

2. CA 安全・安心確保基盤の構築

2023年度までの進捗状況

1. 概要

本研究課題では、サイバネティック・アバター（CA）を安全かつ信頼して利用できる社会の実現に向けて、利用者認証・CA 認証・CA 公証を核とする CA 安全・安心確保基盤の構築を目指します。これにより、操作者のなりすまし、CA の乗っ取り、CA 内に蓄積される技術情報等の不正取得（違法な技能模倣）などに対処します（図1）。具体的には、下記研究開発項目を分担して、プロジェクトを推進します。

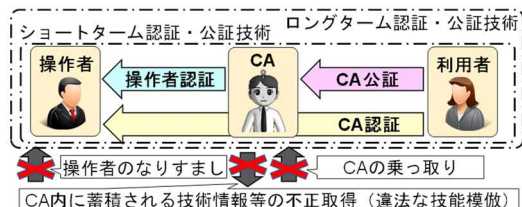


図1：CA 安全・安心確保基盤

① CA 安全・安心確保基盤構築設計

2050 年におけるアバター共生社会の未来像を「CA ビジネスショーケース 2050」という形で考察し、個々の CA サービスの未来像からバックキャストする形でアバター共生社会のセキュリティ課題を検討しています。

② ショートターム型マルチモーダル操作者認証・CA 認証

CA の操作権限の乗っ取りに対抗する技術が、操作者の認証です。CA が自身の操作者を確認する「操作者認証」と、CA と対峙する利用者が目今の CA を介して、その CA の操作者を確認する「CA 認証」の両者が必要であり、これら 2 種類の認証技術を研究開発しています。

③ ショートターム有体物 CA 公証

CA のなりすましに対抗する技術が「CA 公証」です。利用

者が、目今の有体物 CA（物理的な身体を持つ CA）が正規の CA であることを確認する技術を研究開発しています。

④ 無線指紋型ショートターム遠隔操作者認証・CA 公証

CA の利用には無線技術が欠かせません。操作者がスマートフォン・ウェアラブルデバイス・PC を使って CA を遠隔操縦する際の無線電波を、「指紋」と捉えて操作者認証や CA 公証を実現する技術を研究開発しています。

⑤ ロングターム操作者認証・CA 認証・CA 公証

操作者や CA がいつの間にか偽物にすり替わる場合にも対処する必要があります。操作者認証、CA 認証、CA 公証を継続的に担保し続けるための技術を研究開発しています。

2. これまでの主な成果

① CA 安全・安心確保基盤構築設計

未来像の1つとして、身体機能（脳・五感・臓器）がパーツ化された「IoF: Internet of Functions」の世界を考察し、「外部記憶パーツを用いた超強力パスワード認証（図2）を含む、CA 共生社会における新たなセキュリティ機構の提案と概念検証を行いました。（図2）。

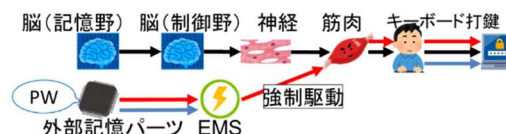


図2：人体がパーツ化されたパスワード認証

② ショートターム型マルチモーダル操作者認証・CA 認証

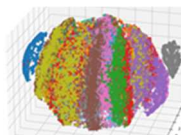
顔・全身写真・脳波・声紋・虹彩・掌静脈・生体信号（心拍を含む）・オンライン署名・歩行を含む計 8 個のモダリティの 912 名からなるマルチモーダルバイオメトリクスデータを収集し、顔認証 API のプロトタイプを構築しました。このような現実環境下での多種かつ大規模なデータセットは世界でも例を見ません。また、CA 認証のための動的特徴表現および非識別化技術に関する調査を実施しました。

③ ショートターム有体物 CA 公証

有体物 CA の高精度計測により得られる偽造困難特徴量を利用した有体物 CA の構築手法として、CA に表出する表情特徴を用いたなりすまし困難な認証方式の提案とプロトタイプシステムの構築、複数操作者による CA 操作時の認証方式の提案とプロトタイプシステムの構築を行いました。

④ 無線指紋型ショートターム遠隔操作者認証・CA 公証

Wi-Fi および BLE データ収集システムを開発し、123 台の IoT デバイスの電波データセットを整備しました。分析を通じて無線指紋に適する特徴値を同定し、認証・公証のためのアルゴリズムを開発しました。デバイス内（図3の同色点群）変動を抑えながら、デバイス間（図3の異色点群）識別を実現しました。図3：無線指紋



⑤ ロングターム操作者認証・CA 認証・CA 公証

CA 操作データのための模擬データベースを構築し、プロジェクトを越えた共通プラットフォームとして活用するための基盤を設計・開発しました。e スポーツのキャラクタ操作を CA 操作の一種と捉え、CA 操作に関するログデータを分析しロングターム認証の可能性を検証した結果、キャラクタの視線パターンなどに含まれる個性を特定しました。

3. 今後の展開

認証技術の深化のためには、豊富なデータセットが欠かせません。データセットの充実を継続するとともに、ショートターム・ロングタームの利用者認証・CA 認証・CA 公証の各技術の高度化に取り組みます。悪意をもった攻撃（敵対的攻撃）への対策、セキュリティとプライバシーの両立、技術と法制度の連携に関する研究開発も加速させていきます。CA 共生社会の未来予測を更に進め、「操作者のなりすまし、CA の乗っ取り、違法な技能模倣を防ぐために、各技術をどのように連携させるべきか」に対する解を導きます。