神奈川工科大学

セキュリティ研究センター研究報告

第3巻

2015

神奈川工科大学

工学教育研究推進機構

セキュリティセンター研究報告
第3巻（２０１５）目次

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

昨今国内ではテレビや雑誌などで相次いで標的型攻撃による個人情報漏えい被害が報告されている．標的型攻撃とは数年前から取り上げられた問題であり，決して新しい脅威ではない．しかし，その攻撃が自社（または自分）に来ることはないと考えた企業や個人も，いよいよ意識せざるを得ない問題になったのではないだろうか? 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，想定される様々な脅威に対してあらゆる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 26 年度は，学内重点配分研究として 2 つの研究テーマ「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に関する研究」，「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方式の研究，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．

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
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
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
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	情報漏えいに向けた新方式に関する研究
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
鳥井　秀幸	情報ネットワーク・コミュニケーション学科・准教授	情報ハイディングにおける埋め込み情報量の増加方法に関する研究
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
須藤　康裕	情報工学科・助教	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

安全なモバイルクラウドサービスを実現するための
録画攻撃耐性を持つユーザ認証方式に関する研究

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，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のアイコン同士を指で操作しながら移動させる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，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、画面上のアイコンを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位置とパズルの要素を加えた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

初めに，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た[1, 2, 3]．この認証方式では，格子状にランダムで表示されたアイコンをタップして隣接するアイコンの上にドラッグして，両アイコンの配置位置を入れ替えることによって，パスワードとして登録したアイコンすべてを登録位置に配置した場合，認証成功となる（図1）．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アイコンと位置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[4, 5, 6]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 2）．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．

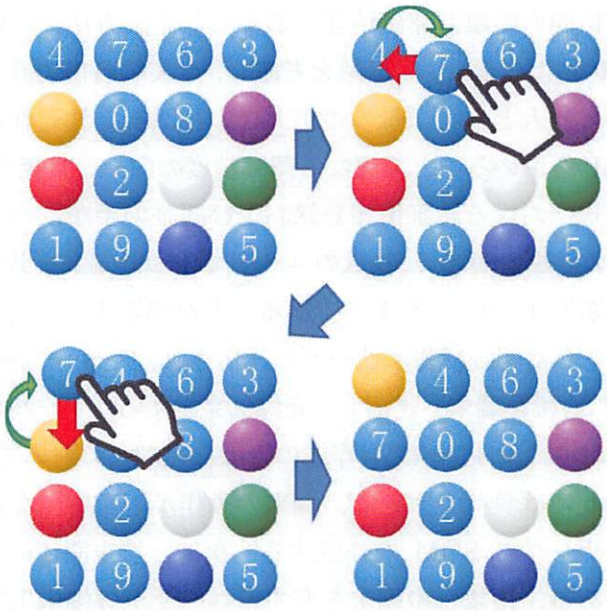

図１．パズル認証の操作例

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．

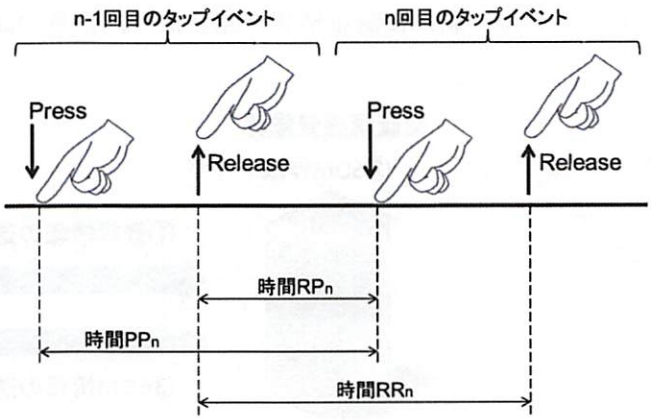

図２．リズム認証におけるタップ時間

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．

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 3 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，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．

図 3. 認証情報登録および認証手順

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] 喜多 義弘, 岡崎 直宣, 西村 広光, 鳥井 秀幸, 岡本 剛, 朴 美娘, "覗き見耐性を持つユーザ認証システムの実装と評価," 電子情報通信学会論文誌 D, Vol.J97-D, No.12, pp.1770-1784, 2014.

[2] Yoshihiro Kita, Kentaro Aburada, Mirang Park, and Naonobu Okazaki, "Proposal of a Puzzle Authentication Method with Shoulder-surfing Attack Resistance and High-usability," IEICE ComEX, Vol.4, No.3, pp.95-98, 2015.

