L-004

適応認証技術に関する現状と今後の考察
Current Status and Future Considerations of Adaptive Authentication Research

原大司 † 金岡晃 ‡ 櫻井幸一 †

Daiji Hara Akira Kanaoka Koichi Sakurai

1. はじめに

現代では様々なオンラインサービスがその利用に，利用者の認証を必要としている．認証は，そのシステムが脆弱であると攻撃者の標的となる．認証システムの強度は，当然システム自体の頑丈性が重要になるが，そのシステムを利用するユーザーのセキュリティ意識も同様に重要である．その際に考慮すべき課題として，システムのユーザビリティが存在する．システムのユーザビリティが低いと，ユーザーのセキュリティ意識が低くなり，脆弱性に繋がるという課題が存在する．

その課題を解決する認証方式である，適応型認証が現在盛んに研究されており，注目を浴びている．適応型認証とは，ユーザーの文脈に応じて認証を適応的に行うことで，セキュリティとユーザビリティを両立する方式をとっている．

本論文では，まず Arias-Cabarcos らによる適応型認証のサーベイ [1] を参考に，適応型認証が持つ性質と認証に用いられる認証子について解説する．次に，適応型認証についての既存研究の紹介を調査手法や実験手法を中心に解説する．その後，現在の COVID-19 による社会情勢の急激な変化において，認証子の価値がどのように変化するのかについて考察を行う．最後に，本論文のまとめを行うことで，本論文を締めくくる．

2. 適応型認証

この章では，Arias-Cabarcos らが適応型認証について調査した内容について説明していく．適応型認証の考え方は，2000 年代初期に Jalal らの研究 [9] で登場している．その後，この認証システムをスマートフォンやウェブへの認証に用いるために，暗黙認証子 (implicit authenticators) と連続認証子 (continuous authenticators) の組み合わせが用いられている．暗黙認証子とは，ユーザーが意識しないで用いられる認証子のことであり，連続認証子は，ユーザーがシステムを用いている間連続的に検証される認証子のことである．適応型認証は，ユーザーの文脈に応じて認証を適応的に行うことができるため，セキュリティとユーザビリティの両立が行える方式となっている．

2.1. 用いられる認証子

適応型認証に用いられる認証子は，通常の認証技術と同様に知る要素 (What You Know)，持つ要素 (What You Have)，生体要素 (What You Are) の三つの要素に分類することができる．知る要素は，パスワードや PIN などが該当し，持つ要素は USB キーや RFID が該当する．生体要素はさらに生理的要素と行動的要素に分類することができる．生理的要素には虹彩や顔，指紋情報などが該当し，行動的要素にはキーストロークや足取りなどが該当する．それぞれの認証子は多様性，連続性，接続性という性質を持っている．適応型認証システムを設計する際には，どの認証子を用いるかによってそのシステムの特性が決定される．そこで以下では，適応型認証システムを設計する際に必要となる，認証子のそれぞれの性質について説明する．

2.2. 認証子の性質

2.2.1. 多様性

認証子の多様性とは，一つの認証システムが利用できる認証子の種類のことである．この種類が多い適応型認証システムは，様々な場面に対して適応できるようになる．Arias-Cabarcos らが既存の研究に用いられる認証子について調査を行ったところ，知る要素は多くの研究で用いられているが，持つ要素はあまり用いられていないという結果が得られた．また，生体要素は知る要素の補完としての役割が多いということも判明した．この理由として，ほとんどの既存研究が適応によるユーザビリティの向上に焦点を当てているからと Arias-Cabarcos らは考えた．生体要素は暗黙的に認証を行うことができるため，ユーザビリティの向上という点において研究対象として扱いやすい．しかし，現実に用いられている認証システムは知る要素，持つ要素を用いていることが多く，生体要素を用いているものは少ないというギャップが発生している．また，Arias-Cabarcos らの調査によると，最も多種の認証子を用いた研究は Gupta らの研究 [2] で 15 種類であったと述べられている．

