイバー攻撃に対して高可用性を実現する道が開ける。

研究②では、モジュールのオーバーヘッドを削減する。削減するアプローチとして、メモリ管理（排他制御）の効率化、機械学習の前処理による工夫、機械学習アルゴリズムの変更が考えられる。また、できる限りサーバアプリケーションの実装に依存しないモジュールの実装も試みる。

6. 研究成果の発表

1. 多羅尾 光宣, 岡本 剛, “ISC BIND9 のための免疫系を模擬したセキュリティモジュールの実装と性能評価,” 第 80 回コンピュータセキュリティ研究会, 情報処理学会研究報告, Vol. 2018-CSEC-80, No. 3, pp. 1-8, 2018.

2. Mitsunobu Tarao, Takeshi Okamoto, “An artificial immunity-enhancing module for internet servers against cyberattacks,” Artificial Life and Robotics Journal, pp. 1-6, 2018. （査読有）

3. Takeshi Okamoto, “Design of a Lightweight Intrusion-Tolerant System for Highly Available Servers,” Procedia Computer Science, Vol. 112, pp. 2319-2327, 2017. （査読有）

4. Mitsunobu Tarao, Takeshi Okamoto, “Performance Evaluation of an Immunity-Enhancing Module for Server Applications,” Procedia Computer Science, Vol. 112, pp. 2165-2327, 2017. （査読有）

5. Takeshi Okamoto, Fumikazu Sano, Idris Winarno, Yoshikazu Hata, Yoshiteru Ishida, “Implementation and Evaluation of an Intrusion-Resilient System for a DNS Service,” International Journal of Innovative Computing, Information and Control, Vol.13, No. 5, pp.1735-1750, 2017. （査読有）

6. Idris Winarno, Takeshi Okamoto, Yoshikazu Hata, Yoshiteru Ishida, “Distributed SRN Manager on a Resilient Server with Multiple Virtualization Engines, ” International Journal of Innovative Computing, Information and Control, Vol.13, No. 2, pp. 365-379, 2017. （査読有）

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．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．H29 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，さらに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．

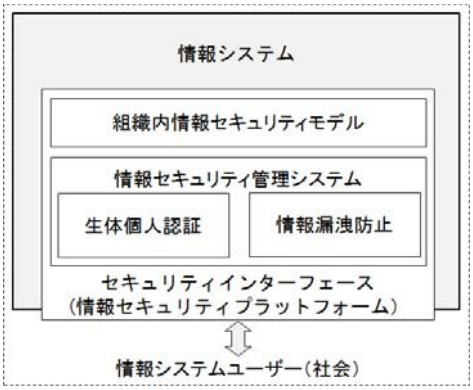


図 1．提案システムイメージ

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．

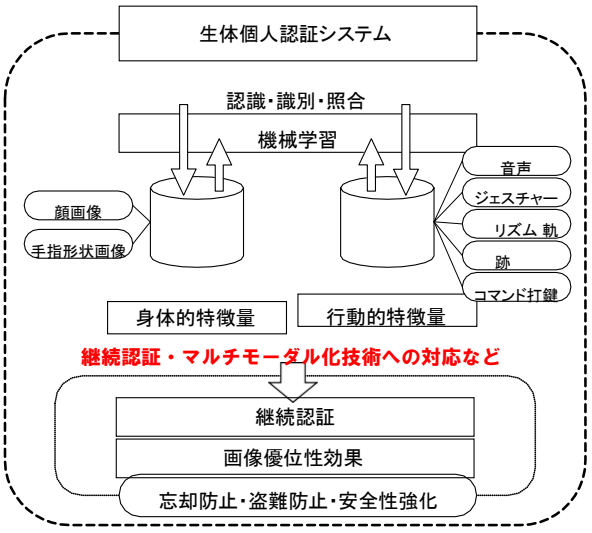


図 2．生体個人認証システムの拡張

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．H29 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，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．

H29 年度の研究成果としては，特に，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．最大85%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認証の実現に近づくことが期待される．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，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

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 29 年度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，昨年度に掲げたことは，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，残念ながら，導入まで至っていない．ただし，平成 30 年度からは，MATLAB 包括ライセンス契約がなされたことにより，自由に活用する道が開けた．これを機会に，こうした既存ツールの導入を図りたい．

６．研究成果の発表

[1] 滝本将司*，納富一宏，斎藤恵一:"サーバ操作時の継続的個人認証 -キーストロークを使用した自己組織化マップによる-"，情報処理学会 第80 回全国大会講演論文集 第3分冊，3W-05, pp.503-504，(2018.03).