[3] Hisaaki Yamaba, Kentaro Aburada, Shinichiro Kubota, Tetsuro Katayama, Mirang Park, Naonobu Okazaki, "An Authentication Method for Mobile Devices that is Independent of Tap-Operation on a Touchscreen," Proc. The International Conference on Artificial Life and Robotics 2015, No.OS7-1, pp.1-4, 2015/01.

[4] Naonobu Okazaki, Yoshihiro Kita, Kentaro Aburada, and Mirang Park, "Proposal of Security Evaluation System using User's Reviews and Permissions for Android Applications," Proc. The International Conference on Artificial Life and Robotics 2015, No.OS7-2, pp.1-4, 2015/01.

[5] Masahiro Sakuma, Yoshihiro Kita, Kentaro Aburada, Mirang Park, Naonobu Okazaki, "Study of Filter Sharing Method using Virtual Peers in P2P Networks," The 29th IEEE International Conference on Advanced Information Networking and Applications (AINA-2015), pp.527-533, 2015.

[6] Kentaro Aburada, Yoshihiro Kita, Mirang Park, Naonobu Okazaki, "Content access control scheme for P2P networks using a reputation value," The 29th IEEE International Conference on Advanced Information Networking and Applications (AINA-2015), pp.720-726, 2015.

[7] 田村拓己, 久保田真一郎, 片山徹郎, 油田健太郎, 朴美娘, 岡崎直宣, "文字認識攻撃に耐性をもつランダム妨害図形を用いた画像ベースCAPTCHA方式の提案," 情報処理学会論文誌 (特集論文　仮想化時代の情報セキュリティと運用技術), Vol.56, No.3, pp.808-818, Mar. 2015.

[8] 岡崎 美蘭：サーバ側とクライアント側とのマルチ手法による DDoS 攻撃対策に関する考察, 神奈川工科大学　研究報告 B 理工学編, 第 39 号, (2015. 03).

(2) 学会発表

[1] 増田 裕仁, 喜多 義弘, 朴 美娘, 岡崎 直宣, "タッチスクリーンを利用した覗き見耐性を持つパズル型認証方式の提案," 情報処理学会マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2014) 論文集, pp.1005-1010, July 2014.

[2] 喜多 義弘，朴 美娘，岡崎 直宣：パズル型認証方式の録画攻撃耐性に関する考察，バイオメトリクス（BioX）研究報告，2014.06

[3] 喜多 義弘，神里 麗葉，朴 美娘，岡崎 直宣，"自己組織化マップを利用したリズム認証方式とその認証精度に関する考察，" 情報処理学会マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2014）論文集，pp.1011-1018，July 2014.

[4] 喜多 義弘，朴 美娘，岡崎 直宣，"ユーザの慣れによる認証精度の低下を考慮したリズム認証方式の提案，" 情報処理学会コンピュータセキュリティシンポジウム（CSS2014）論文集，pp.1034-1041，20141022.

[5] 喜多 義弘，朴 美娘，岡崎 直宣，"自己組織化マップを利用したリズム認証における個人分類手法の提案，" 電子情報通信学会第 4 回バイオメトリクスと認識・認証シンポジウム論文集，No.O-3-4，pp.1-5，20141125.

[6] 和斉 薫，宗 裕文，山場 久昭，久保田 真一郎，朴 美娘，岡崎 直宣，"安全性強度を柔軟に設定できるモバイル端末向け個人認証方式の一検討，" 情報処理学会研究報告，Vol.2014-MBL-73，No.23，pp.1-9 (2014-11-20).

[7] 宗 裕文，和斉 薫，横山 絵美里，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 Tor における悪用ユーザ推定手法の精度に関する検討，" 情報処理学会研究報告，Vol.2014-MBL-73，No.22，pp.1-7 (2014-11-20).

[8] 尾崎 甲子郎，喜多 義弘，朴 美娘，岡崎 直宣“閾値変動を導入したリズム認証方式の提案”，電子情報通信学会　総合大会　B-6-36，2015.03.

[9] 石田 時大，喜多 義弘，朴 美娘，岡崎 直宣“機械学習を利用した通信異常検知システムの提案”，情報処理学会第 77 回全国大会，4X-5，2015.03.