2.2.2. 連続性

認証子の連続性とは，正当なユーザーによる利用をリアルタイムで監視することができる性質である．これによりたまたま一回成功したような不正アクセスを防ぐことができる．Vishal らによる研究 [3] では，適応型認証における連続認証子について調査を行なっている．この結果，連続認証子としては行動的要素かトークンのみが用いられていることが判明した．ここでのトークンは二つの手法で生成することができ，一つはユーザーを識別する位置情報を送信するビーコンを用いることで得られ，もう一つは RFID などを複数取り付けることによって共有秘密を計算することによって得られる．後者は日常的なオブジェクトをトークン化することができるが，こういったオブジェクトによるトークンは，盗難などの危険を孕んでいると Toader らの研究 [10] は指摘している．

†九州大学 Kyushu University
‡東邦大学 Toho University

2.2.3. 接続性

認証子の接続性とは，新しい技術が生まれた時の統合可能性のことである．これによりシステムは高いユーザビリティを得ることができる．新しく頑丈な認証子やデバイスが開発された際には認証システムの改善が必要になる．その際に全く新しい認証システムを設計するとなると多大な労力が必要になるが，現行の認証システムに新しい要素のみを組み込むだけでよければ，その労力は最低限で済む．PAM[4] は，システムを再コーディングしないで済むインターフェースであり，認証システムの設計にはこれを利用するべきである．今回 Arias-Cabarcos たちが調査した既存研究の中では，4 つの研究 [9, 11, 12, 13] のみが接続性について考慮したシステムの設計を行なっていた．

3. 認証子の連続性に着目した適応型認証研究

私たちは 2 章で紹介した認証子の性質の内，認証子の連続性について着目し調査を行った．適応型認証は，認証を行うユーザーの文脈により認証方式を適応することができるという点でメリットがあり，連続性がこのメリットに関わる最大の特徴と考えられるためである．この章では認証子の連続性に着目している既存研究の紹介を行う．

3.1.UFSA(User-Friendly and Secure Archiecture)[5]

UFSA は明示認証子 (explicit authenticators) と暗黙認証子を用いた適応型認証を提案している．明示認証子とは，ユーザー自身が意識して用いる認証子（例：パスワード，SMS コードなど）であり，暗黙認証子とは，ユーザーが意識をしないで用いられる認証子（IP アドレス，時間情報など）のことである．このシステムの構成図を 1 に示す．性能を測定するために，Naive 法と Greedy 法との比較を行う．Naive 法は認証子の選択手法として，最も簡単に使用できる認証子の選択を行う．Greedy 法は困難が高い認証子を優先的に選択する．この比較を行うに当たって，各明示認証子に対して，ユーザーにはあらかじめそれぞれの主観で困難度を設定させておき，管理者はサービスを利用するための閾値 (Operation Sensitivity) を設定しておく必要がある．暗黙認証子による重みと困難度により最終的なスコアが計算され，その値が閾値を超えるとユーザーはサービスを利用できる．UFSA は Greedy 法と比較して最大 18%，Naive 法と比較して最大 20%ユーザーが感じる困難が低いことが結果として得られている．

3.2.Smart Auth[6]

この研究では，ForgeRock 社が提供する OpenAM 上に実装する適応型認証のフレームワーク SmartAuth を提案している．SmartAuth は，認証に用いる認証子の選択を Hoeffding 木を用いて行っている．SmartAuth では，データを類似性保存ハッシュ関数に通してフィンガープリントに変換したものを，認証子として利用している．このシステムの構成図を図 2 に示す．作成したフィンガープリントに対しタイムスタンプなどの情報を加えることで，その認証子を用いて認証を行なうか否かの判断が行われる．この手法により，99%の精度で良悪性の分類を可能とした．これを 6 人に対してユーザー実験を行ったところ，被験者達は概念レベルで SmartAuth の価値を理解した．しかし，被験者達は技術的な背景を持ち合わせており一般人とは言えない点，ユーザー実験には人数が不十分である点で課題が残った．