[2] 滝本将司*，納富一宏，斎藤恵一:"サーバ操作時のキーストローク情報による継続的個人認証"，バイオメディカル・ファジィ・システム学会 第 30 回年次大会講演論文集，pp.135-138, (2017.11).

（*：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いては，個人情報漏洩が引き続き大きな問題となっている．個人が管理する PC 端末や USB メモリに個人情報を保存しておくと，それを紛失したり第三者に盗まれたりした場合には直接個人情報漏洩につながってしまう．そこで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．ただしクラウド方式においても，セキュリティは重要である．特に，クラウド利用に向けての本人確認のための個人認証が重要となってくる．パスワード方式で認証をしていると，パスワードが推測されたり盗まれたりした場合にはなりすましで他人が利用できてしまう可能性がある．そこでパスワード以上に「強い認証」を実現するための認証手段が必要となる．既存技術としては，ワンタイム・パスワードや生体認証，PKI 認証等があるが，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方式である．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，更にはユーザには特別な機器や追加ソフトウェアを必要としないため，簡易にいつでもどこでも利用できる方式であり，クラウド世界における新たな安全安心を実現する技術として期待できる．

２．研究の必要性及び従来の研究

マルチサインオン技術は，「強い認証」を実現するための重要な技術である．マルチサインオン方式では，複数の認証手段を用いて認証を行う．ただしこれら複数の認証手段がユーザ負担あるいはサービス提供側の負担になるようであると，実現が難しい．たとえば既存技術では，ワンタイム・パスワードや第二パスワード方式などがあるが，ワンタイム・パスワード方式では一時的なパスワードを表示するトークンと呼ばれる機器の購入・配布が必要となりサービス提供側にコストがかかるし，ユーザはそれら機器を常に携帯する負担がかかる．また第二パスワード方式では新しく別のパスワードを覚えるといったユーザ負担が追加される．他にも指紋認証方式や PKI 証明書認証など，様々な「強い認証」方式も提案されているが，読み取り機器の準備やそれら維持管理・保守運営にコストがかかり， サービス規模の小さな企業には利用ができない難点がある．そこで簡単なマルチサインオン方式の実現が期待される．

