神奈川工科大学

セキュリティ研究センター研究報告

第4巻

2016

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

すべてのモノがインターネットにつながる「IoT 時代」は，大量に集積されたデータから新たな大きな価値を生み，私たちの生活を変革する原動力となります．我々の日常生活が益々インターネットに依存していく中で，サイバー攻撃は日々巧妙化し進化している．そこで， 想定外の新たなリスクが生まれることとなり，様々な脅威に対してあらゆるサイバーセキュリティ対策を漏れなく講じなければならない．

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 27 年度は，学内重点配分研究として 2 つの研究テーマ「安心・安全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 4 巻（2016）目次

安心・安全な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，第三者による覗き見やカメラなどによる録画攻撃によるモバイル端末の認証情報の流出を避けるための新たな認証方式の研究開発について検討する．そこで，従来のパスワード認証方式にユーザが親しみやすいパズルやリズムなどの要素を付加して，モバイル端末の画面上を複数の指でタップすることによって高いユーザビリティを有し，年代・職種などを問わずに誰でも人の目にさらされる環境でも安心してクラウドサービスを利用でき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，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ショルダーハッキング攻撃を受ける問題がある．そこで，本研究では，利用者が鞄やポケットの中などに端末を入れたまま画面を見ずに認証情報を入力できるリズム認証方式について検討している．本認証方式を実現することで，認証画面を録画されることはなくなる．特に，ユーザは自分が好きなリズムをパスワードとして登録でき，画面上を複数の指でタップして操作するという扱いやすい入力方式によって高いユーザビリティを有し，認証動作を他人に見られたり，カメラなどの録画機器に録画されたりしても認証情報が露呈しない新たな認証方式を開発し実現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，今年度は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[1, 2, 3]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．

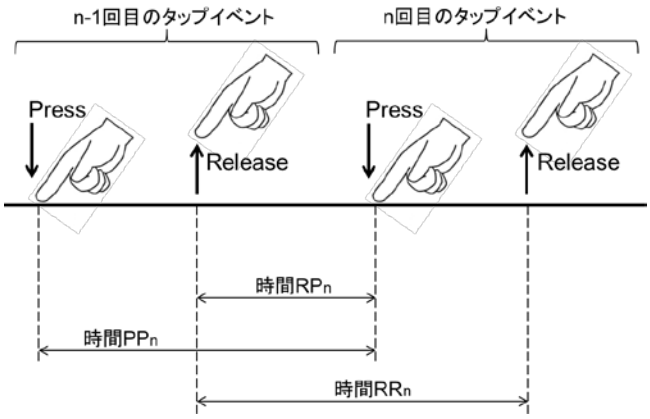


図 1．リズム認証におけるタップ時間

以下では，今年度の本研究の基本となるリズム認証方式について報告する．

4.2　リズム認証方式

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する．また，従来手法による FRR および FAR の低減を考慮し，全ての特徴のうち利用者本人の再現率が高い特徴，および，他人との特徴量の差が大きい特徴をそれぞれ挙げ，それらの特徴量から成る複数の SOM を用いることで更なる認証精度の向上を目指す．

図 2 に，本提案方式における認証情報登録および認証の手順について示す．モバイル端末は個人で所有している場合が多く，複数のユーザで 1 つの端末を共有することは少ない．そのため，ユーザは端末 1 台につき 1 名であることを想定する．認証情報の登録では，ユーザが端末上でタップした認証情報はサーバへ送信され，サーバで SOM を作成する．SOM を作成した後，SOM 情報を端末へ送信し，登録は完了する．サーバで SOM を作成する理由として 2 つ挙げられる．まず，SOM 作成の膨大な処理への対応である．SOM の処理をモバイル端末上で行うには負荷が大きく，端末の動作が不安定になることが考えられるため，処理能力が高いサーバで SOM を作成する．次に，端末間での認証情報の共有によるユーザの負荷軽減がある．複数台の端末を有するユーザが各端末上で本人認証を行う際，