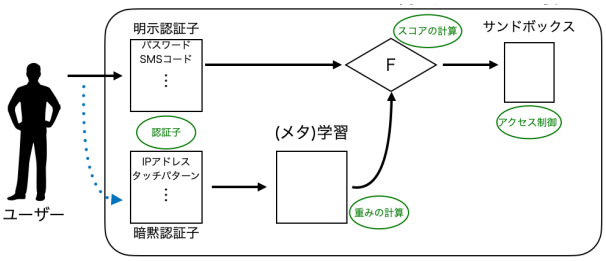

図 1: UFSA のシステム構成図

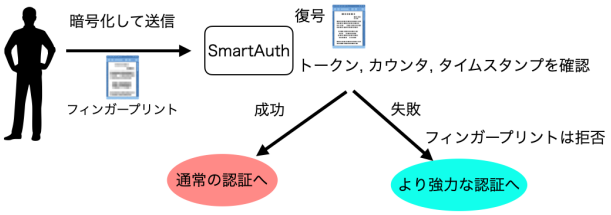

図 2: SmartAuth のシステム構成図

3.3.ASSO(Adaptive Single Sign On)[7]

ASSO はシグルサインオンシステムを適応型にした研究である．この研究の目的は，認証に必要なセキュリティレベルを保ちつつ，ユーザビリティを向上することである．この研究では，168 人からデータを収集している．168 人の参加者がスマートフォンを所持し，一年間に渡って位置情報と時間情報のデータを蓄積した．端末に保存されたデータは特定のアクセスポイントを検知した際にデータベースにアップロードされる．最初の一ヶ月に収集したデータを訓練データ，残りをテストデータとし，SVM によって分類モデルを作成した．これにより，再現率 87.7%，適合率 88.4%という結果が得られた．既存研究では用いられていない位置情報を認証子に用いている点，実際のモバイルデータを用いた実験を行っていることがこの研究の貢献である．

3.4.Reinforced Auth[8]

この研究は，疑わしいログインを識別するフレームワークの開発を行っており，大規模データセットを効率的に評価できるプロトタイプを実装している．本研究のシステム構成図を図 3 に示す．ユーザーがログインを試行したとき，そのユーザーがのログイン履歴，用いている認証子を確認する．それらの情報を基にスコアを計算し，それによりログインを 3 種類に分類する．この実験では，偽陽性率を 10%固定で真陽性率を計算することで ROC 曲線を描き，その AUC により性能を測定している．これにより，ボットネットに対しては

10%の偽陽性率で 95%の検知が可能であり，アカウント侵害に対しては 10%の偽陽性率で 77%検知が可能という結果が得られた．この実験で使用した認証システムと同様の方式が既に大規模ウェブサイトで利用されているが，この研究はこの方式を最初に分析し，ベンチマークを提供したという点で貢献している．

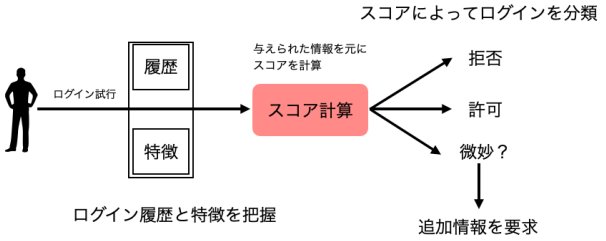

図 3: ReinforcedAuth のシステム構成図

4. 認証子に関する考察

適応型認証は，その認証を行うユーザーの文脈により最善となる認証子を選択する．しかし，認証子はそれ自体の価値が急激な社会情勢の変化に伴って変動する可能性がある．この章では，現在の COVID-19 による社会情勢の急激な変化に伴う環境（以下 COVID-19 環境）によって，認証子の価値がどのように変動するかについて考察を行う．