３．期待される効果

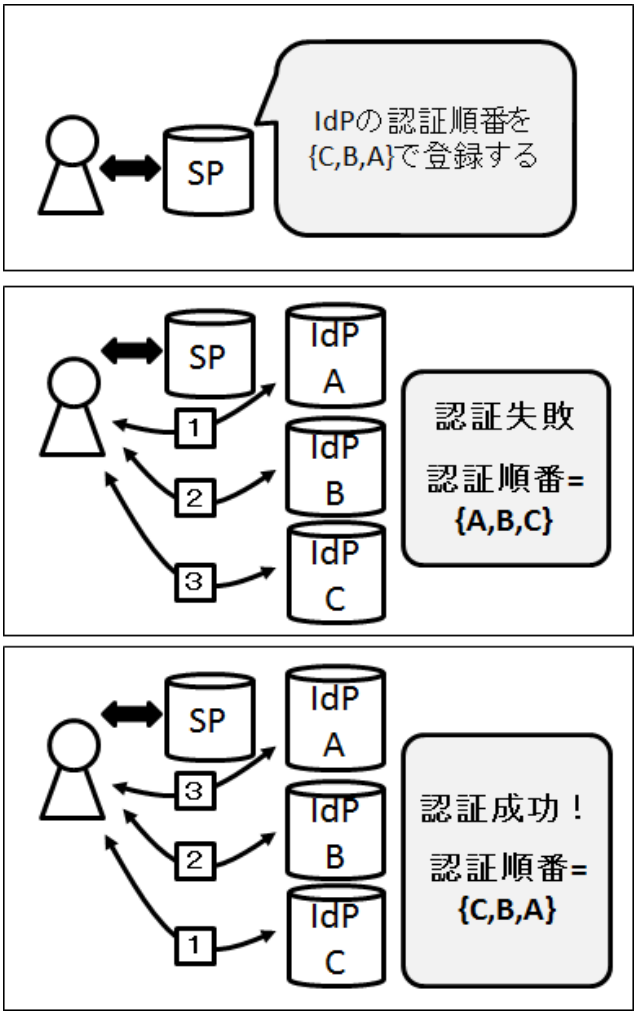
マルチサインオン方式が簡易に利用できれば，大きな資本をもたない中小企業においても「強い認証」を用いた安全安心なサービス参加が可能となり，インターネット上のさらなるサービス追加に期待ができるようになる．特に本研究の「順番マルチサインオン方式」の提案は，ユーザがブラウザのみを用いてその訪問の順番の正しさを用いて認証を行うので，ユーザは何の負担もなく通常の行動を行うことで本人確認を受けることができ，サービス提供側もマルチサインオン利用にあたって新たになんの追加設備・配布物の準備も必要としない点が優れる．

４．研究の経過及び結果

本研究では「順番マルチサインオン」方式を考案し，その基本方式について[1]にて論文発表を行った．「順番マルチサインオン」方式は一種のライフログ認証である．ライフログとしては 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，マルチサインオン方式としてだけでなく，リスクベース認証の一種としても利用可能である．各 Web サイトへの訪問についてはあくまで認証行為を目的としてユーザが意識的に巡回してもよいが，恣意的に振舞って，結果的には「普段どおりの行動」としての自然な流れに従って「いつも通りの Web サイト訪問の順番」となって，その結果本人確認につながることに期待している．

[1]の論文では，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，複数の IdP（Identity Provider）と呼ばれる認証サーバを用いてマルチサインオンを実現させている（下記図を参照）．ユーザは利用したい SP（Service Provider）に接続するにあたって，その SP に事前に登録した順番通りに複数の IdP を訪問する必要がある．SP はユーザが各 IdP を訪問して各 IdP でユーザ認証を受けるたびに認証結果の通知を受け，その順番を記録する．ユーザは順番通りにすべての IdP を周ったところで SP に対して認証要求を行う．SP はユーザの訪問した IdP の順番が正しければユーザを本人と認めてサービス利用を許すが，順番が異なっている場合は利用を認めない．

各 IdP がすべて ID・パスワード方式であっても本マルチサインオン方式は利用できるので，ユーザの負担はこれまでと変わらないし，IdP 側もパスワード方式の提供だけで追加のコスト負担は不要である．一方でユーザの ID・パスワードが漏洩してしまった場合でも， たとえすべての IdP で同じ ID・パスワードに設定してしまっていた場合であっても，SP にはなりすましでログインすることはできない．なぜならすべての IdP でログインできても， それら IdP を訪問してログインする順番が正しくなければ，本人として認められないからである．よってユーザ負担及びサービス提供者負担は軽減したまま，安全安心なマルチサインオン方式が提供できる方式であるといえる．



参考図：順番マルチサインオン認証方式

５．　今後の計画

今後の課題としては，認証情報を提供する IdP と呼ばれる認証サーバの個数の妥当性の検討がある．IdP が多くなればより安全になるが，ユーザが覚える必要がある「正しい順番」もまた長くなり，忘却を招きやすくなる．どの程度の数の IdP を準備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今後の研究では 必要となる．また「訪問行為」以外のライフログを用いた認証方式についても研究を行う ことが必要である．

６．　研究成果の発表

[1] 岡本学 , “順 番マル チ サイン オ ン方式 の 提案” , 情報処 理 学会論 文誌,Vol.58,No.12,pp.1954-1963,2017.12.