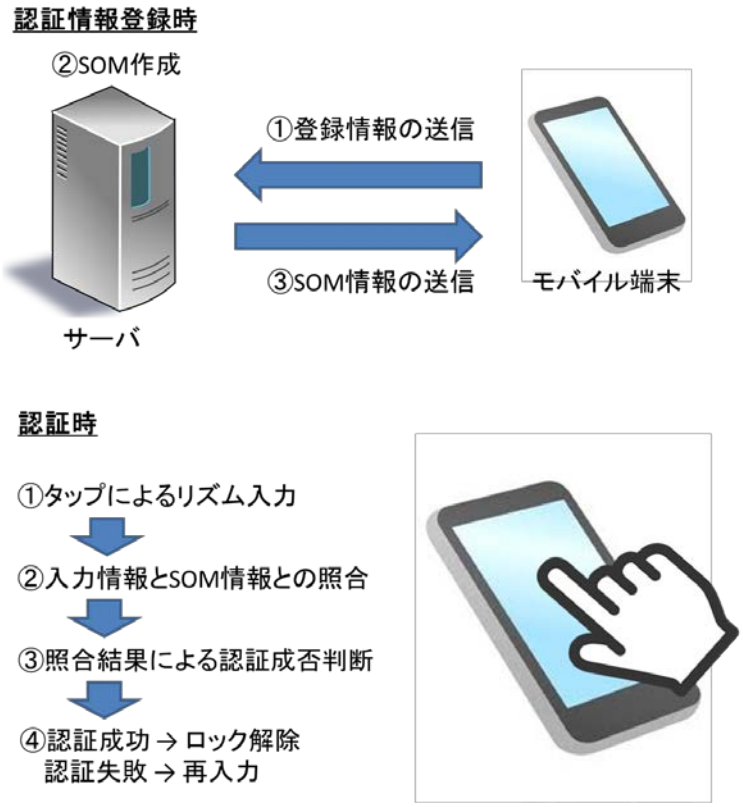


図 2．認証情報登録および認証手順

ユーザ本人の既存 SOM を端末へ送信して認証情報を共有することにより，各端末で認証情報の新規登録や変更を行う必要がなく，普段通りに認証を行うことができる．これによりユーザは，新たに認証情報を覚えたり，複数の認証情報を管理したりする必要がない．

認証時では，まず，ユーザは端末上をタップしてリズムを入力する．次に端末内では，入力情報と SOM とを照合し，入力情報の勝利ノードと近傍領域の中心とのユークリッド距離を求める．そして，その距離が予め定義した閾値内であるか否かによって認証の成否を判断する．認証が成功した場合は画面ロックを解除し，失敗した場合はユーザに対し再度入力を求める．

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] Yoshihiro Kita, Mirang Park, Naonobu Okazaki, " Proposal of Rhythm Authentication Method using Users Classification by Self-Organizing Map," International Conference on Network-Based Information Systems(NBiS2015), pp665-668，2015.

[2] 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 “録画画像を用いた攻撃に耐性を持つパズル型認証方式の一検討”，IPSJ IOT/SPT 研究報告, 2015.09.

[3] 堀 孝浩，喜多 義弘，豊田 健太郎，朴 美娘，岡崎 直宣，"「テンポ感」を特徴量としたリズム認証の認証精度に関する考察," 情報処理学会コンピュータセキュリティシンポジウム（CSS2015）論文集, pp.779-786, 20151022.

[4] N. Okazaki, K. Toyoda, E. Yokoyama, H. So, T. Katayama, and M. Park "Countermeasure against fingerprinting attack in Tor by separated contents retrieval," IEICE ComEX, Vol.4, No.12, pp.370-375, 2015/12.

[5] N. Okazaki, Y. Kita, K. Aburada, and M. Park, "Security Evaluation System for Android Applications Using User's Reviews and Permissions," Journal of Robotics, Networking and Artificial Life, Atlantis Press, Vol.2, No.3, pp.190-193, 2015/12.
[6] 油田健太郎，山場久昭，片山徹郎，朴美娘，岡崎直宣，"Winny ネットワークにおけるクラスタリングを用いたインデックスポイゾニングシステムの実装と評価," 情報処理学会論文誌，推薦論文，Vol.56, No.12, pp.2395-2405, Dec. 2015.
[7] 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.
[8] 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.
[9] 岡崎 美蘭 “安全な M2M 通信システムを実現するためのグループ鍵管理手法に関する一考察”，神奈川工科大学 研究報告 B 理工学編，第 40 号, (2016.03)

(2) 学会発表

[1] 陳 致豪，豊田 健太郎，朴 美娘，岡崎 直宣，"M2Mにおいてｋ平均法を用いたグループ鍵管理端末の効率的な配置手法," 情報処理学会コンピュータセキュリティシンポジウム（CSS2015）論文集，pp.78-85, 20151021.
[2] 板倉尭史，喜多義弘，朴美娘，岡崎直宣,"マウスの操作軌跡を用いた個人認証システムにおける機械学習による判定法に関する考察," IEICE バイオメトリクス（BioX）研究報告，Vol.115，No.266，pp.43-46, 2015.10.
[3] 立田怜平，山場久昭，久保田真一郎，朴美娘，岡崎直宣 “マウストラッキングを用いたCAPTCHA方式の検討”，IPSJ 火の国シンポジウム 2016, 20160302
[4]富田施，横山絵美里，宗裕文，山場久昭，久保田真一郎，朴美娘，岡崎直宣 “匿名通信システムにおける指紋攻撃の対策に関する一検討”，IPSJ 火の国シンポジウム 2016, 20160302
[5]横山絵美里，平田木乃実，宗裕文，山場久昭，久保田真一郎，朴美娘，岡崎直宣 “匿名通信システムにおける複数経路を用いた指紋攻撃対策手法に関する一検討”，IPSJ 火の国シンポジウム 2016, 20160302
[6]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
[7]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

