神奈川工科大学

セキュリティ研究センター研究報告

第２巻

２０１４

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２巻（２０１４）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

現在我々の日常生活はほとんどがインターネットに依存している．すなわち，電気，ガス，水道，鉄道，航空，金融，行政サービス，医療および物流などすべての社会インフラがネットワーク化されている．それに伴い，従来は企業の情報システムの領域にとどまっていたサイバー攻撃がその対象を拡げ，被害を受ける社会インフラシステムが増加している．例えば，2013 年 3 月には韓国で大規模なサイバー攻撃が発生し，銀行の ATM や決済が一時停止するなどの混乱が発生した．

サイバー攻撃は日々進化しており，想定される様々な脅威に対して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，さらに社会学・法学的な側面での，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 25 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基礎的研究」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，セキュリティと法制度の研究においては，現在社会で問題となっているサイバー犯罪と警察の対応などについての問題点を指摘し，今後の対応において課題解決策が必要であることを明らかにした．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
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・専任講師	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
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

覗き見耐性を持つパズル型認証方式を用いた安全な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として，覗き見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，他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，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であるSTDS（Secret Tap with Double Shift）方式[1, 2]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認証情報を入力する方式である．認証の鍵となるアイコンは，ユーザが事前に登録したアイコンから 2 種類の移動法則（シフト機能）を用いて移動した先のアイコンとする．シフト機能による移動量はユーザしか知らず，移動先のアイコンも認証のたびに異なるため，攻撃者は認証動作を目視しても認証情報を盗むこと

図 1.象限間シフトと象限内シフト

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，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であるSTDS（Secret Tap with Double Shift）方式[1, 2]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認証情報を入力する方式である．認証の鍵となるアイコンは，ユーザが事前に登録したアイコンから2種類の移動法則（シフト機能）を用いて移動した先のアイコンとする．シフト機能による移動量はユーザしか知らず，移動先のアイコンも認証のたびに異なるため，攻撃者は認証動作を目視しても認証情報を盗むこと

図 1.象限間シフトと象限内シフト

ができない．被験者に見られながら認証動作を繰り返し行う実験を行い，本方式が高い覗き見耐性を持つことが示された．しかし，利用者によるアンケートより，実用的なユーザビリティを持つことは確認できたが，シフト量を忘れた場合などを考慮した「使いづらい」「あまり使いたくない」というコメントがあった．

そこで，今年度はより使いやすい覗き見耐性を持つパズル認証方式[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，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２）．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．これに対し，今後はユーザビリティの向上とともに，録画攻撃対策に関する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．以下では，今年度の本研究の基本となるパズル認証方式について報告する．

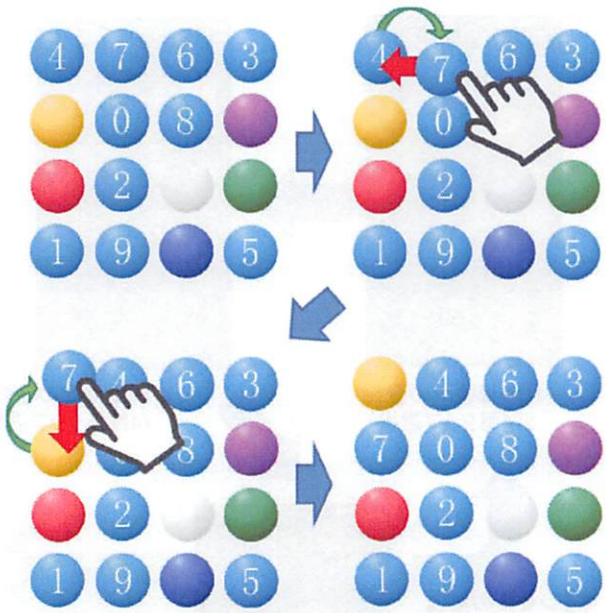

図 2．パズル認証の操作例

4.2　パズル認証方式

本方式では，0 から 9 の数字と赤，青，緑，黄，黒，白のマスを 4×4 の四角形に配置し，認証画面に表示されているマスのいずれか 1 つをタッチし，そのまま上下左右又は斜めへ自由にスライドさせて認証を行う．

最初に，ユーザは認証のための位置とパスワードを登録する．認証開始時に 0 から 9 の数字と赤，青，緑，黄，黒，白のマスがランダムに表示されるので，ユーザは登録したパ

スワードの位置を確認する．その後，認証画面に表示されているマスを 1 つ選択して，そのマスをタッチした後にスライドをさせて，上下左右斜めの隣接マスと入れ替えながら，登録した位置とパスワードを合わせる．

この認証方式では，位置とパスワードを認証情報として登録する．位置については，ユーザが任意の 4 ヶ所を登録することができる．赤いまるで囲まれている位置が，ユーザが登録した位置である．位置は必ず 4 ヶ所を登録しなければならないため，同じ場所を複数登録することはできない．位置については，16 ヶ所の中からユーザが任意で 4 ヶ所選ぶことから，位置登録のパターンの総数は ${}_{16}C_4$=1820 通りとなる．

パスワード登録に関しては，登録した位置にパスワードを合わせるため，パスワードは位置の数と同じく 4 個使用する．しかし，パスワードは登録した位置ごとに移動するのではなく，登録した位置にパスワードが含まれていれば，認証成功としている．パスワードについては，位置と同じく 16 個の中からユーザが任意で 4 個選ぶため，パスワード登録パターンの総数は ${}_{16}C_4$=1820 通りとなる．