[10] 陳　致豪，喜多 義弘，朴 美娘，岡崎 直宣“安全な M2M 通信システムのためのグループ鍵管理手法に関する一検討”，情報処理学会第 77 回全国大会，6W-1，2015.03.

(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

(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，　須藤　康裕

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と法制度に焦点をあて，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，セキュリティの高度化に資する適用可能技術を開発することである．

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ることとする．さらに，H26年度までの研究目的・方針を継承し，各研究担当者の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する．特に，情報セキュリティマネジメントシステム（ISMS: Information Security Management System）の考え方に基づき，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・評価し，PDCA サイクルモデルに則ったセキュリティモデルの構築を目指す．また，セキュリティ高度化につながる要素技術のうち，生体個人認証や情報漏洩防止等によるロバストな保護メカニズムの統合・集約化を目指していく．さらに，「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，さらなる高度化への発展を目指していく．

2．情報セキュリティモデルへの要求

組織における総合的な情報セキュリティを確保するためには，情報セキュリティ管理システムの構築・運用が必須事項と言われている．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．情報セキュリティ管理システムへの要求事項を定めた規格：JIS Q 27001:2014 では，情報セキュリティとは，情報の機密性，完全性及び可用性をバランス良

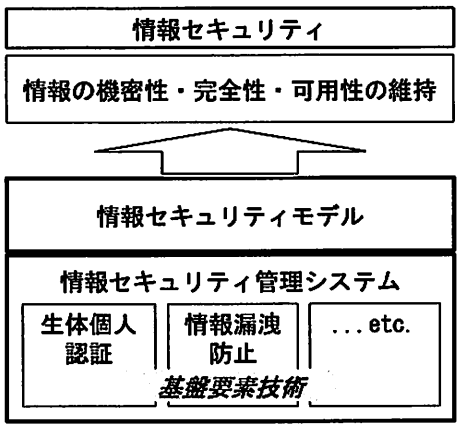

図１．情報セキュリティモデルの位置付け

く維持・改善し，リスクを適切に管理していくことであると規定している．ここで，機密性とは，認可されていない個人，エンティティ又はプロセスに対して情報を使用させず，また開示しない特性をいう．完全性とは，正確さ及び完全さの特性をいう．可用性とは，認可されたエンティティが要求したときに，アクセス及び使用が可能である特性をいう．図１に示すように，情報セキュリティ管理システムは，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管理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．

３．研究の必要性及び従来の研究

インターネット社会における組織改革への関心が高まる中，法制度を正しく理解し遵守すること，危機管理体制意識の向上に努めること，そして組織内情報セキュリティの高度化を実現することが情報通信技術（ICT）の利活用を推進する上での最重要課題の一つとして確たる位置を占めている．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．こうした状況の中，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．また，経済産業省が示すシステム監査基準に基づき，システム監査（特に情報「セキュリティ監査基準」および「セキュリティ管理基準」）に資する情報提供機能の検討が必要である．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．

４．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．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，巧妙なすましへの対応が期待できる．

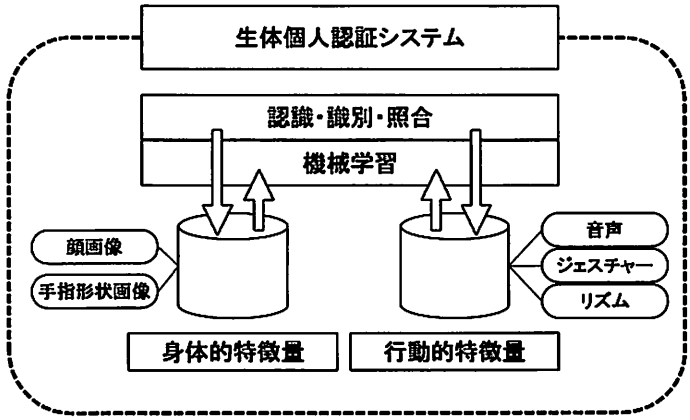

図２．生体個人認証システム

５．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ている．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る．H26 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80～90%程度の認証精度が得られた．H25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低下した．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，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，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を図りたい．

５．今後の計画

生体個人認証に関しては，ラピッドプロトタイピング（rapid prototyping）とアジャイル開発手法（agile software development）を積極的に取り入れることで，実装・評価プロ

セスをスピードアップし，システムの精緻化と評価実験を通した検証を行い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認証方式について検討する．

情報セキュリティモデルの構築に関しては，まず，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を分析する．次に，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．

６．研究成果の発表

【査読無し学会発表】

[1] 河合博之，仲濱正大，納富一宏，斎藤恵一:"個人認証機能を備えた音声認識システムの基礎的検討"，電子情報通信学会 2015 年 総合大会 A-23-2, p.310, (2015.03).