(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

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

研究者名：情報工学科　　納富　一宏，　松田　三知子

１．研究の目的

本研究全体の目的は２つのフェーズから構成される．第１フェーズは組織内情報システムの構成要素に関連した危機管理に焦点をあて，広範囲に渡る脅威や脆弱性から情報資産を守るべく，インターネット社会におけるセキュリティモデルを考案することである．第２フェーズは組織内情報システムの技術面，運用面，管理・監査面に焦点をあて，セキュリティモデル高度化の手法開発に資する適用可能技術を提供することである．なお，第１，第２フェーズ共に，インターネットを情報基盤とする高度グローバル化社会における「安全安心な社会の形成」という統一目標を掲げている． 平成 27 年度は，H26 年度までの研究目的・方針を継承し，研究成果の集積を果たしながらスパイラルアップを意識した取り組みを実践した．特に，「セキュリティと社会」「情報漏洩防止」「生体個人認証」という３つの観点からの研究成果をベースとして，セキュリティモデル全体を汎化（generalize）することで，組織内情報セキュリティモデルの適用可能性を高めることを目指した．

◎ 情報セキュリティモデルへの要求

情報セキュリティマネジメントシステム（ISMS）への要求事項を定めた規格：JIS Q 27001:2014 では，「ISMS は，リスクマネジメントプロセスを適用することによって情報の機密性，完全性及び可用性を維持し，かつ，リスクを適切に管理しているという信頼を利害関係者に与える」と規定している．

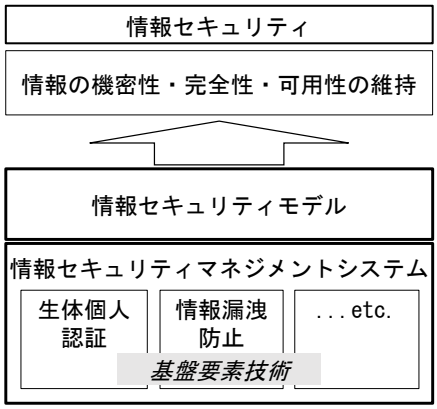


図１．情報セキュリティモデルの位置付け

組織のマネジメントとして自らのリスクアセスメントにより必要なセキュリティレベルを決めて資源を配分して，システムを運用することである．図１に示すように，情報セキュリティマネジメントシステムは，組織のリスクアセスメントに基づいたセキュリティモデルにしたがって構成される．高度な情報セキュリティの実現には，情報セキュリティモデルの高度化が必要である．その高度なセキュリティマネジメントシステムの実現には，精度の高い基盤要素技術，例えば，生体個人認証技術，情報漏洩防止技術などの開発が重要なこととなる．

２．研究の必要性及び従来の研究

一般に情報システムを考えるとき，各分野ごとにあるシステムを統合する形の水平的な全体システム化をする場合が多いが，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，「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の垂直的な情報セキュリティモデル構成法を用いている．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．また，既存研究では人文社会系と理工学系の研究の間には障壁があるが，本研究では他の研究者との共同により，学際的・横断的な研究を目指している．

現在では技術面だけではなく，運用面を含めた管理・監査面からの情報通信システムの研究が必定な段階に達していると言える．企業や組織の機密情報漏洩や国外からのサイバー攻撃など，今日では，情報セキュリティに関する話題がニュースのヘッドラインを賑わせており，本学においても，情報セキュリティポリシーを定め，情報セキュリティの管理運営体制の維持に努めている．これらの背景を踏まえたうえで，より具体的な視点に立った，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の高度化に向け，「セキュリティと社会」「生体個人認証」「情報漏洩防止」という３つの重要な観点において研究を遂行した．今後，各研究成果を包括した先進的なシステム提案に向け，戦略的な取組みを意識すると共に，安全性と快適性の両立的整備を図っていくことが課題となる．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

情報システムにおける個人認証は，従来，パスワードやパスフレーズと呼ばれるキーを扱うが，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．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）技術が注目されている．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．図 2 に示すようなニューラルネットワーク等の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している．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し，最終的にはインタラクティブな認識技術を用いて，継続的な生体個人認証（Continuous Biometric Authentication）の確立を目指すことで，巧妙ななりすましへの対応が期待できる．

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．H27 年度に実験および評価を行った特徴量としては，声紋，タッチ動作，デバイス保持動作，図形手書き動作であり，いずれも行動的特徴量をベースとしており，概ね 85～95%程度の認証精度が得られた．H26 年度までの身体的特徴量をベースとする方式に比べて精度が向上した．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，そのためにはさらなる研究が必要である．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．このため，統合的な精度向上を目指すことが可能であると考える．また，これまでの研究から，今後はクラウド・サーバー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．これまで検討してきたシステム監査に資する情報提供機能の搭載は，企業内情報システムにおける生体個人認証技術の導入と同様に重要な課題である．現在，経済産業省の「情報セキュリティ監査基準」における「一般基準」,「実施基準」,「報告基準」の３基準に適合するための検討を行っている．今後は，生体個人認証機能を搭載した企業内情報システムにおいて，現在検討中の情報提供機能の統合化の推進が必要である．