使いやすさと安全性を両立する認証方式の検討

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．本稿では以上の結果に基づいて設計した，複数の認証方式の組み合わせについて報告する．

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．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

本章では，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に基づいた，認証方式の組み合わせ方について報告する．

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たが，2018 年度 5 月現在，後述の理由によって稼働停止中である．これまでの設計では，システムは 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/

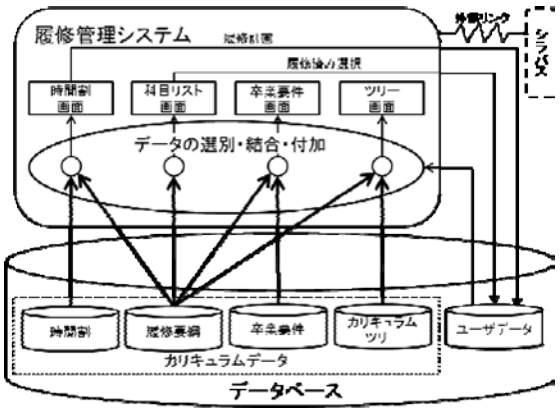


図１　履修管理システム構成図

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　利用者数の推移と認証方式の選択に関する意識調査

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．

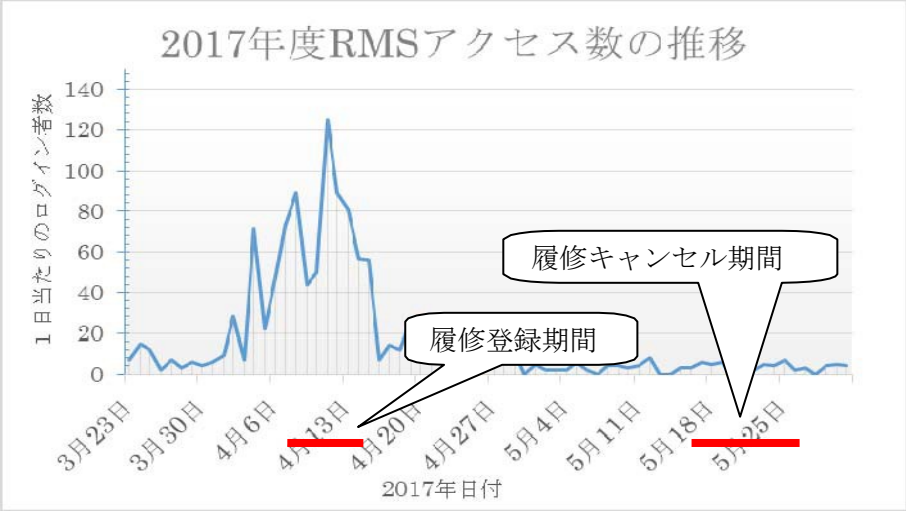


図２　ＲＭＳのユーザログイン数（2017 年度）

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．

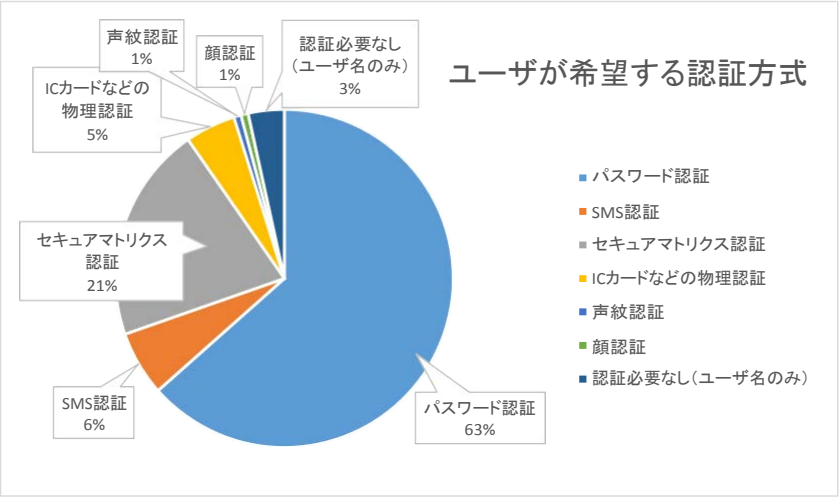


図３　ユーザが希望する認証方式（全ユーザ）

4.3　新認証方式の提案と今後の計画

現在，RMS はシステム再構築のためサービス停止中である．2018 年度より情報工学科のカリキュラム体系が一新され，上位学年との混在に対処できなかったことが一因であるが，カリキュラムツリーという概念がほとんど必要なくなったことなどから，システムのリプレースを行うことを決定したものである．新システムにおいては，次のような認証を組み合わせた方式を実装予定となっている．

・OAuth 認証による Twitter や Facebook との連携

・SSH で用いる公開鍵認証

例えば TwitterOAuth はアプリケーションに Twitter の投稿機能などを実装する場合に利用するライブラリであるが，これを用いれば Twitter アカウントを利用してシステムにログインすることが可能となる．SNS 利用者にとってはログインの手間が少なくなり，手軽にシステムを利用することが可能となる．一方で，ログイン済み端末の放置などによってその　他のサービスまで被害を受ける危険性もあるため，OAuth 認証単体での利用はセキュリティリスクもある．そこで SSH による公開鍵認証の技術を用いて端末を限定することを提案する．この認証方式では SSH や SCP でリモート接続を試みた際に，ユーザ ID とパスワードは使用せず，互いが持っている鍵を用いて認証を行う．具体的には SSH クライアントが持つ秘密鍵と SSH サーバが持つ公開鍵（これは SSH クライアントで生成したもの）を用いる．この方式を導入することでパスワードを入力することなくログイン可能となり，　パスワード総当り攻撃への頑健性も維持することが可能となる．