[2] 星野裕樹，仲濱正大，納富一宏，斎藤恵一:"行動的特徴量付与による拡張ピクチャーパスワードを用いた個人識別手法"，電子情報通信学会 2015 年 総合大会 A-23-3, p.311, (2015.03).

[3] 前川龍介，星野裕樹，納富一宏:"Web による顔認証システムの実装と評価"，電子情報通信学会 2015 年 総合大会 A-7-8, p.142, (2015.03).

[4] 星野裕樹，仲濱正大，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の検討"，バイオメディカル・ファジィ・システム学会 第 27 回年次大会講演論文集, pp.35-36, (2014.11).

[5] 河合博之，仲濱正大，納富一宏，斎藤恵一:"自己組織化マップによる音声認識と音声認証の基礎的検討"，バイオメディカル・ファジィ・システム学会 第 27 回年次大会講演論文集, pp.5-6, (2014.11).

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、情報漏えいは重要な課題のひとつである。情報の漏洩を防止するためには、サービス提供側が、ユーザの本人確認を厳密に実施する必要がある。そのためには、現状もっとも用いられているパスワード方式に加えて、様々な「強い認証」が必要となってくる。そこで本研究では、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、新たな認証方式の提案を行う。

２．研究の必要性及び従来の研究

サービス提供者がユーザの本人確認を行ういわゆる認証行為については、現状ではそのほとんどがパスワード方式で行われている。パスワード方式はもっとも導入が簡単で、誰でも利用できる利点があるが、一方でパスワードは、盗まれたり、忘れてしまったり、推測されてしまったりすることで、利用ができなくなったり、他人になりすましされる危険性が常にある。背後から覗き見ることによりパスワードを盗むこと（ショルダーハッキング）も可能であり、特に近年では監視カメラも小型化されているため、ユーザが気づかないまま録画され、パスワード入力画面を解析される恐れもある。また、キーロガーと呼ばれる秘密のソフトウェアを仕込むことにより、ユーザの打ち込んだキーボード情報をすべて記憶させ、そこからパスワードを盗む攻撃も存在する。実際にこれらアタックによりパスワードが盗まれる事件が多数発生し、金銭を含んだ大きな被害を生んでいる。そこでこれら様々な脅威に対抗できる新たなパスワード入力方式や、パスワード方式にプラスアルファできる新しい認証方式の提案が必要となってきている。

加えて、ひとつの方式の認証行為に頼るのではなく、複数の認証方式を同時に利用するマルチサインオン方式もまた、「強い認証」にむけて必要となる技術である。パスワードに加えて、第二パスワードを要求したり、指紋認証等の追加の本人確認を実施したりする方式である。しかしこれまでのマルチサインオンでは、サービス提供者自身が、すべての認証方式を準備する必要があり、設備構築に多大なコストがかかる点が課題であった。その点を改善するべく、複数の認証サーバに分散させ、それらの間で認証情報を流通させ、サービス提供者が自由に利用できるプラットフォームを作り上げることが求められている。

３．期待される効果

「強い認証」を実現することで、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等によるなりすましの被害にあわなくてすむようになり、これまた安全安心にサービスを利用できるようになる。具体的には、ショルダーハッキングや、キーロガーといった脅威に接したとしても、なりすましされる可能性を低くできる。

また、マルチサインオンのプラットフォーム化においては、サービス提供者自身は認証手段をユーザに提供する必要がなくなるため、設備投資等のコストが格段に下がる効果を生む。つまりプラットフォーム側にセキュリティ部分をまかせてしまうことができ、小規模事業者もより簡単に事業参入が可能となり、サービスの幅が広がる点にも期待ができる。また、様々な認証手段を組み合わせて自由に設定できるため、サービス内容に応じたフレキシブルなセキュリティ設定が可能となる。