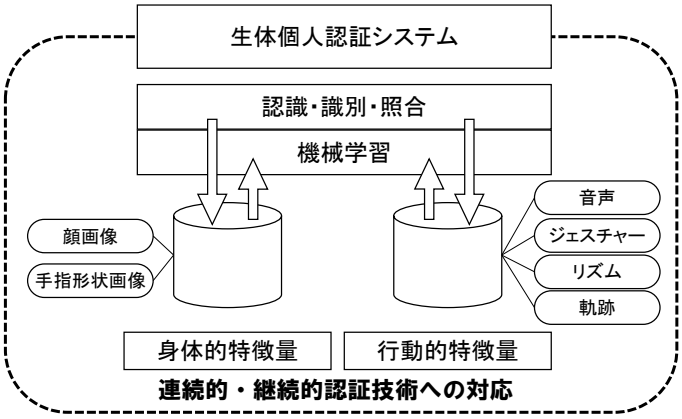


図２．生体個人認証システム

５．今後の計画

今後も組織内情報システムにおける危険度分析およびセキュリティ確保手段および監査手順に関する統合化を目指した検討が重要である．したがって，組織内において各個人がデータベースにアクセスする様々なユースケースを具体的に挙げて，その中で情報漏洩の危険性があるポイントとその危険度分析の継続が必要である．さらに，各ポイントにおいて適用可能な生体個人認証手法とその有効度を検討する．その後，これらの検討結果に基づいて，組織内情報セキュリティモデルをボトムアップ的に構成する．最後に，構成した情報セキュリティモデルをシステム監査の視点から，トップダウン的に検証する．

生体個人認証に関しては，これまでの経験により得られた，ラピッドプロトタイピングおよびアジャイル開発手法をさらに強化することで，実装・評価プロセスを効率化し，システムの精緻化と評価実験を通した検証を行って，一層のセキュリティの高度化を図る．具体的には，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」「ピンチイン／ピンチアウト」「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の形状を認識する「掌指形状認証」，③スマートフォンに搭載されているジャイロセンサ・加速度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不特定話者による音声認識技術とメル周波数ケプストラム係数（MFCC：Mel-Frequency Cepstrum Coefficient）を活用した「音声認証」，⑤顔追跡（face tracking）技術を活用し，継続的に認証を行う「継続的顔認証」の５種類について継続実施する．また，高齢化社会における幅広い年齢層へ対応可能な方式として，「画像有意性効果（picture superiority effect）」を用いた認証方式についても検討を進める．

６．研究成果の発表

[1] 星野裕樹*, 納富一宏, 斎藤恵一:"ピクチャーパスワードへの行動的特徴量付与による生体認証手法の実用性評価", バイオメディカル・ファジィ・システム学会誌, Vol.18, No.1, (7pages), (2016.06 発刊予定) [掲載決定 2016.03.03].

[2] 河合博之*, 納富一宏, 斎藤恵一:"画像優位性効果を用いた音声認証システムの実装", 電子情報通信学会 2016 年 総合大会 A-18-5, 基礎・境界講演論文集, p.246, (2016.03).

[3] 河合博之*, 納富一宏, 斎藤恵一:"画像優位性効果と連想語を用いた音声認証における「なりすまし」の評価", 電子情報通信学会 技術研究報告 Vol.115 No.493, マルチメディア・仮想環境基礎研究会 (MVE), IEICE-IMQ2015-71, IE2015-170, MVE2015-98 (2016-03), pp.243-244, (2016.03).

[4] 河合博之*, 納富一宏, 斎藤恵一:"音声認証システムへの画像優位性効果の適用", 電子情報通信学会 技術研究報告 Vol.115 No.351, 技術と社会・倫理研究会(SITE), IEICE-SITE2015-51, ET2015-79 (2015-12), pp.59-64, (2015.12).

[5] 星野裕樹*, 納富一宏, 斎藤恵一:"ピクチャーパスワードへの行動的特徴量付与による生体認証手法の評価", バイオメディカル・ファジィ・システム学会 第 28 回年次大会講演論文集, pp.85-88, (2015.11).

[6] 河合博之*, 納富一宏, 斎藤恵一:"画像優位性効果を利用した連想語による音声認証システムの評価", バイオメディカル・ファジィ・システム学会 第 28 回年次大会講演論文集, pp.89-92, (2015.11).

[7] 田所龍介*, 納富一宏:"顔追跡による継続認証システムの構築", 情報処理学会 第 14 回情報科学技術フォーラム(FIT2015)講演論文集, 第 3 分冊, J-010, pp.331-332, (2015.09).

[8] 河合博之*, 納富一宏, 斎藤恵一:"画像と連想語を用いた音声認証システムの開発", 情報処理学会 第 14 回情報科学技術フォーラム(FIT2015)講演論文集, 第 4 分冊, L-007, pp.179-180, (2015.09).

[9] 河合博之*, 納富一宏, 斎藤恵一:"画像からの連想語を用いた音声認証手法の検討", 電気学会 平成 27 年 電子・情報・システム部門大会 OS2-1, pp.597-600, (2015.08).