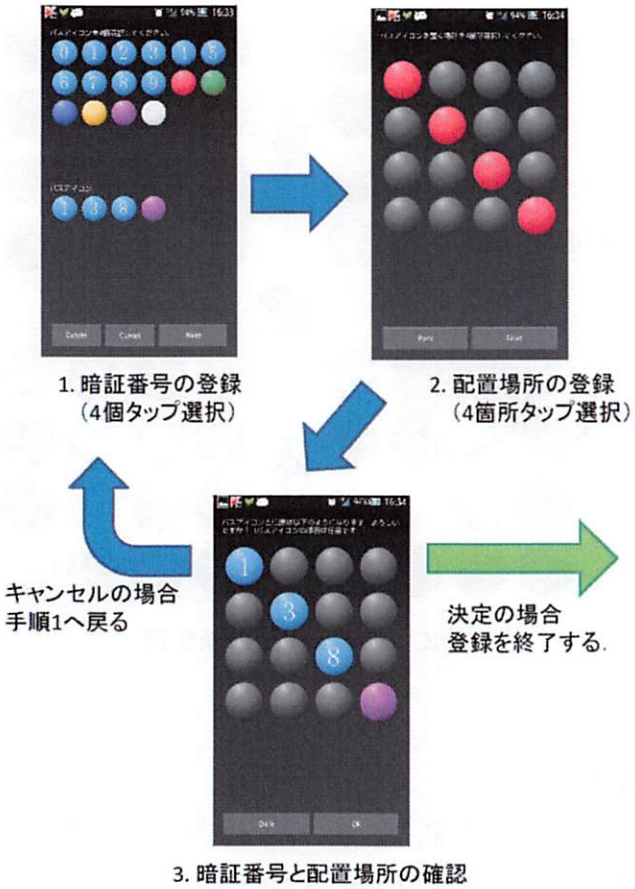

図 3．認証情報登録の手順

スワードの位置を確認する．その後，認証画面に表示されているマスを 1 つ選択して，そのマスをタッチした後にスライドをさせて，上下左右斜めの隣接マスと入れ替えながら，登録した位置とパスワードを合わせる．

この認証方式では，位置とパスワードを認証情報として登録する．位置については，ユーザが任意の 4 ヶ所を登録することができる．赤いまるで囲まれている位置が，ユーザが登録した位置である．位置は必ず 4 ヶ所を登録しなければならないため，同じ場所を複数登録することはできない．位置については，16 ヶ所の中からユーザが任意で 4 ヶ所選ぶことから，位置登録のパターンの総数は ${}_{16}C_4$=1820 通りとなる．

パスワード登録に関しては，登録した位置にパスワードを合わせるため，パスワードは位置の数と同じく 4 個使用する．しかし，パスワードは登録した位置ごとに移動するのではなく，登録した位置にパスワードが含まれていれば，認証成功としている．パスワードについては，位置と同じく 16 個の中からユーザが任意で 4 個選ぶため，パスワード登録パターンの総数は ${}_{16}C_4$=1820 通りとなる．

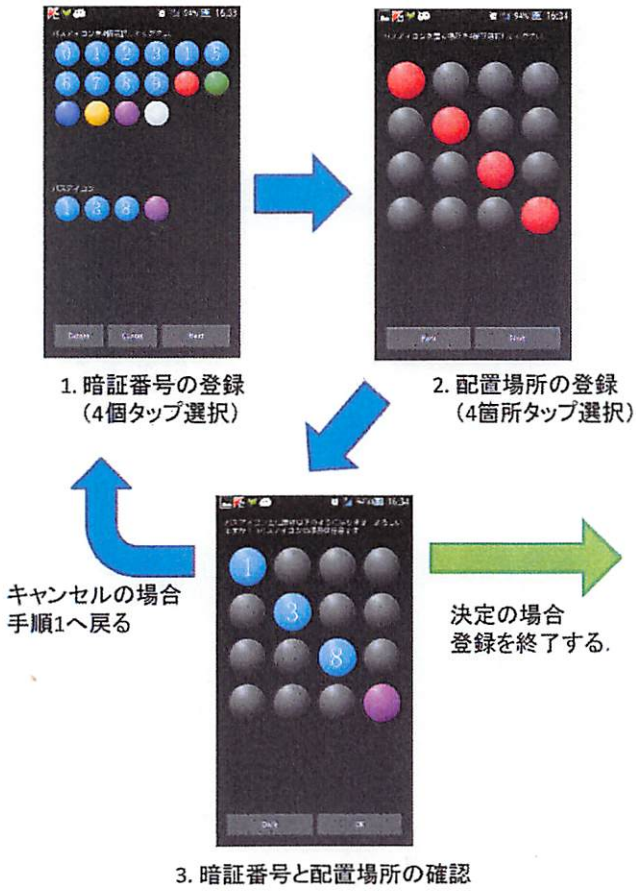

図 3．認証情報登録の手順

4.2 実験結果

本提案手法の覗き見攻撃耐性を評価するために，覗き見攻撃の実験を行った．15 人の被験者から親を 1 人決め，親が他の 14 人が見ている前で，本提案方式の認証方式を行い，他の 14 人はその認証動作を覗き見て，位置とパスワードを特定することができるかの検証を行った．実験の結果，位置とパスワードを全て特定できた人は 1 人もいなかった．これにより，提案の認証方式は第三者による覗き見に十分な耐性を有していることが確認できた．また，実験後に利用者に使いやすさと安心感についてアンケートを行った．アンケートの結果から，使いやすさは従来の方式より上がったことが分かった．また，位置とパスワードは従来の STDS 方式より覚えやすいので，ユーザの記憶への負荷が減ったことが分かった．覗き見に対して高い耐性を持つことによる安心感や，利用場所を選ばない利便性の高さから，本方式を積極的に利用したいという意見が多く，実用的なユーザビリティを持つことが確認された．

5. 今後の計画

録画攻撃への対策として，パスワードの配置場所を複数のパターン登録し，認証時にどの配置場所のパターンを用いるかをモバイル端末に付属しているセンサーデバイスなどを用いた方法が考えられる．しかし，ユーザは複数のパターンを記憶する必要があり，ユーザビリティの問題が考えられる．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] Yoshihiro Kita, Fumio Sugai, Mirang Park, Naonobu Okazaki, "Proposal and its Evaluation of a Shoulder-Surfing Attack Resistant Authentication Method: Secret Tap with Double Shift," International Journal of Cyber-Security and Digital Forensics (IJCSDF), Vol.2, No.1, pp.48-55, 2013.