4．研究の経過及び結果

キーロガーやショルダーハッキングに対抗できる新しい策として、新しいパスワード入力方式の提案を行った。キーロガーや、覗き見によって通常のパスワードは盗まれる恐れがあるが、提案方式では、少数キー（提案では 4 キー）にて従来レベルのパスワードを入力できる。入力に利用するキーが少数で使用範囲が狭い（例：カーソルキーだけでパスワードを打つ）ため、入力の際に手で隠しながらパスワードを打つことが可能であり、ショルダーハッキング・録画等のアタックに対抗することが可能となる。銀行の ATM 等も四桁の暗証番号を打つ部分を背後から見られないように様々工夫がされているが、本方式も同様で、それでいて、銀行 ATM のパスワードは 4 桁の数値でしかないが、本方式は英数字を含めた通常のパスワードとほぼ同様で長さ無制限のものを利用できるため、その点の強度も通常のパスワードと同等となっている点に特徴がある。また本方式では、パスワードそのものを入力しないため、キーロガーで記録された場合でも、ログに残るのは利用された少数キーの情報だけであり、その情報からだけではパスワードそのものは推測できない。またセキュリティ観点とは別に、本方式では少数キーしか利用せず通常のパスワードが利用できるため、一般的なキーボードの利用が困難な身体障害者に向けてのパスワード入力方式としても利用できる。

また「強い認証」の実現に向けて、複数の認証結果を利用してユーザの本人確認を行う「マルチサインオン」方式の提案を行なった。提案方式では、認証情報をユーザの属性情報として流通させることで、複数サーバ間でこれら情報を共有し、マルチサインオンを実現する。特に、認証結果については「認証ポイント」なる評価値をつけることで、サービス内容に応じた認証強度をフレキシブルに設定できる方式として提案している。ユーザは、自分が利用したいサービスが独自に設定した「必要認証ポイント」を集めるべく、複数の認証サーバを周り、ある認証サーバではパスワード方式を使い 100 ポイント、別の認証サーバでは証明書認証を使い 200 ポイント、とポイントを累積させていき、規程のポイント以上になったところで初めてサービスが利用できる、といった方式である。認証情報の流通には、シングルサインオン技術である OpenID を採用し、特にはその属性流通技術である

Attribute Exchange を利用している。標準仕様を用いることで、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。具体的には、まず「少数キーによるパスワード入力方式」については、さらにキーの数を絞った上で Android 端末等の携帯端末上に展開し、ユーザ検証を行って評価を行う。さらには、パスワード方式に追加する認証方式として、ユーザの普段の行動履歴を認証の手段として利用し、本人を追加認証する新たなリスクベース認証方式の検討を行う。また、マルチサインオンについては、複数認証サーバを使う点では同様であるが、「順番」という新たな価値を導入し、正しい順番で認証サーバを利用しなければ最終的な認証が完了しない「順番サーバ認証方式」の提案を行う。

６．　研究成果の発表

[1] Akane Ito, Yui Ohtaka, Yoshie Yamada, Manabu Okamoto,"Input Password Only with Four Keys, Three Times", SOUPS2014, Menlo Park CA, USA, 2014.7.

[2] 石塚貴, 岡本学, "マルチサインオン;認証コレクターの提案", 電子情報通信学会 2015 年暗号と情報セキュリティシンポジウム(SCIS2015), 2015 年 1 月,小倉

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。

26年度の課題としては、25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、カード位置を高精度に検出する手法を確立することが目的であった。

加えて、照明条件を検討することで、さらなる高精度な認証方式の検討を深めることが目的であった。

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で採用されているのものの、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。

25 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、幅広い利用場面を想定した場合には、カードと撮影するカメラとの距離や位置関係に高い自由度があることが望ましいが、25 年度の段階では一定距離、一定角度でしか正しく利用することができていなかった。26 年度の研究では，広い範囲で撮影した映像を利用して高精度にカード位置を特定し、これまでに考案してきたシステムの適用条件を広め、より高い実用性を生み出すことを目的とした不可欠な検討である。

照明条件の検討は、より多様な環境での提案システム実装に向けて不可欠な検討であり、これにより新しい提案システムの利用方法を模索することができると考えられる。

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、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。これにより、低コストで実現できる認証方式であるといえる。

25 年度に行った性能評価実験の結果から、提案手法は認証用カードが盗難された場合においても、非常に堅牢な認証を実現することができることが明らかになった。これにより、高い実用における認証性能を実証することができた。

26 年度に行ったカード位置の高精度検出により、広い範囲で撮影した場合においてもカード位置を数 cm の精度で検出できることを明らかにした。これにより、より広い用途で提案システムを利用することができることを示すことができた。