(*：発表当時，本学学生)

安心・安全な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（情報ハイディングに関する研究）

情報ネットワーク・コミュニケーション学科　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等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を得る手法である。なお、本研究では周波数変換として DWT を利用した。DWT は近年信号処理の分野で注目されている変換であり、情報ハイディングの分野においても、その利用が盛んに検討されている変換である。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。通信分野におけるスペクトル拡散方式において、情報伝送速度を向上させるために M-ary 方式というものが提案されている。これは、複数の拡散系列を使用することにより、拡散系列の選択にも情報を載せる方式である。この M-ary 方式を情報ハイディングに応用すれば、埋め込み可能な情報量を増加させることが可能となる。しかしながら、M-ary 方式を用いると、埋め込み可能な情報量は増大するが誤り率特性は一般に劣化し、結果としてコンテンツの品質劣化をもたらす。情報ハイディングの分野における M-ary 方式に適した拡散系列の条件としては、①真の乱数に近い性質を持つこと、②+１と－１の要素数が等しいこと、③異なる拡散系列間の内積が 0 であることがあげられる。そこで筆者らは、M 系列を元にして M-ary 方式に適した拡散系列の構成方法を提案した。提案した構成方法においては、拡散系列の長さが 2^n である場合、拡散系列の個数は 2^{n-1} となる。昨年度までの研究成果により、提案した拡散系列を M-ary 方式に適用した場合、2^{n-1} 個全てを使用しても透かし情報を正しく復元可能であることが確認されている。しかし、提案した拡散系列と単純な疑似乱数を比較した場合、画質劣化の観点からどの程度の改善効果があるのかについては明らかにされていない。そこで、本研究では、提案した拡散系列と単純な疑似乱数を用いた場合に必要となる強度の比較を行い、提案した拡散系列がどの程度の改善効果を持つのか定量的に検討を行う。

２．研究の必要性及び従来の研究

一般に、相関利用型の情報ハイディングにおいて埋め込む情報量を増大させるためには、使用する拡散系列を小さくする必要があるが、拡散系列を小さくすると、情報を埋め込む際の強度を大きくする必要があり、結果として著しい画質の劣化を招いてしまう。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るが、通信分野におけるスペクトル拡散方式において、情報伝送速度を向上させるために、複数の拡散系列を用いる M-ary 方式が提案されている。この M-ary 方式を情報ハイディングに応用すれば、拡散系列を小さくすることなく埋め込み可能な情報量を増加させることが可能となる。従来、M-ary 方式の相関利用型情報ハイディングとしては、通信分野のスペクトル拡散方式において研究されている拡散系列を用いたものが提案されている。しかし、情報ハイディングの分野において拡散系列に求められる条件と通信分野において拡散系列に求められる条件は必ずしも一致するものではない。したがって、情報ハイディングの分野における M-ary 方式に適した拡散系列を研究することが必要とされている。そこで、筆者らは M 系列を元にして情報ハイディング分野における M-ary 方式に適した拡散系列の構成方法を提案したが、画質劣化の観点から見てどの程度の改善効果があるのかについては明らかにされていなかった。したがって、提案した拡散系列を M-ary 方式に適用した場合において、画質劣化の改善効果を明らかにすることが必要とされている。

３．期待される効果

M-ary 方式の相関利用型情報ハイディングにおいては、複数の拡散系列を使用することにより、拡散系列の選択にも情報を載せることで、拡散系列を小さくすることなく埋め込み可能な情報量の増大を実現している。しかし、埋め込んだ情報を読み出す際には、どの拡散系列が使用されているのかを区別する必要があるため、使用する拡散系列の個数を増やすと、すなわち埋め込み可能な情報量を増やすと、透かし情報を埋め込む際に必要となる強度が増加し、結果として画質の劣化を招いてしまう。このように、一般的には埋め込み可能な情報量と画質はトレードオフの関係にある。したがって、埋め込む情報量が同じである場合、透かし情報を埋め込む際に必要となる強度は小さければ小さいほど良いということになる。提案した拡散系列の強度に関する改善効果を明らかにすることにより、提案した拡散系列が画質劣化の観点から M-ary 方式を用いた相関利用型情報ハイディングに適していることが明らかになると期待される。

４．研究の経過及び結果

情報ハイディングの分野における M-ary 方式に適した拡散系列の条件としては、①真の乱数に近い性質を持つこと、②+１と－１の要素数が等しいこと、③異なる拡散系列間の内積が 0 であることがあげられる。相関利用型電子透かしでは、画像の要素をランダムに正

または負に変換することにより、これらの合計値が 0 に近い値となって埋め込んだ透かし情報のみが検出可能となる。このため、①の条件が必要とされる。また、画像の要素をランダムに正または負に変換したとしても、正または負となる要素数に偏りがある場合は、合計値が 0 に近い値とならない。このため、②の条件が必要とされる。最後に、M-ary 方式では、埋め込んだ透かし情報を読み出す際に、全ての拡散系列と透かし情報を埋め込んだ画像の要素との積を計算し、その合計値の絶対値が一番大きいものを使用された拡散系列であると判定する。画像の成分を無視して考えれば、これは全ての拡散系列と埋め込み時に使用した拡散系列の内積を計算し、その絶対値が最も大きいものを探していることに等しい。実際には、画像の成分が雑音として作用するので、異なる拡散系列間の内積は 0 に近いことが望ましい。このため、③の条件が必要とされる。そこで、筆者らは、M 系列を元にして、上記の三つの条件を満たす M-ary 方式に適した拡散系列を提案した。M 系列は代表的な疑似乱数であり、真の乱数に近い性質を持つことを持つことが明らかにされている。また、1 と 0 の要素数に関しては、0 の要素数が 1 の要素数よりも 1 つ少ないだけで、ほぼ同数と言える。さらに、要素 0 を+1 へ変換し、要素 1 を-1 へ変換した場合、同じ原始多項式から得られる初期値の異なる M 系列間の内積は-1 となることが明らかにされている。これらの性質を元に、筆者らは、M-ary 方式の相関利用型電子透かしに適した拡散系列を提案した。提案された拡散系列の構成方法は以下の通りである。