[2] 喜多 義弘、菅井 文郎、朴 美娘、岡崎 直宣、西村 広光、鳥井 秀幸、岡本 剛, "STDS 認証方式における録画解析による攻撃への耐性に関する一検討," FIT2013(第 12 回情報科学技術フォーラム), 第 4 分冊, pp.7-14, Sept. 2013.

[3] 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

[4] 喜多 義弘，神里 麗葉，朴 美娘，岡崎 直宣：マルチタッチ操作を利用したリズム認証方式の検討，モバイルコンピューティングとユビキタス通信（MBL）研究報告，2014.03.

[5] 喜多 義弘，菅井 文郎，朴 美娘，岡崎 直宣，"ユーザ主体による Android アプリケーションのレビュー評価システムの提案," 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（DICOMO2013）論文集, pp.1341-1347, July 2013.
[6] 喜多 義弘，久保田 真一郎，朴 美娘，岡崎 直宣：Android OS における不正アプリケーション取得防止のためのセキュリティ評価システムの提案，情報処理学会コンピュータセキュリティシンポジウム（CSS2013）論文集, pp.208-215, 2013.
[7] 岡崎 美蘭：モバイルクラウド用プッシュ型通信における相互信頼プロトコルの研究，神奈川工科大学　研究報告 B 理工学編，第 38 号，(2014. 03).

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基礎的研究

研究者名：情報工学科　　納富　一宏

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．１つの組織だけの問題ではないためである．

２．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法制度を考慮した組織内情報セキュリティの高度化に向け，「セキュリティと法制度・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．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，実運用に供するか否かの検証実験によりシステム評価を実施する．

４．研究の経過及び結果

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．H25年度に実験および評価を行った特徴量としては，掌指形状，声紋，キーストローク動作，タッチ動作，図形手書き動作であり，図形手書き動作以外は，ともに95%以上の良好な認証精度が得られた．軌跡情報を用いる図形手書き認証の場合，精度は80%程度まで精度が低下した．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）を用いており，統一的な手法に基づいているため，情報システムに複数の特徴量による生体個人認証を複合的に搭載することが可能である．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，教育機関における USB メモリによる情報漏えいの可能性低減を目指したセキュアな情報管理システムの試作を行った．今後は，生体個人認証機能を追加することで，企業等に導入されているセキュリティ強化製品との差別化を図る必要がある．

５．今後の計画

H26年度以降の研究では，更なる手法の精緻化と評価実験を通して検証を行いセキュリティの高度化を図る．具体的には，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を利用した生体個人認証（バイオメトリクス認証）のうち，①キーボードの打鍵タイミングをキーとする「キーストローク認証」，②キーボードのホームポジションに置かれた手の形状をカメラで撮影し認証を行う「掌指形状認証」，③筆記具に付加した加速度センサからの入力情報とタブレットPC等に採用されているタッチパネルからの軌跡情報を複合化した「手書き図形認証」の３種類のバイオメトリクス認証方式について，認証精度による評価実験を実施し，手法の精緻化を検討することで，セキュリティの高度化を目指す．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．その結果については論文にまとめ，学会等で発表を行う．

６．研究成果の発表

H25年度の研究成果は，国内査読付き論文２件，国内査読付きシンポジウム３件，国内査

読無し学会発表７件である．詳細を以下に示す．

【査読付き論文】(*＝本学学生，在学中の研究成果，以下同様)

[1] 谷村 祐，納富一宏，斎藤恵一:"手指画像におけるカラーヒストグラムによる生体認証手法"，バイオメディカル・ファジィ・システム学会誌，Vol.16，No.1，pp.41-48 (8pages)，(2014.04) [採録決定 2014.02.06].

[2] 山田健一朗*，納富一宏，斎藤恵一:"スマートフォン操作時における行動的特徴量を利用した個人識別手法"，バイオメディカル・ファジィ・システム学会誌，Vol.16，No.1，pp.49-55 (7pages)，(2014.04) [採録決定 2014.02.07].

【査読付き国内シンポジウム】

[1] 谷村 祐*，納富一宏:"受講者の即時的な反応を記録する授業トラッキングシステムの開発と評価"，情報処理学会 マルチメディア，分散，協調とモバイル (DICOMO2013) シンポジウム，4E-1，pp.976-979，(2013.07).

[2] 市村亮太*，納富一宏，斎藤恵一:"覗き見攻撃耐性を考慮したスマートフォンにおけるリズム認証手法 -楽曲の主旋律を用いた際の認証精度評価-"，情報処理学会 マルチメディア，分散，協調とモバイル (DICOMO2013) シンポジウム，1H-4，pp.230-233，(2013.07).

[3] 山田健一朗*，納富一宏，斎藤恵一:"スマートフォンにおけるキー操作熟練度の違いによるキーストローク認証手法の検討"，情報処理学会 マルチメディア，分散，協調とモバイル (DICOMO2013) シンポジウム，1H-5，pp.234-237，(2013.07).