これらの方式の融合には解決しなければならない課題が多いが，新年度へのサービス再開を目標に開発を進めて行きたい．

５．研究成果の発表

とくになし．

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、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実際の情報セキュリティをめぐる問題事例――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。

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つ目の盲点は、技術開発者と実際の利用者の認識の「ずれ」である。例えば、時間軸に注目すれば、技術者が開発した新たなテクノロジーとその実用化までの時間は、それらを利用する人々が変化に対応するまでの時間と必ずしも一致せず、そこにタイムラグが生じうる。目を見張るスピードで進む技術開発は、緩やかに変化する利用者のセキュリティ意識を置き去りにし、技術者が当初（過去に）想定していなかったリスクを生起させる。こうした時間感覚の「ずれ」、すなわち、ICT の発展・拡張と、それに関わる人々の意識との乖離が、情報セキュリティに関する現実の危険性を高めるといえよう。

さらに、技術開発者と利用者の認識の「ずれ」を、空間軸から指摘するならば、技術開発者が想定する画一的な利用状況（均質的な利用者像）と多彩な利用者による様々な利用実態との「ずれ」が挙げられる。利用者は一様で均質的な存在ではなく、セキュリティに関する知識・意識・行動の面で様々な水準にある。こうした空間感覚の「ずれ」、多様な社会集団に対する技術開発者の認識の「ずれ」が、組織内セキュリティの盲点となってリスクを見落としてしまうといえよう。

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。次の「２．研究の必要性及び従来の研究」にて詳述するように、昨今ソーシャル・エンジニアリングの手口を用いたサイバー攻撃に対する国内外の被害拡大は、組織内情報セキュリティとして、「合理的で効果的なセキュリティ技術」という極めて工学的な対策に傾注するあまり、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（漸弱性）への対処が見過ごされてきたことが一因にある。さらに進めて言うならば、文系・理系のセキュリティ研究の断絶・乖離の状況とも相同的である。

そこで本研究では、ICT の進展が、利用者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、実態を調査し分析する。とりわけ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・研究することで、利用者の実態に即した、社会的要請に基づく組織内情