1. 同じ原始多項式から得られる初期値の異なる M 系列を複数用意する
2. それぞれの M 系列において要素 0 を+1 へ変換し、要素 1 を-1 へ変換する
3. それぞれの M 系列の最後に要素として+1 を追加する

M 系列の最後に要素として+１を追加するので、+1 と-1 の要素数は最終的に等しくなる。また、最後に+1 を要素として追加したことにより、異なる拡散系列間の内積は 0 となる。なお、最後に+1 を追加したため、提案する拡散系列は純粋な M 系列ではないが、ほぼ M 系列そのままであるので、疑似乱数としての良好な性質もほとんど失われていないと推測できる。提案した構成方法においては、拡散系列の長さが 2^n である場合、拡散系列の個数は 2^{n-1} となる。昨年度までの検証結果より、拡散系列の個数を 2^{n-1} とした場合においても、問題なく情報が復元できること、また拡散系列の個数を増やした場合も必要となる強度はあまり増加しないことが明らかとなった。したがって、提案した拡散系列においては、構成可能な 2^{n-1} 個を全て使用して埋め込む情報量を増加させても、画質はそれほど劣化しないと言える。そこで、本年度の研究では、提案した拡散系列と単純な疑似乱数を用いた場合において、拡散系列の大きさが同一・拡散系列の個数が同一（埋め込み可能な情報量が同一）という条件のもとに、必要となる情報量の比較を行った。結果より、拡散系列の大きさ、および個数によって違いはあるものの、全体として提案した拡散系列は単純な疑似乱数よりも数%程度、必要となる強度が小さくなることが明らかとなった。

５．今後の計画

検証より、提案した拡散系列と単純な疑似乱数を比較した場合、必要となる強度に関して数%程度の改善効果が確認された。しかし、この強度に関する改善効果が、人間が知覚できる程度の画質の改善につながるのかについては明らかとなっていない。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。また、ディジタル画像は圧縮されて用いられることが多いため、JPEG などの圧縮形式で使用した場合においても、提案した拡散系列が問題なく使用でき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。

情報漏洩防止に向けての研究

研究者名： 情報ネットワーク・コミュニケーション　　岡本 学

１．研究の目的

情報セキュリティの分野では政府機関・企業等での情報漏えい問題の発生を受けて、その防止策の検討が行われている。情報の漏洩を防止する基本技術としては、ユーザの本人確認を厳密に実施する「認証技術」がある。現状では認証技術としてパスワード方式がもっともよく用いられているが、パスワード方式には忘却の問題や推測アタック、更にはフィッシングといった新手の攻撃まで発生している。そこでこれらの課題の解決を目的として、パスワード方式以上に確実に本人確認が実行できる「強い認証」が必要となってくる。本研究では、様々な攻撃者を想定し、安全安心なサービス提供に向けて、新たな本人確認手段・認証方式の提案を行う。

２．研究の必要性及び従来の研究

本人確認に用いられているパスワード方式はもっとも導入が簡単で、誰にでも簡単に利用できる一方で、背後から覗き見ることによりパスワードを盗んだり（ショルダーハッキング)、本人の名前や誕生日からパスワードを推測されたり、フィッシングといって偽ホームページにパスワードを入力させることで盗んだりと、様々な攻撃手法が存在する。かといってパスワードを長く難しいものにしてしまうと、本人である自分が忘れてしまうという問題が発生し、単純にパスワード方式の中だけで解決するのは難しくなっている。

そこで新たな「強い認証」が求められている。しかし「強い認証」を実現するにも様々な課題がある。たとえば「指紋認証」を採用することでパスワード方式以上の安全性を得ることができる一方で、指紋読み取り機器の準備が必要であったり、指紋の登録作業や不具合時の対応が必要であったり負担が大きい。そのためユーザが手軽に利用でき、サービス提供側にも負担が少ない形の「強い認証」が必要となる。