【査読無し国内学会発表】

[1] 山田健一朗*，納富一宏，斎藤恵一:"スマートフォンにおけるタッチジェスチャーを用いたバイオメトリクス認証手法"，電子情報通信学会 2013 年度 HCG シンポジウム A-1-3，pp.14-17，(2013.12).

[2] 谷村　祐*，納富一宏，斎藤恵一:"手指画像におけるカラーヒストグラム間のバタチャリヤ距離による生体認証手法　～認証システムのパラメータ調整～"，電子情報通信学会 2013 年度 HCG シンポジウム I-2-4，pp.541-544，(2013.12).

[3] 谷村　祐*，納富一宏，斎藤恵一:"手指画像におけるカラーヒストグラム間のバタチャリヤ距離による生体認証手法の提案"，バイオメディカル・ファジィ・システム学会 第 26 回年次大会講演論文集，pp.19-22，(2013.10).

[4] 牧野隆典*，山田健一朗*，納富一宏，斎藤恵一: "スマートフォンにおけるパターン認証の強化～軌跡情報および傾き情報に基づく生体認証～"，バイオメディカル・ファジィ・システム学会 第 26 回年次大会講演論文集，pp.25-28，(2013-10).

[5] 山田健一朗*，納富一宏，斎藤恵一:"スマートフォンにおけるフリック操作を用いたバイオメトリクス認証手法—システム利用環境を想定した検証—"，バイオメディカル・ファジィ・システム学会 第 26 回年次大会講演論文集，pp.77-80，(2013.10).

[6] 市村亮太*，納富一宏，斎藤恵一:"スマートフォンにおけるリズム認証手法実用化のための検討"，バイオメディカル・ファジィ・システム学会 第 26 回年次大会講演論文集，pp.81-84，(2013.10).

[7] 山田健一朗*，納富一宏，斎藤恵一: "スマートフォンにおけるフリック操作を用いたバイオメトリクス認証の基礎的検討"，情報処理学会 第 12 回情報科学技術フォーラム(FIT2013)講演論文集，第 4 分冊，L-019，pp.251-252，(2013.09).

情報漏洩に向けた新方式の研究

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学科　　氏名 岡本 学

１．研究の目的

情報漏洩問題が近年多発している。外部からのアタックによる流出や内部者による持ち出し等、様々なケースがあるが、これらを防ぐことは情報セキュリティ上の重要な課題である。そこで本研究では、新しい漏洩防止方式の提案を目的とする。なお研究内容としては、アプリケーションに近い実用的な方式提案から、それらを成り立たせるための個別の要素技術まで幅広く行う。

２．研究の必要性及び従来の研究

これまでの情報漏洩対策としては暗号化やアクセス制御といった「防御」技術が中心であった。防御技術の場合、利便性が犠牲になるケースが多く、スムーズな情報活用に支障をきたす場合がある。

そこで新しい研究では、安全な情報の「流通」に重点を置く必要がある。たとえば自分の住所や電話番号等の個人情報は、インターネットのサービスを利用する際にたびたびフォームに入力することを即されるが、これらを自動提供することはユーザ操作の観点から見ればかなり効果的な技術である。しかし当然個人情報であるから取り扱いは注意すべきであり、漏洩対策をきちんととる必要がある。

現在はクラウドと呼ばれるネットワーク側に情報を預ける方式が発展を続けているが、本研究ではその逆に「自分の手の中に情報をもつ」ことで安全な情報管理を行う方式について研究を行う。常に自身の手の中で情報を管理することは安全性や情報そのものの信頼性につながる重要な情報管理の一手法である。

３．期待される効果

「Information in a hand」＝手の中の情報、の考え方は情報流通において様々な効果を生み出す。自身の手元に情報があれば、情報漏洩に関してはあくまで自身だけが管理者であり、つまり自己管理がすべてとなる。サーバ側に情報を預けた場合は、そのサーバが外部からアタックを受けて情報漏洩したり、サーバ側の管理者が悪意をもって情報を流出させたりする場合が考えられる。さらに情報が手元にあれば最新の情報にすぐに更新ができ、情報の信頼性が上がる。またこれら個人情報の自動入力をソフトウェア等で行う場合、外部のサーバに委託する場合は少なくともそのサーバには情報が漏れ出てしまうことになり、余程信頼性の高いサーバでない限りは情報を預けることはできない。一方で、手元にある情報を手元で自動入力する場合は安全に守られるため漏洩する可能性を低く抑えられる効

果がある。

４．研究の経過及び結果

「Information in a hand」＝手の中の情報、の第一として、「認証情報」を手元におく方式の研究を行った。特にはシングルサインオンと呼ばれる方式において重要な起点となる「認証サーバ」を手元におく方式について研究した。

シングルサインオンとは、ある一つのサイト上で認証を受けることで、複数サイトの認証を完了できる方式である。認証処理の中心はアイデンティティ･プロバイダ(IdP)と呼ばれるサーバが行う。本研究では USB フラッシュドライブ上で運用する個人的な IdP について提案を行った。この方式によればサービスサイト側は IdP としてローカルホスト（127.0.0.1）を 選択すればよいため管理が簡易で済む利点もある。本方式については[1]にて学会発表を行った。

さらには「ネットワーク機能」を手の中にもつ方式についても研究を行った。特には、通常はネットワーク上に配置されているプロキシサーバをパーソナルかつポータブルに活用する方式について研究を行った。具体的には、USB メモリにプロキシサーバを入れて持ち歩くことで新たな機能及びセキュリティの追加等が可能な方式について研究を実施した。実際、プロキシサーバのパーソナル化及びポータブル化，更に加えてインテリジェント化を下記のように実施した。