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資するものとするとともに、これまで組織内で一律に実施してきたセキュリティ研修の在り方などにも再検討の必要性を提起し、より効果的な組織内セキュリティの提案へとつなげたい。その際、時間軸（事前予防から事後対策への重心移動）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て、危機管理の今日的枠組みを提案することを目指している。

２．研究の必要性及び従来の研究

今年（2018 年）1 月に日本国内で、大手仮想通貨交換会社コインチェックが不正アクセスを受け、仮想通貨「NEM」580 億円相当が流出し、大きな話題となった。数か月にわたる取材を経て、5 月 12 日付の NHK-BS ニュースは、この前例のないサイバー攻撃の手口の詳細を報道した。それによれば、不正アクセスの足掛かりとなったのは、ウィルスが仕込まれたメールを社員が開いてしまったためであり、ソーシャル・エンジニアリングと呼ばれる、人間心理の隙を突いて、相手を信用させる詐欺の手口が用いられていたという。犯人は、求人情報サイトに掲載された同社のページから社員の写真・名前・肩書きなどの情報を集めて、複数のシステム管理技術者を割り出したと見られる。犯人は、それぞれの技術者に対して、SNS やメールを介して半年あまりにわたって偽名で交流を重ね、技術者たちの信用を得た。その結果、犯人が送ったウィルスを仕込んだメールを、疑うことなく開いてしまった、というのが発端になっているとされる。この手口は世界中で被害が相次いでおり、一昨年（2016 年）イラン政府の支援を受けたとみられるハッカー集団が、架空の女性写真家を騙ってアメリカの石油会社や通信会社などの社員と SNS で接触したことが、米国セキュリティ会社により報告されている。このハッカー集団は、1 か月以上 SNS で交流を深めた上で、ウィルス付きのファイルを開かせる攻撃を行ったと同社は分析している。

今回のコインチェック社の事例は、周到に行われた新たな標的型攻撃であり、今後は日本でもソーシャル・エンジニアリングを用いた同様の攻撃が急増すると指摘されている。怪しいメールを開かないという個人の主観に依拠した対策だけでは、もはや組織内セキュリティを守ることは困難であり、攻撃を受ける（危険に晒される可能性がある）ことを前提として対策を講じる必要があるとの注意喚起がなされている。言い換えれば、ソーシャル・エンジニアリングを用いたサイバー攻撃に対しては、組織内の個人的な注意や事前の予防という既存の対策だけでは防御が困難であり、詐欺的な手口に対する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といえよう。

このように、求人・広報活動のために公開した企業情報が、ソーシャル・エンジニアリングに用いられ、サイバー攻撃に利用され始めている。しかし、既存のセキュリティ研究では、個人の SNS 利用や組織の求人・広報活動は、セキュリティ「技術」の開発（理工系）とは関係の薄いものとして、情報「モラル」の問題（人文社会系の研究領域）として扱われることが多かった。文系・理系という棲み分けや各々の専門分化した既存研究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

といえよう。

３．期待される効果

本研究は、時間軸および空間軸における認識の「ずれ」がリスクを生むという理論的な視点から現象を体系的に把握することで、個別の事例としてではなく、その問題構造に注目することを可能にする。

例えば、先述したソーシャル・エンジニアリングについても、次にように位置づけることができる。「突然の（短時間での）」「見知らぬ相手（未知の領域＝空間からの相手）」からのメールであれば当然、警戒するものである。しかし犯人は、半年という長い「時間」をかけて交流を重ねることで、未知の危険な外部ではなく安全な内部（安心できる身内）という「空間」に属する人であると、相手の「認識」を変えさせ警戒心を解かせている。さらに、交流開始時に収集した情報は、就職希望者に向けて自社の社員の活躍を分かりやすく紹介した求人情報サイトのものであり、ここでも「将来の新入社員（身内）」となりうる就職希望者に向けて、仲間内での「空間」感覚で組織内の情報を掲載している（もしも、求人情報サイトもまた、組織を攻撃するハッカーたちの目に晒されているという意識があれば、システム管理技術者たちの顔写真や個人名は掲載しなかったかもしれない）。