３．期待される効果

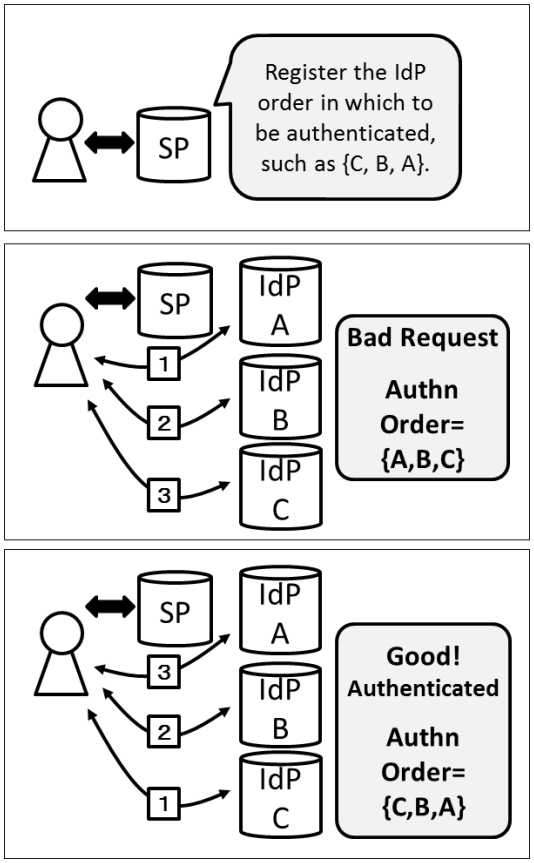
「強い認証」が簡単に実現できることで、サービス提供者は個人情報や金銭に関わるサービスを安全安心に提供できるようになる。またユーザにとっても、個人情報の漏洩や、パスワード等の認証情報の盗難によるなりすましの被害にあわなくてすむようになり、これもまた安全安心にサービスを利用できるようになる。また認証の「簡易化」は、認証に特殊な機器が必要なかったり、運用・管理コストを下げることができたりと利点が多い。

さらに認証をマルチサインオン化、つまり複数の認証を突破して初めて本人として認められる方式を採用することで様々な認証方式を複数組み合わせて自由にその強度を上げる

ことが可能となる。特にマルチサインオンにおいて認証情報を流通させる方式に標準仕様を用いることでより自由度の高い認証方式に発展させることが可能となる。

４．研究の経過及び結果

２７年度は複数のサーバで認証を受けることで初めて利用できるようになる「マルチサインオン」のセキュリティ強度を更に上げた「順番マルチサインオン方式」の研究を行った。この方式では、単純に複数の認証サーバで認証を受けるだけでは認証完了せず、事前に登録した通りの順番で各認証サーバから認証を受けなければ最終的な認証が成功しない方式である（下図参考)。



参考図：順番マルチサインオン

この方式ではすべての認証サーバでパスワード方式が採用され、更にすべてのサーバでパスワードが盗まれた場合においても、この正しい順番が盗まれない限り、攻撃者は最終的な認証を突破することができない。認証を受ける順番をある程度の回数間違えたらアカウントロックをすることで、全件アタックにも対処できる。２７年度は本方式の基本案を下記発表文献[1]にて発表した。

加えて、「認証サーバ」よりもっと簡易に、単純に事前登録したサイトに順番に訪問した

「訪問履歴」を最終的な認証に利用する方式についてもあわせて研究を行い、下記発表文献[2]にて発表を行った。

なおどちらの方式においても、認証情報の流通には、シングルサインオン技術である OpenID を採用することで、認証プラットフォームとして誰でも利用できる方式となっている点もまた大きな特徴である。

５．　今後の計画

今後はさらなる「強い認証」に向けて、方式の多様化を行う。順番マルチサインオンではある程度のセキュリティ強度を守ることが可能だが、キーロガー等ですべての操作記録が保存され盗まれた場合、簡単にその順番を割り出すことが可能となってしまう。この課題に向けてキーロガーに強い認証方式の追加が必要となる。また単純に「認証サーバで認証を受ける」「特定のサーバを訪問する」だけではなく、これら各訪問行為に対し細かいポイントを付与し、ユーザはそれらポイントが与えられたページを渡り歩いてポイントを稼ぐことで最終的な認証をクリアする「ポイント制度」の追加採用も今後の検討課題である。

６．　研究成果の発表

[1] Yuki Kumazawa, Akane Ito and Manabu Okamoto, “Authentication with Plural Servers in the Correct Order ”, IEEE Security and Privacy 2015, San Jose, USA, 2015.5.

[2] Chisa Kuroda, Mizuki Kobayashi, Mioko Watanabe and Manabu Okamoto, “Authentication by web browsing history”, IEEE Security and Privacy 2015, San Jose, USA, 2015.5.

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。

27 年度の課題としては、26 年度までに考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、複数のカメラを利用して高精度に移動するカードの位置を検出する技術を開発することを目的であった。

加えて、さらなる高精度な認証技術を確立するため、紫外線画像による傷画像の分析を行い、これまで開発してきた赤外線を利用した認証技術と組み合わせることができないかについて検討を行った。

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、対応機器が未だすべての 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。

26 年度までに理想環境における提案手法の有効性を確認し、実証実験をかさねてきた。しかし、実際の認証システムとしての利用価値を高めるためには、首からぶら下げられた社員証のようなカードに対して、通路を通りながらカード位置を特定し、開発した認証方式を実現できるようにすることが有効である。これは、降格に撮影された物体の移動を高精度に解析する技術であり、多方面での応用が可能な画像処理の基盤技術の開発であるといえる。