「① USB メモリ上にセットアップ可能でありユビキタスに持ち運び利用することができるプロキシサーバ」、「②どのような PC 及びブラウザからでも利用可能な点でポータブル・ブラウザと住み分ける方式」、「③ USB メモリのハードウェア特性を生かして，USB 使用者＝所有者のユーザならではのパーソナル化を行う」、「④ 様々な HTTP サービスをプロキシサーバ上で追加しインテリジェント化する」、以上の観点である。

なお実際の機能としては、「URL フィルタリング」(個別フィルタリング設定が可能な方式)「閲覧履歴の活用」(先ほどまで家で見ていたネットのページについてプロキシ上の履歴を確認することで，URL をメモする等の面倒なしに，外出先でも継続してページ閲覧が可能な方式)「シングルサインオン」(プロキシサーバが認証サーバを兼ねる方式)「属性情報の自動入力」(名前や住所等のフォーム情報への自動入力)、これら機能を実現することができた。なお本研究は[2]として国際会議にて発表を行った。

５．今後の計画

今後は情報漏えい防止手段のさらなる追加技術として「強い認証」の導入を行っていく。「強い認証」を行うためには、複数サーバ認証や、認証強度によるポイント化、認証サーバの順序規定など、新しい観点を導入していく必要がある。

さらにはパスワード認証のような従来よく用いられている技術についても、その入力方式を改善することで「強い認証」に近づけていく方式の研究も行っていく。

５．研究成果の発表

以下、学会口頭発表（査読なし）１件、国際会議口頭発表（査読あり）１件である。

[1] 石射嵩広，岡本学，“IdP を持ち歩く”，電子情報通信学会 2014 年暗号と情報セキュリティシンポジウム(SCIS2014)， 2014 年 1 月，鹿児島.

[2] Kaoru Azumaya, Shori Sato, and Manabu Okamoto, “Personal Portable Proxy on a USB Flash Drive”, 2014 International Conference on Information Security and Artificial Intelligence (ICISAI 2014), Hanoi, Vietnam, 2014.2.

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
（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）

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・音声および音楽等、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する。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。そこで本研究では、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する。提案した拡散系列がM-ary方式において画質の劣化を抑制するのにどの程度効果があるのかについて検討し、その有用性について明らかにする。

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。

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。しかし、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設計すれば、通信分野で研究されている拡散系列を流用した場合よりも画質劣化を抑制することが可能であると期待される。

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、本研究では、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する。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、本研究では、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する。本研究で提案する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。今回提案した拡散系列、二次元直交系列、単純な疑似乱数の三つを用いて、実際の画像に透かし情報を埋め込んだ場合において、必要となる埋め込み強度を基準として検討を行った。検証結果より、全体的に見て提案した拡散系列は、画質劣化を抑えられるということが明らかとなった。特に、拡散系列の大きさが小さく、拡散系列の個数が多い場合に、すなわち、埋め込む必要のある情報量が多い場合に、提案した拡散系列の有用性が強く表れていることが明らかとなった。さらに、透かし情報を埋め込んだ画像をJPEG圧縮した場合についても検証を行ったが、圧縮なしの場合と同様に提案した拡散系列が優れた特性を有する結果となった。

５．今後の計画

今回の検証では、画像に対してDWTを施した周波数領域のLL成分に透かし情報を埋め込んでいるが、他の位置へ透かし情報を埋め込んだ場合の特性についても検証することにより、最適な埋め込み位置を明らかに必要がある。また、JPEG以外の圧縮形式においても提案した拡散系列が優位性を保持しているのか明らかにする必要がある。さらに、他の周波数変換を用いた場合においても、提案した拡散系列の優位性や最適な埋め込み位置、圧縮に対する耐性などについて同様に検証を行う必要がある。

６．研究成果の発表

特になし。

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の検討

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。

25年度の課題としては、24年度に考案し特許出願を行った認証方式の認証性能評価実験を行い、有効性の確認を行うことにあった。

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 年度に実施した考案した手法の認証性能評価を行うことは、本提案の有効性をはかる上で不可欠な実験である。

3．期待される効果

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

加えて、提案方式で利用する機器は、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。

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。

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。

また現在のシステムにおいて、カードをかざす動作はかなり限定的な位置制約を行っているが、利用者負担を軽減するためには非接触カードを機器にかざす程度の動作で認証を実現する必要がある。そのため、より広角に取得した画像からでもカード位置を正確に検出する手法の開発が必要であり、今後検討を進める計画である。

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（査読通過、発表予定）

- 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

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

セキュリティと法制度

研究者名:　基礎・教養教育センター　山本　聡

1．研究の目的

「サイバー犯罪認知後の追跡可能性」「情報セキュリティとは何を守るのか」

警察庁は、「サイバー犯罪認知後の事後追跡可能性の確保」をテーマとした検討を行っており、また、不正アクセス禁止法の改正の流れに乗り、トレースバック技術の有効性を前提にサイバー犯罪捜査を行っている。トレースバックは有効な技術ではあるが、複雑化するネット環境や国際間の協力など技術以前の様々な課題もあり、電話のように全て IP の逆探知で犯人を特定できるとの過信は、PC 遠隔操作事件のような冤罪を生み出してしまった。ハッカーの技術が警察の取り締まりを先んじている現状を踏まえ、サイバー犯罪への対応を警察と専門家の連携でより有効な施策となるよう現状を分析・検討する。