4.1. 位置情報

認証を行うユーザーの位置情報も認証の要素になる．位置情報を要素として用いるメリットとして，認証を行うユーザーがどこにいるのかを連続的に判断することが可能であること，過去のログイン履歴から考えられない場所からのログインの場合，ログインの安全性に対して疑問を持つことができることなどが存在する．しかし現在の COVID-19 環境では，テレワークや外出が自粛されており，自宅にいる機会が多くなっている．このことから，位置情報は COVID-19 環境によってその価値は変化すると考えられる．

4.2. 時間情報

認証を行うユーザーの時間情報も認証の要素になる．時間情報を認証に用いることで，ユーザーがサービスにアクセスする時間を観測し，過去のログイン履歴と比較することでユーザーの正当性を確認することができる．リモートワークが推奨されている COVID-19 環境では，普段では勤務後にアクセスするようなサービスに対して，平日昼の時間帯でアクセスする可能性が生まれる．これにより正当なユーザーが不正なユーザーと認識され，より強度が強い認証へと移行されるケースが増加すると考えられる．このことから，時間情報も COVID-19 環境によってその価値は変化すると考えられる．

4.3. 持つ要素

持つ要素とは，認証を行うユーザーが所持している機器を利用することで，本人の正当性を証明するために用いられるものである．この要素が抱えるリスクとして，機器の紛失，盗難が考えられる．これは，機器が第三者（攻撃者）に渡ることで，正当な所持者になりすますことが可能であるからである．また，ユーザーは常に機器を持ち歩く必要があるという点で，ユーザビリティが低いことも考慮しなければならない．この要素を用いるメリットとしては，認証を行うユーザーはただ機器を所持していれば良いため余計な入力が必要ないという点で，高いユーザビリティを持つことが挙げられる．COVID-19 環境において，雇用者はリモートで会社のサーバにアクセスする機会が多くなっている．リモート環境では，アクセスユーザーは家から出る必要が無いため，機器が盗難される，紛失するリスクが限りなく低く，持ち歩く必要が無いため，前に挙げた低ユーザビリティに依る課題を克服していると考えられる．これらのことから，持つ要素も COVID-19 環境によってその価値は変化すると考えられる．

4.4. 知る要素

知る要素とは，認証を行うユーザーが所有している知識を用いて本人の正当性を用いるために使用される要素である．この要素は入力を行う際に生じる面倒さと，覚えておかなければならない煩雑さによって，低いユーザービリティを持っており，ユーザーからはあまり好まれていない要素である．しかし，現状最も用いられることの多い要素でもある．COVID-19 環境では外出の自粛などにより，買い物をオンラインで行うケースが増加しているため，脆弱なパスワード設定により，攻撃の被害に遭うリスクは増加すると考えられる．このリスクは従来から存在するものであり，COVID-19 環境によって頻度が変わる程度の事象であるため，知る要素は大きくはその価値は変化しないと考えられる．

4.5. 生体要素

生体要素は，要素の種類によっては COVID-19 環境に影響をうけ，その価値が変化すると考えられる．生体要素は，認証を行うユーザーの生体的な特徴を利用して本人の正当性を証明するために使用するものである．この要素はユーザー側は常に意識せず用いることができるため高いユーザビリティを保持できる．また情報を盗まれる危険性が低いため，高い強度を持つ要素である．生体要素は，以前からその強度によって評価されており，COVID-19 環境においてもその強度に対する評価は揺らぐことは無い．生体要素の種類としては，顔情報，虹彩情報，指紋情報などが存在する．このような要素の中で，その情報の取得のために物理的な接触が必要なものについては，その行為が感染経路となる可能性が存在し，ユーザーから敬遠される傾向にあるため，ユーザビリティが低下すると考えられる．このことから，生体要素も物理的な接触を必要とするものについては，COVID-19 環境によって価値が下がると考えられる．