加えて照明条件をコントロールすることで、環境変化にロバストな認証システムの実現に向けた検討を深めることができると考え、試行を重ねてきた

以上のことより、本研究の提案方式を確立し有効性を実証することは、カード認証が利用されるあらゆる場面での活用が考えられ、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。

5．今後の計画

盗難意外にも、偽造や盗み見などの多様な状況のデータを採取し、提案手法の堅牢性を、実験を通して実証していく計画である。

紫外線照明やカメラを利用して、現在よりもさらに高精度な認証方式の実現を検討しており、これまでに得られた実験データと知見を活用して検討を深めていく計画である。

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。

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）

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）など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。ただし、現実的なコンテンツの品質を維持しながら、2^{n-1} 個の拡散系列を全て使用できるかどうかについては明らかになっていない。そこで本研究では、提案した拡散系列をM-ary方式に適用した場合、使用できる拡散系列の個数について明らかにすることを目的とする。

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、構成可能な拡散系列を全て使用可能であるかどう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、使用できる拡散系列の個数について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、現実的なコンテンツの品質を維持できる情報量を明らかにすることにより、M-ary 方式を相関利用型情報ハイディングに応用することで、現実的にどの程度の情報量の増加が可能なのかについて明らかになることが期待される。

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。そこで、使用する拡散系列の個数を1、2、4、8、・・・2^{n-1}と増加させていき、実際の画像に透かし情報を埋め込んだ場合において、必要となる強度の増加について検討を行った。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。結果より、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。

５．今後の計画

検証より、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が、全く増加しないわけではないため、画像によっては品質劣化が知覚できる可能性がある。今後は、埋め込み可能な情報量と画質劣化の関係を定性的または定量的に明らかにする必要がある。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。

研究課題名「セキュリティと社会」

研究者名：所属学科　基礎・教養教育センター　　氏名　三浦直子

１．研究の目的

学校や企業などの諸組織において、情報通信技術（ICT）を備えたデジタル機器を導入し、また情報ネットワークを活用することは、あまりに一般的で当然のこととなったが、その普及はわずか20～30年ほどの間に急速に行われたものであり、今日ではますます依存の度合いを高めている。加えて、ICTの発展は目覚しく、社会の隅々にまでグローバル化が広がるとともに、学校やオフィスなど組織の情報環境および組織が所有する情報の価値は、現在も刻々と変化している。しかし、ICTを利用する人々の意識や行動は、こうした社会変動や環境の変化に即しているとは言いがたい。そこに、組織内情報セキュリティにとって、大きなリスクが存在している。

例えば、特定の組織を狙って、組織内情報にアクセスするために、従業員にウィルスを送りつけるケースが昨今、ニュースを賑わしている。大きな社会問題として報じられたのは、2015年5月に感染し、翌6月に公表された日本年金機構120万人分の情報漏洩である。このケースでは、二段階のサイバー攻撃への対応のまずさが問題として指摘された。最初に、ウェブ公開しているメールアドレス経由で最初の感染が生じ、このときに組織内名簿が流出したと疑われている。次に、メールアドレスが未公開だった複数の職員のところへウィルスが送信され、開封した複数の職員が感染し、職員のPC内部に作業用にコピーしていた年金情報が流出したことが報道されている。注意すれば、一部で中国語のフォントが漢字に使われているなど、偽装メールを疑うべき点が複数存在していたものの、後者では、未公開の（それゆえ関係者とのやり取りに限定された用途での）メールアドレスであったがゆえに、かえって関係者を装ったメールを容易に信じてしまったことが指摘されている。

これまで、国際的なサイバー攻撃については、言葉の壁によって日本は比較的標的にされにくかったという特徴があった。しかし2010年代以降には、翻訳ソフトの機能向上と普及もあって、組織が保有する機密情報を狙った国内外からの標的型攻撃が盛んとなっている。また、組織の保有する情報の流出だけでなく、情報改竄、監視、サイバー攻撃の踏み台としての利用など、多様な危機に晒されるようになった。そこで本研究では、人々のハビトゥス（認知図式や行動様式）という社会学概念に注目し、社会変動に即した新しい組織内情報セキュリティモデルの高度化に向けて調査・提案することを目的とする。