2．研究の必要性及び従来の研究

最近のサイバー犯罪では、大半が詐欺(オークション利用詐欺を含む)や児童買春・児童ポルノ法違反・わいせつ物頒布・出会い系サイト規制法違反といった性風俗関係のネットワーク利用犯罪であることから、ハッカーが自らの実力を顕示することが主目的であるホームページ改ざんやウィルスの作成・頒布などは、不正アクセス禁止法違反の中では実害が少ないという認識もあり、警察の動きが鈍く、専門的技術を持ったハッカーの行為を従来の犯罪行為のように取り締まろうという認識も薄い。こうしたサイバー犯罪の発生を抑止するためには、犯罪を確実に検挙し、犯罪企図者に「サイバー犯罪を行えば必ず捕まる」という意識を抱かせることが重要であり、確実な取締りを実現するためには、現実空間と同様、捜査機関が捜査を進めるに当たって犯人の特定及び検挙が可能な捜査環境が整備されていなければならない。

しかし、実際の捜査においては、犯人は捜査機関の追跡を免れるために、あらゆる手段を用いて捜査機関の捜査をかく乱させ、これにより捜査が円滑に行われないことがしばしばある。このような手段としては、広く国民に普及している通信機器やサービス、通信手段・環境の構造(ネットカフェなど)を巧妙に利用したものが多く、それらの構造自体が犯罪捜査における事後追跡上の障害となっている場合が見られる。

平成 25 年度総合セキュリティ対策会議(警察庁)では、「サイバー空間の脅威に対処するための産学官連携の在り方」～日本版NCFTAの創設に向けて～をテーマとして選定し、サイバー空間の脅威に対処するための我が国における産学官の連携の在り方について、米国に設立されたNCFTAを参考に、以下のような項目について検討を行っている。1)サイバー空間の脅威に関する産学官の保有する情報の集約・分析の在り方、2)サイバー空間の脅威に関する産学官の連携による研究開発の在り方、3)捜査機関等の職員に対するトレーニングの提供の在り方、4)海外

の関係機関等との連携の在り方等について議論された。その結果、平成26年3月に「サイバー空間の脅威に対処するための新たな産学官連携の在り方 ～日本版 NCFTA の創設に向けて～」という報告書を取りまとめられた。

3．期待される効果

情報セキュリティ分野の先進国である米国では、サイバー空間の脅威に対処するための

産学官の情報共有と協力を促進する枠組みとして、NCFTA（National Cyber-Forensics & TrainingAlliance）が平成9年に設立されている。この NCFTA は、"Industry First"をモットーとして、産業界が直面するサイバー空間の脅威に産学官が共同して対処するため、それぞれが持つ情報を共有・分析し、法執行機関の犯罪捜査、民間企業における情報セキュリティ、学術界における人材育成に大きく貢献している。今後、安全で安心なサイバー空間を実現させていくためには、事後追跡可能性の確保に基づき、通信手段・環境に関わる民間事業者との協力がより重要となる。

我が国の脅威の現状及びそれに関する課題を踏まえると、サイバー空間の脅威に関する生の情報や脅威に対処するための技術・知見等を有する産業界と、情報通信技術に係る研究開発等を通じて貢献する学術機関、そして、証拠の差押えや被疑者の逮捕を始めとする捜査権限を行使できる警察等の間で、それぞれが持つサイバー空間の脅威への対処の経験を、その場限り・当事者限りのものとせず、全体で蓄積・共有し、個別的・事後的な受け身の対応ではなく、警察による捜査権限の行使を始めとする先制的・包括的な対応を可能とする産学官連携の新たな枠組みである日本版 NCFTA を創設する必要がある。

4．研究の経過及び結果

「警察政策フォーラム 」の「サイバー攻撃・不正アクセス対策フォーラム」（2014.2.28 グランドアーク半蔵門） に参加し、「サイバー攻撃の脅威と対策」（警察庁警備企画課課長補佐 間仁田 裕美氏）、「不正アクセス防止対策に関する取組」（警察庁情報技術犯罪対策課専門官 人見 友章氏）、「不正アクセス禁止法改正案の概要」（警察庁情報技術犯罪対策課課長補佐 蔵原 智行氏）の報告および、武田 圭史氏 （慶應義塾大学教授）、佐藤 慶浩氏 （日本ヒューレットパッカード株式会社個人情報保護対策室長兼内閣官房情報セキュリティセンター指導専門官）、星 周一郎氏 （首都大学東京教授）を交えてのパネルディスカッションに参加し、サイバー・テロやサイバーインテリジェンス対策、不正アクセス防止対策を含むサイバー空間の脅威に対する総合対策を論じ合った。

原子力や防衛に携わる企業や国会、政府機関等に対する標的型メール攻撃事案等が相次いで明らかとなり、サイバー攻撃が国の安全保障に影響を及ぼしかねない問題でもあり、サイバー空間の脅威に対する社会全体の対処能力を強化することが喫緊の課題となっているとの認識が高まった。このようなことから、警察庁では「サイバーインテリジェンス情報共有ネットワーク」を構築し、事業者等との情報共有を推進している。また、サイバー空間の脅威に対して警察の各部門が連携して総合的な対策を推進するために、平成 23 年 10 月に「サイバー空間の脅威に対する

総合対策推進要綱」を制定。不正アクセス防止対策については、平成 23 年6月に警察庁等の関係省庁や民間事業者、関係団体等で構成される「不正アクセス防止対策に関する官民意見集約委員会」を設置し、同年 12 月には「不正アクセス防止対策に関する行動計画」が取りまとめられ、現在必要な施策の整備が行われている。このように、サイバー・テロやサイバーインテリジェンス対策、不正アクセス防止対策を含むサイバー空間の脅威に対する総合対策の策定が望まれる。