5. 結論

本論文では，Arias-Cabarcos らの研究 [1] を参考に，それに用いられる認証子と認証子の性質を交えて説明を行った．次に適応型認証の連続性に関連する論文を紹介した．最後に適応型認証に用いられる認証子が，現

在の COVID-19 環境のような急激な社会状況の変化でどのように価値が変動するかについて考察を行った．適応型認証は，ユーザーの文脈により認証に用いる認証子を選択するものであり，本論文ではその認証子の価値が変動する場合認証子の適応の仕方についても考える必要が出てくることを示した..

参考文献

[1] Patricia Arias-Cabarcos, Christian Krupitzer, Christian Becker.: *A Survey on Adaptive Authetication*, ACM Computing Surveys, Vol. 52, No. 4, Article 80. Publication date: September 2019.

[2] Aditi Gupta, Markus Miettinen, N. Asokan, and Marcin Nagy.: *Intuitive security policy configuration in mobile devices using context profiling*, In Proceedings of the International Conference on Privacy, Security, Risk and Trust (PASSAT ' 12) and the International Confernece on Social Computing (SocialCom ' 12). IEEE, 471-480.

[3] Vishal M. Patel, Rama Chellappa, Deepak Chandra, and Brandon Barbello.: *Intuitive security policy configuration in mobile devices using context profiling*, IEEE Signal. Proc. Mag. 33, 4 (2016), 49-61.

[4] Vipin Samar.: *Unified login with pluggable authentication modules (PAM)*, In Proceedings of the ACM Conference on Computer and Communications Security (CCS ' 96). 1-10.

[5] Reza Fathi, Mohsen Amini Salehi, and Ernst L. Leiss.: *User-friendly and secure architecture (UFSA) for authentication of cloud services*, In Proceedings of the IEEE International Conference on Cloud Computing (CLOUD ' 15). 516-523.

[6] Davy Preuveneers and Wouter Joosen.: *SmartAuth: Dynamic context fingerprinting for continuous user authentication*, In Proceedings of the ACM Special Interest Group on Applied Computing (SIGAPP ' 15). 2185-2191.

[7] Zhan Liu, Riccardo Bonazzi, and Yves Pigneur.: *Privacy-based adaptive context-aware authentication system for personal mobile devices*, J. Mob. Multimed. 12, 1-2 (Apr. 2016), 159-180. Retrieved from http://dl.acm.org/citation.cfm?id=3177177.3177187.

[8] David Freeman, Sakshi Jain, Markus Durmuth, Battista Biggio, and Giorgio Giacinto.: *Who are you? A statistical approach to measuring user authenticity*, In Proceedings of the Network and Distributed System Security Symposium (NDSS ' 16). 1-15.

[9] Jalal Al-Muhtadi, Anand Ranganathan, Roy Campbell, and M. Dennis Mickunas. : *Cerberus: A context-aware security scheme for smart spaces* In Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom ' 03). 489-496.

[10] C. Toader and Frank Stajano.: *User authentication for Pico: When to unlock a security token* Master ' s Thesis, University of Cambridge.

[11] Alain Forget, Sonia Chiasson, and Robert Biddle.: *Choose your own authentication.* In Proceedings of the New Security Paradigms Workshop. 1-15.

[12] Daniel Hintze, Rainhard D. Findling, Muhammad Muaaz, Eckhard Koch, and Rene Mayrhofer.: *Cormorant: Towards continuous risk-aware multi-modal cross-device authentication.* In Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing and ACM International Symposium on Wearable Computers. 169-172.

[13] Heiko Witte, Christian Rathgeb, and Christoph Busch.: *Context-aware mobile biometric authentication based on support vector machines.* In Proceedings of the 4th IEEE International Conference on Emerging Security Technologies (EST ' 13). 29-32.