２．研究の必要性及び従来の研究

これまで、刻一刻と進展するICTやグローバル化といった社会変動に対して、情報セキ

ュリティや情報ネットワーク上のリスク回避のために、さまざまな分野で多様な対策が取られてきた。その問題構造を抽出すれば、セキュリティ対策の技術面や法律面では、完全な予防は不可能であることから、事前対策から事後対策に比重が移動しつつある。

▼ウィルス対策ソフト：シマンテック社が開発したアンチウイルス・ソフト「ノートン」は、ウィルス定義を常に最新に維持して、指名手配型で侵入を監視する事前対策に努めてきたが、新種・亜流のウィルスが次々と開発されたり、ユーザーの定義更新が滞っていたりと、全体の 55%もの攻撃を検知できないことを公表するとともに、防ぎ切れずウィルスに感染した後も、通常とは異なる作動を始めた場合、情報流出を制止するヒューリスティックなアプローチの導入を公表した（2014 年 5 月付けウォール・ストリート・ジャーナル)。

▼プライバシー・バイ・デザイン：例えば、監視カメラ映像などの機密情報を流出させないためには、人的対策として、リテラシー教育・研修への注力と、インターネットへの接続禁止やスタンドアロン PC での操作といった環境設計に重きが置かれてきた。しかし、2012 年春に日本のコンビニエンスストアの監視カメラ映像（モニター画面）を、携帯電話で撮影して SNS に投稿するといった事件のように、事前対策だけでは、当初予想もしなかった方法で情報流出するリスクを常に孕んでいる。そこで、情報が流出しても映像のなかの人物が特定できないように、映像記録時に暗号化をかける対策が取り入れられている。

▼忘れられる権利：若気の至りで気軽に投稿した情報が、後の自身の将来に大きな影響を与えることが問題視されて久しい。ヌード画像が原因で就職難に陥ったフランス人女性や、ワル自慢の画像投稿で個人情報が晒された日本の若者による SNS 炎上など、列挙にいとまがない。自ら投稿した情報が将来の自分を苦しめるという意味で、自身が被害者であり加害者でもあるという状況から、「自業自得」「自己責任」と軽んじられることが多く、また事前対策も、学校や家庭での情報モラル教育に任されてきた傾向がある。しかし、EU が法制度化した「忘れられる権利」のように、事後であっても、本人の被害が最小限で留まるように法的に保護すべきという考えが広がりつつある。日本でも、2014 年に Google に対する検索結果表示の削除を判決とする裁判が行われた。

以上のように、セキュリティ対策は、事前対策から事後対策へと比重が移動しつつある。これまで、人的対策については、セキュリティ教育や研修など、情報セキュリティのための予防的措置を中心に据えてきた。しかし、近年の動向を見れば、もはや予防的措置（事前対策）だけで完全に防げるものではないことは明らかである。新しいセキュリティ対策として、事後対策への整備が急務であるといえる。

３．期待される効果

人的対策においても、事前の予防的措置から、事後のリスクが最小限となるようなセキュリティ対策への転換が必要であるといえる。言い換えれば、これまで重きを置かれてきた事前対策が「予防」のための教育・研修であるとしたら、今後、必要になるのは、感染することを前提とした「被害を最小限に留めるための対応」であろう。そこで、本

研究では、事後のセキュリティ対策を重視するべきであるという提案と、運用モデルを検討し、組織内情報セキュリティの高度化に貢献したいと考える。具体的には、避難訓練に喩えられる、組織内の「ウィルス感染対応訓練」の実施提案である。

日本は地震大国であるが、震度の比較的大きな地震が頻繁に生じる割に被害が少ないのは、「建築の耐震化」という側面に加えて、地震が起こることを前提とした「被害を最小限に留めるための対応」としての「避難訓練」の効果が大きいということを指摘したい。学校や企業では、机の下に身を潜めて頭を守り、窓ガラスの破損に気をつけながら最短ルートで屋外に脱出する方法について、繰り返し訓練を受けている。それにより、個々人が、有事の際に何を行えばいいのかシュミレーションできているだけでなく、実際に訓練を実施することにより、どの経路が混みやすいのか確認でき、効果的な対策も検討できる。これらのことが、いざ大きな地震が生じたときの、被害の小ささをもたらしている。また、避難訓練を実施することそのものが、いつなんどき地震が生じるか分からないという危機意識を人々に共有させる効果をもつ。「ウィルス感染対応訓練」によって、自分から遠い話ではなく、身近に起こり得ることとして、セキュリティ・リスクに対して積極的に「用意する」「備える」意識を育むことになる。