5. 今後の計画

セキュリティーのテーマの方向性に個人研究として限界があること、及び学内の業務多忙のため 25 年度限りで任期を終える所存である。

6. 研究成果の発表

犯罪社会学会第 40 回大会 (2013 年度 北大)において、サイバー犯罪の現状と今後の課題を報告するとともに、多数の研究者と議論を交わした。

以上

研究課題名「セキュリティと社会、危機管理」

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

情報通信技術（ICT）を備えた様々なデジタル機器の普及や、それらが提供する情報ネットワークは、今日の便利で豊かな社会に不可欠なものとなった。他方で、ICTがもたらす新たな通信手段（SNS）や情報収集法の変化、ビッグデータの活用や人工知能の進展は、相互に影響し合い、急速な発展を遂げている。それによって、ICTを利用する人々のコミュニケーションのあり方だけでなく、情報や知性に関する意識や安心安全に関する考え方、自己や社会に関する認識をも変容させ、社会的な影響が及ぶと予想される。加えて、急速な技術の進歩や社会変動と、緩やかな人々の意識変容との間に生じるずれ（タイムラグ）は、新たなリスクや社会問題をもたらすと指摘できる。

想像をしのぐ速さで進展するICTは、それゆえ情報技術をめぐる人々の見解を、相反する両極へと引き裂く。今日の高度情報化社会では、多様な領域において二項対立が存在する。例えば、社会＝経済的な領域では、ビッグデータは未開の巨大な情報市場として再発見され、産業構造の再編を促進すると期待されている。他方で、行き過ぎた情報収集や国家による監視に対する反対運動も起きている。学問的な領域では、情報技術の進展によって（ヒッグス粒子の発見など）大きな研究成果を上げたり、ビッグデータの登場によって統計技術と行動科学が人々の行動を予測可能にすると期待されたりしている。他方で、情報技術がもたらす統計的予測への過度な依存は、人々の自由意志や人間らしさを侵害する倫理的な問題を孕むと危惧され、画像処理によって敵味方を自動で判断し殺傷する殺人ロボットを禁じる国際条約も検討されている。また、情報セキュリティに関しても、同様である。事件が報道される度に人々は、自分は大丈夫だという根拠なき楽観とやみくもに恐怖する過度な悲観という二項対立に揺れがちである。

そこで本研究では、組織内情報セキュリティモデルの高度化に向けて、ICTの進展が人々の情報への接し方やリスクへの対応の仕方（人々の認知図式や行動様式：情報社会のハビトゥス）をどのように変容させるのか考察・調査を行い、新たなセキュリティ概念の可能性を検討・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

今年5月4日付のウォール・ストリート・ジャーナルは、シマンテック社の情報セキュリティ担当上級副社長ブライアン・ダイの「ウィルス対策ソフトは死んだ（Antivirus is dead)」という発言を紹介した。ダイはまた、従来のウィルス定義ファイルを用いた防止策

では、全体の 55%もの攻撃を検知できないことを指摘している。今日では、興味関心を同じくする見知らぬ人々と、インターネットを介して時空を超えてつながり、自在に意見や知識を共有することが可能である。これは、組織内情報セキュリティを脅かそうと企むハッカー達にとっても同様である。そのため、発見されたものの未だ対策が取られていない脆弱性を突いたゼロデイ攻撃や、サイト閲覧だけで未定義の亜種に感染するドライブバイ攻撃、人々の心理的な盲点を突いて情報を入手するソーシャルエンジニアリングといった手法が共有され駆使されることで、サイバー攻撃は巧妙化している。

そこで新たに注目されているのが、ヒューリスティック検知である。実行されたファイルの挙動を解析し一般的なプログラムでは稀な（危険な）挙動を見つけると、ウィルスによるものと類推する。すなわち、ウィルスの侵入防止対策（Antivirus）ではなく、万が一侵入されても被害を最小限にとどめることを目的としている。（しかし、現時点では、ウィルス検知の精度に問題が残り、ユーザーによる使用をウィルスだと誤認する場合もある。）

従来の研究では専門分化が進み、（「4.研究の経過及び結果」で後述するとおり）それぞれの領域で同じ問題構造に直面しても、個別に研究がなされ、相同的な機能をもつ対応策を提案してきたように思われる。そのため、学際的・横断的な研究によって、見過ごされがちな学問間の共通項に注目し、高度情報化社会の時代的要請に応えられる「安心安全な社会の形成」とセキュリティについて、社会的・学術的な視点から新しいセキュリティ概念を検討・提案する必要が生じている。

3．期待される効果

来たる高度情報社会の「安心安全な社会の形成」とセキュリティについて、また今日の情報技術の進展がもたらす社会的・学術的な影響について、社会変動とハビトゥスに注目した社会学の視座から検討することには、2つの効果が期待される。

1つは、学際的な視点から、現実社会に対する改善策を検討し提案することである。情報革新がもたらす社会変動というマクロな視点から現代の社会現象を位置づけることで、専門分野や研究領域の細分化によって見落とされがちな、情報社会における技術－産業－個人の関連性を把握することができる。それにより、新たに学際的な視点から、現状の社会問題に対する改善策を検討することができると考える。例えば、急激な社会変動に対する人々のハビトゥスの緩やかな変容というタイムラグがもたらす問題について、学校現場におけるメディア教育で対応しきれるものではないとするならば、どのような対応が可能だろうか。サンスティーンらが提唱した「ナッジ」は行動経済学の概念であり、またレッシグが構想した 4 つの行動要因（道徳教育、経済報酬、法規制、環境設計コード）のうちのコード概念にも近似的である。ここから、ナッジやコードといった概念を、どのようにセキュリティ技術へと応用可能か、その糸口を提案することができる。