さらに、紫外線情報を利用することで、カード表面の傷情報を高精細に取得することができ、完全に複製・偽造されたカードであっても、登録されたカードと同じ傷の情報を持っているかどうかによって高精度な真贋認証を可能にする技術に発展させることができる。この技術も、３次元スキャナや３次元プリンタが普及し、完全な形状コピーが容易になる近い将来に、物体形状の照合を利用した認証を有用に保つために不可欠な技術になると考えられる。

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。

27 年度までに、基盤バイオメトリクス認証方式を確立し、物体移動を高精度にとらえる技術と紫外線による傷認証技術の基礎を、実験を通して確認した。

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 年度まで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。

５．今後の計画

物体移動の高精度なトラッキング技術を、通路天井に設置された複数カメラから得られた情報を利用し、小さい身分証明書サイズのカードで高精度に移動をとらえる技術に発展させていく計画である。

加えて、紫外線画像による傷を利用した真贋認証技術を、物体表面の傷の経年変化に対応できるかについて検討を進め、提案方式の有効性を実験的に示し、国際会議での発表や特許出願に向けて発展させていく計画である。

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。

H28 年度(発表決定)

- 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

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

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

研究者名：情報工学科　須藤康裕

５．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することで，「強くて使いやすい」認証方式の設計に不可欠な情報を収集する．

６．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．

７．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．

８．研究の経過及び結果

本報告では，筆者がアドバイザを担当する「履修管理プロジェクト」のシステムアーキテクチャと，ユーザアクセスログからのセキュリティ意識の調査結果を示す．

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/

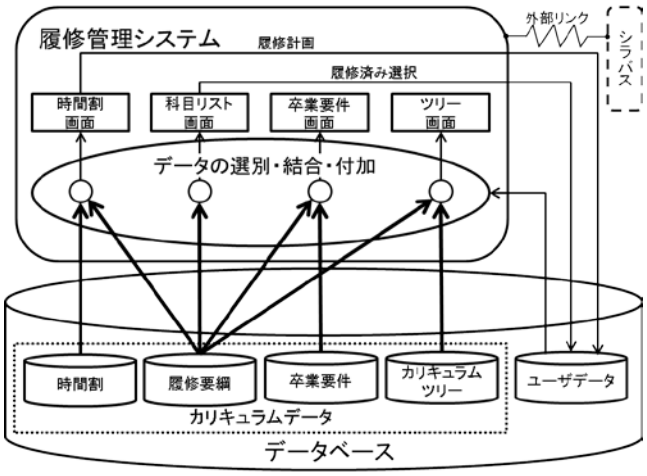


図１　履修管理システム構成図

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　パスワード認証への意識調査

2013 年度から 2015 年度の履修登録期間前後におけるログイン数推移の比較を図 2 に示す．2013 年度における 1 日当たりの最大ログイン数は 120 弱であったが，2014 年度以降は 400 弱まで増加している．2014 年度からはホームエレクトロニクス開発学科の時間割に

も対応し，情報学部以外のユーザも含まれている．ユーザ数は情報工学科に比べ少ないものの，学生数に対する割合は 1 年生が 49.1%，2 年生が 46.6%と，高い利用率を示している．

2014 年度の履修登録期間に関しては，本システムを利用した学生の履修中単位数を学年ごとに集計した結果，1 学年と 2 学年は平均約 43，標準偏差約 6.5 だったのに対し，3 学年は平均約 36.5，標準偏差約 10.4 と，3 学年に大きな特徴が出た．また，期間内における学年毎の一人あたりのログイン回数を集計した結果より，学年が上がるにつれ平均ログイン回数が上昇していることが判明した．

ユーザログインにはパスワードによる認証を行っている．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てみると，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を表わした結果である．

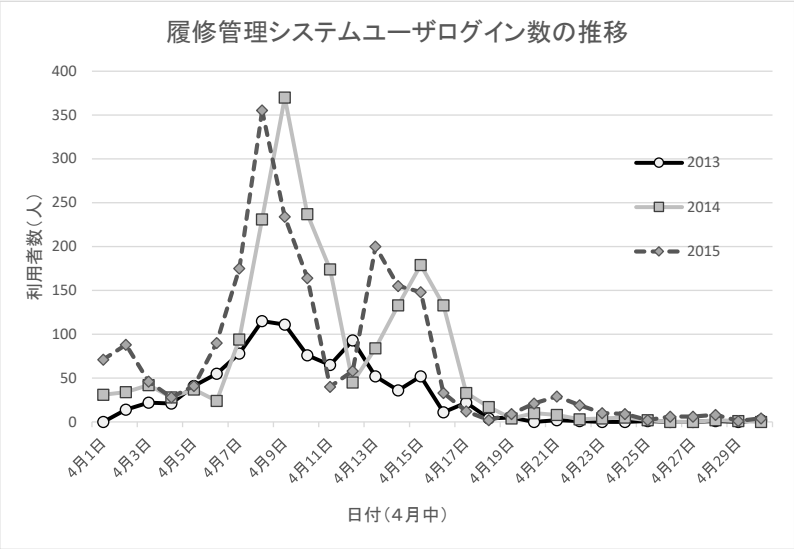


図２　ＲＭＳのユーザログイン数（13～15 年度）

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．