4．研究の経過及び結果

これまでの（H24～25年の）研究成果について、2014年7月に開催された第18回国際社会学会世界会議（ISA 2014）科学社会学の部会で研究発表を行い、また多くの研究者と交流して最新動向の把握に努めた。特に、『The Panoptic Sort』（邦訳『個人情報と権力』）や『Coming to Terms with Chance』等の研究で著名なペンシルバニア大学名誉教授の Oscar H. Gandy Jr.先生からは、その後半年間に及ぶメールでの交流を通じて、多くの知見を得た。

本研究で注目しているハビトゥス論との関係についていえば、ICT教育における社会的格差への注目の必要性が挙げられる。例えば、日本でもICTとして携帯電話（ケータイ、スマホ）を駆使して育った若者世代の一部が、オフィスにおけるPCリテラシーに欠けることが指摘されている。現在の日本社会では、自宅にPCがある家庭とない家庭という格差、すなわち経済面でも文化面（PCを購入し家庭で所有することに価値を置くという文化の有無）でも、家庭ごとの社会的格差は、歴然と存在する。それにもかかわらず、学校教育や組織研修における現行のICT教育では、建前上、家庭環境の平等（均質性）を前提として、PCソフトや情報セキュリティについて教えている。誰もがPCを使う環境にあるはずだという教育の前提（均質化）は、家庭環境に由来する有利さと不利さ（慣れによる得手不得手）を、「個人の能力差」と見なしてしまう。言い換えれば、人々のハビトゥス（社会的位置に由来する特有の認知図式と行動様式）が、教育や研修を通じて「個人の能力差」にまで拡大再生産され、固定化されていくのである。

例えば、Dana Boydらの研究を参照すれば、上述の若者世代にとって身近で不可欠な

ICTとなった携帯電話（ケータイ、スマホ）に関しては、日常的に接して使いこなしているという点で、（どのような家庭環境にあっても）それぞれの社会的位置に応じた特有の護身対策を実践的に習得していることが想定される。しかし、私的な携帯電話と公的な組織内ICTの利用とでは、そのリスクと被害の大きさからも、情報セキュリティとして求められるハビトゥス（認知図式と行動様式）は決定的に異なる。情報セキュリティのためには、単なる知識だけではなく、意識や行動面での改善が求められる。しかし、家庭環境や生活環境で身につけてきたハビトゥスと、組織内情報セキュリティとして求められるハビトゥスとの間の「ずれ」が大きい人々は、その「ずれ」を埋める個人的な努力が更に必要となるが、情報セキュリティのための教育や研修が人々の平等（家庭の均質性）を前提とする現状の内容では、自己責任として放置されてしまうだろう。一人のミスが、組織全体のリスクへと直結する情報セキュリティにあっては、人々の多様なICTをめぐるハビトゥス（認知図式と行動様式）を適切に把握して、個々に応じた対応が必要になるのではないか。

５．　今後の計画

アンケート調査を実施し、人々の日常生活における情報への接し方や情報セキュリティに関する意識の実態を把握する。人々の利用状況における問題点を発見し、対応策の検討を目指す。その際、広義の社会的格差（組織内に存在する社会集団の相違等）に注目し、その影響を検討する。（当初は、アンケート調査を行うための現実的な規模と時間等との関係から、学生調査を予定していたが、調査対象を誰に設定すべきかについては、再検討の余地があるとも考えている。）

その後、人々の実態把握に基づいて、実際に自身のICTがウィルス感染した場合に、どのような手順で何を対応すればよいのか、具体的な「ウィルス感染対応訓練」の内容と運用について検討して提案する。そのためには、人々のハビトゥスに配慮すると共に、情報セキュリティついて技術的な立場から取り組んでいる研究者にアドバイスを仰いで内容に盛り込む。それにより、組織内情報セキュリティモデルの高度化への発展を目指す。

６．　研究成果の発表

[1] 三浦直子：「情報社会のハビトゥス：身体と知の変容」，＜自己・表象＞研究会（2013.03.12），法政大学（査読無し国内研究会）.

[2] MIURA Naoko："Social and Intellectual Antinomies of Information Technology"，XVIII International Sociological Association World Congress（ISA 2014）2014.07.14，Yokohama（査読有り国際学会）.

[3] 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（2014.08.05），神奈川工科大学（国内研修会での招聘講義）.