ここから導出される新たな視点は、セキュリティ対策を実施する組織の内部においてもまた（セキュリティ研究を行う文系・理系のように）、部署ごとに棲み分けや細分化が進んでおり、組織内の情報共有が難しいこと、そして同一組織であっても内部の部署ごとに、セキュリティに関する意識・知識・行動が異なることである。他方で、ソーシャル・エンジニアリングの手口として、今回のケースと逆の方向を検討してみると、「空間」のつながりを経由することで「短時間」に警戒心を解かせる手法が考えられる。つながりを可視化 した SNS をたどって、標的とした相手の友人や家族と親しくなり、身内（安心安全な集団） である友人や家族を紹介してもらうことなどが考えられる（在学生や文科省から大学宛に 届くメールも、就職希望者や業者を騙って企業宛に届くメールも、「つながり」が合理的に推認されるだろうことに注目した同様のソーシャル・エンジニアリングといえる）。

加えて、現在進行形で変化・発展するハッキングの手法やソーシャル・エンジニアリングの手口を「事前に警戒する」ことには限界があり、ウィルス感染の直後・問題発覚後の「事後の迅速な対応」が、組織のセキュリティにとって実効的なものであることが指摘できる。

４．研究の経過及び結果

H29 年度には、前年度までの研究成果（大学生に対する H26、H27、H28 年度の 3 度の調査結果）を踏まえて、「情報セキュリティに関する実際の行動は、回答者のセキュリティ意識や知識と、また回答者の属性や勤務先と、どのような関連性があるか」について、11-12 月にかけてリサーチ会社と打ち合わせを重ねて全国調査を実施した。全国調

査では、まず人々のセキュリティ意識・知識・行動を尋ねる予備的調査として全世代 2 万人に調査を実施し、次に本調査として組織に所属する勤労者（会社員・公務員）2,000 人に対し、上述の意識・知識・行動に加えて、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。調査データは現在も引き続き詳細を解析中だが、これらの調査結果は、社会学的知見（ハビトゥス論）に基づく仮説を支持するものであった。詳しく見ると、大学生に対する既存調査と異なる側面（セキュリティ意識や知識と、実際の情報セキュリティに関する行動との間に関連性が認められる点）と、一致する側面（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点）とが認められる。また、利用者の性別や年齢、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、学歴等）によって、セキュリティ意識・知識・行動に興味深い差異が見られる（例えば性別は、知識に強い影響を、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い。知識＝関心領域に性差があることは既存のジェンダー研究でも指摘されて久しいが、知識が意識に弱い影響を及ぼすものの、行動とは有意差が算出されない、すなわち行動は性別などの属性よりも社会的環境からの要因が大きい）等、新たな知見も得ることができた。さらに、所属する組織の規模や被害経験の有無などの間にも関連性を見出しており、組織内情報セキュリティの向上に資する提案につながるようまとめている。

５．今後の計画

H29 年度に実施した全国調査データの詳細を解析し、人々の情報セキュリティに関する知識・意識・行動に関して得られた実証研究の知見を社会学のハビトゥス論に立脚して分析・考察して、研究成果をまとめる。これらの研究成果を、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）。また、本研究で「セキュリティと教育」「セキュリティ管理手法」「情報漏洩防止」「生体個人認証」を担当する共同研究者と意見交換をし、各領域での研究成果を踏まえて、H30 年度には新たに「組織内セキュリティの実態」を尋ねる全国調査を実施する（その際は、調査対象者の標本抽出方法にも配慮し、高齢化の進む人口構成比を反映する方法を検討する）。調査結果によって明らかとなる国内組織の現状と問題点を、共同研究者と共有して各自の研究に取り入れてもらうとともに、「セキュリティと社会」の研究領域として、組織への ICT 導入がもたらす人々の認識図式や行動様式の変容をハビトゥス論に立脚して解明することを試みる。これにより、「全体システム設計」に貢献する効果的な組織内情報セキュリティ対策の提案へとつなげる。

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（2017,08,01），神奈川工科大学（国内研修での招聘講義）.