2つ目は、現代の社会変動によって、学術研究そのものが受ける影響を考察することが可能となる。マイヤー＝ショーンベルガーは、ビッグデータの登場が既存科学の再編を迫る

ものであると指摘している。統計技術と行動科学の予測によって、因果関係よりも相関関係が重視されるとともに、「安心安全な社会の形成」とセキュリティという面では犯行を罰するよりも予防や予兆発見に傾注する可能性が言及されている。言い換えれば、膨大な情報データ（利用ログやテキストなど量的・質的なデータ）に基づいて高度な客観的予測が可能となる社会では、相関関係に基づいて同定された犯行に結びつく特定の条件が揃った人物に対して「犯行の確率が高い」という理由で監視・矯正するようになるかもしれない。監視対象となっていることが分かると、周囲の人々は当該人物をあたかも犯罪者のように警戒し差別するかもしれない。このような行き過ぎた客観主義の台頭に対して、自由意志や人間らしさといった価値が侵害されると警鐘を鳴らしている。現実的な情報セキュリティの在り方について検討することは、ひるがえって、これら学術的な価値の対立について再検討する契機を内包しているといえる。（社会学のハビトゥス概念自体も、客観主義と主観主義、構造主義と実存主義、社会決定論と自由意志論といった現代思想上の二項対立を超克する過程から構想されたものであり、セキュリティ概念の検討を通じて社会学理論の研究にも今日的な視点を導入することができよう。）

４．研究の経過及び結果

社会学のハビトゥス概念に立脚し、情報技術の進展と人々のハビトゥスとのずれに注目して、最新事例の問題構造を抽出し検討した。2013 年の夏に開催された Black Hat（ハッカーの国際会議）では、ハードウェア（iPhone の充電器）を経由した攻撃が実演された。ハードウェアまでもセキュリティの対象になると話題になったが、インターネット経由でも、ハードウェア経由でも、問題構造は同じである。人々が「安全」だと信じる空間を攻略し、認識にギャップ（ずれ）を生じさせることこそ標的となる。また、同年の夏は、日本の若者たちによる悪ふざけ自慢の画像投稿が twitter 上で相次ぎ、「バカッター」と揶揄された。これもまた、若者が電話やメールの延長として友人との「私的な交流の場（通信メディア）」だと誤認した SNS が、実際にはインターネット上の「公的な情報開示（情報メディア）」だという認識のずれに起因した社会問題である。ここから明らかとなるのは、情報流出・情報漏洩を生じさせないことを目指すのは困難である（問題は認識のずれによって生じるため、刻々と変化し、イタチごっことならざるをえない）ということである。それゆえ、情報セキュリティは、流出・漏洩が生じても最小限の被害でとどまることを目標とする必要があるということである。近年注目を集めている、技術面での「プライバシー・バイ・デザイン」や、法律面での「忘れられる権利」は、いずれも上述のセキュリティ機能を備えているものと位置づけられよう。

他方で、社会学理論の面では、認知図式や行動様式は転移するというハビトゥス概念の特徴に注目して、ビッグデータの活用がもたらす「効率性」の社会的影響を検討した。1 つ目は、過去－現在－未来という時間構造が、社会に与える影響である。ビッグデータが「過去」の業績や傾向によって人々を効率的に分類し、その結果に応じて人々の「現在」の対

応に区別を設けることは、やがて人々に「当然の帰結」として社会的格差の存在そのものを正当化する効果を及ぼしうる。例えば、Google の検索表示結果や Amazon のおすすめ商品機能は、利用者（ユーザー）の「過去」の入力結果に応じて、利用者ごとに異なる「現在」の画面表示を行うようカスタマイズされている。このような「効率性」の追求が、検索結果の表示だけではなく、現実社会の生活機会（ライフ・チャンス）の様々な場面で機能するとしたら、各自の出生時の家庭環境の格差が再生産されてしまうのではないか。2 つ目は、社会空間上の格差を「見える化」することで、他者との比較における相対的剥奪感・不当感を抱きやすくなり、階級対立が深刻化する可能性である。アメリカでは、高額所得者だけが集まる地域が、市として独立を果たした。これまで、高額所得者から徴収した高い税金を低所得者の教育や医療などの福祉へと充て、社会的な富の「再分配」を行ってきた。しかし、良いサービスが受けられる私立校や民間病院を利用する高額所得者にとって、これらの福祉政策は「非効率」と映る。このように、他者のデータと比較し、自分の損得を計算する「効率性」（ここでは福祉政策への糾弾と弱者の社会的排除）がいっそう普及すると、国家や社会の根源を揺るがしうる。

５．　今後の計画

今後は、理論研究に加えて、実証研究を実施することを予定している。具体的には、学生へのアンケート調査によって、日常生活における情報への接し方、効率性への志向や情報セキュリティに関する意識の実態などを把握する。学生の ICT 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。

理論研究の面では、人々の認知図式と行動様式を分析する社会学のハビトゥス概念に立脚し、時代の変化が社会集団ごとにどのような変容を促すのかに注目して検討を行う。また、情報セキュリティをめぐる加害者と被害者という二項対立や、ICT のソフトウェアの脆弱性と人々のミスや盲点という二項対立に陥らずに、問題構造をトータルに把握できるよう、ソーシャルエンジニアリングの手法や、行動経済学、認知心理学など他領域の研究成果を社会学に取り入れ、情報社会における技術・産業・個人の関係を分析して、現代の情報社会における新しいセキュリティ概念の考察を行う。得られた社会学的知見を全体と統合化し、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] MIURA Naoko “Information Technology and its Social Influence: Considering the concept of security”, KAIT International Symposium 2013 (2013.08), Kanagawa Institute of Technology（査読無し国際シンポジウム）.

[2] MIURA Naoko “Social and Intellectual Antinomies of Information Technology”, XVIII ISA World Congress of Sociology, International Sociological Association (ISA 2014.07), Yokohama Japan（Accept 済，査読あり国際会議）.